OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

Assignment #4: Ethical Hacking

Antonio Shields

At the end of this module, each student must submit a report indicating the completion of the following tasks. Make sure you take screenshots as proof.
You need to power on the following VMs for this assignment.

- **Internal Kali (Attacker)**
- pfSense VM (power on only)
- Windows XP or Windows Server 2008 or Windows 7 (depending on the subtasks).

TASK A: EXPLOIT SMB ON WINDOWS XP WITH METASPLOIT (20 PT, 2PT EACH)

In this task, you need to complete the following steps to exploit SMB vulnerability on Windows XP.

1. Run a port scan against the Windows XP using nmap command to identify open ports and services.
2. Identify the SMB port number (default: 445) and confirm that it is open.

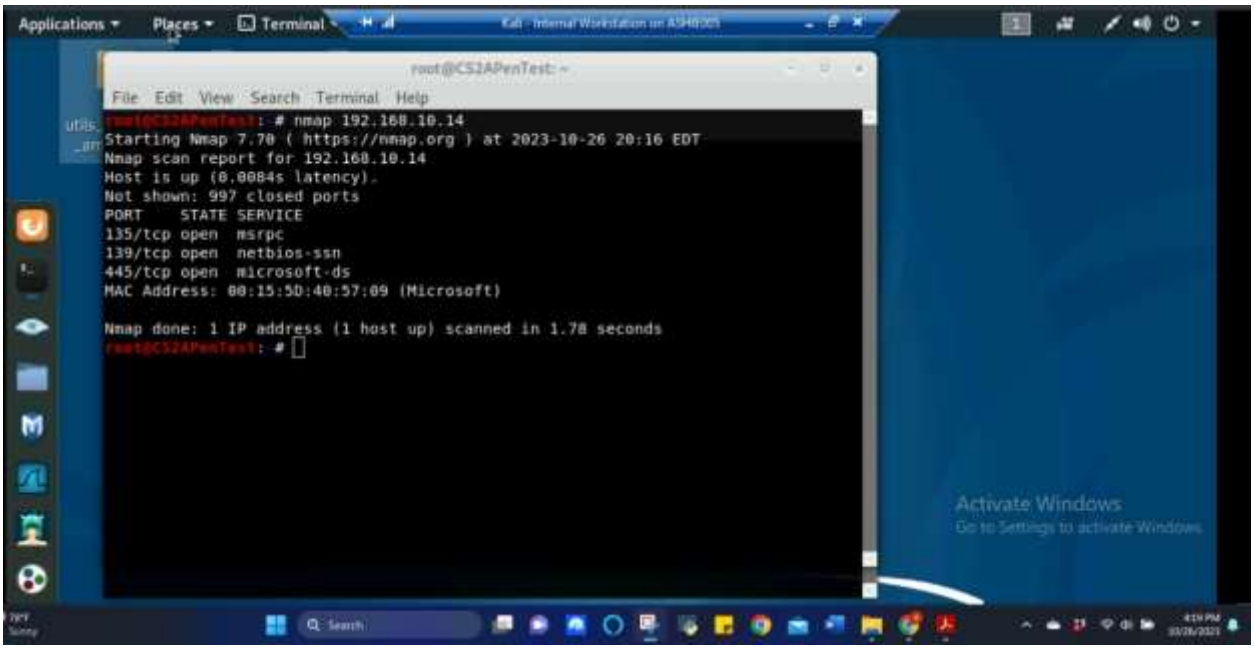

Figure 1 Screenshot of nmap being ran on Internal Kali to perform port scan and confirmation of port 445 being open for Windows XP for Task A.1 and Task A.2

The above screenshot shows nmap being ran on 192.168.10.13 (Internal Kali) to port scan 192.168.217.14 (Windows XP) for open ports and to confirm that port 445 was indeed open.

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

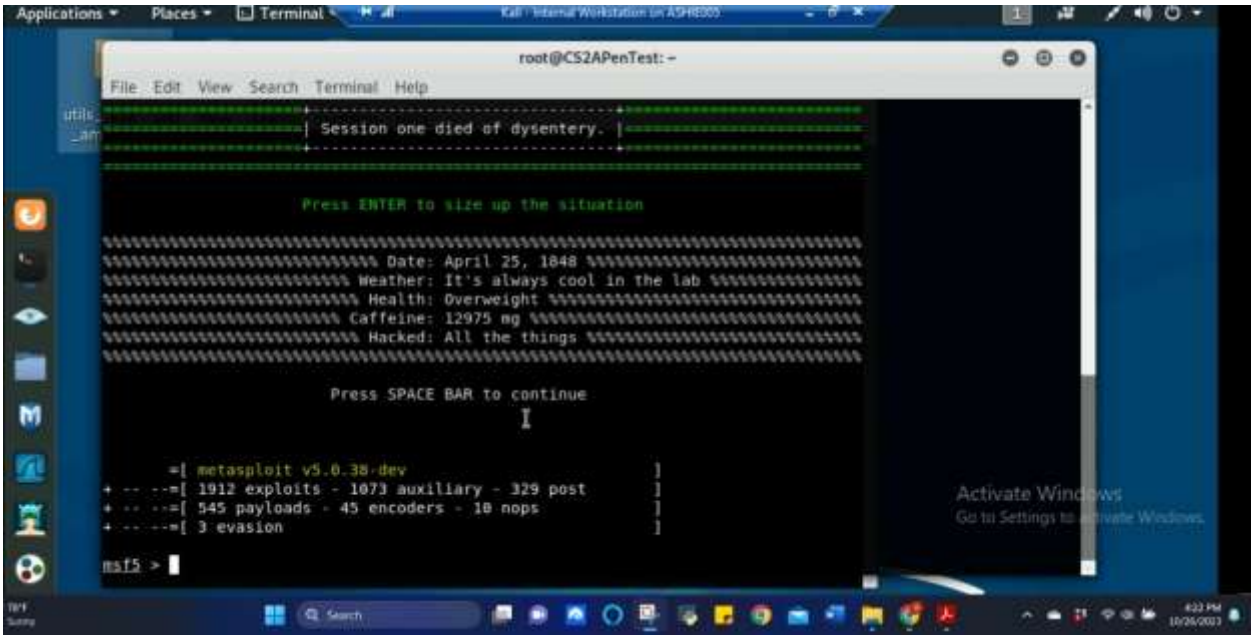

Figure 2 Screenshot of metasploit being open and activated for Task A.3

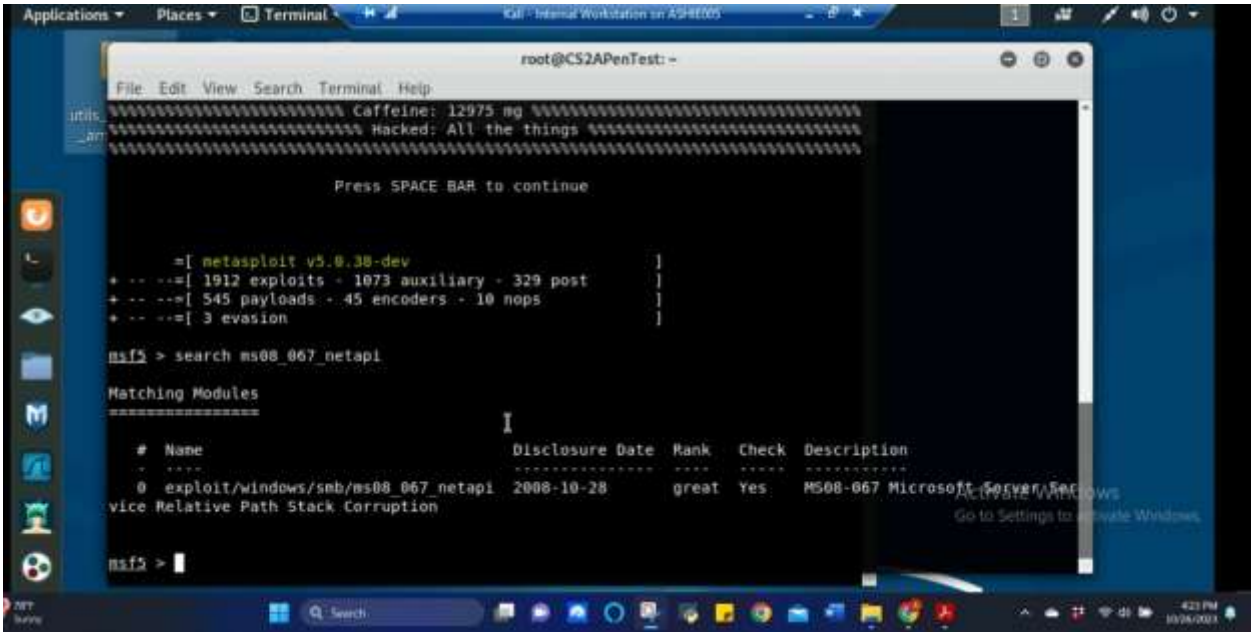

Figure 3 Screenshot of searching ms08_067_netapi in metasploit and the results for Task A.3

The above screenshots shows metasploit being initiated on 192.168.10.13 (Internal Kali) and once loaded, ms08_067_netapi was searched and the exploit results were found.

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

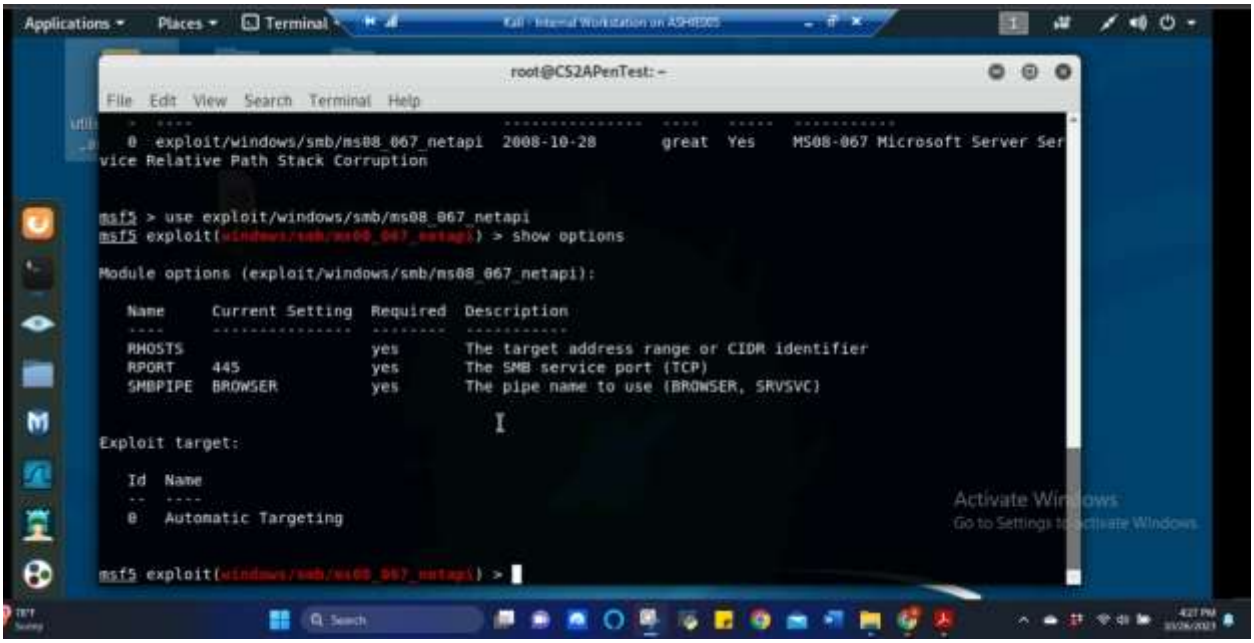

Figure 4 Screenshot of the windows/smb/ms08_067_netapi exploit being used and the options needed prior to the exploit being executed for Task A.4

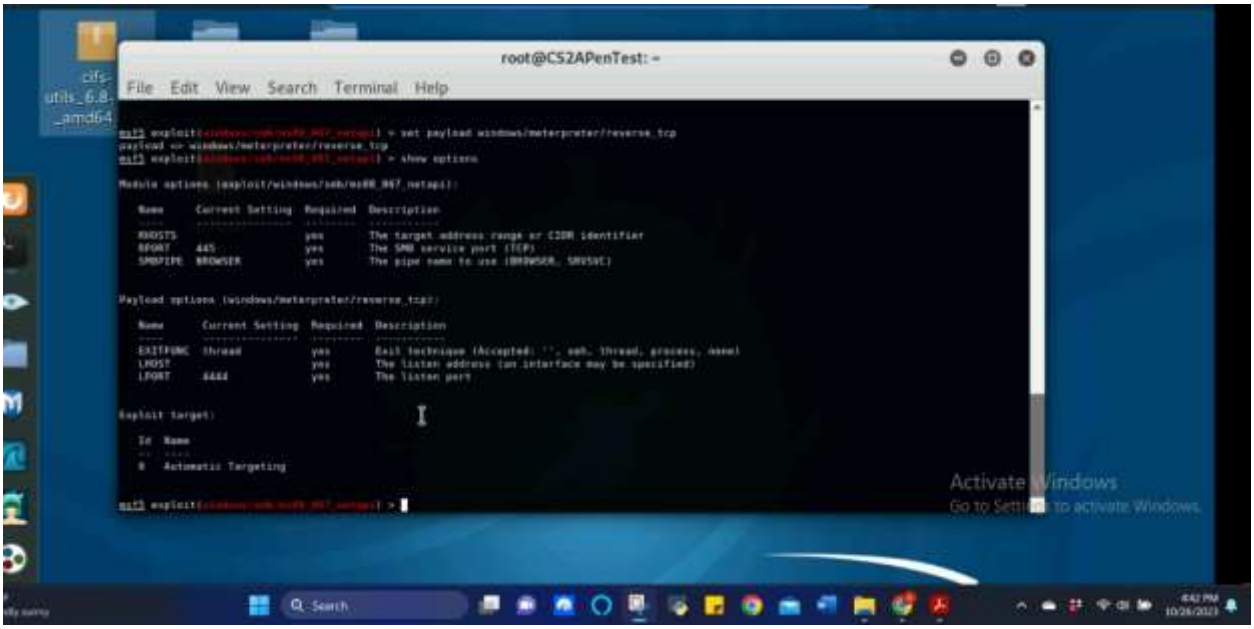

Figure 5 Screenshot of the windows/meterpreter/reverse_tcp payload being set and the options needed prior to the exploit being executed for Task A.4

The above screenshots shows ms08_067_netapi being used as the exploit module and meterpreter reverse_tcp being set as the payload 192.168.10.13 (Internal Kali).

5. Use ***4498*** as the listening port number. Configure the rest of the parameters. Display your configurations and exploit the target.

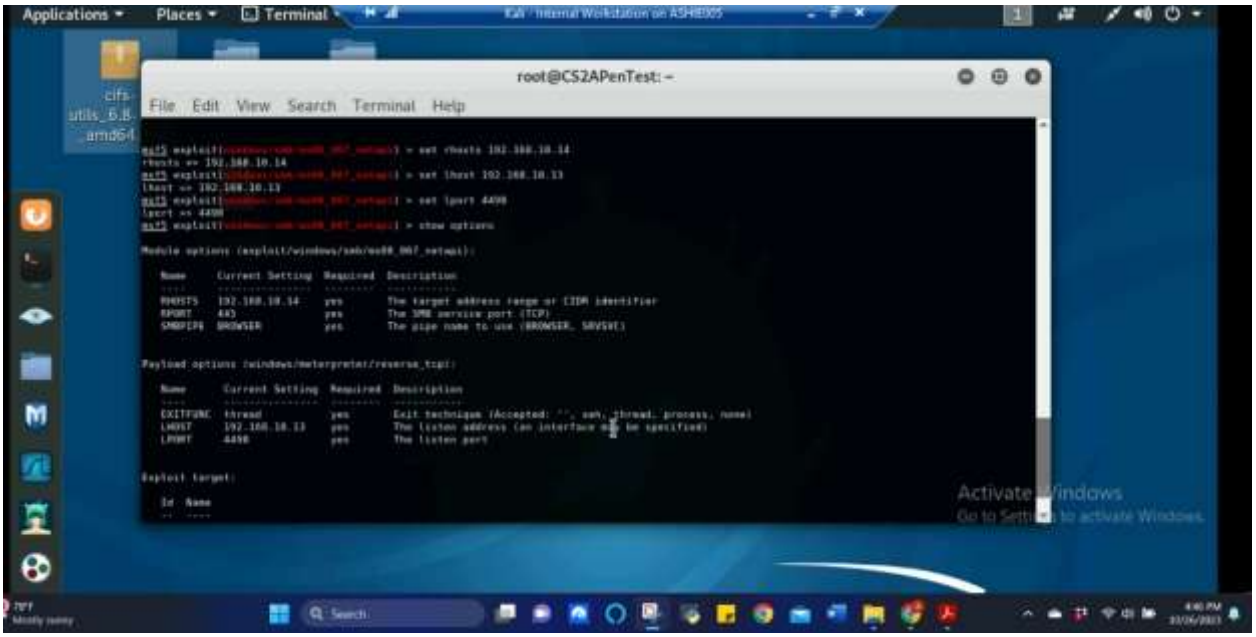

Figure 6 Screenshot of the parameters being set prior to the exploit being executed for Task A.5

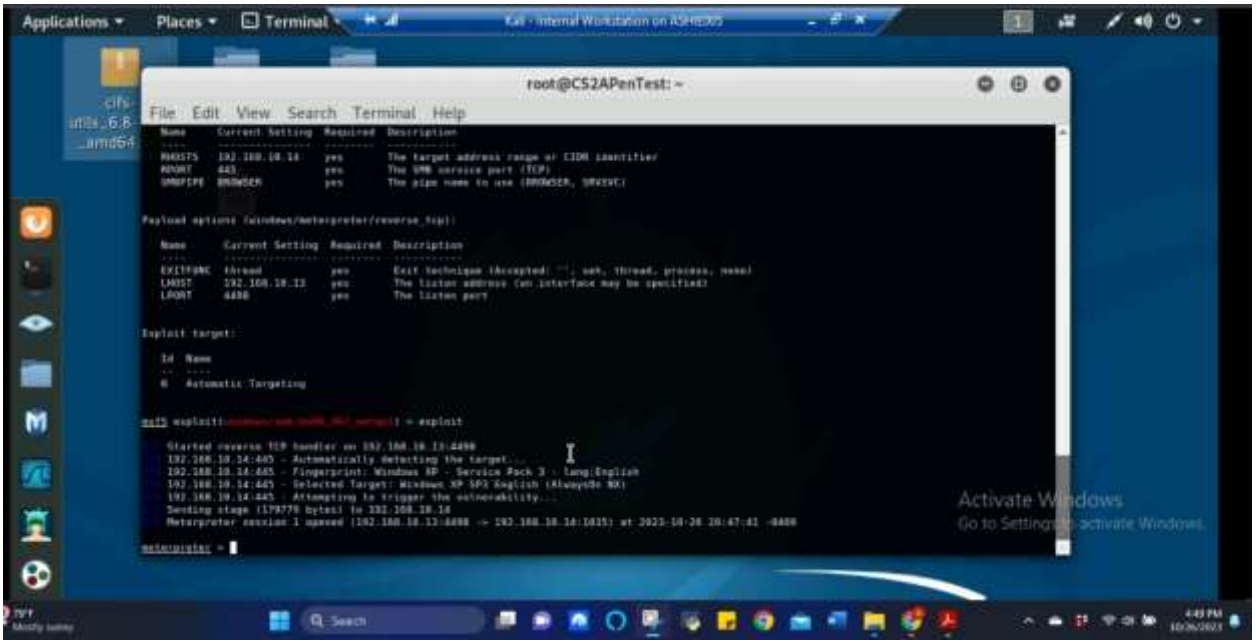

Figure 7 Screenshot of the windows/smb/ms08_067_netapi being exploited for Task A.5

The above screenshots confirmed the parameters being properly set and windows/smb/ms08_067_netapi being successfully exploited.

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

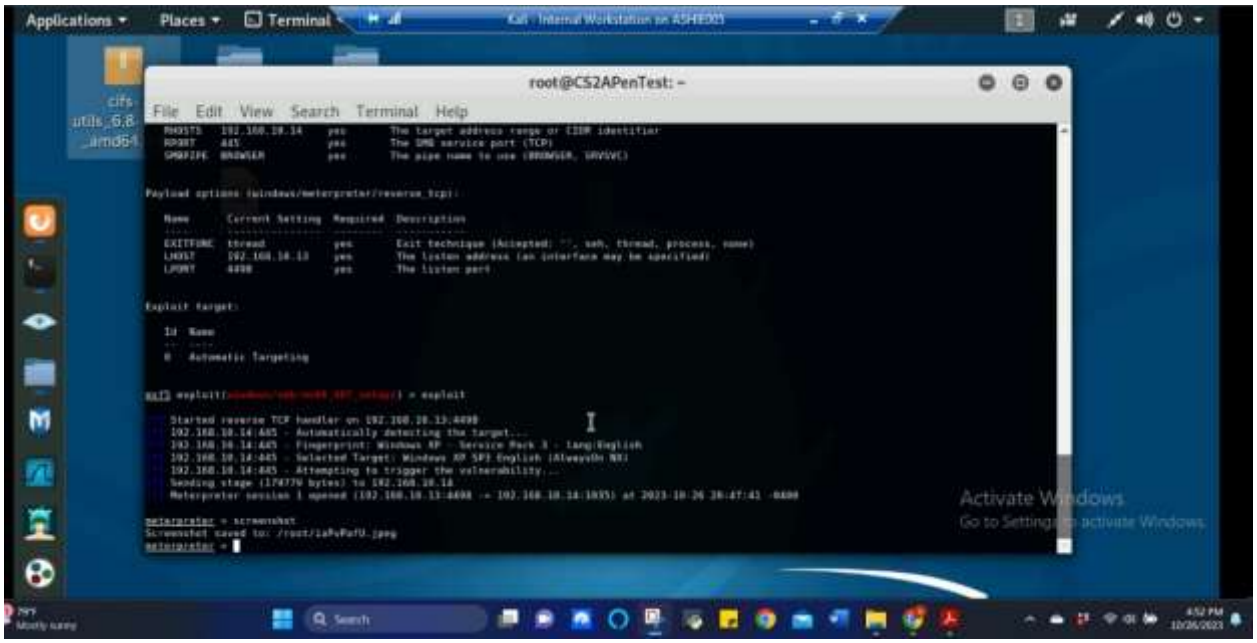

Figure 8 Screenshot of screenshot command being executed for Task A.6

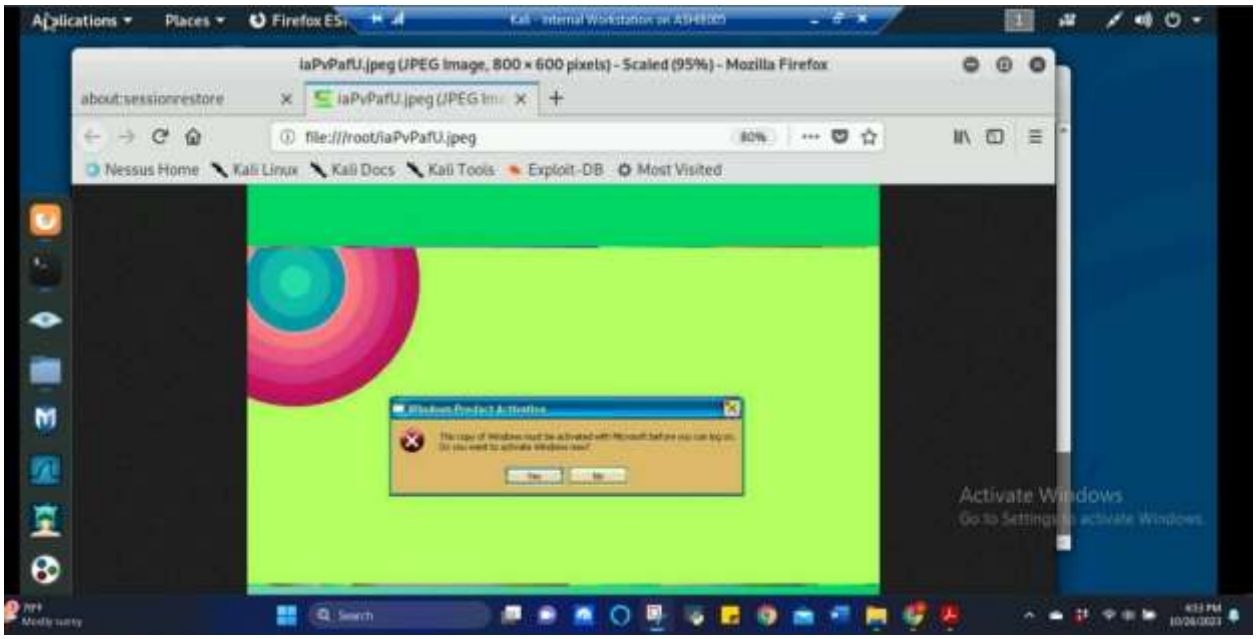

Figure 9 Screenshot of results of the screenshot command being executed for Task A.6

The above screenshots show the screenshot command being executed in meterpreter and the results of that screenshot command.

7. [Post-exploitation] In meterpreter shell, display the target system's local date and time.
8. [Post-exploitation] In meterpreter shell, get the SID of the user.
9. [Post-exploitation] In meterpreter shell, get the current process identifier.
10. [Post-exploitation] In meterpreter shell, get system information about the target.

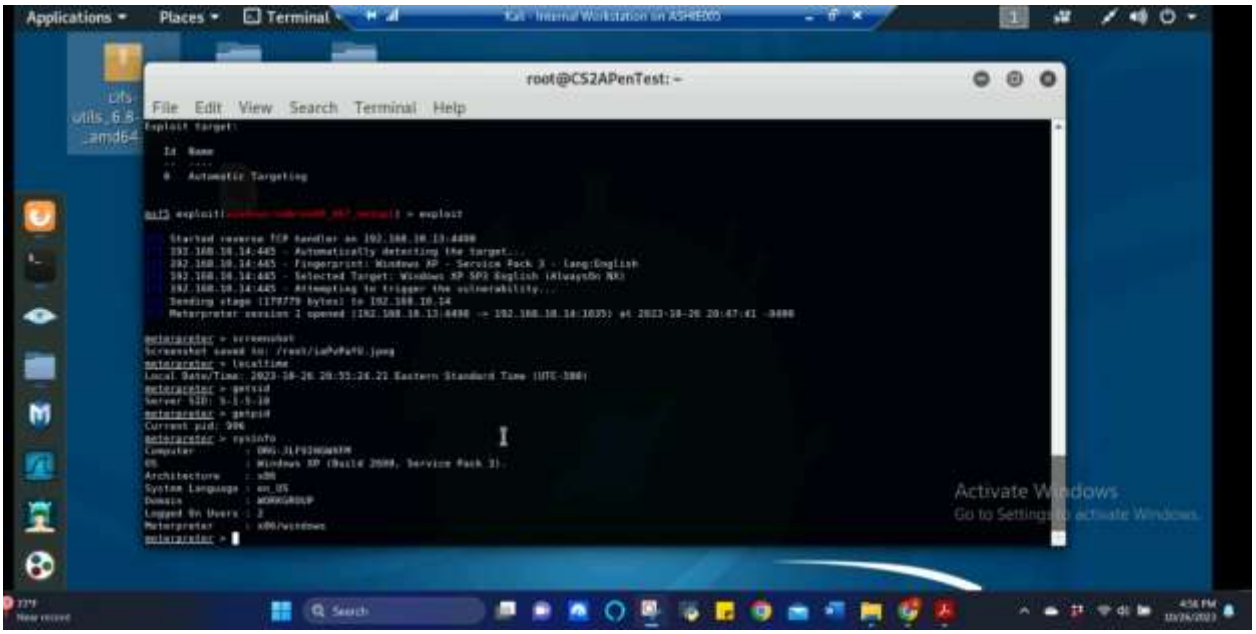

Figure 10 Screenshot of command results for localtime, getsid, getpid, and sysinfo for Task A.7, A.8, A.9, and A.10

The above screenshot shows the localtime, getsid, getpid, and sysinfo commands being executed for Tasks A.7-10 and their respective results in meterpreter.

TASK B. EXPLOIT ETERNALBLUE ON WINDOWS SERVER 2008 WITH METASPLOIT (20PT)

In this task, you need to use similar steps to exploit the **EternalBlue** vulnerability on Windows Server 2008. Make sure to search and replace the exploit module against Windows Server 2008 accordingly.

1. Configure your Metasploit accordingly and set 4498 as the listening port number. Display the configuration and exploit the target. **(10 pt)**

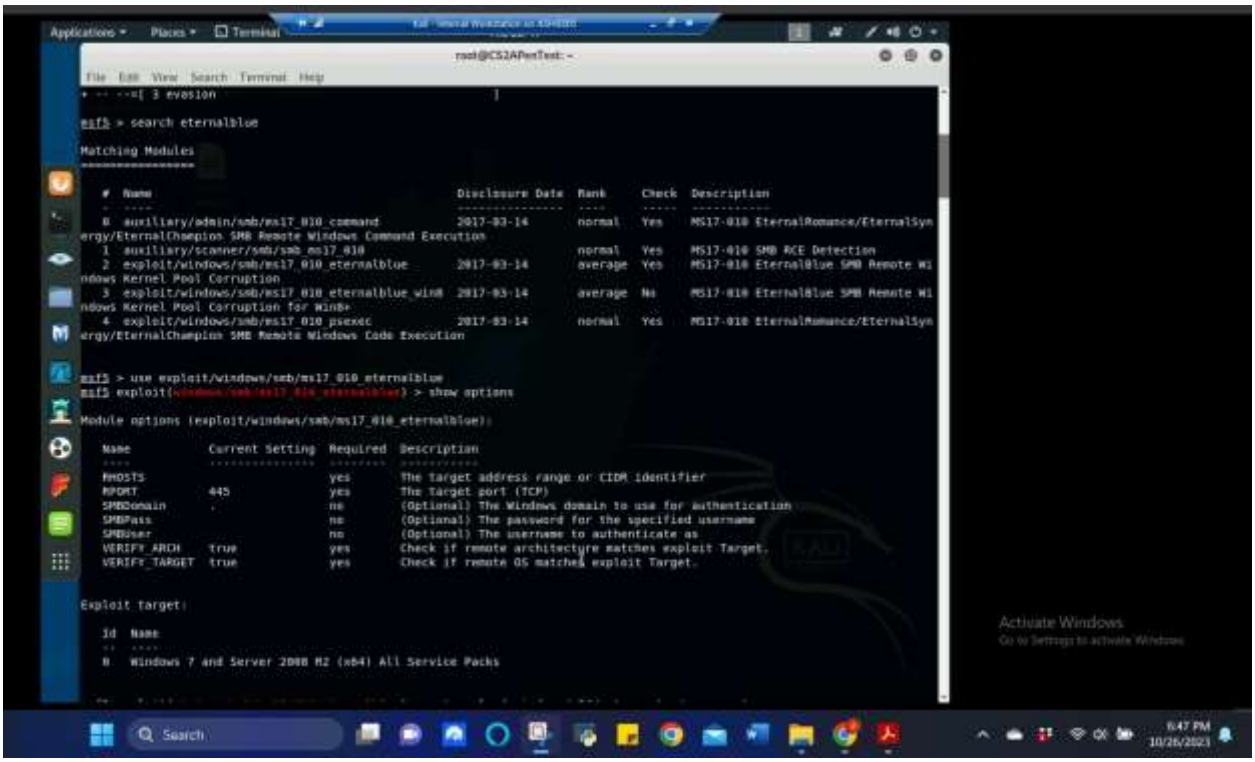

Figure 11 Screenshot of searching eternalblue in Metasploit, the results, and selecting an exploit to use and parameter requirements for Task B.1

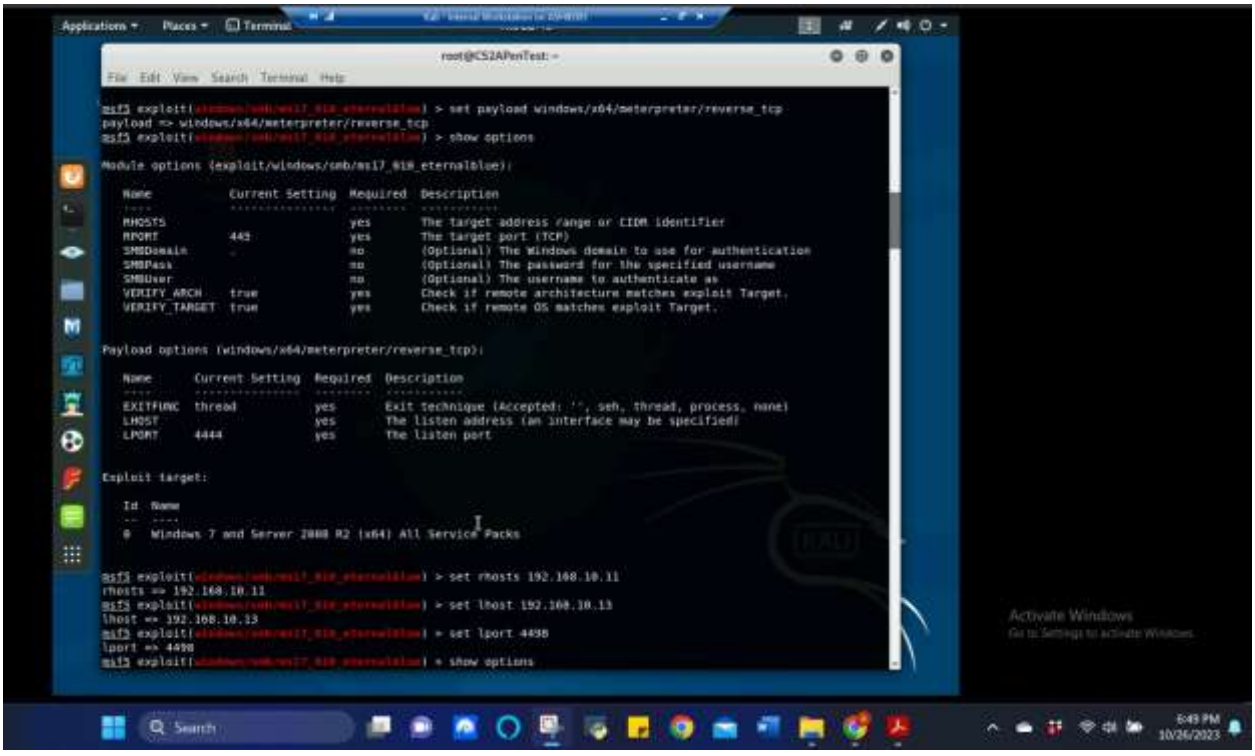

Figure 12 Screenshot of setting parameter requirements for windows/smb/ms17_010_eternalblue and payload windows/x64/meterpreter/reverse_tcp for Task B.1

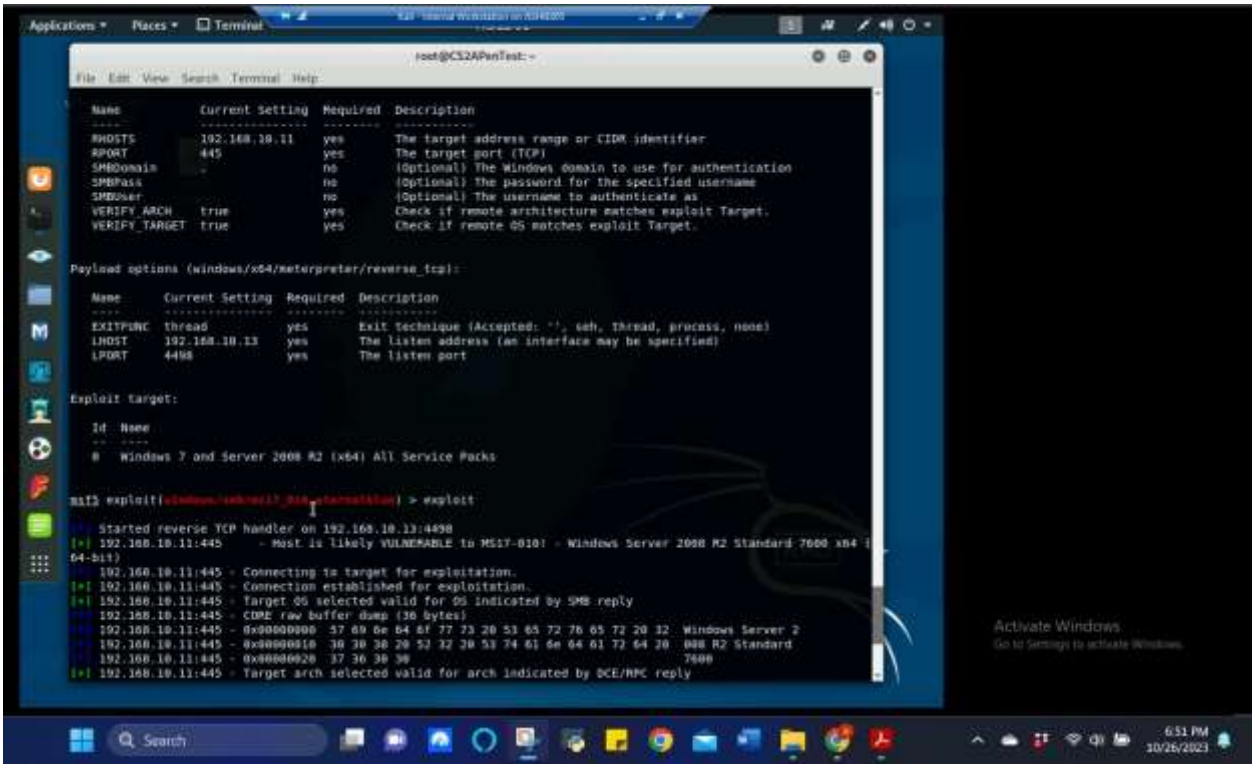

Figure 13 Screenshot of exploit being executed after setting parameter requirements for Task B.1

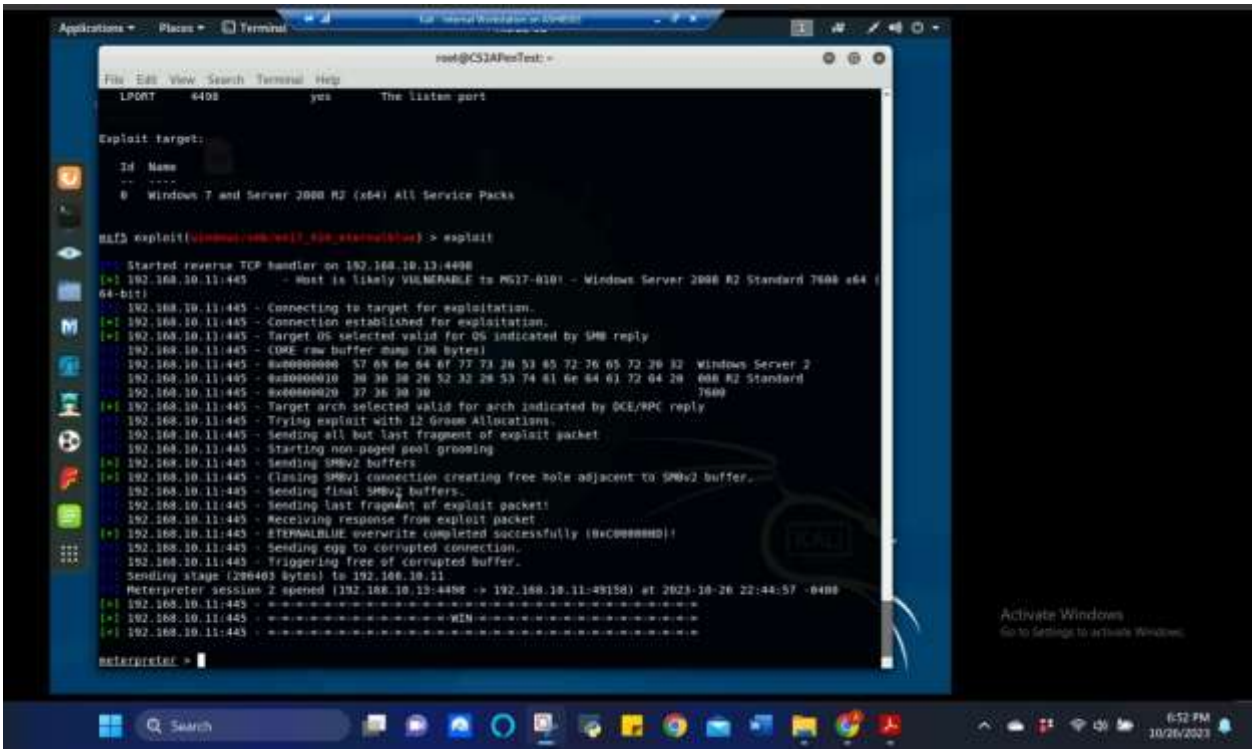

Figure 14 Screenshot of successful execution of exploit for Task B.1

The above screenshots show the configuration of eternalblue exploit in Metasploit with the appropriate payload along with successful execution of the exploit.

2. [Post-exploitation] Execute the screenshot command to take a screenshot of the target machine if the exploit is successful. **(2 pt)**

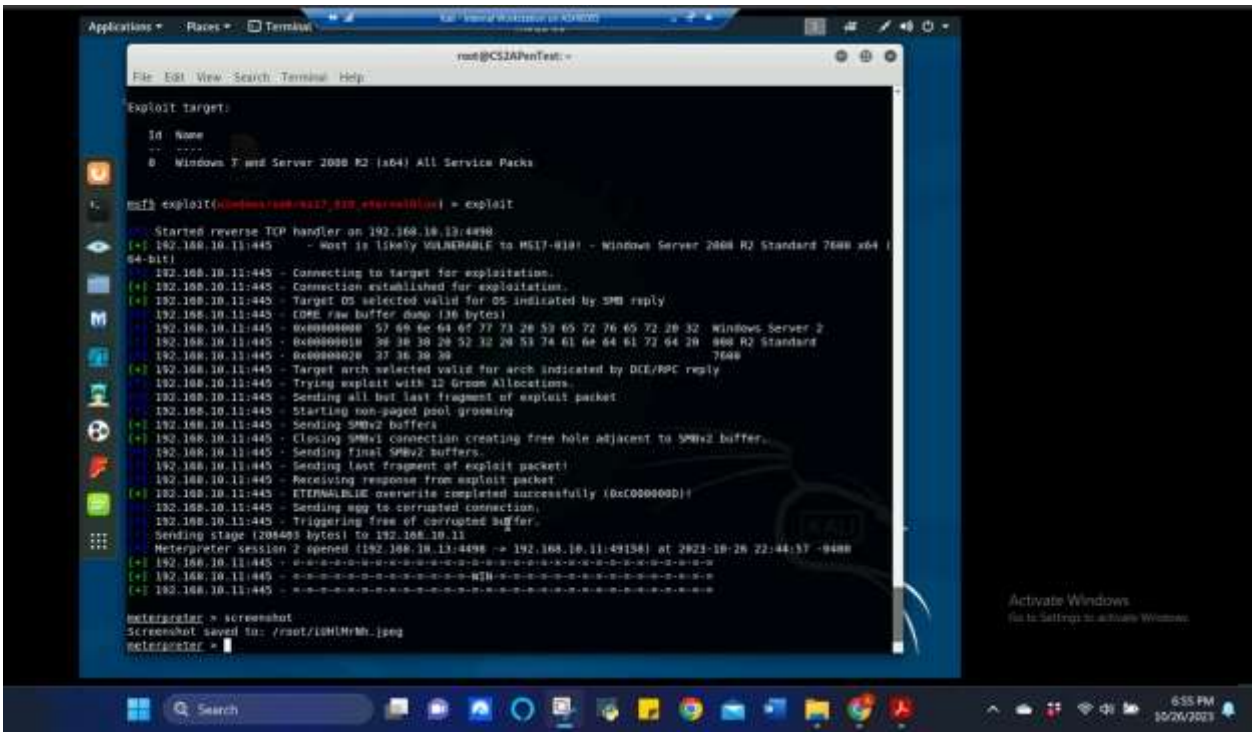

Figure 15 Screenshot of screenshot command being executed for Task B.2

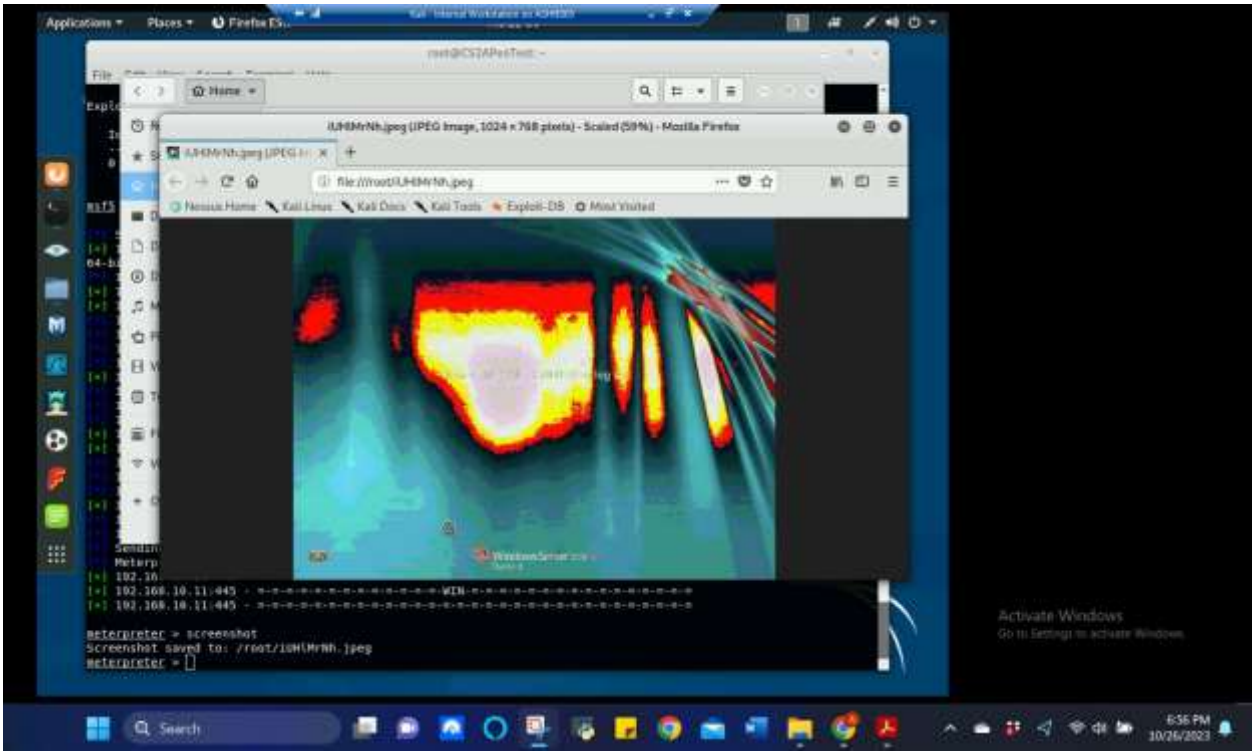

Figure 16 Screenshot of results of screenshot command being executed for Task B.2

The above screenshots show the screenshot command being executed in meterpreter and the results of that screenshot command.

3. [Post-exploitation] In meterpreter shell, display the target system's local date and time. **(2 pt)**
4. [Post-exploitation] In meterpreter shell, get the SID of the user. **(2 pt)**
5. [Post-exploitation] In meterpreter shell, get the current process identifier. **(2 pt)**
6. [Post-exploitation] In meterpreter shell, get system information about the target. **(2 pt)**

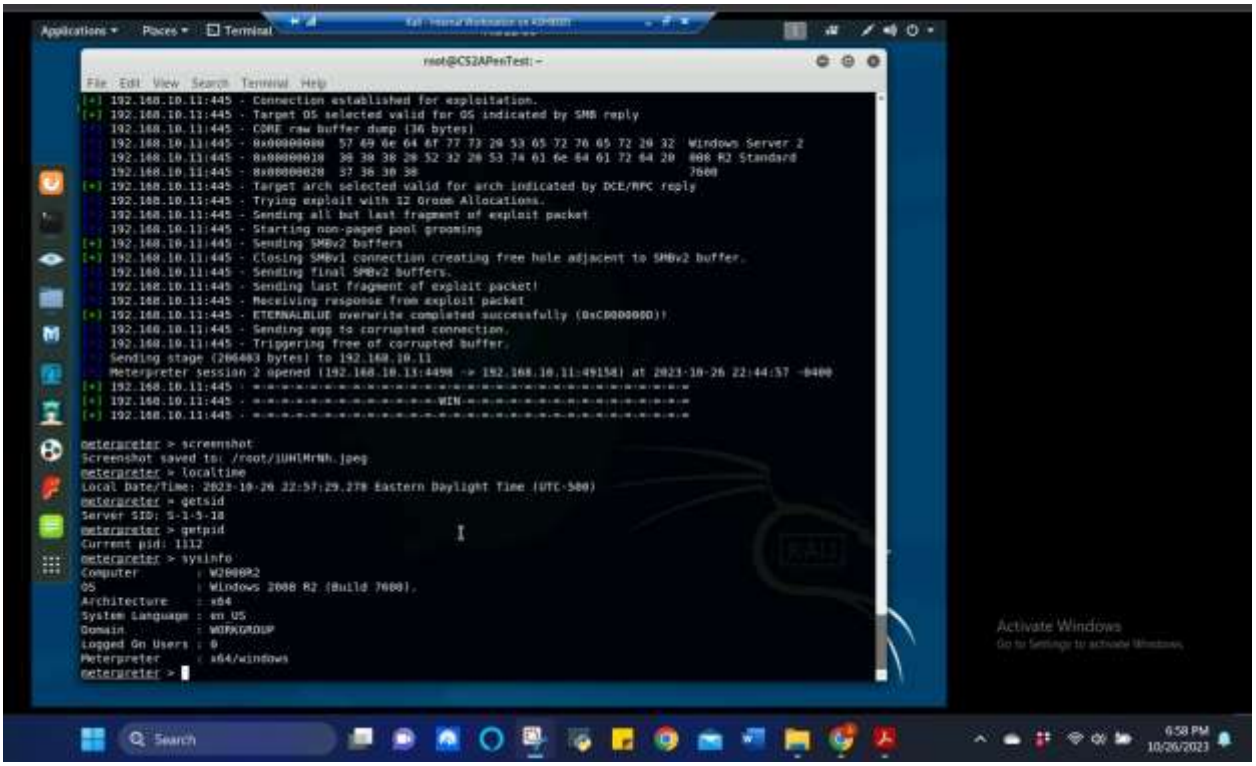

Figure 17 Screenshot of command results for localtime, getsid, getpid, and sysinfo for Task B.3, B.4, B.5, and B.6

The above screenshot shows the localtime, getsid, getpid, and sysinfo commands being executed for Tasks B.3-6 and their respective results in meterpreter.

TASK C. EXPLOIT WINDOWS 7 WITH A DELIVERABLE PAYLOAD.

In this task, you need to create an executable payload with the required configurations below. 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 **(20 pt)**. Of course, don't forget to configure your Metasploit on Kali Linux before the payload is triggered on the target VM.

The requirements for your payload are **(10 pt, 5pt each)**:

- Payload Name: Use your MIDAS ID (for example, pjiang.exe)
- Listening port: ***4498***

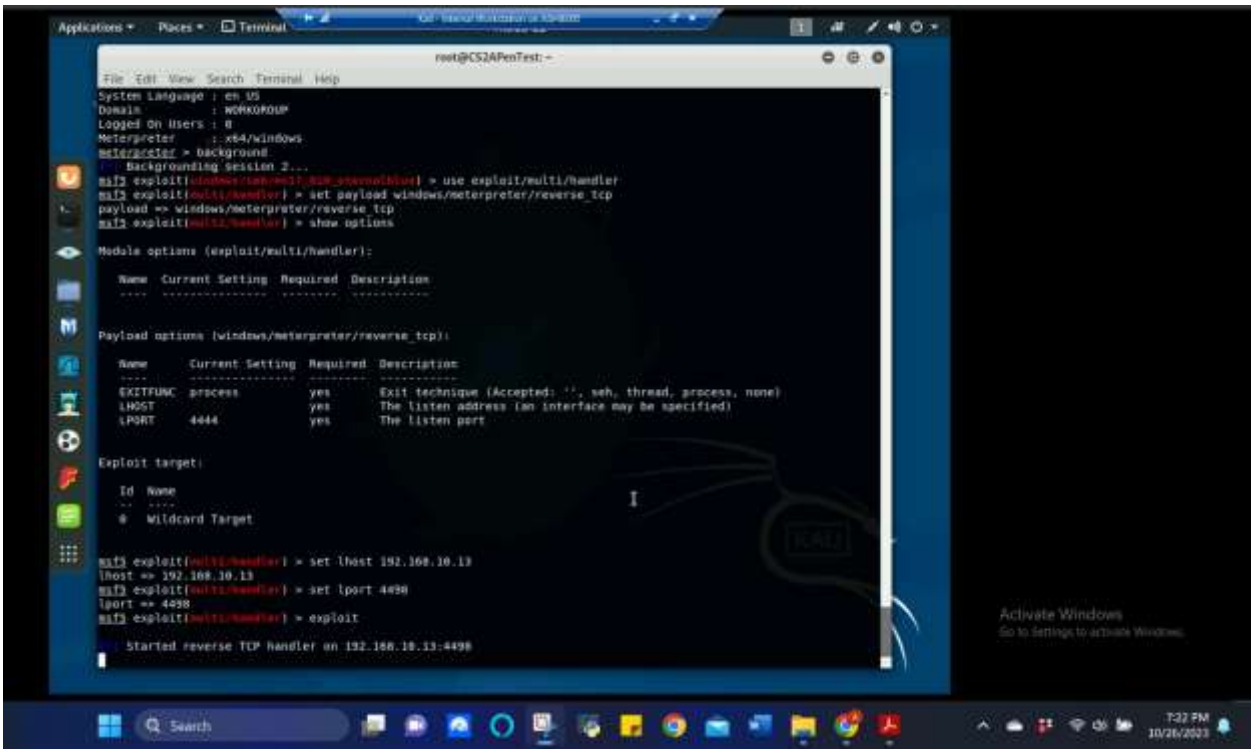

Figure 18 Screenshot of backgrounding session, using multi/handler exploit, windows/meterpreter/reverse_tcp payload, and setting the required parameters for executing the exploit for Task C

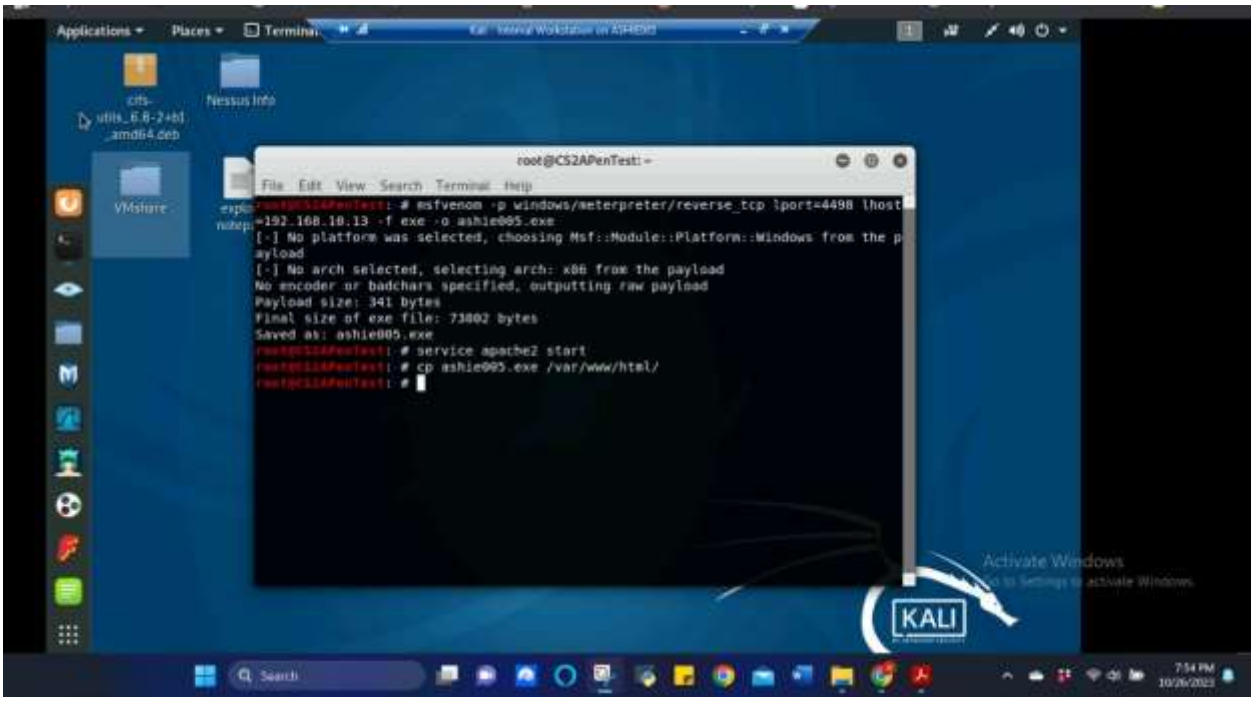

Figure 19 Screenshot of msfvenom being used to create executable payload using MIDAS ID for Task C

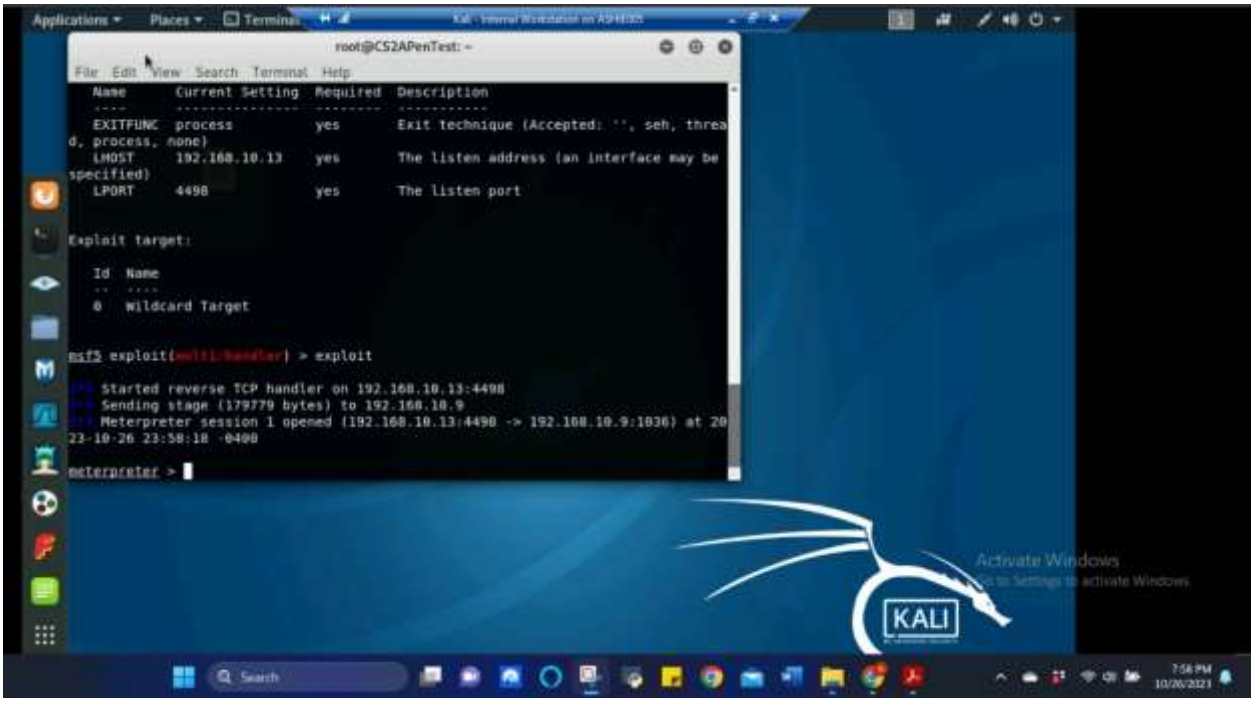

Figure 20 Screenshot of executable payload being successfully exploited from 192.168.10.9 (Windows 7) for Task C

The above screenshots show backgrounding previous session, using multi/handler exploit, windows/meterpreter/reverse_tcp payload, and setting the required parameters for executing the exploit. Msfvenom was also used to create the executable payload to be opened by the Windows 7 user via website using the service apache2 start command. Once the user opens the payload, meterpreter is successfully opened and ready for sending commands.

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

1. Execute the screenshot command to take a screenshot of the target machine if the exploit is successful. **(10 pt)**

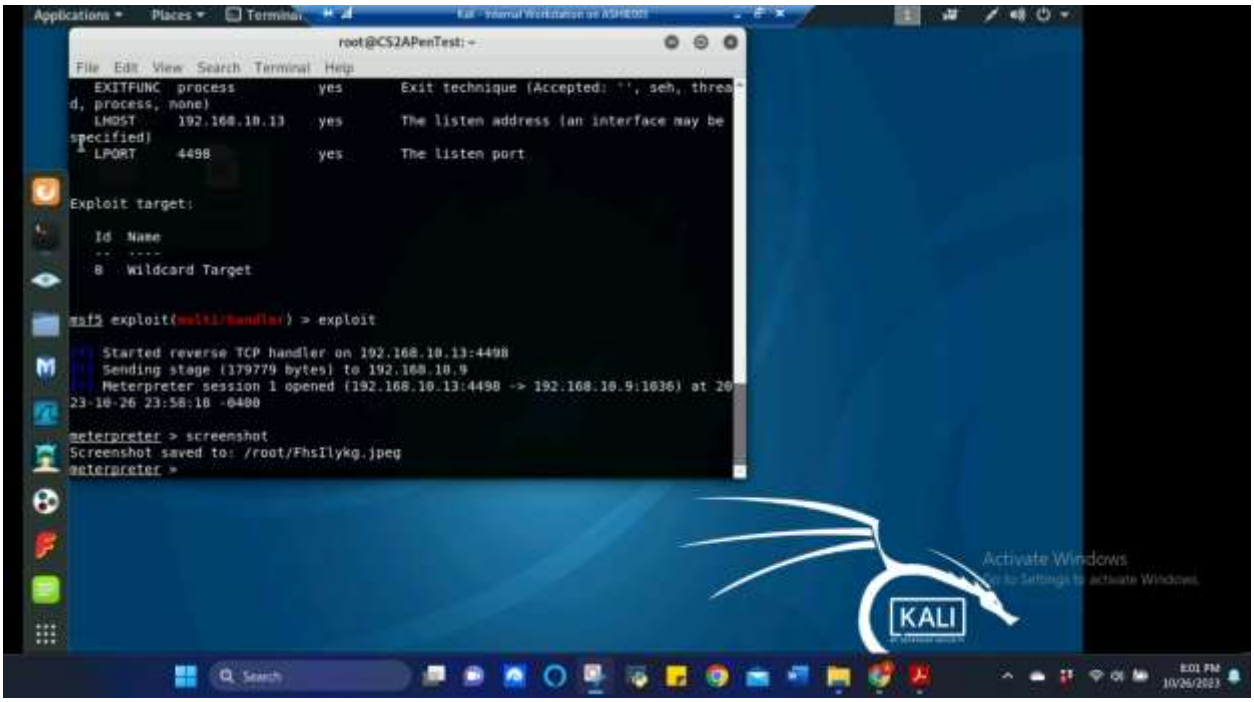

Figure 21 Screenshot results of screenshot command being executed for Task C.1

Figure 22 Screenshot of results of screenshot command being executed for Task C.1

The above screenshots show the screenshot command being executed in meterpreter and the results of that screenshot command.

2. 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.

Then log in to Windows 7 VM and check if the file exists. You need to show me the command that uploads the file. **(20 pt)**

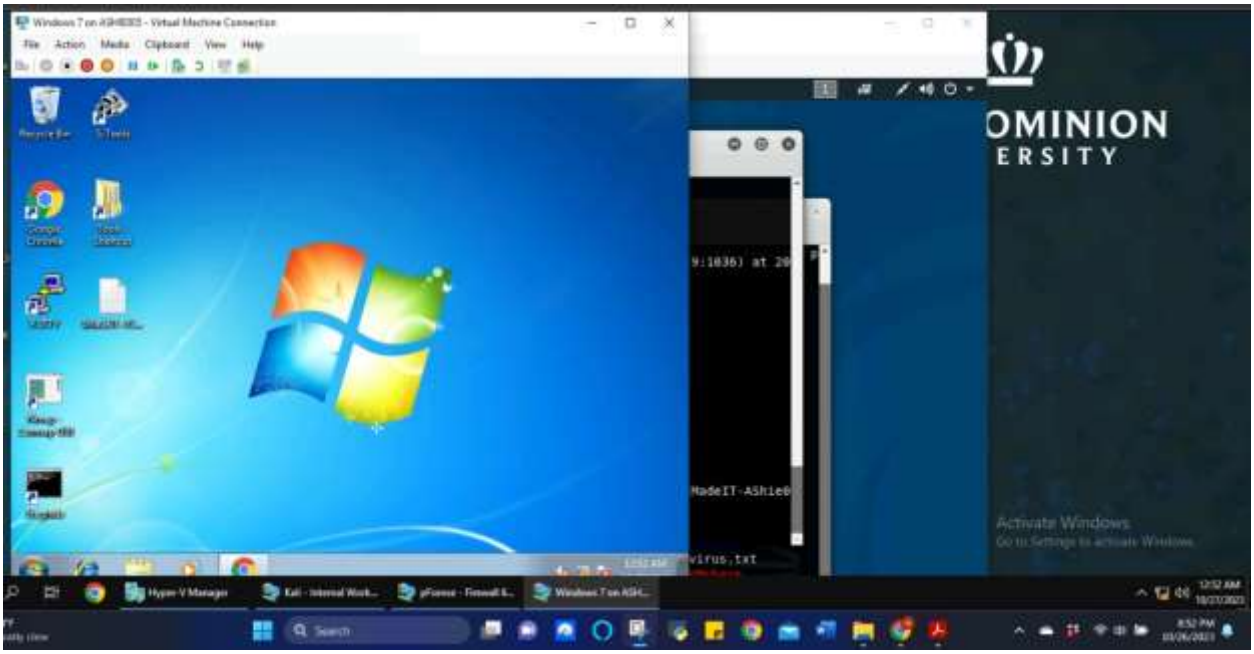

Figure 23 Screenshot of Windows 7 and IMadeIT file shown on user's desktop for Task C.2

Figure 24 Screenshot of the IMadeIT-AShie005.txt file and current time and date shown in the file for Task C.2

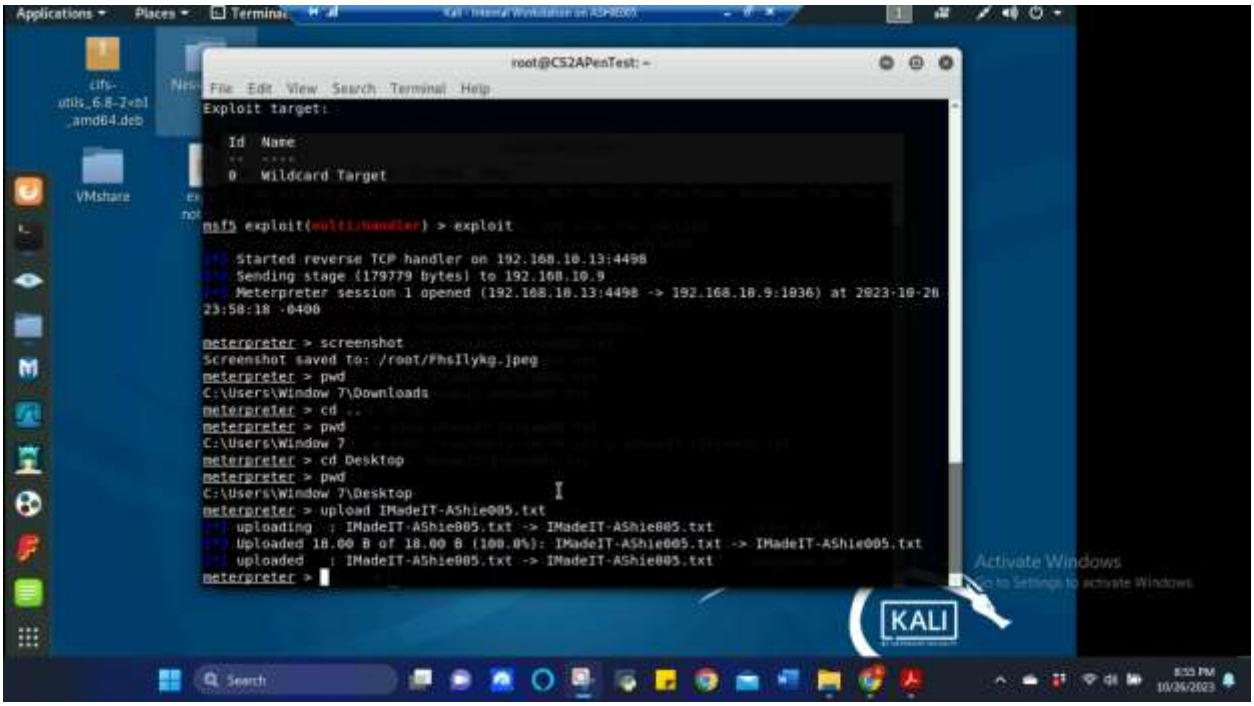

Figure 25 Screenshot of changing directory to the User's Desktop and uploading the IMadeIT-AShie005.txt file to the User's Desktop successfully for Task C.2

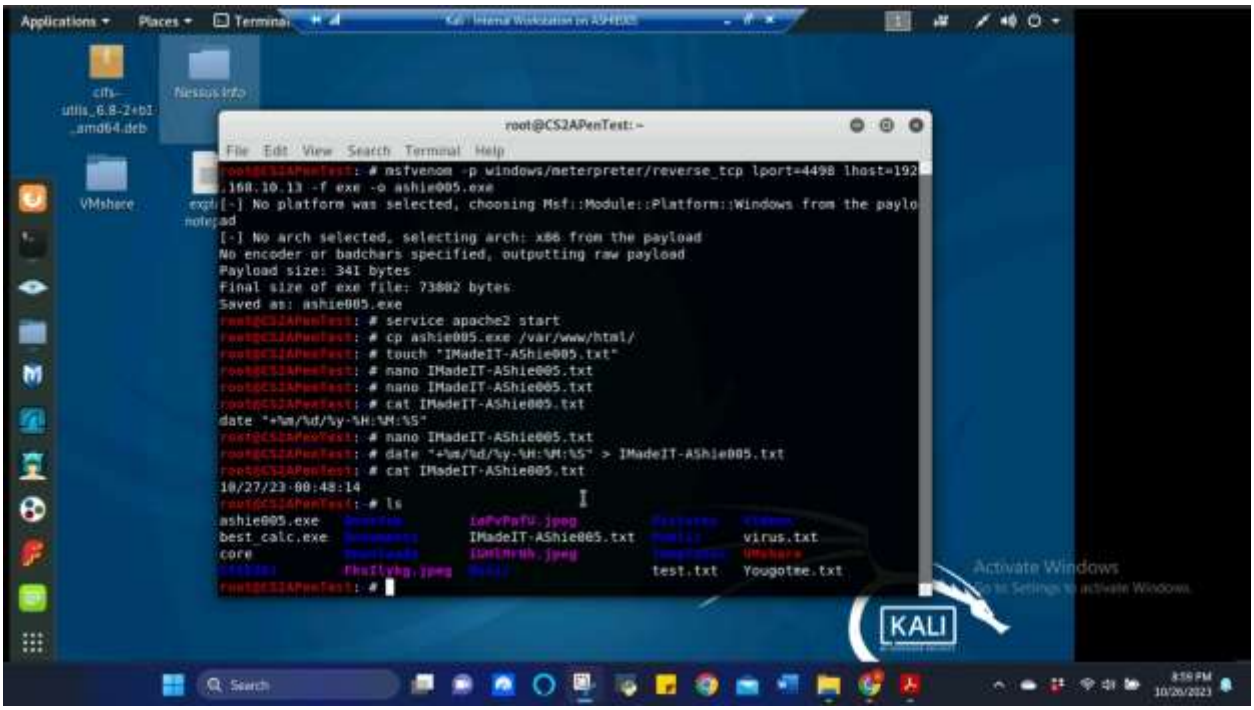

Figure 26 Screenshot of creating the IMadeIT-AShie005.txt file with the required current date and time stamp inputted into the file for Task C.2

The above screenshots show creating the IMadeIT-AShie005.txt file (Figure 26), changing the Windows 7 User's directory to get to their Desktop and uploading the IMadeIT file to their desktop (Figure 25). After uploading the file, confirming that the file uploaded correctly by accessing the Windows 7 User's Desktop (Figure 23) and opening the IMadeIT file (Figure 24).

[Privilege escalation, extra credit] Background your current session, then gain administrator-level privileges on the remote system (**10 pt**). After you escalate the privilege, complete the following tasks:

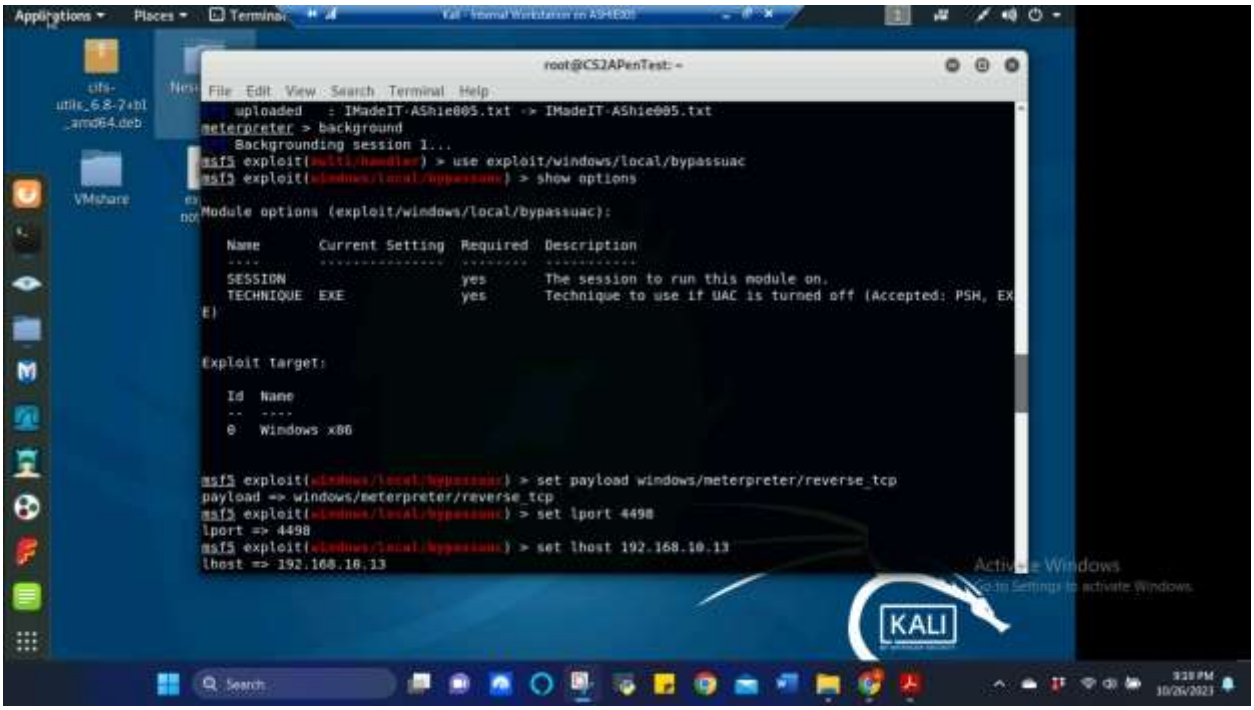

Figure 27 Screenshot of backgrounding the session and using windows/local/bypassuac exploit to escalate privilege to admin user in Windows 7 and setting required parameters and payload for Task C.Privilege Escalation

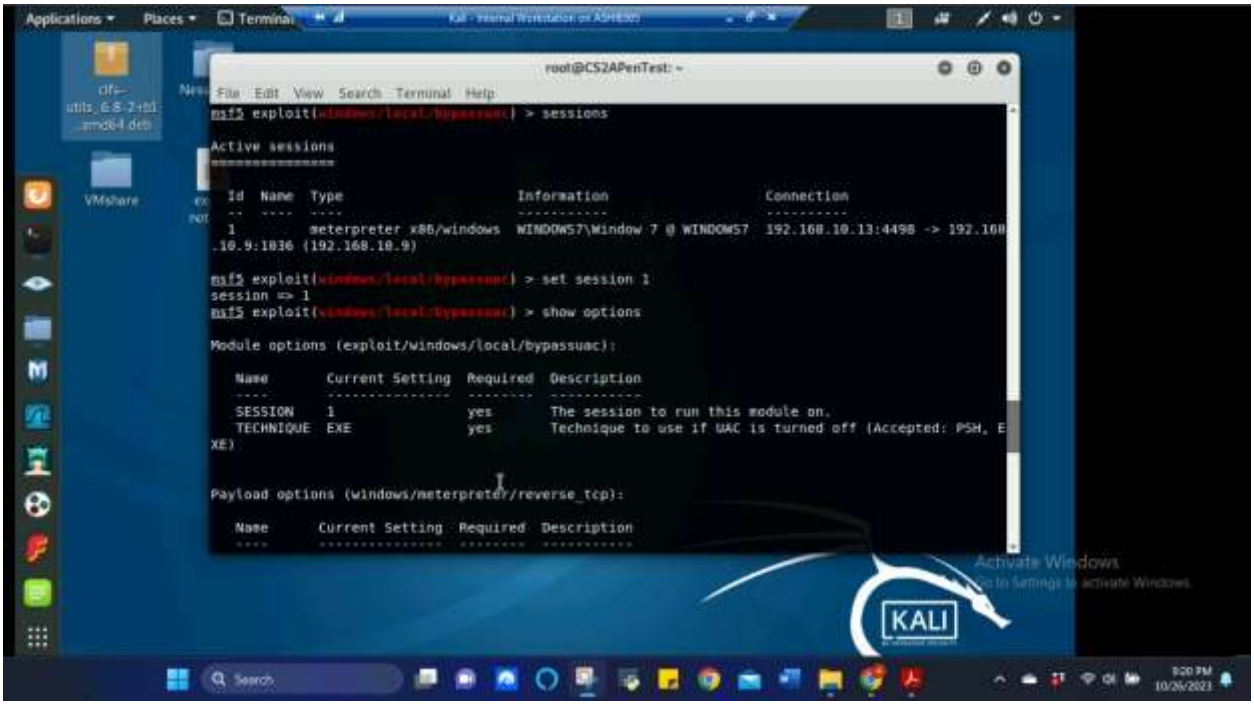

Figure 28 Screenshot of setting the current session to 1 for Task C.Privilege Escalation

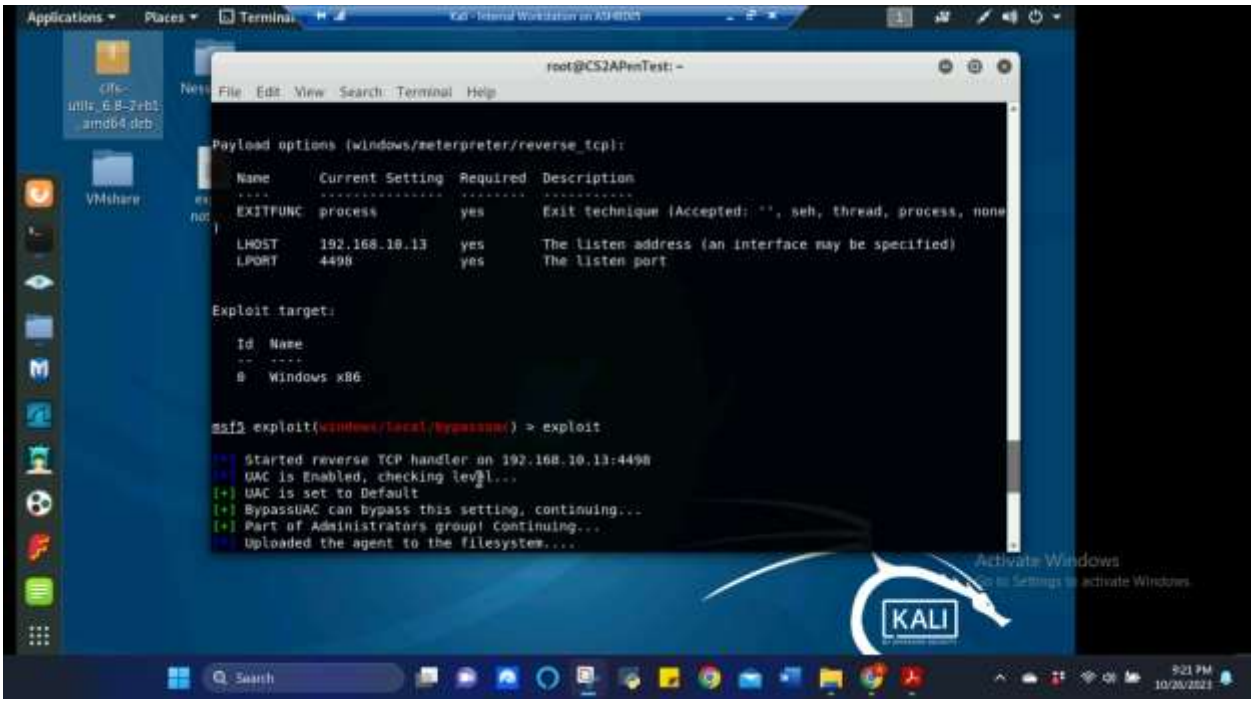

Figure 29 Screenshot executing the exploit for Task C.Privilege Escalation

The above screenshots show backgrounding the previous session, using windows/local/bypassuac exploit to escalate privilege to admin user in Windows 7 and setting required parameters and payload. Once all parameters are set, the exploit is initiated and successfully executed.

3. 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. **(5 pt)**

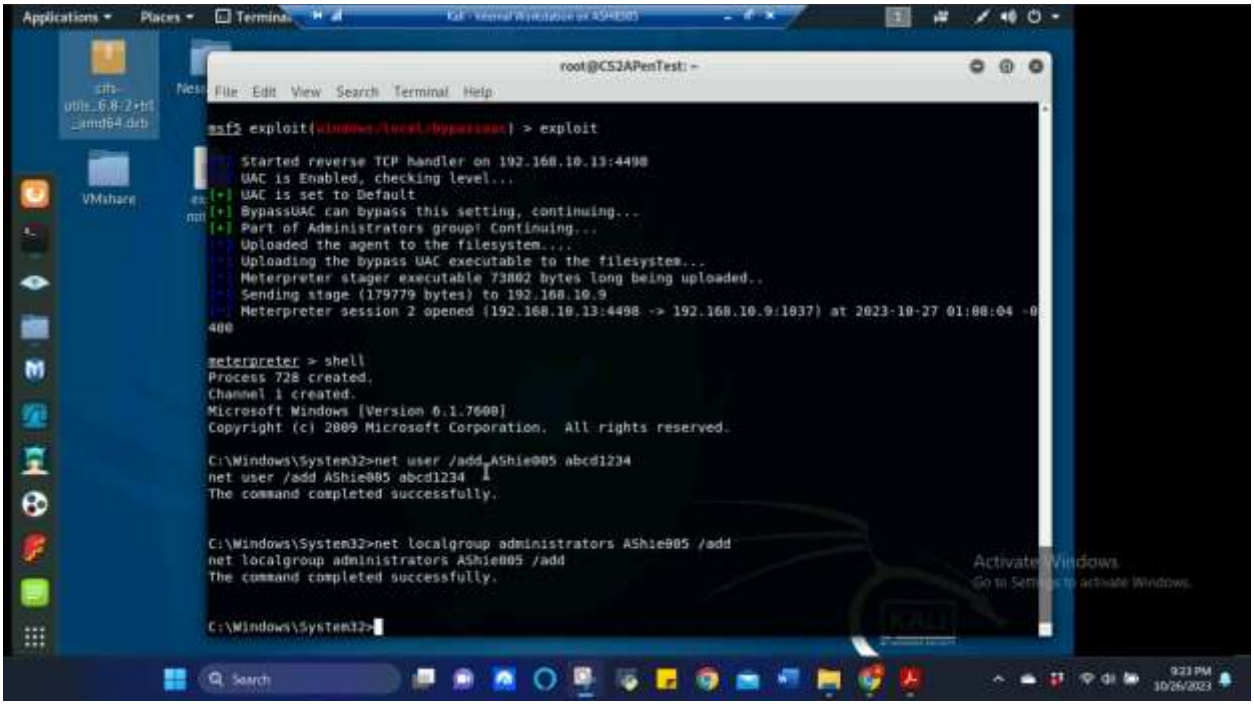

Figure 30 Screenshot of successful execution of exploit, creating a malicious account and adding the created account to the admin group for Task C.3

The above screenshot shows after using the shell command and gaining privilege escalation, the malicious user was created and added to the admin group.

4. Remote access to the malicious account created in the previous step and browse the files belonging to the user, "Windows 7", in RDP. **(5 pt)**

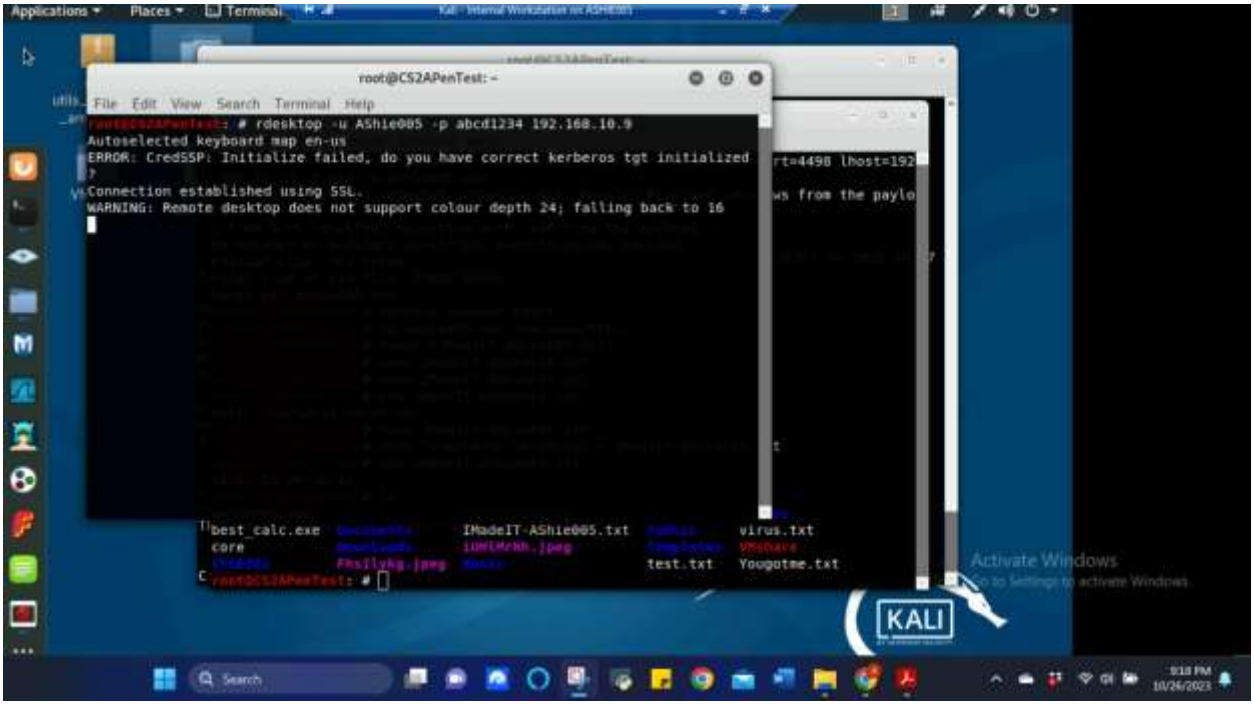

Figure 31 Screenshot of command used to gain remote desktop access from Internal Kali to Windows 7 using the malicious account that was created for Task C.4

Figure 32 Screenshot of remote desktop access from Internal Kali to Windows 7 using the malicious account that was created for Task C.4

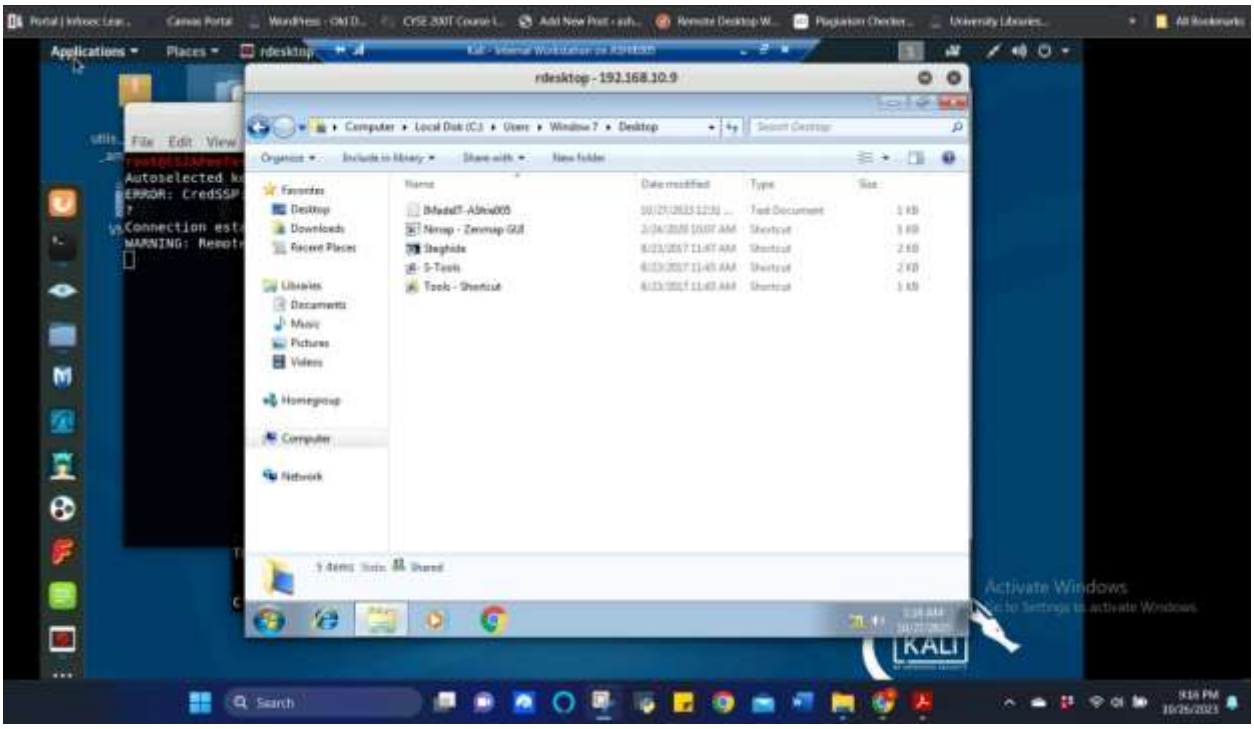

Figure 33 Screenshot of remote desktop access from Internal Kali to Windows 7 using the malicious account that was created and accessing the User's desktop and viewing files for Task C.4

The above screenshot shows gaining remote desktop access from internal kali to Windows 7 using the created malicious account and accessing the User's desktop files through the malicious account.

Task D. Extra Credit (10 points)

• Find another exploit that targets on either Windows XP or Windows Server 2008.

Did not attempt