TAYLOR'S UNIVERSITY

Wisdom · Integrity · Excellence

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING

DEGREE PROGRAMMES

ASSIGNMENT (20%)

AUGUST 2022 SEMESTER

Module Name	:	**Operating System and Computer Networking**
Module Code	:	**ITS66304**
Submission Deadline	:	**18 November 2022 (23.55pm)** [Malaysia Time Zone]
Submission Platform	:	**TiMES (PDF)**
Assignment Weightage	:	**20%**
Presentation	:	**Week 13**

OSBuddies

Student declaration:

I declare that:

1. *I understand what is meant by plagiarism*
2. *The implication of plagiarism have been explained to us by our lecturer*
3. *This project is all our work and I have acknowledged any use of the published or unpublished works of other people.*

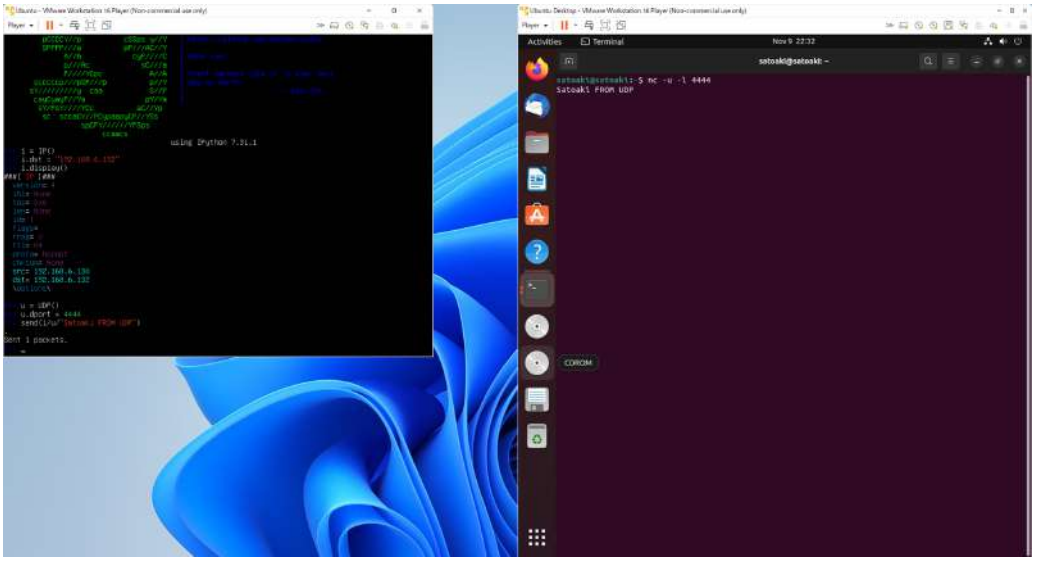
Name	Student ID	Completed Section				
		A	**B**	**C**	**D**	**E**
Ishihara Satoaki	0354208	✓	✓	✓	✓	✓
Mohamed Fahad Farhan	0354487	✓	✓	✓	✓	✓
Mohammad Sameed Khan	0353846	✓	✓	✓	✓	✓

Muhammad Nafay	0353574	✓	✓	✓	✓	✓
Thua Sin Wei	0354566	✓	✓	✓	✓	✓
Teh Ming Heng	0346663	✓	✓	✓	✓	✓
Tang Wai Kin	0346747	✓	✓	✓	✓	✓
Christiaan Tim Vrieling	0356455	✓	✓	✓	✓	✓

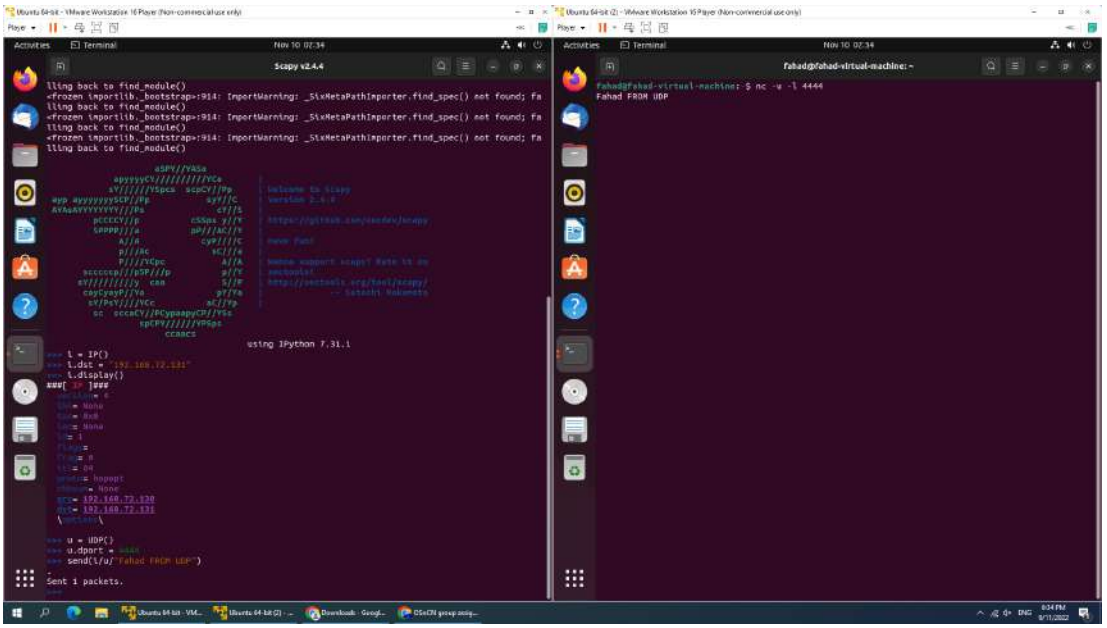
Section A

1.1 Ishihara Satoaki

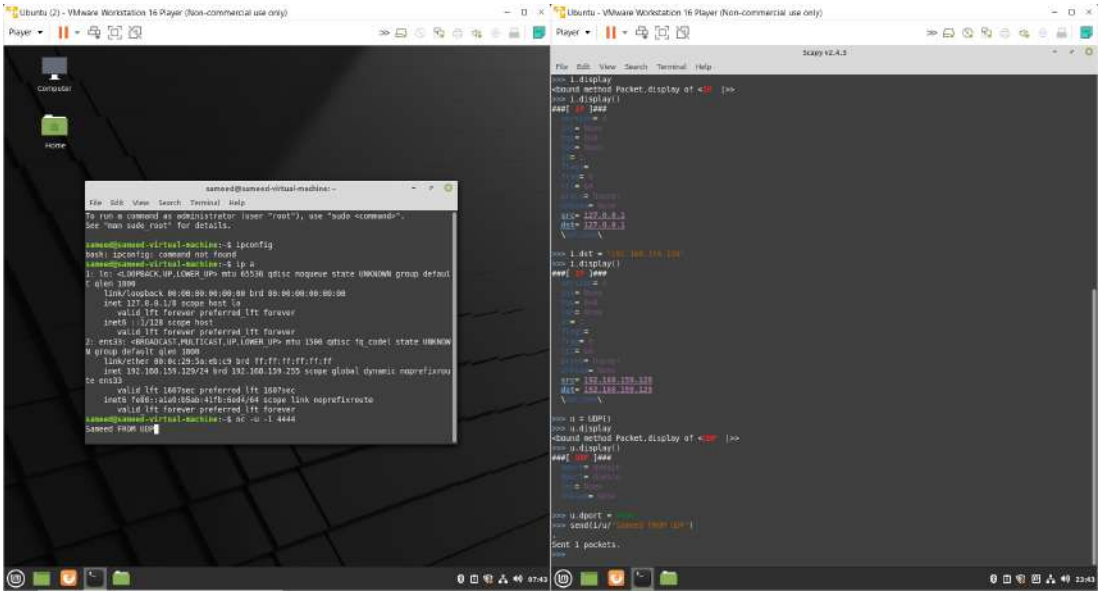
```
[Receiver]
$ nc -u -l 4444

[Sender]
$sudo scapy
|=============================================================|
|i=IP()                                                       |
|i.display                                                    |
|i.display()                                                  |
|i.dst = <destination IP address(mine was 192.168.186.128)>|
|u=UDP()                                                      |
|u.display                                                    |
|u.display()                                                  |
|u.dport = 4444                                               |
|send(i/u/”Satoaki FROM UDP”)                                 |
|=============================================================|
```



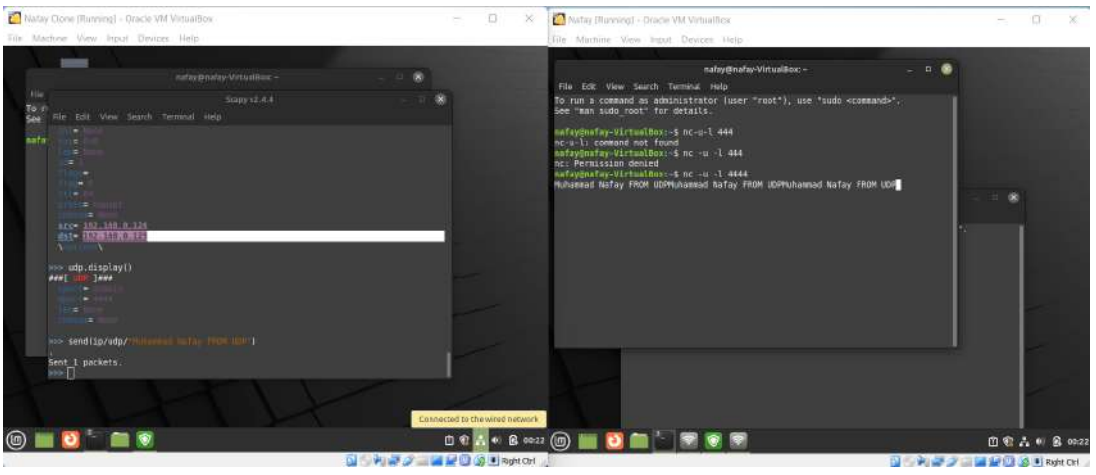
1.2 Mohamed Fahad Farhan



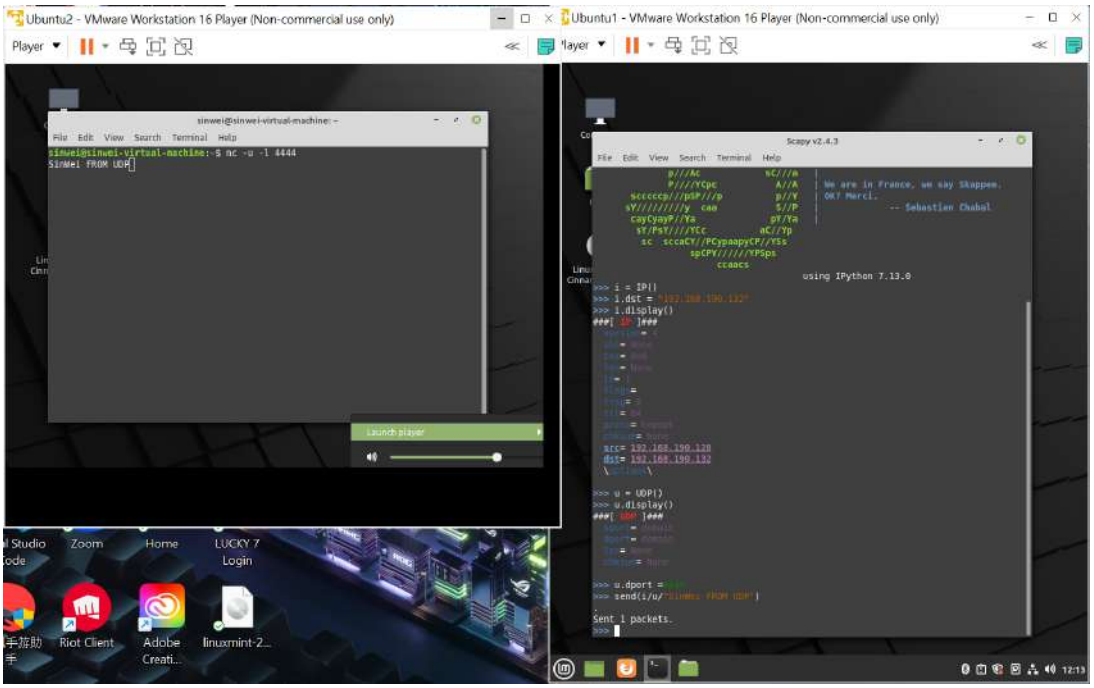
1.3 Mohammad Sameed Khan



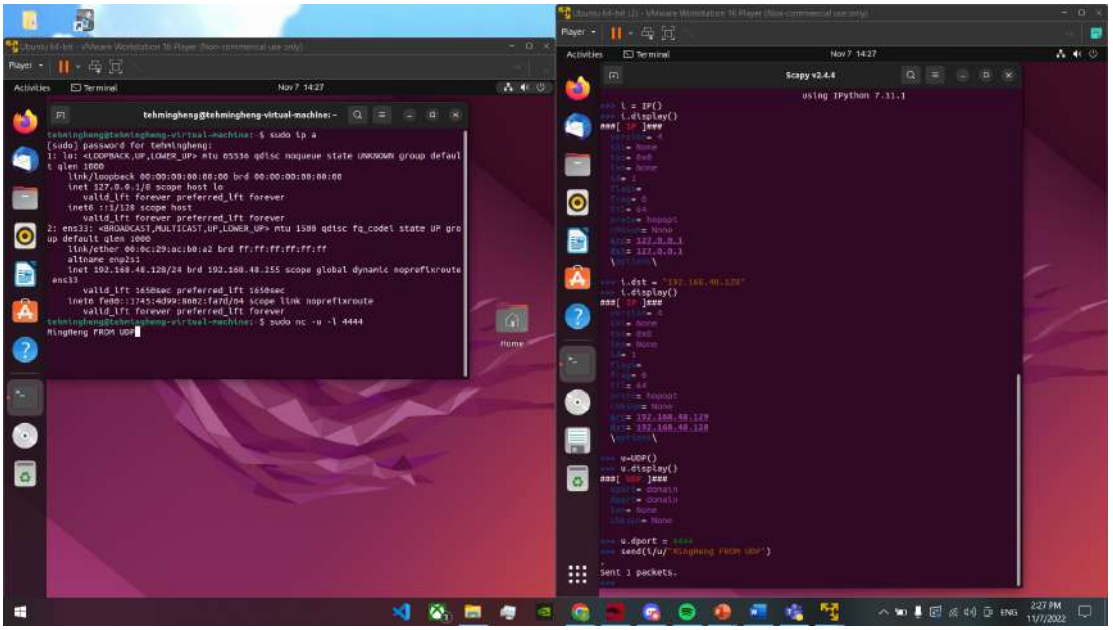
1.4 Muhammad Nafay



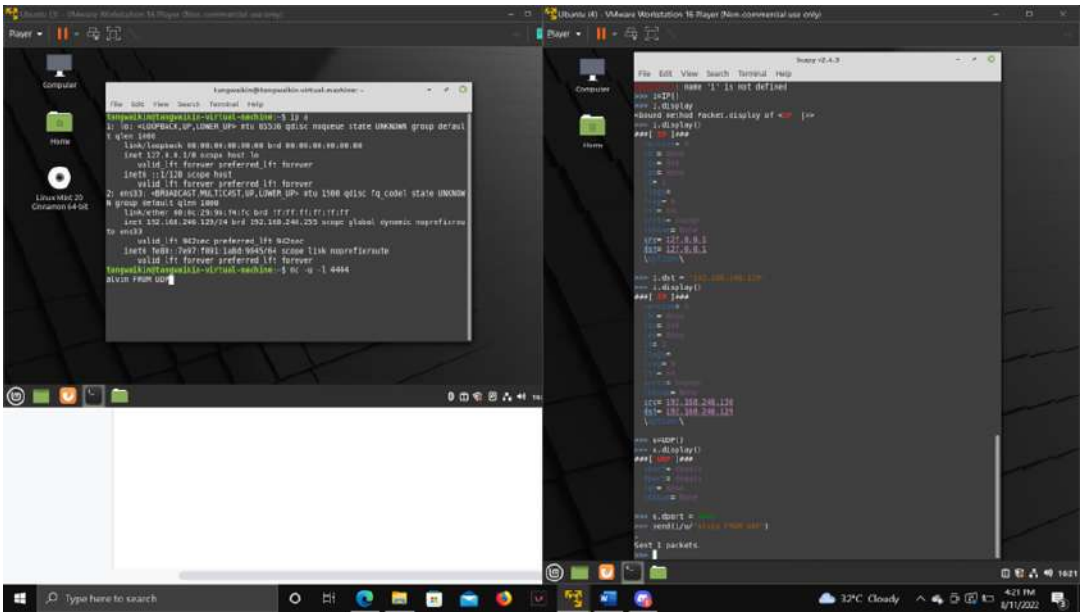
1.5 Thua Sin Wei



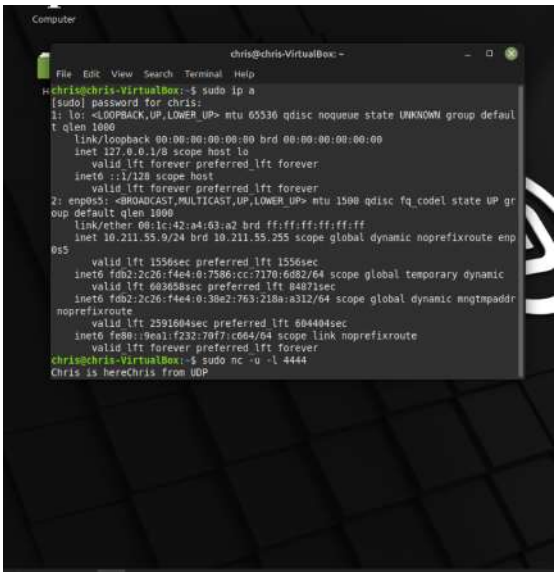
1.6 Teh Ming Heng



1.7 Tang Wai Kin



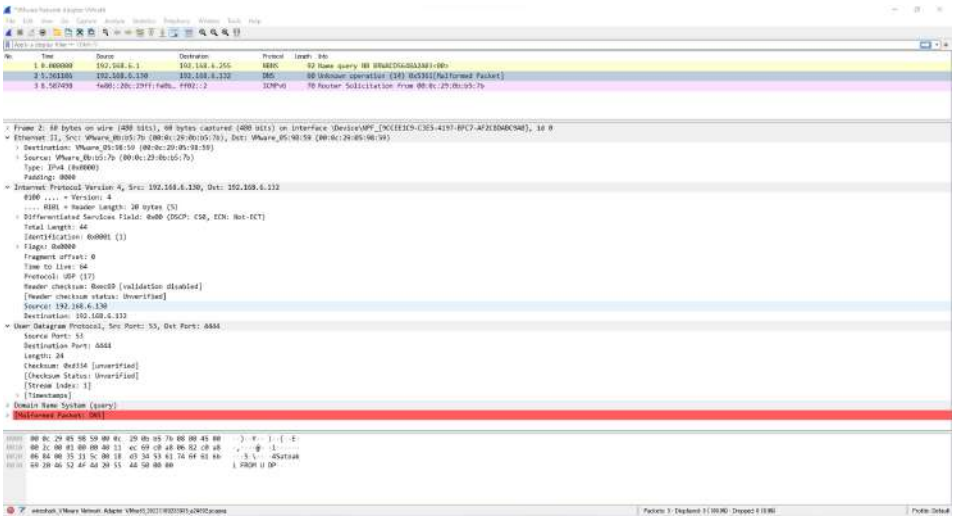
1.8 Christiaan Tim Vrieling



Section B

1.1 Ishihara Satoaki

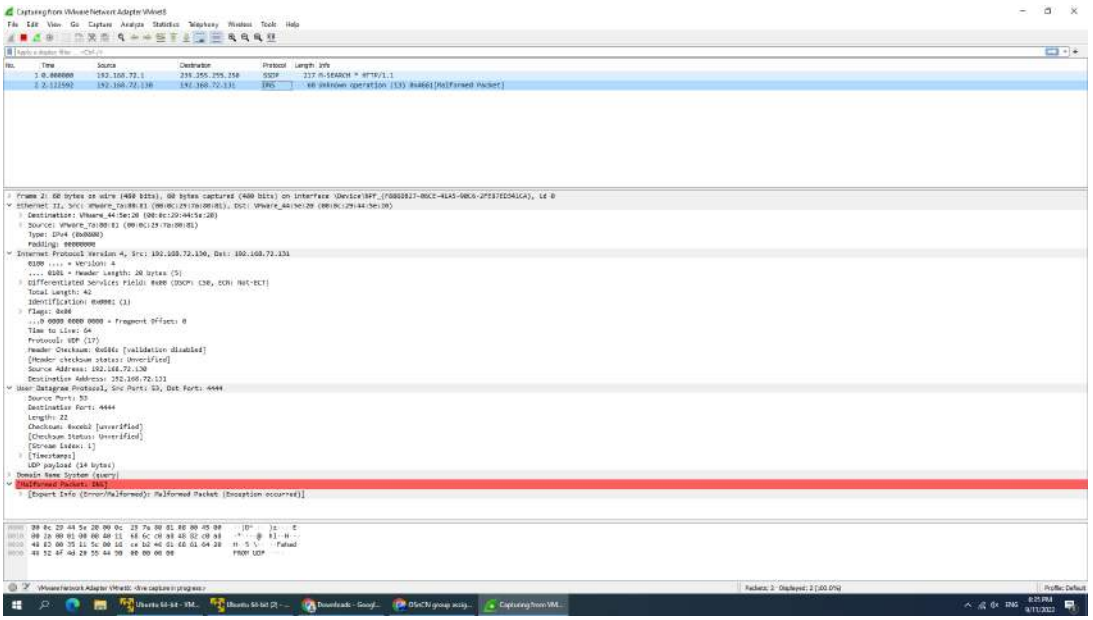
```
[Receiver]
$ nc -u -l 4444

[Sender]
$sudo scapy
|=============================================================|
|i=IP()                                                       |
|i.display                                                    |
|i.display()                                                  |
|i.dst = <destination IP address(mine was 192.168.186.128)>|
|u=UDP()                                                      |
|u.display                                                    |
|u.display()                                                  |
|u.dport = 4444                                               |
|send(i/u/”Satoaki FROM UDP”)                                 |
|=============================================================|
```



Question 5

a. 00:0c:29:0b:b5:7b
b. 00:0c:29:05:98:59
c. 192.168.6.130
d. 192.168.6.132
e. 53
f. 4444

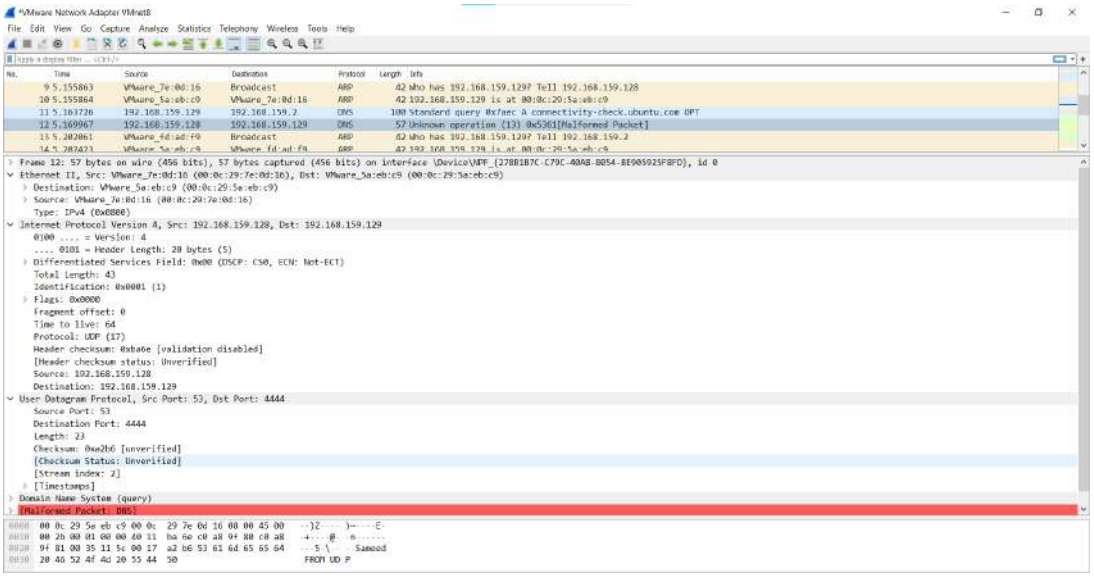
1.2 Mohamed Fahad Farhan



Question 5

a. 00:0c:29:7a:80:81
b. 00:0c:29:44:5e:20
c. 192.168.72.130
d. 192.168.72.131
e. 53
f. 4444

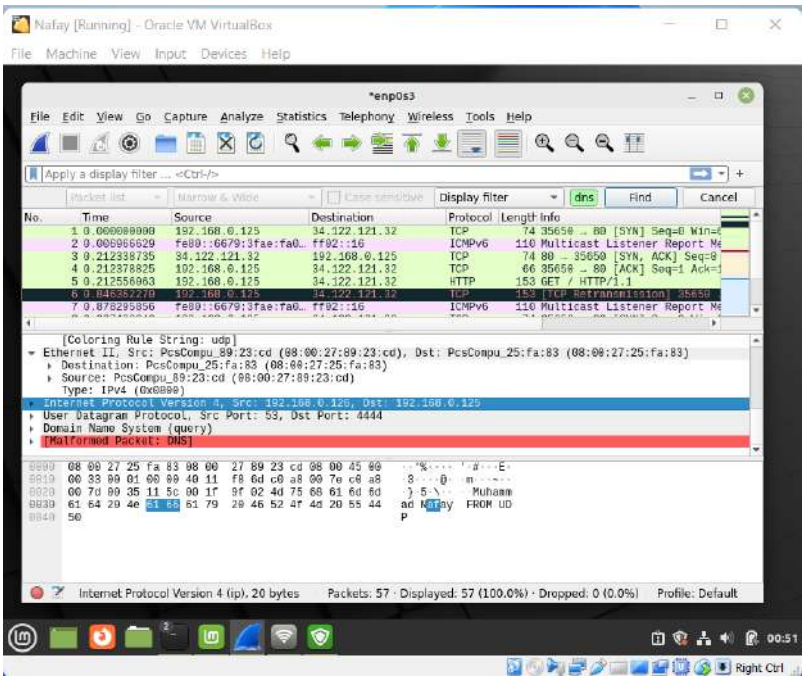
1.3 Mohammad Sameed Khan



Question 5

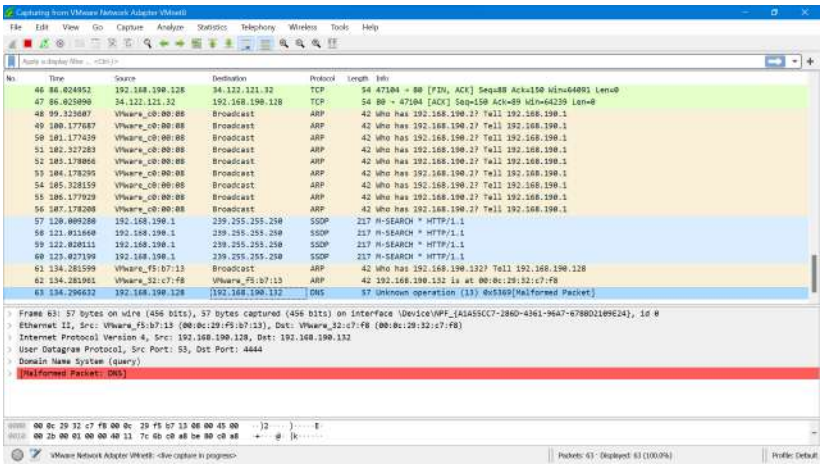
a. 00:0c:29:7e:0d:16
b. 00:0c:29:5a:eb:c9
c. 192.168.159.128
d. 192.168.159.129
e. 53
f. 4444

1.4 Muhammad Nafay



Question 5
a. 08:00:27:89:23:cd
b. 08:00:27:25:fa:83
c.192.168.0.126
d.192.168.0.125
e.53
f.4444

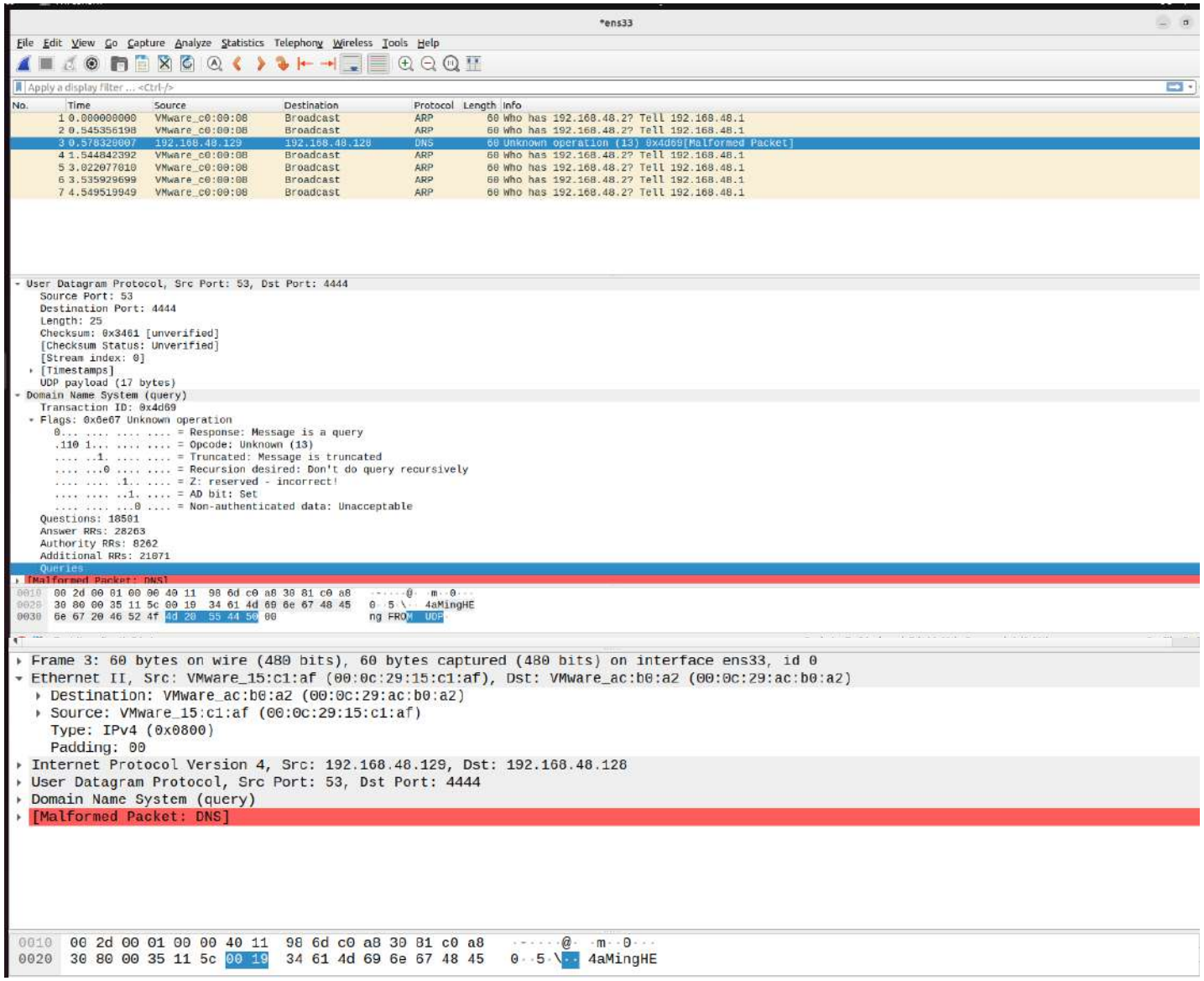
1.5 Thua Sin Wei



Question 5

a. 00:0c:29:f5:b7:13
b. 00:0c:29:32:c7:f8
c. 192.168.190.128
d. 192.168.190.132
e. 53
f. 4444

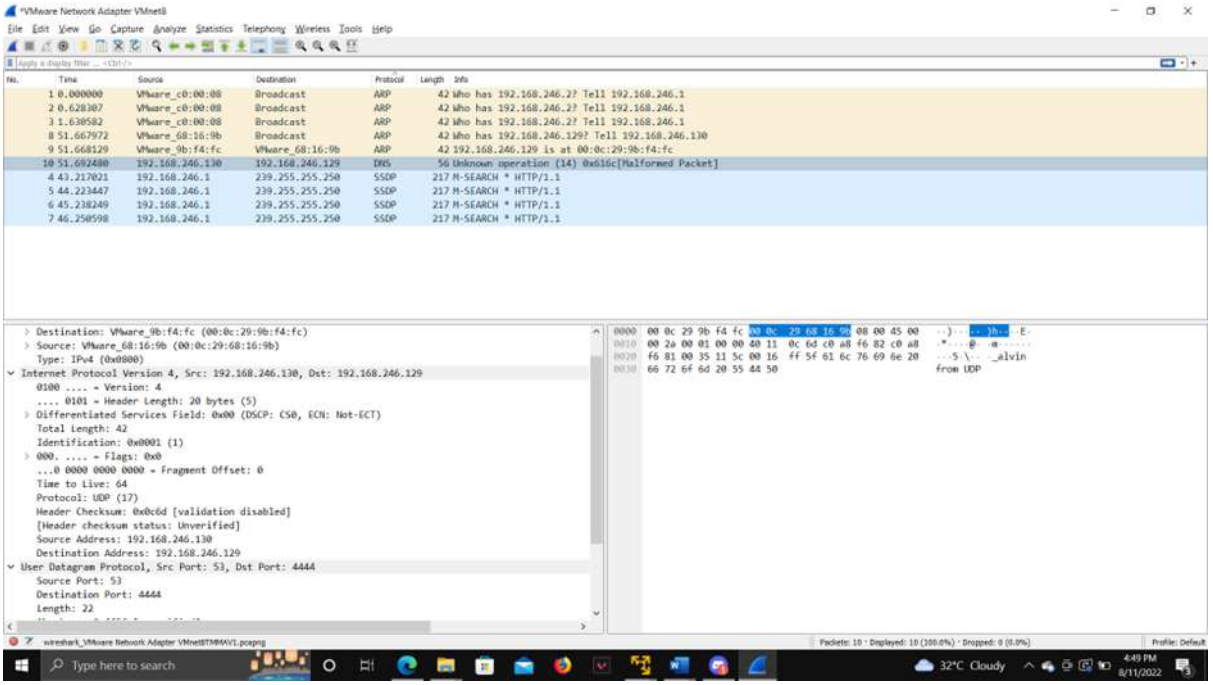
1.6 Teh Ming Heng



Answer the following questions once you find the UDP packet from Wireshark.

a. 00:0c:29:15:c1:af
b. 00:0c:29:ac:b0:a2
c. 192.168.48.129
d. 192.168.48.129
e. 53
f. 4444

1.7 Tang Wai Kin



Answer the following questions once you find the UDP packet from Wireshark.

a. What is the Source MAC address?

Ans: 00:0c:29:68:16:9b

b. What is the Destination MAC address?

Ans: 00:0c:29:9b:f4:fc

c. What is the Source IP address?

Ans: 192.168.246.130

d. What is the Destination IP address?

Ans: 192.168.246.129

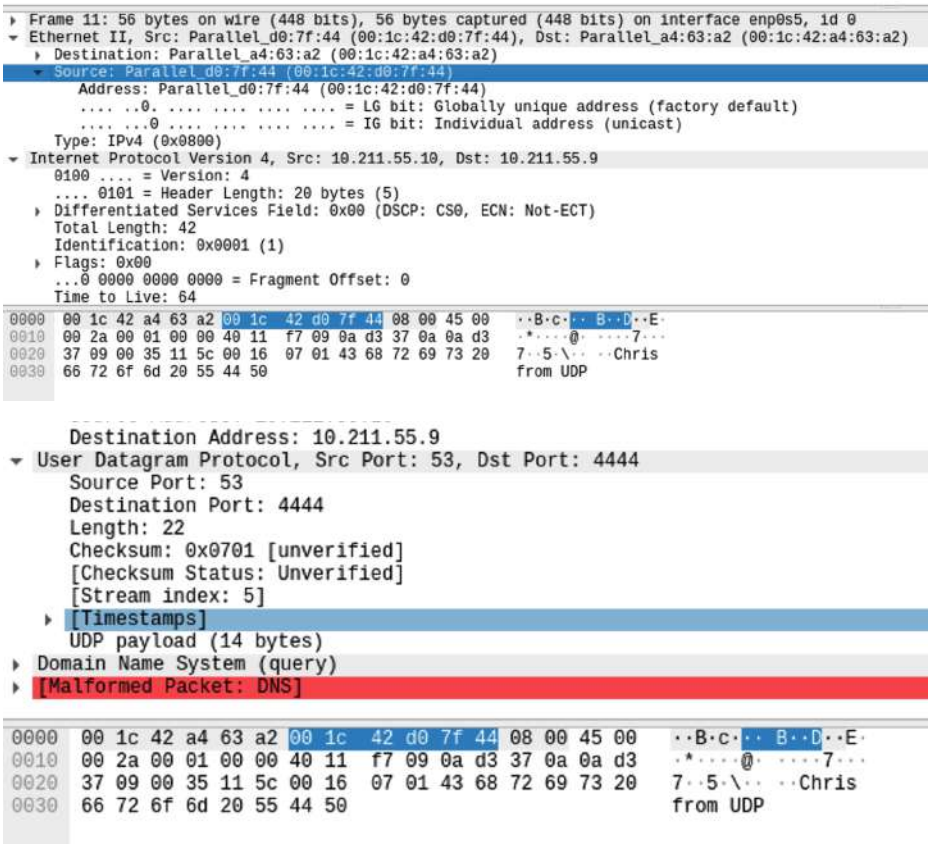
e. What is the Source Port?

Ans: 53

f. What is the Destination Port?

Ans: 4444

1.8 Christiaan Tim Vrieling



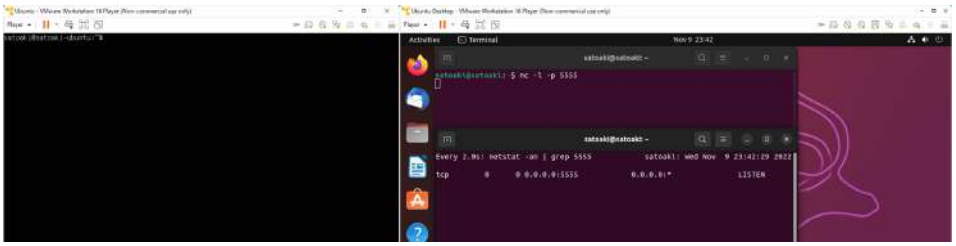
Answer the following questions once you find the UDP packet from Wireshark.

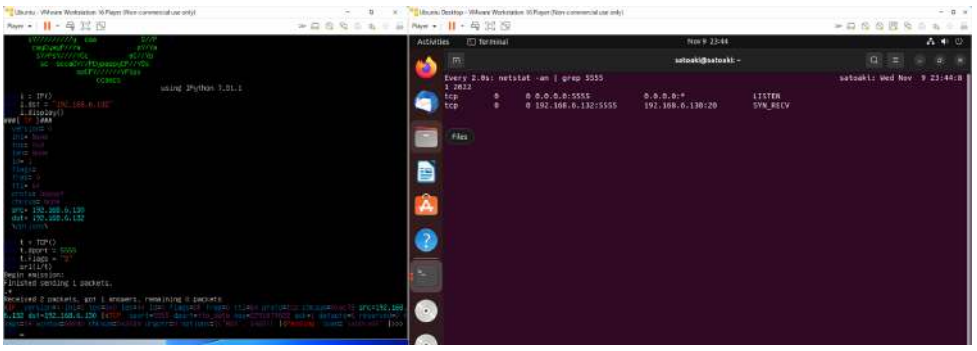
a. 00:1c:42:d0:7f:44
b. 00:1c:42:a4:63:a2
c. 10.211.55.10
d. 10.211.55.9
e. 53
f. 4444

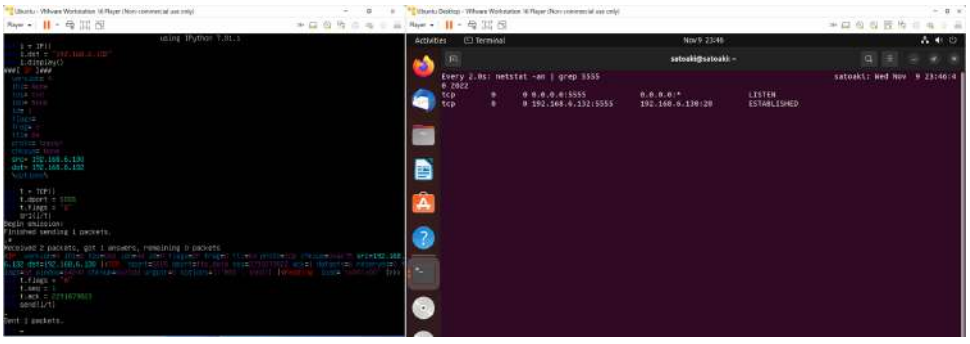
Section C

1.1 Ishihara Satoaki

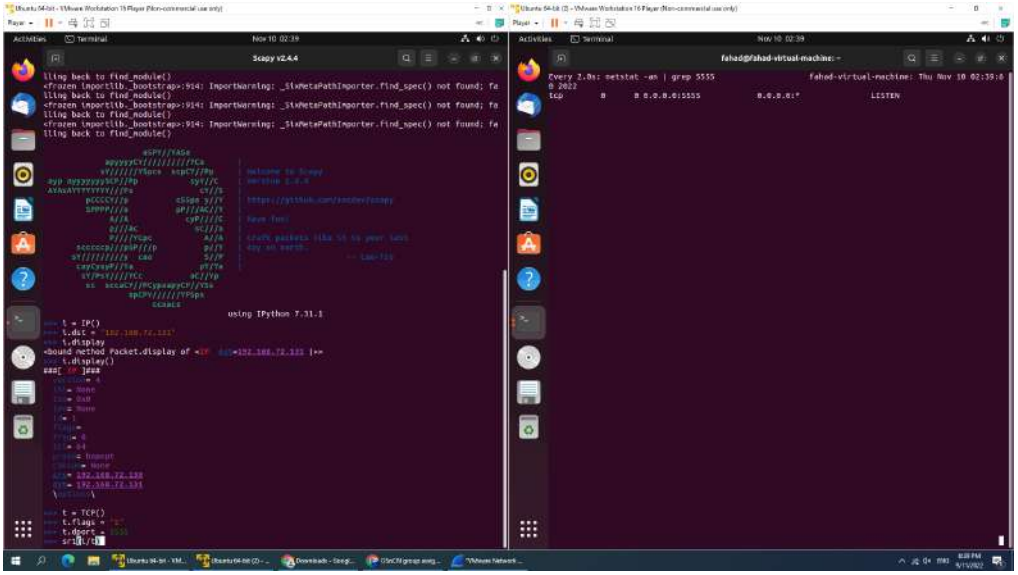
```
[Receiver]
nc -l -p 5555

[Sender]
$ sudo iptables -A OUTPUT -p tcp --tcp-flags RST RST -j DROP
$ sudo iptables -L
$ sudo scapy
|=========================================================|
|i=IP()                                                   |
|i.display                                                |
|i.display()                                              |
|i.dst = <destination IP address(mine was 192.168.186.128)>|
|t=TCP()                                                  |
|t.flags=”S”                                              |
|t.dport=5555                                             |
|sr1(i/t)                                                 |
|t.flags=”A” (execute within 60 seconds)                  |
|t.seq = 1   (execute within 60 seconds)                  |
|t.ack = <seq + 1>     (execute within 60 seconds)        |
|send(i/t)   (execute within 60 seconds)                  |
|=========================================================|
```

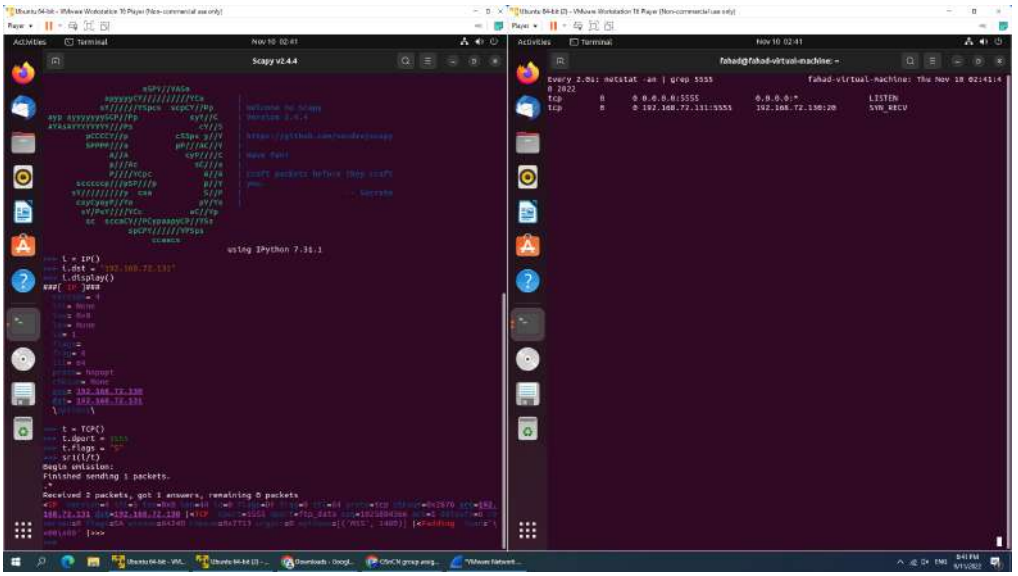


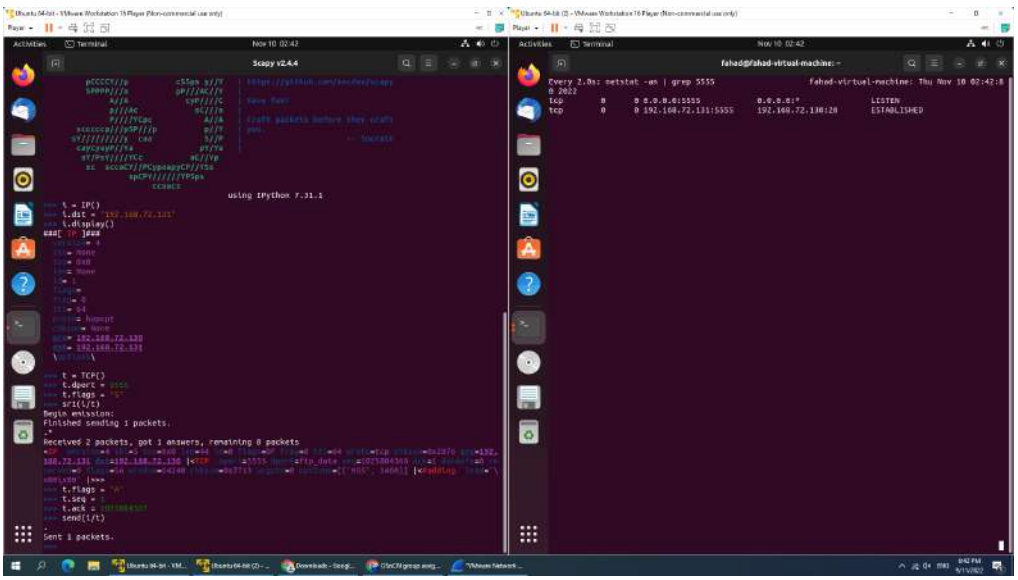




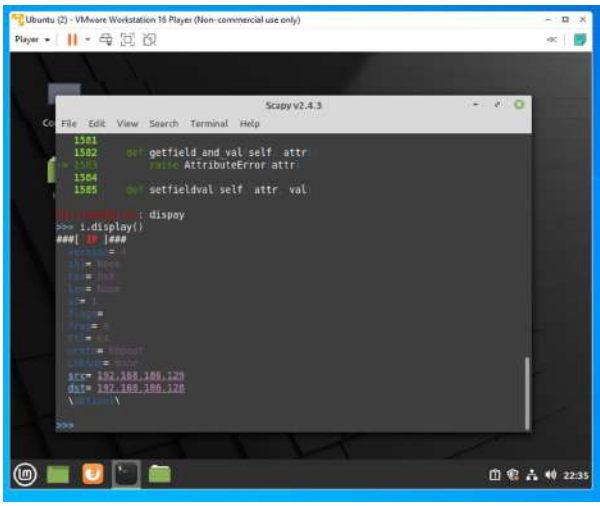
1.2 Mohamed Fahad Farhan

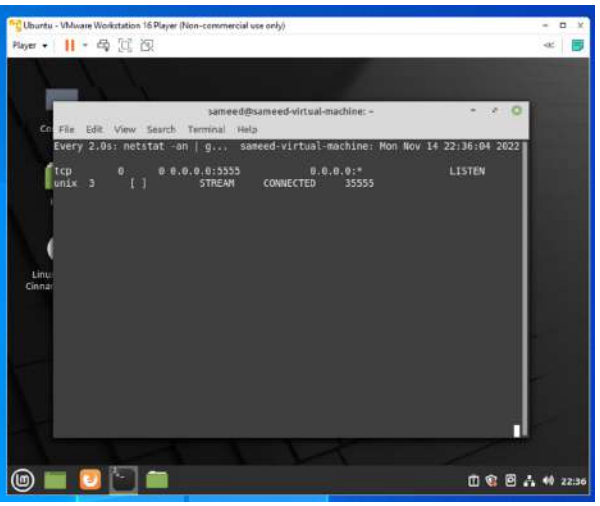


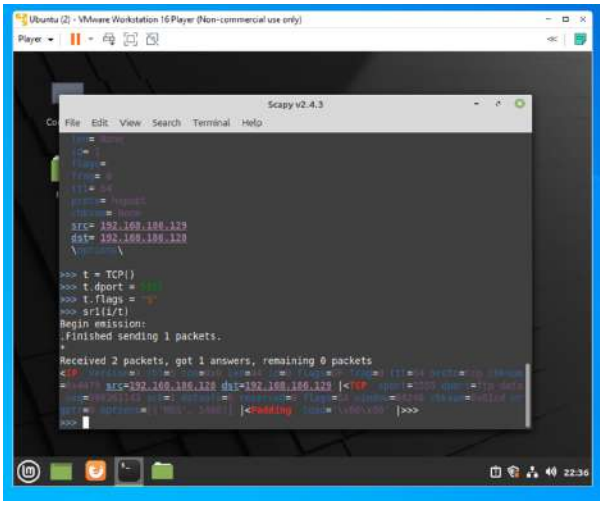


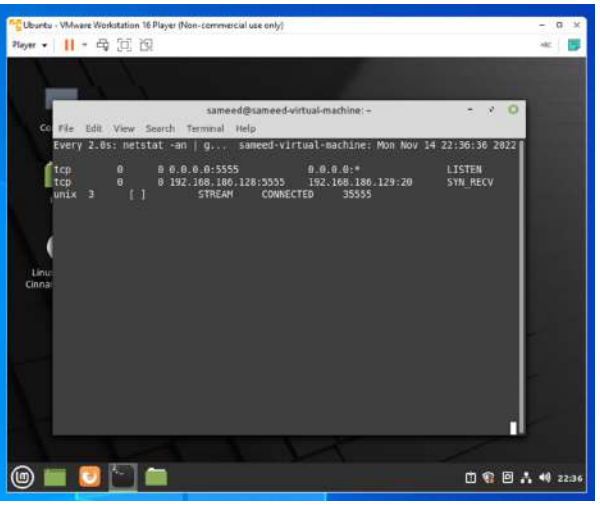


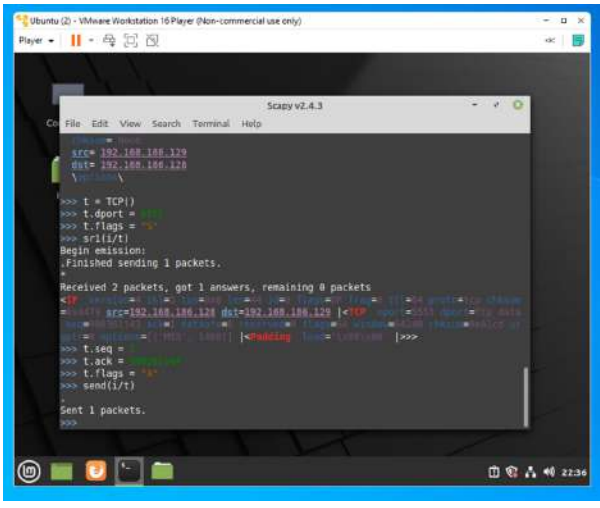
1.3 Mohammad Sameed Khan

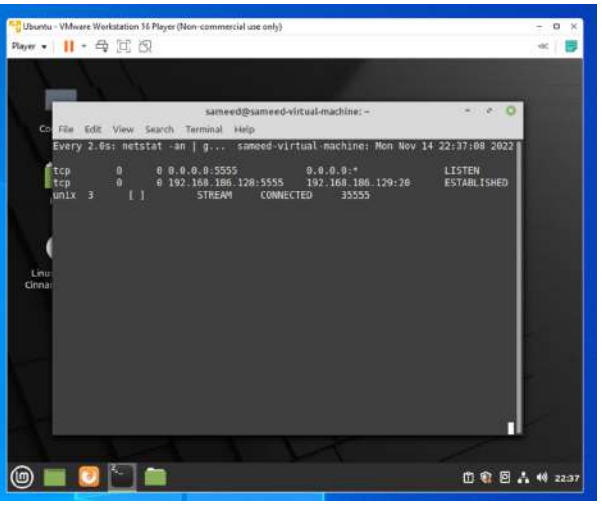




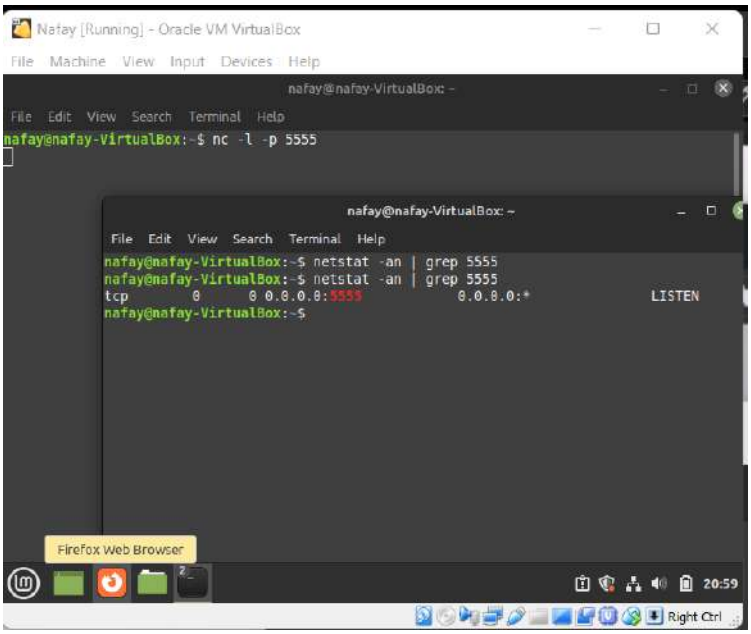


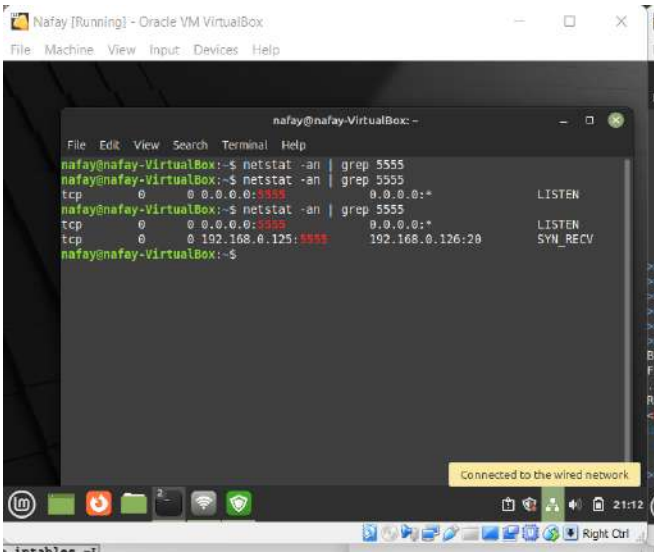


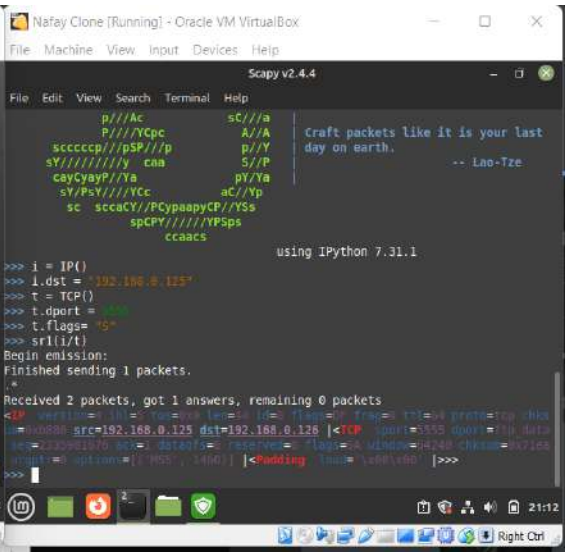


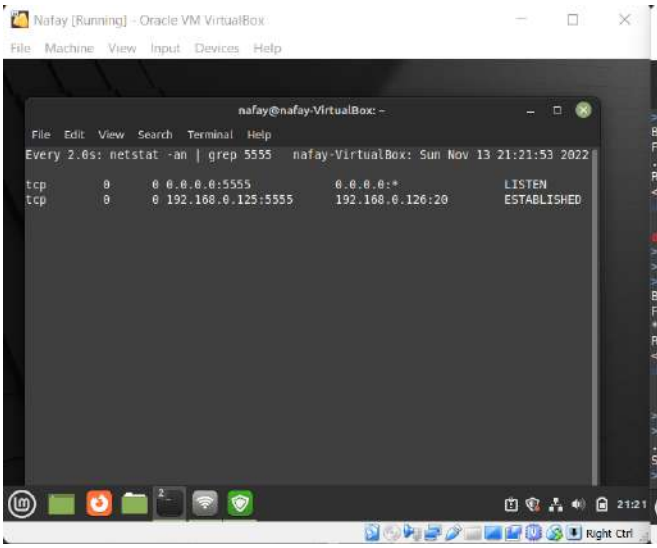


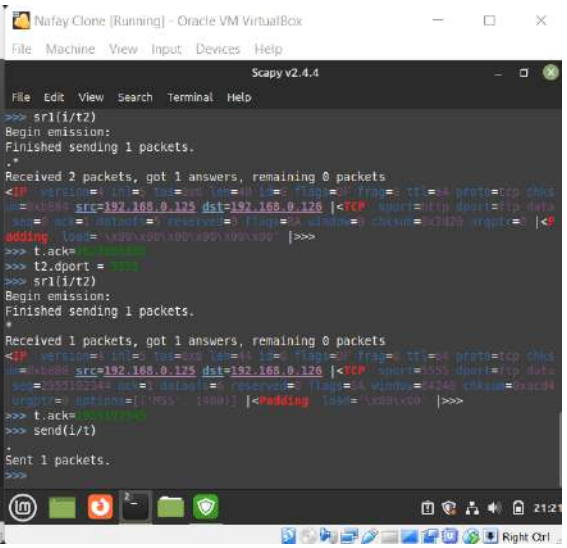
1.4 Muhammad Nafay



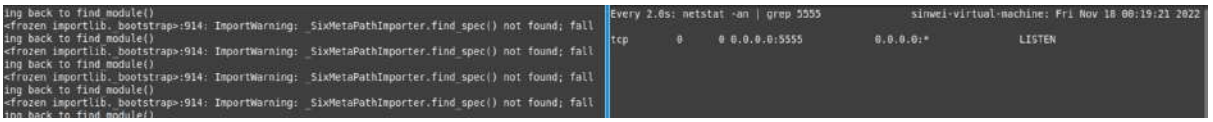


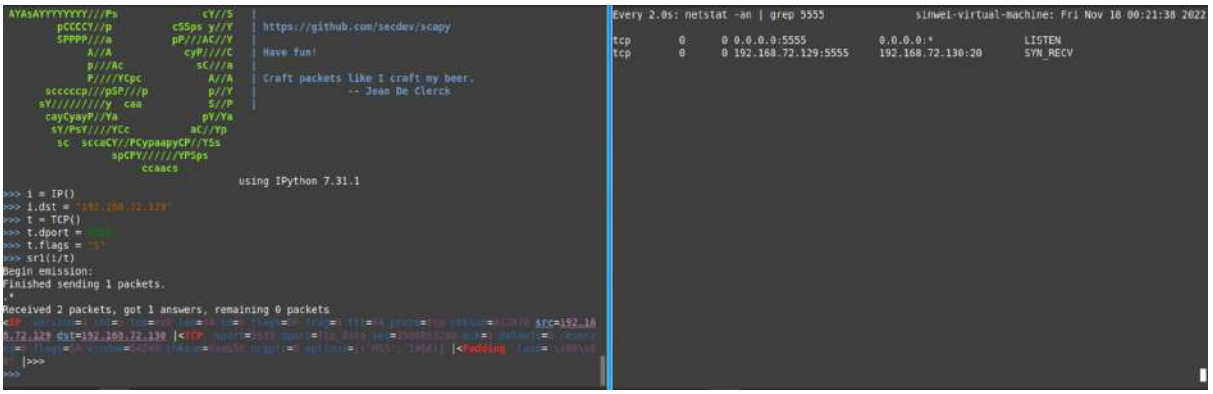




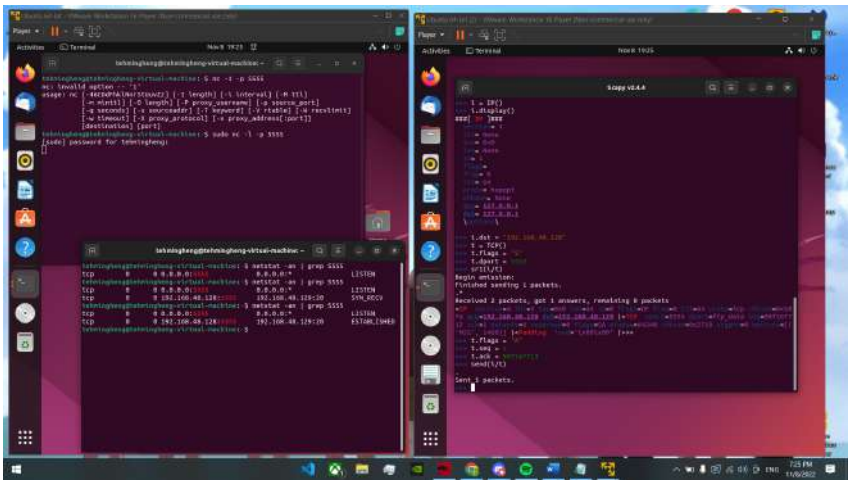


1.5 Thua Sin Wei

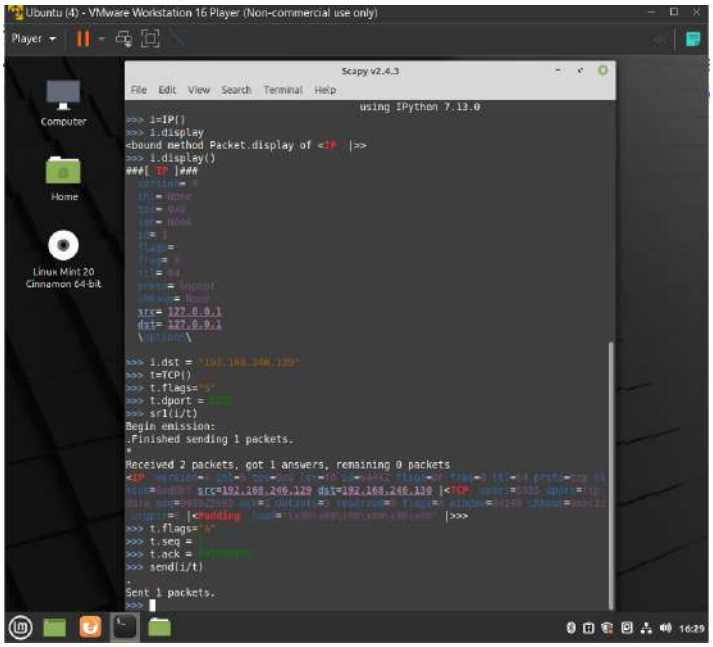


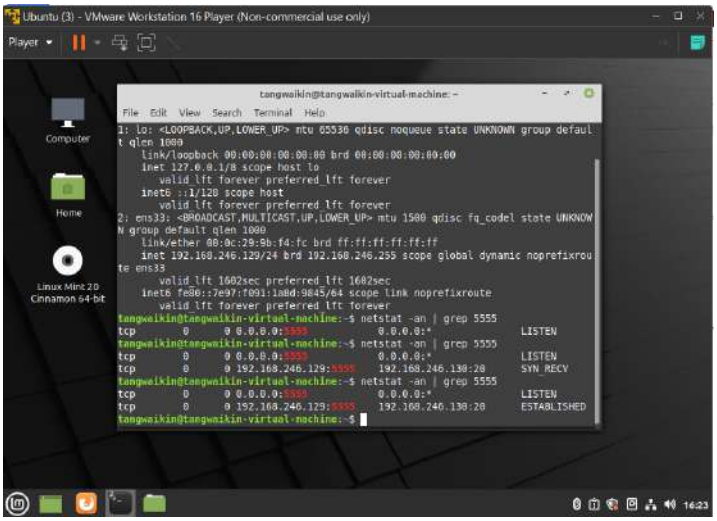


1.6 Teh Ming Heng

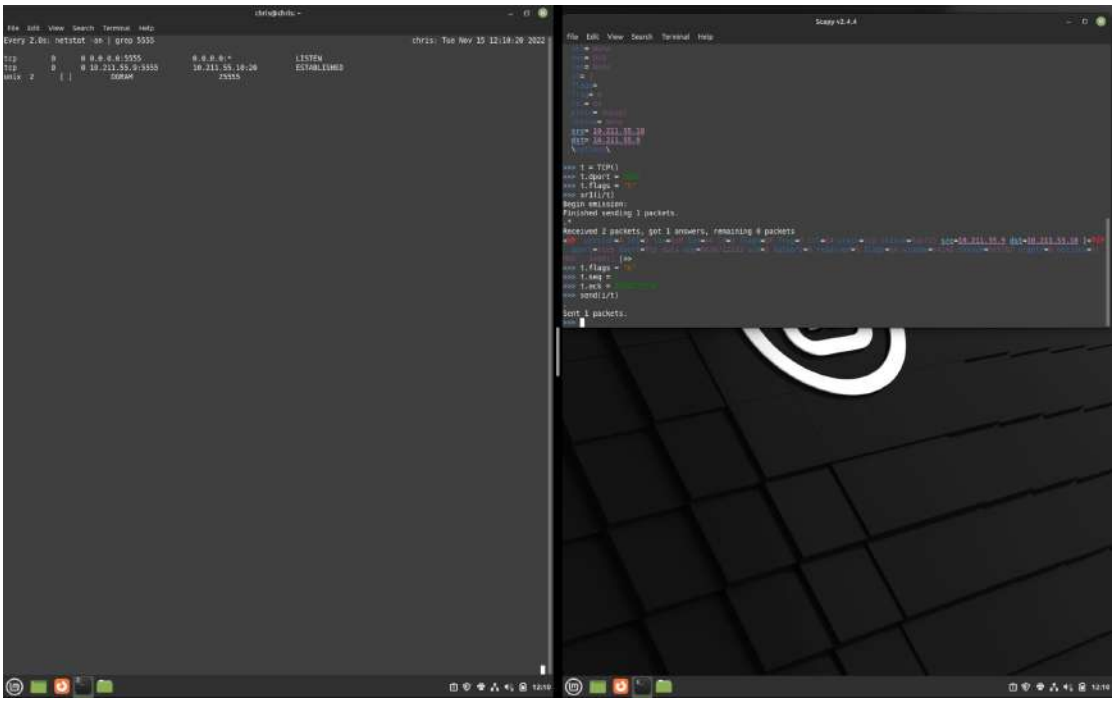


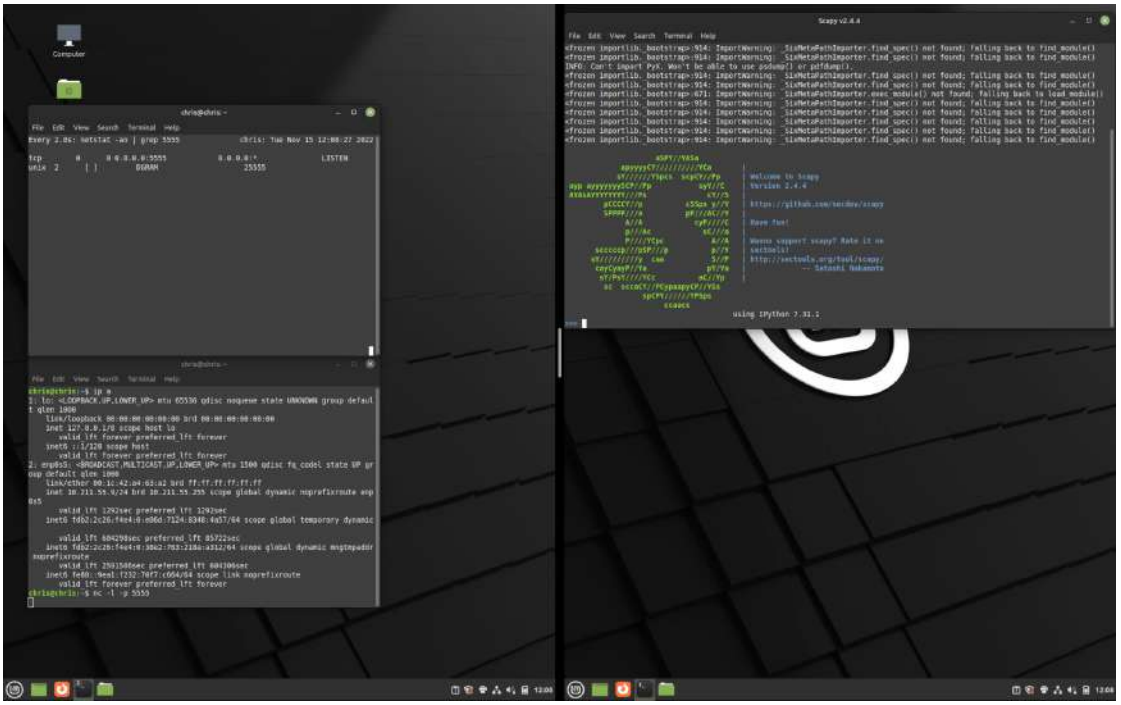
1.7 Tang Wai Kin

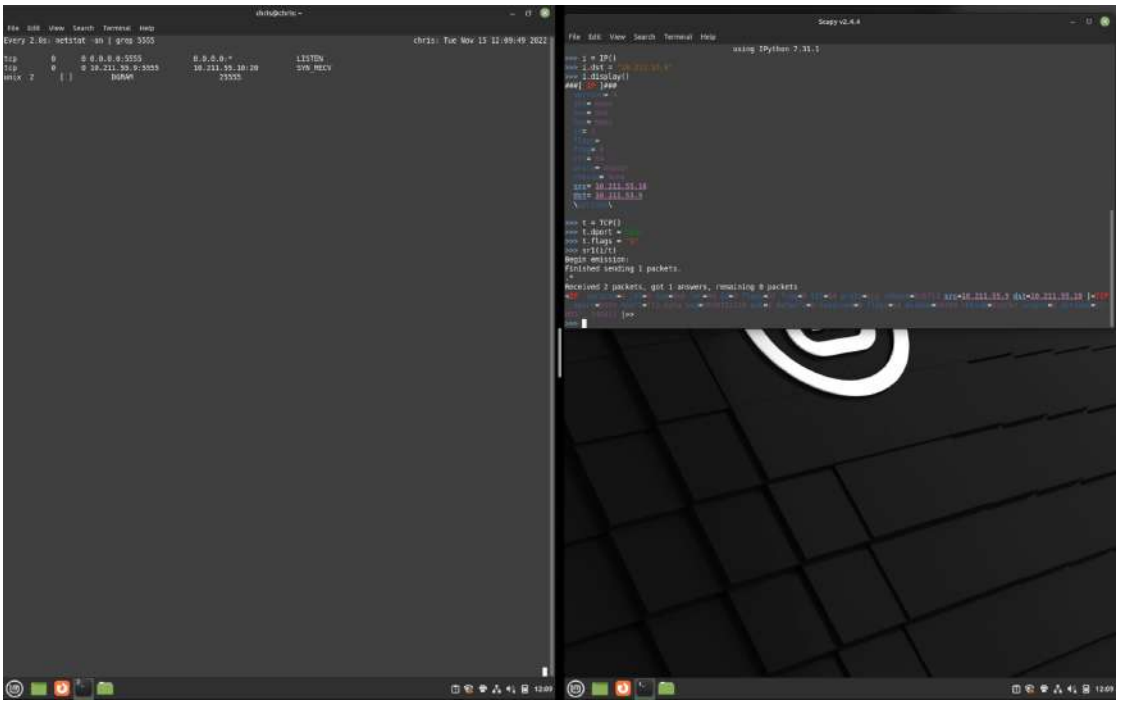




1.8 Christiaan Tim Vrieling






chris@chris: ~
File Edit View Search Terminal Help
Every 2.0s: netstat -an | grep 5555
chris: Tue Nov 15 12:09:49 2022
tcp 0 0 0.0.0.0:5555 0.0.0.0:* LISTEN
tcp 0 0 10.211.55.9:5555 10.211.55.10:20 SYN_RECV
unix 2 [ ] DGRAM 25555
Scapy v2.4.4
File Edit View Search Terminal Help
using IPython 7.31.1
>>> i = IP()
>>> i.dst = "10.211.55.9"
>>> i.display()
###[IP]###
src= 10.211.55.10
dst= 10.211.55.9
>>> t = TCP()
>>> t.dport = 5555
>>> t.flags = "S"
>>> sr1(i/t)
Begin emission:
Finished sending 1 packets.
*
Received 2 packets, got 1 answers, remaining 0 packets
>>>

Section D

1.1 Ishihara Satoaki

Question 1

Ping (Packet Internet or Inter-Network Groper) is an Internet program that allows hosts to test and confirm if a specific destination IP address exists and can receive requests in computer network administration. This tool exists on most OS we are using, such as WIndows OS, MacOS, Linux, etc.

We have to write commands like “ping <domain>” or “ping <IP address>”. Then, the sending of a special type message ICMP Echo Request will be begun.

ping <website>

```
satoaki@satoaki-ubuntu:~$ ping google.com
PING google.com (172.217.26.78) 56(84) bytes of data.
64 bytes from google.com (172.217.26.78): icmp_seq=1 ttl=128 time=39.3 ms
64 bytes from google.com (172.217.26.78): icmp_seq=2 ttl=128 time=8.87 ms
64 bytes from google.com (172.217.26.78): icmp_seq=3 ttl=128 time=9.39 ms
64 bytes from google.com (172.217.26.78): icmp_seq=4 ttl=128 time=9.42 ms
64 bytes from google.com (172.217.26.78): icmp_seq=5 ttl=128 time=8.55 ms
64 bytes from google.com (172.217.26.78): icmp_seq=6 ttl=128 time=10.5 ms
64 bytes from sin10s02-in-f78.1e100.net (172.217.26.78): icmp_seq=7 ttl=128 time=9.38 ms
64 bytes from kul08s14-in-f14.1e100.net (172.217.26.78): icmp_seq=8 ttl=128 time=9.37 ms
64 bytes from kul08s14-in-f14.1e100.net (172.217.26.78): icmp_seq=9 ttl=128 time=8.99 ms
64 bytes from sin10s02-in-f14.1e100.net (172.217.26.78): icmp_seq=10 ttl=128 time=9.19 ms
^C
--- google.com ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9020ms
rtt min/avg/max/mdev = 8.548/12.299/39.292/9.010 ms
```

ping <localhost>

```
satoaki@satoaki-ubuntu:~$ ping 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=1.25 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.089 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.115 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.088 ms
64 bytes from 127.0.0.1: icmp_seq=5 ttl=64 time=0.127 ms
64 bytes from 127.0.0.1: icmp_seq=6 ttl=64 time=0.124 ms
64 bytes from 127.0.0.1: icmp_seq=7 ttl=64 time=0.101 ms
64 bytes from 127.0.0.1: icmp_seq=8 ttl=64 time=0.077 ms
64 bytes from 127.0.0.1: icmp_seq=9 ttl=64 time=0.073 ms
64 bytes from 127.0.0.1: icmp_seq=10 ttl=64 time=0.082 ms
^C
--- 127.0.0.1 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9195ms
rtt min/avg/max/mdev = 0.073/0.212/1.253/0.347 ms
```

ping <other-ip-in-network>

```
satoaki@satoaki-ubuntu:~$ ping 192.168.6.132
PING 192.168.6.132 (192.168.6.132) 56(84) bytes of data.
64 bytes from 192.168.6.132: icmp_seq=1 ttl=64 time=4.77 ms
64 bytes from 192.168.6.132: icmp_seq=2 ttl=64 time=1.35 ms
64 bytes from 192.168.6.132: icmp_seq=3 ttl=64 time=0.703 ms
64 bytes from 192.168.6.132: icmp_seq=4 ttl=64 time=0.964 ms
64 bytes from 192.168.6.132: icmp_seq=5 ttl=64 time=0.585 ms
64 bytes from 192.168.6.132: icmp_seq=6 ttl=64 time=0.681 ms
64 bytes from 192.168.6.132: icmp_seq=7 ttl=64 time=0.712 ms
64 bytes from 192.168.6.132: icmp_seq=8 ttl=64 time=0.704 ms
64 bytes from 192.168.6.132: icmp_seq=9 ttl=64 time=1.28 ms
64 bytes from 192.168.6.132: icmp_seq=10 ttl=64 time=0.709 ms
^C
--- 192.168.6.132 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9018ms
rtt min/avg/max/mdev = 0.585/1.244/4.770/1.201 ms
```

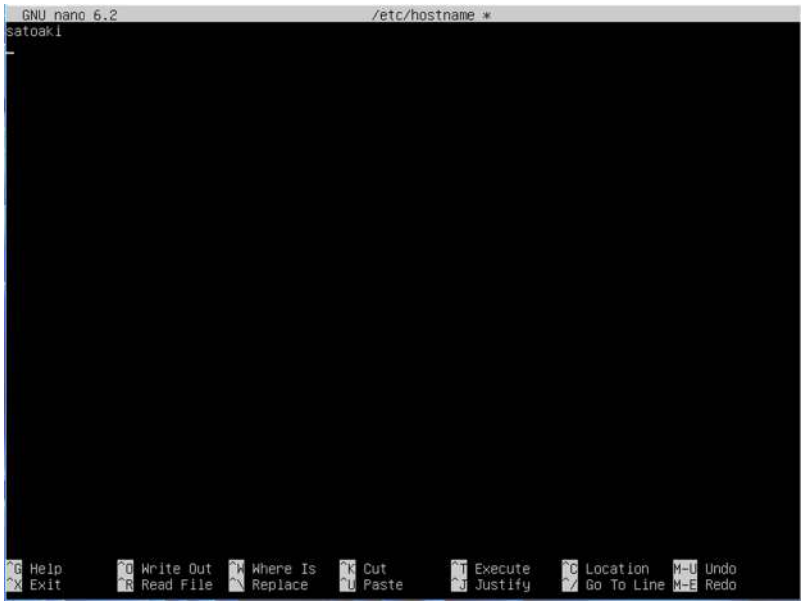
Question 2

“sudo nano /etc/hostname” is the command to change the displayed hostname saved in the “hostname” file in the etc directory.

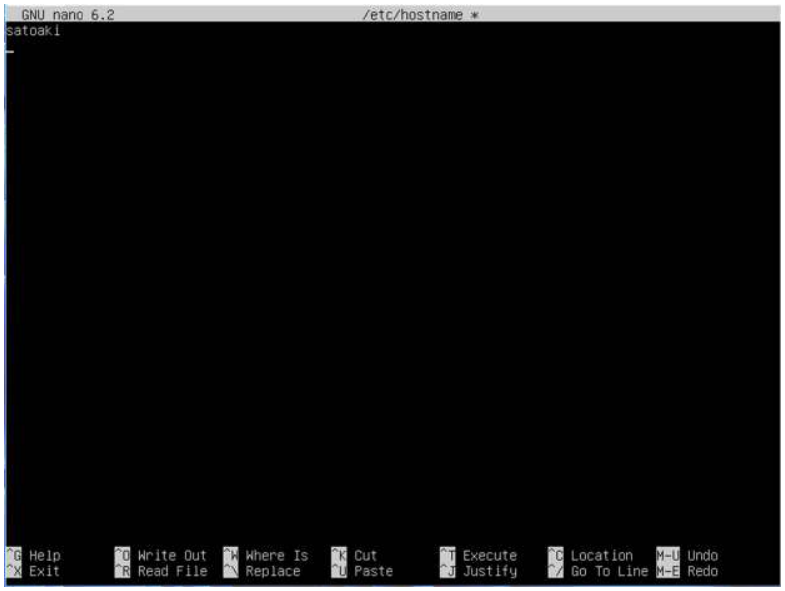
1. First, execute the command “sudo nano /etc/hostname” to open the hostname file as administrator, so that I can change our hostname.

2. Then proceed to the page as like in the image below.

3. change “satoaki-ubuntu” to “satoaki”.



4. Press Ctrl + X to exit the file. Then the Statement “Save modified buffer?”, so press Y to save the hostname file.



5. Execute the command “sudo reboot” to reboot the system to apply the change made on the hostname file.

```
satoaki@satoaki-ubuntu:~$ sudo reboot_
```

6. After I reboot the system and open the terminal, hostname is replaced with my <name>.

```
satoaki@satoaki:~$ sudo hostname
satoaki
```

Question 3

Traceroute is the tool to gather information among IP networks to nodes. There are more than 0 routers when two nodes such as PC or servers communicate with each other on the internet, and the list of routers passed through among the connection can be gathered by traceroute command.

```
satoaki@satoaki:~$ traceroute 192.168.6.130
traceroute to 192.168.6.130 (192.168.6.130), 30 hops max, 60 byte packets
 1  satoaki (192.168.6.130)  3.129 ms  0.016 ms  0.005 ms
```

Question 4

Netstat is the acronym of “network statistics”. It is the command line tool to display the statistical information of each network interface, available on Unix, Unix-like OS such as macOS or Linux, Microsoft Windows NT-based operating systems such as Windows 10, Windows 11, etc.

1. netstat -t

```
satoaki@satoaki:~$ netstat -t
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
```

2. netstat -s -t

```
satoaki@satoaki:~$ netstat -s -t
IcmpMsg:
    InType3: 40
    OutType3: 40
Tcp:
    3 active connection openings
    0 passive connection openings
    0 failed connection attempts
    1 connection resets received
    0 connections established
    91 segments received
    84 segments sent out
    0 segments retransmitted
    0 bad segments received
    1 resets sent
UdpLite:
TcpExt:
    2 TCP sockets finished time wait in fast timer
    3 delayed acks sent
    50 packet headers predicted
    4 acknowledgments not containing data payload received
    9 predicted acknowledgments
    TCPBacklogCoalesce: 1
    1 connections reset due to early user close
    TCPRcvCoalesce: 38
    TCPOrigDataSent: 13
    TCPDelivered: 16
IpExt:
    InBcastPkts: 33
    InOctets: 252198
    OutOctets: 14840
    InBcastOctets: 2574
    InNoECTPkts: 342
MPTcpExt:
```

3. netstat -i

```
satoaki@satoaki:~$ netstat -i
Kernel Interface table
Iface      MTU    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
ens33     1500      302      0      0 0           113      0      0      0 BMRU
lo       65536      100      0      0 0           100      0      0      0 LRU
```

Question 5

Tcpdump is the calculation network research tool we use on the console panel. The user can intercept and display TCP/IP and other packets flowing on the network to which the computer that executed the command is connected. It works on most Unix-like operating systems.

sudo tcpdump

```
satoaki@satoaki:~$ sudo tcpdump
[sudo] password for satoaki:
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on ens33, link-type EN10MB (Ethernet), snapshot length 262144 bytes
16:03:56.652324 IP 192.168.6.1.57931 > 239.255.255.250.1900: UDP, length 175
16:03:56.764021 IP satoaki.35766 > _gateway.domain: 55649+ [1au] PTR? 250.255.255.239.in-addr.arpa.
(57)
16:03:56.771360 IP _gateway.domain > satoaki.35766: 55649 NXDomain 0/1/1 (114)
16:03:56.771602 IP satoaki.35766 > _gateway.domain: 55649+ PTR? 250.255.255.239.in-addr.arpa. (46)
16:03:56.786865 IP _gateway.domain > satoaki.35766: 55649 NXDomain 0/1/0 (103)
16:03:56.787854 IP satoaki.46793 > _gateway.domain: 42542+ [1au] PTR? 1.6.168.192.in-addr.arpa. (53)
16:03:56.802803 IP _gateway.domain > satoaki.46793: 42542 NXDomain 0/0/1 (53)
16:03:56.802972 IP satoaki.46793 > _gateway.domain: 42542+ PTR? 1.6.168.192.in-addr.arpa. (42)
16:03:56.818678 IP _gateway.domain > satoaki.46793: 42542 NXDomain 0/0/0 (42)
16:03:56.854726 IP satoaki.44175 > _gateway.domain: 44105+ [1au] PTR? 2.6.168.192.in-addr.arpa. (53)
16:03:56.859632 IP _gateway.domain > satoaki.44175: 44105 NXDomain 0/0/1 (53)
16:03:56.859878 IP satoaki.44175 > _gateway.domain: 44105+ PTR? 2.6.168.192.in-addr.arpa. (42)
16:03:56.867167 IP _gateway.domain > satoaki.44175: 44105 NXDomain 0/0/0 (42)
16:03:56.868020 IP satoaki.50738 > _gateway.domain: 19468+ [1au] PTR? 130.6.168.192.in-addr.arpa. (5
5)
16:03:56.882729 IP _gateway.domain > satoaki.50738: 19468 NXDomain 0/0/1 (55)
16:03:56.882893 IP satoaki.50738 > _gateway.domain: 19468+ PTR? 130.6.168.192.in-addr.arpa. (44)
16:03:56.897865 IP _gateway.domain > satoaki.50738: 19468 NXDomain 0/0/0 (44)
16:03:57.668042 IP 192.168.6.1.57931 > 239.255.255.250.1900: UDP, length 175
^C
18 packets captured
18 packets received by filter
0 packets dropped by kernel
```

Question 6

Nmap is a security scanner written by Gordon Lyon. In addition to the port scan function, it also combines many other functions, including OS and version detection, and detection of services and their versions.

nmap –sP <ip address>

```
satoaki@satoaki:~$ sudo nmap -sP scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-12 01:06 +08
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.00070s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
```

nmap –sS <ip address>

```
satoaki@satoaki:~$ sudo nmap -sS scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-12 01:06 +08
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.013s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 997 filtered ports
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 64.34 seconds
```

nmap –sT <ip address>

```
satoaki@satoaki:~$ sudo nmap -sT scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-12 01:07 +08
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.0019s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 999 filtered ports
PORT   STATE SERVICE
21/tcp open  ftp

Nmap done: 1 IP address (1 host up) scanned in 23.24 seconds
```

nmap -sV -O <ip address>

```
satoakl@satoakl: $ sudo nmap -sV -O scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-12 01:10 +08
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.0083s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 997 filtered ports
PORT   STATE SERVICE    VERSION
21/tcp open  tcpwrapped
22/tcp open  ssh        OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80/tcp open  http       Apache httpd 2.4.7 ((Ubuntu))
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|specialized
Running: Microsoft Windows XP|7|2012, VMware Player
OS CPE: cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2012 cpe:/a:vmware:player
OS details: Microsoft Windows XP SP3, Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012, VMware Player virtual NAT device
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 95.45 seconds
```

nmap -A <ip address>

```
satoakl@satoakl: $ sudo nmap -A scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-12 01:12 +08
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.023s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 997 filtered ports
PORT   STATE SERVICE    VERSION
21/tcp open  tcpwrapped
22/tcp open  tcpwrapped
|_ssh-hostkey: ERROR: Script execution failed (use -d to debug)
80/tcp open  tcpwrapped
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: specialized|WAP|phone
Running: iPXE 1.X, Linux 2.4.X|2.6.X, Sony Ericsson embedded
OS CPE: cpe:/o:ipxe:ipxe:1.0.0%2b cpe:/o:linux:linux_kernel:2.4.20 cpe:/o:linux:linux_kernel:2.6.22 cpe:/h:sonyericsson:u8i_vivaz
OS details: iPXE 1.0.0+, Tomato 1.28 (Linux 2.4.20), Tomato firmware (Linux 2.6.22), Sony Ericsson U8i Vivaz mobile phone

TRACEROUTE (using port 80/tcp)
HOP RTT    ADDRESS
1   ... 30

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 64.09 seconds
```

1.2 Mohamed Fahad Farhan

ping <website>

```
fahad@fahad-virtual-machine:~$ ping google.com
PING google.com (216.58.199.238) 56(84) bytes of data.
64 bytes from kix05s02-in-f238.1e100.net (216.58.199.238): icmp_seq=1 ttl=128 time=13.2 ms
64 bytes from kul09s15-in-f14.1e100.net (216.58.199.238): icmp_seq=2 ttl=128 time=6.04 ms
64 bytes from kul09s15-in-f14.1e100.net (216.58.199.238): icmp_seq=3 ttl=128 time=5.02 ms
64 bytes from kix05s02-in-f14.1e100.net (216.58.199.238): icmp_seq=4 ttl=128 time=5.94 ms
64 bytes from kix05s02-in-f14.1e100.net (216.58.199.238): icmp_seq=5 ttl=128 time=5.72 ms
64 bytes from kix05s02-in-f238.1e100.net (216.58.199.238): icmp_seq=6 ttl=128 time=6.29 ms
64 bytes from kix05s02-in-f14.1e100.net (216.58.199.238): icmp_seq=7 ttl=128 time=5.33 ms
64 bytes from kix05s02-in-f238.1e100.net (216.58.199.238): icmp_seq=8 ttl=128 time=6.80 ms
64 bytes from kix05s02-in-f14.1e100.net (216.58.199.238): icmp_seq=9 ttl=128 time=6.10 ms
64 bytes from kix05s02-in-f238.1e100.net (216.58.199.238): icmp_seq=10 ttl=128 time=6.08 ms
^C
--- google.com ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9018ms
rtt min/avg/max/mdev = 5.024/6.653/13.216/2.236 ms
```

ping <localhost>

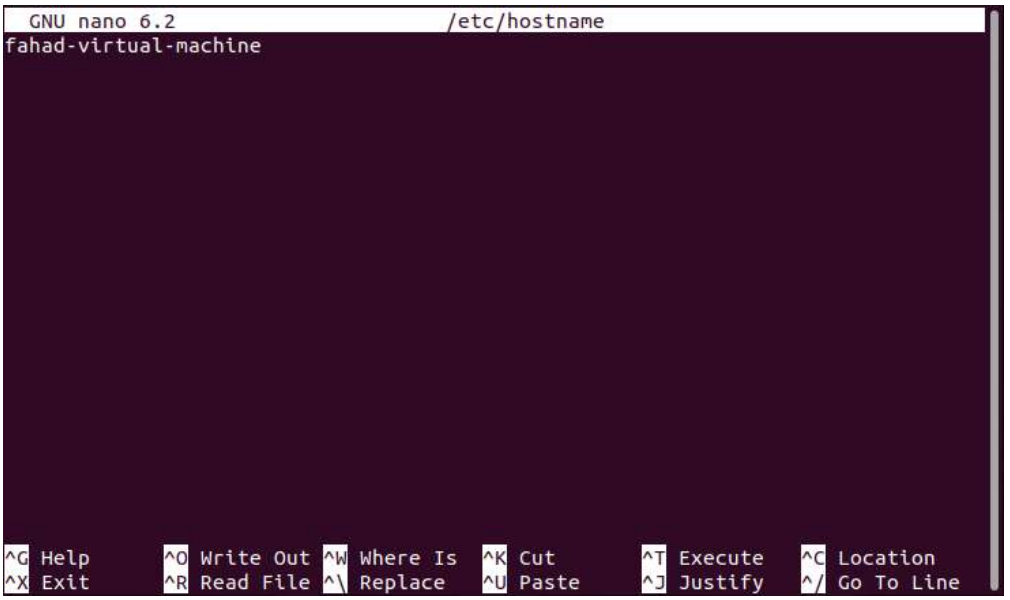
```
fahad@fahad-virtual-machine:~$ ping 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.028 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.069 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.070 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.046 ms
64 bytes from 127.0.0.1: icmp_seq=5 ttl=64 time=0.068 ms
64 bytes from 127.0.0.1: icmp_seq=6 ttl=64 time=0.069 ms
64 bytes from 127.0.0.1: icmp_seq=7 ttl=64 time=0.068 ms
64 bytes from 127.0.0.1: icmp_seq=8 ttl=64 time=0.069 ms
64 bytes from 127.0.0.1: icmp_seq=9 ttl=64 time=0.066 ms
64 bytes from 127.0.0.1: icmp_seq=10 ttl=64 time=0.069 ms
64 bytes from 127.0.0.1: icmp_seq=11 ttl=64 time=0.025 ms
64 bytes from 127.0.0.1: icmp_seq=12 ttl=64 time=0.070 ms
^C
--- 127.0.0.1 ping statistics ---
12 packets transmitted, 12 received, 0% packet loss, time 11251ms
rtt min/avg/max/mdev = 0.025/0.059/0.070/0.016 ms
```

ping <other-ip-in-network>

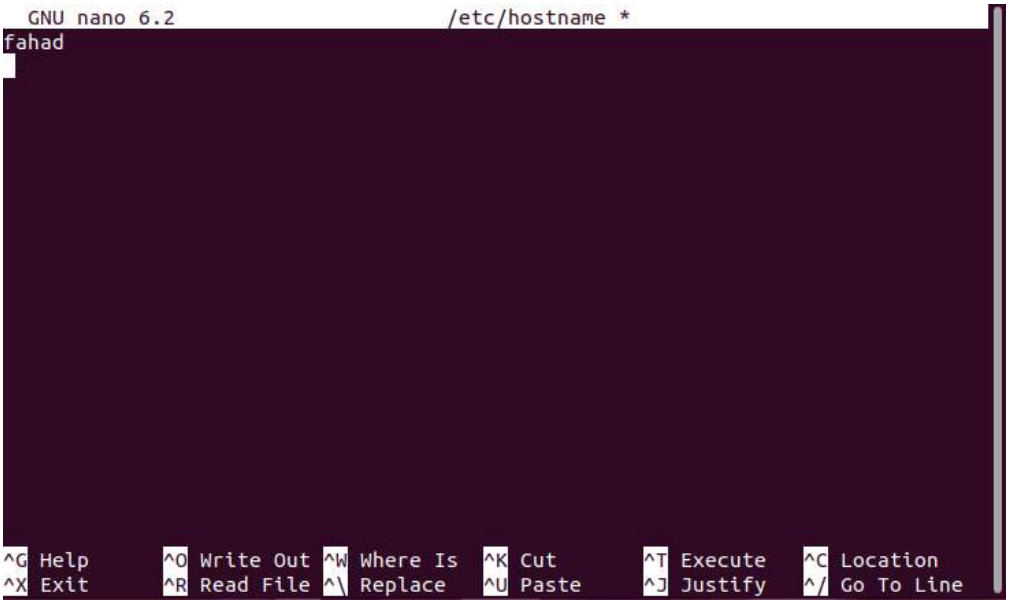
```
fahad@fahad-virtual-machine:~$ ping 192.168.72.131
PING 192.168.72.131 (192.168.72.131) 56(84) bytes of data.
64 bytes from 192.168.72.131: icmp_seq=1 ttl=64 time=0.397 ms
64 bytes from 192.168.72.131: icmp_seq=2 ttl=64 time=1.15 ms
64 bytes from 192.168.72.131: icmp_seq=3 ttl=64 time=1.19 ms
64 bytes from 192.168.72.131: icmp_seq=4 ttl=64 time=1.17 ms
64 bytes from 192.168.72.131: icmp_seq=5 ttl=64 time=0.420 ms
64 bytes from 192.168.72.131: icmp_seq=6 ttl=64 time=0.225 ms
64 bytes from 192.168.72.131: icmp_seq=7 ttl=64 time=1.25 ms
64 bytes from 192.168.72.131: icmp_seq=8 ttl=64 time=0.465 ms
64 bytes from 192.168.72.131: icmp_seq=9 ttl=64 time=0.455 ms
64 bytes from 192.168.72.131: icmp_seq=10 ttl=64 time=0.452 ms
^C
--- 192.168.72.131 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9110ms
rtt min/avg/max/mdev = 0.225/0.716/1.249/0.391 ms
```

Question 2

sudo nano /etc/hostname



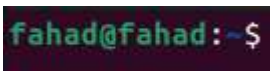
change fahad-virtual-machine to fahad.



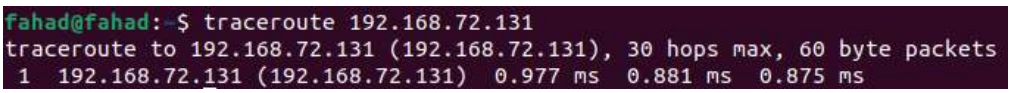
ctrl + x, “Save modified buffer?” => Y (yes)

click “enter” key.

Then, conduct “sudo reboot” command to reboot the system.



Question 3



Question 4

netstat -t

```
fahad@fahad:~$ netstat -t
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 fahad:48652             202.79.184.254:http     TIME_WAIT
```

netstat -s -t

```
fahad@fahad:~$ netstat -s -t
IcmpMsg:
    InType3: 46
    OutType3: 40
Tcp:
    9 active connection openings
    0 passive connection openings
    2 failed connection attempts
    0 connection resets received
    0 connections established
    148 segments received
    133 segments sent out
    4 segments retransmitted
    0 bad segments received
    2 resets sent
UdpLite:
TcpExt:
    1 TCP sockets finished time wait in fast timer
    1 delayed acks sent
    95 packet headers predicted
    8 acknowledgments not containing data payload received
    10 predicted acknowledgments
    TCPLostRetransmit: 3
    TCPTimeouts: 4
    TCPRcvCoalesce: 4
    TCPSynRetrans: 4
    TCPOrigDataSent: 18
    TCPDelivered: 24
    TcpTimeoutRehash: 4
IpExt:
    InMcastPkts: 61
    OutMcastPkts: 56
    InOctets: 512202
    OutOctets: 37075
    InMcastOctets: 6003
    OutMcastOctets: 6120
    InNoECTPkts: 681
MPTcpExt:
```

netstat -i

```
fahad@fahad:~$ netstat -i
Kernel Interface table
Iface      MTU    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
ens33     1500      543      0      0 0           315      0      0      0 BMRU
lo       65536      199      0      0 0           199      0      0      0 LRU
```

Question 5

```
fahad@fahad:~$ sudo tcpdump
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on ens33, link-type EN10MB (Ethernet), snapshot length 262144 bytes
03:00:52.881169 IP 192.168.72.131.36818 > _gateway.domain: 30662+ [1au] AAAA? connectivity-check.ubuntu.com. (58)
03:00:52.885896 IP _gateway.domain > 192.168.72.131.36818: 30662 0/1/1 (119)
03:00:52.888824 IP 192.168.72.131.47257 > _gateway.domain: 22064+ [1au] A? connectivity-check.ubuntu.com. (58)
03:00:52.889180 IP 192.168.72.131.39882 > _gateway.domain: 56497+ [1au] AAAA? connectivity-check.ubuntu.com. (58)
03:00:52.893944 IP _gateway.domain > 192.168.72.131.47257: 22064 3/0/1 A 35.224.170.84, A 35.232.111.17, A 34.122.121.32 (106)
03:00:52.894636 IP _gateway.domain > 192.168.72.131.39882: 56497 0/1/1 (119)
03:00:52.911480 IP fahad.43906 > _gateway.domain: 54381+ [1au] PTR? 2.72.168.192.in-addr.arpa. (54)
03:00:52.928159 IP _gateway.domain > fahad.43906: 54381 NXDomain 0/1/1 (113)
03:00:52.928304 IP fahad.43906 > _gateway.domain: 54381+ PTR? 2.72.168.192.in-addr.arpa. (43)
03:00:52.933056 IP _gateway.domain > fahad.43906: 54381 NXDomain 0/1/0 (102)
03:00:52.933991 IP fahad.46992 > _gateway.domain: 60483+ [1au] PTR? 131.72.168.192.in-addr.arpa. (56)
03:00:52.938262 IP _gateway.domain > fahad.46992: 60483 NXDomain 0/1/1 (115)
03:00:52.938405 IP fahad.46992 > _gateway.domain: 60483+ PTR? 131.72.168.192.in-addr.arpa. (45)
03:00:52.943030 IP _gateway.domain > fahad.46992: 60483 NXDomain 0/1/0 (104)
03:00:53.006425 IP fahad.51268 > _gateway.domain: 21431+ [1au] PTR? 130.72.168.192.in-addr.arpa. (56)
03:00:53.010678 IP _gateway.domain > fahad.51268: 21431 NXDomain 0/1/1 (115)
03:00:53.010726 IP fahad.51268 > _gateway.domain: 21431+ PTR? 130.72.168.192.in-addr.arpa. (45)
03:00:53.014560 IP _gateway.domain > fahad.51268: 21431 NXDomain 0/1/0 (104)
^C
18 packets captured
18 packets received by filter
0 packets dropped by kernel
```

Question 6

```
fahad@fahad:~$ sudo nmap -sP scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-10 03:03 +08
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.00075s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
fahad@fahad:~$ sudo nmap -sS scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-10 03:03 +08
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.018s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 997 filtered ports
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 54.22 seconds
fahad@fahad:~$ sudo nmap -sT scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-10 03:06 +08
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.14s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 997 filtered ports
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 57.10 seconds
```

```
fahad@fahad:~$ sudo nmap -sV -O scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-10 03:08 +08
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.0865s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 997 filtered ports
PORT   STATE SERVICE    VERSION
21/tcp open  tcpwrapped
22/tcp open  ssh        OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80/tcp open  http       Apache httpd 2.4.7 ((Ubuntu))
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: WAP|general purpose
Running: Actiontec embedded, Linux 2.4.X|3.X, Microsoft Windows XP|7|2012
OS CPE: cpe:/h:actiontec:mi424wr-gen3i cpe:/o:linux:linux_kernel cpe:/o:linux:linux_kernel:2.4.37 cpe:/o:linux:linux_kernel:3.2 cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2012
OS details: Actiontec MI424WR-GEN3I WAP, DD-WRT v24-sp2 (Linux 2.4.37), Linux 3.2, Microsoft Windows XP SP3, Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 100.14 seconds
fahad@fahad:~$ sudo nmap -A scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-10 03:10 +08
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.023s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 997 filtered ports
PORT   STATE SERVICE    VERSION
21/tcp open  tcpwrapped
22/tcp open  tcpwrapped
|_ssh-hostkey: ERROR: Script execution failed (use -d to debug)
80/tcp open  tcpwrapped
|_http-server-header: Apache/2.4.7 (Ubuntu)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: specialized|WAP|phone
Running: iPXE 1.X, Linux 2.4.X|2.6.X, Sony Ericsson embedded
OS CPE: cpe:/o:ipxe:ipxe:1.0.0%2b cpe:/o:linux:linux_kernel:2.4.20 cpe:/o:linux:linux_kernel:2.6.22 cpe:/h:sonyericsson:u8i_vivaz
OS details: iPXE 1.0.0+, Tomato 1.28 (Linux 2.4.20), Tomato firmware (Linux 2.6.22), Sony Ericsson U8i Vivaz mobile phone

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   ... 30

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 53.17 seconds
```

1.3 Mohammad Sameed Khan

ping <website>

```
sameed@sameed-virtual-machine:~$ ping google.com
PING google.com (142.250.4.102) 56(84) bytes of data.
64 bytes from sm-in-f102.1e100.net (142.250.4.102): icmp_seq=1 ttl=128 time=11.7 ms
64 bytes from sm-in-f102.1e100.net (142.250.4.102): icmp_seq=2 ttl=128 time=64.2 ms
64 bytes from sm-in-f102.1e100.net (142.250.4.102): icmp_seq=3 ttl=128 time=20.6 ms
64 bytes from sm-in-f102.1e100.net (142.250.4.102): icmp_seq=4 ttl=128 time=43.1 ms
64 bytes from sm-in-f102.1e100.net (142.250.4.102): icmp_seq=5 ttl=128 time=18.5 ms
64 bytes from sm-in-f102.1e100.net (142.250.4.102): icmp_seq=6 ttl=128 time=21.0 ms
64 bytes from sm-in-f102.1e100.net (142.250.4.102): icmp_seq=7 ttl=128 time=21.2 ms
64 bytes from sm-in-f102.1e100.net (142.250.4.102): icmp_seq=8 ttl=128 time=21.5 ms
64 bytes from sm-in-f102.1e100.net (142.250.4.102): icmp_seq=9 ttl=128 time=20.1 ms
64 bytes from sm-in-f102.1e100.net (142.250.4.102): icmp_seq=10 ttl=128 time=21.6 ms
64 bytes from sm-in-f102.1e100.net (142.250.4.102): icmp_seq=11 ttl=128 time=18.2 ms
^C
--- google.com ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 11051ms
rtt min/avg/max/mdev = 11.687/25.606/64.243/14.224 ms
sameed@sameed-virtual-machine:~$
```

ping <localhost>

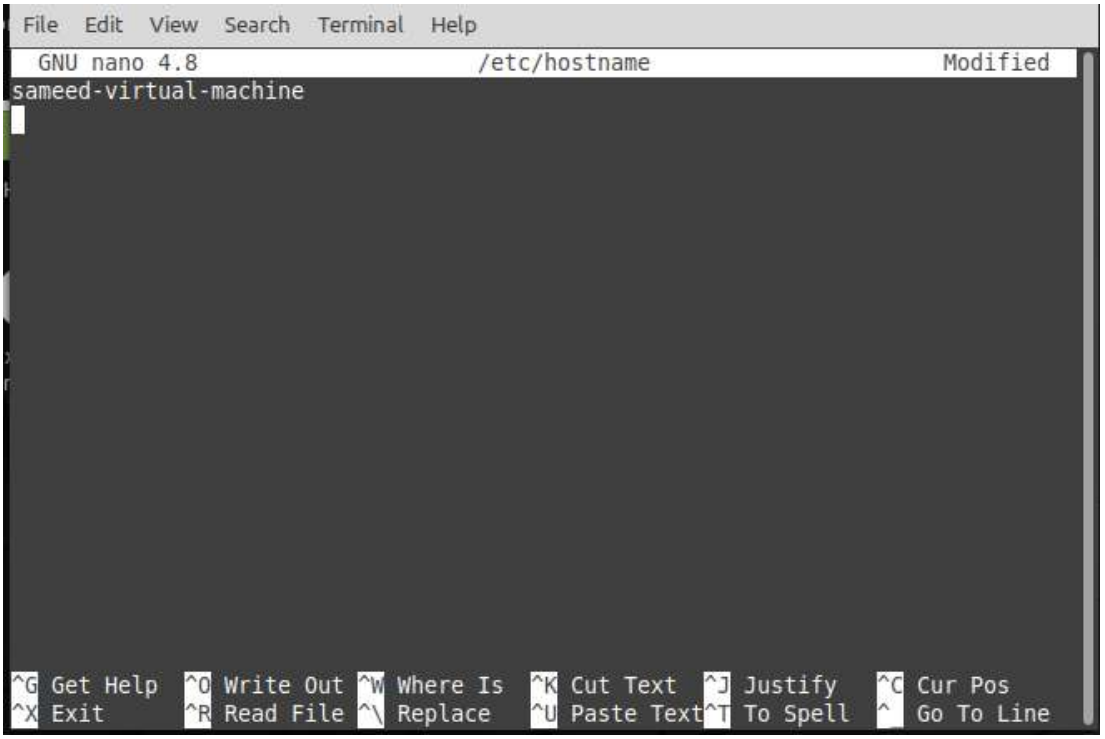
```
sameed@sameed-virtual-machine:~$ ping 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.062 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.054 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.031 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.055 ms
64 bytes from 127.0.0.1: icmp_seq=5 ttl=64 time=0.057 ms
64 bytes from 127.0.0.1: icmp_seq=6 ttl=64 time=0.057 ms
64 bytes from 127.0.0.1: icmp_seq=7 ttl=64 time=0.054 ms
64 bytes from 127.0.0.1: icmp_seq=8 ttl=64 time=0.029 ms
64 bytes from 127.0.0.1: icmp_seq=9 ttl=64 time=0.043 ms
64 bytes from 127.0.0.1: icmp_seq=10 ttl=64 time=0.042 ms
64 bytes from 127.0.0.1: icmp_seq=11 ttl=64 time=0.056 ms
64 bytes from 127.0.0.1: icmp_seq=12 ttl=64 time=0.039 ms
64 bytes from 127.0.0.1: icmp_seq=13 ttl=64 time=0.029 ms
^C
--- 127.0.0.1 ping statistics ---
13 packets transmitted, 13 received, 0% packet loss, time 12267ms
rtt min/avg/max/mdev = 0.029/0.046/0.062/0.011 ms
```

ping <other-ip-in-network>

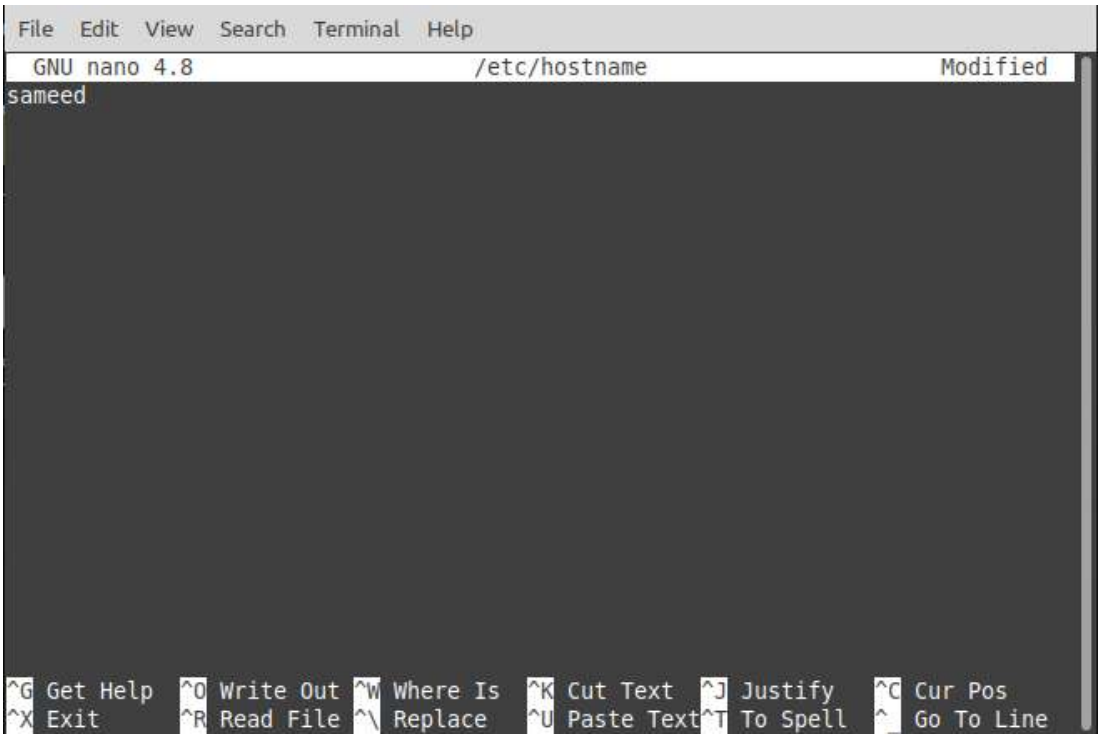
```
sameed@sameed-virtual-machine:~$ ping 192.168.159.128
PING 192.168.159.128 (192.168.159.128) 56(84) bytes of data.
64 bytes from 192.168.159.128: icmp_seq=1 ttl=64 time=0.017 ms
64 bytes from 192.168.159.128: icmp_seq=2 ttl=64 time=0.023 ms
64 bytes from 192.168.159.128: icmp_seq=3 ttl=64 time=0.023 ms
64 bytes from 192.168.159.128: icmp_seq=4 ttl=64 time=0.022 ms
64 bytes from 192.168.159.128: icmp_seq=5 ttl=64 time=0.037 ms
64 bytes from 192.168.159.128: icmp_seq=6 ttl=64 time=0.040 ms
64 bytes from 192.168.159.128: icmp_seq=7 ttl=64 time=0.023 ms
64 bytes from 192.168.159.128: icmp_seq=8 ttl=64 time=0.023 ms
64 bytes from 192.168.159.128: icmp_seq=9 ttl=64 time=0.023 ms
^C
--- 192.168.159.128 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8183ms
rtt min/avg/max/mdev = 0.017/0.025/0.040/0.007 ms
```

Question 2

sudo nano /etc/hostname



change sameed-virtual-machine to sameed.



ctrl + x, “Save modified buffer?” => Y (yes)

click “enter” key.

Then, conduct “sudo reboot” command to reboot the system.

```
sameed@sameed:~$
```

Question 3

```
sameed@sameed:~$ traceroute 192.168.159.128
traceroute to 192.168.159.128 (192.168.159.128), 30 hops max, 60 byte packets
 1  sameed (192.168.159.128)  0.189 ms  0.173 ms  0.108 ms
```

Question 4

netstat -t

```
sameed@sameed:~$ netstat -t
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
```

netstat -s -t

```
sameed@sameed:~$ netstat -s -t
IcmpMsg:
    InType3: 60
    OutType3: 60
Tcp:
    10 active connection openings
    0 passive connection openings
    2 failed connection attempts
    1 connection resets received
    0 connections established
    67 segments received
    61 segments sent out
    1 segments retransmitted
    0 bad segments received
    3 resets sent
UdpLite:
TcpExt:
    1 TCP sockets finished time wait in fast timer
    26 packet headers predicted
    7 acknowledgments not containing data payload received
    8 predicted acknowledgments
    TCPTimeouts: 1
    1 connections reset due to early user close
    TCPSynRetrans: 1
    TCPOrigDataSent: 15
    TCPDelivered: 23
IpExt:
    InMcastPkts: 181
    OutMcastPkts: 45
    InBcastPkts: 5
    OutBcastPkts: 5
    InOctets: 94544
    OutOctets: 31942
    InMcastOctets: 16669
    OutMcastOctets: 4932
    InBcastOctets: 353
    OutBcastOctets: 353
    InNoECTPkts: 534
```

netstat -i

```
sameed@sameed:~$ netstat -i
Kernel Interface table
Iface      MTU    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
ens33     1500      763      0      0 0           211      0      0      0 BMRU
lo       65536      227      0      0 0           227      0      0      0 LRU
```

Question 5

```
sameed@sameed:~$ sudo tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ens33, link-type EN10MB (Ethernet), capture size 262144 bytes
17:13:38.407670 ARP, Request who-has _gateway tell 192.168.159.1, length 46
17:13:38.409727 IP sameed.60010 > _gateway.domain: 1127+ [1au] PTR? 2.159.168.192.in-addr.arpa. (55)
17:13:38.418860 IP _gateway.domain > sameed.60010: 1127 NXDomain 0/0/1 (55)
17:13:38.418232 IP sameed.60010 > _gateway.domain: 1127+ PTR? 2.159.168.192.in-addr.arpa. (44)
17:13:38.424238 IP _gateway.domain > sameed.60010: 1127 NXDomain 0/0/0 (44)
17:13:38.424800 IP sameed.40949 > _gateway.domain: 35535+ [1au] PTR? 1.159.168.192.in-addr.arpa. (55)
17:13:38.431362 IP _gateway.domain > sameed.40949: 35535 NXDomain 0/0/1 (55)
17:13:38.431531 IP sameed.40949 > _gateway.domain: 35535+ PTR? 1.159.168.192.in-addr.arpa. (44)
17:13:38.438048 IP _gateway.domain > sameed.40949: 35535 NXDomain 0/0/0 (44)
17:13:38.439195 IP sameed.55520 > _gateway.domain: 18962+ [1au] PTR? 128.159.168.192.in-addr.arpa. (57)
17:13:38.446806 IP _gateway.domain > sameed.55520: 18962 NXDomain 0/0/1 (57)
17:13:38.446927 IP sameed.55520 > _gateway.domain: 18962+ PTR? 128.159.168.192.in-addr.arpa. (46)
17:13:38.453163 IP _gateway.domain > sameed.55520: 18962 NXDomain 0/0/0 (46)
17:13:38.932284 ARP, Request who-has _gateway tell 192.168.159.1, length 46
17:13:39.942878 ARP, Request who-has _gateway tell 192.168.159.1, length 46
17:13:40.954177 ARP, Request who-has _gateway tell 192.168.159.1, length 46
17:13:41.552575 ARP, Request who-has _gateway tell sameed, length 28
17:13:41.552889 ARP, Reply _gateway is-at 00:50:56:fd:ad:f9 (oui Unknown), length 46
17:13:41.935262 ARP, Request who-has _gateway tell 192.168.159.1, length 46
17:13:42.931479 ARP, Request who-has _gateway tell 192.168.159.1, length 46
17:13:43.975290 ARP, Request who-has _gateway tell 192.168.159.1, length 46
^C
21 packets captured
21 packets received by filter
0 packets dropped by kernel
```

Question 6

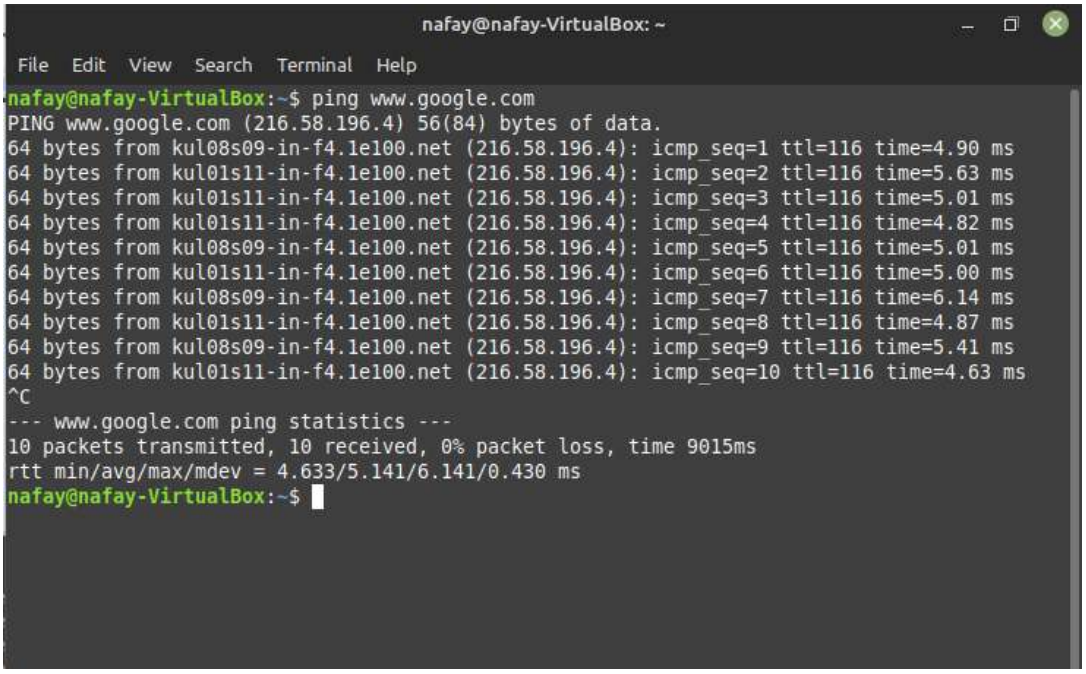
```
sameed@sameed:~$ sudo nmap -sP scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-10 17:18 +08
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.00053s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Nmap done: 1 IP address (1 host up) scanned in 1.10 seconds
sameed@sameed:~$ sudo nmap -sS scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-10 17:19 +08
Stats: 0:00:46 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 84.87% done; ETC: 17:20 (0:00:08 remaining)
Stats: 0:00:52 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 85.13% done; ETC: 17:20 (0:00:09 remaining)
Stats: 0:01:18 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 89.53% done; ETC: 17:20 (0:00:09 remaining)
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (3.0s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 994 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
25/tcp    filtered smtp
80/tcp    open     http
514/tcp   filtered shell
9929/tcp  open     nping-echo
31337/tcp open     Elite

Nmap done: 1 IP address (1 host up) scanned in 127.98 seconds
sameed@sameed:~$ sudo nmap -sT scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-10 17:21 +08
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.00081s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
All 1000 scanned ports on scanme.nmap.org (45.33.32.156) are filtered

Nmap done: 1 IP address (1 host up) scanned in 21.62 seconds
sameed@sameed:~$
```

```
sameed@sameed:~$ sudo nmap -sV -O scanme.nmap.org
[sudo] password for sameed:
Sorry, try again.
[sudo] password for sameed:
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-12 00:29 +08
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.019s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 997 filtered ports
PORT   STATE SERVICE    VERSION
21/tcp open  tcpwrapped
22/tcp open  tcpwrapped
80/tcp open  tcpwrapped
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: specialized|WAP|phone
Running: iPXE 1.X, Linux 2.4.X|2.6.X, Sony Ericsson embedded
OS CPE: cpe:/o:ipxe:ipxe:1.0.0%2b cpe:/o:linux:linux_kernel:2.4.20 cpe:/o:linux:linux_kernel:2.6.22 cpe:/h:sonyericsson:u8i_vivaz
OS details: iPXE 1.0.0+, Tomato 1.28 (Linux 2.4.20), Tomato firmware (Linux 2.6.22), Sony Ericsson U8i Vivaz mobile phone

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 54.88 seconds
sameed@sameed:~$ sudo nmap -A scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-12 00:32 +08
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.0022s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 997 filtered ports
PORT   STATE SERVICE    VERSION
21/tcp open  tcpwrapped
22/tcp open  ssh        OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80/tcp open  http       Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Go ahead and ScanMe!
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 2.4.X|3.X, Microsoft Windows XP|7|2012
OS CPE: cpe:/o:linux:linux_kernel:2.4.37 cpe:/o:linux:linux_kernel:3.2 cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2012
OS details: DD-WRT v24-sp2 (Linux 2.4.37), Linux 3.2, Microsoft Windows XP SP3, Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   0.12 ms _gateway (192.168.204.2)
2   0.16 ms scanme.nmap.org (45.33.32.156)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 181.63 seconds
```

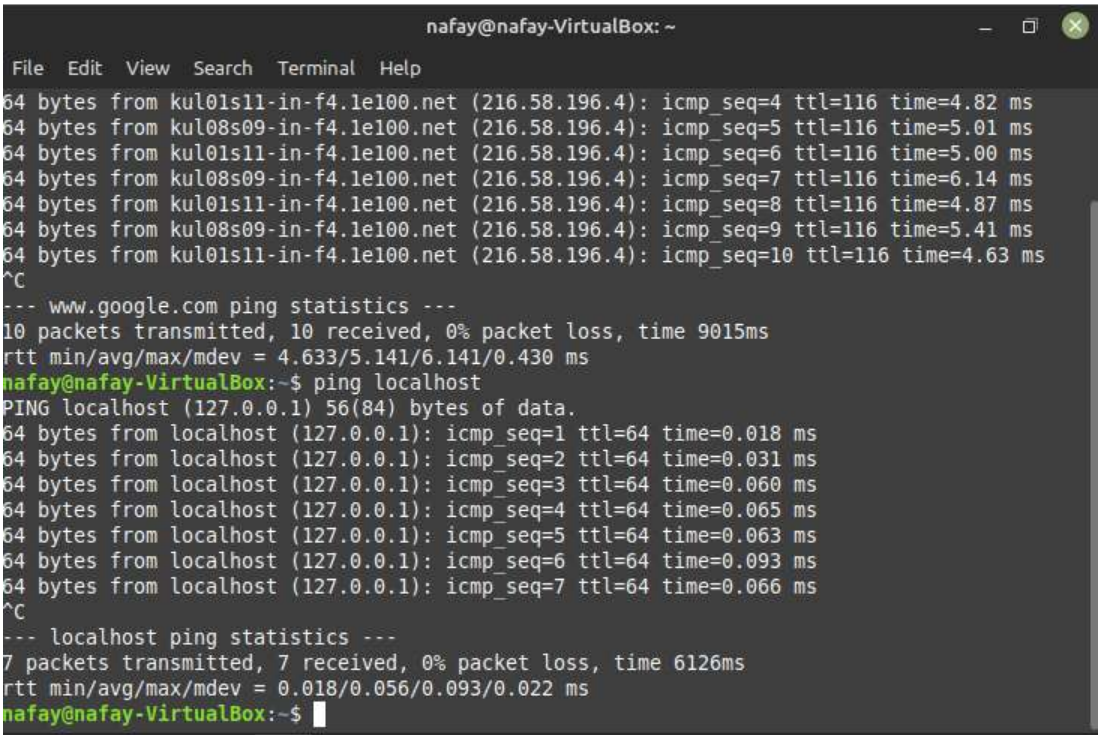
1.4 Muhammad Nafay

Question 1

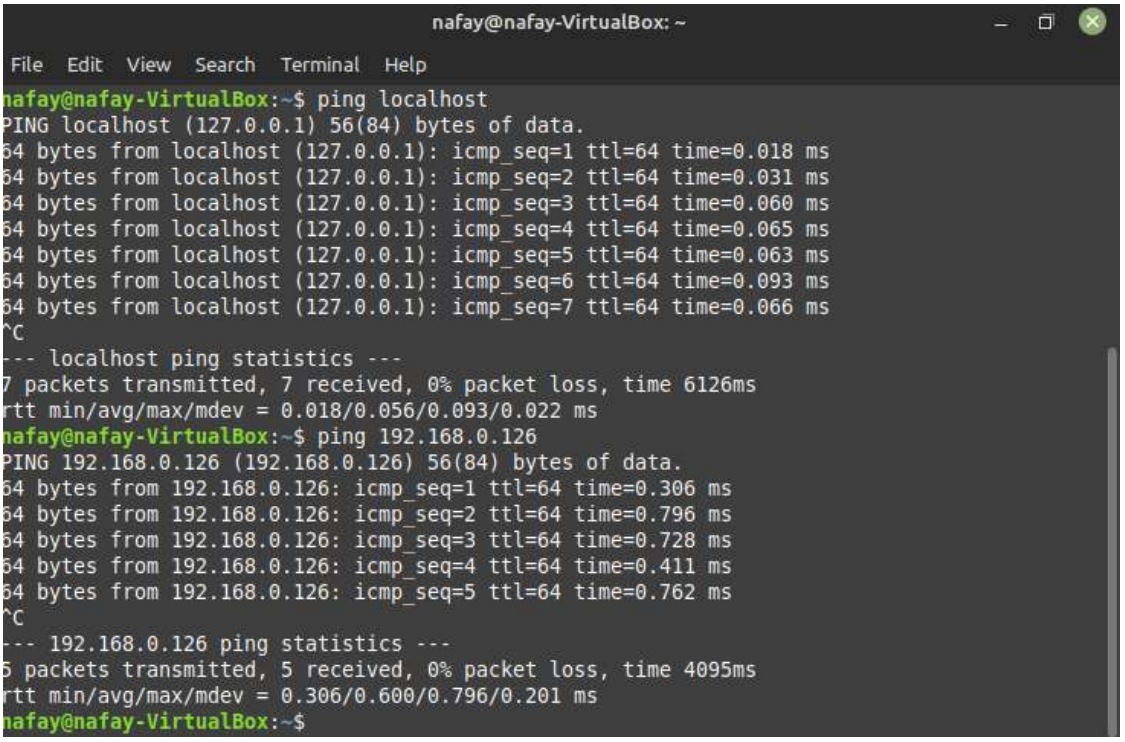
ping<website>



ping<localhost>

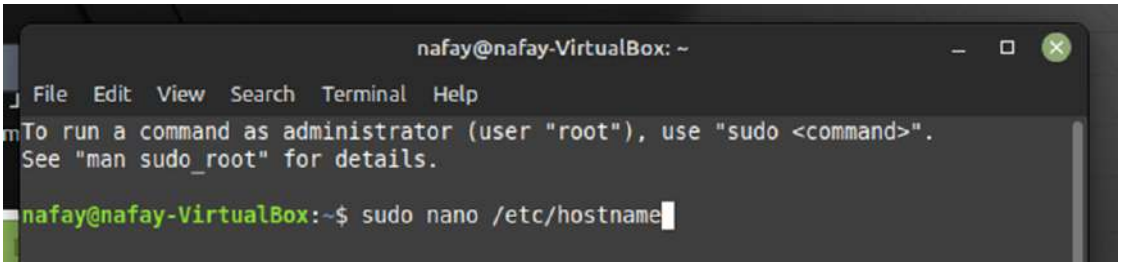


ping<other-ip-in-network>

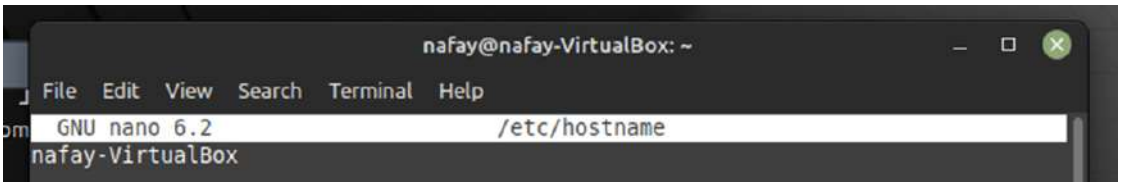


Question 2

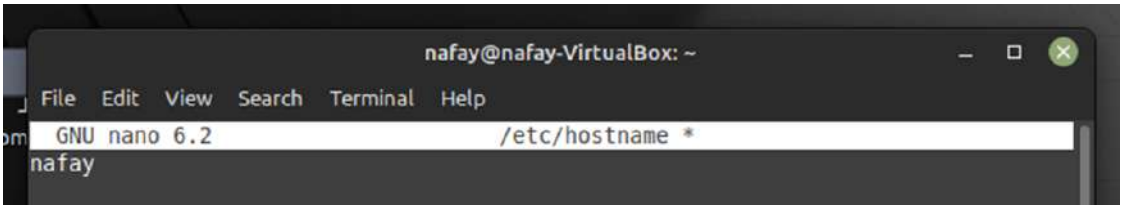
sudo nano /etc/hostname



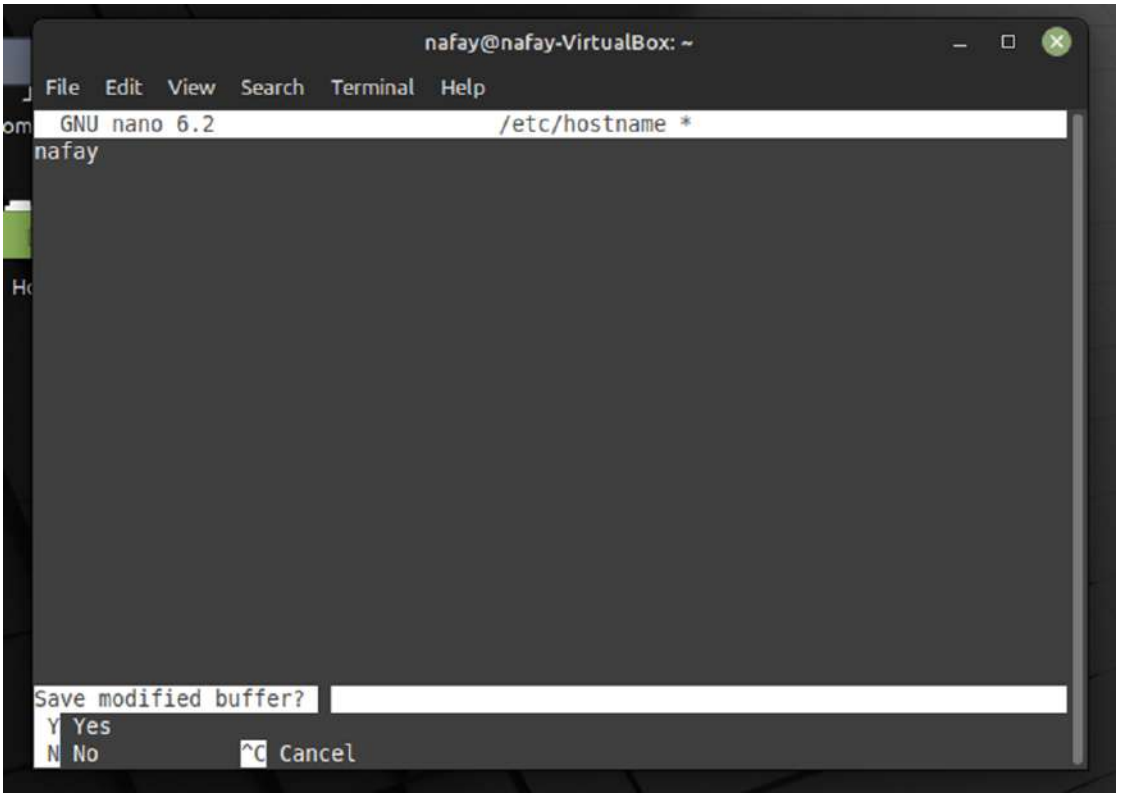
Initial name is nafay-VirtualBox.



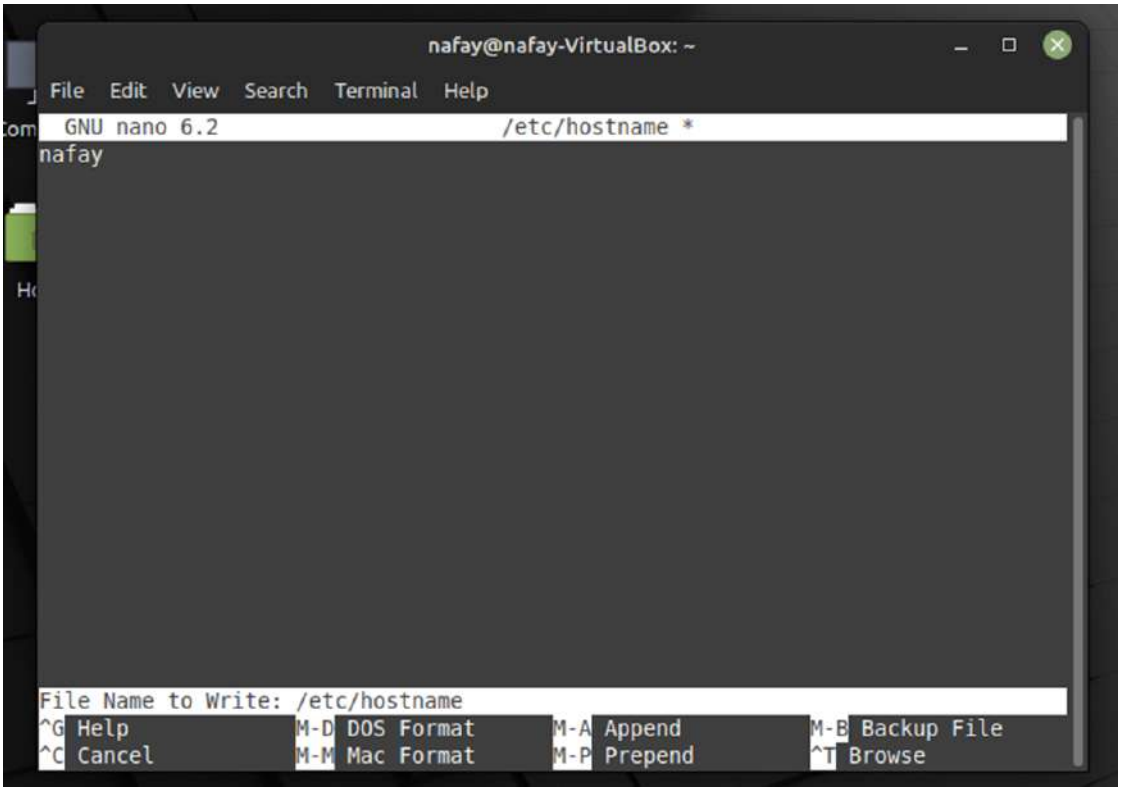
Change nafay-VirtualBox to nafay.



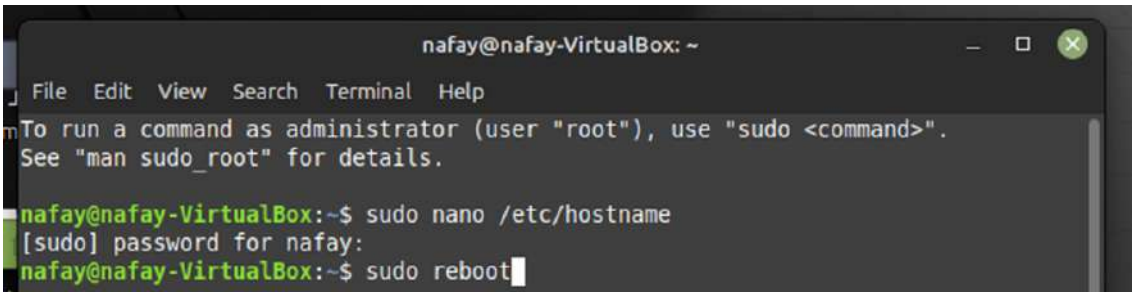
Press ctrl + x, then key in “y” to save the change.



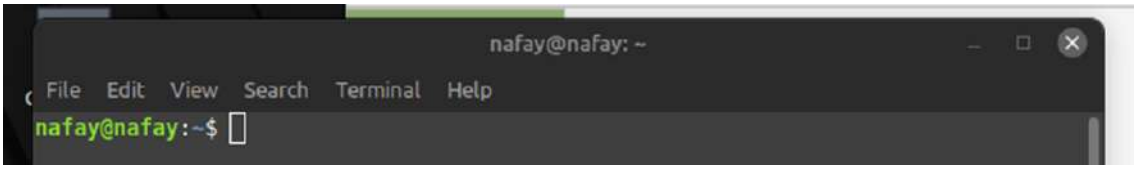
The path to save will be displayed, so press enter.



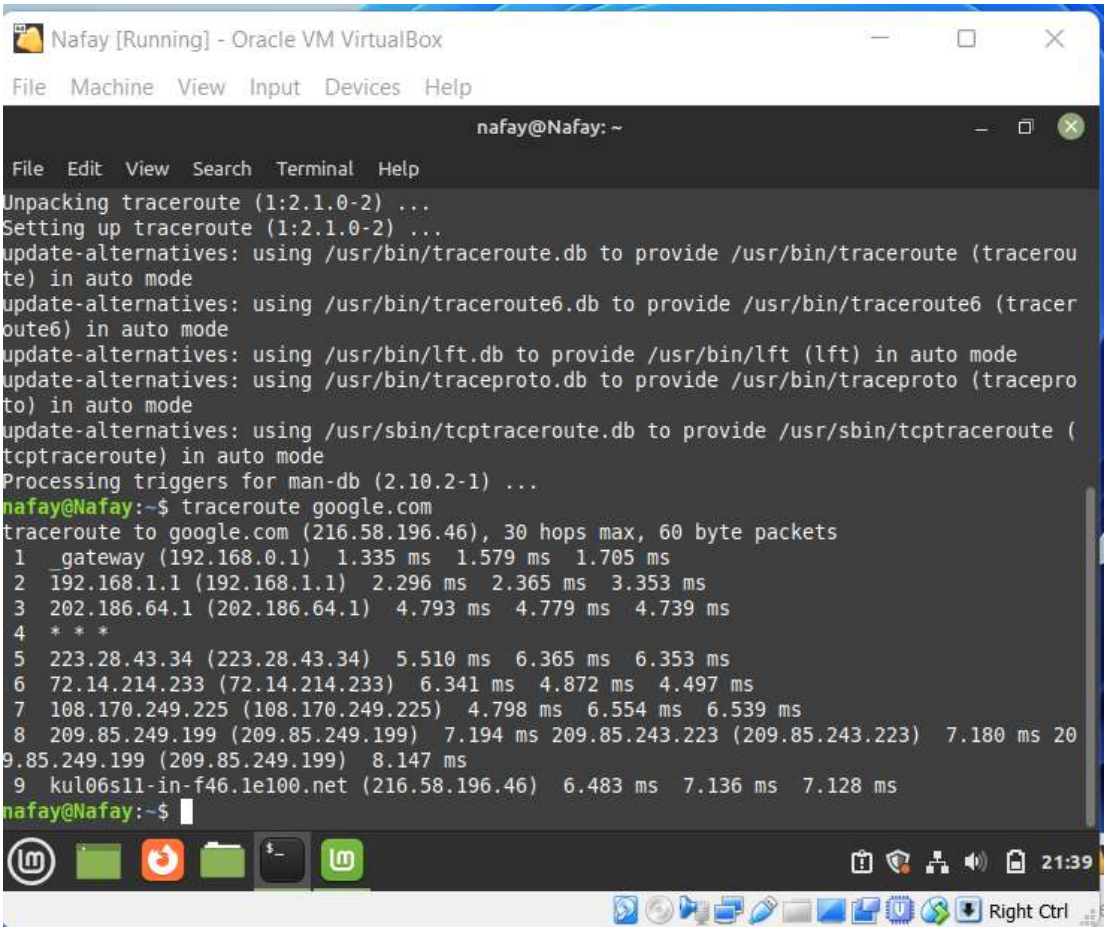
Then execute the “sudo reboot” command to reboot the linux system.



After reboot is finished, the hostname is already changed.



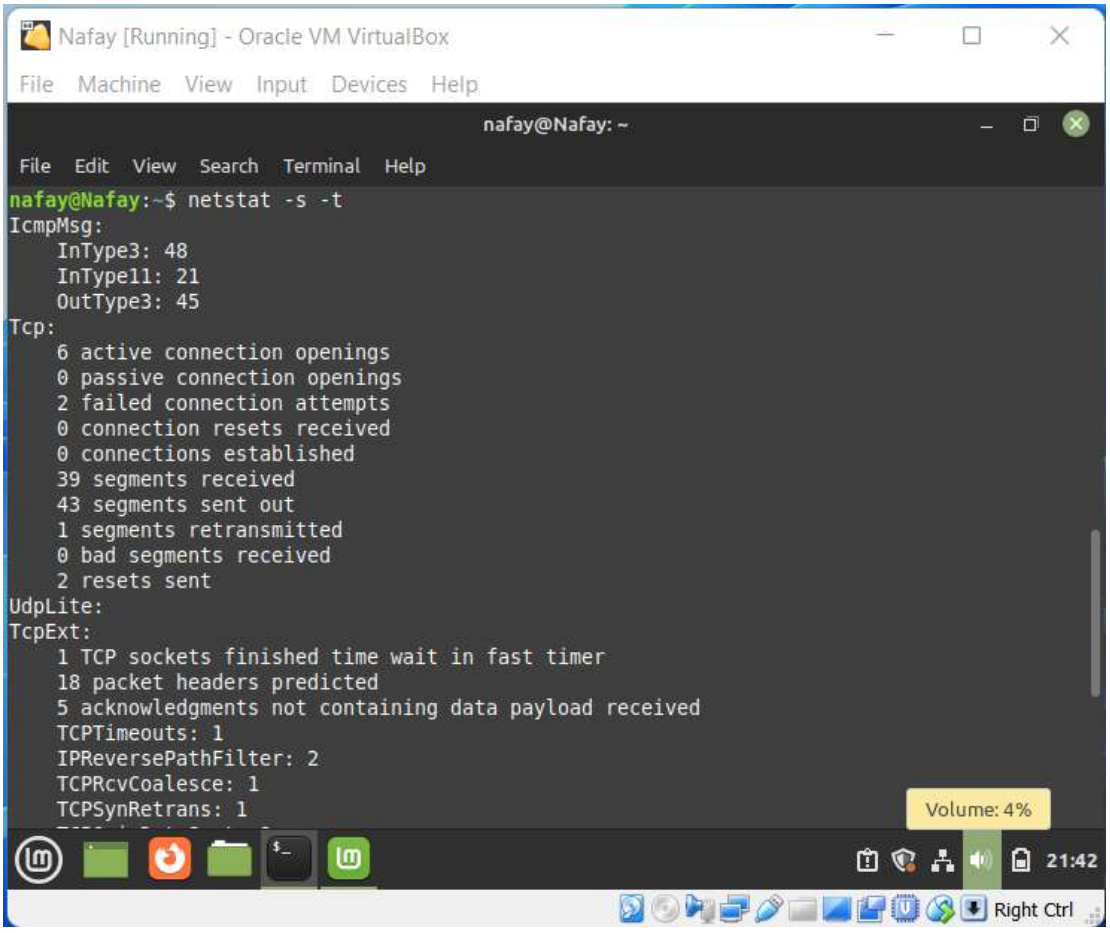
Question 3
traceroute

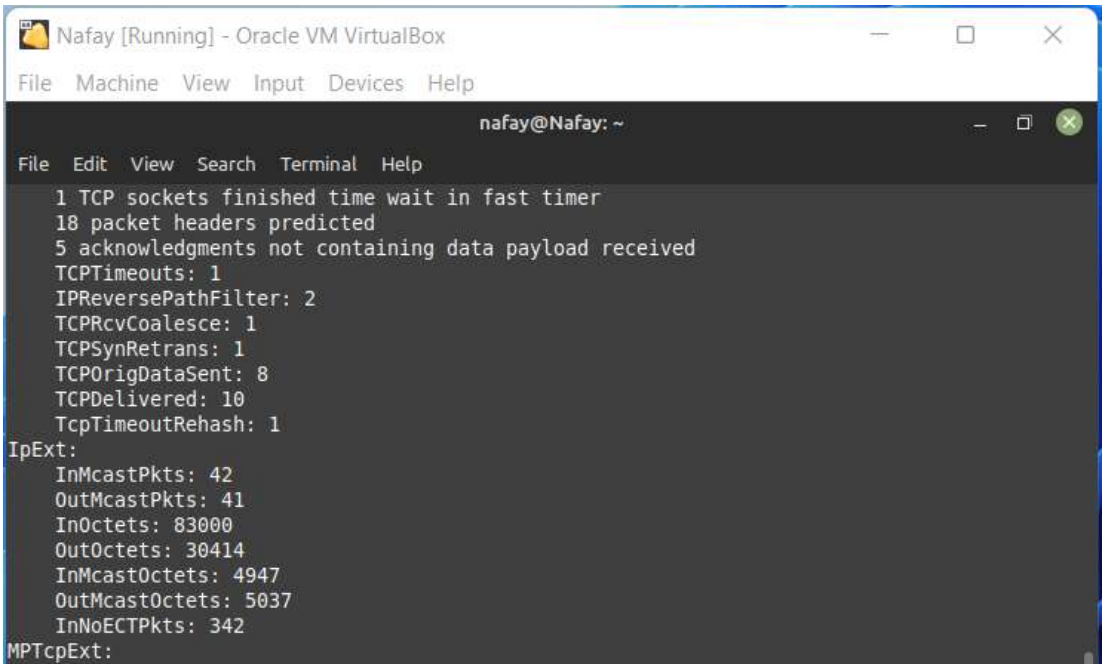


Question 4
netstat -t

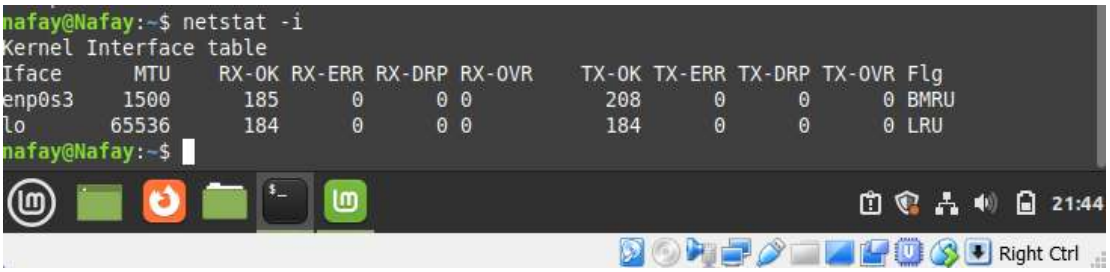

Nafay [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
nafay@Nafay: ~
File Edit View Search Terminal Help
nafay@Nafay:~$ netstat -t
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address Foreign Address State

netstat -s -t


Nafay [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
nafay@Nafay: ~
File Edit View Search Terminal Help
nafay@Nafay:~$ netstat -s -t
IcmpMsg:
InType3: 48
InType11: 21
OutType3: 45
Tcp:
6 active connection openings
0 passive connection openings
2 failed connection attempts
0 connection resets received
0 connections established
39 segments received
43 segments sent out
1 segments retransmitted
0 bad segments received
2 resets sent
UdpLite:
TcpExt:
1 TCP sockets finished time wait in fast timer
18 packet headers predicted
5 acknowledgments not containing data payload received
TCPTimeouts: 1
IPReversePathFilter: 2
TCPRcvCoalesce: 1
TCPSynRetrans: 1
Volume: 4%
21:42
Right Ctrl

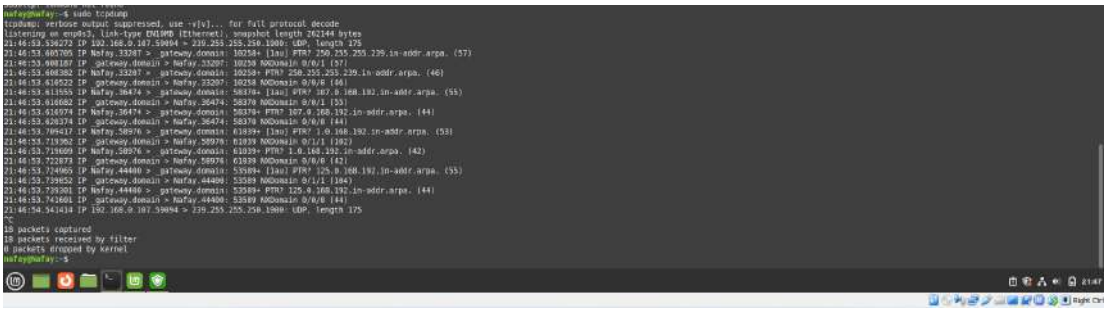


netstat -i



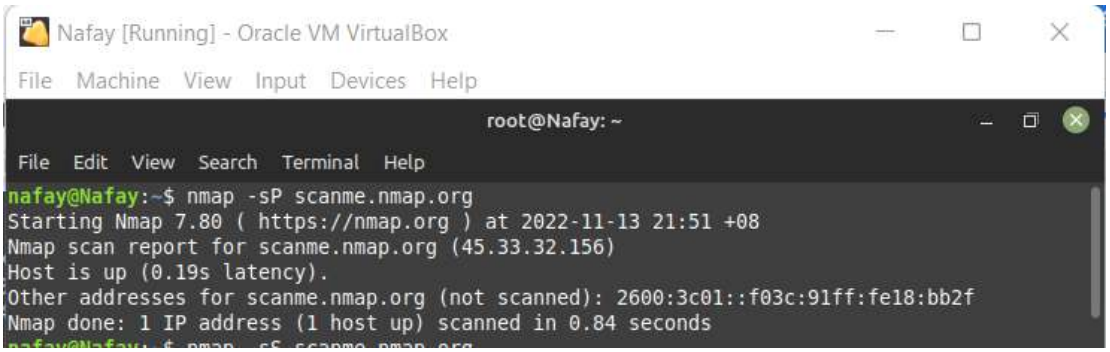
Question 5

Sudo tcpdump



Question 6

nmap -sP <ip address>



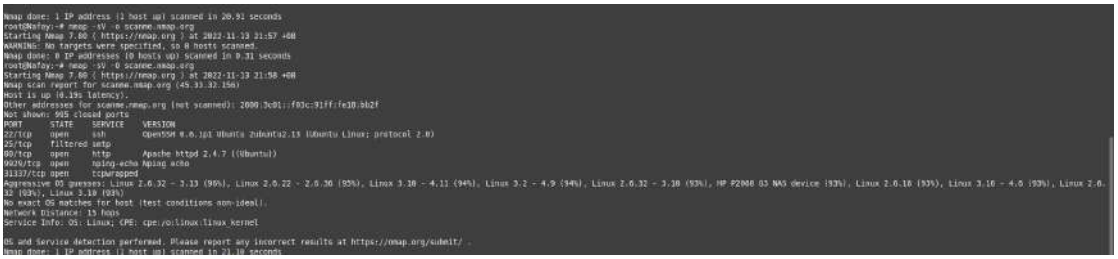
nmap -sS <ip address>

```
nafay@Nafay:~$ sudo su -
root@Nafay:~# nmap -sS scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-13 21:56 +08
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.19s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 995 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
25/tcp    filtered smtp
80/tcp    open     http
9929/tcp  open     nping-echo
31337/tcp open     Elite
```

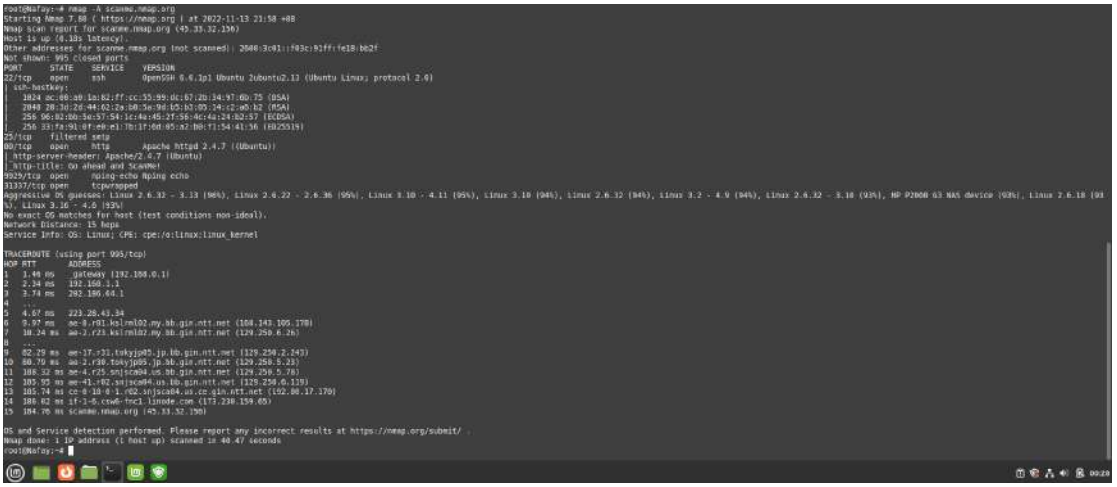
nmap -sT <ip address>

```
Nmap done: 1 IP address (1 host up) scanned in 5.85 seconds
root@Nafay:~# nmap -sT scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-13 21:56 +08
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.18s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 995 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
25/tcp    filtered smtp
80/tcp    open     http
9929/tcp  open     nping-echo
31337/tcp open     Elite
```

nmap -sV -O <ip address>

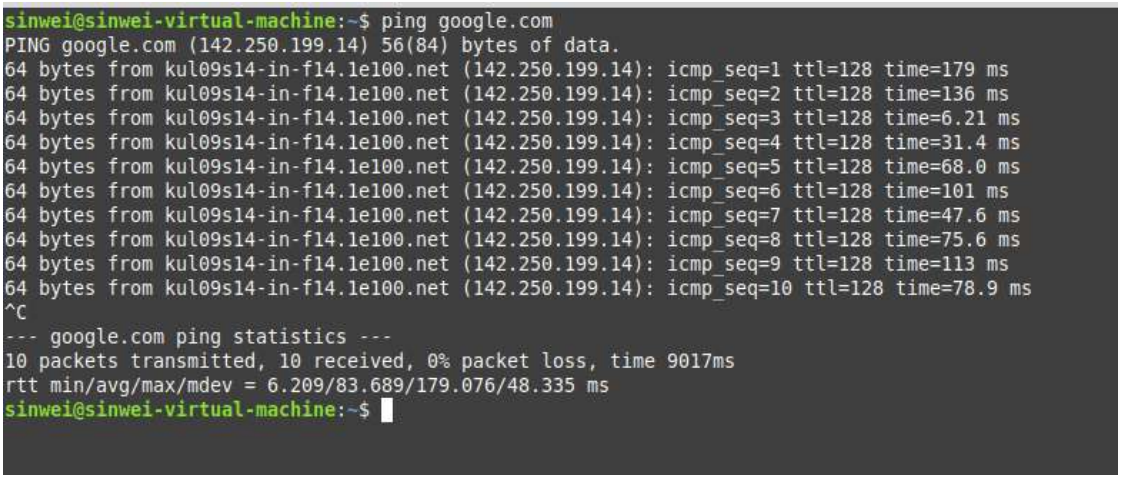


nmap -A <ip address>

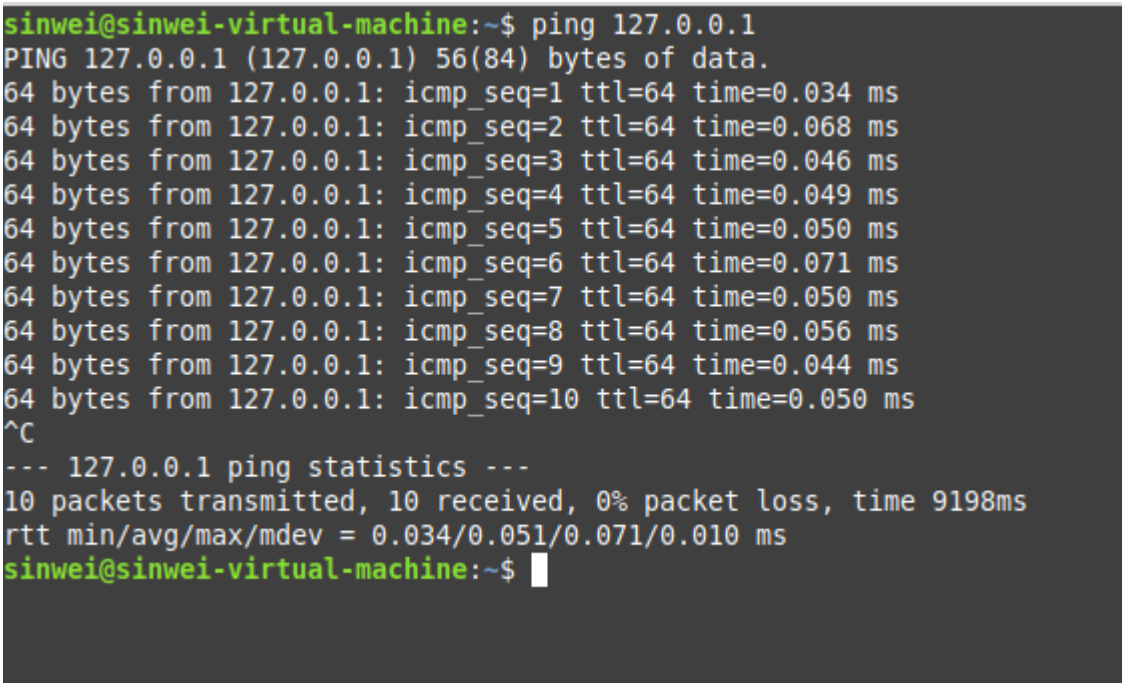


1.5 Thua Sin Wei

Question 1
ping<website>



ping<localhost>



ping<other-ip-in-network>

```
sinwei@sinwei-virtual-machine:~$ ping 192.168.190.132
PING 192.168.190.132 (192.168.190.132) 56(84) bytes of data.
64 bytes from 192.168.190.132: icmp_seq=1 ttl=64 time=1.24 ms
64 bytes from 192.168.190.132: icmp_seq=2 ttl=64 time=0.499 ms
64 bytes from 192.168.190.132: icmp_seq=3 ttl=64 time=0.716 ms
64 bytes from 192.168.190.132: icmp_seq=4 ttl=64 time=0.540 ms
64 bytes from 192.168.190.132: icmp_seq=5 ttl=64 time=0.570 ms
64 bytes from 192.168.190.132: icmp_seq=6 ttl=64 time=0.596 ms
64 bytes from 192.168.190.132: icmp_seq=7 ttl=64 time=0.631 ms
64 bytes from 192.168.190.132: icmp_seq=8 ttl=64 time=0.582 ms
64 bytes from 192.168.190.132: icmp_seq=9 ttl=64 time=0.598 ms
64 bytes from 192.168.190.132: icmp_seq=10 ttl=64 time=0.652 ms
^C
--- 192.168.190.132 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9177ms
rtt min/avg/max/mdev = 0.499/0.662/1.242/0.201 ms
sinwei@sinwei-virtual-machine:~$
```

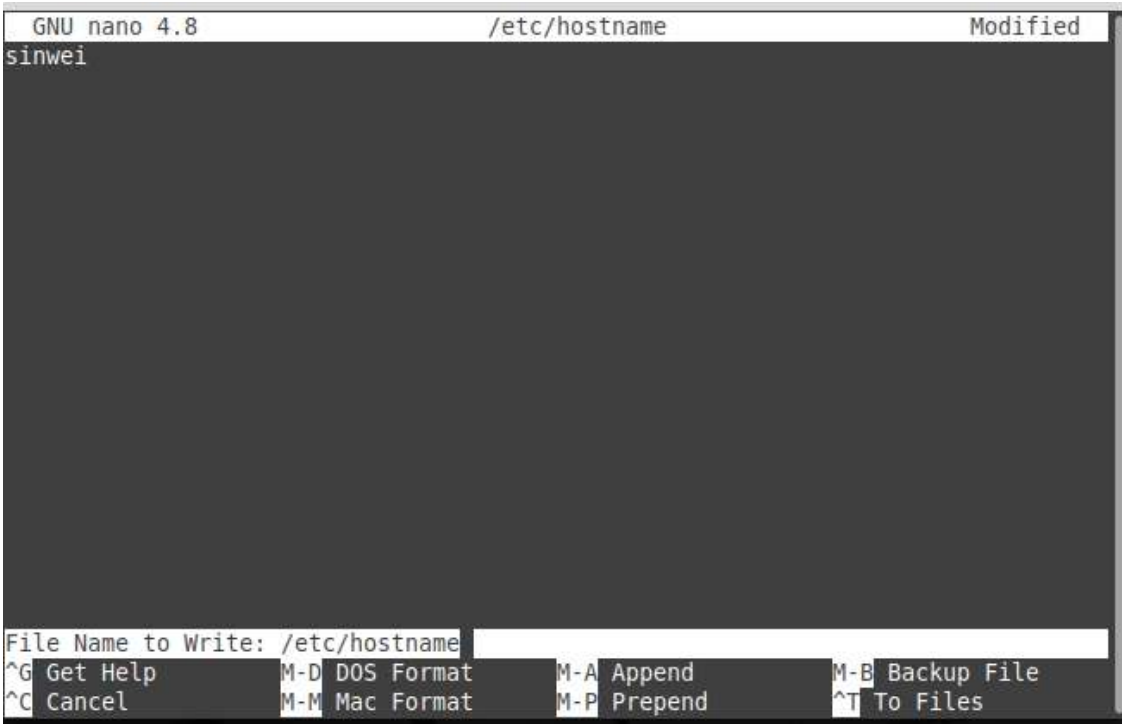
Question 2

sudo nano /etc/hostname

```
  GNU nano 4.8                    /etc/hostname
sinwei-virtual-machine


                          [ Read 1 line ]
^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos
^X Exit      ^R Read File ^\ Replace   ^U Paste Text^T To Spell  ^_ Go To Line
```

change sinwei-virtual-machine to sinwei.

ctrl + x, “Save modified buffer?” => Y (yes)



Execute with the command “sudo reboot” to reboot the system to apply the change made on the host name file.

After reboot, open the terminal and check the hostname.

```
sinwei@sinwei:~$ hostname
sinwei
sinwei@sinwei:~$
```

Question 3

```
sinwei@sinwei:~$ traceroute 192.168.190.128
traceroute to 192.168.190.128 (192.168.190.128), 30 hops max, 60 byte packets
 1  sinwei (192.168.190.128)  0.018 ms  0.002 ms  0.002 ms
sinwei@sinwei:~$
```

Question 4

netstat -t

```
sinwei@sinwei:~$ netstat -t
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
```

netstat -s -t

```
sinwei@sinwei:~$ netstat -s -t
Tcp:
    5 active connection openings
    0 passive connection openings
    2 failed connection attempts
    0 connection resets received
    0 connections established
    16 segments received
    16 segments sent out
    0 segments retransmitted
    0 bad segments received
    2 resets sent
UdpLite:
TcpExt:
    0 packet headers predicted
    3 acknowledgments not containing data payload received
    3 predicted acknowledgments
    TCPOrigDataSent: 6
    TCPDelivered: 9
IpExt:
    InMcastPkts: 46
    OutMcastPkts: 40
    InBcastPkts: 5
    OutBcastPkts: 5
    InOctets: 25008
    OutOctets: 20577
    InMcastOctets: 5160
    OutMcastOctets: 4592
    InBcastOctets: 353
    OutBcastOctets: 353
    InNoECTPkts: 245
sinwei@sinwei:~$
```

netstat -i

```
sinwei@sinwei:~$ netstat -i
Kernel Interface table
Iface      MTU    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
ens33     1500      184      0      0 0           128      0      0      0 BMRU
lo       65536      158      0      0 0           158      0      0      0 LRU
sinwei@sinwei:~$
```

Question 5

```
sinwei@sinwei:~$ sudo tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ens33, link-type EN10MB (Ethernet), capture size 262144 bytes
21:09:06.267649 ARP, Request who-has _gateway tell sinwei, length 28
21:09:06.267966 ARP, Reply _gateway is-at 00:50:56:e9:82:ca (oui Unknown), length 46
21:09:06.268997 IP sinwei.33731 > _gateway.domain: 14981+ [1au] PTR? 2.190.168.192.in-addr.arpa. (55)
21:09:06.493201 IP _gateway.domain > sinwei.33731: 14981 NXDomain 0/1/1 (132)
21:09:06.493511 IP sinwei.33731 > _gateway.domain: 14981+ PTR? 2.190.168.192.in-addr.arpa. (44)
21:09:06.684588 IP _gateway.domain > sinwei.33731: 14981 NXDomain 0/1/0 (121)
21:09:06.685625 IP sinwei.56954 > _gateway.domain: 4720+ [1au] PTR? 128.190.168.192.in-addr.arpa. (57)
21:09:07.199164 IP _gateway.domain > sinwei.56954: 4720 NXDomain 0/1/1 (134)
21:09:07.199513 IP sinwei.56954 > _gateway.domain: 4720+ PTR? 128.190.168.192.in-addr.arpa. (46)
21:09:07.402945 IP _gateway.domain > sinwei.56954: 4720 NXDomain 0/1/0 (123)
21:09:18.928280 IP 192.168.190.1.56324 > 239.255.255.250.1900: UDP, length 175
21:09:18.929181 IP sinwei.33379 > _gateway.domain: 48773+ [1au] PTR? 250.255.255.239.in-addr.arpa. (57)
21:09:18.935915 IP 192.168.190.1.56329 > 239.255.255.250.1900: UDP, length 175
21:09:19.018875 IP _gateway.domain > sinwei.33379: 48773 NXDomain 0/1/1 (114)
21:09:19.019213 IP sinwei.33379 > _gateway.domain: 48773+ PTR? 250.255.255.239.in-addr.arpa. (46)
21:09:19.054822 IP _gateway.domain > sinwei.33379: 48773 NXDomain 0/1/0 (103)
21:09:19.056259 IP sinwei.43177 > _gateway.domain: 22529+ [1au] PTR? 1.190.168.192.in-addr.arpa. (55)
21:09:19.226389 IP _gateway.domain > sinwei.43177: 22529 NXDomain 0/1/1 (132)
21:09:19.226583 IP sinwei.43177 > _gateway.domain: 22529+ PTR? 1.190.168.192.in-addr.arpa. (44)
21:09:19.429270 IP _gateway.domain > sinwei.43177: 22529 NXDomain 0/1/0 (121)
21:09:19.930720 IP 192.168.190.1.56324 > 239.255.255.250.1900: UDP, length 175
21:09:19.938168 IP 192.168.190.1.56329 > 239.255.255.250.1900: UDP, length 175
21:09:20.938324 IP 192.168.190.1.56324 > 239.255.255.250.1900: UDP, length 175
21:09:20.945724 IP 192.168.190.1.56329 > 239.255.255.250.1900: UDP, length 175
21:09:21.947134 IP 192.168.190.1.56324 > 239.255.255.250.1900: UDP, length 175
21:09:21.953569 IP 192.168.190.1.56329 > 239.255.255.250.1900: UDP, length 175
21:09:24.503983 IP 192.168.190.1.mdns > 224.0.0.251.mdns: 0 PTR (QM)? _sleep-proxy._udp.local. (41)
21:09:24.504688 IP sinwei.45451 > _gateway.domain: 50229+ [1au] PTR? 251.0.0.224.in-addr.arpa. (53)
21:09:24.517252 IP _gateway.domain > sinwei.45451: 50229 NXDomain 0/1/1 (110)
21:09:24.517652 IP sinwei.45451 > _gateway.domain: 50229+ PTR? 251.0.0.224.in-addr.arpa. (42)
21:09:24.548874 IP _gateway.domain > sinwei.45451: 50229 NXDomain 0/1/0 (99)
21:09:42.910729 IP 192.168.190.1.mdns > 224.0.0.251.mdns: 0 A (QM)? wpad.local. (28)
21:09:42.911393 IP6 fe80::956b:9e37:bcec:b35.mdns > ff02::fb.mdns: 0 A (QM)? wpad.local. (28)
21:09:42.911899 IP sinwei.34667 > _gateway.domain: 18166+ [1au] PTR? b.f.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.
0.0.0.0.2.0.f.f.ip6.arpa. (101)
21:09:42.913201 IP 192.168.190.1.mdns > 224.0.0.251.mdns: 0 A (QM)? wpad.local. (28)
21:09:42.913649 IP6 fe80::956b:9e37:bcec:b35.mdns > ff02::fb.mdns: 0 A (QM)? wpad.local. (28)
21:09:42.915097 IP6 fe80::956b:9e37:bcec:b35.51356 > ff02::1:3.hostmon: UDP, length 22
21:09:42.915316 IP 192.168.190.1.51356 > 224.0.0.252.hostmon: UDP, length 22
21:09:42.965897 IP _gateway.domain > sinwei.34667: 18166 NXDomain 0/1/1 (165)
21:09:42.966202 IP sinwei.34667 > _gateway.domain: 18166+ PTR? b.f.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.
0.2.0.f.f.ip6.arpa. (90)
21:09:43.009844 IP _gateway.domain > sinwei.34667: 18166 NXDomain 0/1/0 (154)
21:09:43.010865 IP sinwei.54047 > _gateway.domain: 63779+ [1au] PTR? 5.3.b.0.c.e.c.b.7.3.e.9.b.6.5.9.0.0.0.0.0.0.0.0.
0.0.0.0.0.8.e.f.ip6.arpa. (101)
21:09:43.016716 IP _gateway.domain > sinwei.54047: 63779 NXDomain 0/1/1 (165)
21:09:43.016913 IP sinwei.54047 > _gateway.domain: 63779+ PTR? 5.3.b.0.c.e.c.b.7.3.e.9.b.6.5.9.0.0.0.0.0.0.0.0.0.0.
0.0.8.e.f.ip6.arpa. (90)
21:09:43.026875 IP _gateway.domain > sinwei.54047: 63779 NXDomain 0/1/0 (154)
21:09:43.027917 IP sinwei.57416 > _gateway.domain: 52321+ [1au] PTR? 3.0.0.0.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.
```

```
0.0.0.0.2.0.f.f.ip6.arpa. (101)
21:09:43.052004 IP _gateway.domain > sinwei.57416: 52321 NXDomain 0/1/1 (165)
21:09:43.052324 IP sinwei.57416 > _gateway.domain: 52321+ PTR? 3.0.0.0.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.
0.2.0.f.f.ip6.arpa. (90)
21:09:43.088343 IP _gateway.domain > sinwei.57416: 52321 NXDomain 0/1/0 (154)
21:09:43.089143 IP sinwei.60350 > _gateway.domain: 65084+ [1au] PTR? 252.0.0.224.in-addr.arpa. (53)
21:09:43.325842 IP6 fe80::956b:9e37:bcec:b35.51356 > ff02::1:3.hostmon: UDP, length 22
21:09:43.325858 IP 192.168.190.1.51356 > 224.0.0.252.hostmon: UDP, length 22
21:09:43.362727 ARP, Request who-has _gateway tell 192.168.190.1, length 46
21:09:43.870862 IP _gateway.domain > sinwei.60350: 65084 NXDomain 0/1/1 (110)
21:09:43.871104 IP sinwei.60350 > _gateway.domain: 65084+ PTR? 252.0.0.224.in-addr.arpa. (42)
21:09:43.910302 IP 192.168.190.1.mdns > 224.0.0.251.mdns: 0 A (QM)? wpad.local. (28)
21:09:43.910915 IP6 fe80::956b:9e37:bcec:b35.mdns > ff02::fb.mdns: 0 A (QM)? wpad.local. (28)
21:09:43.913128 IP 192.168.190.1.mdns > 224.0.0.251.mdns: 0 A (QM)? wpad.local. (28)
21:09:43.913918 IP6 fe80::956b:9e37:bcec:b35.mdns > ff02::fb.mdns: 0 A (QM)? wpad.local. (28)
21:09:44.090014 IP _gateway.domain > sinwei.60350: 65084 NXDomain 0/1/0 (99)
21:09:44.414676 ARP, Request who-has _gateway tell 192.168.190.1, length 46
21:09:45.362758 ARP, Request who-has _gateway tell 192.168.190.1, length 46
^C
62 packets captured
62 packets received by filter
0 packets dropped by kernel
sinwei@sinwei:~$
```

Question 6

nmap-sP<ipaddress>

```
sinwei@sinwei:~$ sudo nmap -sP 192.168.190.128
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-13 14:12 +08
Nmap scan report for sinwei (192.168.190.128)
Host is up.
Nmap done: 1 IP address (1 host up) scanned in 0.02 seconds
sinwei@sinwei:~$
```

nmap-sS<ipaddress>

```
sinwei@sinwei:~$ sudo nmap -sS 192.168.190.128
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-13 14:11 +08
Nmap scan report for sinwei (192.168.190.128)
Host is up (0.0000020s latency).
All 1000 scanned ports on sinwei (192.168.190.128) are closed

Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
sinwei@sinwei:~$
```

nmap-sT<ipaddress>

```
sinwei@sinwei:~$ sudo nmap -sT 192.168.190.128
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-13 14:13 +08
Nmap scan report for sinwei (192.168.190.128)
Host is up (0.000042s latency).
All 1000 scanned ports on sinwei (192.168.190.128) are closed

Nmap done: 1 IP address (1 host up) scanned in 0.05 seconds
sinwei@sinwei:~$
```

nmap-sV-O<ipaddress>

```
sinwei@sinwei:~$ sudo nmap -sV -O 192.168.190.128
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-13 14:14 +08
Nmap scan report for sinwei (192.168.190.128)
Host is up (0.000045s latency).
All 1000 scanned ports on sinwei (192.168.190.128) are closed
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS and Service detection performed. Please report any incorrect results at https
://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.06 seconds
sinwei@sinwei:~$
```

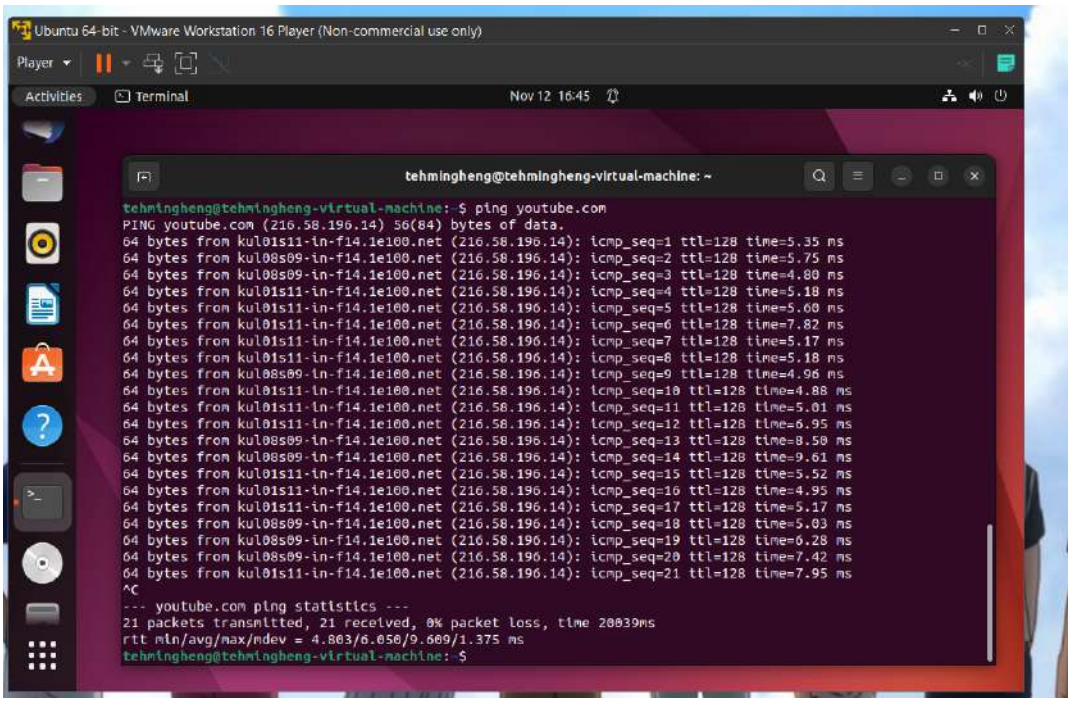
nmap-A<ipaddress>


sinwei@sinwei:~$ sudo nmap -A 192.168.190.128
Starting Nmap 7.80 (https://nmap.org) at 2022-11-13 14:15 +08
Nmap scan report for sinwei (192.168.190.128)
Host is up (0.000044s latency).
All 1000 scanned ports on sinwei (192.168.190.128) are closed
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops
OS and Service detection performed. Please report any incorrect results at https
://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.07 seconds
sinwei@sinwei:~$

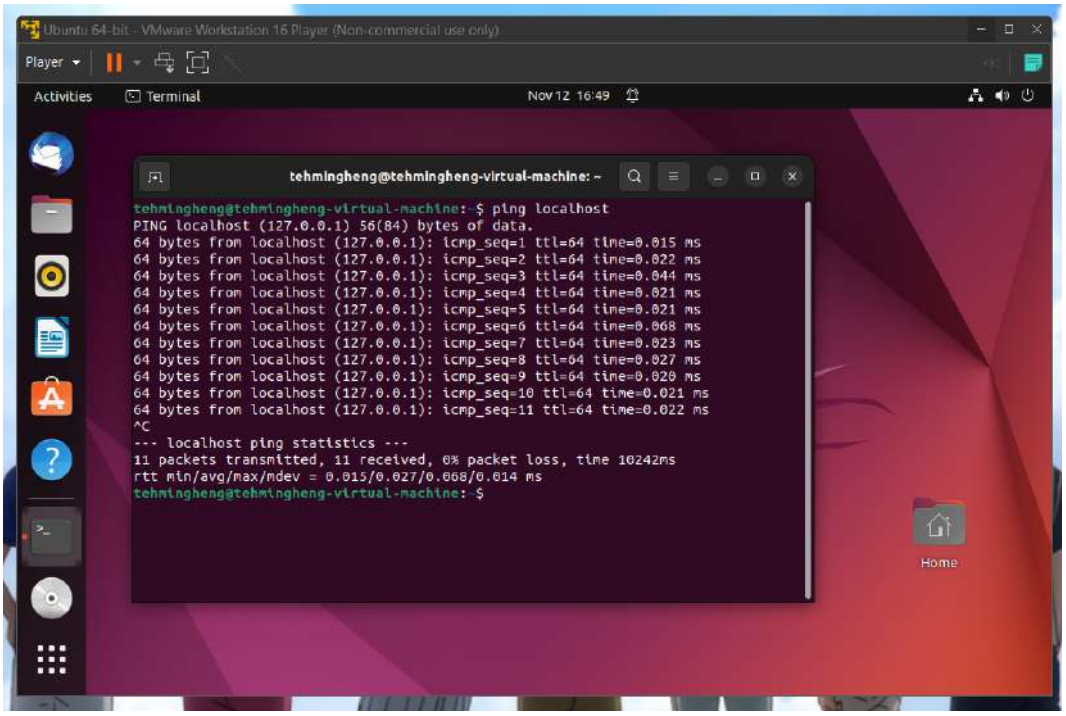
1.6 Teh Ming Heng

Question 1

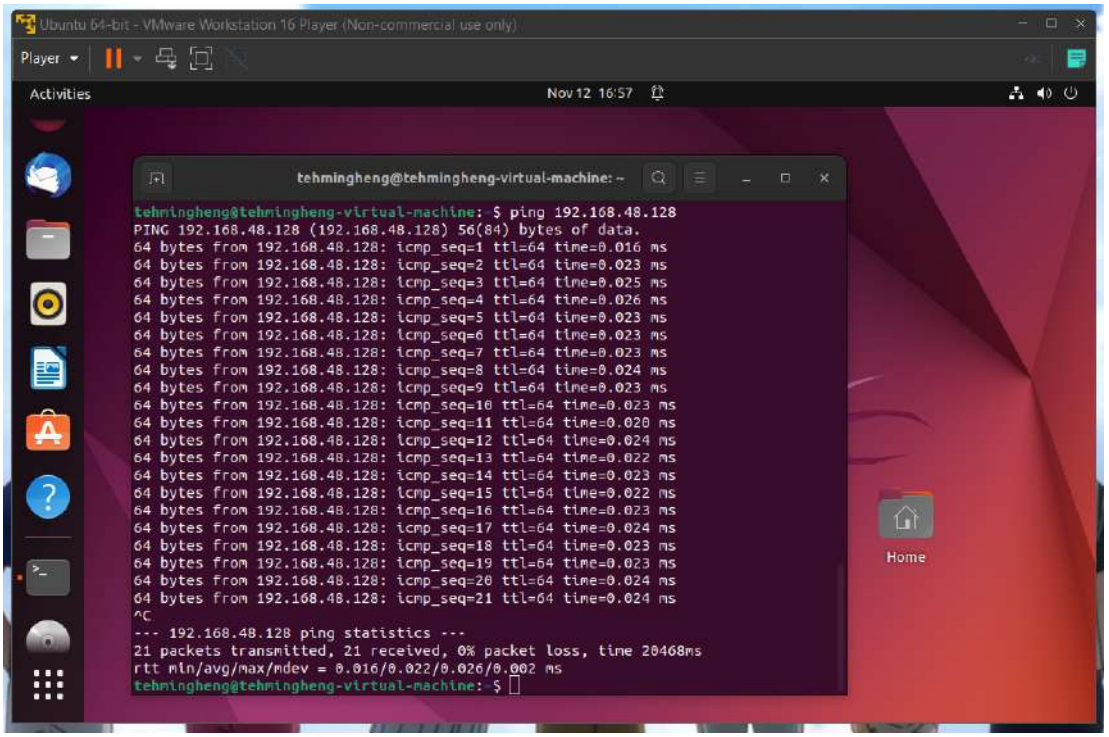
Ping <WebSite>



Ping <LocalHost>

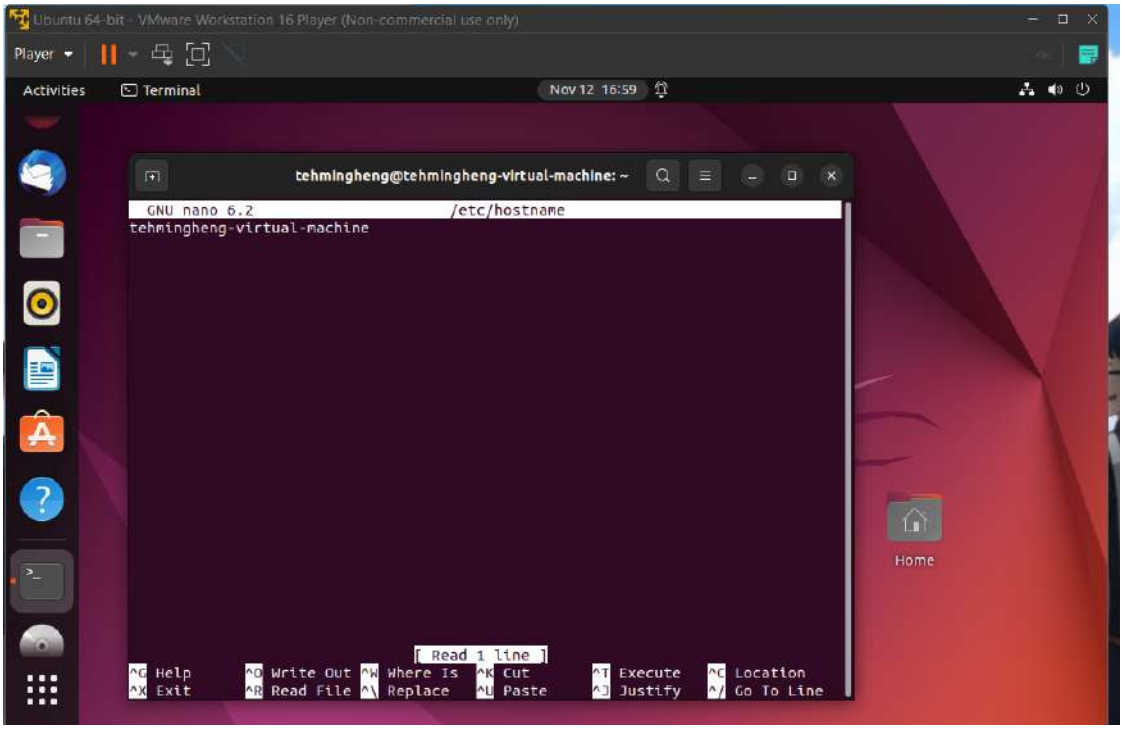


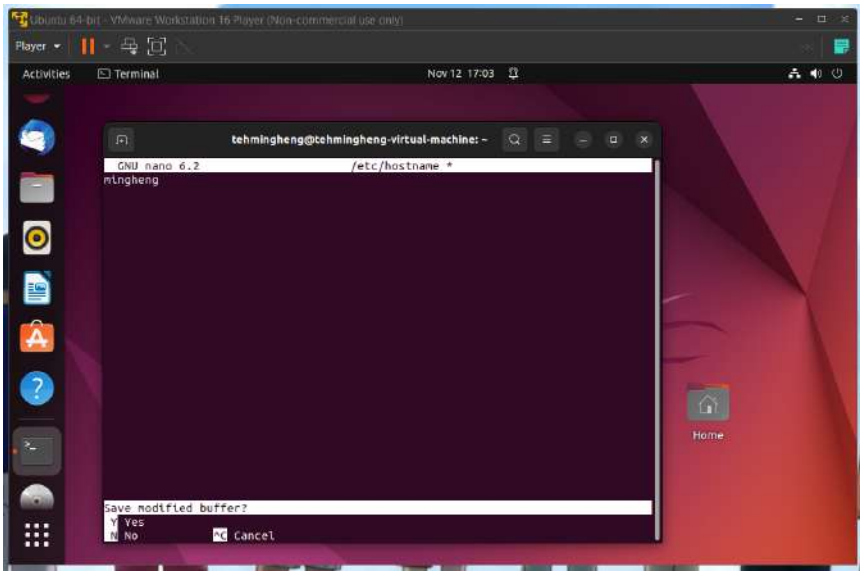
ping <other-ip-in-network>

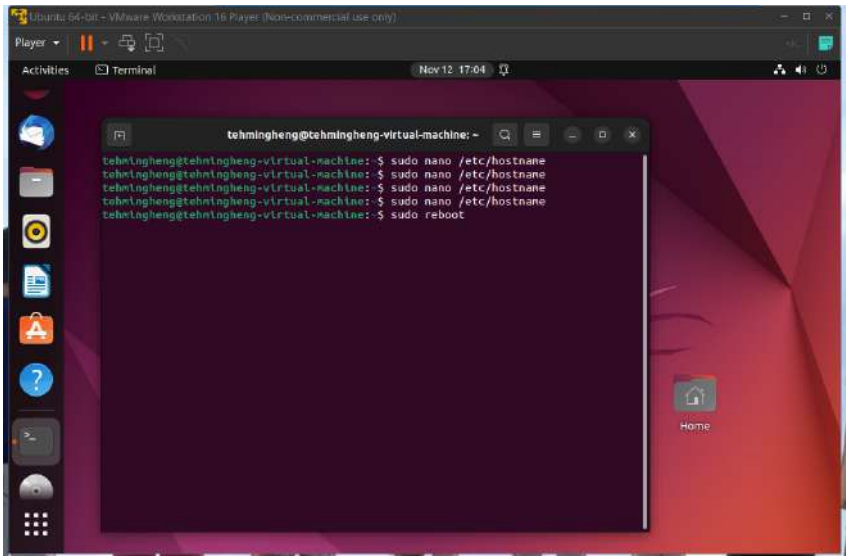


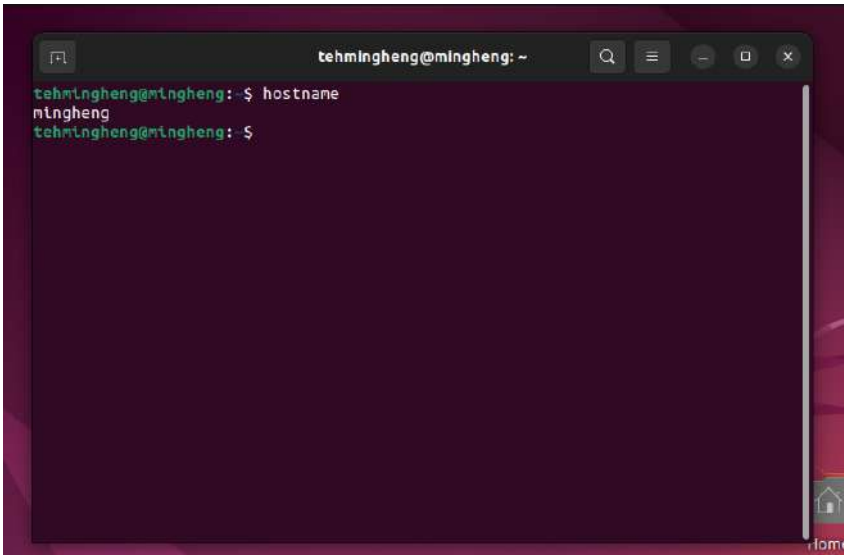
Question 2

sudo nano /etc/hostname



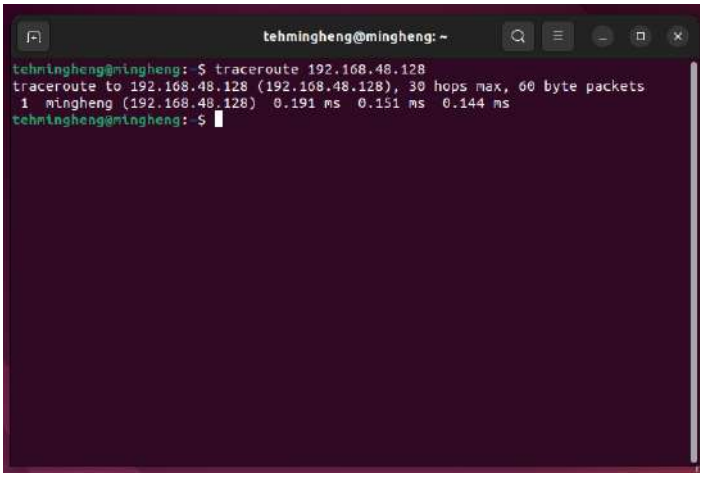

Ubuntu 64-bit - VMware Workstation 16 Player (Non-commercial use only)
Player
Activities
Terminal
Nov 12 17:03
tehmingheng@tehmingheng-virtual-machine: ~
GNU nano 6.2 /etc/hostname *
mingheng
Save modified buffer?
Y Yes
N No
^C Cancel
Home


Ubuntu 64-bit - VMware Workstation 16 Player (Non-commercial use only)
Player
Activities
Terminal
Nov 12 17:04
tehmingheng@tehmingheng-virtual-machine: ~
tehmingheng@tehmingheng-virtual-machine:~$ sudo nano /etc/hostname
tehmingheng@tehmingheng-virtual-machine:~$ sudo nano /etc/hostname
tehmingheng@tehmingheng-virtual-machine:~$ sudo nano /etc/hostname
tehmingheng@tehmingheng-virtual-machine:~$ sudo nano /etc/hostname
tehmingheng@tehmingheng-virtual-machine:~$ sudo reboot
Home

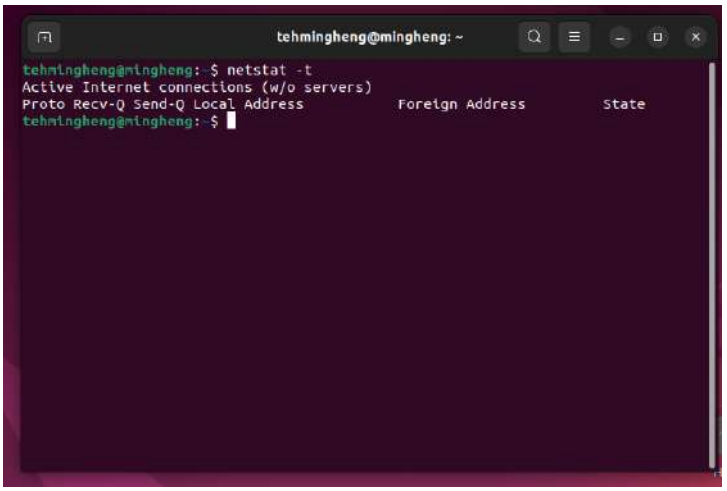

tehmingheng@mingheng: ~
tehmingheng@mingheng:~$ hostname
mingheng
tehmingheng@mingheng:~$

Question 3
Ping it to see if the packet was successful in getting to its endpoint, whereas traceroute shows a path for information on the internet from point a to point b.

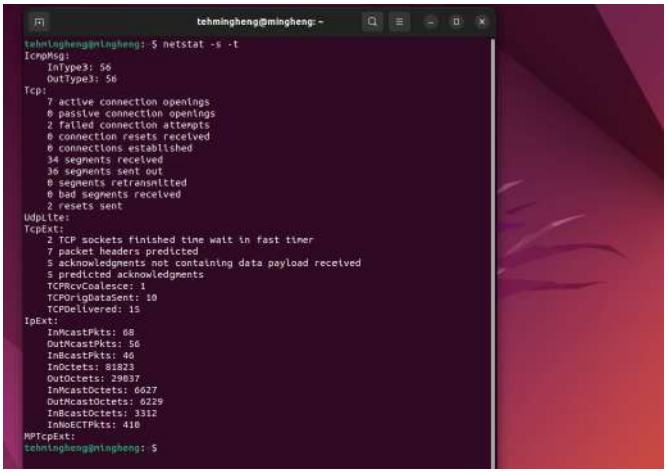
traceroute <ip-address>



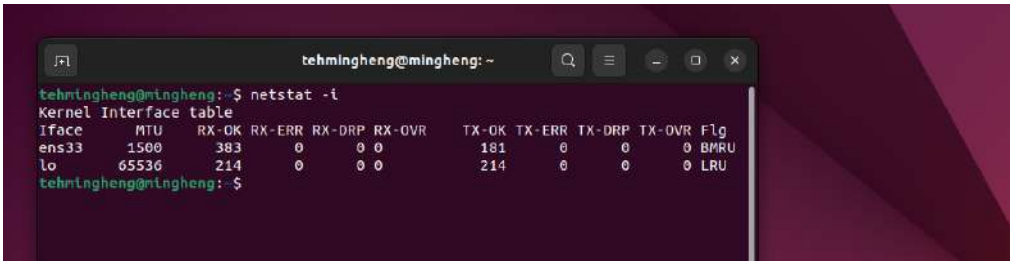
Question 4
netstat -t



netstat -s -t



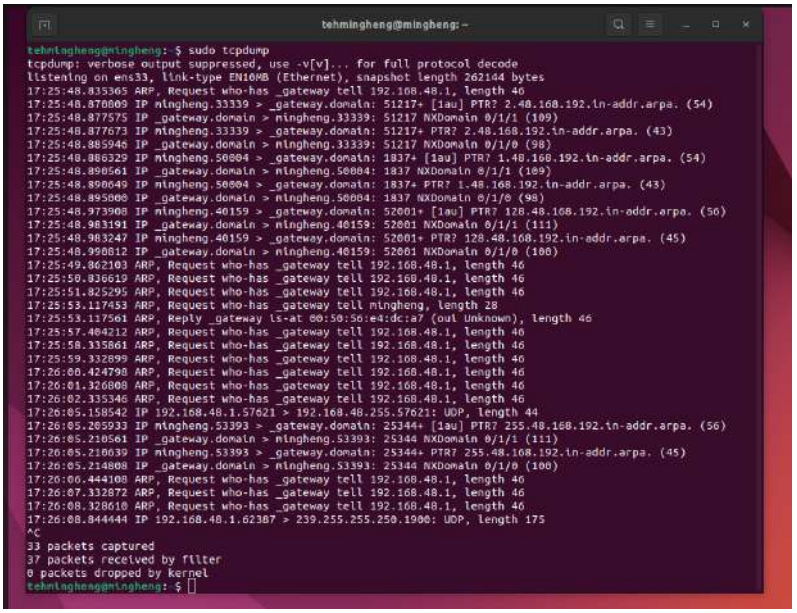
netstat -i



Question 5

A packet analyzer's obvious purpose is to evaluate; specifically, it analyses network traffic by capturing and visualising packets that the computer it is operating on is sending or receiving.

sudo tcpdump



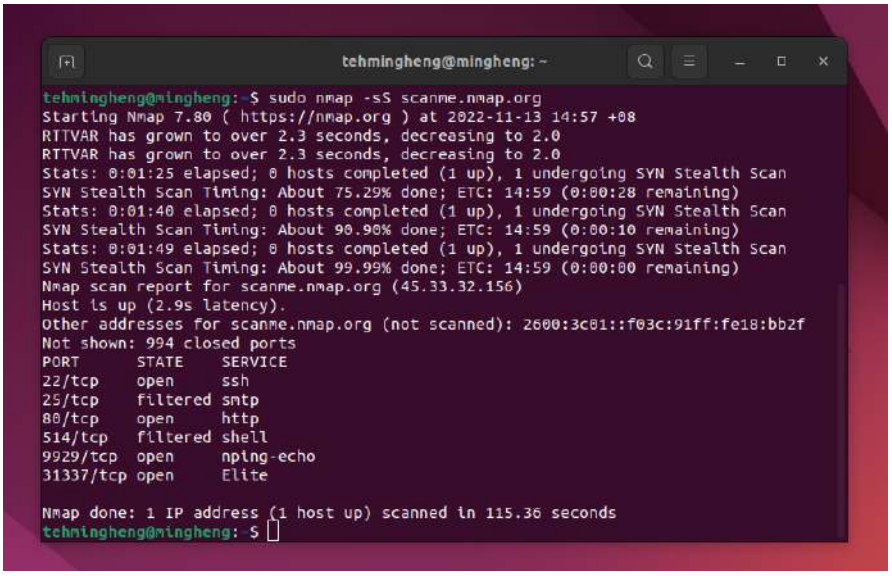
Question 6

nmap -sP <scanme.nmap.org>

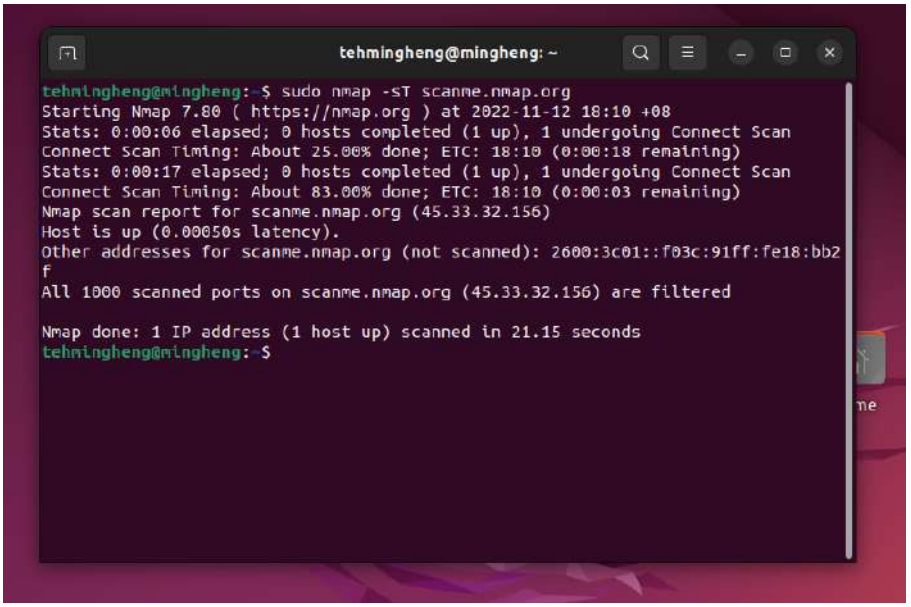
performs a ping scanning instead of a port scanning, enables us to determine which machine is available.

nmap -sS <scanning scanme.nmap.org>

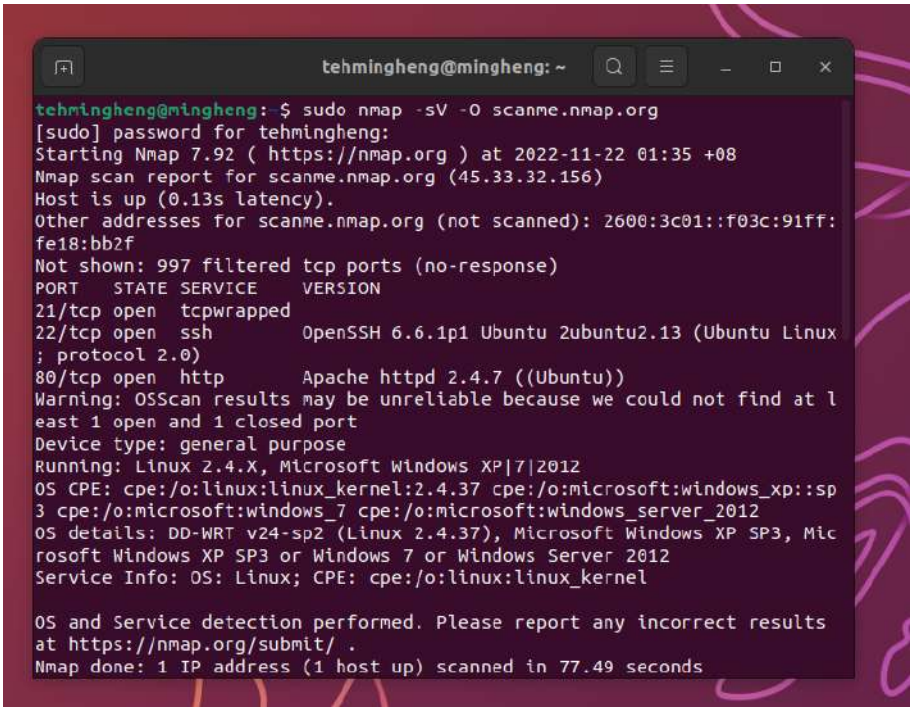
also known as a half open scanning. its the ability to able to check for the open ports



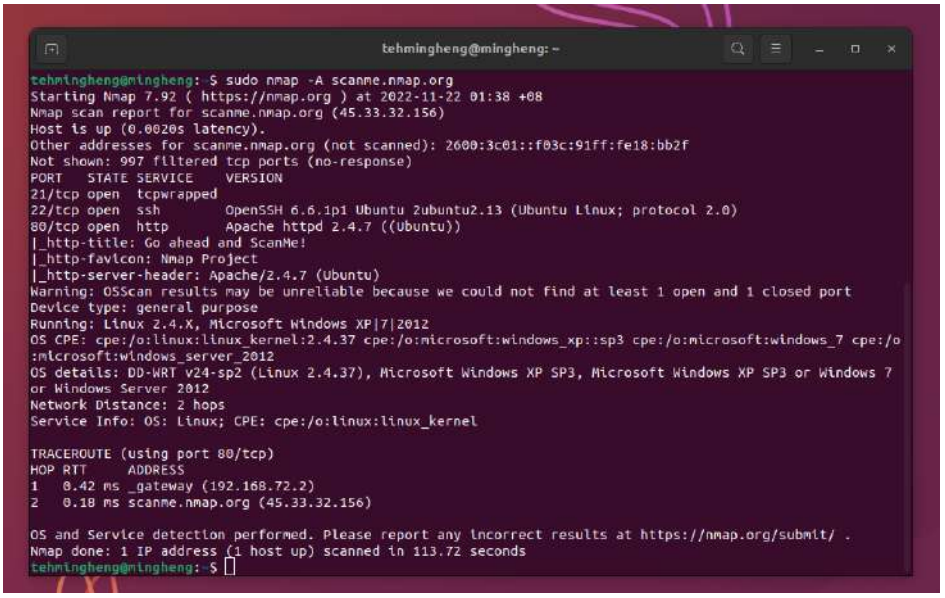
nmap -sT <scanme.nmap.org>



Nmap -sV -O <scanme.nmap.org>



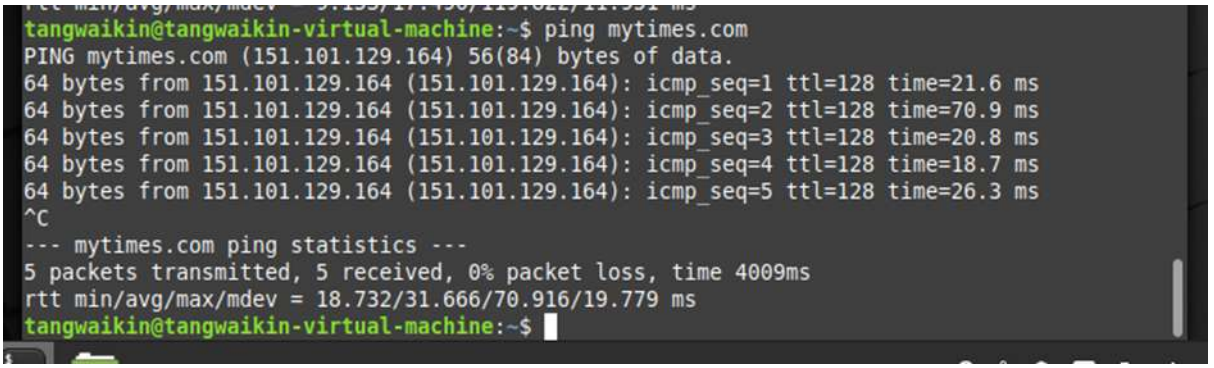
Nmap -A <scanme.nmap.org>



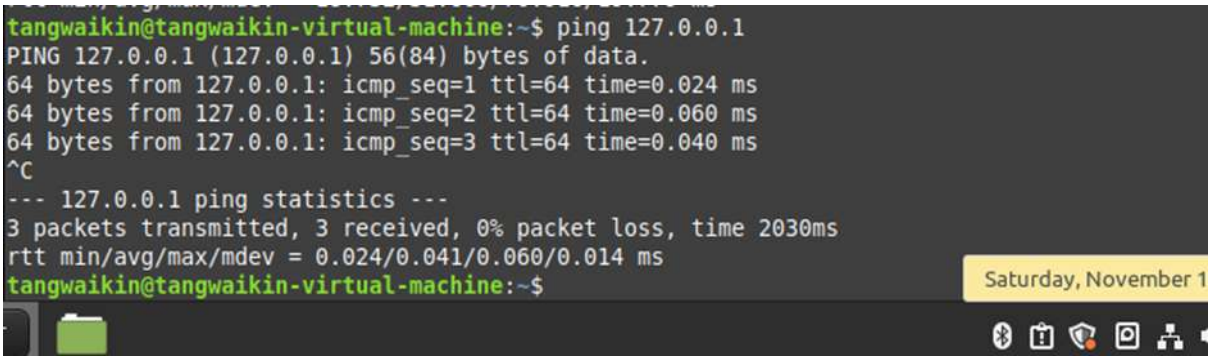
1.7 Tang Wai Kin

Question 1

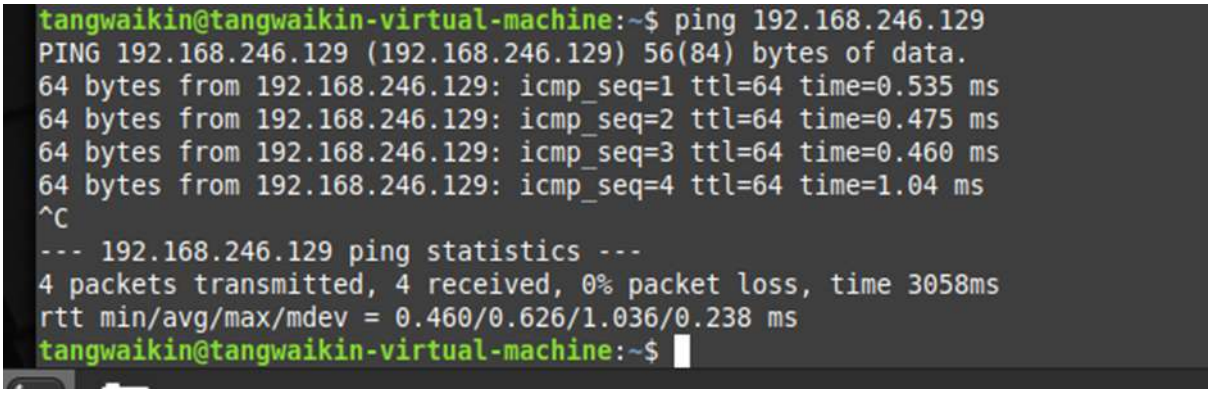
Ping <website> , in order to find out the reachability of a website



ping <localhost> , testing connectivity between hosts and debugging connectivity-related issues on an internet work.



Ping <other-ip-in-network>,



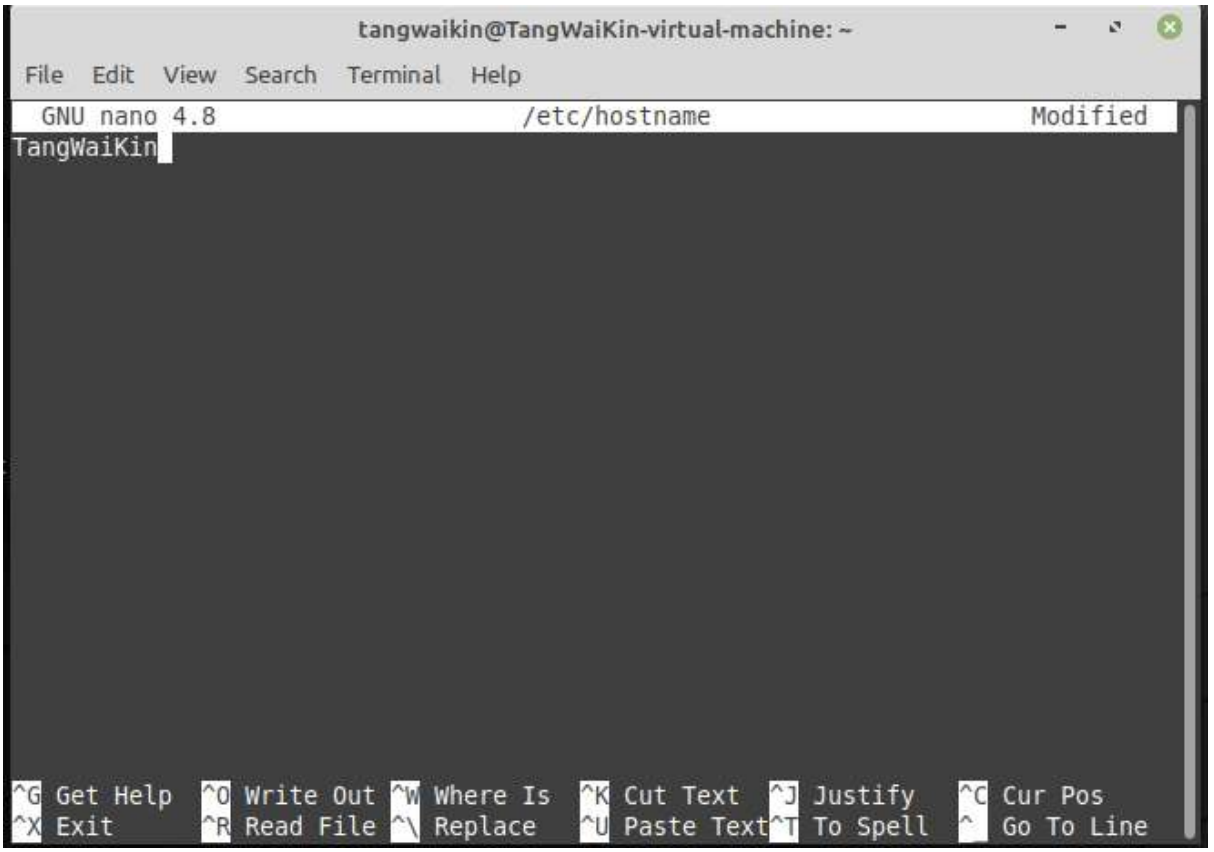
Question 2

```
tangwaikin@TangWaiKin:~$ sudo hostname
TangWaiKin-Virtual-Machine
tangwaikin@TangWaiKin:~$ sudo hostname TangWaiKin
tangwaikin@TangWaiKin:~$ sudo hostname
TangWaiKin
tangwaikin@TangWaiKin:~$
```

Type sudo nano /etc/hostname

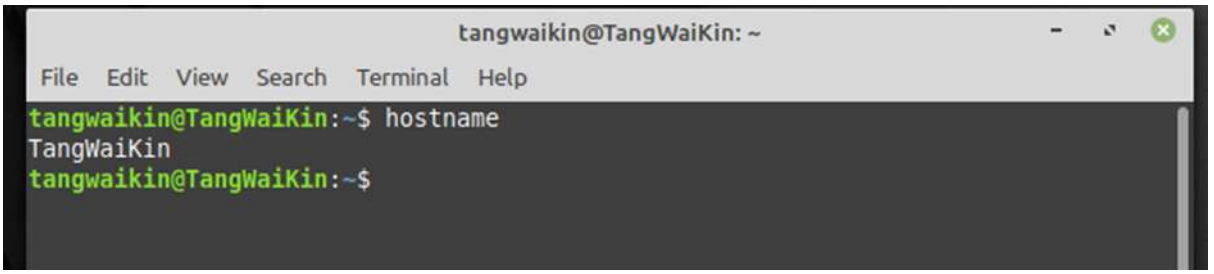
```
tangwaikin@TangWaiKin-virtual-machine:~$ hostname
TangWaiKin-virtual-machine
tangwaikin@TangWaiKin-virtual-machine:~$ sudo nano /etc/hostname
[sudo] password for tangwaikin:
```

change TangWaiKin-Virtual-Machine to TangWaiKin



after that press ctrl+ x , Y then enter

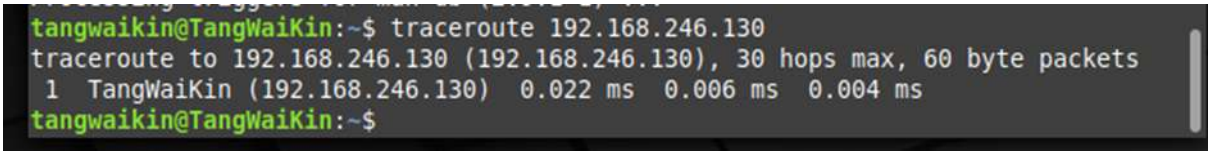
hostname, to display host name



Question 3

- **Explain the difference between ping and traceroute.**

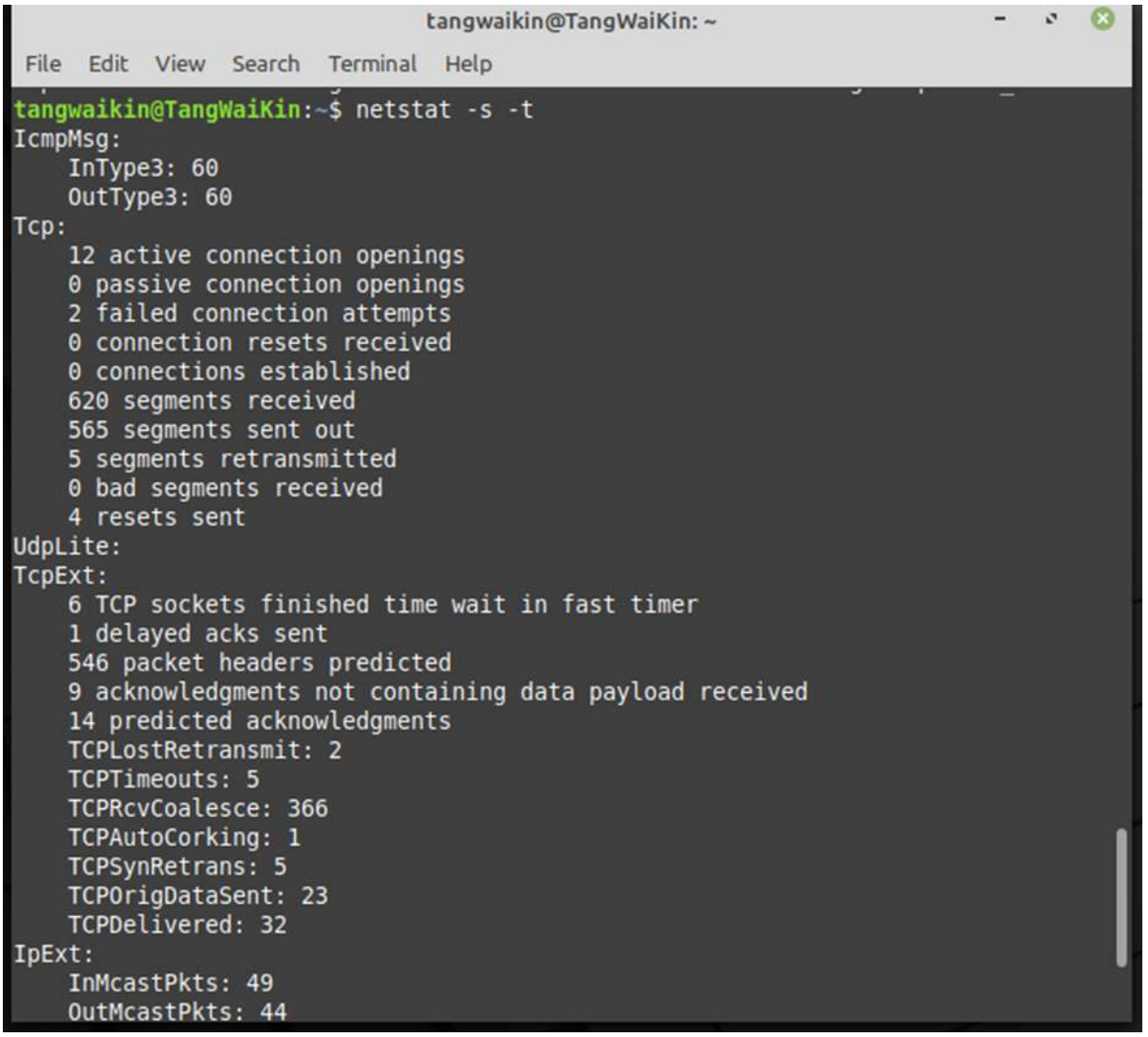
ping it to verify if the packet is able to reach the destination successfully while traceroute is to a map of data on the internet to from source to destination.



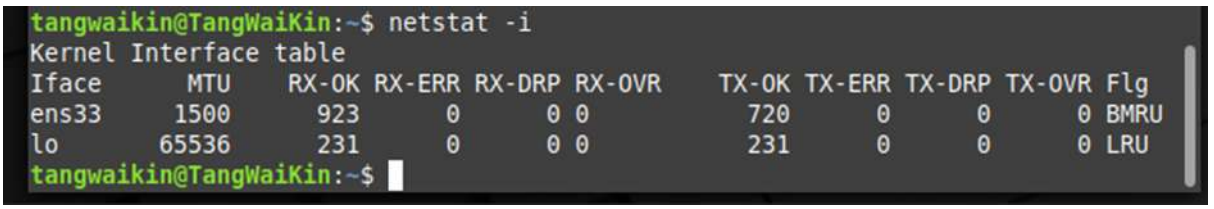
Question 4

1. Netstat -t

2. netstat -s -t



3. netstat -i



Question 5

tcpdump, it is used to capture packets and analyze network traffic.

```
tangwaikin@TangWaiKin:~$ sudo tcpdump
[sudo] password for tangwaikin:
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ens33, link-type EN10MB (Ethernet), capture size 262144 bytes
17:31:50.144073 ARP, Request who-has _gateway tell TangWaiKin, length 28
17:31:50.144643 ARP, Reply _gateway is-at 00:50:56:fe:af:ba (oui Unknown), lengt
h 46
17:31:50.145906 IP TangWaiKin.48747 > _gateway.domain: 31991+ [1au] PTR? 2.246.1
68.192.in-addr.arpa. (55)
17:31:50.158815 IP _gateway.domain > TangWaiKin.48747: 31991 NXDomain- 0/0/1 (55
)
17:31:50.159043 IP TangWaiKin.48747 > _gateway.domain: 31991+ PTR? 2.246.168.192
.in-addr.arpa. (44)
17:31:50.189135 IP _gateway.domain > TangWaiKin.48747: 31991 NXDomain- 0/0/0 (44
)
17:31:50.190889 IP TangWaiKin.58082 > _gateway.domain: 38321+ [1au] PTR? 130.246
.168.192.in-addr.arpa. (57)
17:31:50.209504 IP _gateway.domain > TangWaiKin.58082: 38321 NXDomain- 0/0/1 (57
)
17:31:50.209695 IP TangWaiKin.58082 > _gateway.domain: 38321+ PTR? 130.246.168.1
92.in-addr.arpa. (46)
17:31:50.220037 IP _gateway.domain > TangWaiKin.58082: 38321 NXDomain- 0/0/0 (46
)
17:31:55.909627 IP 192.168.246.129.bootpc > 192.168.246.254.bootps: BOOTP/DHCP,
Request from 00:0c:29:9b:f4:fc (oui Unknown), length 304
17:31:55.910017 IP TangWaiKin.58178 > _gateway.domain: 54698+ [1au] PTR? 254.246
.168.192.in-addr.arpa. (57)
17:31:55.910940 IP 192.168.246.254.bootps > 192.168.246.129.bootpc: BOOTP/DHCP,
```

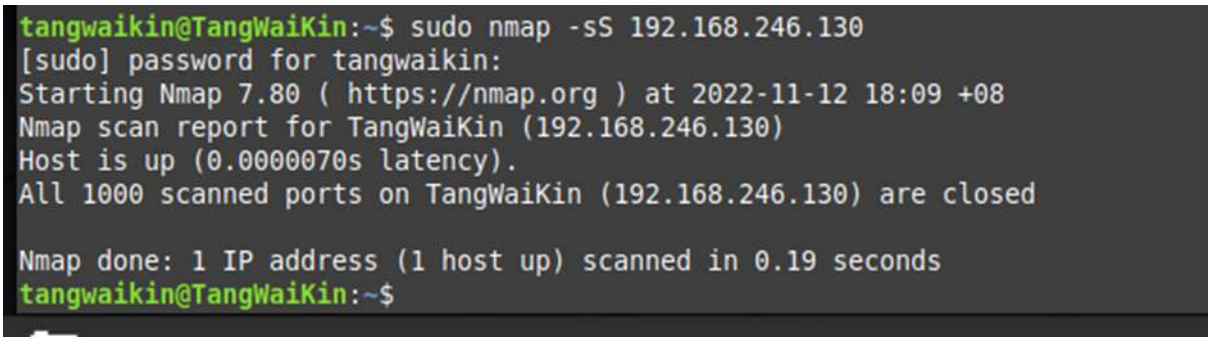
```
17:32:01.092098 ARP, Reply 192.168.246.254 is-at 00:50:56:e8:61:6f (oui Unknown)
, length 46
^C
30 packets captured
30 packets received by filter
0 packets dropped by kernel
tangwaikin@TangWaiKin:~$
```

Question 6

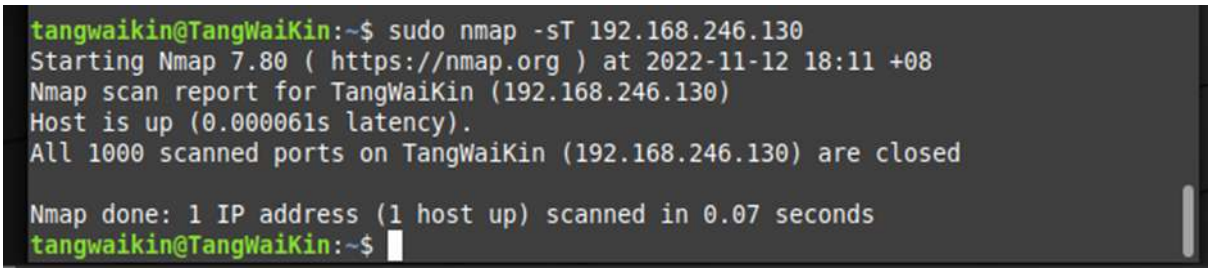
nmap –sP <ip address>, it is a ping scan that allow us to check which computer is online rather than which port is open.

```
tangwaikin@TangWaiKin:~$ sudo nmap -sP scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-12 17:41 +08
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.0015s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2
f
Nmap done: 1 IP address (1 host up) scanned in 0.56 seconds
tangwaikin@TangWaiKin:~$
```

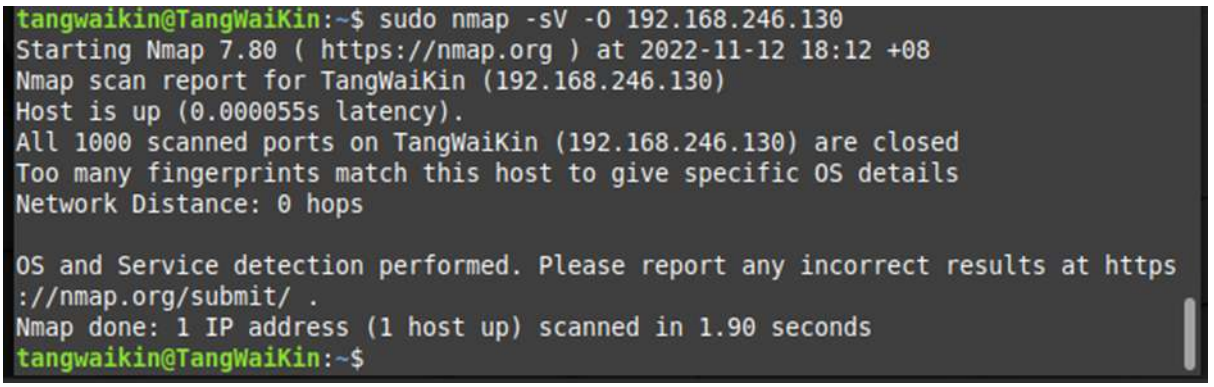
nmap –sS <ip address>, it can called as half open scan as well. it is to scan which ports are open.



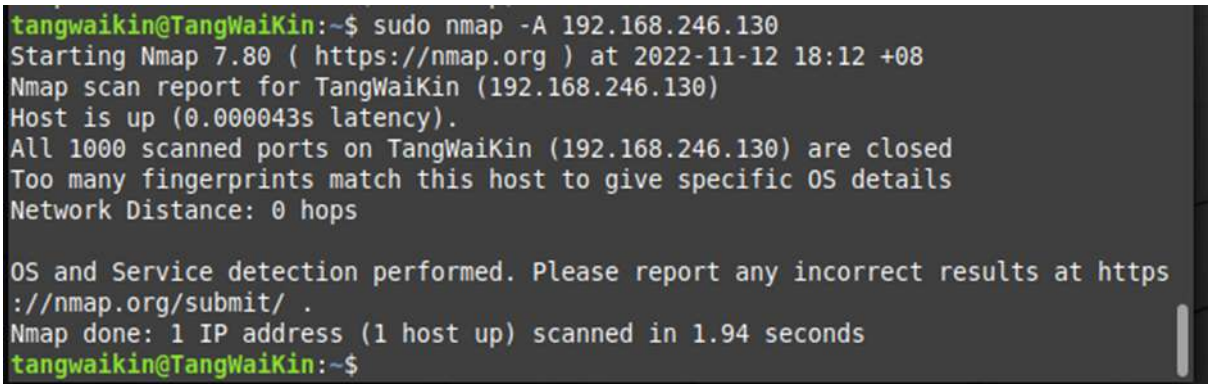
nmap –sT <ip address> this scanning is very effective to provide user informations about which ports are available to access and which ports are not.



nmap -sV -O <ip address>

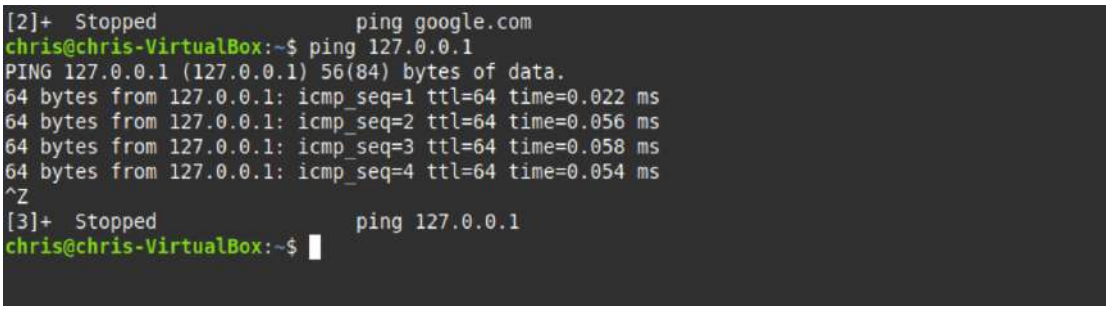


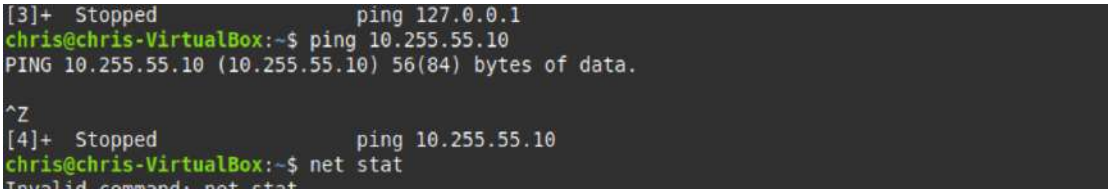
nmap -A <ip address>



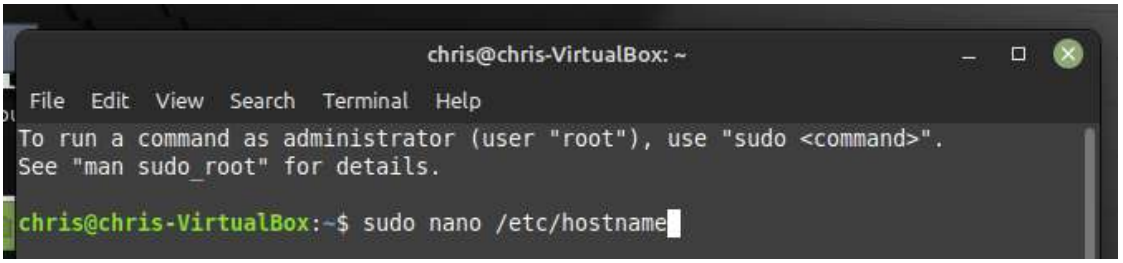
1.8 Christiaan Tim Vrieling

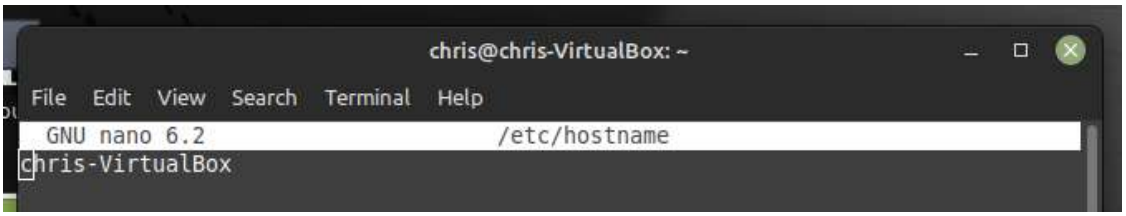
Question 1

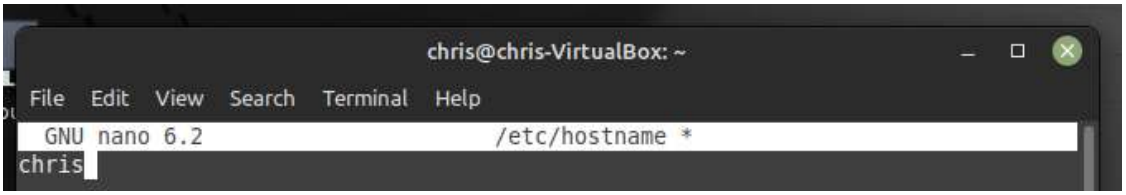


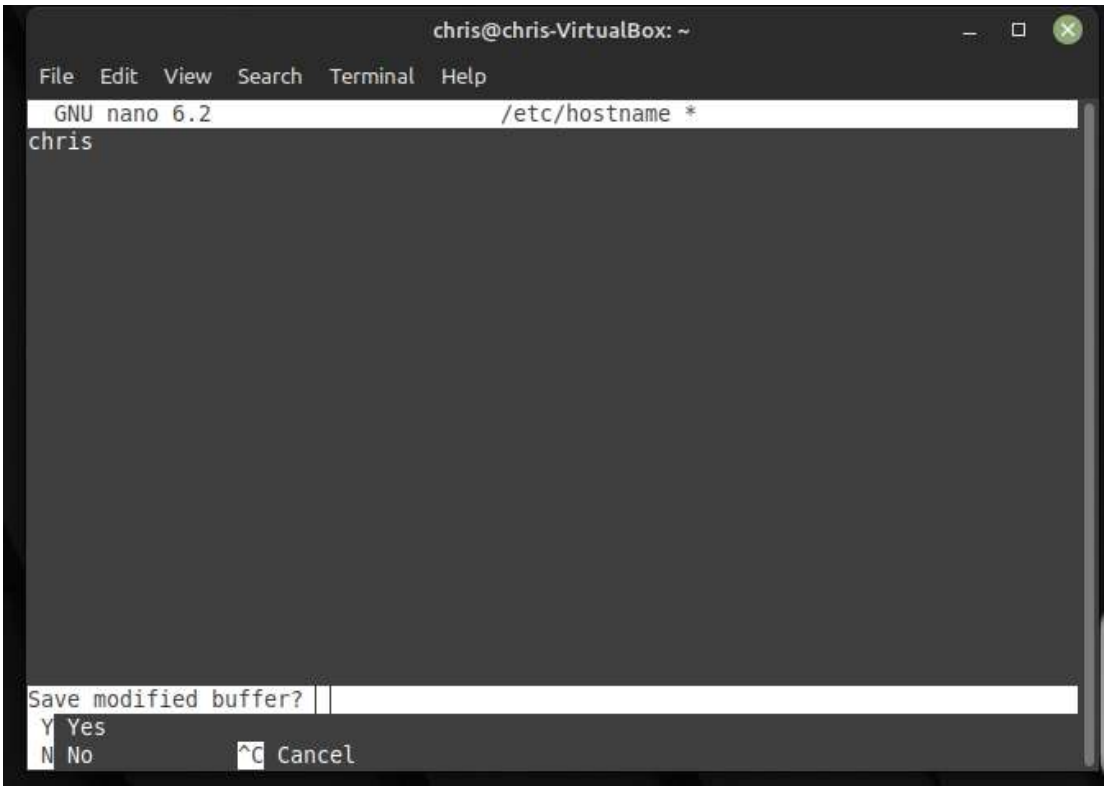


Question 2

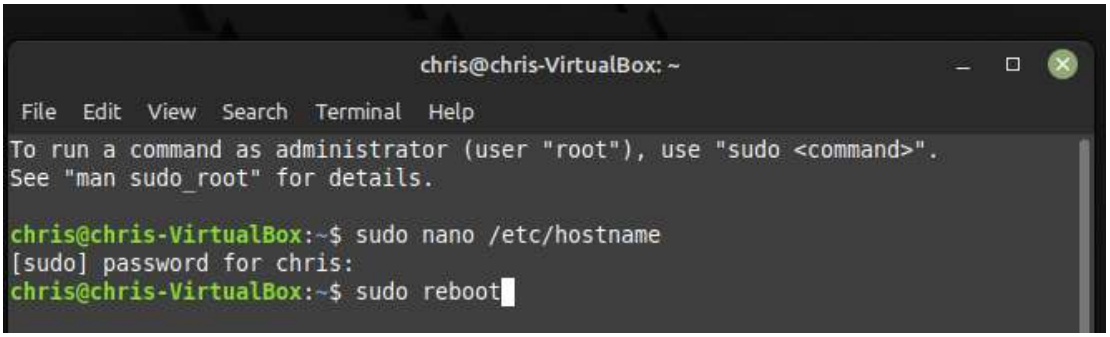


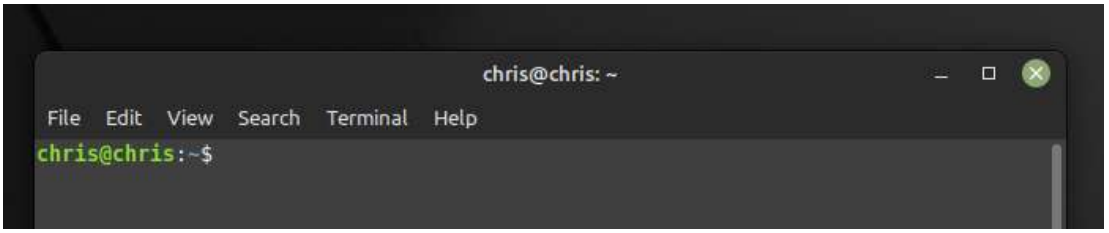




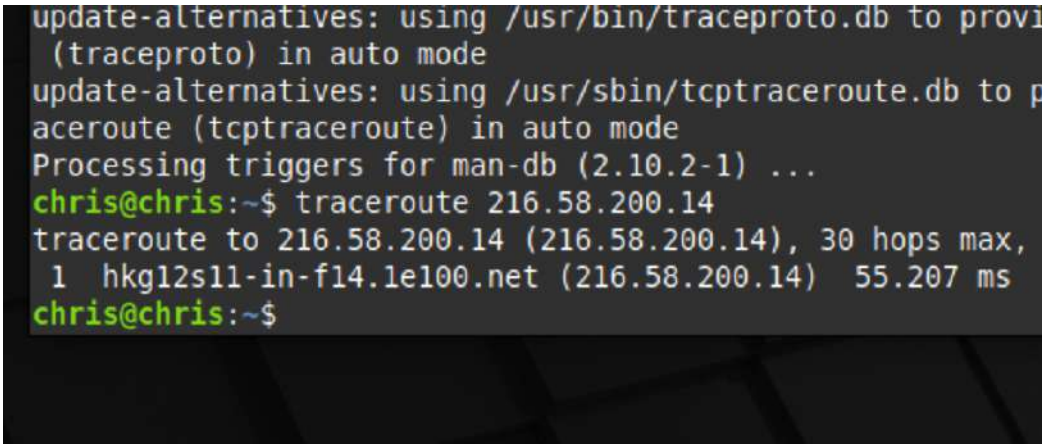

chris@chris-VirtualBox: ~
File Edit View Search Terminal Help
GNU nano 6.2 /etc/hostname *
chris
Save modified buffer?
Y Yes
N No ^C Cancel


File Name to Write: /etc/hostname
^G Help M-D DOS Format M-A Append M-B Backup File
^C Cancel M-M Mac Format M-P Prepend ^T Browse


chris@chris-VirtualBox: ~
File Edit View Search Terminal Help
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
chris@chris-VirtualBox:~$ sudo nano /etc/hostname
[sudo] password for chris:
chris@chris-VirtualBox:~$ sudo reboot


chris@chris: ~
File Edit View Search Terminal Help
chris@chris:~$

Question 3



Question 4

```
chris@chris:~$ netstat -t
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
chris@chris:~$ netstat -s -t
IcmpMsg:
    InType3: 40
    OutType3: 40
Tcp:
    335 active connection openings
    0 passive connection openings
    2 failed connection attempts
    0 connection resets received
    0 connections established
    22618 segments received
    19724 segments sent out
    4 segments retransmitted
    0 bad segments received
    2 resets sent
UdpLite:
TcpExt:
    328 TCP sockets finished time wait in fast timer
    32 delayed acks sent
    18510 packet headers predicted
    333 acknowledgments not containing data payload received
    978 predicted acknowledgments
    TCPLostRetransmit: 1
    TCPTimeouts: 4
    TCPBacklogCoalesce: 252
    TCPRcvCoalesce: 7241
    TCPSynRetrans: 4
    TCPOrigDataSent: 1319
    TCPDelivered: 1652
    TcpTimeoutRehash: 4
IpExt:
    InMcastPkts: 108
    OutMcastPkts: 47
    InOctets: 72500719
    OutOctets: 1222753
    InMcastOctets: 74880
    OutMcastOctets: 5532
    InNoECTPkts: 54094
MPTcpExt:
chris@chris:~$ netstat -i
Kernel Interface table
Iface      MTU    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
ens33     1500    52859      0      0 0         20100      0      0      0 BMRU
lo       65536     1457      0      0 0          1457      0      0      0 LRU
```

Question 5

```
    InNoECTPkts: 393
MPTcpExt:
chris@chris:~$ sudo tcpdump
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on enp0s5, link-type EN10MB (Ethernet), snapshot length 262144 bytes
00:42:22.752345 IP 10.211.55.2.57621 > 10.211.55.255.57621: UDP, length 44
00:42:22.846874 IP chris.49797 > _gateway.domain: 40287+ PTR? 255.55.211.10.in-addr.arpa. (44)
00:42:22.895644 IP _gateway.domain > chris.49797: 40287 NXDomain 0/0/0 (44)
00:42:22.898847 IP chris.45275 > _gateway.domain: 17530+ PTR? 2.55.211.10.in-addr.arpa. (42)
00:42:22.969759 IP _gateway.domain > chris.45275: 17530 NXDomain 0/0/0 (42)
00:42:22.970510 IP chris.59852 > _gateway.domain: 1095+ PTR? 1.55.211.10.in-addr.arpa. (42)
00:42:22.991377 IP _gateway.domain > chris.59852: 1095 NXDomain 0/0/0 (42)
00:42:22.992106 IP chris.56400 > _gateway.domain: 33683+ PTR? 9.55.211.10.in-addr.arpa. (42)
00:42:23.019624 IP _gateway.domain > chris.56400: 33683 NXDomain 0/0/0 (42)
00:42:28.043503 ARP, Request who-has _gateway tell chris, length 28
00:42:28.044016 ARP, Reply _gateway is-at 00:1c:42:00:00:18 (oui Unknown), length 28
00:42:50.671563 IP 10.211.55.2.mdns > 224.0.0.251.mdns: 0 [1a] [16q] PTR (QM)? lb._dns-sd._udp.local. PTR (QM)? _airpor
kit._tcp.local. PTR (QM)? _uscan._tcp.local. PTR (QM)? _uscans._tcp.local. PTR (QM)? _ippusb._tcp.local. PTR (QM)? _sca
pdl-datastream._tcp.local. PTR (QM)? _ptp._tcp.local. PTR (QM)? _googlecast._tcp.local. PTR (QM)? _companion-link._tcp.
ee._sub._apple-mobdev2._tcp.local. PTR (QM)? _apple-pairable._tcp.local. (345)
00:42:50.671564 IP6 fe80::f8ff:c2ff:fe66:e064.mdns > ff02::fb.mdns: 0 [1a] [16q] PTR (QM)? lb._dns-sd._udp.local. PTR (
 (QM)? _homekit._tcp.local. PTR (QM)? _uscan._tcp.local. PTR (QM)? _uscans._tcp.local. PTR (QM)? _ippusb._tcp.local. PT
 PTR (QM)? _pdl-datastream._tcp.local. PTR (QM)? _ptp._tcp.local. PTR (QM)? _googlecast._tcp.local. PTR (QM)? _companio
(QM)? 919107ee._sub._apple-mobdev2._tcp.local. PTR (QM)? _apple-pairable._tcp.local. (345)
00:42:50.750482 IP chris.50909 > _gateway.domain: 52846+ PTR? 251.0.0.224.in-addr.arpa. (42)
00:42:51.381864 IP _gateway.domain > chris.50909: 52846 NXDomain 0/0/0 (42)
00:42:51.384307 IP chris.40940 > _gateway.domain: 30476+ PTR? b.f.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2
00:42:51.420121 IP _gateway.domain > chris.40940: 30476 NXDomain 0/0/0 (90)
00:42:52.772201 IP 10.211.55.2.57621 > 10.211.55.255.57621: UDP, length 44
00:43:22.790202 IP 10.211.55.2.57621 > 10.211.55.255.57621: UDP, length 44
00:43:40.600876 IP chris.39430 > _gateway.domain: 28420+ AAAA? connectivity-check.ubuntu.com. (47)
00:43:41.542197 IP6 chris.mdns > ff02::fb.mdns: 0 [2q] PTR (QM)? _ipp._tcp.local. PTR (QM)? _ipps._tcp.local. (45)
00:43:41.542499 IP chris.mdns > 224.0.0.251.mdns: 0 [2q] PTR (QM)? _ipp._tcp.local. PTR (QM)? _ipps._tcp.local. (45)
00:43:41.557455 IP chris.43791 > _gateway.domain: 26410+ PTR? 2.1.3.a.a.8.1.2.3.6.7.0.2.e.8.3.0.0.0.0.4.e.4.f.6.2.c.2.2
00:43:41.803846 IP _gateway.domain > chris.43791: 26410 NXDomain 0/0/0 (90)
00:43:45.612511 ARP, Request who-has _gateway tell chris, length 28
00:43:45.614378 ARP, Reply _gateway is-at 00:1c:42:00:00:18 (oui Unknown), length 28
00:43:45.696437 IP 10.211.55.2.mdns > 224.0.0.251.mdns: 0 PTR (QM)? _spotify-connect._tcp.local. (45)
00:43:45.697482 IP6 fe80::f8ff:c2ff:fe66:e064.mdns > ff02::fb.mdns: 0 PTR (QM)? _spotify-connect._tcp.local. (45)
00:43:45.767570 IP chris.39430 > _gateway.domain: 28420+ AAAA? connectivity-check.ubuntu.com. (47)
00:43:45.808378 IP _gateway.domain > chris.39430: 28420 0/0/0 (47)
00:43:45.810046 IP chris.48112 > _gateway.domain: 34926+ AAAA? connectivity-check.ubuntu.com. (47)
00:43:45.873816 IP _gateway.domain > chris.48112: 34926 0/0/0 (47)
00:43:52.809089 IP 10.211.55.2.57621 > 10.211.55.255.57621: UDP, length 44
```

Question 6

```
chris@chris:~$ sudo nmap -sP 216.58.200.14
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-13 00:57 +08
Nmap scan report for hkg12s11-in-f14.1e100.net (216.58.200.14)
Host is up (0.00080s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
chris@chris:~$
```

```
chris@chris:~$ sudo nmap -sS 216.58.200.14
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-13 00:59 +08
Nmap scan report for hkg12s11-in-f14.1e100.net (216.58.200.14)
Host is up (0.00011s latency).
All 1000 scanned ports on hkg12s11-in-f14.1e100.net (216.58.200.14) are closed

Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
chris@chris:~$
```

```
chris@chris:~$ sudo nmap -sT 216.58.200.14
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-13 00:58 +08
Nmap scan report for kul09s16-in-f14.1e100.net (216.58.200.14)
Host is up (0.00016s latency).
All 1000 scanned ports on kul09s16-in-f14.1e100.net (216.58.200.14) are closed

Nmap done: 1 IP address (1 host up) scanned in 11.46 seconds
chris@chris:~$
```

```
chris@chris:~$ sudo nmap -sV -O scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-22 00:32 +08
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.020s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2
f
Not shown: 997 filtered ports
PORT   STATE SERVICE    VERSION
21/tcp open  tcpwrapped
22/tcp open  tcpwrapped
80/tcp open  tcpwrapped
Warning: OSScan results may be unreliable because we could not find at least 1 o
pen and 1 closed port
Device type: specialized|WAP|phone
Running: iPXE 1.X, Linux 2.4.X|2.6.X, Sony Ericsson embedded
OS CPE: cpe:/o:ipxe:ipxe:1.0.0%2b cpe:/o:linux:linux_kernel:2.4.20 cpe:/o:linux:
linux_kernel:2.6.22 cpe:/h:sonyericsson:u8i_vivaz
OS details: iPXE 1.0.0+, Tomato 1.28 (Linux 2.4.20), Tomato firmware (Linux 2.6.
22), Sony Ericsson U8i Vivaz mobile phone

OS and Service detection performed. Please report any incorrect results at https
://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 47.96 seconds
```

```
chris@chris:~$ sudo nmap -A 216.58.200.14
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-13 01:00 +08
WARNING: RST from 216.58.200.14 port 443 -- is this port really open?
WARNING: RST from 216.58.200.14 port 443 -- is this port really open?
WARNING: RST from 216.58.200.14 port 443 -- is this port really open?
WARNING: RST from 216.58.200.14 port 443 -- is this port really open?
WARNING: RST from 216.58.200.14 port 443 -- is this port really open?
WARNING: RST from 216.58.200.14 port 443 -- is this port really open?
WARNING: RST from 216.58.200.14 port 443 -- is this port really open?
WARNING: RST from 216.58.200.14 port 443 -- is this port really open?
WARNING: RST from 216.58.200.14 port 443 -- is this port really open?
WARNING: RST from 216.58.200.14 port 443 -- is this port really open?
WARNING: RST from 216.58.200.14 port 443 -- is this port really open?
WARNING: RST from 216.58.200.14 port 443 -- is this port really open?
Nmap scan report for hkg12s11-in-f14.1e100.net (216.58.200.14)
Host is up (0.0022s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE    VERSION
53/tcp  open  tcpwrapped
80/tcp  open  tcpwrapped
443/tcp open  tcpwrapped
OS fingerprint not ideal because: Didn't receive UDP response. Please try again with -sSU
No OS matches for host
Network Distance: 1 hop

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   0.71 ms hkg12s11-in-f14.1e100.net (216.58.200.14)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.56 seconds
chris@chris:~$
```

Section E

1.

Access point found in the third floor of the library, the area besides the Computer Lab.

Access point found in the Block C level 6 classroom 4, one of the classrooms for Masters Degree students' modules.

2.

Location: third floor of the library, the area besides the Computer Lab
Model: Aruba Networks AP220 series AP-225
Antenna information: three integrated omni directional downtilt antennas

Location: Block E Chemistry Lab 1
Model: Aruba Networks AP105
Antenna information: 4 integrated, omni-directional antenna elements (supporting up to 2x2 MIMO)

Location: Student Life
Model: Aruba Networks AP220 series AP-225
Antenna information: three integrated omni directional downtilt antennas

3.

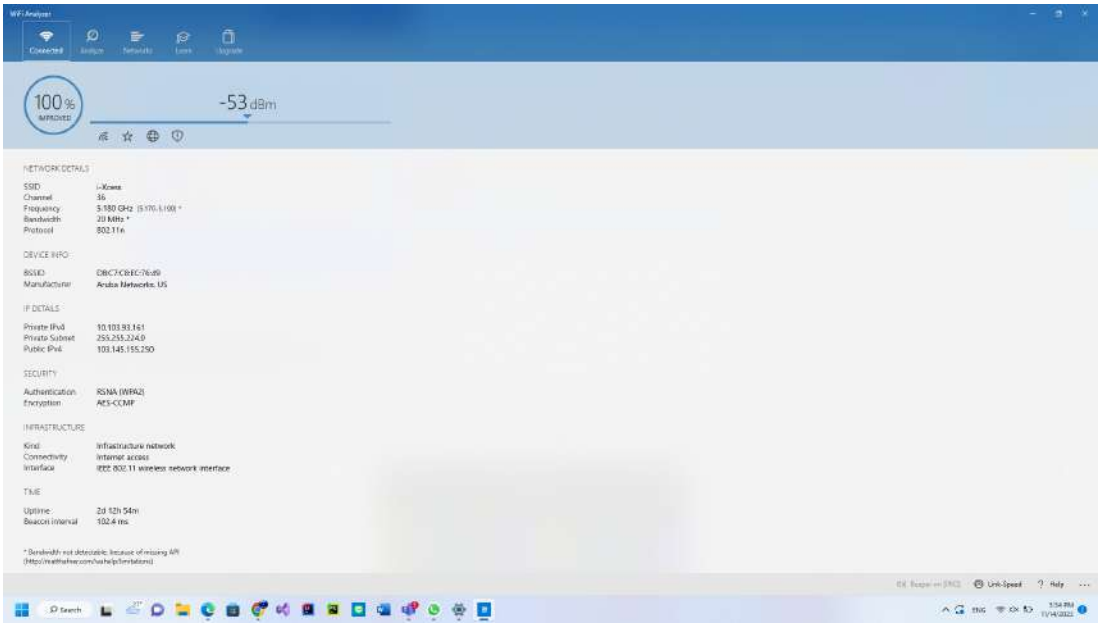
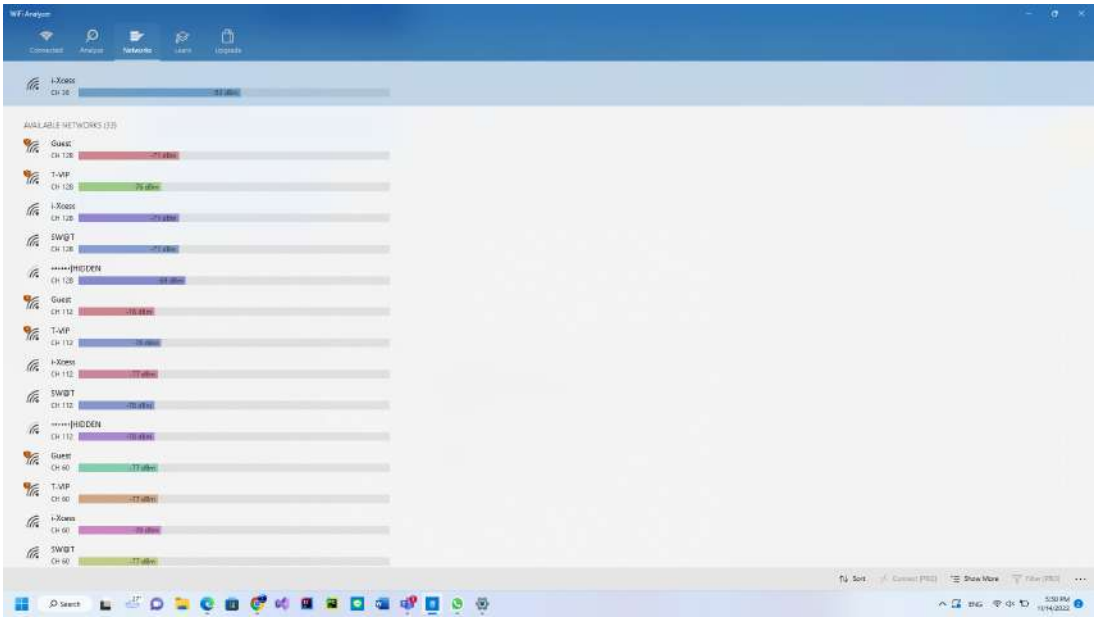


figure 1 - details of SSID “i-Xcess” accessed from Library Droom 3-1.



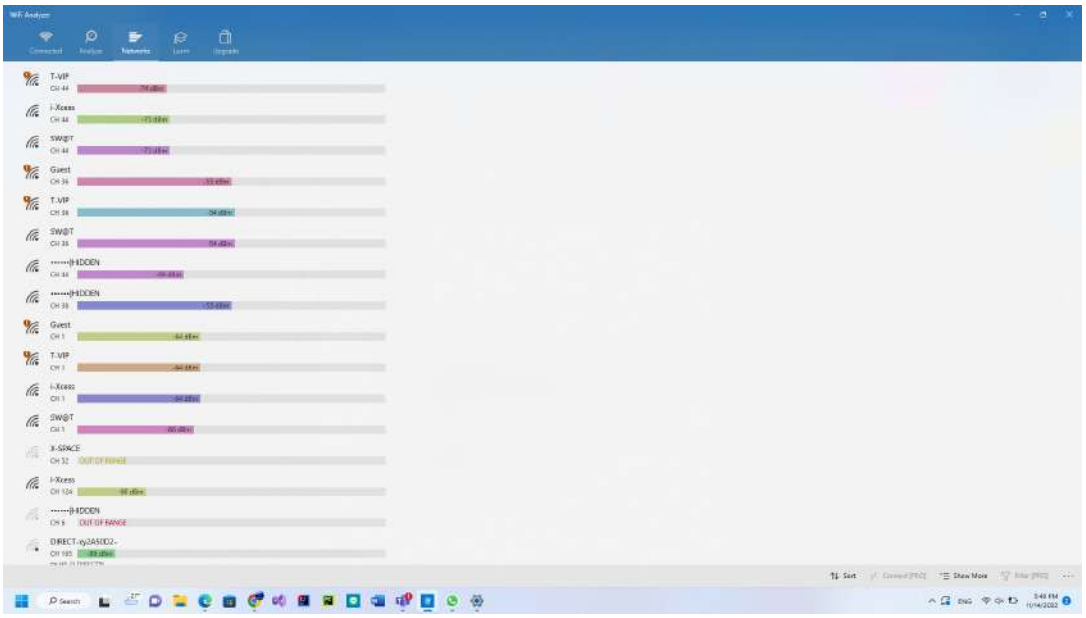


figure 2 and 3 - SSIDs detected in the same place with figure 1 location.

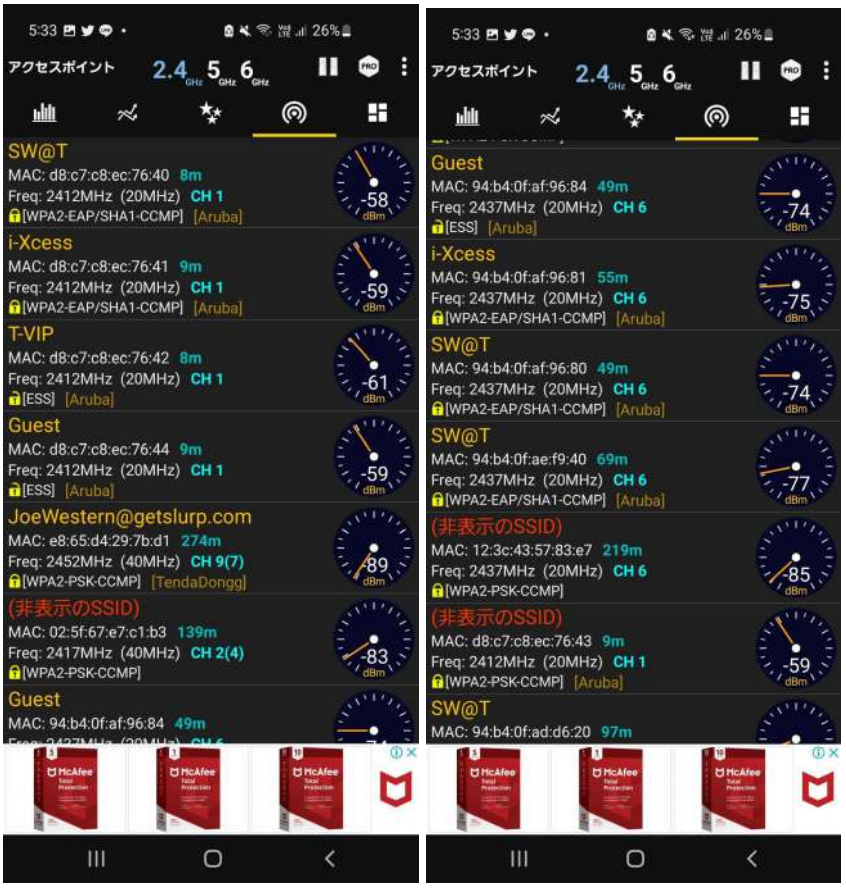


figure 4 and 5 - display of a couple of SSID and BSSID (not all but just few)

a. D8:C7:C8:EC:76:49

b. According to the Wi-Fi analyzer screenshot above, 33 Wi-Fis were discovered. SSID is normally considered as Wi-Fi, so 33 SSIDs are discovered.

c. Totally 5 SSIDs were being broadcasted from the router.

d. BSSID is unique information, so each SSID holds a single BSSID. In the location introduced above detected 33 SSIDs, so 33 BSSIDs were also detected at the same location.

e. To confirm whether the BSSID is broadcasted by the same access point or not, refer to the BSSID. If BSSID is broadcasted from the same access point, multiple BSSID must have exactly the same first 10 digits out of 12 hexadecimal digits. and also the last 2 digits must be continuous with each other. Then we can say that those BSSID are assigned in order by the same access point.

f. The Wi-Fi broadcasting is using 5 Ghz.

g. RSNA (WPA2) for security and AES-CCMP for encryption.

   WPA2, also known as Wi-Fi Protected Access 2, is one of the security systems used in Wireless LAN security that performs a higher level of security than WPA. Initially, WEP was developed for network security, but the system used the same password many times, so the security system became vulnerable. Therefore, the security method changes password many times which is known as “WPA” developed as an alternative, and WPA2 is the newer security technology that complements the vulnerability of WPA. WPA2 can perform the more complicated encryption system, and it is the popular security system used in many Wireless LAN nowadays.

   Counter mode with CBC-MAC Protocol is also known as CCMP, AES-CCMP is the CCMP using encryption method of AES. AES, also known as Advanced Encryption Standard, is the encryption algorithm used in the security of Wireless LAN, is the symmetric-key algorithm that both data sender and receiver use the same encryption key for encryption and decryption. At first, DES was developed for encryption but this one has a huge fragility that the size of the key was short. The DES key had only a 56 bit size and it was weak with the brute-force attack. 2DES or 3DES have developed, but these were still vulnerable and could not supersede the DES, so AES was developed. AES key length can be chosen from 3 different sizes, 128 bit, 192 bit, and 256 bit. Furthermore, AES has four steps of interpretation: SubBytes, ShiftRows, MixColumns, and AddRoundKey. After undergoing these

four interpretation steps, the information will be encrypted to one of the sizes of the encryption key. AES-CCMP is used in WPA2.

h. -53 dBm

i. CH 36

4.

a. Model or type of antennas might affect the speed of network connection. This is because, generally new models of antennas are maximizing network speed, while older models might delay the network speed. Type of antennas might also affect network connectivity speed, so it is crucial to use them properly in case by case. Nevertheless, the number of antennas might not affect the speed of network connectivity. It improves the quality of network connectivity, but that does not mean that it “fastens” the speed of the network. Hence, we think it is a good choice to choose the network connectivity by the model or type of antennas, but number of antennas.

   The three access points are all having the same model/type of antennas, which is “omnidirectional” antennas. This antenna type ensures the stable, consistent connectivity in a wide range so the type of antennas for those access points are already suitable. Besides that, the price of the APs can be improved, its cost is higher compared to other competitors.

b. For types of antennas, omnidirectional antennas are recommended because of their consistency in wide range coverage. More than WPA2 is good condition for network security, and also better to cover both 2.4 GHz and 5 GHz network connectivity.

   Currently, the access points we found and raised above are covering all of these criteria, so those types of routers are already enough, fulfilling in current.

c. There are mainly two types of antennas, omnidirectional and directional.

   Omnidirectional antennas are polarized in a way that they can receive consistent signals from all 360 degrees. Therefore, omnidirectional antennas are stable, but because the antennas are handling signals in all directions, the power of signals is not as strong as directional antennas.

   On the other hand, directional antennas are polarized in a way that they can receive powerful signals from particular directions. Therefore,

directional antennas are powerful, but because the antennas are handling only a few directions, consistency is not as much as omnidirectional antennas.

Due to these conditions, we will propose omnidirectional antennas than directional antennas for routers. Router is the access point we use 24/7, mostly our lifeline because we humans are fully relying on the internet in daily life in recent years. For meetings in schools, businesses, saving backups of important, confidential documents, chatting with families or friends, and so on. All these daily instructions are dependent on network connectivity, so we need consistent network connectivity.

Furthermore, the router is set on the specific place, but humans are always moving around. So handling network connection in all directions is crucial for users. Omnidirectional antennas are able to cope with this requirement because they are consistent in every 360 degrees direction, but directional antennas are not available in all directionals, or vulnerable in ranges that they are not dealing with.

Hence, omnidirectional antennas are better than directional antennas for use in routers. Above routers in Section E question 1 and 2 are all using omnidirectional antennas, so their antennas already have enough functions and conditions.

d.

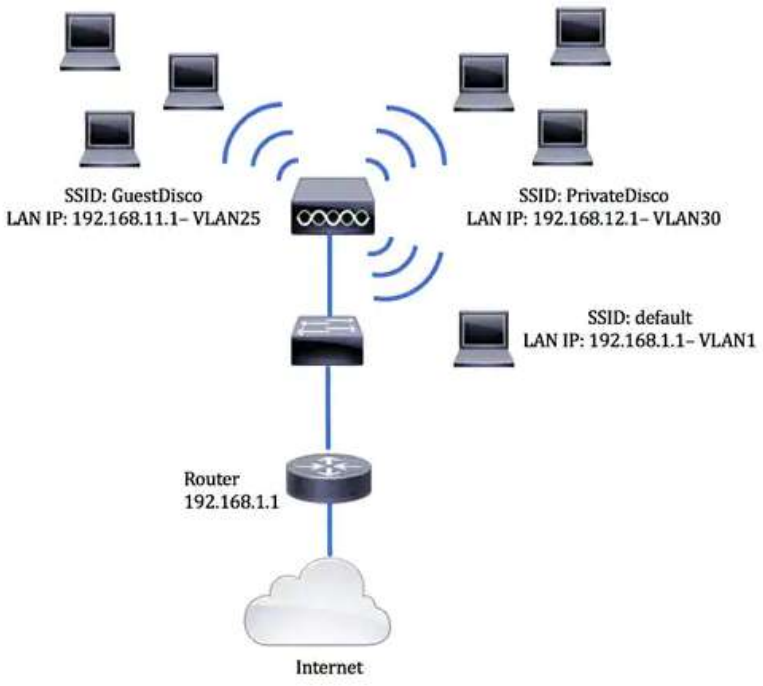
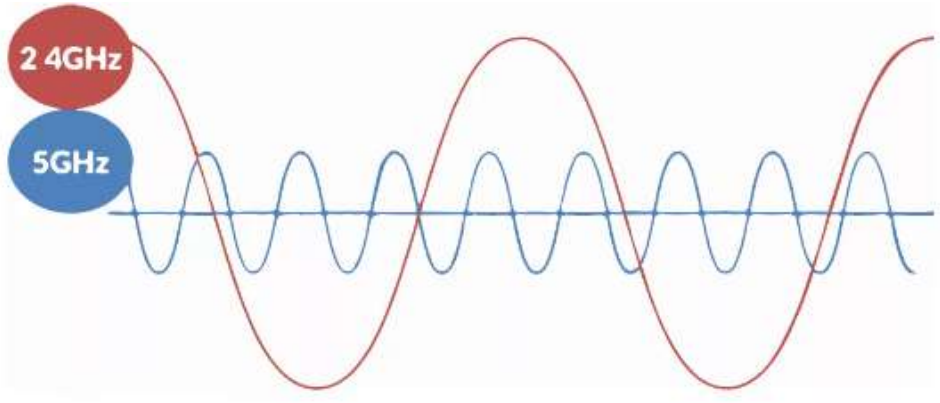
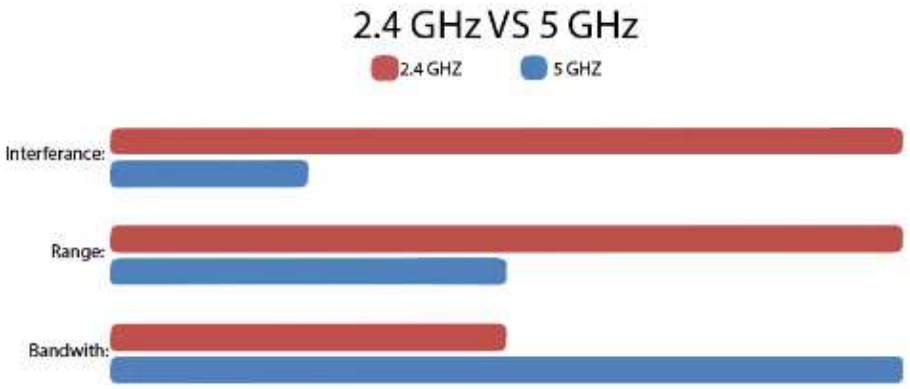


Figure - 3 different SSID from the same access point.
(picture by CISCO)

This is because it is better practice to use multiple SSID than single. Multiple SSID usage allows segment networks, such as division in private networks for workers and guest networks for customers. This enhances the security and persistent network connectivity, and security policy enforcement. For example, consider there is worker A who is using the PC whose security level is high due to AES, and guest B who is using the portable gaming device that security level is low because of using WEP. If they use the same SSID, then the issue of unification of security in the lower level is caused. In a word, A's PC security AES will be graded down to the security of B's gaming device security WEP. This problem is solved by multiple SSID because the SSID handles AES will be available for A's PC, and SSID handles WEP will be available for B's gaming device. Similar cases always happen in school, that school staffs are administering a lot of personal information such as student phone number, address, ID, etc with the SSID and students are normally using SSID for basic actions such as games on mobile phones, daily conversations via chatting app among families or friends, so while guests use low security level SSID, staffs can use higher security level SSID. Furthermore the IT department could also be doing traffic dividing which means having a few SSID dedicated for the 2.4GHz for longer reaching connection devices and connecting devices for low bandwidth activities like browsing google , youtube etc. And some SSID split into 5 GHZ as its the well suited for high-bandwidth communication devices or activities that require high-bandwidth In conclusion, the IT department decided to broadcast several SSID instead of just using a single SSID for better security on each individual device network, and stability; and help divide traffic to satisfied different user needs for their application

e.





Two graphs from afrihost Help Center

The situation of which network to use varies. The 2.4 GHz radio wave is slower but has a longer range of travel distance, and higher interference. Nevertheless, 5 GHz radio waves are faster but have a shorter range of travel distance, and lower interference.

Therefore, if we are near an access point and no obstacles among us, 5 Ghz will be suitable to use. On the other hand, if we are in a different room with an access point or have a couple of obstacles among us and access point for example, it is better to use 2.4 GHz for more stable network connectivity.

In conclusion, users should pick 2.4GHz for a consistent, stable network connectivity, and if the users need a higher speed or performance, 5GHz band is the best choice to pick but we also have to take into consideration of the coverage range.

f.

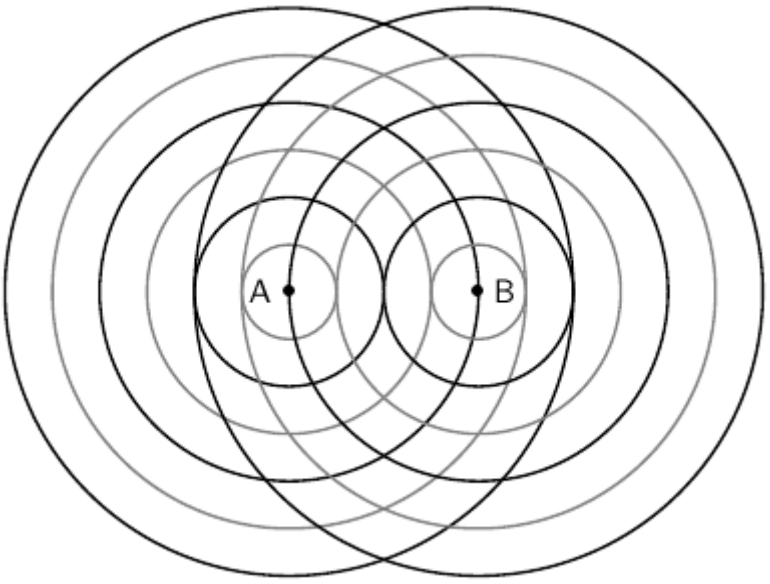


Diagram of two Wi-Fi signals interfering with each other.

Wi-Fi signals are wireless, sending and receiving waves for communication. Therefore, the WIFI signal broadcasted by the router possibly interfered with another signal like in the picture above. This will cause the worst cases, network connectivity drop or decrease of power of connectivity because two different signals are interfering and offset each other.

To avoid these effects, it is highly recommended to keep a enough distance among different routers sending different signals, or separate each signal to 2.4 and 5, but do not use both.

g. WPA2 with AES-CCMP is already suitable as a security for the network.

As already mentioned in above questions, AES-CCMP has three different long, complicated sizes for encryption keys, multiple encryption stages in operations. Thanks to these complex security technologies, WPA2 is already fulfilling an intensive level of user information protection.

Of course WPA2 also has its own vulnerability. The potential vulnerability WPA2 has is called KRACKs. This was discovered by the university in Belgium, the thesis was published in 2017. According to the research study of KRACKs, hackers can pretend on both client side and server side, so to deceive a client as hackers are the server side, a server as hackers are the client side. So both sides cannot detect the existence of hackers, and hackers can gather non-encrypted information easily.

Nevertheless, the new firmware to cope with KRACKs is already released 2 months later from the research study report, so current risk is not as much as old-fashioned security systems. Users can prevent unauthorized interception of communications by anonymous third-party. Furthermore, it is quite difficult to make bad use of the KRACKs. Normally students just access the student portal and exchange chats with their friends, classmates, and so on, so they are not exchanging confidential privacies as much as in the business. Eventually, WPA2 with AES-CCMP is enough as security due to the complexity of abuse, and the importance of information students access and exchange.

5.

We have researched 6G technology infrastructure that might be able to improve the present campus WIFI network either from the aspects of coverage, connectivity experience, security, etc.

6G is also known as the sixth generation mobile system standard. It is a more advanced next-generation mobile communication system than 1G to 5G. With the expeditious international commercialization of 5G beginning around 2020, not only will society be better connected with the enhanced data communication capabilities, but also more devices in most kinds of scenarios in business and education will be connected, moving from an era of connected society (4G) to one of connected everything (5G). Following this trend and idiosyncrasy of 5G, 6G will provide a better network connectivity for people and things, and will invigorate the flow of trend to a smart society with IoT, continuing the transformation from connection among people and things (5G) to connection among not only things, but also intelligence and senses.

However, there are also a couple of challenges. Because the capability and ability will be intensively enhanced than 5G, the hardware and infrastructure are expected to be luxurious to introduce. Furthermore, the security issue is not established until people can use it safely and with peace of mind.

In the world, the network has been evolved from 1G to 5G until now, 2022. The first generation is also known as 1G, launched by Nippon Telegraph and Telephone, introduced to the public consumers in the

1970s. It uses analog signals, and the users of this network could freely call with other users within the network. Nevertheless, the speed was limited to 2.4kB per second, and the security system was not established so the information preservation was critically fragile. Therefore, the second generation, also known as 2G, launched on the Global System for Mobile Communications in 1991. SMS or MMS were introduced with this network, and from the 2G network, digital signals have been used. But the speed was still as low as 5 kB per second, and the security was still vulnerable.

Third generation was released in Japan by NTT DoCoMo in 2001, enabling high-speed internet service, watching videos online through YouTube, sending mails, video calling, and so on. The connectivity speed also improved dramatically, the range is from 144 kb per second to maximum 2 Mb per second. Fourth generation enabled cloud computing, video live streaming etc. and the speed also increased until the range of 1Gb per second. Security has also dramatically enhanced. Now, the fifth generation network is on the stage of developing since 2019, the network known as ridiculously faster than the 4G network.

The communication speed and capacity of 6G is also endless compared to 5G. Even the minimum bandwidth of 5G was 100 MHz, but 6G will cover from 500MHz to 1 GHz as the most "cost-effective" way for wide network coverage. Furthermore, the mmWave bands will be mature and popular in 6G, which the bandwidth is roughly 40 to 50 thousands of GHz. The 6G bandwidth will reach the THz in maximum, for AI and sending, and communication. These bands will be provided from artificial satellites and core network centers to cover 99.9999999...% of all over the world, providing network connectivity to the people.

6G has a lot of usages and applications in the real world.

- **eMBB+**

  eMBB+ is the enhanced mobile broadband that advanced from 5G eMBB. It is for humanistic communication use cases, will enable exceedingly mesmeric experience and multimodal interactions in the XR applications such as AR, VR and MR.

- **Glass-free 3D displays**

  Visual accommodation is expected to be the next innovative solution, relying on the techniques such as a light field and a holographic display. Such displays would allow users to see far-away family members up close without wearing luxurious

glasses we see sometimes in the catalog, delivering an mesmeric and authentic experience.

- **mMTC+**

  mMTC+ is the resumed evolution of the 5G massive machine type of communication (mMTC) which is characterized by the massive number of lightly connected devices with sporadic traffic in a wide variety of situations such as healthcare, smart cities, transportation, buildings, manufacturing, agriculture, etc.

- **Smart healthcare**

  As the mobile communication system evolves, the system will enable a wide variety of new use cases to emerge. Smart healthcare is one example, involving dynamic monitoring of personal health, remote diagnosis and pathology inference, holographic medical and rehabilitation activities, and telesurgery. In particular, with the new sensing and AI capabilities in 6G, real-time analysis on patient data can prove exceptionally beneficial. Moreover, use cases such as remote diagnosis and tele-surgery will significantly reduce the pressure for an aging population, especially in rural regions that lack sufficient medical resources.

- **URLLC+**

  The usage scenario is the continuous development of 5G ultra-reliable low-latency communications (URLLC) for critical MTC (machine-type communication) in Industry 4.0 and beyond. It also applies to new applications enabled by the everywhere utilization of robots, UAVs, and new HMIs (human-machine interfaces) in manufacturing, public service, autonomous automobile driving, household management, and so on.

- **Collaborative robots in groups**

  In factories of the future, almost all of the major, simple works will be performed by robots instead of humans. During production, a myriad of types of robots — such as automated guided vehicles (AGVs) and drones — will transport things such as raw materials, spares, and accessories from warehouses to production lines. For large or heavy things, multiple robots will collaborate to transport them together — this is known as collaborative carrying.

- **Sensing**

Networked sensing creates a new type of usage scenario beyond communication. It covers a range of use cases such as localization for device-based or even device-free targets, imaging, environment reconstruction and monitoring, and gesture and activity recognition.

- **High-accuracy localization and tracking**

  High-accuracy 3D localization and tracking down to the centimeter level scale allows significant association between the cyber information and locations of physical entities. As such, this will make various applications practicable, across from factories to warehouses, hospitals to retails, and agriculture to mining. For instance, this could enable robots in an automated factory to easily repair parts on a warehouse shelf and install them accordingly.

- **Artificial Intelligence**

  AI aims to connect distributed intelligent agents efficiently and wisely in order to snowball large-scale deployment of AI in all industry fields. High capacity, spectrally efficient, and lower delay transmission for distributed learning — including data and model parameter exchange among large numbers of intelligent agents — is expected for real-time AI.

- **AI-enhanced network automation**

  Recently, mobile networks need huge workforces for operation, administration and maintenance of networks (OA&M). For this, AI has great potential to compensate and undertake this major labor and financial cost. For example, the network system itself can conduct, manage, and operate network configurations and function deployment. Traditional Manual passive OA&M will evolve into zero-touch proactive OA&M — for example, by using predictive network analytic services and end-to-end system OA&M across all technical domains.

These are popularly expected usages in the future.

The 6G network communicates with the enhanced access points, network stations and antennas, and topologies will be used. Satellites, HAPS and electricity factories will send the wave to the network stations, the network stations will receive the bands with the Ultra-Massive MIMO technology. Then the network will be distributed to the small cell access points, which individuals such as humans, schools, will use in daily life.

Based on this, we have designed a thinkable application case on campus. First, the network station belonging to the city receives the bands, sends the network to the small cell access points in the campus. Then the access point will distribute DHCP to the smart devices in the campus and enable users to use the internet via the network. The structure and flows seem to be exactly the same as our campus's current network topology, but the access points and network station are enhanced, the Ultra-Massive MIMO technology is used in this topology and this will enormously increase the network speed then 4G or 5G. Due to the network improvement in campus, interactive lectures or improving senses with metaverse or horogram will be available in the future.

On the other hand, because it is still in the conceptual stage, 6G has potential uncertainties in several areas, especially in terms of security. First, since 6G will be much more publicly open than 4G and 5G have been to date, the IPsec, firewalls, WPA series systems, and AES-CCMP encryption systems used in conventional security measures may lose significant effectiveness.

For this reason, a security model called "Zero Trust" is proposed, which involves mutual authentication, including verification of the identity and integrity of devices without boundaries, without trusting them at all, even if they are connected to an authorized network or verified in advance. With respect to the actual security technology being devised based on this model, Homomorphic encryption, lattice-based cryptography etc. are studied, but there are no security systems that have been proven to be solidly reliable, and more research needs to be done for the future.

Due to these tips and reasons, we will propose the 6G network technology as the future technology that can improve the present campus WIFI network.

Reference

Reinhardt, H. (2021) *From 1G to 5G: A Brief History of the Evolution of Mobile Standards*. (online). Available at: From 1G to 5G: A Brief History of the Evolution of Mobile Standards | Brainbridge

Galazzo, R. (2022) *Timeline from 1g to 5G: A brief history on cell phones.* (online). Available at: Timeline from 1G to 5G: A Brief History on Cell Phones - CENGN

Rajiv. (2022) *Evolution of wireless technologies 1G to 5G in mobile communication.* (online). Available at: Evolution of wireless technologies 1G to 5G in mobile communication - RF Page

Impact of 4G/5G/6G in Education. (online). Available at: MADSmania - Impact of 4G/5G/6G in Education

AES-CCMP, *Encyclopedia in PCmag*. (online). Available at: Definition of AES-CCMP | PCMag

Eric, M. (2015) *Why is almost everything negative in Wireless?*. (online). Available at: Why is almost everything negative in Wireless? - Cisco Community

tp-link. (2022) *How to configure Multi-SSID mode of the Wireless N Access Point (new logo)*. (online). Available at: How to configure Multi-SSID mode of the Wireless N Access Point (new logo) | TP-Link

CenturyLink. () *The difference between 2.4 GHz and 5 GHz WiFi*. (online). Available at: Should I use 2.4 GHz or 5 GHz WiFi? | CenturyLink

Shimaa A. Abdel Hakeem. (2022) 'Security Requirements and Challenges of 6G Technologies and Applications'. *National Library of Medicine: National Centre for Biotechnology Information*. 22(5). Available at: Security Requirements and Challenges of 6G Technologies and Applications - PMC (nih.gov)

==========【Academic Paper referred in Section E Question 5】==========

Huawei Technologies Co., LTD. (2022) *6G: The Next Horizon -From Connected People and Things to Connected Intelligence*. (Online). Available at: https://www-file.huawei.com/-/media/corp2020/pdf/tech-insights/1/6g-white-paper-en.pdf?la=en