OLD DOMINION UNIVERSITY

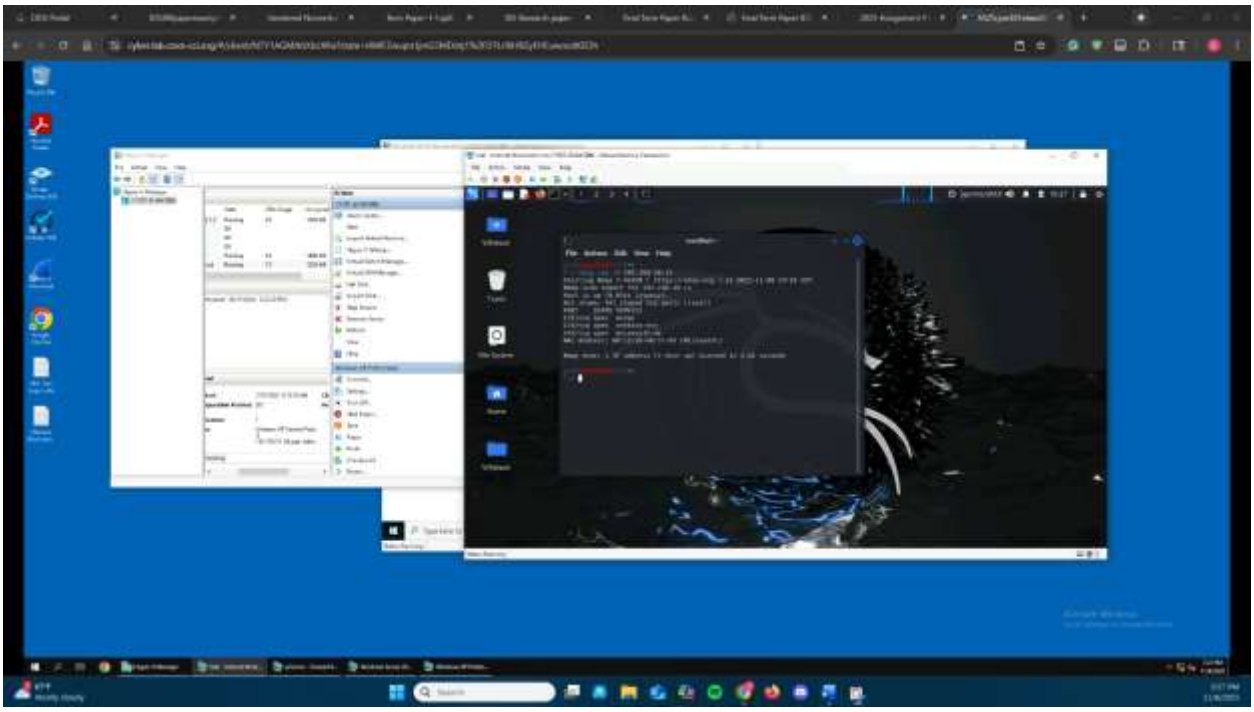
CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

Assignment #1 Basic Linux Commands

Ethan Lawson

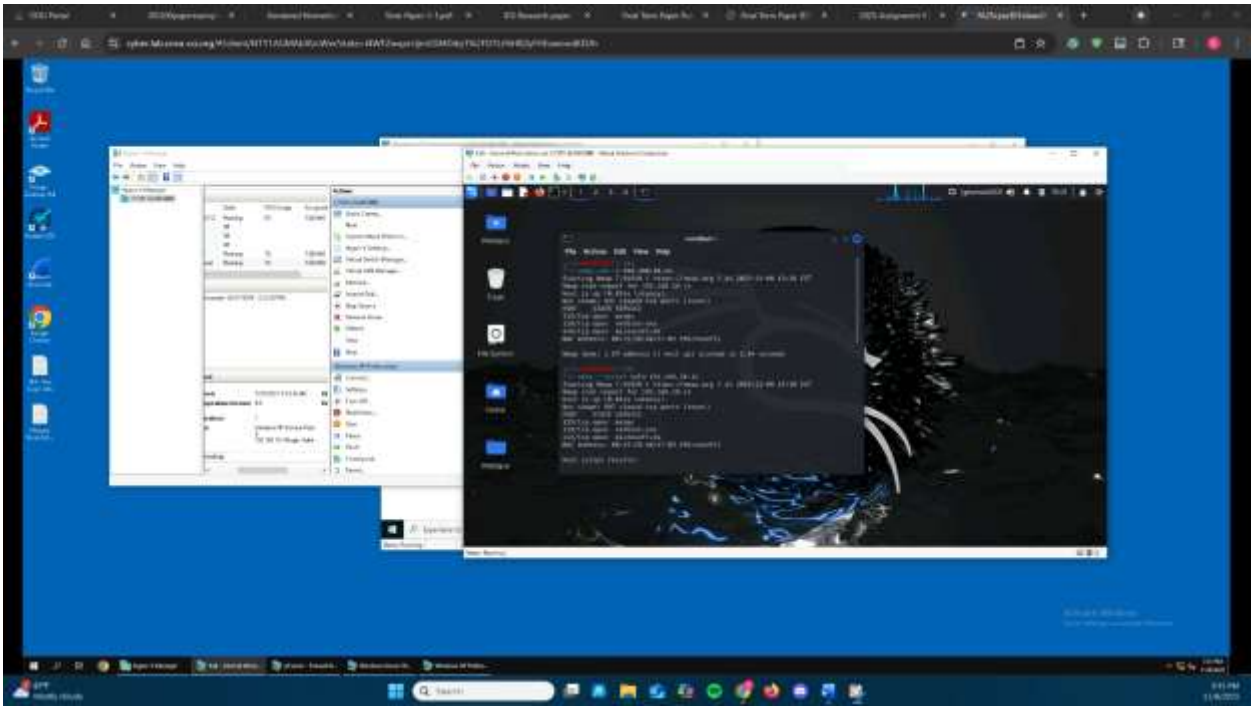
TASK A

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



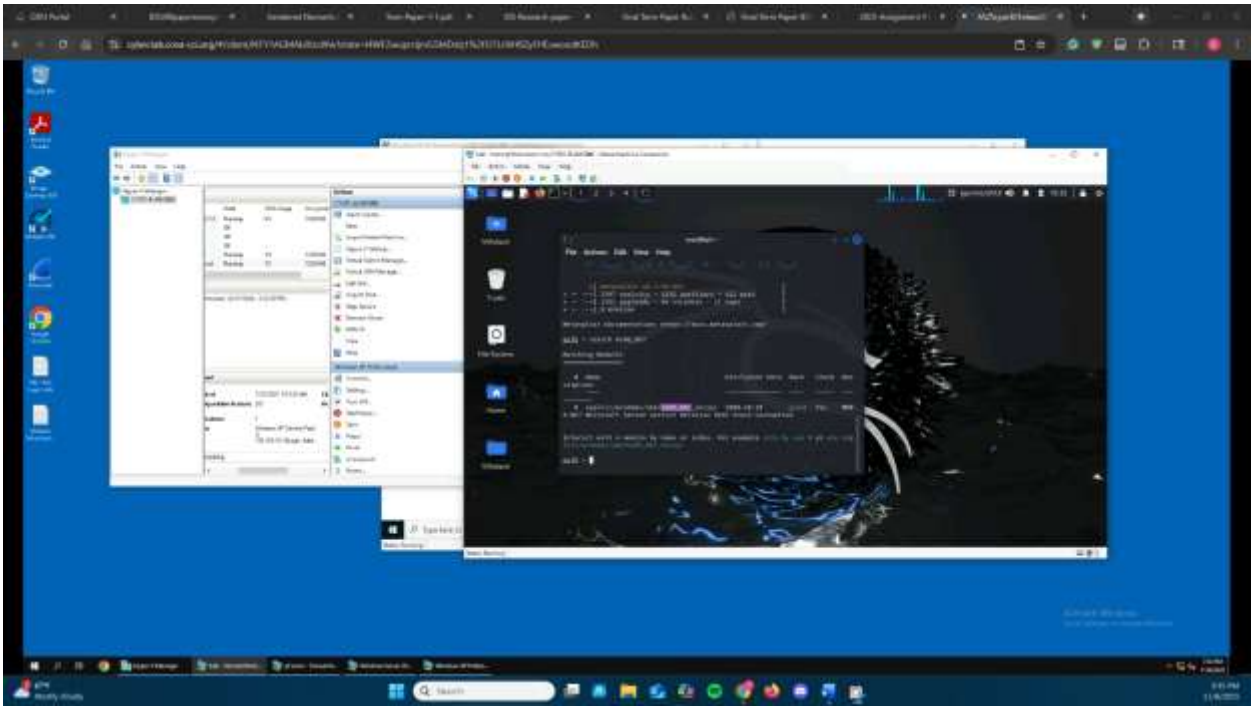
I used this nmap command to see common ports and services on the Windows XP machine.

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



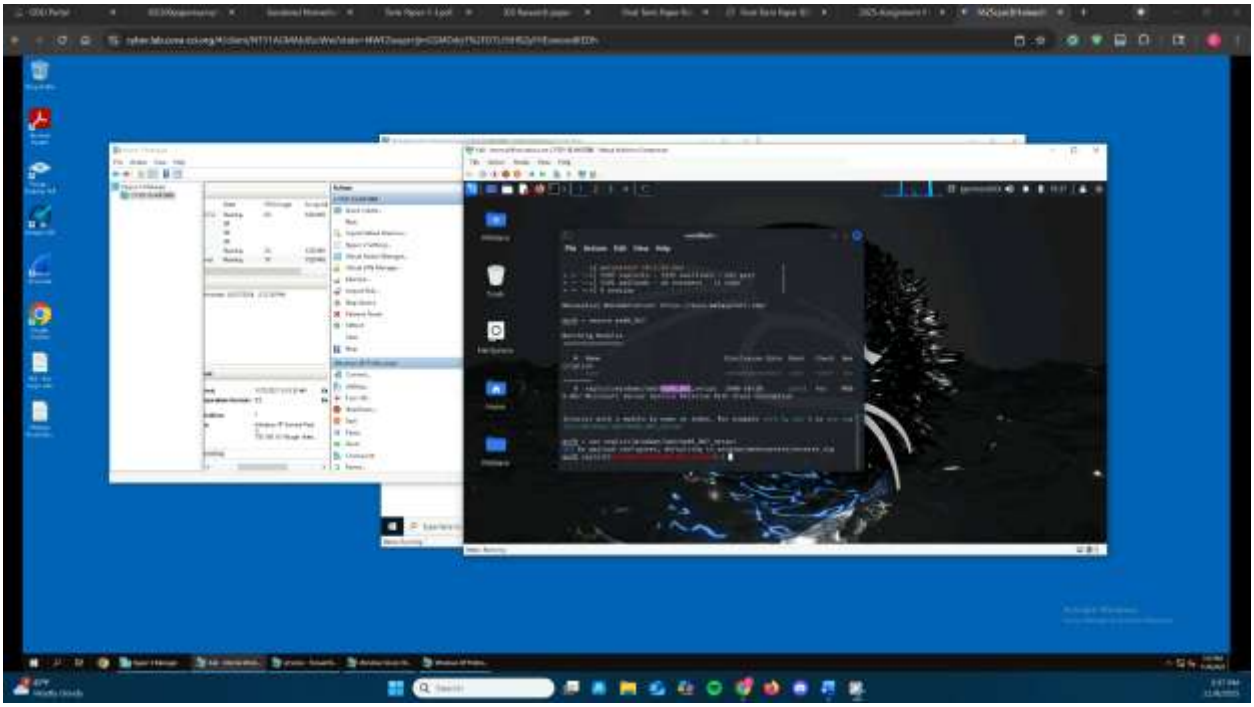
The command shows that port 445 on Windows XP is open.

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



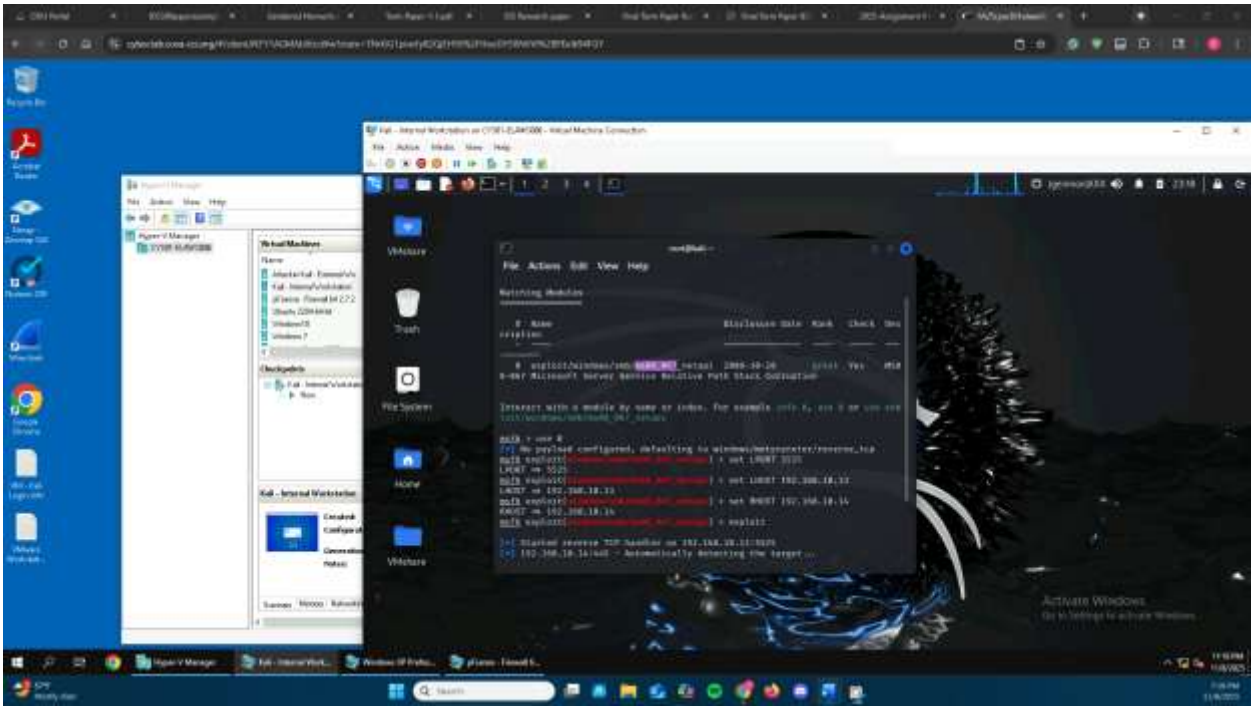
This returned the corresponding module and full path.

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



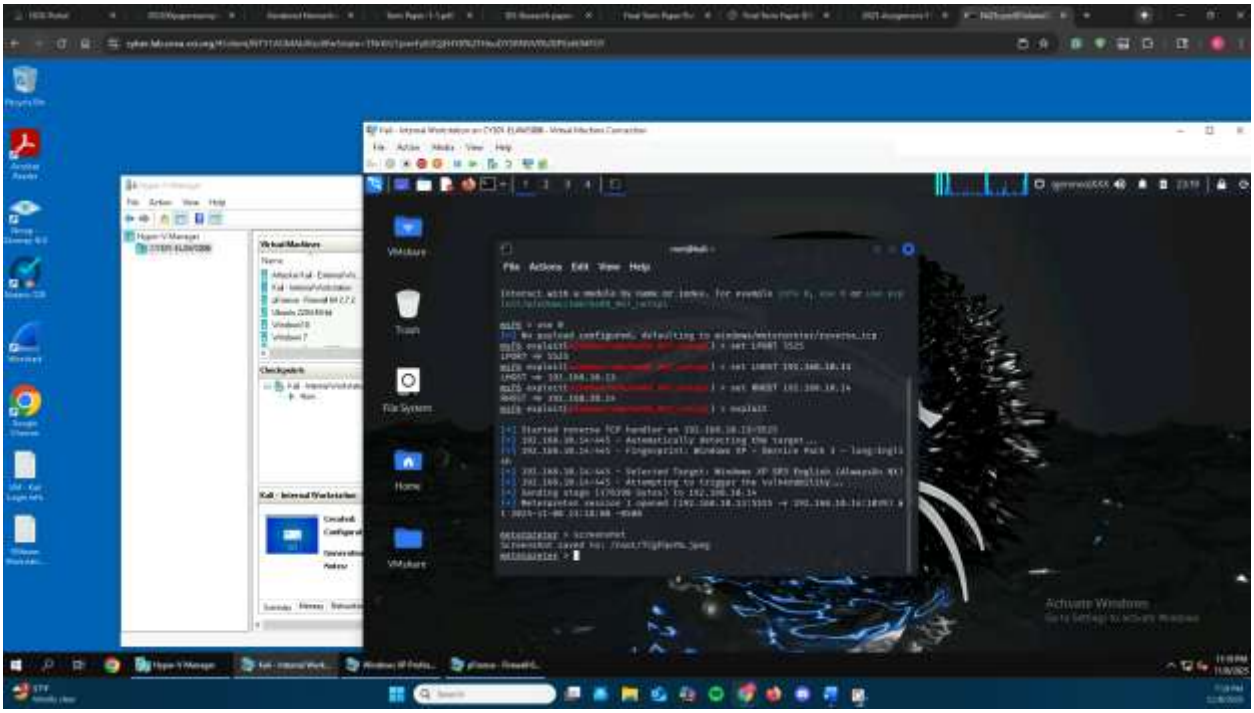
I set the exploit module to ms08_067_netapi using its full path and the payload defaulted correctly. If not, I would have used PAYLOAD windows/meterpreter/reverse_tcp.

5. Use 5525 as the listening port number. Configure the rest of the parameters. Display your configurations and exploit the target.



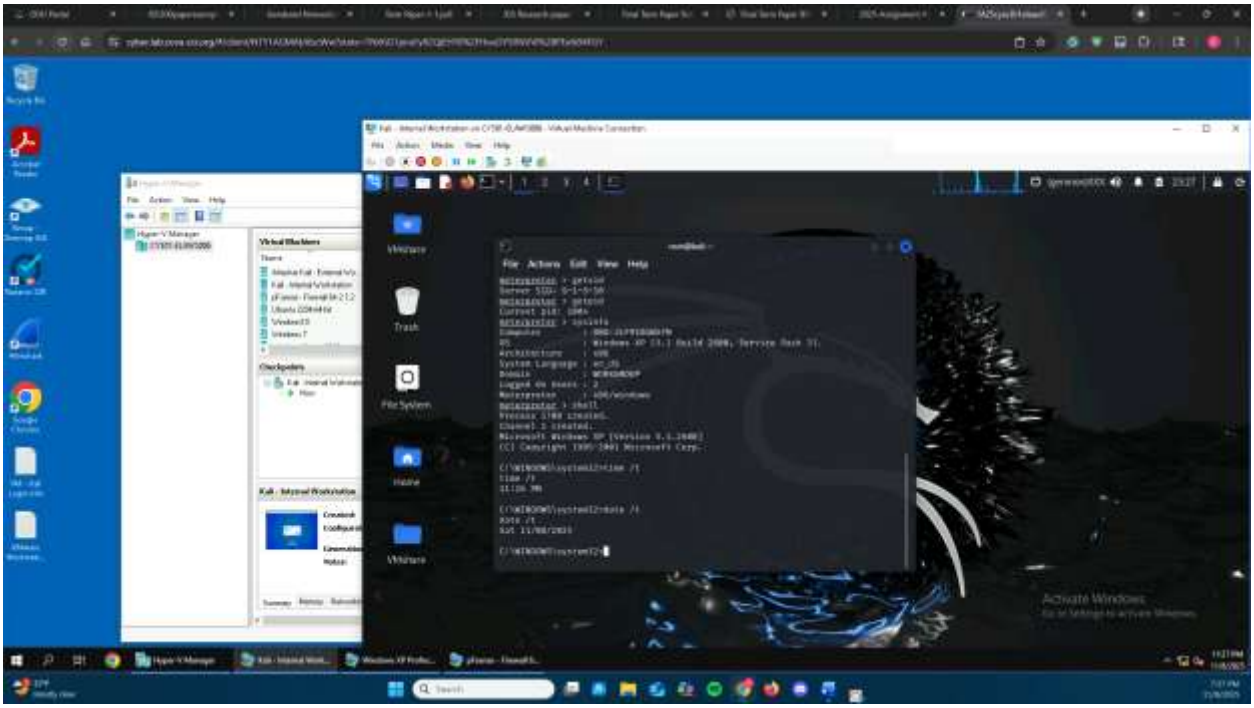
I set the necessary parameters-LPORT, LHOST, and RHOST. I used the command ‘exploit’ to begin.

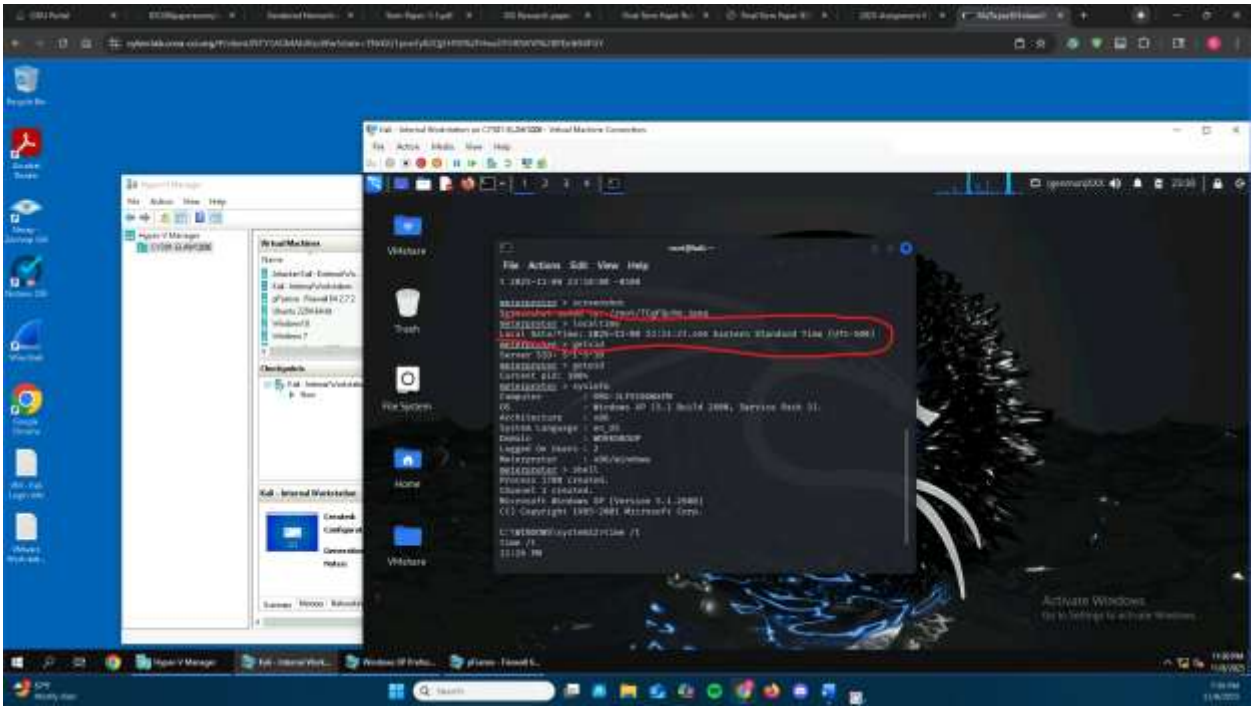
6. [Post-exploitation] Execute the screenshot command to take a screenshot of the target machine if the exploit is successful.



The exploit was successful, so I took a screenshot.

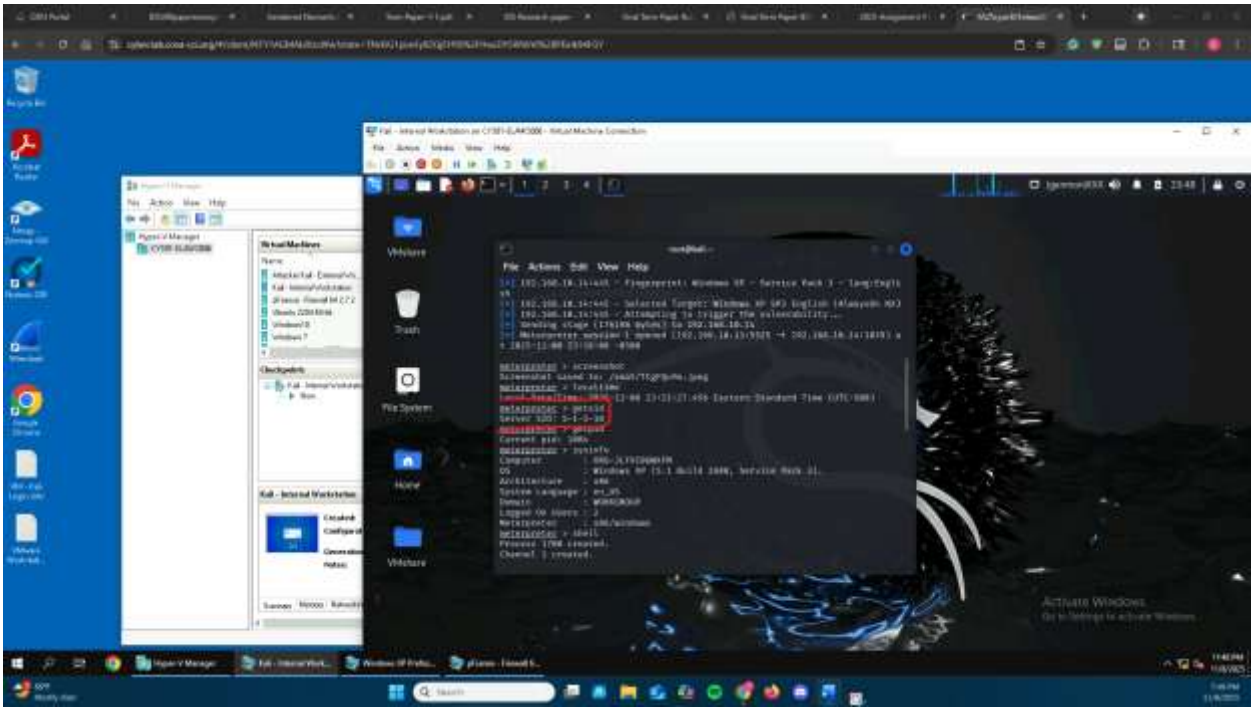
7. [Post-exploitation] In the meterpreter shell, display the target system's local date and time.

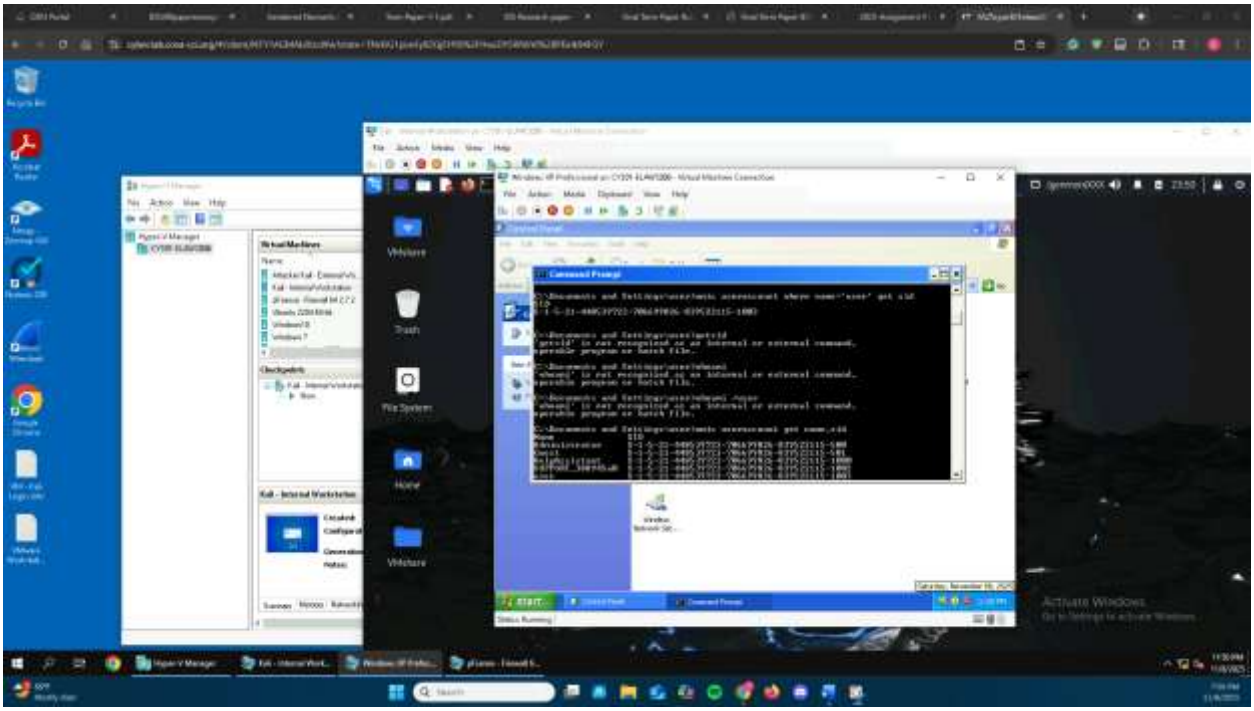




I used localtime from meterpreter and dropped to the shell and used date /t, time /t.

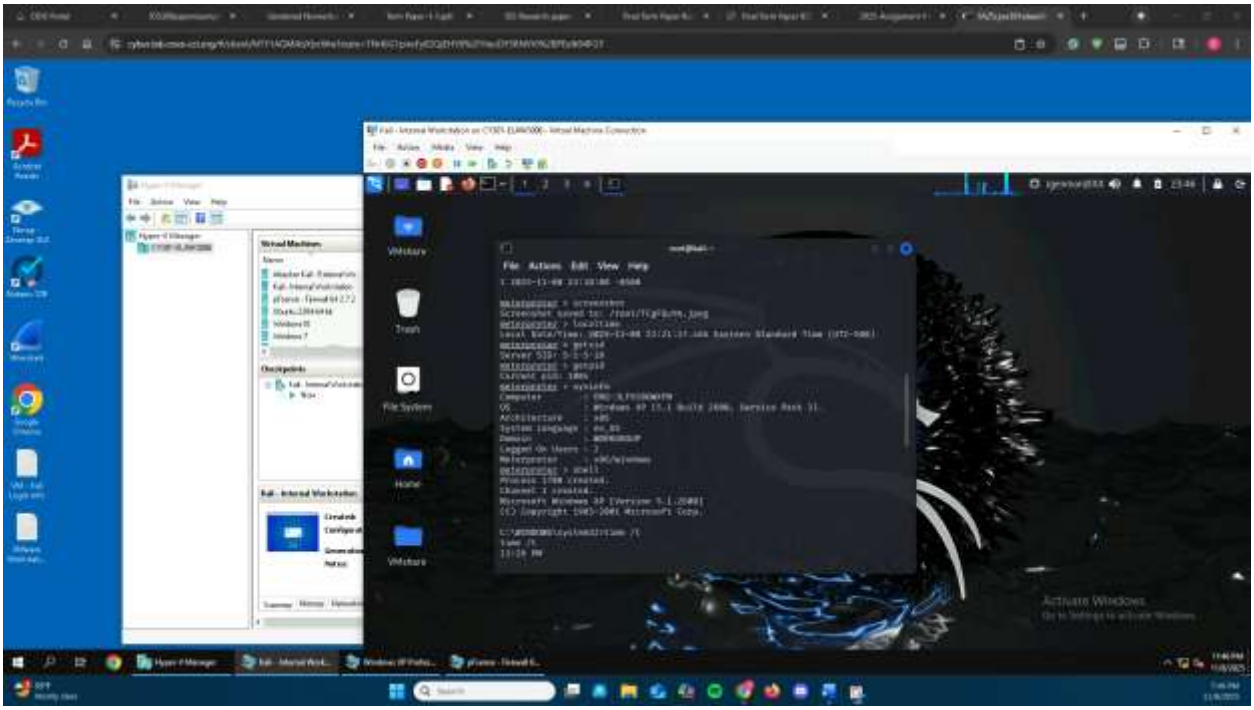
8. [Post-exploitation] In the meterpreter shell, get the SID of the user.





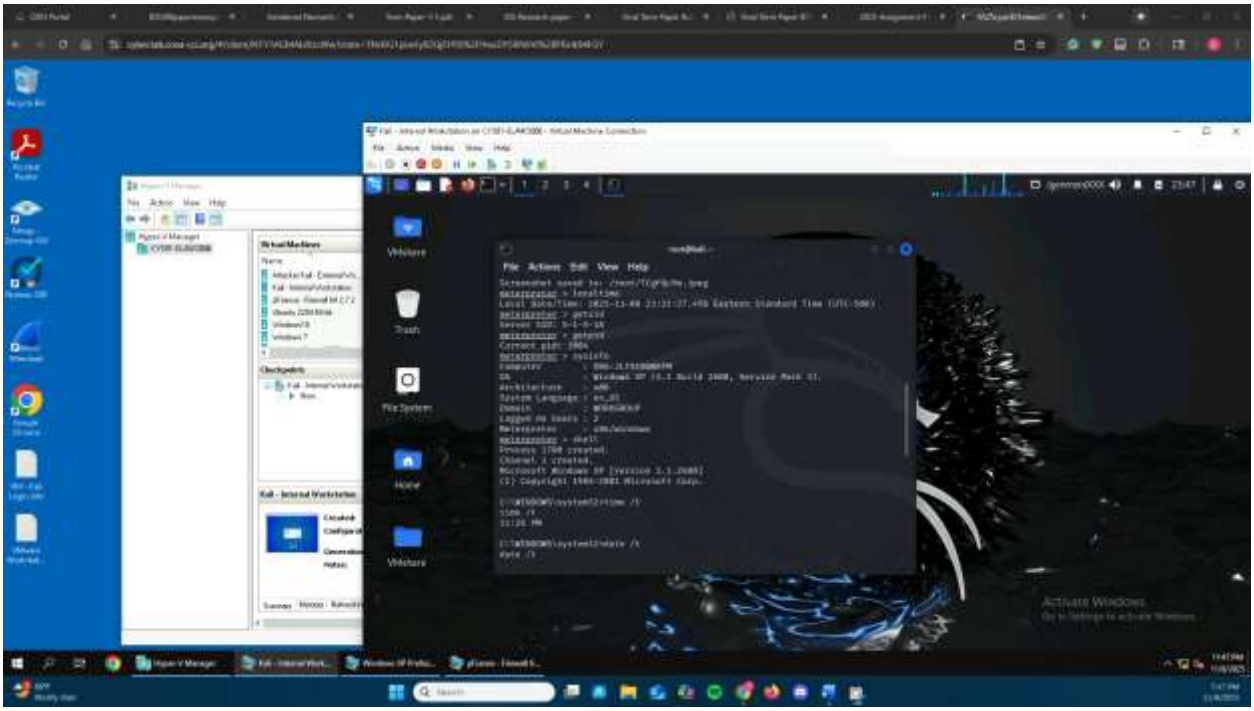
I used ‘getsid’ from the meterpreter shell which returned the Server SID. I know this isn’t the user’s SID. However, none of the commands would work when I dropped to the shell. I even double checked by trying them in Windows XP command prompt directly where they worked.

9. [Post-exploitation] In the meterpreter shell, get the current process identifier.



I used ‘getpid’ which returned ‘Current pid: 1004’.

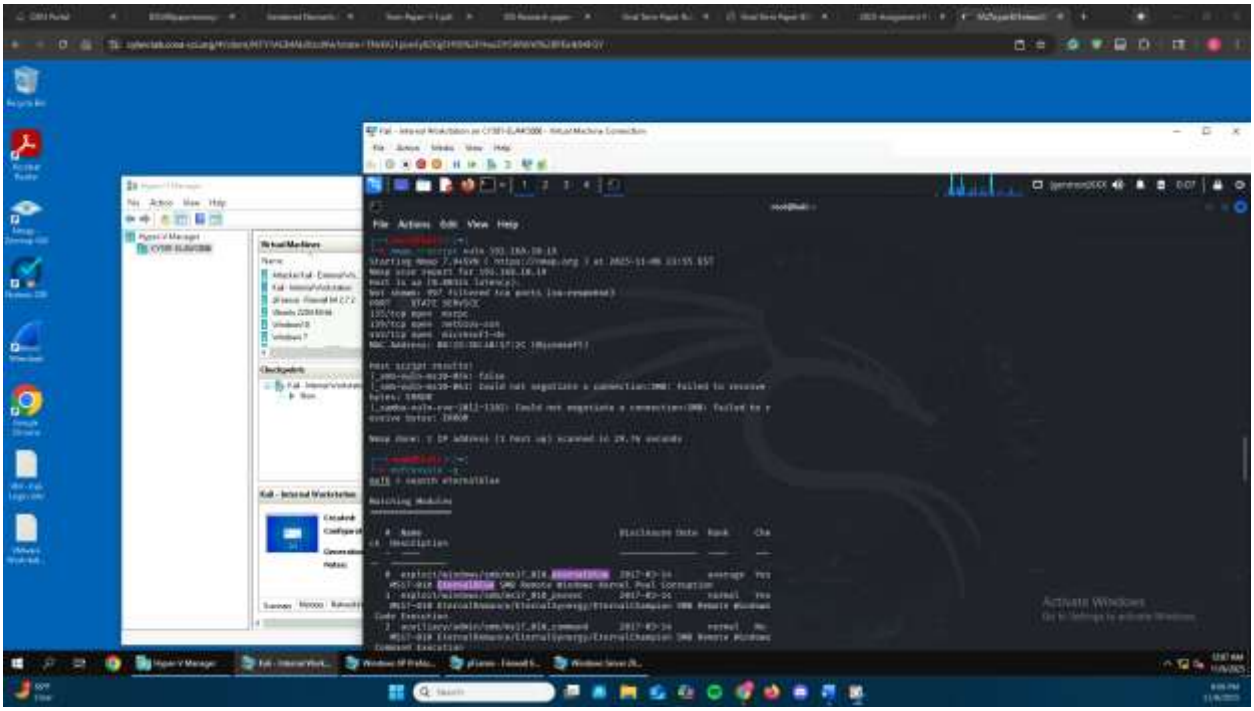
10. [Post-exploitation] In the meterpreter shell, get system information about the target.

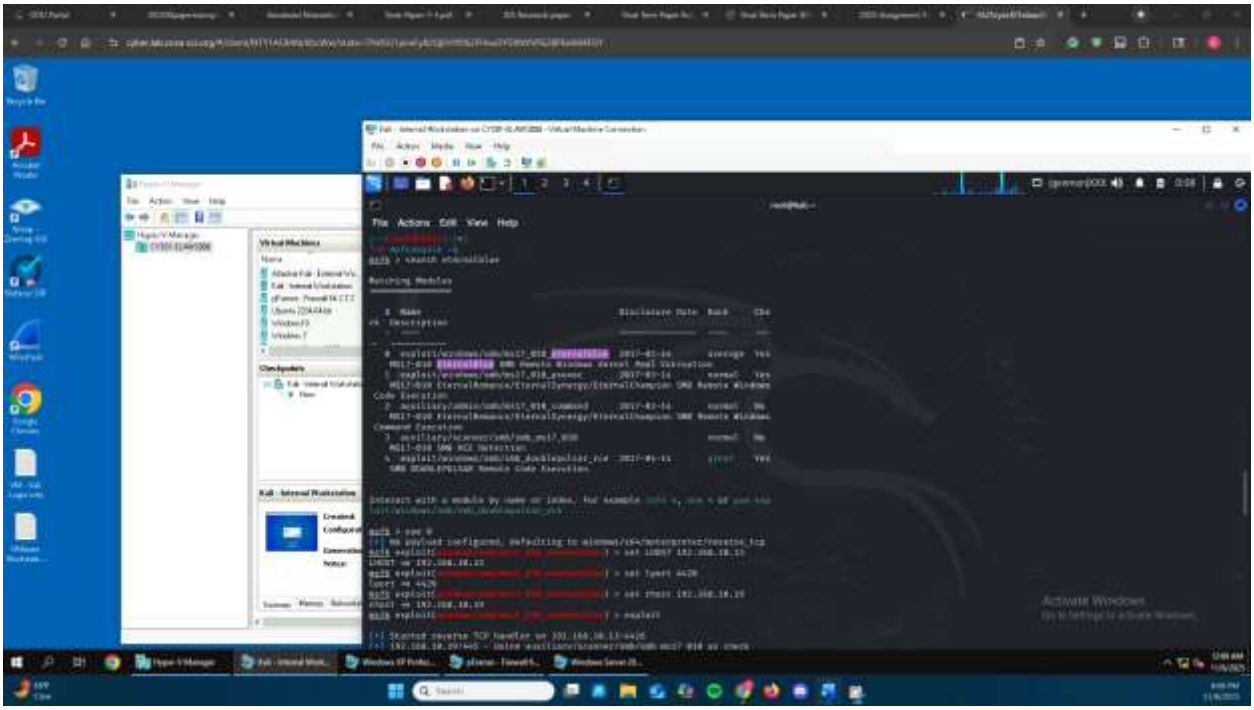


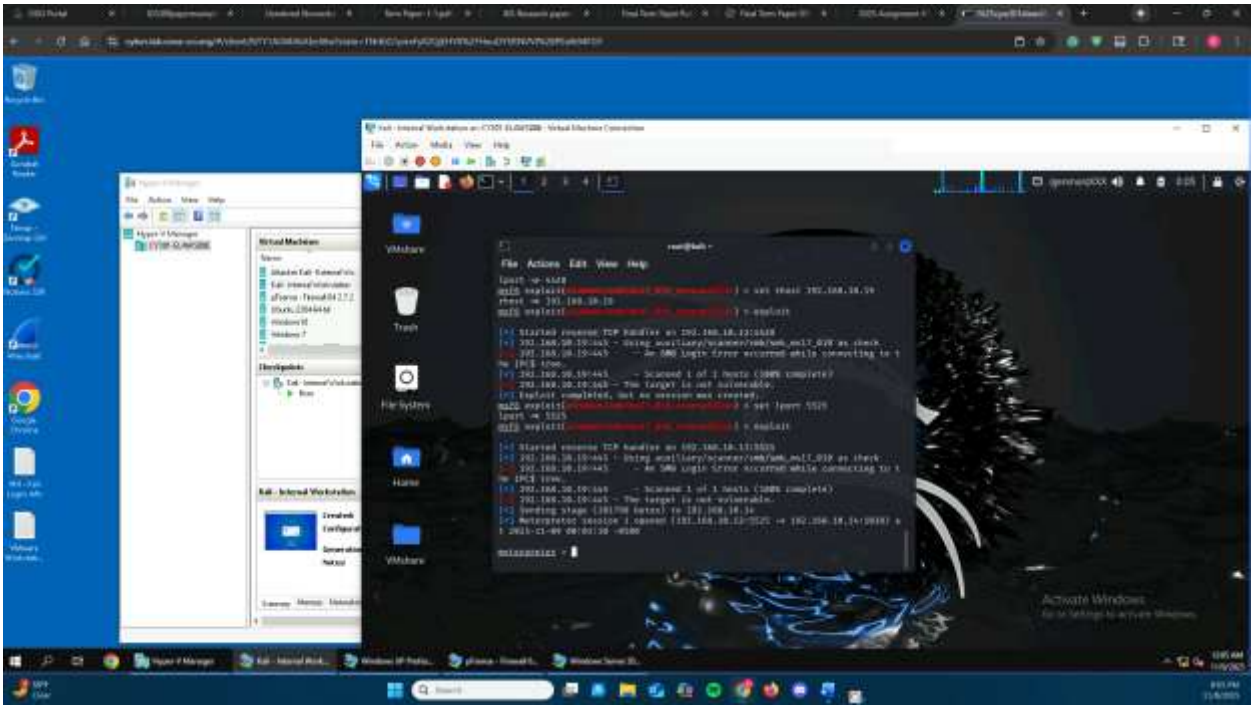
I used the command sysinfo which displayed system information about the target.

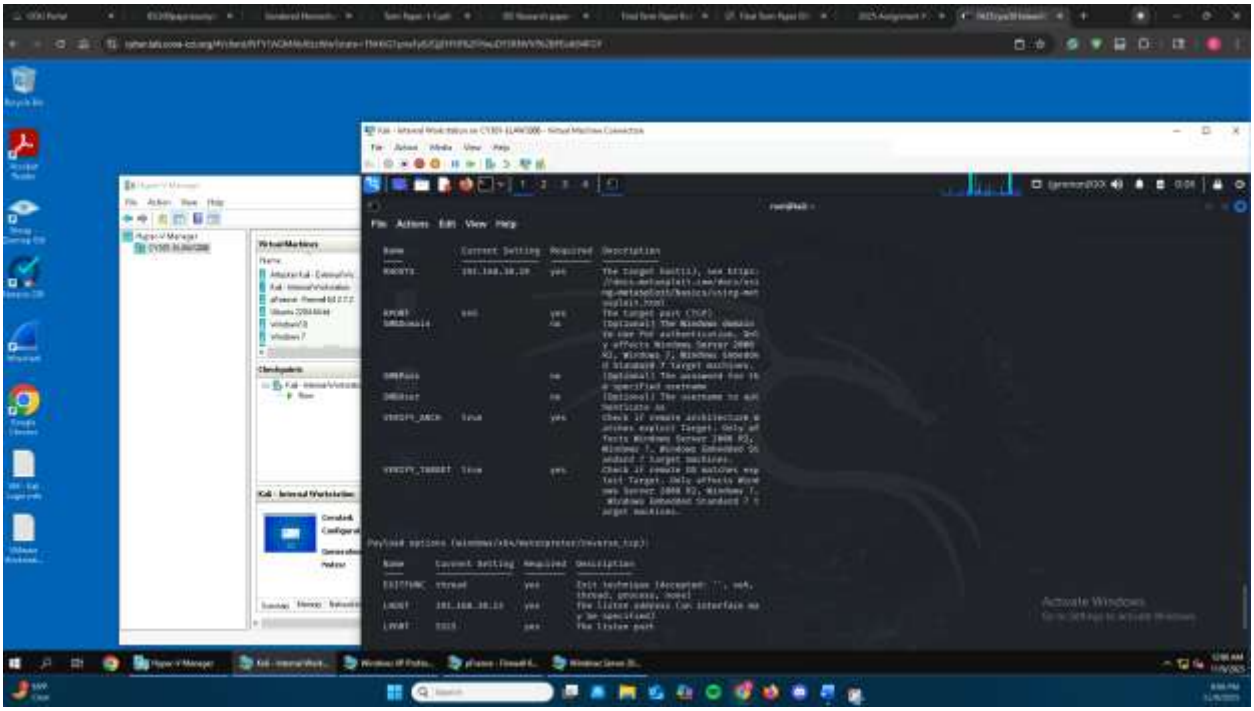
TASK B

In this task, try to use the same steps as shown in the video lecture to exploit the EternalBlue vulnerability on Windows Server 2022. You may or may not establish a reverse shell connection to the Windows Server 2022 using the same method as hacking Windows Server 2008. Document your steps and show me your results. You won't lose points for a failed reverse shell connection. But you will lose points for incorrect configurations, such as putting the wrong IP address for LHOST/RHOST, etc.









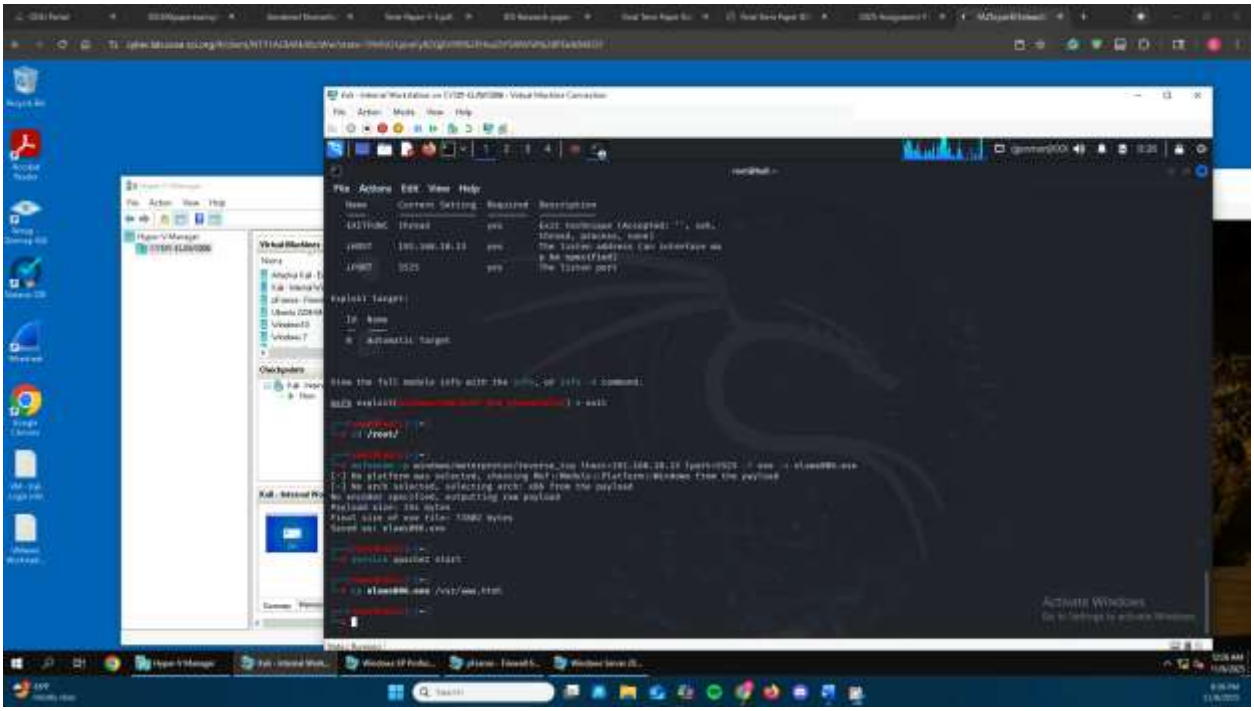
I began by identifying vulnerabilities on the Windows server. I was able to successfully exploit the eternalblue vulnerability once I switched the lport to 5525. Lhost was 192.168.10.13 and rhost was 192.168.10.19. The payload defaulted to windows/x64/meterpreter/reverse_tcp. My success was signaled by a meterpreter session being opened after running the exploit command.

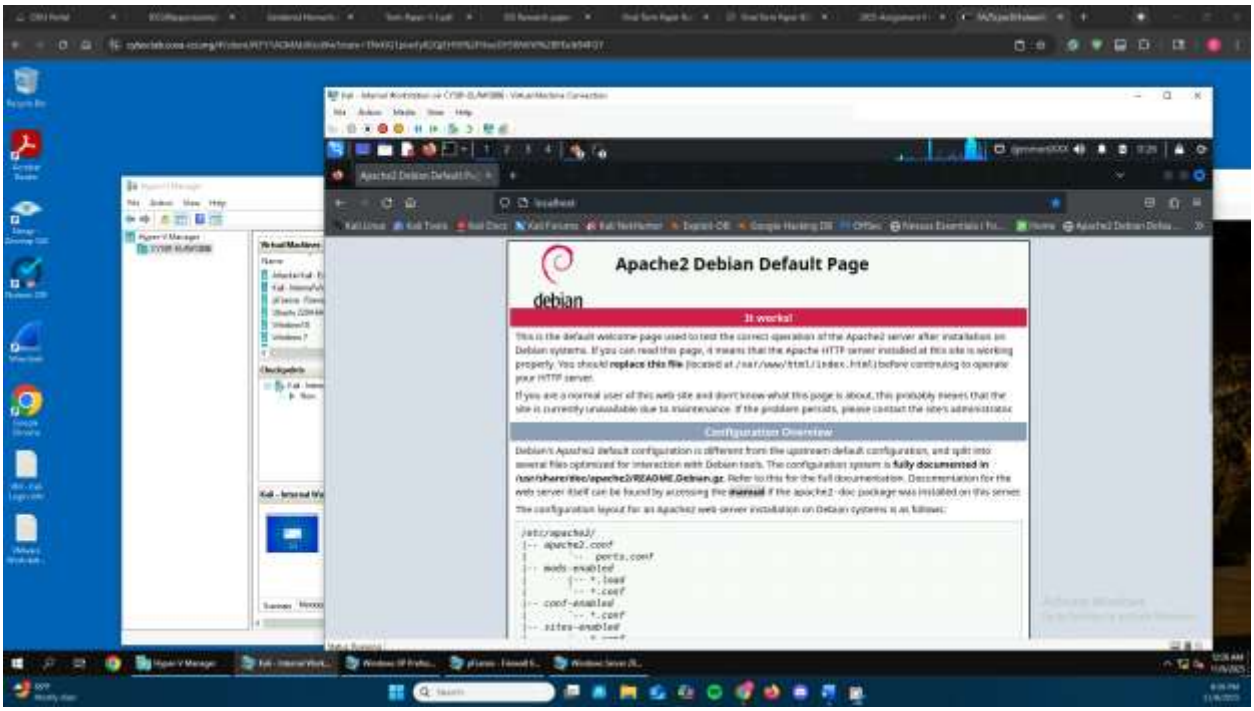
TASK C

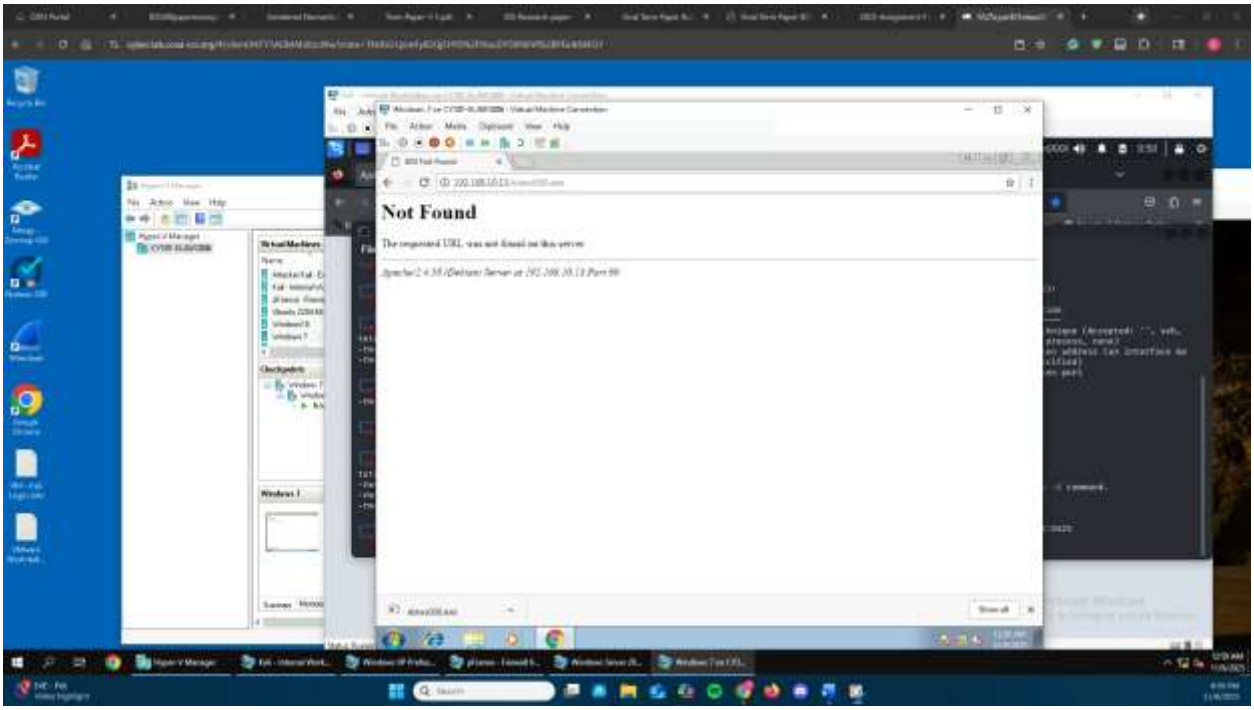
In this task, you need to create an executable payload with the required configurations below.
1. Once your payload is ready, you should upload it to the web server running on Kali Linux and, download the payload from Windows 7, then execute it on the target to make a reverse shell. Of course, don't forget to configure your Metasploit on Kali Linux before the payload is triggered on the target VM. (10 pt).
The requirements for your payload are :
• Payload Name: Use your MIDAS ID (for example, svatsa.exe) (5pt)
• Listening port: 5525 (5pt)
[Post-exploitation] Once you have established the reverse shell connection to the target Windows 7, complete the following tasks in your meterpreter shell:

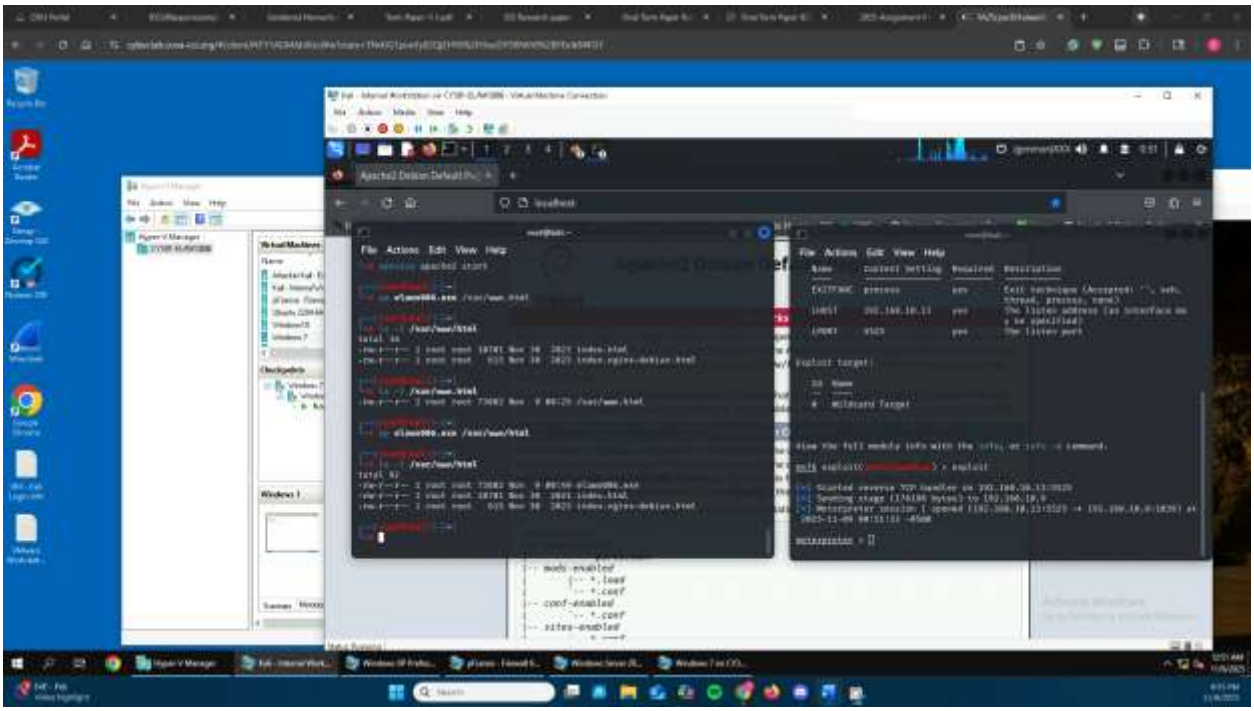
2. Execute the screenshot command to take a screenshot of the target machine if the exploit is successful. (10 pt)
3. Create a text file on the attacker Kali named "YourMIDAS.txt" (replace YourMIDAS with your university MIDAS ID) and put the current timestamp in the file. Upload this file to the target's desktop. Then, log in to Windows 7 VM and check if the file exists. You need to show me the command that uploads the file. (10 pt)
[Privilege escalation]
4. Background your current session, then gain administrator-level privileges on the remote system (10 pt).
5. After you escalate the privilege, complete the following tasks:
a. 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. (10 pt)
b. Remote access to the malicious account created in the previous step and browse the files belonging to the user, "Windows 7", in RDP. (10 pt) You may follow the pdf for Pen testing

1.



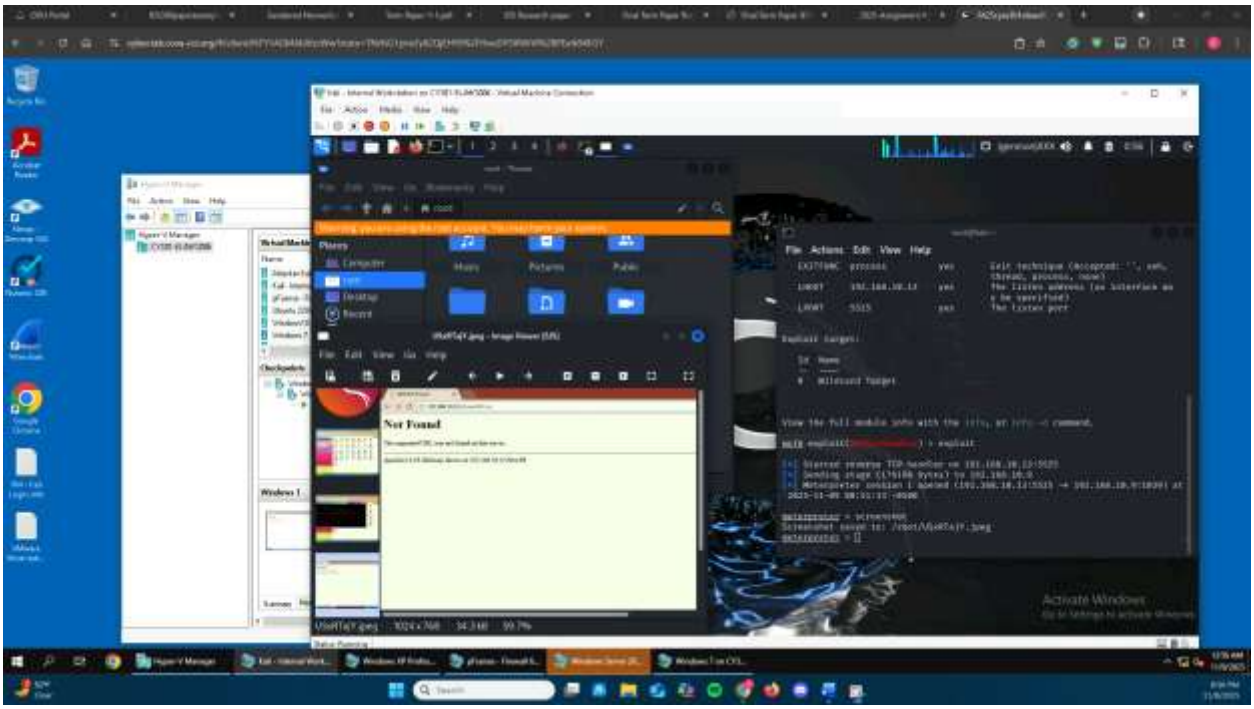

Apache2 Debian Default Page
debian
It works!
This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should replace this file (located at /var/www/html/index.html) before continuing to operate your HTTP server.
If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.
Configuration Overview
Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is fully documented in /usr/share/doc/apache2/README.Debian.gz. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the manual if the apache2-doc package was installed on this server.
The configuration layout for an Apache2 web server installation on Debian systems is as follows:
/etc/apache2/
|-- apache2.conf
| `-- ports.conf
|-- mods-enabled
| |-- *.load
| `-- *.conf
|-- conf-enabled
| `-- *.conf
|-- sites-enabled


Not Found
The requested URL was not found on this server.
Apache/2.4.58 (Debian) Server at 192.168.10.13 Port 80



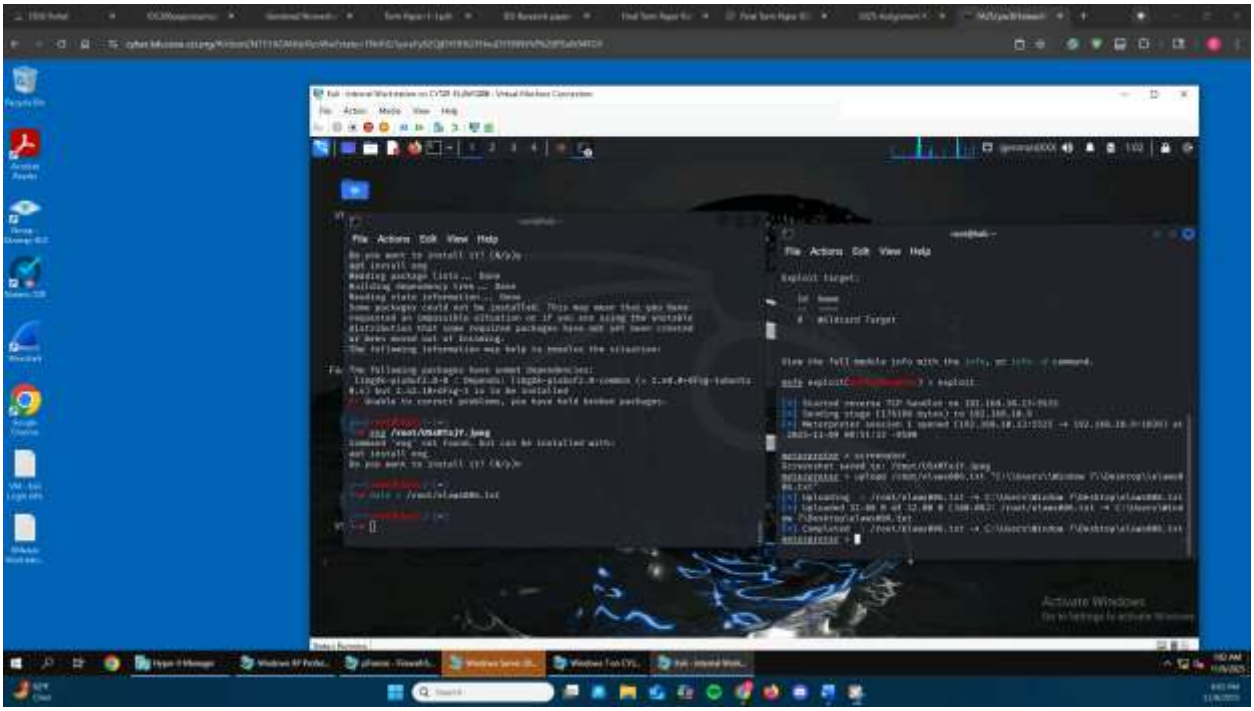
I first used msfvenom to create the payload with the correct name and listening port. I started the apache2 server on my Kali machine and checked it on my browser. From the Windows 7 machine I accessed the server using Kali's IP which installed the executable which I ran. This formed a connection which my meterpreter shell confirmed.

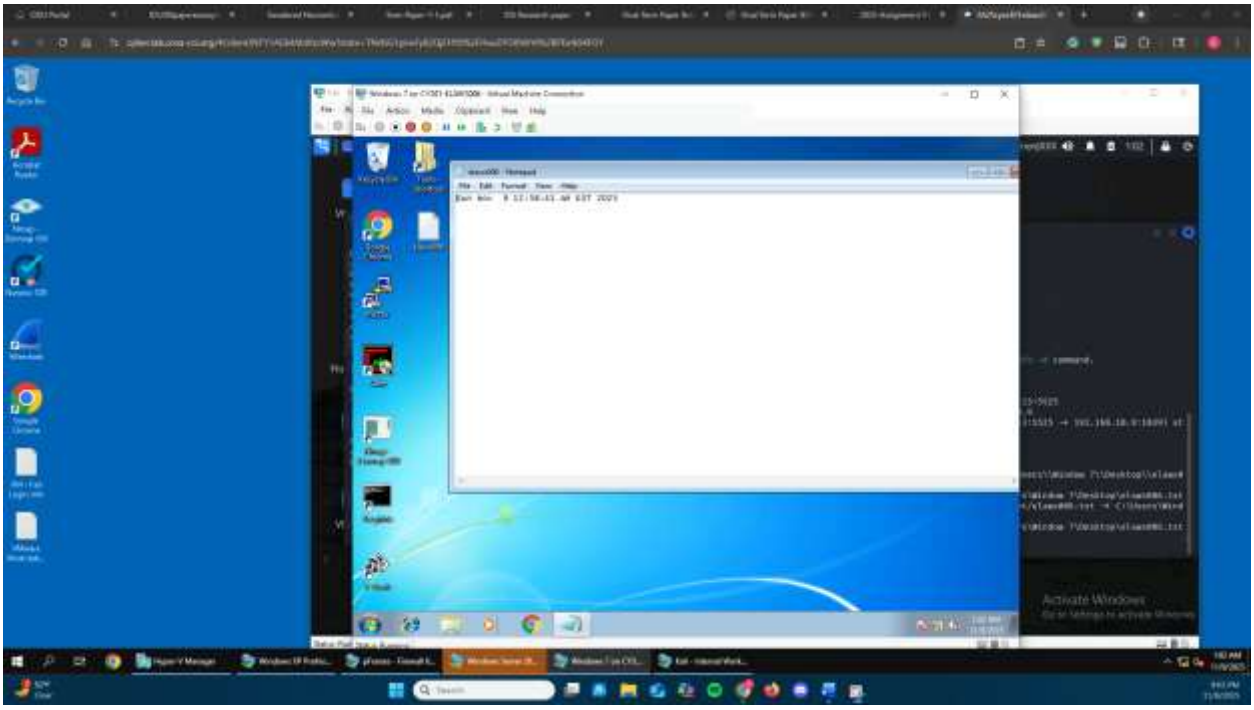
2.



I executed the screenshot command and displayed the image.

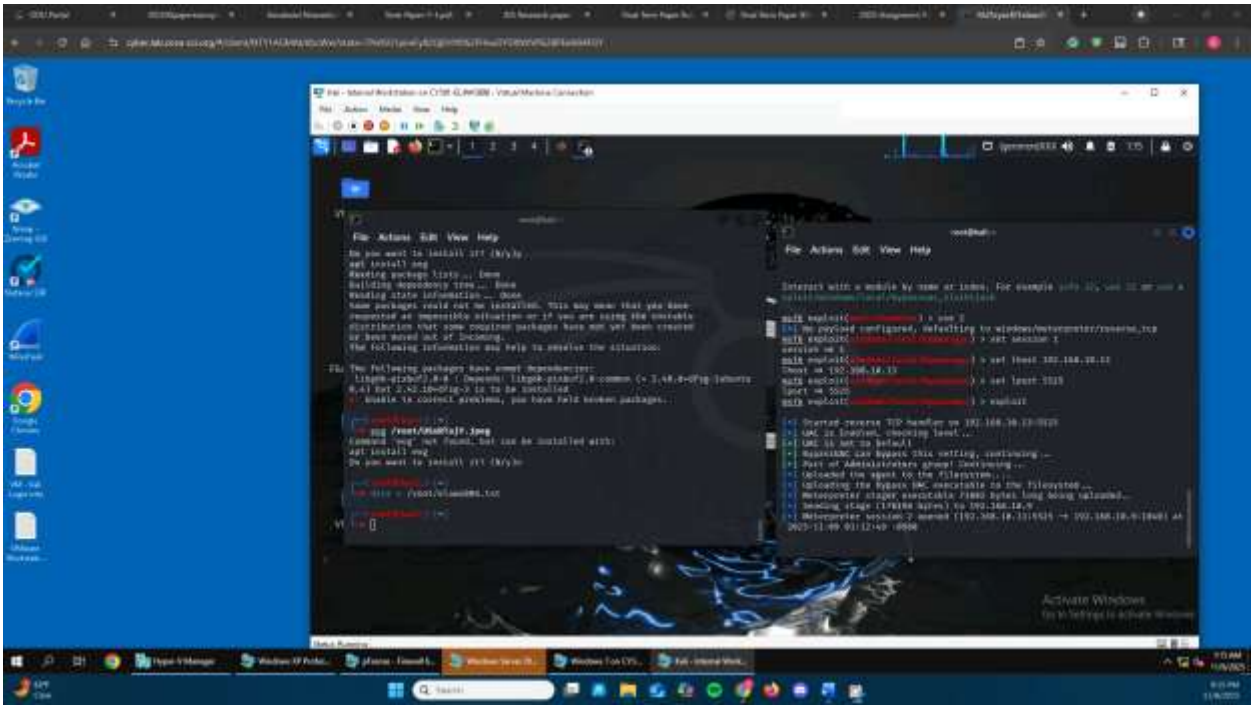
3.





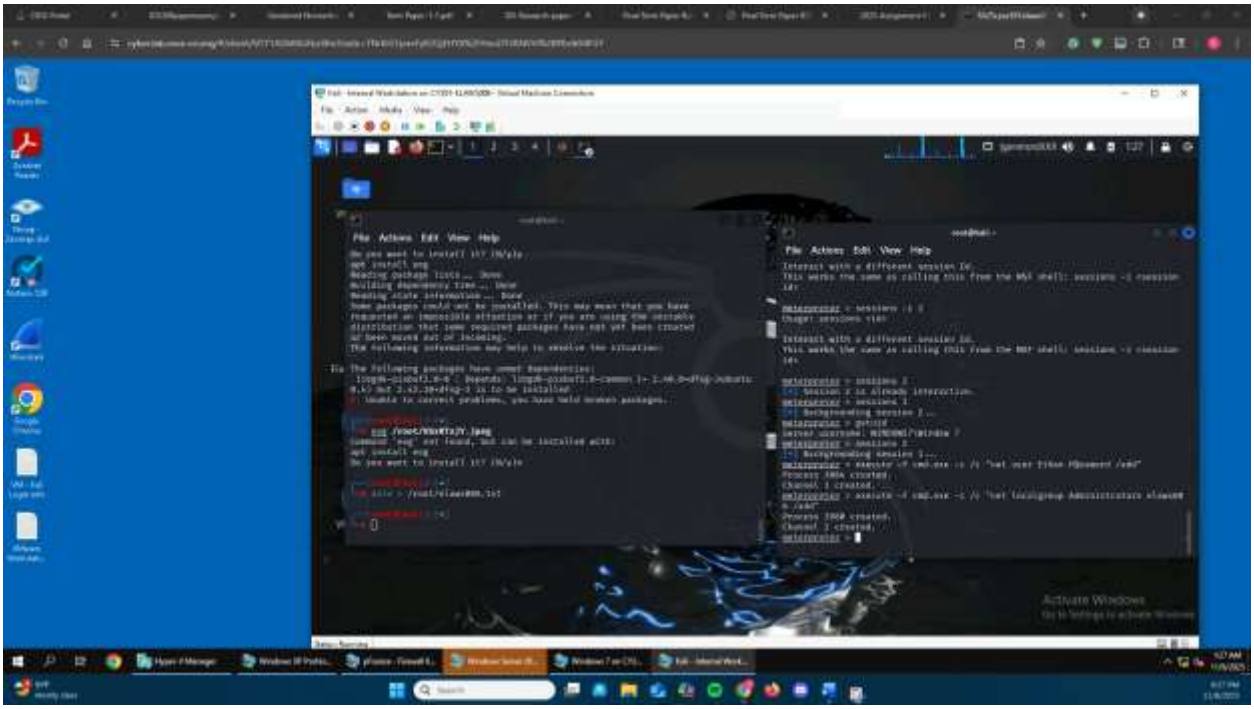
I created the text file with a timestamp and used the upload command to place it on the desktop of the Windows 7 machine. The command is on the top photo on the right.

4.



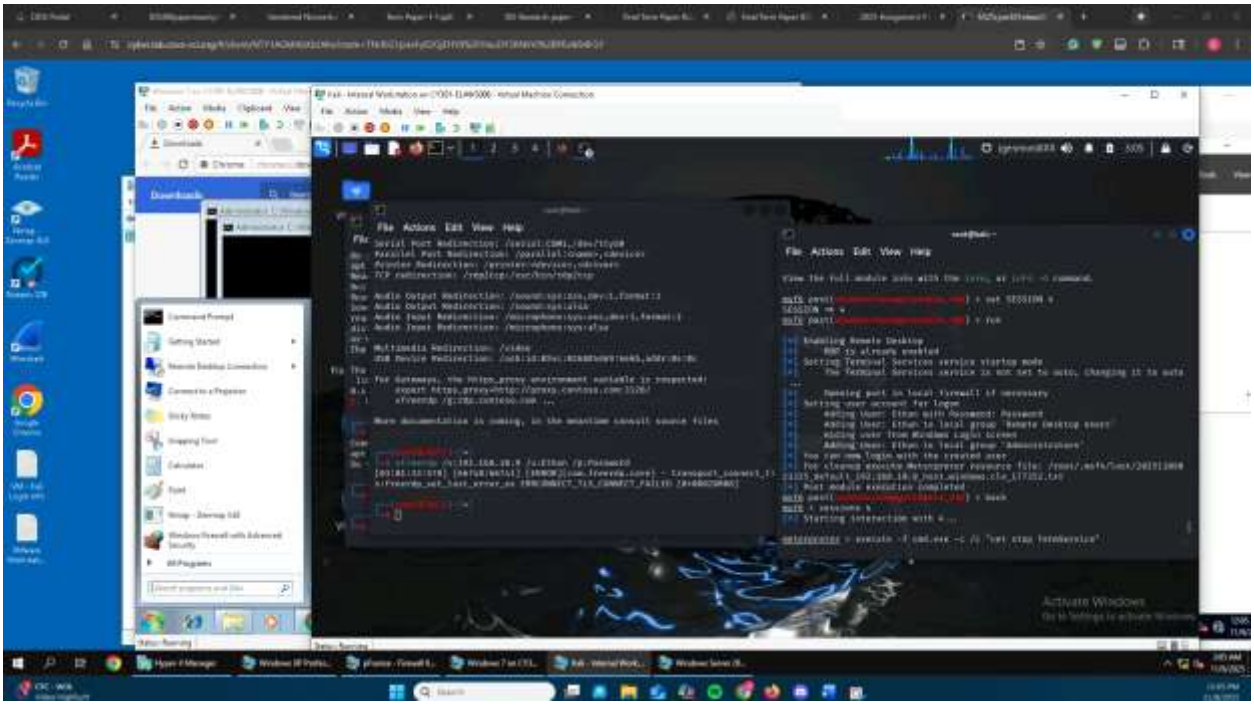
I gained administrator level privileges by backgrounding the current session and utilizing the bypassuac module.

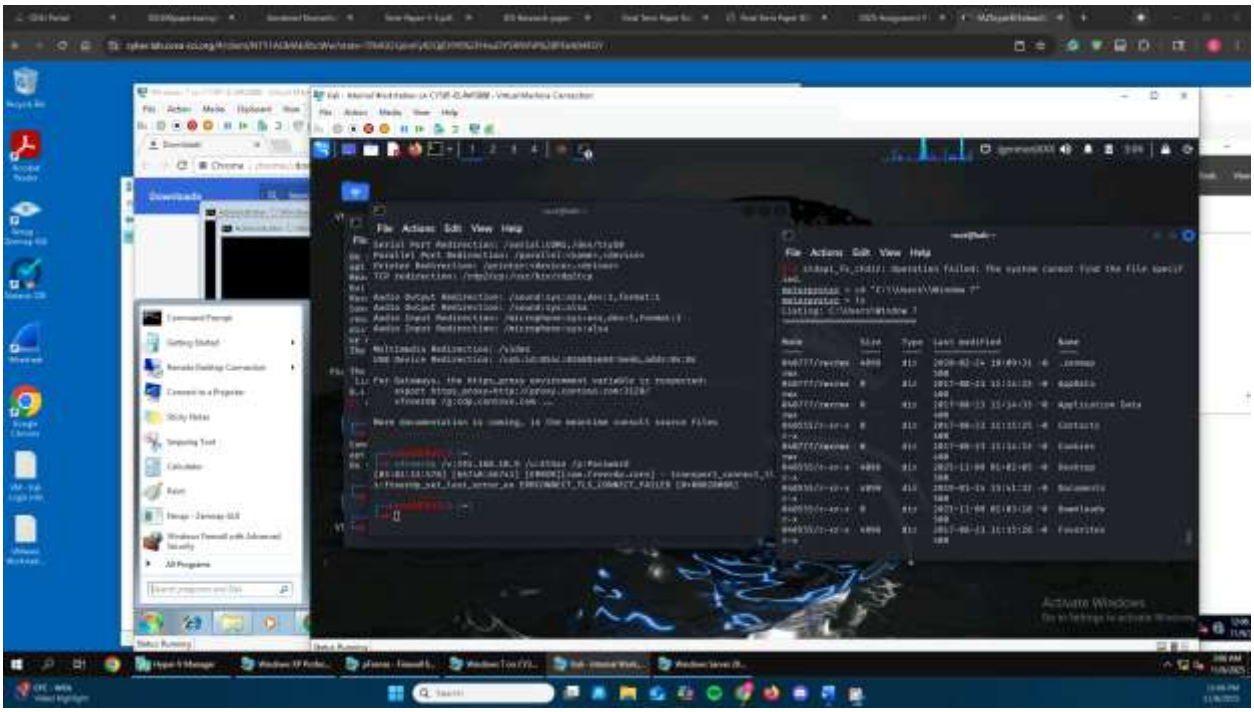
5a.



Using my advanced privileges I created a new account and added it to the administrator group.

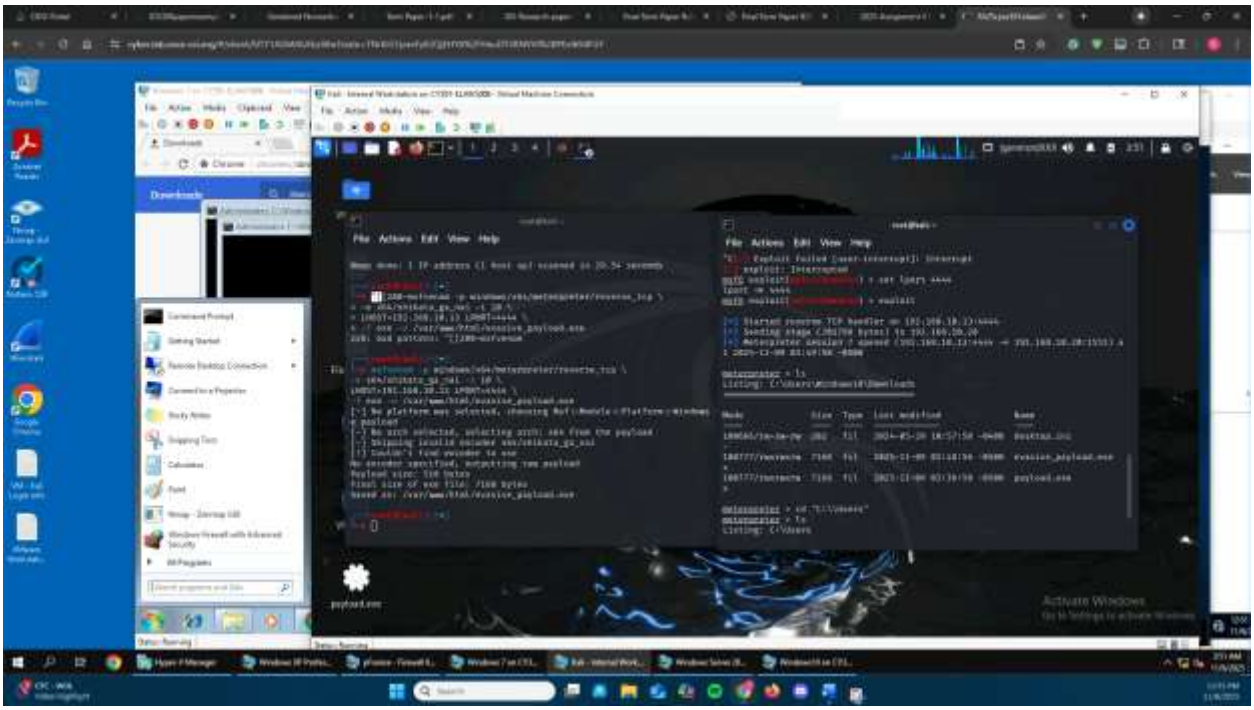
b.

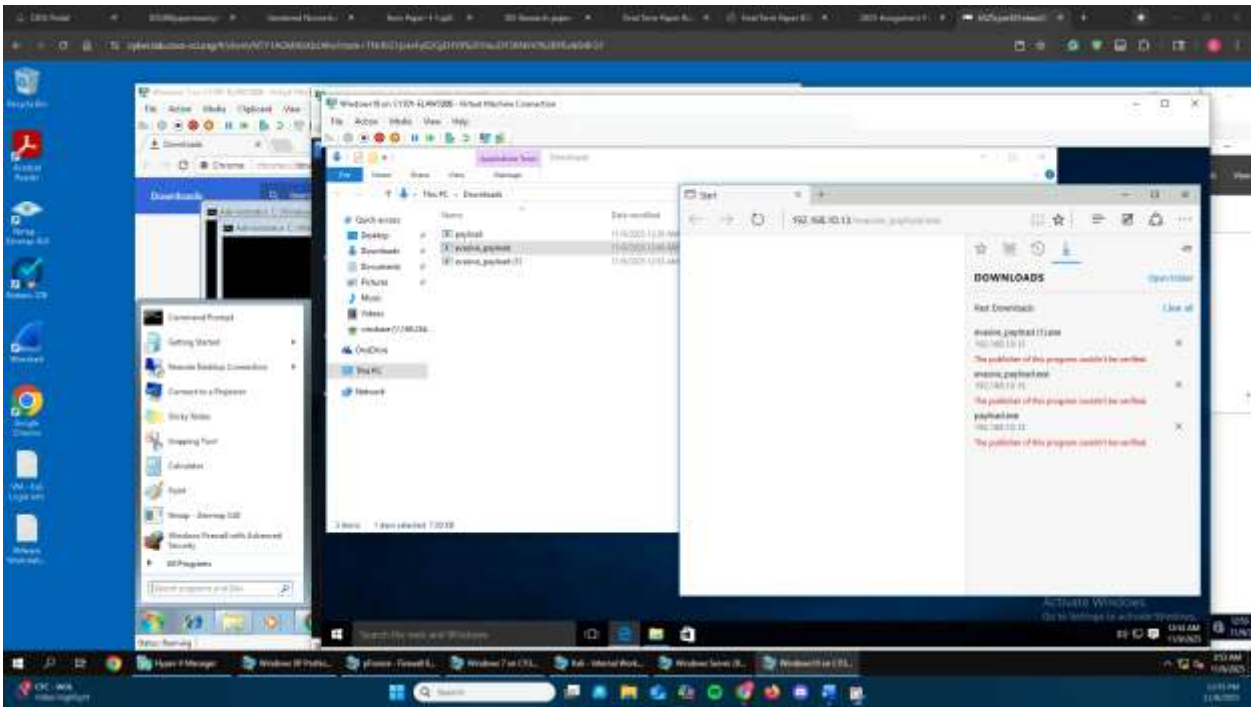




Bypassuac allowed me to create new users and add them to the administrator group. In the photo you can see that I set the wrong user to administrator which led to me accidentally exiting the entire msfconsole ending my sessions (big oof). I had to go through some of the steps again but corrected my mistake. I then used enable_rdp to access the Windows 7 machine with the account I created. From there I was able to navigate the directory on that machine and browse folders belonging to the “Window 7” user.

TASK D





I made a payload and uploaded it to the apache server which I installed and ran from Windows 10. This established a reversed shell connection and allowed me access to its files.

Your lab report MUST satisfy the following Requirements. Otherwise, you will lose points.

- R1 - Include a cover page with your UIN and name.
- R2 - Align your screenshot(s) with the task ID and description.
- R3 – Use “Snipping tool” or other tools, such as “Snipaste”, to take screenshot. MacOS user can follow this post to take screenshots.
- R4 - Include the running VMs (1), system timestamp (2) and session information (3) in every single screenshot.
- R5 - Explain your step(s).