Task C.

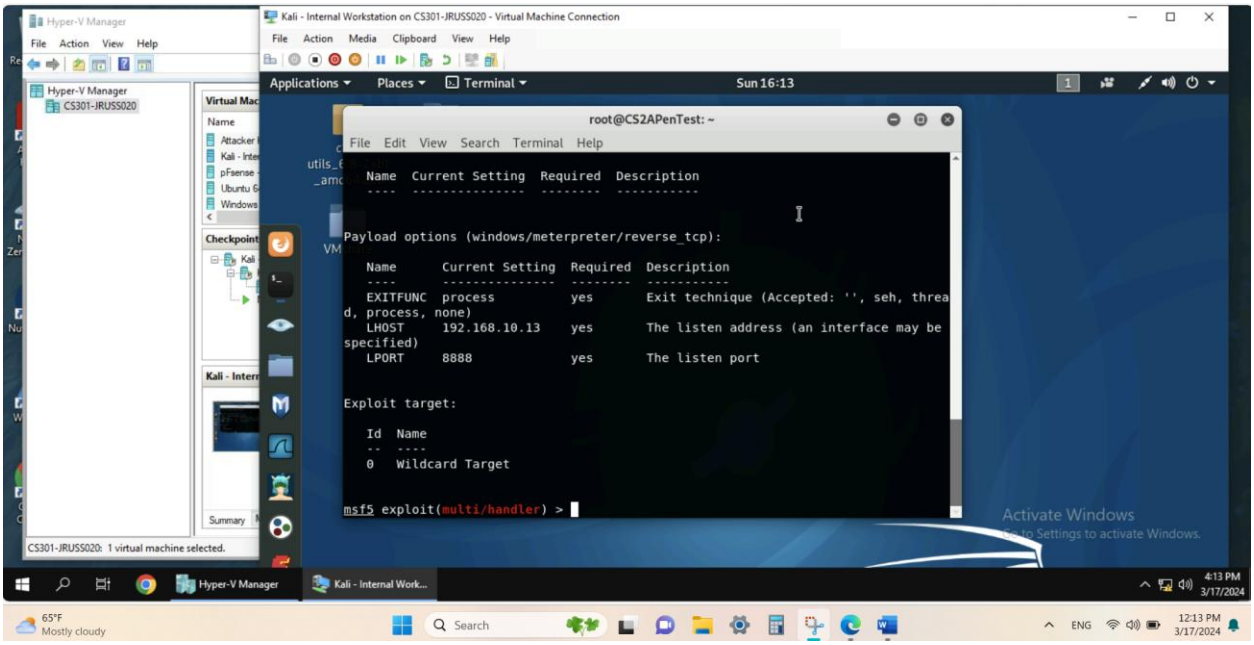
Exploit Windows 7 with a deliverable payload (60 pt).

In this task, you need to 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 (10 pt). Of course, 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 (10 pt, 5pt each):

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

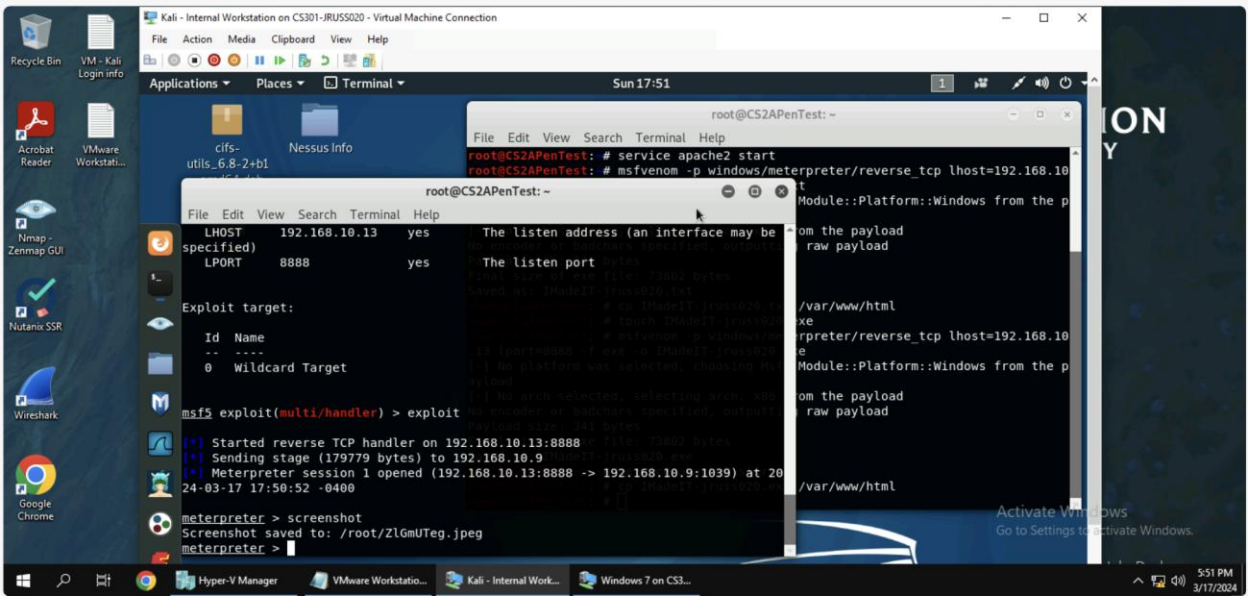
• Listening port: XXXX (follow the lab instruction)

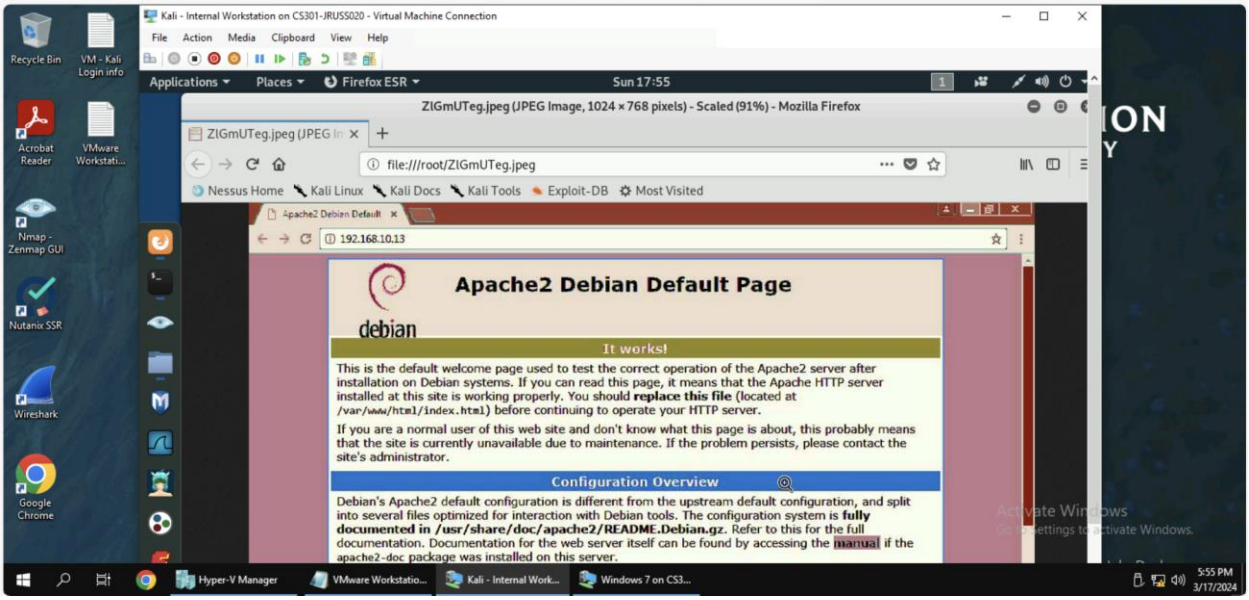


(In the above screenshot, port 8888 is set to the listening port)

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

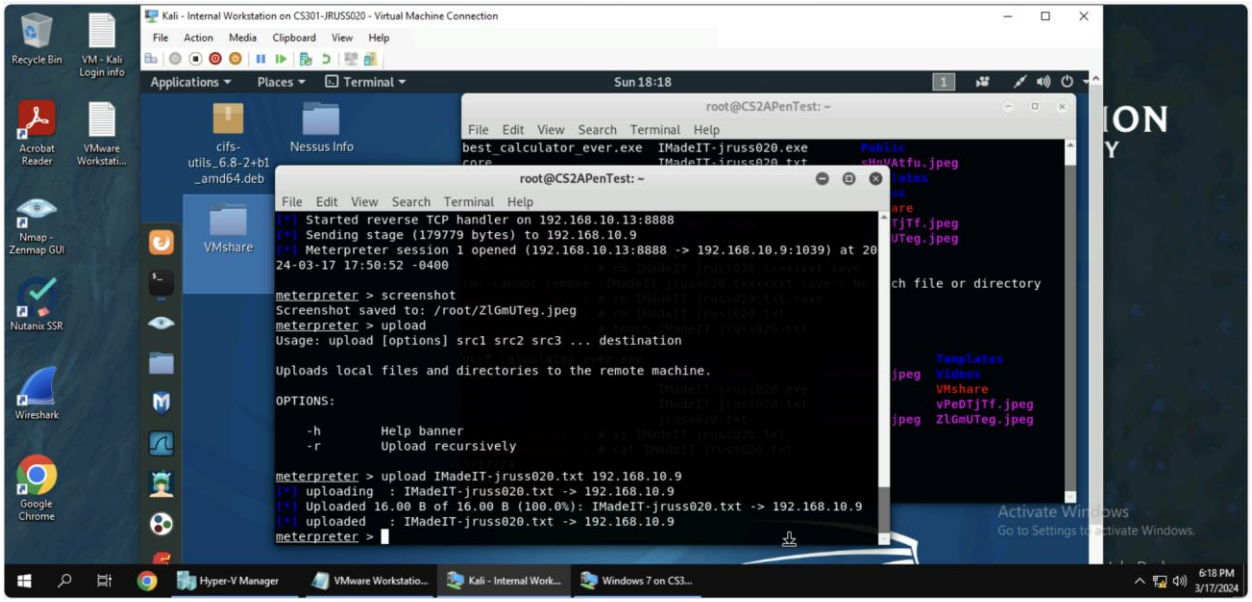
1. Execute the screenshot command to take a screenshot of the target machine if the exploit is successful. (10 pt)

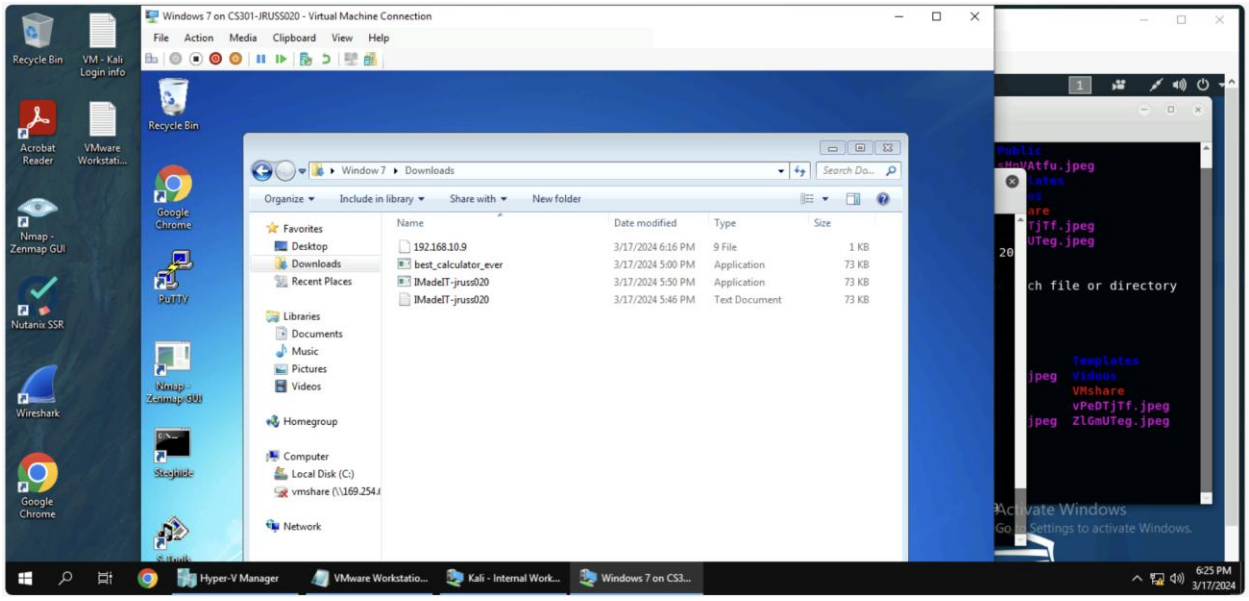




(In the above screenshots, the screenshot command verifies the exploit worked. The second picture is a screenshot of Windows 7 server desktop)

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. You need to show me the command that uploads the file. (10 pt)

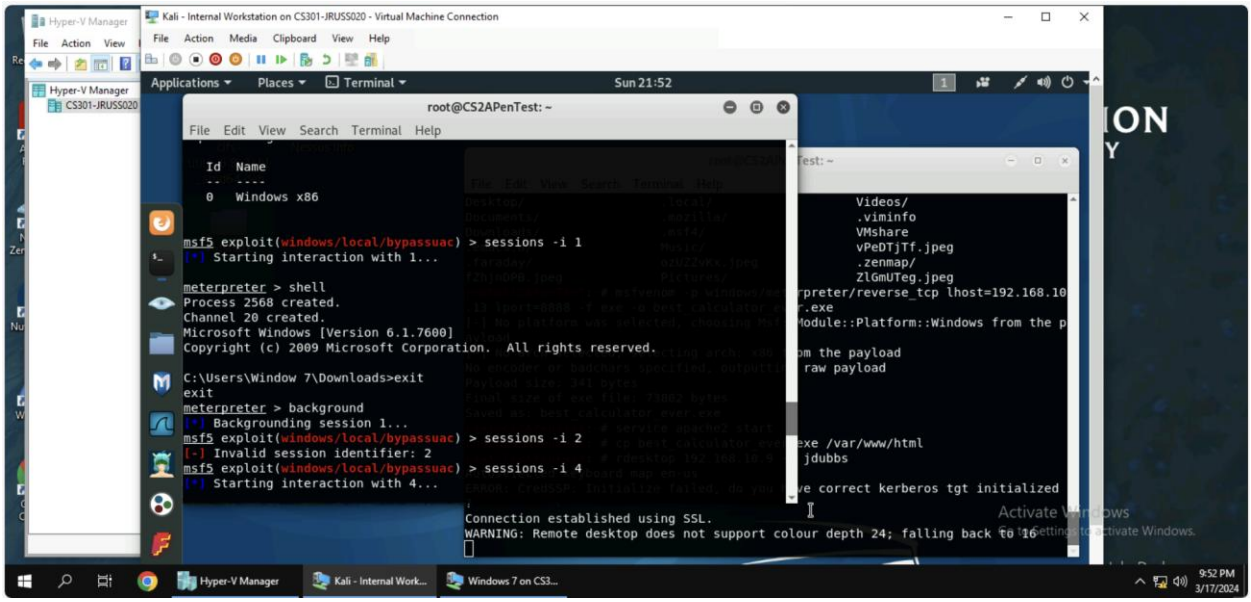


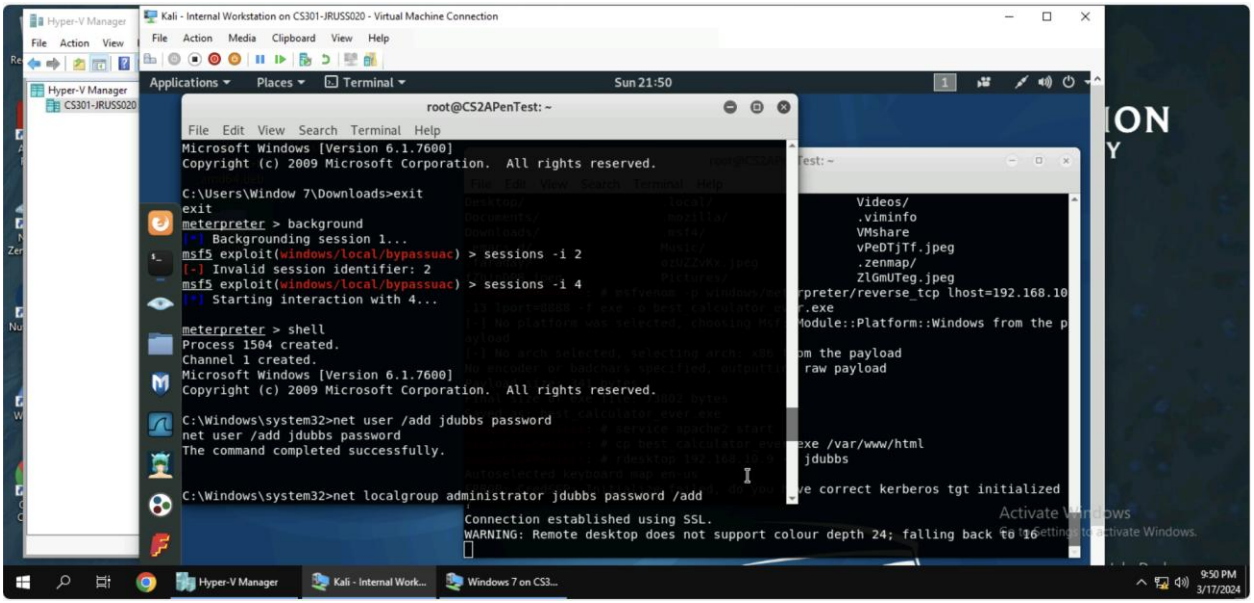


(In the above screenshots, a txt file was made in Kali and sent to the Windows 7 server machine)

[Privilege escalation] Background your current session, then gain administrator-level privileges on the remote system (10 pt). After you escalate the privilege, complete the following tasks:

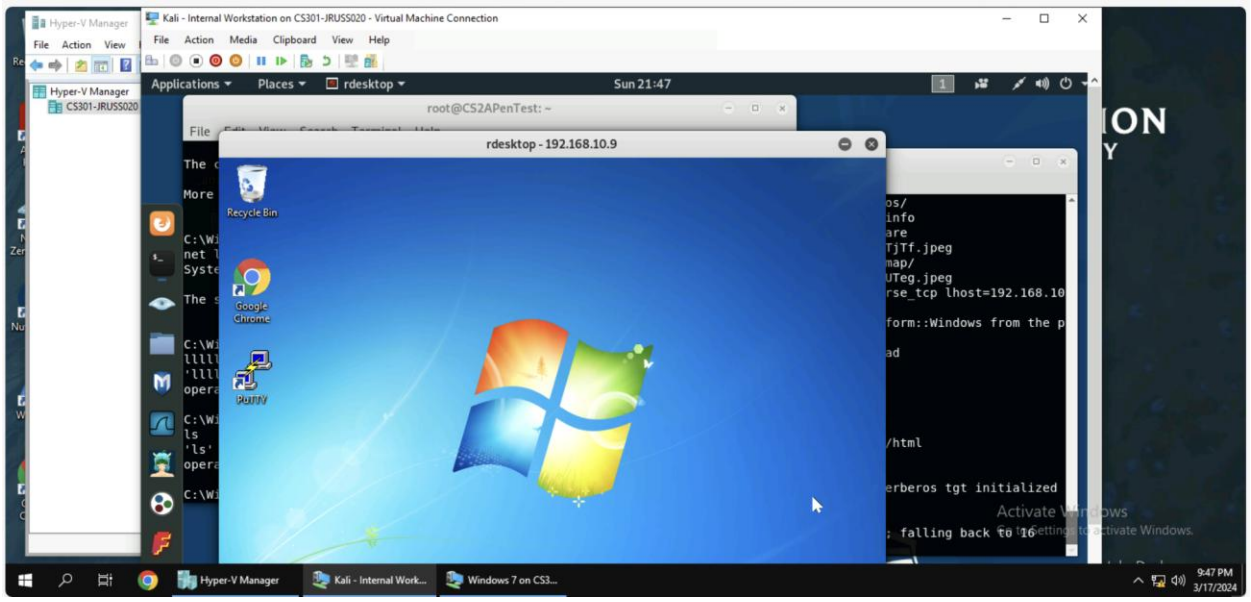
3. Create a malicious account with your name and add this account to the administrator group. You need to complete this step on the Attacker Side. (5 pt)





(In the above screenshot, a malicious user was created and given administrator privilege)

4. Remote access to the malicious account created in the previous step and browse the files belonging to the user, "Windows 7", in RDP. (5 pt)



(In the above screenshot, rdesktop command was used to log into the Windows 7 server from Kali Linux)