Ethical Hacking and Countermeasures

Version 11

Lab Manual

EC-Council

Copyright © 2020 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 may not be reproduced for publication without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law. For permission requests, write to EC-Council, addressed "Attention: EC-Council," at the address below:

EC-Council New Mexico
101C Sun Ave NE
Albuquerque, NM 87109

Information contained in this publication has been obtained by EC-Council from sources believed to be reliable. EC-Council takes reasonable measures 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 nor for 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 all over the world. Due credits for all such contributions and references are given in the courseware in the research endnotes. We are committed to protecting intellectual property rights. If you are a copyright owner (an exclusive licensee or their agent) and you believe that any part of the courseware constitutes an infringement of copyright, or a breach of an agreed license 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 us at **support@eccouncil.org**.

NOTICE TO THE READER

EC-Council does not warrant or guarantee any of the products, methodologies, or frameworks described herein nor does it perform any independent analysis in connection with any of the product information contained herein. EC-Council does not assume, and expressly disclaims, any obligation to obtain and include information other than that provided to it by the manufacturer. The reader is expressly warned to consider and adopt all safety precautions that might be indicated by the activities described herein and to avoid all potential hazards. By following the instruction contained herein, the reader willingly assumes all risks in connection with such instructions. EC-Council makes no representations or warranties of any kind, including but not limited to the warranties of fitness for particular purpose or merchantability, nor are any such representations implied with respect to the material set forth herein, and EC-Council takes no responsibility with respect to such material. EC-Council shall not be liable for any special, consequential, or exemplary damages resulting, in whole or in part, from the reader's use of or reliance upon this material.

9h\JW'< UW]b[UbX7ci blYfa YUg fYg 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	180
04	Enumeration	317
05	Vulnerability Analysis	410
06	System Hacking	494
07	Malware Threats	710
08	Sniffing	881
09	Social Engineering	1027
10	Denial-of-Service	1084
11	Session Hijacking	1123
12	Evading IDS, Firewalls, and Honeypots	1150
13	Hacking Web Servers	1215
14	Hacking Web Applications	1262
15	SQL Injection	1424
16	Hacking Wireless Networks	1470
17	Hacking Mobile Platforms	1560
18	IoT and OT Hacking	1618
19	Cloud Computing	1649
20	Cryptography	1679

9h\JW'< UW]b[UbX7ci blYa YUg fYg Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Footprinting and Reconnaissance

Module 02

Footprinting and Reconnaissance

Footprinting refers to collecting as much information as possible regarding a target network from publicly accessible sources.

ICON KEY

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

Lab Scenario

Reconnaissance refers to collecting information about a target, which is the first step in any attack on a system. It has its roots in military operations, where the term refers to the mission of collecting information about an enemy. Reconnaissance helps attackers narrow down the scope of their efforts and aids in the selection of weapons of attack. Attackers use the gathered information to create a blueprint, or "footprint," of the organization, which helps them select the most effective strategy to compromise the system and network security.

Similarly, the security assessment of a system or network starts with the reconnaissance and footprinting of the target. Ethical hackers and penetration (pen) testers must collect enough information about the target of the evaluation before initiating assessments. Ethical hackers and pen testers should simulate all the steps that an attacker usually follows to obtain a fair idea of the security posture of the target organization.

In this scenario, you work as an ethical hacker with a large organization. Your organization is alarmed at the news stories concerning new attack vectors plaguing large organizations around the world. Furthermore, your organization was the target of a major security breach in the past where the personal data of several of its customers were exposed to social networking sites.

You have been asked by senior managers to perform a proactive security assessment of the company. Before you can start any assessment, you should discuss and define the scope with management; the scope of the assessment identifies the systems, network, policies and procedures, human resources, and any other component of the system that requires security evaluation. You should also agree with management on rules of engagement (RoE)—the "do's and don'ts" of assessment. Once you have the necessary approvals to perform ethical hacking, you should start gathering information about the target organization.

Once you methodologically begin the footprinting process, you will obtain a blueprint of the security profile of the target organization. The term "blueprint" refers to the unique system profile of the target organization as the result of footprinting.

The labs in this module will give you real-time experience in collecting a variety of information about the target organization from various open or publicly accessible sources.

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

Lab Objectives

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

- **Organization Information**

  Employee details, partner details, weblinks, web technologies, patents, trademarks, etc.

- **Network Information**

  Domains, sub-domains, network blocks, network topologies, trusted routers, firewalls, IP addresses of the reachable systems, the Whois record, DNS records, and other related information

- **System Information**

  Operating systems, web server OSes, user accounts and passwords, etc.

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 200 Minutes

Overview of Footprinting

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance

Footprinting refers to the process of collecting information about a target network and its environment, which helps in evaluating the security posture of the target organization's IT infrastructure. It also helps to identify the level of risk associated with the organization's publicly accessible information.

Footprinting can be categorized into passive footprinting and active footprinting:

- **Passive Footprinting:** Involves gathering information without direct interaction. This type of footprinting is principally useful when there is a requirement that the information-gathering activities are not to be detected by the target.
- **Active Footprinting:** Involves gathering information with direct interaction. In active footprinting, the target may recognize the ongoing information gathering process, as we overtly interact with the target network.

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

Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to collect information about the target. Recommended labs that will assist you in learning various footprinting techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	iLabs ***
1	Perform Footprinting Through Search Engines	√	√	√
	1.1 Gather Information using Advanced Google Hacking Techniques	√		√
	1.2 Gather Information from Video Search Engines		√	√
	1.3 Gather Information from FTP Search Engines		√	√
	1.4 Gather Information from IoT Search Engines		√	√
2	Perform Footprinting Through Web Services	√	√	√
	2.1 Find the Company's Domains and Sub-domains using Netcraft	√		√
	2.2 Gather Personal Information using PeekYou Online People Search Service		√	√
	2.3 Gather an Email List using theHarvester		√	√
	2.4 Gather Information using Deep and Dark Web Searching		√	√
	2.5 Determine Target OS Through Passive Footprinting		√	√
3	Perform Footprinting Through Social Networking Sites	√	√	√
	3.1 Gather Employees' Information from LinkedIn using theHarvester	√		√
	3.2 Gather Personal Information from Various Social Networking Sites using Sherlock		√	√
	3.3 Gather Information using Followerwonk		√	√
4	Perform Website Footprinting	√	√	√
	4.1 Gather Information About a Target Website using Ping Command Line Utility	√		√

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

	4.2 Gather Information About a Target Website using Website Informer		√	√
	4.3 Extract a Company's Data using Web Data Extractor		√	√
	4.4 Mirror a Target Website using HTTrack Web Site Copier	√		√
	4.5 Gather a Wordlist from the Target Website using CeWL		√	√
5	Perform Email Footprinting	√		√
	5.1 Gather Information About a Target by Tracing Emails using eMailTrackerPro	√		√
6	Perform Whois Footprinting	√		√
	6.1 Perform Whois Lookup using DomainTools	√		√
7	Perform DNS Footprinting	√	√	√
	7.1 Gather DNS Information using nslookup Command Line Utility and Online Tool	√		√
	7.2 Perform Reverse DNS Lookup using Reverse IP Domain Check and DNSRecon		√	√
8	Perform Network Footprinting	√	√	√
	8.1 Locate the Network Range		√	√
	8.2 Perform Network Tracerouting in Windows and Linux Machines	√		√
	8.3 Perform Advanced Network Route Tracing using Path Analyzer Pro		√	
9	Perform Footprinting using Various Footprinting Tools	√	√	√
	9.1 Footprinting a Target using Recon-ng	√		√
	9.2 Footprinting a Target using Maltego		√	√
	9.3 Footprinting a Target using OSRFramework		√	√
	9.4 Footprinting a Target using FOCA		√	√
	9.5 Footprinting a Target using BillCipher		√	√
	9.6 Footprinting a Target using OSINT Framework		√	√

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

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

*Core - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

**Self-study - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv11 volume 1 book.

***iLabs - Lab exercise(s) marked under iLabs are available in our iLabs solution. iLabs is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed from anywhere with an Internet connection. If you are interested to learn more about our iLabs solution, please contact your training center or visit https://ilabs.eccouncil.org.

Lab Analysis

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

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

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

Lab

Perform Footprinting Through Search Engines

Search engines are the main information sources to extract critical information about a target organization from the Internet.

ICON KEY

- Valuable Information
- Test Your Knowledge
- Web Exercise
- Workbook Review

Lab Scenario

As a professional ethical hacker or pen tester, your first step is to gather maximum information about the target organization by performing footprinting using search engines; you can perform advanced image searches, reverse image searches, advanced video searches, etc. Through the effective use of search engines, you can extract critical information about a target organization such as technology platforms, employee details, login pages, intranet portals, contact details, etc., which will help you in performing social engineering and other types of advanced system attacks.

Lab Objectives

- Gather information using advanced Google hacking techniques
- Gather information from video search engines
- Gather information from FTP search engines
- Gather information from IoT search engines

Lab Environment

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance

To carry out this lab, you need:

- Windows 10 virtual machine
- Administrator privileges to run the tools
- Web browsers with an Internet connection

Lab Duration

Time: 20 Minutes

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

Overview of Search Engines

Search engines use crawlers, automated software that continuously scans active websites, and add the retrieved results to the search engine index, which is further stored in a huge database. When a user queries a search engine index, it returns a list of Search Engine Results Pages (SERPs). These results include web pages, videos, images, and many different file types ranked and displayed based on their relevance. Examples of major search engines include Google, Bing, Yahoo, Ask, Aol, Baidu, WolframAlpha, and DuckDuckGo.

Lab Tasks

TASK 1 — Gather Information using Advanced Google Hacking Techniques

Advanced Google hacking refers to the art of creating complex search engine queries by employing advanced Google operators to extract sensitive or hidden information about a target company from the Google search results. This can provide information about websites that are vulnerable to exploitation

Note: Here, we will consider **EC-Council** as a target organization.

1. Turn on **Windows 10** virtual machine.
2. Login to the **Windows 10** virtual machine with Username: **Admin** and Password: **Pa$$w0rd**.

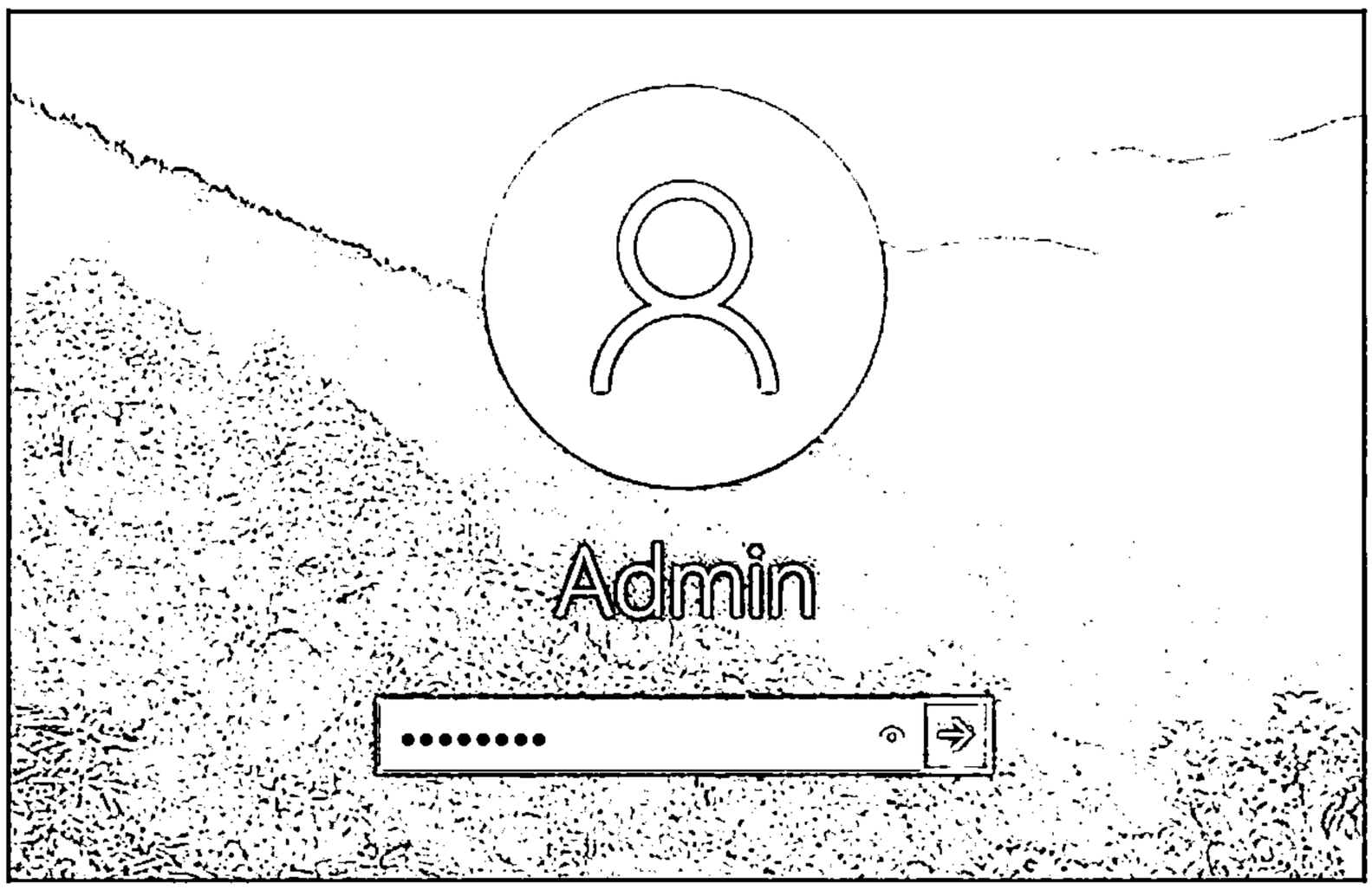


Figure 1.1.1: Login window

3. Open any web browser (here, **Mozilla Firefox**) and navigate to **https://www.google.com**.

Note:

- If the **Default Browser** pop-up window appears, uncheck the **Always perform this check when starting Firefox** checkbox and click the **Not now** button.

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

- If a **New in Firefox: Content Blocking** pop-up window appears, follow the step and click **Got it** to finish viewing the information.

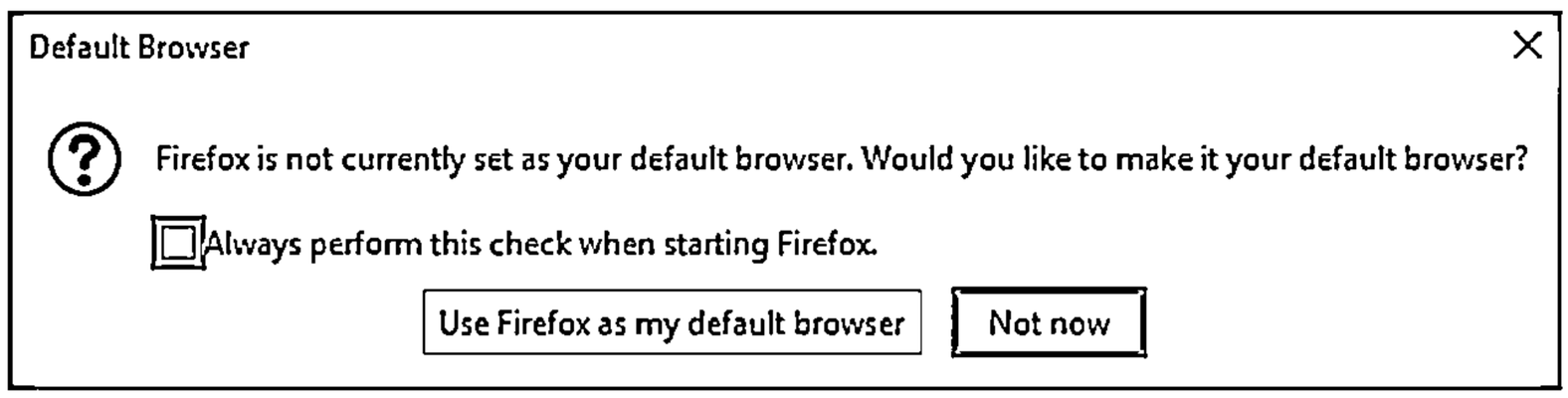


Figure 1.1.2: Default browser pop-up window

4. Once the **Google** search engine appears, you should see a search bar.

Note: If any pop-up window appears at the top-right corner, click **No, thanks**

Figure 1.1.3: Google Search bar

TASK 1.1

Perform Advanced Google Hacking for Password Files

5. Type **intitle:password site:www.eccouncil.org** and press **Enter**. This search command uses **intitle** and **site** Google advanced operators, which restrict results to pages on the **www.eccouncil.org** website that contain the term **password** in the title. An example is shown in the screenshot below.

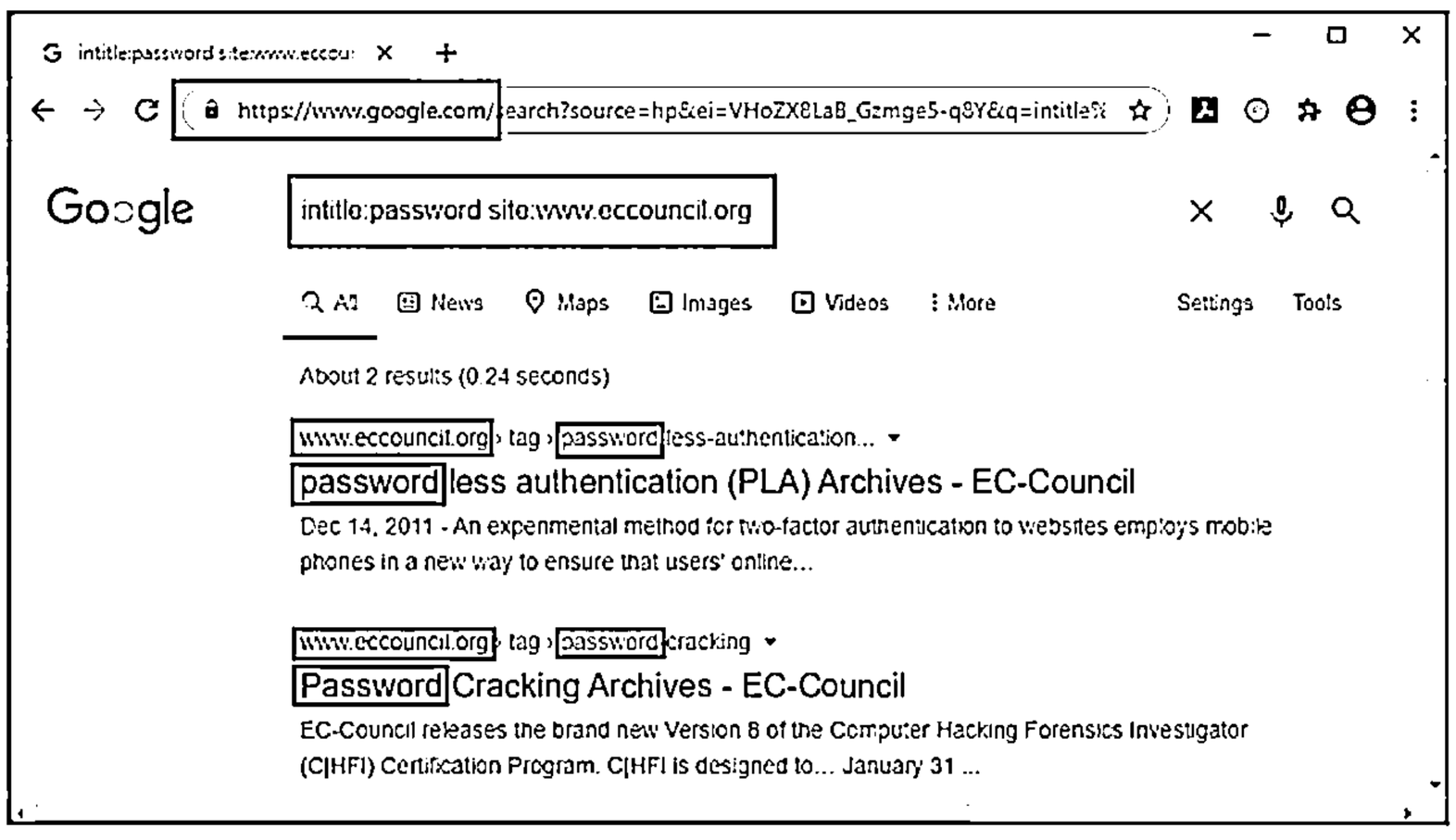


Figure 1.1.4: Search result with advanced google operators

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

TASK 1.2

Perform Advanced Google Hacking for PDF Files

6. Now, navigate back to **https://www.google.com**. In the search bar, type the command **EC-Council filetype:pdf** and press **Enter** to search your results based on the file extension.

Note: Here, the file type pdf is searched for the target organization EC-Council.

7. Now, click on any link from the results (here, first link) to view the pdf file.

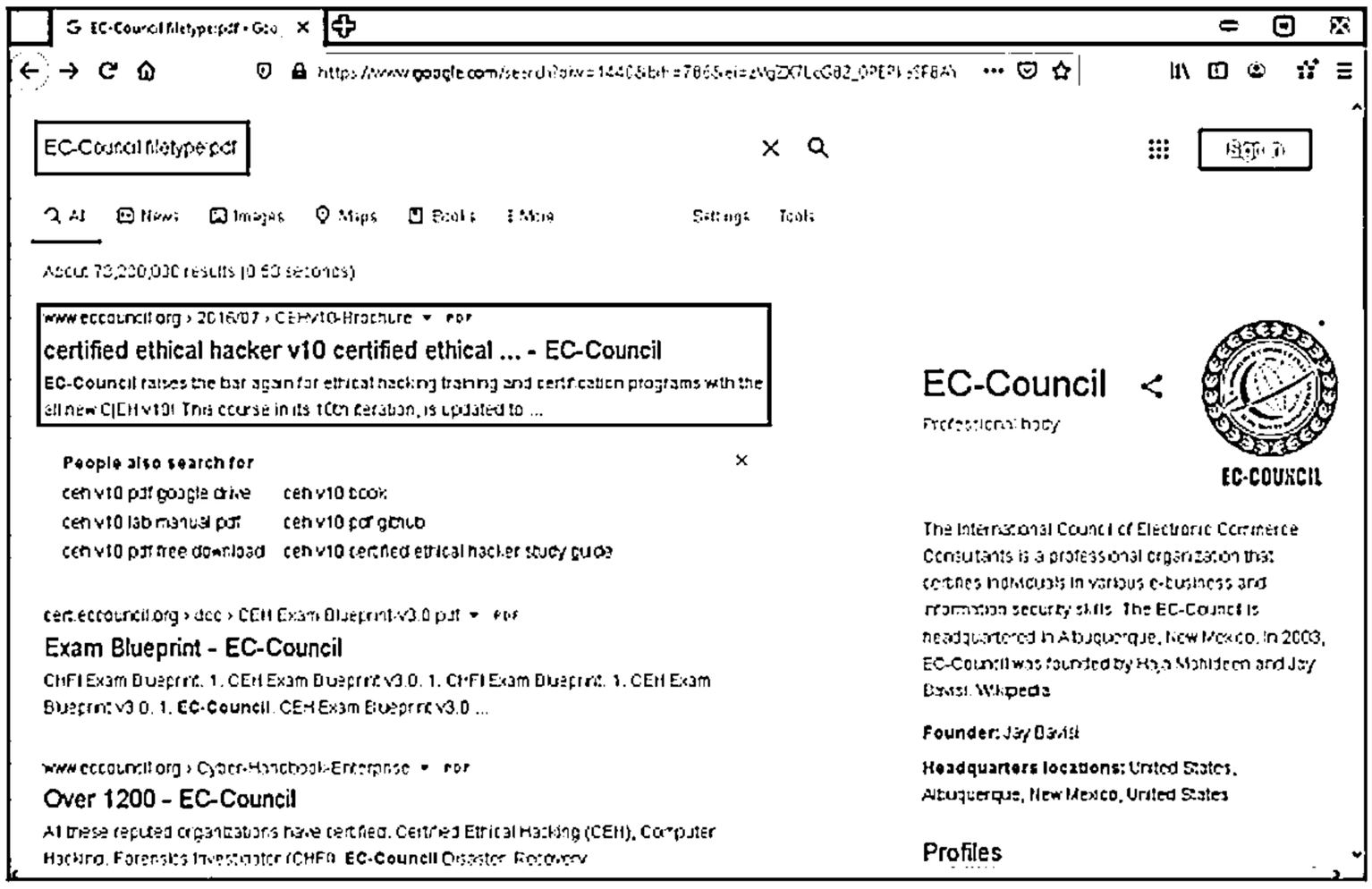


Figure 1.1.5: Results showing various pdf files

8. The page appears displaying the PDF file, as shown in the screenshot.

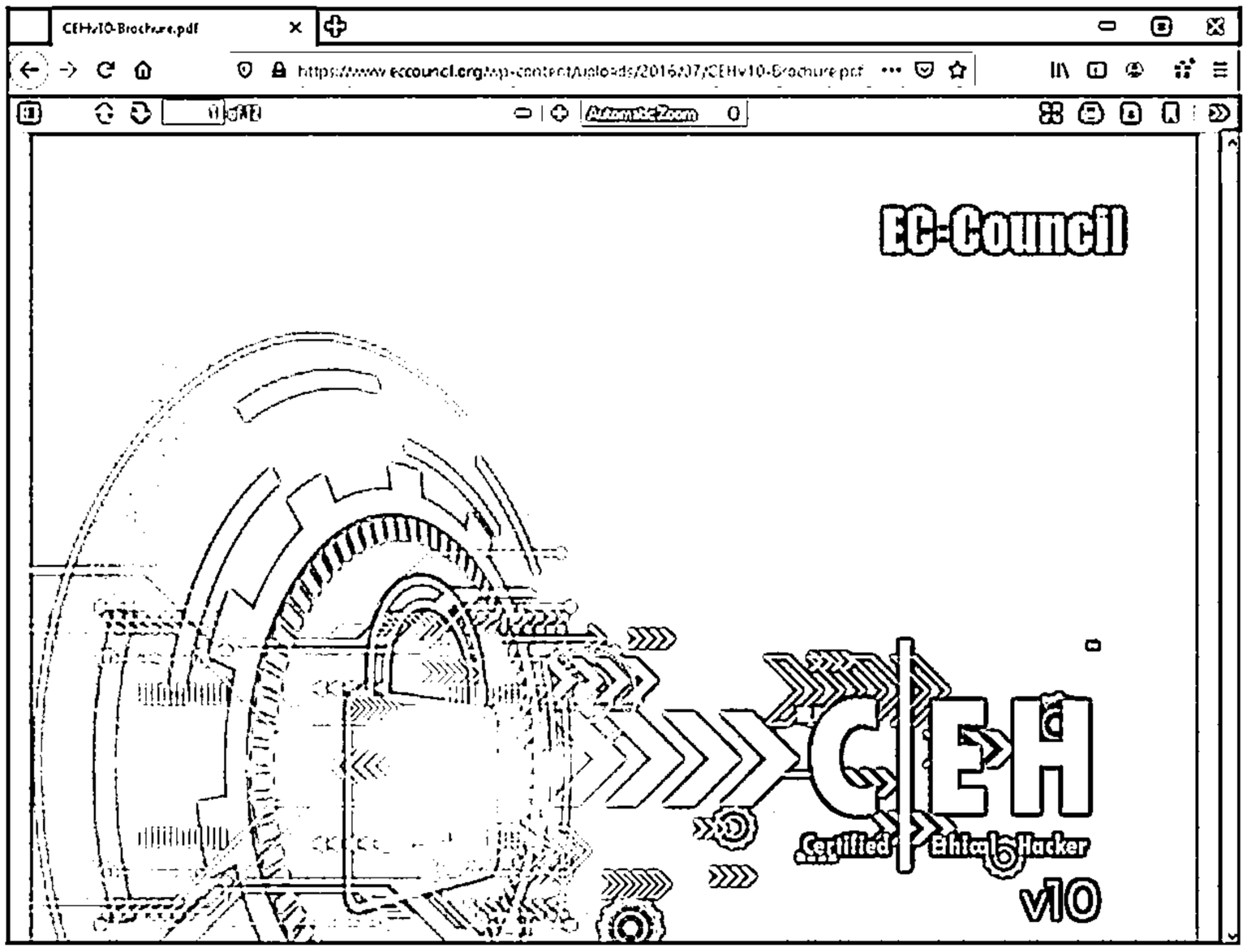


Figure 1.1.6: PDF file

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

9. Apart from the aforementioned advanced Google operators, you can also use the following to perform an advanced search to gather more information about the target organization from publicly available sources.

   - **cache**: This operator allows you to view cached version of the web page.

     [cache: www.google.com]- Query returns the cached version of the website www.google.com

   - **allinurl**: This operator restricts results to pages containing all the query terms specified in the URL.

     [allinurl: google career]—Query returns only pages containing the words "google" and "career" in the URL

   - **inurl:** This operator restricts the results to pages containing the word specified in the URL

     [inurl: copy site:www.google.com]—Query returns only pages in Google site in which the URL has the word "copy"

   - **allintitle:** This operator restricts results to pages containing all the query terms specified in the title.

     [allintitle: detect malware]—Query returns only pages containing the words "detect" and "malware" in the title

   - **inanchor:** This operator restricts results to pages containing the query terms specified in the anchor text on links to the page.

     [Anti-virus inanchor:Norton]—Query returns only pages with anchor text on links to the pages containing the word "Norton" and the page containing the word "Anti-virus"

   - **allinanchor:** This operator restricts results to pages containing all query terms specified in the anchor text on links to the page.

     [allinanchor: best cloud service provider]—Query returns only pages in which the anchor text on links to the pages contain the words "best," "cloud," "service," and "provider"

   - **link:** This operator searches websites or pages that contain links to the specified website or page.

     [link:www.googleguide.com]—Finds pages that point to Google Guide's home page

   - **related:** This operator displays websites that are similar or related to the URL specified.

     [related:www.certifiedhacker.com]—Query provides the Google search engine results page with websites similar to certifiedhacker.com

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

- **info:** This operator finds information for the specified web page.

  [info:gothotel.com]—Query provides information about the national hotel directory GotHotel.com home page

- **location:** This operator finds information for a specific location.

  [location: 4 seasons restaurant]—Query give you results based around the term 4 seasons restaurant

10. This concludes the demonstration of gathering information using advanced Google hacking techniques. You can conduct a series of queries on your own by using these advanced Google operators and gather the relevant information about the target organization.
11. Close all open windows and document all the acquired information.

TASK 2 Gather Information from Video Search Engines

Here, we will perform an advanced video search and reverse image search using the YouTube search engine and Youtube DataViewer video analysis tool.

Video search engines are Internet-based search engines that crawl the web looking for video content. These search engines either provide the functionality of uploading and hosting the video content on their own web servers or they can parse the video content, which is hosted externally.

1. In the **Windows 10** virtual machine, open any web browser (here, **Mozilla Firefox**) and navigate to **https://www.youtube.com/**.
2. In the search bar, search for your target organization (here, **ec-council**). You will see all the latest videos uploaded by the target organization.

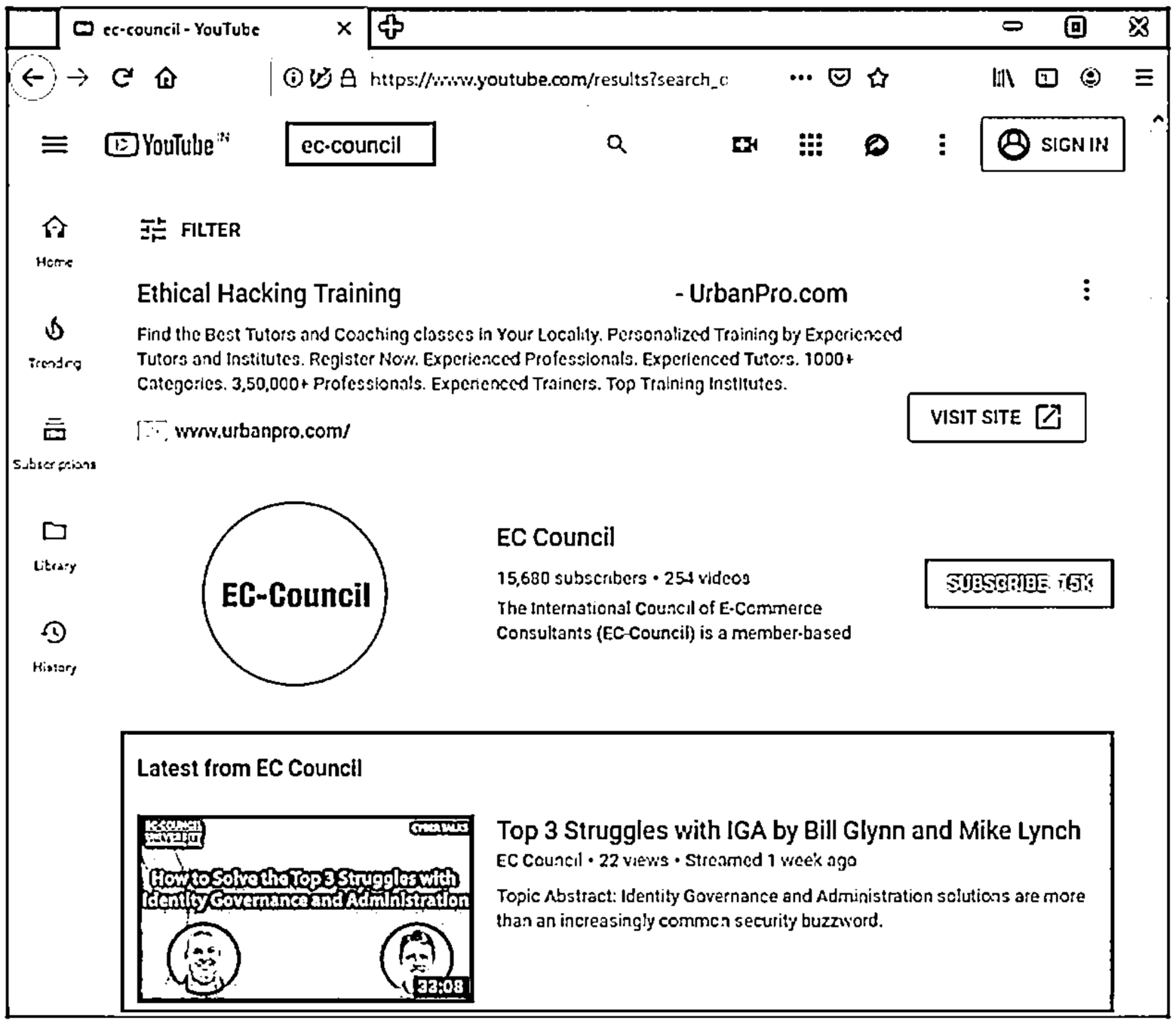


Figure 1.2.1: YouTube search result for ec-council query

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

3. Select any video of your choice, right-click on the video title, and click **Copy Link Location.** (here, **Top 3 Struggles with IGA by Bill Glynn and Mike Lynch**)

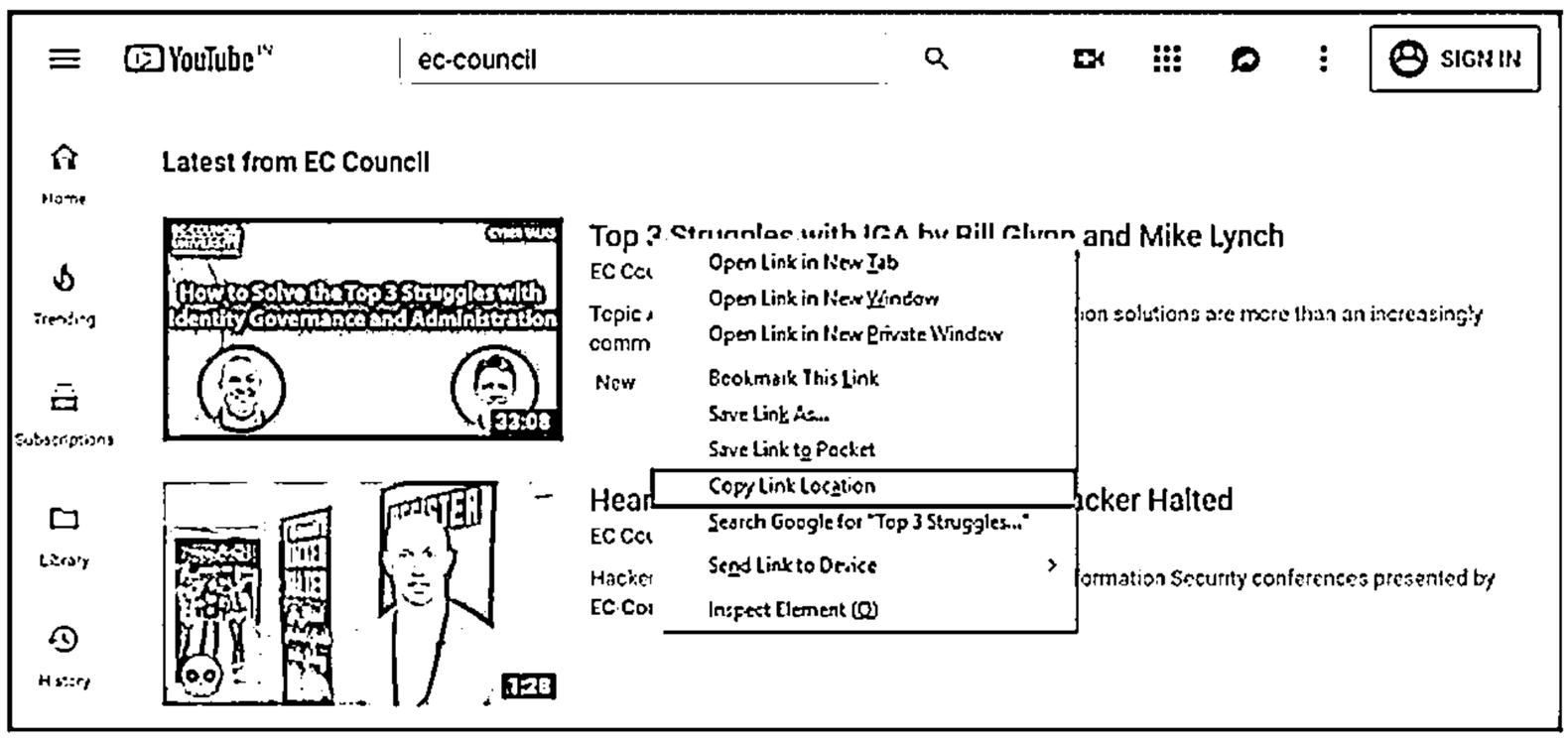


Figure 1.2.2: Copy Link Location option

4. After the video link is copied, open another browser tab in **Mozilla Firefox**, and then navigate to **https://citizenevidence.amnestyusa.org/**. In the **Enter YouTube URL** search box, paste the copied YouTube video link and click **Go**.

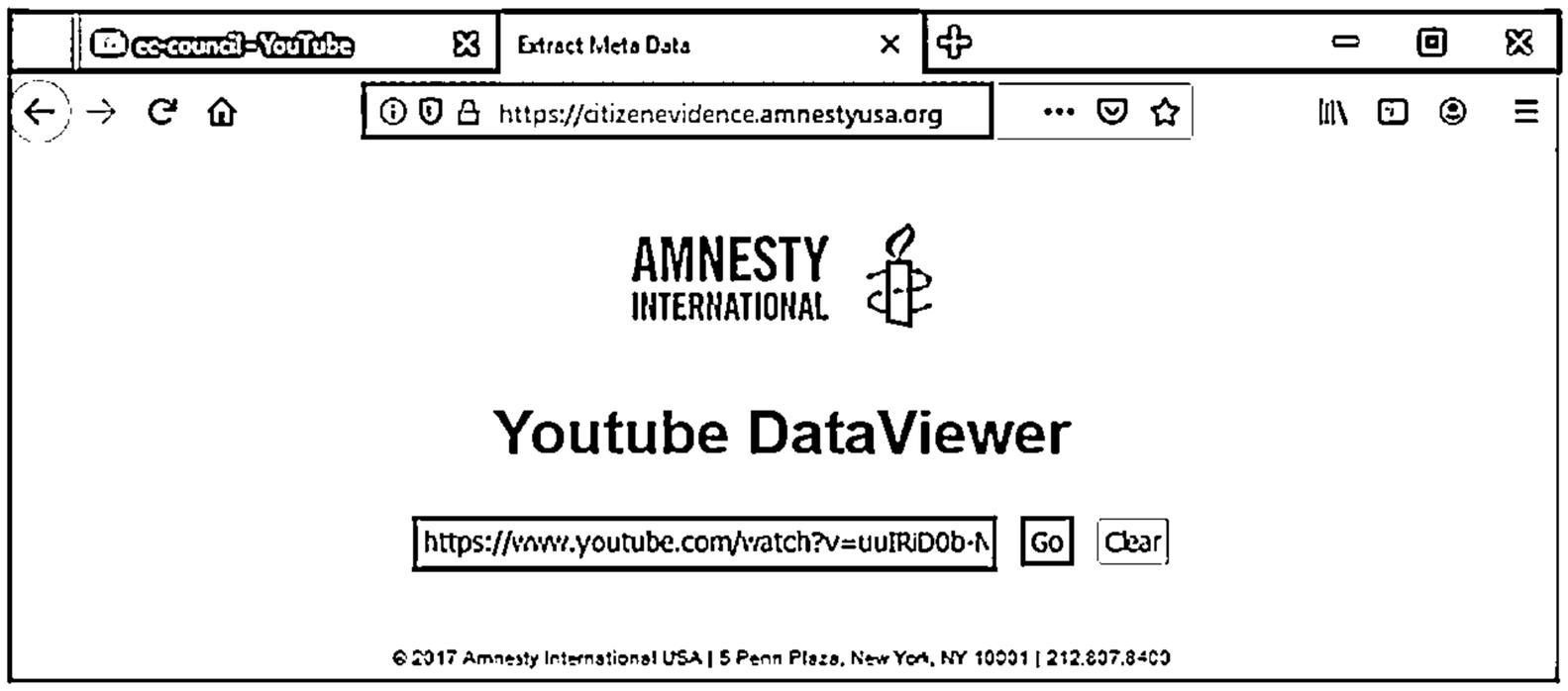


Figure 1.2.3: Paste copied YouTube Link

5. In the search result, you can observe the details related to the video such as **Topic Abstract**, **Video ID**, **Upload Date**, **Upload Time**, etc. You can also find **Thumbnails** to perform a reverse image search. Click on the **reverse image search** option for any thumbnail.

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

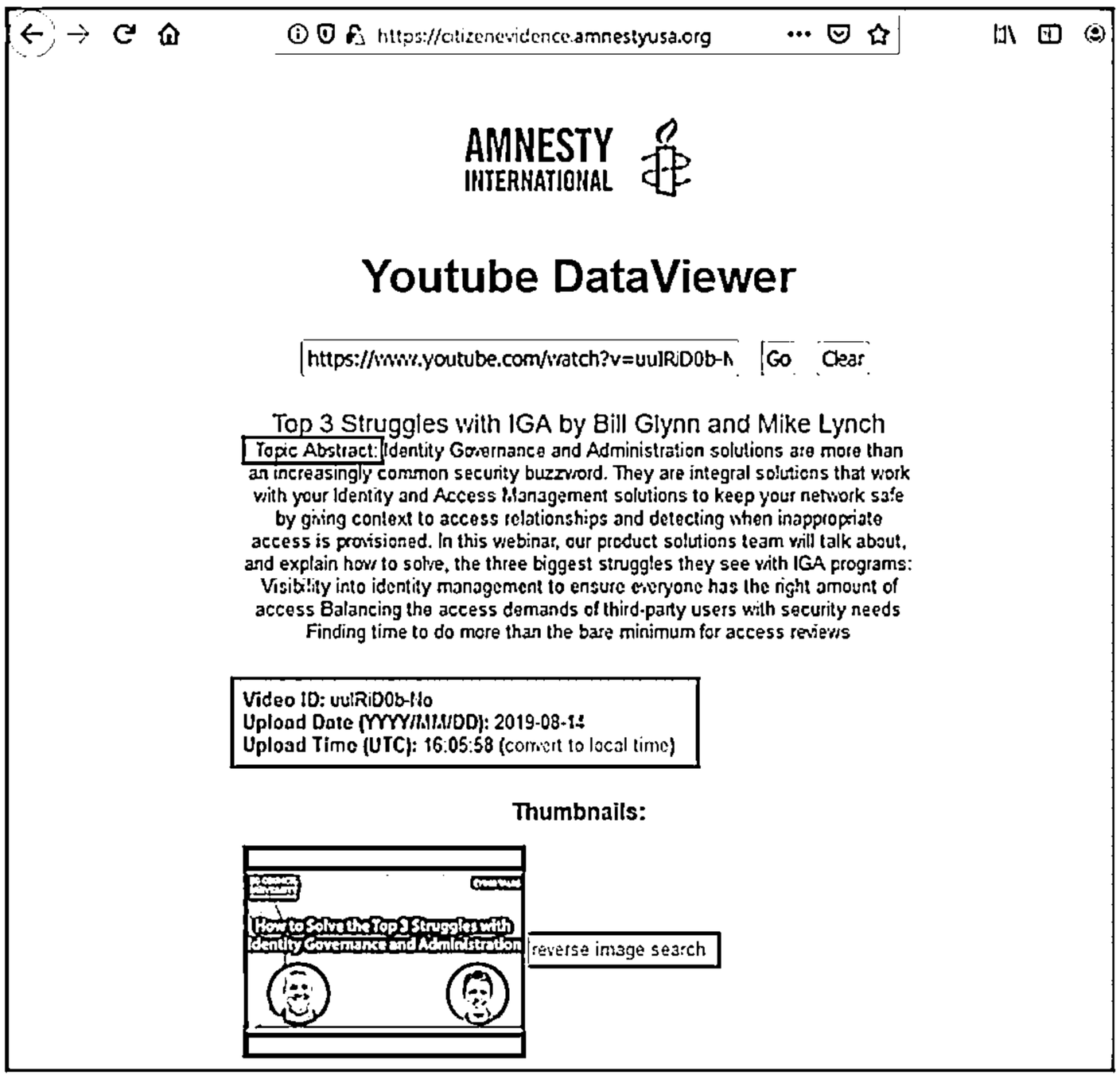


Figure 1.2.4: Youtube DataViewer Result

6. A new tab in **Google** opens, and the results for the reverse image search are displayed.

You can use other video search engines such as **Google videos** (https://video.google.com), **Yahoo videos** (https://video.search.yahoo.com), etc.; video analysis tools such as **EZGif** (https://ezgif.com), **VideoReverser.com**, etc.; and reverse image search tools such as **TinEye Reverse Image Search** (https://tineye.com), **Yahoo Image Search** (https://images.search.yahoo.com), etc. to gather crucial information about the target organization

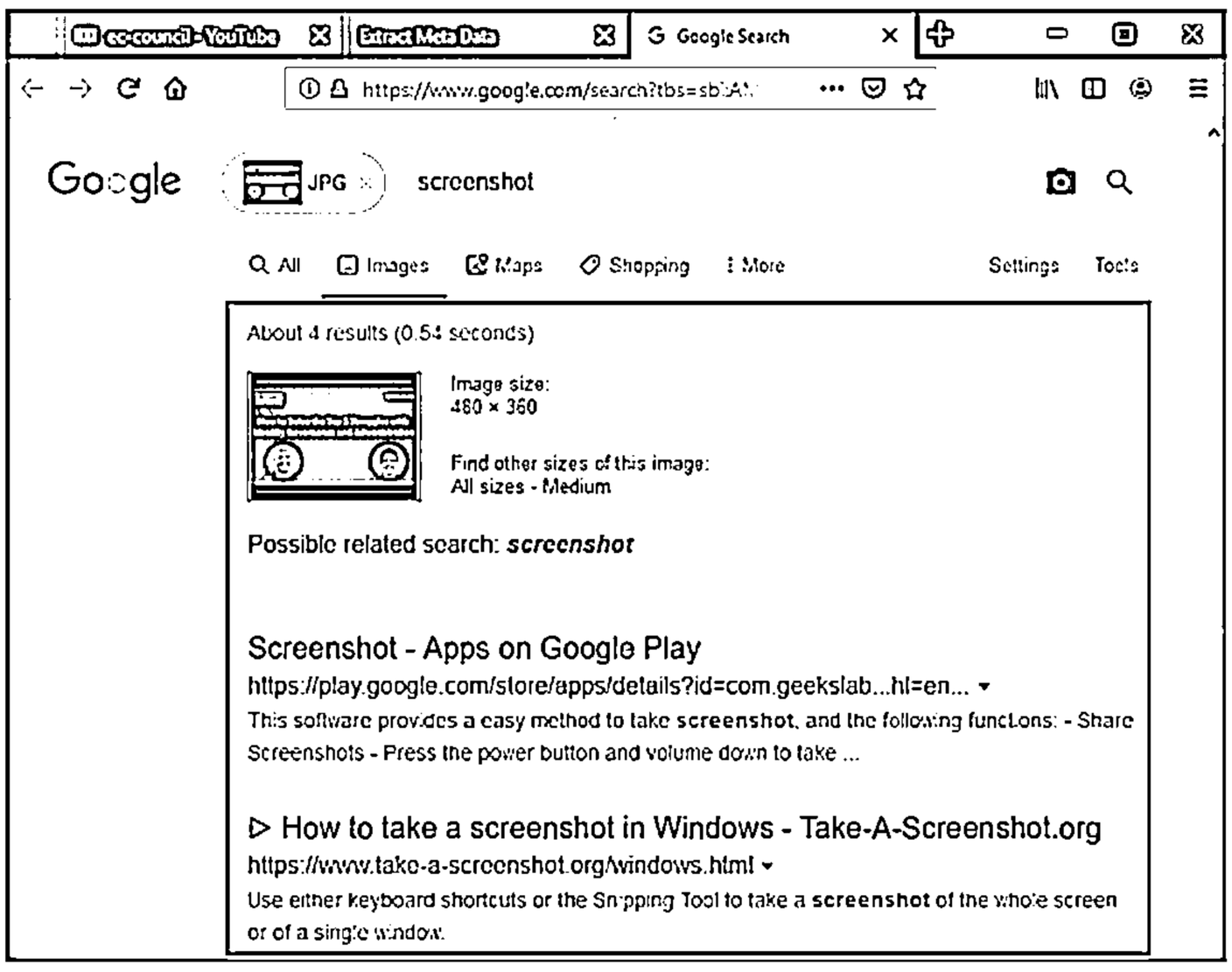


Figure 1.2.5: Reverse image search result

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

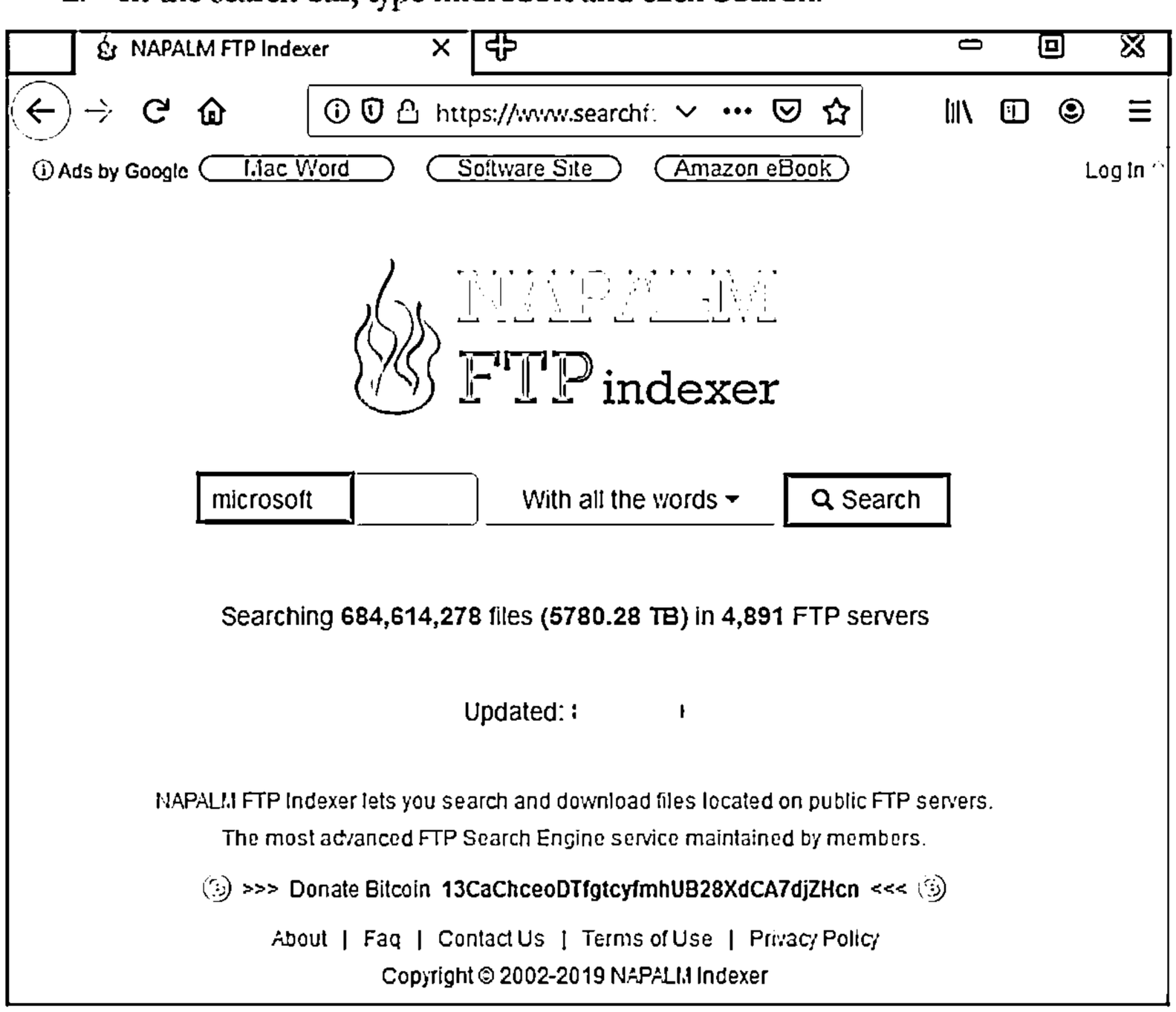
7. This concludes the demonstration of gathering information from the advanced video search and reverse image search using the YouTube search engine and Youtube DataViewer video analysis tool.
8. Close all open windows and document all acquired information.

TASK 3 Gather Information from FTP Search Engines

Here, we will use the NAPALM FTP indexer FTP search engine to extract critical FTP information about the target organization.

File Transfer Protocol (FTP) search engines are used to search for files located on the FTP servers; these files may hold valuable information about the target organization. Many industries, institutions, companies, and universities use FTP servers to keep large file archives and other software that are shared among their employees.

1. In the **Windows 10** virtual machine, open any web browser (here, **Mozilla Firefox**) and navigate to **https://www.searchftps.net/**.
2. In the search bar, type **microsoft** and click **Search**.



FTP search engines provide information about critical files and directories, including valuable information such as business strategies, tax documents, employee's personal records, financial records, licensed software, and other confidential information

Figure 1.3.1: NAPALM FTP indexer search result

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

3. You will get the search results with the details of the FTP in the target organization, as shown in the screenshot.

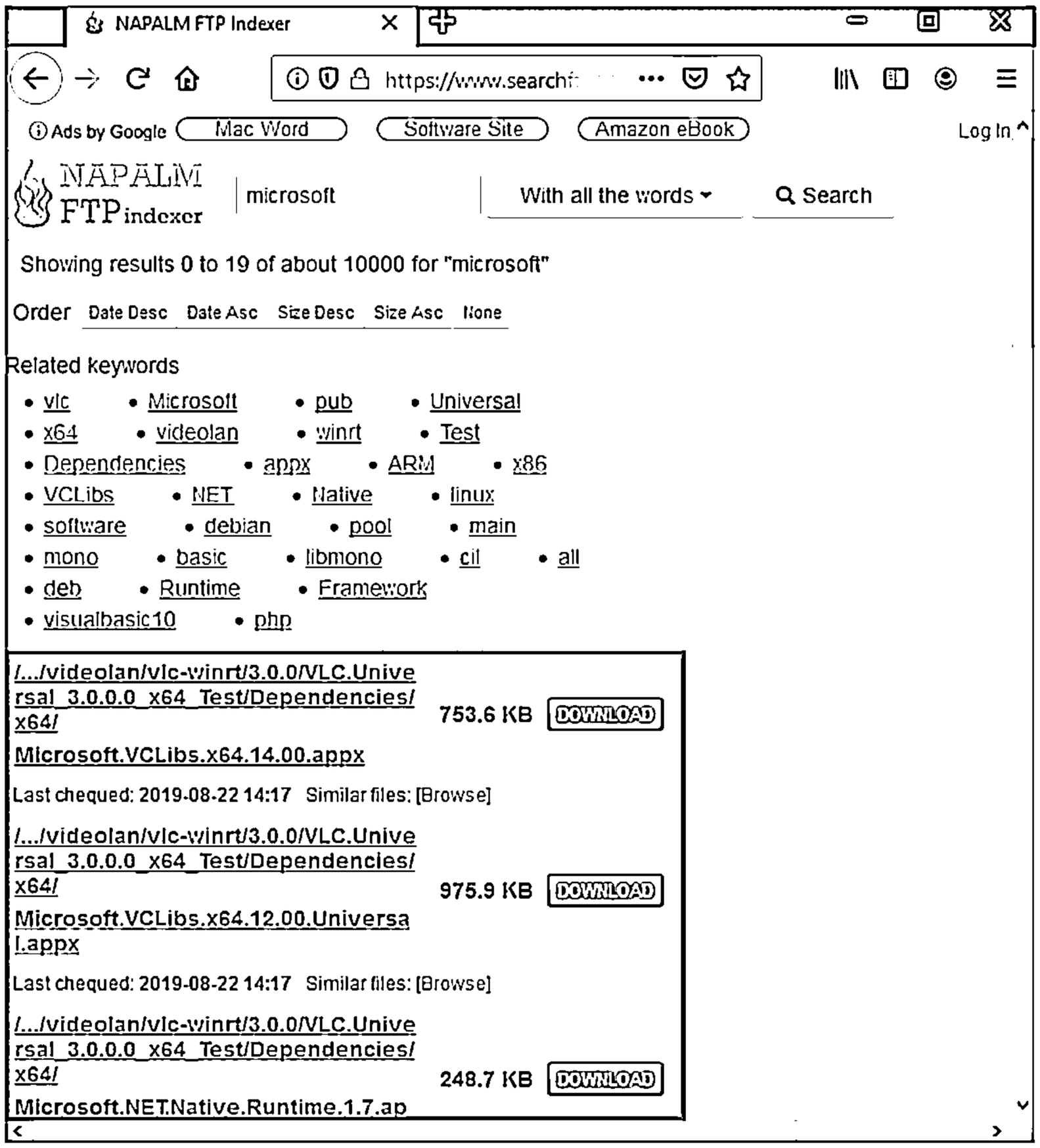


Figure 1.3.2: FTP search result

You can also use FTP search engines such as **Global FTP Search Engine** (https://globalfilesearch.com), **FreewareWeb FTP File Search** (http://www.freewareweb.com), etc. to gather crucial FTP information about the target organization.

4. This concludes the demonstration of gathering information from the FTP search engine.
5. Close all open windows and document all the acquired information.

TASK 4 Gather Information from IoT Search Engines

Here, we will search for information about any vulnerable IoT device in the target organization using the Shodan IoT search engine.

1. In the **Windows 10** virtual machine, open any web browser (here, **Mozilla Firefox**) and navigate to **https://www.shodan.io/**.
2. In the search bar, type **amazon** and press **Enter**. You will obtain the search results with the details of all the vulnerable IoT devices related to amazon in various countries, as shown in the screenshot.

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

IoT search engines crawl the Internet for IoT devices that are publicly accessible. These search engines provide crucial information, including control of SCADA (Supervisory Control and Data Acquisition) systems, traffic control systems, Internet-connected household appliances, industrial appliances, CCTV cameras, etc.

Note: The screenshot might differ in your lab environment.

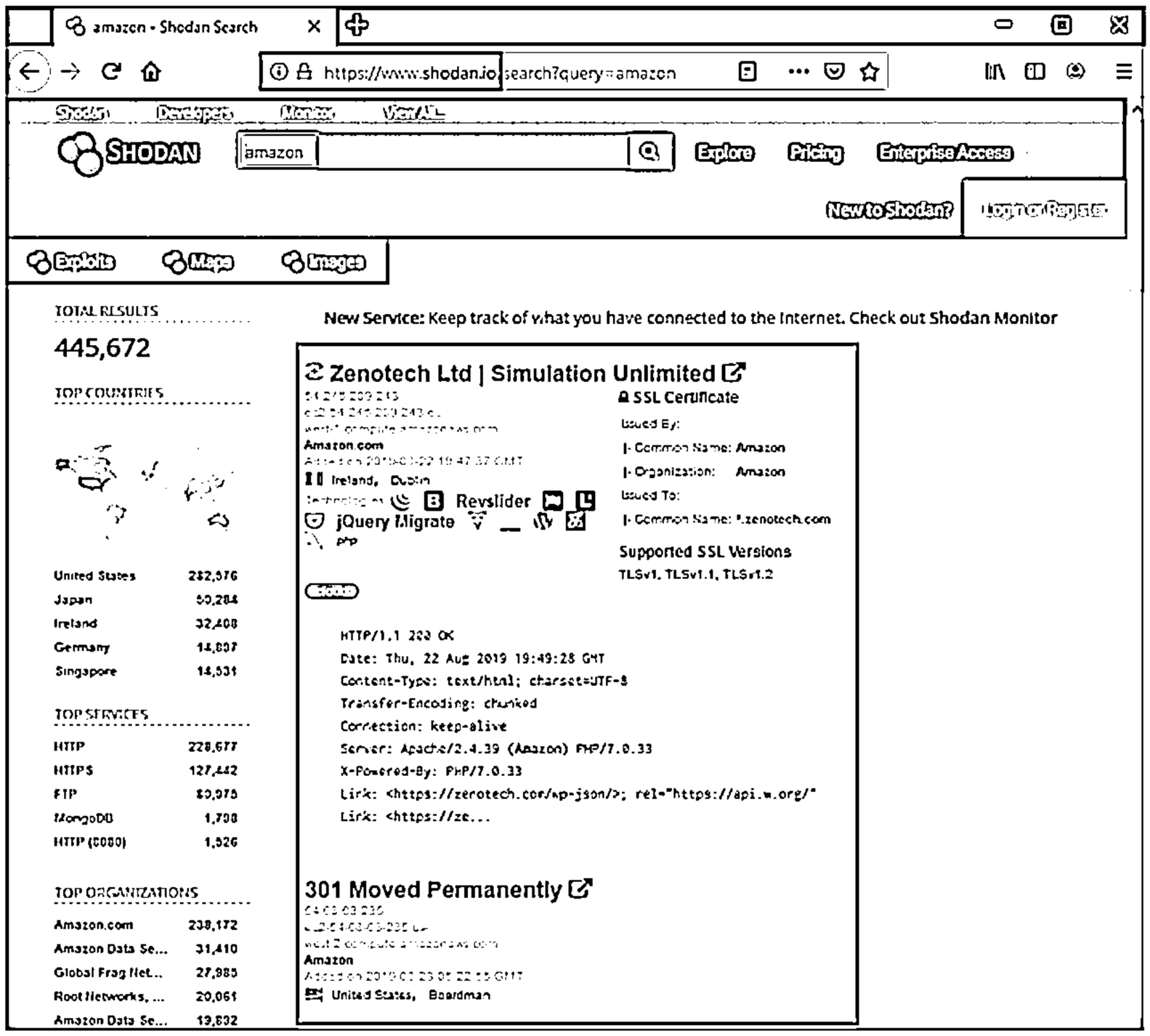


Figure 1.4.1: Shodan search result

3. This concludes the demonstration of gathering vulnerable IoT information using the Shodan search engine.
4. Close all open windows and document all the acquired information.
5. Turn off the **Windows 10** virtual machine.

You can also use **Censys** (https://censys.io), **Thingful** (https://www.thingful.net), etc., which are IoT search engines, to gather information such as manufacturer details, geographical location, IP address, hostname, open ports, etc.

Lab Analysis

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

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT 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

Perform Footprinting Through Web Services

Web services are online applications or sources that provide a variety of publicly accessible information related to the target organization.

Lab Scenario

ICON KEY

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

As a professional ethical hacker or pen tester, you should be able to extract a variety of information about your target organization from web services. By doing so, you can extract critical information such as a target organization's domains, sub-domains, operating systems, geographic locations, employee details, emails, financial information, infrastructure details, hidden web pages and content, etc.

Using this information, you can build a hacking strategy to break into the target organization's network and can carry out other types of advanced system attacks.

Lab Objectives

- Find the company's domains and sub-domains using Netcraft
- Gather personal information using PeekYou online people search service
- Gather an email list using theHarvester
- Gather information using deep and dark web searching
- Determine target OS through passive footprinting

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Parrot Security virtual machine
- Administrator privileges to run the tools
- Web browsers with an Internet connection

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

- Tor Browser located at **E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance\Deep and Dark Web Footprinting Tools\Tor Browser**
- You can also download the latest version of Tor Browser from its official website. If you decide to download the latest version, the screenshots shown in the lab might differ.

Lab Duration

Time: 25 Minutes

Overview of Web Services

Web services such as social networking sites, people search services, alerting services, financial services, and job sites, provide information about a target organization; for example, infrastructure details, physical location, employee details, etc. Moreover, groups, forums, and blogs may provide sensitive information about a target organization such as public network information, system information, and personal information. Internet archives may provide sensitive information that has been removed from the World Wide Web (WWW).

Lab Tasks

TASK 1 — Find the Company's Domains and Sub-domains using Netcraft

Here, we will extract the company's domains and sub-domains using the Netcraft web service.

Domains and sub-domains are part of critical network infrastructure for any organization. A company's top-level domains (TLDs) and sub-domains can provide much useful information such as organizational history, services and products, and contact information. A public website is designed to show the presence of an organization on the Internet and is available for free access.

1. Turn on the **Windows 10** virtual machine.
2. Login to the **Windows 10** virtual machine with Username: **Admin** and Password: **Pa$$w0rd**.
3. Open a web browser (here, **Mozilla Firefox**), type the URL **https://www.netcraft.com** in the address bar, and press **Enter**. The Netcraft website appears, as shown in the screenshot.

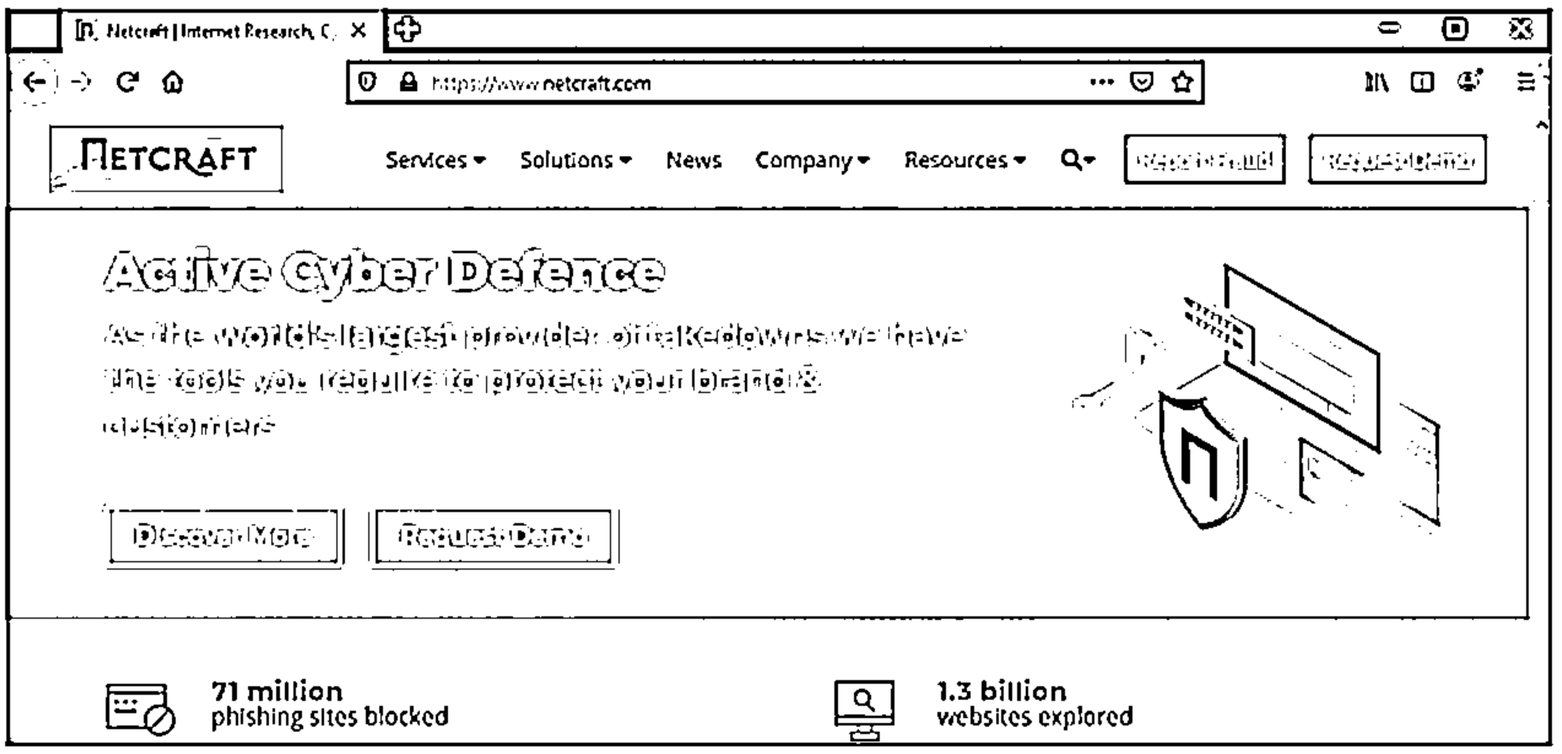


Figure 2.1.1: Netcraft website

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

4. Click the **Resources** tab from the menu bar and click on the **Site Report** link under the **Tools** section.

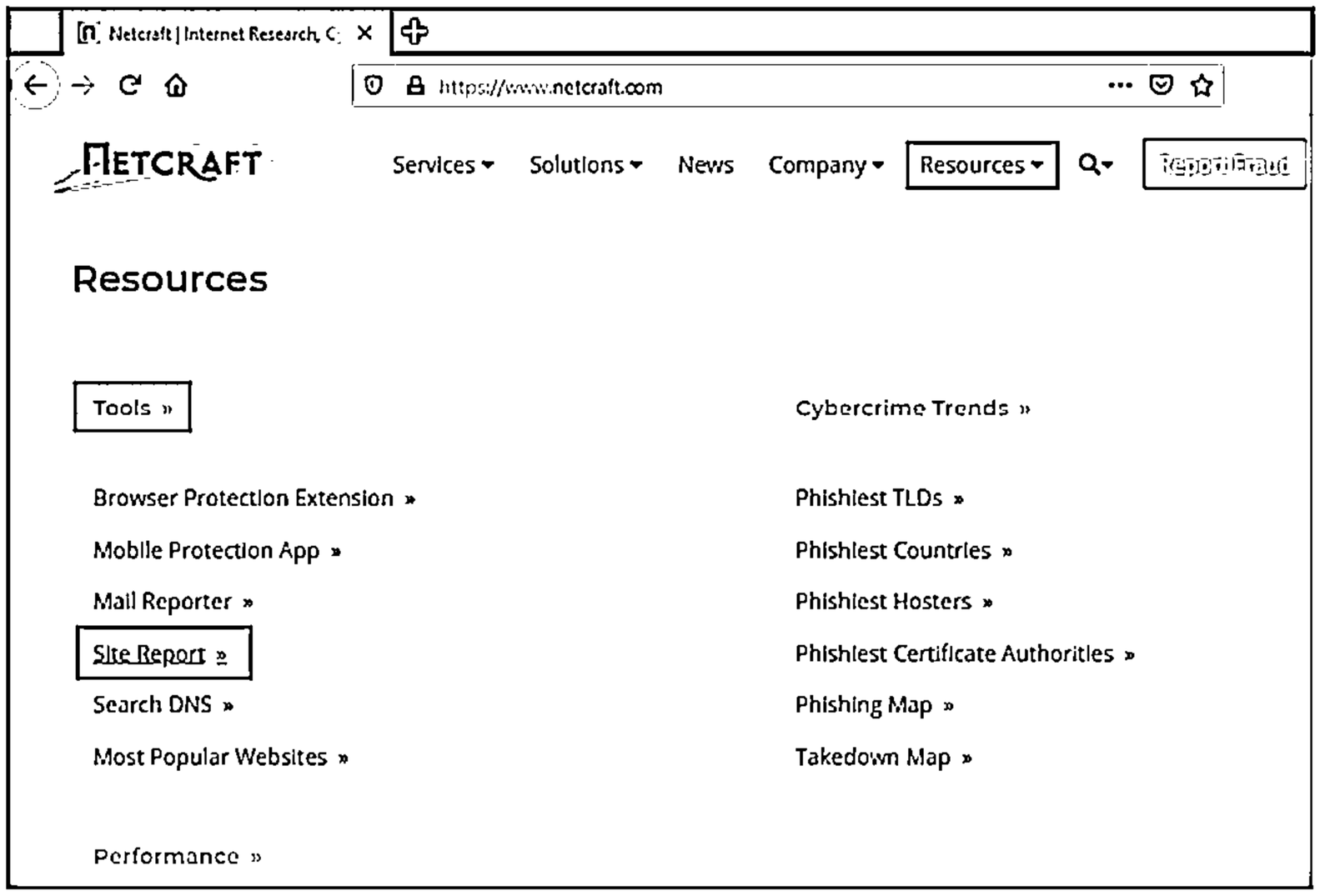


Figure 2.1.2: Netcraft website Resources tab options

5. The **What's that site running?** page appears. To extract information associated with the organizational website such as infrastructure, technology used, sub domains, background, network, etc., type the target website's URL (here, **https://www.eccouncil.org**) in the text field, and then click the **Lookup** button, as shown in the screenshot.

Figure 2.1.3: Enter the target website

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

6. The **Site report for https://www.eccouncil.org** page appears, containing information related to **Background**, **Network**, **Hosting History**, etc., as shown in the screenshot.

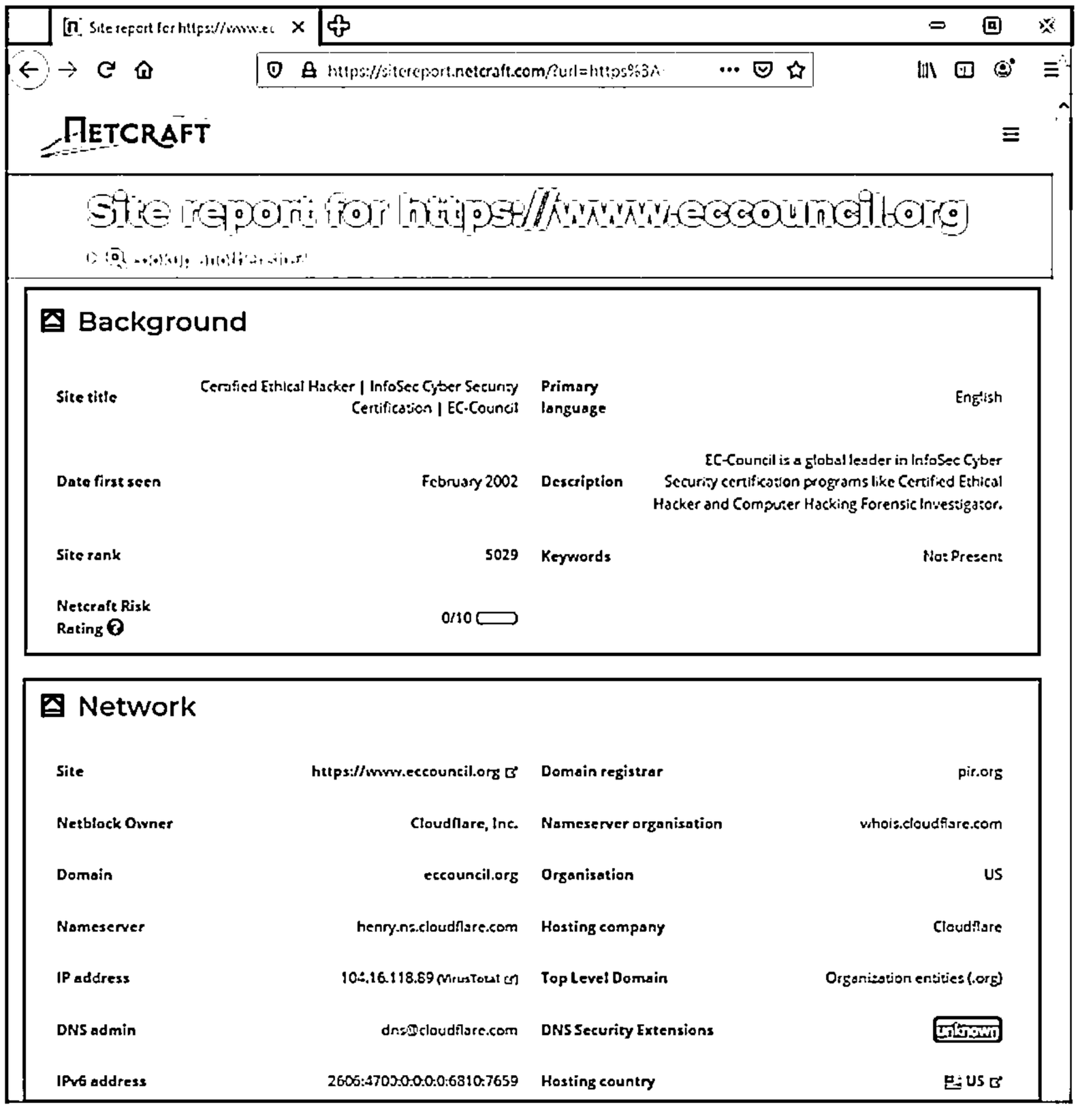


Figure 2.1.4: Report generated by Netcraft

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

7. In the **Network** section, click on the website link (here, **eccouncil.org**) in the **Domain** field to view the subdomains

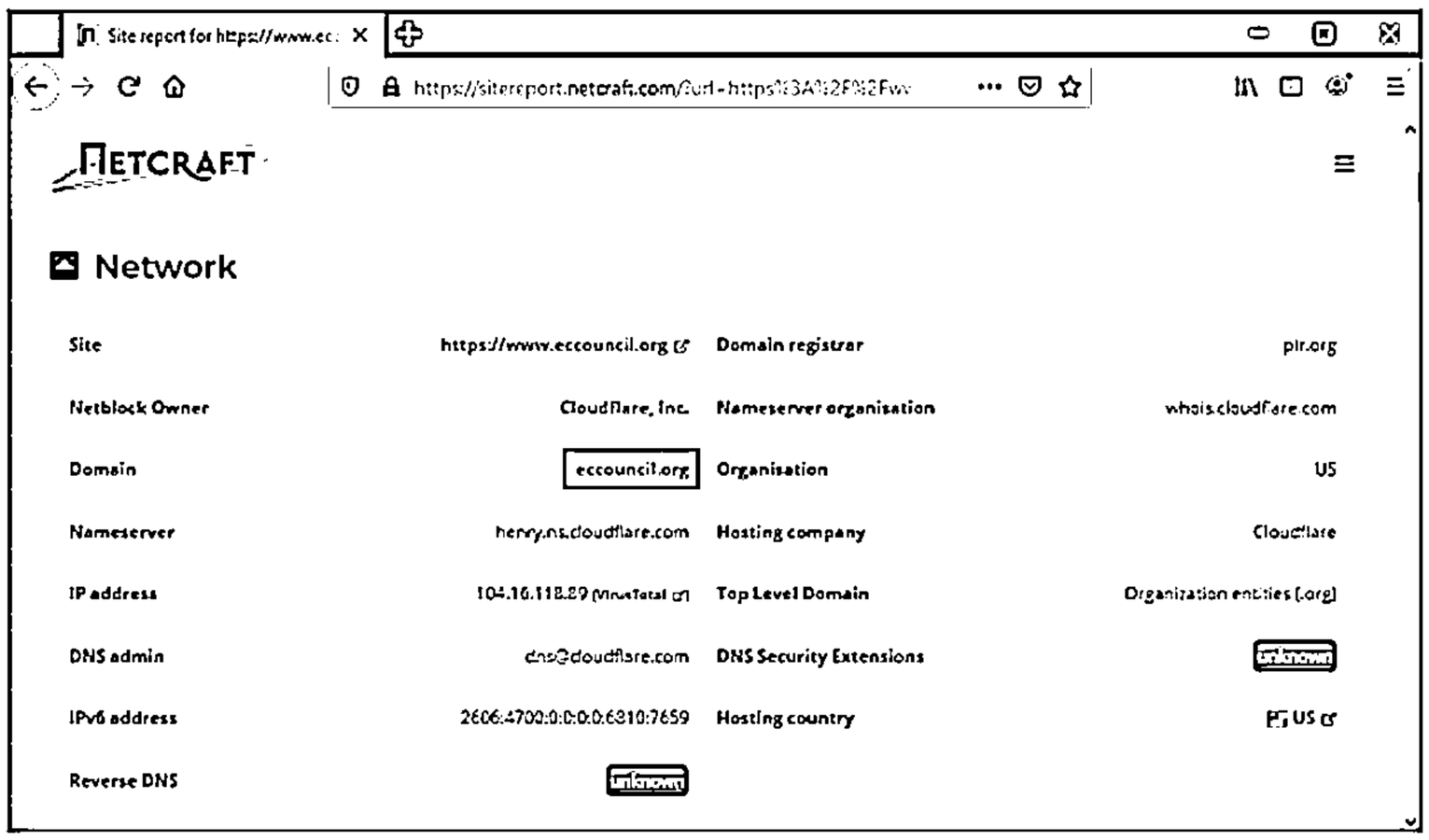


Figure 2.1.5: Report generated by Netcraft showing domain information

8. The result will display subdomains of the target website along with netblock and operating system information, as shown in the screenshot.

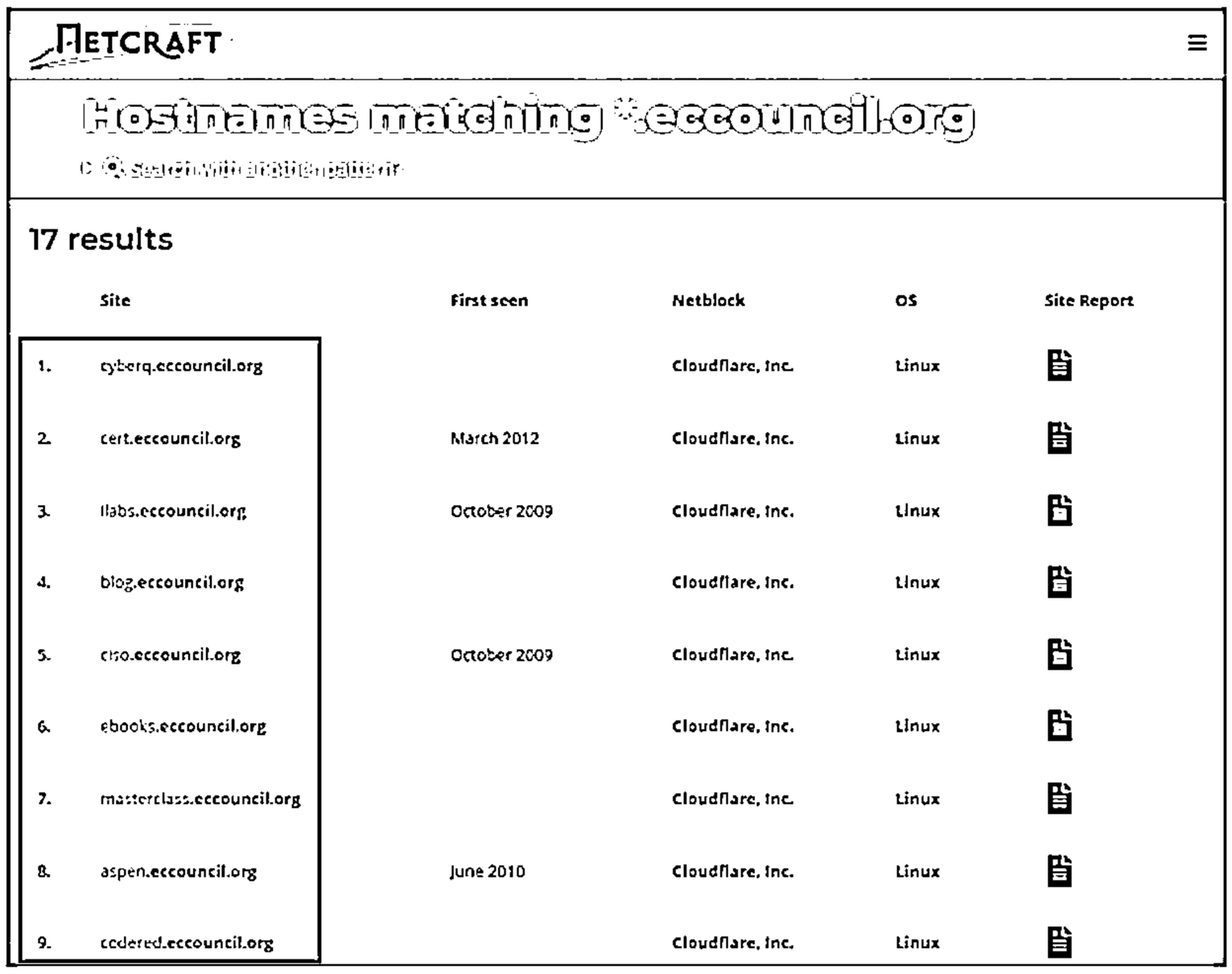


Figure 2.1.6: Report generated by Netcraft showing subdomains

You can also use tools such as **Sublist3r** (https://github.com), **Pentest-Tools Find Subdomains** (https://pentest-tools.com), etc. to identify the domains and sub-domains of any target website.

9. This concludes the demonstration of finding the company's domains and sub-domains using the Netcraft tool.
10. Close all open windows and document all the acquired information.

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

TASK 2

Gather Personal Information using PeekYou Online People Search Service

Here, we will gather information about a person from the target organization by performing people search using the PeekYou online people search service.

Online people search services, also called public record websites, are used by many individuals to find personal information about others; these services provide names, addresses, contact details, date of birth, photographs, videos, profession, details about family and friends, social networking profiles, property information, and optional background on criminal checks.

1. In the **Windows 10** virtual machine, open any web browser (here, **Mozilla Firefox**) and navigate to **https://www.peekyou.com**.
2. In the **First Name** and **Last Name** fields, type **Satya** and **Nadella**, respectively. In the **Location** drop-down box, select **Washington, DC**. Then, click the **Search** icon.

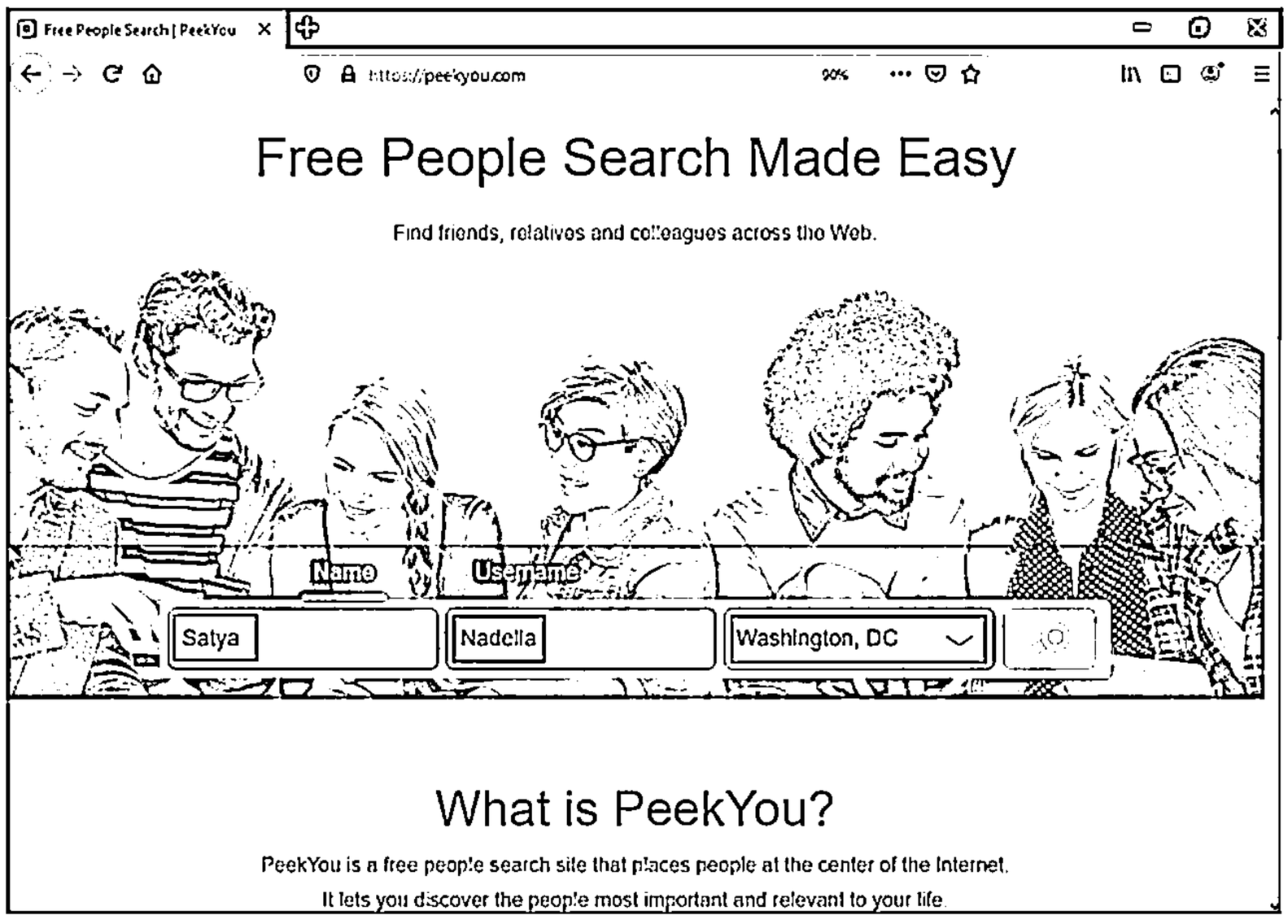


Figure 2.2.1: PeekYou Search Bar

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

3. The people search begins, and the best matches for the provided search parameters will be displayed.

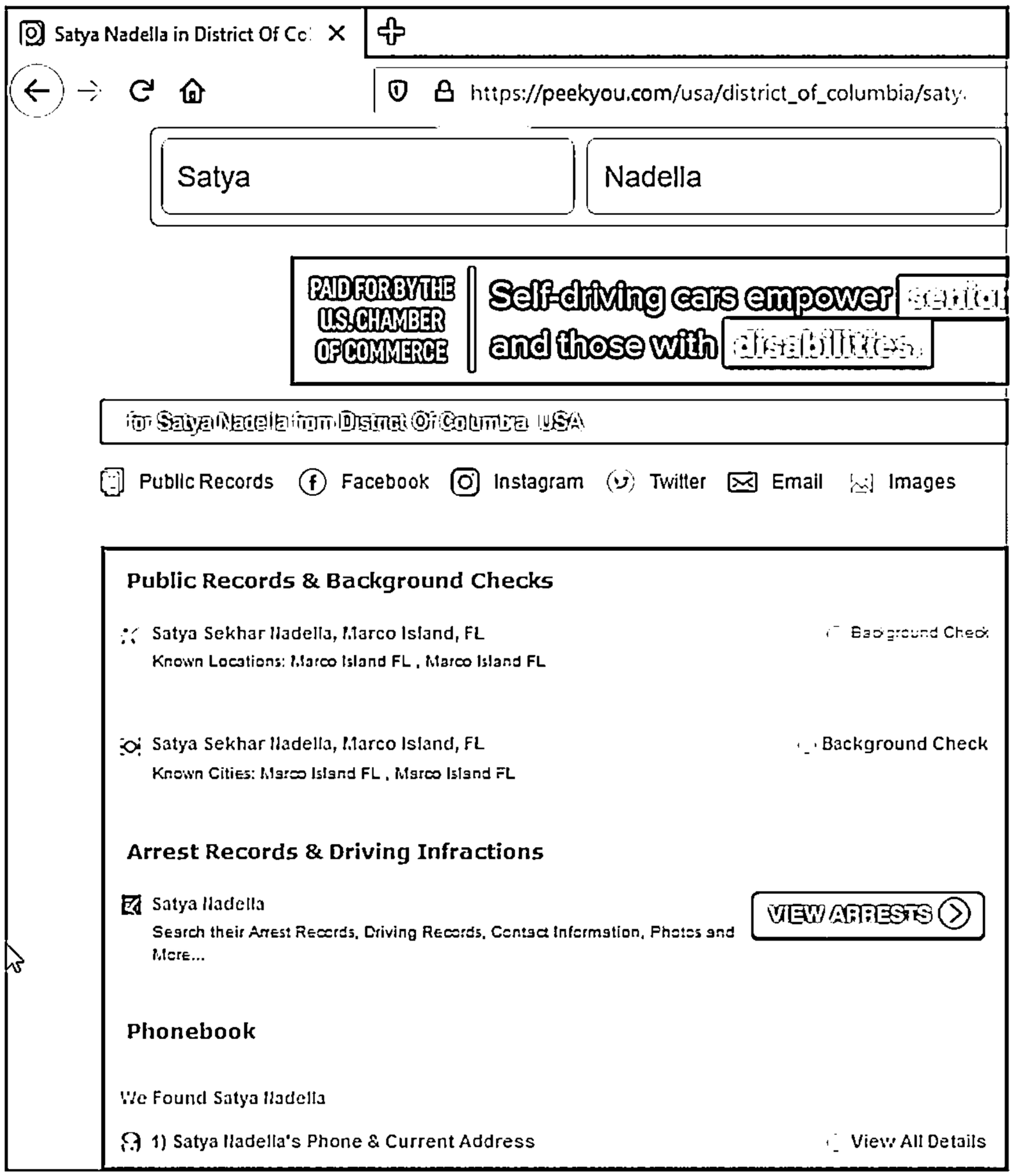


Figure 2.2.2: PeekYou Search Bar

4. You can further click on the appropriate result to view the detailed information about the target person to see a detailed information about the target person.

Note: After you click on any result, you will be redirected to a different website and it will take some time to load the information about the target.

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

5. Scroll down to view the entire information about the target person.

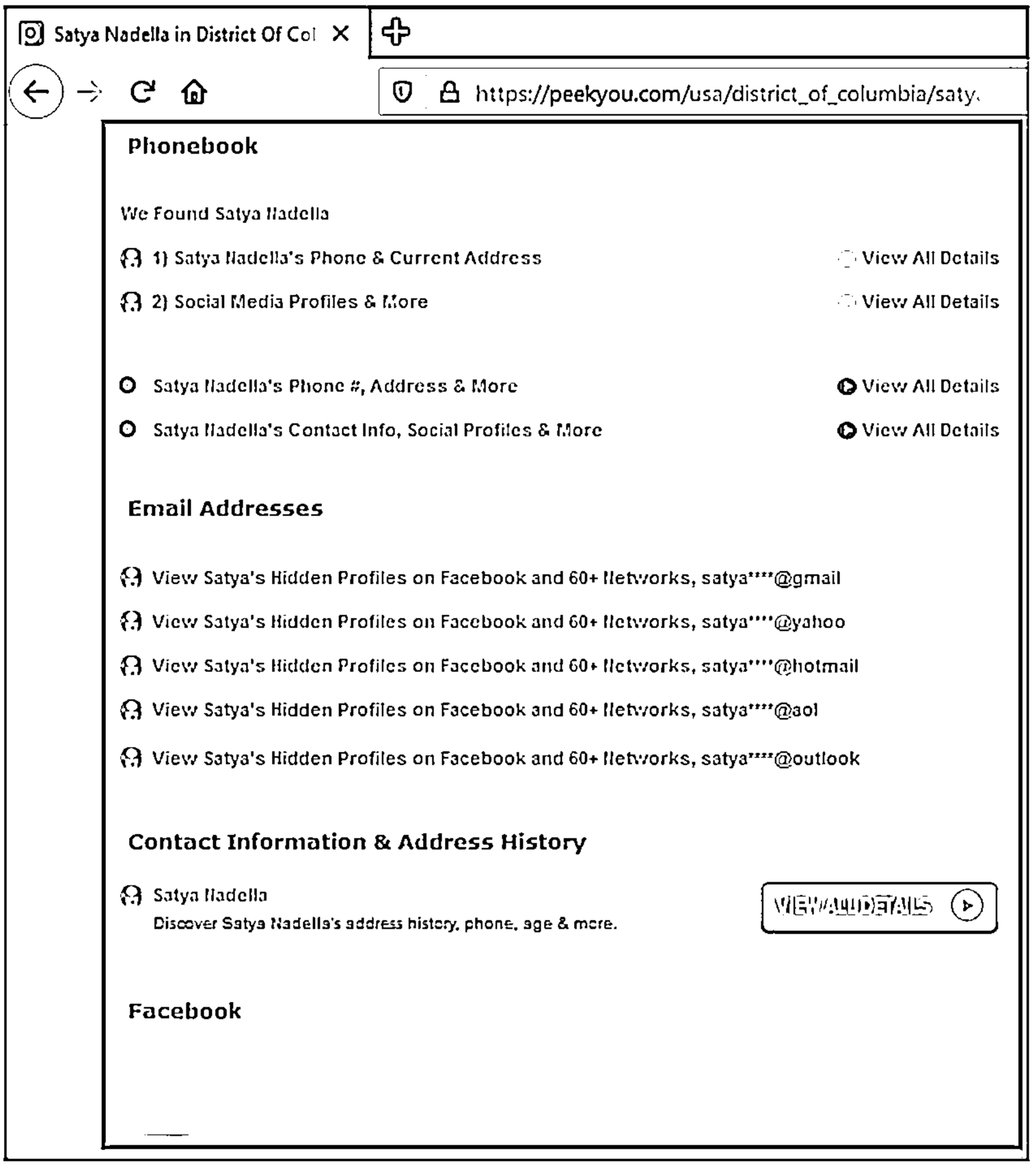


Figure 2.2.3: PeekYou Search result

You can also use pipl (https://pipl.com), Intelius (https://www.intelius.com), BeenVerified (https://www.beenverified.com), etc., which are people search services to gather personal information of key employees in the target organization

6. This concludes the demonstration of gathering personal information using the PeekYou online people search service.
7. Close all open windows and document all the acquired information.

TASK 3 Gather an Email List using theHarvester

Here, we will gather the list of email IDs related to a target organization using theHarvester tool.

1. Turn on **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

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

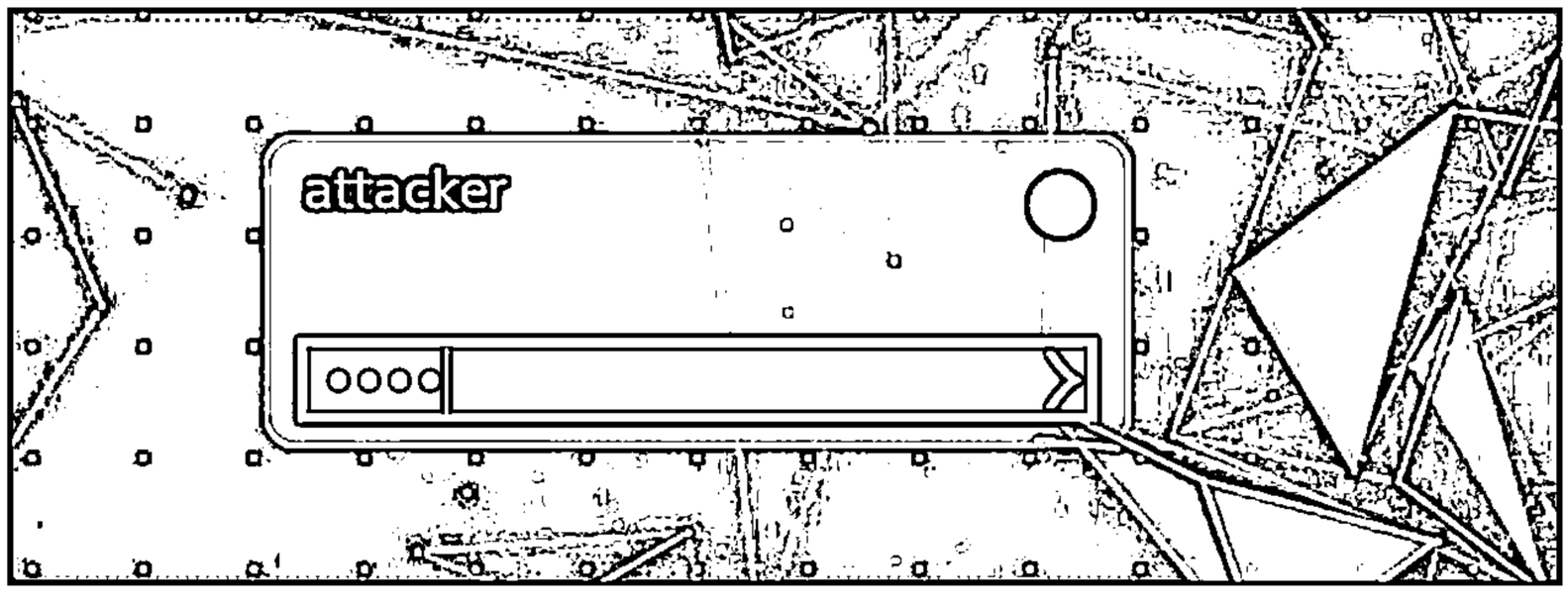


Figure 2.3.1: Parrot Security login page

Emails are messaging sources that are crucial for performing information exchange. Email ID is considered by most people as the personal identification of employees or organizations. Thus, gathering the email IDs of critical personnel is one of the key tasks of ethical hackers.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

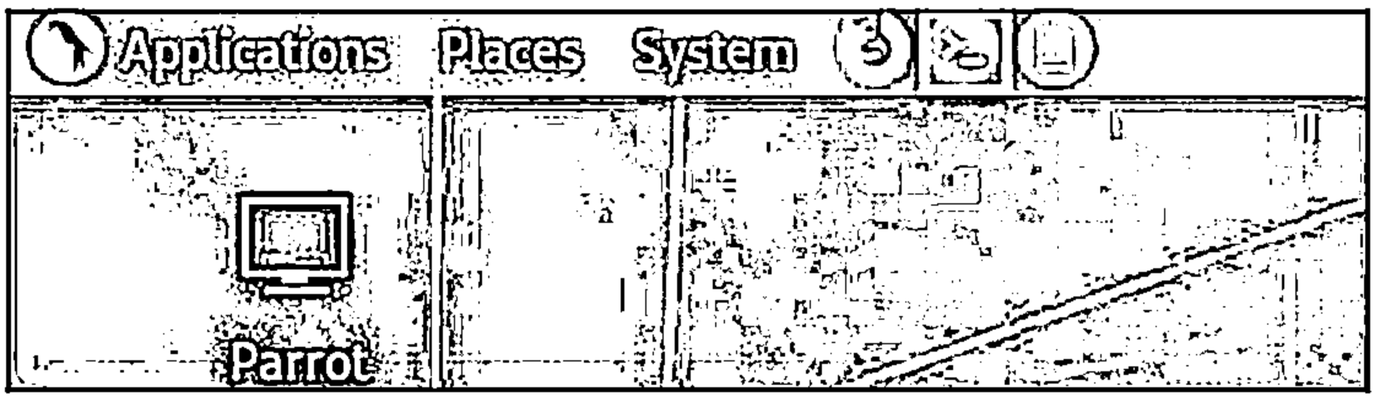


Figure 2.3.2: MATE Terminal Icon

4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

   Note: The password that you type will not be visible.
6. Now, type **cd** and press **Enter** to jump to the root directory.

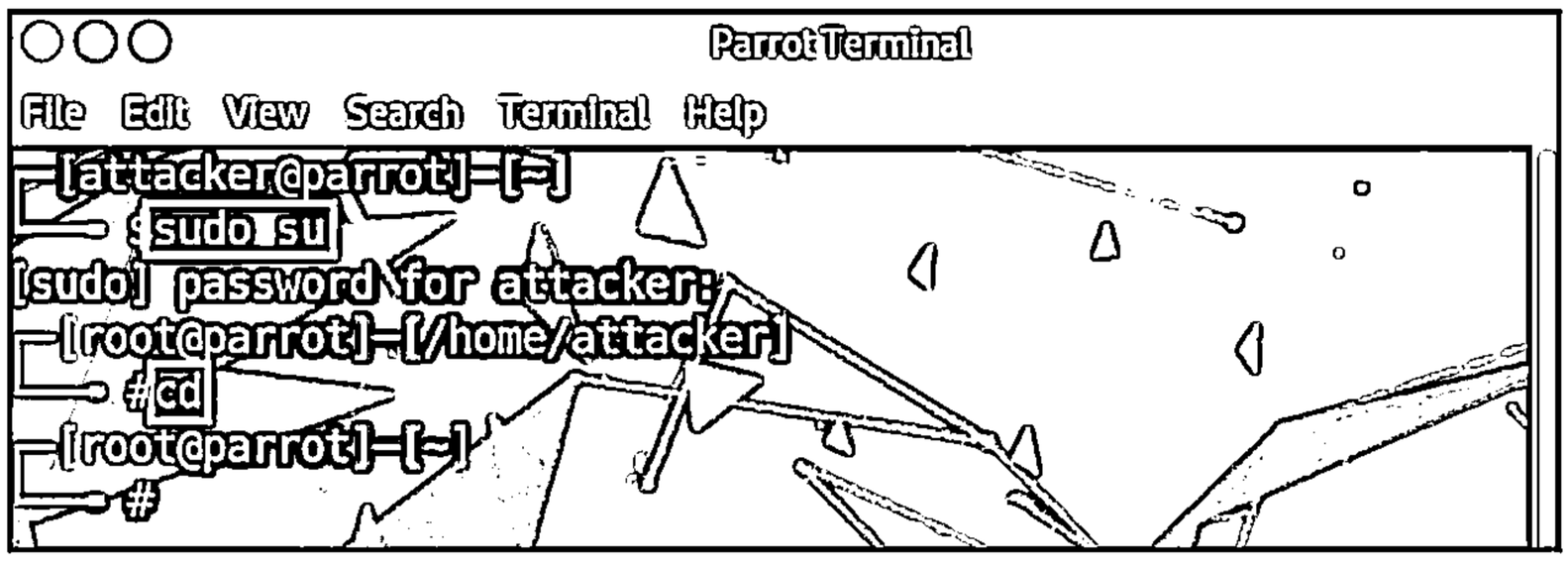


Figure 2.3.3: Running the programs as a root user

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

TASK 3.1

Extract Email List

theHarvester: This tool gathers emails, subdomains, hosts, employee names, open ports, and banners from different public sources such as search engines, PGP key servers, and the SHODAN computer database as well as uses Google, Bing, SHODAN, etc. to extract valuable information from the target domain. This tool is intended to help ethical hackers and pen testers in the early stages of the security assessment to understand the organization's footprint on the Internet. It is also useful for anyone who wants to know what organizational information is visible to an attacker.

7. In the terminal window, type **theHarvester -d microsoft.com -l 200 -b baidu** and press **Enter**.

Note: In this command, **-d** specifies the domain or company name to search, **-l** specifies the number of results to be retrieved, and **-b** specifies the data source.

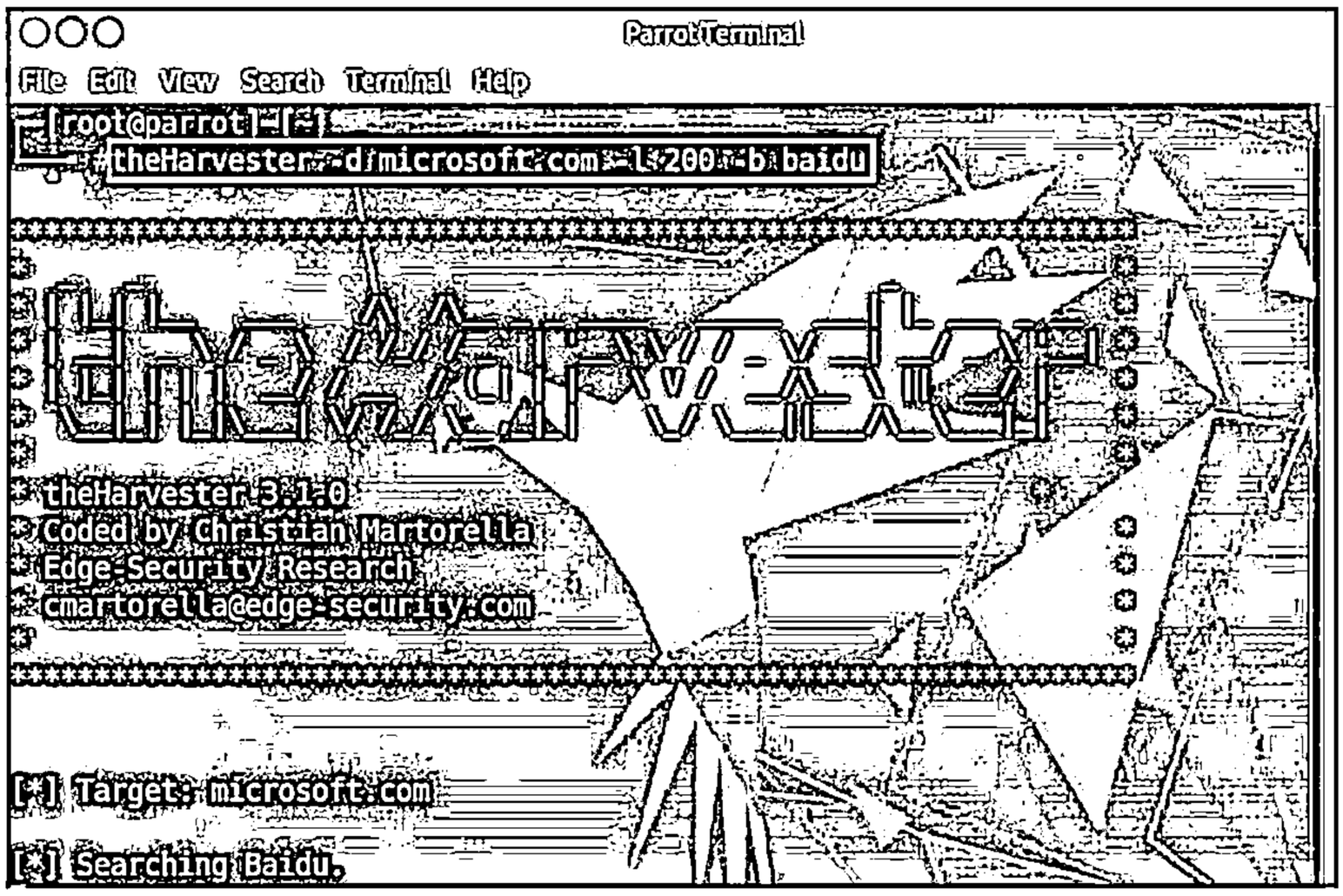


Figure 2.3.4: theHarvester search command

Note: Here, we specify Baidu search engine as a data source. You can specify different data sources (e.g., Baidu, bing, bingapi, dogpile, Google, GoogleCSE, Googleplus, Google-profiles, linkedin, pgp, twitter, vhost, virustotal, threatcrowd, crtsh, netcraft, yahoo, all) to gather information about the target.

8. theHarvester starts extracting the details and displays them on the screen. Scroll down to see the email IDs related to the target company from the Baidu source. It will also extract the target company hosts.

Note: Screenshots shown in this lab might differ.

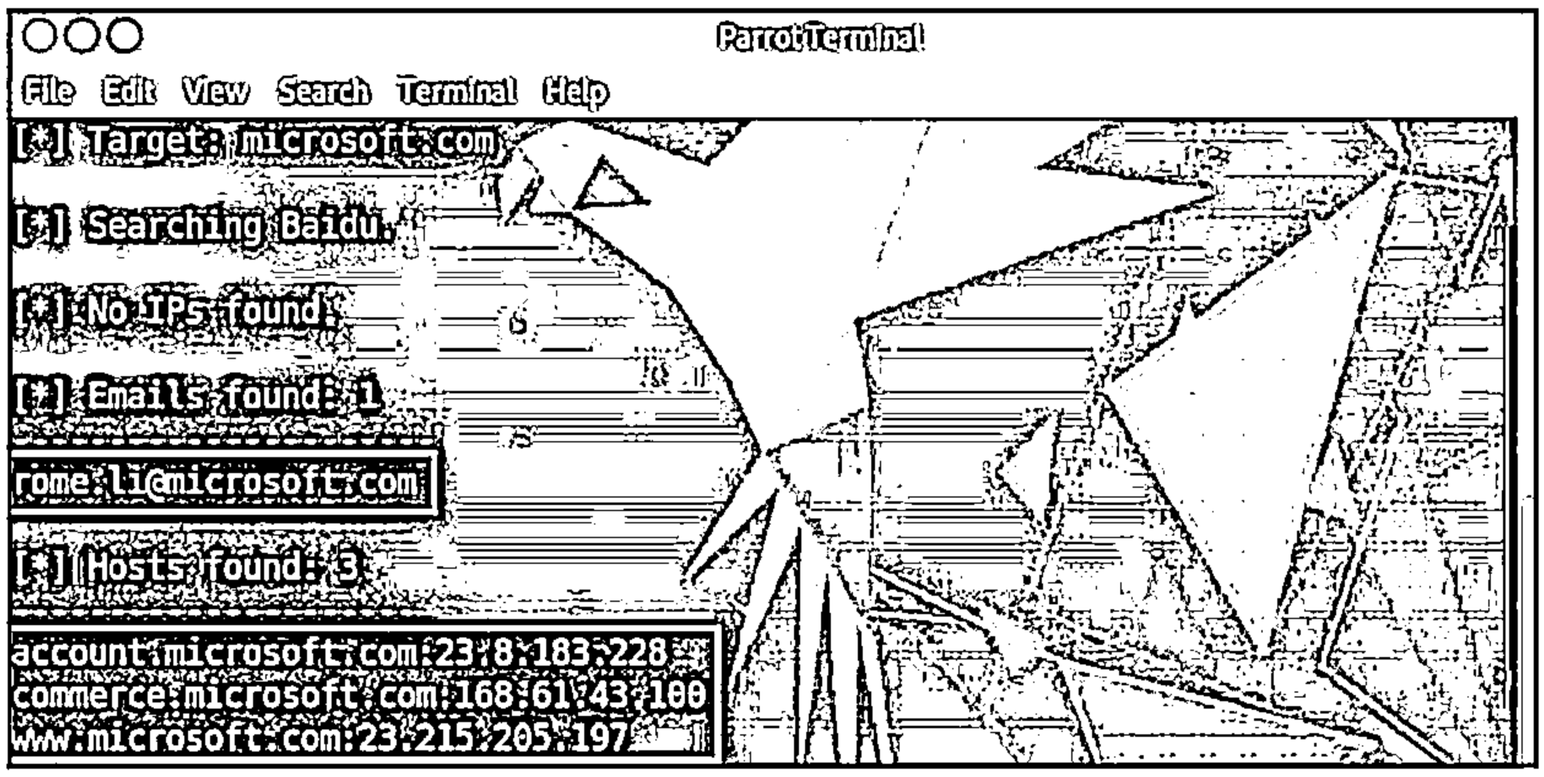


Figure 2.3.5: theHarvester result showing email list and hosts

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

9. This concludes the demonstration of gathering an email list using theHarvester.
10. Close all open windows and document all the acquired information.
11. Turn off the **Parrot Security** virtual machine.

TASK 4 Gather Information using Deep and Dark Web Searching

Here, we will understand the difference between surface web search and dark web search using Mozilla Firefox and Tor Browser.

The deep web consists of web pages and content that are hidden and unindexed and cannot be located using a traditional web browser and search engines. It can be accessed by search engines such as Tor Browser and The WWW Virtual Library.

1. Switch to the **Windows 10** virtual machine. Login to the **Windows 10** virtual machine with Username: **Admin** and Password: **Pa$$w0rd**.
2. Open a **File Explorer**, navigate to **E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance\Deep and Dark Web Footprinting Tools\Tor Browser**, and double-click **torbrowser-install-win64-8.5.4_en-US.exe**.
3. If the **Open File - Security Warning** window appears, click **Run**.
4. If the **User Account Control** pop-up appears, click **Yes**.
5. If the **Installer Language** window appears, select your preferred language (here, **English**) and click **OK**.
6. The **Tor Browser Setup** window appears. Follow the wizard steps (by selecting default options) to install Tor Browser.

The dark web or dark net is a subset of the deep web, where anyone can navigate anonymously without being traced. Deep and dark web search can provide critical information such as credit card details, passports information, identification card details, medical records, social media accounts, Social Security Numbers (SSNs), etc.

7. After the installation is complete, click the **Finish** button to launch Tor Browser.

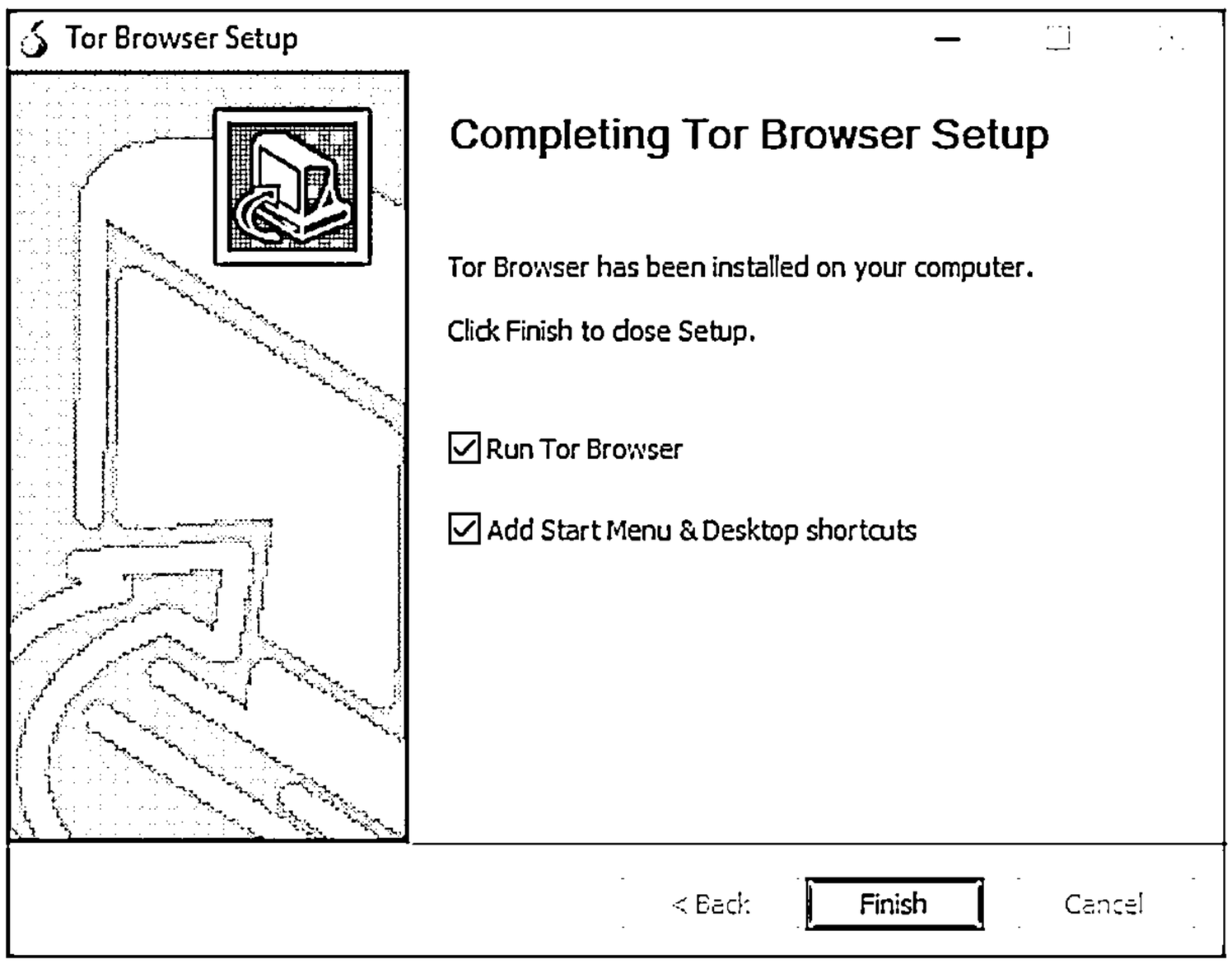


Figure 2.4.1: Tor Browser installation complete

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

8. The **Connect to Tor** window appears. Click the **Connect** button to directly browse through Tor Browser's default settings.

Note: If Tor is censored in your country or if you want to connect through Proxy, click the **Configure** button and continue.

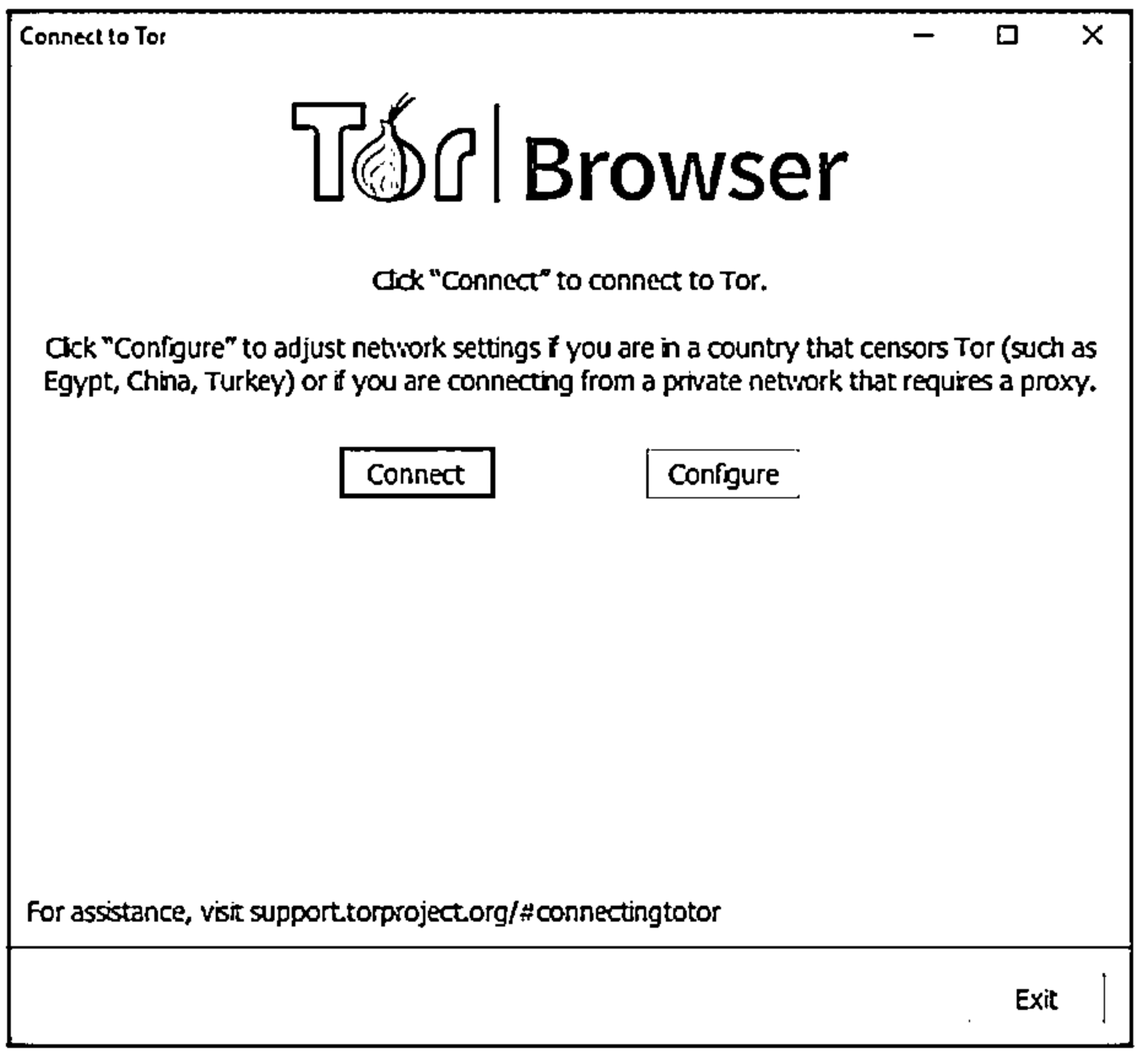


Figure 2.4.2: Tor Browser – Connect button

9. After a few seconds, the Tor Browser home page appears. The main advantage of Tor Browser is that it maintains the anonymity of the user throughout the session.

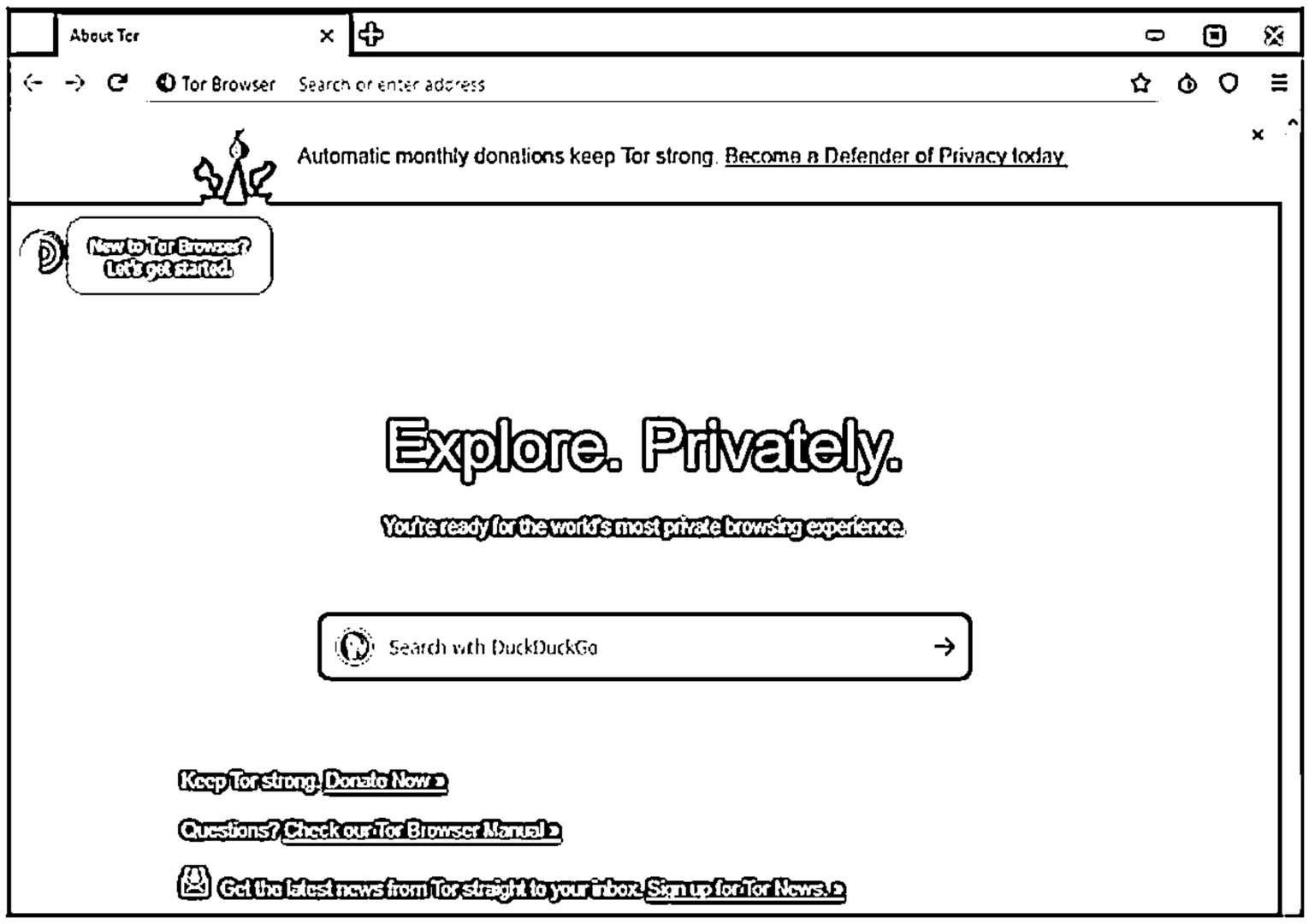


Figure 2.4.3: Tor Browser – Home Page

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

10. As an ethical hacker, you need to collect all possible information related to the target organization from the dark web. Before doing so, you must know the difference between surface web searching and dark web searching.

TASK 4.1

Perform Surface Web Search

11. To understand surface web searching, first, minimize **Tor Browser** and open **Mozilla Firefox**. Navigate to **www.google.com**; in the Google search bar, search for information related to **hacker for hire**. You will be presented with much irrelevant data, as shown in the screenshot.

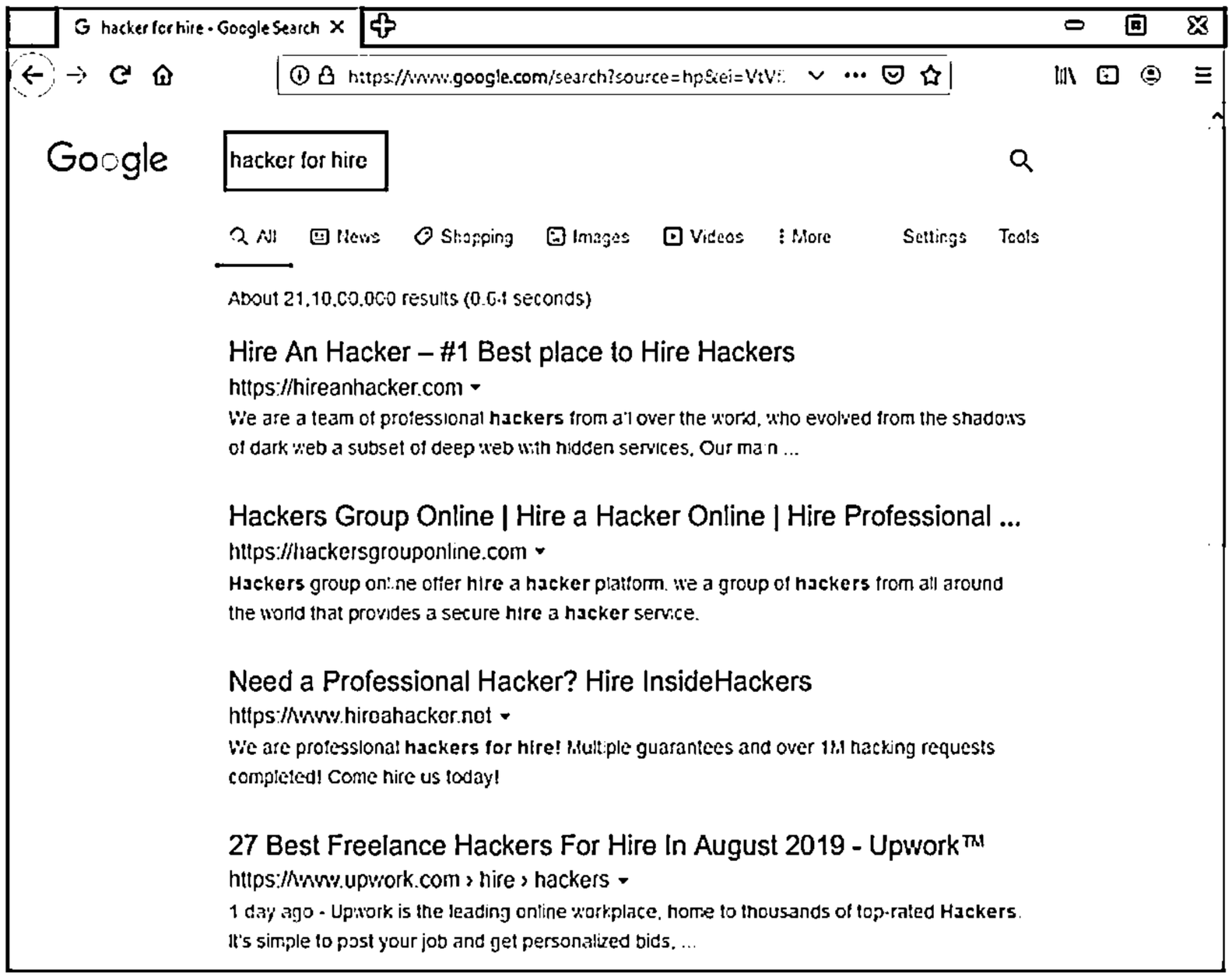


Figure 2.4.4: Normal search result

TASK 4.2

Perform Deep and Dark Web Search

12. Now switch to **Tor Browser** and search for the same (i.e., **hacker for hire**). You will find the relevant links related to the professional hackers who operate underground through the dark web.

Note: Tor uses the **DuckDuckGo** search engine to perform a dark web search. The results may vary in your environment.

13. Now, click on the toggle button that specifies the country of VPN/Proxy (here, by default **Germany** is selected) and select a relevant country (here, **Australia**).

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

Note: The default country of VPN/Proxy may vary in your environment, since it is randomly chosen by Tor while initiating a session.

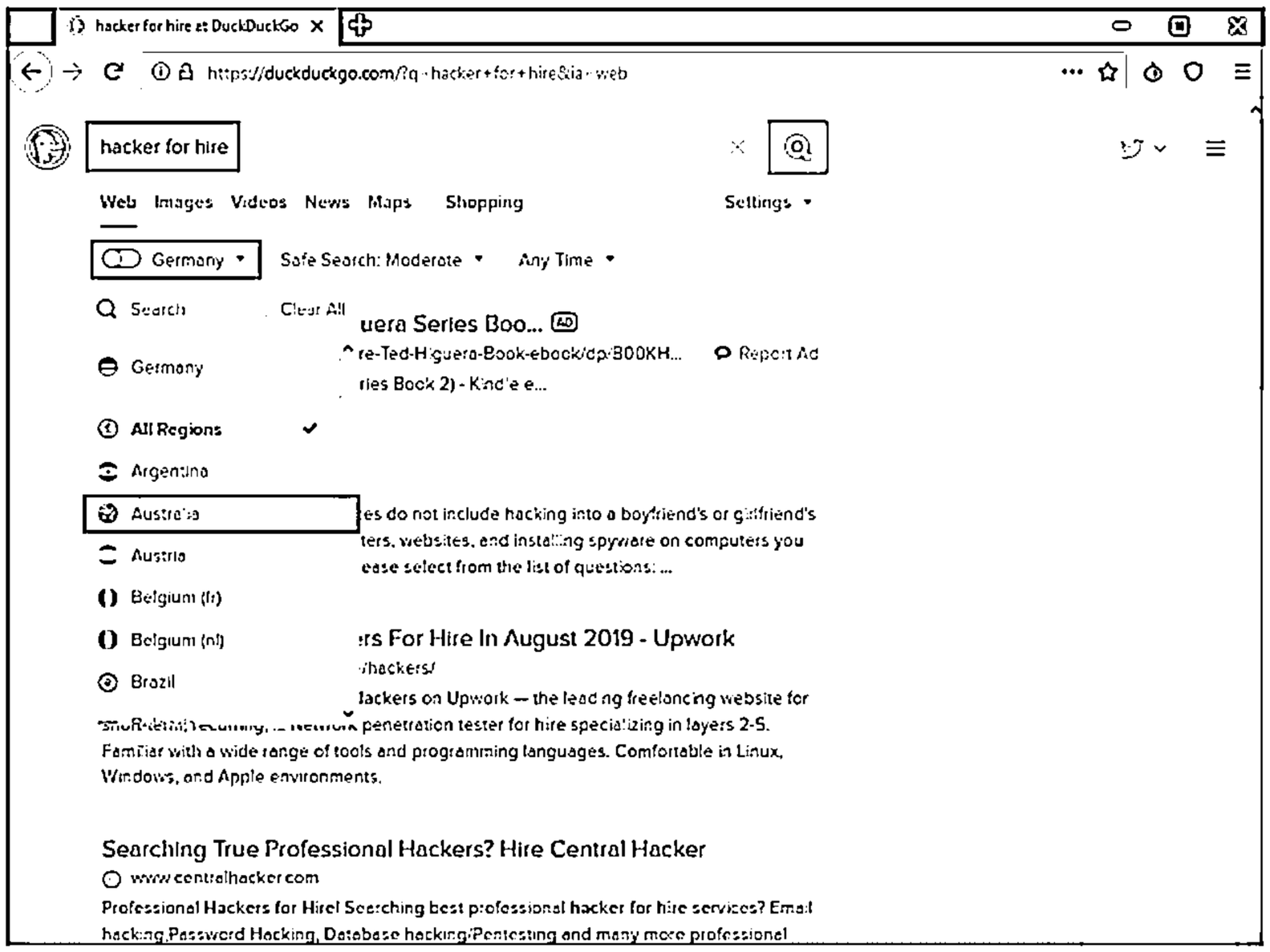


Figure 2.4.5: VPN/Proxy setting for search

14. Search results for **hacker for hire** will be loaded, as shown in the screenshot. Click to open any of the search results (here, **https://hackerforhire.com**).

Note: Screenshots shown in this lab might differ.

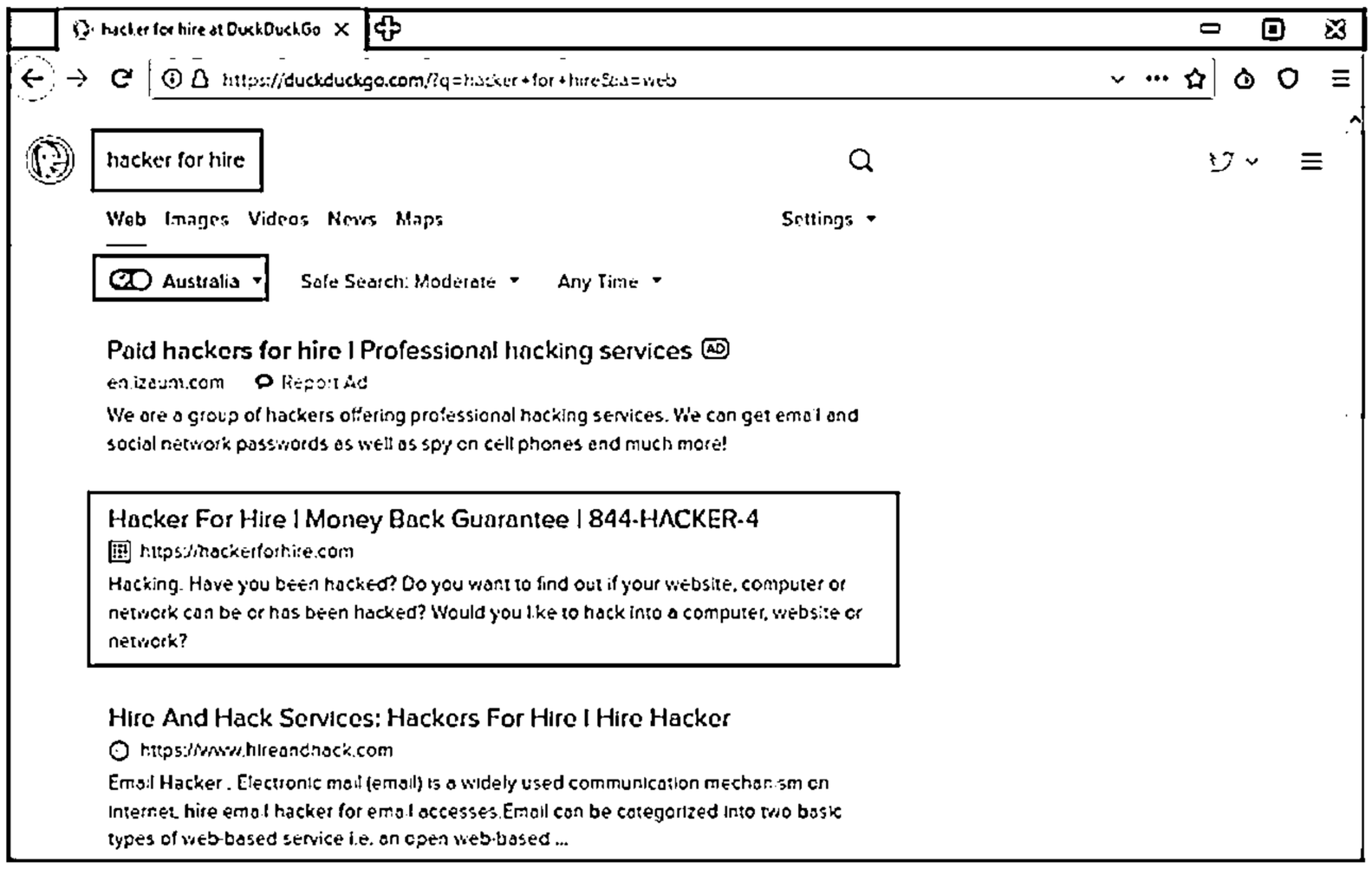


Figure 2.4.6: Tor dark web search result

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

15. The **https://hackerforhire.com** webpage opens up, as shown in the screenshot. You can see that the site belongs to professional hackers who operate underground.

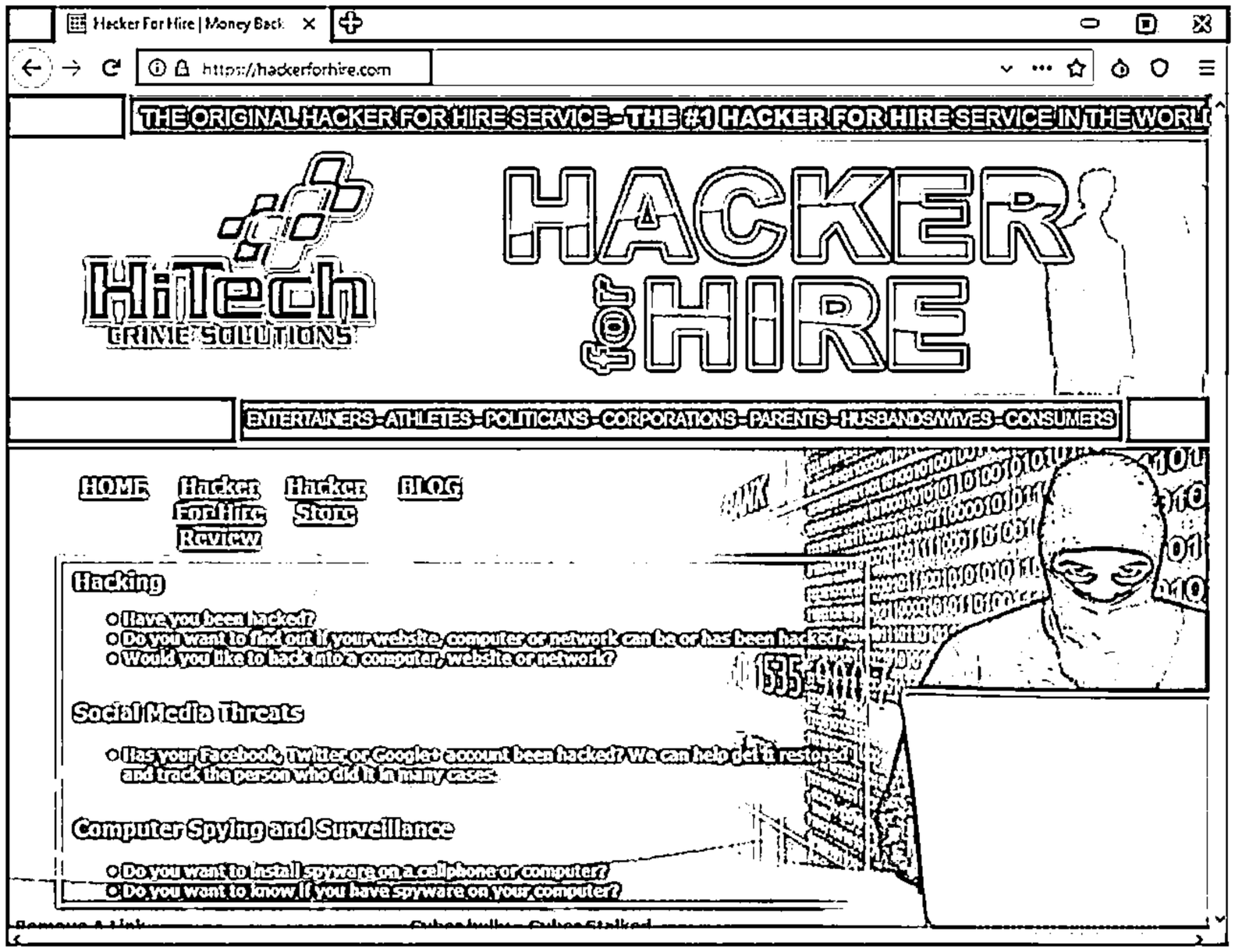


Figure 2.4.7: hackerforhire.com website

16. Hackerforhire.com is an example. These search results will help you in identifying professional hackers. However, as an ethical hacker, you can gather critical and sensitive information about your target organization using deep and dark web search.

17. You can also anonymously explore the following onion sites using Tor Brower to gather other relevant information about the target organization:

You can also use tools such as **ExoneraTor** (https://metrics.torproject.org), **OnionLand Search engine** (https://onionlandsearchengine.com), etc. to perform deep and dark web browsing.

- **The Hidden Wiki** is an onion site that works as a Wikipedia service of hidden websites. (http://zqktlwi4fecvo6ri.onion/wiki/index.php/Main_Page)
- **FakeID** is an onion site for creating fake passports (http://fakeidskhfik46ux.onion/)
- **The Paypal Cent** is an onion site that sells PayPal accounts with good balances (http://nare7pqnmnojs2pg.onion/)

18. This concludes the demonstration of gathering information using deep and dark web searching using Tor Browser.

19. Close all open windows and document all the acquired information.

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

TASK 5 Determine Target OS Through Passive Footprinting

Operating system information is crucial for every ethical hacker. Ethical hackers can acquire details of the operating system running on the target machine by performing various passive footprinting techniques.

Here, we will gather target OS information through passive footprinting using the Censys web service.

1. In the **Windows 10** virtual machine, open any web browser (here, **Mozilla Firefox**) and navigate to **https://censys.io/domain?q=**.
2. In the **Websites** search bar, type the target website (here, **eccouncil.org**) and press **Enter**. From the results, click any result (here, **eccouncil.org**) from which you want to gather the OS details.

Note: Screenshots shown in this lab might differ.

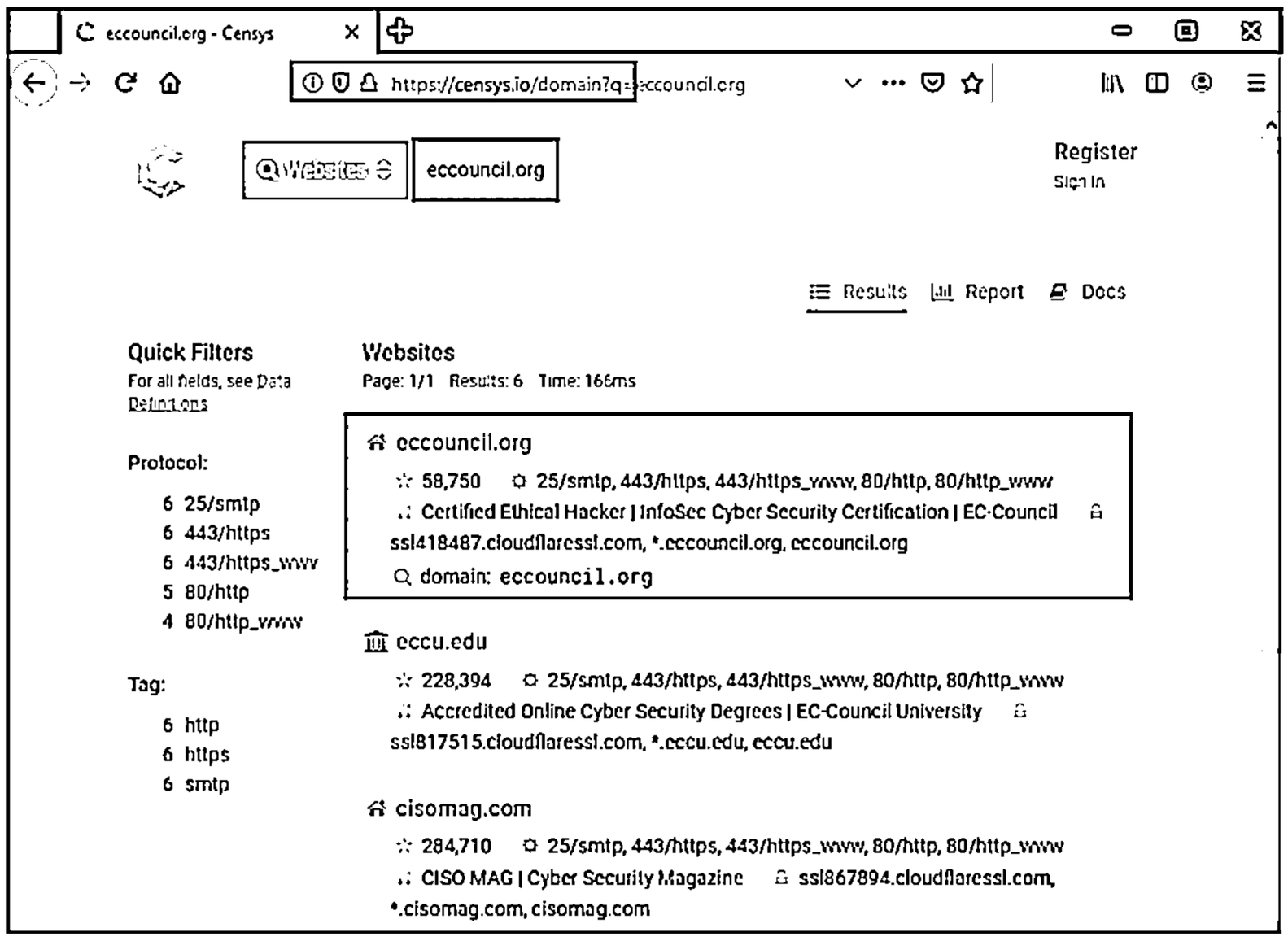


Figure 2.5.1: Censys result about the target website

3. The **eccouncil.org** page appears, as shown in the screenshot. Under the **Basic Information** section, you can observe that the **OS** is **Windows**. Apart from this, you can also observe that the **Server** on which the **HTTP** is running is **cloudflare**.

Note: Screenshots shown in this lab might differ.

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

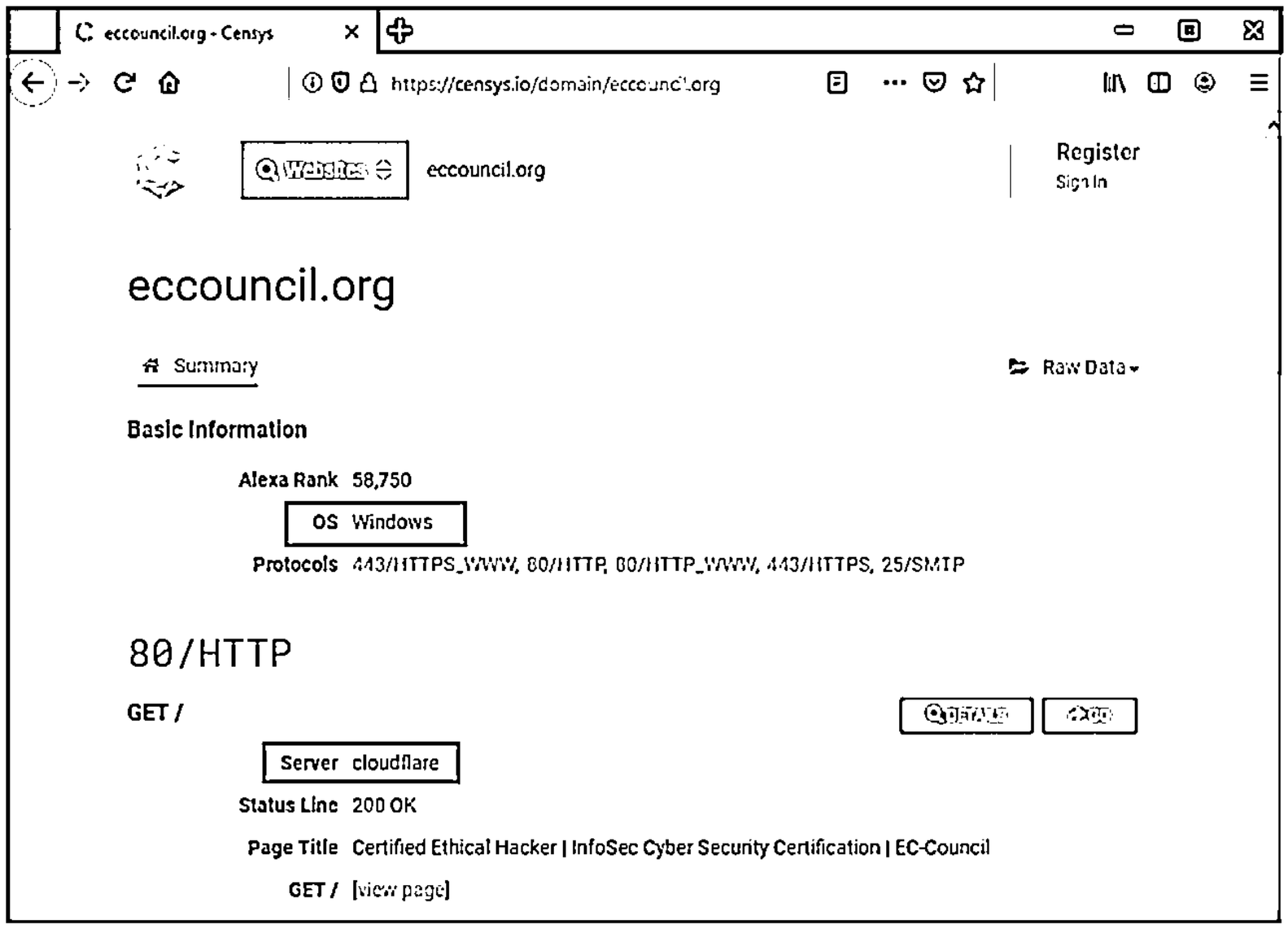


Figure 2.5.2: Censys result - OS details

You can also use web services such as **Netcraft** (https://www.netcraft.com), **Shodan** (https://www.shodan.io), etc. to gather OS information of target organization through passive footprinting.

4. This concludes the demonstration of gathering OS information through passive footprinting using the Censys web service.
5. Close all open windows and document all the acquired information.
6. Turn off the **Windows 10** virtual machine.

Lab Analysis

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

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT 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

Perform Footprinting Through Social Networking Sites

Social networking services are online services, platforms, or sites that focus on facilitating the building of social networks or social relations among people.

ICON KEY

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

Lab Scenario

As a professional ethical hacker, during information gathering, you need to gather personal information about employees working in critical positions in the target organization; for example, the Chief Information Security Officer, Security Architect, or Network Administrator. By footprinting through social networking sites, you can extract personal information such as name, position, organization name, current location, and educational qualifications. Further, you can find professional information such as company or business, current location, phone number, email ID, photos, videos, etc. The information gathered can be useful to perform social engineering and other types of advanced attacks.

Lab Objectives

- Gather employees' information from LinkedIn using theHarvester
- Gather personal information from various social networking sites using Sherlock
- Gather information using Followerwonk

Lab Environment

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance

To carry out this lab, you need:

- Windows 10 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

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

Lab Duration

Time: 15 Minutes

Overview of Social Networking Sites

Social networking sites are online services, platforms, or other sites that allow people to connect and build interpersonal relations. People usually maintain profiles on social networking sites to provide basic information about themselves and to help make and maintain connections with others; the profile generally contains information such as name, contact information (cellphone number, email address), friends' information, information about family members, their interests, activities, etc. On social networking sites, people may also post their personal information such as date of birth, educational information, employment background, spouse's names, etc. Organizations often post information such as potential partners, websites, and upcoming news about the company. Thus, social networking sites often prove to be valuable information resources. Examples of such sites include LinkedIn, Facebook, Instagram, Twitter, Pinterest, YouTube, etc.

Lab Tasks

TASK 1

Gather Employees' Information from LinkedIn using theHarvester

LinkedIn is a social networking website for industry professionals. It connects the world's human resources to aid productivity and success. The site contains personal information such as name, position, organization name, current location, educational qualifications, etc.

Here, we will gather information about the employees (name and job title) of a target organization that is available on LinkedIn using theHarvester tool.

1. Turn on **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

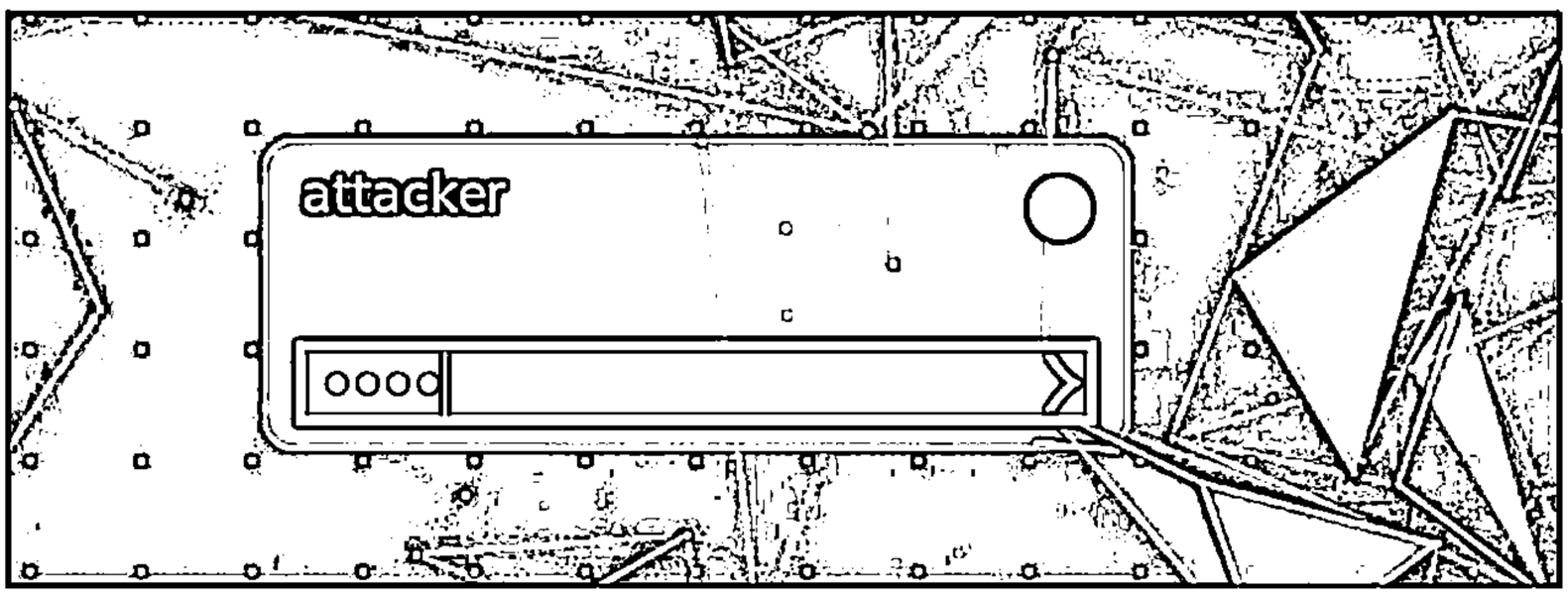


Figure 3.1.1: Parrot Security login page

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

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

- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

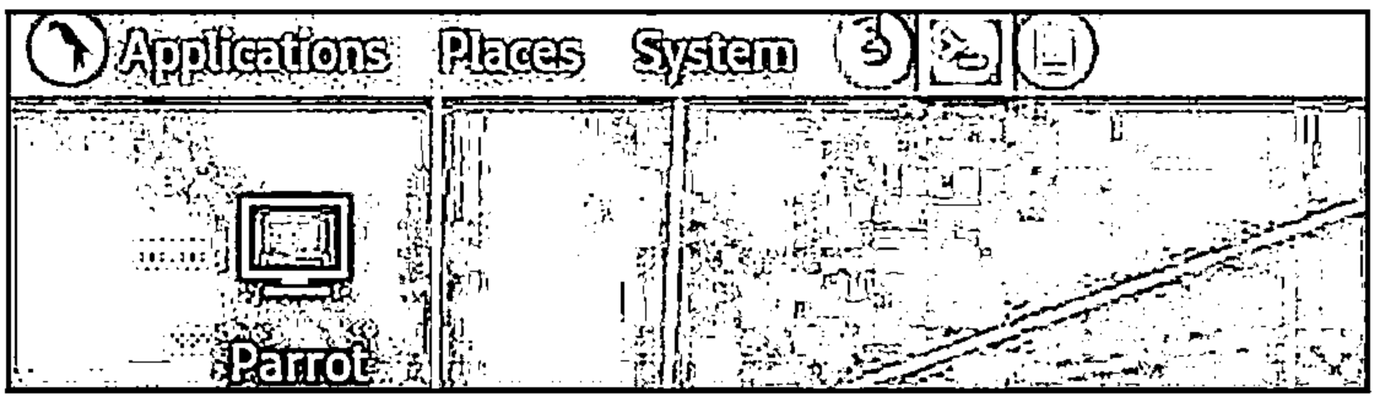


Figure 3.1.2: MATE Terminal Icon

4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

6. Now, type **cd** and press **Enter** to jump to the root directory.

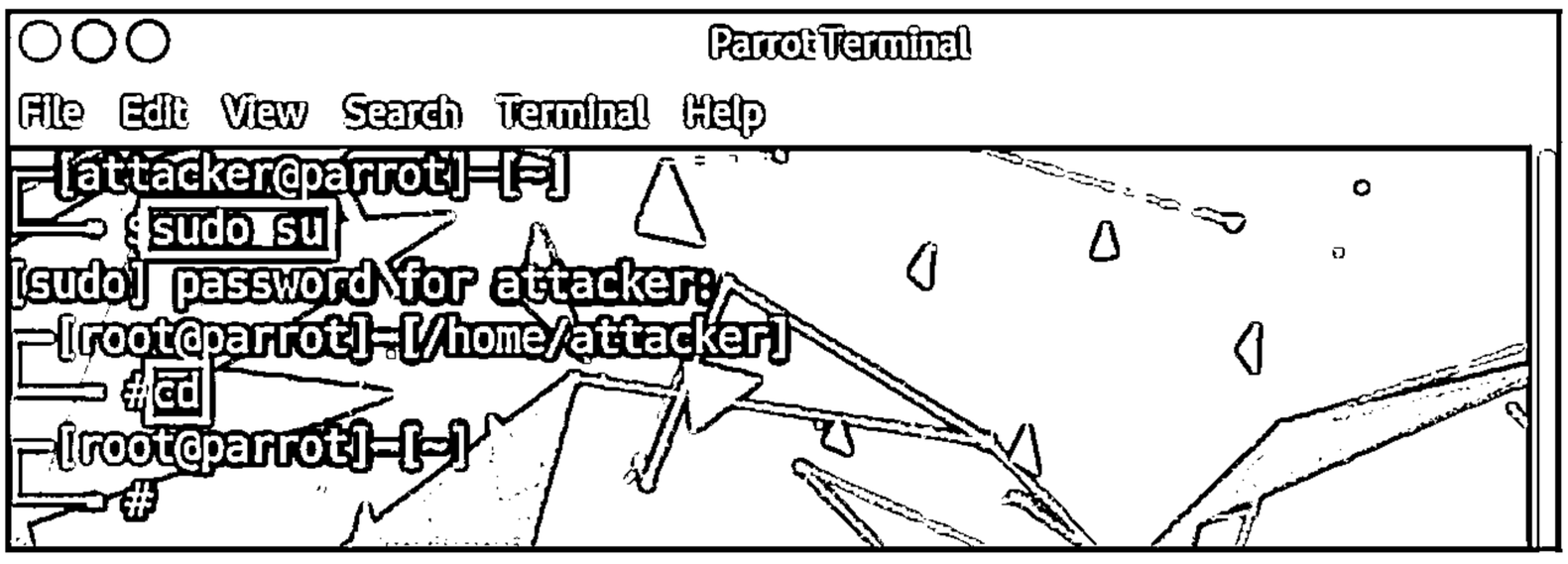


Figure 3.1.3: Running the programs as a root user

7. In the terminal window, type **theHarvester -d eccouncil -l 200 -b linkedin** and press **Enter** to see 200 results of EC-Council from the LinkedIn source. Scroll down to view all the 200 results of the employees of the EC-Council.

Note: In this command, **-d** specifies the domain or company name to search, **-l** specifies the number of results to be retrieved, and **-b** specifies the data source as LinkedIn.

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

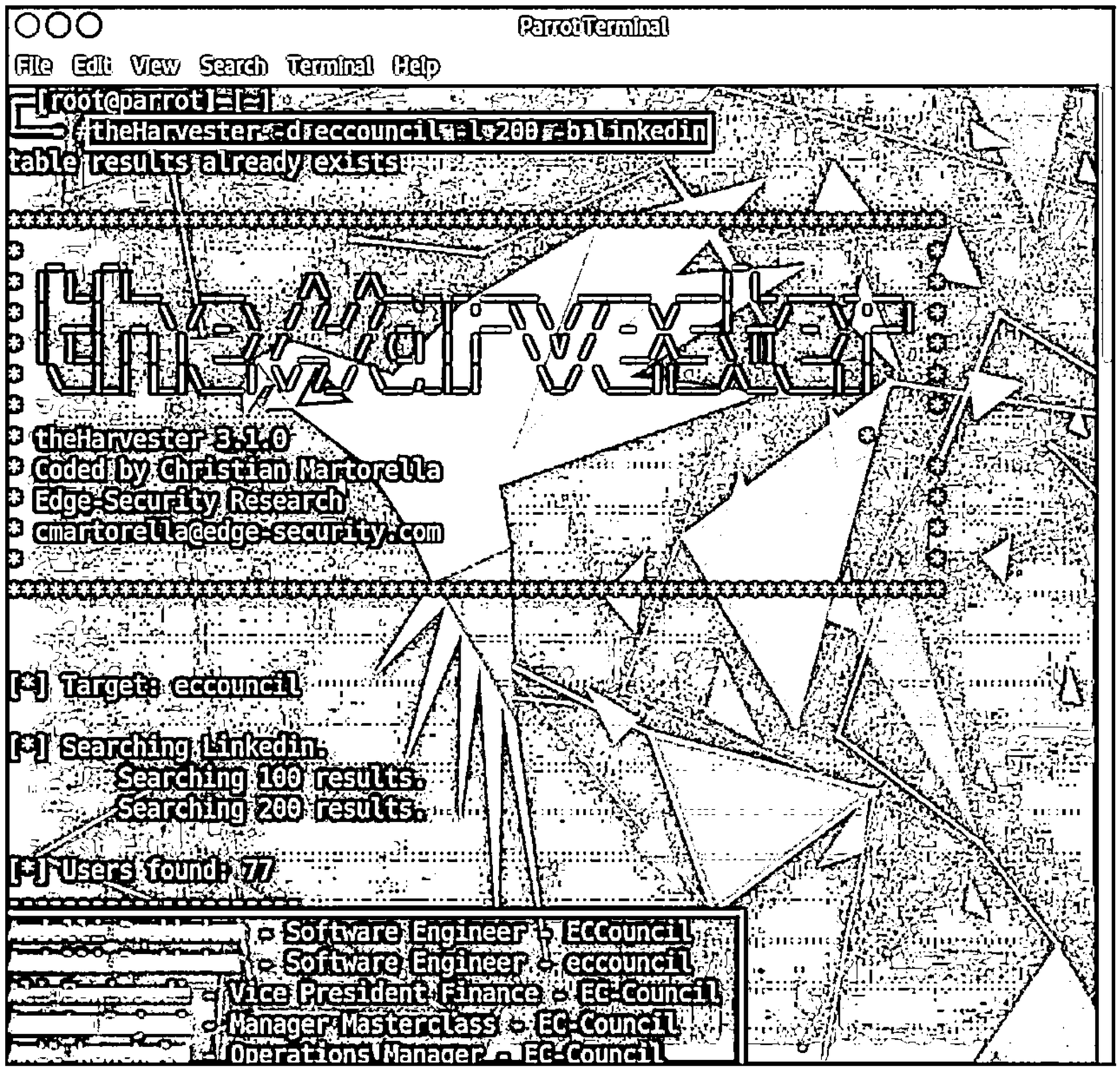


Figure 3.1.4: theHarvester result

8. This concludes the demonstration of gathering employees' information from LinkedIn using theHarvester.
9. Close all open windows and document all the acquired information.

TASK 2 Gather Personal Information from Various Social Networking Sites using Sherlock

Sherlock is a python-based tool that is used to gather information about a target person over various social networking sites. Sherlock searches a vast number of social networking sites for a given target user, locates the person, and displays the results along with the complete URL related to the target person.

1. In the **Parrot Security** virtual machine, click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

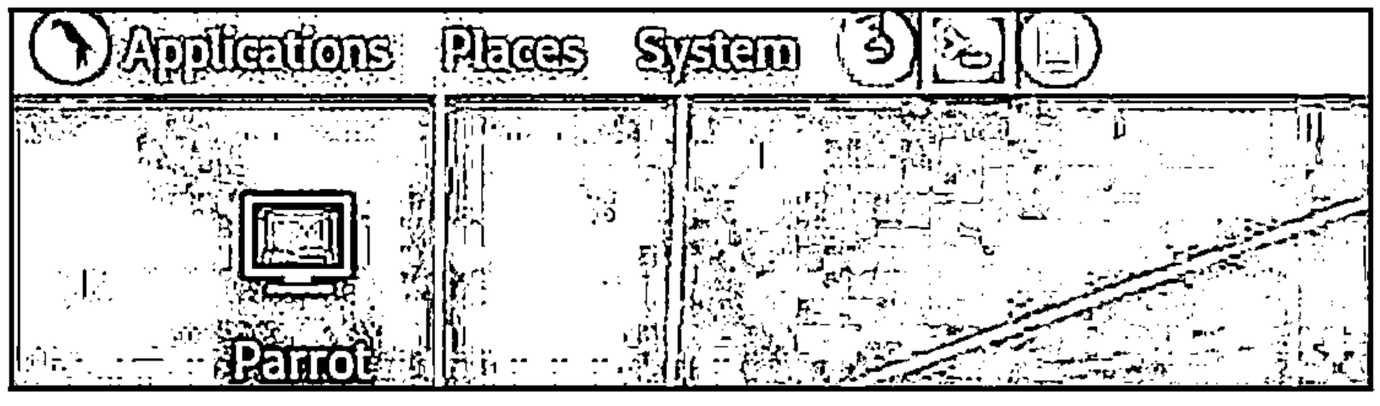


Figure 3.2.1: MATE Terminal Icon

2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

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

3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

4. Now, type **cd** and press **Enter** to jump to the root directory.

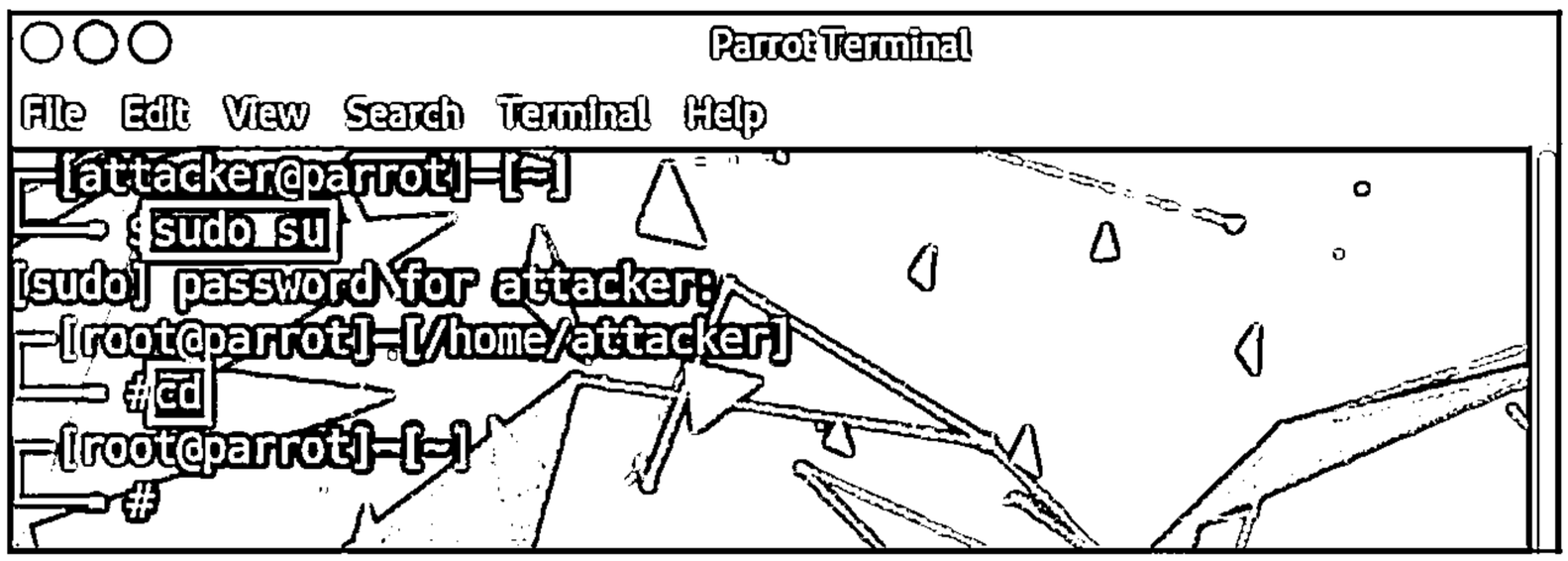


Figure 3.2.2: Running the programs as a root user

5. In the **Parrot Terminal** window, type **git clone https://github.com/sherlock-project/sherlock.git** and press **Enter**.

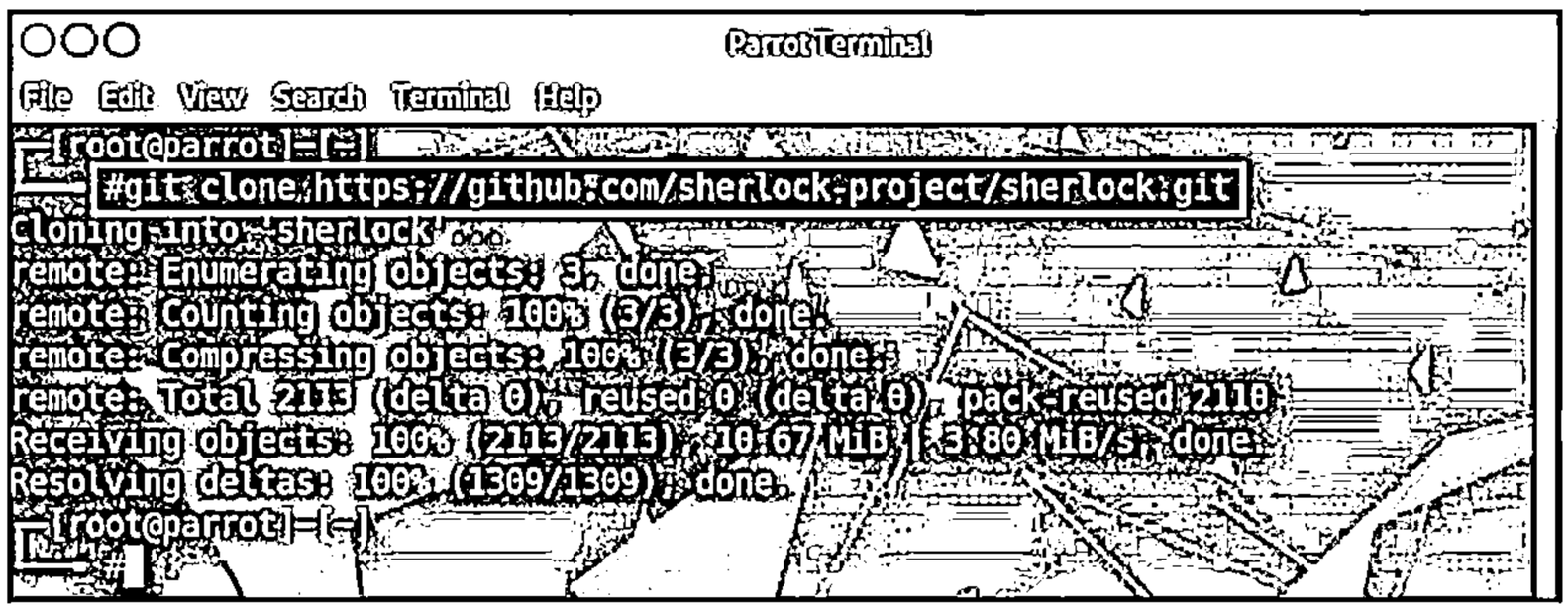


Figure 3.2.3: Cloning Sherlock tool

Note: You can also access the tool repository from the **CEH-Tools** folder available in **Windows 10** virtual machine, in case, the GitHub link does not exist, or you are unable to clone the tool repository. Follow the steps below in order to access **CEH-Tools** folder from the **Parrot Security** virtual machine:

- Open any explorer window and press **Ctrl+L**. The **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access **Windows 10** shared folders.

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

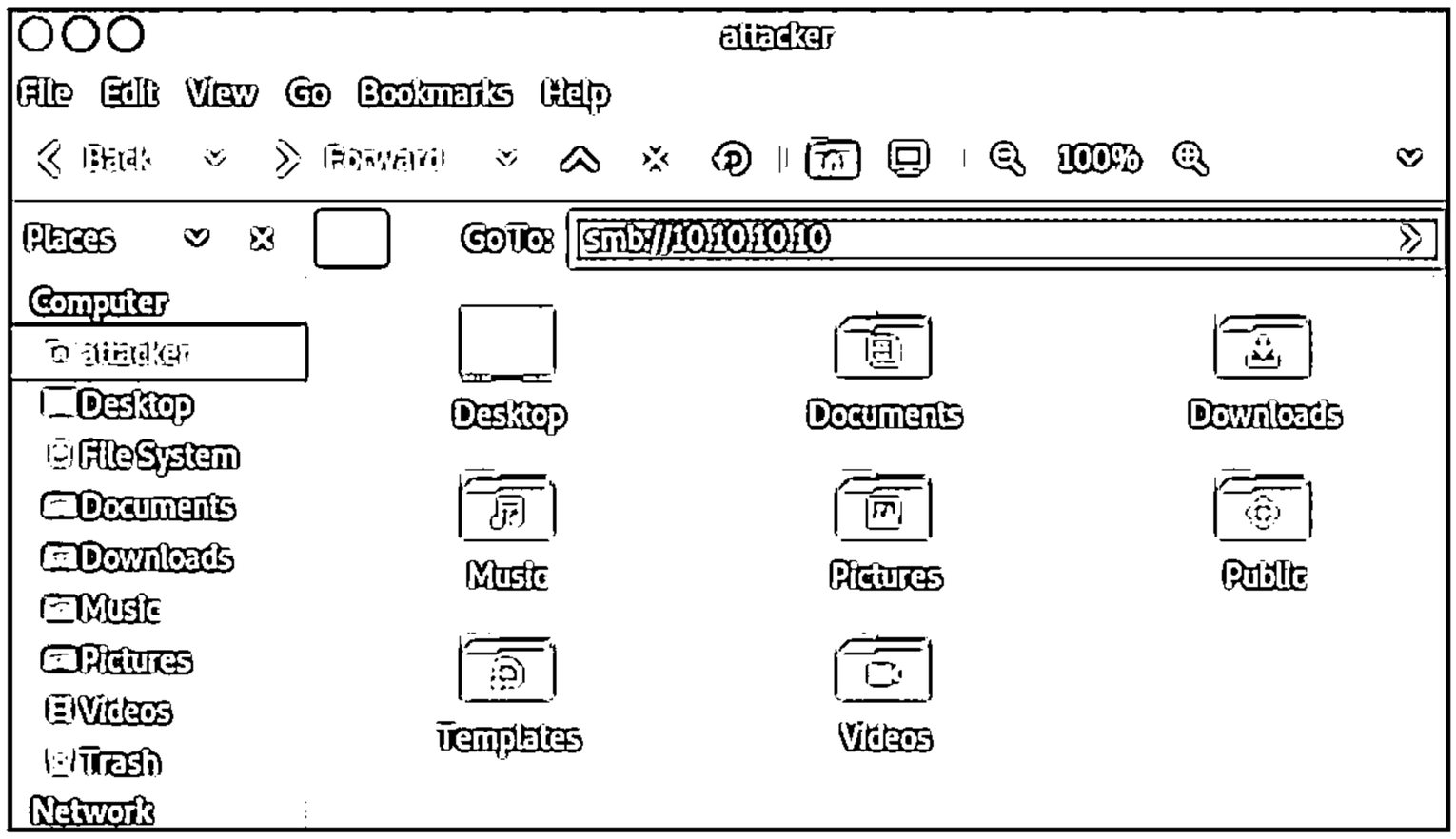


Figure 3.2.4: Accessing Windows 10 shared folder

- The security pop-up appears; enter the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.

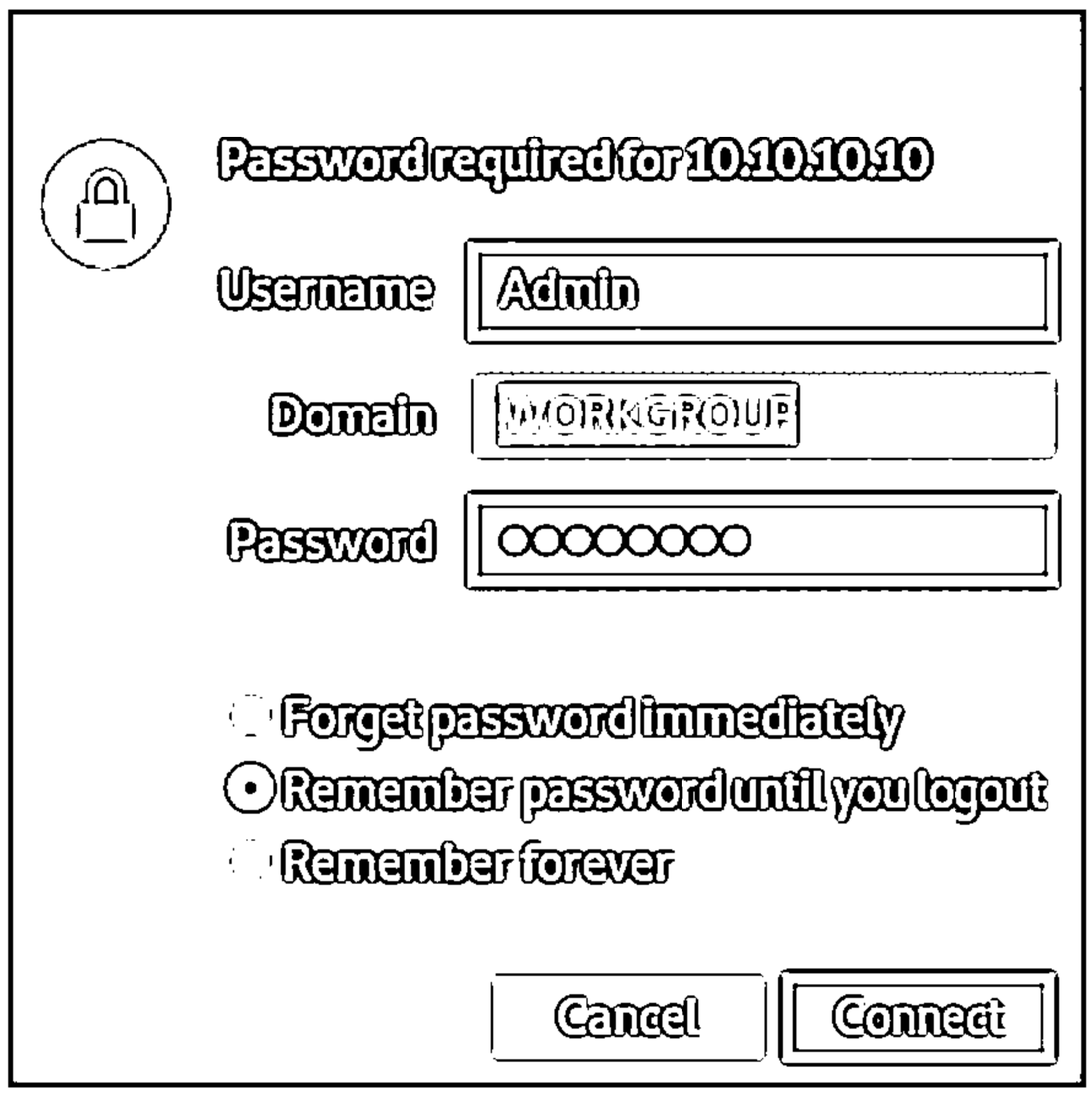


Figure 3.2.5: Security pop-up

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

- The **Windows shares on 10.10.10.10** window appears; navigate to the location **CEH-Tools/CEHv11 Module 02 Footprinting and Reconnaissance/GitHub Tools/** and copy the **sherlock** folder.

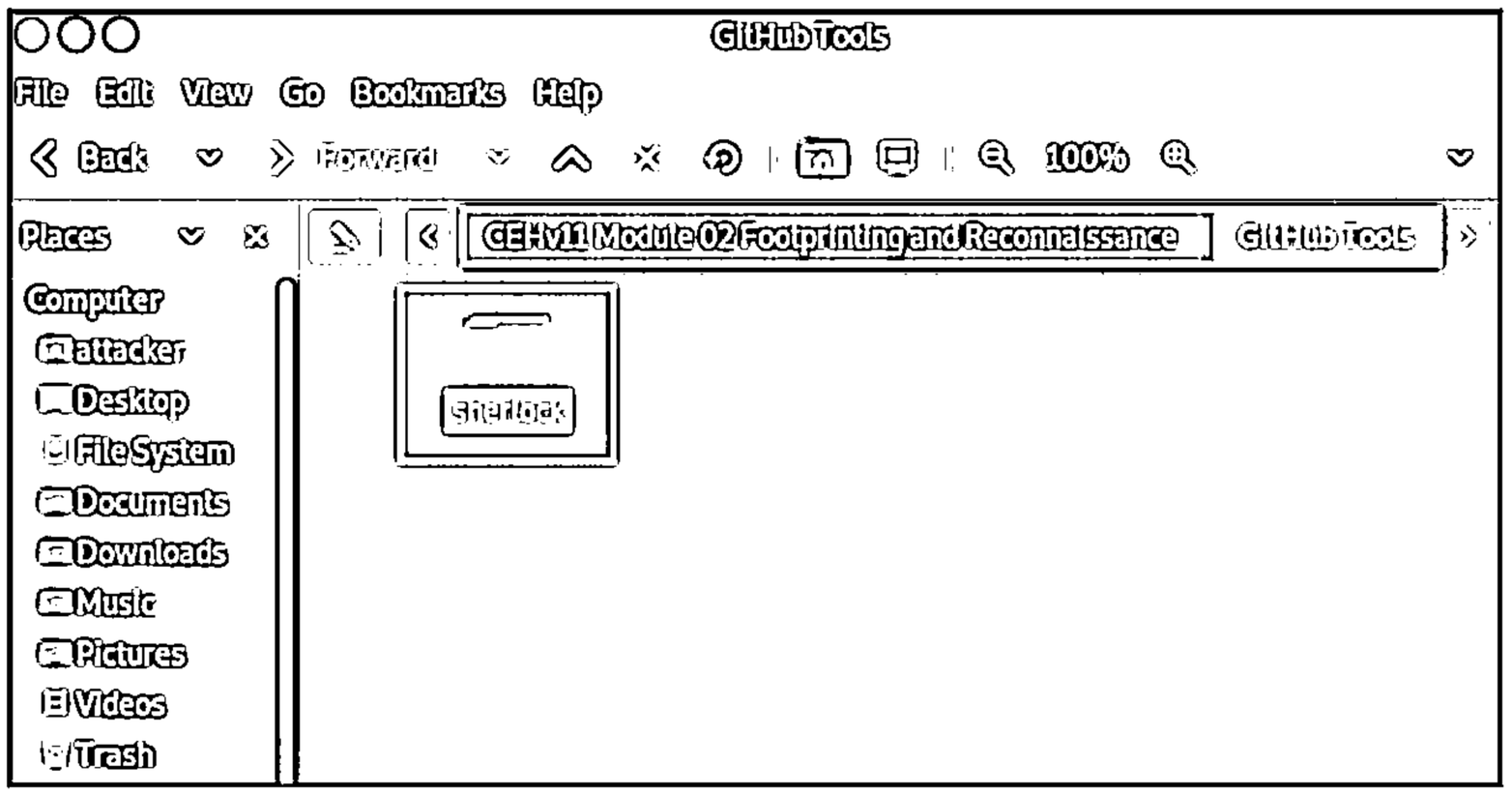


Figure 3.2.6: Copy sherlock folder

- Paste the copied **sherlock** folder on the location **/home/attacker/.**

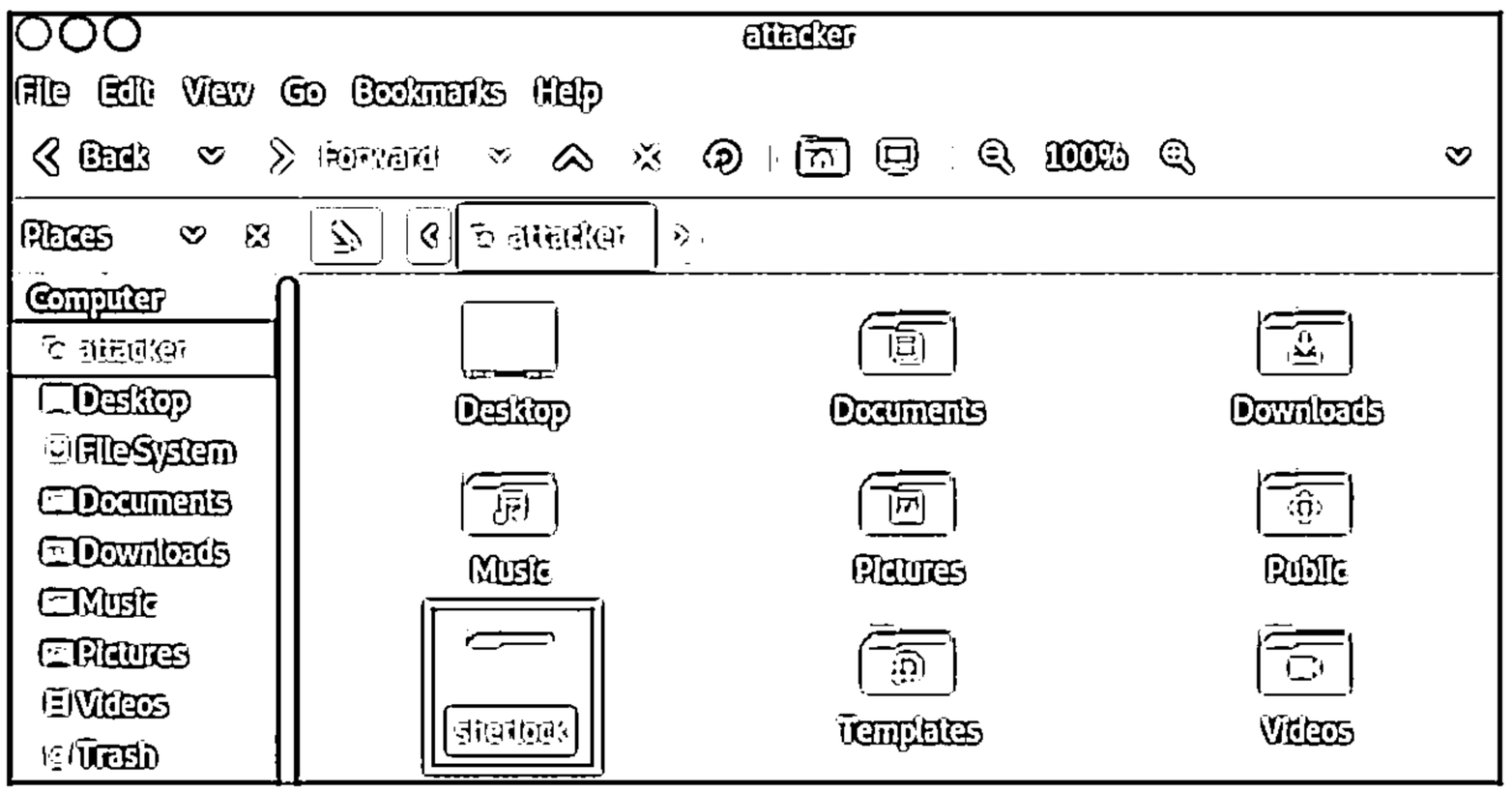


Figure 3.2.7: Paste the directory

- In the terminal window, type **mv /home/attacker/sherlock /root/.**

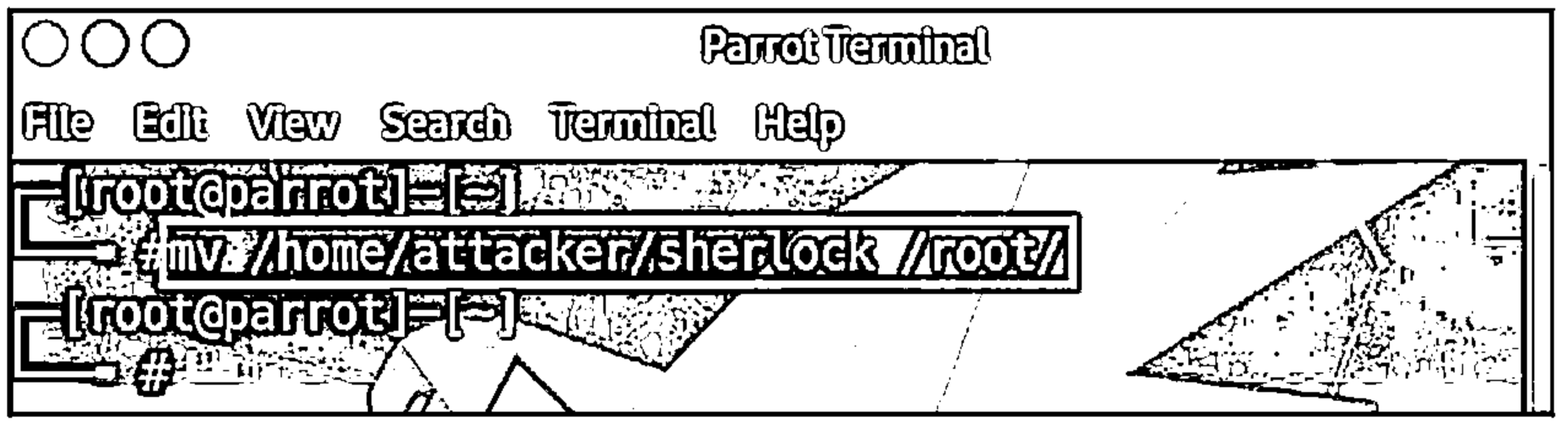


Figure 3.2.8: Move the directory to root folder

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

6. Type **cd sherlock** and press **Enter** to navigate to the **sherlock** folder. To install the python-pip requirements, type **python3 -m pip install -r requirements.txt** and press **Enter**.

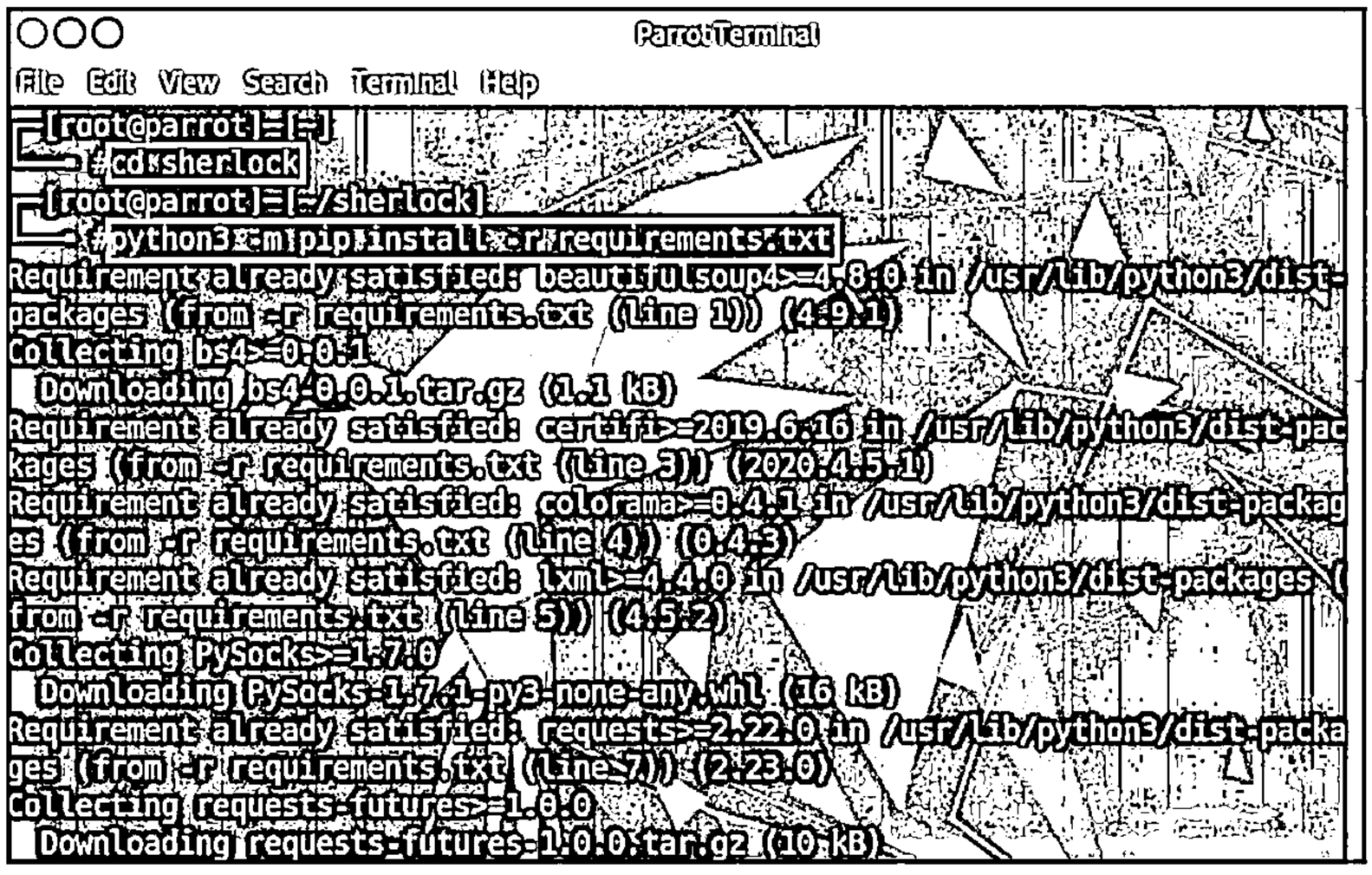


Figure 3.2.9: requirements.txt installation

7. Once the installation is complete, type **cd sherlock** and press **Enter**.

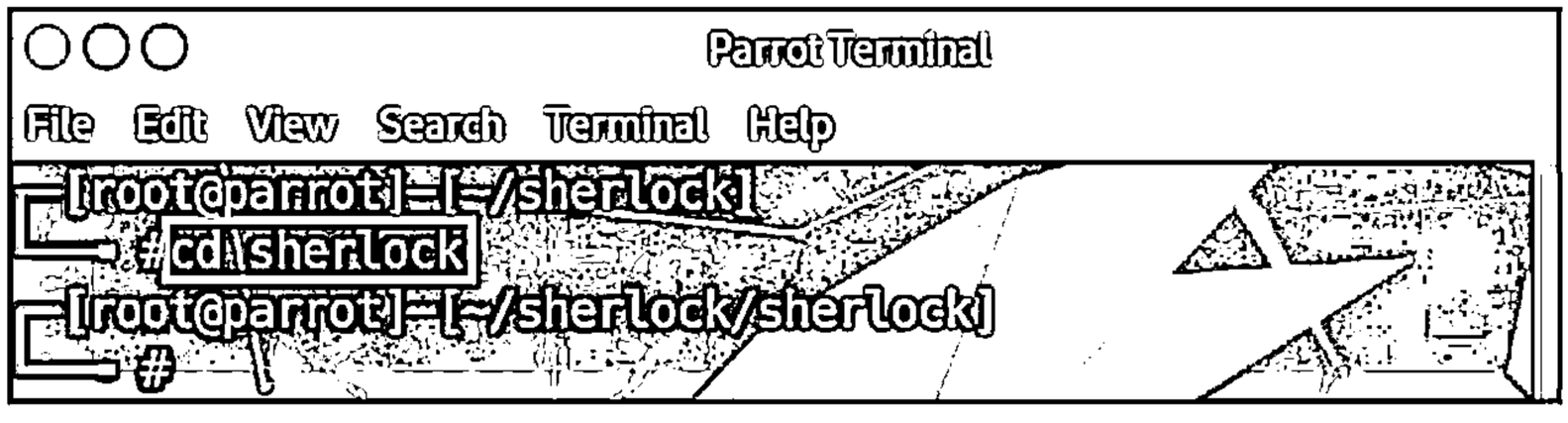


Figure 3.2.10: Navigate to the sherlock folder

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

8. Now, type **python3 sherlock.py satya nadella** and press **Enter**. You will get all the URLs related to Satya Nadella, as shown in the screenshot. Scroll down to view all the results.

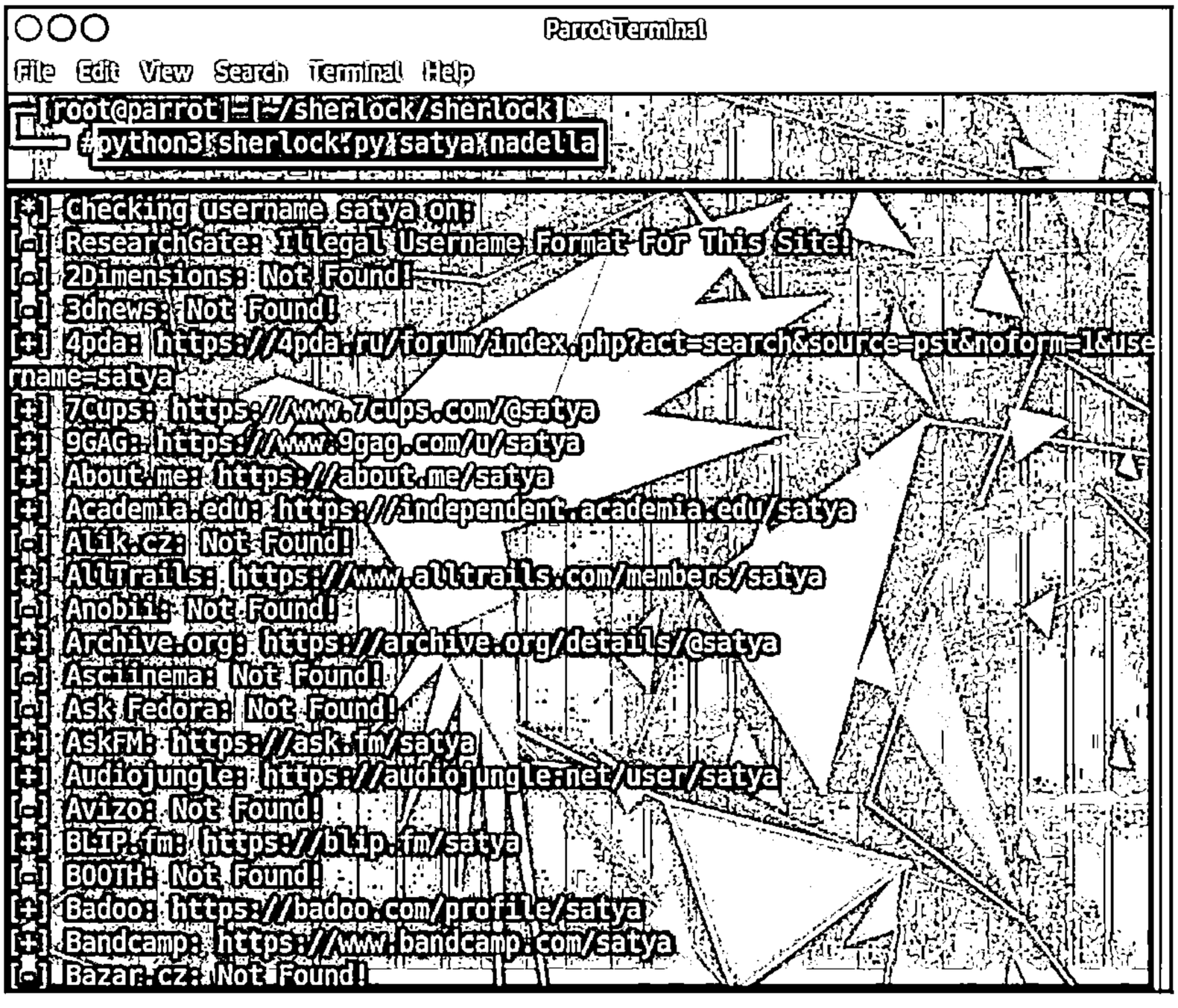


Figure 3.2.11: sherlock search result

You can also use tools such as Social Searcher (https://www.social-searcher.com), UserRecon (https://github.com), etc. to gather additional information related to the target company and its employees from social networking sites.

9. This concludes the demonstration of gathering person information from various social networking sites using Sherlock.
10. Close all open windows and document all the acquired information.
11. Turn off the **Parrot Security** virtual machine.

TASK 3 Gather Information using Followerwonk

Followerwonk is an online tool that helps you explore and grow your social graph, digging deeper into Twitter analytics; for example, Who are your followers? Where are they located? When do they tweet? This can be used to gather Twitter information about any target organization or individual.

1. Turn on the **Windows 10** virtual machine.
2. Login to the **Windows 10** virtual machine with Username: **Admin** and Password: **Pa$$w0rd**.

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

3. Open any web browser (here, **Mozilla Firefox**) and navigate to **https://followerwonk.com/analyze**. In the **screen name** search bar, type your target individual's twitter tag (here, **@satyanadella**) and click the **Do it** button to analyze the users whom the target person follows.

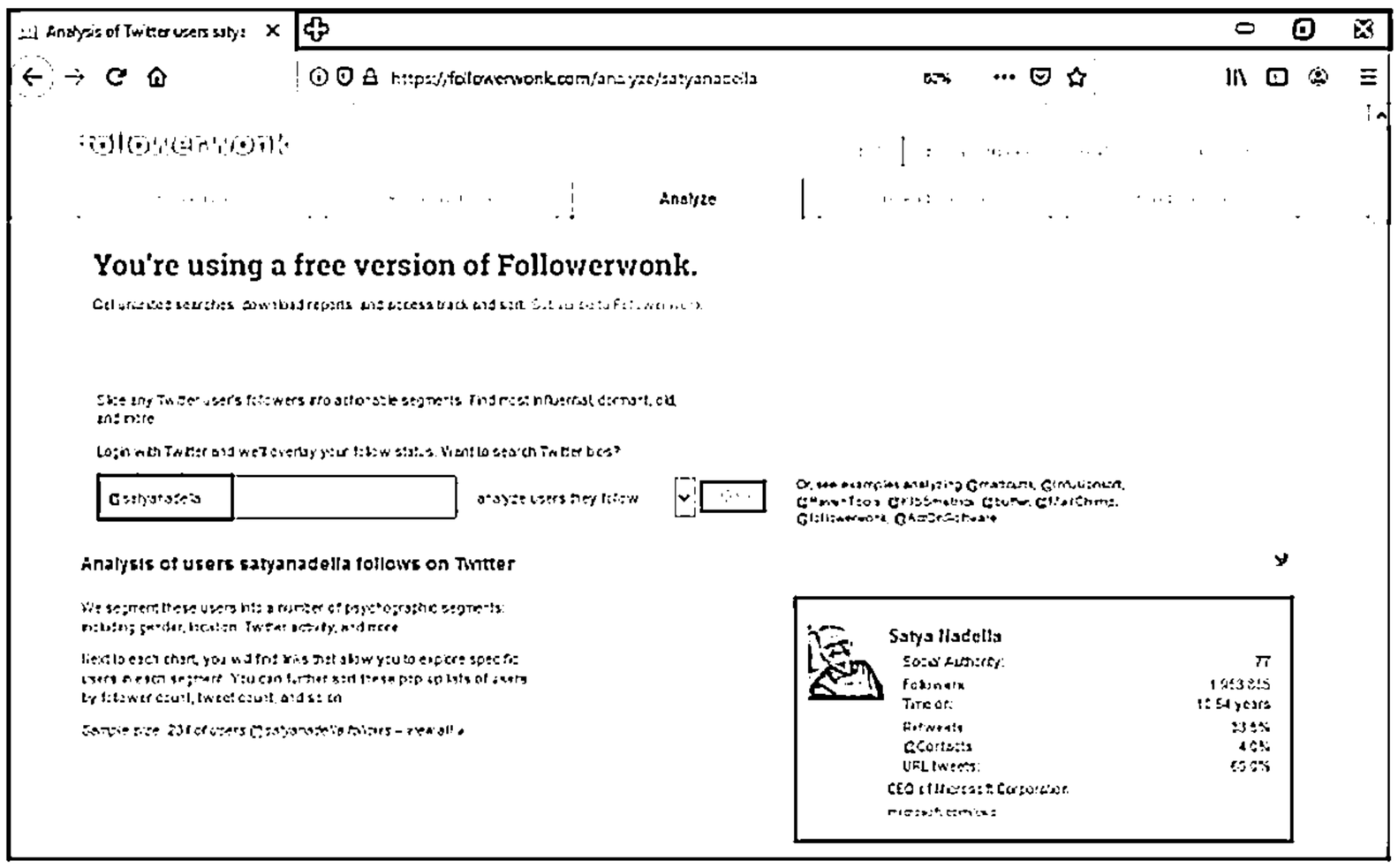


Figure 3.3.1: Followerwonk search result

4. Scroll down to view the detailed analysis, as shown in the screenshot.

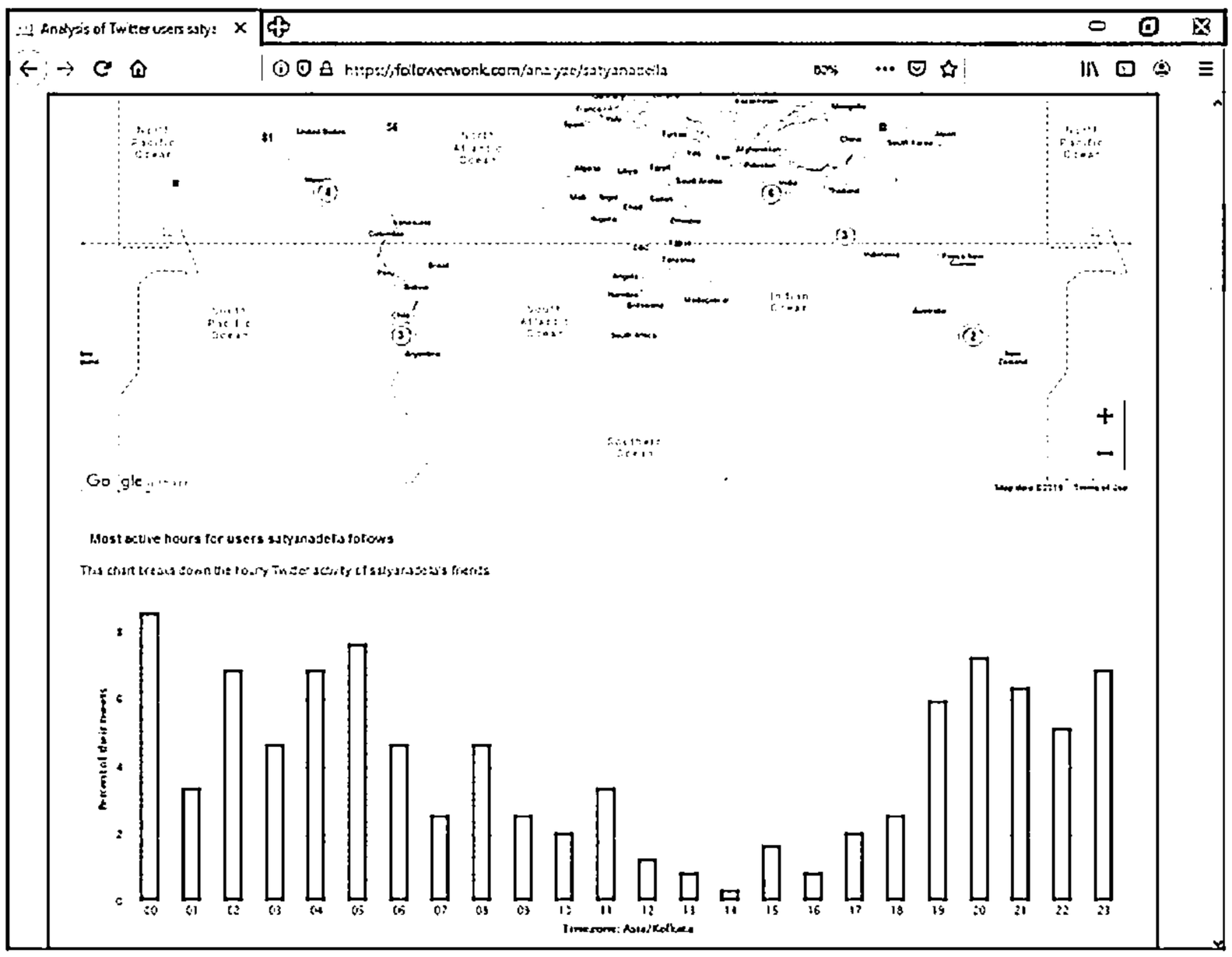


Figure 3.3.2: Followerwonk detailed search result

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

5. This concludes the demonstration of gathering information using Followerwonk.
6. Close all open windows and document all the acquired information.
7. Turn off the **Windows 10** virtual machine.

🗁 You can also use **Hootsuite** (https://hootsuite.com), **Sysomos** (https://www.sysomos.com), etc. to gather additional information related to the target company and its employees from social networking sites

Lab Analysis

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

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT 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

Perform Website Footprinting

Website footprinting refers to monitoring and analyzing the target organization's website for information.

Lab Scenario

ICON KEY

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

As a professional ethical hacker, you should be able to extract a variety of information about the target organization from its website; by performing website footprinting, you can extract important information related to the target organization's website such as the software used and the version, operating system details, filenames, paths, database field names, contact details, CMS details, the technology used to build the website, scripting platform, etc. Using this information, you can further plan to launch advanced attacks on the target organization.

Lab Objectives

- Gather information about a target website using ping command line utility
- Gather information about a target website using Website Informer
- Extract a company's data using Web Data Extractor
- Mirror the target website using HTTrack Web Site Copier
- Gather a wordlist from the target website using CeWL

Lab Environment

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance

To carry out this lab, you need:

- Windows 10 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- Web Data Extractor located at **E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance\Web Spiders\Web Data Extractor**

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

- HTTrack Web Site Copier located at **E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance\Website Mirroring Tools\HTTrack Web Site Copier**
- You can also download the latest versions of **Web Data Extractor** and **HTTrack Web Site Copier** from their official websites. If you decide to download the latest versions, the screenshots shown in the lab might differ.

Lab Duration

Time: 35 Minutes

Overview of Website Footprinting

Website footprinting is a technique used to collect information regarding the target organization's website. Website footprinting can provide sensitive information associated with the website such as registered names and addresses of the domain owner, domain names, host of the sites, OS details, IP details, registrar details, emails, filenames, etc.

Lab Tasks

TASK 1 — Gather Information About a Target Website using Ping Command Line Utility

1. Turn on the **Windows 10** virtual machine.
2. Login to the **Windows 10** virtual machine with Username: **Admin** and Password: **Pa$$w0rd**.

TASK 1.1

Finding the IP Address of a Target Domain

3. Open the **Command Prompt** window. Type **ping www.certifiedhacker.com** and press **Enter** to find its IP address. The displayed response should be similar to the one shown in the screenshot.

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

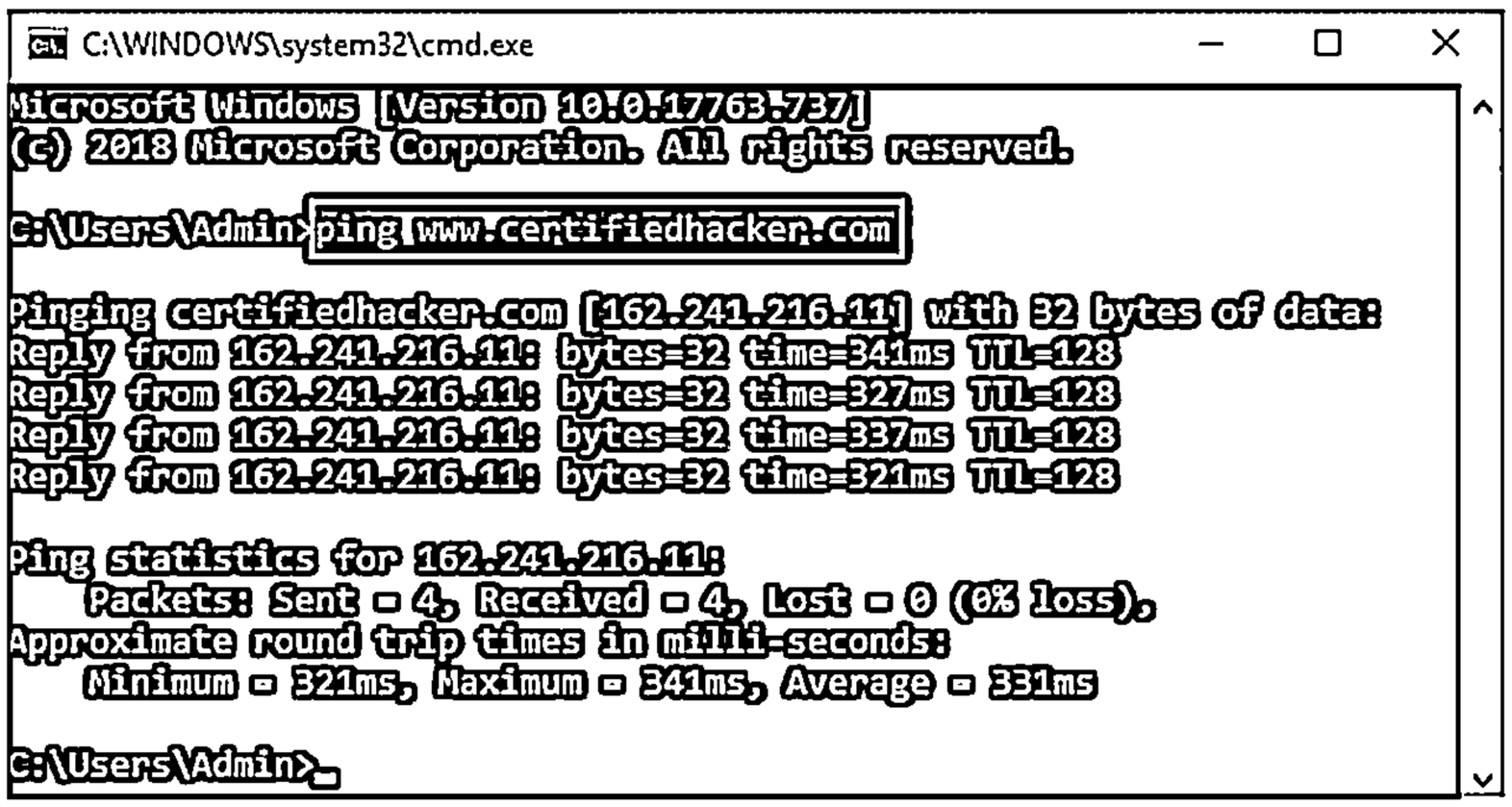


Figure 4.1.1: The ping command to extract the IP address for www.certifiedhacker.com

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

4. Note the target domain's IP address in the result above (here, **162.241.216.11**). You also obtain information on Ping Statistics such as packets sent, packets received, packets lost, and approximate round-trip time.

Note: The IP address of the target website may differ in your lab environment.

TASK 1.2

Finding Maximum Frame Size

5. In the **Command Prompt** window, type **ping www.certifiedhacker.com -f -l 1500** and press **Enter**.

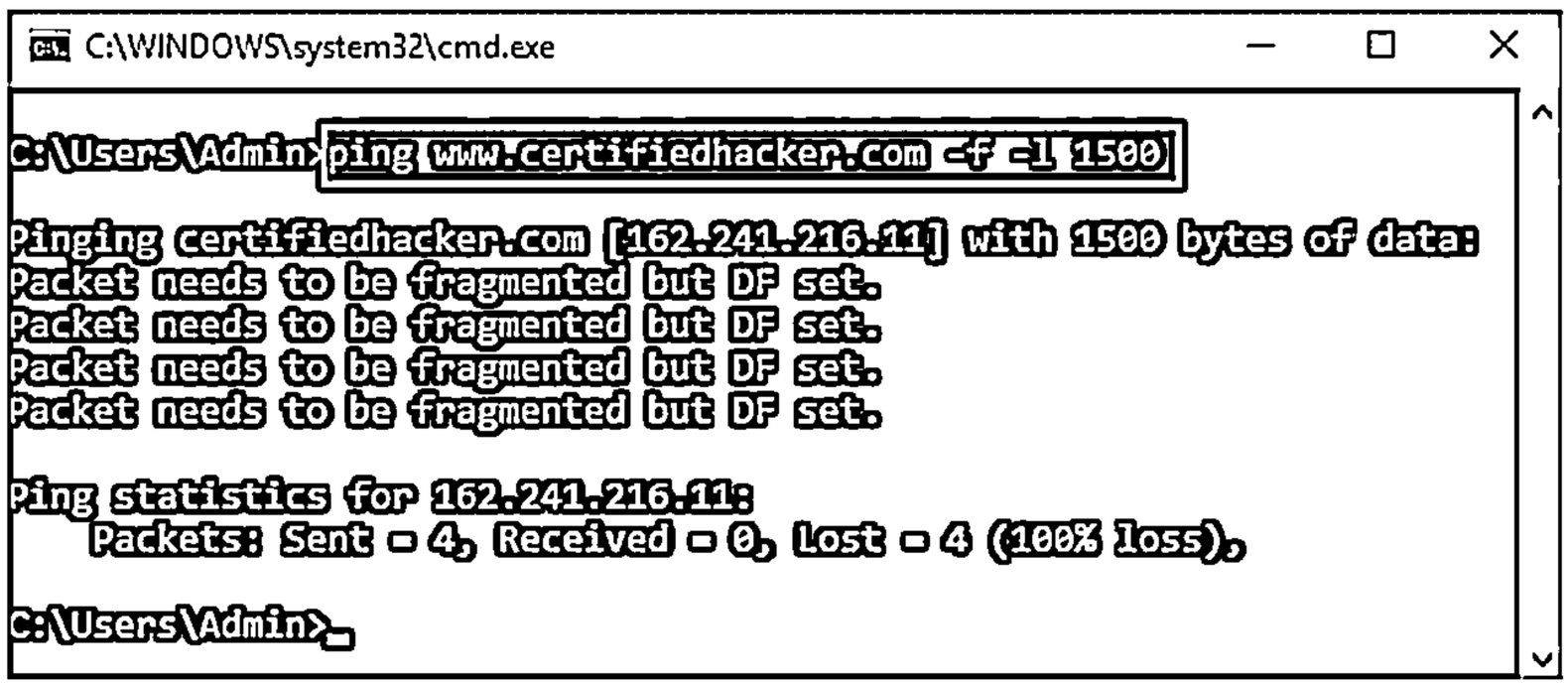


Figure 4.1.2: The ping command for www.certifiedhacker.com with -f -l 1500 options

The ping command sends an ICMP echo request 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 round-trip time, and records any loss of packets. The ping command assists in obtaining domain information and the IP address of the target website.

6. The response, **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. The packet was not sent as we used the **-f** switch with the ping command, and the ping command returned this error.

7. In the **Command Prompt** window, type **ping www.certifiedhacker.com -f -l 1300** and press **Enter**.

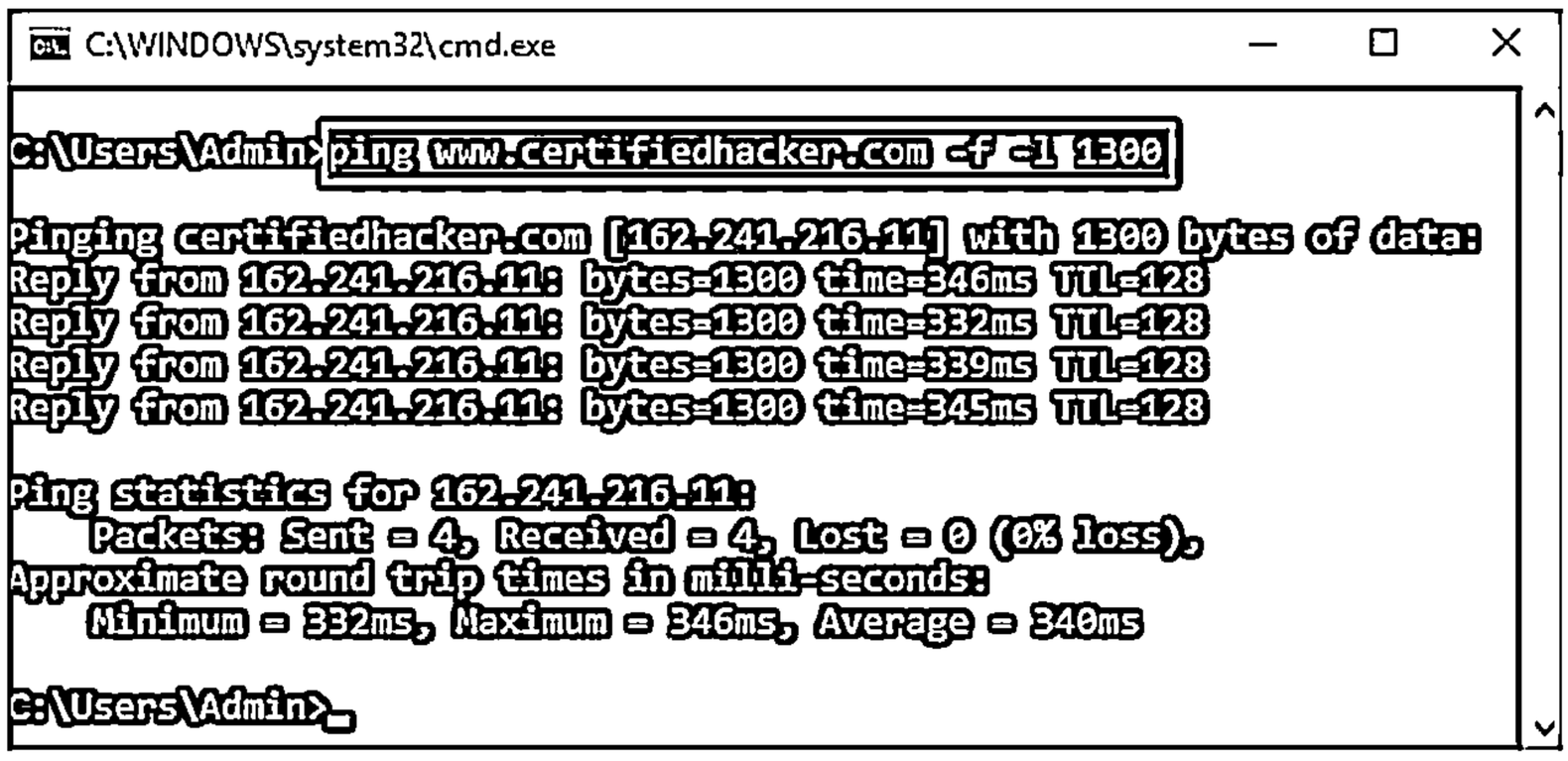


Figure 4.1.3: The ping command for www.certifiedhacker.com with -f -l 1300 options

8. Observe that the maximum packet size is less than **1500** bytes and more than **1300** bytes.

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

9. 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 are the maximum frame size on this machine's network.

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

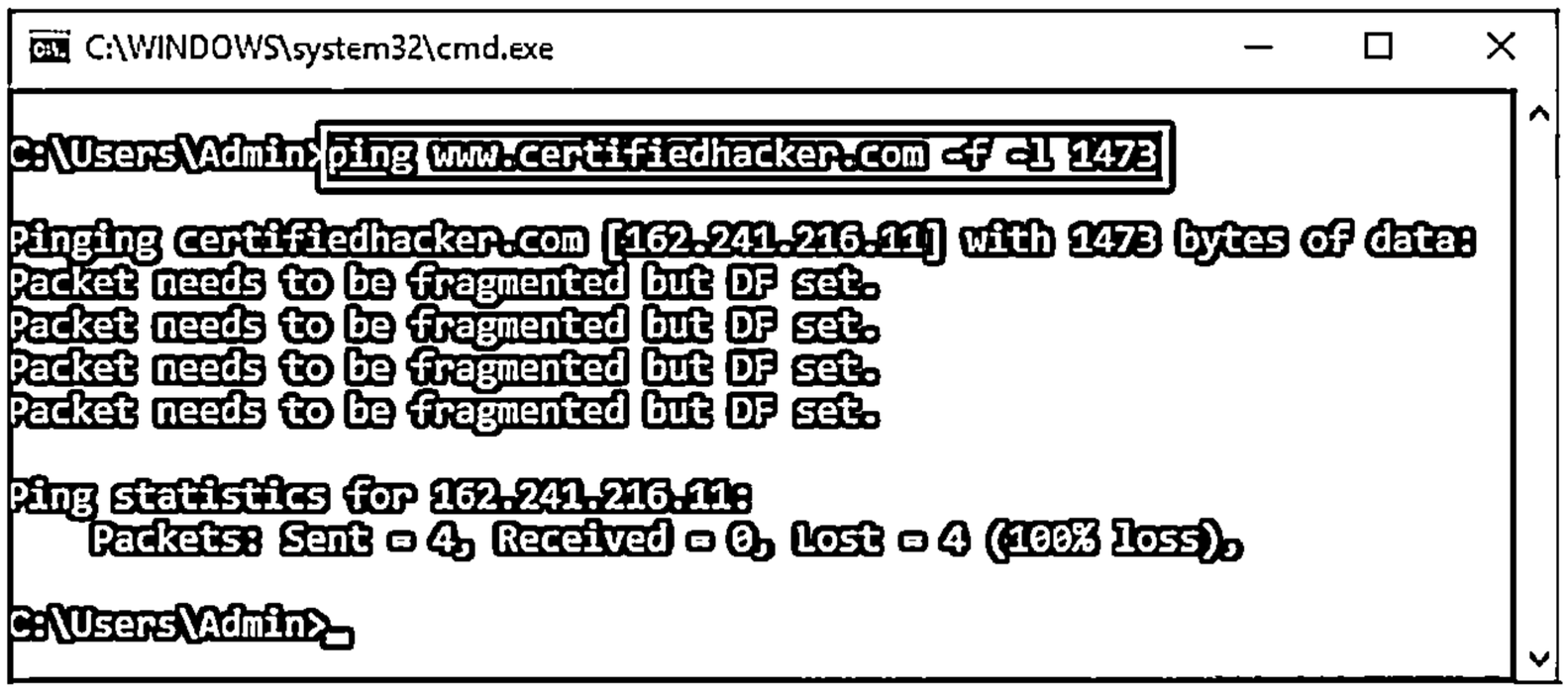


Figure 4.1.4: The ping command for www.certifiedhacker.com with -f -l 1473 options

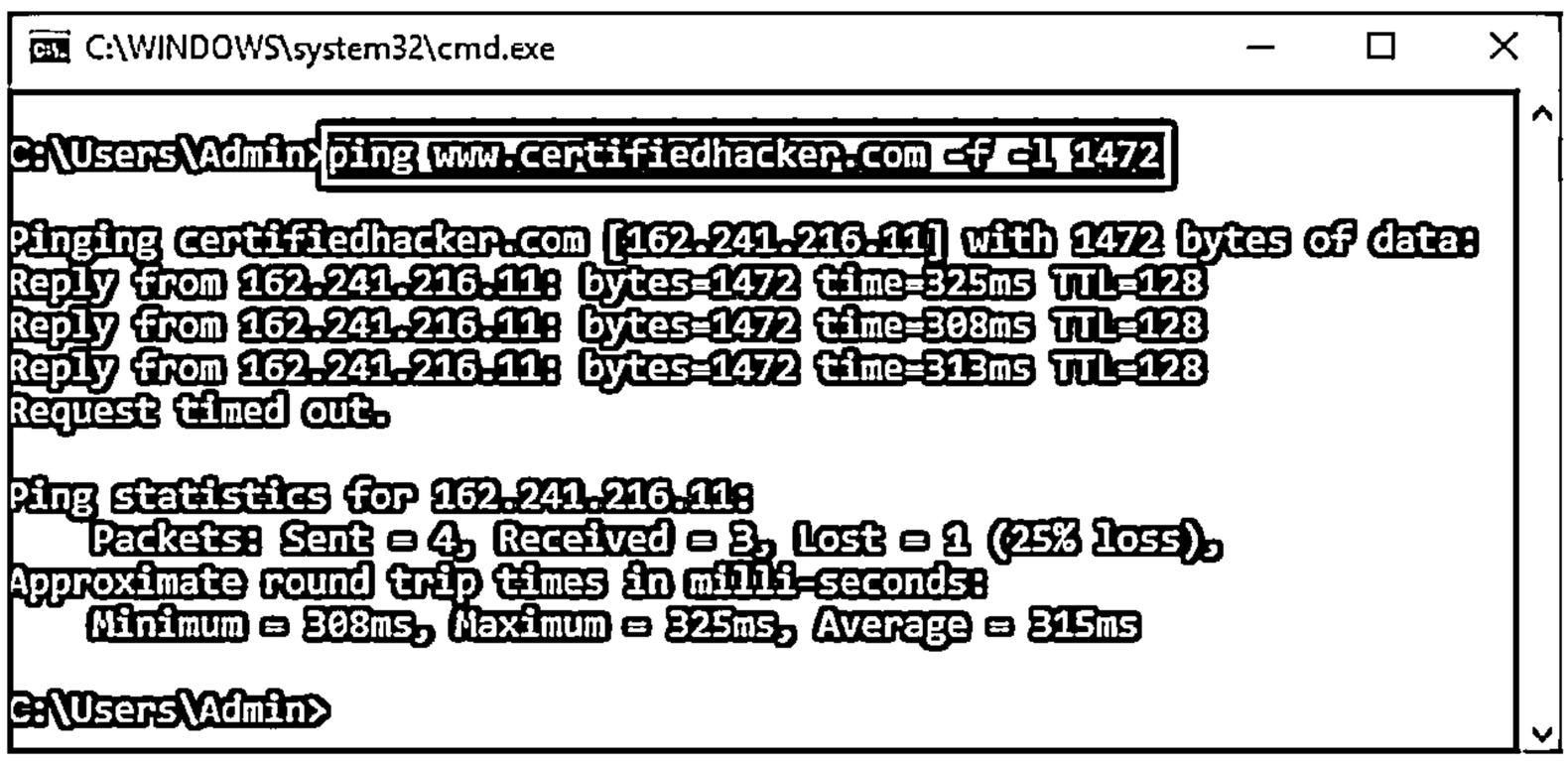


Figure 4.1.5: The ping command for www.certifiedhacker.com with -f -l 1472 options

10. Now, discover 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.

TASK 1.3

Finding Hop Count using TTL Value

11. In **Command Prompt**, type **ping www.certifiedhacker.com -i 3** and press **Enter**. This option sets the time to live (**-i**) value as **3**.

Note: The maximum value you can set for TTL is 255.

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

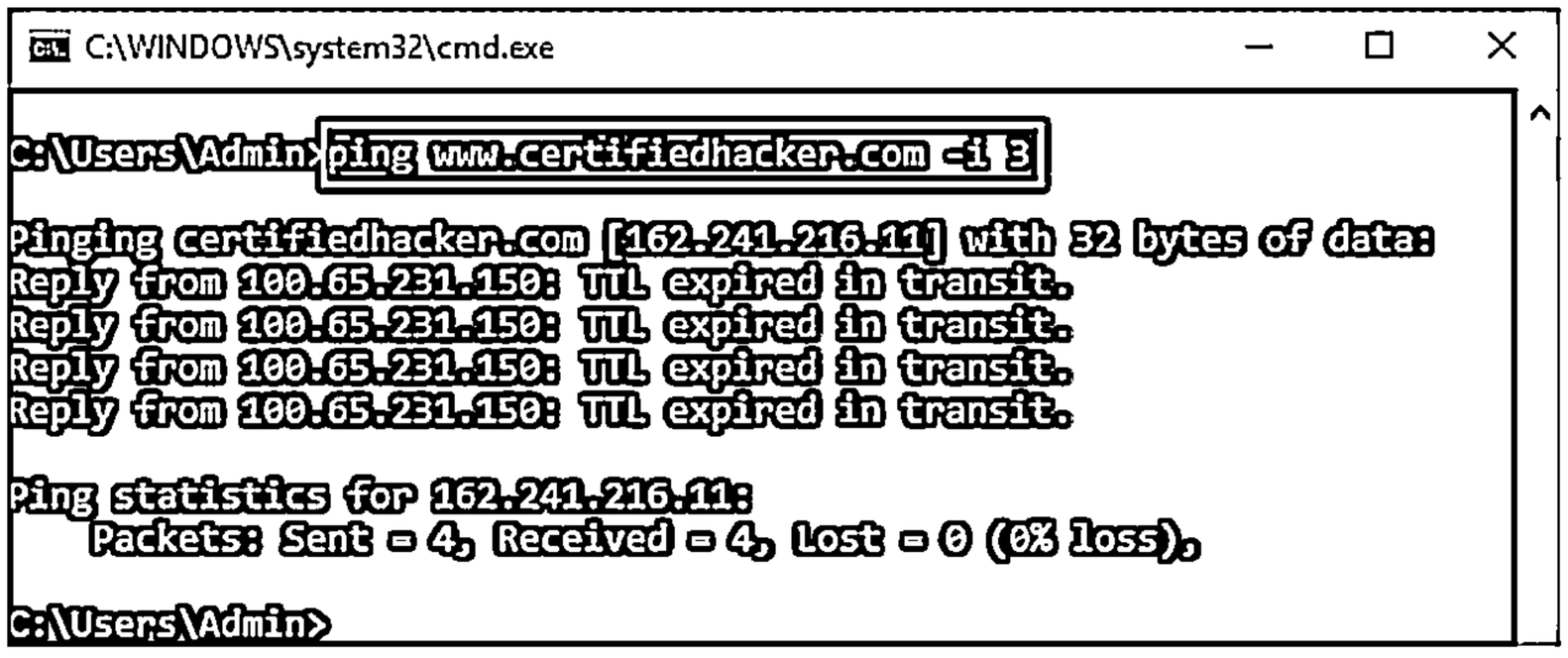


Figure 4.1.6: The ping command for www.certifiedhacker.com with –i 3 options

12. **Reply from 100.65.231.150: TTL expired in transit** means that the router (100.65.231.150, students will have some other IP address) discarded the frame because its TTL has expired (reached 0).

Note: The IP address 100.65.231.150 may vary in your lab environment.

Note: If you get the **Request timed out** reply for the above query, then use **Command Prompt of your host machine** instead of the Windows 10 virtual machine to run the query.

13. Minimize the command prompt shown above and launch a new **command prompt**. Type **ping www.certifiedhacker.com -i 2 -n 1** and press **Enter**. Here, we set the TTL value to **2** and the **-n** value to 1 to check the life span of the packet.

Note: **-n** specifies the number of echo requests to be sent to the target.

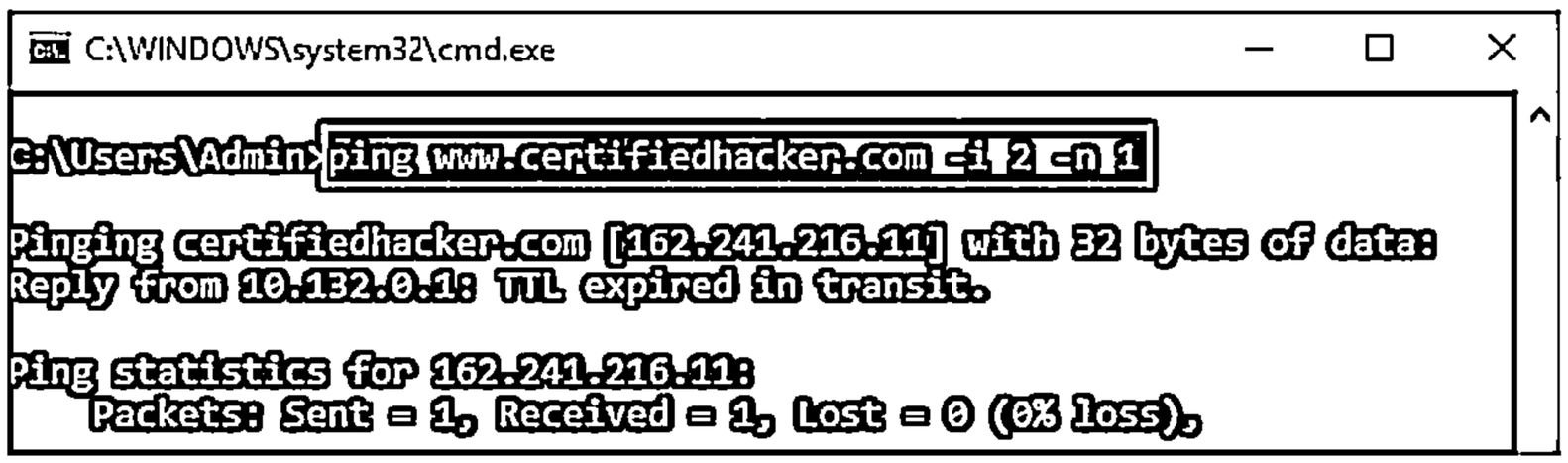


Figure 4.1.7: The ping command for www.certifiedhacker.com with –i 2 –n 1 options

14. Type **ping www.certifiedhacker.com -i 3 -n 1**. This sets the TTL value to **3**.

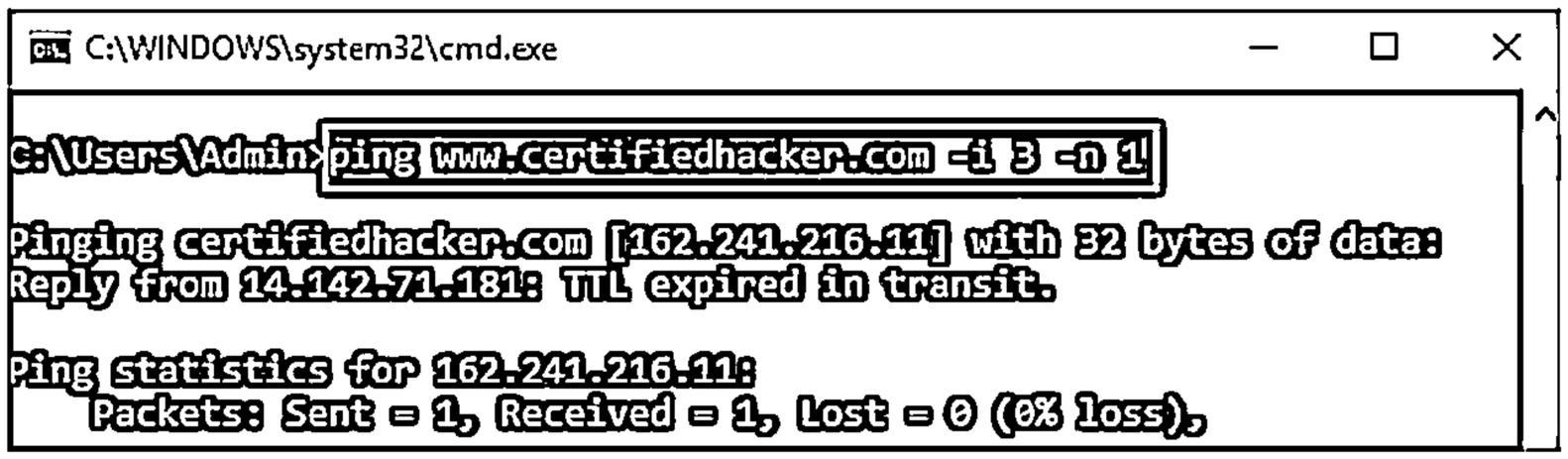


Figure 4.1.8: The ping command for www.certifiedhacker.com with –i 3 –n 1 options

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

15. Observe that there is a reply coming from the IP address **162.241.216.11**, and there is no packet loss.

Note: The result displayed in the above step might differ in your lab environment.

16. Now, change the time to live value to **4** by typing,
ping www.certifiedhacker.com -i 4 -n 1 and press **Enter**.

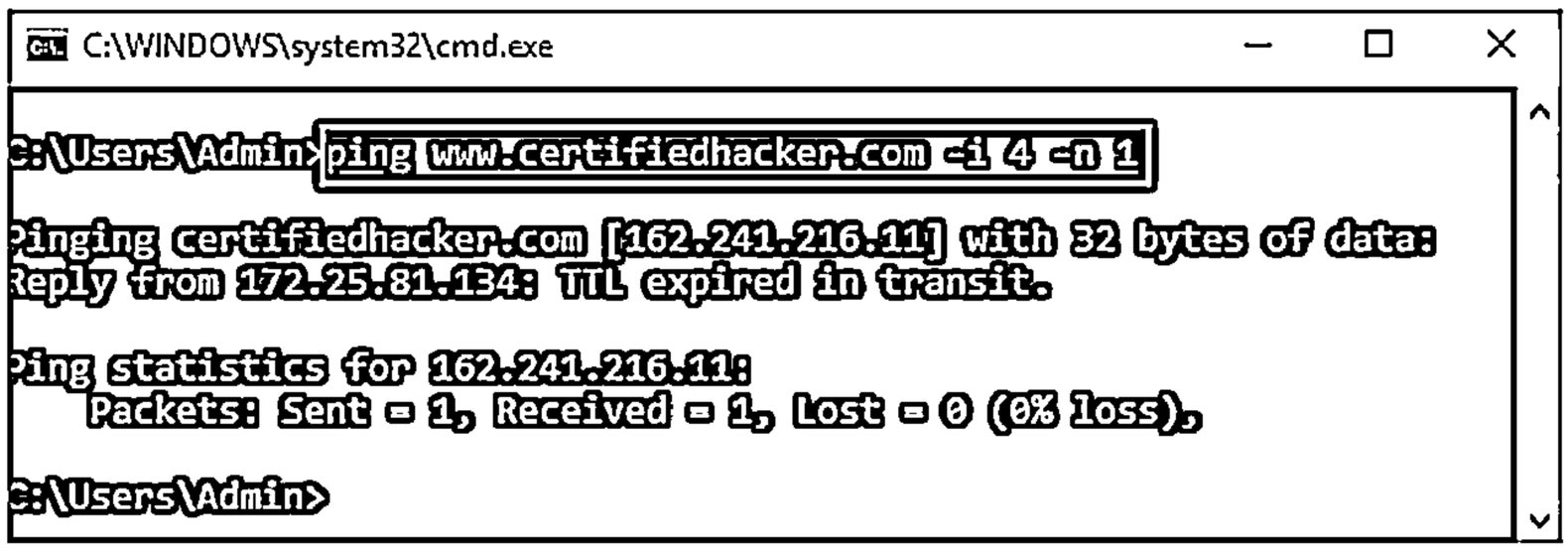


Figure 4.1.9: The ping command for www.certifiedhacker.com with –i 4 –n 1 options

17. Repeat the above step until you reach the IP address for **www.certifiedhacker.com** (in this case, **162.241.216.11**).

18. Here, the successful ping to reach **www.certifiedhacker.com** is **27** hops.

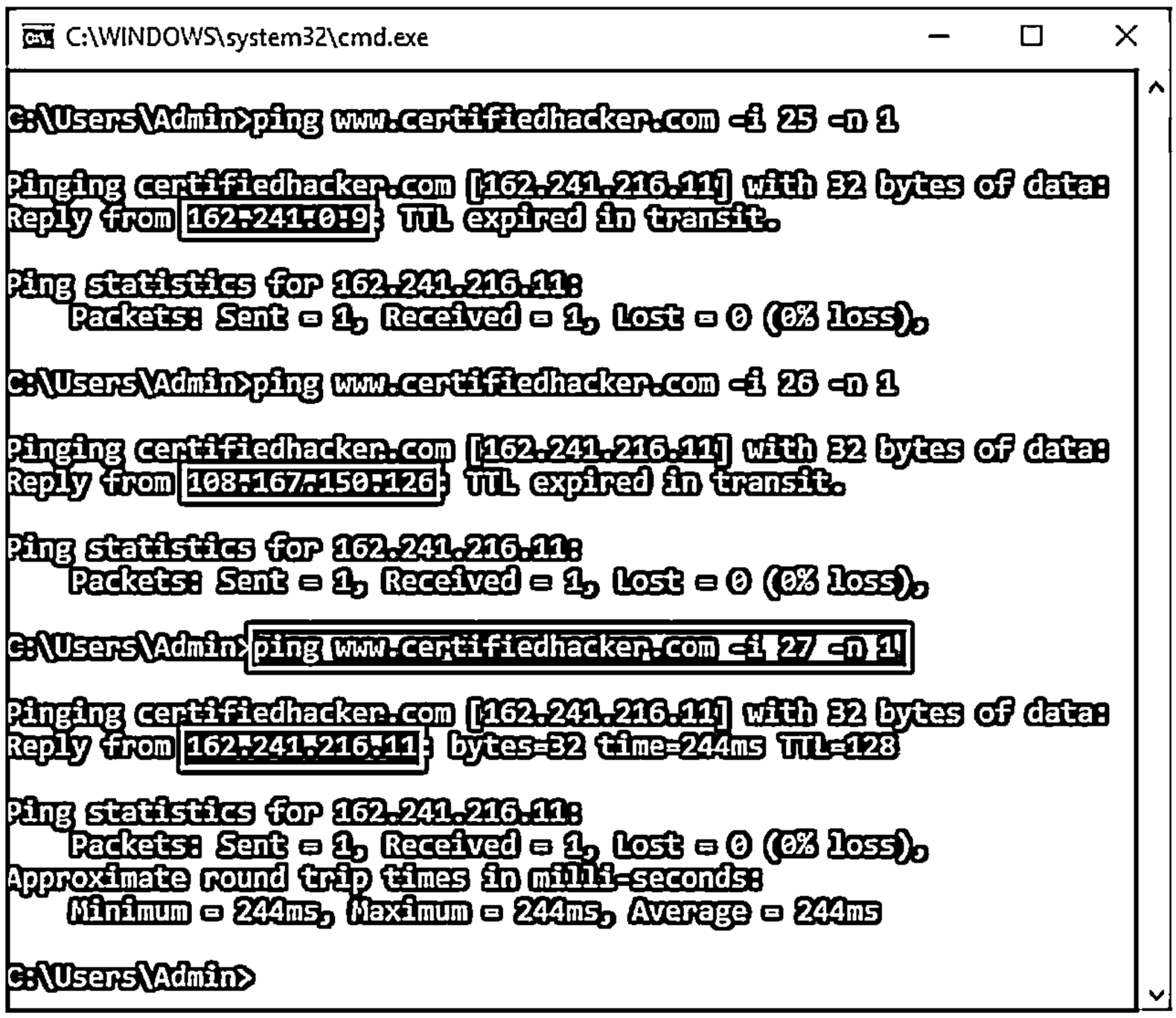


Figure 4.1.10: The ping command for www.certifiedhacker.com with –i 27 –n 1

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

19. This implies that, at a time to live value of **27**, the reply is received from the destination host (**162.241.216.11**).

Note: The result might vary in your lab environment.

20. This concludes the demonstration of gathering information about a target website using Ping command-line utility (such as the IP address of the target website, hop count to the target, and value of maximum frame size allowed on the target network).
21. Close all open windows and document all the acquired information.

TASK 2 Gather Information about a Target Website using Website Informer

Website Informer is an online tool that gathers detailed information on a website such as a website's traffic rank, daily visitors rate, page views, etc. Website Informer discovers the main competitors of the website, reveals DNS servers used by the website, and also obtains the Whois record of the target website.

1. In the **Windows 10** virtual machine, open a web browser (here, **Mozilla Firefox**), type **https://website.informer.com** in the address bar, and press **Enter**. The Website Informer website appears, as shown in the screenshot.

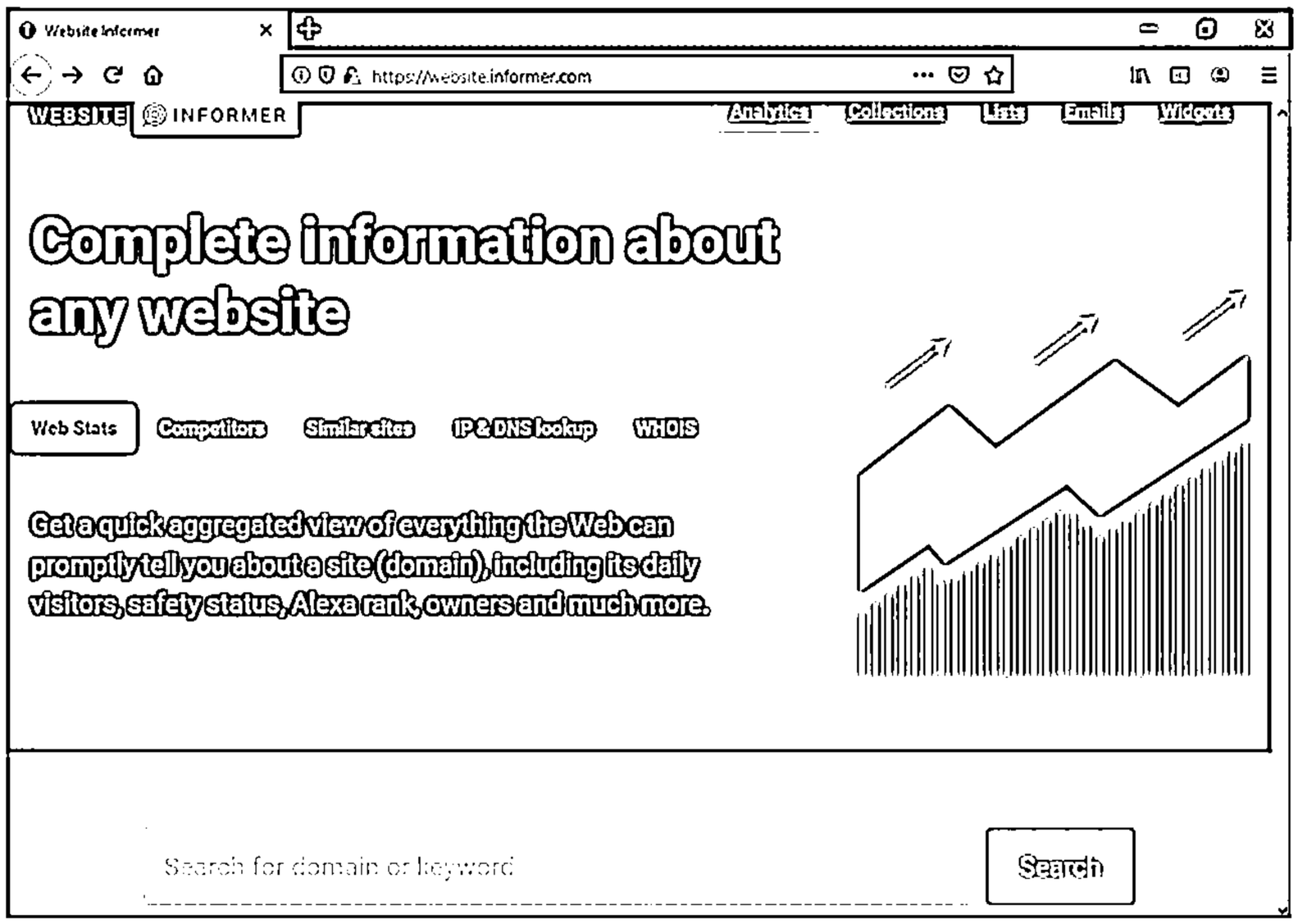


Figure 4.2.1: Website Informer website

2. To extract information associated with the target organization website, type the target website's URL (here, **www.certifiedhacker.com**) in the text field, and then click on the **Search** button, as shown in the screenshot below.

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

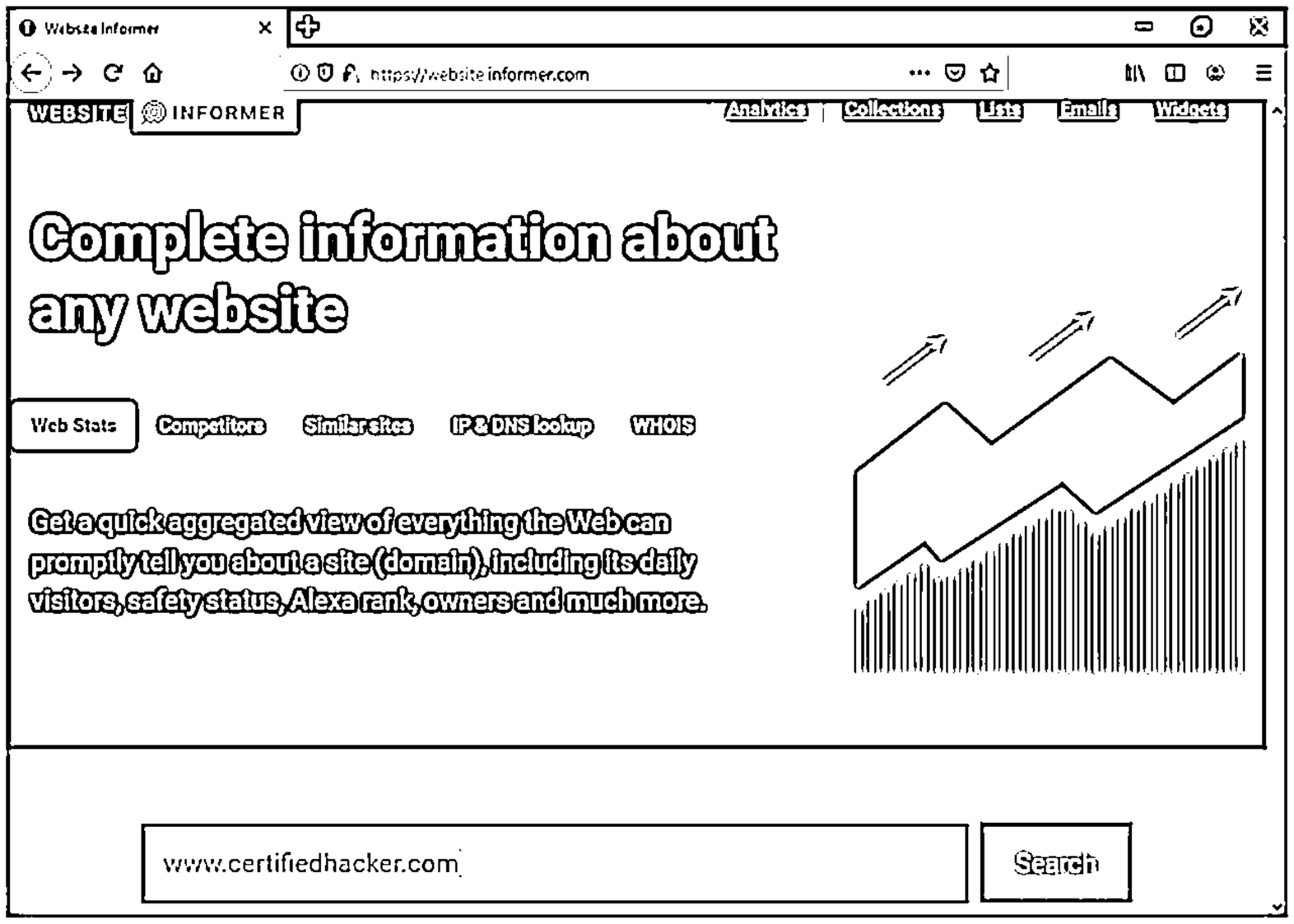


Figure 4.2.2: Enter the target website

3. A search result for **WWW.CERTIFIEDHACKER.COM** containing information such as **General Info**, **Stats & Details**, **Whois**, and **IP Whois** is displayed, as shown in the screenshot.

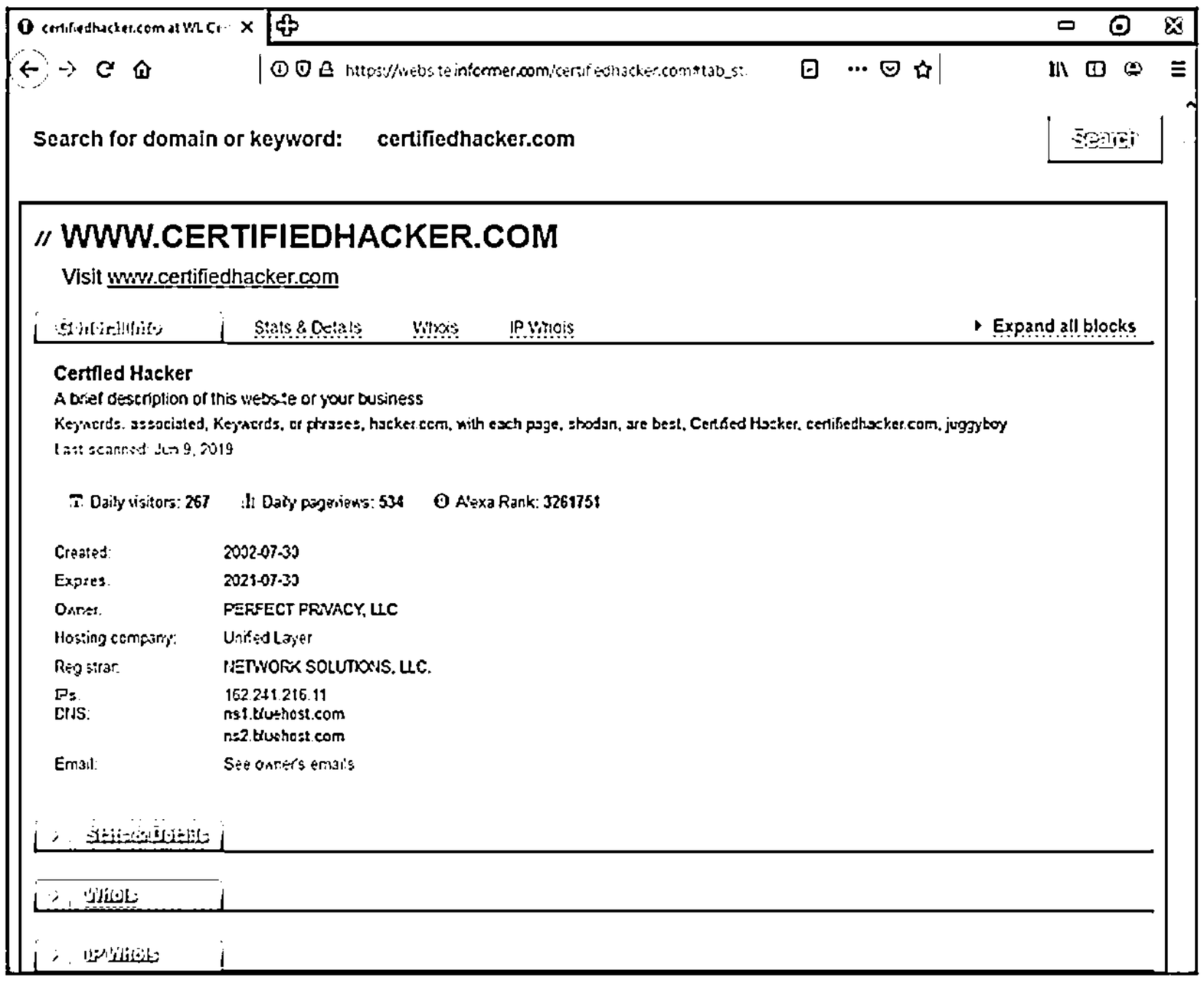


Figure 4.2.3: Search result generated by Website Informer

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

4. In the **General Info** tab, information such as **Created, Expires, Owner, Hosting company, Registrar, IPs, DNS**, and **Email** associated with the target website is displayed as shown in the screenshot.

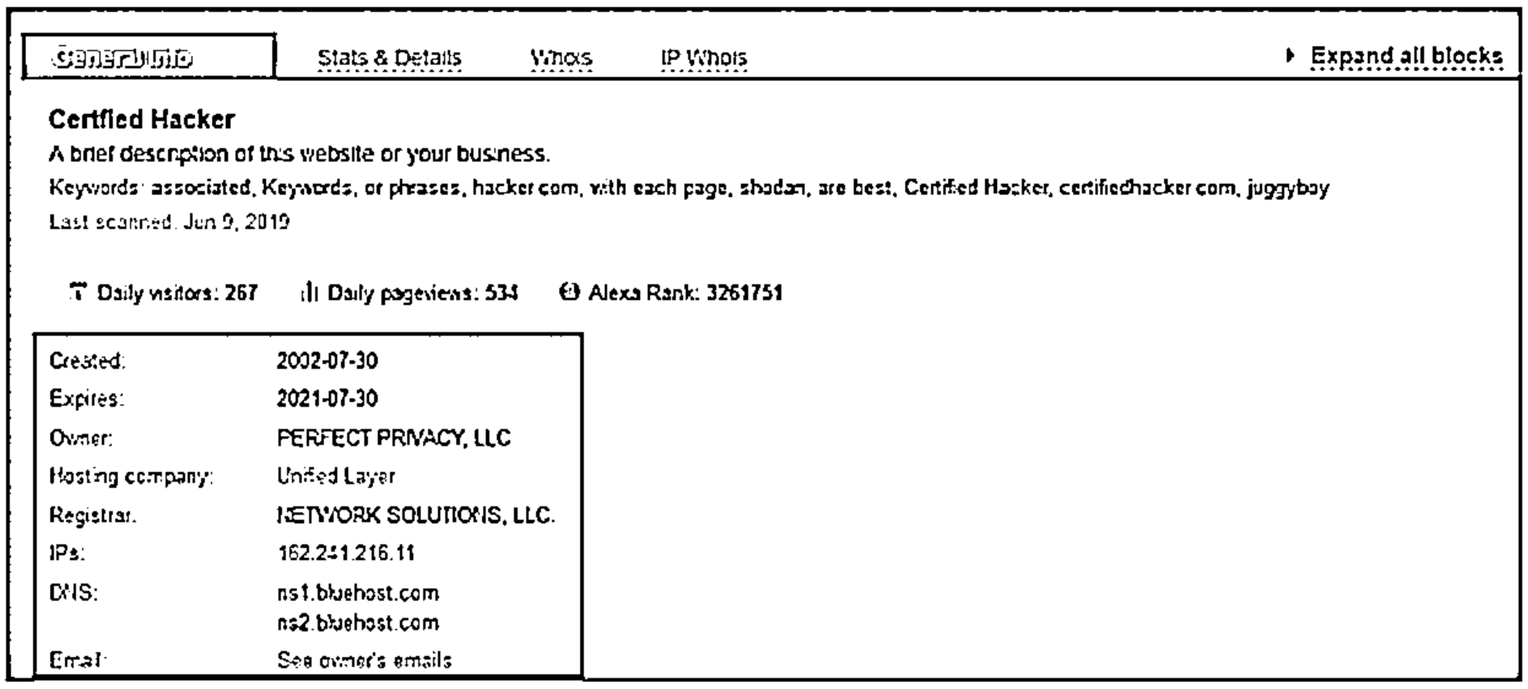


Figure 4.2.4: Website Informer General Info

5. Click on the **Whois** tab to view detailed Whois information about the target website, as shown in the screenshot.

Figure 4.2.5: Website Informer Whois information

You can also use tools such as **Burp Suite** (https://portswigger.net), **Zaproxy** (https://www.owasp.org), etc. to perform website footprinting on a target website.

6. Similarly, you can click on the **Stats & Details** and **IP Whois** tabs to view the detailed information of the target website.
7. This concludes the demonstration of gathering information about a target website using the Website Informer online tool.
8. Close all open windows and document all the acquired information.

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

TASK 3 Extract a Company's Data using Web Data Extractor

Here, we will gather the target company's data using the Web Data Extractor tool.

TASK 3.1

Install Web Data Extractor

1. In the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance\Web Spiders\Web Data Extractor** and double-click **wde.exe**.
2. If the **User Account Control** pop-up appears, click **Yes**.

Note: If the **Open File - Security Warning** pop-up appears, click **Run**.

3. Follow the wizard steps to install Web Data Extractor and click **Finish**.

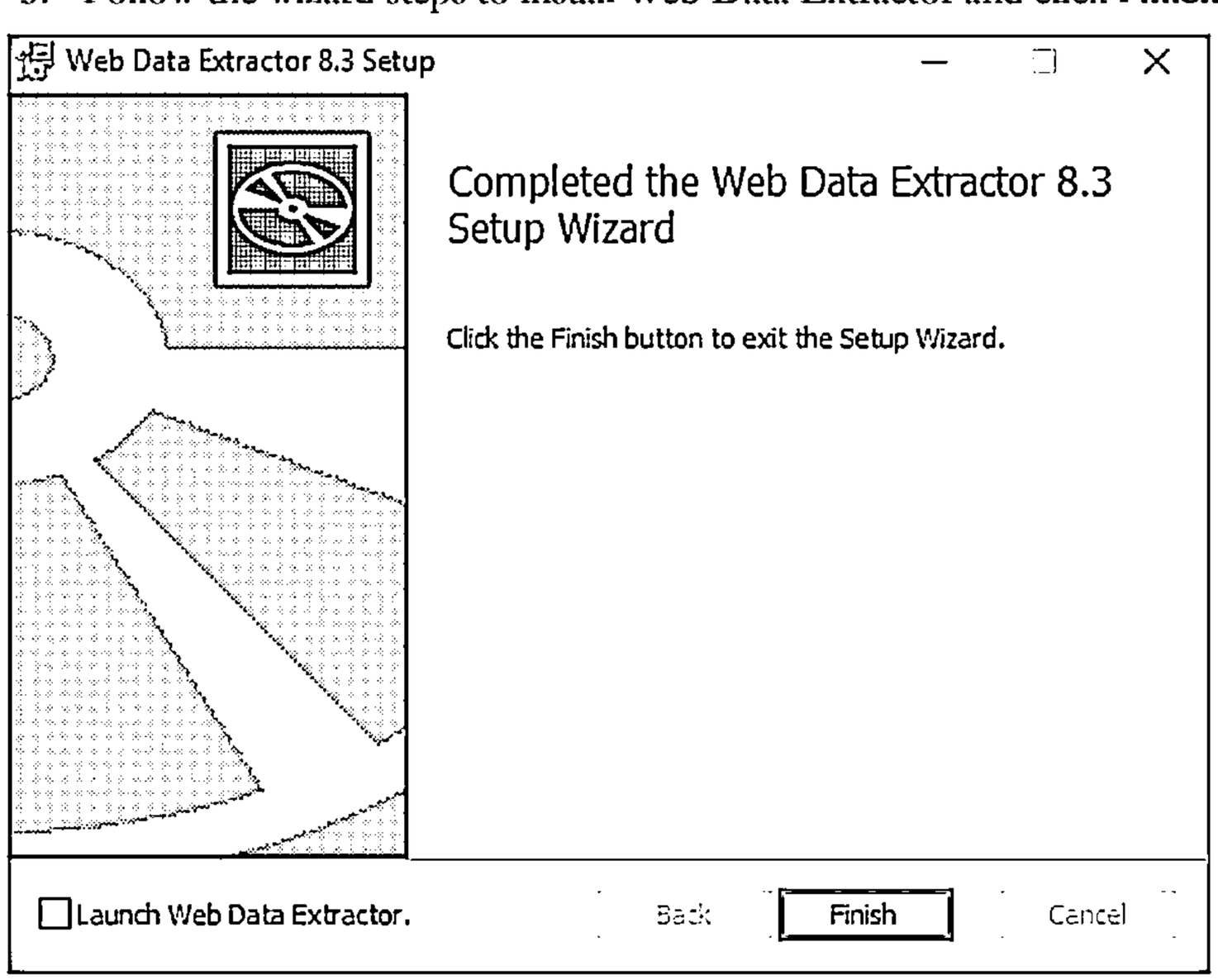


Figure 4.3.1: Web Data Extractor Setup Pop-up Wizard

Web data extraction is the process of extracting data from web pages available on the company's website. A company's data such as contact details (email, phone, and fax), URLs, meta tags (title, description, keyword) for website promotion, directories, web research, etc. are important sources of information for an ethical hacker.

Web spiders (also known as a web crawler or web robot) such as Web Data Extractor perform automated searches on the target website and extract specified information from the target website.

4. After installation, launch **Web Data Extractor** from **Desktop**.

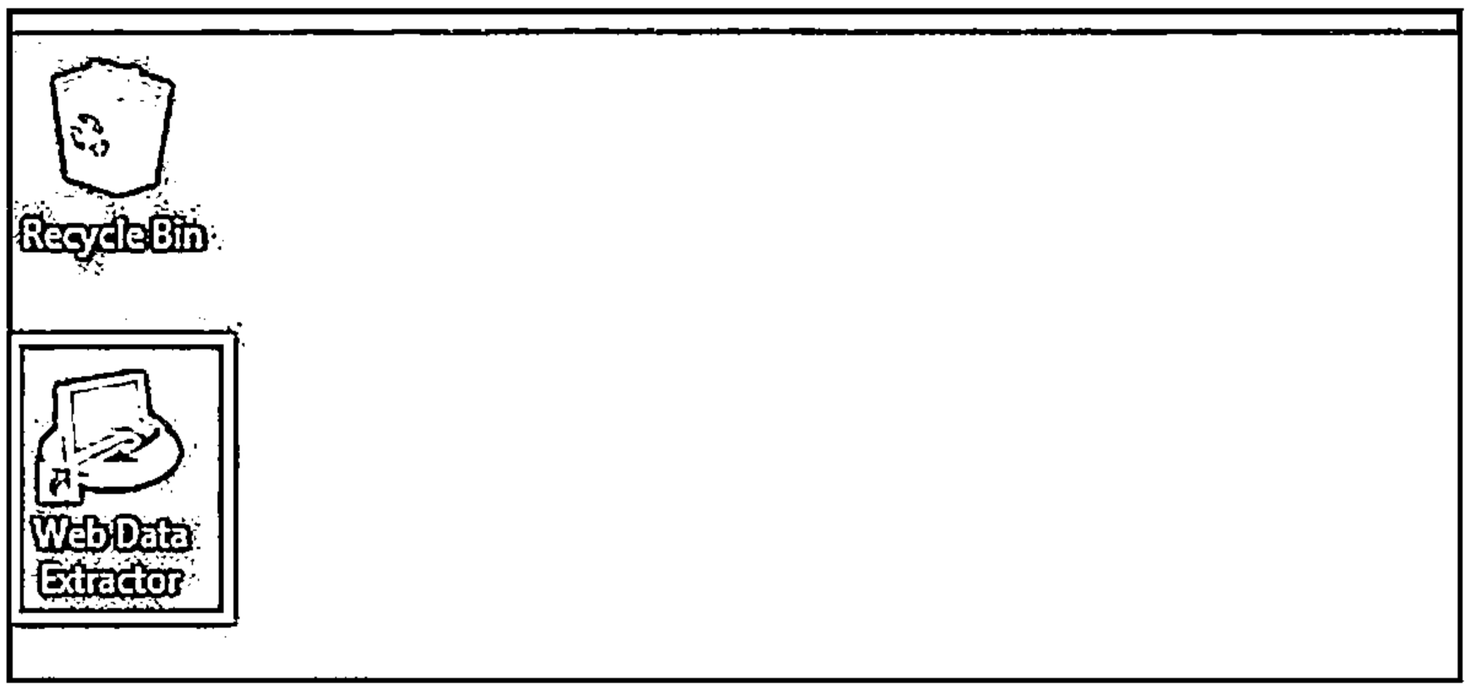


Figure 4.3.2: Installed apps in Windows 10 - Selecting Web Data Extractor

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

TASK 3.2

Configure Web Data Extractor

5. The **Web Data Extractor** main window appears. Click **New** to start a new session.

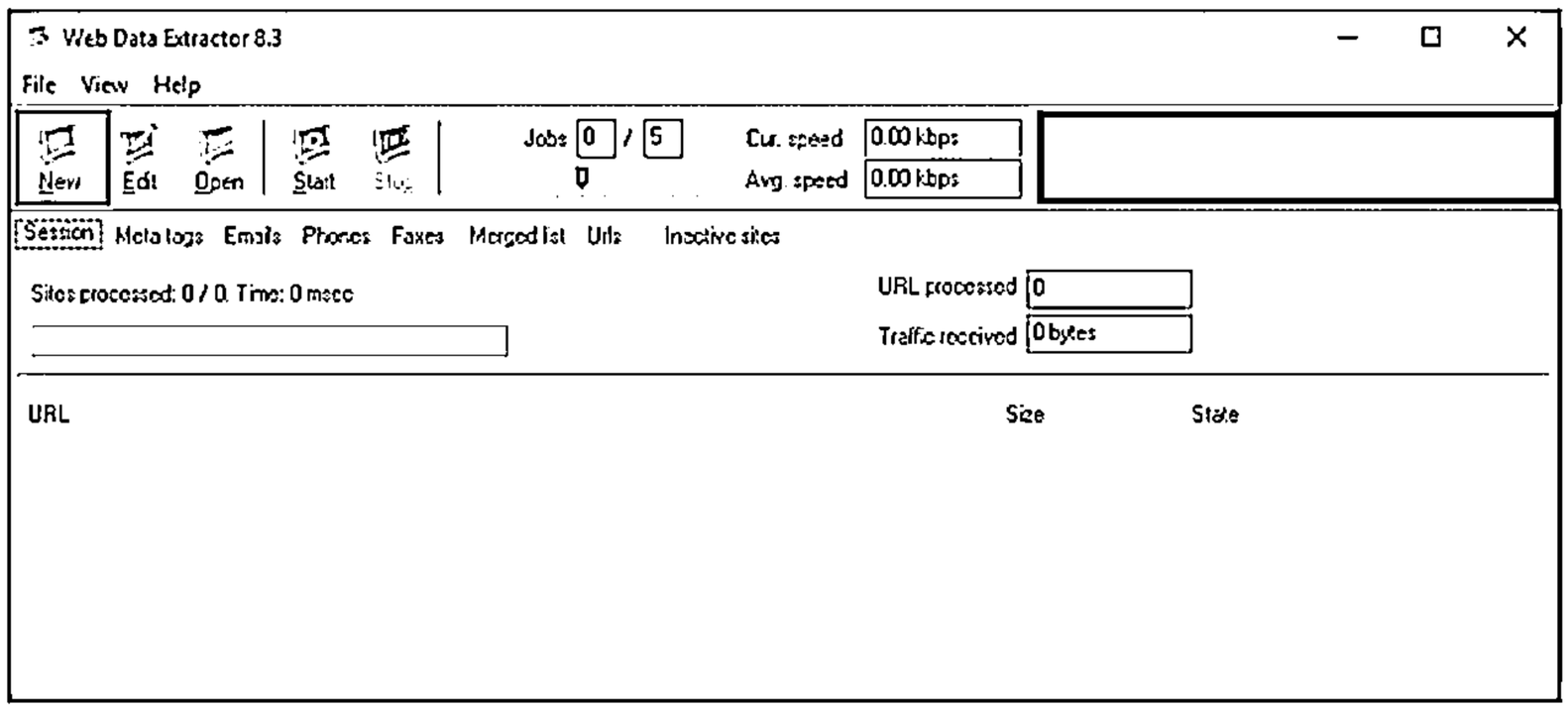


Figure 4.3.3: The Web Data Extractor main window

6. The **Session settings** window appears; type a URL (here, **http://www.certifiedhacker.com**) in the **Starting URL** field. Check all the options, as shown in the screenshot, and click **OK**.

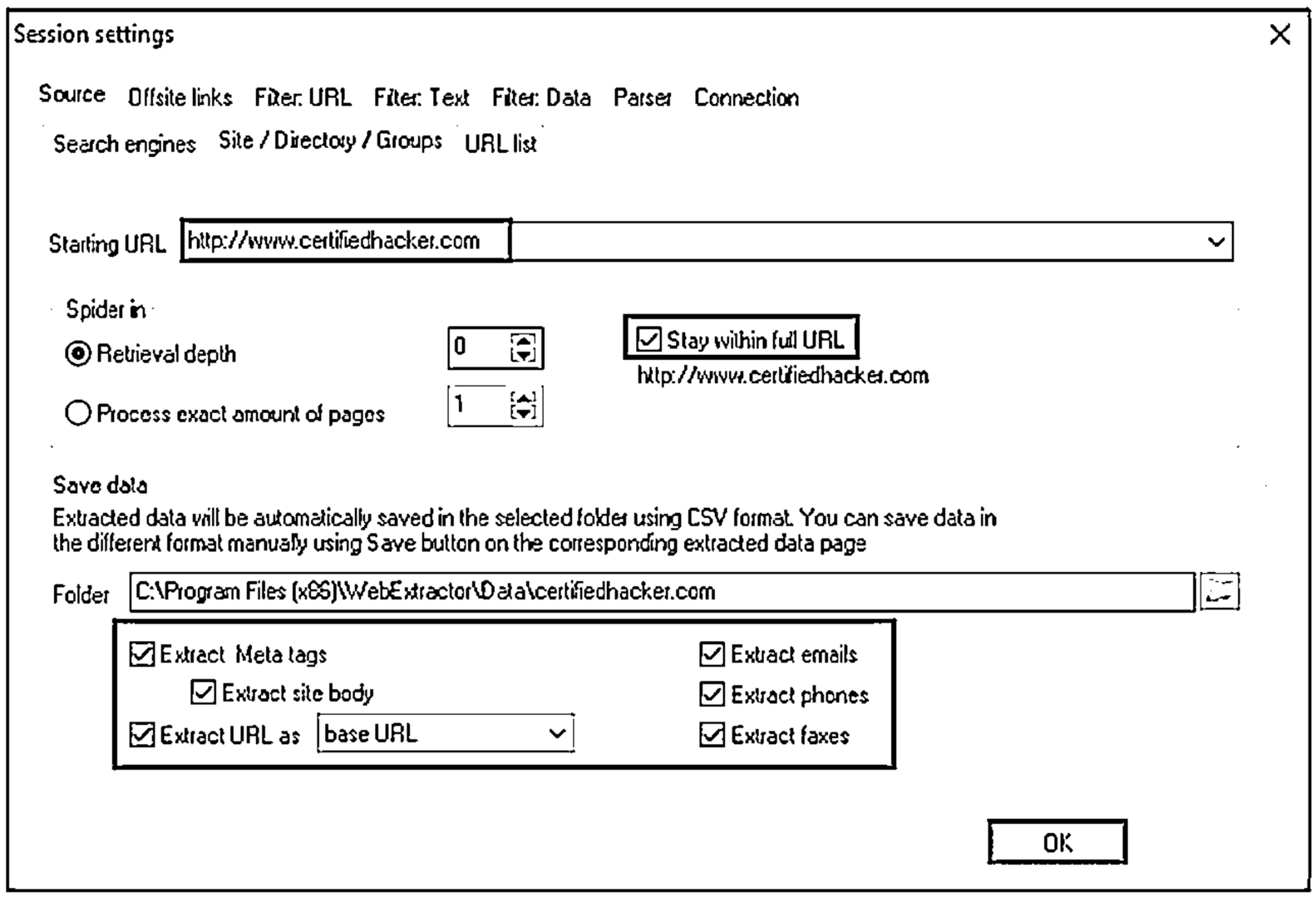


Figure 4.3.4: Web Data Extractor - Session settings window

TASK 3.3

Extract Target Website Data

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

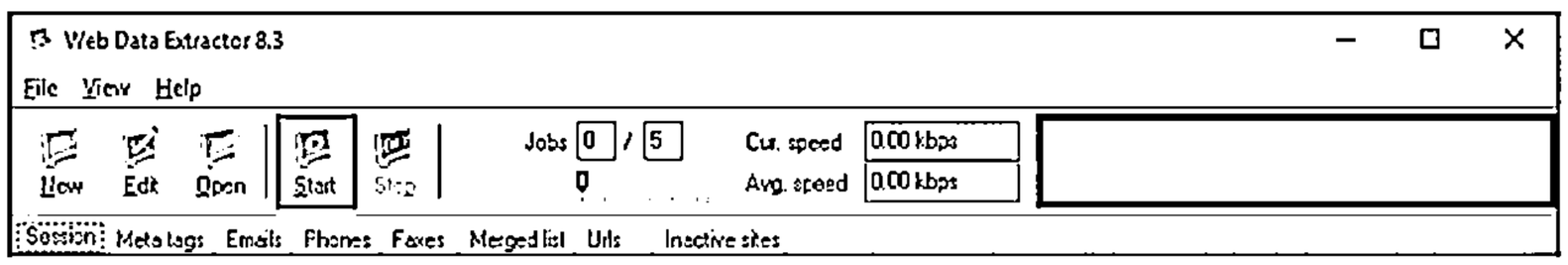


Figure 4.3.5: Web Data Extractor initiating the data extraction

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

8. Web Data Extractor will start collecting information (**Session**, **Meta tags**, **Emails**, **Phones**, **Faxes**, **Merged list**, **URLs**, and **Inactive sites**).

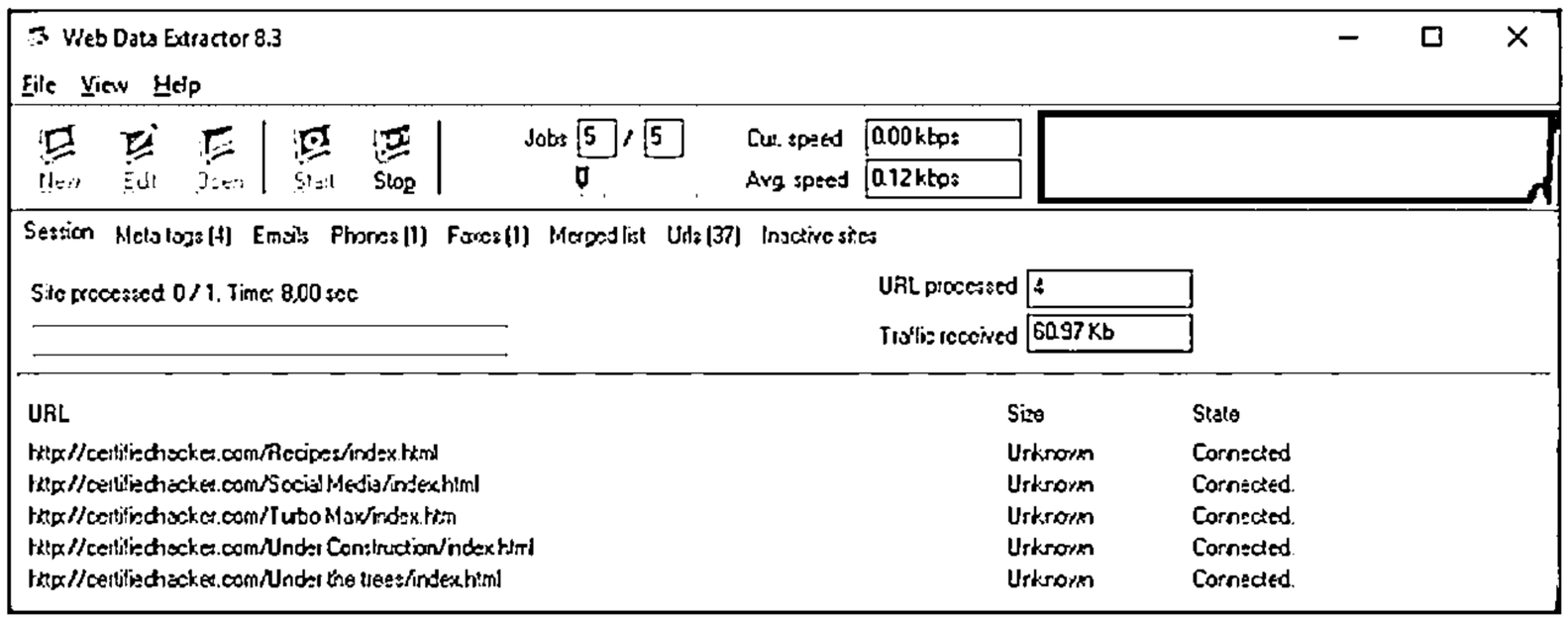


Figure 4.3.6: Web Data Extractor collecting information

9. Once the data extraction process is completed, an **Information** dialog box appears; click **OK**.

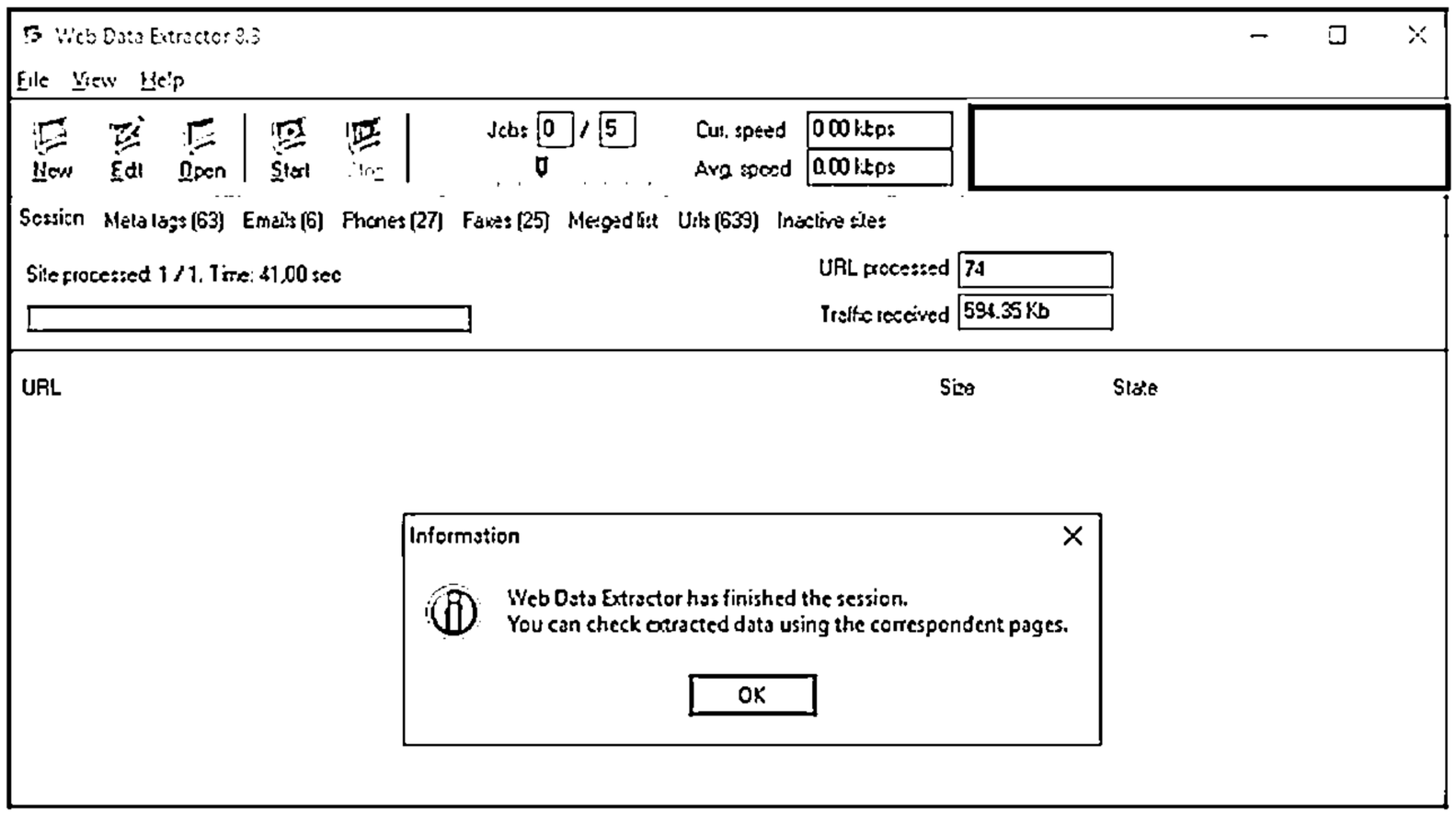


Figure 4.3.7: Web Data Extractor Data Extraction information window

10. View the extracted information by clicking the tabs.

TASK 3.4

Examine the Collected Data

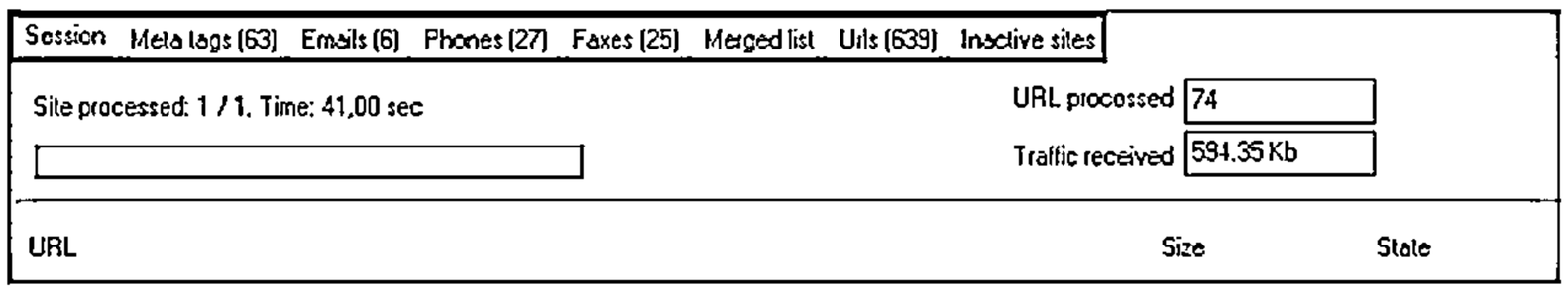


Figure 4.3.8: Web Data Extractor Data Extraction window

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

11. Select the **Meta tags** tab to view the URL, Title, Keywords, Description, Host, Domain, page size, etc.

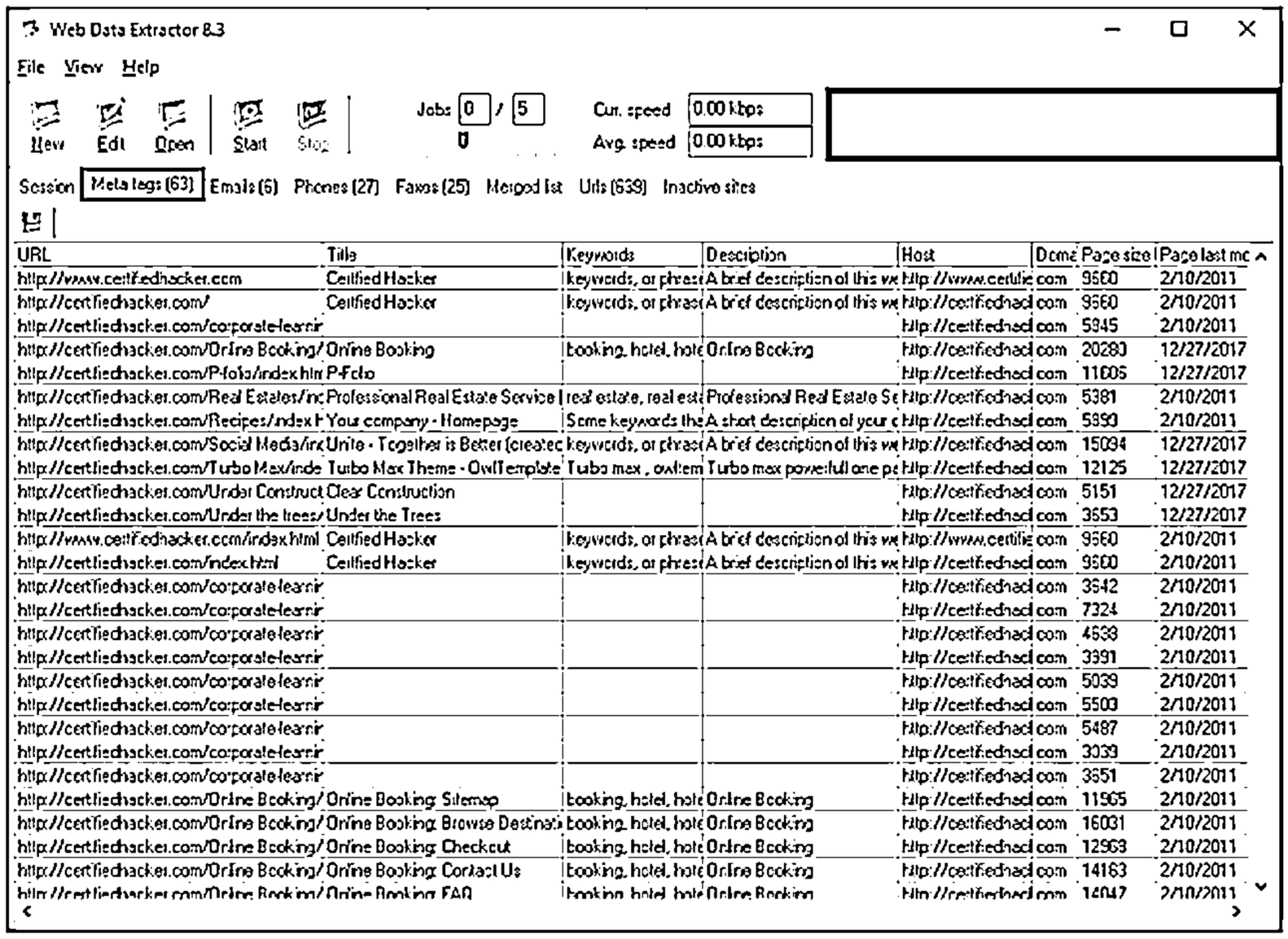


Figure 4.3.9: Web Data Extractor- Meta tags tab

12. Select the **Emails** tab to view information related to emails such as Email address, Name, URL, Title, etc.

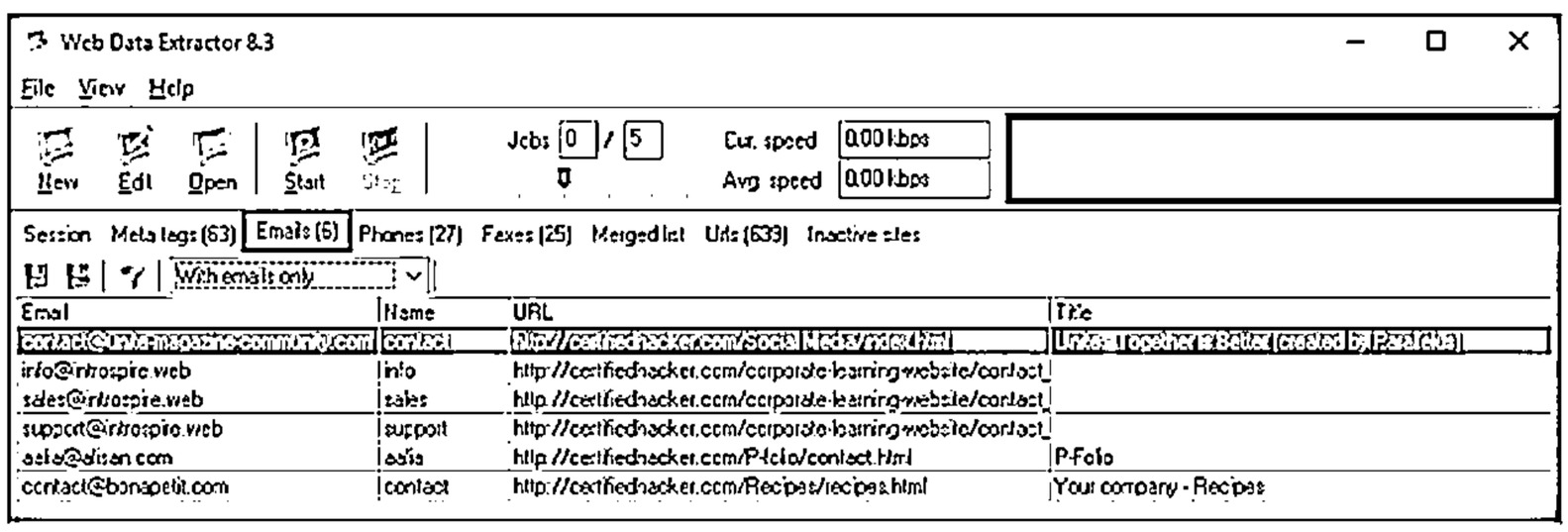


Figure 4.3.10: Web Data Extractor- Emails tab

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

13. Select the **Phones** tab to view the Phone, Source, Tag, URL, etc.

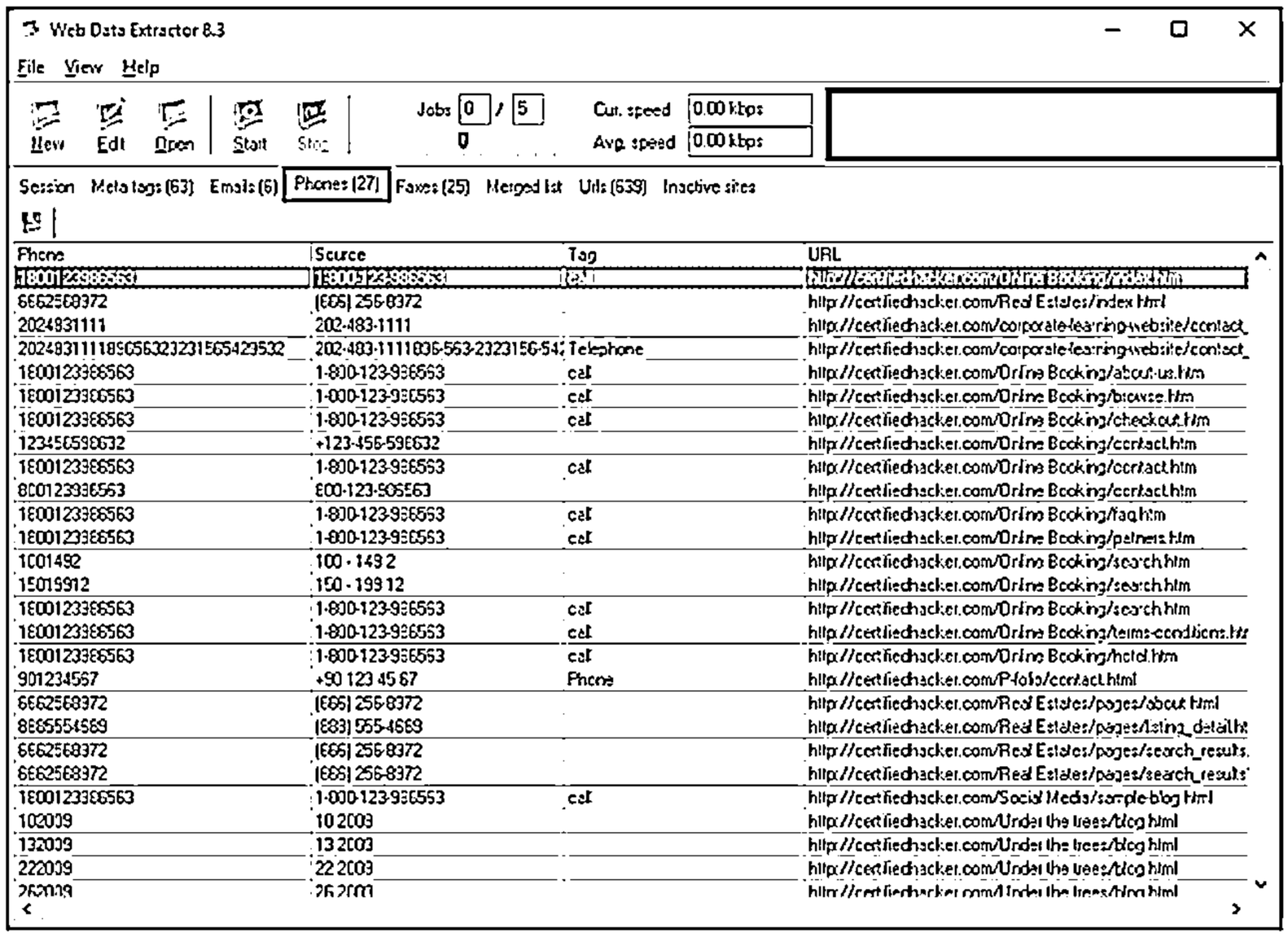


Figure 4.3.11: Web Data Extractor- Phones tab

14. Check for more information under the **Faxes**, **Merged list**, **URLs**, and **Inactive sites** tabs.

TASK 3.5

Save a Session

15. To save the session, choose **File** and click **Save session**.

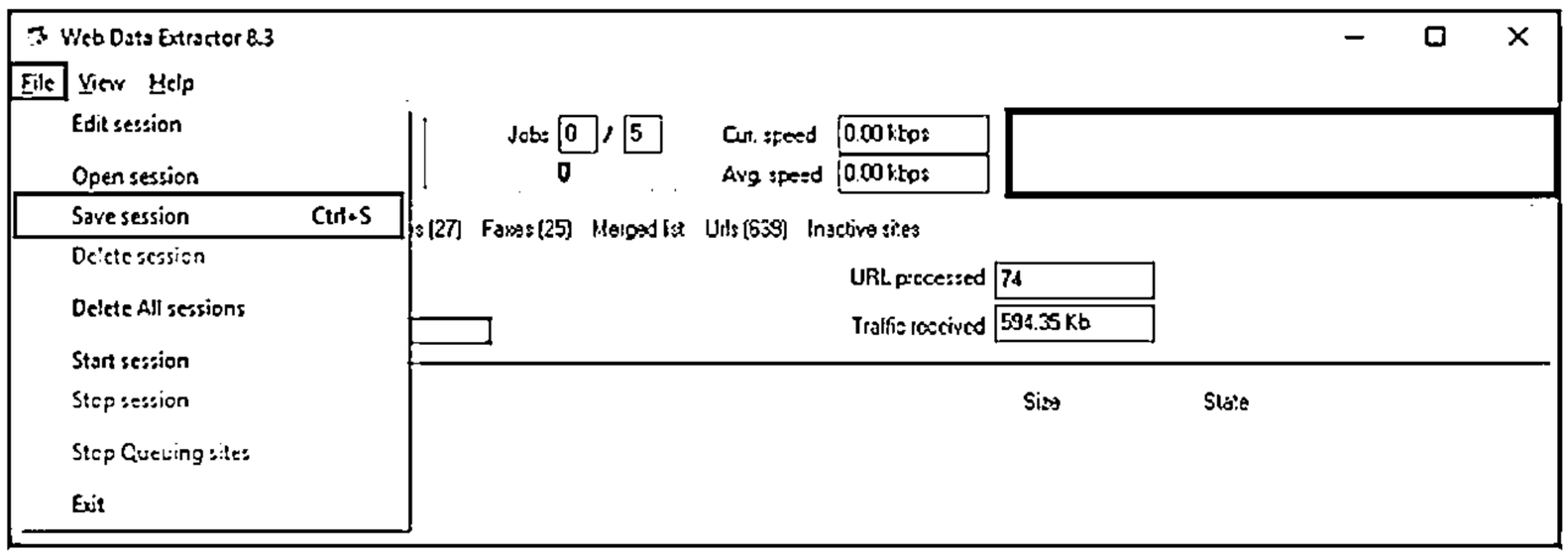


Figure 4.3.12: Web Data Extractor session saving window

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

16. Specify the session name (here, **certifiedhacker.com**) in the **Save session** dialog box and click **OK**.

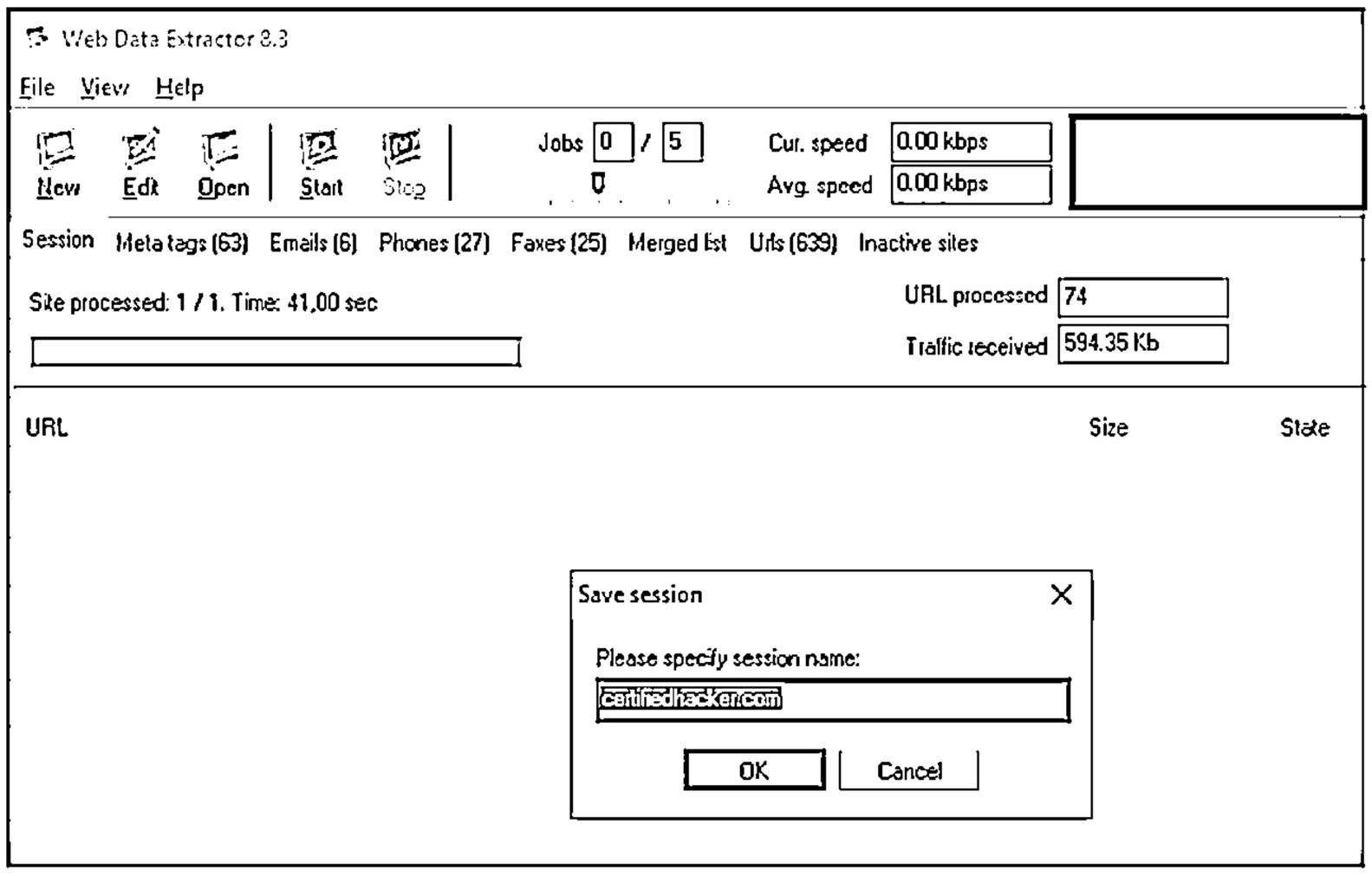


Figure 4.3.13: Web Data Extractor specifying the session name

17. Click the **Meta tags** tab, and then click the **floppy** icon.

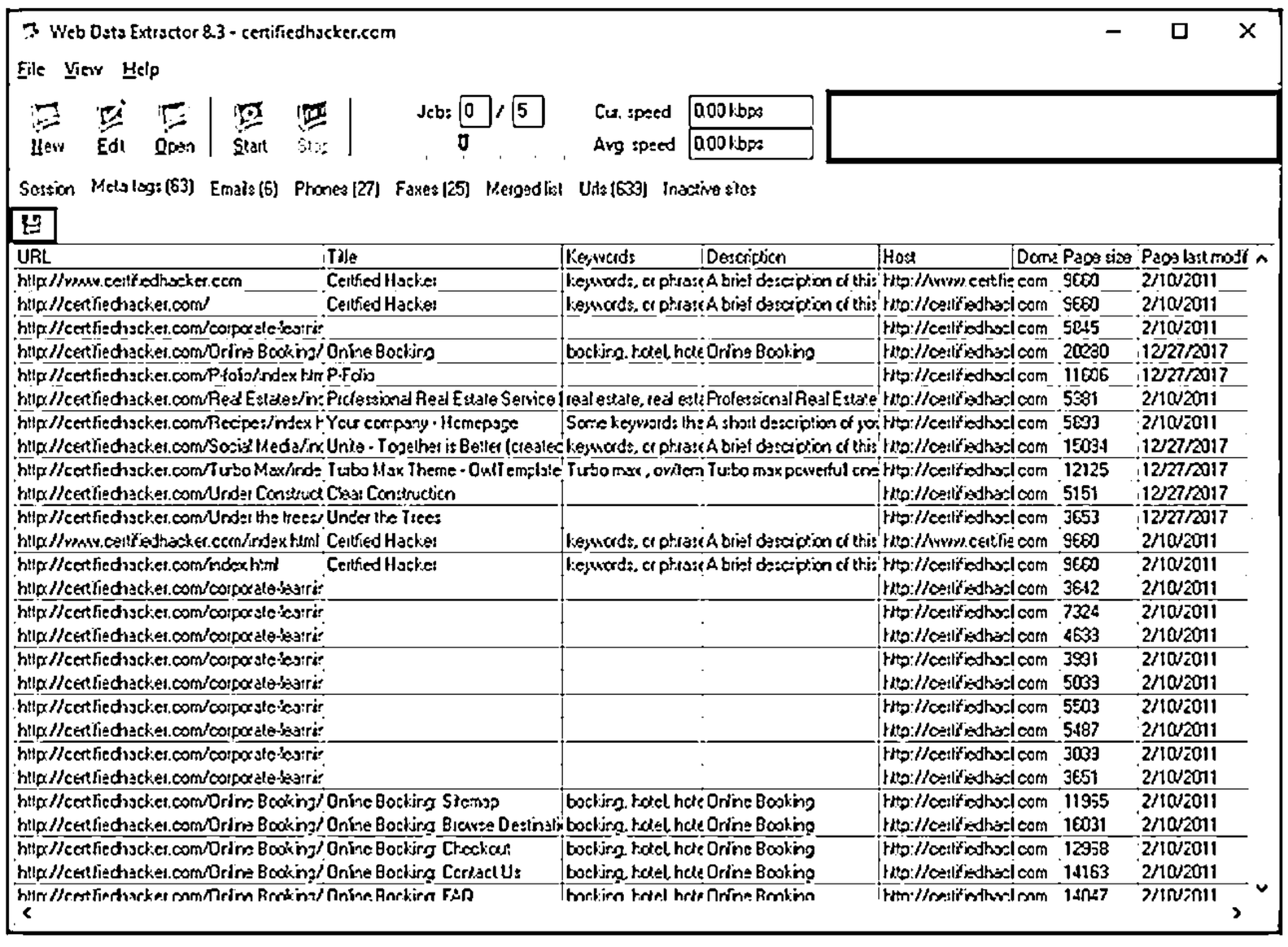


Figure 4.3.14: Web Data Extractor - Meta tags tab

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

18. An **Information** pop-up may appear with the message **You cannot save more than 10 records in Demo Version**; click **OK**.

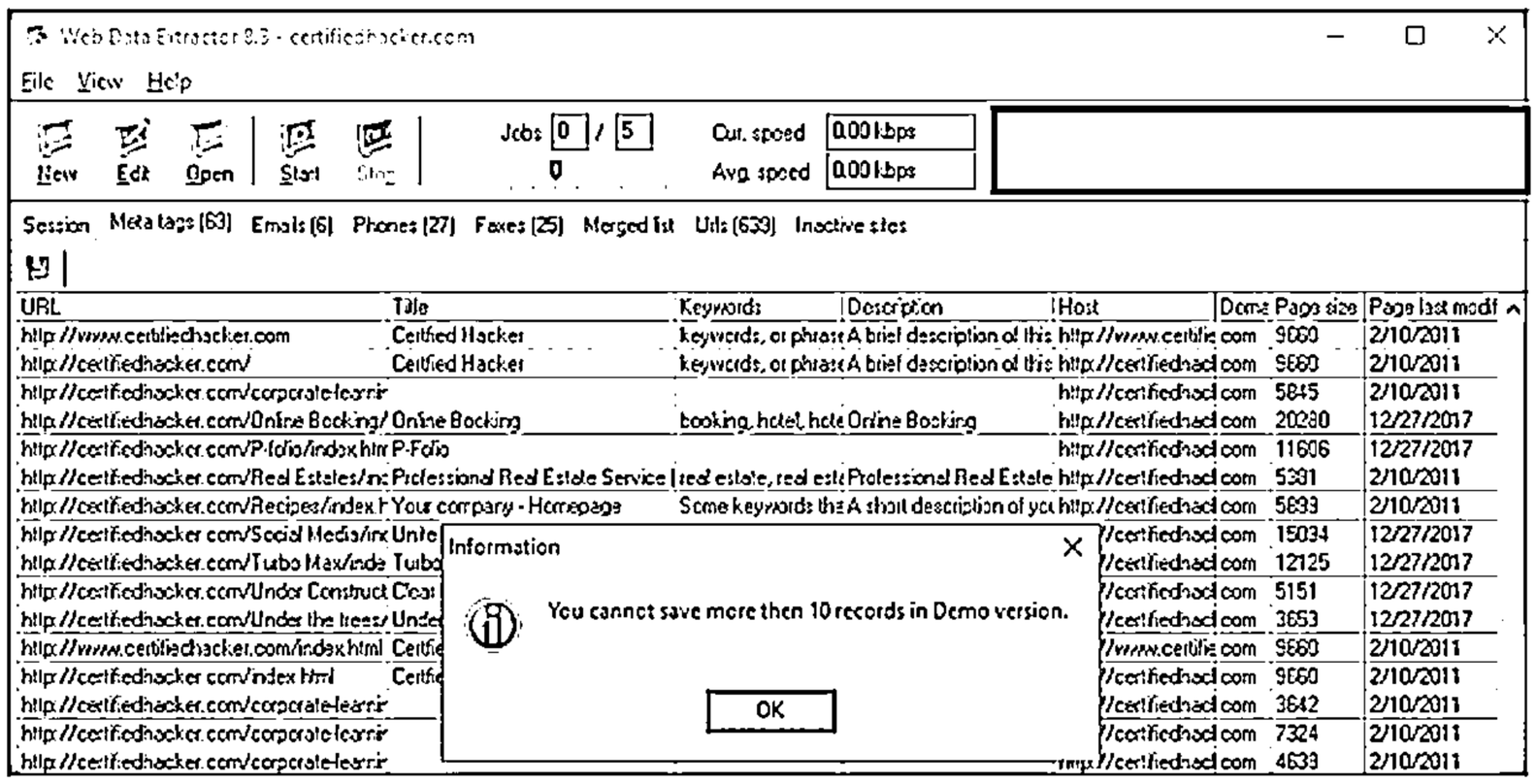


Figure 4.3.15: Web Data Extractor saving information window

19. The **Save Meta tags** window appears. In the **File name** field, click on the **folder icon**, select the location where you want to save the file, choose **File format**, and click **Save**.

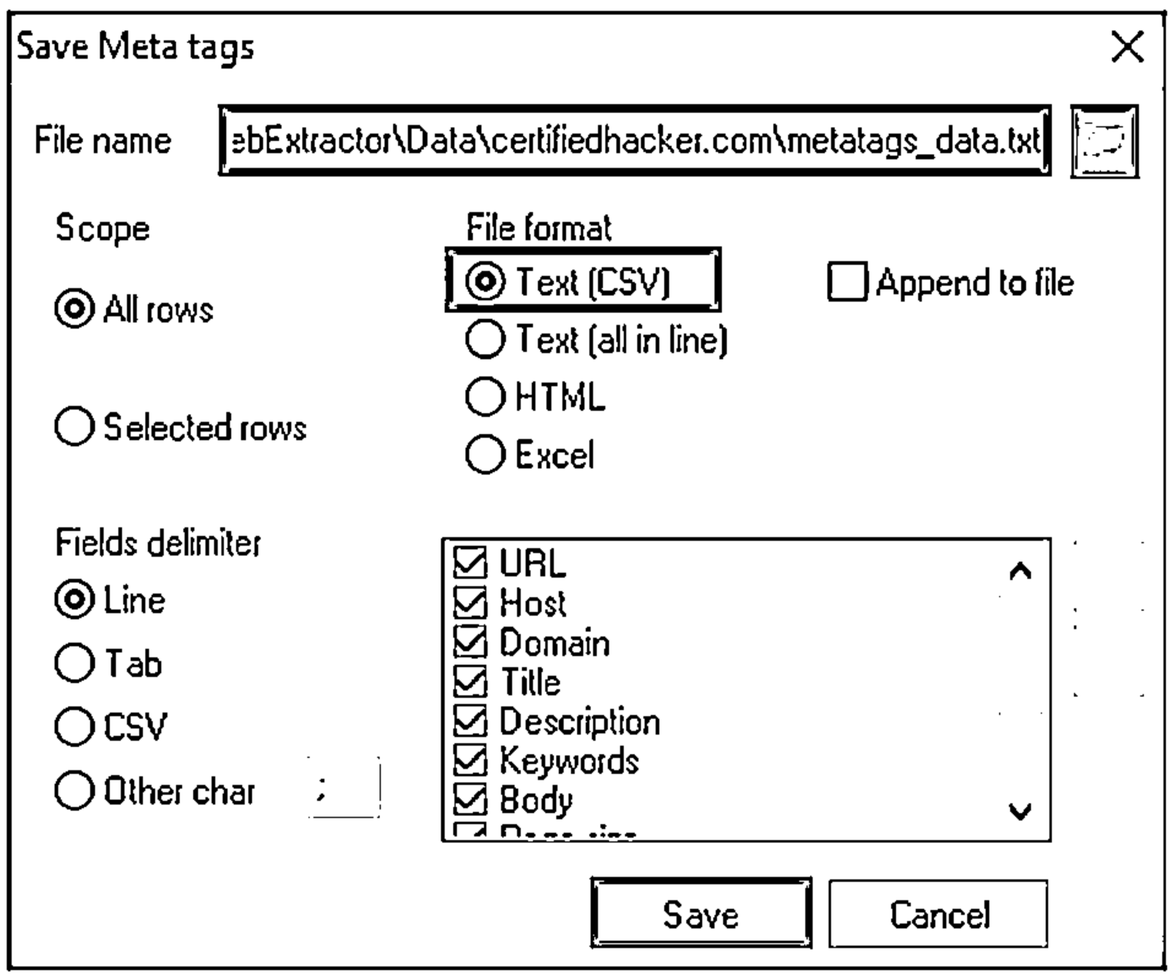


Figure 4.3.16: Web Data Extractor saving window

You can also use other web spiders such as **ParseHub** (https://www.parsehub.com), **SpiderFoot** (https://www.spiderfoot.net), etc. to extract the target organization's data.

20. By default, the session will be saved at **C:\Program Files (x86)\WebExtractor\Data\certifiedhacker.com**. You can choose your desired location to save the file.
21. This concludes the demonstration of extracting a company's data using the Web Data Extractor tool.
22. Close all open windows and document all the acquired information.

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

TASK 4 Mirror a Target Website using HTTrack Web Site Copier

Here, we will use the HTTrack Web Site Copier tool to mirror the entire website of the target organization, store it in the local system drive, and browse the local website to identify possible exploits and vulnerabilities.

TASK 4.1

Install HTTrack Web Site Copier

1. In the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance\Website Mirroring Tools\HTTrack Web Site Copier** and double-click **httrack-3.49.2.exe**.
2. If the **User Account Control** pop-up appears, click **Yes**.

Note: If the **Open File - Security Warning** pop-up appears, click **Run**.

3. Follow the wizard steps to install **HTTrack Web Site Copier**.
4. In the last step of the installation wizard, uncheck the **View history.txt file** option and click **Finish**.

Website mirroring is the process of creating a replica or clone of the original website; this mirroring of the website helps you to footprint the web site thoroughly on your local system, and allows you to download a website to a local directory, analyze all directories, HTML, images, flash, videos, and other files from the server on your computer.

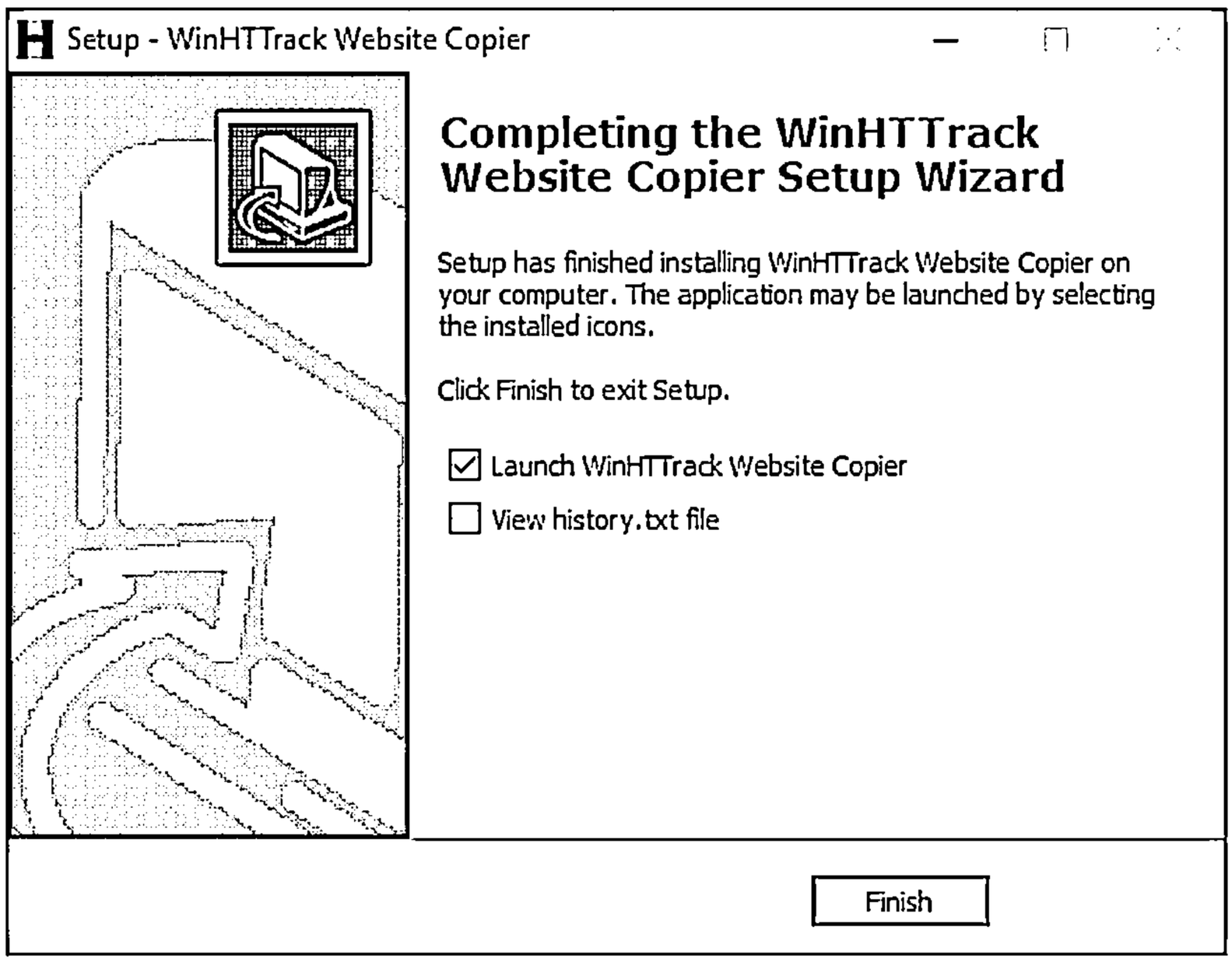


Figure 4.4.1: HTTrack Website Copier Setup Pop-up Wizard

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

TASK 4.2

Mirror the Target Website

5. The **WinHTTrack Website Copier** window appears. Click **OK** in the pop-up window, and then click **Next >** to create a **New Project**.

Note: If the application does not launch, you can launch it manually from the **Apps** screen.

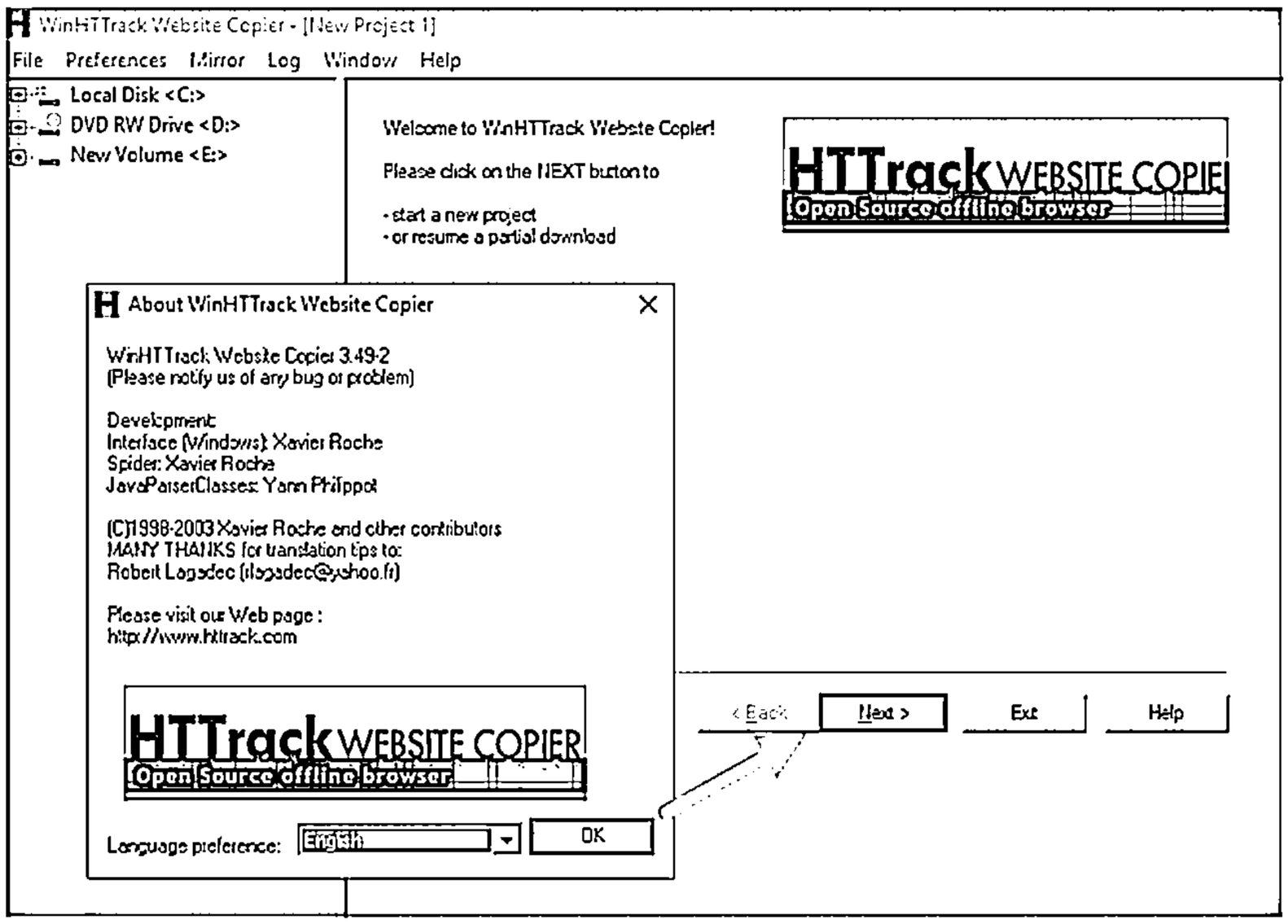


Figure 4.4.2: HTTrack Website Copier main window

You can duplicate websites by using website mirroring tools such as HTTrack Web Site Copier. HTTrack is an offline browser utility that downloads a website from the Internet to a local directory, builds all directories recursively, and transfers HTML, images, and other files from the webserver to another computer.

6. Enter the name of the project (here, **Test Project**) in the **New project name:** field. Select the **Base path:** to store the copied files; click **Next >**.

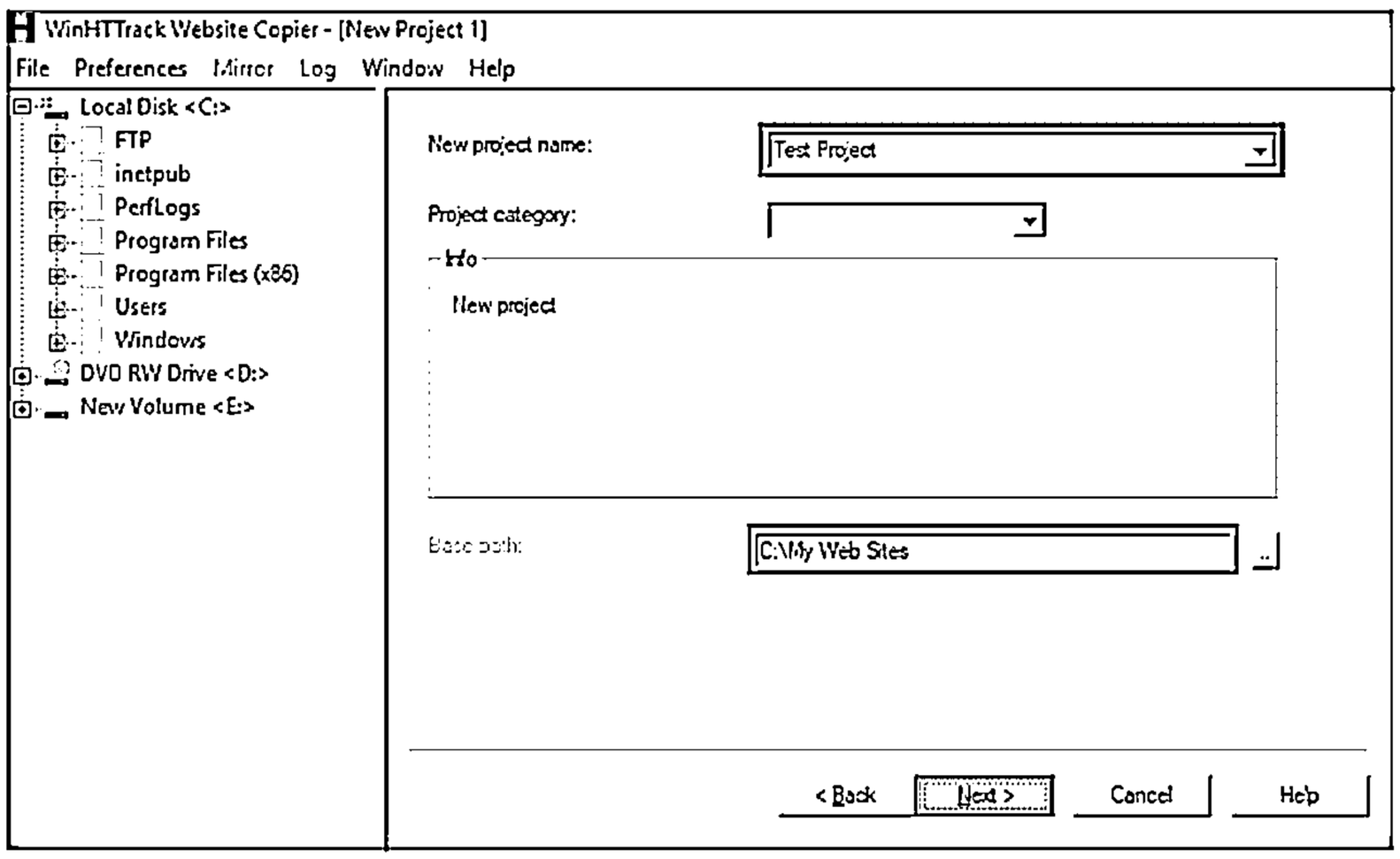


Figure 4.4.3: HTTrack Website Copier selecting a New Project

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

7. Enter a target URL (here, **www.certifiedhacker.com**) in the **Web Addresses: (URL)** field and click **Set options...**

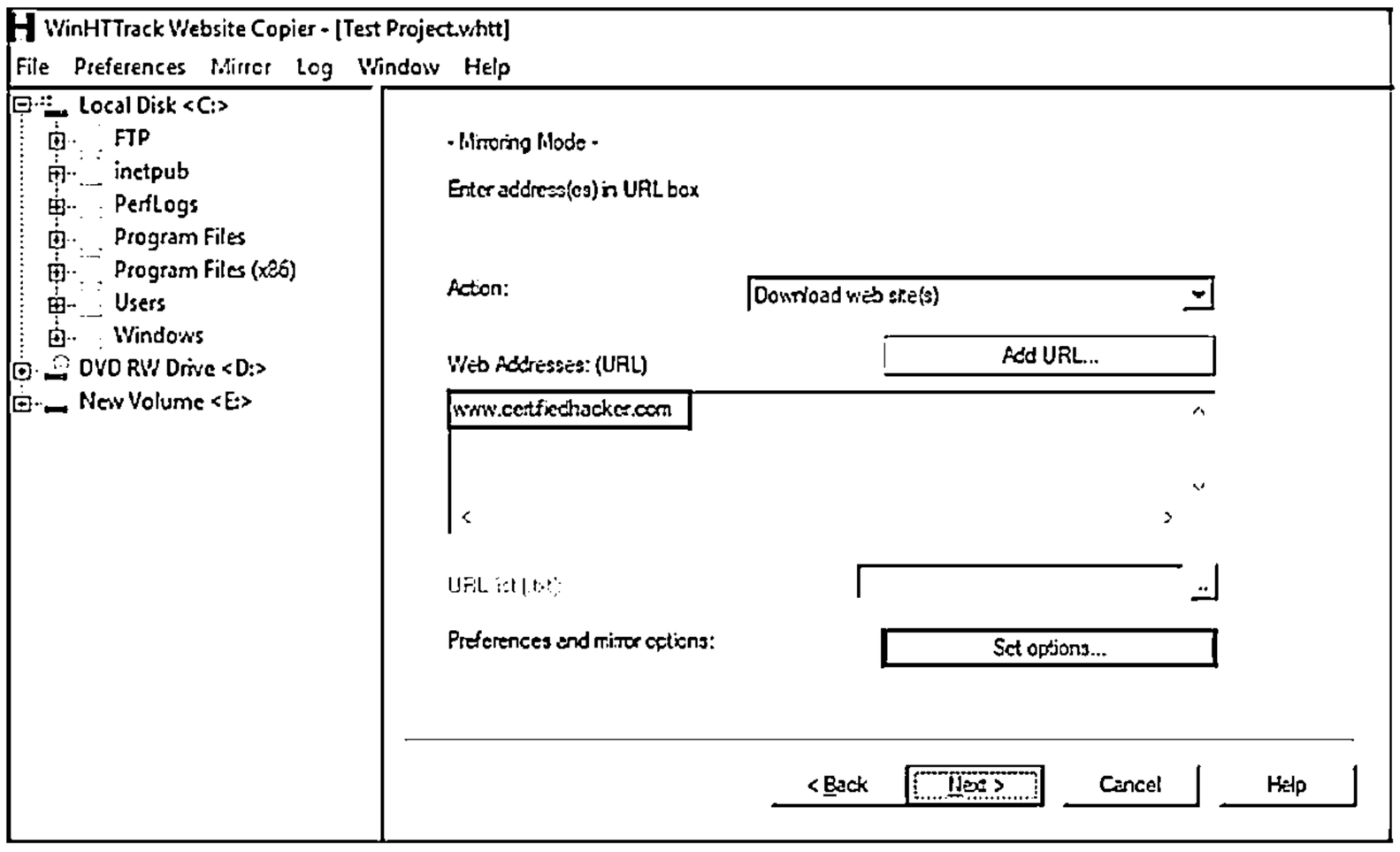


Figure 4.4.4: Setting options in HTTrack Website Copier

8. **WinHTTrack** window appears, click the **Scan Rules** tab and select the checkboxes for the file types as shown in the following screenshot; click **OK**.

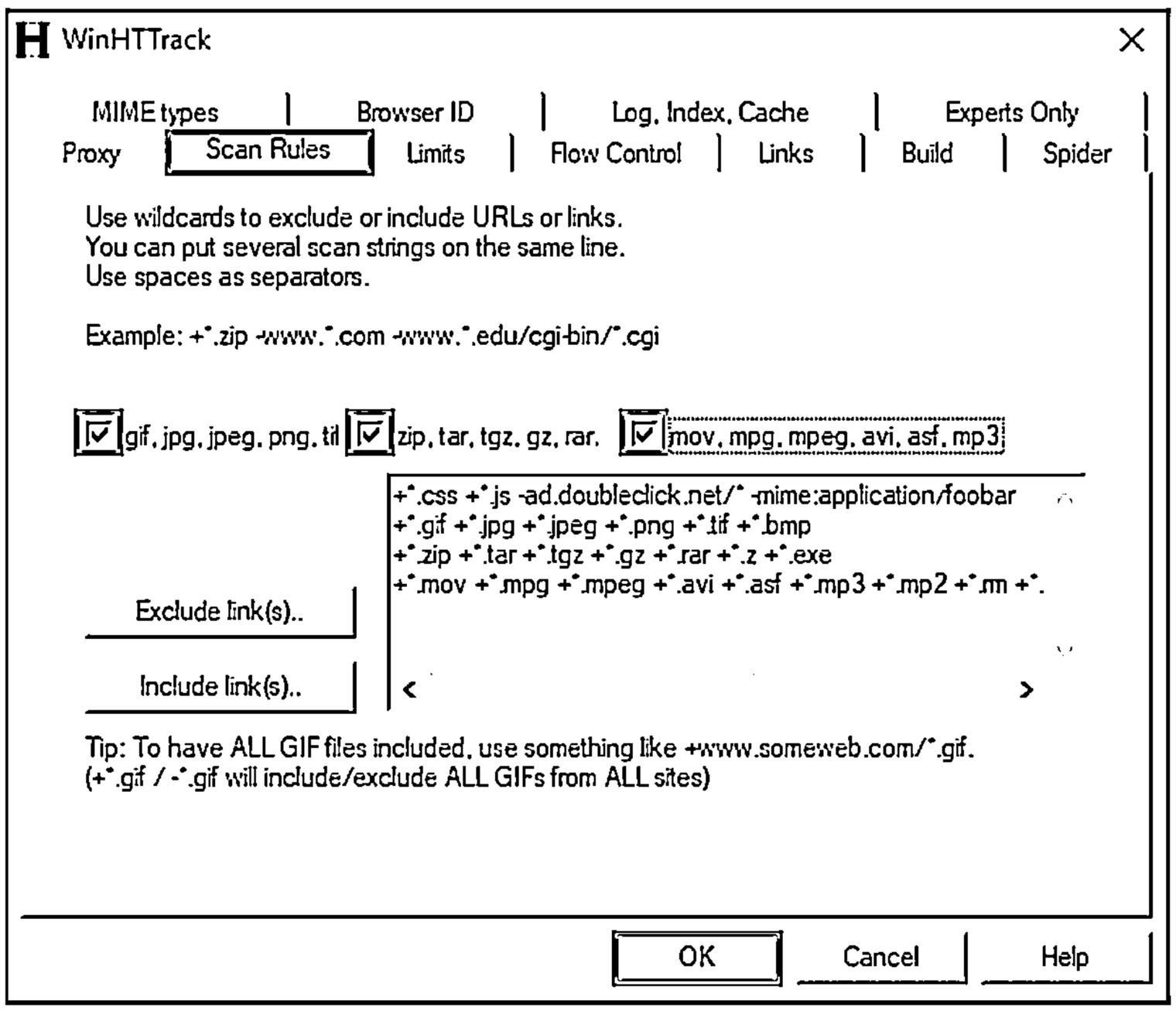


Figure 4.4.5: Scan Rules tab in HTTrack Website Copier

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

9. Click the **Next >** button.

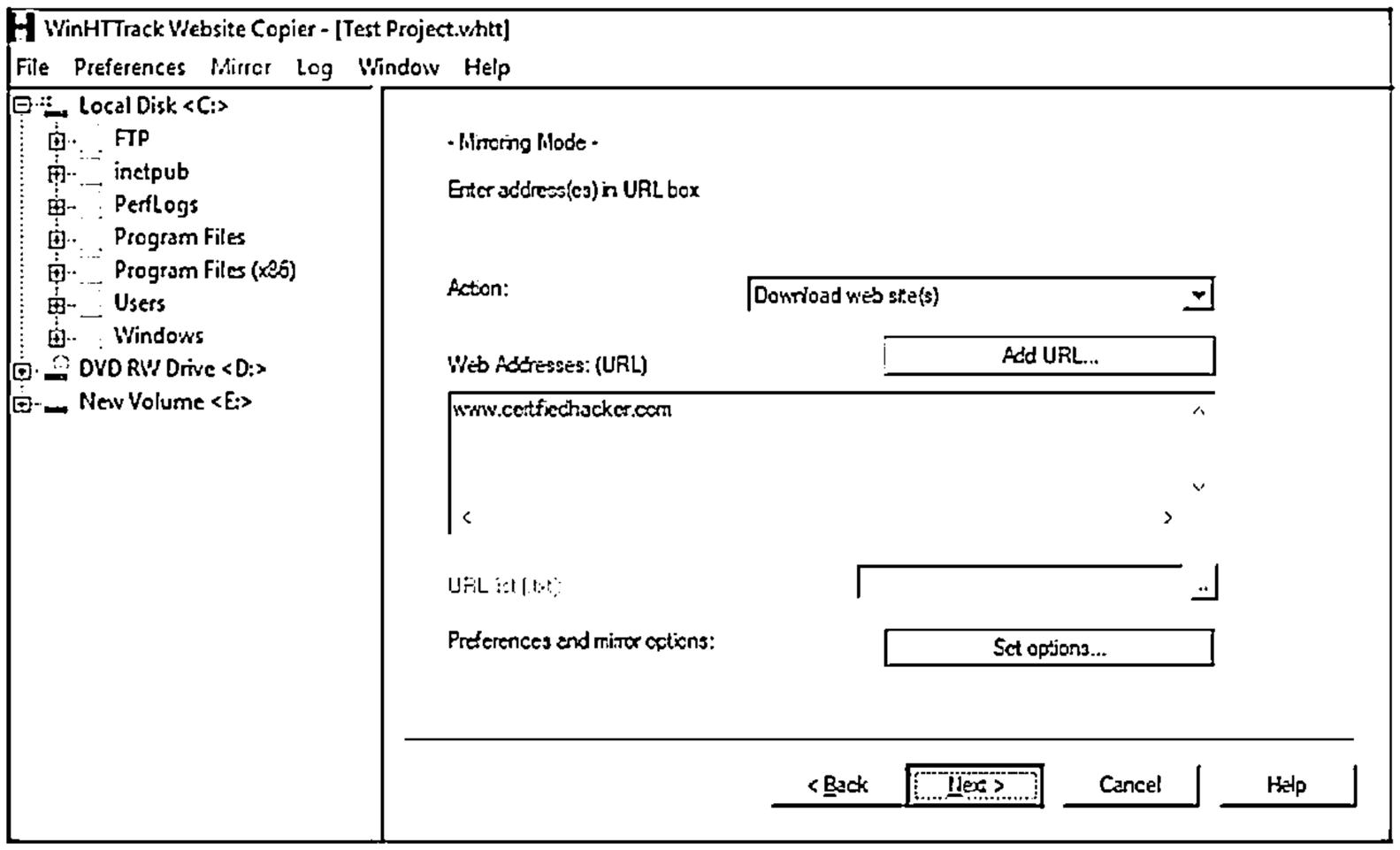


Figure 4.4.6: HTTrack Website Copier Select a project window

10. By default, the radio button will be selected for **Please adjust connection parameters if necessary, then press FINISH to launch the mirroring operation.** Check **Disconnect when finished** and click **Finish** to start mirroring the website.

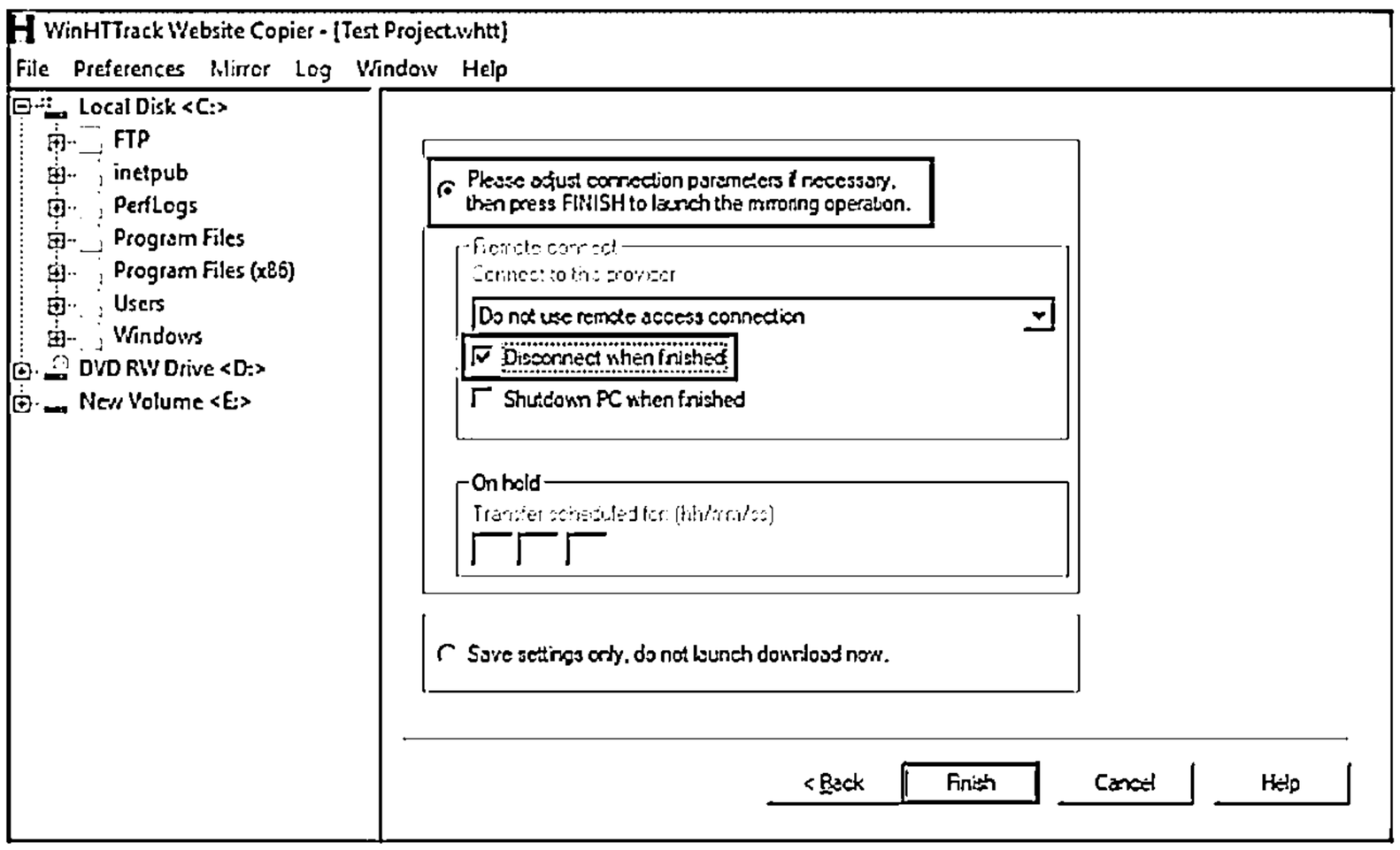


Figure 4.4.7: HTTrack Website Copier launching mirroring operation

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

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

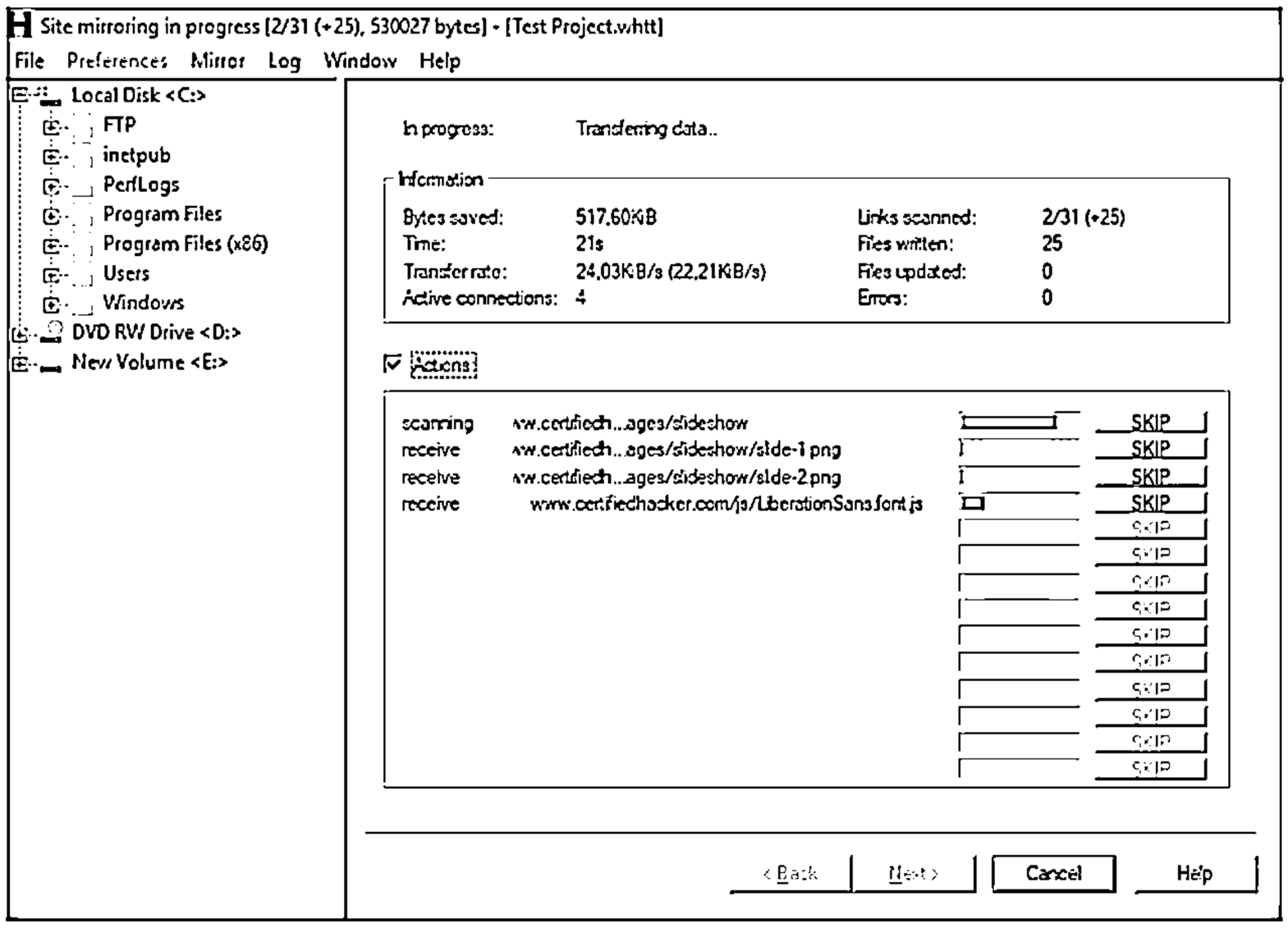


Figure 4.4.8: HTTrack Website Copier displaying site mirroring progress

12. Once the site mirroring is completed, WinHTTrack displays the message **Mirroring operation complete**; click on **Browse Mirrored Website**.

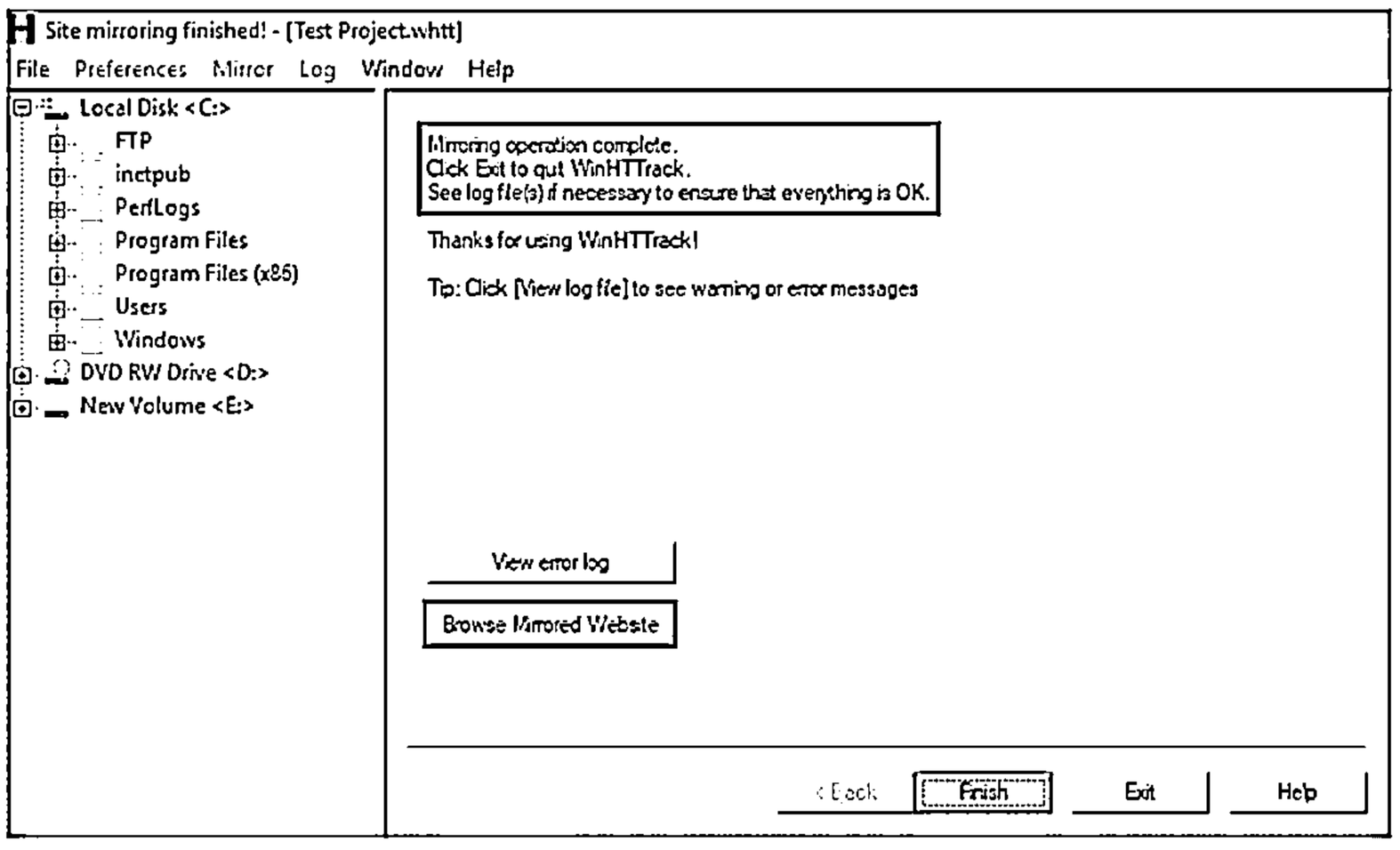


Figure 4.4.9: HTTrack Website Copier displaying site mirroring is complete

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

TASK 4.3

Browse the Mirrored Website

13. If the **How do you want to open this file?** pop up appears, select any web browser (here, **Mozilla Firefox**) and click **OK**.

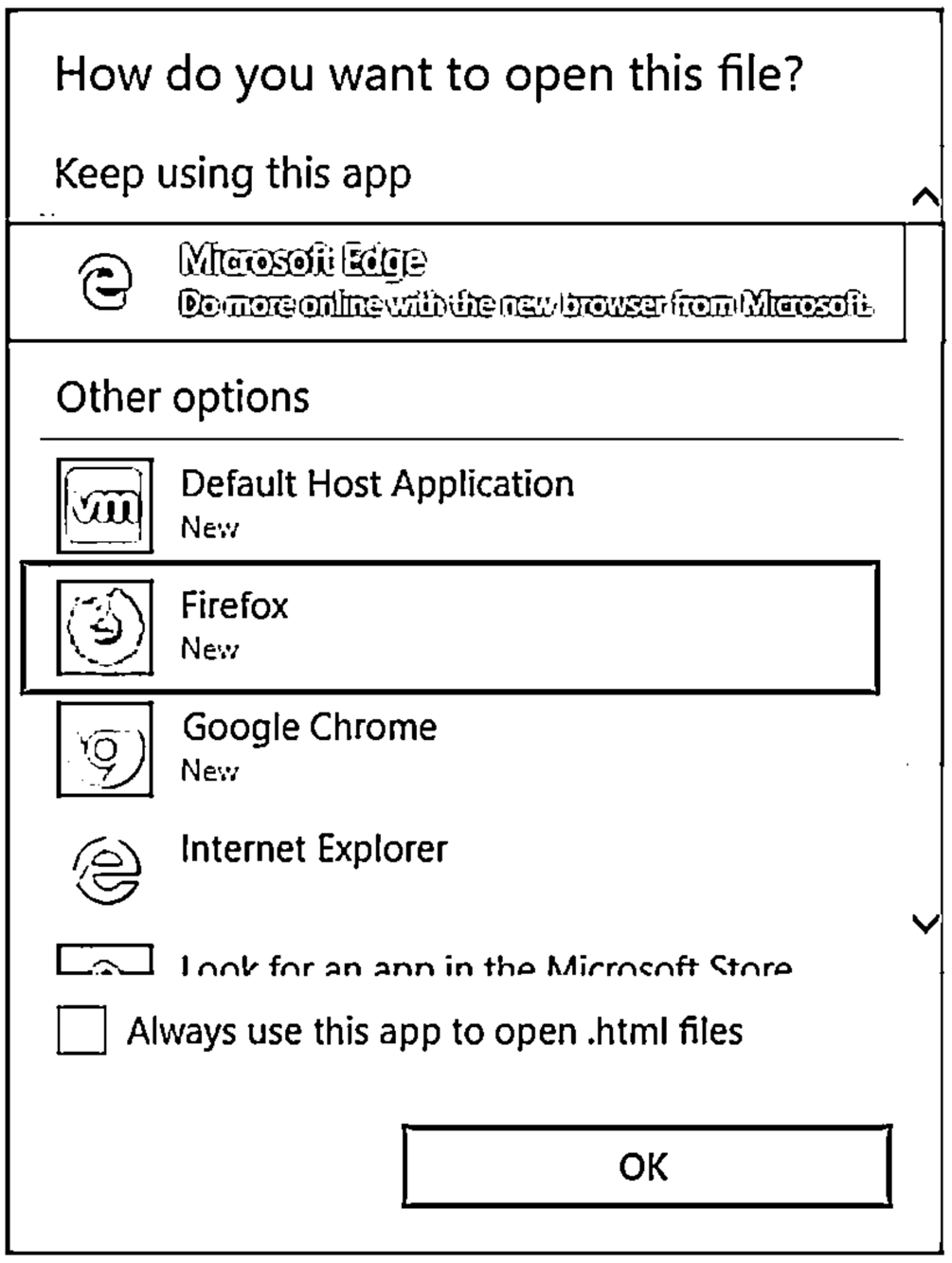


Figure 4.4.10: Selecting Mozilla Firefox

14. The mirrored website for **www.certifiedhacker.com** launches. The URL displayed in the address bar indicates that the website's image is stored on the local machine.

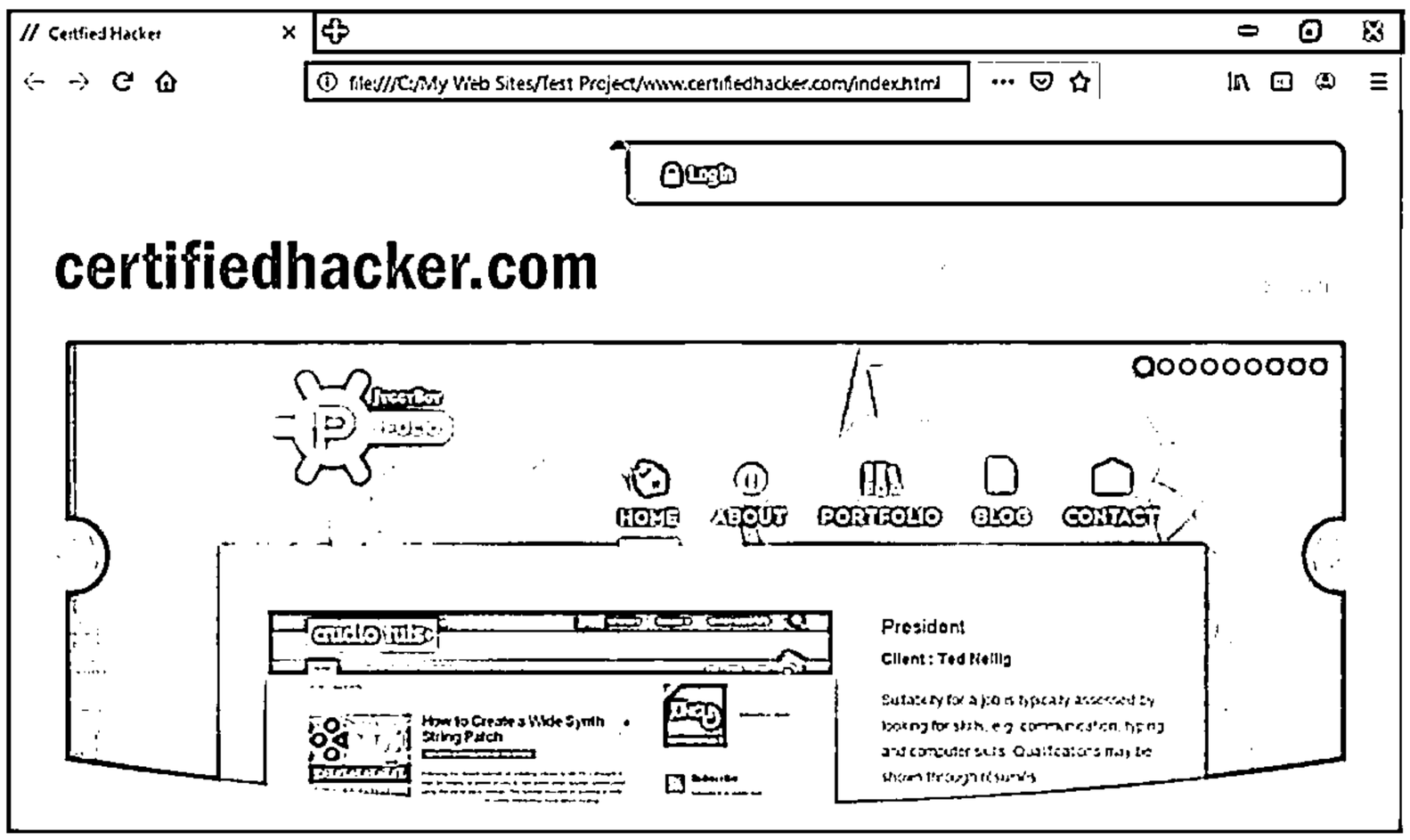


Figure 4.4.11: HTTrack Website Copier Mirrored Website Image

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

15. Analyze all directories, HTML, images, flash, videos, and other files available on the mirrored target website. You can also check for possible exploits and vulnerabilities. The site will work like a live hosted website.

Note: If the webpage does not open, navigate to the directory where you mirrored the website and open **index.html** with any browser.

16. Once done with your analysis, close the **Firefox** window and click **Finish** on the **WinHTTrack** window to complete the process

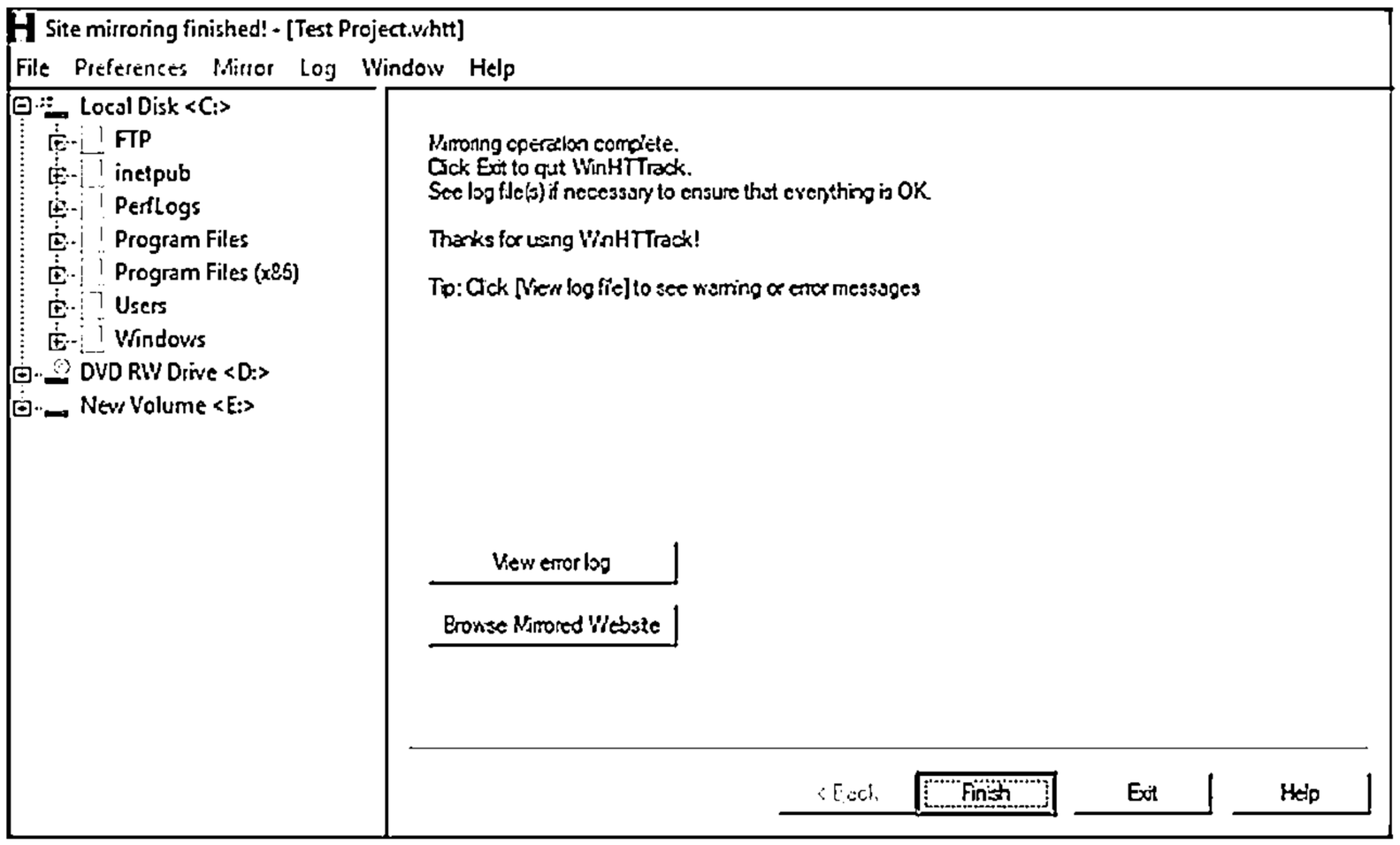


Figure 4.4.12: HTTrack Website Copier displaying site mirroring is complete

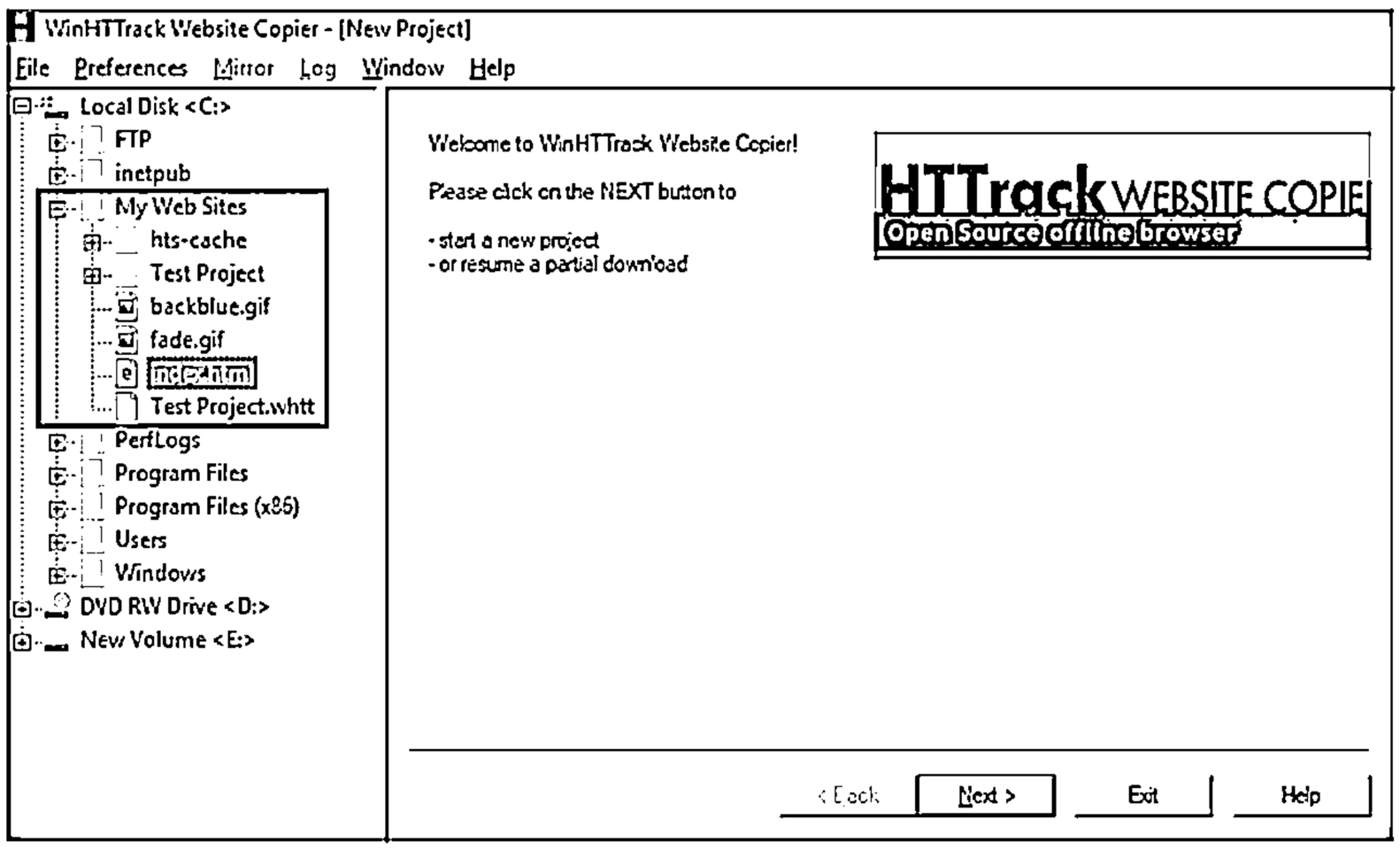


Figure 4.4.13: HTTrack Website Copier displaying mirrored website location

17. Some websites are very large, and it might take a long time to mirror the complete site.

You can also use other mirroring tools such as **NCollector Studio** (http://www.calluna-software.com), **Cyotek WebCopy** (https://www.cyotek.com), etc. to mirror a target website.

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

18. This concludes the demonstration of mirroring a target website using HTTrack Web Site Copier.
19. Close all open windows and document all the acquired information.
20. Turn off the **Windows 10** virtual machine.

TASK 5 Gather a Wordlist from the Target Website using CeWL

The words available on the target website may reveal critical information that can assist in performing further exploitation. CeWL is a ruby app that is used to spider a given target URL to a specified depth, optionally following external links, and returns a list of unique words that can be used for cracking passwords.

1. Turn on **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

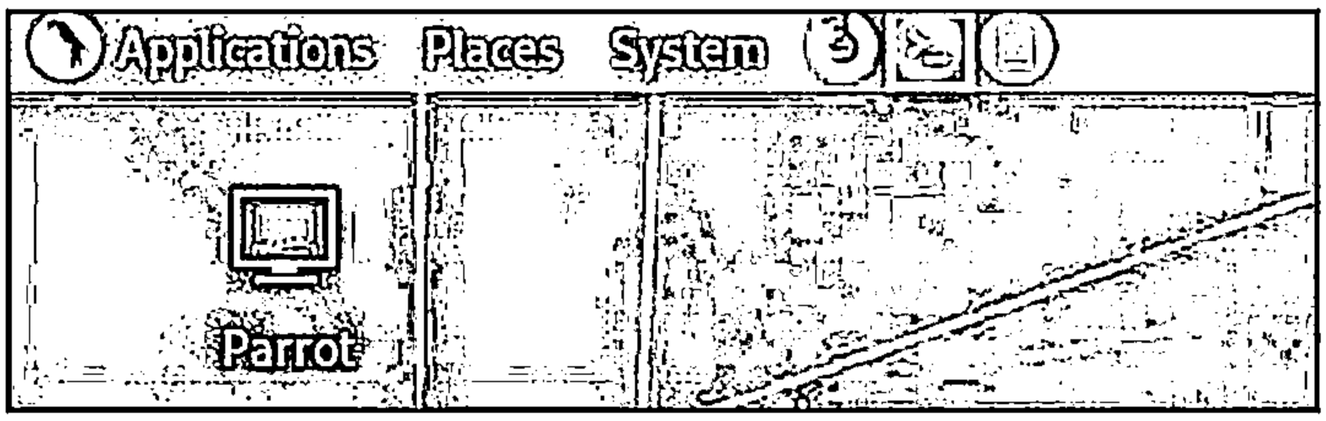


Figure 4.5.1: MATE Terminal Icon

4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

6. Now, type **cd** and press **Enter** to jump to the root directory.

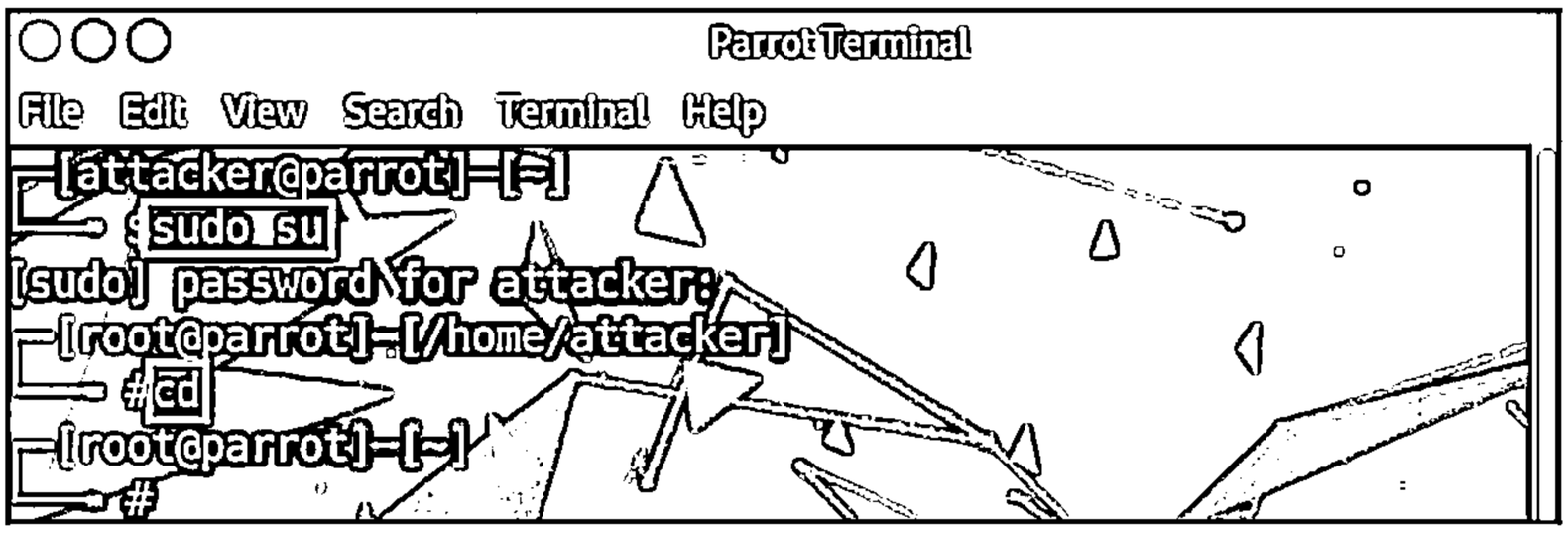


Figure 4.5.2: Running the programs as a root user

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

7. In the **Parrot Terminal** window, type **cewl -d 2 -m 5 www.certifiedhacker.com** and press **Enter**.

Note: **-d** represents the depth to spider the website (here, **2**) and **-m** represents minimum word length (here, **5**).

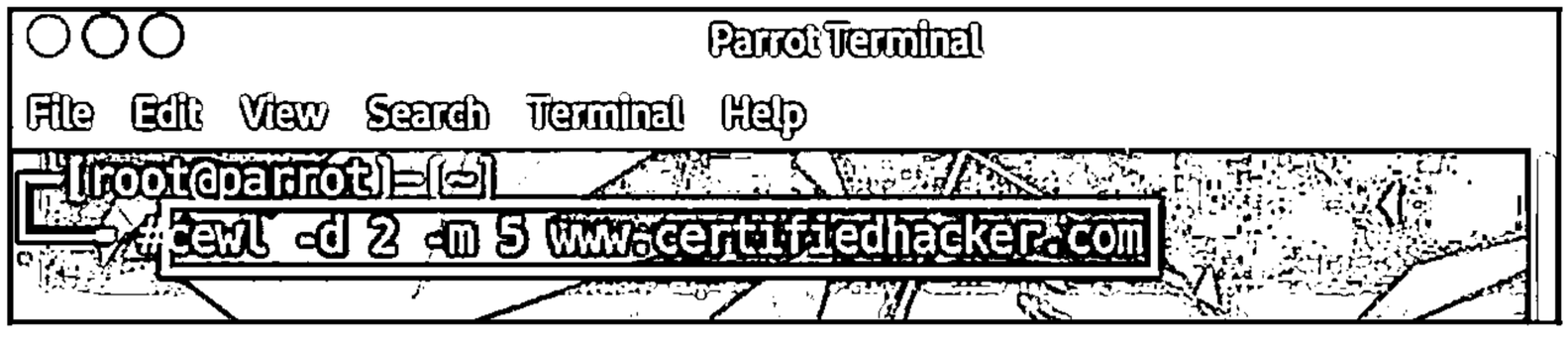


Figure 4.5.3: Gathering wordlist

8. A unique wordlist from the target website is gathered, as shown in the screenshot.

Note: The minimum word length is 5, and the depth to spider the target website is 2.

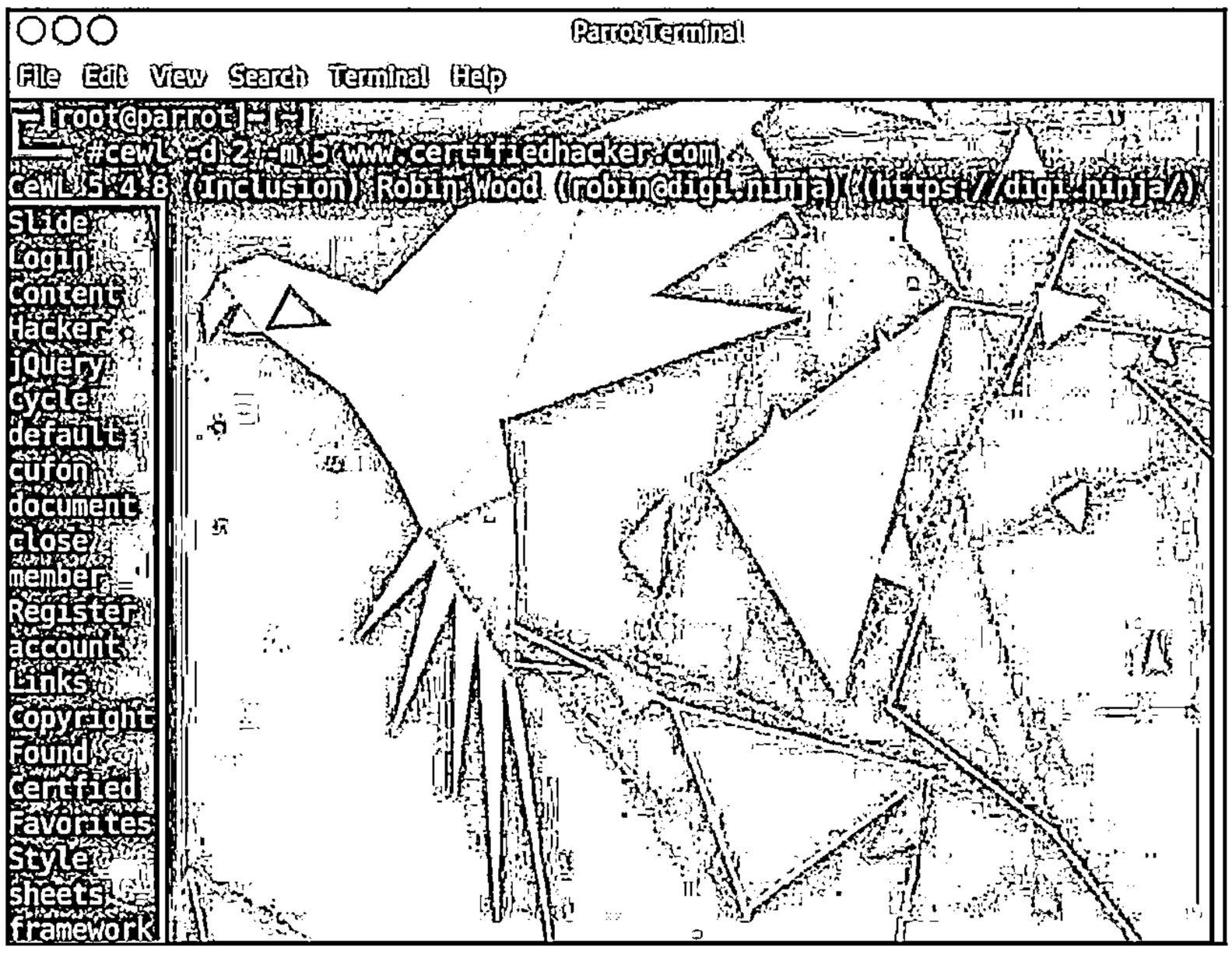


Figure 4.5.4: Wordlist gathered from the target website

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

9. Alternatively, this unique wordlist can be written directly to a text file by typing **cewl -w wordlist.txt -d 2 -m 5 www.certifiedhacker.com**.

Note: -w - Write the output to the file (here, **wordlist.txt**)

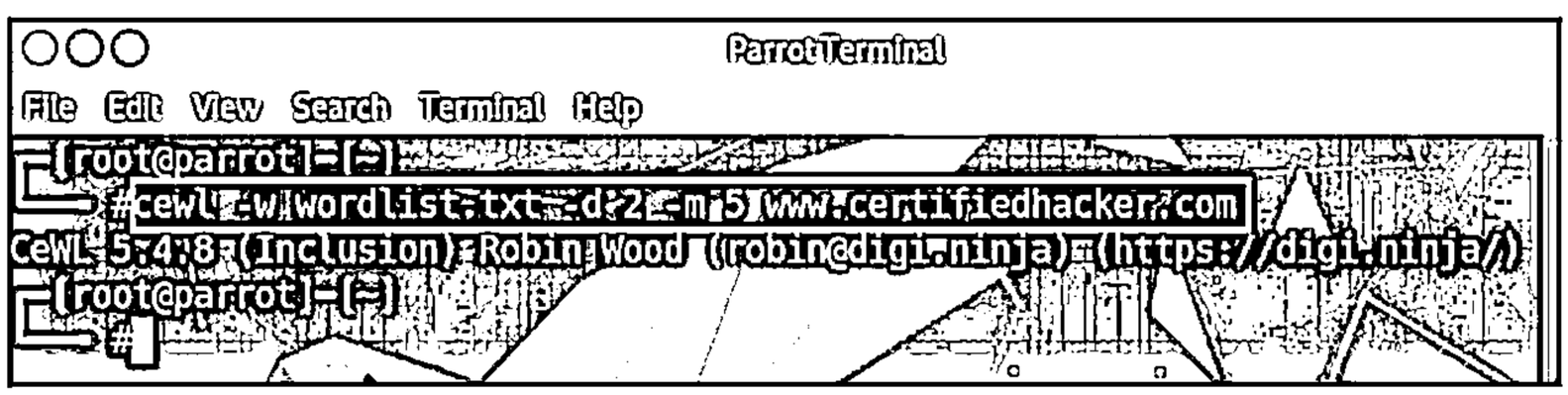


Figure 4.5.5: Wordlist written to wordlist.txt file

10. By default, the wordlist file gets saved in the **root** directory. Type **pluma wordlist.txt** and press **Enter** to view the extracted wordlist.

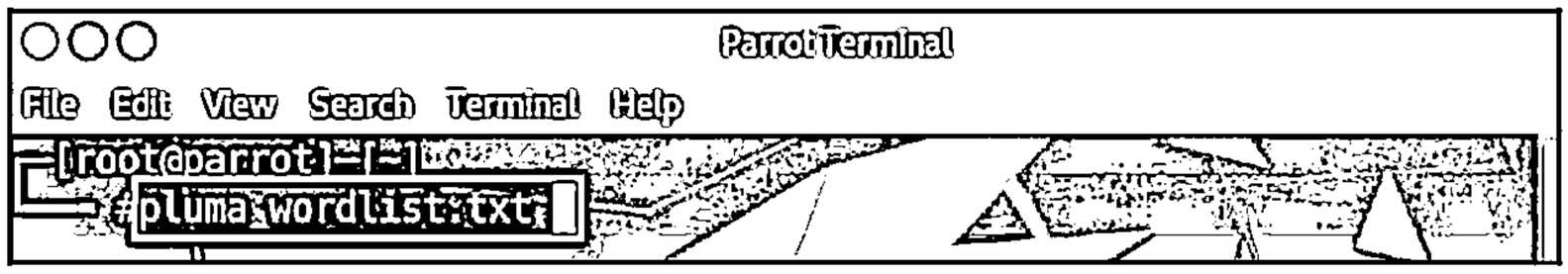


Figure 4.5.6: Open wordlist.txt file

11. The file containing a unique wordlist extracted from the target website opens, as shown in the screenshot.

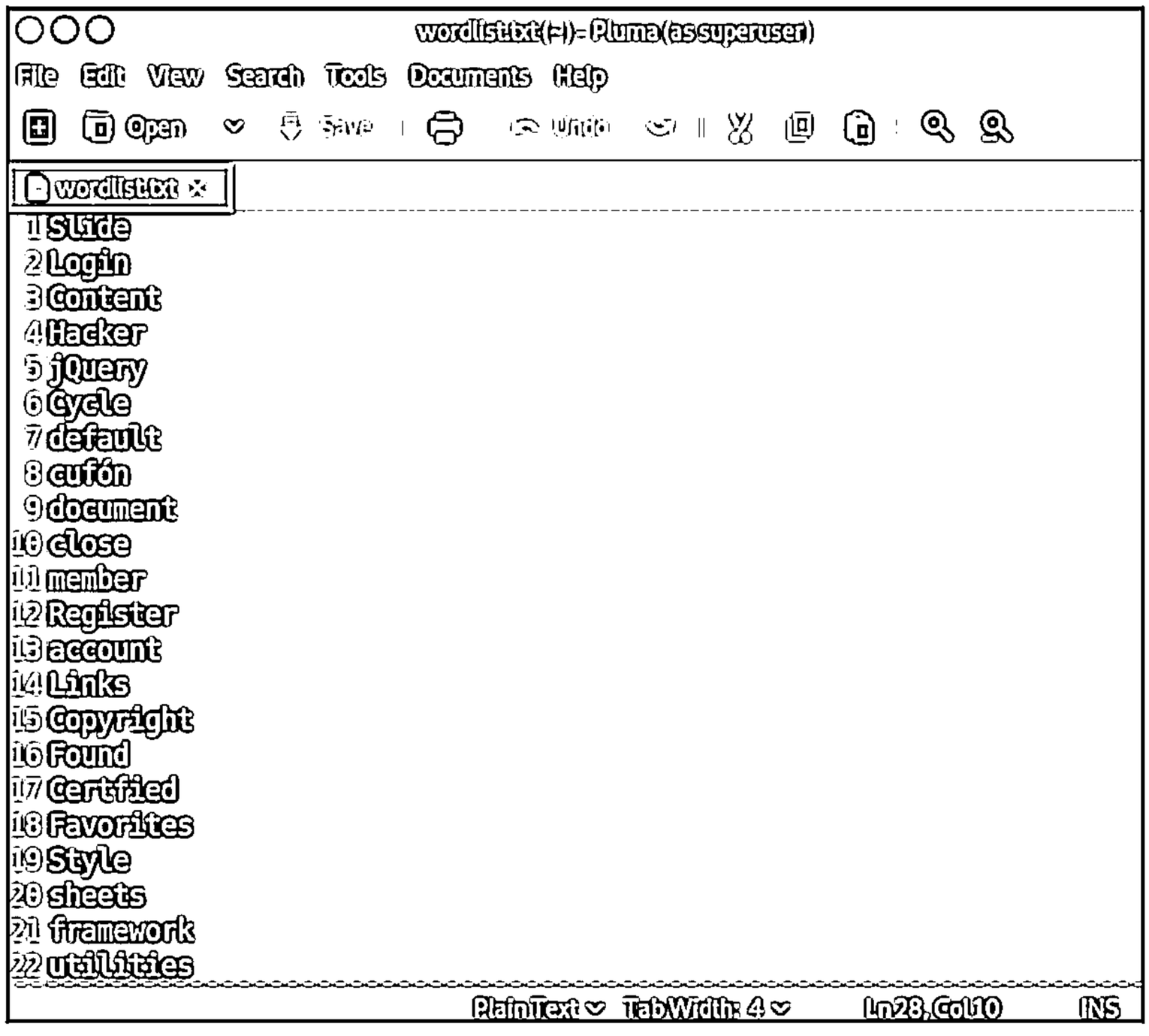


Figure 4.5.7: wordlist.txt file

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

12. This wordlist can be used further to perform brute-force attacks against the previously obtained emails of the target organization's employees.
13. This concludes the demonstration of gathering wordlist from the target website using CeWL.
14. Close all open windows and document all the acquired information.
15. Turn off the **Parrot Security** virtual machine.

Lab Analysis

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

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT 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

Perform Email Footprinting

Email footprinting or tracing emails involves analyzing the email header to discover details about the sender.

Lab Scenario

ICON KEY

Valuable information

Test your knowledge

Web exercise

Workbook review

As a professional ethical hacker, you need to be able to track emails of individuals (employees) from a target organization for gathering critical information that can help in building an effective hacking strategy. Email tracking allows you to collect information such as IP addresses, mail servers, OS details, geolocation, information about service providers involved in sending the mail etc. By using this information, you can perform social engineering and other advanced attacks.

Lab Objectives

- Gather information about a target by tracing emails using eMailTrackerPro

Lab Environment

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance

To carry out this lab, you need:

- Windows 10 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- eMailTrackerPro located at **E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance\Email Tracking Tools\eMailTrackerPro**
- You can also download the latest version of eMailTrackerPro from its official website. If you decide to download the latest version, the screenshots shown in the lab might differ.

Lab Duration

Time: 10 Minutes

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

Overview of Email Footprinting

E-mail footprinting, or tracking, is a method to monitor or spy on email delivered to the intended recipient. This kind of tracking is possible through digitally time-stamped records that reveal the time and date when the target receives and opens a specific email.

Email footprinting reveals information such as:

- Recipient's system IP address
- The GPS coordinates and map location of the recipient
- When an email message was received and read
- Type of server used by the recipient
- Operating system and browser information
- If a destructive email was sent
- 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 were set to expire after a specified time

Lab Tasks

TASK 1 — Gather Information about a Target by Tracing Emails using eMailTrackerPro

Here, we will gather information by analyzing the email header using eMailTrackerPro.

1. Turn on the **Windows 10** virtual machine.
2. Login to the **Windows 10** virtual machine with Username: **Admin** and Password: **Pa$$w0rd**.

TASK 1.1 — Install eMailTrackerPro

3. Open **File Explorer** and navigate to **E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance\Email Tracking Tools\eMailTrackerPro** and double-click **emt.exe**.
4. If the **User Account Control** pop-up appears, click **Yes**.
5. The **eMailTrackerPro Setup** window appears. Follow the wizard steps (by selecting default options) to install eMailTrackerPro.

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

The email header is a crucial part of any email and it is considered a great source of information for any ethical hacker launching attacks against a target. An email header contains the details of the sender, routing information, addressing scheme, date, subject, recipient, etc. Additionally, the email header helps ethical hackers to trace the routing path taken by an email before delivering it to the recipient.

6. After the installation is complete, in the **Completing the eMailTrackerPro Setup Wizard,** uncheck the **Show Readme** check-box and click the **Finish** button to launch the eMailTrackerPro.

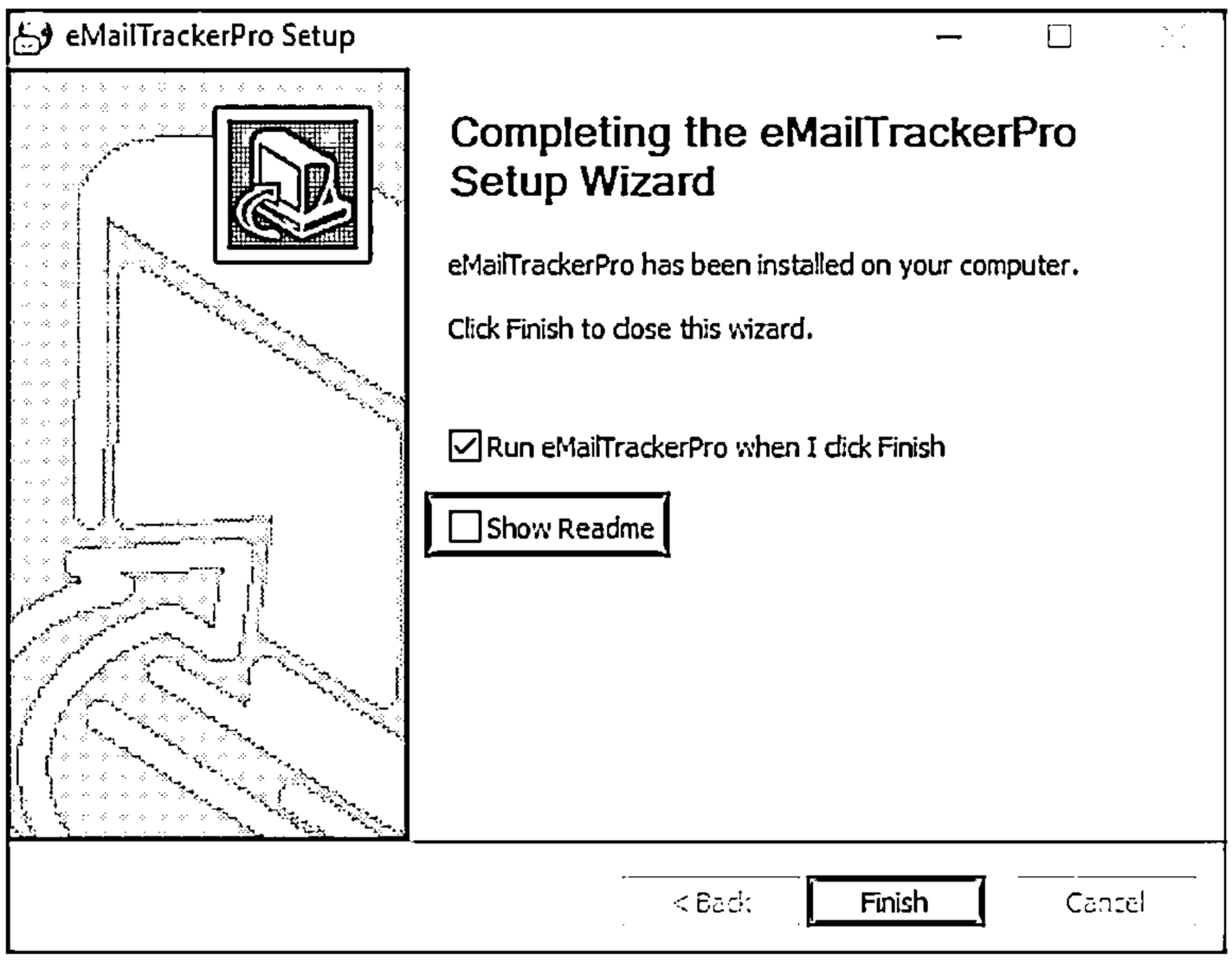


Figure 5.1.1: eMailTrackerPro installation Complete

7. The main window of **eMailTrackerPro** appears along with the **Edition Selection** pop-up; click **OK**.

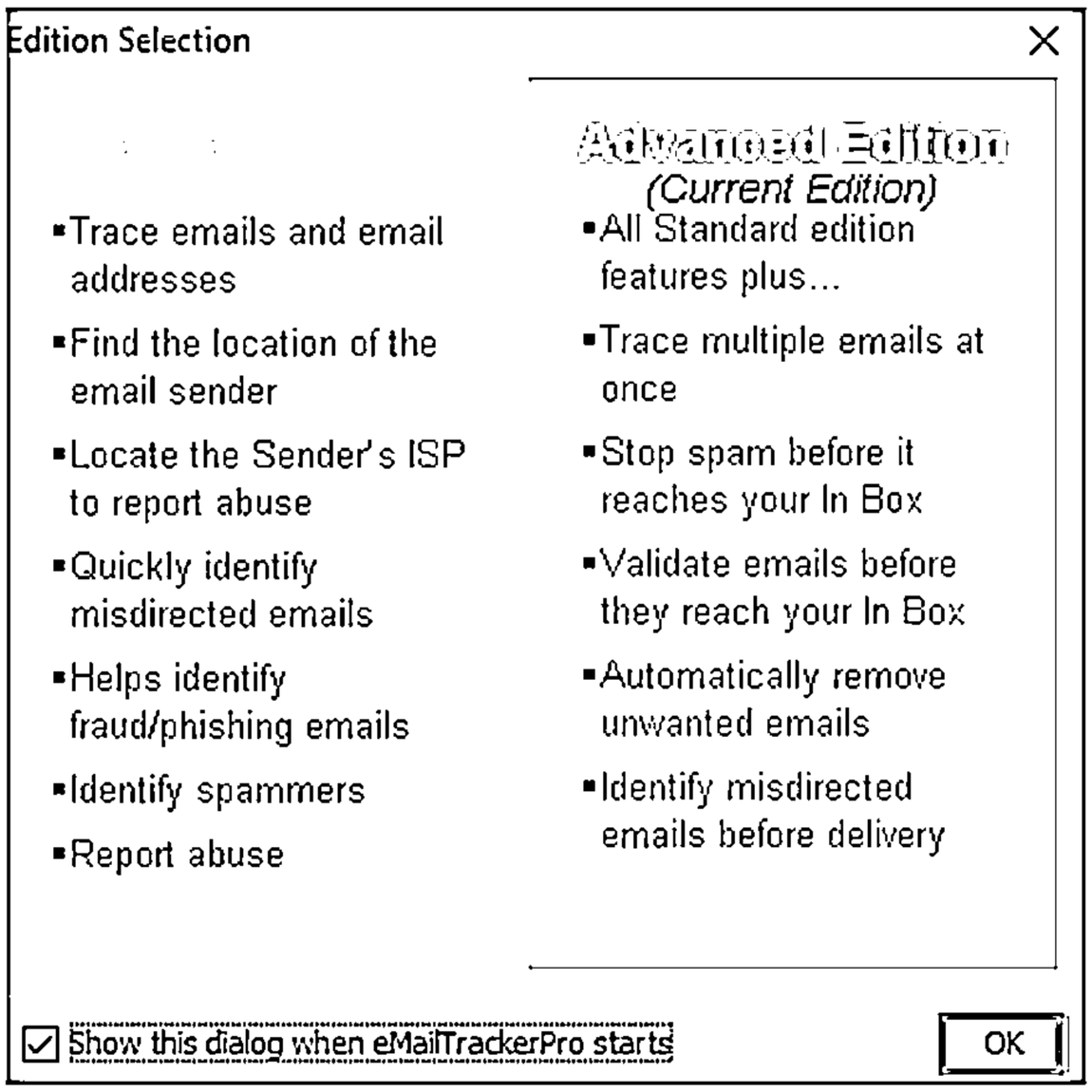


Figure 5.1.2: eMailTrackerPro - Edition Selection pop-up window

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

8. The **eMailTrackerPro** main window appears, as shown in the screenshot.

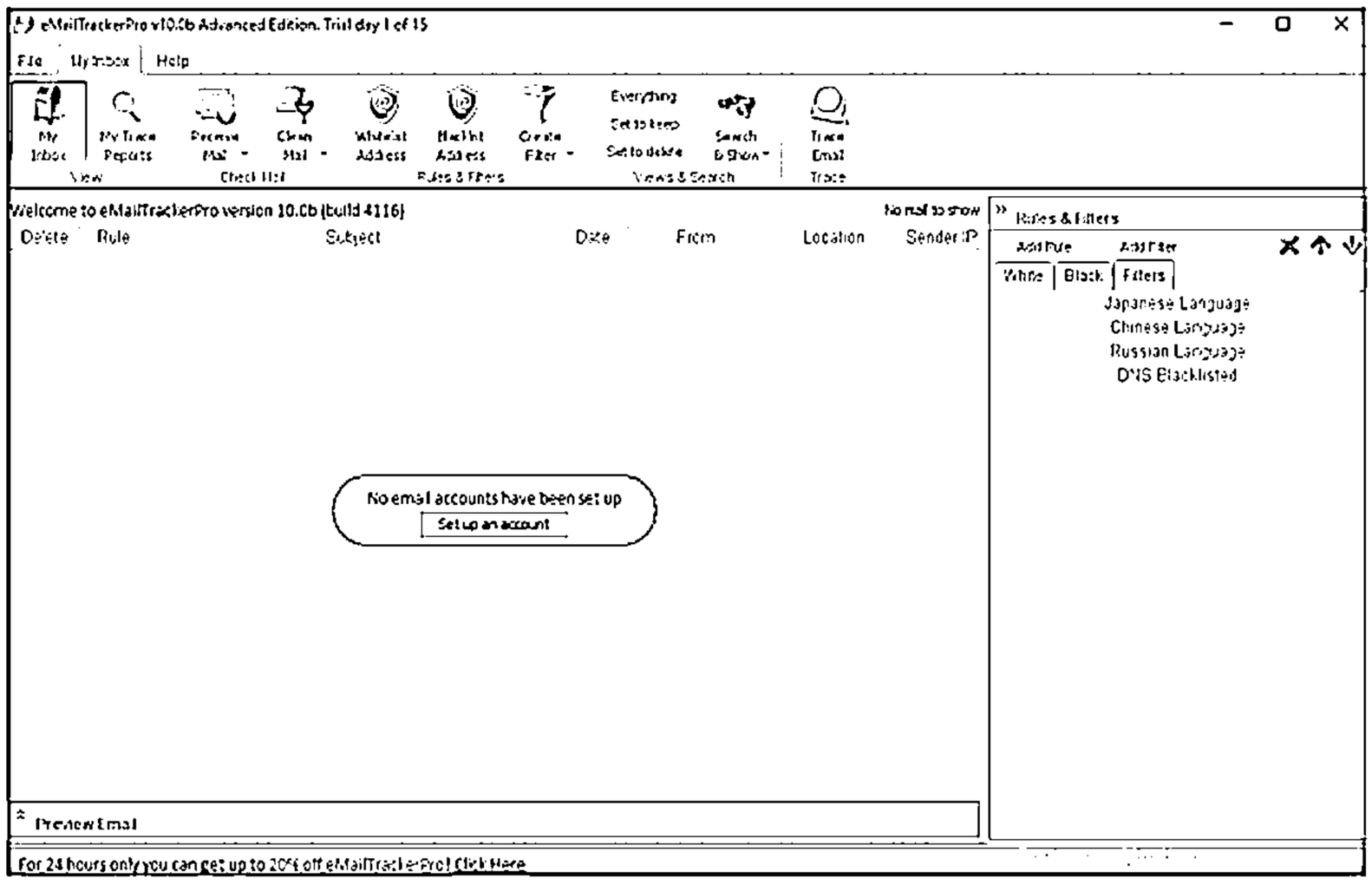


Figure 5.1.3: eMailTrackerPro main window

TASK 1.2

Trace Email Header

9. To trace email headers, click the **My Trace Reports** icon from the **View** section. (here, you will see the output report of the traced email header)
10. Click the **Trace Headers** icon from the **New Email Trace** section to start the trace.

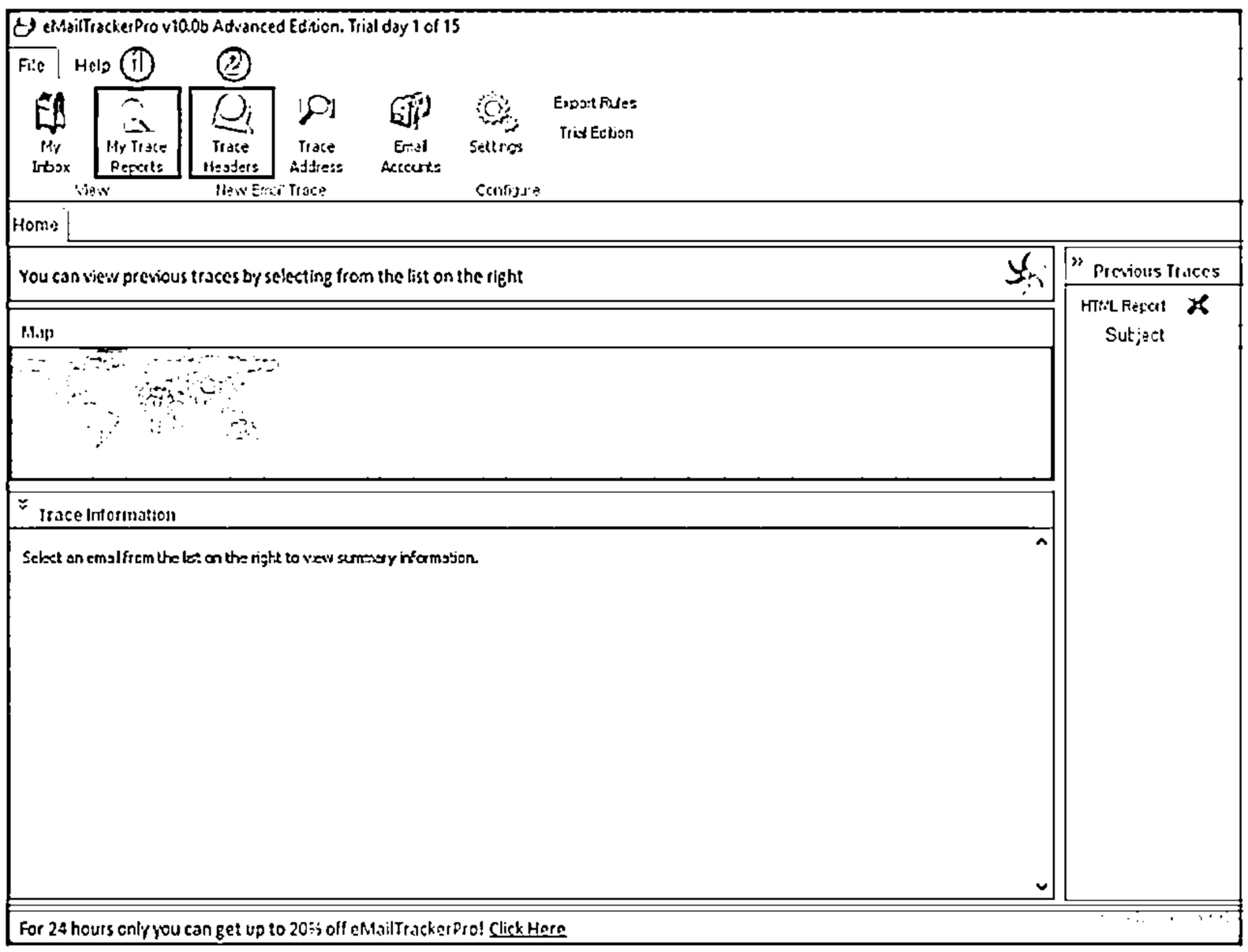


Figure 5.1.4: The eMailTrackerPro main window

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

11. A pop-up window will appear; select **Trace an email I have received.** Copy the email header from the suspicious email you wish to trace and paste it in the **Email headers:** field under **Enter Details** section.

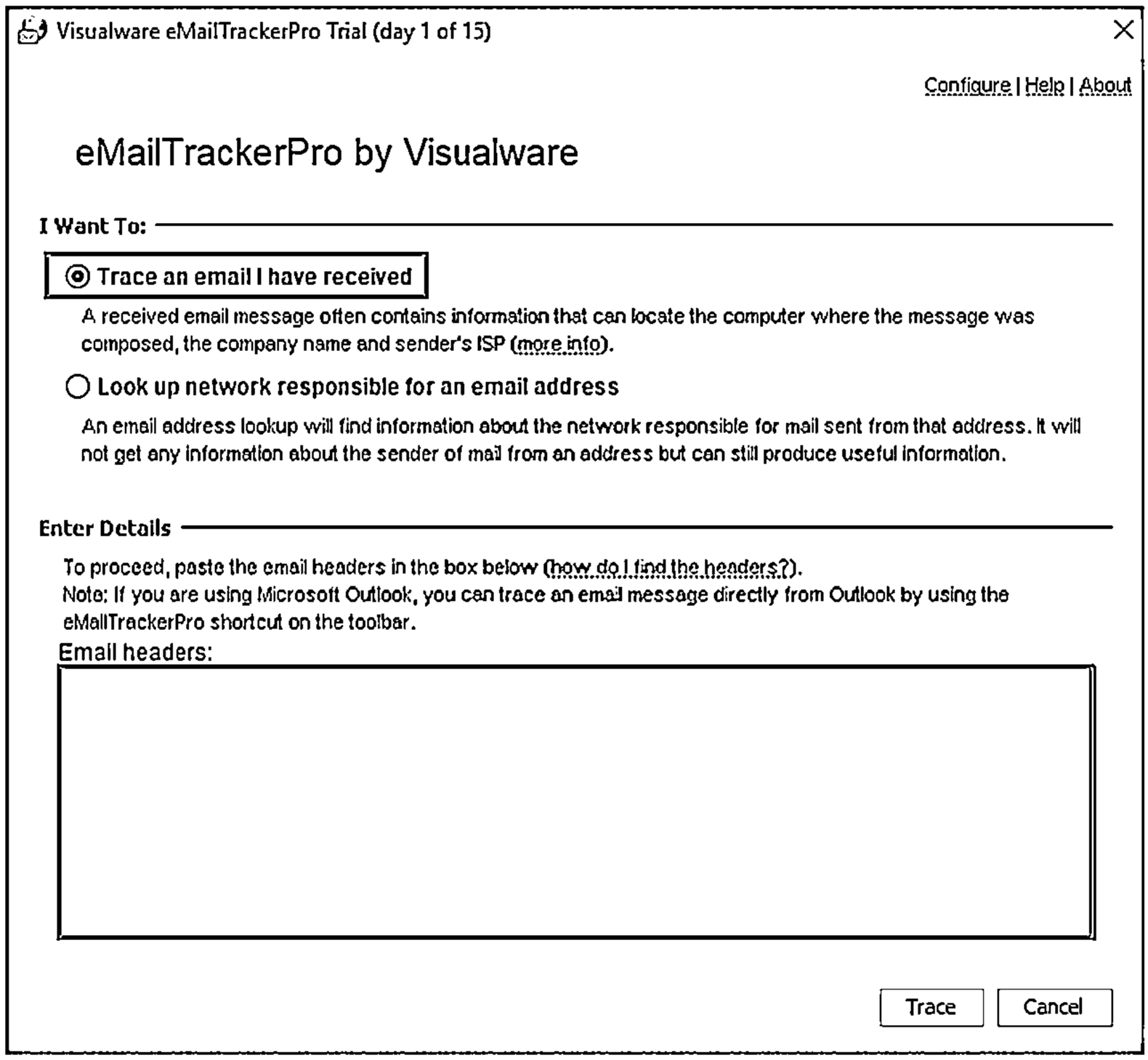


Figure 5.1.5: The eMailTrackerPro entering details window

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

12. For finding email headers, open any web browser and log in to any email account of your choice; from the email inbox, open the message you would like to view headers for.

Note: In **Gmail**, find the email header by following the steps:

- Open an email; click the dots (**More**) icon arrow next to the **Reply** icon at the top-right corner of the message pane.
- Select **Show original** from the list.
- The **Original Message** window appears in a new browser tab with all the details about the email, including the email header.

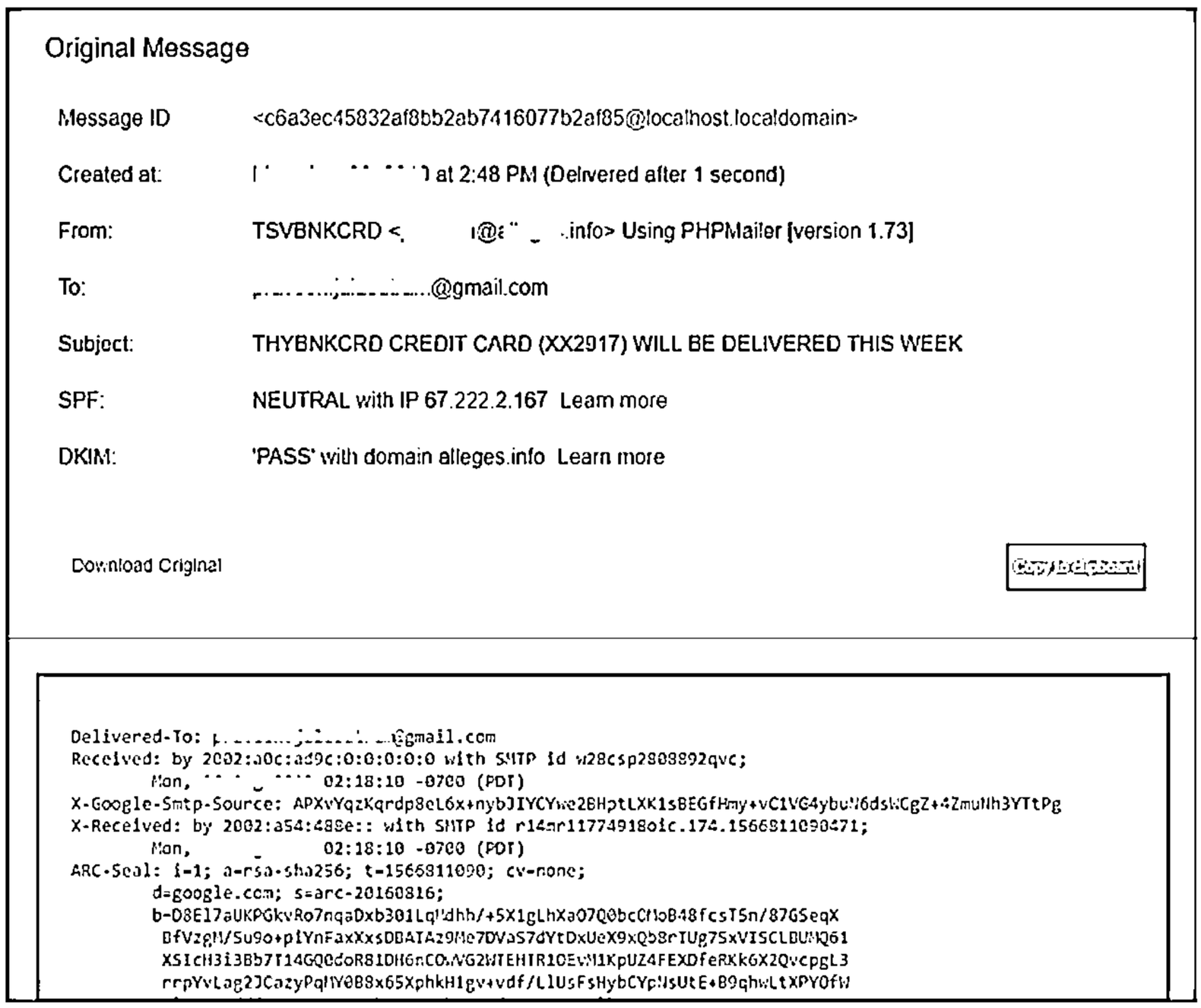


Figure 5.1.6: Sample Email Header in Gmail

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

- Double-click the email to open it in a new window
- Click the **...** (**More actions**) icon present at the right of the message-pane to open message options
- From the options, click **View message details**
- The **message details** window appears with all the details about the email, including the email header

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

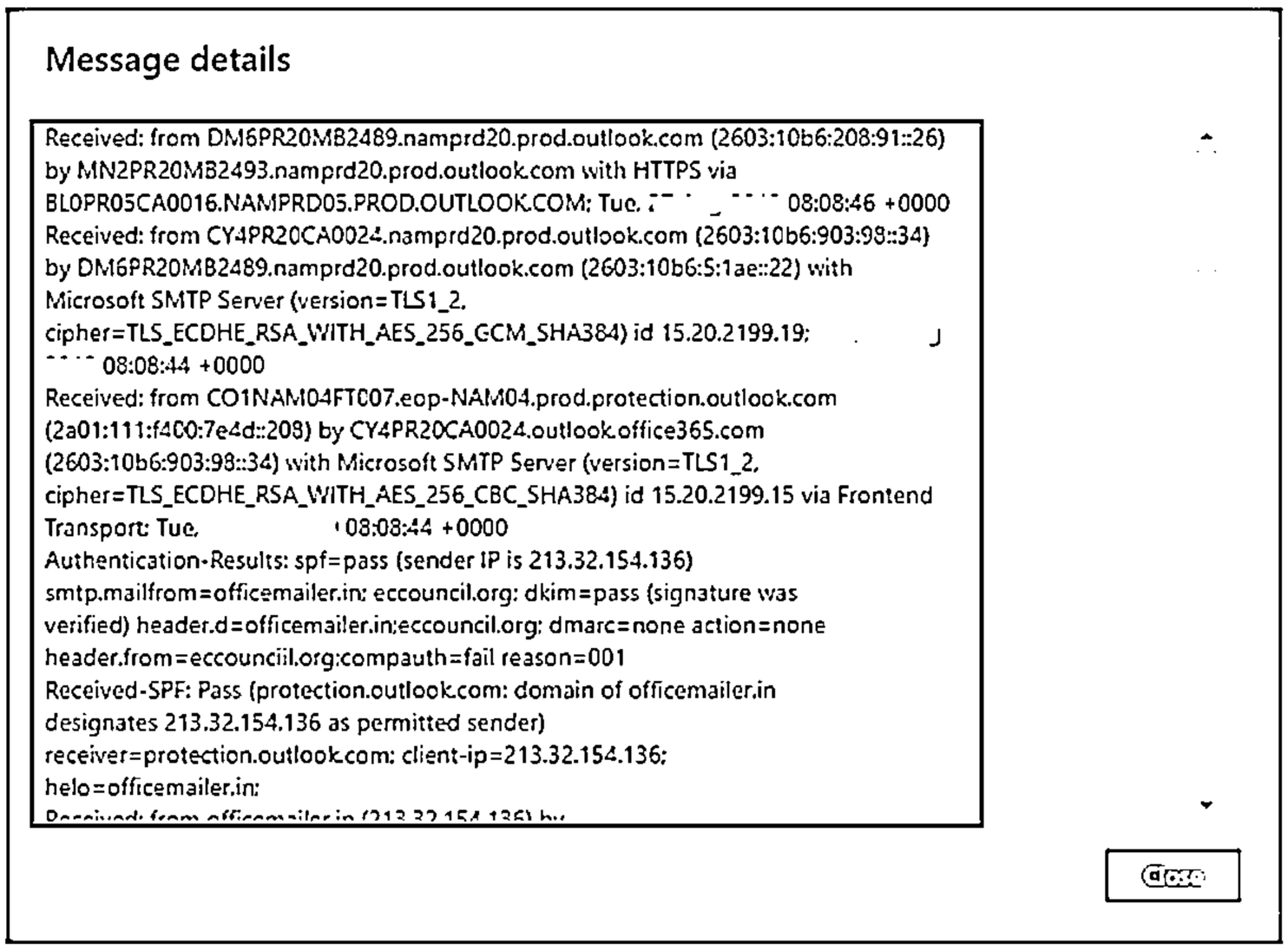


Figure 5.1.7: Sample Email Header in Outlook

13. Copy the entire email header text and paste it into the **Email headers:** field of eMailTrackerPro, and click **Trace**.

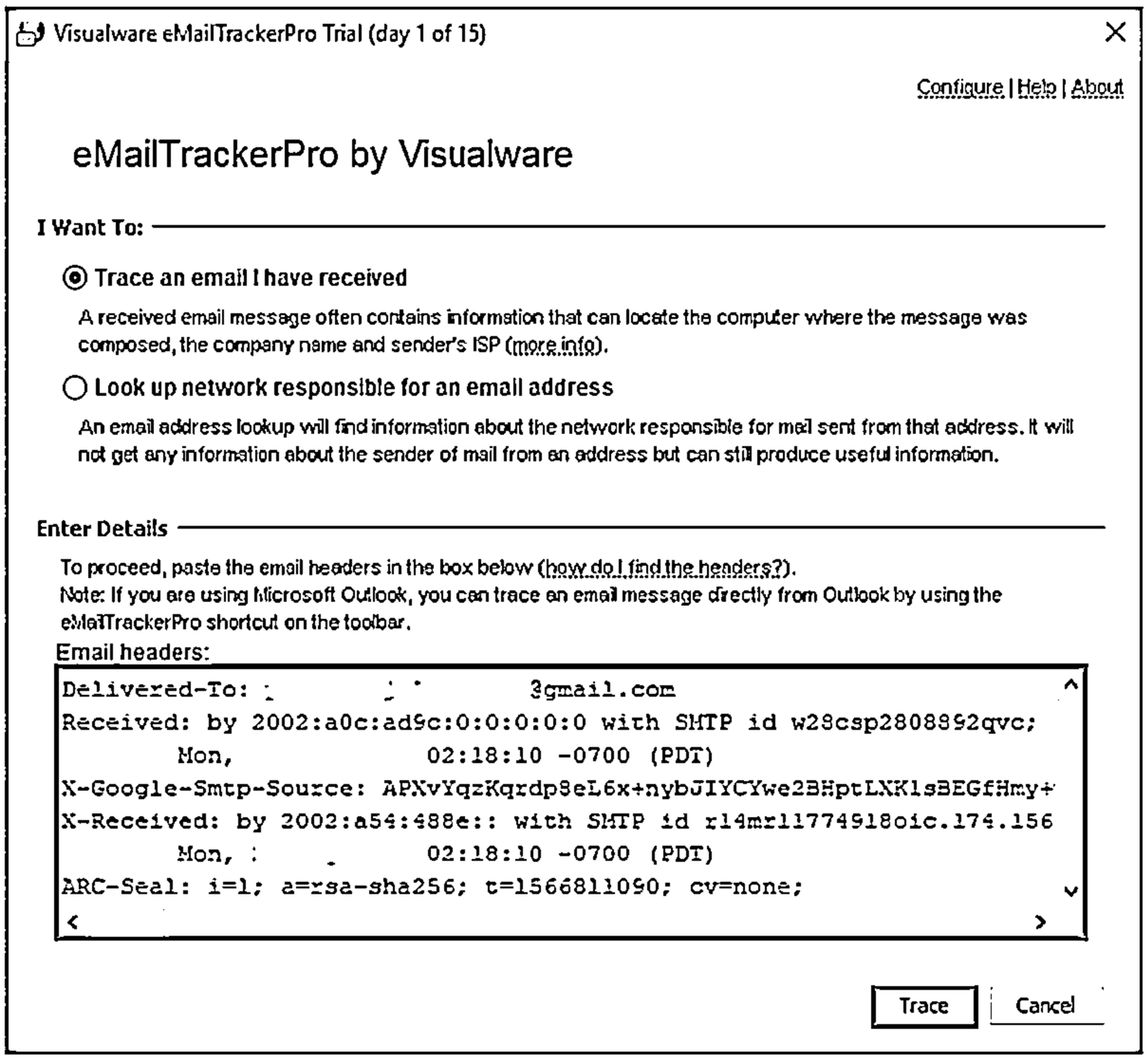


Figure 5.1.8: Email headers and Tracing emails

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

14. The **My Trace Reports** window opens.
15. The email location will be traced in a **Map** (world map GUI). You can also view the summary by selecting **Email Summary** on the right-hand side of the window. The **Table** section right below the Map shows the entire hop in the route, with the **IP** and suspected locations for each hop.

Note: The location and IP addresses may vary according to your email header.

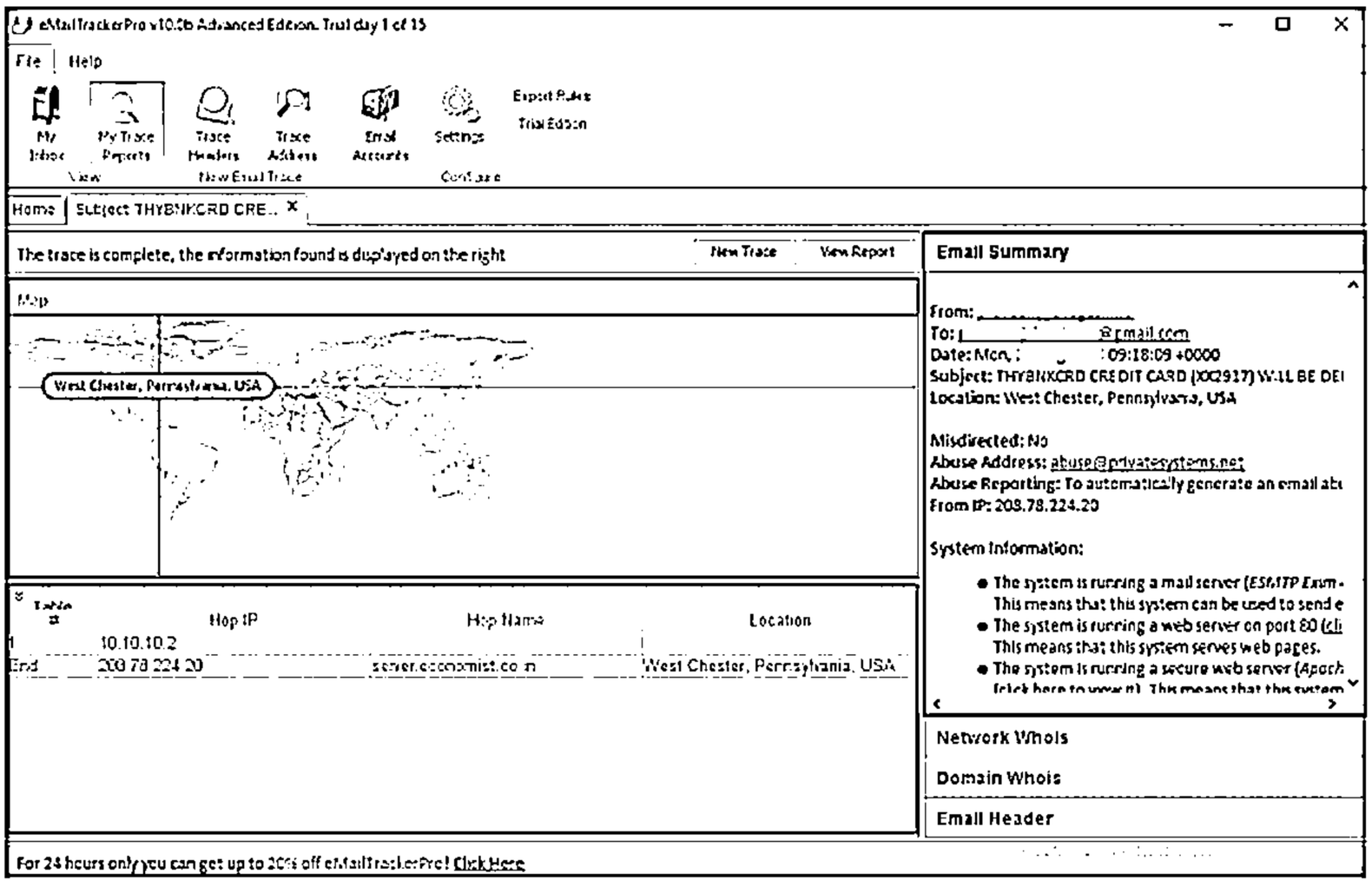


Figure 5.1.9: eMailTrackerPro – Email Trace Report

TASK 1.3

Examine the Report

16. To examine the report, click the **View Report** button above **Map** to view the complete trace report.

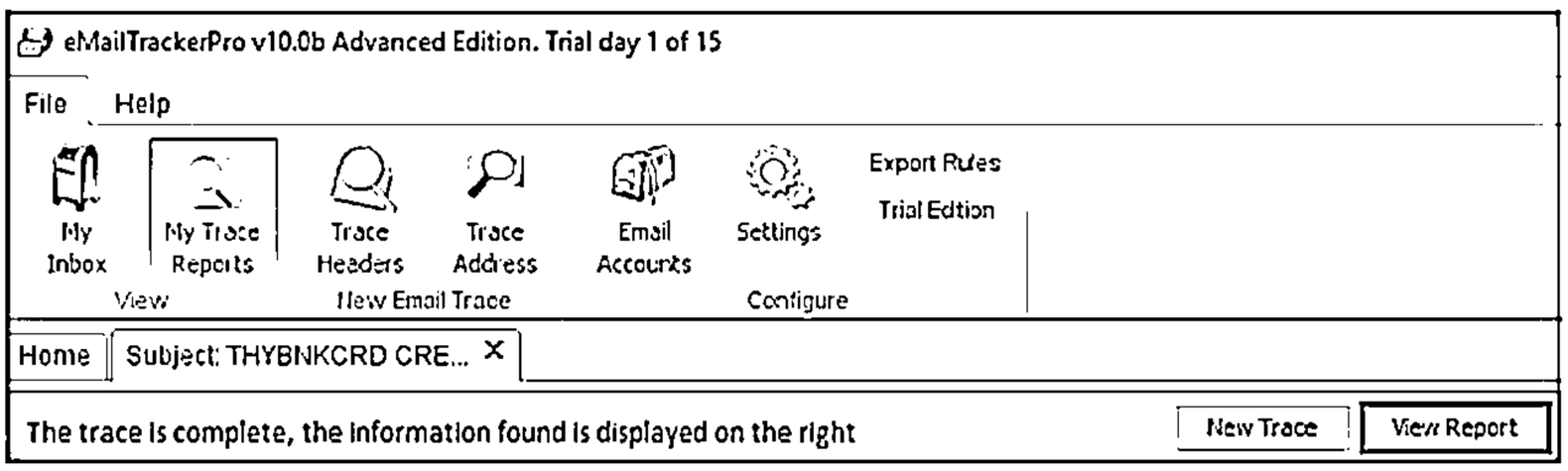


Figure 5.1.10: The eMailTrackerPro – My Trace Reports tab

17. The complete report appears in the default browser.

Note: If a pop-up window appears asking for a browser to be selected, select **Firefox** and click **OK**.

18. Expand each section to view detailed information.

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

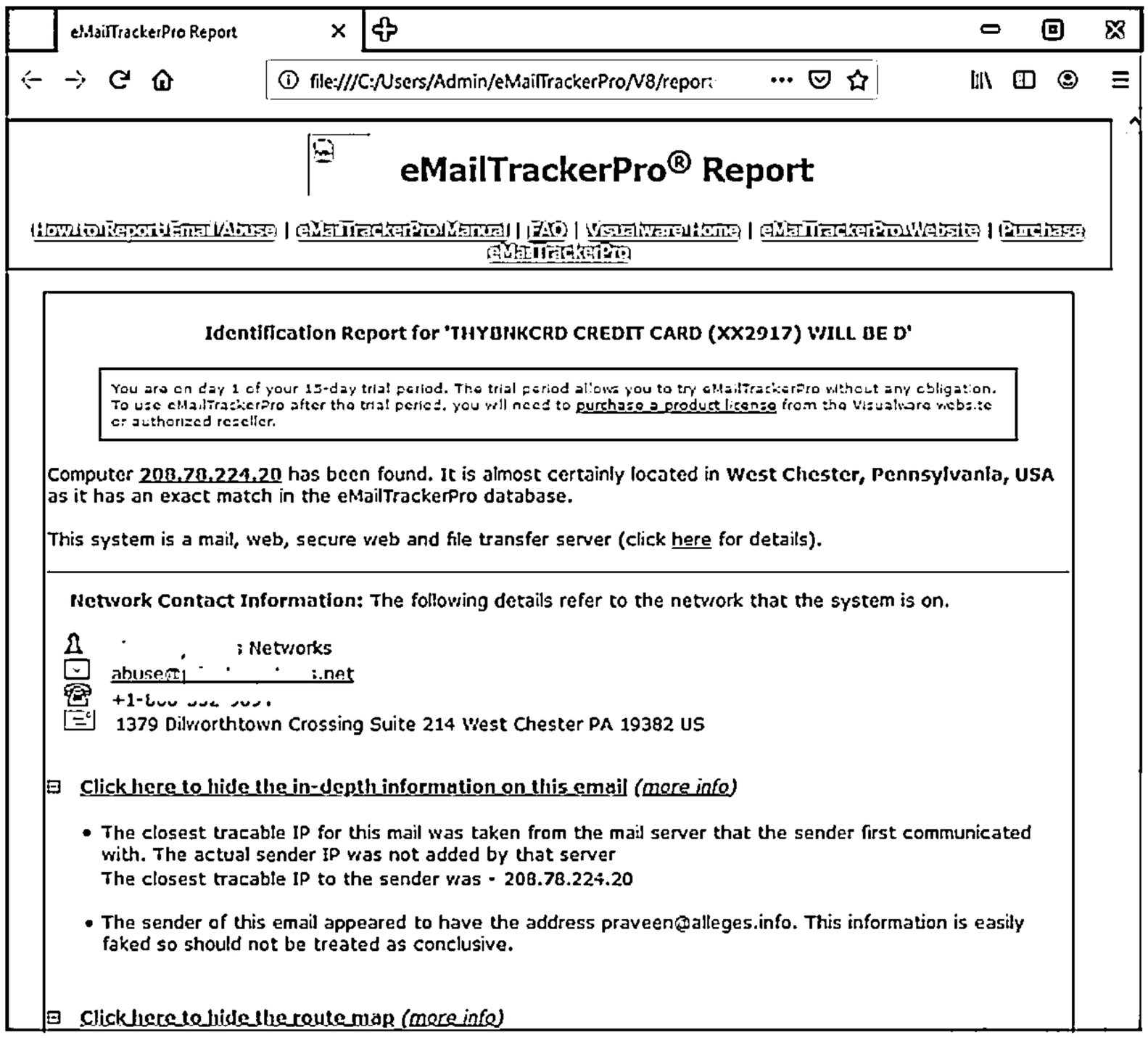


Figure 5.1.11: eMailTrackerPro – detailed information Report

19. This concludes the demonstration of gathering information through analysis of the email header using eMailTrackerPro.
20. Close all open windows and document all the acquired information.
21. Turn off the **Windows 10** virtual machine.

You can also use email tracking tools such as Infoga (https://github.com), Mailtrack (https://mailtrack.io), etc. to track an email and extract target information such as sender identity, mail server, sender's IP address, location, etc.

Lab Analysis

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

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT 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

Perform Whois Footprinting

Whois lookup reveals available information on a hostname, IP address, or domain

ICON KEY

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

Lab Scenario

During the footprinting process, gathering information on the target IP address and domain obtained during previous information gathering steps is important. As a professional ethical hacker or penetration tester, you should be able to perform Whois footprinting on the target; this method provides target domain information such as the owner, its registrar, registration details, name server, contact information, etc. Using this information, you can create a map of the organization's network, perform social engineering attacks, and obtain internal details of the network.

Lab Objectives

- Perform Whois lookup using DomainTools

Lab Environment

To carry out this lab, you need:

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance

- Windows 10 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 5 Minutes

Overview of Whois Footprinting

This lab focuses on how to perform a Whois lookup and analyze the results. Whois is a query and response protocol used for querying databases that store the registered users or assignees of an Internet resource such as a domain name, an IP address block, or an autonomous system. This protocol listens to requests on port 43 (TCP). Regional Internet Registries (RIRs) maintain Whois databases, and contains the personal information of domain owners. For each resource, the Whois database

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

provides text records with information about the resource itself and relevant information of assignees, registrants, and administrative information (creation and expiration dates).

Lab Tasks

TASK 1 Perform Whois Lookup using DomainTools

Here, we will gather target information by performing Whois lookup using DomainTools.

1. Turn on the **Windows 10** virtual machine.
2. Login to the **Windows 10** virtual machine with Username: **Admin** and Password: **Pa$$w0rd**.
3. Open any web browser (here, **Mozilla Firefox**) and navigate to **http://whois.domaintools.com**. In the **Enter a domain or IP address...** search bar, type **www.certifiedhacker.com** and click **Search**.

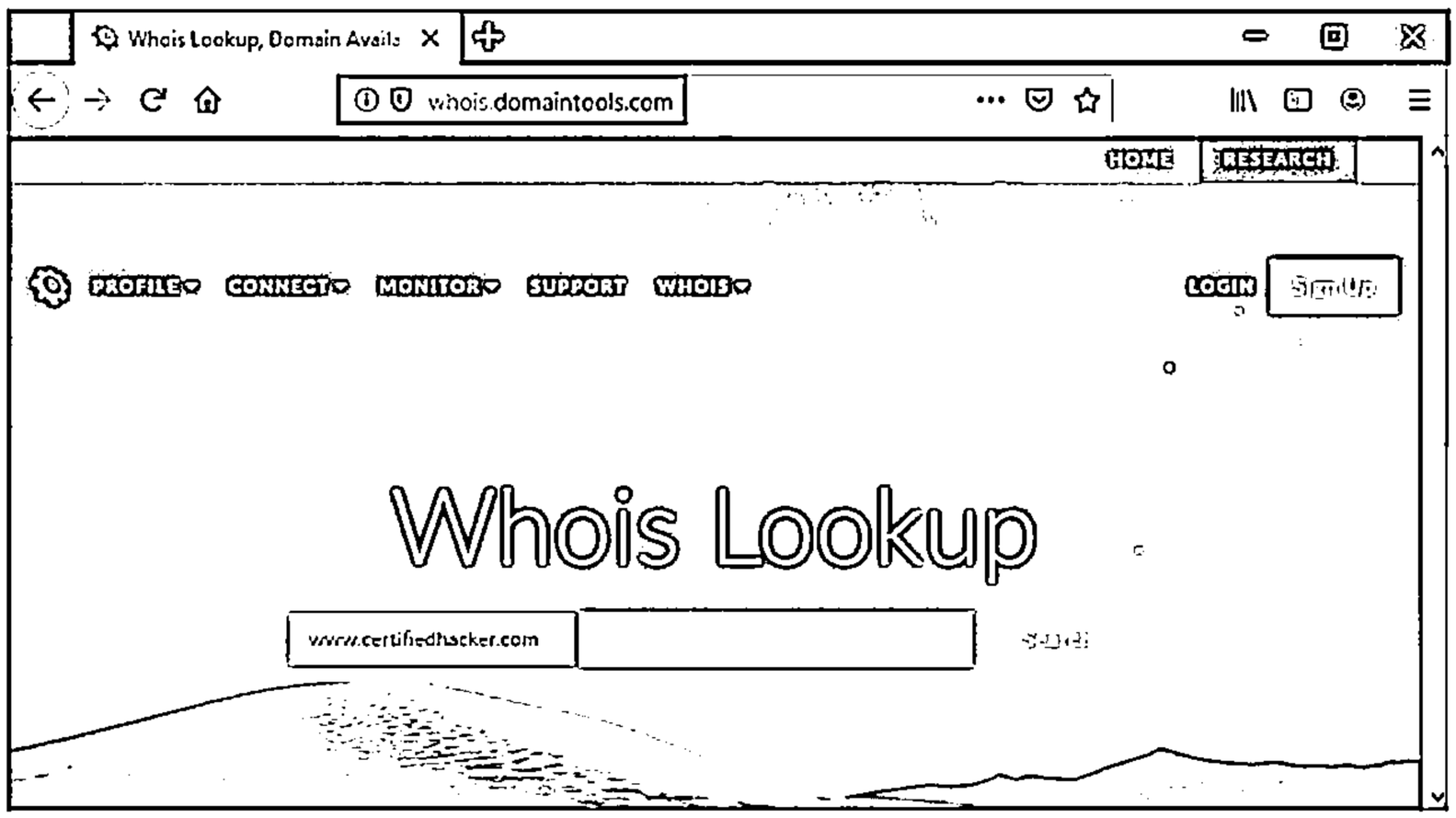


Figure 6.1.1: Whois Domain website

4. This search result reveals the details associated with the URL entered, **www.certifiedhacker.com**, which includes organizational details such as registration details, name servers, IP address, location, etc., as shown in the screenshots.

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

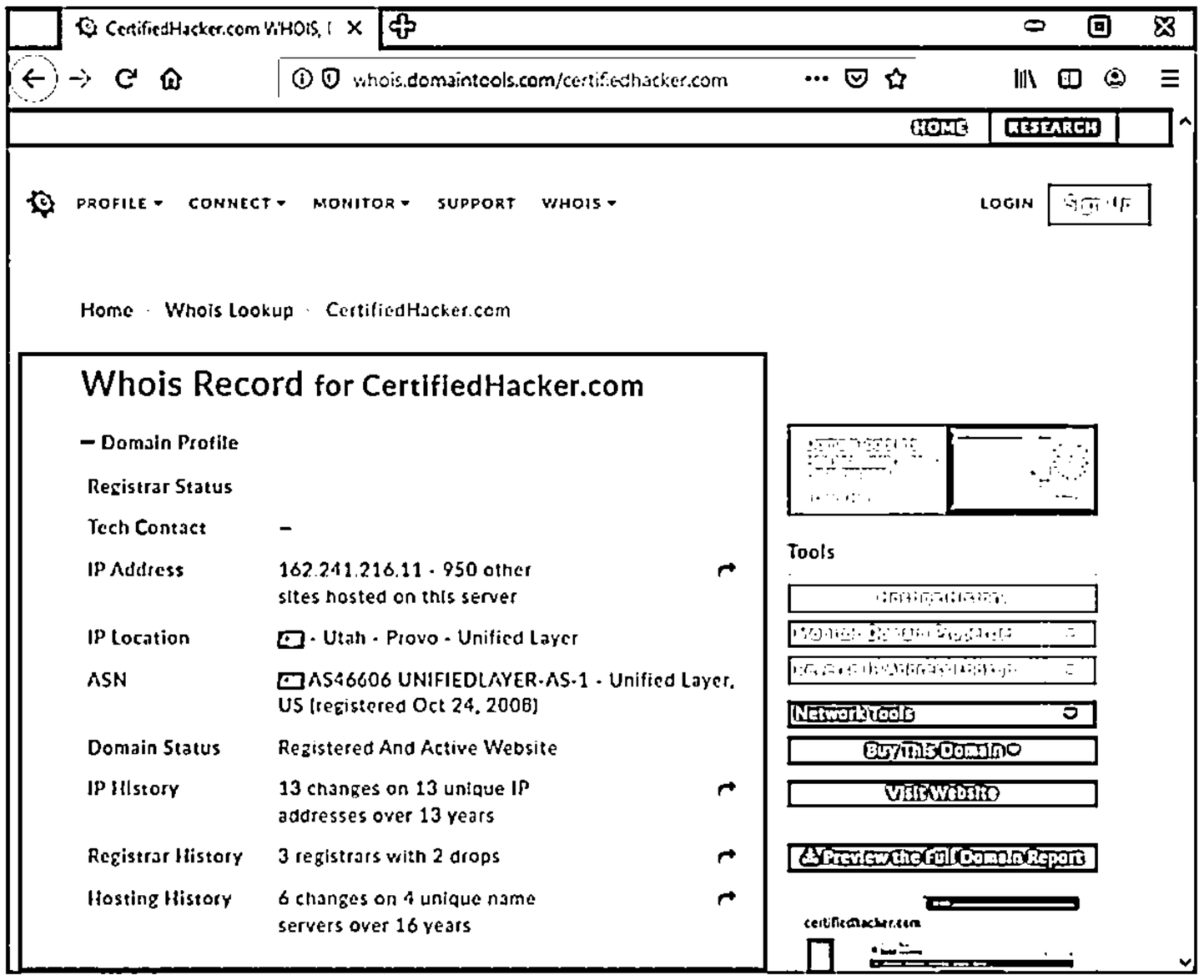


Figure 6.1.2: whois.domaintools.com search results

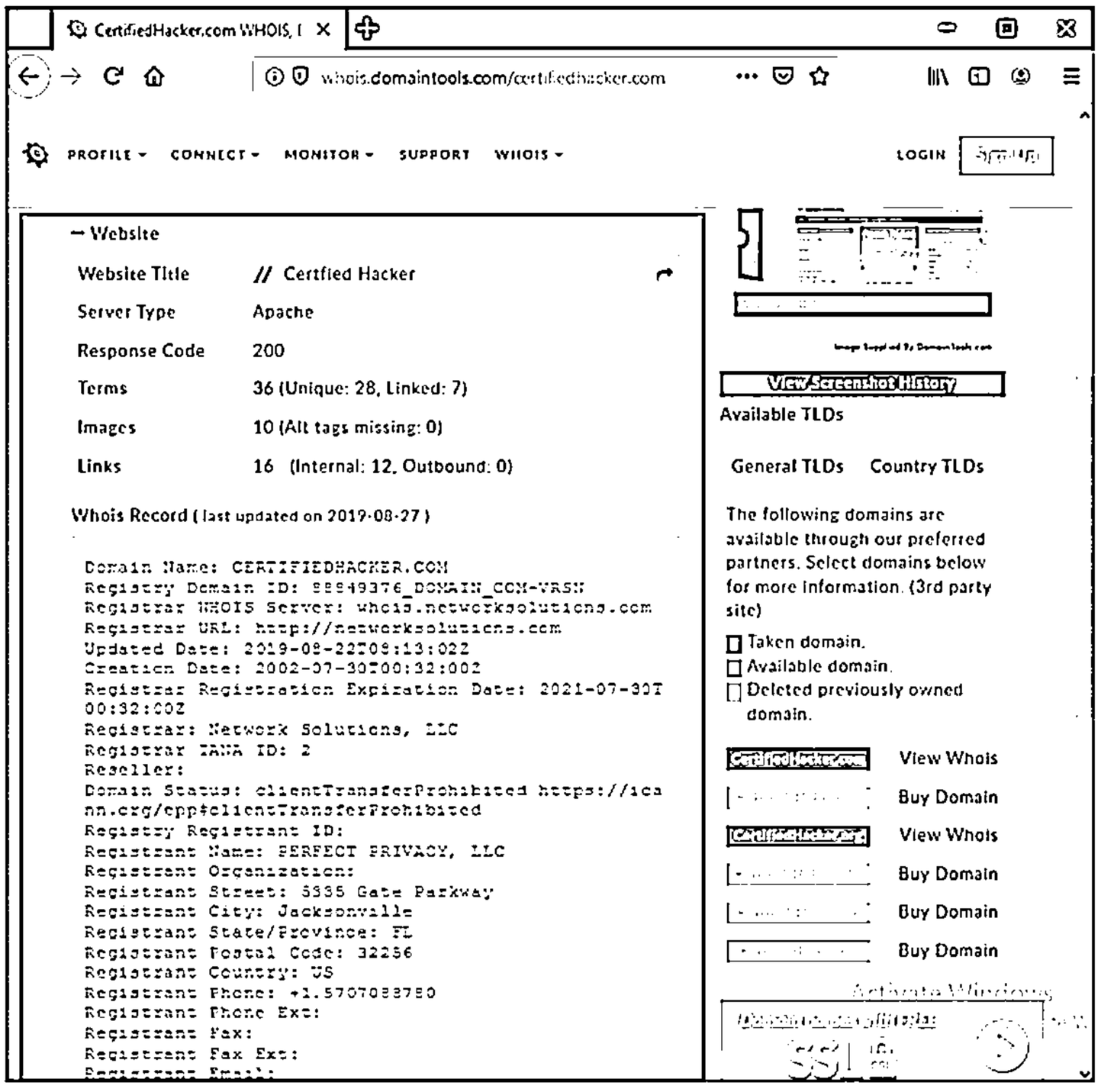


Figure 6.1.3: whois.domaintools.com search results

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

You can also use other Whois lookup tools such as **SmartWhois** (https://www.tamos.com), **Batch IP Converter** (http://www.sabsoft.com), etc. to extract additional target Whois information.

5. This concludes the demonstration of gathering information about a target organization by performing the Whois lookup using DomainTools.
6. Close all open windows and document all the acquired information.
7. Turn off the **Windows 10** virtual machine.

Lab Analysis

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

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT 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

Perform DNS Footprinting

DNS, or Domain Name System, footprinting reveals information about DNS zone data.

ICON KEY

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

Lab Scenario

As a professional ethical hacker, you need to gather the DNS information of a target domain obtained during the previous steps. You need to perform DNS footprinting to gather information about DNS servers, DNS records, and types of servers used by the target organization. DNS zone data include DNS domain names, computer names, IP addresses, domain mail servers, service records, and much more about a target network.

Using this information, you can determine key hosts connected in the network and perform social engineering attacks to gather even more information.

Lab Objectives

- Gather DNS information using nslookup command line utility and online tool
- Perform reverse DNS lookup using reverse IP domain check and DNSRecon

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance

Lab Duration

Time: 10 Minutes

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

Overview of DNS

DNS considered the intermediary source for any Internet communication. The primary function of DNS is to translate a domain name to IP address and vice-versa to enable human-machine-network-internet communications. Since each device has a unique IP address, it is hard for human beings to memorize all IP addresses of the required application. DNS helps in converting the IP address to a more easily understandable domain format, which eases the burden on human beings.

Lab Tasks

TASK 1

Gather DNS Information using nslookup Command Line Utility and Online Tool

Here, we will perform DNS information gathering about target organizations using the nslookup command-line utility and NSLOOKUP web application.

1. Turn on the **Windows 10** virtual machine.
2. Login to the **Windows 10** virtual machine with Username: **Admin** and Password: **Pa$$w0rd**.

TASK 1.1

Launch nslookup Terminal

3. Launch a command prompt, type **nslookup**, and press **Enter**. This displays the default server and its address assigned to the **Windows 10** virtual machine.

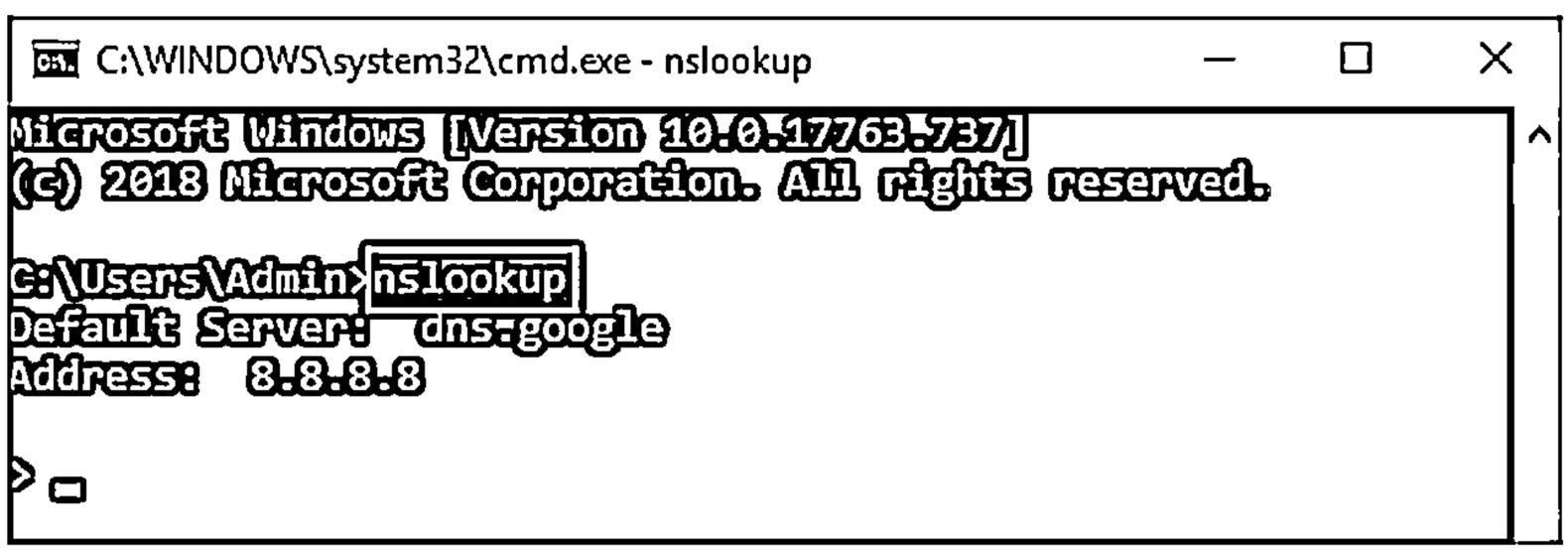


Figure 7.1.1: Command prompt with nslookup command

TASK 1.2

Obtain the IP Address of the Target Domain using nslookup

Note: The DNS server address (8.8.8.8) may differ in your lab environment.

4. In the nslookup **interactive** mode, type **set type=a** and press **Enter**. Setting the type as "**a**" configures nslookup to query for the IP address of a given domain.

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

5. Type the target domain **www.certifiedhacker.com** and press **Enter**. This resolves the IP address and displays the result, as shown in the screenshot.

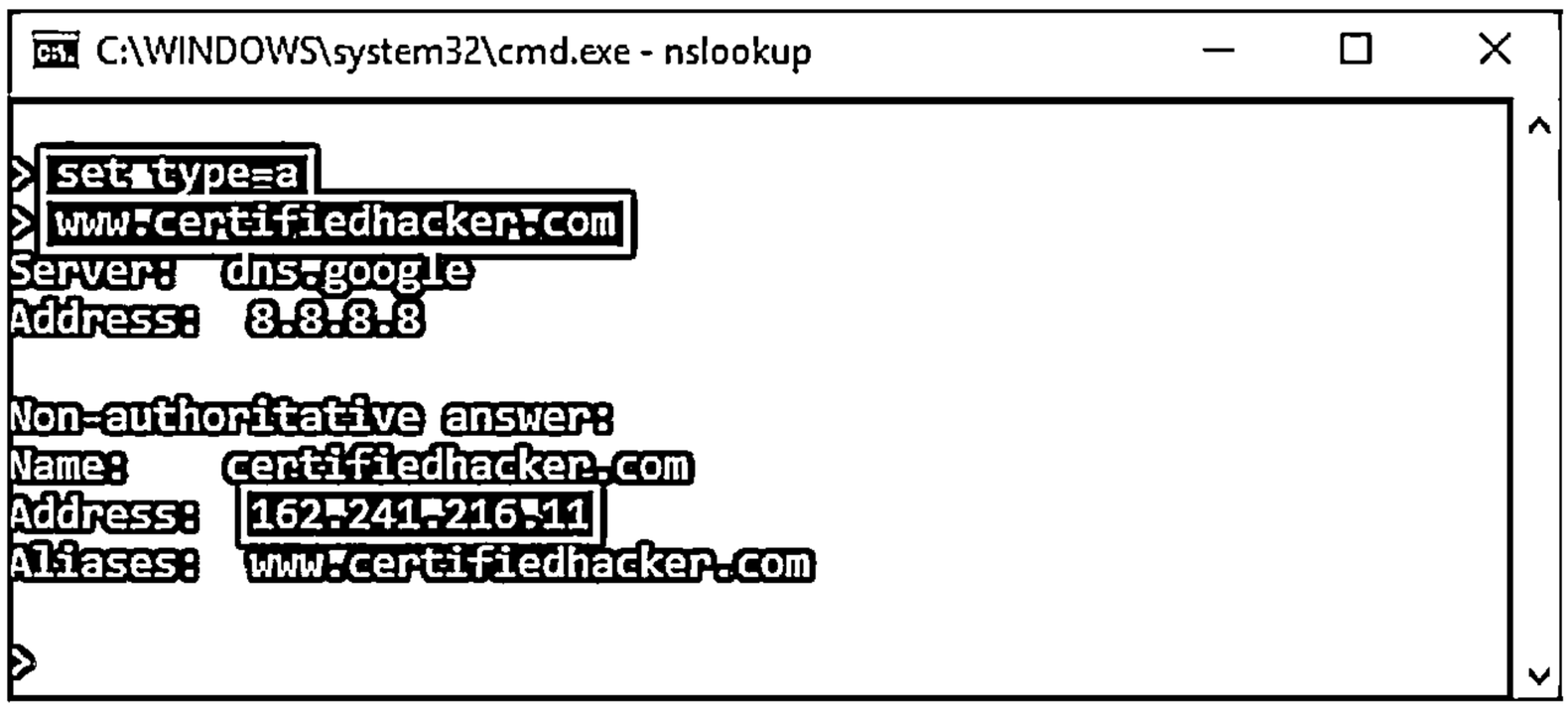


Figure 7.1.2: In nslookup command, set type=a option

nslookup is a network administration command-line utility, generally used for querying the DNS to obtain a domain name or IP address mapping or for any other specific DNS record. This utility is available both as a command-line utility and web application.

6. The first two lines in the result are:

   Server: dns.google and **Address: 8.8.8.8**

   This specifies that the result was directed to the default server hosted on the local machine (**Windows 10**) that resolves your requested domain.

7. Thus, if the response is coming from your local machine's server (Google), but not the server that legitimately hosts the domain **www.certifiedhacker.com**; it is considered to be a non-authoritative answer. Here, the IP address of the target domain **www.certifiedhacker.com** is **162.241.216.11**.

Note: The IP address of the target may differ in your lab environment.

8. Since the result returned is non-authoritative, you need to obtain the domain's authoritative name server.

TASK 1.3

Find Cname

9. Type **set type=cname** and press **Enter**. The CNAME lookup is done directly against the domain's authoritative name server and lists the CNAME records for a domain.
10. Type **certifiedhacker.com** and press **Enter**.
11. This returns the domain's authoritative name server (**ns1.bluehost.com**), along with the mail server address (**dnsadmin.box5331.bluehost.com**), as shown in the screenshot.

Note: The results may differ in your lab environment.

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

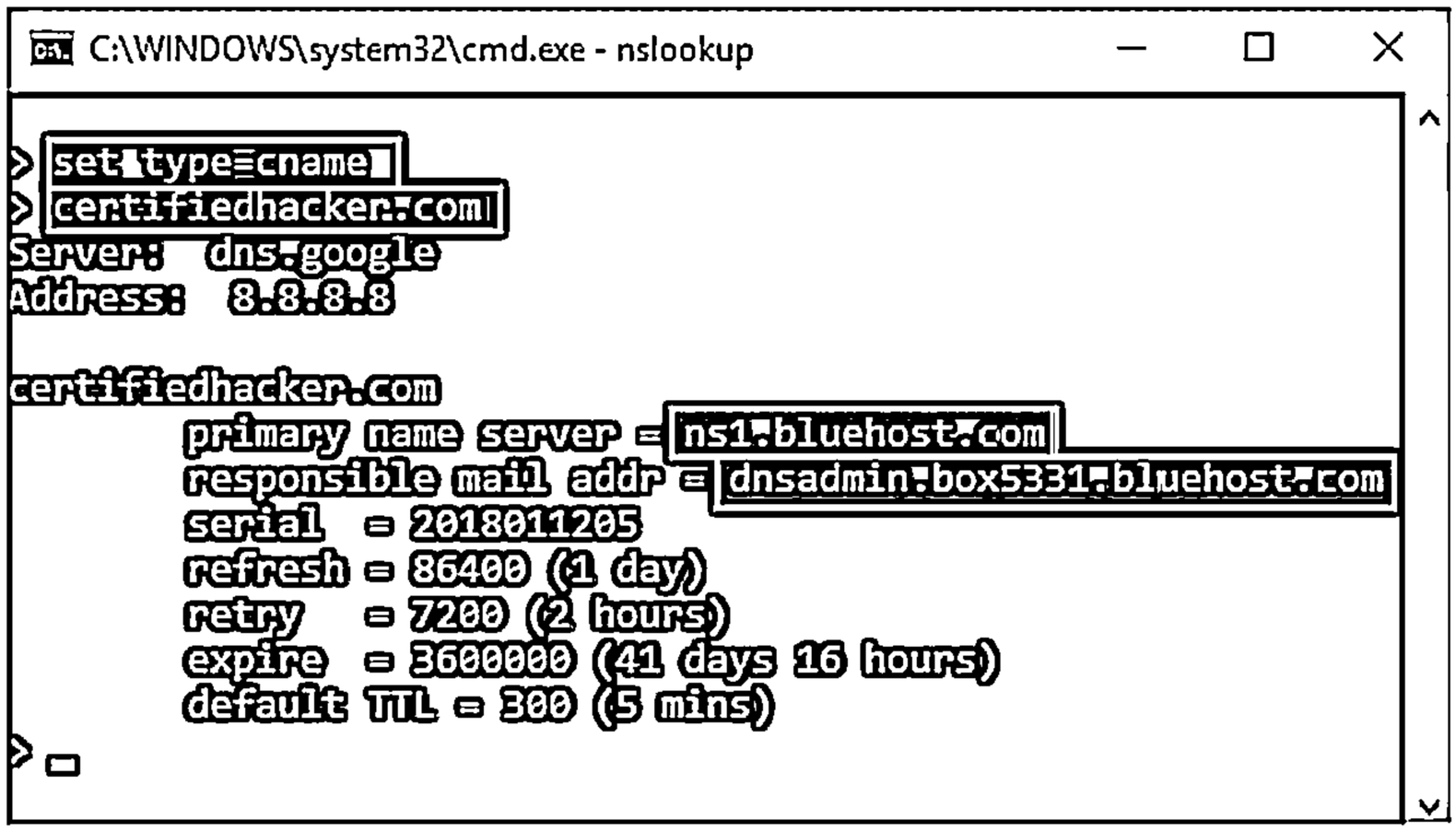


Figure 7.1.3: In nslookup command, set type=cname option

12. Since you have obtained the authoritative name server, you will need to determine the IP address of the name server.

TASK 1.4

Obtain the IP Address of the Primary Name Server

13. Issue the command **set type=a** and press **Enter**.
14. Type **ns1.bluehost.com** (or the primary name server that is displayed in your lab environment) and press **Enter**. This returns the IP address of the server, as shown in the screenshot.

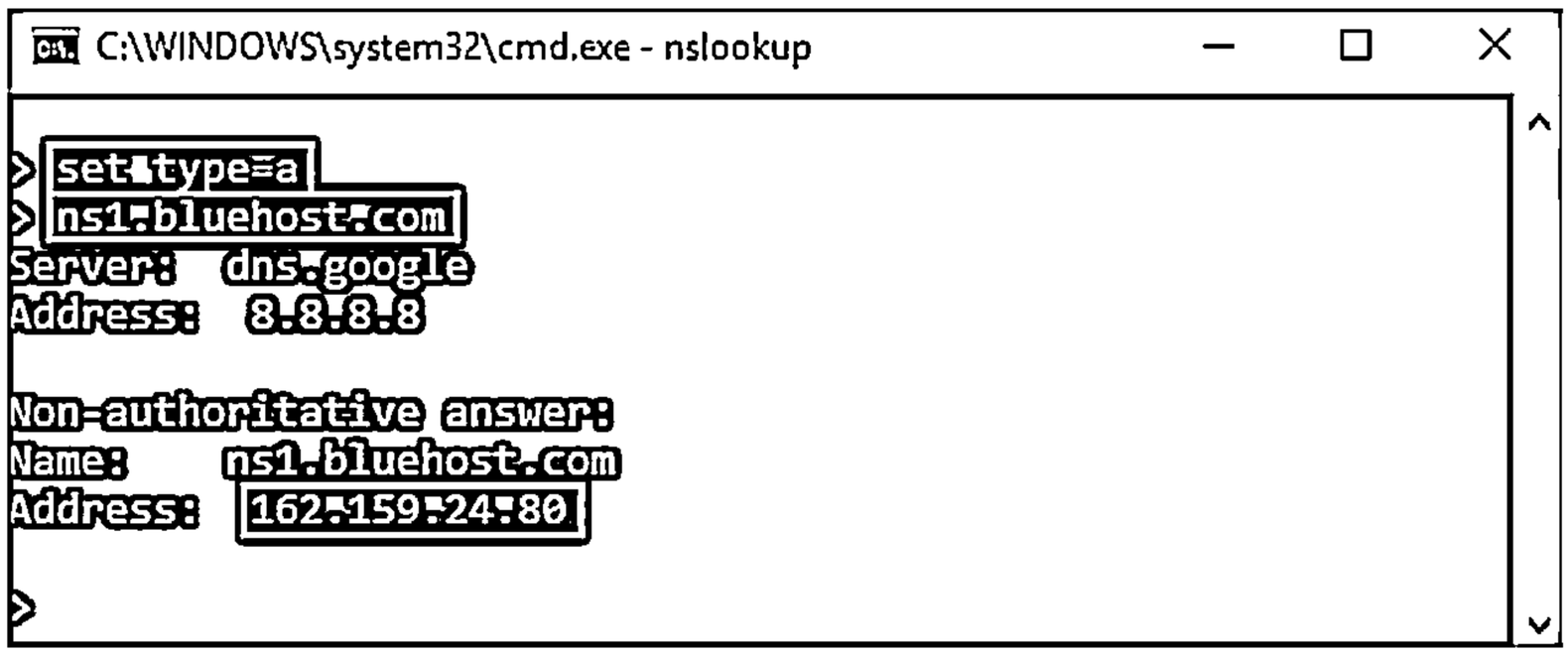


Figure 7.1.4: Screenshot showing returns the IP address of the server

15. The authoritative name server stores the records associated with the domain. So, if an attacker can determine the authoritative name server (primary name server) and obtain its associated IP address, he/she might attempt to exploit the server to perform attacks such as DoS, DDoS, URL Redirection, etc.
16. You can also perform the same operations using the NSLOOKUP online tool. Conduct a series of queries and review the information to gain familiarity with the NSLOOKUP tool and gather information.
17. Now, we will use an online tool NSLOOKUP to gather DNS information about the target domain.

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

TASK 1.5

Perform DNS Footprinting using NSLOOKUP Online Utility

18. Open any web browser (here, **Mozilla Firefox**) and navigate to **http://www.kloth.net/services/nslookup.php**.
19. Once the site opens, in the **Domain:** field, enter **certifiedhacker.com**. Set the **Query:** field to default [**A (IPv4 address)**] and click the **Look it up** button to review the results that are displayed.

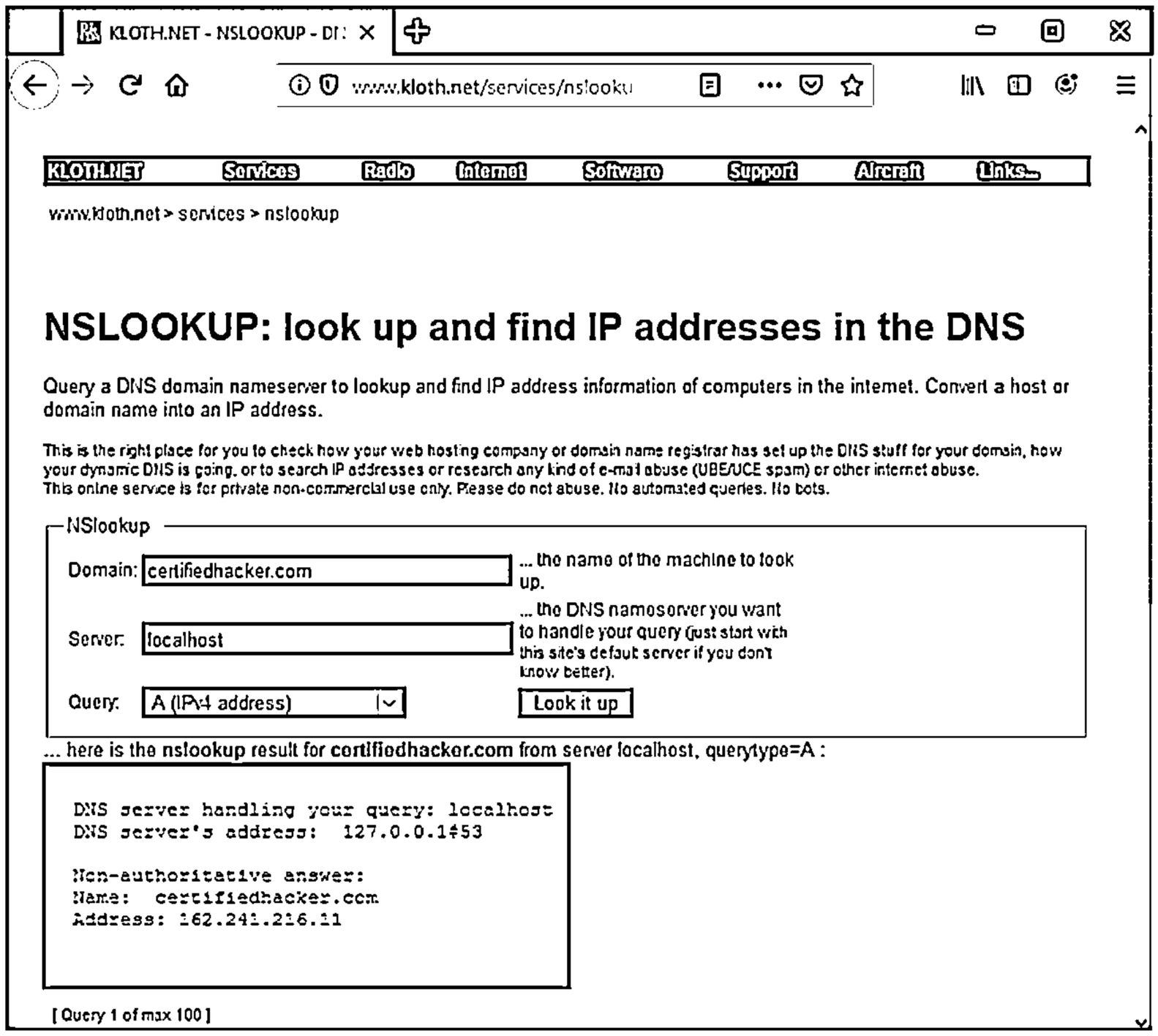


Figure 7.1.5: NSLOOKUP search page

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

20. In the **Query:** field, click the drop-down arrow and check the different options that are available, as shown in the screenshot.

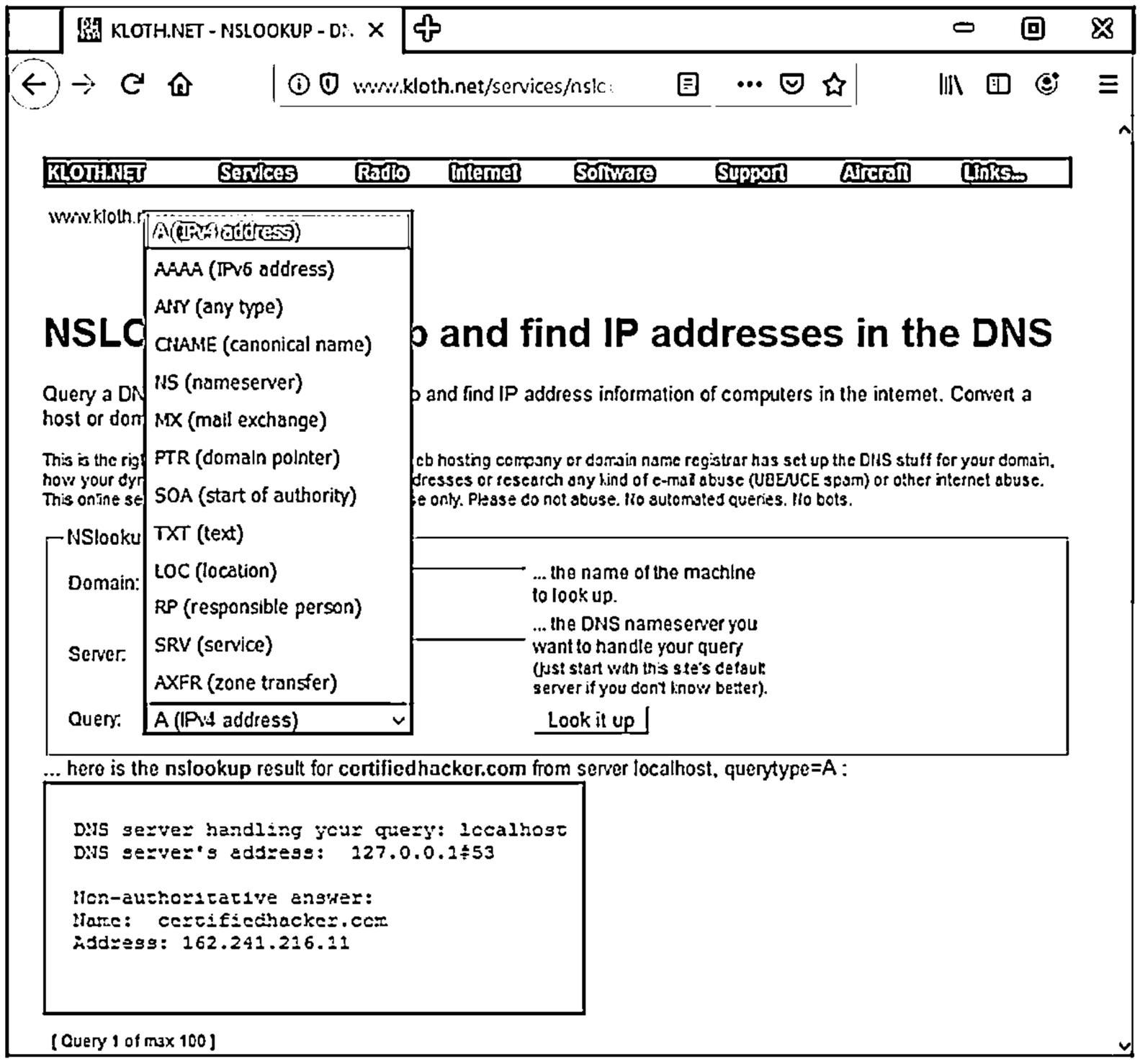


Figure 7.1.6: Screenshot showing different options for the query

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

21. As you can see, there is an option for **AAAA (IPv6 address)**; select that and click **Look it up**. Perform queries related to this, since there are attacks that are possible over IPv6 networks as well.

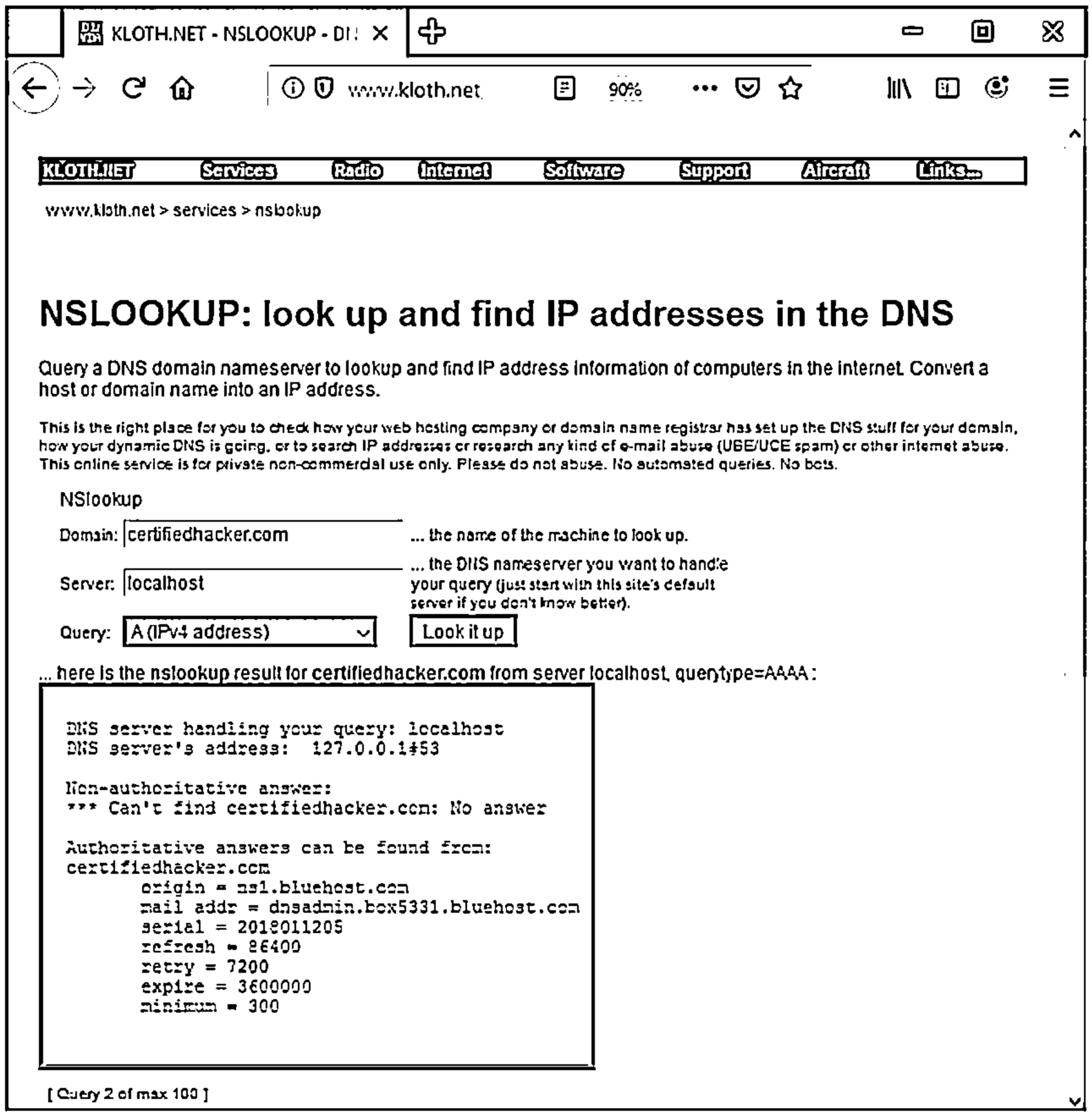


Figure 7.1.7: Screenshot showing IPv6 query results

You can also use DNS lookup tools such as **Professional Toolset** (https://tools.dnsstuff.com), **DNS Records** (https://network-tools.com), etc. to extract additional target DNS information.

22. This concludes the demonstration of DNS information gathering using the nslookup command-line utility and NSLOOKUP online tool.
23. Close all open windows and document all the acquired information.

TASK 2

Perform Reverse DNS Lookup using Reverse IP Domain Check and DNSRecon

DNS lookup is used for finding the IP addresses for a given domain name, and the reverse DNS operation is performed to obtain the domain name of a given IP address.

Here, we will perform reverse DNS lookup using you get signal's Reverse IP Domain Check tool to find the other domains/sites that share the same web server as our target server.

Here, we will also perform a reverse DNS lookup using DNSRecon on IP range in an attempt to locate a DNS PTR record for those IP addresses.

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

TASK 2.1

Perform Reverse DNS Lookup using Reverse IP Domain Check

1. In the **Windows 10** virtual machine, open any web browser (here, **Mozilla Firefox**) and navigate to **https://www.yougetsignal.com**. On the website, click **Reverse IP Domain Check**.

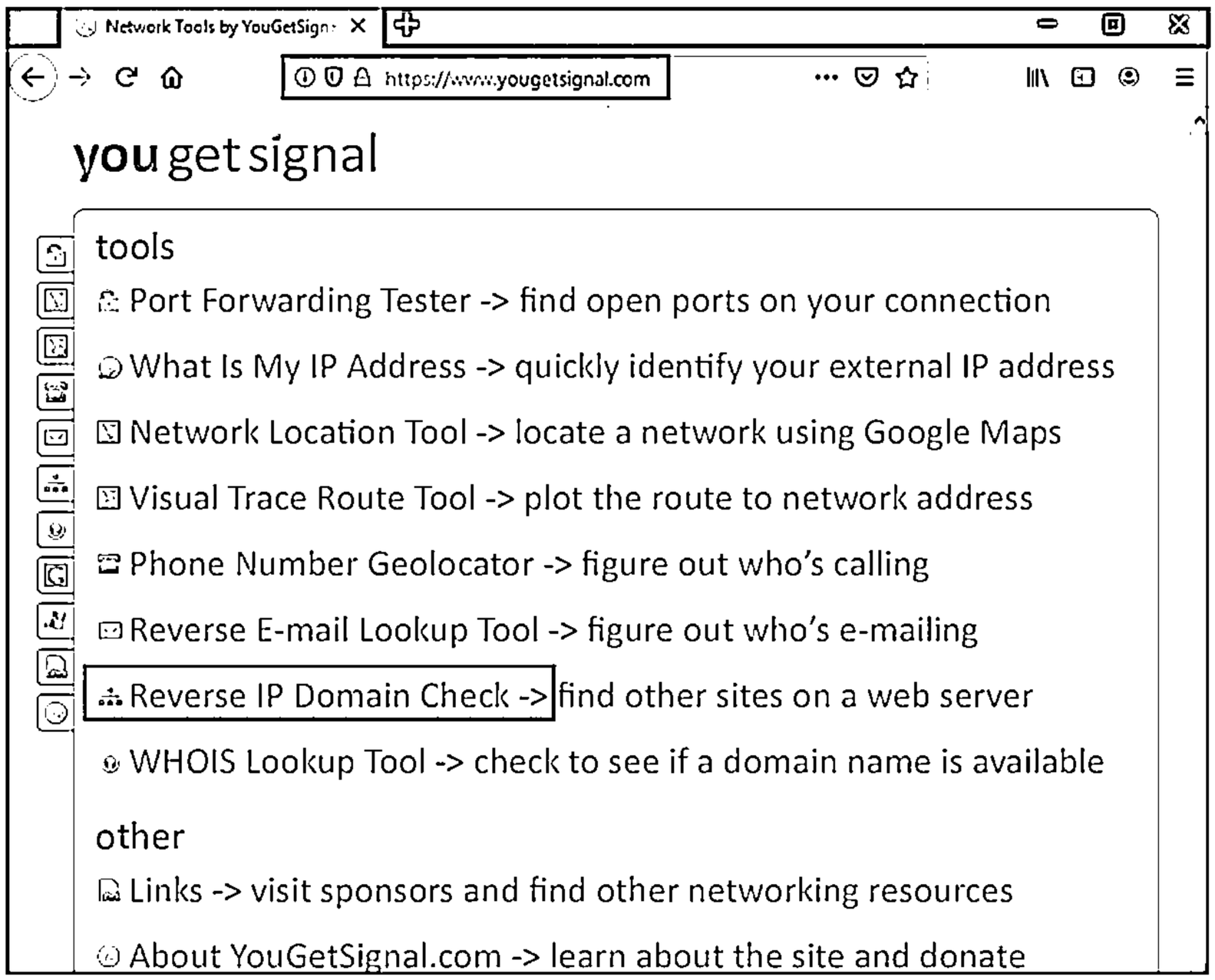


Figure 7.2.1: You Get Signal website

2. On the **Reverse IP Domain Check** page, enter **www.certifiedhacker.com** in the **Remote Address** field and click **Check** to find other domains/sites hosted on a certifiedhacker.com web server. You will get the list of domains/sites hosted on the same server as **www.certifiedhacker.com,** as shown in the screenshot

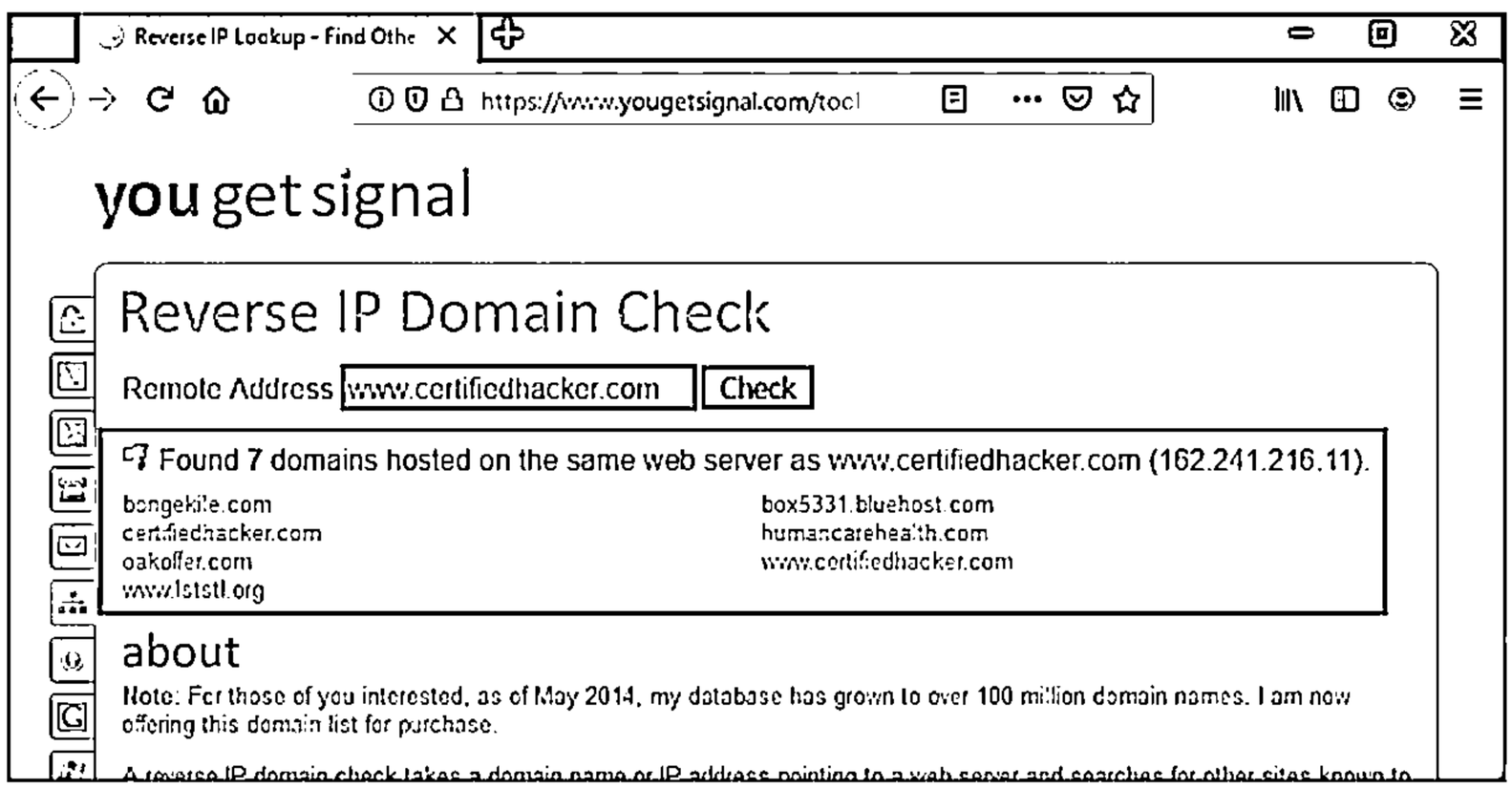


Figure 7.2.2: Reverse IP Domain Check

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

TASK 2.2

Perform Reverse DNS Lookup using DNSRecon

3. Close all open windows, document all the acquired information, and then turn off the **Windows 10** virtual machine
4. Turn on **Parrot Security** virtual machine.
5. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

6. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
7. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
8. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

9. Now, type **cd** and press **Enter** to jump to the root directory.

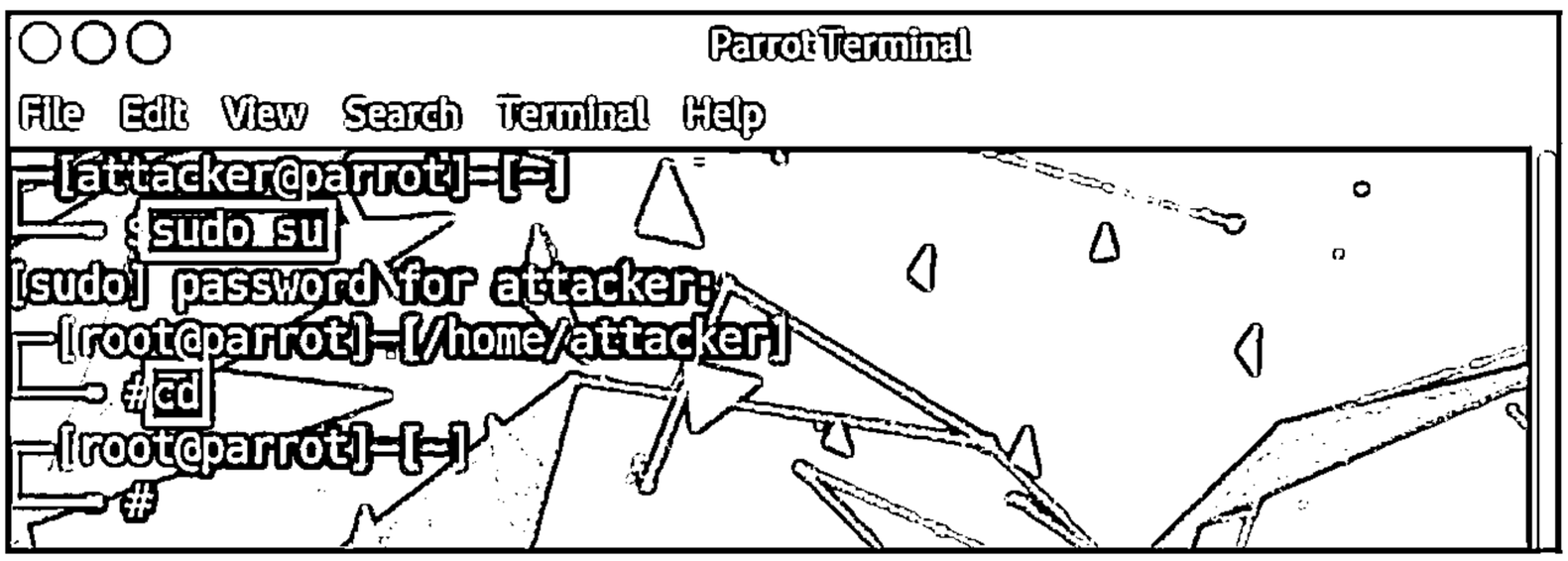


Figure 7.2.3: Running the programs as a root user

10. In the **Parrot Terminal** window, type **dnsrecon -r 162.241.216.0-162.241.216.255** and press **Enter** to locate a DNS PTR record for IP addresses between 162.241.216.0 - 162.241.216.255.

Note: Here, we will use the IP address range, which includes the IP address of our target, that is, the certifiedhacker.com domain (162.241.216.11), which we acquired in the previous steps.

Note: -r option specifies the range of IP addresses (first-last) for reverse lookup brute force.

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

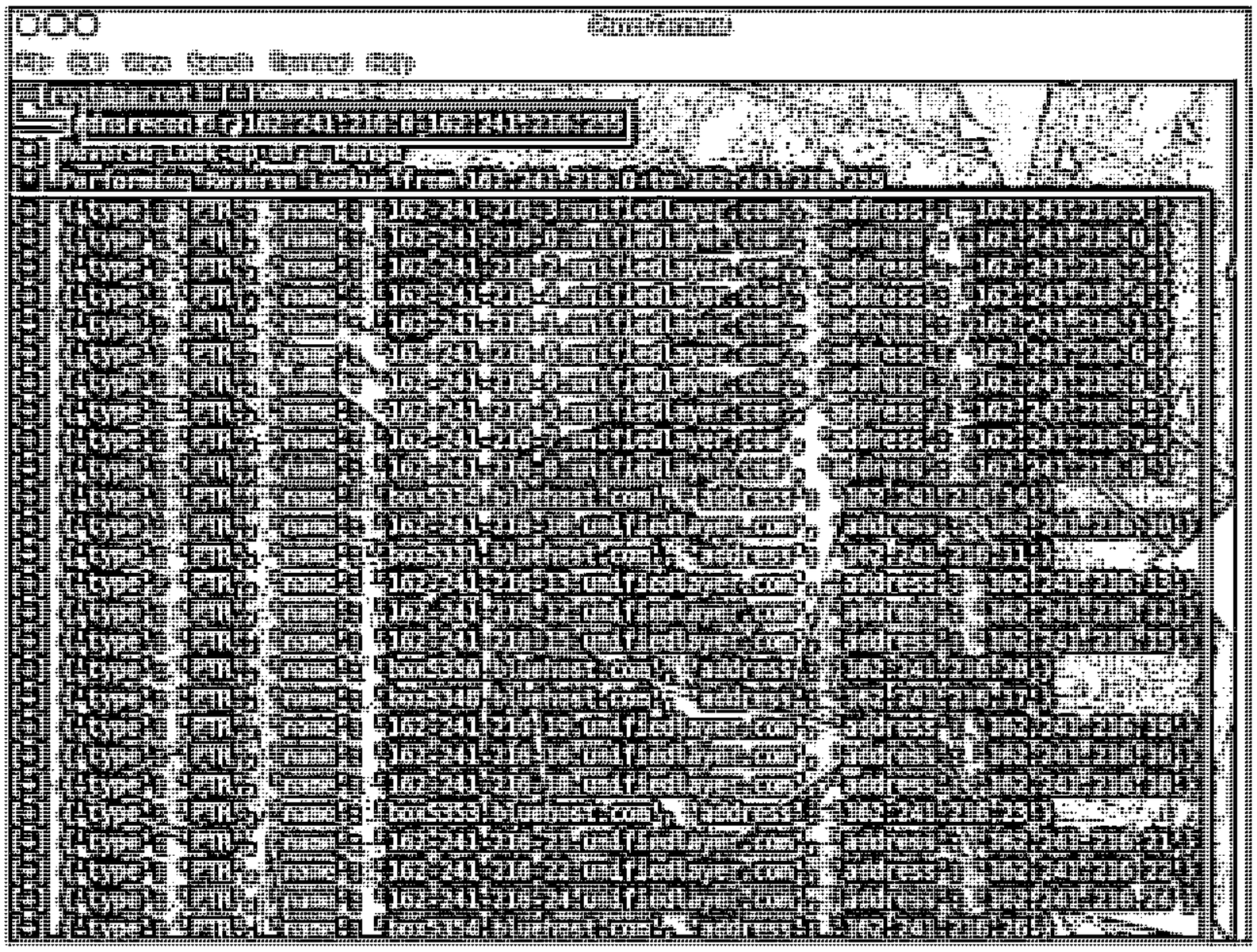


Figure 7.2.4: Reverse IP Domain Check using DNSRecon

11. This concludes the demonstration of gathering information about a target organization by performing reverse DNS lookup using "you get signal's" Reverse IP Domain Check and DNSRecon tool.
12. Close all open windows and document all the acquired information.
13. Turn off the **Parrot Security** virtual machine.

Lab Analysis

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

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT 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

Perform Network Footprinting

Network footprinting is a process of gathering network-related information of a target organization.

ICON KEY

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

Lab Scenario

With the IP address, hostname, and domain obtained in the previous information gathering steps, as a professional ethical hacker, your next task is to perform network footprinting to gather the network-related information of a target organization such as network range, traceroute, TTL values, etc. This information will help you to create a map of the target network and perform a man-in-the-middle attack.

Lab Objectives

- Locate the network range
- Perform network tracerouting in Windows and Linux Machines
- Perform advanced network route tracing using Path Analyzer Pro

Lab Environment

To carry out this lab, you need:

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance

- Windows 10 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- Path Analyzer Pro located at **E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance\Traceroute Tools\Path Analyzer Pro**
- You can also download the latest version of Path Analyzer Pro from its official website. If you decide to download the latest version, the 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: 15 Minutes

Overview of Network Footprinting

Network footprinting is a process of accumulating data regarding a specific network environment. It enables ethical hackers to draw a network diagram and analyze the target network in more detail to perform advanced attacks.

Lab Tasks

TASK 1 Locate the Network Range

Here, we will locate the network range using the ARIN Whois database search tool.

Network range information assists in creating a map of the target network. Using the network range, you can gather information about how the network is structured and which machines in the networks are alive. Further, it also helps to identify the network topology and access the control device and operating system used in the target network.

1. Turn on the **Windows 10** virtual machine.
2. Login to the **Windows 10** virtual machine with Username: **Admin** and Password: **Pa$$w0rd**.
3. Open any web browser (here, **Mozilla Firefox**) and navigate to **https://www.arin.net/about/welcome/region**.
4. In the search bar, enter the IP address of the target organization (here, the target organization is **certifiedhacker.com**, whose IP is **162.241.216.11**), and then click the **Search** button.

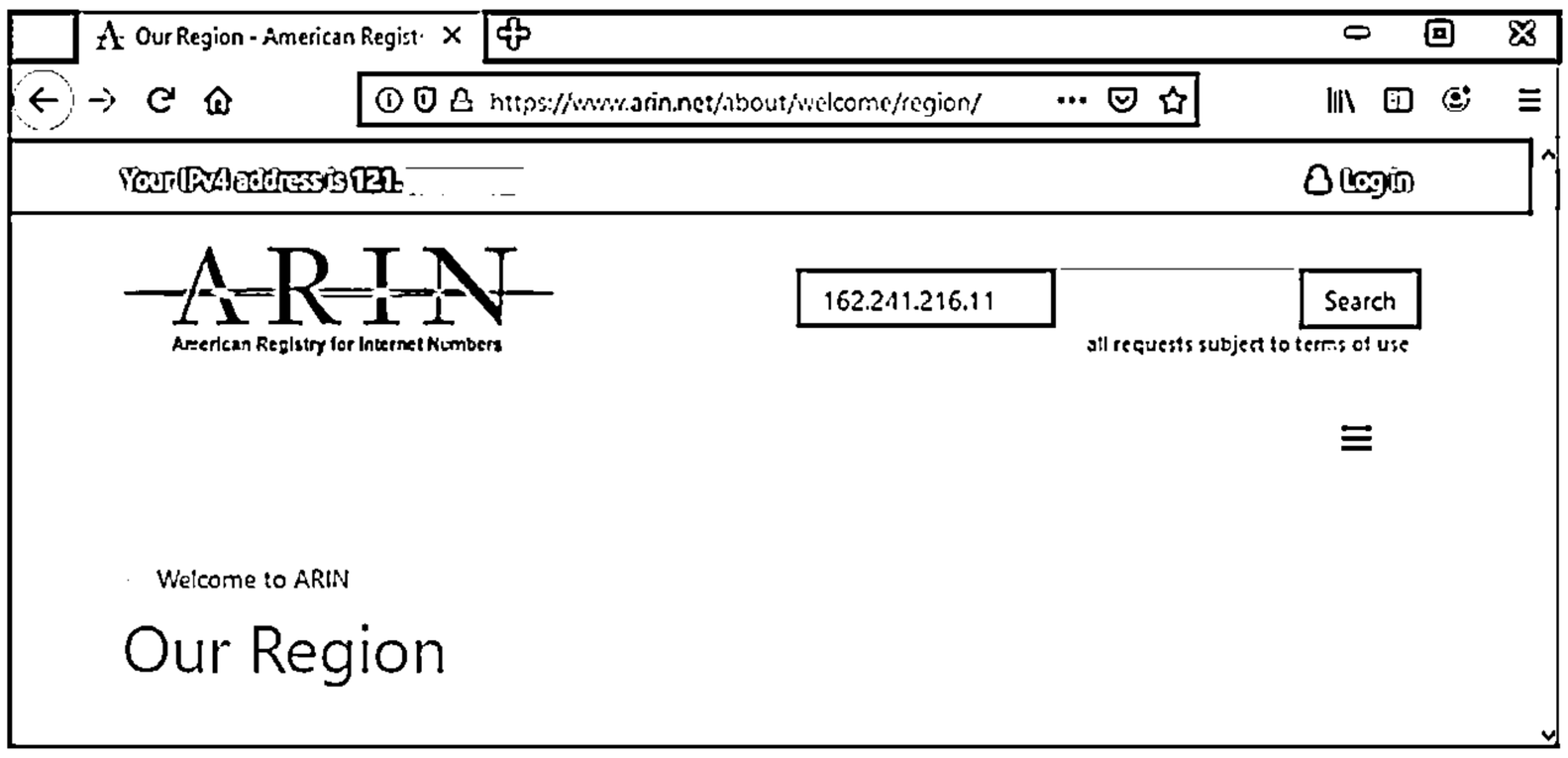


Figure 8.1.1: Entering the target IP address in the ARIN whois database search tool

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

5. You will get the information about the network range along with the other information such as network type, registration information, etc.

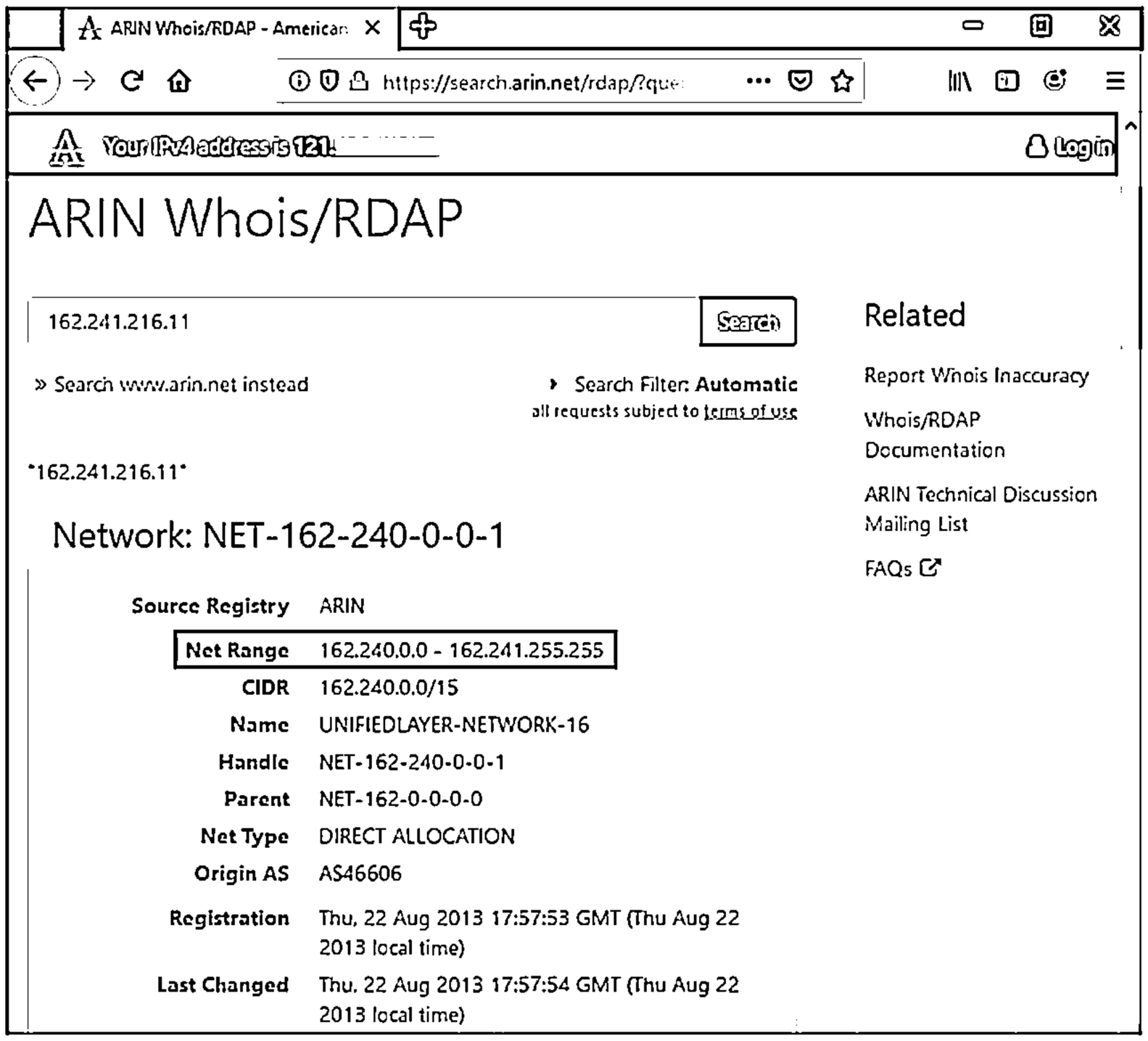


Figure 8.1.2: Network range information of the target organization

6. This concludes the demonstration of locating network range using the ARIN Whois database search tool.
7. Close all open windows and document all the acquired information.

TASK 2 Perform Network Tracerouting in Windows and Linux Machines

Here, we will perform network tracerouting using both Windows and Linux machines.

TASK 2.1 Tracerouting using Windows Machine

1. In the **Windows 10** virtual machine, open the **Command Prompt** window. Type **tracert www.certifiedhacker.com** and press **Enter** to view the hops that the packets made before reaching the destination.

Note: If you get the **Request timed out** reply for the above query, then use **Command Prompt of your host machine** instead of the Windows 10 virtual machine to run the query.

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

The route is the path that the network packet traverses between the source and destination. Network tracerouting is a process of identifying the path and hosts lying between the source and destination. Network tracerouting provides critical information such as the IP address of the hosts lying between the source and destination, which enables you to map the network topology of the organization. Traceroute can be used to extract information about network topology, trusted routers, firewall locations, etc.

Note: Screenshots may vary depending on the target destination.

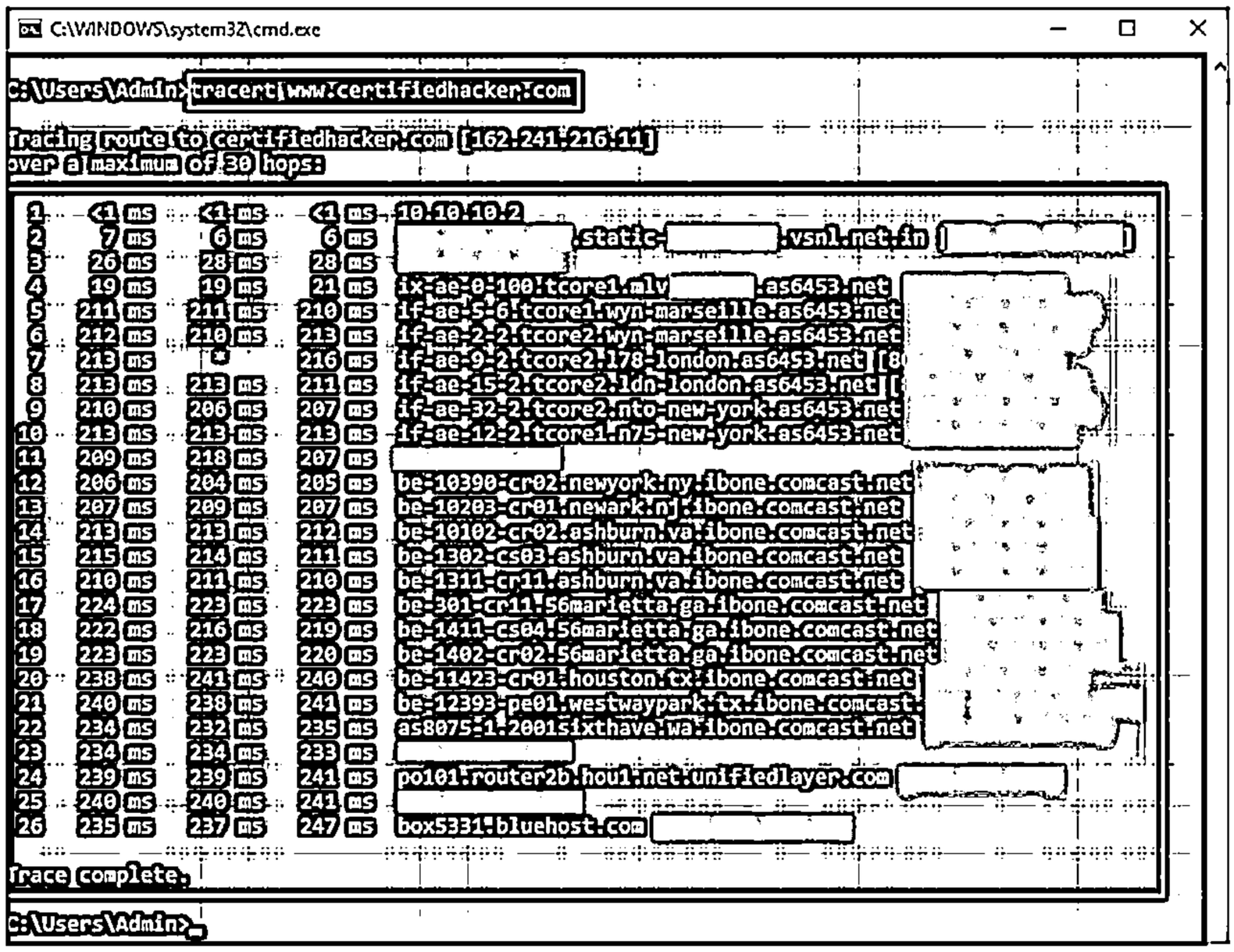


Figure 8.2.1: tracert command in windows machine

2. Type **tracert /?** and press **Enter** to show the different options for the command, as shown in the screenshot.

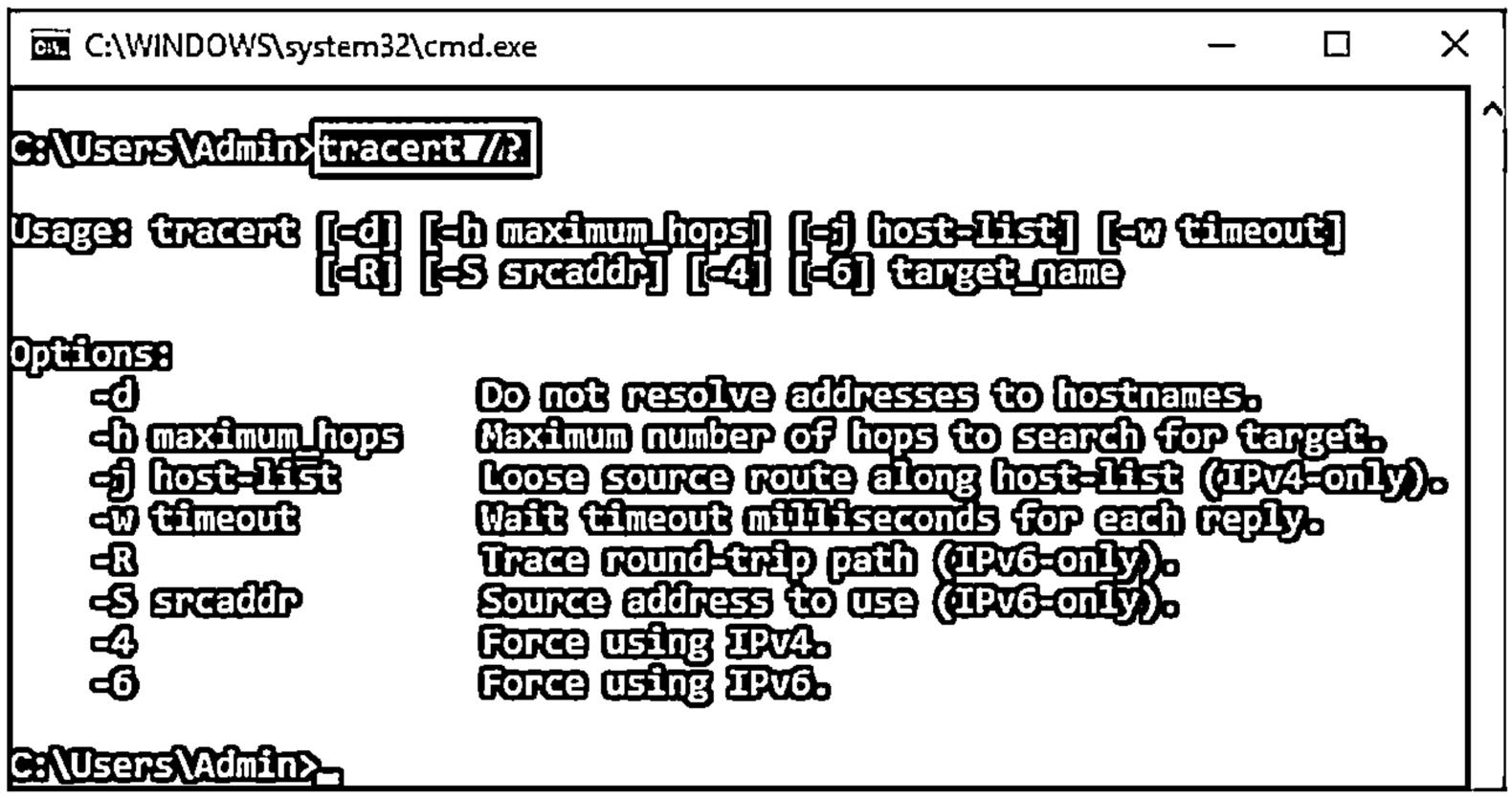


Figure 8.2.2: Tracert help command

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

3. Type **tracert -h 5 www.certifiedhacker.com** and press **Enter** to perform the trace, but with only 5 maximum hops allowed.

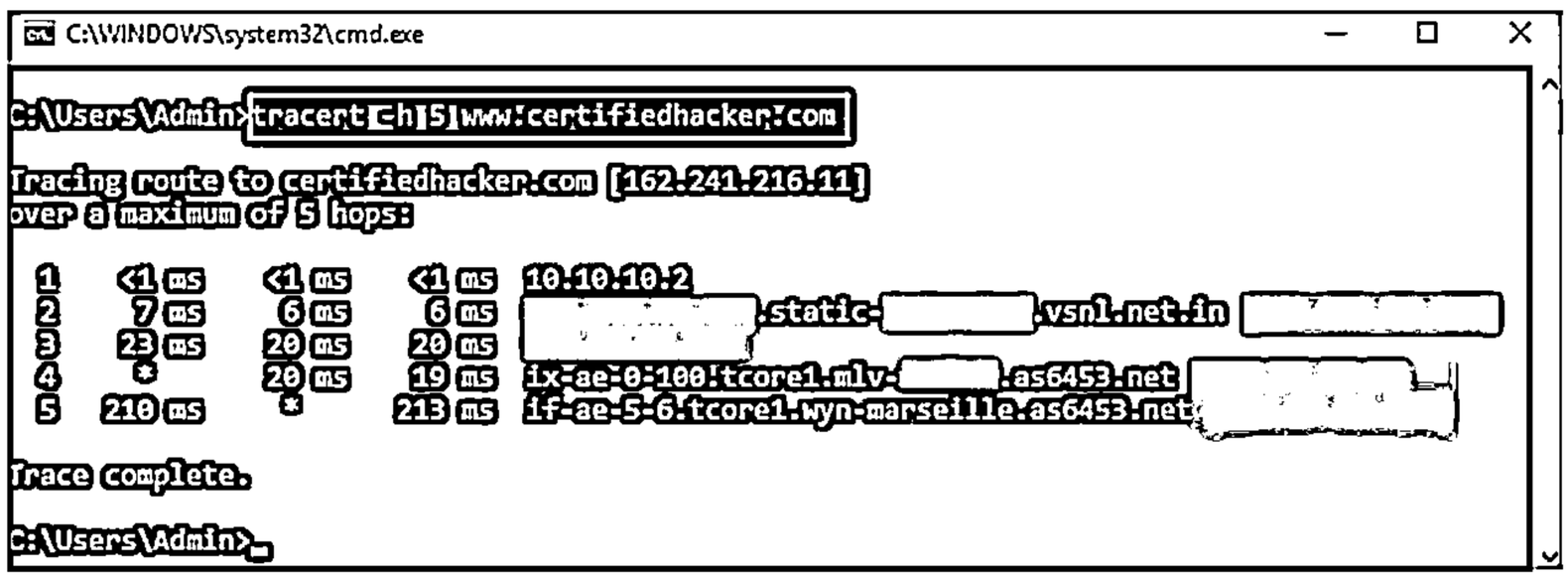


Figure 8.2.3: tracing the route with only 5 hops

4. After viewing the result, close the command prompt window.

TASK 2.2

Traceroutes using Linux Machine

5. Turn on the **Parrot Security** virtual machine.
6. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

7. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
8. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
9. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

10. Now, type **cd** and press **Enter** to jump to the root directory.

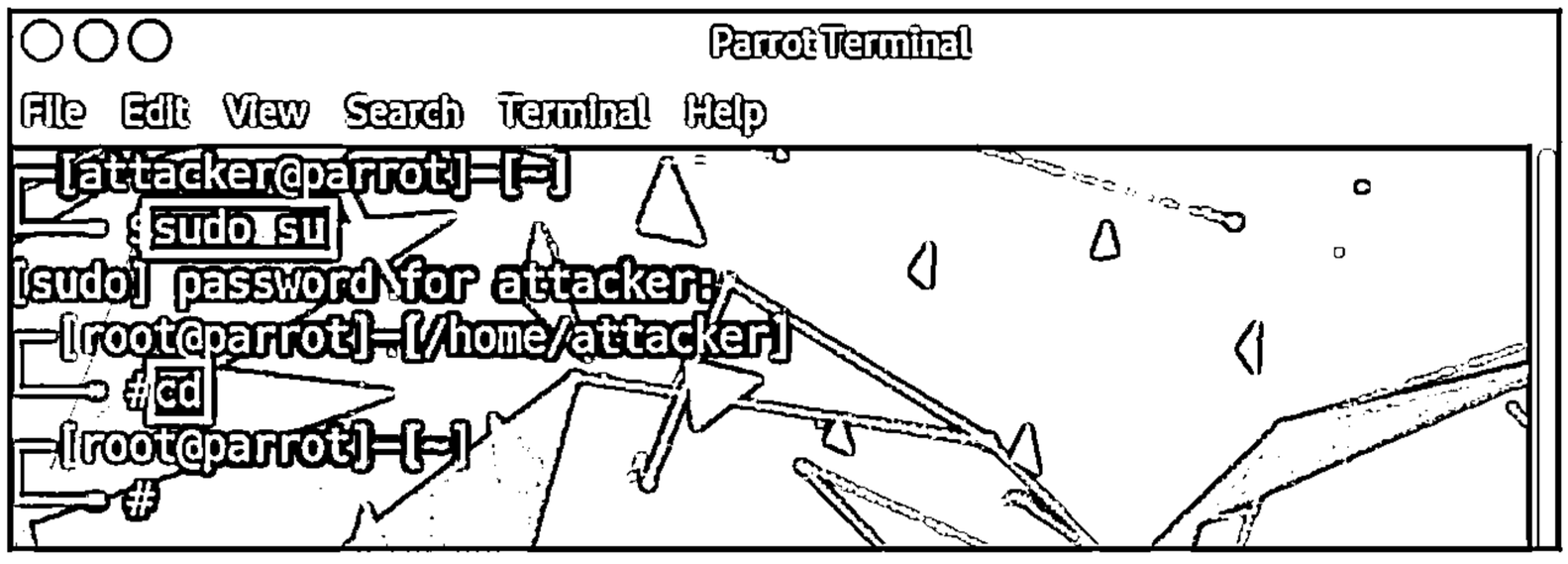


Figure 8.2.4: Running the programs as a root user

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

11. In the terminal window, type **traceroute www.certifiedhacker.com** and press **Enter** to view the hops that the packets made before reaching the destination.

Note: Since we have set up a simple network, you can find the direct hop from the source to the target destination. However, screenshots may vary depending on the target destination.

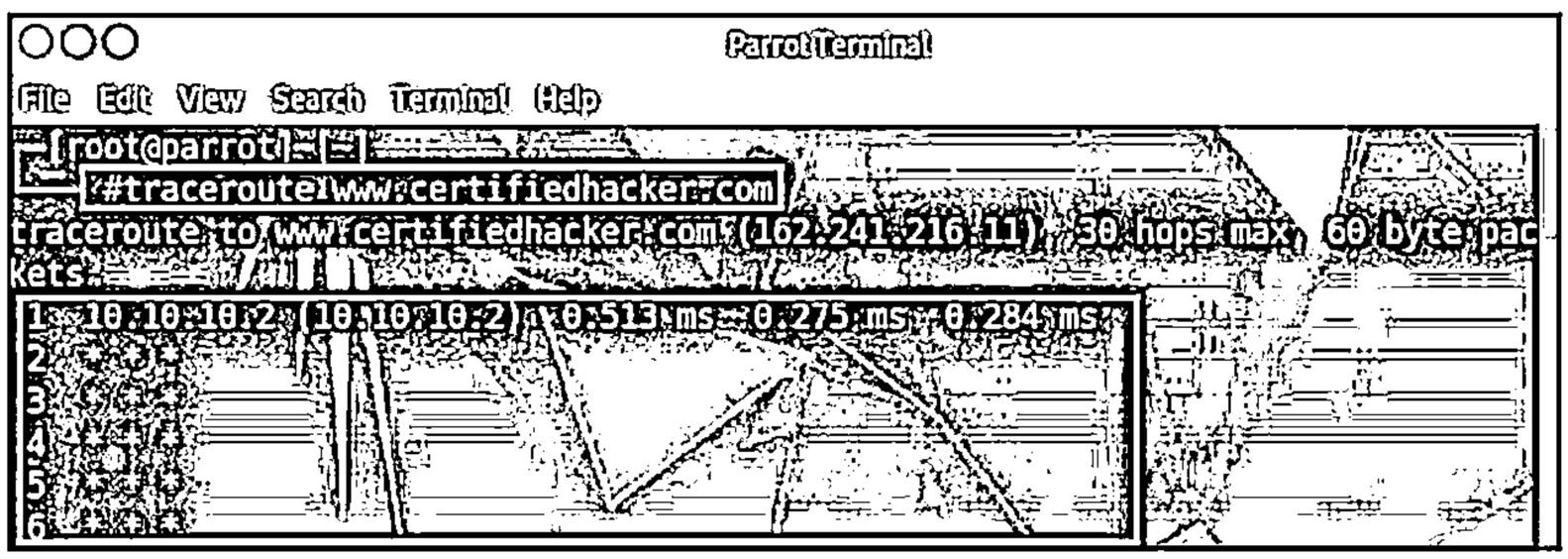


Figure 8.2.5: traceroute command in Linux machine

12. This concludes the demonstration of performing network tracerouting using the Windows and Linux machines.
13. Close all open windows and document all the acquired information.
14. Turn off the **Parrot Security** virtual machine.

TASK 3 Perform Advanced Network Route Tracing Using Path Analyzer Pro

Traceroute is a system administrator utility to trace the route IP packets take from a source system to some destination system, and Path Analyzer Pro summarizes a given trace to any destination within seconds by generating a simple report with all the important information on the target. Path Analyzer Pro is an advanced network tracerouting tool where you can input any of the target details such as IP address, a hostname, or an email address.

Here, we will perform network tracerouting using Path Analyzer Pro.

1. In the **Windows 10** virtual machine, open **File Explorer** and navigate to **E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance\Traceroute Tools\Path Analyzer Pro** and double-click **PAPro27.msi**.
2. The **Path Analyzer Pro 2.7** setup window appears.
3. Follow the wizard steps (by selecting default options) to install Path Analyzer Pro.

Note: If a **User Account Control** window appears, click **Yes**.

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

4. Click the **Start** menu and right-click **Path Analyzer Pro 2.7**. Expand **More** and click the **Run as administrator** options.

Note: If a **User Account Control** window appears, click **Yes**.

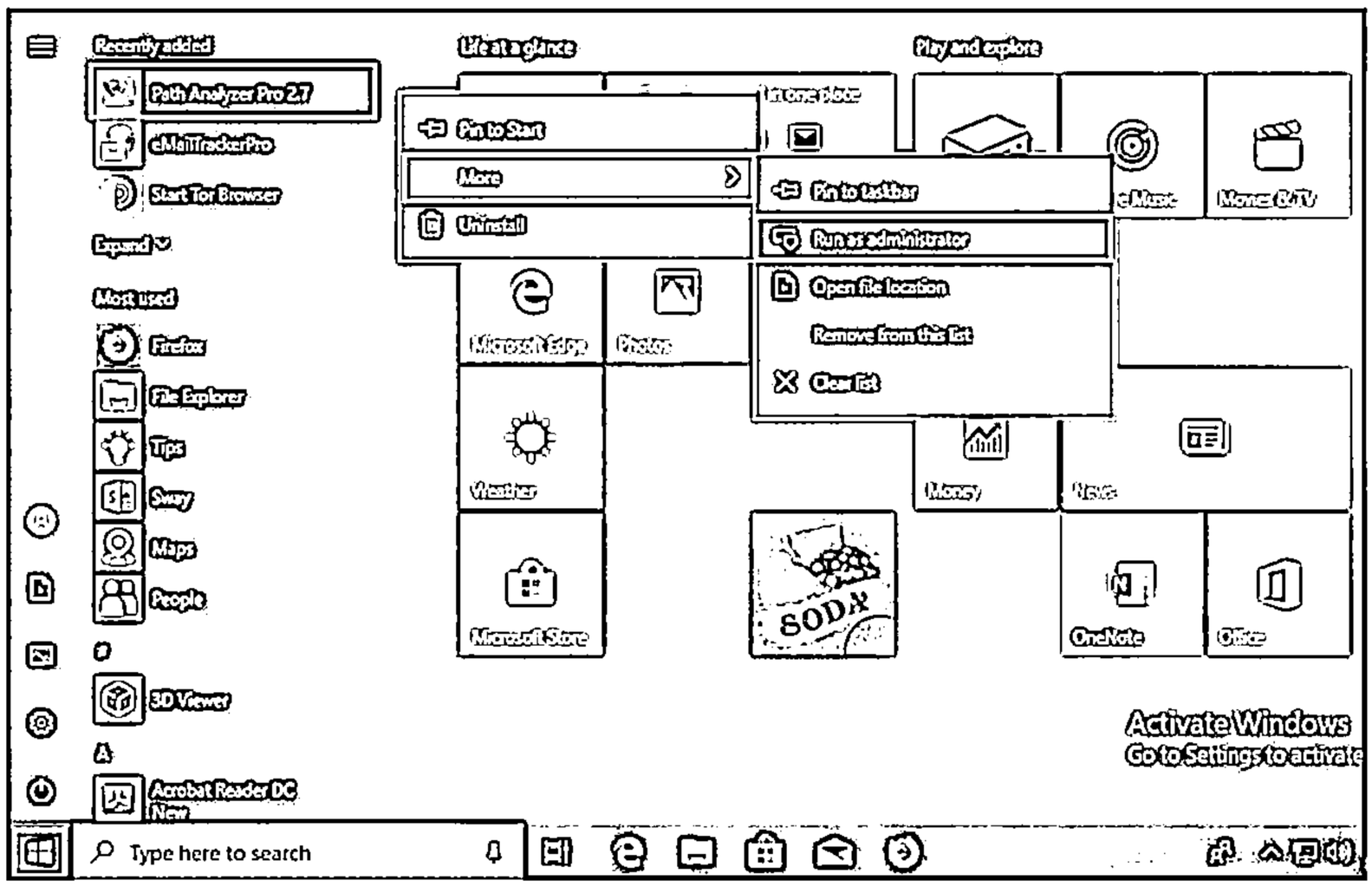


Figure 8.3.1: Launch Path Analyzer Pro 2.7

5. The **Path Analyzer Pro** window appears along with a **Registration Form** pop-up; click **Evaluate** in the pop-up.

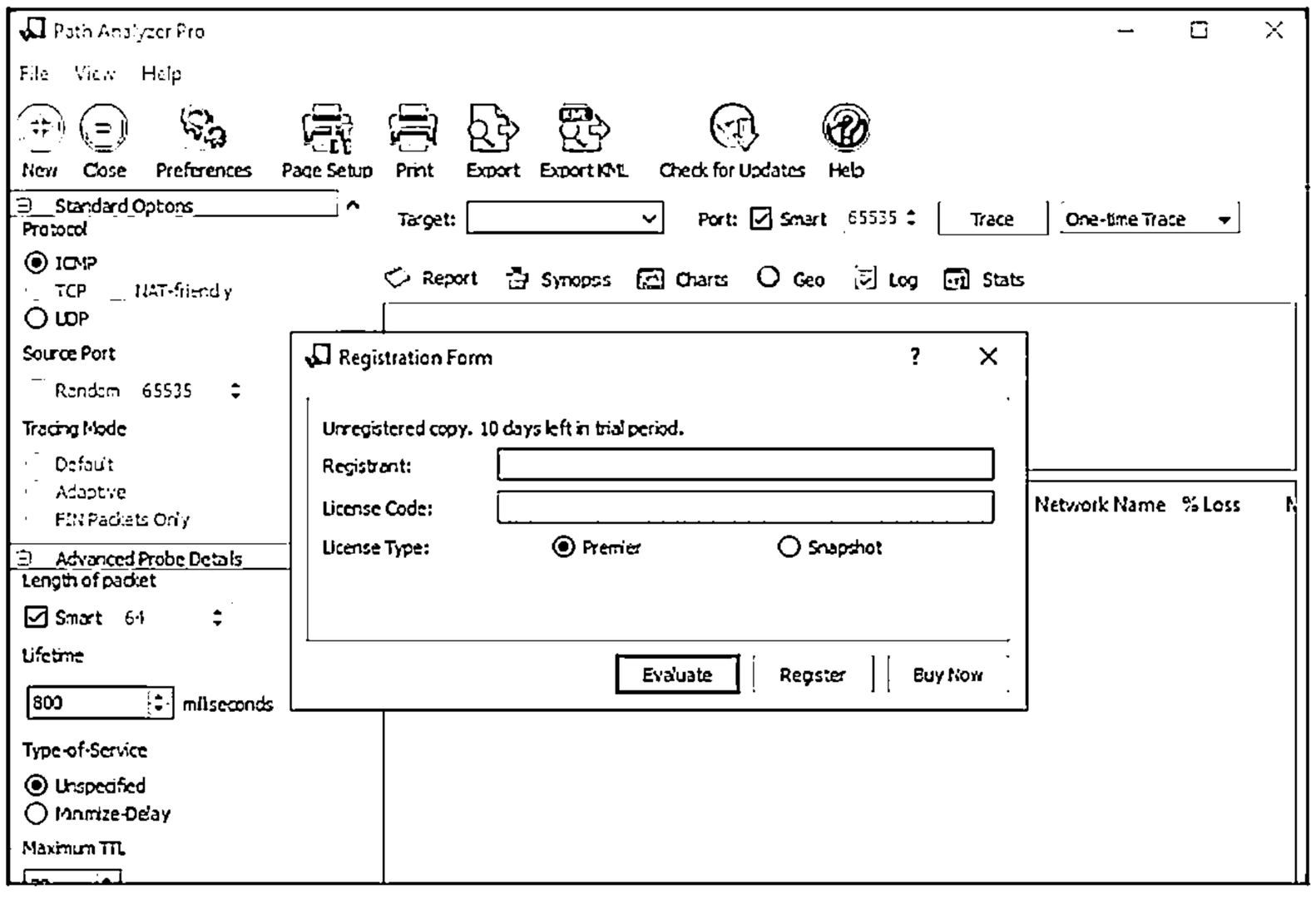


Figure 8.3.2: Path Analyzer Pro 2.7 Registration Form window

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

TASK 3.1

Trace a Target Network

6. In the left-pane of the **Path Analyzer Pro** window, a few options are set to default in the **Standard Options** and **Advanced Probe Details** sections. Ensure that the **ICMP** radio button under the **Protocol** field of **Standard Options** is selected and the **Smart** option under the **Length of packet** field of the **Advanced Probe Details** section is checked.

Note: If you have a firewall, it must be disabled for appropriate output.

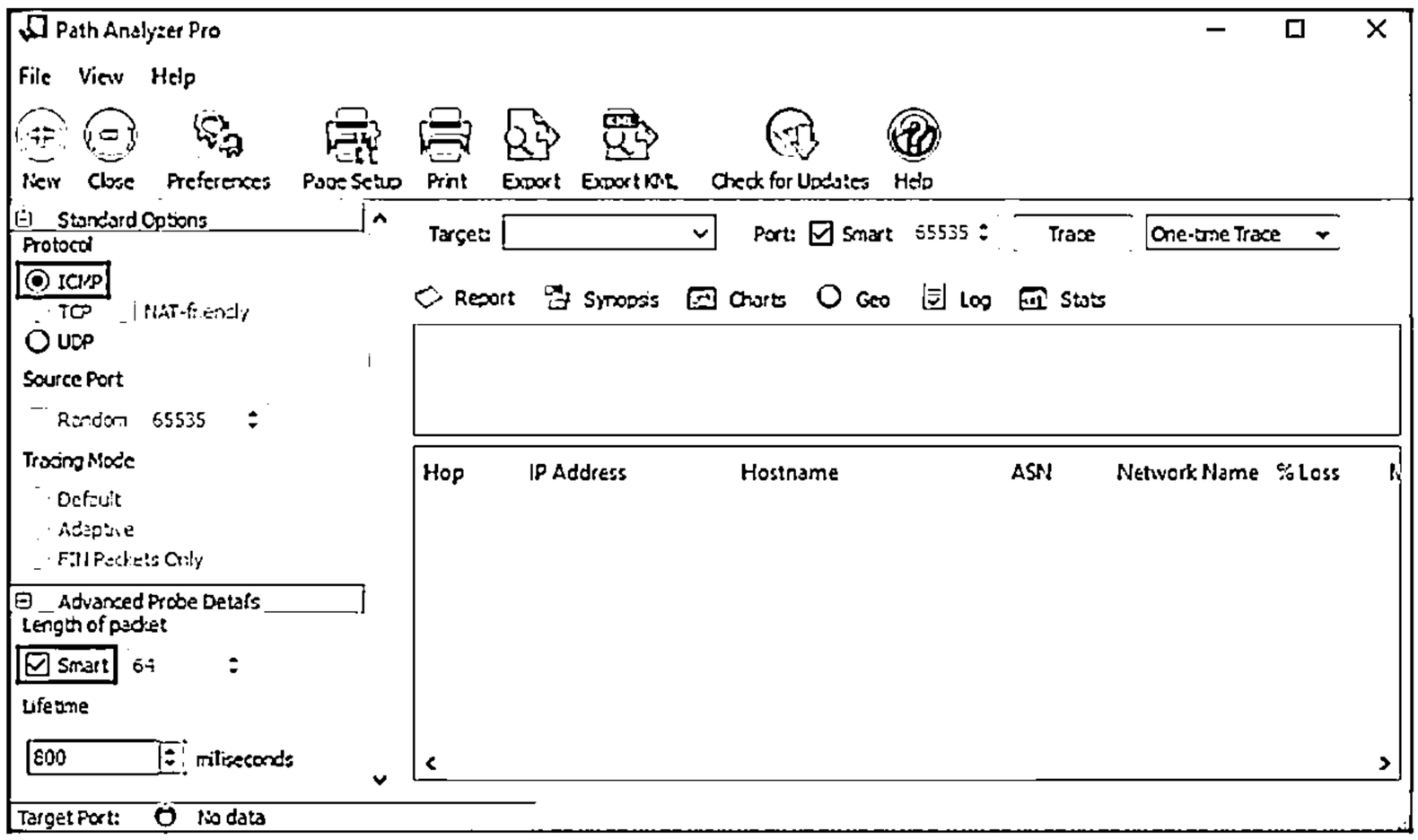


Figure 8.3.3: The Path Analyzer Pro Advanced Probe Details window

7. In the **Advanced Tracing Details** section, a few options are set to default. Ensure that the **Stop on control messages (ICMP)** option is checked in the **Advanced Tracing Details** section.

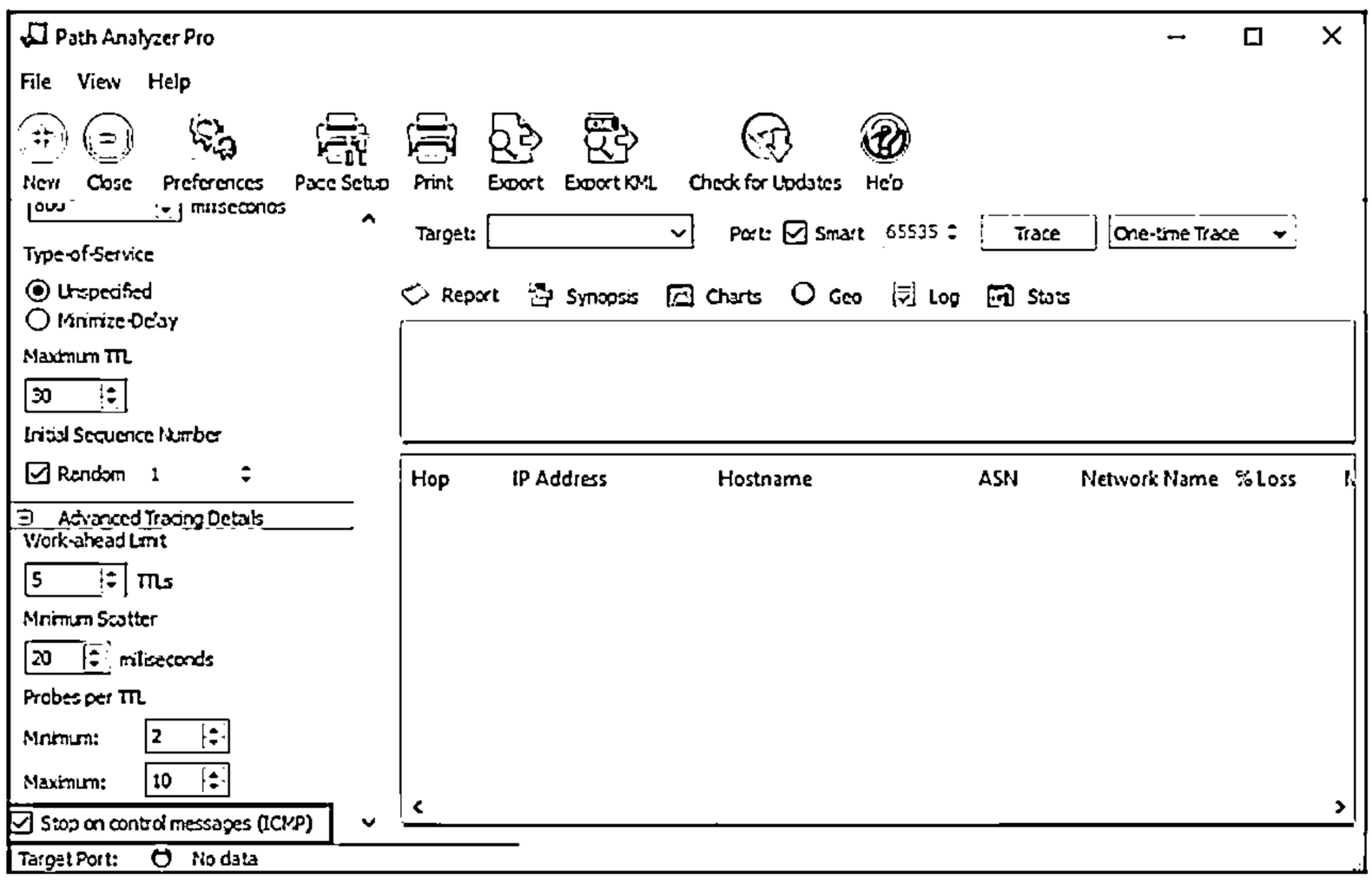


Figure 8.3.4: Advanced Tracing Details window

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

8. To perform the trace, enter the hostname in the **Target:** field (for instance, **www.google.com**) and ensure that **Smart** under the **Port:** field is checked (here, default is **65535**). From the drop-down menu, choose **Timed Trace** and click **Trace**.

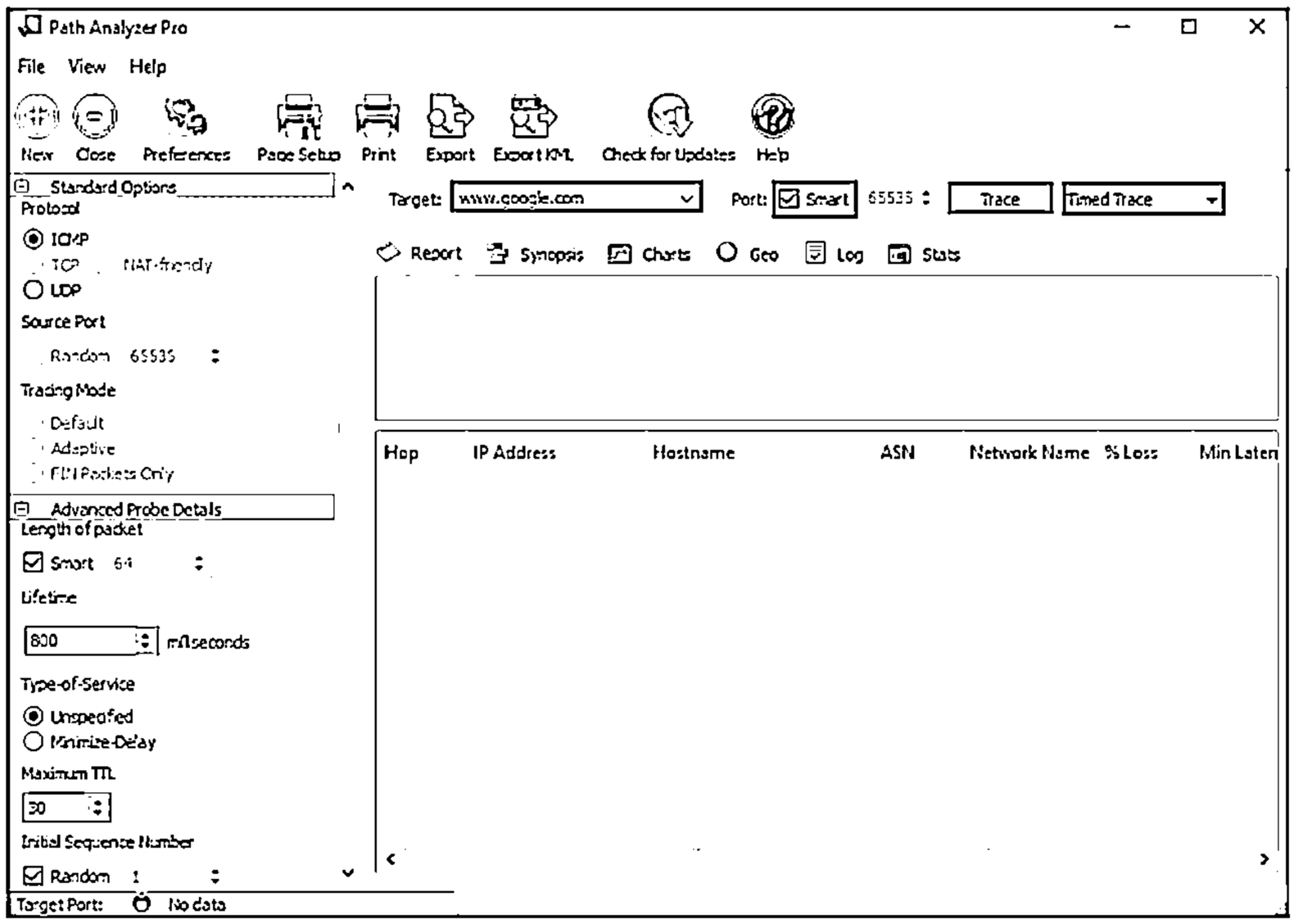


Figure 8.3.5: A Path Analyzer Pro Advanced Tracing Details option

9. The **Type time of trace** dialog box appears. Specify the time of trace (here, **mm** is changed to **3**) in the **hh: mm: ss** format and click **Accept**.

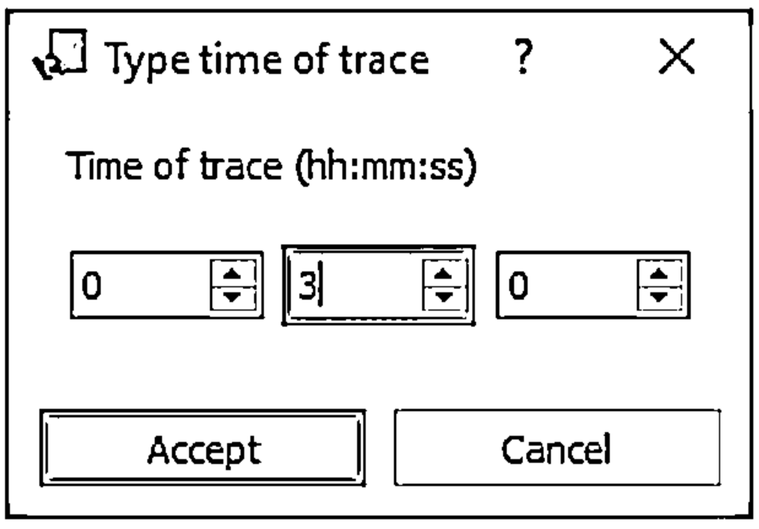


Figure 8.3.6: The Path Analyzer Pro Type time of trace option

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

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

TASK 3.2

Examine the Results

11. After the trace is complete, the trace results are displayed under the **Report** tab in the form of a **linear chart** depicting the number of hops between you and the target.

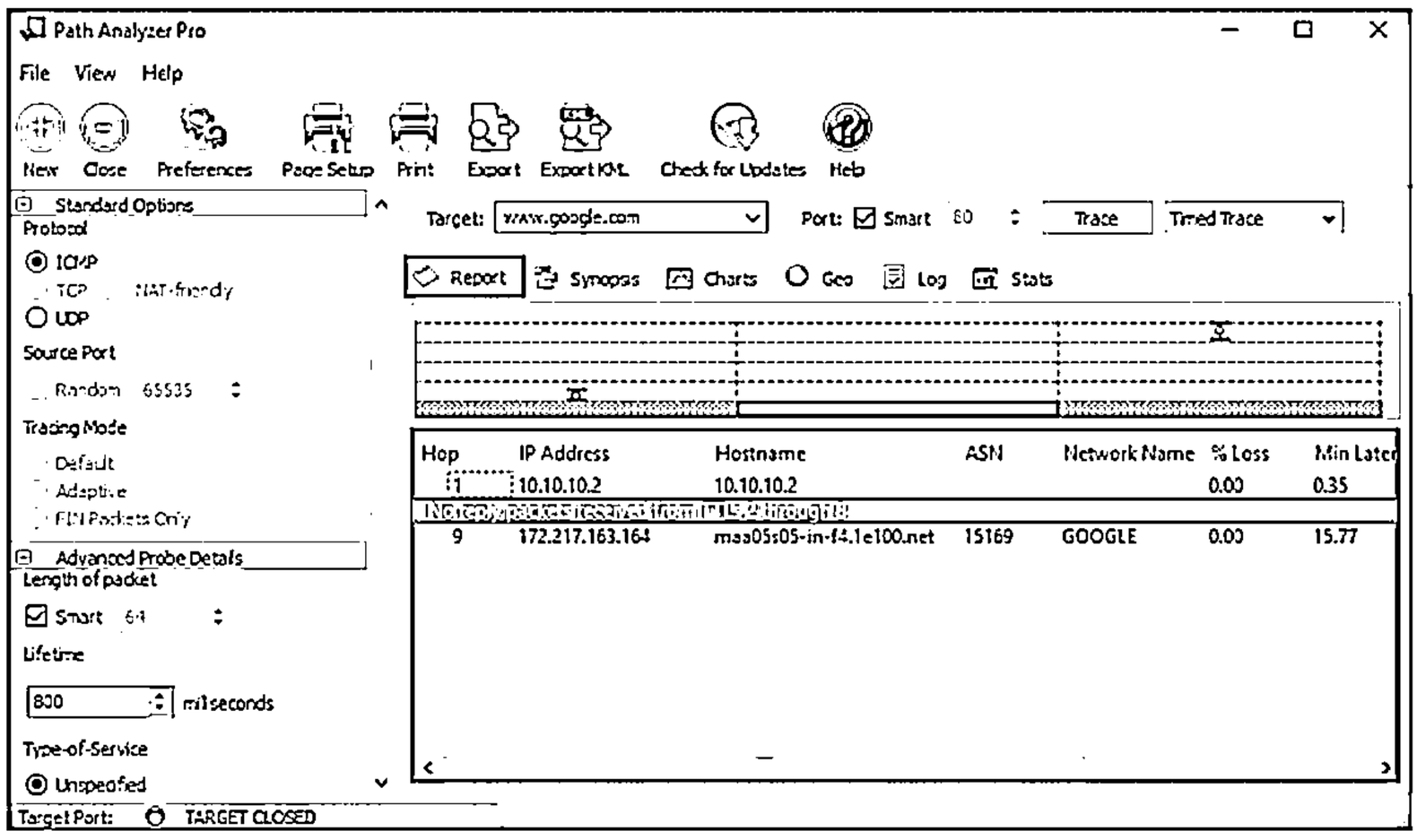


Figure 8.3.7: A Path Analyzer Pro Target option

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

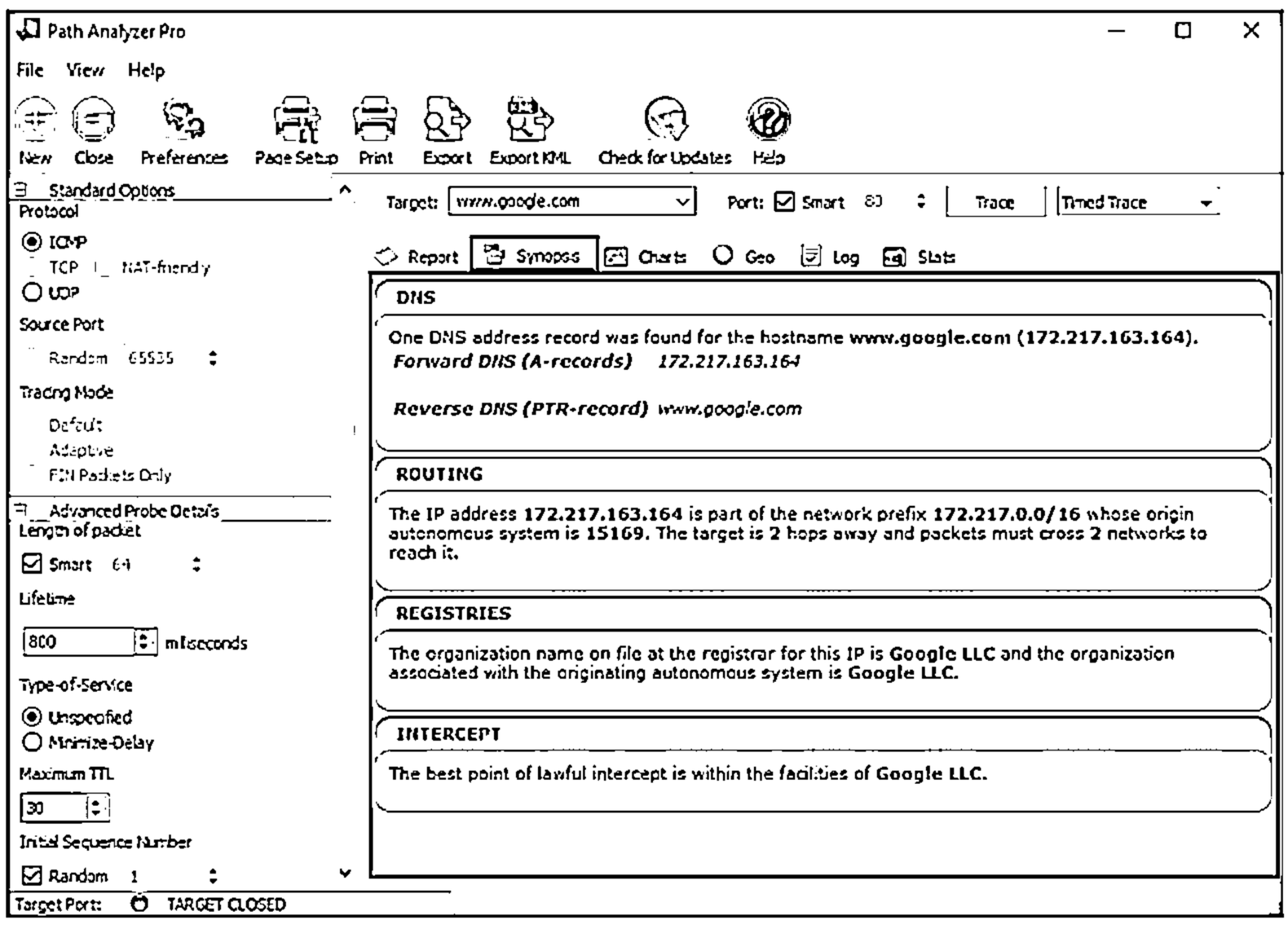


Figure 8.3.8: A Path Analyzer Pro Target option

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

TASK 3.3

View Charts

13. Click the **Charts** tab to view the results of the trace.

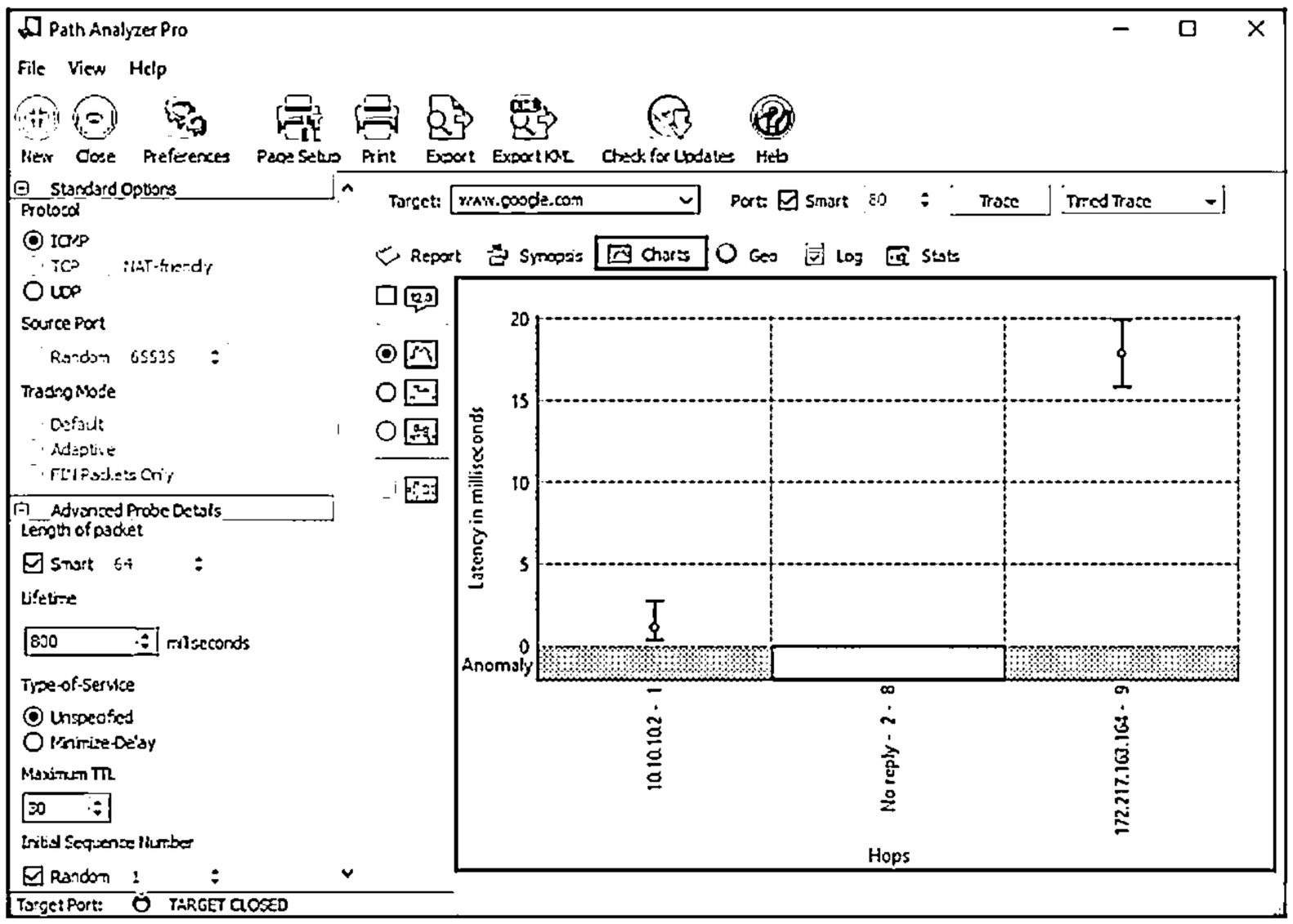


Figure 8.3.9: The Path Analyzer Pro Chart Window

TASK 3.4

Inspect the Geographical Location

14. Click **Geo**, which displays a world map of the traceroute.

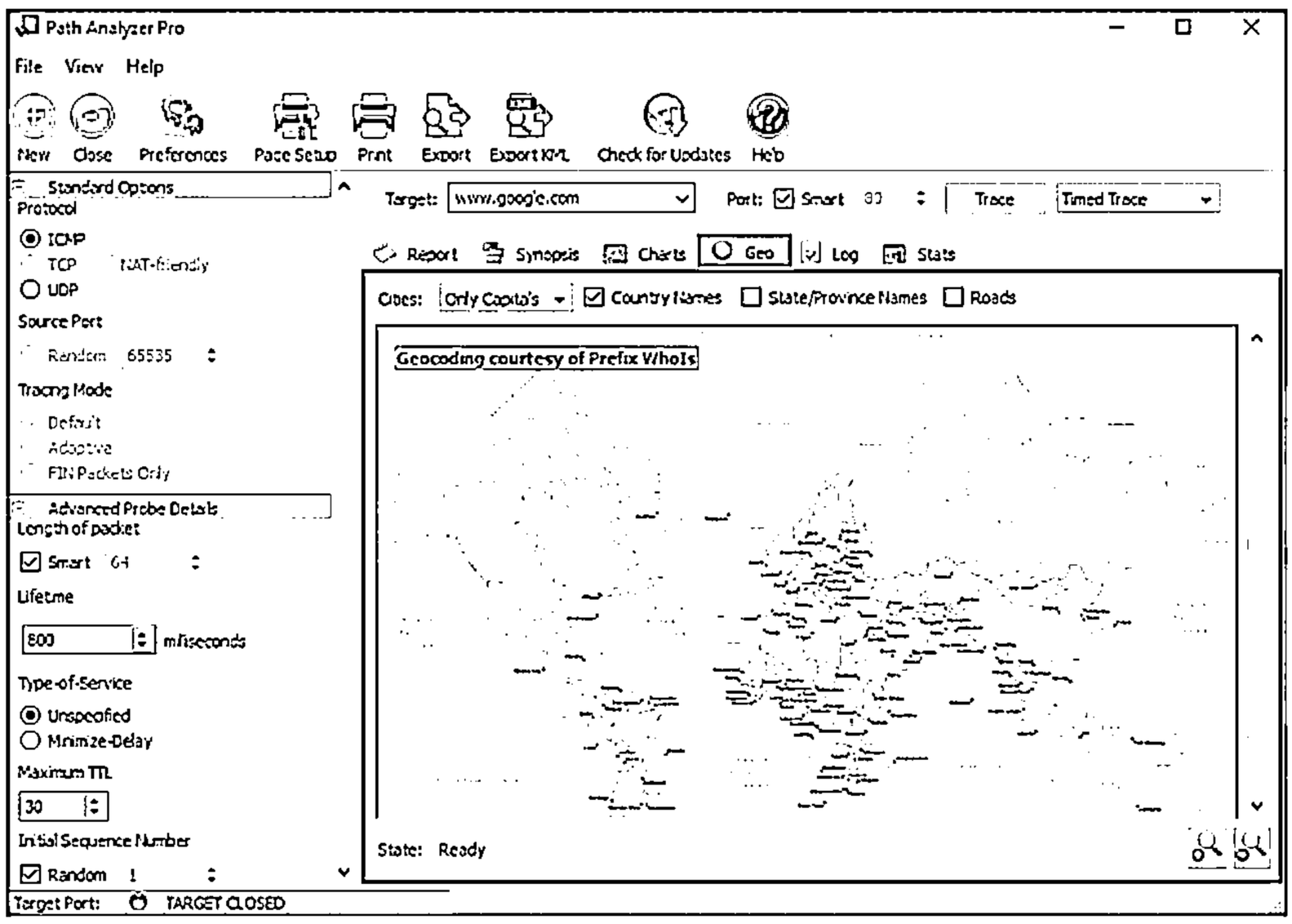


Figure 8.3.10: The Path Analyzer Pro chart window

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

TASK 3.5

Examine the Logs

15. Click the **Log** tab to view **Current Trace Log** and **Session Log.**

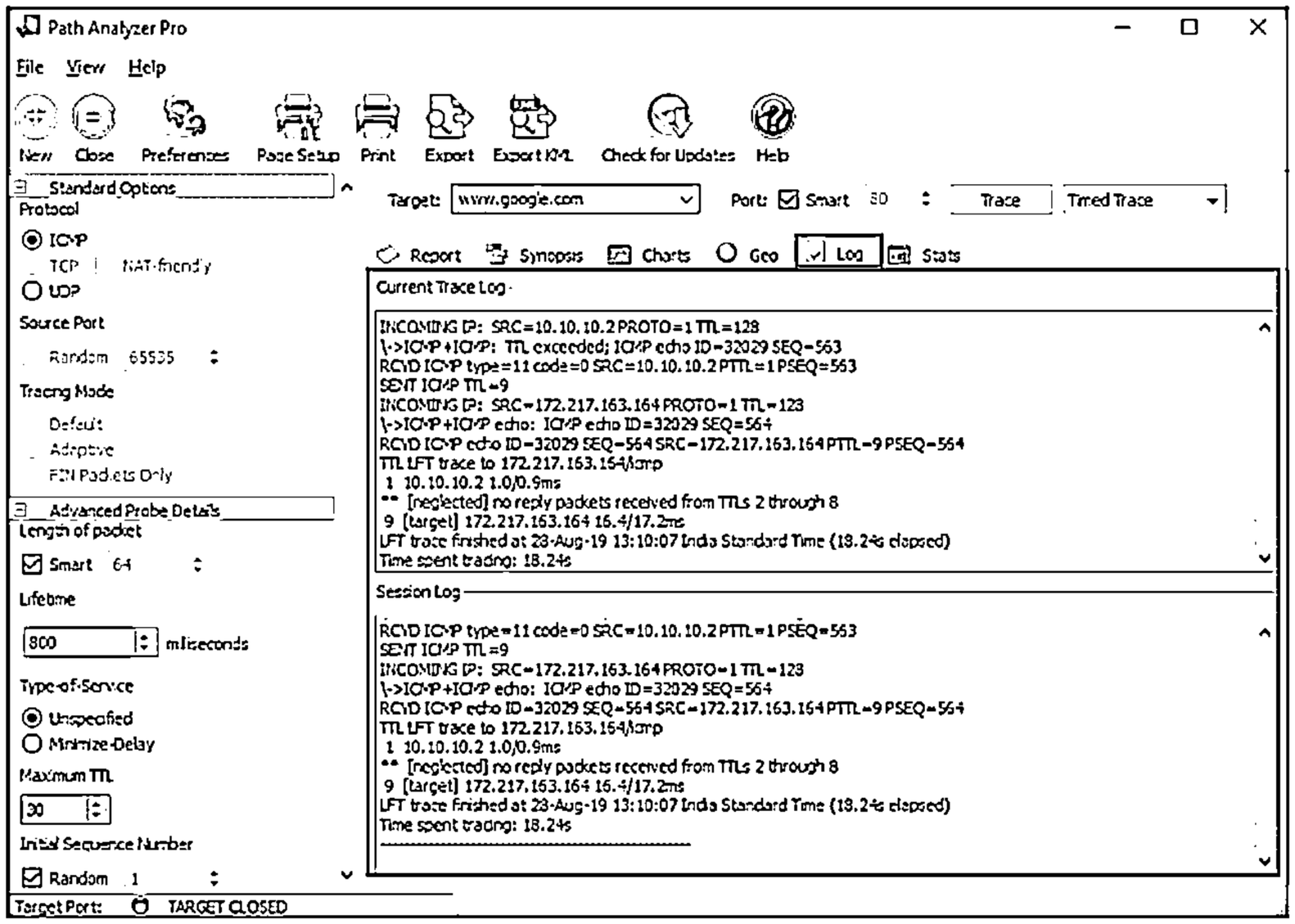


Figure 8.3.11: The Path Analyzer Pro Current Trace Log and Session Log window

TASK 3.6

Observe the Statistics

16. Click the **Stats** tab, which features the current trace's **Vital Statistics.**

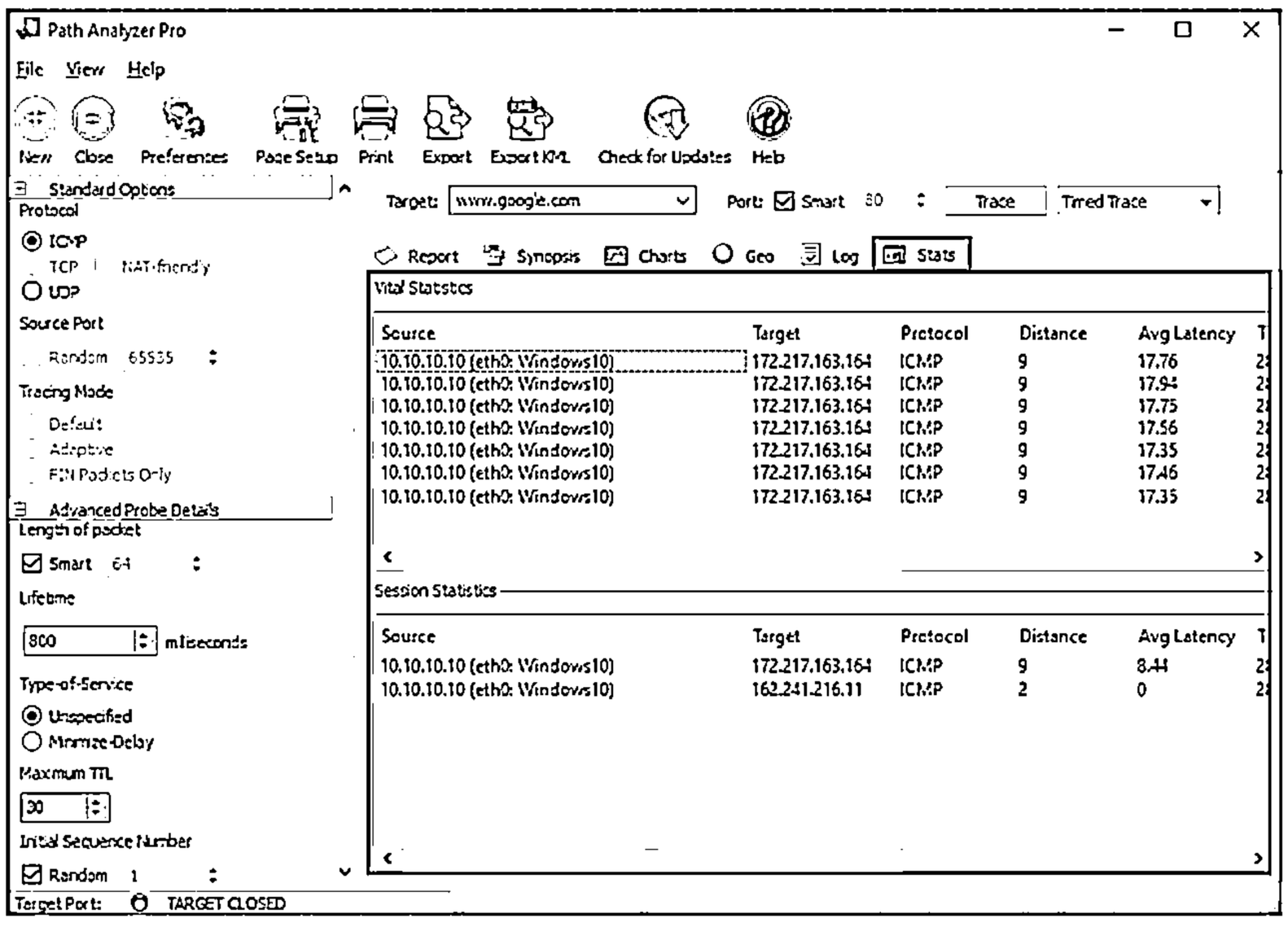


Figure 8.3.12: The Path Analyzer Pro Statistics window

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

TASK 3.7

Export Results

17. Click **Export** in the toolbar to export the report.

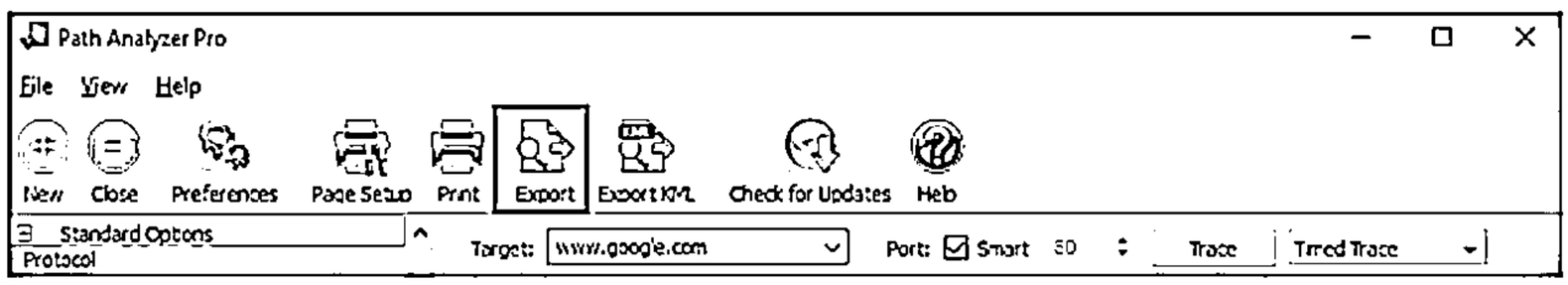


Figure 8.3.13: The Path Analyzer Pro Save Report As window

18. The **Save Statistics As** window appears. Specify your desired name for the file in **File name:** field (here, **Sample Report**) and click **Save**.

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

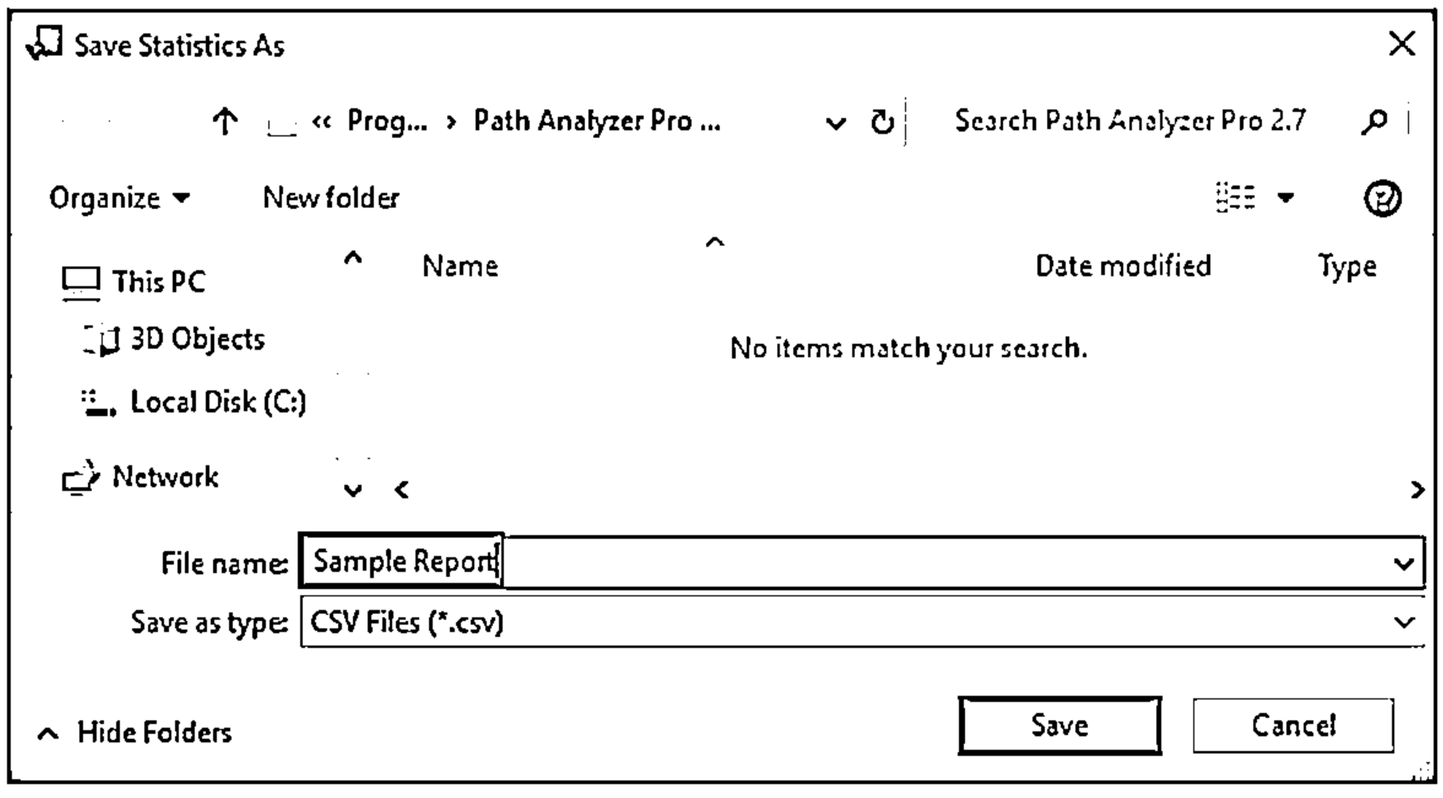


Figure 8.3.14: The Path Analyzer Pro Save Report As window

19. This concludes the demonstration of gathering information about a target organization by performing network tracerouting using Path Analyzer Pro.
20. Close all open windows and document all acquired information.
21. Turn off the **Windows 10** virtual machine.

You can also use other traceroute tools such as **VisualRoute** (http://www.visualroute.com), **Traceroute NG** (https://www.solarwinds.com), etc. to extract additional network information of the target organization.

Lab Analysis

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

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT 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

Perform Footprinting using Various Footprinting Tools

Ethical hackers and penetration testers perform footprinting with the help of various tools that make information gathering an easy task.

ICON KEY

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

Lab Scenario

The information gathered in the previous steps may not be sufficient to reveal the potential vulnerabilities of the target. There could be more information available that could help in finding loopholes in the target. As an ethical hacker, you should look for as much information as possible about the target using various tools. This lab activity will demonstrate what other information you can extract from the target using various footprinting tools.

Lab Objectives

- Footprinting a target using Recon-ng
- Footprinting a target using Maltego
- Footprinting a target using OSRFramework
- Footprinting a target using FOCA
- Footprinting a target using BillCipher
- Footprinting a target using OSINT Framework

Lab Environment

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance

To carry out this lab, you need:

- Windows 10 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

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

- FOCA located at **E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance\Footprinting Tools\FOCA\bin**
- You can also download the latest version of FOCA from its official website. If you decide to download the latest version, the screenshots shown in the lab might differ.

Lab Duration

Time: 65 Minutes

Overview of Footprinting Tools

Footprinting tools are used to collect basic information about the target systems in order to exploit them. Information collected by the footprinting tools contains the target's IP location information, routing information, business information, address, phone number and social security number, details about the source of an email and a file, DNS information, domain information, etc.

Lab Tasks

TASK 1

Recon-ng is a web reconnaissance framework with independent modules and database interaction that provides an environment in which open-source web-based reconnaissance can be conducted. Here, we will use Recon-ng to perform network reconnaissance, gather personnel information, and gather target information from social networking sites.

Footprinting a Target using Recon-ng

1. Turn on **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

6. Now, type **cd** and press **Enter** to jump to the root directory.

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

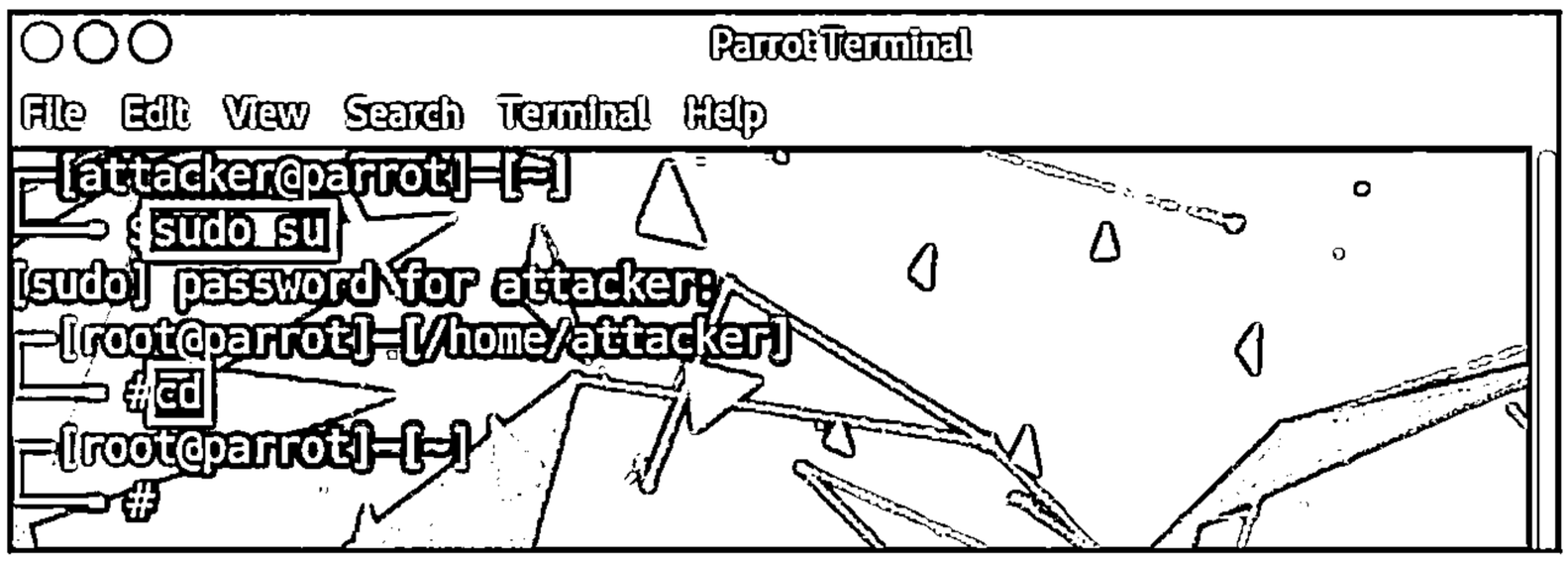


Figure 9.1.1: Running the programs as a root user

7. Type the command **recon-ng** and press **Enter** to launch the application.

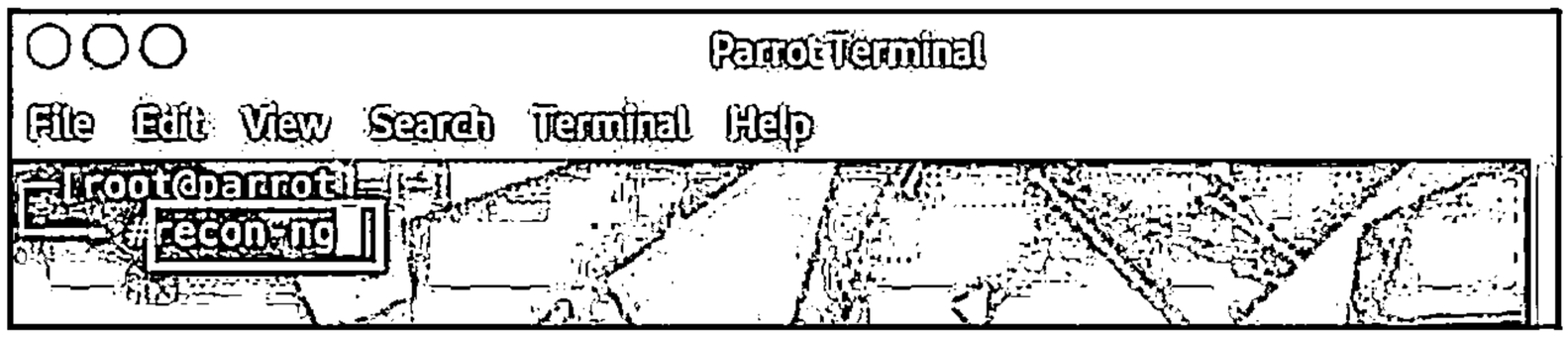


Figure 9.1.2: Launching recon-ng

8. Type **help** and press **Enter** to view all the commands that allow you to add/delete records to a database, query a database, etc.

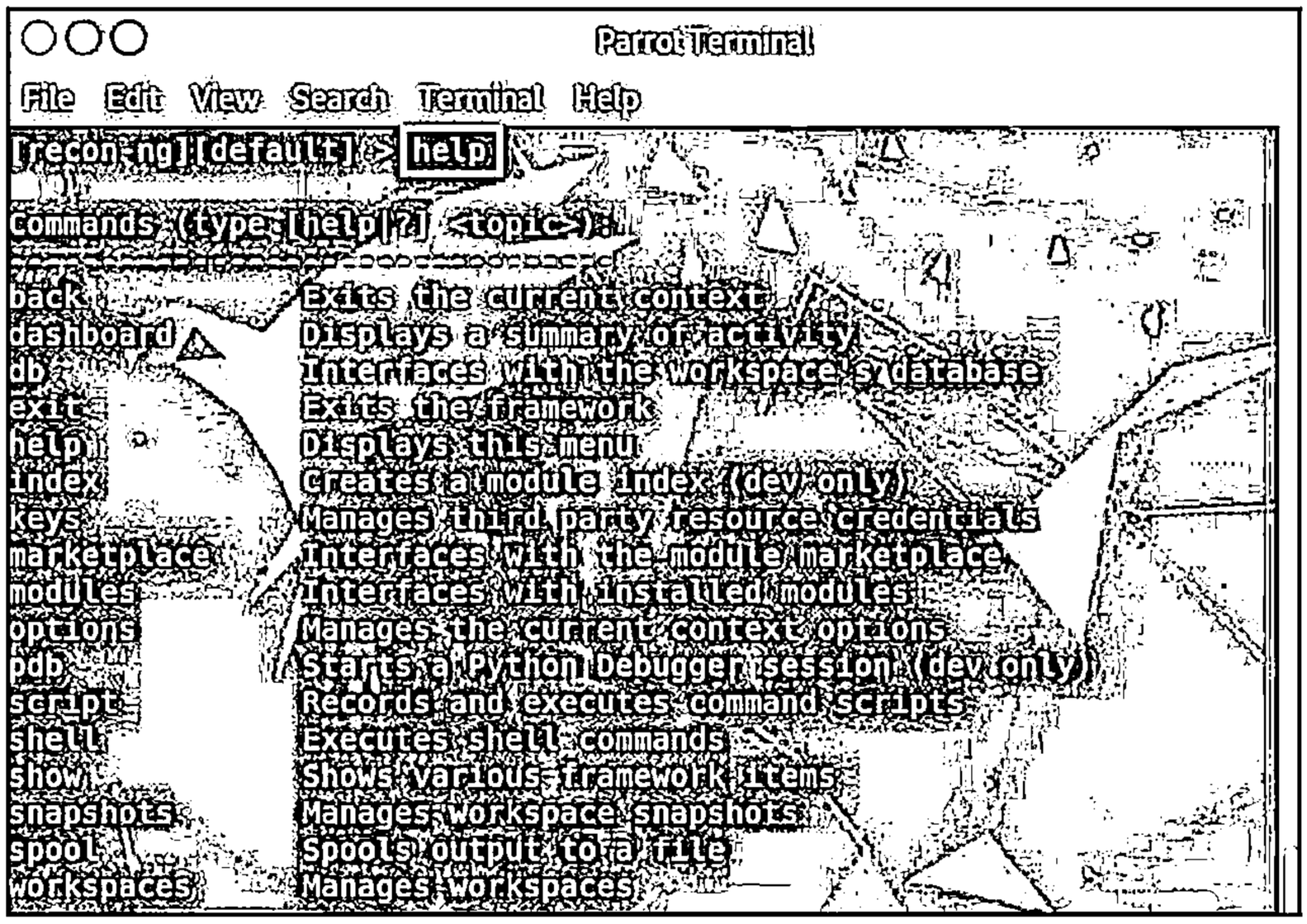


Figure 9.1.3: Viewing recon-ng Commands

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

9. Type **marketplace install all** and press **Enter** to install all the modules available in recon-ng.

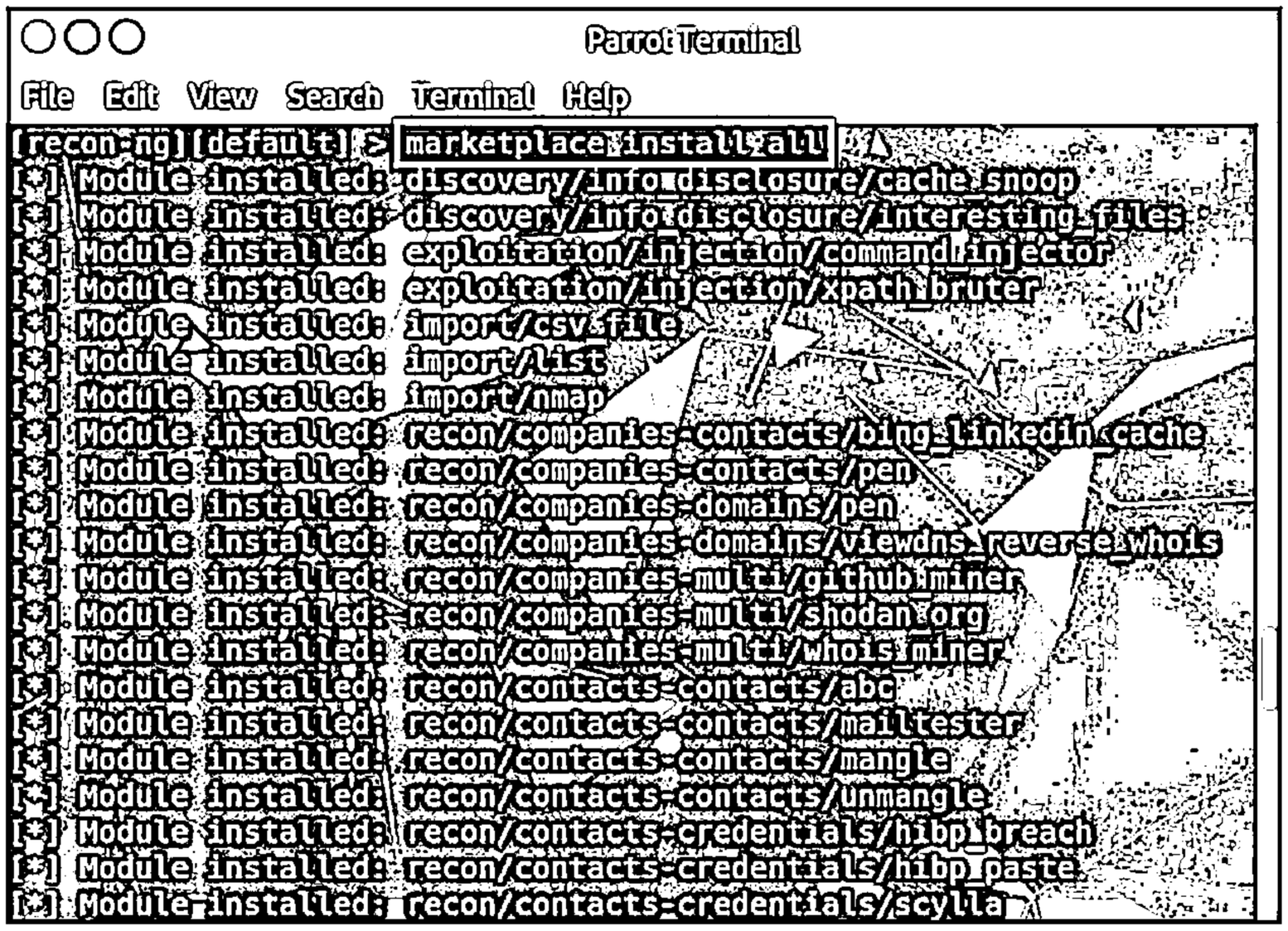


Figure 9.1.4: Installing Modules

10. Type the **modules search** command and press **Enter**. This displays all the modules available in recon-ng.

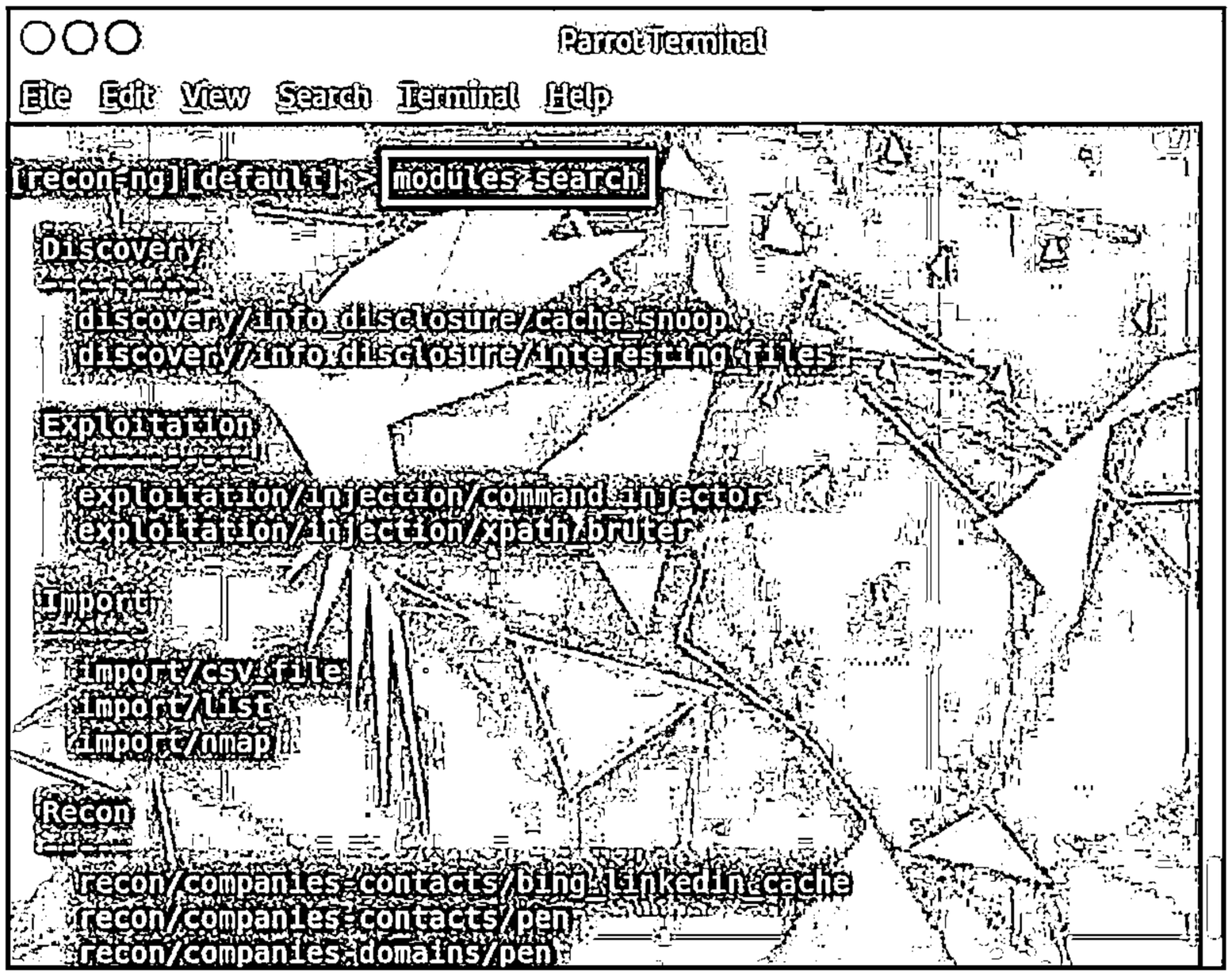


Figure 9.1.5: Viewing Modules

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

11. You will be able to perform network discovery, exploitation, reconnaissance, etc. by loading the required modules.
12. Type the **workspaces** command and press **Enter**. This displays the commands related to the workspaces.

TASK 1.1

Create a Workspace

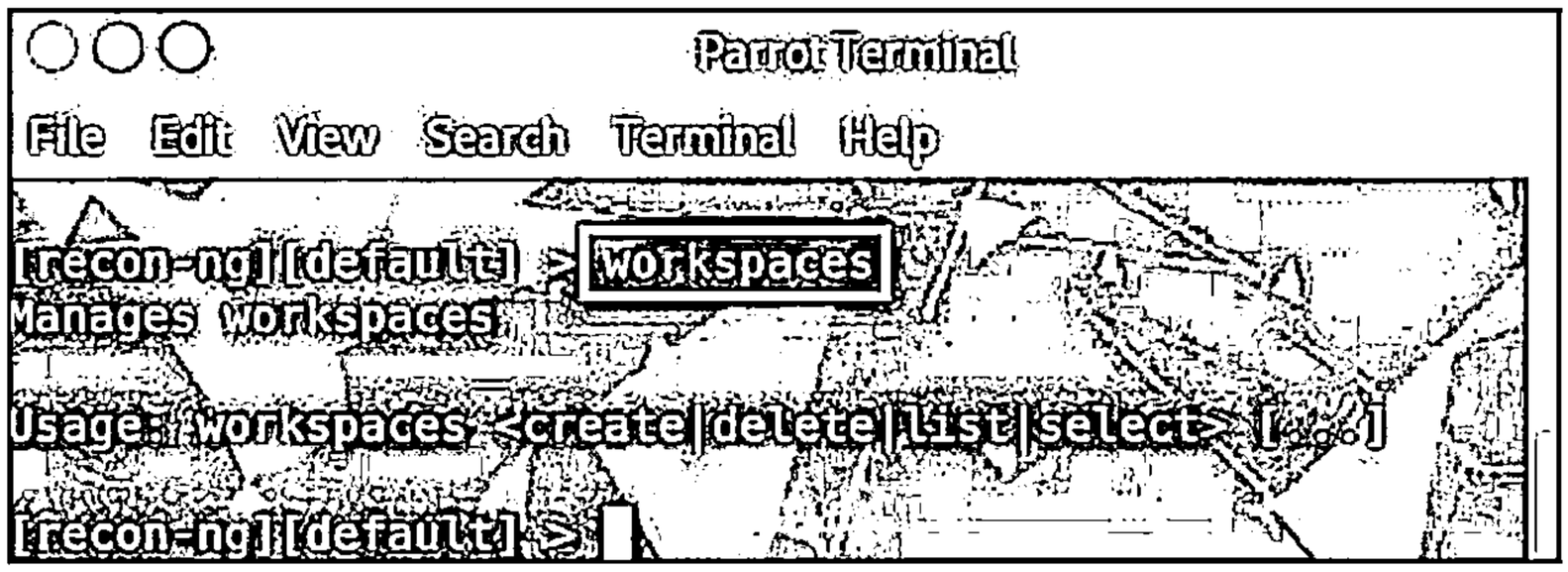


Figure 9.1.6: Viewing Workspaces Related Commands

13. Create a workspace in which to perform network reconnaissance. In this lab, we shall be creating a workspace named **CEH**.
14. To create the workspace, type the command **workspaces create CEH** and press **Enter**. This creates a workspace named CEH.

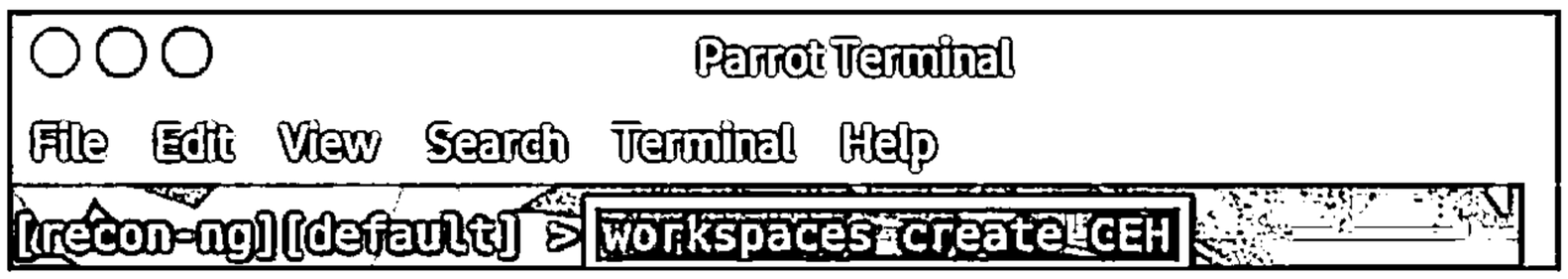


Figure 9.1.7: Creating a Workspace

Note: You can alternatively issue the command **workspaces select CEH** to create a workspace named CEH. Ignore the errors while running the commands

15. Enter **workspaces list**. This displays a list of workspaces (along with the workspace added in the previous step) that are present within the workspaces databases.

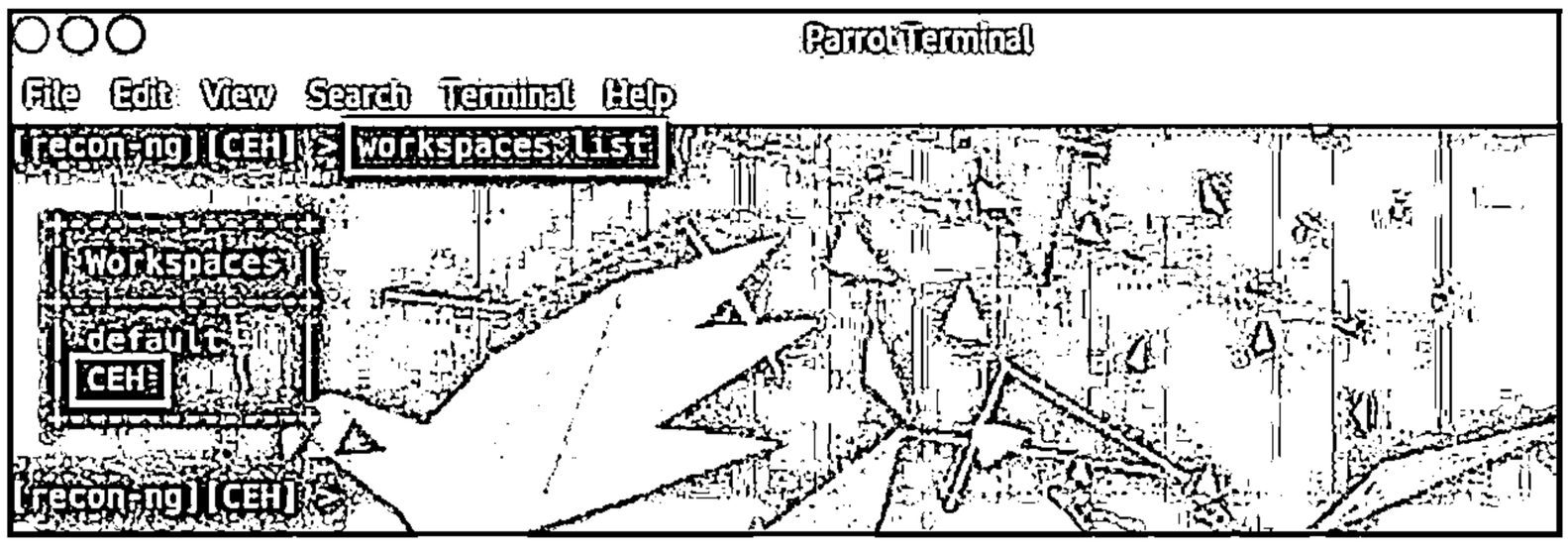


Figure 9.1.8: Viewing the Added Workspaces

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

TASK 1.2

Add a Domain

16. Add a domain in which you want to perform network reconnaissance
17. Type the command **db insert domains** and press **Enter**.
18. In the **domain (TEXT)** option, type **certifiedhacker.com** and press **Enter**. In the **notes (TEXT)** option, press **Enter**. This adds certifiedhacker.com to the present workspace.
19. You can view the added domain by issuing the **show domains** command, as shown in the screenshot.

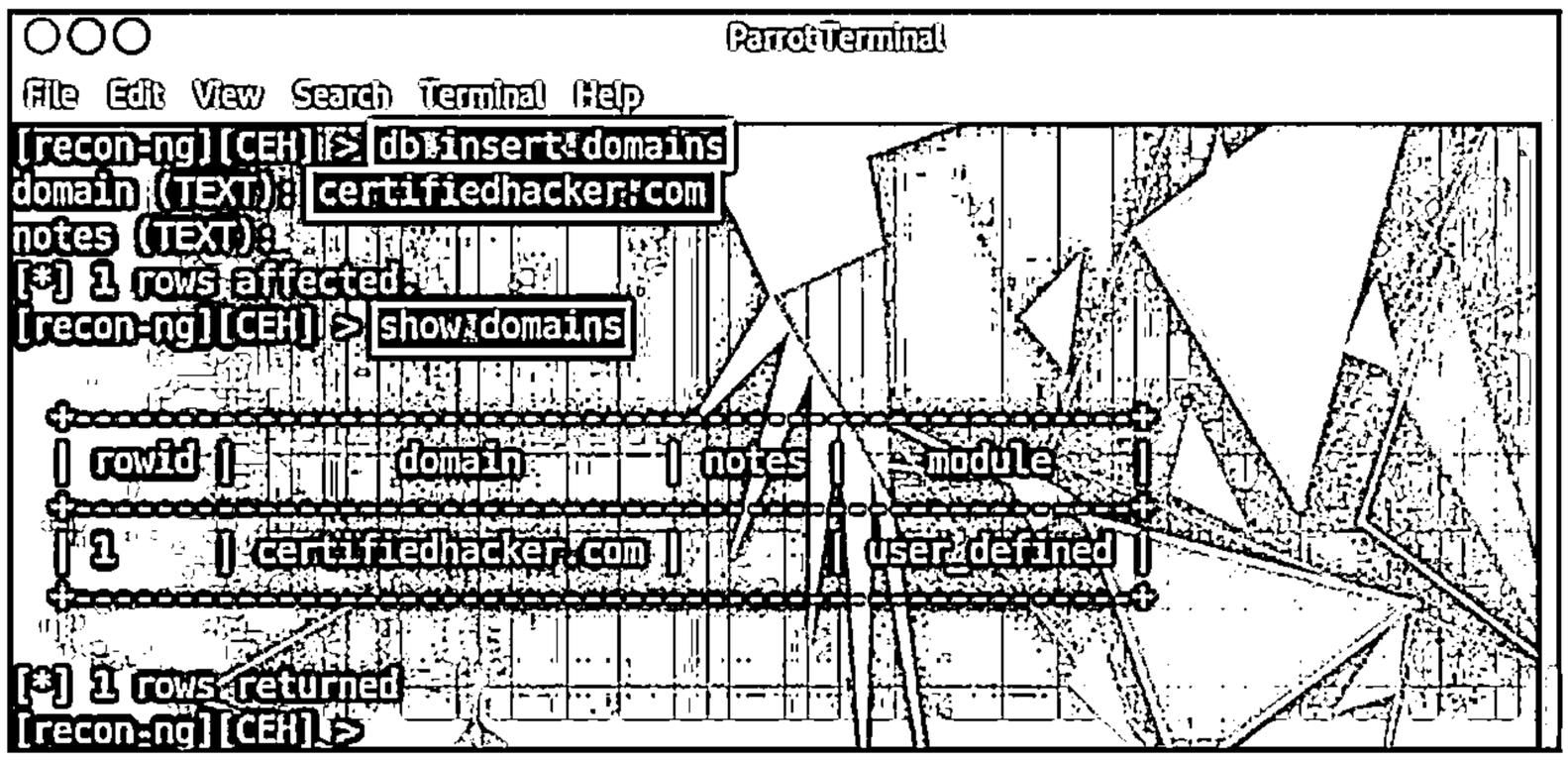


Figure 9.1.9: Viewing the Added Domain

20. Harvest the hosts-related information associated with **certifiedhacker.com** by loading network reconnaissance modules such as brute_hosts, Netcraft, and Bing.

TASK 1.3

Resolve Hosts Using brute_hosts Module

21. Type **modules load brute** and press **Enter** to view all the modules related to brute forcing. In this lab, we will be using the **recon/domains-hosts/brute_hosts** module to harvest hosts.

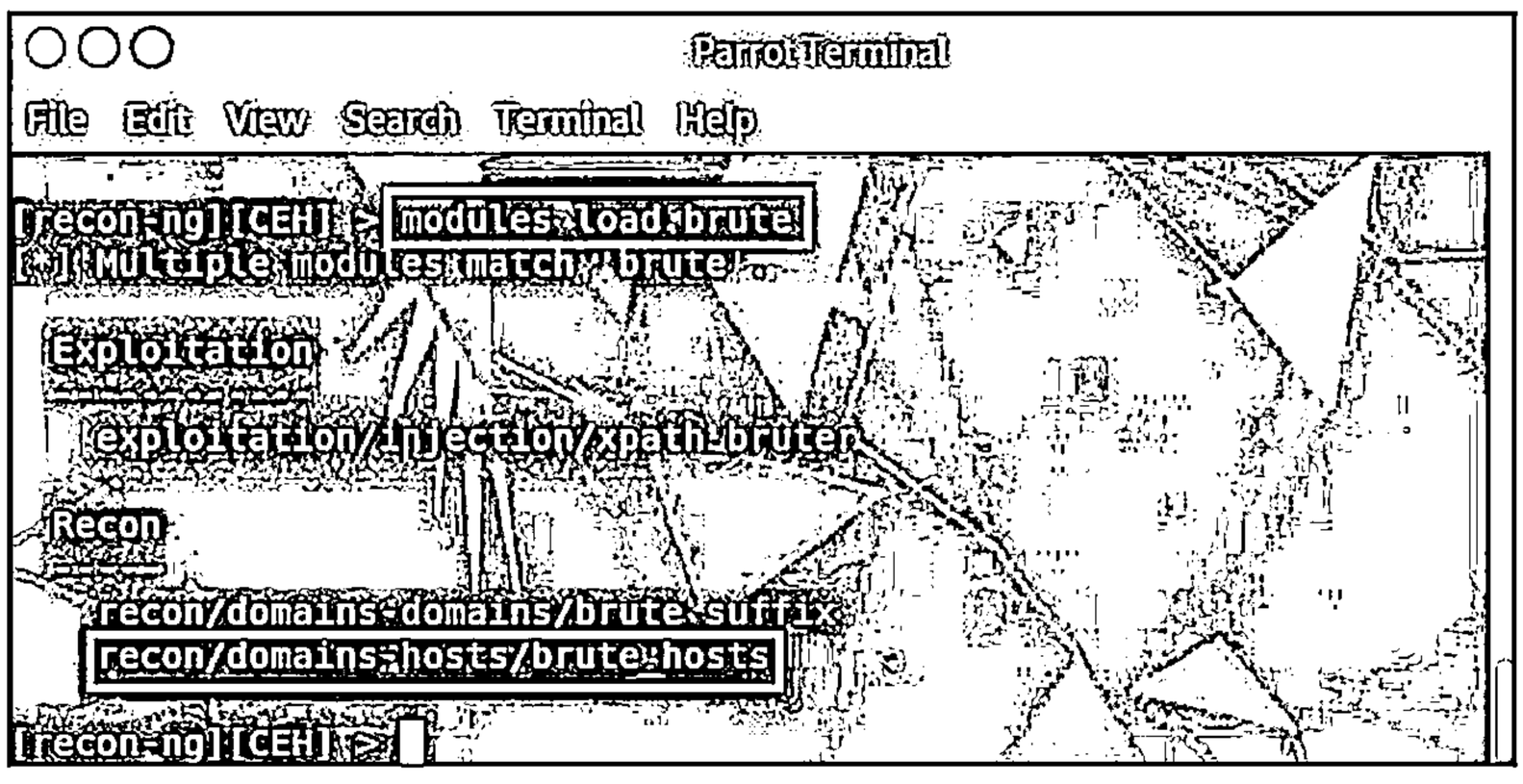


Figure 9.1.10: Searching for brute Module

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

22. To load the **recon/domains-hosts/brute_hosts** module, type the **modules load recon/domains-hosts/brute_hosts** command and press **Enter**.

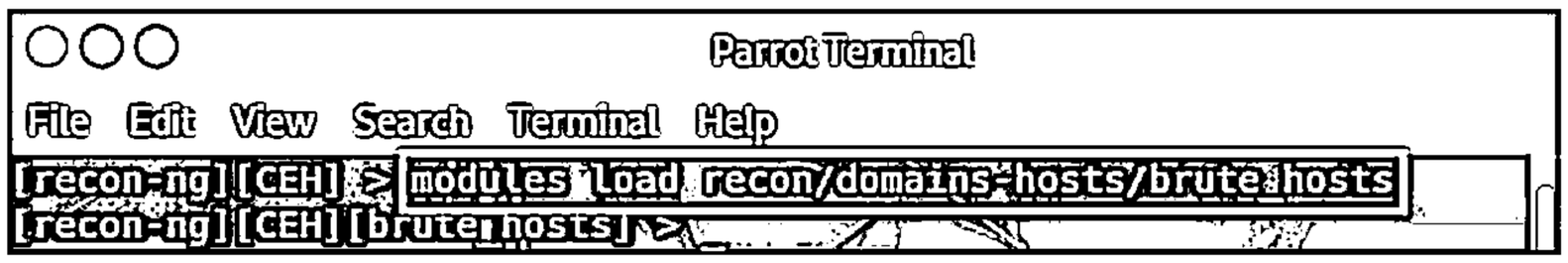


Figure 9.1.11: Loading brute Module

23. Type **run** and press **Enter**. This begins to harvest the hosts, as shown in the screenshot.

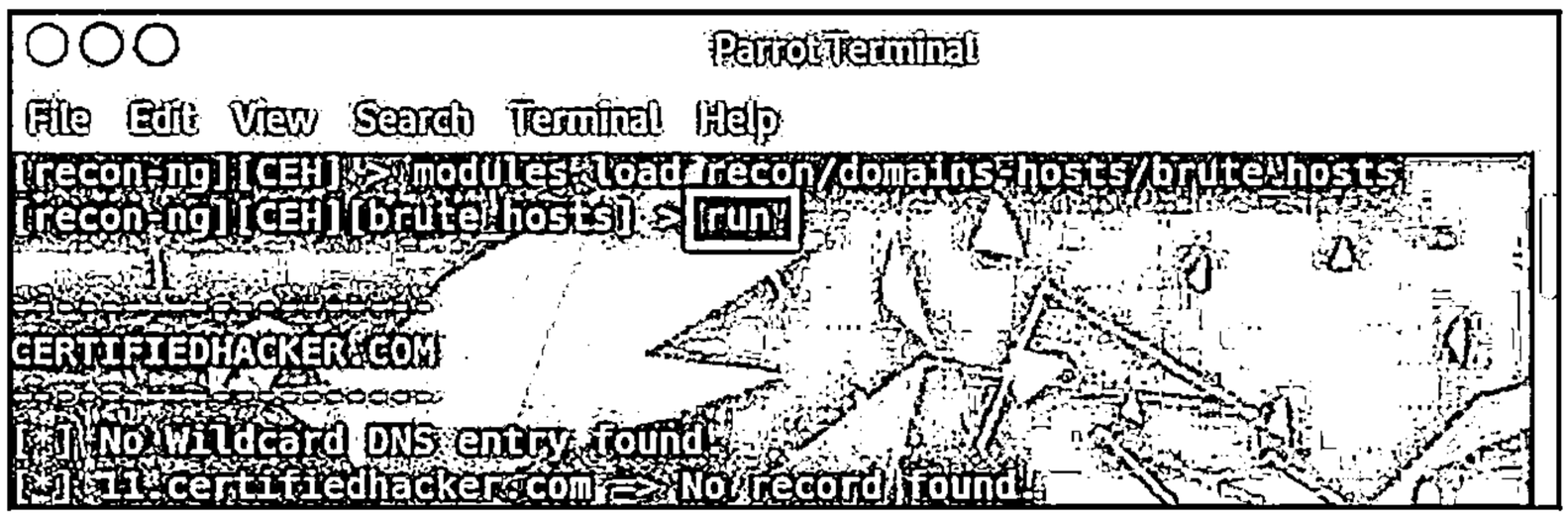


Figure 9.1.12: Running brute Module

24. Observe that hosts have been added by running the **recon/domains-hosts/brute_hosts** module.

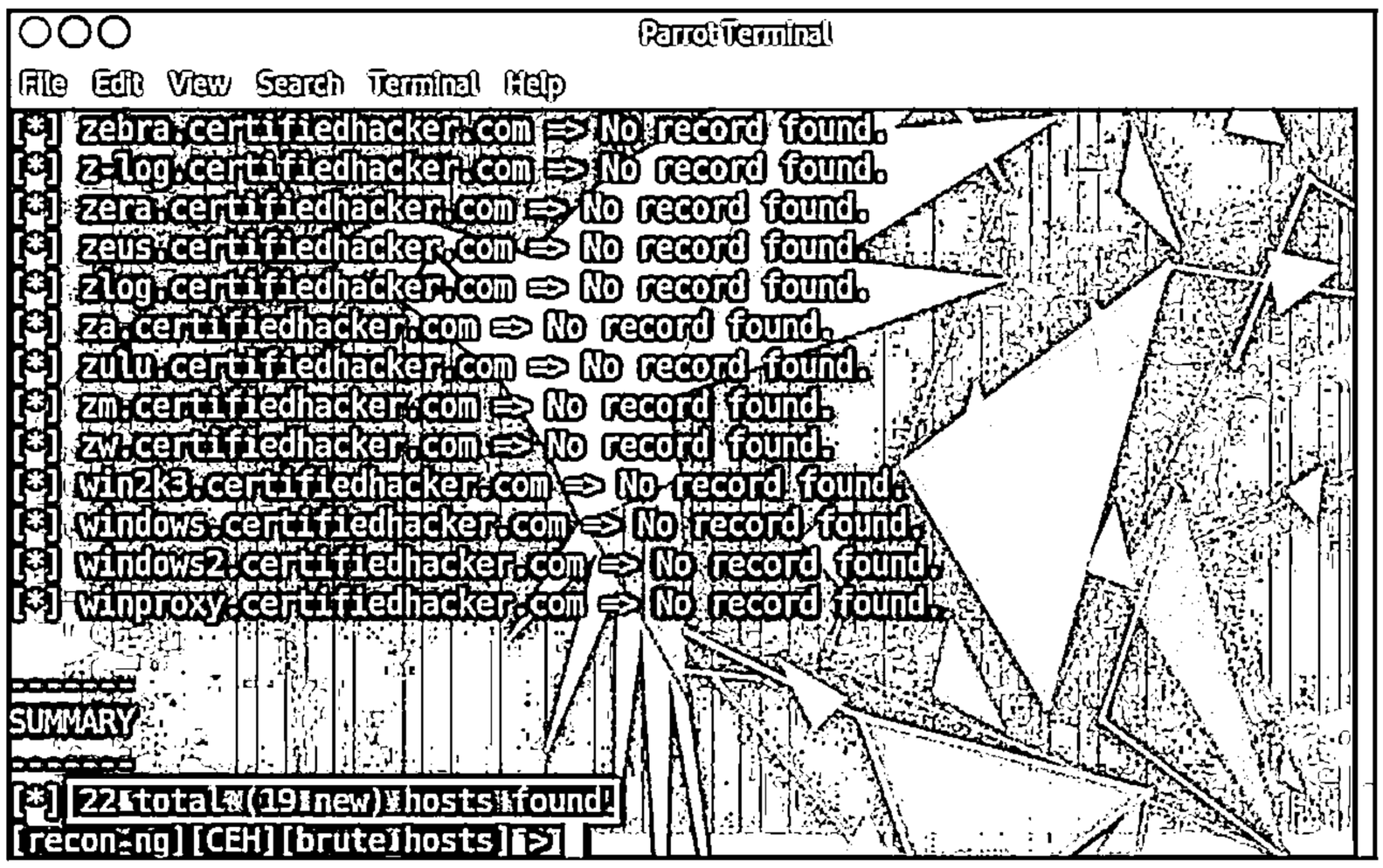


Figure 9.1.13: Newly Added Hosts

25. You have now harvested the hosts related to certifiedhacker.com using the brute_hosts module. You can use other modules such as Netcraft and Bing to harvest more hosts.

Note: Use the **back** command to go back to the CEH attributes terminal

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

To resolve hosts using the Bing module, use the following commands:

- **back**
- **modules load recon/domains-hosts/bing_domain_web**
- **run**

26. Now, perform a reverse lookup for each IP address (the IP address that is obtained during the reconnaissance process) to resolve to respective hostnames.

TASK 1.4

Perform Reverse Lookup Using reverse_resolve module

27. Type **modules load reverse_resolve** command and press **Enter** to view all the modules associated with the reverse_resolve keyword. In this lab, we will be using the **recon/hosts-hosts/reverse_resolve** module.
28. Type the **modules load recon/hosts-hosts/reverse_resolve** command and press **Enter** to load the module.

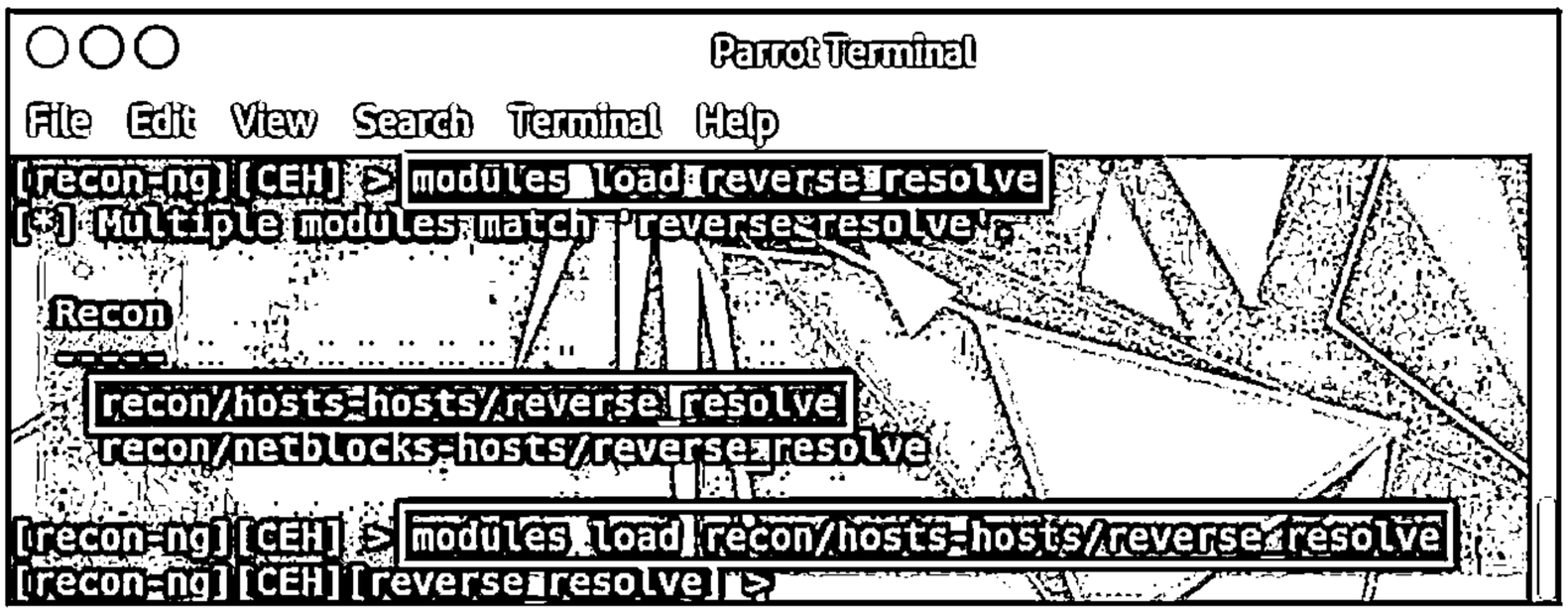


Figure 9.1.14: Search for reverse_resolve Module

29. Issue the **run** command to begin the reverse lookup

Note: Ignore the if any Syntax Error occurs.

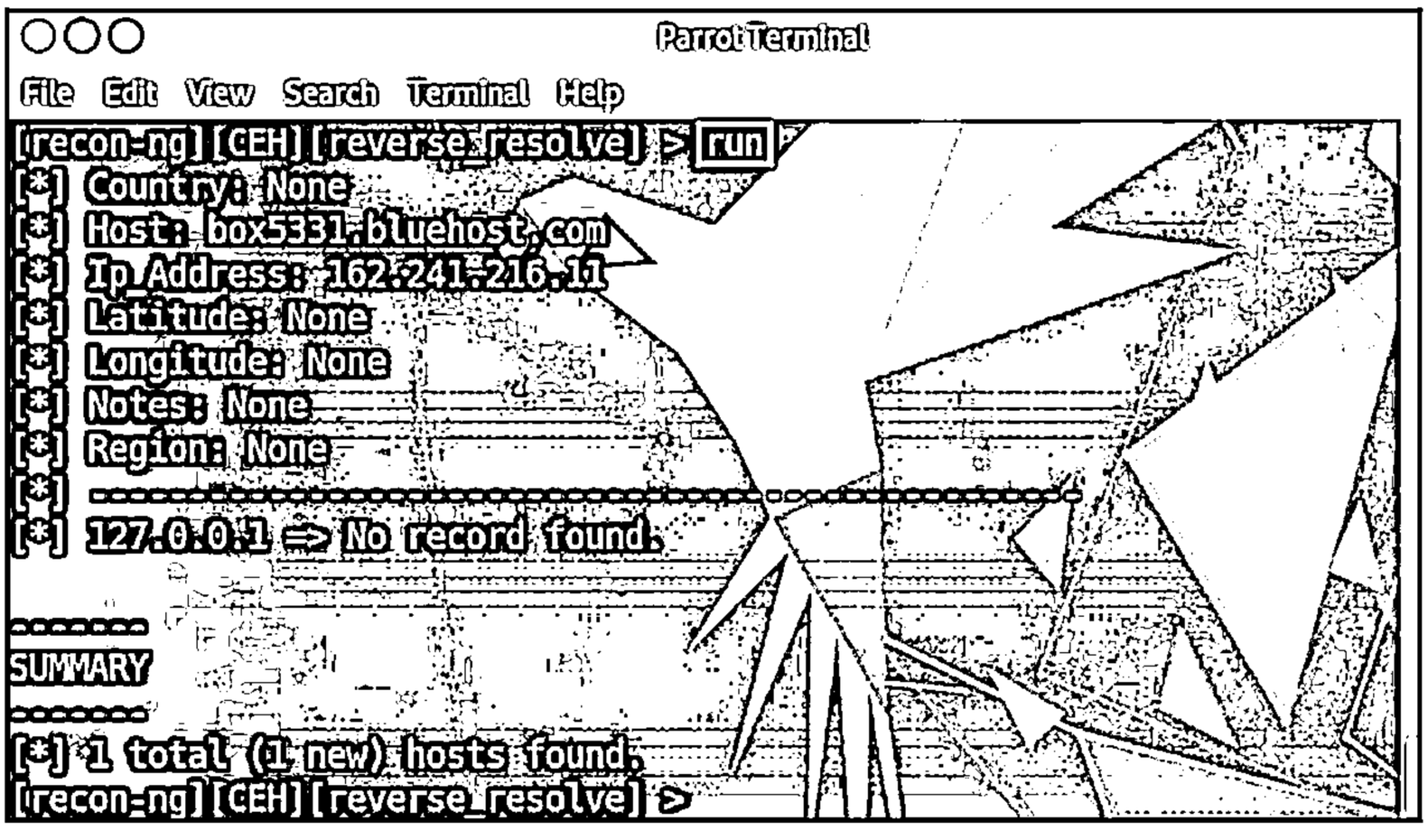


Figure 9.1.15: Running the Module

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

30. Once done with the reverse lookup process, type the **show hosts** command and press **Enter**. This displays all the hosts that are harvested so far, as shown in the screenshot.

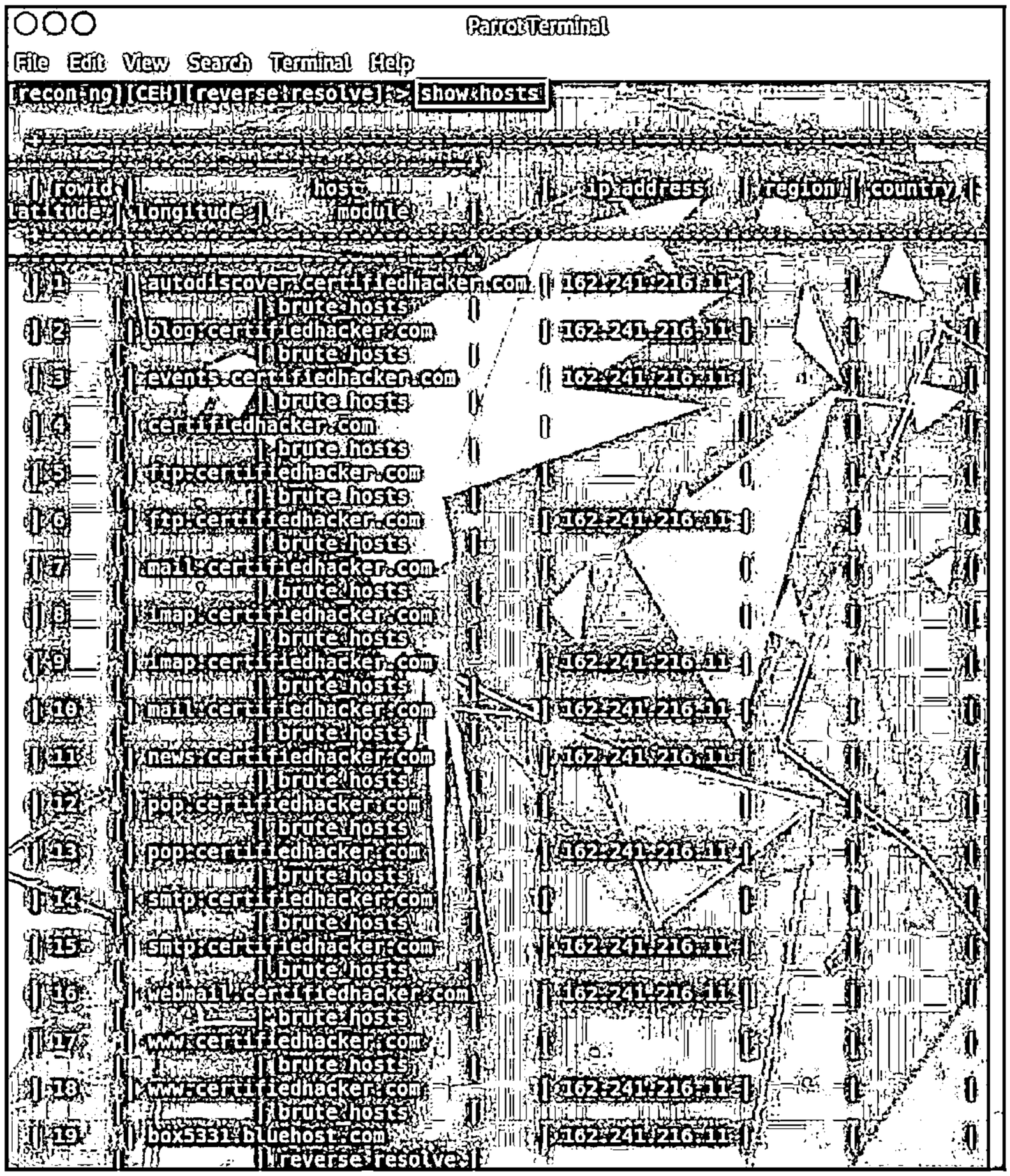


Figure 9.1.16: Viewing the Harvested Hosts

31. Now, type the **back** command and press **Enter** to go back to the **CEH** attributes terminal

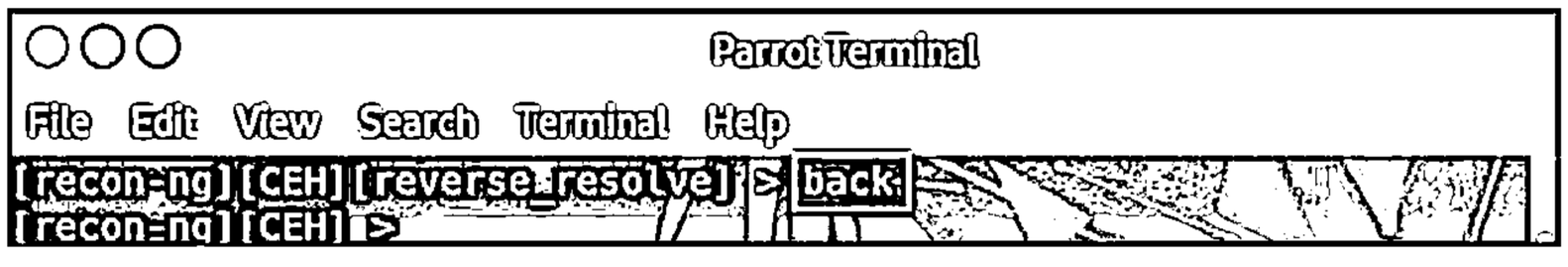


Figure 9.1.17: Going back to the Attributes Section

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

TASK 1.5

Generate a Report

32. Now, that you have harvested several hosts, we will prepare a report containing all the hosts.
33. Type the **modules load reporting** command and press **Enter** to view all the modules associated with the reporting keyword. In this lab, we will save the report in HTML format. So, the module used is **reporting/html**.

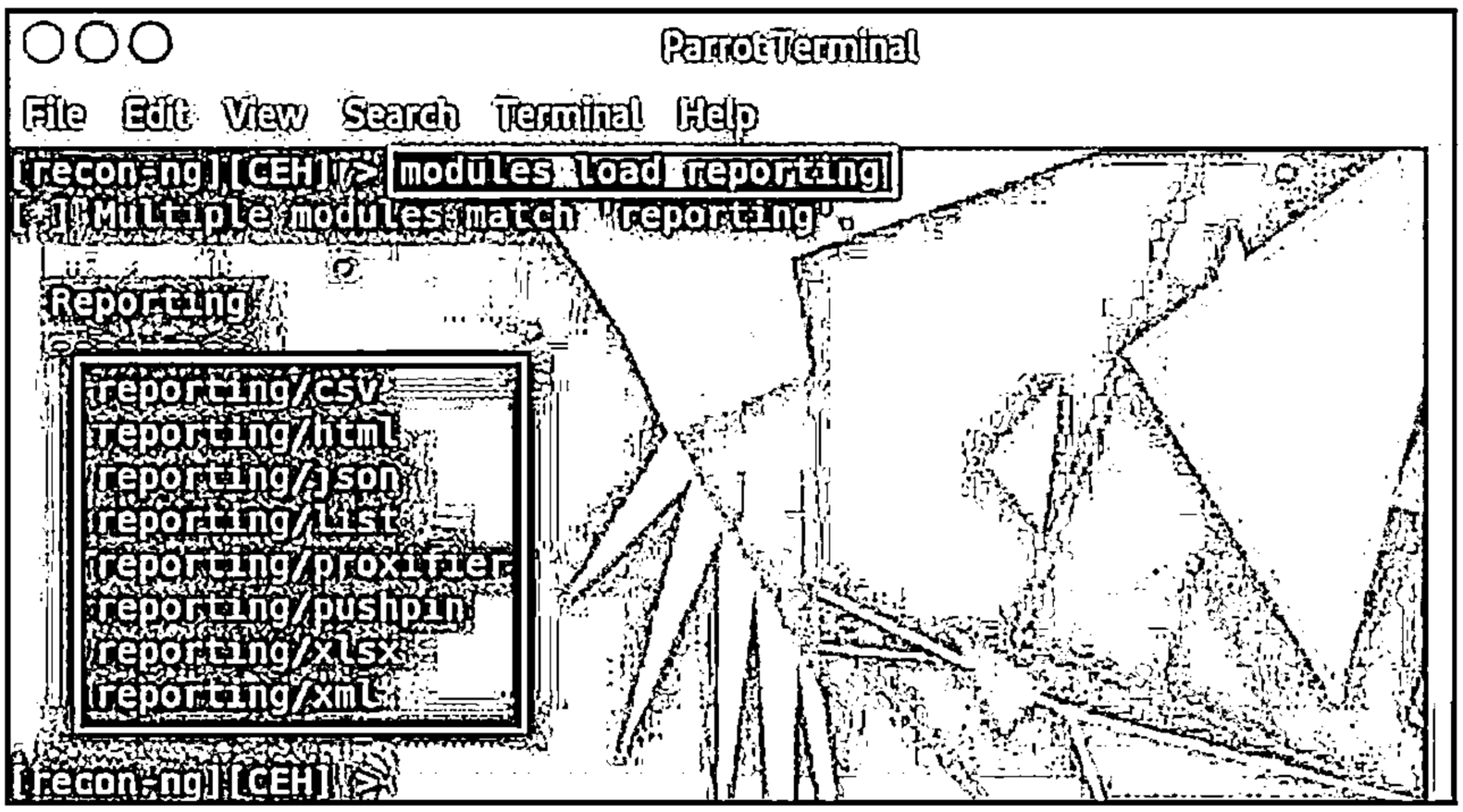


Figure 9.1.18: Searching for reporting Module

34. Type the **modules load reporting/html** command and press **Enter**.
35. Observe that you need to assign values for **CREATOR** and **CUSTOMER** options while the **FILENAME** value is already set, and you may change the value if required.
36. Type:
    a. **options set FILENAME /root/Desktop/results.html** and press **Enter.** By issuing this command, you are setting the report name as **results.html** and the path to store the file as **Desktop**.
    b. **options set CREATOR [your name]** (here, **Jason**) and press **Enter.**
    c. **options set CUSTOMER Certifiedhacker Networks** (since you have performed network reconnaissance on **certifiedhacker.com** domain) and press **Enter.**

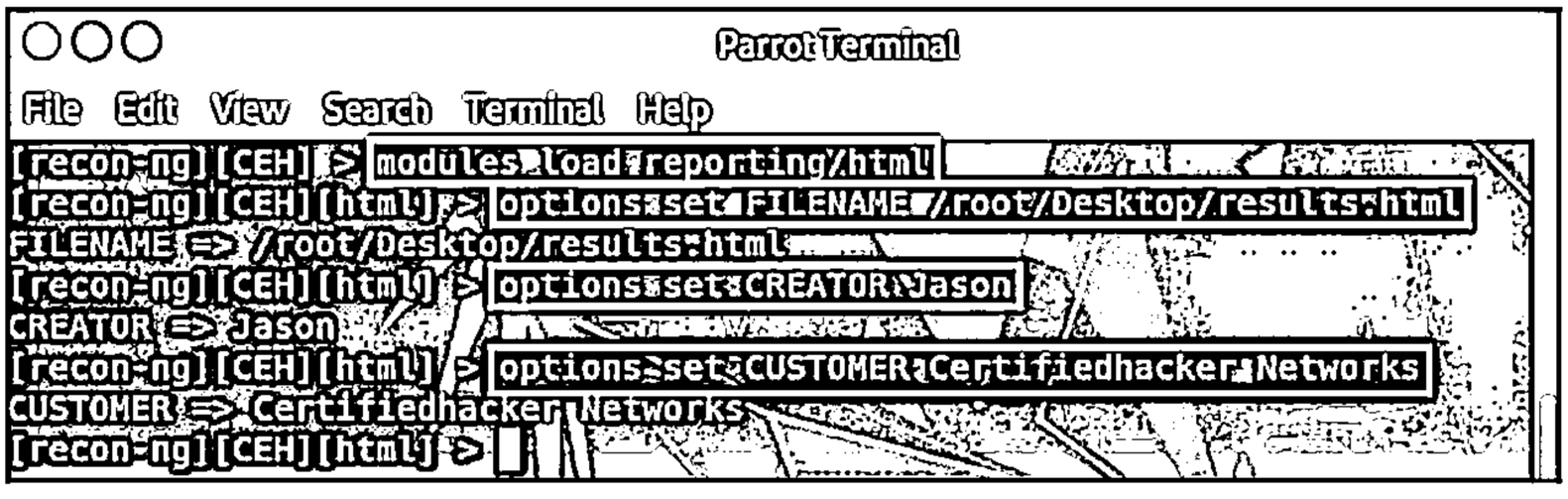


Figure 9.1.19: Saving a Report

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

37. Type the **run** command and press **Enter** to create a report for all the hosts that have been harvested.

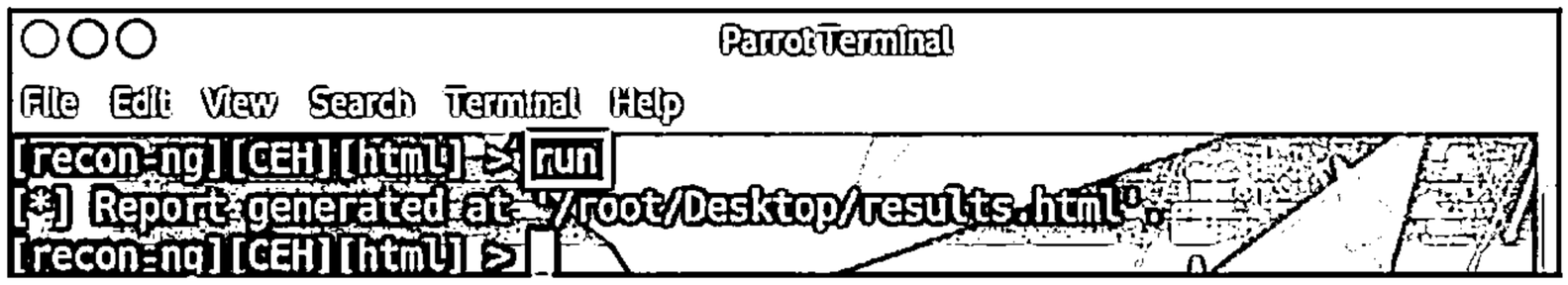


Figure 9.1.20: Running the Module

38. Click **Places** from the top-section of the **Desktop** and click **Home Folder** from the drop-down options.

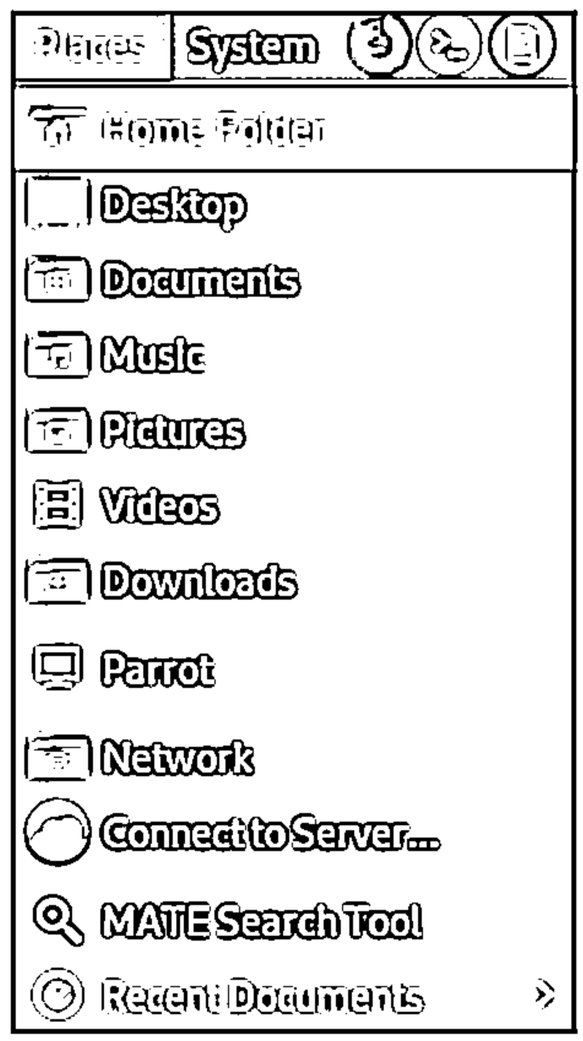


Figure 9.1.21: Navigate to the Home Folder

39. The **attacker** window appears, click **File System** from the left-pane and navigate to the location **root/Desktop**.
40. The generated report is saved to **/root/Desktop/**. Navigate to the location, right-click on the **results.html** file, click on **Open With**, and select the **Firefox** browser from the available options.

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

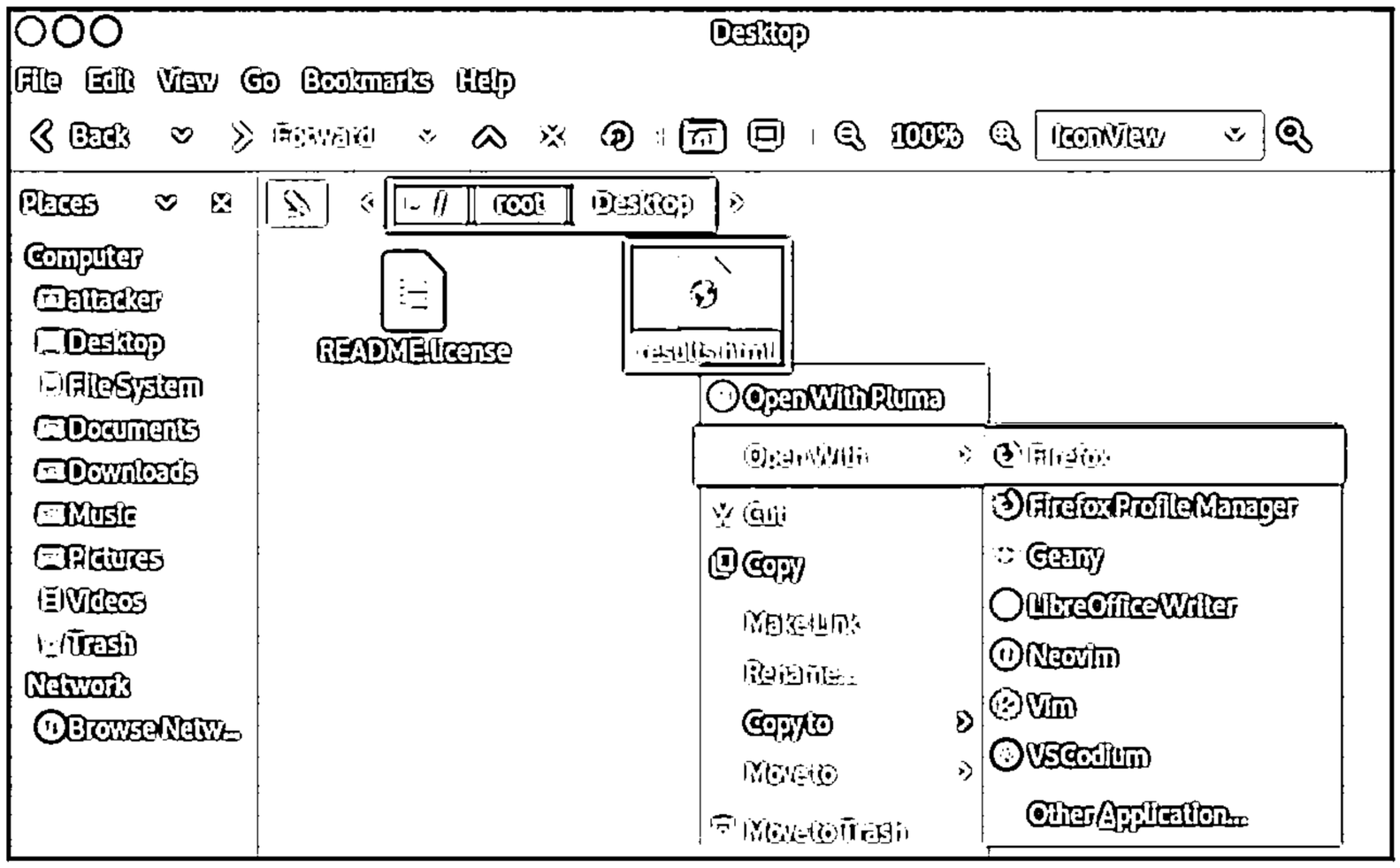


Figure 9.1.22: Viewing the Report

41. The generated report appears in the **Firefox** browser, displaying the summary of the harvested hosts.

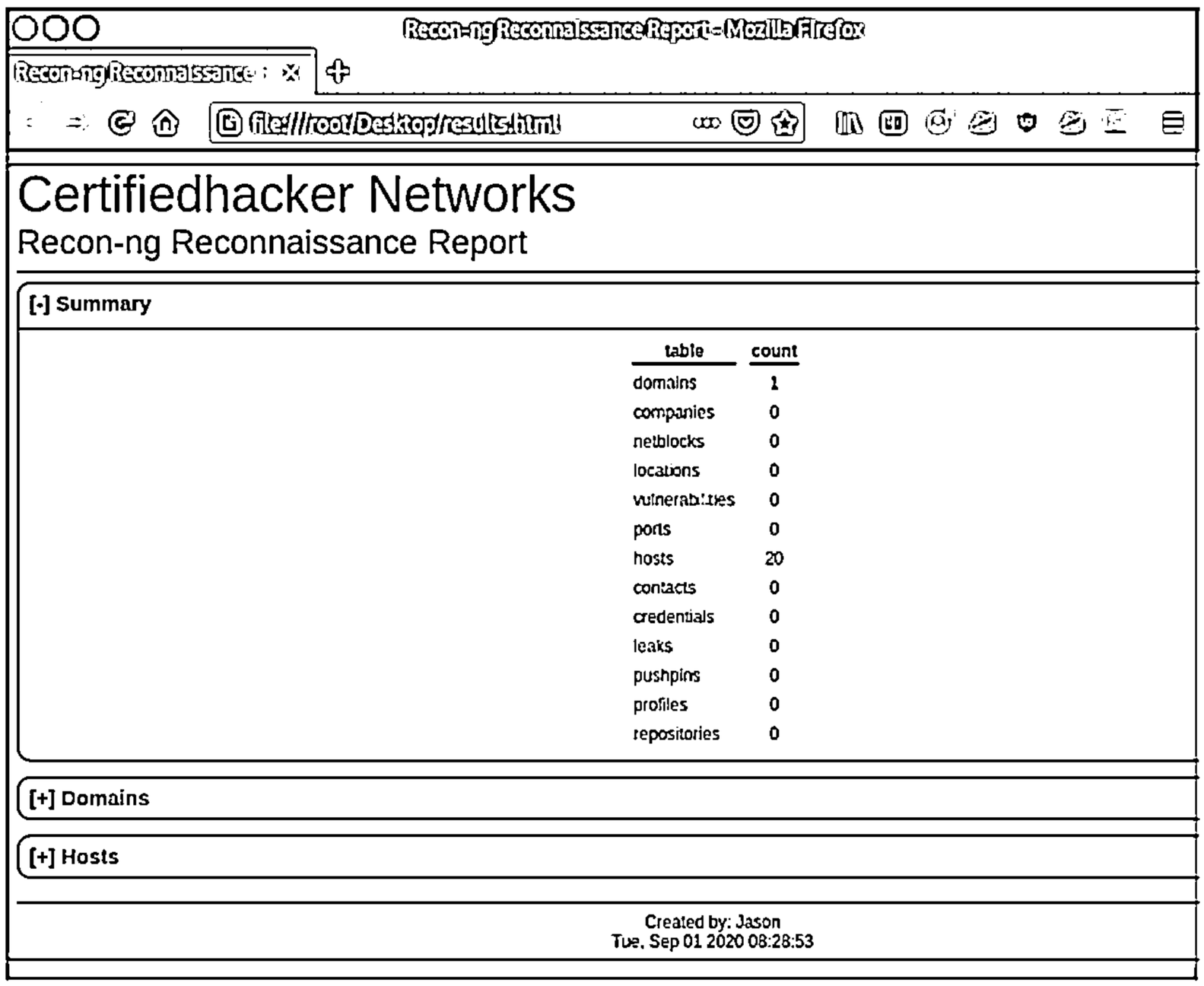


Figure 9.1.23: Viewing the Report

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

42. You can expand the **Hosts** node to view all the harvested hosts, as shown in the screenshot.

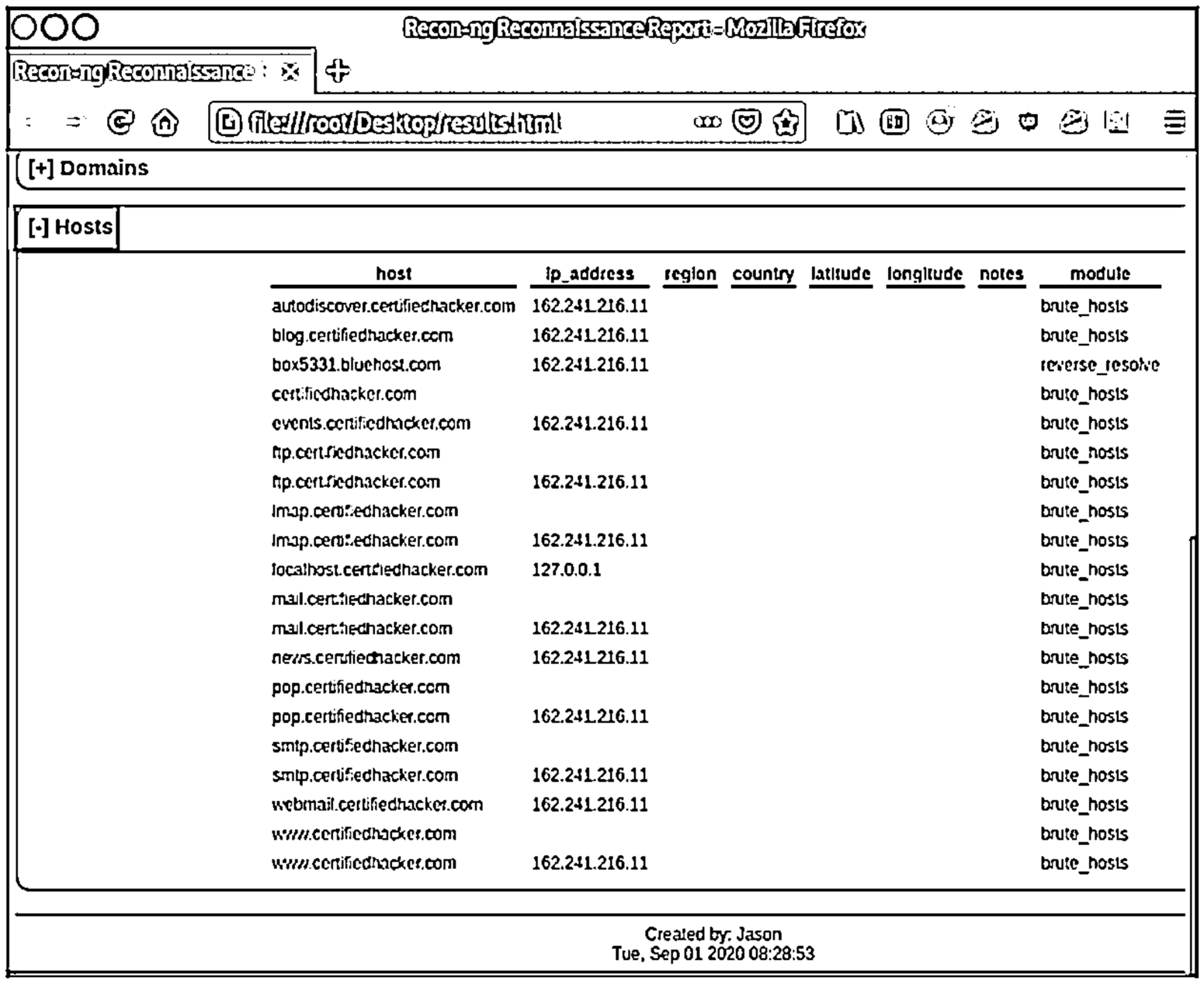


Figure 9.1.24: Expanding Hosts tab

43. Close the **Firefox** window.
44. Until now, we have used the Recon-ng tool to perform network reconnaissance on a target domain.

TASK 1.6

Create a Workspace

45. Now, we will use Recon-ng to gather personnel information.
46. Open a new **Parrot Terminal** window, type **sudo su** and press **Enter** to run the programs as a root user.
47. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**. Type **cd** and press **Enter** to jump to the root directory.
48. Now, type **recon-ng**, and press **Enter**.

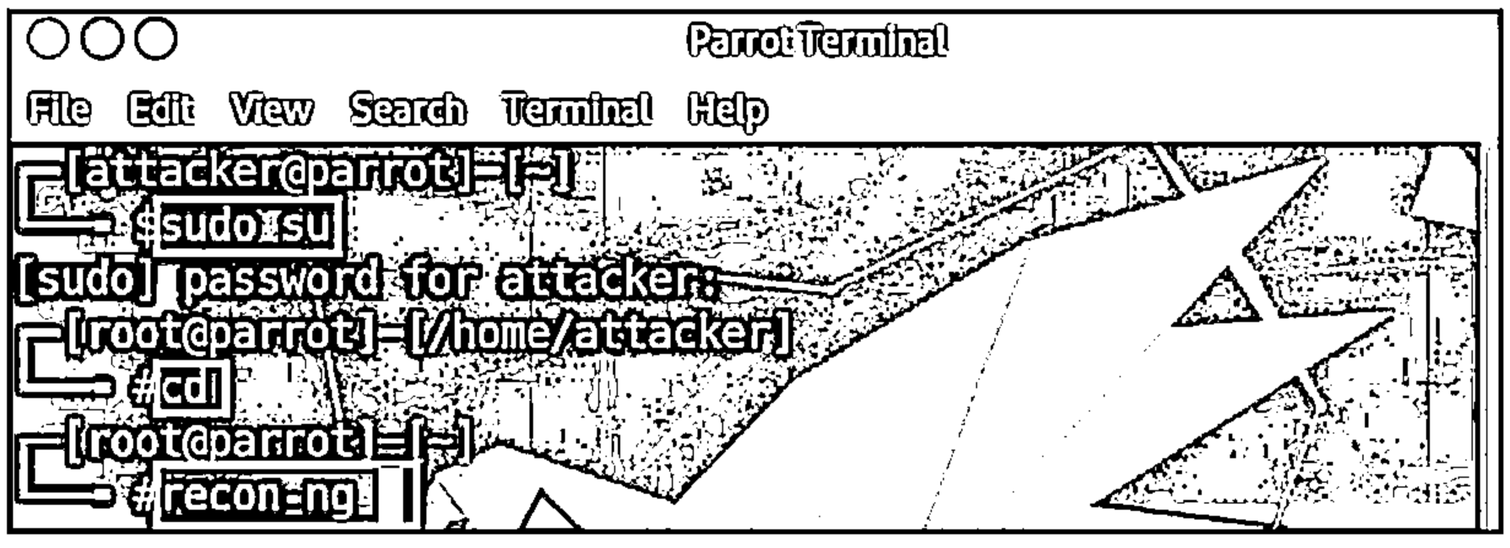


Figure 9.1.25: Launch recon-ng

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

49. Add a workspace by issuing the command **workspaces create reconnaissance** and press **Enter**. This creates a workspace named reconnaissance.

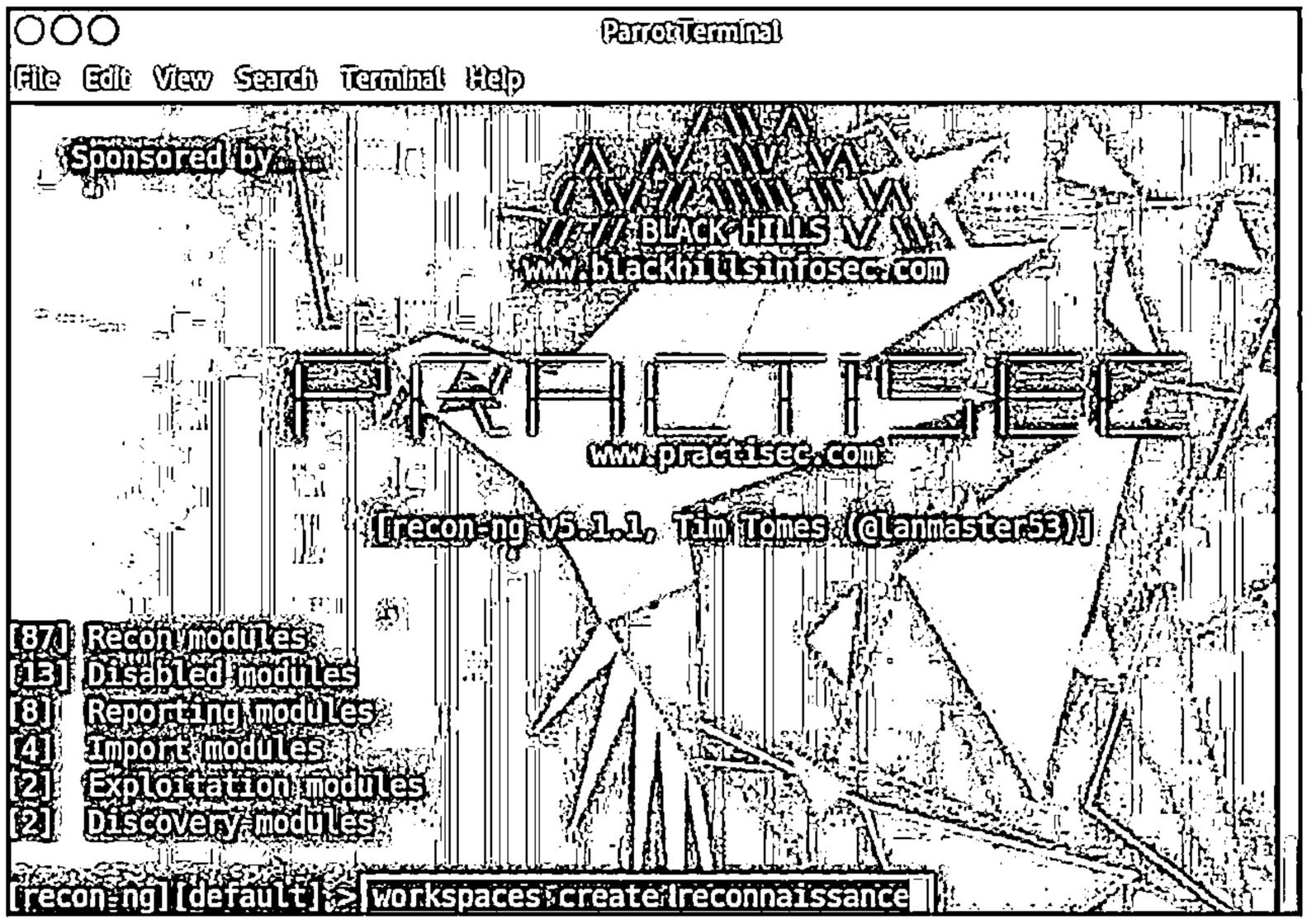


Figure 9.1.26: Launching recon-ng

TASK 1.7

Gather Contacts Associated with a Domain

50. Set a domain and perform footprinting on it to extract contacts available in the domain.
51. Type **modules load recon/domains-contacts/whois_pocs** and press **Enter**. This module uses the ARIN Whois RWS to harvest POC data from Whois queries for the given domain.
52. Type the **info** command and press **Enter** to view the options required to run this module.
53. Type **options set SOURCE facebook.com** and press **Enter** to add facebook.com as a target domain.

Note: Here, we are using facebook.com as a target domain to gather contact details.

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

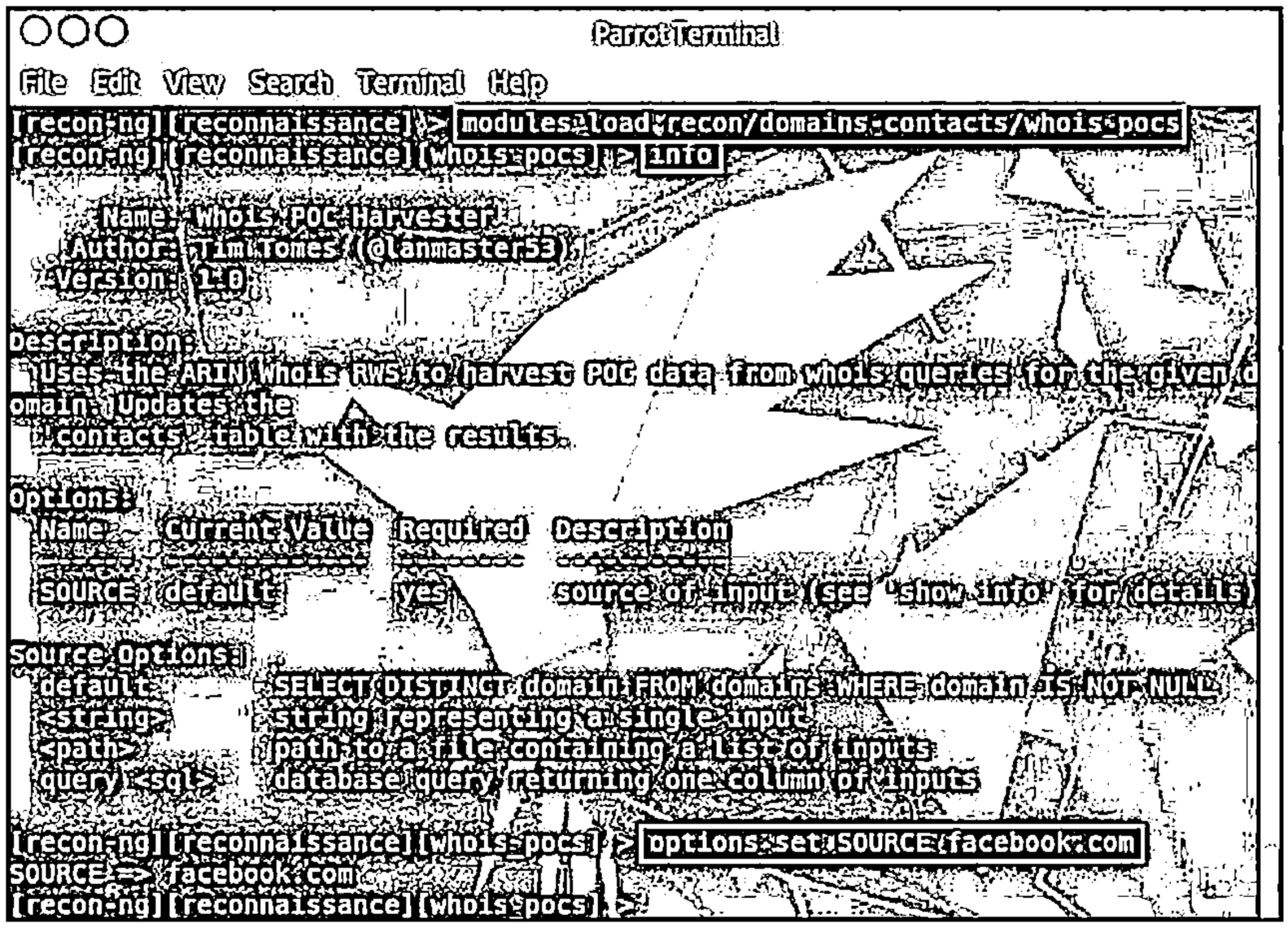


Figure 9.1.27: Harvesting Contacts from Domain

54. Type the **run** command and press **Enter**. The **recon/domains-contacts/whois_pocs** module extracts the contacts associated with the domain and displays them, as shown in the screenshot.

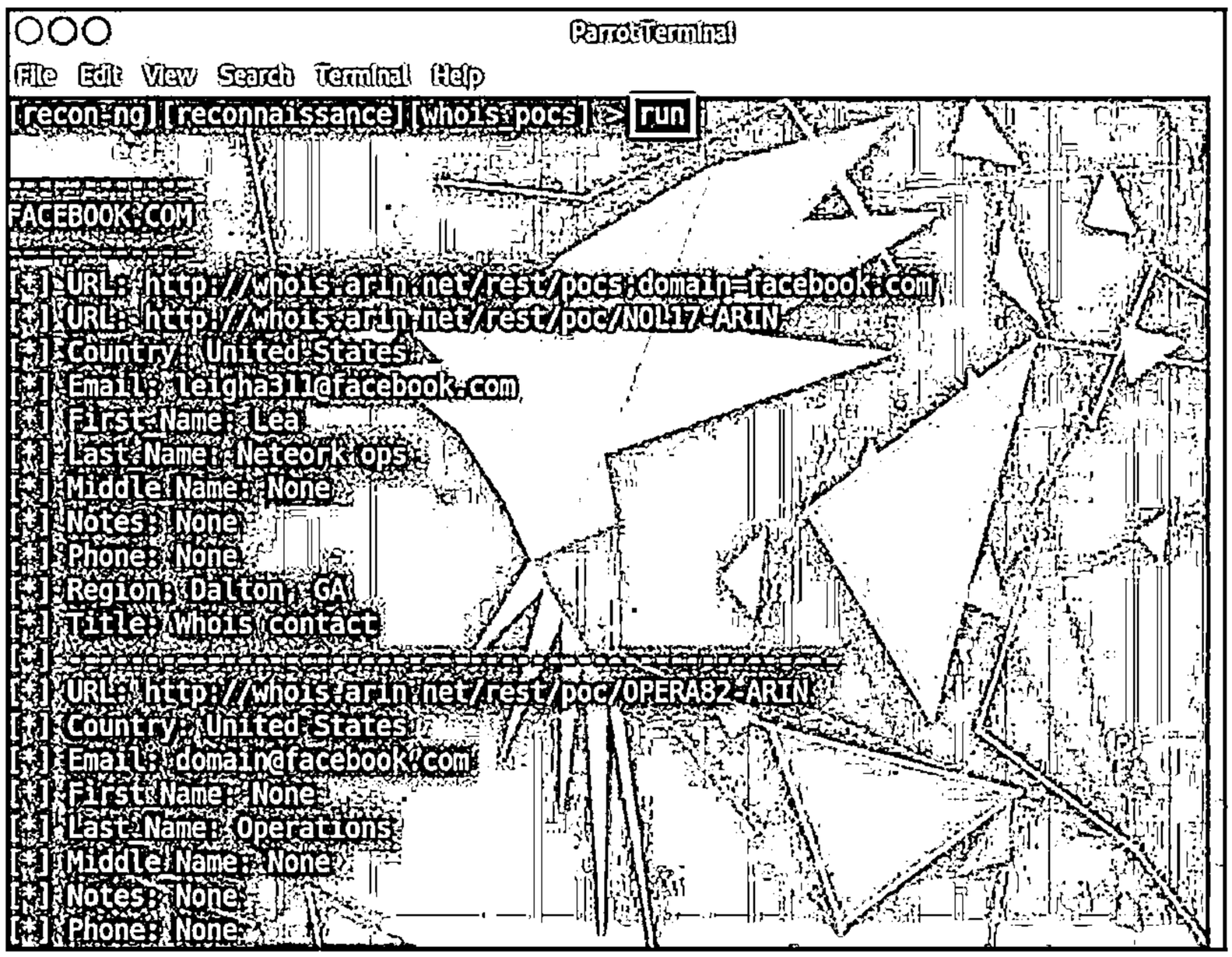


Figure 9.1.28: Running Module

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

55. Type **back** and press **Enter** to go back to the workspaces (**reconnaissance**) terminal

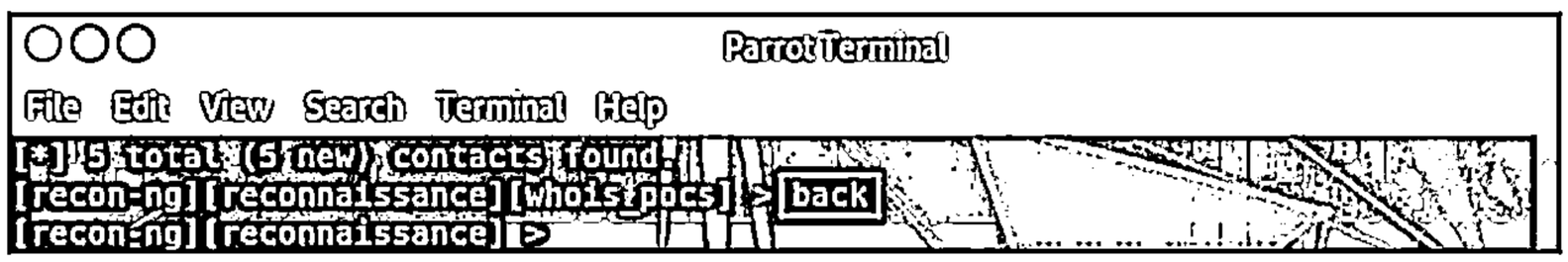


Figure 9.1.29: Going back to workspaces terminal

TASK 1.8

Check for User Existence

56. Until now, we have obtained contacts related to the domains. Note down these contacts' names
57. Now, we will validate the existence of names (usernames) on specific websites.
58. The **recon/profiles-profiles/namechk** module validates the username existence of a specified contact. The contact we will use in this lab is **Mark Zuckerberg**.
59. Type the **modules load recon/profiles-profiles/namechk** command and press **Enter** to load this module
60. Type **options set SOURCE MarkZuckerberg** and press **Enter**. This command sets MarkZuckerberg as the source for which you want to find the user existence on specific websites.
61. Type **run** and press **Enter**. This begins the search for the keyword MarkZuckerberg on various websites.
62. Recon-ng begins to search the Internet for the presence of the username on websites and, if found, it returns the result stating "**User Exists!**".

Note: Here, no results are obtained.

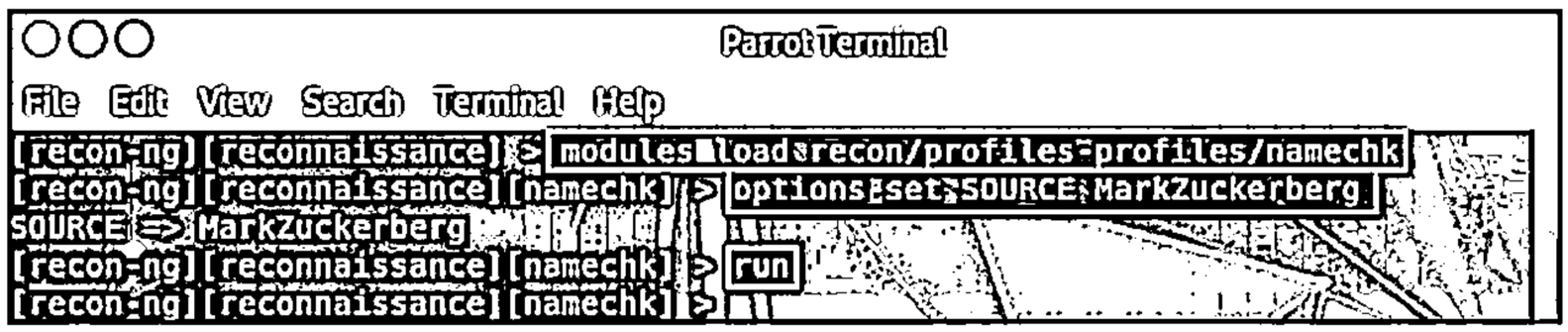


Figure 9.1.30: Running a Module

63. Type the **back** command and press **Enter** to go back to the workspaces (reconnaissance) terminal.

TASK 1.9

Check for Profile Existence

64. To find the existence of user-profiles on various websites, you need to load the **recon/profiles-profiles/profiler** module.
65. Type the **modules load recon/profiles-profiles/profiler** command and press **Enter**

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

66. Type the **options set SOURCE MarkZuckerberg** command and press **Enter.**

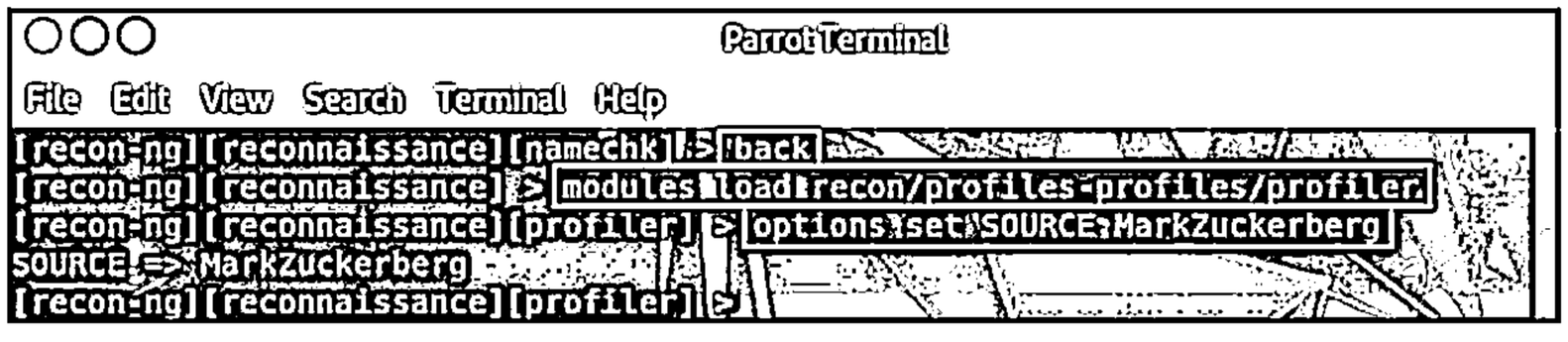


Figure 9.1.31: Configuring Module

67. Type the **run** command and press **Enter.** The recon/profiles-profiles/profiler module searches for this username and returns the URL of the profile (found with the matching username):

Note: Ignore the Errors.

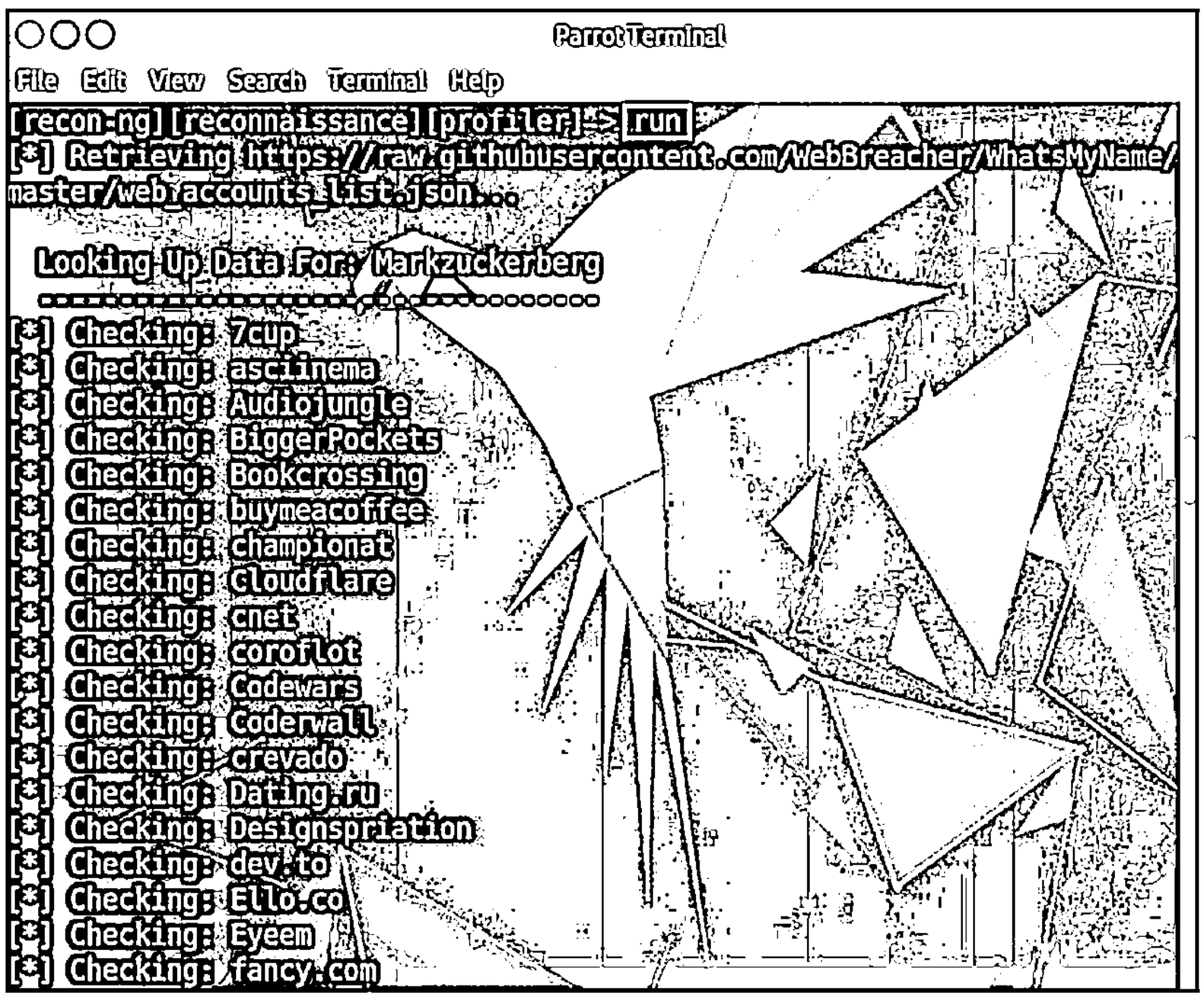


Figure 9.1.32: Running Module

TASK 1.10

Generate a Report

68. Type **back** and press **Enter** to go back to the workspaces terminal.
69. Now that we have verified the user existence and obtained the profile URL, we will prepare a report containing the result.
70. Type the **modules load reporting/html** command and press **Enter.** Assign values for **FILENAME, CREATOR**, and **CUSTOMER.**

Note: In this lab, we are saving the report in HTML format; therefore, **reporting/html** module is used.

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

71. Type:

    - **options set FILENAME /root/Desktop/Reconnaissance.html** and press **Enter**. By issuing this command, you are setting the report name as **Reconnaissance**.

    Note: Here, the Reconnaissance.html is saved at location **/root/Desktop/**

    - **options set CREATOR [your name]** (here, **Jason**) and press **Enter**
    - **options set CUSTOMER Mark Zuckerberg** (since you have performed information gathering on the name of **Mark Zuckerberg**) and press **Enter**.

72. After entering the above details, type the **run** command and press **Enter** to create a report for all the hosts that have been harvested, as shown in the screenshot.

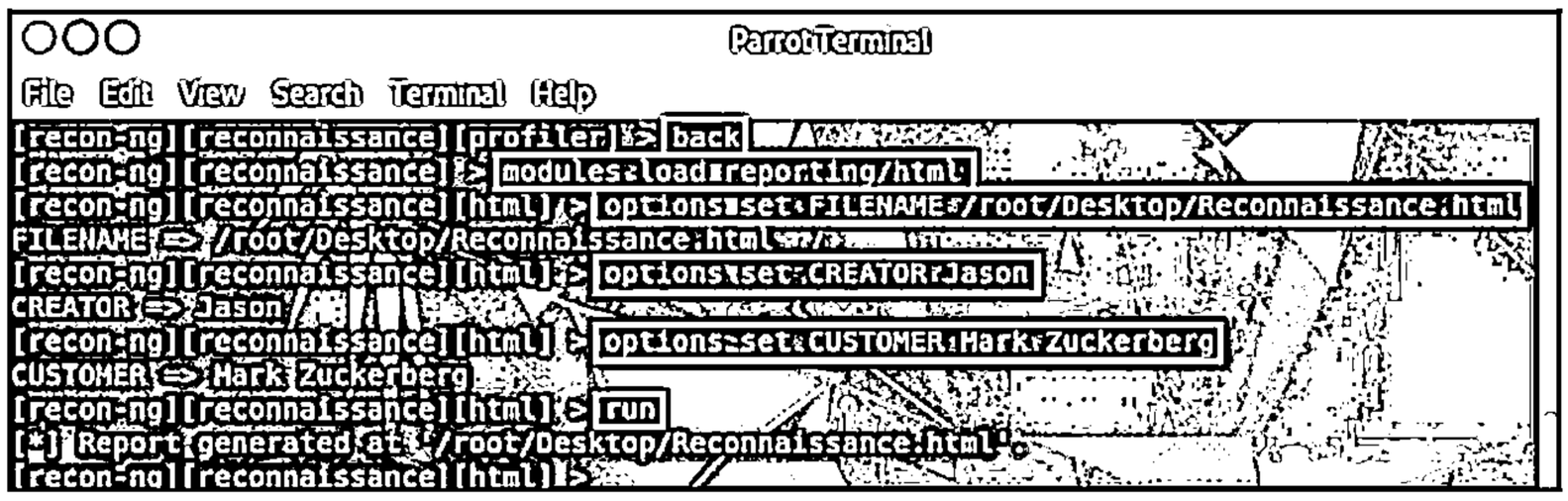


Figure 9.1.33: Configuring and running the Report module

73. The generated report is saved to **/root/Desktop/**. Navigate to the location, right-click on the **Reconnaissance.html** file, click on **Open With**, and select the **Firefox** browser from the available options.

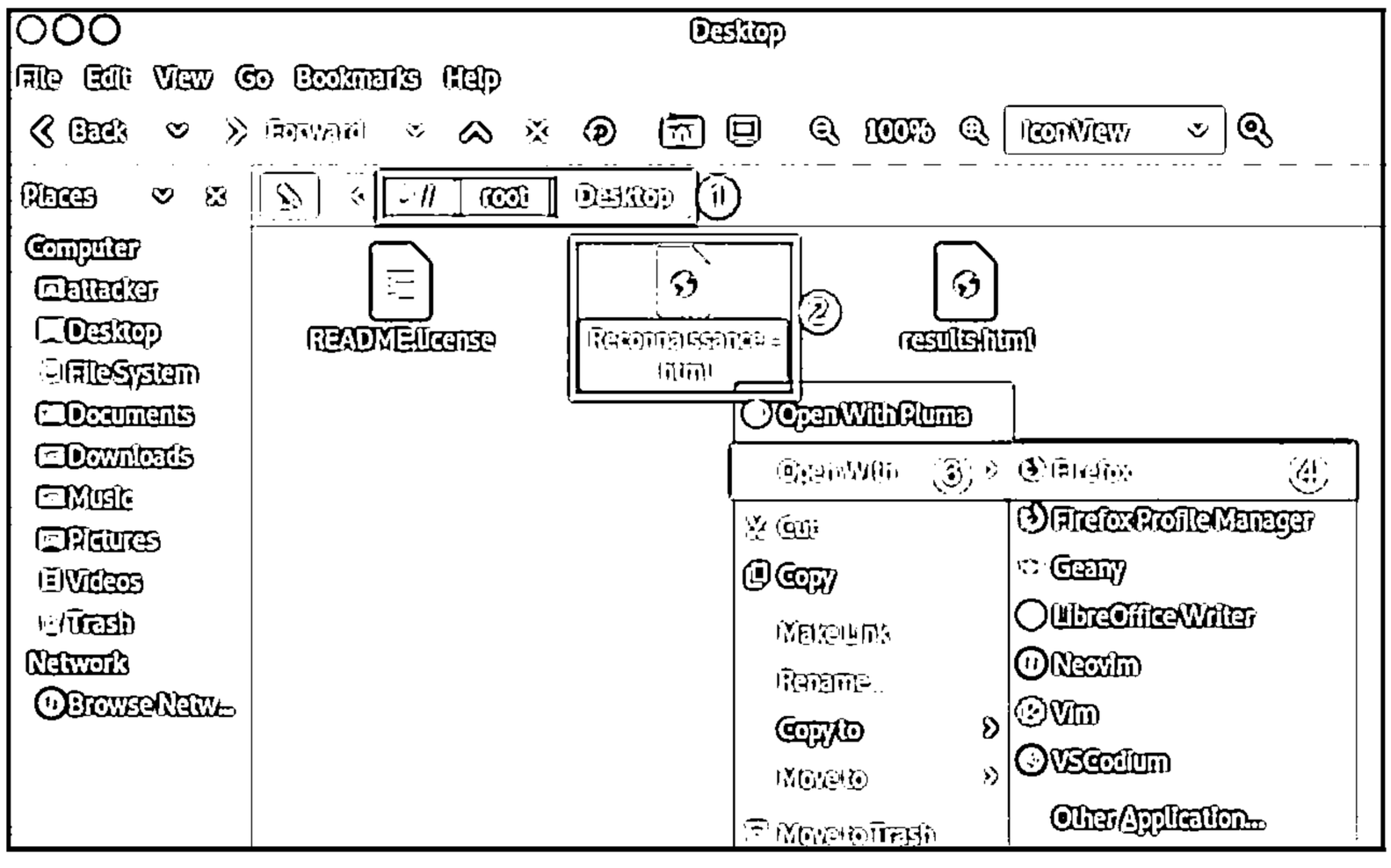


Figure 9.1.34: Viewing the Report

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

74. The generated report appears in the **Firefox** browser, displaying a summary of the result. You can expand the **Contacts** and **Profiles** nodes to view all the obtained results.

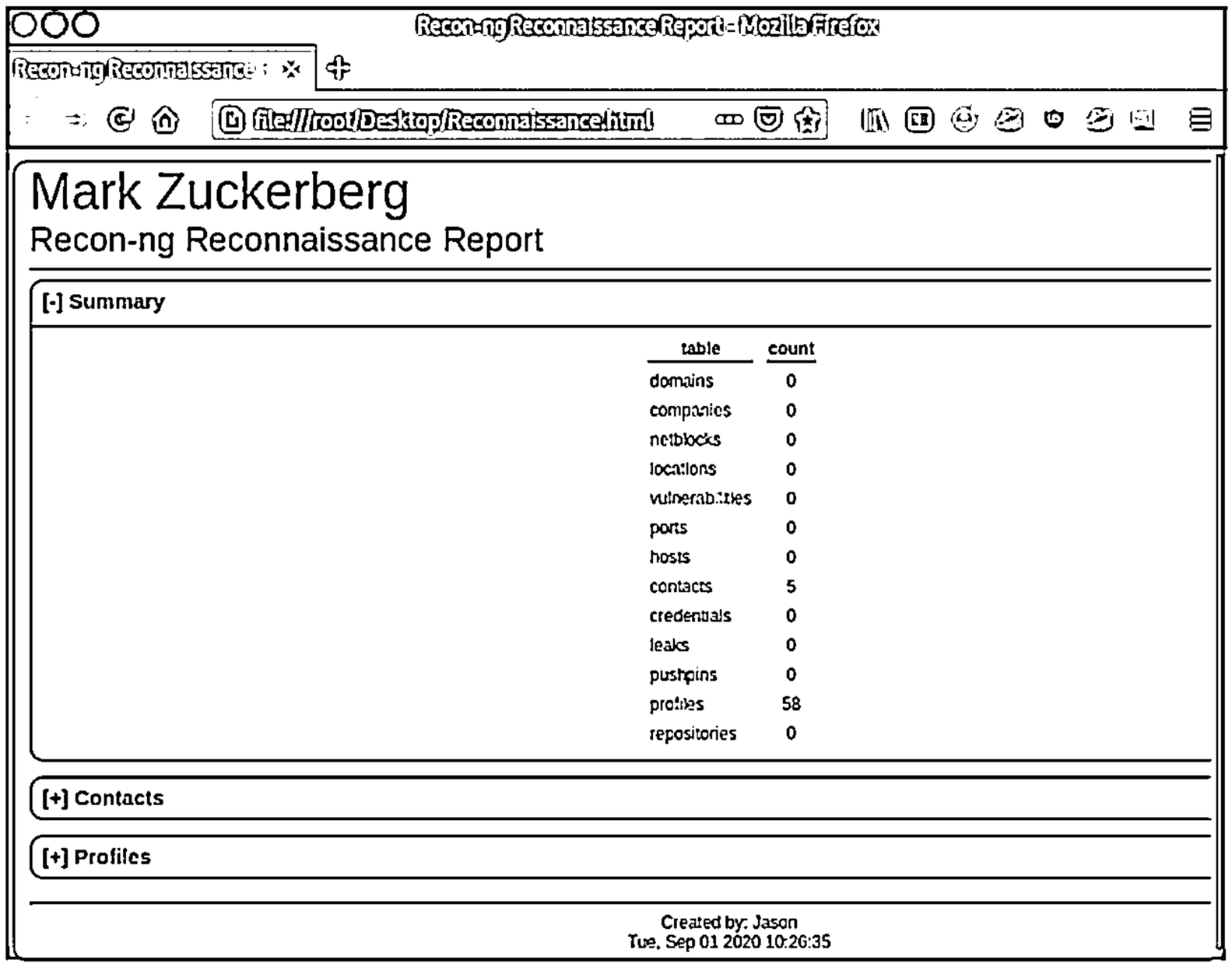


Figure 9.1.35: Viewing the Report

75. You can further expand the **Contacts** and **Profiles** node to view detailed information about the target.

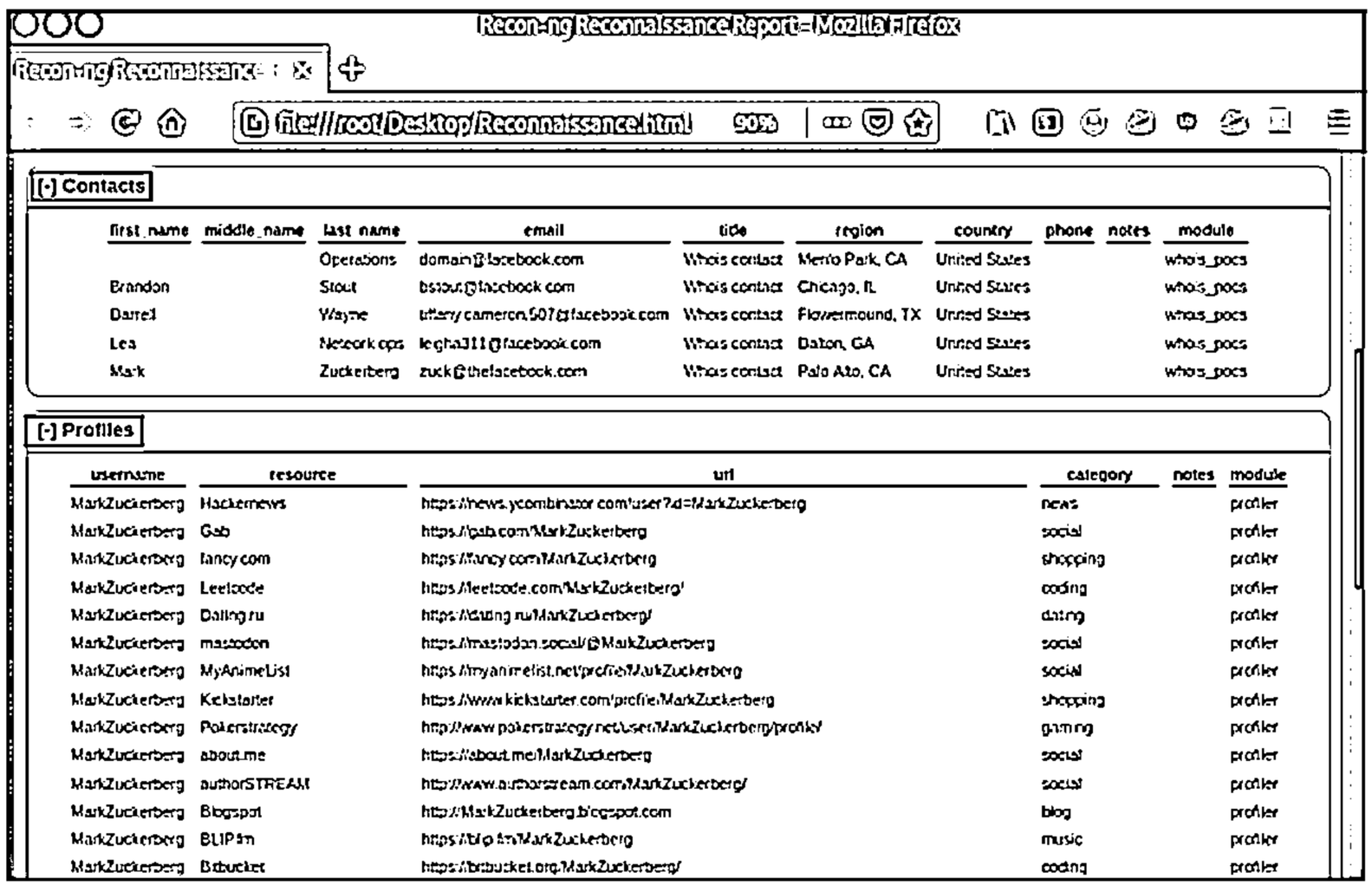


Figure 9.1.36: Expand Contacts and Profiles

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

76. We have now gathered information about the employee working in a target organization.
77. This concludes the demonstration of gathering host information of the target domain and gathering personnel information of a target organization.
78. Close all open windows and document all the acquired information.

TASK 2 Footprinting a Target using Maltego

Here, we will gather a variety of information about the target organization using Maltego.

TASK 2.1

Configure Maltego

1. In the **Parrot Security** virtual machine, launch **Maltego** by navigating to **Applications → Pentesting → Information Gathering → maltego**, as shown in the screenshot.

Maltego is a footprinting tool used to gather maximum information for the purpose of ethical hacking, computer forensics, and pentesting. It provides a library of transforms to discover data from open sources and visualizes that information in a graph format, suitable for link analysis and data mining.

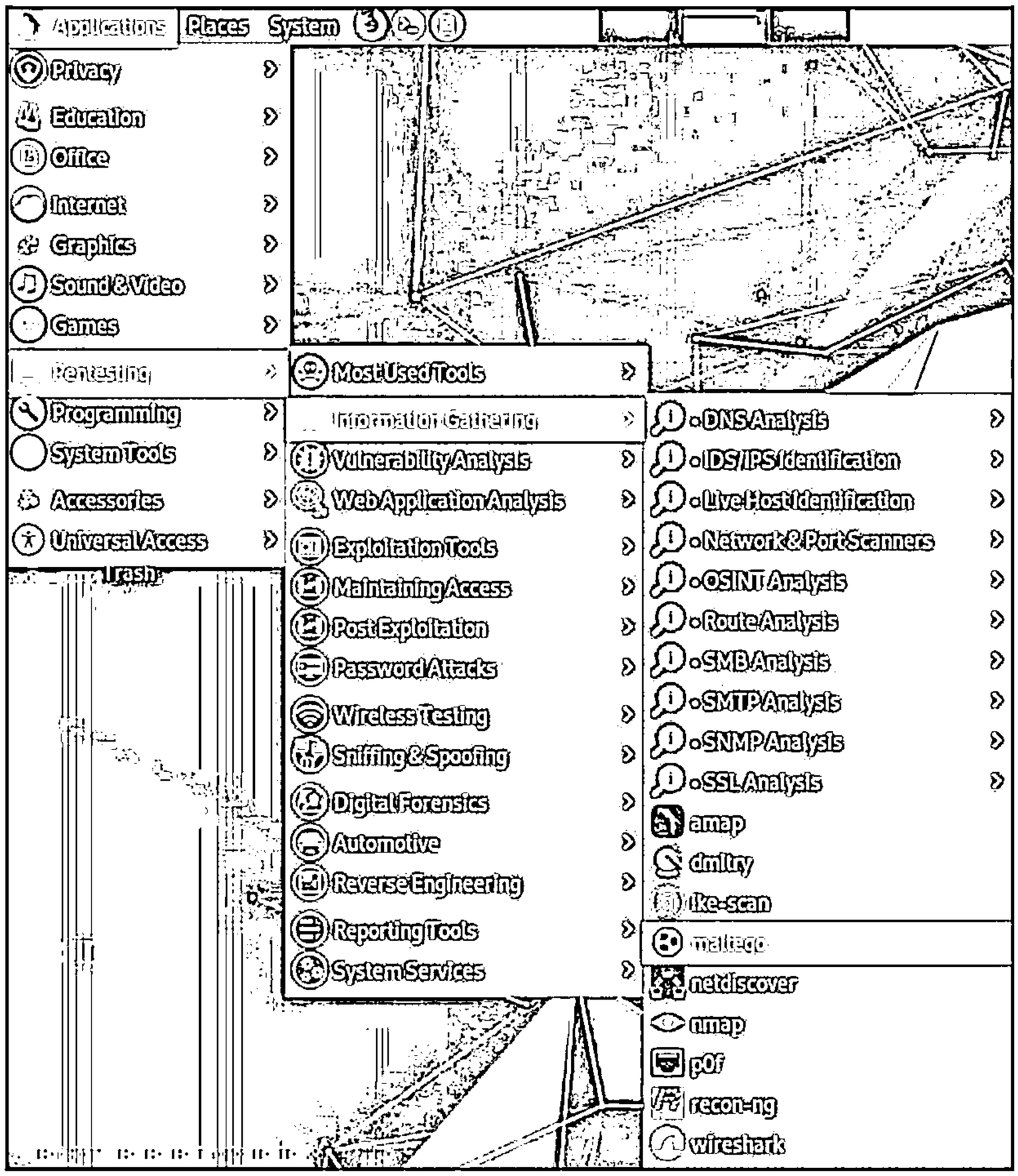


Figure 9.2.1: Maltego Product Selection wizard

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

2. A security pop-up appears, enter password as **toor** in the **Password** field and click **OK**.
3. A **Product Selection** wizard appears on the Maltego GUI; click **Run** from **Maltego CE (Free)** option.

Note: If the **Memory Settings Optimized** pop-up appears, click **Restart Now**.

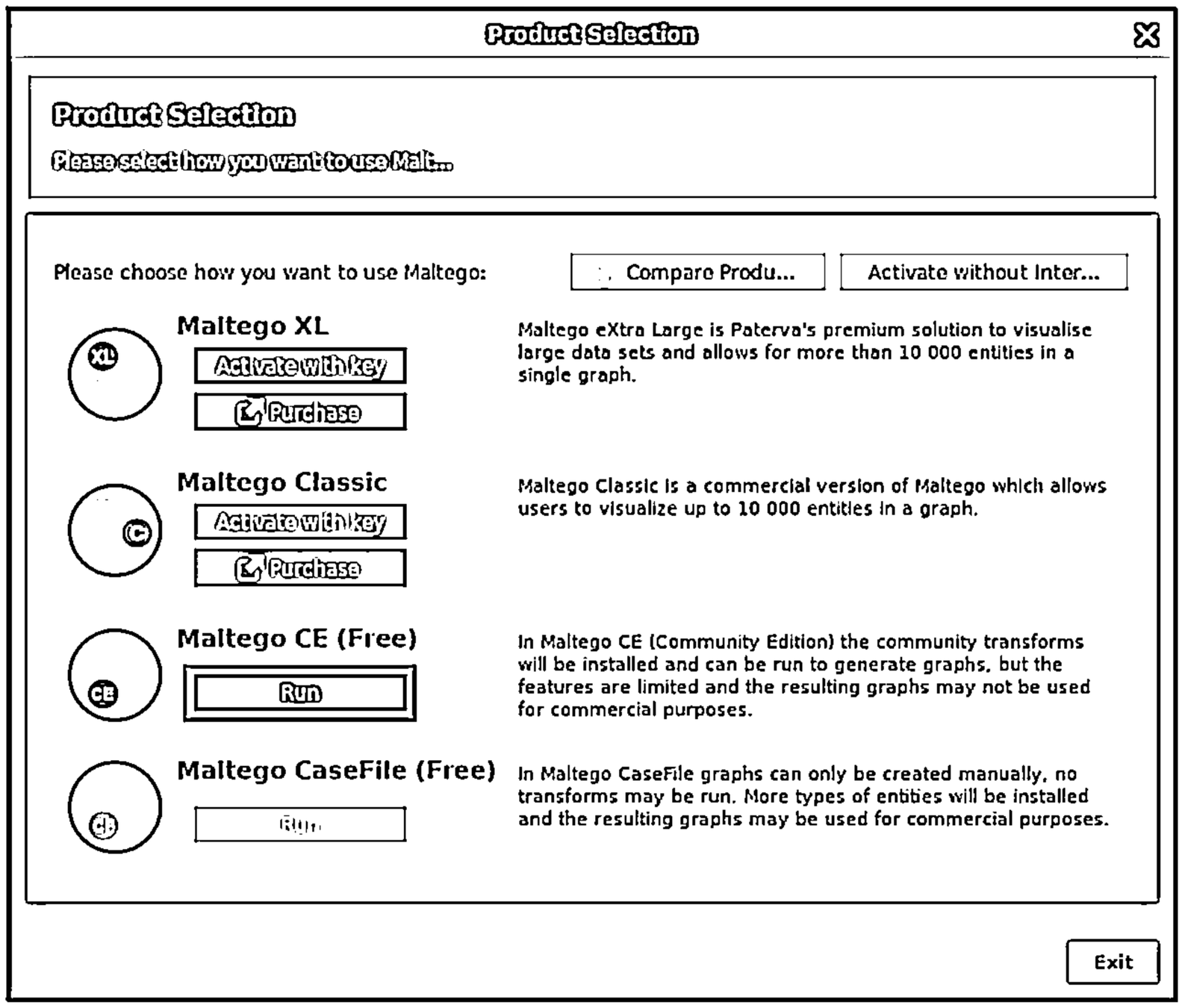


Figure 9.2.2: Maltego Product Selection wizard

Maltego provides you with a graphical interface that makes seeing these relationships instant and accurate, and even making it possible to see hidden connections.

4. As the **Configure Maltego** window appears along with a **LICENSE AGREEMENT** form, check the **Accept** checkbox and click **Next**.

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

5. You will be redirected to the **Login** section; leave the **Maltego** window as it is and click **Firefox** icon from the top-section of the window to launch the Firefox browser.

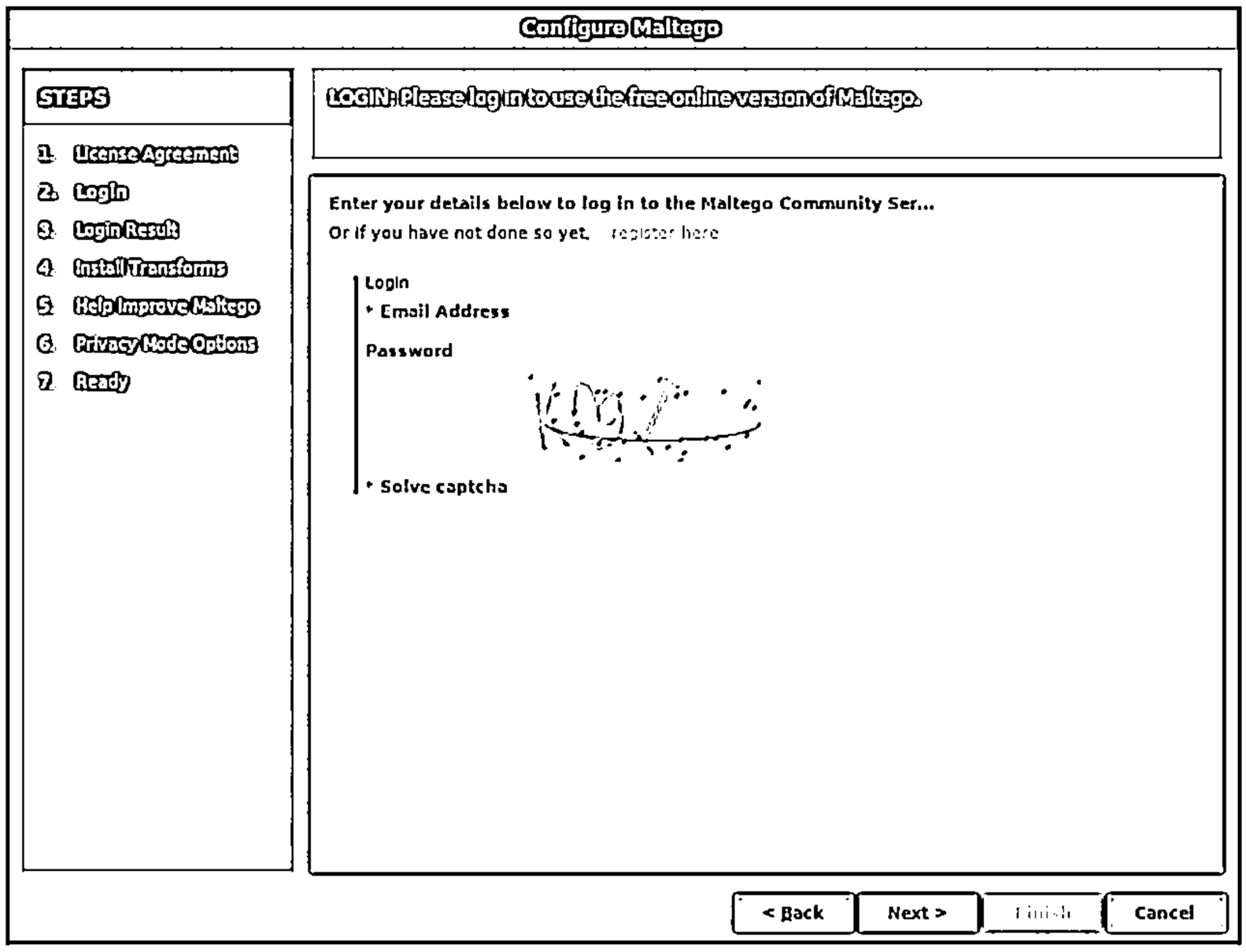


Figure 9.2.3: Maltego Login section

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

6. The **Firefox** window appears, in the address type **https://www.maltego.com/ce-registration** and press **Enter**
7. A **Register a Maltego CE Account** page appears, enter your details and confirm the captcha, and click **REGISTER** button to register your account and activate it.

Note: Please provide a working email ID at the time of registration. Once the registration is done, you will receive an activation email. Activate your account as instructed in the email to use the tool.

Note: If cookie notification appears in the lower section of the browser, click **Accept**.

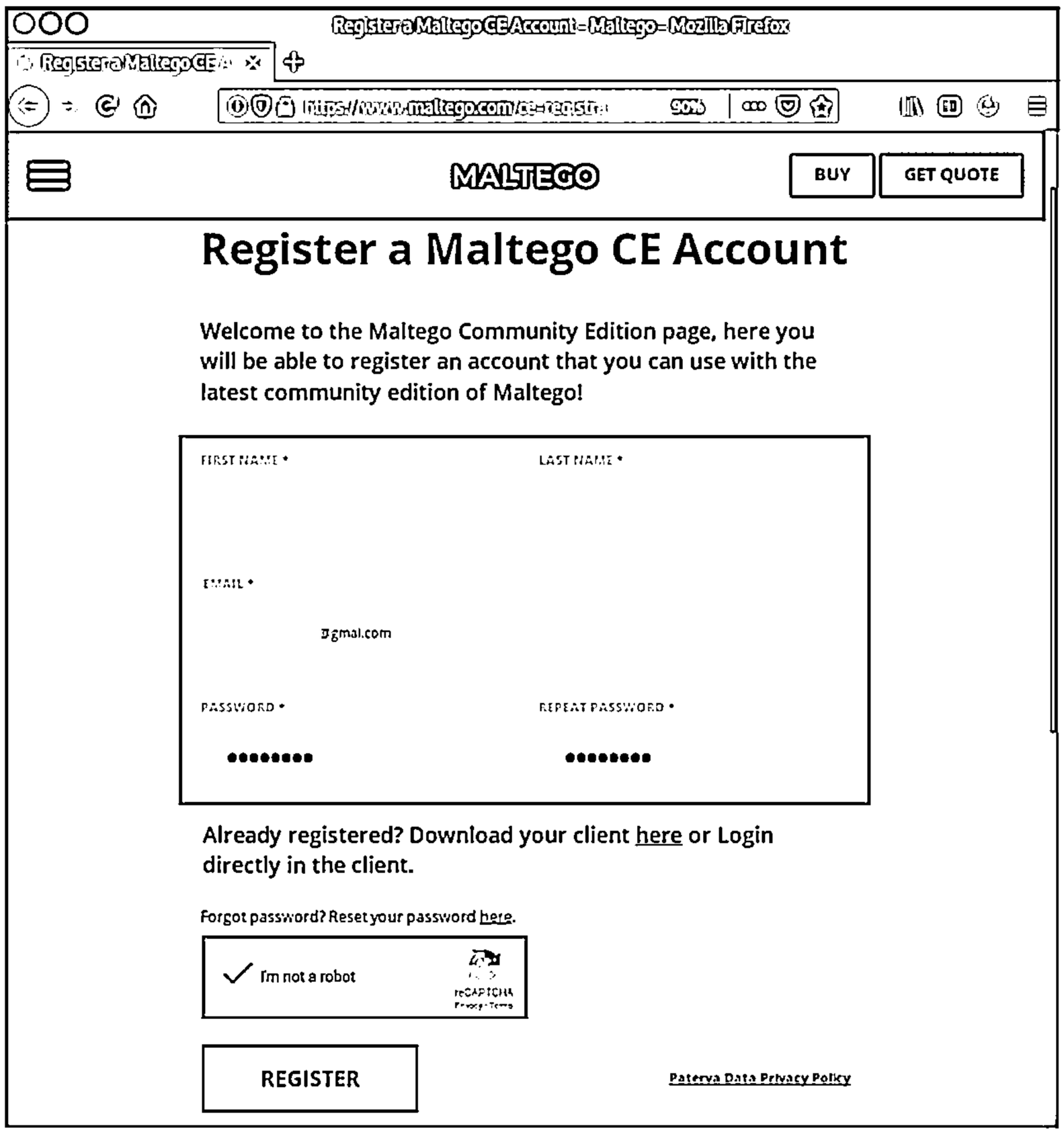


Figure 9.2.4: Registration Section

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

8. Minimize the web browser and go back to the setup wizard and enter the **Email Address** and **Password** specified at the time of registration; solve the **captcha** and click **Next**.

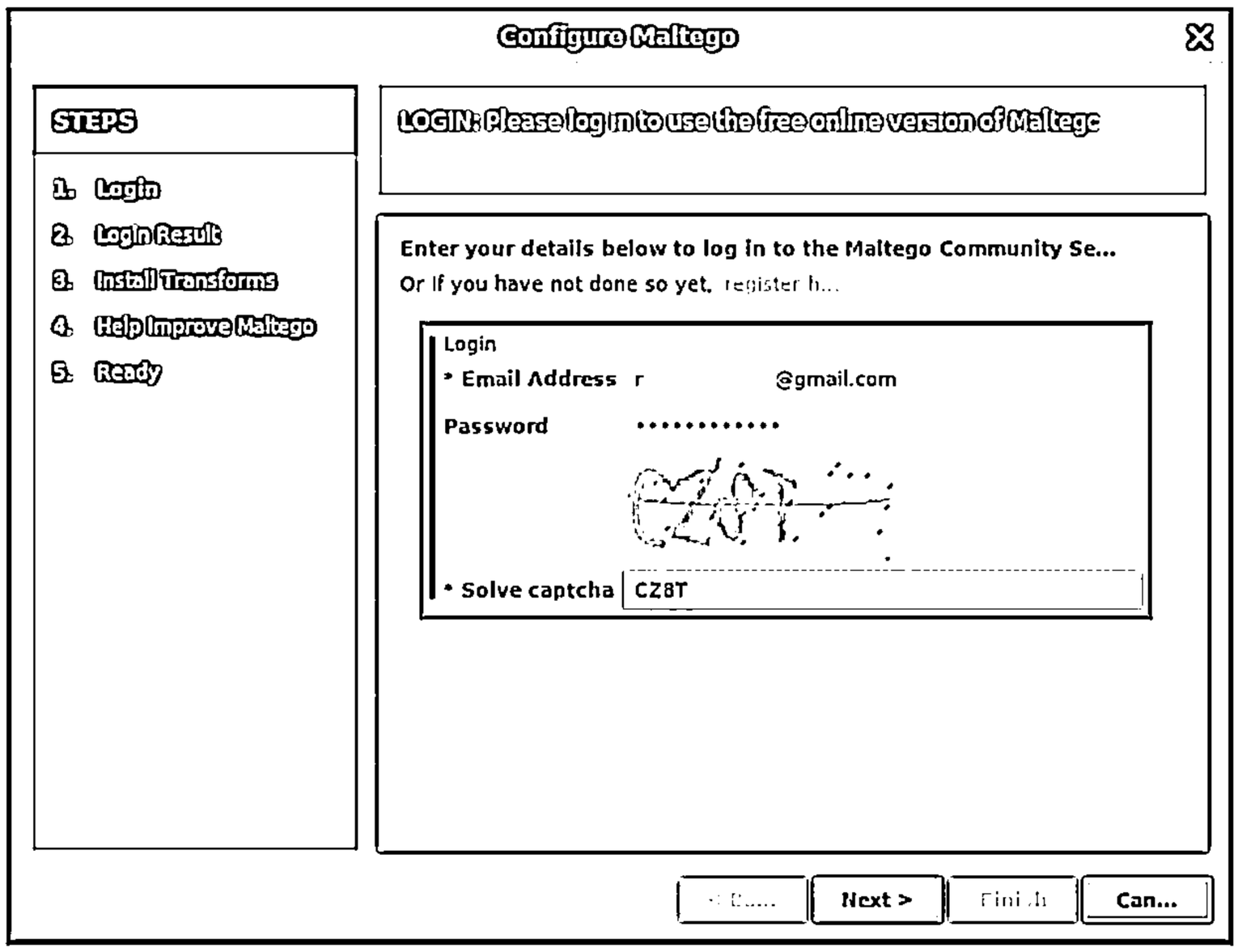


Figure 9.2.5: Maltego Login Section

9. The **Login Result** section displays your personal details; click **Next**.

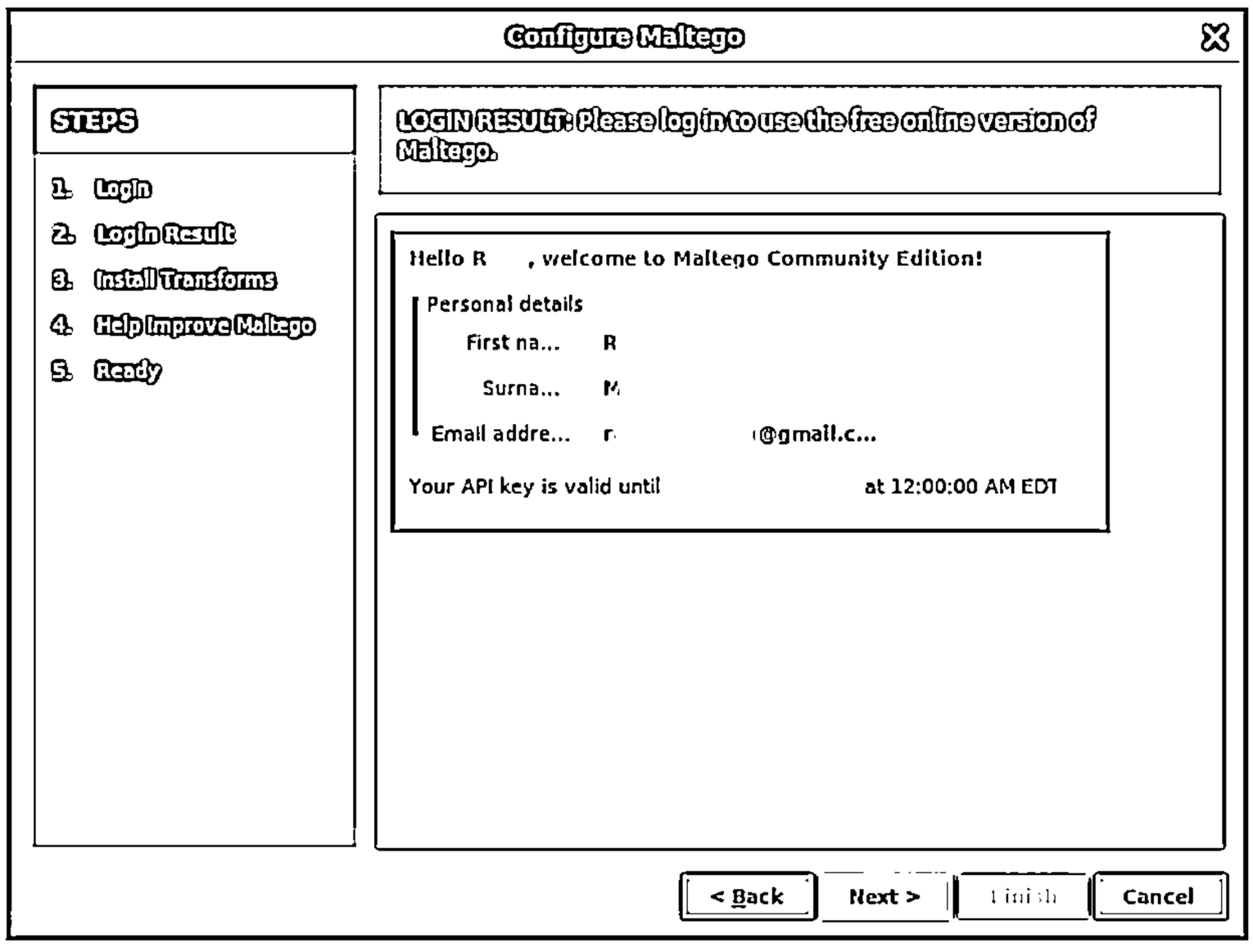


Figure 9.2.6: Maltego Login result section

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

10. The **Install Transforms** section appears, which will install items from the chosen transform server. Leave the settings to default and click **Next**.

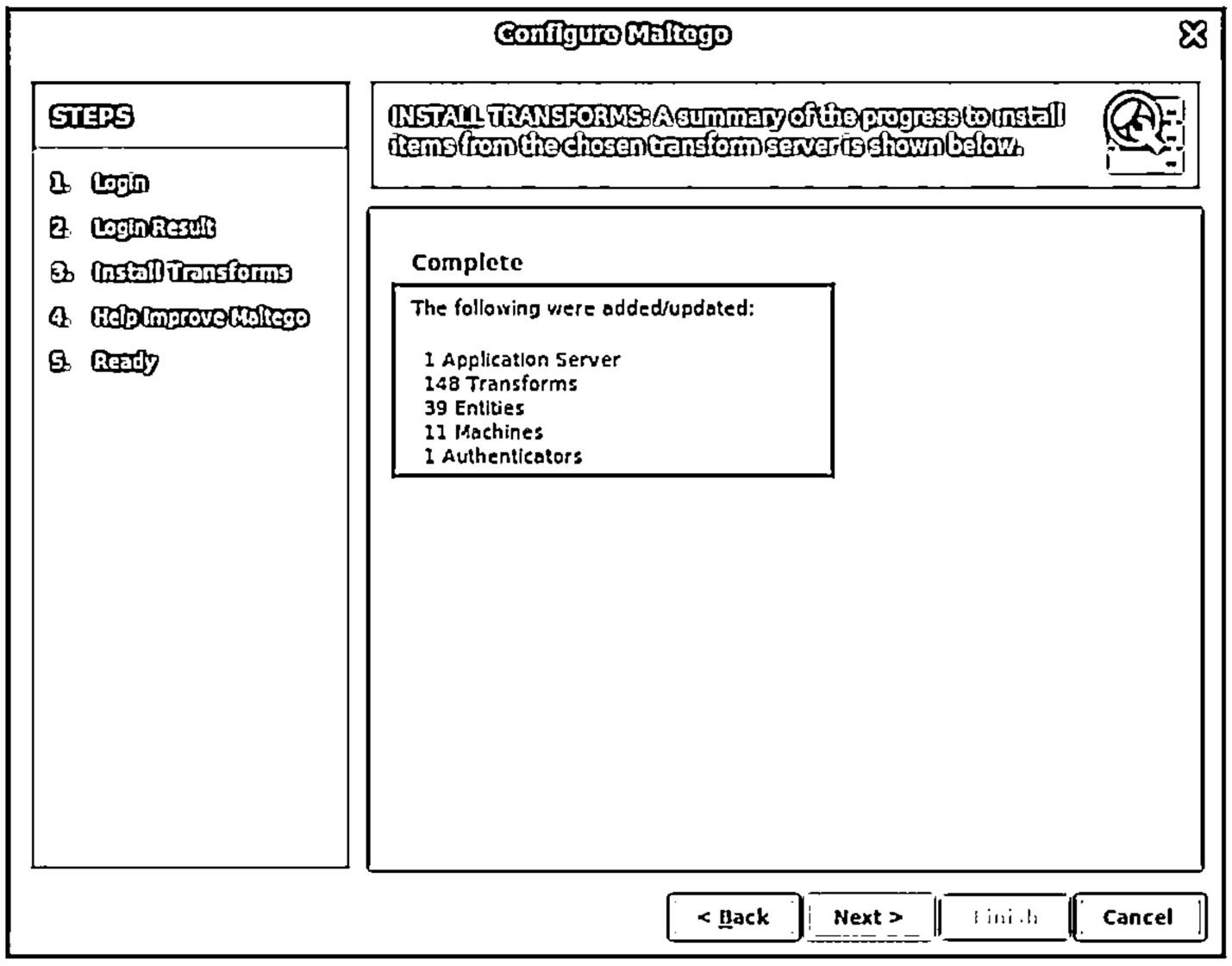


Figure 9.2.7: Maltego Install Transforms section

11. The **Help Improve Maltego** section appears. Leave the options set to default and click **Next**.

Note: The screenshot might differ in your lab environment.

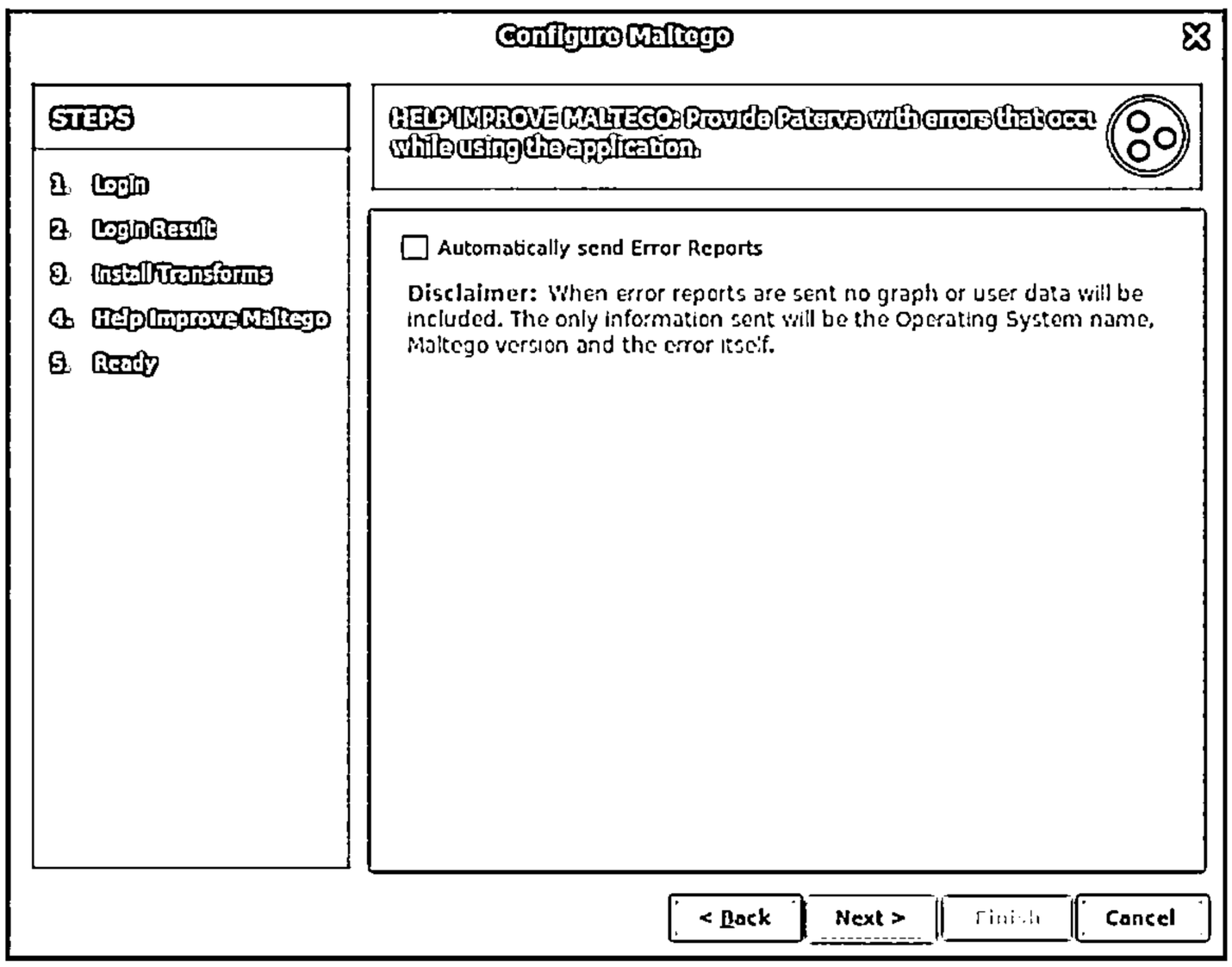


Figure 9.2.8: Maltego Help Improve Maltego section

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

12. The **Ready** section appears. Select the radio button of **Open a blank graph and let me play around** and click **Finish** to perform footprinting manually.

Note: If the **Privacy Policy Change Notice** appears, click **Acknowledge**.

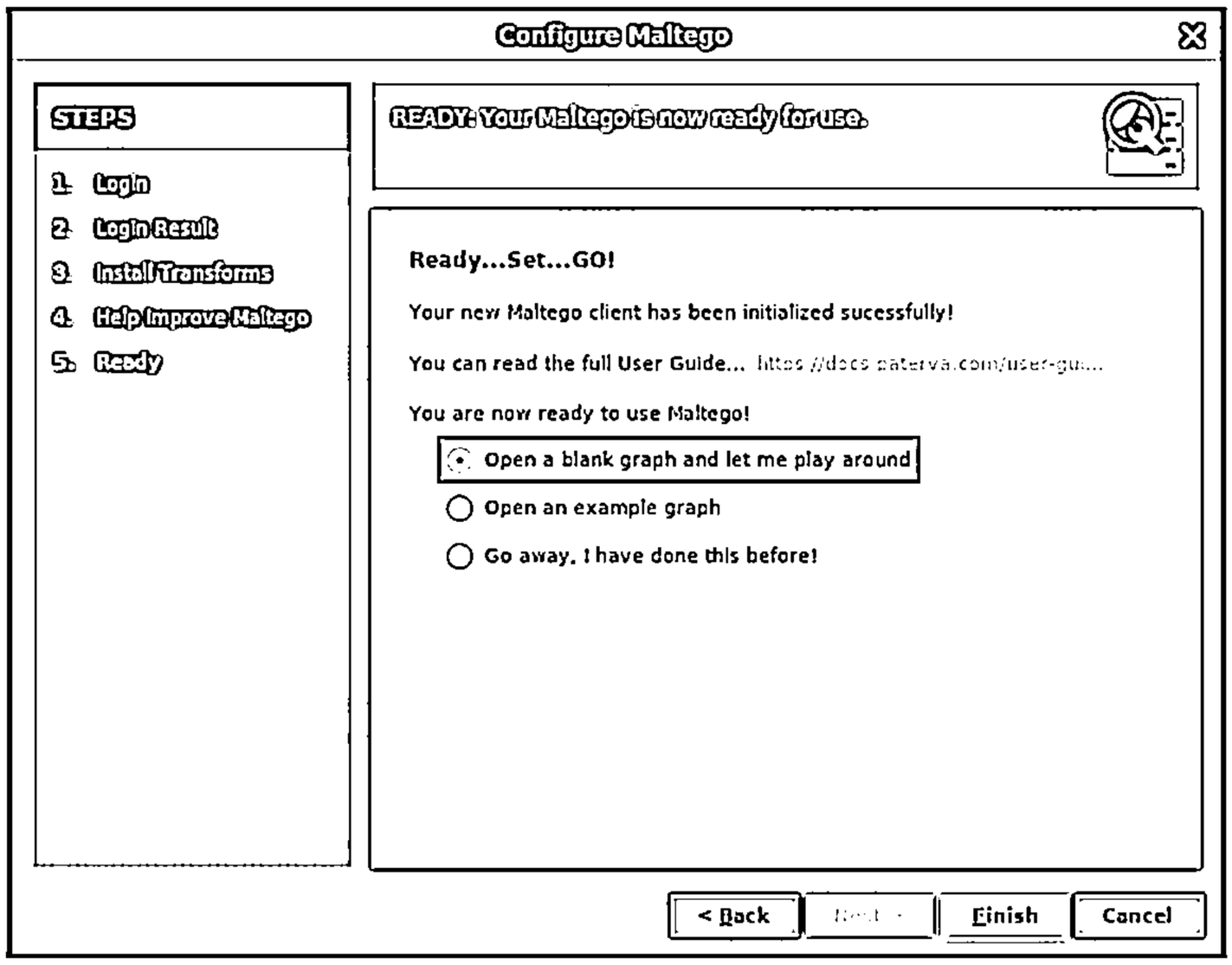


Figure 9.2.9: Maltego Ready wizard

13. The **Maltego Community Edition** GUI appears, and the **New Graph (1)** window will be automatically launched, as shown in the screenshot.

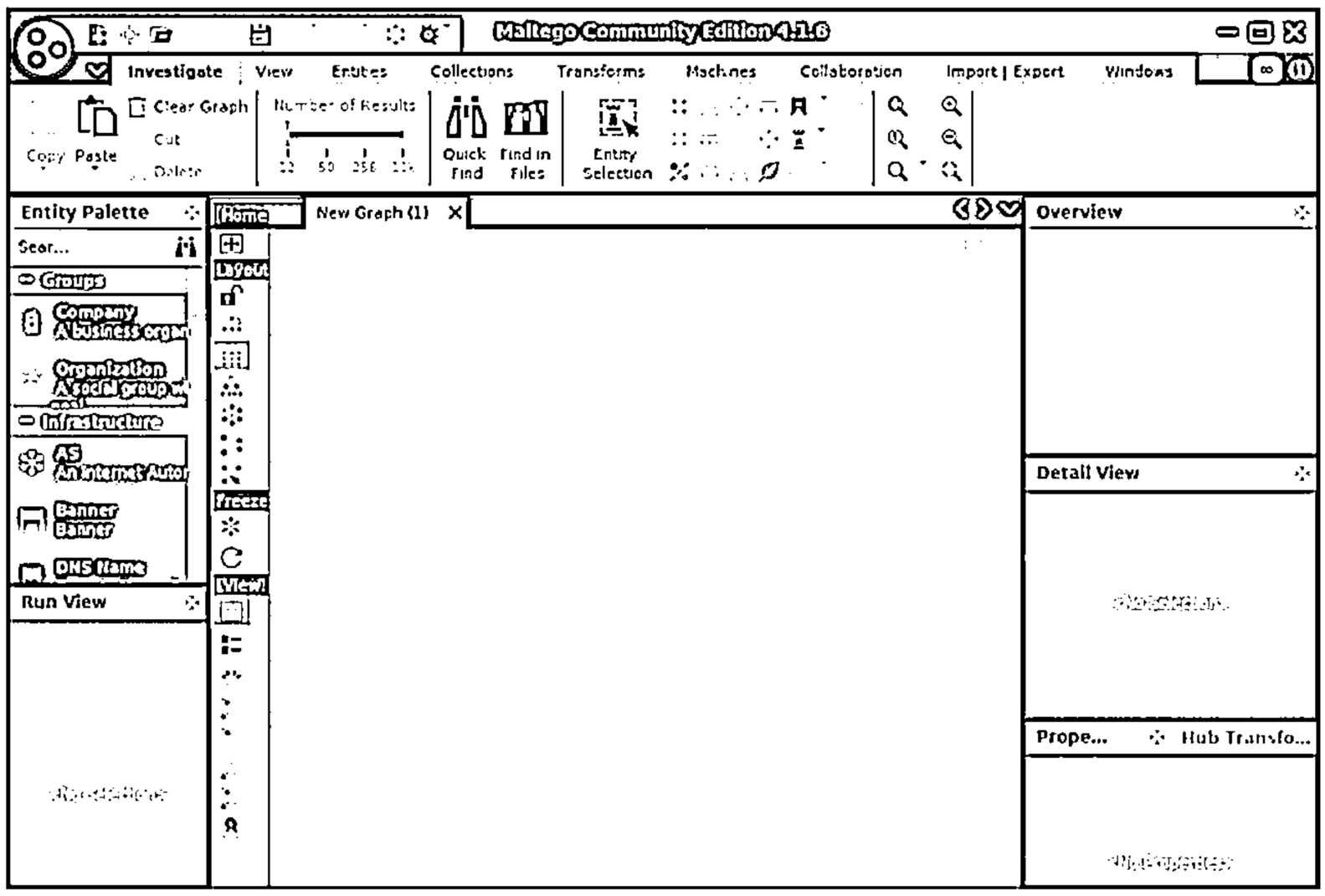


Figure 9.2.10: Maltego GUI

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

Note: If the **New Graph (1)** window does not open automatically, click the icon located at the top-left corner of the GUI (in the toolbar) to start a new graph.

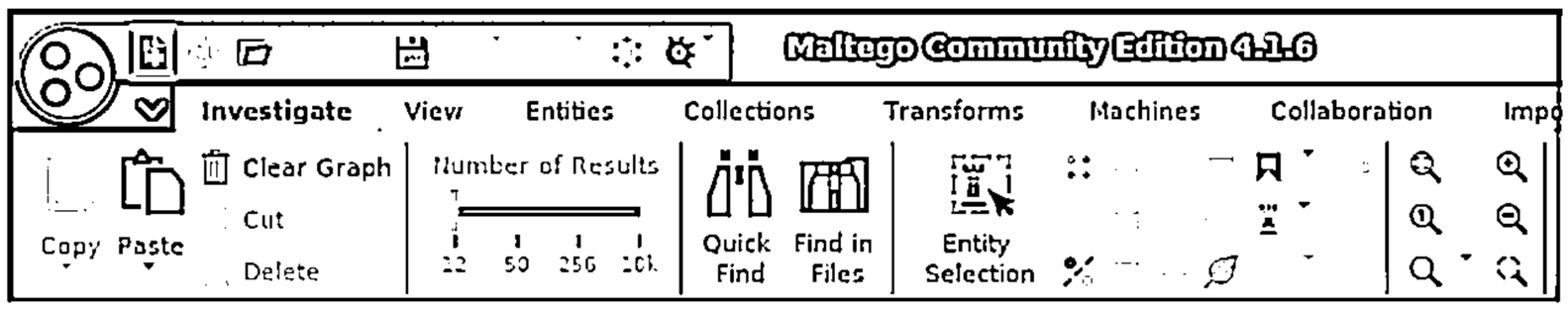


Figure 9.2.11: Maltego Toolbar

TASK 2.2

Add a Domain Entity

14. In the left-pane of **Maltego GUI**, you can find the **Entity Palette** box, which contains a list of default built-in transforms. In the **Infrastructure** node under **Entity Palette**, observe a list of entities such as **AS**, **DNS Name**, **Domain**, **IPv4 Address**, **URL**, **Website**, etc.
15. Drag the **Website** entity onto the **New Graph (1)** window.

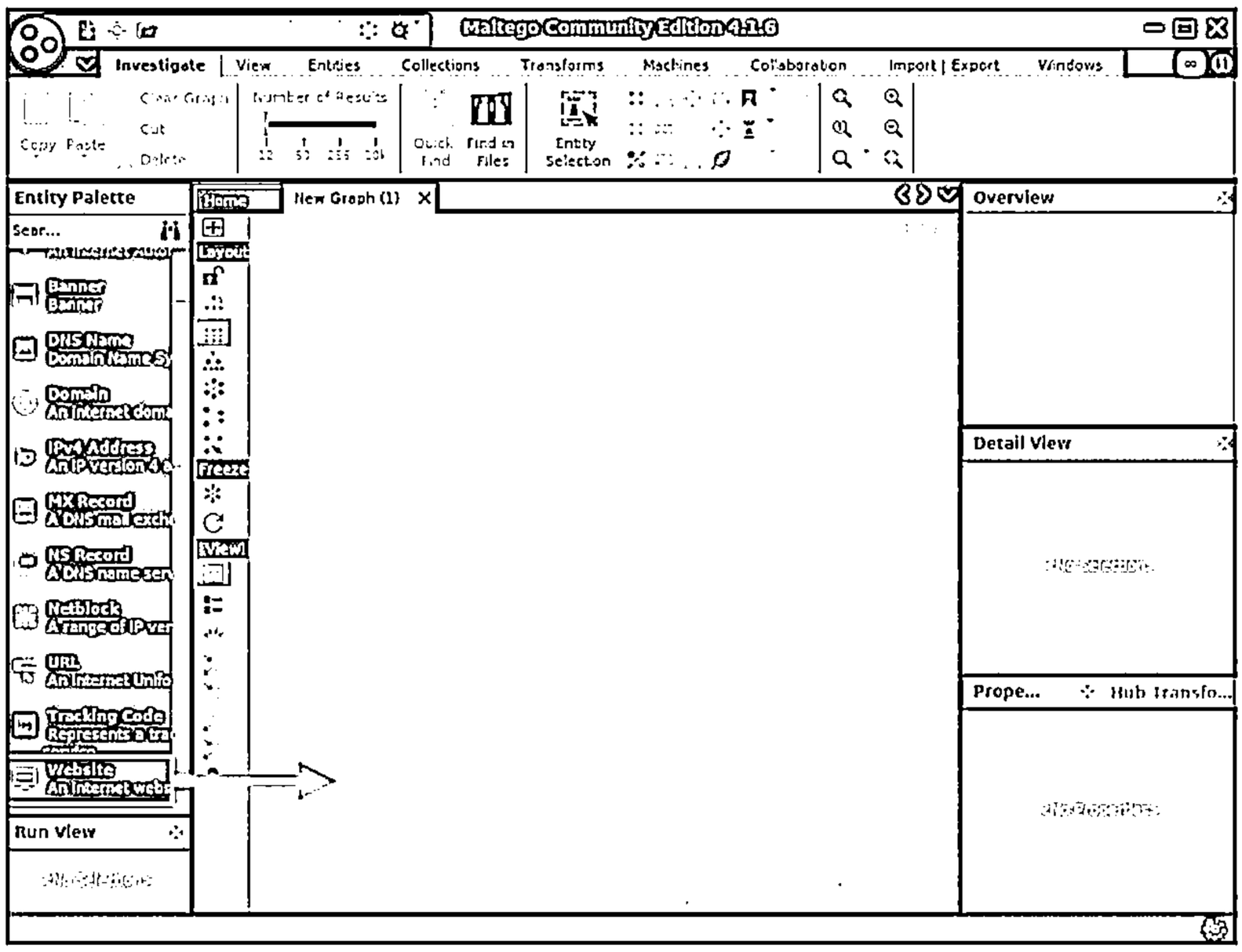


Figure 9.2.12: Selecting a Website Entity

16. The entity appears on the new graph, with the **www.paterva.com** URL selected by default.

Note: If you are not able to view the entity as shown in the screenshot, click in the **New Graph (1)** window and **scroll up**, which will increase the size of the entity.

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

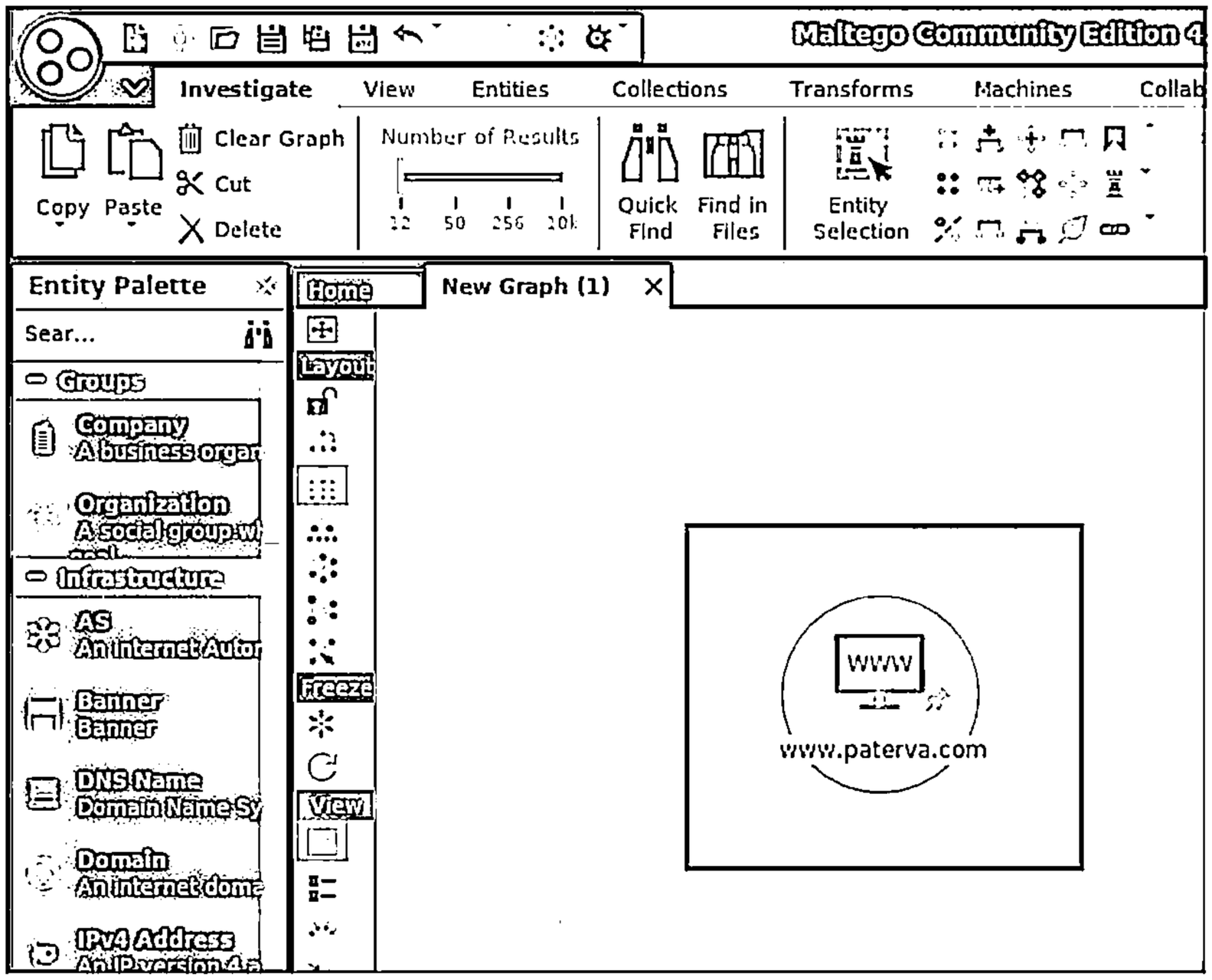


Figure 9.2.13: Website Entity in the New Graph (1) Section

17. Double-click the name **www.paterva.com** and change the domain name to **www.certifiedhacker.com**; press **Enter**.

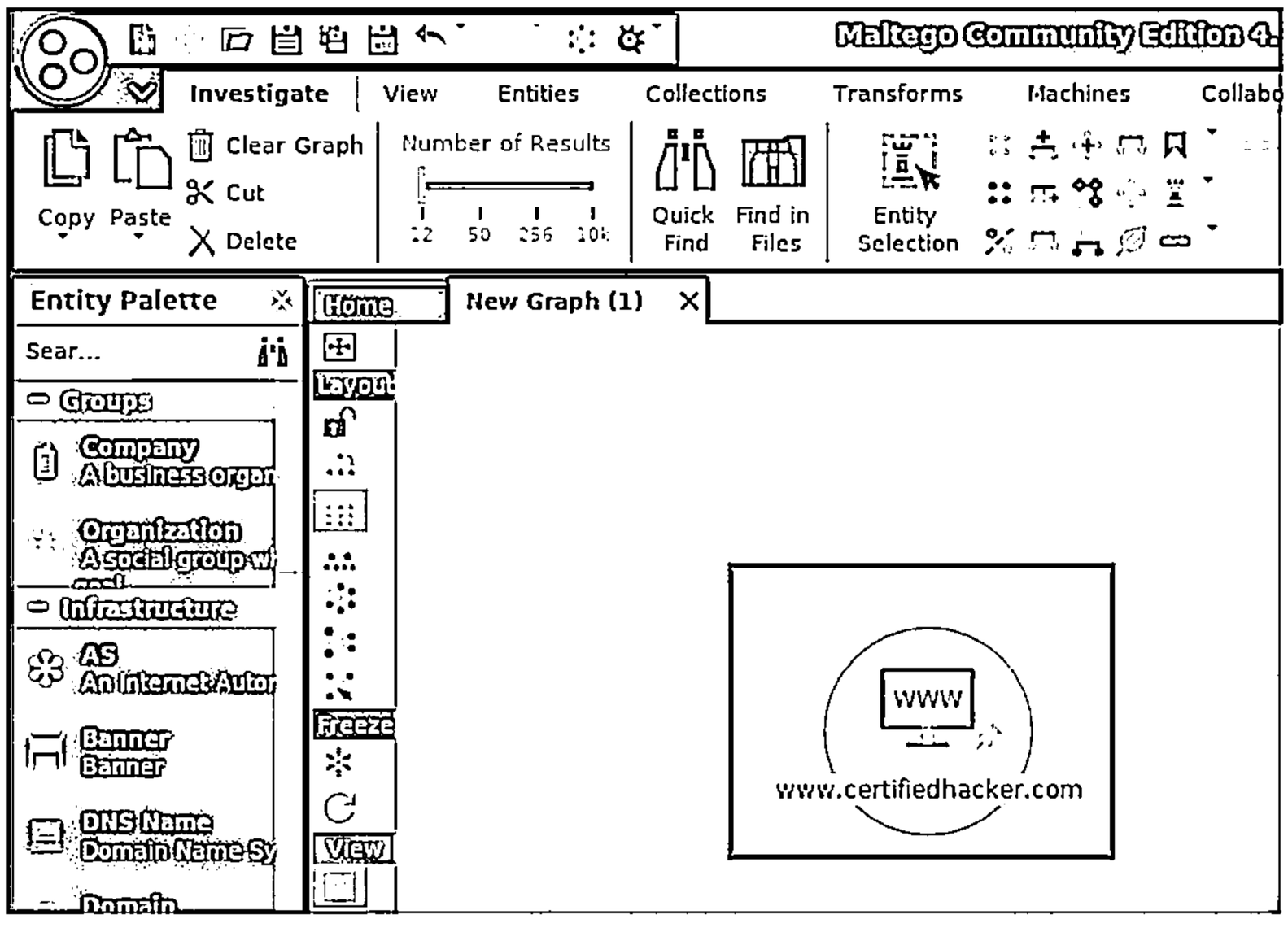


Figure 9.2.14: Website Entity in the New Graph (1) Section

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

TASK 2.3

Identify the Server-Side Technology

18. Right-click the entity and select **All Transforms**.

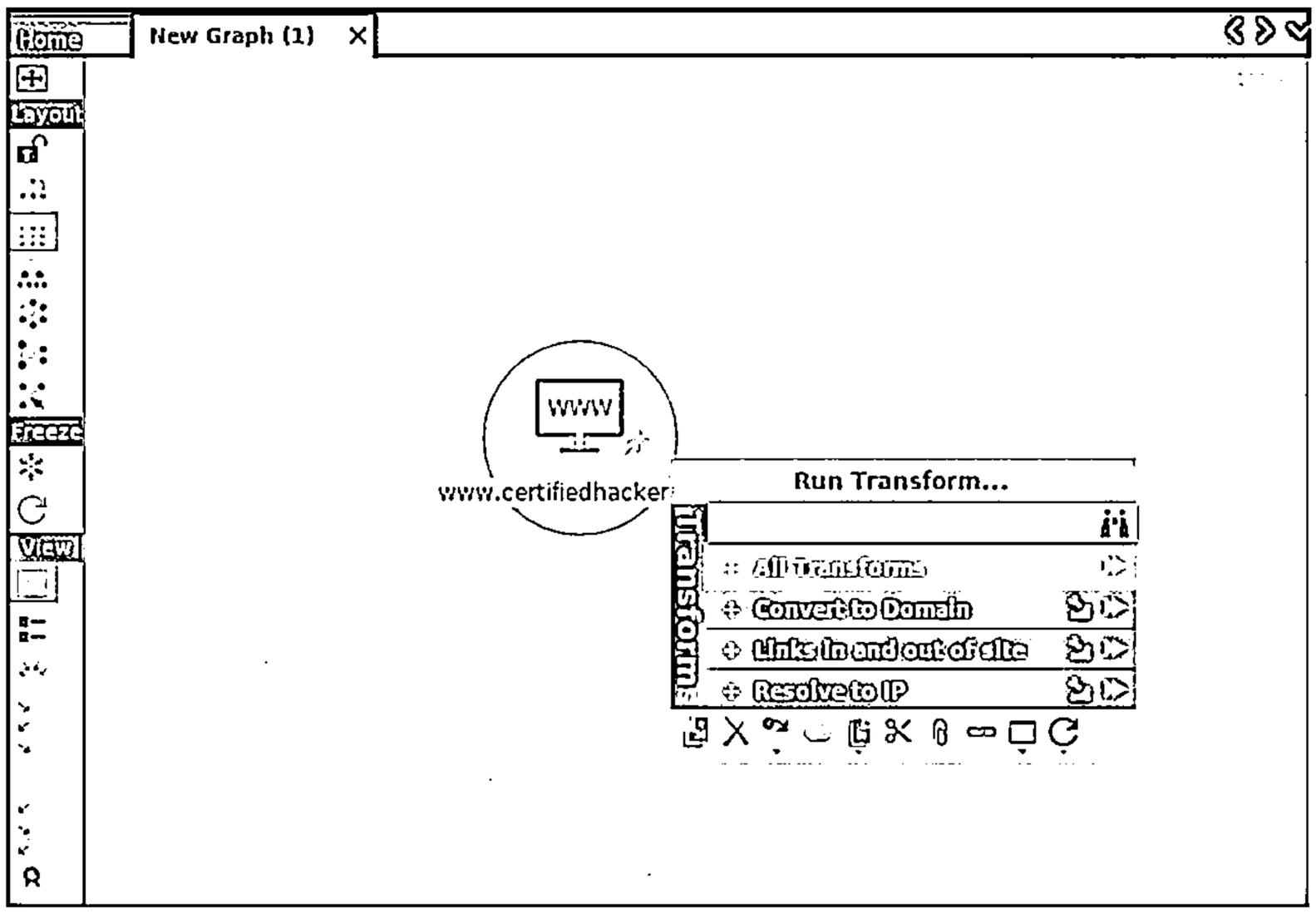


Figure 9.2.15: Selecting to Server Technologies Website

19. The **Run Transform(s)** list appears; click **To Server Technologies [Using BuiltWith]**.

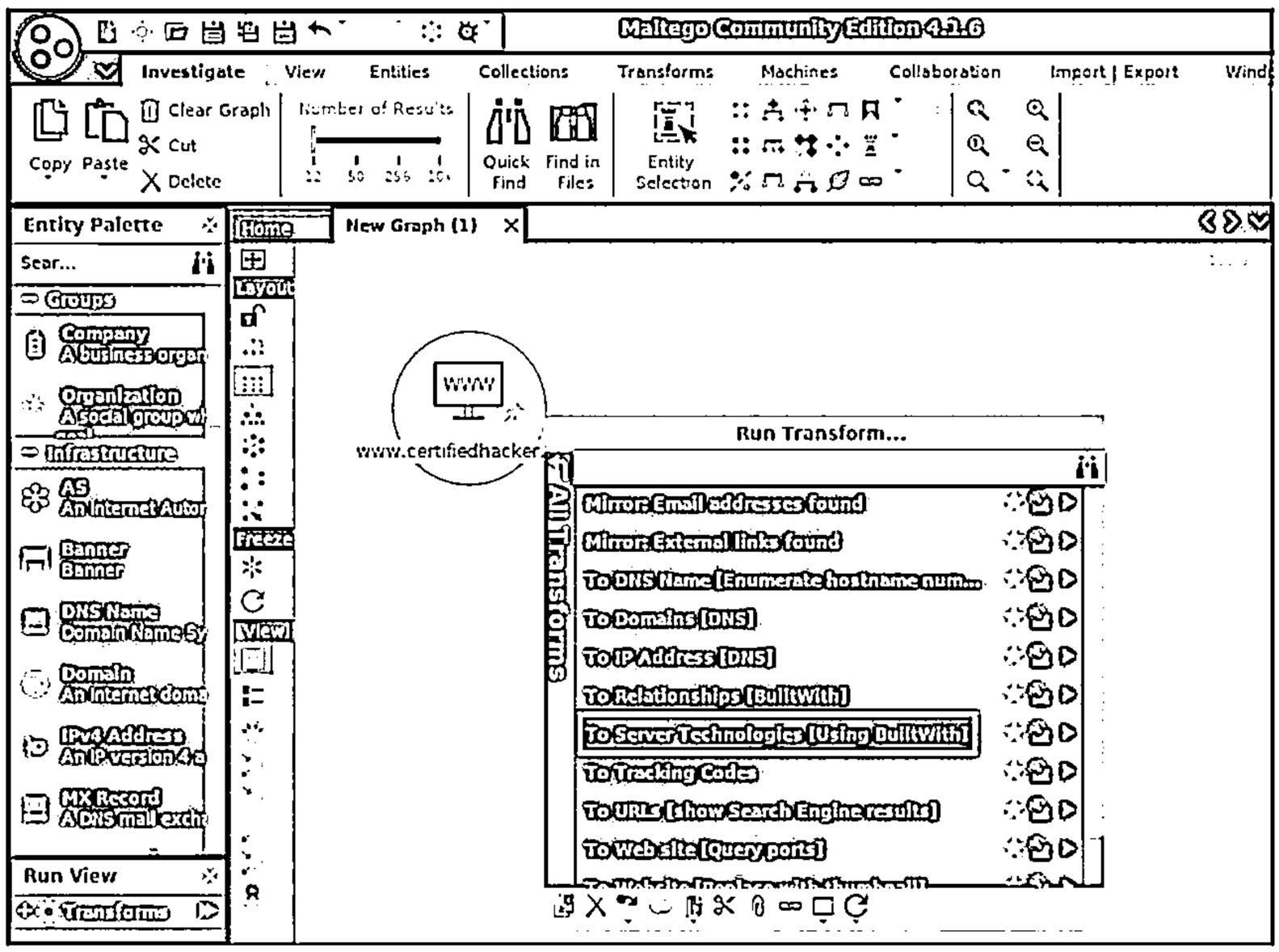


Figure 9.2.16: Run Transform(s) list

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

20. Maltego starts running the transform the **To Server Technologies [Using BuiltWith]** entity. Observe the status in the progress bar.

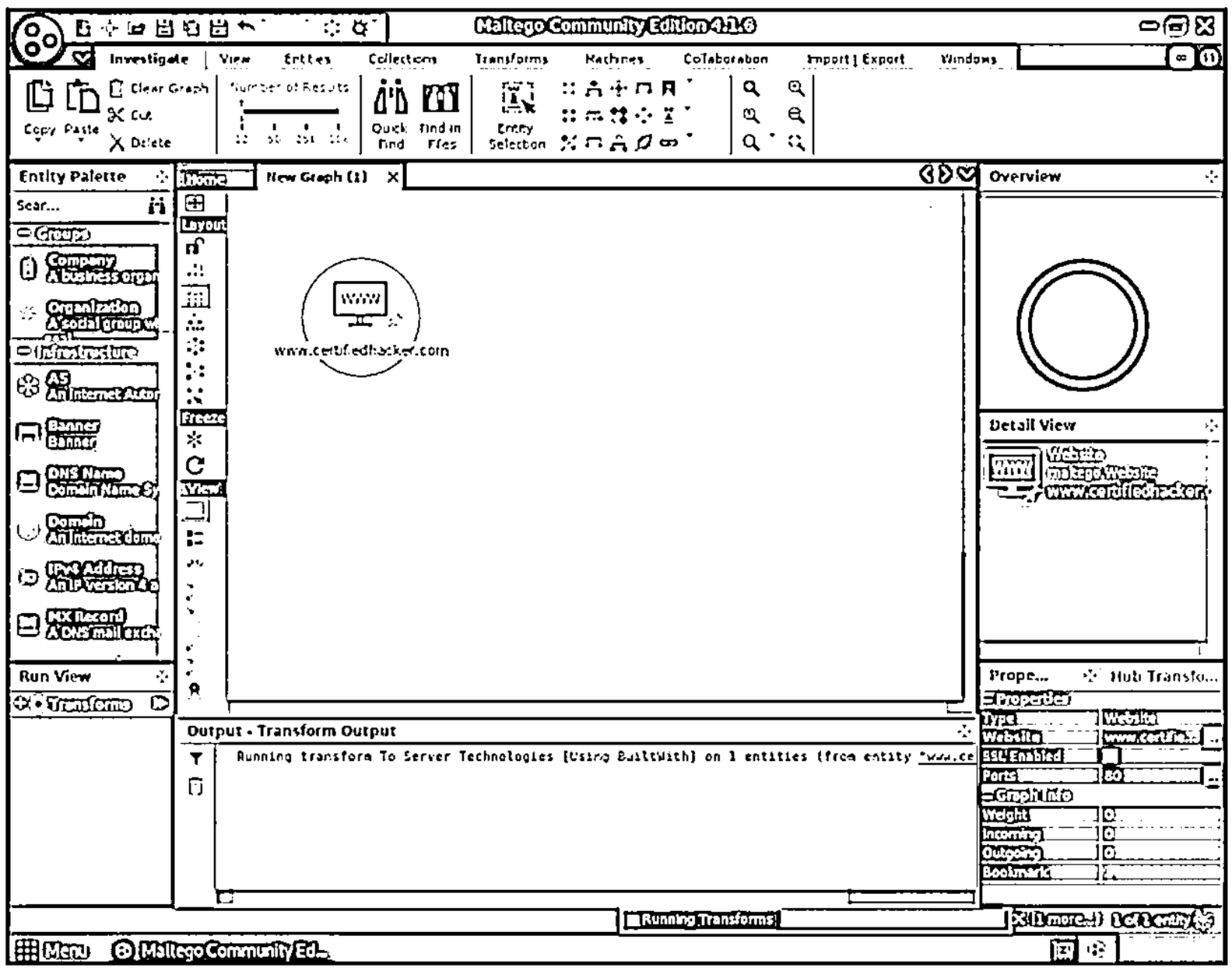


Figure 9.2.17: Progress bar pop-up

21. Once Maltego completes the transforming server-side technologies, it displays the technology implemented on the server that hosts the website, as shown in the following screenshot.

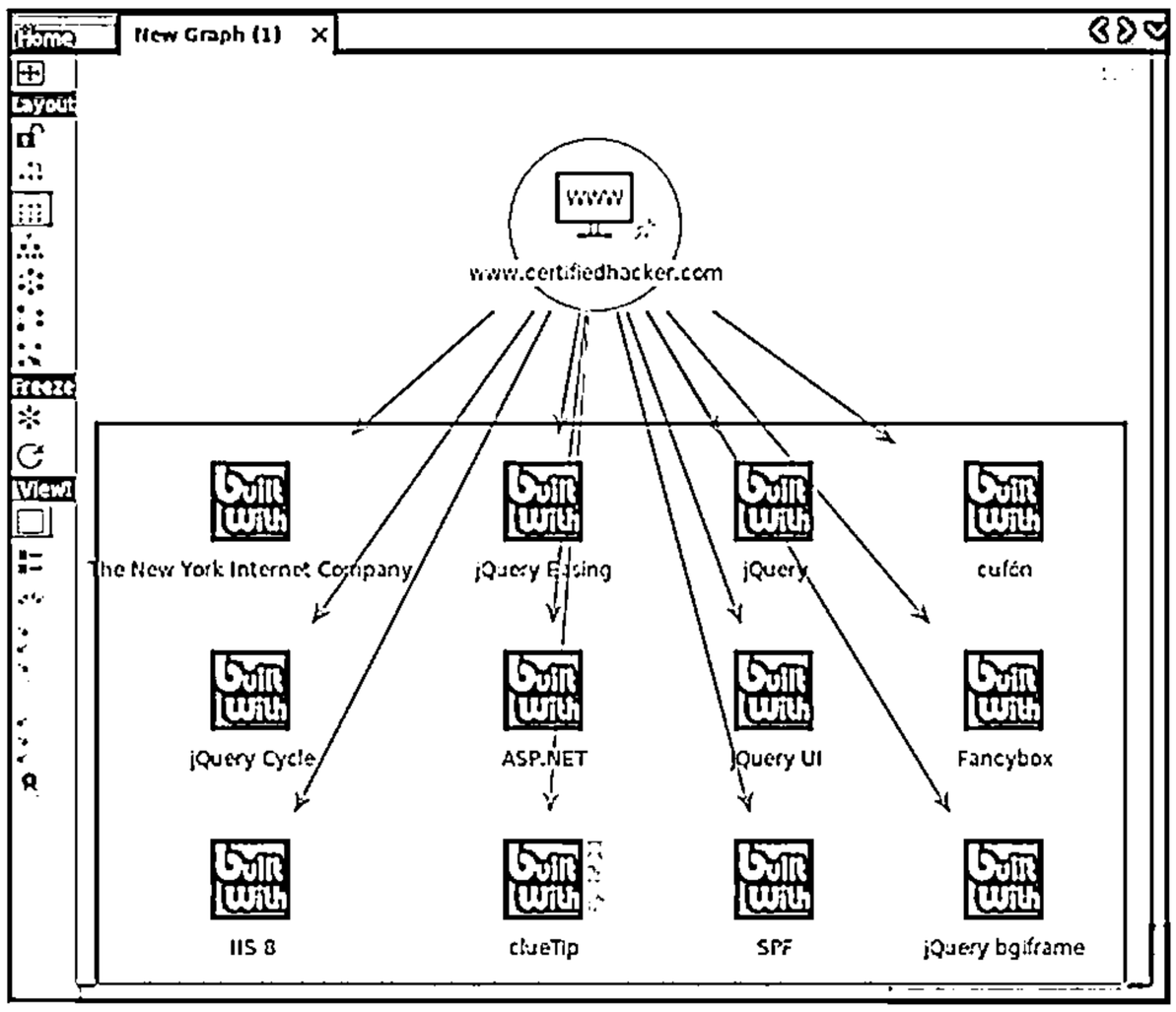


Figure 9.2.18: Server-Side Technologies in www.certifiedhacker.com

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

22. After obtaining the built-in technologies of the server, you can search for related vulnerabilities and simulate exploitation techniques to hack them.
23. To start a new transform, select all the entities, excluding the **www.certifiedhacker.com** website entity, and press **Delete**.
24. A **Delete** pop-up appears; click **Yes**.

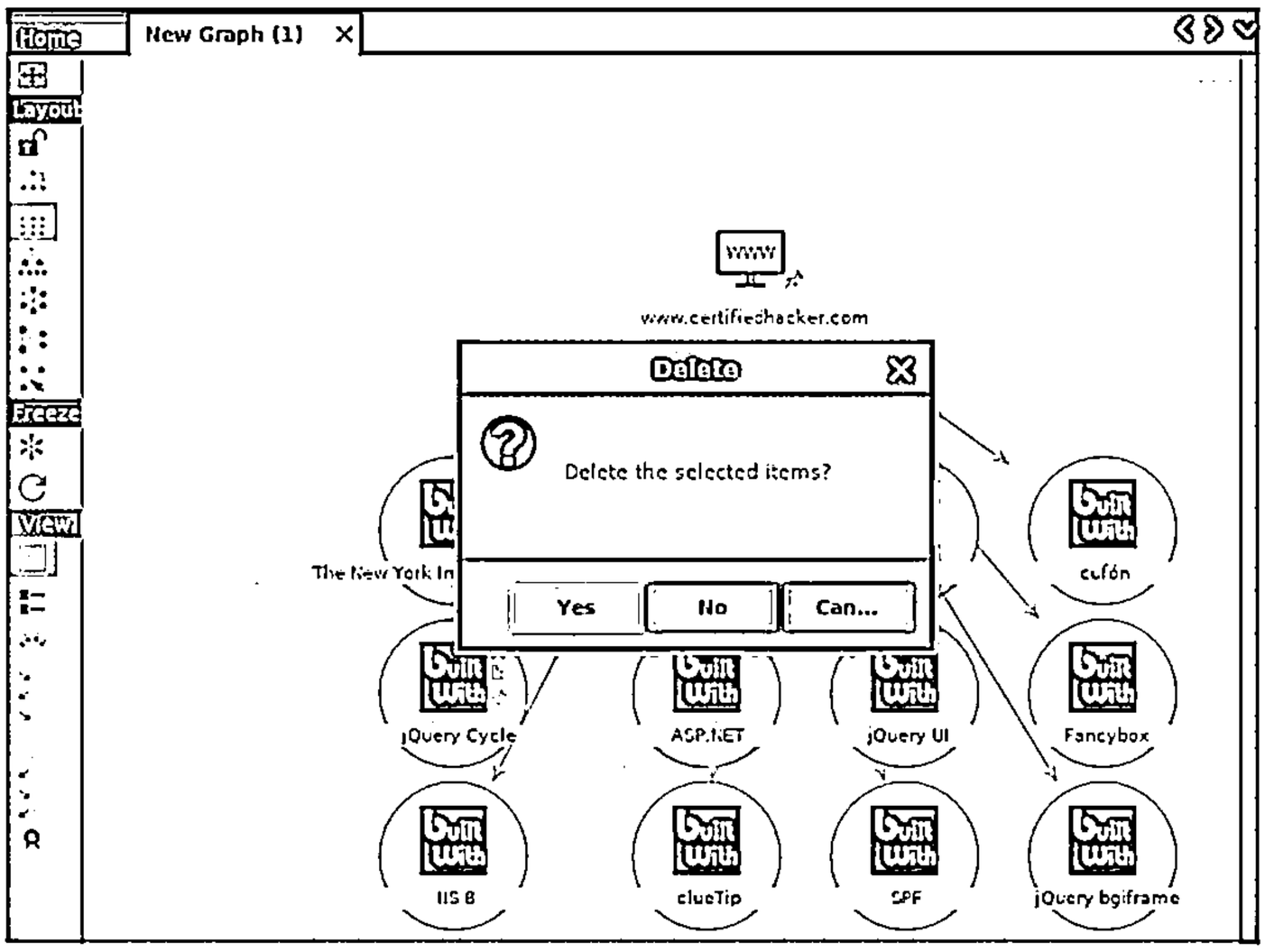


Figure 9.2.19: Delete pop-up

TASK 2.4

Identify the Domain

25. Now, right-click the **www.certifiedhacker.com** website entity and select **All Transforms → To Domains [DNS]**.

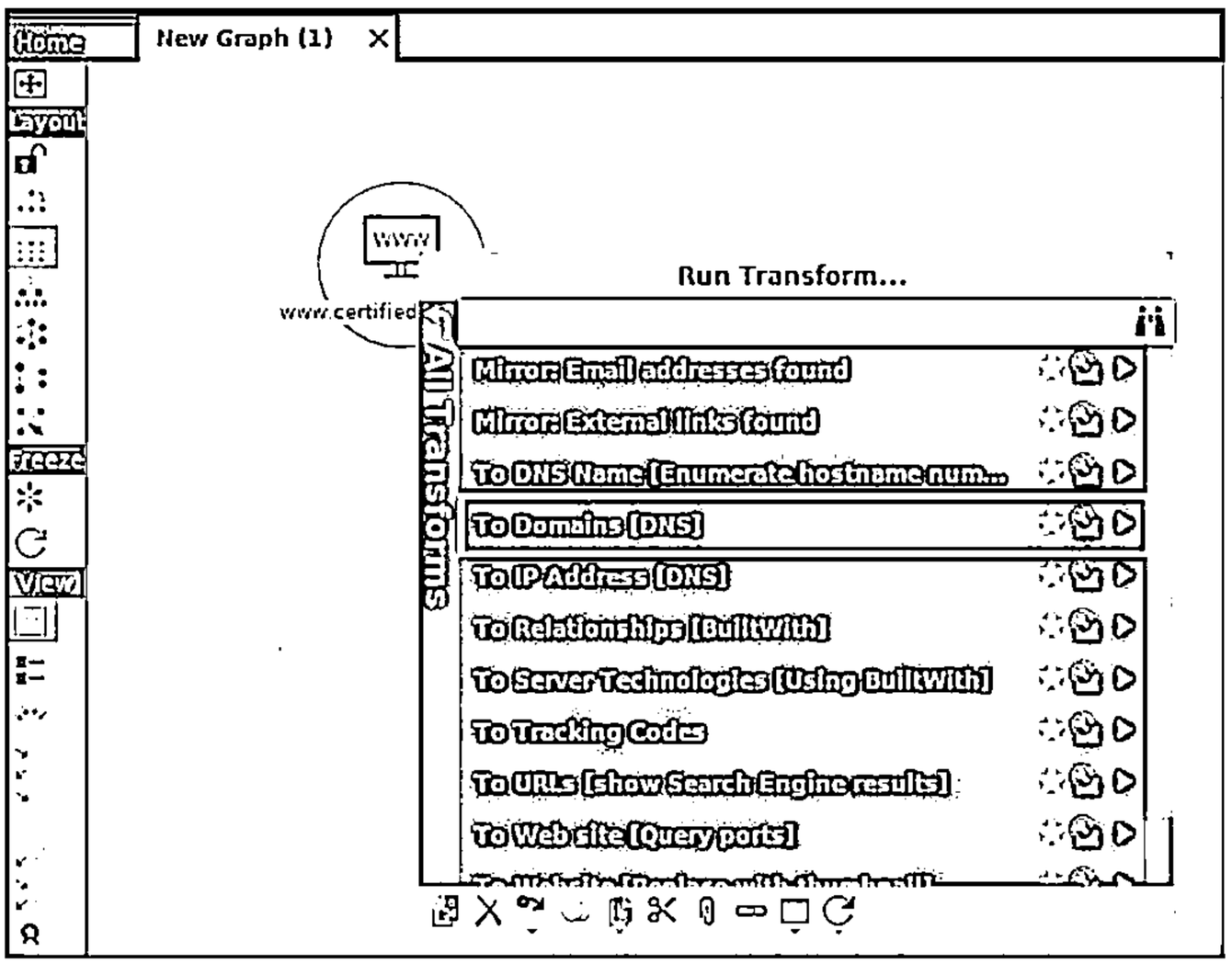


Figure 9.2.20: Selecting To Domains [DNS]

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

26. The domain corresponding to the website displays, as shown in the following screenshot.

Note: Screenshots may differ in your lab environment.

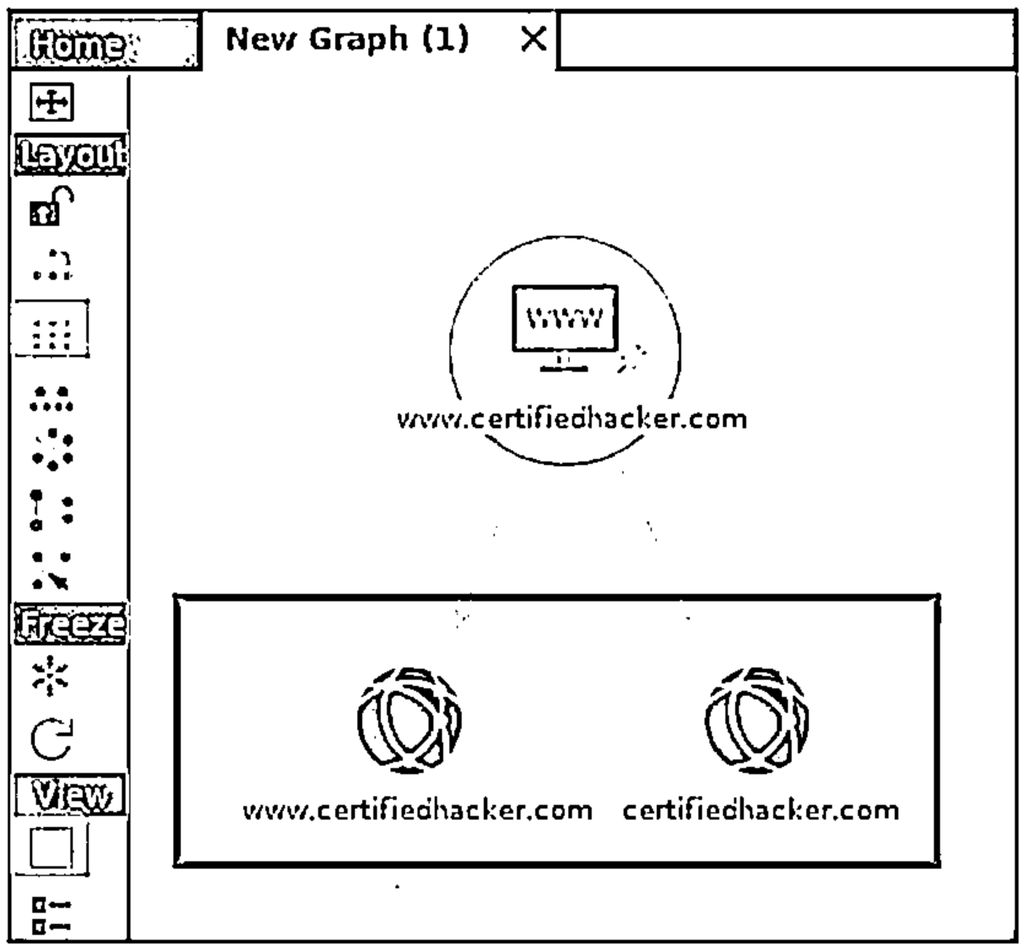


Figure 9.2.21: Domain Name of the Corresponding Website

TASK 2.5

Identify the Domain Name Schema

27. Right-click the **certifiedhacker.com** entity and select **All Transforms → To DNS Name [Using Name Schema diction...]**.

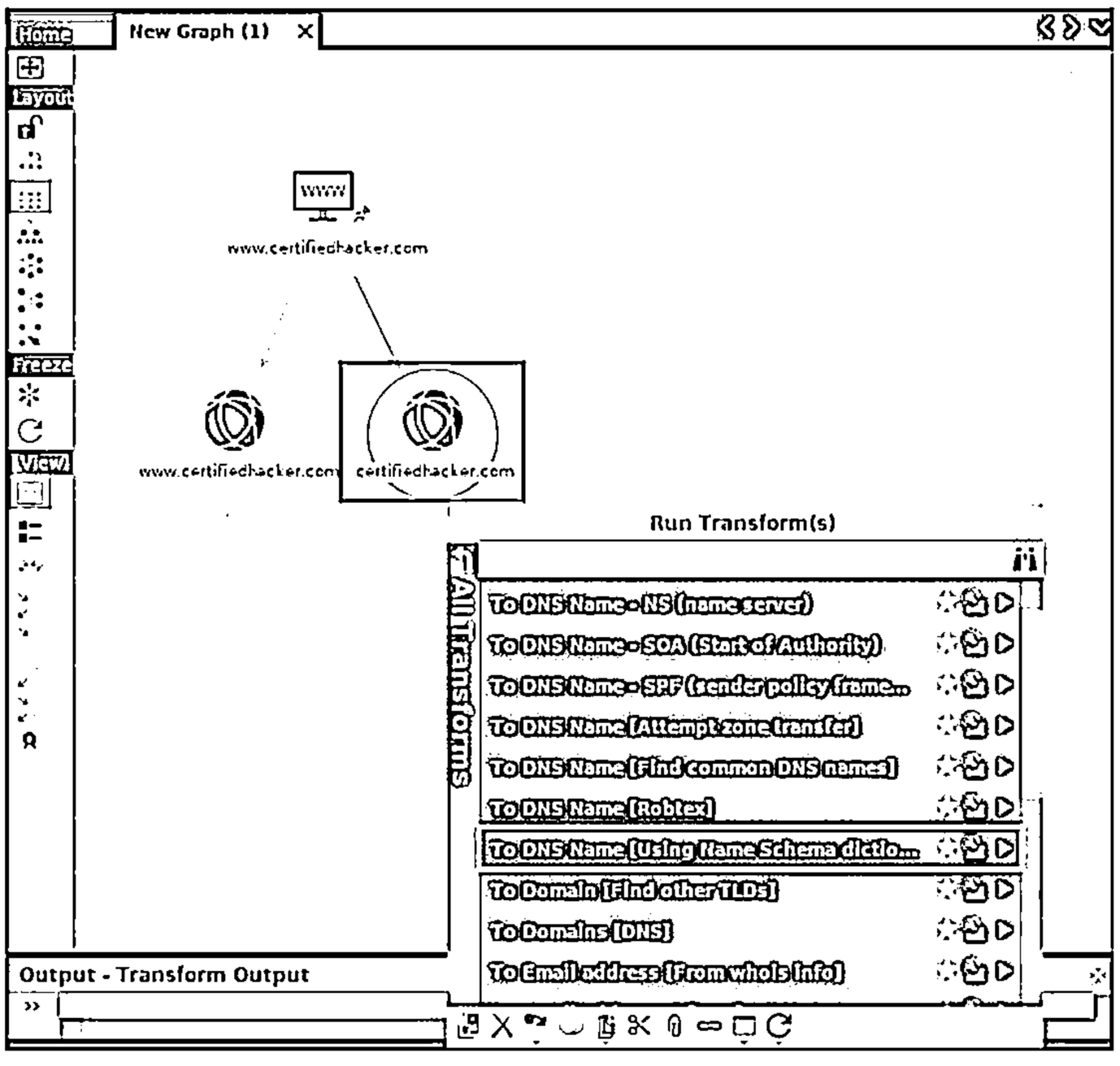


Figure 9.2.22: Selecting To DNS Name [Using Name Schema diction...]

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

28. Observe the status in the progress bar. This transform will attempt to test various name schemas against a domain and try to identify a specific name schema for the domain, as shown in the following screenshot.

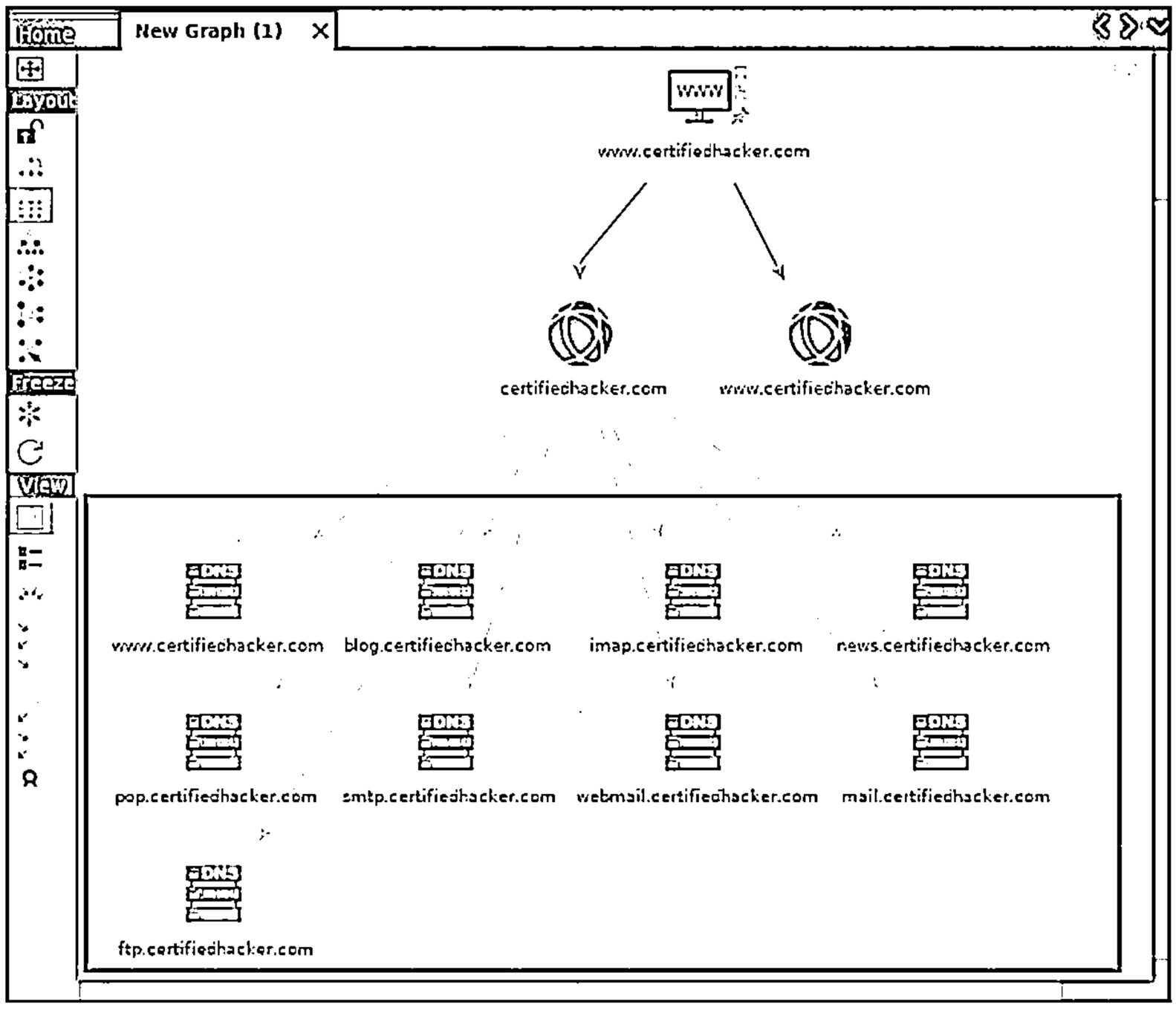


Figure 9.2.23: DNSNameSchema of certifiedhacker.com

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

29. After identifying the name schema, attackers attempt to simulate various exploitation techniques to gain sensitive information related to the resultant name schemas. For example, an attacker may implement a brute-force or dictionary attack to log in to **ftp.certifiedhacker.com** and gain confidential information.

30. Select only the name schemas by dragging and deleting them.

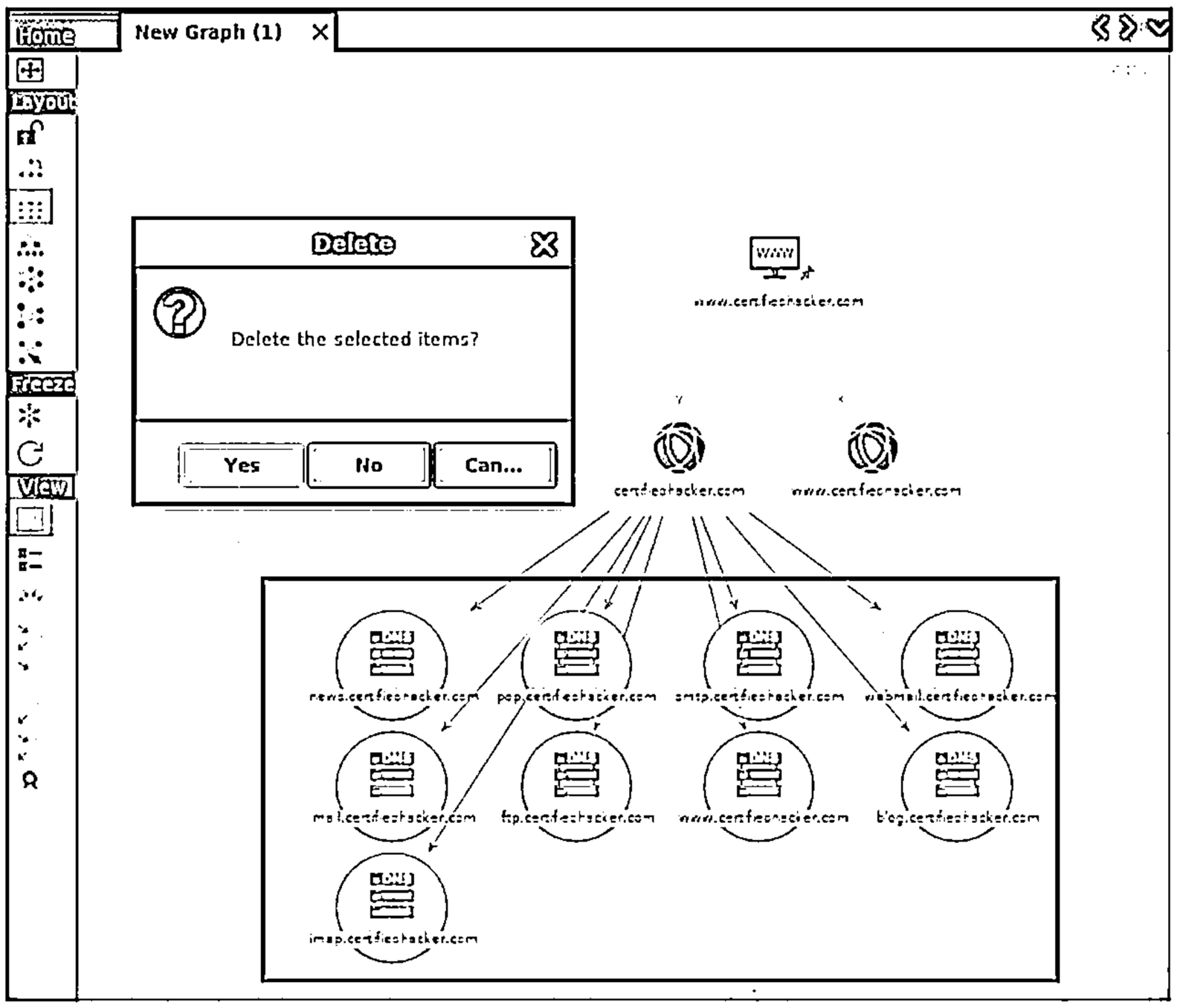


Figure 9.2.24: Deleting the Name Schemas

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

TASK 2.6

Identify the Service Oriented Architecture (SOA) Information

31. Right-click the **certifiedhacker.com** entity and select **All Transforms → To DNS Name - SOA (Start of Authority).**

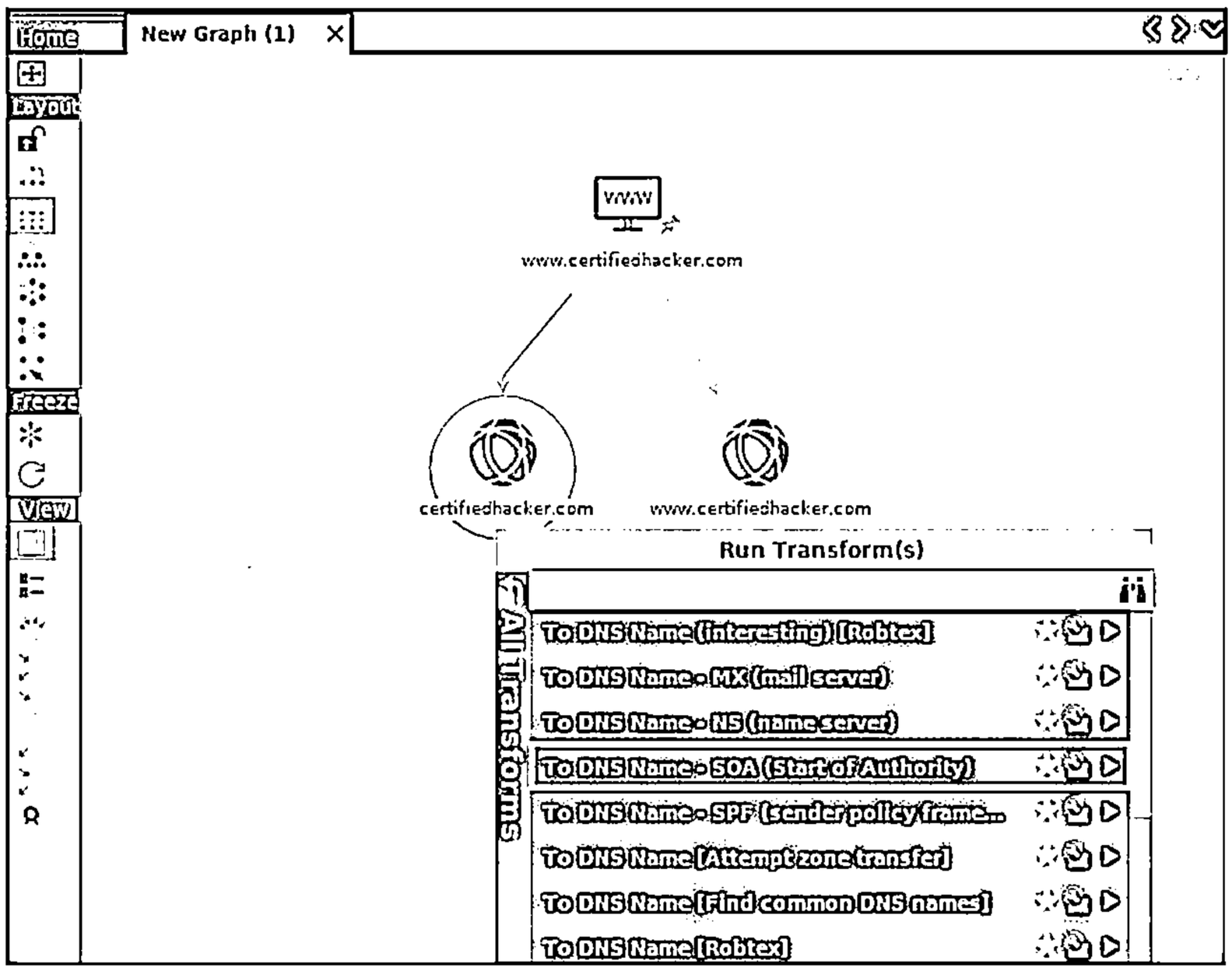


Figure 9.2.25: Selecting To DNS Name - SOA

32. This returns the primary name server and the email of the domain administrator, as shown in the following screenshot.

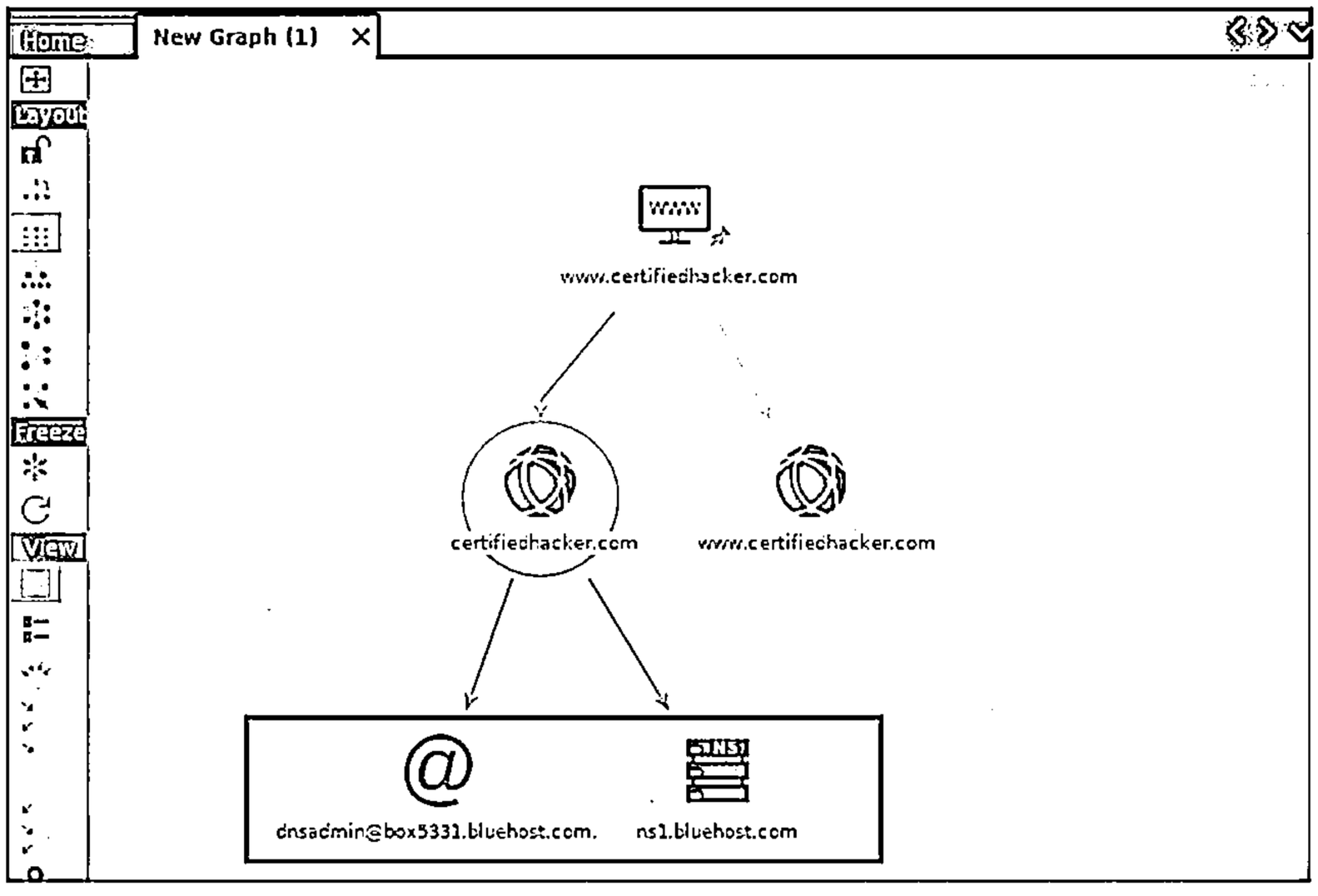


Figure 9.2.26: Primary Name Server and the Email of the Domain

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

33. By extracting the SOA related information, attackers attempt to find vulnerabilities in their services and architectures and exploit them.
34. Select both the name server and the email by dragging and deleting them.

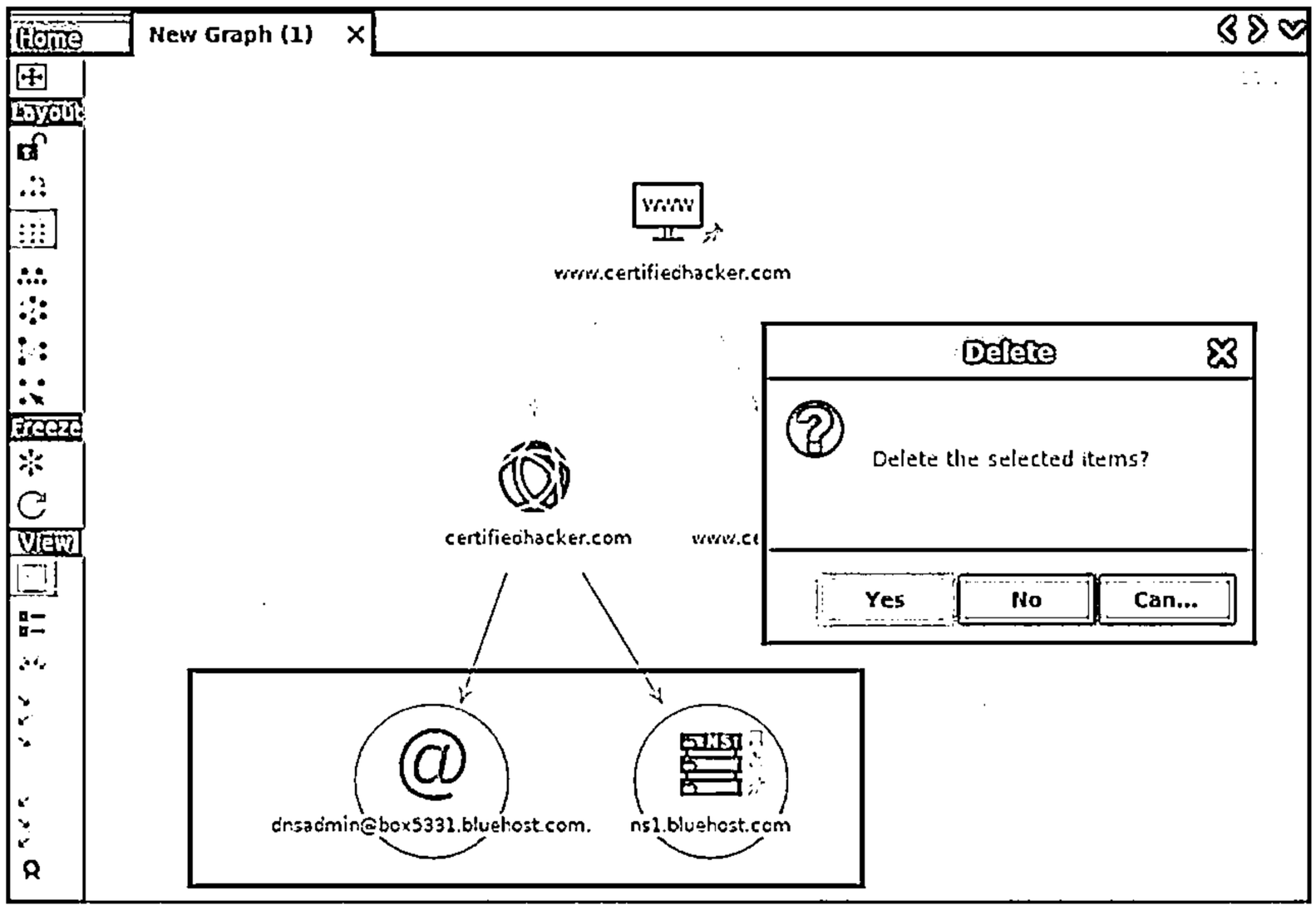


Figure 9.2.27: Deleting the Primary Name Server and the Email of the Domain

TASK 2.7

Identify the Mail Exchanger

35. Right-click the **certifiedhacker.com** entity and select **All Transforms → To DNS Name - MX (mail server).**

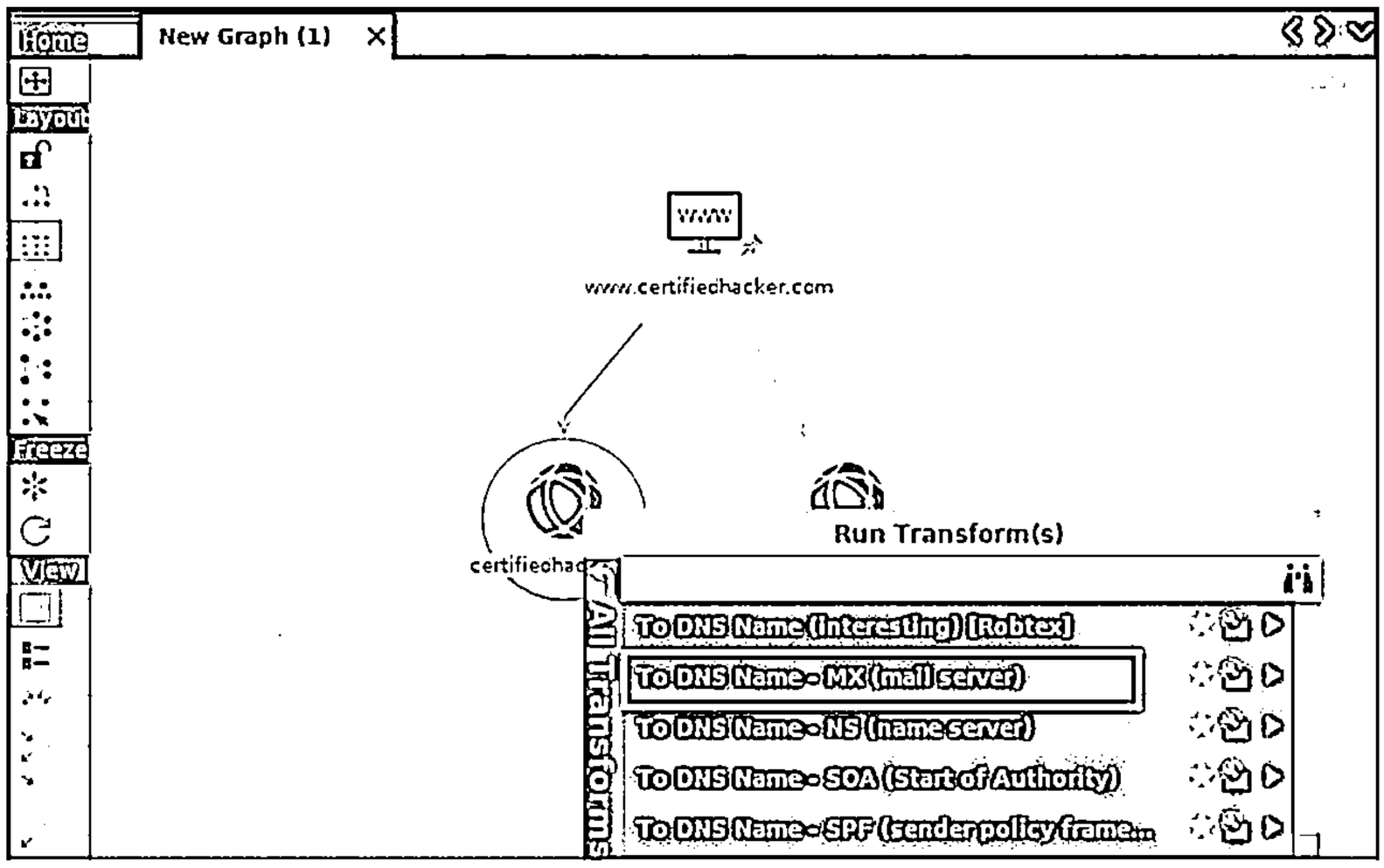


Figure 9.2.28: Selecting To DNS Name - MX (mail server)

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

36. This transform returns the mail server associated with the certifiedhacker.com domain, as shown in the following screenshot.

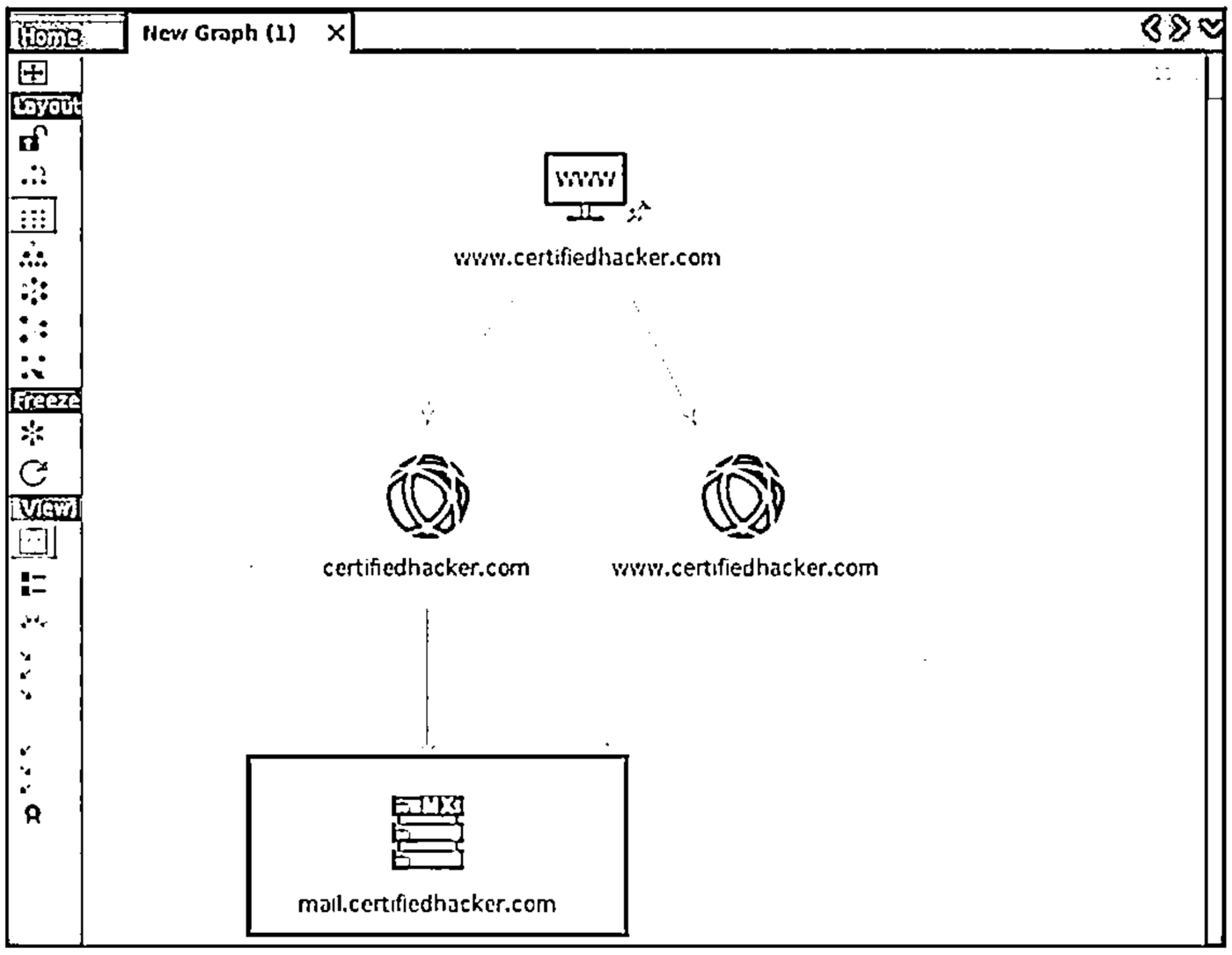


Figure 9.2.29: Mail Server Associated with the certifiedhacker.com

37. By identifying the mail exchanger server, attackers attempt to exploit the vulnerabilities in the server and, thereby, use it to perform malicious activities such as sending spam e-mails.

38. Select only the mail server by dragging and deleting it.

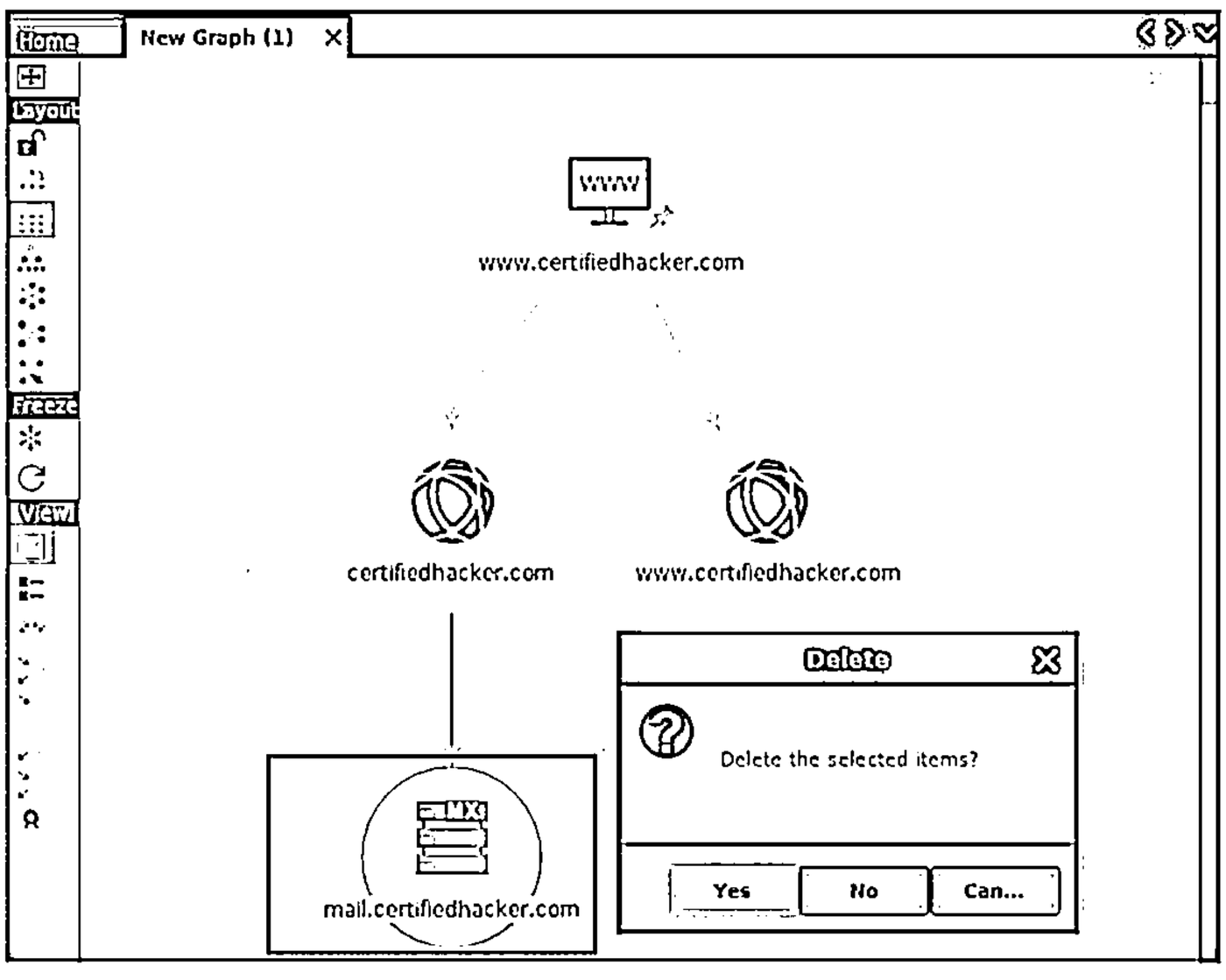


Figure 9.2.30: Deleting the Mail Server Entity

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

TASK 2.8

Identify the Name Server

39. Right-click the **certifiedhacker.com** entity and select **All Transforms → To DNS Name - NS (name server).**

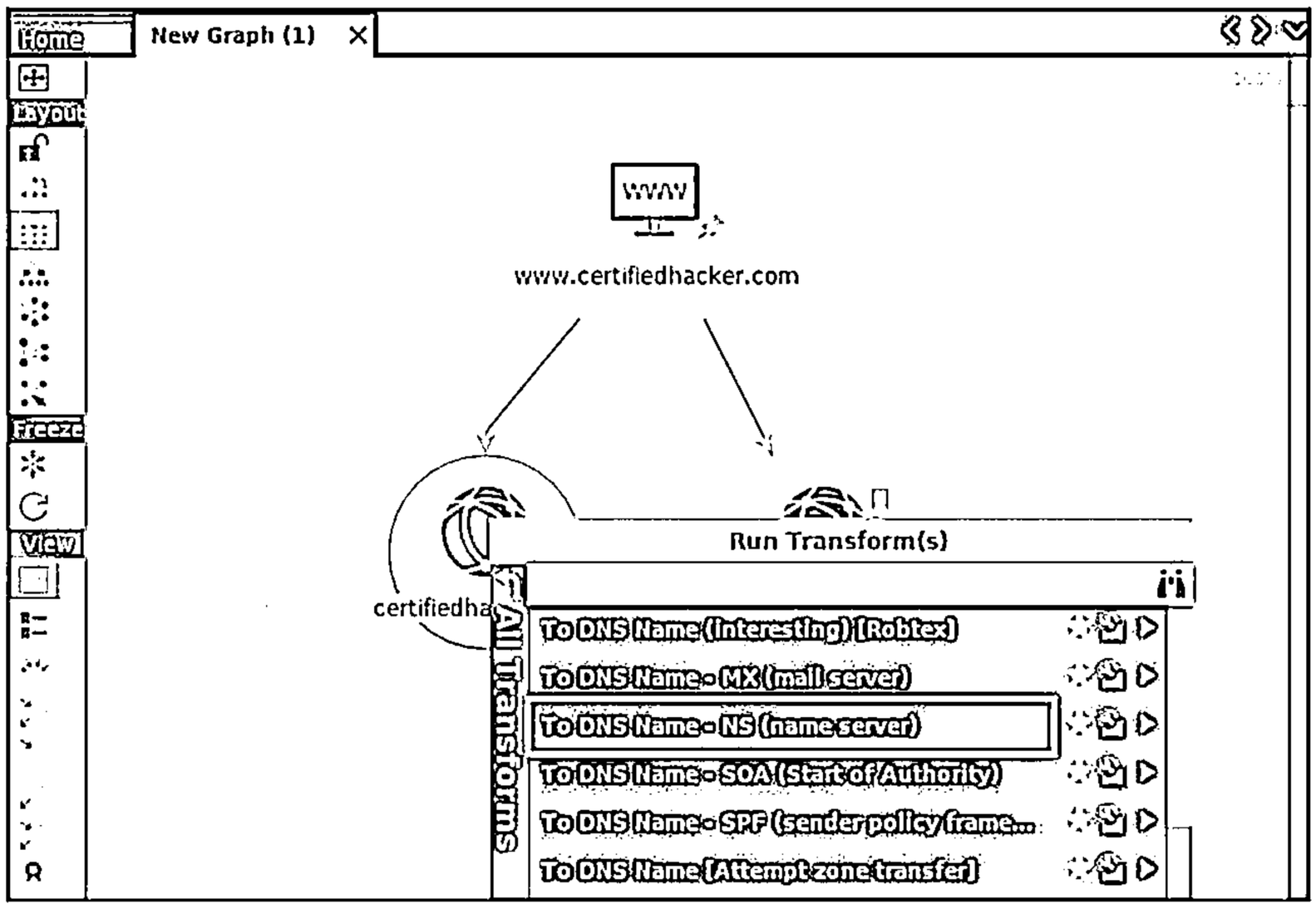


Figure 9.2.31: Selecting To DNS Name - NS (name server)

40. This returns the name servers associated with the domain, as shown in the following screenshot.

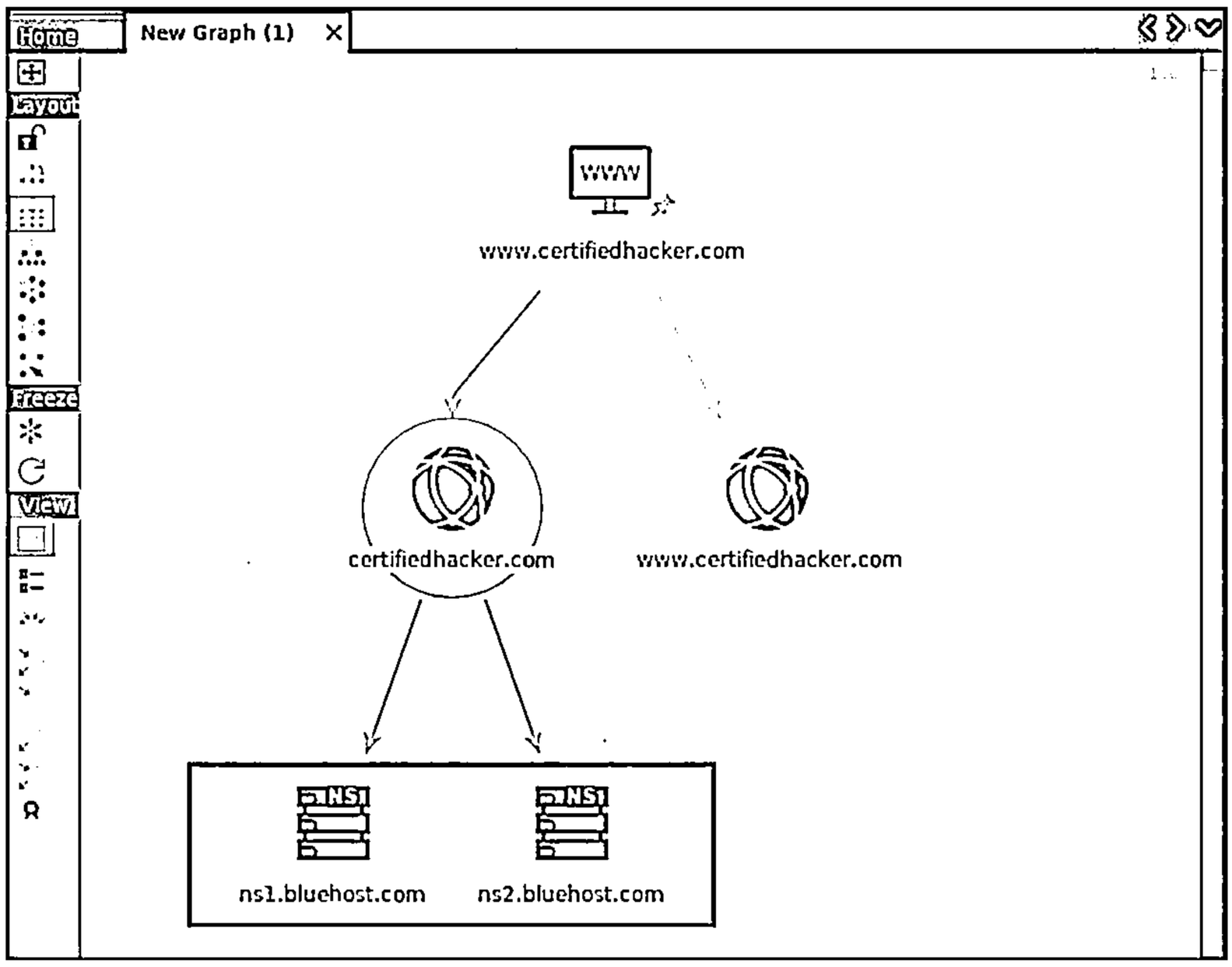


Figure 9.2.32: Name Server Associated with the Domain

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

41. By identifying the primary name server, an attacker can implement various techniques to exploit the server and thereby perform malicious activities such as DNS Hijacking and URL redirection.
42. Select both the domain and the name server by dragging and deleting them.

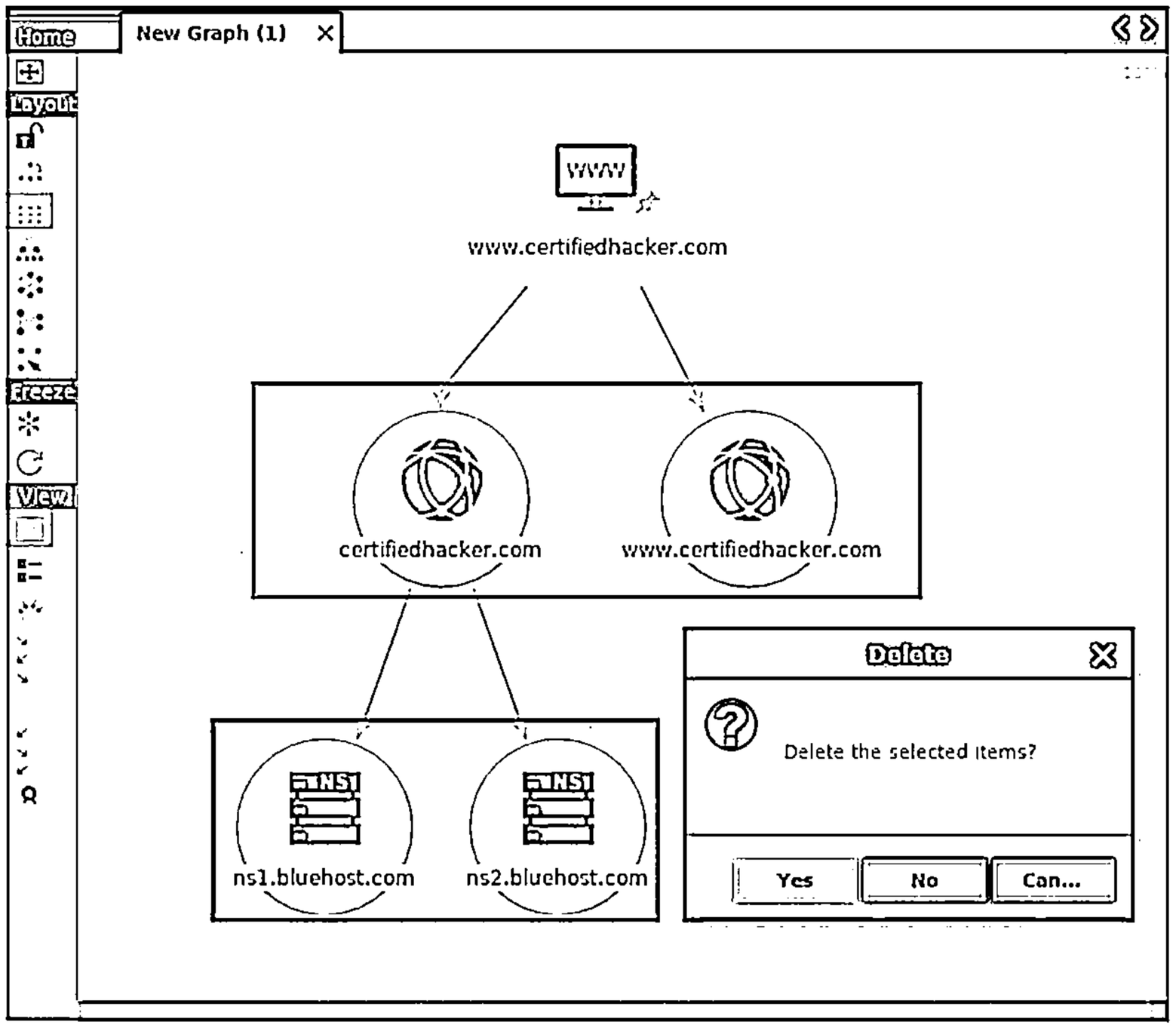


Figure 9.2.33: Delete Name Server and the Domain

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

TASK 2.9

Identify the IP Address

43. Right-click the entity and select **All Transforms → To IP Address [DNS]**.

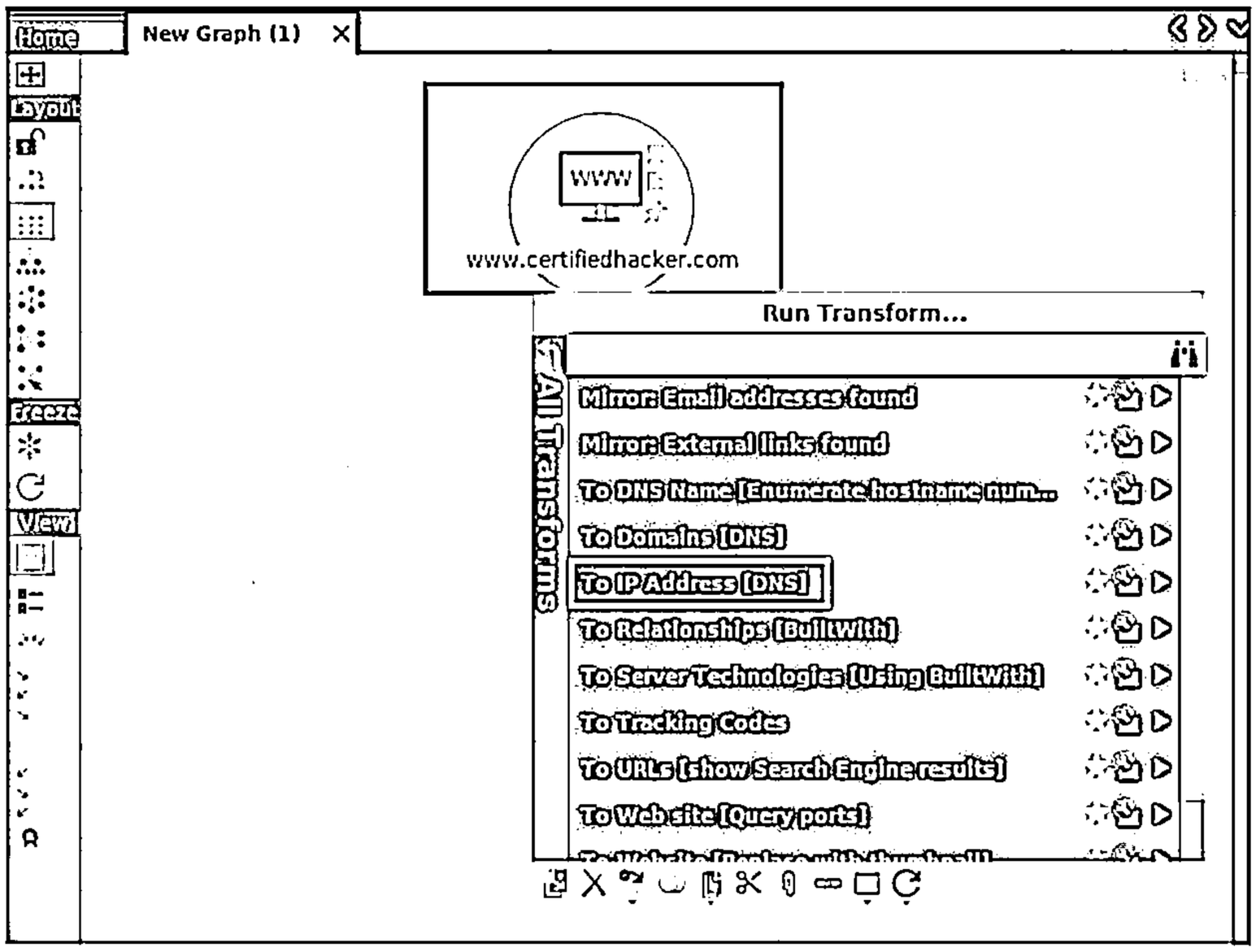


Figure 9.2.34: Selecting To IP Address [DNS]

44. This displays the IP address of the website, as shown in the following screenshot.

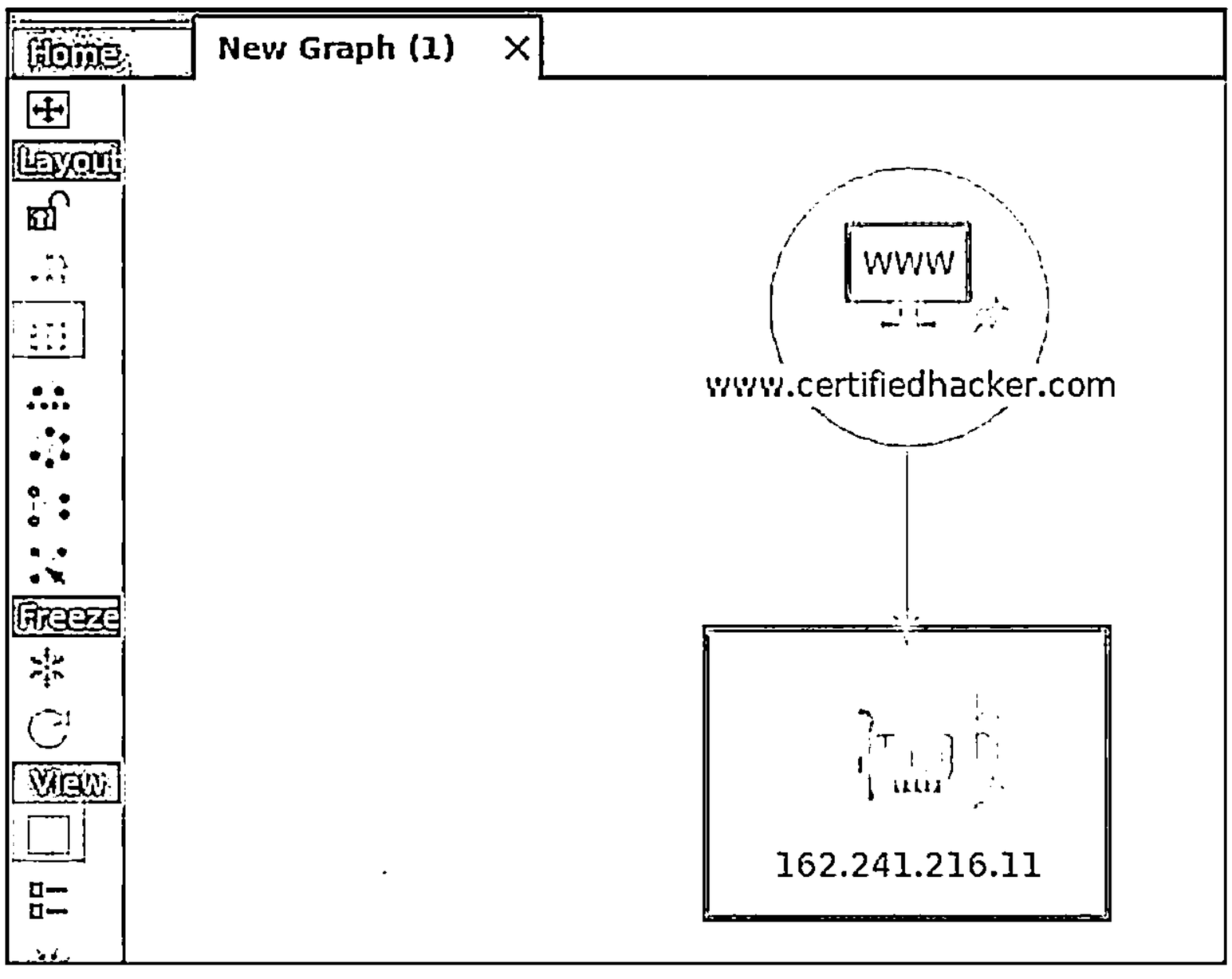


Figure 9.2.35: IP address of the website

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

45. By obtaining the IP address of the website, an attacker can simulate various scanning techniques to find open ports and vulnerabilities and, thereby, attempt to intrude in the network and exploit them.

TASK 2.10

Identify the Geographical Location

46. Right-click the IP address entity and select **All Transforms → To location [city, country]**.

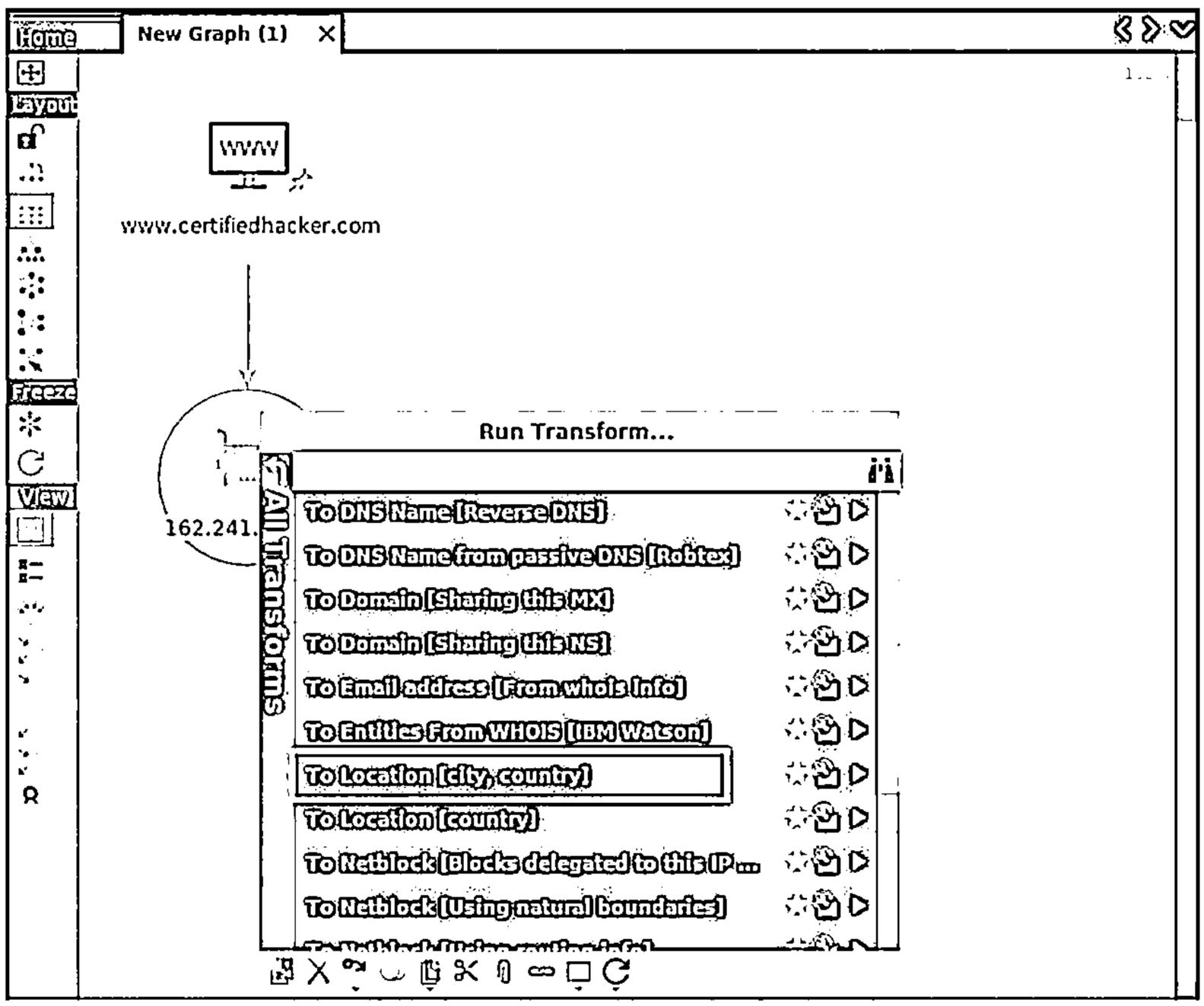


Figure 9.2.36: Selecting To location [city, country]

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

47. This transform identifies the geographical location of the IP address, as shown in the following screenshot.

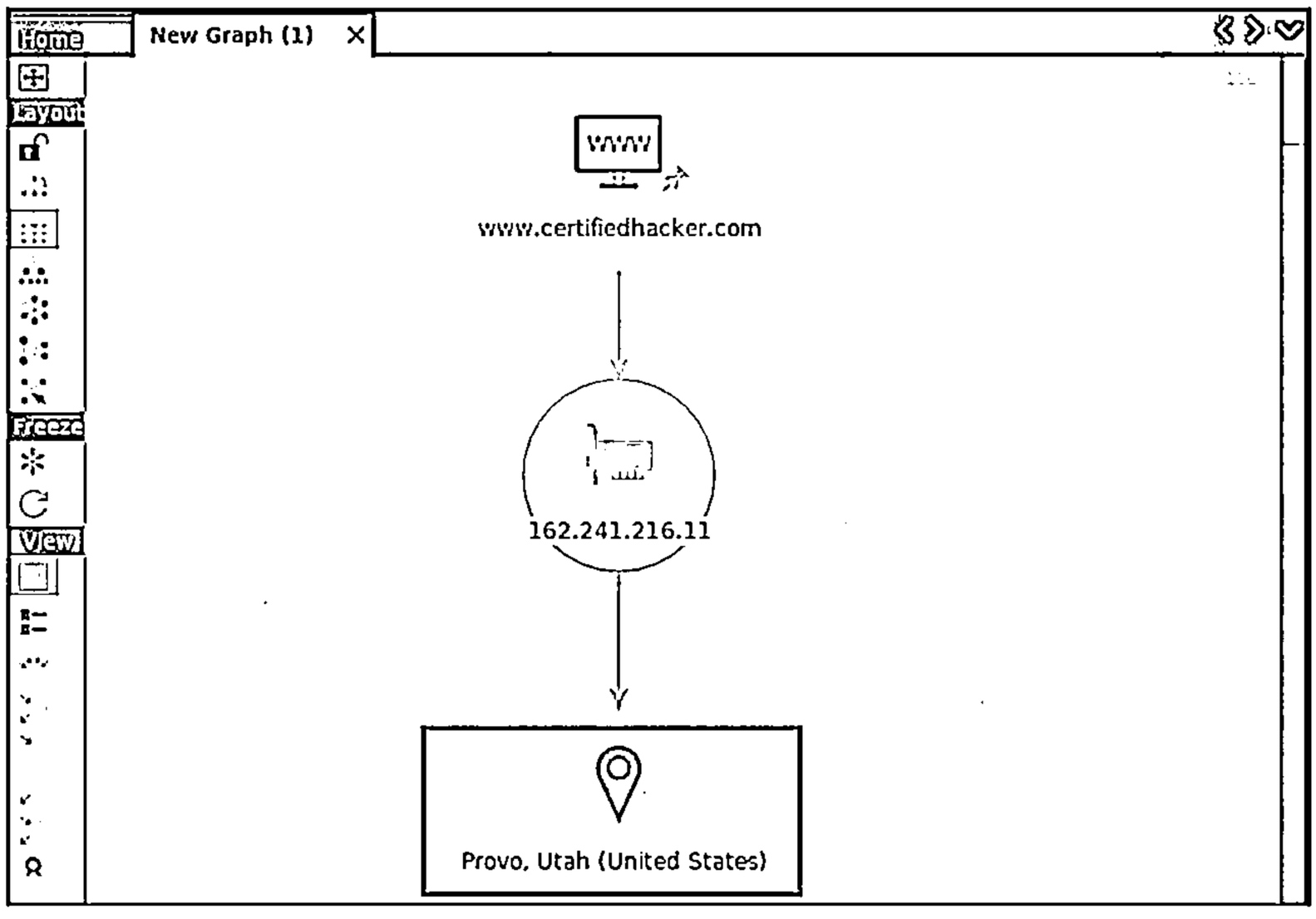


Figure 9.2.37: Geographical Location where the IP Address is Located

48. By obtaining the information related to geographical location, attackers can perform social engineering attacks by making voice calls (vishing) to an individual in an attempt to leverage sensitive information.

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

49. Now, right-click the **www.certifiedhacker.com** website entity and select **All Transforms → To Domains [DNS]**. The domains corresponding to the website display, as shown in the screenshot.

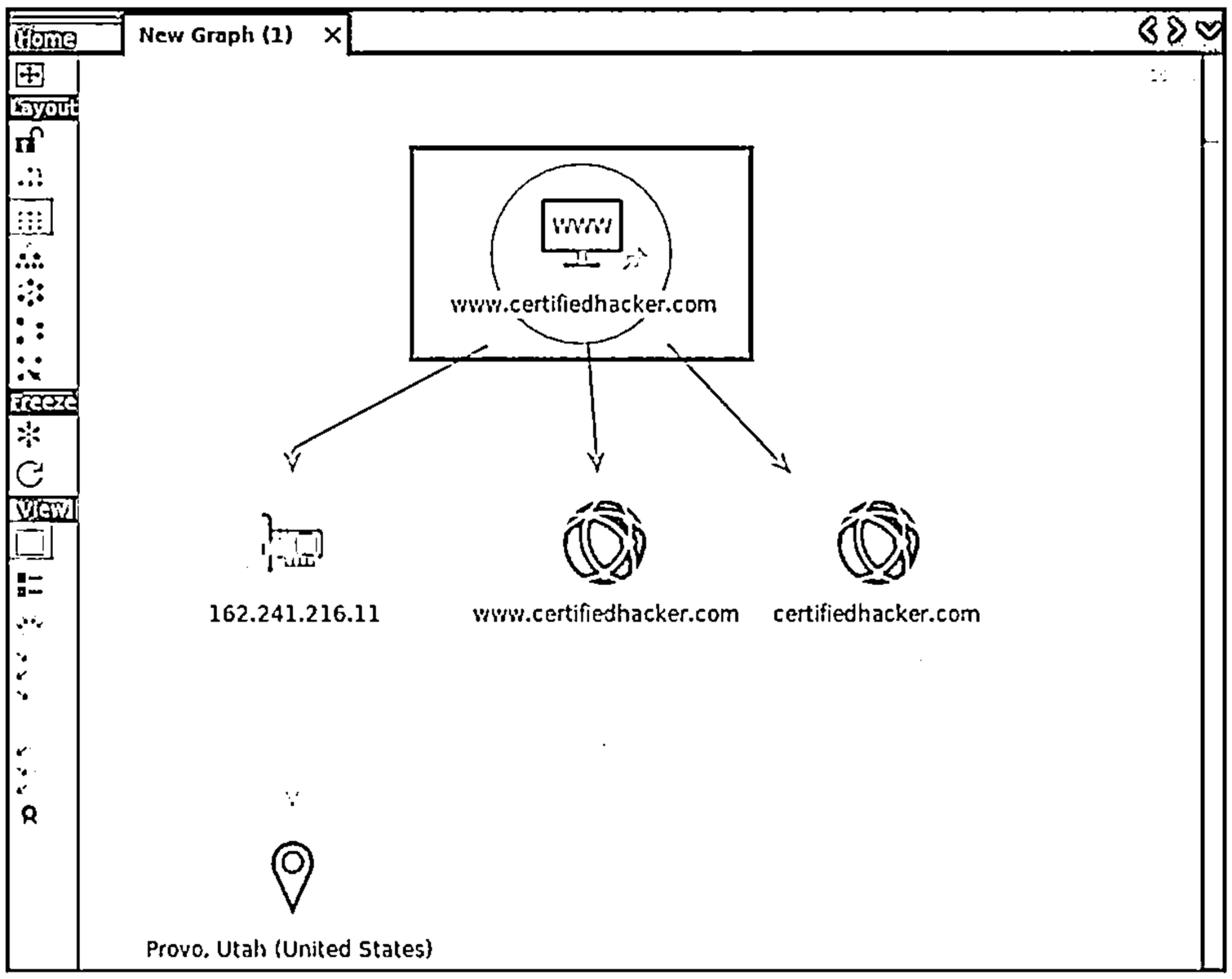


Figure 9.2.38: Domain Name Corresponding to the Website

TASK 2.11

Identify the Entities

50. Right-click the domain entity (**certifiedhacker.com**) and select **All Transform → To Entities from WHOIS [IBM Watson].**

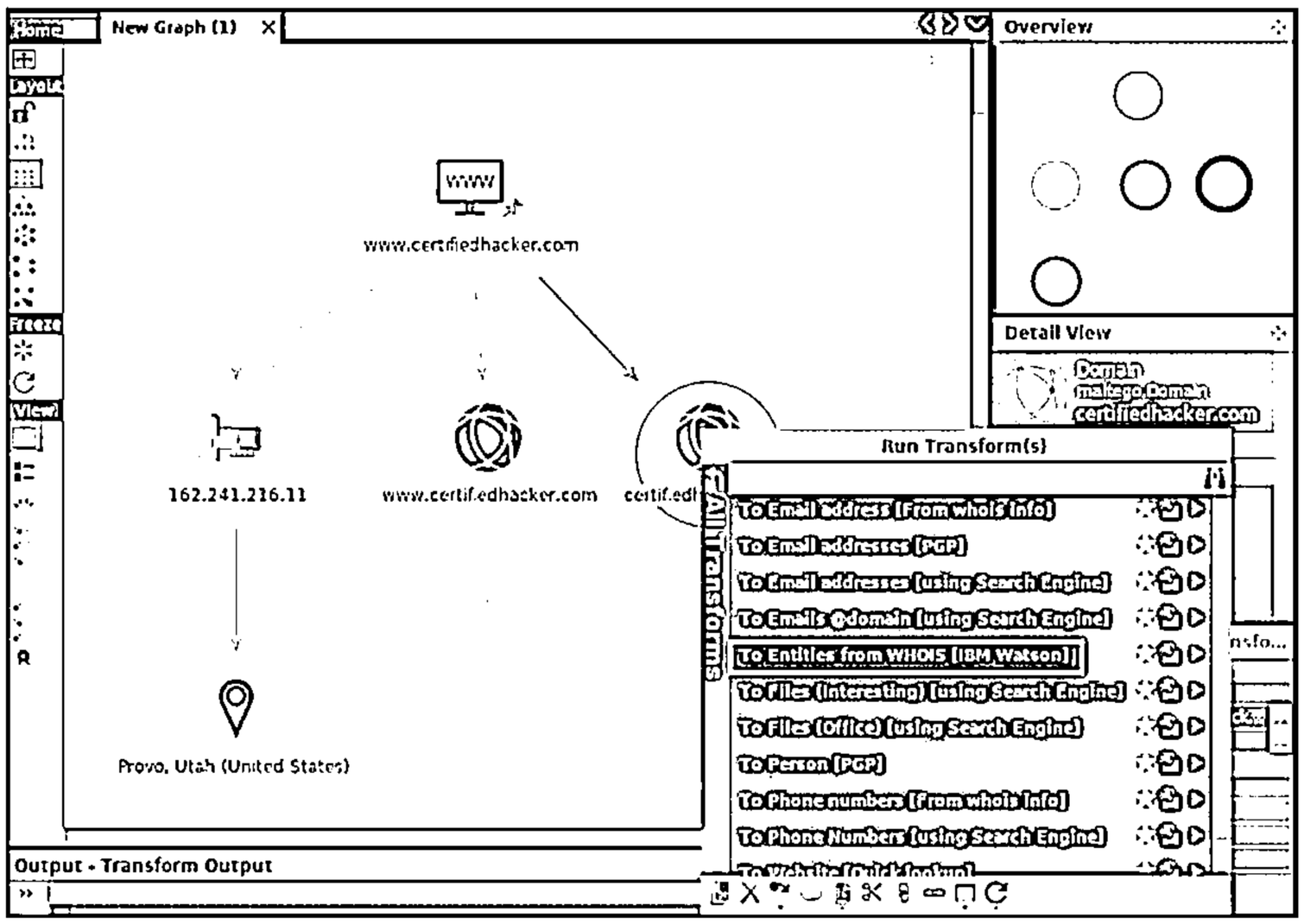


Figure 9.2.39: Selecting To Entities from whois [Alchemy]

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

51. This transform returns the entities pertaining to the owner of the domain, as shown in the following screenshot.

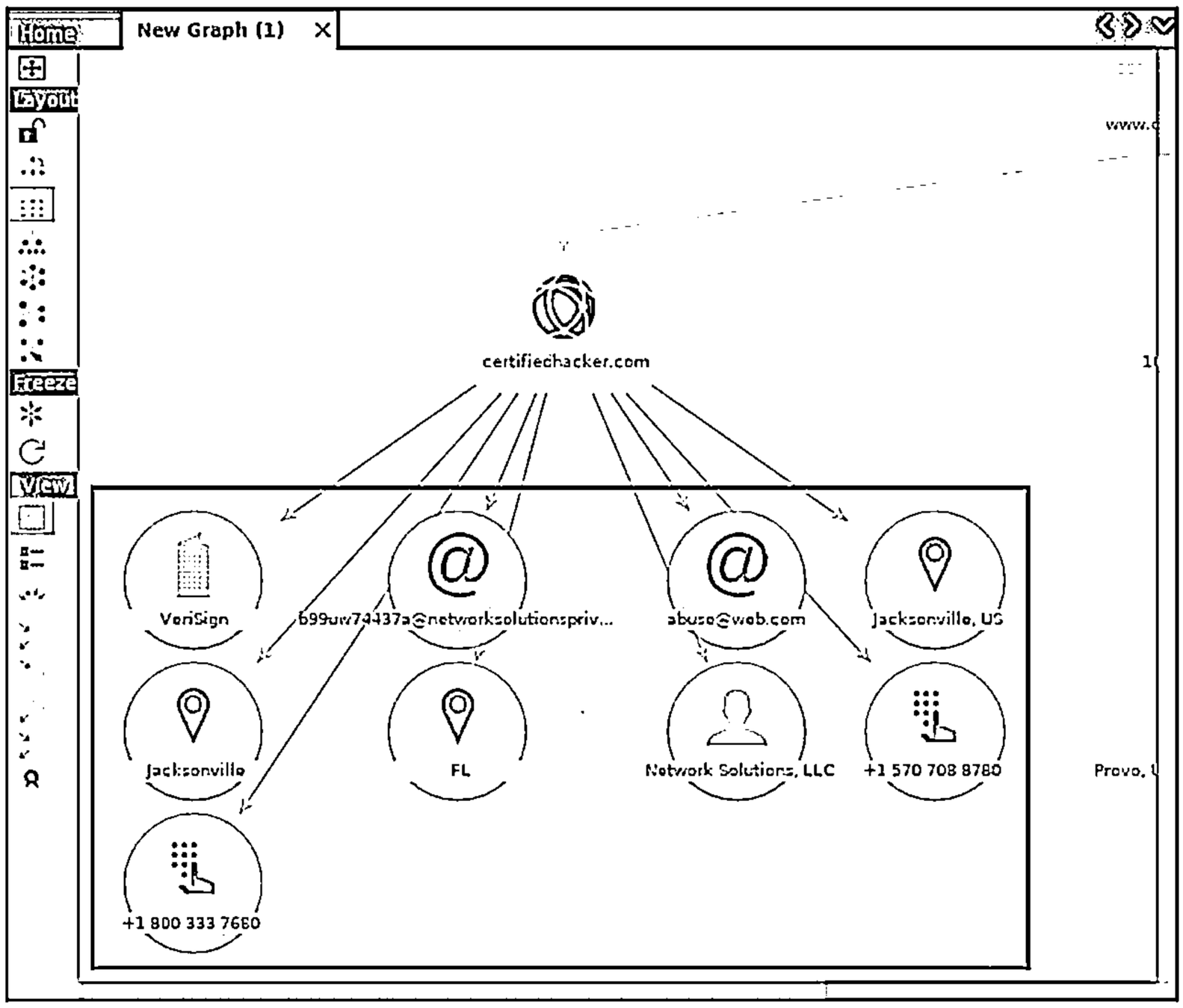


Figure 9.2.40: Entities Pertaining to the Owner of the Domain

52. By obtaining this information, you can exploit the servers displayed in the result or simulate a brute force attack or any other technique to hack into the admin mail account and send phishing emails to the contacts in that account.

TASK 2.12
Extract Other Information

53. Apart from the aforementioned methods, you can perform footprinting on the critical employee from the target organization to gather additional personal information such as email addresses, phone numbers, personal information, image, alias, phrase, etc.

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

54. In the left-pane of the Maltego GUI, click the **Personal** node under **Entity Palette** to observe a list of entities such as **Email Address**, **Phone Numbers**, **Image**, **Alias**, **Phrase**, etc.

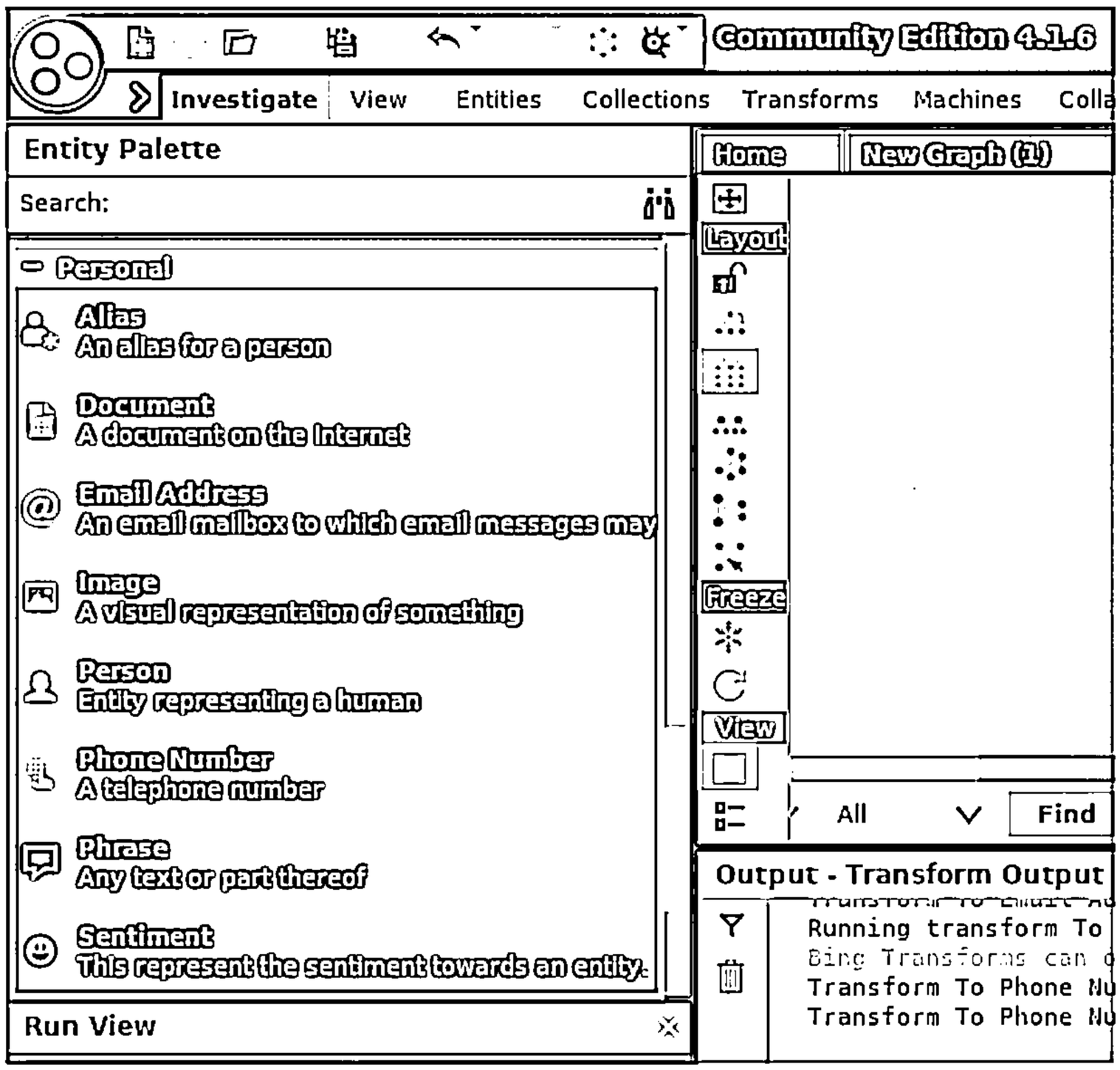


Figure 9.2.41: List of transforms to gather personal information

55. Apart from the transforms mentioned above, other transforms can track accounts and conversations of individuals who are registered on social networking sites such as Twitter. Extract all possible information.
56. By extracting all this information, you can simulate actions such as enumeration, web application hacking, social engineering, etc., which may allow you access to a system or network, gain credentials, etc.
57. This concludes the demonstration of footprinting a target using Maltego.
58. Close all open windows and document all the acquired information.

TASK 3 Footprinting a Target using OSRFramework

1. In the **Parrot Security** virtual machine, click the **MATE Terminal** icon at the top-left corner of the **Desktop** window to open a **Parrot Terminal** window.
2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

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

3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

4. Now, type **cd** and press **Enter** to jump to the root directory.

TASK 3.1

Install OSRFramework

5. In the **Parrot Terminal** window, type **git clone https://github.com/i3visio/osrframework** and press **Enter**.

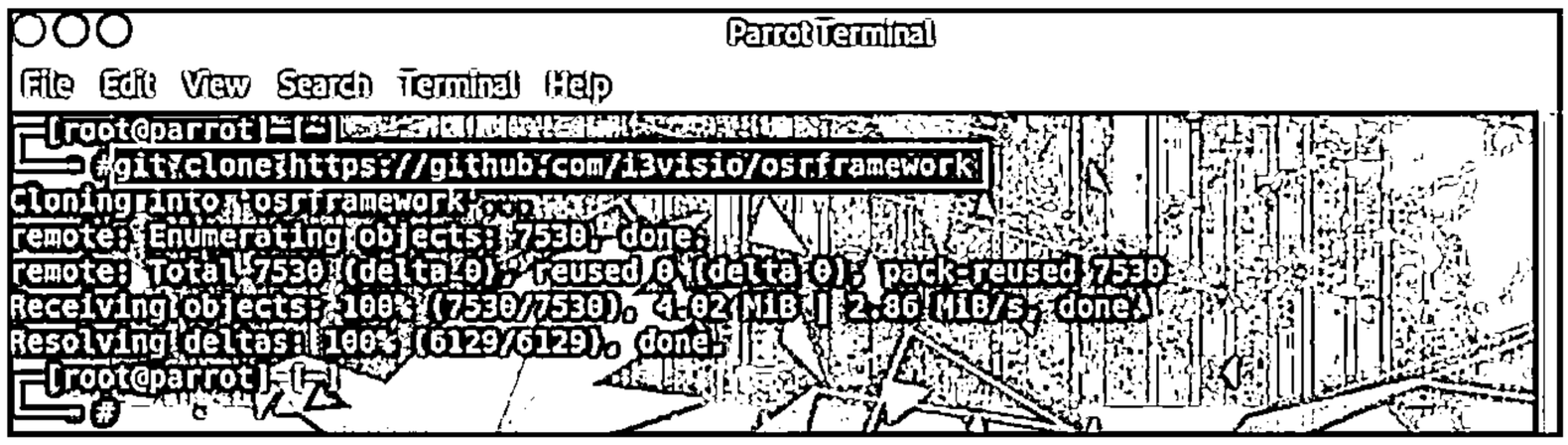


Figure 9.3.1: Cloning OSRFramework tool

OSRFramework is a set of libraries that are used to perform Open Source Intelligence tasks. They include references to many different applications related to username checking, DNS lookups, information leaks research, deep web search, regular expressions extraction, and many others. It also provides a way of making these queries graphically as well as several interfaces to interact with such as OSRFConsole or a Web interface.

Note: You can also access the tool repository from the **CEH-Tools** folder available in **Windows 10** virtual machine, in case, the GitHub link does not exist, or you are unable to clone the tool repository. Follow the steps below in order to access **CEH-Tools** folder from the **Parrot Security** virtual machine:

- Open any explorer window and press **Ctrl+L**. The **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access **Windows 10** shared folders.
- The security pop-up appears; enter the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.
- The **Windows shares on 10.10.10.10** window appears; navigate to the location **CEH-Tools/CEHv11 Module 02 Footprinting and Reconnaissance/GitHub Tools/** and copy the **osrframework** folder.
- Paste the copied **osrframework** folder on the location **/home/attacker/**.
- In the terminal window, type **mv /home/attacker/osrframework /root/**.

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

6. Type **pip3 install osrframework** and press **Enter** to install the OSRFramework.

Note: If **osrframework** is already installed, skip to **Step #8**.

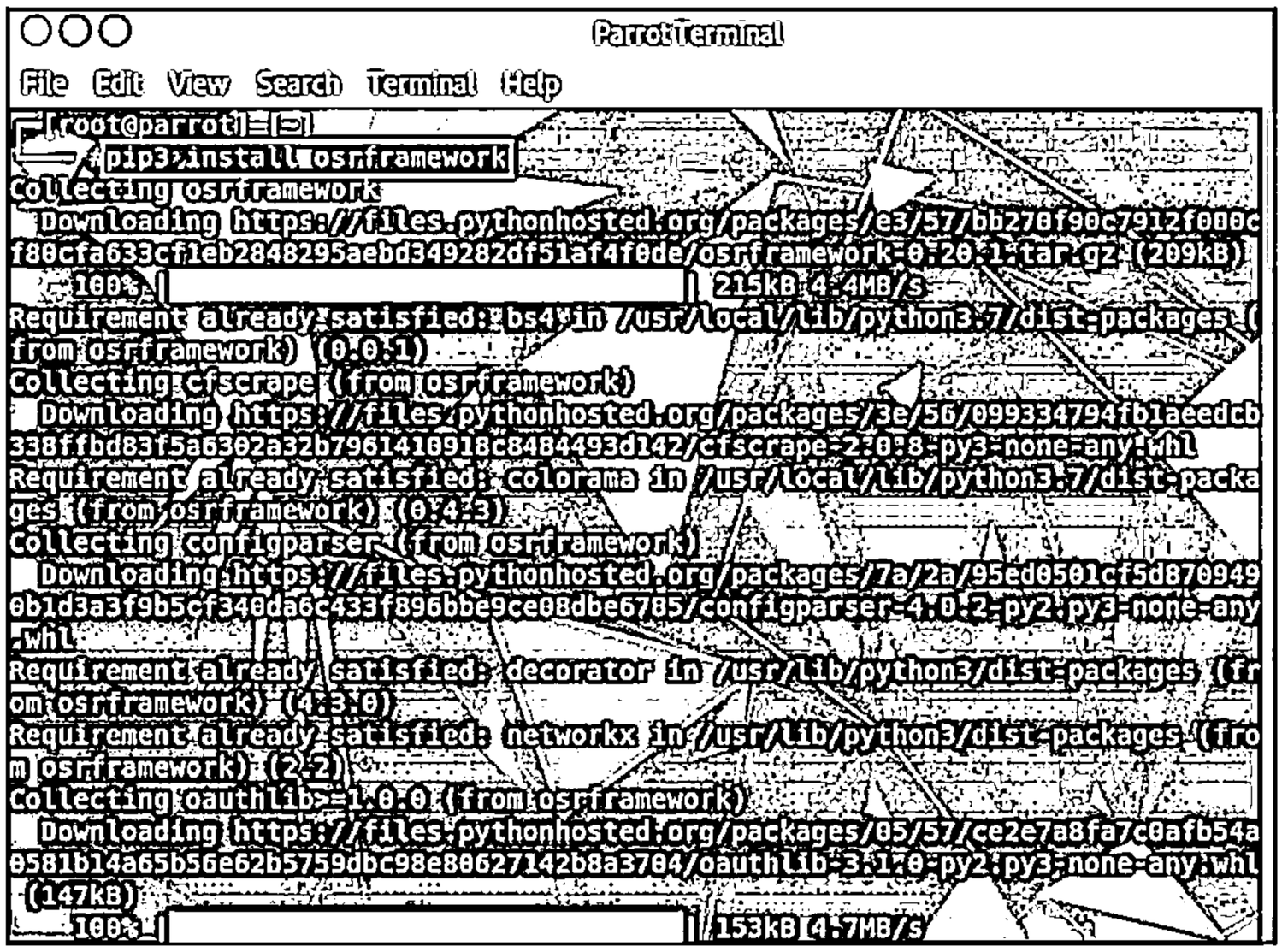


Figure 9.3.2: Installing OSRFramework through command line

7. To upgrade the OSRFramework to its latest version, type **pip3 install osrframework --upgrade** and press **Enter**. If the tool is not updated, the updates will start installing, as shown in the screenshot.

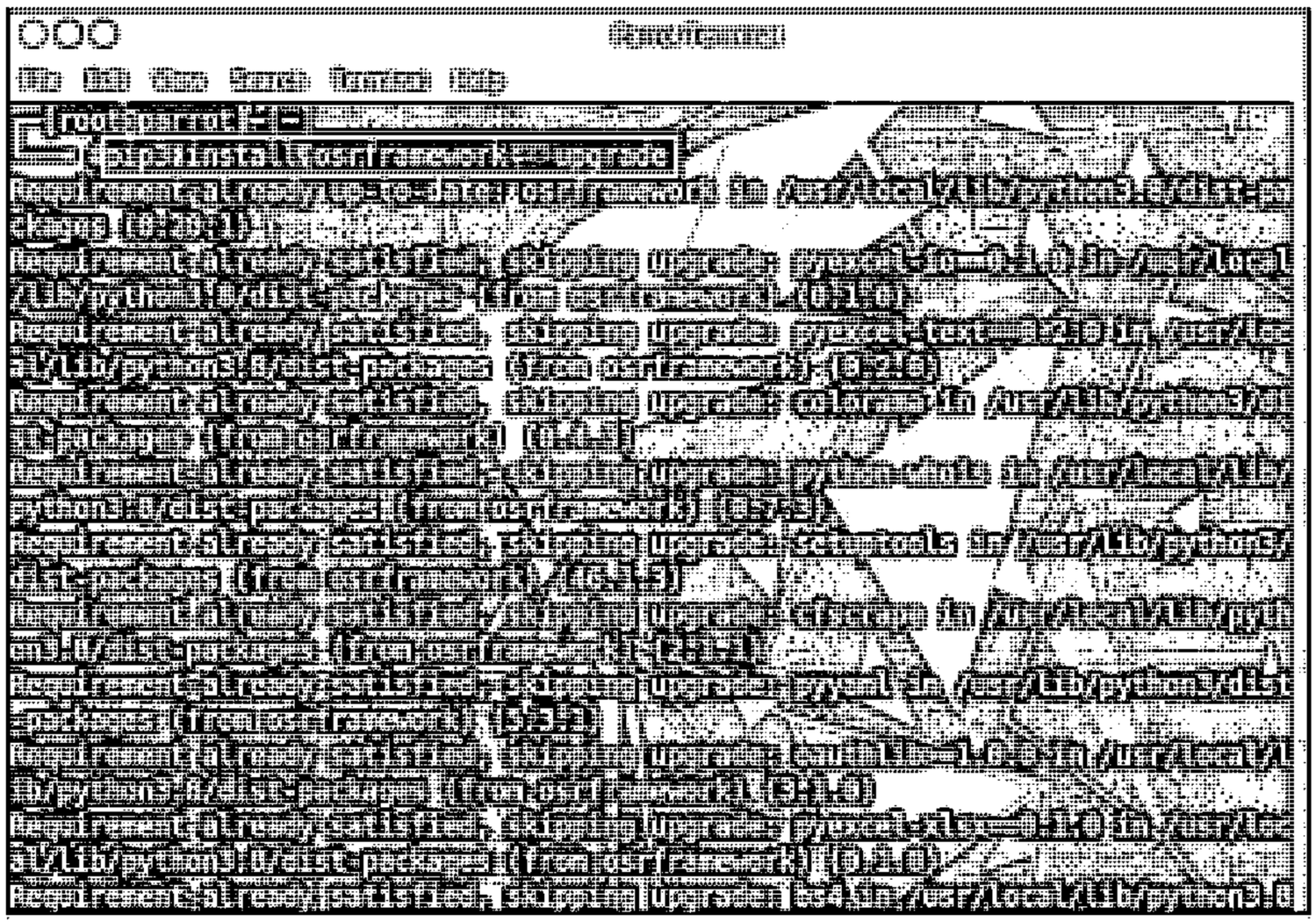


Figure 9.3.3: Upgrading OSRFramework

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

TASK 3.2

Check the Target User Profile on Social Networking Platforms

8. Use **usufy.py** to check for the existence of a profile for given user details on different social networking platforms. Type **usufy.py -n <target user name or profile name> -p <target platform>** (here, the target user name or profile is **Mark Zuckerberg** and the target platforms are **twitter, facebook**, and **youtube**) and press **Enter**.

Note: **-n** is the list of nicknames to process and **-p** is for the platform for search.

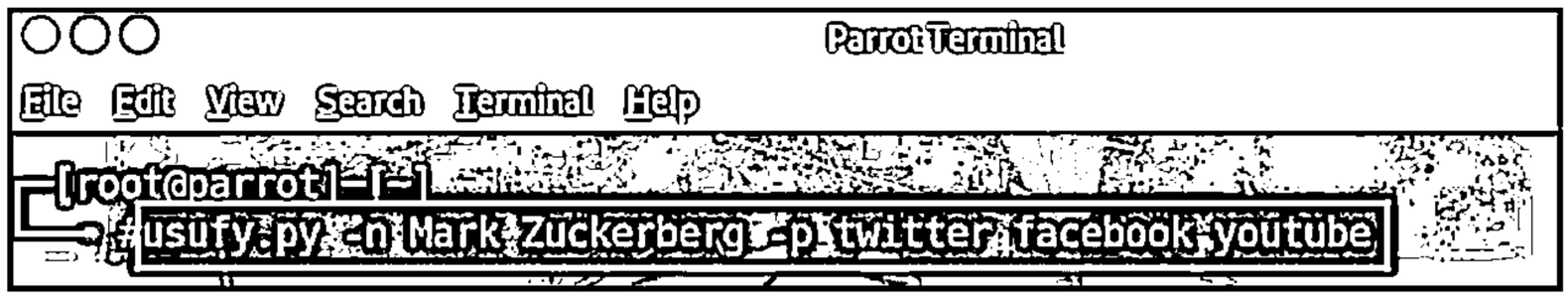


Figure 9.3.4: Using usufy.py to search twitter, facebook, and youtube for users

9. The usufy.py will search the user details in the mentioned platforms and will provide you with the existence of the user, as shown in the screenshot.

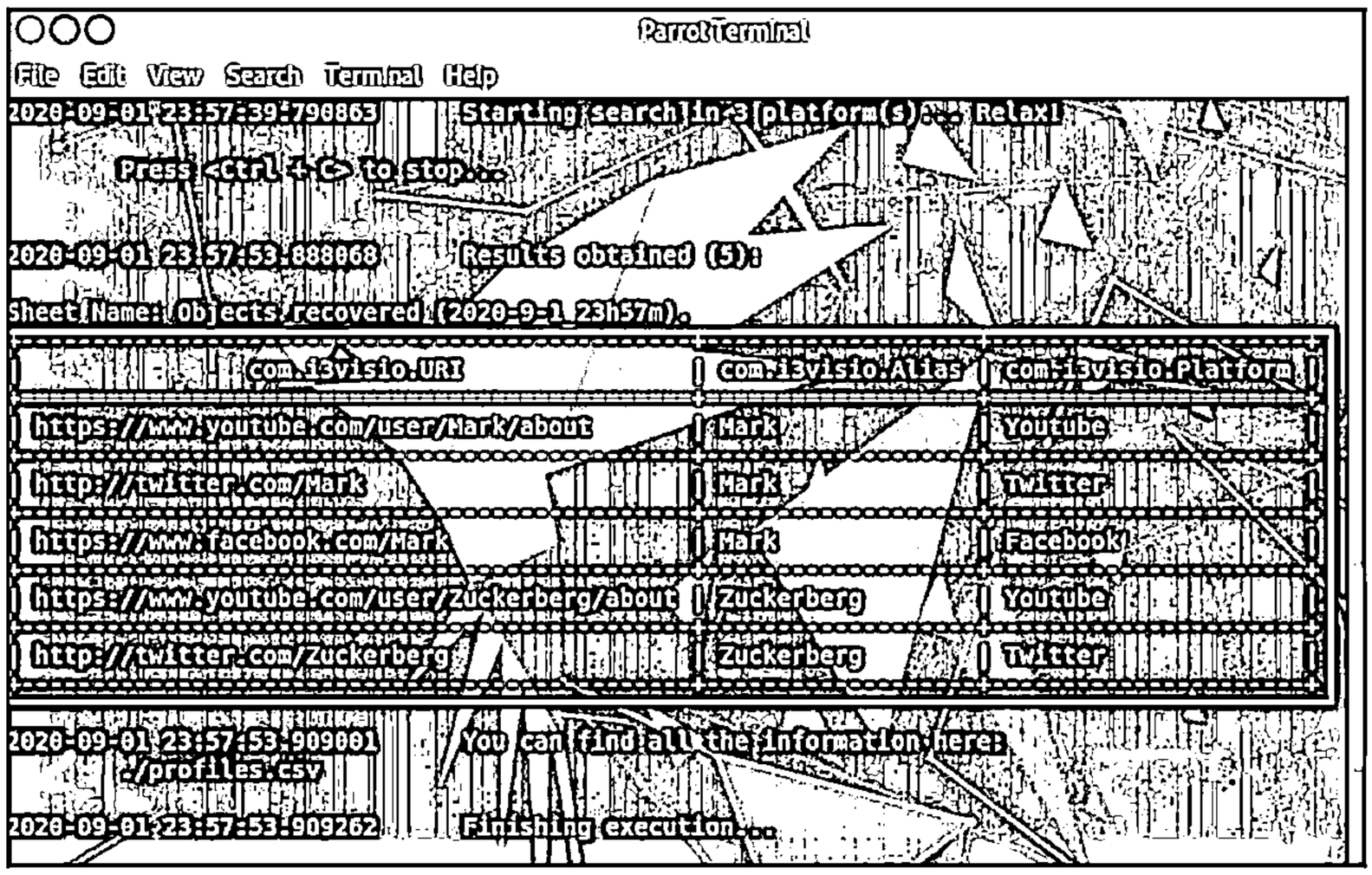


Figure 9.3.5: usufy.py showing a summary of the results obtained through search

TASK 3.3

Check the Pages of a Target on Social Networking Platforms

10. Use **domainfy.py** to check with the existing domains using words and nicknames. Type **domainfy.py -n [Domain Name] -t all** (here, the target domain name is **eccouncil**) and press **Enter**.

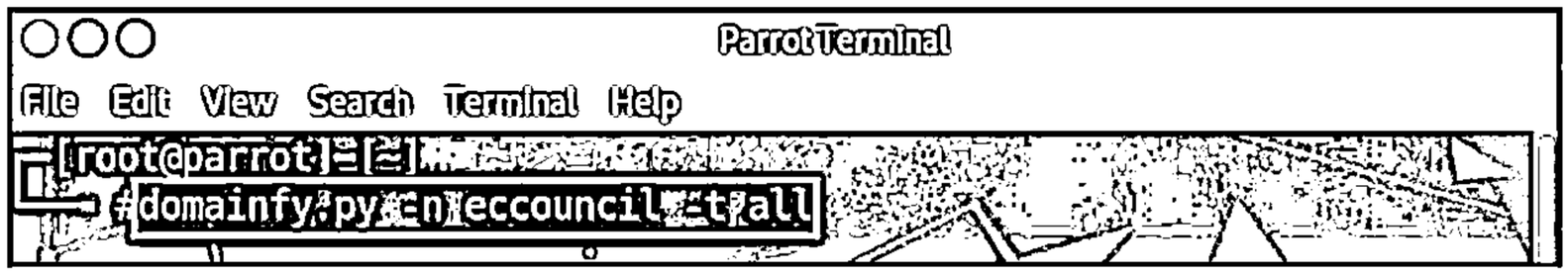


Figure 9.3.6: using searchfy.py with ECCOUNCIL as a target page

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

11. The tool will retrieve all the domains related to the target domain.

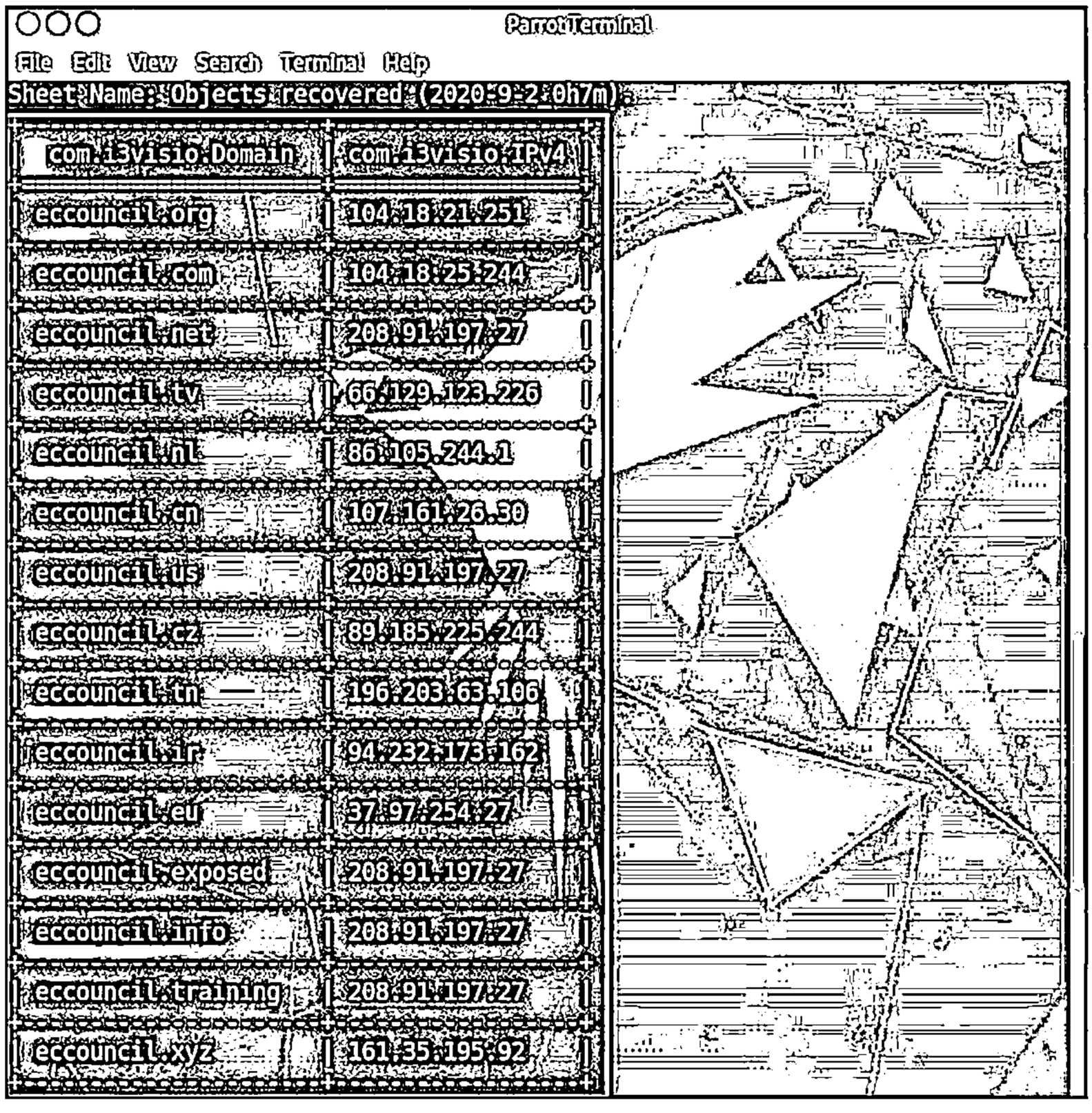


Figure 9.3.7: List of users on targeted social webpages

12. Similarly, you can use following OSRFramework packages to gather information about the target.
    - **searchfy.py** – Gathers information about the users on social networking pages
    - **mailfy.py** – Gathers information about email accounts
    - **phonefy.py** – Checks for the existence of a given series of phones
    - **entify.py** – Extracts entities using regular expressions from provided URLs
13. This concludes the demonstration of gathering information about the target user aliases from multiple social media platforms using OSRFramework.
14. Close all open windows and document all the acquired information.
15. Turn off the **Parrot Security** virtual machine.

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

TASK 4 Footprinting a Target using FOCA

TASK 4.1

Launch FOCA

1. Turn on the **Windows 10** virtual machine.
2. Login to the **Windows 10** virtual machine with Username: **Admin** and Password: **Pa$$w0rd**.
3. To launch **FOCA**, navigate to **E:\CEH-Tools\CEHv11 Module 02 Footprinting and Reconnaissance\Footprinting Tools\FOCA\bin** and double-click **FOCA.exe**.
4. The **FOCA** main window appears, as shown in the screenshot.

FOCA (Fingerprinting Organizations with Collected Archives) is a tool that reveals metadata and shrouded data. It examines a wide mixture of records, with the most widely recognized being Microsoft Office, Open Office, or PDF documents. It may also work with Adobe InDesign or SVG files. These archives may be on-site pages and can be downloaded and dissected with FOCA.

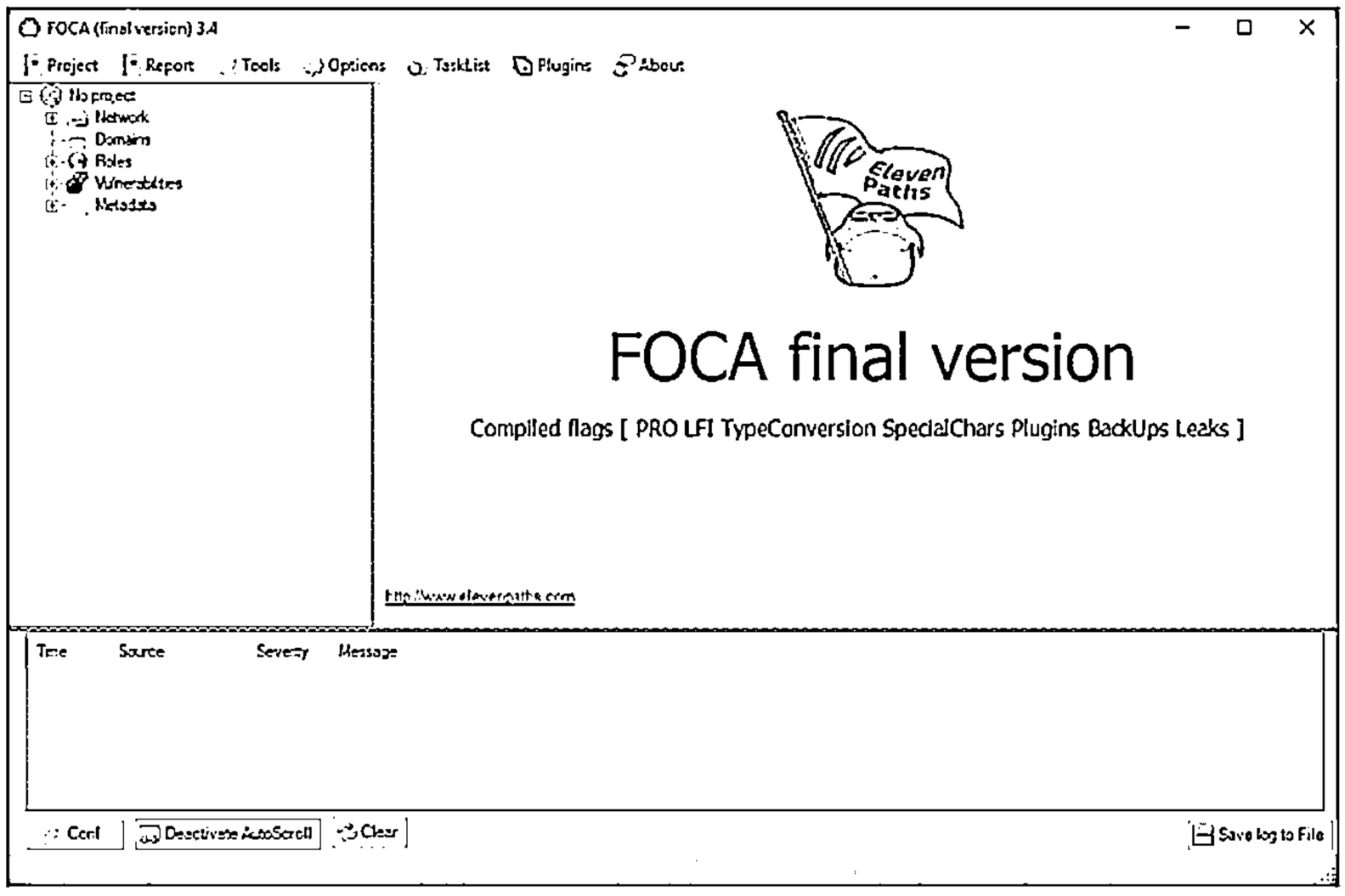


Figure 9.4.1: FOCA main window

TASK 4.2

Create a New Project

5. Create a new project by navigating to **Project** and click **New project** on the menu bar.

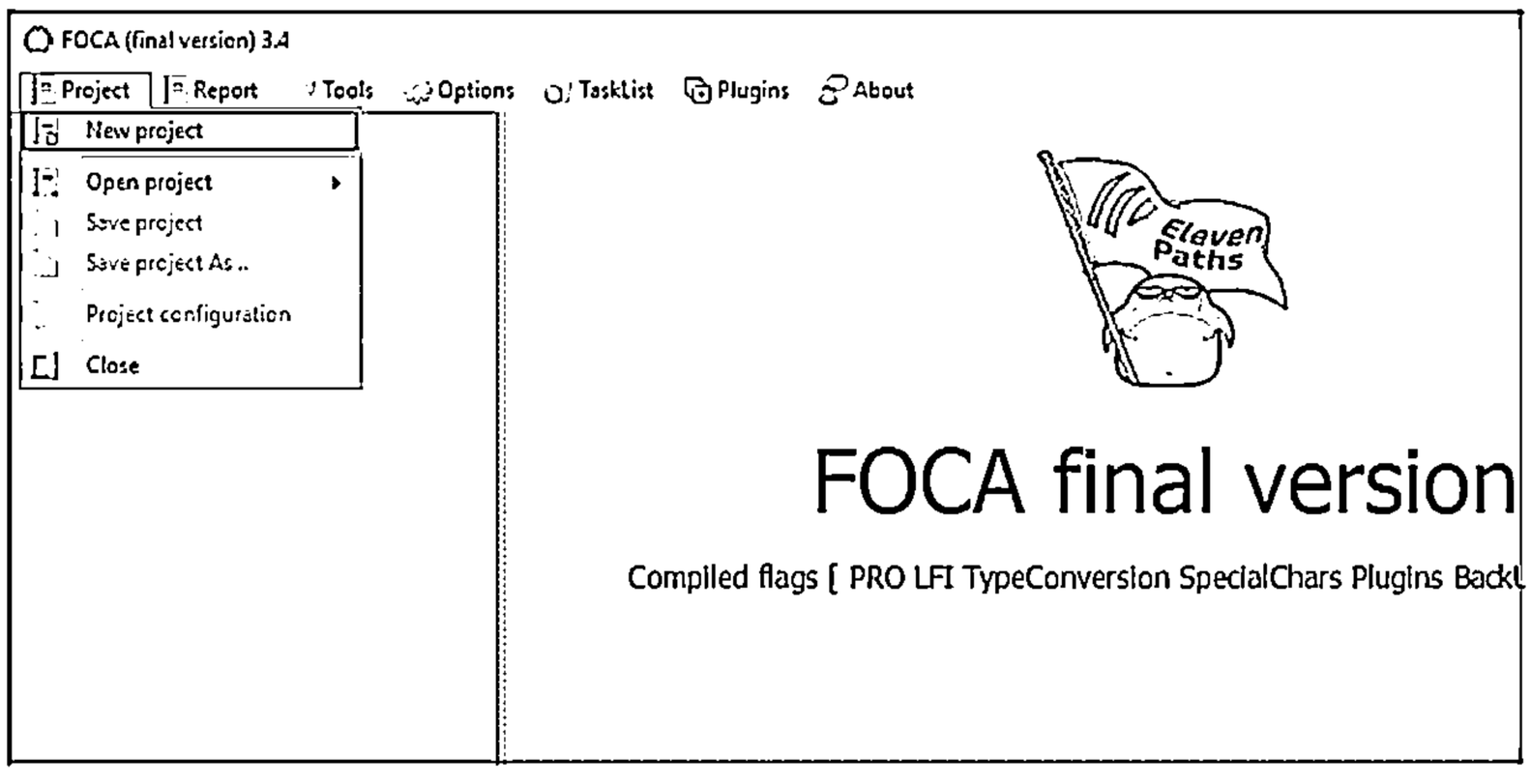


Figure 9.4.2: FOCA creating a new project

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

6. The **FOCA** new project wizard appears:
   a. Enter a project name in the **Project name** field (here, **Project of www.eccouncil.org**).
   b. Enter the domain website in the **Domain website** field (here, **www.eccouncil.org**).
   c. You can leave the optional **Alternative domains** field empty.
   d. Under the **Folder where save documents** field, click on the **Folder** icon. When the **Browse For Folder** pop up window appears, select the location to save the document that is extracted by FOCA (here, **Desktop**) and click **OK**.
   e. Leave the other settings to default and click the **Create** button.

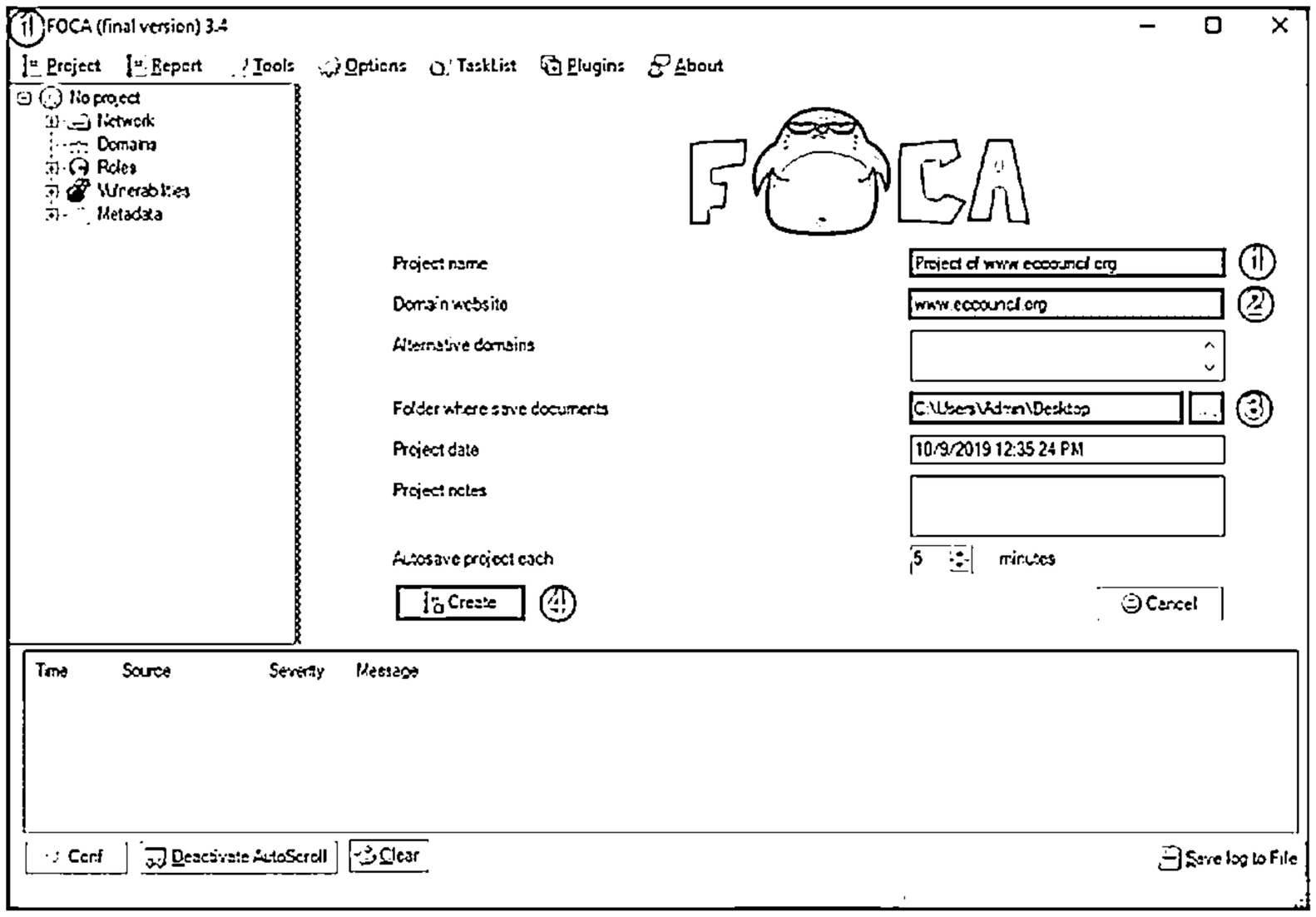


Figure 9.4.3: FOCA providing details for a new project

7. The **Save project as ...** window appears. Provide the desired location (here, **Desktop**) to save the FOCA project and type a file name in the **File name** field and click **Save**.

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

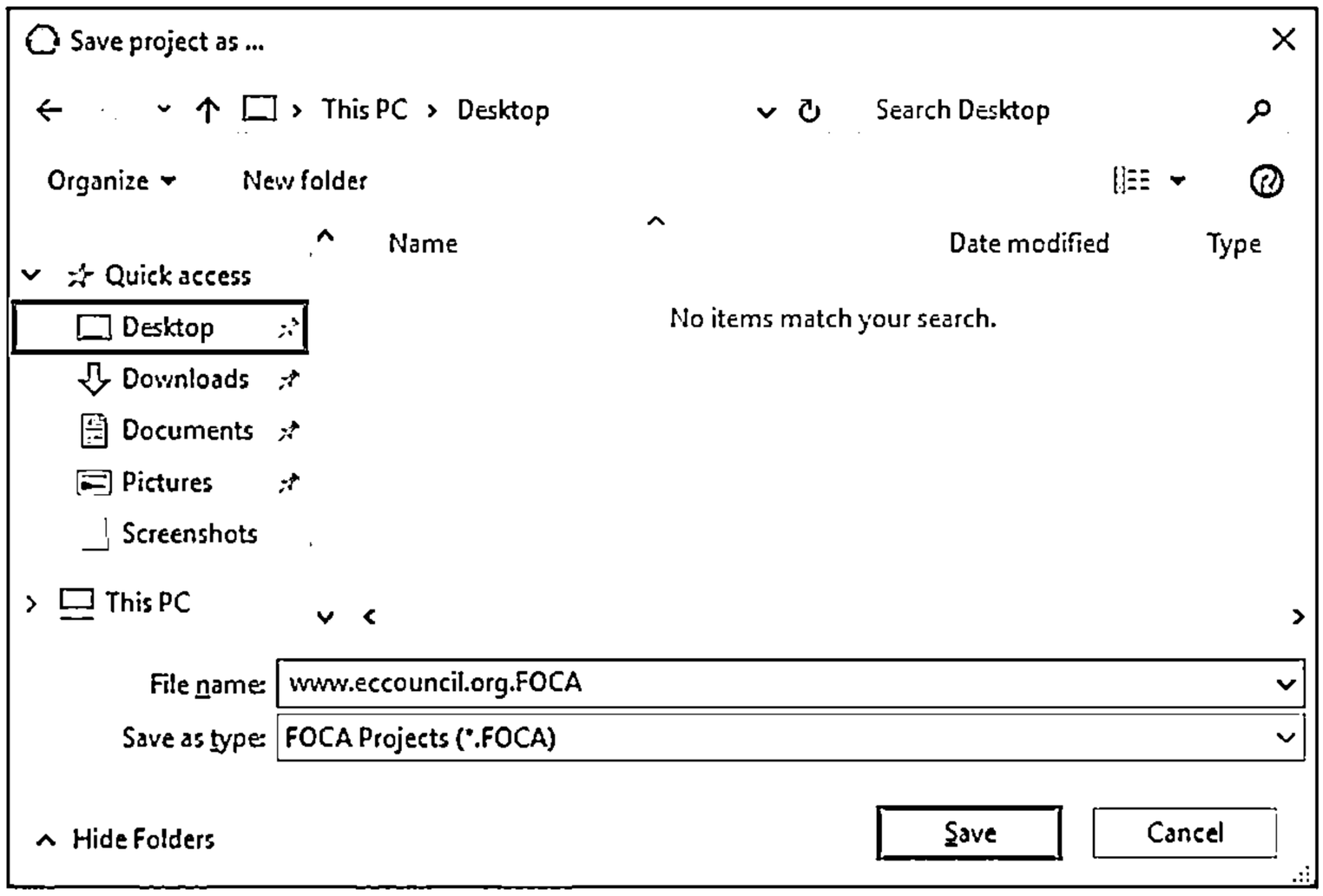


Figure 9.4.4: FOCA Save project as window

8. The **Project saved successfully!** pop-up window appears; click **OK**.

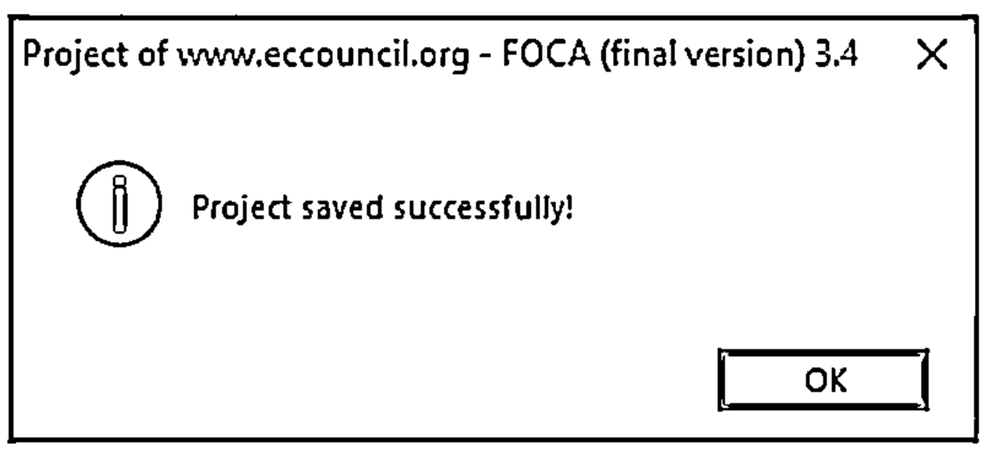


Figure 9.4.5: FOCA Project Saved

TASK 4.3

Extract Metadata of a Target Domain

9. To extract the information of the targeted domain, select all three search engines (**Google**, **Bing**, and **Exalead**) present under **Search engines**, and then click the **Search All** button.

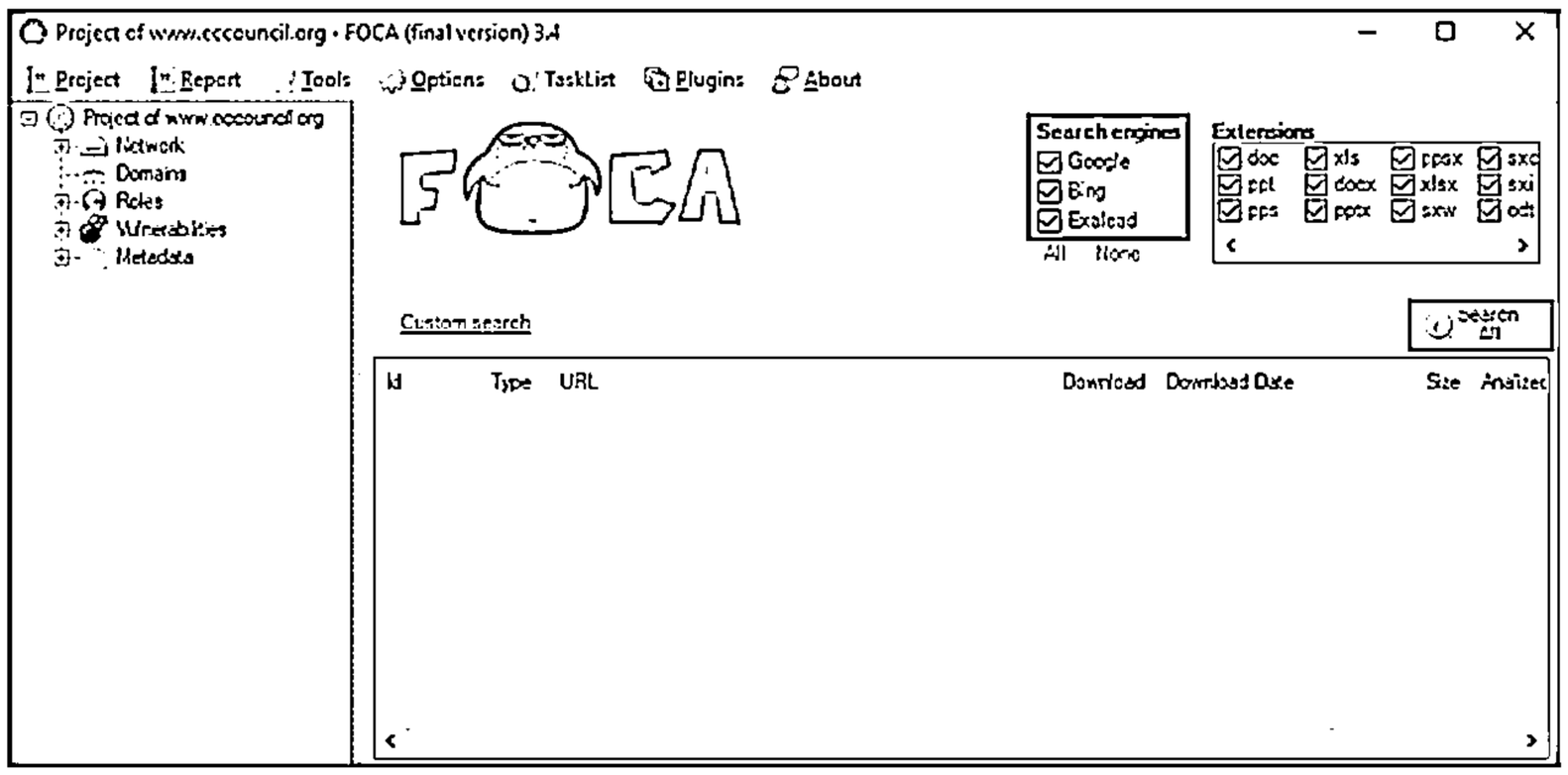


Figure 9.4.6: FOCA selecting Search engines

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

10. The **Search All** button automatically toggles the **Stop** button, and you can see the result in the lower panes.

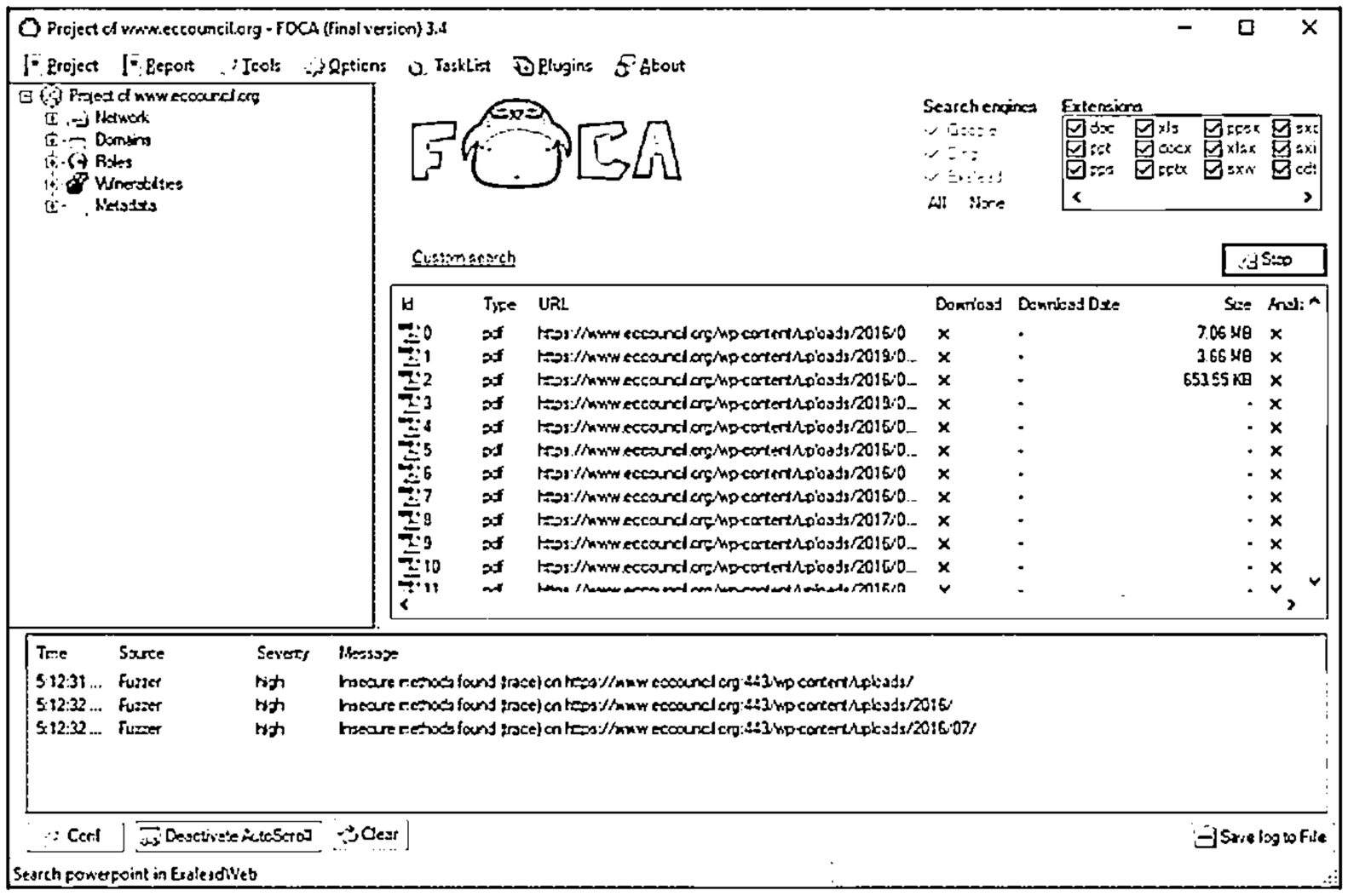


Figure 9.4.7: FOCA Extracted Information

11. After the scans complete, the **Stop** button automatically toggles back to the **Search All** button. The gathered result on the **Metadata** associated with the target domain appears, as shown in the screenshot.

Note: The gathered result includes various sub-domains associated with the target domains consisting of metafiles.

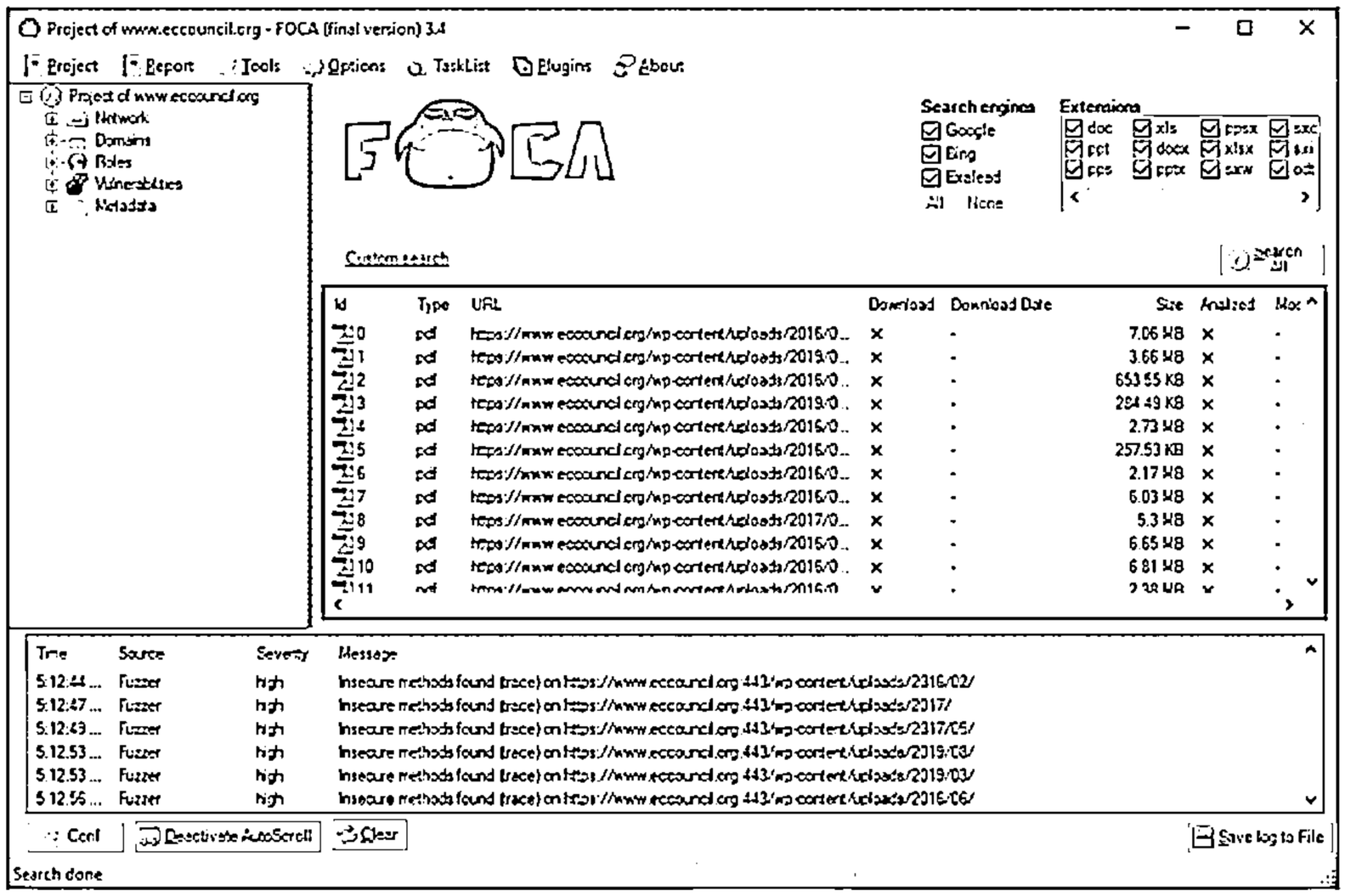


Figure 9.4.8: FOCA examining the extracted information of the file

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

12. To view the file information stored in the sub-domain, right-click on any URL and click **Link → Open in browser** from the context menu.

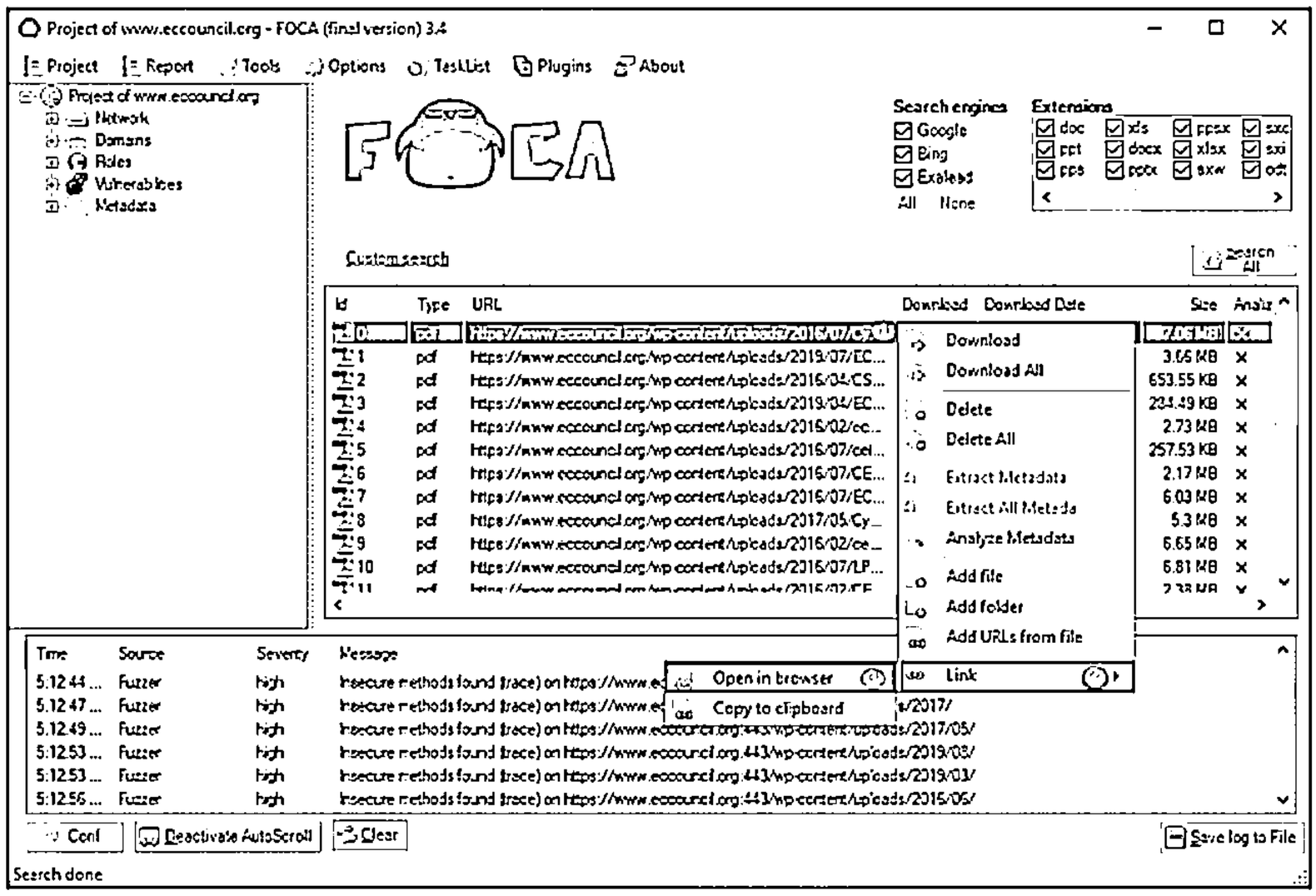


Figure 9.4.9: FOCA examining the extracted information of the file

13. If a **How do you want to open this?** pop up appears, select any web browser (here, **Mozilla Firefox**) and click **OK**.

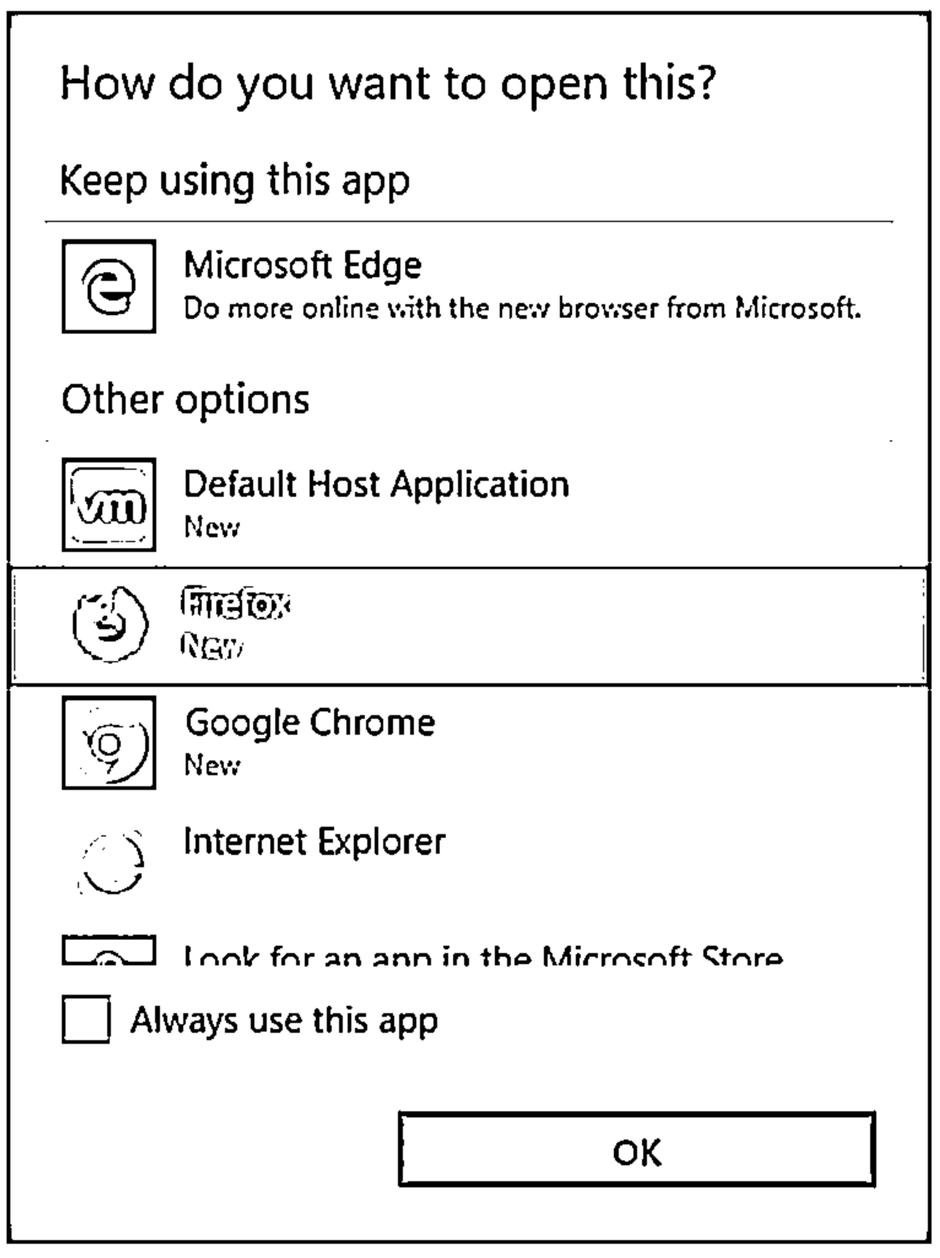


Figure 9.4.10: Selecting Mozilla Firefox

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

14. The extracted file from the domain by using **FOCA** appears on the web browser, as shown in the screenshot.

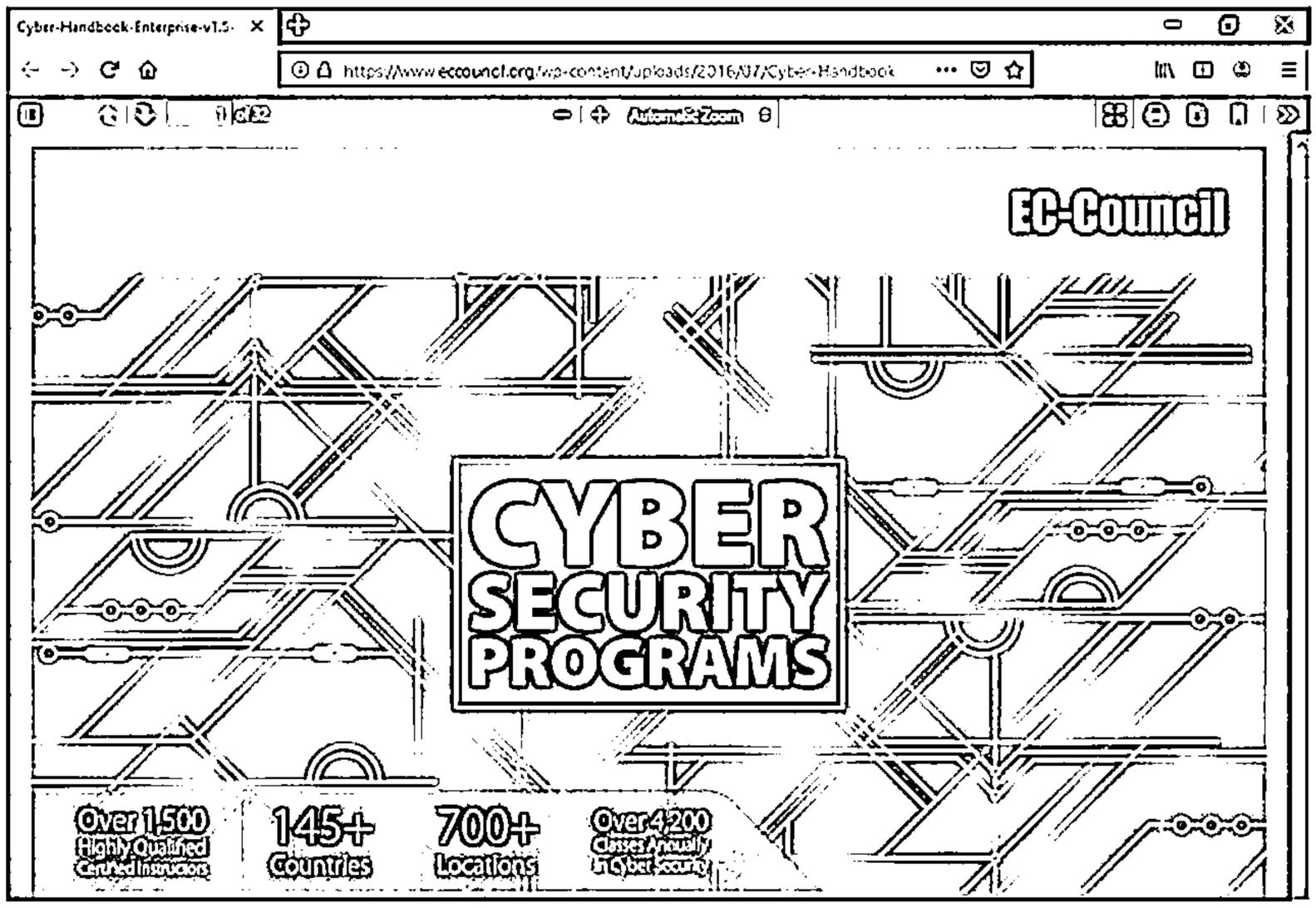


Figure 9.4.11: FOCA Extracted file

TASK 4.4

Extract Network Structure Information

15. Close the web browser.
16. Navigate back to the FOCA window and click the **Network** node to expand the node in the left pane of the window to view the network structure.

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

17. If the domain has any of the associated **Clients** or **Servers**, it displays the related information.

Note: In this lab, the domain we used does not have associated clients or servers.

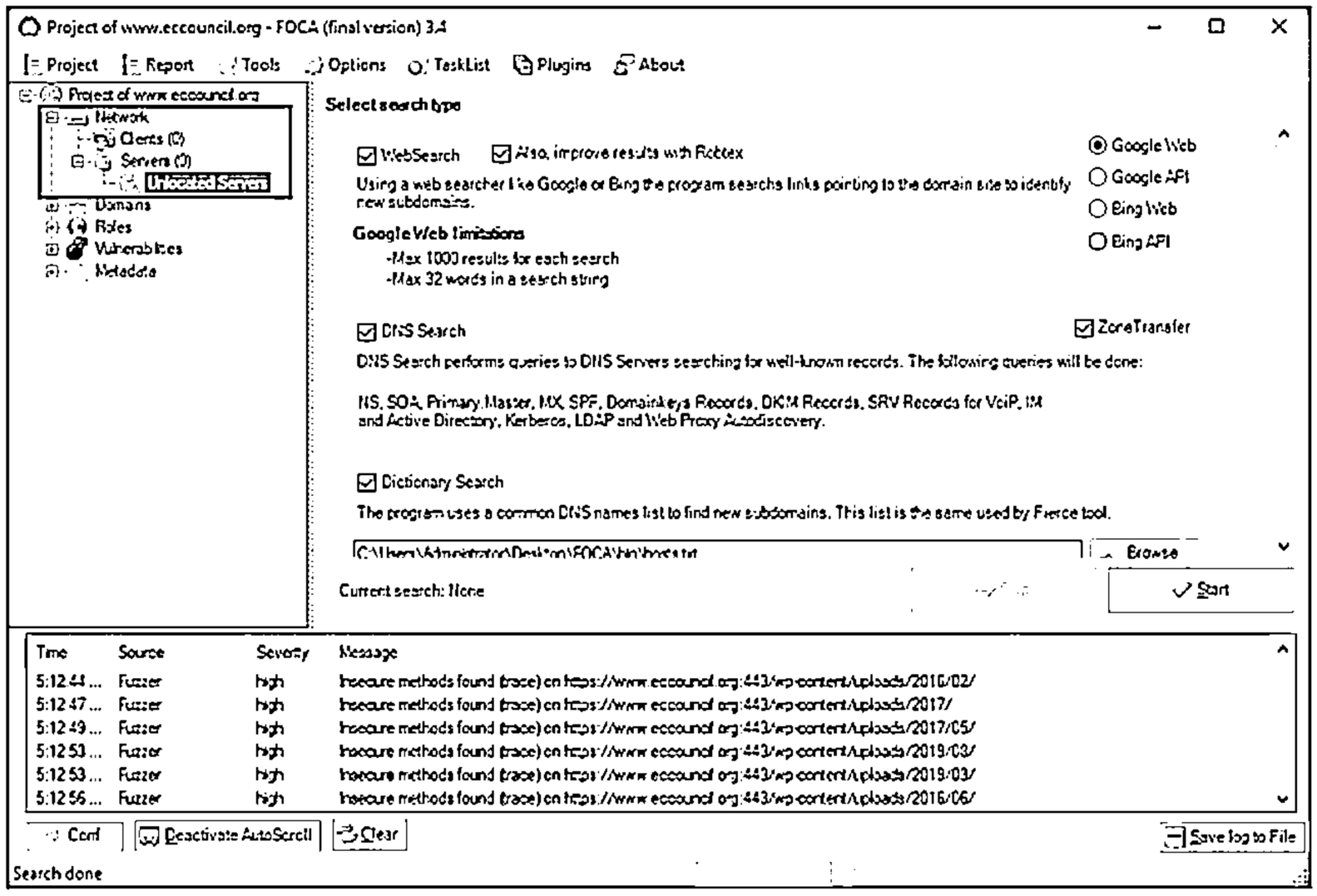


Figure 9.4.12: FOCA Network Information

TASK 4.5

Extract Domain Information

18. Expand the **Domains** node and click on the target domain (here, **eccouncil.org**) to view the domain-related information.

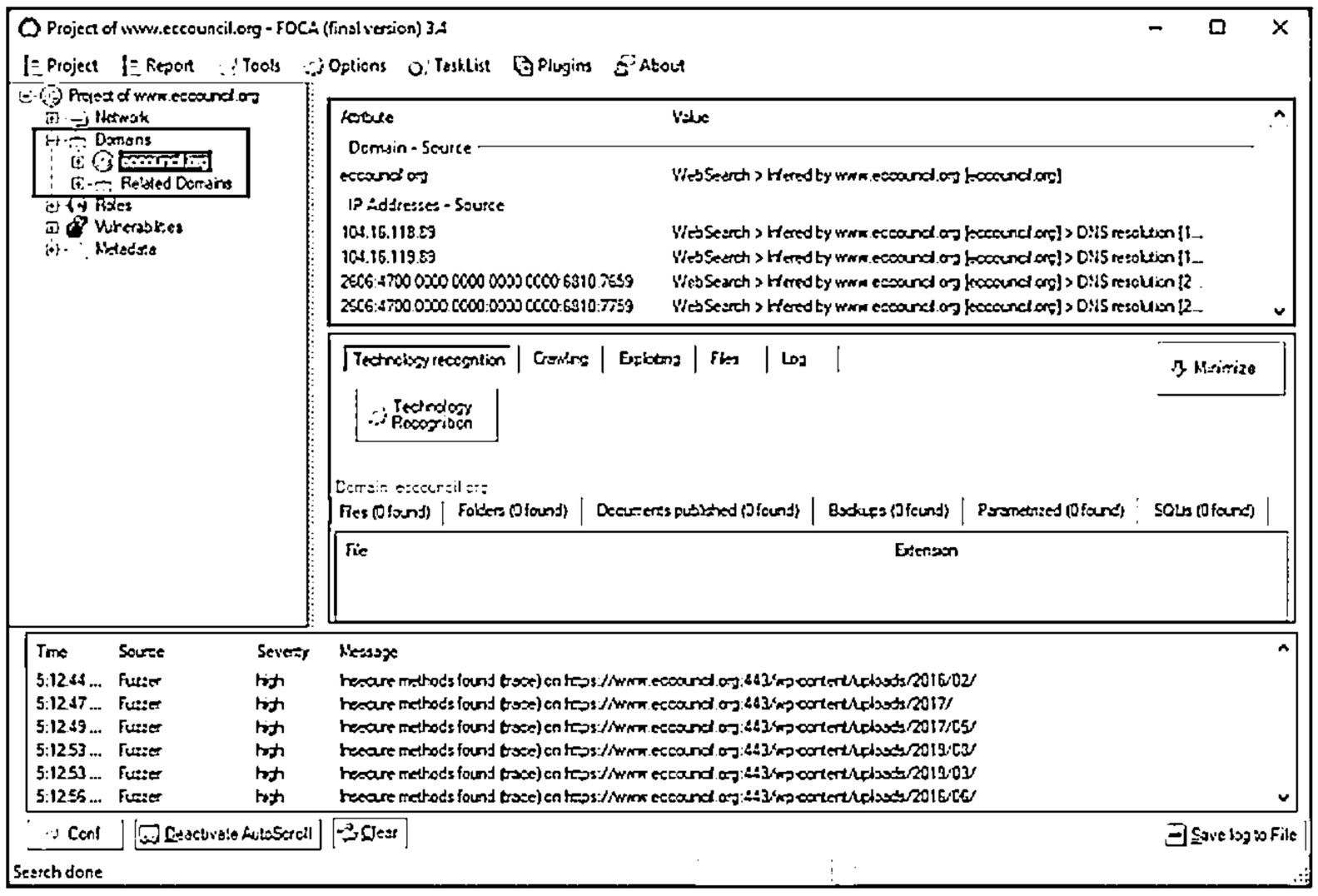


Figure 9.4.13: FOCA Domain Information

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

TASK 4.6

Extract Https Information

19. Expand the **Roles** node; further expand the **Https** node and click on the target domain (here, **www.eccouncil.org**) to see the detailed information such as **IP - Source**, **Roles in IP**, **Domains in IP - Source**, **FingerPrinting – HTTP**, and **HTML Title** in the righthand pane.

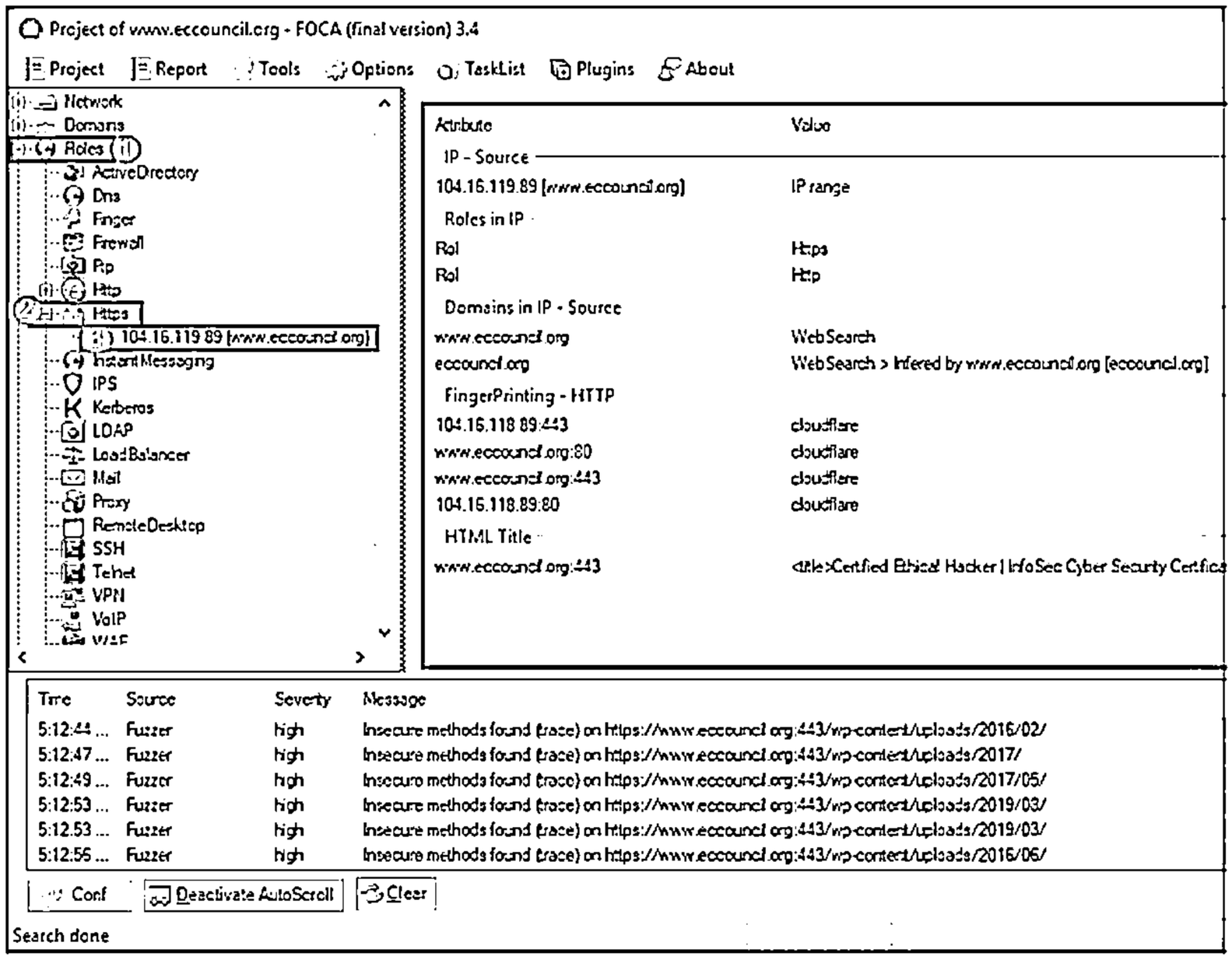


Figure 9.4.14: FOCA Https Information

20. This concludes the demonstration of gathering useful information about the target organization using the FOCA tool.
21. Close all open windows and document all the acquired information.
22. Turn off the **Windows 10** virtual machine.

TASK 5

Footprinting a Target using BillCipher

Here, we will use the BillCipher tool to footprint a target website URL.

BillCipher is an information gathering tool for a Website or IP address. Using this tool, you can gather information such as DNS Lookup, Whois lookup, GeoIP Lookup, Subnet Lookup, Port Scanner, Page Links, Zone Transfer, HTTP Header, etc.

1. Turn on **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

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

3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

6. Now, type **cd** and press **Enter** to jump to the root directory.

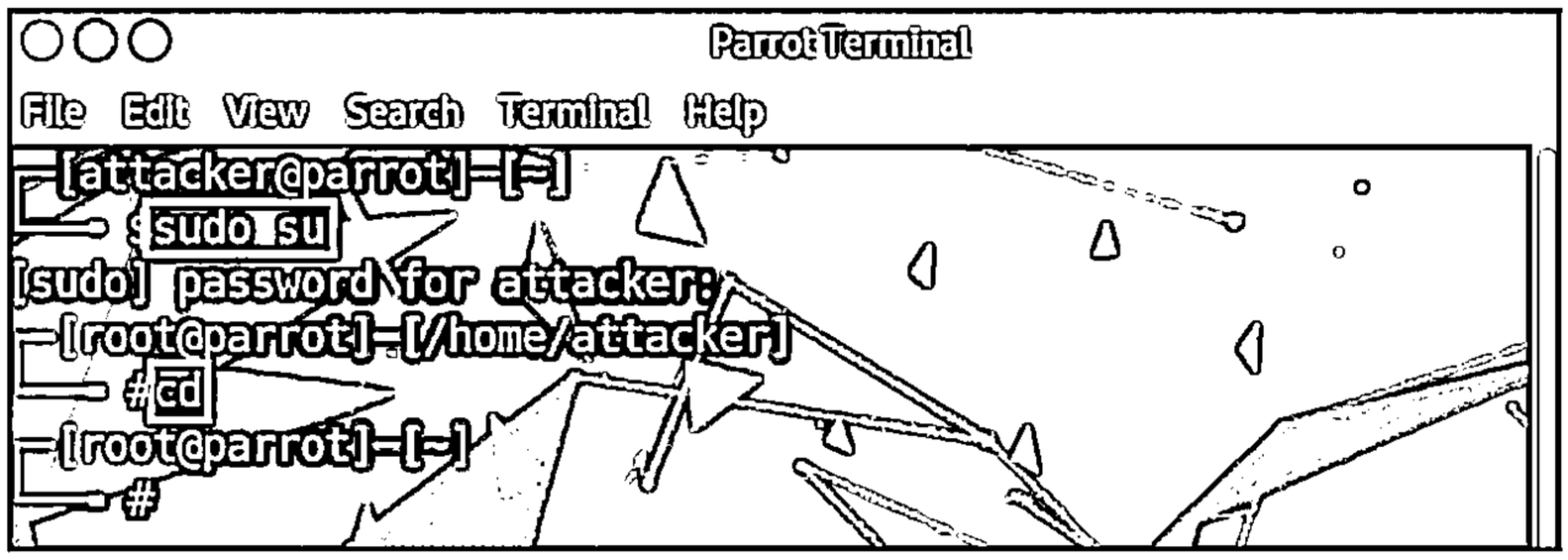


Figure 9.5.1: Running the programs as a root user

TASK 5.1

Clone and Launch BillCipher

7. In the **Parrot Terminal** window, type **git clone https://github.com/GitHackTools/BillCipher** and press **Enter** to clone the **BillCipher** directory.

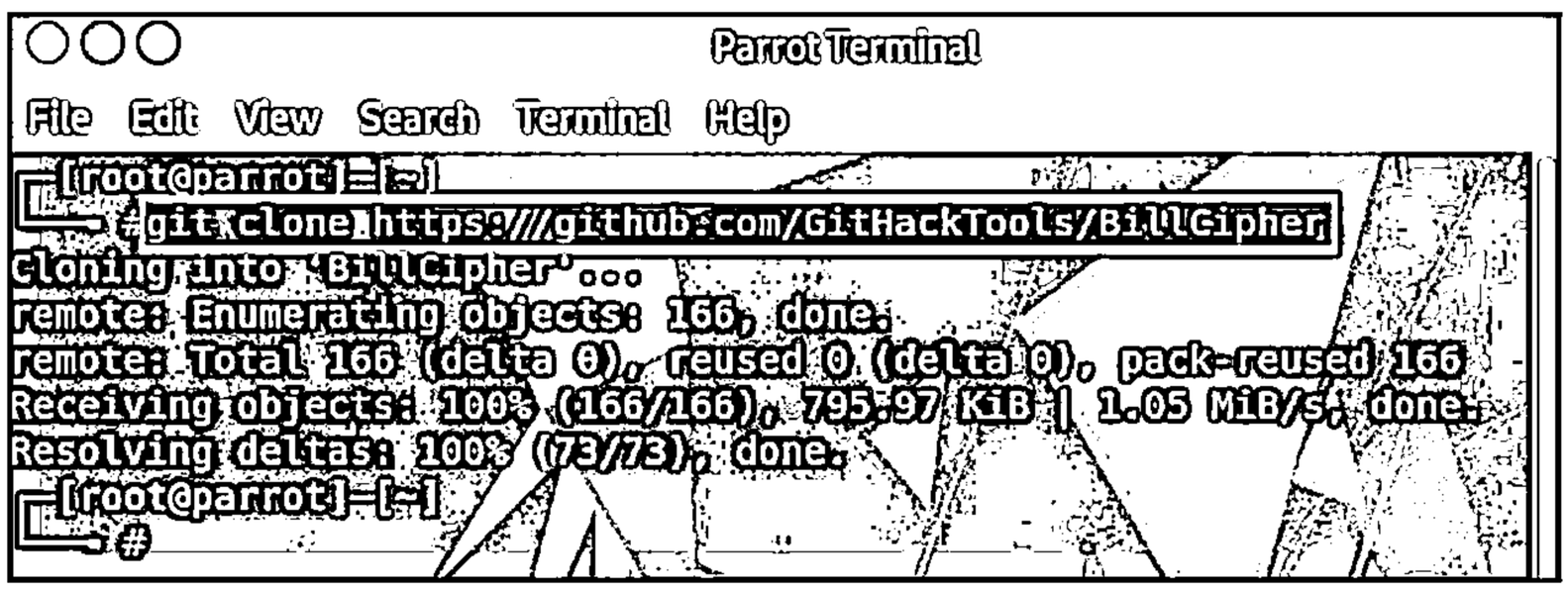


Figure 9.5.2: Cloning BillCipher

Note: You can also access the tool repository from the **CEH-Tools** folder available in **Windows 10** virtual machine, in case, the GitHub link does not exist, or you are unable to clone the tool repository. Follow the steps below in order to access **CEH-Tools** folder from the **Parrot Security** virtual machine:

- Open any explorer window and press **Ctrl+L**. The **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access **Windows 10** shared folders.
- The security pop-up appears; enter the **Windows 10** virtual machine credentials (**Username: Admin** and **Password: Pa$$w0rd**) and click **Connect**.

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

- The **Windows shares on 10.10.10.10** window appears; navigate to the location **CEH-Tools/CEHv11 Module 02 Footprinting and Reconnaissance/GitHub Tools/** and copy the **BillCipher** folder.
- Paste the copied **BillCipher** folder on the location **/home/attacker/**.
- In the terminal window, type **mv /home/attacker/BillCipher /root/**.

8. In the terminal window, type **cd BillCipher** and press **Enter** to navigate to the **BillCipher** directory.

Note: By default, BillCipher application gets cloned to the **/root** directory.

9. Now, type **python3 billcipher.py** and press **Enter** to launch the application.

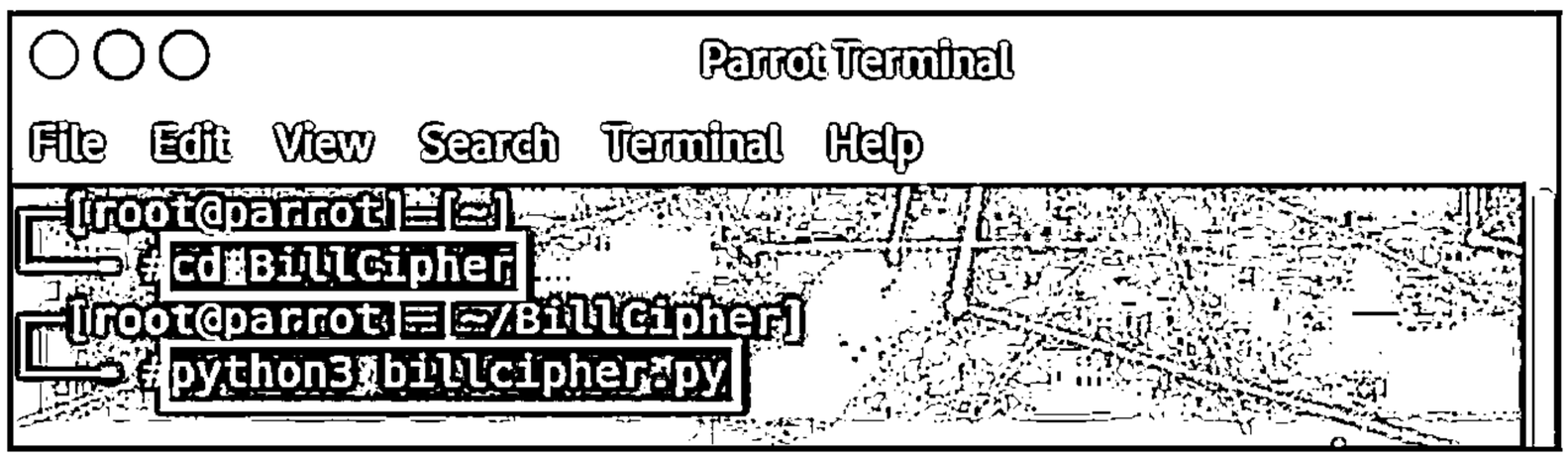


Figure 9.5.3: Launching BillCipher application

10. BillCipher application initializes. In the **Do you want to collect information of a website or IP address?** option, type **website** and press **Enter**.
11. In the **Enter the website address** option, type the target website URL (here, **www.certifiedhacker.com**) and press **Enter**.

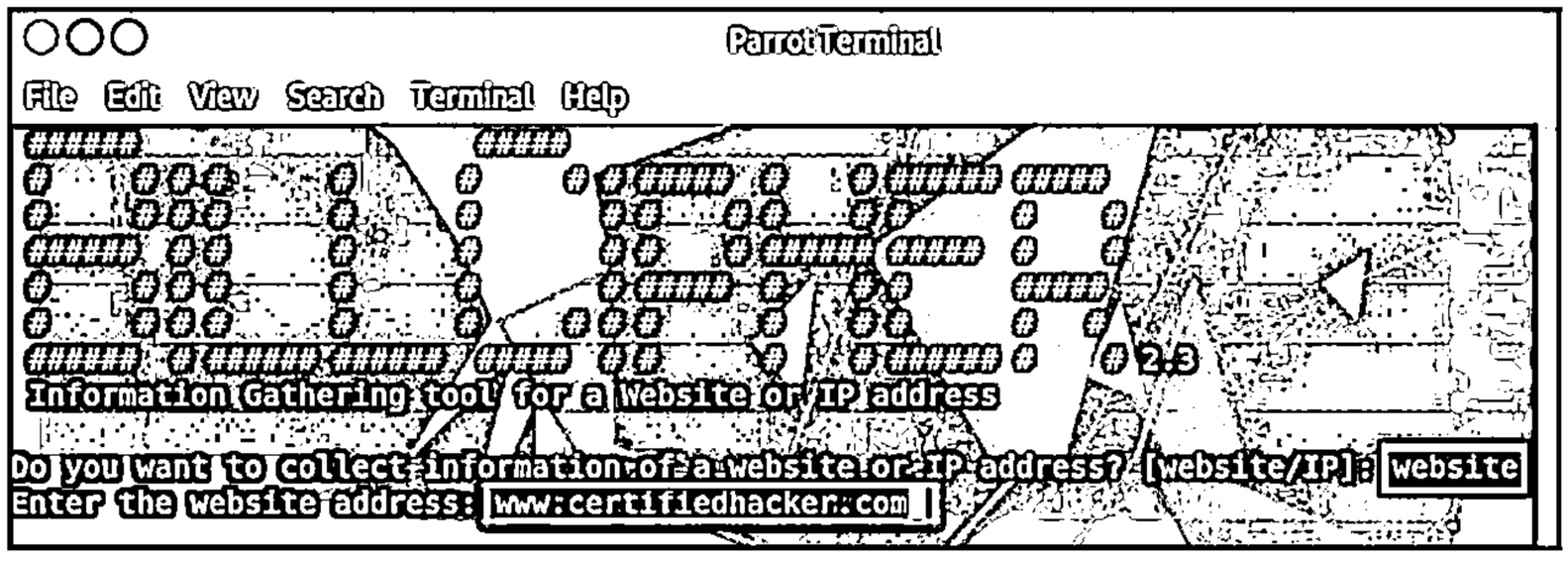


Figure 9.5.4: BillCipher initializes

TASK 5.2

Perform Information Gathering

12. BillCipher displays various available options that you can use to gather information regarding a target website.
13. In the **What information would you like to collect?** option, type **1** to choose the **DNS Lookup** option and press **Enter**.

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

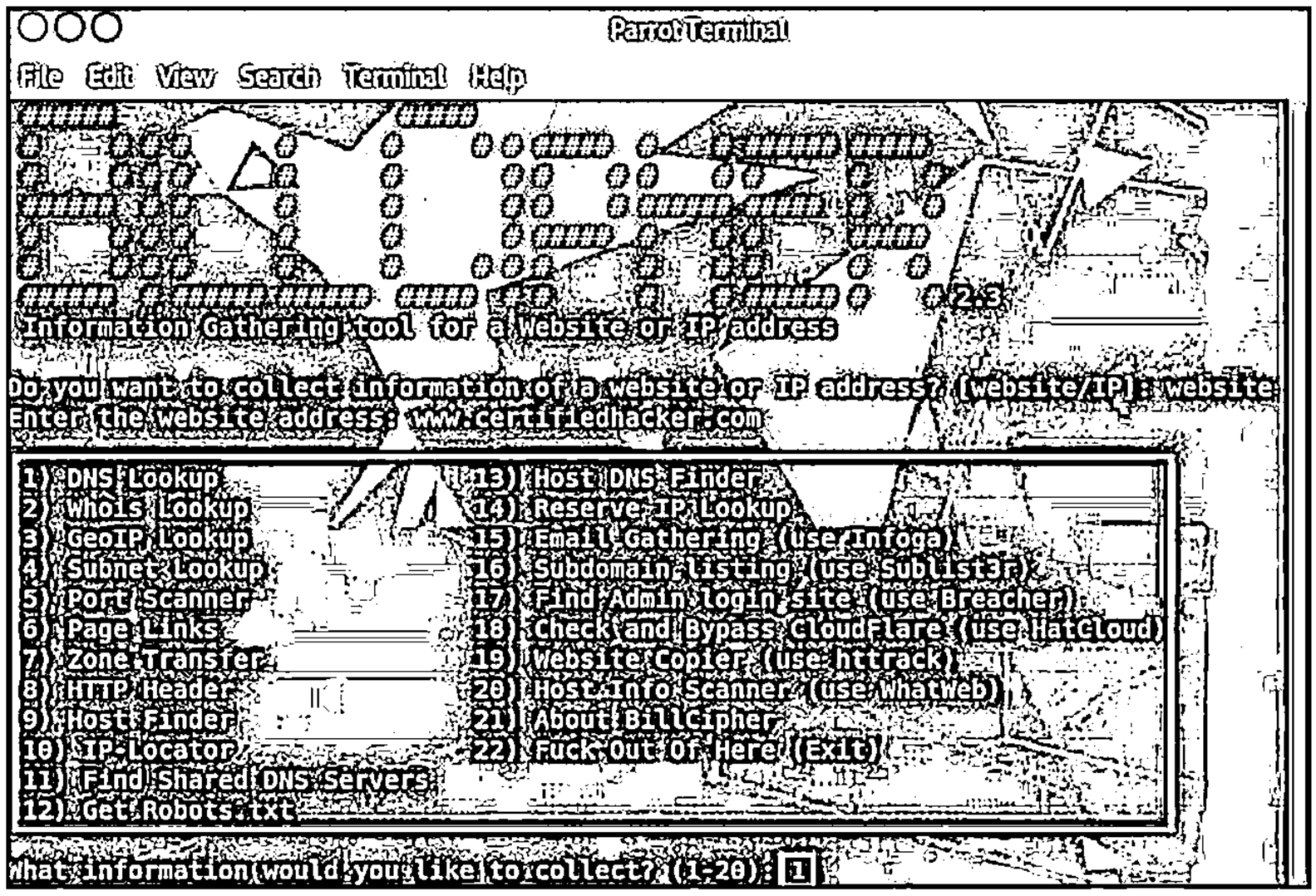


Figure 9.5.5: BillCipher options

14. The result appears, displaying the DNS information regarding the target website, as shown in the screenshot.

15. In the **Do you want to continue?** option, type **Yes** and press **Enter** to continue.

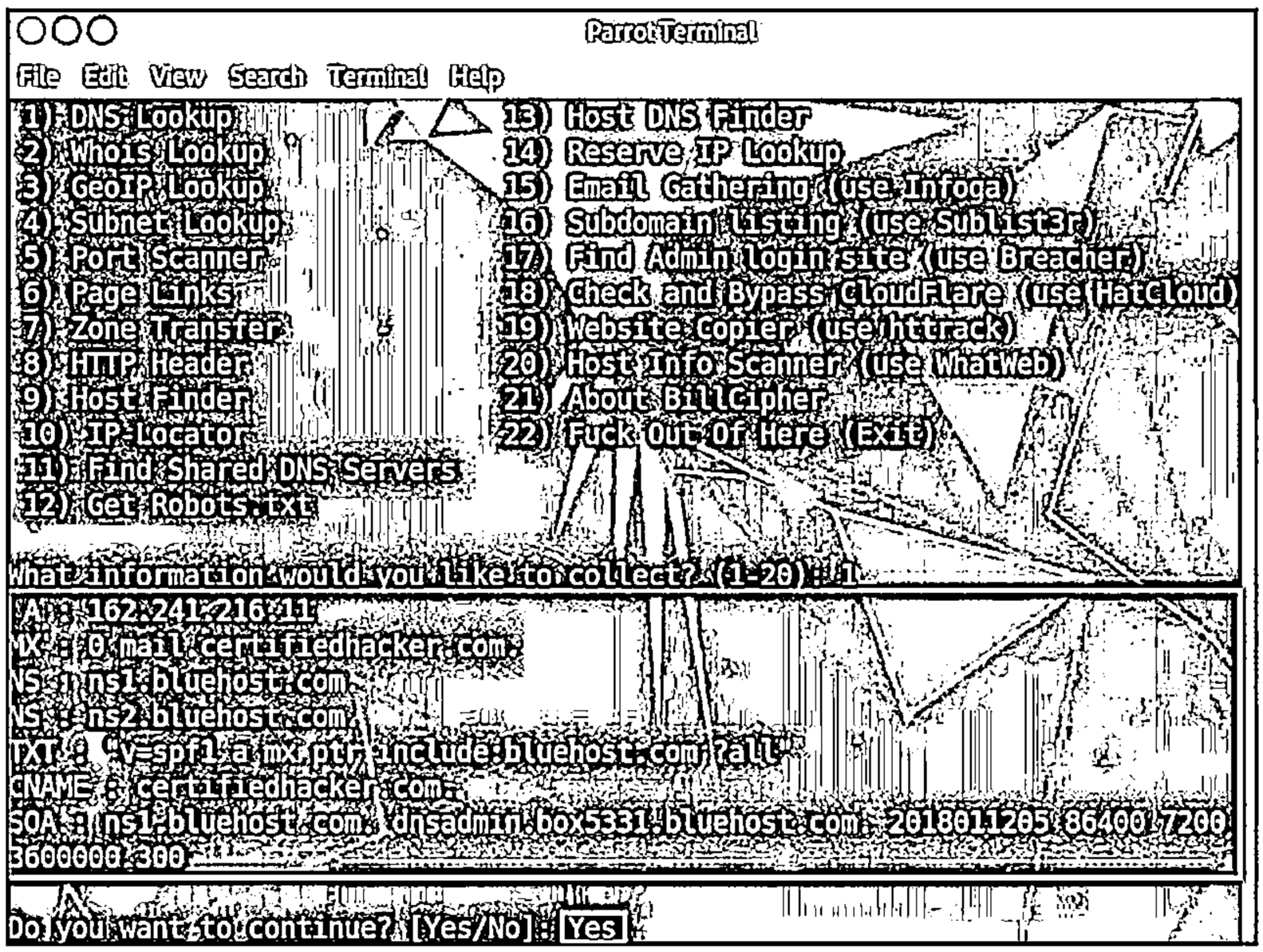


Figure 9.5.6: DNS Lookup result

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

16. **Do you want to collect information of a website or IP address?** option appears, type **website** and press **Enter**.
17. In the **Enter the website address** option, type the target website URL (here, **www.certifiedhacker.com**) and press **Enter**.
18. Now, type **3** and press **Enter** to choose the **GeoIP Lookup** option from the available information gathering options.

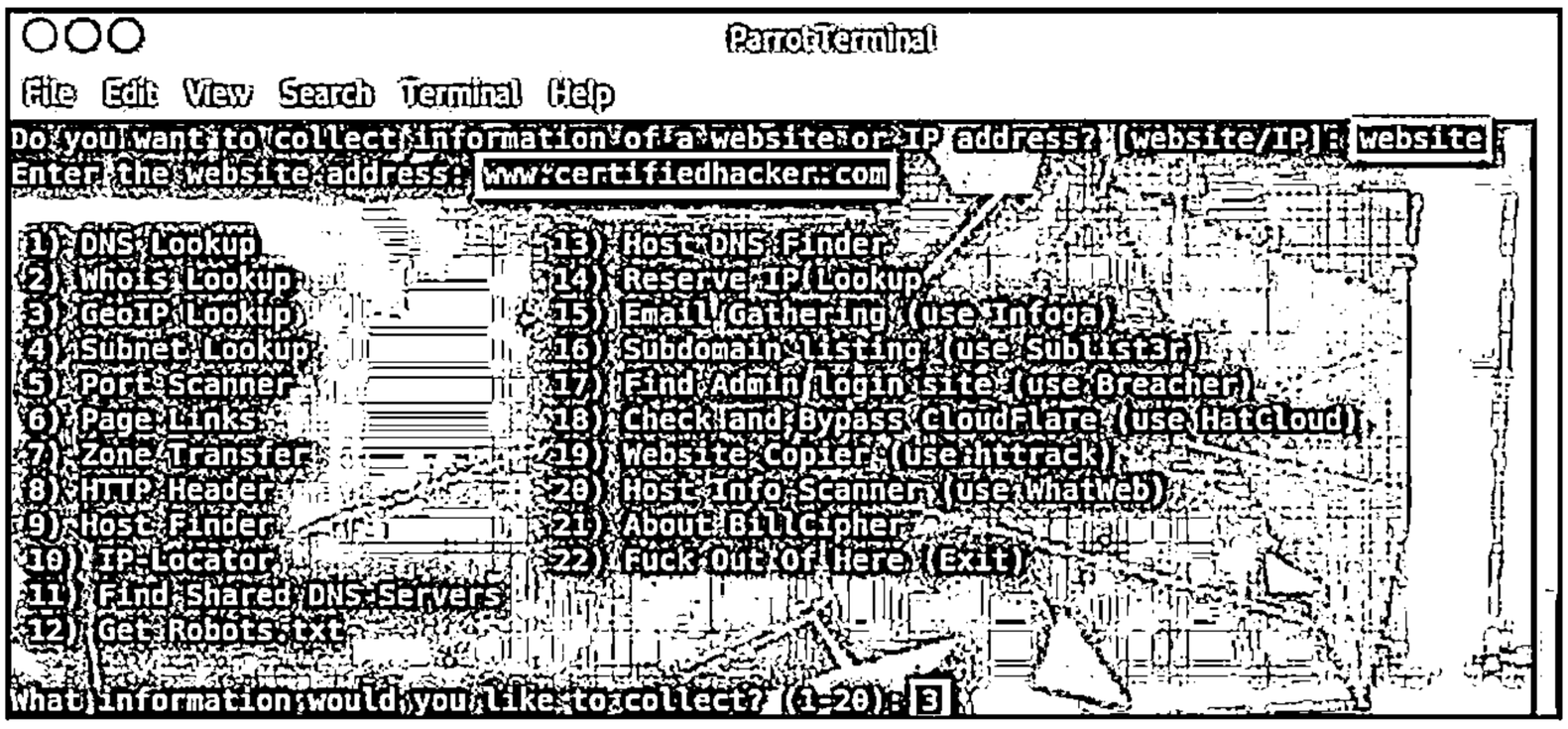


Figure 9.5.7: Choose option 3

19. The result appears, displaying the **GeoIP Lookup** information of the target website, as shown in the screenshot.
20. In the **Do you want to continue?** option, type **Yes** and press **Enter** to continue.

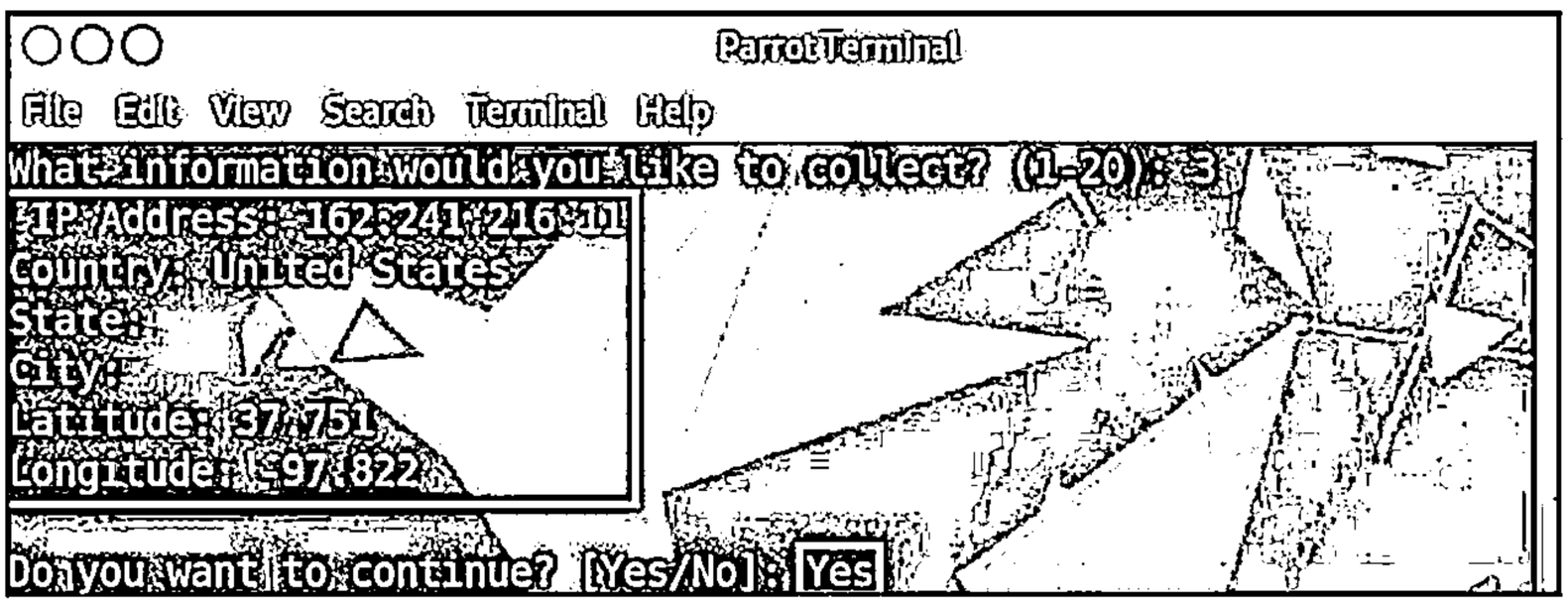


Figure 9.5.8: GeoIP Lookup result

21. The **Do you want to collect information of a website or IP address?** option appears; type **website** and press **Enter**.
22. In the **Enter the website address** option, type the target website URL (here, **www.certifiedhacker.com**) and press **Enter**.
23. Now, type **4** and press **Enter** to choose the **Subnet Lookup** option from the available information gathering options.

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

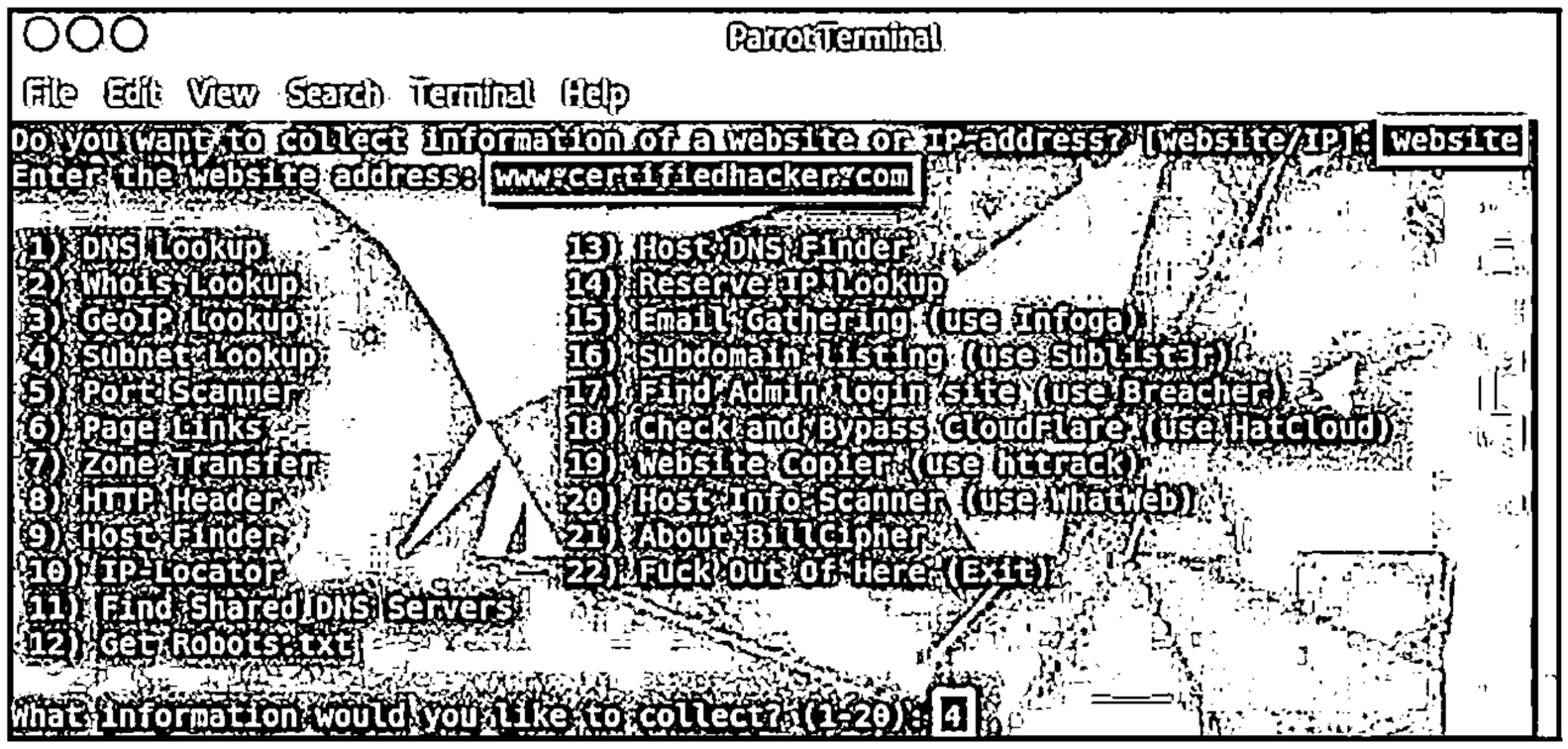


Figure 9.5.9: Choose option 4

24. The result appears, displaying the **Subnet Lookup** information of the target website.
25. In the **Do you want to continue?** option, type **Yes** and press **Enter** to continue.

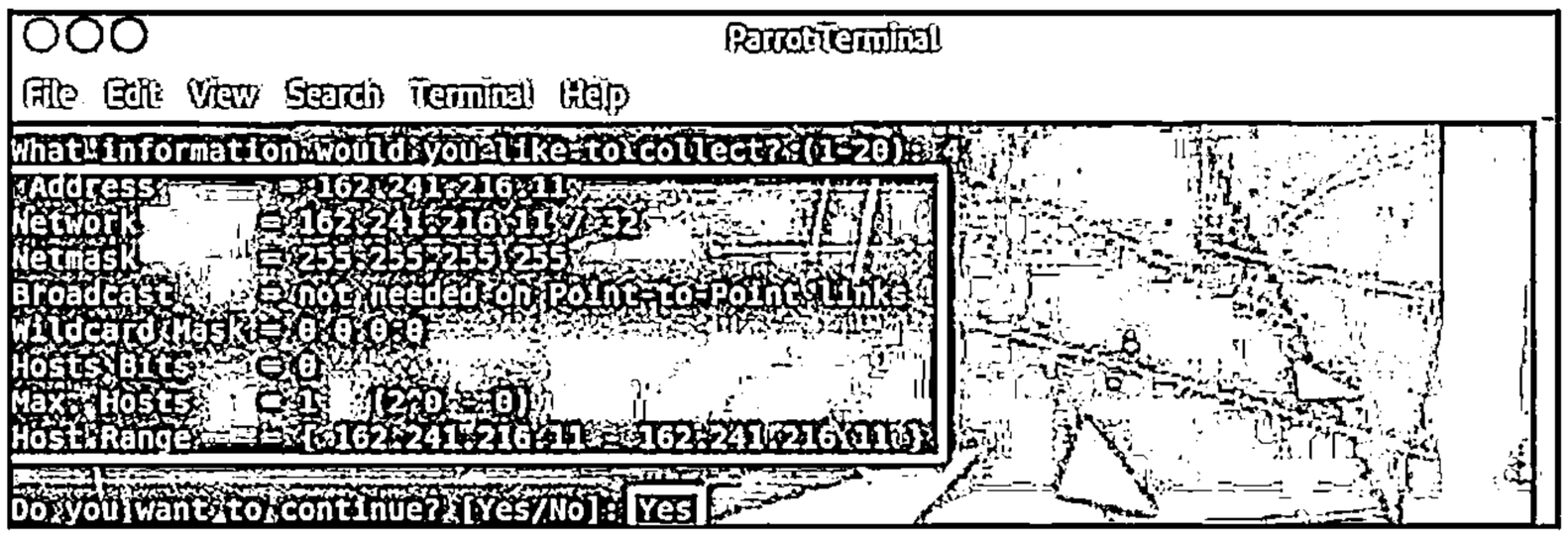


Figure 9.5.10: Choose option 4

26. The **Do you want to collect information of a website or IP address?** option appears; type **website** and press **Enter**.
27. In the **Enter the website address** option, type the target website URL (here, **www.certifiedhacker.com**) and press **Enter**.
28. Now, type **6** and press **Enter** to choose the **Page Links** option from the available information gathering options.
29. The result appears, displaying a list of **Visible links** and **Hidden links** of the target website, as shown in the screenshot.
30. In the **Do you want to continue?** option, type **Yes** and press **Enter** to continue.

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

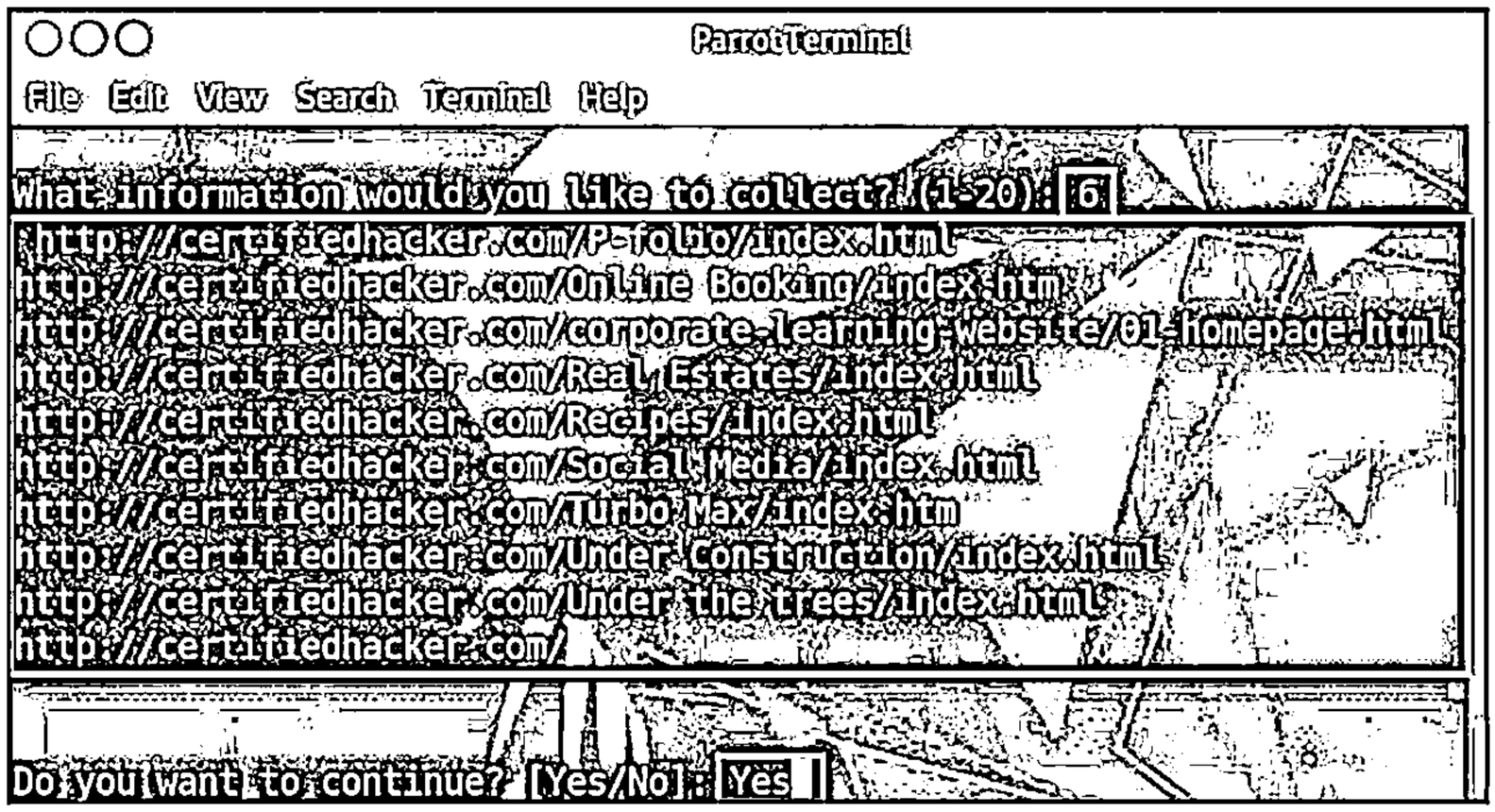


Figure 9.5.11: Page Links option results

31. The **Do you want to collect information of a website or IP address?** option appears; type **website** and press **Enter**.
32. In the **Enter the website address** option, type the target website URL (here, **www.certifiedhacker.com**) and press **Enter**.
33. Now, type **8** and press **Enter** to choose the **HTTP Header** option from the available information gathering options.
34. The result appears, displaying information regarding the HTTP header of the target website, as shown in the screenshot.
35. In the **Do you want to continue?** option, type **Yes** and press **Enter** to continue.

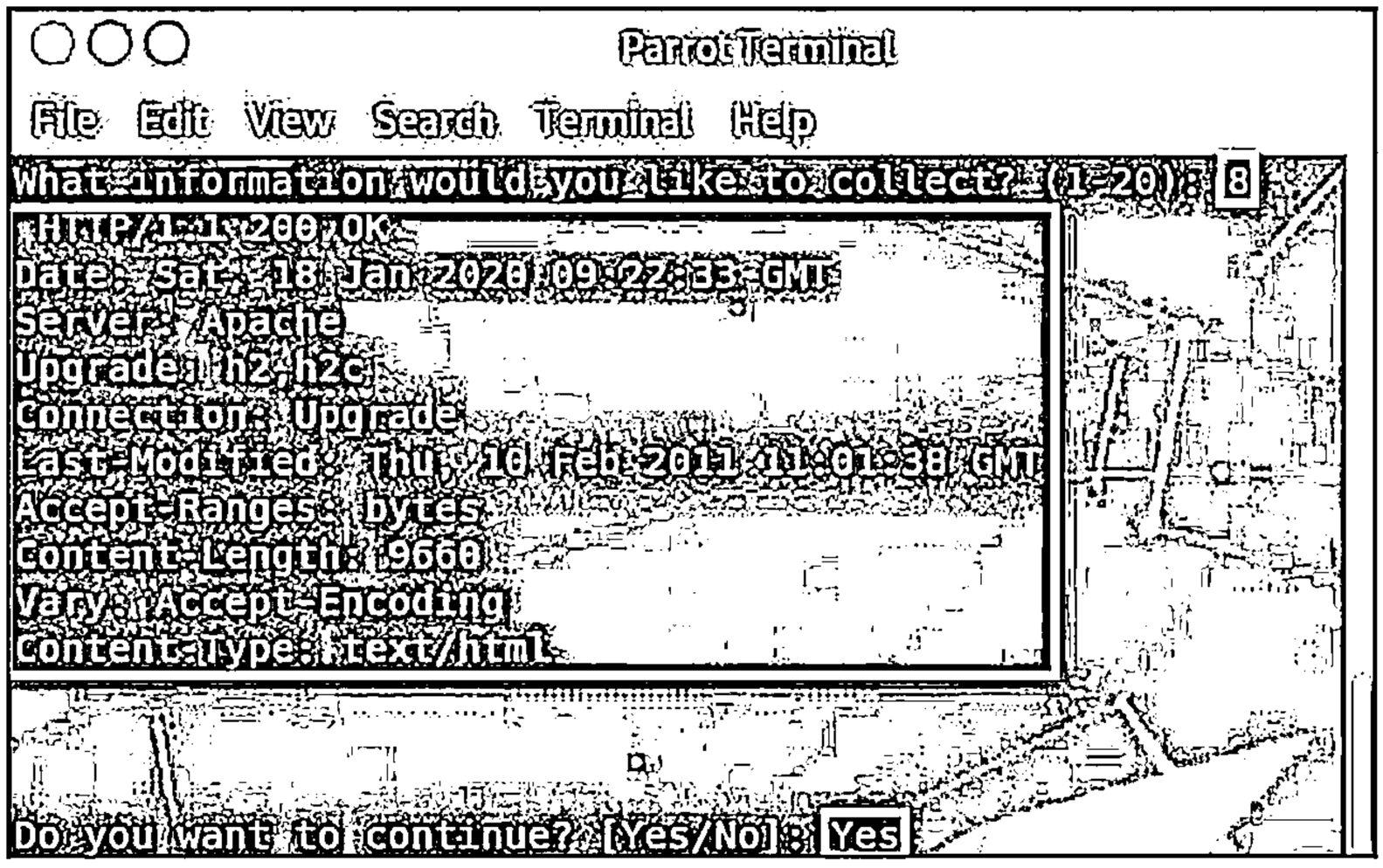


Figure 9.5.12: HTTP Header option results

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

36. The **Do you want to collect information of a website or IP address?** option appears; type **website** and press **Enter**.
37. In the **Enter the website address** option, type the target website URL (here, **www.certifiedhacker.com**) and press **Enter**.
38. Now, type **9** and press **Enter** to choose **Host Finder** option from the available information gathering options.
39. The result appears, displaying information regarding the IP address of the target website, as shown in the screenshot.
40. In the **Do you want to continue?** option, type **Yes** and press **Enter** to continue.

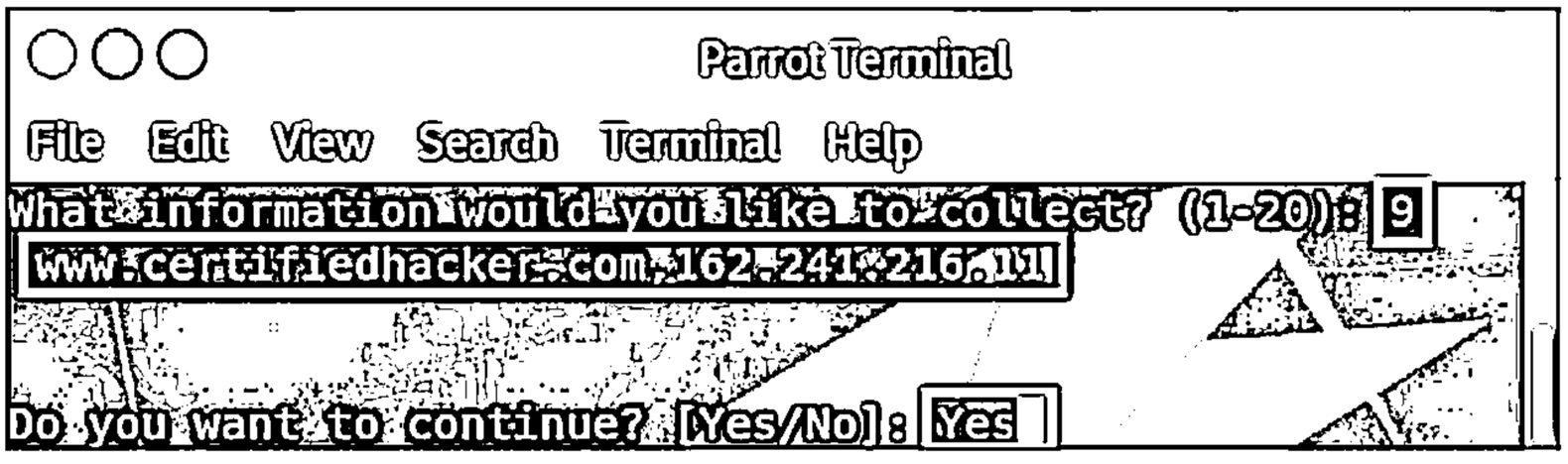


Figure 9.5.13: Host Finder option results

41. The **Do you want to collect information of a website or IP address?** option appears; type **website** and press **Enter**.
42. In the **Enter the website address** option, type the target website URL (here, **www.certifiedhacker.com**) and press **Enter**.
43. Now, type **13** and press **Enter** to choose **Host DNS Finder** option from the available information gathering options.
44. The result appears, displaying information regarding host DNS of the target website, as shown in the screenshot.
45. In the **Do you want to continue?** option, type **Yes** and press **Enter** to continue.

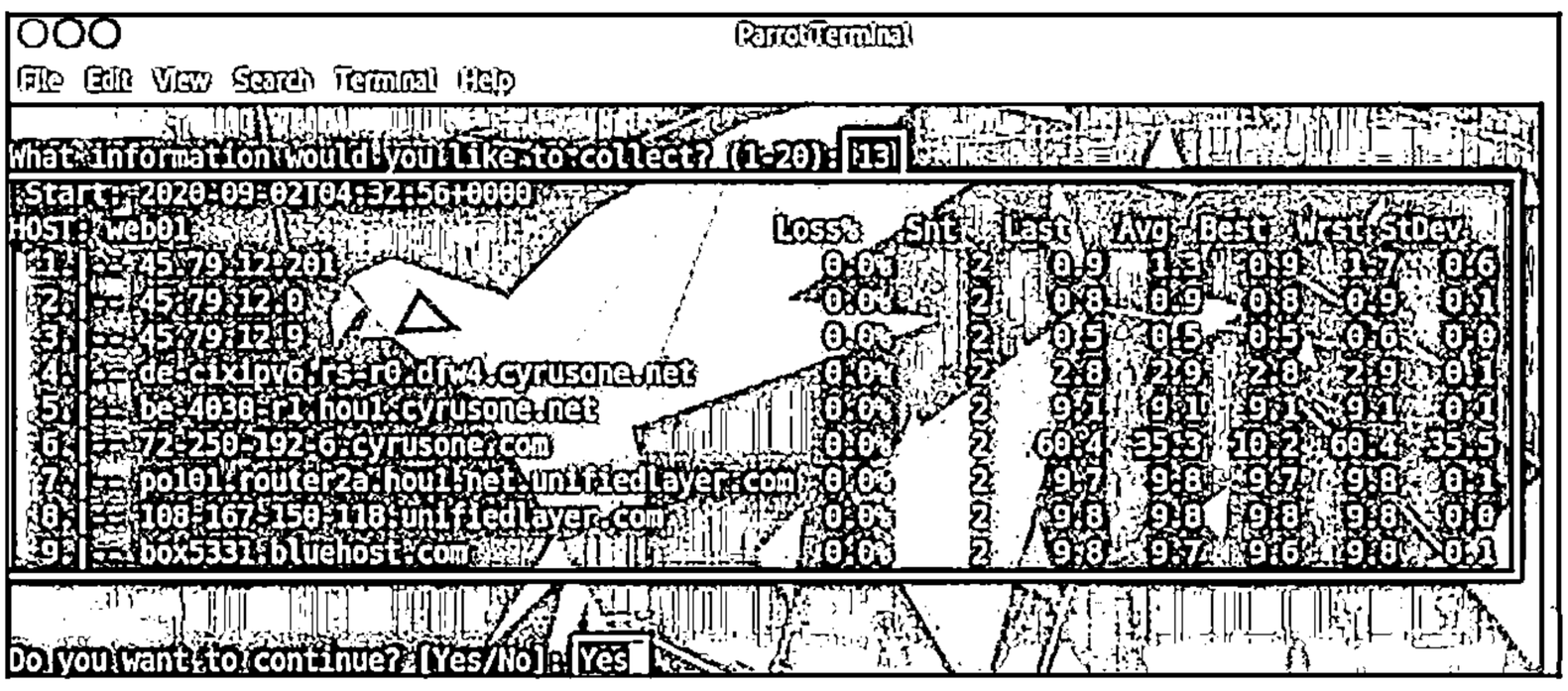


Figure 9.5.14: Host DNS Finder option results

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

46. The **Do you want to collect information of a website or IP address?** option appears; type **website** and press **Enter**.
47. In the **Enter the website address** option, type the target website URL (here, **www.certifiedhacker.com**) and press **Enter**.
48. Now, type **19** and press **Enter** to choose the **Website Copier (use httrack)** option from the available information gathering options.
49. The tool starts mirroring the target website; this will take approximately 5 minutes.
50. After completion of the mirroring process, the mirrored website gets saved in the folder **websource**, as shown in the screenshot.

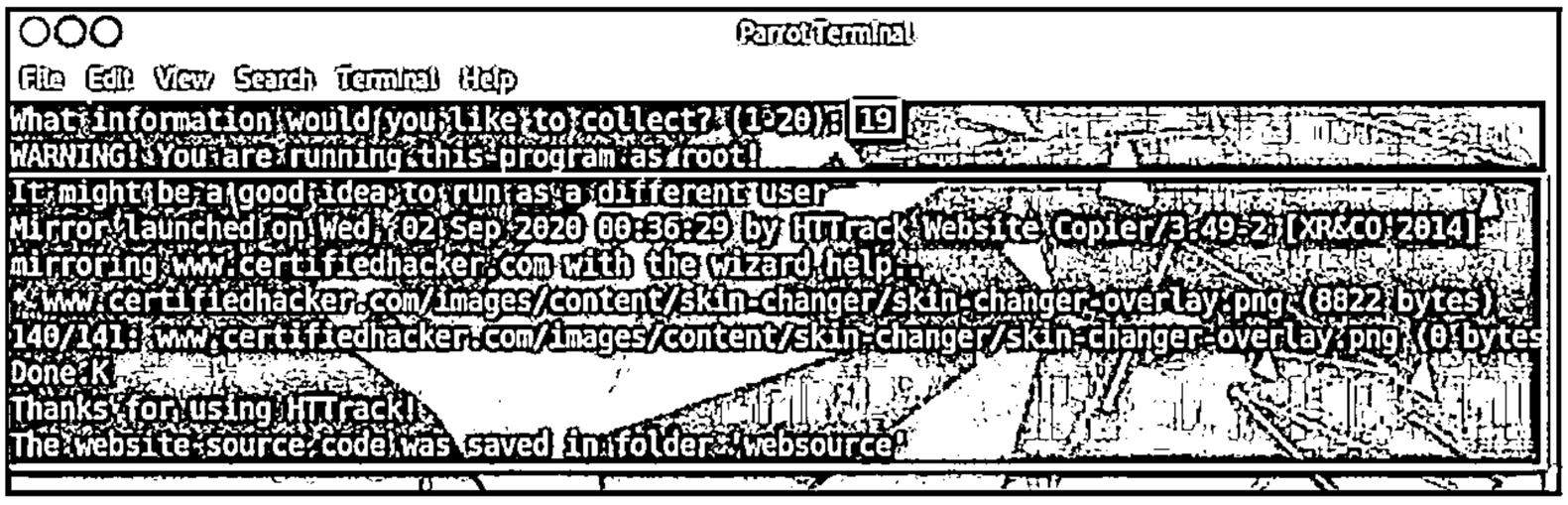


Figure 9.5.15: Copying website

51. Press **Ctrl+C** to exit BillCipher and close the terminal window.
52. Click **Places** from the top-section of the **Desktop** and click **Home Folder** from the drop-down options.

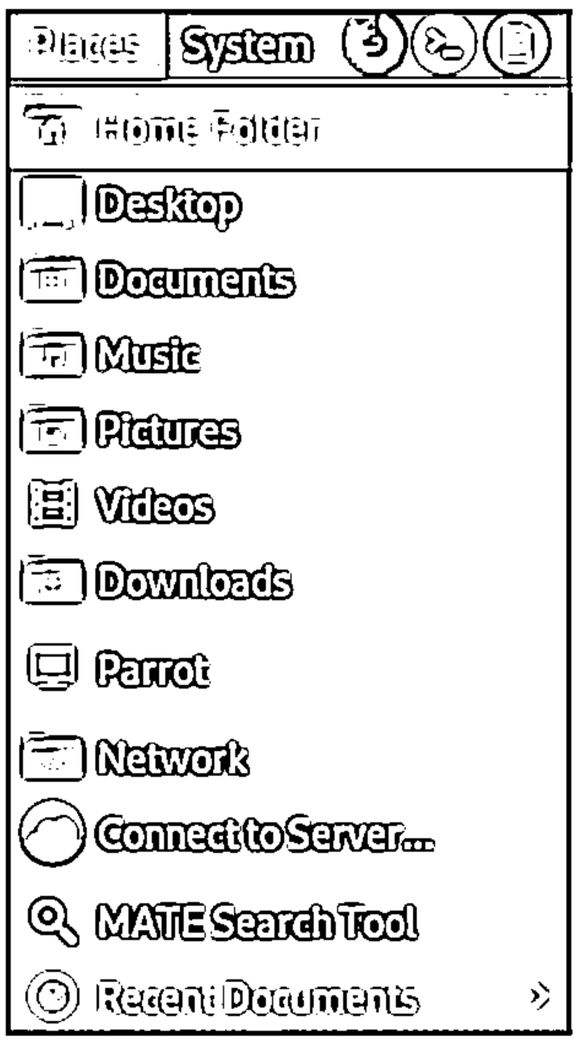


Figure 9.5.16: Navigate to the Home Folder

53. The **attacker** window appears, click **File System** from the left-pane and navigate to the location **root**.

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

54. The **root** directory window appears; navigate to **BillCipher → websource → www.certifiedhacker.com → www.certifiedhacker.com**. Right-click the **index.html** file and navigate to **Open With → Firefox** to open the mirrored website.

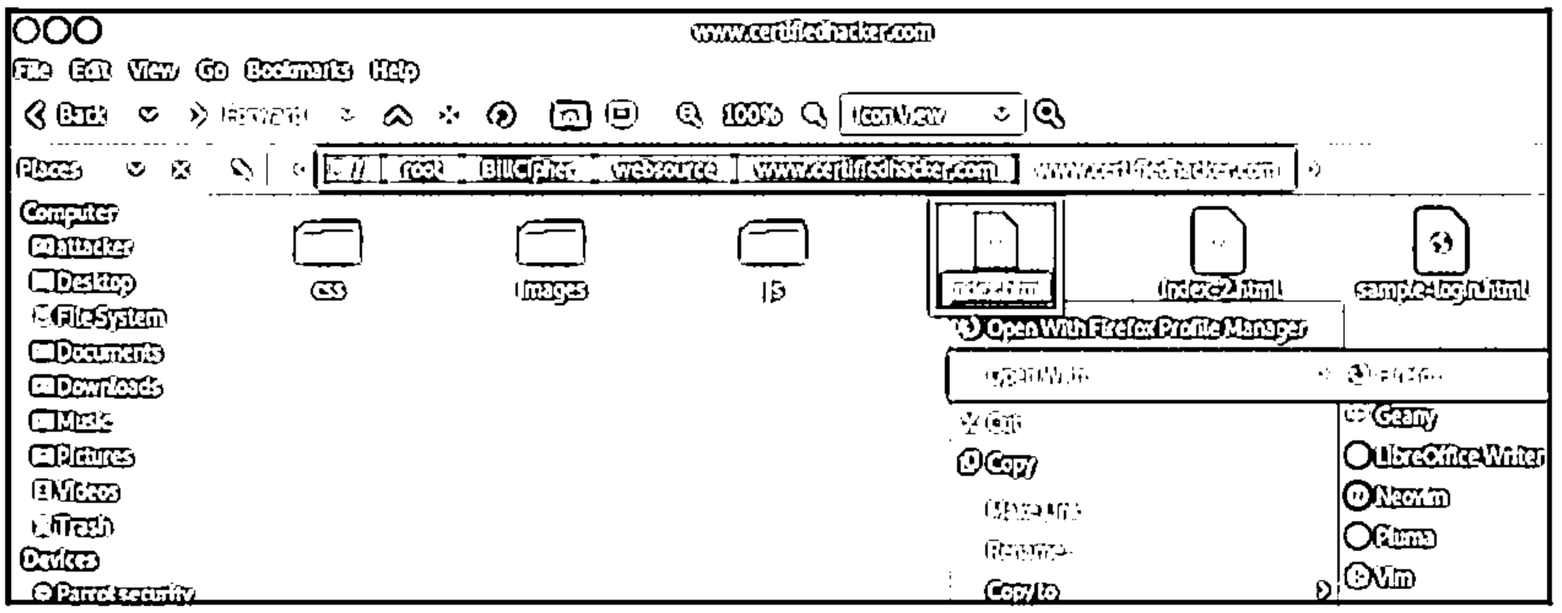


Figure 9.5.17: Opening index.html file

55. The mirror target website (**www.certifiedhacker.com**) appears in the **Mozilla Firefox** browser, as shown in the screenshot.

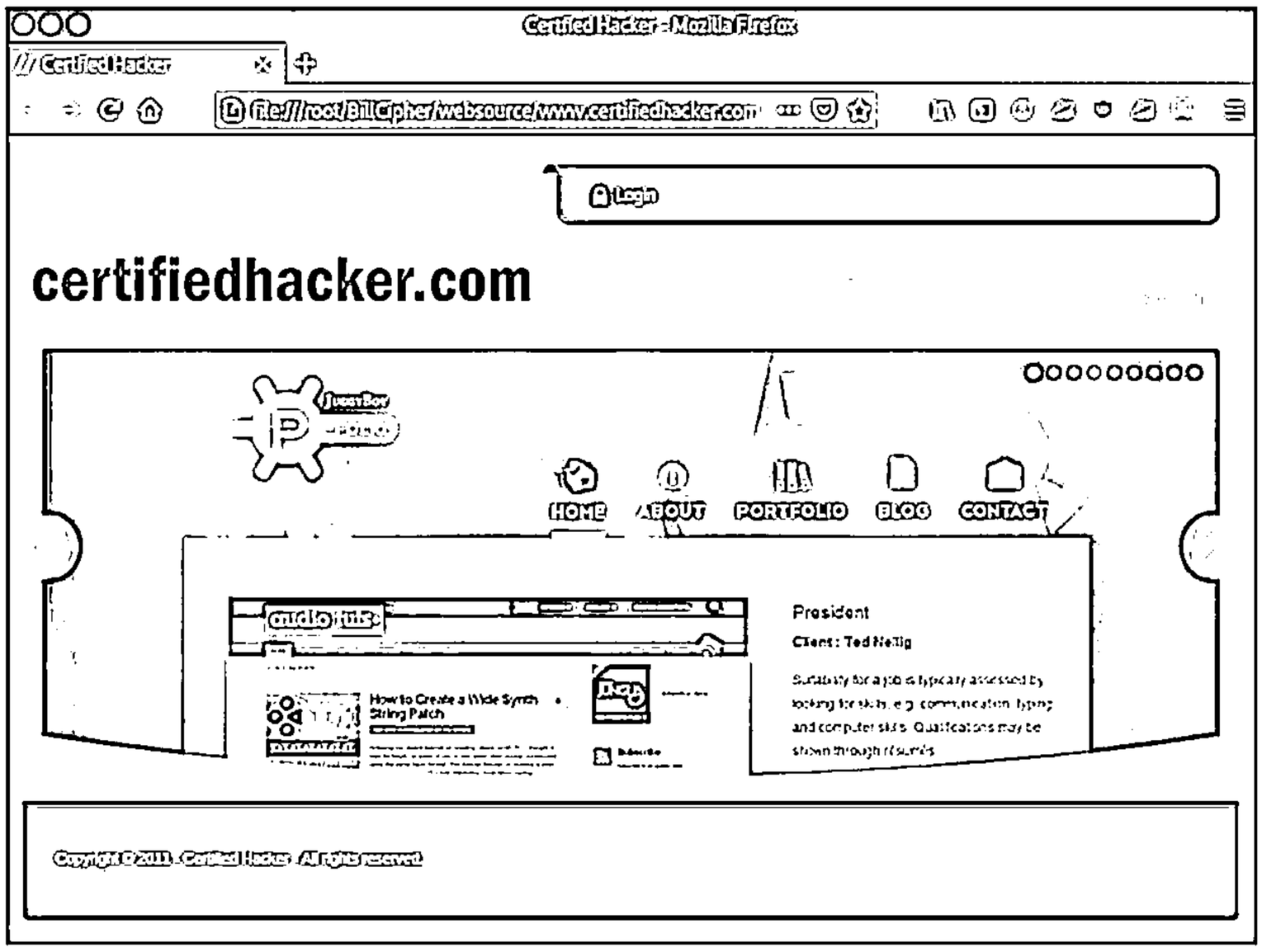


Figure 9.5.18: Mirrored target website

56. Similarly, you can use other information gathering options to gather information about the target.
57. This concludes the demonstration of footprinting the target website URL using BillCipher.
58. Close all open windows and document all the acquired information.
59. Turn off the **Parrot Security** virtual machine.

You can also use footprinting tools such as **Recon-Dog** (https://www.github.com), **Th3Inspector** (https://github.com), **Raccoon** (https://github.com), **Orb** (https://github.com), etc. to gather additional information related to the target company.

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

TASK 6 Footprinting a Target using OSINT Framework

Here, we will use the OSINT Framework to explore footprinting categories and associated tools.

1. Turn on the **Windows 10** virtual machine and login with credentials **Admin/Pa$$w0rd**.
2. Open any web browser (here, **Mozilla Firefox**); type **https://osintframework.com/** in the address bar and press **Enter**.

TASK 6.1

Navigate to OSINT Framework

3. **OSINT Framework** website appears; you can observe the OSINT tree on the left side of screen, as shown in the screenshot.

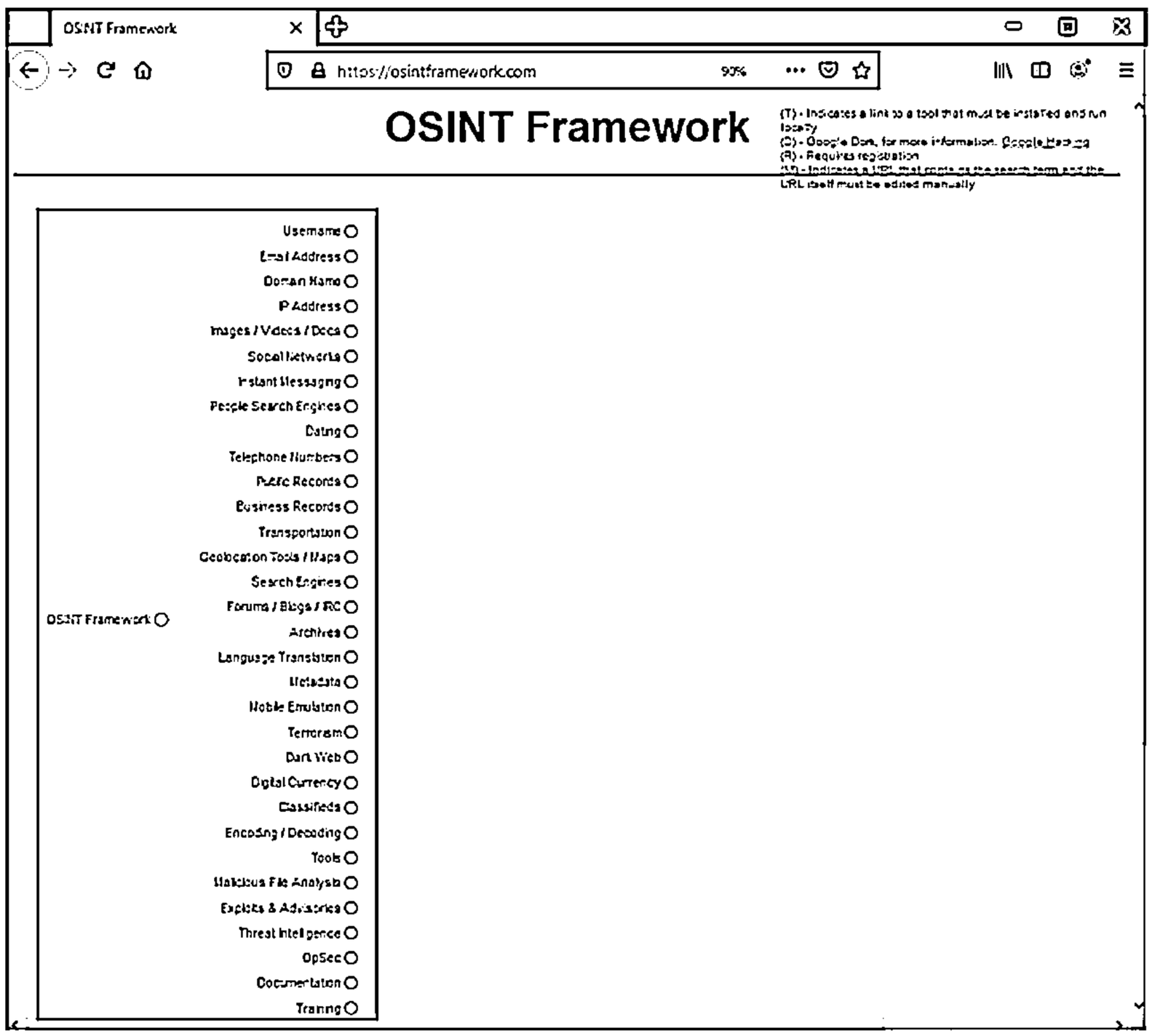


Figure 9.6.1: OSINT tree

OSINT Framework is an open source intelligence gathering framework that helps security professionals for performing automated footprinting and reconnaissance, OSINT research, and intelligence gathering. It is focused on gathering information from free tools or resources. This framework includes a simple web interface that lists various OSINT tools arranged by category and is shown as an OSINT tree structure on the web interface.

TASK 6.2

View Username Category

4. Clicking on any of the categories such as **Username**, **Email Address**, or **Domain Name** will make many useful resources appear on the screen in the form of a sub-tree.
5. Click the **Username** category and click to expand the **Username Search Engines** and **Specific Sites** sub-categories.
6. You can observe a list of OSINT tools filtered by sub-categories (**Username Search Engines** and **Specific Sites** sub-categories).

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

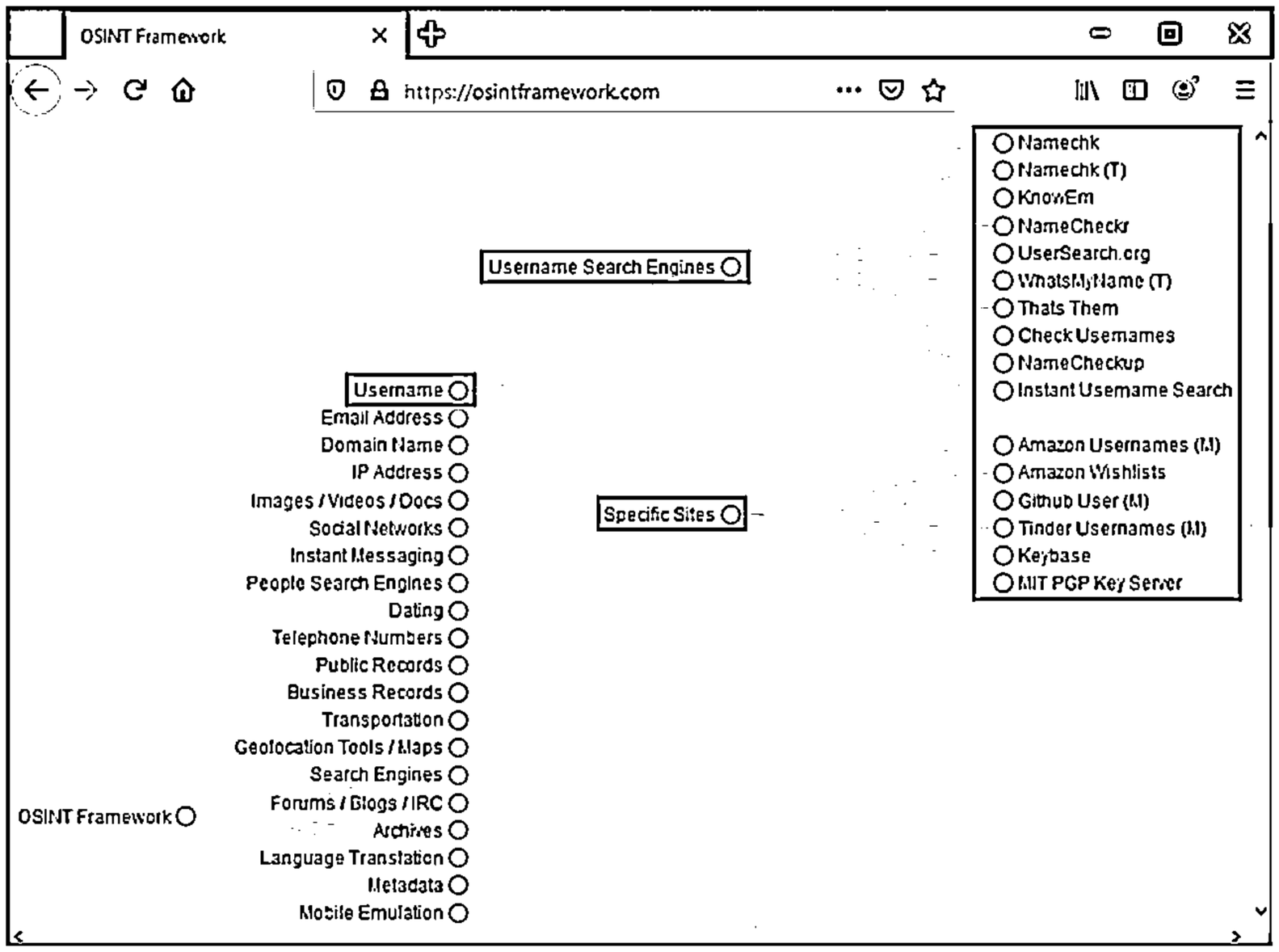


Figure 9.6.2: Username categories

7. From the list of available tools under the **Username Search Engines** category, click on the **Namechk** tool to navigate to the **Namechk** website.

Note: If a cookie notification appears at the lower section of the window, click **Got it!** and close the ads appearing on the screen.

8. The **Namechk** website appears, as shown in the screenshot.

Note: Namechk is used to see if your desired username or vanity URL is still available at dozens of popular social networking and social bookmarking websites. You can also find the best username with Namechk.

The OSINT Framework includes the following indicators with the available tools:

- (T) - Indicates a link to a tool that must be installed and run locally
- (D) - Google Dork
- (R) - Requires registration
- (M) - Indicates a URL that contains the search term and the URL itself must be edited manually.

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

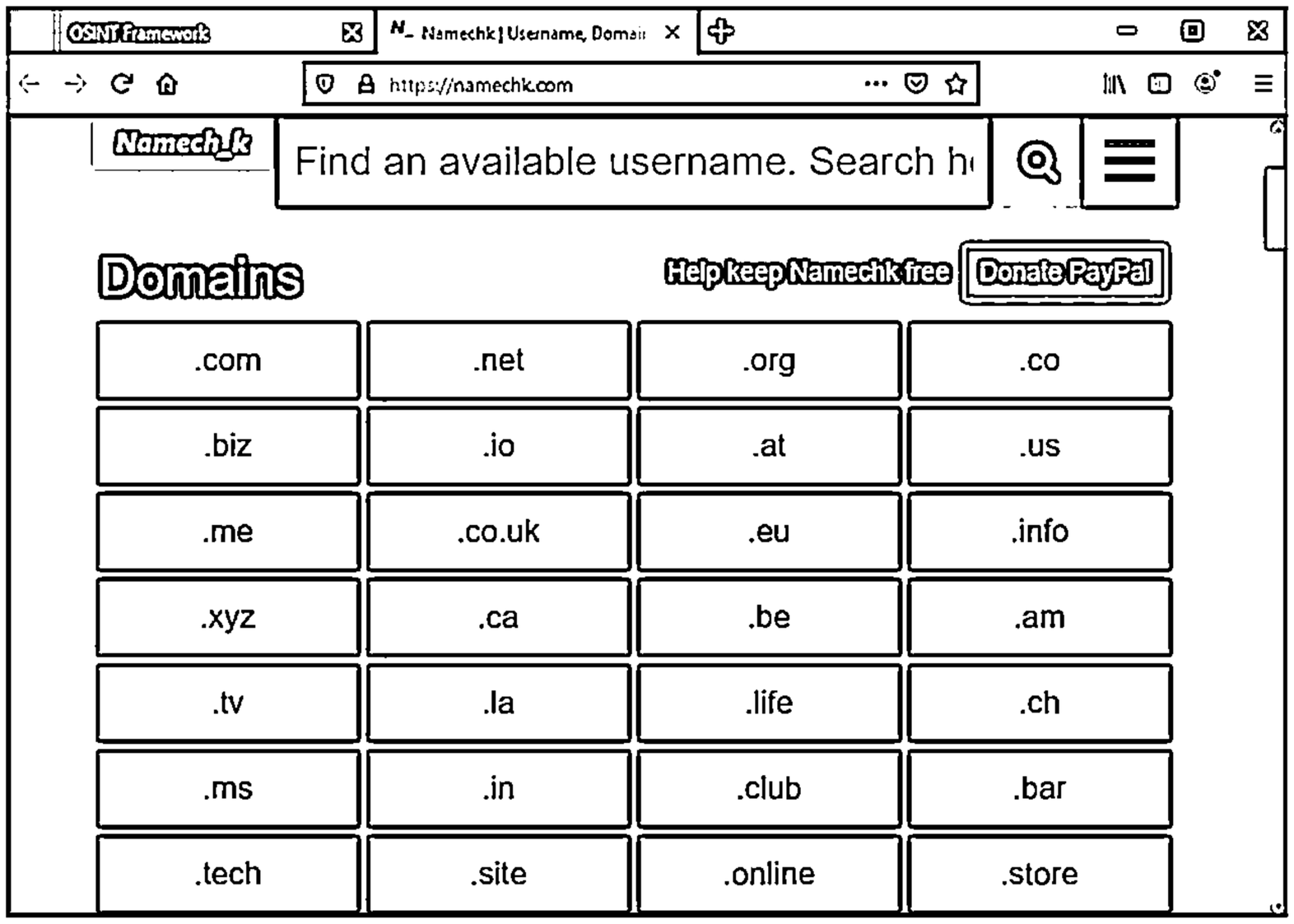


Figure 9.6.3: Namechk website

9. Close the current tab to navigate back to the **OSINT Framework** webpage.
10. Similarly, you can explore other tools from the list of mentioned tools under the **Username Search Engines** and **Specific Sites** sub-categories.

TASK 6.3

View Domain Name Category

11. Now, click the **Domain Name** category, and its sub-categories appear. Click to expand the **Whois Records** sub-category.
12. A list of tools under the **Whois Records** sub-category appears; click the **Domain Dossier** tool.

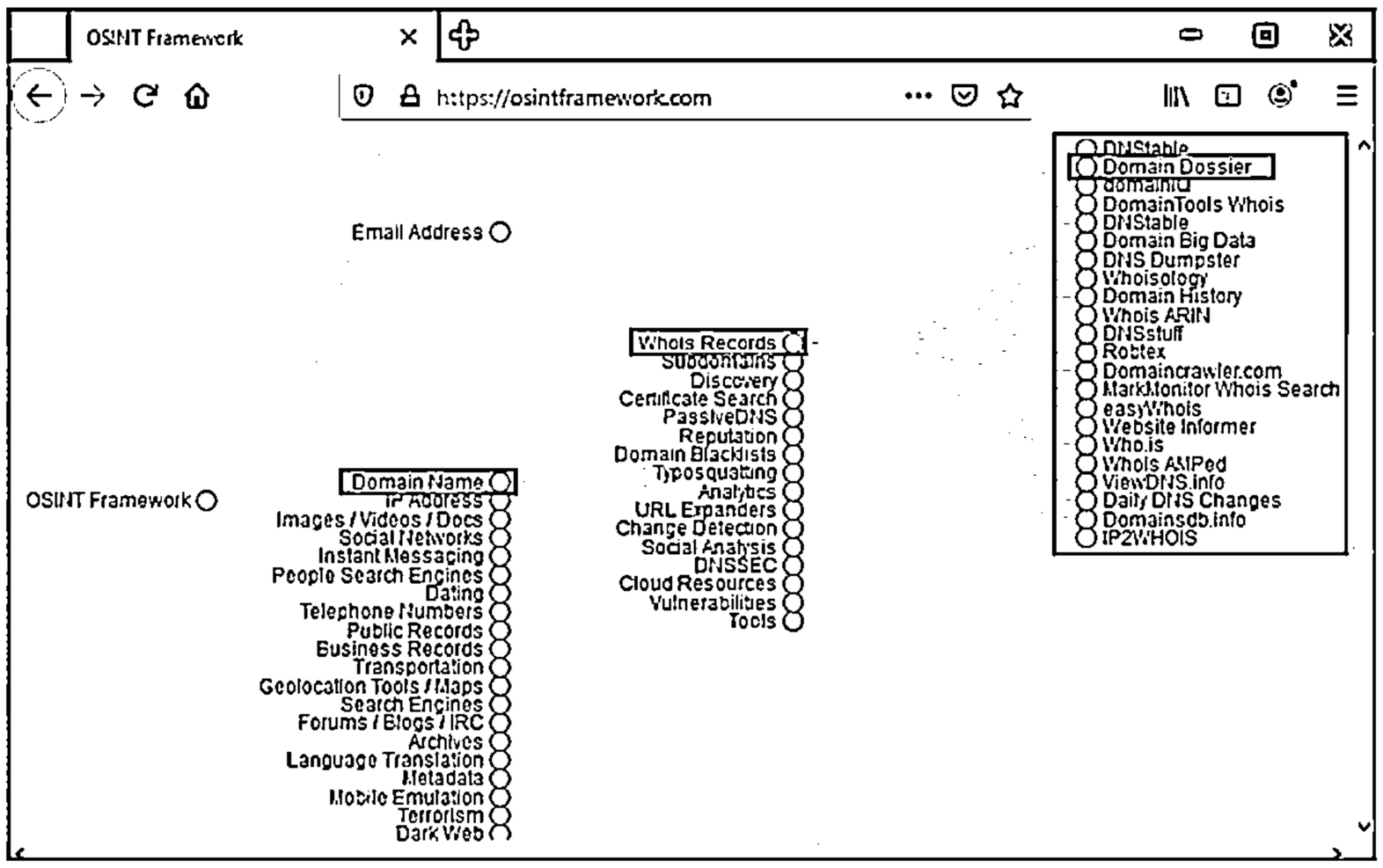


Figure 9.6.4: Clicking on Domain Dossier

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

13. The **Domain Dossier** website appears, as shown in the screenshot.

Note: The Domain Dossier tool generates reports from public records about domain names and IP addresses to help solve problems, investigate cybercrime, or just to better understand how things are set up.

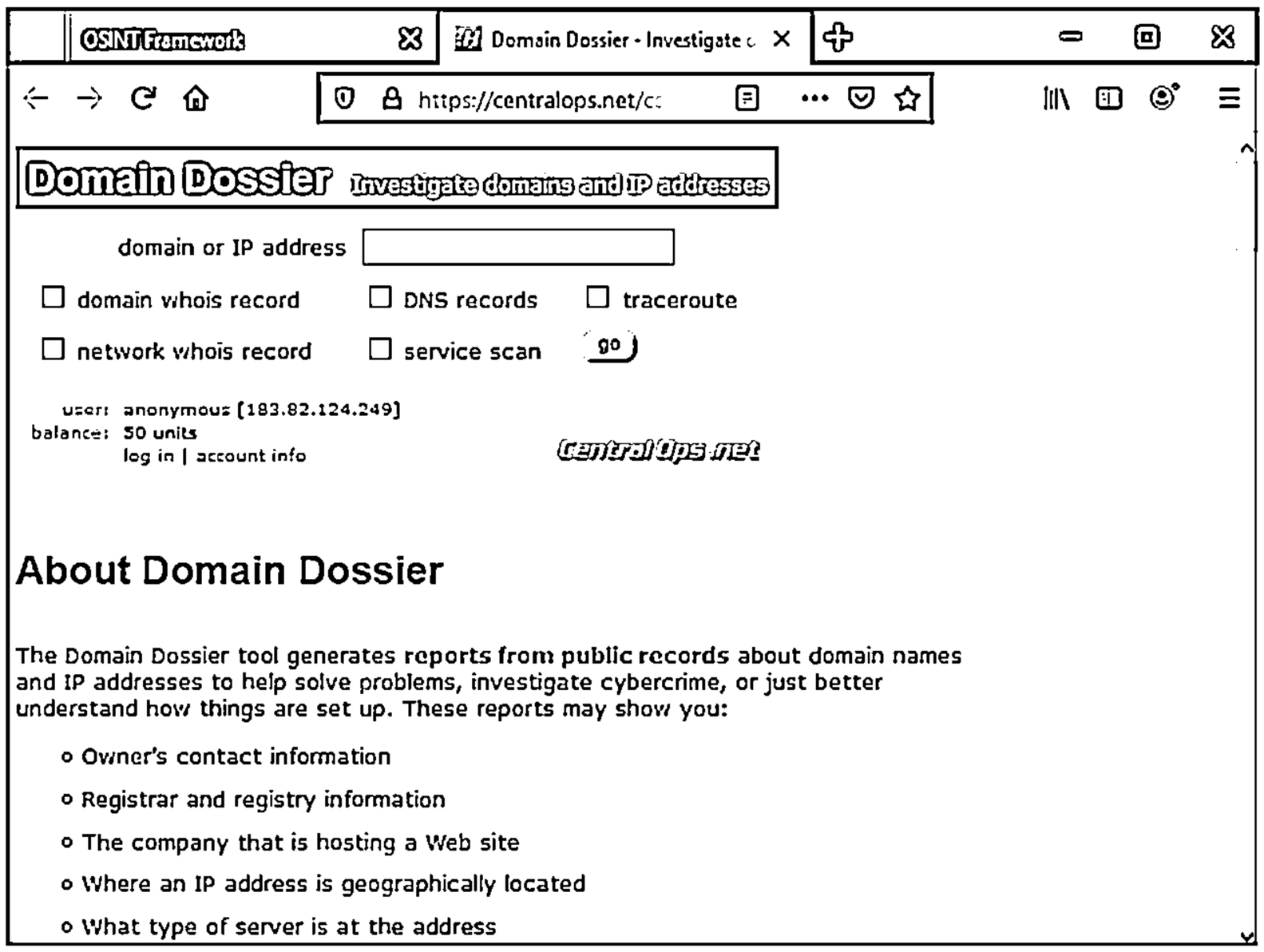


Figure 9.6.5: Domain Dossier website

14. Close the current tab to navigate back to the **OSINT Framework** webpage.

TASK 6.4

View Metadata Category

15. Now, click the **Metadata** category and click the **FOCA** tool from a list of available tools.

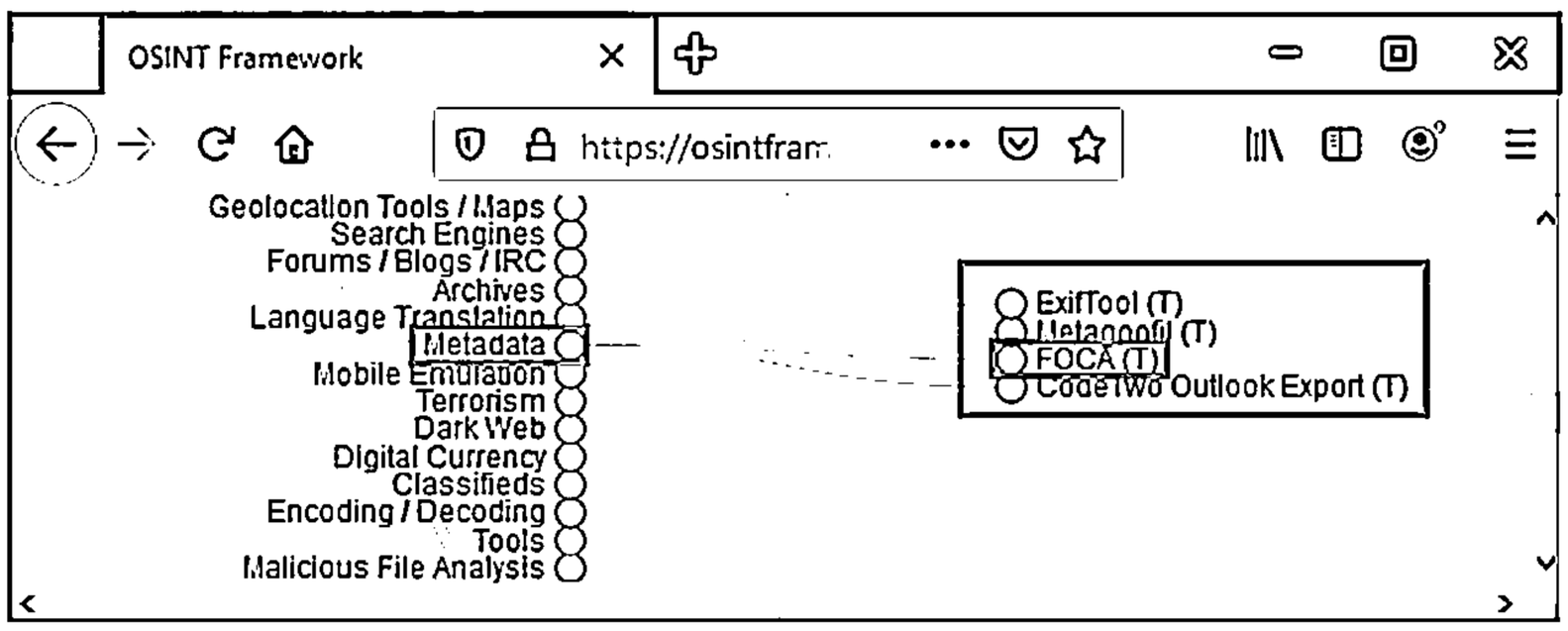


Figure 9.6.6: Metadata category

16. The **FOCA** website appears, displaying information about the tool along with its download link, as shown in the screenshot.

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

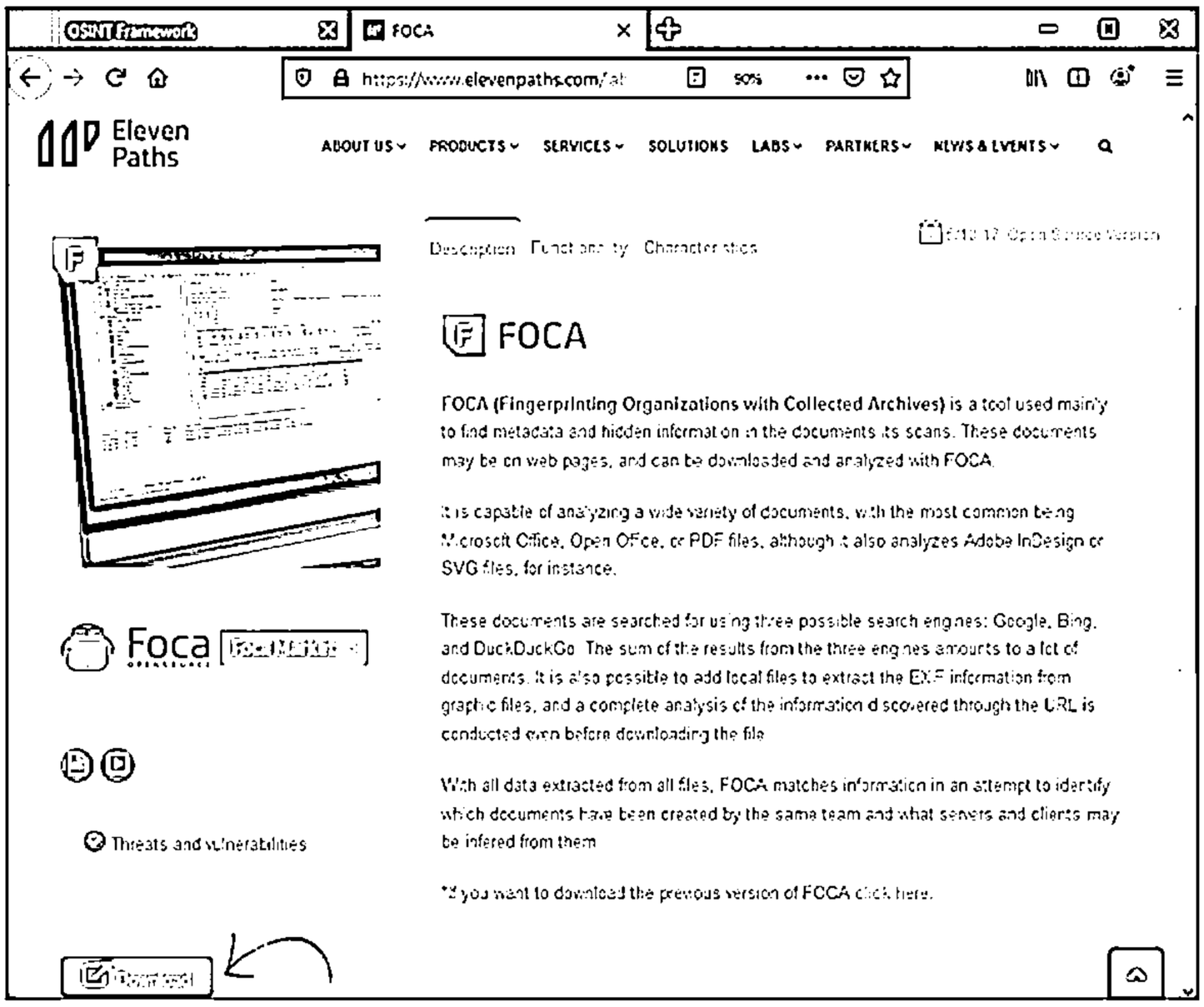


Figure 9.6.7: FOCA website

17. Similarly, you can explore other available categories such as **Email Address, IP Address, Social Networks, Instant Messaging,** etc. and the tools associated with each category. Using these tools, you can perform footprinting on the target organization.
18. This concludes the demonstration of performing footprinting using the OSINT Framework.
19. Close all open windows and document all the acquired information.
20. Turn off the **Windows 10** virtual machine.

Lab Analysis

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

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT 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.

Scanning Networks

Module 03

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

Scanning a Target Network

Network scanning refers to a set of procedures performed to identify the hosts, ports, and services running in a network.

Lab Scenario

ICON KEY

Valuable information

Test your knowledge

Web exercise

Workbook review

Earlier, you gathered all possible information about the target such as organization information (employee details, partner details, web links, etc.), network information (domains, sub-domains, IP addresses, network topology, etc.), and system information (OS details, user accounts, passwords, etc.).

Now, as an ethical hacker, or as a penetration tester (hereafter, pen tester), your next step will be to perform port scanning and network scanning on the IP addresses that you obtained in the information-gathering phase. This will help you to identify an entry point into the target network.

Scanning itself is not the actual intrusion, but an extended form of reconnaissance in which the ethical hacker and pen tester learns more about the target, including information about open ports and services, OSes, and any configuration lapses. The information gleaned from this reconnaissance helps you to select strategies for the attack on the target system or network.

This is one of the most important phases of intelligence gathering, which enables you to create a profile of the target organization. In the process of scanning, you attempt to gather information, including the specific IP addresses of the target system that can be accessed over the network (live hosts), open ports, and respective services running on the open ports and vulnerabilities in the live hosts.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 03 Scanning Networks

Port scanning will help you identify open ports and services running on specific ports, which involves connecting to Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) system ports. Port scanning is also used to discover the vulnerabilities in the services running on a port.

The labs in this module will give you real-time experience in gathering information about the target organization using various network scanning and port scanning techniques.

Lab Objectives

The objective of this lab is to conduct network scanning, port scanning, analyzing the network vulnerabilities, etc.

Network scans are needed to:

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

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

Lab Environment

To carry out this lab, you need:

- Windows Server 2019 virtual machine
- Windows Server 2016 virtual machine
- Windows 10 virtual machine
- Ubuntu virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 140 Minutes

Overview of Scanning Networks

Network scanning is the process of gathering additional detailed information about the target by using highly complex and aggressive reconnaissance techniques. The purpose of scanning is to discover exploitable communication channels, probe as many listeners as possible, and keep track of the responsive ones.

Types of scanning:

- **Port Scanning:** Lists open ports and services
- **Network Scanning:** Lists the active hosts and IP addresses
- **Vulnerability Scanning:** Shows the presence of known weaknesses

Lab Tasks

Ethical hackers and pen testers use numerous tools and techniques to scan the target network. Recommended labs that will assist you in learning various network scanning techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	iLabs ***
1	Perform Host Discovery	√	√	√
	1.1 Perform Host Discovery using Nmap	√		√
	1.2 Perform Host Discovery using Angry IP Scanner		√	√
2	Perform Port and Service Discovery	√	√	√
	2.1 Perform Port and Service Discovery using MegaPing		√	√

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

	2.2 Perform Port and Service Discovery using NetScanTools Pro		√	√
	2.3 Explore Various Network Scanning Techniques using Nmap	√		√
	2.4 Explore Various Network Scanning Techniques using Hping3		√	√
3	Perform OS Discovery	√	√	√
	3.1 Identify the Target System's OS with Time-to-Live (TTL) and TCP Window Sizes using Wireshark		√	√
	3.2 Perform OS Discovery using Nmap Script Engine (NSE)	√		√
	3.3 Perform OS Discovery using Unicornscan		√	√
4	Scan beyond IDS and Firewall	√	√	√
	4.1 Scan beyond IDS/Firewall using various Evasion Techniques	√		√
	4.2 Create Custom Packets using Colasoft Packet Builder to Scan beyond IDS/Firewall		√	√
	4.3 Create Custom UDP and TCP Packets using Hping3 to Scan beyond IDS/Firewall	√		√
	4.4 Create Custom Packets using Nmap to Scan beyond IDS/Firewall		√	√
	4.5 Browse Anonymously using Proxy Switcher		√	
	4.6 Browse Anonymously using CyberGhost VPN		√	
5	Draw Network Diagrams		√	√
	5.1 Draw Network Diagrams using Network Topology Mapper		√	√
6	Perform Network Scanning using Various Scanning Tools	√		√
	6.1 Scan a Target Network using Metasploit	√		√

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

***Core** - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv11 volume 1 book.

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

***iLabs - Lab exercise(s) marked under iLabs are available in our iLabs solution. iLabs is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed from anywhere with an Internet connection. If you are interested to learn more about our iLabs solution, please contact your training center or visit https://ilabs.eccouncil.org.

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

Perform Host Discovery

Host discovery is the process of identifying active hosts in the target network.

ICON KEY

- Valuable Information
- Test Your Knowledge
- Web Exercise
- Workbook Review

Lab Scenario

As a professional ethical hacker or pen tester, you should be able to scan and detect the active network systems/devices in the target network. During the network scanning phase of security assessment, your first task is to scan the network systems/devices connected to the target network within a specified IP range and check for live systems in the target network.

Lab Objectives

- Perform host discovery using Nmap
- Perform host discovery using Angry IP Scanner

Lab Environment

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 03 Scanning Networks

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2016 virtual machine
- Ubuntu virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- Nmap located at **E:\CEH-Tools\CEHv11 Module 03 Scanning Networks\Scanning Tools\Nmap**
- Angry IP Scanner located at **E:\CEH-Tools\CEHv11 Module 03 Scanning Networks\Ping Sweep Tools\Angry IP Scanner**
- You can also download the latest version of the above-mentioned tools from their official websites. If you decide to download the latest version, the 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 Host Discovery

Host discovery is considered the primary task in the network scanning process. It is used to discover the active/live hosts in a network. It provides an accurate status of the systems in the network, which, in turn, reduces the time spent on scanning every port on every system in a sea of IP addresses in order to identify whether the target host is up.

The following are examples of host discovery techniques:

- ARP ping scan
- UDP ping scan
  - ICMP ping scan (ICMP ECHO ping, ICMP timestamp, ping ICMP, and address mask ping)
  - TCP ping scan (TCP SYN ping and TCP ACK ping)
- IP protocol scan

Lab Tasks

TASK 1

Perform Host Discovery using Nmap

Nmap is a utility used for network discovery, network administration, and security auditing. It is also used to perform tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime

Here, we will use Nmap to discover a list of live hosts in the target network. We can use Nmap to scan the active hosts in the target network using various host discovery techniques such as ARP ping scan, UDP ping scan, ICMP ECHO ping scan, ICMP ECHO ping sweep, etc.

1. Turn on one or more virtual machines. In this lab task, we have used the **Windows 10**, **Windows Server 2016**, and **Parrot Security** virtual machines.

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

2. In the **Windows 10** virtual machine, log in with the credentials Username: **Admin** and Password: **Pa$$w0rd**.

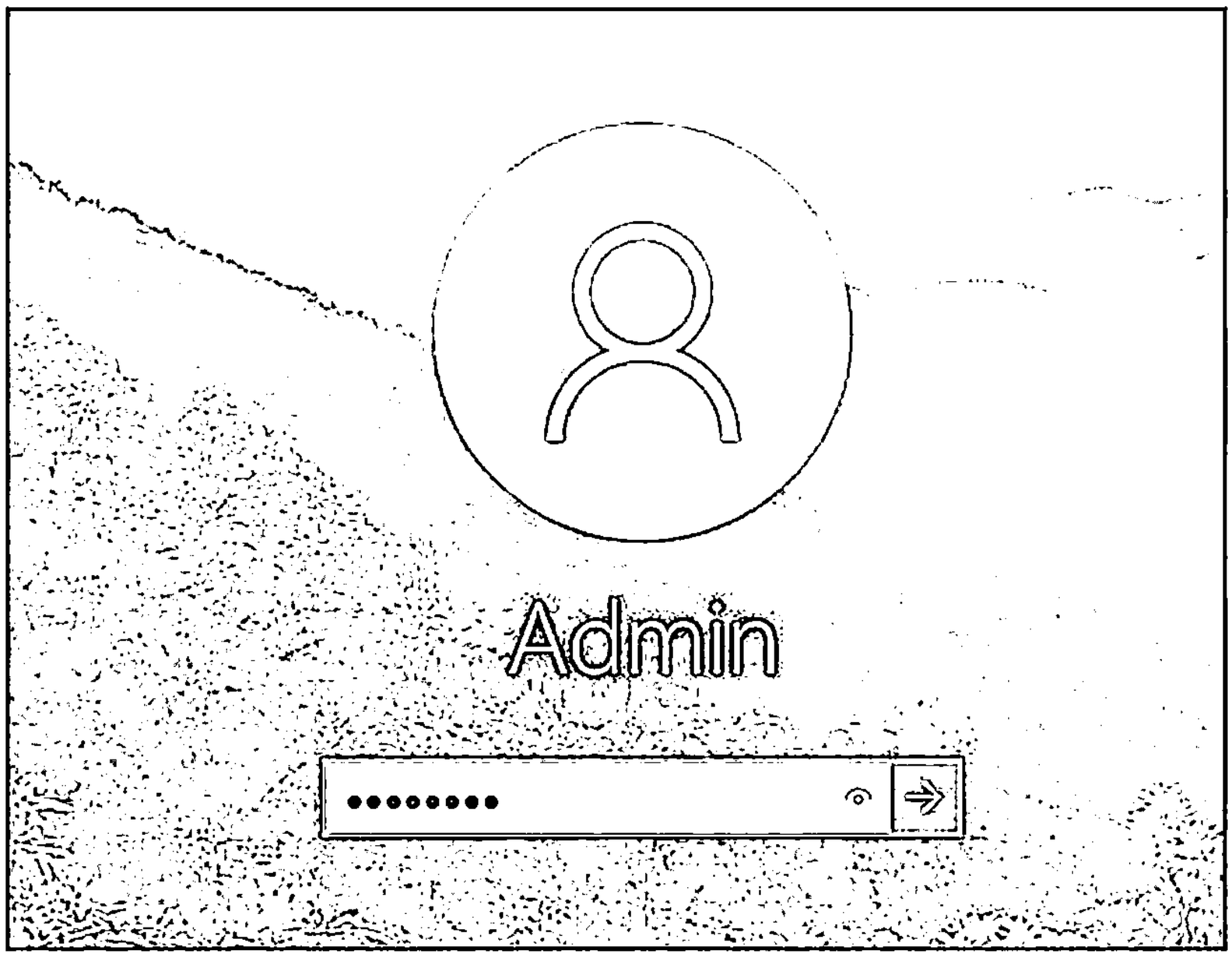


Figure 1.1.1: Login window

TASK 1.1

Install Nmap

3. Navigate to **E:\CEH-Tools\CEHv11 Module 03 Scanning Networks\Scanning Tools\Nmap**; then, double-click **nmap-7.80-setup.exe**.

Note: If a **User Account Control** window appears, click **Yes**.

Note: If an **Open File - Security Warning** pop-up appears, click **Run**.

4. In the **Nmap Setup** window, click **I Agree** and follow the installation steps to install Nmap using all default settings.

Note: If an **Npcap Setup** window appears, click **Install** and follow the installation steps. After the completion of the installation, click **Finish**.

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

5. In the **Nmap Setup** window, follow the wizard-driven steps to install Nmap and click **Finish**.

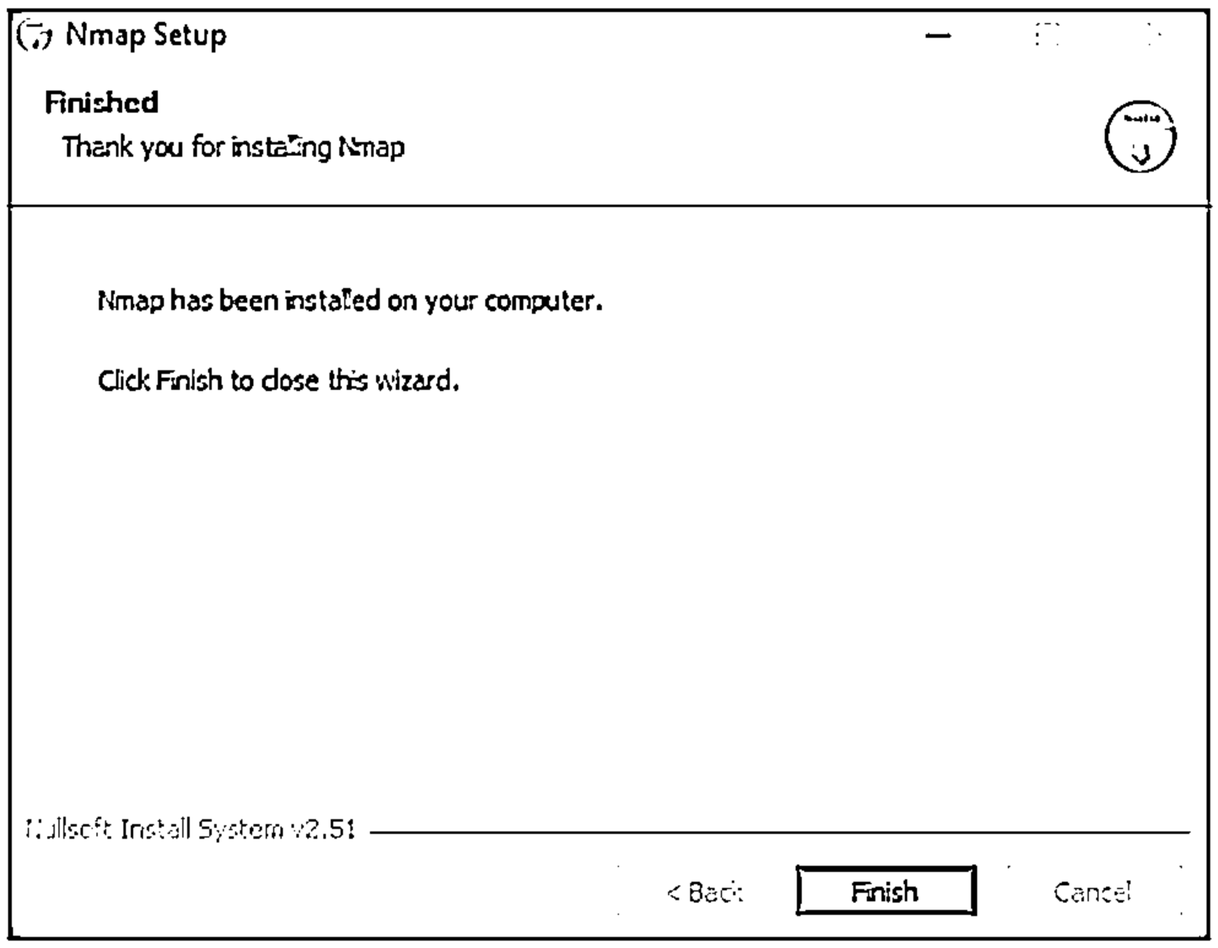


Figure 1.1.2: Nmap Setup pop-up wizard

6. On the completion of the installation, click on the **Start** menu on the bottom-left corner of **Desktop** and launch **Nmap - Zenmap GUI** from the applications, as shown in the screenshot.

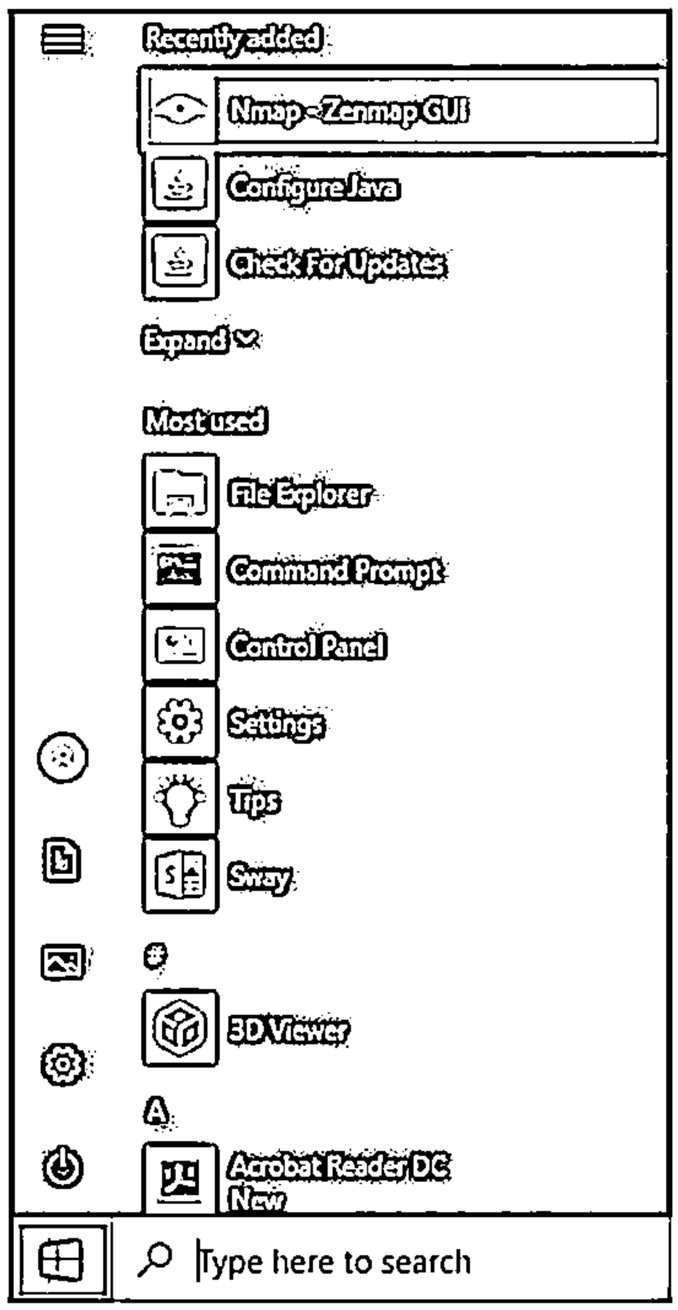


Figure 1.1.3: Launch Nmap - Zenmap

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

TASK 1.2

Perform ARP Ping Scan

7. The **Nmap - Zenmap** GUI appears; in the **Command** field, type the command **nmap -sn -PR <Target IP Address>** (here, the target IP address is **10.10.10.16**) and click **Scan**.

Note: **-sn**: disables port scan and **-PR**: performs ARP ping scan.

8. The scan results appear, indicating that the target **Host is up**, as shown in the screenshot.

Note: In this lab, we are targeting the **Windows Server 2016** (**10.10.10.16**) virtual machine.

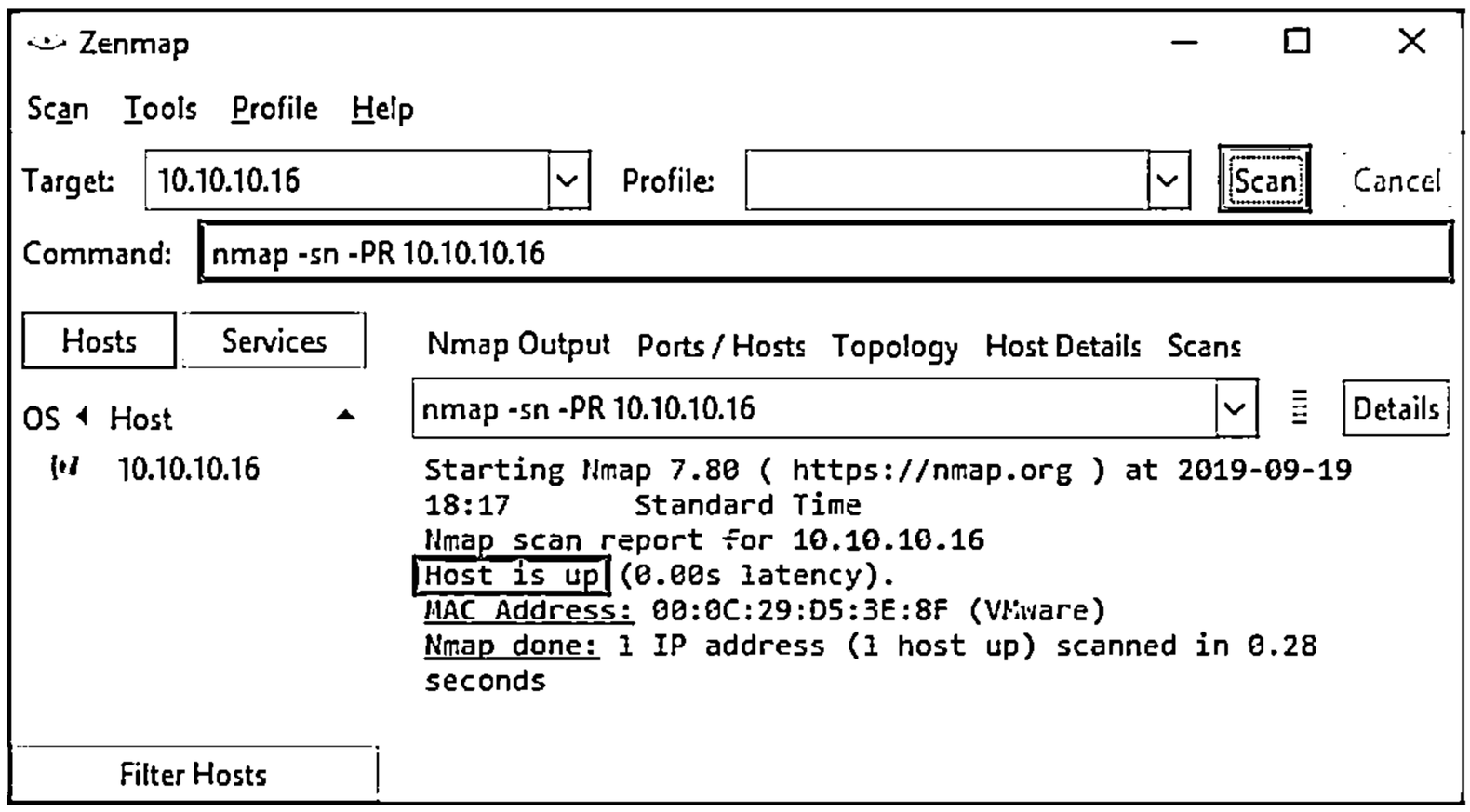


Figure 1.1.4: Zenmap scan results for ARP ping scan

Note: The ARP ping scan probes ARP request to target host; an ARP response means that the host is active.

TASK 1.3

Perform UDP Ping Scan

9. In the **Command** field, type **nmap -sn -PU <Target IP Address>**, (here, the target IP address is **10.10.10.16**) and click **Scan**. The scan results appear, indicating the target **Host is up**, as shown in the screenshot.

Note: **-PU**: performs the UDP ping scan.

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

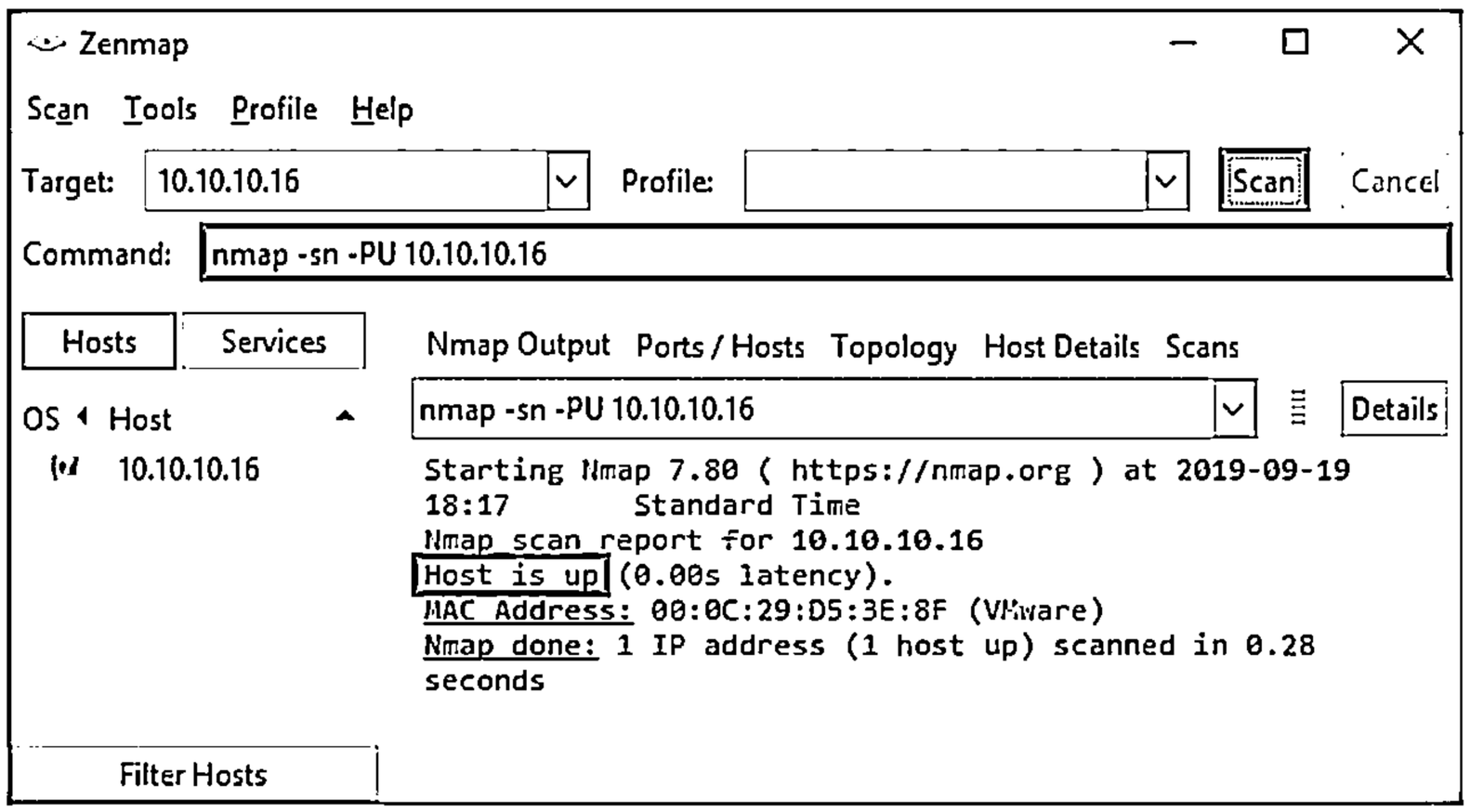


Figure 1.1.5: Zenmap scan results for UDP ping scan

Note: The UDP ping scan sends UDP packets to the target host; a UDP response means that the host is active. If the target host is offline or unreachable, various error messages such as "host/network unreachable" or "TTL exceeded" could be returned.

TASK 1.4

Perform ICMP ECHO Ping Scan

10. Now, we will perform the ICMP ECHO ping scan. In the **Command** field, type **nmap -sn -PE <Target IP Address>**, (here, the target IP address is **10.10.10.16**) and click **Scan**. The scan results appear, indicating that the target **Host is up**, as shown in the screenshot.

Note: **-PE**: performs the ICMP ECHO ping scan.

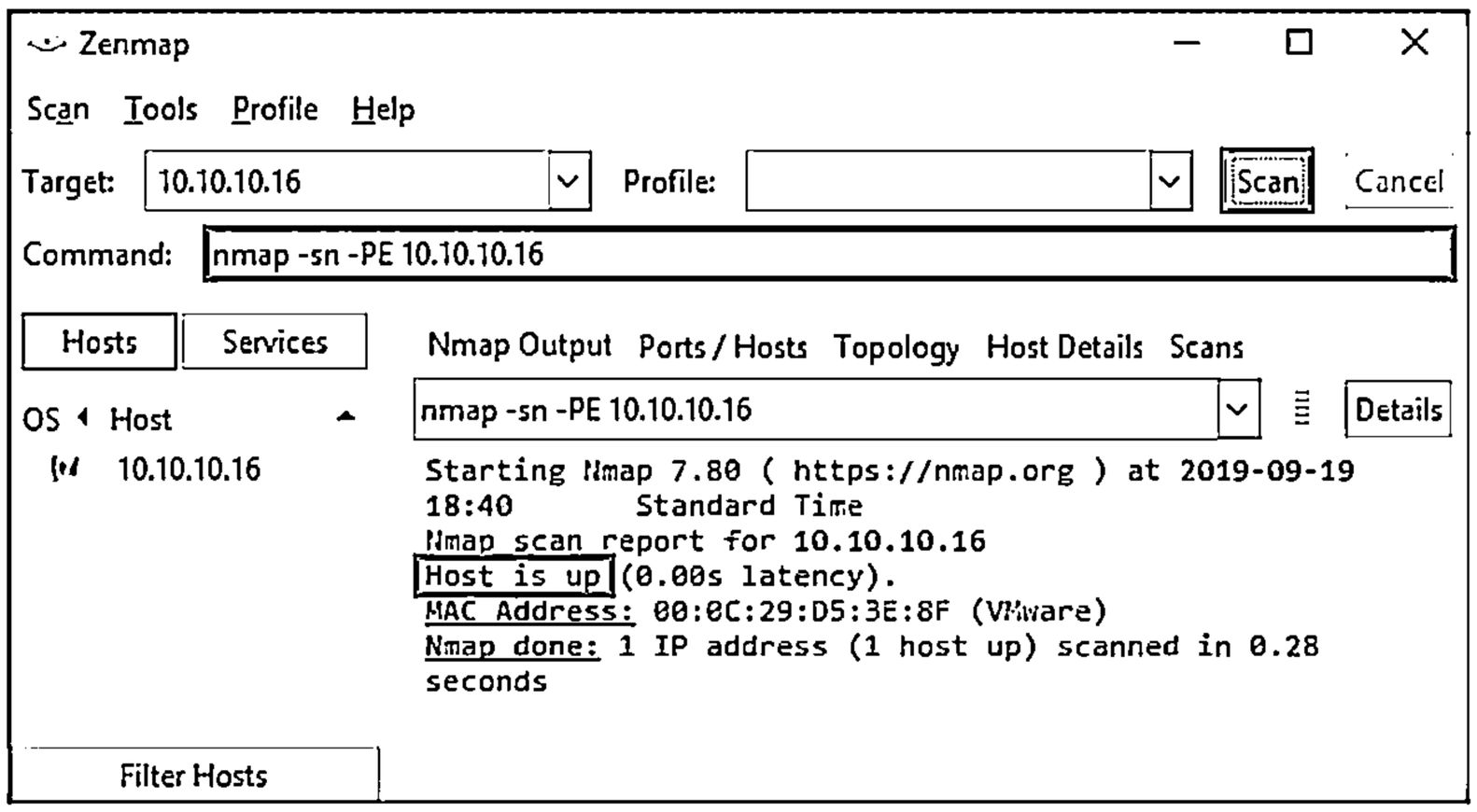


Figure 1.1.6: Zenmap scan results for ICMP ECHO ping scan

Note: The ICMP ECHO ping scan involves sending ICMP ECHO requests to a host. If the target host is alive, it will return an ICMP ECHO reply. This scan is useful for locating active devices or determining if the ICMP is passing through a firewall.

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

TASK 1.5

Perform ICMP ECHO Ping Sweep

11. Now, we will perform an ICMP ECHO ping sweep to discover live hosts from a range of target IP addresses. In the **Command** field, type **nmap -sn -PE <Target Range of IP Addresses>** (here, the target range of IP addresses is **10.10.10.11-20**) and click **Scan**. The scan results appear, indicating the target **Host is up**, as shown in the screenshot

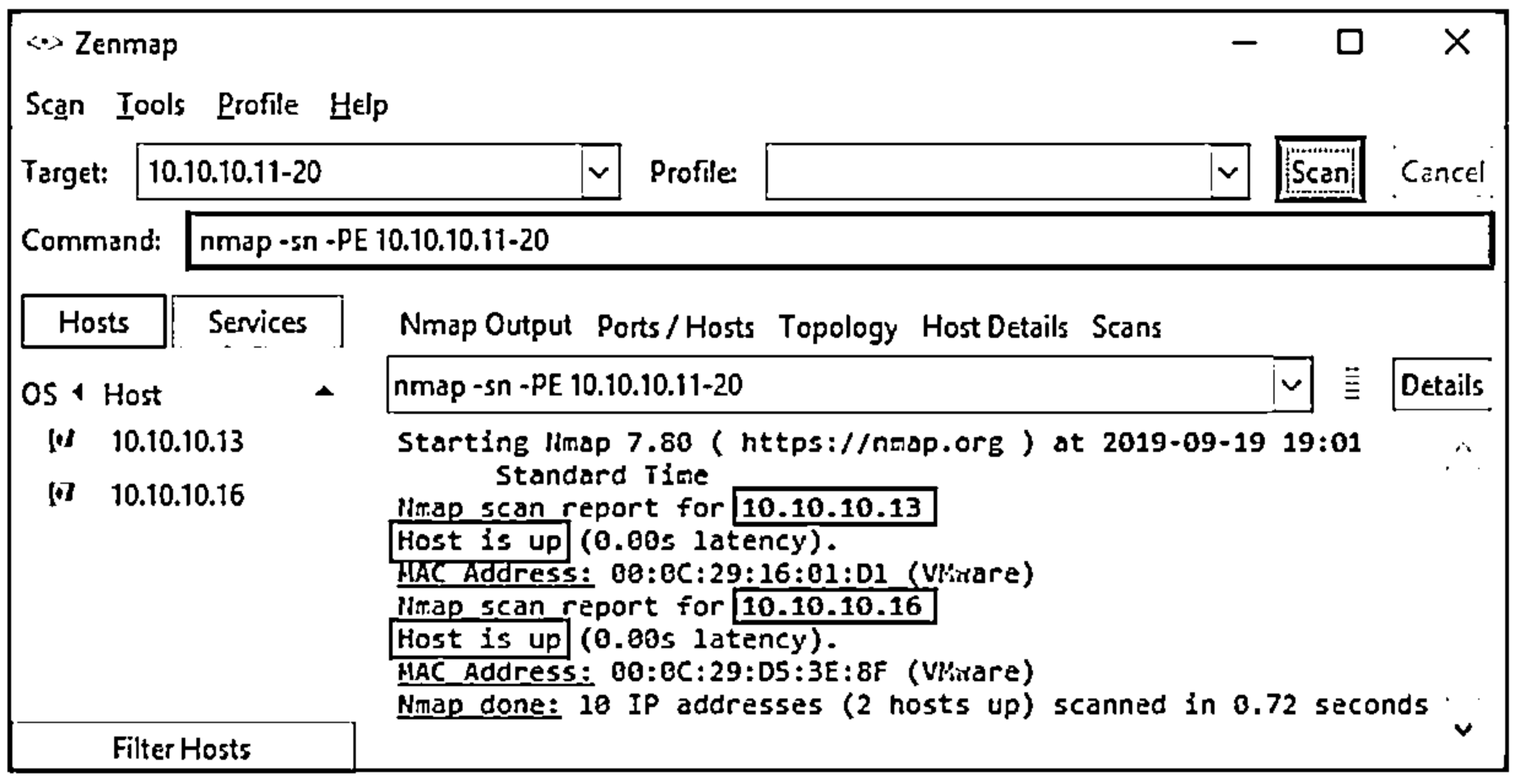


Figure 1.1.7: Zenmap scan results for ICMP ECHO ping sweep scan

Note: The ICMP ECHO ping sweep is used to determine the live hosts from a range of IP addresses by sending ICMP ECHO requests to multiple hosts. If a host is alive, it will return an ICMP ECHO reply.

12. Apart from the aforementioned network scanning techniques, you can also use the following scanning techniques to perform a host discovery on a target network.

- **ICMP Timestamp and Address Mask Ping Scan:** These techniques are alternatives for the traditional ICMP ECHO ping scan, which are used to determine whether the target host is live specifically when administrators block the ICMP ECHO pings.

  Example –

  ICMP timestamp ping scan

  # nmap -sn -PP <target IP address>

  ICMP address mask ping scan

  # nmap -sn -PM <target IP address>

- **TCP SYN Ping Scan:** This technique sends empty TCP SYN packets to the target host, ACK response means that the host is active.

  # nmap -sn -PS <target IP address>

- **TCP ACK Ping Scan:** This technique sends empty TCP ACK packets to the target host; an RST response means that the host is active.

  # nmap -sn -PA <target IP address>

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

- **IP Protocol Ping Scan:** This technique sends different probe packets of different IP protocols to the target host, any response from any probe indicates that a host is active.

  # nmap -sn -PO <target IP address>

13. This concludes the demonstration of discovering the target host(s) in the target network using various host discovery techniques.
14. Close all open windows and document all the acquired information.

TASK 2 Perform Host Discovery using Angry IP Scanner

Here, we will use the Angry IP Scanner tool to discover the active hosts in the target network.

1. Turn on the **Ubuntu** virtual machine.

Note: Ensure that the **Windows 10**, **Windows Server 2016**, and **Parrot Security** virtual machines are turned on.

2. In the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 03 Scanning Networks\Ping Sweep Tools\Angry IP Scanner** and double-click **ipscan-win64-3.6.1.exe**.

TASK 2.1

Install Angry IP Scanner

Angry IP Scanner is an open-source and cross-platform network scanner designed to scan IP addresses as well as ports. It simply pings each IP address to check if it is alive; then, optionally by resolving its hostname, determines the MAC address, scans ports, etc. The amount of gathered data about each host can be extended with plugins

3. Angry IP Scanner starts, and a **Getting Started** window pops up. Click **Next**, follow the wizard, and click **Close**.

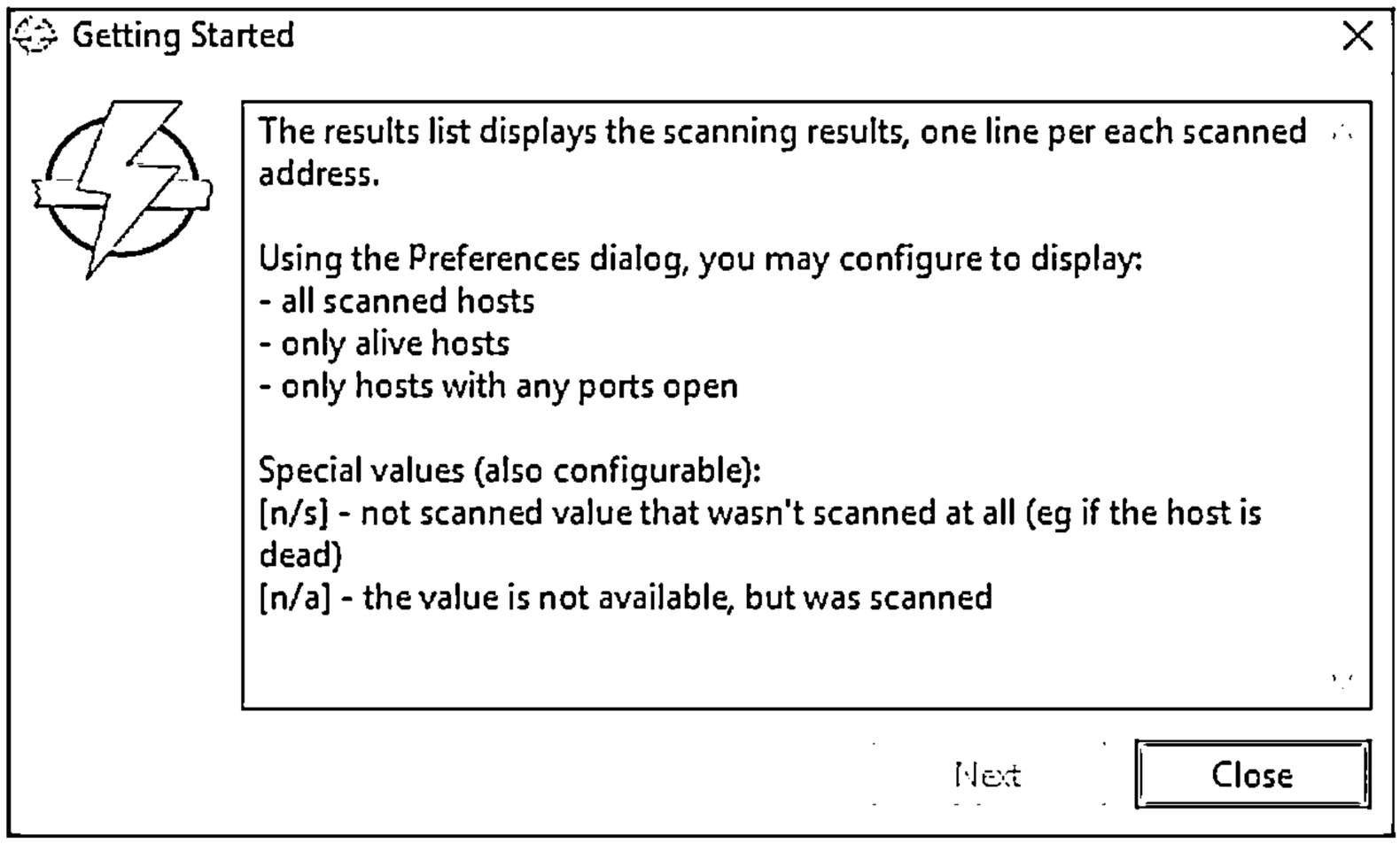


Figure 1.2.1: Getting Started window

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

4. The **IP Range - Angry IP Scanner** window appears, as shown in the screenshot.

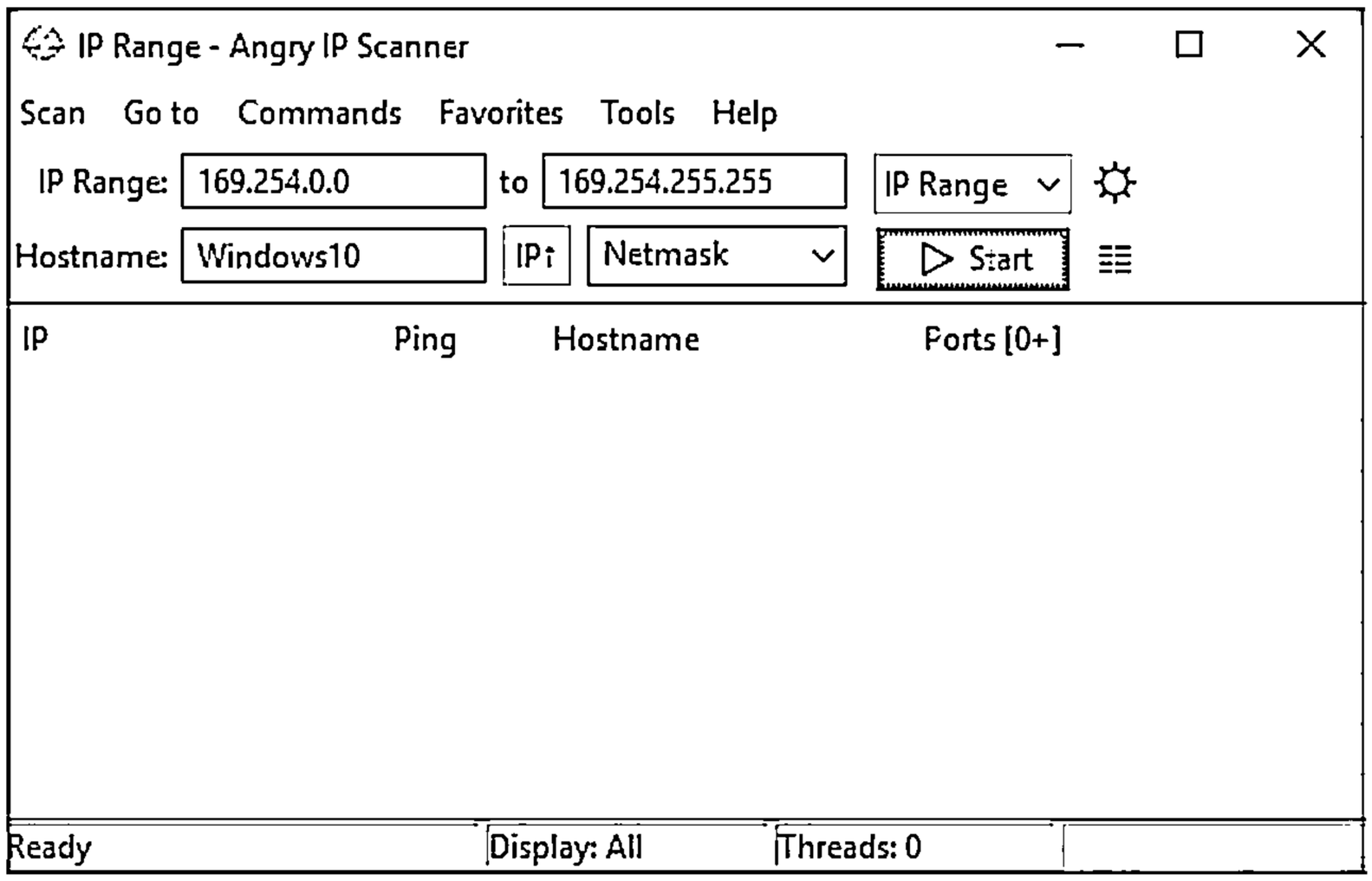


Figure 1.2.2: IP Range - Angry IP Scanner Window

TASK 2.2

Perform the Scan

5. In the **IP Range** fields, type the IP range as **10.10.10.0** to **10.10.10.255** and click the **Preferences** icon beside the **IP Range** menu, as shown in the screenshot.

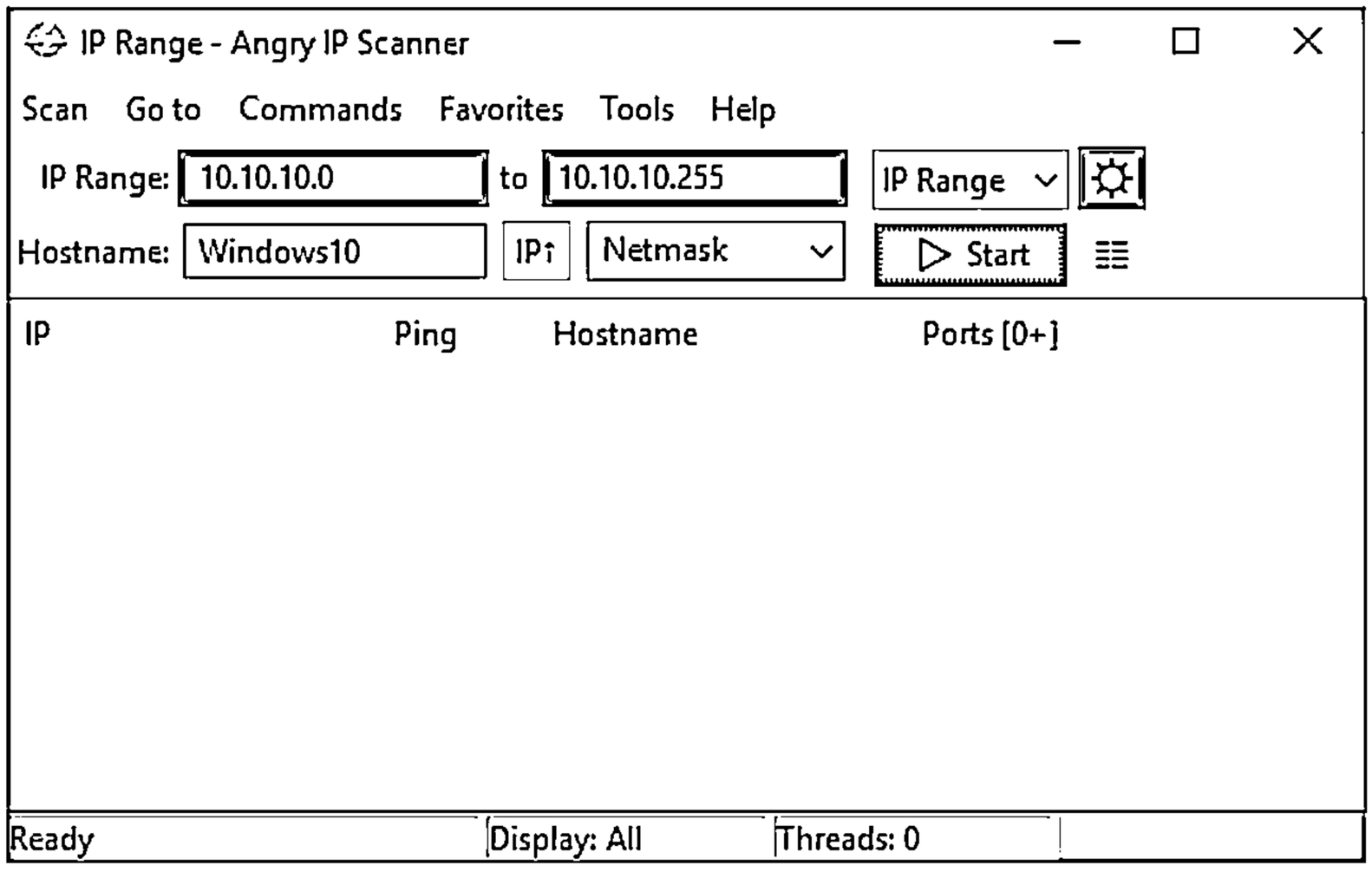


Figure 1.2.3: Filling the IP range

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

6. The **Preferences** window appears. In the **Scanning** tab, under the **Pinging** section, select the **Pinging method** as **Combined UDP+TCP** from the drop-down list.

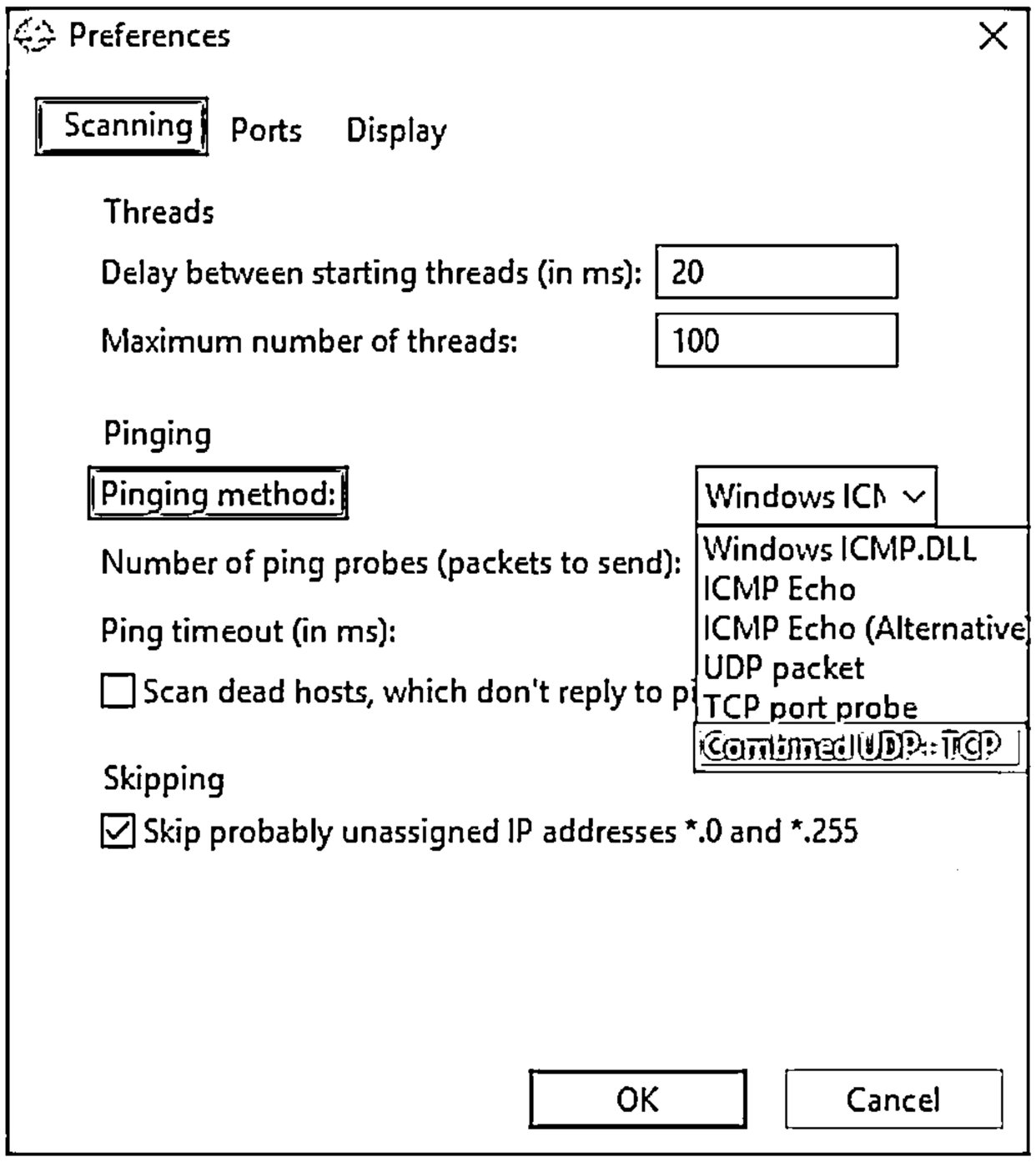


Figure 1.2.4: Angry IP Scanner Preferences window

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

7. Now, switch to the **Display** tab. Under the **Display in the results list** section, select the **Alive hosts (responding to pings) only** radio button and click **OK**.

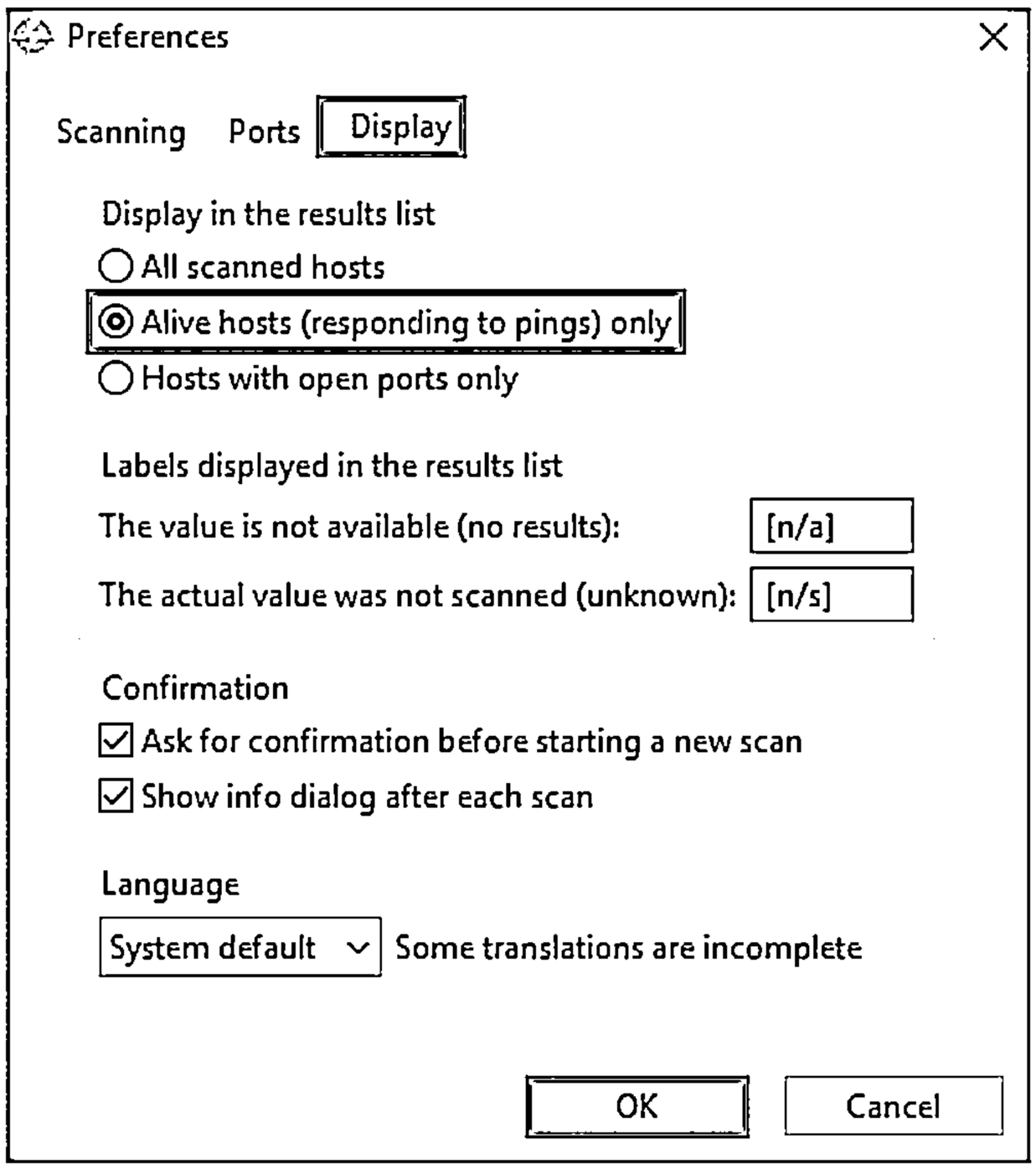


Figure 1.2.5: Display tab options in the preferences window

8. In the **IP Range - Angry IP Scanner** window, click the **Start** button to start scanning the IP range that you entered.

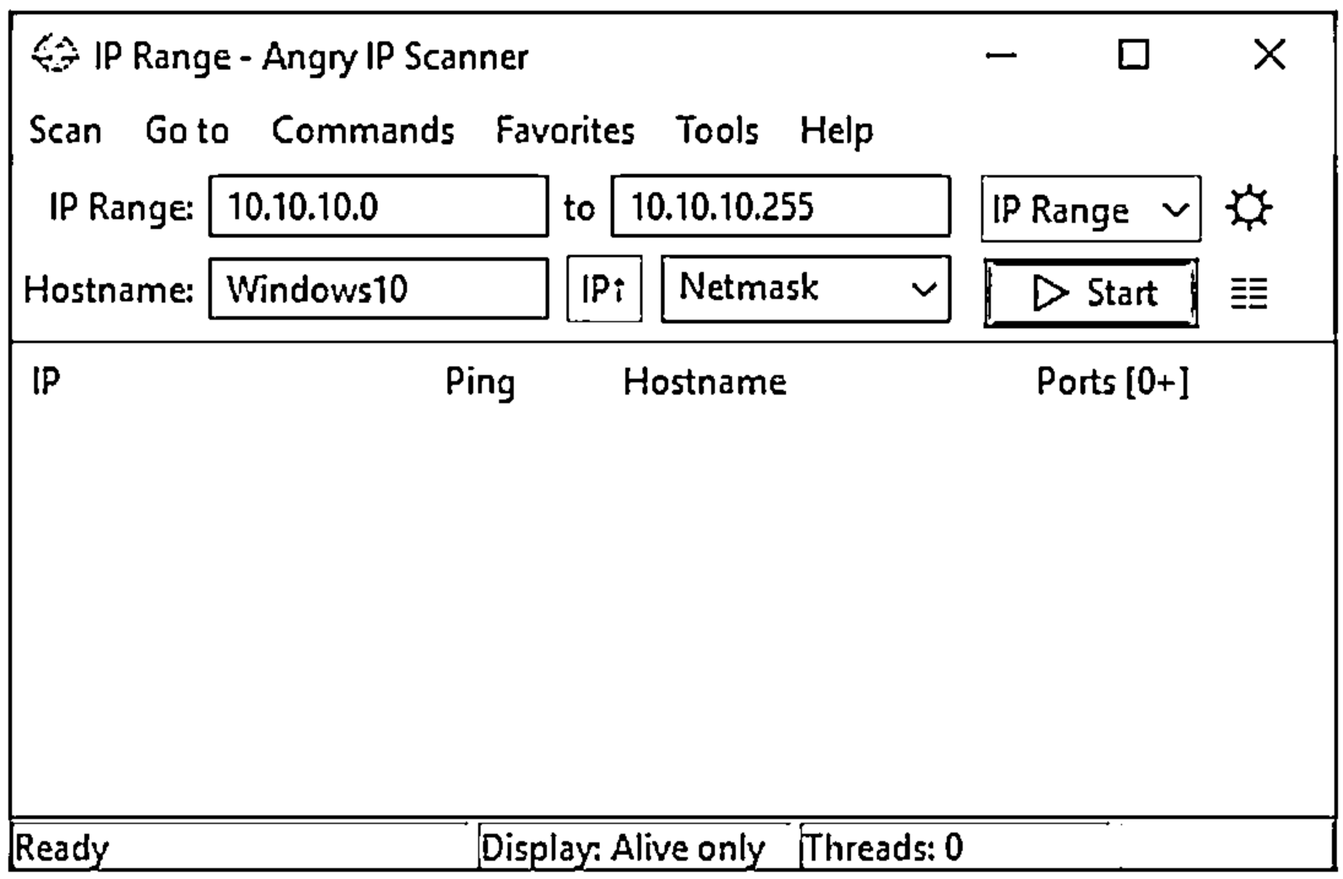


Figure 1.2.6: Starting the scan

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

9. **Angry IP Scanner** starts scanning the IP range and begins to list out the alive hosts found. Check the progress bar on the bottom-right corner to see the progress of the scanning.

Note: IP addresses may differ in your lab environment.

10. After the scanning is completed, a **Scan Statistics** pop-up appears. Note the total number of **Hosts alive** (here, 6) and click **Close**.

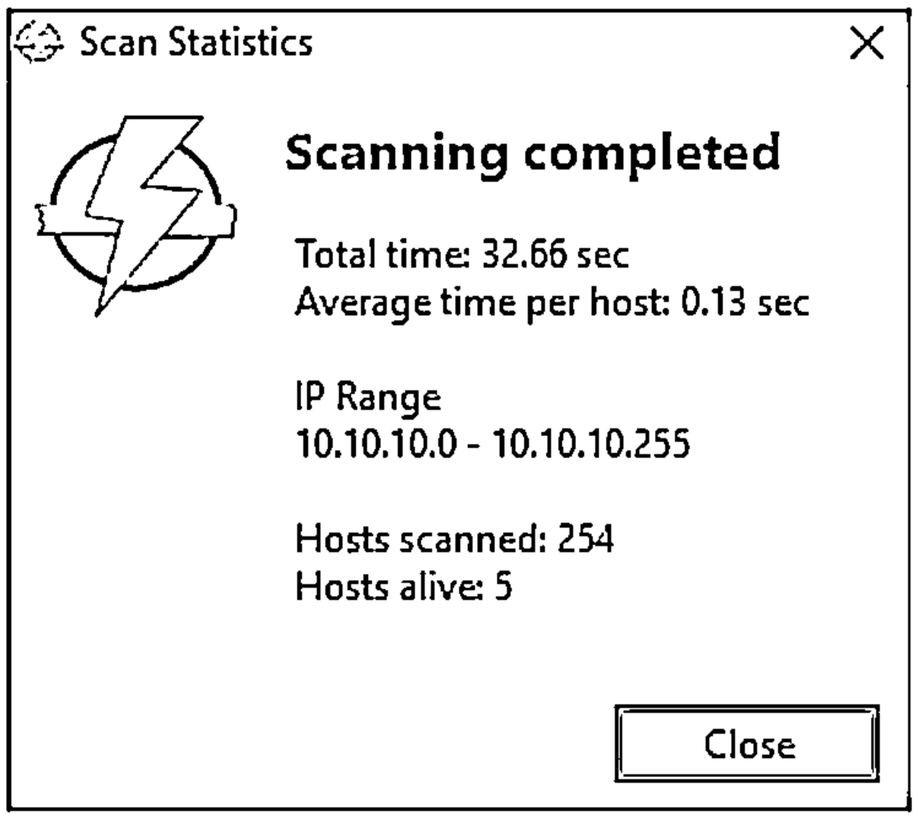


Figure 1.2.7: Scanning Completed prompt

You can also use other ping sweep tools such as **SolarWinds Engineer's Toolset** (https://www.solarwinds.com), **NetScanTools Pro** (https://www.netscantools.com), **Colasoft Ping Tool** (https://www.colasoft.com), **Visual Ping Tester** (http://www.pingtester.net), and **OpUtils** (https://www.manageengine.com) to discover active hosts in the target network

11. The results of the scan appear in the **IP Range - Angry IP Scanner** window. You can see all active IP addresses with their hostnames listed in the main window.

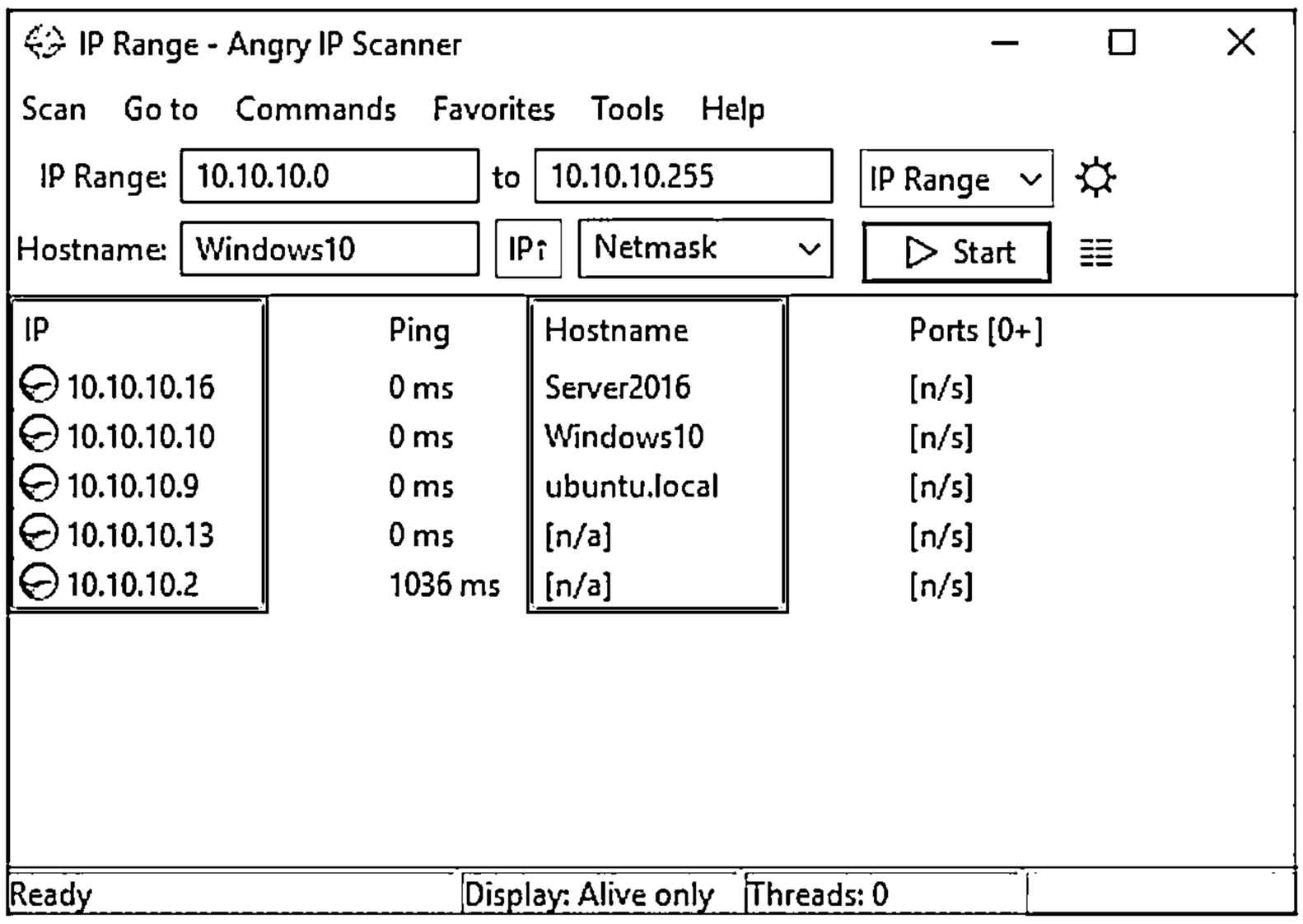


Figure 1.2.8: Scan results

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

12. This concludes the demonstration of discovering alive hosts in the target range of IP addresses using various Angry IP Scanner.
13. Close all open windows and document all the acquired information.
14. Turn off all the virtual machines.

Lab Analysis

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

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT 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

Perform Port and Service Discovery

Port and service discovery is the process of identifying open ports and services running on the target IP addresses/active hosts.

ICON KEY

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

Lab Scenario

As a professional ethical hacker or a pen tester, the next step after discovering active hosts in the target network is to scan for open ports and services running on the target IP addresses in the target network. This discovery of open ports and services can be performed by using various port scanning tools and techniques.

Lab Objectives

- Perform port and service discovery using MegaPing
- Perform port and service discovery using NetScanTools Pro
- Explore various network scanning techniques using Nmap
- Explore various network scanning techniques using Hping3

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2016 virtual machine
- Parrot Security virtual machine
- Ubuntu virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- MegaPing located at **E:\CEH-Tools\CEHv11 Module 03 Scanning Networks\Scanning Tools\MegaPing**

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

- NetScanTools Pro located at **E:\CEH-Tools\CEHv11 Module 03 Scanning Networks\Scanning Tools\NetScanTools Pro**
- You can also download the latest version of the above-mentioned tools from their official websites. If you decide to download the latest version, the screenshots shown in the lab might differ.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 03 Scanning Networks

Lab Duration

Time: 40 Minutes

Overview of Port and Service Discovery

Port scanning techniques are categorized according to the type of protocol used for communication within the network.

- **TCP Scanning**
  - Open TCP scanning methods (TCP connect/full open scan)
  - Stealth TCP scanning methods (Half-open Scan, Inverse TCP Flag Scan, ACK flag probe scan, third party and spoofed TCP scanning methods)
- **UDP Scanning**
- **SCTP Scanning**
  - SCTP INIT Scanning
  - SCTP COOKIE/ECHO Scanning
- **SSDP and List Scanning**
- **IPv6 Scanning**

Lab Tasks

TASK 1 — Perform Port and Service Discovery using MegaPing

Here, we will use the MegaPing tool to scan for open ports and services running on the target range of IP addresses.

1. Before beginning this lab, turn on the **Windows 10**, **Windows Server 2016**, **Parrot Security**, and **Ubuntu** virtual machines.

TASK 1.1

Install MegaPing

2. In the **Windows 10** virtual machine, log in with the credentials Username: **Admin** and Password: **Pa$$w0rd**.
3. Navigate to **E:\CEH-Tools\CEHv11 Module 03 Scanning Networks\Scanning Tools\MegaPing** and double-click **megaping_setup.exe**.

Note: If a **User Account Control** pop-up appears, click **Yes**.

4. The **MegaPing - InstallShield Wizard** window appears; click **Next** and follow the wizard-driven installation steps to install **MegaPing**.

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

MegaPing is a toolkit that provides essential utilities for Information System specialists, system administrators, IT solution providers, and individuals. It is used to detect live hosts and open ports of the system in the network, and 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, etc.

5. After the completion of the installation, click on the **Launch the program** checkbox and click **Finish**.

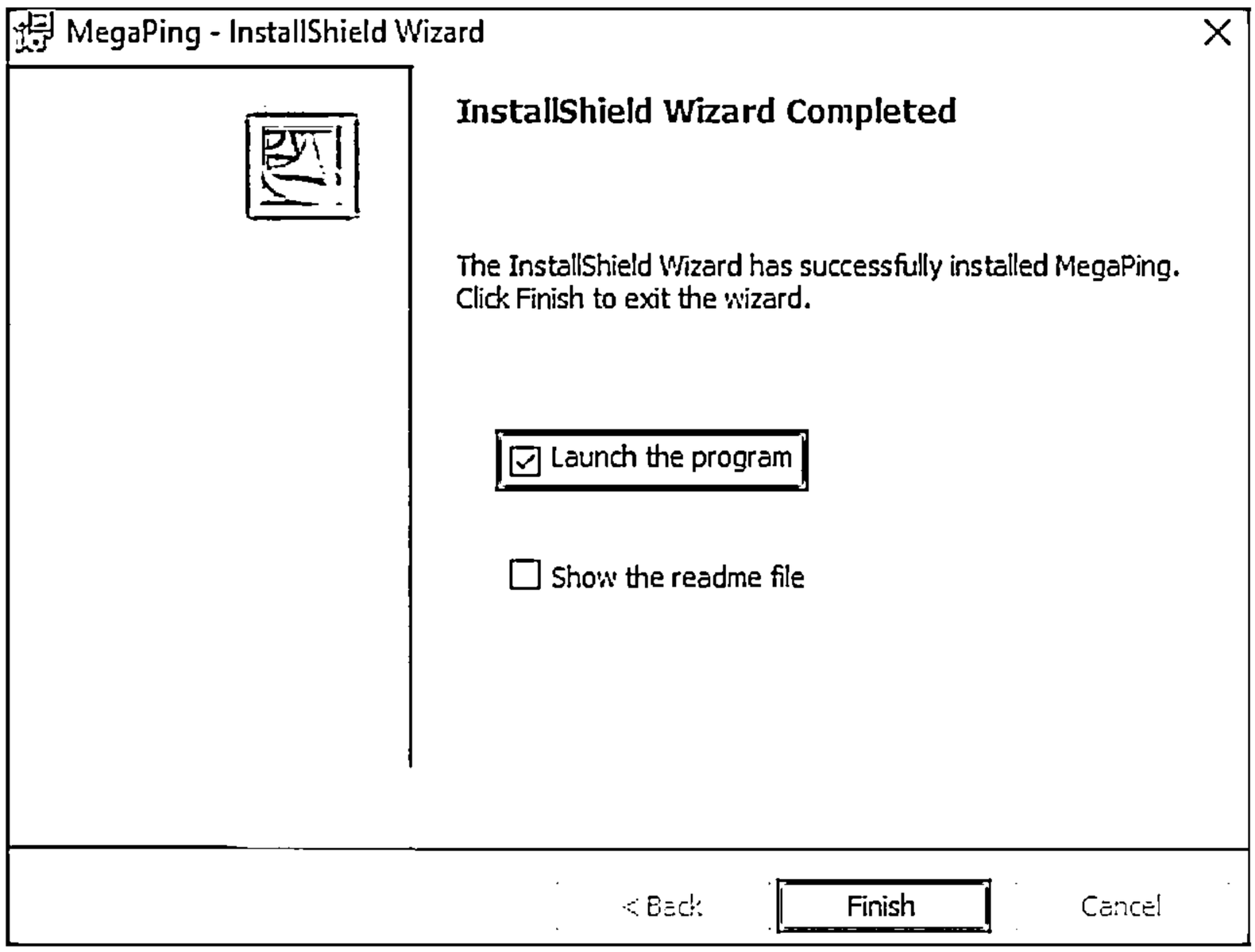


Figure 2.1.1: Launching MegaPing from Start menu

You can also perform various network troubleshooting activities with the help of integrated network utilities such as DNS lookup name, DNS list hosts, Finger, host monitor, IP scanner, NetBIOS scanner, ping, port scanner, share scanner, traceroute, and Whois.

6. The **About MegaPing** window appears; click the **I Agree** button.

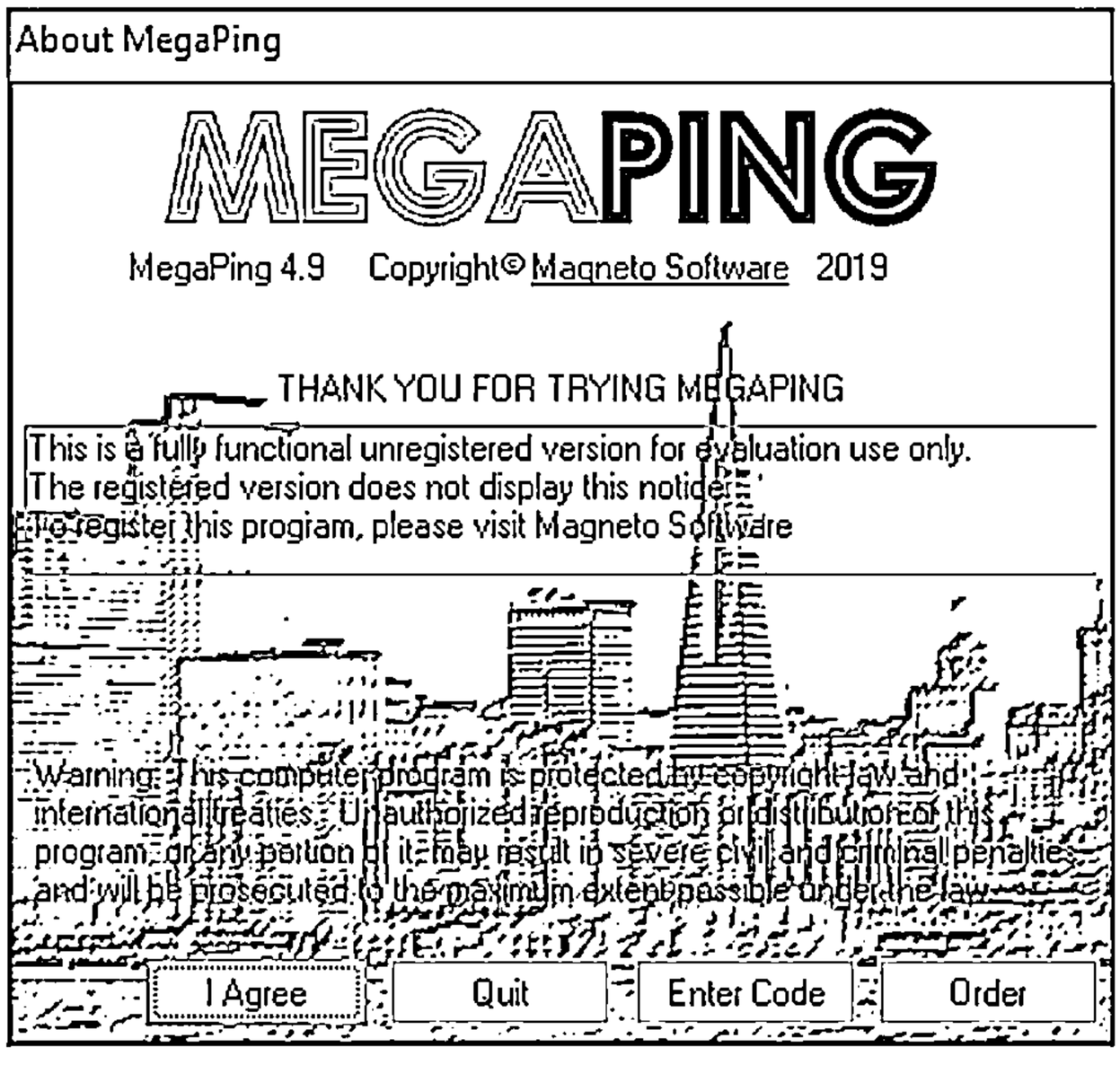


Figure 2.1.2: About MegaPing pop-up

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

7. The **MegaPing (Unregistered)** GUI appears displaying the **System Info**, as shown in the screenshot.

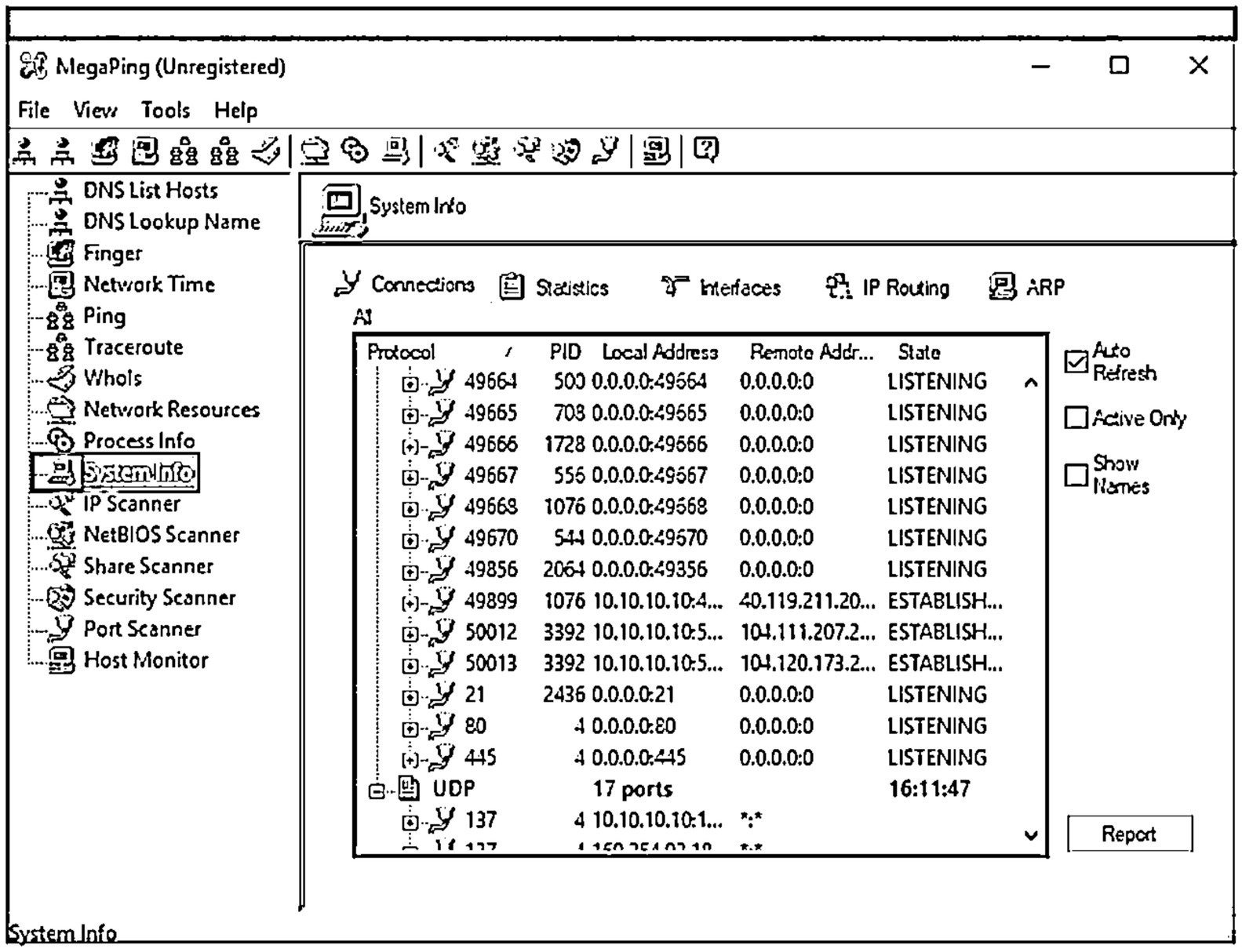


Figure 2.1.3: MegaPing GUI

TASK 1.2

Scan for Live Hosts

8. Select the **IP Scanner** option from the left pane. In the **IP Scanner** tab in the right-hand pane, enter the IP range in the **From** and **To** fields; in this lab, the IP range is **10.10.10.5** to **10.10.10.20**; then, click **Start**.

Note: You may specify the IP range depending on your network.

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

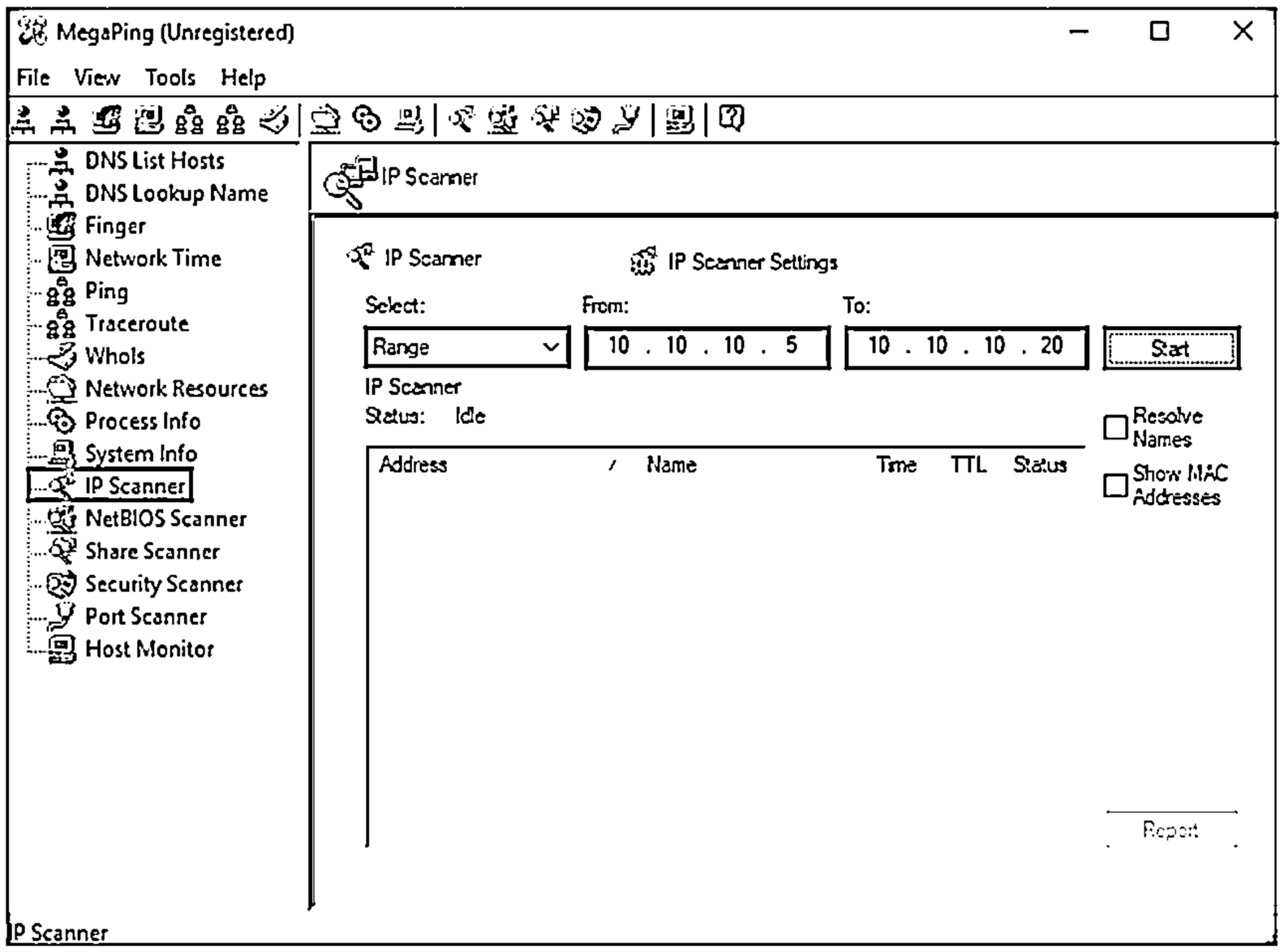


Figure 2.1.4: Configuring MegaPing

9. MegaPing lists all IP addresses under the specified target range with their TTL value, Status (dead or alive), and statistics of the dead and alive hosts, as shown in the screenshot.

Note: The results may vary in your lab environment.

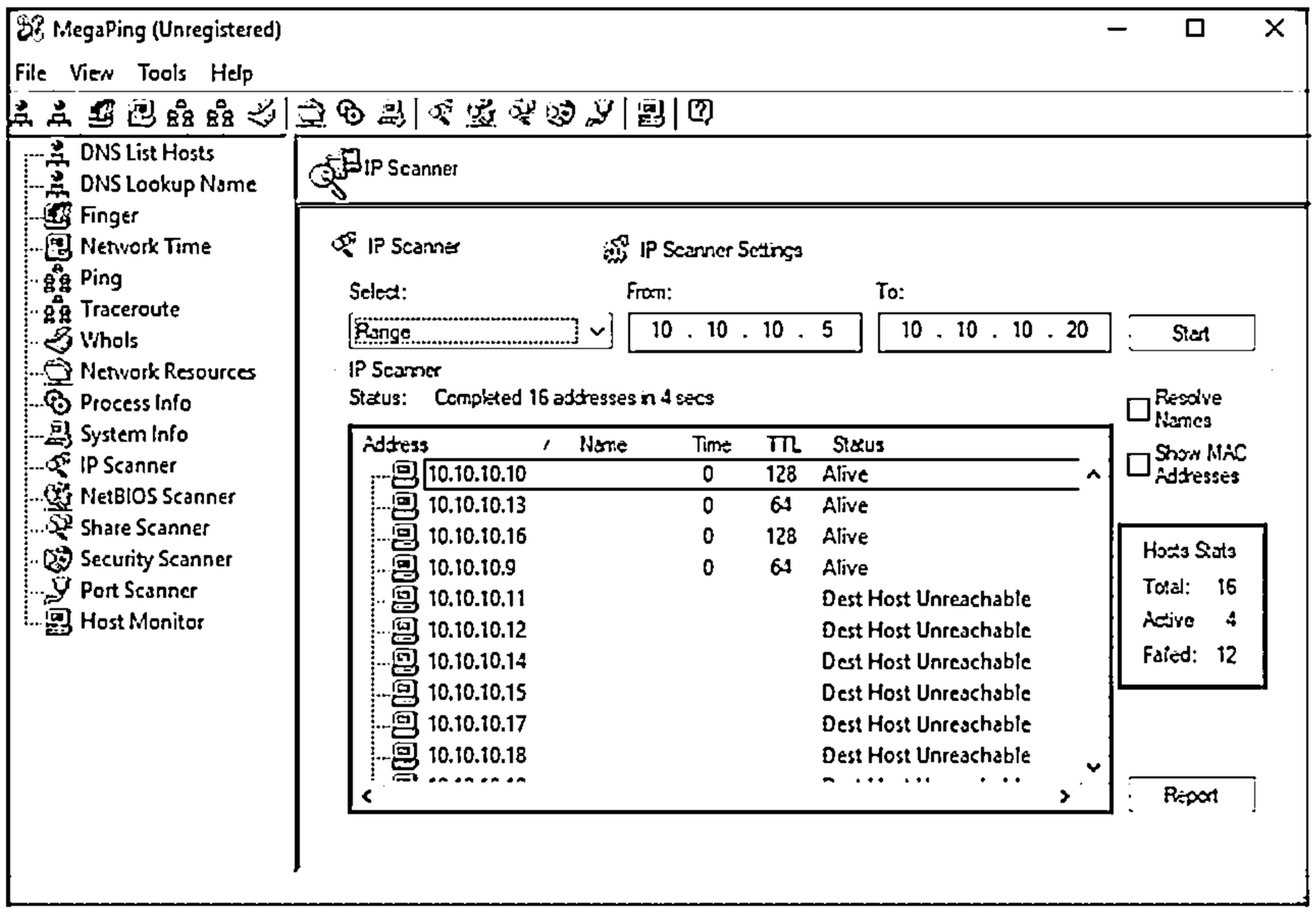


Figure 2.1.5: MegaPing IP Scanning Report

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

TASK 1.3

Perform Port Scan

10. Select the **Port Scanner** option from the left-hand pane. In the **Port Scanner** tab in the right-hand pane, enter the IP address of the **Windows Server 2016** (**10.10.10.16**) machine into the **Destination Address List** field and click **Add**.

Note: The IP address listed below might vary in your lab environment.

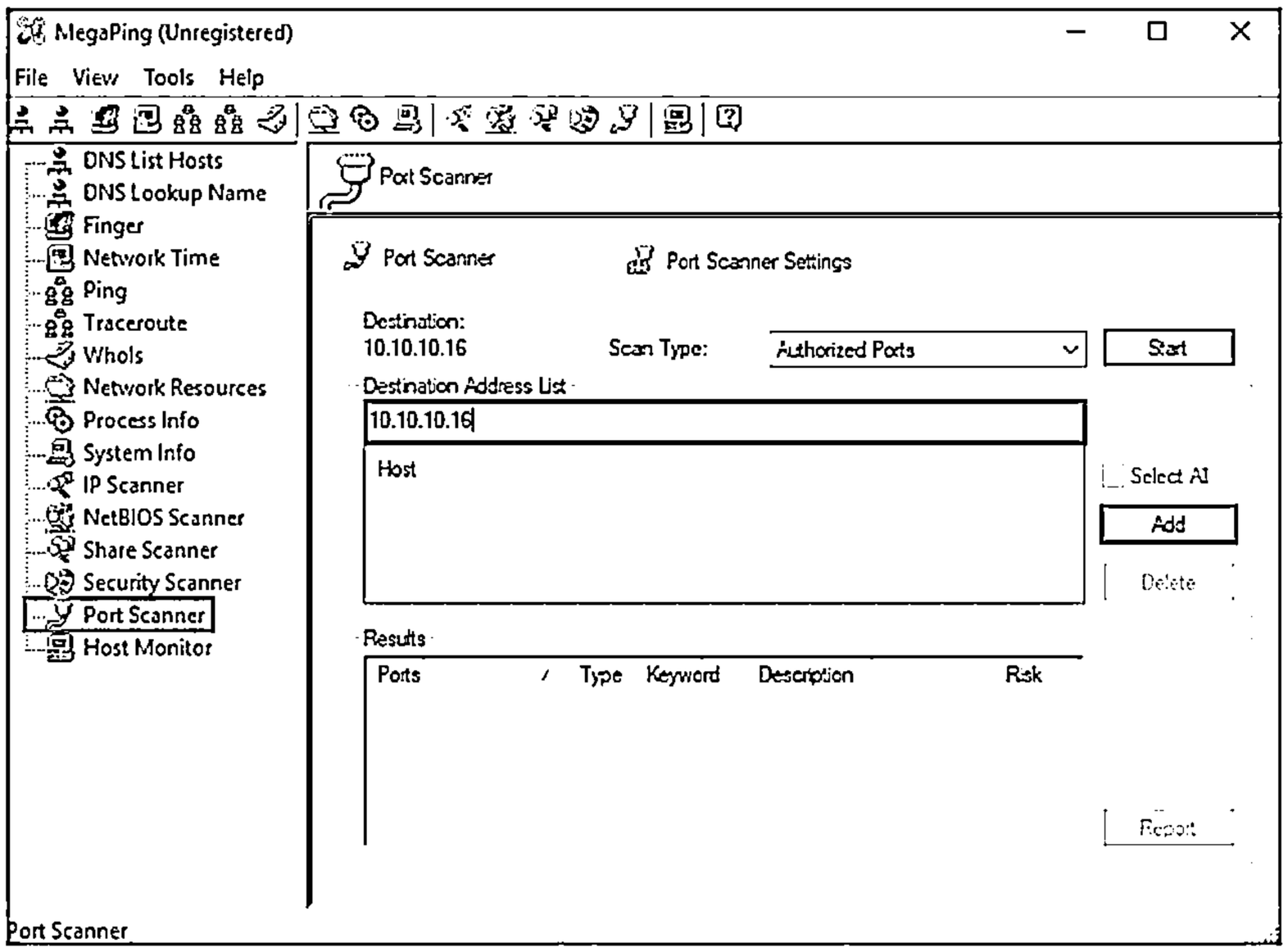


Figure 2.1.6: Adding a host in MegaPing

11. Select the **10.10.10.16** checkbox and click the **Start** button to start listening to the traffic on 10.10.10.16.

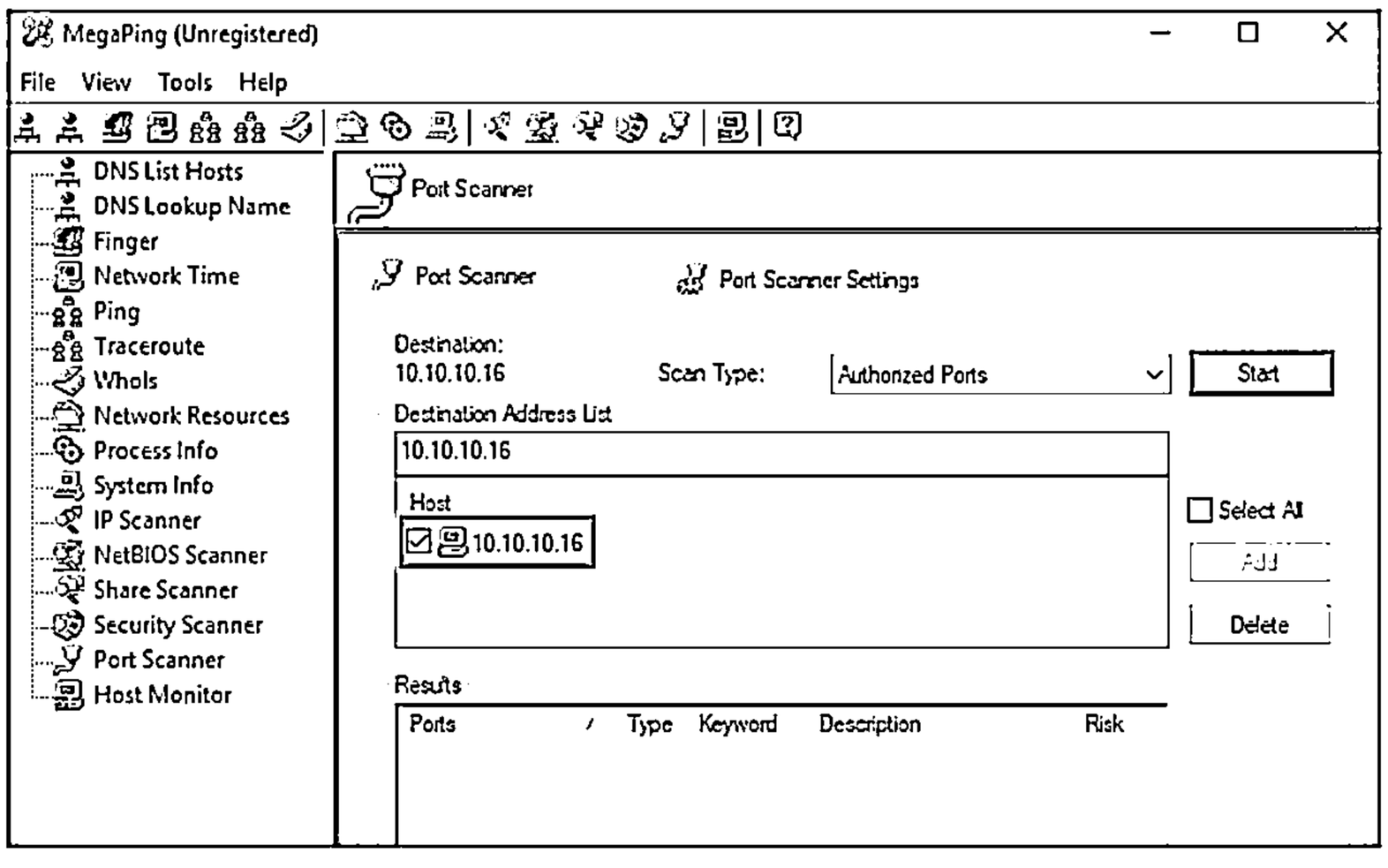


Figure 2.1.7: Starting MegaPing on the selected host

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

12. MegaPing lists the ports associated with **Windows Server 2016** (**10.10.10.16**), with detailed information on port number and type, service running on the port along with the description, and associated risk, as shown in the screenshot.

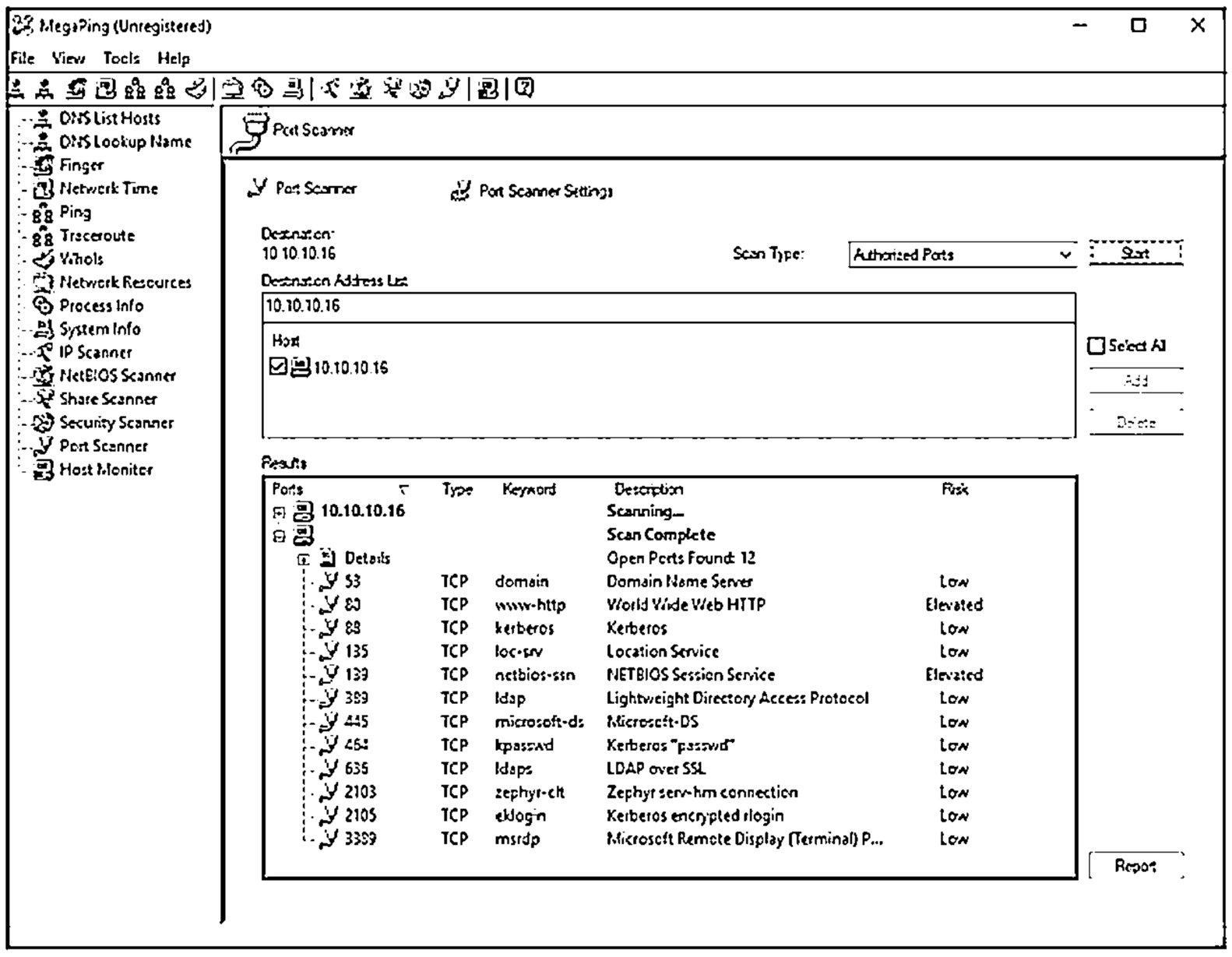


Figure 2.1.8: MegaPing Port Scanning Report

13. Similarly, you can perform port and service scanning on other target machines.

14. This concludes the demonstration of discovering open ports and services running on the target IP address using MegaPing.

15. Close all open windows and document all the acquired information.

TASK 2 Perform Port and Service Discovery using NetScanTools Pro

Here, we will use the NetScanTools Pro tool to discover open ports and services running on the target range of IP addresses.

TASK 2.1

Install NetScanTools Pro

1. In the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 03 Scanning Networks\Scanning Tools\NetScanTools Pro**, and double-click **nstp11demo.exe**.

Note: If a **User Account Control** pop-up appears, click **Yes**.

Note: If an **Open File - Security Warning** pop-up appears, click **Run**.

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

NetScanTools Pro is an integrated collection of utilities that gathers information on the Internet and troubleshoots networks for Network Professionals. With the available tools, you can research IPv4/IPv6 addresses, hostnames, domain names, e-mail addresses, and URLs on the target network.

2. The **Setup - NetScanTools Pro Demo** window appears; click **Next** and follow the wizard-driven installation steps to install **NetScanTools Pro**.

Note: If the **WinPcap Setup** window appears, click **Next** and install it.

3. After the completion of the installation, click **Finish**.

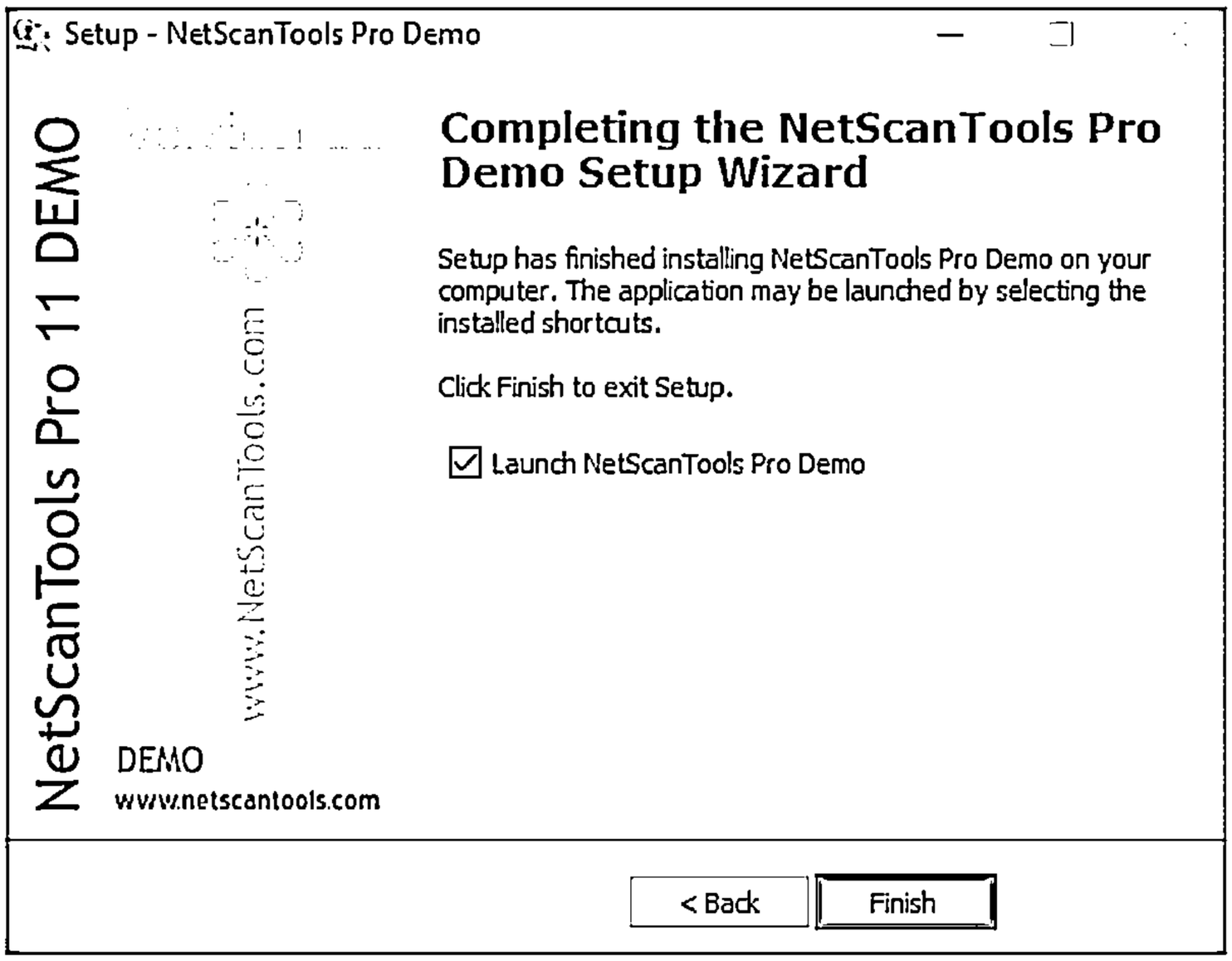


Figure 2.2.1: NetScanTools Setup window

4. The **Reminder** window appears; if you are using a demo version of NetScanTools Pro, click the **Start the DEMO** button.

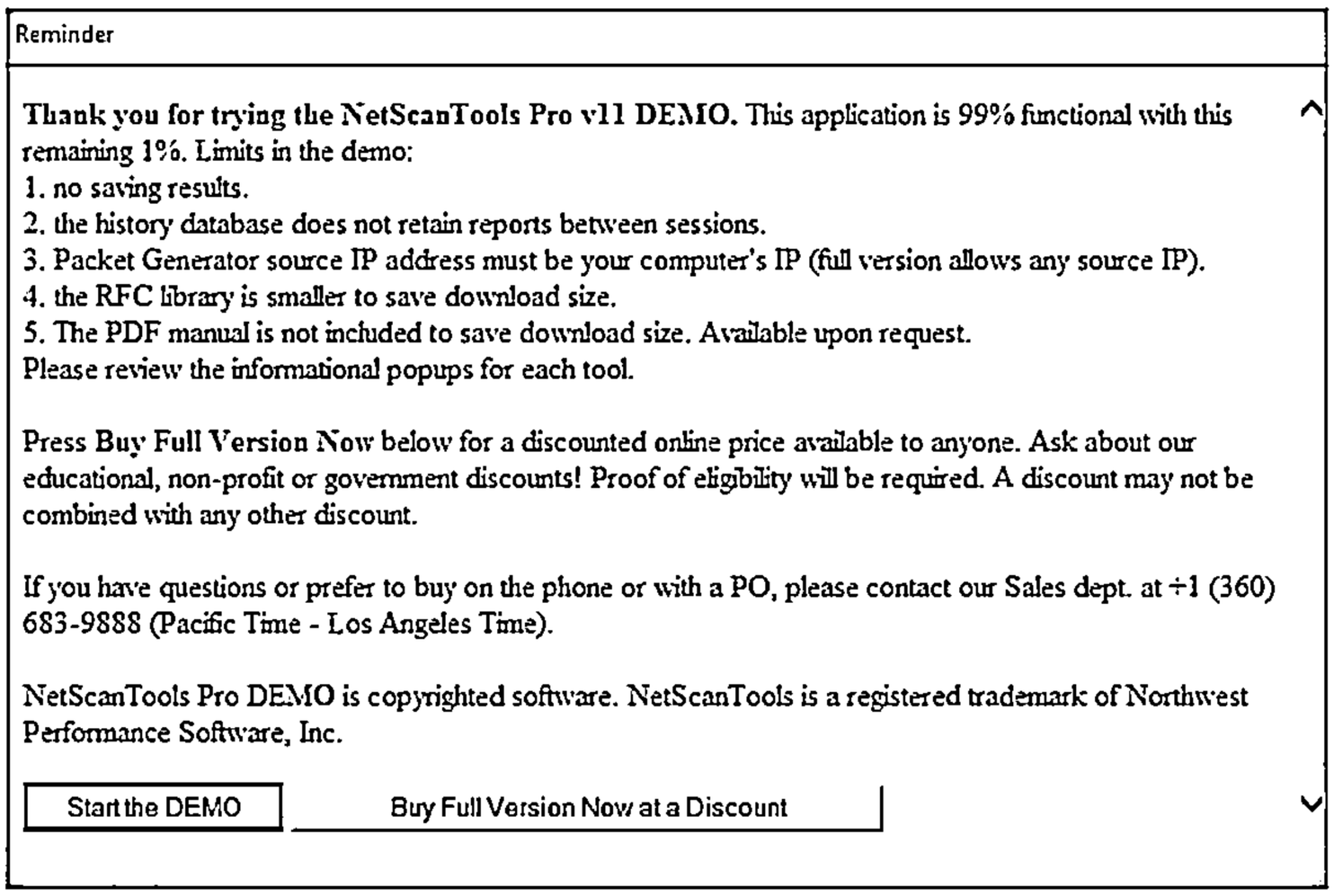


Figure 2.2.2: NetScan Tools Pro reminder window

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

5. A **DEMO Version** pop-up appears; click the **Start NetScanTools Pro Demo...** button.

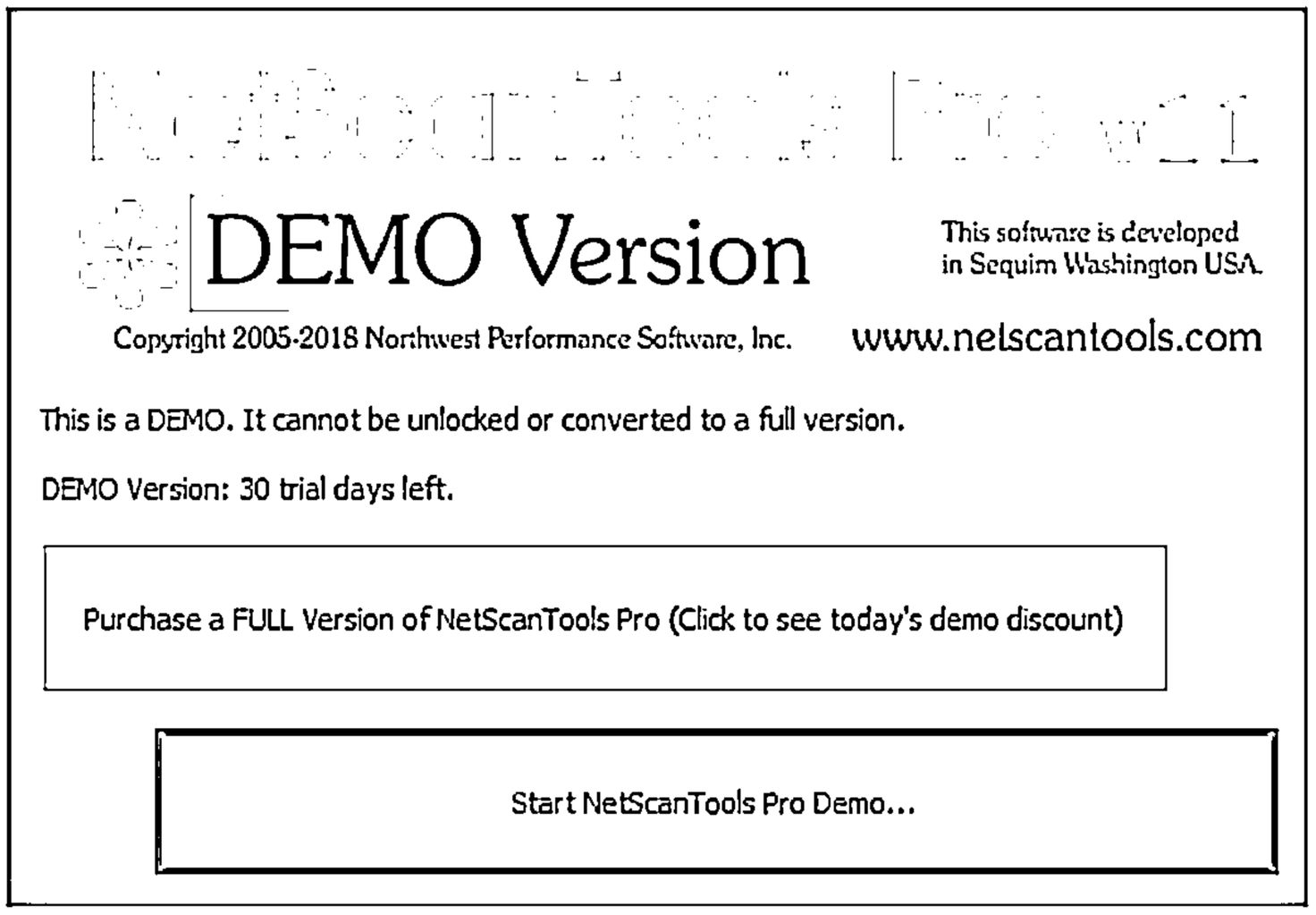


Figure 2.2.3: DEMO Version pop-up

6. The **NetScanTools Pro** main window appears, as shown in the screenshot.

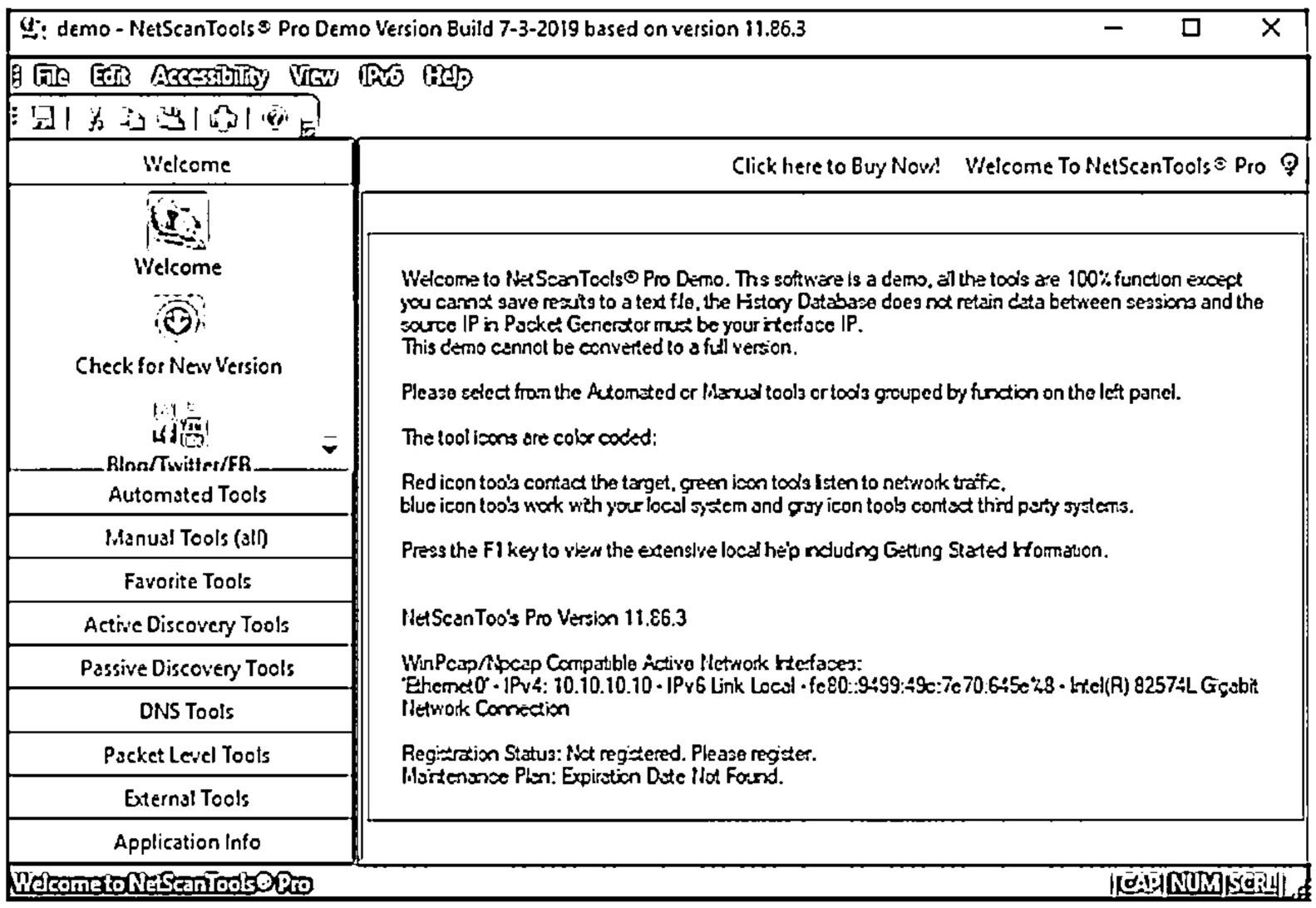


Figure 2.2.4: Main window of NetScan Tools Pro

TASK 2.2

Perform Ping Scan

7. In the left-hand pane, under the **Manual Tools (all)** section, scroll down and click the **Ping Scanner** option, as shown in the screenshot.

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

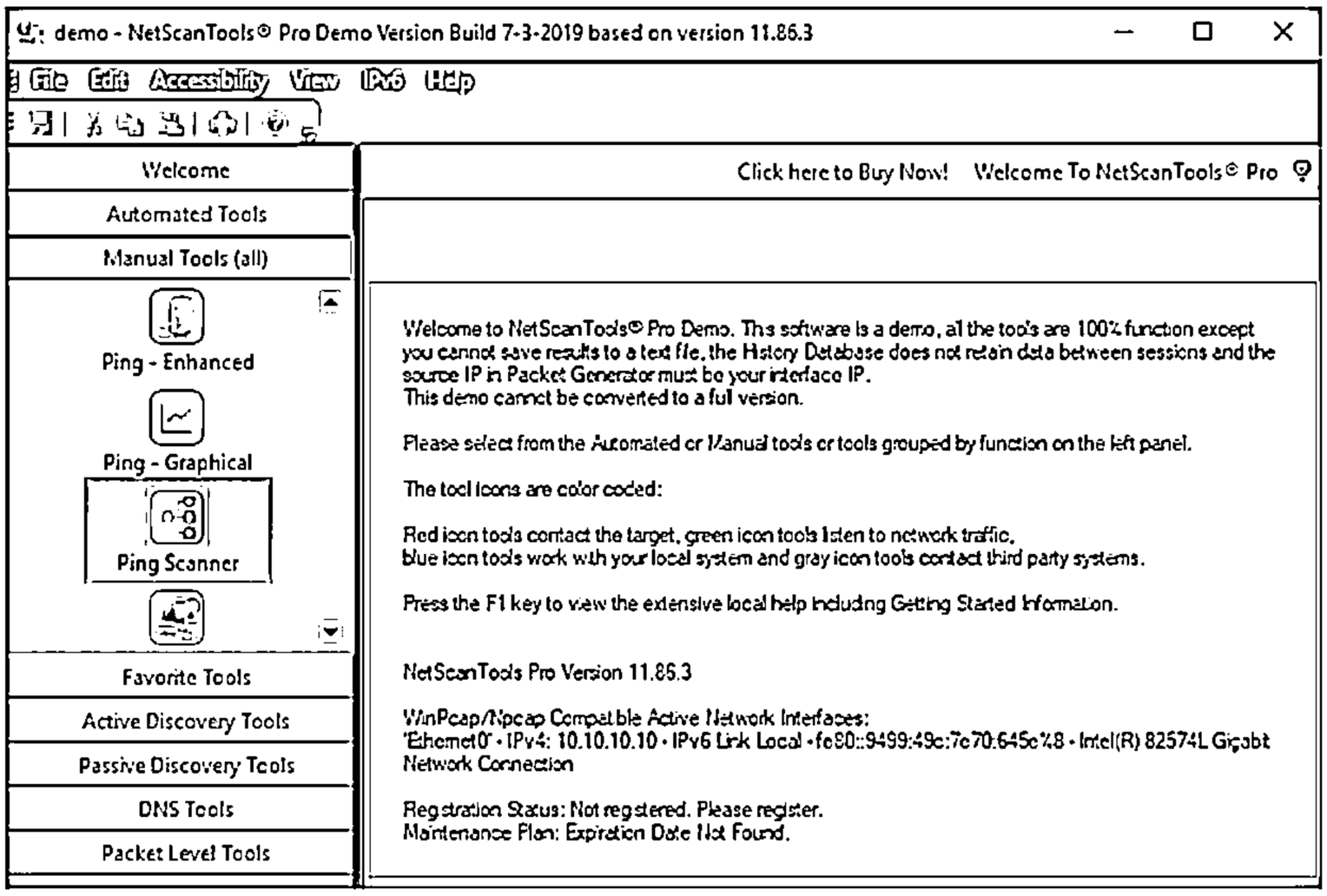


Figure 2.2.5: Selecting Ping Scanner option

8. A dialog box opens explaining the **Ping Scanner** tool; click **OK**.
9. Ensure that **Use Default System DNS** is selected. Enter the range of IP addresses into the **Start IP** and **End IP** fields (here, **10.10.10.5 - 10.10.10.20**); then, click **Start**.

Note: The IP address range might differ in your lab environment.

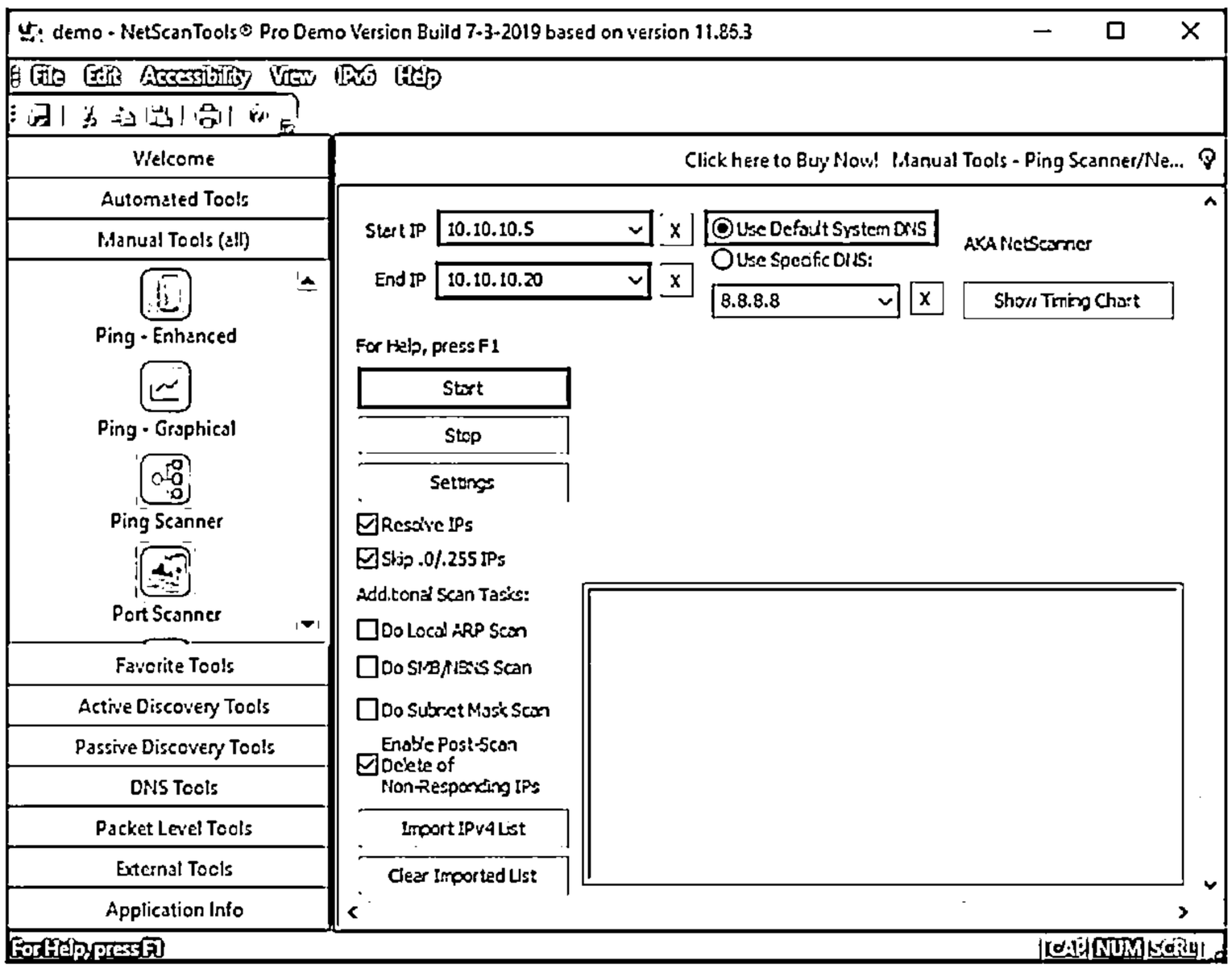


Figure 2.2.6: Configuring the Ping Scanner tool

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

10. A **Ping Scanner** notice pop-up appears; click **I Accept**.
11. After the completion of the scan, if a **How do you want to open this file?** pop-up appears, select any web browser (here, **Mozilla Firefox**) and click **OK**.

Note: If the browser opens automatically, skip to the next step.

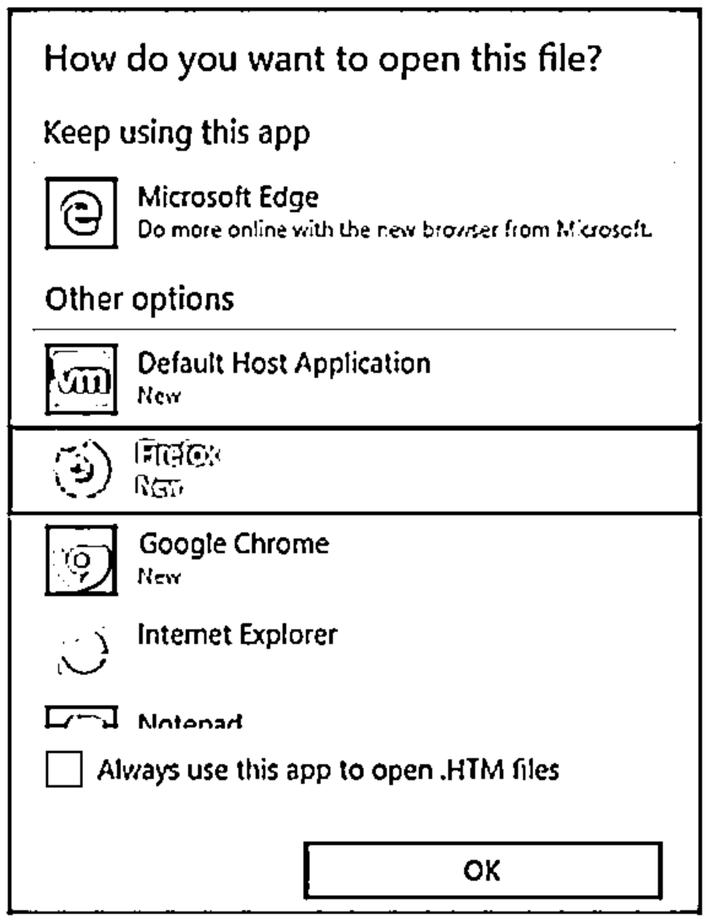
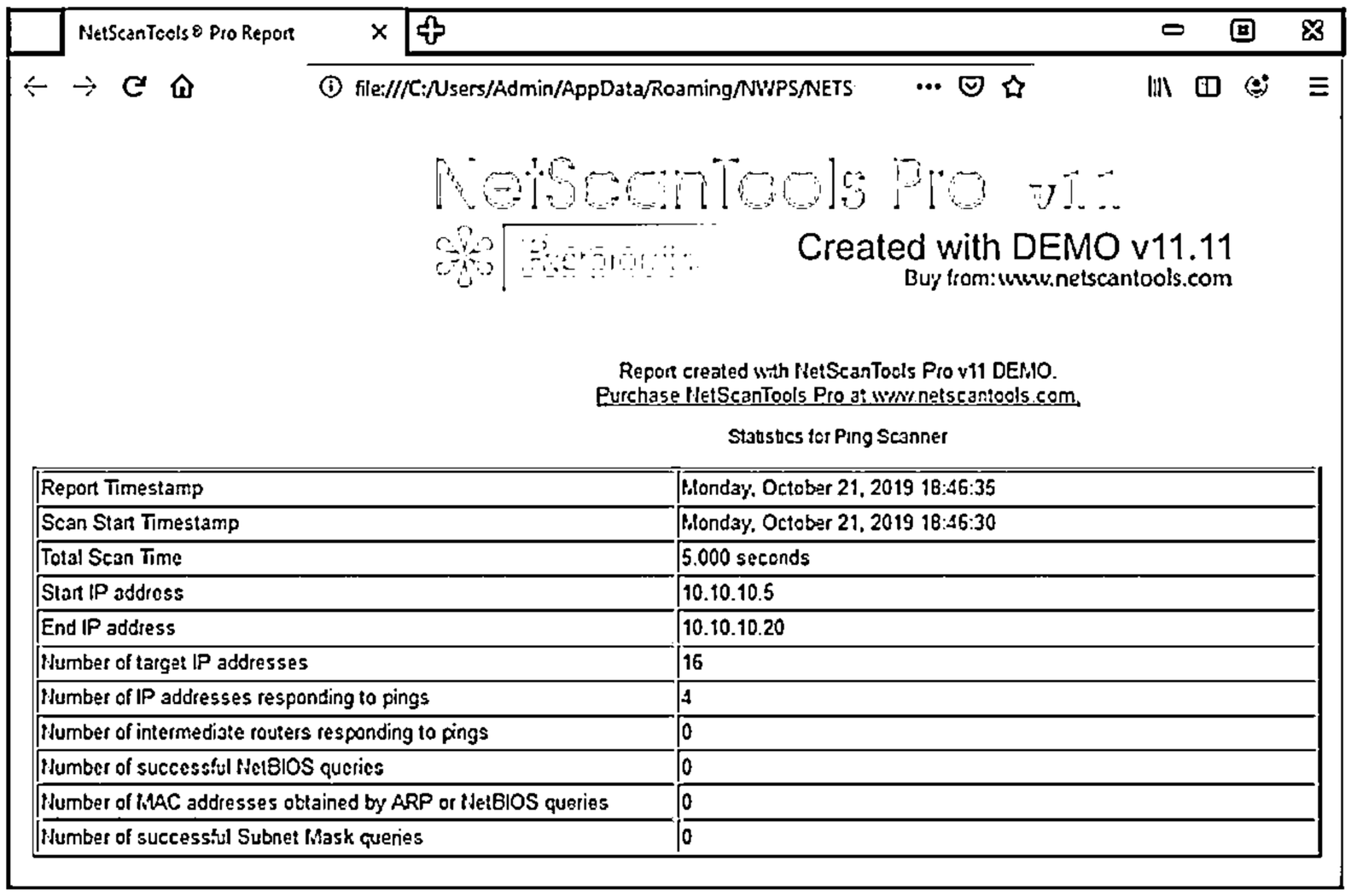


Figure 2.2.7: Choosing a browser to open the HTM file

12. A report appears in the browser displaying values such as **Start IP address, End IP address, Number of target IP addresses, Number of IP addresses responding to pings**, etc.

Note: The results might vary in your lab environment.



Report Timestamp	Monday, October 21, 2019 18:46:35
Scan Start Timestamp	Monday, October 21, 2019 18:46:30
Total Scan Time	5.000 seconds
Start IP address	10.10.10.5
End IP address	10.10.10.20
Number of target IP addresses	16
Number of IP addresses responding to pings	4
Number of intermediate routers responding to pings	0
Number of successful NetBIOS queries	0
Number of MAC addresses obtained by ARP or NetBIOS queries	0
Number of successful Subnet Mask queries	0

Figure 2.2.8: Browser displaying the scan report

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

TASK 2.3

Perform Port Scan

13. Close the browser and switch to the **NetScanTools Pro** window.
14. Now, click the **Port Scanner** option from the left-hand pane under the **Manual Tools (all)** section.

Note: If a dialog box appears explaining the **Port Scanner** tool, click **OK**.

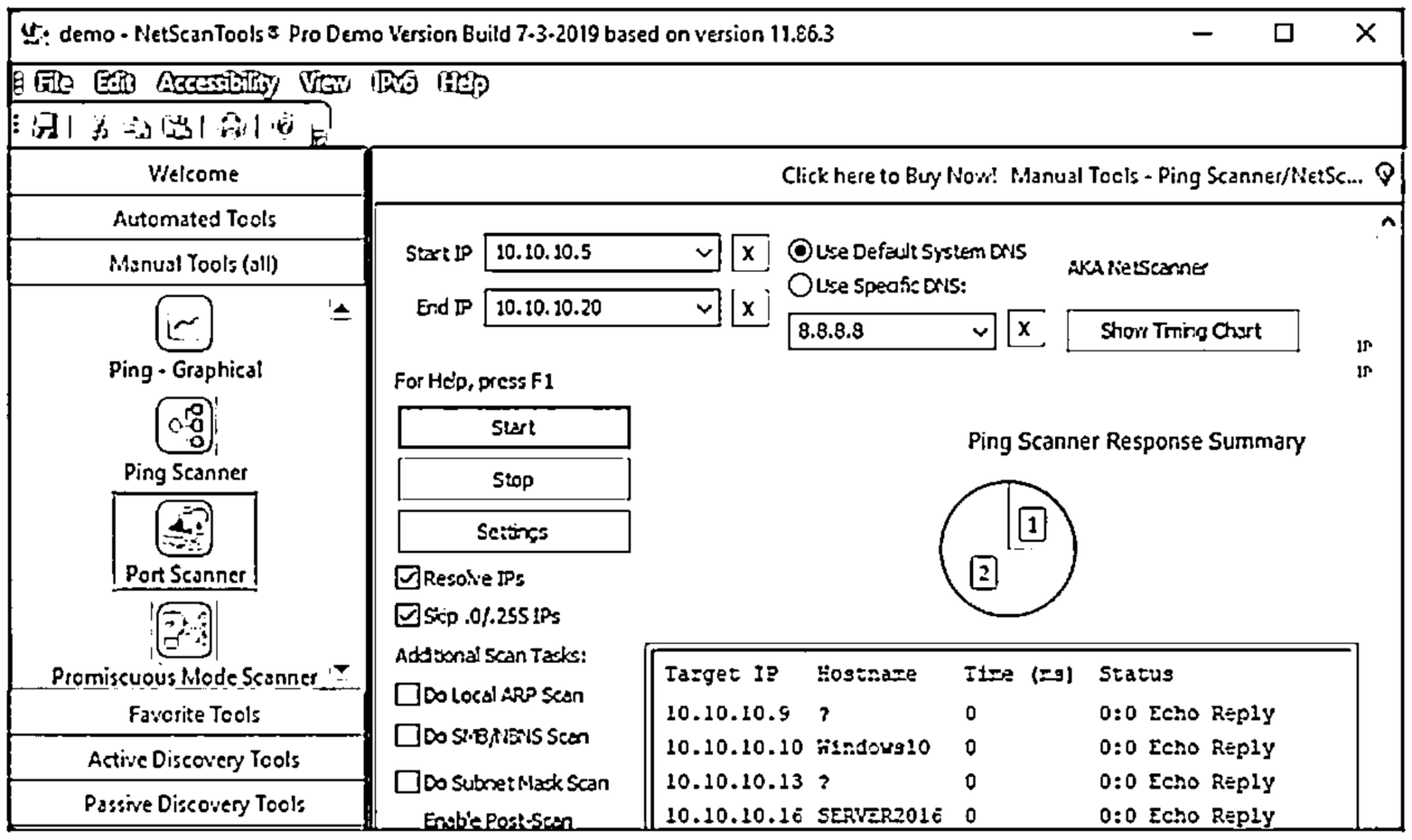


Figure 2.2.9: Selecting Port scanner option

15. In the **Target Hostname or IP Address** field, enter the IP address of the target (here, **10.10.10.16**). Ensure that **TCP Full Connect** is selected, and then click the **Scan Range of Ports** button.

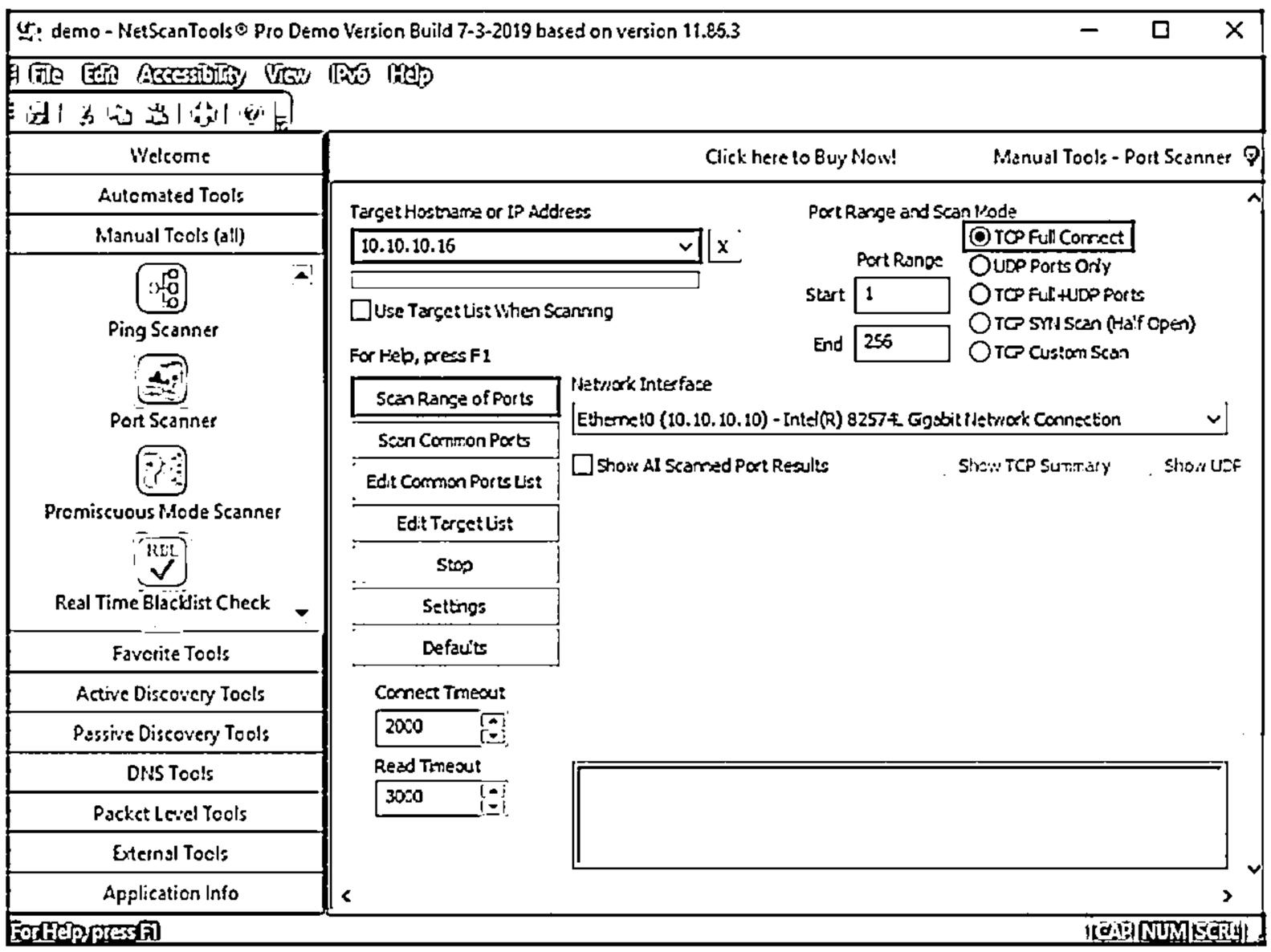


Figure 2.2.10: Configuring the Port Scanner tool

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

16. A **Port Scanner** notice pop-up appears; click **I Accept**.
17. A result appears displaying the active ports and their descriptions, as shown in the screenshot.

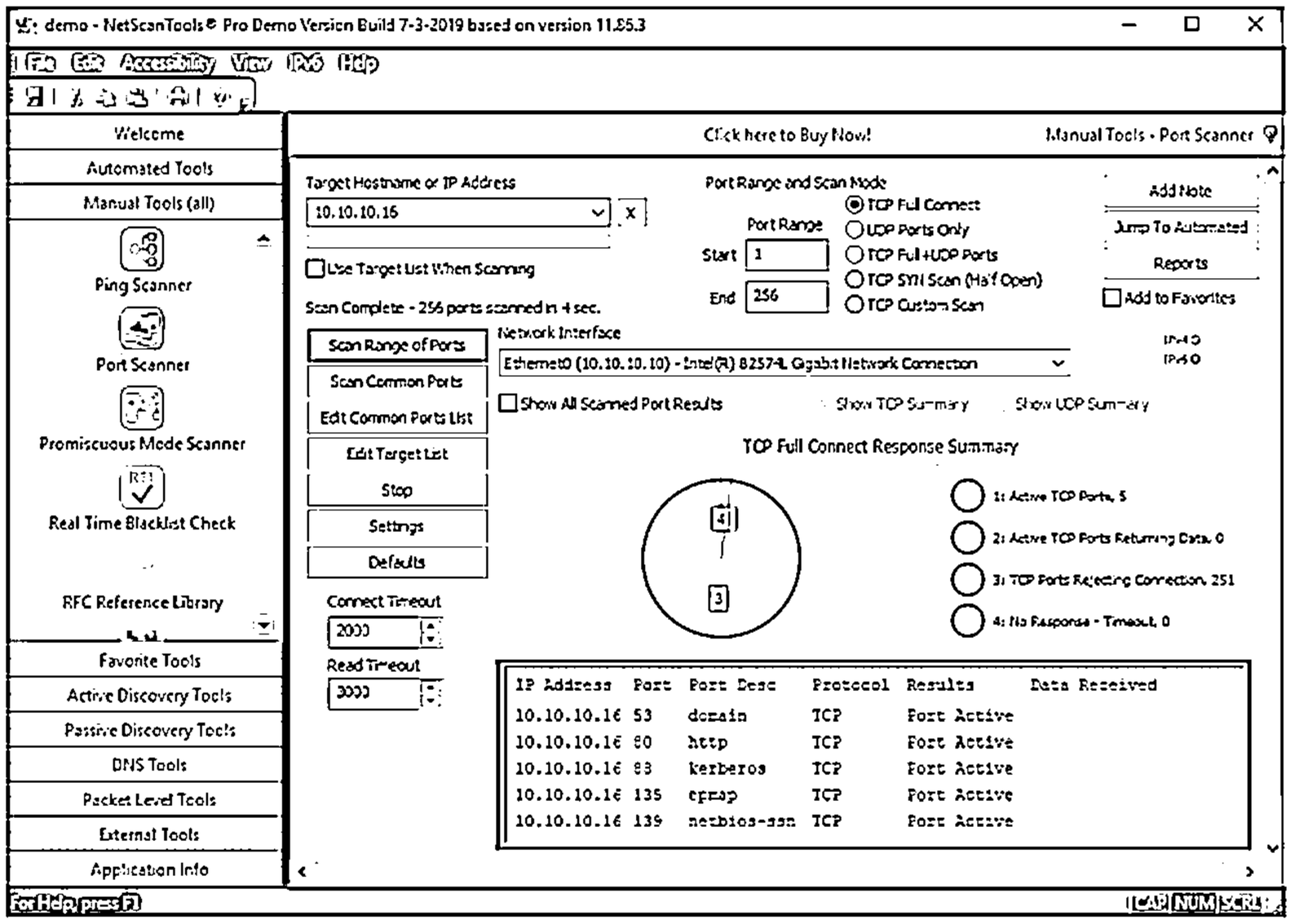


Figure 2.2.11: Port Scanner result

Note: By performing the above scans, you will be able to obtain a list of active machines in the network, their respective IP addresses and hostnames, and a list of all the open ports and services that will allow you to choose a target host in order to enter into its network and perform malicious activities such as ARP poisoning, sniffing, etc.

18. This concludes the demonstration of discovering open ports and services running on the target IP address using NetScanTools Pro.
19. Close all open windows and document all the acquired information.
20. Turn off the **Parrot Security** and **Ubuntu** virtual machines.

TASK 3 Explore Various Network Scanning Techniques using Nmap

Here, we will use Nmap to discover open ports and services running on the live hosts in the target network.

1. Before beginning this lab task, ensure that the **Windows Server 2016** virtual machine is turned on.

Note: In this lab task, we are using **Windows Server 2016** as a target machine.

2. In the **Windows 10** virtual machine, click on the **Start** menu and launch the **Nmap - Zenmap GUI** from the applications.

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

TASK 3.1

Perform TCP Connect/Full Open Scan

Nmap comes with various inbuilt scripts that can be employed during a scanning process in an attempt to find the open ports and services running on the ports. It sends specially crafted packets to the target host, and then analyzes the responses to accomplish its goal. Nmap includes many port scanning mechanisms (TCP and UDP), OS detection, version detection, ping sweeps, etc.

3. The **Nmap - Zenmap** GUI appears; in the **Command** field, type the command **nmap -sT -v <Target IP Address>** (here, the target IP address is **10.10.10.16**) and click **Scan**.

Note: **-sT**: performs the TCP connect/full open scan and **-v**: enables the verbose output (include all hosts and ports in the output).

4. The scan results appear, displaying all the open TCP ports and services running on the target machine, as shown in the screenshot.

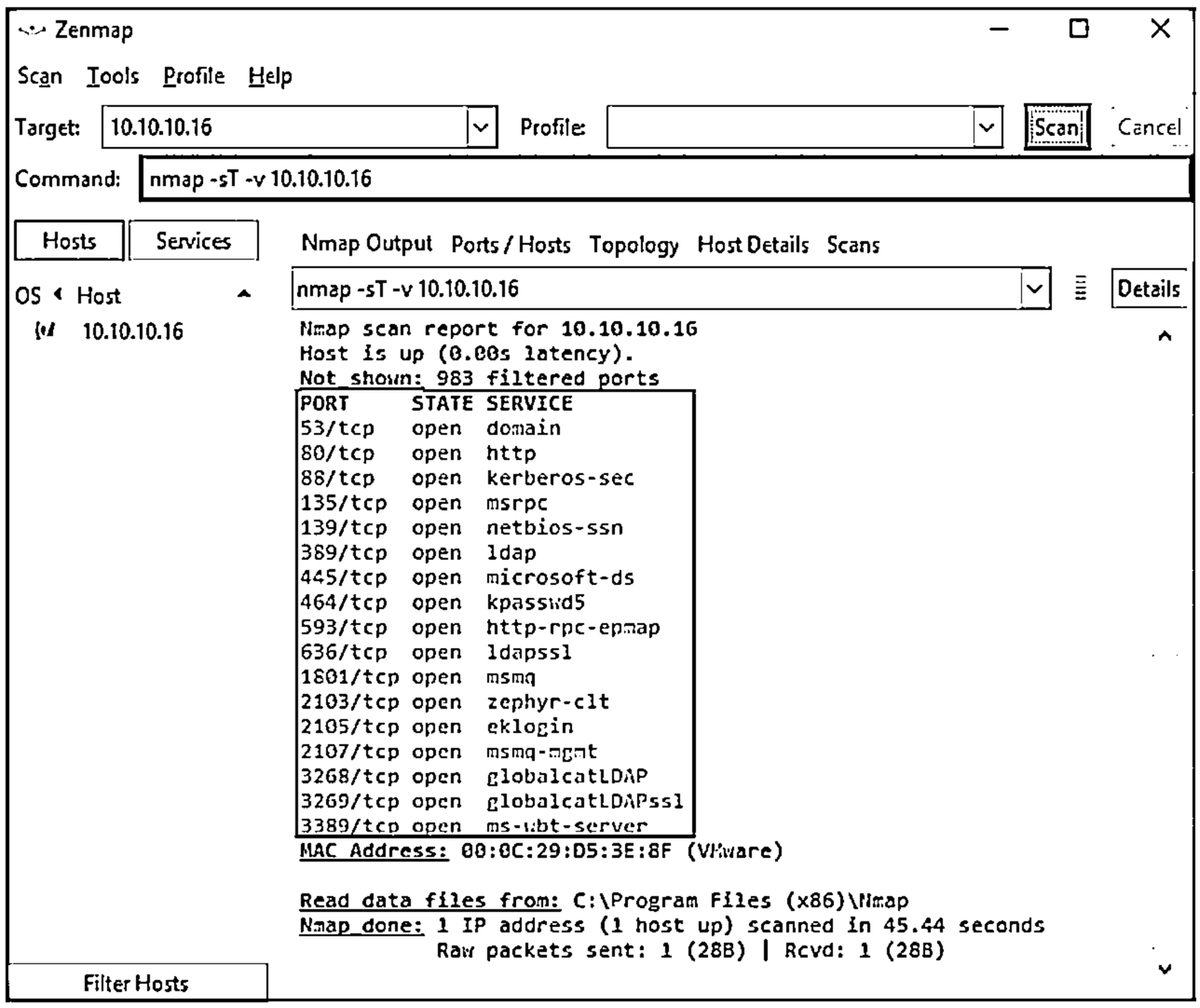


Figure 2.3.1: Zenmap scan results for TCP connect scan

Note: TCP connect scan completes a three-way handshake with the target machine. In the TCP three-way handshake, the client sends a SYN packet, which the recipient acknowledges with the SYN+ACK packet. In turn, the client acknowledges the SYN+ACK packet with an ACK packet to complete the connection. Once the handshake is completed, the client sends an RST packet to end the connection.

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

5. Click the **Ports/Hosts** tab to gather more information on the scan results. Nmap displays the Port, Protocol, State, Service, and Version of the scan.

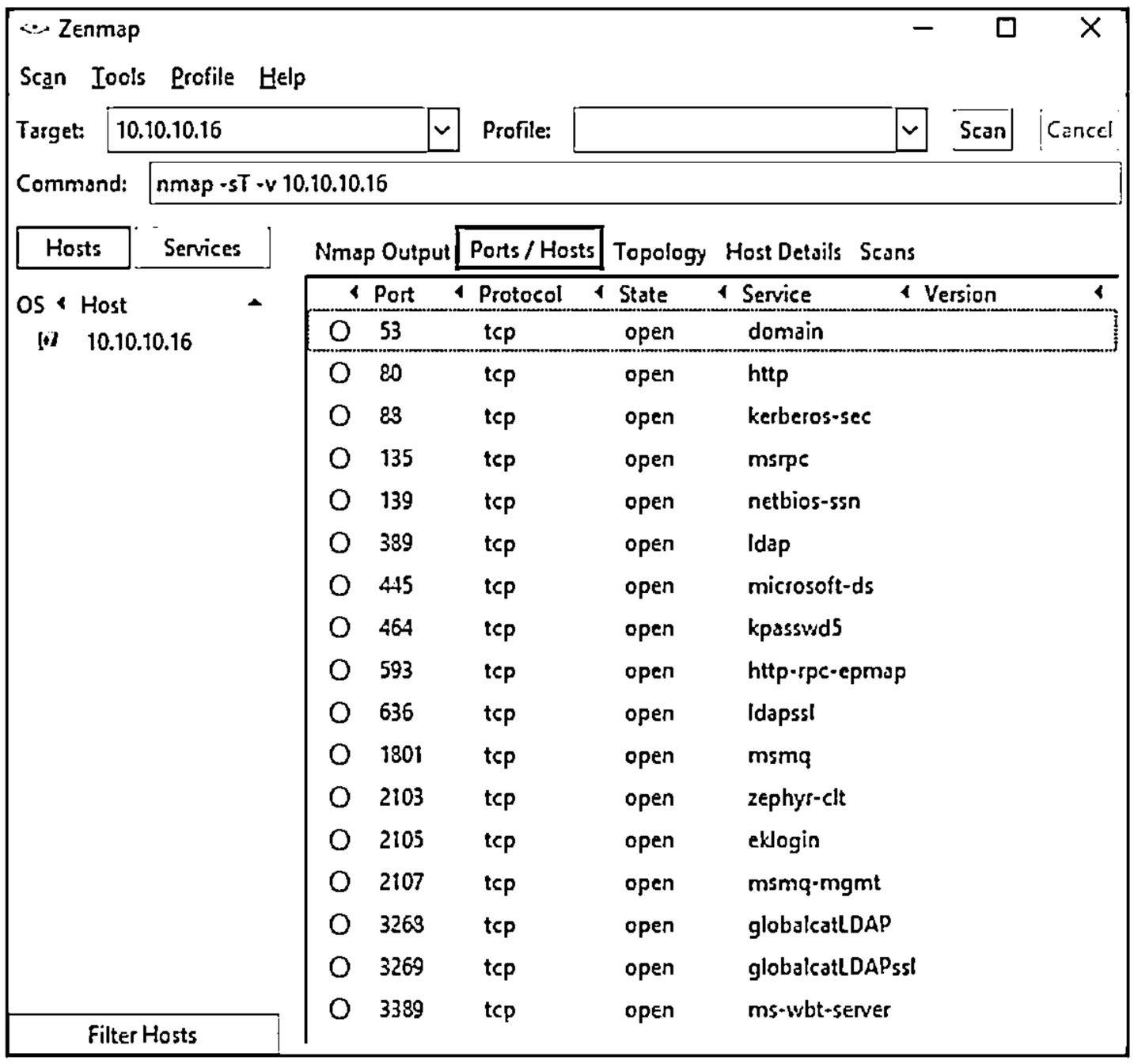


Figure 2.3.2: Zenmap Ports / Hosts tab

6. Click the **Topology** tab to view the topology of the target network that contains the provided IP address and click the **Fisheye** option to view the topology clearly.

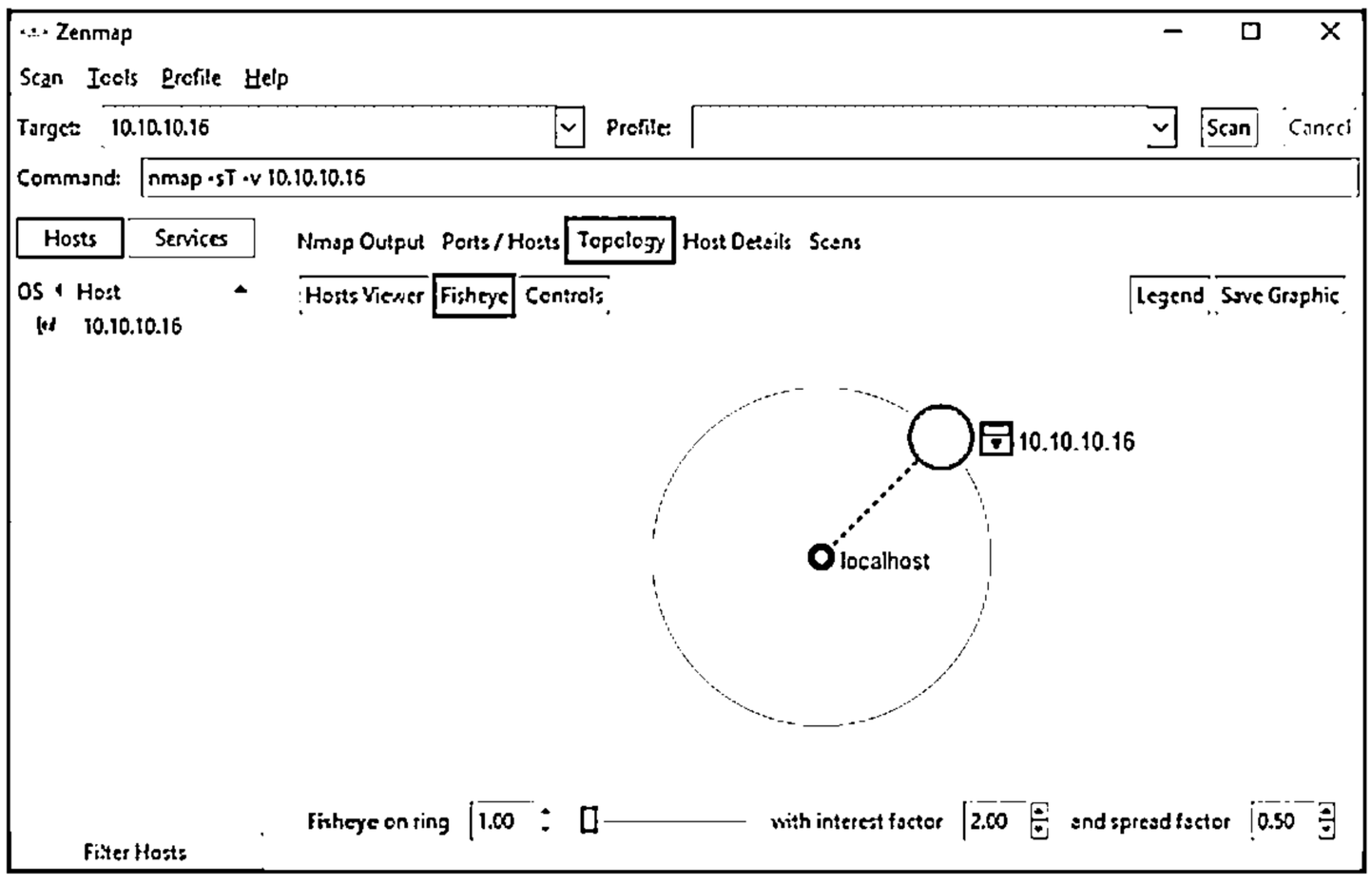


Figure 2.3.3: Zenmap displaying topology of the selected target

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

7. In the same way, click the **Host Details** tab to view the details of the TCP connect scan.
8. Click the **Scans** tab to view the command used to perform TCP connect/full open scan.
9. Click the **Services** tab located in the right pane of the window. This tab displays a list of services.

Note: You can use any of these services and their open ports to enter into the target network/host and establish a connection.

10. In this lab, we shall be performing a stealth scan/TCP half-open scan, Xmas scan, TCP Maimon scan, and ACK flag probe scan on a firewall-enabled machine (i.e., **Windows Server 2016**) in order to observe the result. To do this, we need to enable **Windows Firewall** in the **Windows Server 2016** virtual machine.
11. Switch to the **Windows Server 2016** virtual machine and log in with the credentials **Administrator/Pa$$w0rd**.
12. Navigate to **Control Panel → System and Security → Windows Firewall → Turn Windows Firewall on or off**, enable Windows Firewall and click **OK**, as shown in the screenshot.

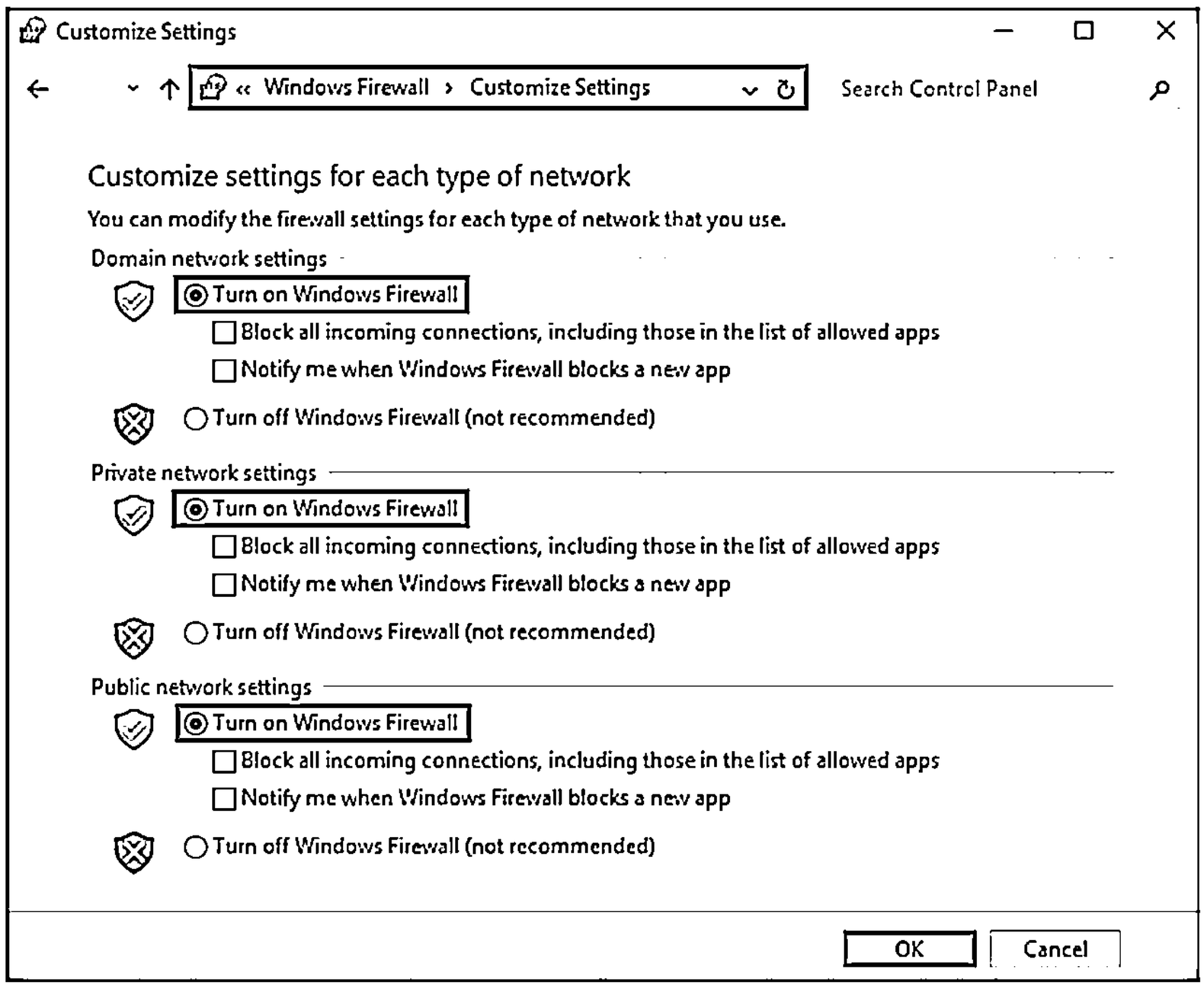


Figure 2.3.4: Turn on Windows Firewall

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

TASK 3.2

Perform Stealth Scan/TCP Half Open Scan

13. Now, switch to the **Windows 10** virtual machine. In the **Command** field of **Zenmap**, type the command **nmap -sS -v <Target IP Address>** (here, the target IP address is **10.10.10.16**) and click **Scan**.

Note: **-sS**: performs the stealth scan/TCP half-open scan and **-v**: enables the verbose output (include all hosts and ports in the output).

14. The scan results appear, displaying all open TCP ports and services running on the target machine, as shown in the screenshot.

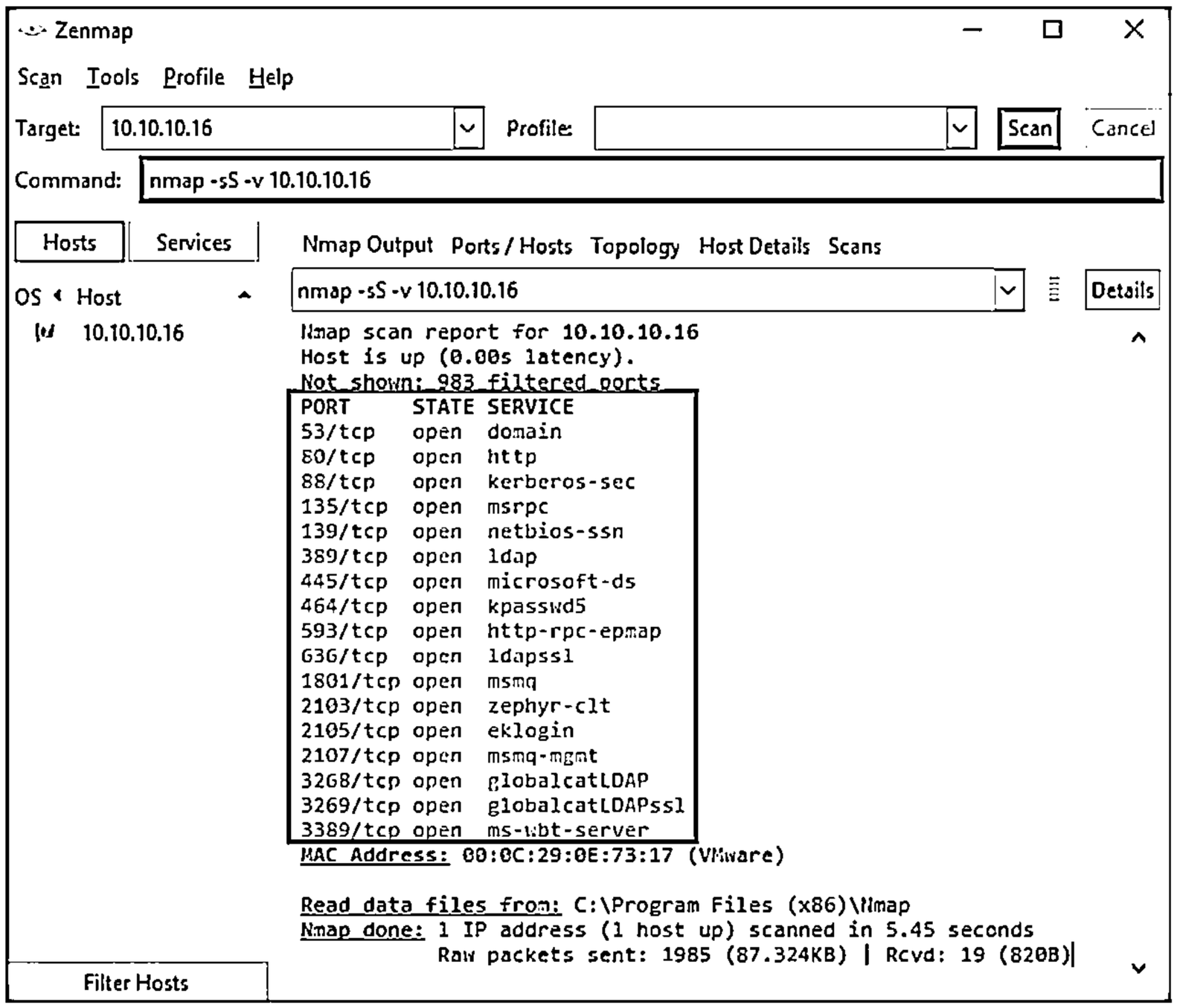


Figure 2.3.5: Zenmap scan results for Stealth scan

Note: The stealth scan involves resetting the TCP connection between the client and server abruptly before completion of three-way handshake signals, and hence leaving the connection half-open. This scanning technique can be used to bypass firewall rules, logging mechanisms, and hide under network traffic.

15. As shown in the last task, you can gather detailed information from the scan result in the **Ports/Hosts**, **Topology**, **Host Details**, and **Scan** tab.

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

TASK 3.3

Perform Xmas Scan

16. In the **Command** field of **Zenmap**, type the command **nmap -sX -v <Target IP Address>** (here, the target IP address is **10.10.10.16**) and click **Scan**.

Note: **-sX**: performs the Xmas scan and **-v**: enables the verbose output (include all hosts and ports in the output).

17. The scan results appear, displaying that the ports are either open or filtered on the target machine, which means a firewall has been configured on the target machine.

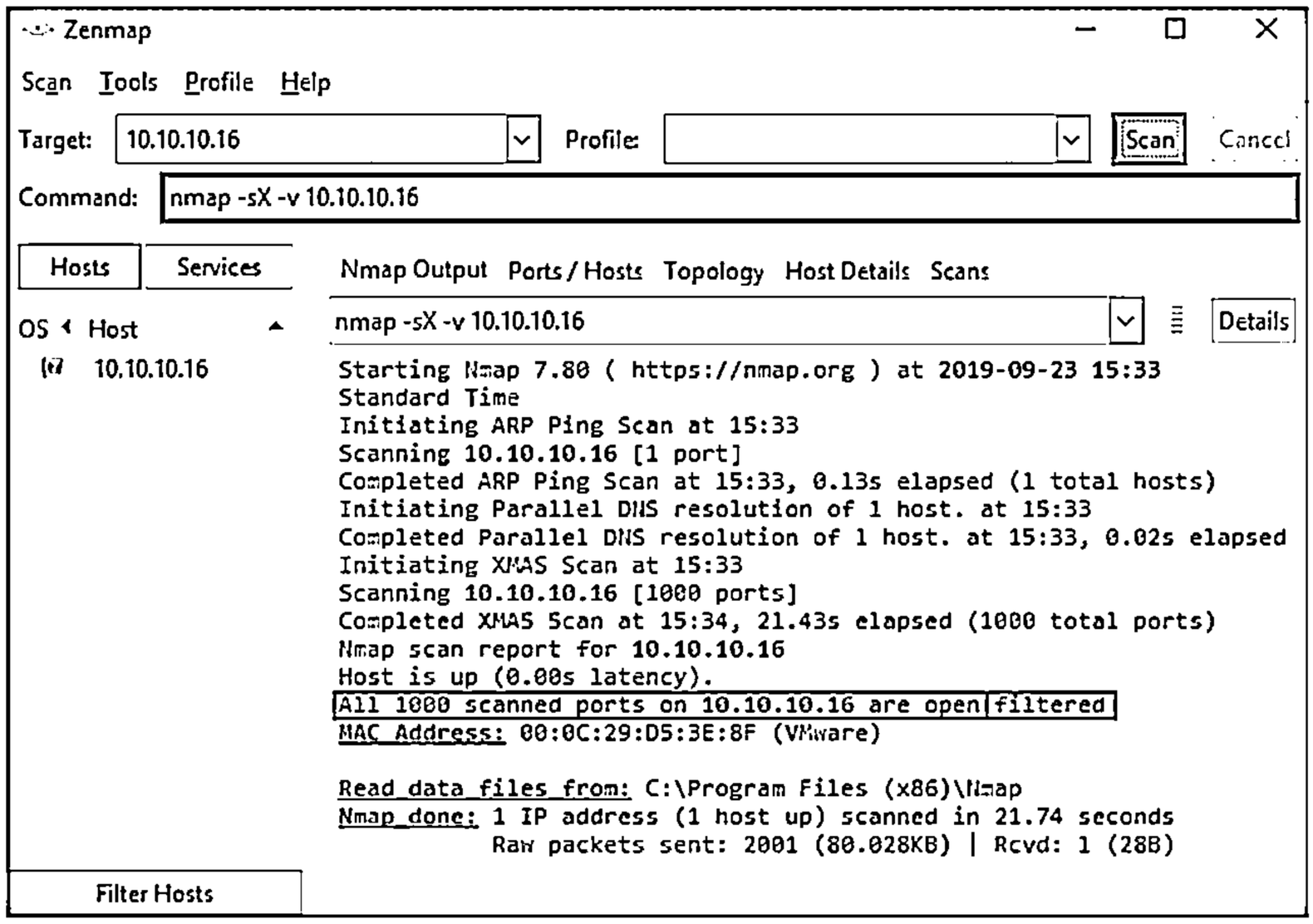


Figure 2.3.6: Zenmap scan results for Xmas scan

Note: Xmas scan sends a TCP frame to a target system with FIN, URG, and PUSH flags set. If the target has opened the port, then you will receive no response from the target system. If the target has closed the port, then you will receive a target system reply with an RST.

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

TASK 3.4

Perform TCP Maimon Scan

18. In the **Command** field, type the command **nmap -sM -v <Target IP Address>** (here, the target IP address is **10.10.10.16**) and click **Scan**

Note: **-sM**: performs the TCP Maimon scan and **-v**: enables the verbose output (include all hosts and ports in the output).

19. The scan results appear, displaying either the ports are open/filtered on the target machine, which means a firewall has been configured on the target machine.

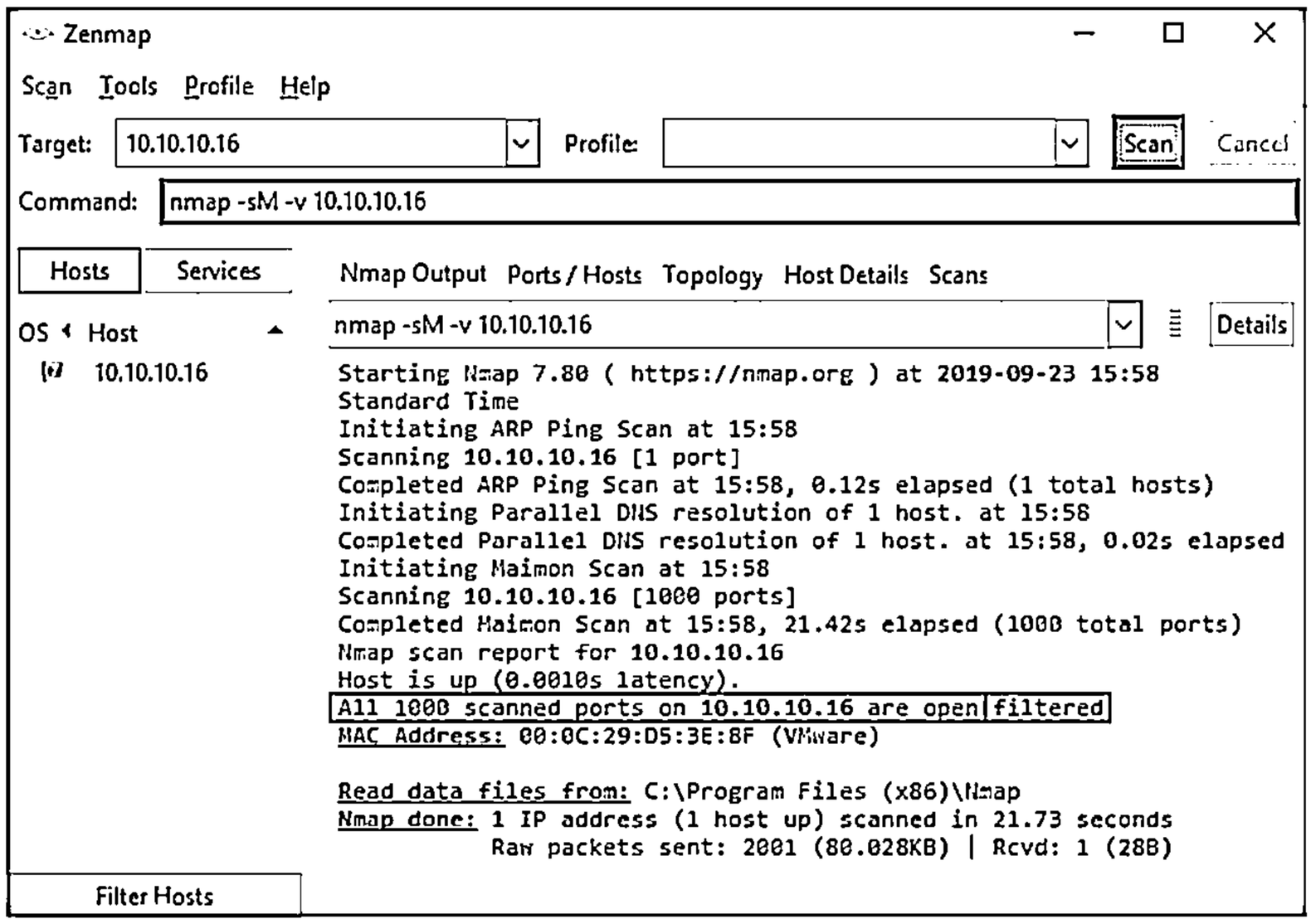


Figure 2.3.7: Zenmap scan results for Stealth scan

Note: In the TCP Maimon scan, a FIN/ACK probe is sent to the target; if there is no response, then the port is Open|Filtered, but if the RST packet is sent as a response, then the port is closed.

TASK 3.5

Perform ACK Flag Probe Scan

20. In the **Command** field, type the command **nmap -sA -v <Target IP Address>** (here, the target IP address is **10.10.10.16**) and click **Scan**.

Note: **-sA**: performs the ACK flag probe scan and **-v**: enables the verbose output (include all hosts and ports in the output).

21. The scan results appear, displaying that the ports are unfiltered on the target machine, as shown in the screenshot.

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

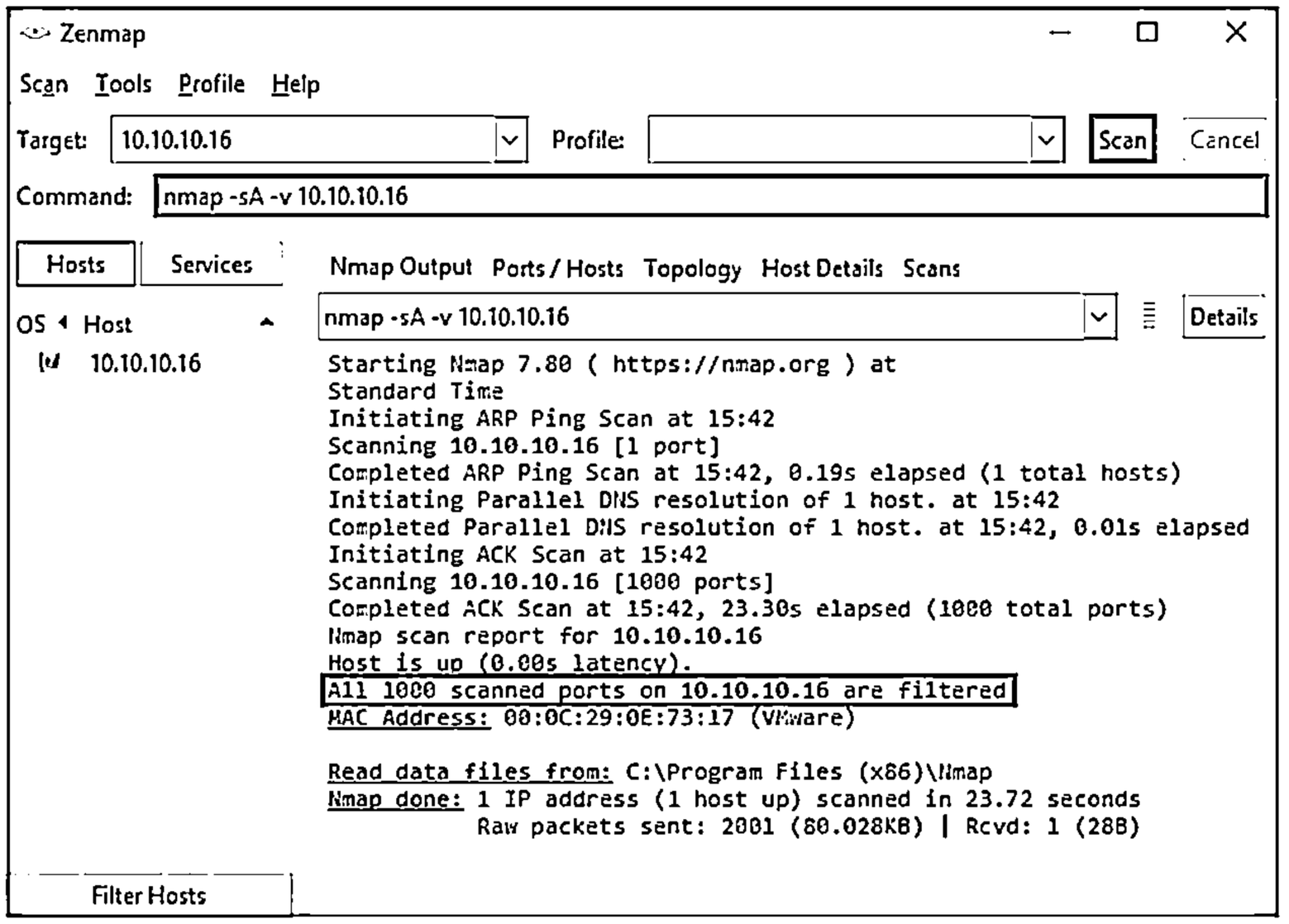


Figure 2.3.8: Zenmap scan results for Stealth scan

Note: The ACK flag probe scan sends an ACK probe packet with a random sequence number; no response implies that the port is filtered (stateful firewall is present), and an RST response means that the port is not filtered.

22. Now, switch to the **Windows Server 2016** virtual machine and turn off the **Windows Firewall** from **Control Panel**.

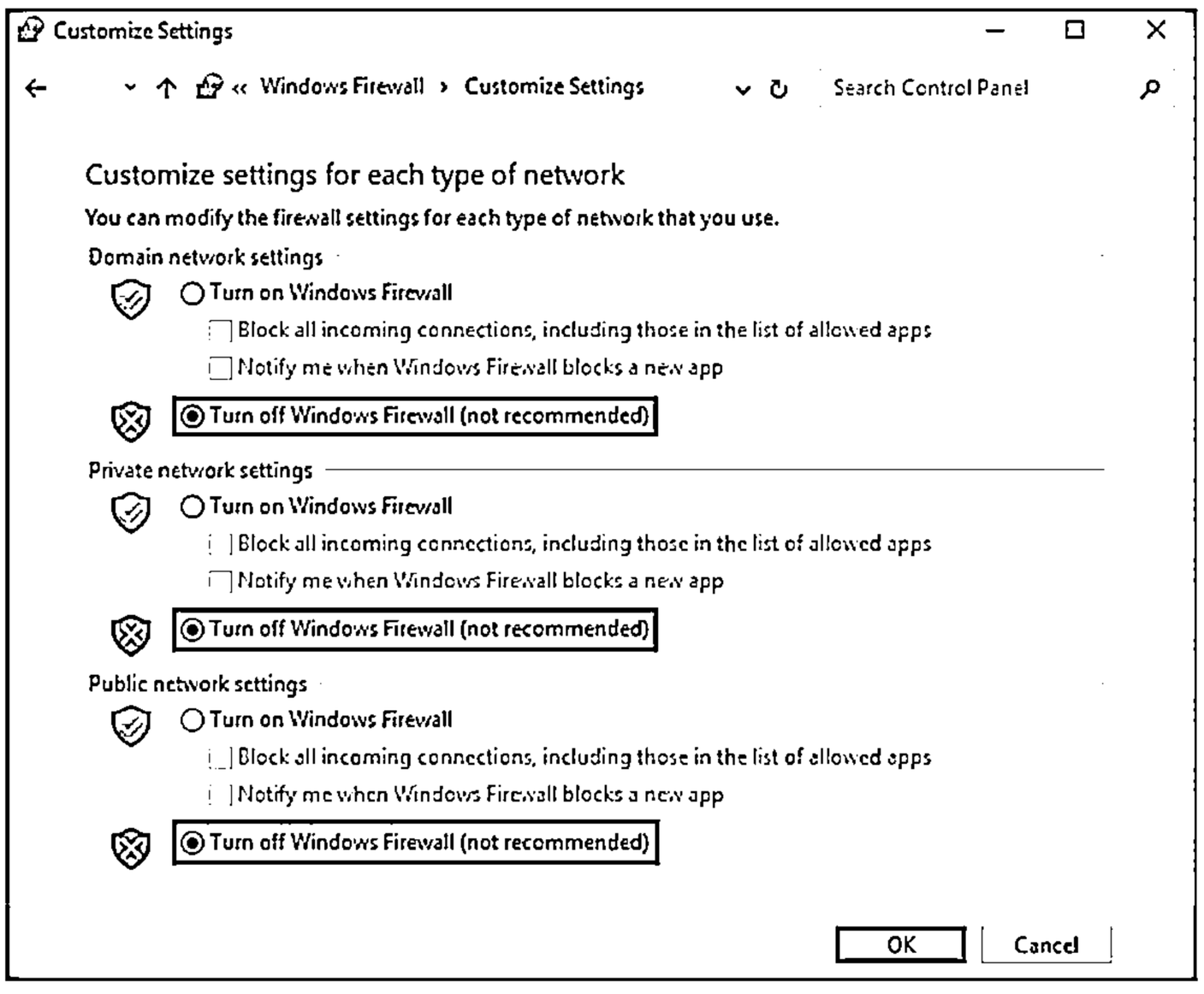


Figure 2.3.9: Turning off Windows Firewall

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

TASK 3.6

Perform UDP Scan

23. Now, return to the **Windows 10** virtual machine. In the **Command** field, type the command **nmap -sU -v <Target IP Address>** (here, the target IP address is **10.10.10.16**) and click **Scan**.

Note: **-sU**: performs the UDP scan and **-v**: enables the verbose output (include all hosts and ports in the output).

24. The scan results appear, displaying all open UDP ports and services running on the target machine, as shown in the screenshot.

Note: This scan will take approximately 20 minutes to finish the scanning process and the results might differ in your lab environment.

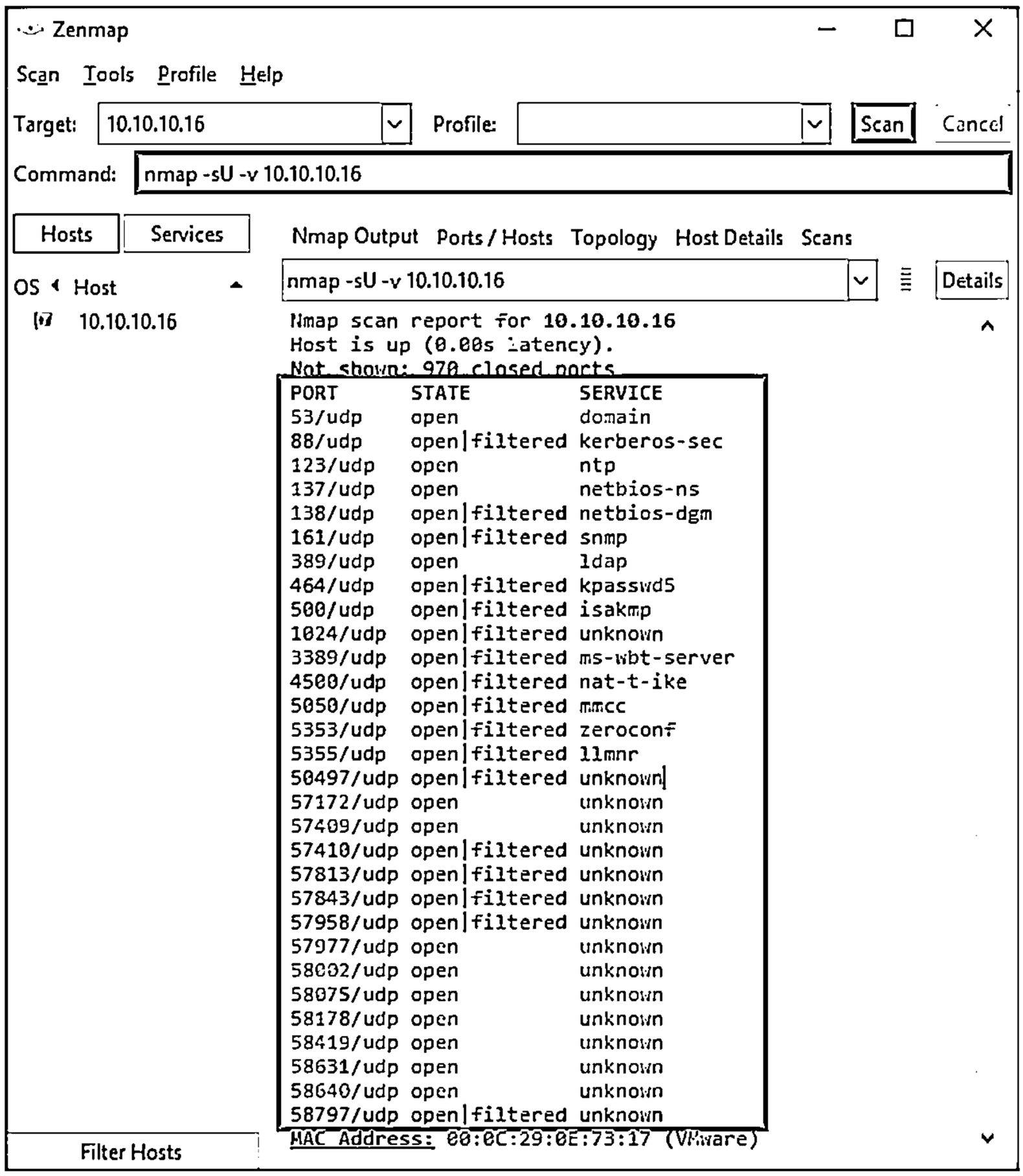


Figure 2.3.10: Zenmap- scan results for UDP scan

Note: The UDP scan uses UDP protocol instead of the TCP. There is no three-way handshake for the UDP scan. It sends UDP packets to the target host; no response means that the port is open. If the port is closed, an ICMP port unreachable message is received.

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

25. Close the **Zenmap** window.
26. You can create your scan profile, or you can also choose the default scan profiles available in Nmap to scan a network
27. Double-click the **Nmap - Zenmap GUI** shortcut from **Desktop** to launch Nmap.
28. To choose the default scan profiles available in Nmap, click on the drop-down icon in the **Profile** field and select the scanning technique you want to use.

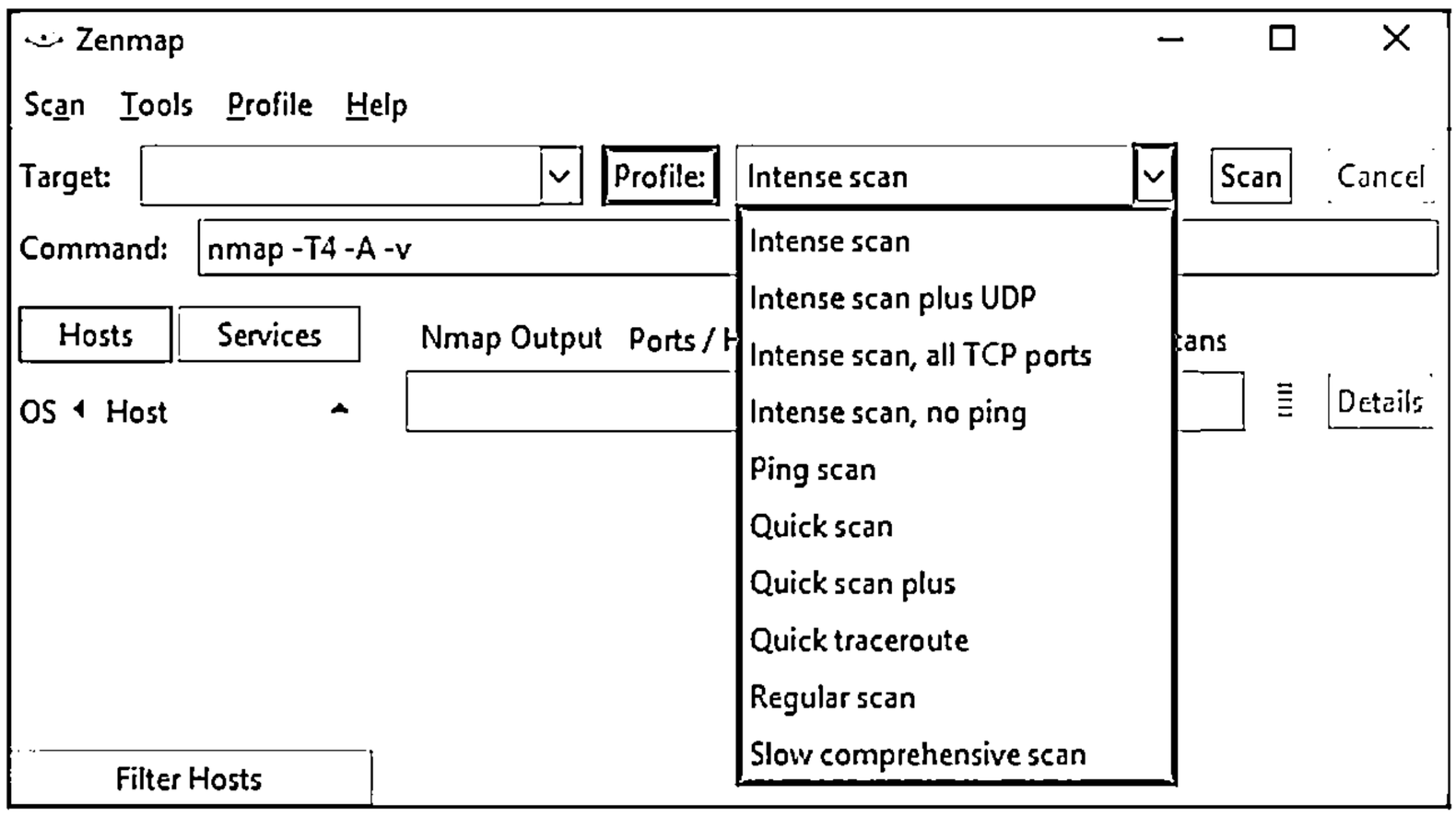


Figure 2.3.11: Zenmap Default Scan Options

TASK 3.7

Create a Scan Profile

29. To create a scan profile; click **Profile → New Profile or Command.**

Note: If a **User Account Control** pop-up appears, click **Yes.**

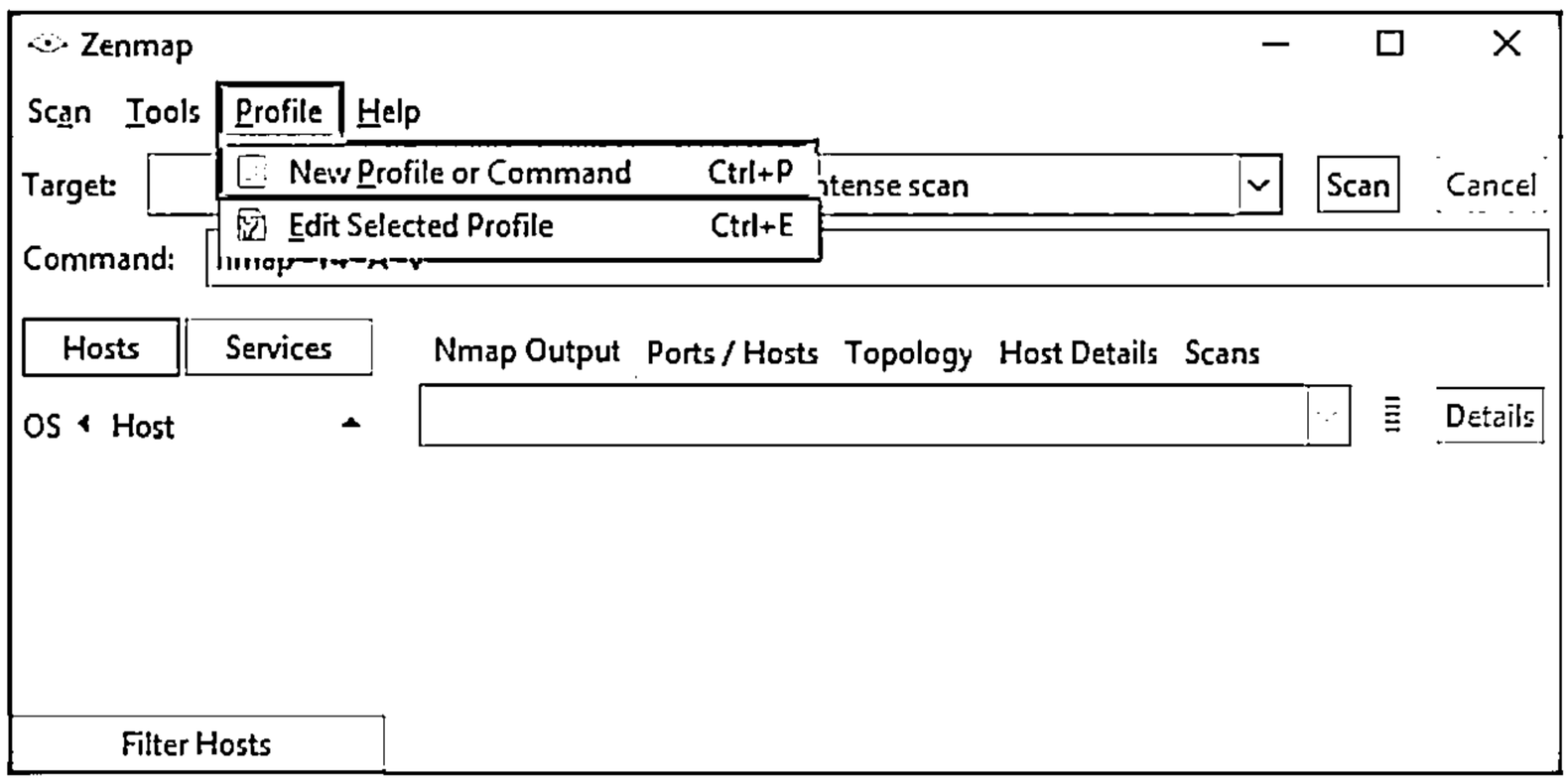


Figure 2.3.12: Creating a New Profile

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

30. The **Profile Editor** window appears. In the **Profile** tab, under the **Profile Information** section, input a profile name (here, **Null Scan**) into the **Profile name** field.

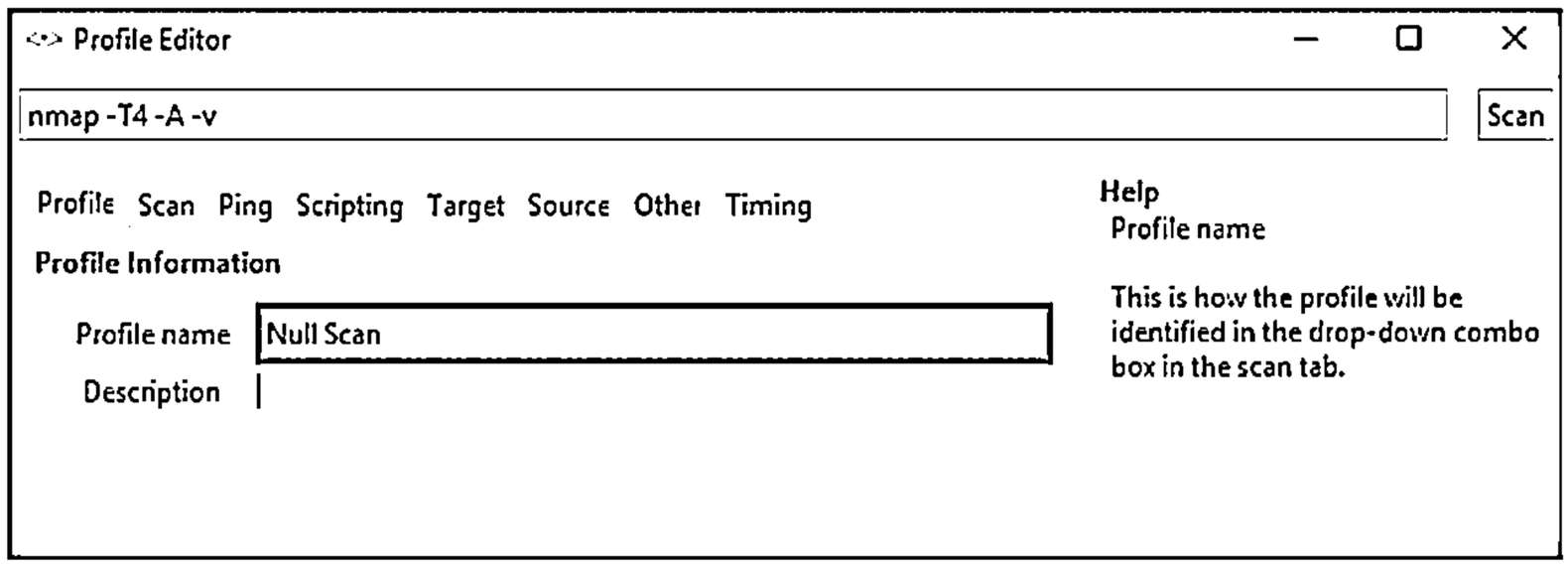


Figure 2.3.13: Entering Profile Name

31. Now, click the **Scan** tab and select the scan option (here, **Null scan (-sN)**) from the **TCP scan** drop-down list.
32. Select **None** in the **Non-TCP scans** drop-down list and **Aggressive (-T4)** in the **Timing template** list. Ensure that the **Enable all advanced/aggressive options (-A)** checkbox is selected and click **Save Changes**, as shown in the screenshot.

Note: Using this configuration, you are setting Nmap to perform a null scan with the time template as **-T4** and all **aggressive** options enabled.

33. This will create a new profile, and will thus be added to the profile list.

Note: You can select any other scan options as per your requirements.

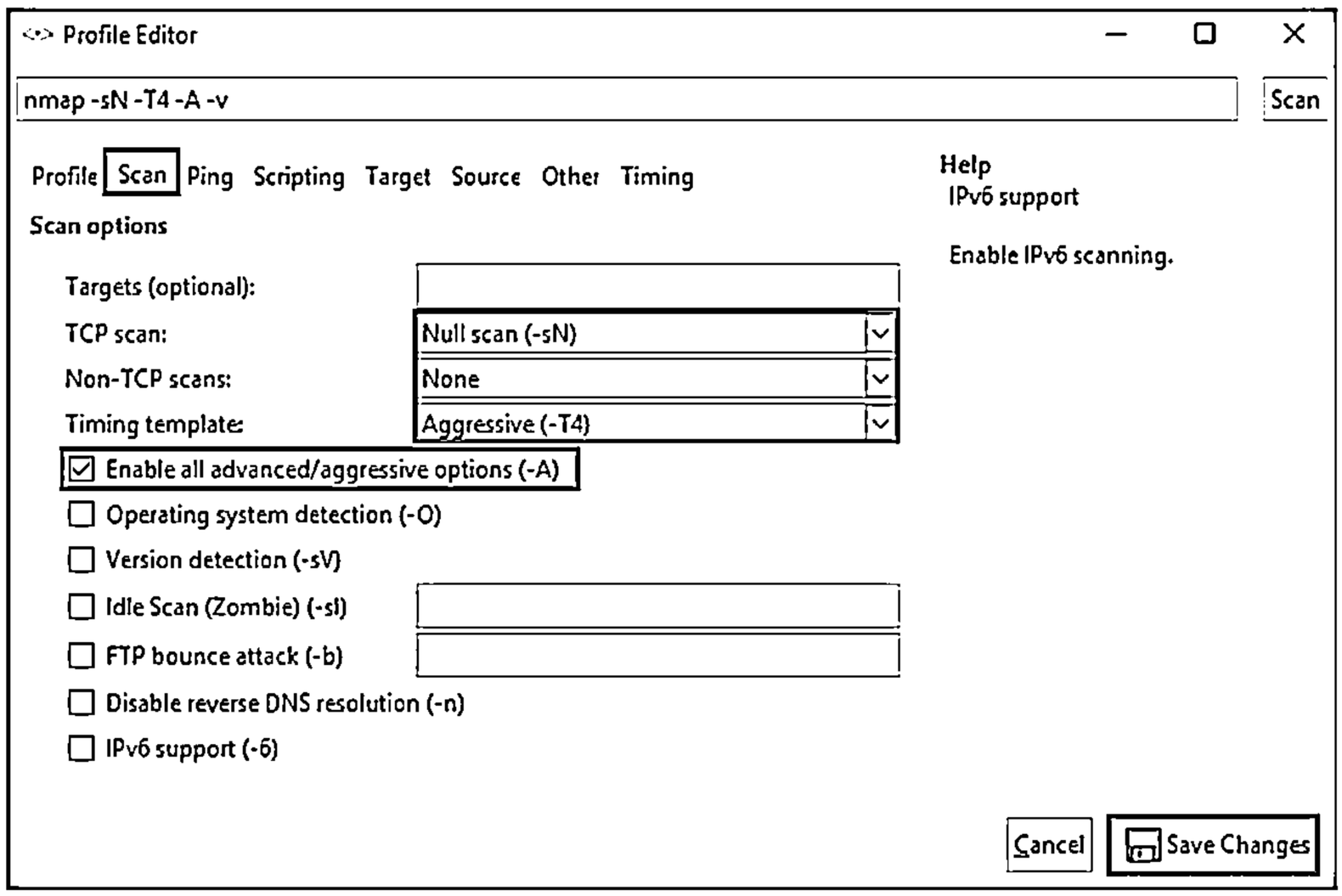


Figure 2.3.14: Configuring Null Scan Profile

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

34. In this task, we will be targeting the **Ubuntu** virtual machine (**10.10.10.9**). Therefore, before starting this task, turn on the **Ubuntu** virtual machine.

35. In the main window of **Zenmap**, enter the target IP address (here, **10.10.10.9**) in the **Target** field to scan. Select the **Null Scan** profile, which you created from the **Profile** drop-down list, and then click **Scan**.

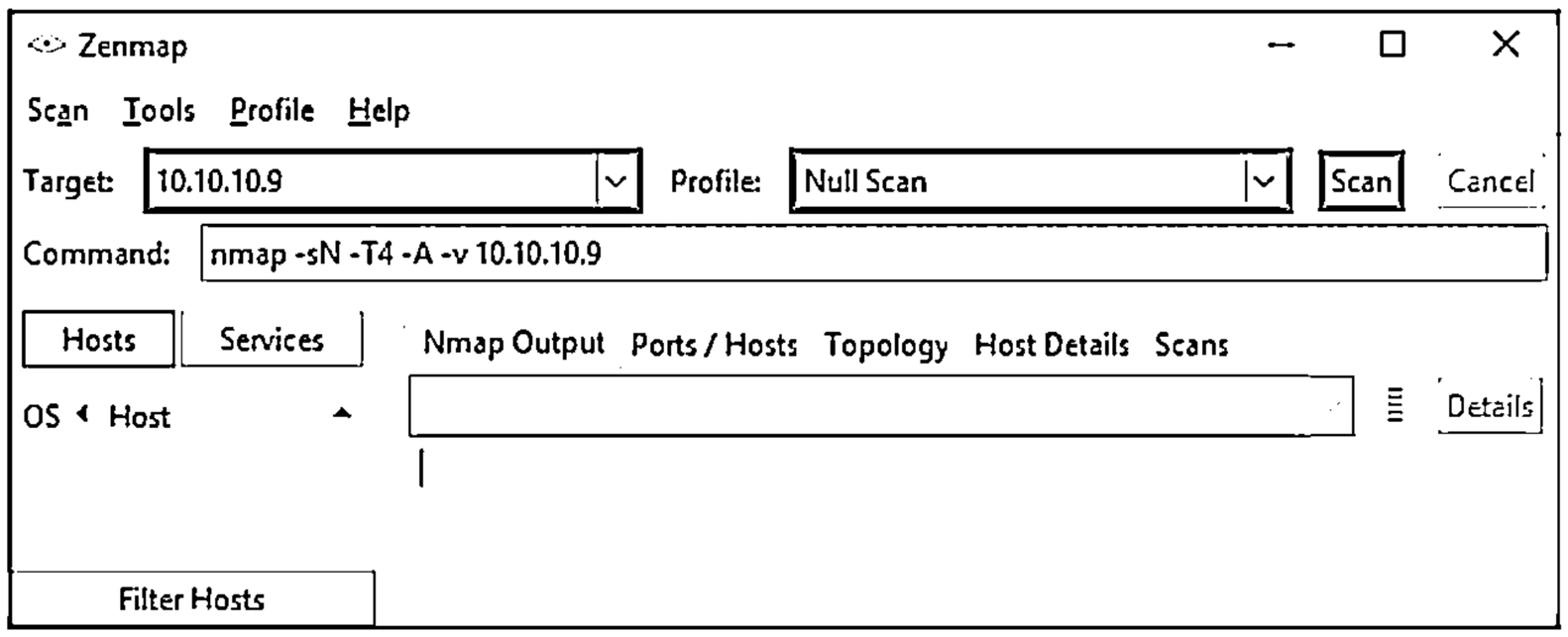


Figure 2.3.15: Initiating Null Scan

36. Nmap scans the target and displays results in the **Nmap Output** tab, as shown in the screenshot.

Note: The results obtained in your lab environment may differ.

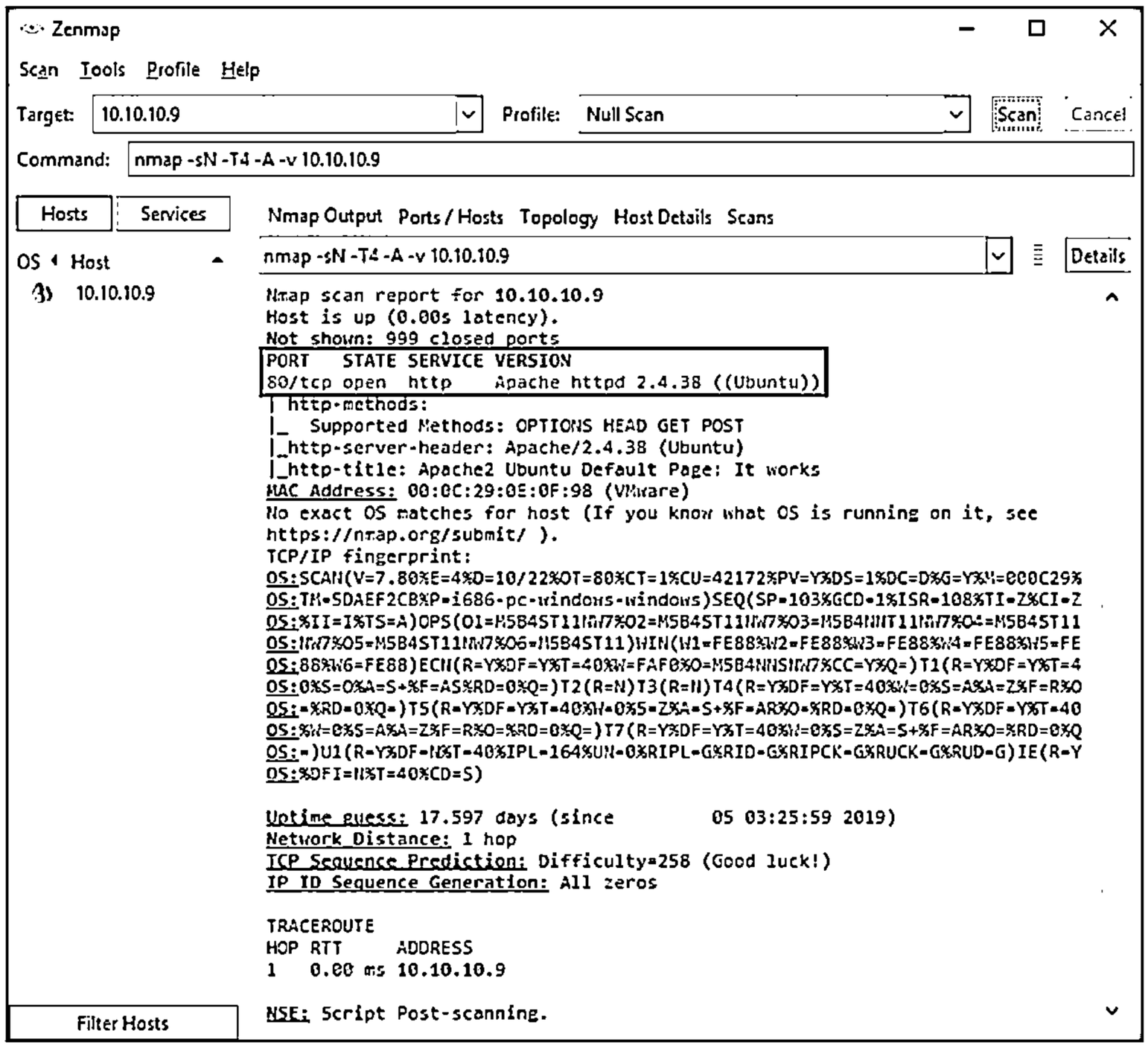


Figure 2.3.16: Null Scan Result

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

37. Apart from the aforementioned port scanning and service discovery techniques, you can also use the following scanning techniques to perform a port and service discovery on a target network using Nmap.

    - **IDLE/IPID Header Scan:** A TCP port scan method that can be used to send a spoofed source address to a computer to discover what services are available.

      # nmap -sI -v <target IP address>

    - **SCTP INIT Scan:** An INIT chunk is sent to the target host; an INIT+ACK chunk response implies that the port is open, and an ABORT Chunk response means that the port is closed.

      # nmap -sY -v <target IP address>

    - **SCTP COOKIE ECHO Scan:** A COOKIE ECHO chunk is sent to the target host; no response implies that the port is open and ABORT Chunk response means that the port is closed.

      # nmap -sZ -v <target IP address>

TASK 3.8

Perform Service Version Discovery

38. In the **Command** field, type the command **nmap -sV <Target IP Address>** (here, the target IP address is **10.10.10.16**) and click **Scan**.

Note: **-sV**: detects service versions.

39. The scan results appear, displaying that open ports and the version of services running on the ports, as shown in the screenshot.

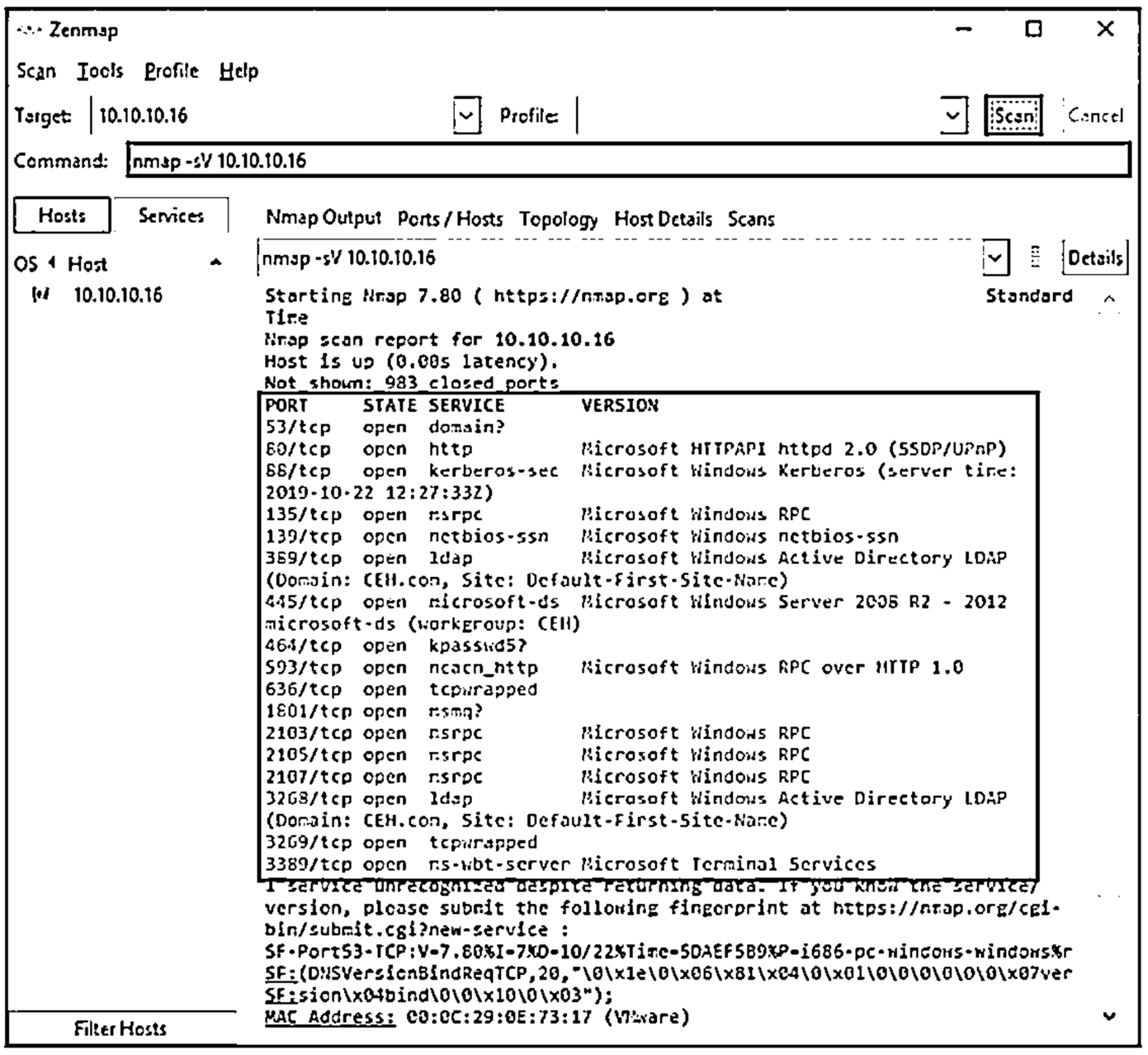


Figure 2.3.17: Zenmap scan results for Service Version Discovery

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

Note: Service version detection helps you to obtain information about the running services and their versions on a target system. Obtaining an accurate service version number allows you to determine which exploits the target system is vulnerable to.

40. Before starting the next sub-task, ensure that the **Parrot Security** and **Ubuntu** virtual machines are turned on.

TASK 3.9

Scan a Whole Subnet

41. In the **Command** field, type the command **nmap -A <Target Subnet>** (here, target subnet is **10.10.10.***) and click **Scan**. By providing the "*" (asterisk) wildcard, you can scan a whole subnet or IP range.

Note: **-A**: enables aggressive scan. The aggressive scan option supports OS detection (-O), version scanning (-sV), script scanning (-sC), and traceroute (--traceroute). You should not use -A against target networks without permission.

42. Nmap scans the entire network and displays information for all the hosts that were scanned, along with the open ports and services, device type, details of OS, etc. as shown in the screenshot.

Note: This scan will take some time to finish the scanning process. The results might differ in your lab environment.

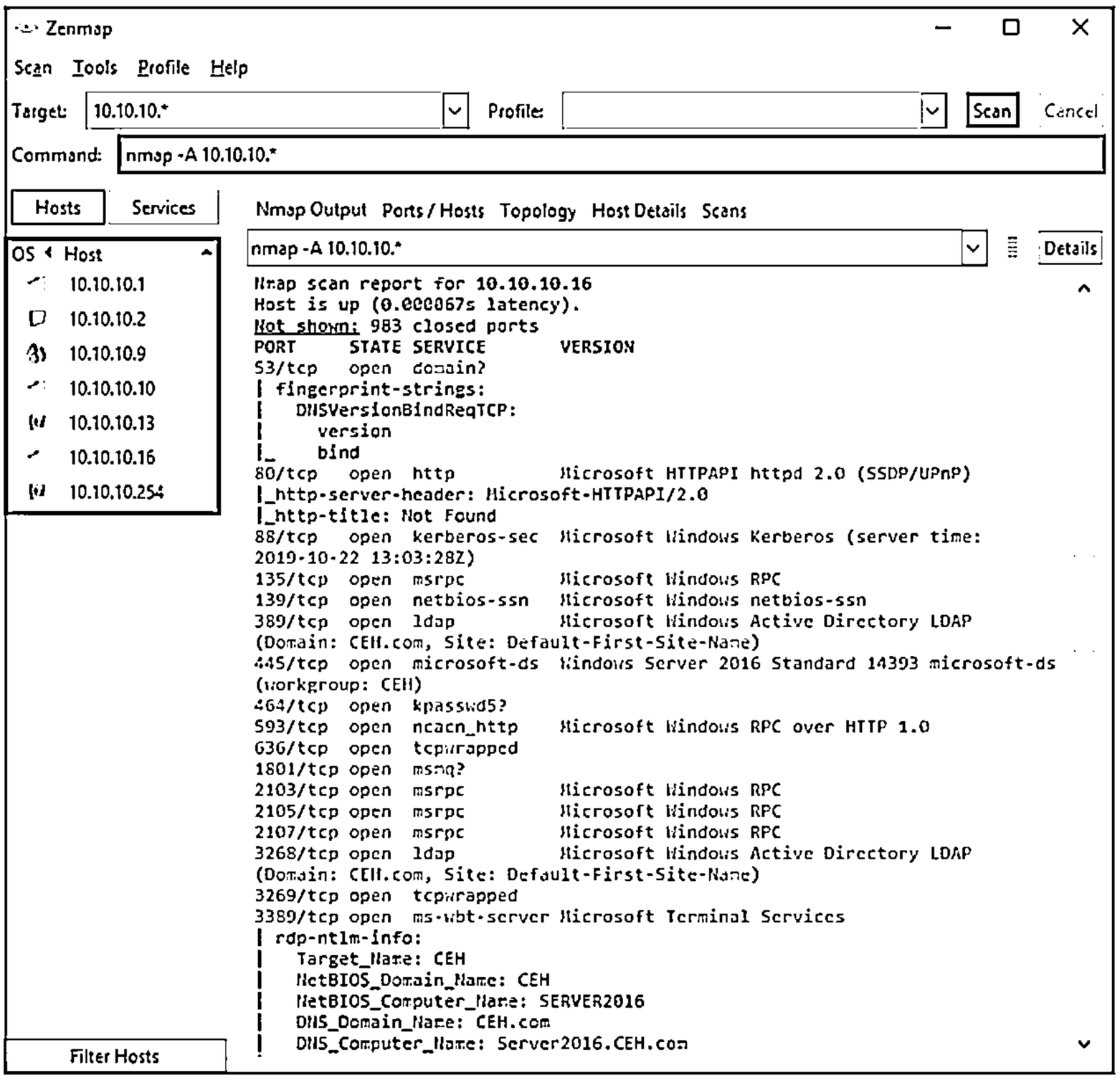


Figure 2.3.18: Zenmap displaying output for a Whole Subnet Scan

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

43. Choose an IP address **10.10.10.16** from the list of hosts in the left-pane and click the **Host Details** tab. This tab displays information such as **Host Status**, **Addresses**, **Operating System**, **Ports used**, **OS Classes**, etc. associated with the selected host.

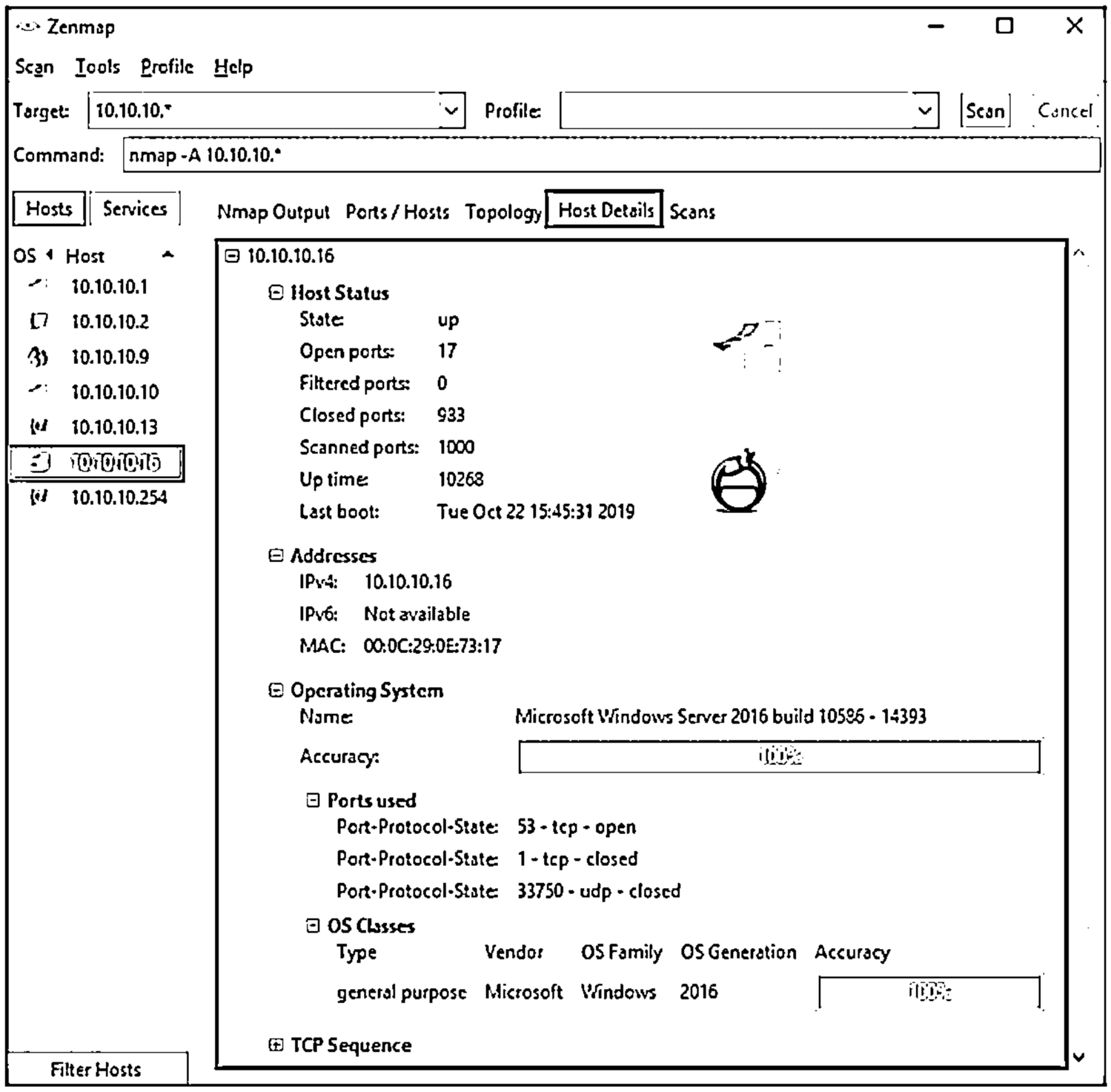


Figure 2.3.19: Zenmap displaying the Open Ports under Ports/Hosts tab

44. This concludes the demonstration of discovering target open ports, services, services versions, device type, OS details, etc. of the active hosts in the target network using various scanning techniques of Nmap.
45. Close all open windows and document all the acquired information.
46. Turn off the **Windows 10** and **Ubuntu** virtual machine.

TASK 4 Explore Various Network Scanning Techniques using Hping3

Here, we will use Hping3 to discover open ports and services running on the live hosts in the target network.

1. Switch to the **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

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

Hping2/Hping3 is a command-line-oriented network scanning and packet crafting tool for the TCP/IP protocol that sends ICMP echo requests and supports TCP, UDP, ICMP, and raw-IP protocols. Using Hping, you can study the behavior of an idle host and gain information about the target such as the services that the host offers, the ports supporting the services, and the OS of the target.

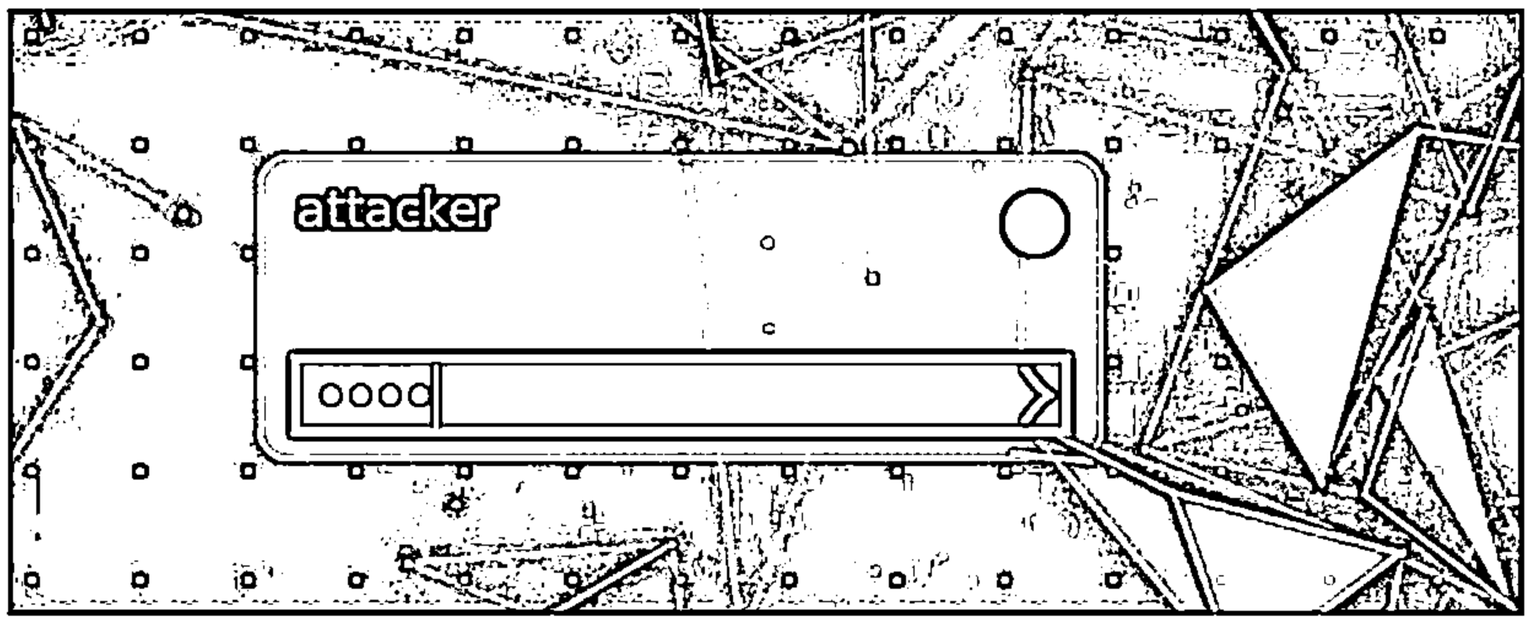


Figure 2.4.1: Parrot Security login page

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

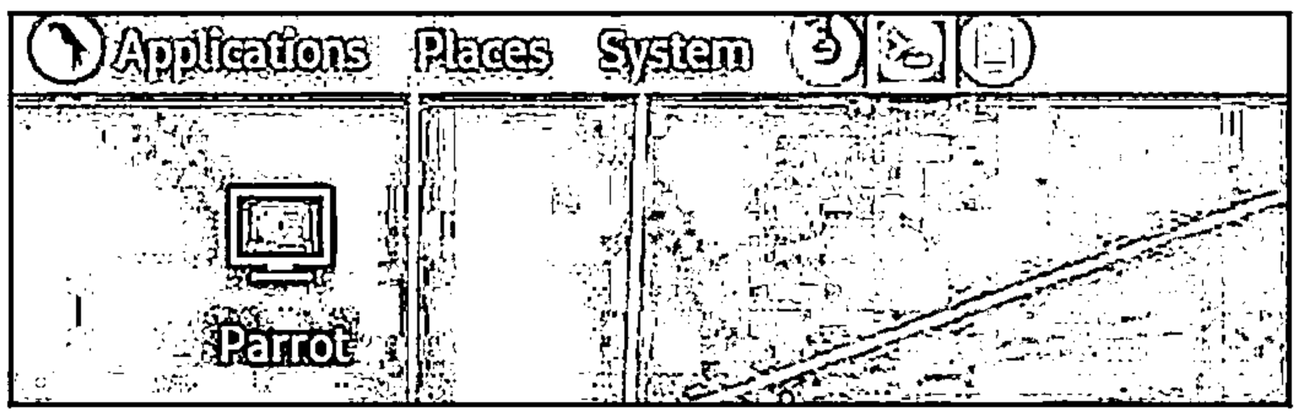


Figure 2.4.2: MATE Terminal Icon

4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

   Note: The password that you type will not be visible.

6. Now, type **cd** and press **Enter** to jump to the root directory.

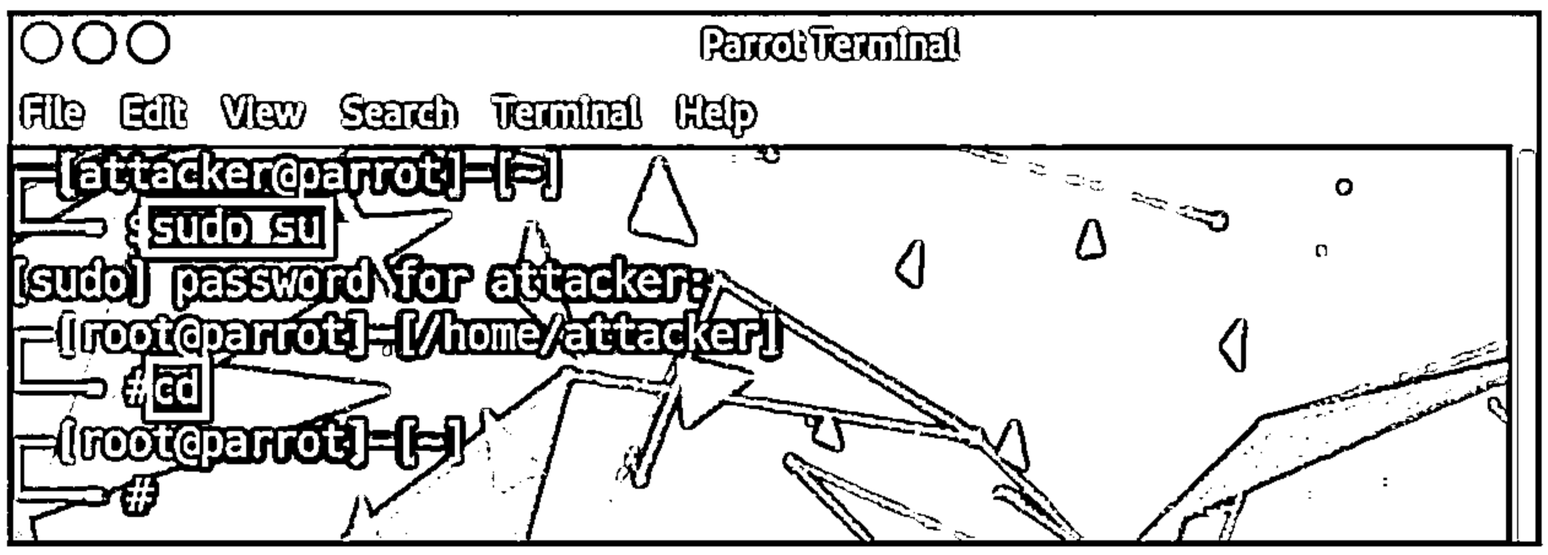


Figure 2.4.3: Running the programs as a root user

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

TASK 4.1

Perform ACK Scan

7. In the terminal window, type **hping3 -A <Target IP Address> -p 80 -c 5** (here, the target machine is Windows Server 2016 [**10.10.10.16**]) and press **Enter**.

Note: In this command, **-A** specifies setting the ACK flag, **-p** specifies the port to be scanned (here, **80**), and **-c** specifies the packet count (here, **5**).

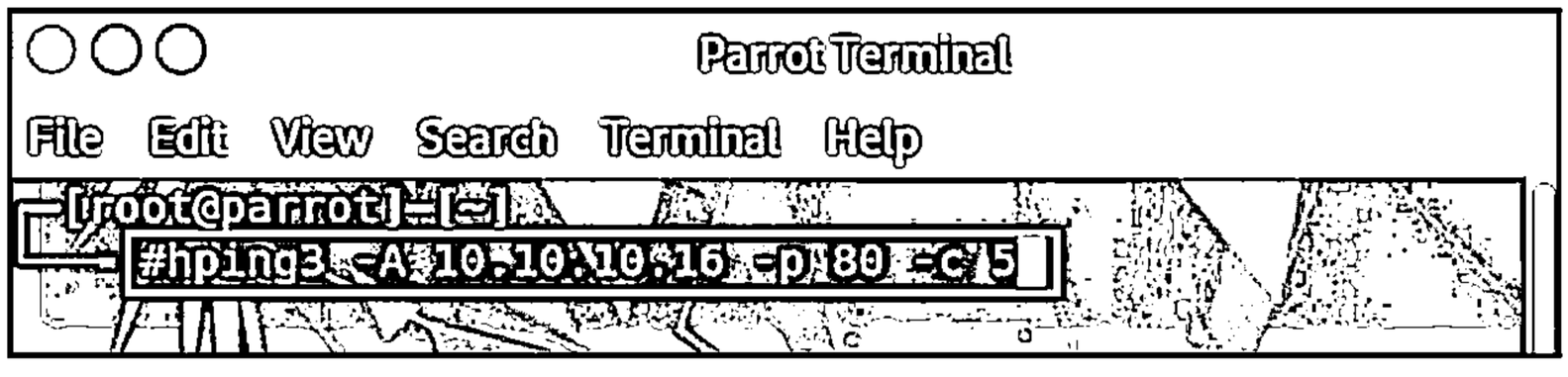


Figure 2.4.4: Hping3 TCP ACK scan command

8. In a result, the number of packets sent and received is equal, indicating that the respective port is open, as shown in the screenshot.

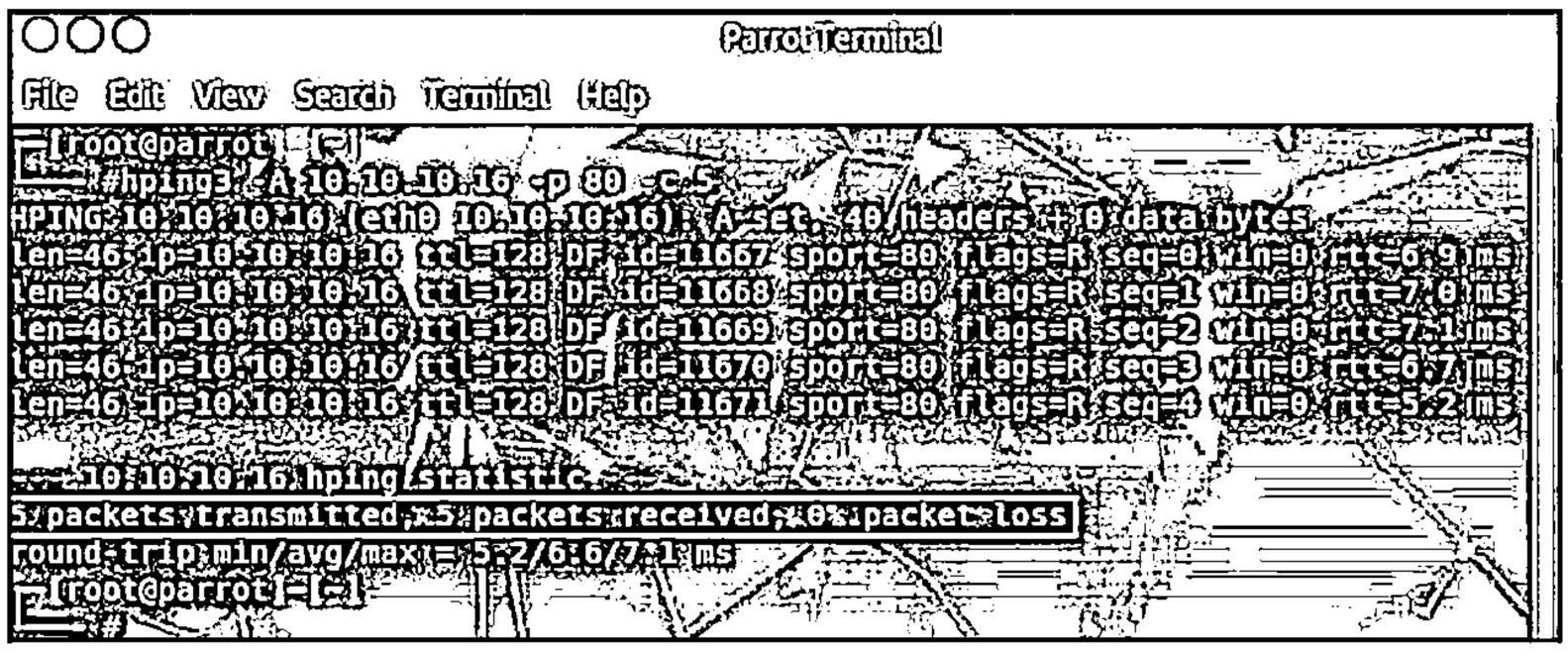


Figure 2.4.5: Hping3 ACK scan result

Note: The ACK scan sends an ACK probe packet to the target host; no response means that the port is filtered. If an RST response returns, this means that the port is closed.

TASK 4.2

Perform SYN Scan

9. In the terminal window, type **hping3 -8 0-100 -S <Target IP Address> -V** (here, the target machine is Windows Server 2016 [**10.10.10.16**]) and press **Enter**.

Note: In this command, **-8** specifies a scan mode, **-p** specifies the range of ports to be scanned (here, **0-100**), and **-V** specifies the verbose mode.

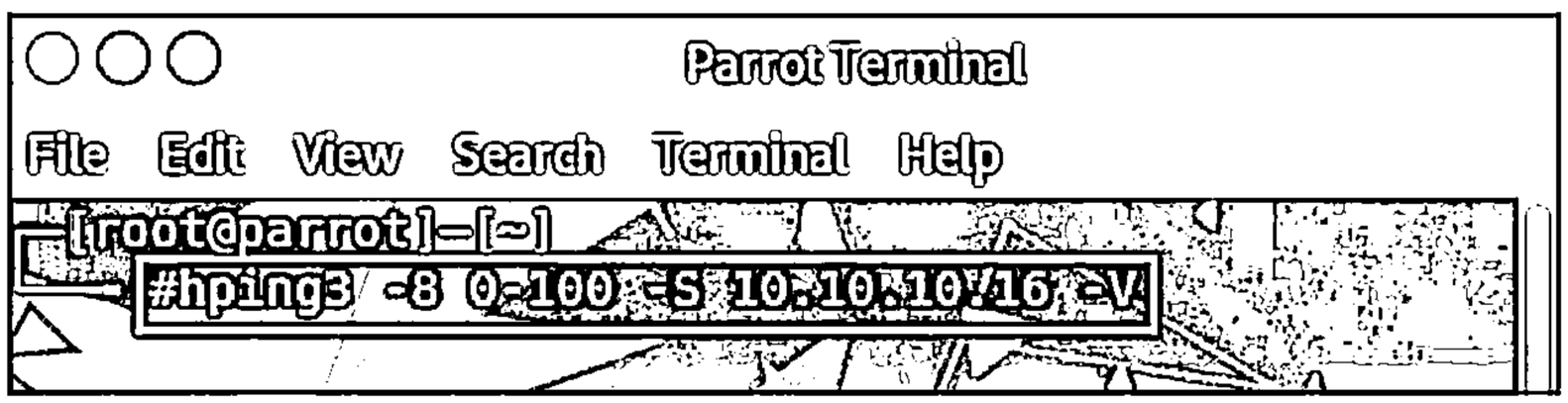


Figure 2.4.6: Hping3 TCP SYN scan command

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

10. The result appears, displaying the open ports along with the name of service running on each open port, as shown in the screenshot.

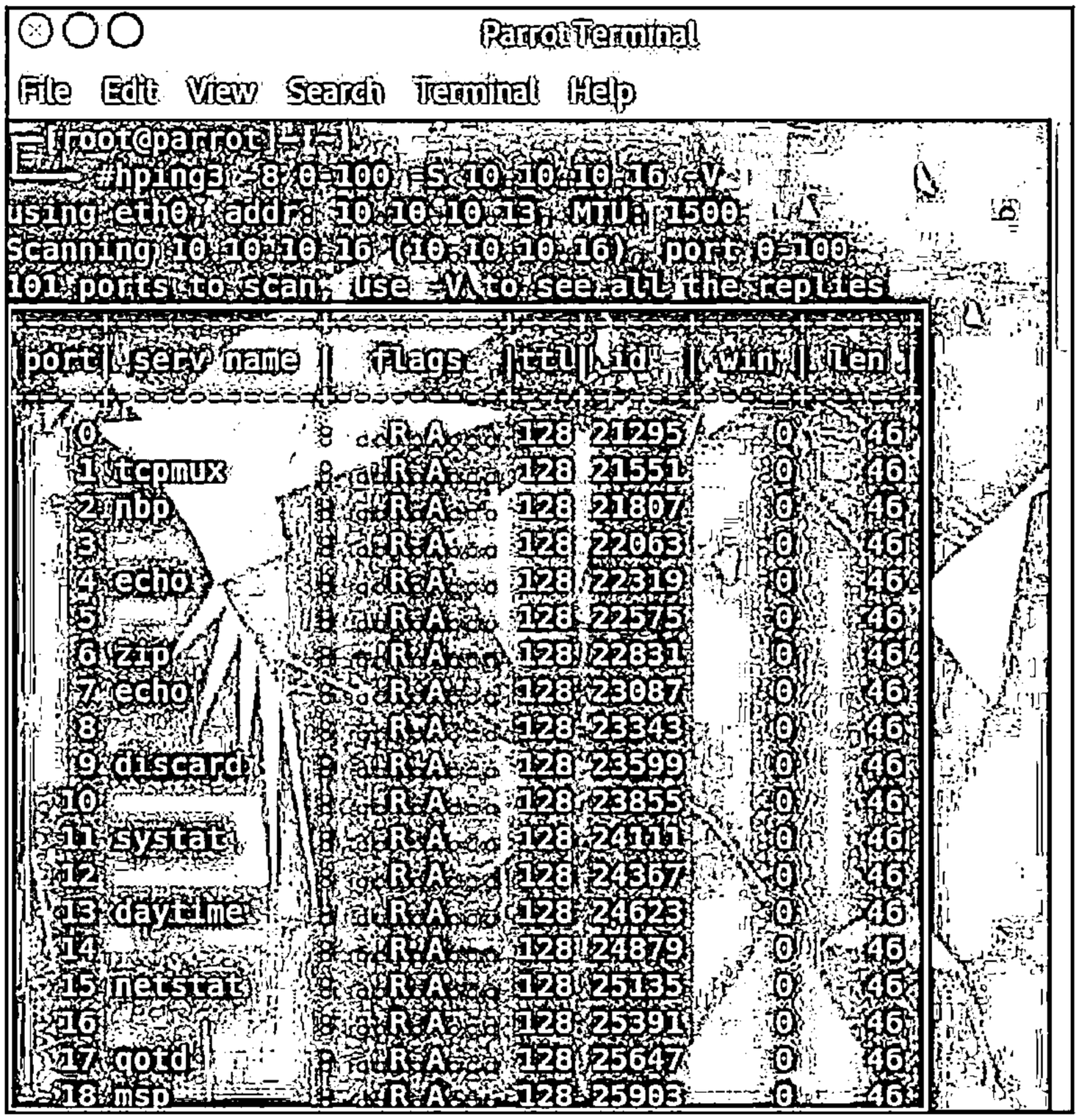


Figure 2.4.7: Hping3 SYN scan result

Note: The SYN scan principally deals with three of the flags: SYN, ACK, and RST. You can use these three flags for gathering illegal information from servers during the enumeration process.

TASK 4.3

Perform FIN, PUSH, and URG Scan

11. In the terminal window, type **hping3 -F -P -U <Target IP Address> -p 80 -c 5** (here, the target machine is Windows Server 2016 [**10.10.10.16**]) and press **Enter**.

Note: In this command, **-F** specifies setting the FIN flag, **-P** specifies setting the PUSH flag, **-U** specifies setting the URG flag, **-c** specifies the packet count (here, **5**), and **-p** specifies the port to be scanned (here, **80**).

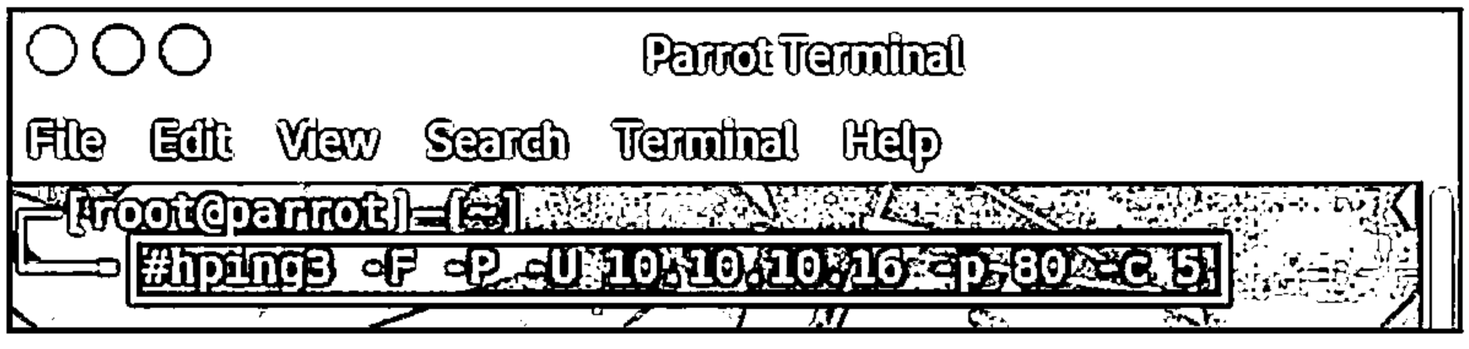


Figure 2.4.8: Hping3 FIN, PUSH, and URG scan command

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

12. The results demonstrate that the number of packets sent and received is equal, thereby indicating that the respective port is open, as shown in the screenshot.

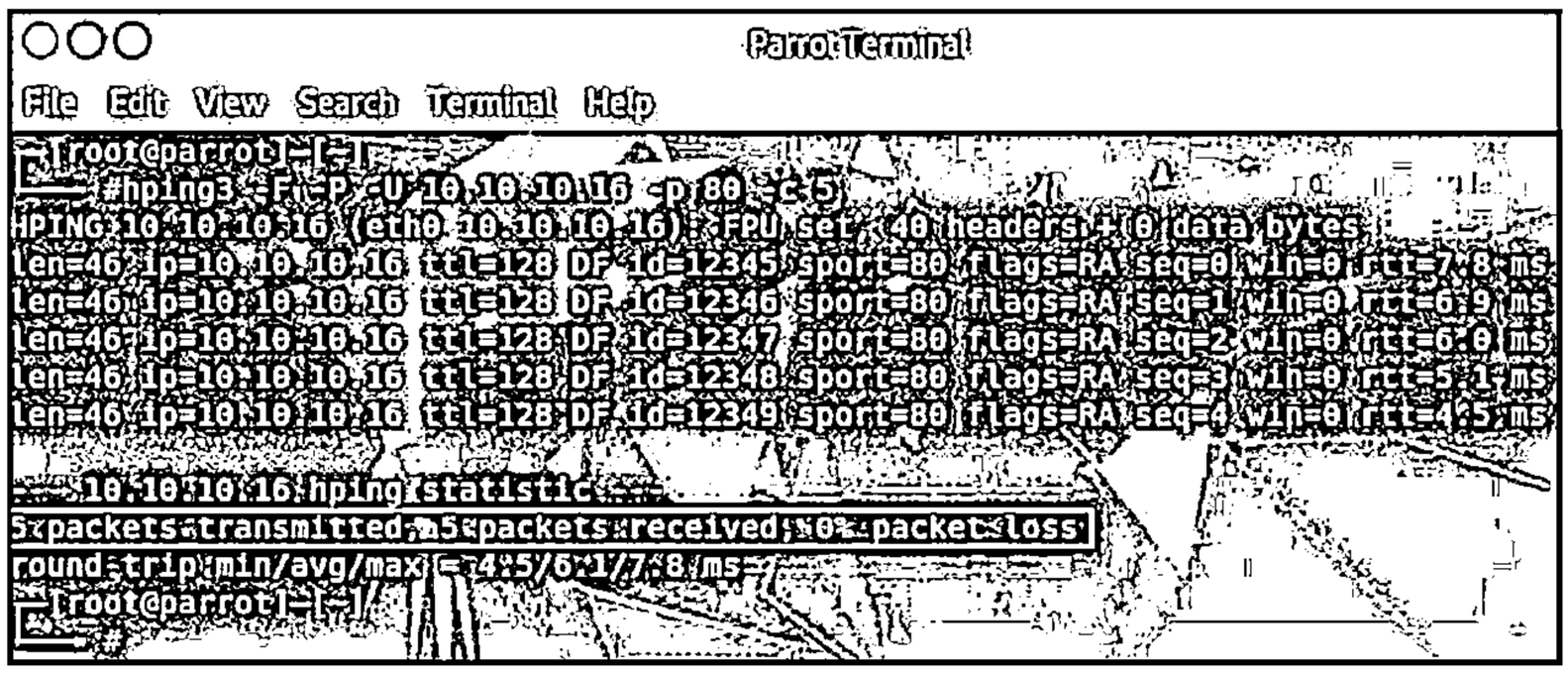


Figure 2.4.9: Hping3 FIN, PUSH, and URG scan result

Note: FIN, PUSH, and URG scan the port on the target IP address. If a port is open on the target, you will not receive a response. If the port is closed, Hping will return an RST response.

TASK 4.4

Perform TCP Stealth Scan

13. In the terminal window, type **hping3 --scan 0-100 -S <Target IP Address>** (here, the target machine is Windows Server 2016 [**10.10.10.16**]) and press **Enter**.

Note: In this command, **--scan** specifies the port range to scan, **0-100** specifies the range of ports to be scanned, and **-S** specifies setting the SYN flag.

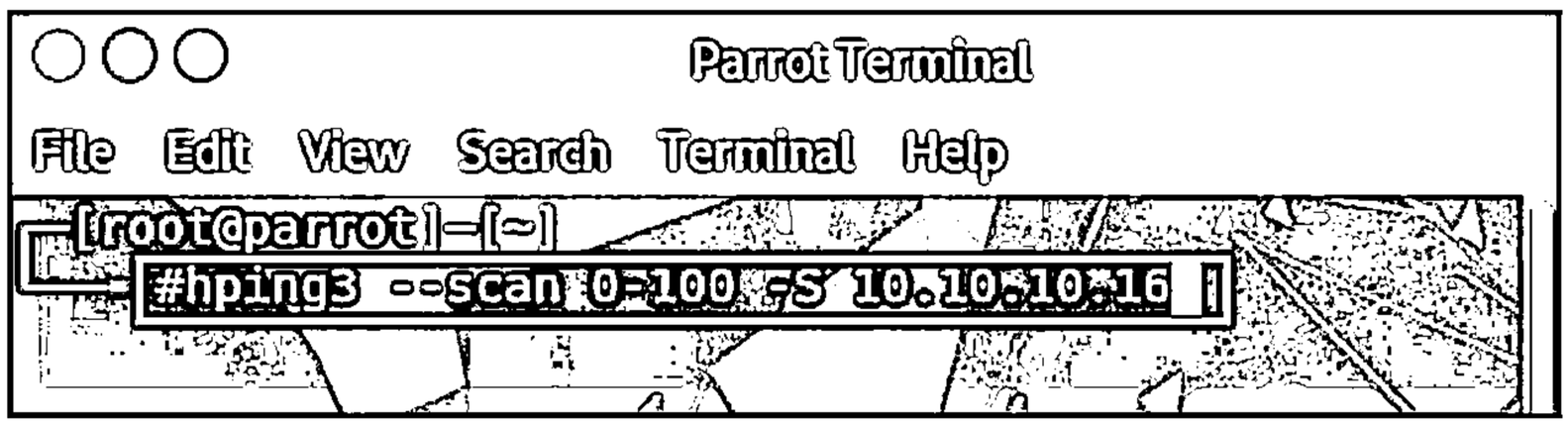


Figure 2.4.10: Hping3 TCP stealth scan command

14. The result appears displaying the open ports and names of the services running on the target IP address, as shown in the screenshot.

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

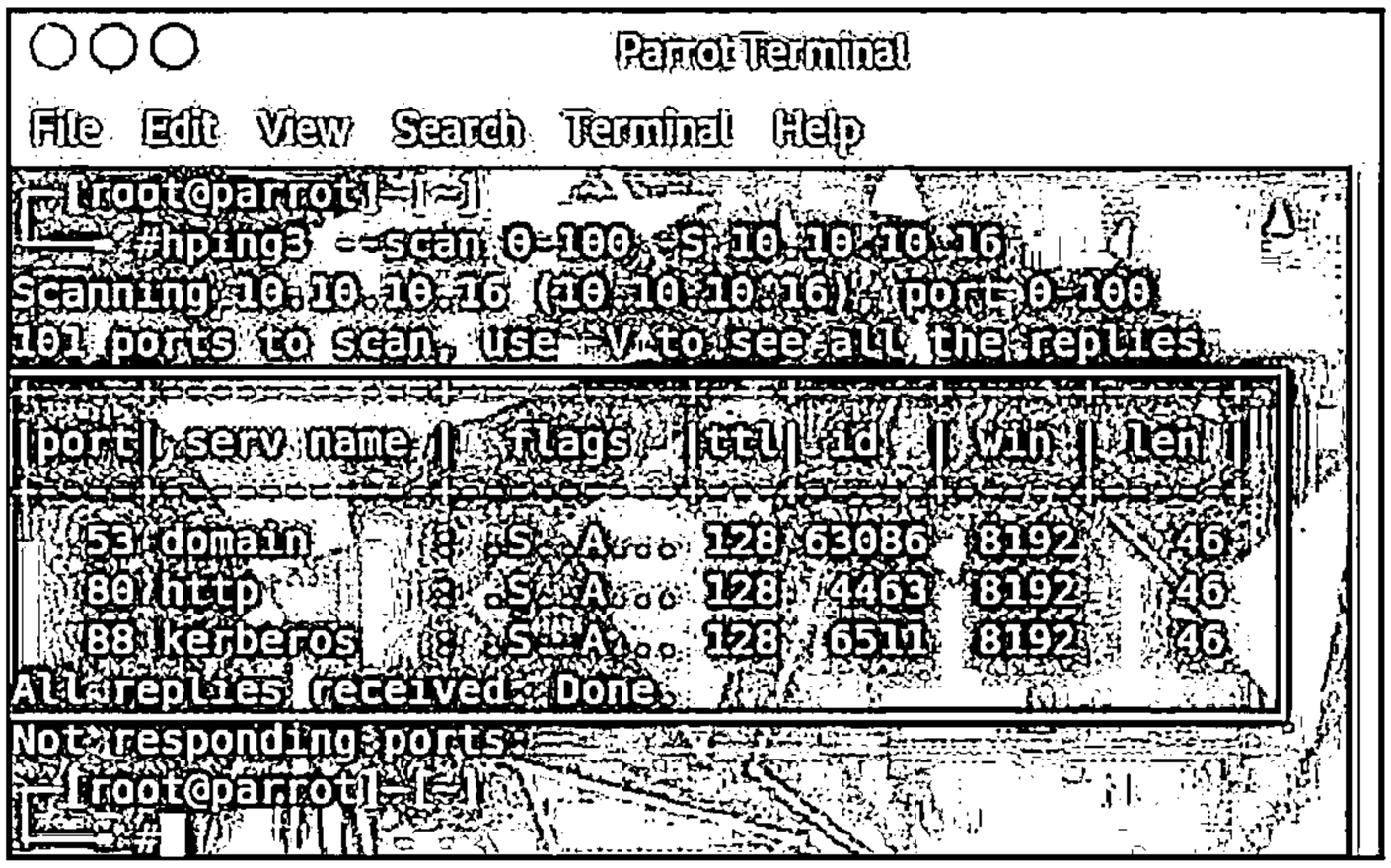


Figure 2.4.11: Hping3 TCP stealth scan result

Note: In the TCP stealth scan, the TCP packets are sent to the target host; if a SYN+ACK response is received, it indicates that the ports are open.

15. Apart from the aforementioned port scanning and service discovery techniques, you can also use the following scanning techniques to perform a port and service discovery on a target network using Hping3.
    - ICMP scan: **hping3 -1 <Target IP Address> -p 80 -c 5**
    - Entire subnet scan for live host: **hping3 -1 <Target Subnet> –rand-dest -I eth0**
    - UDP scan: **hping3 -2 <Target IP Address> -p 80 -c 5**
16. This concludes the demonstration of discovering open ports and services running on the live hosts in the target network using Hping3.
17. Close all open windows and document all the acquired information.
18. Turn off the **Parrot Security** and **Windows Server 2016** virtual machine.

Lab Analysis

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

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT 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

Perform OS Discovery

Banner grabbing, or OS fingerprinting, is used to determine the OS running on a remote target system.

ICON KEY

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

Lab Scenario

As a professional ethical hacker or a pen tester, the next step after discovering the open ports and services running on the target range of IP addresses is to perform OS discovery. Identifying the OS used on the target system allows you to assess the system's vulnerabilities and the exploits that might work on the system to perform additional attacks.

Lab Objectives

- Identify the target system's OS with Time-to-Live (TTL) and TCP window sizes using Wireshark
- Perform OS discovery using Nmap Script Engine (NSE)
- Perform OS discovery using Unicornscan

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2016 virtual machine
- Parrot Security virtual machine
- Ubuntu virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- Wireshark located at **E:\CEH-Tools\CEHv11 Module 03 Scanning Networks\Banner Grabbing Tools\Wireshark**
- You can also download the latest version of Wireshark from its official website. If you decide to download the latest version, the screenshots shown in the lab might differ.

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

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 03 Scanning Networks

Lab Duration

Time: 15 Minutes

Overview of OS Discovery/Banner Grabbing

Banner grabbing, or OS fingerprinting, is a method used to determine the OS that is running on a remote target system.

There are two types of OS discovery or banner grabbing techniques:

- **Active Banner Grabbing**

  Specially crafted packets are sent to the remote OS, and the responses are noted, which are then compared with a database to determine the OS. Responses from different OSes vary, because of differences in the TCP/IP stack implementation.

- **Passive Banner Grabbing**

  This depends on the differential implementation of the stack and the various ways an OS responds to packets. Passive banner grabbing includes banner grabbing from error messages, sniffing the network traffic, and banner grabbing from page extensions.

Parameters such as TTL and TCP window size in the IP header of the first packet in a TCP session plays an important role in identifying the OS running on the target machine. The TTL field determines the maximum time a packet can remain in a network, and the TCP window size determines the length of the packet reported. These values differ for different OSes: you can refer to the following table to learn the TTL values and TCP window size associated with various OSes.

Operating System (OS)	Time To Live	TCP Window Size
Linux (Kernel 2.4 and 2.6)	64	5840
Google Linux	64	5720
FreeBSD	64	65535
OpenBSD	64	16384
Windows 95	32	8192
Windows 2000	128	16384
Windows XP	128	65535
Windows 98, Vista and 7 (Server 2008)	128	8192
iOS 12.4 (Cisco Routers)	255	4128
Solaris 7	255	8760
AIX 4.3	64	16384

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

Lab Tasks

TASK 1

Identify the Target System's OS with Time-to-Live (TTL) and TCP Window Sizes using Wireshark

Here, we will use the Wireshark tool to perform OS discovery on the target host(s).

1. Before beginning this lab, turn on the **Windows 10**, **Windows Server 2016**, and **Ubuntu** virtual machine.
2. In the **Windows 10** virtual machine log in with the credentials Username: **Admin** and Password: **Pa$$w0rd**.

TASK 1.1

Install Wireshark

3. Navigate to **E:\CEH-Tools\CEHv11 Module 03 Scanning Networks\Banner Grabbing Tools\Wireshark** and double-click **Wireshark-win64-3.0.5.exe**.

Note: If a **User Account Control** window appears, click **Yes**.

Wireshark is a network protocol analyzer that allows capturing and interactively browsing the traffic running on a computer network. It is used to identify the target OS through sniffing/ capturing the response generated from the target machine to the request-originated machine. Further, you can observe the TTL and TCP window size fields in the captured TCP packet. Using these values, the target OS can be determined.

4. **Wireshark Setup** window appears; follow the steps to install Wireshark using all default settings.

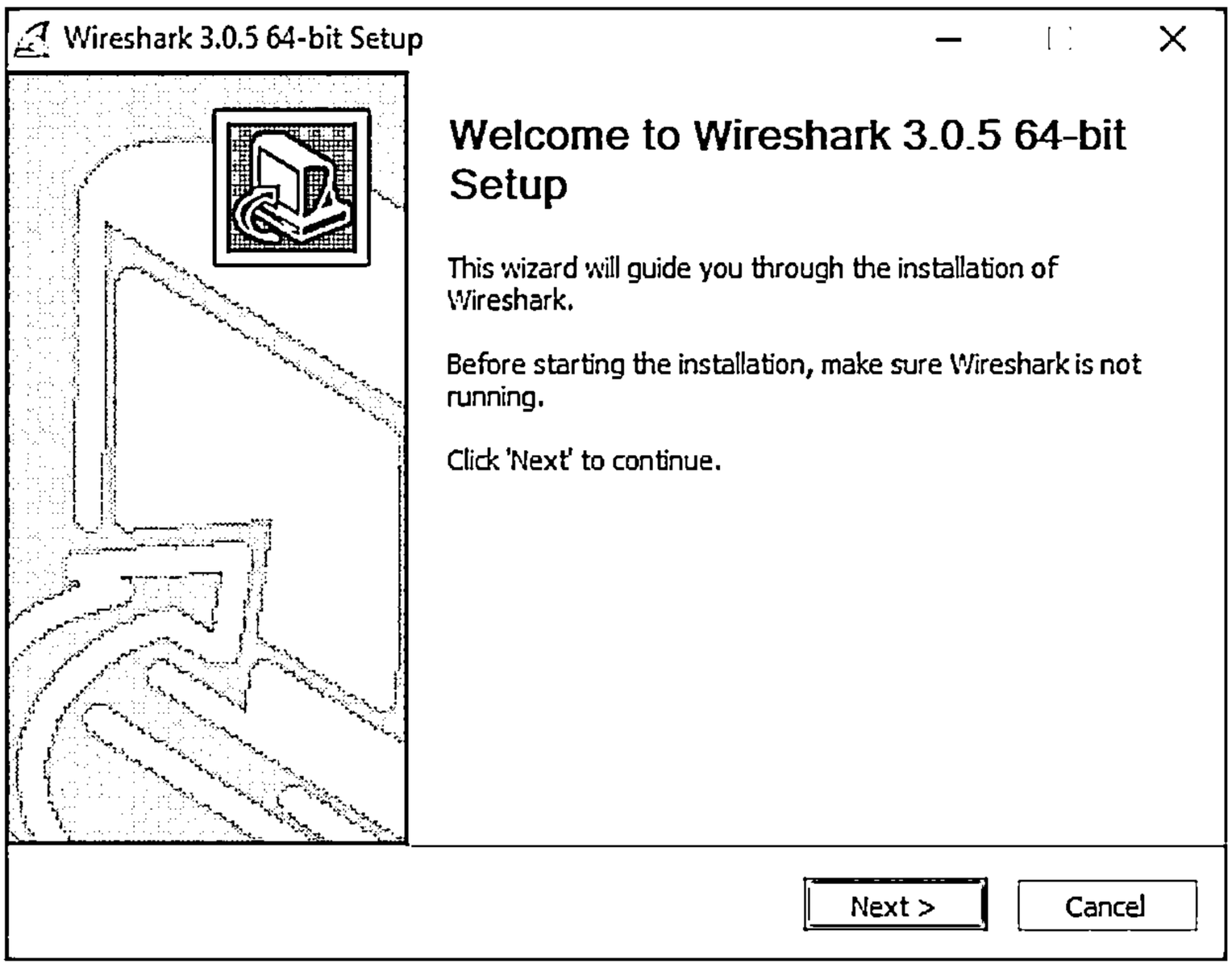


Figure 3.1.1: Wireshark Setup window

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

5. In the **Packet Capture** wizard, ensure that the **Install Npcap 0.9983** checkbox is selected and click **Next**.

Note: The version of Npcap may differ in your lab environment.

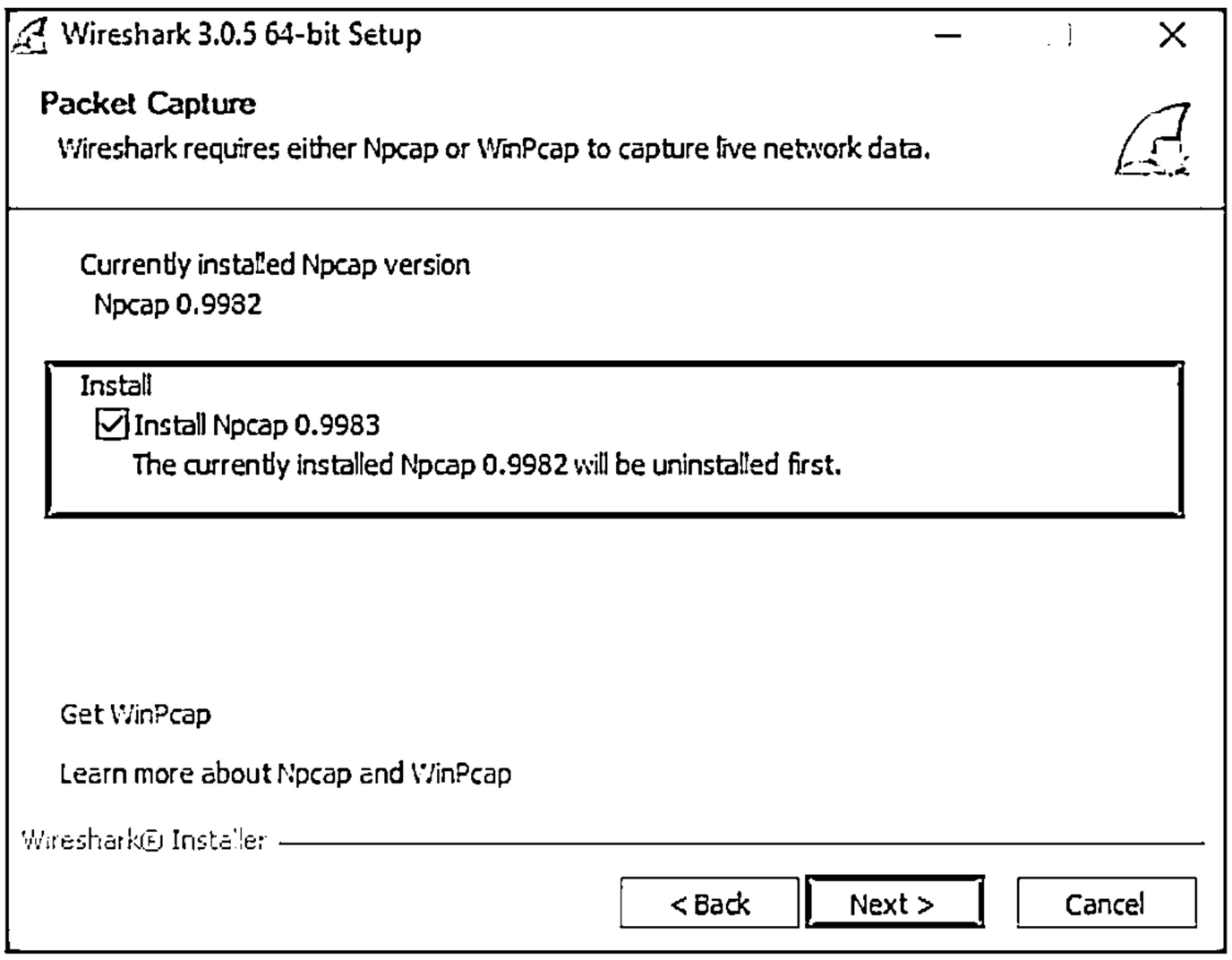


Figure 3.1.2: Packet Capture wizard

6. In the **USB Capture** wizard, select the **Install USBPcap 1.3.0.0** checkbox and click **Install**.

Note: The version of USBPcap may differ in your lab environment.

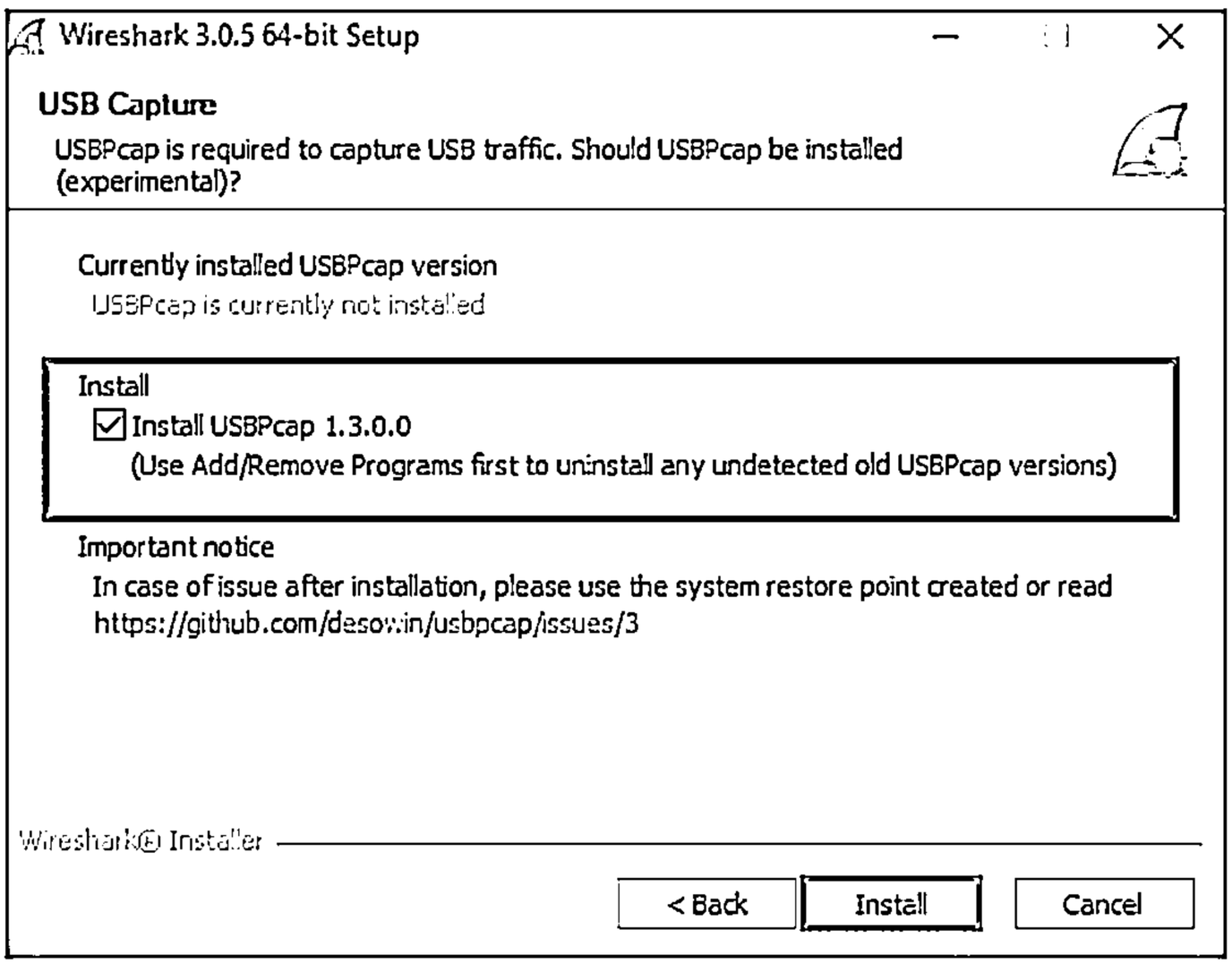


Figure 3.1.3: USB Capture wizard

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

7. Follow the wizard steps to install Npcap and USBPcap using all default settings.
8. After the completion of the installation, in the **Wireshark Setup** windows, ensure that the **Reboot now** radio button is selected, and click **Finish**.

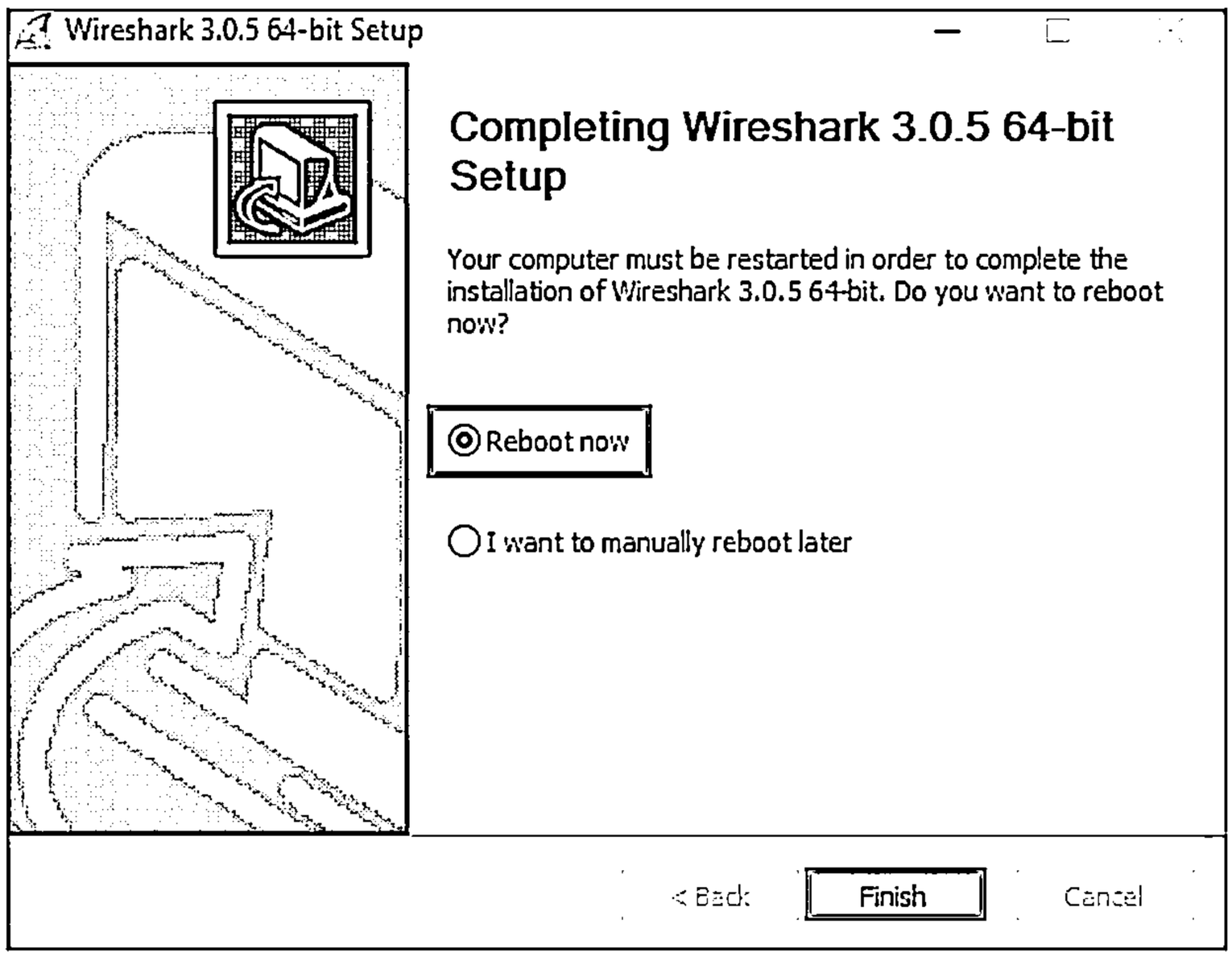


Figure 3.1.4: Wireshark setup window

9. The **Windows 10** virtual machine will restart. Log in with the credentials **Admin/Pa$$w0rd**.
10. Click on the **Start** menu and launch **Wireshark** from the applications.

TASK 1.2

Run Wireshark

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

11. The **Wireshark Network Analyzer** main window appears; double-click the available ethernet or interface (here, **Ethernet0**) to start the packet capture, as shown in the screenshot.

Note: The available interface might vary in your lab environment.

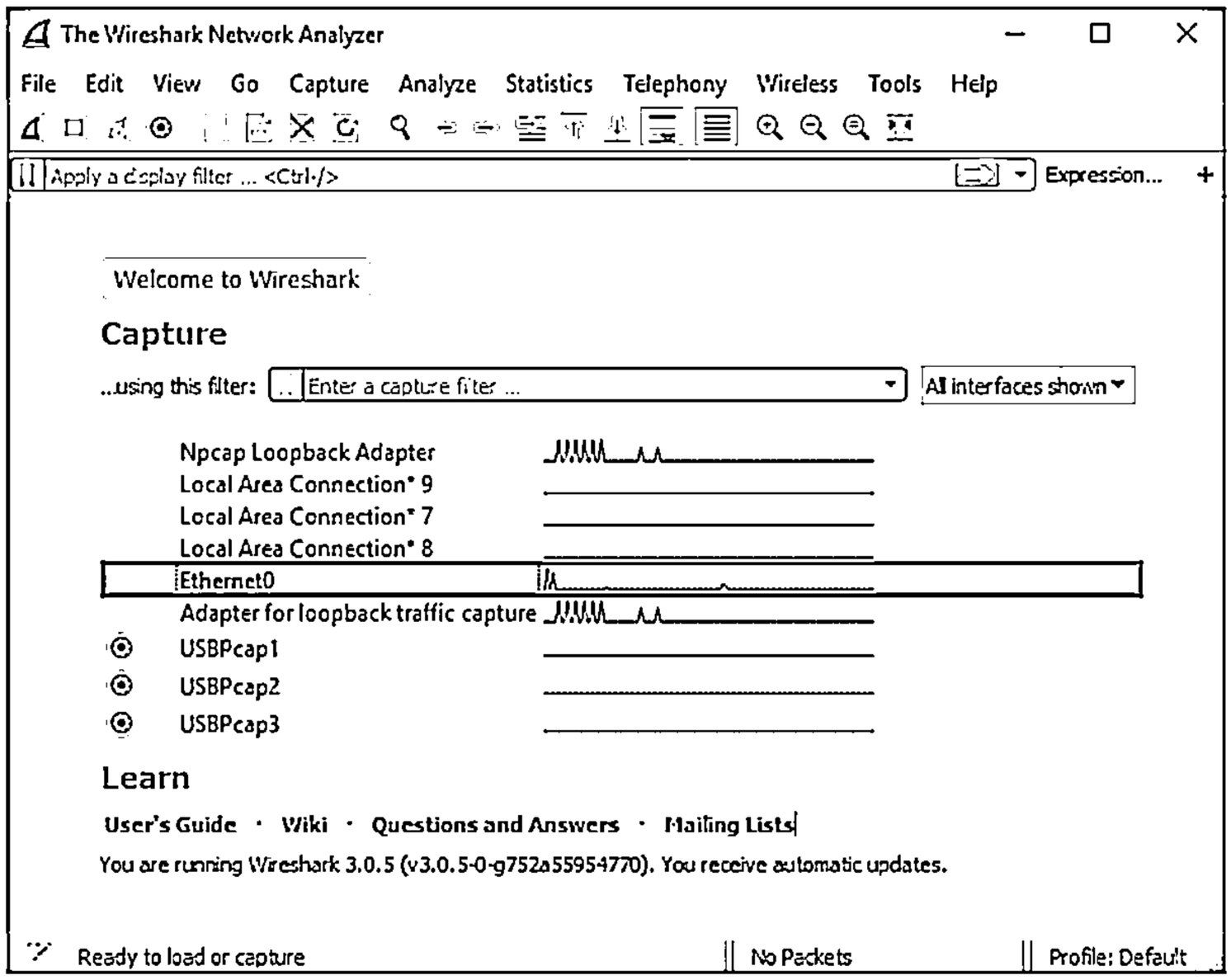


Figure 3.1.5: Wireshark main window, enabling to start the capture

TASK 1.3

Perform Ping on Target Machine (Windows)

12. Open the **Command Prompt**, type **ping 10.10.10.16** and press **Enter**.

Note: **10.10.10.16** is the IP address of the **Windows Server 2016** virtual machine; this may vary in your lab environment.

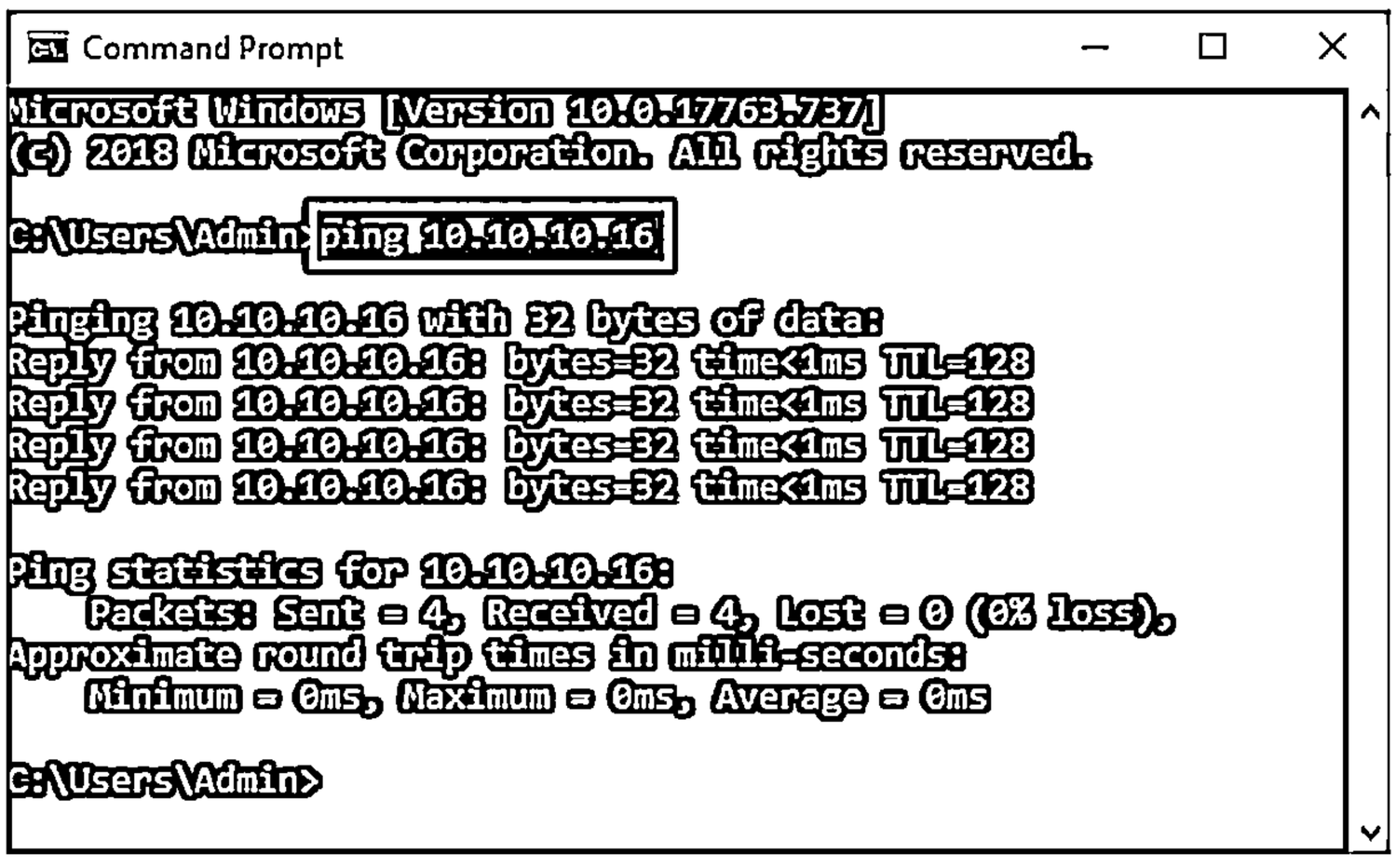


Figure 3.1.6: Sending ICMP requests to Windows Server 2016 virtual machine

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

TASK 1.4

Analyze the TTL Value

13. Observe the packets captured by **Wireshark**.

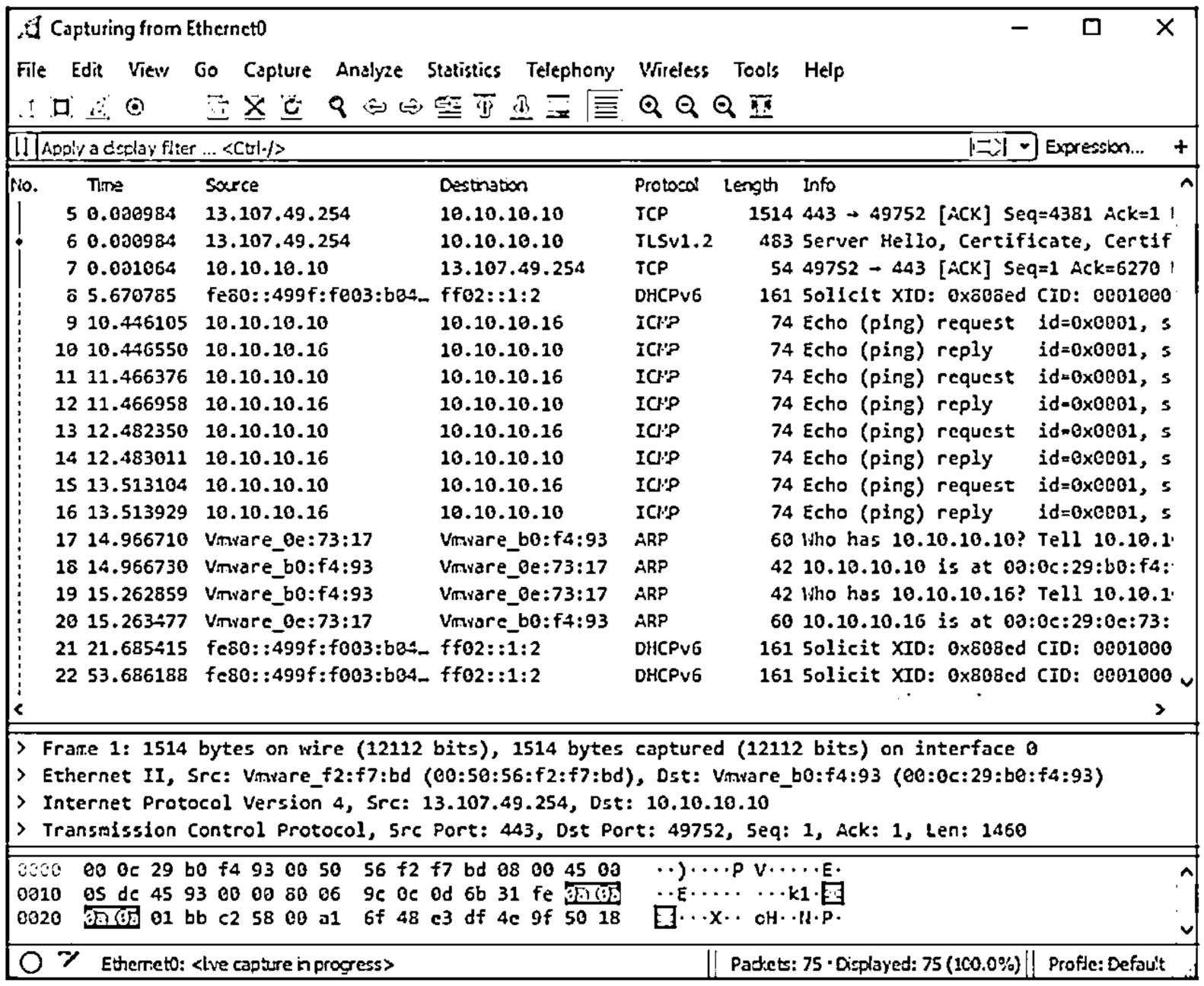


Figure 3.1.7: Packets Captured by Wireshark

14. Choose any packet of the ICMP reply from the **Windows Server 2016** (**10.10.10.16**) to **Windows 10** (**10.10.10.10**) virtual machines and expand the **Internet Protocol Version 4** node in the **Packet Details** pane.

Note: The IP address may vary in your lab environment.

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

15. The TTL value is recorded as **128**, which means that the ICMP reply possibly came from a Windows-based machine.

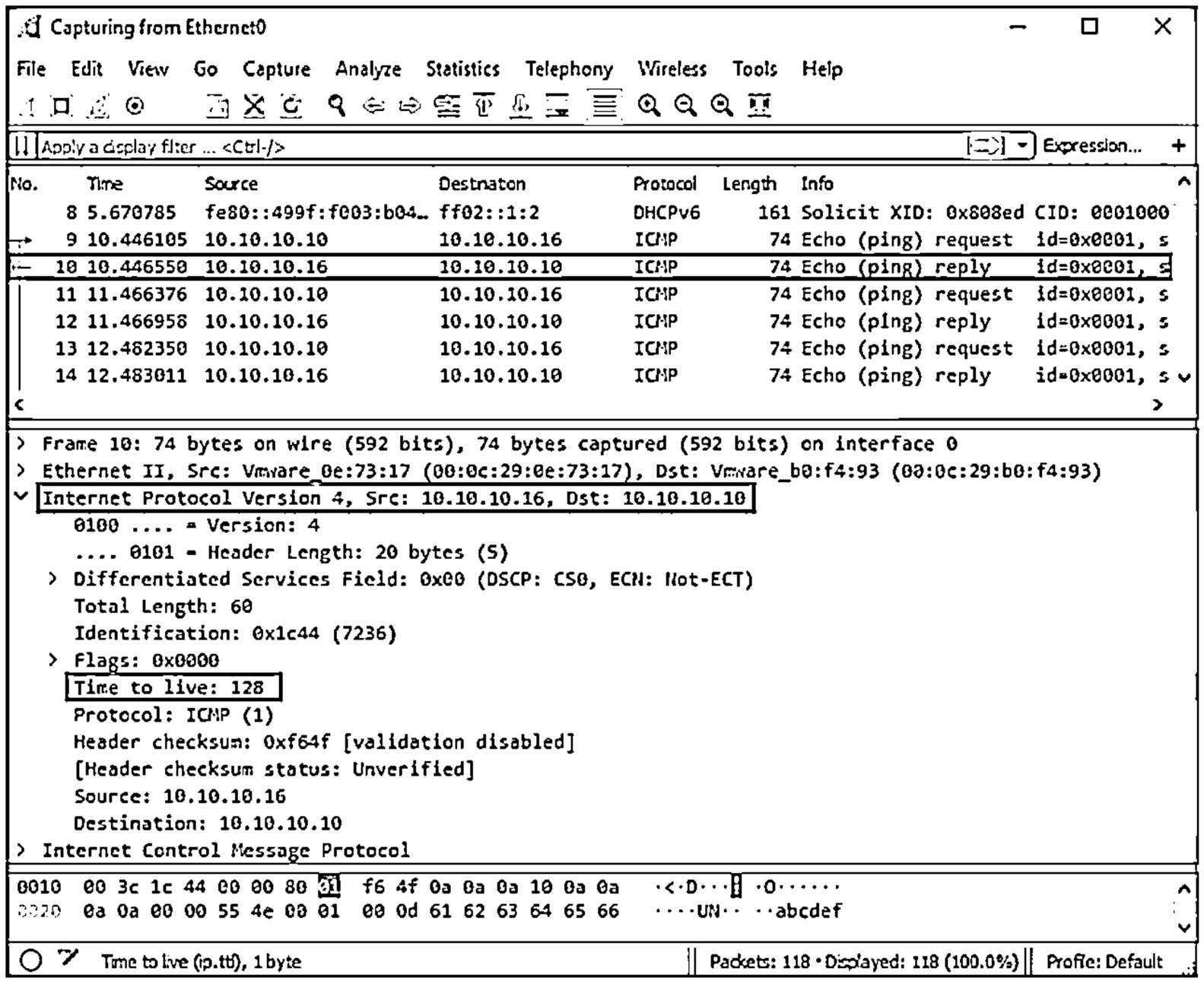


Figure 3.1.8: TTL value detected by Wireshark for Windows Server 2016 virtual machine

16. Now, stop the capture in the **Wireshark** window by clicking on the **Stop** button.

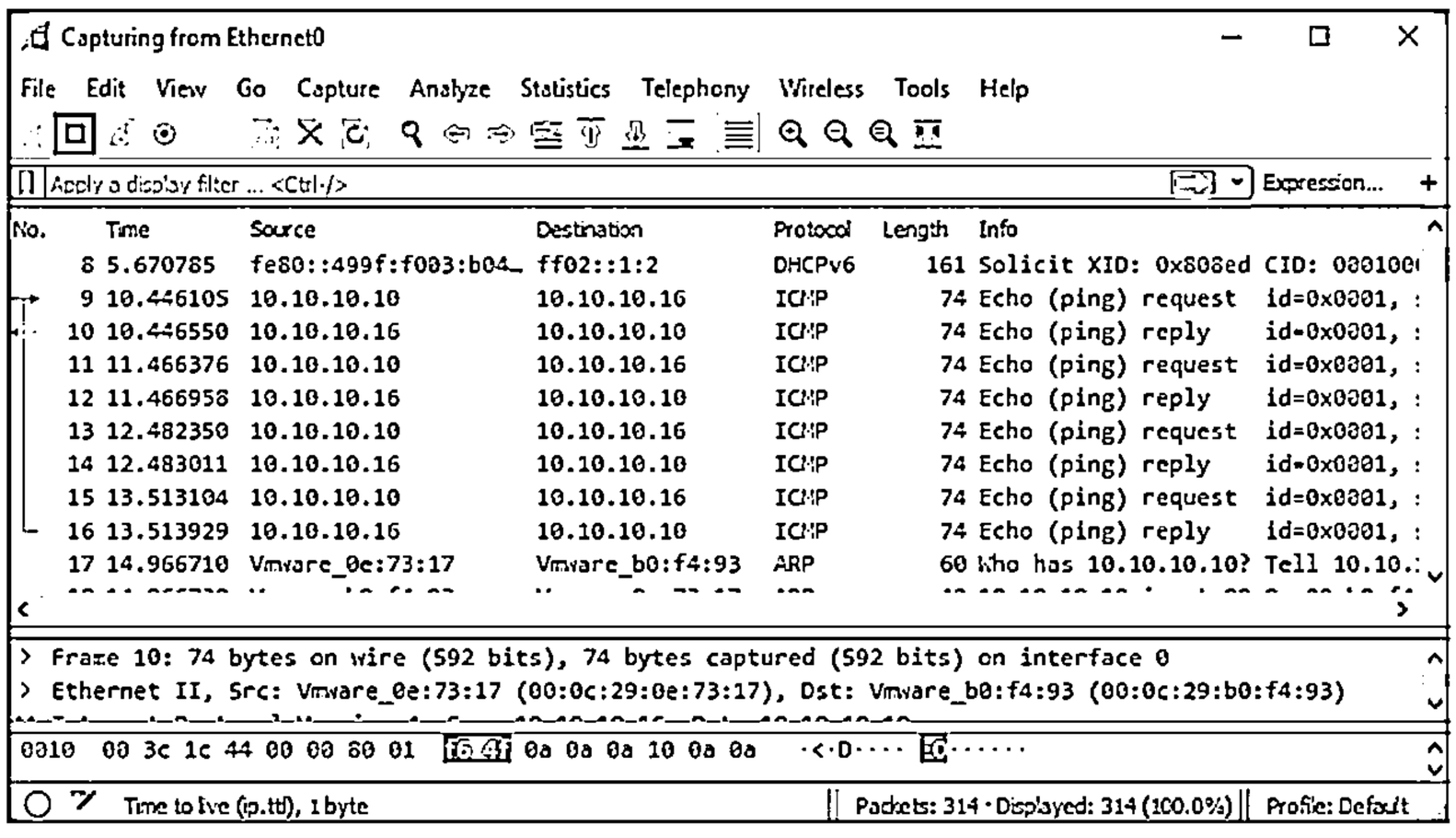


Figure 3.1.9: Stop Live Capture in Wireshark

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

17. Now, click the **Start capturing packets** ( ) button. If an **Unsaved packets...** pop-up appears, click **Continue without Saving**.

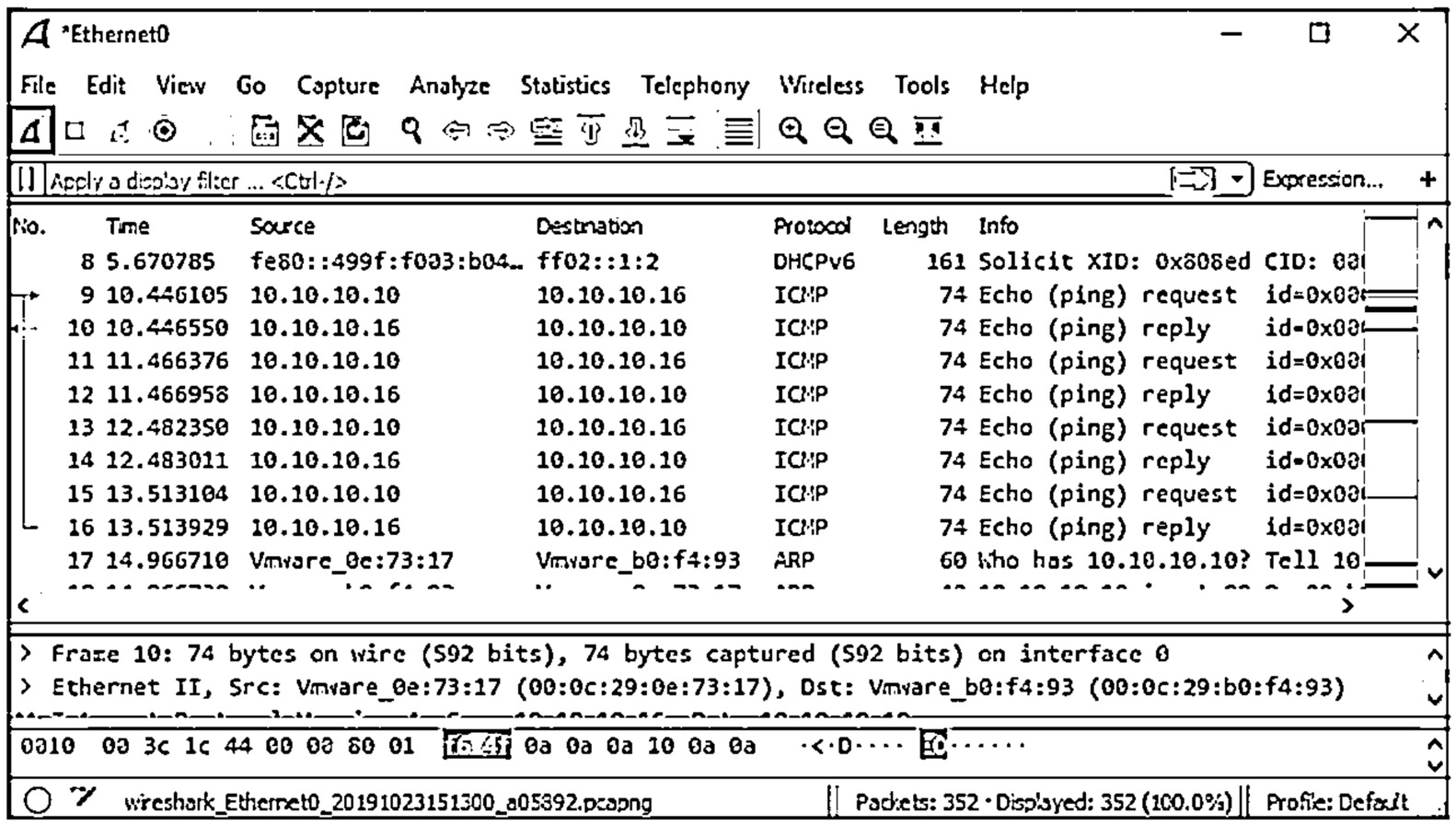


Figure 3.1.10: Start Live Capture in Wireshark

18. Wireshark will start capturing the new packets.

TASK 1.5

Perform Ping on Target Machine (Linux)

19. In the **Command Prompt** window, type **ping 10.10.10.9** and press **Enter**.

Note: **10.10.10.9** is the IP address of the **Ubuntu** virtual machine; this may vary in your lab environment.

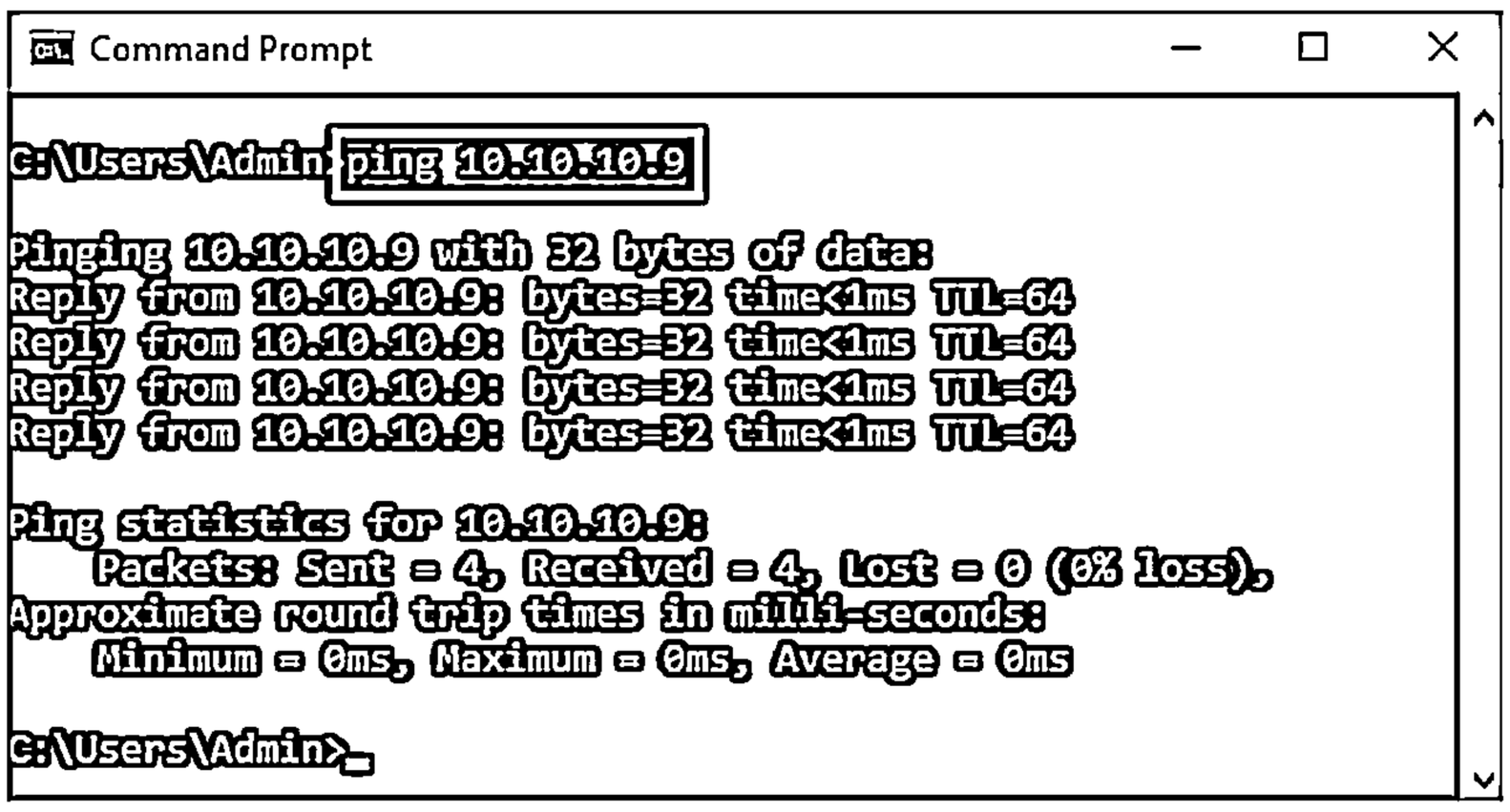


Figure 3.1.11: Sending ICMP requests to Ubuntu virtual machine

20. Observe the packets captured by **Wireshark**.

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

21. Choose any packet of ICMP reply from the **Ubuntu** (**10.10.10.9**) to **Windows 10** (**10.10.10.10**) virtual machine and expand the **Internet Protocol Version 4** node in the **Packet Details** pane.

TASK 1.6

Analyze the TTL Value

Note: The IP address may vary in your lab environment.

22. The TTL value is recorded as **64**, which means the ICMP reply possibly came from a Linux-based machine.

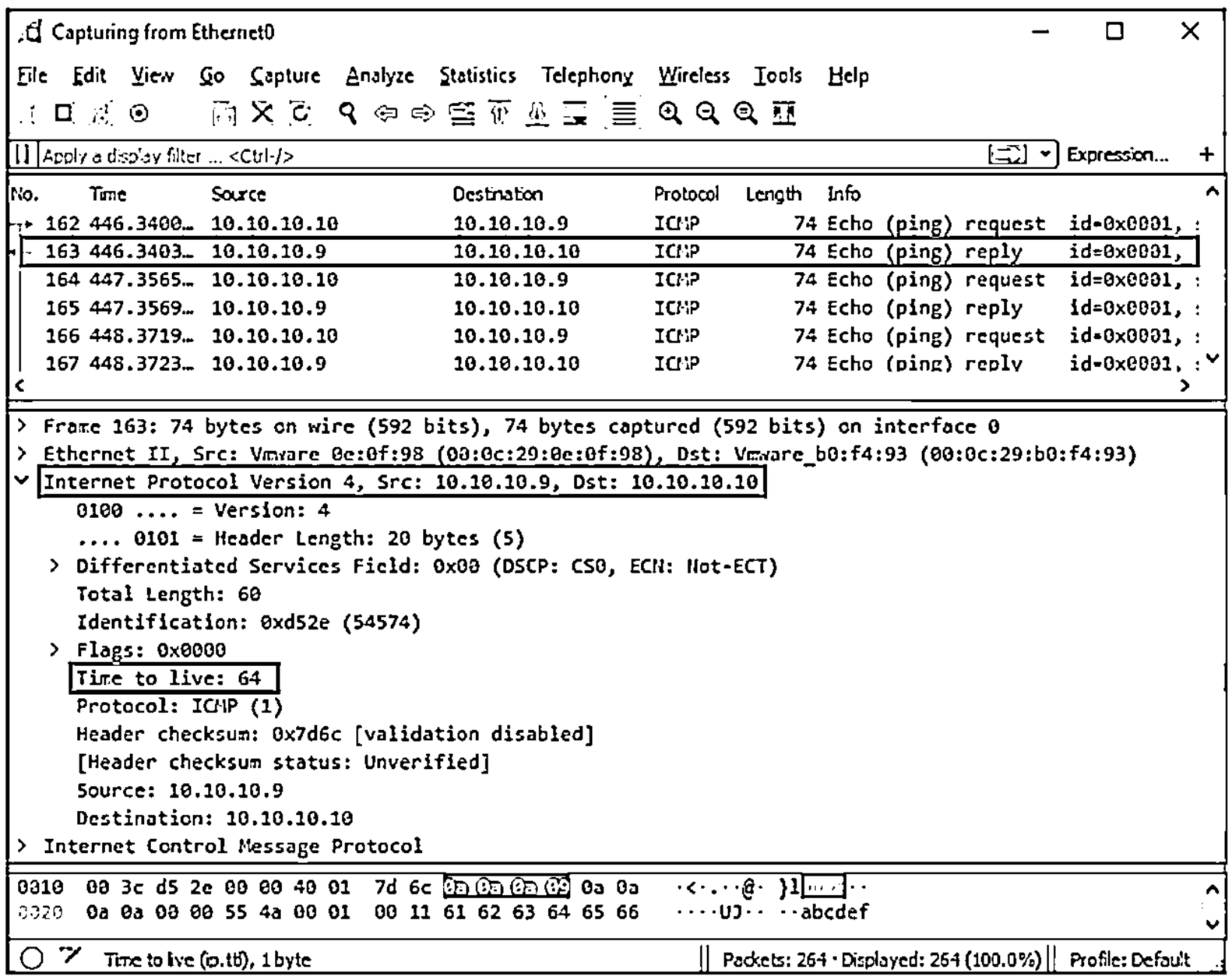


Figure 3.1.12: Time-to-Live value detected by Wireshark for Linux machine

23. Stop the capture in the **Wireshark** window by clicking on the **Stop** button.

24. This concludes the demonstration of identifying the OS of the target system using Wireshark.

25. Close all open windows and document all the acquired information.

26. Turn off the **Ubuntu** virtual machine.

TASK 2 Perform OS Discovery using Nmap Script Engine (NSE)

Here, we will use Nmap to perform OS discovery using -A parameter, -O parameter, and NSE.

Note: Before beginning this lab, ensure that the **Windows 10** and **Windows Server 2016** virtual machines are turned on.

1. In the **Windows 10** virtual machine, click on the **Start** menu and launch **Nmap - Zenmap GUI** from the applications.

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

TASK 2.1

Perform OS Discovery Using -A Parameter (Aggressive Scan)

2. The **Zenmap** GUI appears. In the **Command** field, type the command **nmap -A <Target IP Address>** (here, the target machine is Windows Server 2016 [**10.10.10.16**]) and click **Scan**.

Note: **-A**: to perform an aggressive scan.

3. The scan results appear, displaying the open ports and running services along with their versions and target details such as OS, computer name, NetBIOS computer name, etc. under the **Host script results** section.

Nmap, along with Nmap Script Engine (NSE), can extract considerable valuable information from the target system. In addition to Nmap commands, NSE provides scripts that reveal all sorts of useful information from the target system. Using NSE, you may obtain information such as OS, computer name, domain name, forest name, NetBIOS computer name, NetBIOS domain name, workgroup, system time of a target system, etc.

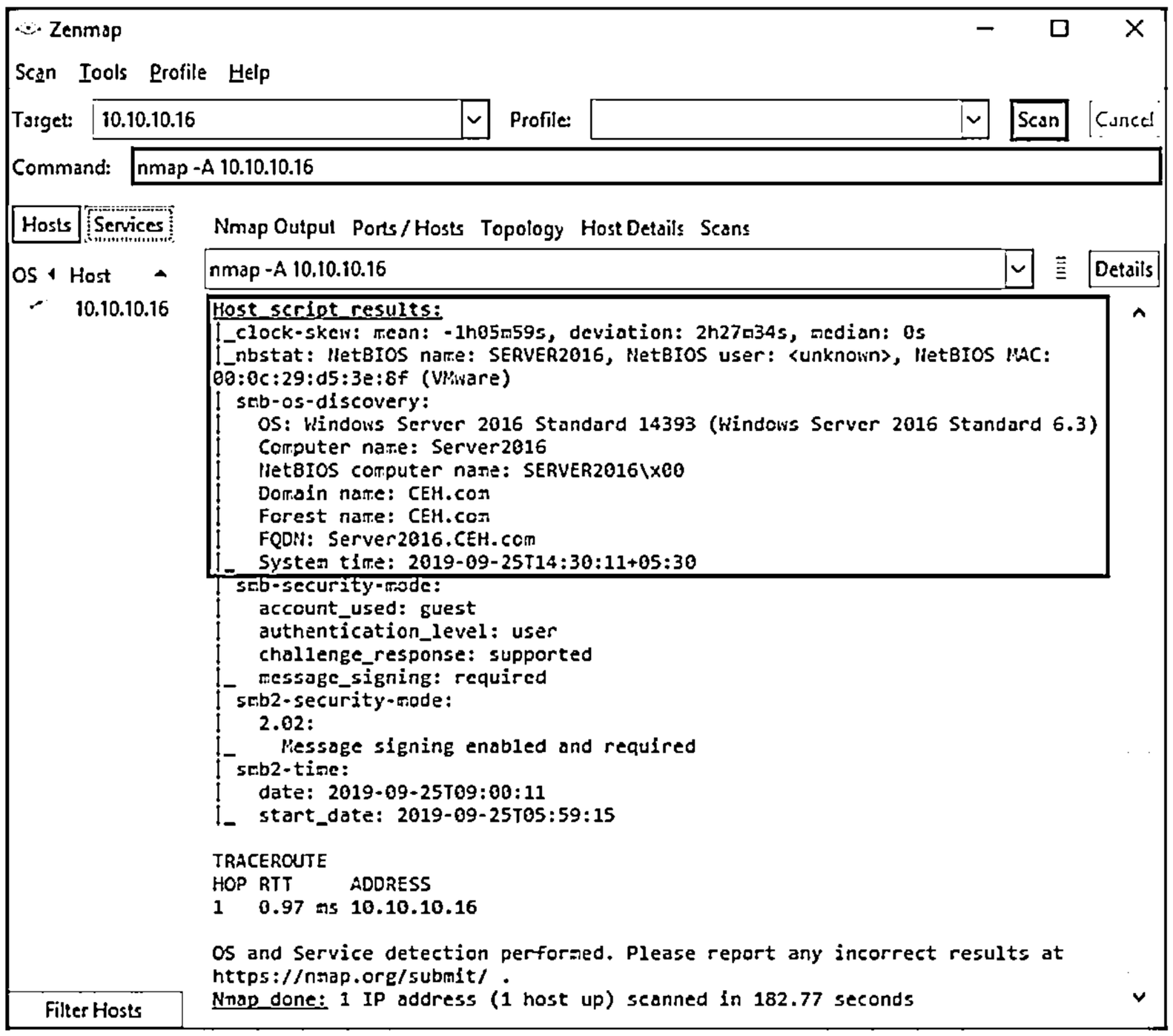


Figure 3.2.1: Zenmap scan results for -A parameter

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

TASK 2.2

Perform OS Discovery Using -O Parameter

4. In the **Command** field, type the command **nmap -O <Target IP Address>** (here, the target machine is Windows Server 2016 [**10.10.10.16**]) and click **Scan**.

Note: **-O**: performs the OS discovery.

5. The scan results appear, displaying information about open ports, respective services running on the open ports, and the name of the OS running on the target system.

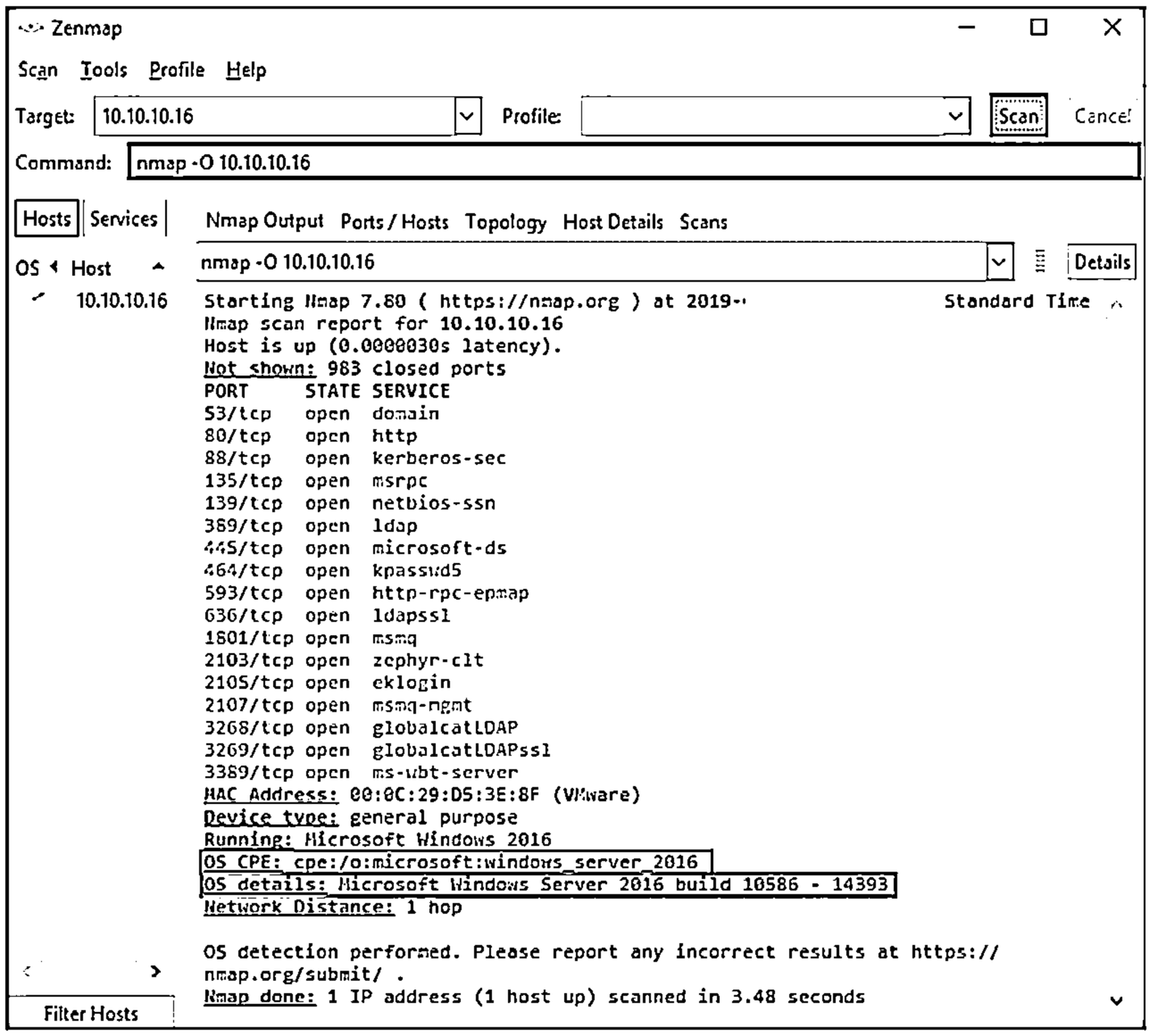


Figure 3.2.2: Zenmap scan results for -O parameter

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

TASK 2.3

Perform OS Discovery Using NSE

6. In the **Command** field, type the command **nmap --script smb-os-discovery.nse <Target IP Address>** (here, the target machine is Windows Server 2016 [**10.10.10.16**]) and click **Scan**.

Note: **--script**: specifies the customized script and **smb-os-discovery.nse**: attempts to determine the OS, computer name, domain, workgroup, and current time over the SMB protocol (ports 445 or 139).

7. The scan results appear, displaying the target OS, computer name, NetBIOS computer name, etc. details under the **Host script results** section.

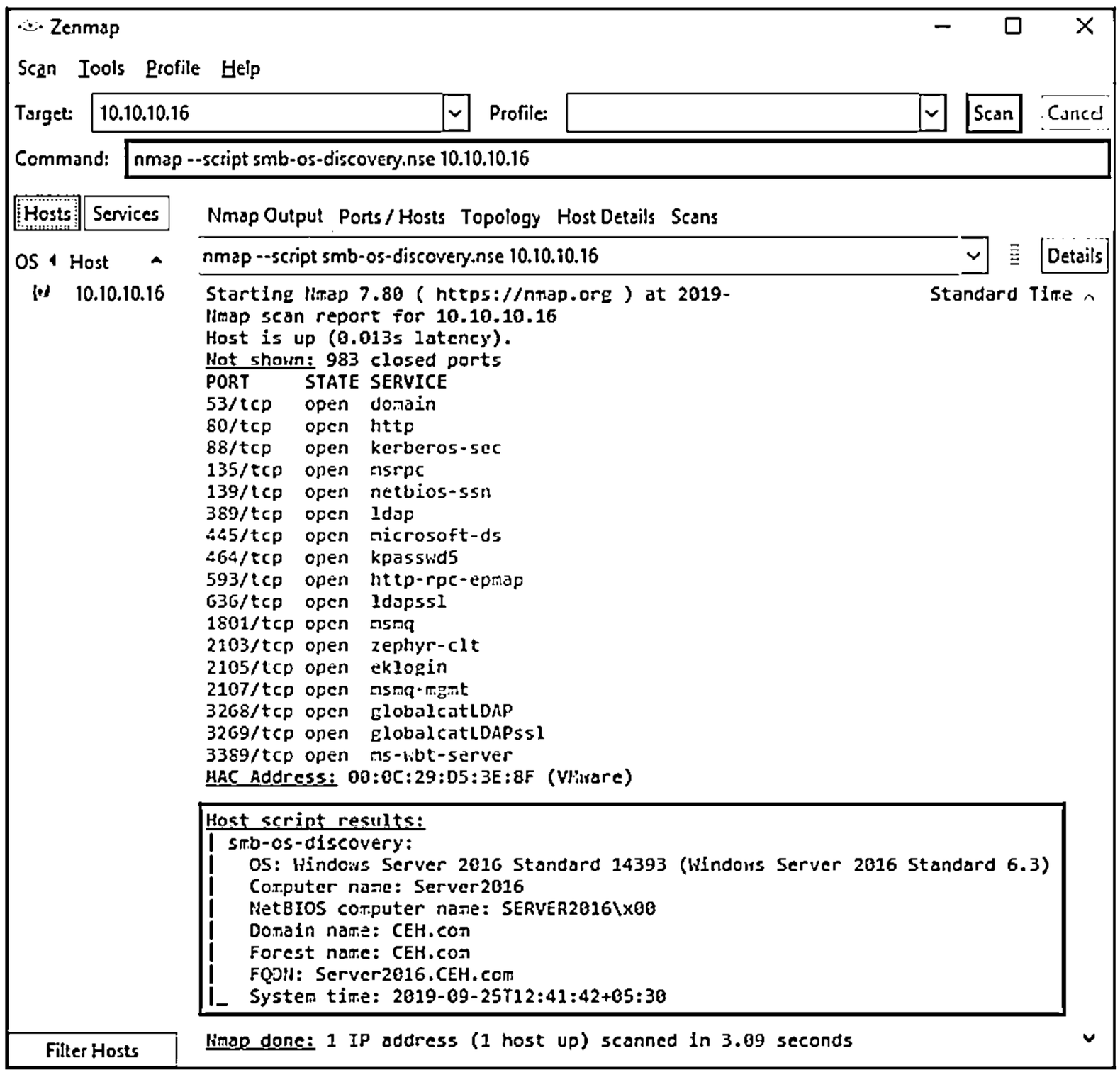


Figure 3.2.3: Zenmap scan results for NSE

8. This concludes the demonstration of discovering the OS running on the target system using Nmap.
9. Close all open windows and document all the acquired information.

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

TASK 3

Unicornscan is a Linux-based command line-oriented network information-gathering and reconnaissance tool. It is an asynchronous TCP and UDP port scanner and banner grabber that enables you to discover open ports, services, TTL values, etc. running on the target machine. In Unicornscan, the OS of the target machine can be identified by observing the TTL values in the acquired scan result.

Perform OS Discovery using Unicornscan

Here, we will use the Unicornscan tool to perform OS discovery on the target system.

1. Before beginning this lab, turn on the **Parrot Security** and **Ubuntu** virtual machine.

Note: Ensure that the **Windows Server 2016** virtual machine is also running.

2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

6. Now, type **cd** and press **Enter** to jump to the root directory.

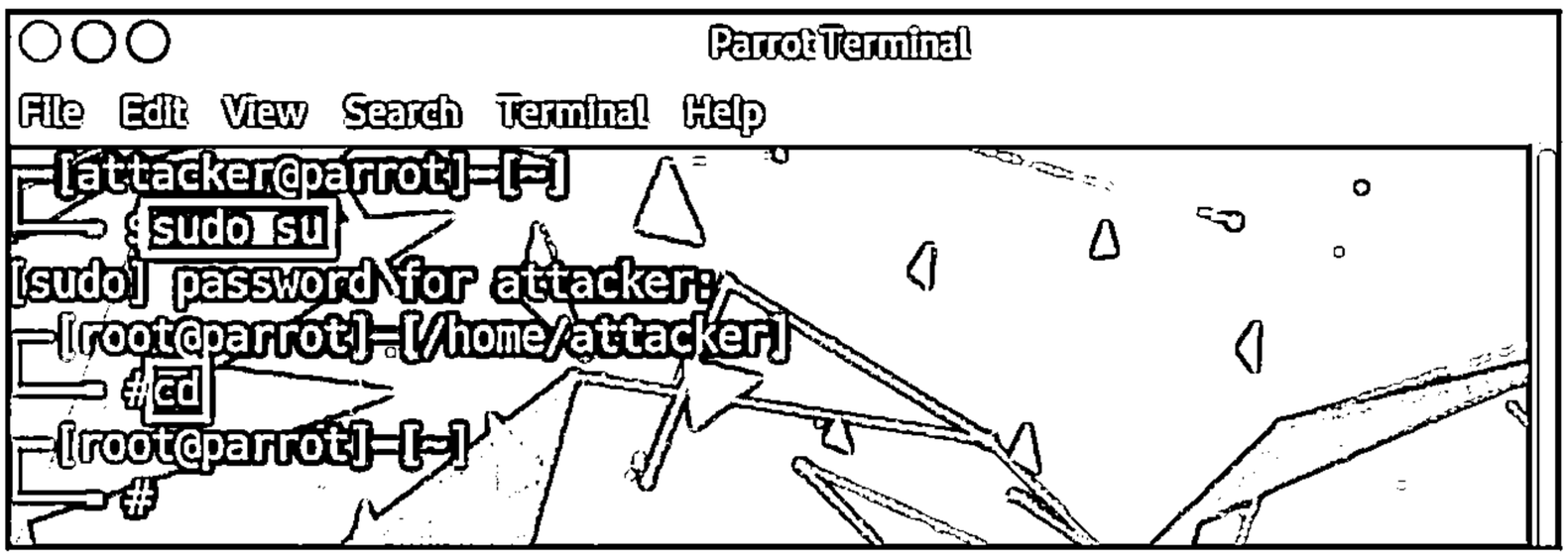


Figure 3.3.1: Running the programs as a root user

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

TASK 3.1

Perform OS Discovery on Windows-based Machine

7. In the terminal window, type **unicornscan <Target IP Address> -Iv** (here, the target machine is Windows Server 2016 [**10.10.10.16**]) and press **Enter**.

Note: In this command, -I specifies an immediate mode and **v** specifies a verbose mode.

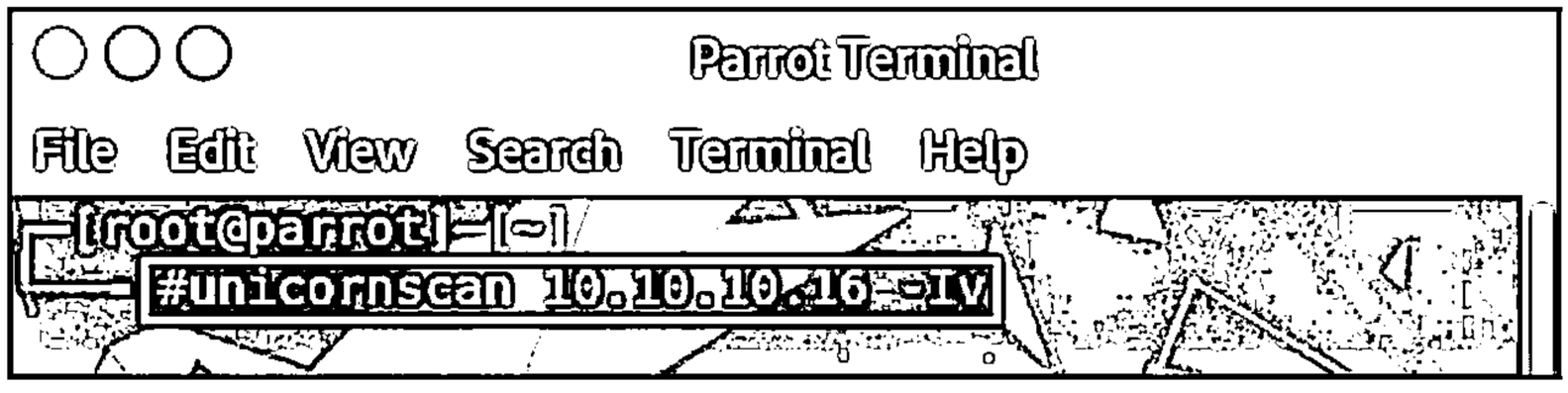


Figure 3.3.2: Unicornscan OS discovery command

8. The scan results appear, displaying the open TCP ports along with the obtained TTL value of **128**. As shown in the screenshot, the **ttl** values acquired after the scan are **128**; hence, the OS is possibly Microsoft Windows (Windows 7/8/8.1/10 or Windows Server 2008/12/16).

Note: Here, the target machine is **Windows Server 2016** (10.10.10.16).

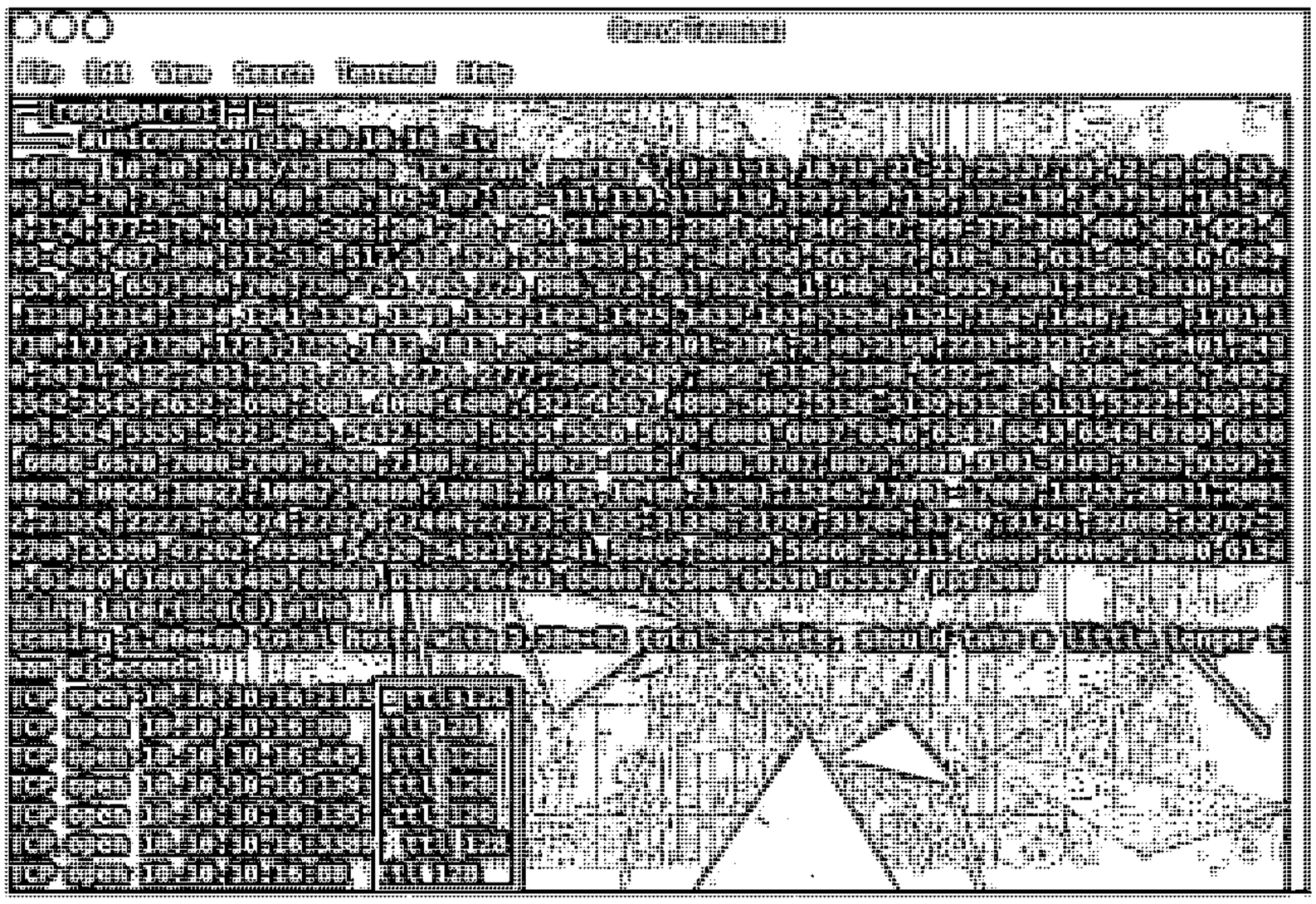


Figure 3.3.3: Unicornscan OS discovery command result Windows-based virtual machine

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

TASK 3.2

Perform OS Discovery on Linux-based Machine

9. In the **Parrot Terminal** window, type **unicornscan <Target IP Address> -Iv** (here, the target machine is Ubuntu [**10.10.10.9**]) and press **Enter**.
10. The scan results appear, displaying the open TCP ports along with a TTL value of **64**. As shown in the screenshot, the **ttl** value acquired after the scan is **64**; hence, the OS is possibly a Linux-based machine (Google Linux, Ubuntu, Parrot, or Kali).

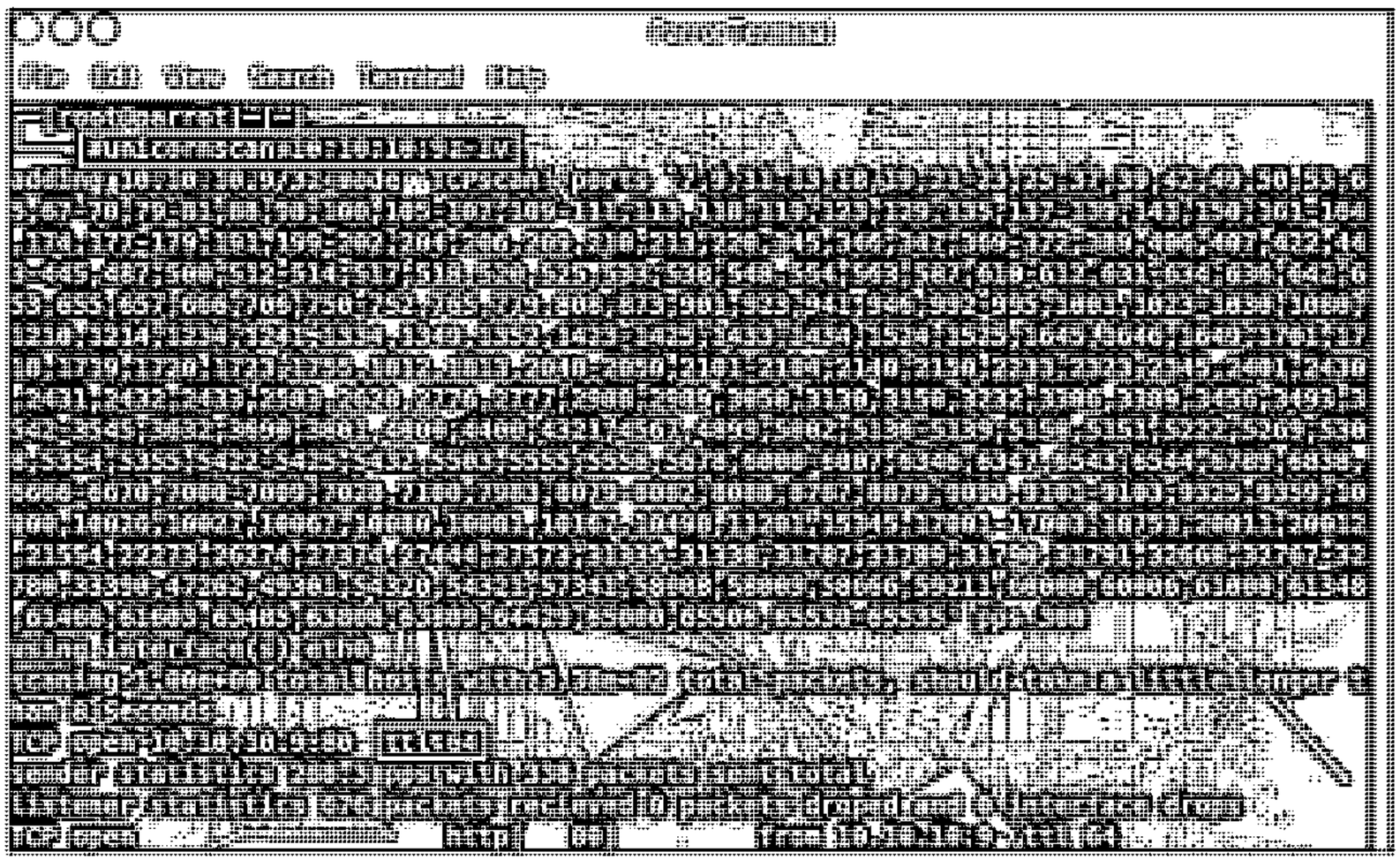


Figure 3.3.4: Unicornscan OS discovery command result for Linux-based virtual machine

11. This concludes the demonstration of discovering the OS of the target machine using Unicornscan.
12. Close all open windows and document all the acquired information.
13. Turn off the **Windows 10**, **Parrot Security**, **Windows Server 2016**, and **Ubuntu** virtual machines.

Lab Analysis

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

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT 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

Scan beyond IDS and Firewall

Scanning beyond IDS and firewall is a process of sending intended packets to the target system in order to exploit IDS/firewall limitations.

ICON KEY

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

Lab Scenario

As a professional ethical hacker or a pen tester, the next step after discovering the OS of the target IP address(es) is to perform network scanning without being detected by the network security perimeters such as the firewall and IDS. IDSs and firewalls are efficient security mechanisms; however, they still have some security limitations. You may be required to launch attacks to exploit these limitations using various IDS/firewall evasion techniques such as packet fragmentation, source routing, IP address spoofing, etc. Scanning beyond the IDS and firewall allows you to evaluate the target network's IDS and firewall security.

Lab Objectives

- Scan beyond IDS/firewall using various evasion techniques
- Create custom packets using Colasoft Packet Builder to scan beyond the IDS/firewall
- Create custom UDP and TCP packets using Hping3 to scan beyond the IDS/firewall
- Create custom packets using Nmap to scan beyond the IDS/firewall
- Browse anonymously using Proxy Switcher
- Browse anonymously using CyberGhost VPN

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2016 virtual machine
- Parrot Security virtual machine
- Ubuntu virtual machine

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

- Web browsers with an Internet connection
- Administrator privileges to run the tools
- Colasoft Packet Builder located at **E:\CEH-Tools\CEHv11 Module 03 Scanning Networks\Packet Crafting Tools\Colasoft Packet Builder**
- Proxy Switcher located at **E:\CEH-Tools\CEHv11 Module 03 Scanning Networks\Proxy Tools\Proxy Switcher**
- CyberGhost VPN located at **E:\CEH-Tools\CEHv11 Module 03 Scanning Networks\Proxy Tools\CyberGhost VPN**
- You can also download the latest version of the above-mentioned tools from their official websites. If you decide to download the latest version, the screenshots shown in the lab might differ.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 03 Scanning Networks

Lab Duration

Time: 45 Minutes

Overview of Scanning beyond IDS and Firewall

An Intrusion Detection System (IDS) and firewall are the security mechanisms intended to prevent an unauthorized person from accessing a network. However, even IDSs and firewalls have some security limitations. Firewalls and IDSs intend to avoid malicious traffic (packets) from entering into a network, but certain techniques can be used to send intended packets to the target and evade IDSs/firewalls.

Techniques to evade IDS/firewall:

- **Packet Fragmentation**: Send fragmented probe packets to the intended target, which re-assembles it after receiving all the fragments
- **Source Routing**: Specifies the routing path for the malformed packet to reach the intended target
- **Source Port Manipulation**: Manipulate the actual source port with the common source port to evade IDS/firewall
- **IP Address Decoy**: Generate or manually specify IP addresses of the decoys so that the IDS/firewall cannot determine the actual IP address
- **IP Address Spoofing**: Change source IP addresses so that the attack appears to be coming in as someone else
- **Creating Custom Packets**: Send custom packets to scan the intended target beyond the firewalls
- **Randomizing Host Order**: Scan the number of hosts in the target network in a random order to scan the intended target that is lying beyond the firewall
- **Sending Bad Checksums**: Send the packets with bad or bogus TCP/UPD checksums to the intended target
- **Proxy Servers**: Use a chain of proxy servers to hide the actual source of a scan and evade certain IDS/firewall restrictions

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

- **Anonymizers:** Use anonymizers that allow them to bypass Internet censors and evade certain IDS and firewall rules

Lab Tasks

TASK 1 — Scan beyond IDS/Firewall using various Evasion Techniques

Here, we will use Nmap to evade IDS/firewall using various techniques such as packet fragmentation, source port manipulation, MTU, and IP address decoy.

1. Turn on the **Windows 10** and **Parrot Security** virtual machines.

Note: In this lab, we are using the **Parrot Security** (10.10.10.13) virtual machine as a host machine and the **Windows 10** (10.10.10.10) virtual machine as a target machine.

2. In the **Windows 10** virtual machine, log in with the credentials **Admin/Pa$$w0rd**.

TASK 1.1

Turn on Windows Defender Firewall

3. Navigate to **Control Panel → System and Security → Windows Defender Firewall → Turn Windows Defender Firewall on or off**, enable Windows Defender Firewall and click **OK**, as shown in the screenshot.

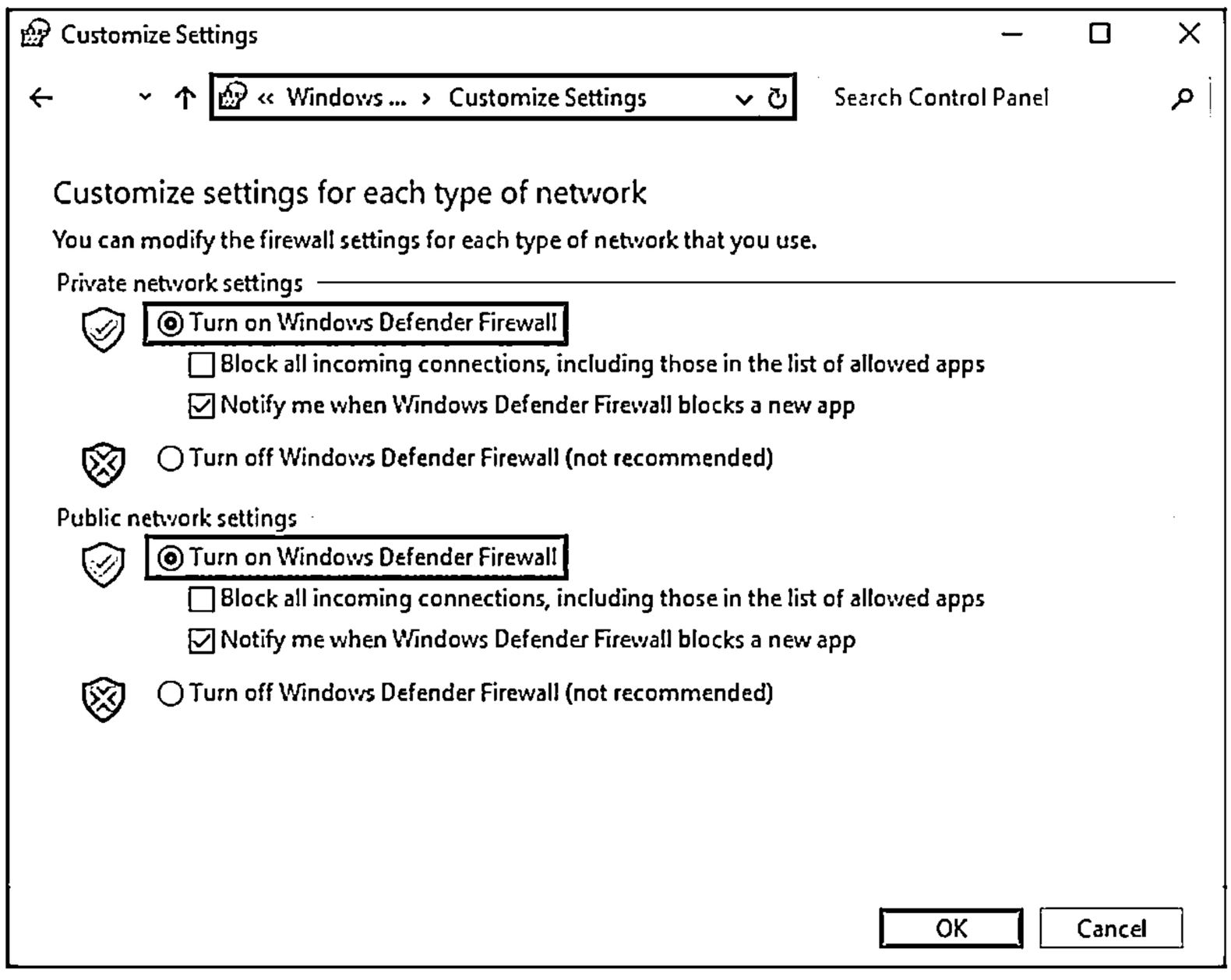


Figure 4.1.1: Turn on Windows Defender Firewall

4. Click on the **Start** menu and launch **Wireshark** from the applications. Start capturing packets by double-clicking the available ethernet or interface (here, **Ethernet0**).

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

Note: In this lab, the available interface might vary in your lab environment.

Nmap offers many features to help understand complex networks with enabled security mechanisms and supports mechanisms for bypassing poorly implemented defenses. Using Nmap, various techniques can be implemented, which can bypass the IDS/firewall security mechanisms.

5. Now, switch to the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

6. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
7. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
8. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

9. Now, type **cd** and press **Enter** to jump to the root directory.

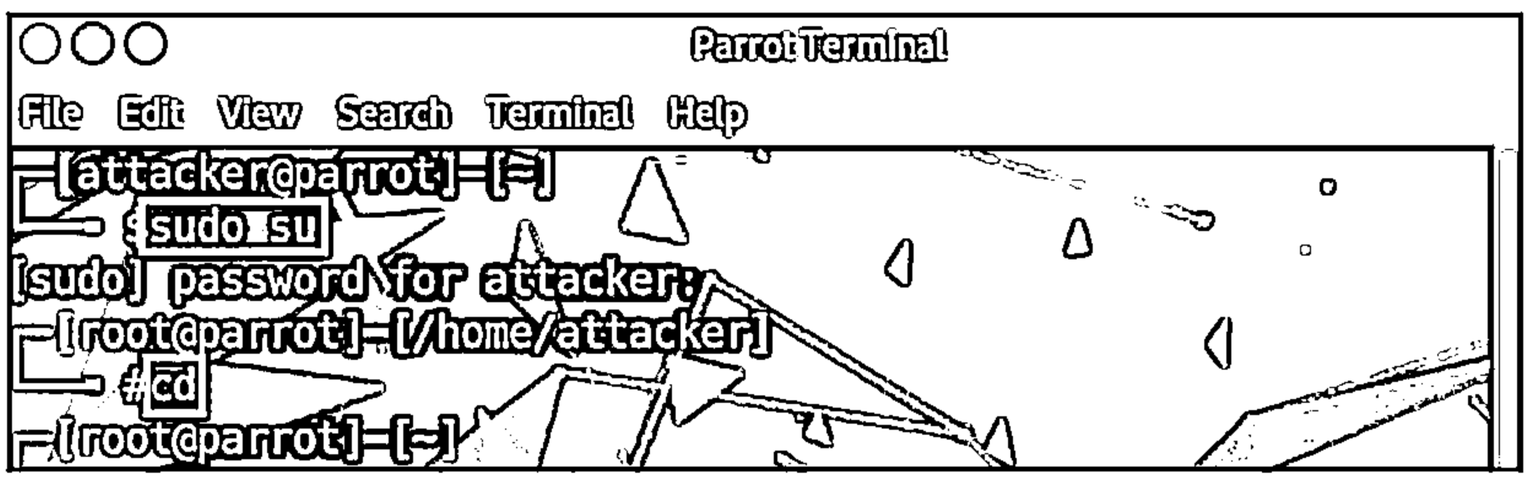


Figure 4.1.2: Running the programs as a root user

10. In the terminal window, type **nmap -f <Target IP Address>**, (here, the target machine is Windows 10 [**10.10.10.10**]) and press **Enter**.

Note: **-f** switch is used to split the IP packet into tiny fragment packets.

TASK 1.2

Perform Packet Fragmentation

Note: Packet fragmentation refers to the splitting of a probe packet into several smaller packets (fragments) while sending it to a network. When these packets reach a host, IDSs and firewalls behind the host generally queue all of them and process them one by one. However, since this method of processing involves greater CPU consumption as well as network resources, the configuration of most of IDSs makes it skip fragmented packets during port scans.

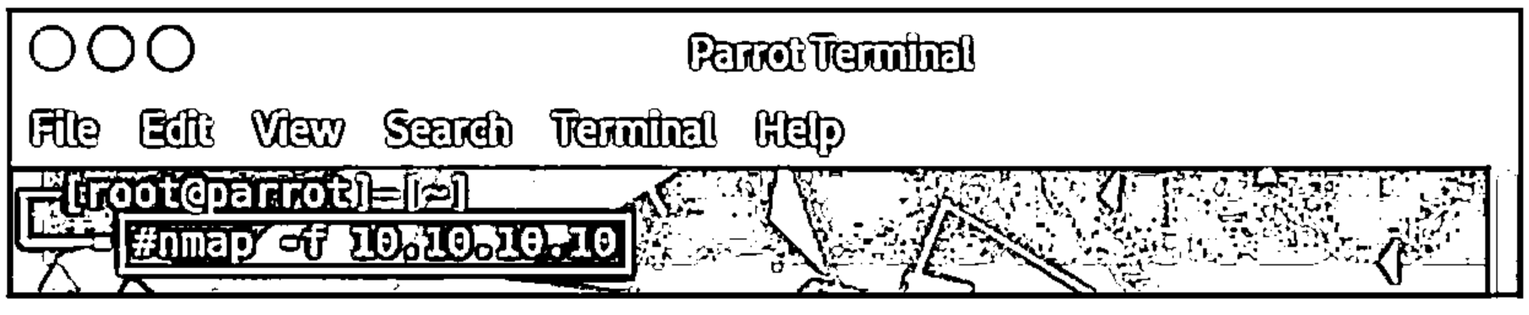


Figure 4.1.3: Nmap fragment scan

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

11. Although **Windows Defender Firewall** is turned on in the target system (here, **Windows 10**), you can still obtain the results displaying all open TCP ports along with the name of services running on the ports, as shown in the screenshot.

Note: Depending upon the target machine that you are using, the results might vary in your lab environment.

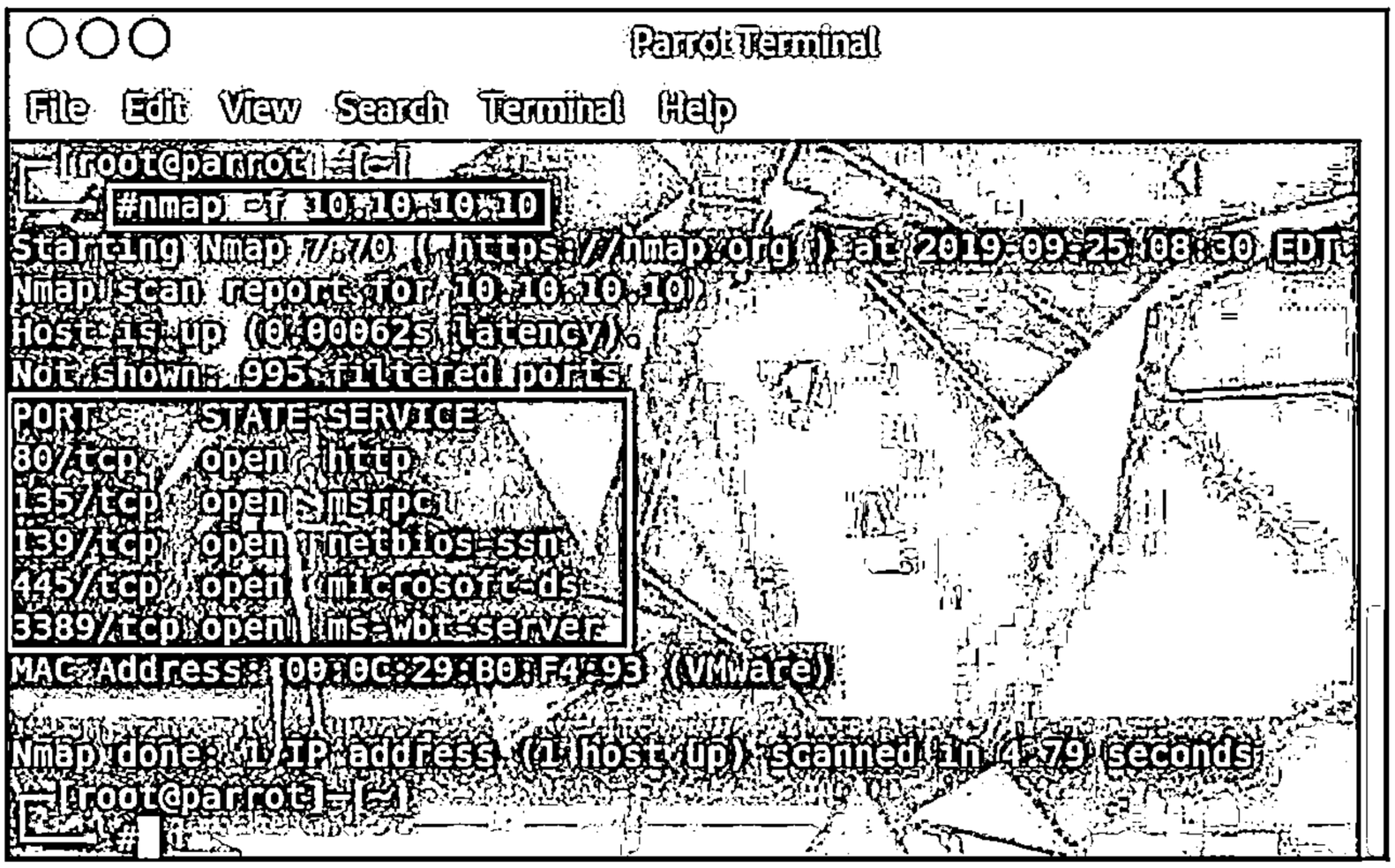


Figure 4.1.4: Nmap fragment scan output

TASK 1.3

Perform Source Port Manipulation

12. In the **Parrot Terminal** window, type **nmap -g 80 <Target IP Address>**, (here, target IP address is **10.10.10.10**) and press **Enter**.

Note: In this command, you can use the **-g** or **--source-port** option to perform source port manipulation.

Note: Source port manipulation refers to manipulating actual port numbers with common port numbers to evade IDS/firewall: this is useful when the firewall is configured to allow packets from well-known ports like HTTP, DNS, FTP, etc.

13. The results appear, displaying all open TCP ports along with the name of services running on the ports, as shown in the screenshot.

Note: Depending upon the target machine that you are using, the results might vary in your lab environment.

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

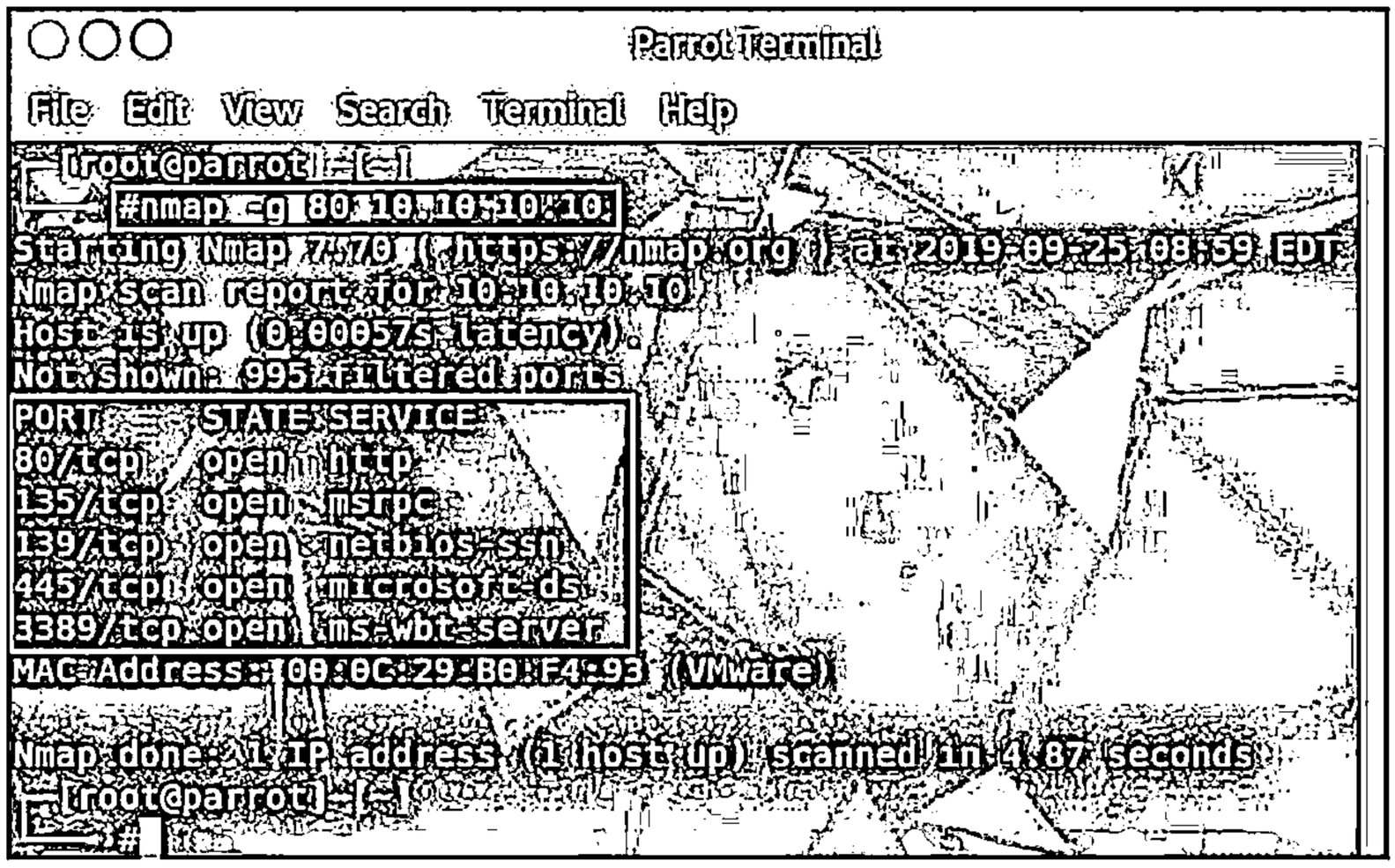


Figure 4.1.5: Nmap source port manipulation scan output

TASK 1.4

Perform Maximum Transmission Unit

14. Now, type **nmap -mtu 8 <Target IP Address>** (here, target IP address is **10.10.10.10**) and press **Enter**.

Note: In this command, **-mtu**: specifies the number of Maximum Transmission Unit (MTU) (here, **8** bytes of packets).

Note: Using MTU, smaller packets are transmitted instead of sending one complete packet at a time. This technique evades the filtering and detection mechanism enabled in the target machine.

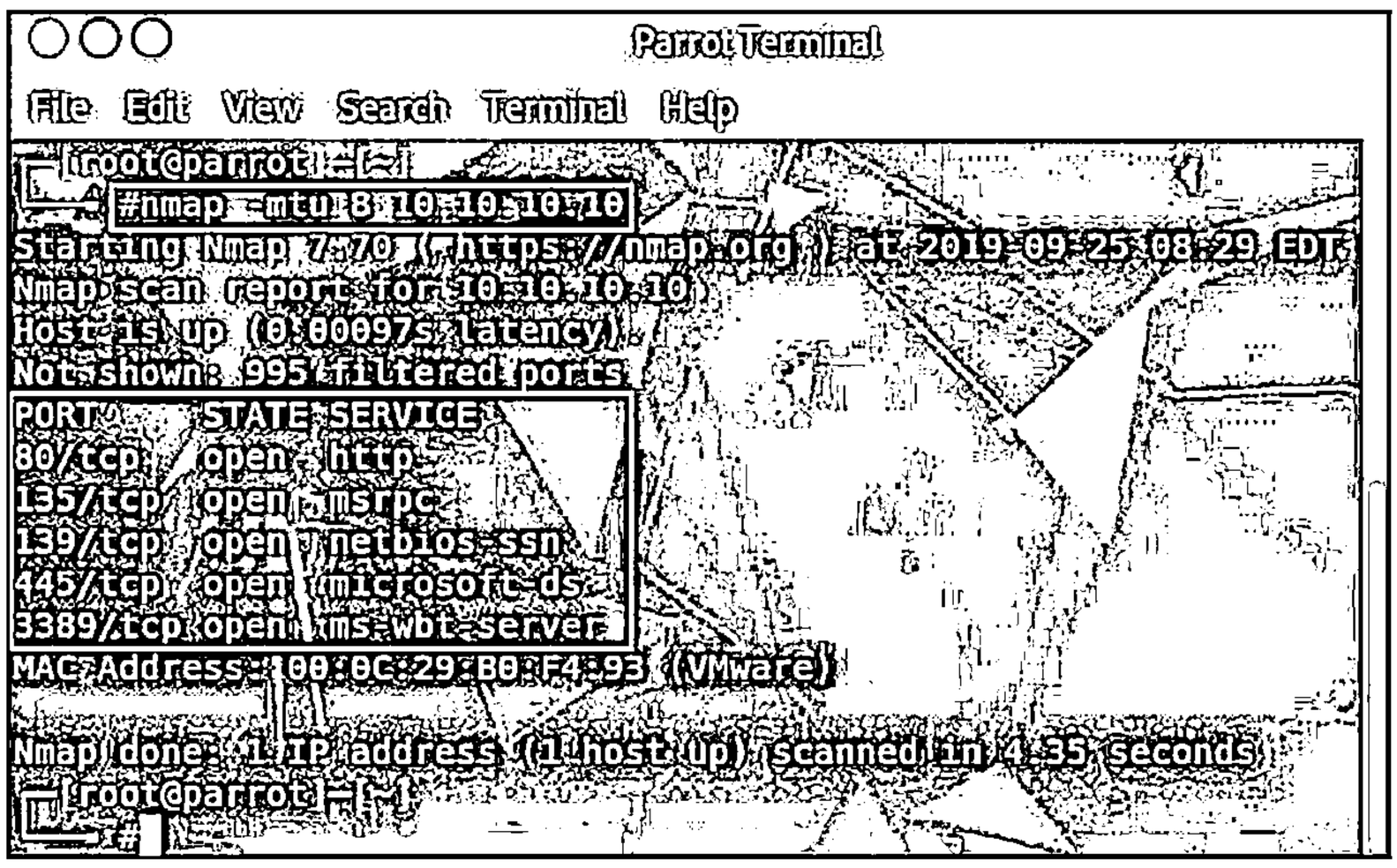


Figure 4.1.6: Nmap Maximum Transmission Unit scan

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

TASK 1.5

Perform IP Address Decoy

15. Now, type **nmap -D RND:10 <Target IP Address>** (here, target IP address is **10.10.10.10**) and press **Enter**.

Note: In this command, **-D**: performs a decoy scan and **RND**: generates a random and non-reserved IP addresses.

Note: The IP address decoy technique refers to generating or manually specifying IP addresses of the decoys to evade IDS/firewall. This technique makes it difficult for the IDS/firewall to determine which IP address was actually scanning the network and which IP addresses were decoys.

By using this command, Nmap automatically generates a random number of decoys for the scan and randomly positions the real IP address between the decoy IP addresses.

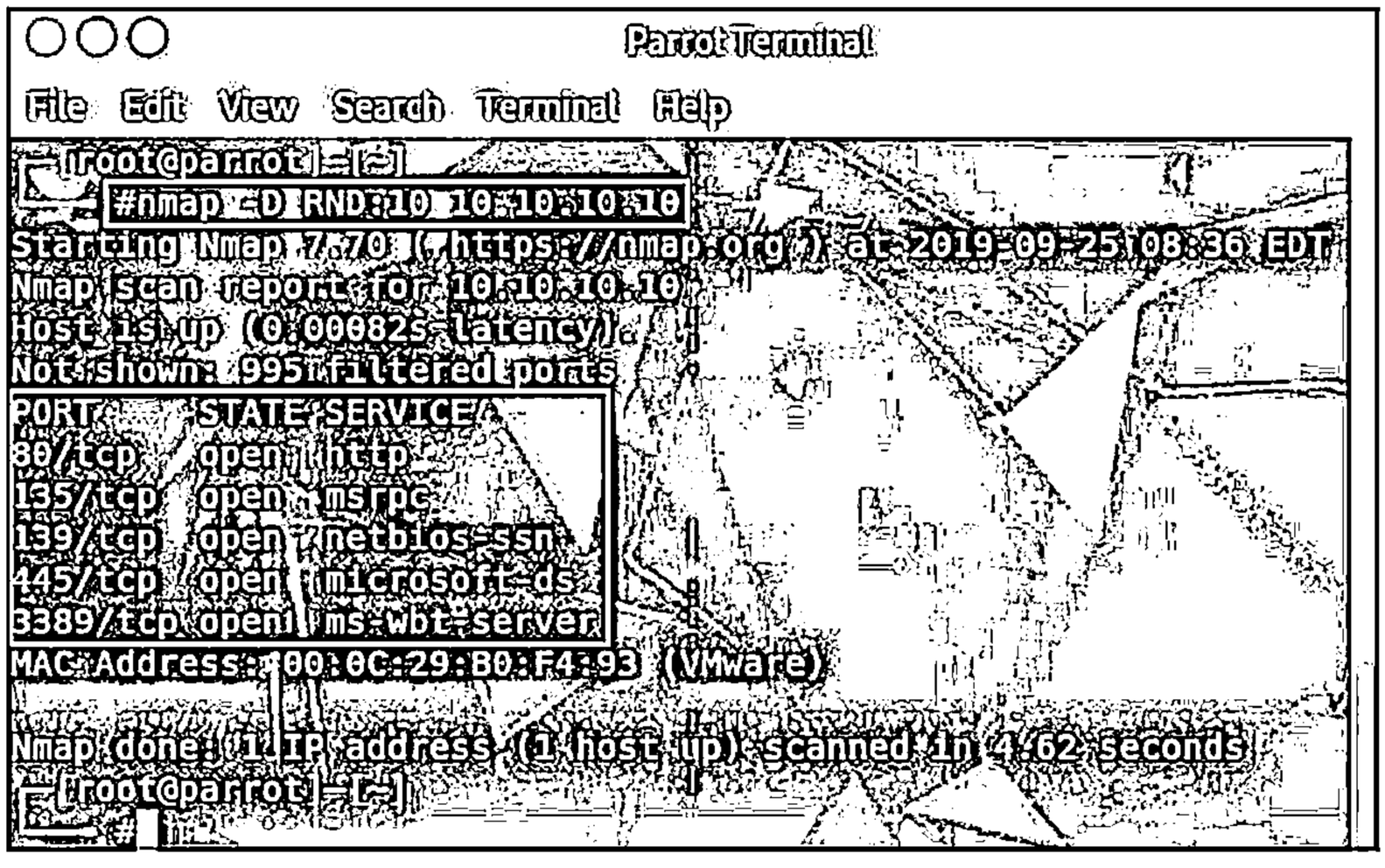


Figure 4.1.7: Nmap Decoying IP Addresses

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

16. Now, return to the **Windows 10** virtual machine (target machine) and observe packets captured by Wireshark, which displays the multiple IP addresses in the source section, as shown in the screenshot.

Note: The results may vary in your lab environment.

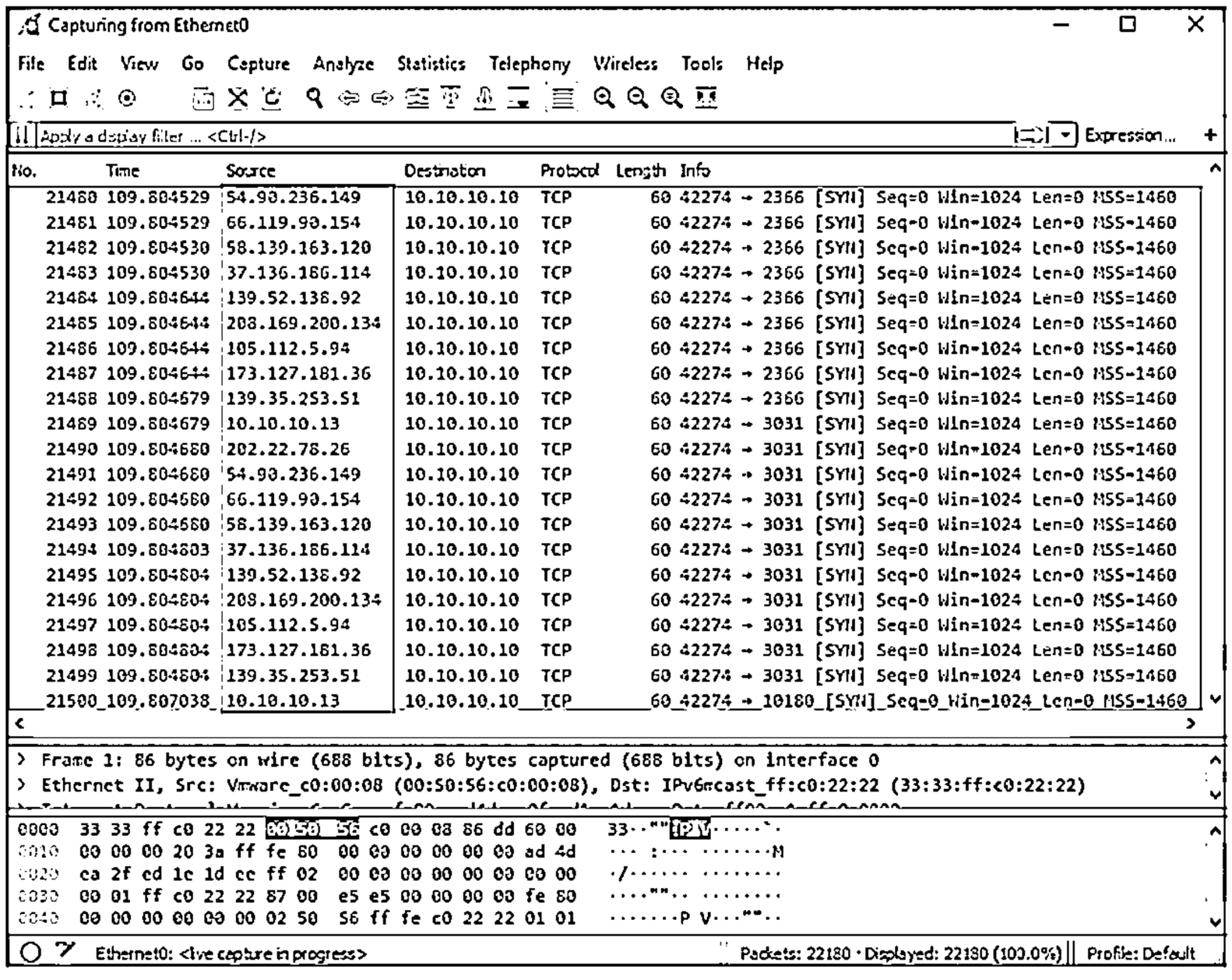


Figure 4.1.8: Decoyed IP Addresses in Windows 10 Wireshark

17. This concludes the demonstration of evading IDS and firewall using various evasion techniques in Nmap.
18. Close all open windows and document all the acquired information.
19. Turn off the **Parrot Security** virtual machine.

TASK 2 Create Custom Packets using Colasoft Packet Builder to Scan beyond IDS/Firewall

Here, we will use the Colasoft Packet Builder tool to create custom TCP packets to scan the target host by bypassing the IDS/firewall.

1. Turn on the **Windows Server 2019** virtual machine and log in with the credentials **Administrator/Pa$$w0rd**.
2. Install **Wireshark** available at **Z:\CEHv11 Module 03 Scanning Networks\Banner Grabbing Tools\Wireshark** with all the default settings.
3. **Windows Server 2019** virtual machine will restart. Log in with the credentials **Administrator/Pa$$w0rd**.

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

4. Click on the **Start** menu and launch **Wireshark** from the applications.
5. The **Wireshark Network Analyzer** main window appears; double-click the available ethernet or interface (here, **Ethernet0**) to start the packet capture.

TASK 2.1

Install Colasoft Packet Builder

6. Navigate to **Z:\CEHv11 Module 03 Scanning Networks\Packet Crafting Tools\Colasoft Packet Builder** and double-click **pktbuilder_2.0.0.212.exe**.
7. Follow the wizard-driven installation steps to install **Colasoft Packet Builder**.
8. After the completion of the installation, click on the **Launch Colasoft Packet Builder 2.0** checkbox and click **Finish**.

Colasoft Packet Builder is a tool that allows you to create custom network packets to assess network security. You can also select a TCP packet from the provided templates and change the parameters in the decoder editor, hexadecimal editor, or ASCII editor to create a packet. In addition to building packets, the Colasoft Packet Builder supports saving packets to packet files and sending packets to the network.

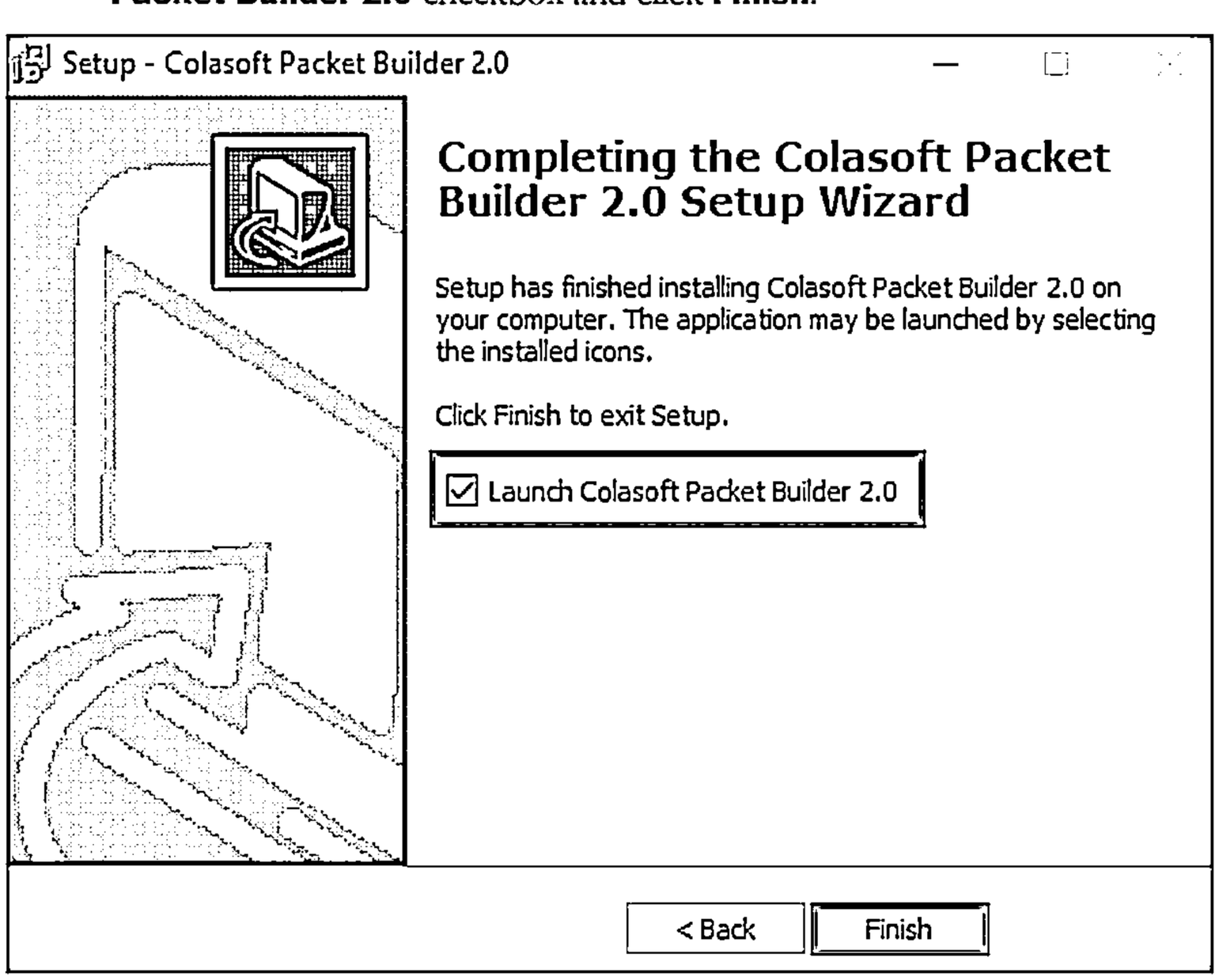


Figure 4.2.1: Colasoft Packet Builder Setup

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

TASK 2.2

Choose a Network Interface

9. The **Colasoft Packet Builder** GUI appears; click on the **Adapter** icon, as shown in the screenshot.

Note: If a pop-up appears, close the window.

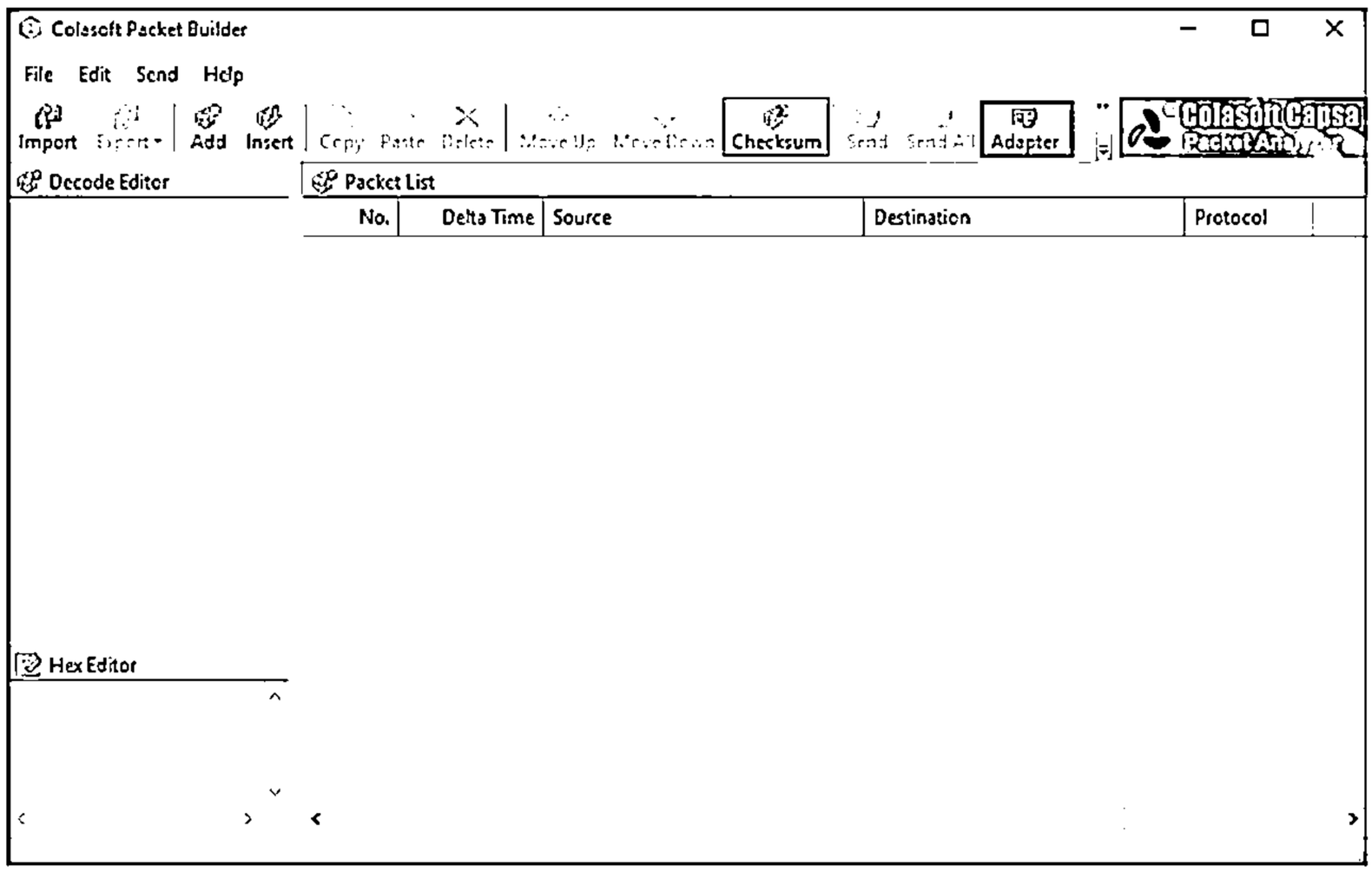


Figure 4.2.2: Colasoft Packet Builder GUI: click on adapter icon

10. When the **Select Adapter** window appears, check the **Adapter** settings and click **OK**.

Note: The adapter configuration might differ in your lab environment.

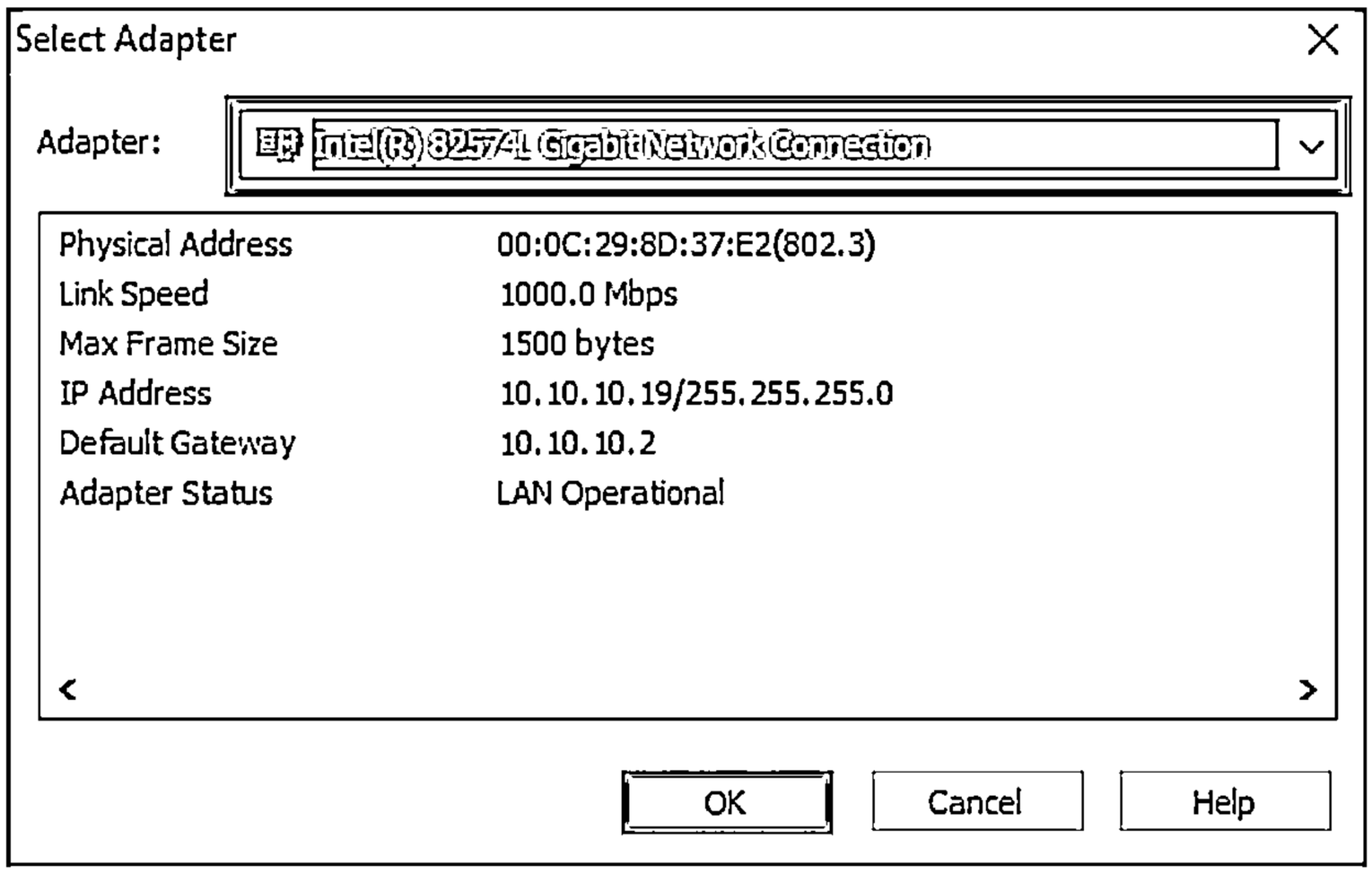


Figure 4.2.3: Choosing an adapter in Colasoft

TASK 2.3

Create an ARP Packet

11. To add or create a packet, click the **Add** (Add) icon in the **Menu** bar.

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

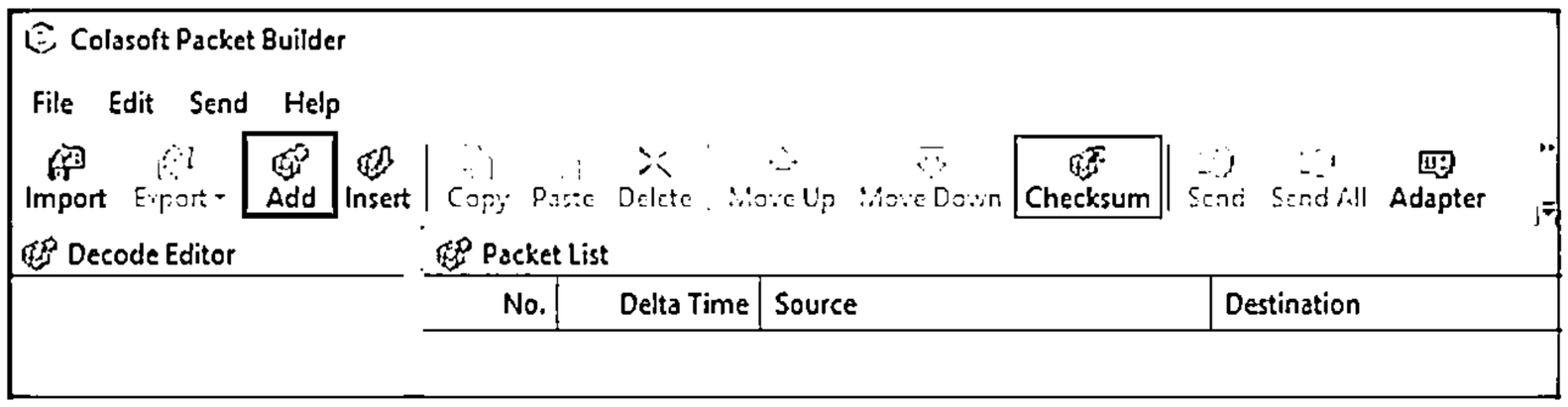


Figure 4.2.4: Adding a packet in Colasoft Packet Builder

12. In the **Add Packet** dialog box, select the **ARP Packet** template, set **Delta Time** as **0.1** seconds, and click **OK**.

Figure 4.2.5: Add Packet dialog box

13. You can view the added packets list on the right-hand side of the window, under **Packet List**.

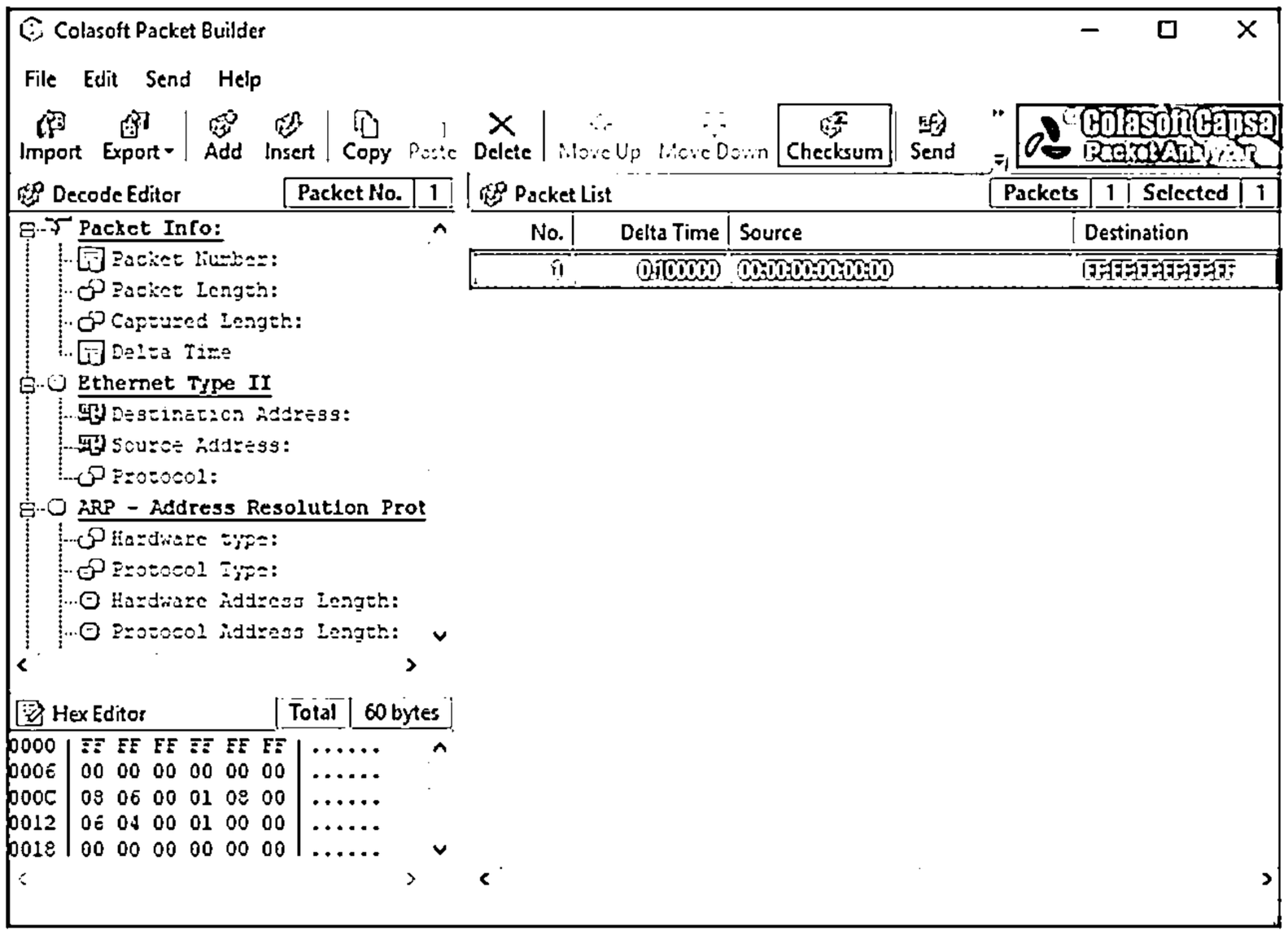


Figure 4.2.6: Viewing the added packets

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

14. **Colasoft Packet Builder** allows you to edit the decoding information in the two editors, **Decode Editor** and **Hex Editor**, located in the left pane of the window.

    - The **Decode Editor** section allows you to edit the packet decoding information by double-clicking the item that you wish to decode.
    - **Hex Editor** displays the actual packet contents in raw hexadecimal value on the left and its ASCII equivalent on the right.

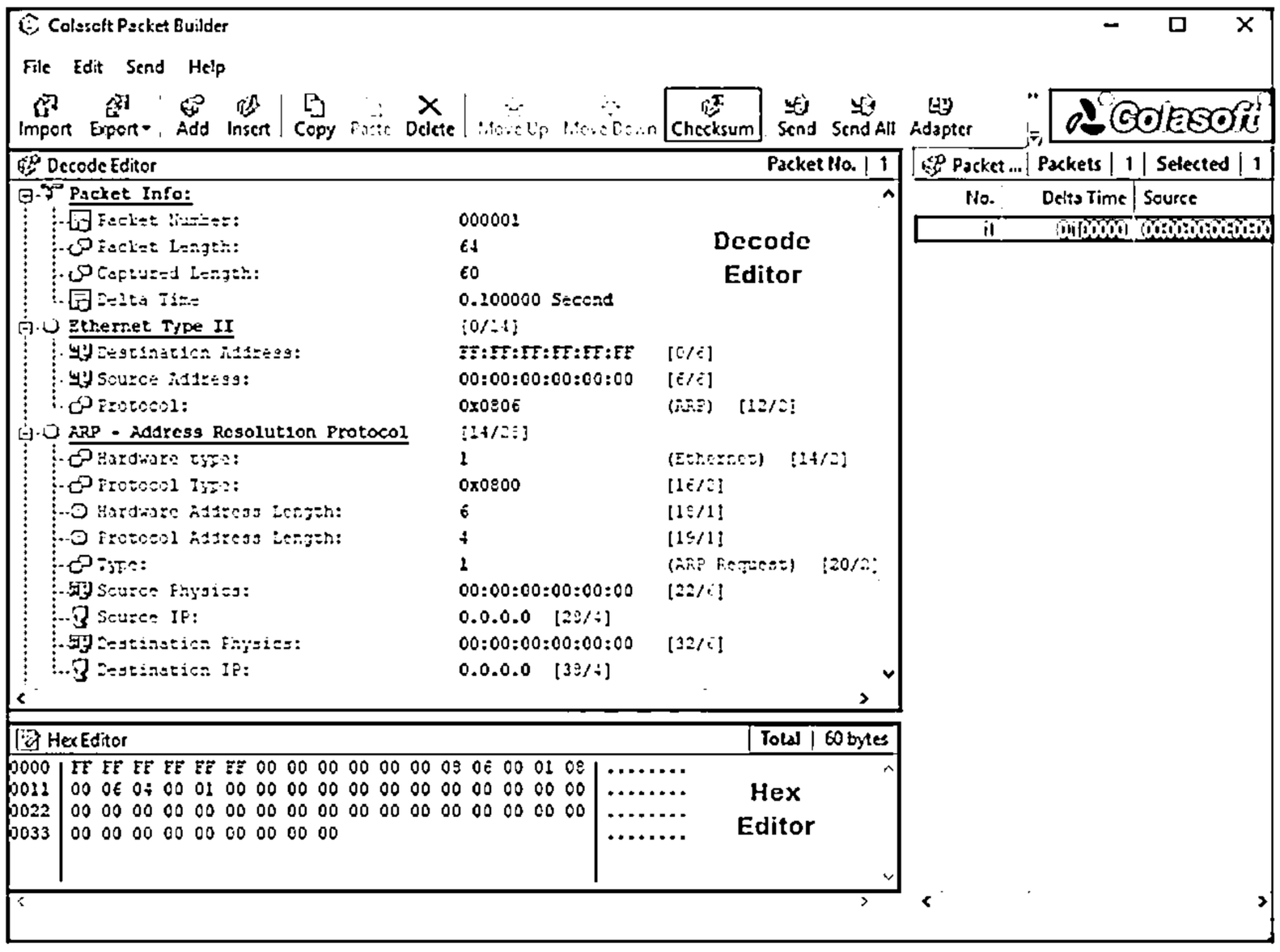


Figure 4.2.7: Colasoft Packet Builder Decode and Hex Editors

TASK 2.4

Send the Created ARP Packet to the Target

15. To send the packet, click **Send** from the **Menu** bar.

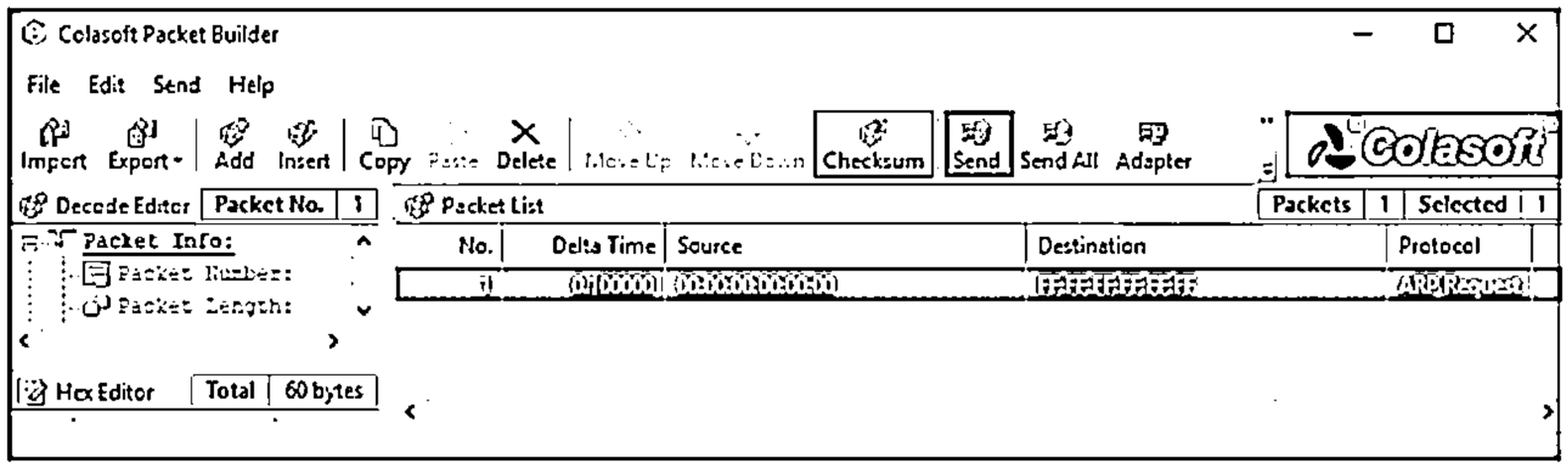


Figure 4.2.8: Sending all packets

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

16. In the **Send Selected Packets** window, select the **Burst Mode (no delay between packets)** option, and then click **Start**.

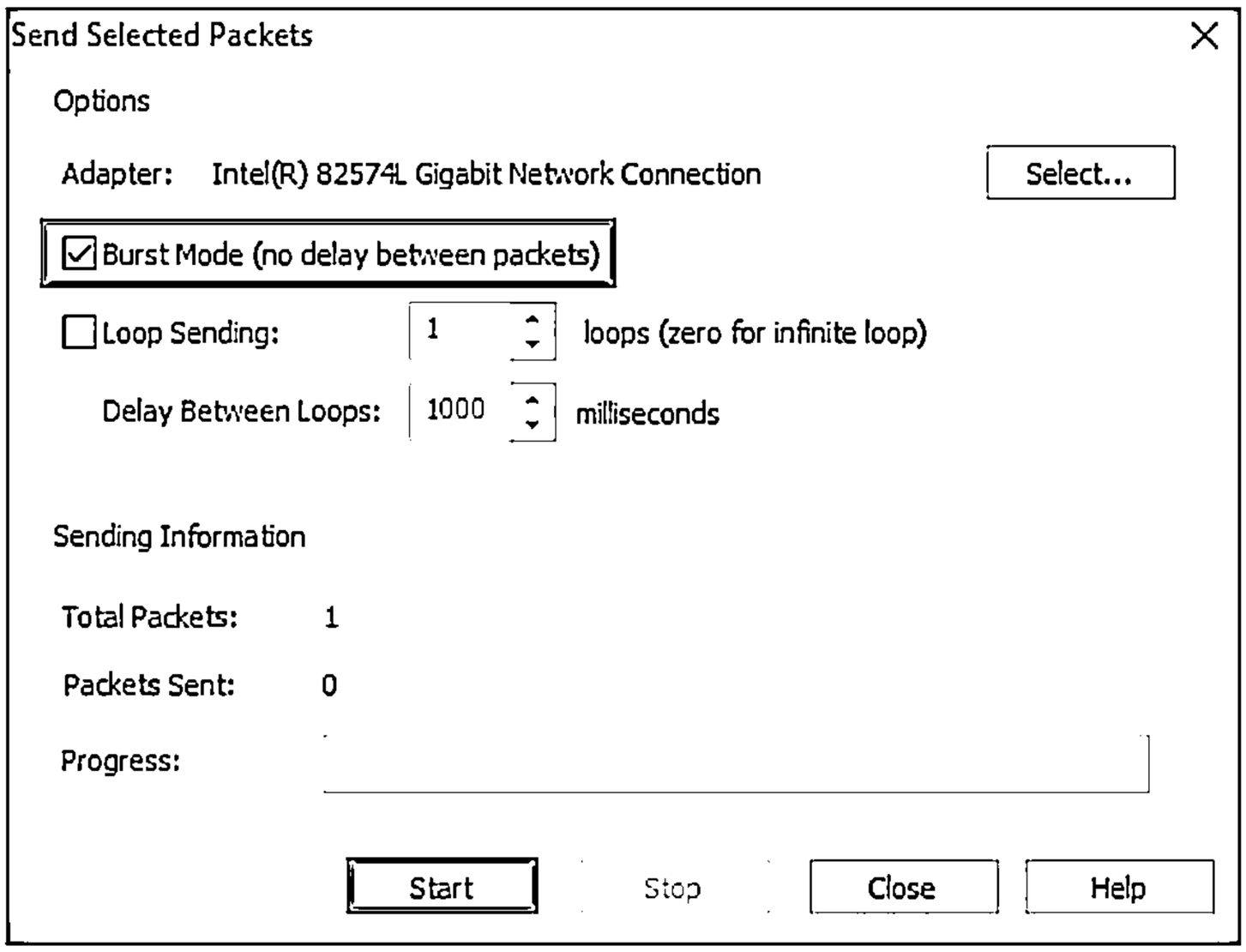


Figure 4.2.9: Setting Burst Mode option

17. After the **Progress** bar completes, click **Close**.

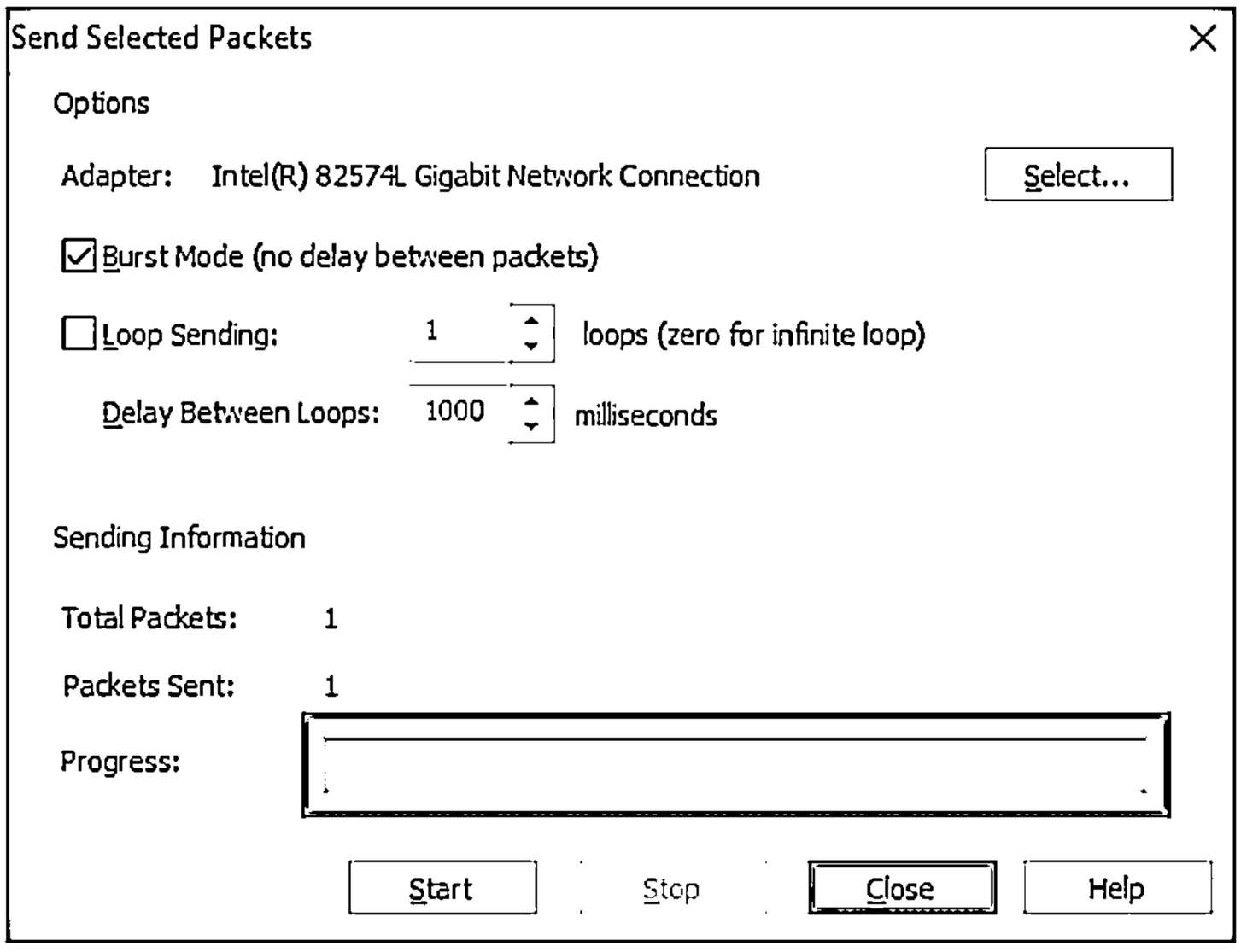


Figure 4.2.10: All packets successfully sent

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

18. Now, when this ARP packet is broadcasted in the network, the active machines receive the packet, and a few start responding with an ARP reply. To evaluate which machine is responding to the ARP packet, you need to observe packets captured by the **Wireshark** tool.

Note: Here, the host machine (**10.10.10.19**) is broadcasting ARP packets, prompting the target machine (**10.10.10.10**) to reply to the message.

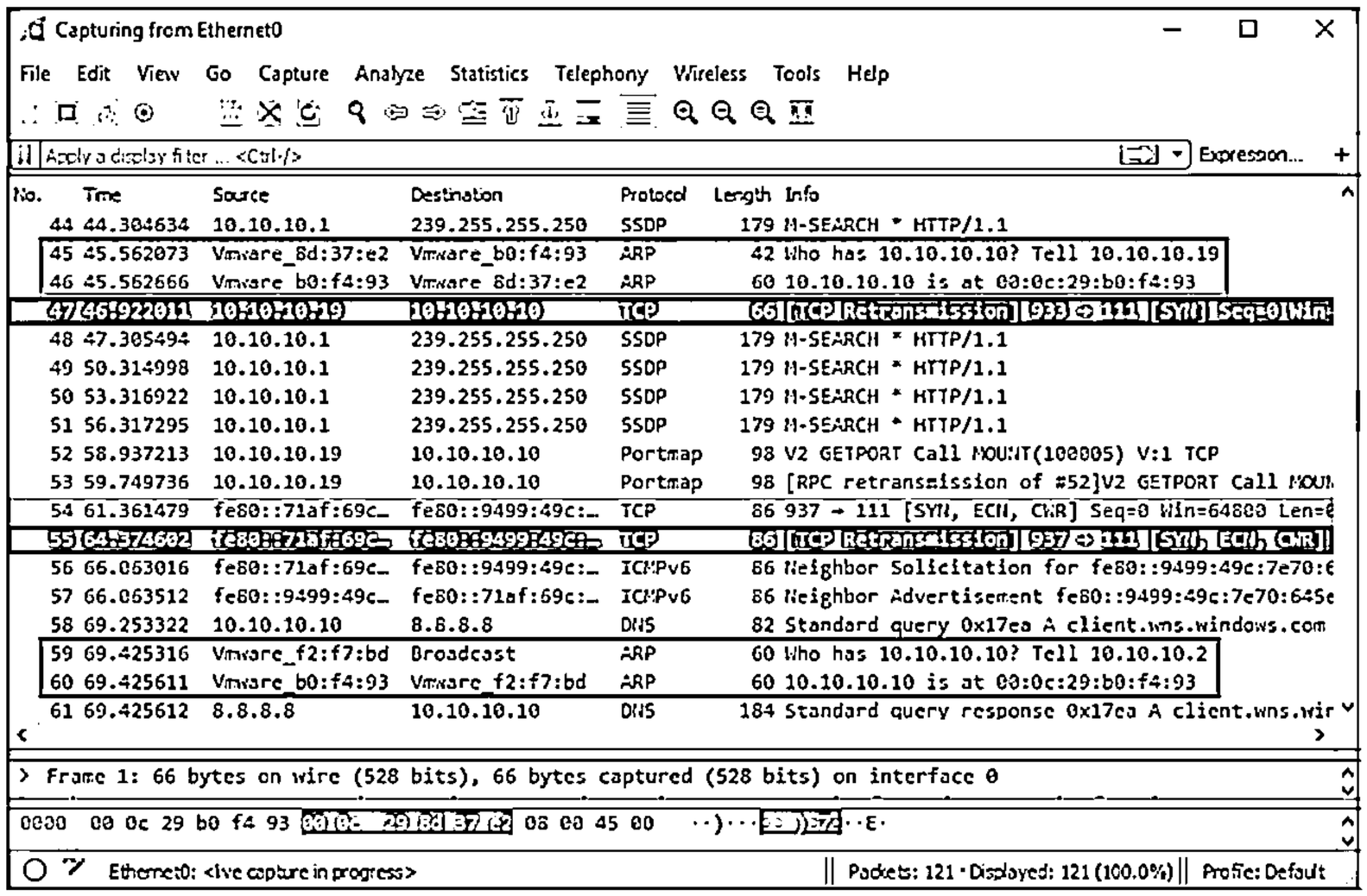


Figure 4.2.11: Wireshark captured packets

19. To export the packet, click **Export → Selected Packets....**

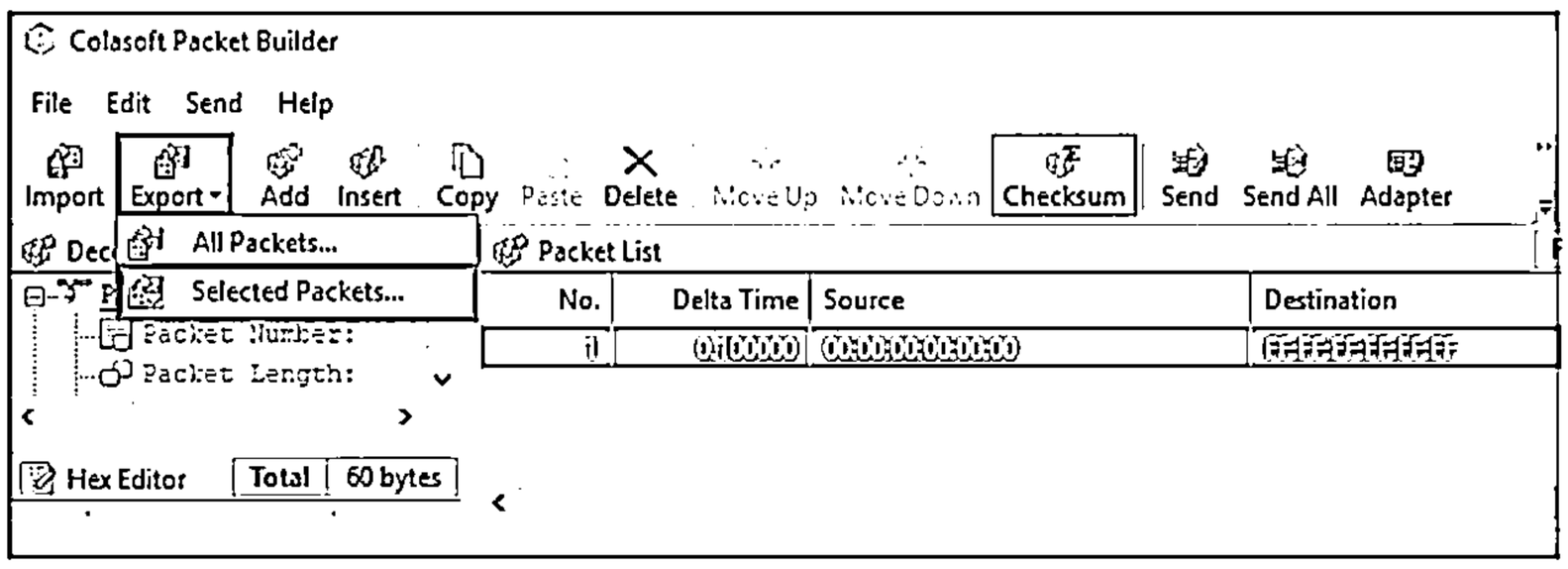


Figure 4.2.12: Exporting the packets in Colasoft

20. In the **Save As** window, select a destination folder in the **Save in** field, specify **File name** and **Save as type**, and click **Save**.
21. This saved file can be used for future reference.
22. This concludes the demonstration of creating a custom TCP packets to scan the target host by bypassing the IDS/firewall.
23. Close all open windows and document all the acquired information.
24. Turn off the **Windows Server 2019** virtual machine.

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

TASK 3

Create Custom UDP and TCP Packets using Hping3 to Scan beyond IDS/Firewall

Hping3 is a scriptable program that uses the TCL language, whereby packets can be received and sent via a binary or string representation describing the packets.

Here, we will use Hping3 to create custom UDP and TCP packets to evade the IDS/firewall in the target network.

Note: Before beginning this task, ensure that the **Windows 10** virtual machine is running and that **Windows Defender Firewall** is enabled.

1. In the **Windows 10** virtual machine, launch **Wireshark** and double-click the available ethernet or interface (here, **Ethernet0**) to start the packet capture.
2. Turn on the **Parrot Security** virtual machine.
3. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

4. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
5. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
6. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

7. Now, type **cd** and press **Enter** to jump to the root directory.

TASK 3.1

Perform UDP Packet Crafting

8. In the terminal window, type **hping3 <Target IP Address> --udp --rand-source --data 500** (here, the target machine is Windows 10 [**10.10.10.10**]) and press **Enter**.

Note: Here, **--udp** specifies sending the UDP packets to the target host, **--rand-source** enables the random source mode and **--data** specifies the packet body size.

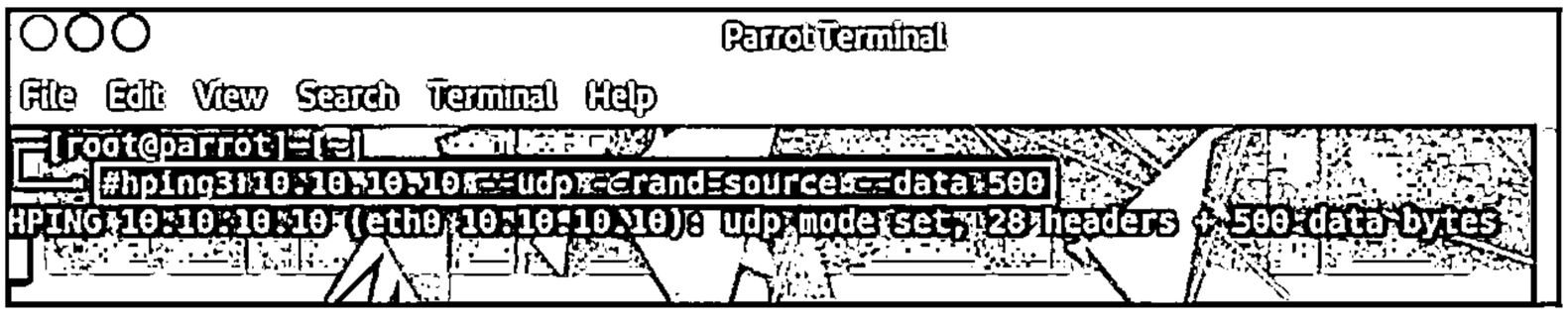


Figure 4.3.1: Hping3 Output of 3 Packets sent to the target machine

9. Now, switch to the **Windows 10** virtual machine and observe the UDP packets captured by **Wireshark**.

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

Note: You can double-click any UDP packet and observe the details.

10. Expand the **Data** node in the **Packet Details** pane and observe the size of **Data** and its **Length** (the length is the same as the size of the packet body that we specified in Hping3 command, i.e., **500**).

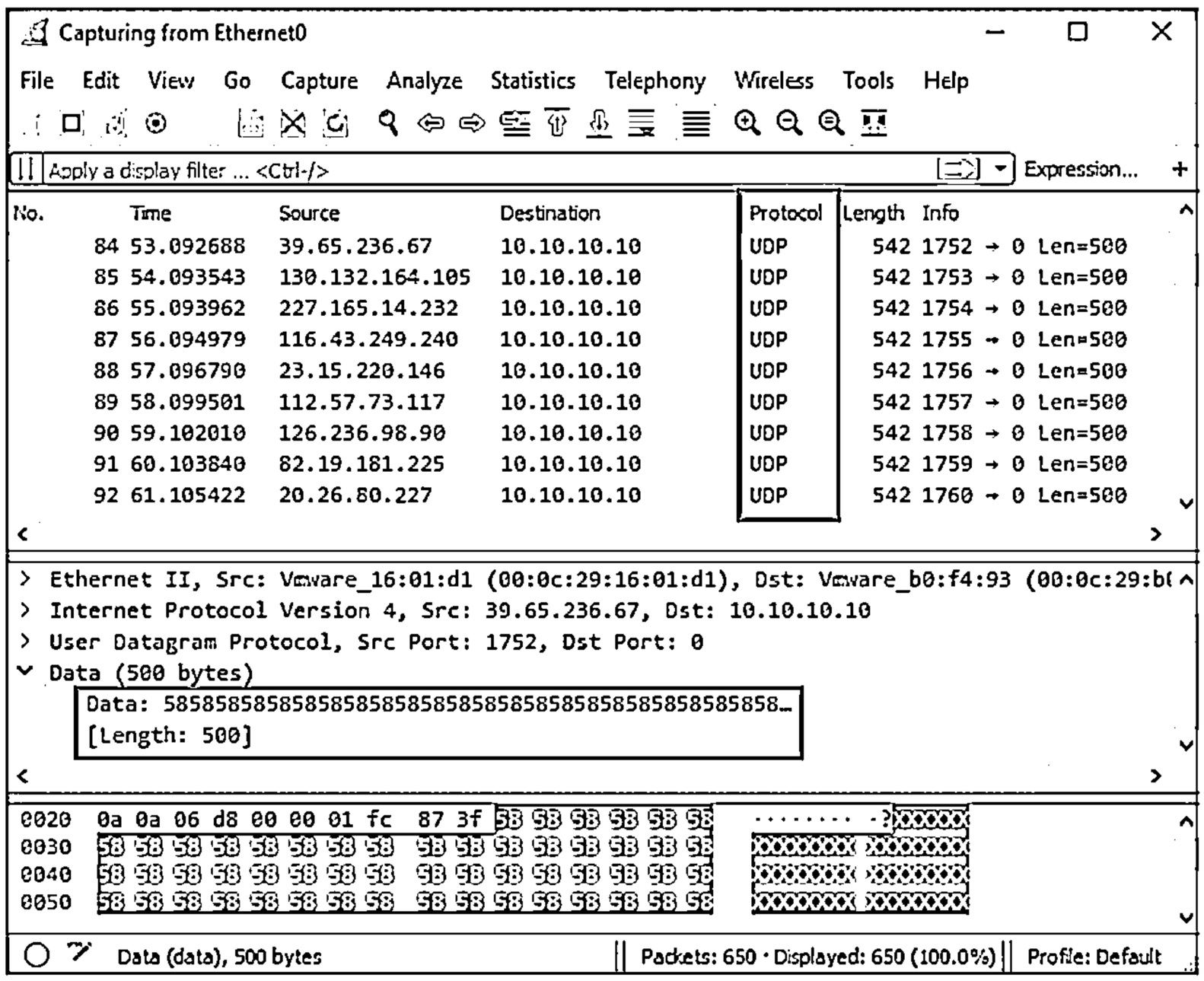


Figure 4.3.2: Wireshark capturing UDP packets in the target machine (Windows 10)

TASK 3.2

Send TCP SYN Request

11. Switch to the **Parrot Security** virtual machine. In the **Parrot Terminal** window, first press **Control+C** and type **hping3 -S <Target IP Address> -p 80 -c 5** (here, target IP address is **10.10.10.10**), and then press **Enter**.

Here, **-S** specifies the TCP SYN request on the target machine, **-p** specifies assigning the port to send the traffic, and **-c** is the count of the packets sent to the target machine.

Note: The IP addresses might vary in your lab environment.

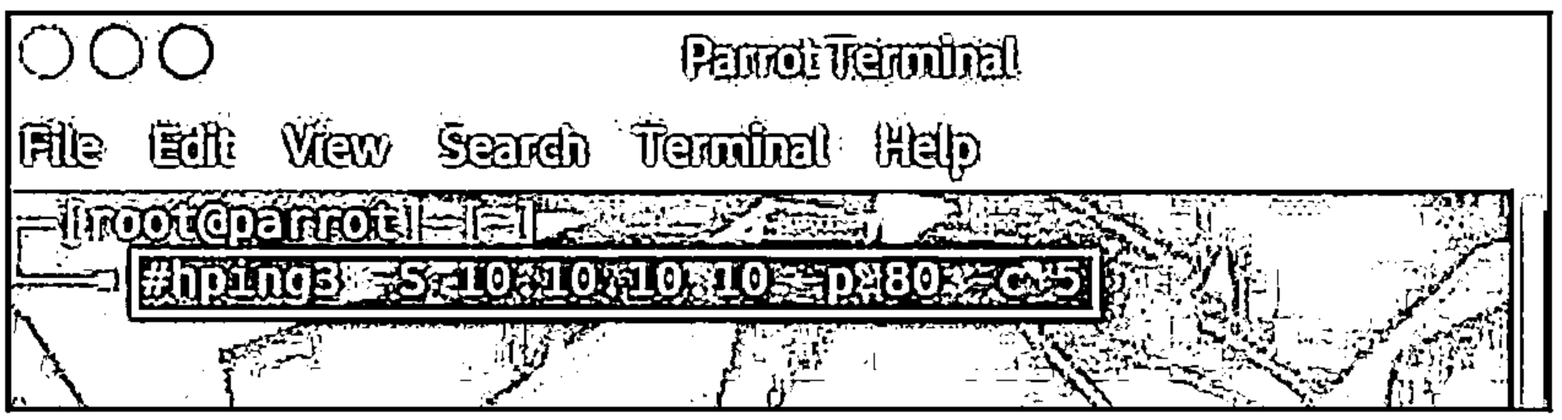


Figure 4.3.3: Hping3 sending TCP SYN packets

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

12. In the result, it is indicated that five packets were sent and received through port 80.

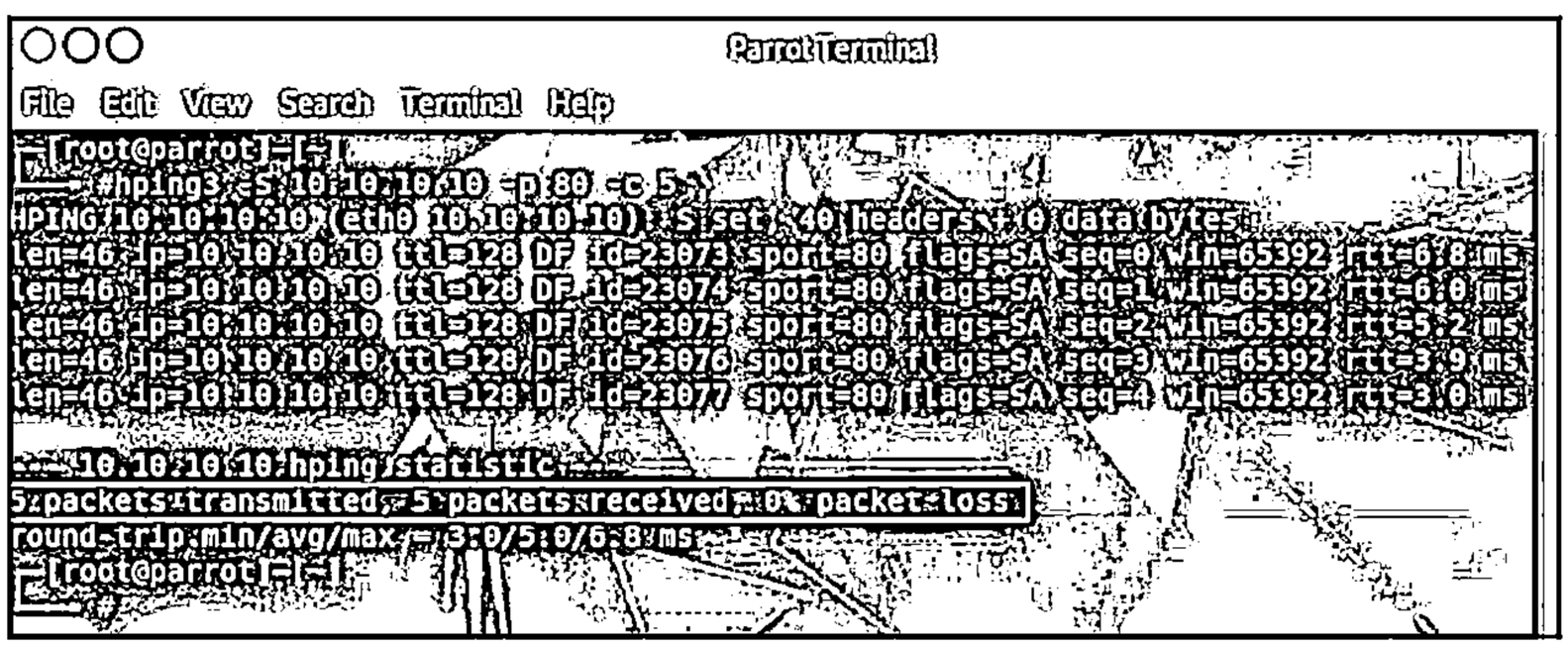


Figure 4.3.4: Hping3 sent TCP SYN packets to the target machine

13. Now, switch to the target machine (i.e., **Windows 10**) and observe the TCP packets captured via Wireshark.

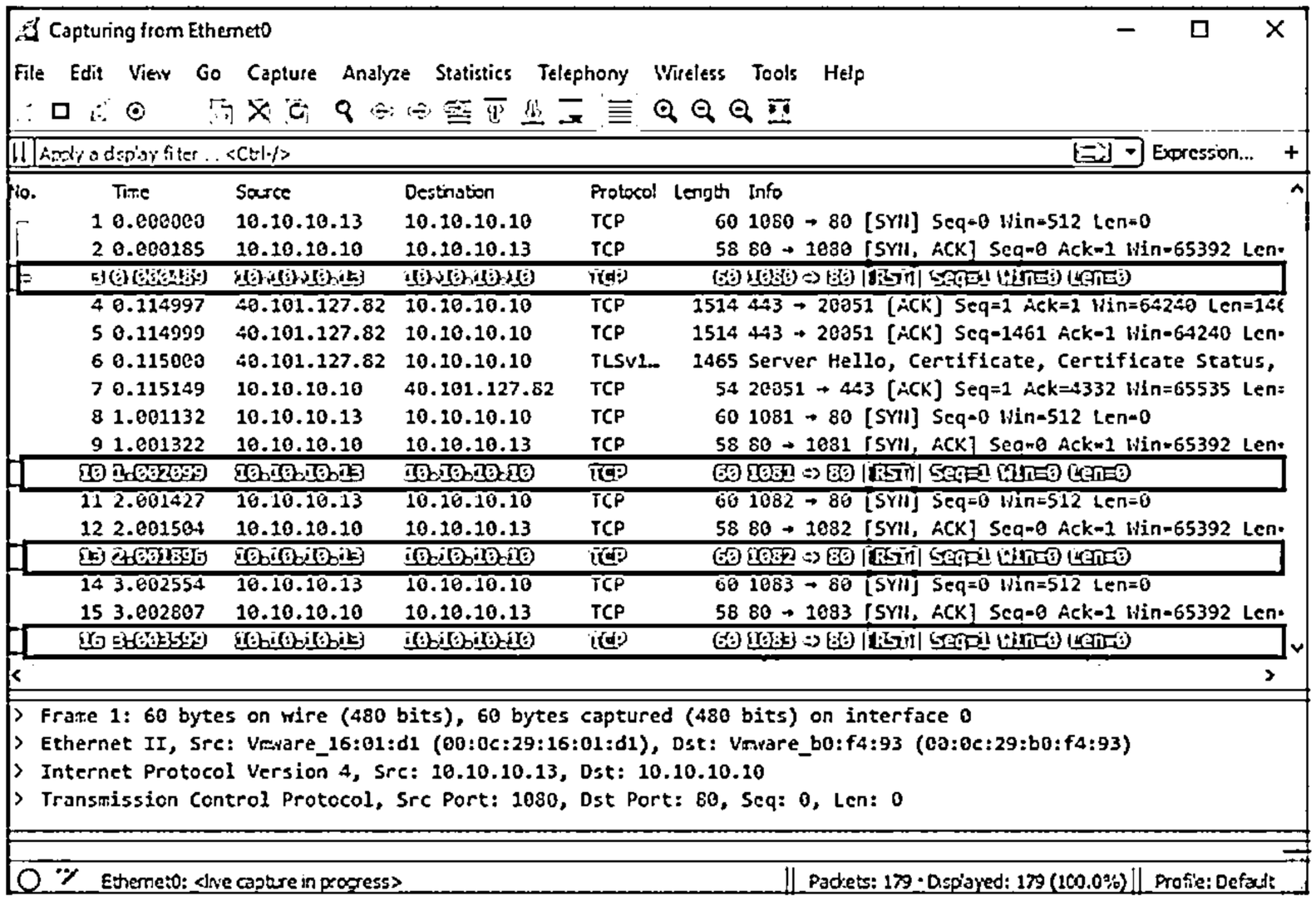


Figure 4.3.5: Wireshark TCP SYN Packets captured in the target machine

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

TASK 3.3

Perform TCP Flooding

14. Switch to the **Parrot Security** virtual machine and try to flood the target machine (here, **Windows 10**) with TCP packets.
15. In the **Parrot Terminal** window, type **hping3 <Target IP Address> --flood** (here, target IP address is **10.10.10.10**) and press **Enter**.

Note: **--flood**: performs the TCP flooding.

16. Once you flood traffic to the target machine, it will respond in the **hping3** terminal.

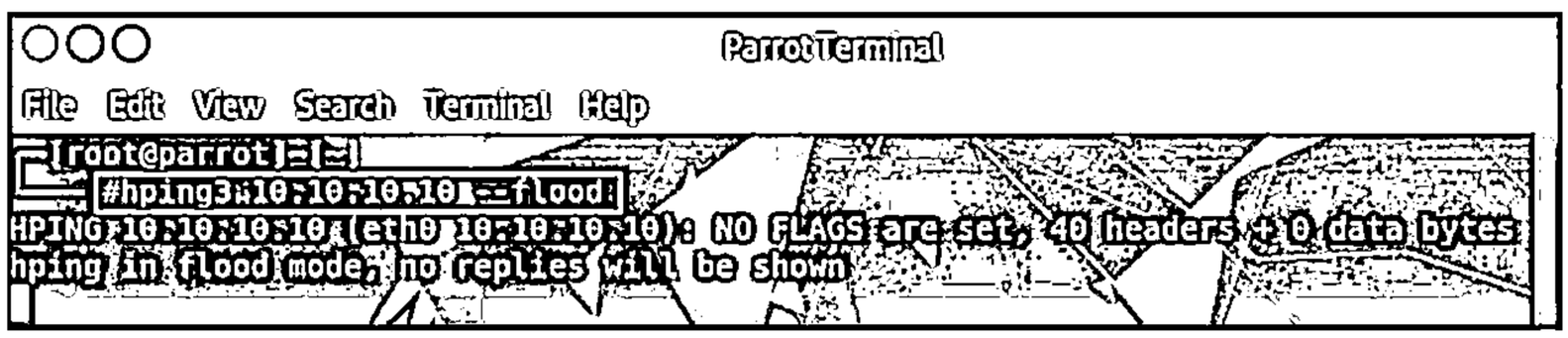


Figure 4.3.6: TCP Packets flooded to Target machine

17. Switch to **Windows 10** (target machine) and stop the packet capture in the Wireshark window after a while.
18. Observe the **Wireshark** window, which displays the TCP packet flooding from the host machine.

Note: You can double-click the TCP packet stream to observe the TCP packet information.

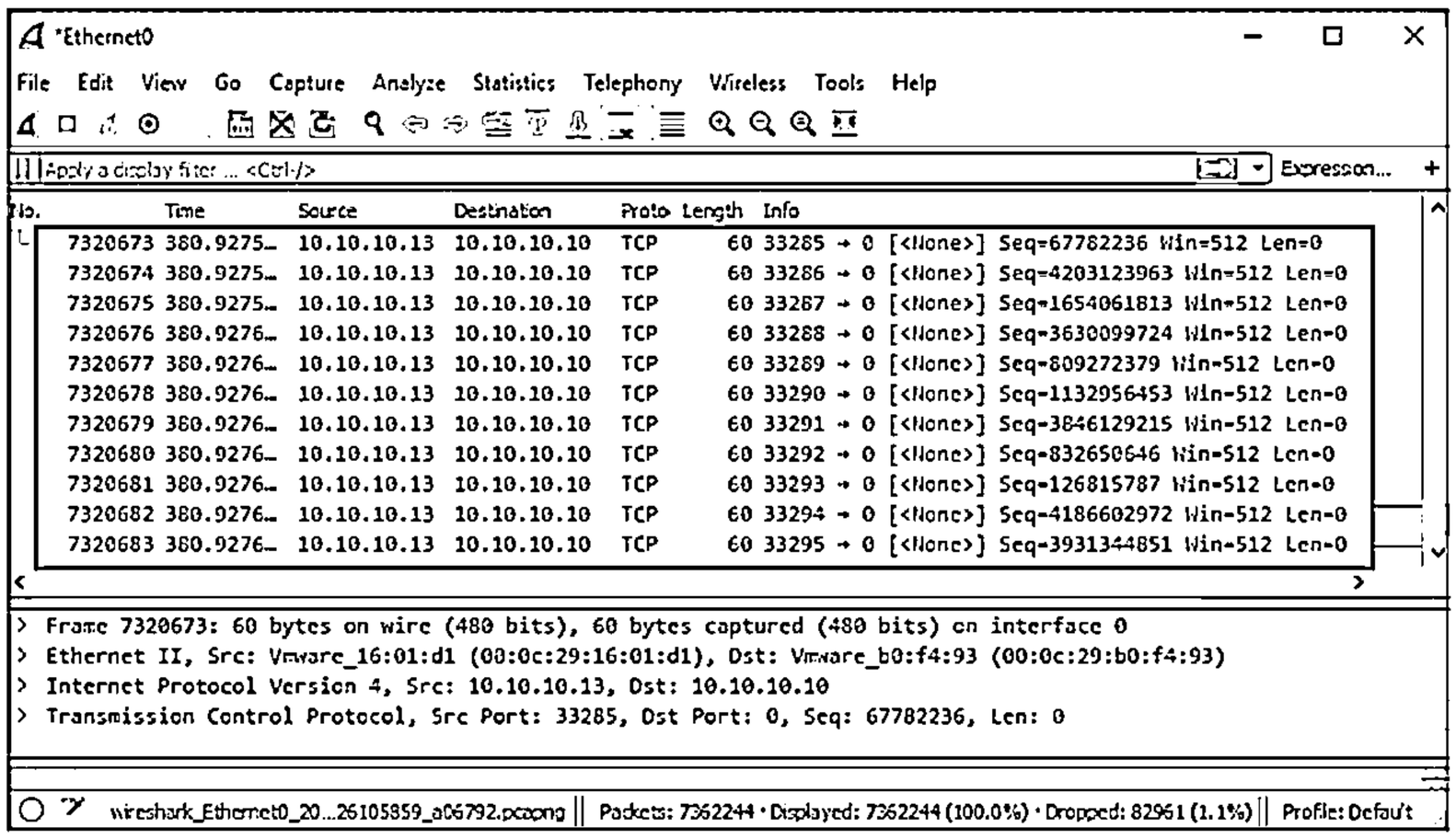


Figure 4.3.7: TCP Packets in Wireshark

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

19. The TCP packet stream displays the complete information of TCP packets such as the source and destination of the captured packet, source port, destination port, etc.

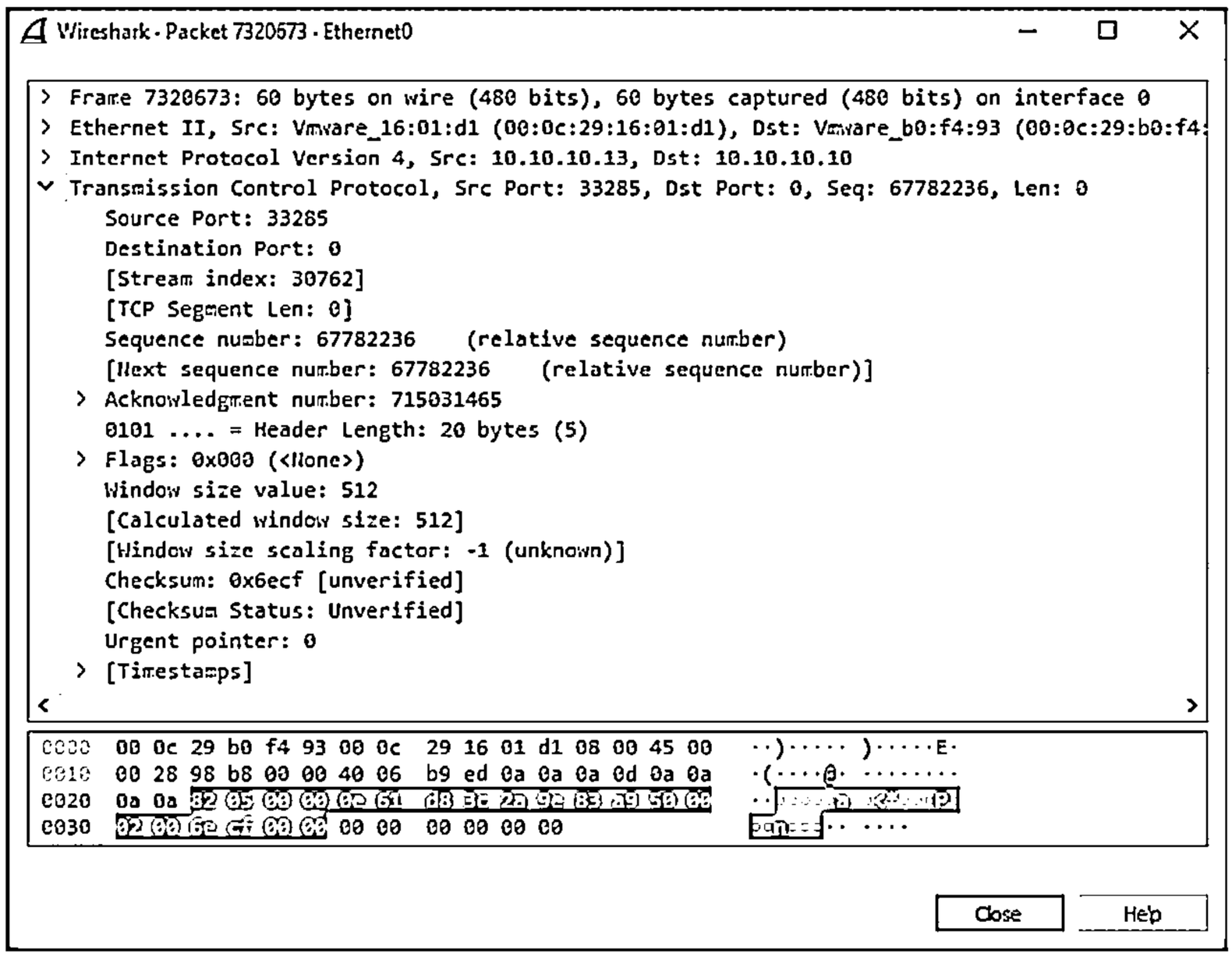


Figure 4.3.8: TCP packet Stream information

20. This concludes the demonstration of evading the IDS and firewall using various evasion techniques in Hping3.
21. Close all open windows and document all the acquired information.
22. Turn off the **Parrot Security** virtual machine.

TASK 4 Create Custom Packets using Nmap to Scan beyond IDS/Firewall

Nmap is a network scanning tool that can be used for sending customized data packets to scan the target host, thus bypassing various security mechanisms such as the IDS/firewall.

Here, we will use Nmap to perform various scanning techniques such as appending custom binary data, appending a custom string, appending random data, randomizing host order, and sending bad checksums to scan the target host beyond the IDS/firewall.

Note: In this task, we are using the **Windows 10** (10.10.10.10) virtual machine as a host machine and the **Windows Server 2016** (10.10.10.16) virtual machine as a target machine.

1. Turn on the **Windows Server 2016** virtual machine and log in the with credentials **Administrator/Pa$$w0rd**.
2. Navigate to **Control Panel → System and Security → Windows Firewall → Turn Windows Firewall on or off**, enable Windows Firewall, and click **OK**.

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

TASK 4.1

Append Custom Binary Data

3. Switch to the **Windows 10** virtual machine and launch **Nmap** by double-clicking on the **Nmap - Zenmap GUI** icon available on **Desktop**.
4. The **Nmap - Zenmap** GUI appears. In the **Command** field, type the command **nmap <Target IP Address> --data 0xdeadbeef** (here, target IP address is **10.10.10.16**) and click **Scan**.

Note: Nmap uses **--data <hex string>** (here, **0xdeadbeef**) to send the binary data (o's and 1's) as payloads in the sent packets to scan beyond firewalls.

5. The scan results appear, displaying all open TCP ports and services running on the target machine, as shown in the screenshot.

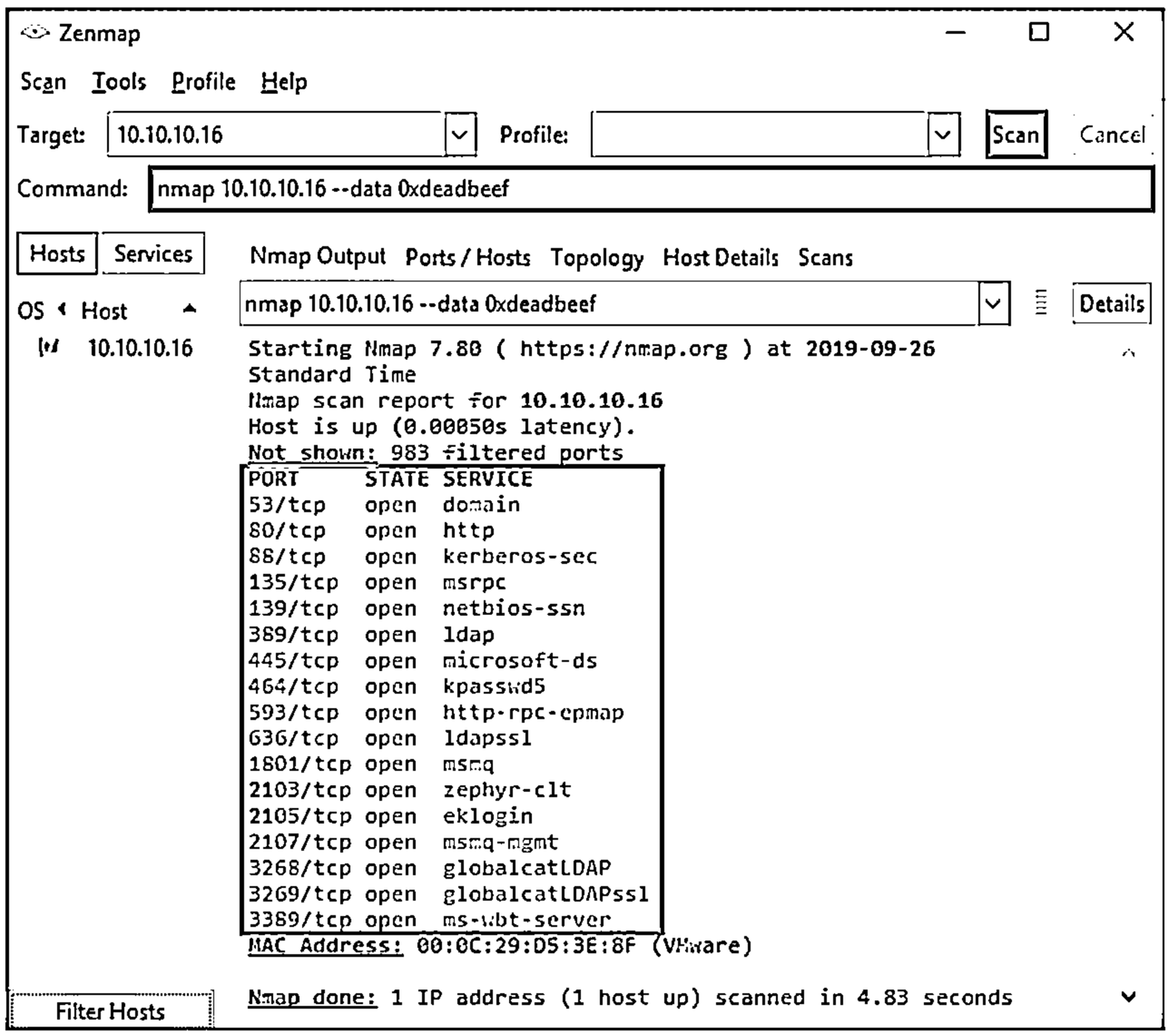


Figure 4.4.1: Zenmap scan results for Appending Custom Binary Data

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

TASK 4.2

Append Custom String

6. In the **Command** field, type the command **nmap <Target IP Address> --data-string "Ph34r my l33t skills"** (here, target IP address is **10.10.10.16**) and click **Scan**.

Note: Nmap uses **--data-string <string>** (here, "**Ph34r my l33t skills**") to send a regular string as payloads in the sent packets to the target machine for scanning beyond the firewall.

7. The scan results appear, displaying all open TCP ports and services running on the target machine, as shown in the screenshot.

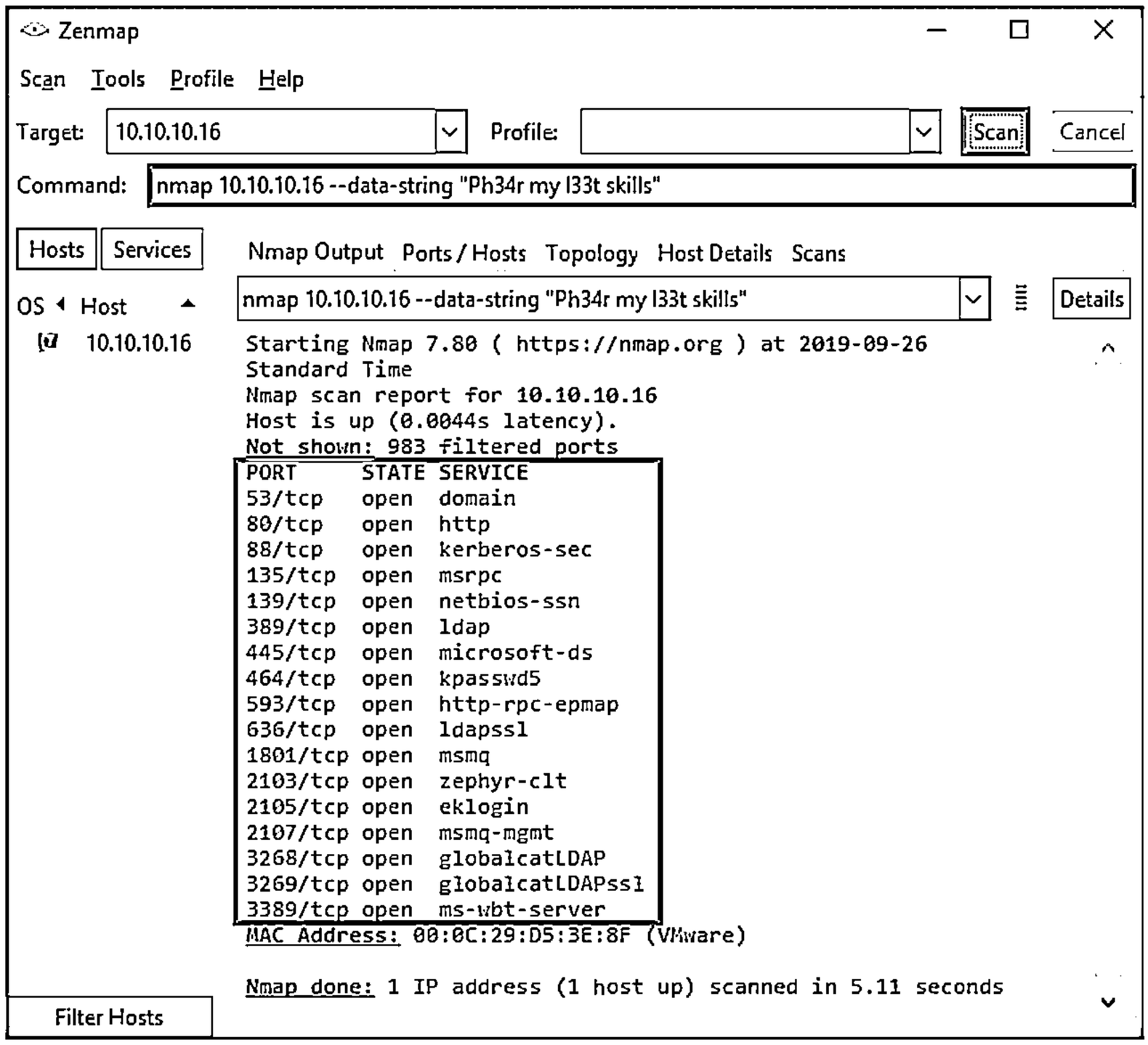


Figure 4.4.2: Zenmap scan results for Appending Custom String

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

TASK 4.3

Append Random Data

8. In the **Command** field, type the command **nmap --data-length 5 <Target IP Address>** (here, the target IP address is **10.10.10.16**) and click **Scan**.

Note: Nmap uses **--data-length <len>** (here, **5**) to append the number of random data bytes to most of the packets sent without any protocol-specific payloads.

9. The scan results appear, displaying all open TCP ports and services running on the target machine, as shown in the screenshot.

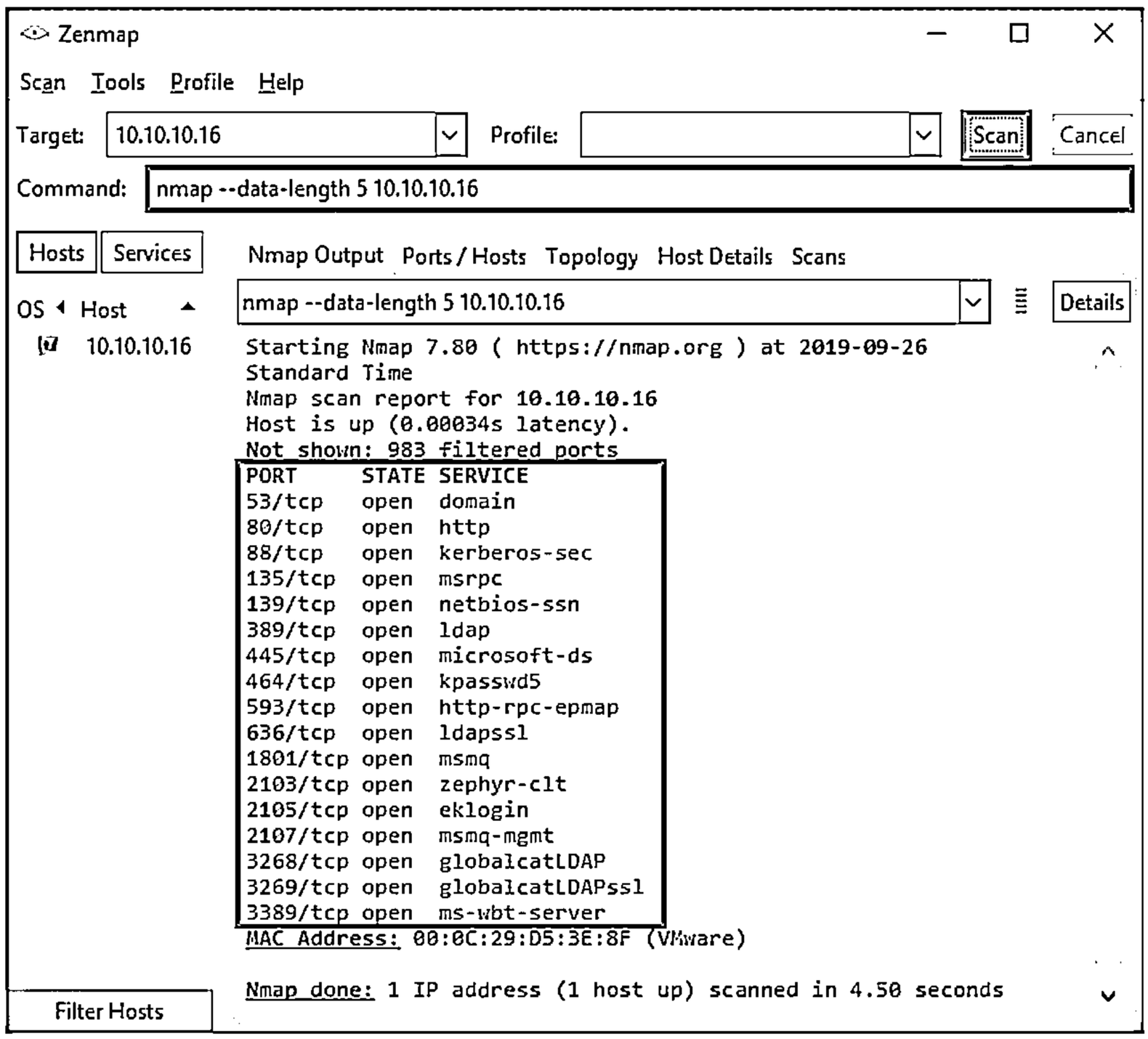


Figure 4.4.3: Zenmap scan results for Appending Random Data

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

TASK 4.4

Randomizing Host Order

10. In the **Command** field, type the command **nmap --randomize-hosts <Target IP Address>** (here, the target IP address is **10.10.10.16**) and click **Scan**.

Note: Nmap uses **--randomize-hosts** to scan the number of hosts in the target network in random order to scan the intended target that is beyond the firewall.

11. The scan results appear, displaying all open TCP ports and services running on the target machine, as shown in the screenshot.

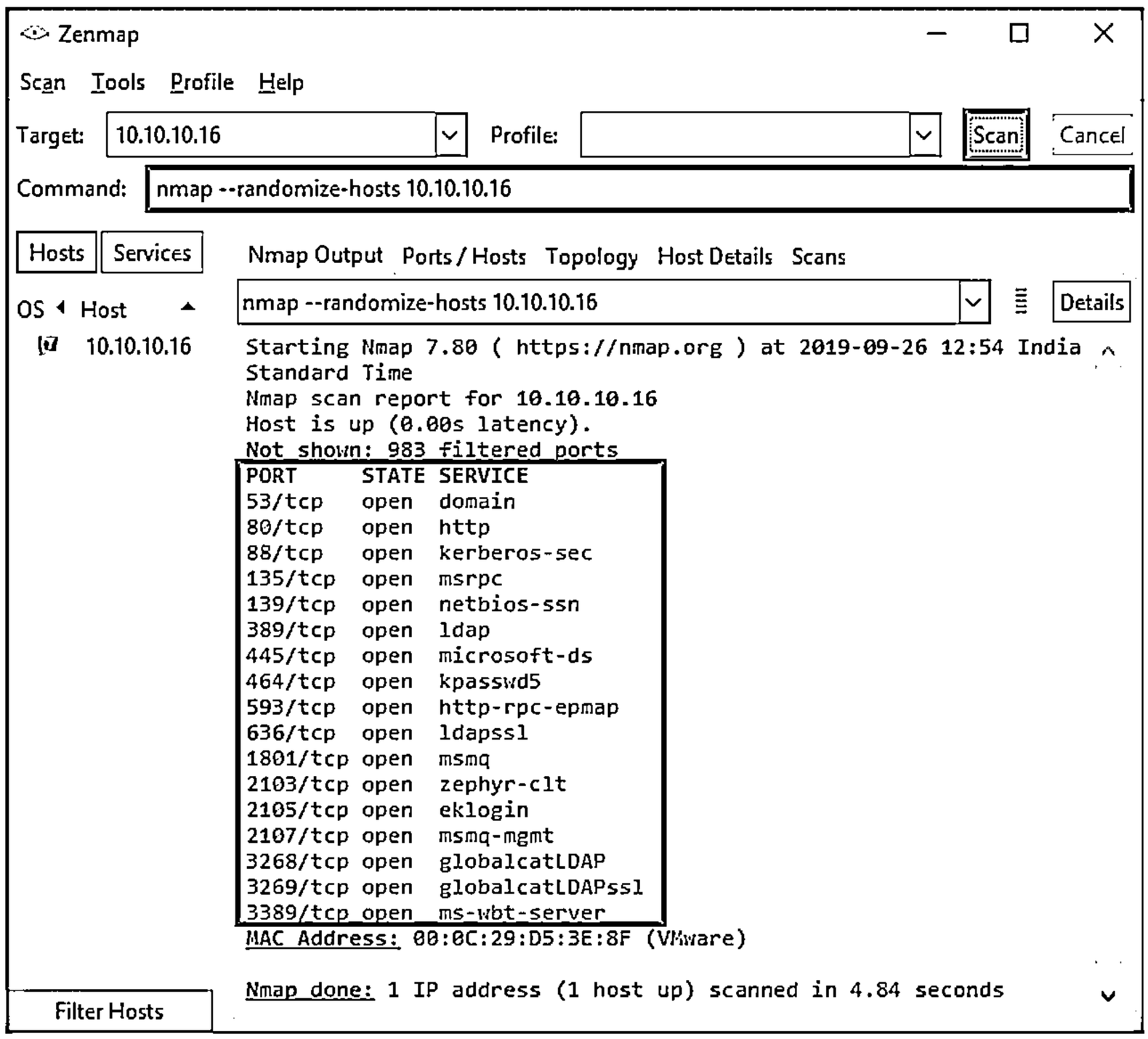


Figure 4.4.4: Zenmap scan results for Randomizing Host Order

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

TASK 4.5

Send Bad Checksums

12. In the **Command** field, type the command **nmap --badsum <Target IP Address>** (here, the target IP address is **10.10.10.16**) and click **Scan**.

Note: Nmap uses **--badsum** to send the packets with bad or bogus TCP/UPD checksums to the intended target to avoid certain firewall rulesets.

13. The scan results appear, demonstrating that all ports are filtered, indicating that there is no response or the packets are dropped, and thus it can be inferred that the system is configured.

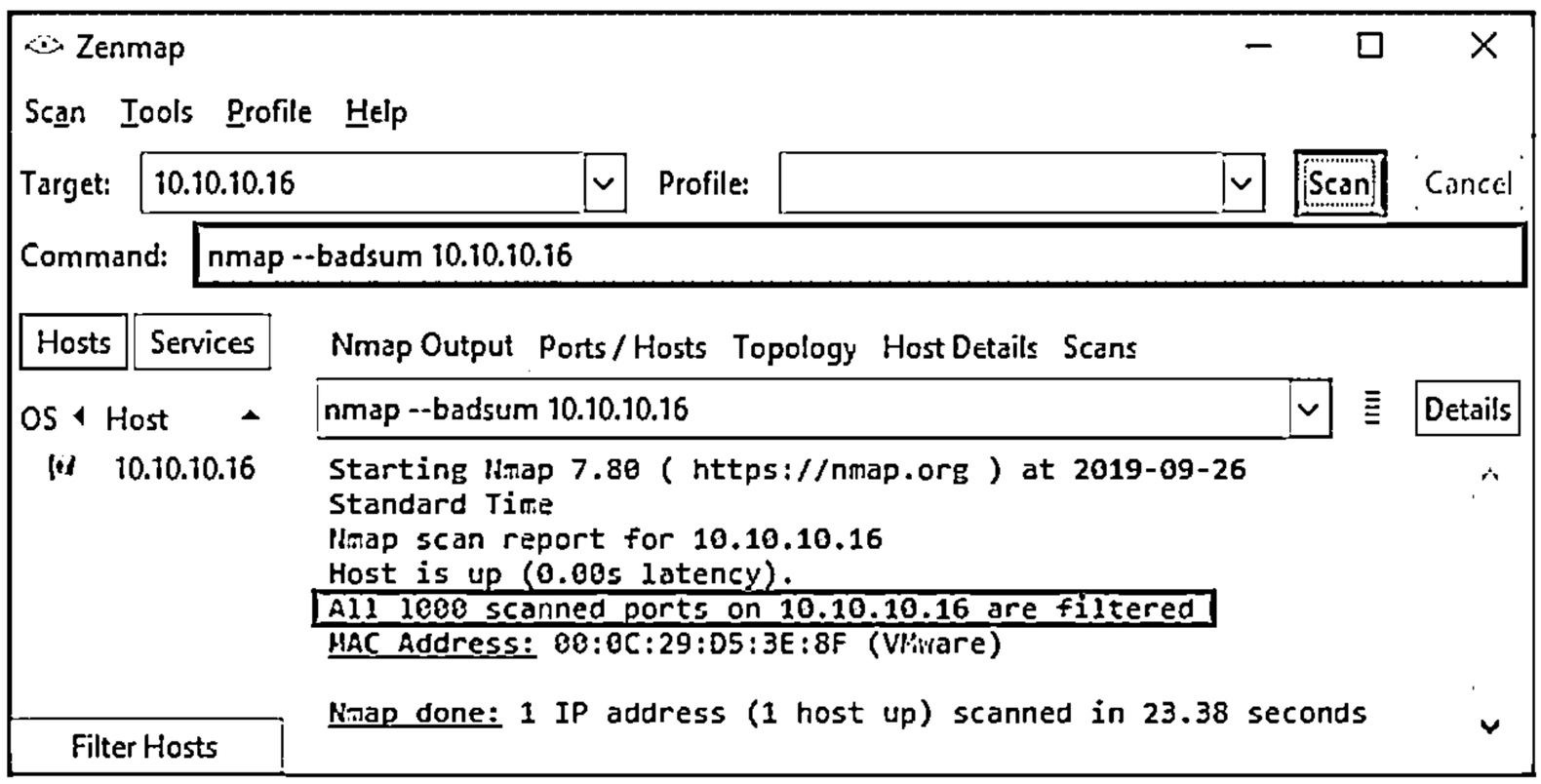


Figure 4.4.5: Zenmap scan results for Bad Checksum

You can also use other packet crafting tools such as **NetScanTools Pro** (https://www.netscantools.com), **Ostinato** (https://www.ostinato.org), and **WAN Killer** (https://www.solarwinds.com) to build custom packets to evade security mechanisms.

14. This concludes the demonstration of creating custom packets using Nmap to scan beyond the IDS and firewall.
15. Close all open windows and document all the acquired information.
16. Turn off the Windows Firewall in the **Windows 10** and **Windows Server 2016** virtual machines by navigating to **Control Panel → System and Security → Windows Firewall → Turn Windows Defender Firewall on or off.**
17. Turn off **Windows Server 2016** virtual machine.

TASK 5 Browse Anonymously using Proxy Switcher

Here, we will use Proxy Switcher to browse the Internet anonymously.

TASK 5.1

Install Proxy Switcher

1. In the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 03 Scanning Networks\Proxy Tools\Proxy Switcher** and double-click **ProxySwitcherStandard.exe**.

Note: If a **User Account Control** window appears, click **Yes**.

2. Follow the installation steps to install Proxy Switcher using all default settings.
3. Once the installation is complete, uncheck all options in the final step of the wizard, and click **Finish**.

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

Proxy Switcher allows you to surf the Internet anonymously without disclosing the IP address of your system, and helps to access various blocked sites in the organization. It avoids all types of limitations imposed by target sites.

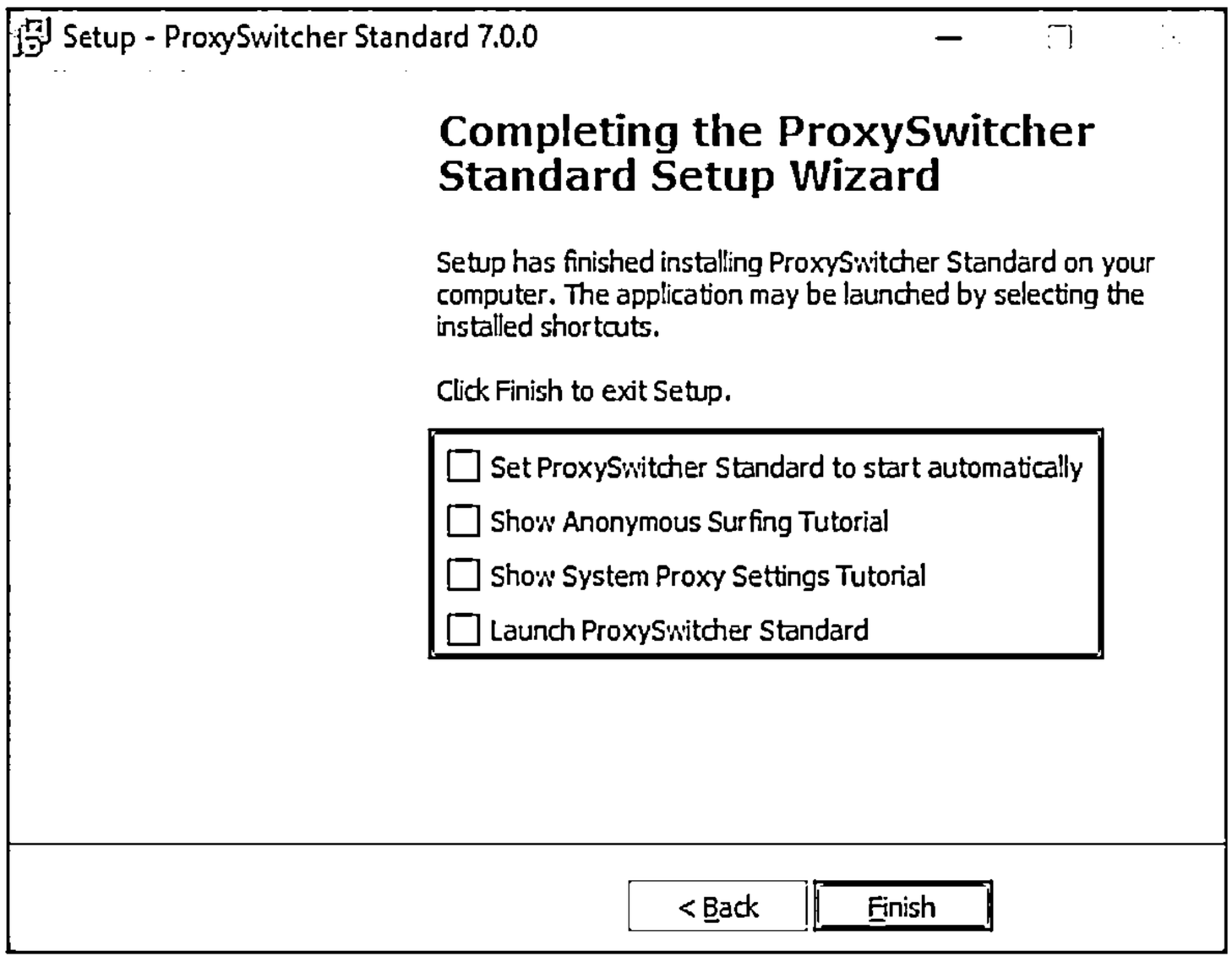


Figure 4.5.1: ProxySwitcher finish wizard

TASK 5.2

Configure Local Proxy in a Web Browser

4. Now, launch the **Firefox** browser.

Note: If a **Default Browser** pop-up appears, click **Not now**.

5. Click the **Open menu** icon in the top-right corner of the browser window and click **Options**.

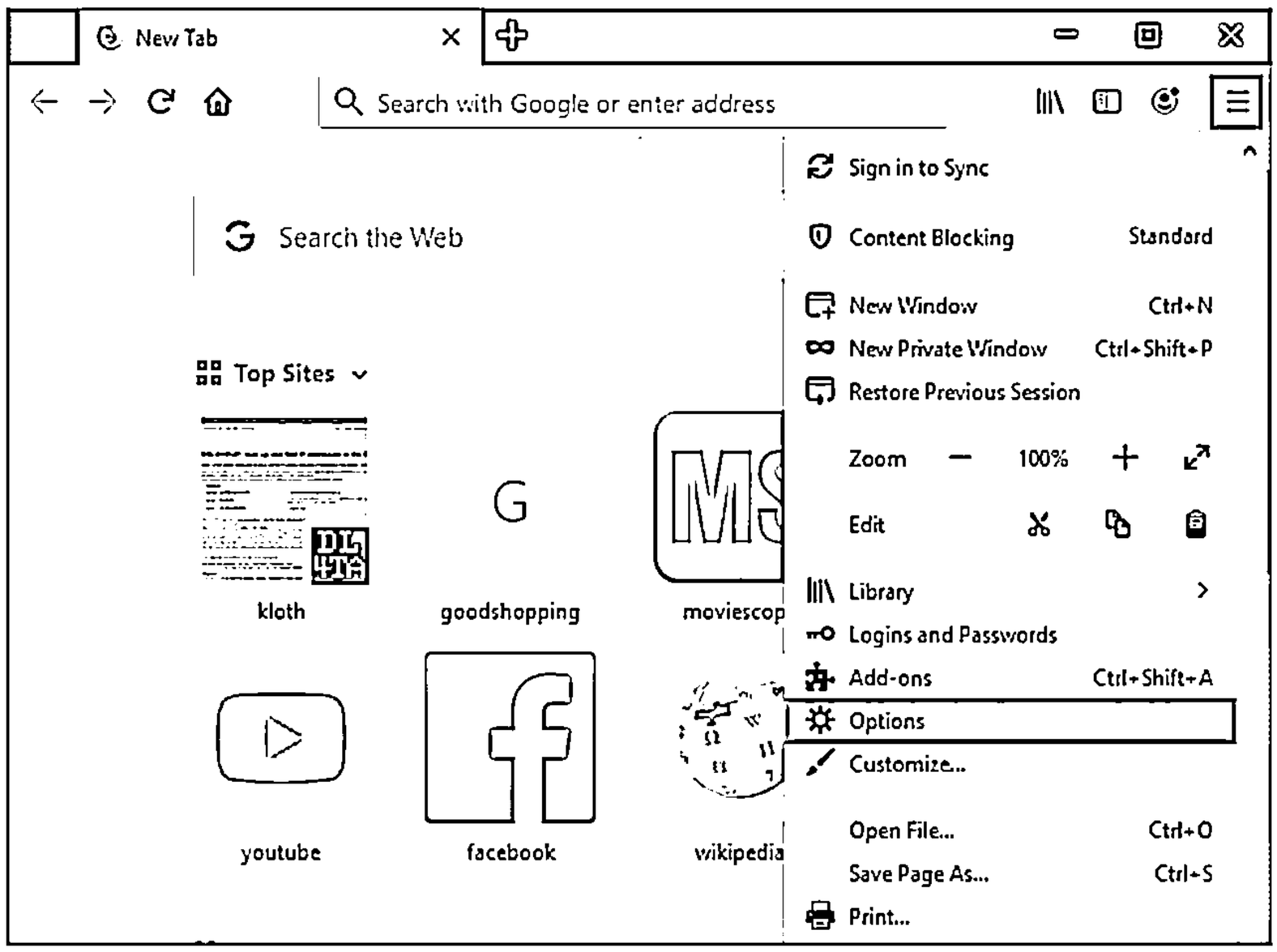


Figure 4.5.2: Firefox clicking on Options

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

6. In the **Options** wizard, scroll down to the end of the page and click **Settings...** under the **Network Settings** section.

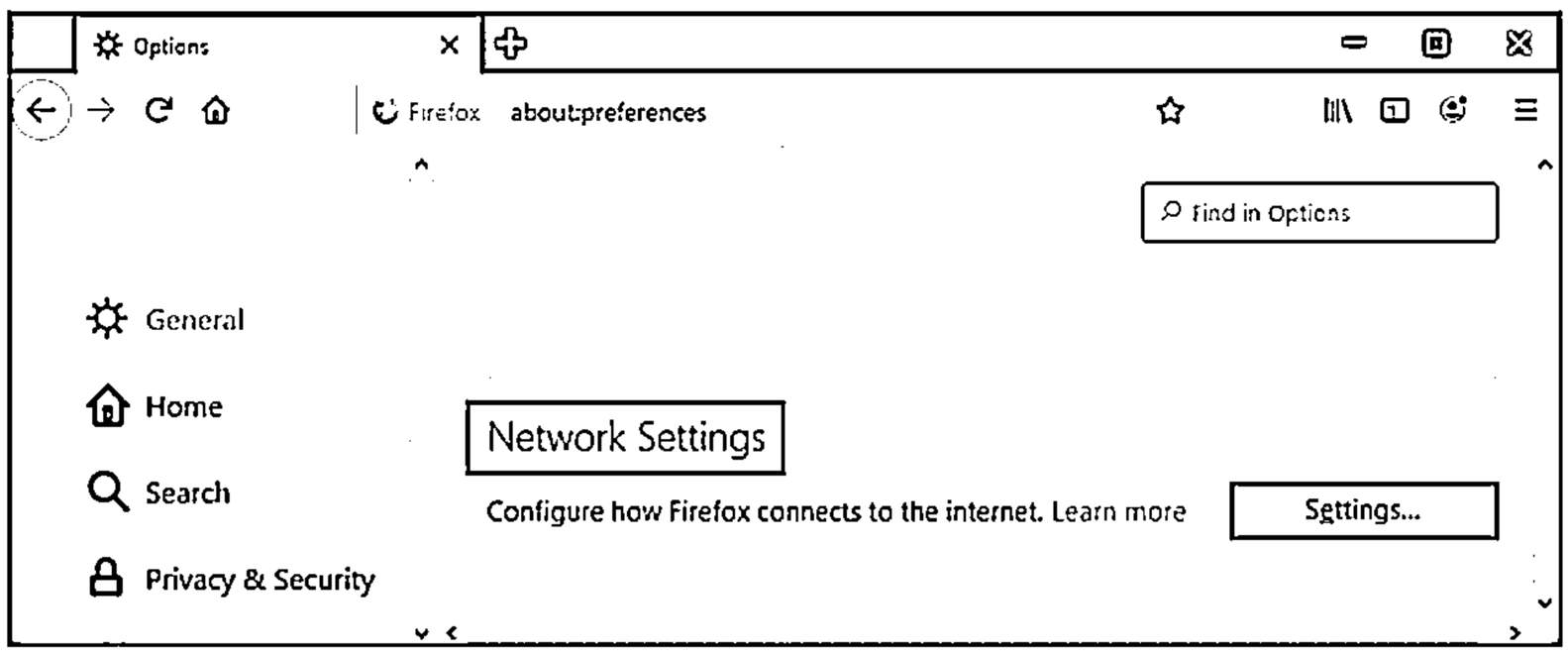


Figure 4.5.3: Firefox Network Settings

7. The **Connection Settings** window appears; under the **Configure Proxy Access to the Internet** section, ensure that the **Use system proxy settings** radio button is selected. Click **OK** and close the **Firefox** browser window.

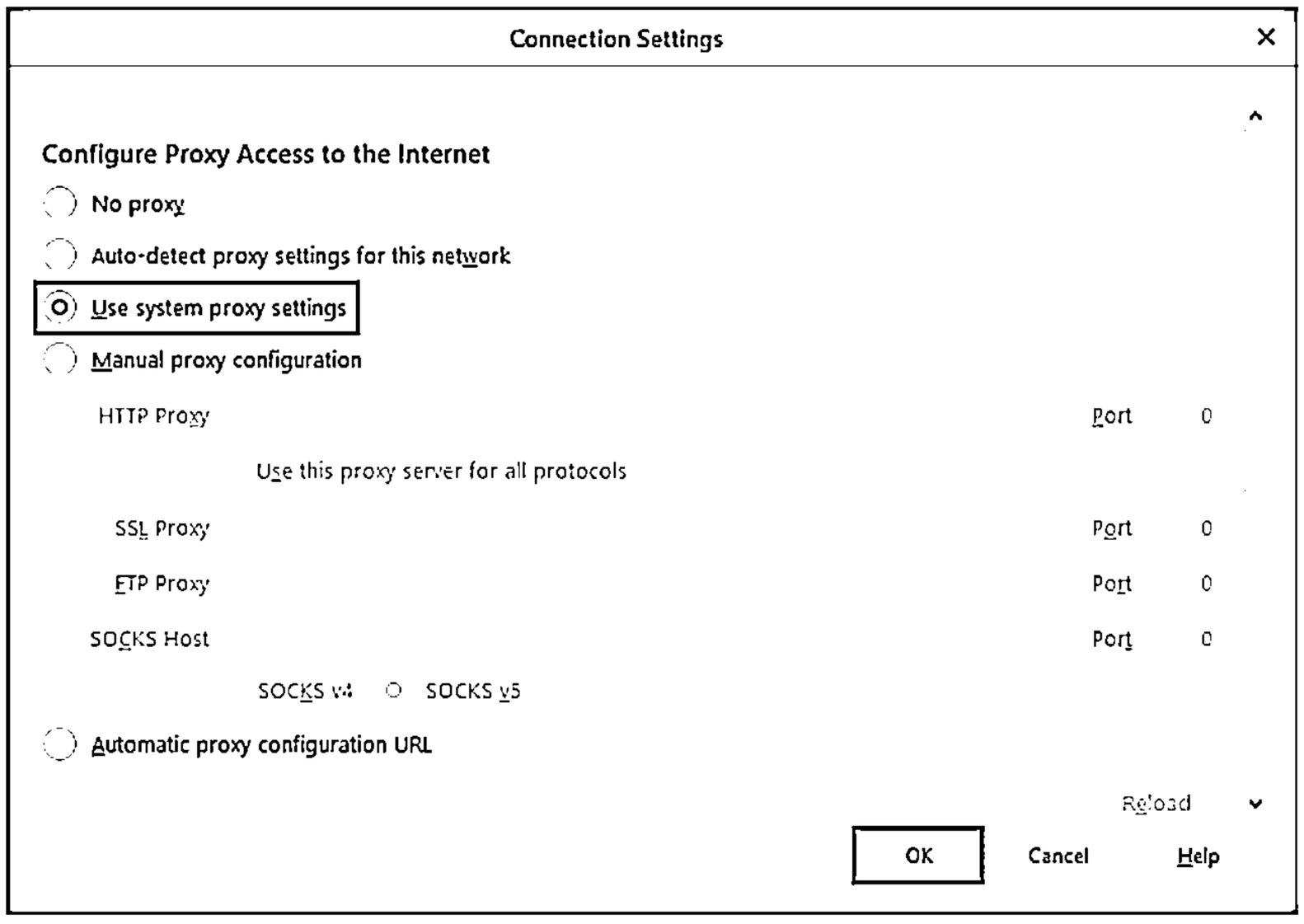


Figure 4.5.4: Firefox Connection Settings

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

8. Now, click on the **Start** menu and launch **ProxySwitcher Standard** from the applications.

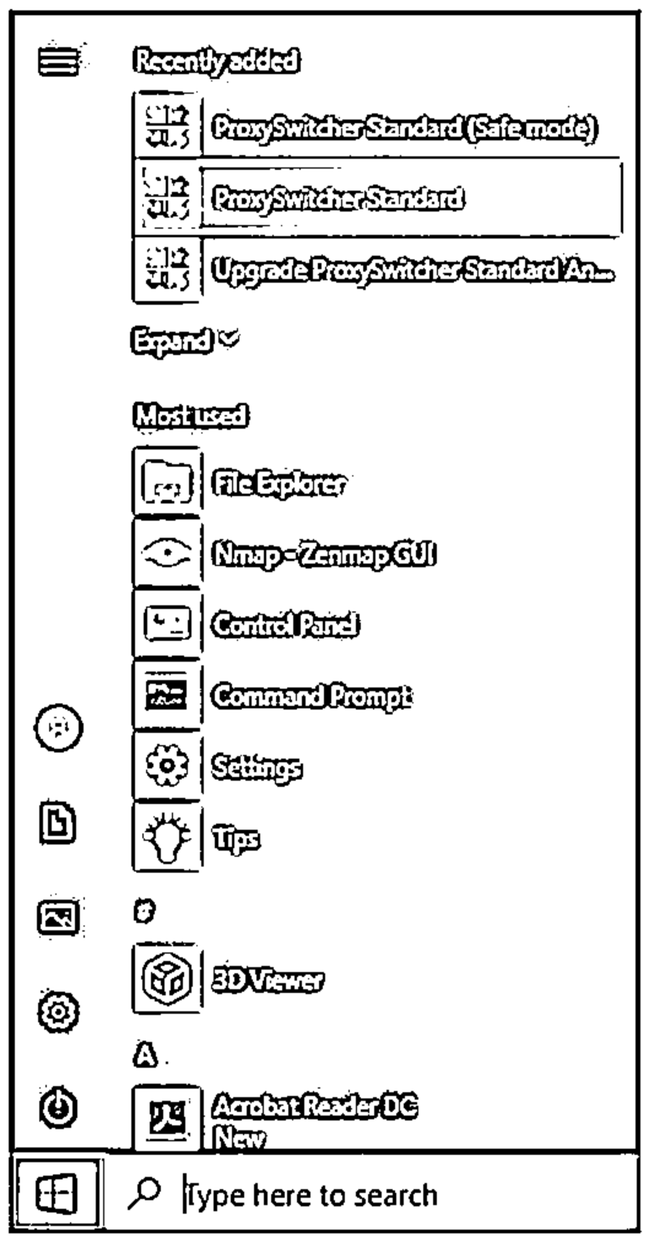


Figure 4.5.5: Windows 10 Apps list

9. The **ProxySwitcher Standard** loads, and its icon appears on **Taskbar**.
10. Click the **Taskbar** icon in the bottom-right corner of the desktop and the click **ProxySwitcher Standard** icon to launch the application.

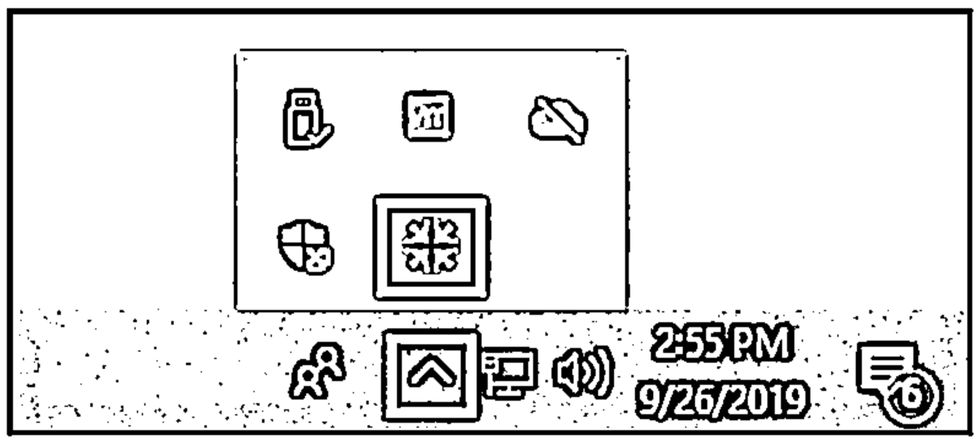


Figure 4.5.6: Selecting ProxySwitcher Standard icon from the taskbar

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

TASK 5.3

Configure Proxy Switcher

11. The **Please Register** window appears; click the **Start 15 Day Trial** button to proceed.
12. The **Common Tasks Wizard** window appears; under **Welcome to the Proxy Switcher**, click **Next**.

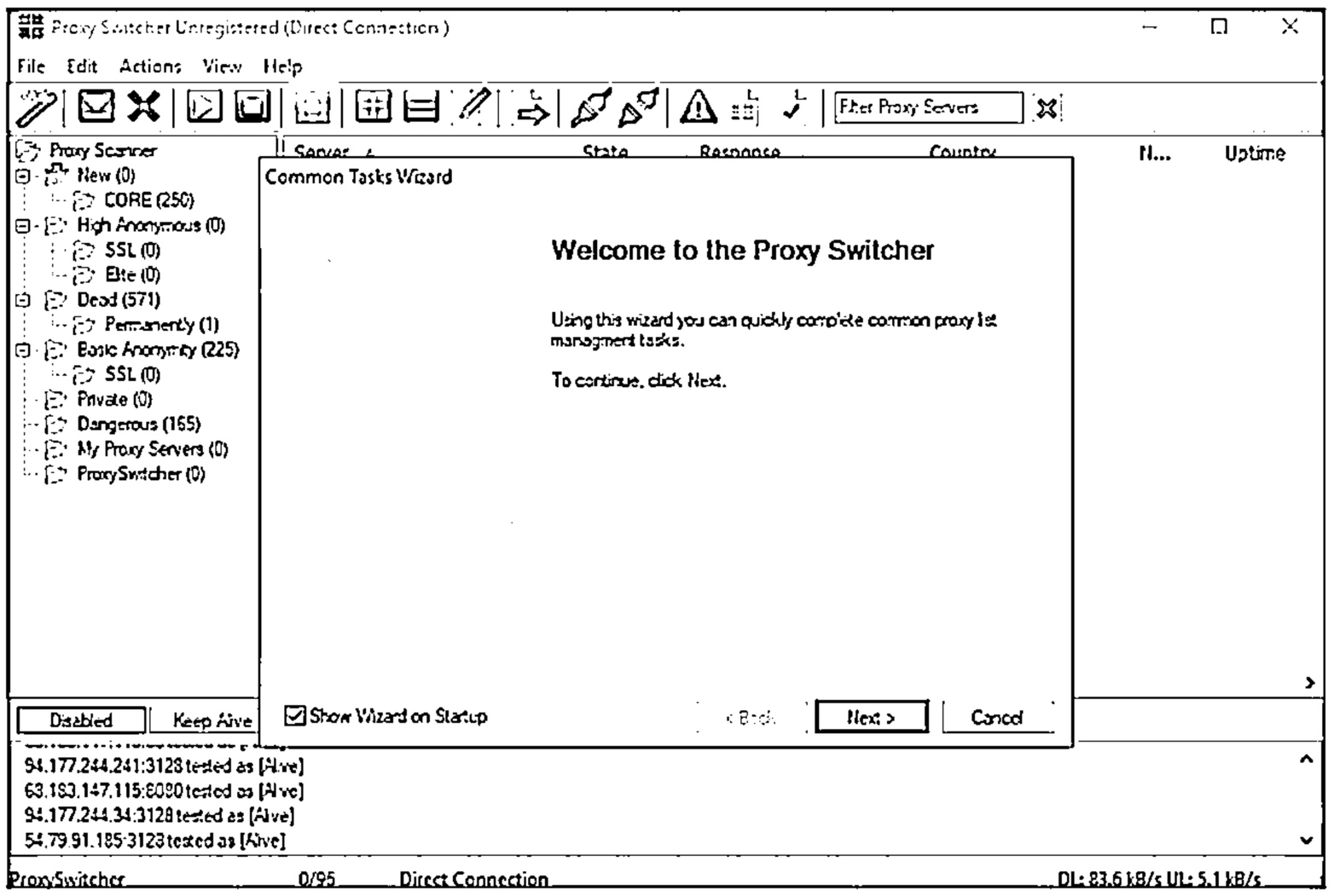


Figure 4.5.7: Proxy List wizard

13. Ensure that the **Find New Server, Rescan Servers, Recheck Dead** radio button is selected under the **Common Tasks** section, and click **Finish**.

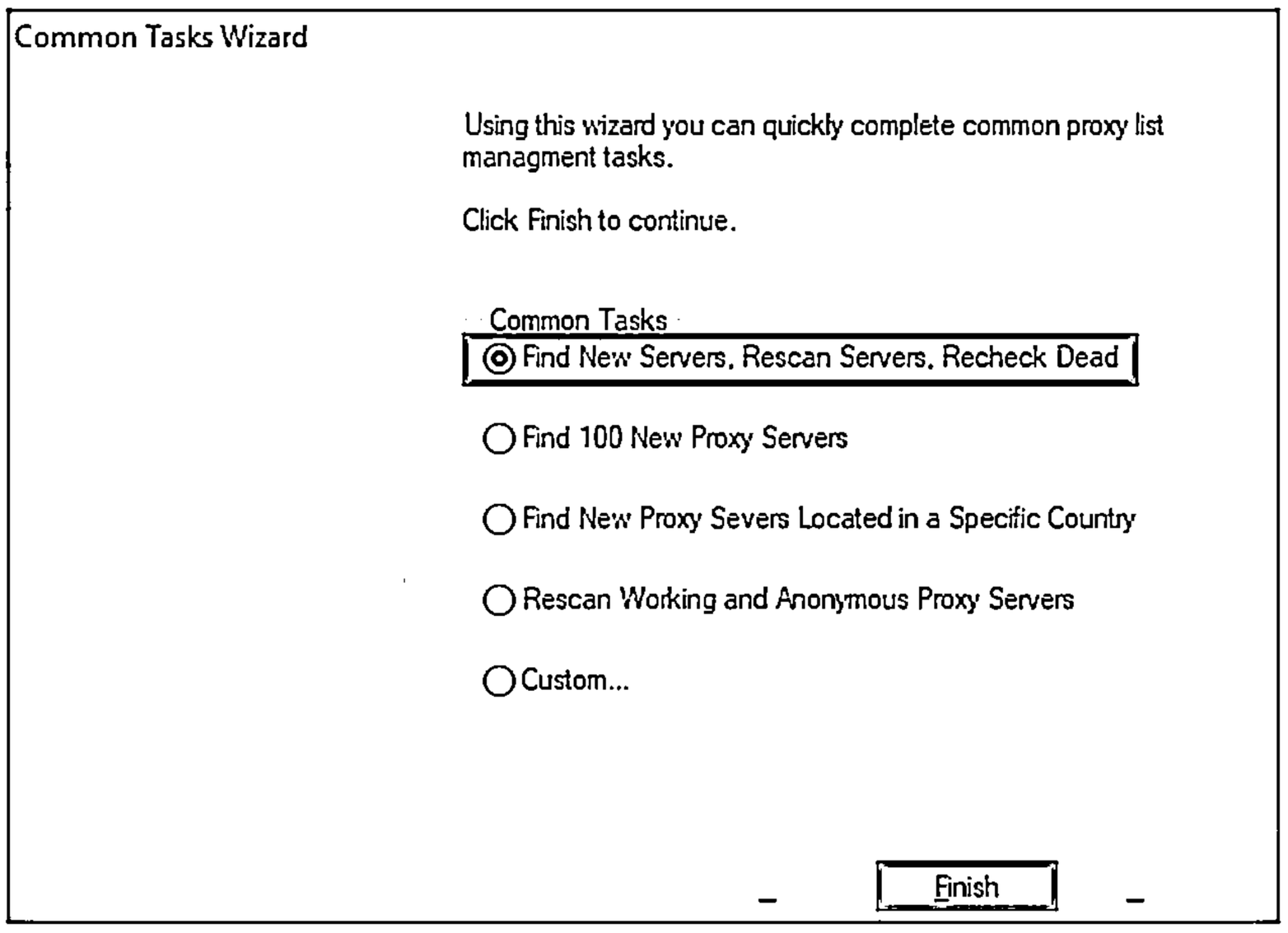


Figure 4.5.8: Selecting common tasks

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

14. **Proxy Switcher** window appears, showing a list of proxy servers in the right pane, as shown in the following screenshot.

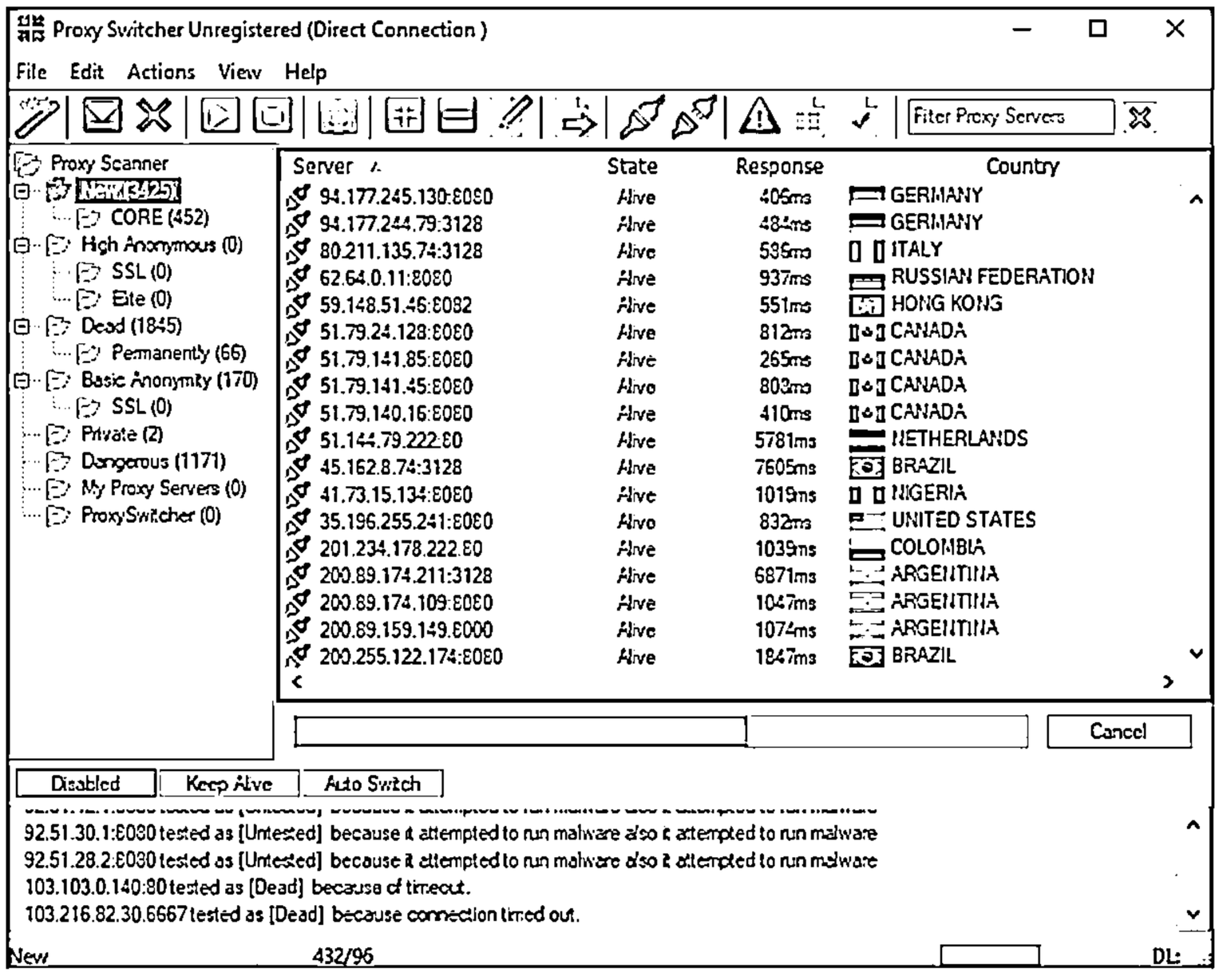


Figure 4.5.9: List of downloaded Proxy Servers

Note: The list of proxy servers might vary in your lab environment.

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

15. Observe the search bar below the server section; once it is completed, click the **Download Proxy Lists** icon ( ) to download the proxy list.

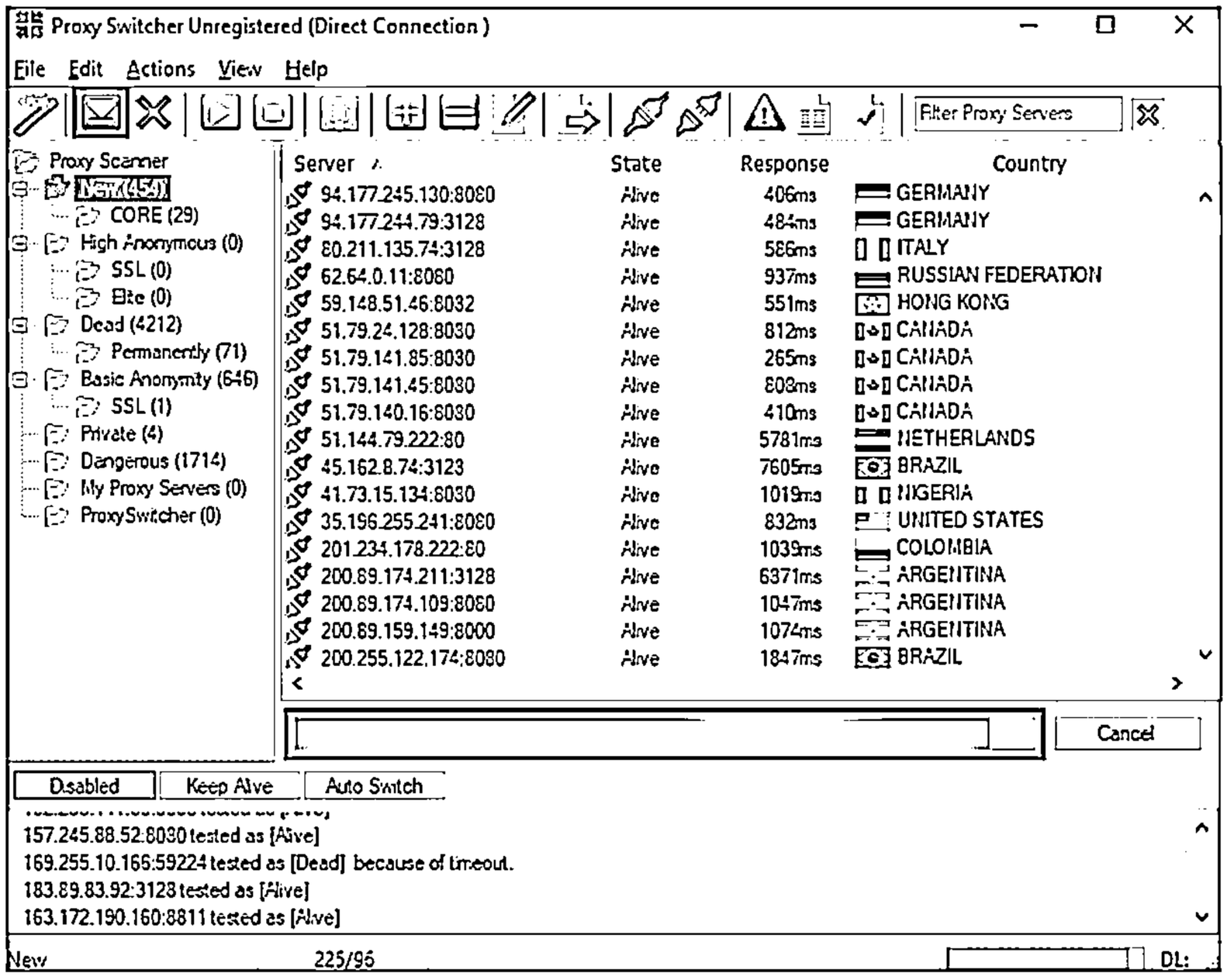


Figure 4.5.10: Downing a list of proxy servers

16. Wait until all the proxy servers are downloaded. This can take a significant amount of time.
17. If you have enough downloaded proxy servers, you can click the **Stop Download** ( ) icon to cancel the download.

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

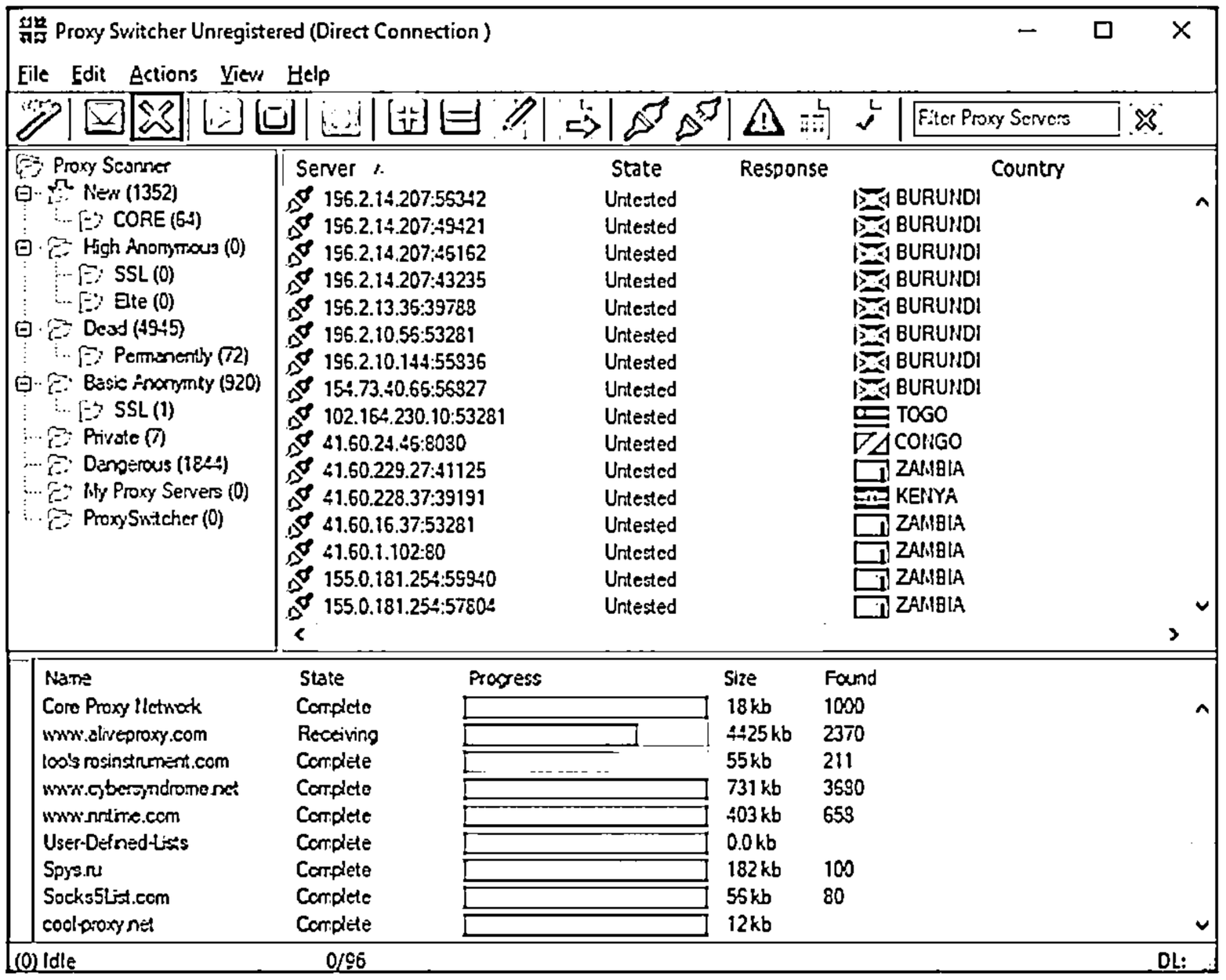


Figure 4.5.11: Proxies being downloaded

TASK 5.4

Assign Proxies

18. Click the **Basic Anonymity** folder in the left-hand pane to display a list of alive proxy servers, as shown in the screenshot.

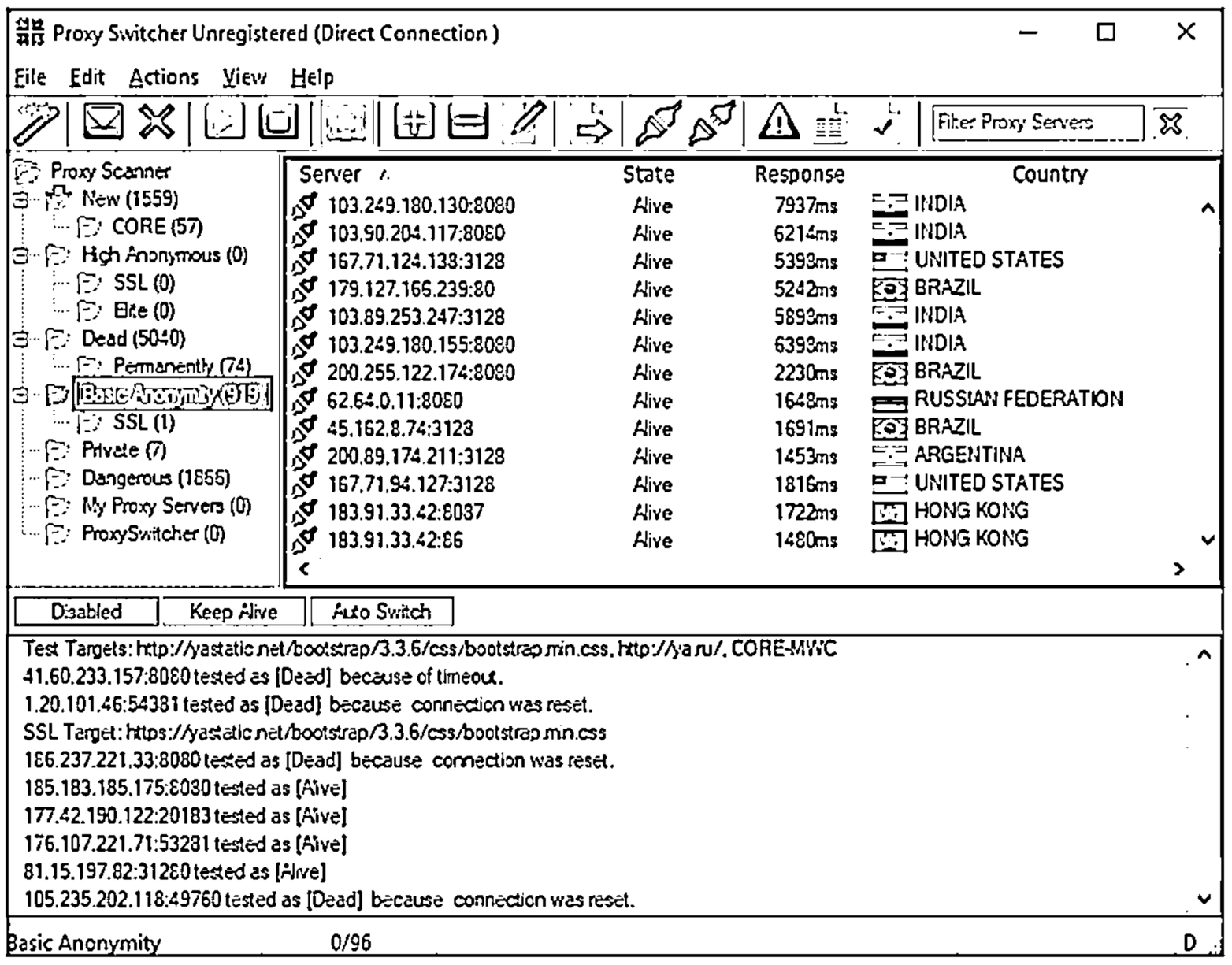


Figure 4.5.12: Searching for alive proxy servers

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

19. Select one proxy server IP address in the right-hand pane. To switch to the selected proxy server, click the **Switch to Selected Proxy Server** ( ) icon.

Note: The proxy selected in this lab might vary in your lab environment.

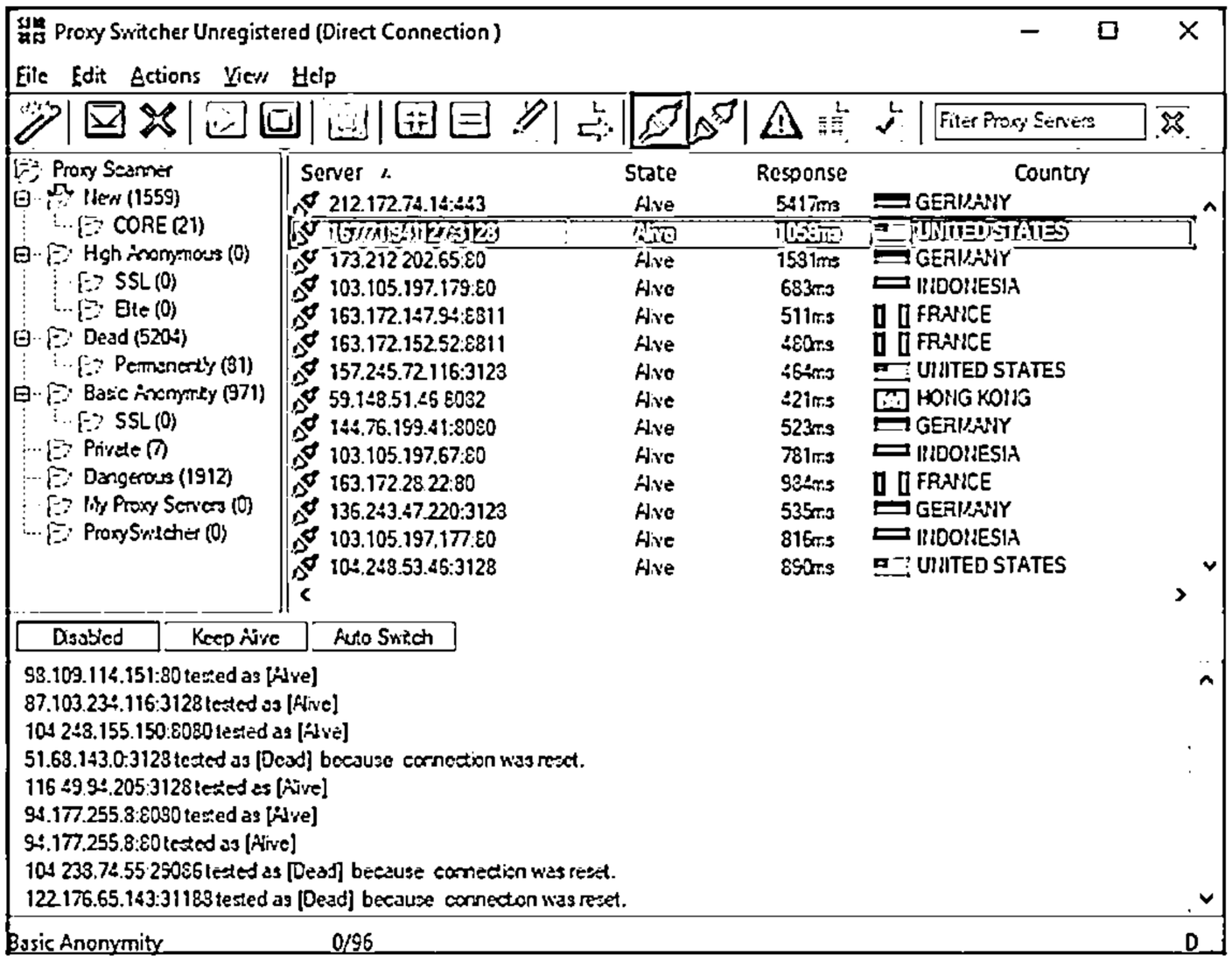


Figure 4.5.13: Selecting a proxy server

20. When the proxy server is connected, it will show the connection icon as .

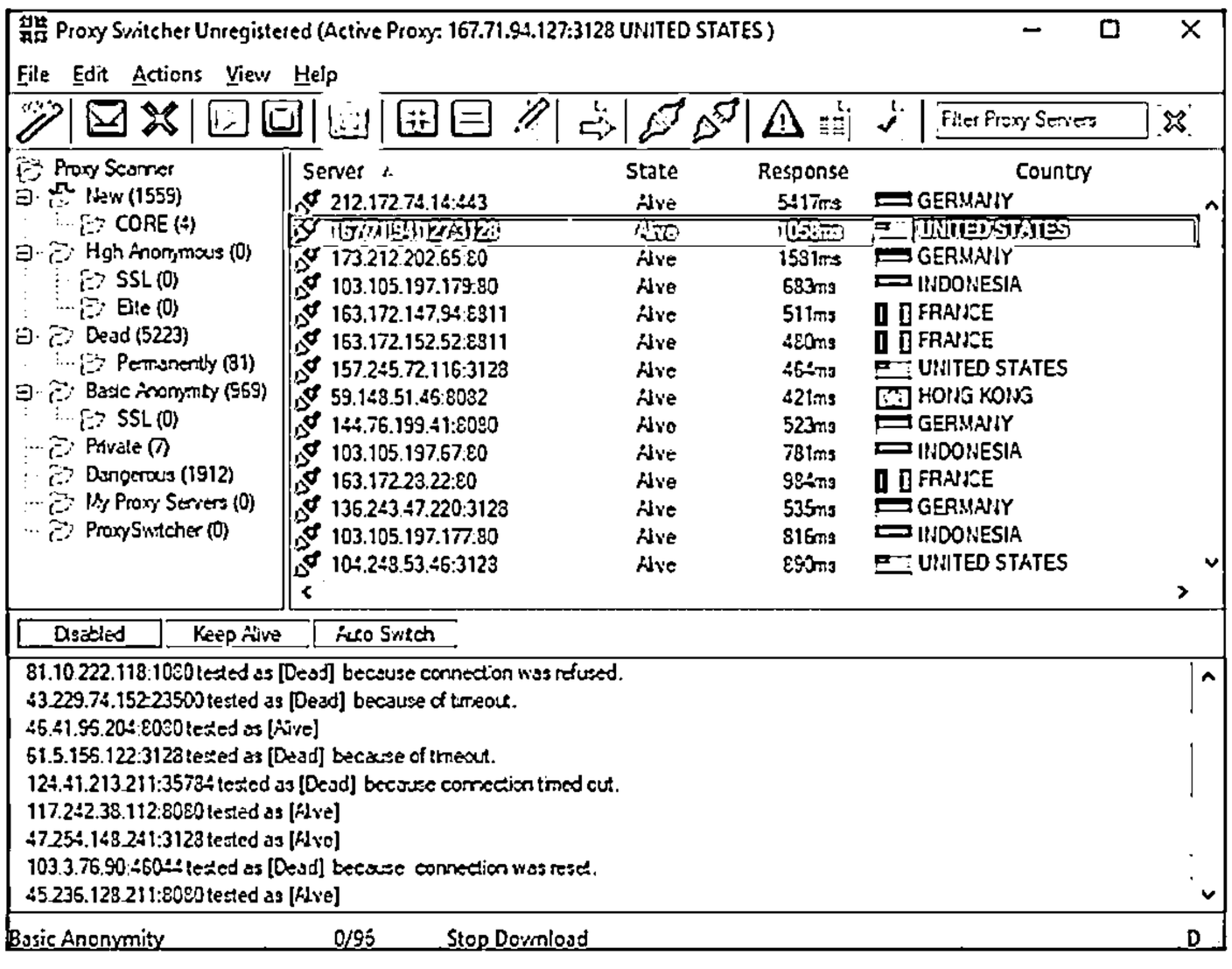


Figure 4.5.14: Proxy server successfully connected

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

TASK 5.5

Test Proxies

21. Launch the **Mozilla Firefox** web browser and enter the URL **http://www.proxyswitcher.com/check.php** to check the selected proxy-server connectivity. If the connection is successful, the following information is displayed in the browser:

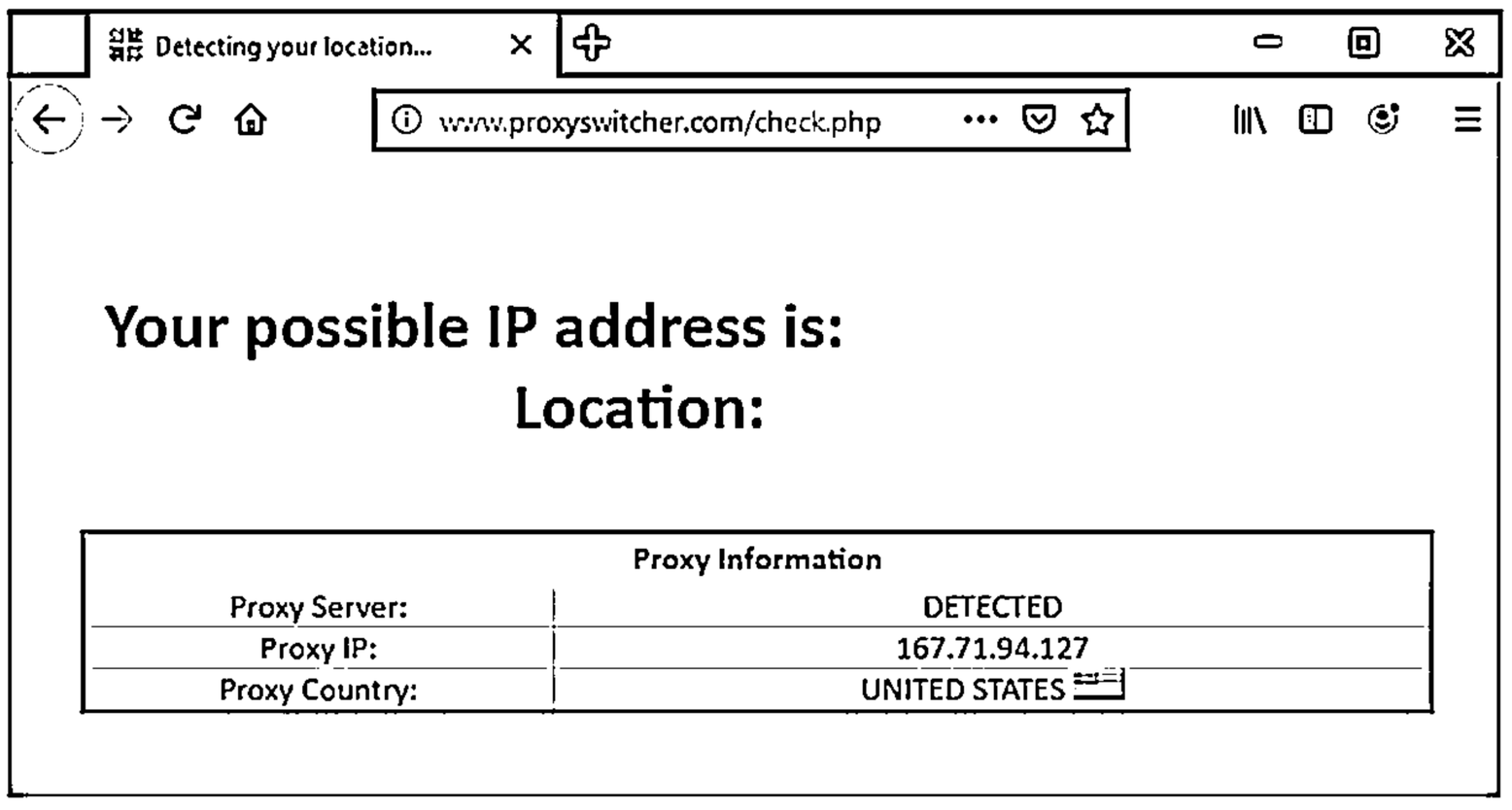


Figure 4.5.15: Detected Proxy Server

Note: The information displayed above may differ in your lab environment.

22. If the connection is unsuccessful, try selecting another proxy from **Proxy Switcher**, and repeat **Step 19**.

23. To ensure that the proxy is assigned, open a new tab and browse **https://www.google.com/**. In the search field, type **What is my ip** and press **Enter**.

24. The proxy IP address (**167.71.94.127**) is displayed, which infers that the legitimate address is masked and the proxy is in use.

Note: The displayed IP address might differ in your lab environment.

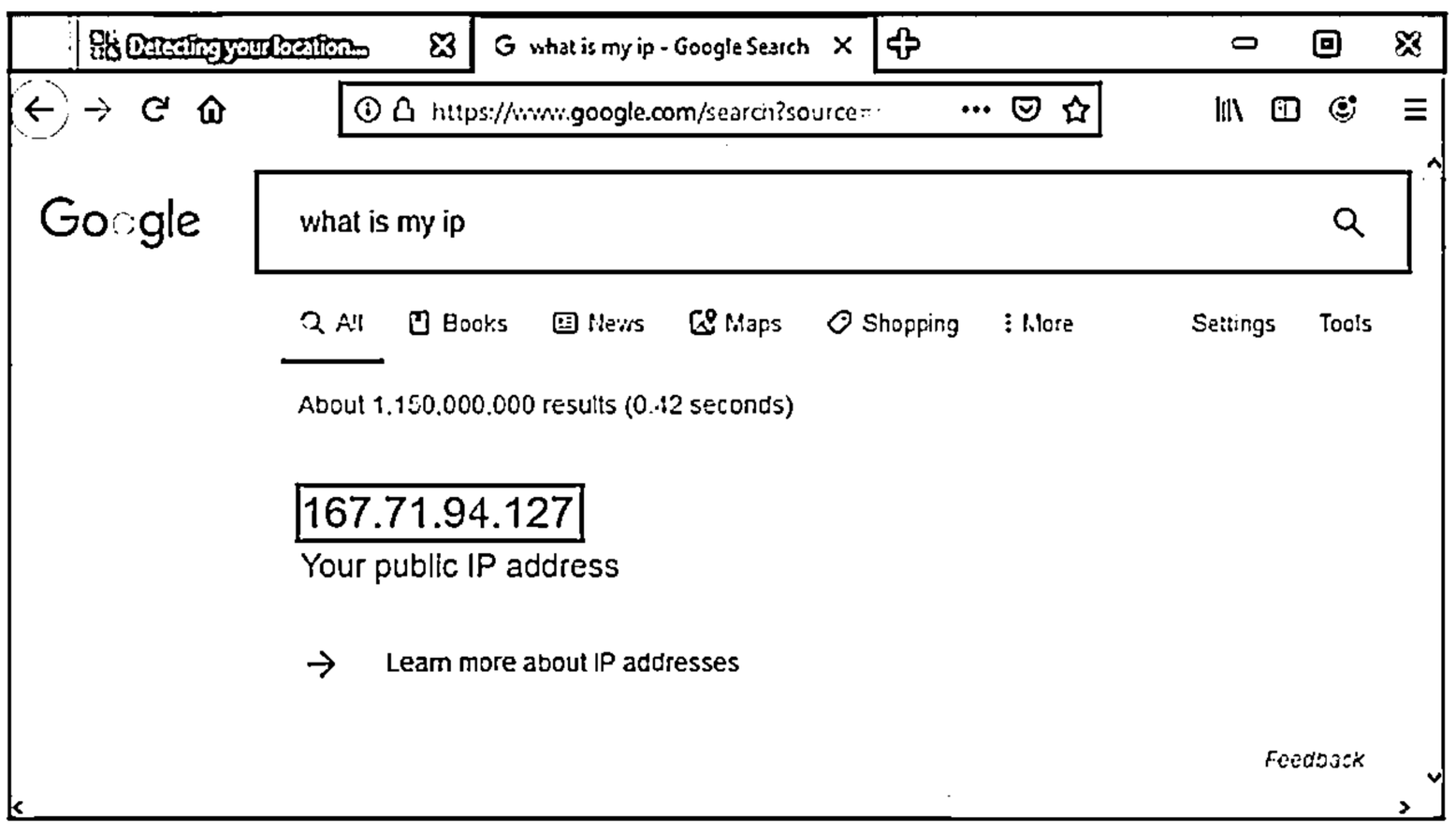


Figure 4.5.16: Testing your IP address

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

25. Open a new tab in your **web browser** and surf anonymously using this proxy.

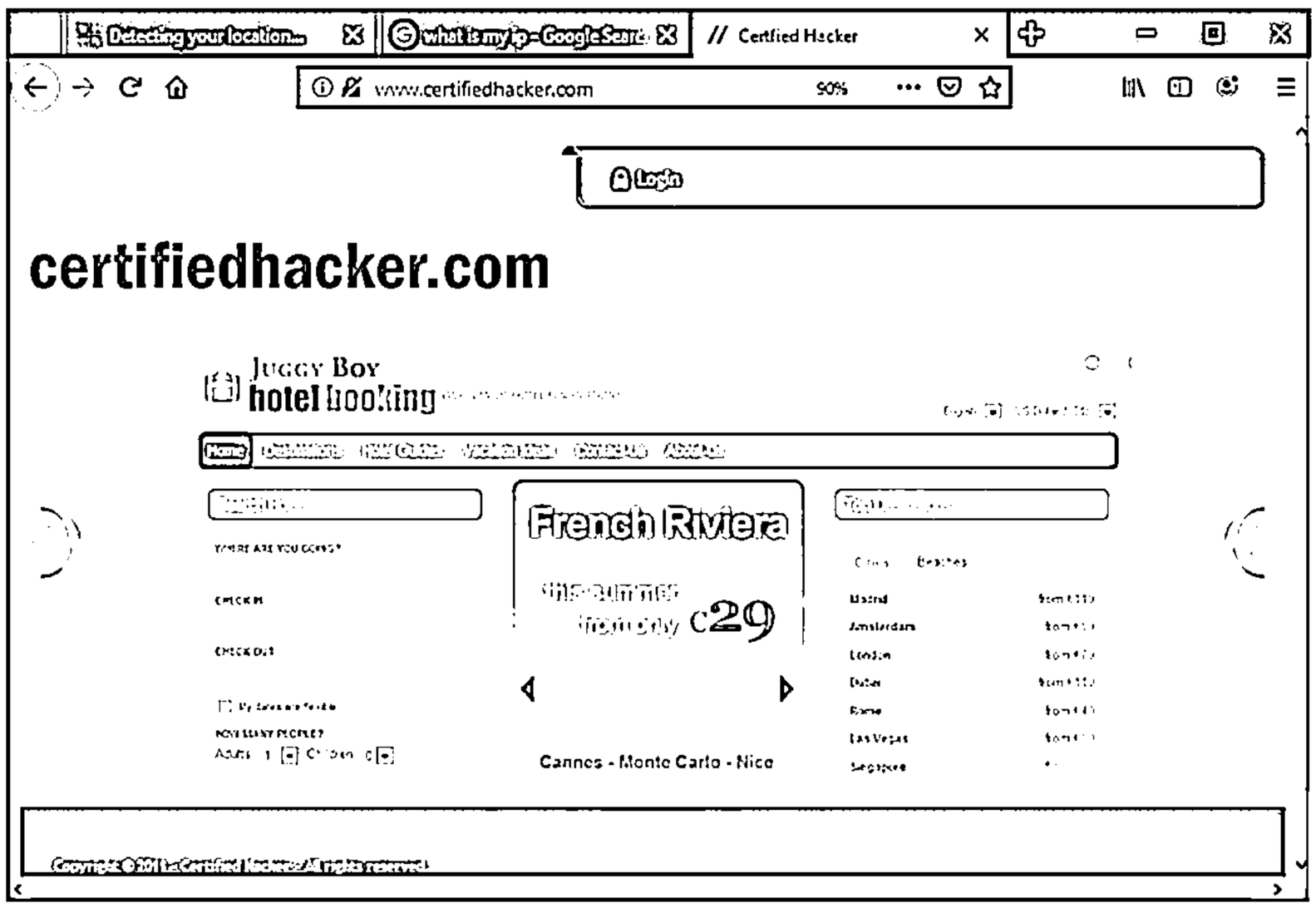


Figure 4.5.17: Surfing internet using Proxy server

26. This concludes the demonstration of anonymously surfing the Internet using Proxy Switcher.
27. Close all open windows and document all the acquired information.
28. Navigate to **Control Panel → Programs → Programs and Features** and uninstall the **Proxy Switcher** application

TASK 6 Browse Anonymously using CyberGhost VPN

Here, we will use CyberGhost VPN to browse the Internet anonymously.

TASK 6.1
Install CyberGhost VPN

1. In the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 03 Scanning Networks\Proxy Tools\CyberGhost VPN** and double-click **cgsetup_en_NMKh64apsGD93kapeBUc.exe**.

Note: If a **User Account Control** window appears, click **Yes**.

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

CyberGhost VPN hides your IP and replaces it with one of their choice, thereby allowing you to surf anonymously and access blocked or censored content. It encrypts the connection and does not keep logs, thus securing data.

2. **Downloading CyberGhost installer...** appears; once the **CyberGhost Setup** window appears, click **Accept**.

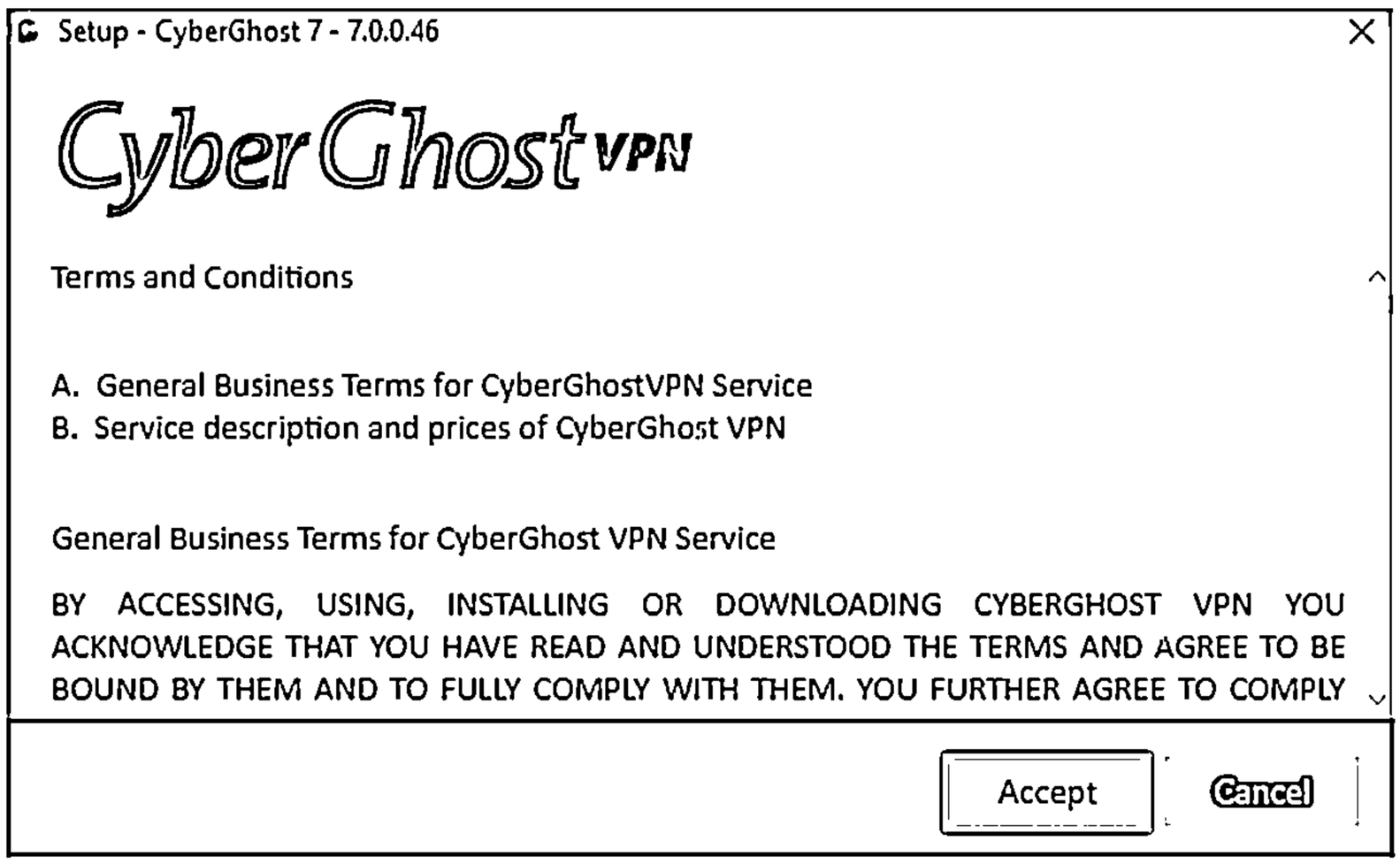


Figure 4.6.1: CyberGhost Setup window

3. Follow the installation steps to install **CyberGhost**.
4. If a **Windows Security** pop-up appears, click **Install**.

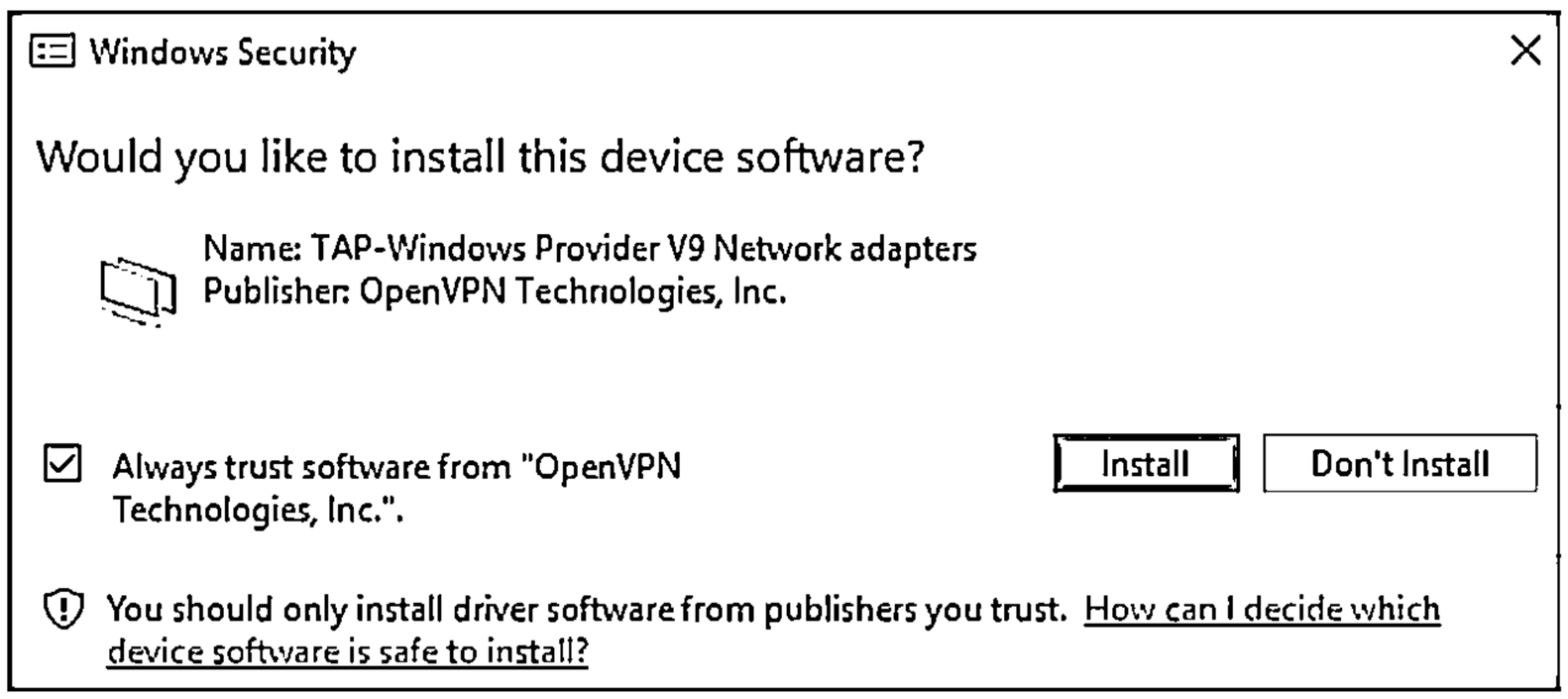


Figure 4.6.2: Windows Security pop-up

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

5. Once the installation is complete, the CyberGhost **Create account** window appears.

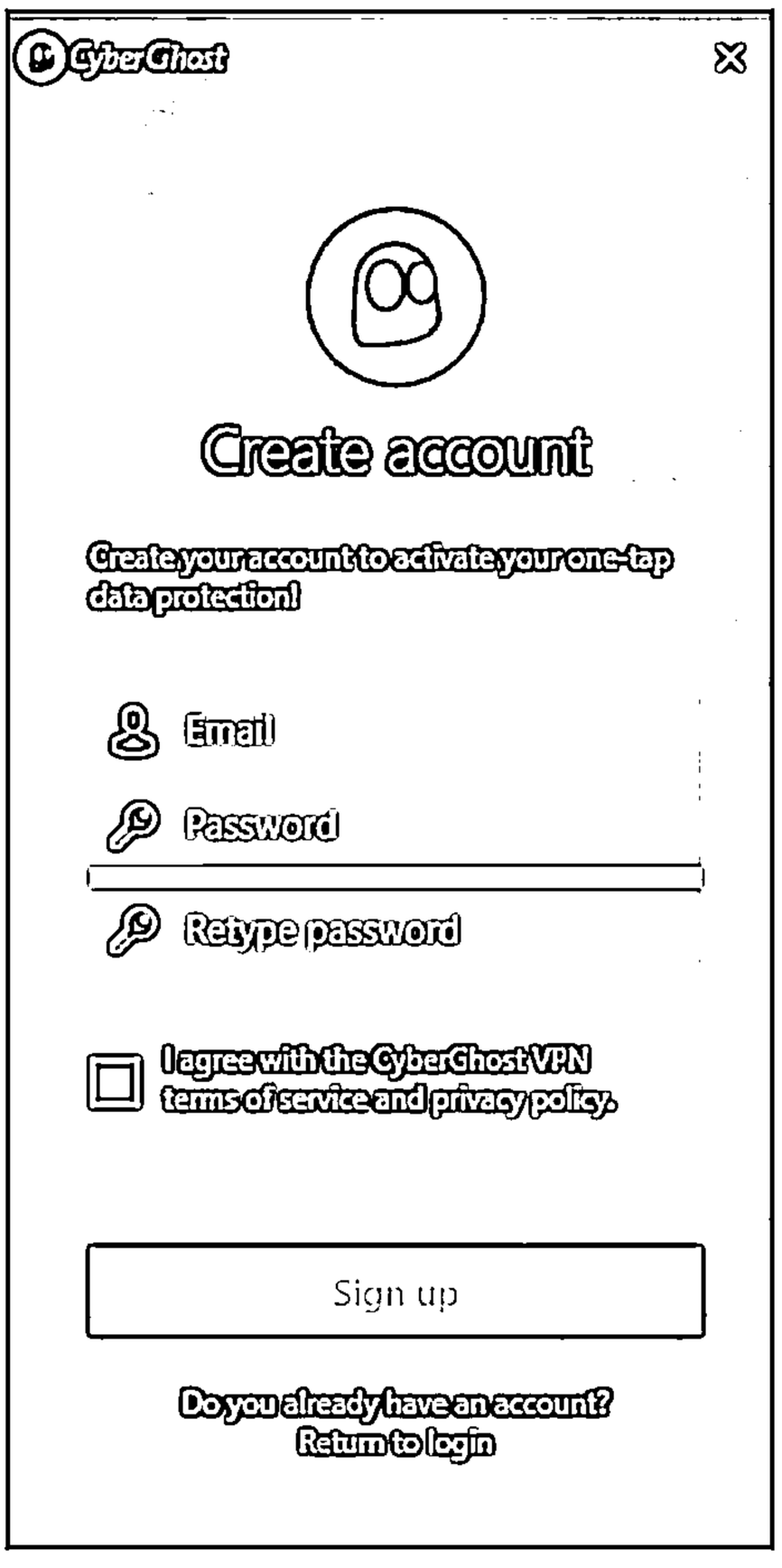


Figure 4.6.3: CyberGhost Create account window

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

TASK 6.2

Create Account

6. Create an account using your personal details and click on **Sign Up**.

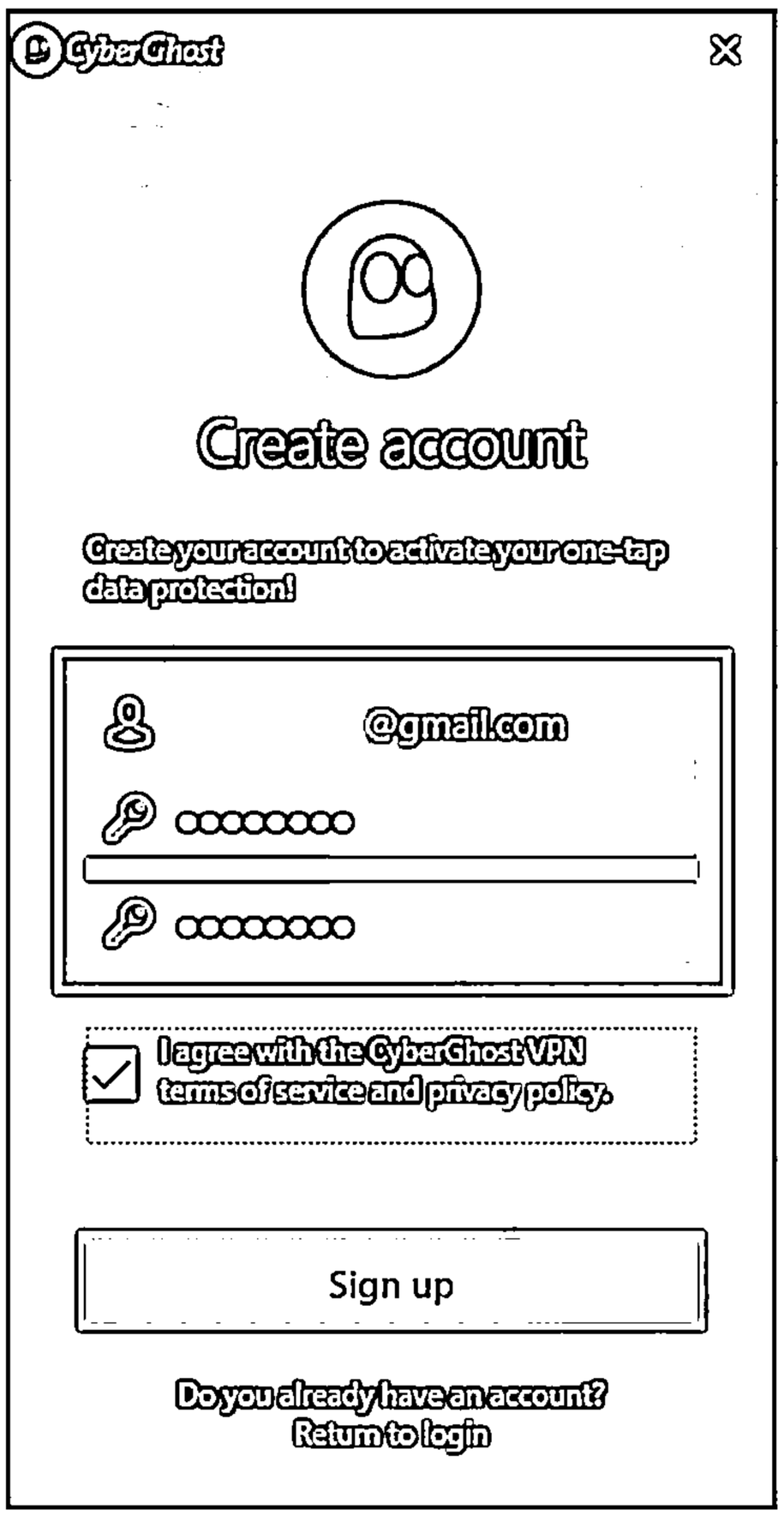


Figure 4.6.4: CyberGhost creating account

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

7. You will receive an activation email on your personal email. Open the email and click on **Activate Trial** to start your trial version of CyberGhost.

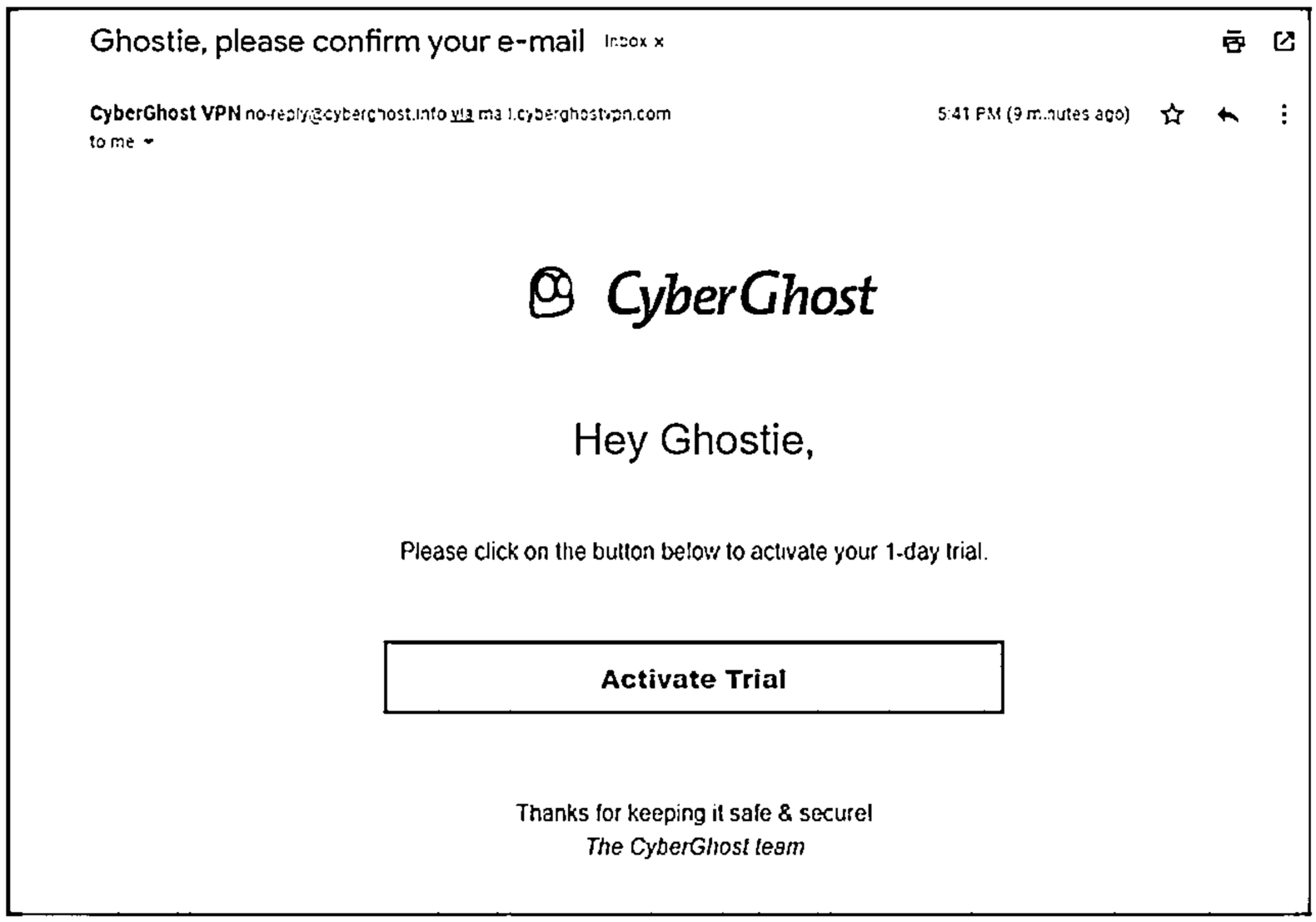


Figure 4.6.5: Email for Activation of a trial version

8. Now, switch to the **CyberGhost** login page and log in with the email address and password provided earlier; click **Log in.**

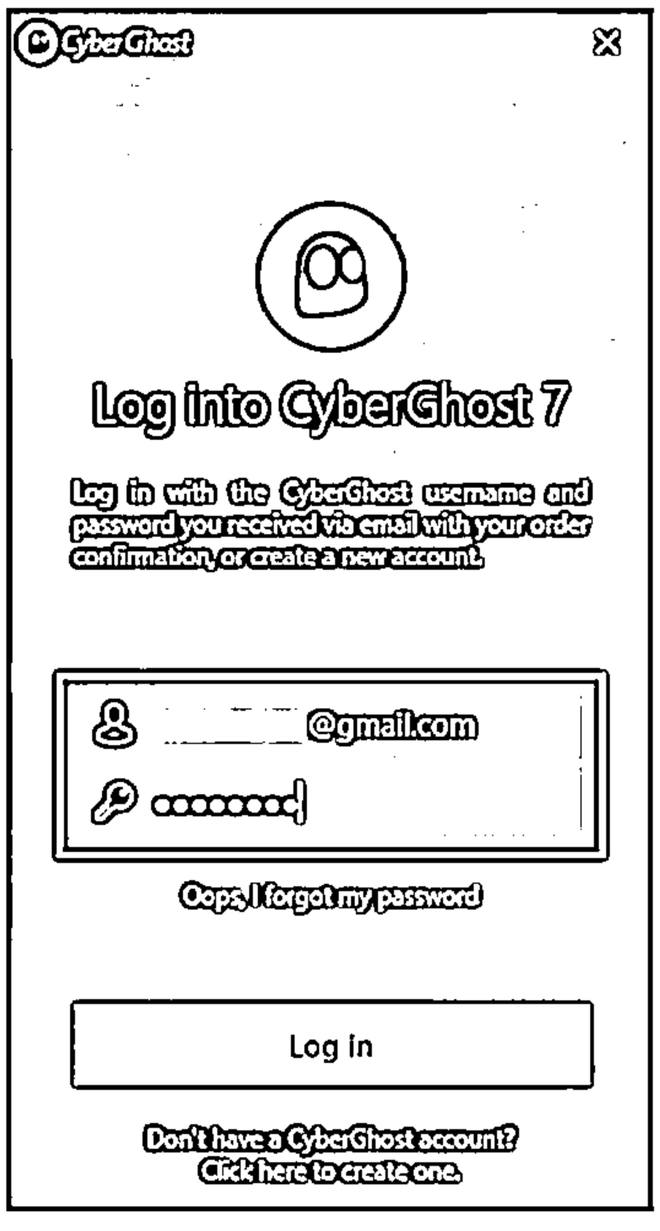


Figure 4.6.6: CyberGhost Log in

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

9. The CyberGhost window appears, displaying **VPN not connected!**

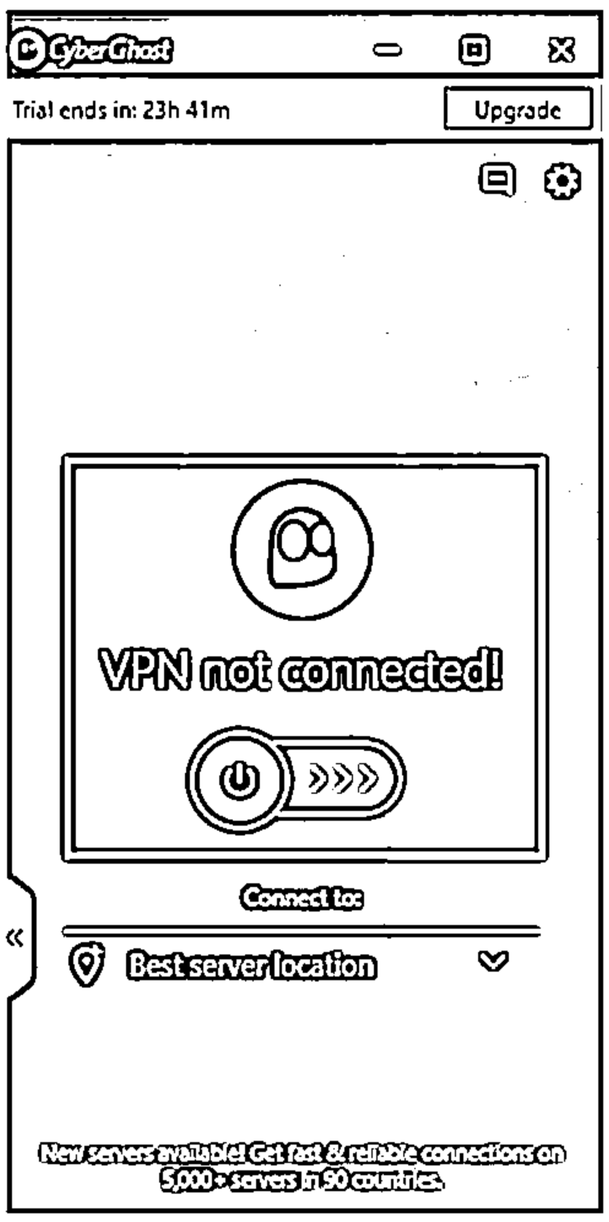


Figure 4.6.7: CyberGhost window

10. Now, click the **Settings** icon and select **Settings** from the options.

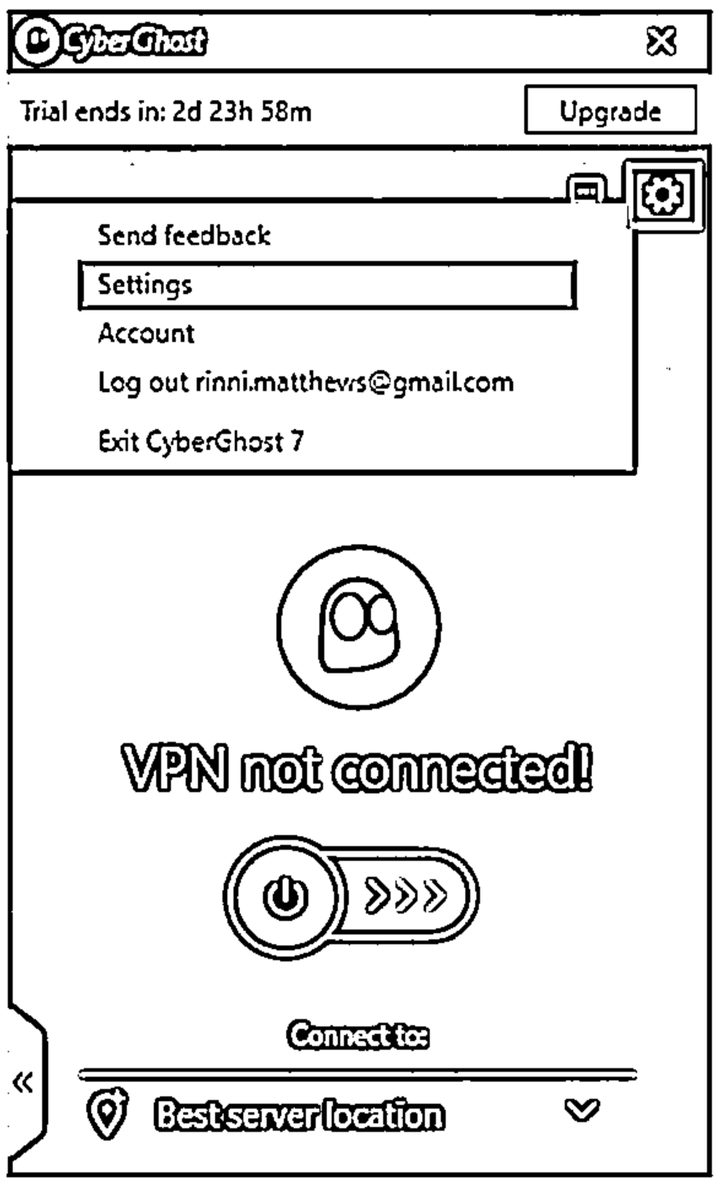


Figure 4.6.8: CyberGhost selecting the setting icon

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

TASK 6.3

Choose a Proxy from CyberGhost

11. The **CyberGhost Settings** window appears; click on **All server** from the left-hand pane.

Note: The list of the servers may vary in your lab environment

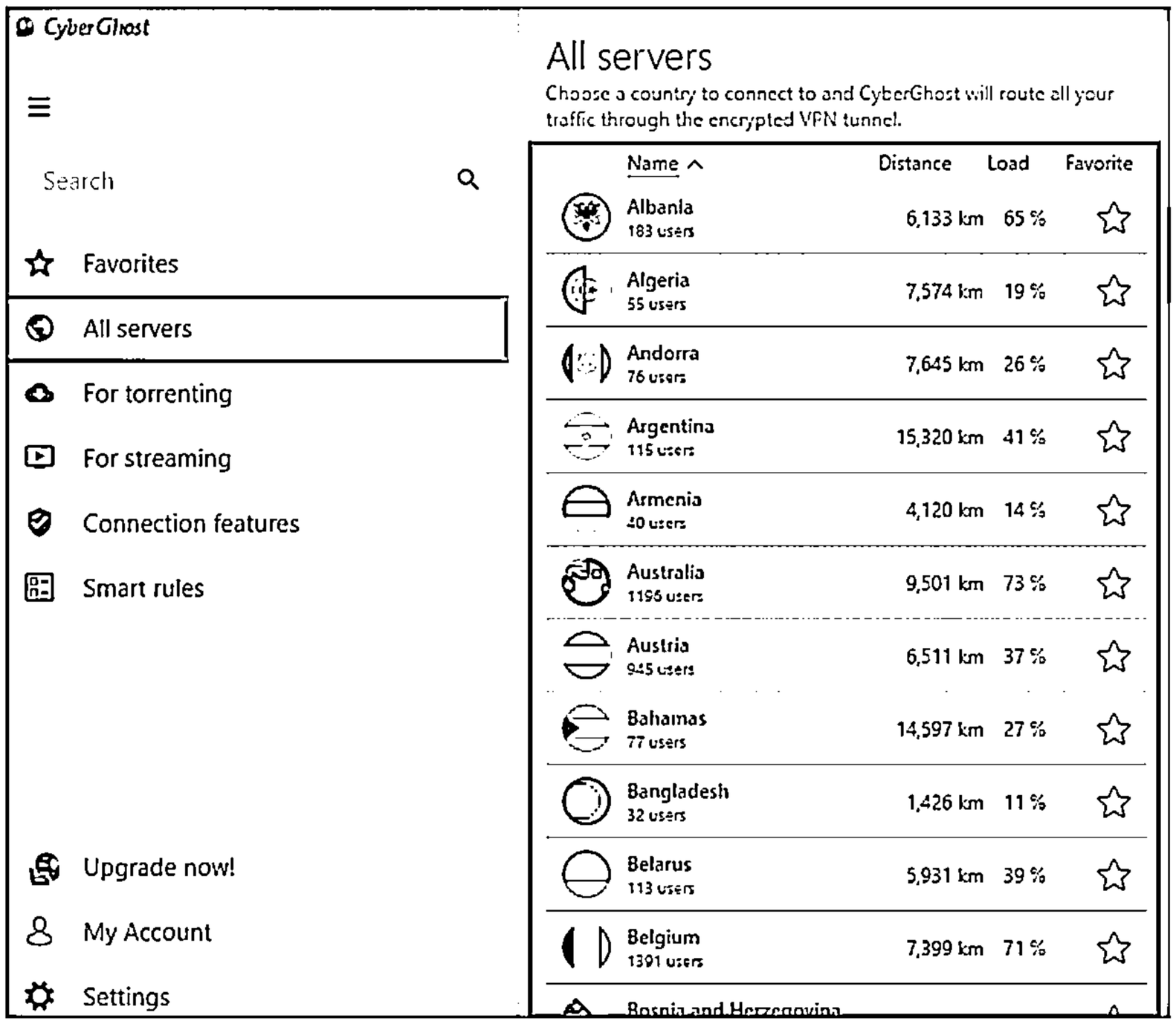


Figure 4.6.9: CyberGhost All servers window

12. Click to select any proxy server from the available options in the **All servers** section (here, **Albania**) and click on the power icon ( ) under **VPN now connected!**, as shown in the screenshot.

Note: If the CyberGhost window appears indicating that all free user slots are booked, then close the window and select another proxy server from the "all servers" list.

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

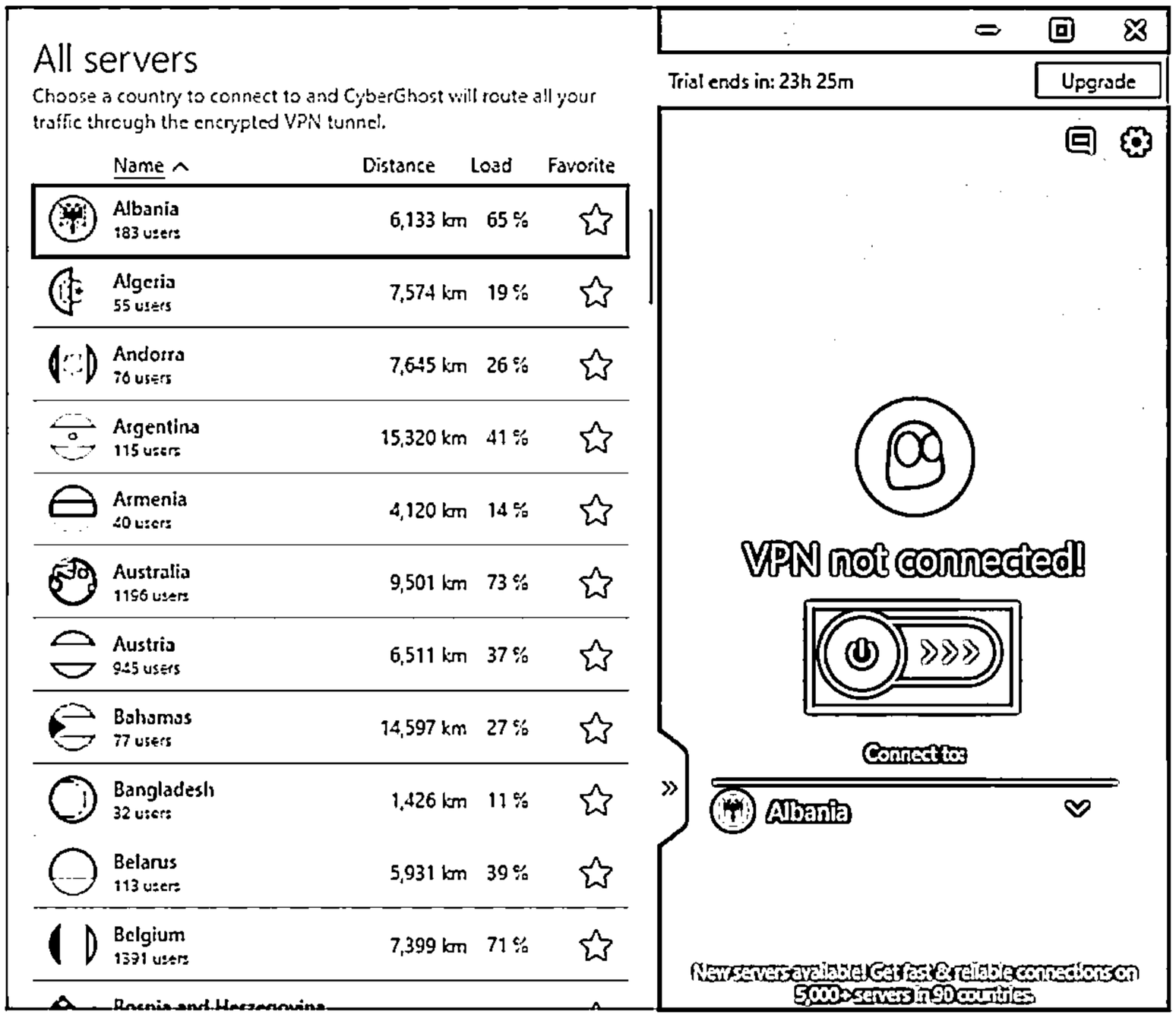


Figure 4.6.10: CyberGhost selecting proxy server

13. **CyberGhost** attempts to establish a connection to the proxy server. On successfully establishing a connection, **VPN connected!** appears.

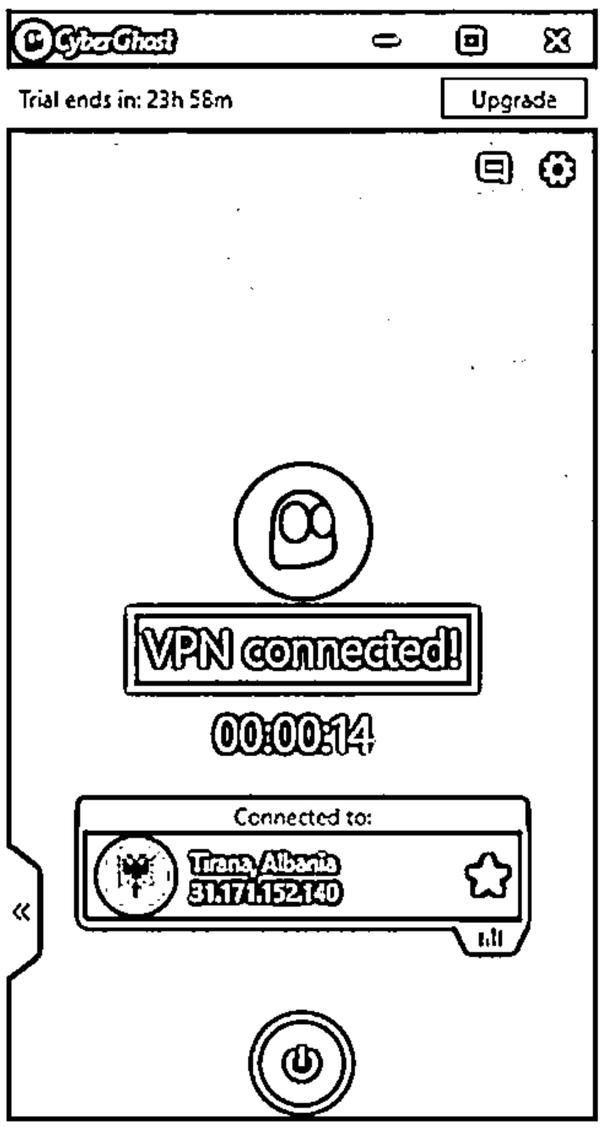


Figure 4.6.11: CyberGhost connection established

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

TASK 6.4

Browse Internet

14. Minimize the **CyberGhost** window and launch the **Mozilla Firefox** web browser; type the URL **https://whatismyipaddress.com/location-feedback** in the address bar and press **Enter**.

Note: If a **Will you allow whatismyipaddress.com to access your location?** pop-up appears, click **Allow Location Access**.

15. Scroll down to the **Geographical Details** section. Observe that the server IP address and location has changed to **31.171.152.140** and **Albania**.

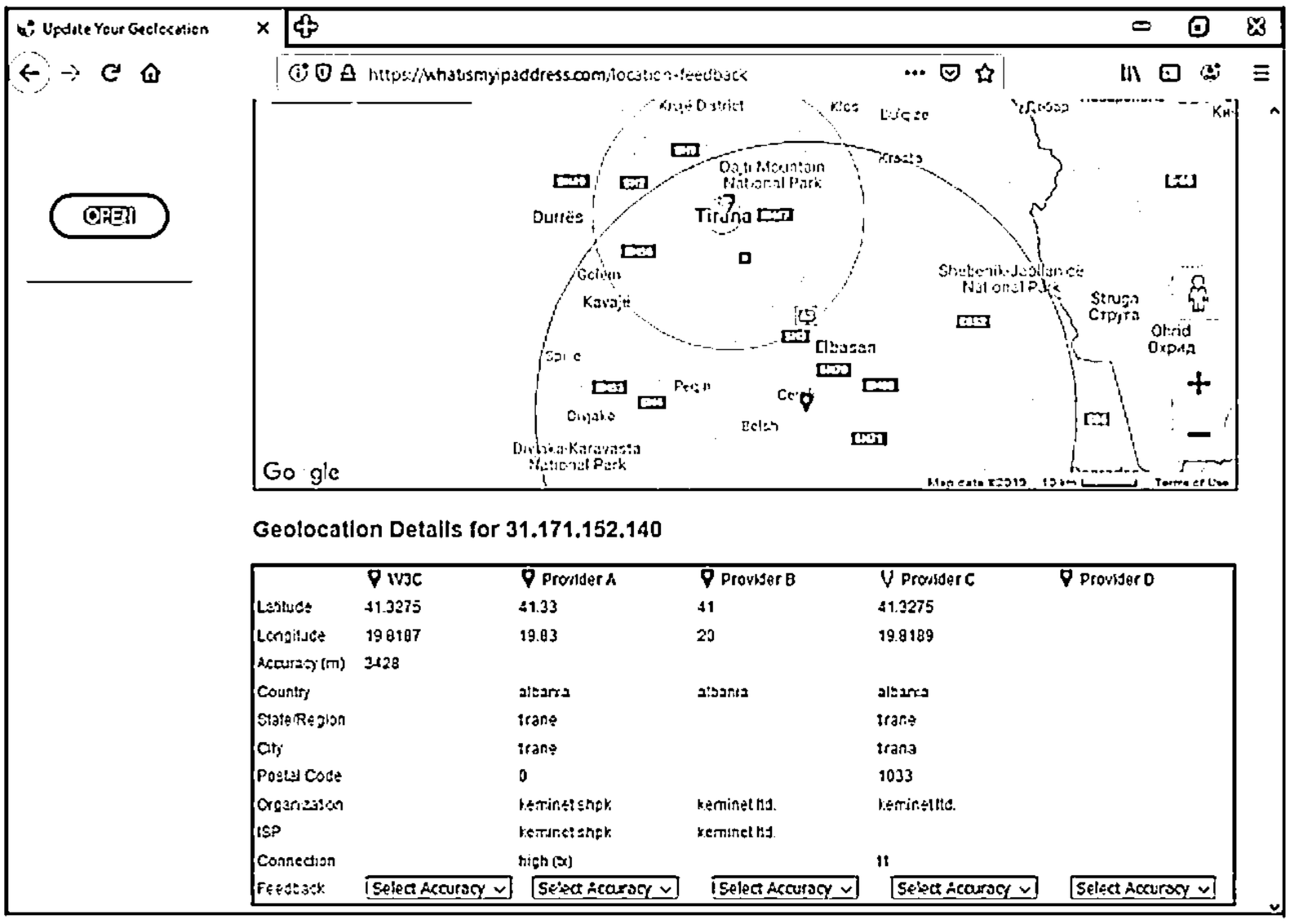


Figure 4.6.12: Testing your IP address

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

16. Open a new tab in the **web browser** and surf anonymously using this proxy.

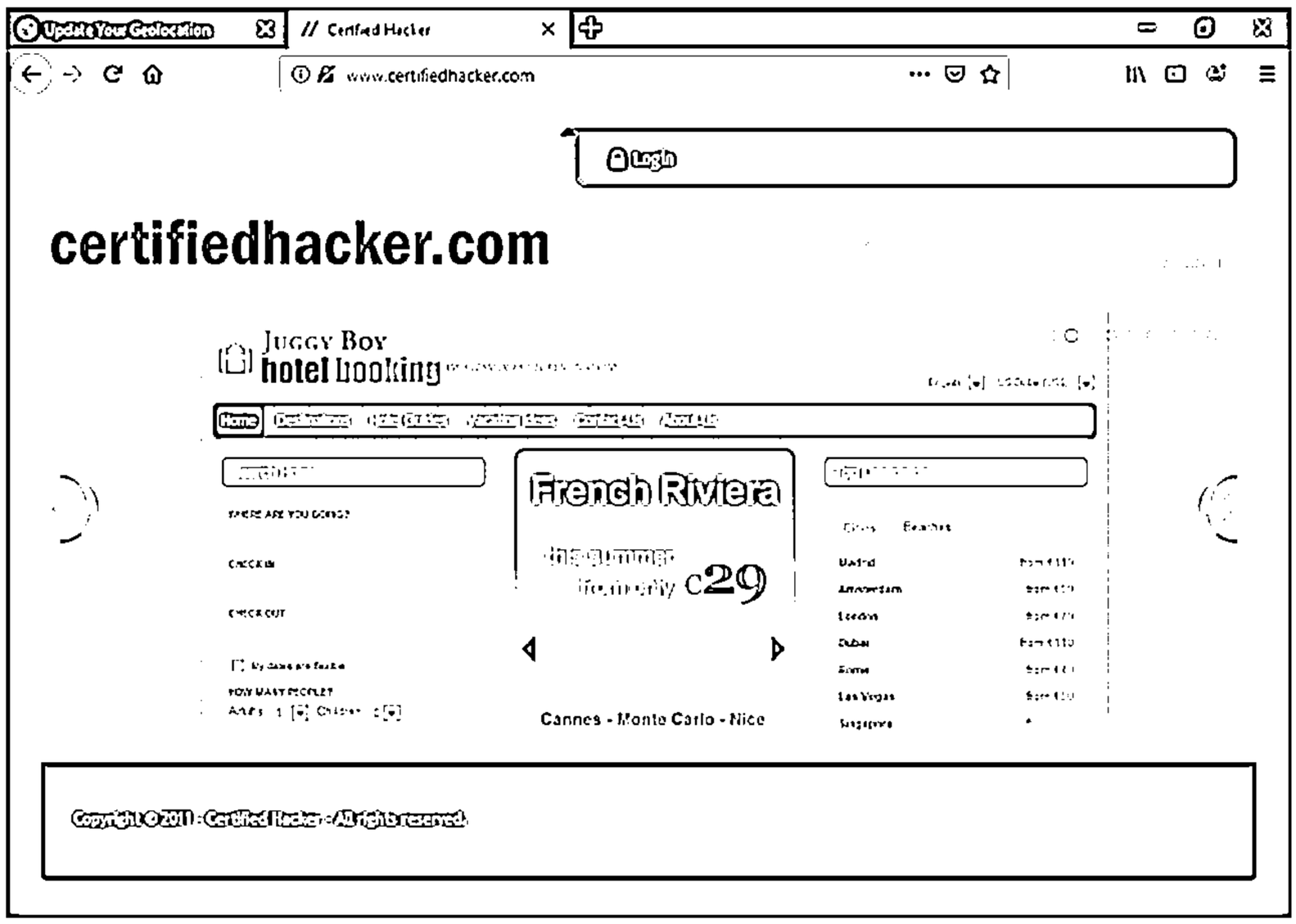


Figure 4.6.13: Surfing internet using Proxy server

17. Once you are done browsing, in the CyberGhost window, click the **Power** icon to disconnect the proxy, as shown in the screenshot.

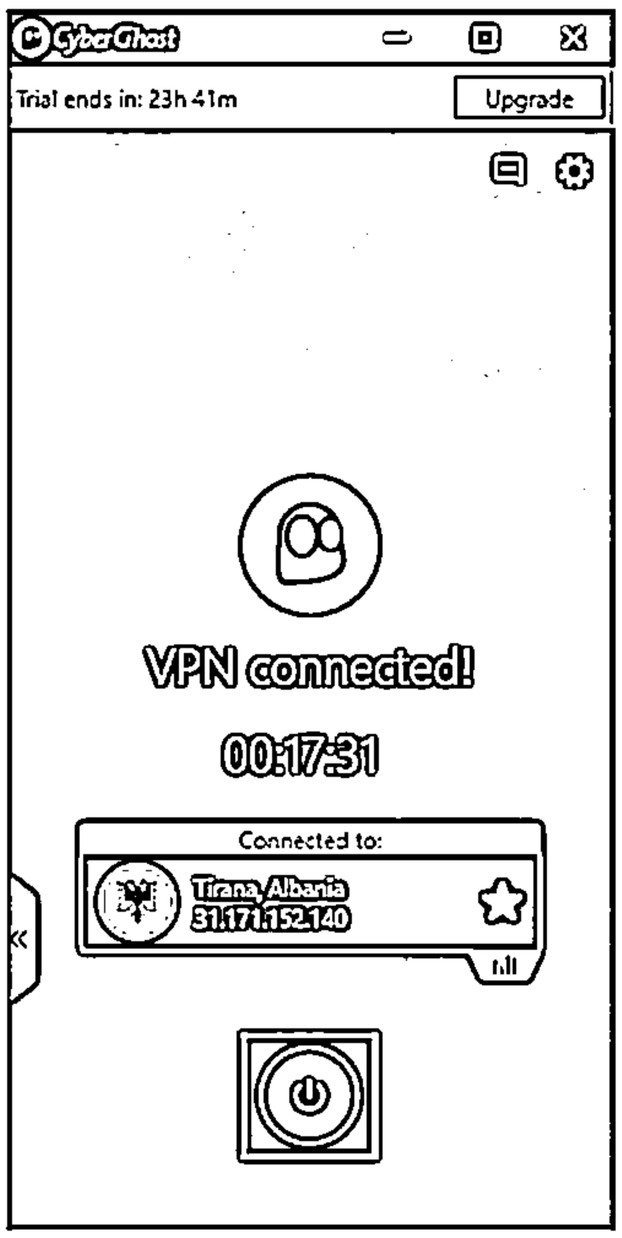


Figure 4.6.14: Turning Off the Proxy

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

18. This concludes the demonstration of anonymously surfing the Internet using CyberGhost.
19. Close all open windows and document all the acquired information.
20. Navigate to **Control Panel** → **Programs** → **Programs and Features** and uninstall the **CyberGhost VPN** application
21. Turn off the **Windows 10** virtual machine.

You can also use other proxy tools such as **Burp Suite** (https://www.portswigger.net), **Tor** (https://www.torproject.org), **CCProxy** (https://www.youngzsoft.net), and **Hotspot Shield** (https://www.hotspotshield.com) to browse the Internet anonymously.

Lab Analysis

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

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT 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

Draw Network Diagrams

A network diagram helps to analyze complete network topology.

ICON KEY

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

Lab Scenario

Until now, you have gathered information about the open ports, services running on the ports, OS details, security mechanisms details, etc. of the target network using various port and network scanning techniques and tools.

As a professional ethical hacker or a pen tester, the last step in the penetration process is to draw a network diagram that assists in identifying the topology or architecture of a target network. The network diagram also helps to trace the path to the target host in the network and enables you to understand the position of firewalls, IDSs, routers, and other access control devices.

As a professional ethical hacker or pen tester, you should be able to create a pictorial representation of network topology used in the target network. The network diagrams can be used to launch further attacks on the target network.

Lab Objectives

- Draw network diagrams using Network Topology Mapper

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2016 virtual machine
- Parrot Security virtual machine
- Ubuntu virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- Network Topology Mapper located at **E:\CEH-Tools\CEHv11 Module 03 Scanning Networks\Network Discovery Tools\Network Topology Mapper**
- You can also download the latest version of the above-mentioned tool from its official website. If you decide to download the latest version, the screenshots shown in the lab might differ.

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

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 03 Scanning Networks

Lab Duration

Time: 10 Minutes

Overview of Network Diagrams

Drawing a network diagram assists in the identification of the topology or architecture of a target network, and further assists you in finding the vulnerabilities or weak points of security mechanisms. These vulnerabilities can then be exploited to bypass the target's network. The network diagram also helps the network administrators to manage their networks.

Lab Tasks

TASK 1

Draw Network Diagrams using Network Topology Mapper

Here, we will use Network Topology Mapper to draw network diagrams of the target network.

TASK 1.1

Install Network Topology Mapper

1. Turn on the **Windows 10**, **Windows Server 2016**, **Parrot Security**, and **Ubuntu** virtual machines
2. In the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 03 Scanning Networks\Network Discovery Tools\Network Topology Mapper**, and then double-click **SolarWinds Network Topology Mapper.exe**.
3. The **SolarWinds Registration** dialog-box opens. Enter a working email address, and then click **Continue**.

Network Topology Mapper discovers a network and produces a comprehensive network diagram that integrates OSI Layer 2 and Layer 3 topology data. It automatically detects new devices and changes to network topology, simplifies inventory management for hardware and software assets, and addresses reporting needs for PCI compliance and other regulatory requirements.

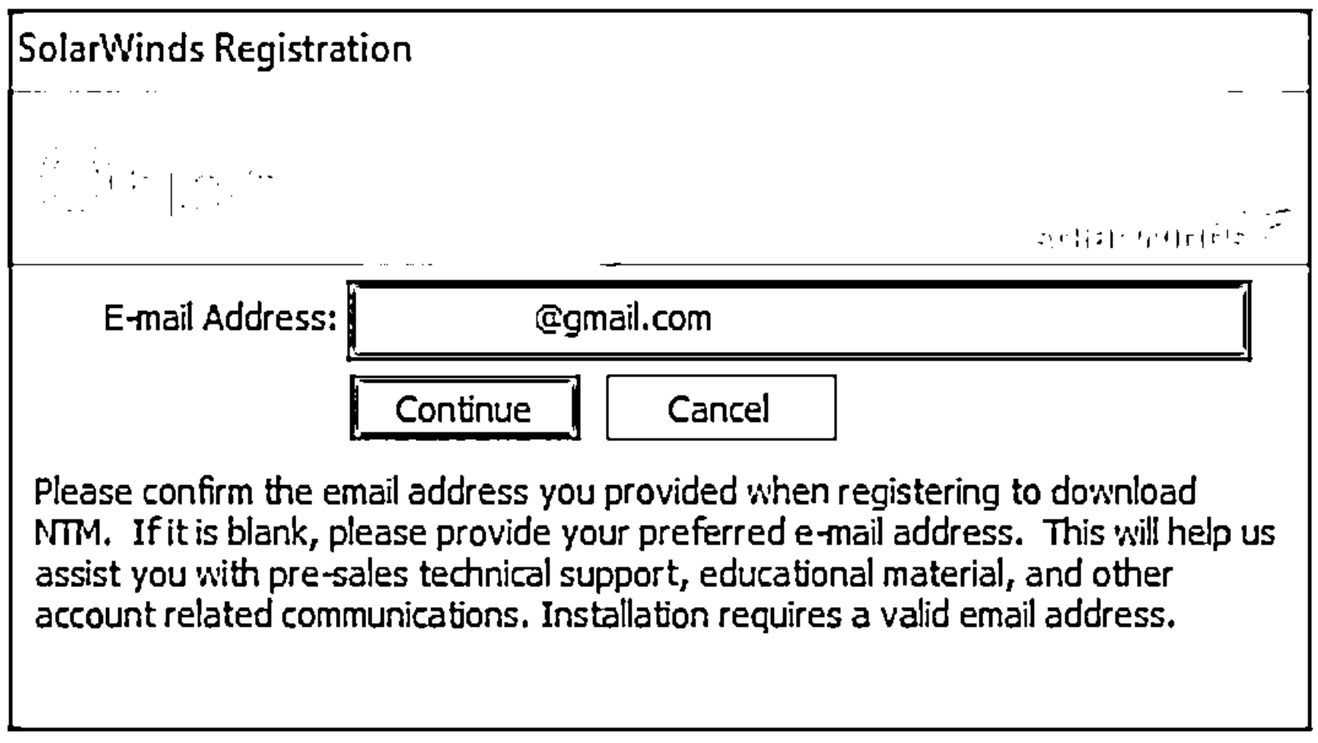


Figure 5.1.1: SolarWinds Registration dialog-box

4. In the next window, accept the license agreement and click **Install**.

Note: If a **User Account Control** window appears, click **Yes**.

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

5. The SolarWinds license pop-up appears; click **Continue Evaluation**.

Figure 5.1.2: Solarwinds license pop-up

6. The **Help SolarWinds Improve** window appears. Click the **No, I would not like to participate** radio button, and then click **OK**.

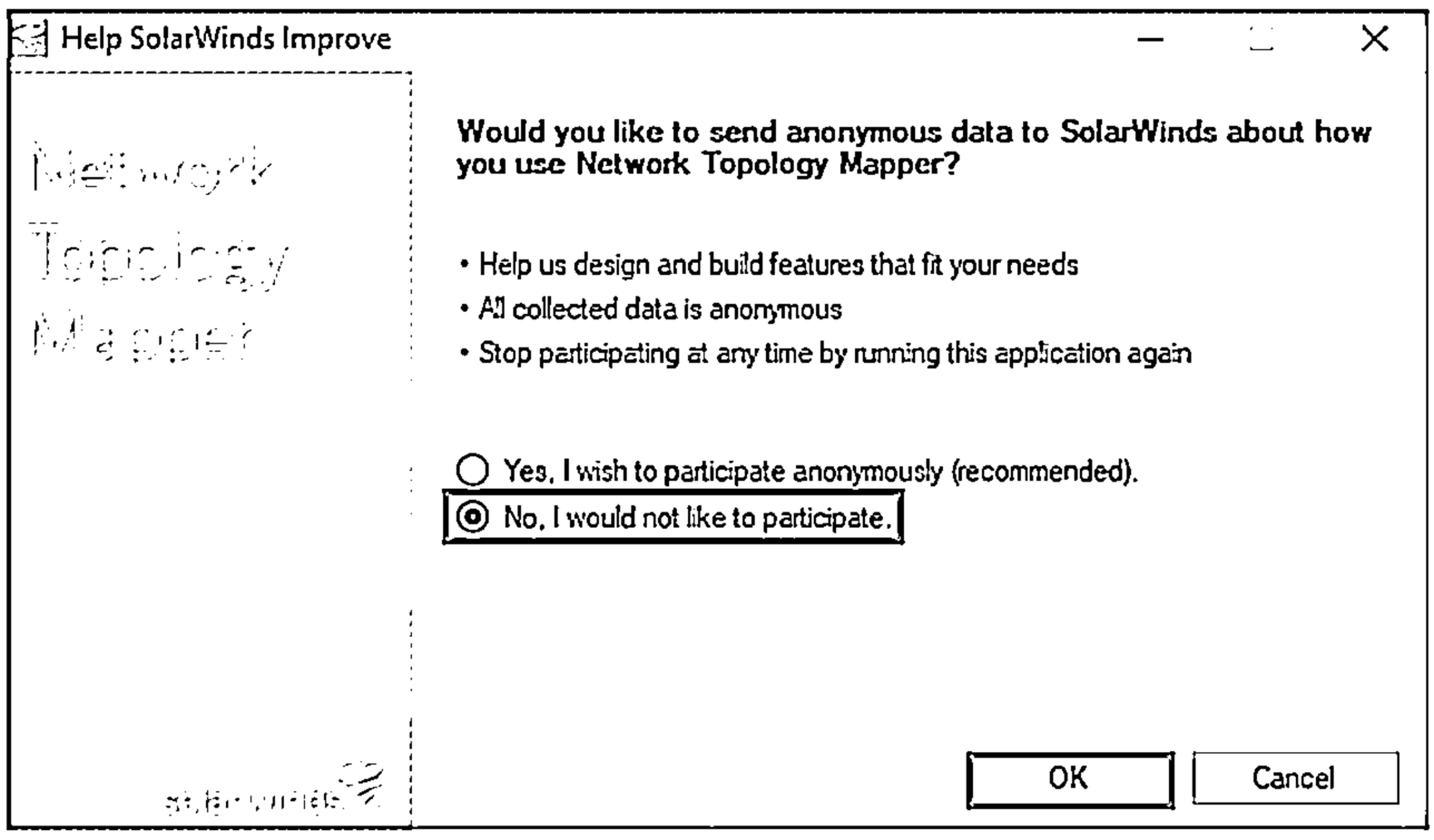


Figure 5.1.3: Help SolarWinds Improve window

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

7. Once the installation is complete, and the **SolarWinds Network Topology Mapper** window opens, click **Close**.

Note: Ensure that the **Run SolarWinds Network Topology Mapper now** option is selected.

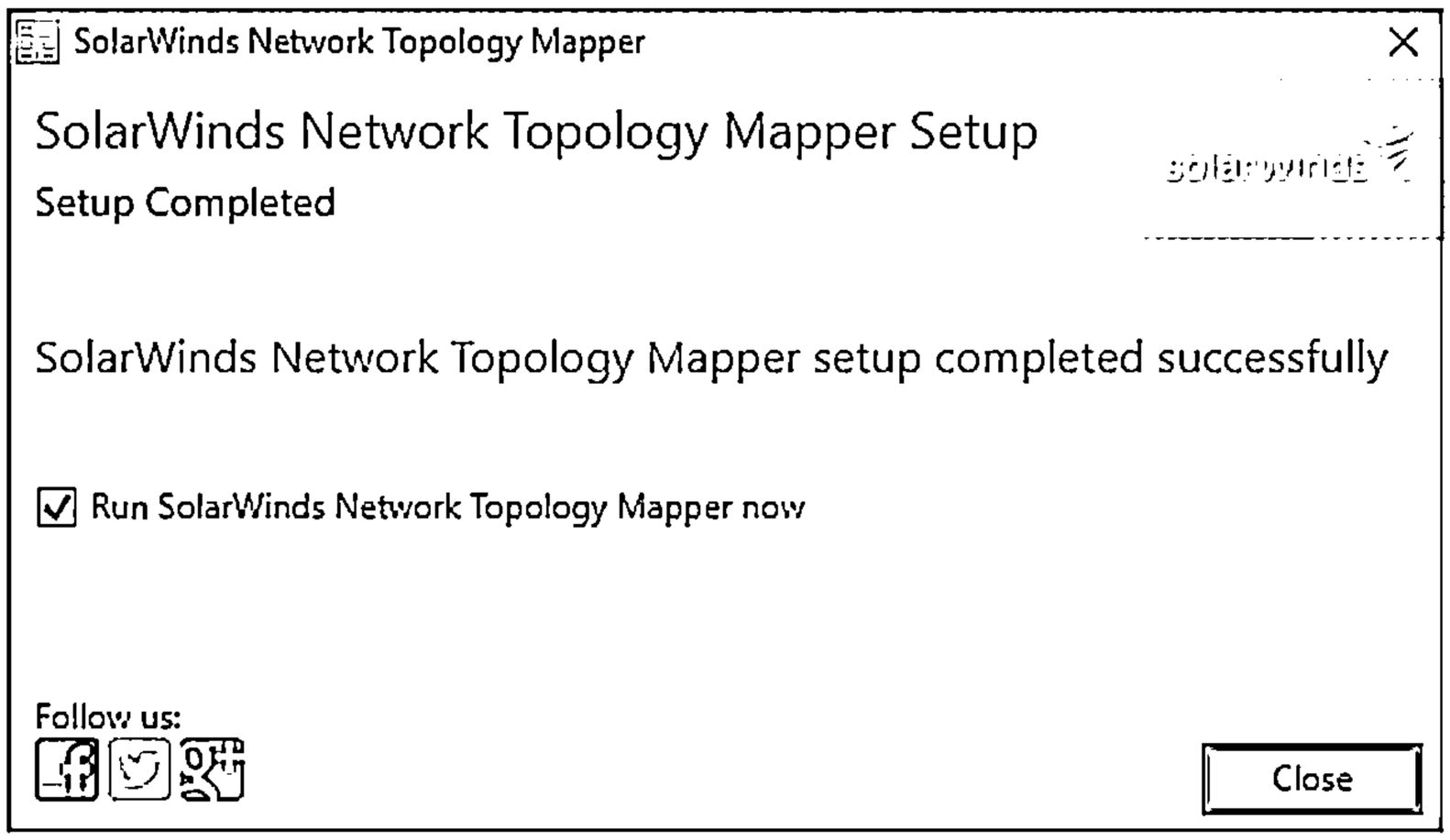


Figure 5.1.4: SolarWinds setup completed window

8. The **Solarwinds** pop-up opens; click **Continue Evaluation**.
9. The **SolarWinds Network Topology Mapper** main window appears, along with the **Welcome Screen...**. Click **New Scan** in the left-hand pane of the **Welcome Screen**.

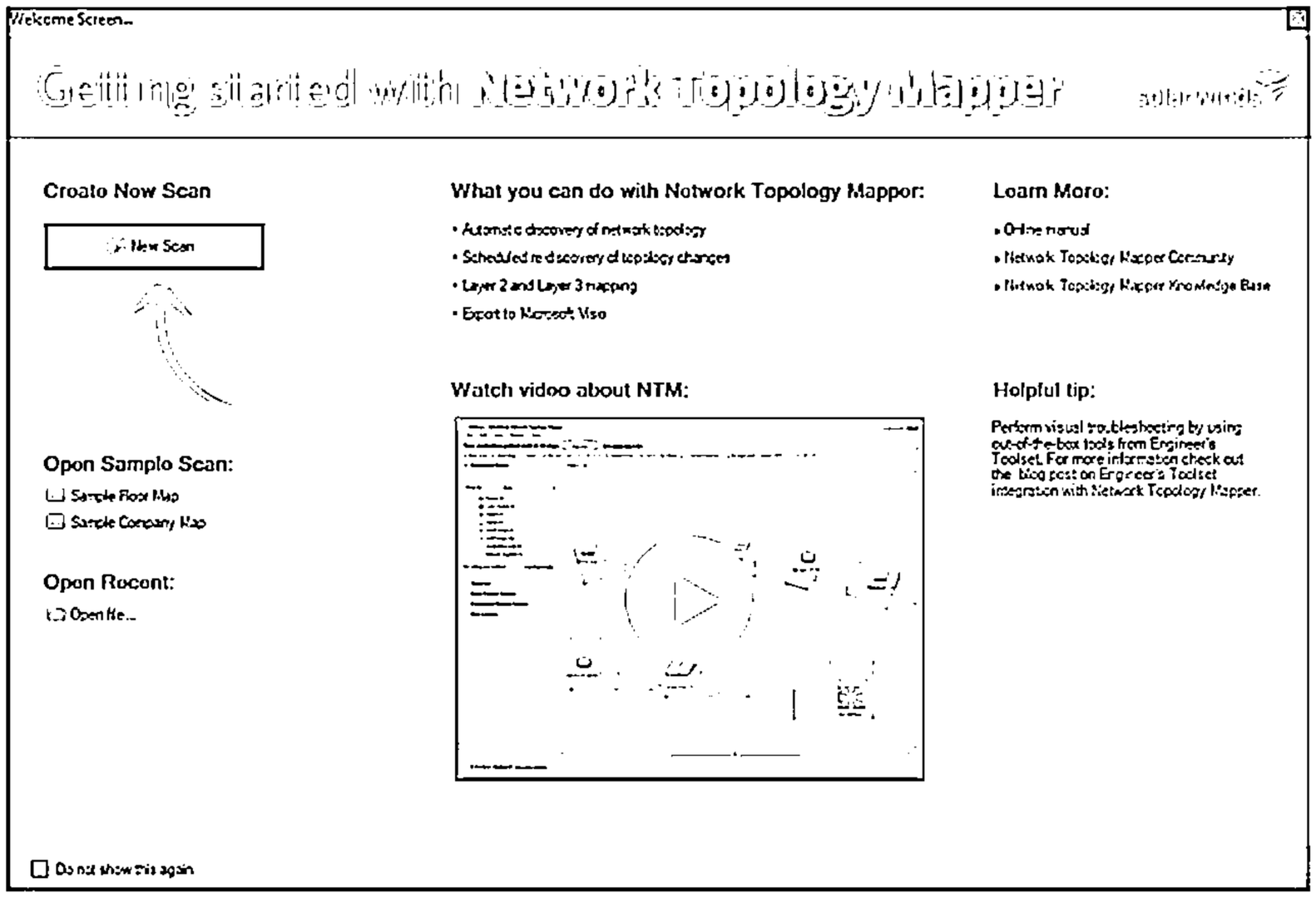


Figure 5.1.5: SolarWinds Network Topology Mapper main window

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

10. The **Set a Maps Password** pop-up appears. Enter a password (here **qwerty@123**) of your choice in the **New Password** field, re-enter the same password in the **Confirm Password** field, and click **Save**.

Figure 5.1.6: Set a Maps Password window

TASK 1.2

Configure Network Topology Mapper

11. The **Network Topology Scan** window appears. In the **SNMP Credentials** section, select the **private** credential under the **Stored Credentials** section and **public** credential under the **Discovery Credentials** section, and then click **Next**.

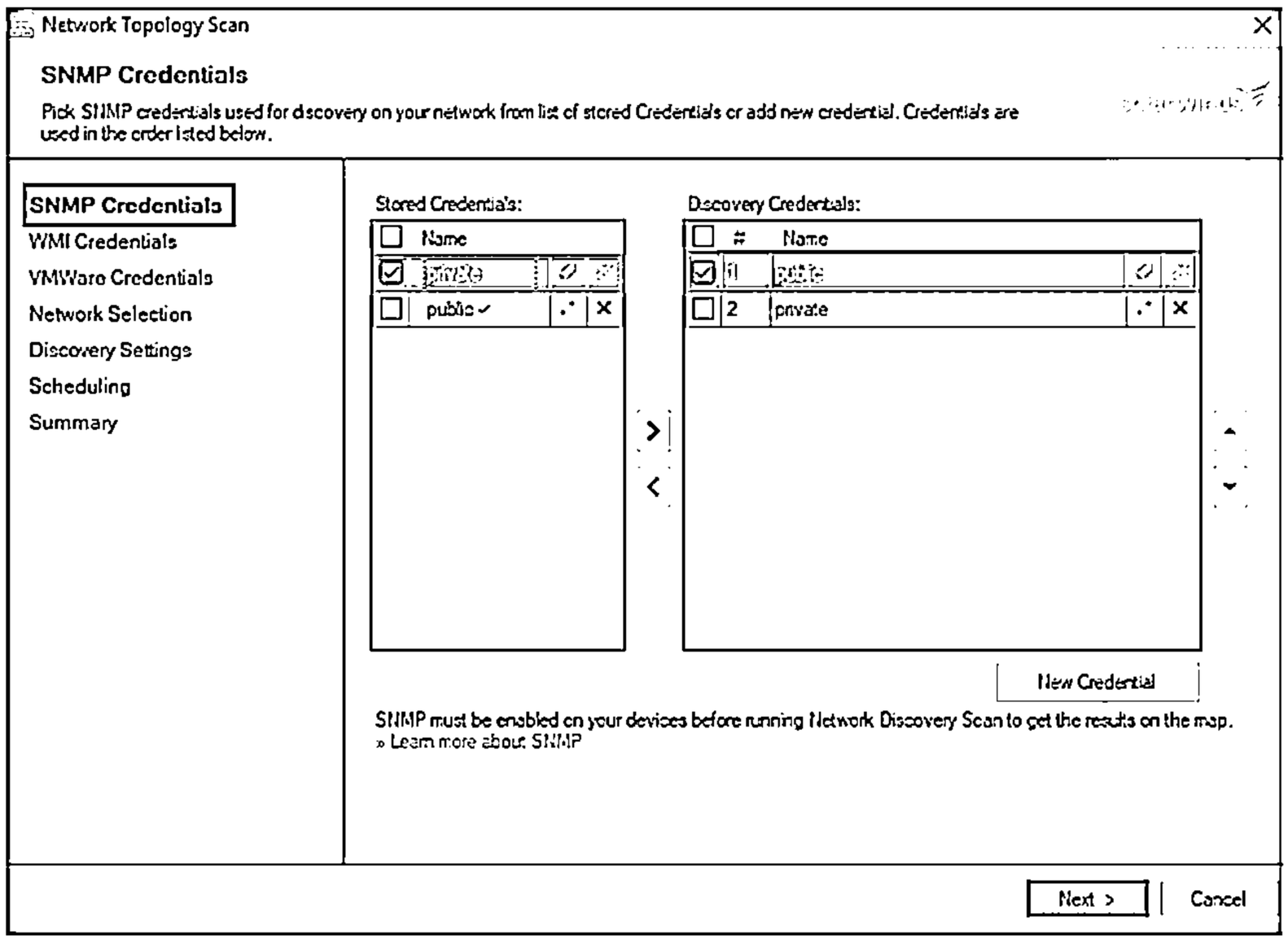


Figure 5.1.7: SNMP Credentials section

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

12. Leave the **WMI Credentials** and **VMWare Credentials** section to default and click **Next**.
13. The **Network Selection** section appears. Click the **IP Ranges** tab in the right-pane, enter the IP address range (**10.10.10.3 - 10.10.10.254**) in the **Start Address** and **End Address** fields, and click **Next**.

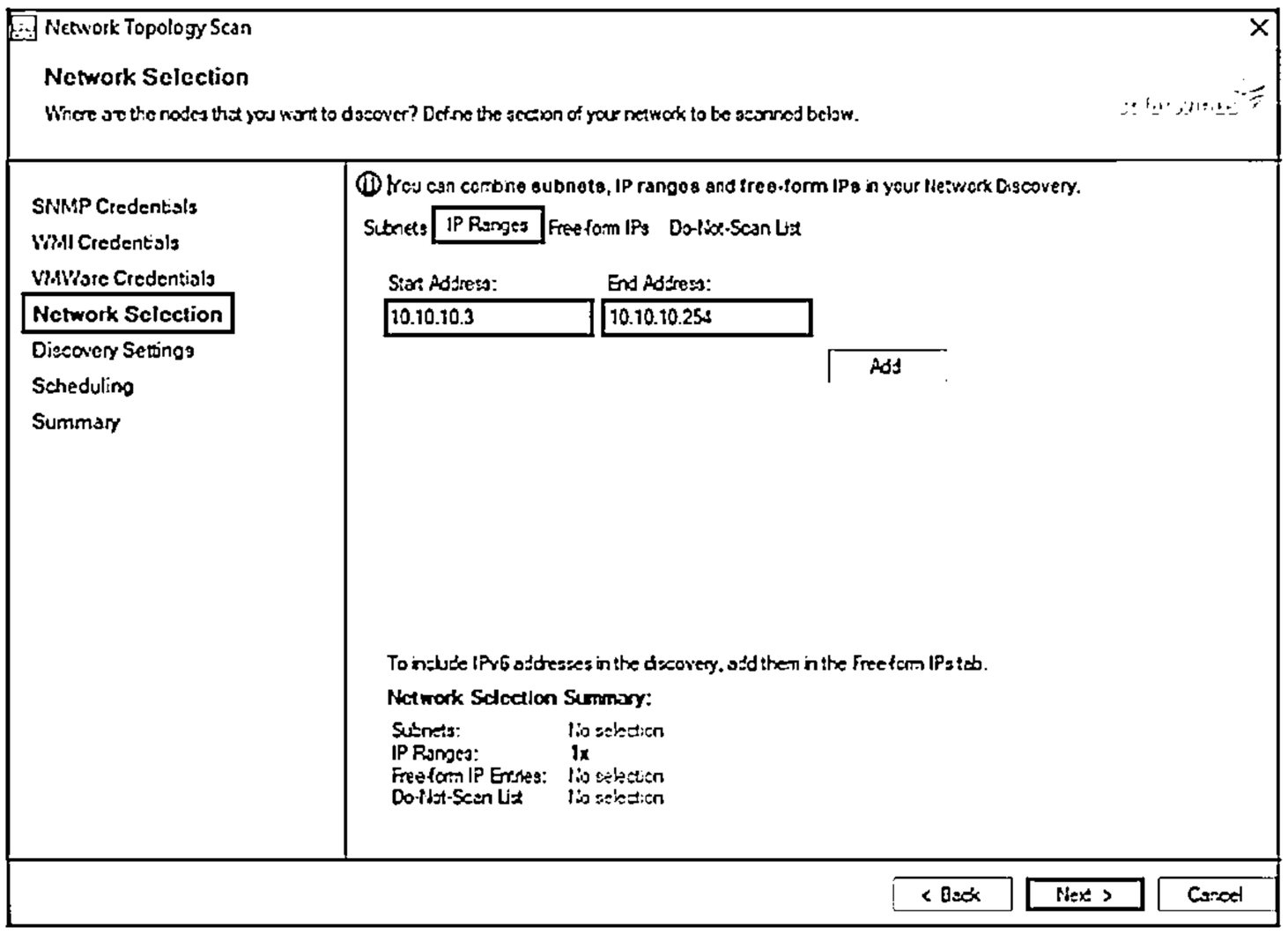


Figure 5.1.8: Network Selection section

14. The **Discovery Settings** section appears. Enter a name under the **Scan name** field (here, "**Network Topology**") and click **Next**.

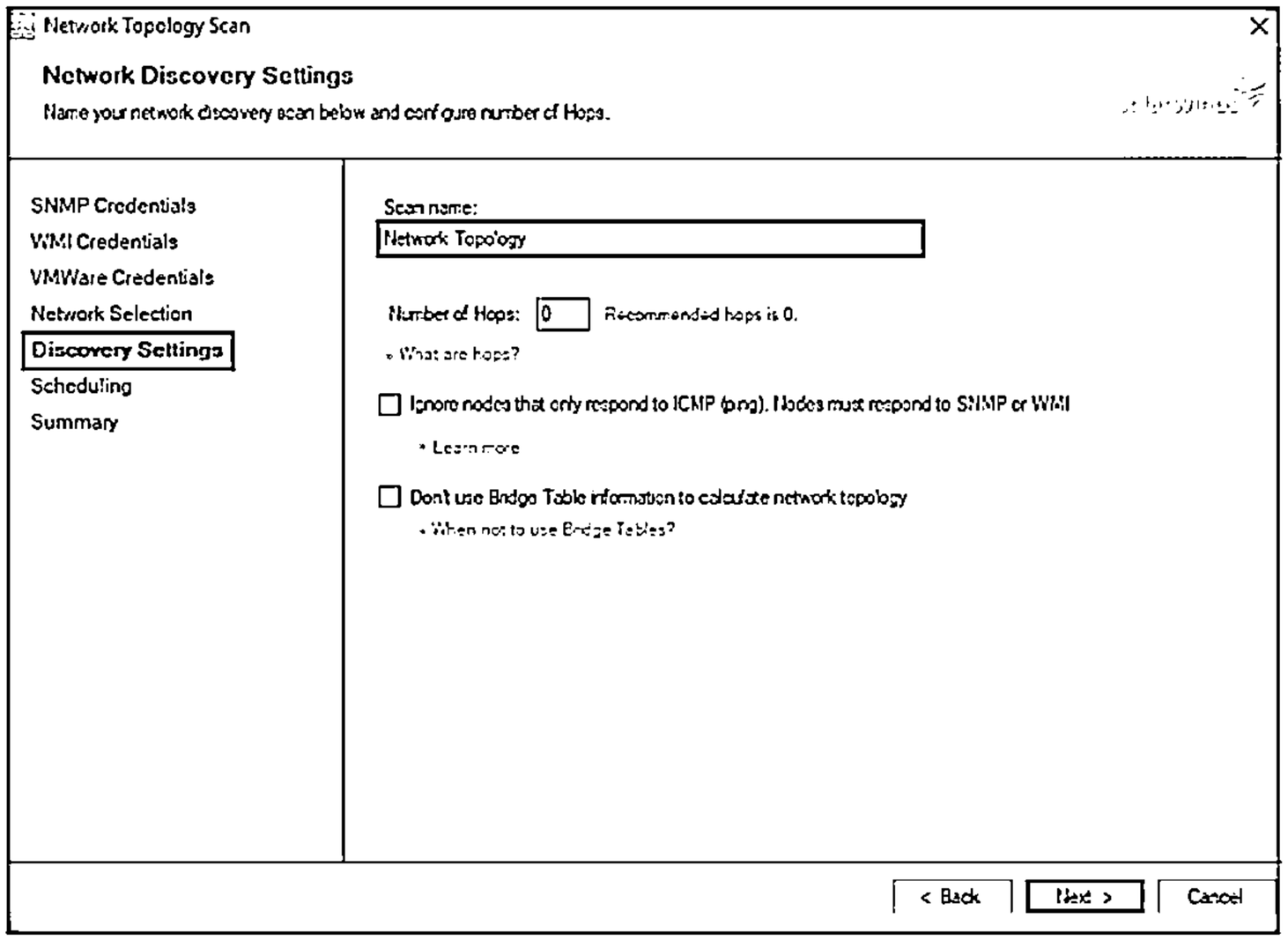


Figure 5.1.9: Discovery Settings section

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

15. The **Scheduling** section appears. Ensure that **Once** is selected in the **Frequency** drop-down menu; under the **Execute immediately** radio button **Yes, run this discovery now** is selected; then, click **Next**.

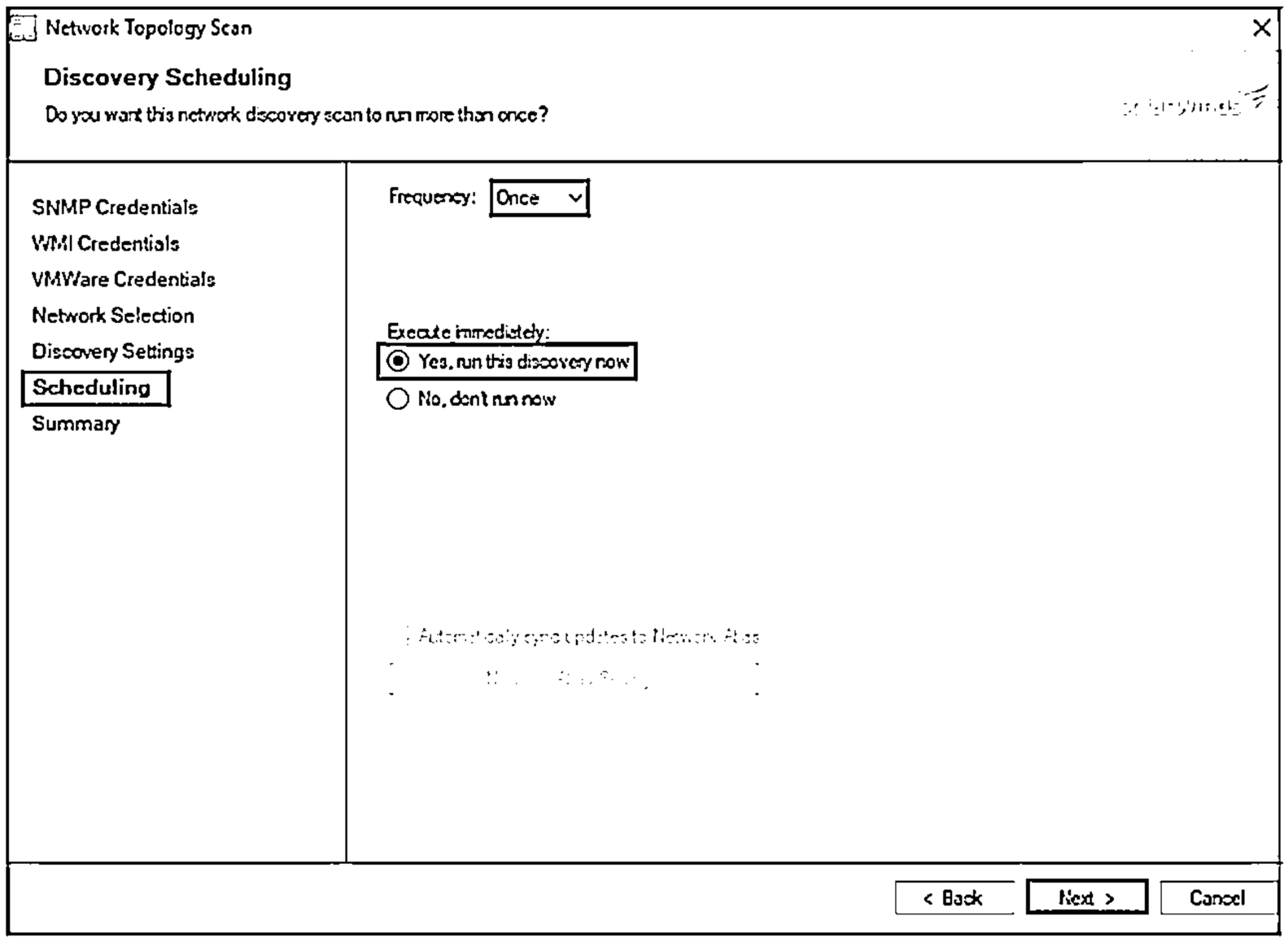


Figure 5.1.10: Scheduling section

16. The **Summary** section appears; click **Discover**.

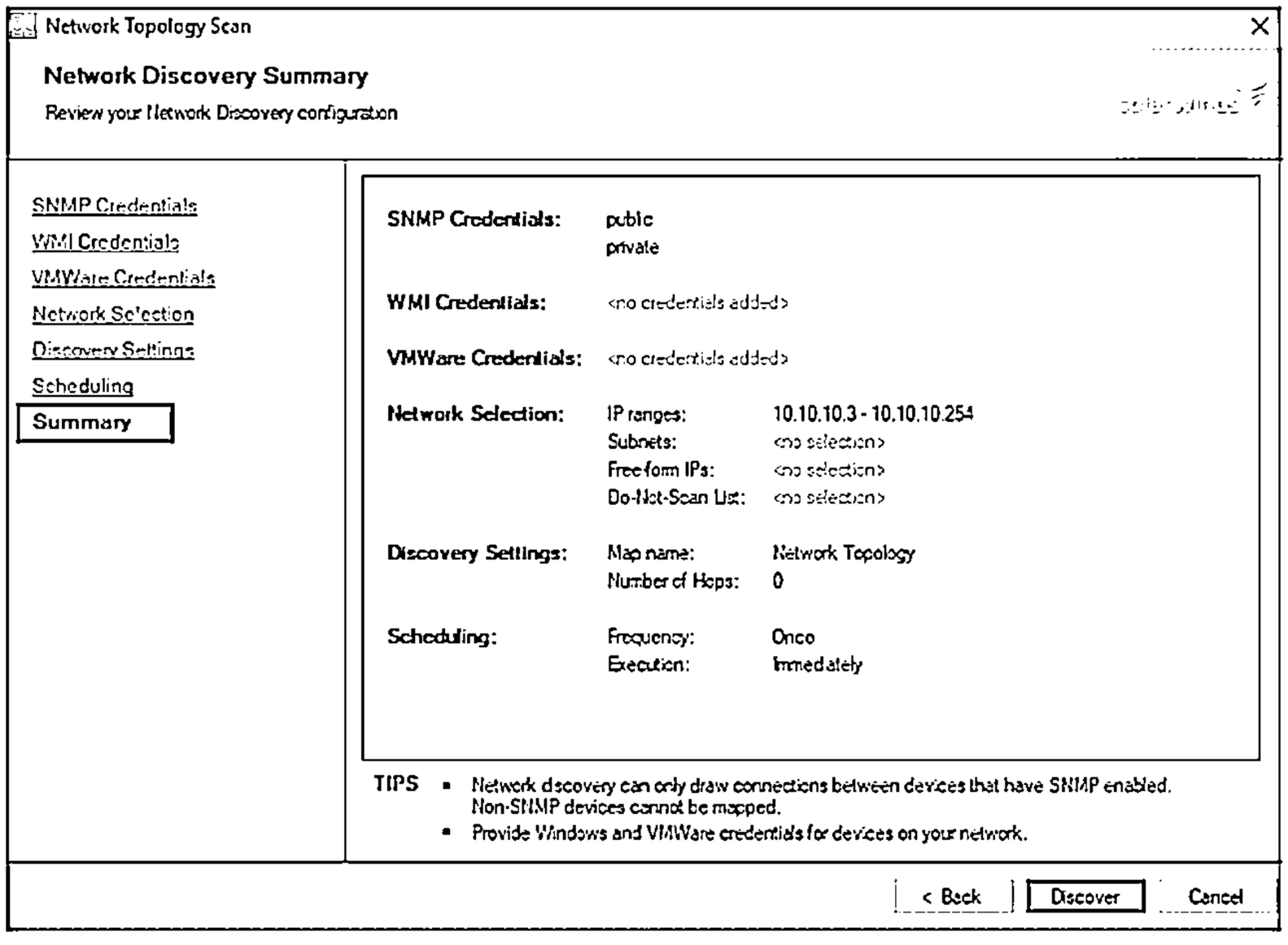


Figure 5.1.11: Summary section

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

17. The **New Network Scan** window appears; the Network Topology Mapper starts scanning the network for live hosts.

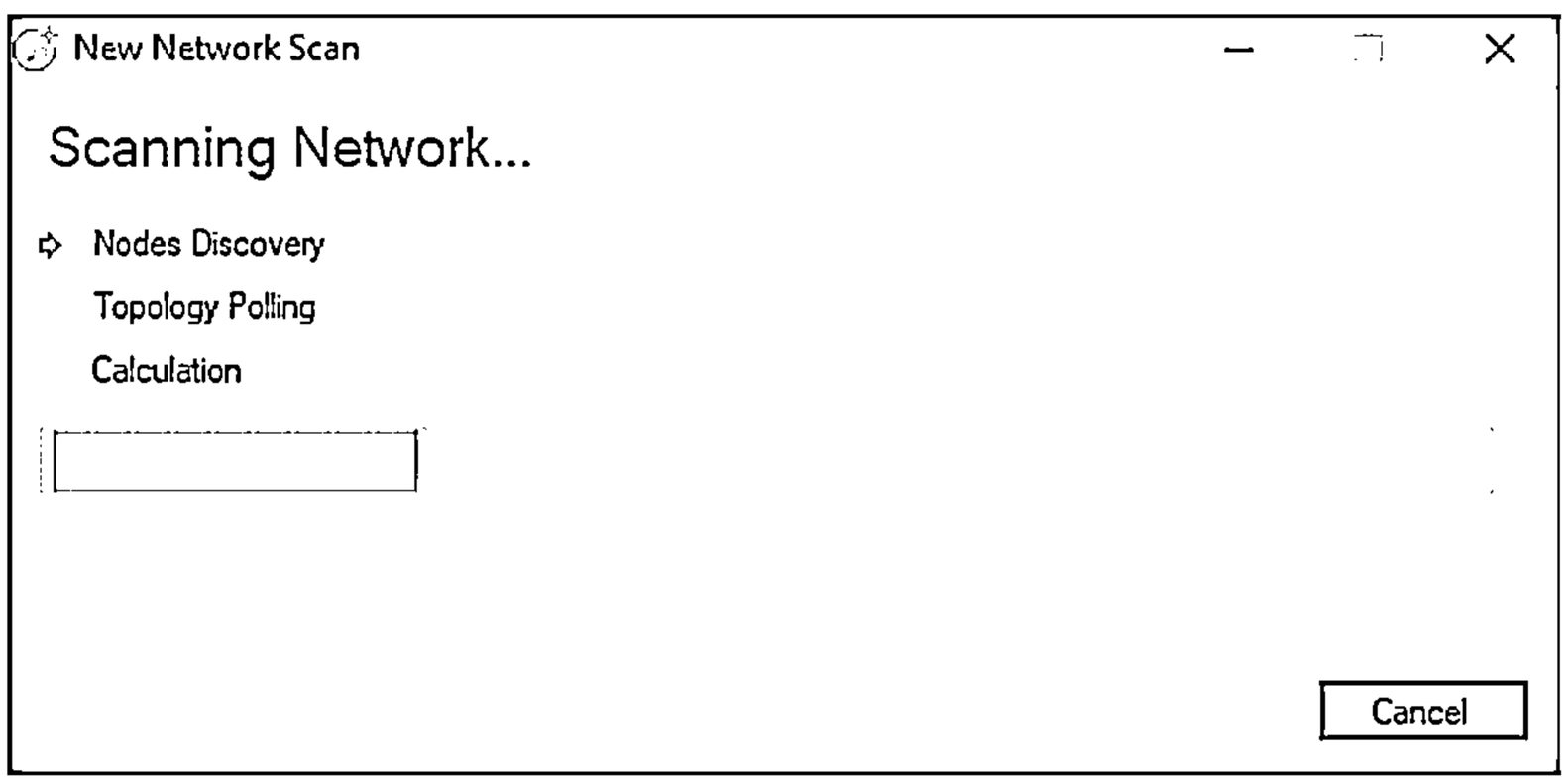


Figure 5.1.12: Network Topology Mapper scanning the network

TASK 1.3

Draw Network Diagram

18. The **Network Topology - SolarWinds Network Topology Mapper** window appears. Close the **Map Navigator** window.

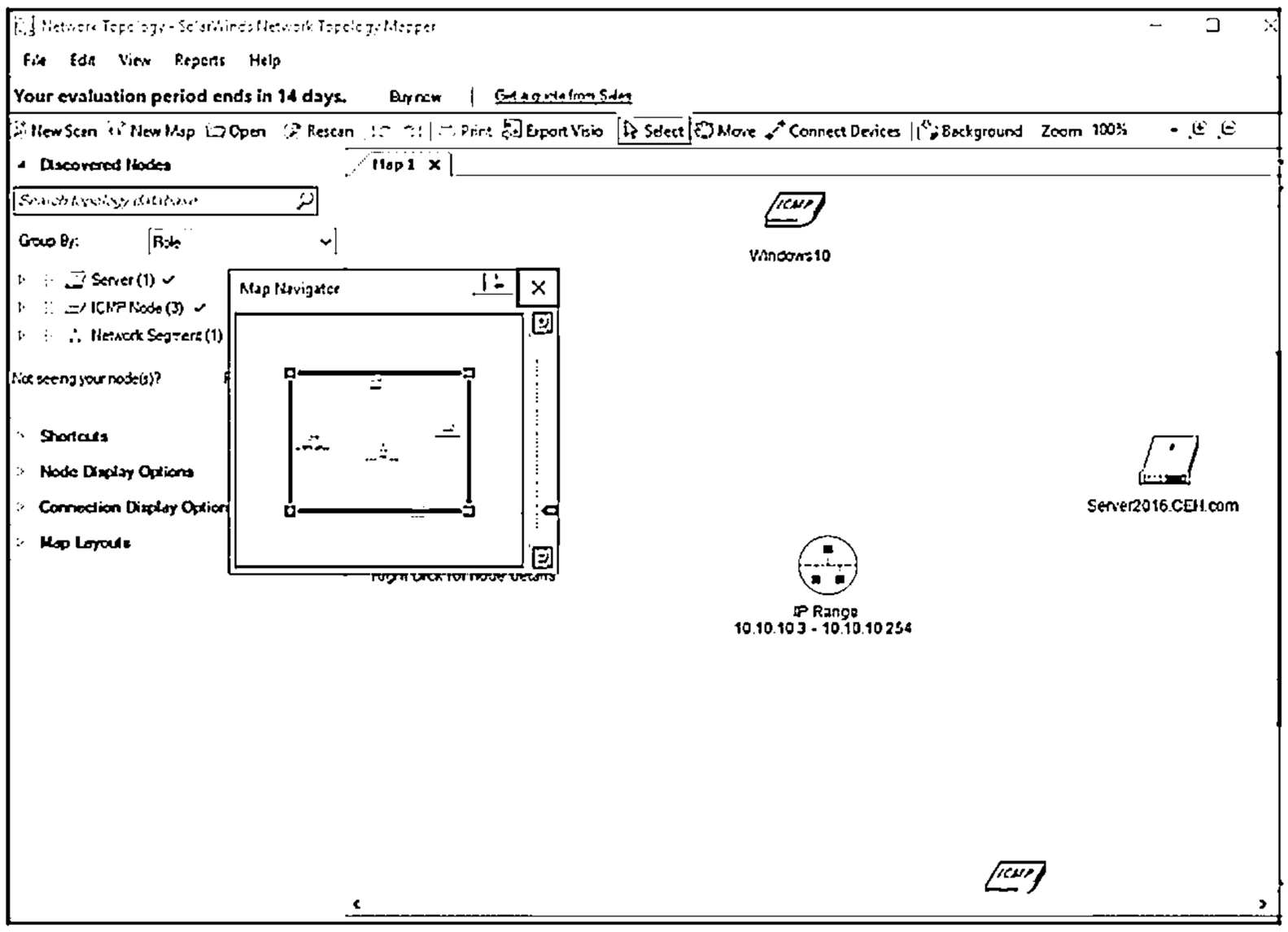


Figure 5.1.13: Network Scan results window

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

19. The **Network Topology Mapper** displays a network topology diagram for the provided IP address range, as shown in the following screenshot.

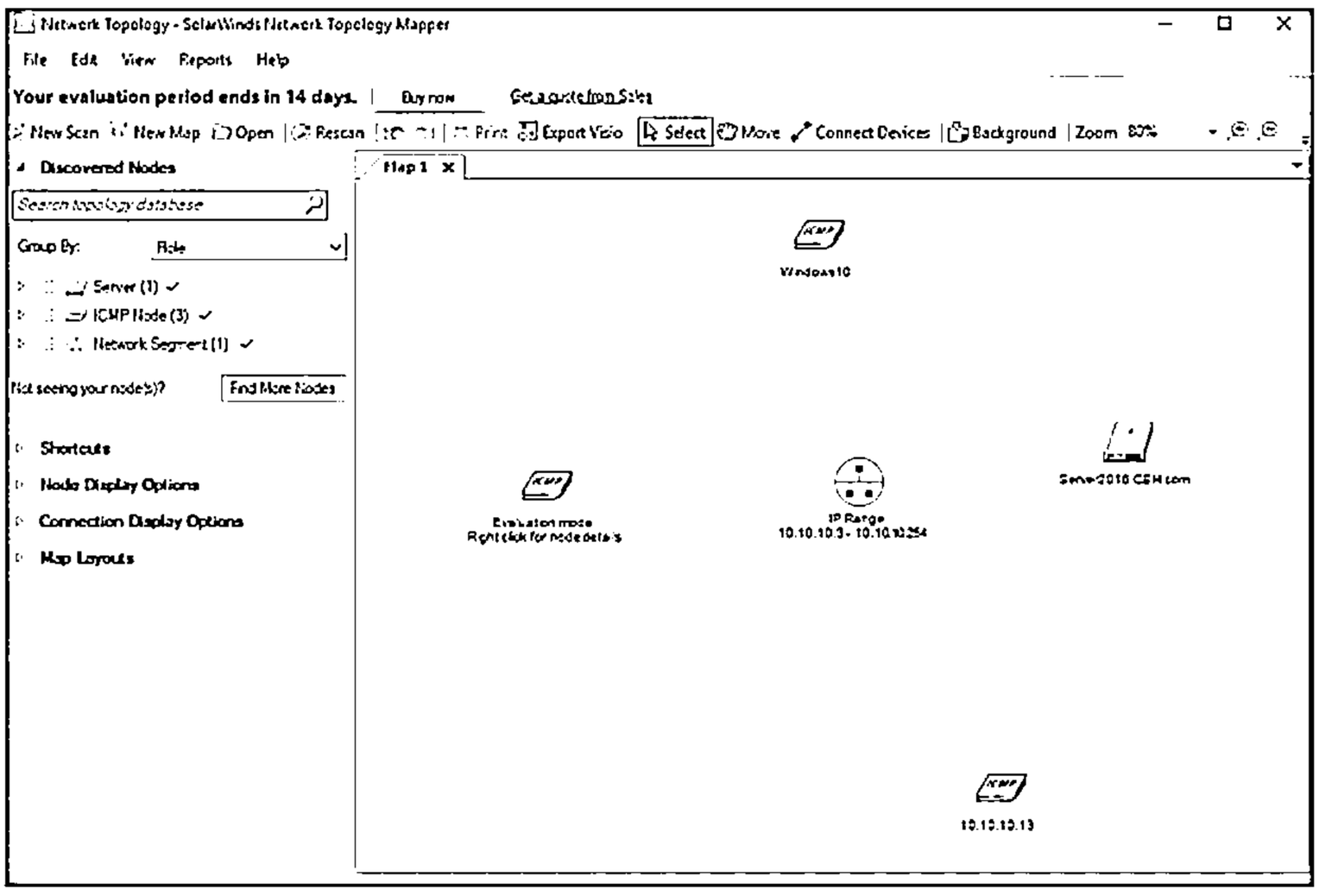


Figure 5.1.14: Network topology diagram

20. Expand **Node Display Options** in the right-hand pane and select the **IP address** checkbox. This displays IP addresses for all nodes in the layout.

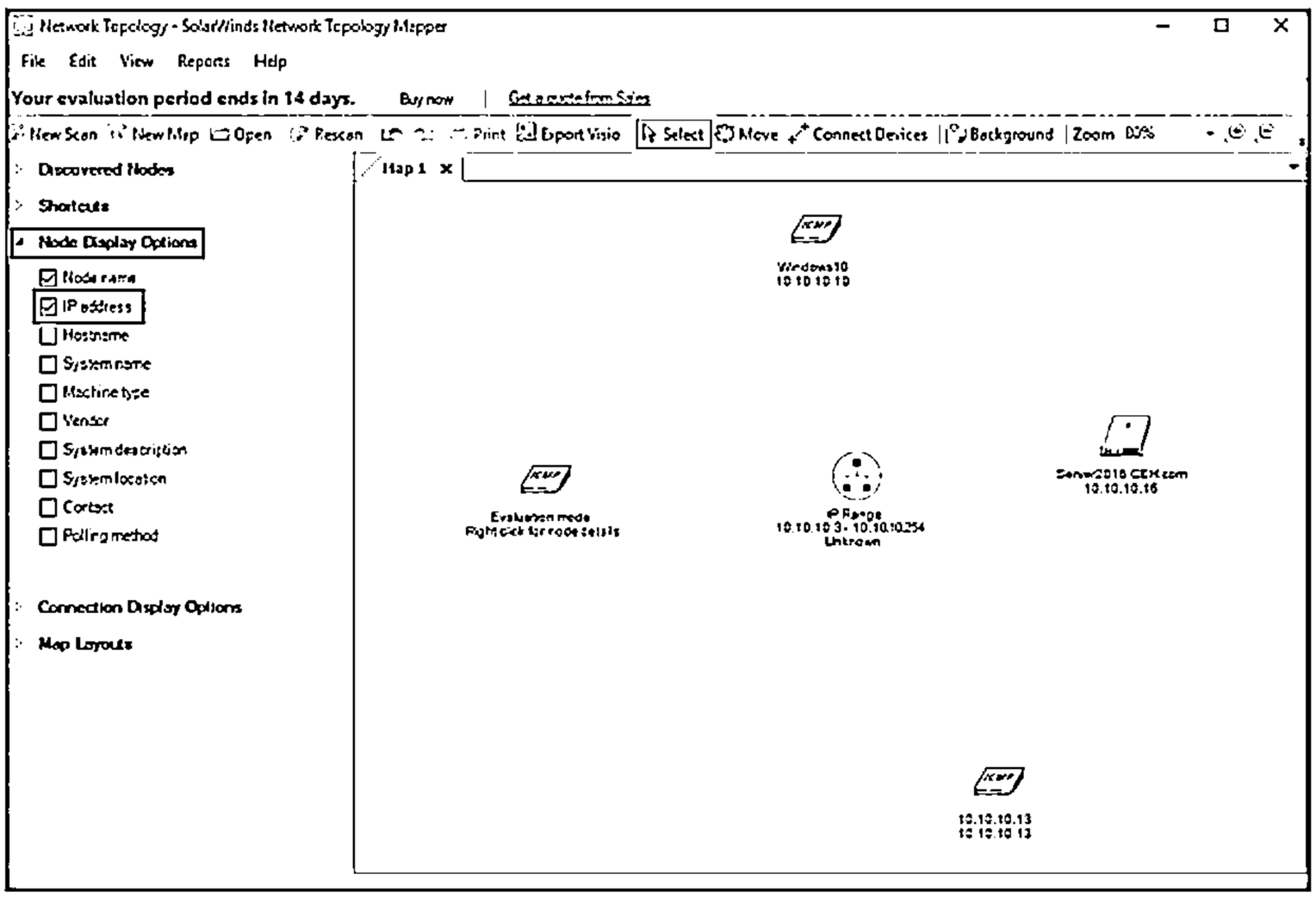


Figure 5.1.15: Node Display Options: selecting the IP address

21. Now, expand the **Map Layouts** node, and select **Symmetrical** under the **Auto Arrange** section to change the topology layout of the mapped network. Each time you click **Symmetrical**, all nodes are rearranged randomly.

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

Note: You may select the node display options of your choice: whichever options you choose, they are added to the topology map. These topology maps are saved automatically to **C:\ProgramData\Solarwinds\Network Topology Mapper\UserMaps.**

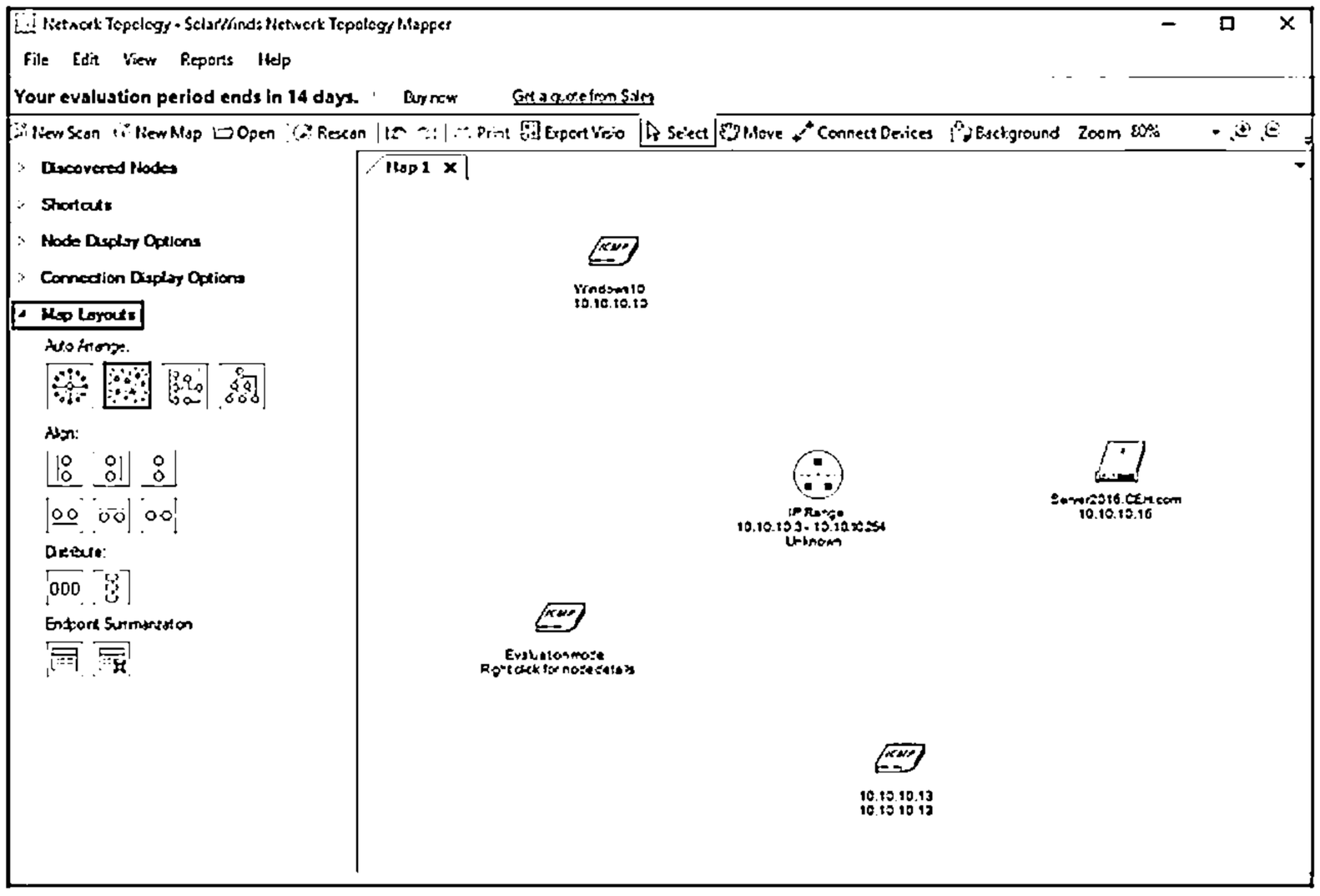


Figure 5.1.16: Map Layouts Options: selecting Symmetrical

22. Right-click on a node (here **Server2016** with IP address **10.10.10.16**) and select **Node Properties** to view information about the selected node.

Note: The network diagram and the IP addresses might differ in your lab environment

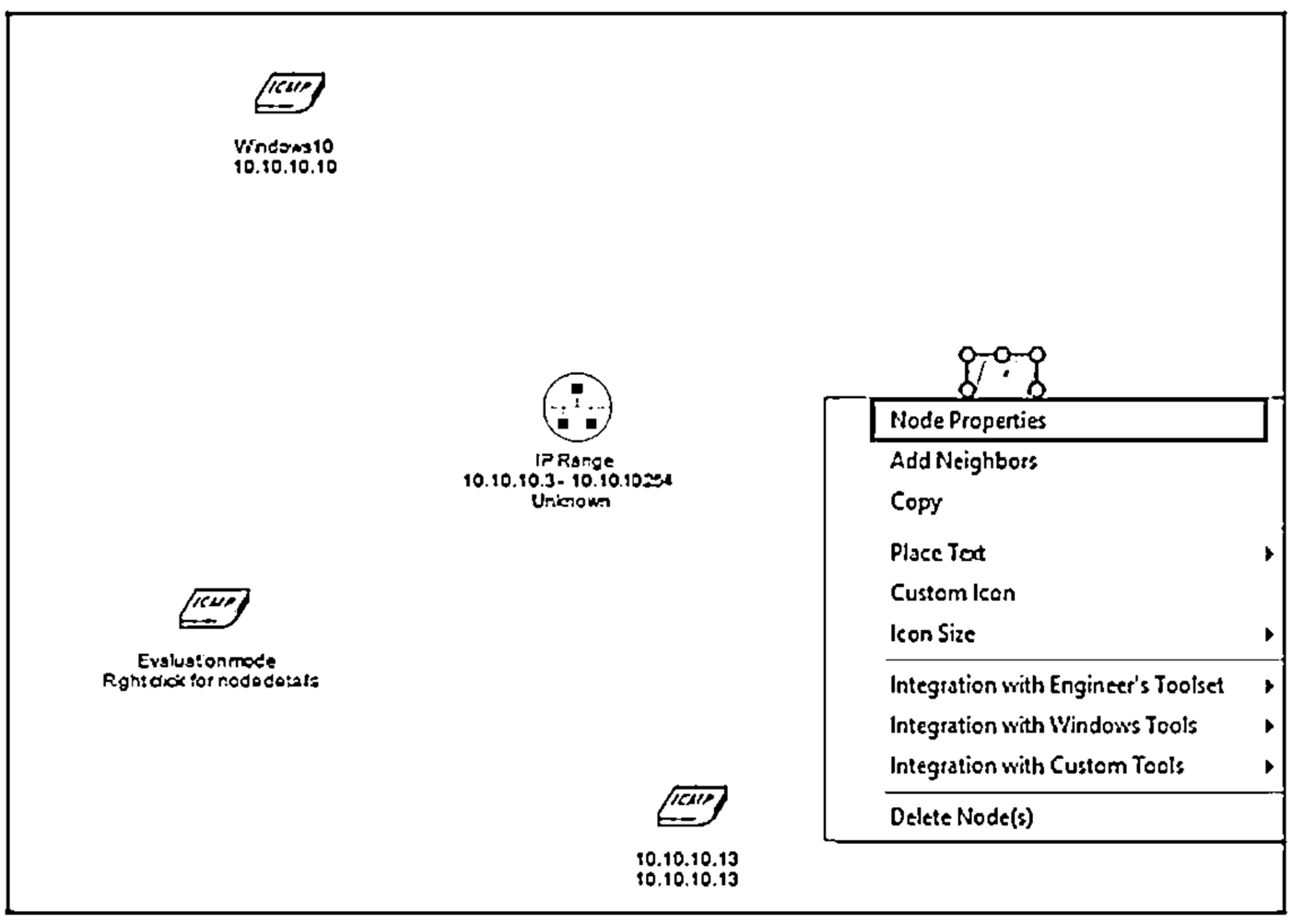


Figure 5.1.17: Viewing the details of a selected target machine

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

23. The **Node Details** window appears, displaying information about the selected node. Click **Close** to close the window.

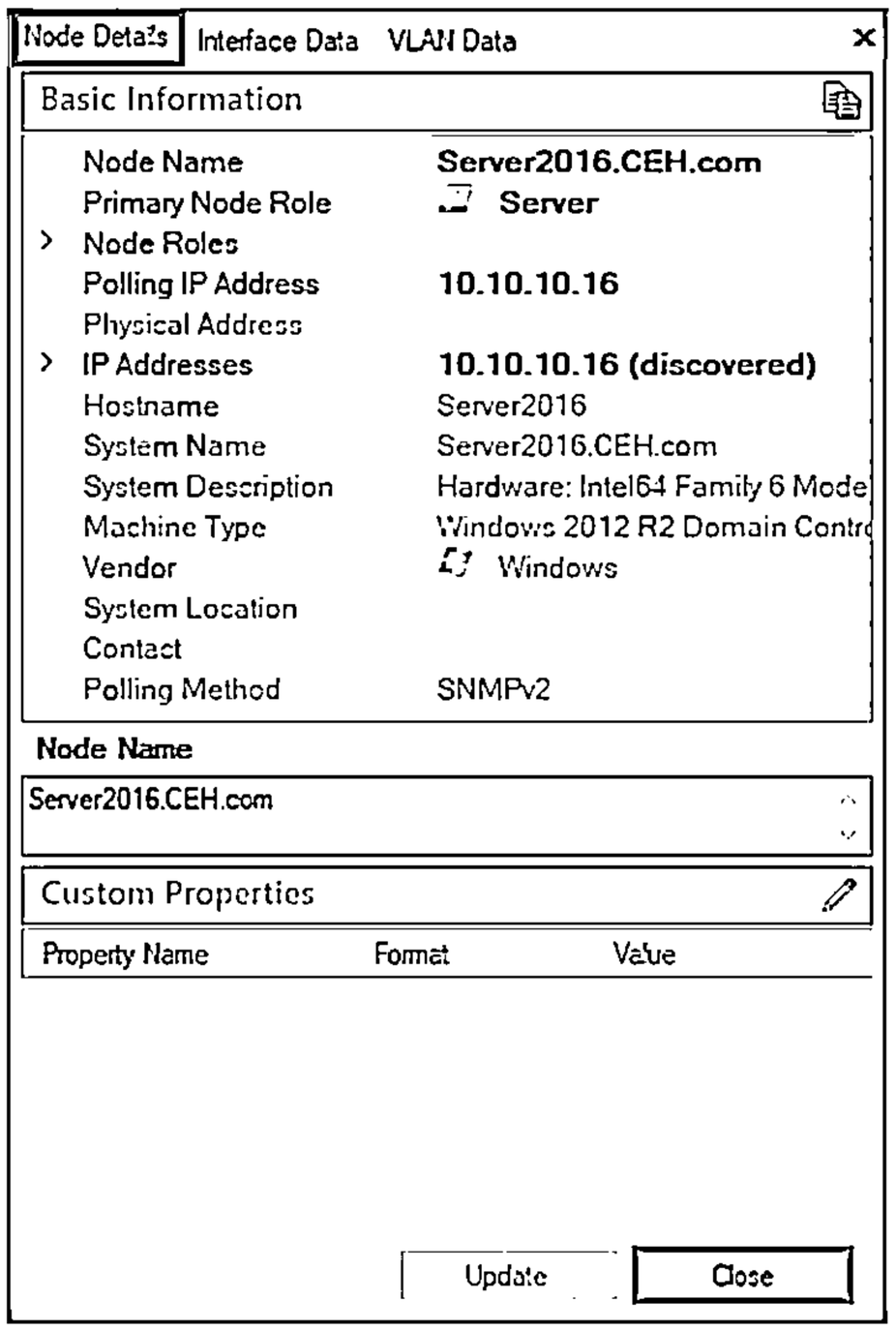


Figure 5.1.18: Details window

TASK 1.4

Additional Features in Network Topology Mapper

24. Right-click on a node (**Server2016** with IP address **10.10.10.16**) and select **Integration with Windows Tools** and click **Remote Desktop**.

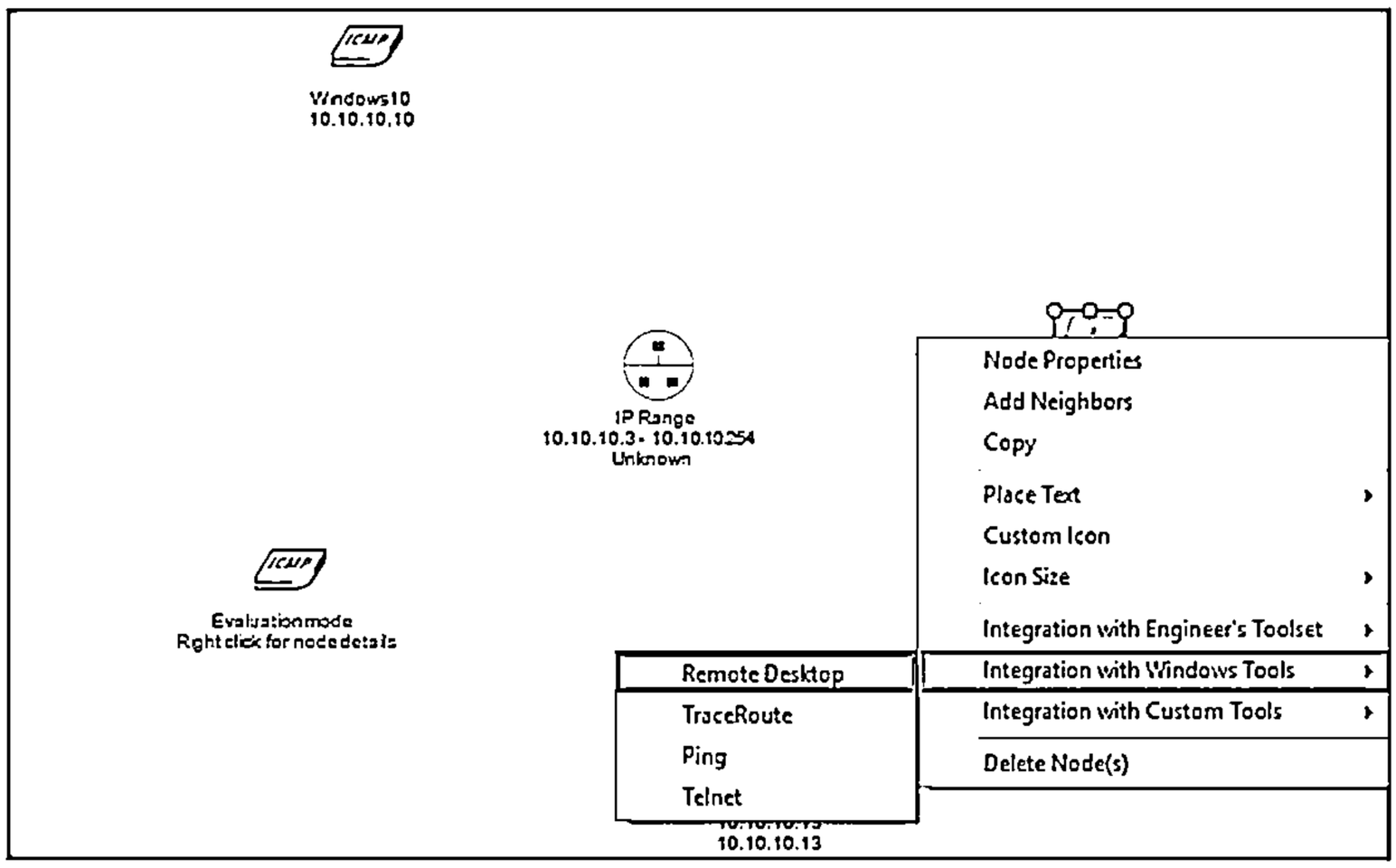


Figure 5.1.19: Establishing a Remote Desktop Connection with the target machine

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

25. The **Windows Security** dialog box appears. Enter **Username** as **Administrator** and **Password** as **Pa$$w0rd** for **Windows Server 2016**, and click **OK**.

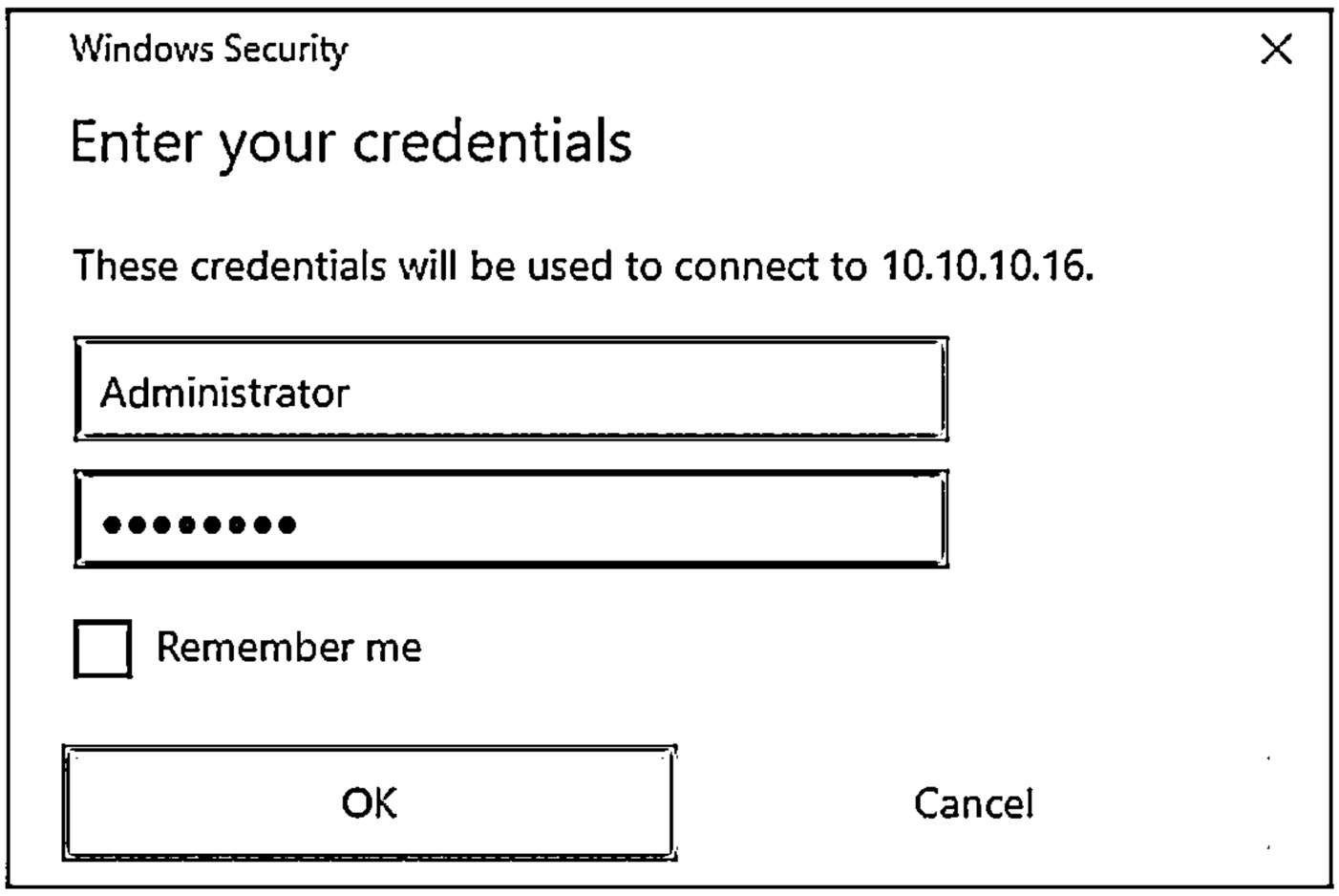


Figure 5.1.20: Establishing a Remote Desktop Connection with the target machine

26. The **Remote Desktop Connection** pop-up appears; click **Yes**.

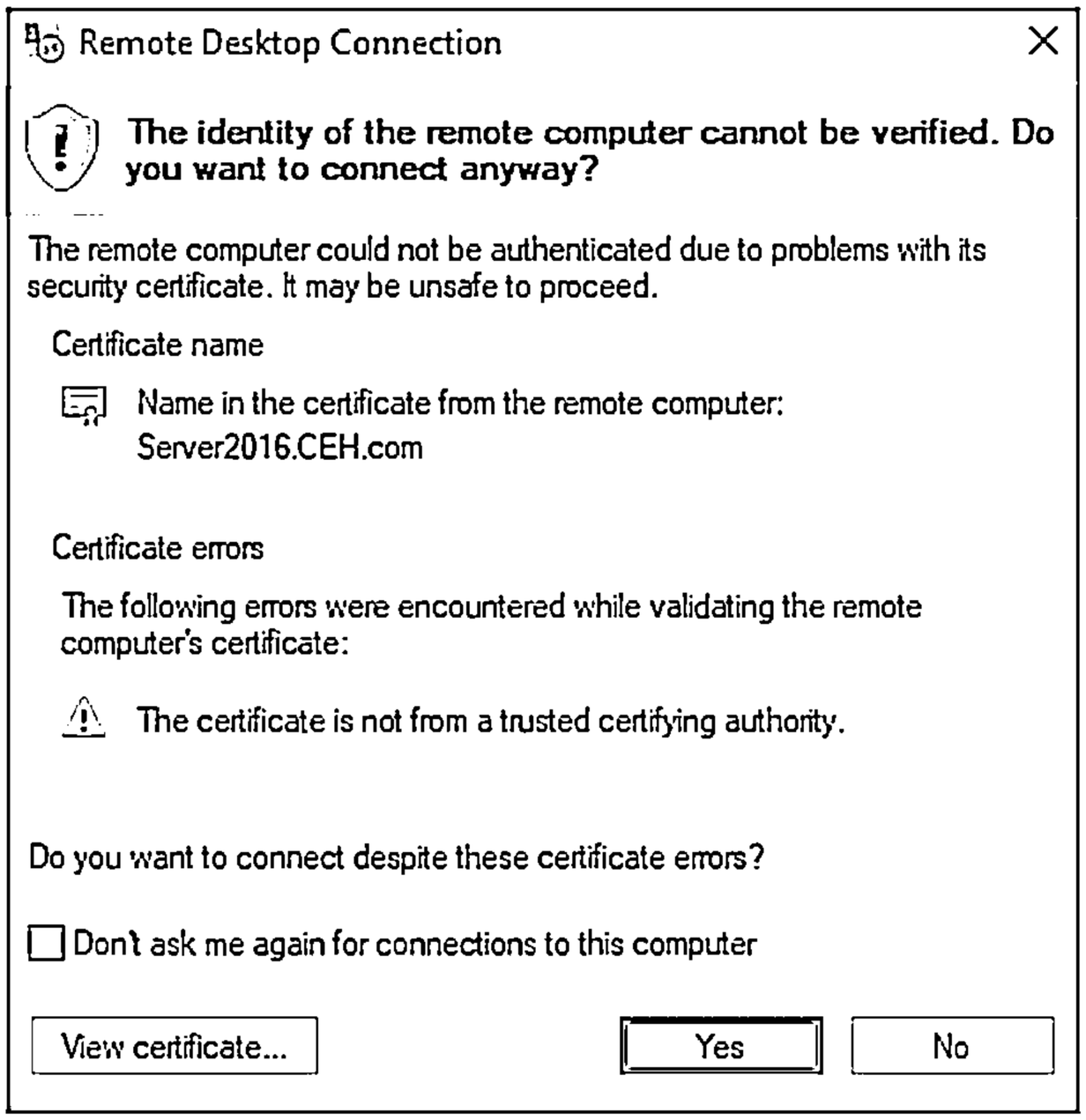


Figure 5.1.21: Establishing a remote desktop connection with the target machine

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

27. The **Remote Desktop Connection** is successfully set to the target virtual machine (here, **Windows Server 2016**), as shown in the following screenshot.

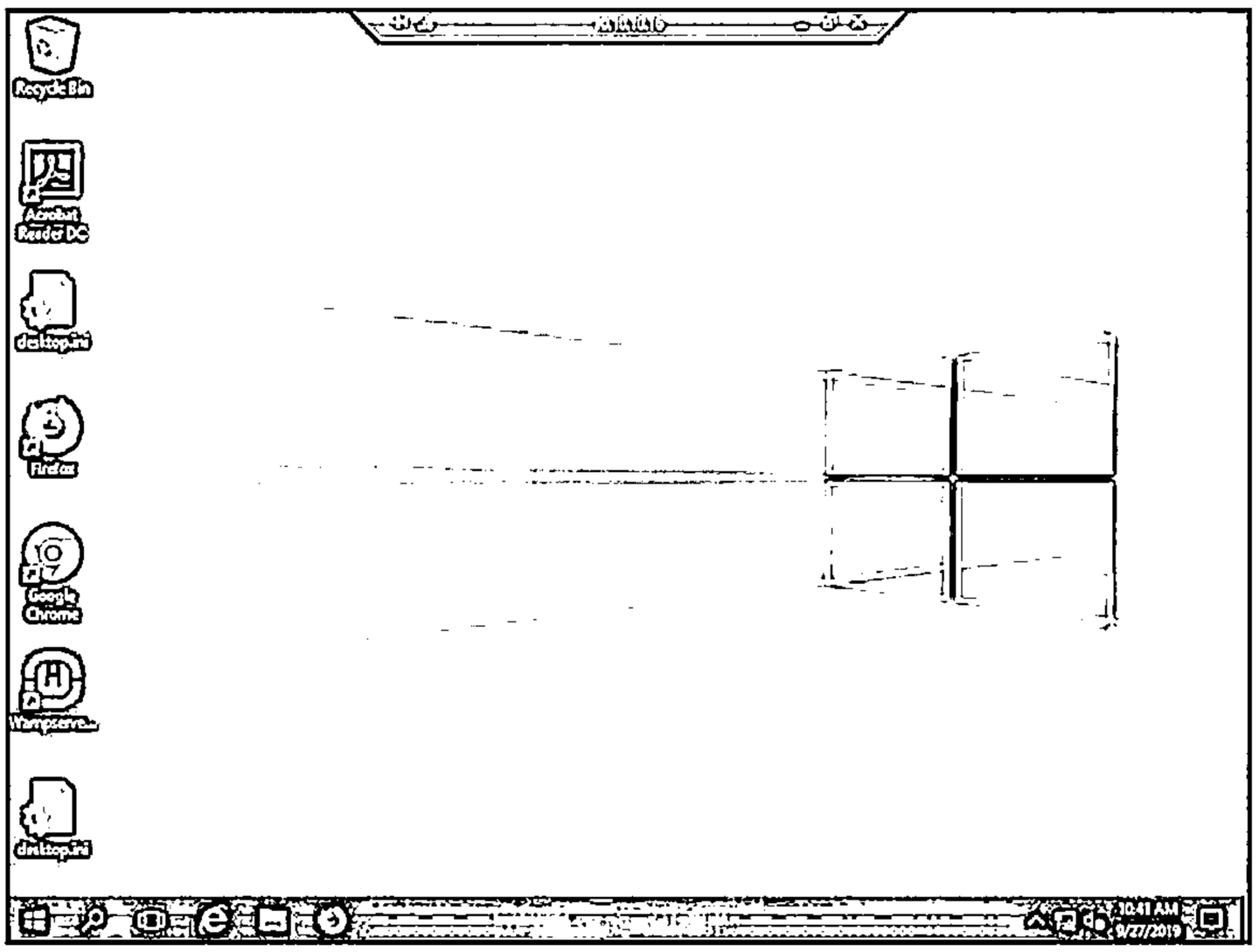


Figure 5.1.22: Remote Desktop Connection established with the target machine

28. You can use other options such as **Ping**, **Telnet**, and **Traceroute**. Similarly, an attacker can use this application to draw network diagrams, find the active hosts on the network, perform Ping, Telnet, etc.
29. This concludes the demonstration of drawing network diagram of the target network using Network Topology Mapper.
30. Close all open windows and document all the acquired information.
31. Turn off all the virtual machines.

You can also use other network discovery tools such as **OpManager** (https://www.manageengine.com), **The Dude** (https://mikrotik.com), **NetSurveyor** (http://nutsaboutnets.com), **NetBrain** (https://www.netbraintech.com), and **Spiceworks Network Mapping Tool** (https://www.spiceworks.com) to draw network diagram of the target network.

Lab Analysis

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

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT 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

Perform Network Scanning using Various Scanning Tools

Ethical hackers and pen testers are aided in network scanning with the help of various scanning tools, which make scanning a target network an easy task.

ICON KEY

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

Lab Scenario

The information obtained in the previous steps might be insufficient to reveal potential vulnerabilities in the target network: there may be more information available that could help in finding loopholes in the target network. As an ethical hacker and pen tester, you should look for as much information as possible about systems in the target network using various network scanning tools when needed. This lab will demonstrate other techniques/commands/methods that can assist you in extracting information about the systems in the target network using various scanning tools.

Lab Objectives

- Scan a target network using Metasploit

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 03 Scanning Networks

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2016 virtual machine
- Parrot Security virtual machine
- Ubuntu virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 20 Minutes

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

Overview of Network Scanning Tools

Scanning tools are used to scan and identify live hosts, open ports, running services on a target network, location-info, NetBIOS info, and information about all TCP/IP and UDP open ports. Information obtained from these tools will assist an ethical hacker in creating the profile of the target organization and to scan the network for open ports of the devices connected.

Lab Tasks

TASK 1 — Scan a Target Network using Metasploit

Here, we will use Metasploit to discover active hosts, open ports, services running, and OS details of systems present in the target network.

TASK 1.1

Link Metasploit Framework to Database

Metasploit Framework is a tool that provides information about security vulnerabilities in the target organization's system, and aids in penetration testing and IDS signature development. It facilitates the tasks of attackers, exploit writers, and payload writers. A major advantage of the framework is the modular approach, that is, allowing the combination of any exploit with any payload.

1. Before starting this task, turn on the **Windows 10**, **Windows Server 2016**, **Parrot Security**, and **Ubuntu** virtual machine.
2. Switch to the **Parrot Security** virtual machine.
3. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

4. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
5. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
6. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

   Note: The password that you type will not be visible.
7. Now, type **cd** and press **Enter** to jump to the root directory.

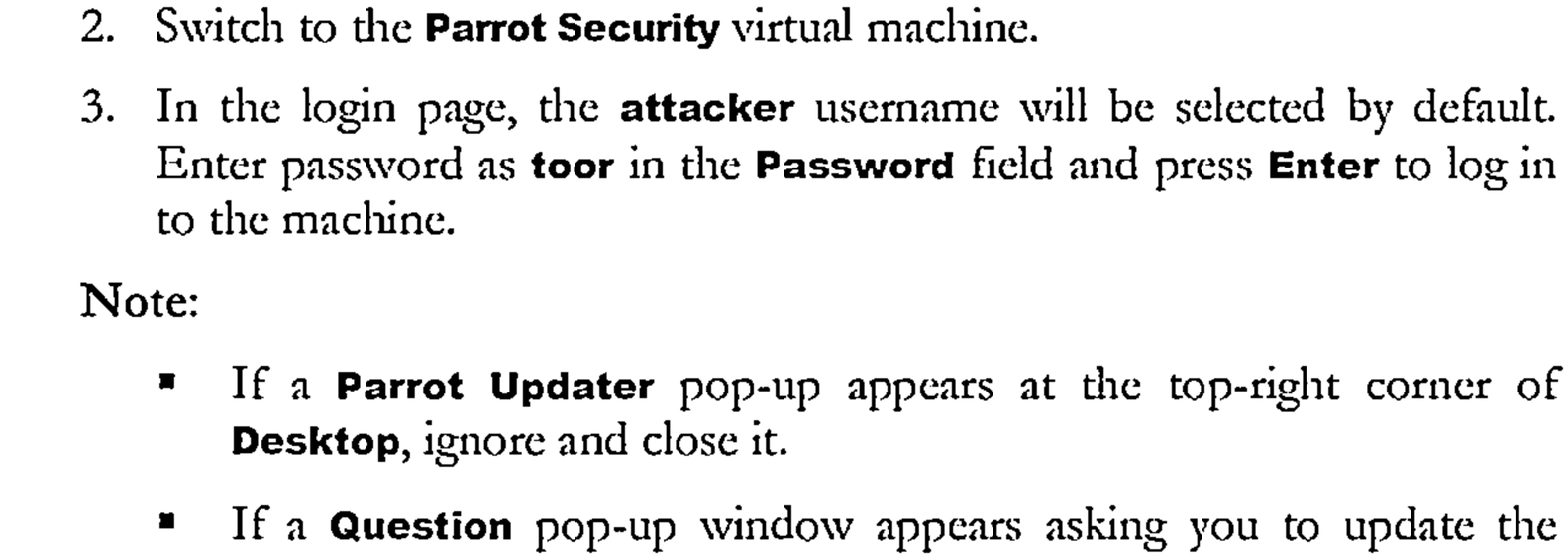


Figure 6.1.1: Running the programs as a root user

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

8. In the **Parrot Terminal** window, type **service postgresql start** and hit **Enter.**

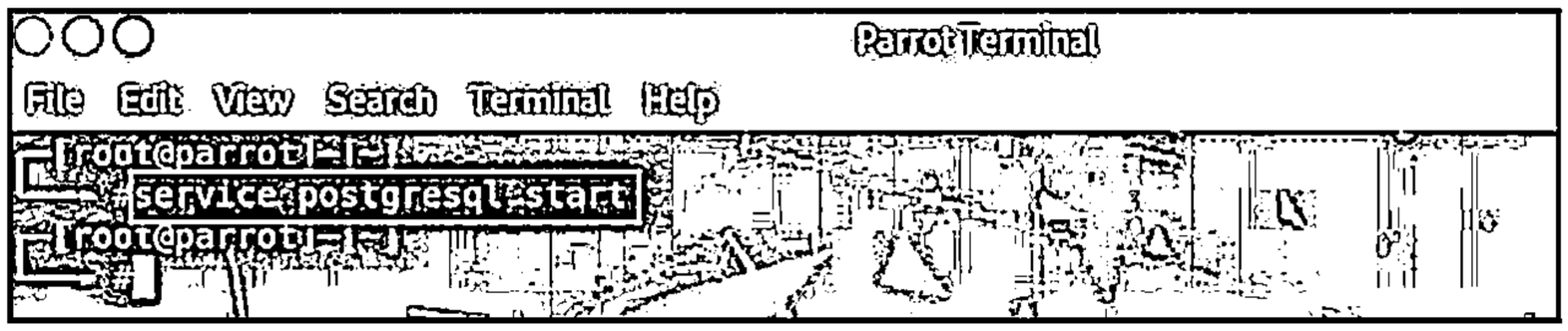


Figure 6.1.2: Start postgresql service through the command line

9. Now, type **msfconsole** and hit **Enter** to launch Metasploit.

Note: The version of Metasploit might differ in your lab environment.

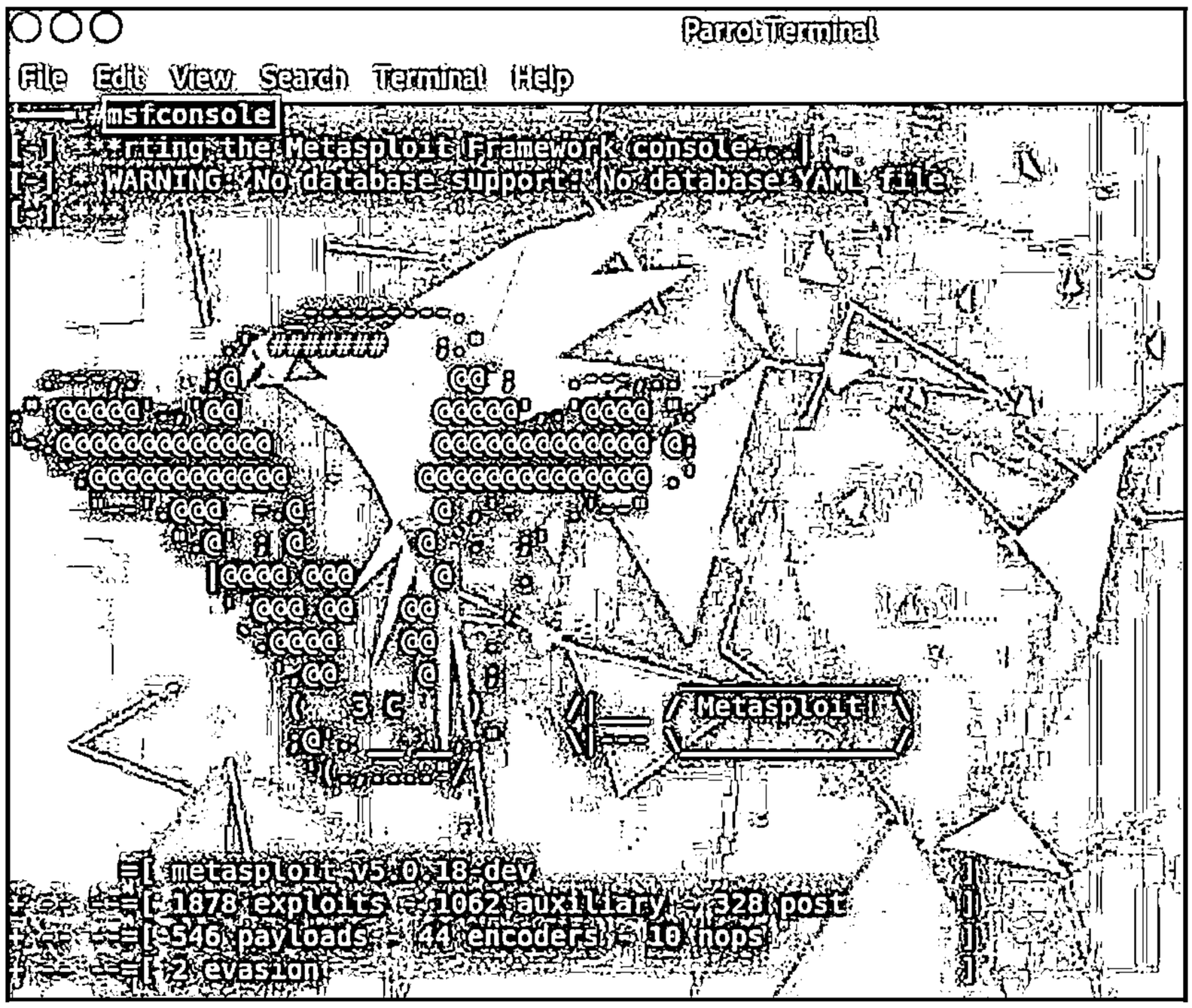


Figure 6.1.3: Launch Metasploit framework

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

10. An msf command line appears. Type **db_status** and hit **Enter** to check if Metasploit has connected to the database successfully. If you receive the message "**postgersql selected, no connection,**" then the database did not connect to msf.

Note: If the message you receive is "**connected to msf,**" then skip to **Step #14**.

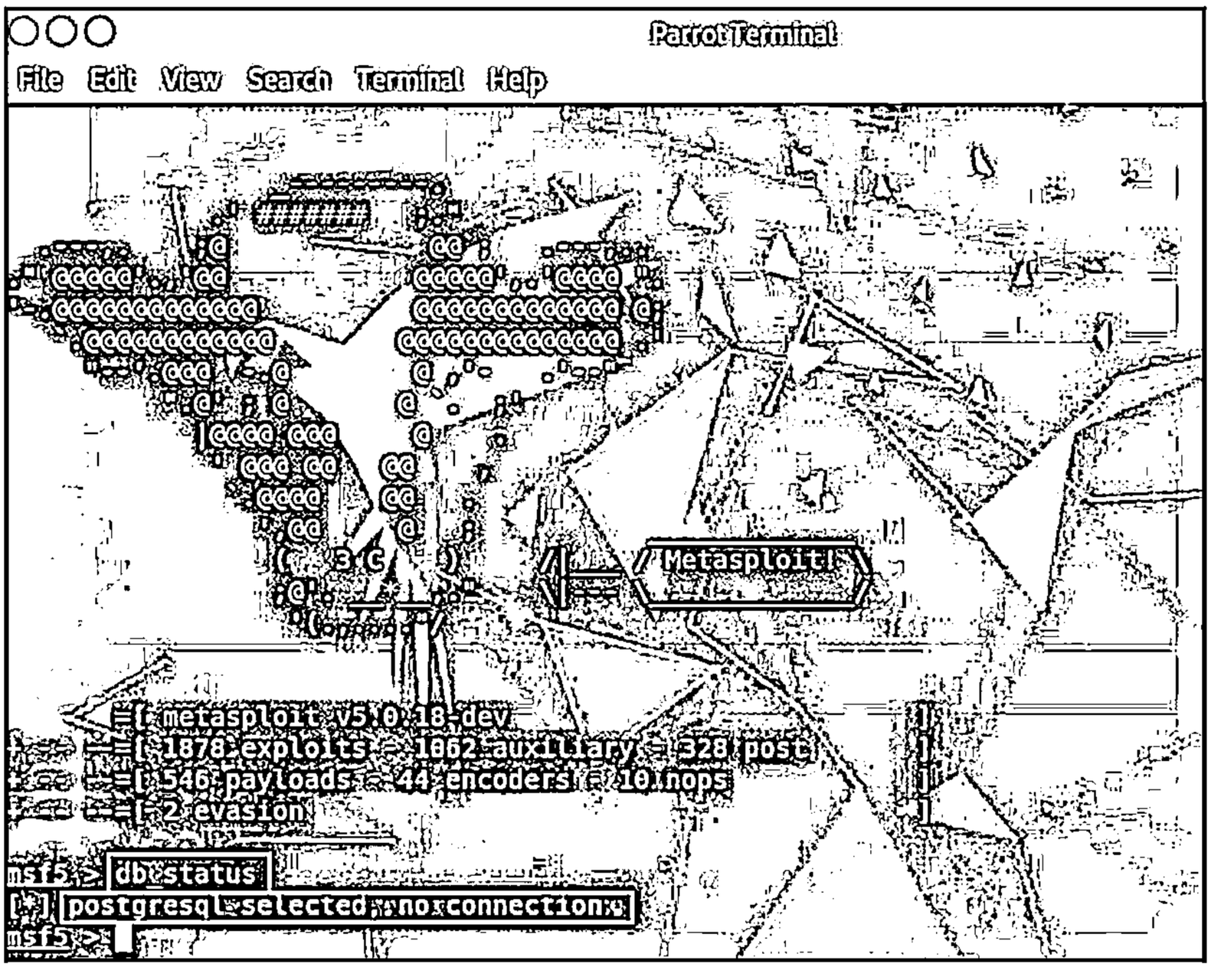


Figure 6.1.4: Database not connected to msf

11. Exit the Metasploit framework by typing **exit** and press **Enter**. Then, to initiate the database, type **msfdb init**, and press **Enter**.

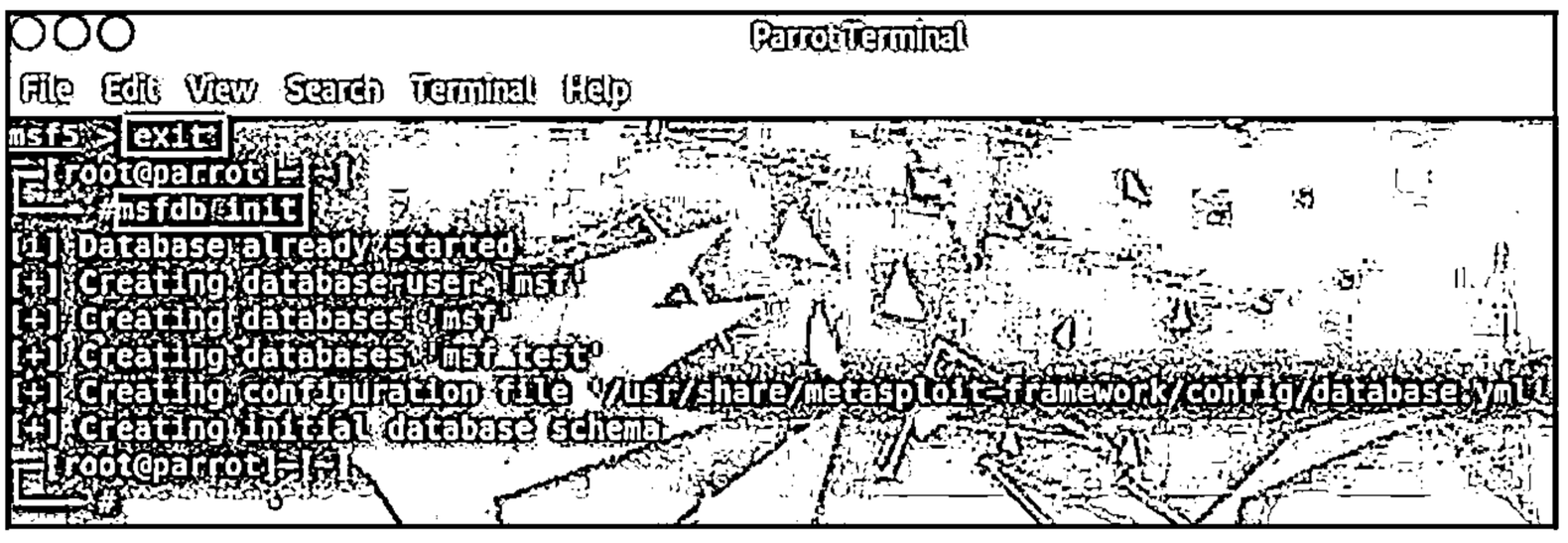


Figure 6.1.5: Initialize the database

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

12. To restart the postgresql service, type **service postgresql restart** and press **Enter**. Now, start the Metasploit Framework again by typing **msfconsole** and pressing **Enter**.

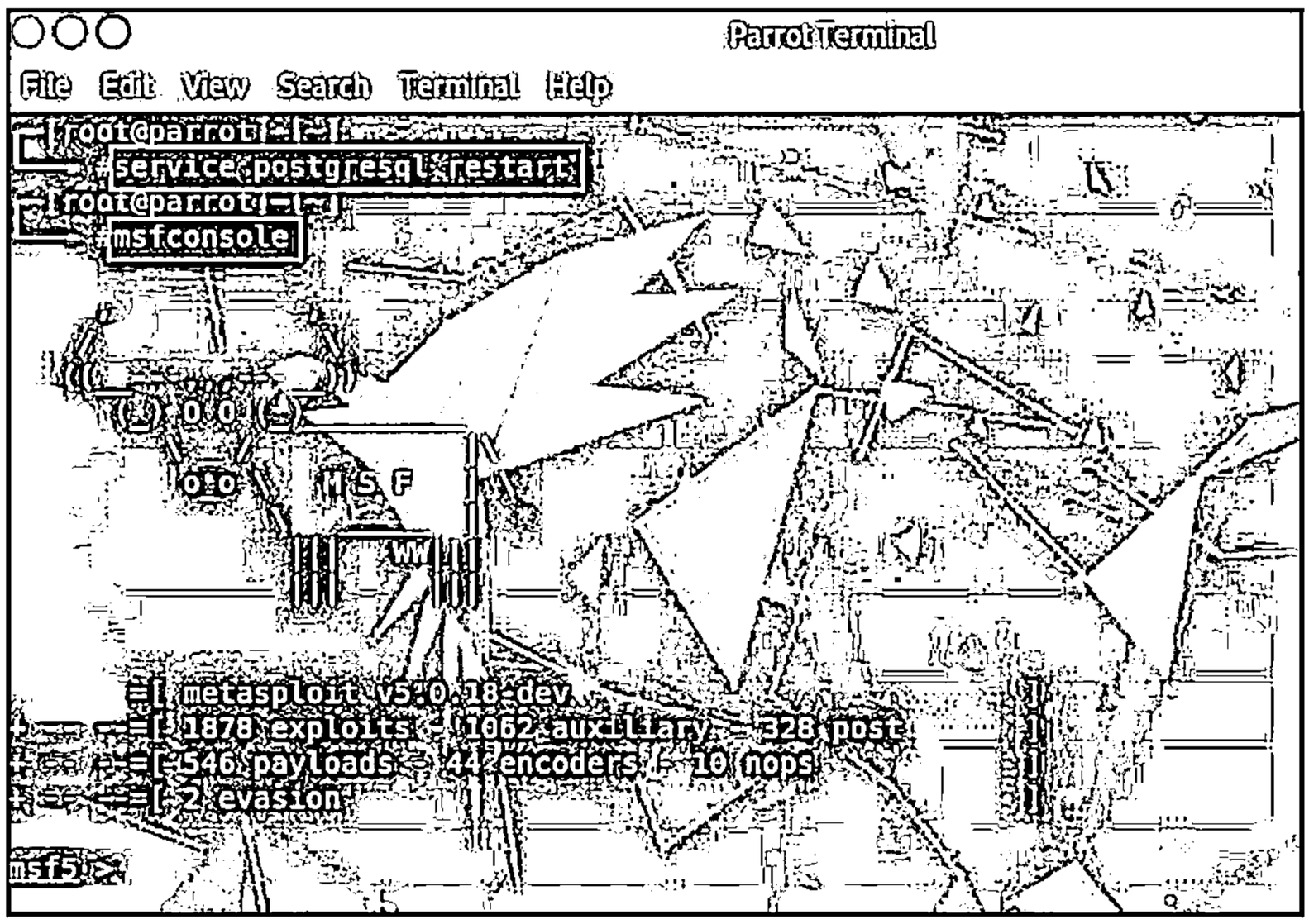


Figure 6.1.6: Launch Metasploit framework

13. Check the database status by typing **db_status** and press **Enter**. This time, the database should successfully connect to msf, as shown in the screenshot.

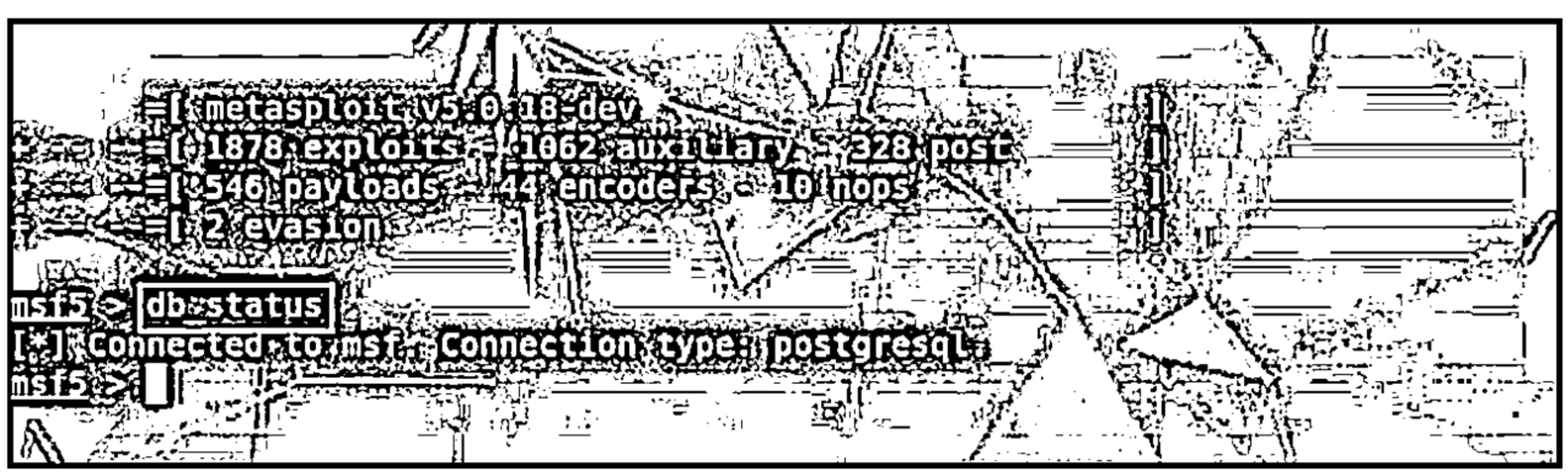


Figure 6.1.7: Verify that database is successfully connected to Metasploit framework

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

TASK 1.2

Information Gathering Using Metasploit

14. Type **nmap -Pn -sS -A -oX Test 10.10.10.0/24** and hit **Enter** to scan the subnet, as shown in the screenshot.

Here, we are scanning the whole subnet 10.10.10.0/24 for active hosts.

Note: The target IP address subnet might differ in your lab environment.

15. Nmap begins scanning the subnet and displays the results. It takes approximately 5 minutes for the scan to complete.

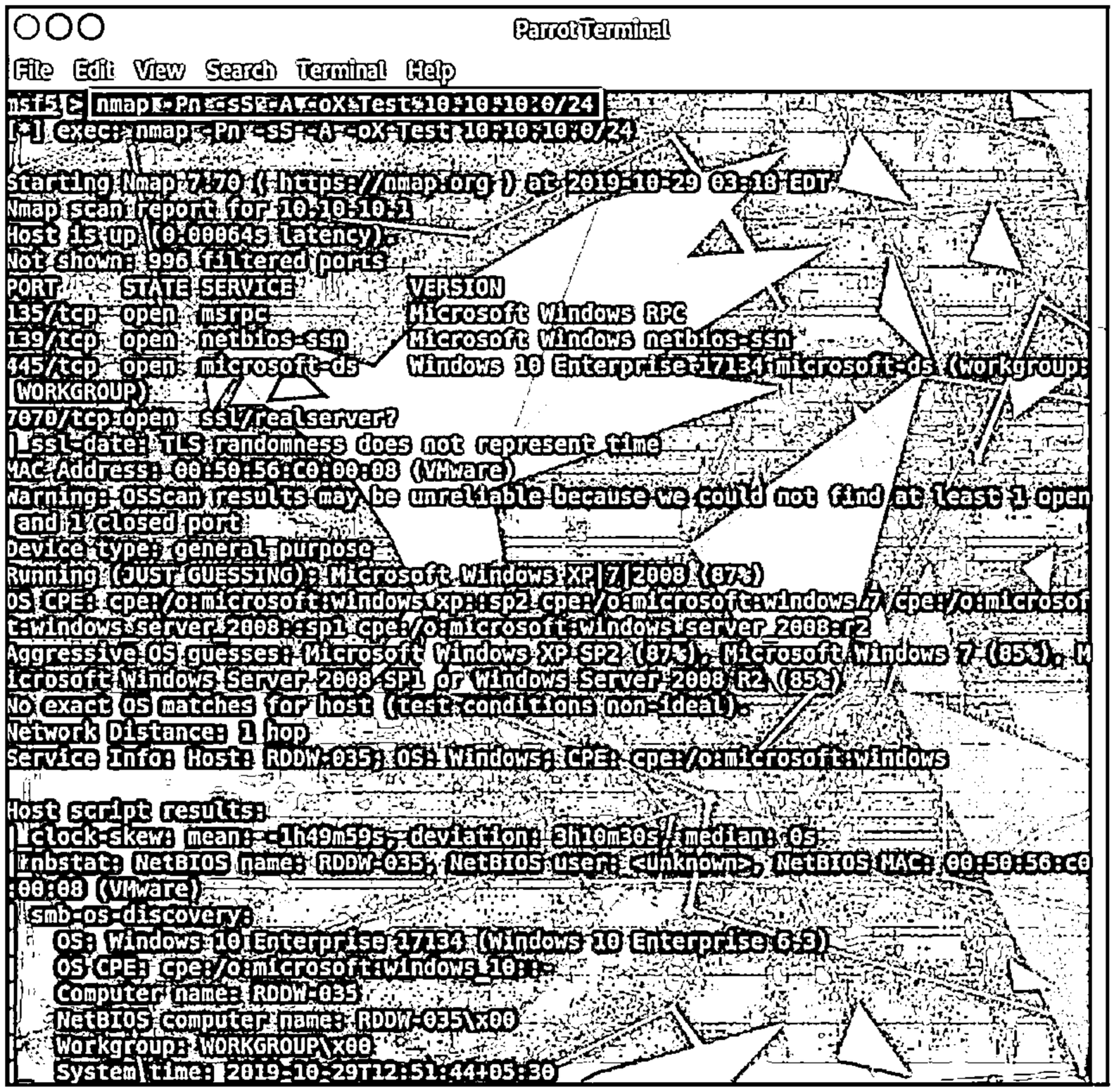


Figure 6.1.8: Nmap scan result

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

16. After the scan completes, Nmap displays the number of active hosts in the target network (here, **6**).

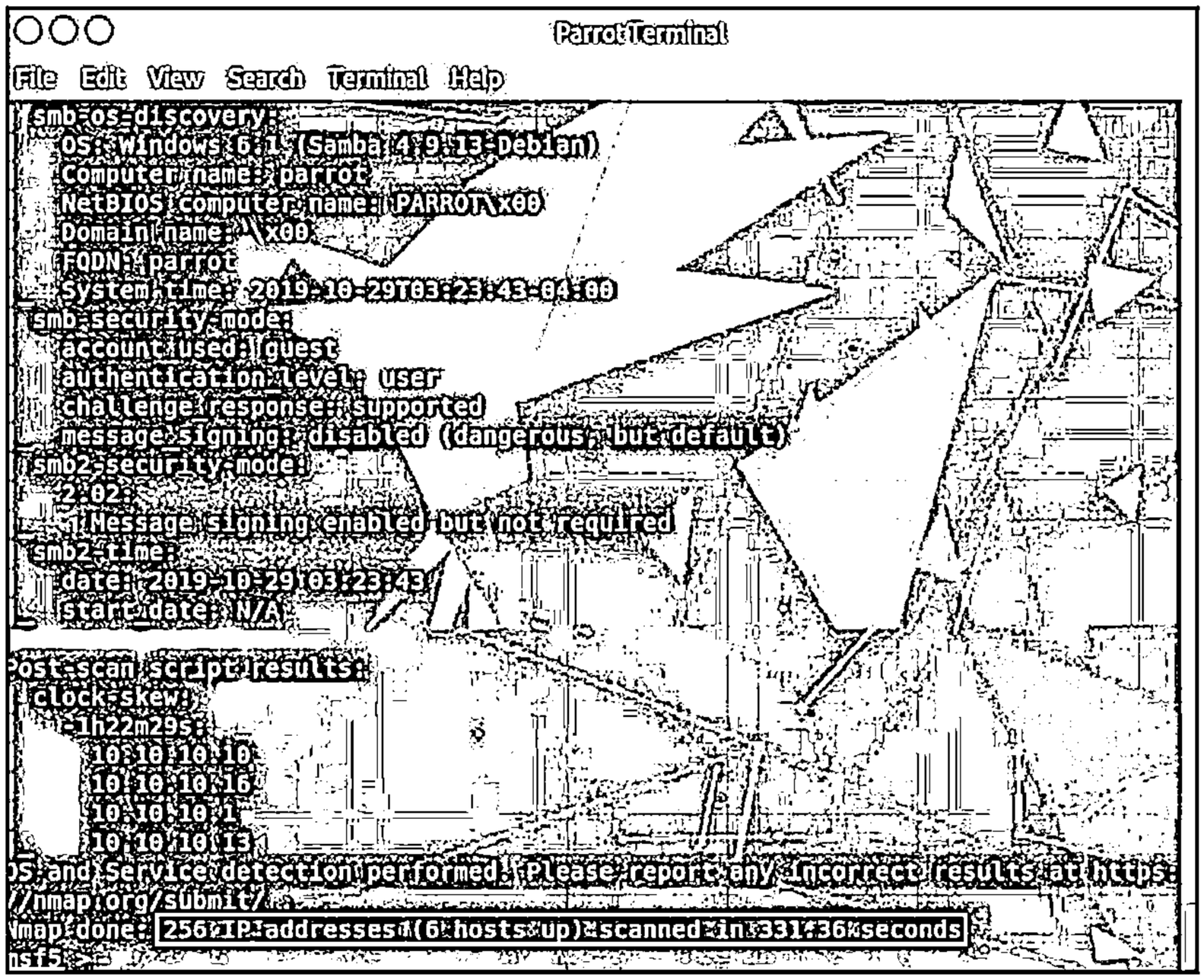


Figure 6.1.9: Nmap showing new found hosts in the subnet

17. Now, type **db_import Test** and hit **Enter** to import the Nmap results from the database.

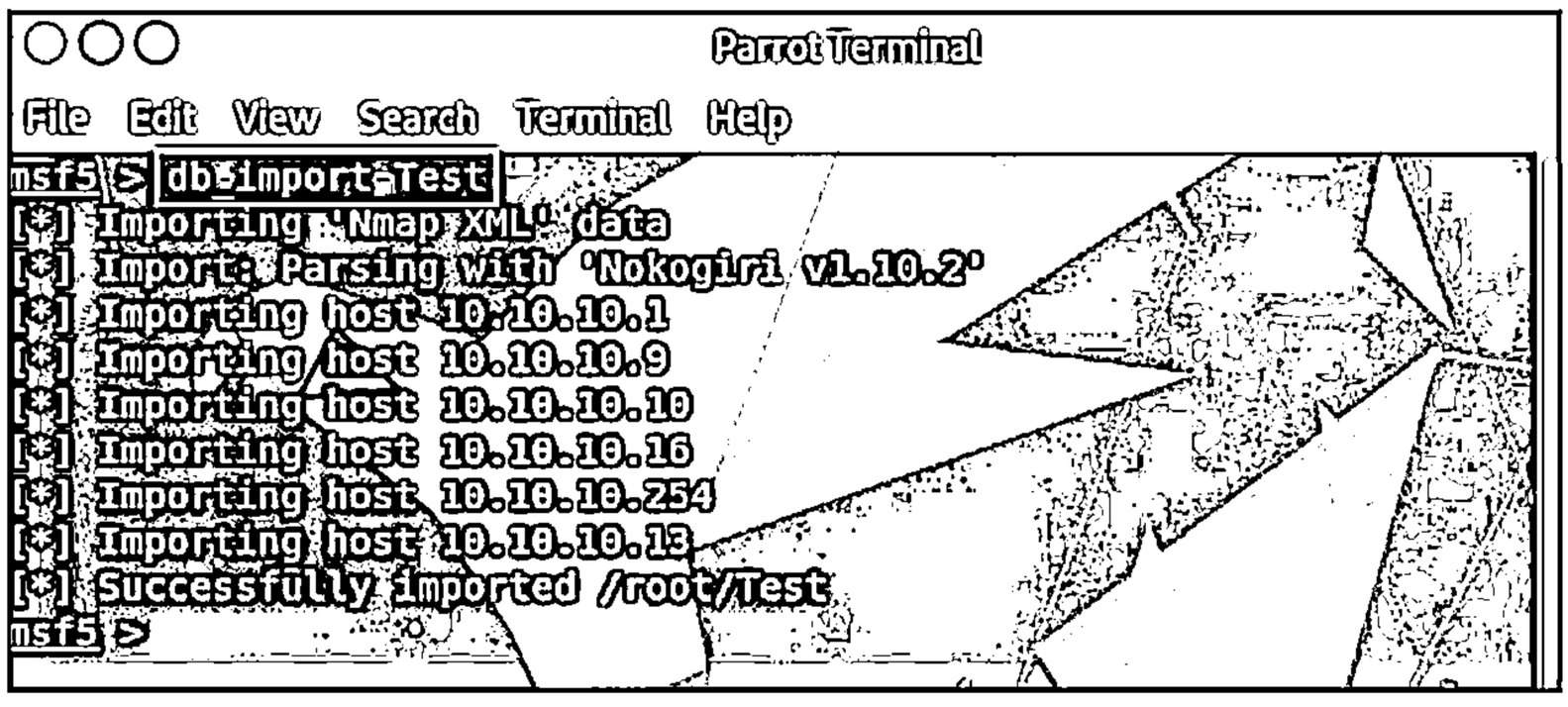


Figure 6.1.10: Importing Nmap results from the database using Metasploit

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

18. Type **hosts** and hit **Enter** to view the list of active hosts along with their MAC addresses, OS names, etc. as shown in the screenshot.

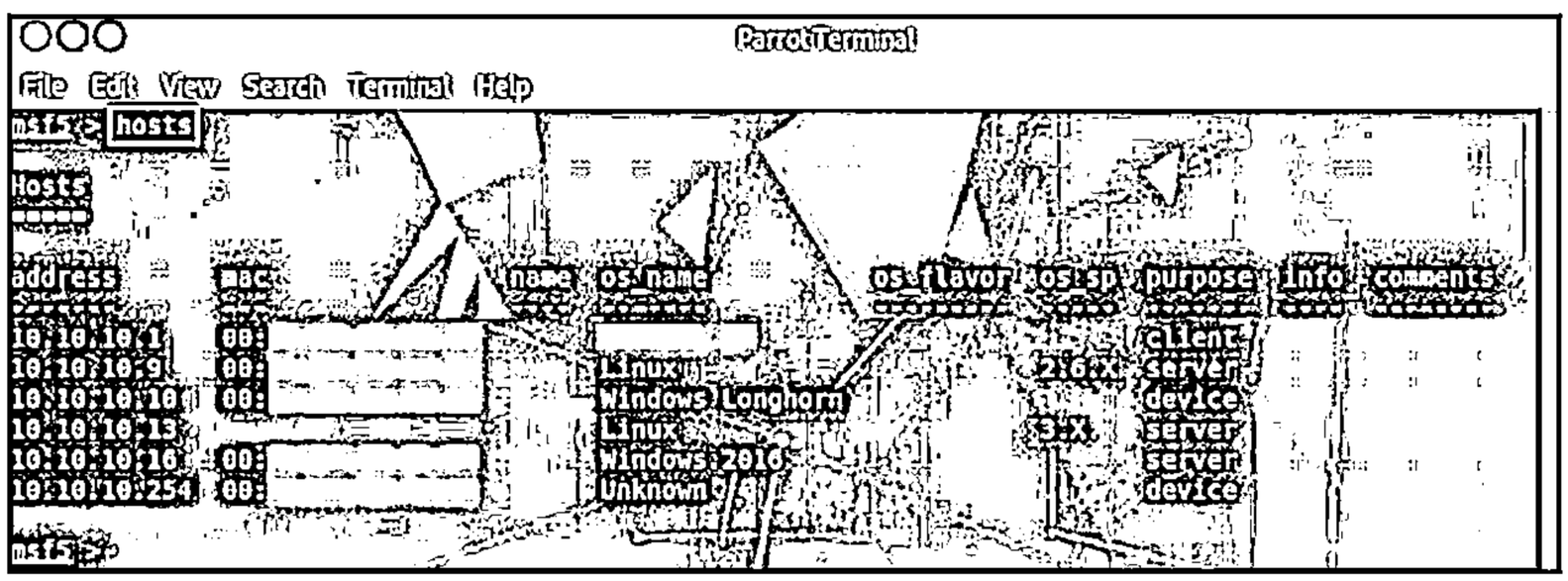


Figure 6.1.11: List of live hosts in the subnet

19. Type **services** or **db_services** and hit **Enter** to receive a list of the services running on the active hosts, as shown in the screenshot.

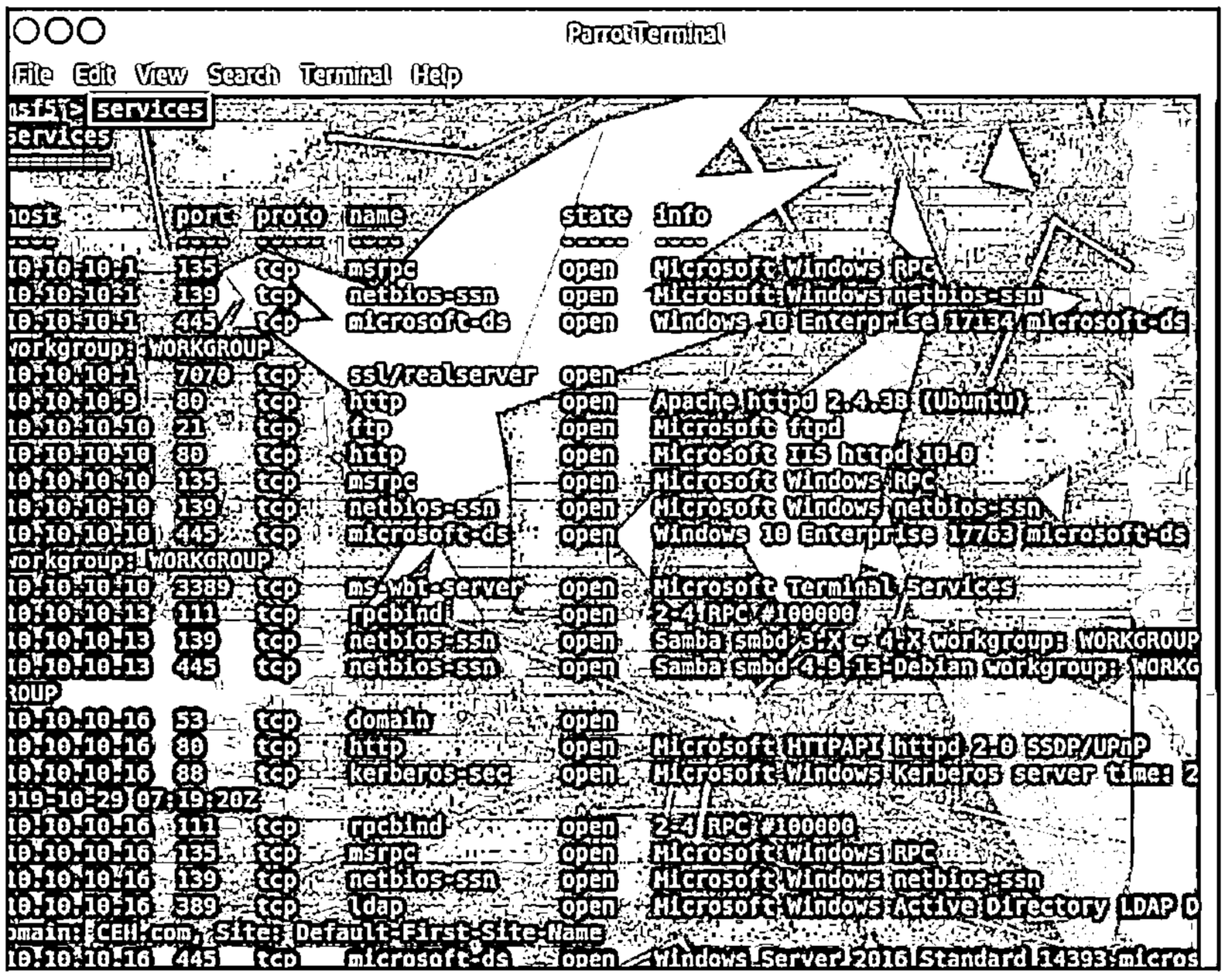


Figure 6.1.12: List of services running on the hosts in the subnet

Note: In addition to running Nmap, there are a variety of other port scanners that are available within the Metasploit framework to scan the target systems.

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

TASK 1.3

Perform Port Scanning Using MSF Modules

20. Type **search portscan** and hit **Enter**. The Metasploit port scanning modules appear, as shown in the screenshot.

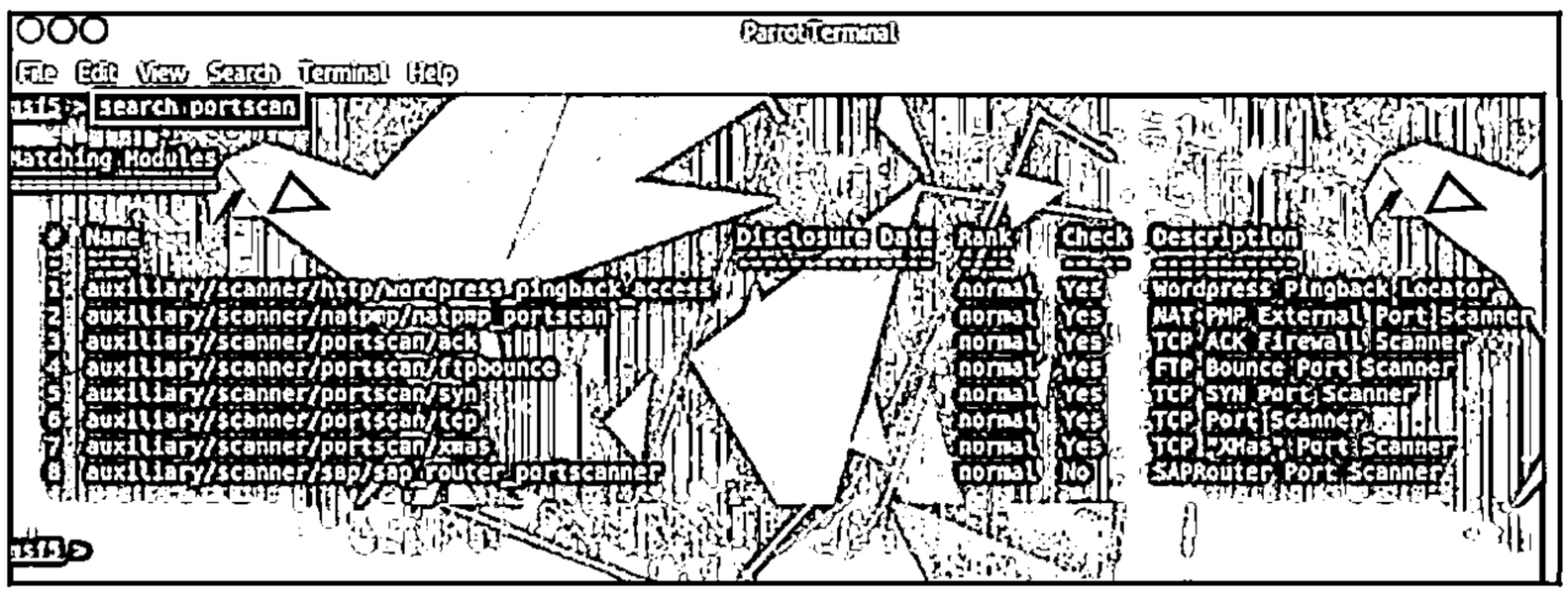


Figure 6.1.13: List portscan modules

21. Here, we will use the **auxiliary/scanner/portscan/syn** module to perform an SYN scan on the target systems. To do so, type **use auxiliary/scanner/portscan/syn** and press **Enter.**

22. We will use this module to perform an SYN scan against the target IP address range (**10.10.10.5-20**) to look for open port 80 through the eth0 interface.

    To do so, issue the below commands:

    - **set INTERFACE eth0**
    - **set PORTS 80**
    - **set RHOSTS 10.10.10.5-20**
    - **set THREADS 50**

Note: **PORTS**: specifies the ports to scan (e.g., 22-25, 80, 110-900), **RHOSTS**: specifies the target address range or CIDR identifier, and **THREADS**: specifies the number of concurrent threads (default 1).

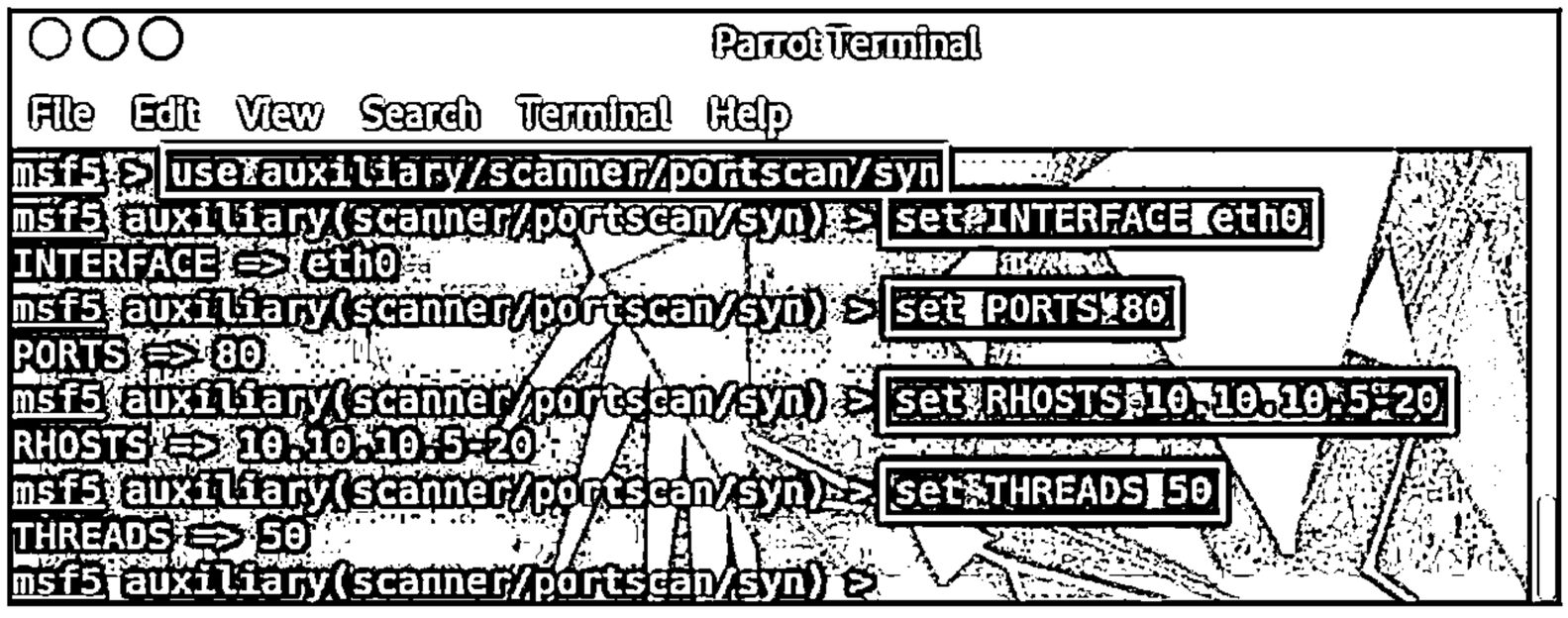


Figure 6.1.14: Setting values to perform a port scan

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

23. After specifying the above values, type **run**, and press **Enter** to initiate the scan against the target IP address range.

Note: Similarly, you can also specify a range of ports to be scanned against the target IP address range.

24. The result appears, displaying open port 80 in active hosts, as shown in the screenshot.

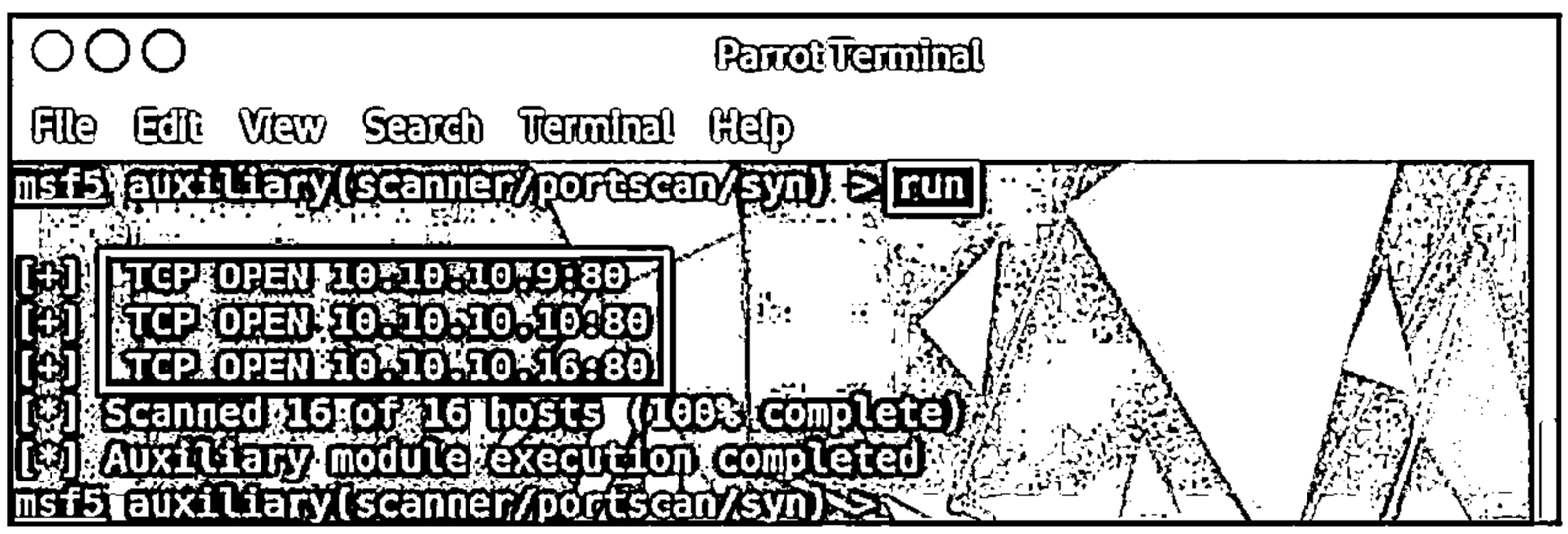


Figure 6.1.15: Port scan result

25. Now, we will perform a TCP scan for open ports on the target systems. To do so, first type **back**, and then press **Enter** to revert to the msf command line.

26. To load the auxiliary/scanner/portscan/tcp module, type **use auxiliary/scanner/portscan/tcp** and press **Enter**.

27. Type **hosts -R** and press **Enter** to automatically set this option with the discovered hosts present in our database.

Or

Type **set RHOSTS <Target IP Address>** and press **Enter**.

Note: Here, we will perform a TCP scan for open ports on a single IP address (**10.10.10.16**), as scanning multiple IP addresses consumes much time.

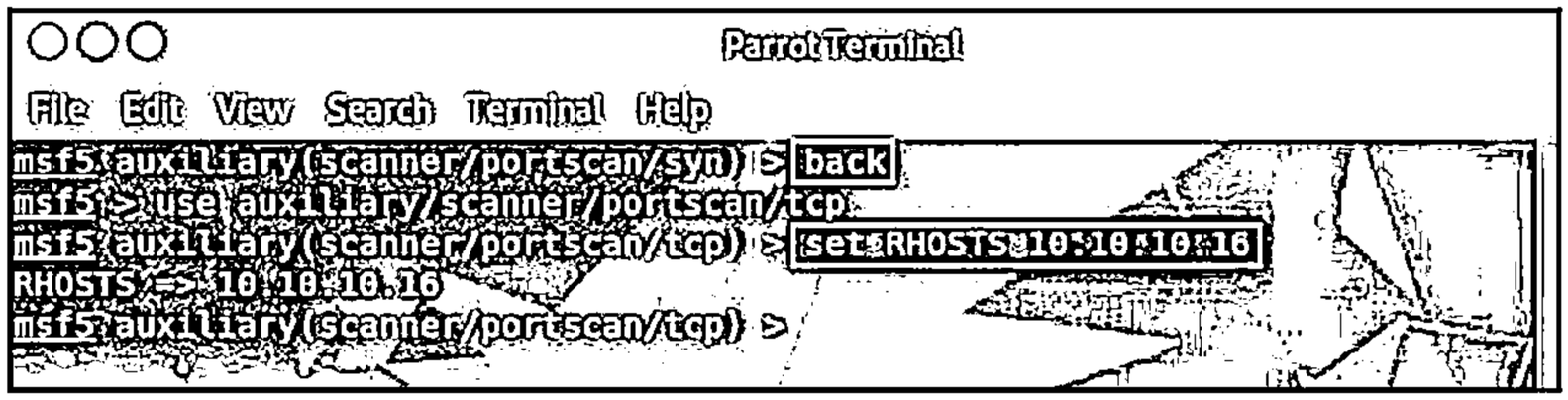


Figure 6.1.16: Port scanning using TCP scan

28. Type **run** and press **Enter** to discover open TCP ports in the target system.

29. The results appear, displaying all open TCP ports in the target IP address (10.10.10.16).

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

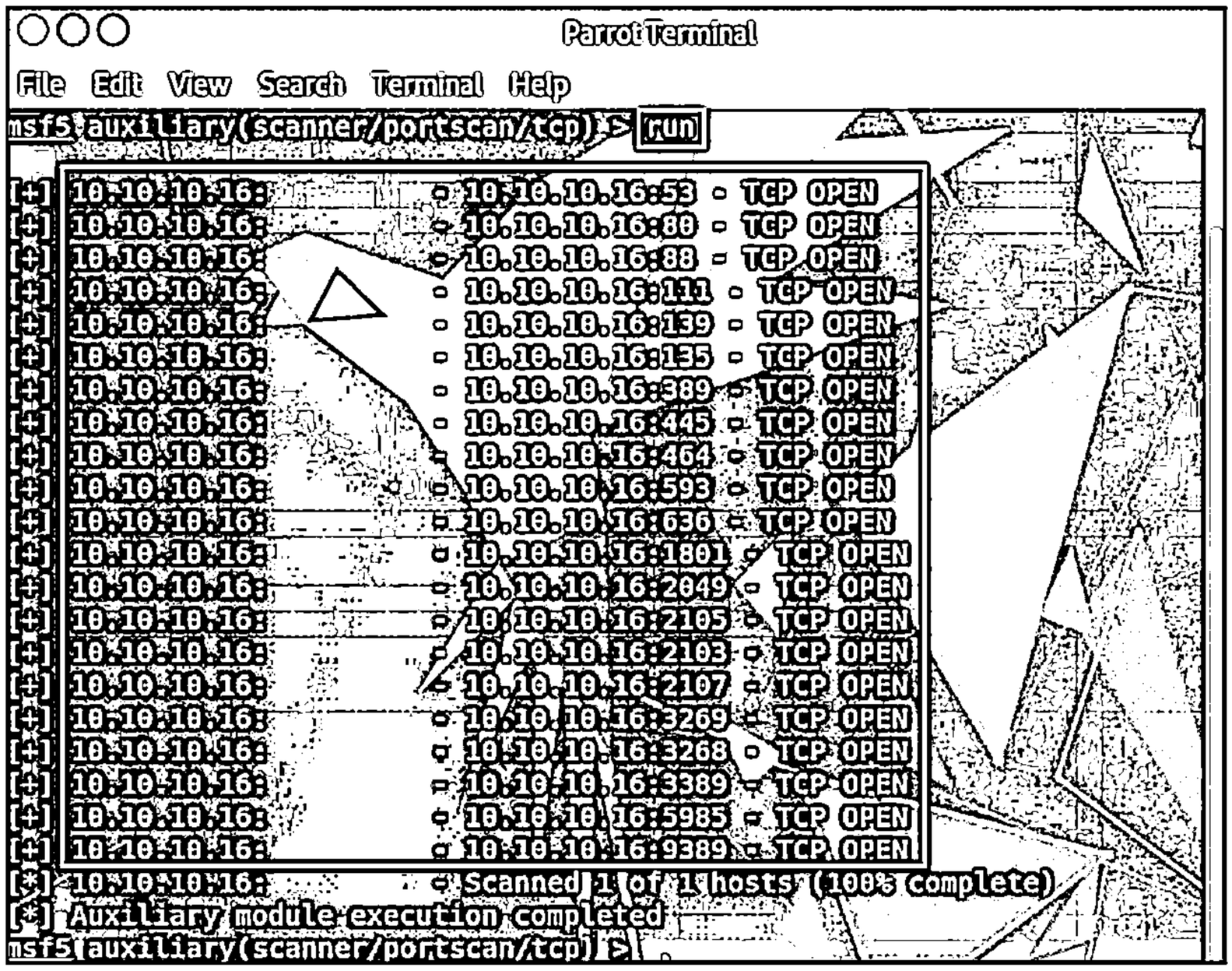


Figure 6.1.17: Port scanning using TCP scan

30. Now that we have determined the active hosts on the target network, we can further attempt to determine the OSes running on the target systems. As there are systems in our scan that have port 445 open, we will use the module scanner/smb/version to determine which version of Windows is running on a target and which Samba version is on a Linux host.

TASK 1.4

SMB Version Scan

31. To do so, first type **back**, and then press **Enter** to revert to the msf command line. Then, type **use auxiliary/scanner/smb/smb_version** and press **Enter**.

32. We will use this module to run a SMB version scan against the target IP address range (**10.10.10.5-20**). To do so, issue the below commands:

- **set RHOSTS 10.10.10.5-20**
- **set THREADS 11**

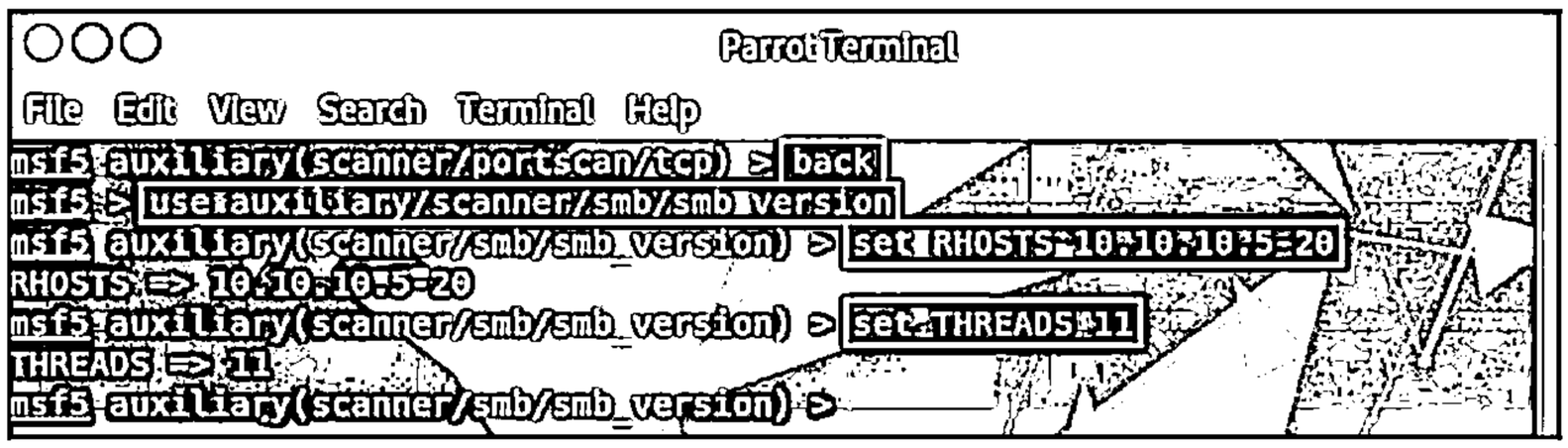


Figure 6.1.18: SMB version scanning

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

33. Type **run** and press **Enter** to display the SMB versions of the target hosts.

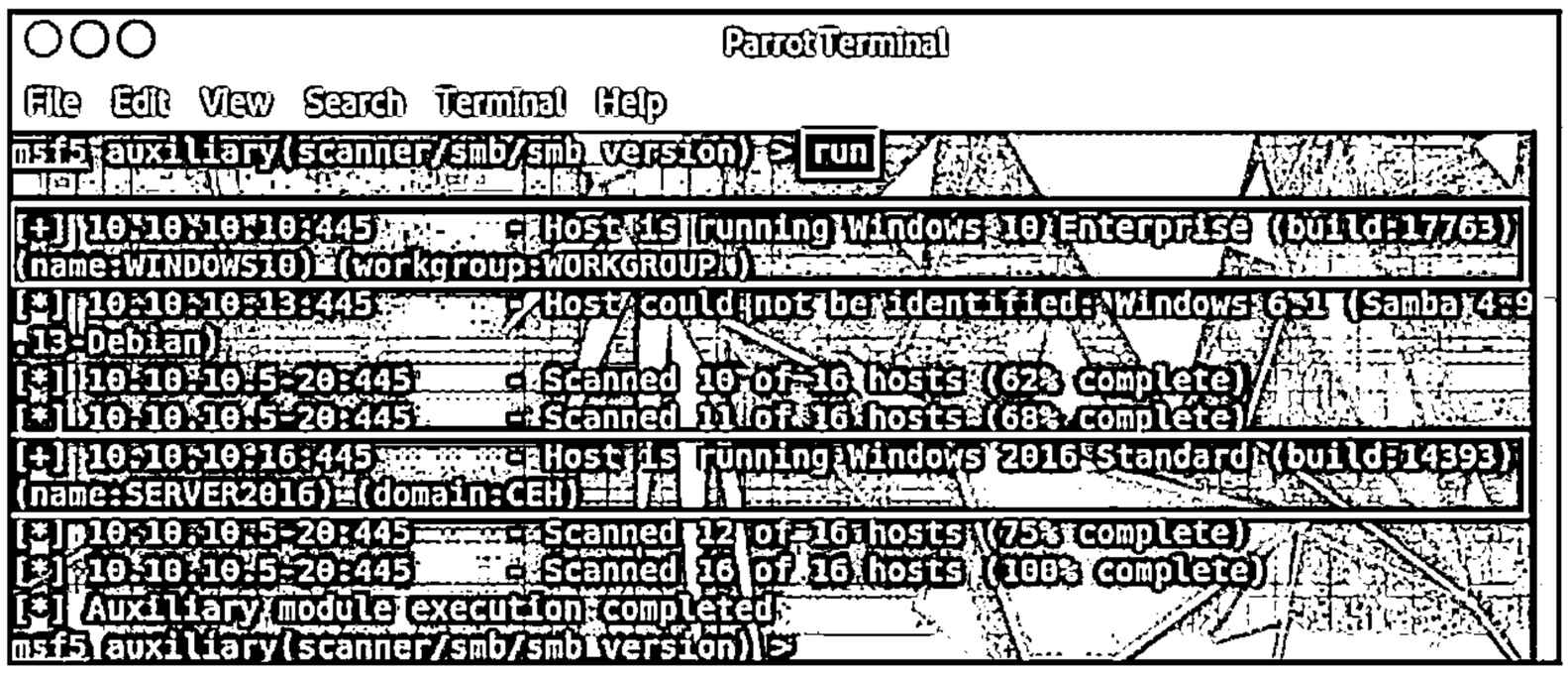


Figure 6.1.19: SMB version scanning results

TASK 1.5

FTP Version Identification

34. While performing a scan using Nmap, we discovered that the FTP port 21 is open on the host 10.10.10.10 in the target network. Now, we will scan the target host to identify the FTP version.
35. Type **back** and press **Enter**. To load an FTP module, type **use auxiliary/scanner/ftp/ftp_version** and press **Enter**.
36. Type **set RHOSTS 10.10.10.10** and press **Enter** to specify the target host.

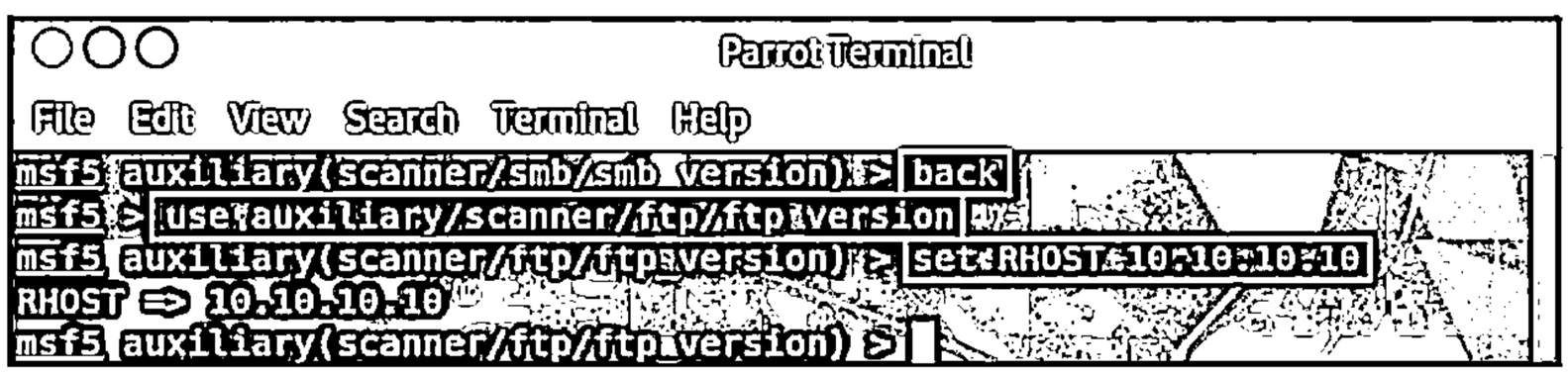


Figure 6.1.20: FTP version scanning

37. Type **run** and press **Enter** to initiate the FTP version identification scan.
38. The result appears, displaying the FTP version details of the target host, as shown in the screenshot.

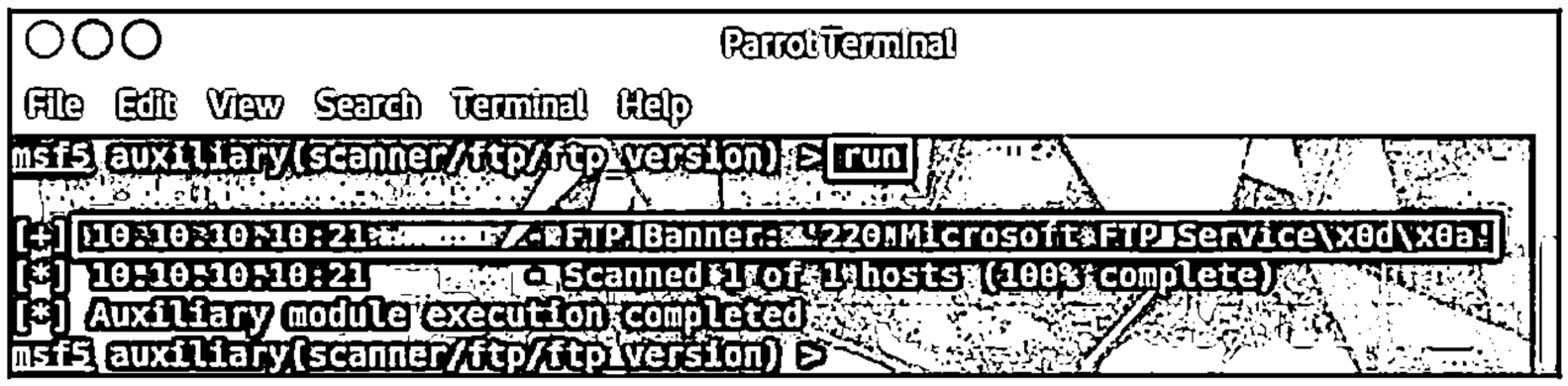


Figure 6.1.21: FTP version identification scan results

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

39. Type **hosts** and press **Enter** to view detailed information on active hosts in the target network.

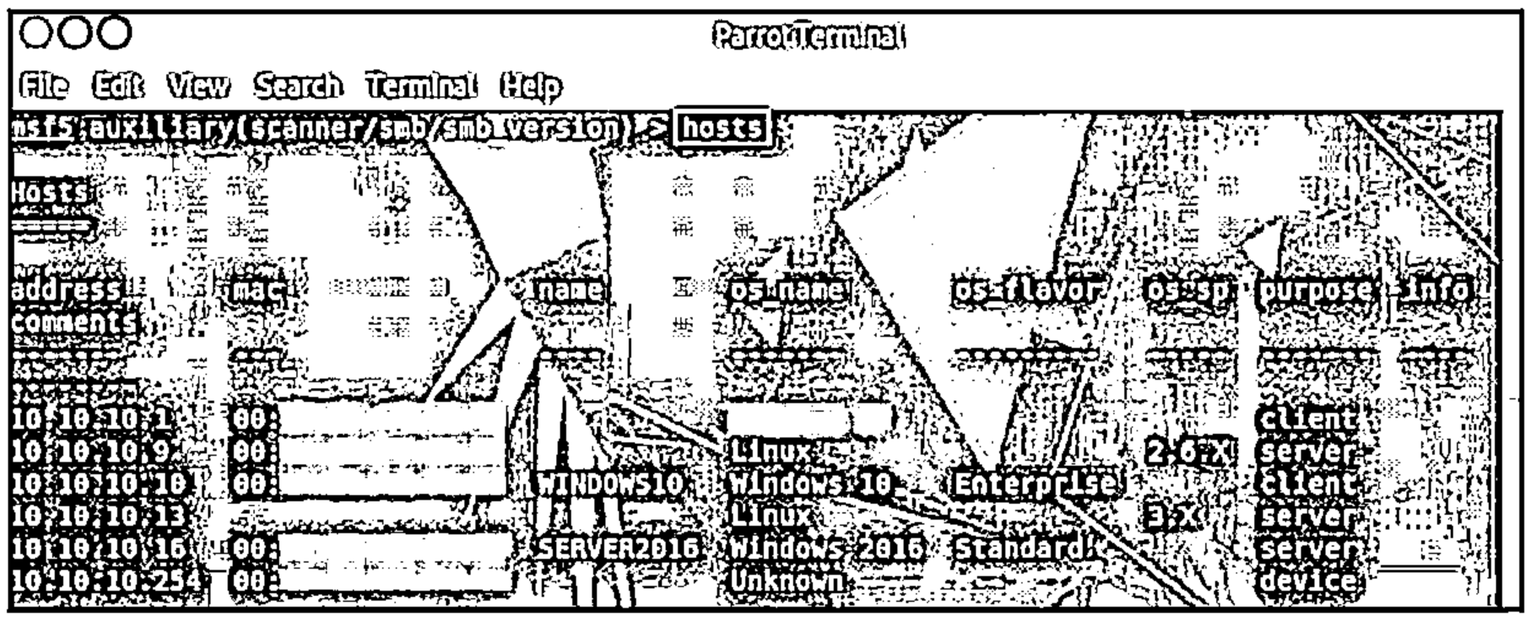


Figure 6.1.22: List of live hosts in the target IP range

TASK 1.6

Export Scan Result

40. You can further export this information to a CSV file. To do so, first type **back**, and then press **Enter**. Now, type **hosts -o /root/Desktop/Metasploit_Scan_Results.csv** and press **Enter**.

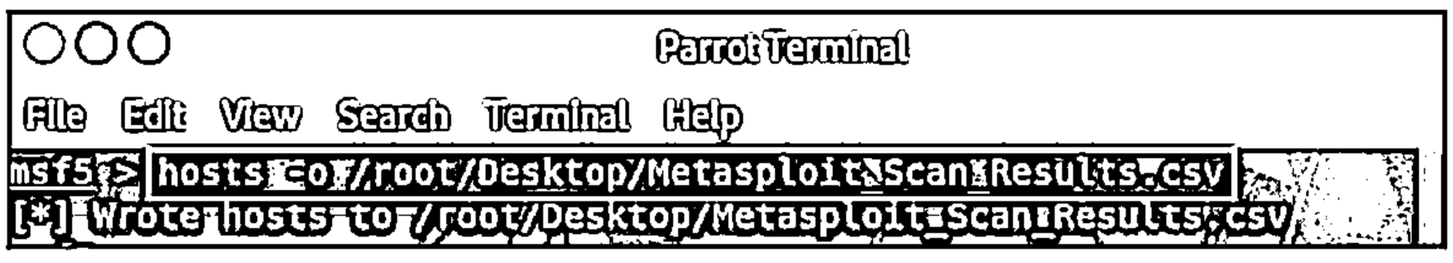
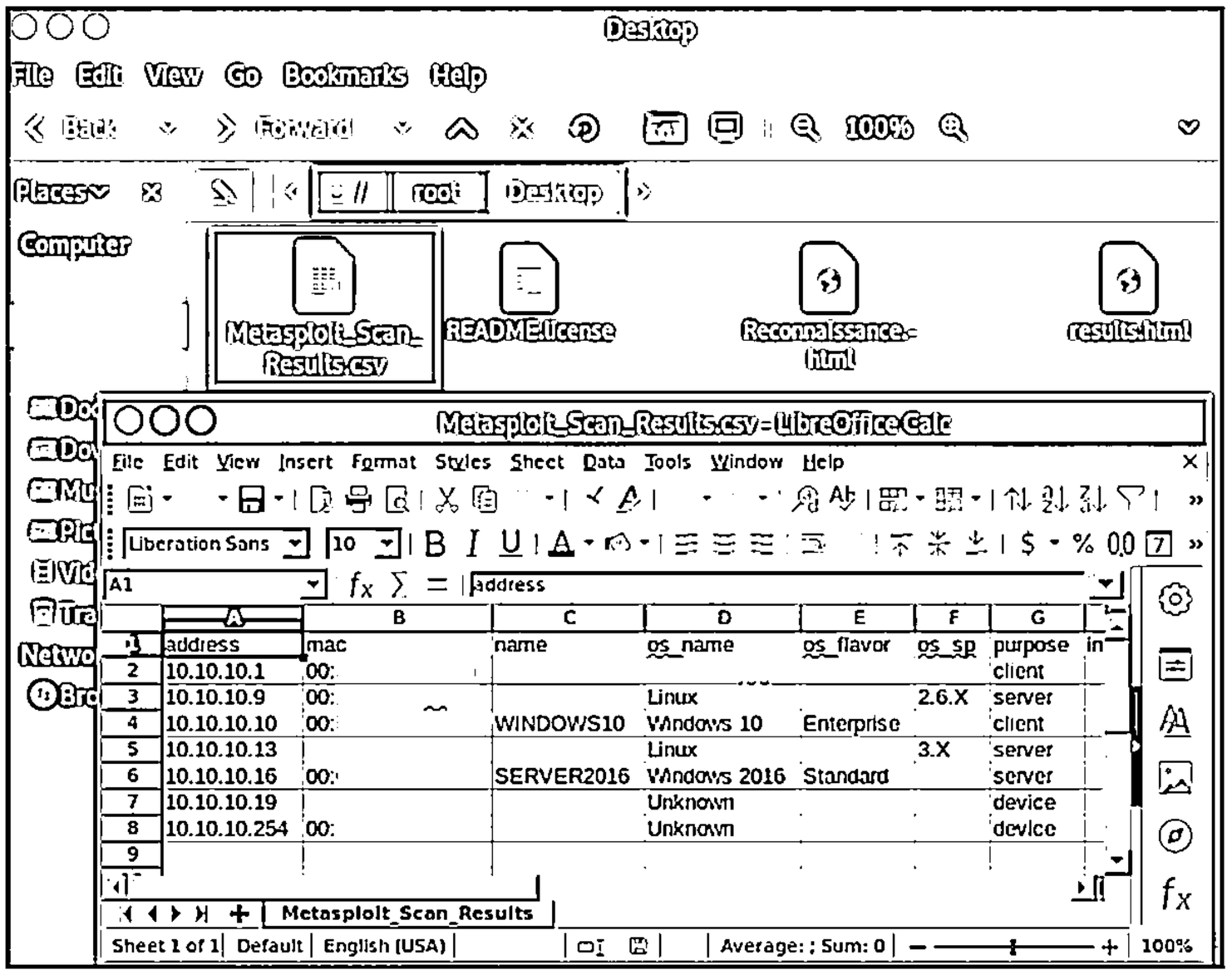


Figure 6.1.23: Exporting hosts data

41. Navigate to the location **/root/Desktop** and double-click the **Metasploit_Scan_Results.csv** file. The CSV file appears, displaying detailed information on the active hosts in the target IP range.

Note: To navigate to the **Desktop** directory, click **Places** from the top-section of the **Desktop** and click **Home Folder** from the drop-down options. In the **attacker** window, click **File System** from the left-pane and navigate to the location **root/Desktop**.

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



	A	B	C	D	E	F	G	
1	address	mac	name	os_name	os_flavor	os_sp	purpose	in
2	10.10.10.1	00:					client	
3	10.10.10.9	00:		Linux		2.6.X	server	
4	10.10.10.10	00:	WINDOWS10	Windows 10	Enterprise		client	
5	10.10.10.13			Linux		3.X	server	
6	10.10.10.16	00:	SERVER2016	Windows 2016	Standard		server	
7	10.10.10.19			Unknown			device	
8	10.10.10.254	00:		Unknown			device	
9								

Figure 6.1.24: Exported hosts information

42. This information can further be used to perform vulnerability analysis on the open services discovered in the target hosts.
43. This concludes the demonstration of gathering information on open ports, a list of services running on active hosts, and information related to OSes, amongst others.
44. Close all open windows and document all the acquired information.
45. Turn off the **Windows 10**, **Windows Server 2016**, **Ubuntu**, and **Parrot Security** virtual machines.

Lab Analysis

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

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT 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

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

Enumeration

Enumeration is the process of extracting usernames, machine names, network resources, shares, and services from a system or network.

ICON KEY

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

Lab Scenario

With the development of network technologies and applications, network attacks are greatly increasing in both number and severity. Attackers continuously search for service and application vulnerabilities on networks and servers. When they find a flaw or loophole in a service run over the Internet, they immediately exploit it to compromise the entire system. Any other data that they find may be further used to compromise additional network systems. Similarly, attackers seek out and use workstations with administrative privileges, and which run flawed applications, to execute arbitrary code or implant viruses in order to intensify damage to the network.

In the first step of the security assessment and penetration testing of your organization, you gather open-source information about your organization. In the second step, you collect information about open ports and services, OSes, and any configuration lapses.

The next step for an ethical hacker or penetration tester is to probe the target network further by performing enumeration. Using various techniques, you should extract more details about the network such as lists of computers, usernames, user groups, ports, OSes, machine names, network resources, and services.

The information gleaned from enumeration will help you to identify the vulnerabilities in your system's security that attackers would seek to exploit. Such information could also enable attackers to perform password attacks to gain unauthorized access to information system resources.

In the previous steps, you gathered necessary information about a target without contravening any legal boundaries. However, please note that enumeration activities may be illegal depending on an organization's policies and any laws that are in effect in your location. As an ethical hacker or penetration tester, you should always acquire proper authorization before performing enumeration.

Lab Objectives

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

- Machine names, their OSes, services, and ports
- Network resources
- Usernames and user groups
- Lists of shares on individual hosts on the network

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

- Policies and passwords
- Routing tables
- Audit and service settings
- SNMP and FQDN details

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 04 Enumeration

Lab Environment

To carry out this lab, you need:

- Windows Server 2019 virtual machine
- Windows Server 2016 virtual machine
- Windows 10 virtual machine
- Parrot Security virtual machine
- Ubuntu virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 115 Minutes

Overview of Enumeration

Enumeration creates an active connection with the system and performs directed queries to gain more information about the target. It extracts lists of computers, usernames, user groups, ports, OSes, machine names, network resources, and services using various techniques. Enumeration techniques are conducted in an intranet environment.

Lab Tasks

Ethical hackers or penetration testers use several tools and techniques to enumerate the target network. Recommended labs that will assist you in learning various enumeration techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	iLabs ***
1	Perform NetBIOS Enumeration	√	√	√
	1.1 Perform NetBIOS Enumeration using Windows Command-Line Utilities	√		√
	1.2 Perform NetBIOS Enumeration using NetBIOS Enumerator		√	√
	1.3 Perform NetBIOS Enumeration using an NSE Script		√	√

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

2	Perform SNMP Enumeration	√	√	√
	2.1 Perform SNMP Enumeration using snmp-check	√		√
	2.2 Perform SNMP Enumeration using SoftPerfect Network Scanner		√	√
3	Perform LDAP Enumeration	√		√
	3.1 Perform LDAP Enumeration using Active Directory Explorer (AD Explorer)	√		√
4	Perform NFS Enumeration	√		√
	4.1 Perform NFS Enumeration using RPCScan and SuperEnum	√		√
5	Perform DNS Enumeration	√	√	√
	5.1 Perform DNS Enumeration using Zone Transfer	√		√
	5.2 Perform DNS Enumeration using DNSSEC Zone Walking		√	√
6	Perform RPC, SMB, and FTP Enumeration		√	√
	6.1 Perform RPC and SMB Enumeration using NetScanTools Pro		√	√
	6.2 Perform RPC, SMB, and FTP Enumeration using Nmap		√	√
7	Perform Enumeration using Various Enumeration Tools	√	√	√
	7.1 Enumerate Information using Global Network Inventory	√		√
	7.2 Enumerate Network Resources using Advanced IP Scanner		√	√
	7.3 Enumerate Information from Windows and Samba Hosts using Enum4linux		√	√

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

***Core** - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv11 volume 1 book.

*****iLabs** - Lab exercise(s) marked under iLabs are available in our iLabs solution. iLabs is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed from anywhere with an Internet connection. If you are interested to learn more about our iLabs solution, please contact your training center or visit https://ilabs.eccouncil.org.

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

Lab Analysis

Analyze and document the results related to this lab exercise. Provide your opinion of 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

Perform NetBIOS Enumeration

NetBIOS enumeration is a process of obtaining sensitive information about the target such as a list of computers belonging to a target domain, network shares, policies, etc.

ICON KEY

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

Lab Scenario

As a professional ethical hacker or penetration tester, your first step in the enumeration of a Windows system is to exploit the NetBIOS API. NetBIOS enumeration allows you to collect information about the target such as a list of computers that belong to a target domain, shares on individual hosts in the target network, policies, passwords, etc. This data can be used to probe the machines further for detailed information about the network and host resources.

Lab Objectives

- Perform NetBIOS enumeration using Windows command-line utilities
- Perform NetBIOS enumeration using NetBIOS Enumerator
- Perform NetBIOS enumeration using an NSE Script

Lab Environment

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 04 Enumeration

To carry out this lab, you need:

- Windows Server 2019 virtual machine
- Windows Server 2016 virtual machine
- Windows 10 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- NetBIOS Enumerator located at **E:\CEH-Tools\CEHv11 Module 04 Enumeration\NetBIOS Enumeration Tools\NetBIOS Enumerator**
- You may also download the latest version of **NetBIOS Enumerator** from the official website. Please note, however, that if you decide to download the latest version, the 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: 20 Minutes

Overview of NetBIOS Enumeration

NetBIOS stands for Network Basic Input Output System. Windows uses NetBIOS for file and printer sharing. A NetBIOS name is a unique computer name assigned to Windows systems, comprising a 16-character ASCII string that identifies the network device over TCP/IP. The first 15 characters are used for the device name, and the 16th is reserved for the service or name record type.

The NetBIOS service is easily targeted, as it is simple to exploit and runs on Windows systems even when not in use. NetBIOS enumeration allows attackers to read or write to a remote computer system (depending on the availability of shares) or launch a denial of service (DoS) attack.

Lab Tasks

TASK 1

Perform NetBIOS Enumeration using Windows Command-Line Utilities

Here, we will use the *Nbtstat*, and *Net use* Windows command-line utilities to perform NetBIOS enumeration on the target network.

Note: We will use a **Windows Server 2019** (10.10.10.19) virtual machine to target a **Windows 10** (10.10.10.10) virtual machine.

1. Start the **Windows Server 2019** and **Windows 10** virtual machines.
2. In the **Windows Server 2019** virtual machine, log in with the credentials **Administrator** and **Pa$$w0rd**.

TASK 1.1

View the NetBIOS Name Table of a Remote Computer

3. Open a **Command Prompt** window.
4. Type **nbtstat -a <IP address of the remote machine>** (in this example, the target IP address is **10.10.10.10**) and press **Enter**.

Note: In this command, **-a** displays the NetBIOS name table of a remote computer.

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

🗁 Nbtstat helps in troubleshooting NETBIOS name resolution problems. The nbtstat command removes and corrects preloaded entries using several case-sensitive switches. Nbtstat can be used to enumerate information such as NetBIOS over TCP/IP (NetBT) protocol statistics, NetBIOS name tables for both the local and remote computers, and the NetBIOS name cache.

5. The result appears, displaying the NetBIOS name table of a remote computer (in this case, the **WINDOWS10** virtual machine), as shown in the screenshot.

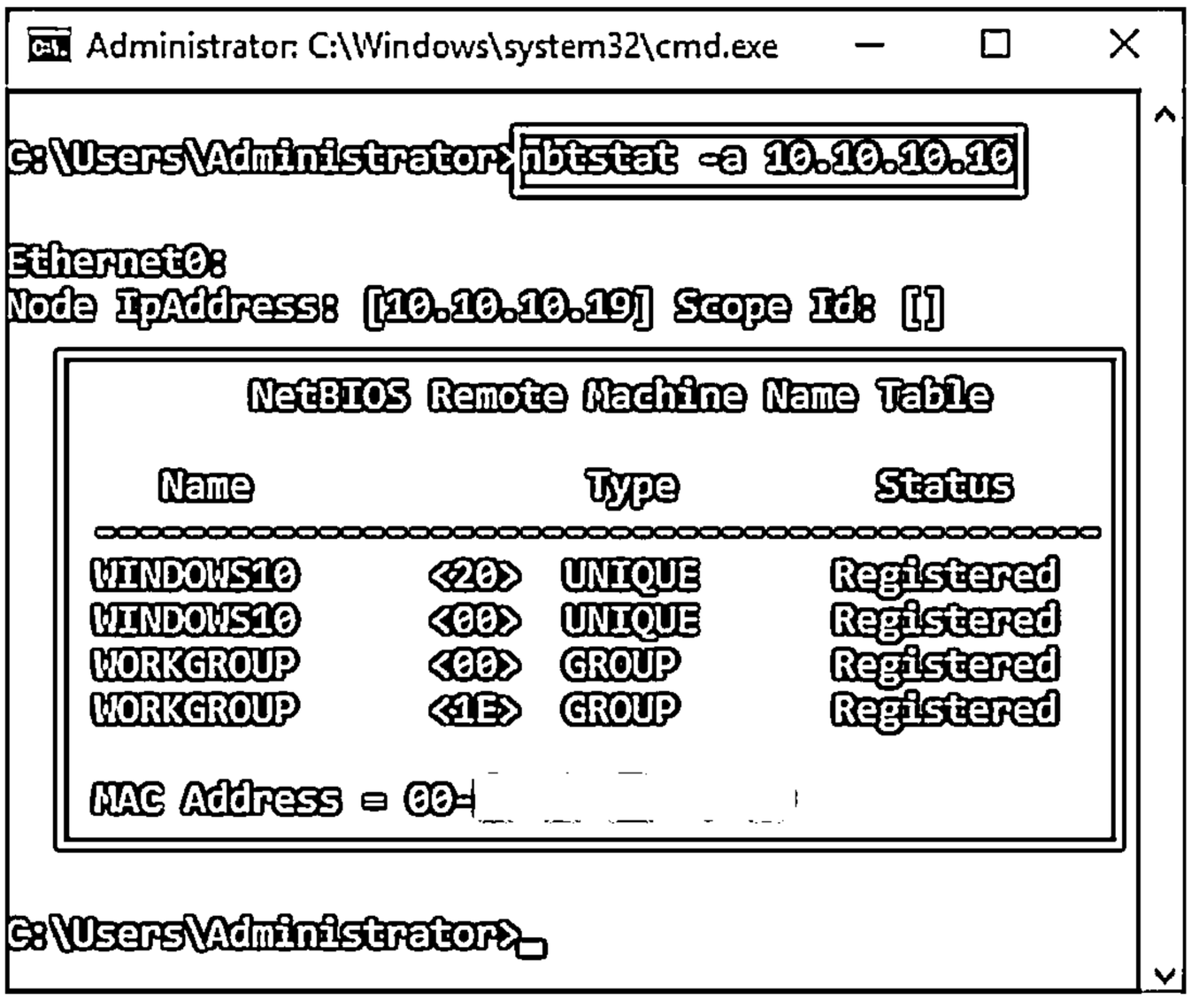


Figure 1.1.1: Nbtstat Remote Machine Name Table

TASK 1.2

View the Contents of the NetBIOS Name Cache

6. In the same **Command Prompt** window, type **nbtstat -c** and press **Enter**.

Note: In this command, **-c** lists the contents of the NetBIOS name cache of the remote computer.

7. The result appears, displaying the contents of the NetBIOS name cache, the table of NetBIOS names, and their resolved IP addresses.

Note: It is possible to extract this information without creating a **null session** (an unauthenticated session).

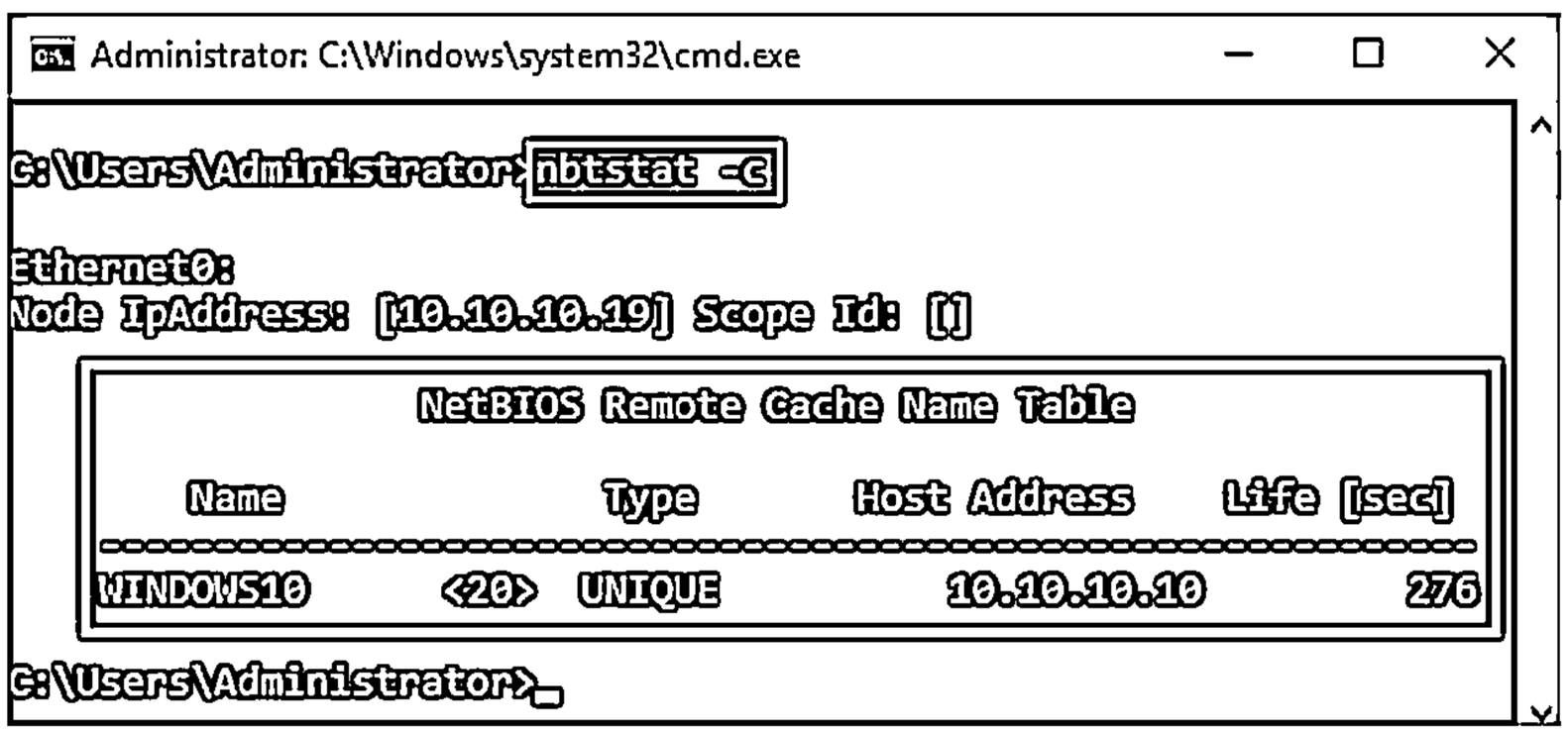


Figure 1.1.2: Nbtstat Remote Cache Name Table

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

8. Now, type **net use** and press **Enter.** The output displays information about the target such as connection status, shared folder/drive and network information, as shown in the screenshot.

TASK 1.3

View Shared Resources

Net use connects a computer to, or disconnects it from, a shared resource. It also displays information about computer connections.

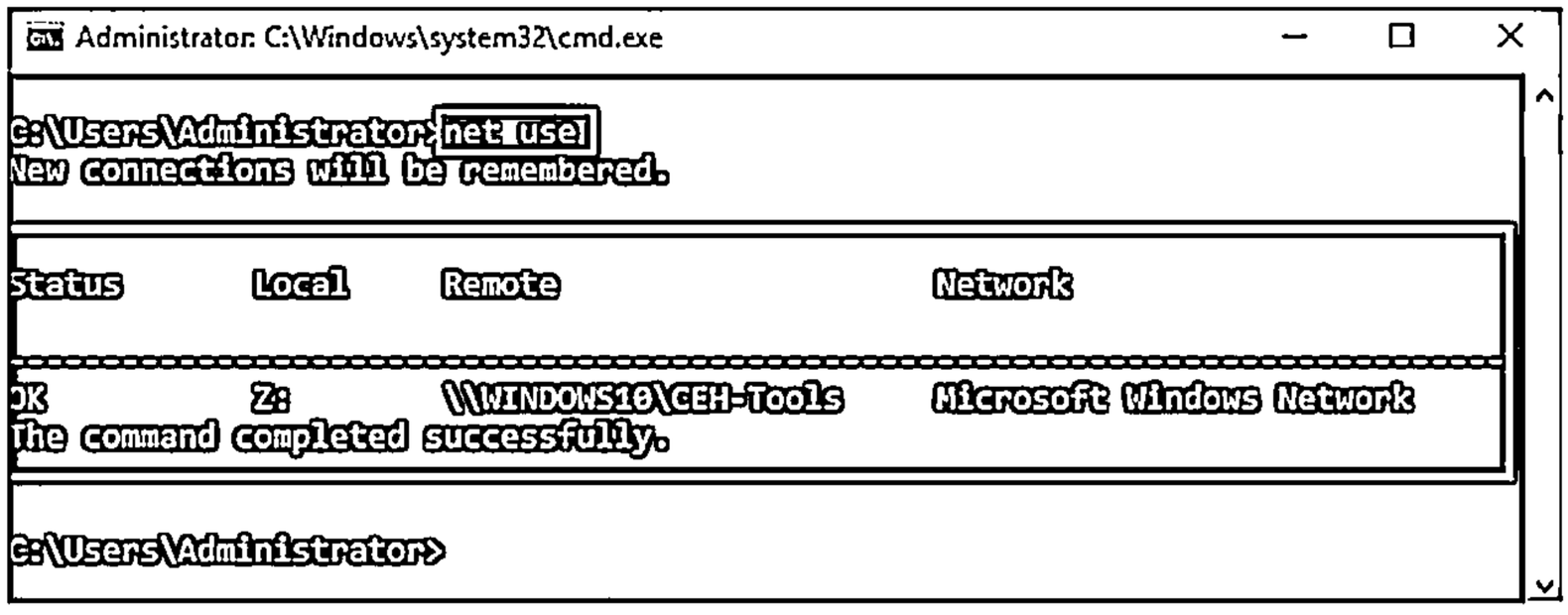


Figure 1.1.3: Nbtstat displaying shared folder

9. This concludes the demonstration of performing NetBIOS enumeration using Windows command-line utilities such as Nbtstat and Net use.
10. Close all open windows and document all the acquired information.

TASK 2 Perform NetBIOS Enumeration using NetBIOS Enumerator

Here, we will use the NetBIOS Enumerator to perform NetBIOS enumeration on the target network.

Note: We will use a **Windows 10** virtual machine to target **Windows Server 2016** and **Windows Server 2019** virtual machines.

TASK 2.1

Launch NetBIOS Enumerator

1. Before beginning this task, start the **Windows Server 2016** virtual machine. Ensure that the **Windows Server 2019** and **Windows 10** virtual machines are also running.
2. In the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 04 Enumeration\NetBIOS Enumeration Tools\NetBIOS Enumerator** and double-click **NetBIOS Enumerater.exe**.

Note: If the **Open - File Security Warning** pop-up appears, click **Run**.

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

NetBIOS Enumerator is a tool that enables the use of remote network support and several other techniques such as SMB (Server Message Block). It is used to enumerate details such as NetBIOS names, usernames, domain names, and MAC addresses for a given range of IP addresses.

3. The **NetBIOS Enumerator** main window appears, as shown in the screenshot.

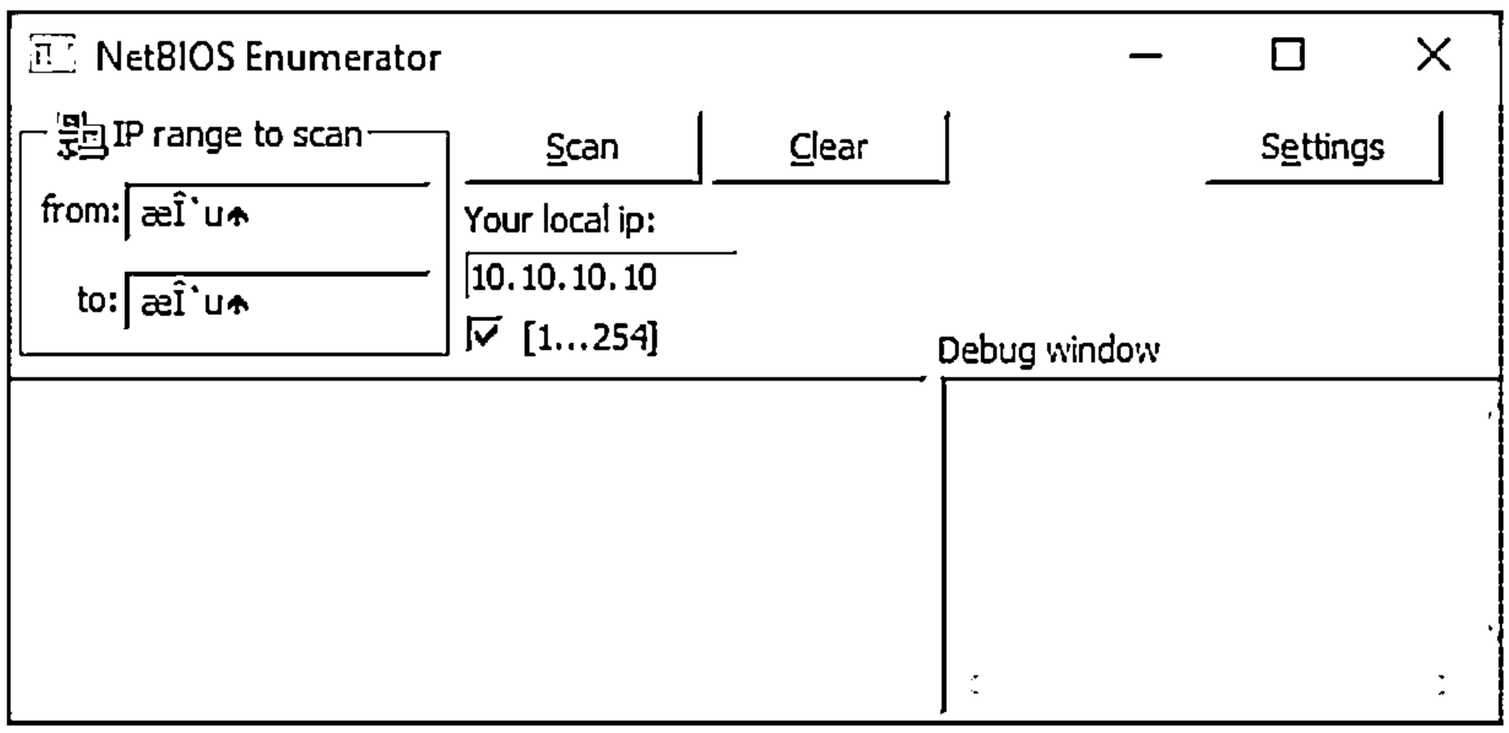


Figure 1.2.1: The NetBIOS Enumerator main window

TASK 2.2

Perform Scan

4. Under **IP range to scan**, enter an **IP range** in the **from** and **to** fields and click the **Scan** button to initiate the scan (In this example, we are targeting the IP range **10.10.10.15-10.10.10.20**).

Note: The IP range might differ in your lab environment.

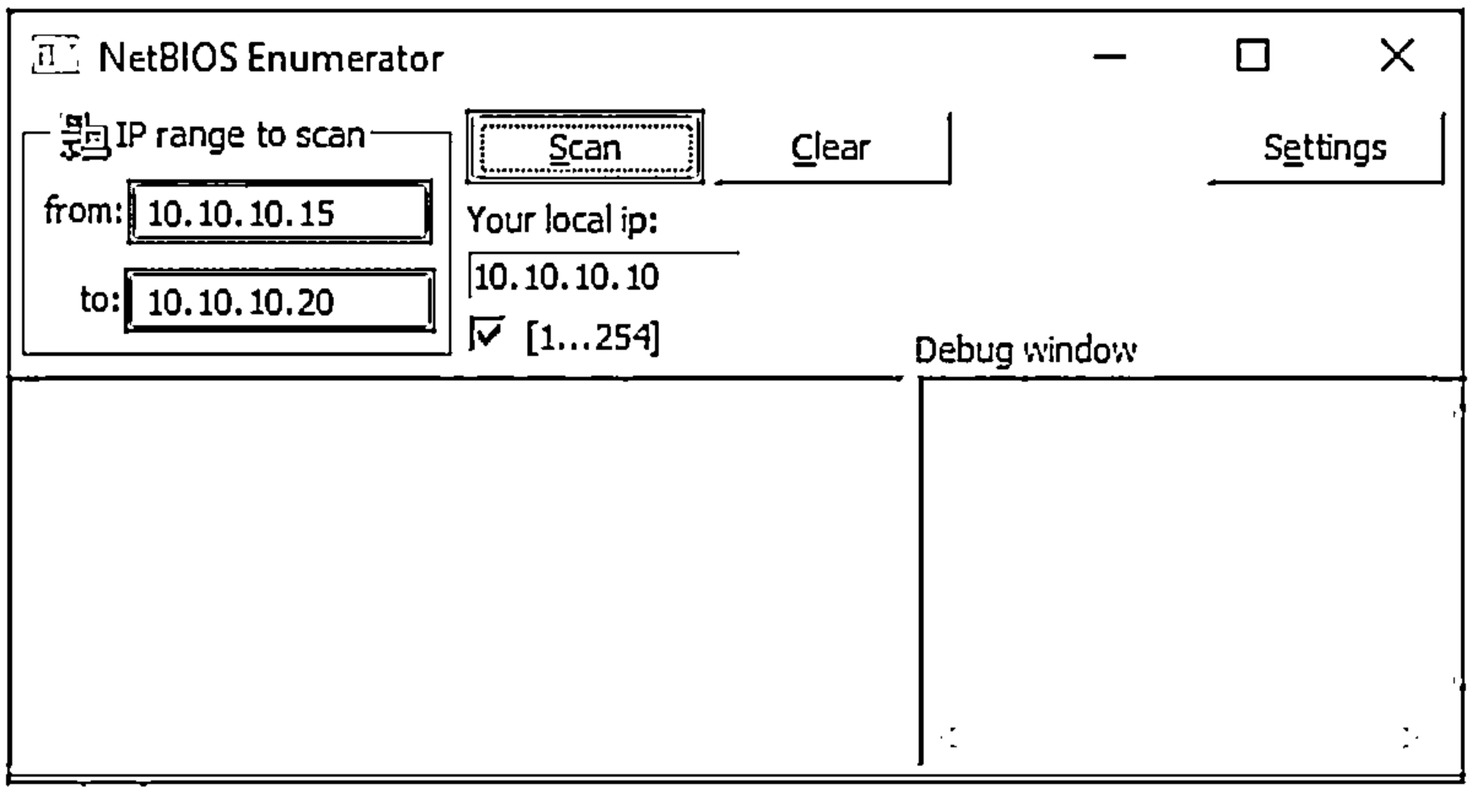


Figure 1.2.2: NetBIOS Enumerator with IP range to scan

5. NetBIOS Enumerator scans for the provided IP address range. On completion, the scan results are displayed in the left pane, as shown in the screenshot.

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

6. The **Debug window** section in the right pane shows the scanning range of IP addresses and displays **Ready!** after the scan is finished.

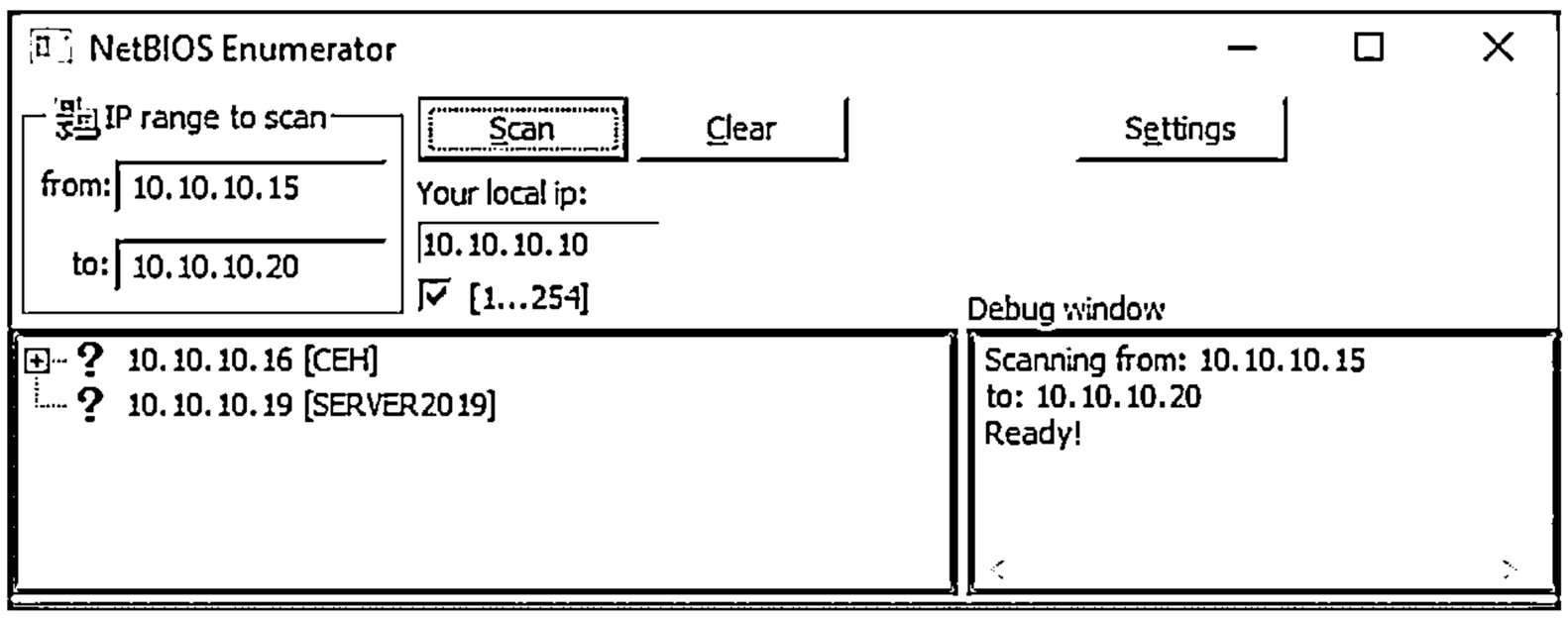


Figure 1.2.3: NetBIOS Enumerator results

Note: The scan result might differ in your lab environment.

TASK 2.3

Examine the Results

7. Click on the expand icon (+) to the left of the **10.10.10.16** and **10.10.10.19** IP addresses in the left pane of the window. Then click on the expand icon to the left of **NetBIOS Names** to display NetBIOS details of the target IP address, as shown in the screenshot.

Note: The result might differ in your lab environment.

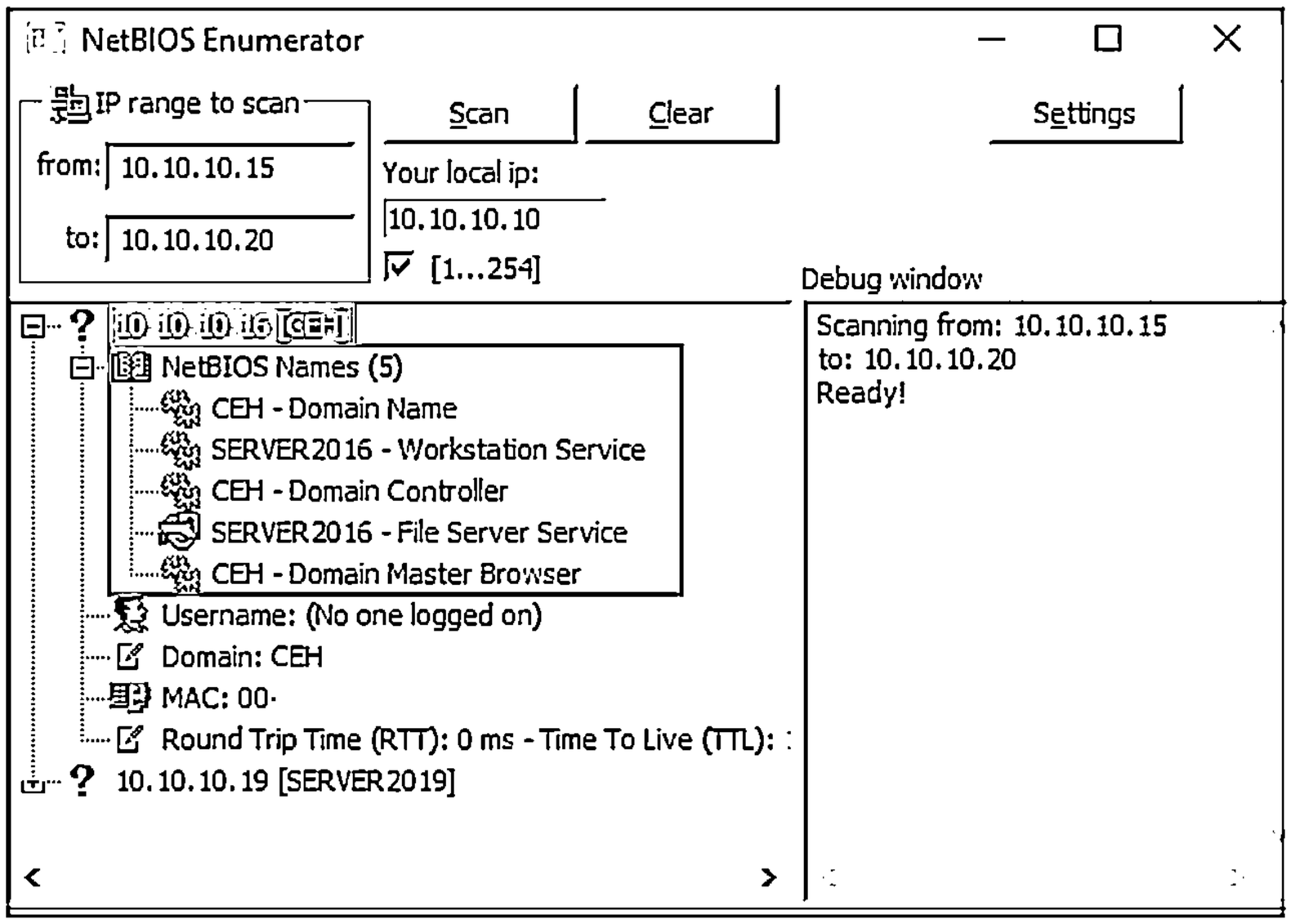


Figure 1.2.4: NetBIOS Enumerator NetBIOS Names section

8. This concludes the demonstration of performing NetBIOS enumeration using NetBIOS Enumerator. This enumerated NetBIOS information can be used to strategize an attack on the target.
9. Close all open windows and document all the acquired information.

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

Perform NetBIOS Enumeration using an NSE Script

TASK 3

Here, we will run the nbstat script to enumerate information such as the name of the computer and the logged-in user.

TASK 3.1

Launch Nmap - Zenmap GUI

1. In the **Windows 10** virtual machine, click on the **Start** button on the left-bottom corner of **Desktop** and launch **Nmap - Zenmap GUI** from the applications, as shown in the screenshot.

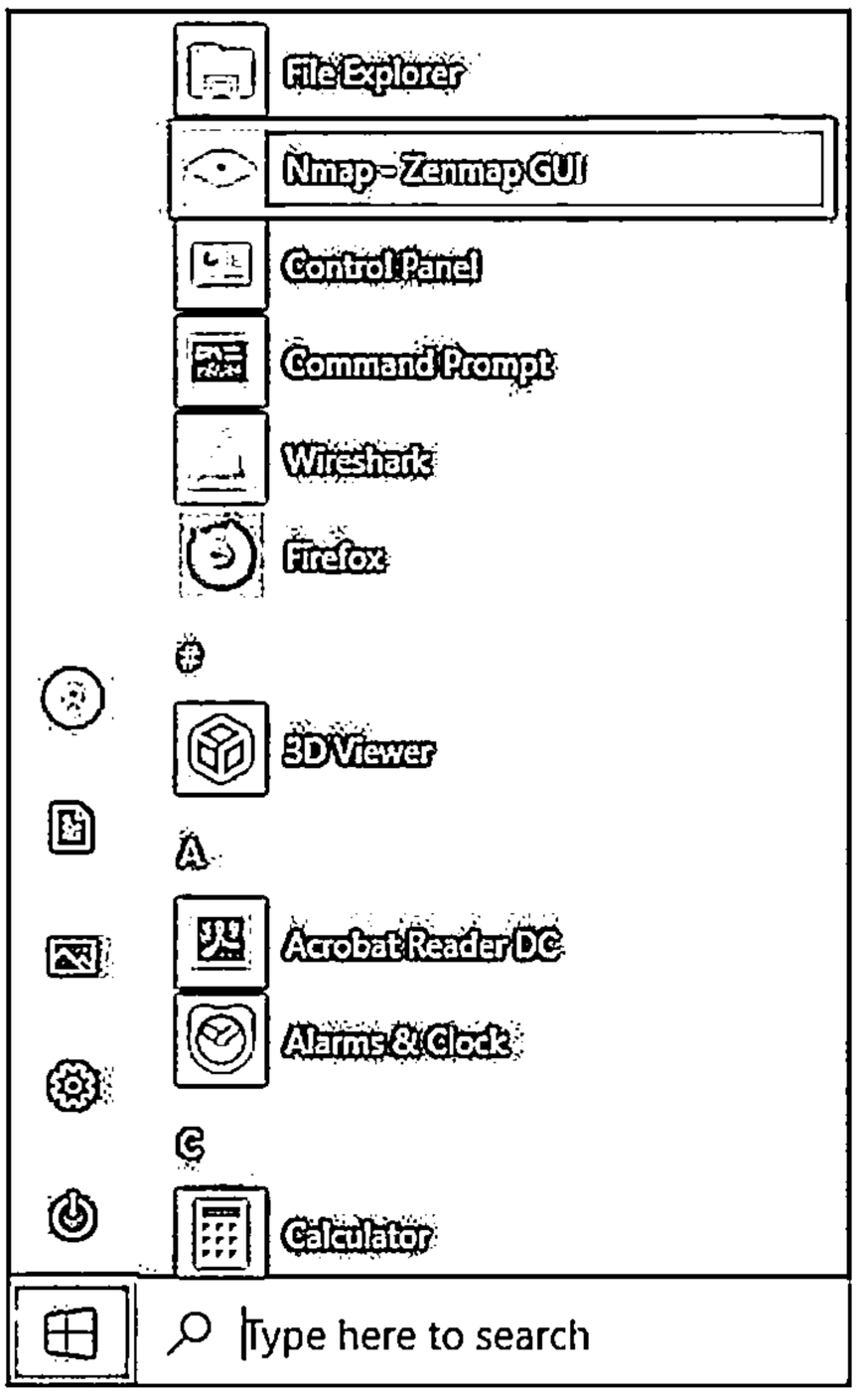


Figure 1.3.1: Launch Nmap: Zenmap

TASK 3.2

Enumeration using Stealth Scan

2. The **Zenmap** window appears. In the **Command** field, type the command **nmap -sV -v --script nbstat.nse <Target IP Address>** (in this example, the target IP address is **10.10.10.16**) and click **Scan**.

Note: **-sV** detects the service versions, **-v** enables the verbose output (that is, includes all hosts and ports in the output), and **--script nbtstat.nse** performs the NetBIOS enumeration.

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

3. The scan results appear, displaying the open ports and services, along with their versions. Displayed under the **Host script results** section are details about the target system such as the NetBIOS name, NetBIOS user, and NetBIOS MAC address, as shown in the screenshot.

NSE allows users to write (and share) simple scripts to automate a wide variety of networking tasks. NSE scripts can be used for discovering NetBIOS shares on the network. Using the nbstat NSE script, for example, you can retrieve the target's NetBIOS names and MAC addresses. Moreover, increasing verbosity allows you to extract all names related to the system.

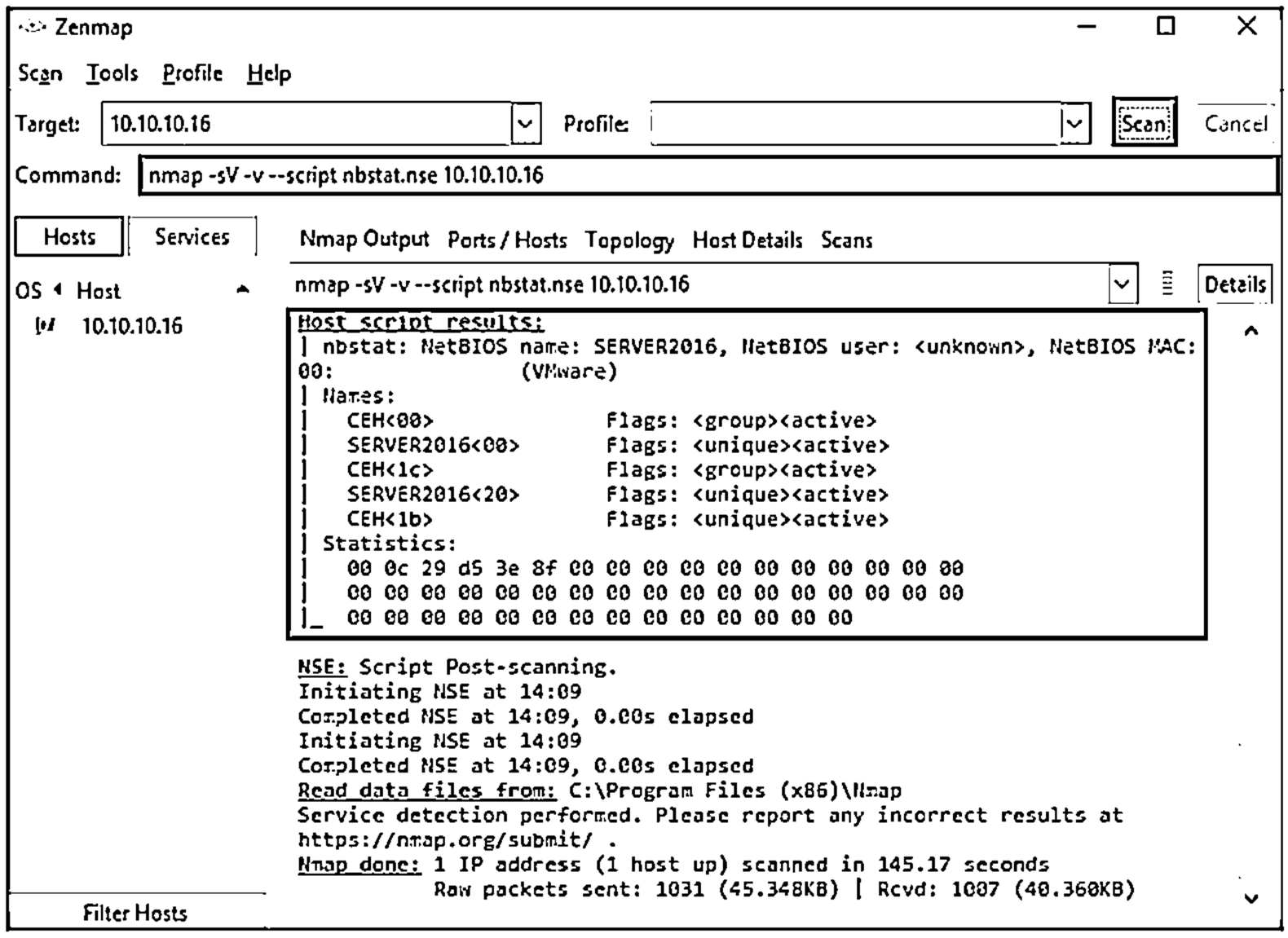


Figure 1.3.2: The Stealth scan output using Zenmap

TASK 3.3

Enumeration using UDP Scan

4. In the **Command** field of **Zenmap**, type **nmap -sU -p 137 -script nbstat.nse <Target IP Address>** (in this case, the target IP address is **10.10.10.16**) and click **Scan**.

Note: **-sU** performs a UDP scan, **-p** specifies the port to be scanned, and **--script nbtstat.nse** performs the NetBIOS enumeration.

5. The scan results appear, displaying the open NetBIOS port (137) and, under the **Host script results** section, NetBIOS details such as NetBIOS name, NetBIOS user, and NetBIOS MAC of the target system, as shown in the screenshot.

Other tools may also be used to perform NetBIOS enumeration on the target network such as **Global Network Inventory** (http://www.magnetosoft.com), **Advanced IP Scanner** (http://www.advanced-ip-scanner.com), **Hyena** (https://www.systemtools.com), and **Nsauditor Network Security Auditor** (https://www.nsauditor.com).

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

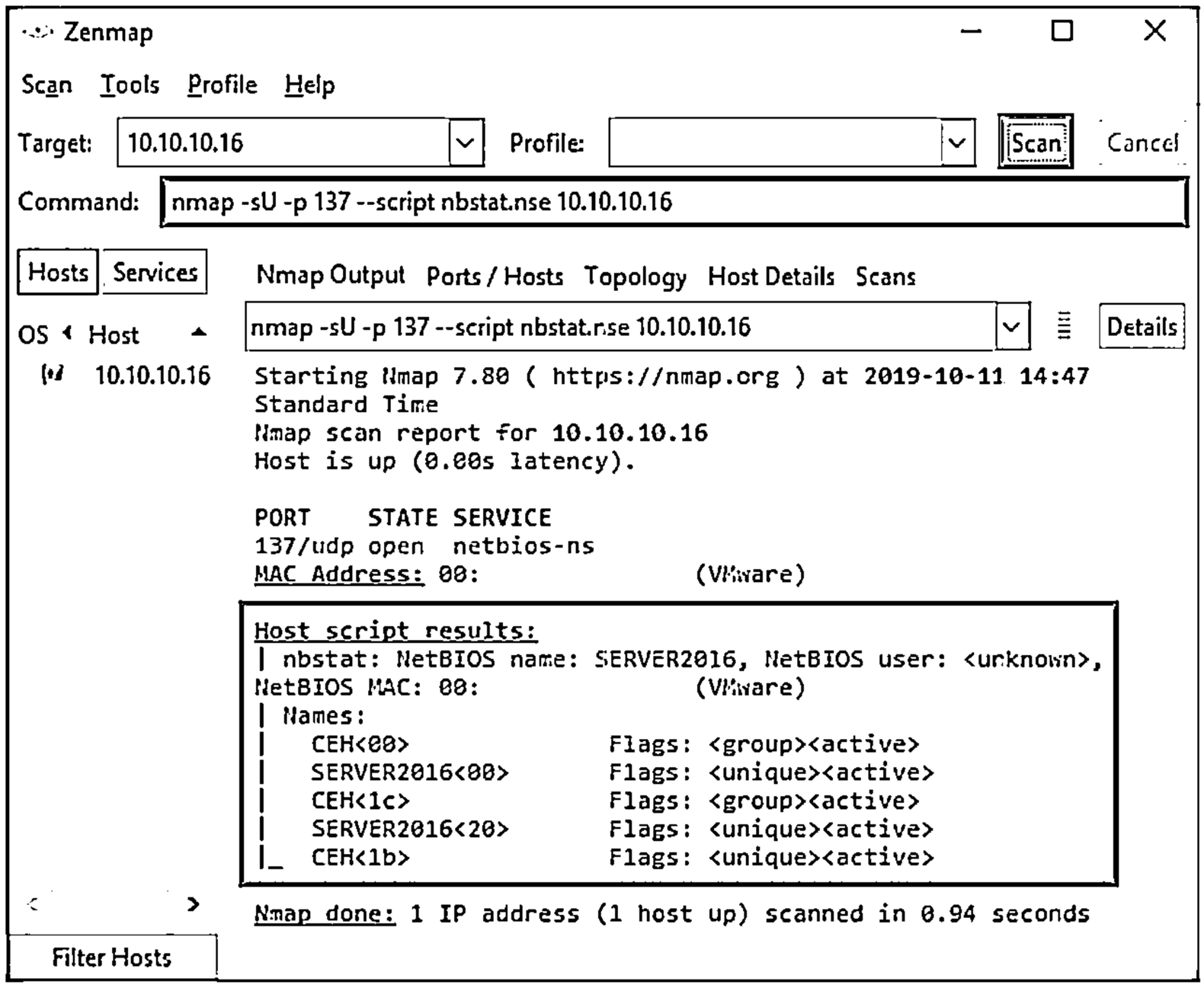


Figure 1.3.3: The UDP scan output using Zenmap

6. This concludes the demonstration of performing NetBIOS enumeration using an NSE script.
7. Close all open windows and document all the acquired information.
8. Turn off the **Windows 10, Windows Server 2019** and **Windows Server 2016** virtual machines.

Lab Analysis

Analyze and document the results related to this lab exercise. Provide your opinion on your target's security posture and exposure.

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

Perform SNMP Enumeration

SNMP enumeration uses SNMP to obtain a list of user accounts and devices on a target system.

ICON KEY

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

Lab Scenario

As a professional ethical hacker or penetration tester, your next step is to carry out SNMP enumeration to extract information about network resources (such as hosts, routers, devices, and shares) and network information (such as ARP tables, routing tables, device-specific information, and traffic statistics).

Using this information, you can further scan the target for underlying vulnerabilities, build a hacking strategy, and launch attacks.

Lab Objectives

- Perform SNMP enumeration using snmp-check
- Perform SNMP enumeration using SoftPerfect Network Scanner

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 04 Enumeration

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2016 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Ubuntu virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- SoftPerfect Network Scanner located at **Z:\CEHv11 Module 04 Enumeration\SNMP Enumeration Tools\SoftPerfect Network Scanner**
- You may also download the latest version of SoftPerfect Network Scanner from its official website. If you do so, the 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 SNMP Enumeration

SNMP (Simple Network Management Protocol) is an application layer protocol that runs on UDP (User Datagram Protocol) and maintains and manages routers, hubs, and switches on an IP network. SNMP agents run on networking devices on Windows and UNIX networks. WSS

SNMP enumeration uses SNMP to create a list of the user accounts and devices on a target computer. SNMP employs two types of software components for communication: the SNMP agent and SNMP management station. The SNMP agent is located on the networking device, and the SNMP management station communicates with the agent.

Lab Tasks

TASK 1

Perform SNMP Enumeration using snmp-check

snmp-check is a tool that enumerates SNMP devices, displaying the output in a simple and reader-friendly format. The default community used is "public." As an ethical hacker or penetration tester, it is imperative that you find the default community strings for the target device and patch them up.

Here, we will use the snmp-check tool to perform SNMP enumeration on the target IP address.

Note: We will use a **Parrot Security** (10.10.10.13) virtual machine to target a **Windows Server 2016** (10.10.10.16) virtual machine.

1. Start the **Parrot Security** and **Windows Server 2016** virtual machines.
2. Switch to the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

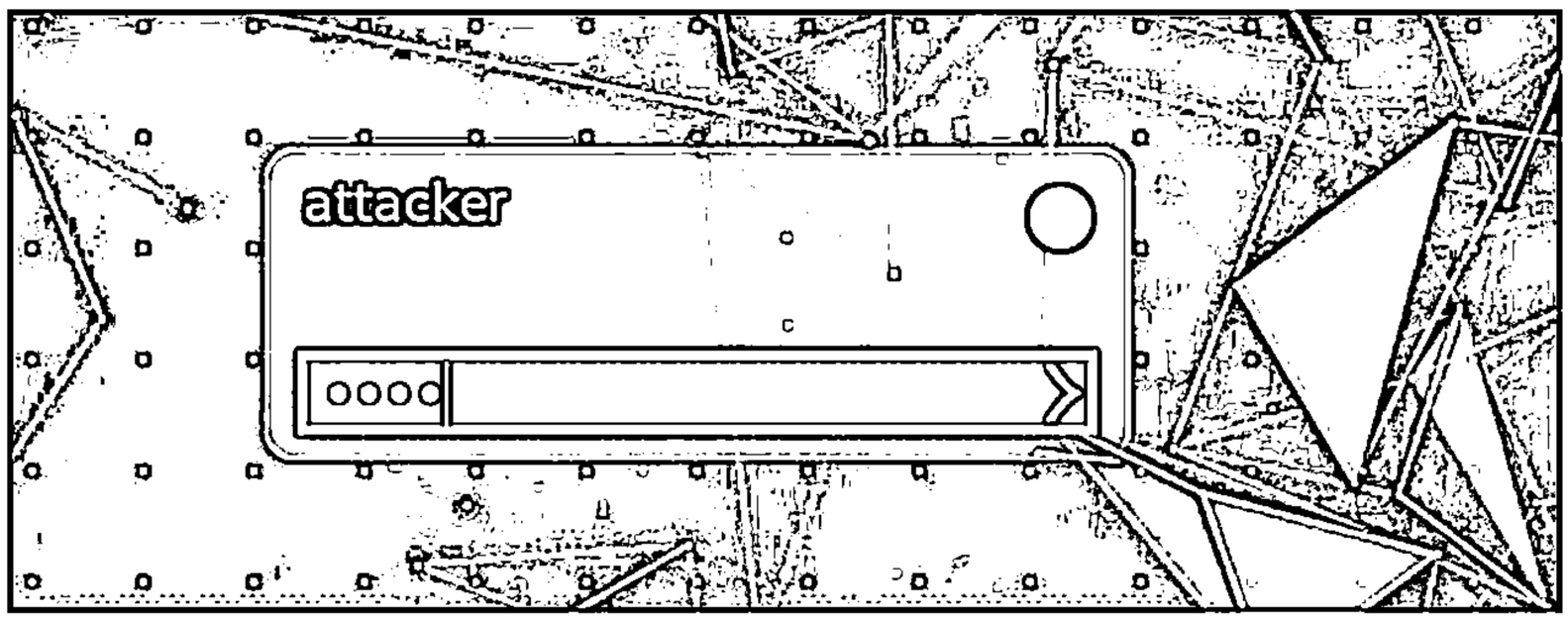


Figure 2.1.1: Parrot Security login page

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

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

3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

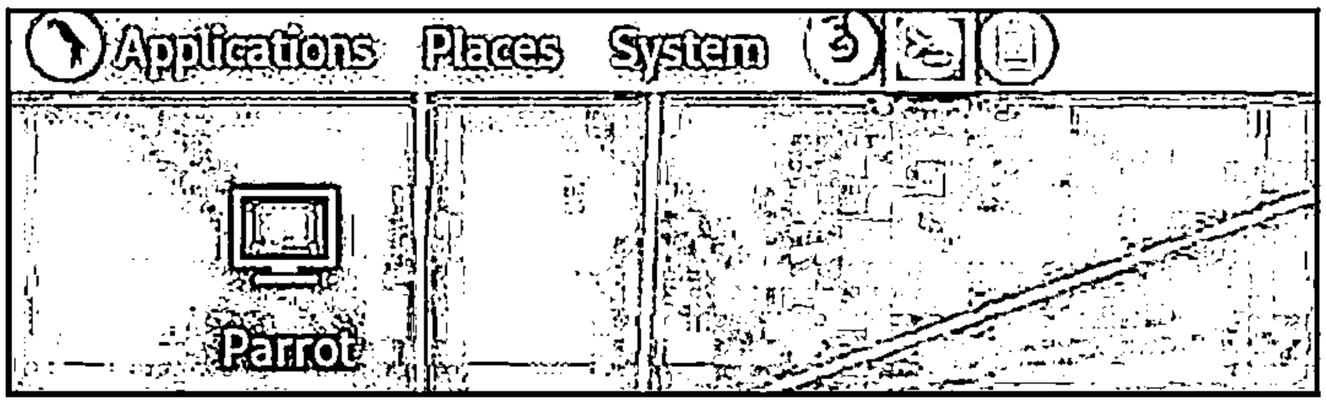


Figure 2.1.2: MATE Terminal Icon

4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

6. Now, type **cd** and press **Enter** to jump to the root directory.

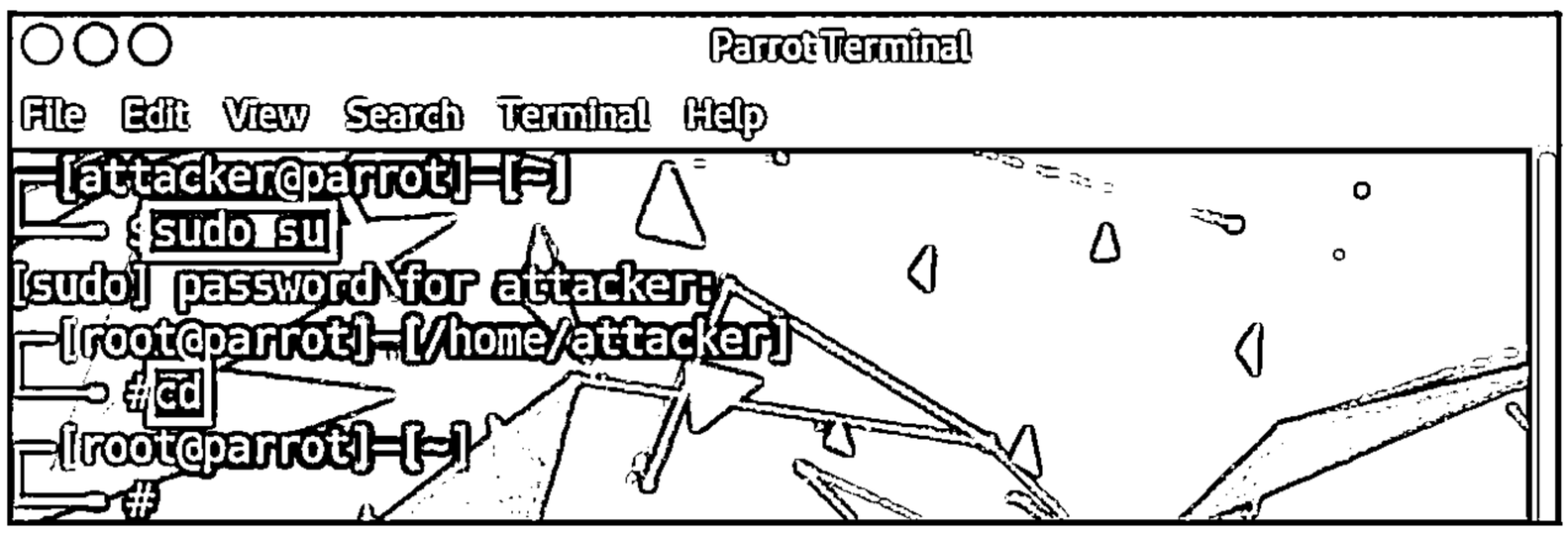


Figure 2.1.3: Running the programs as a root user

Note: Before starting SNMP enumeration, we must first discover whether the SNMP port is open. SNMP uses port 161 by default; to check whether this port is opened, we will first run Nmap port scan.

TASK 1.1

Check the SNMP Port Status

7. In the **Parrot Terminal** window, type **nmap -sU -p 161 <Target IP address>** (in this example, the target IP address is **10.10.10.16**) and press **Enter.**

Note: **-sU** performs a UDP scan and **-p** specifies the port to be scanned.

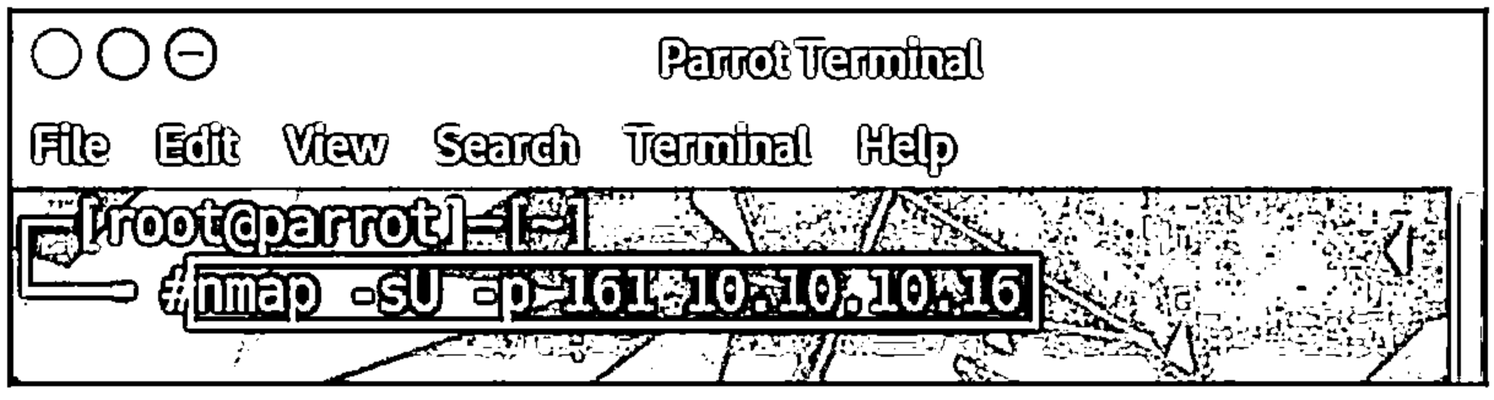


Figure 2.1.4: Performing the Nmap UDP scan

8. The results appear, displaying that port 161 is **open/filtered** and being used by SNMP, as shown in the screenshot.

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

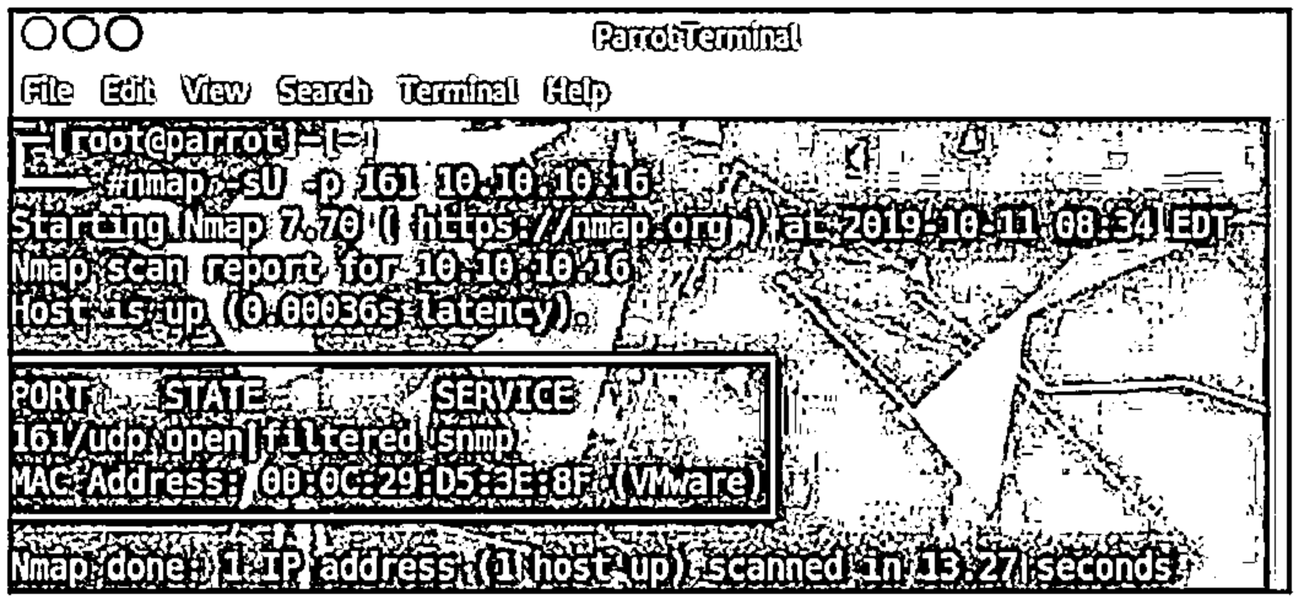


Figure 2.1.5: Nmap UDP scan result

TASK 1.2

Perform SNMP Enumeration

9. We have established that the SNMP service is running on the target machine. Now, we shall exploit it to obtain information about the target system.
10. In the **Parrot Terminal** window, type **snmp-check <Target IP Address>** (in this example, the target IP address is **10.10.10.16**) and press **Enter**.
11. The result appears as shown in the screenshot. It reveals that the extracted SNMP port 161 is being used by the default "public" community string.

Note: If the target machine does not have a valid account, no output will be displayed.

12. The snmp-check command enumerates the target machine, listing sensitive information such as **System information** and **User accounts**.

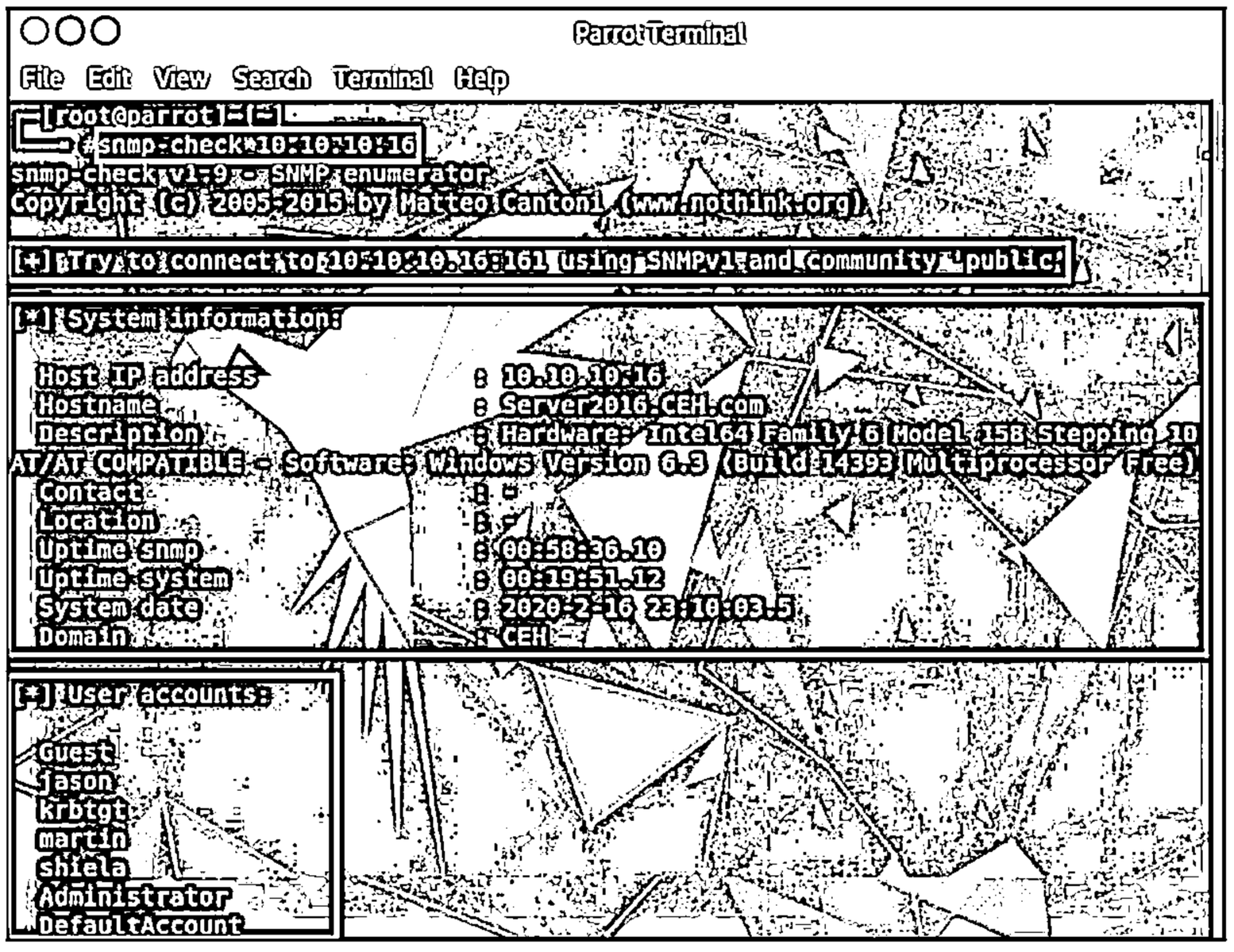


Figure 2.1.6: snmp-check reveals the SNMP community string

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

13. Scroll down to view detailed information regarding the target network under the following sections: **Network information, Network interfaces, Network IP** and **Routing information**, and **TCP connections and listening ports.**

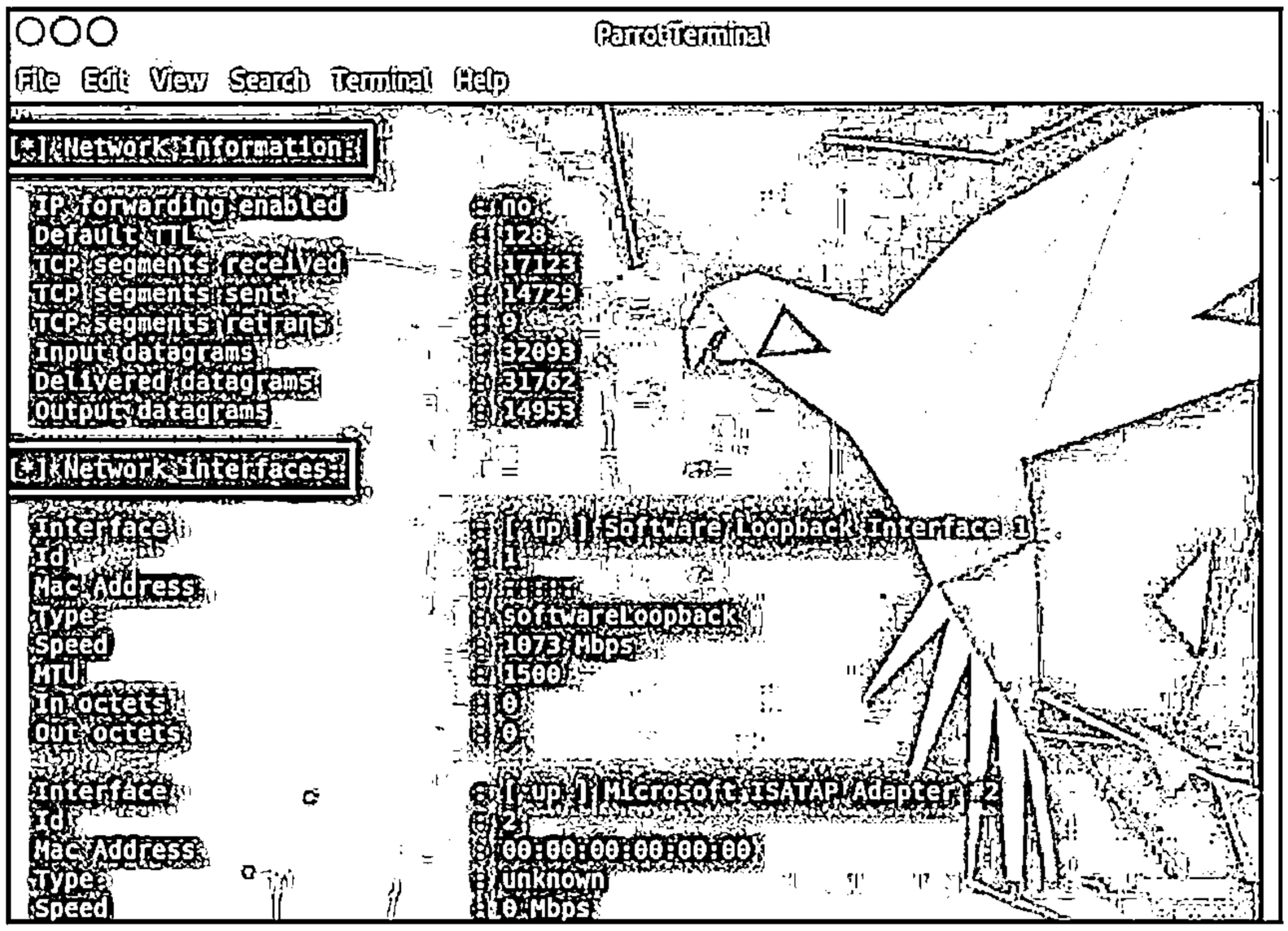


Figure 2.1.7: Details of network information and network interfaces

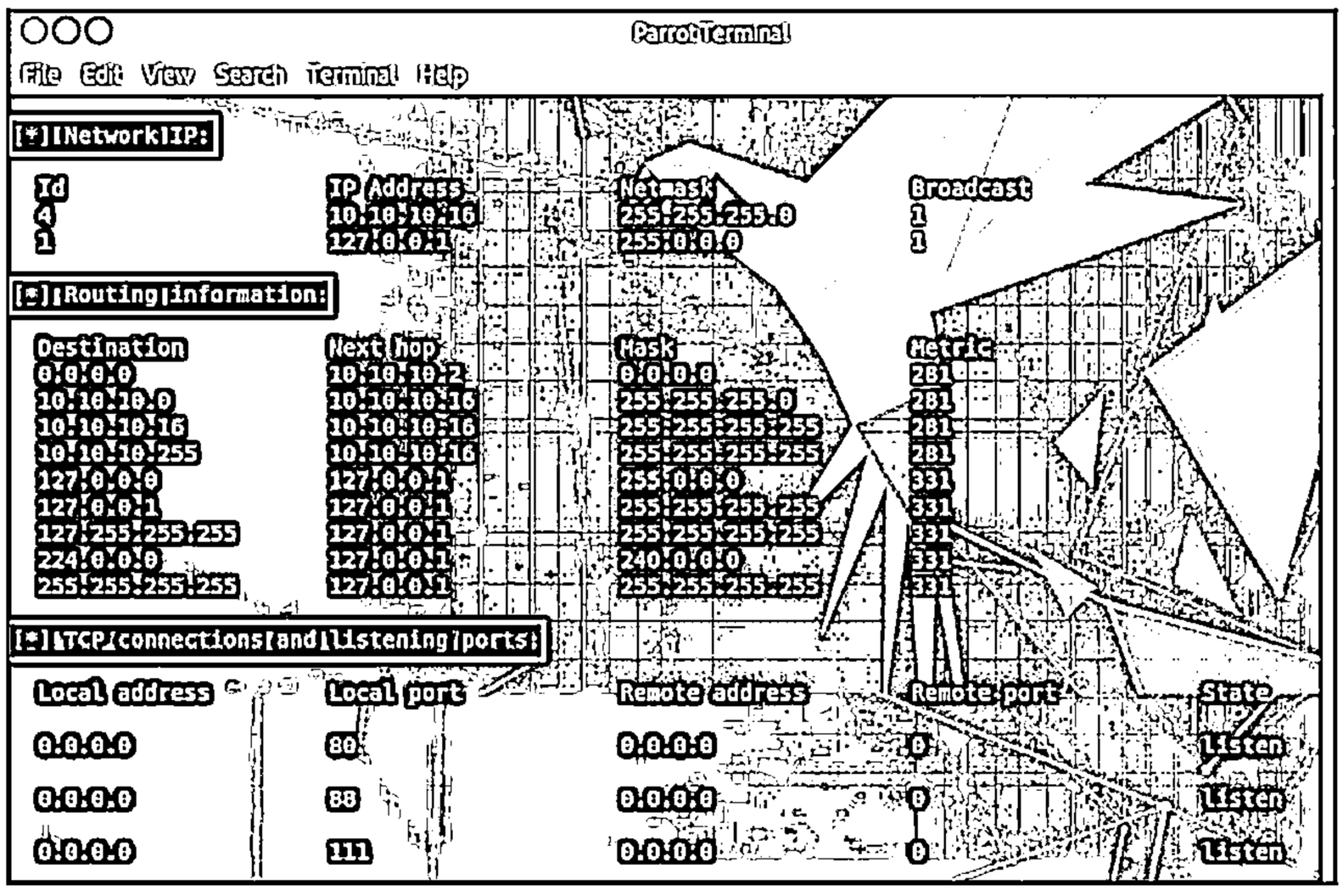


Figure 2.1.8: Details of network IP, routing information, and TCP connections and listening ports

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

14. Similarly, scrolling down reveals further sensitive information on **Processes, Storage information, File system information, Device information, Share**, etc.

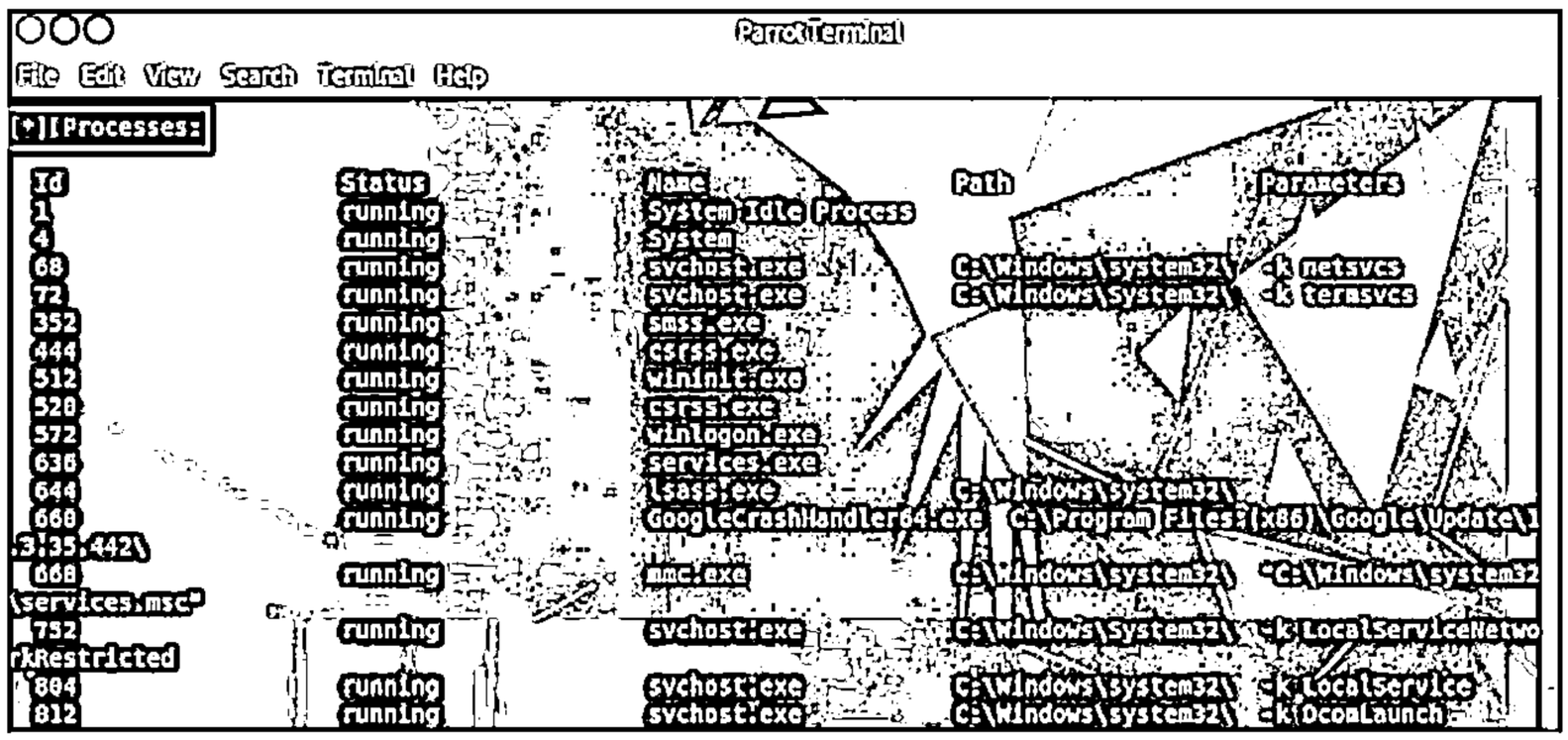


Figure 2.1.9: Details of running processes

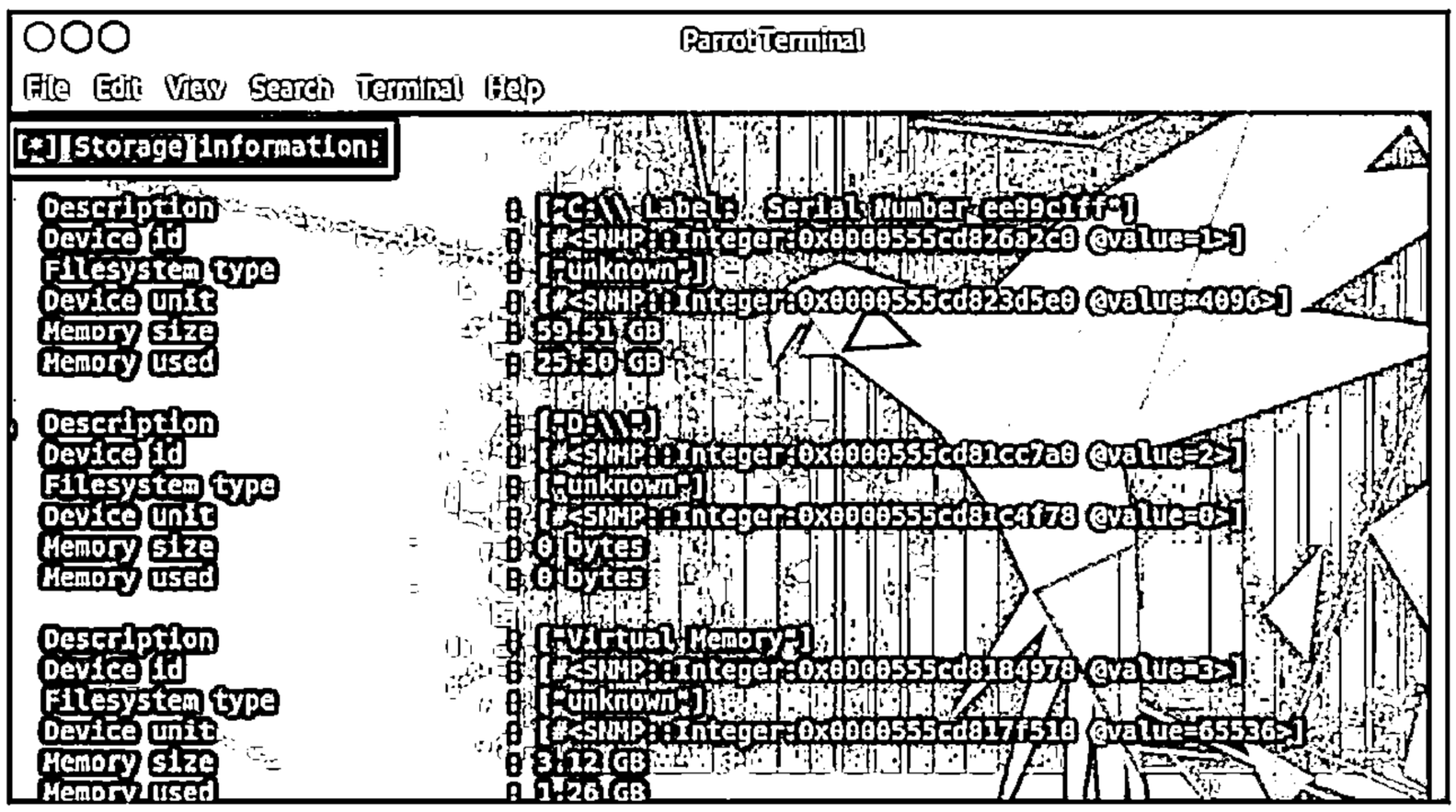


Figure 2.1.10: Details of storage information

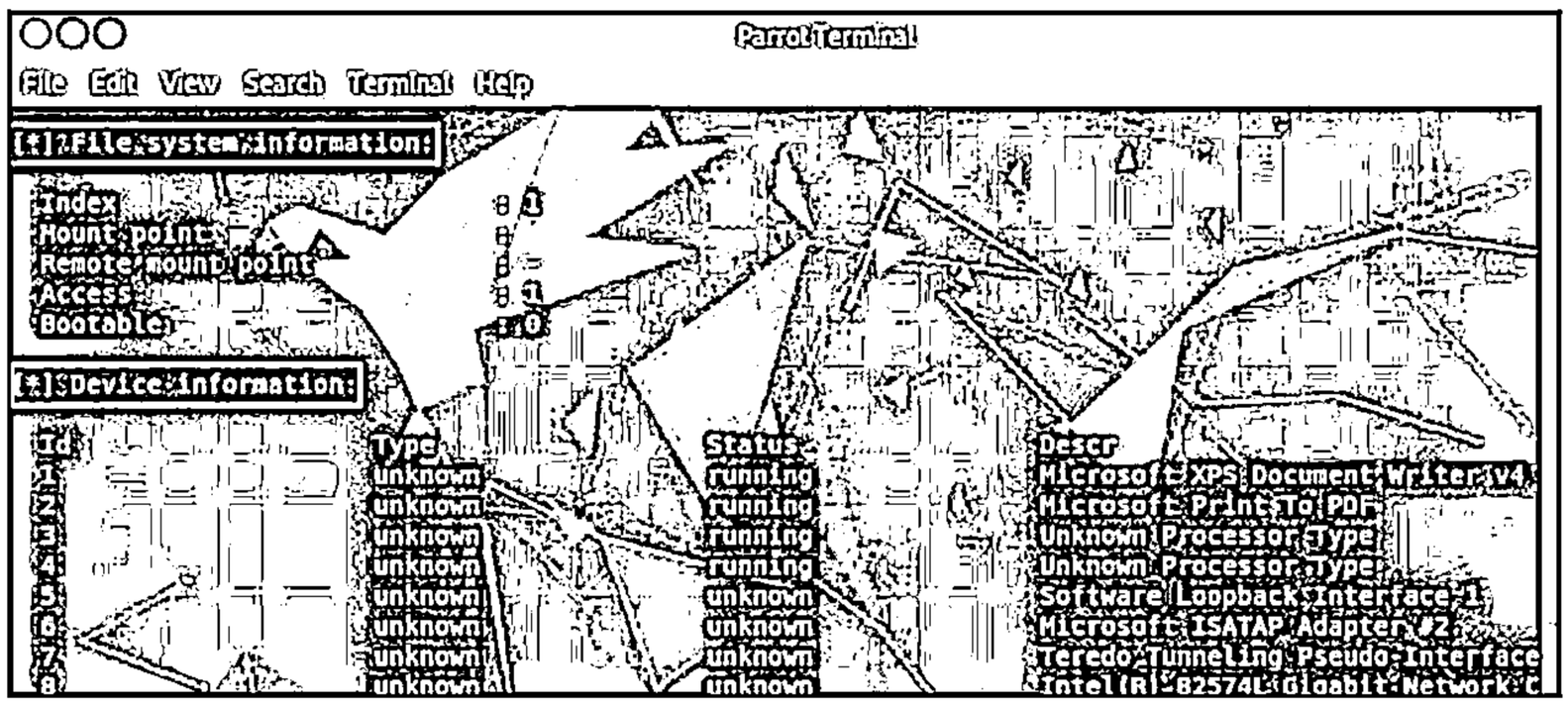


Figure 2.1.11: Details of file system and device information

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

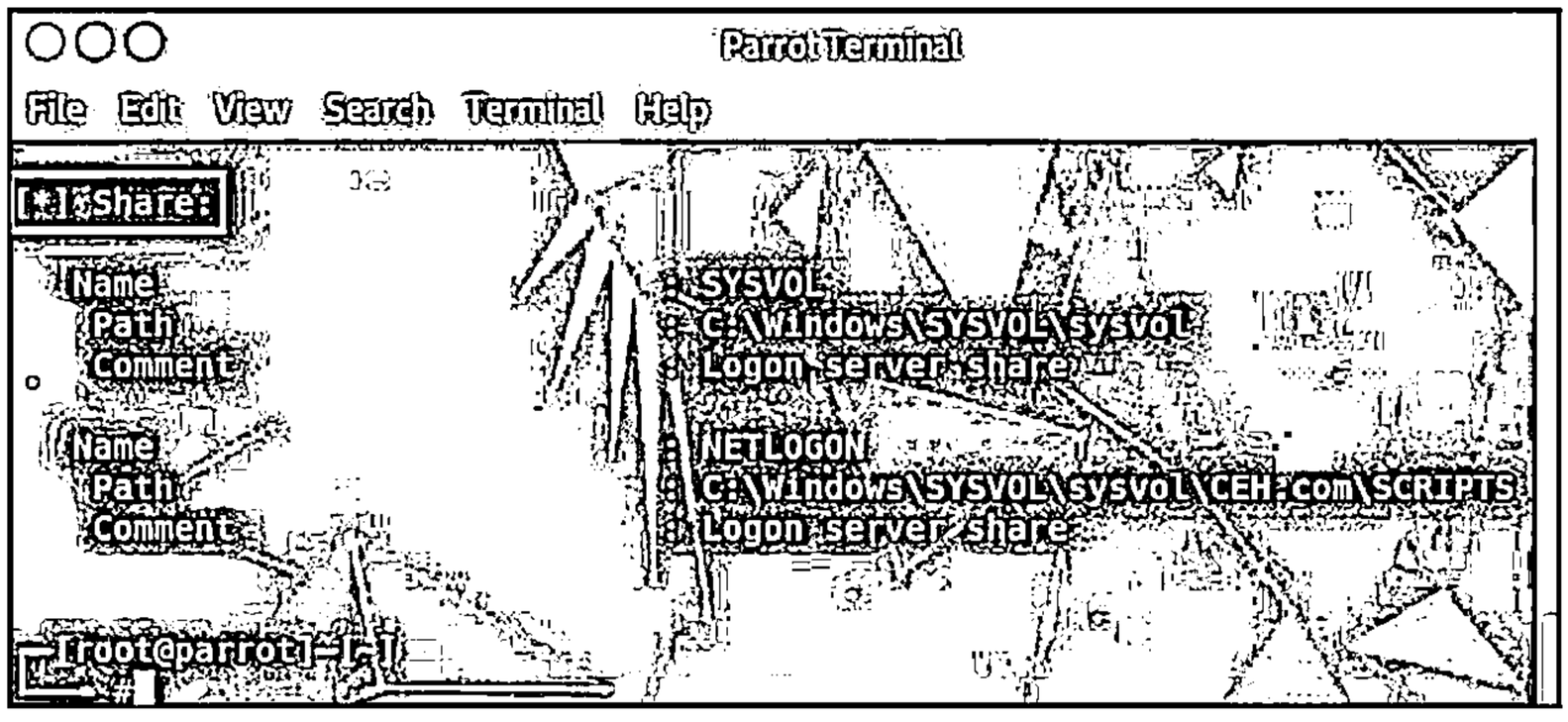


Figure 2.1.12: Details of shares

15. This concludes the demonstration of performing SNMP enumeration using the snmp-check.
16. Close all open windows and document all the acquired information.
17. Turn off the **Parrot Security** virtual machine.

Perform SNMP Enumeration using SoftPerfect Network Scanner

TASK 2

Here, we will use the SoftPerfect Network Scanner to perform SNMP enumeration on a target system.

TASK 2.1

Install SoftPerfect Network Scanner

1. Before beginning this task, start the **Windows Server 2019**, **Windows 10**, and **Ubuntu** virtual machines. Ensure that the **Windows Server 2016** virtual machine is running.
2. In the **Windows Server 2019** virtual machine, log in with the credentials **Administrator** and **Pa$$w0rd**.
3. Navigate to **Z:\CEHv11 Module 04 Enumeration\SNMP Enumeration Tools\SoftPerfect Network Scanner** and double-click **netscan_setup.exe**.

Note: If a **User Account Control** pop-up appears, click **Yes**.

4. When the **Setup - SoftPerfect Network Scanner** window appears, click **Next** and follow the installation steps to install SoftPerfect Network Scanner, using all default settings.

SoftPerfect Network Scanner can ping computers, scan ports, discover shared folders, and retrieve practically any information about network devices via WMI (Windows Management Instrumentation), SNMP, HTTP, SSH, and PowerShell.

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

The program also scans for remote services, registries, files, and performance counters. It can check for a user-defined port and report if one is open, and is able to resolve hostnames as well as auto-detect your local and external IP range. SoftPerfect Network Scanner offers flexible filtering and display options, and can export the NetScan results to a variety of formats, from XML to JSON. In addition, it supports remote shutdown and Wake-On-LAN.

5. On completion of the installation, click **Finish**.

Note: Ensure that the **Launch SoftPerfect Network Scanner** option is selected.

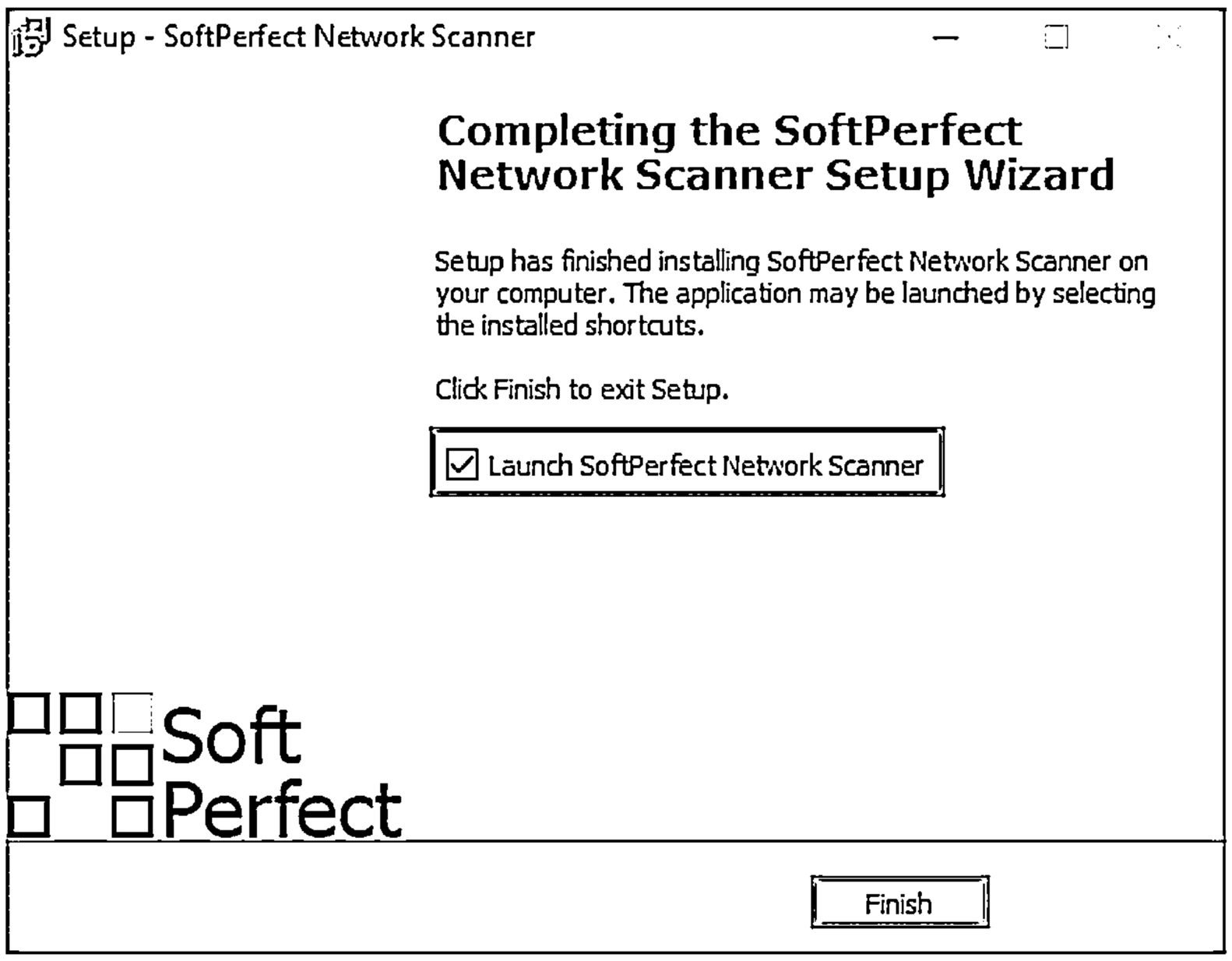


Figure 2.2.1: Network Scanner installation dialog-box

6. When the **Welcome to the Network Scanner** wizard appears, click **Continue.**

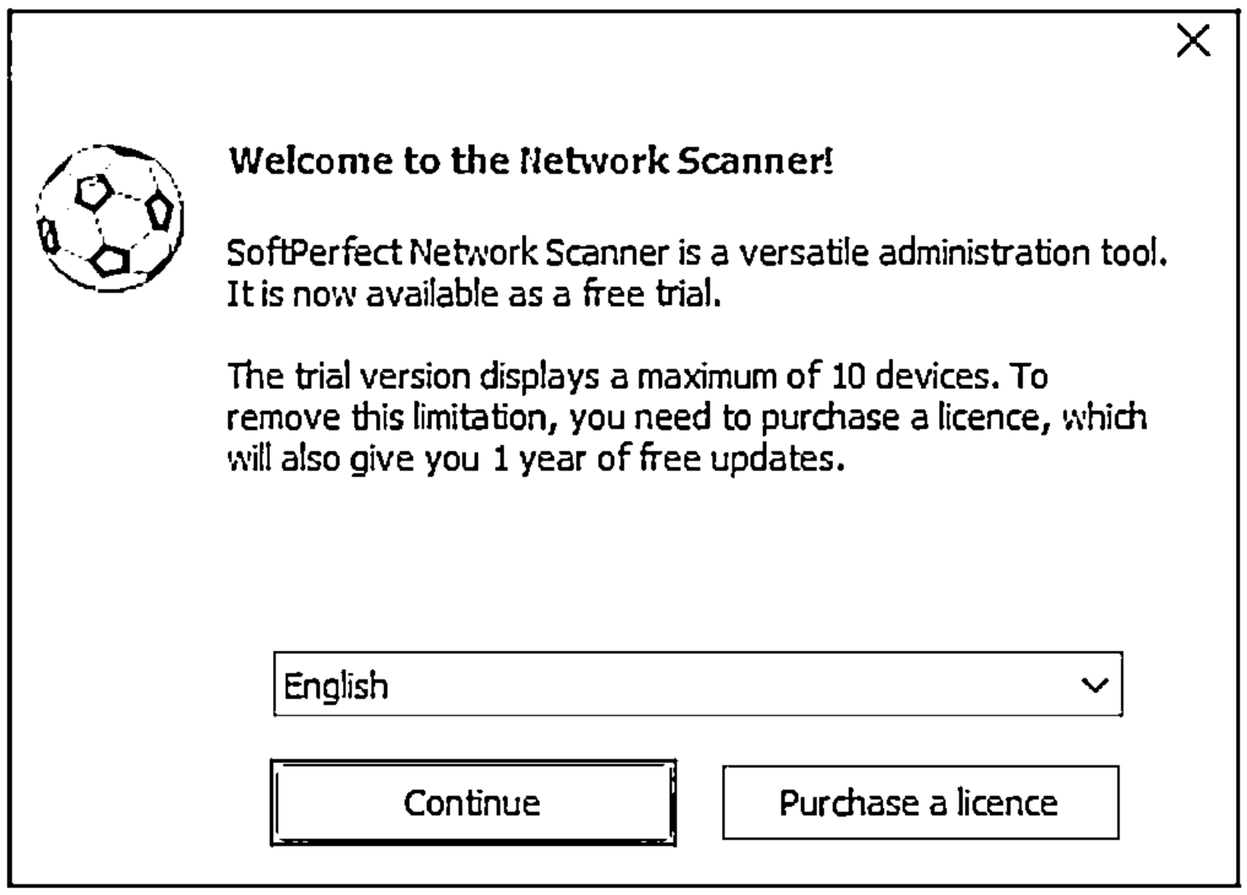


Figure 2.2.2: Network Scanner dialog-box

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

TASK 2.2

Perform SNMP Enumeration

7. The **SoftPerfect Network Scanner** GUI window will appear, as shown in the screenshot.

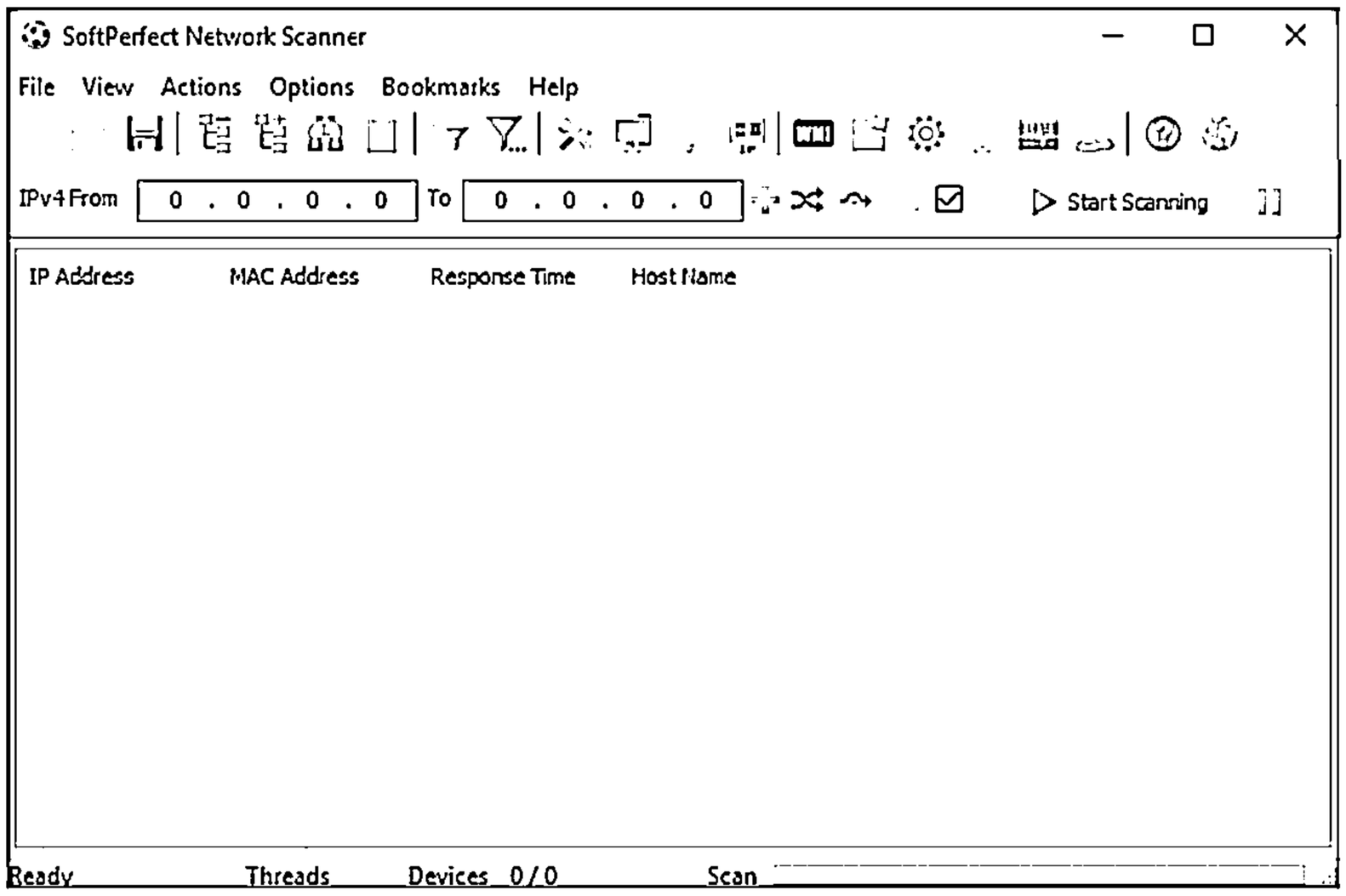


Figure 2.2.3: SoftPerfect Network Scanner main window

8. In the **Options** menu, click **Remote SNMP...**. The **SNMP** pop-up window will appear.
9. Click the **Mark All/None** button to select all the items available for SNMP scanning and close the window.

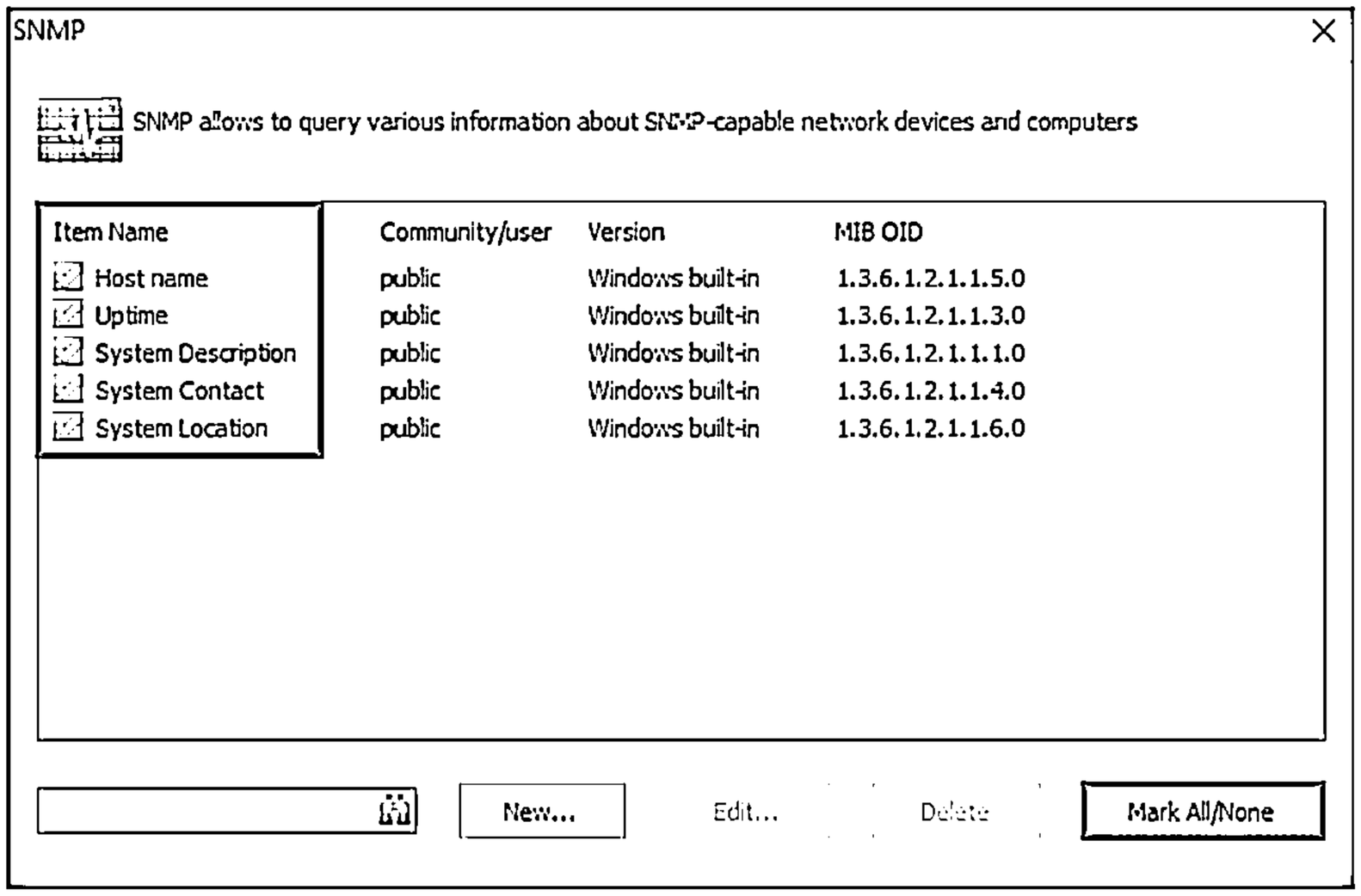


Figure 2.2.4: SoftPerfect Network Scanner, showing the SNMP setting

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

10. To scan your network, enter an IP range in the **IPv4 From** and **To** fields (in this example, the target IP address range is **10.10.10.5-10.10.10.20**), and click the **Start Scanning** button.

Note: The IP range might differ in your lab environment.

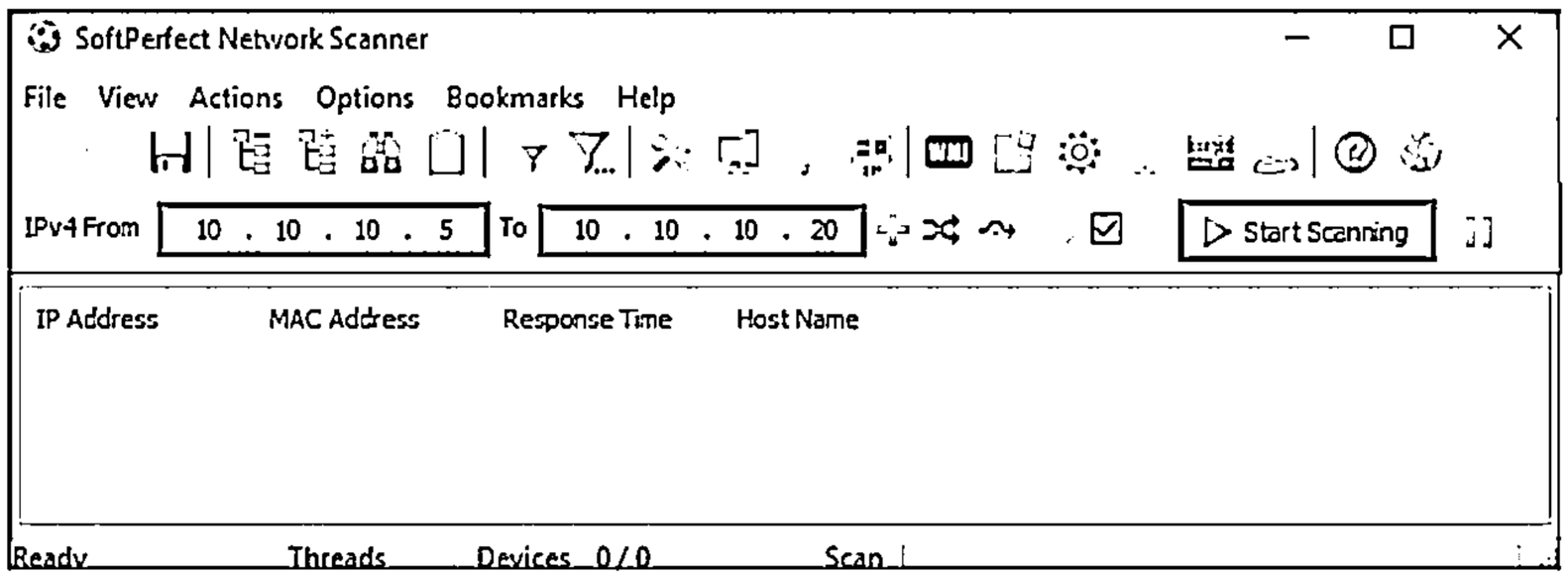


Figure 2.2.5: Setting an IP range to scan

TASK 2.3

Examine the Enumerated Results

11. The **status bar** at the lower-right corner of the GUI displays the status of the scan.
12. The scan results appear, displaying the active hosts in the target IP address range, as shown in the screenshot.

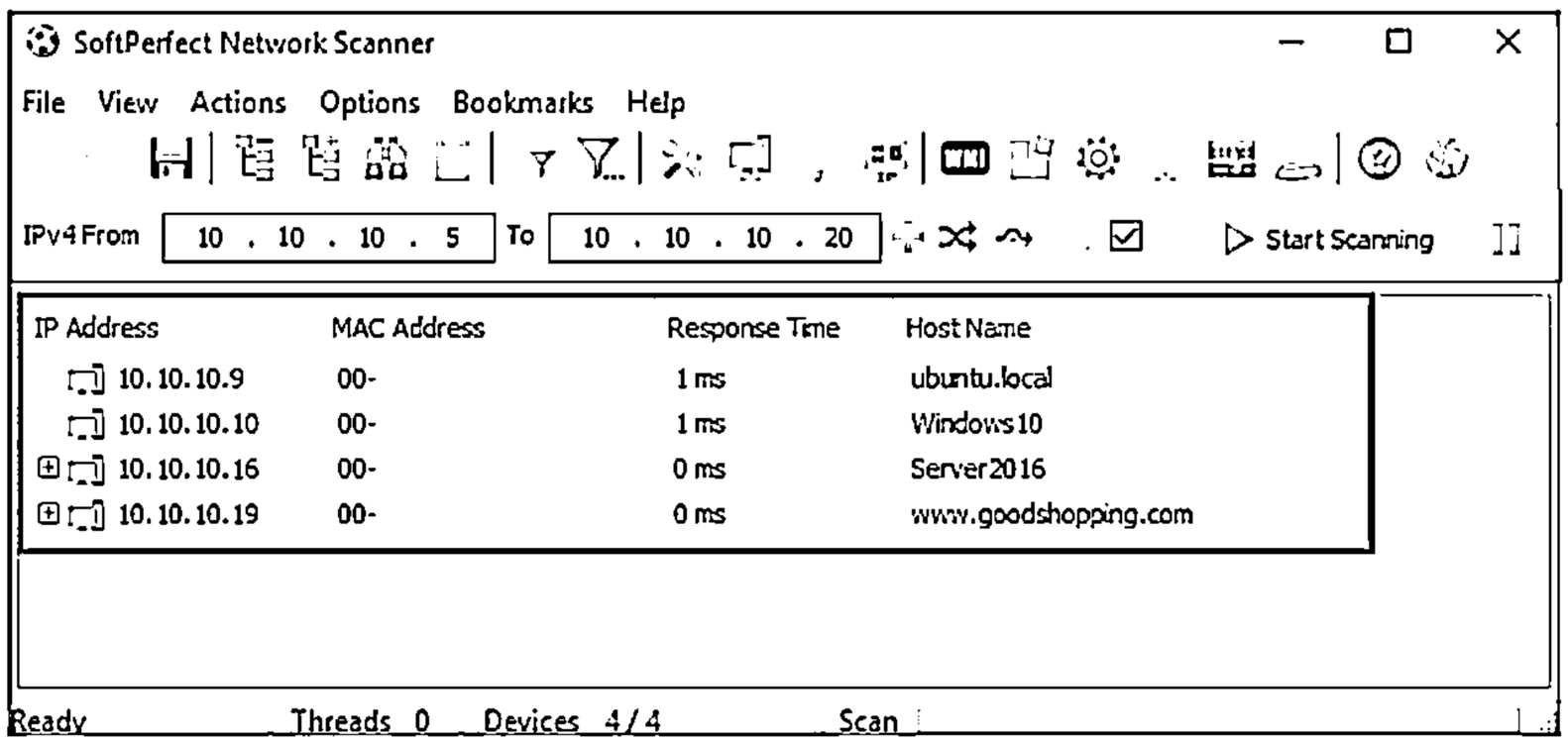


Figure 2.2.6: Scan results show active hosts in the target IP range

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

13. To view the properties of an individual IP address, right-click a particular IP address (in this example, **10.10.10.16**) and select **Properties**, as shown in the screenshot.

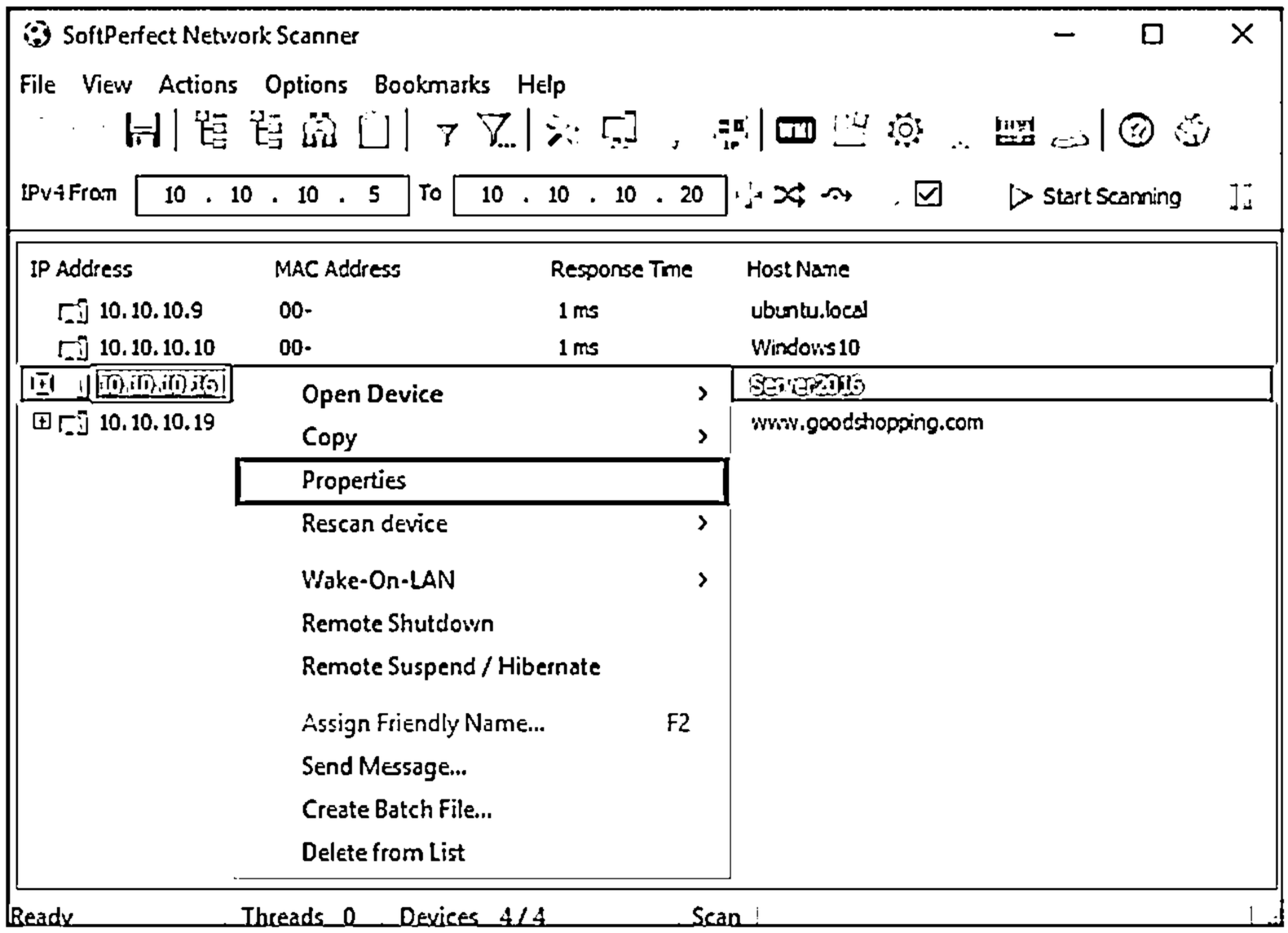


Figure 2.2.7: Details of the scanned IP address

14. The **Properties** window appears, displaying the **Shared Resources** and **Basic Info** of the machine corresponding to the selected IP address.

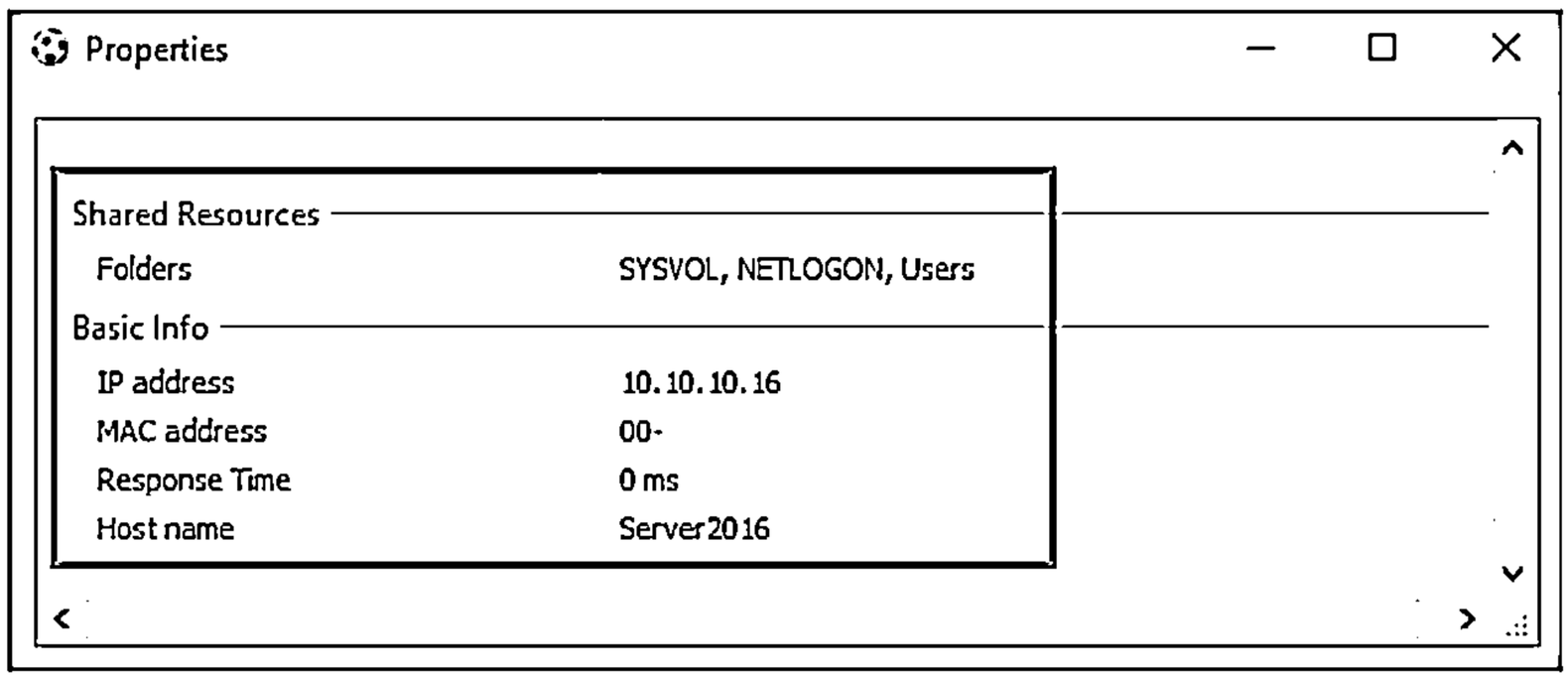


Figure 2.2.8: Properties window

15. Close the **Properties** window.

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

16. To view the shared folders, note the scanned hosts that have a + node before them. Expand the node to view all the shared folders.

Note: In this example, we are targeting the Windows Server 2016 virtual machine (10.10.10.16).

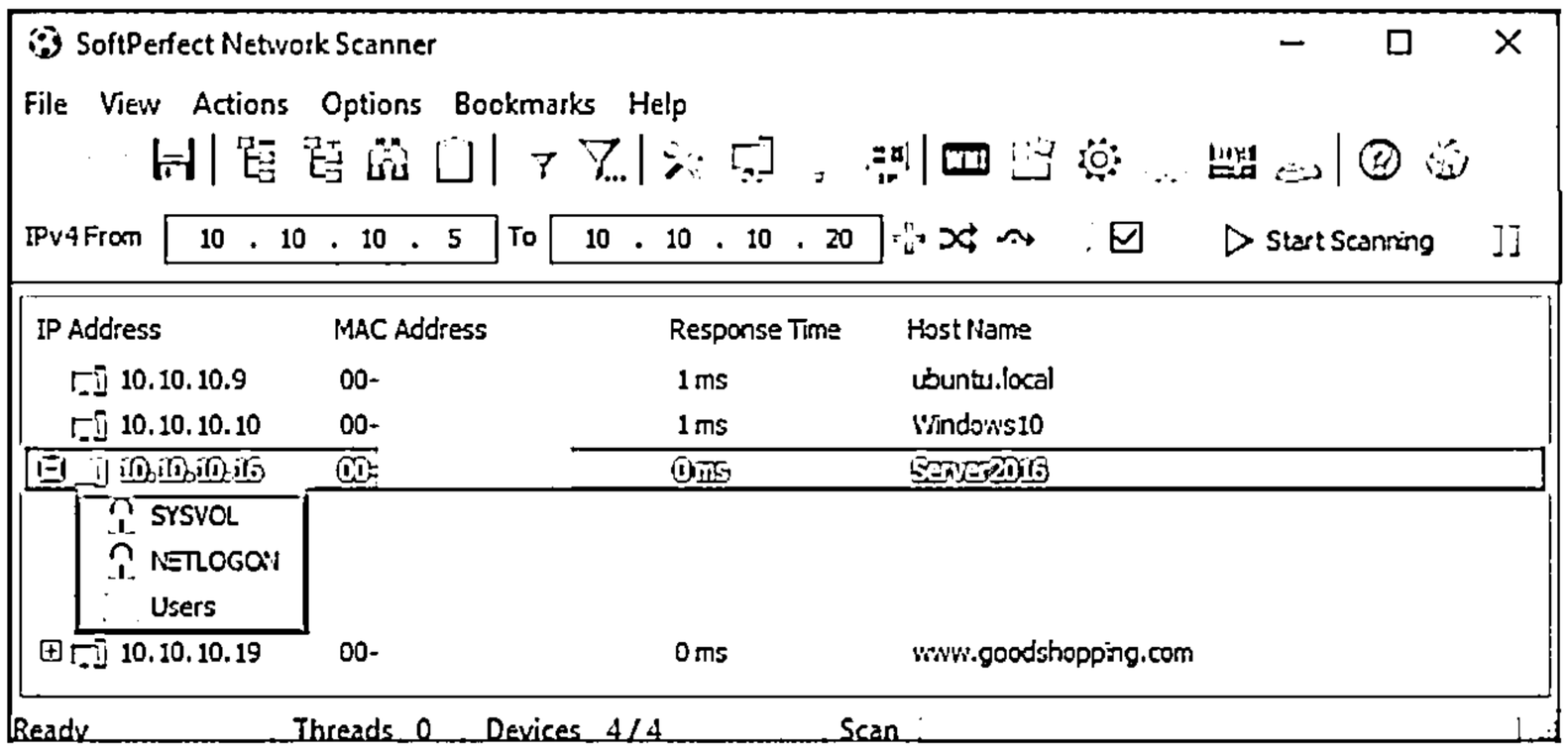


Figure 2.2.9: SoftPerfect Network Scanner displaying the shared folders

17. Right-click the selected host, and click **Open Device**. A drop-down list appears, containing options that allow you to connect to the remote machine over HTTP, HTTPS, FTP, and Telnet.

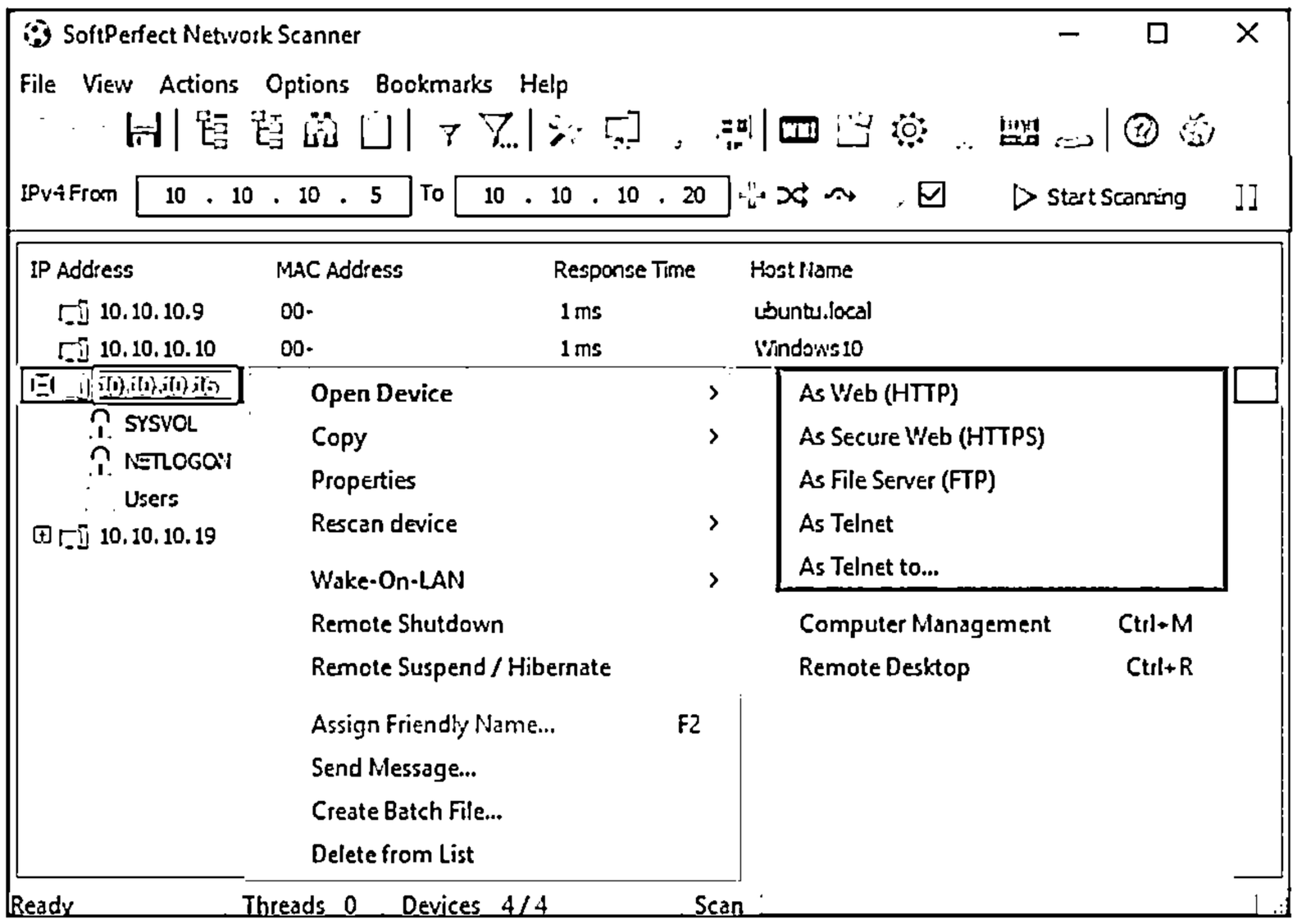


Figure 2.2.10: SoftPerfect Network Scanner showing remote connection options

You can also use other SNMP enumeration tools such as **Network Performance Monitor** (https://www.solarwinds.com), **OpUtils** (https://www.manageengine.com), **PRTG Network Monitor** (https://www.paessler.com), **Engineer's Toolset** (https://www.solarwinds.com), and **WhatsUp® Gold** (https://www.ipswitch.com) to perform SNMP enumeration on the target network.

Note: If the selected host is not secure enough, you may use these options to connect to the remote machines. You may also be able to perform activities such as sending a message and shutting down a computer remotely. These features are applicable only if the selected machine has a poor security configuration.

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

18. This concludes the demonstration of performing SNMP enumeration using the SoftPerfect Network Scanner.
19. Close all open windows and document all the acquired information.
20. Turn off the **Windows Server 2019, Windows 10, Windows Server 2016**, and **Ubuntu** virtual machines.

Lab Analysis

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

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT 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

Perform LDAP Enumeration

This method of enumeration uses LDAP to generate a list of distributed directory services on the target system.

ICON KEY

Valuable information

Test your knowledge

Web exercise

Workbook review

Lab Scenario

As a professional ethical hacker or penetration tester, the next step after SNMP enumeration is to perform LDAP enumeration to access directory listings within Active Directory or other directory services. Directory services provide hierarchically and logically structured information about the components of a network, from lists of printers to corporate email directories. In this sense, they are similar to a company's org chart.

LDAP enumeration allows you to gather information about usernames, addresses, departmental details, server names, etc.

Lab Objectives

- Perform LDAP enumeration using Active Directory Explorer (AD Explorer)

Lab Environment

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 04 Enumeration

To carry out this lab, you need:

- Windows Server 2019 virtual machine
- Windows Server 2016 virtual machine
- Windows 10 Virtual Machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 10 Minutes

Overview of LDAP Enumeration

LDAP (Lightweight Directory Access Protocol) is an Internet protocol for accessing distributed directory services over a network. LDAP uses DNS (Domain Name

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

System) for quick lookups and fast resolution of queries. A client starts an LDAP session by connecting to a DSA (Directory System Agent), typically on TCP port 389, and sends an operation request to the DSA, which then responds. BER (Basic Encoding Rules) is used to transmit information between the client and the server. One can anonymously query the LDAP service for sensitive information such as usernames, addresses, departmental details, and server names.

Lab Tasks

TASK 1

Perform LDAP Enumeration using Active Directory Explorer (AD Explorer)

Here, we will use the AD Explorer to perform LDAP enumeration on an AD domain and modify the domain user accounts.

1. Start the **Windows 10**, **Windows Server 2019** and **Windows Server 2016** virtual machines.
2. Log in to the **Windows Server 2019** virtual machine with the credentials **Administrator** and **Pa$$w0rd**.

TASK 1.1

Launch AD Explorer

3. Navigate to **Z:\CEHv11 Module 04 Enumeration\LDAP Enumeration Tools\Active Directory Explorer** and double-click **ADExplorer.exe**.
4. The **Active Directory Explorer License Agreement** window appears; click **Agree**.

Active Directory Explorer (AD Explorer) is an advanced Active Directory (AD) viewer and editor. It can be used to navigate an AD database easily, define favorite locations, view object properties and attributes without having to open dialog boxes, edit permissions, view an object's schema, and execute sophisticated searches that can be saved and re-executed.

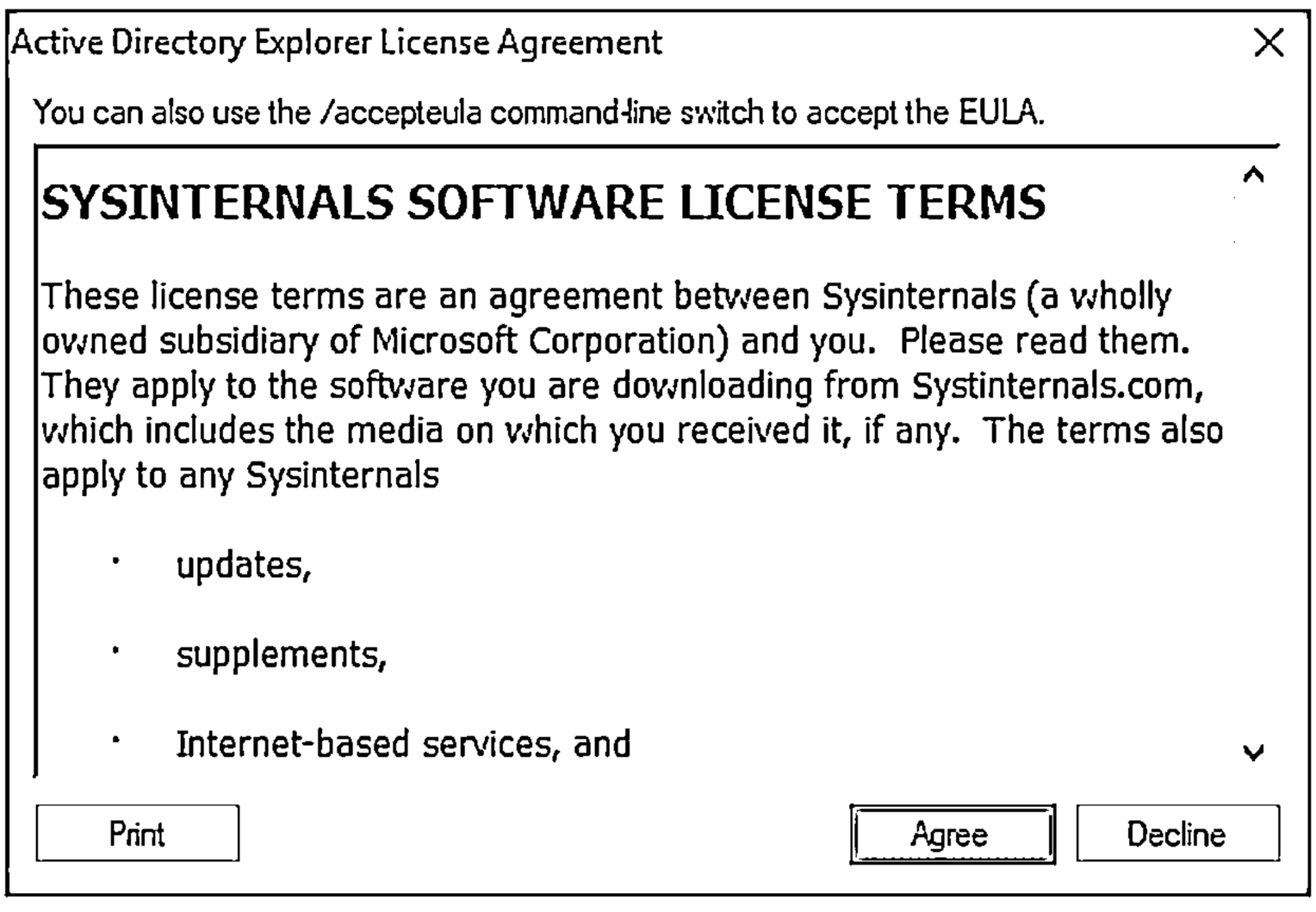


Figure 3.1.1: AD Explorer License Agreement window

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

TASK 1.2

Connect to Active Directory Machine

5. The **Connect to Active Directory** pop-up appears; type the IP address of the target in the **Connect to** field (in this example, we are targeting the **Windows Server 2016** virtual machine: **10.10.10.16**) and click **OK.**

Note: IP addresses may differ in your lab environment.

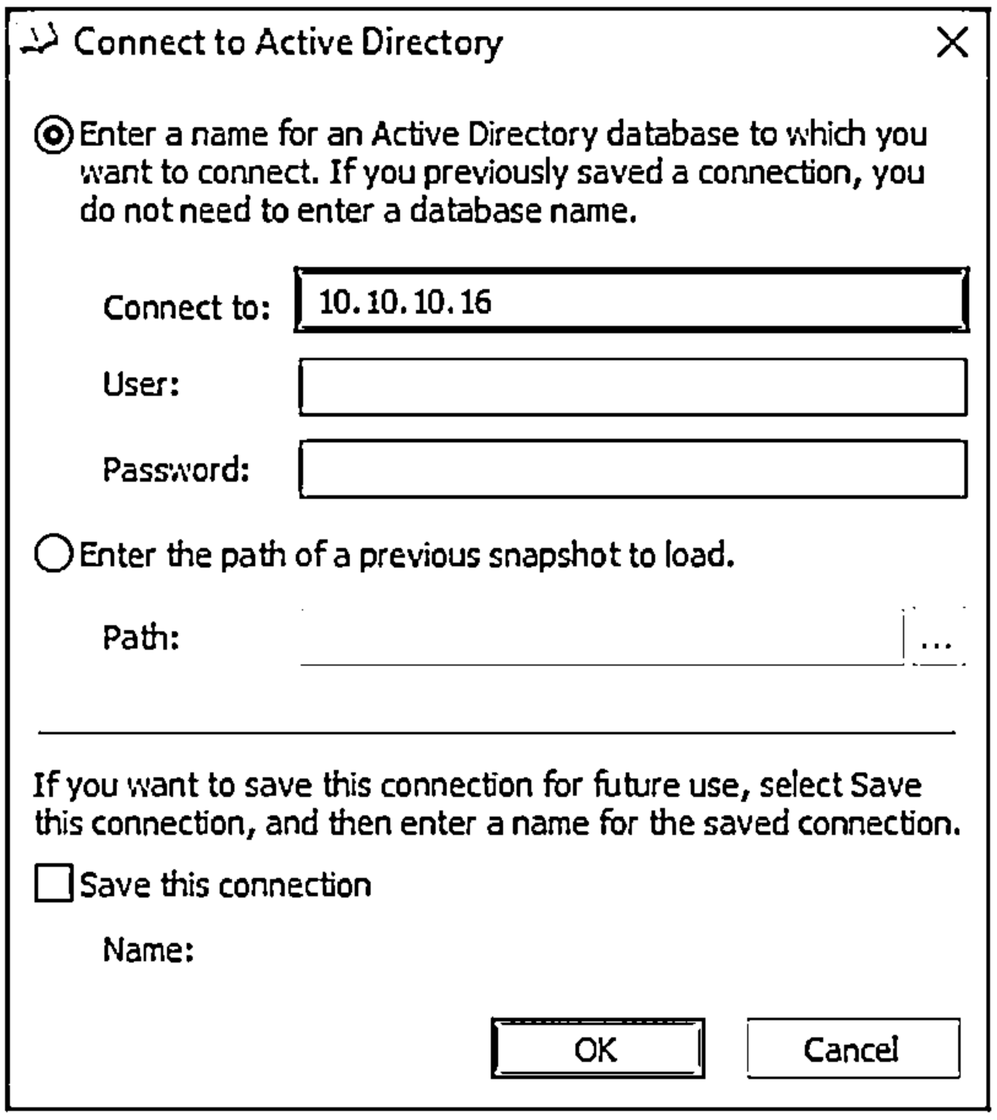


Figure 3.1.2: AD Explorer Connect to Active Directory window

6. The **Active Directory Explorer** displays the active directory structure in the left pane, as shown in the screenshot.

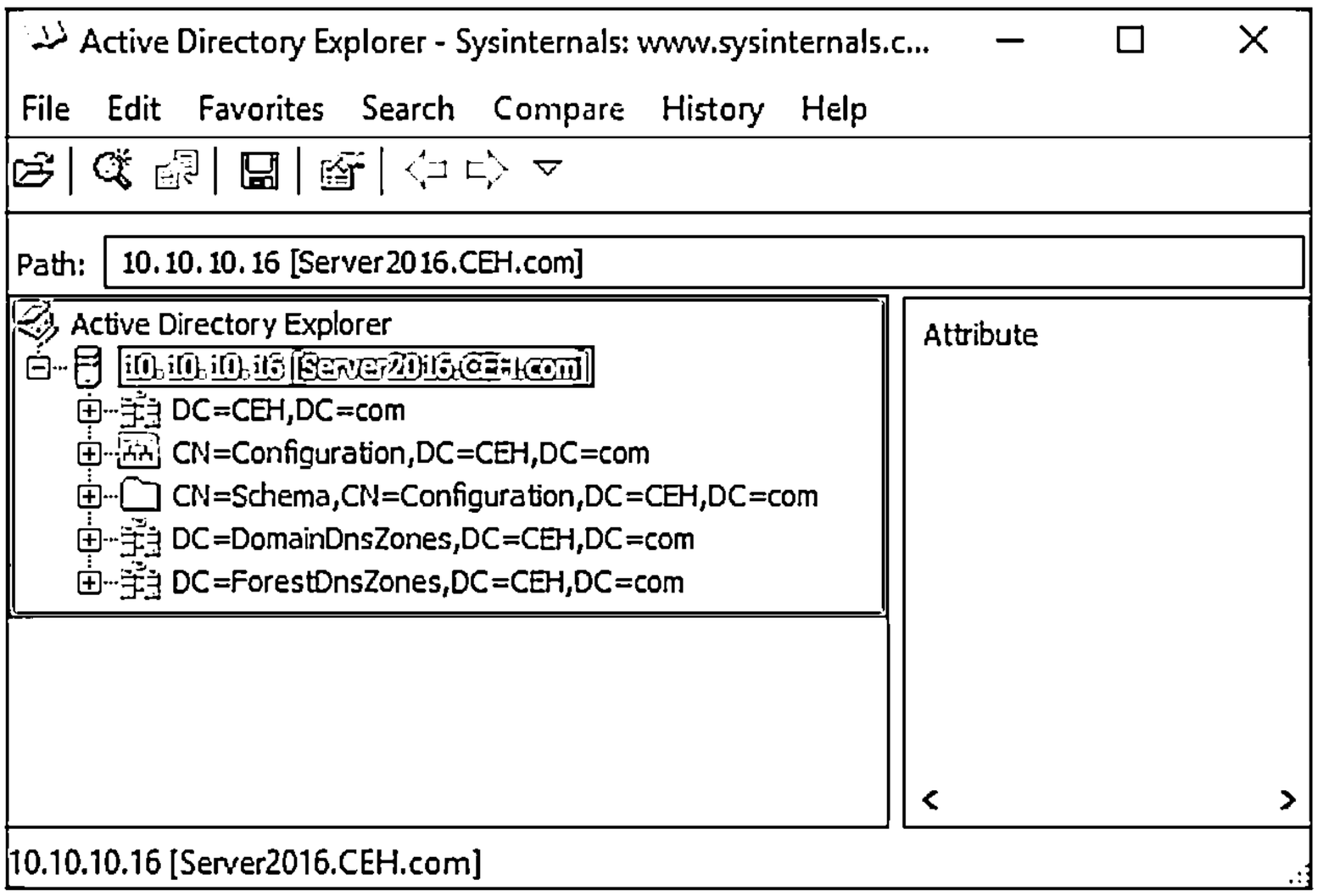


Figure 3.1.3: Active Directory structure

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

7. Now, expand **DC=CEH**, **DC=com**, and **CN=Users** by clicking "**+**" to explore domain user details.

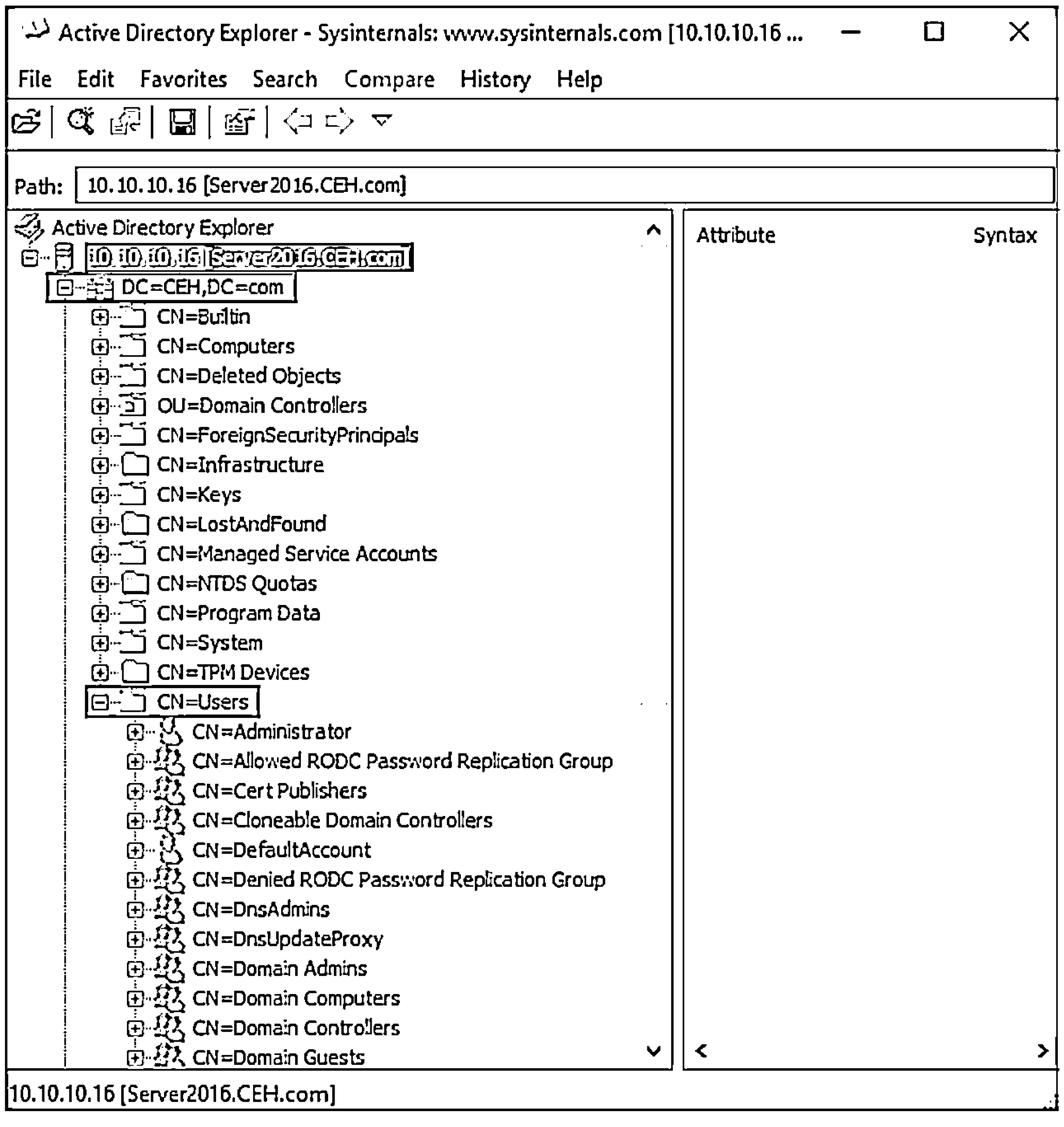


Figure 3.1.4: AD Explorer domain users node

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

8. Click any **username** (in the left pane) to display its properties in the right pane.

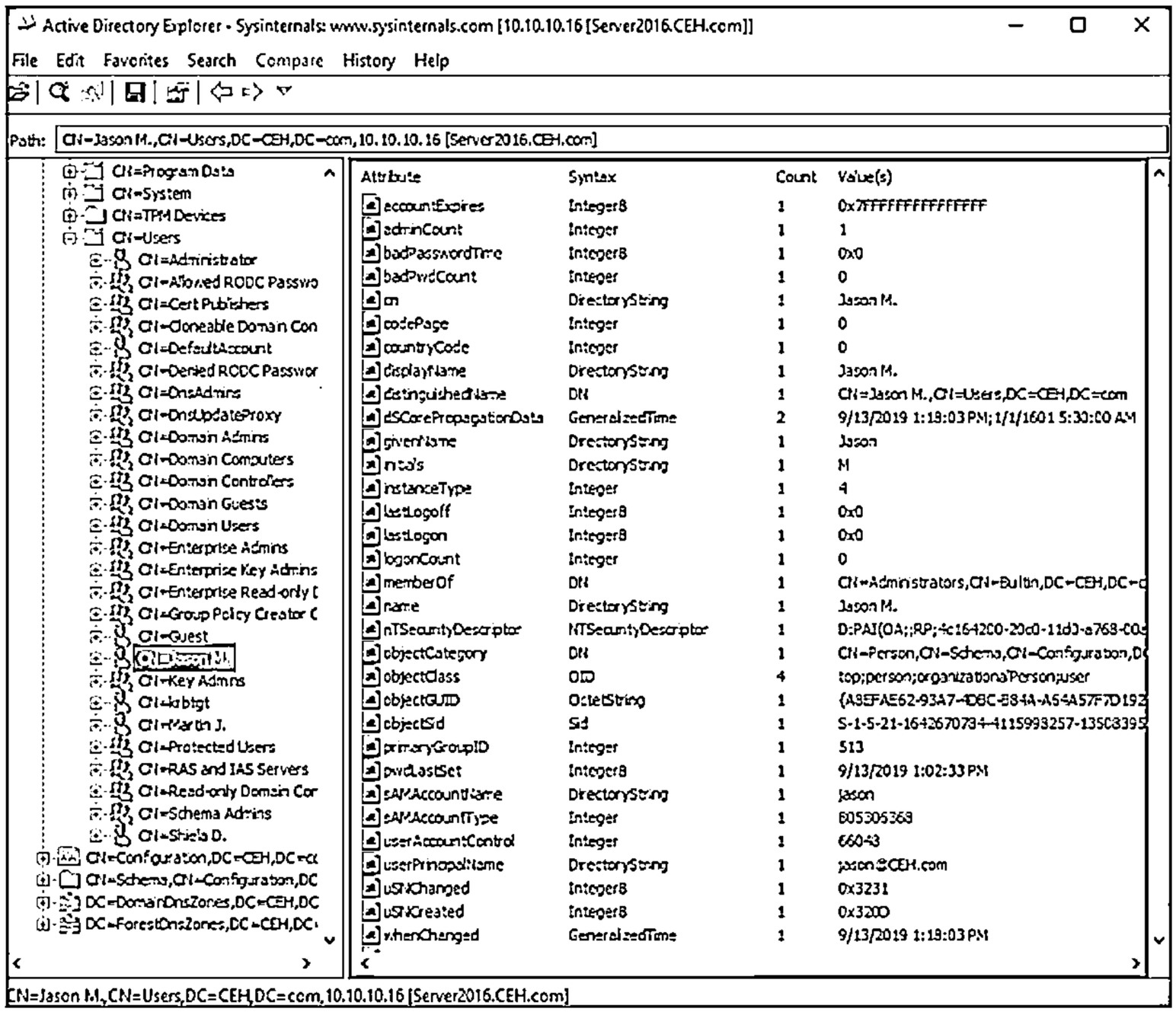


Figure 3.1.5: AD Explorer domain users profile attributes

TASK 1.3

Modifying User Attributes

9. Right-click any attribute in the right pane (in this case, **displayName**) and click **Modify...** from the context menu to modify the user's profile.

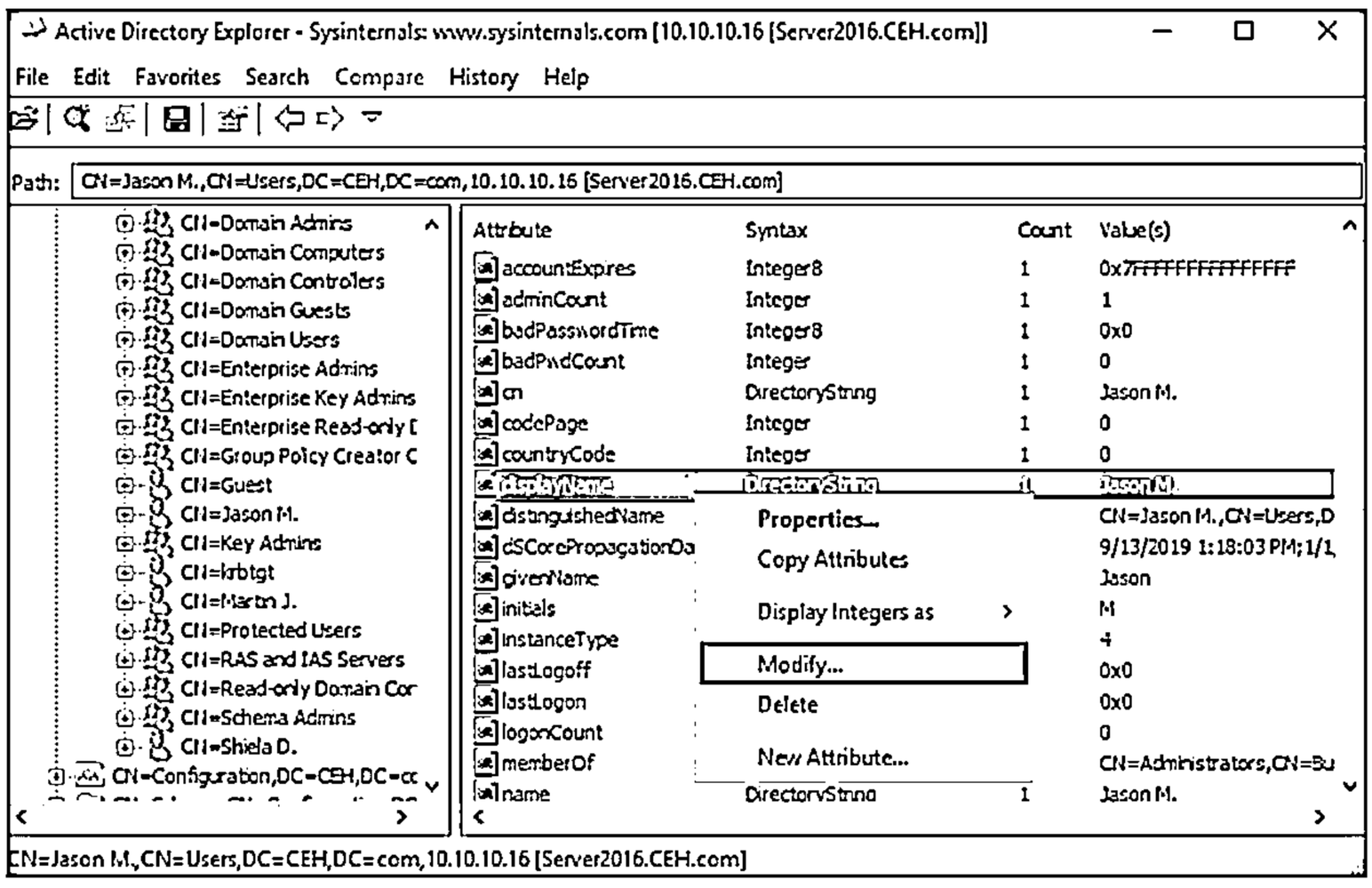


Figure 3.1.6: AD Explorer user profile modification

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

10. The **Modify Attribute** window appears. First, select the username under the **Value** section, and then click the **Modify...** button. The **Edit Value** pop-up appears. Rename the username in the **Value data** field and click **OK** to save the changes.

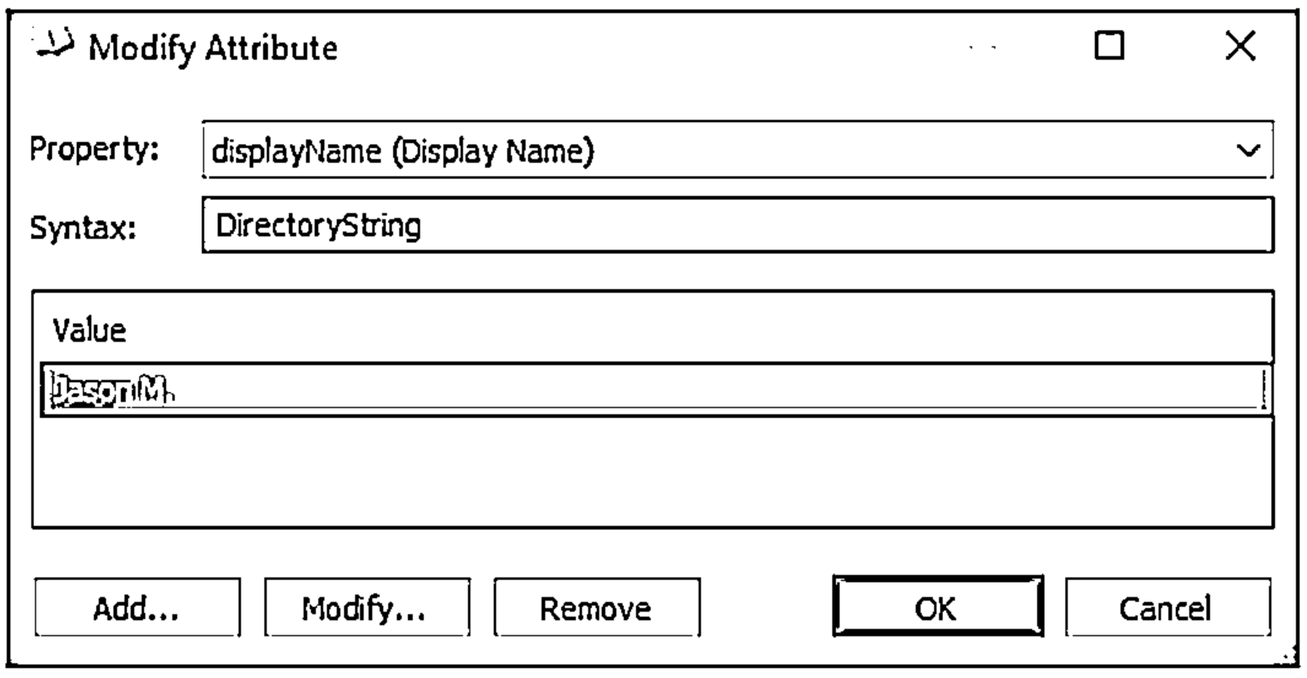


Figure 3.1.7: Modifying attributes

11. You can read and modify other user profile attributes in the same way.
12. This concludes the demonstration of performing LDAP enumeration using AD Explorer.
13. Close all open windows and document all the acquired information.
14. Turn off the **Windows Server 2019**, **Windows 10** and **Windows Server 2016** virtual machines.

You can also use other LDAP enumeration tools such as **Softerra LDAP Administrator** (https://www.ldapadministrator.com), **LDAP Admin Tool** (https://www.ldapsoft.com), **LDAP Account Manager** (https://www.ldap-account-manager.org), **LDAP Search** (https://securityxploded.com), and **JXplorer** (http://www.jxplorer.org) to perform LDAP enumeration on the target.

Lab Analysis

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

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT 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

Perform NFS Enumeration

NFS enumeration is a method by which exported directories and shared data on target systems is extracted.

ICON KEY

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

Lab Scenario

As a professional ethical hacker or penetration tester, the next step after LDAP enumeration is to perform NFS enumeration to identify exported directories and extract a list of clients connected to the server, along with their IP addresses and shared data associated with them.

After gathering this information, it is possible to spoof target IP addresses to gain full access to the shared files on the server.

Lab Objectives

- Perform NFS enumeration using RPCScan and SuperEnum

Lab Environment

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 04 Enumeration

To carry out this lab, you need:

- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 10 Minutes

Overview of NFS Enumeration

NFS (Network File System) is a type of file system that enables computer users to access, view, store, and update files over a remote server. This remote data can be accessed by the client computer in the same way that it is accessed on the local system.

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

TASK 1

Perform NFS Enumeration using RPCScan and SuperEnum

Here, we will use RPCScan and SuperEnum to enumerate NFS services running on the target machine.

Note: Before starting this lab, it is necessary to enable the NFS service on the target machine (**Windows Server 2019**). This will be done in **Steps 1-6**.

TASK 1.1

Enable NFS Service

1. Start the **Windows Server 2019** virtual machine and log in with the credentials **Administrator** and **Pa$$w0rd**. Click the **Start** button at the bottom-left corner of **Desktop** and open **Server Manager**.
2. The **Server Manager** main window appears. By default, **Dashboard** will be selected; click **Add roles and features**.

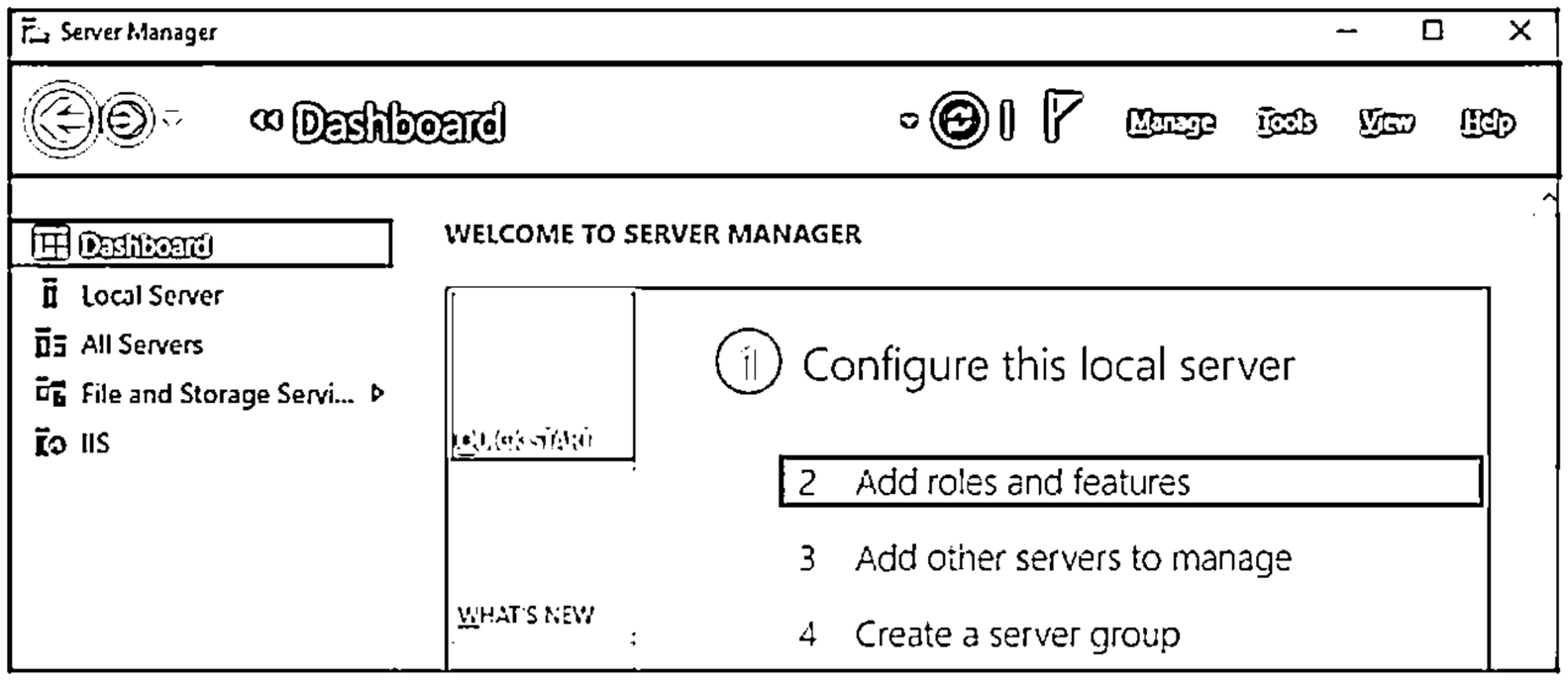


Figure 4.1.1: Server Manager: selecting Add roles and features

RPCScan communicates with RPC (remote procedure call) services and checks misconfigurations on NFS shares. It lists RPC services, mountpoints, and directories accessible via NFS. It can also recursively list NFS shares. SuperEnum includes a script that performs a basic enumeration of any open port, including the NFS port (2049).

3. The **Add Roles and Features Wizard** window appears. Click **Next** here and in the **Installation Type** and **Server Selection** wizards.
4. The **Server Roles** section appears. Expand **File and Storage Services** and select the checkbox for **Server for NFS** under the **File and iSCSI Services** option, as shown in the screenshot. Click **Next**.

Note: In the **Add features that are required for Server for NFS?** pop-up window, click the **Add Features** button.

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

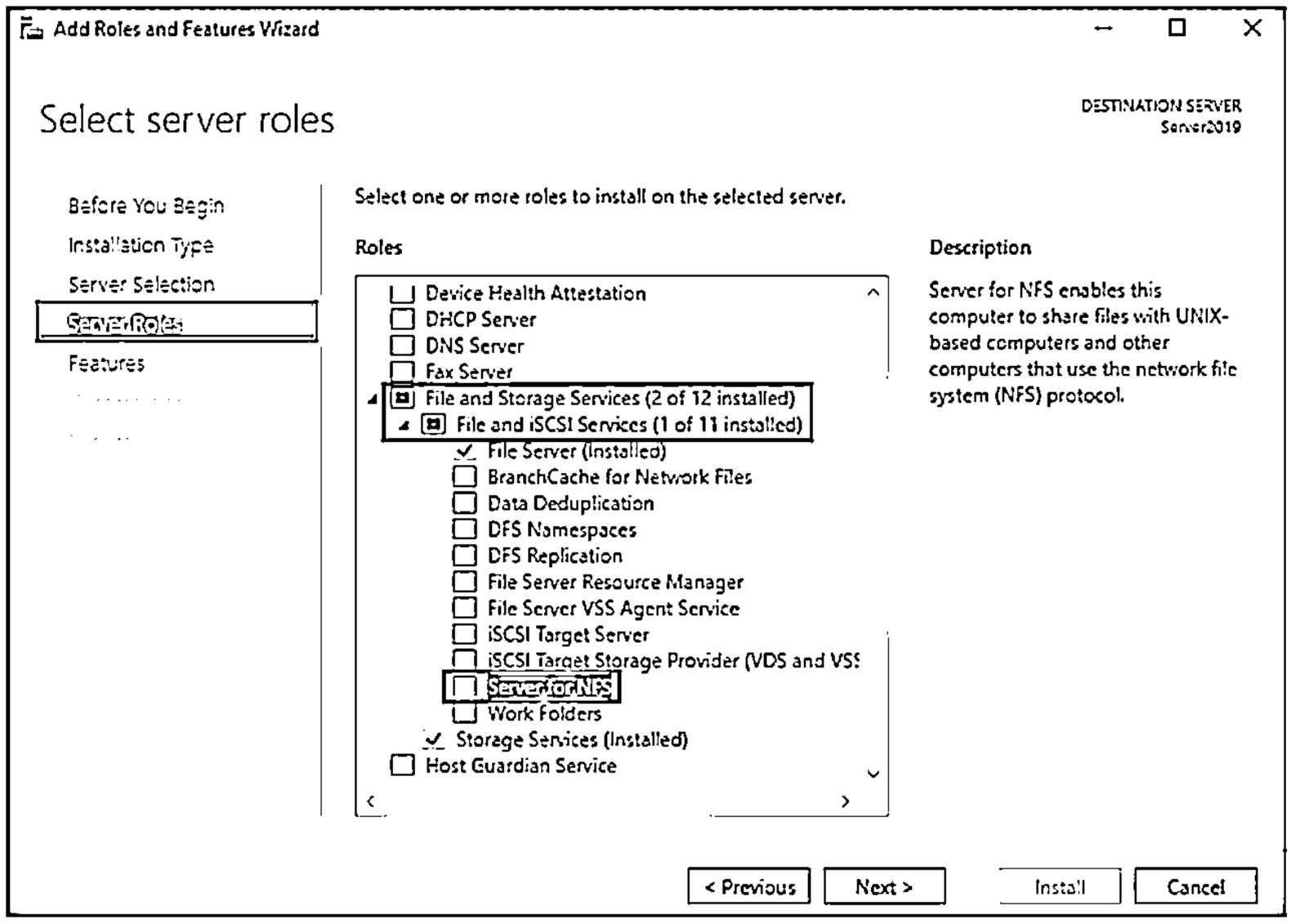


Figure 4.1.2: Server Roles: selecting a server for NFS

5. In the **Features** section, click **Next**. The **Confirmation** section appears; click **Install** to install the selected features.
6. The features begin installing, with progress shown by the **Feature installation** status bar. When installation completes, click **Close**.

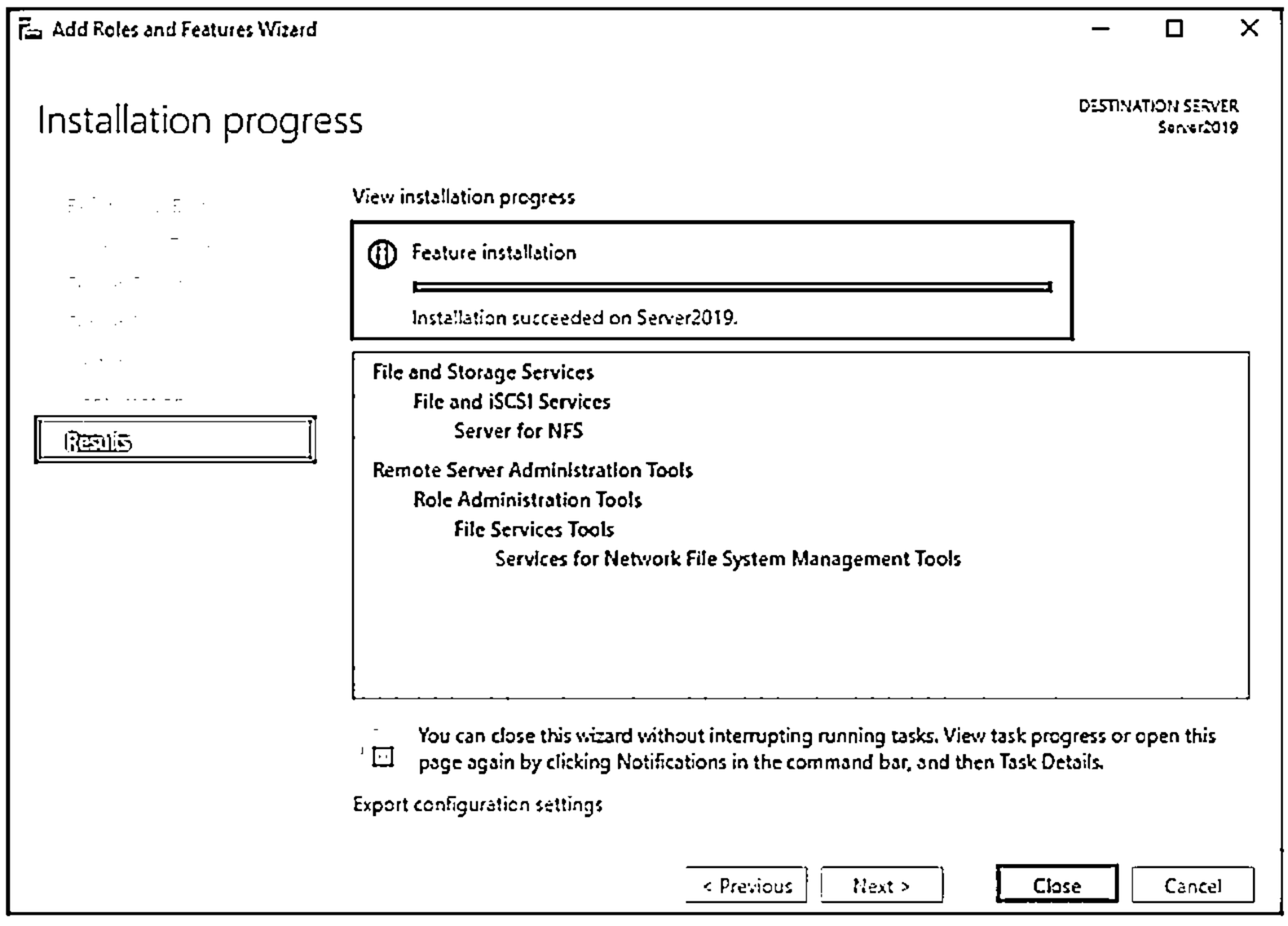


Figure 4.1.3: Results: click Close

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

TASK 1.2

Check for Open NFS Port

7. Having enabled the NFS service, it is necessary to check if it is running on the target system (**Windows Server 2019**). In order to do this, start the **Parrot Security** virtual machine.
8. In the **Parrot Security** virtual machine login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

9. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
10. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
11. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

12. Now, type **cd** and press **Enter** to jump to the root directory.

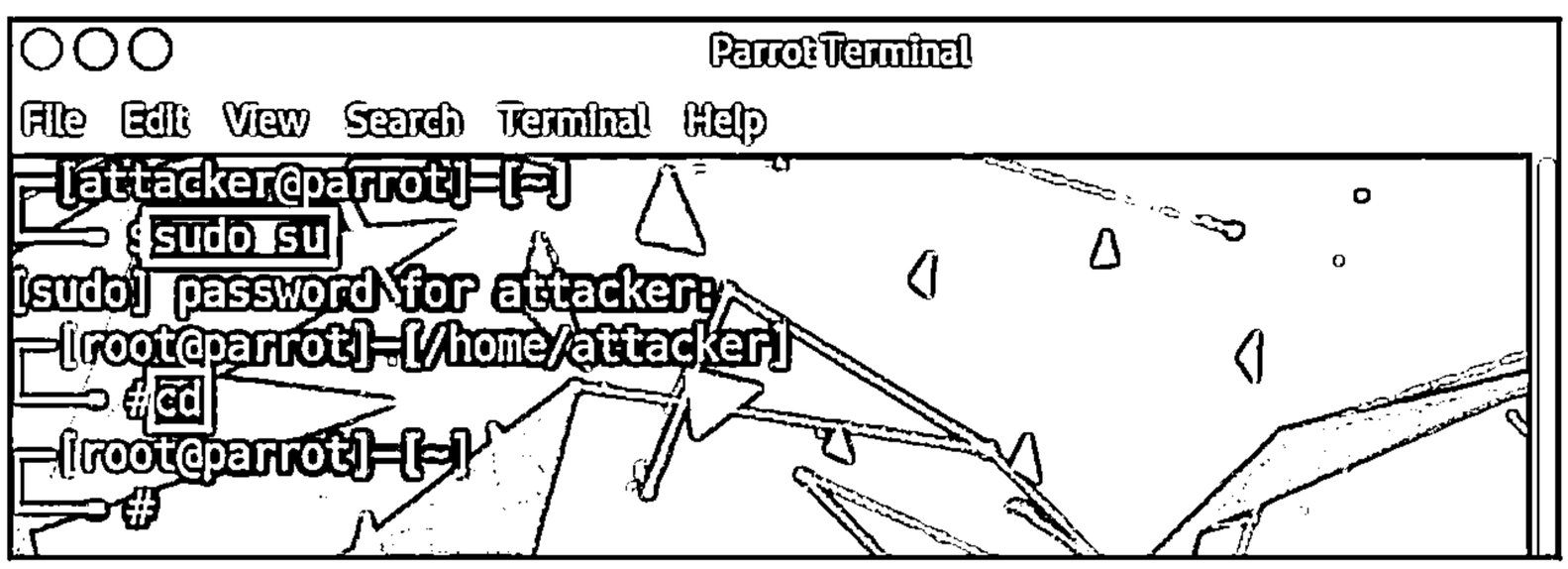


Figure 4.1.4: Running the programs as a root user

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

13. In the terminal, type **nmap -p 2049 <Target IP Address>** (in this case, **10.10.10.19**) and press **Enter**.
14. The scan result appears indicating that port 2049 is opened, and the NFS service is running on it, as shown in the screenshot.

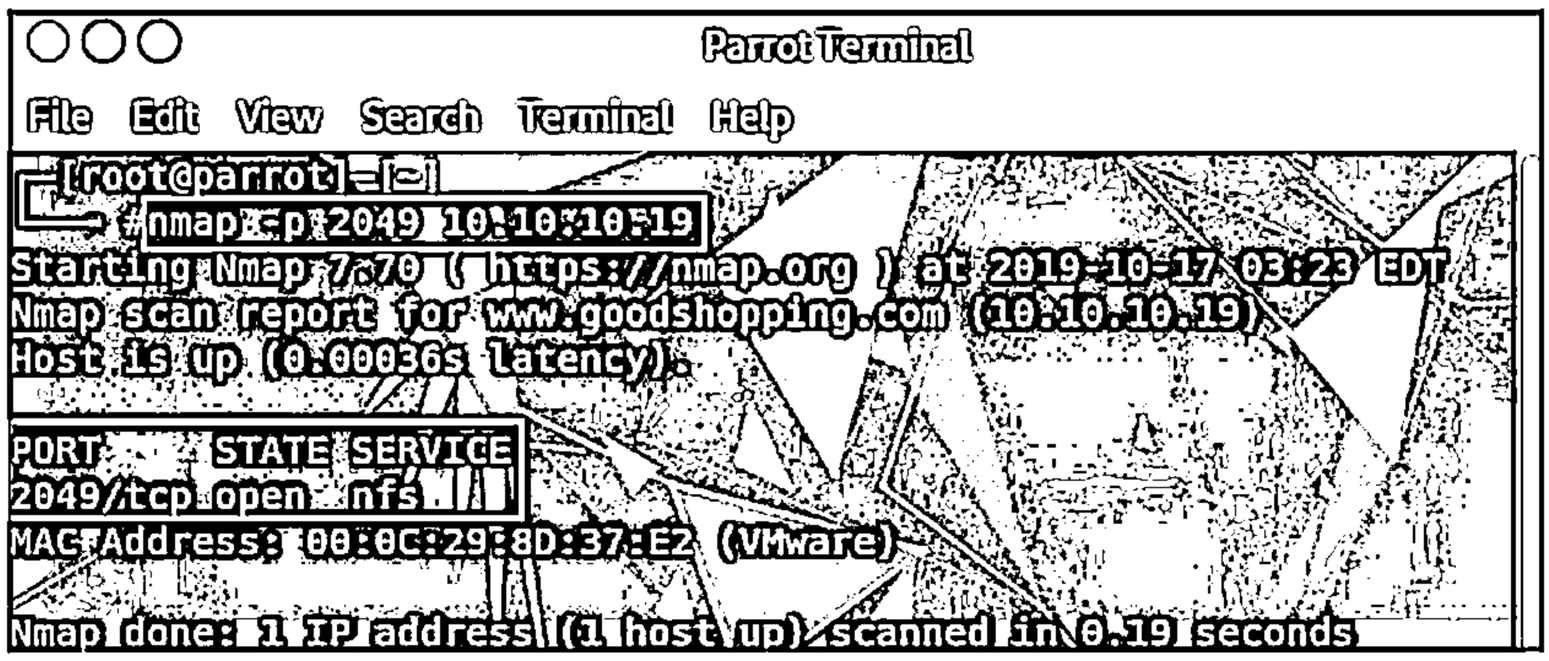


Figure 4.1.5: Nmap scan result

TASK 1.3

Clone SuperEnum Tool

15. In the terminal window, type **git clone https://github.com/p4pentest/SuperEnum** and press **Enter** to download the SuperEnum repository.

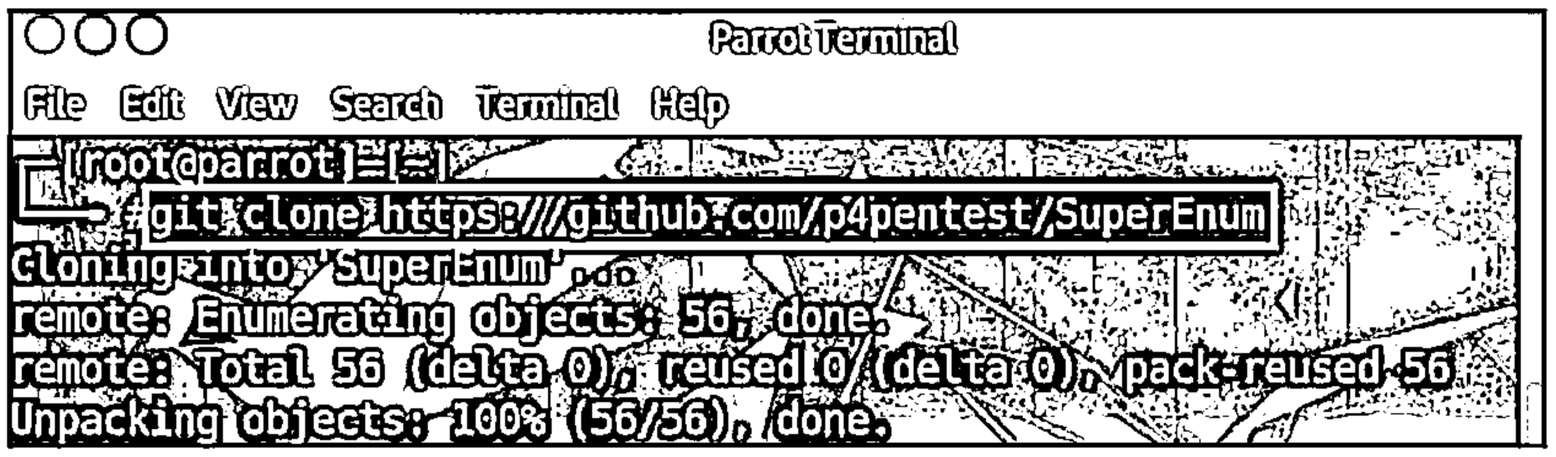


Figure 4.1.6: Cloning SuperEnum

Note: You can also access the tool repository from the **CEH-Tools** folder available in **Windows 10** virtual machine, in case, the GitHub link does not exist, or you are unable to clone the tool repository. Follow the steps below in order to access **CEH-Tools** folder from the **Parrot Security** virtual machine:

- Open any explorer window and press **Ctrl+L**. The **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access **Windows 10** shared folders.
- The security pop-up appears; enter the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.
- The **Windows shares on 10.10.10.10** window appears; navigate to the location **CEH-Tools/CEHv11 Module 04 Enumeration/GitHub Tools/** and copy the **SuperEnum** folder.
- Paste the copied **SuperEnum** folder on the location **/home/attacker/**.
- In the terminal window, type **mv /home/attacker/SuperEnum /root/**.

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

TASK 1.4

Create a File Containing Target IP

16. After the download completes, in the terminal window, type **cd SuperEnum** and press **Enter** to navigate to the SuperEnum tool folder.

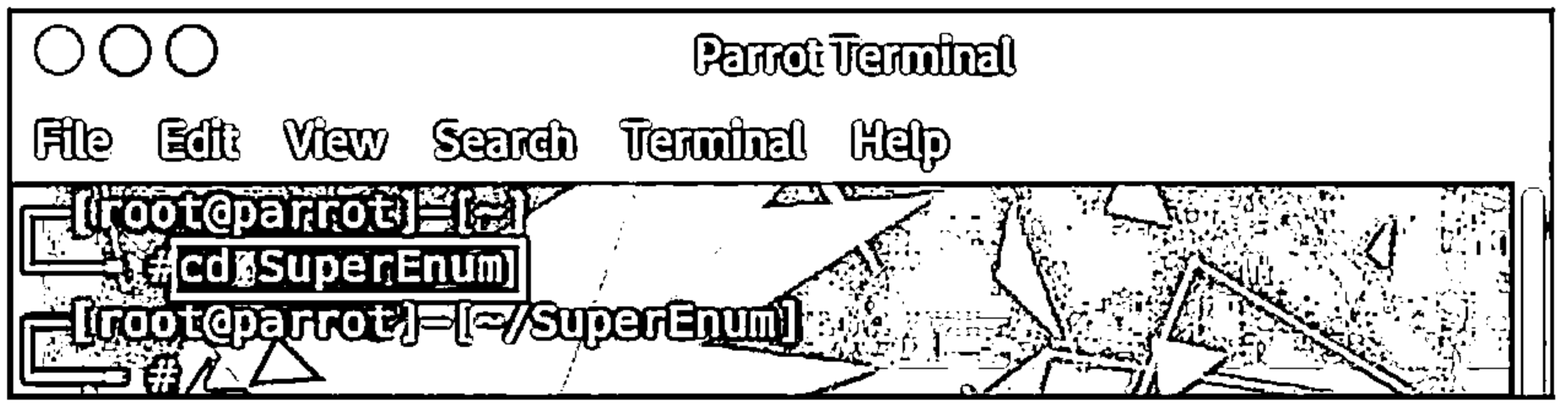


Figure 4.1.7: Navigate to the SuperEnum folder

17. Type **echo "10.10.10.19" >> Target.txt** and press **Enter** to create a target file containing IP address.

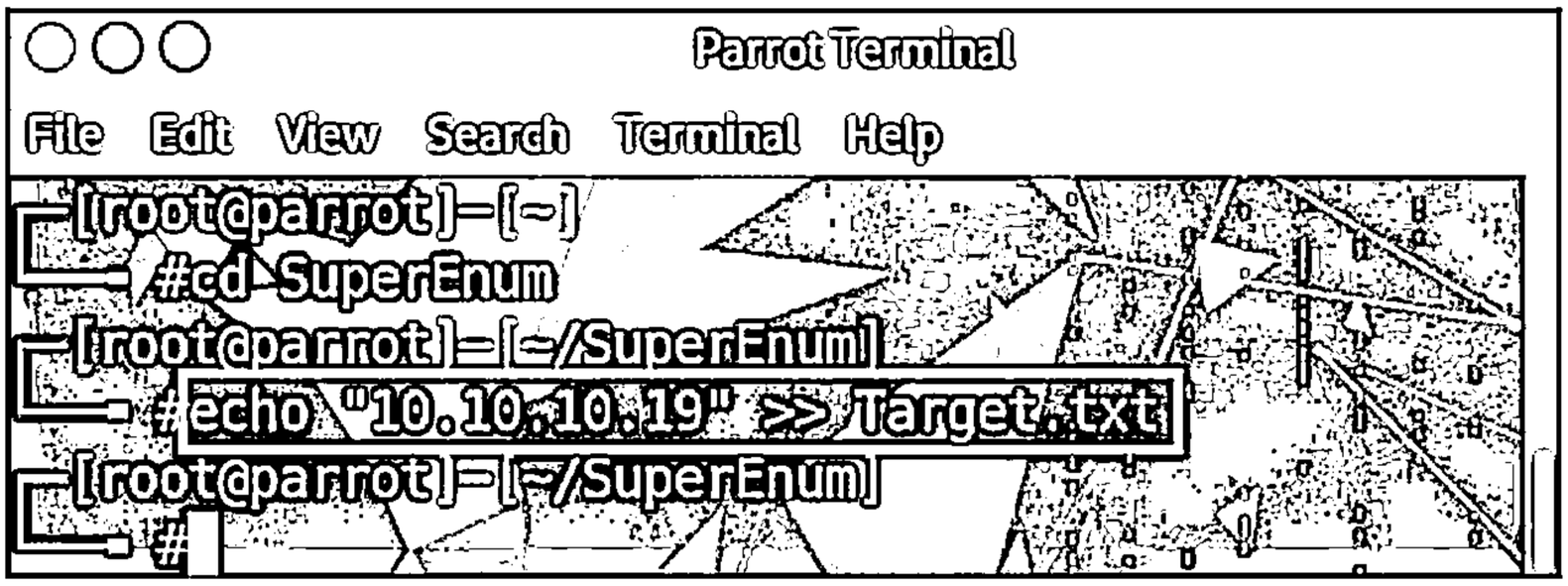


Figure 4.1.8: Create Target.txt file

Note: You may enter multiple IP addresses in the **Target.txt** file. However, in this task we are targeting only one machine, the **Windows Server 2019** (**10.10.10.19**). The IP address may vary in your lab environment.

TASK 1.5

Run ./superenum Script

18. Type **./superenum** and press **Enter**. Under **Enter IP List filename with path**, type **Target.txt**, and press **Enter**.

Note: If you get an error running the ./superenum script, type **chmod +x superenum** and press **Enter**, then repeat **Step 18**.

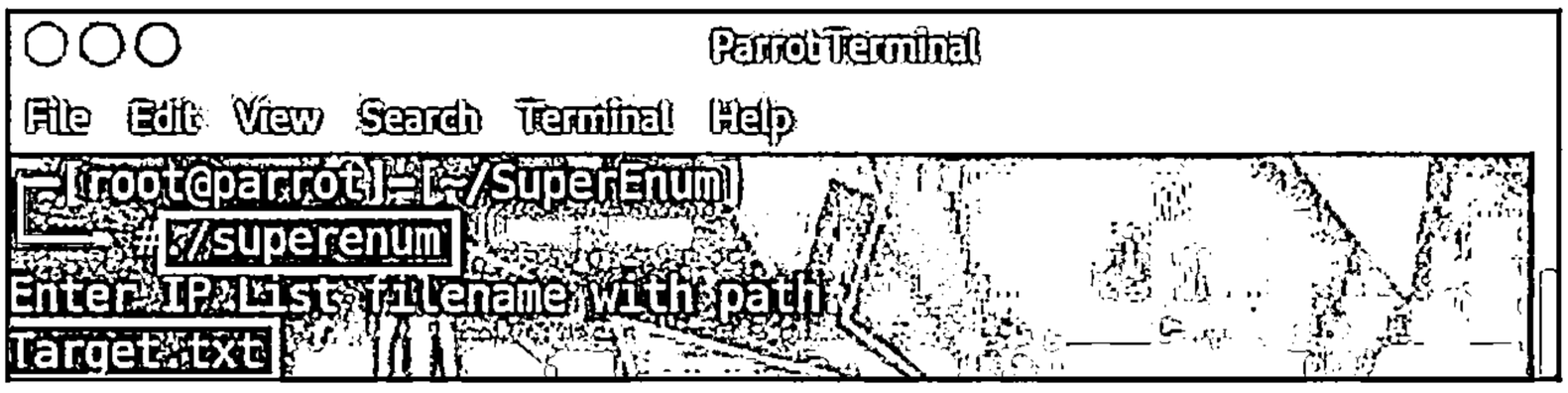


Figure 4.1.9: Run the ./superenum script and enter filename

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

19. The script starts scanning the target IP address for open NFS and other.

Note: The scan will take approximately 15-20 mins to complete.

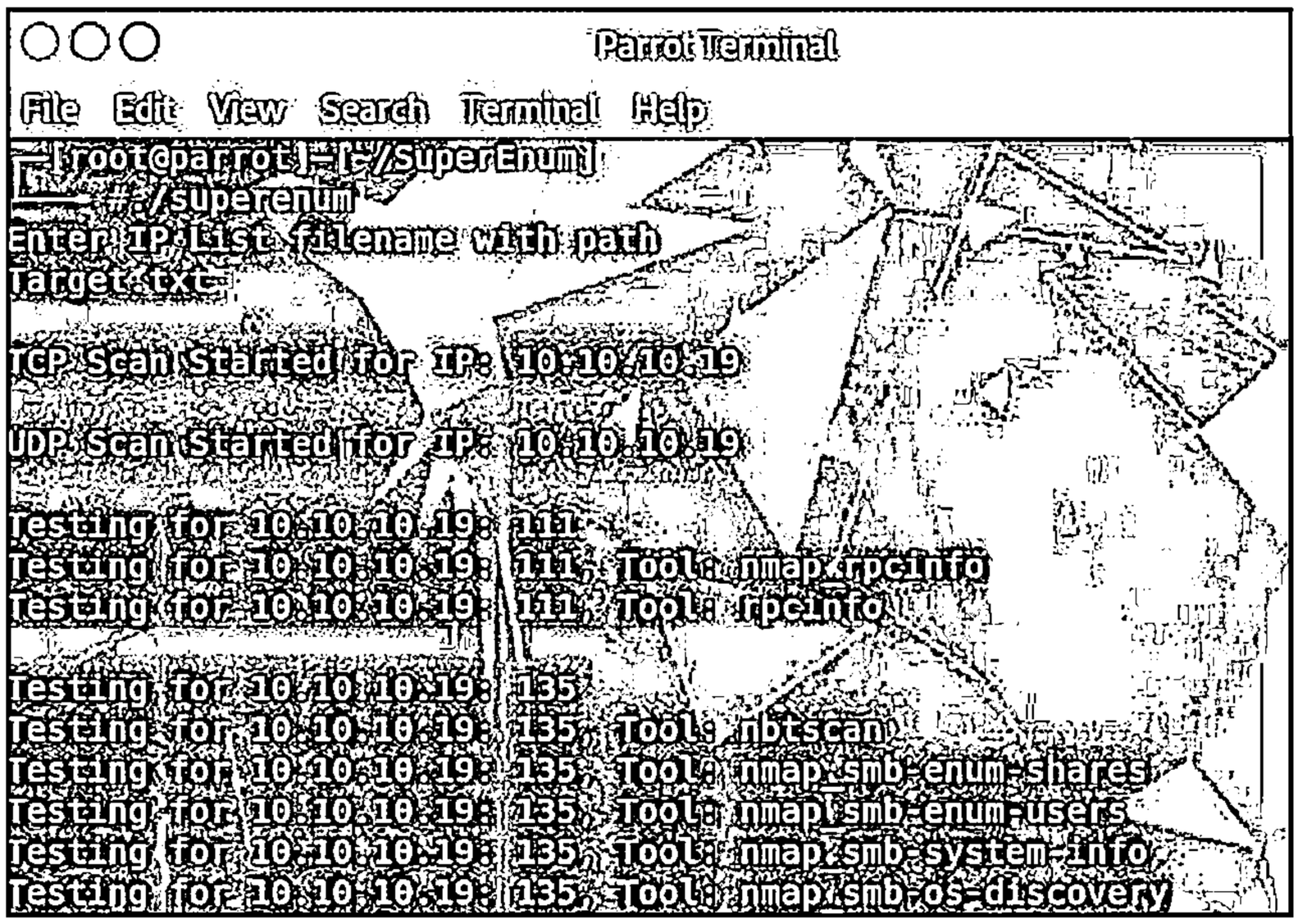


Figure 4.1.10: Scanning the target IP address

TASK 1.6

Analyze the Result

20. After the scan is finished, scroll down to review the results. Note that port 2049 is open and the NFS service is running on it.

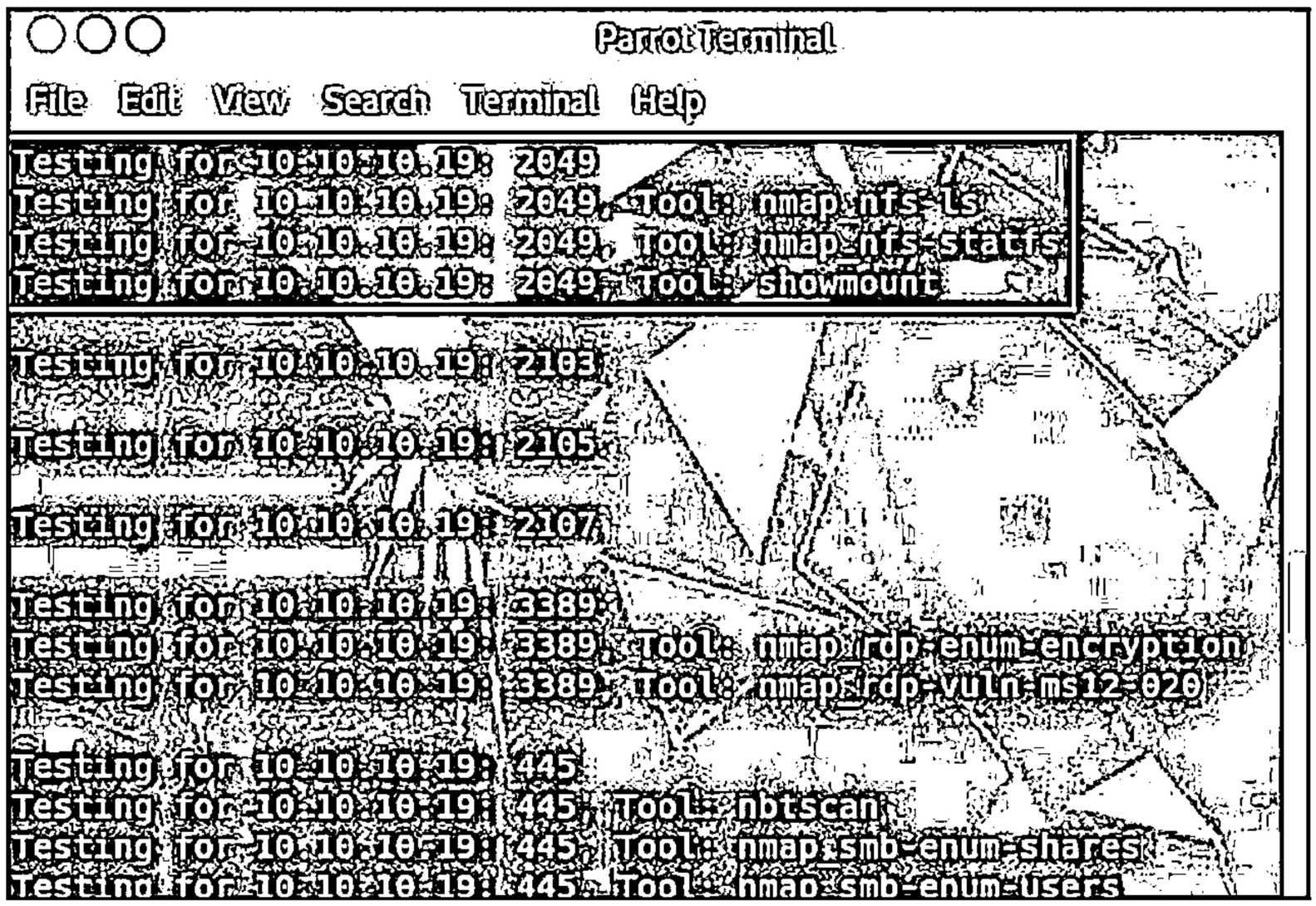


Figure 4.1.11: The open NFS port

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

21. You can also observe the other open ports and the services running on them.
22. In the terminal window, type **cd ..** and press **Enter** to return to the root directory.
23. Now, we will perform NFS enumeration using RPCScan. To do so, in the terminal window, type **git clone https://github.com/hegusung/RPCScan** and press **Enter** to download the RPCScan repository.

TASK 1.7

Clone RPCScan Tool

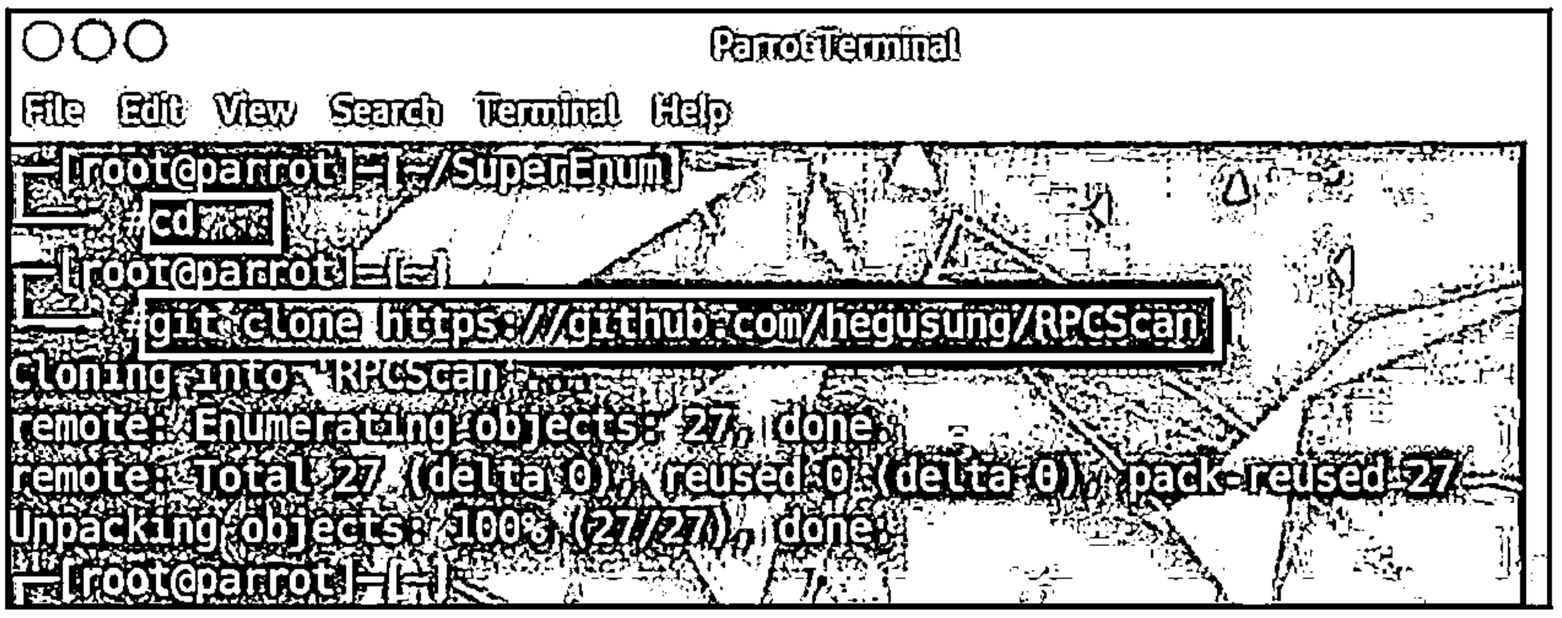


Figure 4.1.12: Cloning RPCScan

Note: You can also access the tool repository from the **CEH-Tools** folder available in **Windows 10** virtual machine, in case, the GitHub link does not exist, or you are unable to clone the tool repository. Follow the steps below in order to access **CEH-Tools** folder from the **Parrot Security** virtual machine:

- Open any explorer window and press **Ctrl+L**. The **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access **Windows 10** shared folders.
- The security pop-up appears; enter the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.
- The **Windows shares on 10.10.10.10** window appears; navigate to the location **CEH-Tools/CEHv11 Module 04 Enumeration/GitHub Tools/** and copy the **RPCScan** folder.
- Paste the copied **RPCScan** folder on the location **/home/attacker/**.
- In the terminal window, type **mv /home/attacker/RPCScan /root/**.

24. After the download completes, navigate to the RPCScan folder by typing **cd RPCScan** and press **Enter**.

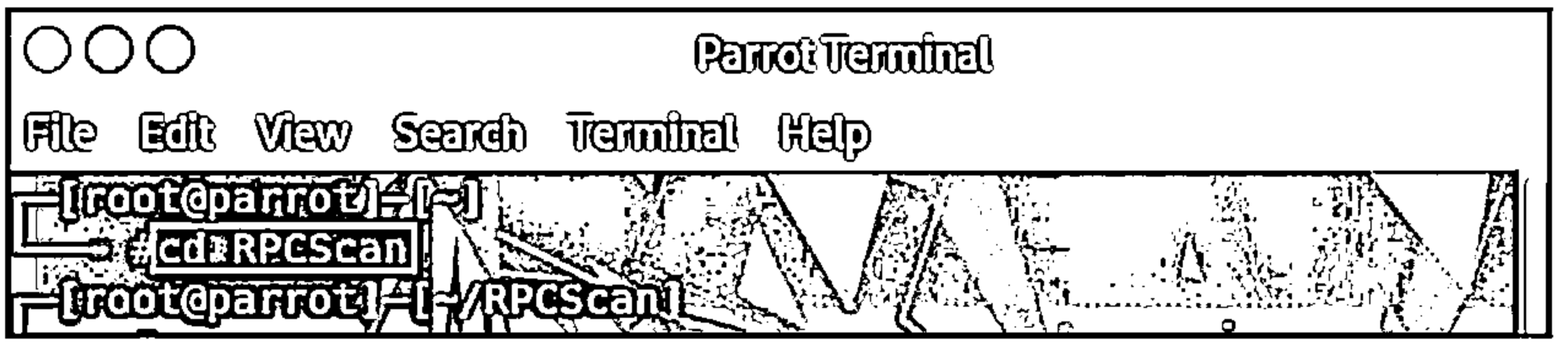


Figure 4.1.13: Navigate to the RPCScan folder

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

25. Type **python3 rpc-scan.py <Target IP address> --rpc** (in this case, the target IP address is **10.10.10.19**, the **Windows Server 2019** virtual machine); press **Enter**.

Note: **--rpc**: lists the RPC (portmapper); the target IP address may differ in your lab environment.

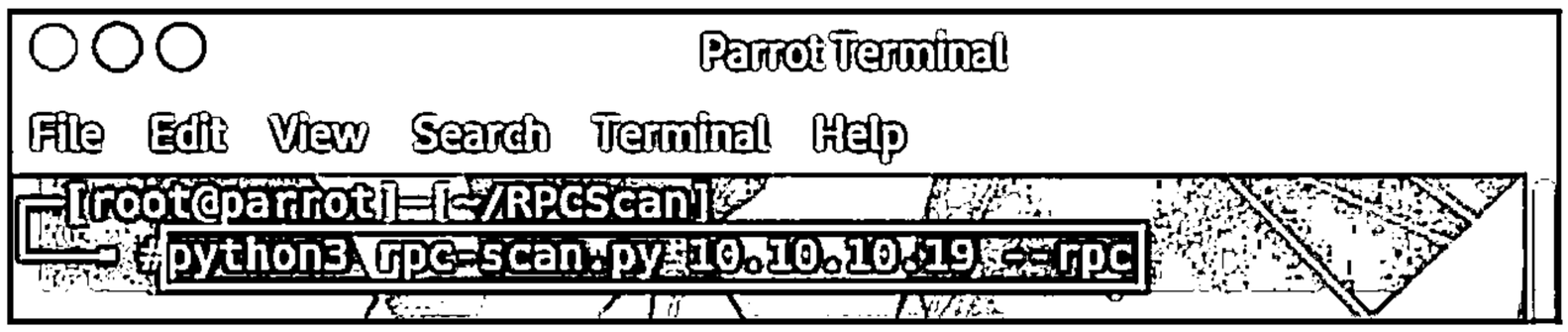


Figure 4.1.14: Run RPCScan

TASK 1.8

Analyze the Result

26. The result appears, displaying that port 2049 is open, and the NFS service is running on it.

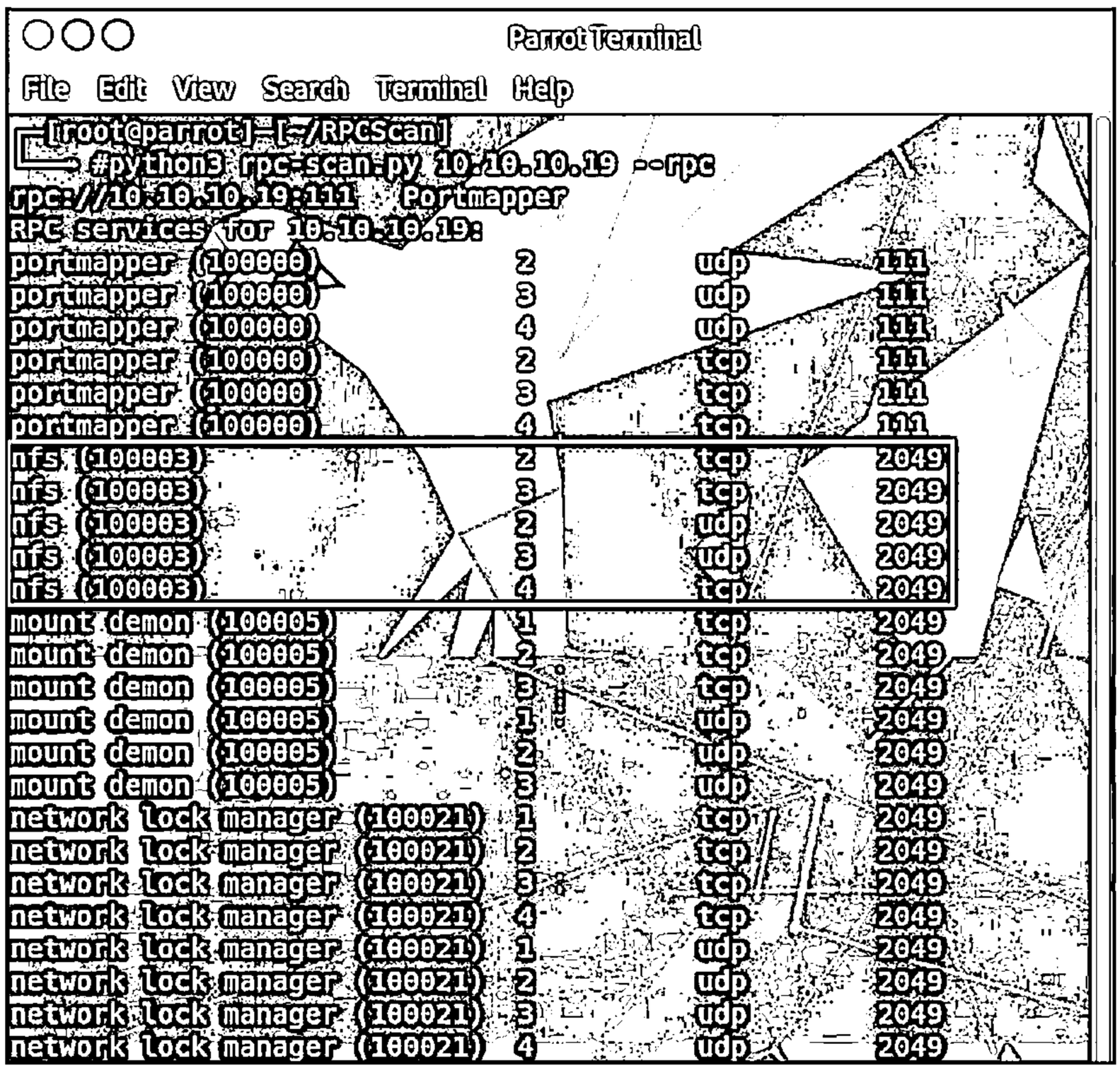


Figure 4.1.15: RPCScan result

27. This concludes the demonstration of performing NFS enumeration using SuperEnum and RPCScan.

28. Close all open windows and document all the acquired information.

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

29. Turn off the **Windows Server 2019** and **Parrot Security** virtual machines.

Lab Analysis

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

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT 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

Perform DNS Enumeration

DNS enumeration is a process that locates and lists all possible DNS records for a target domain, including usernames.

ICON KEY

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

Lab Scenario

As a professional ethical hacker or penetration tester, the next step after NFS enumeration is to perform DNS enumeration. This process yields information such as DNS server names, hostnames, machine names, usernames, IP addresses, and aliases assigned within a target domain.

Lab Objectives

- Perform DNS enumeration using zone transfer
- Perform DNS enumeration using DNSSEC zone walking

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 04 Enumeration

Lab Duration

Time: 15 Minutes

Overview of DNS Enumeration

DNS enumeration techniques are used to obtain information about the DNS servers and network infrastructure of the target organization. DNS enumeration can be performed using the following techniques:

- Zone transfer
- DNS cache snooping
- DNSSEC zone walking

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

Lab Tasks

TASK 1

Perform DNS Enumeration using Zone Transfer

DNS zone transfer is the process of transferring a copy of the DNS zone file from the primary DNS server to a secondary DNS server. In most cases, the DNS server maintains a spare or secondary server for redundancy, which holds all information stored in the main server.

Here, we will perform DNS enumeration through zone transfer by using the dig (Linux-based systems) and nslookup (Windows-based systems) tool.

1. We will begin with DNS enumeration of Linux DNS servers.
2. Start the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

If the DNS transfer setting is enabled on the target DNS server, it will give DNS information; if not, it will return an error saying it has failed or refuses the zone transfer.

3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

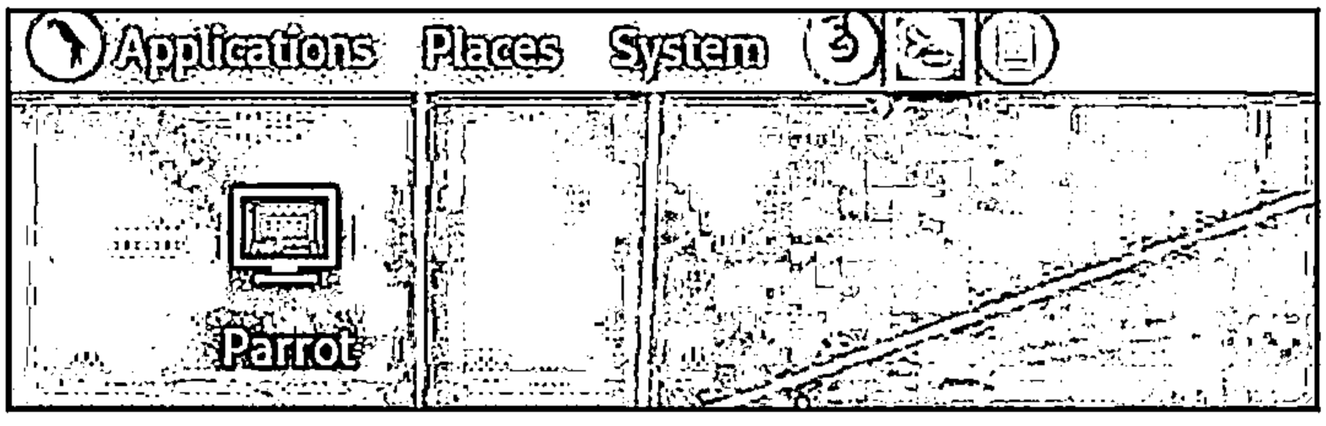


Figure 5.1.1: MATE Terminal Icon

4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

6. Now, type **cd** and press **Enter** to jump to the root directory.

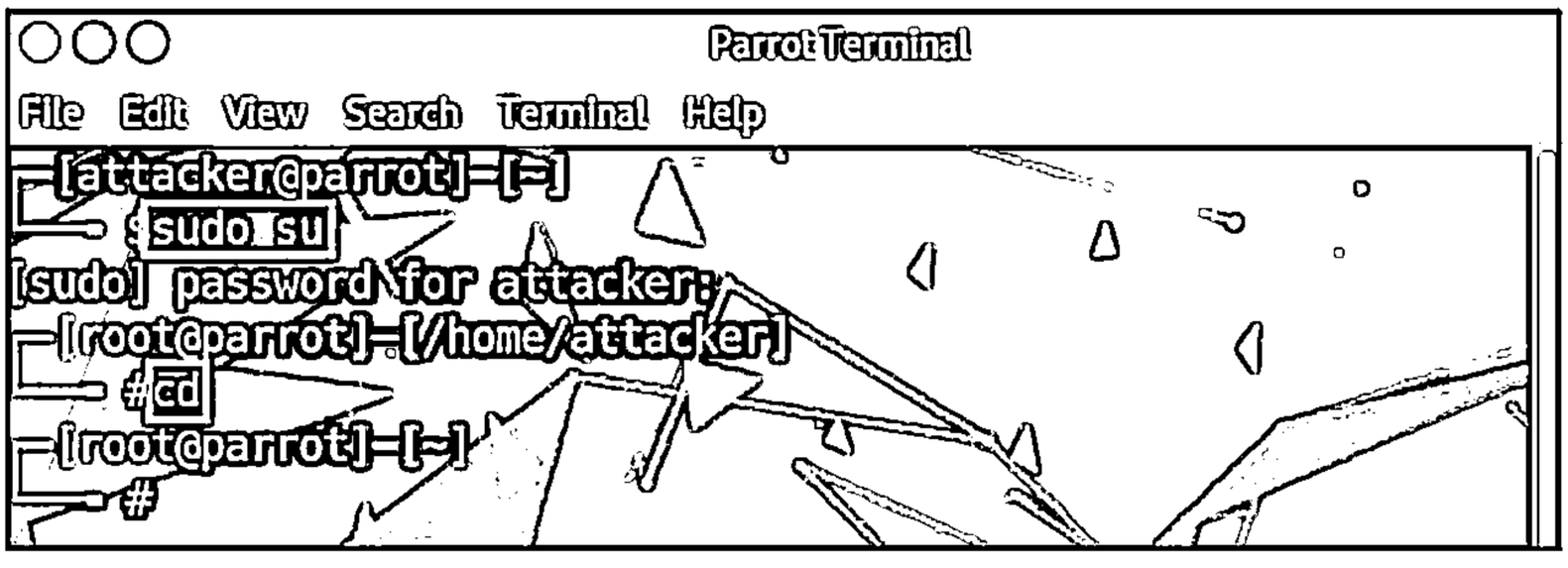


Figure 5.1.2: Running the programs as a root user

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

TASK 1.1

Gather Name Server Info using Dig

7. In the terminal window, type **dig ns <Target Domain>** (in this case, the target domain is **www.certifiedhacker.com**); press **Enter**.

Note: In this command, **ns** returns name servers in the result.

8. The above command retrieves information about all the DNS name servers of the target domain and displays it in the **ANSWER SECTION**, as shown in the screenshot.

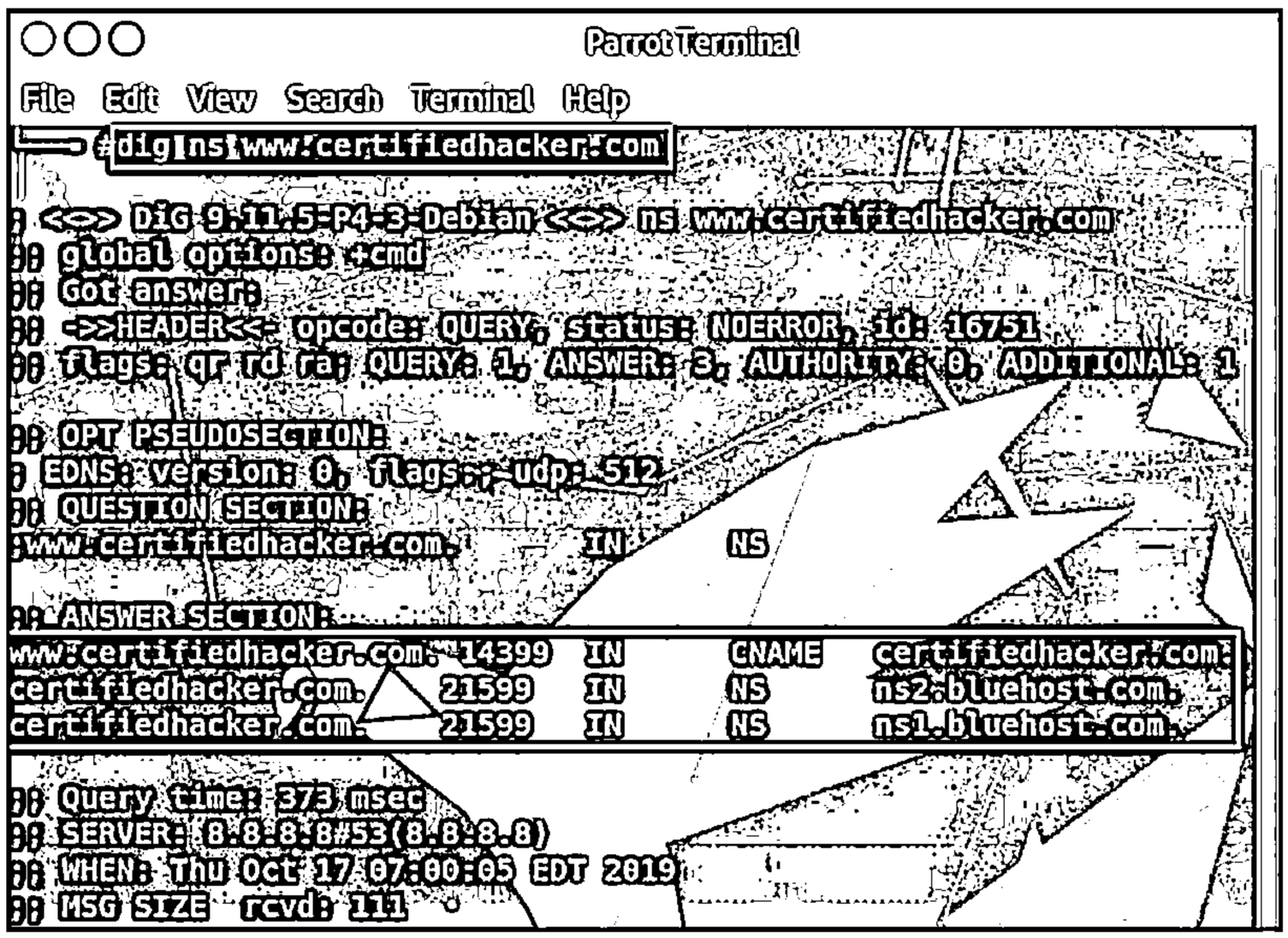


Figure 5.1.3: Result of the dig ns command

Note: On Linux-based systems, the dig command is used to query the DNS name servers to retrieve information about target host addresses, name servers, mail exchanges, etc.

TASK 1.2

Perform Zone Transfer using Dig

9. In the terminal window type **dig @<Name Server> <Target Domain> axfr** (in this example, the name server is **ns1.bluhost.com** and the target domain is **www.certifiedhacker.com**); press **Enter**.

Note: In this command, **axfr** retrieves zone information.

10. The result appears, displaying that the server is available, but that the **Transfer failed.**, as shown in the screenshot.

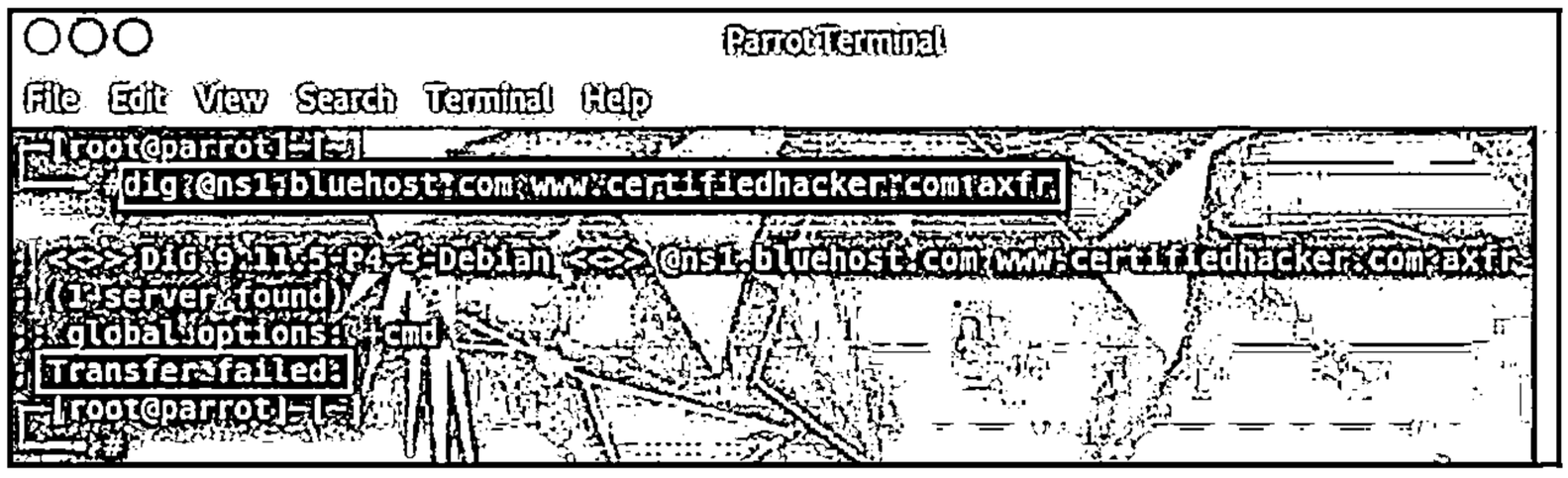


Figure 5.1.4: Result of the dig axfr command result

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

Note: After retrieving DNS name server information, the attacker can use one of the servers to test whether the target DNS allows zone transfers or not. In this case, zone transfers are not allowed for the target domain; this is why the command resulted in the message: **Transfer failed.** A penetration tester should attempt DNS zone transfers on different domains of the target organization.

TASK 1.3

Gather Name Server Info using Nslookup

11. We now move on to DNS enumeration of Windows DNS servers.
12. Start the **Windows 10** virtual machine and log in with the credentials **Admin** and **Pa$$w0rd**.
13. Click **Start** at the bottom of **Desktop**, click **Type here to search**, and type **cmd**; click **Command Prompt**.

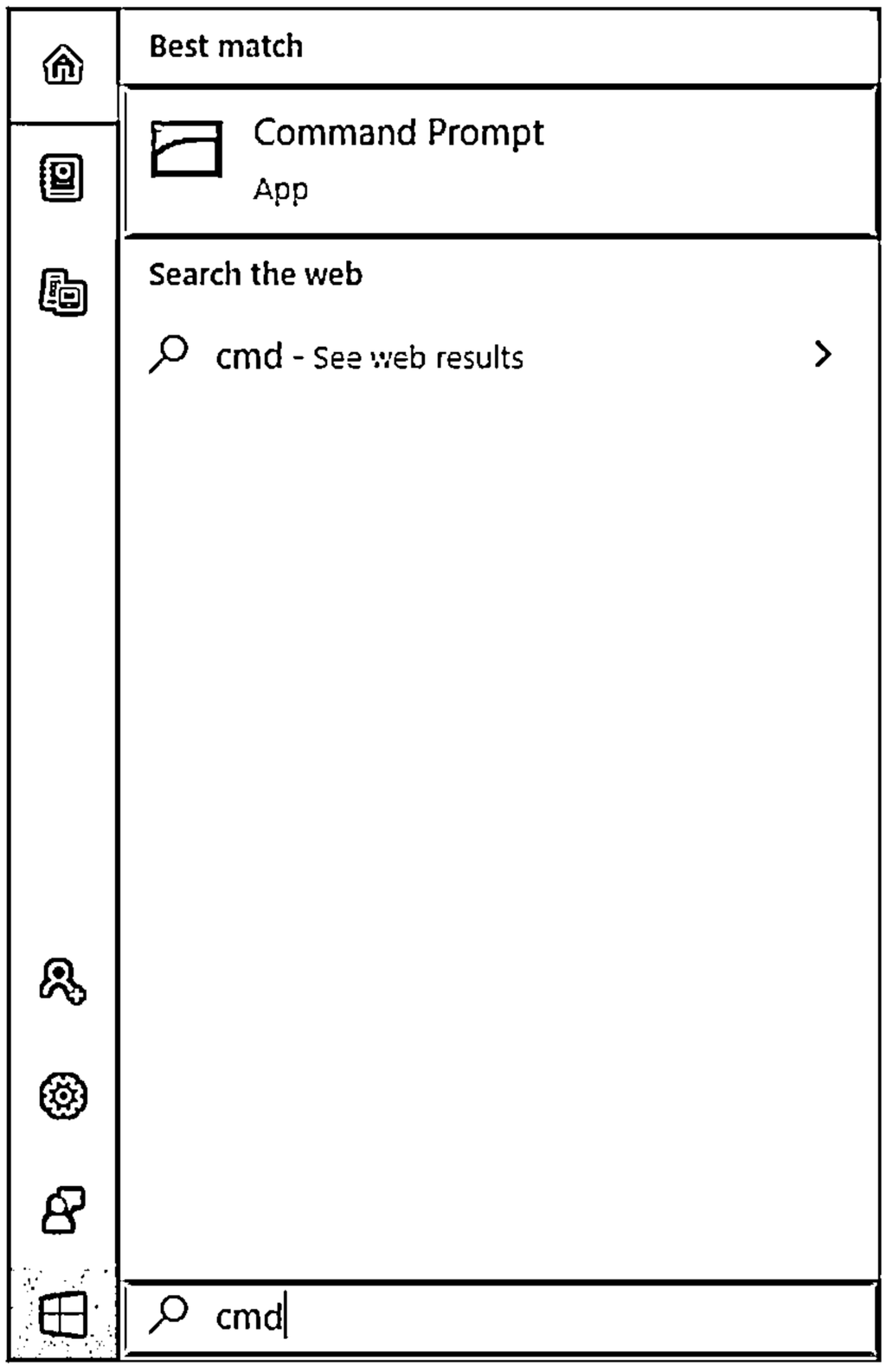


Figure 5.1.5: Open Command Prompt

14. The **Command Prompt** window appears; type **nslookup**, and press **Enter.**
15. In the nslookup **interactive** mode, type **set querytype=soa**, and press **Enter.**
16. Type the target domain **certifiedhacker.com** and press **Enter.** This resolves the target domain information.

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

Note: **set querytype=soa** sets the query type to SOA (Start of Authority) record to retrieve administrative information about the DNS zone of the target domain **certifiedhacker.com**.

17. The result appears, displaying information about the target domain such as the **primary name server** and **responsible mail addr**, as shown in the screenshot.

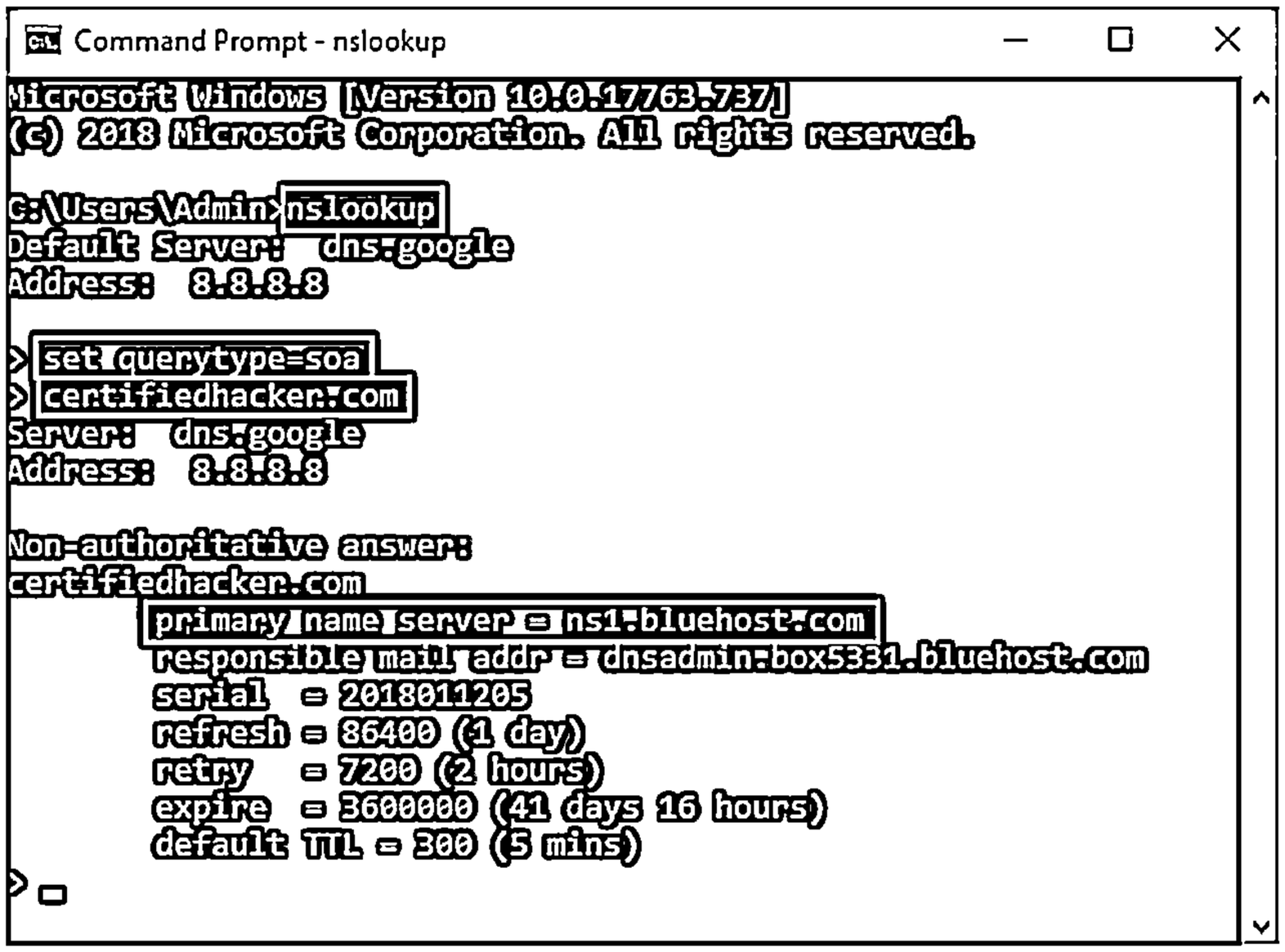


Figure 5.1.6: Results of nslookup

TASK 1.4

Perform Zone Transfer using Nslookup

18. In the **nslookup** interactive mode, type **ls -d <Name Server>** (in this example, the name is **ns1.bluehost.com**) and press **Enter**, as shown in the screenshot.

Note: In this command, **ls -d** requests a zone transfer of the specified name server.

19. The result appears, displaying that the DNS server refused the zone transfer, as shown in the screenshot.

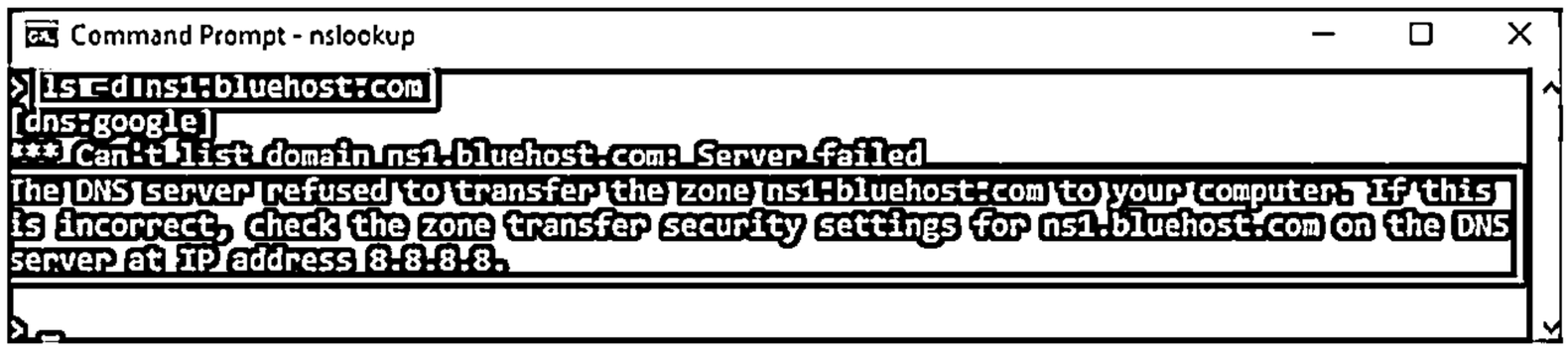


Figure 5.1.7: Result of nslookup ls -d

Note: After retrieving DNS name server information, the attacker can use one of the servers to test whether the target DNS allows zone transfers or not. In this case, the zone transfer was refused for the target domain. A

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

penetration tester should attempt DNS zone transfers on different domains of the target organization.

20. This concludes the demonstration of performing DNS zone transfer using dig and nslookup commands.
21. Close all open windows and document all the acquired information.
22. Turn off the **Windows 10** virtual machine.

TASK 2 Perform DNS Enumeration using DNSSEC Zone Walking

Here, we will use the DNSRecon tool to perform DNS enumeration through DNSSEC zone walking.

1. In the **Parrot Security** virtual machine, click the **MATE Terminal** icon at the top-left corner of **Desktop** to open a **Terminal** window.
2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

4. Now, type **cd** and press **Enter** to jump to the root directory.

TASK 2.1

Check DNSRecon Tools Options

DNSSEC zone walking is a DNS enumeration technique that is used to obtain the internal records of the target DNS server if the DNS zone is not properly configured. The enumerated zone information can assist you in building a host network map. There are various DNSSEC zone walking tools that can be used to enumerate the target domain's DNS record files.

5. A **Parrot Terminal** window appears. Type **dnsrecon -h** and press **Enter** to view all the available options in the DNSRecon tool.

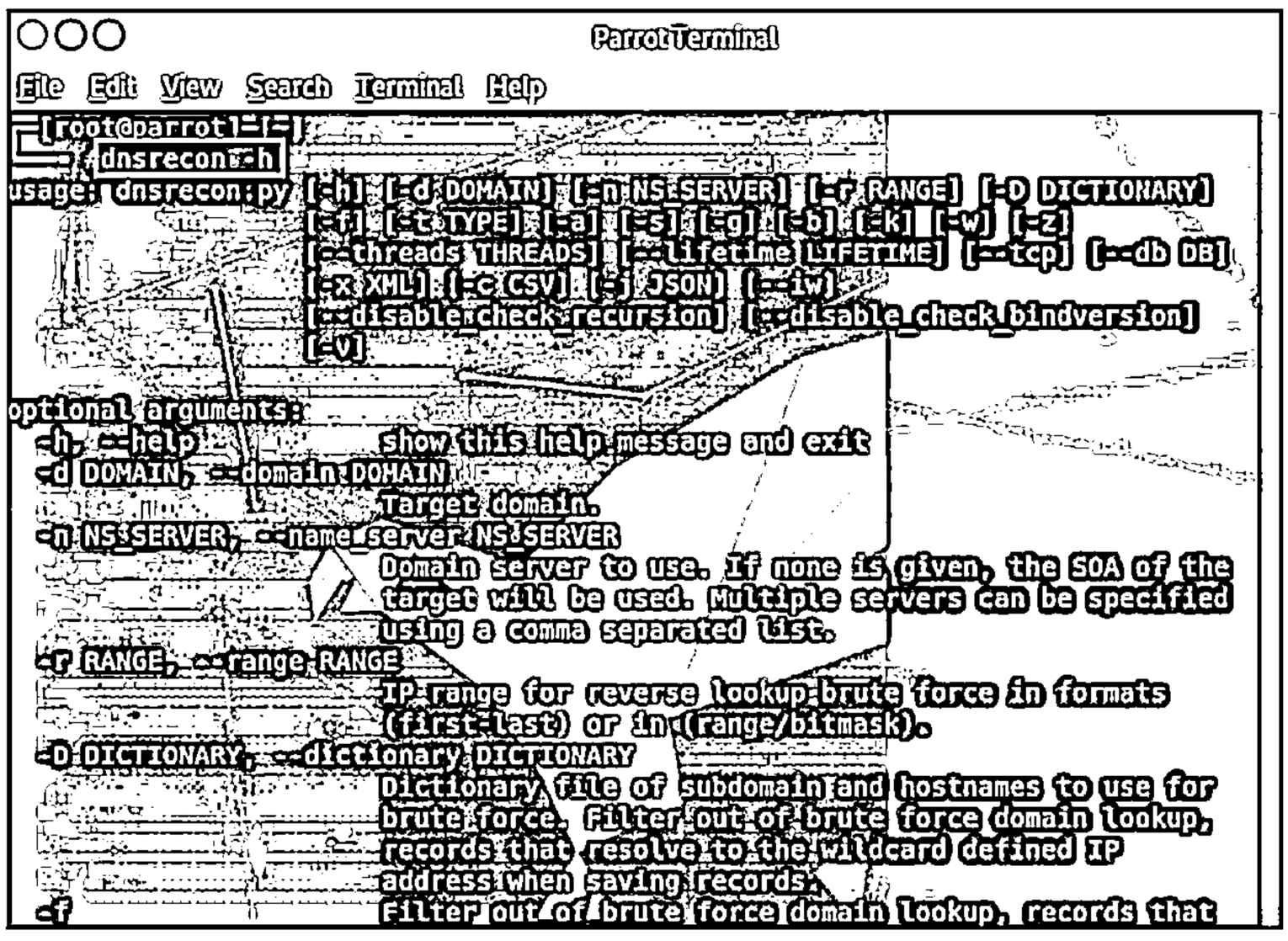


Figure 5.2.1: DNSRecon options

TASK 2.2

Perform DNSSEC Zone Walking

6. Type **dnsrecon -d <Target domain> -z** (in this example, the target domain is **www.certifiedhacker.com**); press **Enter**.

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

Note: In this command, **-d** specifies the target domain and **-z** specifies that the DNSSEC zone walk be performed with standard enumeration.

7. The result appears, displaying the enumerated DNS records for the target domain. In this case, DNS record file **A** is enumerated, as shown in the screenshot.

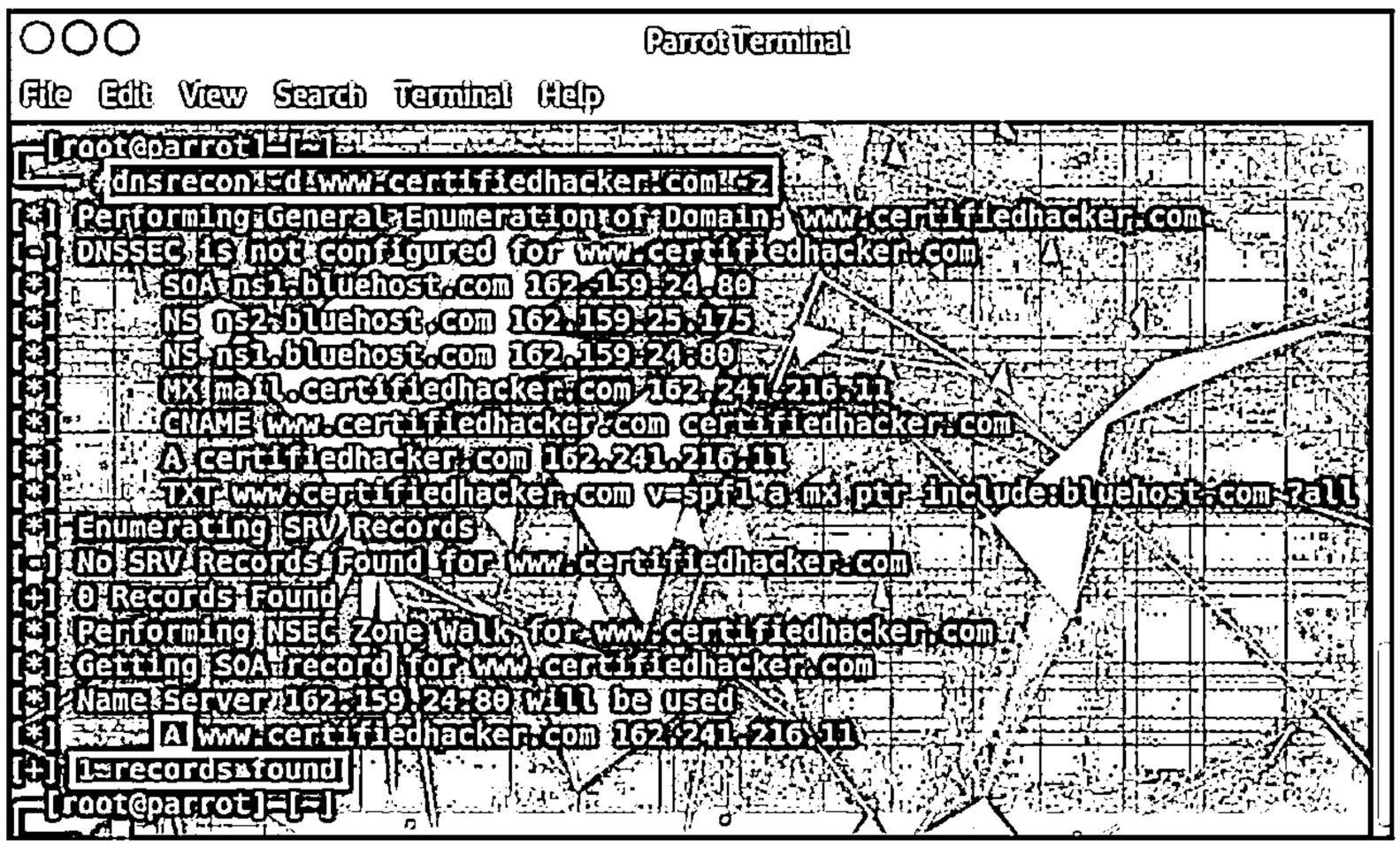


Figure 5.2.2: The DNSRecon zone walk result

You can also use other DNS enumeration tools such as **LDNS** (https://www.nlnetlabs.nl), **nsec3map** (https://github.com), **nsec3walker** (https://dnscurve.org), and **DNSwalk** (https://github.com) to perform DNS enumeration on the target domain.

Note: Using the DNSRecon tool, the attacker can enumerate general DNS records for a given domain (MX, SOA, NS, A, AAAA, SPF, and TXT). These DNS records contain digital signatures based on public-key cryptography to strengthen authentication in DNS.

8. This concludes the demonstration of performing DNS Enumeration using DNSSEC zone walking.
9. Close all open windows and document all the acquired information.
10. Turn off the **Parrot Security** virtual machine.

Lab Analysis

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

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT 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

Perform RPC, SMB, and FTP Enumeration

There are various techniques that ethical hackers and penetration testers can use to make information-gathering easier.

ICON KEY

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

Lab Scenario

As an ethical hacker or penetration tester, you should use different enumeration techniques to obtain as much information as possible about the systems in the target network. This lab will demonstrate various techniques for extracting detailed information that can be used to exploit underlying vulnerabilities in target systems, and to launch further attacks.

Lab Objectives

- Perform RPC and SMB enumeration using NetScanTools Pro
- Perform RPC, SMB, and FTP enumeration using Nmap

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 04 Enumeration

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2016 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 20 Minutes

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

Overview of Other Enumeration Techniques

Besides the methods of enumeration covered so far (NetBIOS, SNMP, LDAP, NFS, and DNS), various other techniques such as RPC, SMB, and FTP enumeration can be used to extract detailed network information about the target.

- **RPC Enumeration**: Enumerating RPC endpoints enables vulnerable services on these service ports to be identified
- **SMB Enumeration**: Enumerating SMB services enables banner grabbing, which obtains information such as OS details and versions of services running
- **FTP Enumeration**: Enumerating FTP services yields information about port 21 and any running FTP services; this information can be used to launch various attacks such as FTP bounce, FTP brute force, and packet sniffing

Lab Tasks

TASK 1 — Perform RPC and SMB Enumeration using NetScanTools Pro

Here, we will use the NetScanTools Pro tool to perform RPC and SMB enumeration.

TASK 1.1 — Launch NetScanTools Pro

1. Start the **Windows 10**, **Windows Server 2019**, and **Windows Server 2016** virtual machines.
2. Switch to the **Windows 10** virtual machine and log in with the credentials **Admin** and **Pa$$w0rd**.
3. Double-click the **NetScanTools Pro Demo** icon from **Desktop** to launch the tool.

Note: If the **Reminder** window opens, click **Start the DEMO**, and in the **DEMO Version** window, click **Start NetScanTools Pro Demo...**.

NetScanTools Pro is an integrated collection of Internet information-gathering and network-troubleshooting utilities for network professionals. The utility makes it easy to find IPv4/IPv6 addresses, hostnames, domain names, email addresses, and URLs related to the target system.

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

4. The **NetScanTools Pro** main window appears, as shown in the screenshot.

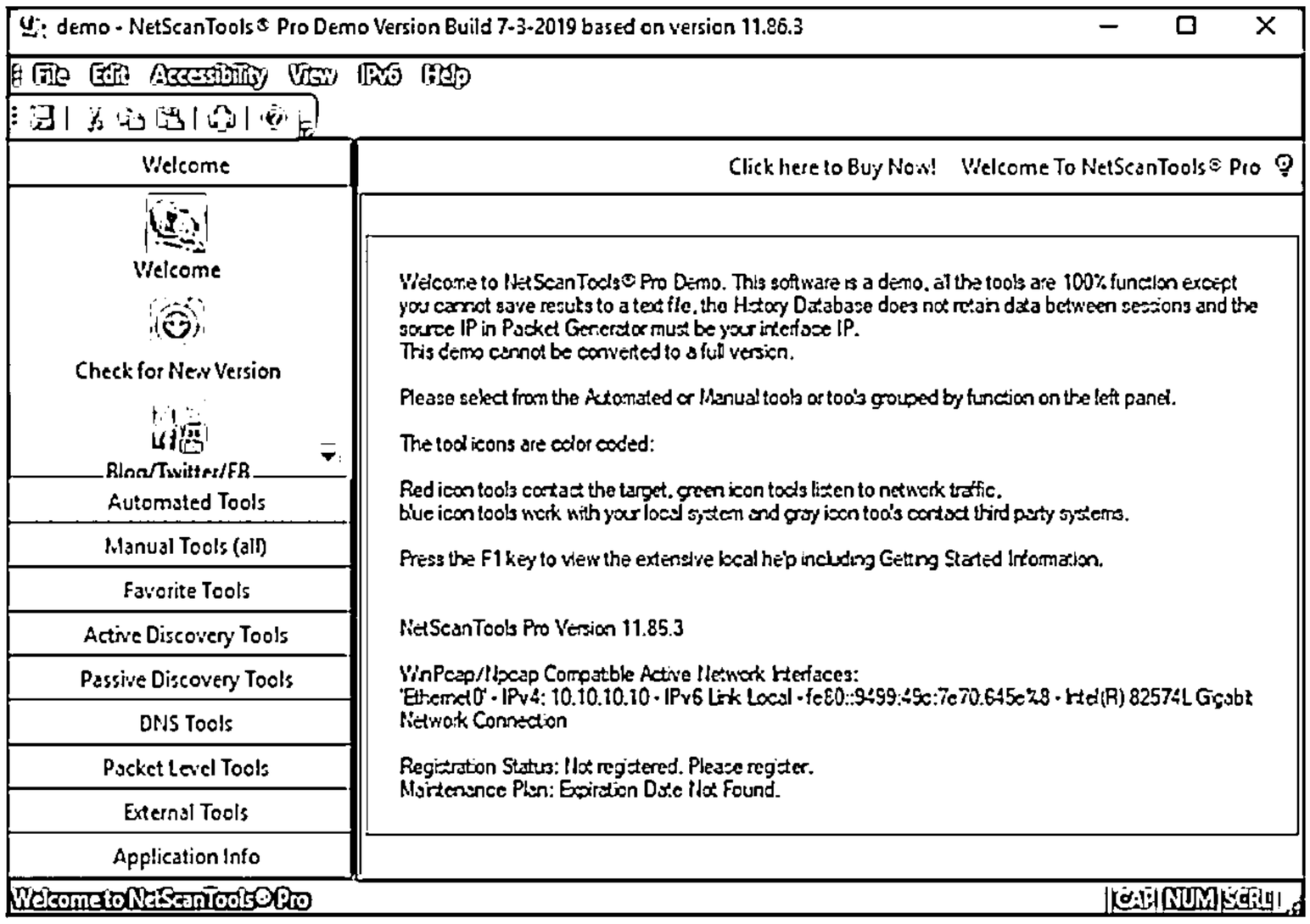


Figure 6.1.1: NetScanTools Pro main window

TASK 1.2

Perform RPC Enumeration

5. In the left pane, under **Manual Tools (all)**, scroll down and click ***nix RPC Info**, as shown in the screenshot.

Note: If a dialog box appears explaining the tool, click **OK**.

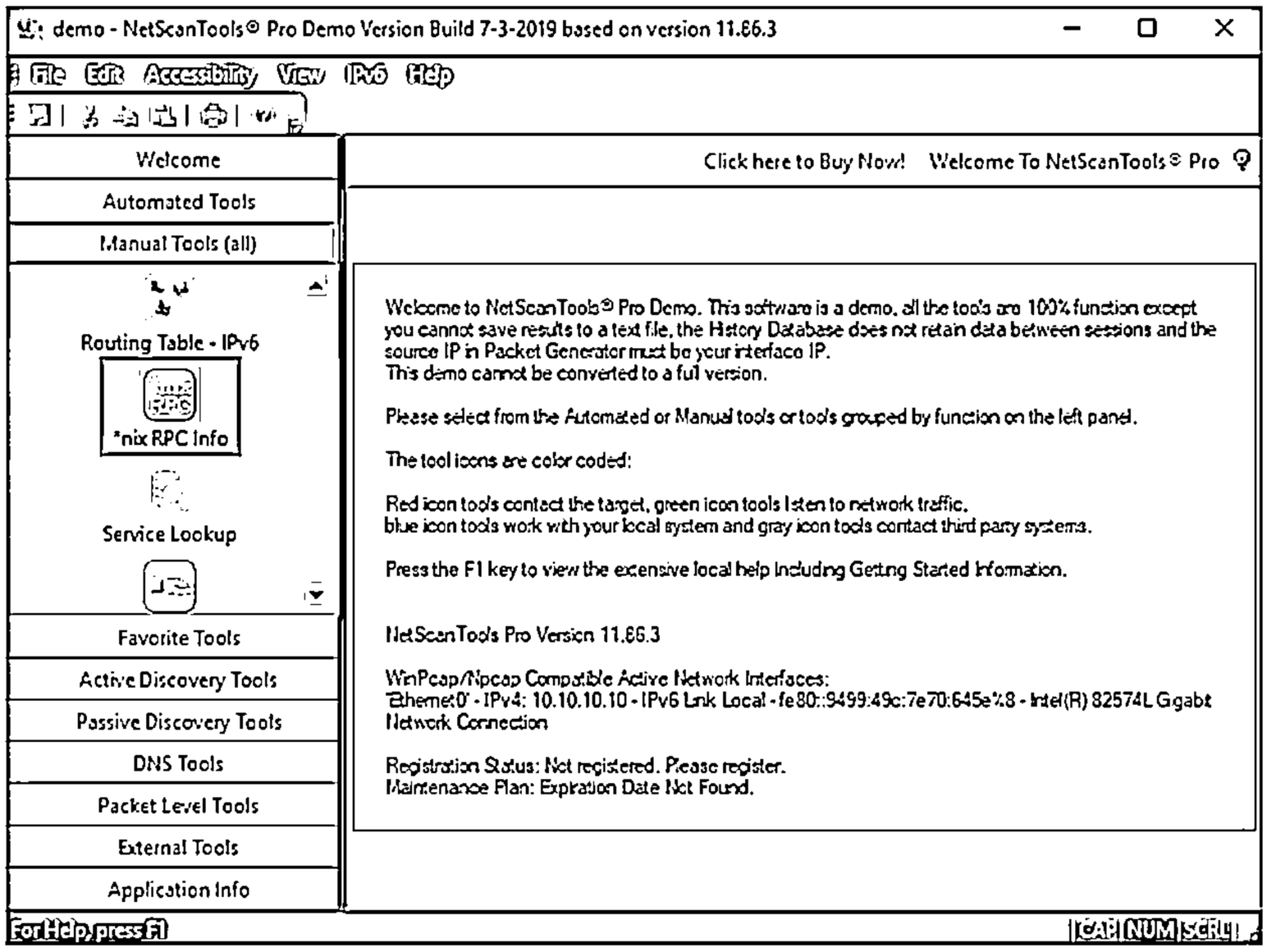


Figure 6.1.2: Select the *nix RPC info option

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

It also captures the RPC information of the target network and enables detection of and access to the Portmapper daemon/service, which typically runs on port 111 on the target machine.

6. In the **Target Hostname or IPv4 Address** field in the right pane, enter the target IP address (in this case, **10.10.10.19**) and click the **Dump Portmap** button to start RPC enumeration.

Note: In this example, we are targeting the **Windows Server 2019** virtual machine. The target IP address might differ in your lab environment.

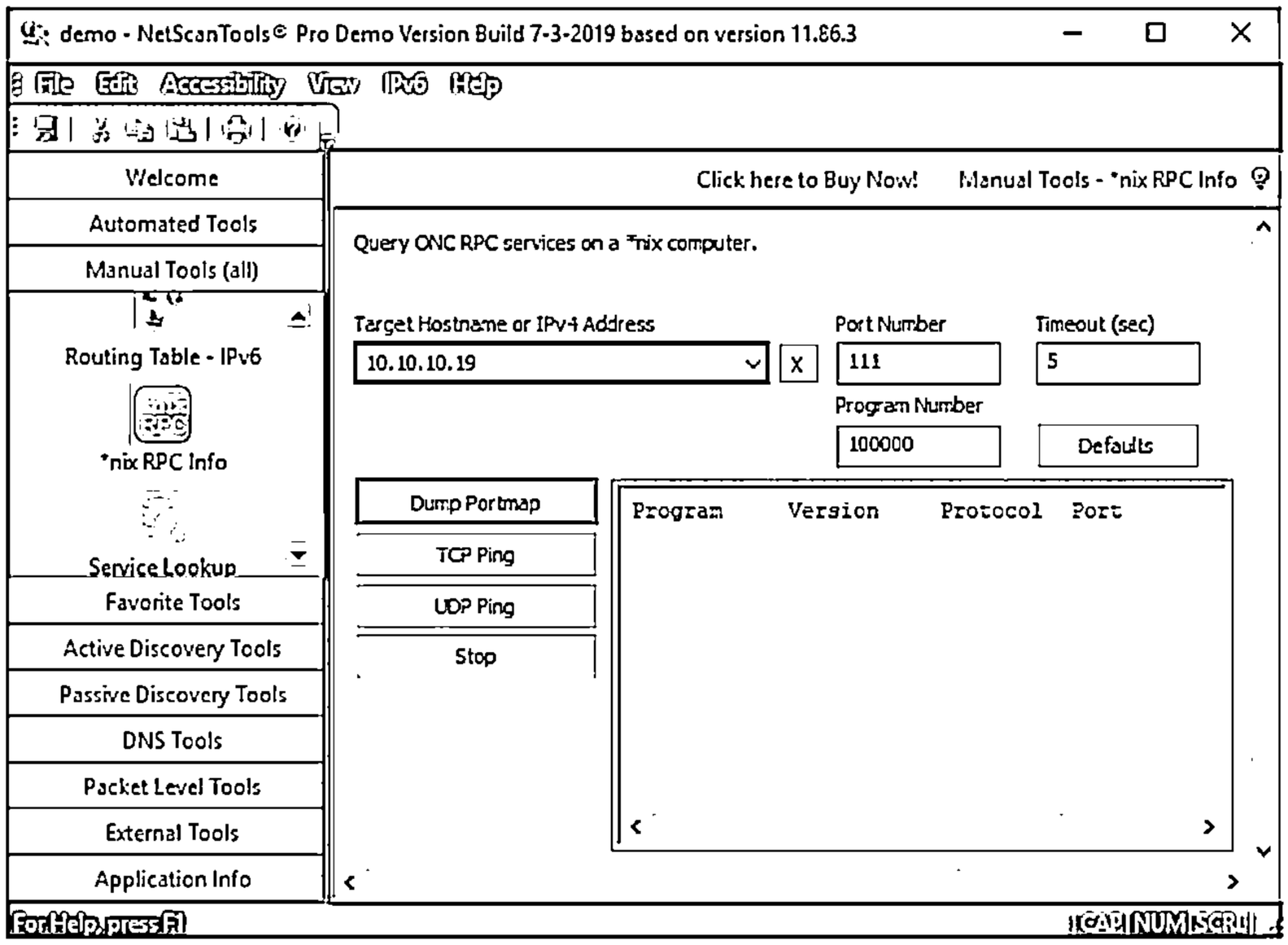


Figure 6.1.3: Performing RPC enumeration

7. The result appears, displaying the enumerated Program ID, Version, Protocol, and Port of the target system.

Note: **Dump Portmap** scans and retrieves a list of all running registered daemons (programs that run as background processes) on the target system.

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

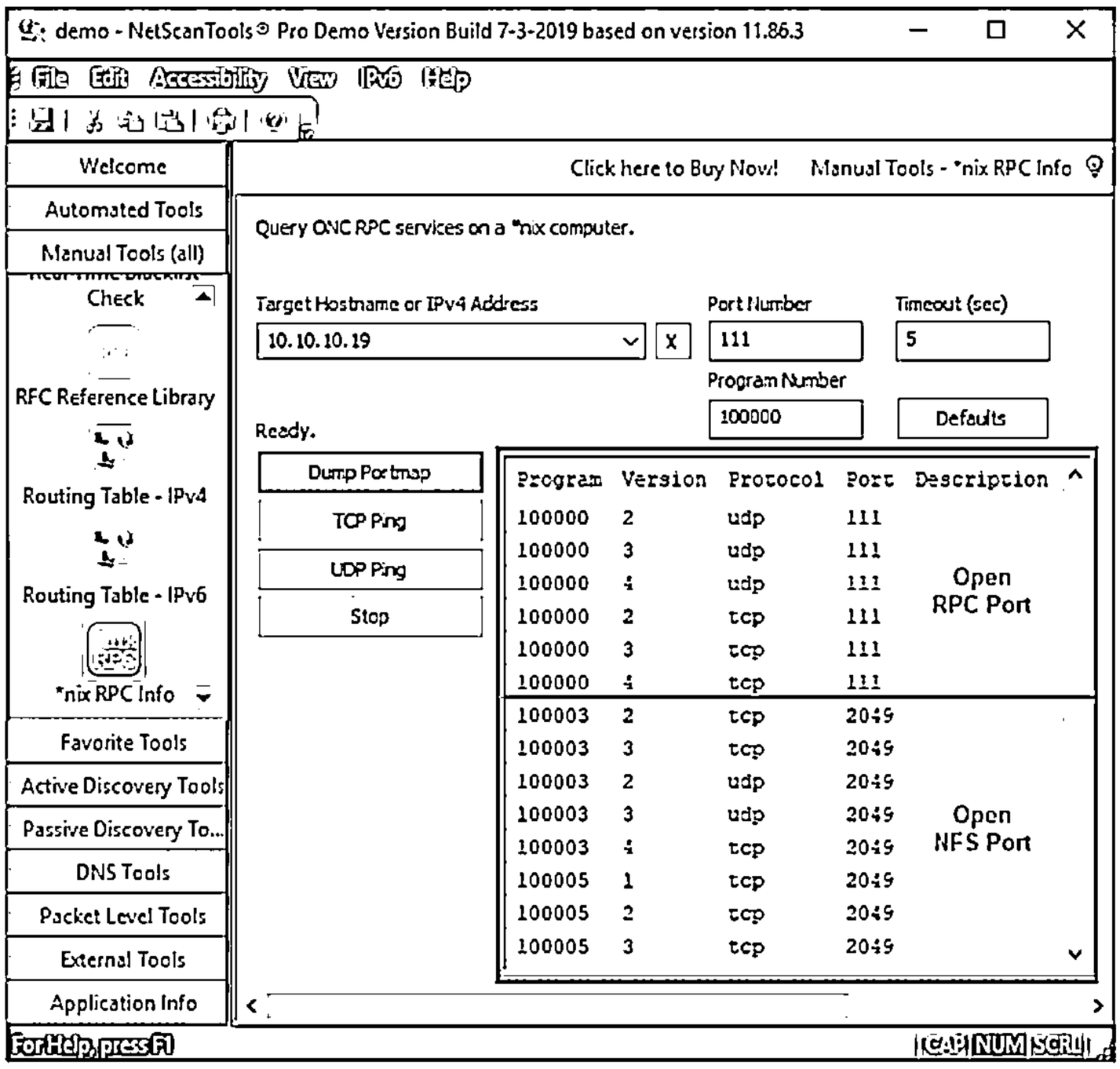


Figure 6.1.4: Scan result

TASK 1.3

Perform SMB Enumeration

8. In the left pane, under the **Manual Tools (all)** section, scroll down and click the **SMB Scanner** option, as shown in the screenshot.

Note: If a dialog box appears explaining the tool, click **OK**.

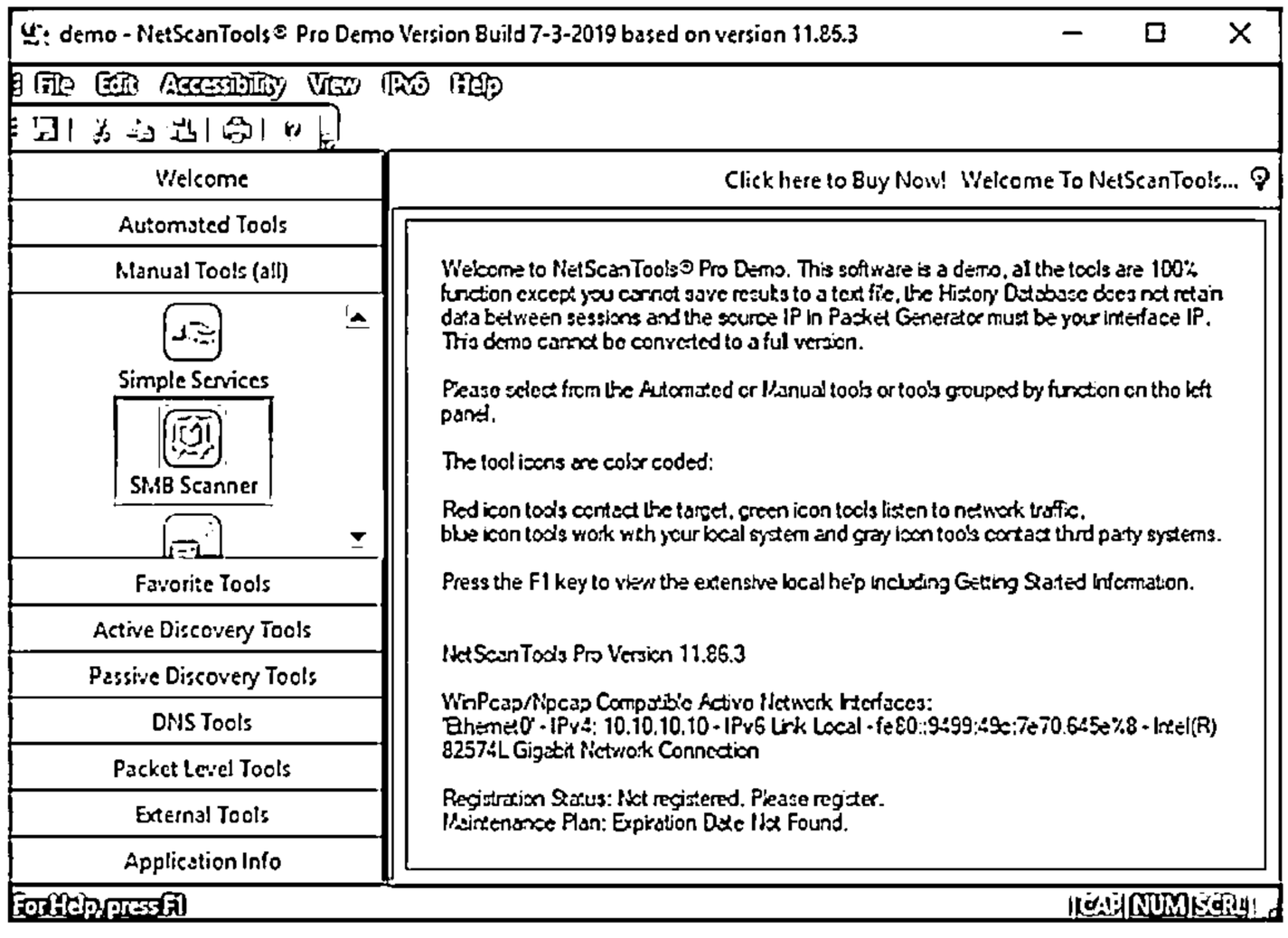


Figure 6.1.5: Performing SMB enumeration

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

9. In the right pane, click the **Start SMB Scanner (external App)** button.

Note: If the **Demo Version Message** pop-up appears, click **OK**. In the **Reminder** window, click **Start the DEMO**.

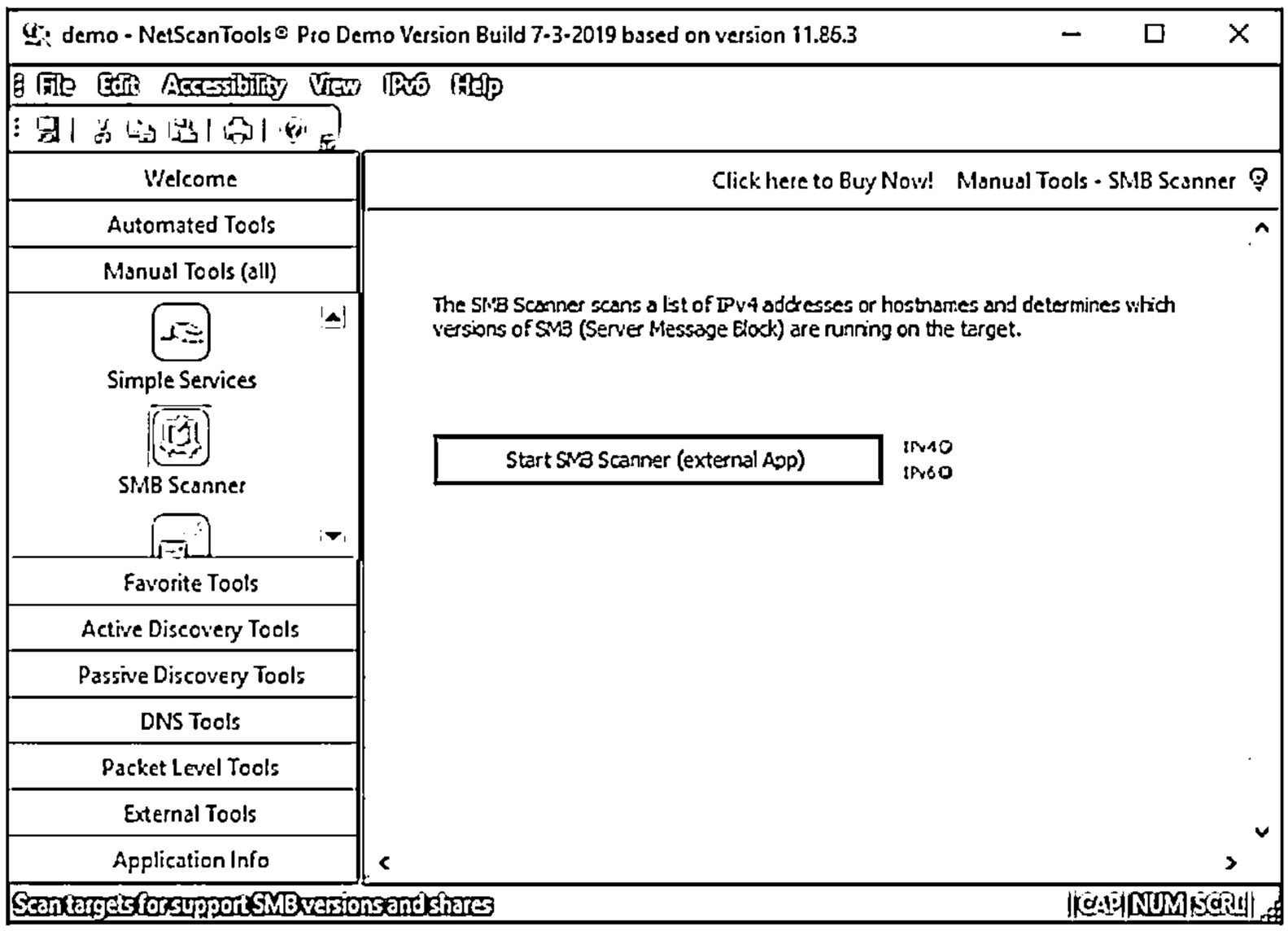


Figure 6.1.6: Launching SMB Scanner

10. The **SMB Scanner** window appears; click the **Edit Target List** button.

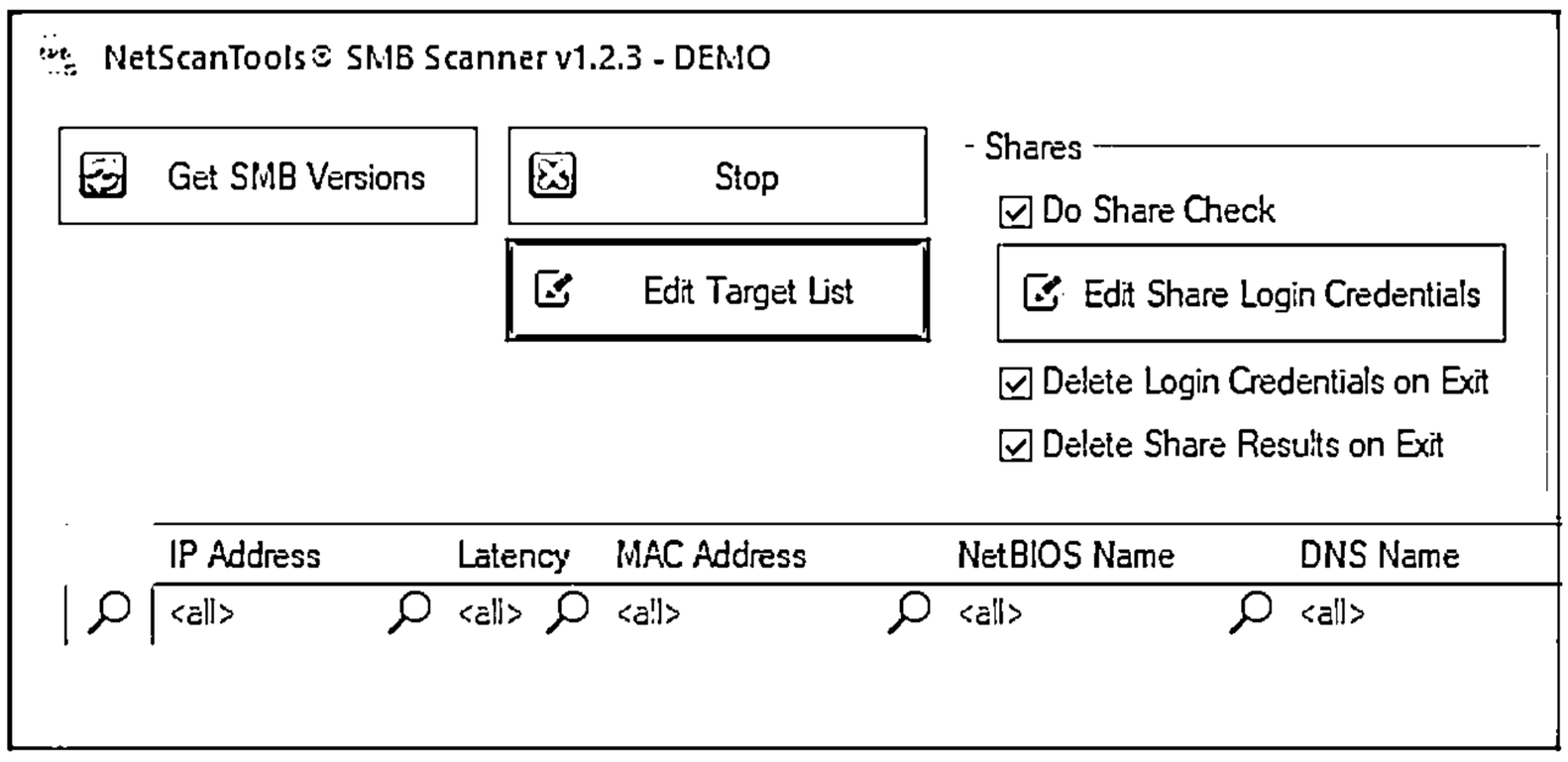


Figure 6.1.7: Click Edit Target List

TASK 1.4

Add Target IP Addresses

11. The **Edit Target List** window appears. In the **Hostname or IPv4 Address** field, enter the target IP address (**10.10.10.19**, in this example). Click the **Add to List** button to add the target IP address to **Target List.**
12. Similarly, add another target IP address (**10.10.10.16**, in this example) to **Target List** and click **OK**.

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

Note: In this task, we are targeting the **Windows Server 2019** (10.10.10.19) and **Windows Server 2016** (10.10.10.16) virtual machines.

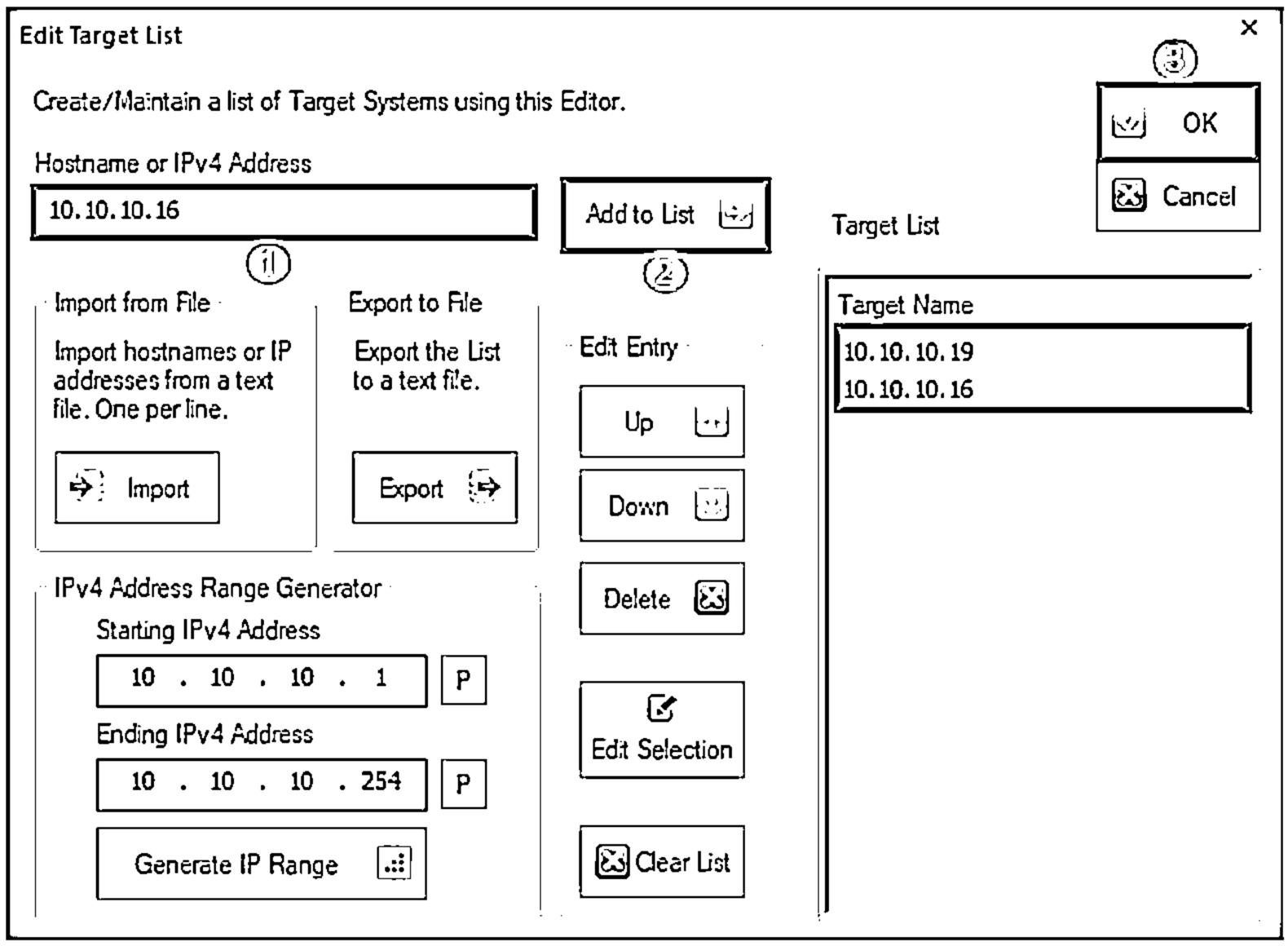


Figure 6.1.8: Adding target IP addresses

13. Now, click **Edit Share Login Credentials** to add credentials to access the target systems.

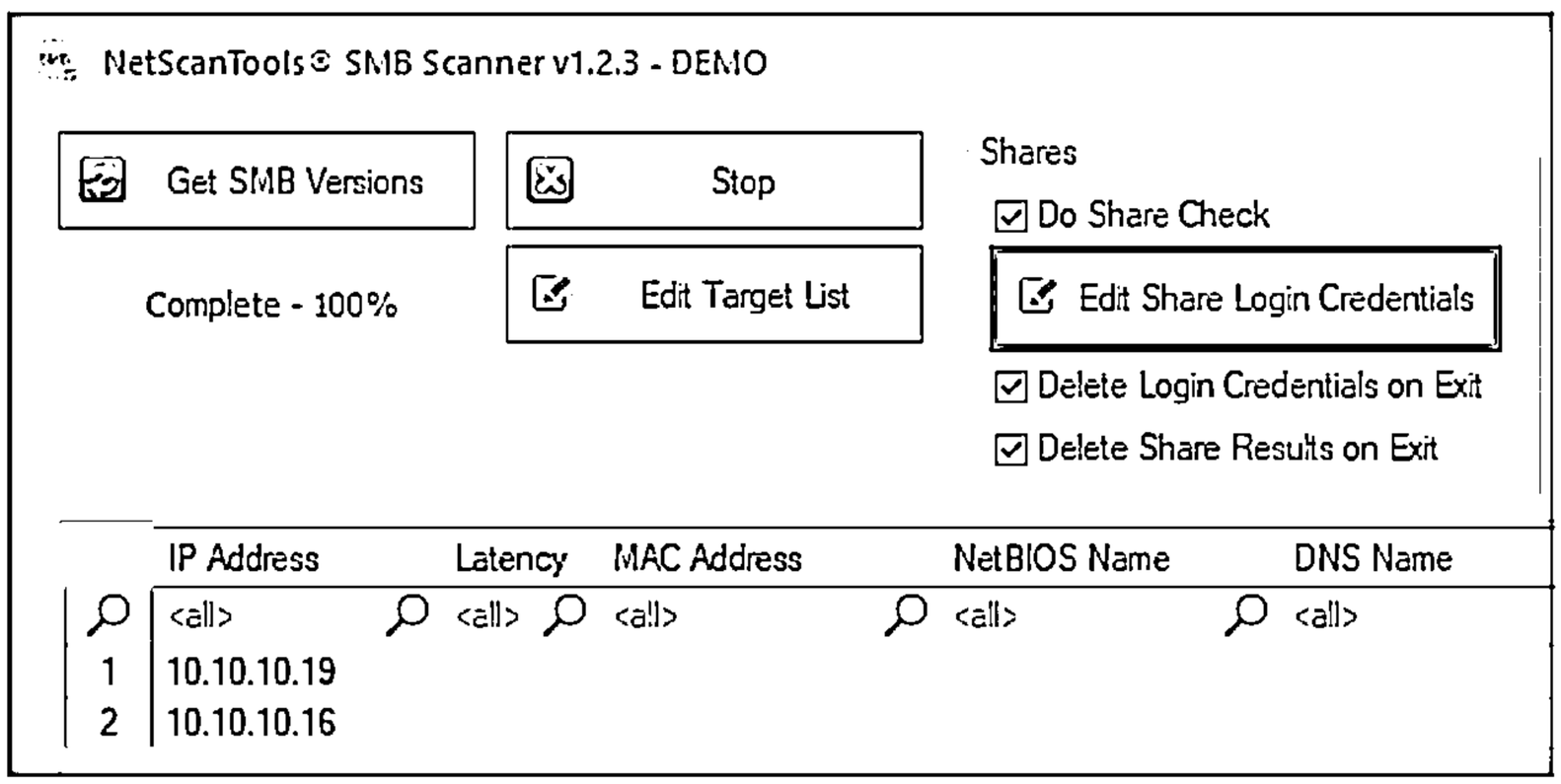


Figure 6.1.9: Click Edit Share Login Credentials

TASK 1.5

Add Login Credentials

14. The **Login Credentials List for Share Checking** window appears. Enter **Administrator** and **Pa$$w0rd** in the **Username** and **Password** fields, respectively. Click **Add to List** to add the credentials to the list and click **OK**.

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

Note: In this task, we are using the login credentials for the **Windows Server 2019** and **Windows Server 2016** virtual machines to understand the tool. In reality, attackers may add a list of login credentials by which they can log in to the target machines and obtain the required SMB share information.

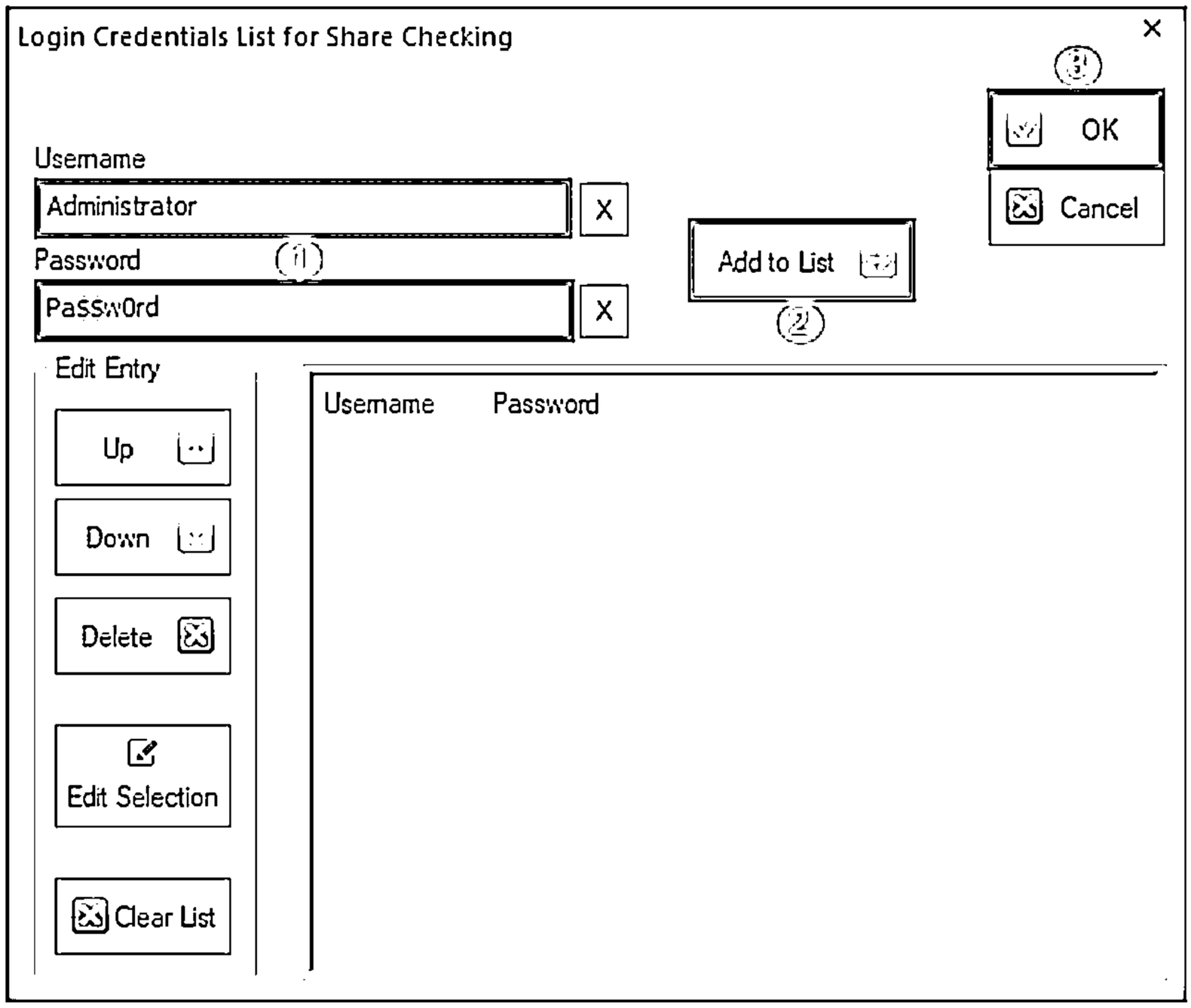


Figure 6.1.10: Adding credentials

15. In the **SMB Scanner** window, click the **Get SMB Versions** button.

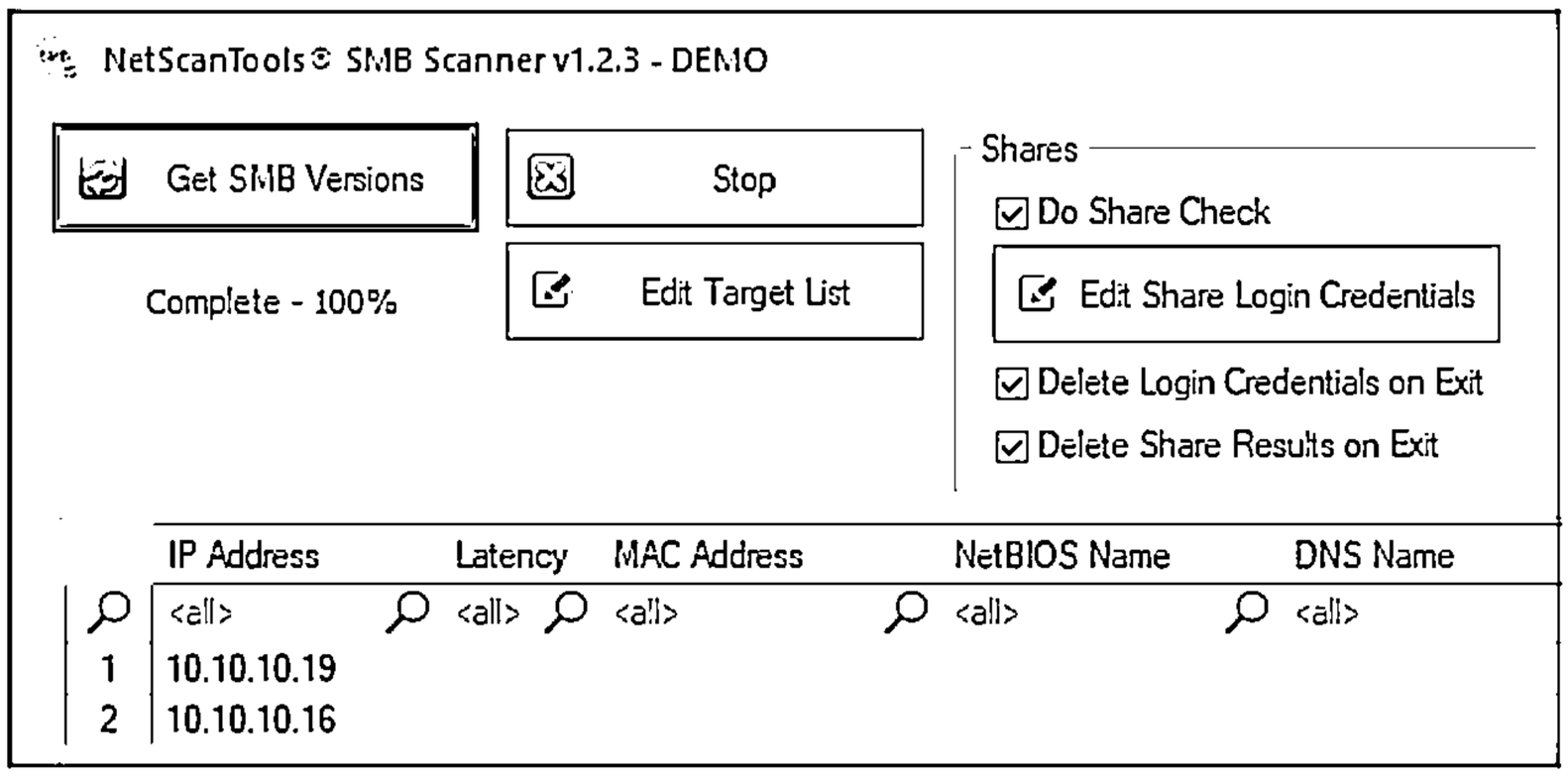


Figure 6.1.11: Running SMB Scanner

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

TASK 1.6

Analyze the Results

16. Once the scan is complete, the result appears, displaying information such as the NetBIOS Name, DNS Name, SMB versions, and Shares for each target IP address.

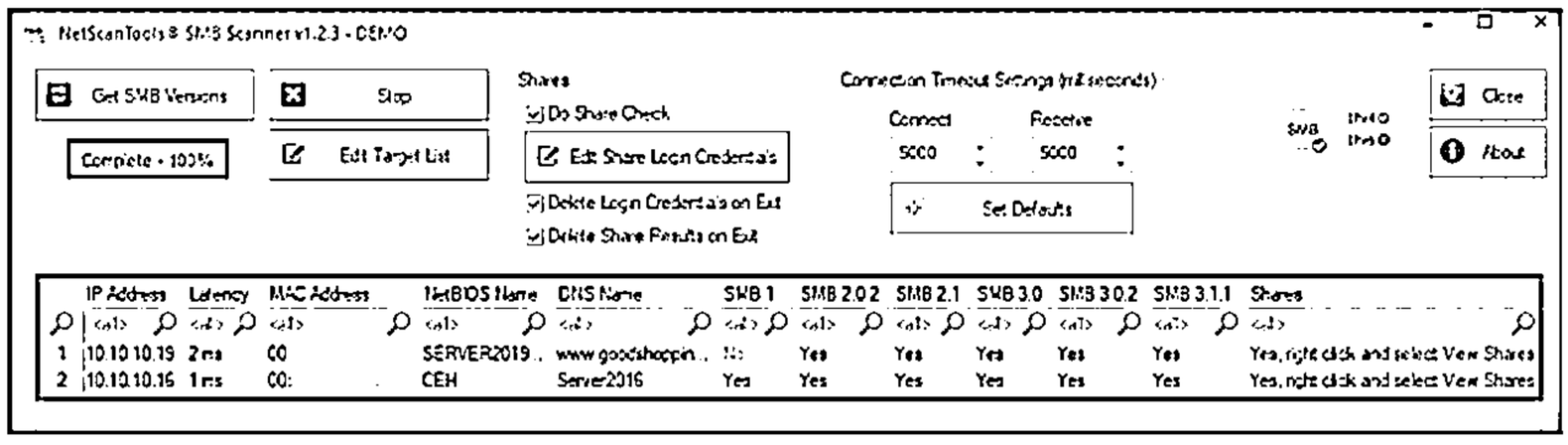


Figure 6.1.12: SMB Scanner results

17. Right-click on any of the machines (in this example, we will use **10.10.10.19**) and click **View Shares** from the available options.

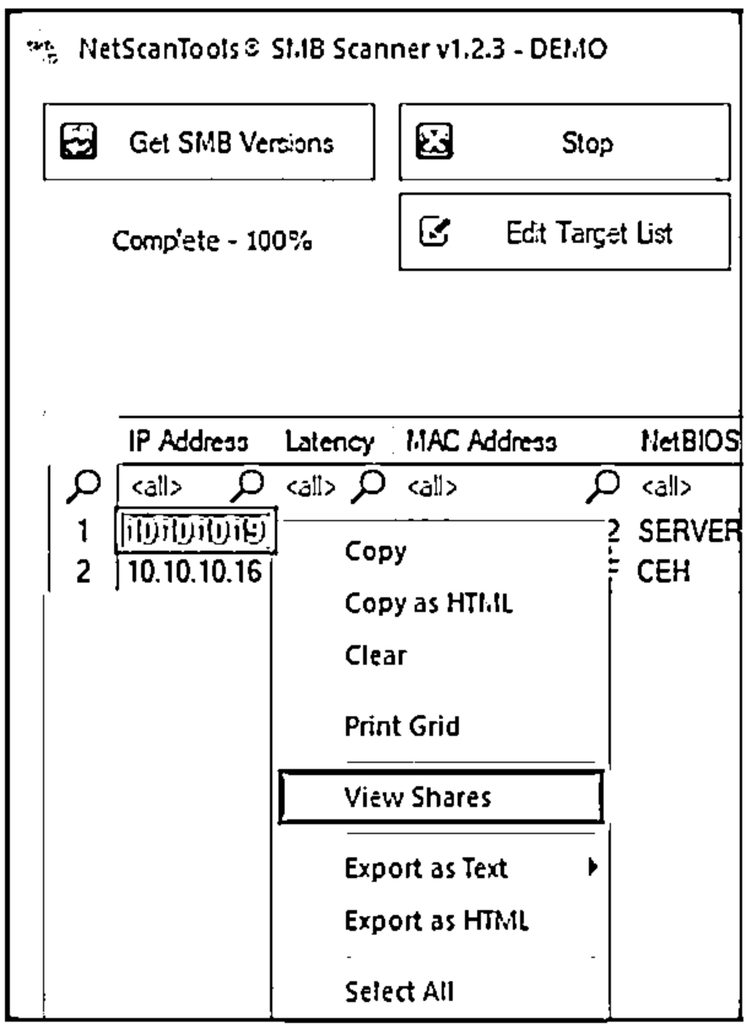


Figure 6.1.13: Clicking the View Shares option

TASK 1.7

View Shared Folders

18. The **Shares for 10.10.10.19** window appears, displaying detailed information about shared files such as Share Name, Type, Remark, Path, Permissions, and Credentials Used.

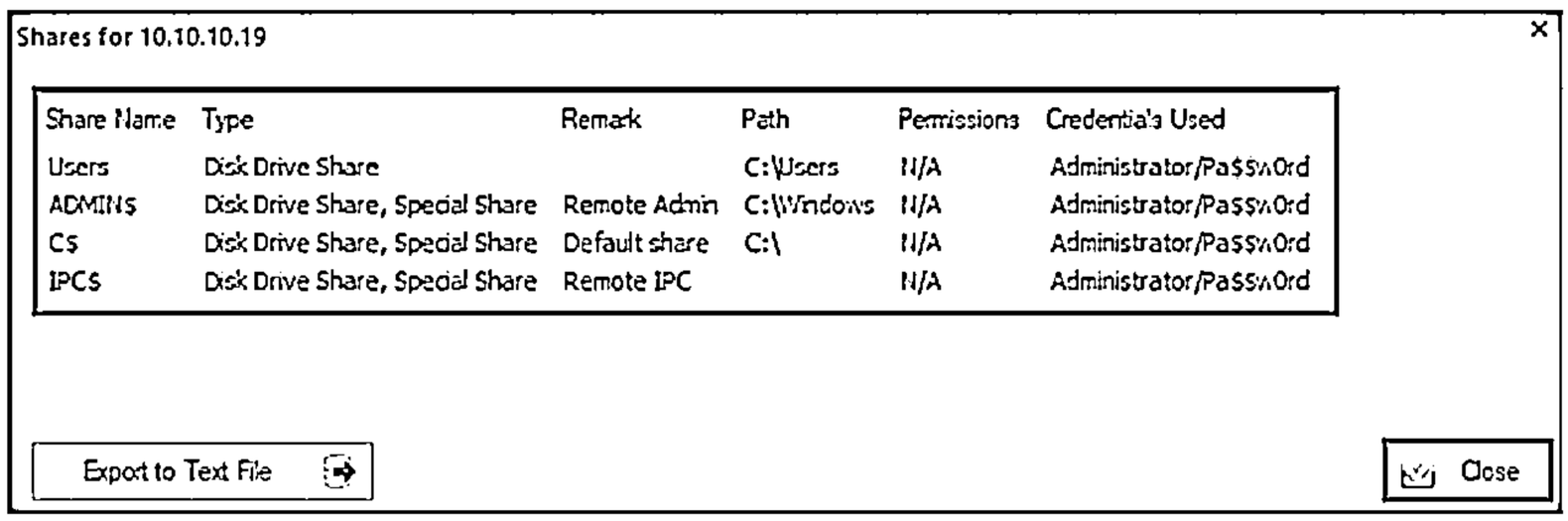


Figure 6.1.14: Shared file details

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

19. You can view the details of the shared files for the target IP address **10.10.10.16** in the same way.
20. This concludes the demonstration of performing RPC and SMB enumeration on the target systems using NetScanTools Pro.
21. Close all open windows and document all the acquired information.
22. Turn off the **Windows Server 2016** and **Windows 10** virtual machines.

TASK 2 Perform RPC, SMB, and FTP Enumeration using Nmap

Here, we will use Nmap to carry out RPC, SMB, and FTP enumeration.

Note: Before starting this lab, we must configure the FTP service in the target machine (**Windows Server 2019**). To do so, follow **Steps 1-10**.

TASK 2.1 Configure FTP Service

Nmap is a utility used for network discovery, network administration, and security auditing. It is also used to perform tasks such as network inventory, service upgrade schedule management, and host or service uptime monitoring.

1. Log in to the **Windows Server 2019** virtual machine using the credentials **Administrator/Pa$$w0rd**.
2. Click on the **File Explorer** icon at the bottom of **Desktop**. In the **File Explorer** window, right-click on **Local Disk (C:)** and click **New → Folder**.

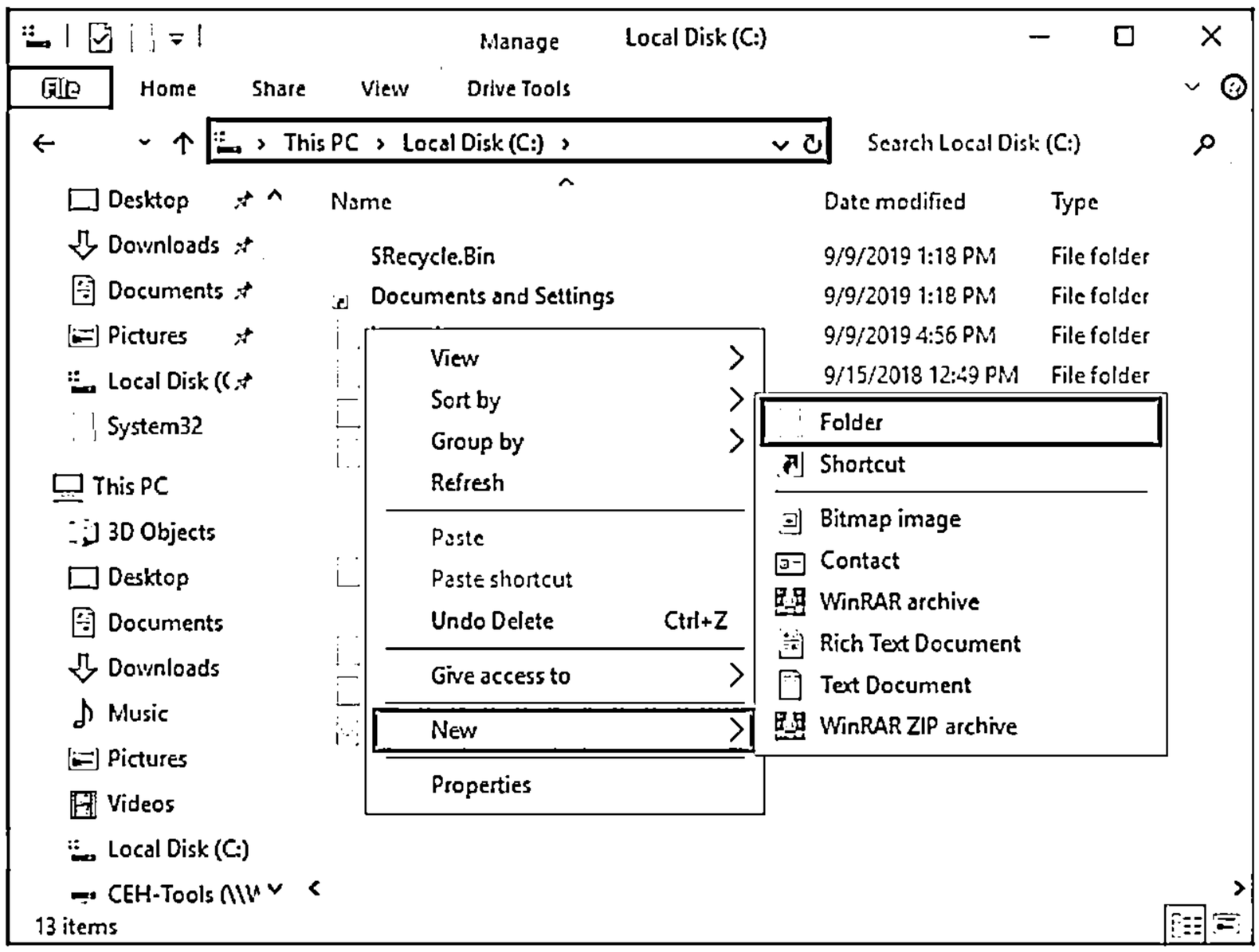


Figure 6.2.1: Creating a New Folder

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

3. A **New Folder** appears. Rename it to **FTP-Site Data**, as shown in the screenshot.

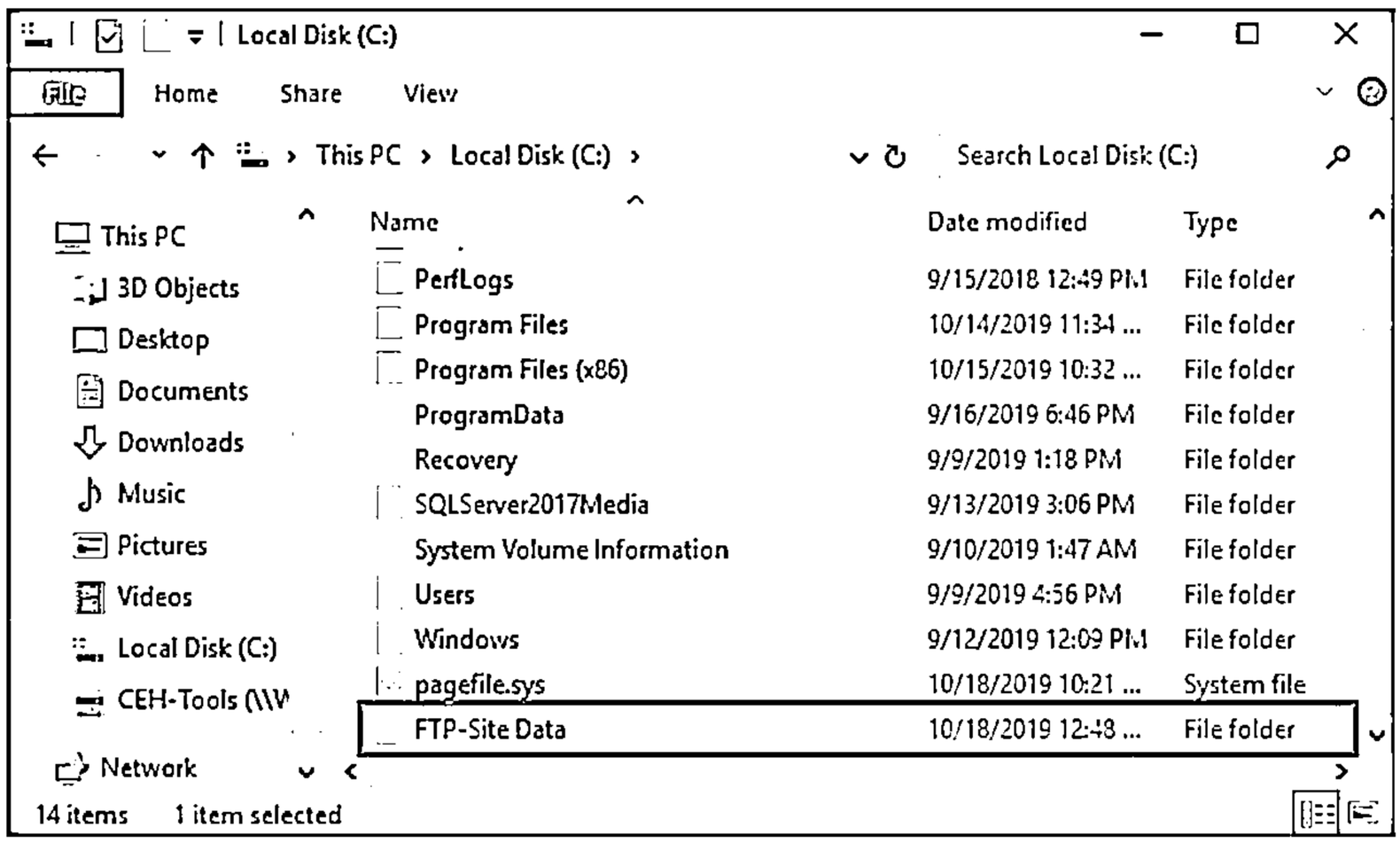


Figure 6.2.2: Renaming the Folder "FTP-Site Data"

4. Close the window and click on the **Type here to search** icon at the bottom of the **Desktop.** Type **iis**. In the search results, click on **Internet Information Services Manager (IIS) Manager**, as shown in the screenshot.

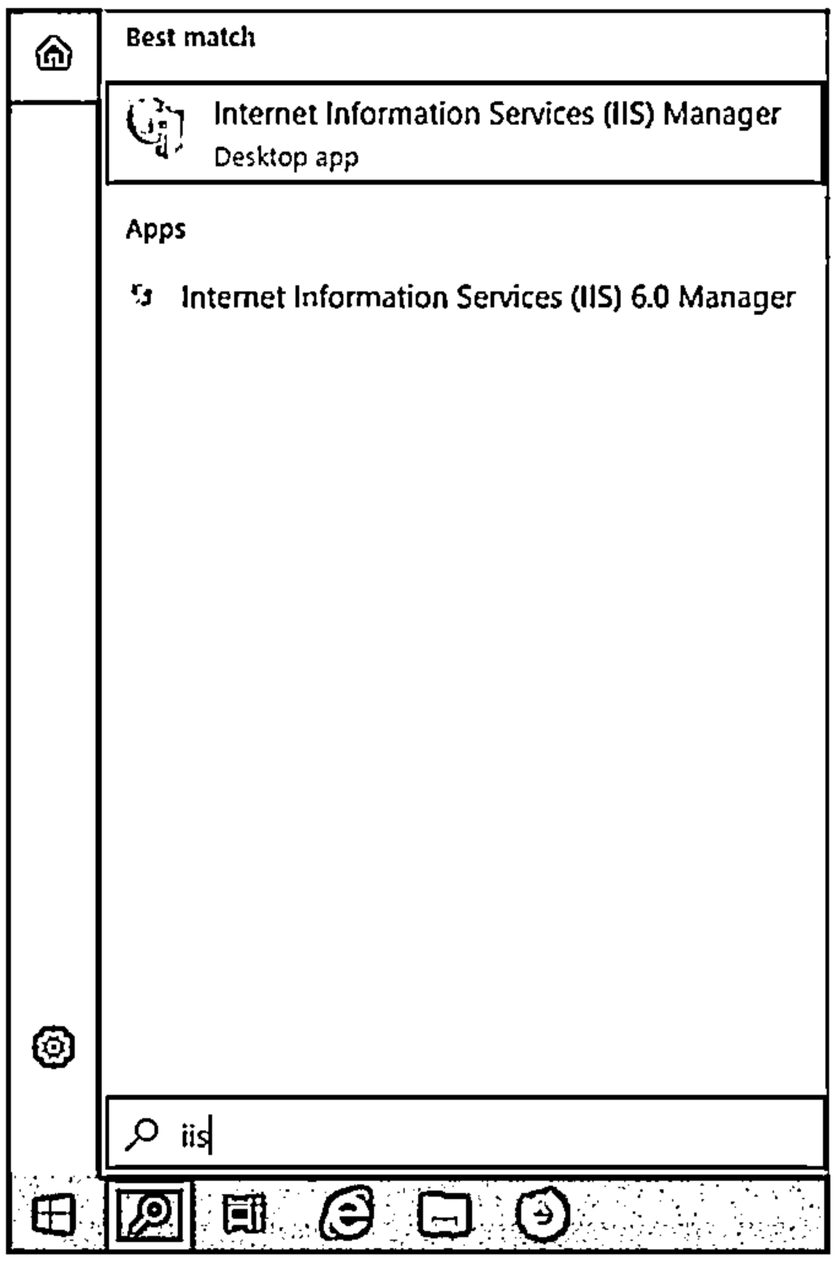


Figure 6.2.3: Search result for "iis"

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

5. In the **Internet Information Services (IIS) Manager** window, click to expand **SERVER2019 (SERVER2019\Administrator)** in the left pane. Right-click **Sites**, and then click **Add FTP Site....**

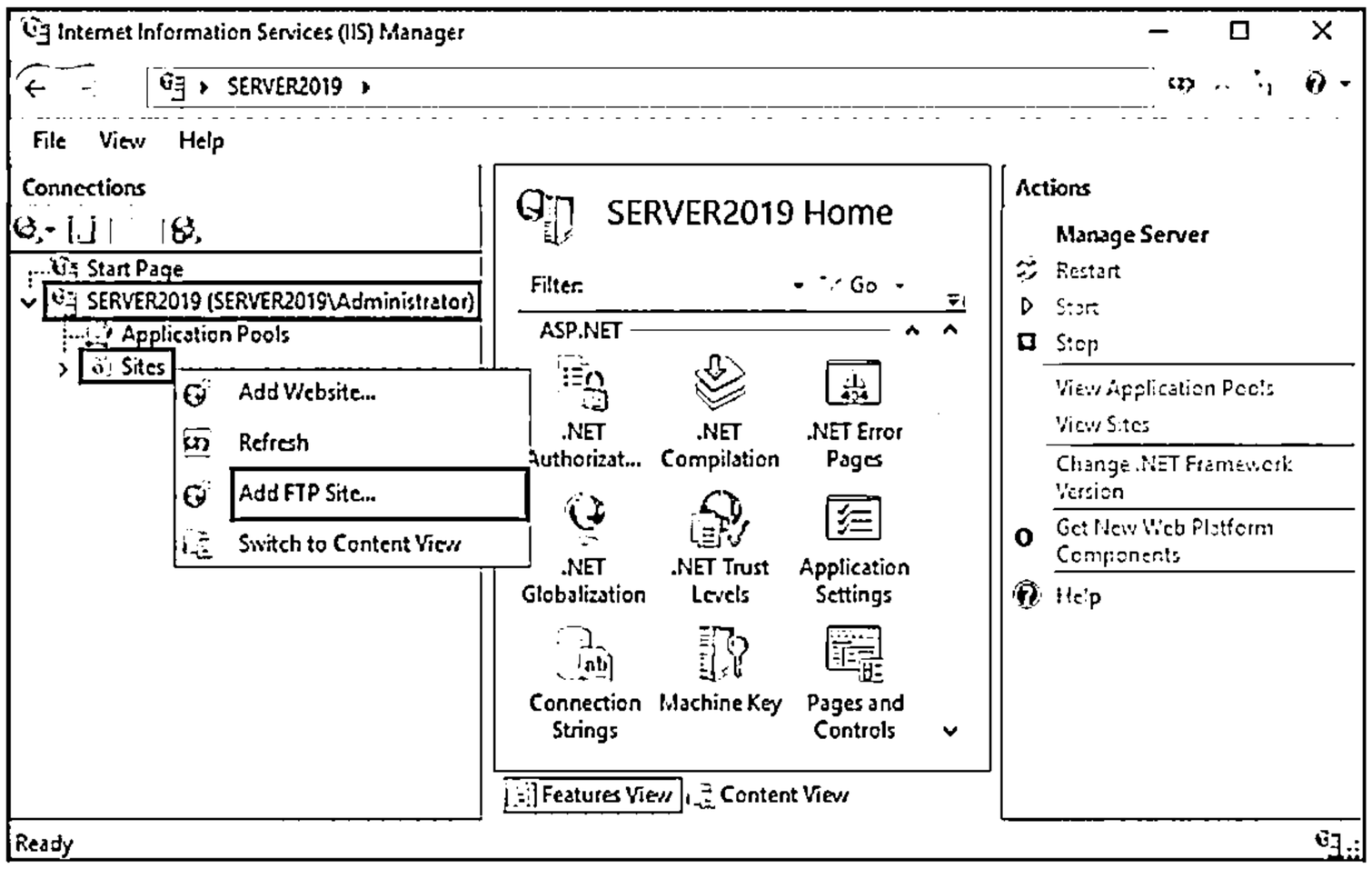


Figure 6.2.4: IIS Manager window

6. In the **Add FTP Site** window, type **CEH.com** in the **FTP site name** field.

   In the **Physical path** field, click on the (...) icon. In the **Browse For Folder** window, click **Local Disk (C:)** and **FTP-Site Data**, and then click **OK**.

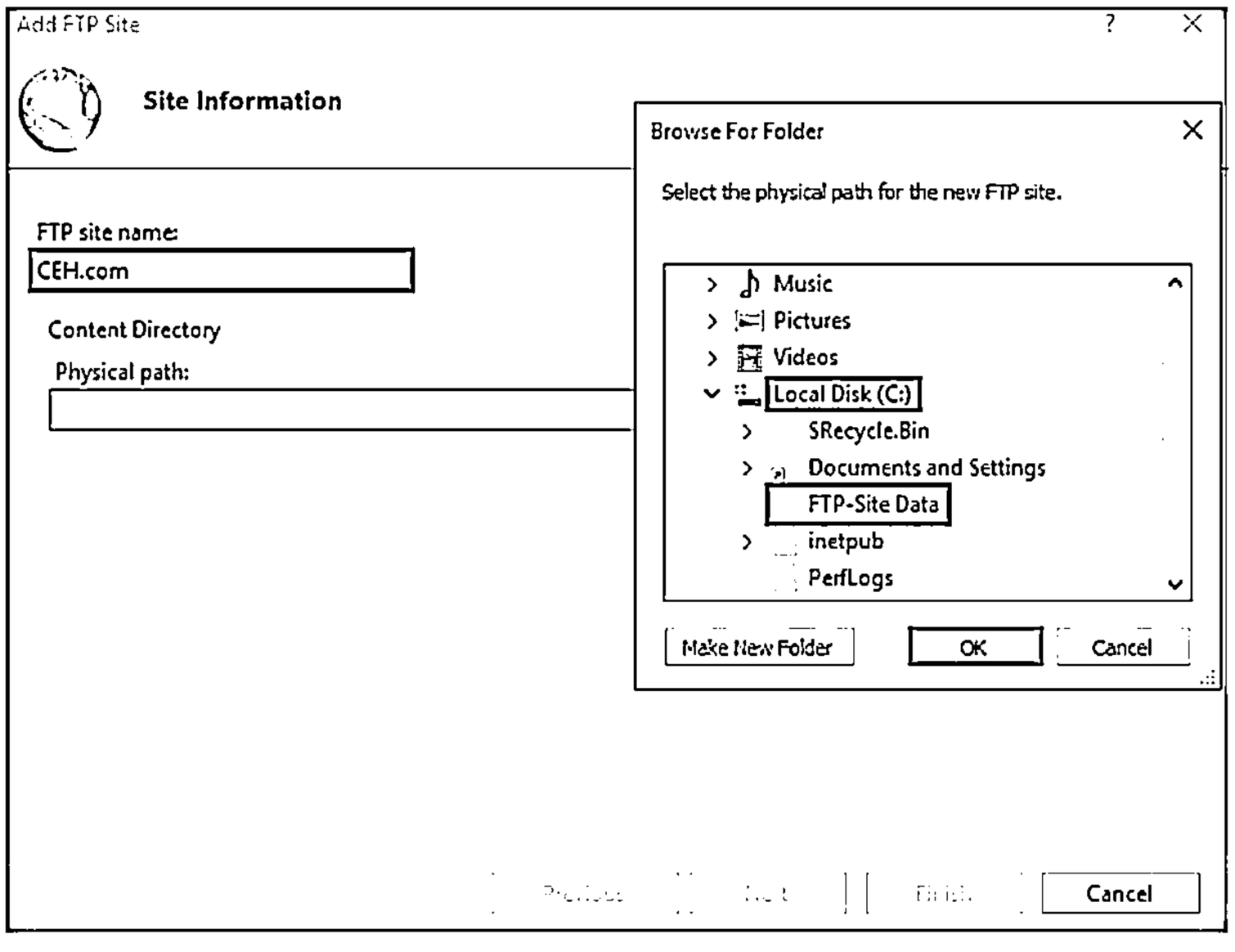


Figure 6.2.5: Entering details in the Add FTP Site window

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

7. In the **Add FTP Site** window, check the entered details and click **Next**.

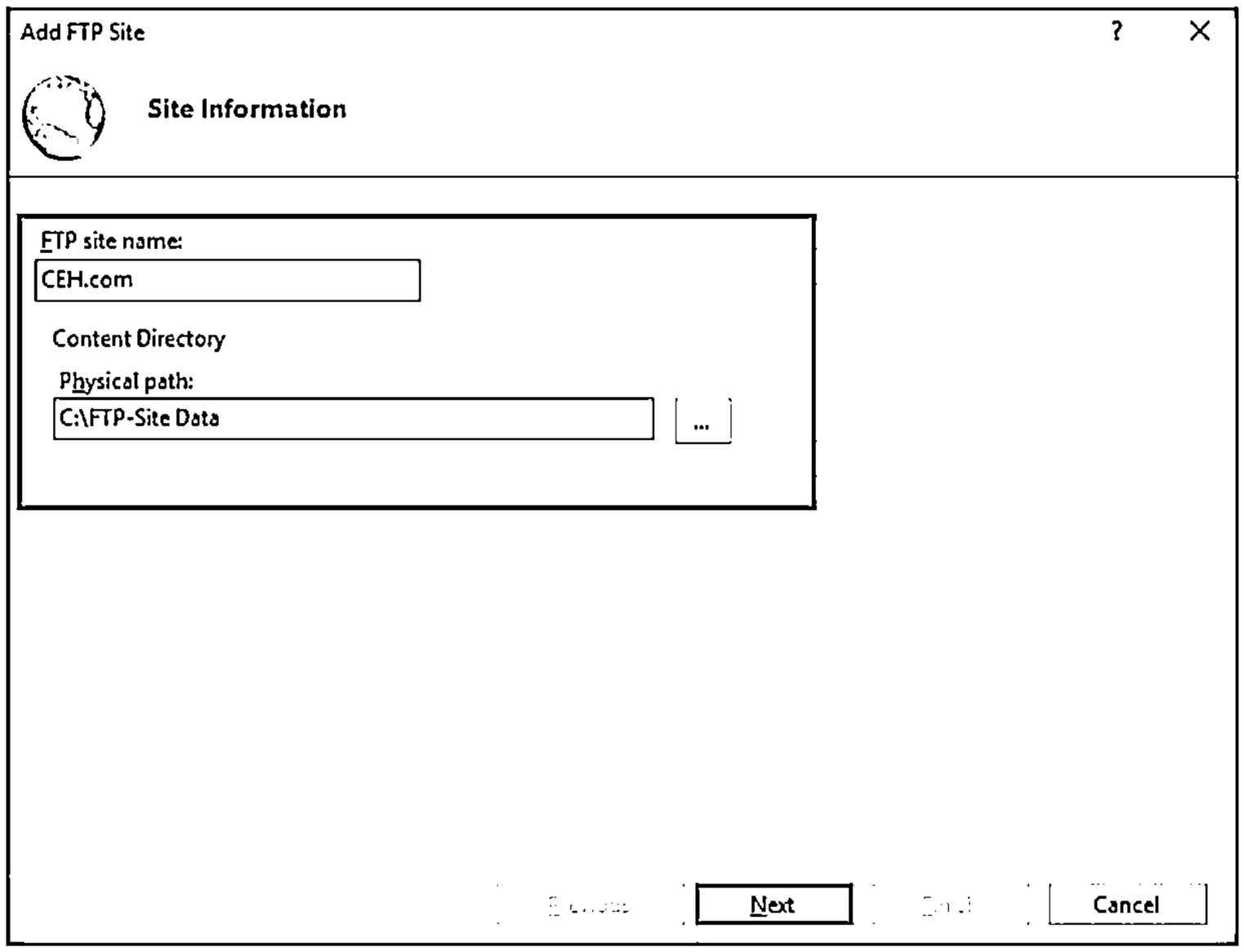


Figure 6.2.6: The Add FTP Site window: click Next

8. The **Binding and SSL Settings** wizard appears. Under the **Binding** section, in the **IP Address** field, click the drop-down icon and select **10.10.10.19**. Under the **SSL** section, select the **No SSL** radio button and click **Next**.

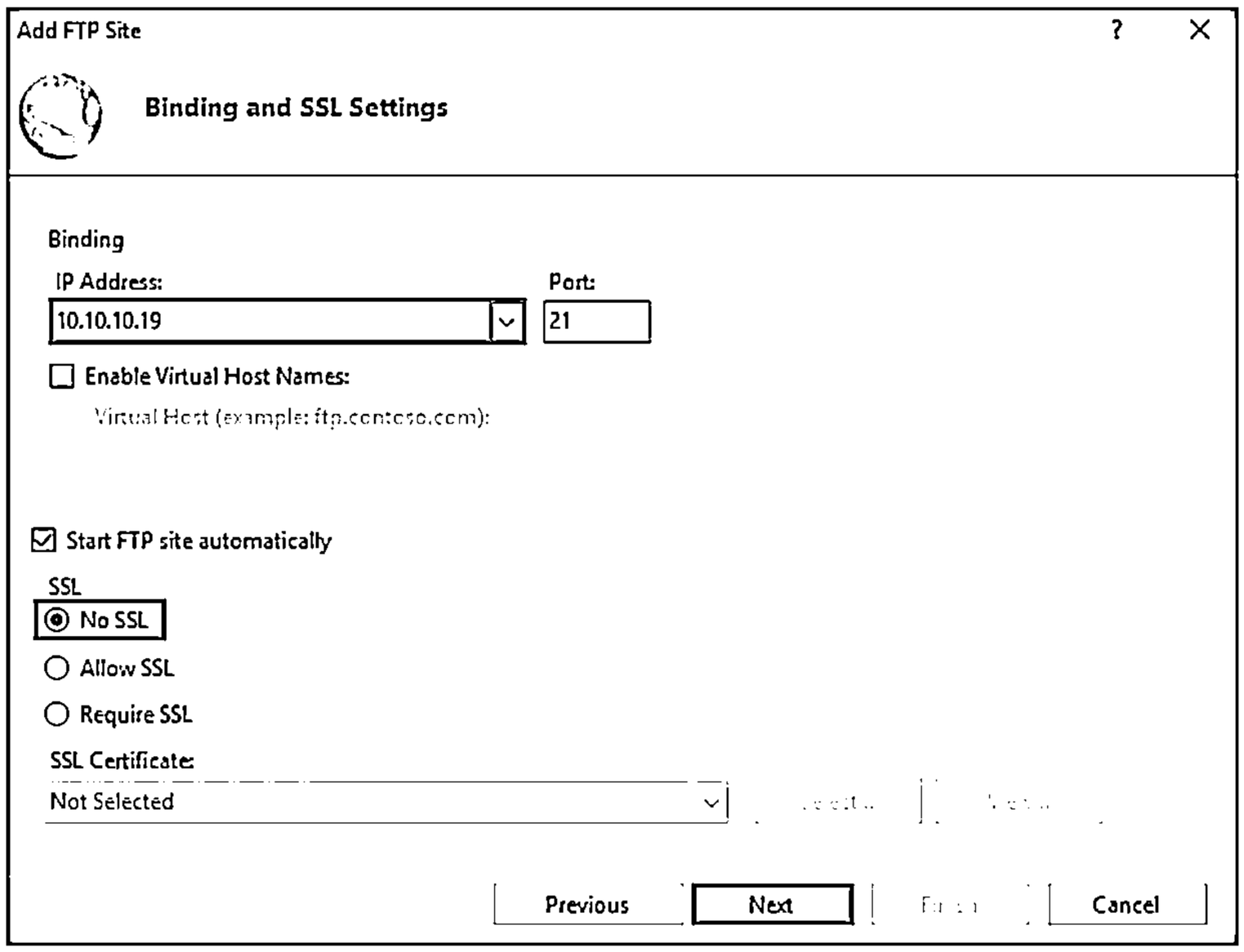


Figure 6.2.7: Binding and SSL settings

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

9. The **Authentication and Authorization Information** wizard appears. In the **Allow access to** section, select **All users** from the drop-down list. In the **Permissions** section, select both the **Read** and **Write** options and click **Finish.**

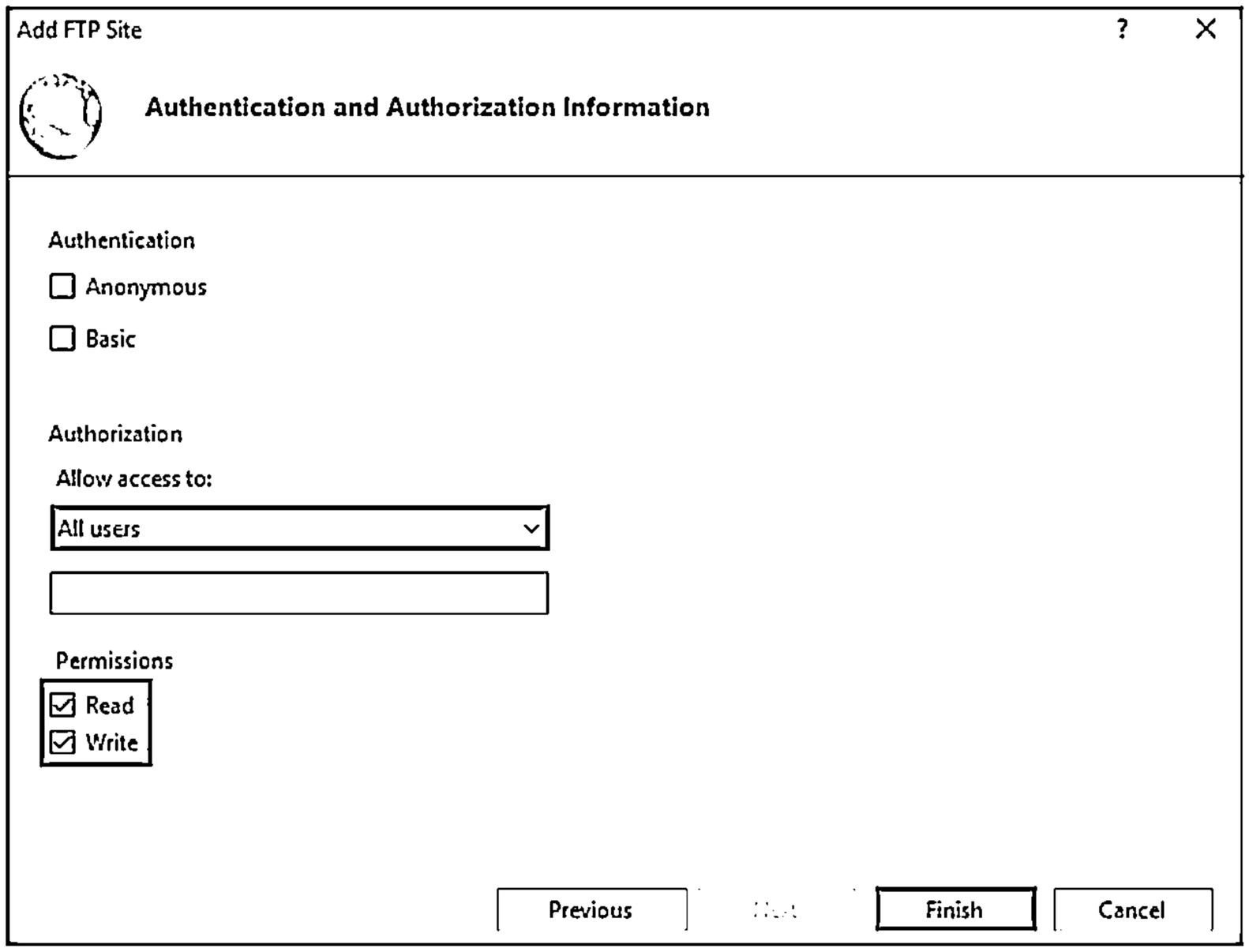


Figure 6.2.8: Authentication and authorization information

10. The **Internet Information Services (IIS) Manager** window appears with a newly added FTP site (**CEH.com**) in the left pane. Click the **Site** node in the left pane and note that the **Status** is **Started (ftp)**, as shown in the screenshot.

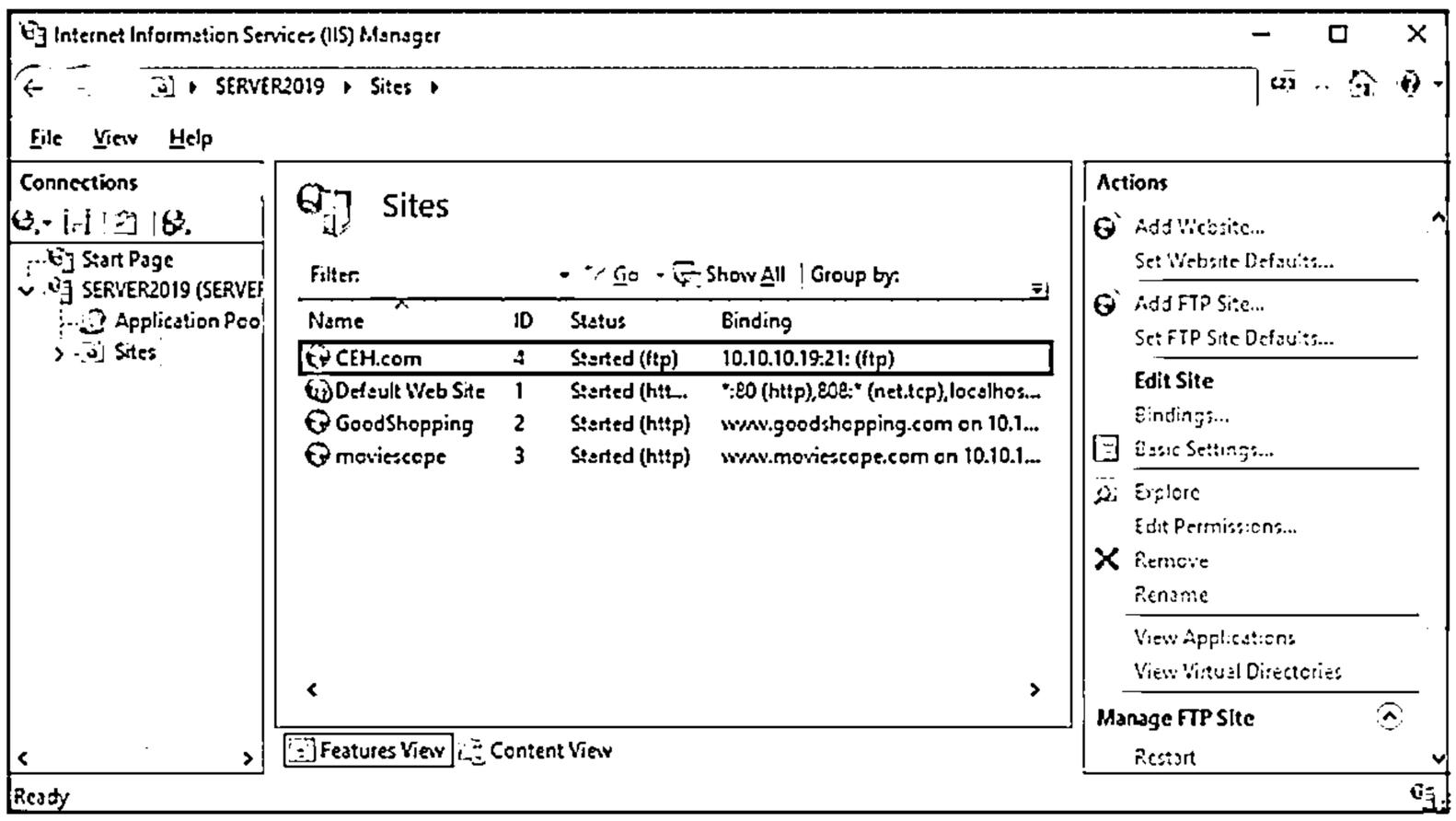


Figure 6.2.9: Added FTP site

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

11. Close all windows.
12. Turn on **Parrot Security** virtual machine.
13. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

14. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

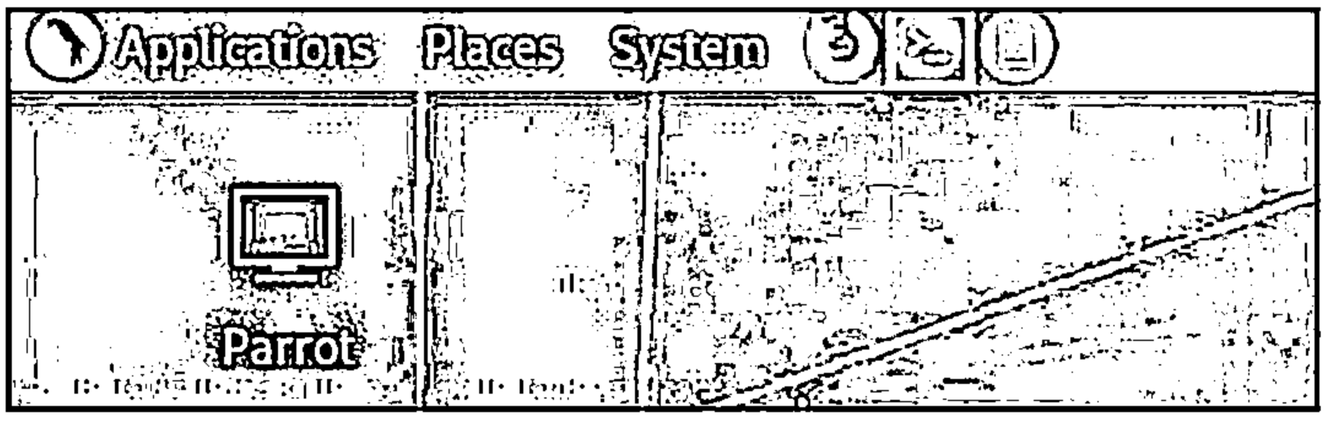


Figure 6.2.10: MATE Terminal Icon

15. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
16. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

17. Now, type **cd** and press **Enter** to jump to the root directory.

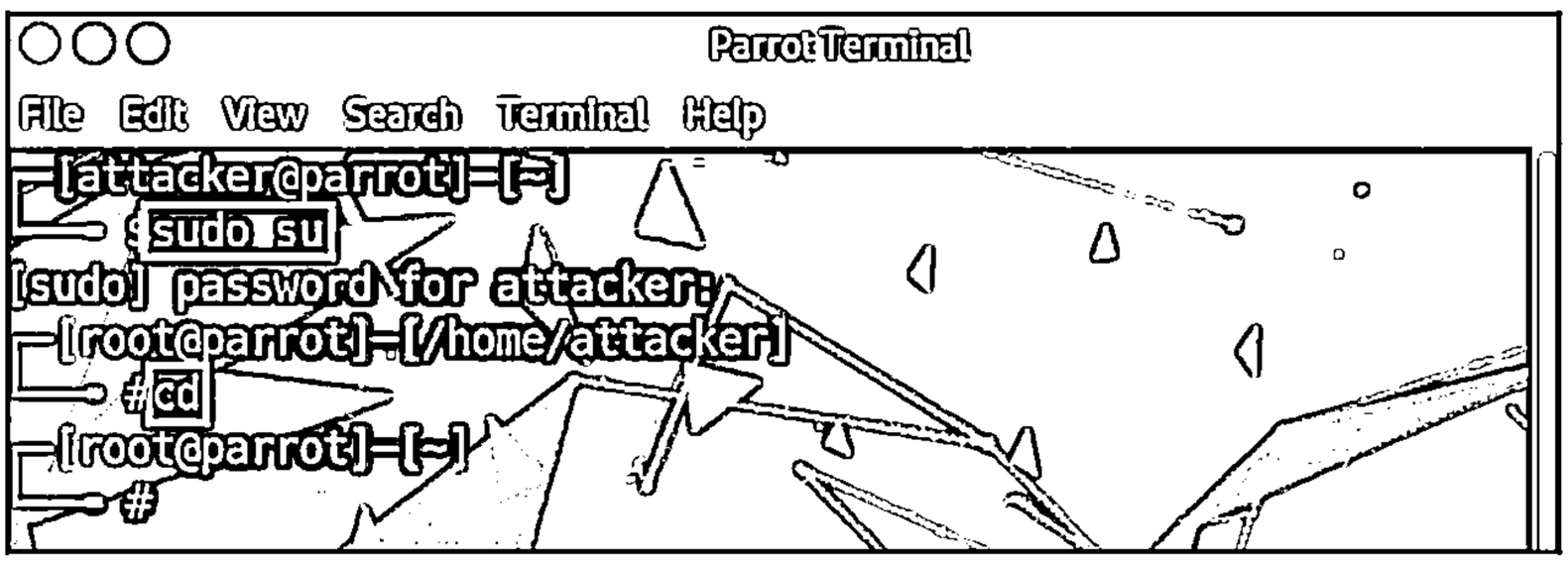


Figure 6.2.11: Running the programs as a root user

TASK 2.2

Check for Open FTP Port

18. In the **Parrot Terminal** window, type **nmap -p 21 <Target IP Address>** (in this case, **10.10.10.19**) and press **Enter**.
19. The scan result appears, indicating that port 21 is open and the FTP service is running on it, as shown in the screenshot.

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

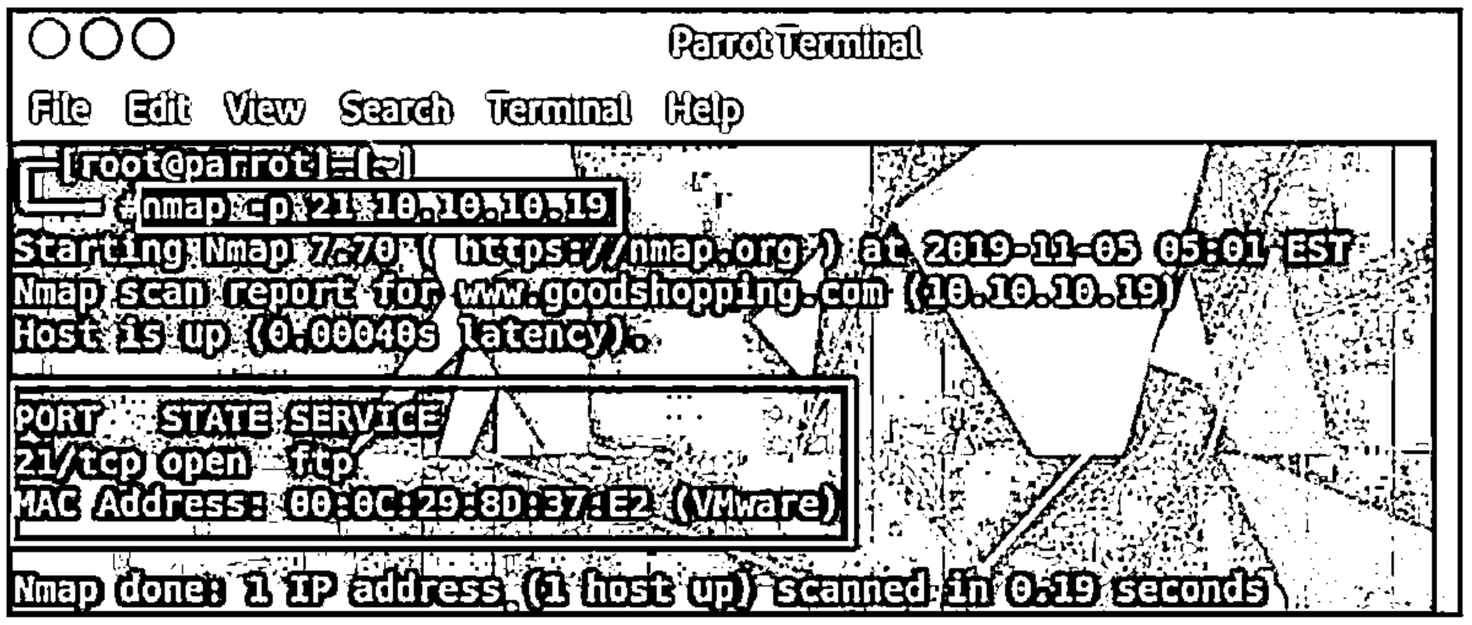


Figure 6.2.12: Nmap scan result displaying the open FTP port

TASK 2.3

Perform RPC Enumeration

20. In the terminal window, type **nmap -T4 -A <Target IP Address>** (in this example, the target IP address is **10.10.10.19**) and press **Enter**.

Note: In this command, **-T4** specifies the timing template (the number can be 0-5) and **-A** specifies that the ACK flag is set.

21. The scan result appears, displaying that port 111 is open, and giving detailed information about the services running on it, along with their versions.

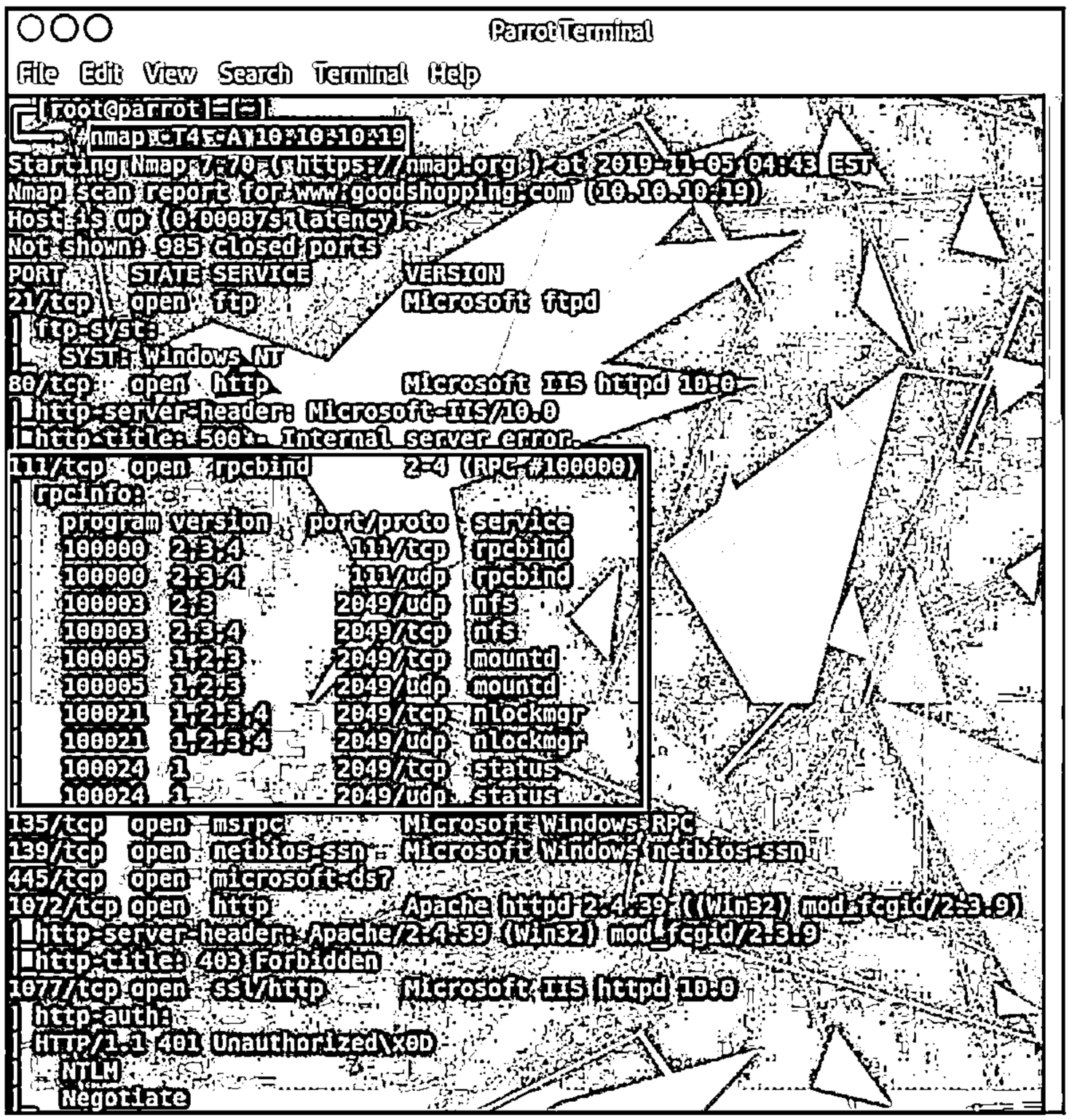


Figure 6.2.13: Nmap scan result displaying information about the open RPC port

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

TASK 2.4

Perform SMB Enumeration

22. In the terminal window, type **nmap -p <Target Port> -A <Target IP Address>** (in this example, the target port is **445** and the target IP address is **10.10.10.19**) and press **Enter**.

Note: In this command, **-p** specifies the port to be scanned, and **-A** specifies that the ACK flag is set.

23. The scan result appears, displaying that port 445 is open, and giving detailed information under the **Host script results** section about the running SMB, as shown in the screenshot.

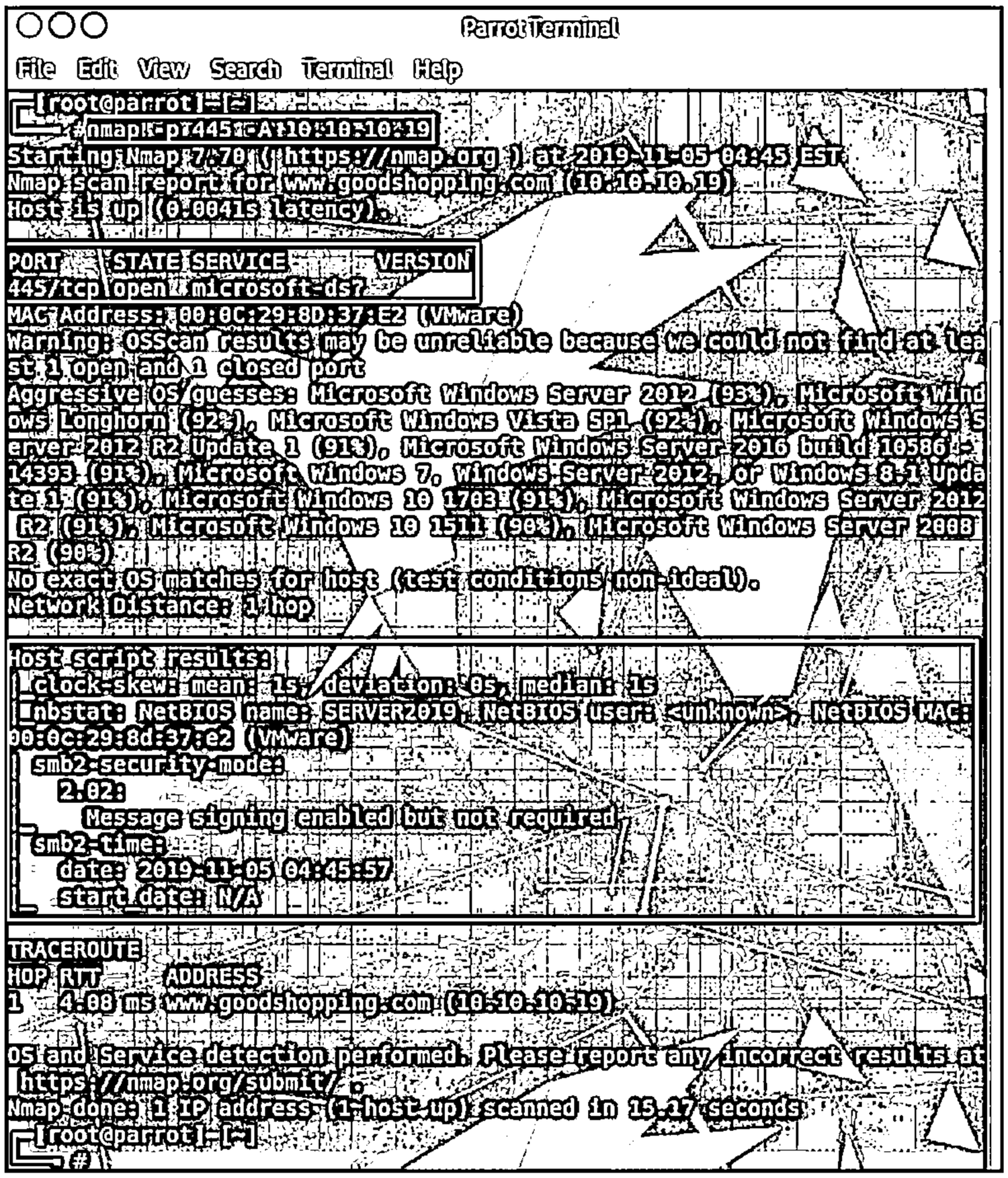


Figure 6.2.14: Nmap scan result displaying information on the open SMB port

TASK 2.5

Perform FTP Enumeration

24. In the terminal window, type **nmap -p <Target Port> -A <Target IP Address>** (in this example, the target port is **21** and target IP address is **10.10.10.19**) and press **Enter**.

Note: In this command, **-p** specifies the port to be scanned and **-A** specifies that the ACK flag is set.

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

25. The scan result appears, displaying that port 21 is open, and giving traceroute information, as shown in the screenshot.

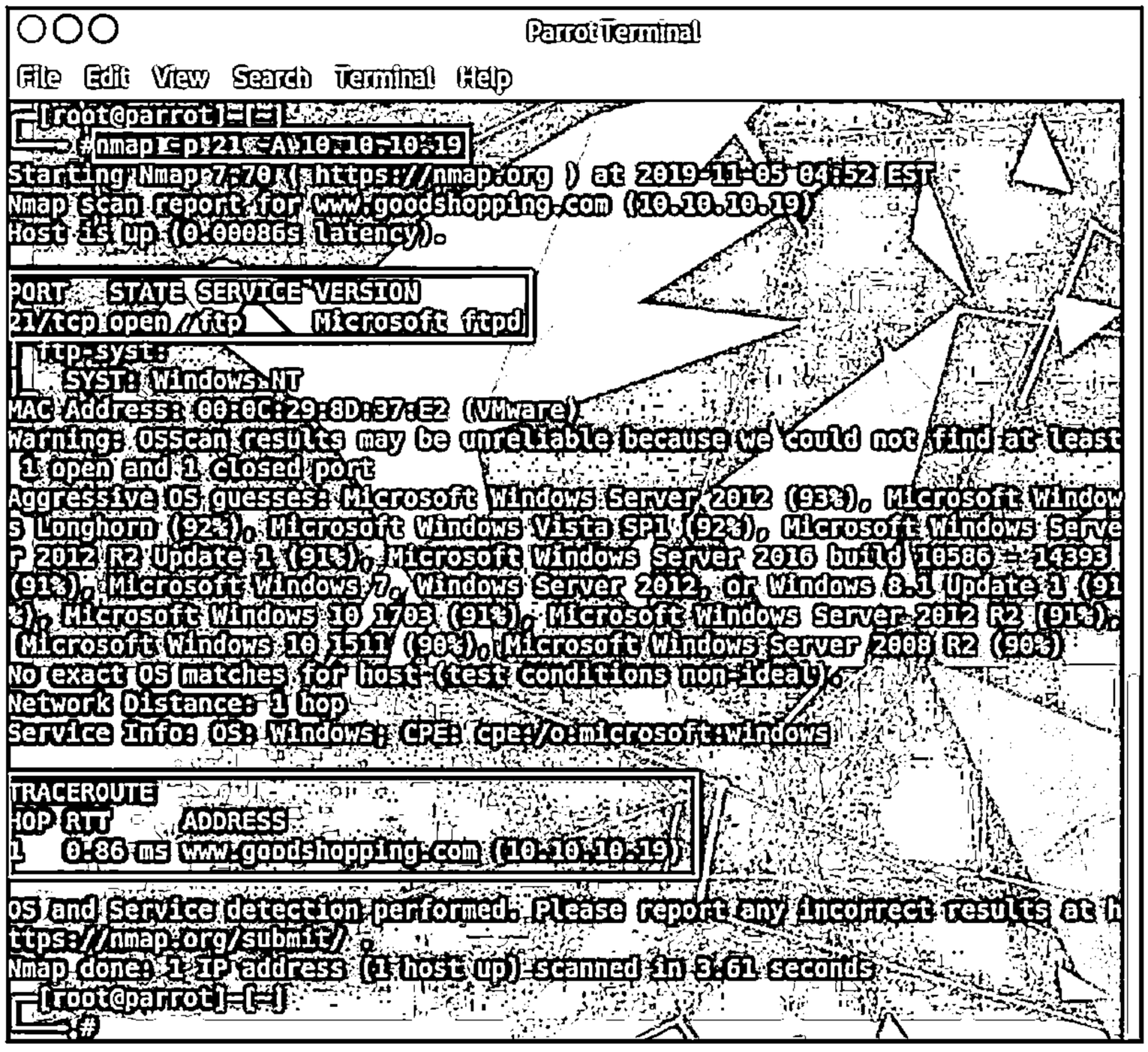


Figure 6.2.15: Nmap scan result displaying information on the open FTP port

26. This concludes the demonstration of performing RPC, SMB, and FTP enumeration using Nmap.
27. Close all open windows and document all the acquired information.
28. Turn off the **Parrot Security** and **Windows Server 2019** virtual machines.

Lab Analysis

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

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT 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

Perform Enumeration using Various Enumeration Tools

Ethical hackers and penetration testers make used of various other tools that simplify the enumeration process.

ICON KEY

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

Lab Scenario

The details obtained in the previous steps might not reveal all potential vulnerabilities in the target network. There may be more information available that could help attackers to identify loopholes to exploit. As an ethical hacker, you should use a range of tools to find as much information as possible about the target network's systems. This lab activity will demonstrate further enumeration tools for extracting even more information about the target system.

Lab Objectives

- Enumerate information using Global Network Inventory
- Enumerate network resources using Advanced IP Scanner
- Enumerate information from Windows and Samba host using Enum4linux

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2019 virtual machine
- Windows Server 2016 virtual machine
- Parrot Security virtual machine
- Ubuntu virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

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

- Global Network Inventory located at **E:\CEH-Tools\CEHv11 Module 03 Scanning Networks\Scanning Tools\Global Network Inventory**
- Advanced IP Scanner located at **Z:\CEHv11 Module 03 Scanning Networks\Ping Sweep Tools\Advanced IP Scanner**
- You may also download the latest versions of the abovementioned tools from their official websites. If you do so, the screenshots shown in the lab might differ.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 04 Enumeration

Lab Duration

Time: 30 Minutes

Overview of Enumeration Tools

To recap what you have learned so far, enumeration tools are used to collect detailed information about target systems in order to exploit them. The information collected by these enumeration tools includes data on the NetBIOS service, usernames and domain names, shared folders, the network (such as ARP tables, routing tables, traffic, etc.), user accounts, directory services, etc.

Lab Tasks

TASK 1

Enumerate Information using Global Network Inventory

Here, we will use the Global Network Inventory to enumerate various types of data from a target IP address range or single IP.

TASK 1.1

Install Global Network Inventory

1. Start the **Windows 10** and **Windows Server 2016** virtual machines.
2. In the **Windows 10** virtual machine, log in with the credentials **Admin/Pa$$w0rd** and navigate to **E:\CEH-Tools\CEHv11 Module 03 Scanning Networks\Scanning Tools\Global Network Inventory**; then, double-click **gni_setup.exe**.

Note: If a **User Account Control** pop-up appears, click **Yes**.

Global Network Inventory is used as an audit scanner in zero deployment and agent-free environments. It scans single or multiple computers by IP range or domain, as defined by the Global Network Inventory host file.

3. The **Global Network Inventory - InstallShield Wizard** appears. Follow the steps to install the application, using the default settings.
4. On completing the installation, ensure that the **Launch Global Network Inventory** checkbox is selected in the **Global Network Inventory - InstallShield Wizard** window; click **Finish**.

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

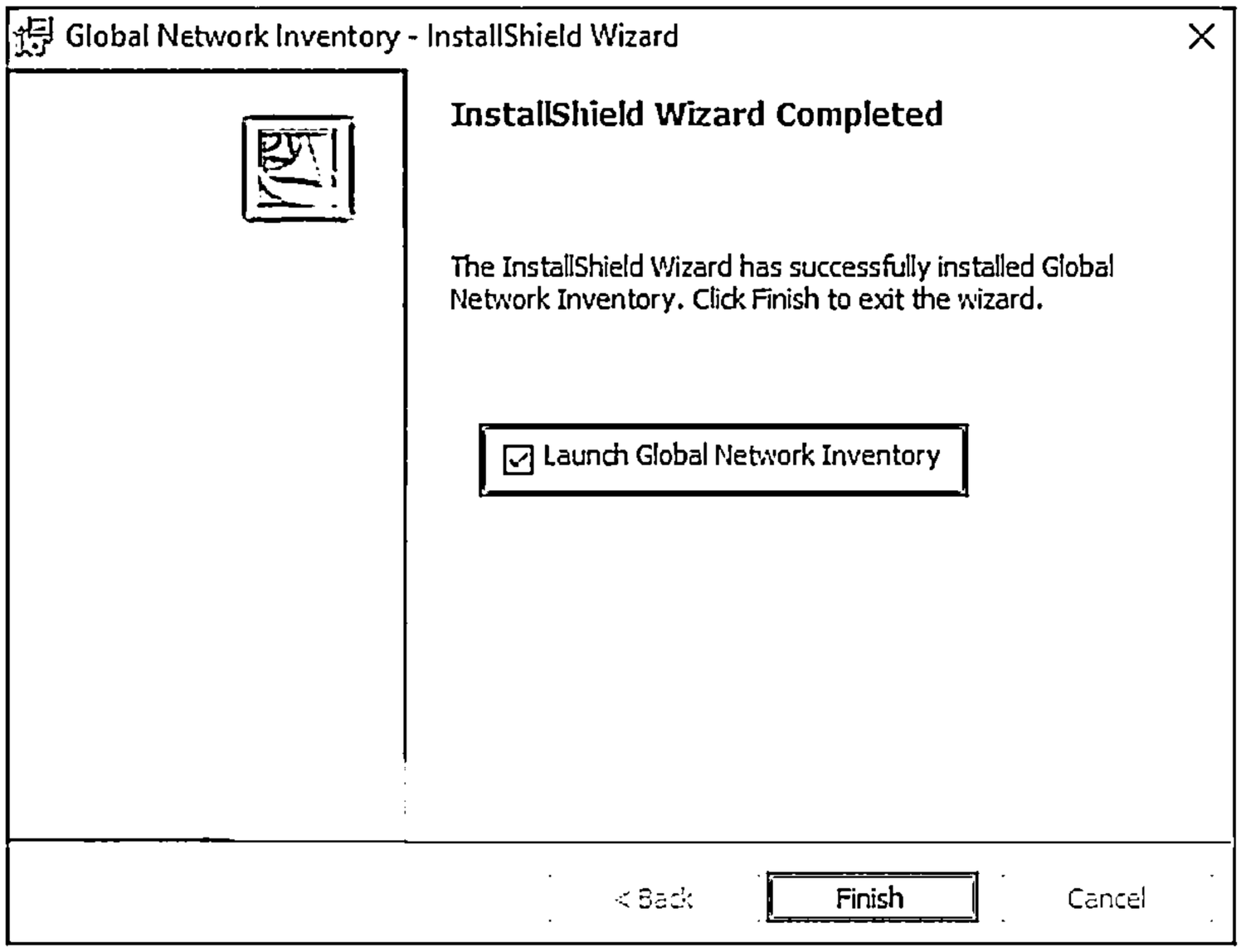


Figure 7.1.1: Global Network Inventory Installation Wizard

5. The **About Global Network Inventory** wizard appears; click **I Agree**.

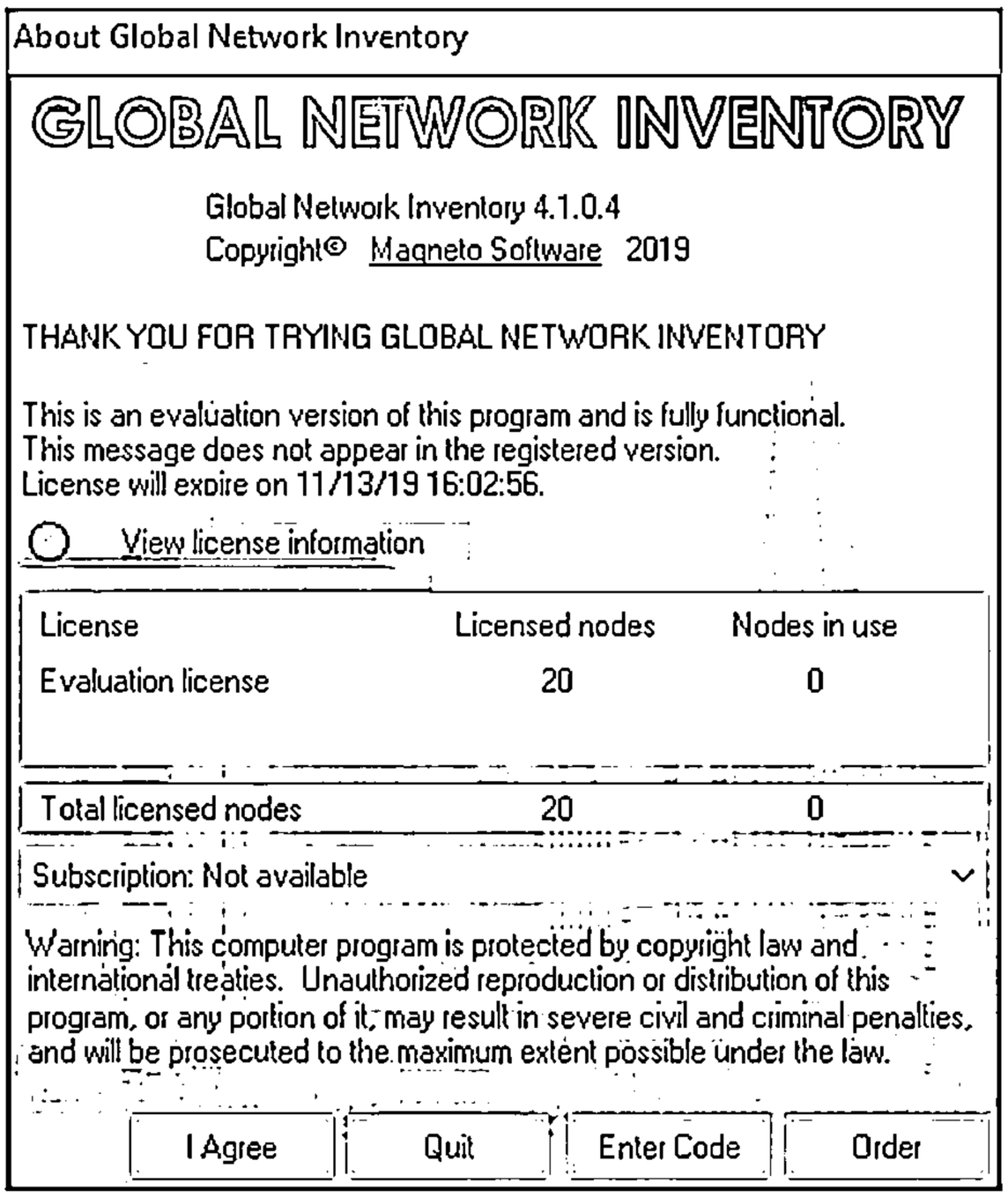


Figure 7.1.2: The Global Network Inventory License information screen

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

6. The **Global Network Inventory** GUI appears. Click **Close** on the **Tip of the Day** pop-up.

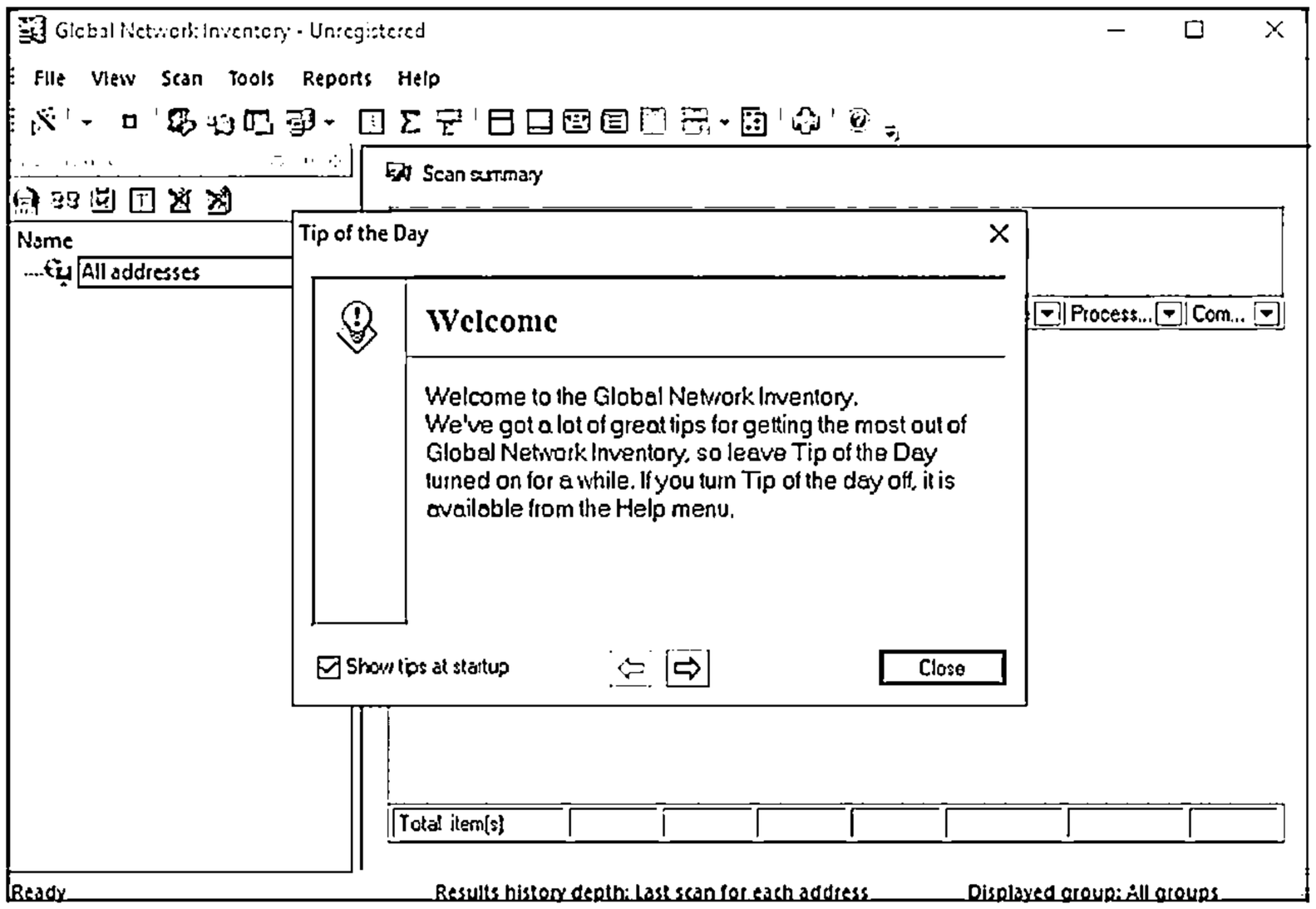


Figure 7.1.3: The Global Network Inventory main window

7. The **New Audit Wizard** window appears; click **Next.**

TASK 1.2

Configure Global Inventory Scanner

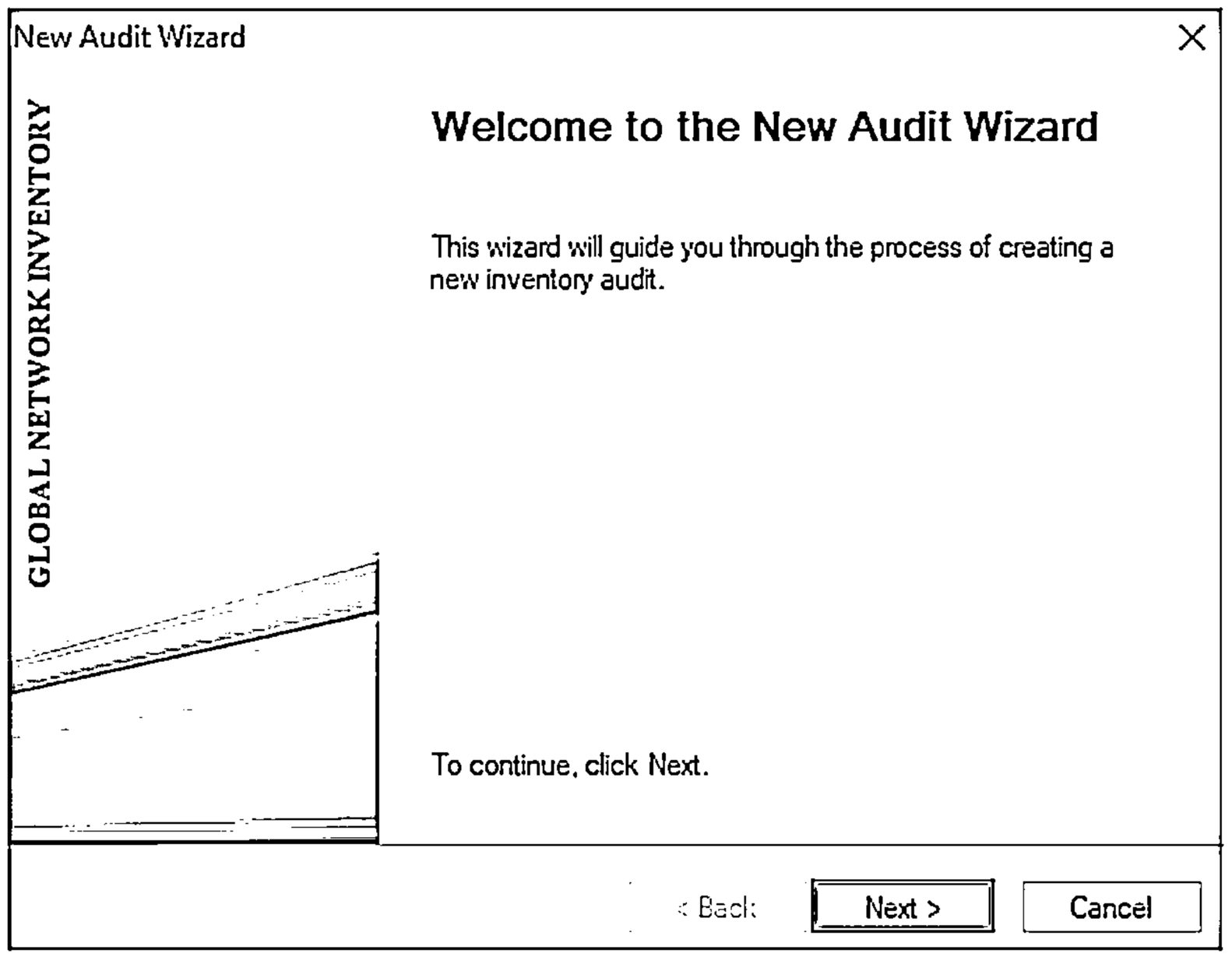


Figure 7.1.4: The Global Network Inventory new audit wizard

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

8. Under the **Audit Scan Mode** section, click the **Single address scan** radio button, and then click **Next**.

Note: You can also scan an IP range by clicking on the **IP range scan** radio button, after which you will specify the target IP range.

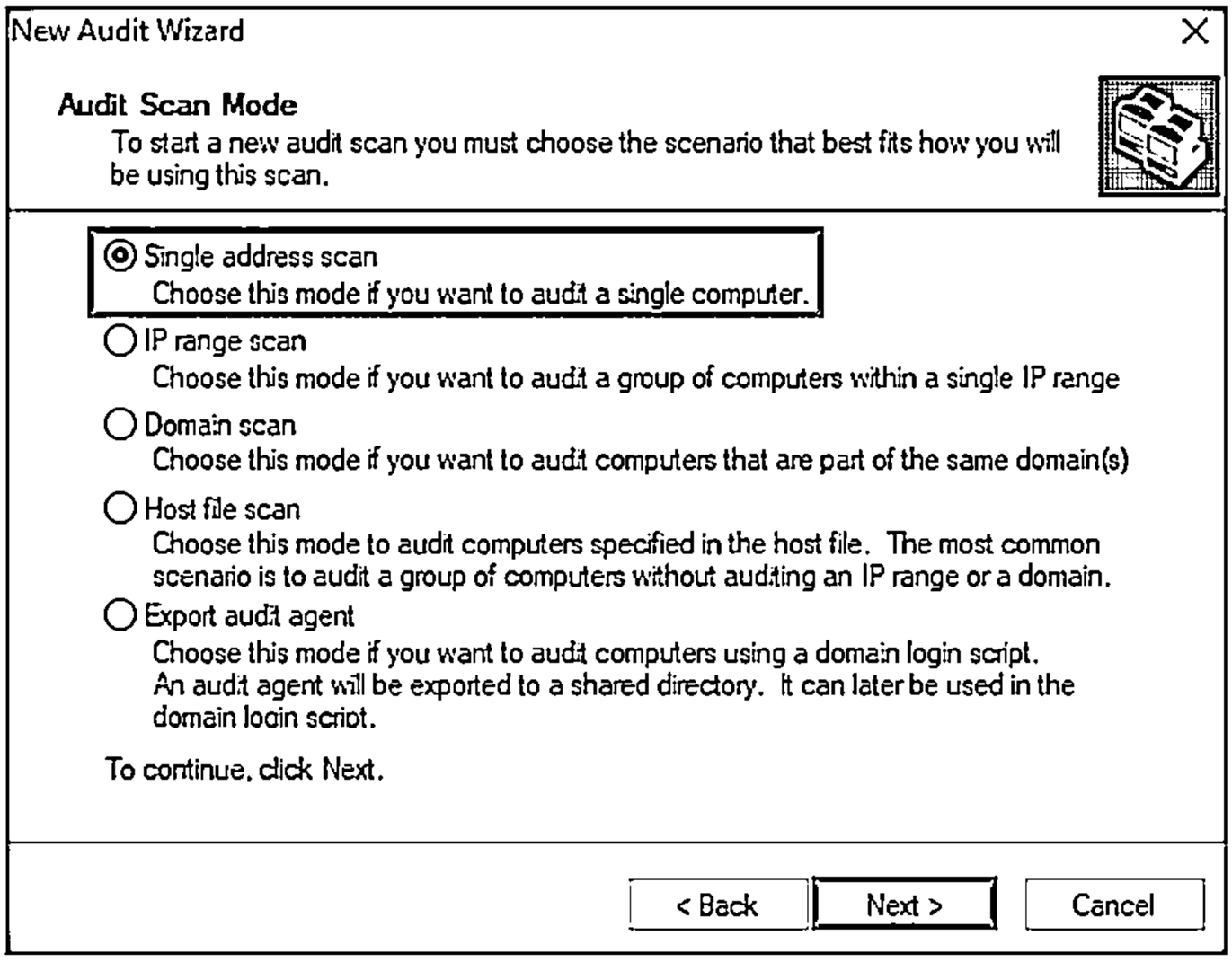


Figure 7.1.5: The Global Network Inventory Audit Scan Mode section

9. Under the **Single Address Scan** section, specify the target IP address in the **Name** field of the **Single address** option (in this example, the target IP address is **10.10.10.16**); Click **Next**.

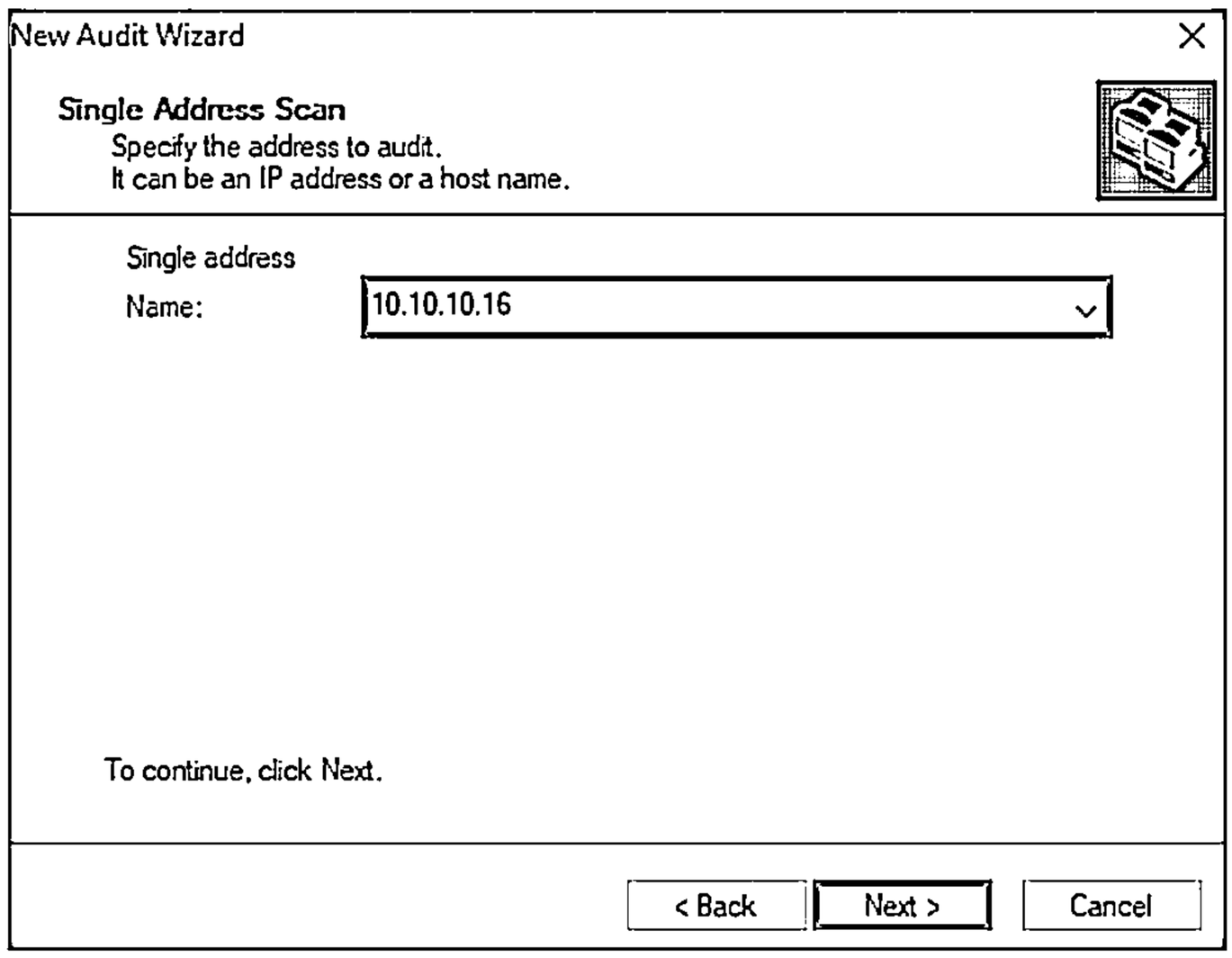


Figure 7.1.6: Inputting the target IP address

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

10. The next section is **Authentication Settings**; select the **Connect as** radio button and enter the **Windows Server 2016** virtual machine credentials (Domain\Username: **Administrator** and Password: **Pa$$w0rd**), and then click **Next.**

Note: In reality, attackers do not know the credentials of the remote machine(s). In this situation, they choose the **Connect as currently logged on user** option and perform a scan to determine which machines are active in the network. With this option, they will not be able to extract all the information about the target system. Because this lab is just for assessment purposes, we have entered the credentials of the remote machine directly.

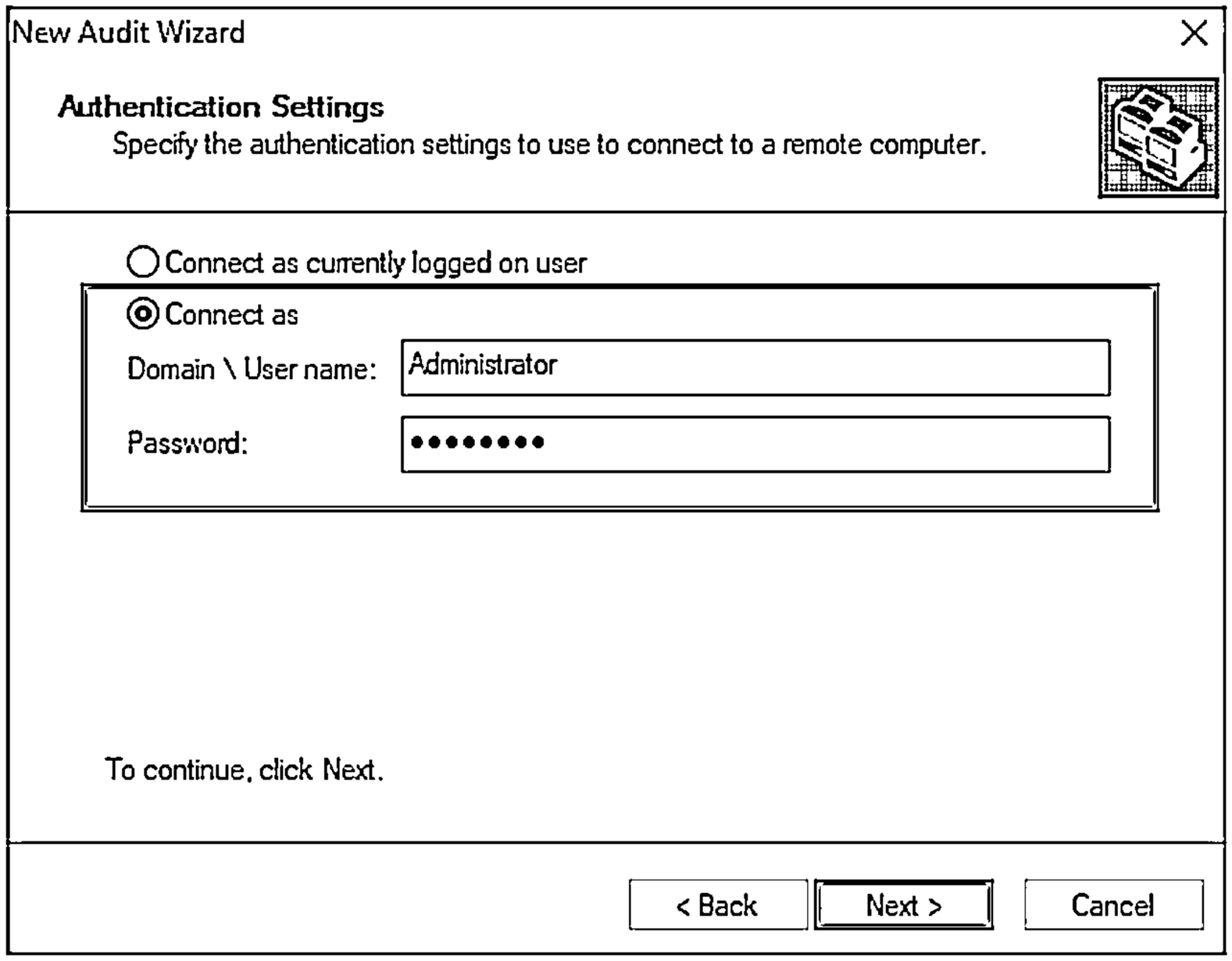


Figure 7.1.7: Global Network Inventory Authentication settings

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

11. In the final step of the wizard, leave the default settings unchanged and click **Finish**.

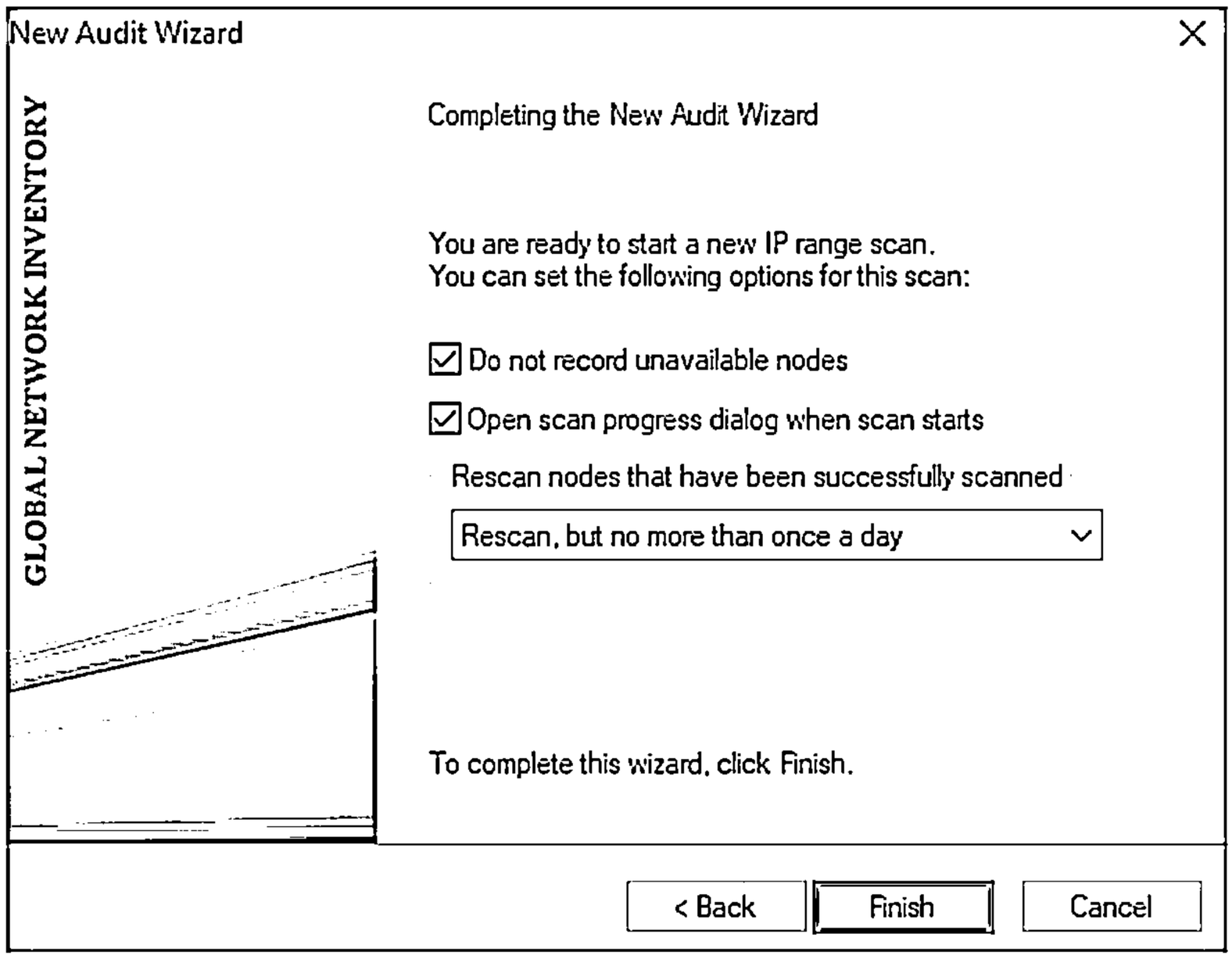


Figure 7.1.8: Global Network Inventory Audit wizard final step

12. The **Scan progress** window will appear.

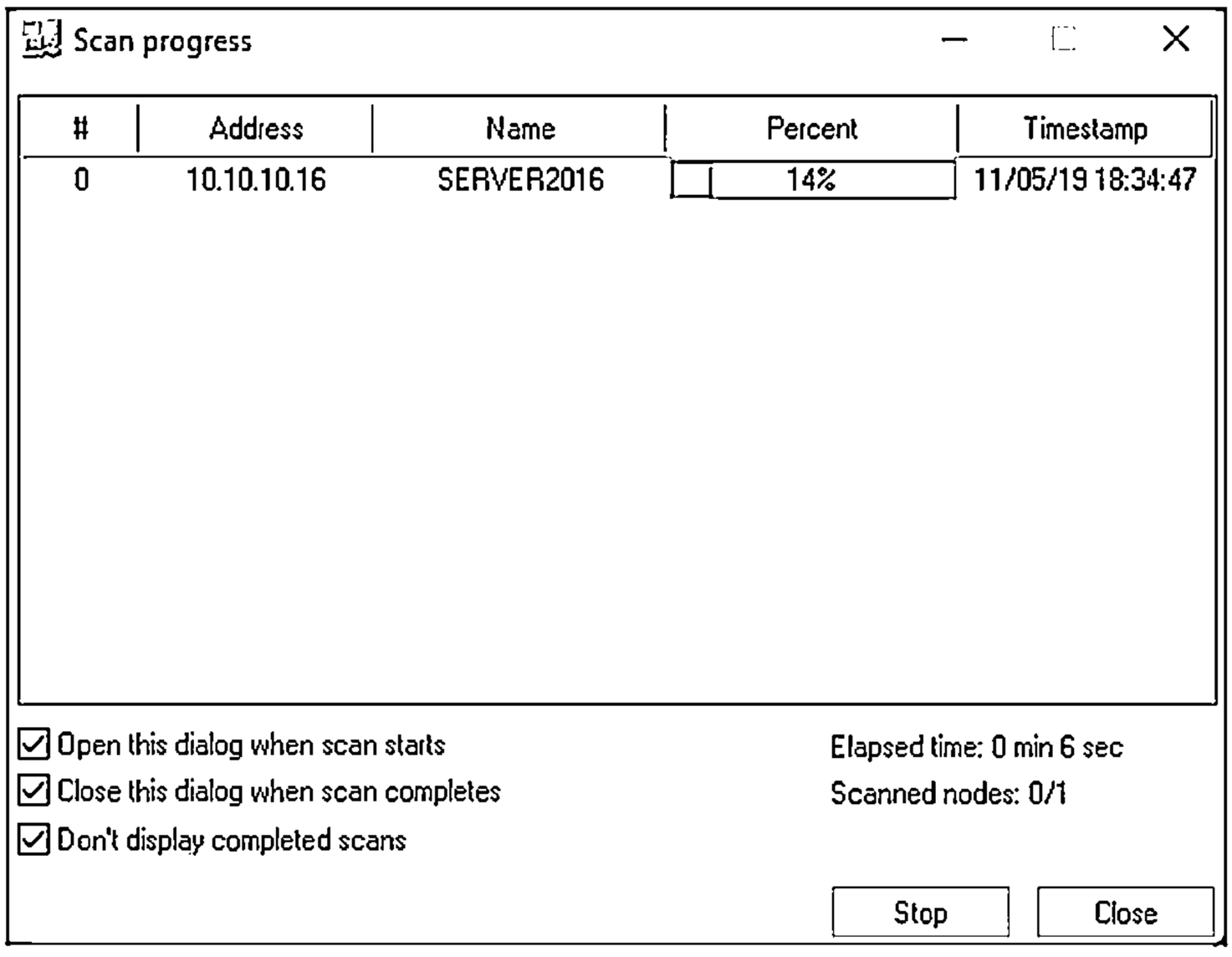


Figure 7.1.9: Global Network Inventory scan progress

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

13. The results are displayed when the scan finished. The **Scan summary** of the scanned target IP address (**10.10.10.16**) appears.

Note: The scan result and summary in each tab might vary in your lab environment.

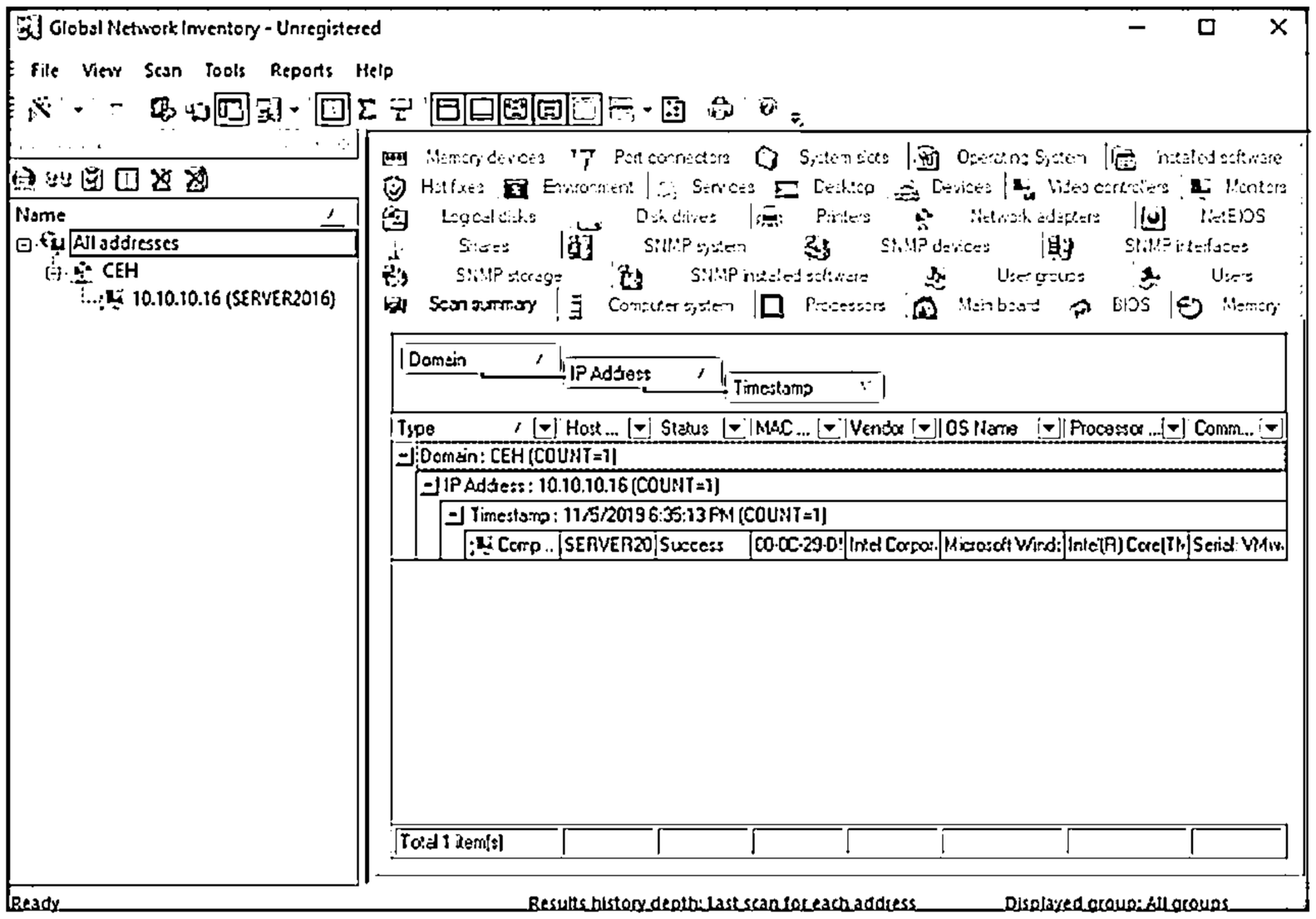


Figure 7.1.10: Global Network Inventory result window

TASK 1.3

Examine the Scanned Machine

14. Hover your mouse cursor over the **Computer details** under the **Scan summary** tab to view the scan summary, as shown in the screenshot.

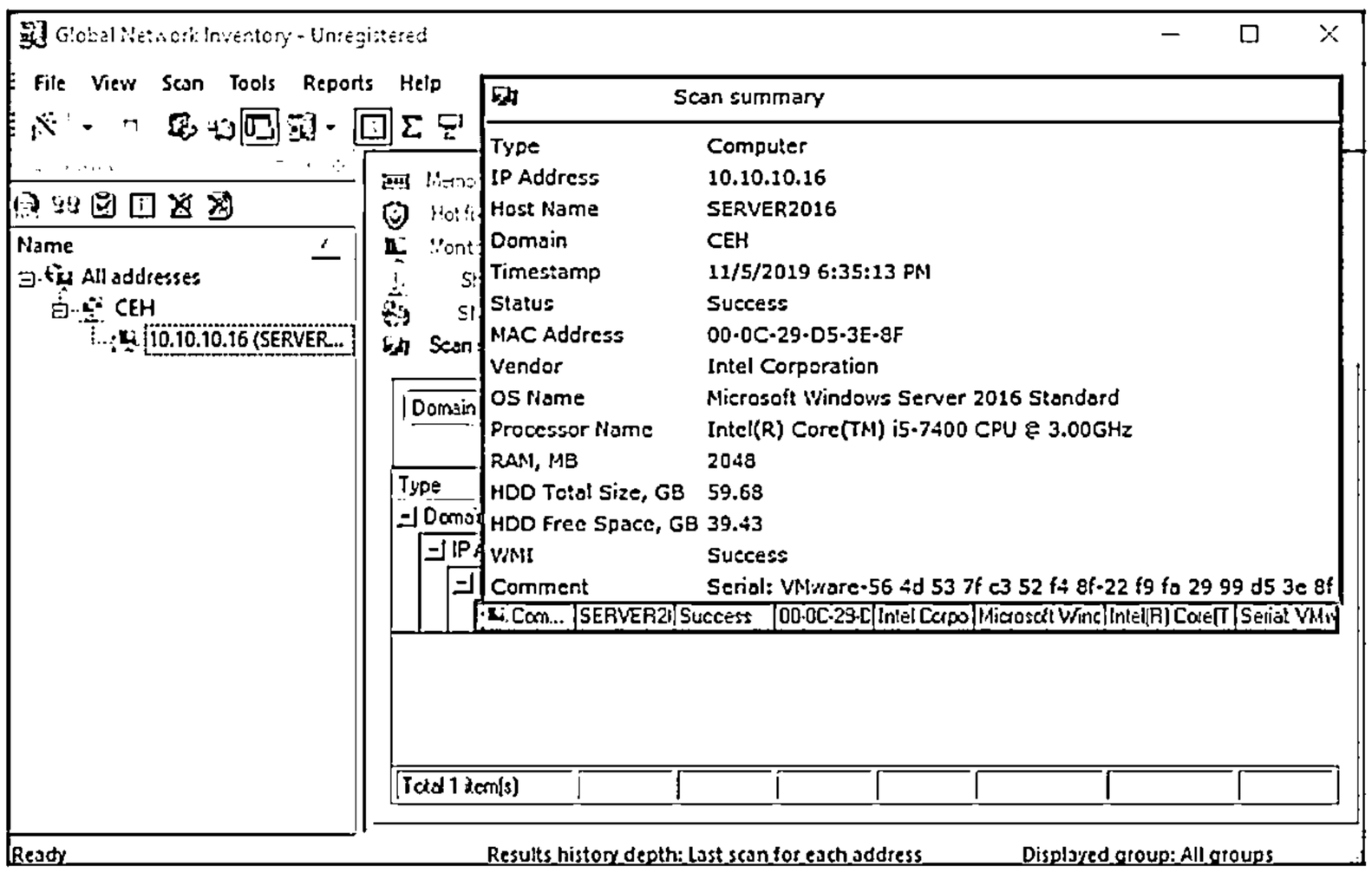


Figure 7.1.11: Global Network Inventory scan summary

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

15. Click the **Operating System** tab and hover the mouse cursor over **Windows details** to view the complete details of the machine.

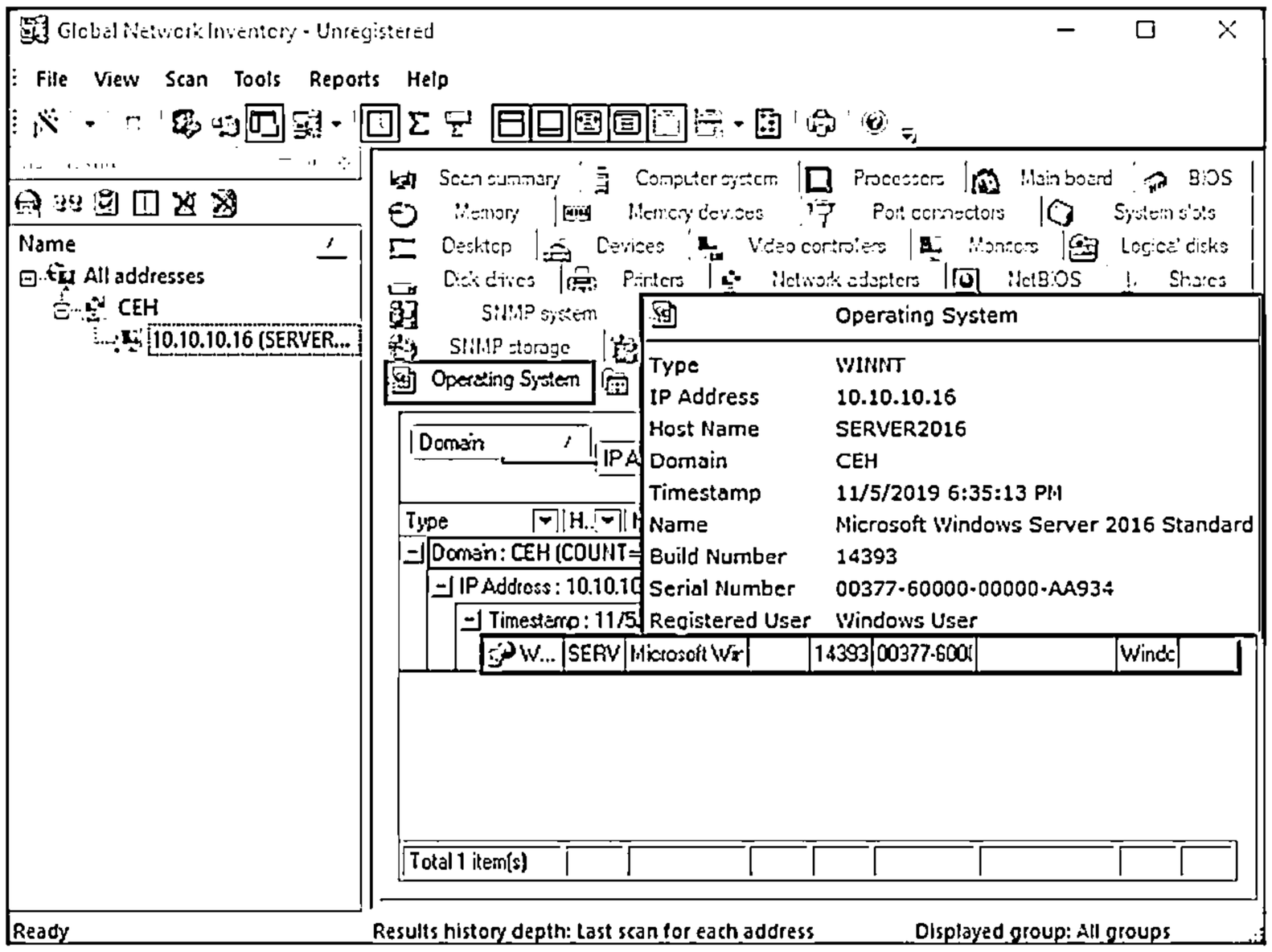


Figure 7.1.12: Global Inventory Operating System tab

16. Click the **BIOS** tab, and hover the mouse cursor over windows details to display detailed BIOS settings information.

Note: The results might differ in your lab environment.

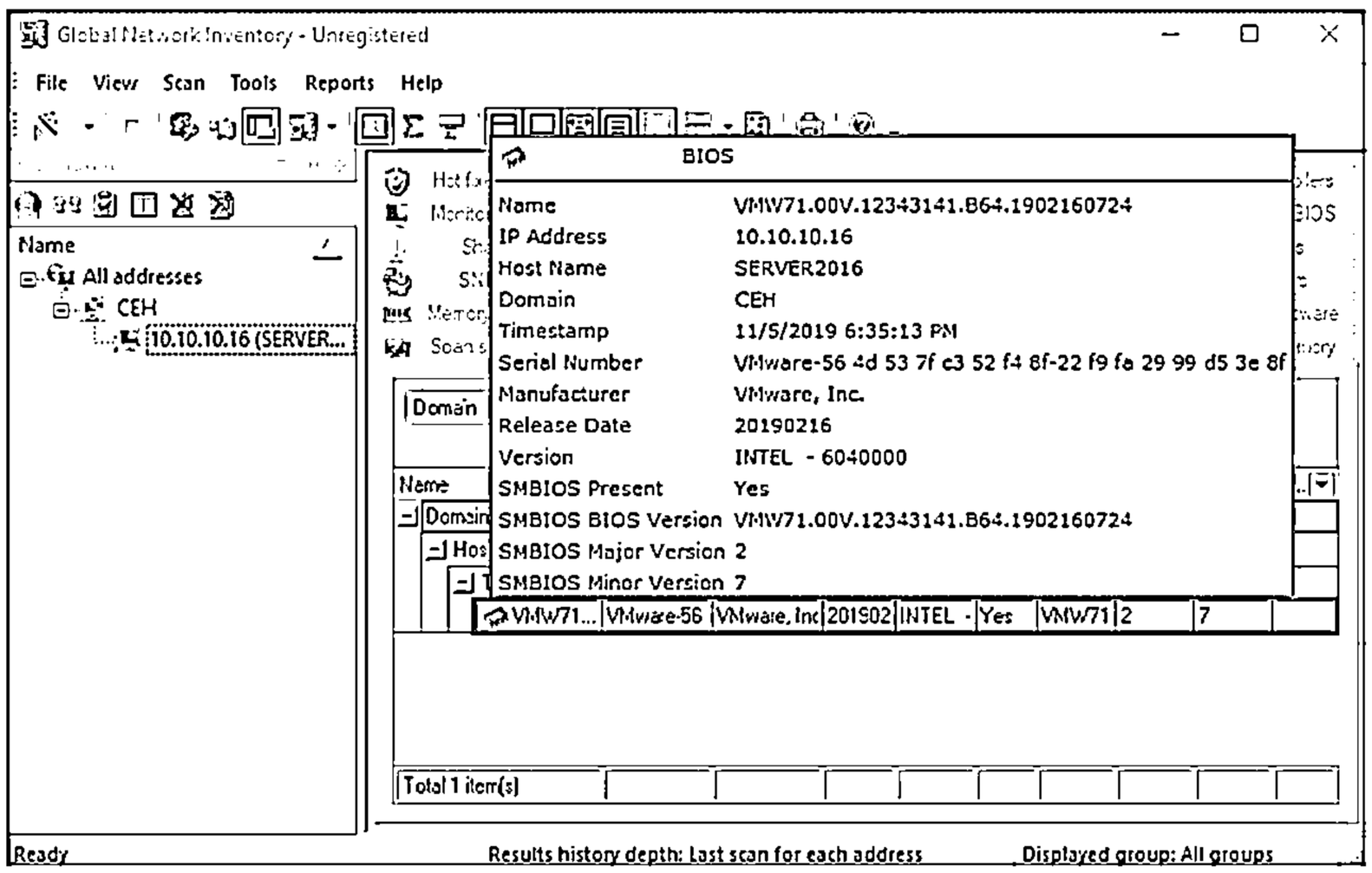


Figure 7.1.13: Global Network Inventory BIOS summary

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

17. Click the **NetBIOS** tab, and hover the mouse cursor over any NetBIOS application to display the detailed NetBIOS information about the target.

Note: Hover the mouse cursor over each NetBIOS application to view its details.

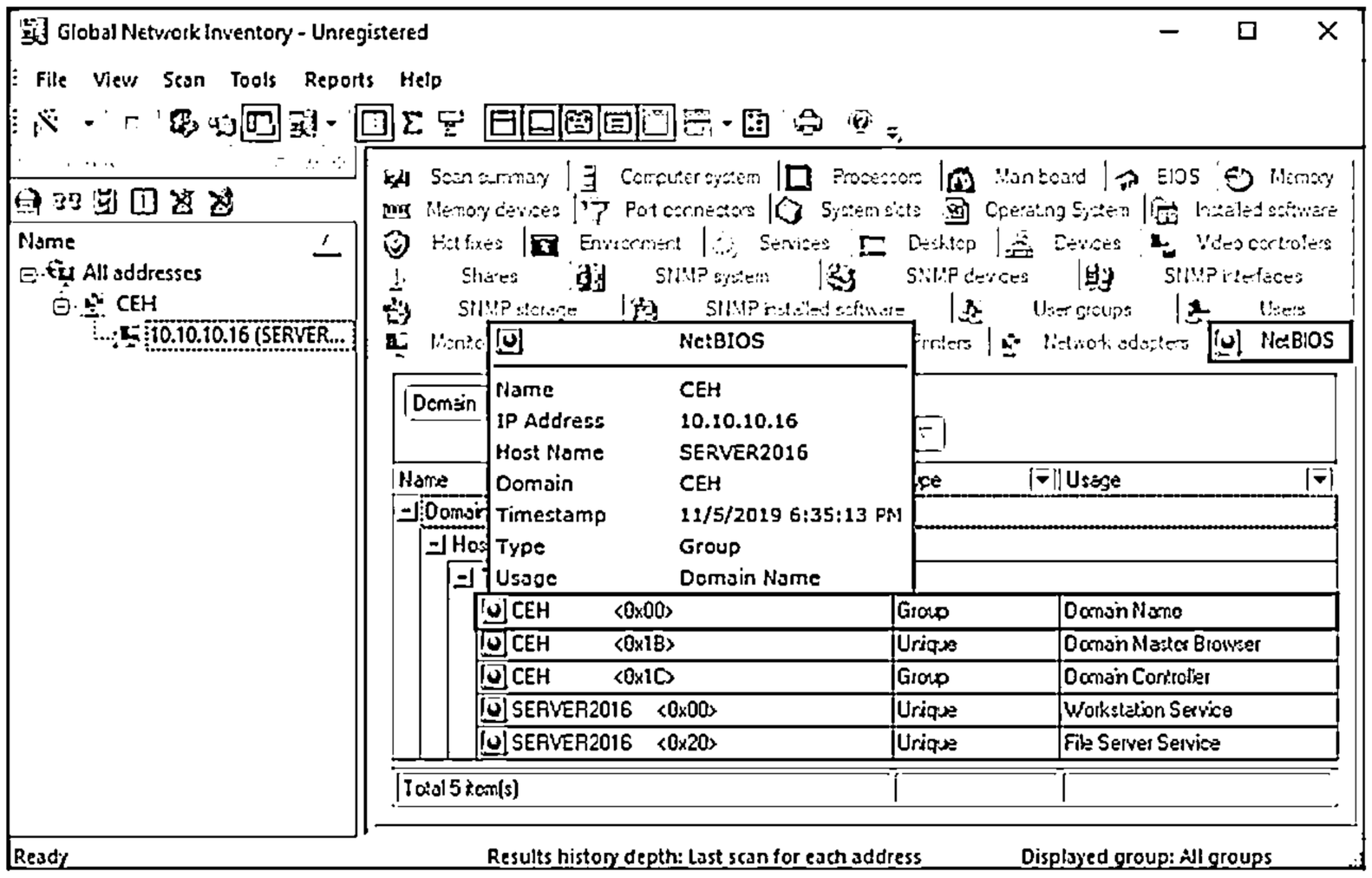


Figure 7.1.14: Global Network Inventory NetBIOS information

18. Click the **User groups** tab and hover the mouse cursor over any username to display detailed user groups information.

Note: Hover the mouse cursor over each username to view its details.

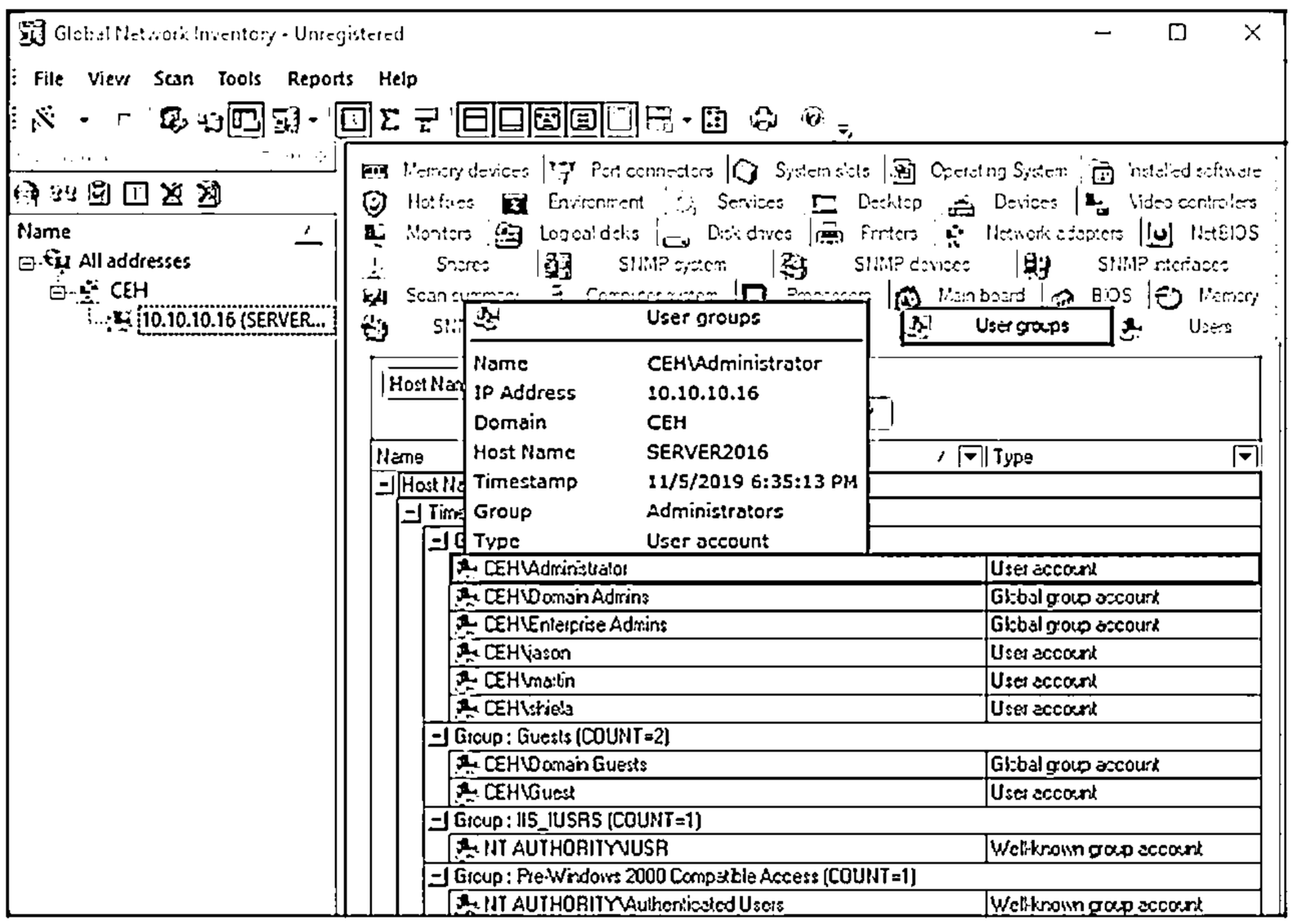


Figure 7.1.15: Global Network Inventory User groups tab

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

19. Click the **Users** tab, and hover the mouse cursor over the username to view login details for the target machine.

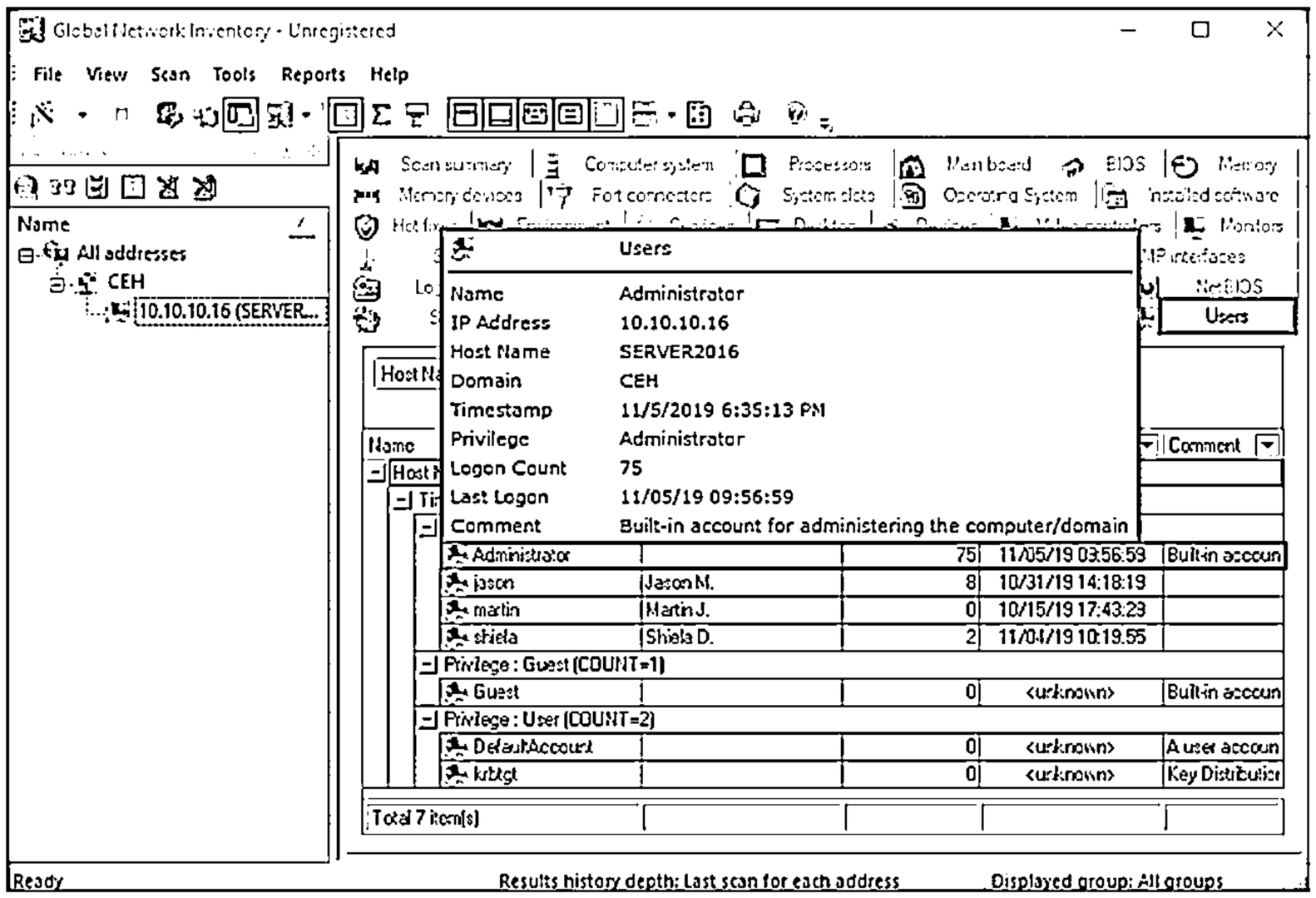


Figure 7.1.16: Global Network Inventory Users tab

20. Click the **Services** tab and hover the mouse cursor over any service to view its details.

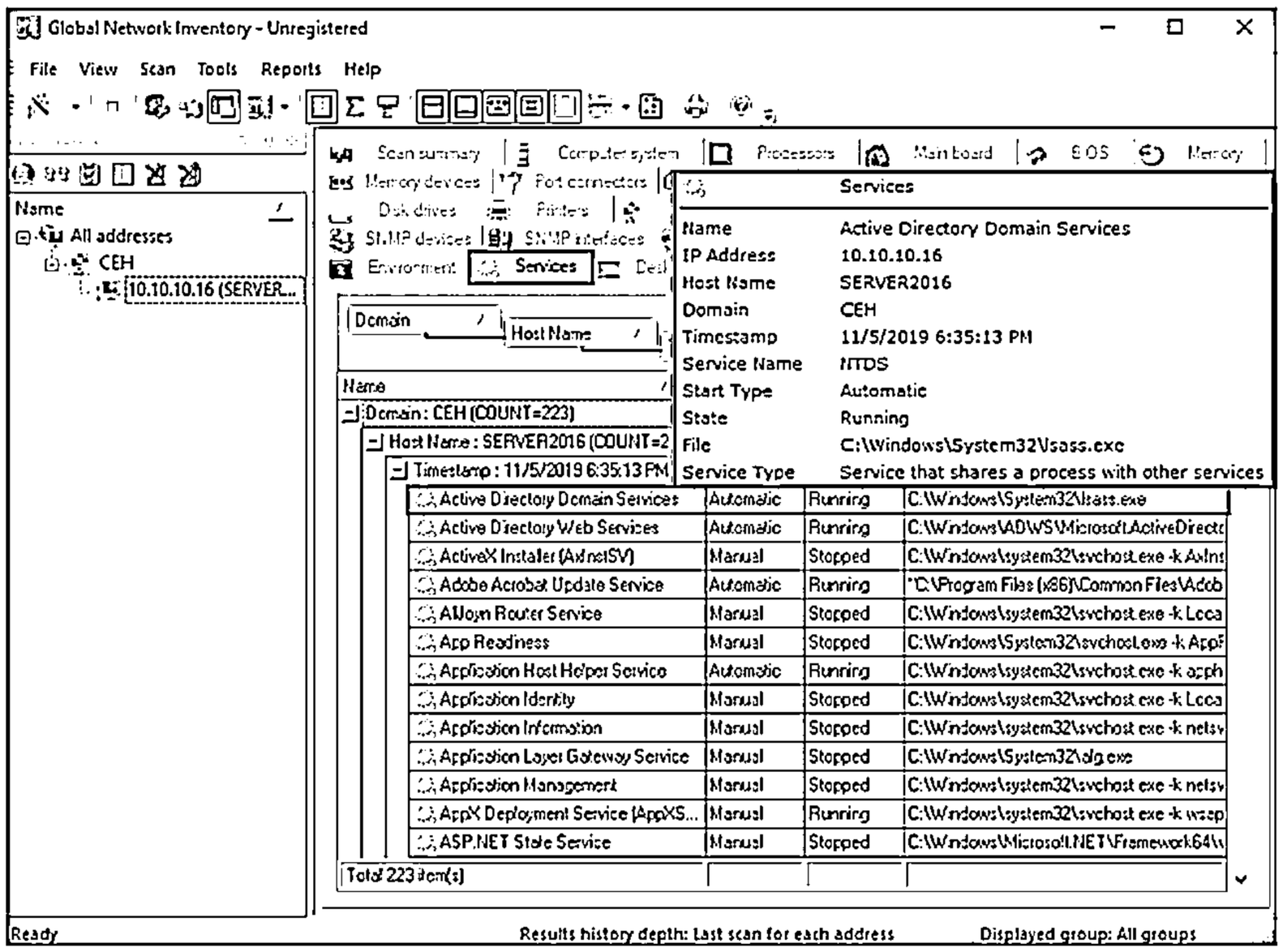


Figure 7.1.17: Global Network Inventory Services tab

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

21. Click the **Installed software** tab, and hover the mouse cursor over any software to view its details.

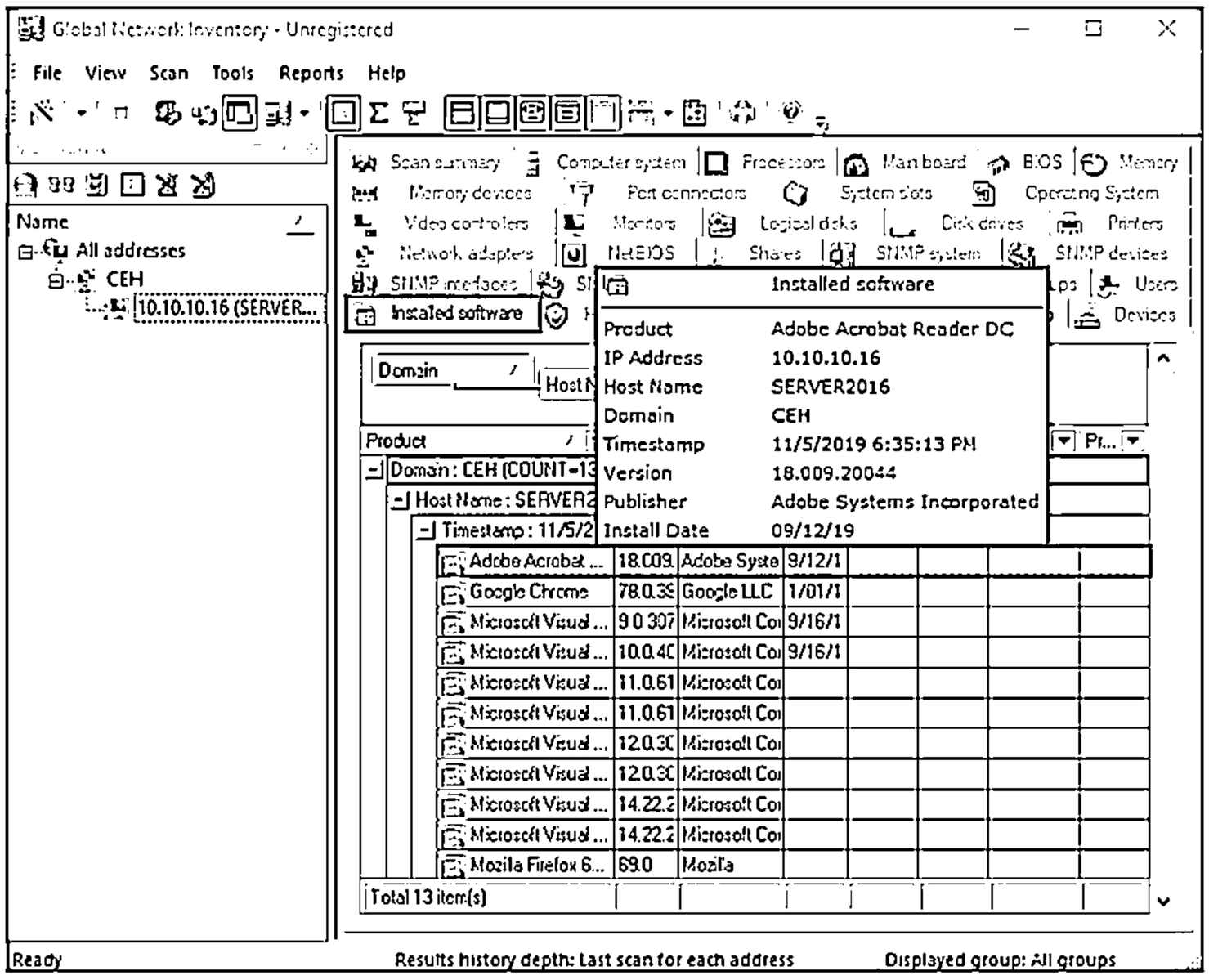


Figure 7.1.18: Global Network Inventory Installed software tab

22. Click the **Shares** tab, and hover the mouse cursor over any shared folder to view its details.

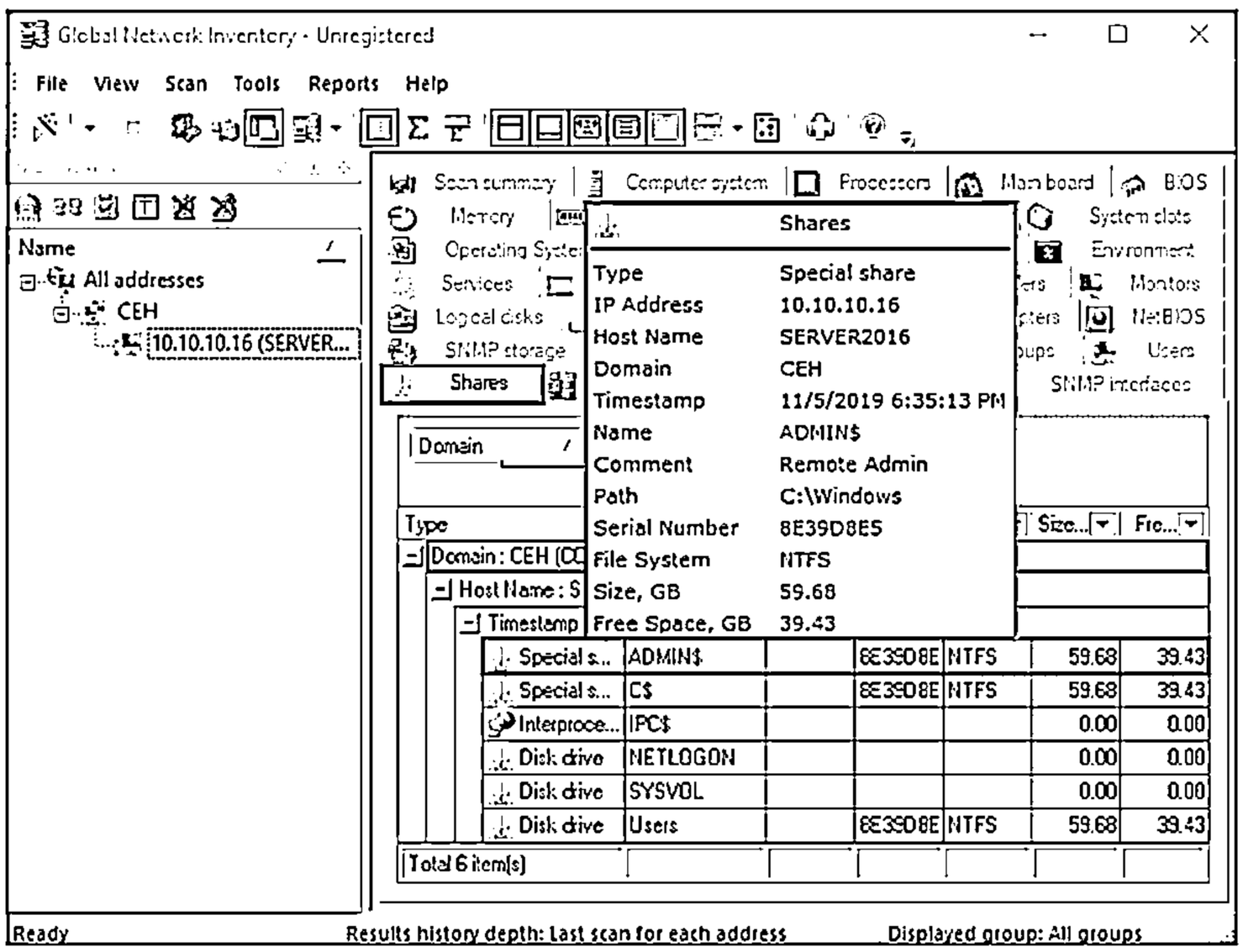


Figure 7.1.19: Global Network Inventory Shares tab

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

23. Similarly, you can click other tabs such as **Computer System**, **Processors**, **Main board**, **Memory**, **SNMP systems**, **Main board**, and **Hot fixes**. Hover the mouse cursor over elements under each tab to view their detailed information.
24. This concludes the demonstration of performing enumeration using the Global Network Inventory.
25. Close all open windows and document all the acquired information.

TASK 2 Enumerate Network Resources using Advanced IP Scanner

Here, we will use the Advanced IP Scanner to enumerate the network resources of the target network.

TASK 2.1 Install Advanced IP Scanner

Advanced IP Scanner provides various types of information about the computers on a target network. The program shows all network devices, gives you access to shared folders, provides remote control of computers (via RDP and Radmin), and can even remotely switch computers off.

1. Start the **Windows Server 2019** and **Ubuntu** virtual machines.

Note: Ensure that the **Windows 10** and **Windows Server 2016** virtual machines are still running.

2. In the **Windows Server 2019** virtual machine, log in with the credentials **Administrator** and **Pa$$w0rd**.
3. Navigate to **Z:\CEHv11 Module 03 Scanning Networks\Ping Sweep Tools\Advanced IP Scanner** and double-click **Advanced_IP_Scanner_2.5.3850.exe**.
4. Follow the installation steps to install Advanced IP Scanner, using all the default settings.
5. After the installation completes, ensure that the **Run Advanced IP Scanner** option is selected and click **Finish**.

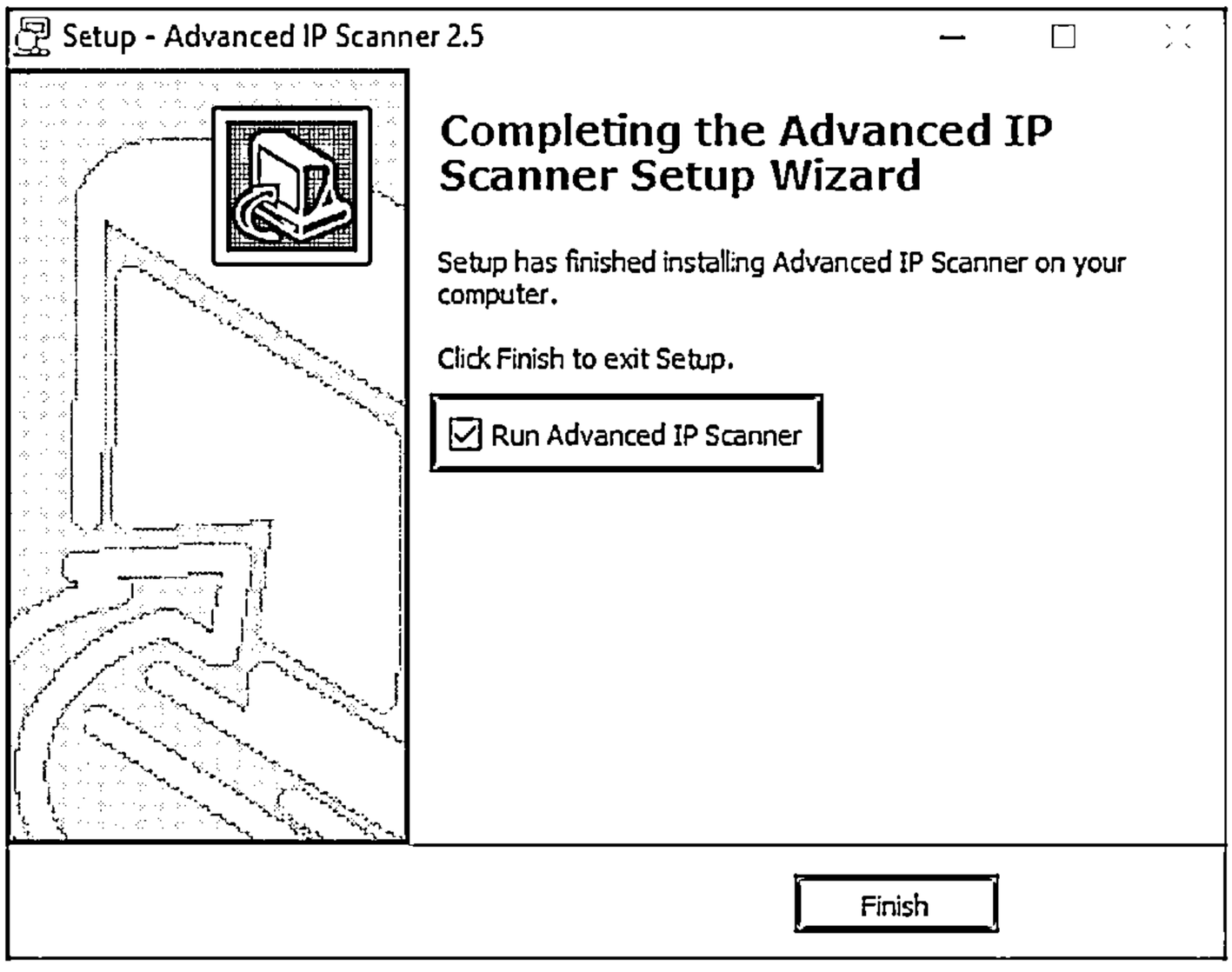


Figure 7.2.1: Advanced IP Scanner setup

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

6. The **Advanced IP Scanner** GUI appears, as shown in the screenshot.

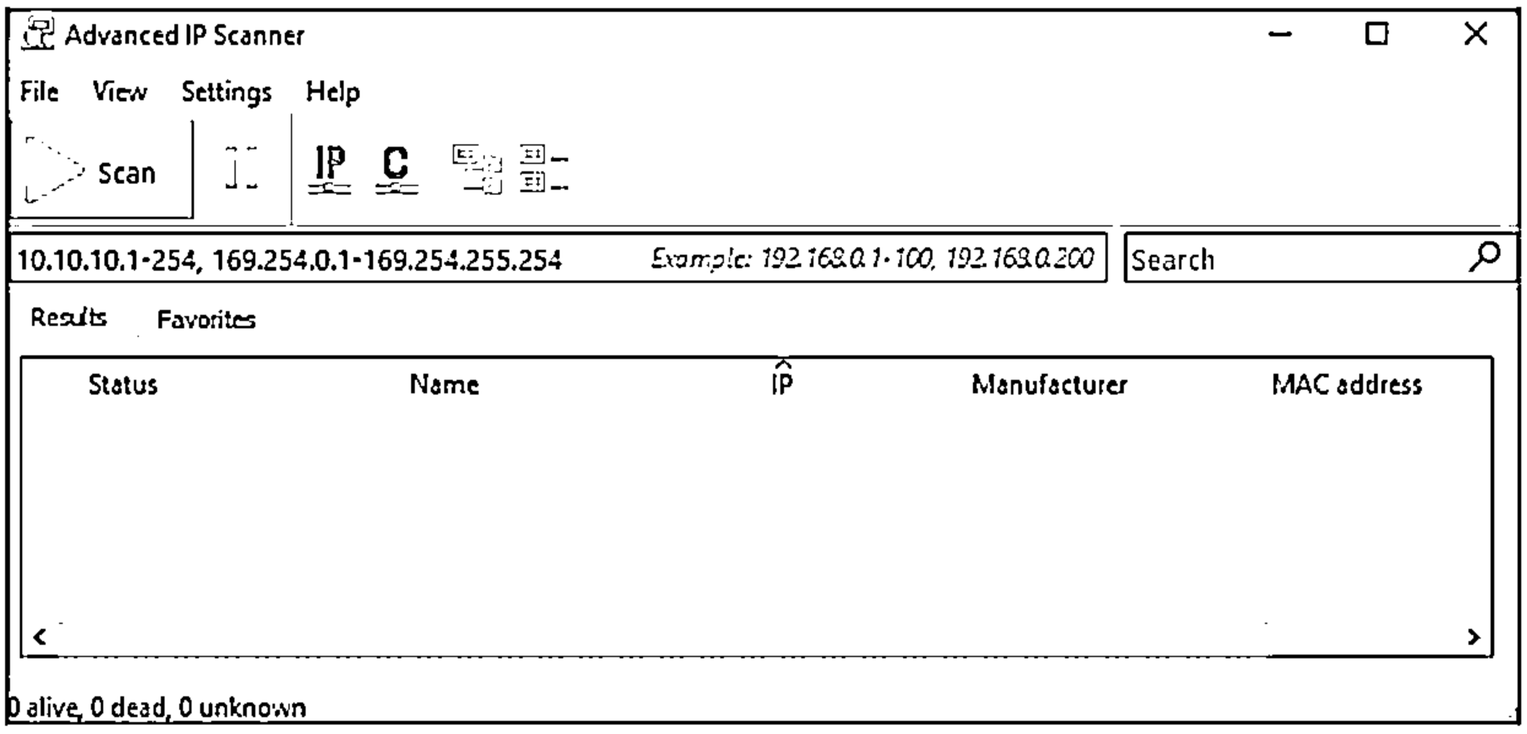


Figure 7.2.2: Advanced IP Scanner main window

TASK 2.2

Scan a Network to Discover Hosts

7. In the **IP address range** field, specify the IP range (in this example, we will target **10.10.10.5-10.10.10.20**). Click the **Scan** button.

Note: The IP address range might vary in your lab environment.

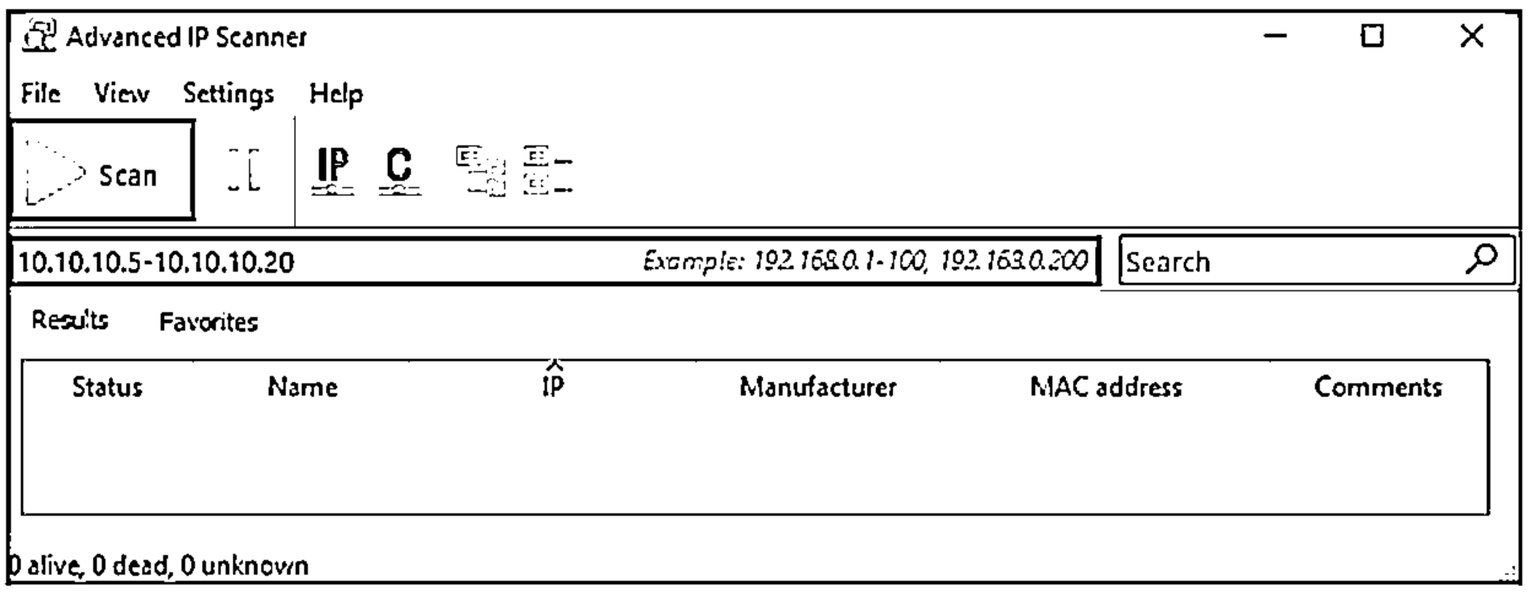


Figure 7.2.3: Scanning a Subnet

8. **Advanced IP Scanner** scans the target IP address range, with progress tracked by the status bar at the bottom of the window. Wait for the scan to complete.

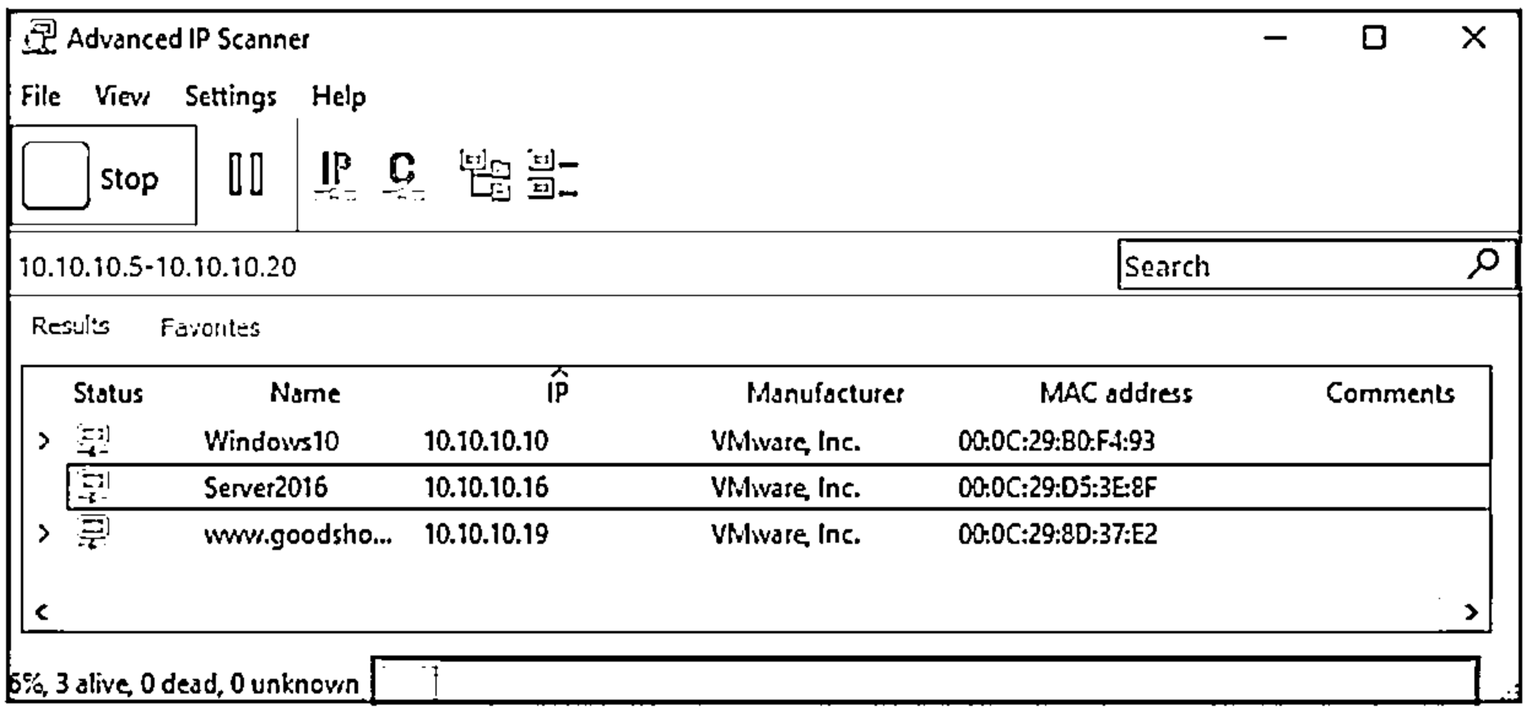


Figure 7.2.4: Advanced IP Scanner displaying the list of alive hosts

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

9. The scan results appear, displaying information about active hosts in the target network such as status, machine name, IP address, manufacturer name, and MAC addresses, as shown in the screenshot.

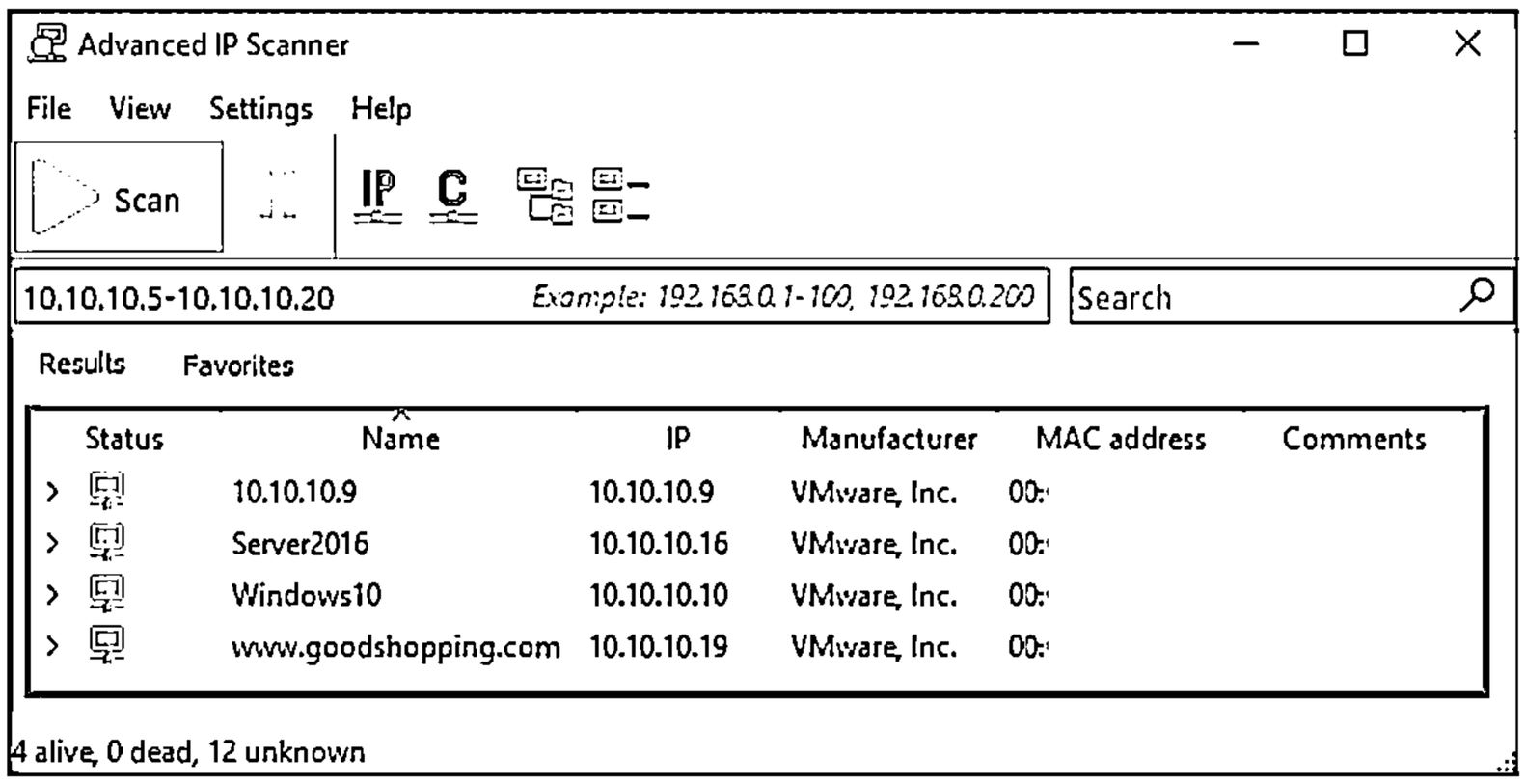


Figure 7.2.5: Advanced IP Scanner results

10. Click the **Expand all** icon ( ) to view the shared folders and services running on the target network.

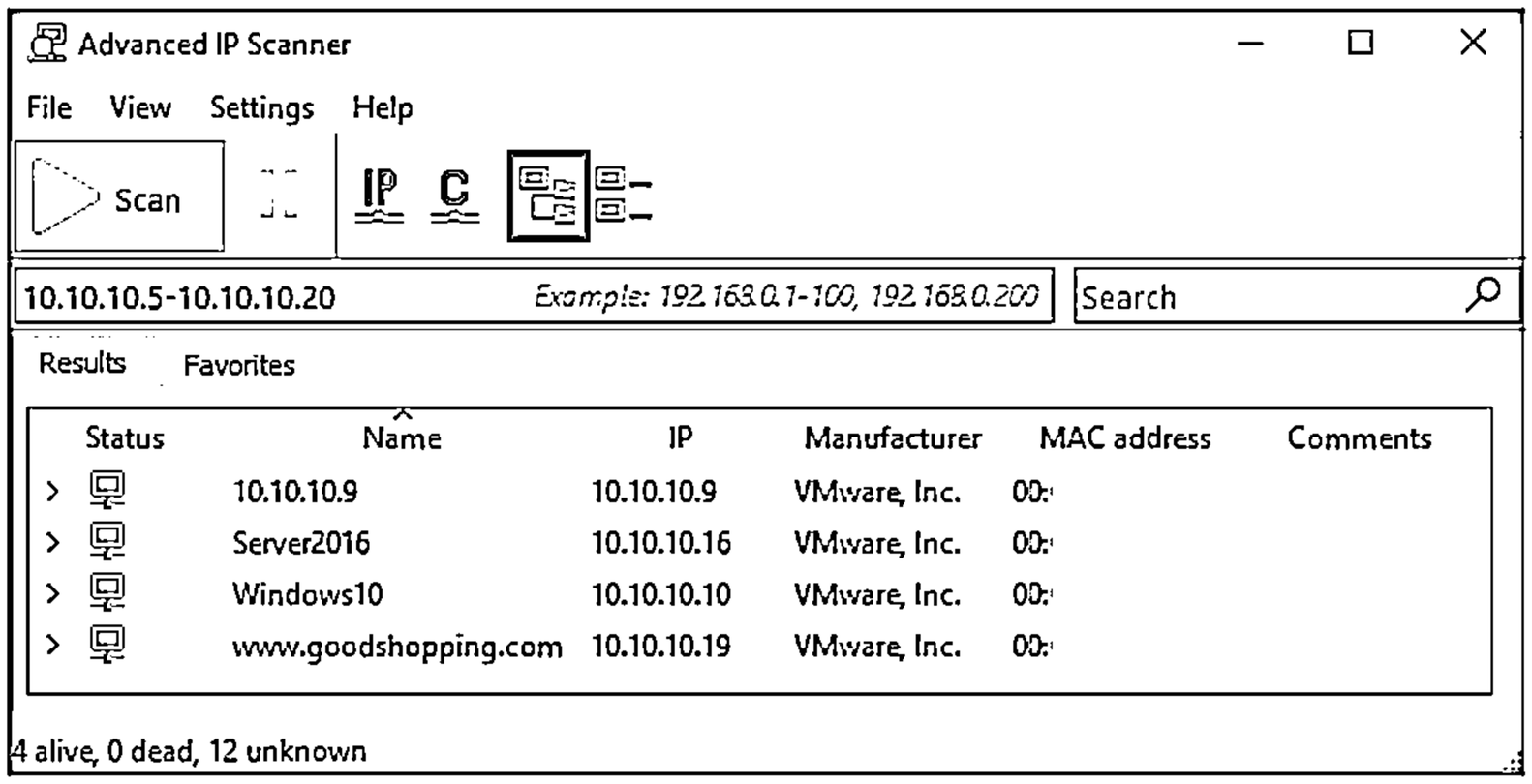


Figure 7.2.6: Advanced IP Scanner click the Expand all icon

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

11. The shared folders and services running on the target network appear, as shown in the screenshot.

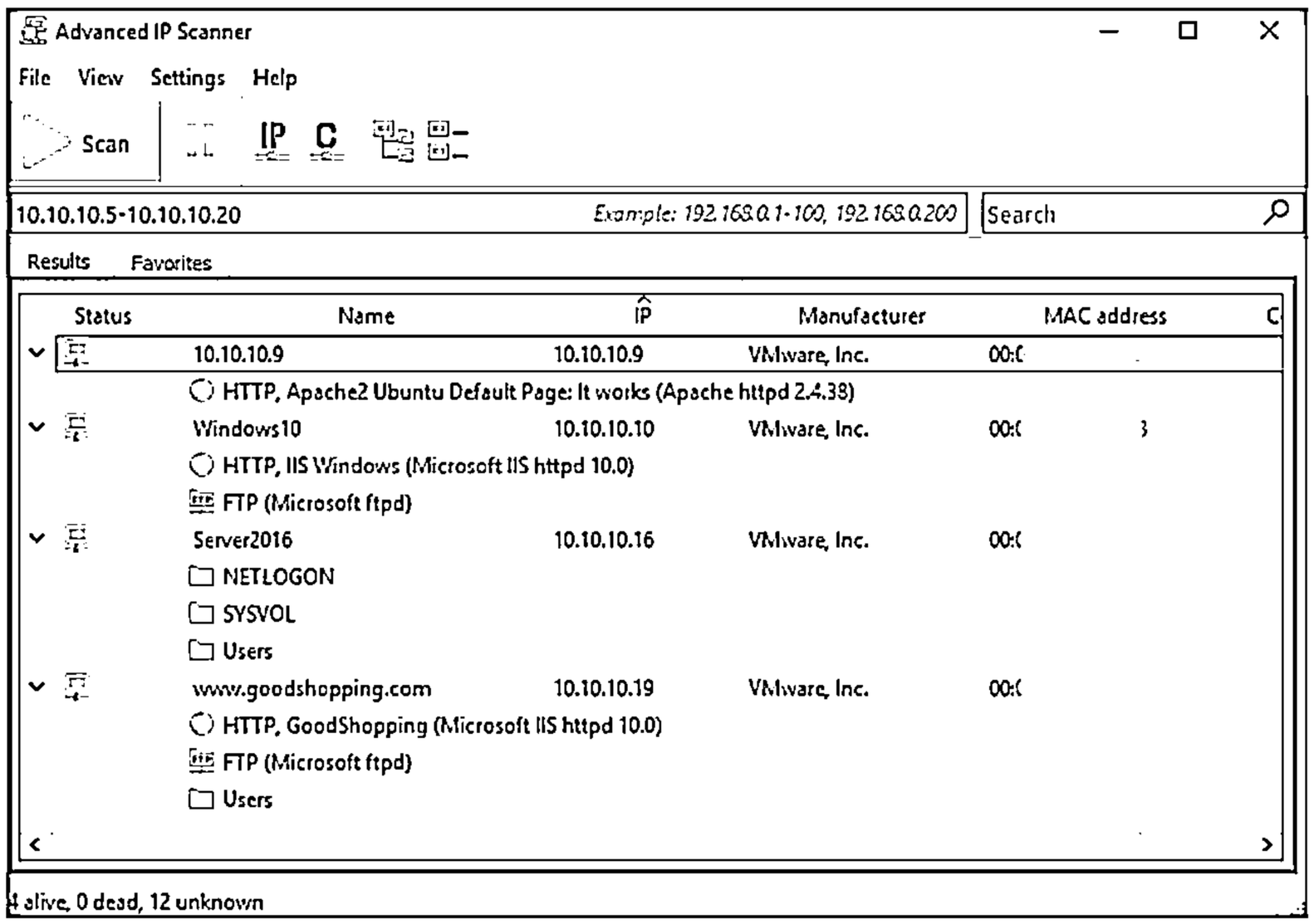


Figure 7.2.7: Advanced IP Scanner displaying shared folders and services

TASK 2.3

Examine the Options

12. Right-click any of the detected IP addresses to list available options.

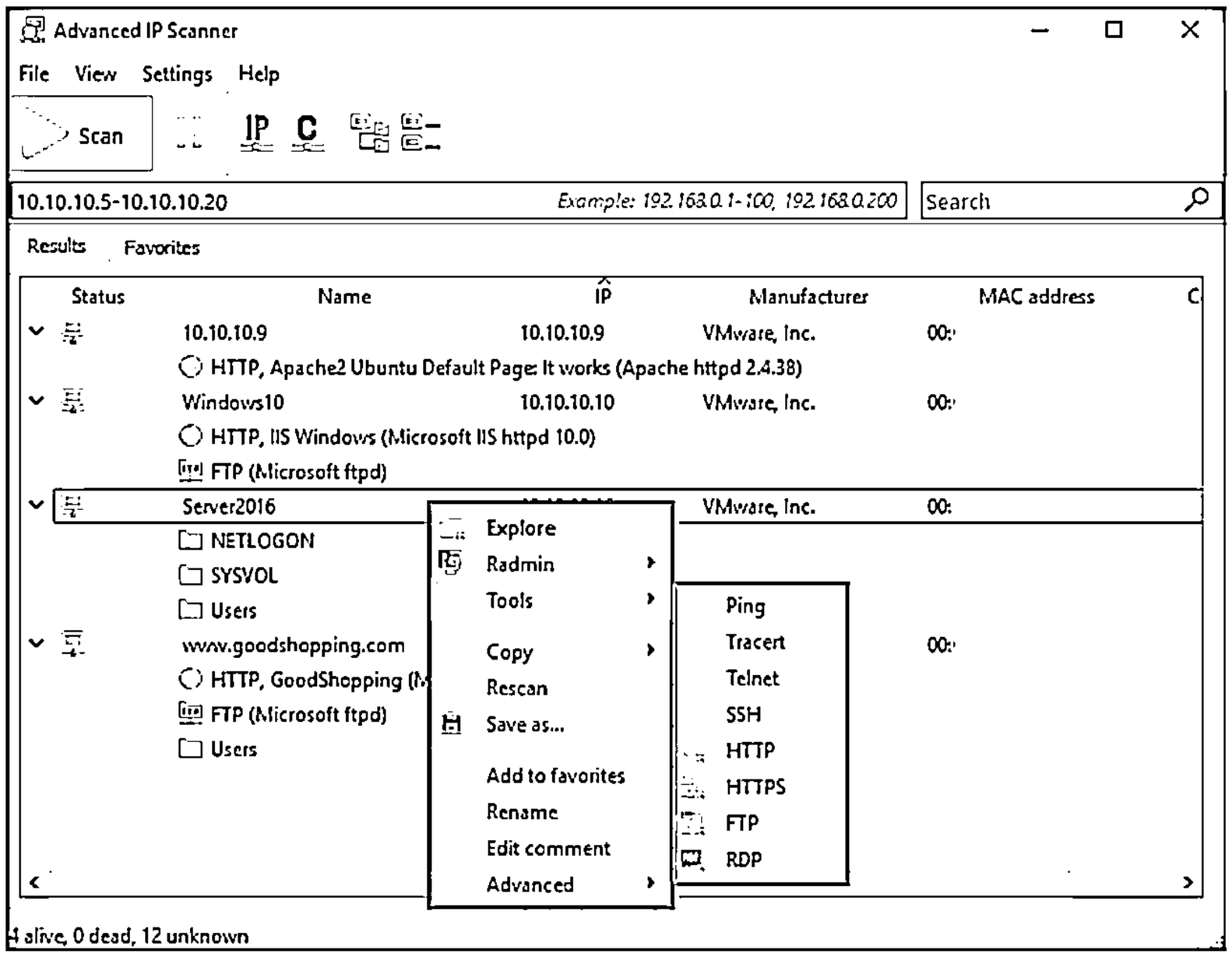


Figure 7.2.8: Exploring the available options

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

13. Using these options, you can ping, traceroute, transfer files, chat, send a message, connect to the target machine remotely (using **Radmin**), etc.

Note: To use the Radmin option, you need to install Radmin viewer, which you can download at **http://www.radmin.com**.

14. In the same way, you can select various other options to retrieve shared files, view system-related information, etc.
15. This concludes the demonstration of enumerating network resources using Advanced IP Scanner.
16. Close all open windows and document all the acquired information.
17. Turn off the **Windows 10**, **Windows Server 2019**, and **Ubuntu** virtual machines.

TASK 3 Enumerate Information from Windows and Samba Hosts using Enum4linux

Enum4linux is a tool for enumerating information from Windows and Samba systems. It is used for share enumeration, password policy retrieval, identification of remote OSes, detecting if hosts are in a workgroup or a domain, user listing on hosts, listing group membership information, etc.

Here, we will use the Enum4Linux to perform enumeration on a Windows and a Samba host.

1. Start the **Parrot Security** virtual machine.

Note: Ensure that the **Windows Server 2016** virtual machine is still running.

2. Switch to **Parrot Security** virtual machine.
3. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

4. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

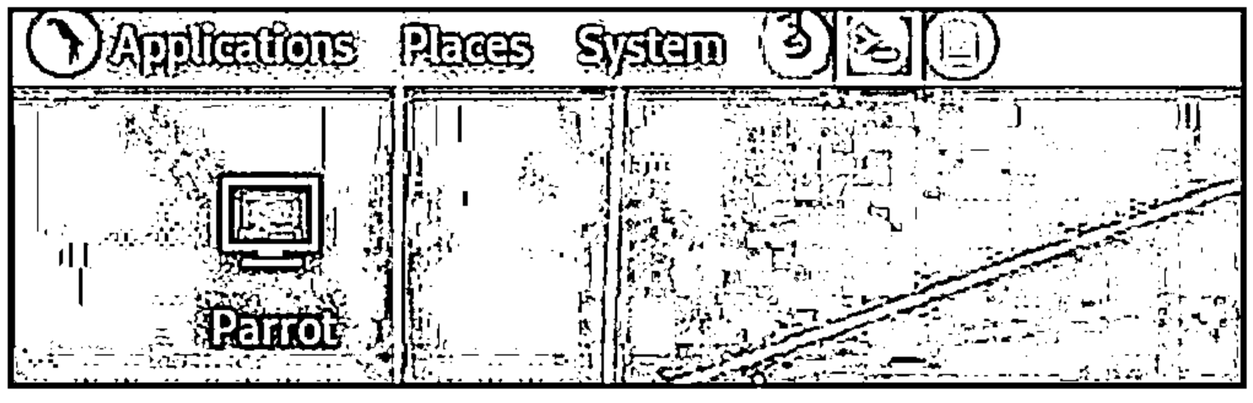


Figure 7.3.1: MATE Terminal Icon

5. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

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

6. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

7. Now, type **cd** and press **Enter** to jump to the root directory.

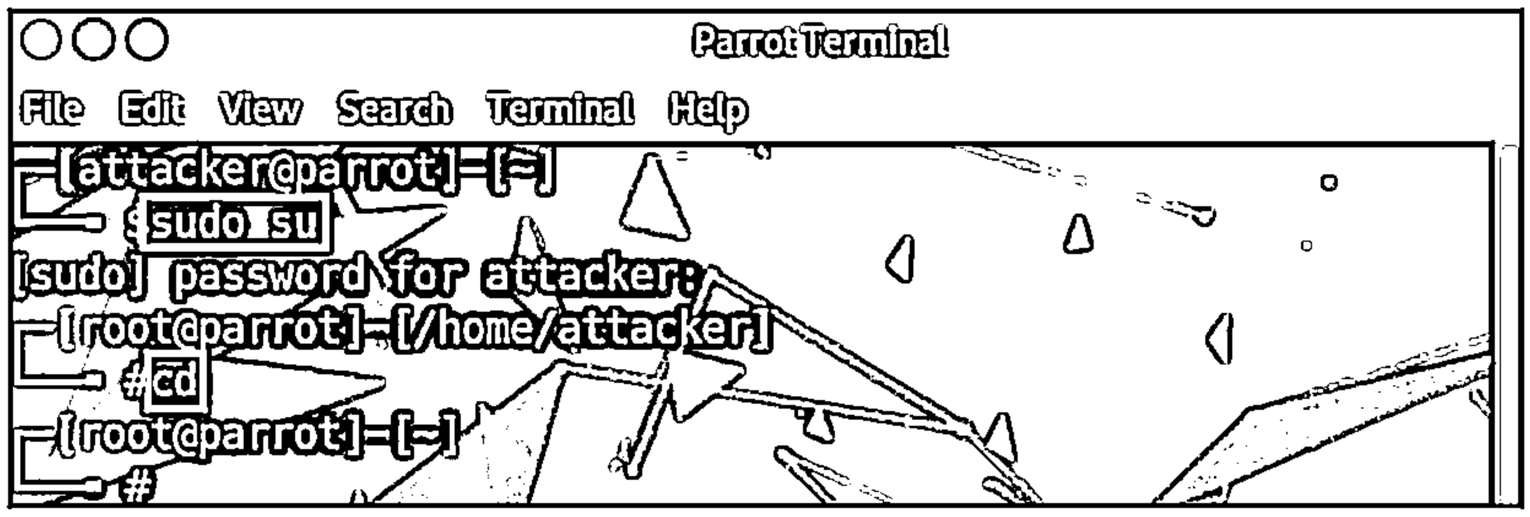


Figure 7.3.2: Running the programs as a root user

TASK 3.1

Check Enum4linux Options

8. In the **Parrot Terminal** window, type **enum4linux -h** and press **Enter** to view the various options available with enum4linux.

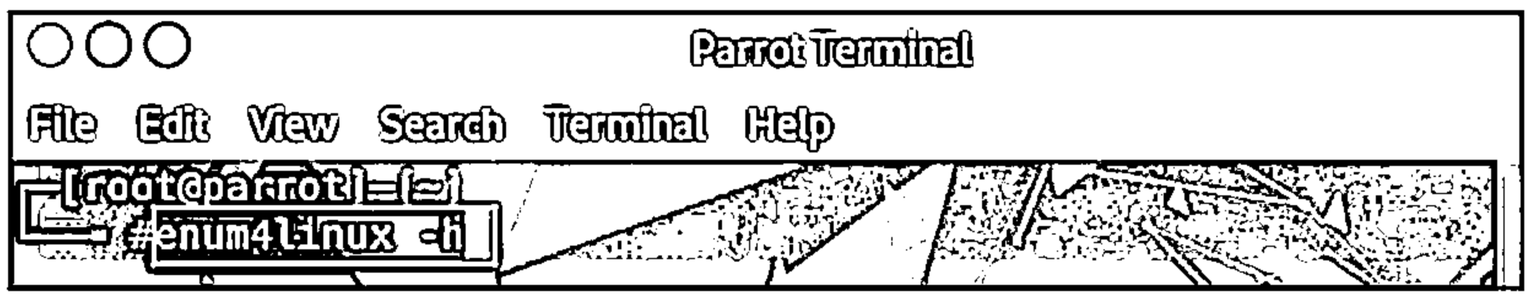


Figure 7.3.3: Enum4linux help command

9. The help options appear, as shown in the screenshot. In this lab, we will demonstrate only a few options to conduct enumeration on the target machine.

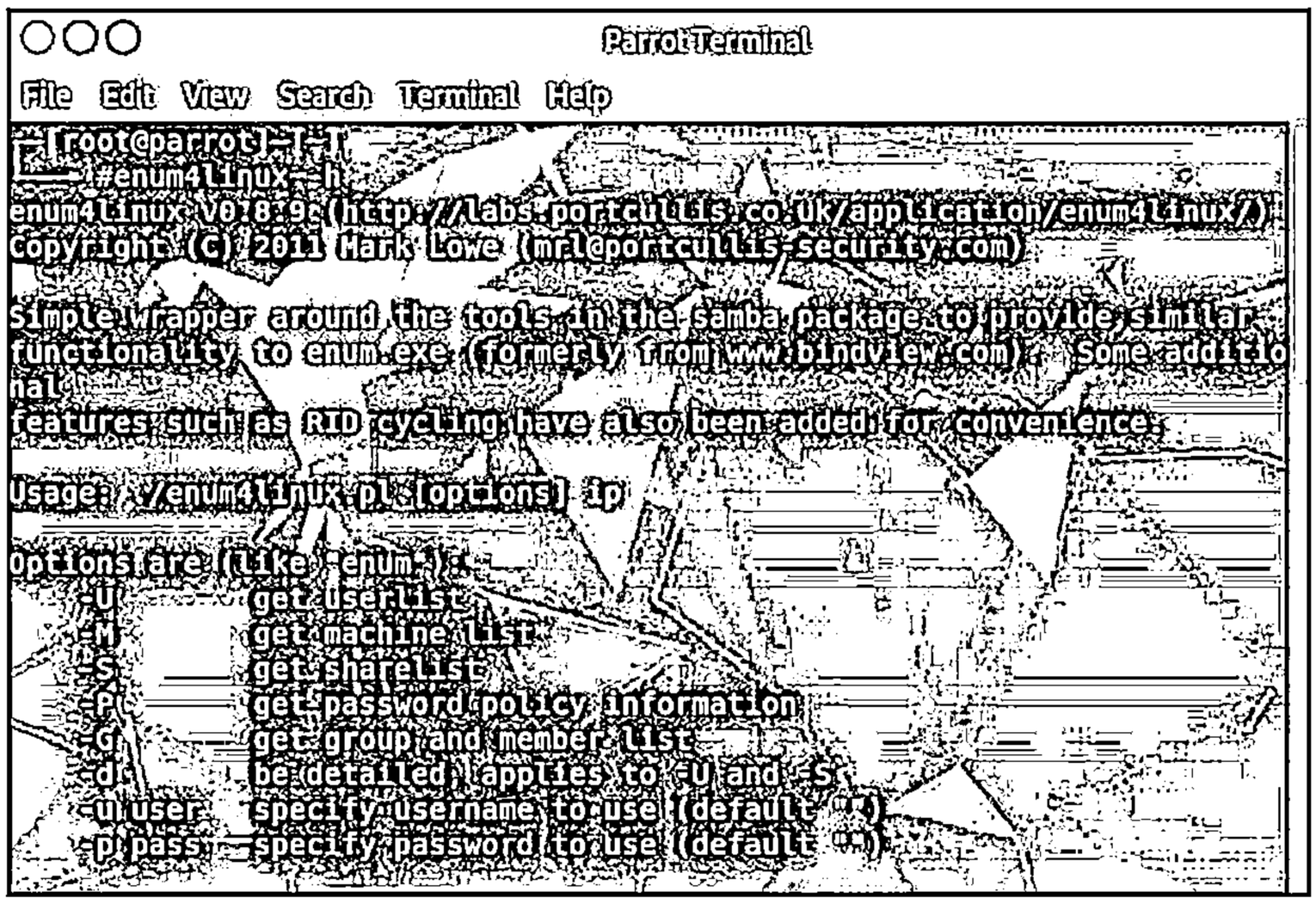


Figure 7.3.4: Enum4linux help options

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

TASK 3.2

Test for NetBIOS Info

10. We will first enumerate the NetBIOS information of the target machine. In the terminal window, type **enum4linux -u martin -p apple -n <Target IP Address>** (in this case, **10.10.10.16**) and hit **Enter**.

Note: In this command, **-u user** specifies the username to use and **-p pass** specifies the password.

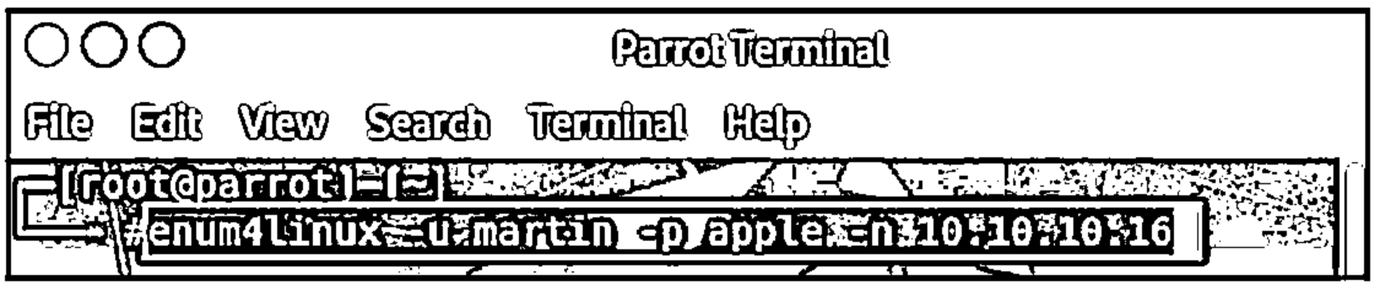


Figure 7.3.5: Enum4linux command for nbtstat info

11. The tool enumerates the target system and displays the NetBIOS information under the **Nbtstat Information** section.

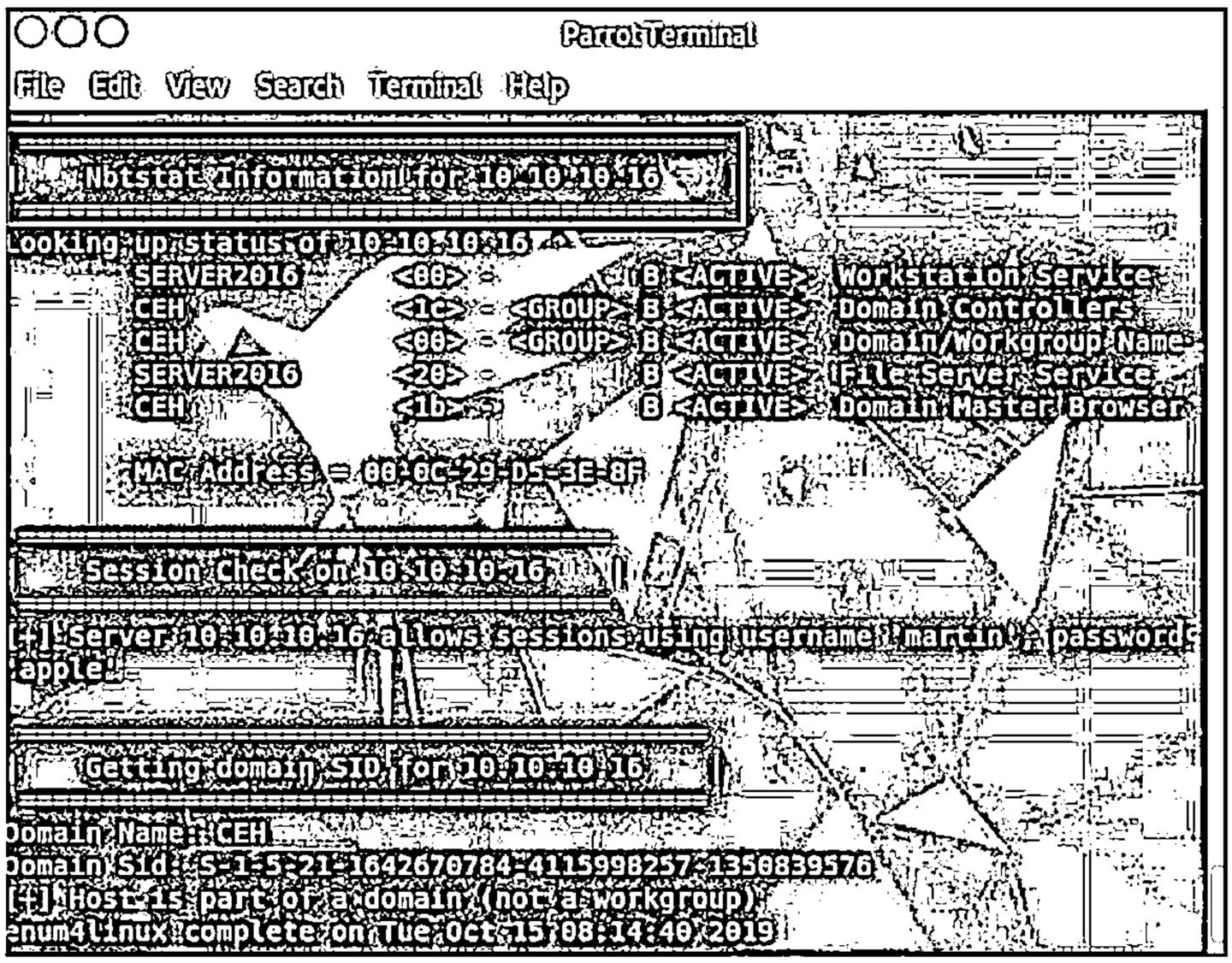


Figure 7.3.6: The target's NetBIOS information

TASK 3.3

Test for User Info

12. In the terminal window, type **enum4linux -u martin -p apple -U <Target IP Address>** (in this case, **10.10.10.16**) and hit **Enter** to run the tool with the "get userlist" option.

Note: In this case, **10.10.10.16** is the IP address of the **Windows Server 2016**; this might be different in your lab environment.

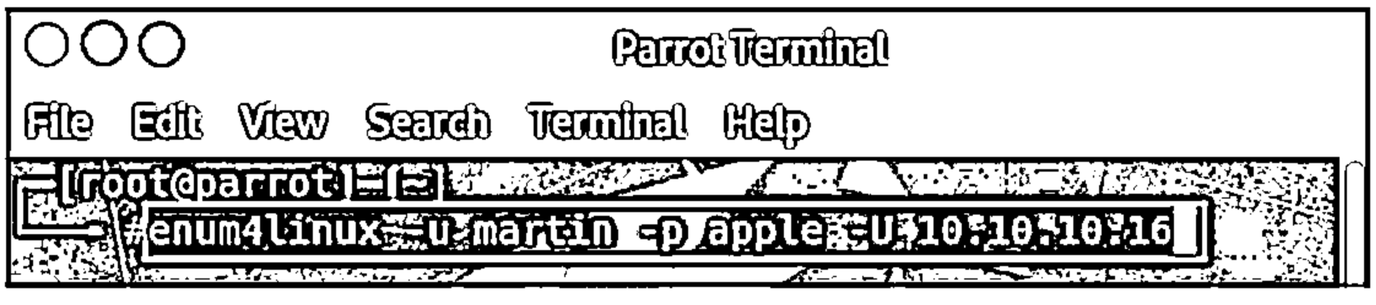


Figure 7.3.7: Enum4linux command with Get userlist option enabled

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

13. Enum4linux starts enumerating and displays data such as Target Information, Workgroup/Domain, domain SID (security identifier), and the list of users, along with their respective RIDs (relative identifier), as shown in the screenshots below.

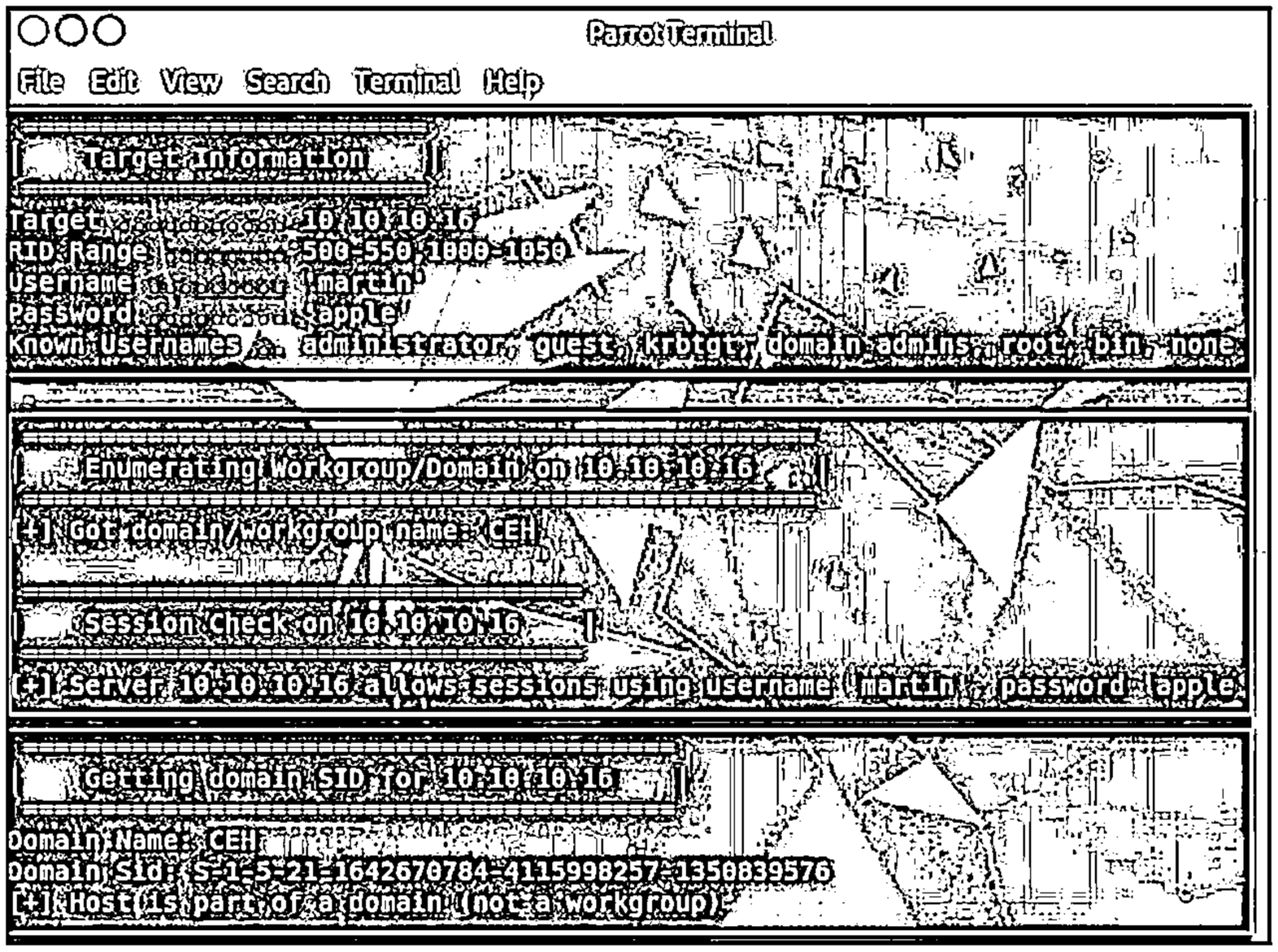


Figure 7.3.8: Enum4linux enumerating the target's domain information

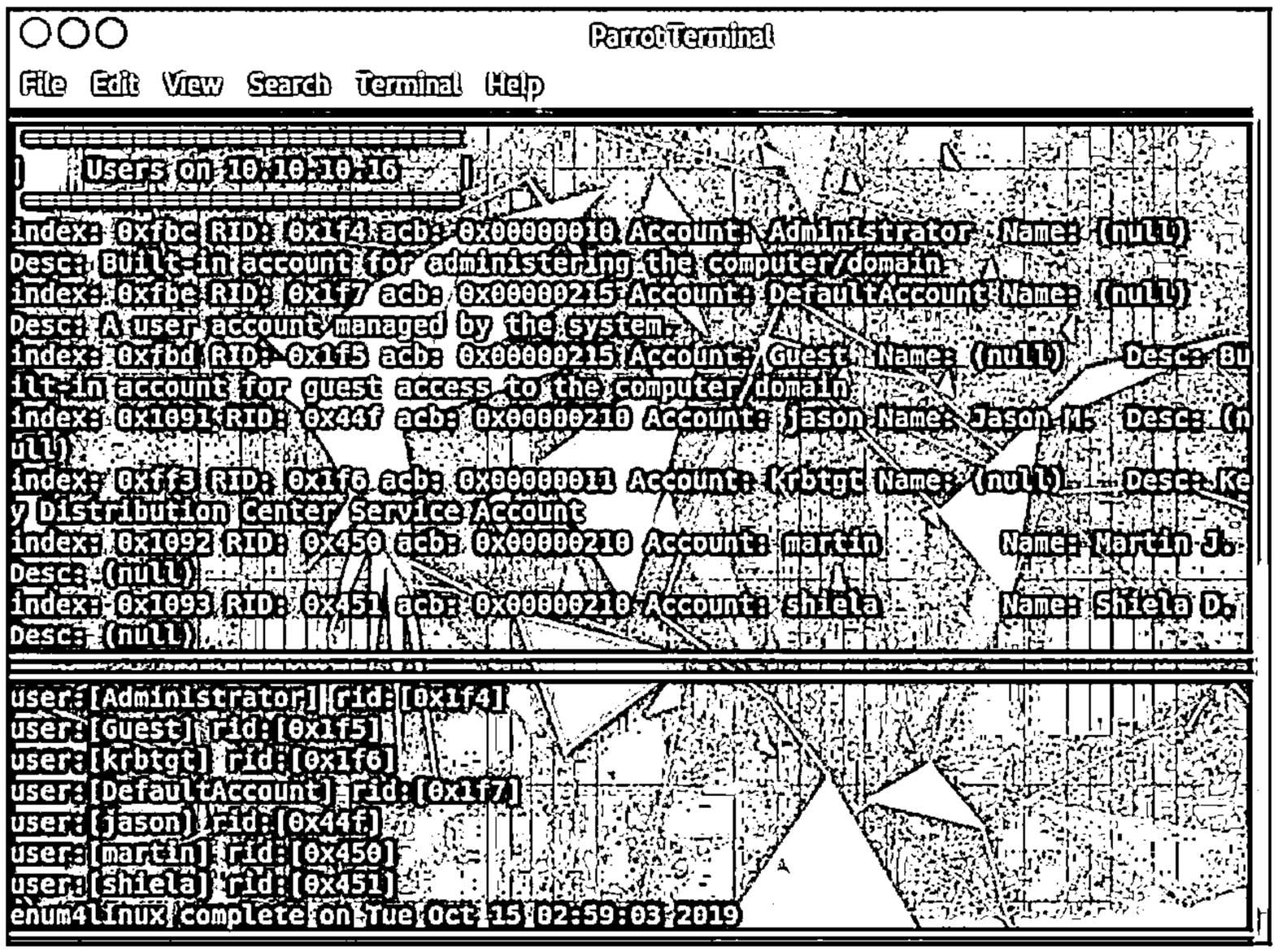


Figure 7.3.9: User information with their respective RIDs

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

TASK 3.4

Test for OS Info

14. Second, we will obtain the OS information of the target; type **enum4linux -u martin -p apple -o <Target IP Address>** (in this case, **10.10.10.16**) and hit **Enter**.

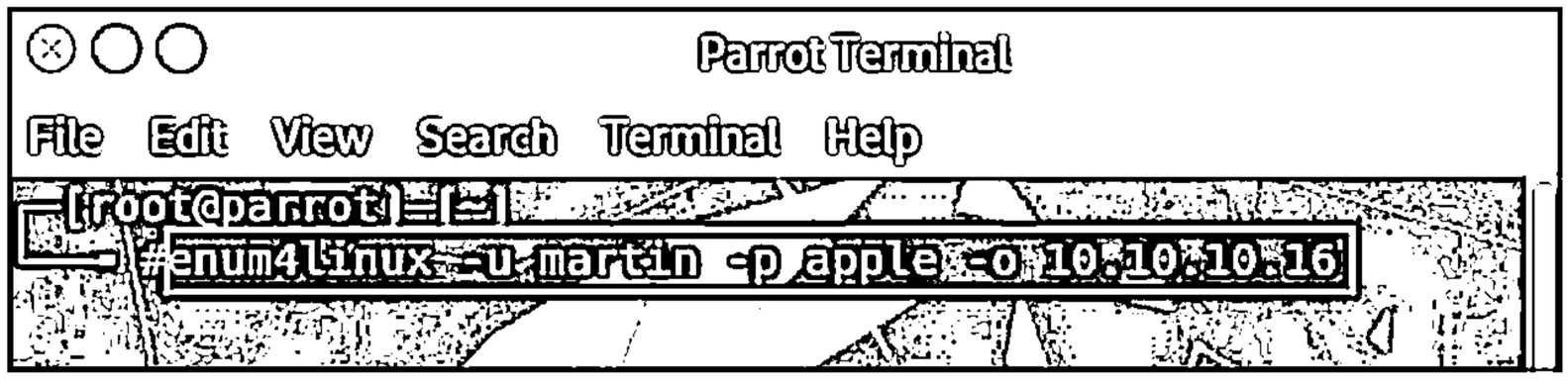


Figure 7.3.10: Enum4linux command for enumerating OS information

15. The tool enumerates the target system and lists its OS details, as shown in the screenshot.

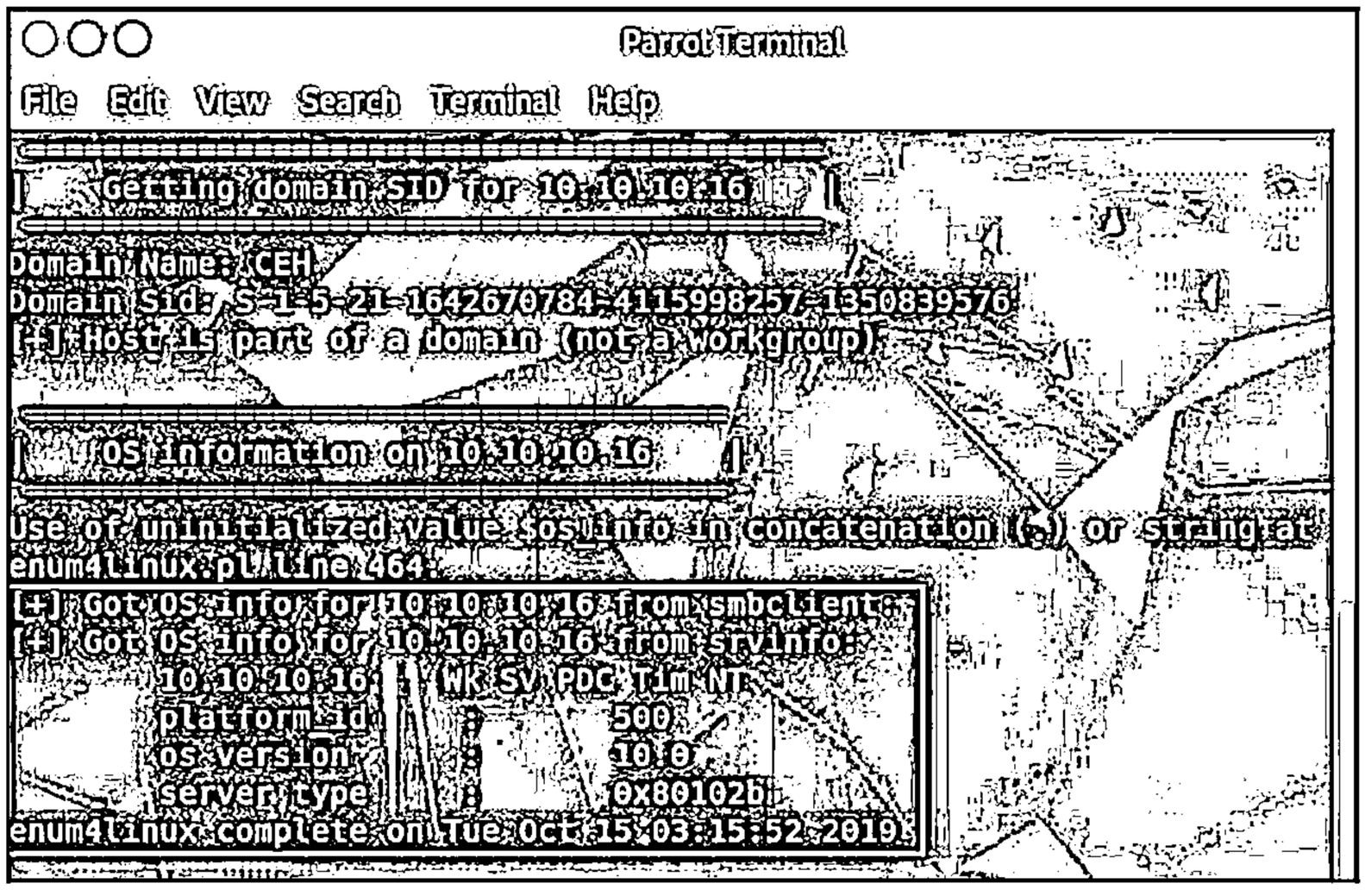


Figure 7.3.11: OS information of the target

TASK 3.5

Test for Password Policy Info

16. Third, we will enumerate the password policy information of our target machine. In the terminal window, type **enum4linux -u martin -p apple -P <Target IP Address>** (in this case, **10.10.10.16**) and hit **Enter**.

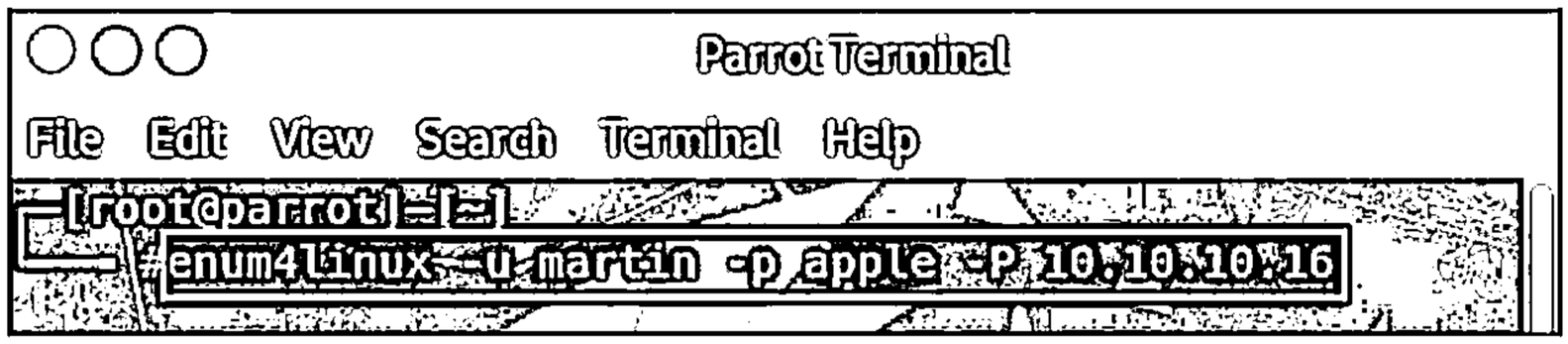


Figure 7.3.12: Enum4linux command to enumerate password policy information

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

17. The tool enumerates the target system and displays its password policy information, as shown in the screenshot.

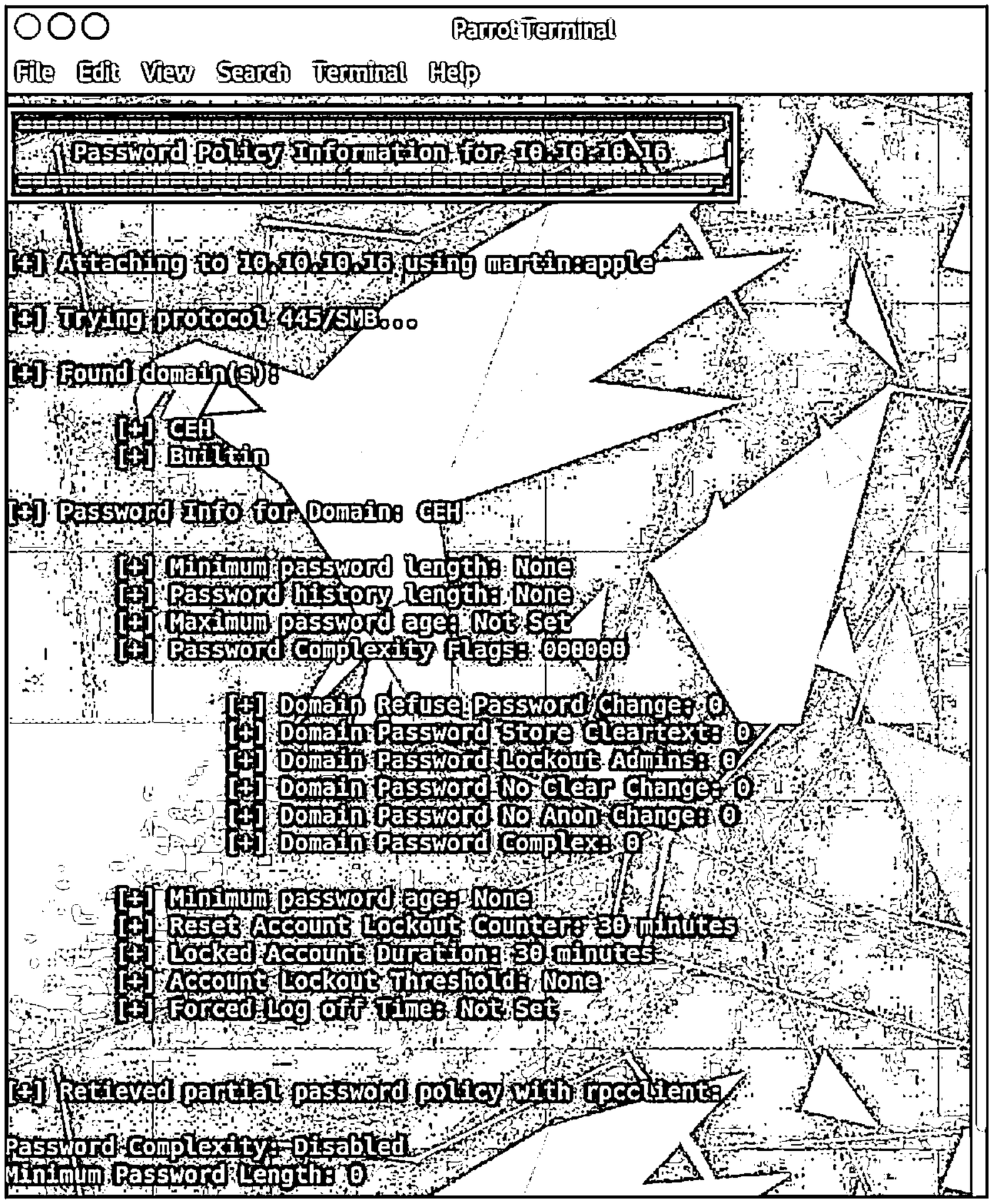


Figure 7.3.13: The password policy information for the target system

TASK 3.6

Test for Group Info

18. Fourth, we will enumerate the target machine's group policy information. In the terminal window, type **enum4linux -u martin -p apple -G <Target IP Address>** (in this case, **10.10.10.16**) and hit **Enter**.

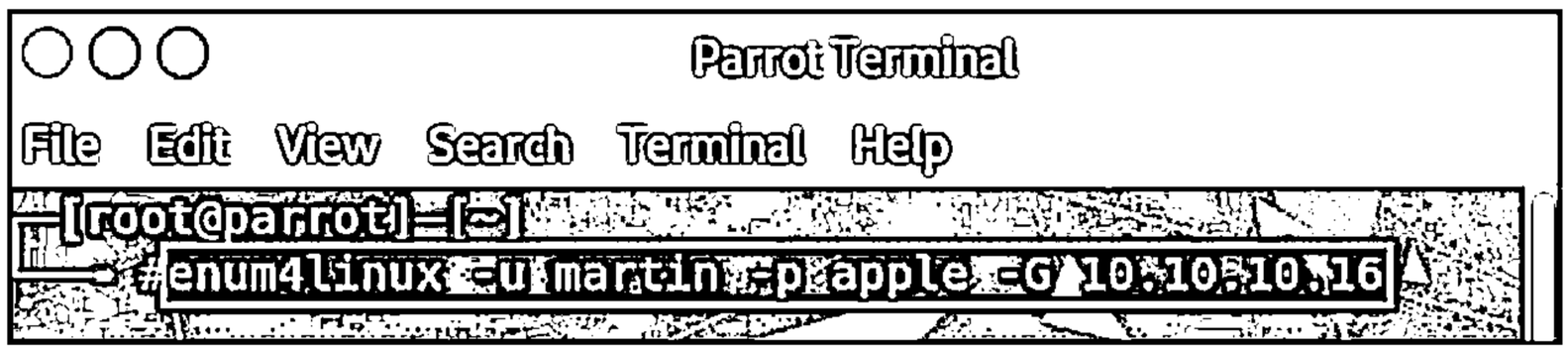


Figure 7.3.14: Enum4linux command for group and domain information

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

19. The tool enumerates the target system and displays the group policy information, as shown in the screenshot.

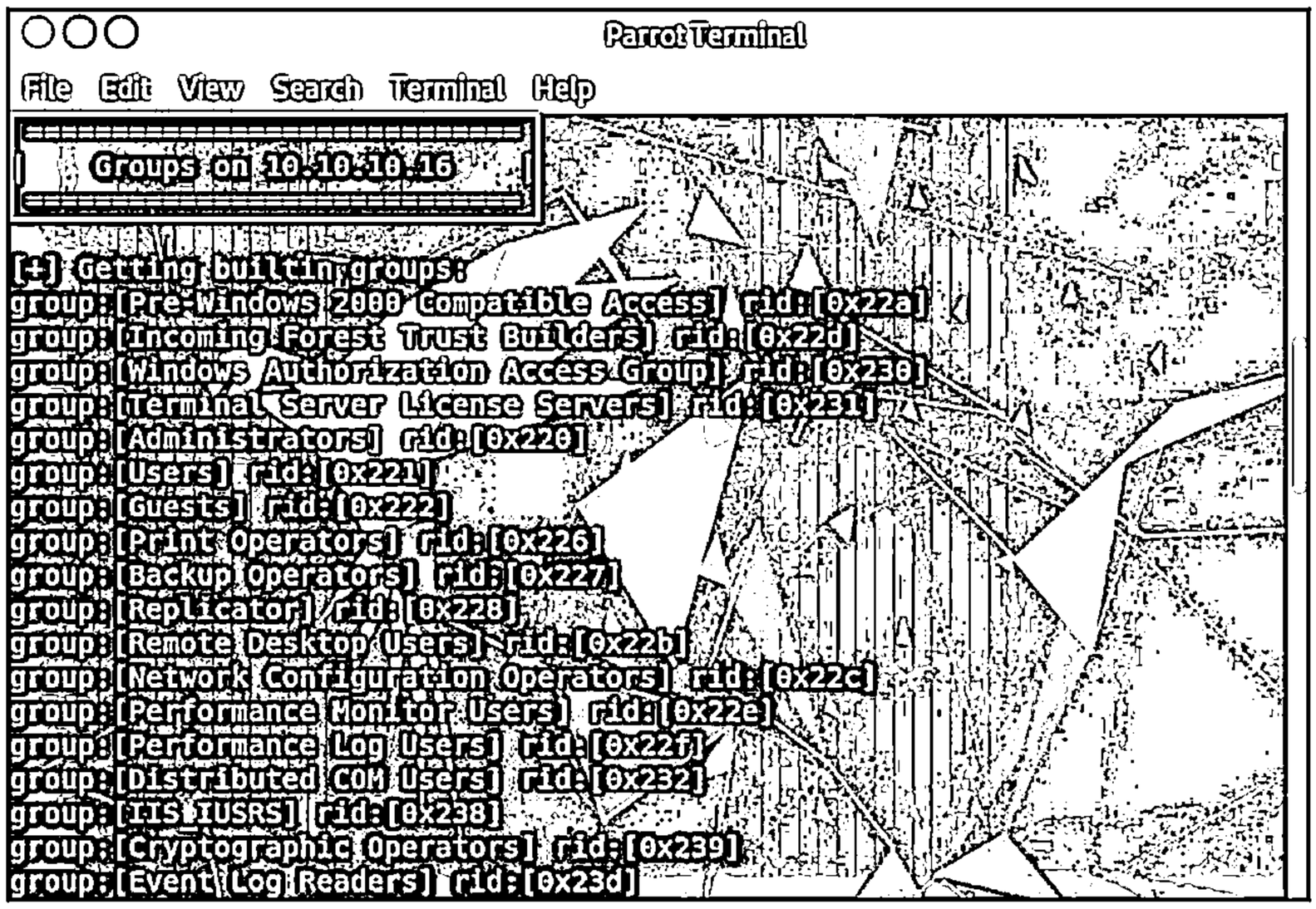


Figure 7.3.15: The target's group policy information

20. It further enumerates the built-in group memberships, local group memberships, etc. displaying them as shown in the screenshot.

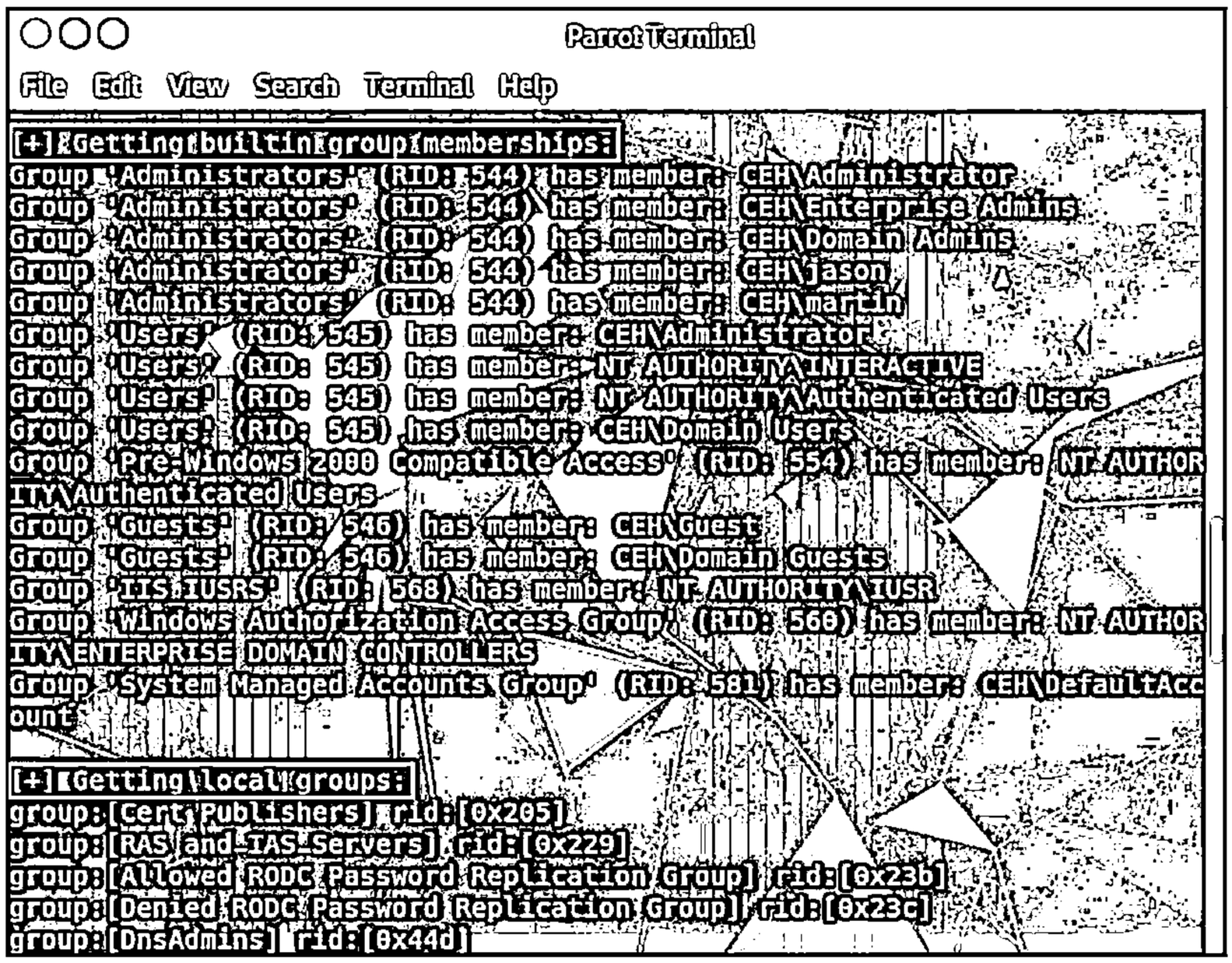


Figure 7.3.16: The target system's domain and group memberships

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

TASK 3.7

Test for Share Info

21. Finally, we will enumerate the share policy information of our target machine. Type **enum4linux -u martin -p apple -S <Target IP Address>** (in this case, **10.10.10.16**) and hit **Enter**.

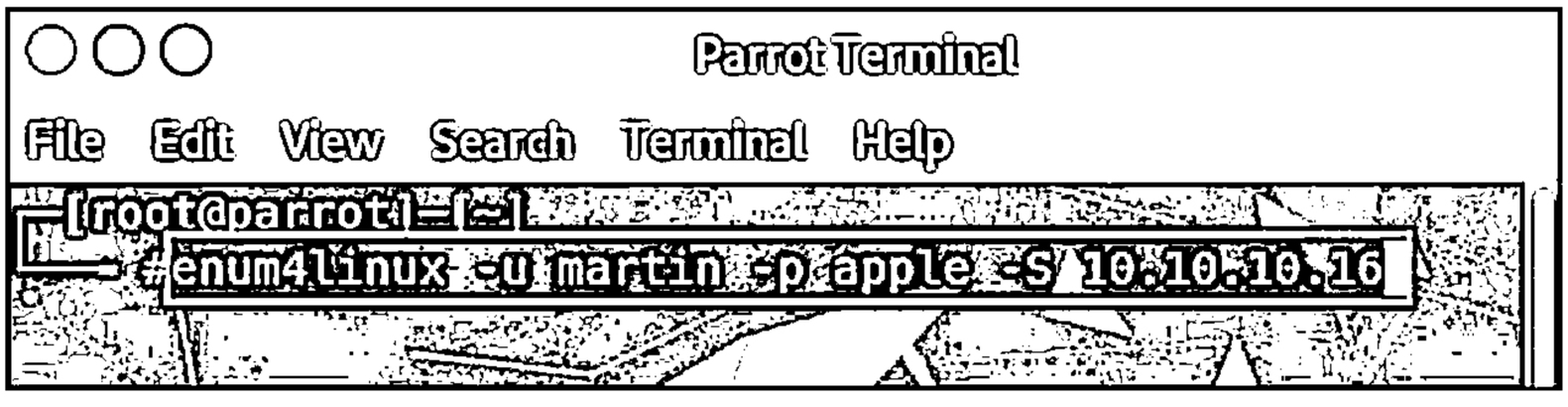


Figure 7.3.17: The enum4linux command that obtains the target system's share policy information

22. The result appears, displaying the enumerate shared folders on the target system.

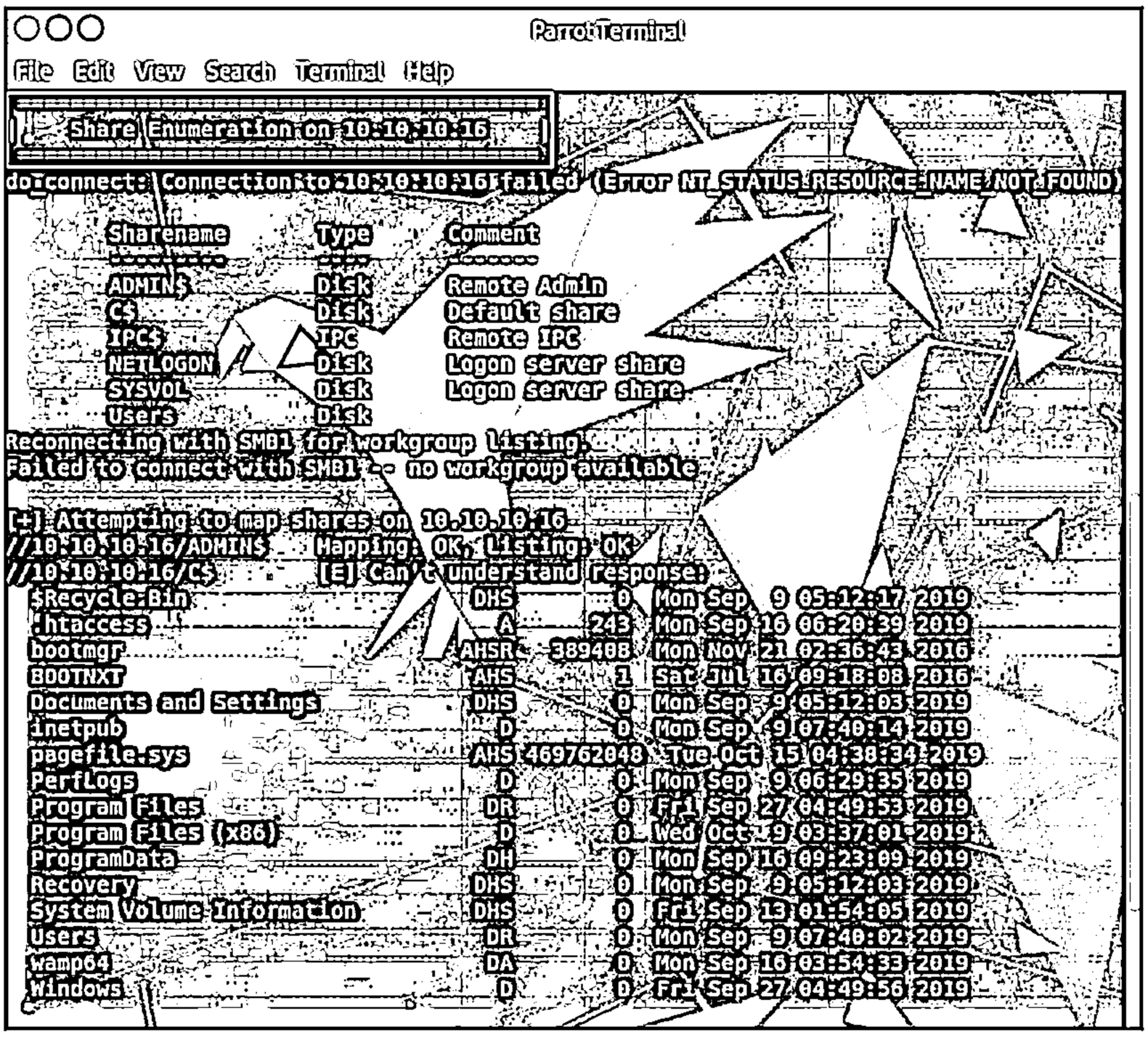


Figure 7.3.18: Share information for the target system

23. This concludes the demonstration performing enumeration using Enum4linux.
24. Close all open windows and document all the acquired information.
25. Turn off the **Parrot Security** and **Windows Server 2016** virtual machines.

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

Lab Analysis

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

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT 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.

Vulnerability Analysis

Module 05

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

Vulnerability Assessment

Vulnerability assessment is an examination of the ability of a system or application, including current security procedures and controls, to withstand an assault. Vulnerability research is the process of discovering vulnerabilities and design flaws that leave an OS and its applications open to attack or misuse.

Lab Scenario

ICON KEY

Valuable information

Test your knowledge

Web exercise

Workbook review

Earlier, all possible information about a target system such as system name, OS details, shared network resources, policies and passwords details, and users and user groups were gathered.

Now, as an ethical hacker or penetration tester (hereafter, pen tester), your next step is to perform vulnerability research and a vulnerability assessment on the target system or network. Ethical hackers or pen testers need to conduct intense research with the help of information acquired in the footprinting and scanning phases to discover vulnerabilities.

Vulnerability assessments scan networks for known security weaknesses: it recognizes, measures, and classifies security vulnerabilities in a computer system, network, and communication channel; and evaluates the target systems for vulnerabilities such as missing patches, unnecessary services, weak authentication, and weak encryption. Additionally, it assists security professionals in securing the network by determining security loopholes or vulnerabilities in the current security mechanism before attackers can exploit them.

The information gleaned from a vulnerability assessment helps you to identify weaknesses that could be exploited and predict the effectiveness of additional security measures in protecting information resources from attack.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 05 Vulnerability Analysis

The labs in this module will give you real-time experience in collecting information regarding underlying vulnerabilities in the target system using various online sources and vulnerability assessment tools.

Lab Objectives

The objective of this lab is to extract information about the target system that includes, but not limited to:

- Network vulnerabilities
- IP and Transmission Control Protocol/User Datagram Protocol (TCP/UDP) ports and services that are listening
- Application and services configuration errors/vulnerabilities
- The OS version running on computers or devices
- Applications installed on computers
- Accounts with weak passwords

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

- Files and folders with weak permissions
- Default services and applications that may have to be uninstalled
- Mistakes in the security configuration of common applications
- Computers exposed to known or publicly reported vulnerabilities

Lab Environment

To carry out this lab, you need:

- Windows Server 2019 virtual machine
- Windows Server 2016 virtual machine
- Windows 10 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 75 Minutes

Overview of Vulnerability Assessment

Vulnerability assessment plays a major role in providing security to any organization's resources and infrastructure from various internal and external threats. To secure a network, an administrator needs to perform patch management, install proper antivirus software, check configurations, solve known issues in third-party applications, and troubleshoot hardware with default configurations. All these activities together constitute vulnerability assessment.

Network vulnerability scanning can be categorized into active scanning and passive scanning:

- **Active Scanning:** Interacts directly with the target network to find vulnerabilities by sending probes and specially crafted requests to the target host in the network
- **Passive Scanning:** Finds vulnerabilities without directly interacting with the target network and identifying vulnerabilities via information exposed by systems in their normal communications

Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to collect information about the underlying vulnerability in a target system or network. Recommended labs that will assist you in learning various vulnerability assessment techniques include:

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

Lab No.	Lab Exercise Name	Core*	Self-study**	iLabs ***
1	Perform Vulnerability Research with Vulnerability Scoring Systems and Databases	√	√	√
	1.1 Perform Vulnerability Research in Common Weakness Enumeration (CWE)	√		√
	1.2 Perform Vulnerability Research in Common Vulnerabilities and Exposures (CVE)		√	√
	1.3 Perform Vulnerability Research in National Vulnerability Database (NVD)		√	√
2	Perform Vulnerability Assessment using Various Vulnerability Assessment Tools	√	√	√
	2.1 Perform Vulnerability Analysis using OpenVAS	√		√
	2.2 Perform Vulnerability Scanning using Nessus		√	√
	2.3 Perform Vulnerability Scanning using GFI LanGuard		√	√
	2.4 Perform Web Servers and Applications Vulnerability Scanning using CGI Scanner Nikto		√	√

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

***Core** - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv11 volume 1 book.

*****iLabs** - Lab exercise(s) marked under iLabs are available in our iLabs solution. iLabs is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed from anywhere with an Internet connection. If you are interested to learn more about our iLabs solution, please contact your training center or visit https://ilabs.eccouncil.org.

Lab Analysis

Analyze and document the results related to the lab exercise. Give an opinion on your target's security posture and exposure using information collected through a vulnerability assessment.

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

Perform Vulnerability Research with Vulnerability Scoring Systems and Databases

Vulnerability scoring systems and databases are used by security analysts to rank information system vulnerabilities and to provide a composite score of the overall severity and risk associated with identified vulnerabilities.

ICON KEY

- Valuable Information
- Test Your Knowledge
- Web Exercise
- Workbook Review

Lab Scenario

As a professional ethical hacker or pen tester, your first step is to search for vulnerabilities in the target system or network using vulnerability scoring systems and databases. Vulnerability research provides awareness of advanced techniques to identify flaws or loopholes in the software that could be exploited. Using this information, you can use various tricks and techniques to launch attacks on the target system.

Lab Objectives

- Perform vulnerability research in Common Weakness Enumeration (CWE)
- Perform vulnerability research in Common Vulnerabilities and Exposures (CVE)
- Perform vulnerability research in National Vulnerability Database (NVD)

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 05 Vulnerability Analysis

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 20 Minutes

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

Overview of Vulnerabilities in Vulnerability Scoring Systems and Databases

Vulnerability databases collect and maintain information about various vulnerabilities present in the information systems.

The following are some of the vulnerability scoring systems and databases:

- Common Weakness Enumeration (CWE)
- Common Vulnerabilities and Exposures (CVE)
- National Vulnerability Database (NVD)
- Common Vulnerability Scoring System (CVSS)

Lab Tasks

TASK 1

Perform Vulnerability Research in Common Weakness Enumeration (CWE)

Here, we will use CWE to view the latest underlying system vulnerabilities.

Common Weakness Enumeration (CWE) is a category system for software vulnerabilities and weaknesses. It has numerous categories of weaknesses that means that CWE can be effectively employed by the community as a baseline for weakness identification, mitigation, and prevention efforts.

1. Turn on the **Windows 10** virtual machine and log in with the credentials **Admin** and **Pa$$w0rd**.

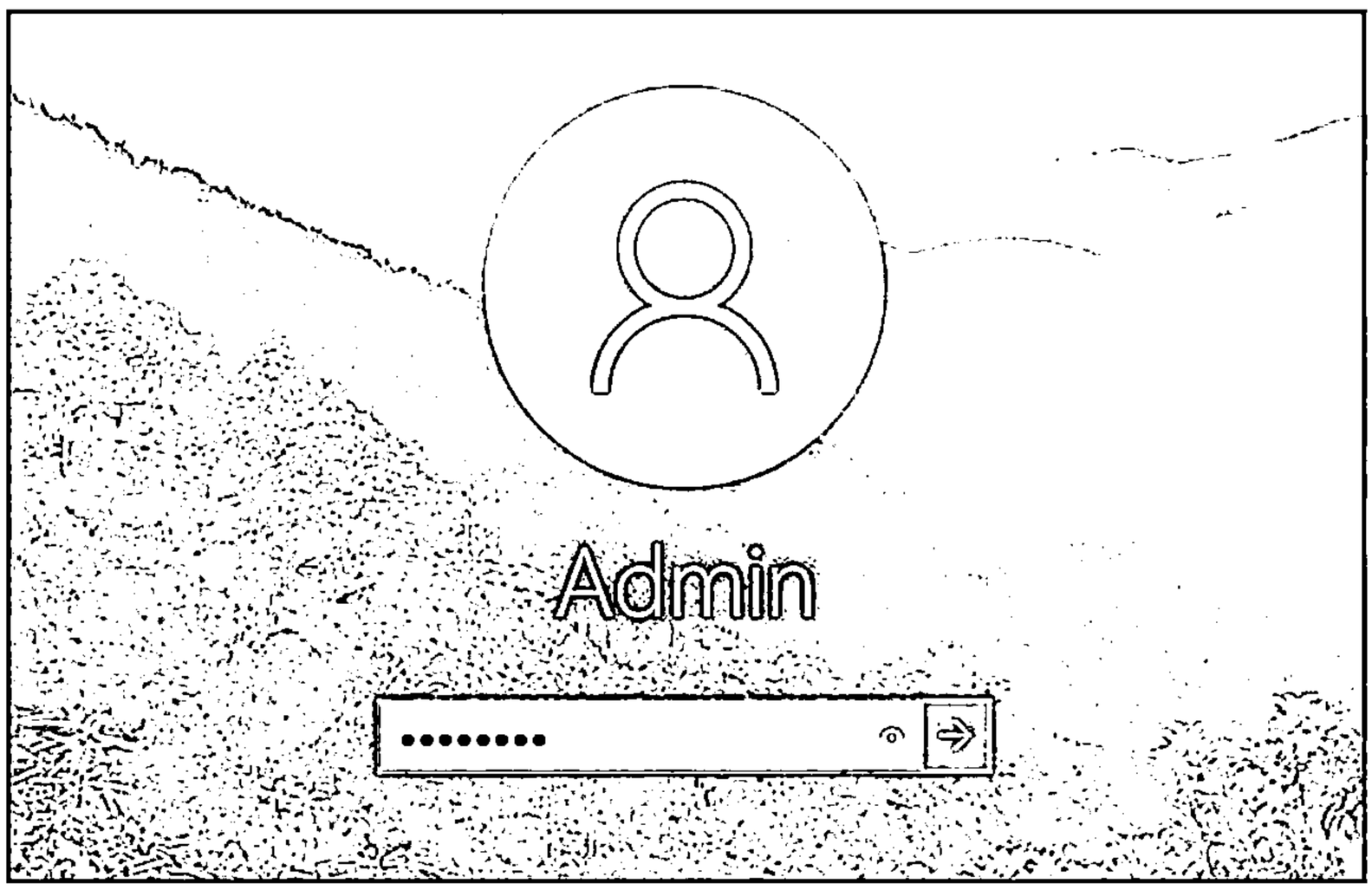


Figure 1.1.1: Login window

Further, CWE has an advanced search technique with which you can search and view the weaknesses based on research concepts, development concepts, and architectural concepts

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

2. Open any web browser (here, **Mozilla Firefox**) and navigate to **https://cwe.mitre.org/.**

Note:

- If the **Default Browser** pop-up window appears, uncheck the **Always perform this check when starting Firefox** checkbox and click the **Not now** button.
- If a **New in Firefox: Content Blocking** pop-up window appears, follow the step and click **Got it** to finish viewing the information.

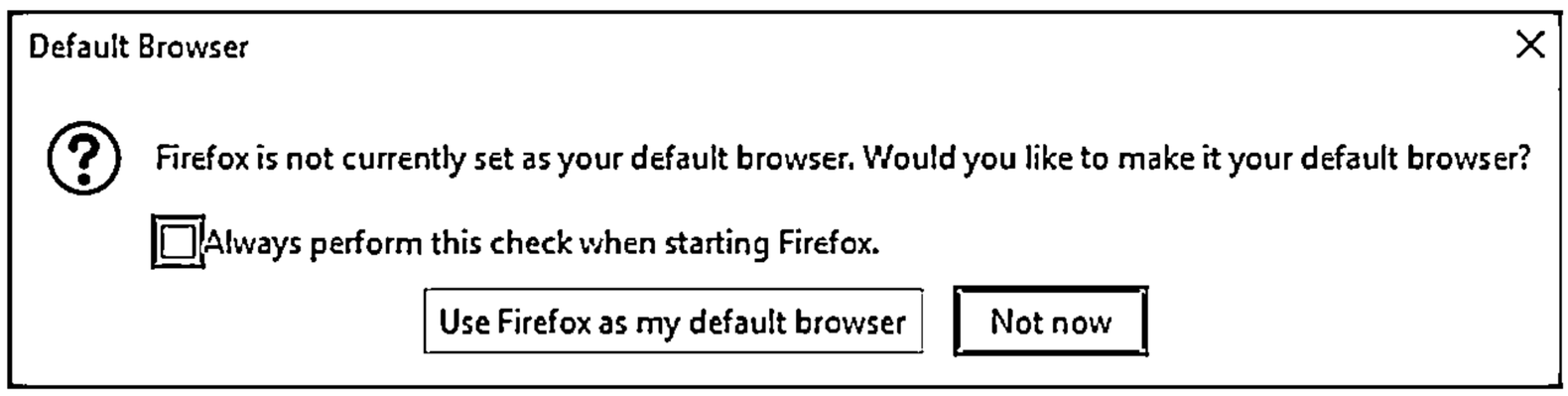


Figure 1.1.2: Default browser pop-up window

3. **CWE** website appears. In the **Google Custom Search** under **Search CWE** section, type **SMB** and click the search ( ) icon.

Note: Here, we are searching for the vulnerabilities of the running services that were found in the target systems in previous module labs (Module 04 Enumeration).

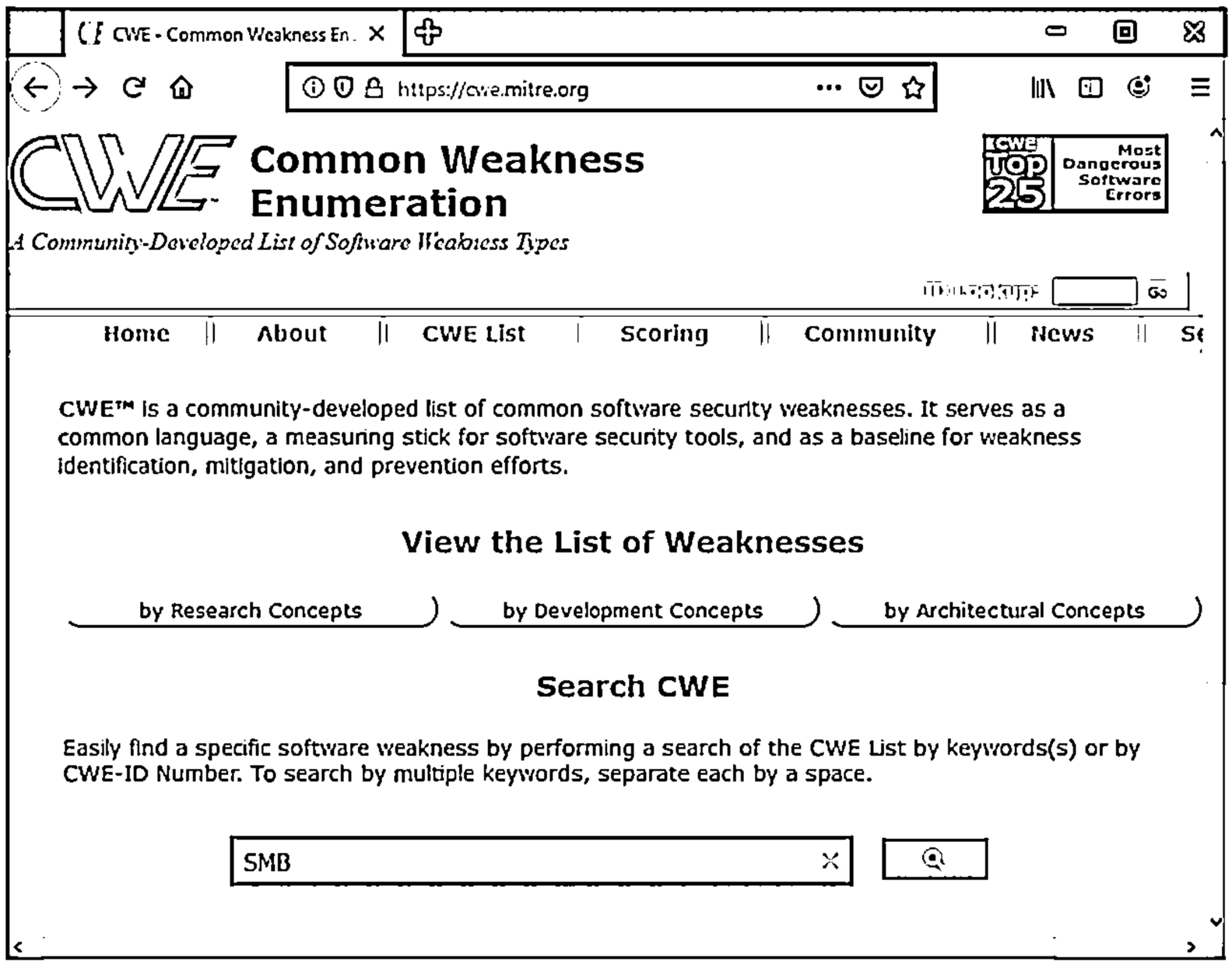


Figure 1.1.3: CWE website: searching for vulnerabilities in the service

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

4. The search results appear, displaying the underlying vulnerabilities in the target service (here, **SMB**). You can click any link to view detailed information on the vulnerability.

Note: The search results might differ in your lab environment.

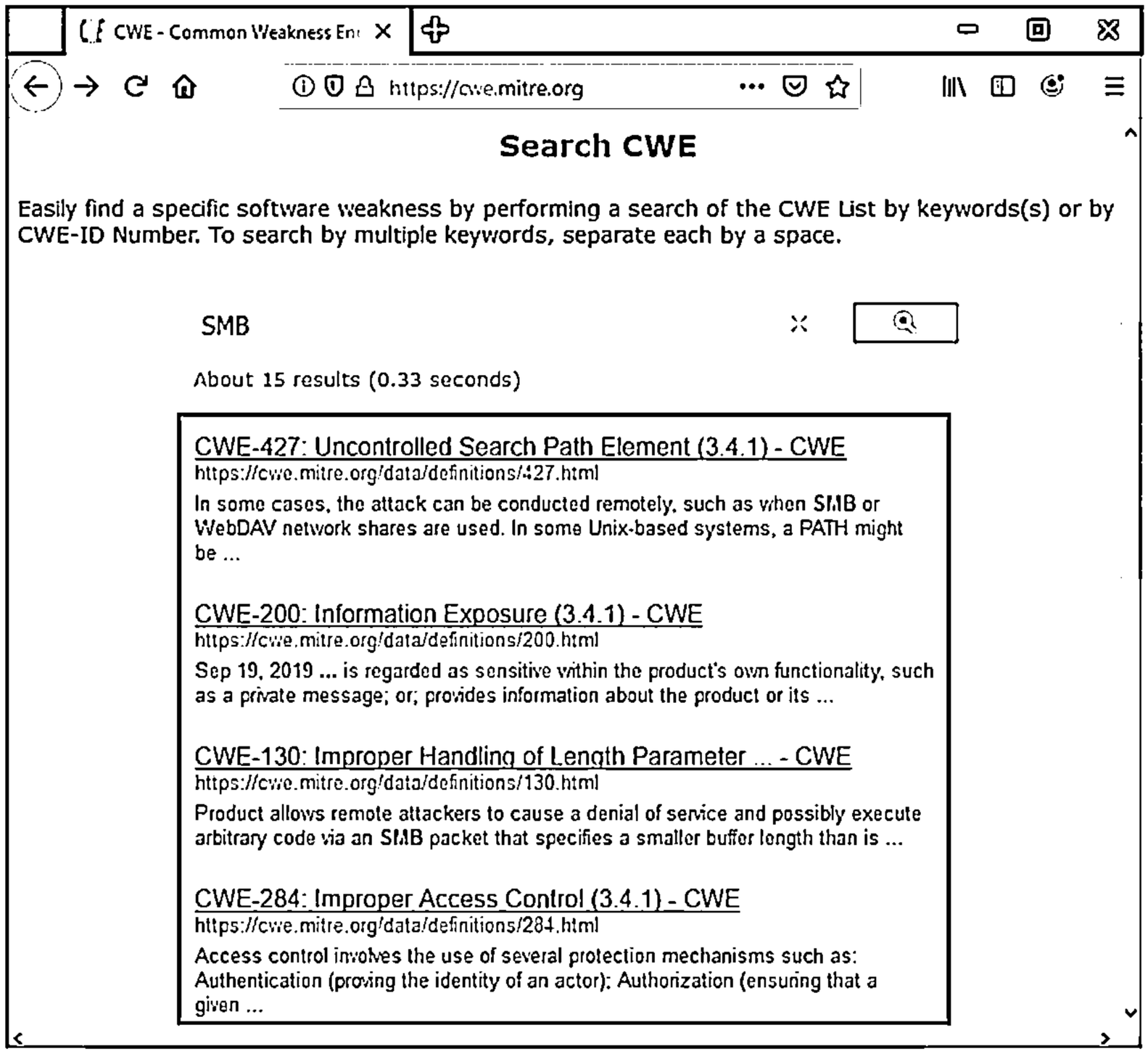


Figure 1.1.4: CWE search result

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

5. Now, click any link (here, **CWE-427**) to view detailed information about the vulnerability.
6. A new webpage appears in the new tab, displaying detailed information regarding the vulnerability. You can scroll-down further to view more information.

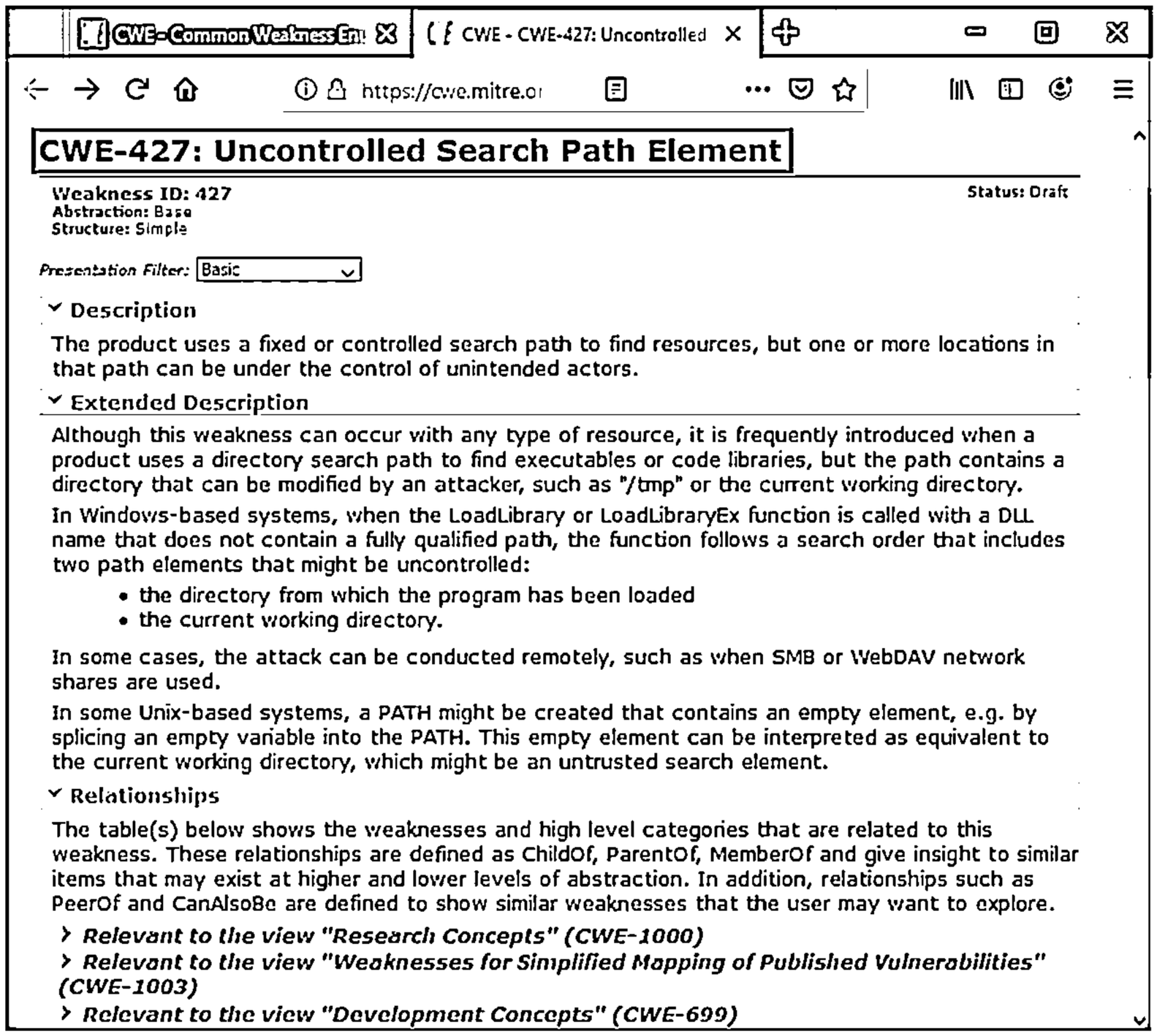


Figure 1.1.5: CWE: vulnerability information

7. Similarly, you can click on other vulnerabilities and view detailed information.

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

8. Now, navigate back to the **CWE** website, scroll down, and click the **CWE List** link present below the searched results.

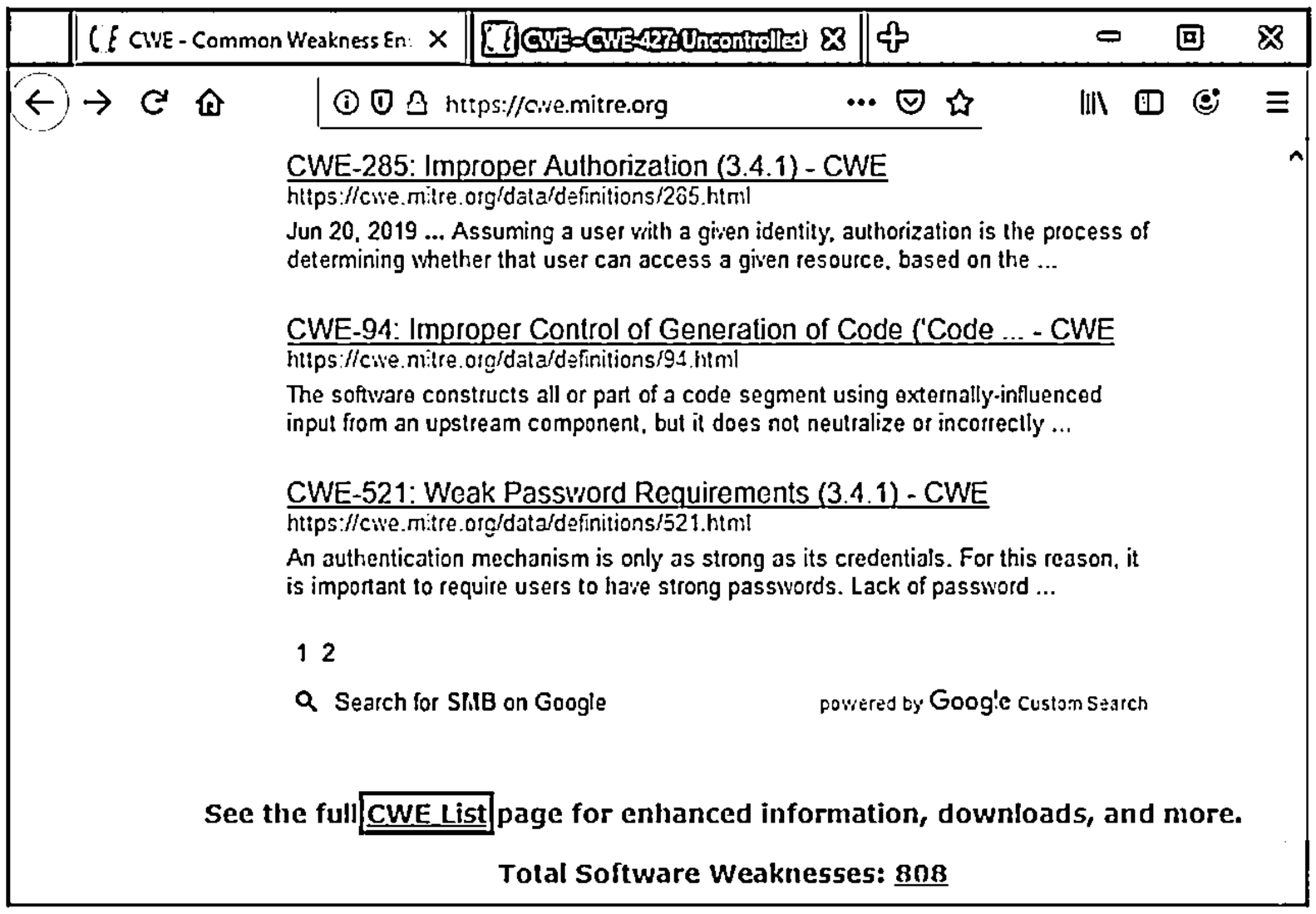


Figure 1.1.6: CWE click on CWE List

9. A new webpage appears, displaying **CWE List Version**. Scroll down, and under the **External Mappings** section, click **CWE Top 25 (2019)**.

Note: Result might differ.

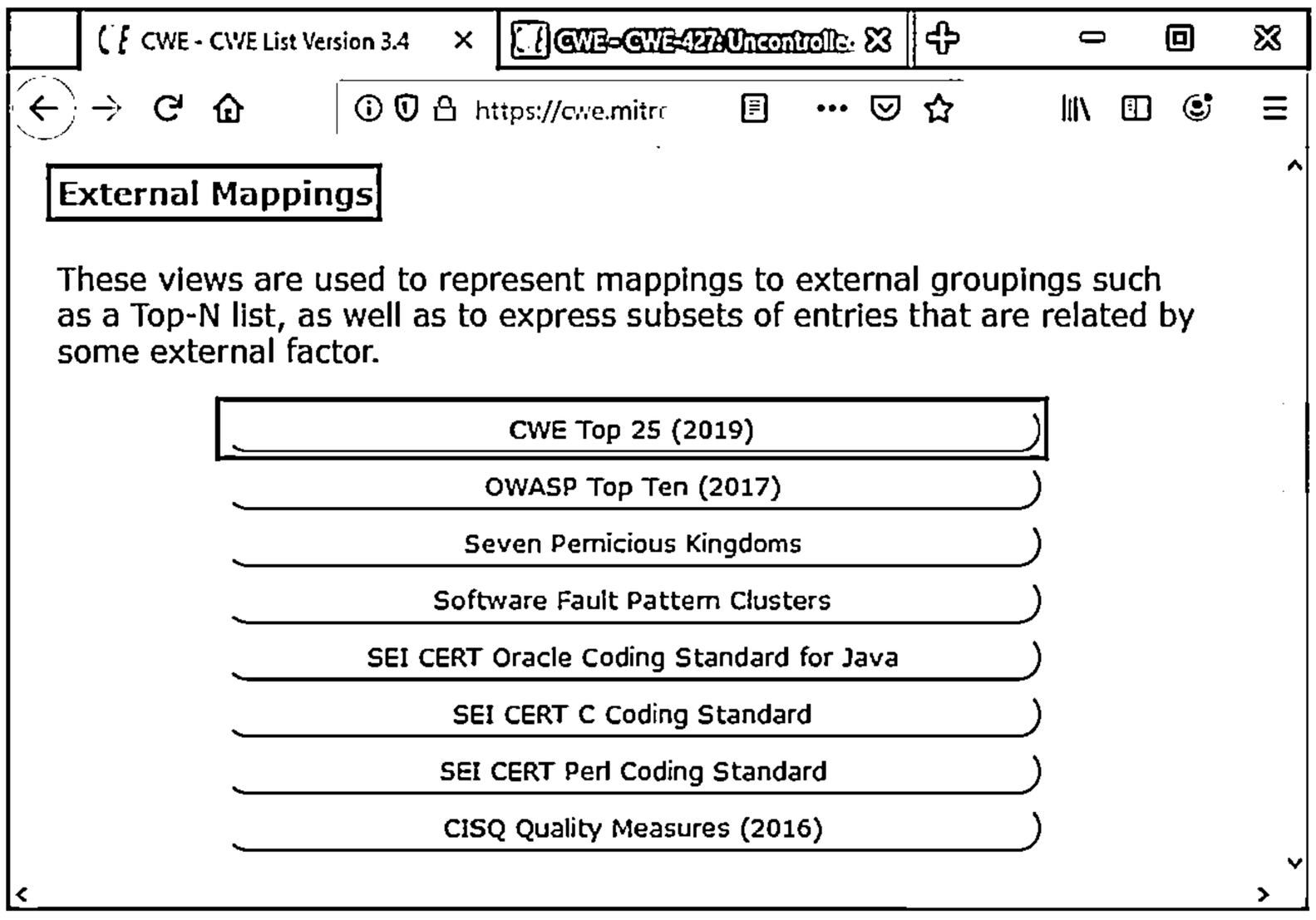


Figure 1.1.7: CWE click on CWE Top 25 (2019)

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

10. A webpage appears, displaying **CWE VIEW: Weaknesses in the 2019 CWE Top 25 Most Dangerous Software Errors**. Scroll down and view a list of **Weaknesses in the 2019 CWE Top 25 Most Dangerous Software Errors** under the **Relationships** section. You can click on each weakness to view detailed information on it.

Note: This information can be used to exploit the vulnerabilities in the software and further launch attacks.

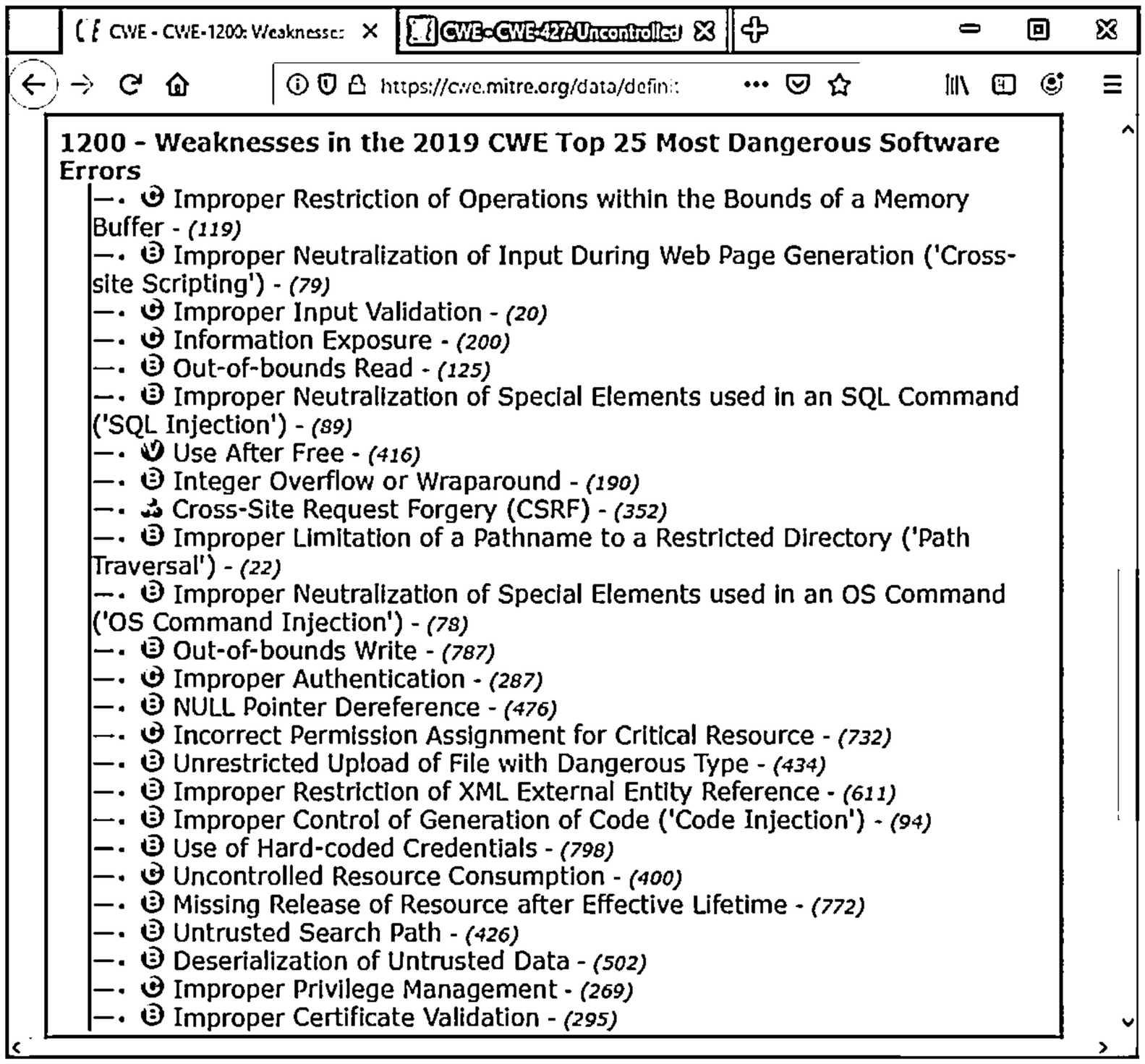


Figure 1.1.8: CWE: CWE Top 25 result

11. Similarly, you can go back to the CWE website and explore other options, as well.
12. This concludes the demonstration of checking vulnerabilities in the Common Weakness Enumeration (CWE).
13. Close all open windows and document all the acquired information.

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

TASK 2

Perform Vulnerability Research in Common Vulnerabilities and Exposures (CVE)

Here, we will use CVE to view the latest underlying system and software vulnerabilities.

Common Vulnerabilities and Exposures (CVE) is a publicly available and free-to-use list or dictionary of standardized identifiers for common software vulnerabilities and exposures. It is used to discuss or share information about a unique software or firmware vulnerability, provides a baseline for tool evaluation, and enables data exchange for cybersecurity automation.

1. In the **Windows 10** virtual machine, open any web browser (here, **Mozilla Firefox**) and navigate to **https://cve.mitre.org/**.
2. **CVE** website appears. In the right pane, under the **Newest CVE Entries** section, recently discovered vulnerabilities are displayed.

Note: The results might differ in your lab environment.

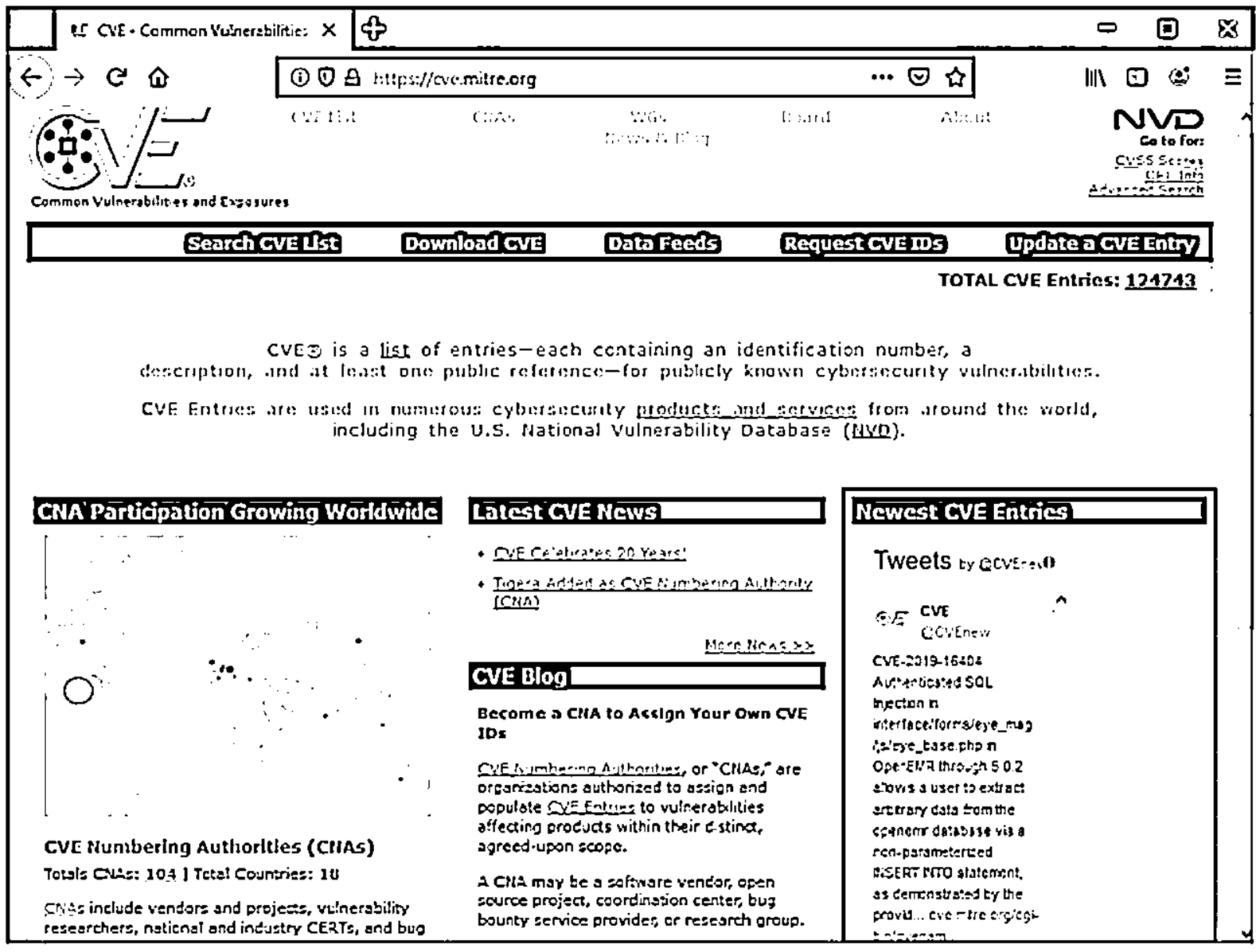


Figure 1.2.1: CVE website

3. You can copy the name of any vulnerability under the **Newest CVE Entries** section and search on CVE to view detailed information on it. (here, we are selecting the vulnerability **CVE-2019-16404**)
4. Now, click on the **Search CVE List** tab. Under **Search CVE List** section, type the vulnerability name (here, **CVE-2019-16404**) in the search bar, and click **Submit**.

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

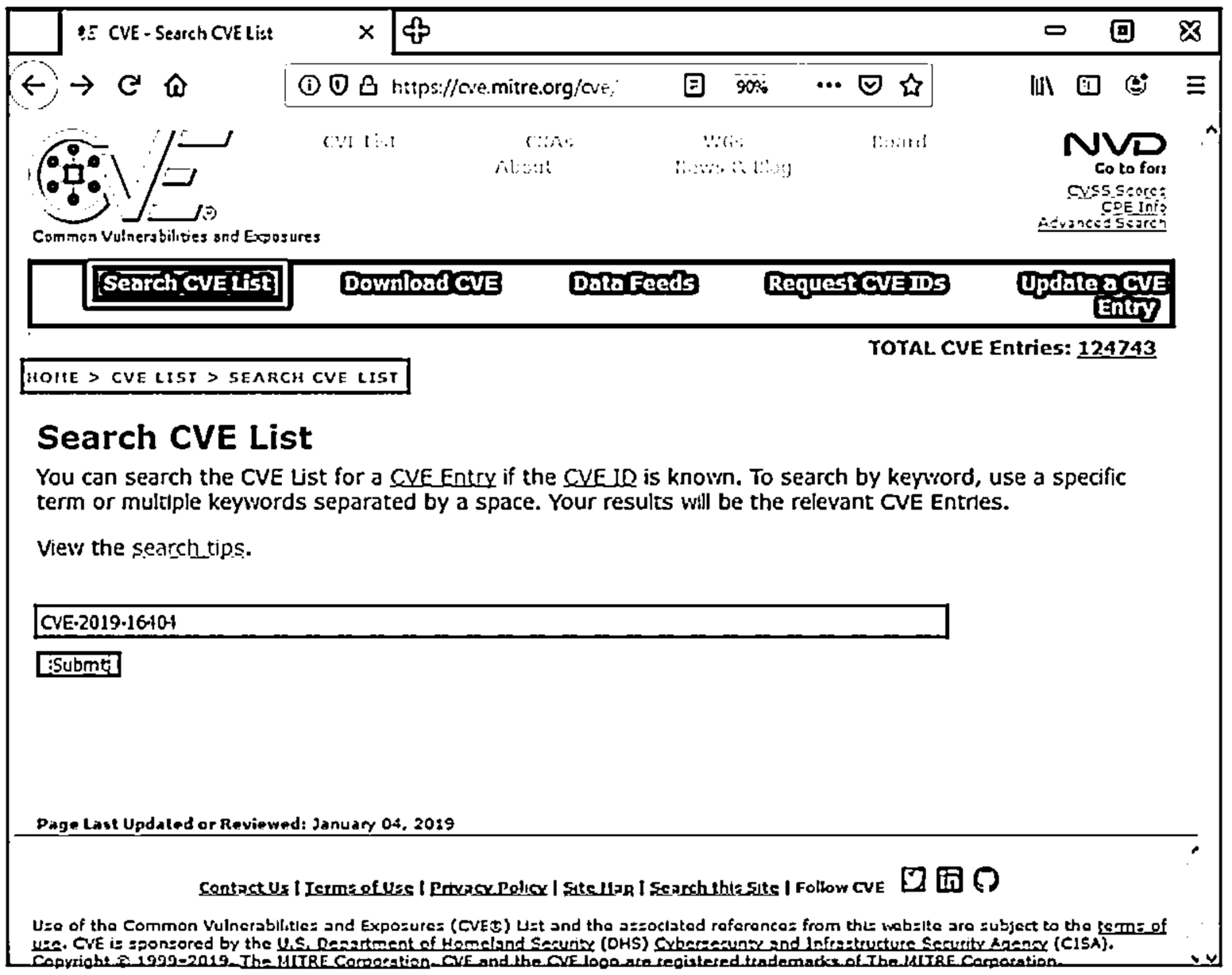


Figure 1.2.2: CVE - Search CVE List

5. **Search Results** page appears, displaying the information regarding the searched vulnerability. You can click the vulnerability link to view further detailed information regarding the vulnerability.

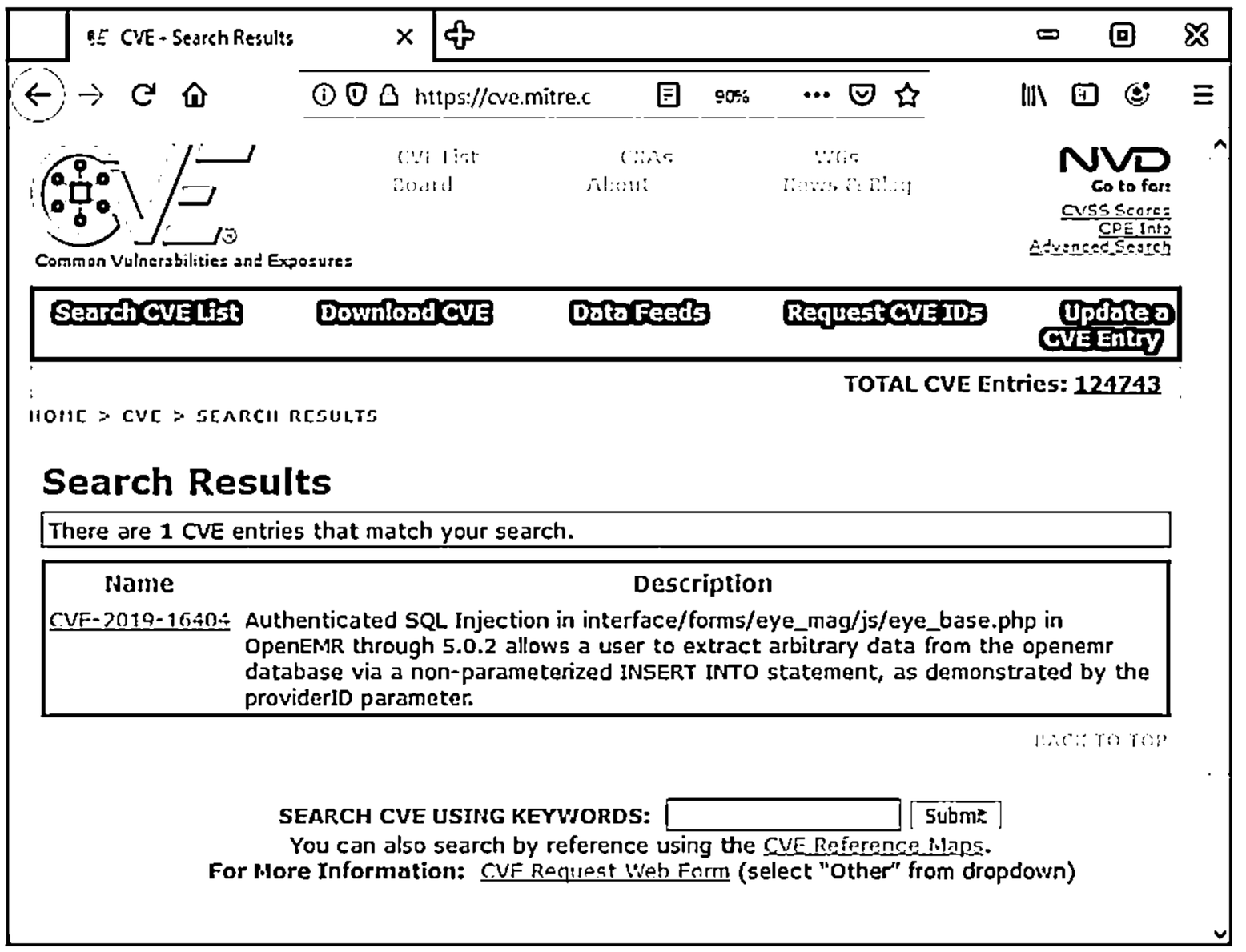


Figure 1.2.3: CVE - Search Results

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

6. Similarly, in the **Search CVE List** section, you can search for a service-related vulnerability by typing the service name (here, **SMB**) and click **Submit**.

Note: You can search for the vulnerabilities of the running services that were found in the target systems in previous module labs (Module 04 Enumeration).

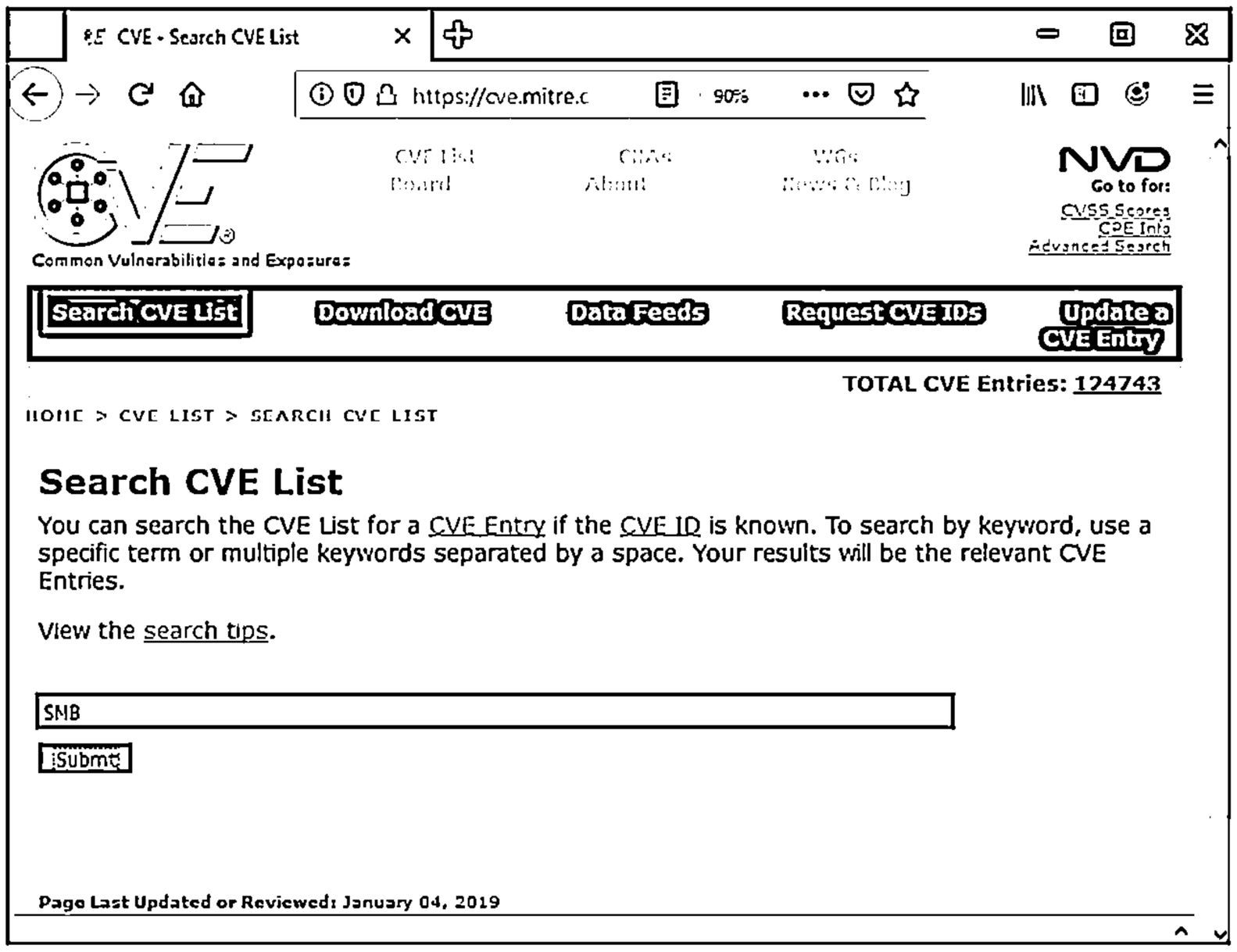


Figure 1.2.4: CVE - Search CVE List

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

7. **Search Results** page appears, displaying a list of vulnerabilities in the target service (**SMB**) along with their description, as shown in the screenshot.

Note: The results might vary in your lab environment.

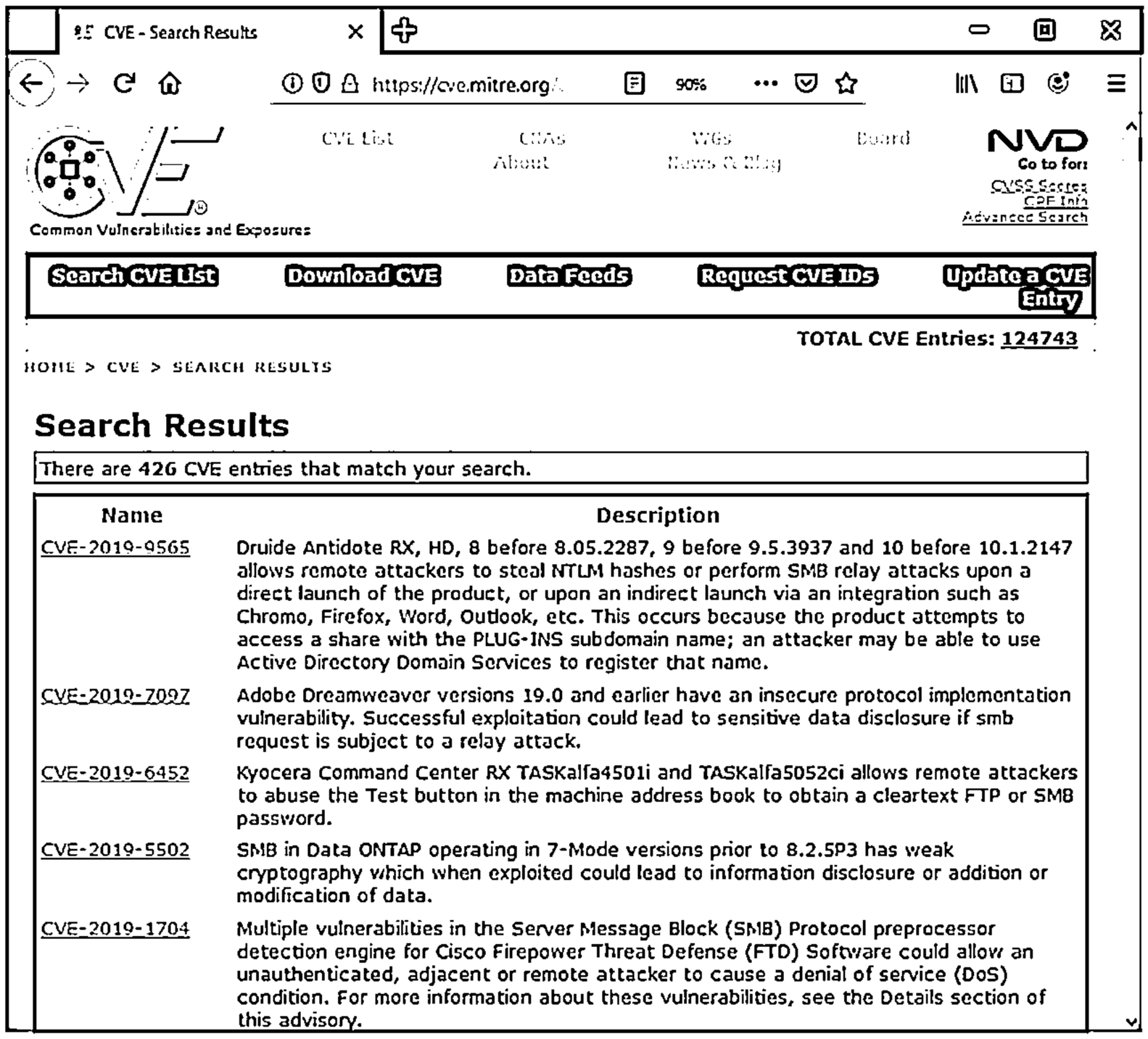


Figure 1.2.5: CVE - Search Results

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

8. Further, you can click on **CVE-ID** of any vulnerability to view its detailed information. Here, we will click on the first CVE-ID link.
9. Detailed information regarding the vulnerability is displayed such as its **Description**, **References**, and **Date Entry Created**. Further, you can click on links under the **References** section to view more information on the vulnerability.

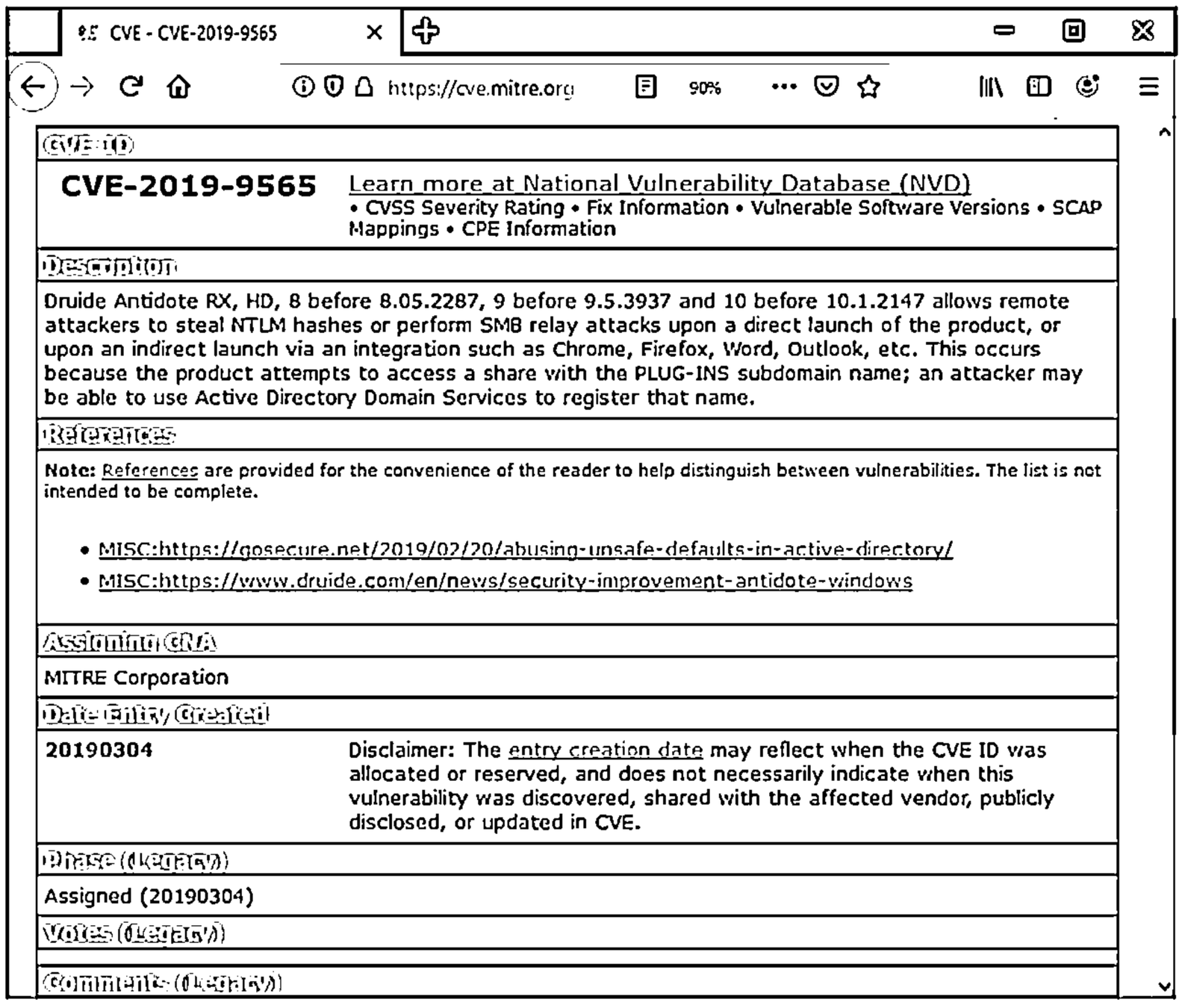


Figure 1.2.6: CVE: vulnerability information

10. Likewise, you can search for other target services for the underlying vulnerabilities in the **Search CVE List** section.
11. This concludes the demonstration of checking vulnerabilities in the Common Vulnerabilities and Exposures (CVE).
12. Close all open windows and document all the acquired information.

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

TASK 3 Perform Vulnerability Research in National Vulnerability Database (NVD)

Here, we will use the NVD to view the latest underlying system and software vulnerabilities.

1. In the **Windows 10** virtual machine, open any web browser (here, **Mozilla Firefox**) and navigate to **https://nvd.nist.gov/**.
2. **NATIONAL VULNERABILITY DATABASE** website appears: the recently discovered vulnerabilities can be viewed.
3. You can click on the CVE-ID link (here, **CVE-2019-2981**) to view detailed information about the vulnerability.

The National Vulnerability Database (NVD) is the U.S. government repository of standards-based vulnerability management data represented using the Security Content Automation Protocol (SCAP). These data enable the automation of vulnerability management, security measurement, and compliance. The NVD includes databases of security checklist references, security-related software flaws, misconfigurations, product names, and impact metrics.

Note: The results might differ in your lab environment.

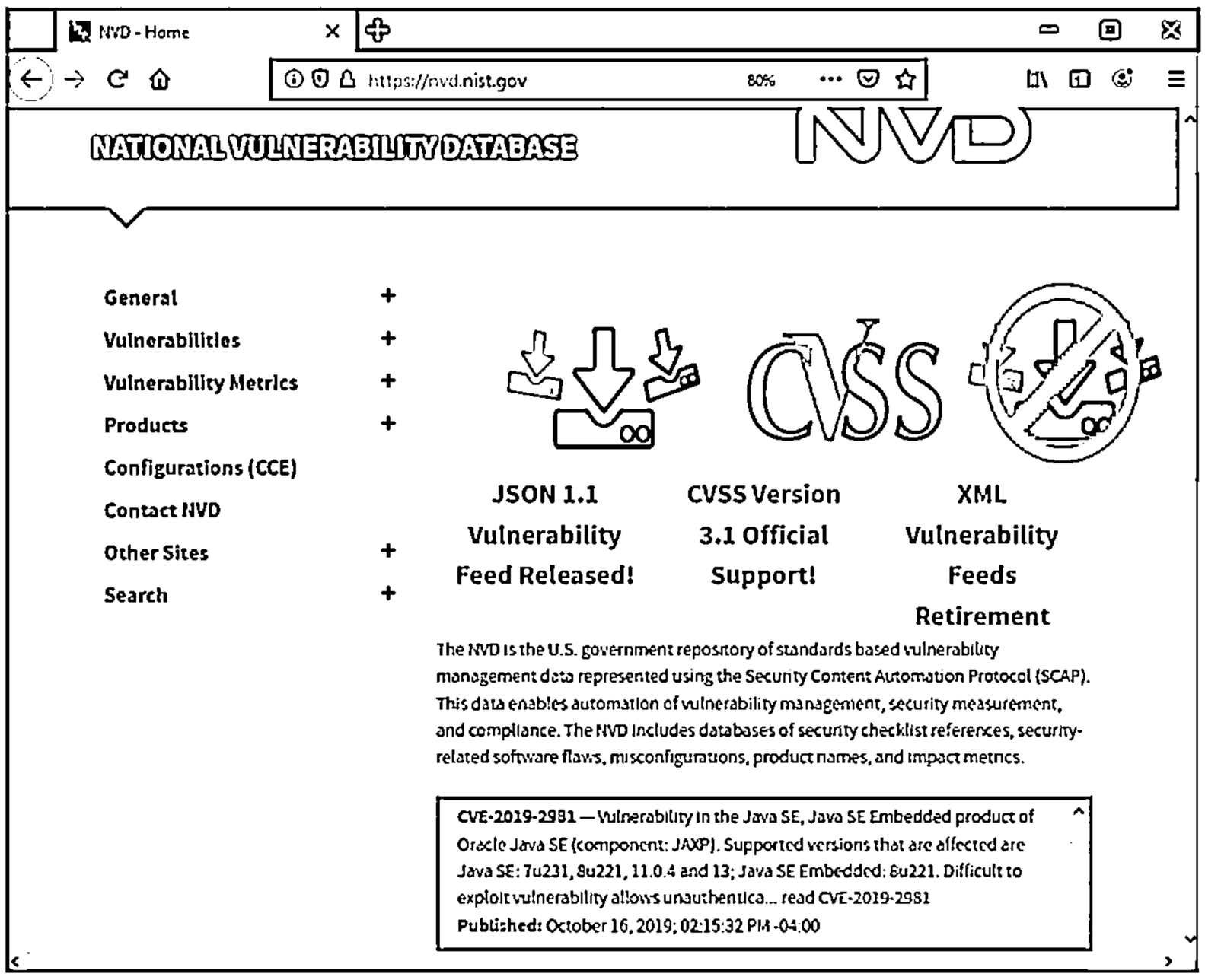


Figure 1.3.1: NVD website

4. A new webpage appears, displaying **CVE-2019-2981 Detail**. You can view detailed information such as **Current Description**, **Severity**, **References**, and **Weakness Enumeration**.

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

5. Under the **Severity** section, click the **Base Score** link to view the CVSS details regarding the vulnerability.

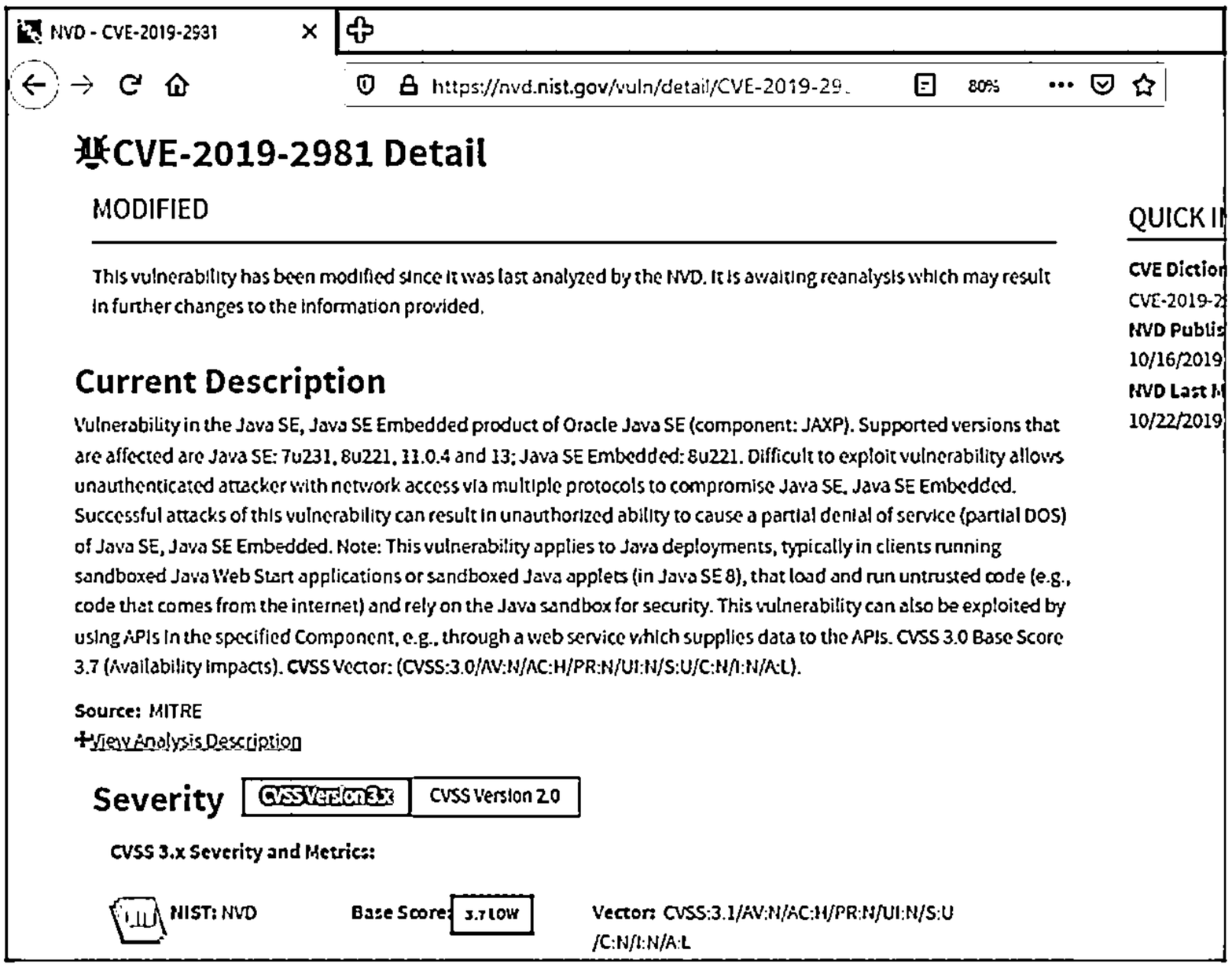


Figure 1.3.2: NVD: results

6. A new webpage appears, displaying information such as **Base Scores**, **Temporal Score**, and **Environmental Score Overall Score** related to a vulnerability in graphical form, under **Common Vulnerability Scoring System Calculator CVE-2019-2981**.

Note:

- Base Score: The metric most relied upon by enterprises and deals with the inherent qualities of a vulnerability. The table below describes the severity of a vulnerability depending upon the Base Score range:

CVSS v3.0 Ratings

Severity	Base Score Range
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

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

CVSS v2.0 Ratings

Severity	Base Score Range
Low	0.0-3.9
Medium	4.0-6.9
High	7.0-10

- **Temporal Score:** Represents the qualities of the vulnerability that change over time, and the Environmental score represents the qualities of the vulnerability that are specific to the affected user's environment.
- **Overall Score:** Sum total of both the scores (CVSS Base Score, CVSS Temporal Score).

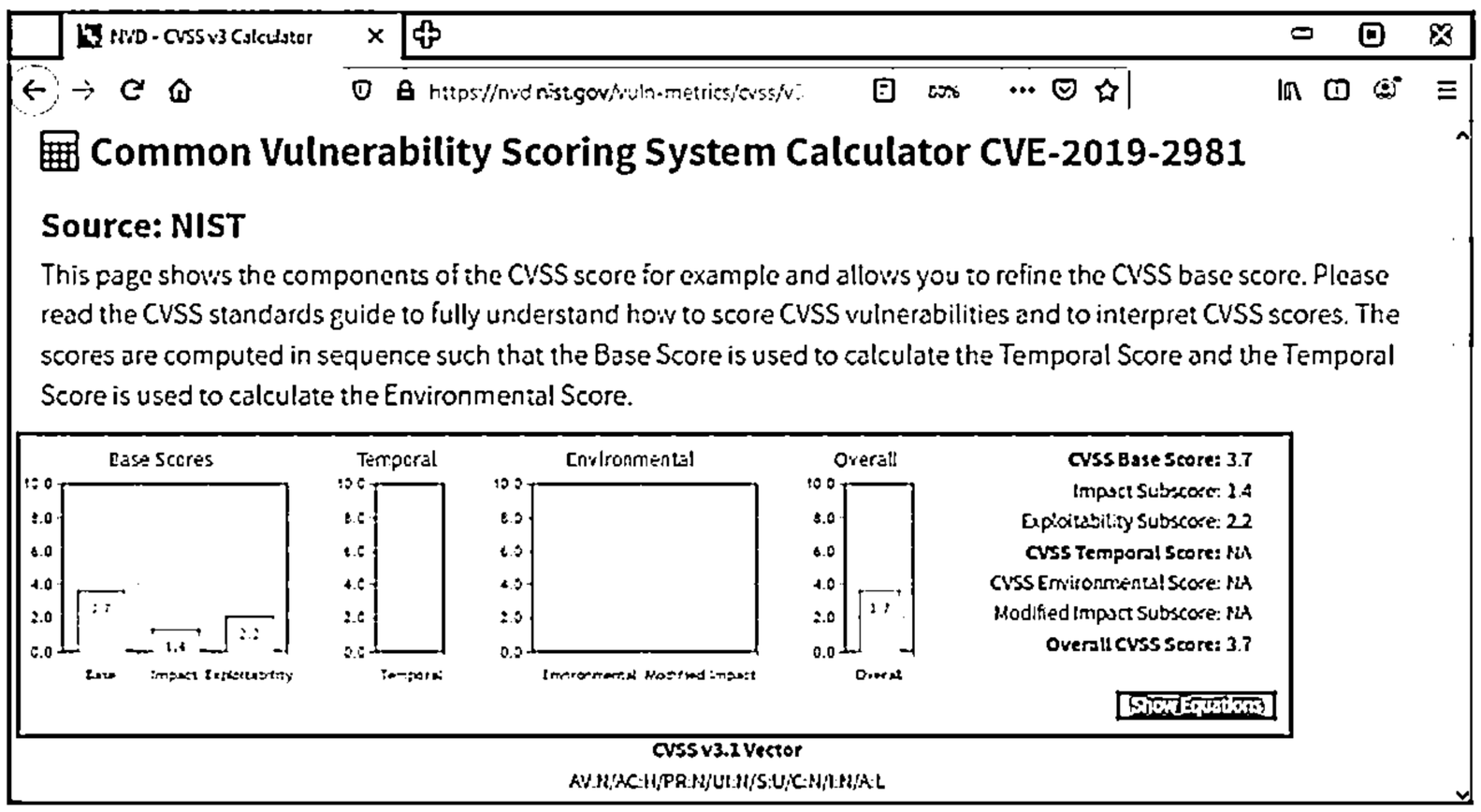


Figure 1.3.3: NVD: CVSS details

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

7. Scroll down to view more detailed information on different score metrics such as **Base Score Metrics, Temporal Score Metrics,** and **Environmental Score Metrics.**

Note: The results might differ depending upon the selected vulnerability.

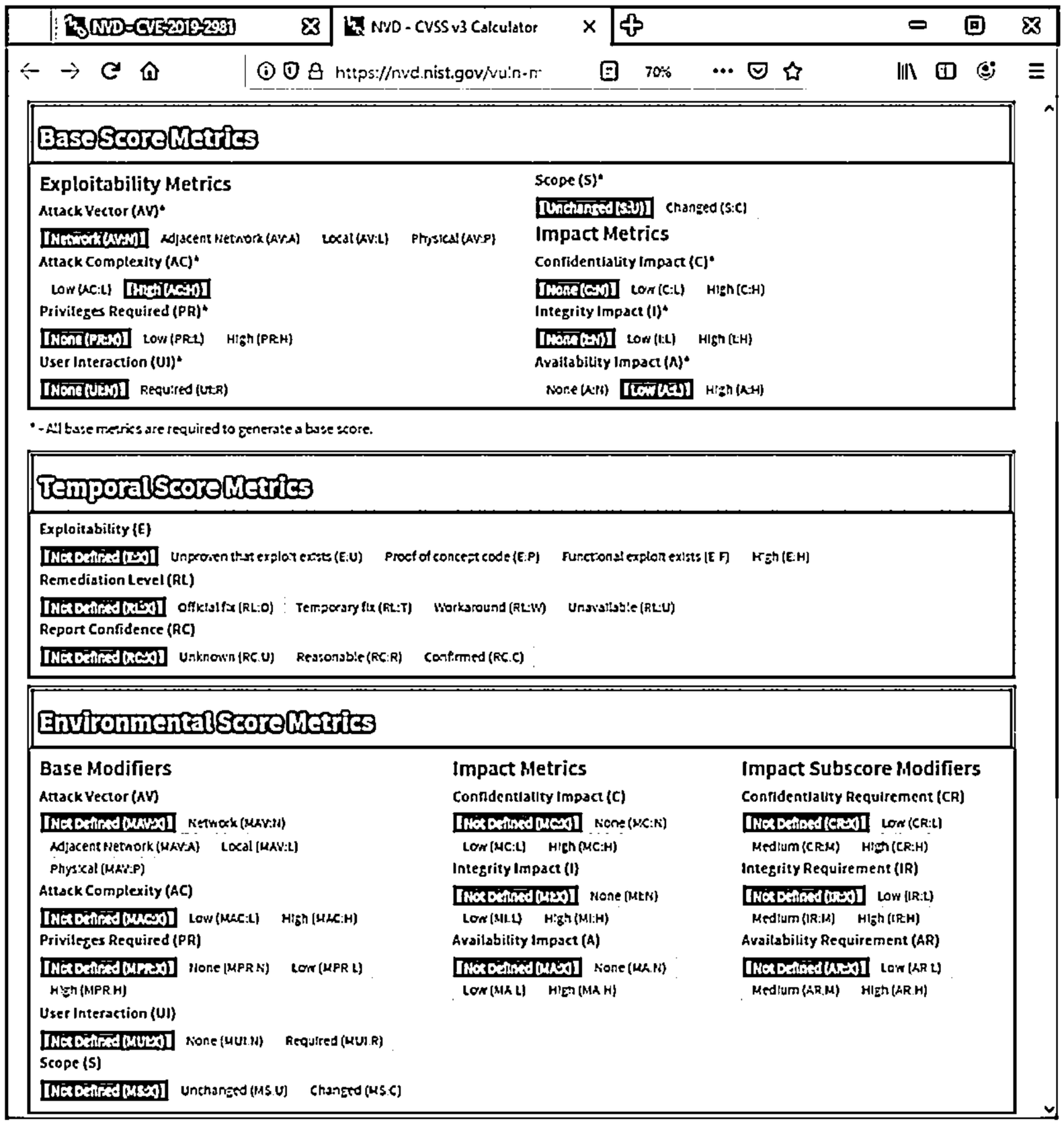


Figure 1.3.4: NVD: CVSS details

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

8. Now, navigate back to the main page of the **NATIONAL VULNERABILITY DATABASE** website. Expand **Vulnerabilities** and click **Search & Statistics** option, as shown in the screenshot.

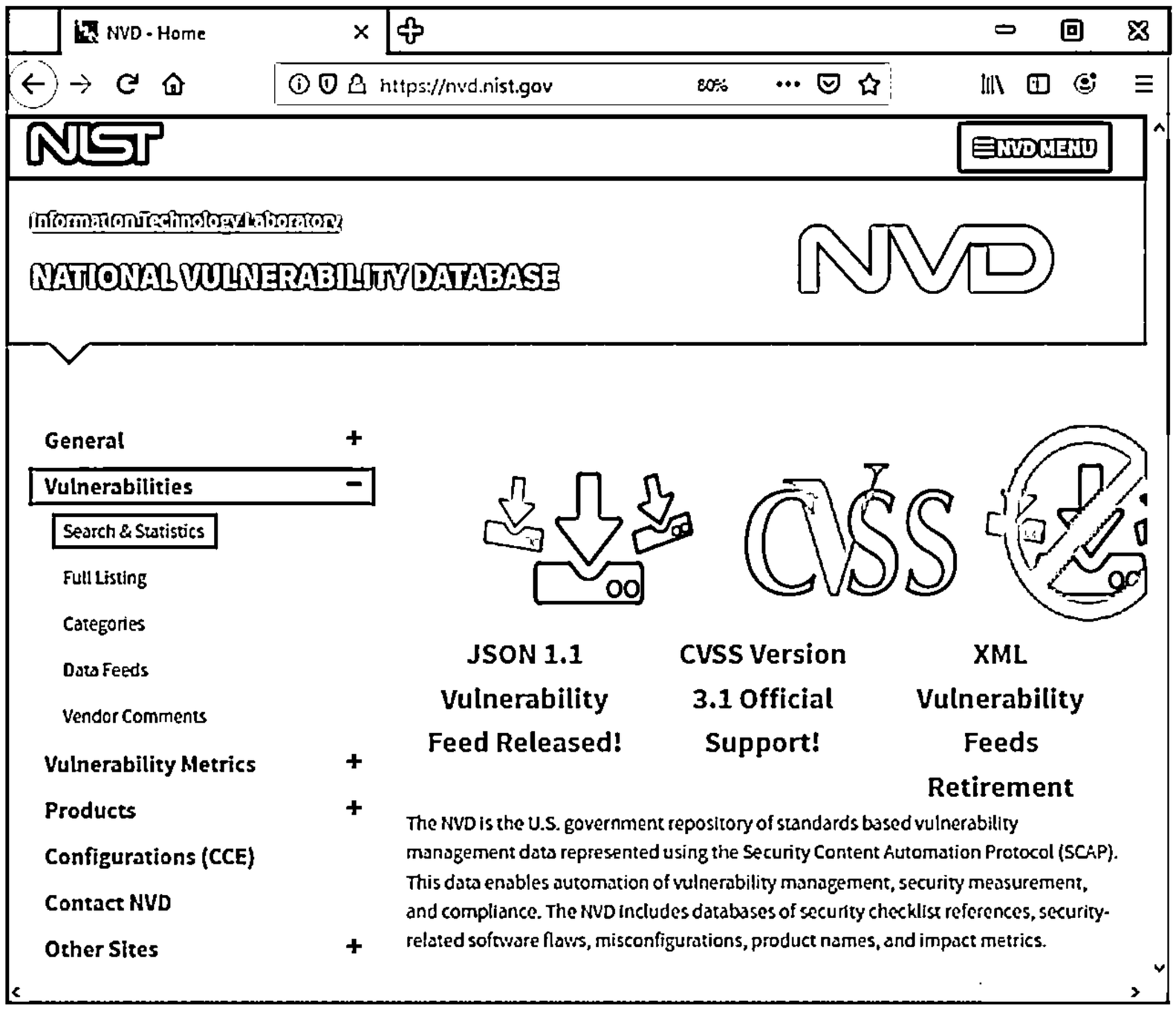


Figure 1.3.5: NVD: Select Search & Statistics option

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

9. **Search Vulnerability Database** page appears. In the **Keyword Search** field, type a target service (here, **SMB**) to find vulnerabilities associated with it and click **Search**.

Note: You can search for the vulnerabilities of the running services that were found in the target systems in previous module labs (Module 04 Enumeration).

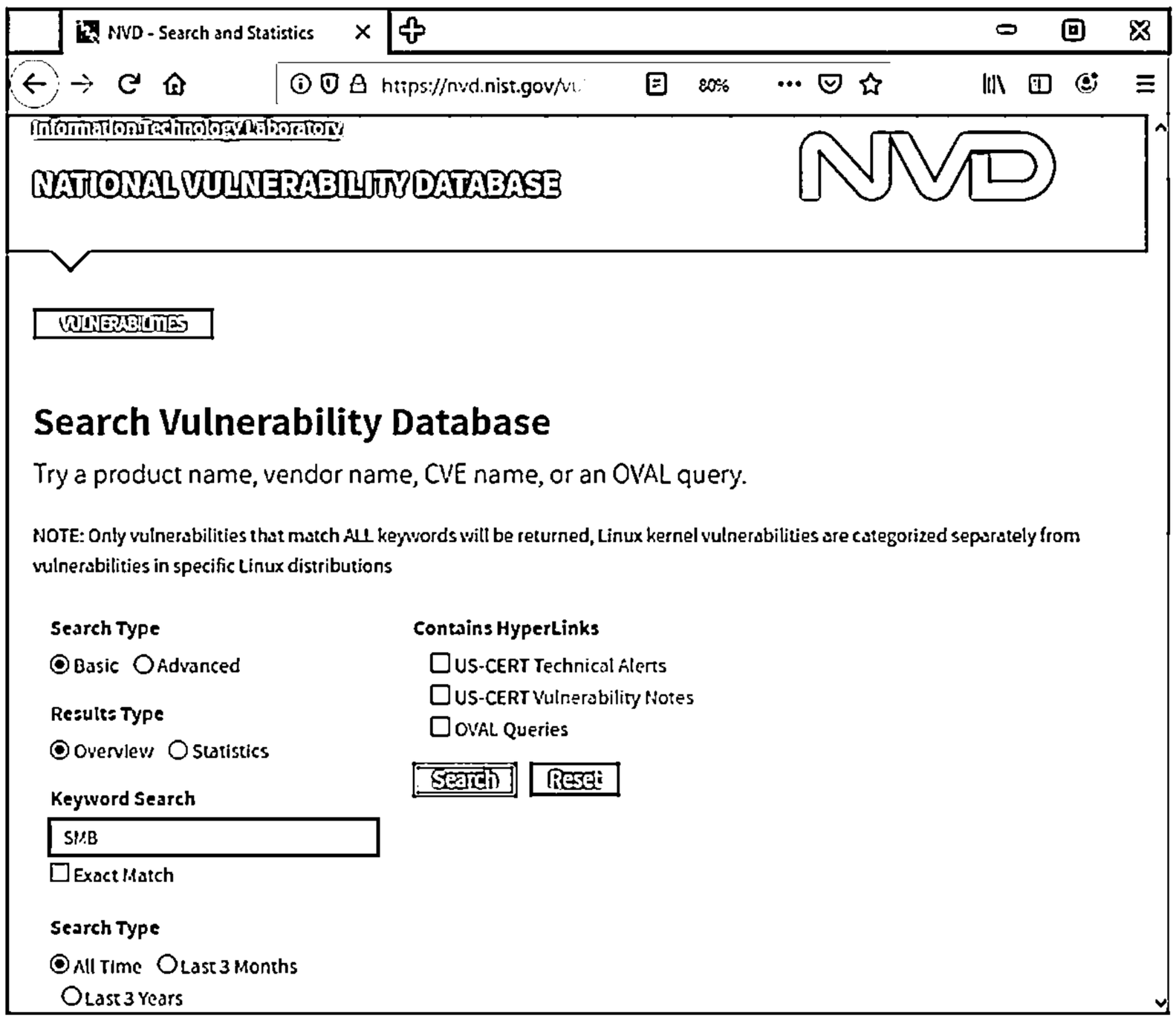


Figure 1.3.6: NVD - Search target service

10. The **Search Results** page appears, displaying detailed information on the underlying vulnerabilities in the target service.
11. You can further view detailed information on each vulnerability by clicking on the **Vuln ID** link.

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

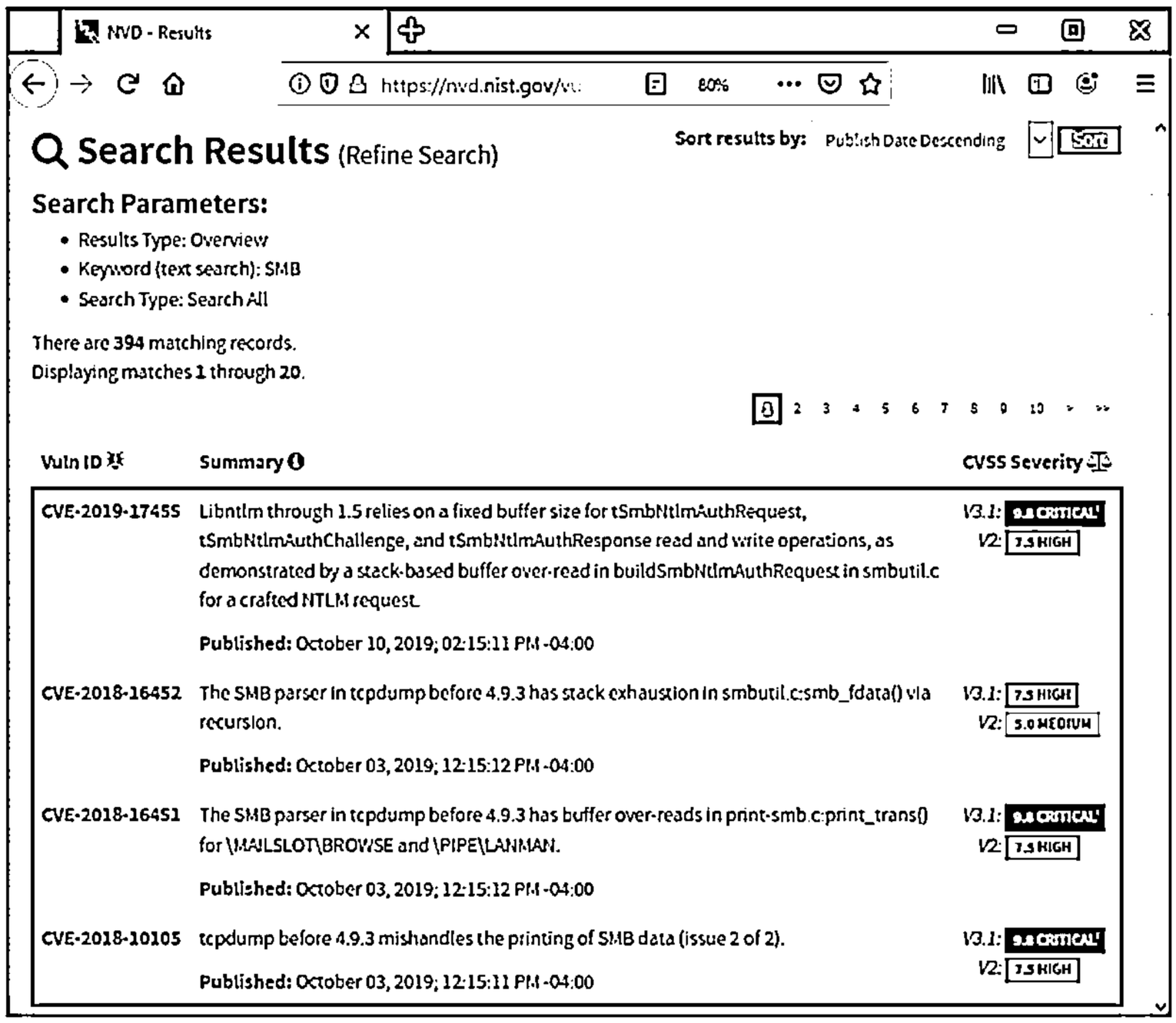


Figure 1.3.7: NVD: Search Results

12. Likewise, you can search for other target services for the underlying vulnerability in the **Search Vulnerability Database** section.
13. This concludes the demonstration of checking vulnerabilities in the National Vulnerability Database (NVD).
14. Close all open windows and document all the acquired information.
15. Turn off **Windows 10** virtual machine.

Lab Analysis

Analyze and document the results related to this lab exercise. Provide your opinion of your target's security posture and exposure.

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

Perform Vulnerability Assessment using Various Vulnerability Assessment Tools

Ethical hackers and pen testers are aided in vulnerability assessments with the help of various tools that make vulnerability assessment an easy task.

ICON KEY

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

Lab Scenario

The information gathered in the previous labs might not be sufficient to reveal potential vulnerabilities of the target: there could be more information available that may help in finding loopholes. As an ethical hacker, you should look for as much information as possible using all available tools. This lab will demonstrate other information that you can extract from the target using various vulnerability assessment tools.

Lab Objectives

- Perform vulnerability analysis using OpenVAS
- Perform vulnerability scanning using Nessus
- Perform vulnerability scanning using GFI LanGuard
- Perform web servers and applications vulnerability scanning using CGI Scanner Nikto

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 05 Vulnerability Analysis

Lab Environment

To carry out this lab, you need:

- Windows Server 2019 virtual machine
- Windows Server 2016 virtual machine
- Windows 10 virtual machine
- Parrot Security virtual machine

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

- Web browsers with an Internet connection
- Administrator privileges to run the tools
- Nessus located at **E:\CEH-Tools\CEHv11 Module 05 Vulnerability Analysis\Vulnerability Assessment Tools\Nessus**
- You can also download the latest version of **Nessus** from the official websites. If you decide to download the latest version, the screenshots shown in the lab might differ.

Lab Duration

Time: 55 Minutes

Overview of Vulnerability Assessment Tools

Vulnerability assessment tools are used to secure and protect the organization's system or network: security analysts can use these tools to identify weaknesses present in the organization's security posture and remediate the identified vulnerabilities before an attacker exploits them. Network vulnerability scanners analyze and identify vulnerabilities in the target network or network resources using vulnerability assessment and network auditing. These tools also assist in overcoming weaknesses in the network by suggesting various remediation techniques.

Lab Tasks

TASK 1 Perform Vulnerability Analysis using OpenVAS

Here, we will perform a vulnerability analysis using OpenVAS.

OpenVAS is a framework of several services and tools offering a comprehensive and powerful vulnerability scanning and vulnerability management solution. Its capabilities include unauthenticated testing, authenticated testing, various high level and low-level Internet and industrial protocols, performance tuning for large-scale scans, and a powerful internal programming language to implement any vulnerability test.

Note: In this task, we will use the **Parrot Security** (**10.10.10.13**) virtual machine as a host machine and the **Windows Server 2016** (**10.10.10.16**) virtual machine as a target machine.

1. Turn on the **Parrot Security** and **Windows Server 2016** virtual machines.
2. Switch to the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

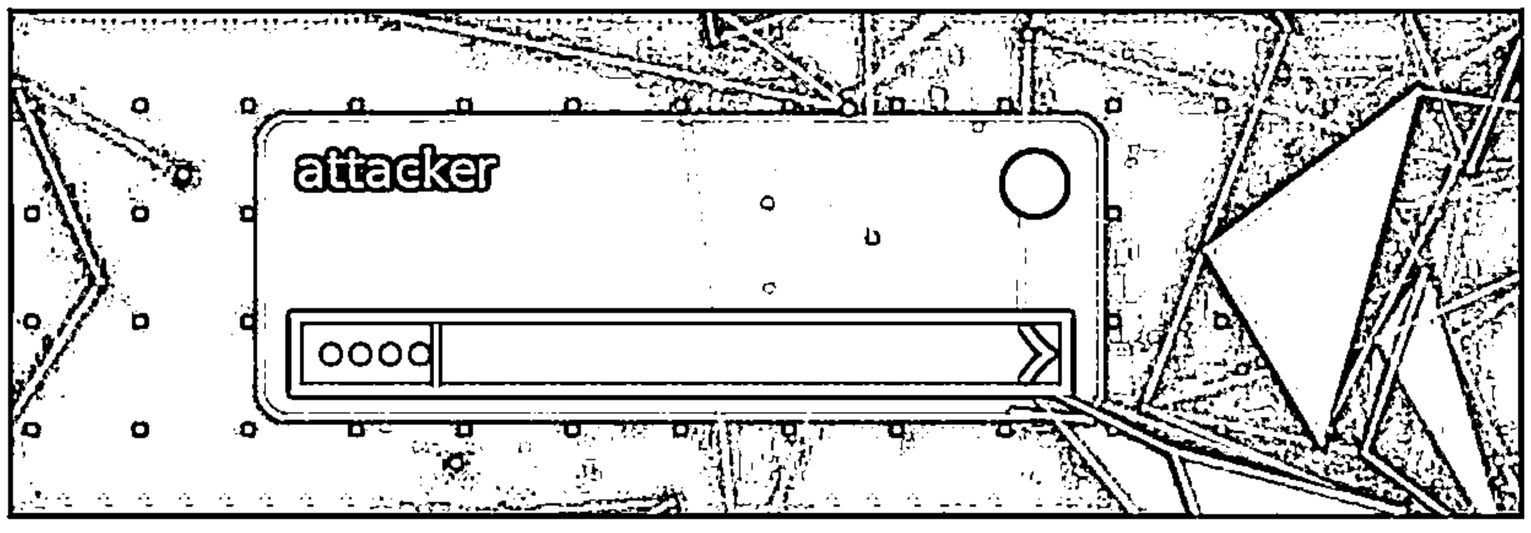


Figure 2.1.1: Parrot Security login page

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

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

TASK 1.1

Launch OpenVAS Tool

3. Click **Applications** at the top of the **Desktop** window and navigate to **Pentesting → Vulnerability Analysis → OpenVAS - Greenbone→ Start** to launch OpenVAS tool.
4. A terminal window appears, in the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**. OpenVAS initializes.
5. After the tool initializes, click **Firefox** icon from the top-section of the **Desktop**.
6. The **Firefox** browser appears, in the address bar, type **https://127.0.0.1:9392** and press **Enter**.
7. OpenVAS login page appears, log in with **Username** and **Password** as **admin** and **password** and click the **Login** button.

The actual security scanner is accompanied with a regularly updated feed of Network Vulnerability Tests (NVTs)—over 50,000 in total.

Note: The version of OpenVAS might differ in your lab environment.

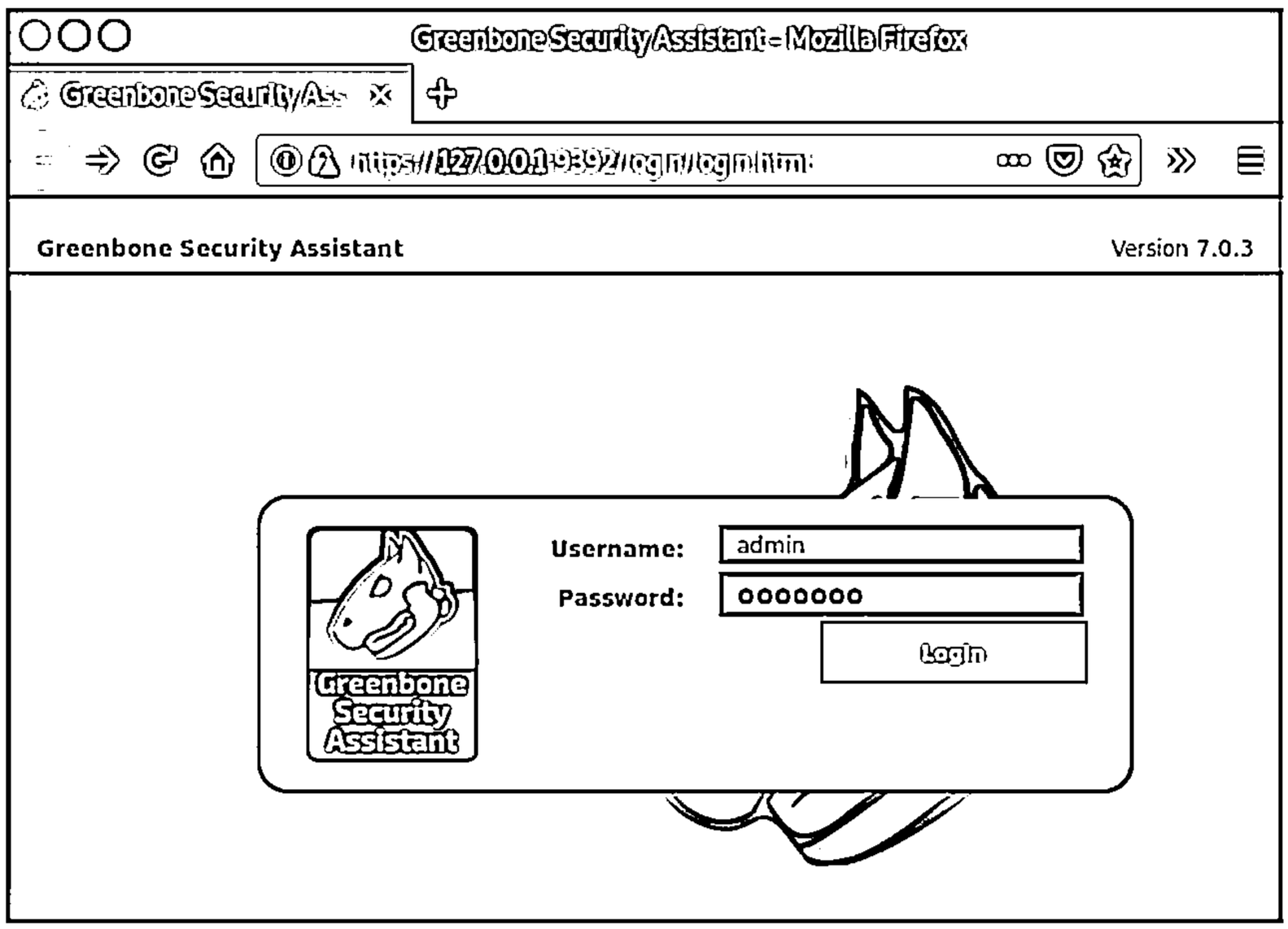


Figure 2.1.2: OpenVAS Login page

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

8. **OpenVAS Dashboard** appears, as shown in the screenshot.

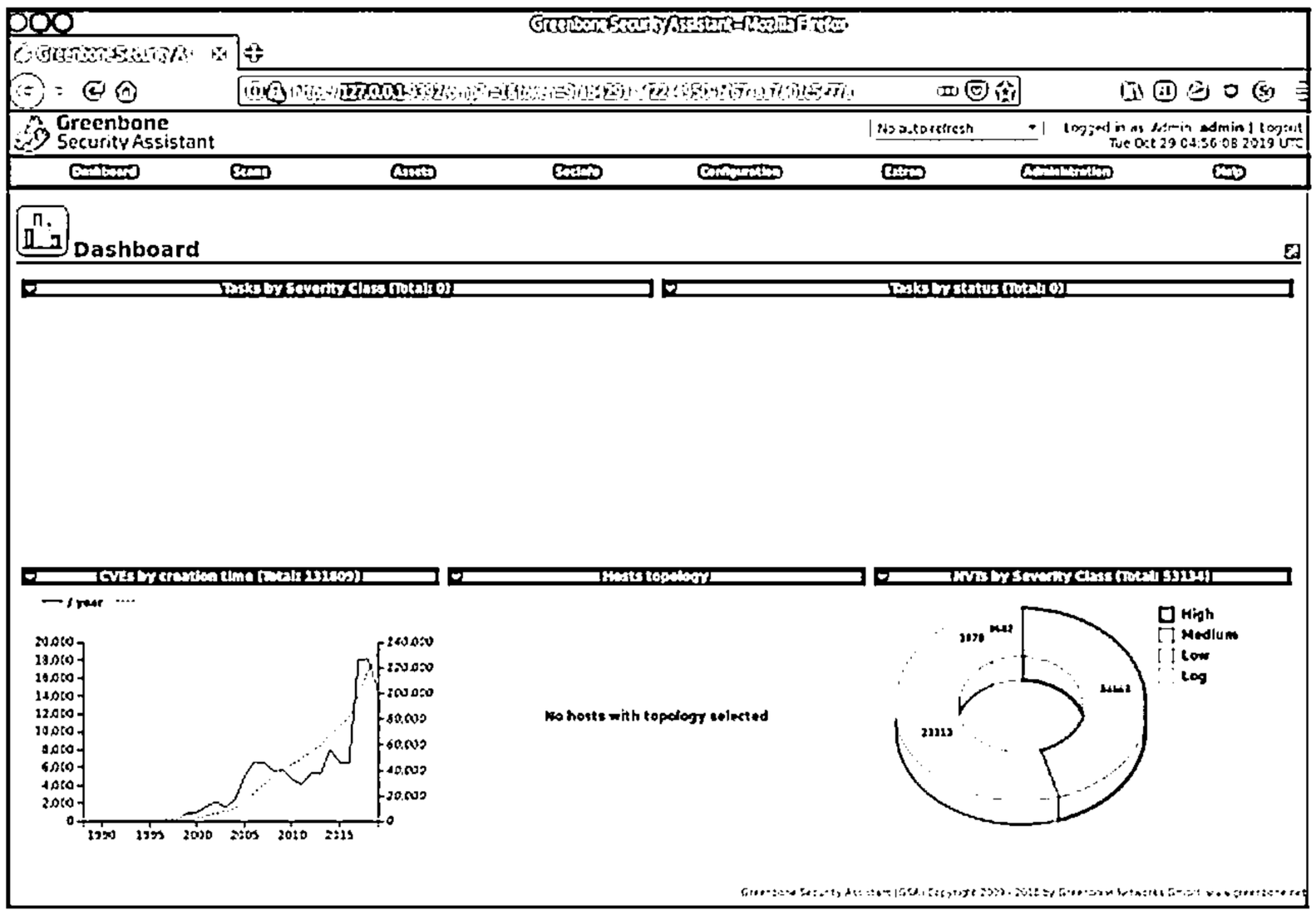


Figure 2.1.3: OpenVAS dashboard

9. Navigate to **Scans → Tasks** from the **Menu** bar.

Note: If a **Welcome to the scan management!** pop-up appears, close it.

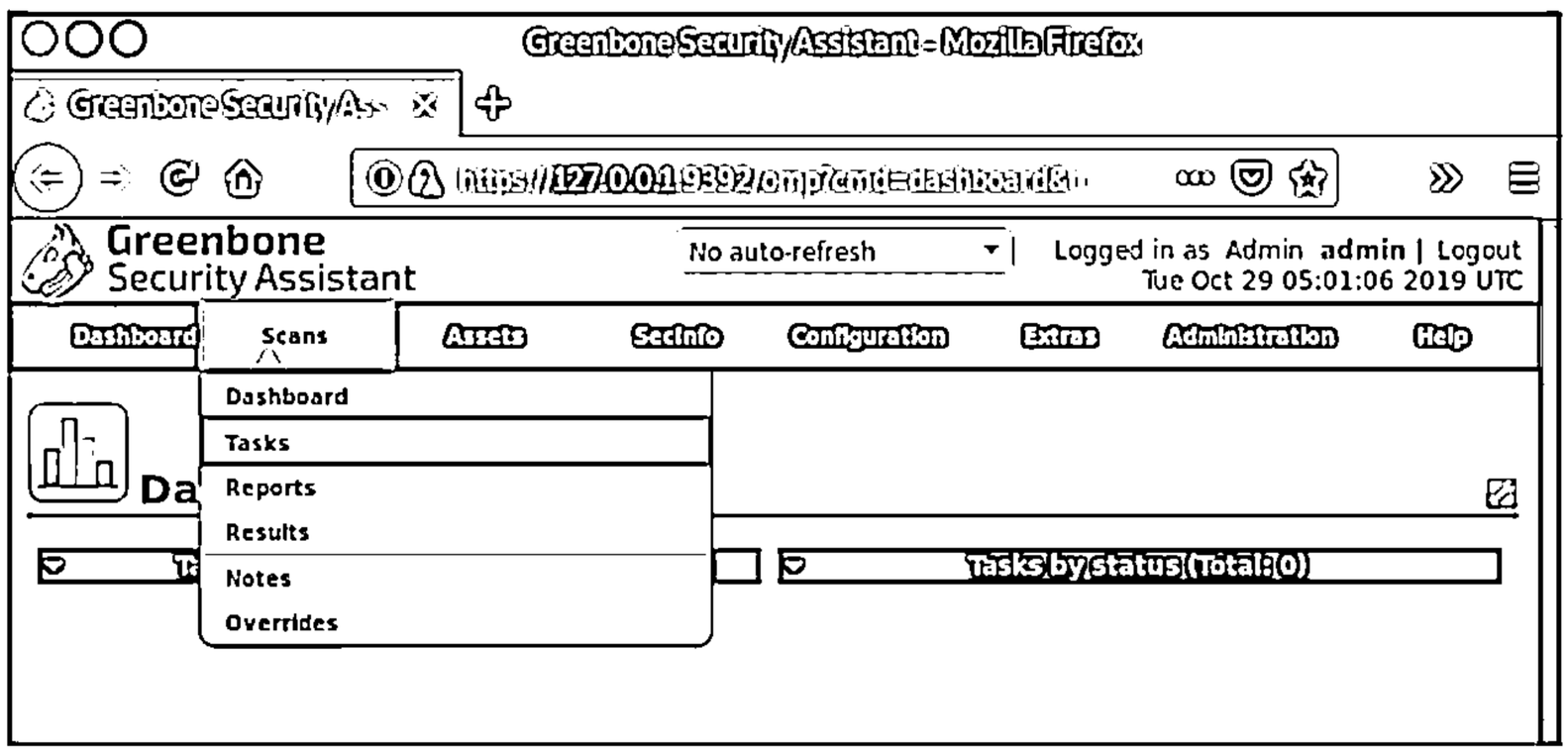


Figure 2.1.4: OpenVAS: select Scans option

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

TASK 1.2

Scan the Target

10. Hover over ( ) icon and click the **Task Wizard** option.

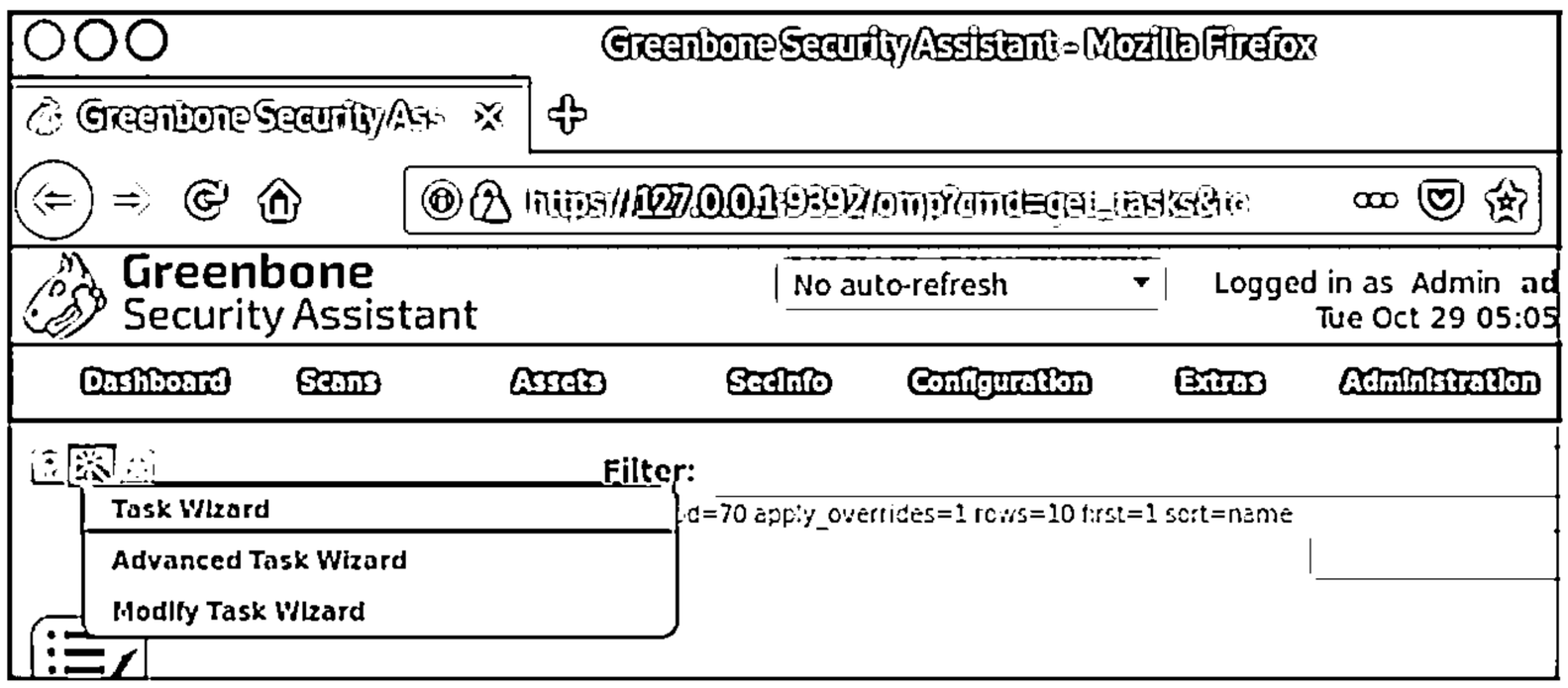


Figure 2.1.5: OpenVAS: select Task Wizard option

11. The **Task Wizard** window appears; enter the target IP address in the **IP address or hostname** field (here, the target system is **Windows Server 2016** [**10.10.10.16**]) and click the **Start Scan** button.

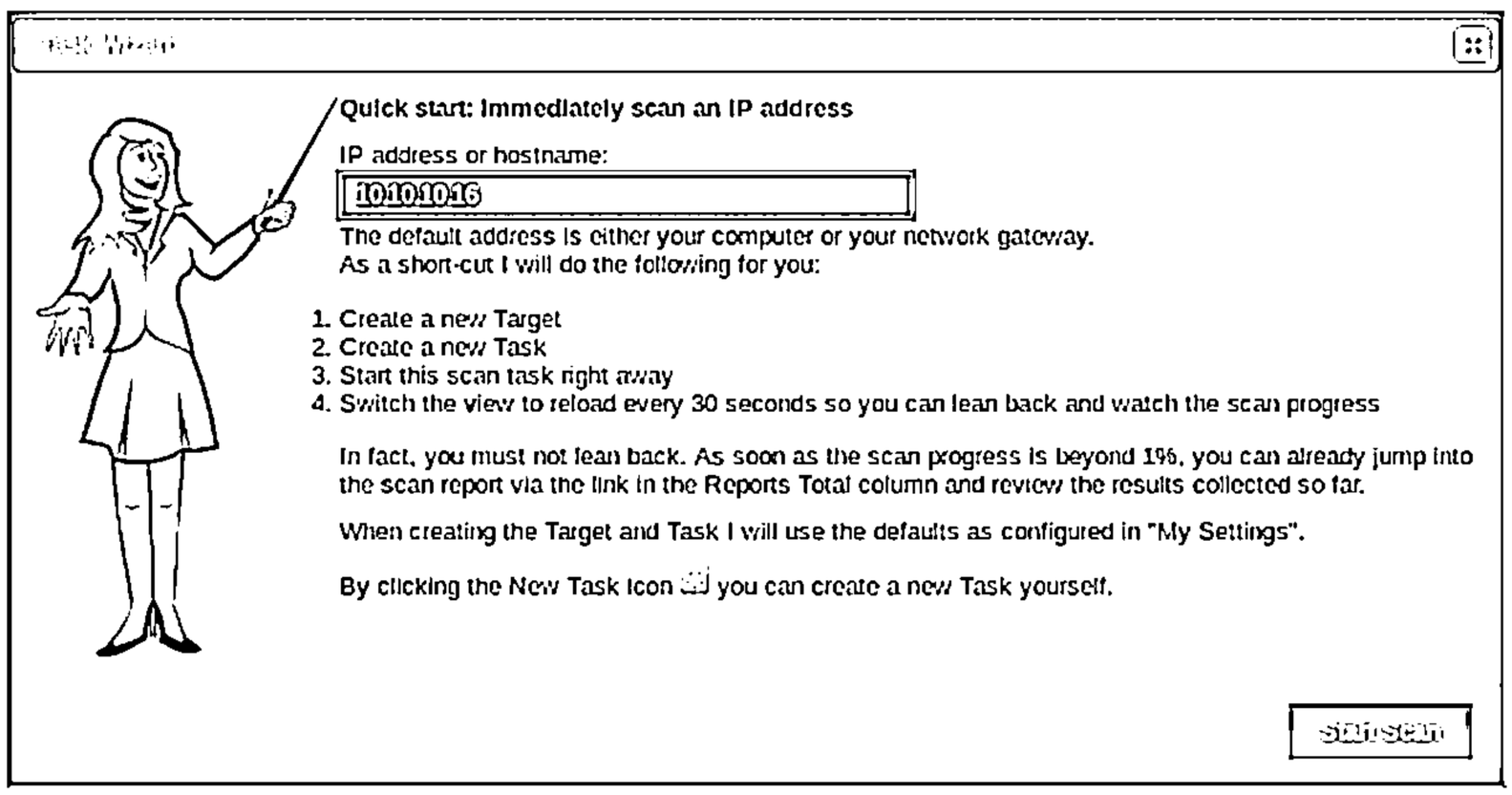


Figure 2.1.6: OpenVAS: enter the target IP address

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

12. The task appears under the **Tasks** section; OpenVAS starts scanning the target IP address.

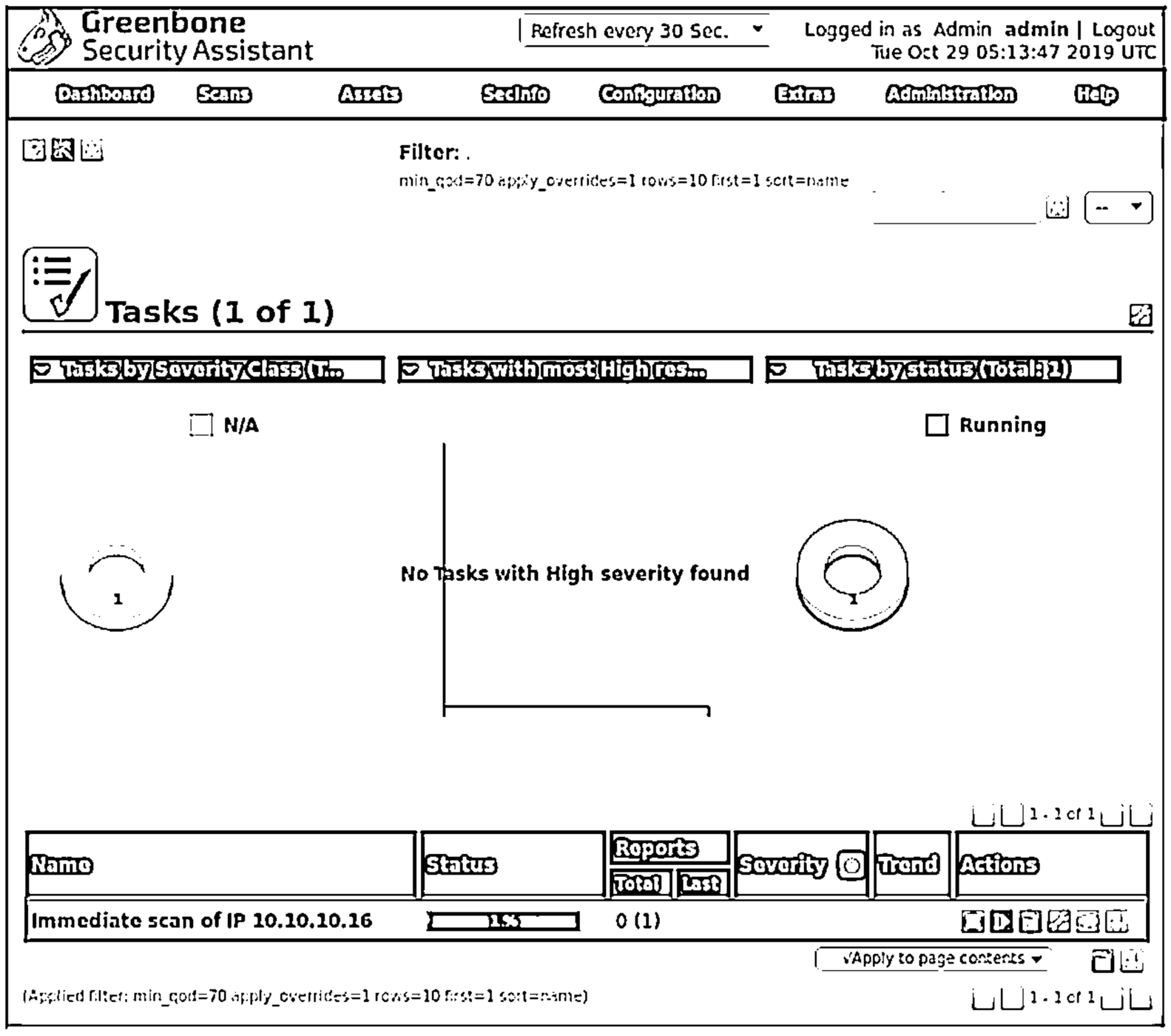


Figure 2.1.7: OpenVAS: Scan initiates

13. Wait for the **Status** to change from **Requested** to **Done**. Once it is completed, click the **Done** button under the **Status** column to view the vulnerabilities found in the target system.

Note: The scan will take approximately 10 minutes to complete.

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

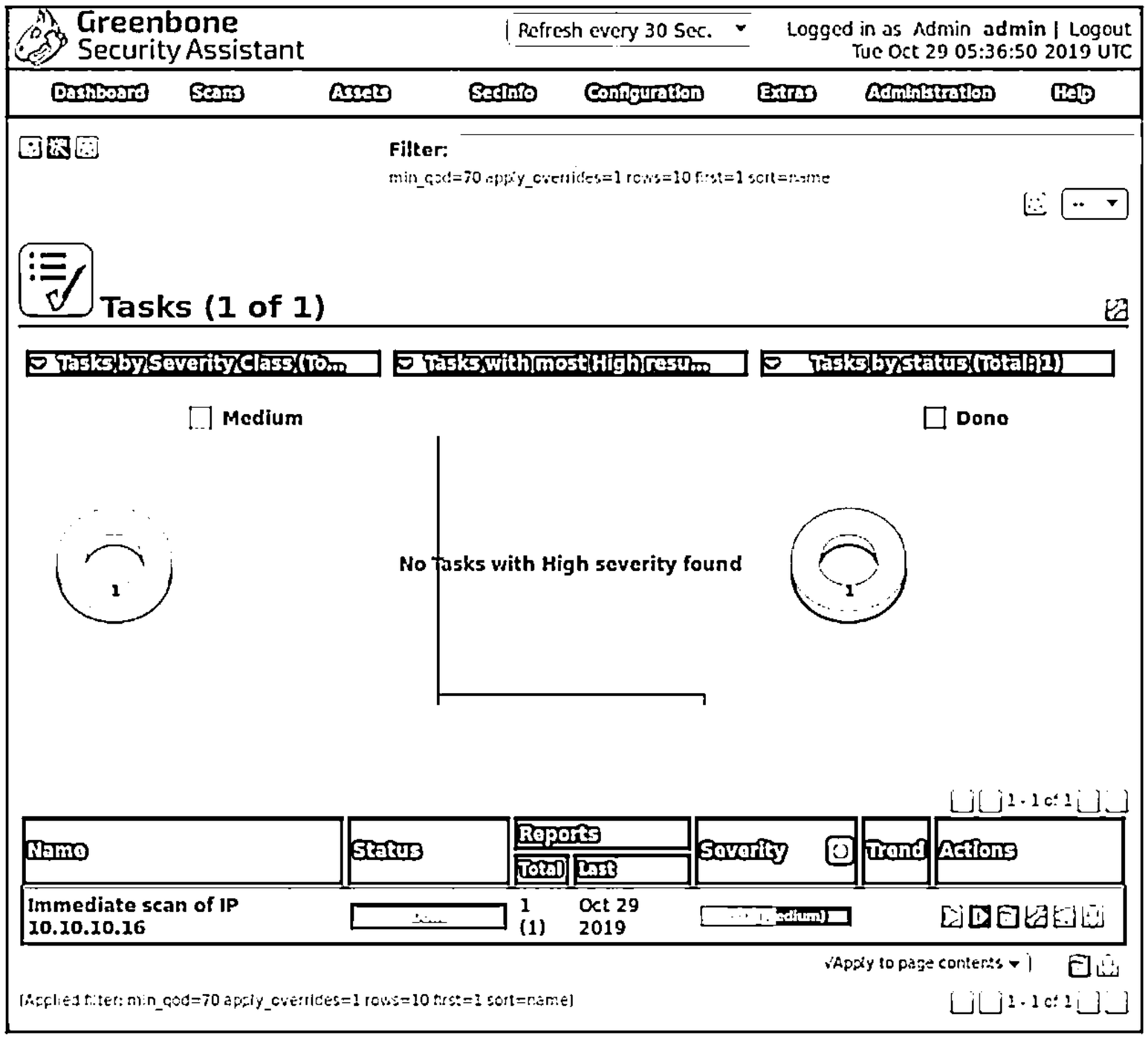


Figure 2.1.8: OpenVAS: Scan Completes

14. **Report: Results** appears, displaying the discovered vulnerabilities along with their severity and port numbers on which they are running.

Note: The results might vary in your lab environment.

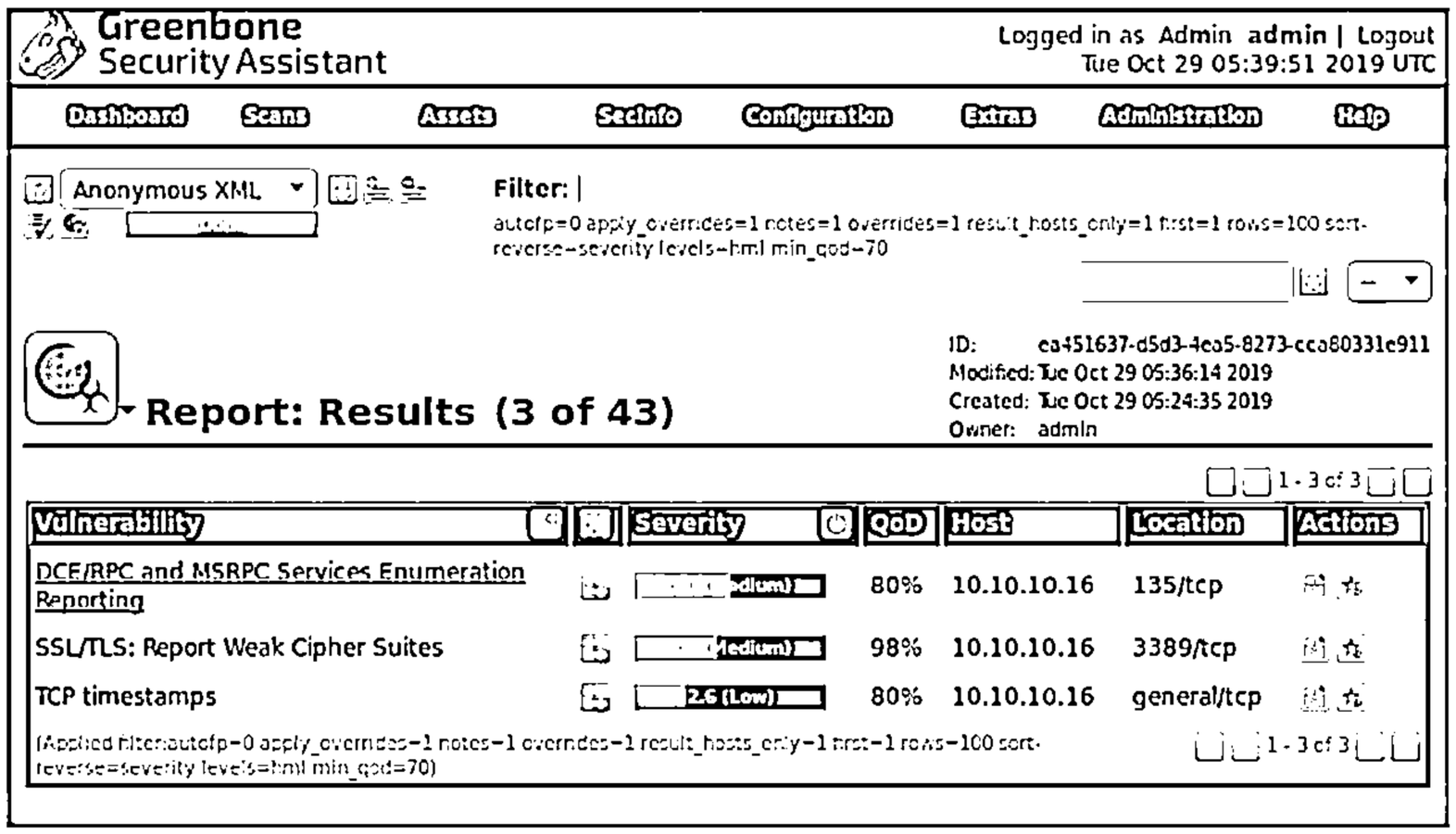


Figure 2.1.9: OpenVAS: Report: Results

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

15. Click on any vulnerability under the **Vulnerability** column (here, **DCE/RPC and MSRPC Services Enumeration Reporting**) to view its detailed information.
16. Detailed information regarding selected vulnerability appears, as shown in the screenshot.

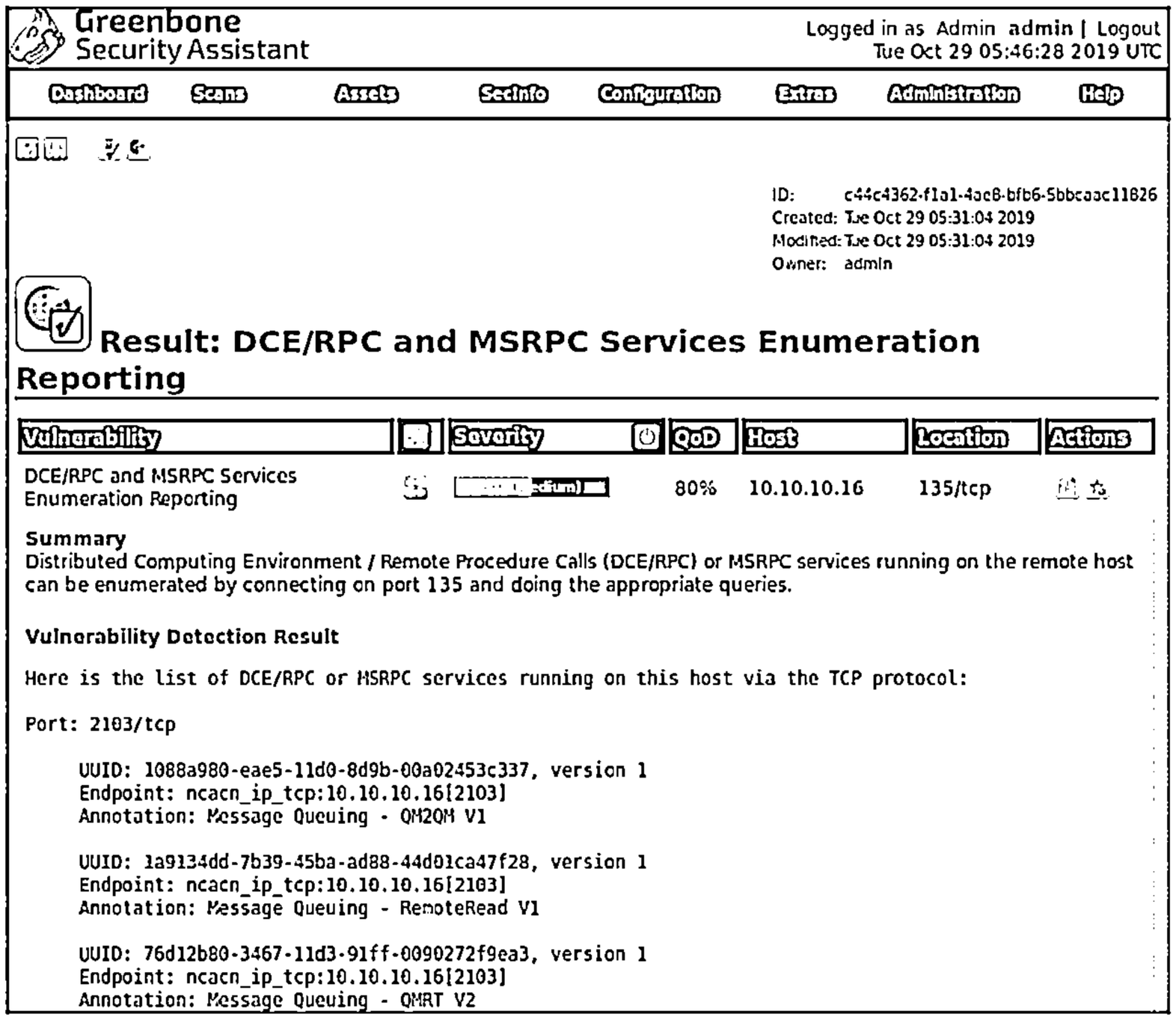


Figure 2.1.10: OpenVAS: Vulnerability Results

17. Similarly, you can click other discovered vulnerabilities under the **Report: Results** section to view detailed information regarding the vulnerabilities in the target system.
18. Next, go through the findings, including all high or critical vulnerabilities. Manually use your skills to verify the vulnerability. The challenge with vulnerability scanners is that they are quite limited; they work well for an internal or white box test only if the credentials are known. We will explore that now: return to your OpenVAS tool, and set up for the same scan again; but this time, turn your **firewall ON** in the **Windows Server 2016** virtual machine.

TASK 1.3

Scan the Target with Firewall Enabled

19. Now, we will enable **Windows Firewall** in the target system and scan it for vulnerabilities.
20. Switch to the **Windows Server 2016** virtual machine and log in with the credentials **Administrator** and **Pa$$w0rd**.

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

21. Navigate to **Control Panel → System and Security → Windows Firewall → Turn Windows Firewall on or off**, enable Windows Firewall, and click **OK**.

Note: By turning the Firewall ON, you are making it more difficult for the scanning tool to scan for vulnerabilities in the target system.

22. Perform **Steps# 9-11** to create another task for scanning the target system.
23. A newly created task appears under the **Tasks** section and starts scanning the target system for vulnerabilities.

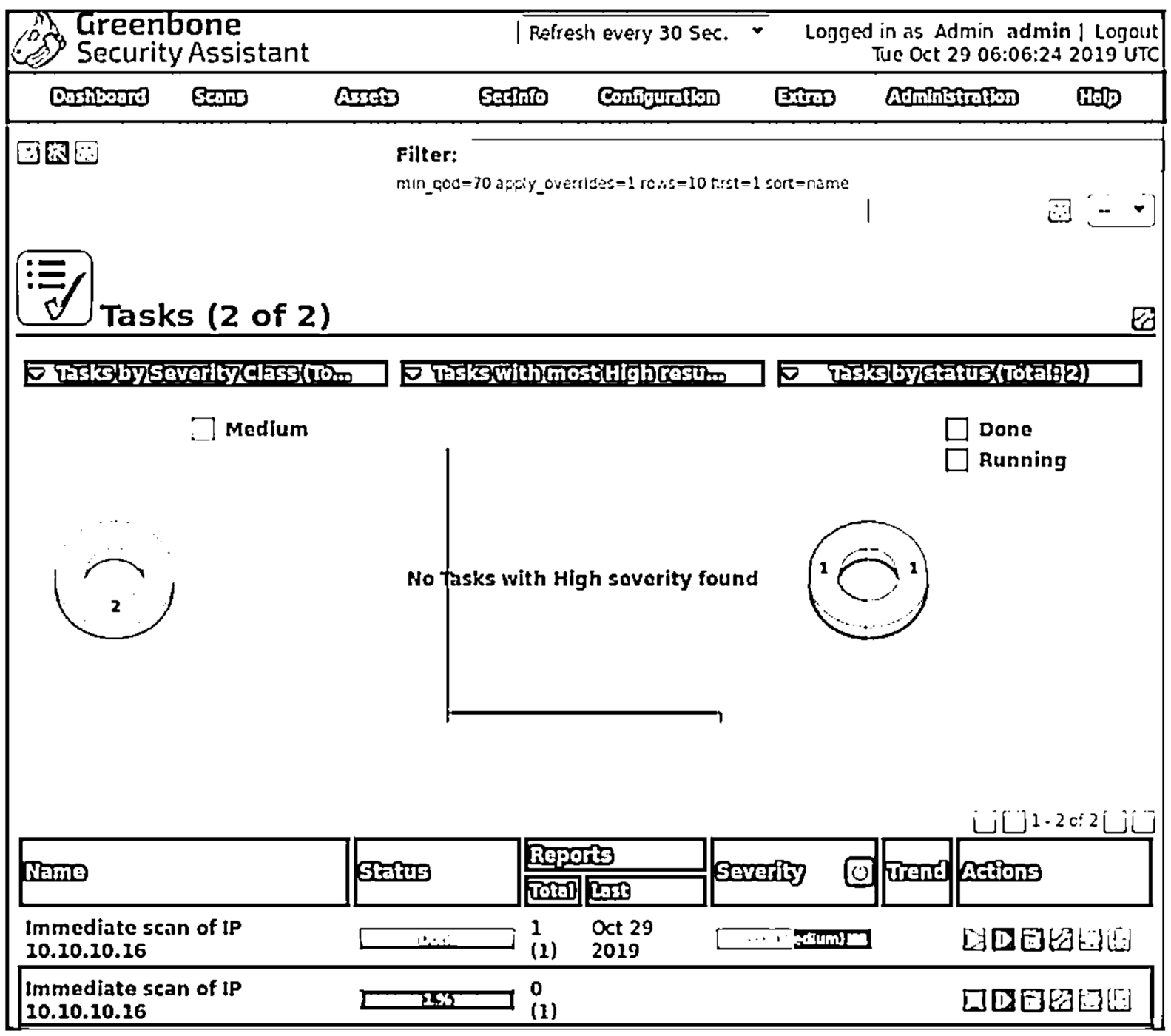


Figure 2.1.11: OpenVAS: Scanning the target IP address

24. After the completion of the scan, click the **Done** button under the **Status** column.
25. **Report: Results** appears, displaying the discovered vulnerabilities along with their severity and port numbers on which they are running.

Note: The results might vary in your lab environment.

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

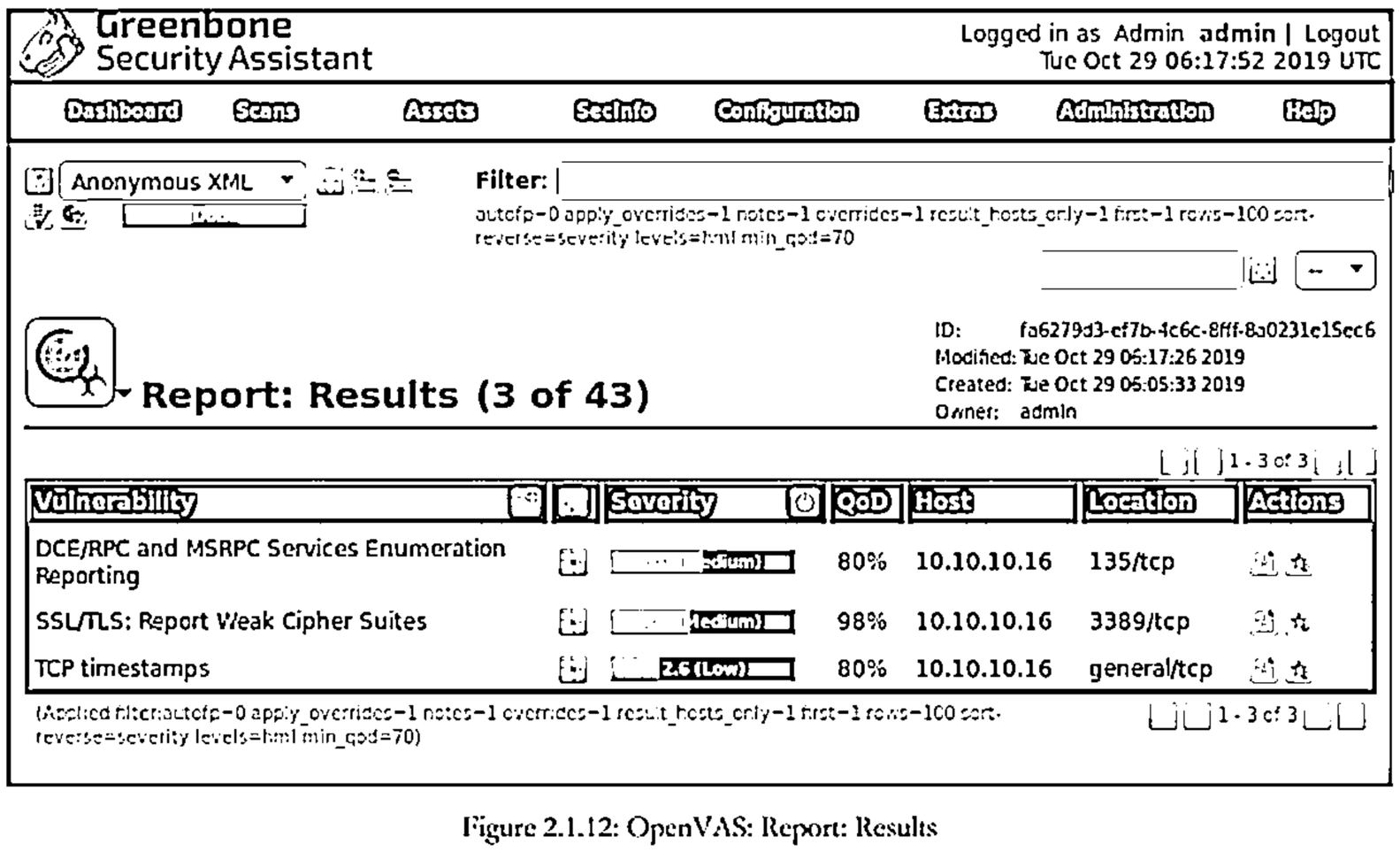


Figure 2.1.12: OpenVAS: Report: Results

26. The scan results for the target machine before and after the Windows Firewall was enabled are the same, thereby indicating that the target system is vulnerable to attack even if the Firewall is enabled.
27. This concludes the demonstration performing vulnerabilities analysis using OpenVAS.
28. Close all open windows and document all the acquired information.
29. Switch to **Windows Server 2016** virtual machine. Navigate to **Control Panel → System and Security → Windows Firewall → Turn Windows Firewall on or off**, disable Windows Firewall, and click **OK**.
30. Turn off **Parrot Security** virtual machine.

TASK 2 Perform Vulnerability Scanning using Nessus

Here, we will use Nessus to perform vulnerability scanning on the target system.

TASK 2.1 Install Nessus

1. Turn on **Windows 10** virtual machines.

Note: Ensure that the **Windows Server 2016** virtual machine is turned on.

2. In the **Windows 10** virtual machine, log in with the credentials **Admin** and **Pa$$w0rd**.
3. Navigate to **E:\CEH-Tools\CEHv11 Module 05 Vulnerability Analysis\Vulnerability Assessment Tools\Nessus** and double-click **Nessus-8.7.2-x64.msi**.
4. **Tenable Nessus InstallShield Wizard** appears. Follow the installation steps to install Nessus with all default settings.

Note: If **User Account Control** pop-up appears, click **Yes**.

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

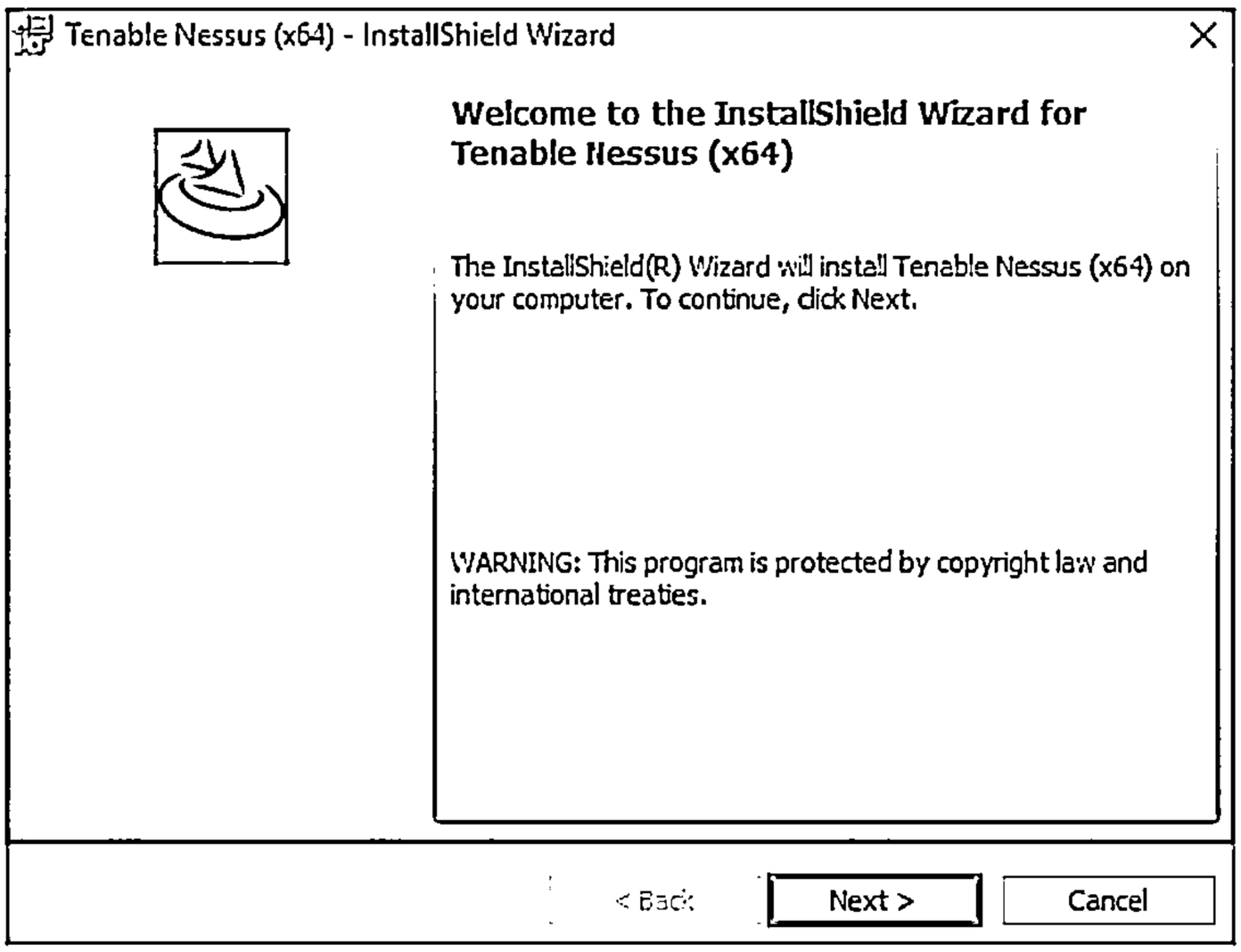


Figure 2.2.1: Nessus Install Shield Wizard

Nessus is an assessment solution for identifying vulnerabilities, configuration issues, and malware, which can be used to penetrate networks. It performs vulnerability, configuration, and compliance assessment.

Note: During installation, if a **Windows Security** pop-up appears, click **Install** or skip to the next step.

Note: During installation, if a **WinPcap Setup** window appears, click **Install** and follow the installation wizard to install WinPcap with default settings. Once the installation finishes, click **Finish**.

5. After the completion of the installation, in the **Tenable Nessus InstallShield Wizard** window, click **Finish**.

It supports various technologies such as OSes, network devices, hypervisors, databases, tablets/phones, web servers, and critical infrastructure.

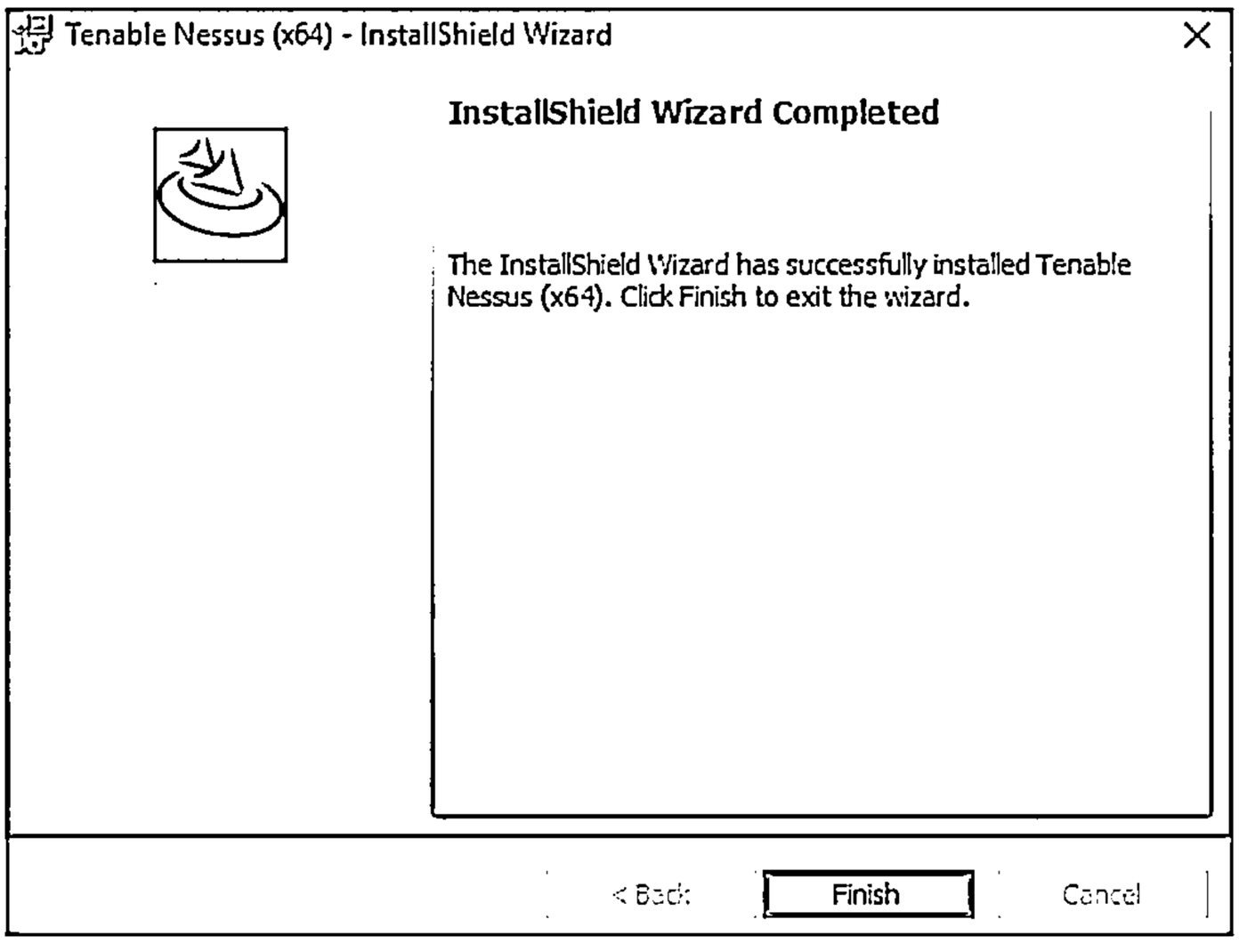


Figure 2.2.2: Nessus window

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

6. The **Nessus** opens-up in the default browser. Click **Connect via SSL** button to proceed.

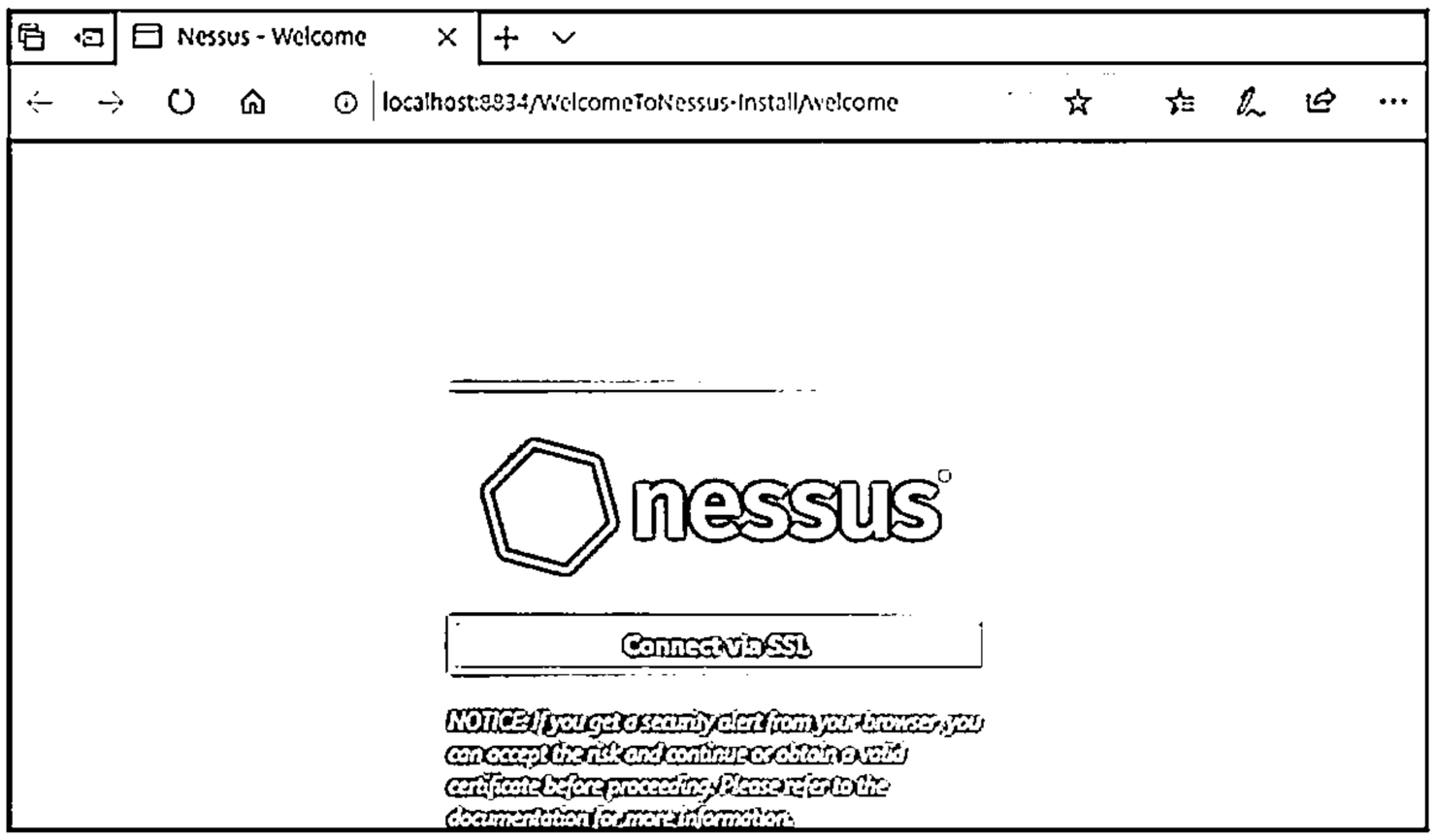


Figure 2.2.3: Nessus window: click Connect via SSL

7. **Tenable Nessus (x64) Installer Information** pop-up appears asking to restart the system for the configuration changes; click **No**.
8. **This site is not secure** page appears, expand the **Details** section and click **Go on to the webpage**.

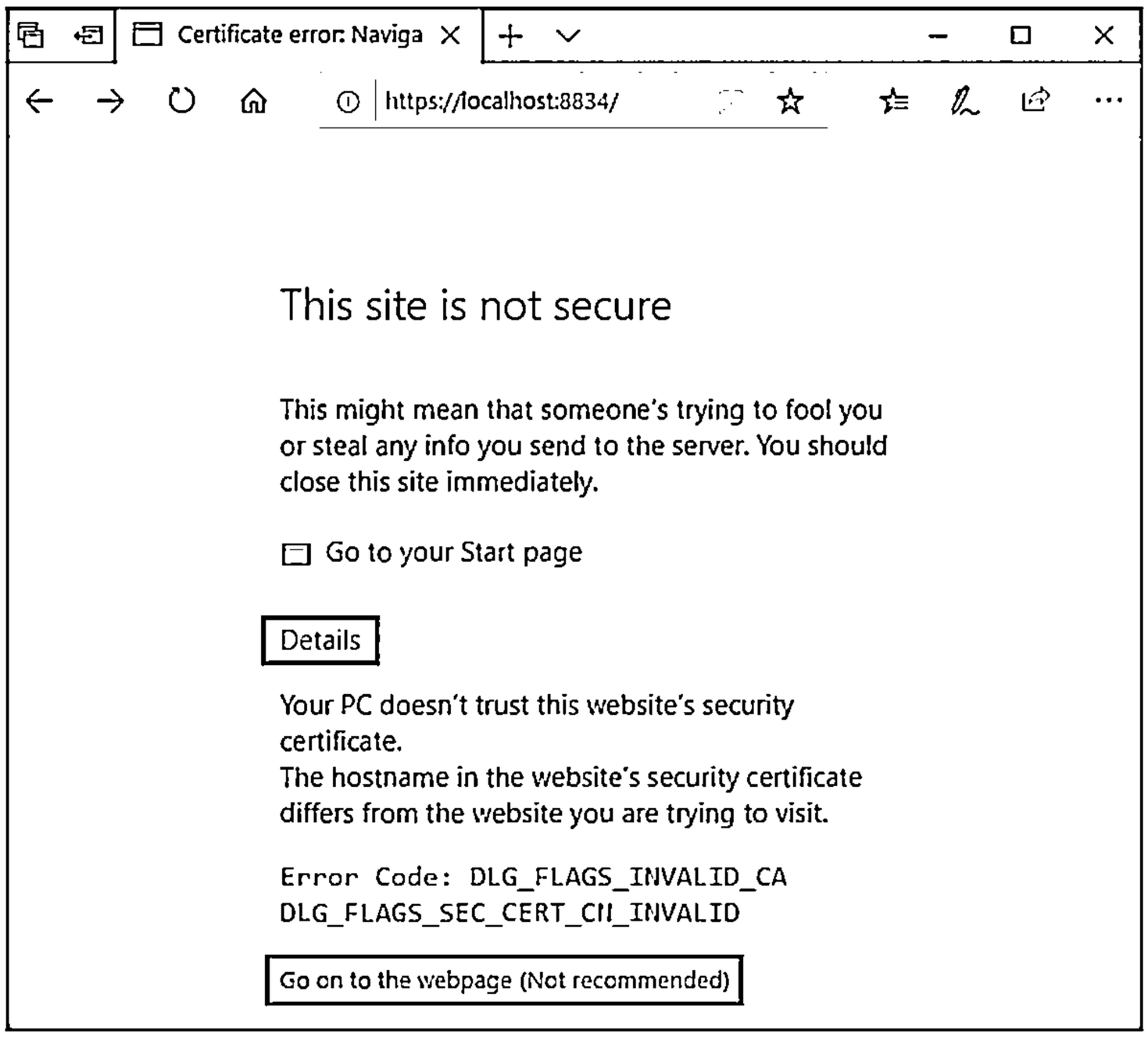


Figure 2.2.4: This site is not a secure webpage

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

9. **Welcome to Nessus** page appears, ensure that **Nessus Essentials** radio button is selected and click **Continue**.

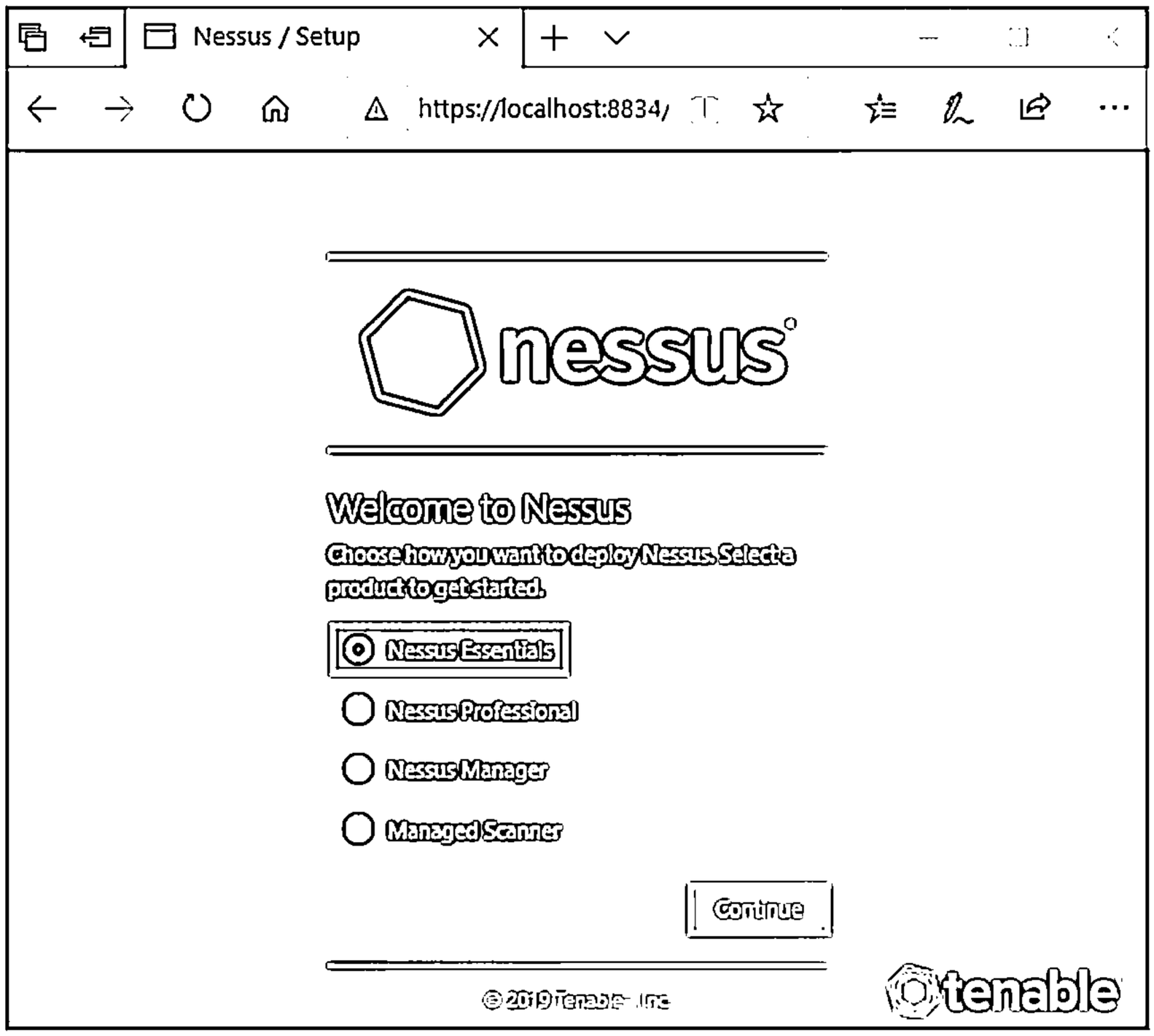


Figure 2.2.5: Welcome to Nessus

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

TASK 2.2

Register in Nessus to Obtain the Activation Code

10. The **Get an activation code** page appears. Enter your personal details and click the **Email** button.

Note: You can use an alias, however, you will need a valid e-mail to retrieve the activation code. Consider creating an alias e-mail account if you do not have one.

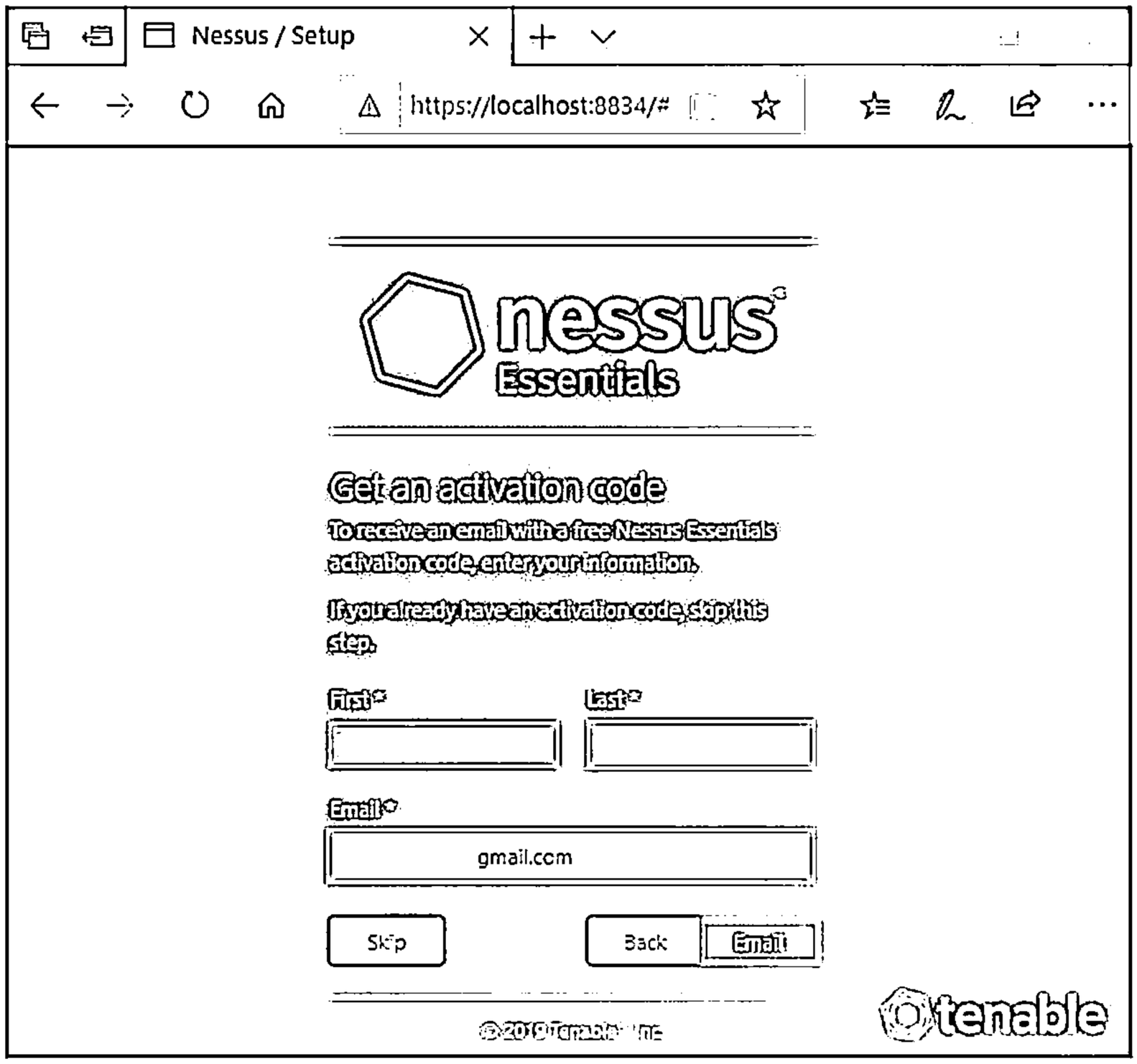


Figure 2.2.6: Get an activation code wizard

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

11. Once the above is completed, open a new tab and log in to your email account provided in the previous step, open the mail from **Tenable Nessus Essentials**, and copy the activation code. Close the web browser.

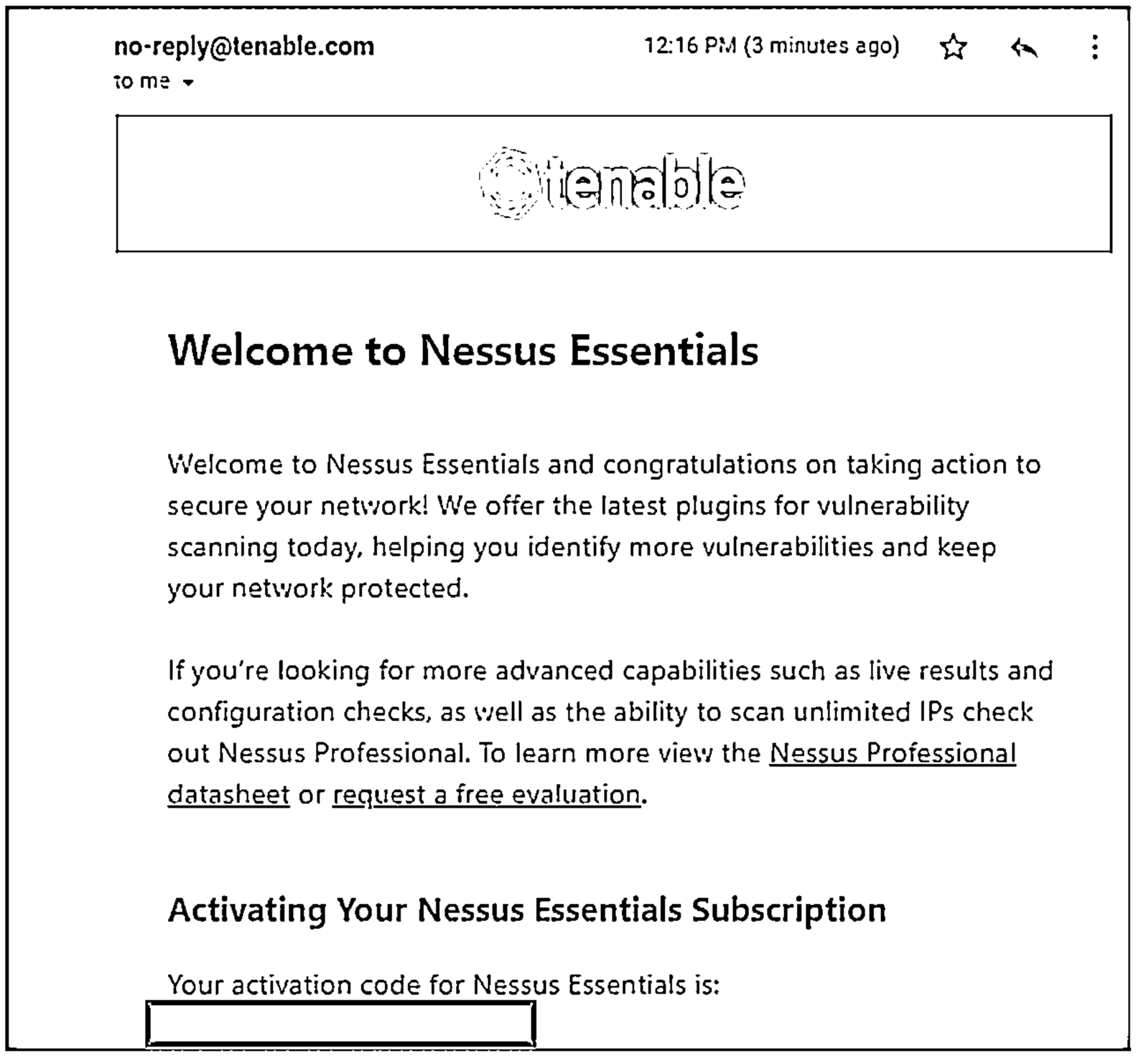


Figure 2.2.7: Activation code sent to your personal mail

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

12. Switch back to the **Microsoft Edge** web browser; in the **Register Nessus** page, paste the copied activation code in the **Activation Code** field; then, click **Continue**.

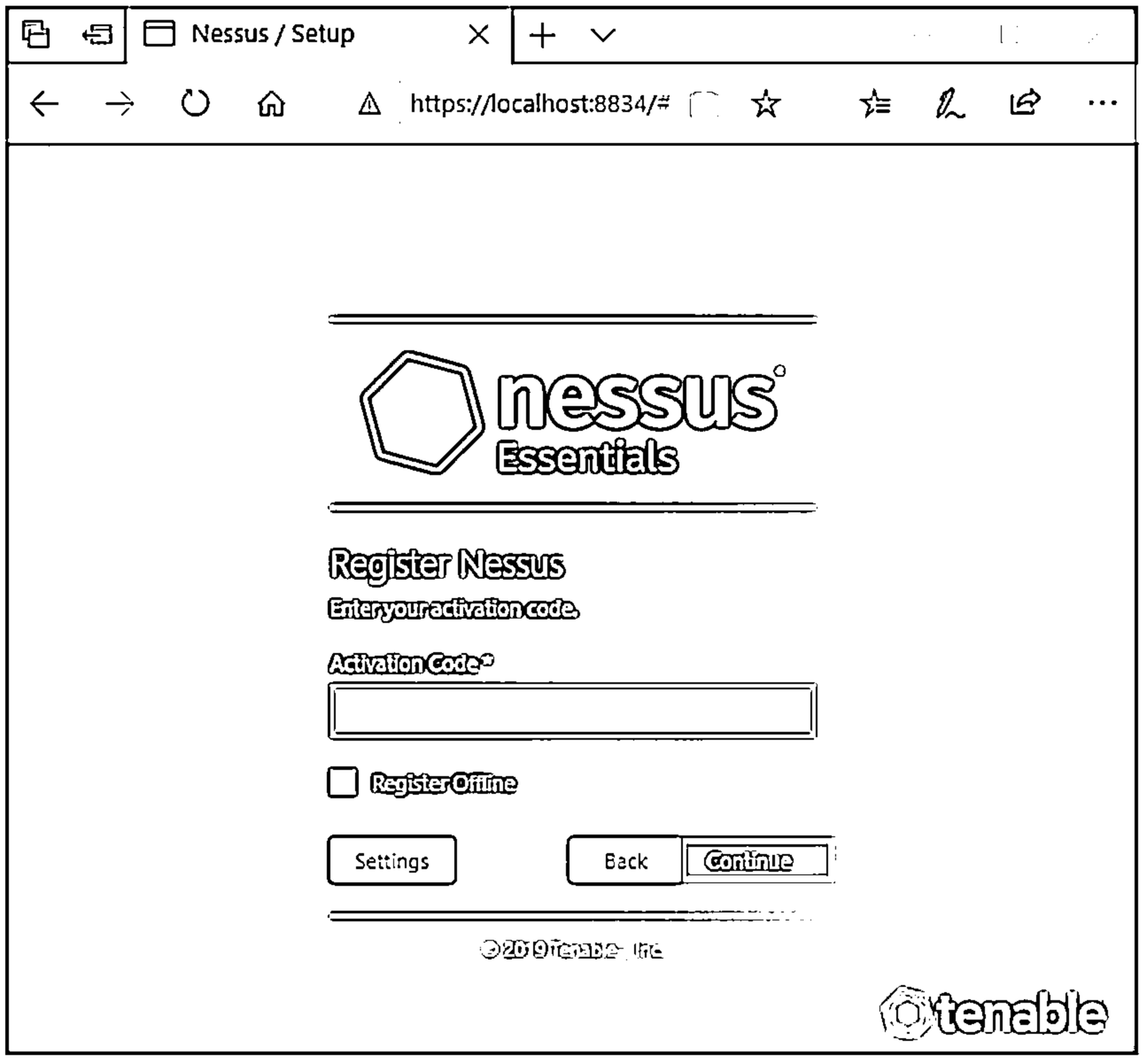


Figure 2.2.8: Register Nessus: Enter Activation Code

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

TASK 2.3

Create a User Account

13. **Create a user account** page appears. Create credentials for administrative control of the scanner. (here, Username: **Admin** and Password: **password**); then, click **Submit**.

Note: These credentials will be used to log in to Nessus at the time of vulnerability scanning.

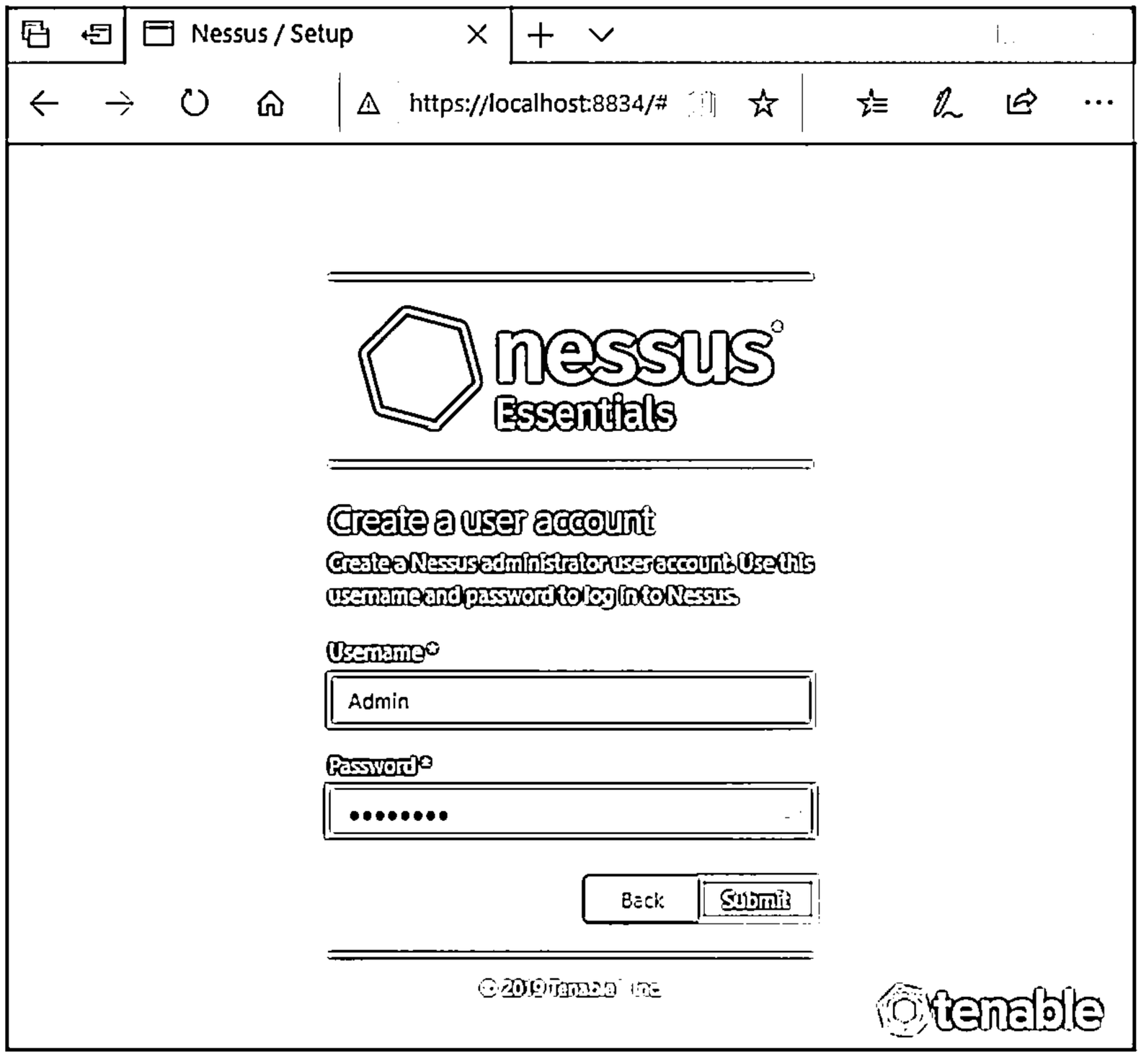


Figure 2.2.9: Create a user account: enter credentials

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

14. The **Downloading plugins...** wizard appears. Nessus will start fetching the plugins and will install them.

Note: It will take approximately 10 minutes to download plugins and perform the initialization.

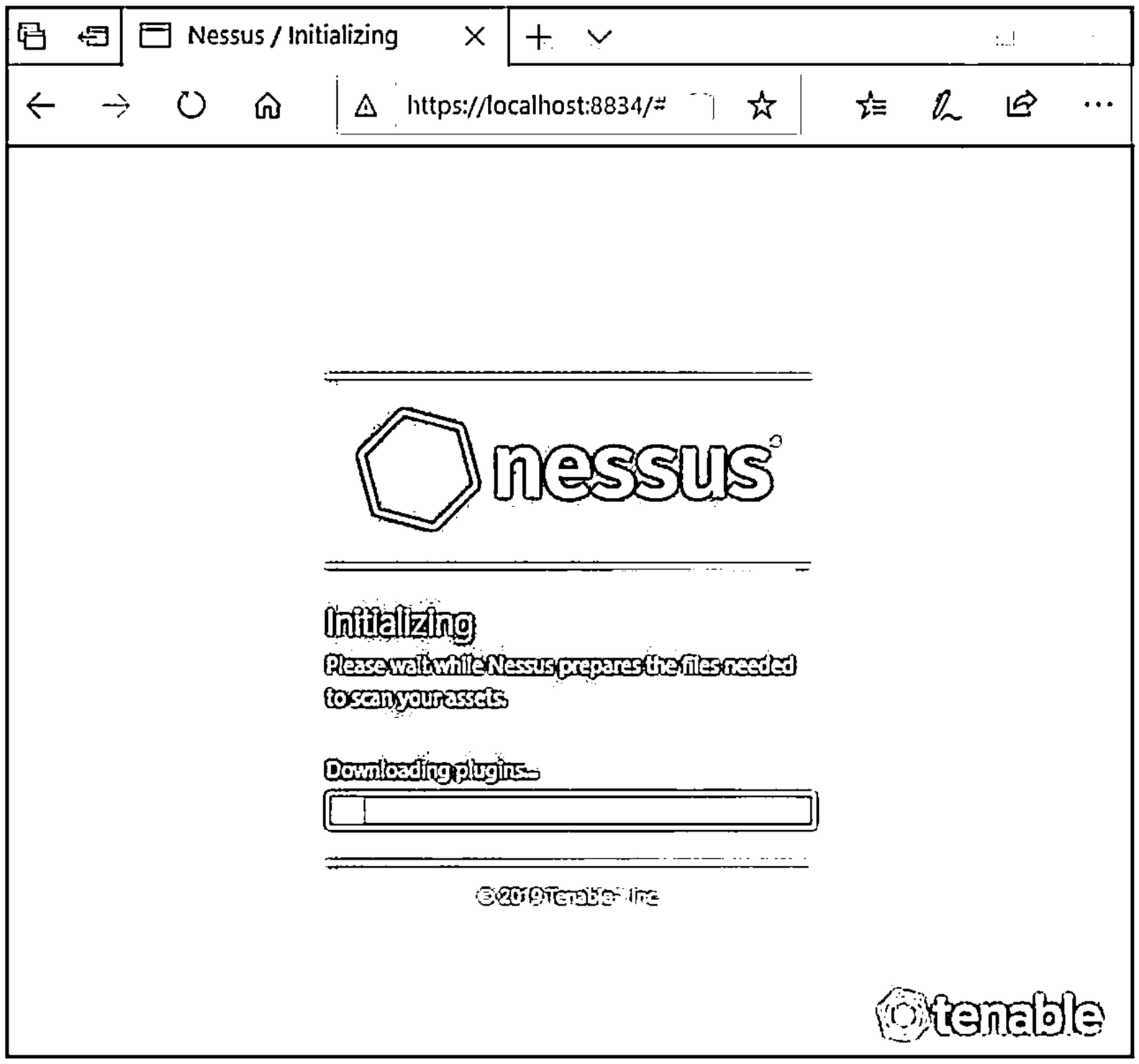


Figure 2.2.10: Nessus: Downloading plugins…

15. Nessus begins to initialize; this will take some time. On completion of initialization, the Nessus dashboard appears along with the **Welcome to Nessus Essentials** pop-up. Close the pop-up.

Note: In the **Let Microsoft Edge save and fill your password for this site next time?** pop-up, click **Never**.

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

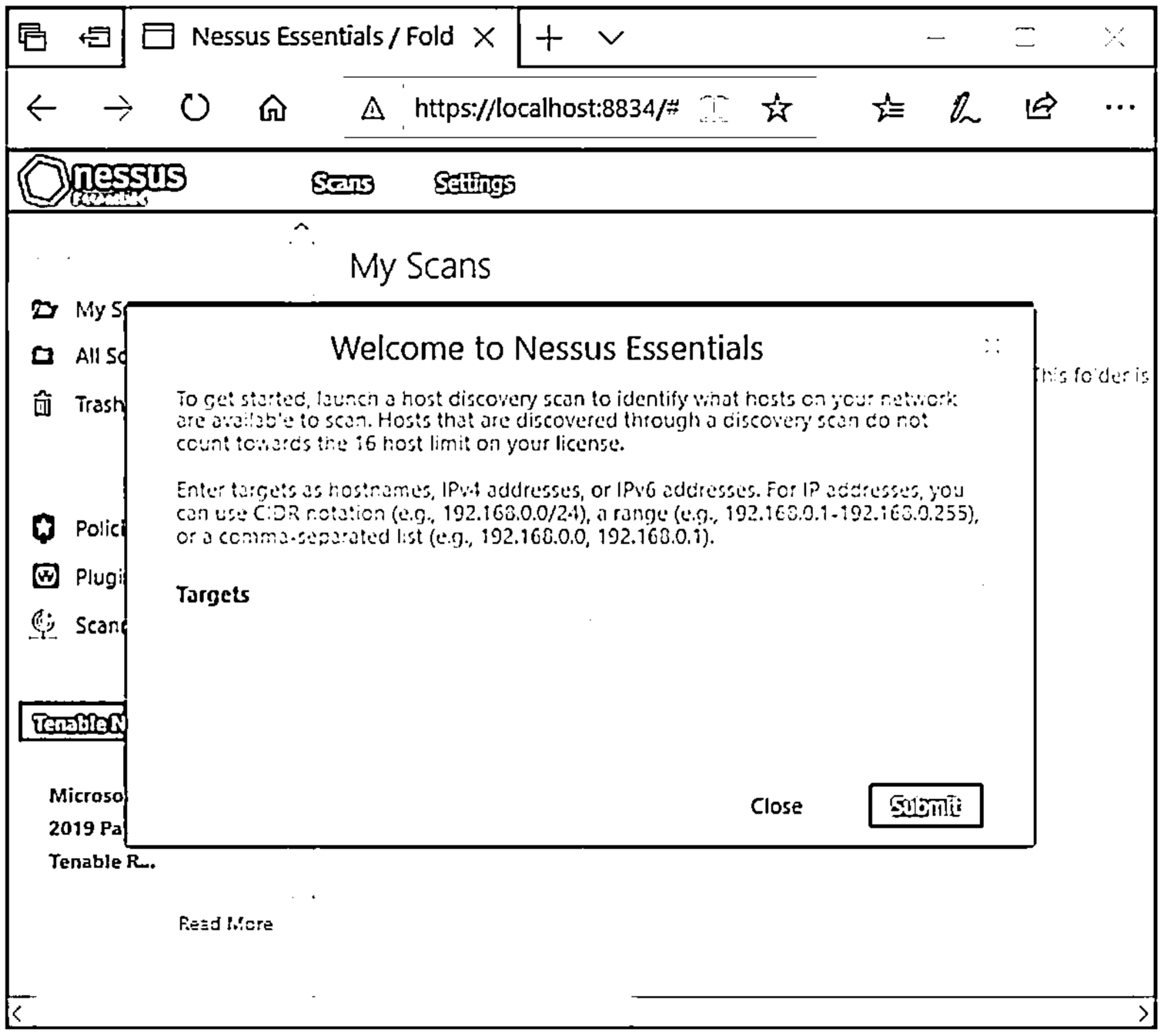


Figure 2.2.11: Welcome to Nessus Essentials page

TASK 2.4

Add a Network Policy

16. The **Nessus Essentials** dashboard appears; click **Policies** under **RESOURCES** section from the pane on the left.

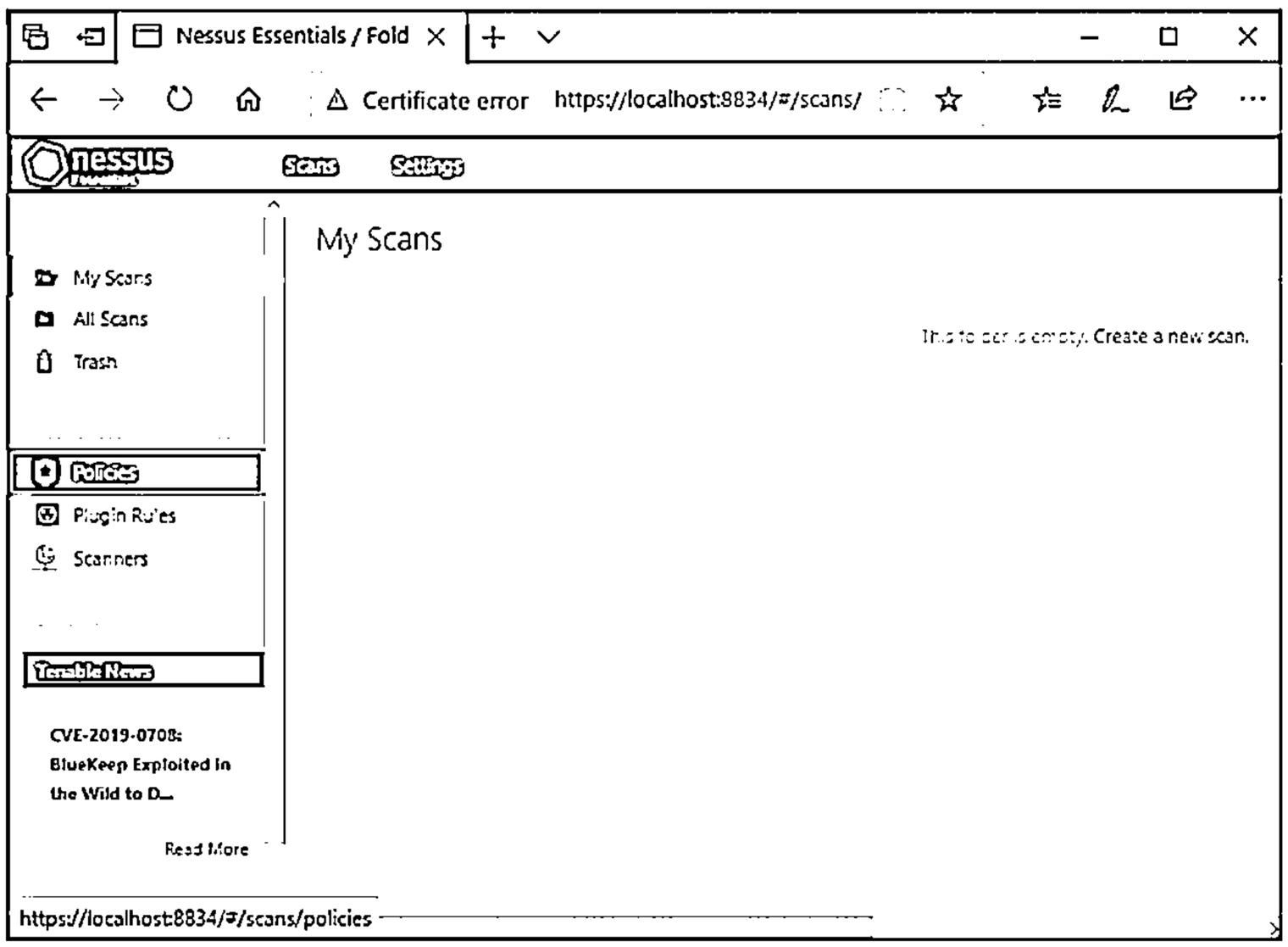


Figure 2.2.12: Nessus Essentials dashboard: Click Policies

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

17. The **Policies** window appears; click **Create a new policy.**

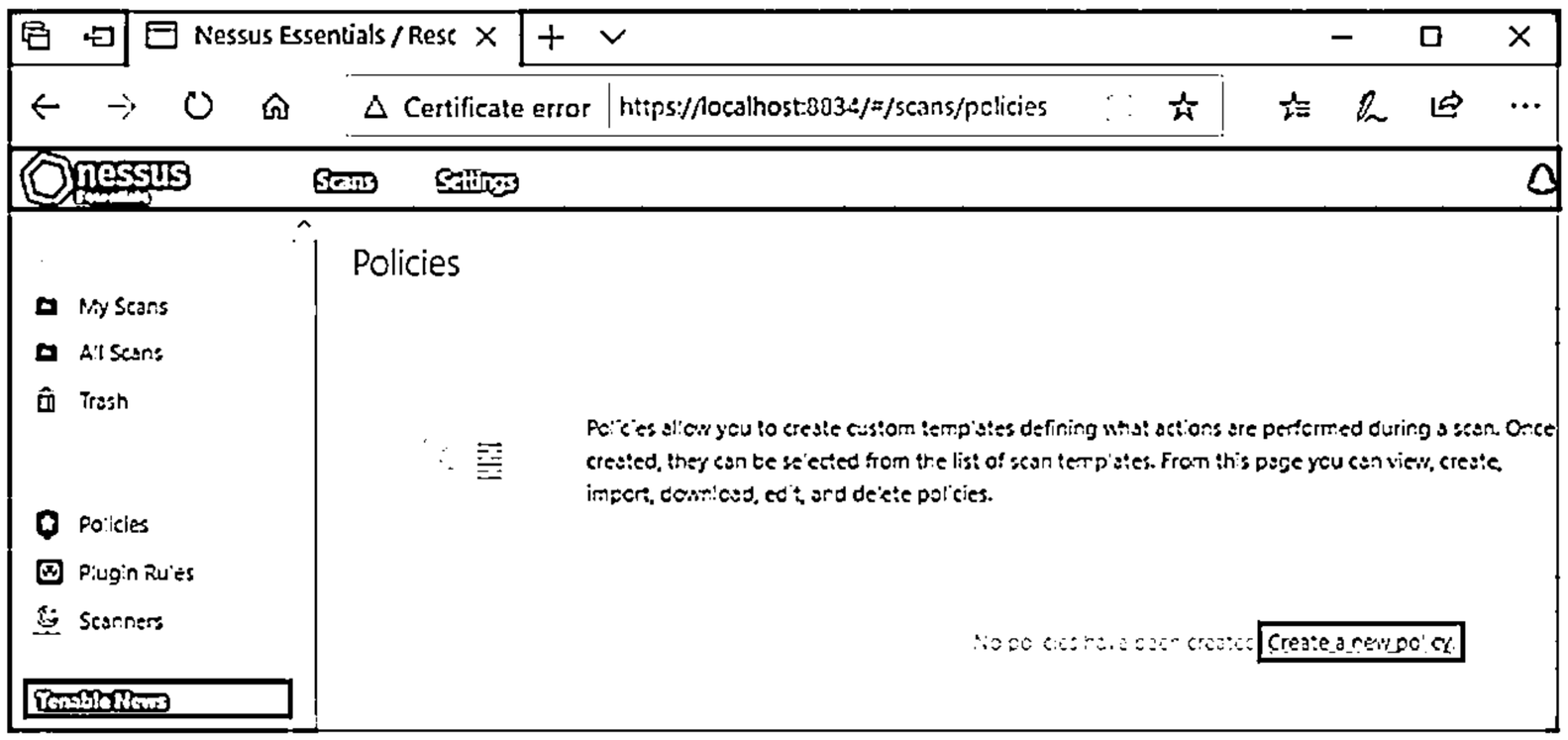


Figure 2.2.13: Adding a new policy in Nessus

18. The **Policy Templates** window appears; click **Advanced Scan.**

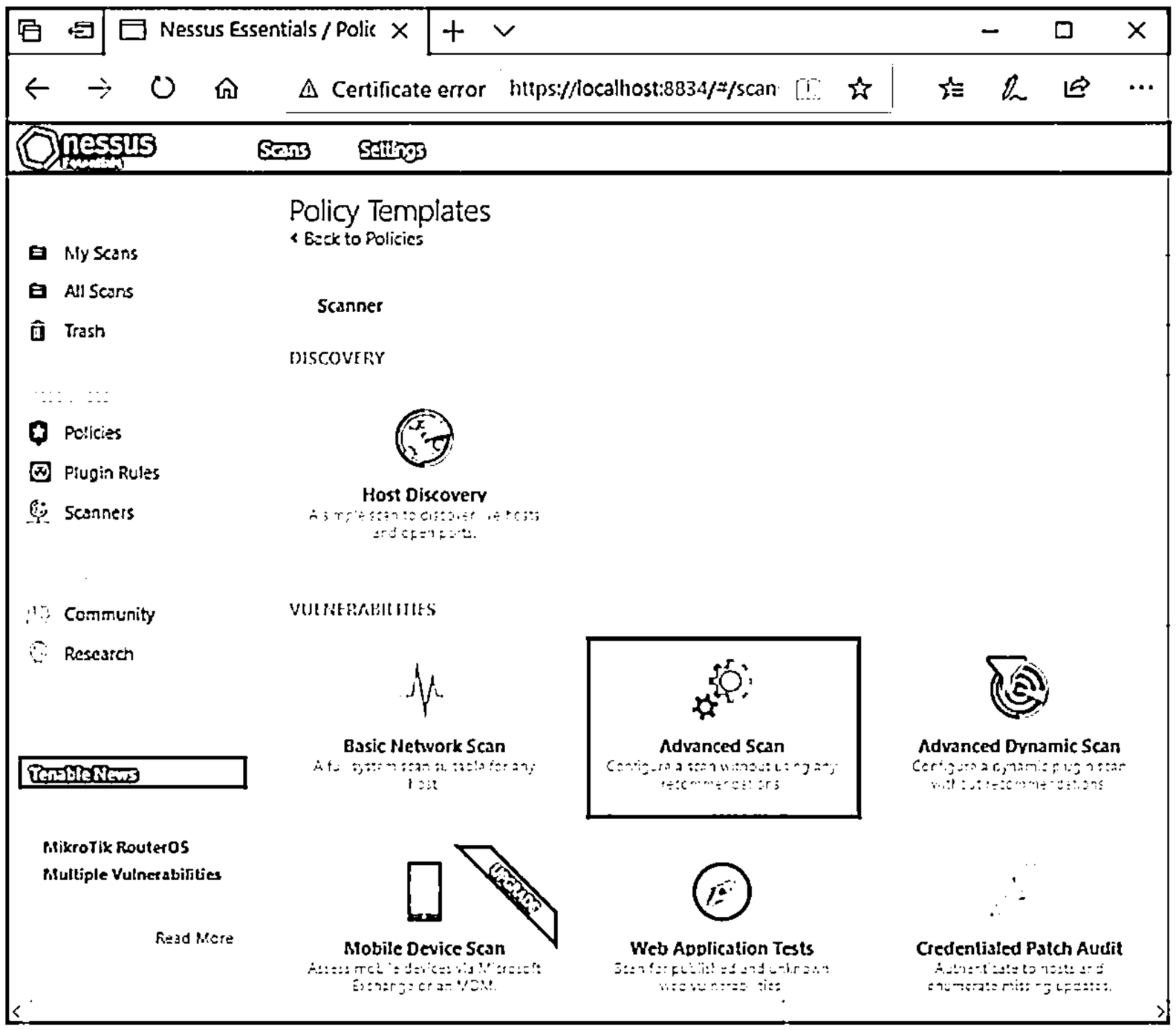


Figure 2.2.14: Choosing Advance Policy from the policy templates

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

TASK 2.5

Configure a Network Policy

19. The **New Policy / Advanced Scan** section appears. In the **Settings** tab under the **BASIC** setting type, specify a policy name in the **Name** field (here, **NetworkScan_Policy**), and give a **Description** about the policy (here, **Scanning a Network**).

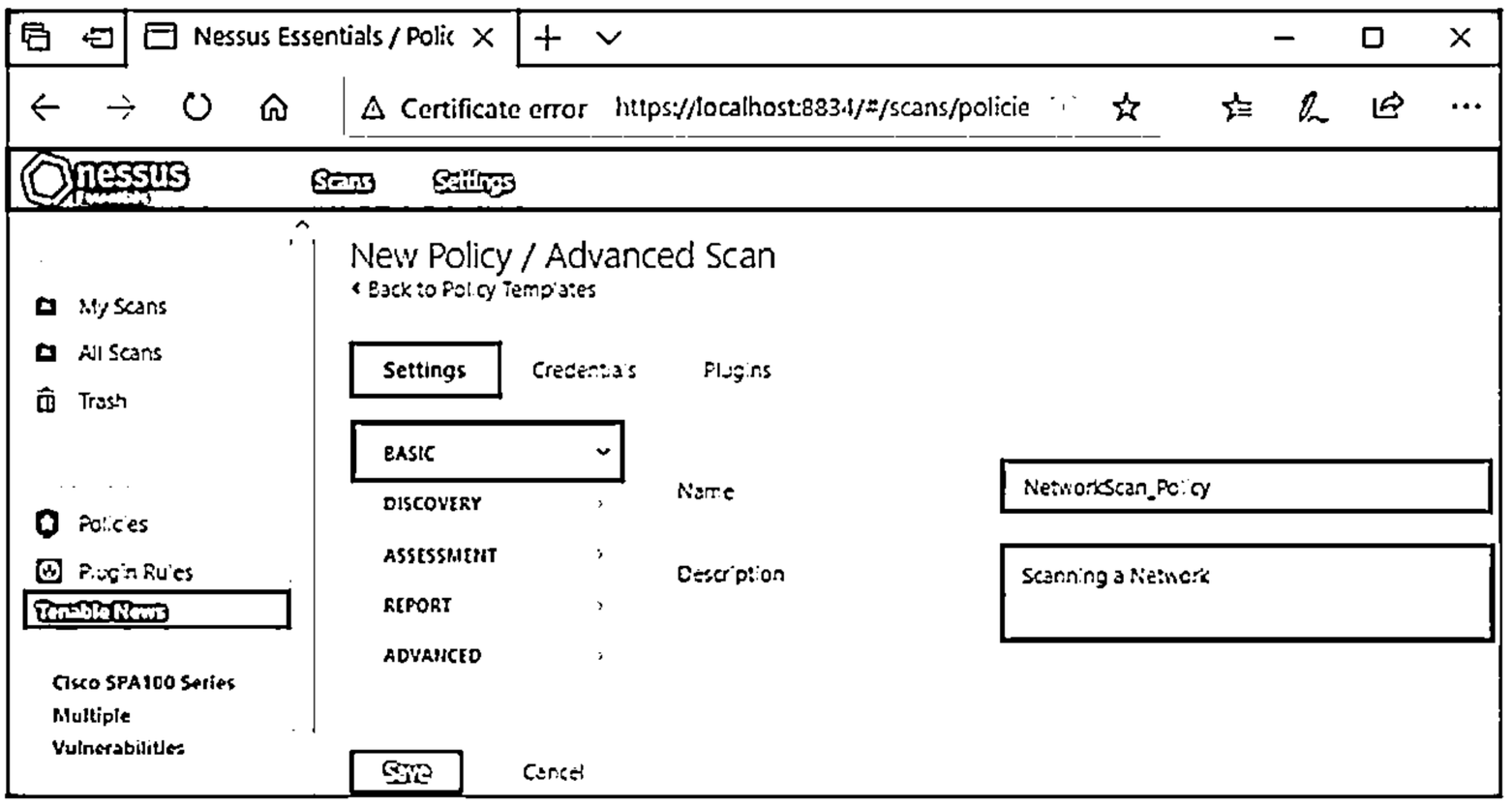


Figure 2.2.15: Customizing the general settings

20. In the **Settings** tab, click **DISCOVERY** setting type and turn off the **Ping the remote host** option from the right pane.

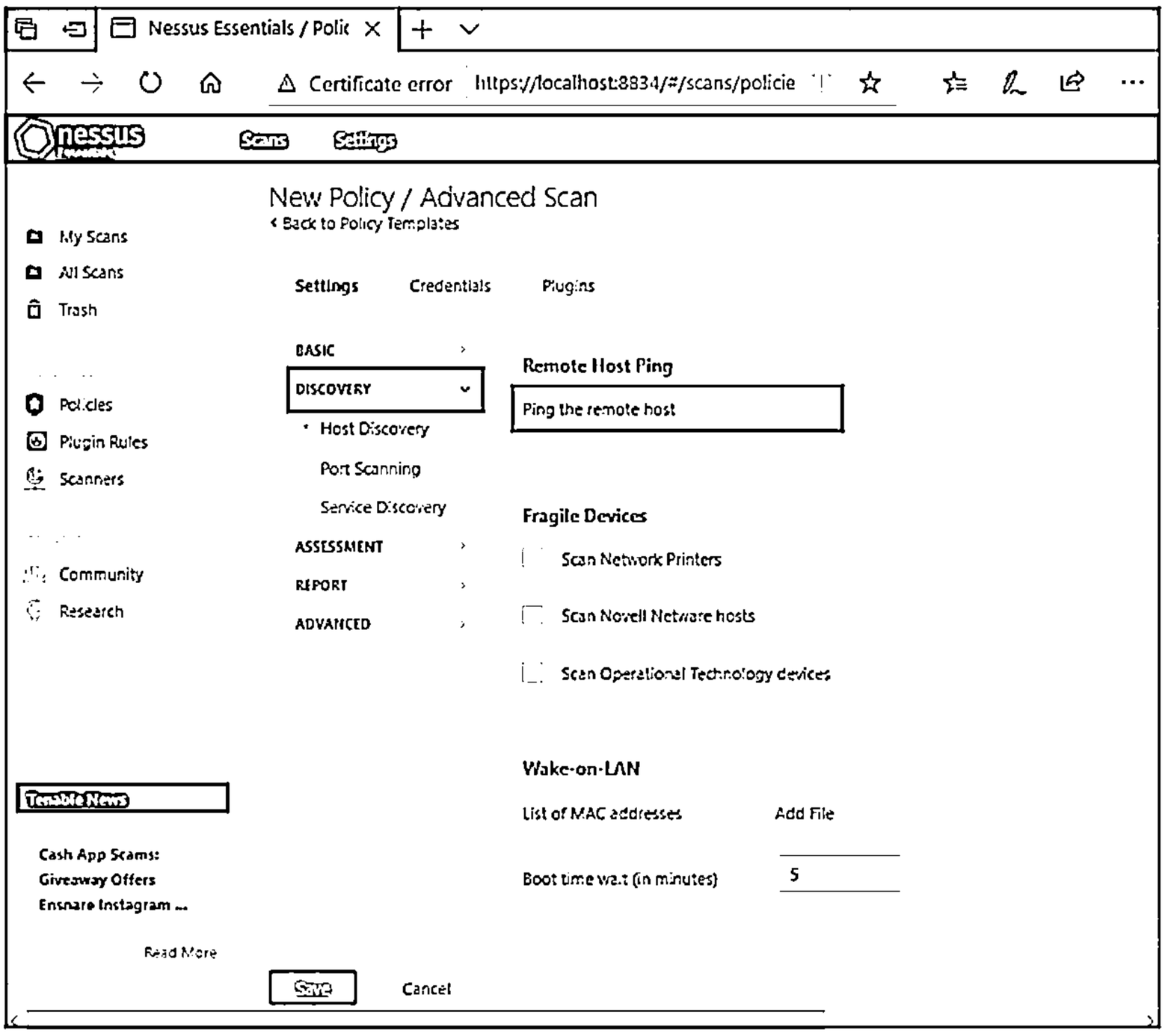


Figure 2.2.16: Policy General Settings window with Port Scanning Setting Type

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

21. Select the **Port Scanning** option under the **DISCOVERY** setting type, and then click the **Verify open TCP ports found by local port enumerators** checkbox. Leave the other fields with default options, as shown in the screenshot.

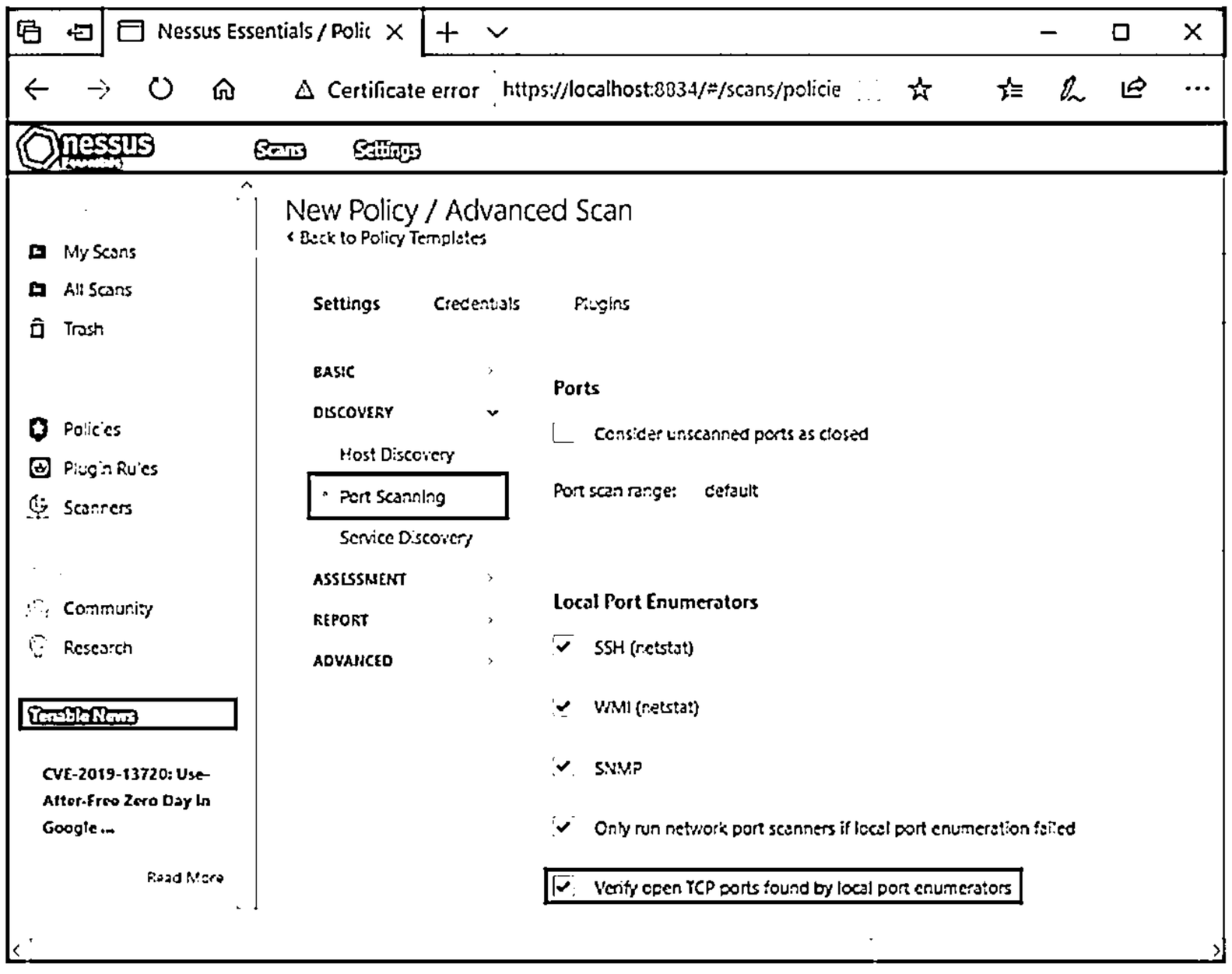


Figure 2.2.17: Customizing the Port Scanning Setting Type

22. Select the **ADVANCED** setting type. In the right pane, under the **Performance Options** settings, set the values of **Max number of concurrent TCP sessions per host** and **Max number of concurrent TCP sessions per scan** to **Unlimited**.

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

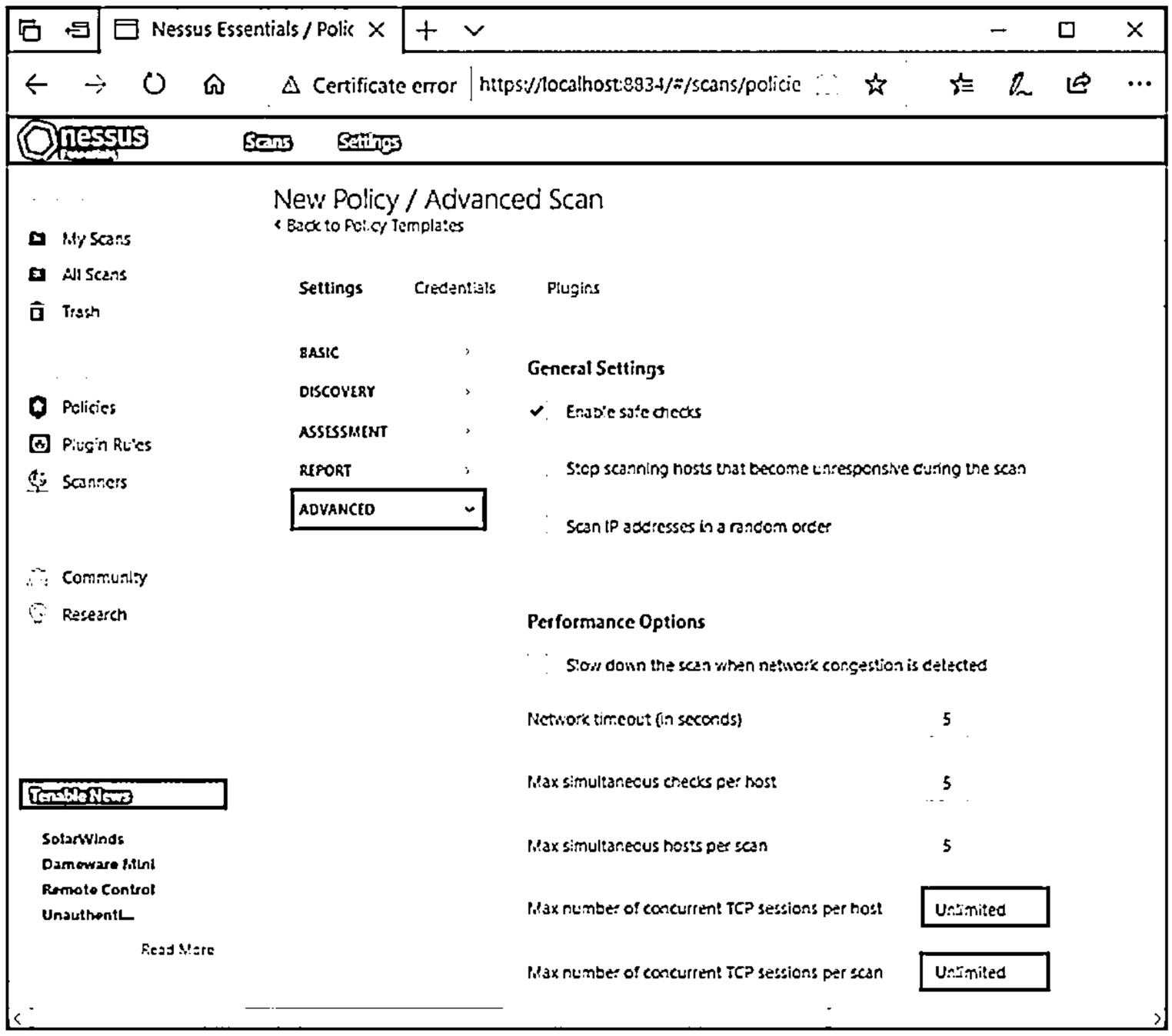


Figure 2.2.18: Advanced Setting Type window

23. To configure the credentials of a new policy, click the **Credentials** tab and select **Windows** from the options.

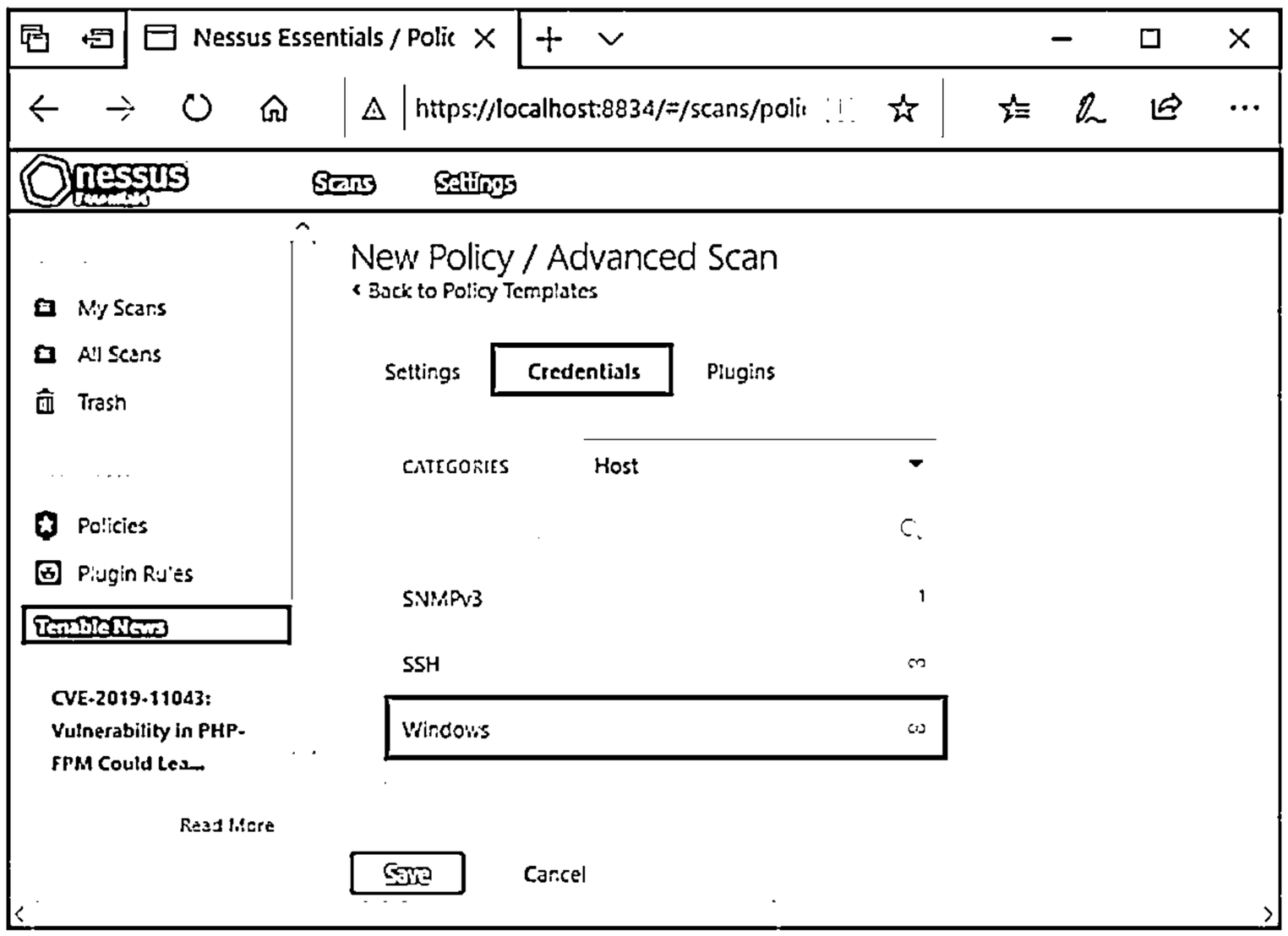


Figure 2.2.19: Adding Policies and setting Credentials

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

24. Specify the **Username** and **Password** in the window. Here, the specified credentials are **CEH123/qwerty@123**.

Note: Re-enter the created user account credentials, **Admin/password**, if session timeout notification pop-up appears.

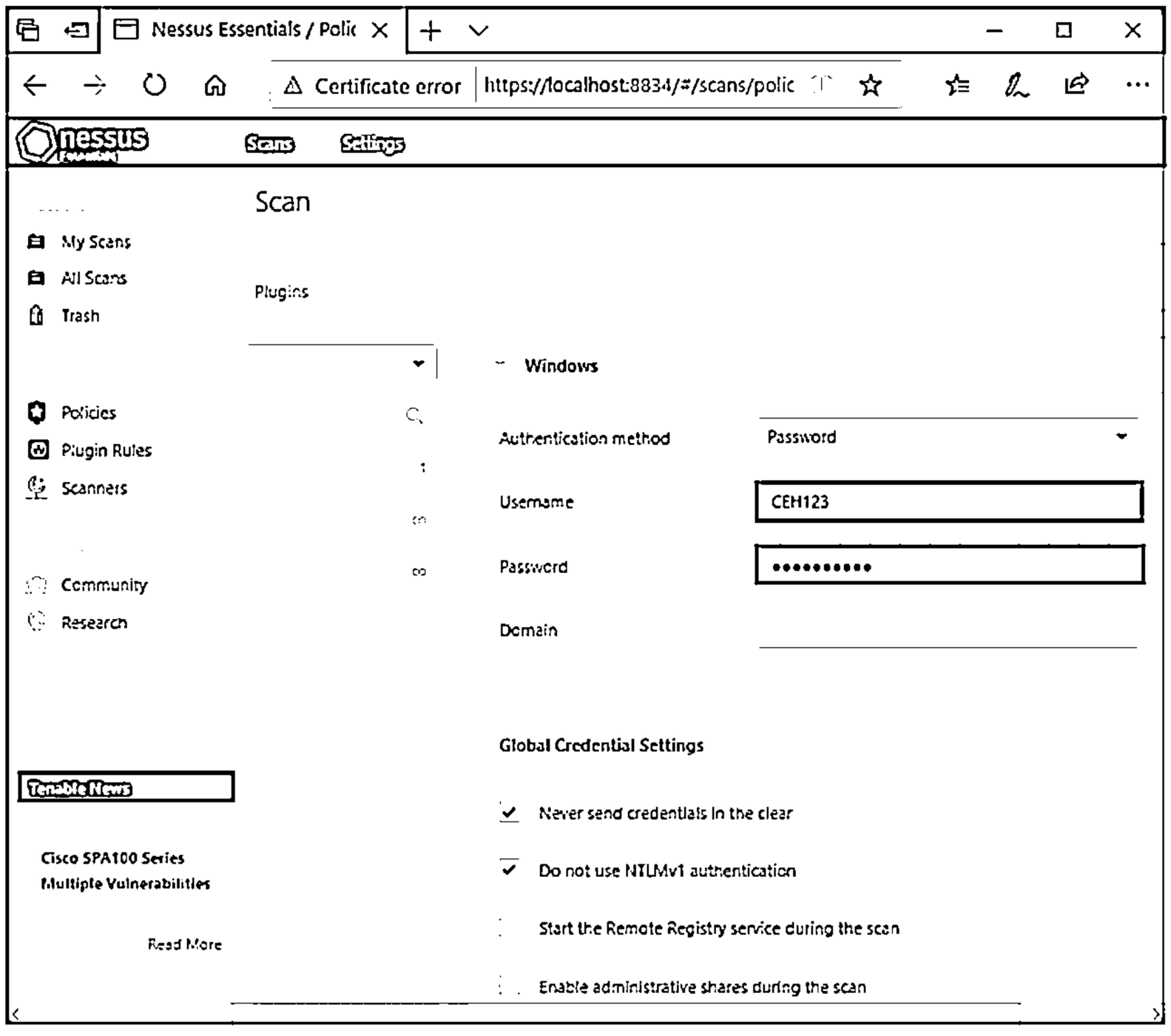


Figure 2.2.20: Customizing the windows credentials

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

25. Click the **Plugins** tab and do not alter any of the options in this window. Click the **Save** button.

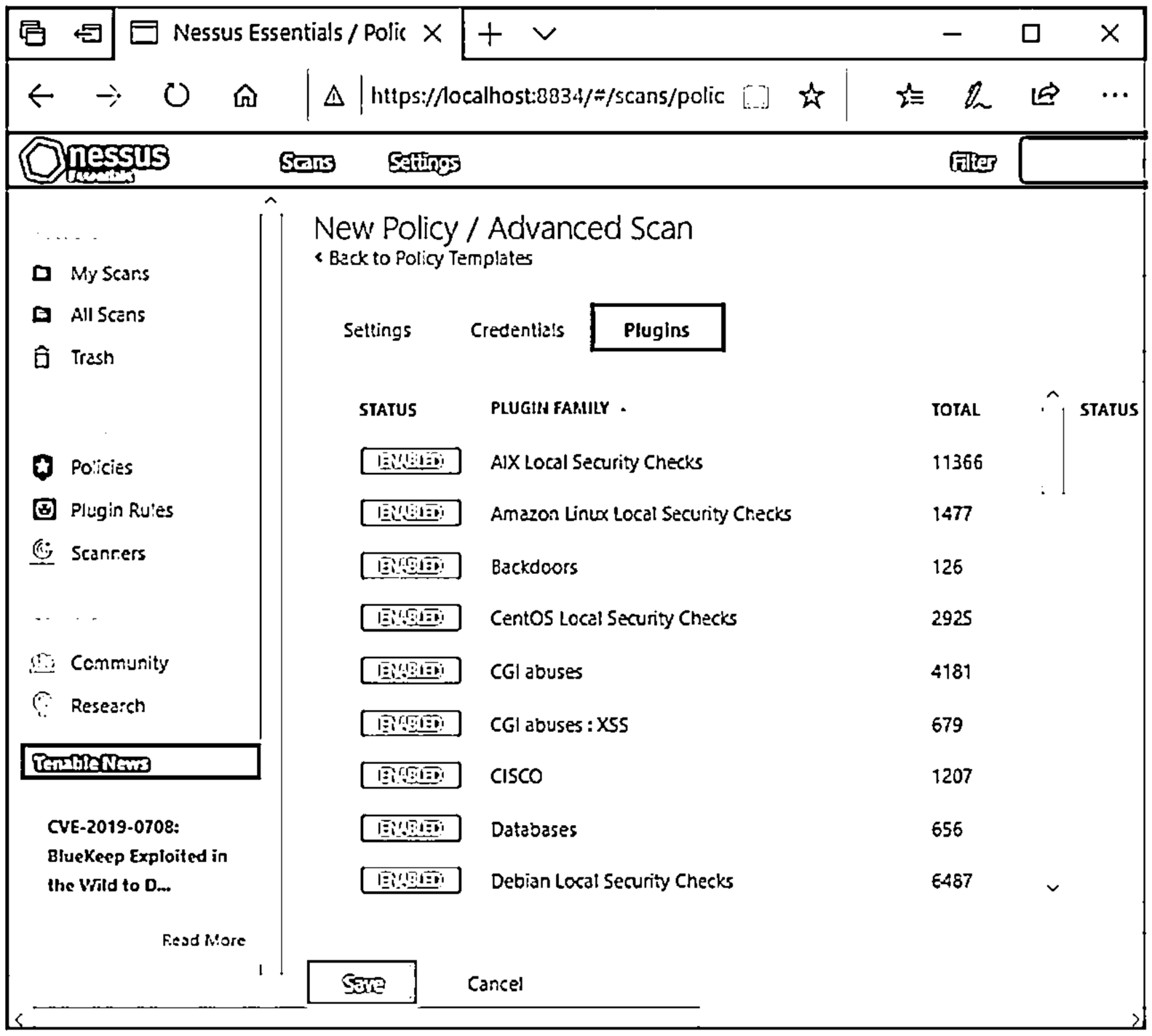


Figure 2.2.21: The Nessus: Policy Plugin Configurations window

26. A **Policy saved successfully** notification pop-up appears, and the policy is added in the **Policies** window, as shown in the screenshot.

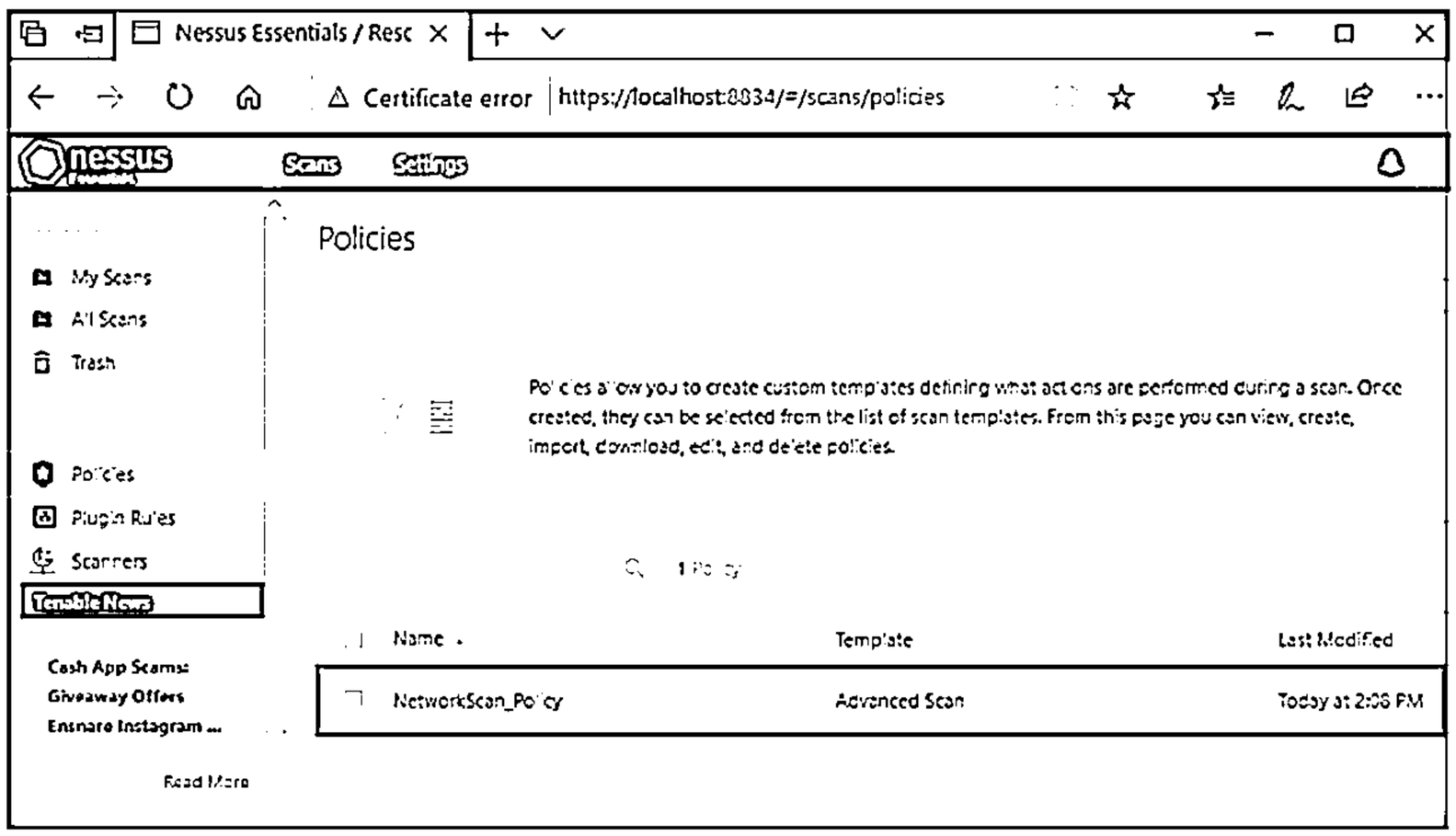


Figure 2.2.22: The Nessus: Policies window with the newly added policy

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

27. Now, click **Scans** from the menu bar to open **My Scans** window; click **Create a new scan.**

Figure 2.2.23: Setting a new scan in Nessus

28. The **Scan Templates** window appears. Click the **User Defined** tab and select **NetworkScan Policy.**

Note: If an **API Disabled** pop-up appears, refresh the browser and log in again to the **Nessus Essentials** using credentials (**Admin/password**).

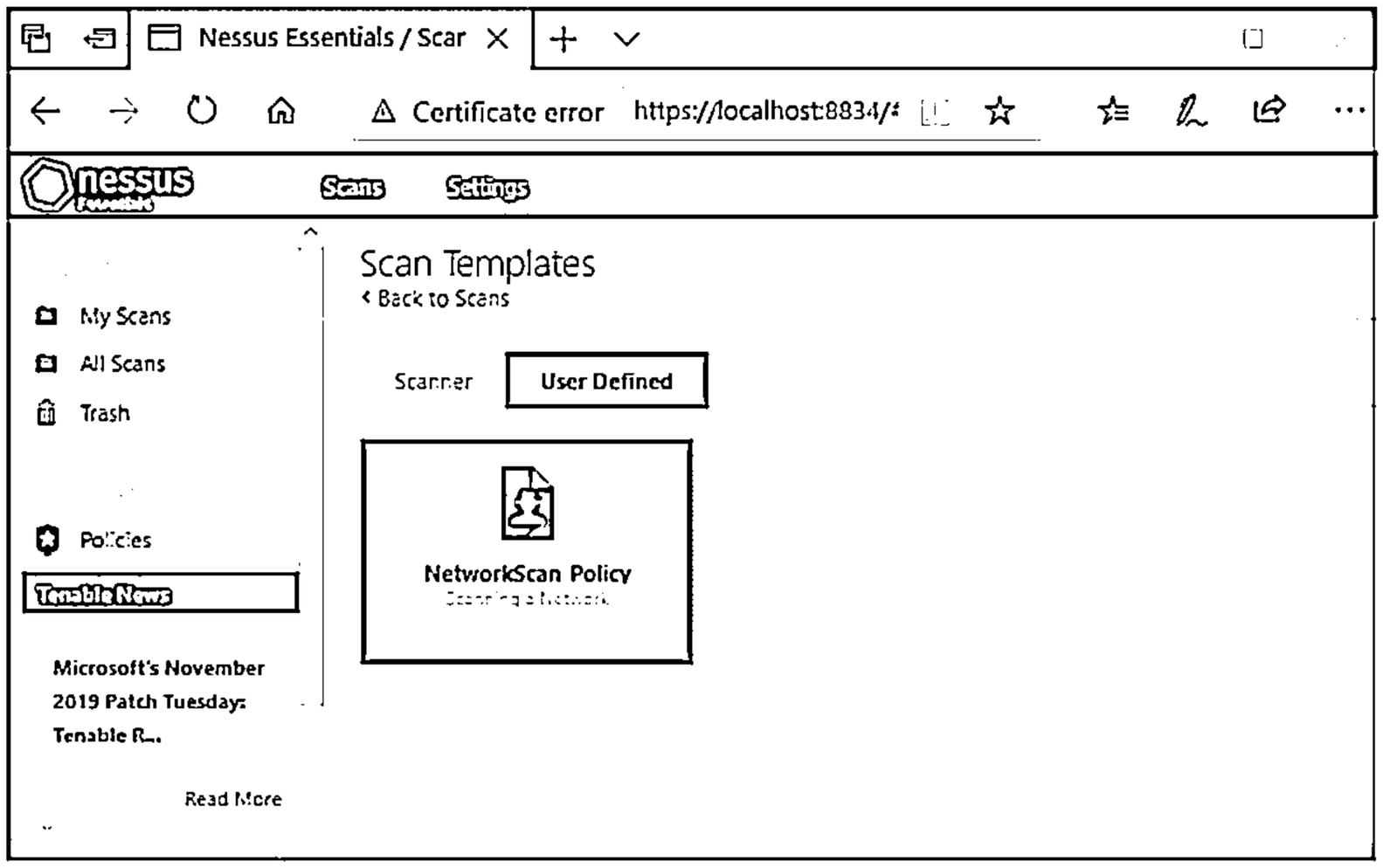


Figure 2.2.24: Setting a new scan in Nessus

29. The **New Scan / NetworkScan_Policy** window appears. Under **General Settings** in the right pane, input the **Name** of the scan (here, **Local Network**) and enter the **Description** for the scan (here, **Scanning a local network**); in the **Targets** field, enter the IP address of the target on which you want to perform the vulnerability analysis. In this lab, the target IP address is **10.10.10.16** (**Windows Server 2016**).

Note: The IP addresses may vary in your lab environment.

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

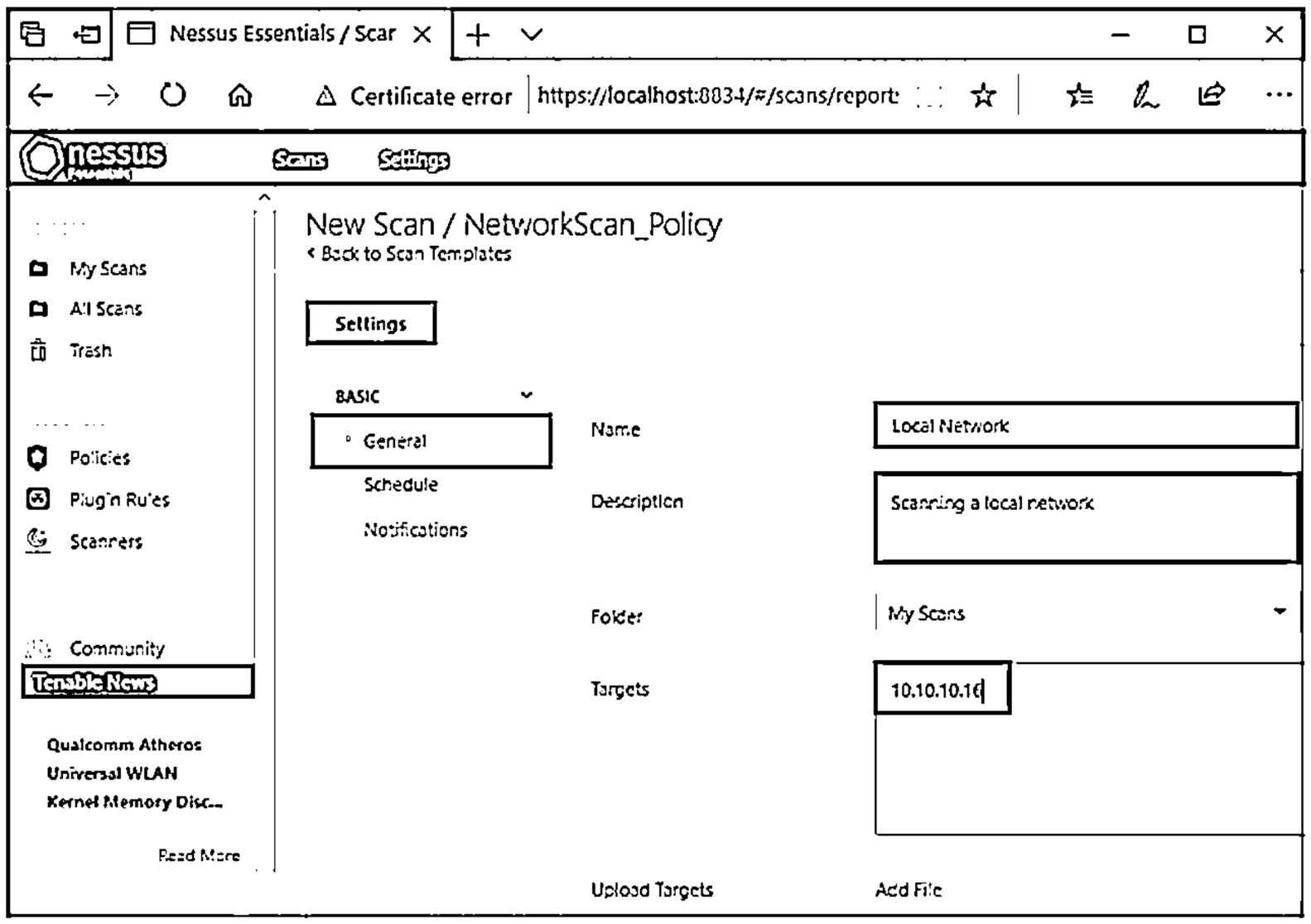


Figure 2.2.25: Configuring the basic settings in the scans window

TASK 2.6

Launch a Network Scan

30. Click **Schedule** settings; ensure that the **Enabled** switch is turned off. Click the drop-down icon next to the **Save** button and select **Launch** to start the scan.

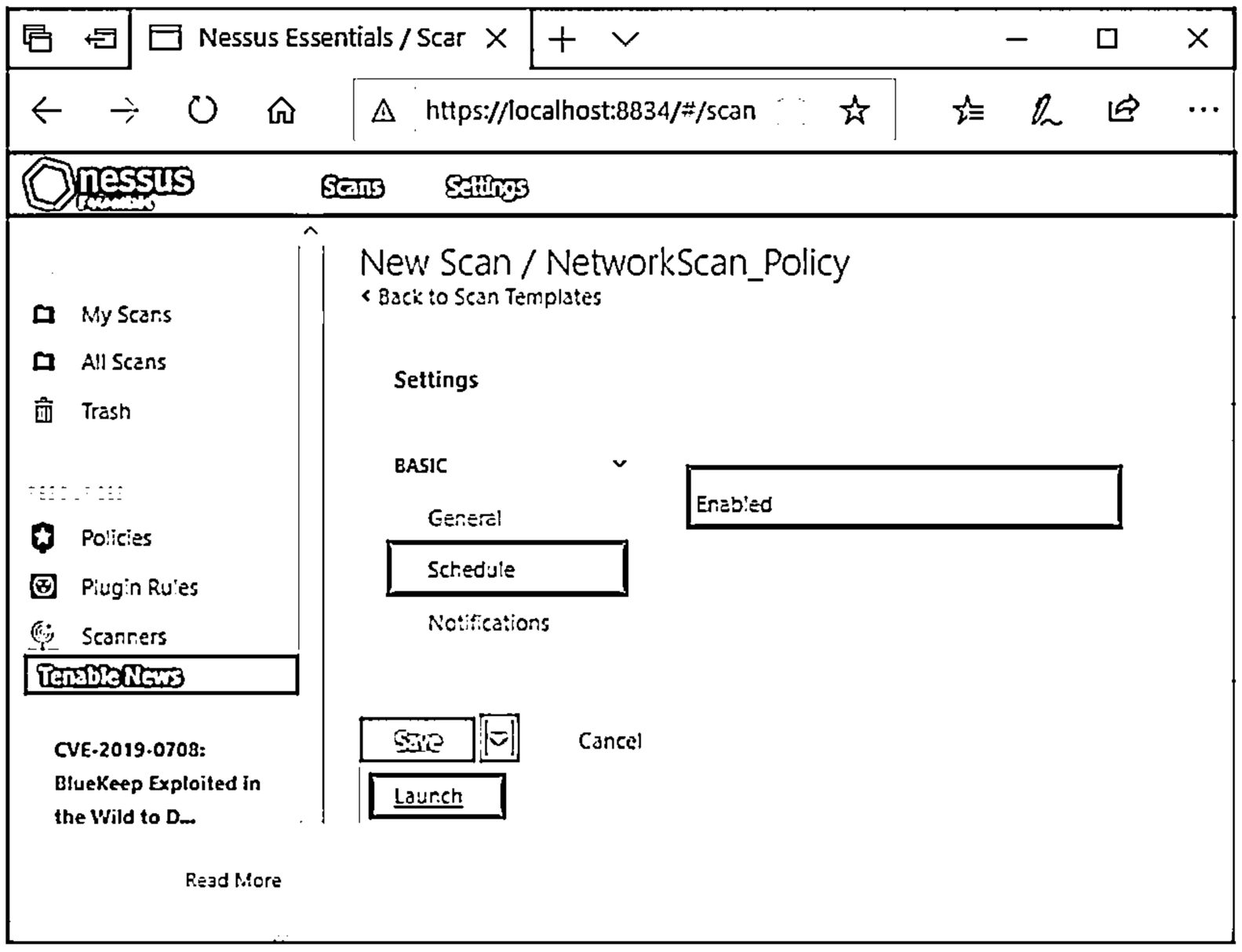


Figure 2.2.26: Setting a scan schedule

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

31. The **Scan saved and launched successfully** notification pop-up appears. The scan is launched, and Nessus begins to scan the target.

Figure 2.2.27: Local Network scanning

32. After the completion of the scan: click **Local Network** to view the detailed results.

TASK 2.7

Examine the Vulnerabilities

33. The **Local Network** window appears, displaying the summary of target hosts, as well as the **Scan Details** and **Vulnerabilities** categorization under the **Hosts** tab, as shown in the screenshot.

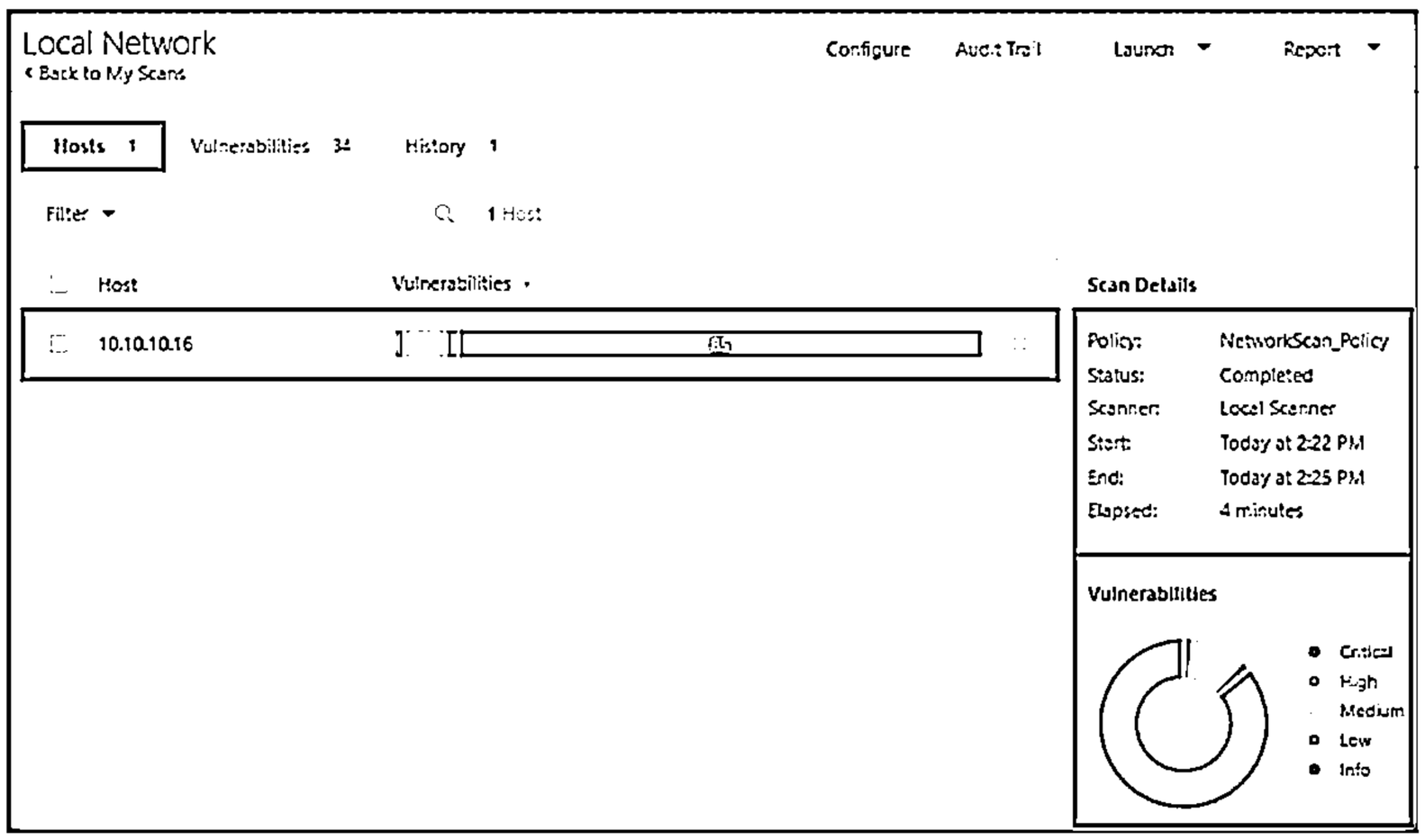


Figure 2.2.28: Hosts Summary window

34. Click the **Vulnerabilities** tab, and scroll down to view all the vulnerabilities associated with the target machine.

Note: The list of vulnerabilities may differ in your lab environment.

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

35. Click these vulnerabilities to view detailed reports about each. For instance, in this lab, we are selecting the first vulnerability in the list, that is, **SNMP (Multiple Issues)**.

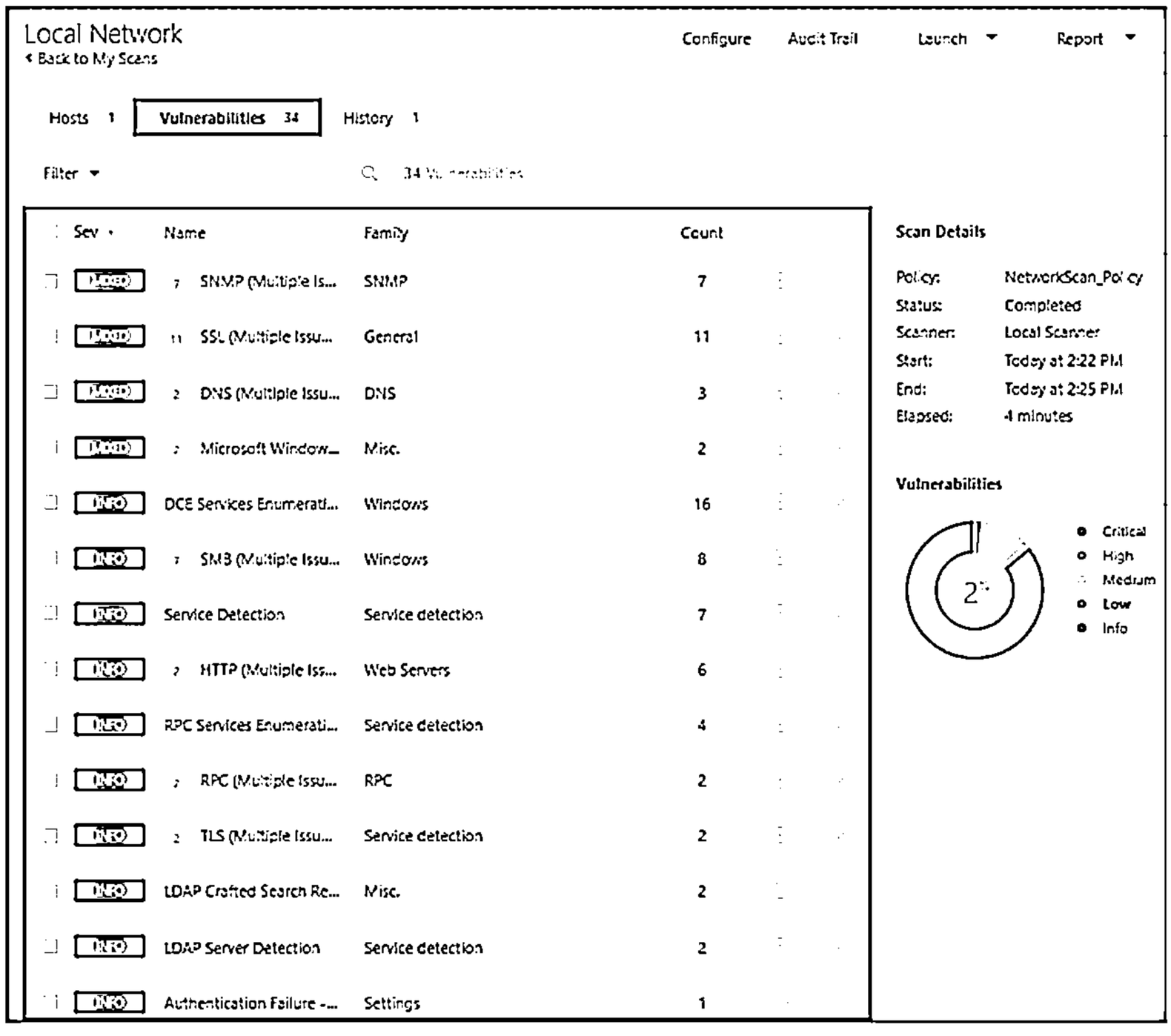


Figure 2.2.29: Vulnerability Summary window

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

36. The **Local Network / SNMP (Multiple Issues)** window appears, displaying multiple issues in SNMP service. Click on any issue (here, **SNMP Agent Default**) to view its detailed information.

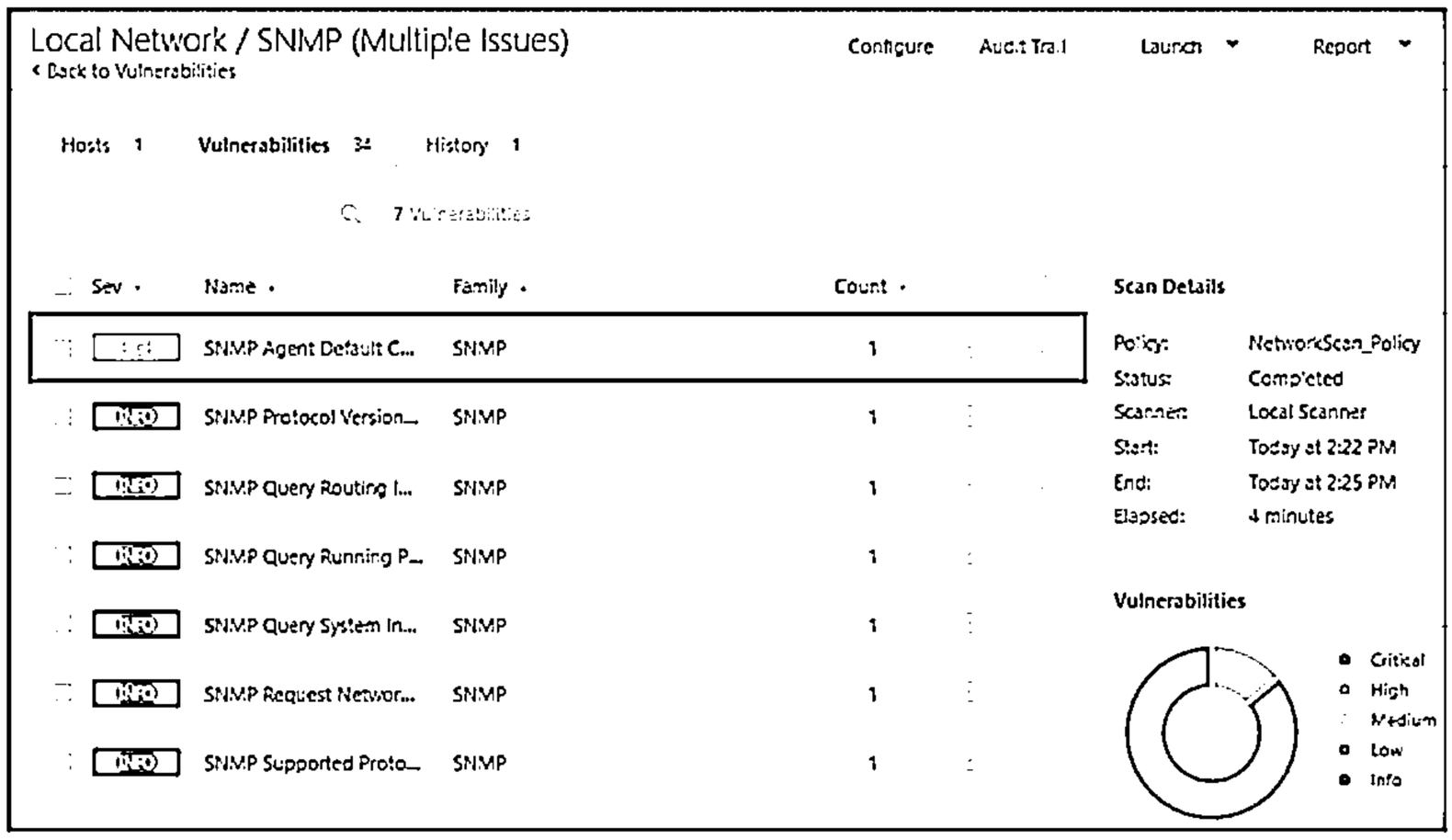


Figure 2.2.30: List of issues in SNMP

37. The report regarding selected vulnerability **SNMP Agent Default Community Name (public)** appears with detailed information such as plugin details, risk information, vulnerability information, reference information and the solution, and output, as shown in the screenshot.

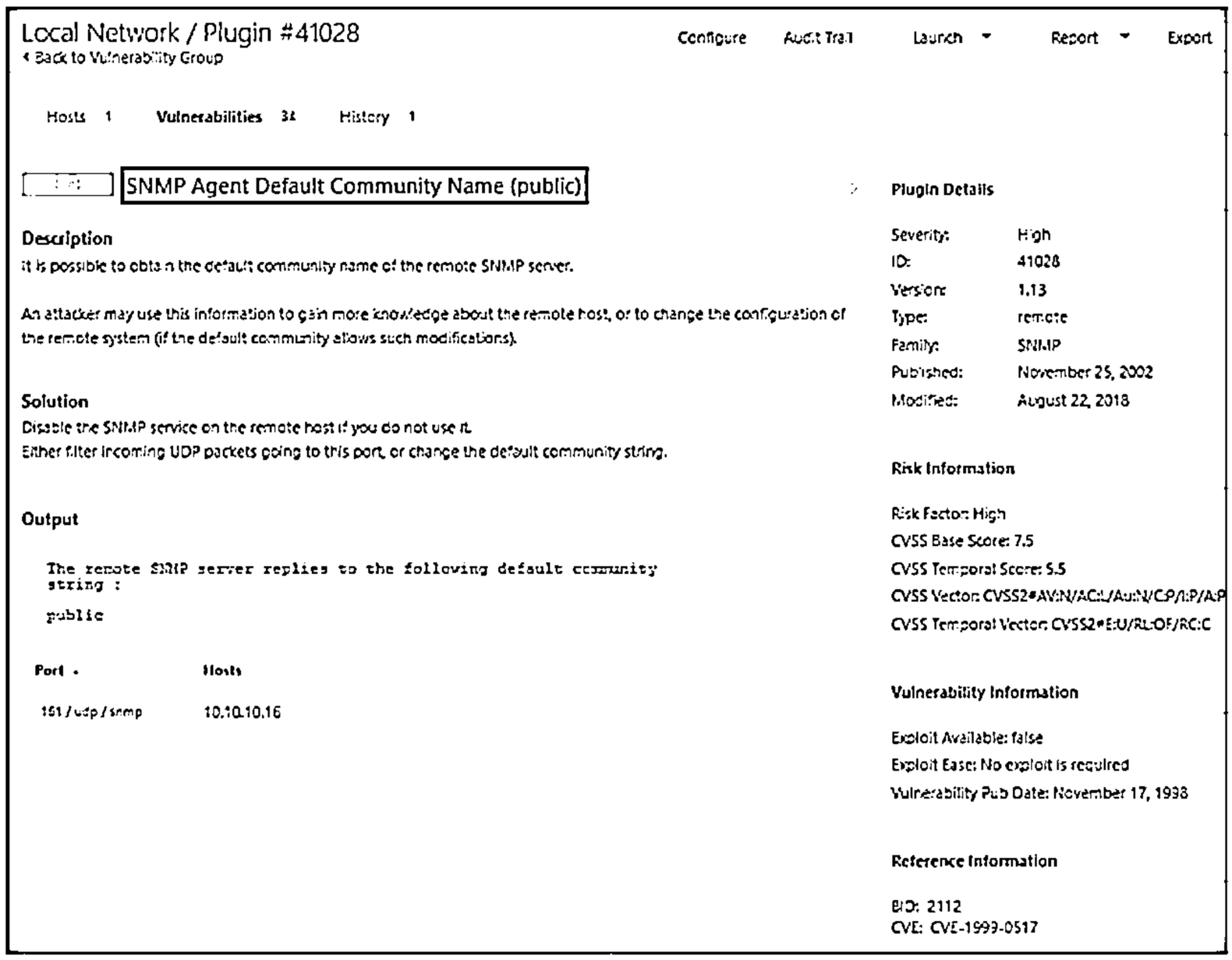


Figure 2.2.31: Vulnerability report

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

38. On completing the vulnerability analysis, click **Scans**, and then click the recently performed scan (here, **Local Network**).

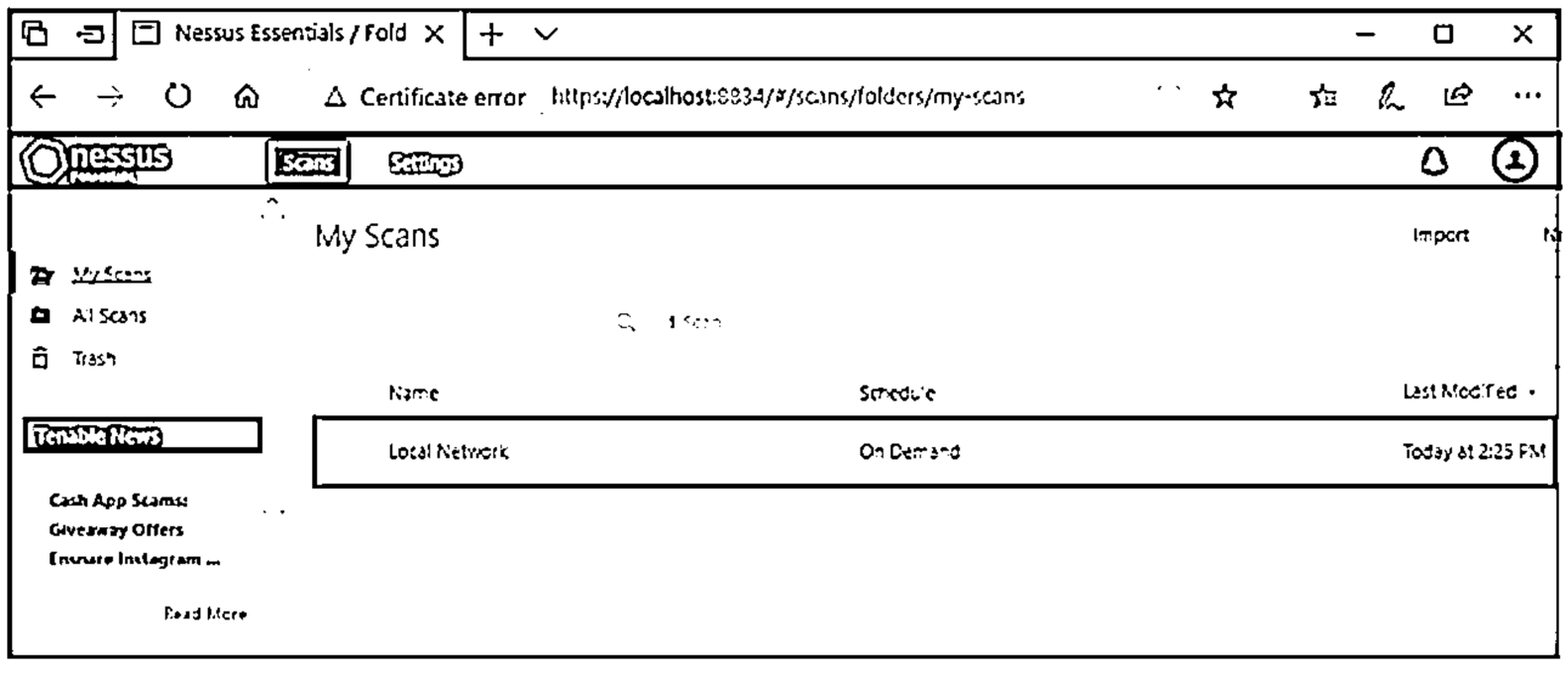


Figure 2.2.32: Selecting a Local Network Scan

39. In the **Local Network** window, click the **Report** tab from the top-right corner, and choose a file format (here, **HTML**) from the drop-down list. By downloading a report, you can access it anytime, instead of logging in to Nessus again and again.

TASK 2.8

Generate a Vulnerability Report

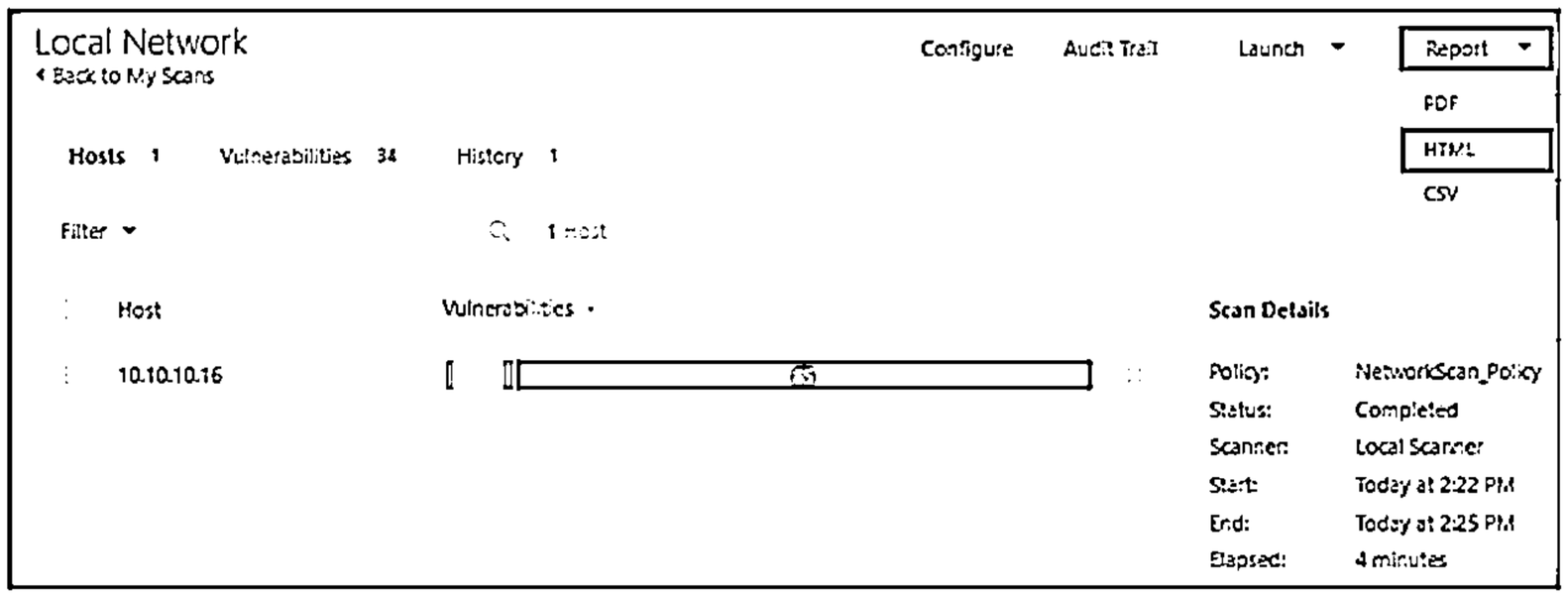


Figure 2.2.33: Exporting Report to HTML Format

40. The **Generate HTML Report** pop-up appears: leave the **Report** type option on default (**Executive Summary**). Click **Generate Report** to download the report.

Note: If the **What do you want to do with Local_Network_5cfvy7.html?** pop-up appears, click **Save**.

Note: The file name might differ in your lab environment.

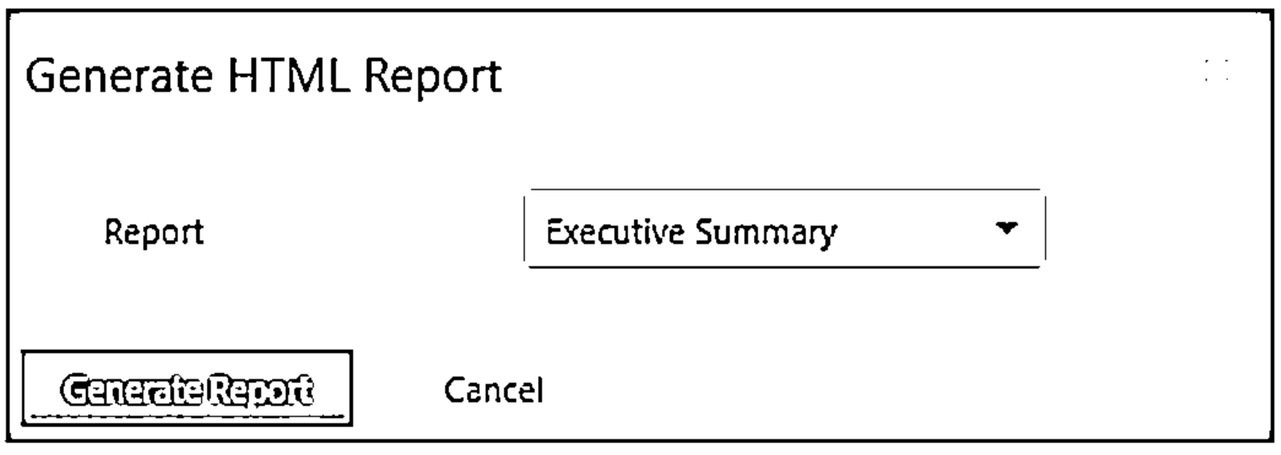


Figure 2.2.34: Export as HTML window appears

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

41. Once the download is finished, a pop-up appears at the bottom of the browser; click **Open**.
42. If the **How do you want to open this file?** pop-up appears, choose any browser (here, **Firefox**) to view the downloaded HTML file.

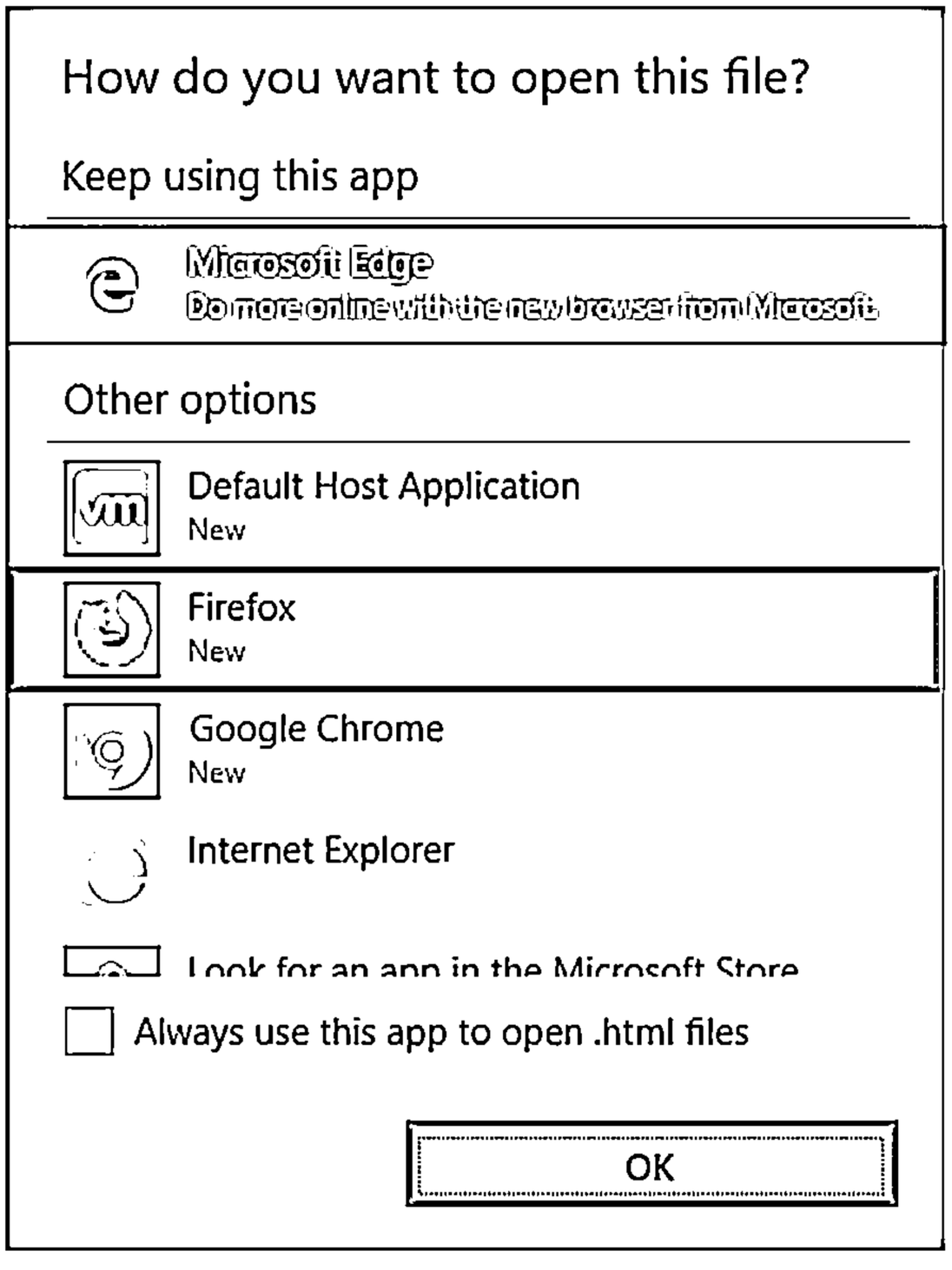


Figure 2.2.35: Choosing a browser to view the HTML

43. The Nessus scan report appears in the **Firefox** web browser, as shown in the screenshot.

Note: Screenshots might differ in your lab environment.

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

44. You can click the **Expand All** option to view the detailed scan report.

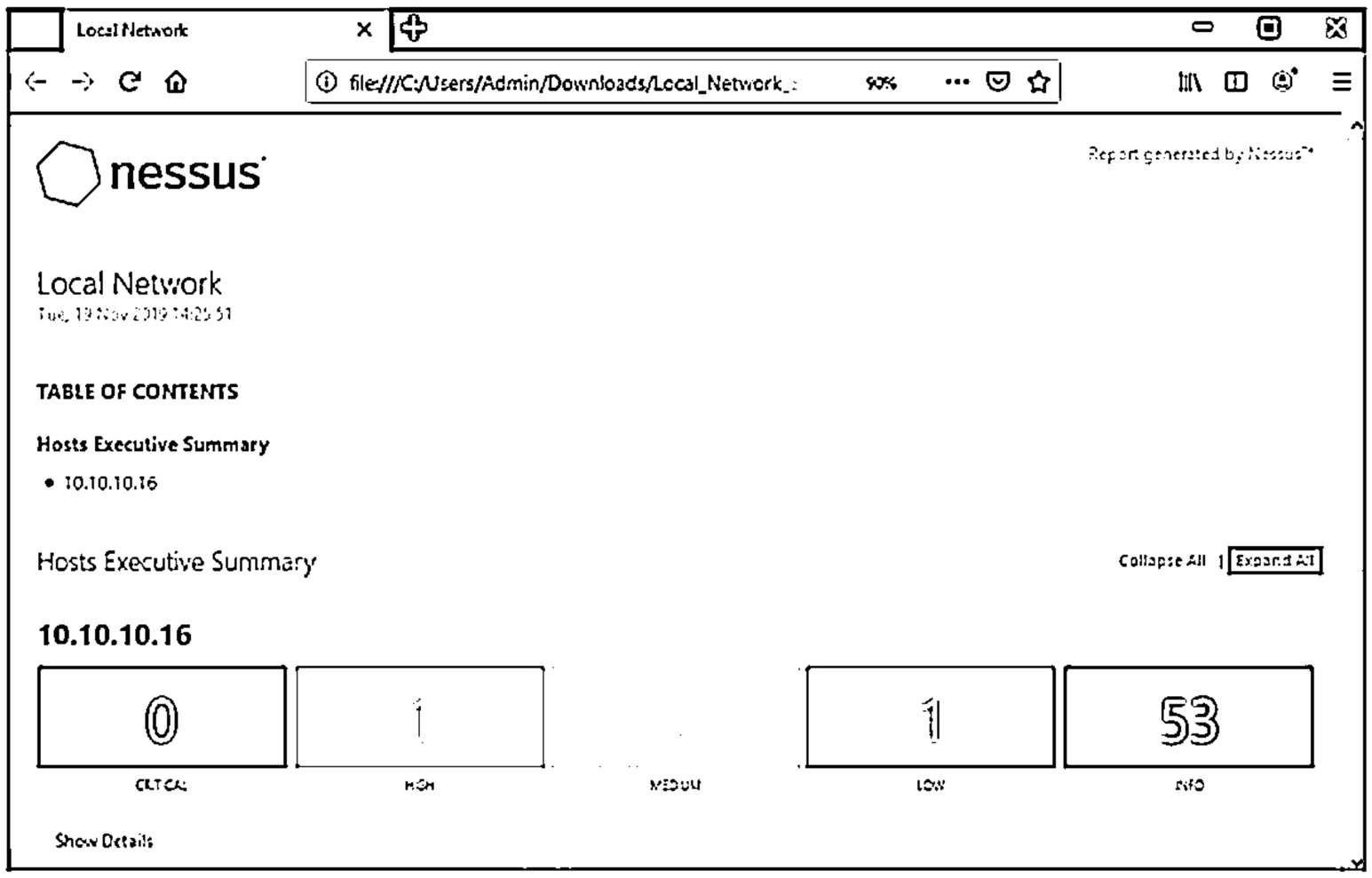


Figure 2.2.36: Vulnerability Report Displayed in HTML Format

45. A list of discovered vulnerabilities appears. You can further click on plugins (here, **41028**) to view more detailed information on the vulnerability.

Note: The results might differ in your lab environment.

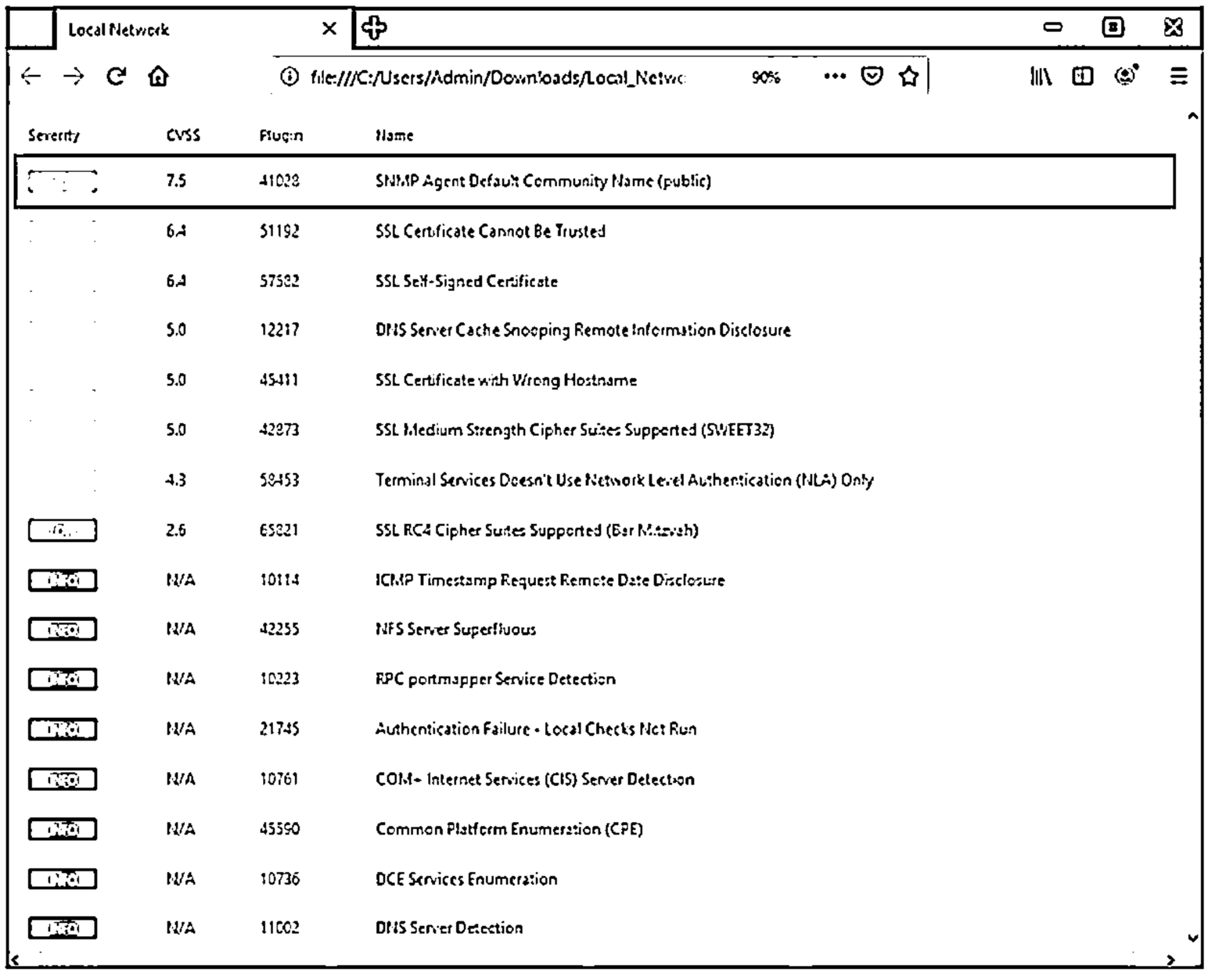


Figure 2.2.37: Viewing a Vulnerability in the Report

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

46. The selected plugin details are displayed, as shown in the screenshot.

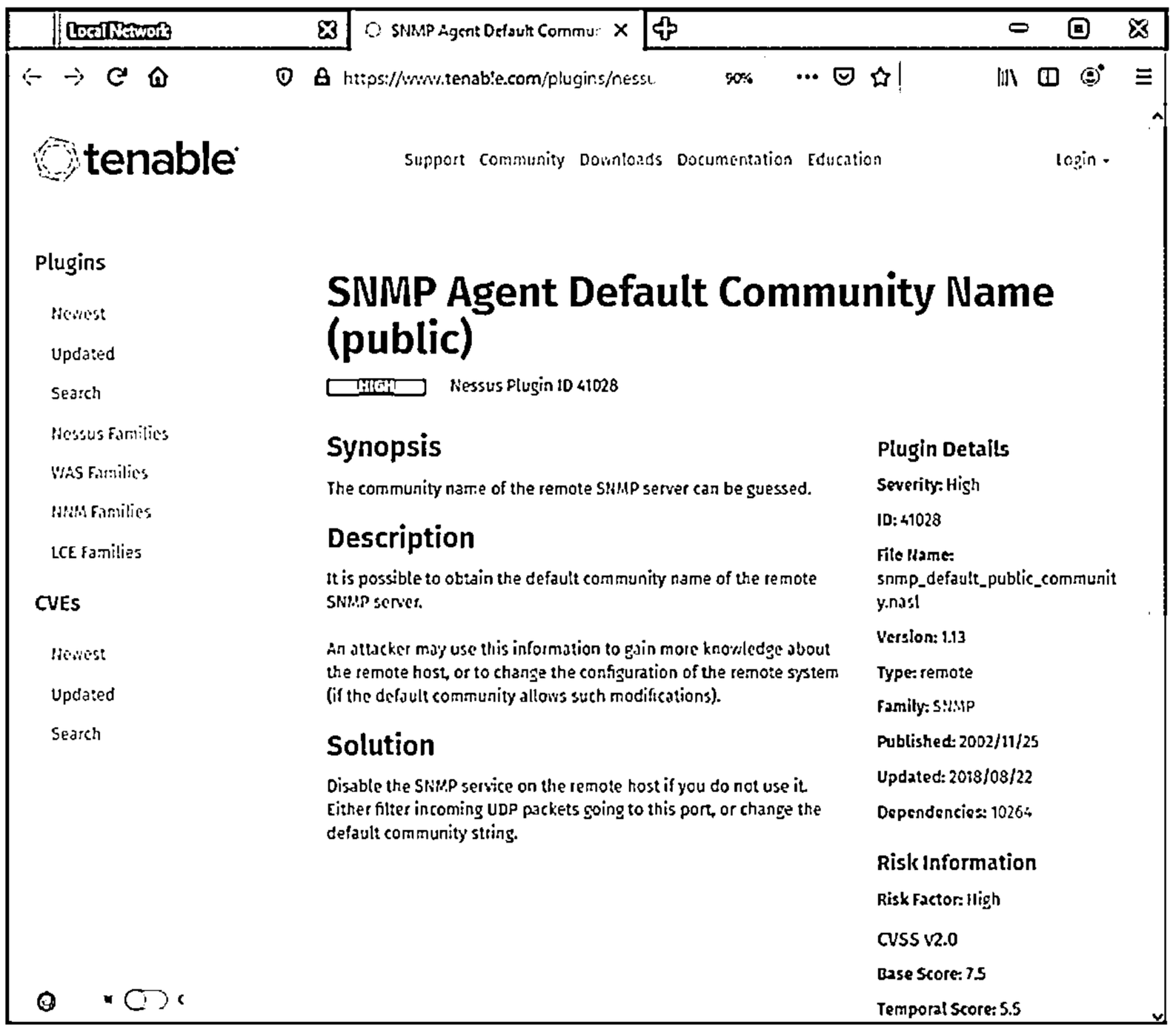


Figure 2.2.38: Details of the Selected Vulnerability

47. In this way, you can select a vulnerability of your choice to view the complete details.

48. Once the vulnerability analysis is done, switch back to **Microsoft Edge** where Nessus is running and click **Admin → Sign Out** in the top-right corner.

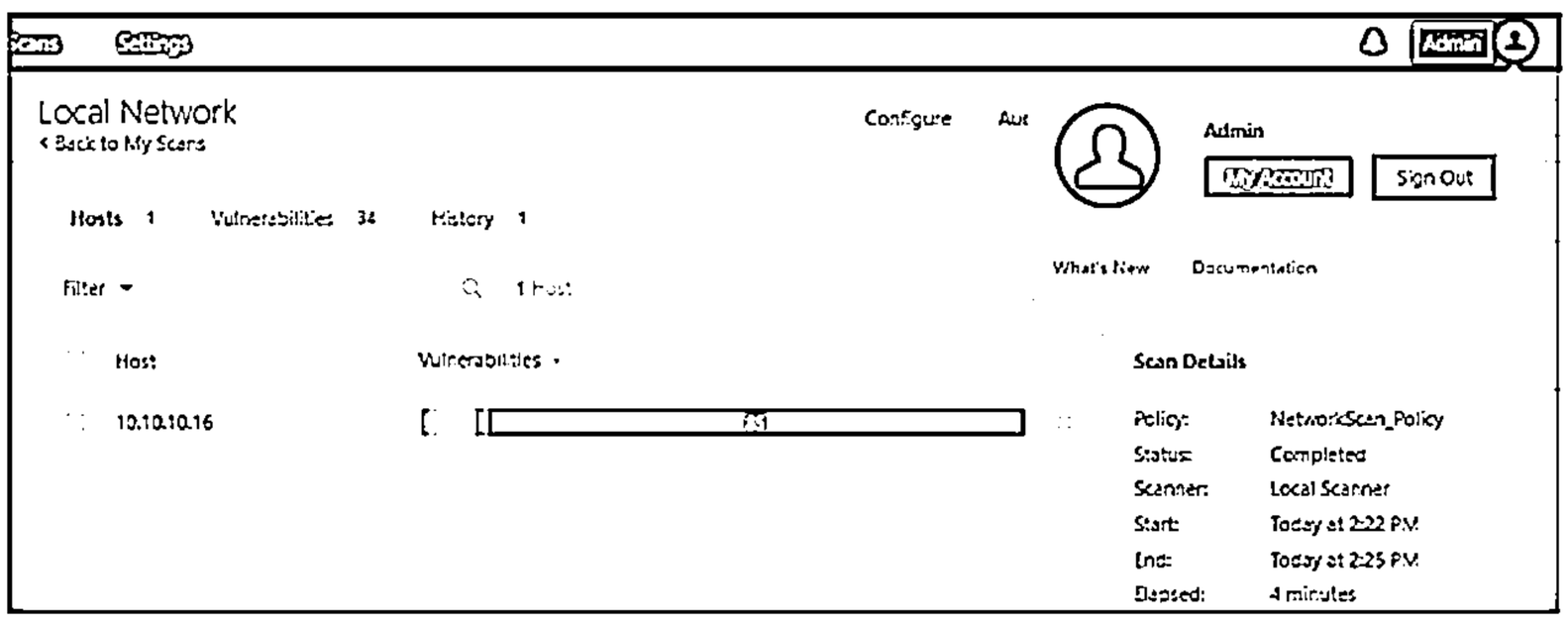


Figure 2.2.39: Signing out of Nessus

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

49. Once the session is successfully logged out, a **Signed out successfully. Goodbye, admin** notification appears.

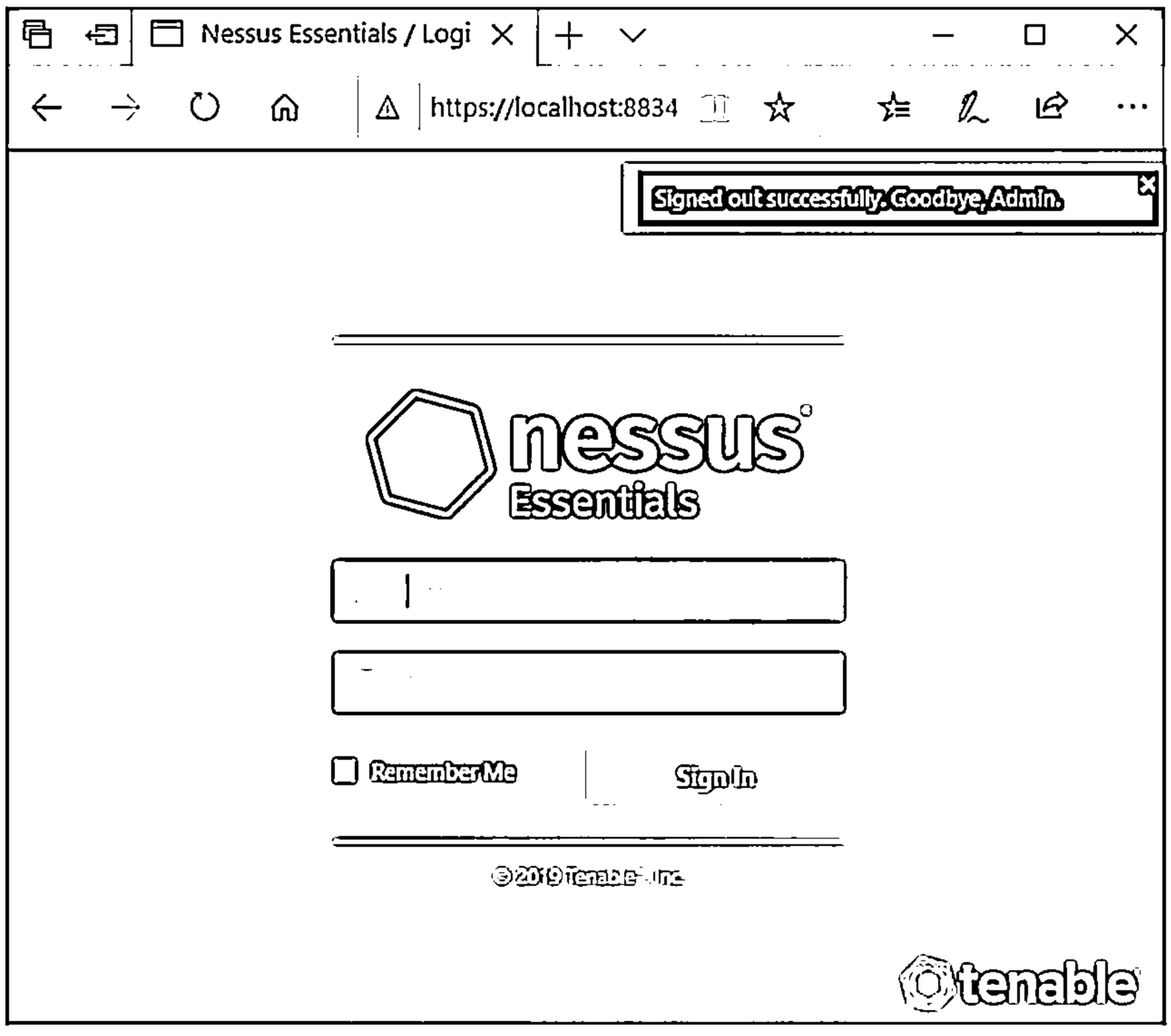


Figure 2.2.40: Signed out successfully

50. This concludes the demonstration of performing vulnerability assessment using Nessus.
51. Close all open windows and document all the acquired information.
52. Turn off the **Windows 10** virtual machine.

TASK 3 — Perform Vulnerability Scanning using GFI LanGuard

Here, we will use GFI LanGuard to perform vulnerability scanning on the target system.

1. Turn on the **Windows Server 2019** virtual machine.

Note: Ensure that the **Windows Server 2016** virtual machine is also turned on.

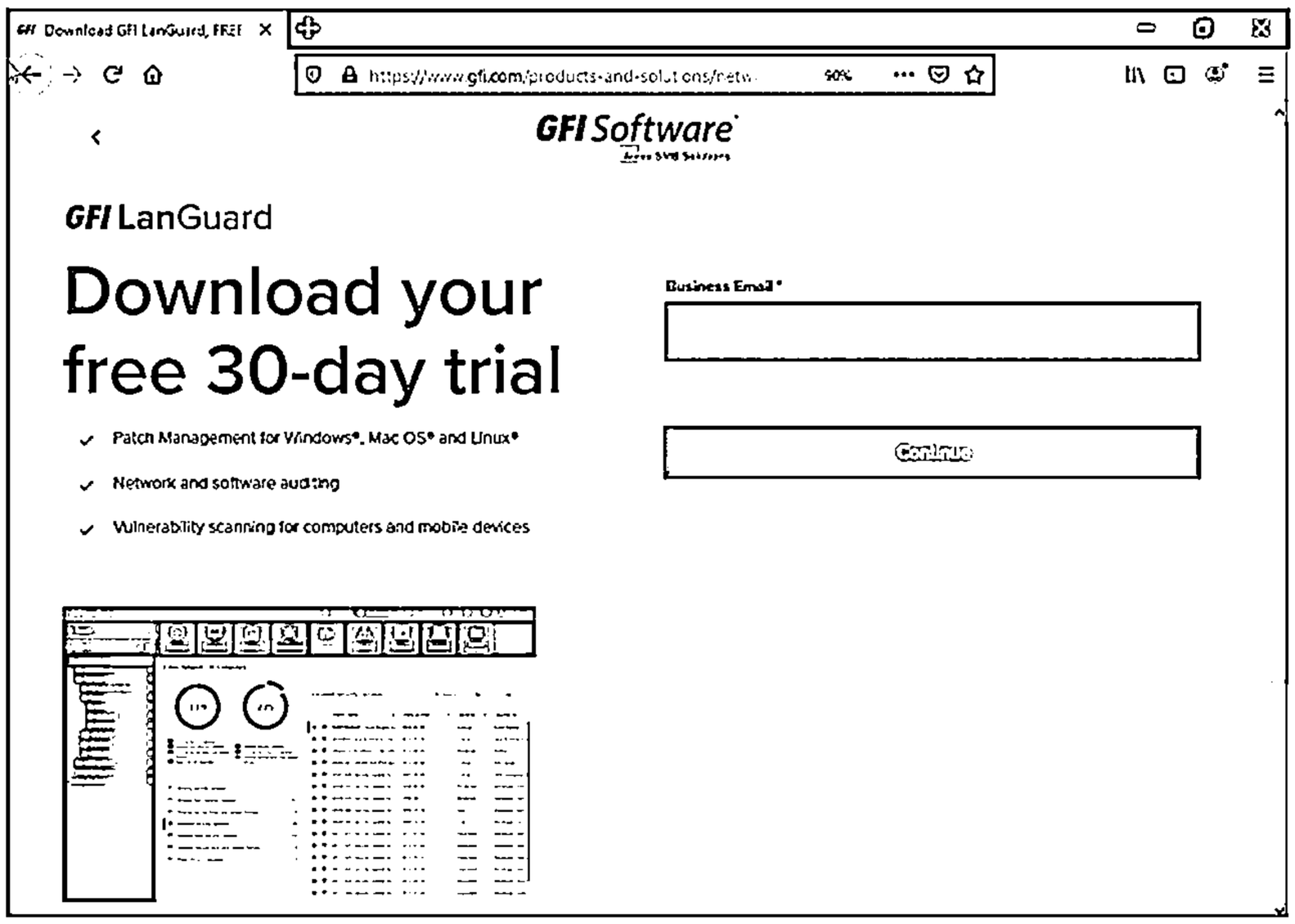
2. In the **Windows Server 2019** virtual machine, log in with the credentials **Administrator** and **Pa$$w0rd**.

TASK 3.1 — Register and Download GFI LanGuard

3. Launch any web browser (here, **Mozilla Firefox**), type the URL **https://www.gfi.com/products-and-solutions/network-security-solutions/gfi-languard/download** in the address bar and press **Enter**.

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

4. The **GFI LanGuard** registration page appears. Enter your business email under the **Business Email** field and click **Continue**.



GFI LanGuard scans, detects, assesses, and rectifies security vulnerabilities in your network and connected devices. It scans the network and ports to detect, assess, and correct security vulnerabilities, with minimal administrative effort.

Figure 2.3.1: GFI LanGuard Registration page

5. On the next page, enter the required details and select the **I agree to GFI Software terms of service and privacy policy and consent to GFI Software to process data** checkbox and click **Start my free trial**.

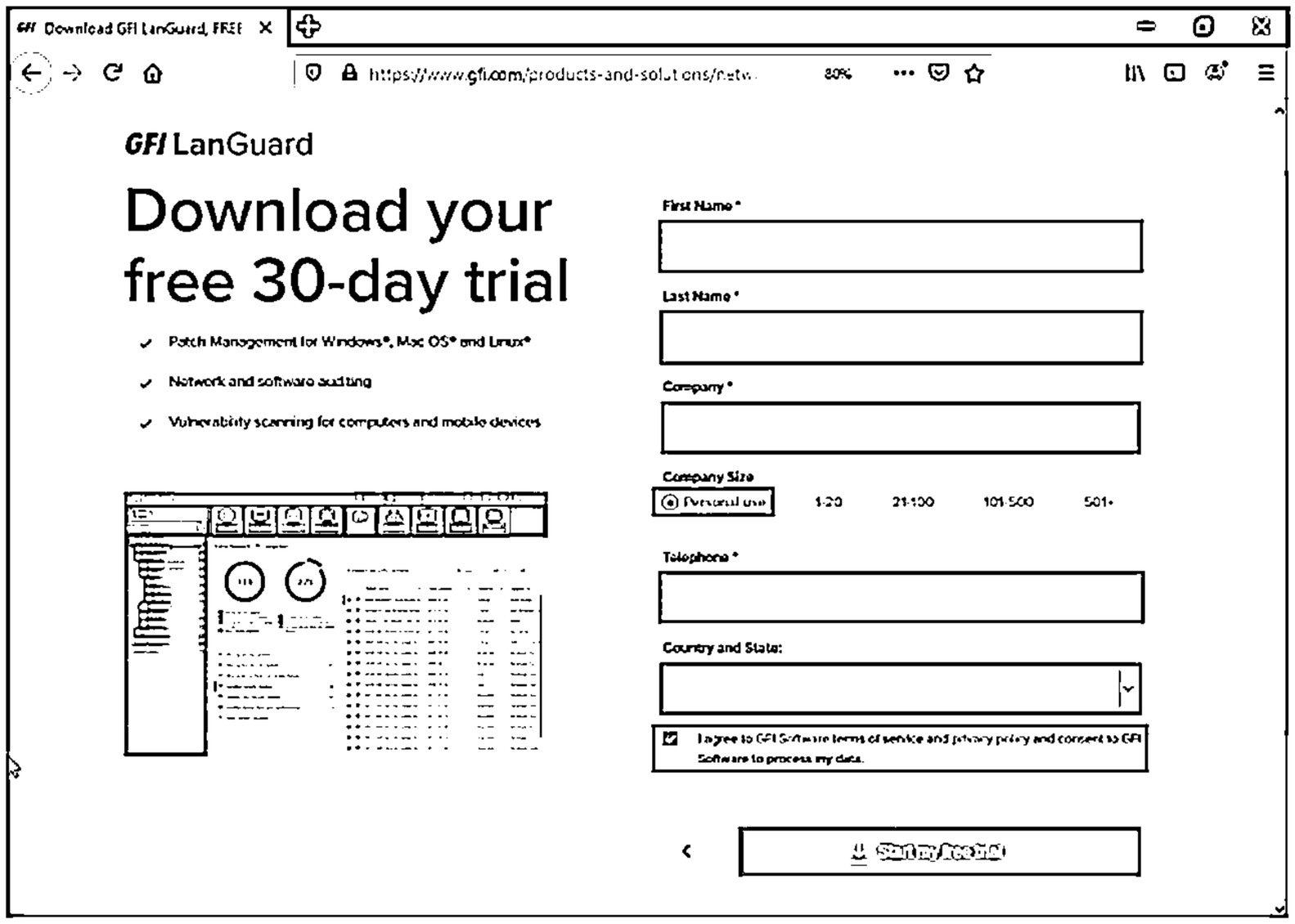


Figure 2.3.2: GFI LanGuard Download page

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

6. The **Download the latest version of GFI LanGuard** page appears; click the **Download Trial** button.

GFI LanGuard scans your OSes, virtual environments, and installed applications through vulnerability check databases. It enables you to analyze the state of your network security, identify risks, and address how to take action before it is compromised.

Note: The **Opening languard.exe** pop-up appears; click **Save File.**

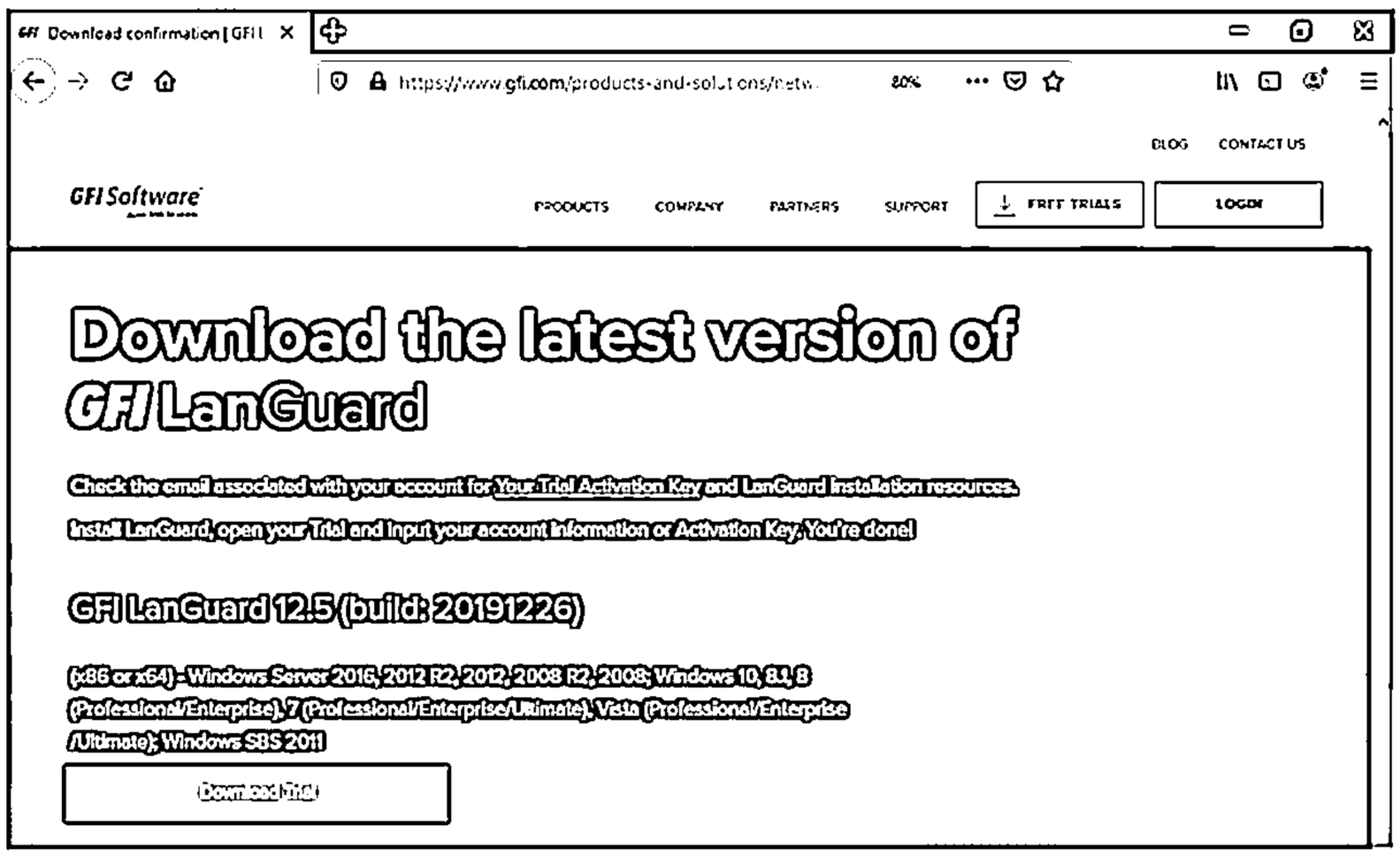


Figure 2.3.3: Complete Registration

TASK 3.2

Install GFI LanGuard

7. Now, navigate to the download location (here, **Downloads**) and double-click **languard.exe** to install.

Note: If the **User File - Security Warning** pop-up appears, click **Run**.

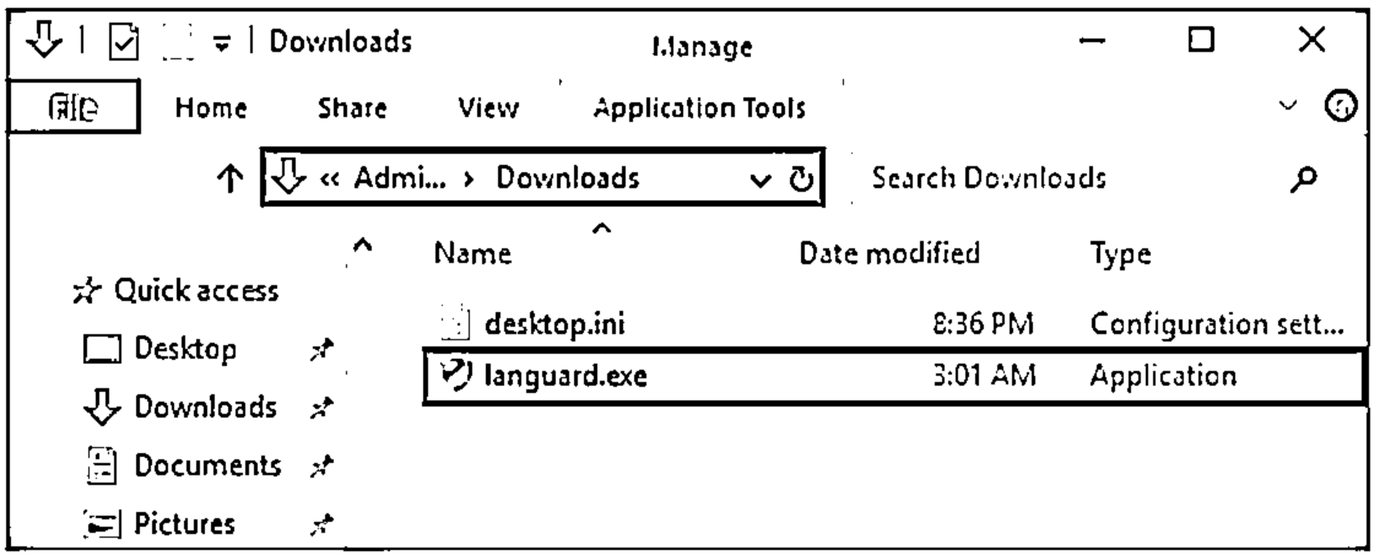


Figure 2.3.4: GFI LanGuard exe file

8. The **GFI LanGuard** dialog box appears; select preferred language (here, **English**) and click **OK**.

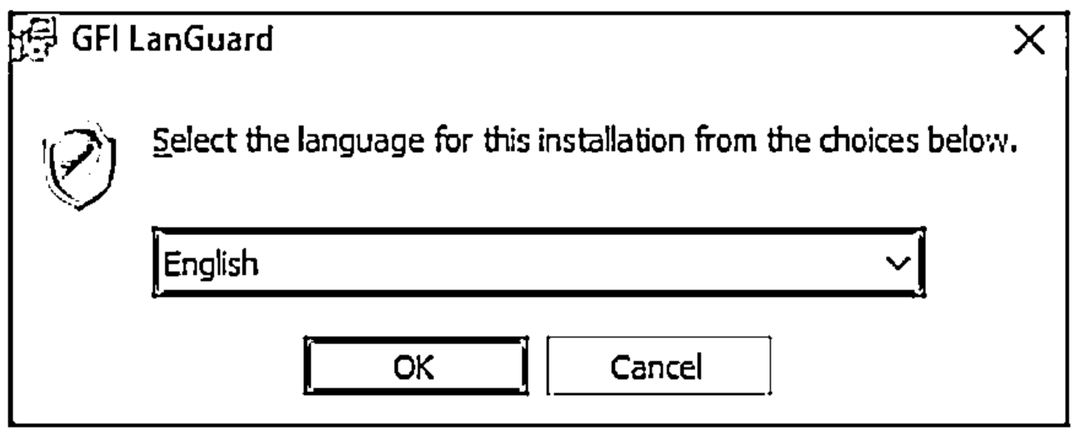


Figure 2.3.5: Selecting a language

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

9. The **GFI LanGuard** wizard appears with selected components for installation; click **Next** to proceed.

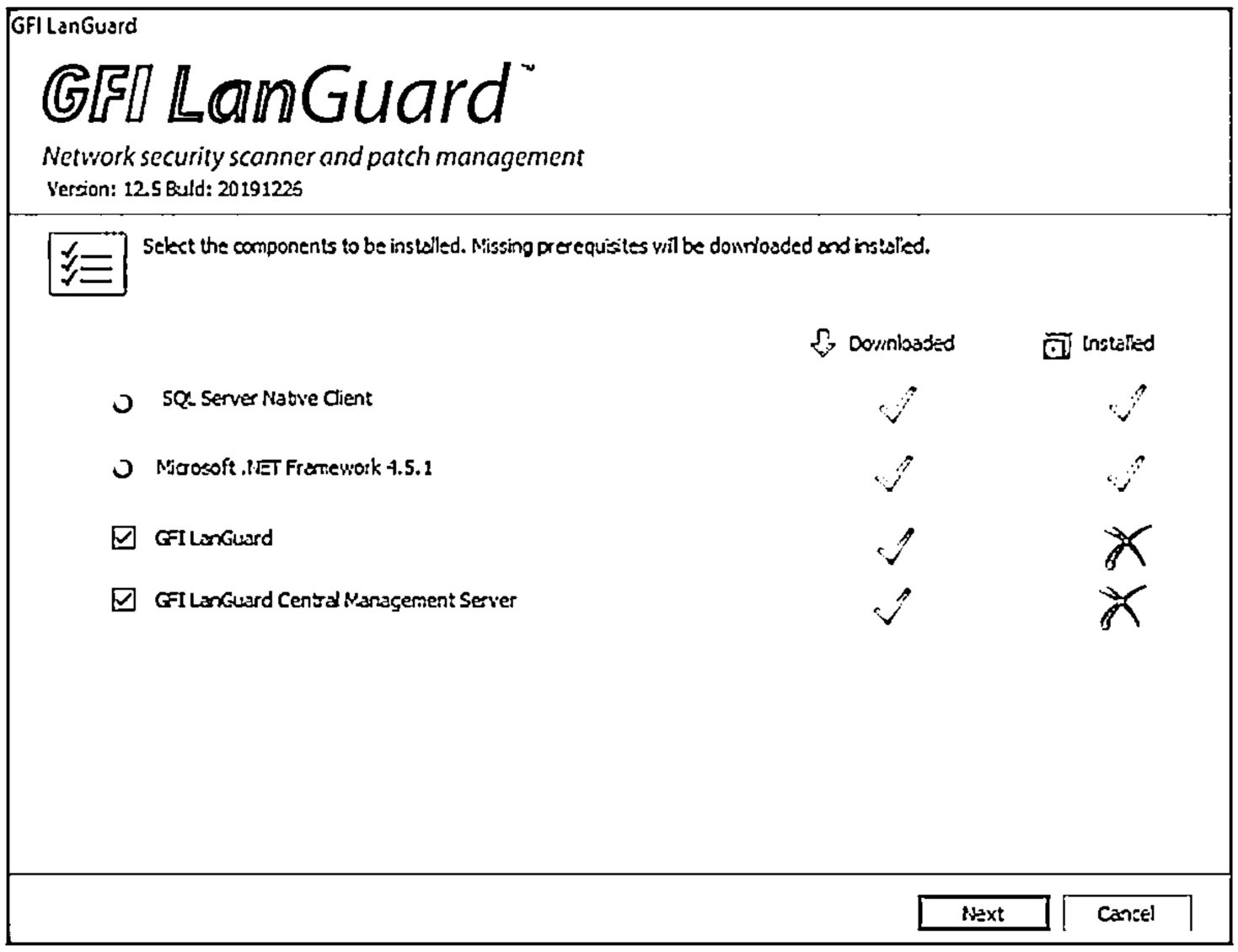


Figure 2.3.6: Installation wizard

10. The **Database Configuration** window appears. In the **SQL server name** field, type **.\SQLEXPRESS** and leave **SQL database name** as default. Ensure that the **Use Windows Authentication** checkbox is selected and click **OK**.

Note: The SQL server name might differ in your lab environment.

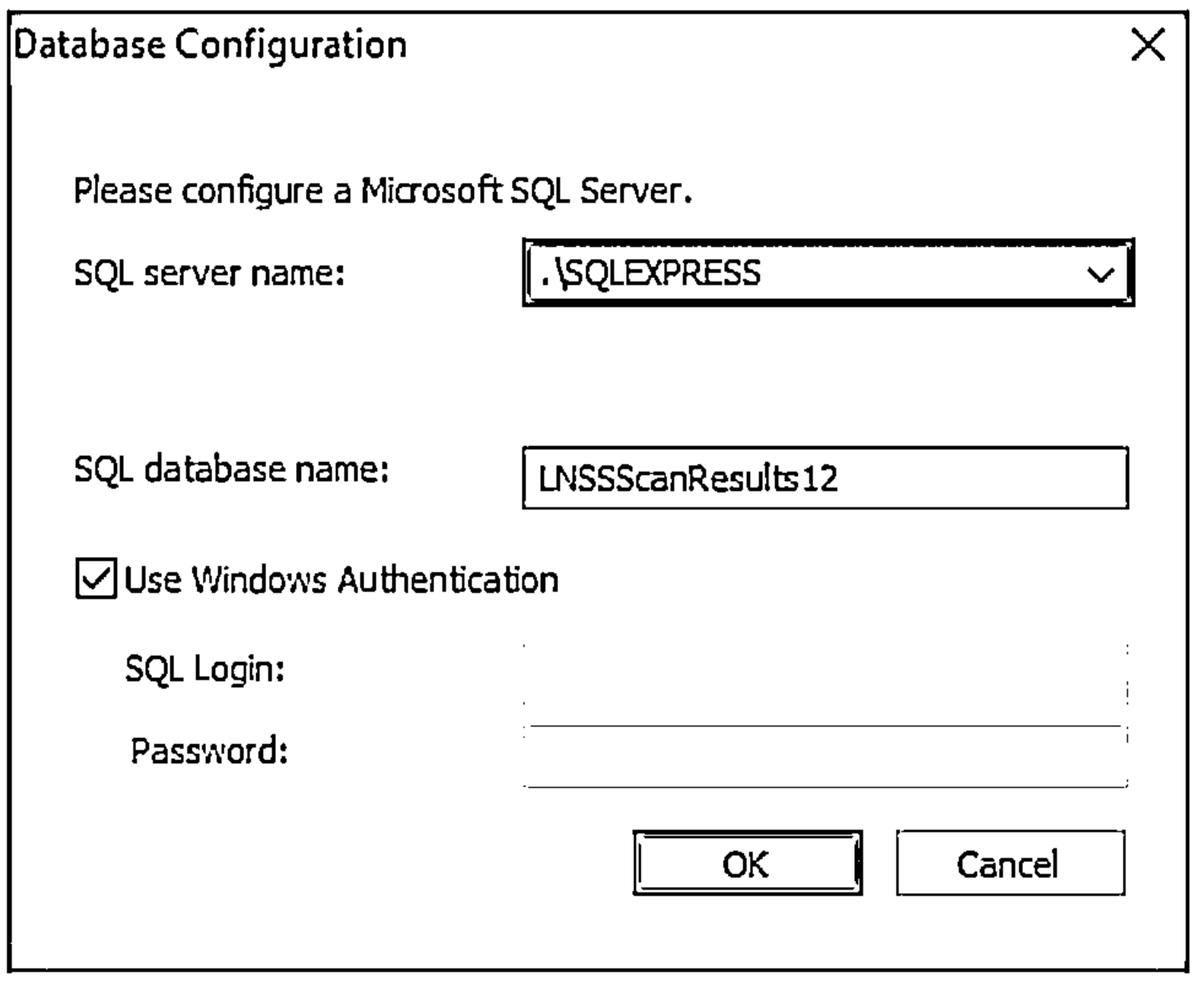


Figure 2.3.7: Database Configure window

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

11. Now, switch back to the **Mozilla Firefox** browser, open a new tab, and log in to your email account that you have given while registration.
12. Open an email from **GFI Downloads** and copy the activation key.

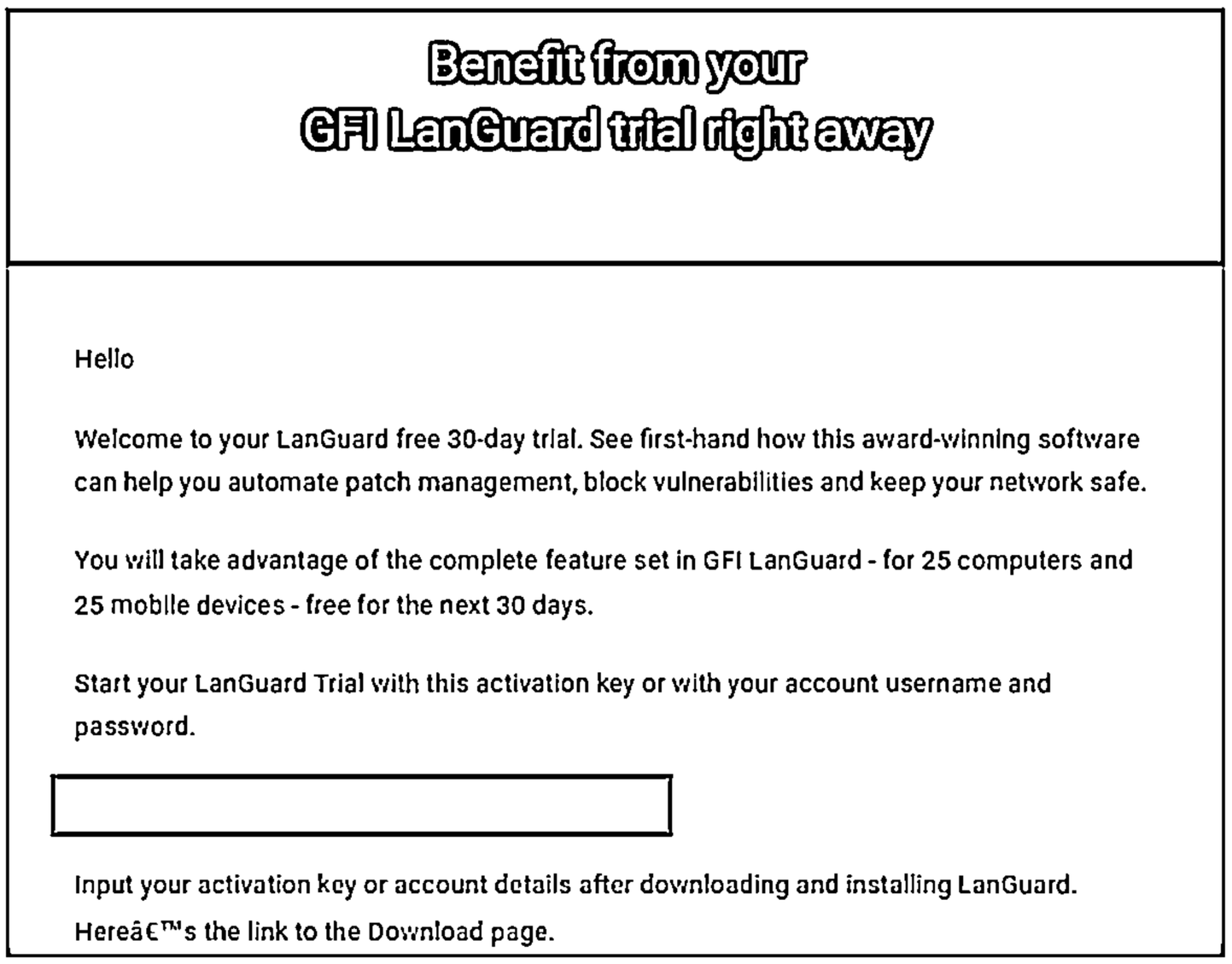


Figure 2.3.8: GFI LanGuard Trial Key

13. The **GFI LanGuard License Key** window appears. Paste the received activation key in the **Enter License Key** field and click **OK**.

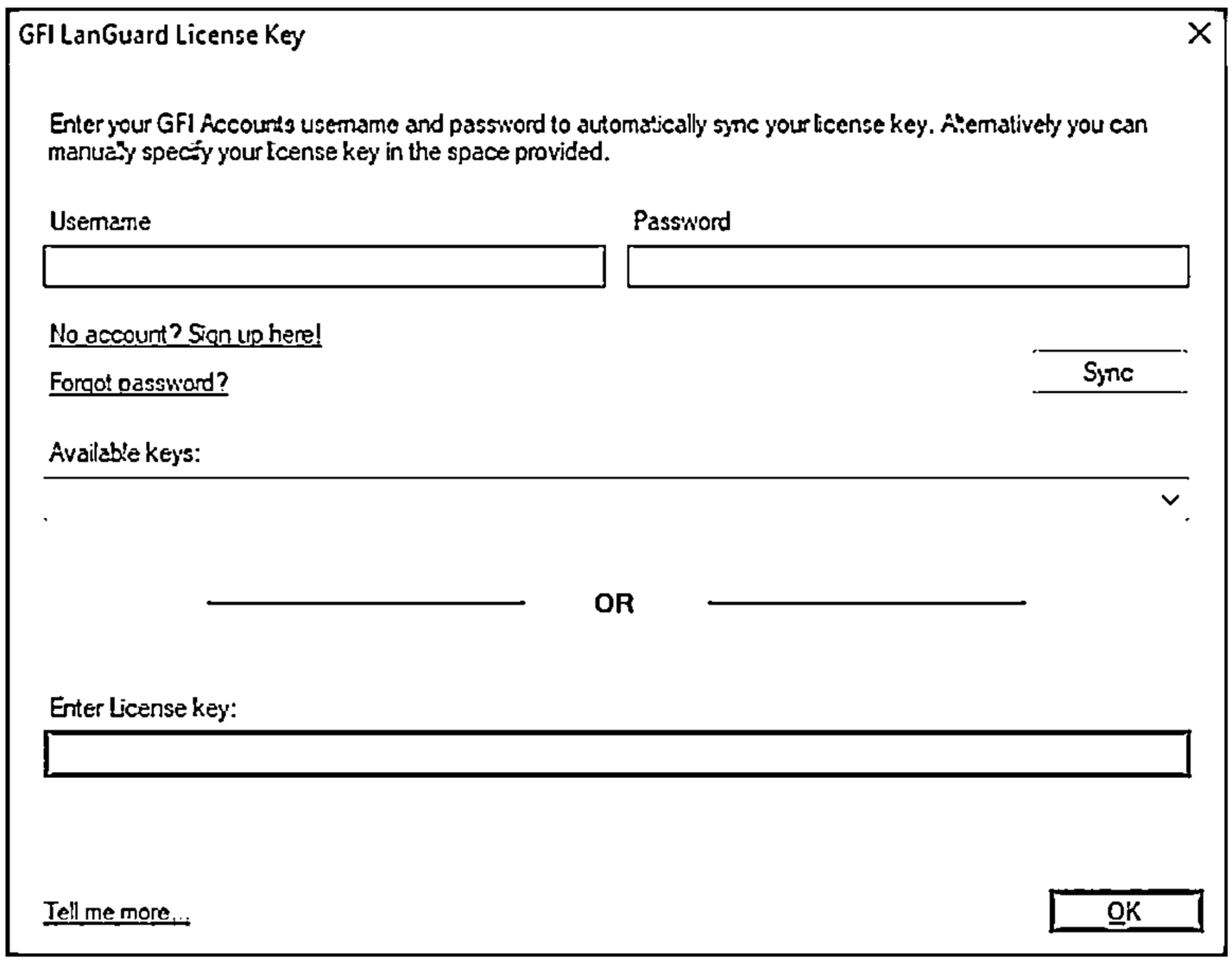


Figure 2.3.9: GFI LanGuard License window

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

14. GFI LanGuard starts installing after the completion of the installation; when the **GFI LanGuard Setup** window appears, click **Next**.

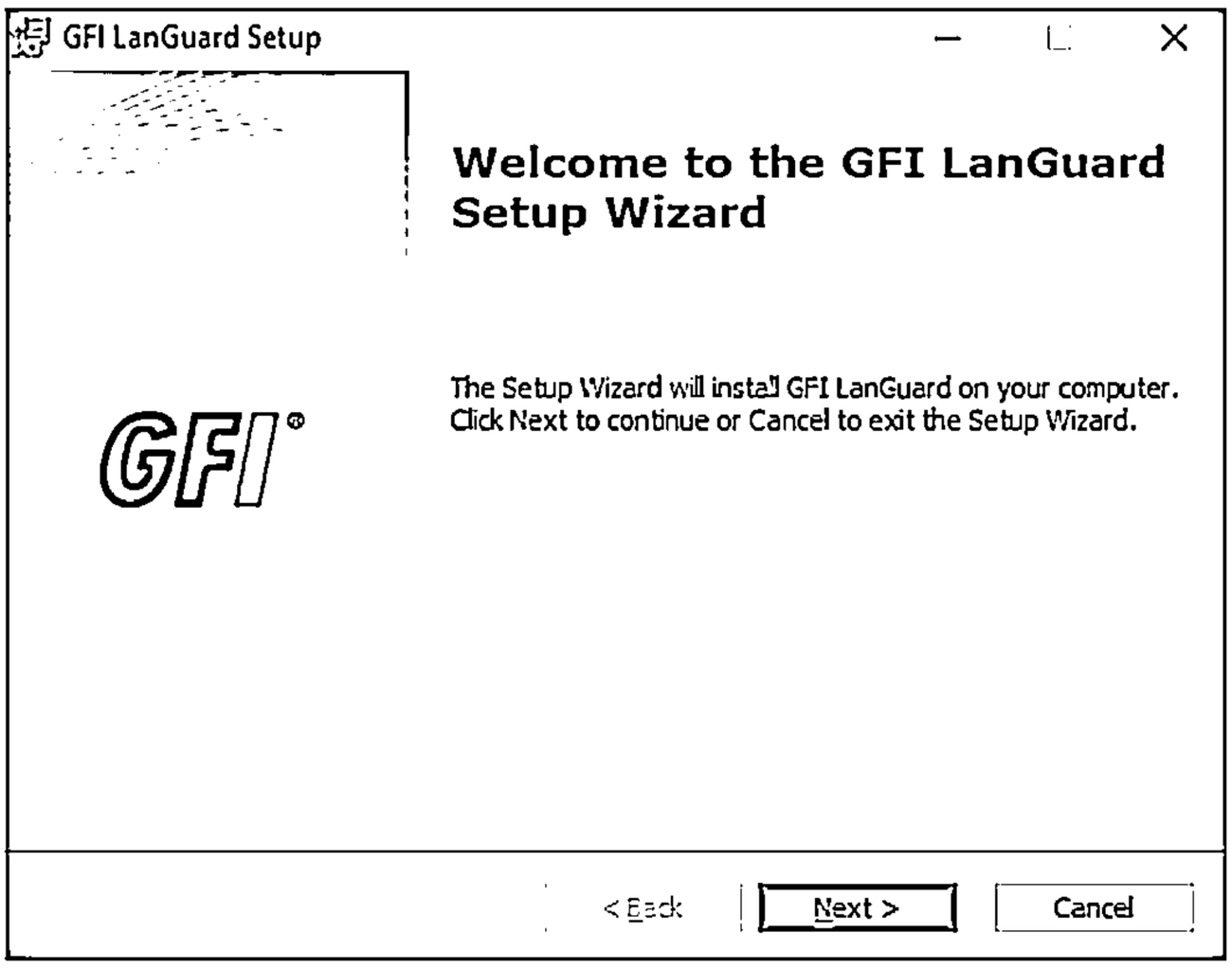


Figure 2.3.10: GFI LanGuard Setup window

15. The **End-User License Agreement** wizard appears; accept the terms and click **Next**.
16. In the **Attendant service credentials** wizard, leave the **Name** field as default (here, **SERVER2019\Administrator**) and enter the **Password** of the administrator account (here, **Pa$$w0rd**); then, click **Next**.

Note: The **Name** field might differ in your lab environment.

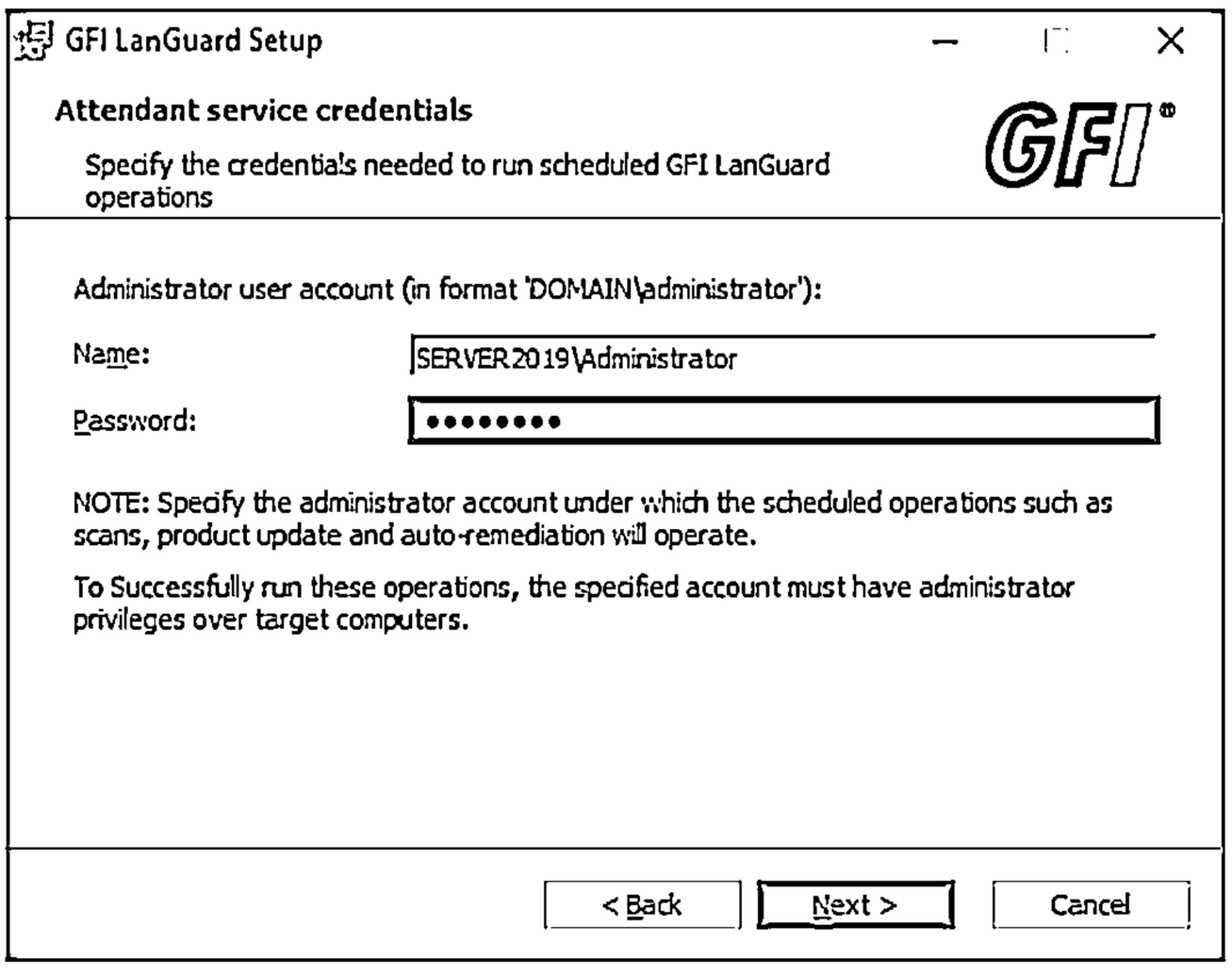


Figure 2.3.11: GFI LanGuard Attendant service credentials section

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

17. In the **Choose Destination Location** wizard, leave the **Folder** location set to default and click **Install**.

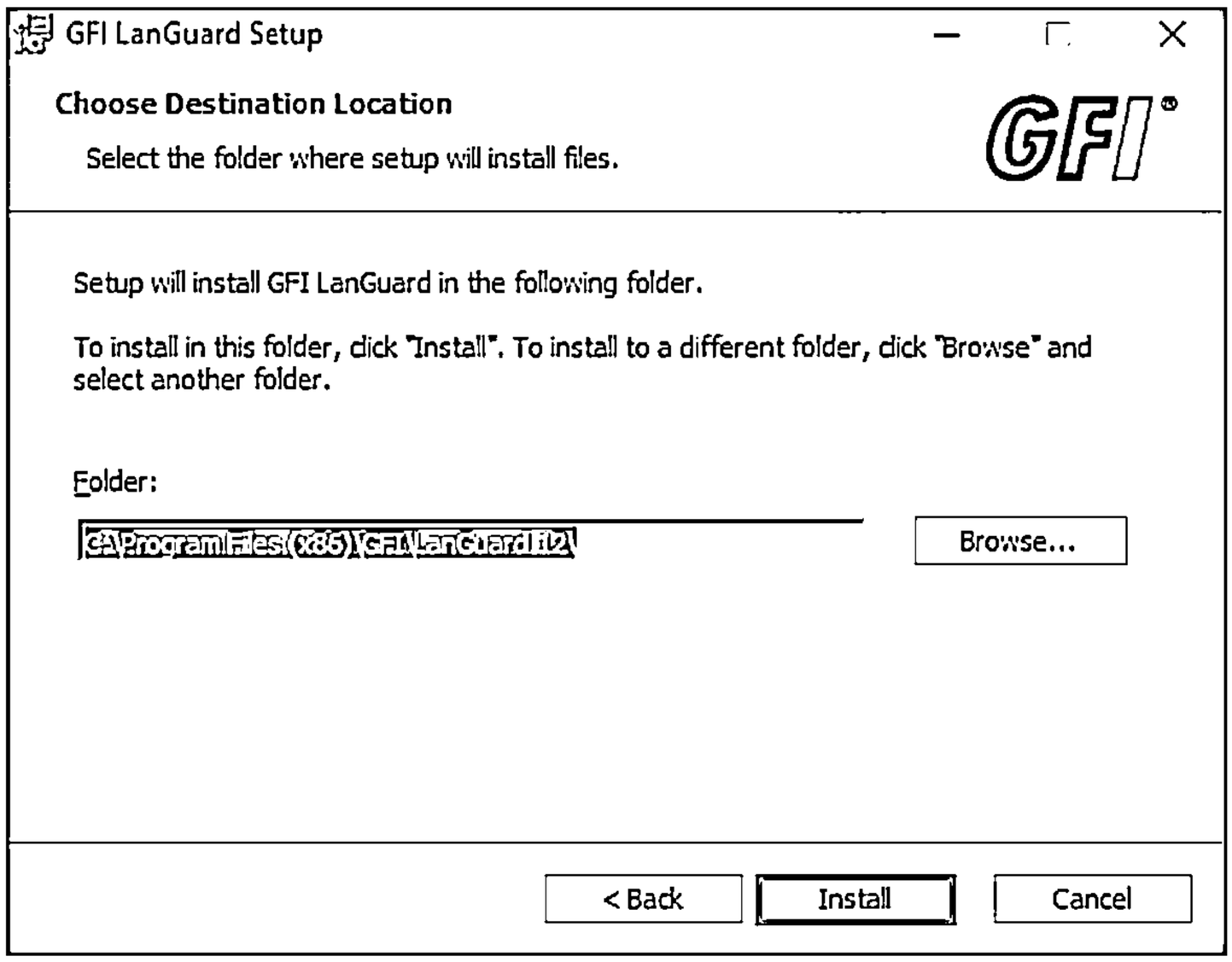


Figure 2.3.12: Choosing a folder location

18. The **Installing GFI LanGuard** wizard appears. After the completion of installation, the **GFI LanGuard Central Management Server Setup** window appears; then, click **Next**.

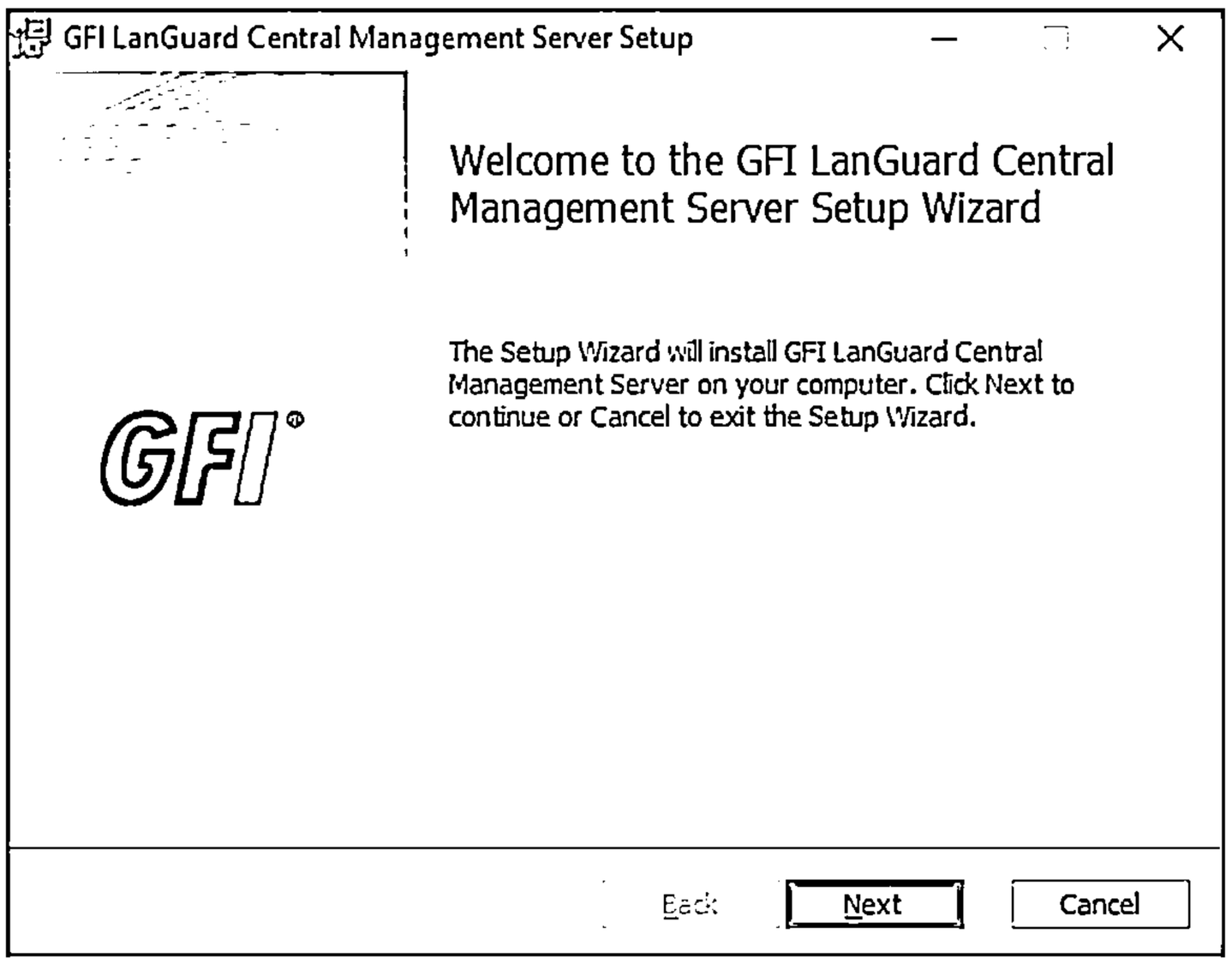


Figure 2.3.13: GFI LanGuard Central Management Server Setup window

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

19. In the **Service logon information** wizard, leave the **User Name** field (Administrator user account) set to its default, enter the **Password** of the administrator account (here, **Pa$$w0rd**), and click **Next**.

Note: The **Name** field might differ in your lab environment.

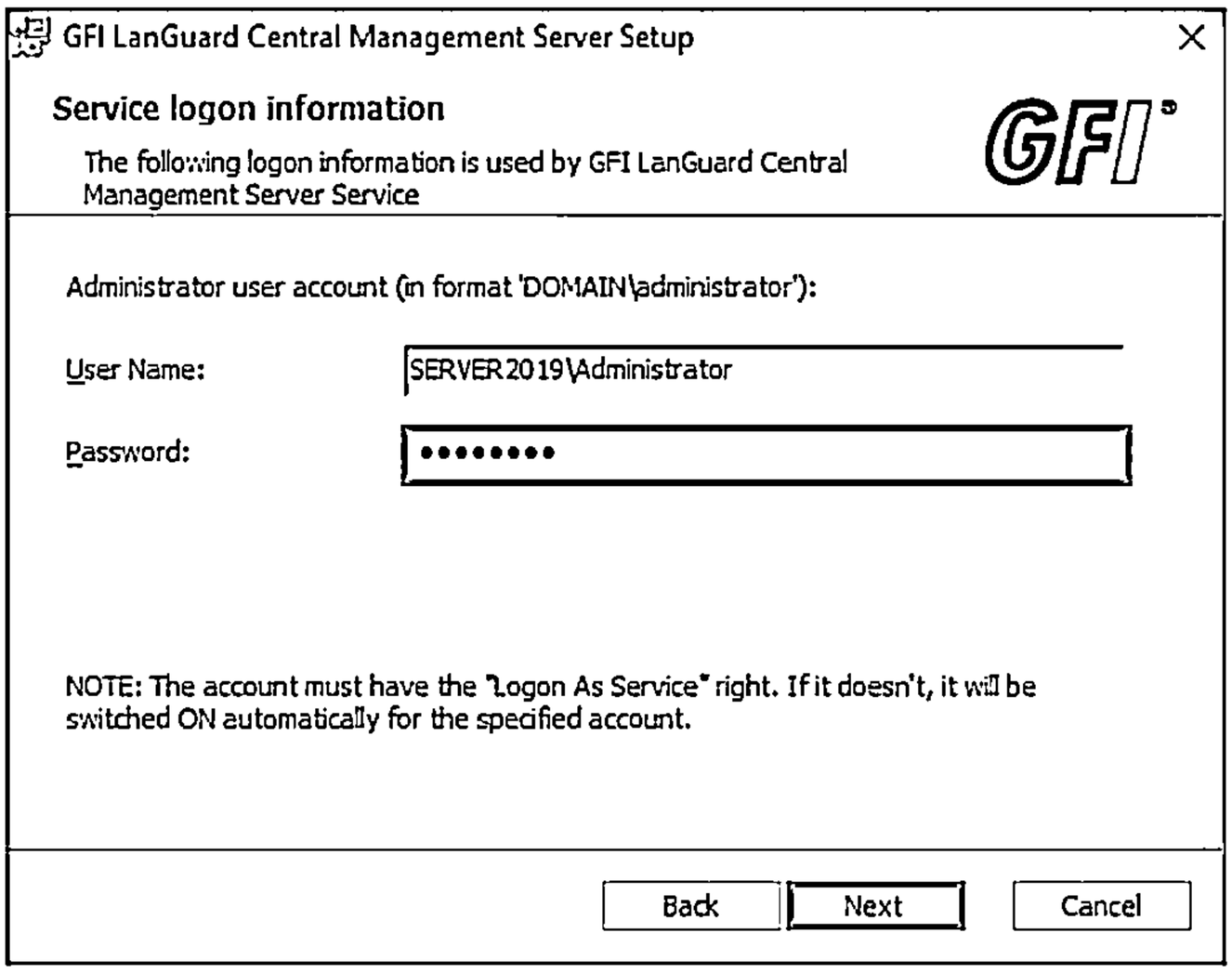


Figure 2.3.14: GFI LanGuard Service logon information section

20. The **HTTPS Settings** wizard appears; keep the name in its default and click **Next**.

Note: The name field might differ in your lab environment.

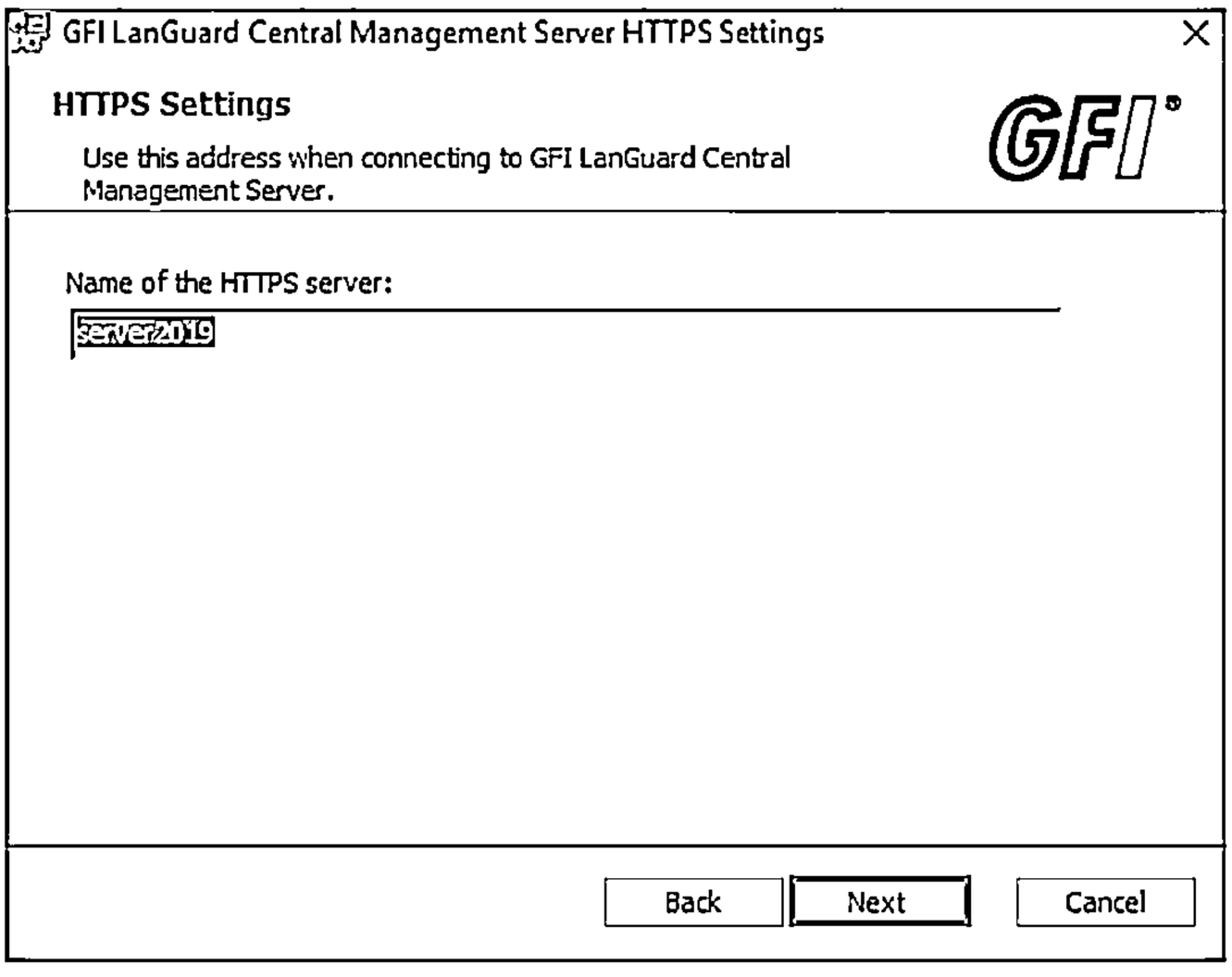


Figure 2.3.15: GFI LanGuard HTTPS Settings section

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

21. In the **Destination Folder** wizard, choose the location where you want to install the application (here, the default location is selected) and click **Next**.

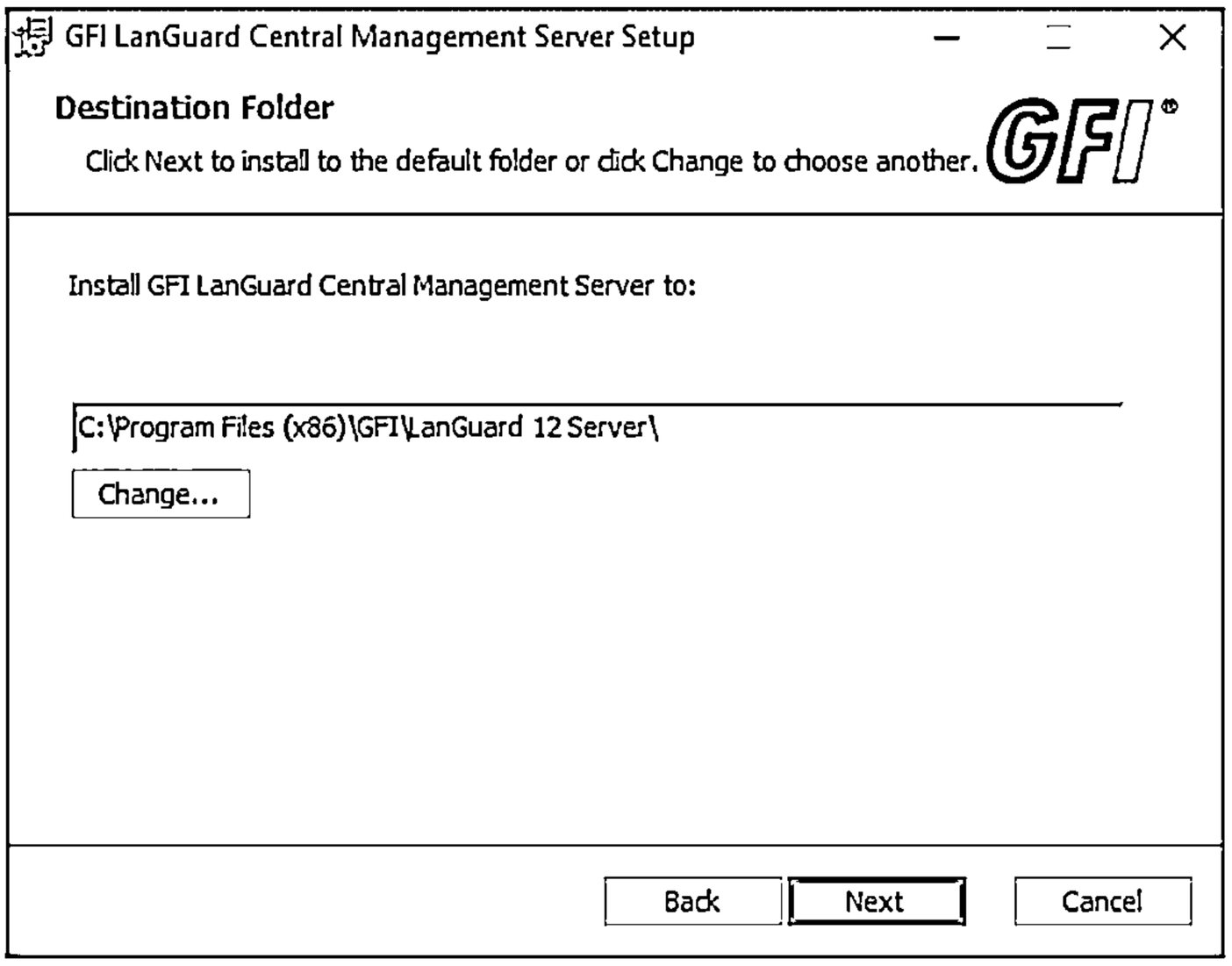


Figure 2.3.16: Choosing a folder destination

22. In the **Ready to install** wizard, click **Install** to proceed.

23. Once the installation is complete in the **GFI LanGuard Central Management Server Setup** window, click **Finish**.

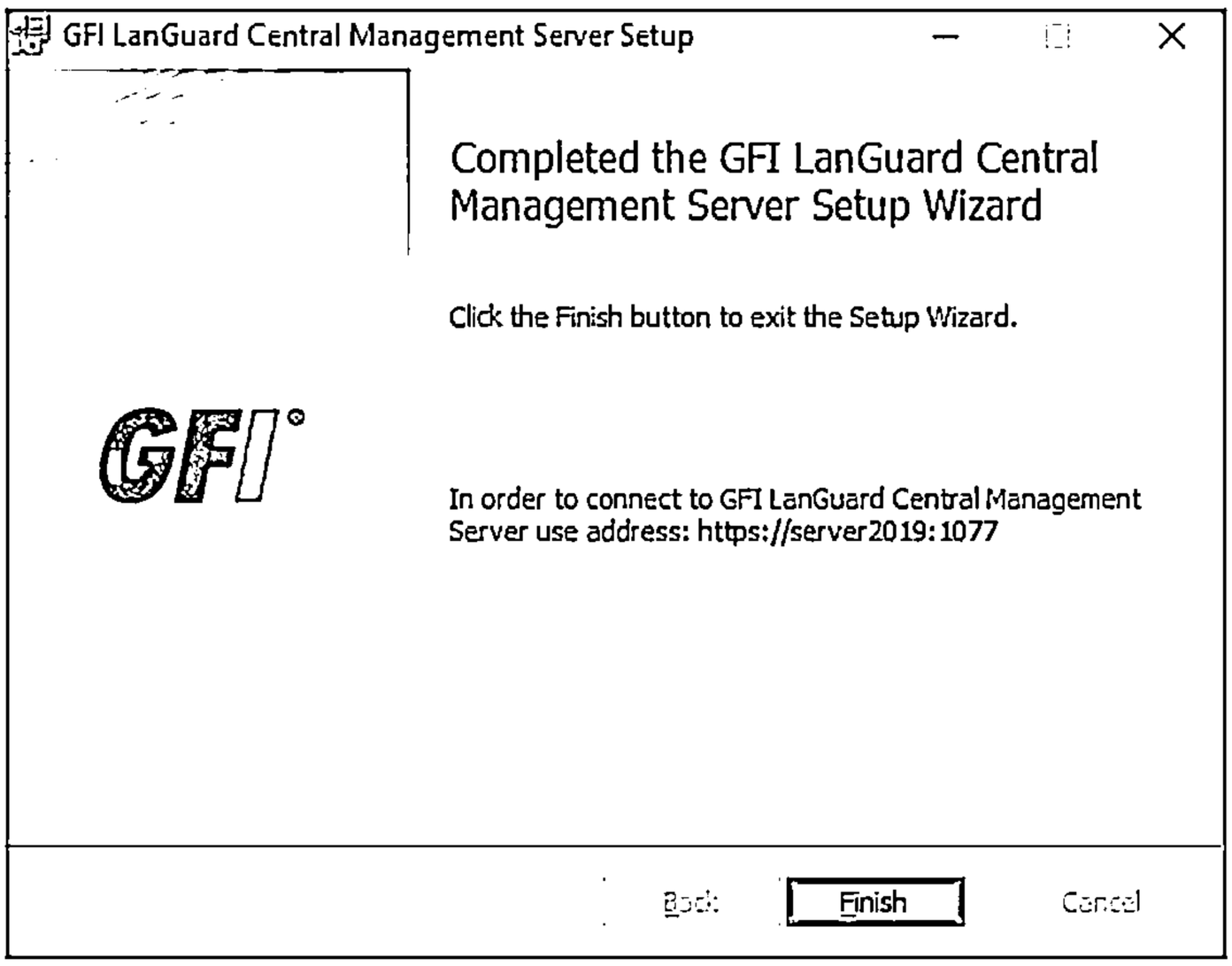


Figure 2.3.17: GFI LanGuard: click Finish

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

24. In the **GFI LanGuard Setup** window, ensure that the **Launch GFI LanGuard** checkbox is selected. De-select the **Launch GFI LanGuard Central Management Server** checkbox and click **Finish**.

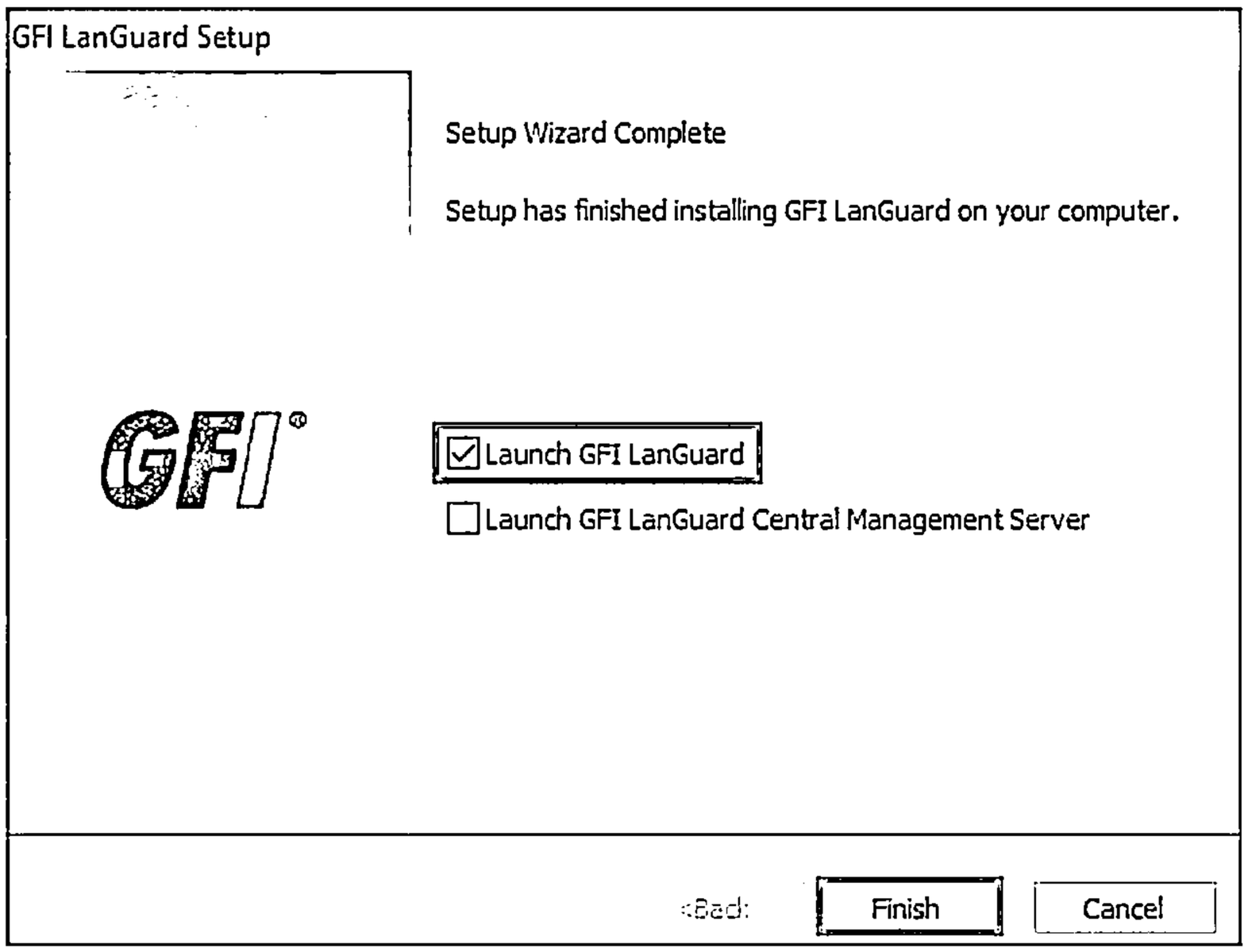


Figure 2.3.18: GFI LanGuard Setup: click Finish

25. A **GFI LanGuard** pop-up appears on the main window of the application; click **Continue evaluation**.

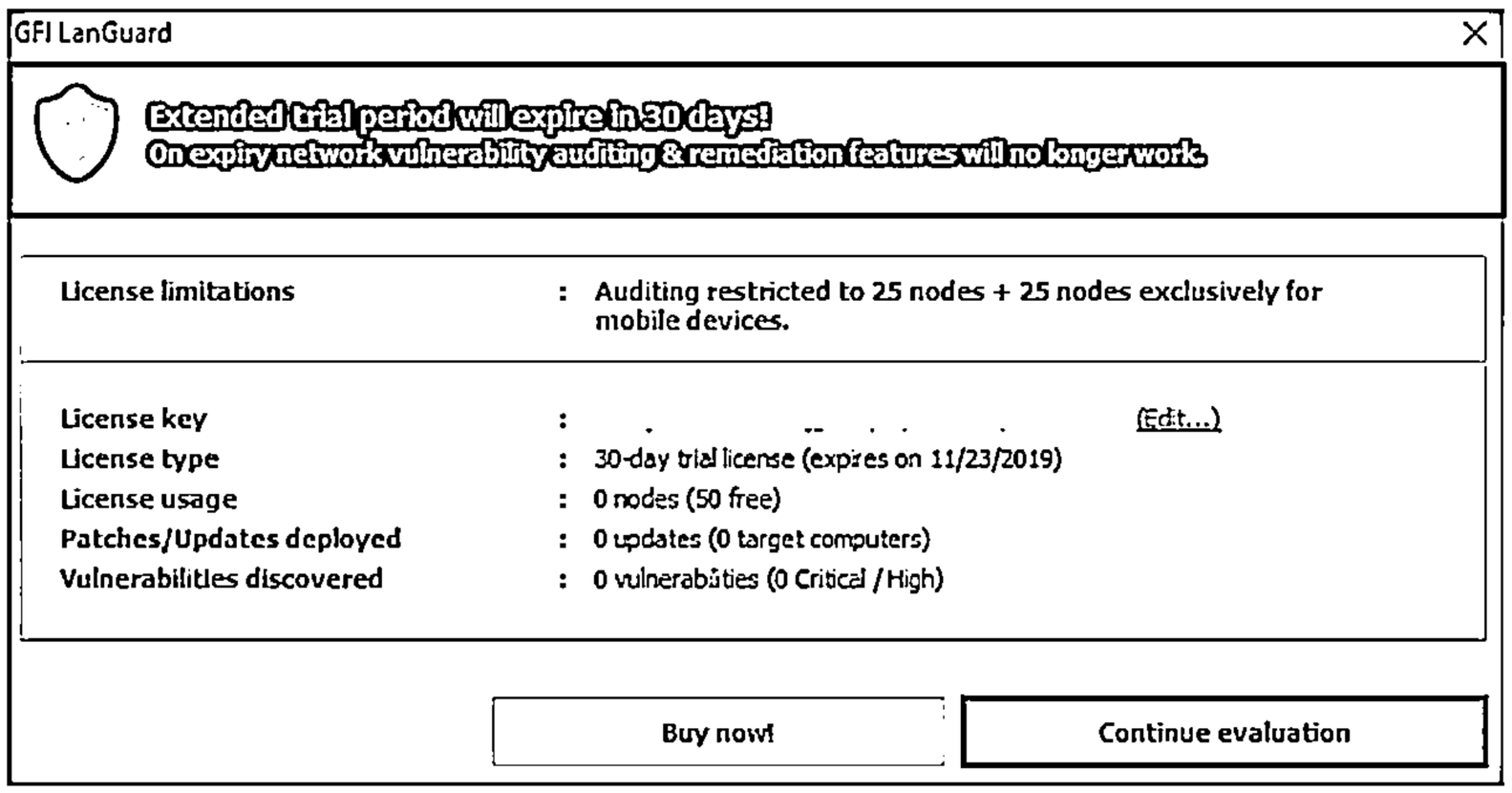


Figure 2.3.19: GFI LanGuard pop-up

26. The **GFI LanGuard** main window appears, and it begins to inspect the security status of the local computer.

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

27. Click **Launch a Scan** or **View details.**

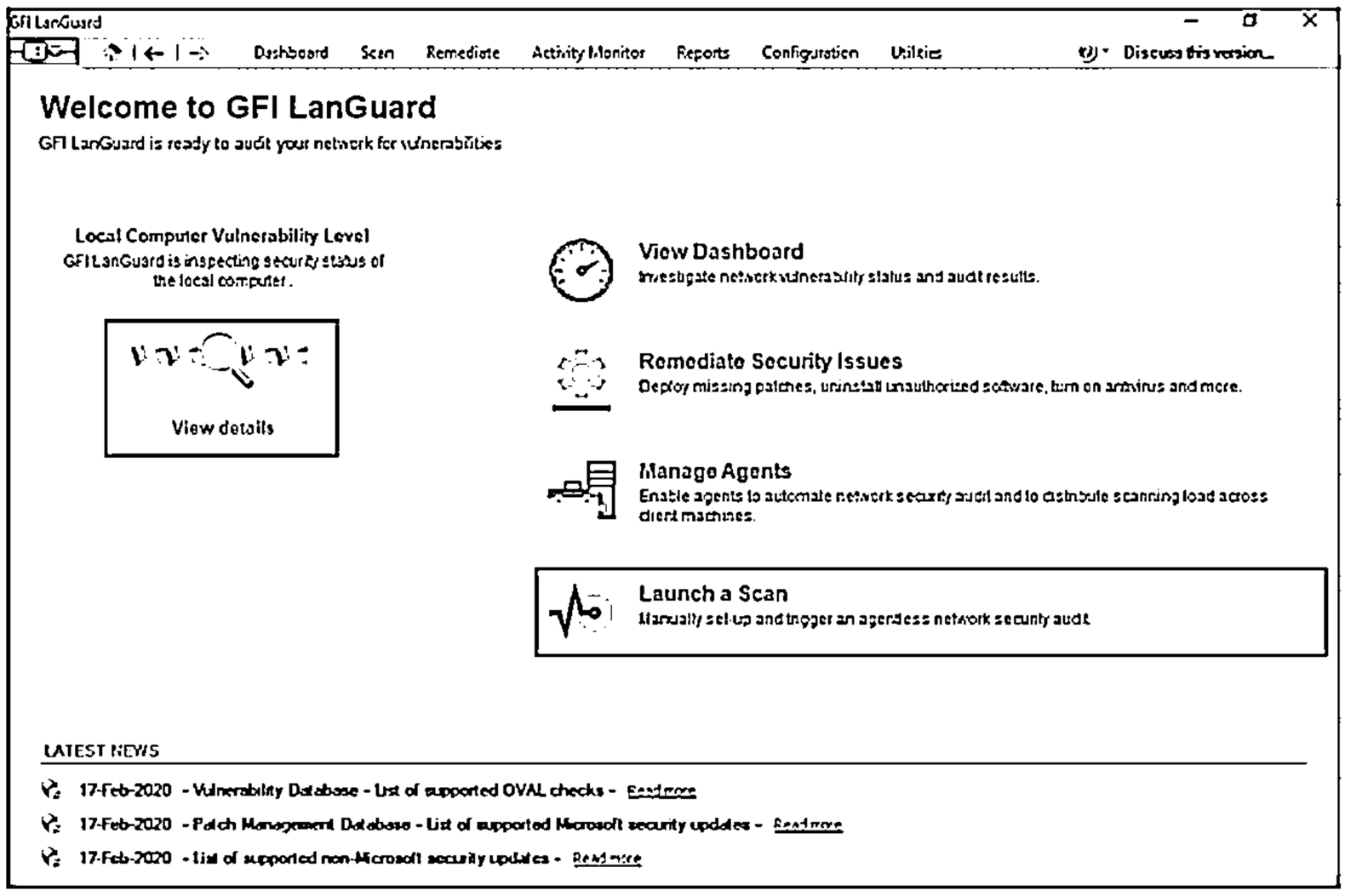


Figure 2.3.20: Launching a scan in GFI LanGuard

28. A window indicates that a scan on the local machine is already in progress.

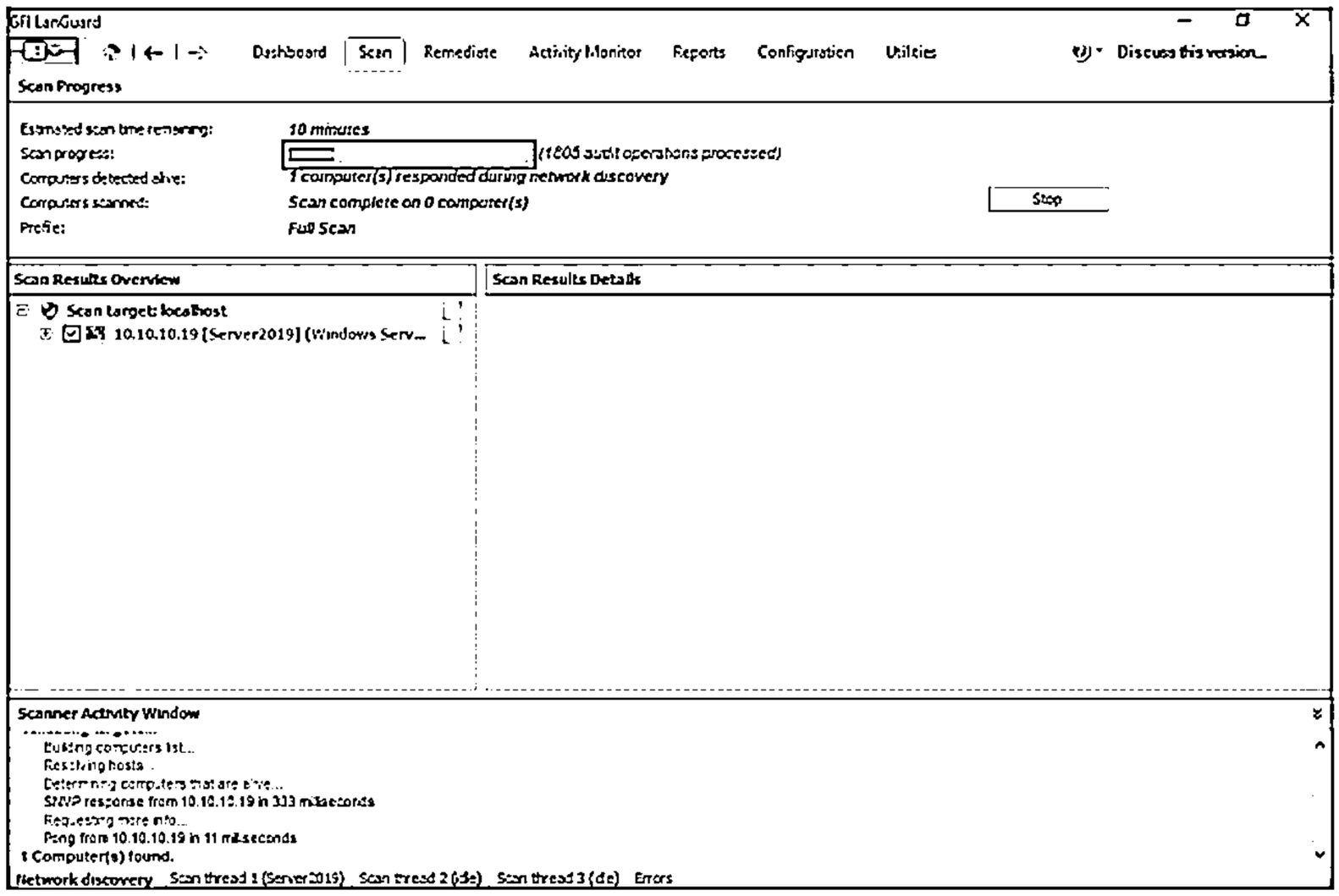


Figure 2.3.21: GFI LanGuard scanning the local machine

Note: Allow the scan to finish analyzing vulnerabilities in the host machine.

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

29. Click **Stop** to halt the vulnerability scan on the host machine.

Note: If the **Stop scanning confirmation** pop-up appears, click **Yes**.

Note: The scan might take time to stop.

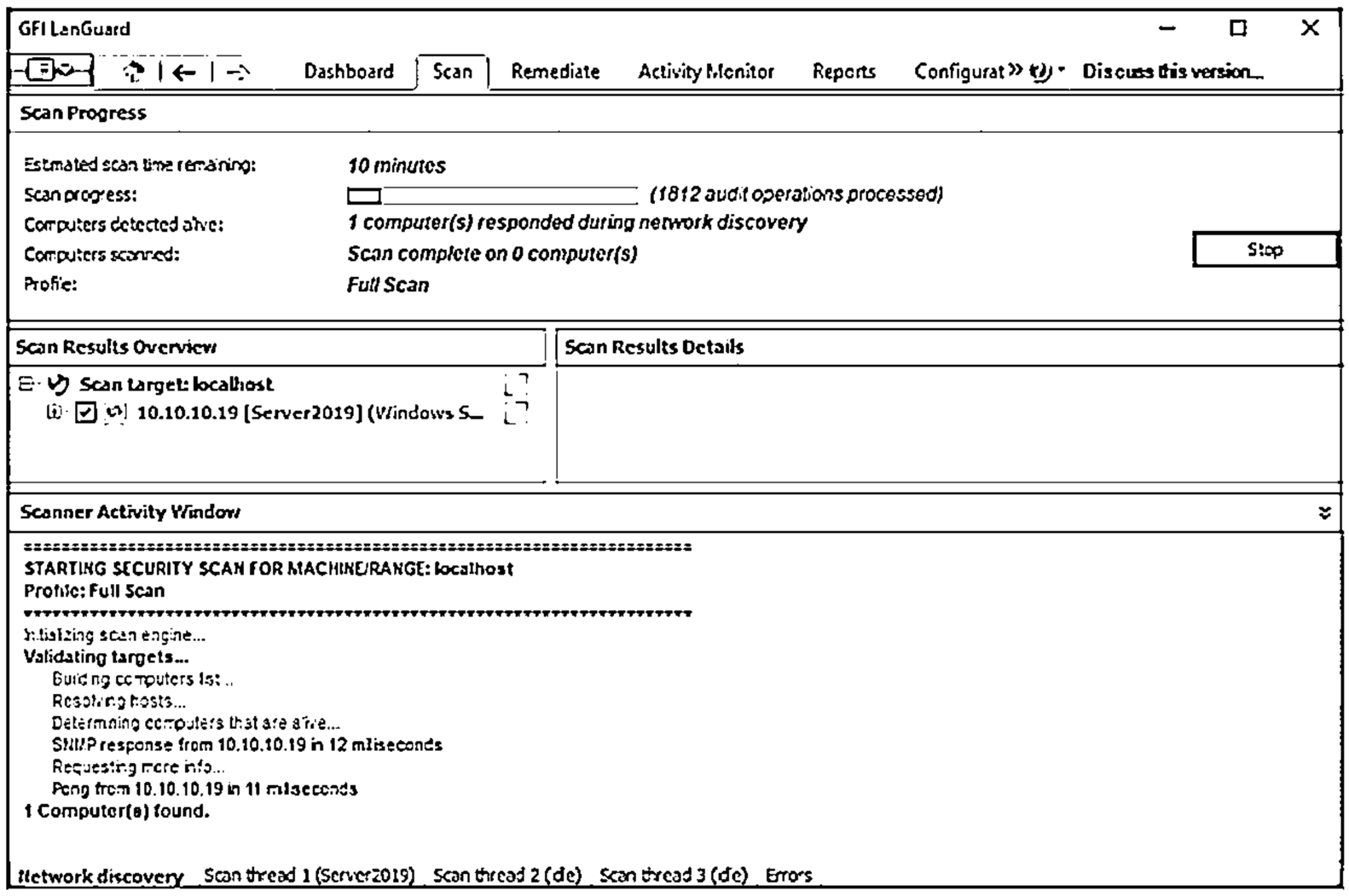


Figure 2.3.22: Stopping the scan

TASK 3.3

Scan a Target

30. The **Launch a New Scan** page appears: specify the details required to scan a target/virtual machine as follows:

    - Enter the IP address of the virtual machine in the **Scan Target** field (here, the target machine is **Windows Server 2016** [**10.10.10.16**]), and ensure that the **Full Scan** option is selected from the **Profile** drop-down list.
    - Ensure that **Currently logged on user** is selected in the **Credentials** drop-down list.
    - Click **Scan**.

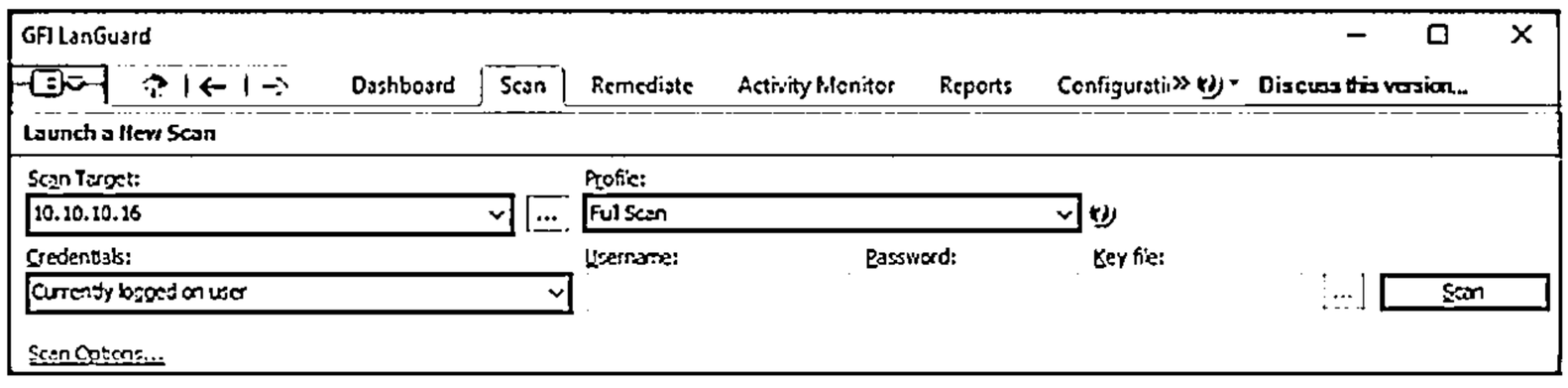


Figure 2.3.23: Customizing the scan settings

Note: This may vary in your lab environment.

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

31. GFI LanGuard takes some time to perform the vulnerability assessment on the intended virtual machine.

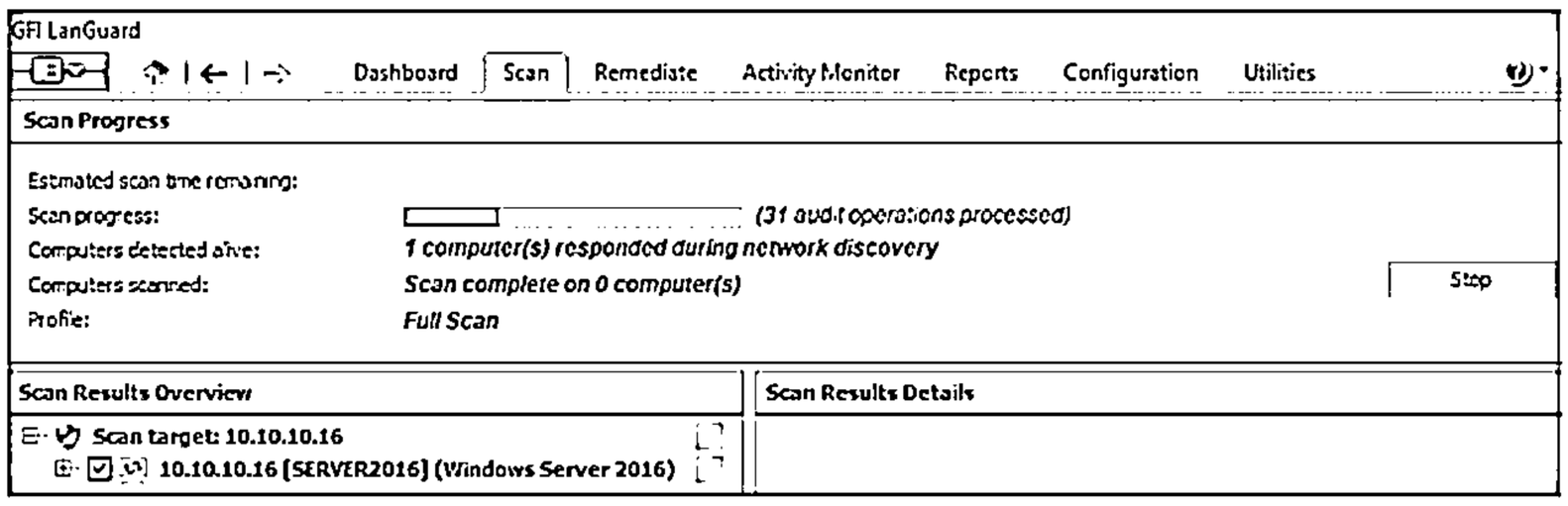


Figure 2.3.24: Vulnerability assessment being performed

32. Once the scanning is complete, a **Scan completed!** message is displayed under **Scan Results Details**, as shown in the screenshot.

Note: The scanning takes approximately 20–30 minutes to complete.

TASK 3.4

Examine the Scan Results

33. To examine the scanned result, in the left pane under **Scan Results Overview**, click the IP address (**10.10.10.16**) node to expand it. The **Vulnerability Assessment** and **Network & Software Audit** nodes are displayed, as shown in the screenshot.

Note: The results might differ in your lab environment.

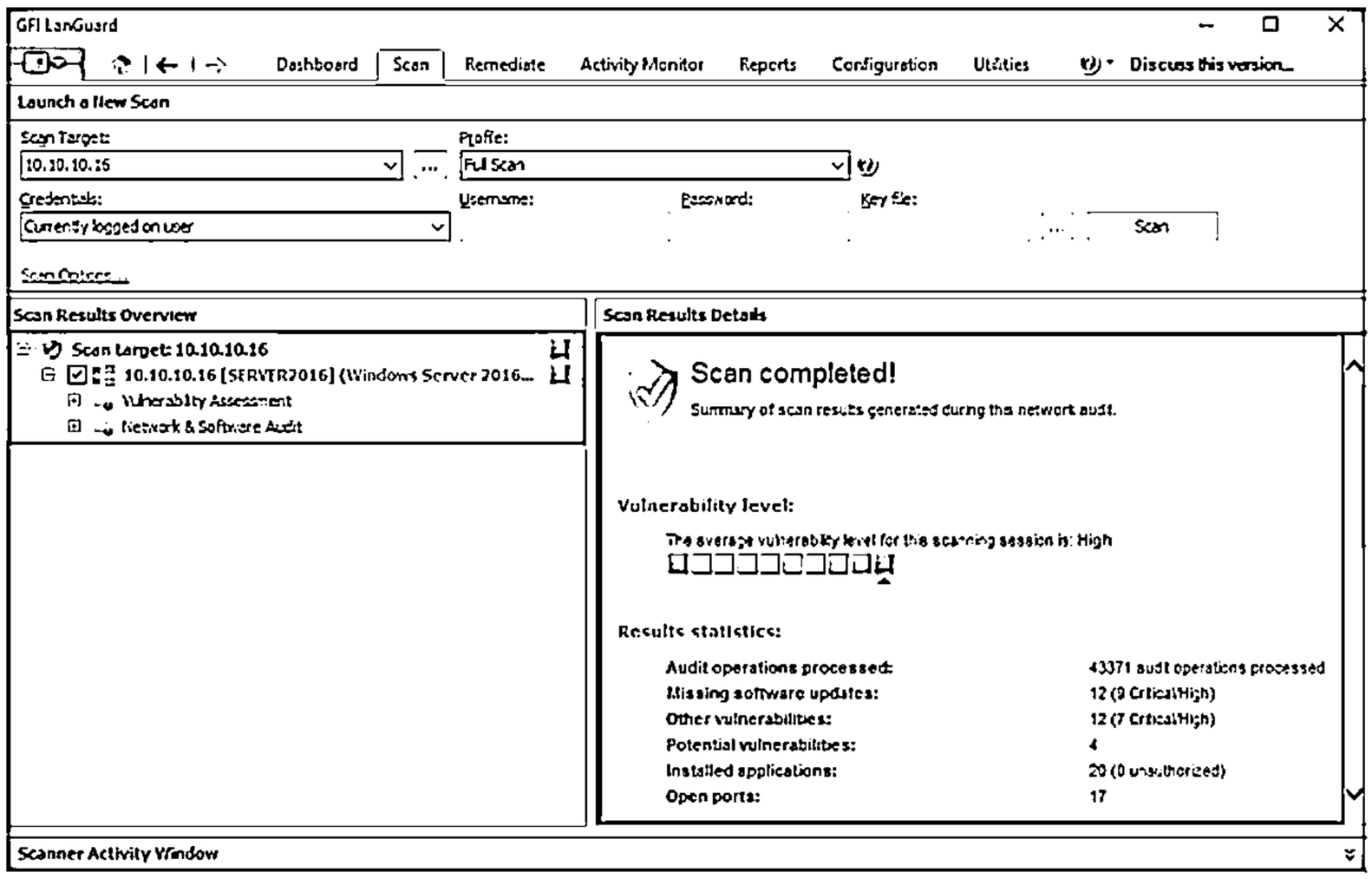


Figure 2.3.25: Viewing the scan results

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

34. Click the **Vulnerability Assessment** node. This shows category-wise details of assessed vulnerabilities. Click each category to view the vulnerabilities in detail.

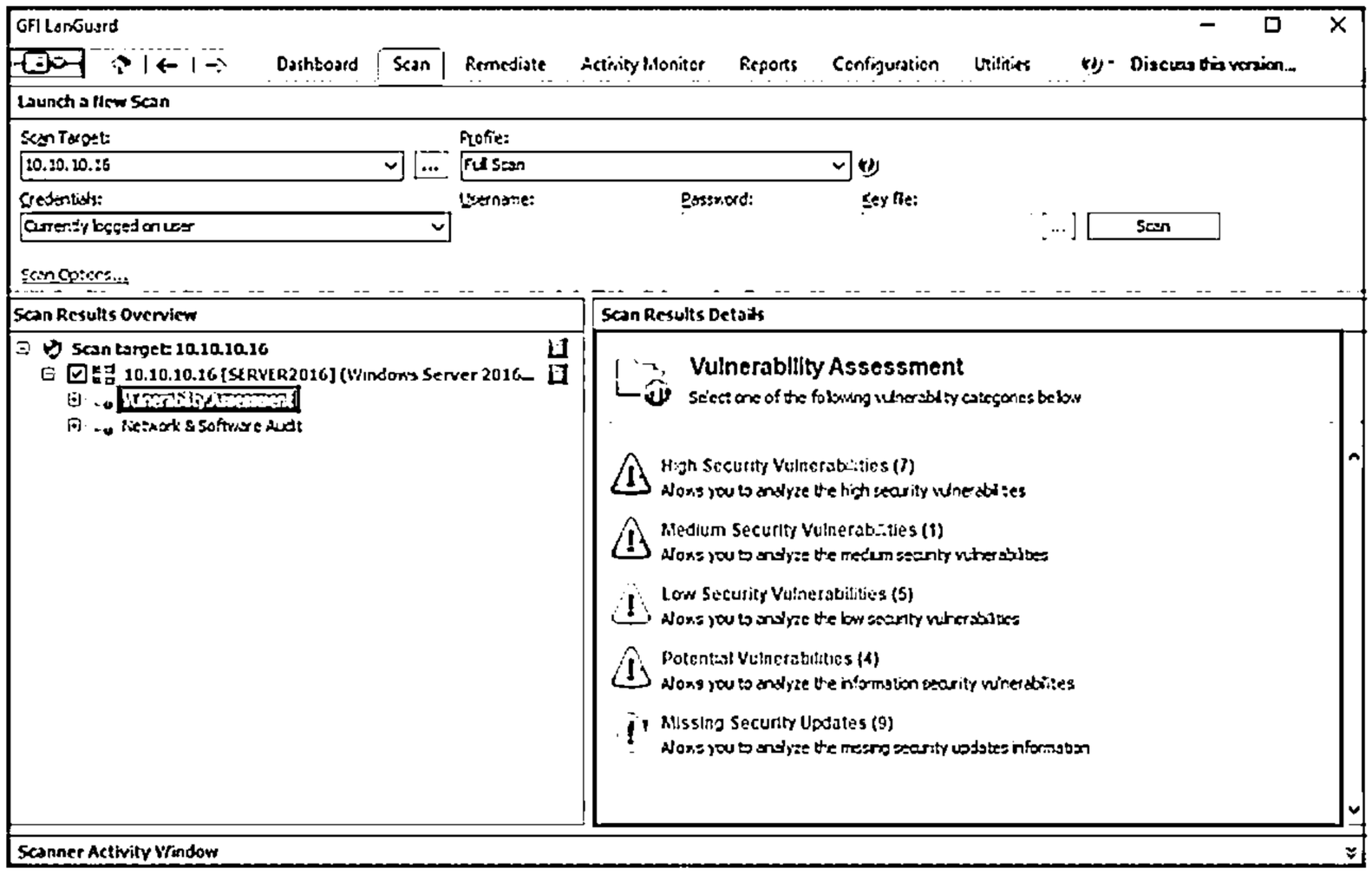


Figure 2.3.26: Vulnerability Assessment categories

35. Expand the **Network & Software Audit** node in the left pane. Click **System patching status**; detailed information regarding system patches is displayed under the **Scan Results Details** section in the right pane, as shown in the screenshot.

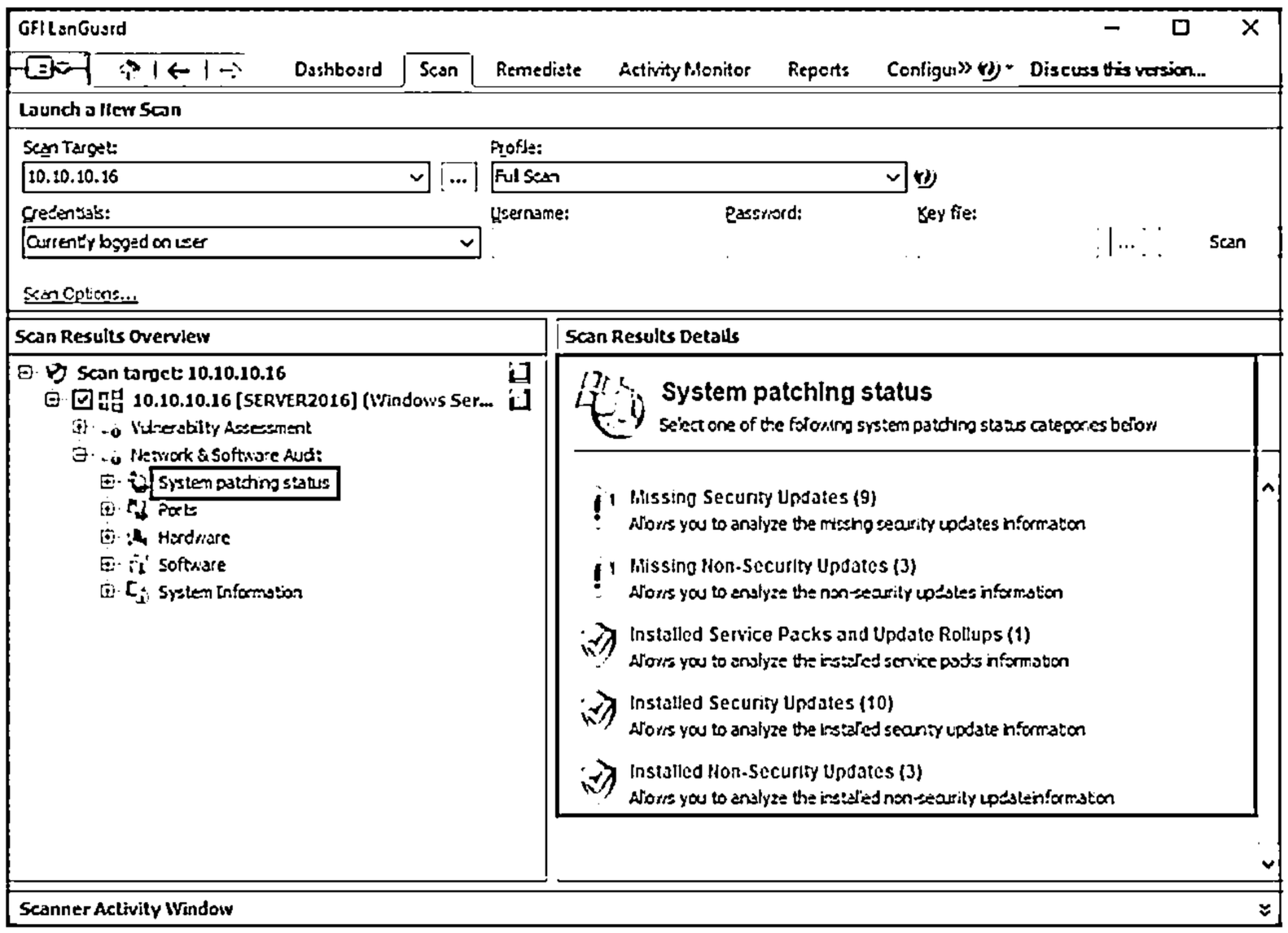


Figure 2.3.27: System patches status information

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

36. Expand **Ports** and click **Open TCP Ports** to view all the open TCP Ports under the **Scan Results Details** section in the right pane, as shown in the screenshot.

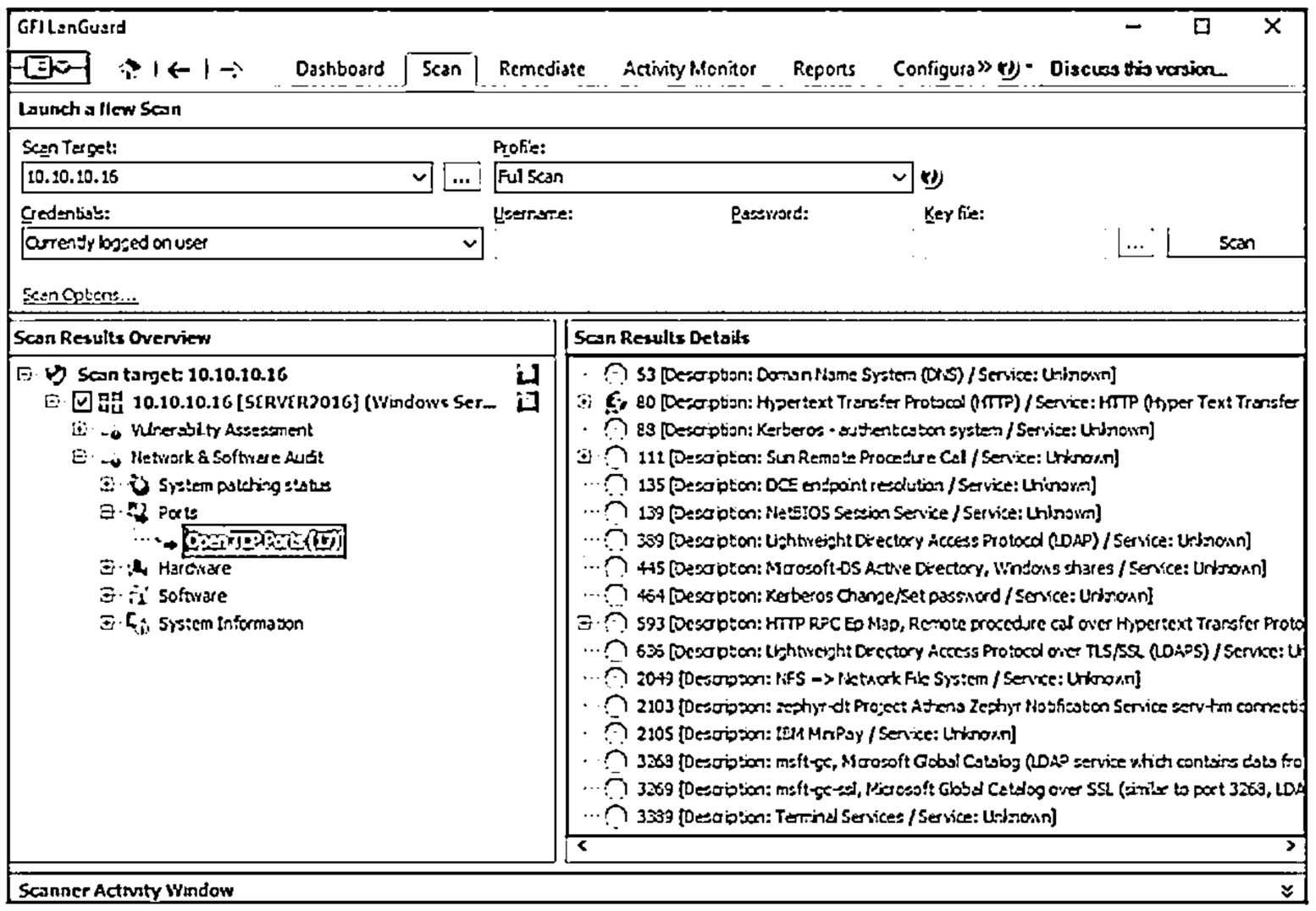


Figure 2.3.28: Scan results for open TCP Ports

37. Click **System Information** to view detailed information about the target system under the **Scan Results Details** section in the right pane.

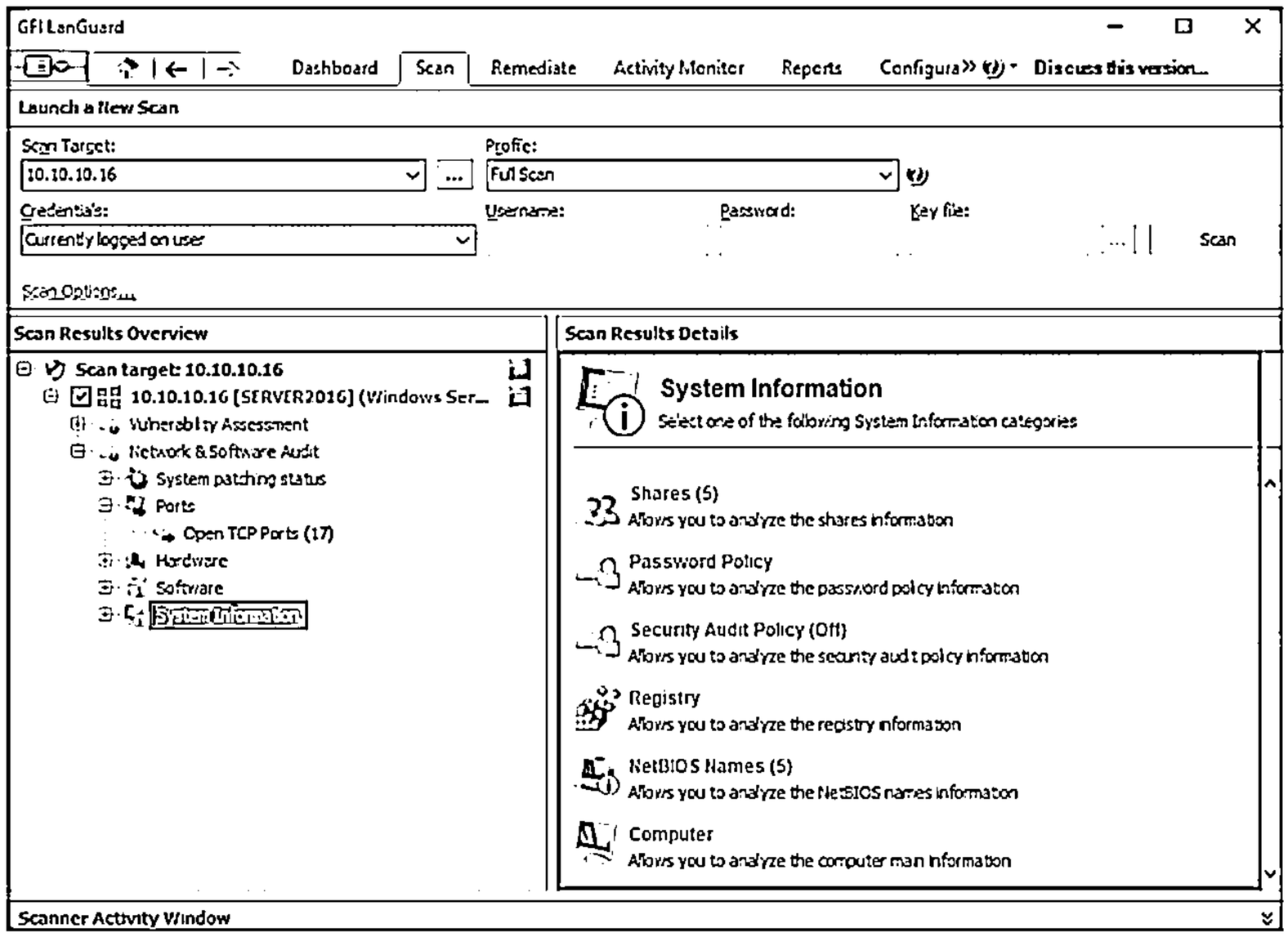


Figure 2.3.29: Scan results System Information

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

38. Expand the **System Information** node and click **Shares** to view the details of shared folders in the target virtual machine.

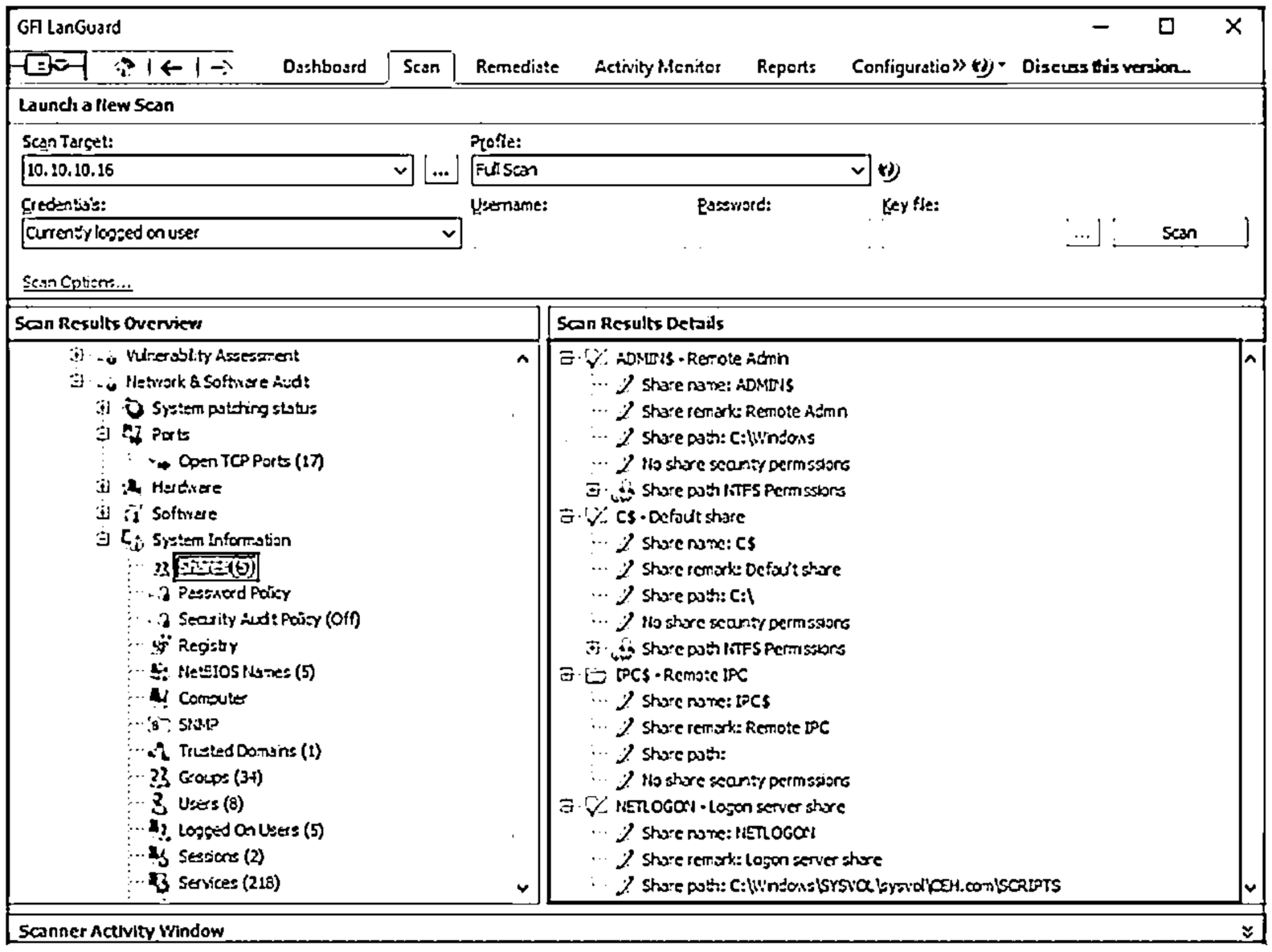


Figure 2.3.30: Scan results for Shared folders

39. Similarly, you can click the **Hardware** and **Software** nodes to view detailed scan information.

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

40. Click the **Dashboard** tab to display the scanned network information. In the left pane, expand **Entire Network**, and then **CEH**; then, click **SERVER2016**.
41. Detailed information such as **Vulnerability Level**, **Security Sensors**, **Computer Details**, **Scan Activity**, and **Results Statistics** are displayed in the right pane, as shown in the screenshot.

Note: In real-time, using this vulnerability information about the target systems can be used to develop and design exploits suitable to break into a network or a single target.

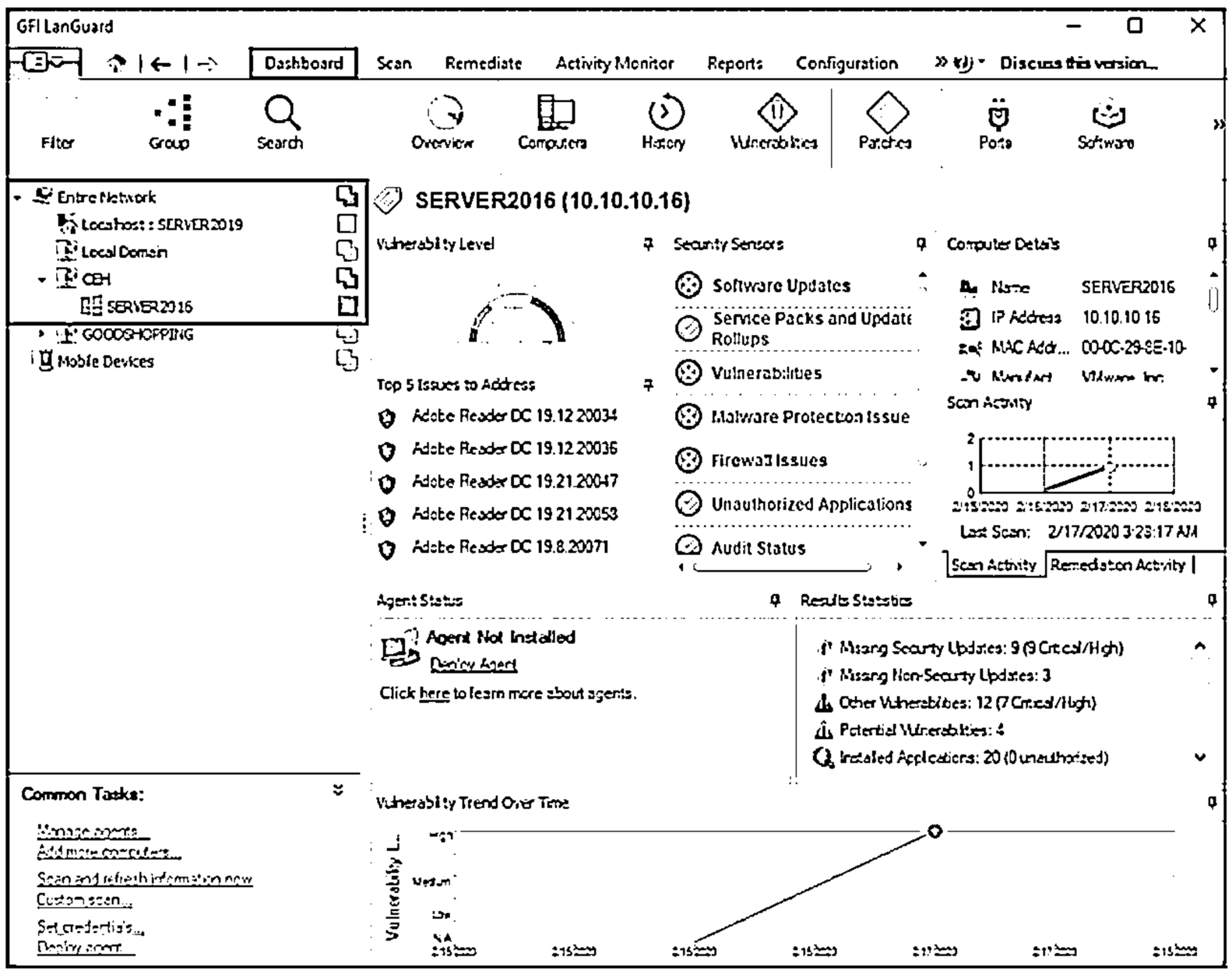


Figure 2.3.31: Overview of the Scan in Dashboard

42. You can further explore the tool by clicking on various options. For instance, click on **Software** from the options at the top to view a list of applications installed on the target machine under the **Application Category** list. You can also click on any application (here, **Google Chrome**) to view its detailed information under **Details** sections, as shown in the screenshot.

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

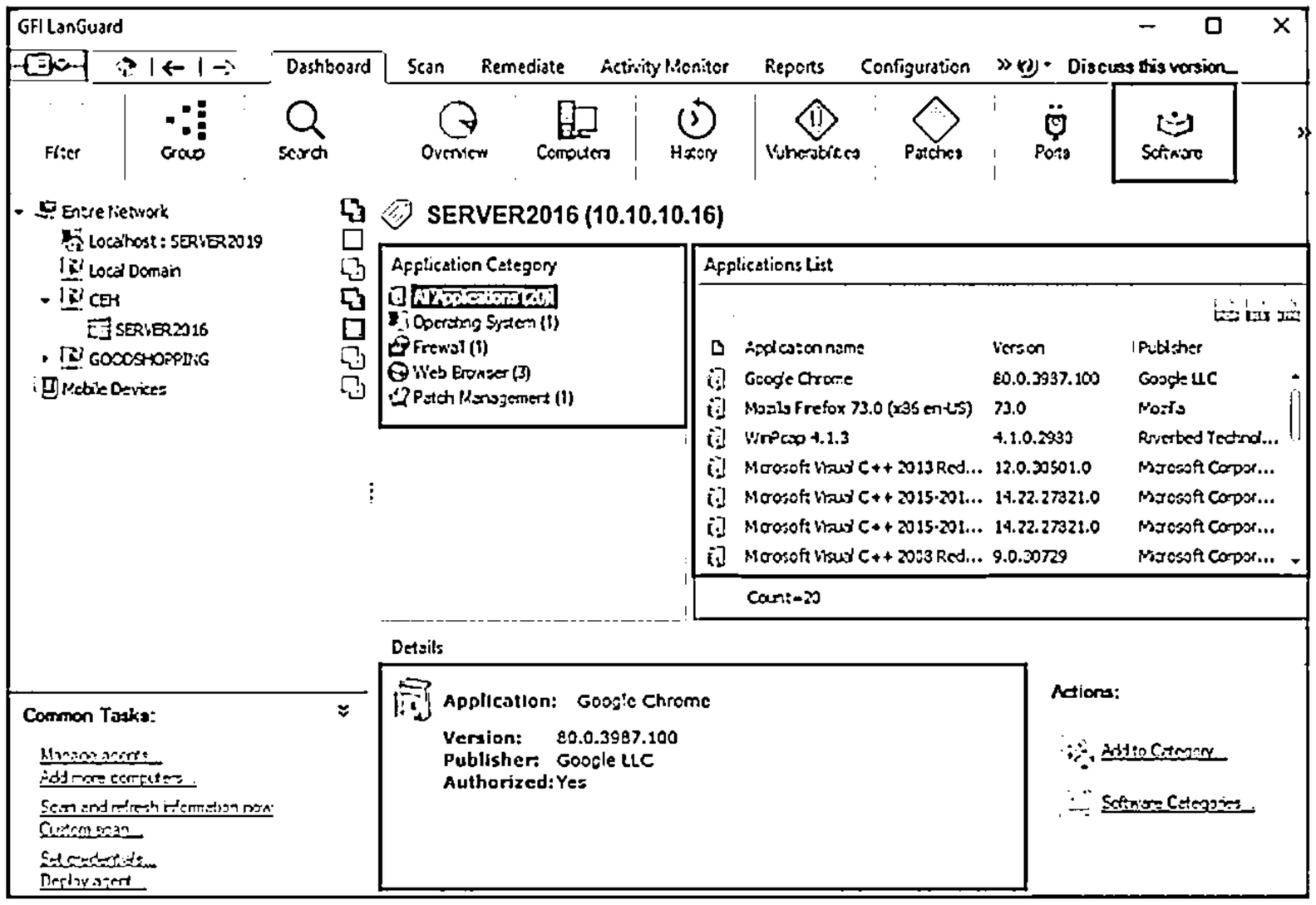


Figure 2.3.32 List of open ports

43. Click on the **Vulnerabilities** option; a list of various categories of vulnerabilities appears under the **Vulnerability Types** section. Click on any category of vulnerability (here, **High Security Vulnerabilities**): detailed information on this category is displayed under the **Details** section, and a list of vulnerabilities is displayed under the **Vulnerability List** section.

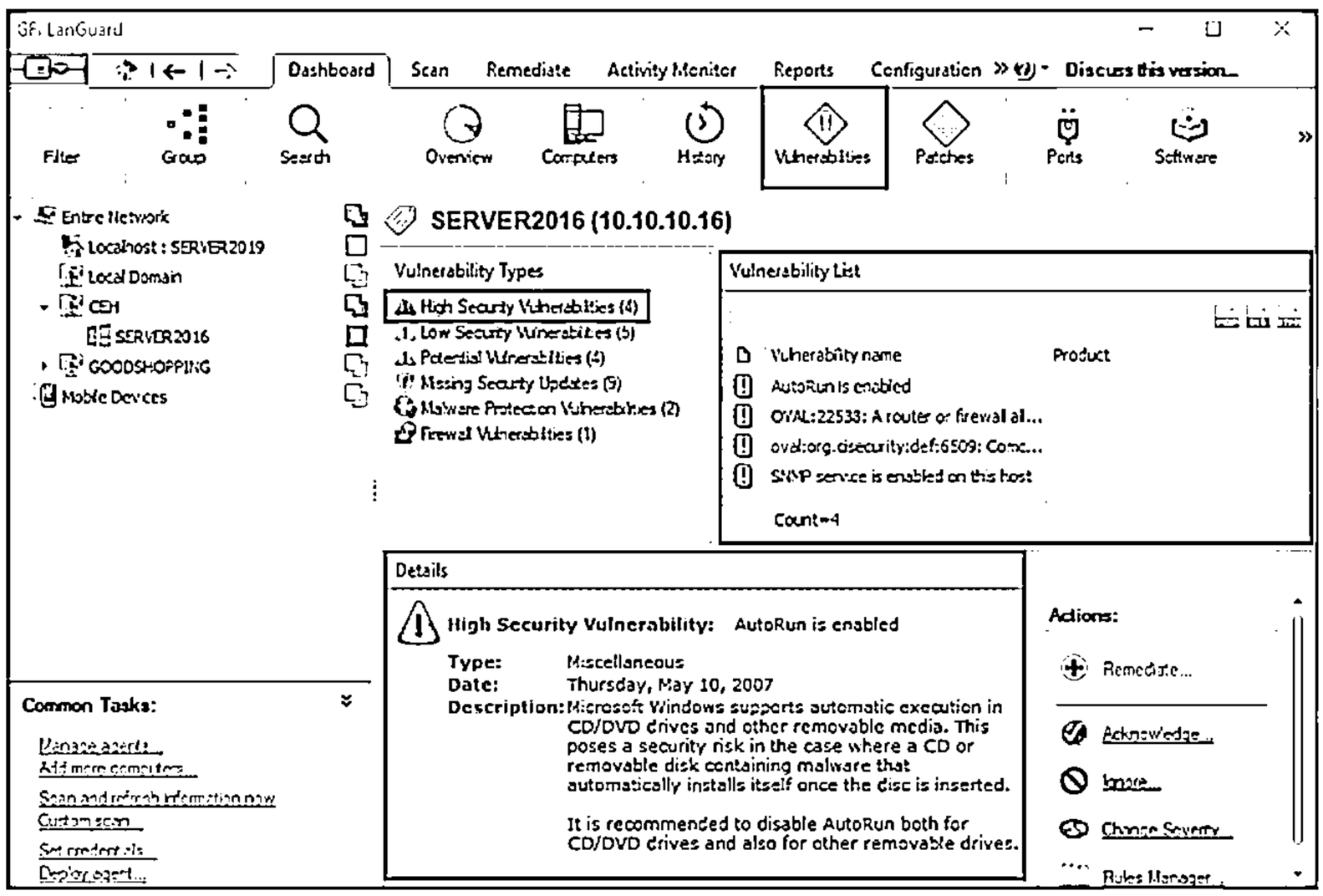


Figure 2.3.33: List of vulnerabilities

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

TASK 3.5

Generate Report

44. You can further explore scanned results by clicking various options such as **Patches, System Information, Hardware**, and **Ports**.

45. Now, click on the **Report** tab and click the **Vulnerability Status** type under **General Reports** from the right pane.

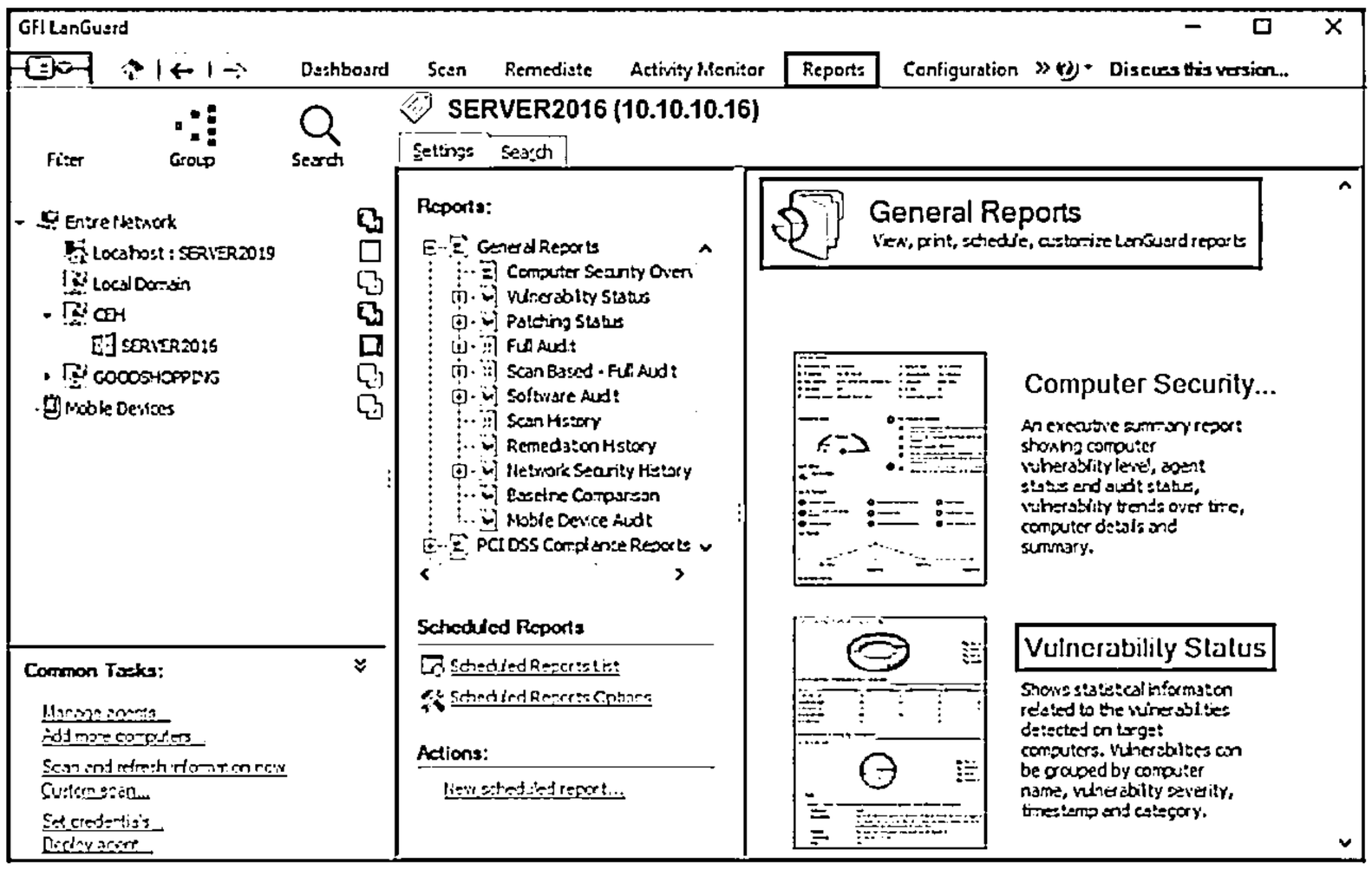


Figure 2.3.34: Generate vulnerability report

46. Information about the **Vulnerability Status** report appears in the right pane; click the **Generate Report** button to create the vulnerability report.

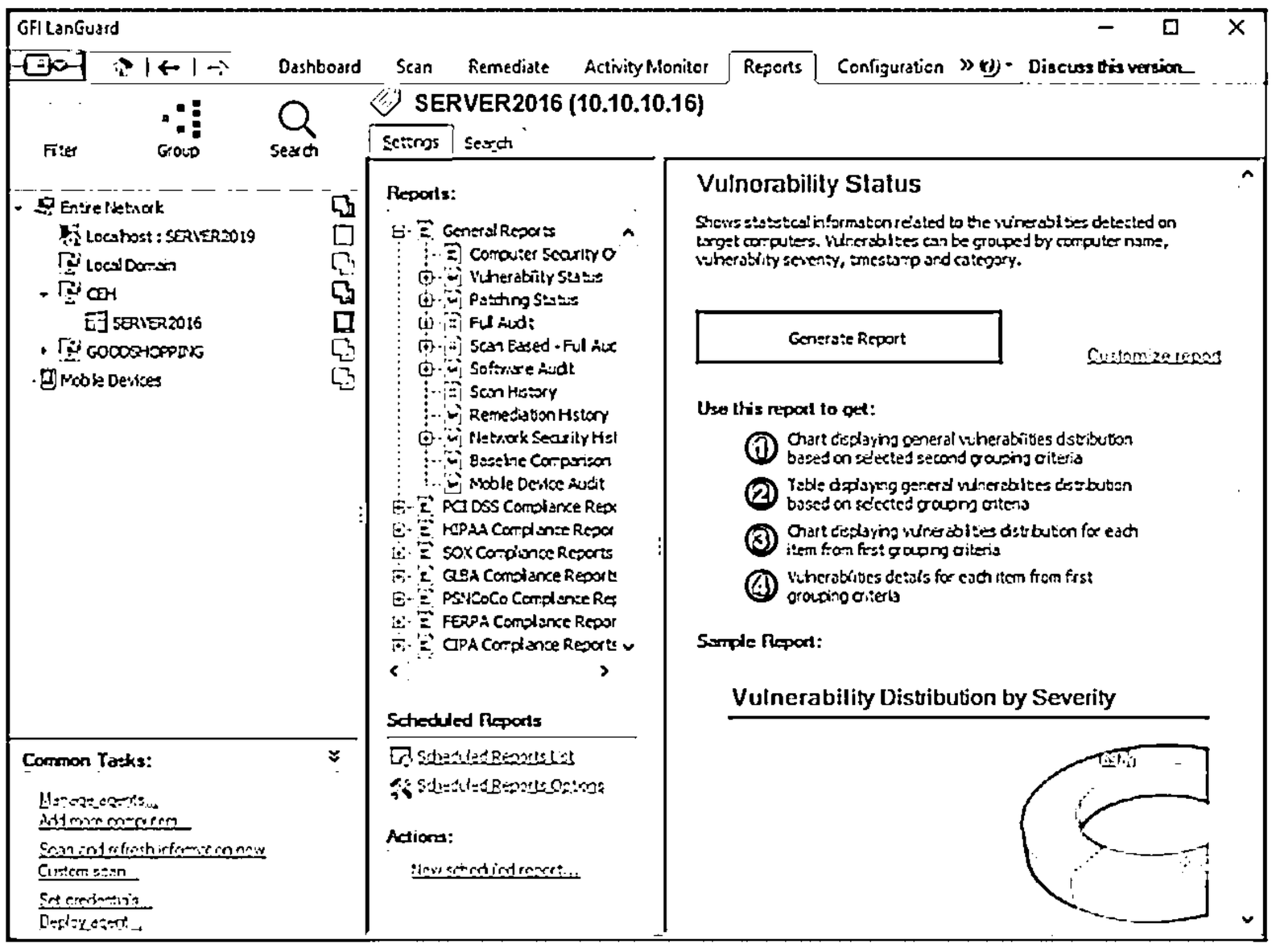


Figure 2.3.35: Generate Report

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

47. The **Vulnerability Status** report appears in the right pane. Click on the drop-down icon next to ( ) icon and choose the **HTML File** format.

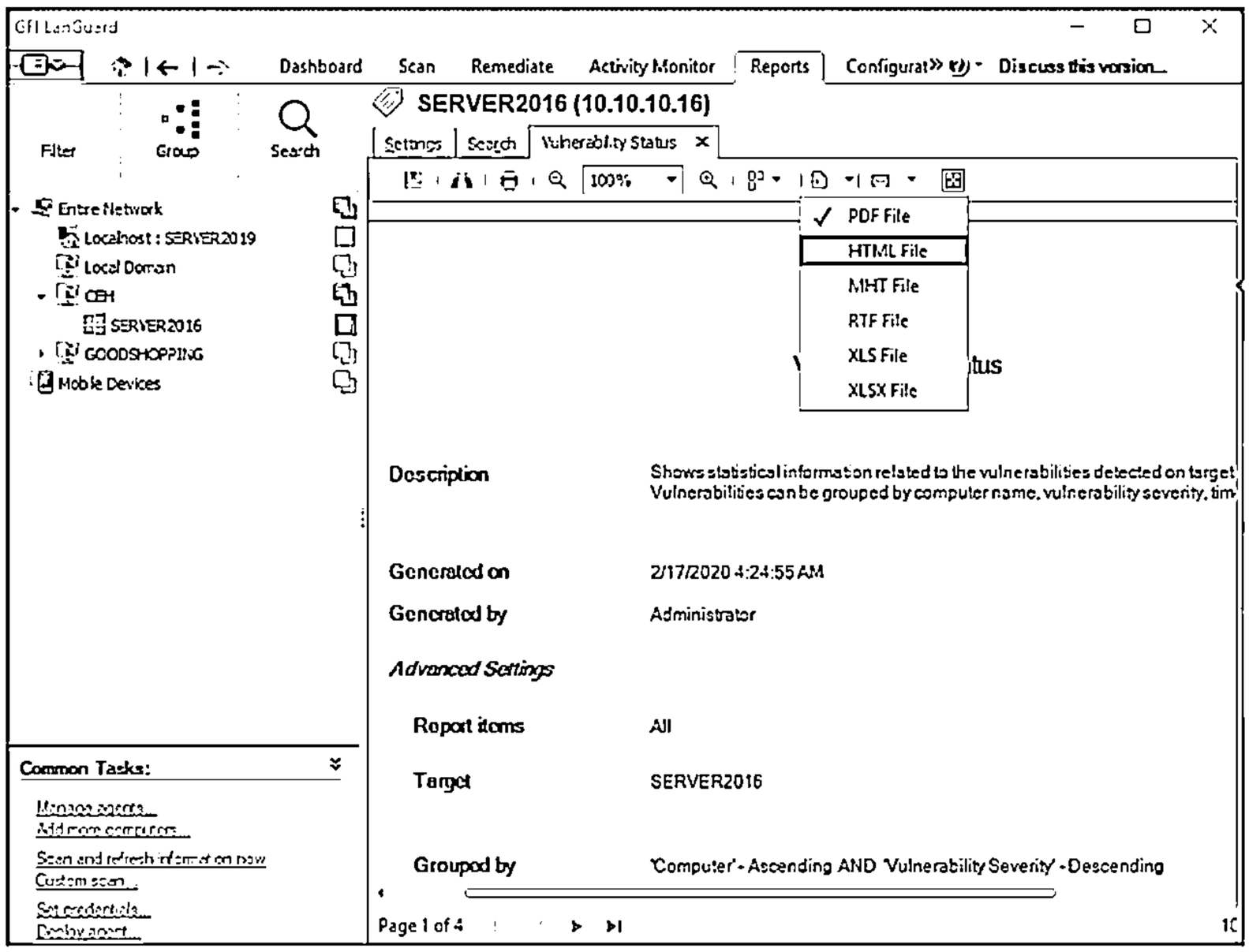


Figure 2.3.36: Report format

48. The **HTML Export Options** window appears; leave the settings to default and click **OK**.

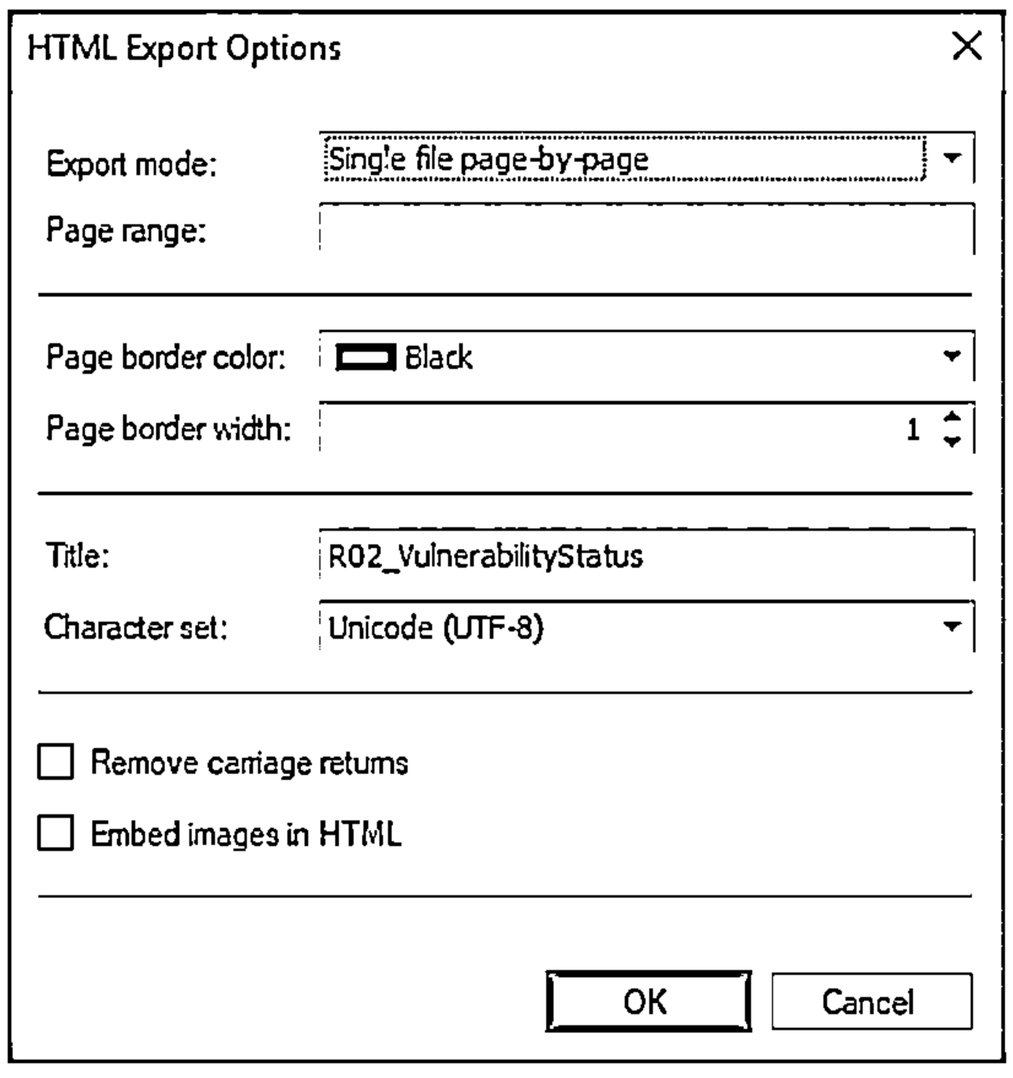


Figure 2.3.37: HTML Export Options

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

49. The **Save As** window appears; set the download location to **Desktop**. Rename the file to **Vulnerability Status Report.html** and click **Save**.

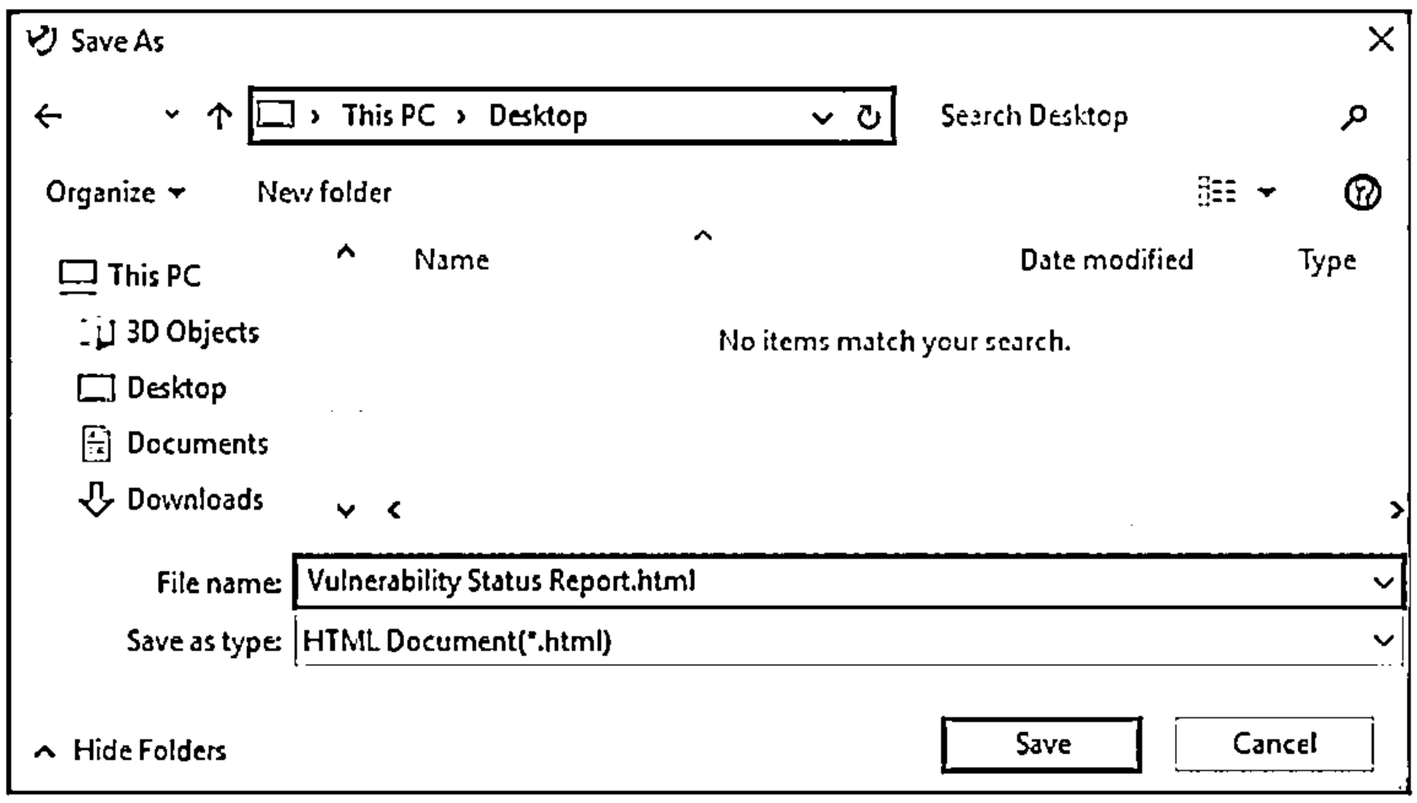


Figure 2.3.38: Save As window

50. The **GFI LanGuard** pop-up appears; click **Yes** to open the file.

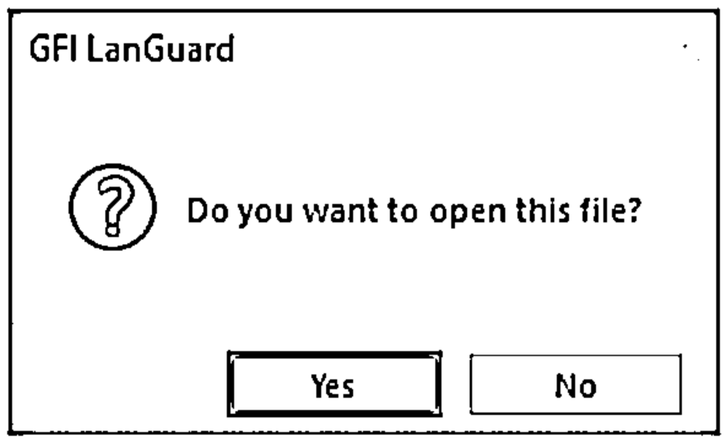


Figure 2.3.39: Open the file

51. In the **How do you want to open this file?** pop-up, select any web browser (here, **Firefox**) and click **OK**.

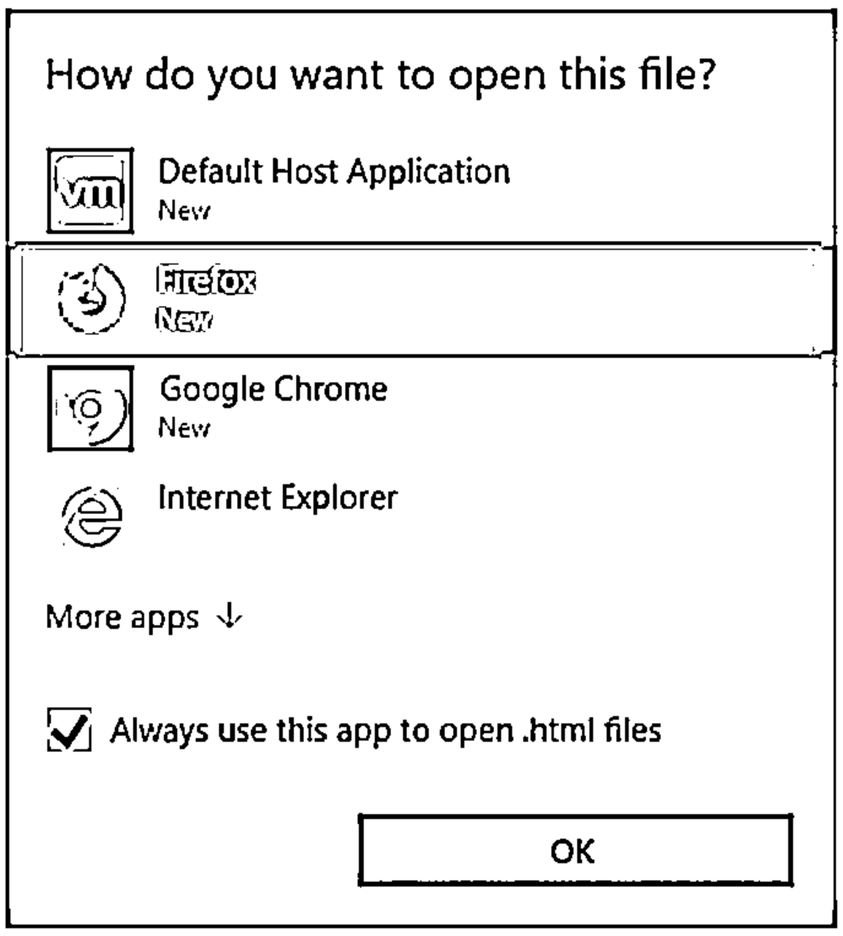


Figure 2.3.40: Selecting a web browser

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

52. The **Vulnerability Status** report appears; you can scroll down to view detailed information regarding discovered vulnerabilities.

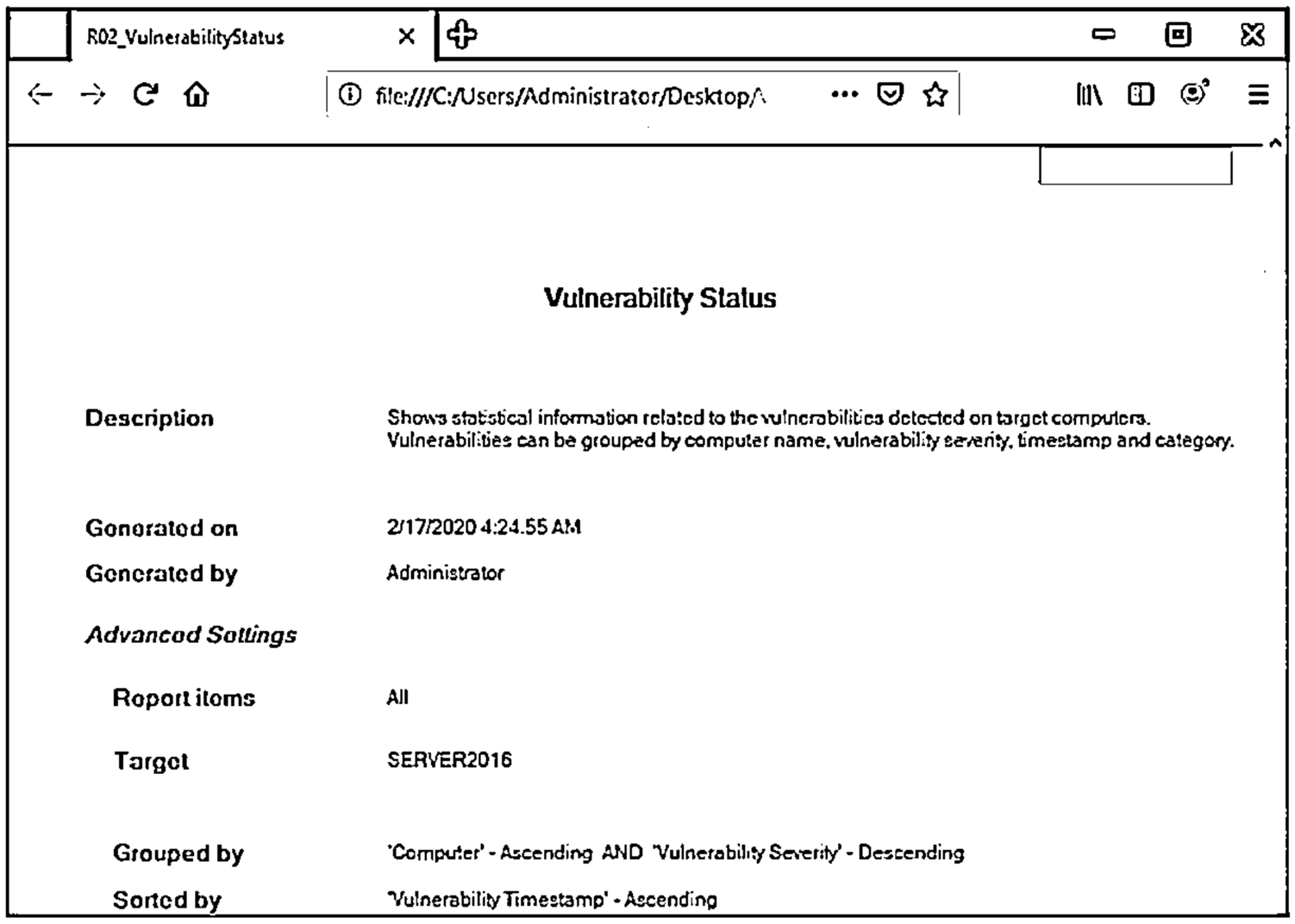


Figure 2.3.41: Vulnerability Status Report

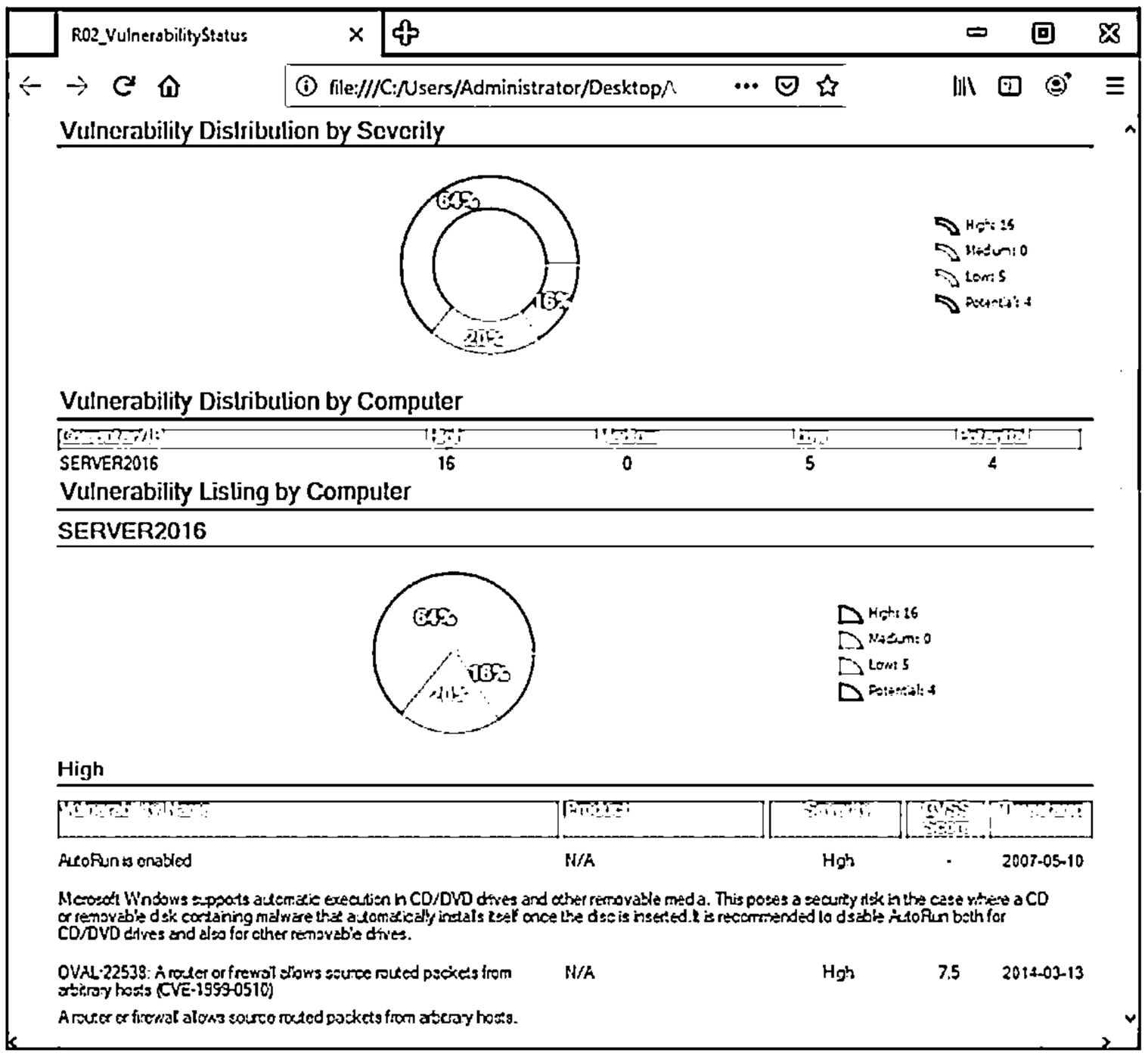


Figure 2.3.42 Vulnerability Status Report

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

53. This concludes the demonstration of scanning network vulnerabilities using GFI LanGuard.
54. Close all open windows and document all the acquired information.
55. Turn off the **Windows Server 2016** and **Windows Server 2019** virtual machines.

TASK 4

Perform Web Servers and Applications Vulnerability Scanning using CGI Scanner Nikto

Here, we will perform web servers and applications vulnerability scanning using CGI scanner Nikto.

Note: In this task, we will target the **www.certifiedhacker.com** website.

1. Turn on the **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking for you to update the machine, click **No** to close the window.

3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

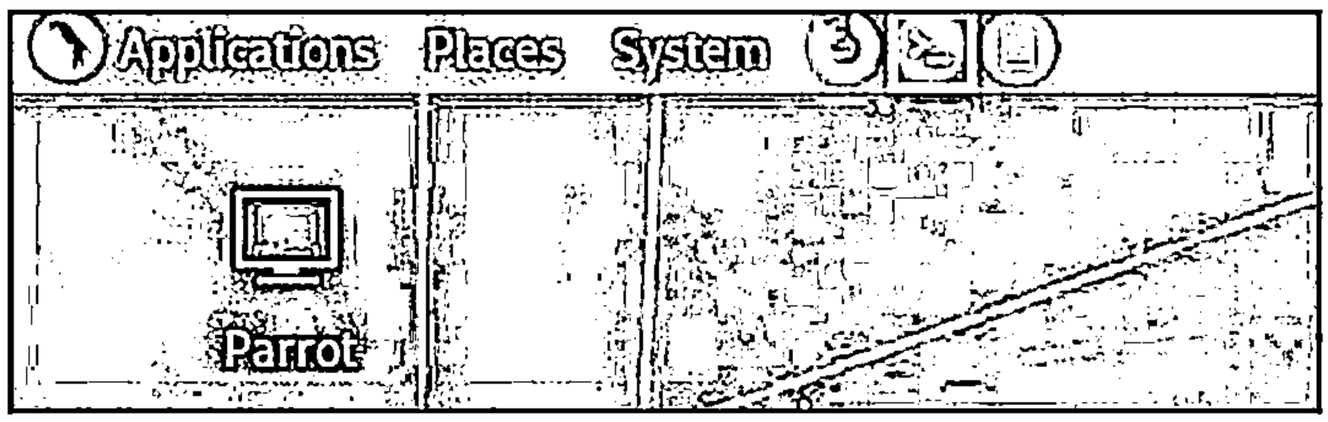


Figure 2.4.1: MATE Terminal Icon

4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

6. Now, type **cd** and press **Enter** to jump to the root directory.

TASK 4.1

Launch Nikto Tool

7. Type **nikto -H** and press **Enter** to view various available commands with full help text

Nikto is an Open Source (GPL) web server scanner that performs comprehensive tests against web servers for multiple items, including over 6700 potentially dangerous files/programs, checks for outdated versions of over 1250 servers, and version specific problems on over 270 servers.

It also checks for server configuration items such as the presence of multiple index files and HTTP server options; it will also attempt to identify installed web servers and software.

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

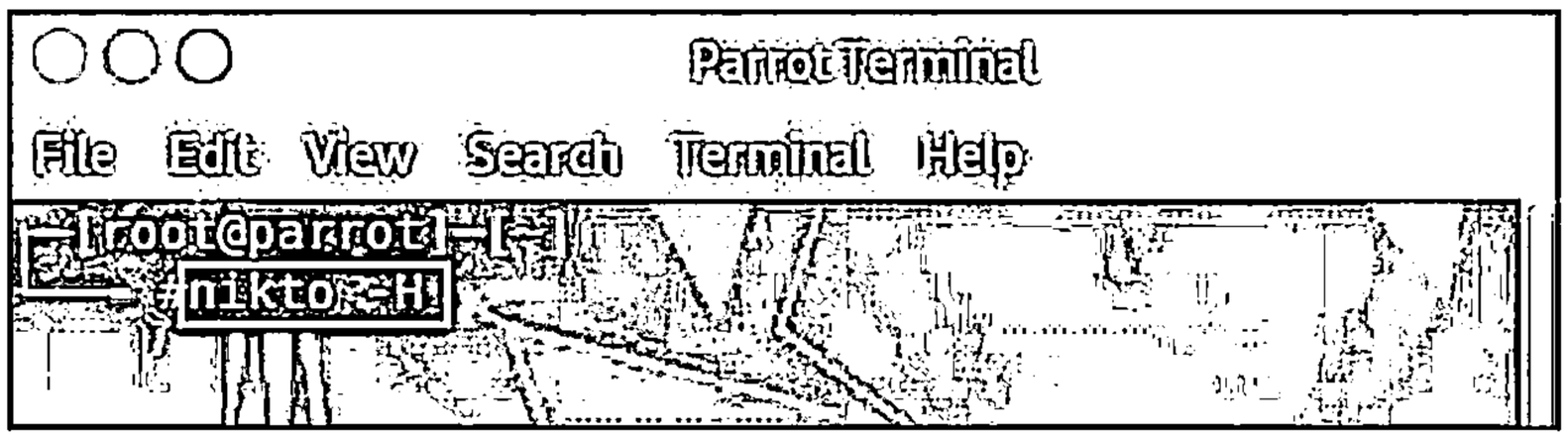


Figure 2.4.2: Nikto help command

8. The result appears, displaying various available options in Nikto. We will use the **Tuning** option to do a deeper and more comprehensive scan on the target webserver.

Note: A tuning scan can be used to decrease the number of tests performed against a target. By specifying the type of test to include or exclude, faster and focused testing can be completed. This is useful in situations where the presence of certain file types such as XSS or simply "interesting" files is undesired.

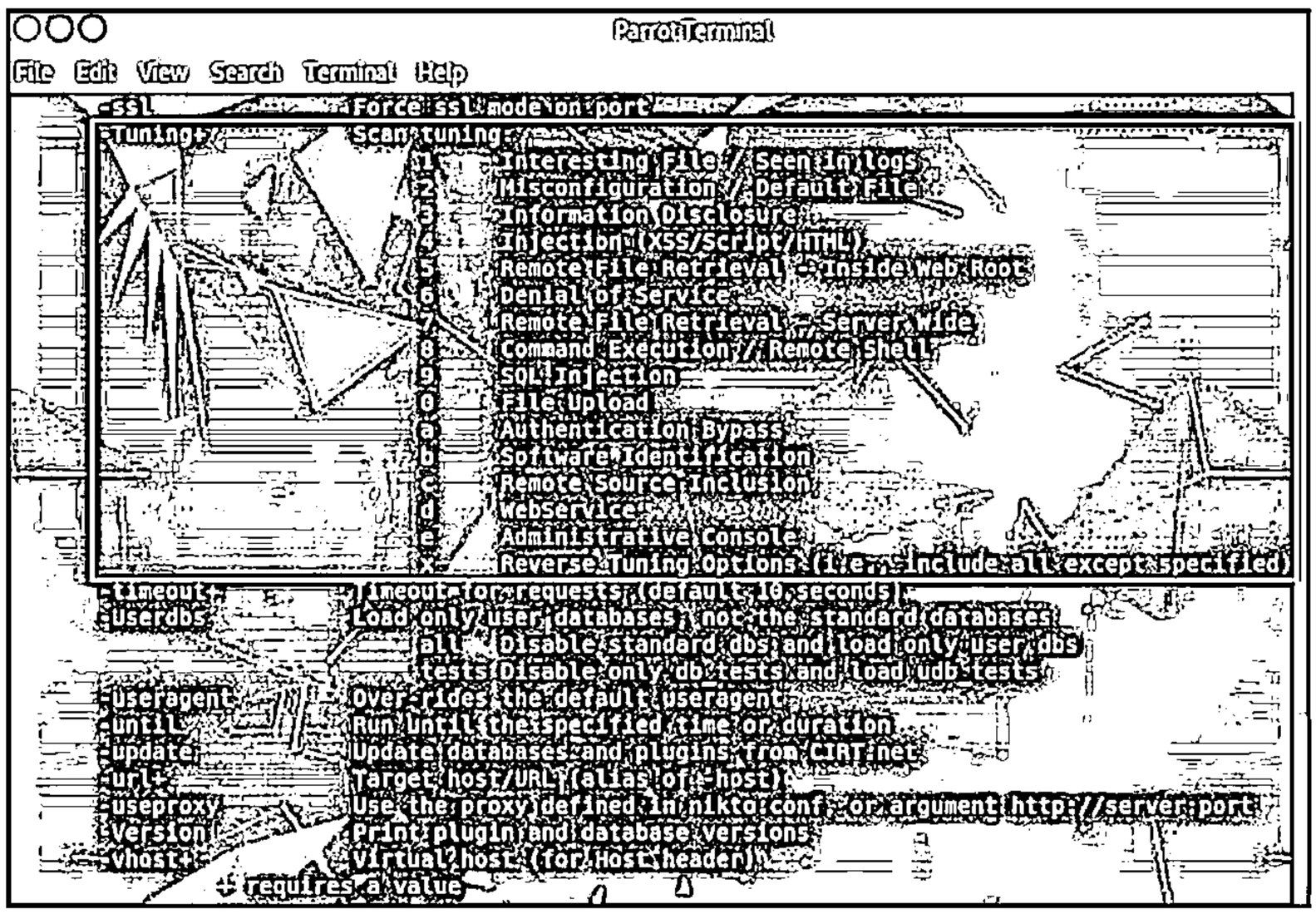


Figure 2.4.3: Nikto tuning options

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

9. In the terminal window, type **nikto -h <Target Website> -Tuning x** (here, the target website is **www.certifiedhacker.com**) and press **Enter**. Nikto starts scanning with all the tuning options enabled.

Note: **-h**: specifies the target host and **x**: specifies the Reverse Tuning Options (i.e., include all except specified)

10. The result appears, displaying various information such as the name of the server, IP address, target port, retrieved files, and vulnerabilities details of the target website.

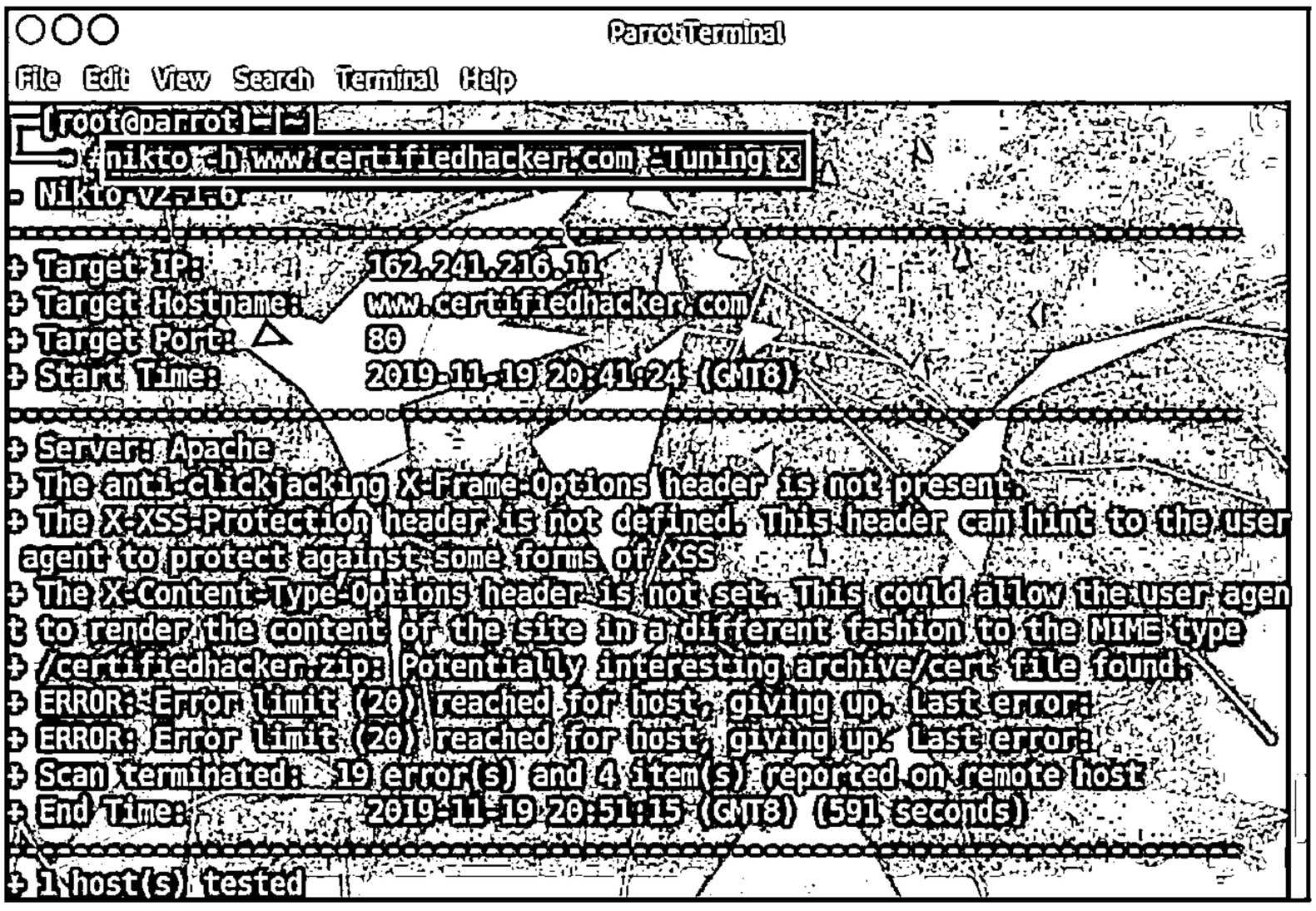


Figure 2.4.4: Nikto scan output

11. Here, we will check for cgi directories with the **-Cgidirs** option. In this option, search for specific directories or use **all** options to search for all the available directories.
12. In the terminal window, type **nikto -h <Target Website> -Cgidirs all**, (here, the target website is **www.certifiedhacker.com**) and hit **Enter**.

Note: **-Cgidirs**: scans the specified CGI directories; users can use filters such as "**none**" or "**all**" to scan all CGI directories or none).

13. The target website does not have any CGI directory; therefore, the same result as the previous scan was obtained.

Note: You can use try this command on another website to obtain information about CGI directories.

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

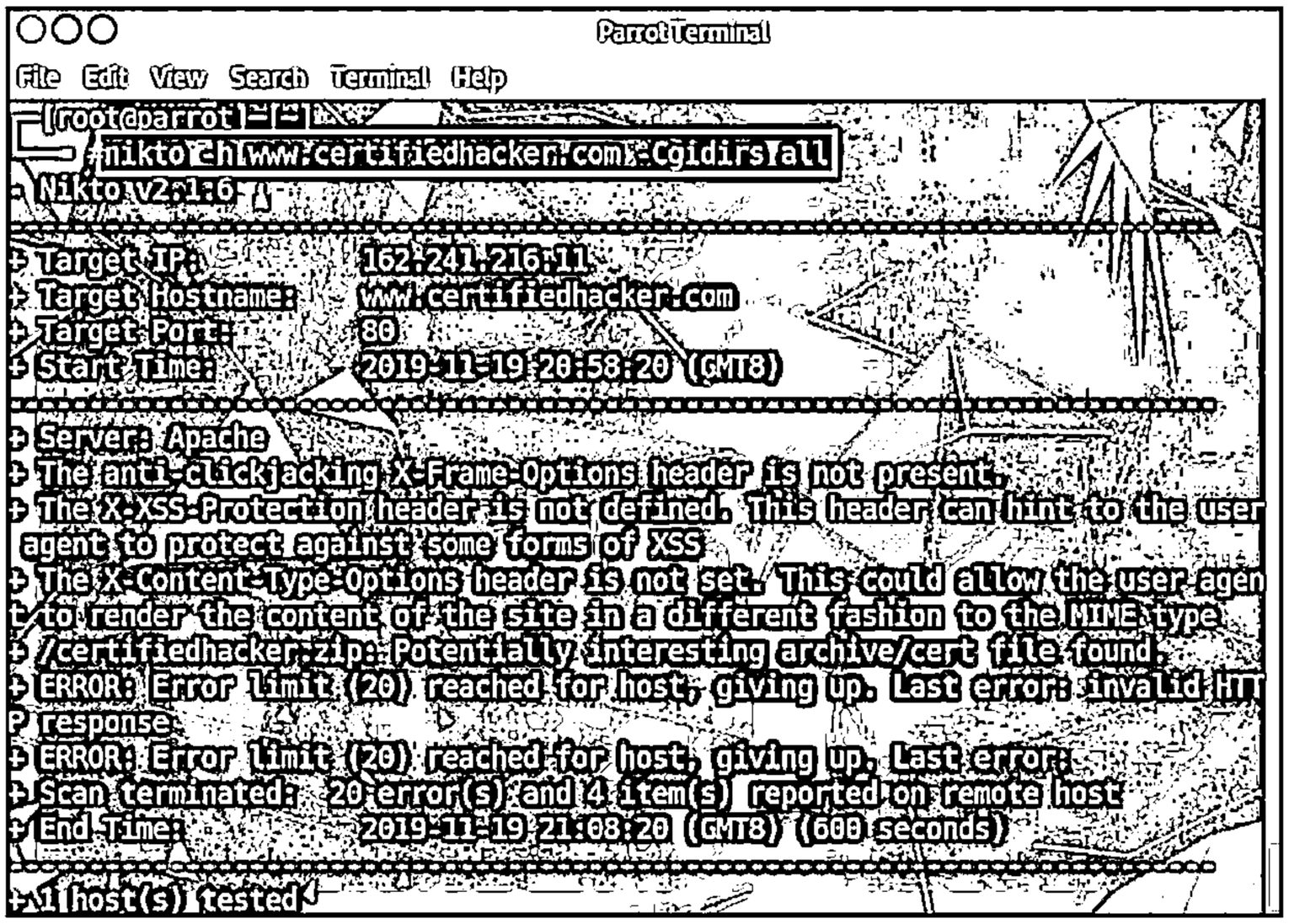


Figure 2.4.5: Nikto option to scan CGI directories

TASK 4.2

Save Scan Results

14. Now, we will save the scan results in the form of a text file on **Desktop**. To do so, type **cd Desktop** and press **Enter**. Type **nikto -h <Target IP Address> -o <File_Name> -F txt** and press **Enter**.

Note: **-h**: specifies the target, **-o**: specifies the name of the output file, and **-F**: specifies the file format.

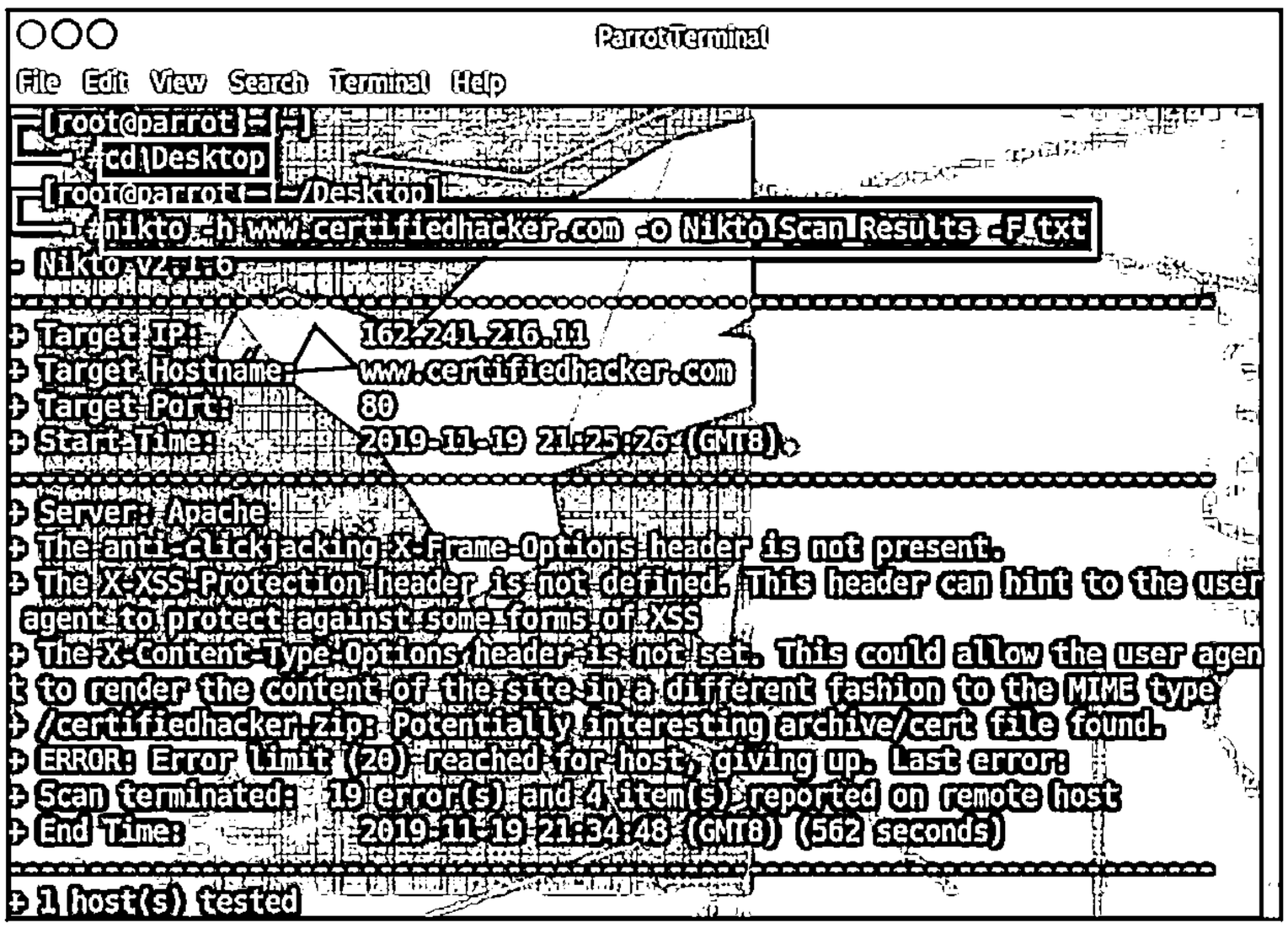


Figure 2.4.6: Saving Vulnerability Analysis Results

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

15. Navigate to **/root/Desktop** and open the **Nikto_Scan_Results** file. The file appears displaying the scanned results.

Note: To navigate to the **Desktop** folder, click **Places** from the top-section of the **Desktop** and click **Home Folder** from the drop-down options. In the **attacker** window, click **File System** from the left-pane and navigate to the location **/root/Desktop**

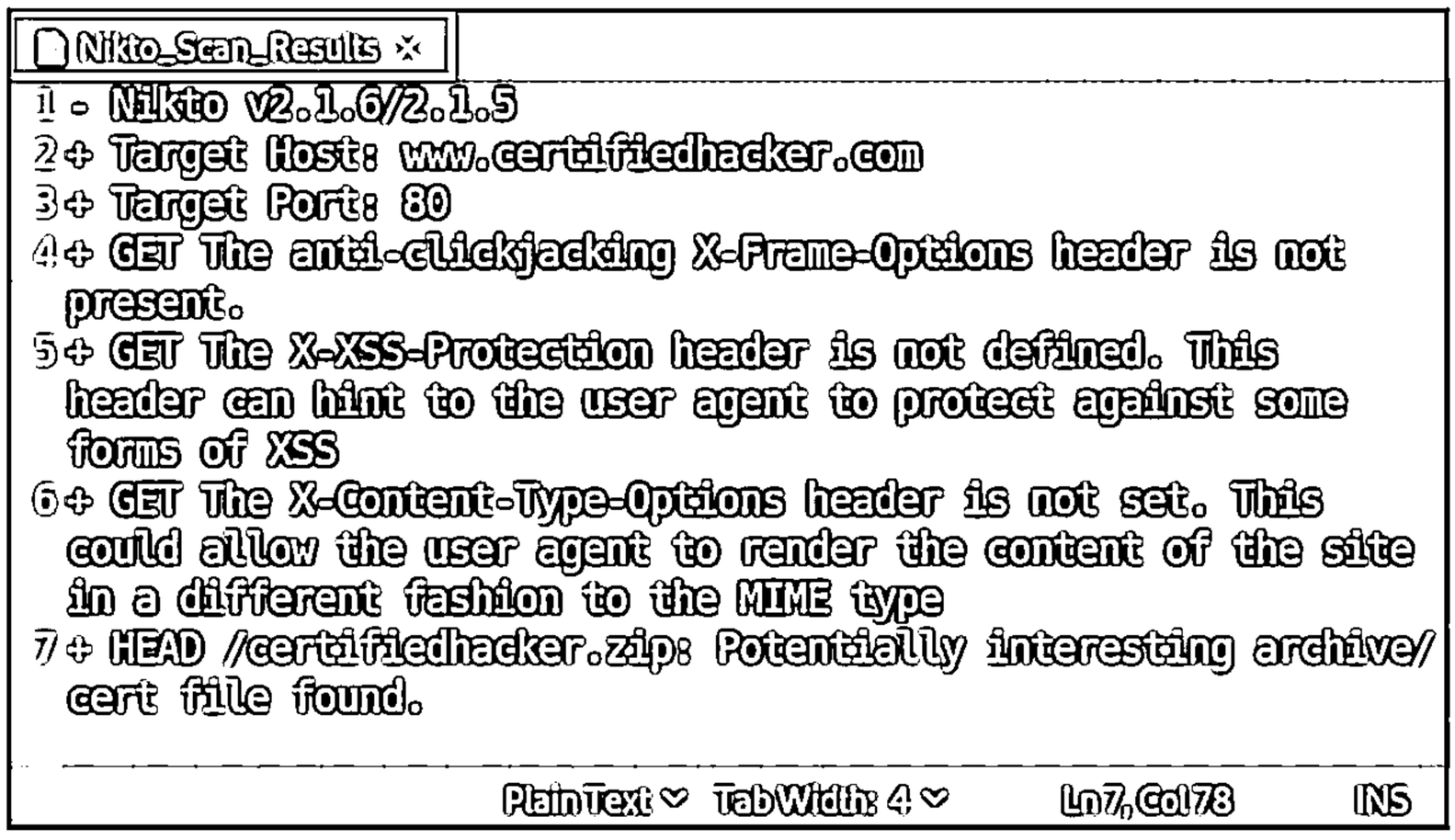


Figure 2.4.7: Nikto Scan Results File

16. This concludes the demonstration of checking vulnerabilities in the target website using Nikto.
17. Close all open windows and document all the acquired information.
18. Turn off the **Parrot Security** virtual machine.

Lab Analysis

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

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT 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.