

Lab 6 – Nmap

TERM	NAME – Student ID	COURSE CODE	WEIGHT
Winter 2022	Ishan Aakash Patel - 146151238	CYT130	5%

Lab Objectives

Upon completion of this lab, you will be able to perform the following:

- Become familiar with nmap switches;
- Use necessary switches to perform OS fingerprinting;
- Discover target host vulnerabilities.
- Extra miles will test your skills – but not mandatory
 - Point booster

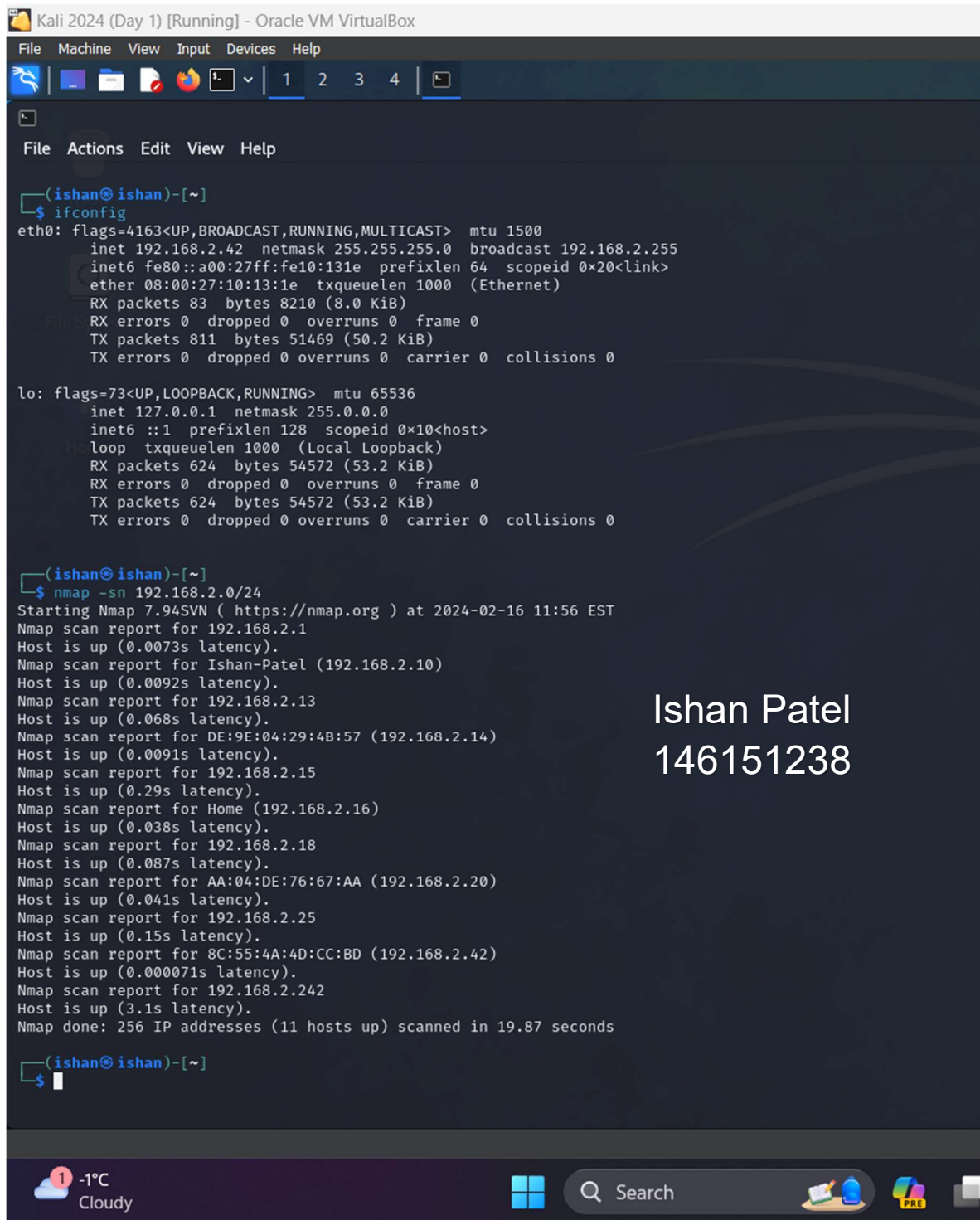
Part 1: No screenshots are required from Part 1.

I have used my home network for scanning using nmap. So the IP range will be 192.168.2.0/24. I don't have a ethernet which uses Realtek Controller.

Part 2: Scanning

Use the IP range 172.16.11.0/26 as your target range.

1. What is NMAP switch to detect active IP addresses?
Include a screenshot for detecting active hosts within the target range.



The screenshot shows a Kali Linux terminal window titled "Kali 2024 (Day 1) [Running] - Oracle VM VirtualBox". The terminal displays the output of the `ifconfig` command, showing details for the `eth0` and `lo` interfaces. Following this, the `nmap -sn 192.168.2.0/24` command is executed, resulting in a scan report that identifies 11 active hosts within the specified range. The hosts listed include 192.168.2.1, 192.168.2.10, 192.168.2.13, 192.168.2.14, 192.168.2.15, 192.168.2.16, 192.168.2.18, 192.168.2.20, 192.168.2.25, 192.168.2.42, and 192.168.2.242. The scan is completed in 19.87 seconds.

```
(ishan@ishan)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.2.42 netmask 255.255.255.0 broadcast 192.168.2.255
    inet6 fe80::a00:27ff:fe10:131e prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:10:13:1e txqueuelen 1000 (Ethernet)
    RX packets 83 bytes 8210 (8.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 811 bytes 51469 (50.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 624 bytes 54572 (53.2 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 624 bytes 54572 (53.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(ishan@ishan)-[~]
$ nmap -sn 192.168.2.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-16 11:56 EST
Nmap scan report for 192.168.2.1
Host is up (0.0073s latency).
Nmap scan report for Ishan-Patel (192.168.2.10)
Host is up (0.0092s latency).
Nmap scan report for 192.168.2.13
Host is up (0.068s latency).
Nmap scan report for DE:9E:04:29:4B:57 (192.168.2.14)
Host is up (0.0091s latency).
Nmap scan report for 192.168.2.15
Host is up (0.29s latency).
Nmap scan report for Home (192.168.2.16)
Host is up (0.038s latency).
Nmap scan report for 192.168.2.18
Host is up (0.087s latency).
Nmap scan report for AA:04:DE:76:67:AA (192.168.2.20)
Host is up (0.041s latency).
Nmap scan report for 192.168.2.25
Host is up (0.15s latency).
Nmap scan report for 8C:55:4A:4D:CC:BD (192.168.2.42)
Host is up (0.000071s latency).
Nmap scan report for 192.168.2.242
Host is up (3.1s latency).
Nmap done: 256 IP addresses (11 hosts up) scanned in 19.87 seconds

(ishan@ishan)-[~]
$
```

Ishan Patel
146151238

- 2. What is NMAP switch to detect running service version on open port? Include one screenshot for each target found in the range with the results of service versions.**

[illegible]

Host is up (0.013s latency).

All 1000 scanned ports on 192.168.2.13 are in ignored states.

Not shown: 1000 closed tcp ports (conn-refused)

Nmap scan report for DE:9E:04:29:4B:57 (192.168.2.14)

Host is up (0.017s latency).

Not shown: 999 closed tcp ports (conn-refused)

PORT	STATE	SERVICE	VERSION
62078/tcp	open	tcpwrapped	

Nmap scan report for 192.168.2.15

Host is up (0.015s latency).

All 1000 scanned ports on 192.168.2.15 are in ignored states.

Not shown: 1000 closed tcp ports (conn-refused)

Nmap scan report for Home (192.168.2.16)

Host is up (0.061s latency).

All 1000 scanned ports on Home (192.168.2.16) are in ignored states.

Not shown: 1000 closed tcp ports (conn-refused)

Nmap scan report for 192.168.2.18

Host is up (0.014s latency).

Not shown: 998 closed tcp ports (conn-refused)

PORT	STATE	SERVICE	VERSION
49152/tcp	open	tcpwrapped	
62078/tcp	open	tcpwrapped	

Nmap scan report for EA:66:3E:2E:5F:C3 (192.168.2.23)

Host is up (0.015s latency).

Not shown: 998 closed tcp ports (conn-refused)

PORT	STATE	SERVICE	VERSION
49152/tcp	open	tcpwrapped	
62078/tcp	open	iphone-sync?	

Nmap scan report for 192.168.2.25

Host is up (0.016s latency).

All 1000 scanned ports on 192.168.2.25 are in ignored states.

Not shown: 1000 closed tcp ports (conn-refused)

Nmap scan report for 8C:55:4A:4D:CC:BD (192.168.2.42)

Host is up (0.00070s latency).

All 1000 scanned ports on 8C:55:4A:4D:CC:BD (192.168.2.42) are in ignored states.

Not shown: 1000 closed tcp ports (conn-refused)

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 256 IP addresses (10 hosts up) scanned in 103.91 seconds

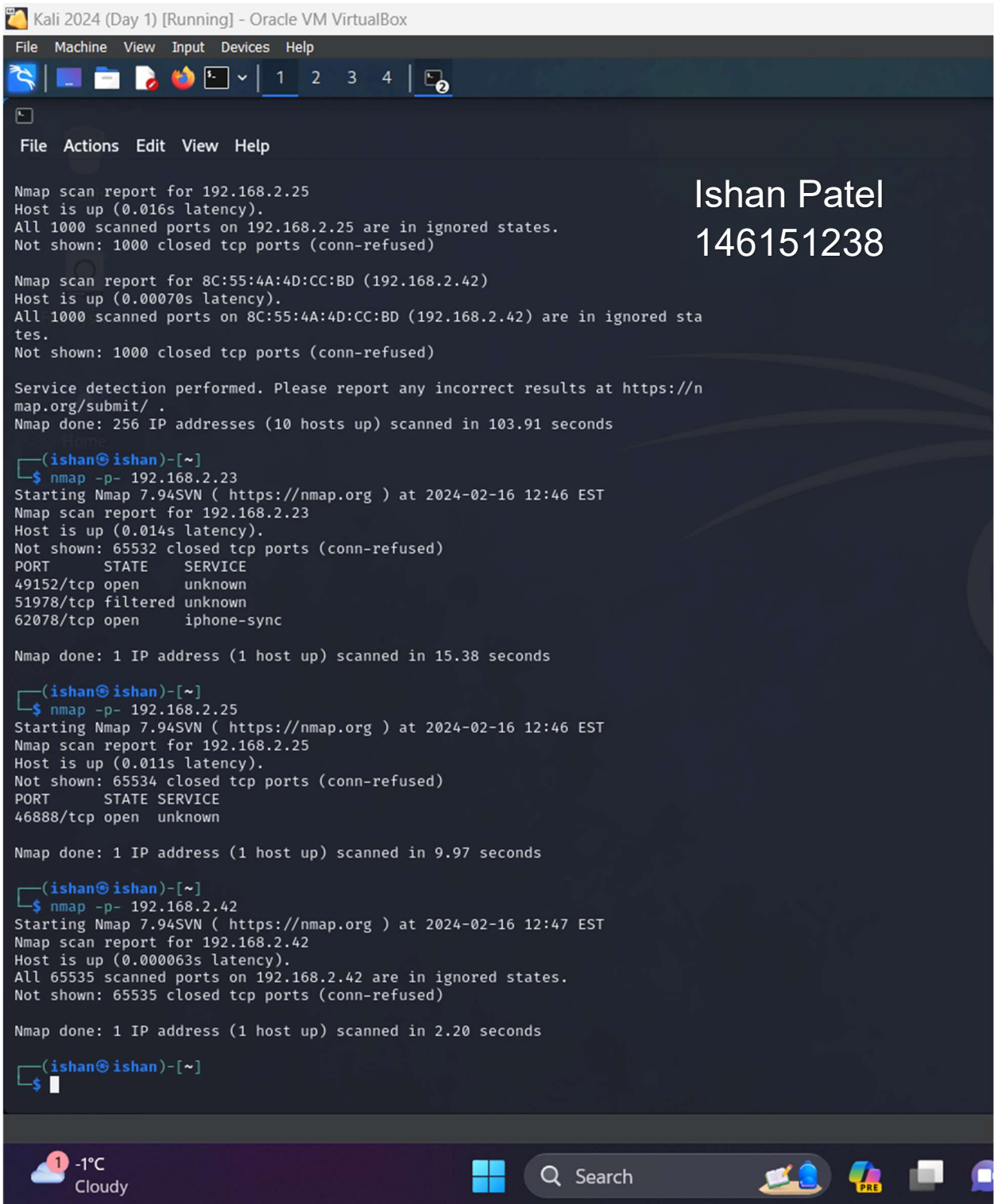
(ishan@ishan)-[~]

\$

Ishan Patel
146151238

3. What is NMAP switch to scan ALL ports?

Include a screenshot for running this command on one of the targets found in the range.



```
Kali 2024 (Day 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4 2

File Actions Edit View Help

Nmap scan report for 192.168.2.25
Host is up (0.016s latency).
All 1000 scanned ports on 192.168.2.25 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap scan report for 8C:55:4A:4D:CC:BD (192.168.2.42)
Host is up (0.00070s latency).
All 1000 scanned ports on 8C:55:4A:4D:CC:BD (192.168.2.42) are in ignored sta
tes.
Not shown: 1000 closed tcp ports (conn-refused)

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 256 IP addresses (10 hosts up) scanned in 103.91 seconds

(ishan@ishan)-[~]
$ nmap -p- 192.168.2.23
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-16 12:46 EST
Nmap scan report for 192.168.2.23
Host is up (0.014s latency).
Not shown: 65532 closed tcp ports (conn-refused)
PORT      STATE      SERVICE
49152/tcp  open      unknown
51978/tcp  filtered  unknown
62078/tcp  open      iphone-sync

Nmap done: 1 IP address (1 host up) scanned in 15.38 seconds

(ishan@ishan)-[~]
$ nmap -p- 192.168.2.25
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-16 12:46 EST
Nmap scan report for 192.168.2.25
Host is up (0.011s latency).
Not shown: 65534 closed tcp ports (conn-refused)
PORT      STATE      SERVICE
46888/tcp  open      unknown

Nmap done: 1 IP address (1 host up) scanned in 9.97 seconds

(ishan@ishan)-[~]
$ nmap -p- 192.168.2.42
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-16 12:47 EST
Nmap scan report for 192.168.2.42
Host is up (0.000063s latency).
All 65535 scanned ports on 192.168.2.42 are in ignored states.
Not shown: 65535 closed tcp ports (conn-refused)

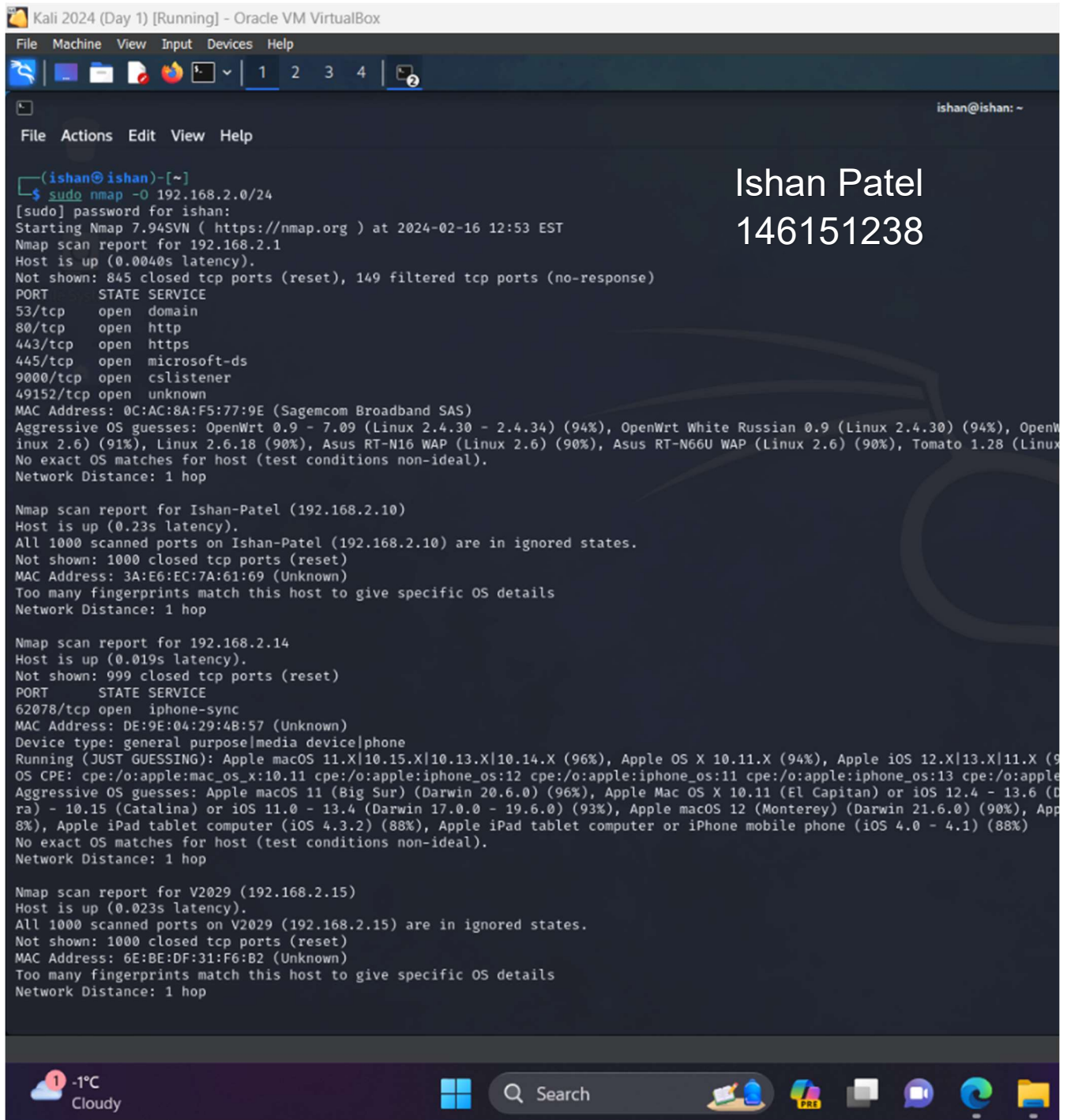
Nmap done: 1 IP address (1 host up) scanned in 2.20 seconds

(ishan@ishan)-[~]
$
```

Ishan Patel
146151238

-1°C Cloudy Search PRE

4. What is the NMAP switch to detect the operating system?
Include one screenshots showing the operating system detected for each target found within the range.



```
Kali 2024 (Day 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4

(ishan@ishan)-[~]
$ sudo nmap -O 192.168.2.0/24
[sudo] password for ishan:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-16 12:53 EST
Nmap scan report for 192.168.2.1
Host is up (0.0040s latency).
Not shown: 845 closed tcp ports (reset), 149 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https
445/tcp   open  microsoft-ds
9000/tcp  open  cslistener
49152/tcp open  unknown
MAC Address: 0C:AC:8A:F5:77:9E (Sagemcom Broadband SAS)
Aggressive OS guesses: OpenWrt 0.9 - 7.09 (Linux 2.4.30 - 2.4.34) (94%), OpenWrt White Russian 0.9 (Linux 2.4.30) (94%), OpenWrt 2.6 (91%), Linux 2.6.18 (90%), Asus RT-N16 WAP (Linux 2.6) (90%), Tomato 1.28 (Linux 2.6) (90%), Linux 2.6.18 (90%), Asus RT-N16 WAP (Linux 2.6) (90%), Tomato 1.28 (Linux 2.6) (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

Nmap scan report for Ishan-Patel (192.168.2.10)
Host is up (0.23s latency).
All 1000 scanned ports on Ishan-Patel (192.168.2.10) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 3A:E6:EC:7A:61:69 (Unknown)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for 192.168.2.14
Host is up (0.019s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
62078/tcp open  iphone-sync
MAC Address: DE:9E:04:29:4B:57 (Unknown)
Device type: general purpose|media device|phone
Running (JUST GUESSING): Apple macOS 11.X|10.15.X|10.13.X|10.14.X (96%), Apple OS X 10.11.X (94%), Apple iOS 12.X|13.X|11.X (94%)
OS CPE: cpe:/o:apple:mac_os_x:10.11 cpe:/o:apple:iphone_os:12 cpe:/o:apple:iphone_os:11 cpe:/o:apple:iphone_os:13 cpe:/o:apple:iphone_os:14
Aggressive OS guesses: Apple macOS 11 (Big Sur) (Darwin 20.6.0) (96%), Apple Mac OS X 10.11 (El Capitan) or iOS 12.4 - 13.6 (Darwin 19.0.0 - 21.0.0) (94%), Apple macOS 11 (Big Sur) (Darwin 20.6.0) (96%), Apple Mac OS X 10.11 (El Capitan) or iOS 12.4 - 13.6 (Darwin 19.0.0 - 21.0.0) (94%), Apple macOS 12 (Monterey) (Darwin 21.6.0) (90%), Apple iPad tablet computer (iOS 4.3.2) (88%), Apple iPad tablet computer or iPhone mobile phone (iOS 4.0 - 4.1) (88%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

Nmap scan report for V2029 (192.168.2.15)
Host is up (0.023s latency).
All 1000 scanned ports on V2029 (192.168.2.15) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 6E:BE:DF:31:F6:B2 (Unknown)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

Ishan Patel
146151238

-1°C Cloudy Search



MAC Address: 6E:BE:DF:31:F6:B2 (Unknown)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for 192.168.2.16
Host is up (0.028s latency).
All 1000 scanned ports on 192.168.2.16 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 44:61:32:7C:07:5A (ecobee)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for 46:40:33:74:FA:7C (192.168.2.18)
Host is up (0.014s latency).
Not shown: 998 closed tcp ports (reset)
PORT STATE SERVICE
49152/tcp open unknown
62078/tcp open iphone-sync
MAC Address: 46:40:33:74:FA:7C (Unknown)
Device type: general purpose
Running: Apple macOS 11.X
OS details: Apple macOS 11 (Big Sur) (Darwin 20.6.0)
Network Distance: 1 hop

Nmap scan report for 192.168.2.25
Host is up (0.0074s latency).
All 1000 scanned ports on 192.168.2.25 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 4A:23:93:03:D2:E0 (Unknown)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for 192.168.2.43
Host is up (0.0014s latency).
All 1000 scanned ports on 192.168.2.43 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 3A:7B:10:44:E5:7C (Unknown)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for 192.168.2.42
Host is up (0.000058s latency).
All 1000 scanned ports on 192.168.2.42 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at <https://nmap.org/submit/>.
Nmap done: 256 IP addresses (9 hosts up) scanned in 99.79 seconds

(ishan@ishan)-[~]

\$

Ishan Patel
146151238

5. Vulnerability Scanning: Use “nikto” web vulnerability scanner to scan one target host running web services. Include screenshots showing the command used and the results of the scan.

```
Kali 2024 (Day 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4

ishan@ishan: ~
File Actions Edit View Help
0 upgraded, 0 newly installed, 0 to remove and 18 not upgraded.

(ishan@ishan)-[~]
$ nmap -p 80,443 192.168.2.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-16 13:20 EST
Nmap scan report for 192.168.2.1
Host is up (0.0069s latency).

PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap scan report for Ishan-Patel (192.168.2.10)
Host is up (0.092s latency).

PORT      STATE SERVICE
80/tcp    closed http
443/tcp   closed https

Nmap scan report for 192.168.2.14
Host is up (0.070s latency).

PORT      STATE SERVICE
80/tcp    closed http
443/tcp   closed https

Nmap scan report for V2029 (192.168.2.15)
Host is up (0.025s latency).

PORT      STATE SERVICE
80/tcp    closed http
443/tcp   closed https

Nmap scan report for 192.168.2.16
Host is up (0.061s latency).

PORT      STATE SERVICE
80/tcp    closed http
443/tcp   closed https

Nmap scan report for 46:40:33:74:FA:7C (192.168.2.18)
Host is up (0.031s latency).

PORT      STATE SERVICE
80/tcp    closed http
443/tcp   closed https

Nmap scan report for 192.168.2.23
Host is up (0.062s latency).

PORT      STATE SERVICE
80/tcp    closed http

Name : Ishan Aakash Patel
Student ID : 146151238

Ln 2, Col 23 48 characters 100% Window UTF-8
```


Kali 2024 (Day 1) [Running] - Oracle VM VirtualBox

FileMachineViewInputDevicesHelp

1234

ishan@ishan: ~

FileActionsEditViewHelp

Nmap scan report for 46:40:33:74:FA:7C (192.168.2.18)
Host is up (0.031s latency).

PORT STATE SERVICE
80/tcp closed http
443/tcp closed https

Nmap scan report for 192.168.2.23
Host is up (0.062s latency).

PORT STATE SERVICE
80/tcp closed http
443/tcp closed https

Nmap scan report for realme-X7-Pro-5G (192.168.2.25)
Host is up (0.0065s latency).

PORT STATE SERVICE
80/tcp closed http
443/tcp closed https

Nmap scan report for 192.168.2.42
Host is up (0.0049s latency).

PORT STATE SERVICE
80/tcp closed http
443/tcp closed https

Nmap done: 256 IP addresses (9 hosts up) scanned in 18.96 seconds

(ishan@ishan)-[~]
\$ nikto -h 192.168.2.1
- Nikto v2.5.0

+ Target IP: 192.168.2.1
+ Target Hostname: 192.168.2.1
+ Target Port: 80
+ Start Time: 2024-02-16 13:21:29 (GMT-5)

+ Server: HTTP Server
+ /XzKzBMyV.org: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the
ilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8102 requests: 0 error(s) and 2 item(s) reported on remote host
+ End Time: 2024-02-16 13:22:54 (GMT-5) (85 seconds)

+ 1 host(s) tested

(ishan@ishan)-[~]
\$

FileEditView

Name : Ishan Aakash Patel
Student ID : 146151238

Ln 2, Col 23 48 characters 100% Window UTF-8

-1°C
Cloudy

Search

Extra Mile – not mandatory

Scan the provided IP address with nmap and provide screenshot:

- a. All TCP ports and treat host as “online”
- b. Top 100 UDP ports
- c. List Open TCP ports (if any)
- d. List open UDP ports (if any)

Part 2: Submit your lab



- Doublecheck all your answers.
- Save the file on your computer for future reference.
- Save the file again as a “.pdf” file.
- Submit the PDF file for grading.