OLD DOMINION UNIVERSITY

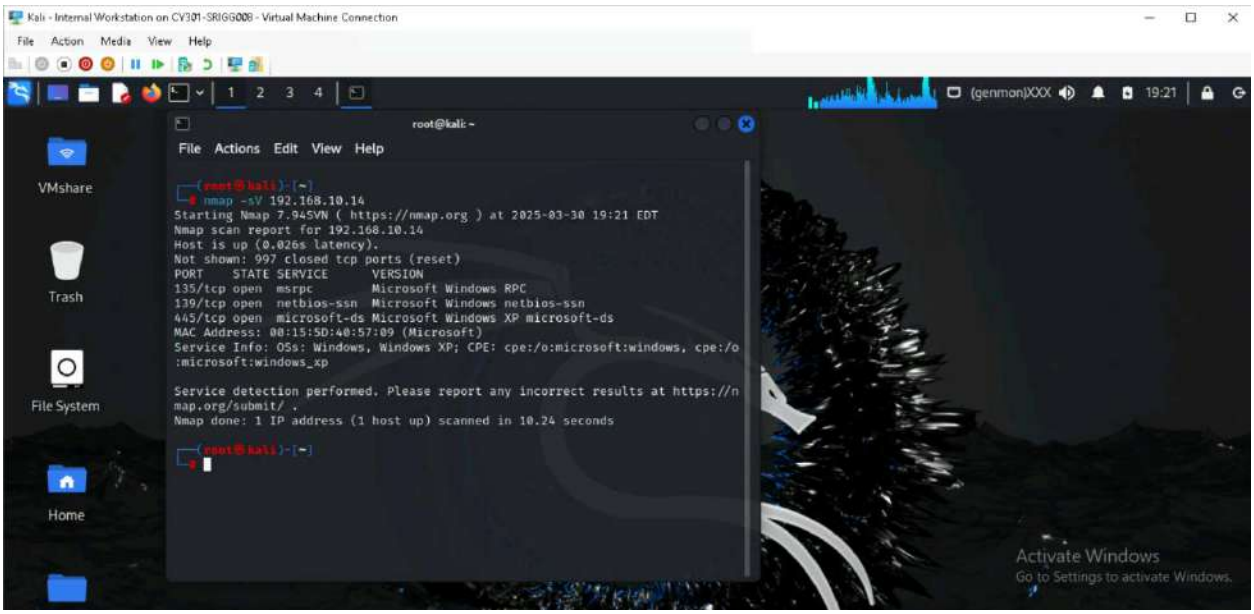
CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

ASSIGNMENT 4 – ETHICAL HACKING

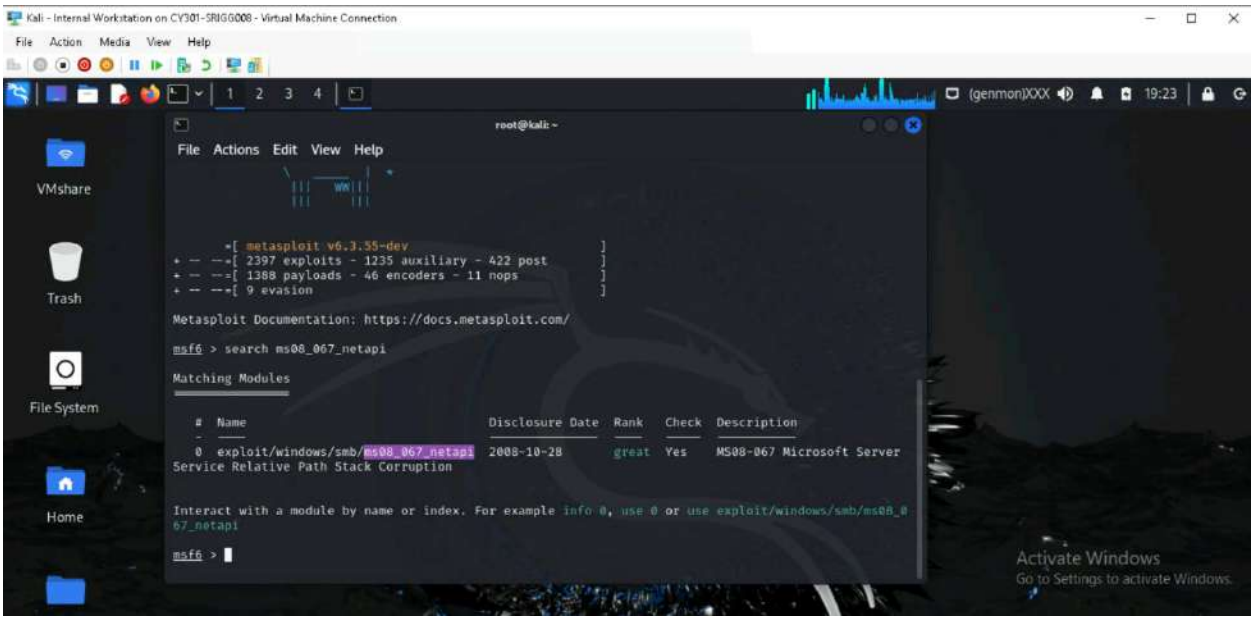
Samantha Riggs

TASK A: EXPLOIT SMB ON WINDOWS XP WITH METASPLOIT

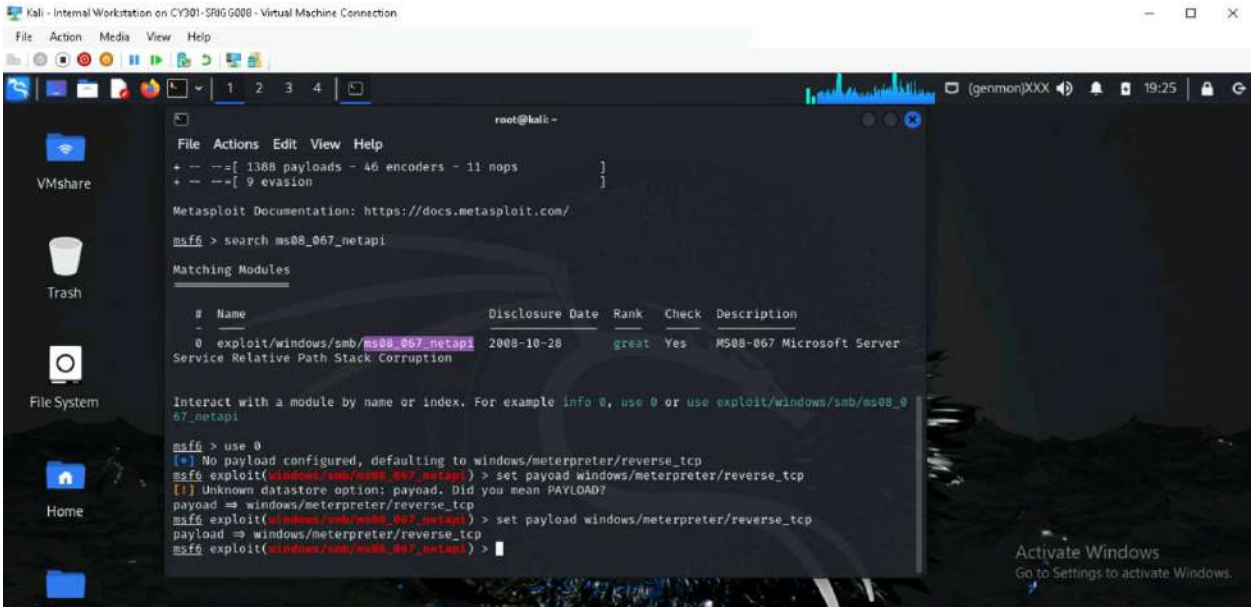
1-2. Run a port scan against Windows XP, identify SMB port number, and confirm it is open:



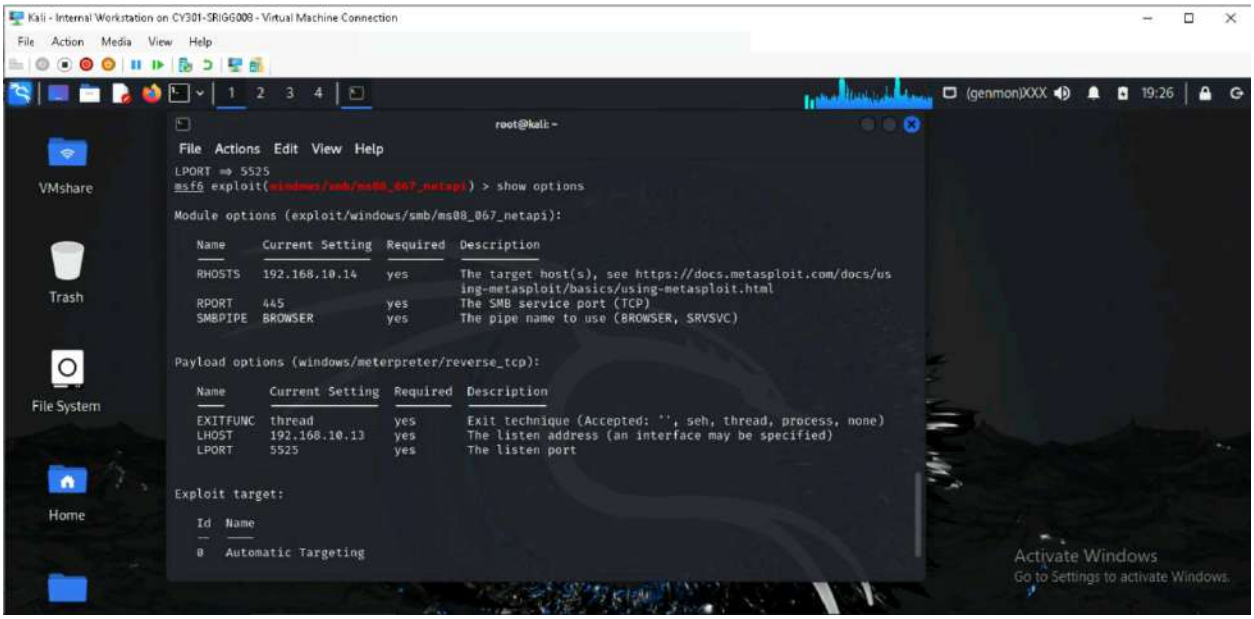
3. Search for exploit module ms08_067_netapi:

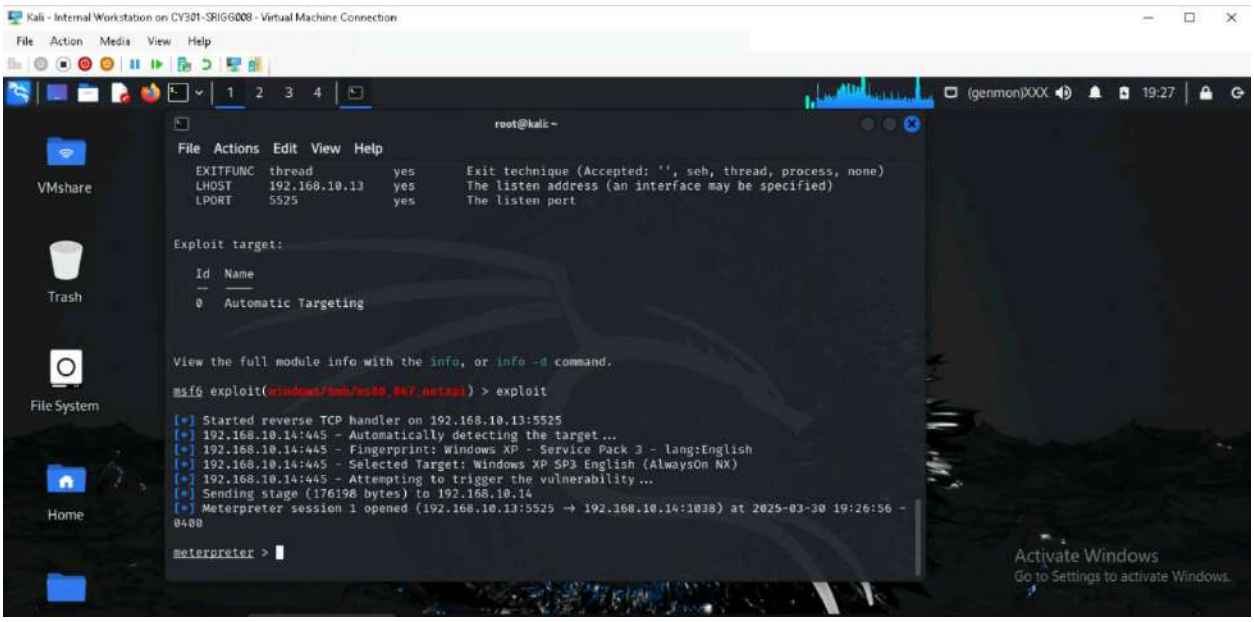


4. Set payload:

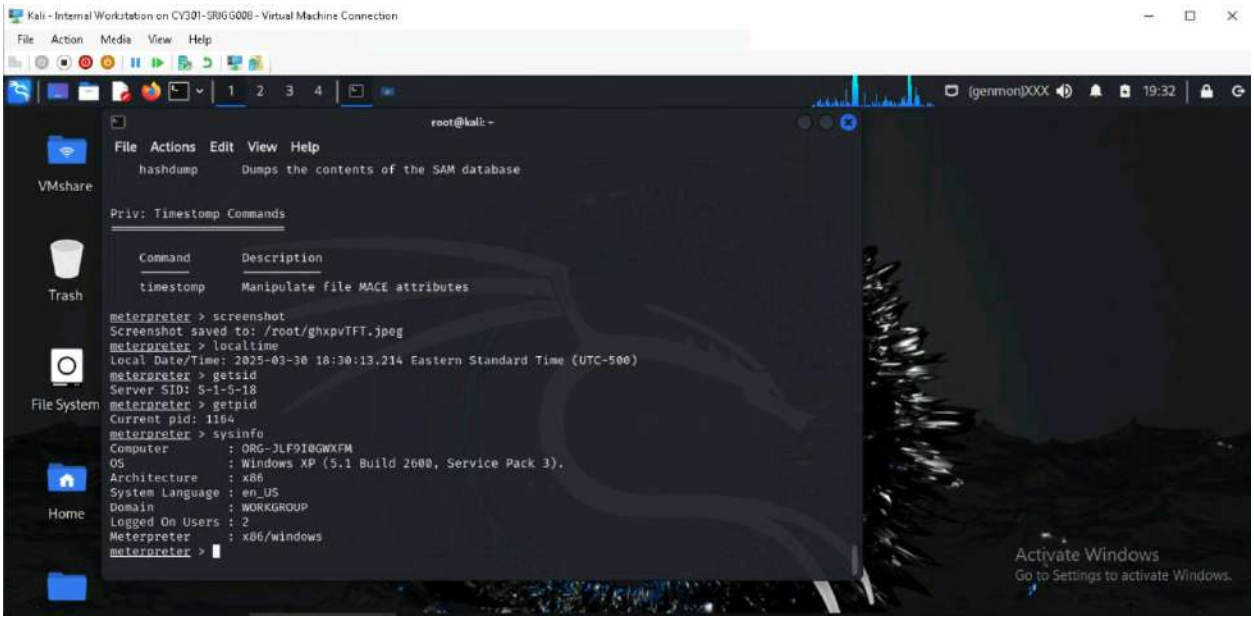


5. Configure exploit module and exploit the target:



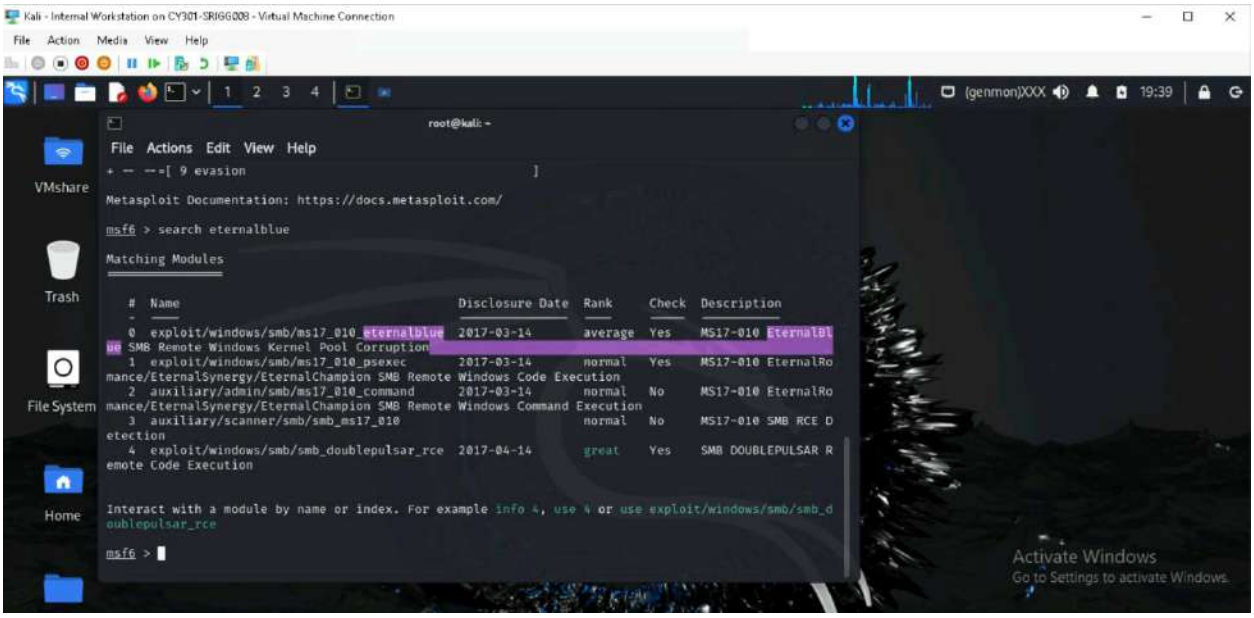


6-10. Display the target system's local date and time, SID, PID, and system information:

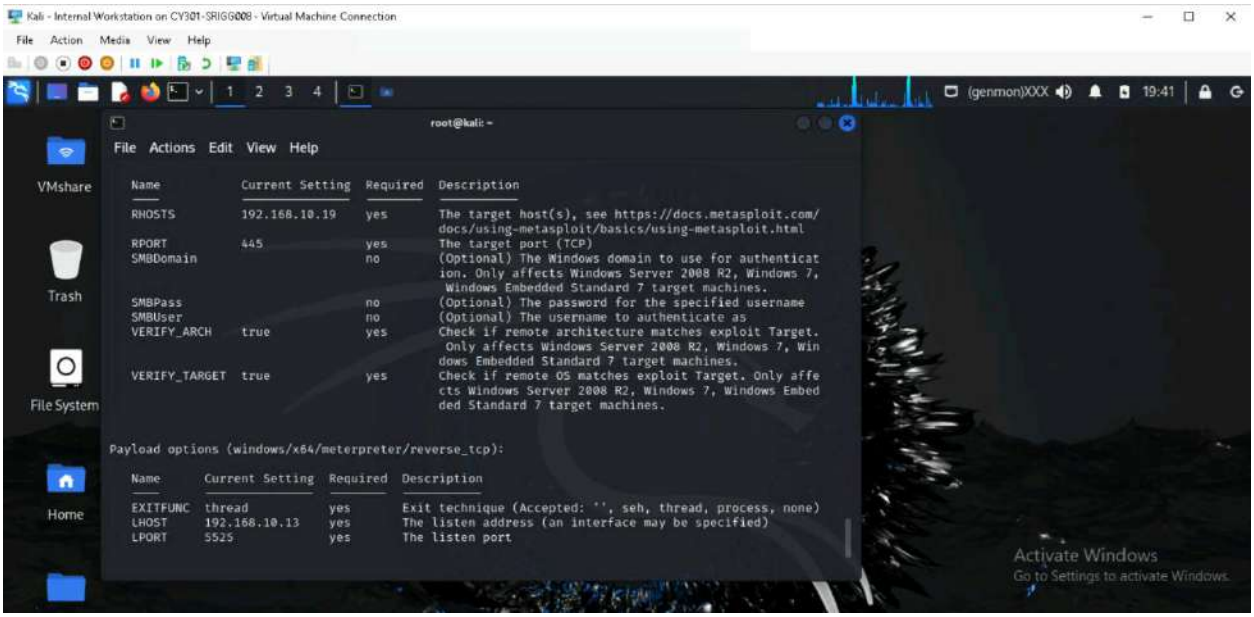


TASK B: EXPLOIT ETERNALBLUE ON WINDOWS SERVER 2022 WITH METASPLOIT

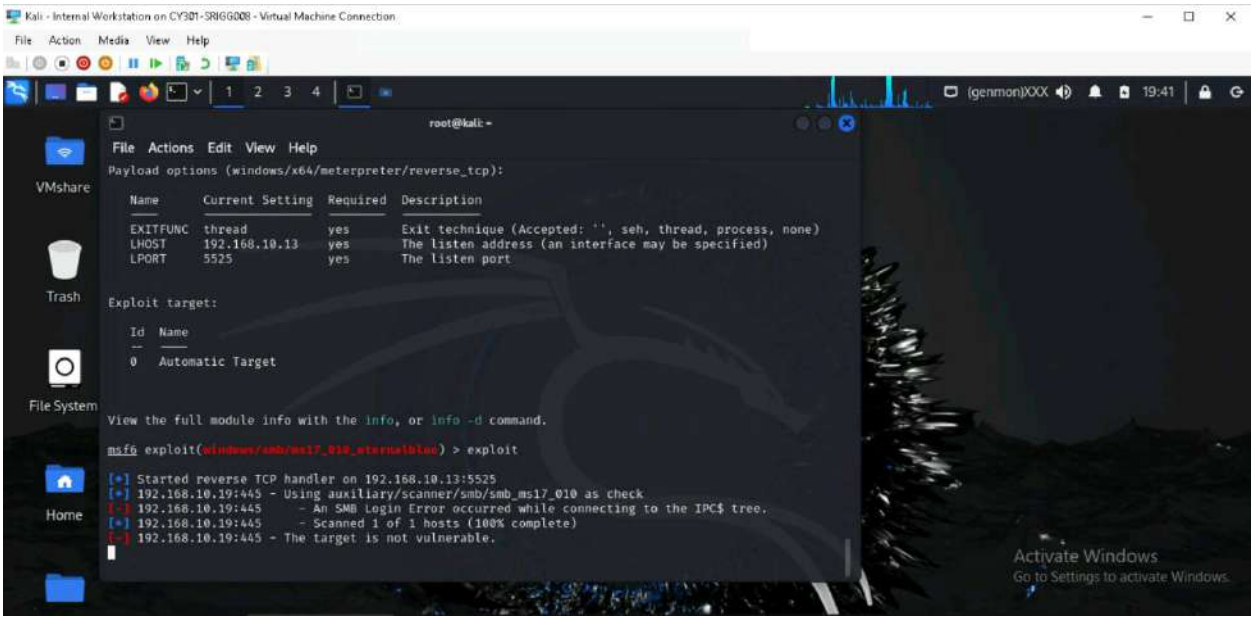
Search for exploit module eternal blue:



Exploit configuration:

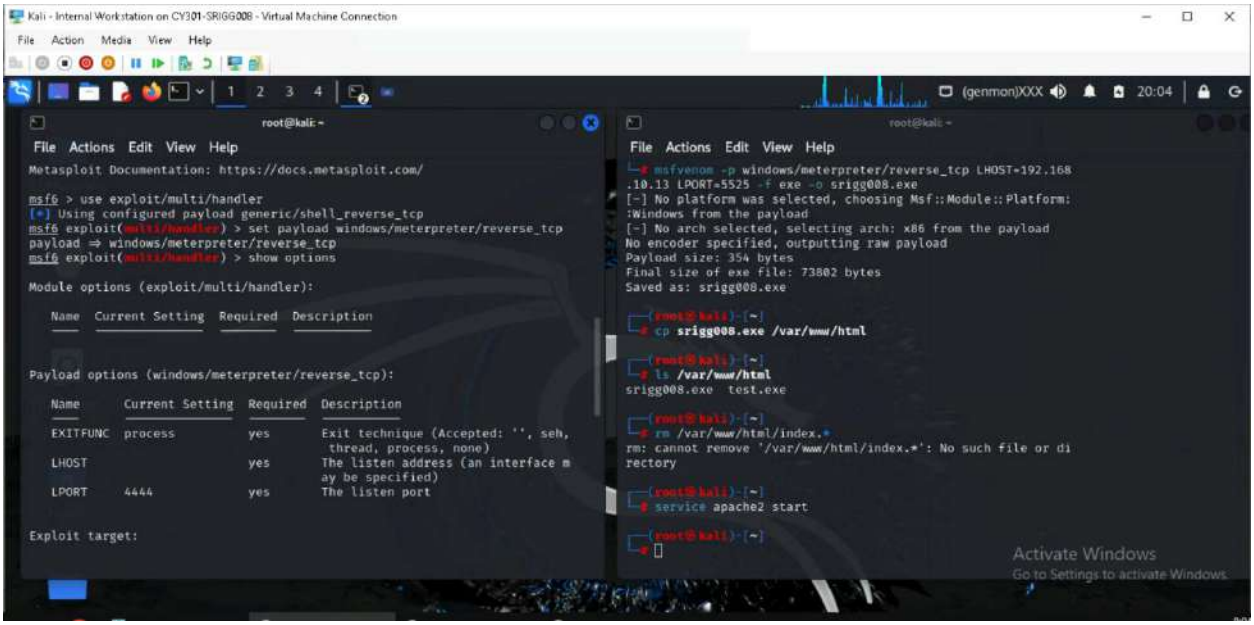


Attempt exploitation:

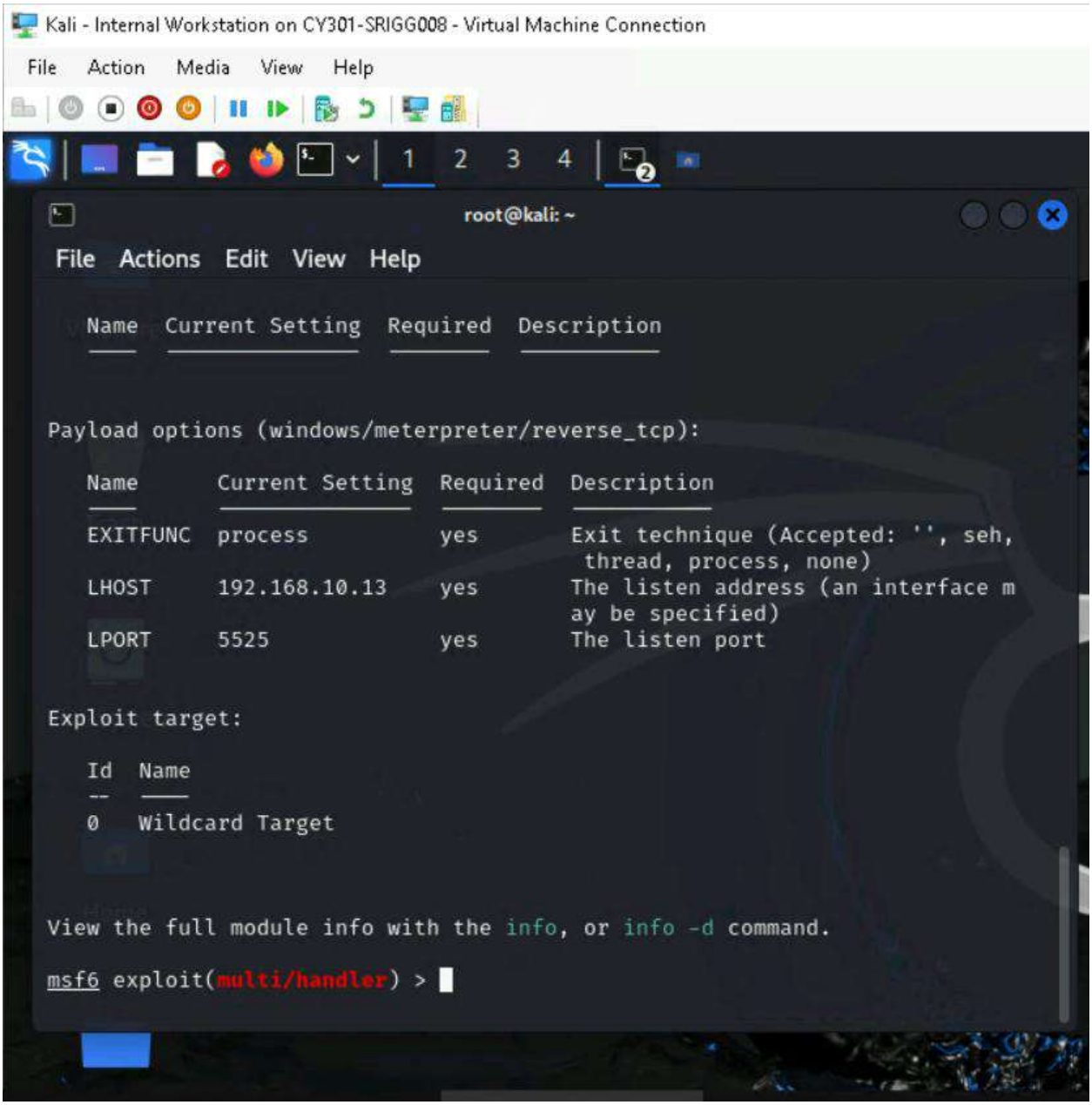


TASK C: EXPLOIT WINDOWS 7 WITH A DELIVERABLE PAYLOAD

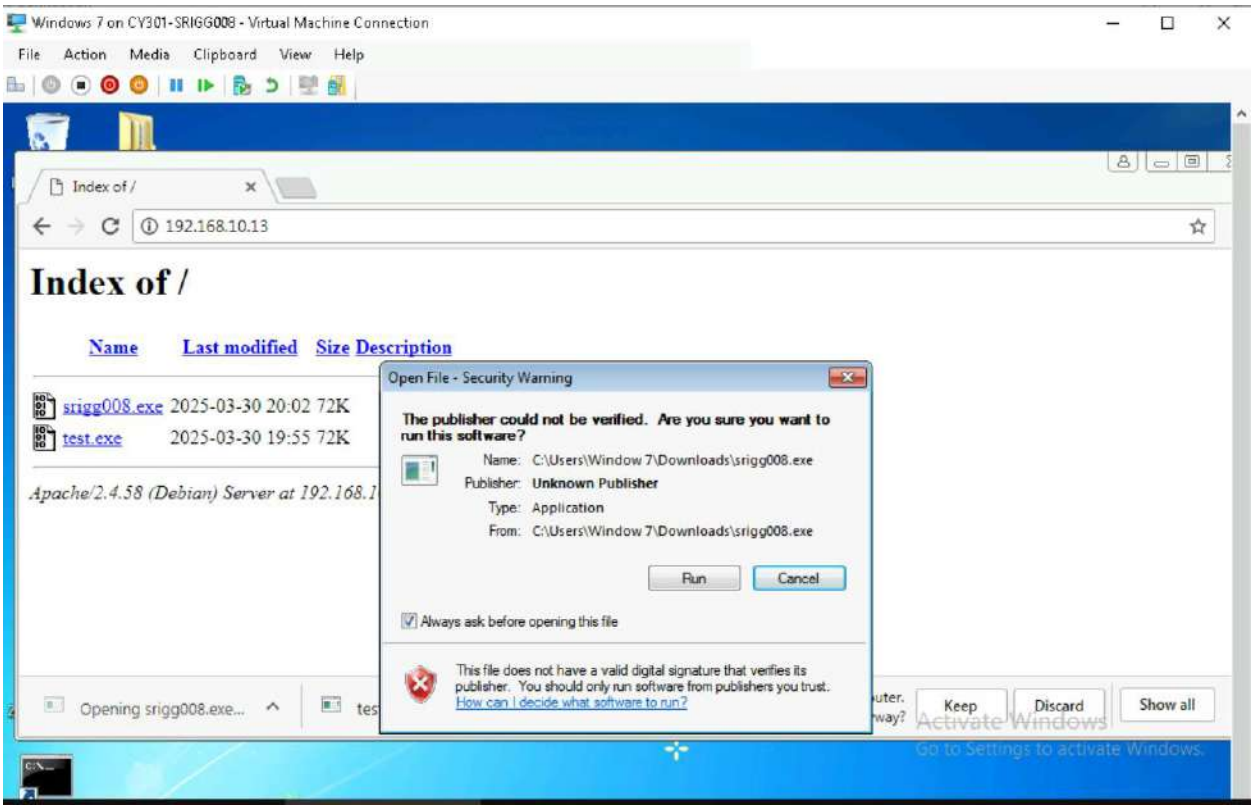
1. **Create an executable payload:**



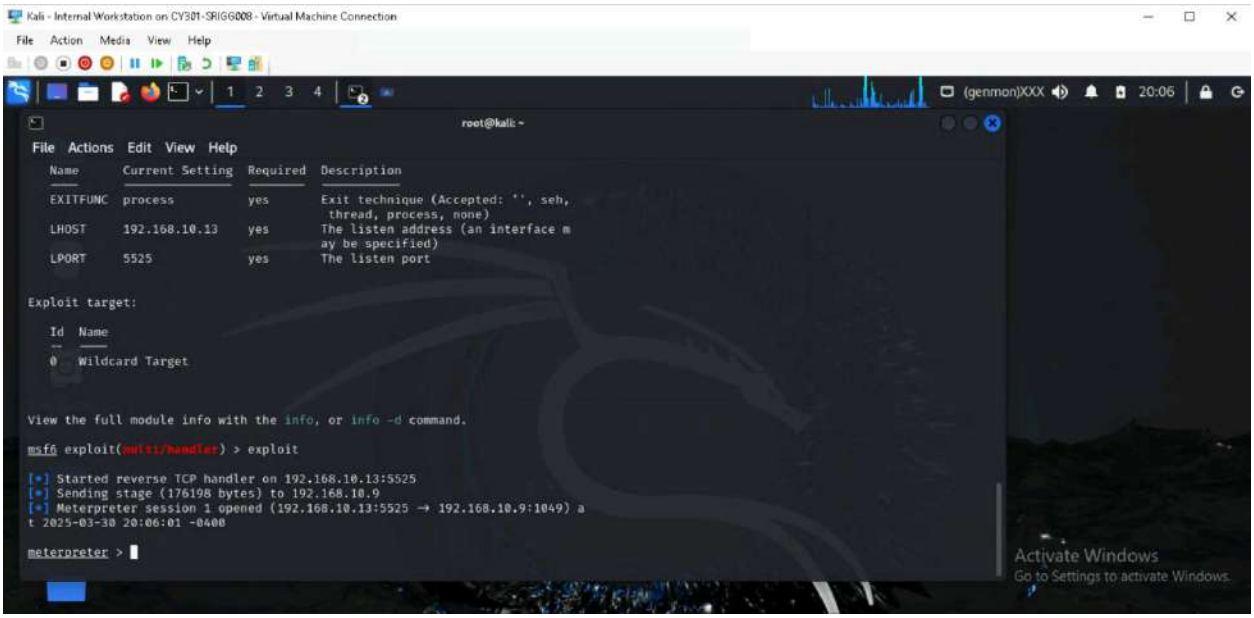
Payload configuration:



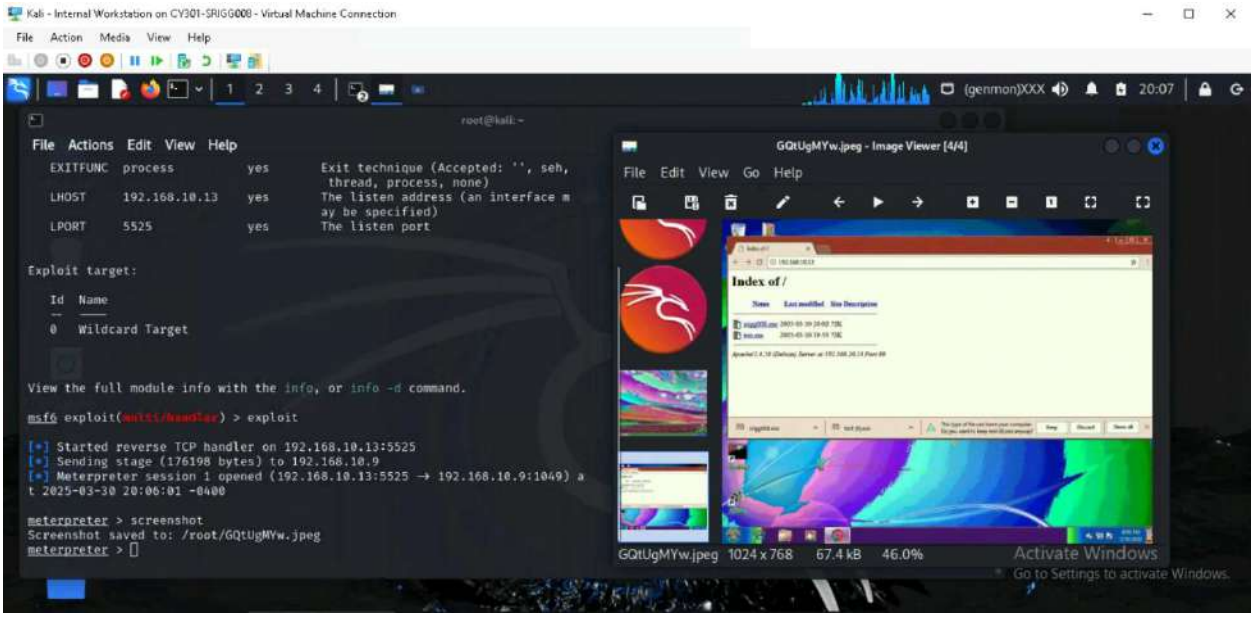
Run the payload on the target system:



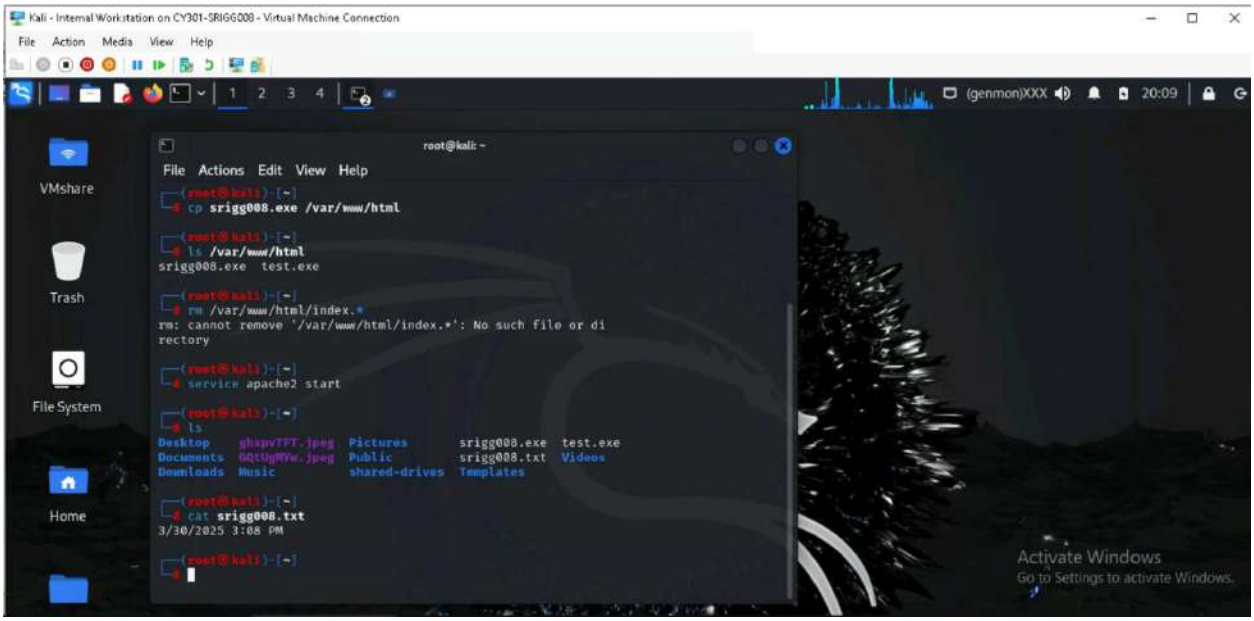
Successful exploit:

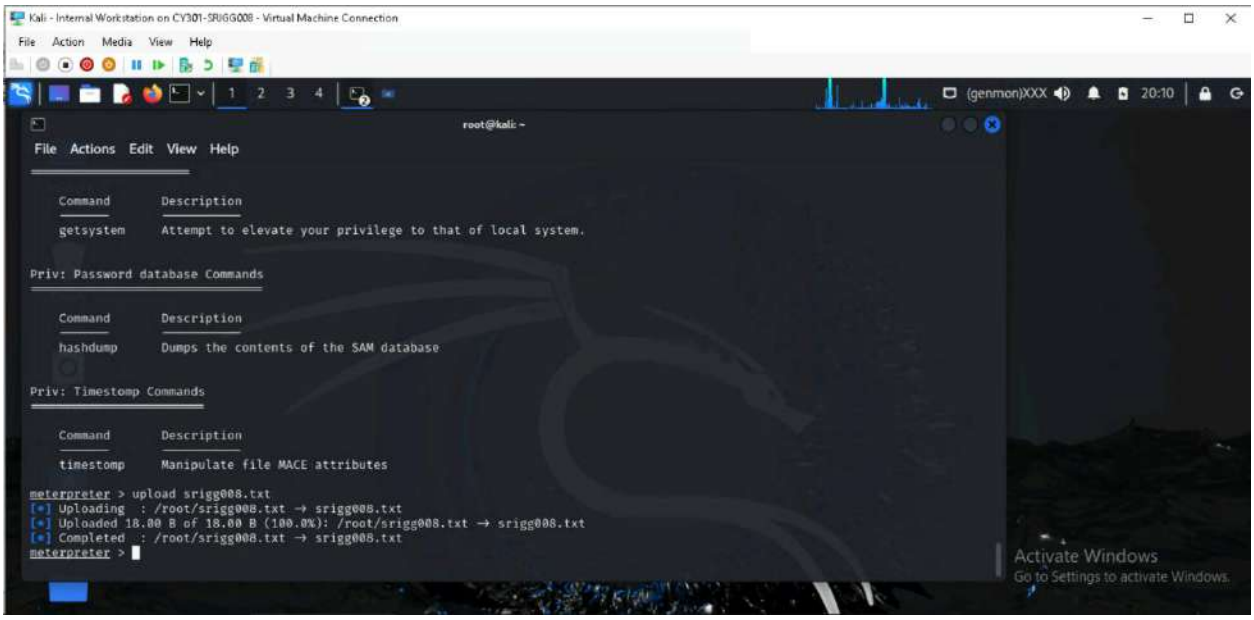


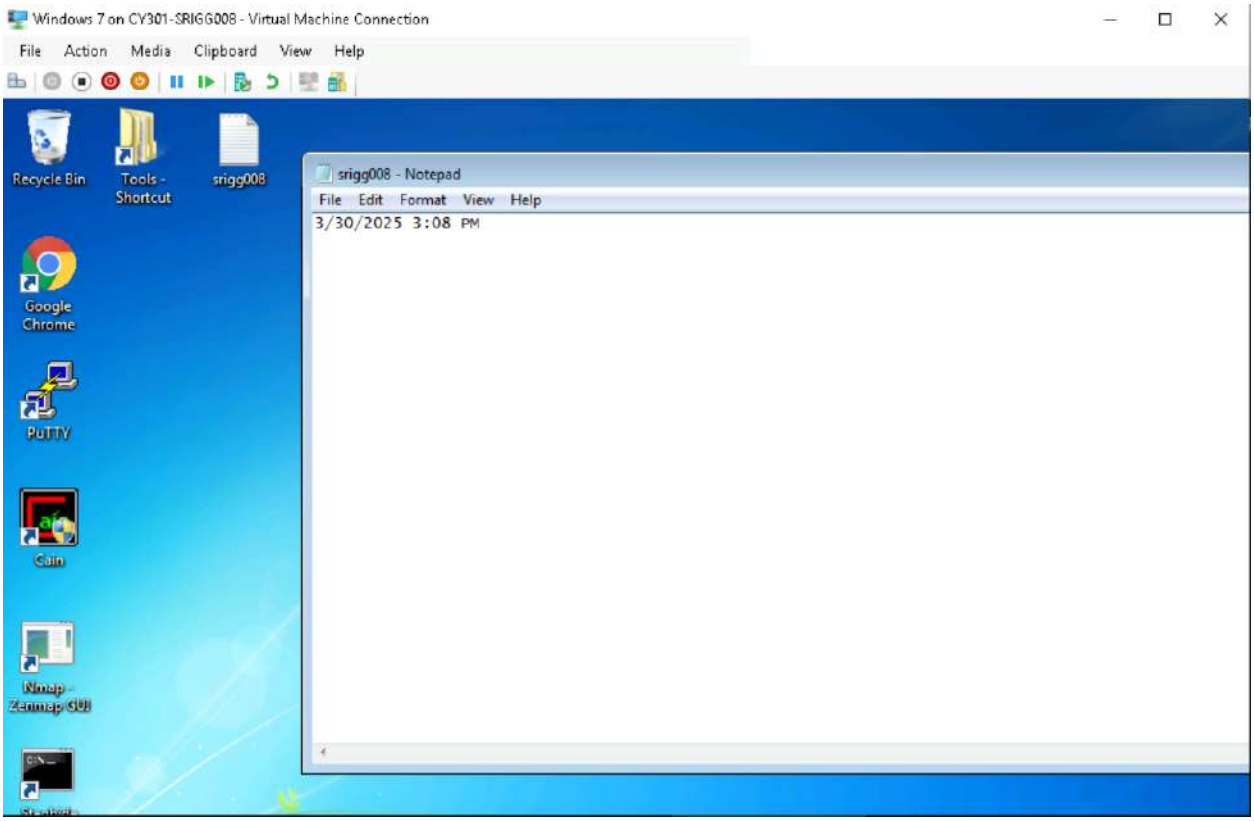
2. Execute the screenshot command:



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

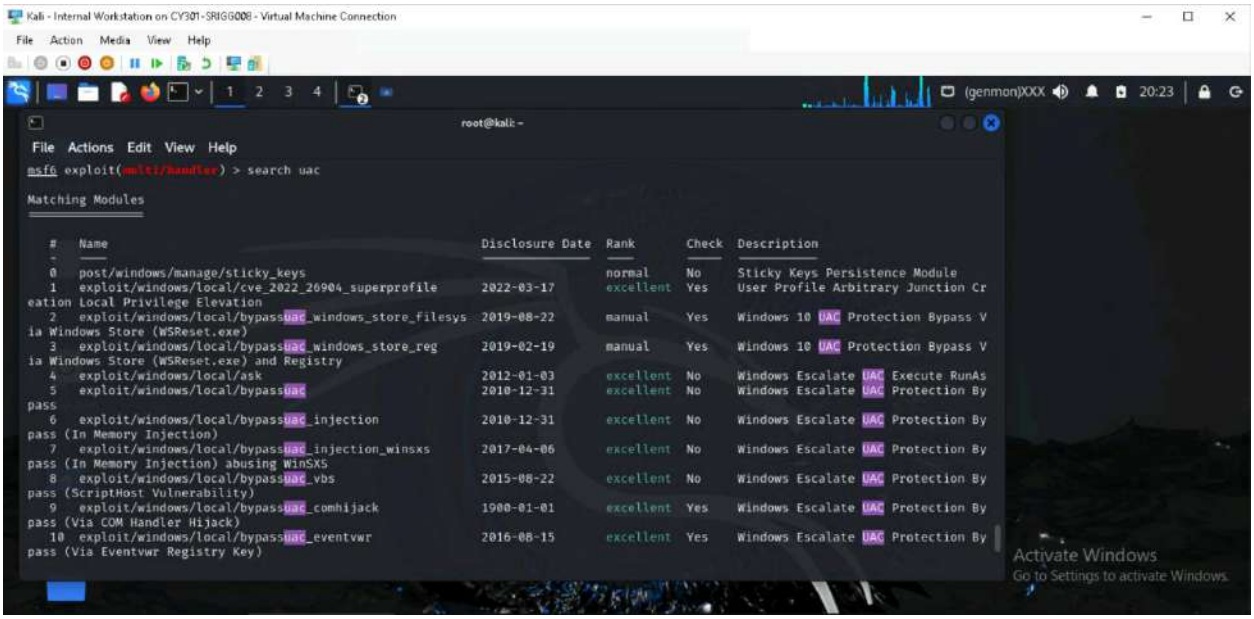



Kali - Internal Workstation on CY301-SRIGG008 - Virtual Machine Connection
File Action Media View Help
root@kali: ~
File Actions Edit View Help
Command Description
getsystem Attempt to elevate your privilege to that of local system.
Priv: Password database Commands
Command Description
hashdump Dumps the contents of the SAM database
Priv: Timestomp Commands
Command Description
timestomp Manipulate file MACE attributes
meterpreter > upload srigg008.txt
[*] Uploading : /root/srigg008.txt → srigg008.txt
[*] Uploaded 18.00 B of 18.00 B (100.0%): /root/srigg008.txt → srigg008.txt
[*] Completed : /root/srigg008.txt → srigg008.txt
meterpreter >
Activate Windows
Go to Settings to activate Windows.

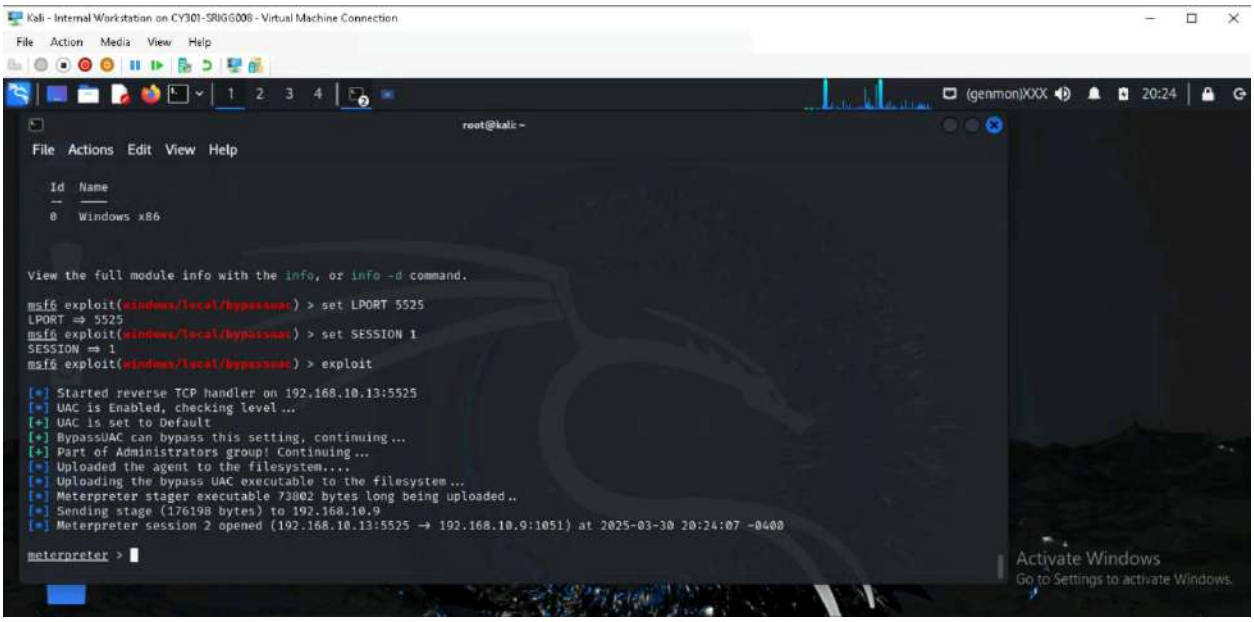

Windows 7 on CY301-SRIGG008 - Virtual Machine Connection
File Action Media Clipboard View Help
Recycle Bin
Tools - Shortcut
srigg008
Google Chrome
PuTTY
Cain
Nmap - Zenmap GUI
srigg008 - Notepad
File Edit Format View Help
3/30/2025 3:08 PM

4. Gain administrator-level privileges.

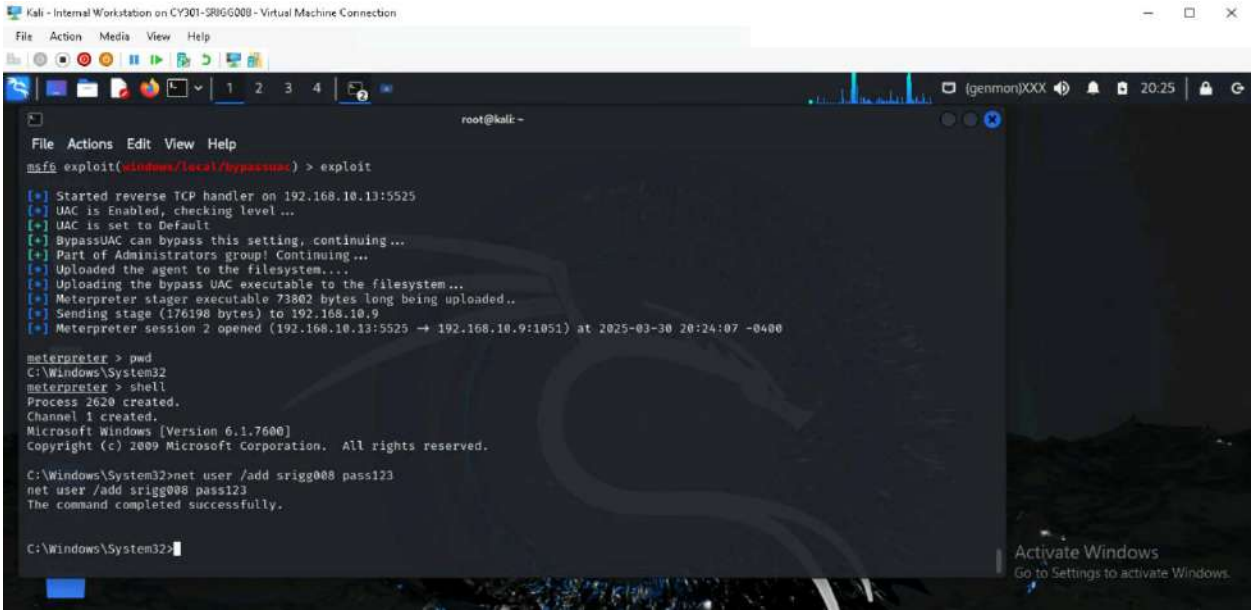
Search for uac exploit modules:



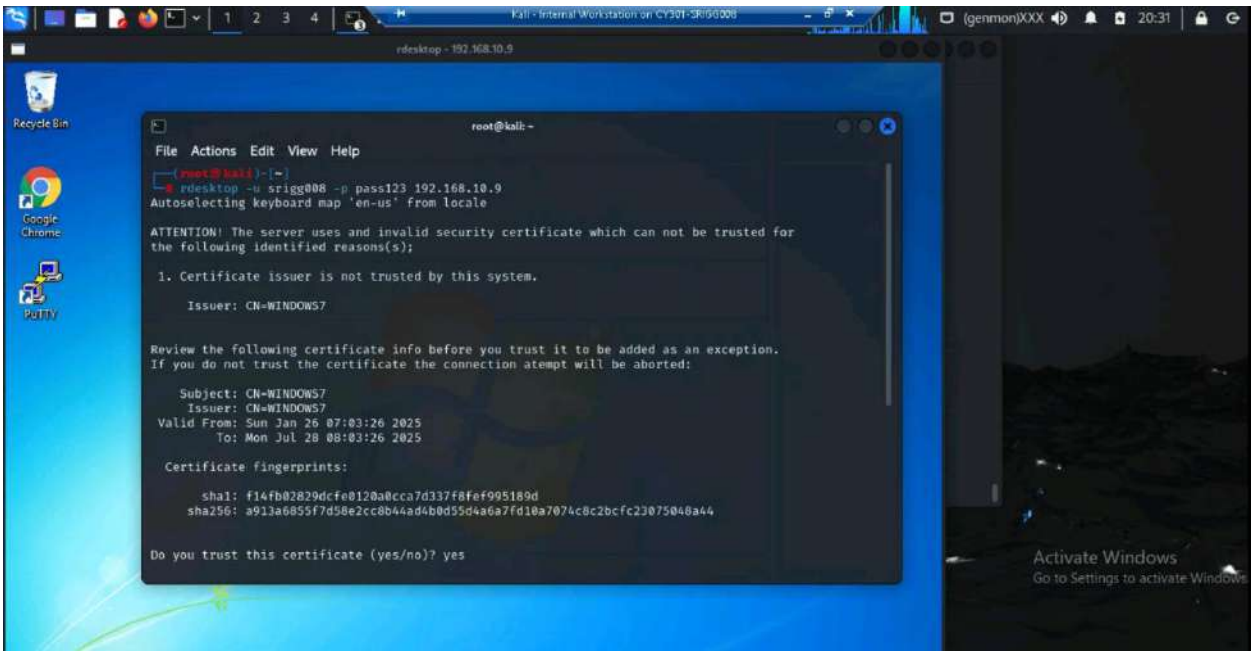
Configure and run the module:

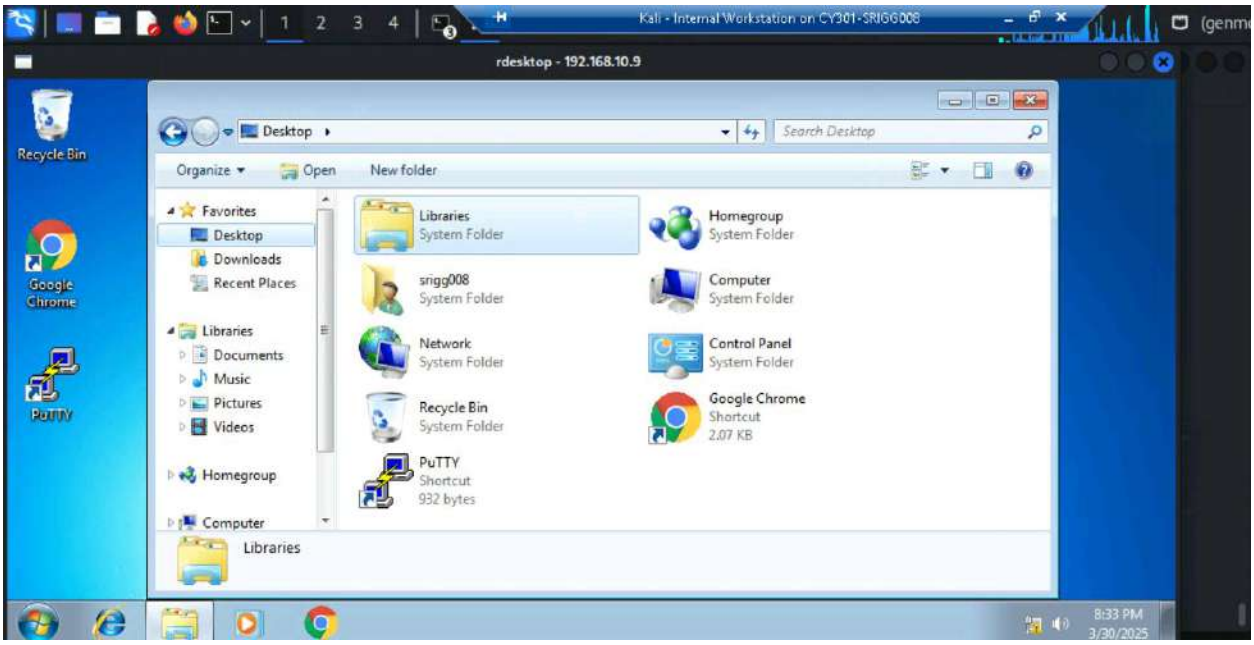


Gain administrative privileges and create a malicious account:



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




Kali - Internal Workstation on CY301-SRIG0008
rdesktop - 192.168.10.9
Recycle Bin
Google Chrome
PuTTY
Desktop
Search Desktop
Organize
Open
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Homegroup
Computer
Libraries
System Folder
Homegroup
System Folder
srigg008
System Folder
Computer
System Folder
Network
System Folder
Control Panel
System Folder
Recycle Bin
System Folder
Google Chrome
Shortcut
2.07 KB
PuTTY
Shortcut
932 bytes
8:33 PM
3/30/2025