PART 1

1.1 Use 'ip a' command to determine the block of IP addresses used by the virtual local network where you run Kali. Write your answer into the lab report. Your answer should be in the form of /<#mask-bits>, e.g., 192.168.221.0/24

192.168.1.0/24

1.2 Use n-map with appropriate options to discover which hosts are alive on this local network without scanning ports on these hosts.

a) What is your command line used?

sudo nmap -sn 192.168.1.0/24

b) Include the list of discovered active hosts into your lab report.

192.168.1.1
192.168.1.101
192.168.1.102
192.168.1.103

1.3 Find out the IP addresses of the gateway, the Kali VM, the Win7 VM and the Metasploitable2 VM as you did in Lab 1.

a) Write each machine and its IP address into your lab report.

Windows: 192.168.1.101
Kali: 192.168.1.102
Met: 192.168.1.103

b) Check whether these IP addresses appear in the active hosts list above. Simply answer yes or no in your lab report

Yes.

1.4 Start Wireshark to capture all traffic on the network. Then, run the command line for task 1.2 again. Observe the Wireshark capture. Based on the observation, explain in your report how nmap discovers active hosts in a local network.

It has 5 ways to discover hosts on a network.

Send ARP request (if within the same LAN) the most effective way

Send ICMP Echo Request

Send TCP SYN to port 443

Send TCP ACK to port 80

Send ICMP Timestamp Request

In this case it does this using ARP requests, if the ARP succeeded, it won't try the others. The ARP request sends ARP messages through the ARP protocol and the list of addresses according to the subnet group specified gets a message and it responds to see if they are alive.

PART 2

2.1 Use nmap to detect whether the top 200 TCP ports on the WinXP VM are open. Write your command line and the scan results into your lab report.

sudo nmap --top-ports 200 192.168.1.101 [could add -sS but nmap scans TCP ports by default]

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap --top-ports 200 192.168.1.101
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-21 15:14 AEDT
Nmap scan report for 192.168.1.101
Host is up (0.00028s latency).
Not shown: 186 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
23/tcp    open  telnet
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  icslap
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 00:50:56:94:17:C5 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.56 seconds
```

2.2 Start Wireshark to capture all traffic on the network. Then, use nmap with proper arguments to only detect whether the TCP port 80 on the Metasploitable2 VM is open (Hint: see how to specify ports in our slides).

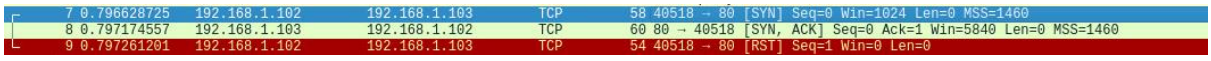
a) Write your command line into the lab report.

sudo nmap -p 80 192.168.1.103 [could add -sS but nmap scans TCP ports by default]

b) Observe the Wireshark capture. Based on the observation, explain in your report how nmap determines whether a port is open or not.

It establishes a connection using the TCP SYN protocol.

1. It sends a SYN
2. Other side responds with an ACK
3. After detecting port is open, nmap sends a RST, to reset connection- Prevents connections from being established, thus saving memory resources and being secretive.



PART 3

3.1 Use nmap with proper arguments to detect services possibly provided by the top 200 TCP ports on the WinXP VM.

a) Write your command line and the scan results into your lab report.

sudo nmap -sV --top-ports 200 192.168.1.101 [could add -sS but nmap scans TCP ports by default]

b) Compare the output with the one from Task 2.1. What are the differences?

There is extra information about the service and the versions of those services by providing a name for those services that are supported by TCP, It also provides extra information like

- Hostname

- Deduced OS:

- Common Platform Enumeration (CPE) representation:

this is other service information [host,CPE, OS], essentially you can learn about the OS and programs that are operating on the ports in greater detail that is running on the other end.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV --top-ports 200 192.168.1.101
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-16 19:21 AEDT
Stats: 0:00:19 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 42.86% done; ETC: 19:21 (0:00:21 remaining)
Stats: 0:00:24 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 42.86% done; ETC: 19:21 (0:00:28 remaining)
Stats: 0:00:34 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 50.00% done; ETC: 19:22 (0:00:31 remaining)
Stats: 0:01:39 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 92.86% done; ETC: 19:22 (0:00:07 remaining)
Stats: 0:02:02 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 92.86% done; ETC: 19:23 (0:00:00 remaining)
Nmap scan report for 192.168.1.101
Host is up (0.00039s latency).
Not shown: 186 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          Microsoft ftpd
23/tcp    open  telnet       Microsoft Windows XP telnetd
80/tcp    open  http         Microsoft IIS httpd 7.5
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
554/tcp   open  rtsp?
2869/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:50:56:94:17:C5 (VMware)
Service Info: Host: EH21-W7-1630117; OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft: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 129.10 seconds
```

3.2 Use nmap with proper arguments to detect services possibly provided by the top 50 TCP ports on Metasploitable2 VM and skip host discovery as you already know that it is running. Write your command line and the scan results into your lab report.

sudo nmap -sV -Pn --top-ports 50 192.168.1.103 [could add -sS but nmap scans TCP ports by default]

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -Pn --top-ports 50 192.168.1.103
[sudo] password for kali:
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-17 09:53 AEDT
Nmap scan report for 192.168.1.103
Host is up (0.00020s latency).
Not shown: 38 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
514/tcp  open  tcpwrapped
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5900/tcp open  vnc         VNC (protocol 3.3)
MAC Address: 00:50:56:94:3E:A9 (VMware)
Service Info: Host:  metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.62 seconds
```

3.3 Use nmap with proper arguments to detect service on UDP port 53 on the gateway. (Hint: see service detection part in our slides). Write your command line and the scan results into your lab report.

sudo nmap -sUV -p U:53 192.168.1.1

```
└─$ sudo nmap -sUV -p U:53 192.168.1.1
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-21 15:21 AEDT
Nmap scan report for pfSense.scem.uws.edu.au (192.168.1.1)
Host is up (0.00072s latency).

PORT   STATE SERVICE VERSION
53/udp open  domain  Unbound
MAC Address: 00:50:56:94:46:C5 (VMware)

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.84 seconds
```

Part 4

4.1 Use nmap with proper arguments to detect OS on the Metasploitable2 VM.

a) Write your command line into your lab report.

sudo nmap -O 192.168.1.103

b) What OS does nmap thinks the Metasploitable2 VM is running?

Running: Linux 2.6.X

c) If it is Linux, what is the kernel version number believed by nmap?

OS CPE: cpe:/o:linux:linux_kernel:2.6

4.2 Use nmap with proper arguments to detect OS on the WinXP VM.

a) Write your command line into your lab report.

sudo nmap -O 192.168.1.101

b) What OS does nmap thinks the WinXP VM is running?

Running: Microsoft Windows 7|2008|8.1

c) If it is WinXP, can nmap be sure that it is XP SP3?

Yes it is in the OS details. OS details: Microsoft Windows 7 SP0 - SP1. The windows 7 that we are using is actually running service pack 1.

4.3 Use nmap with proper arguments to detect OS on the gateway (which is your virtual NAT box).

a) Write your command line into your lab report.

sudo nmap -O 192.168.1.1

b) What OS does nmap thinks the gateway device is running?

It appears as if it is uncertain or that it is guessing. It specified that it guesses "Comau embedded)"; "No exact OS matches for host (test conditions non-ideal)."

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.1.1
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-21 15:30 AEDT
Nmap scan report for pfSense.scem.uws.edu.au (192.168.1.1)
Host is up (0.00066s latency).
Not shown: 997 filtered ports
PORT    STATE SERVICE
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https
MAC Address: 00:50:56:94:46:C5 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: specialized
Running (JUST GUESSING): Comau embedded (92%)
Aggressive OS guesses: Comau C4G robot control unit (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
```

PART 5

5.1 Make sure you are currently in the directory of "/home/kali".

a) Create a new directory under it called "outputs" using command "mkdir". If you are unsure how to use "mkdir", do "man mkdir".

```
┌──(kali㉿kali)-[~]
└─$ mkdir outputs

┌──(kali㉿kali)-[~]
└─$ ls
Desktop  Documents  Downloads  Music  outputs  Pictures  Public  Templates  Videos  whois.txt
```

b) Execute "cd outputs".

```
┌──(kali㉿kali)-[~]
└─$ cd outputs
```

c) Execute "pwd". What's the result of this command?

/home/kali/outputs

5.2 Use nmap with proper arguments to detect whether the TCP ports in the range of 8001-8010 on Metasploitable2 VM are open, and output in all three formats of Normal, XML, and Grepable. The output file names without the suffix part should use "ports8001-8010". Write your command line into your lab report.

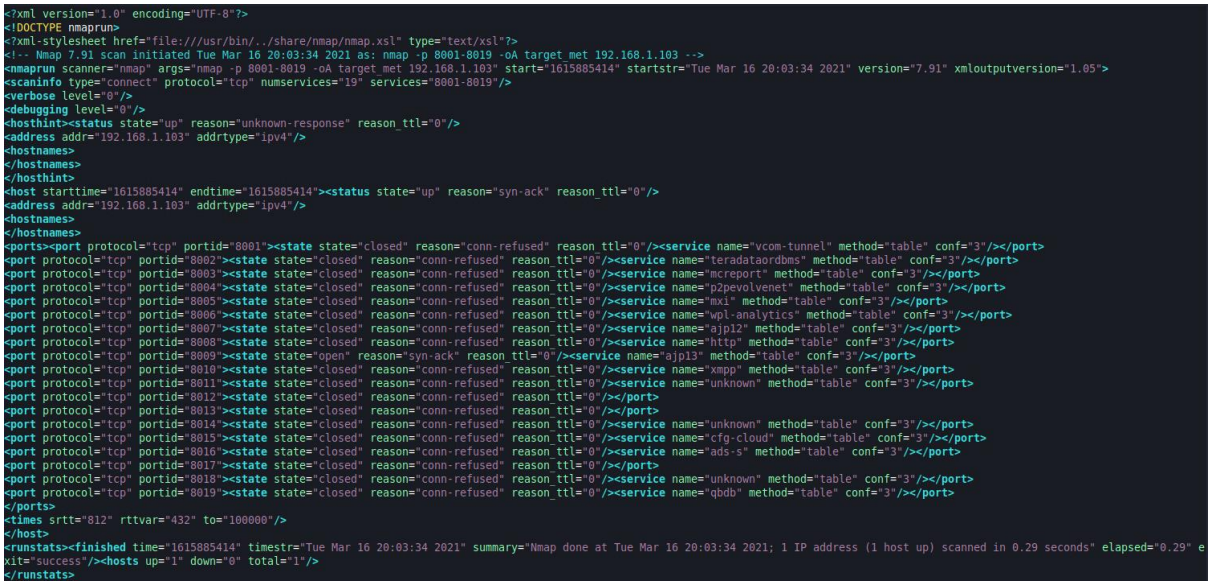
sudo nmap -p 8001-8019 -oA ports8001-8010 192.168.1.103 [could add -sS but nmap scans TCP ports by default]

5.3 What are the full file names of the three output files from Task 5.2?

1. ports8001-8010.gnmap [Greppable]
2. ports8001-8010.nmap [normal]
3. ports8001-8010.xml [XML output]

5.4 Examine the contents of the XML output file, which is convenient for exporting nmap output to other programs. An XML file typically includes a hierarchy of tags. For example, you'll notice that the <scaninfo> tag is nested inside the <nmaprun> tag in XML output file. Similarly, which tag is the <port> tag nested in?

It's nested in the "<ports>" tag



PART 6

6.1 Decompress this file using the 'unzip' command. Write your command line into the lab report. (If you are unsure how to use 'unzip', do a 'man unzip'.)

unzip /home/kali/Downloads/treasure.zip

6.2 After decompressing, you should see a directory called "treasure". Under this directory, you see many further directories and files. Only one of these files contains a line with the following string "Secret:OpenSeseme". Use 'grep' to find out which file it is. (Suppose you

are now under the directory “/home/kali/Downloads/treasure”). Write your command line and result into the lab report.

grep -r "Secret:OpenSeseme"