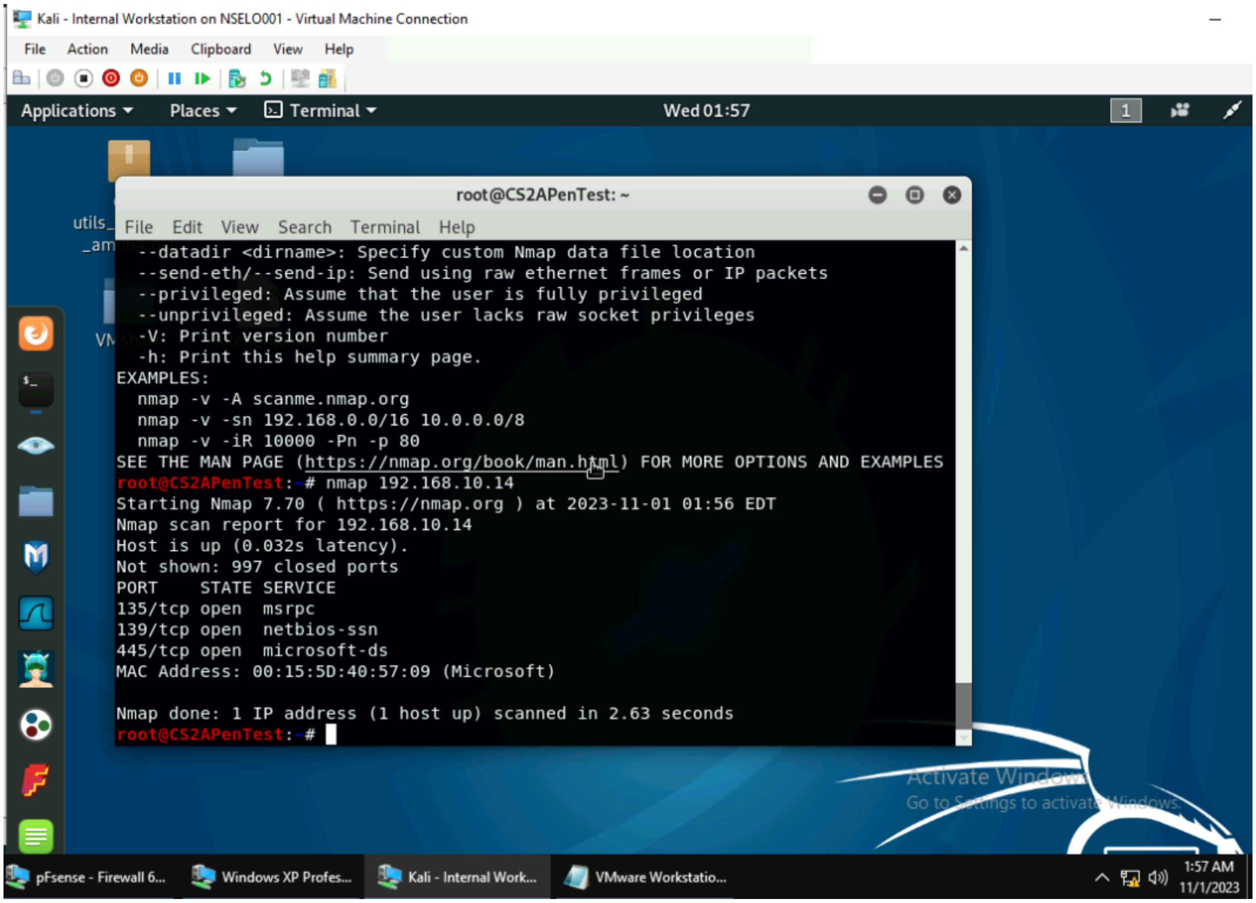
CYSE 301: Cybersecurity Technique and Operations
Assignment 4: Ethical Hacking

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.

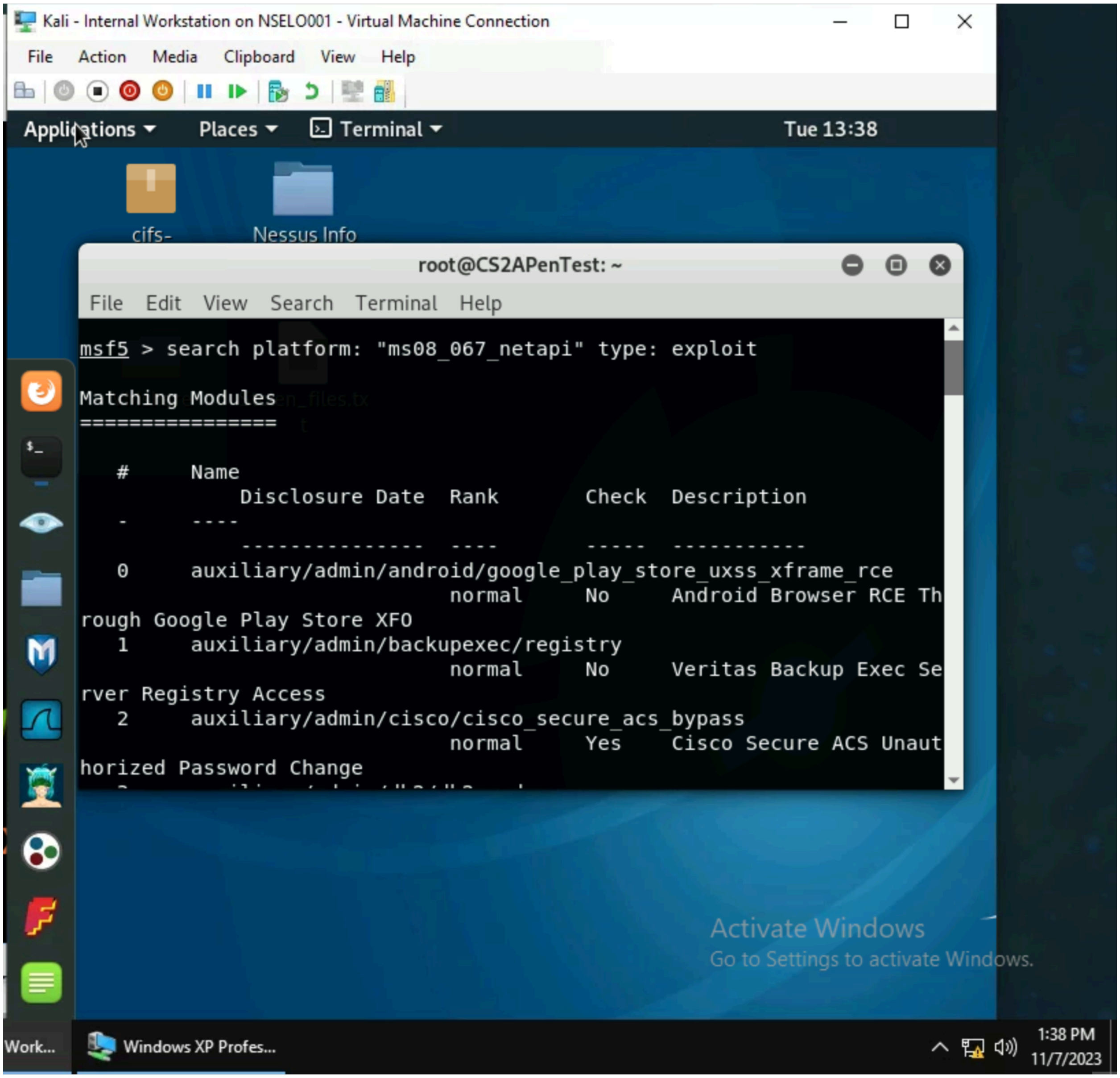
1. Run a port scan against the Windows XP using nmap command to identify open ports and services.
2. Identify the SMB port number (default: 445) and confirm that it is open.


Kali - Internal Workstation on NSELO001 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal
Wed 01:57
root@CS2APenTest: ~
File Edit View Search Terminal Help
pFsense - Firewall 6...
Windows XP Profes...
Kali - Internal Work...
VMware Workstatio...
1:57 AM
11/1/2023

```
  --datadir <dirname>: Specify custom Nmap data file location
  --send-eth/--send-ip: Send using raw ethernet frames or IP packets
  --privileged: Assume that the user is fully privileged
  --unprivileged: Assume the user lacks raw socket privileges
  -V: Print version number
  -h: Print this help summary page.
EXAMPLES:
  nmap -v -A scanme.nmap.org
  nmap -v -sn 192.168.0.0/16 10.0.0.0/8
  nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
root@CS2APenTest:~# nmap 192.168.10.14
Starting Nmap 7.70 ( https://nmap.org ) at 2023-11-01 01:56 EDT
Nmap scan report for 192.168.10.14
Host is up (0.032s 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 2.63 seconds
root@CS2APenTest:~#
```

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



Kali - Internal Workstation on NSELO001 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal
Tue 13:38
cifs-
Nessus Info
root@CS2APenTest: ~
File Edit View Search Terminal Help
Activate Windows
Go to Settings to activate Windows.
Work...
Windows XP Profes...
1:38 PM
11/7/2023

```
msf5 > search platform: "ms08_067_netapi" type: exploit

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

   #     Name
                                        Disclosure Date  Rank       Check  Description
   -     ----
                                        ---------------  ----       -----  -----------
   0     auxiliary/admin/android/google_play_store_uxss_xframe_rce
                                                         normal     No     Android Browser RCE Th
rough Google Play Store XFO
   1     auxiliary/admin/backupexec/registry
                                                         normal     No     Veritas Backup Exec Se
rver Registry Access
   2     auxiliary/admin/cisco/cisco_secure_acs_bypass
                                                         normal     Yes    Cisco Secure ACS Unaut
horized Password Change
```