CYSE 301: Cybersecurity Technique and Operations

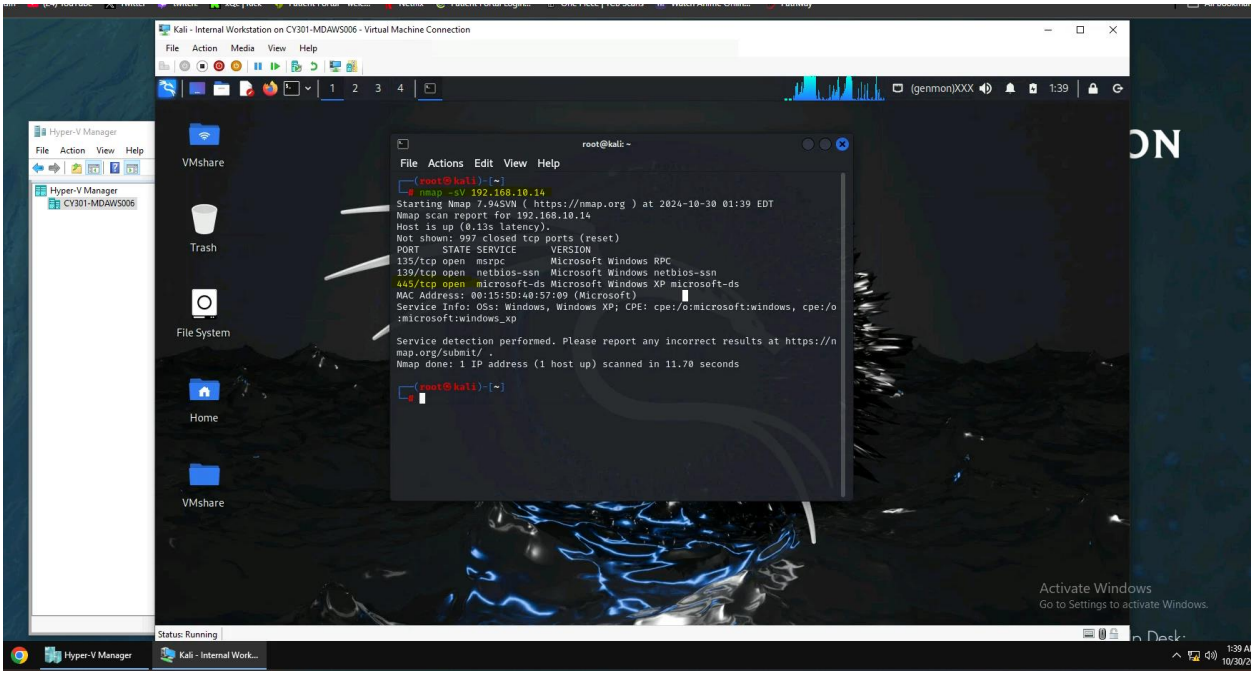
Assignment 4: Ethical Hacking

Michael Dawson

Task A: Exploit SMB on Windows XP with Metasploit

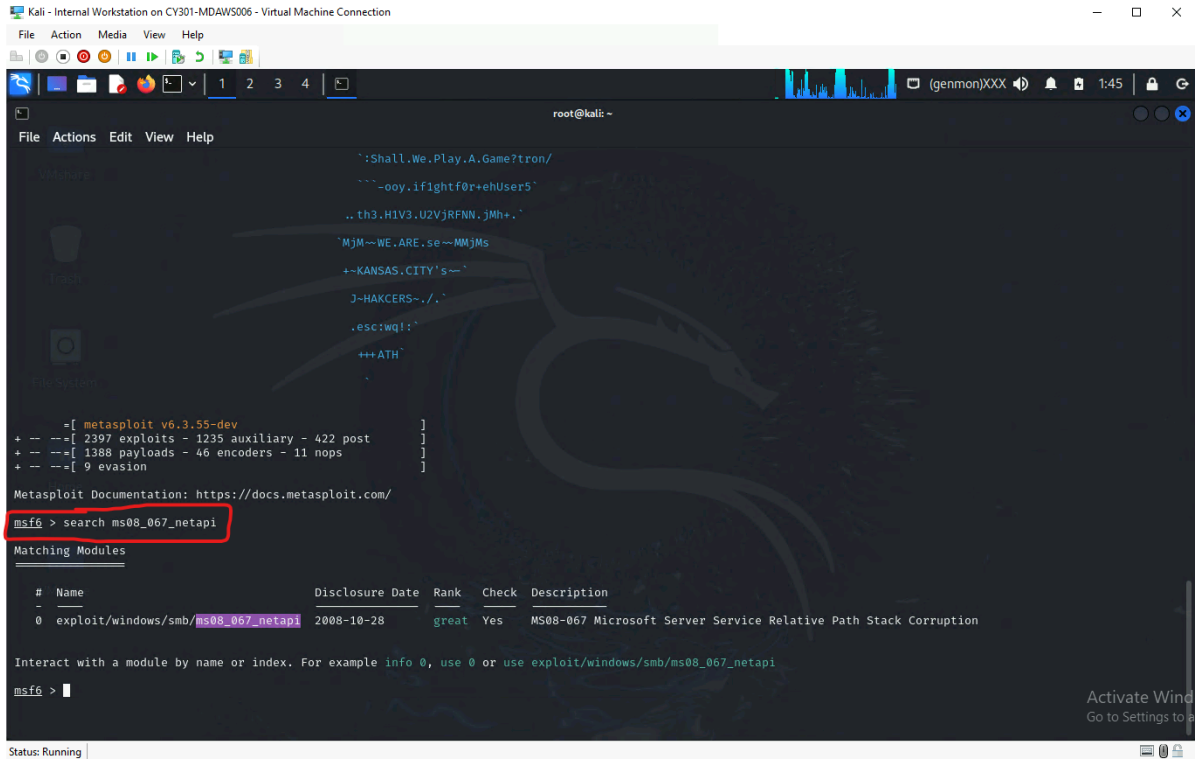
1. Run a port scan against the Windows XP using the nmap command to identify open ports and services.

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

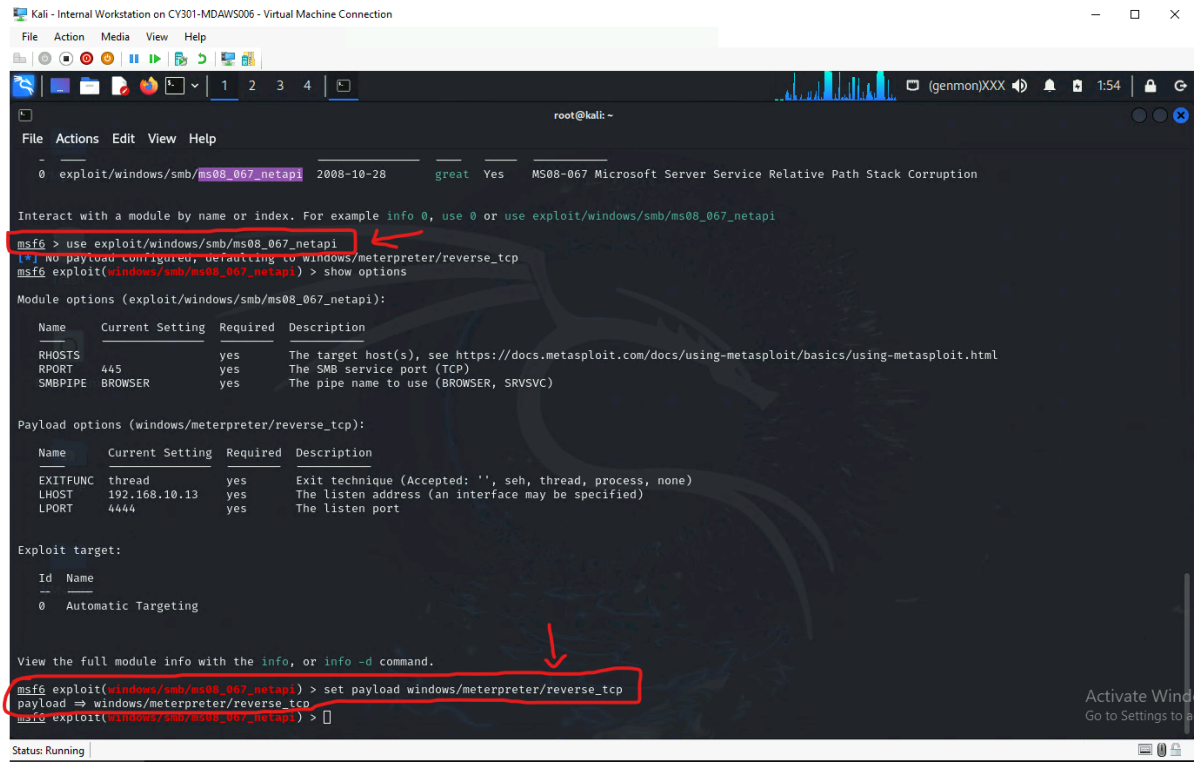


I ran an Nmap scan against the Windows XP server to identify port 445 is open

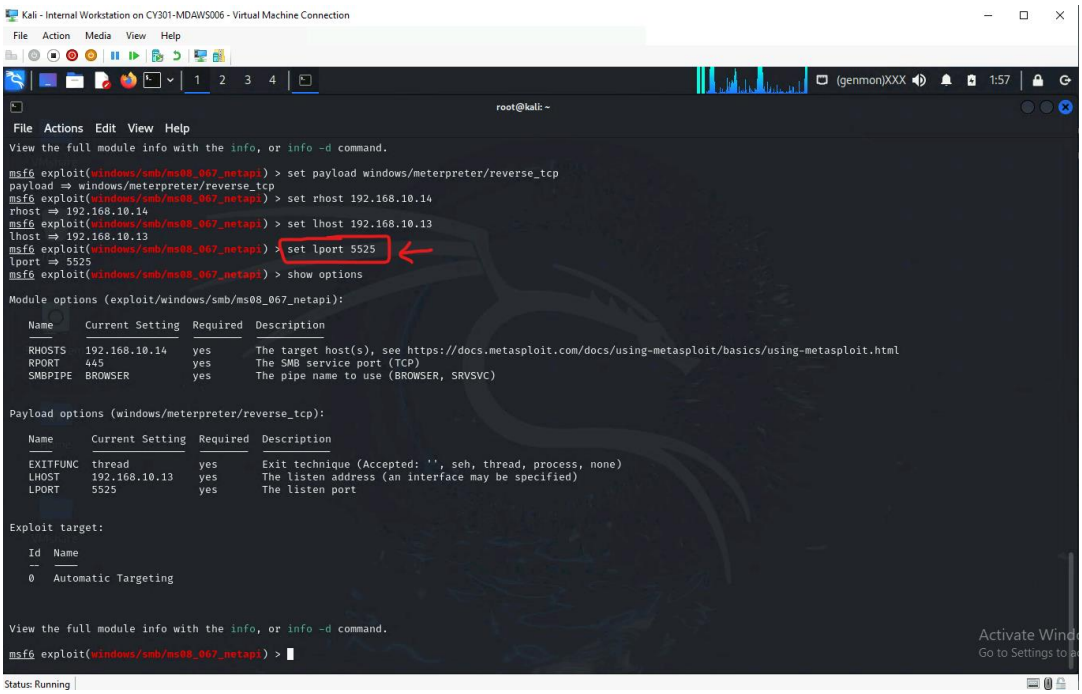
3. Launch Metasploit Framework and search for the exploit module: *ms08_067_netapi*



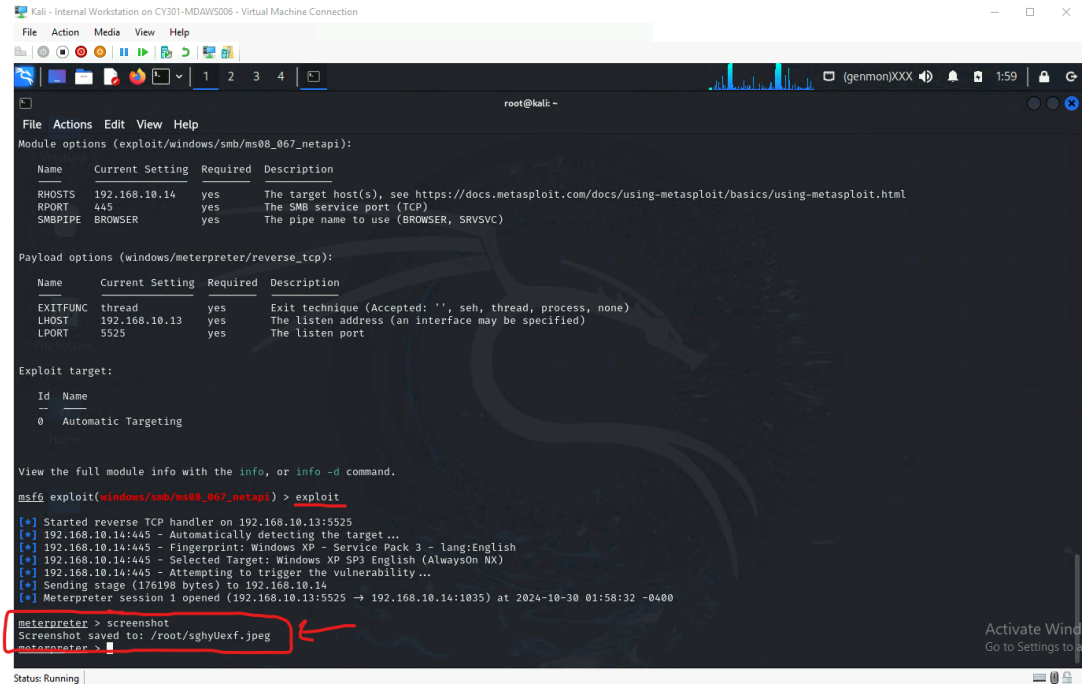
4. Use ms08_067_netapi as the exploit module and set meterpreter reverse_tcp as the payload.



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.

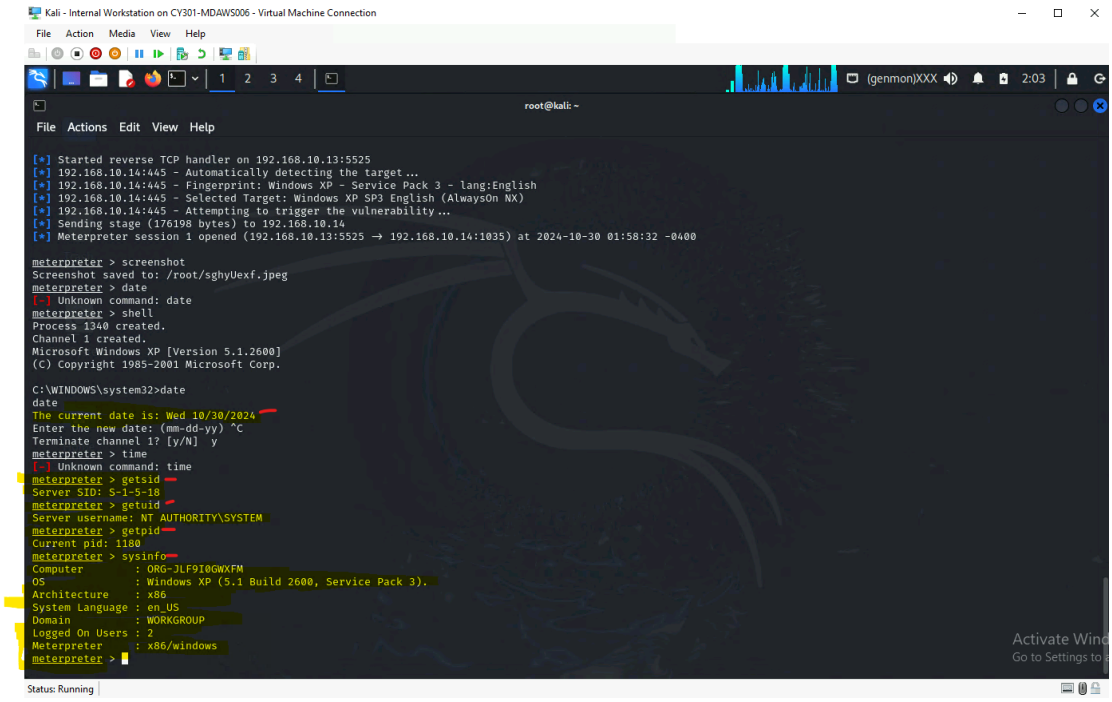


7. [Post-exploitation] In the meterpreter shell, display the target system's local date and time.

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

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

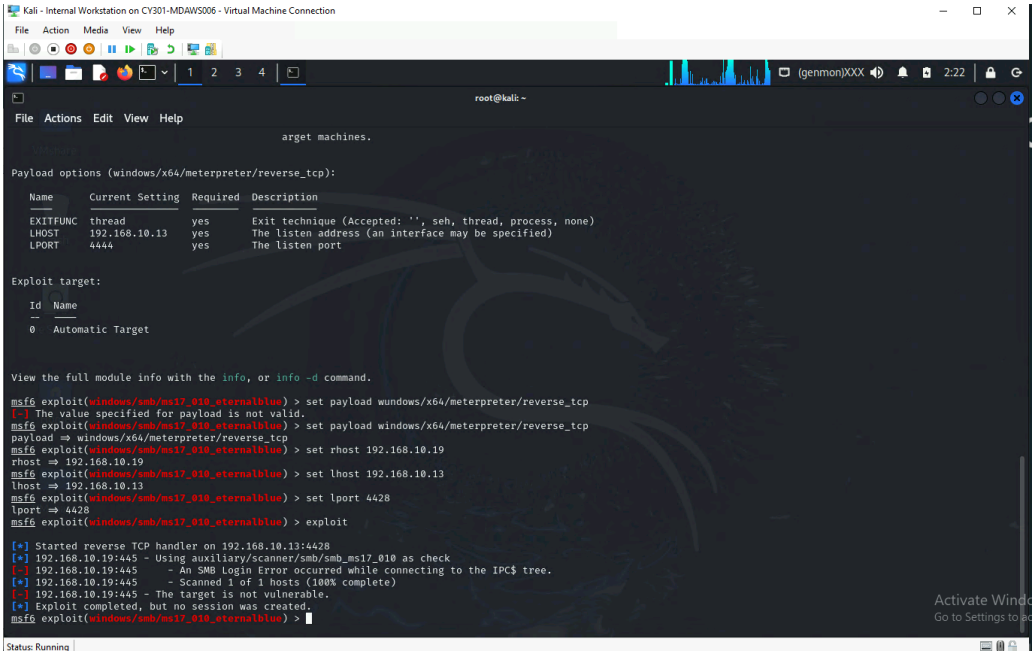
10. [Post-exploitation] In the meterpreter shell, get system information about the target.



Task B: Exploit EternalBlue on Windows Server 2022 with Metasploit

In this task, try to use the same steps as shown in the video 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 using the same method as hacking Windows

Server 2008. Document your steps and show me your results.



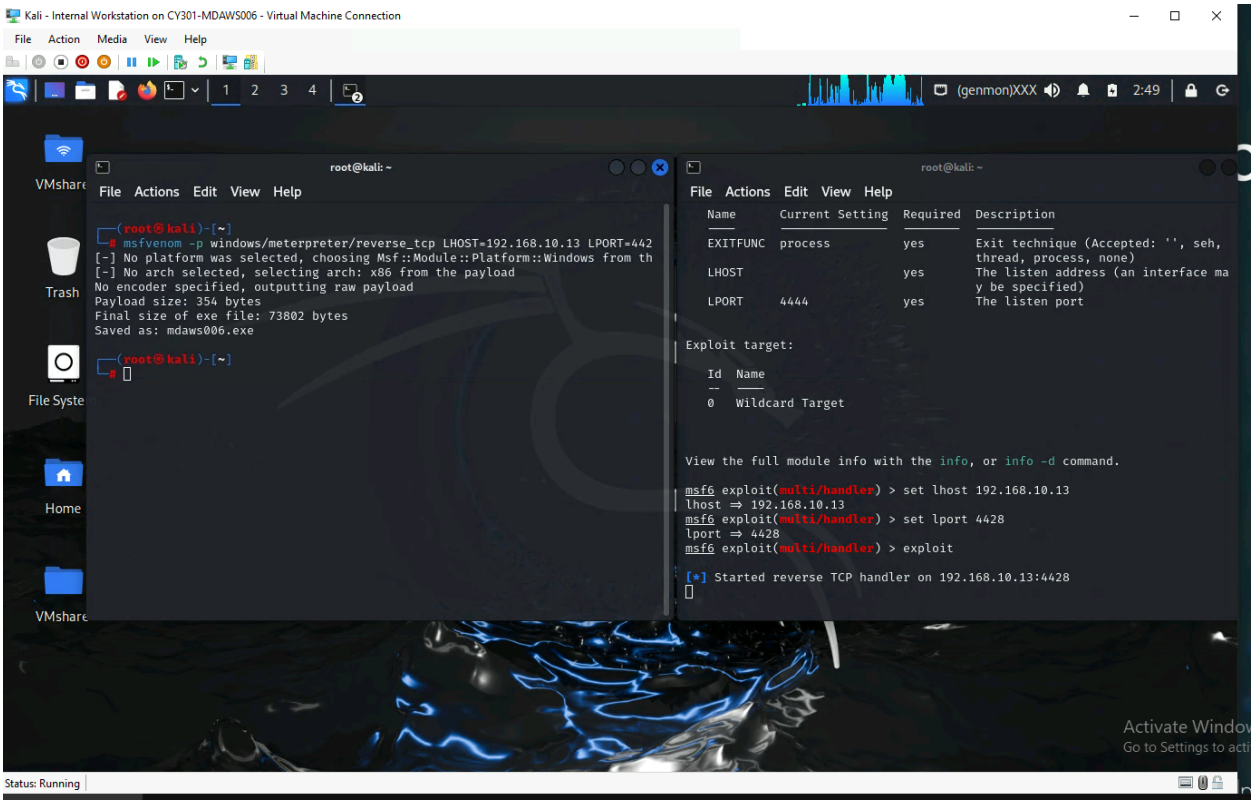
- I opened msfconsole
- I searched for eternal blue
- I used eternal blue and set the payload to meterpreter reverse_tcp
- I set the rhost as the windows 2022 server ip which is 192.168.10.19 and the lhost to the internal kali station which I am exploiting from which is 192.168.10.13.
- I set the lport to 4428
- Then I exploited

Task C: Exploit Windows 7 with a deliverable payload

1. 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. Of course, don't forget to configure your Metasploit on Kali Linux before the payload is triggered on the target VM. (10 pt).

The requirements for your payload are:

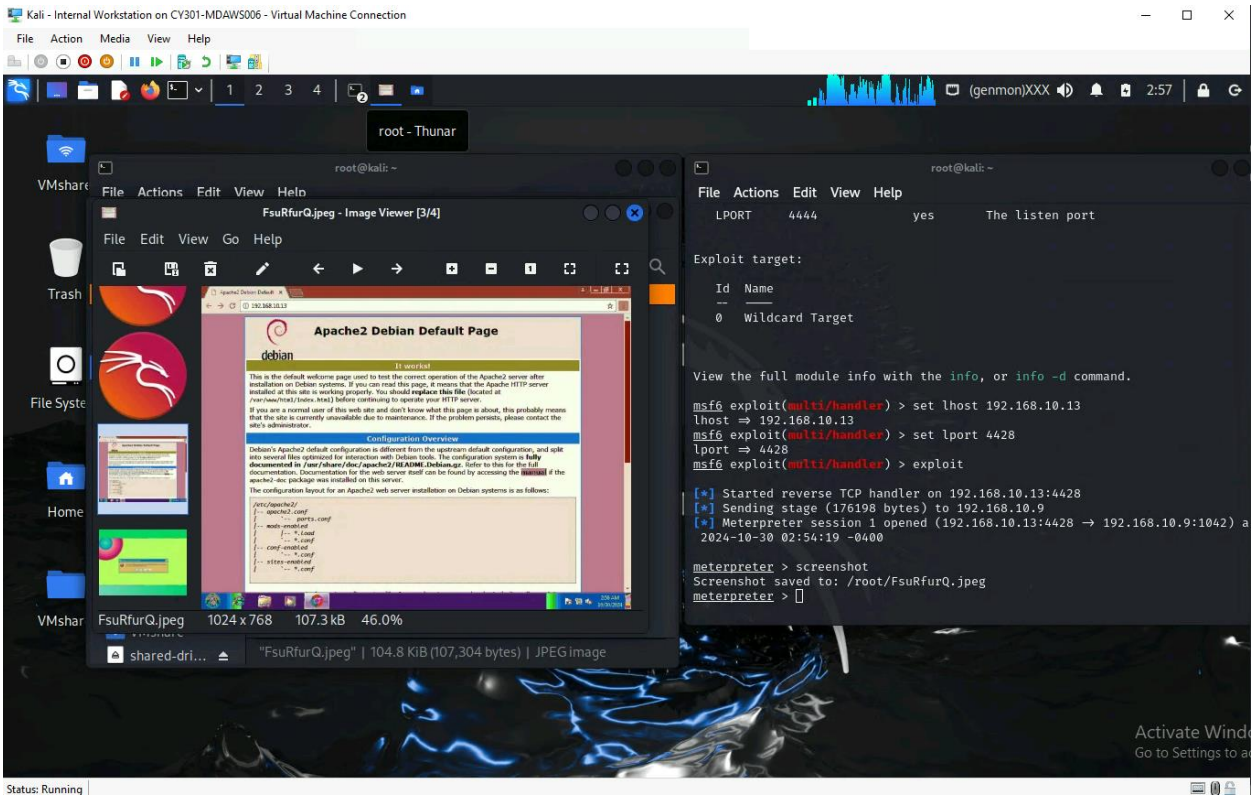
- **Payload Name: Use your MIDAS ID (for example, svatsa.exe) (5pt)**
- **Listening port: *5525* (5pt) CANVAS SAYS TO USE 4428**



After uploading the payload and downloading it from 192.168.10.13/mdaws006.exe, I ran the exe on the Windows 7 server which then starter the meterpreter session on the listening machine.

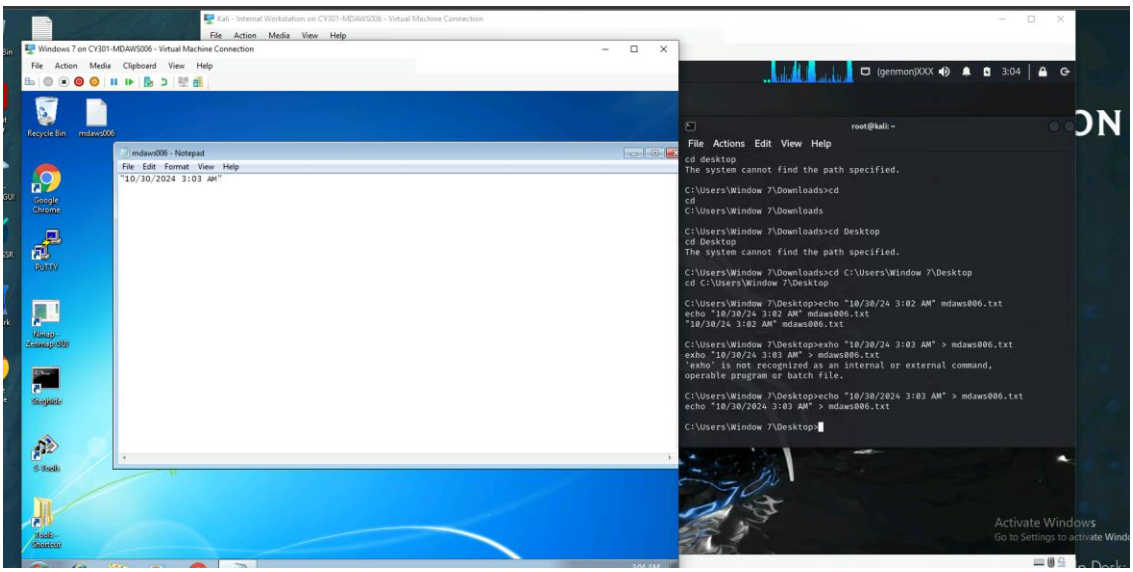
[Post-exploitation] Once you have established the reverse shell connection to the target Windows 7, complete the following tasks in your meterpreter shell:

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



2. 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)

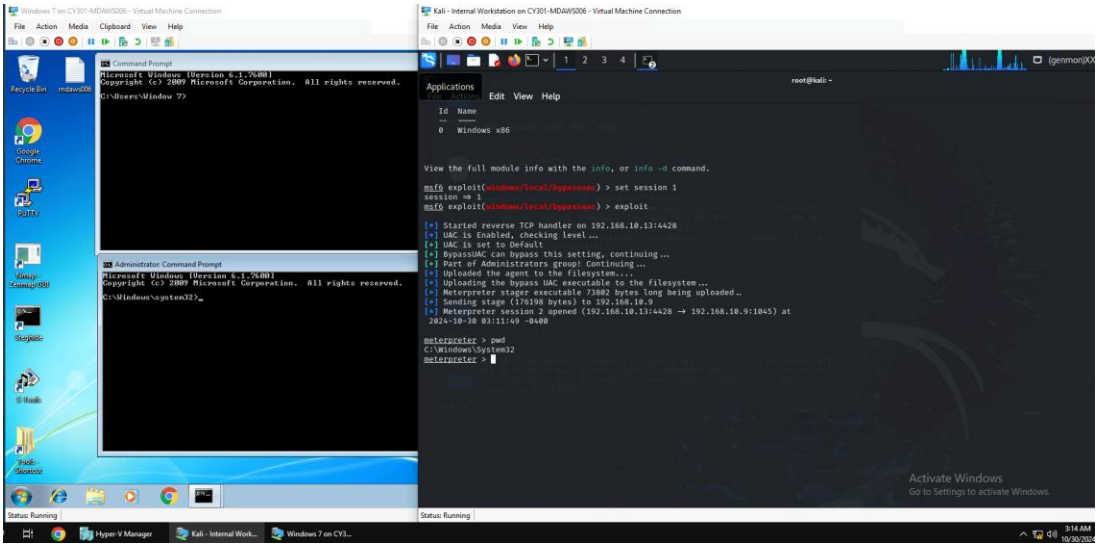
Using the echo command in the meterpreter terminal in the desktop directory automatically uploaded the txt file to the deskop.



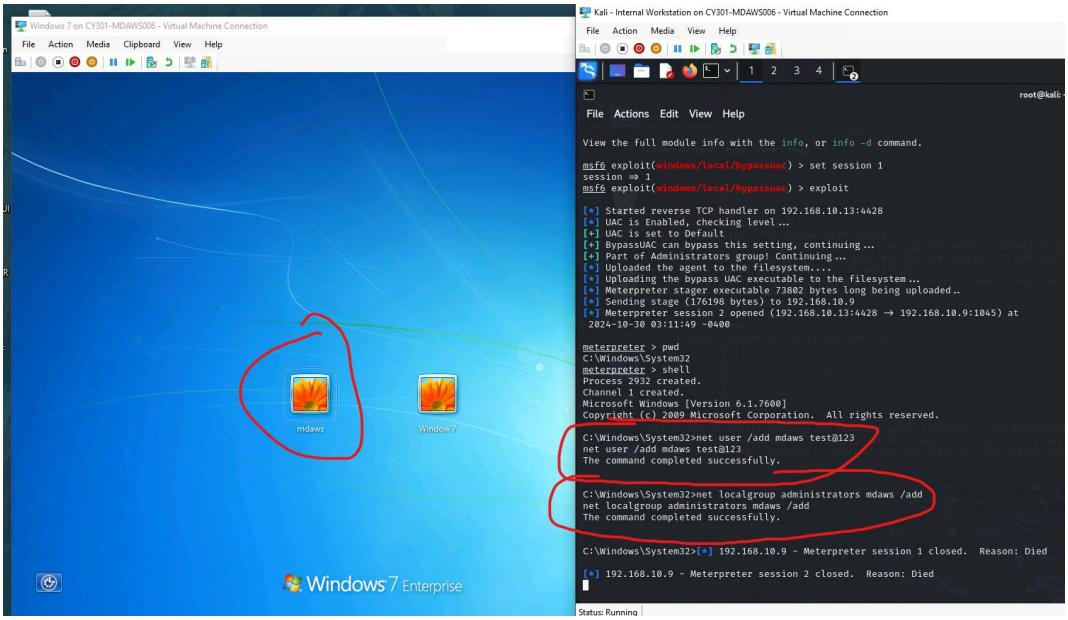
[Privilege escalation]

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

Using the bypassuuac exploit I set the session to the windows 7 server and set the lport to 4428 then exploited it to gain administrator-level privileges



After you escalate the privilege, complete the following tasks: 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)



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