Local Network Analysis

Note :

We have provided you with these files for local network analysis part **:**
1 automation_code.py
2 output.csv
3 Hosts_and_Servers.pdf
4 OS_discovered.pdf

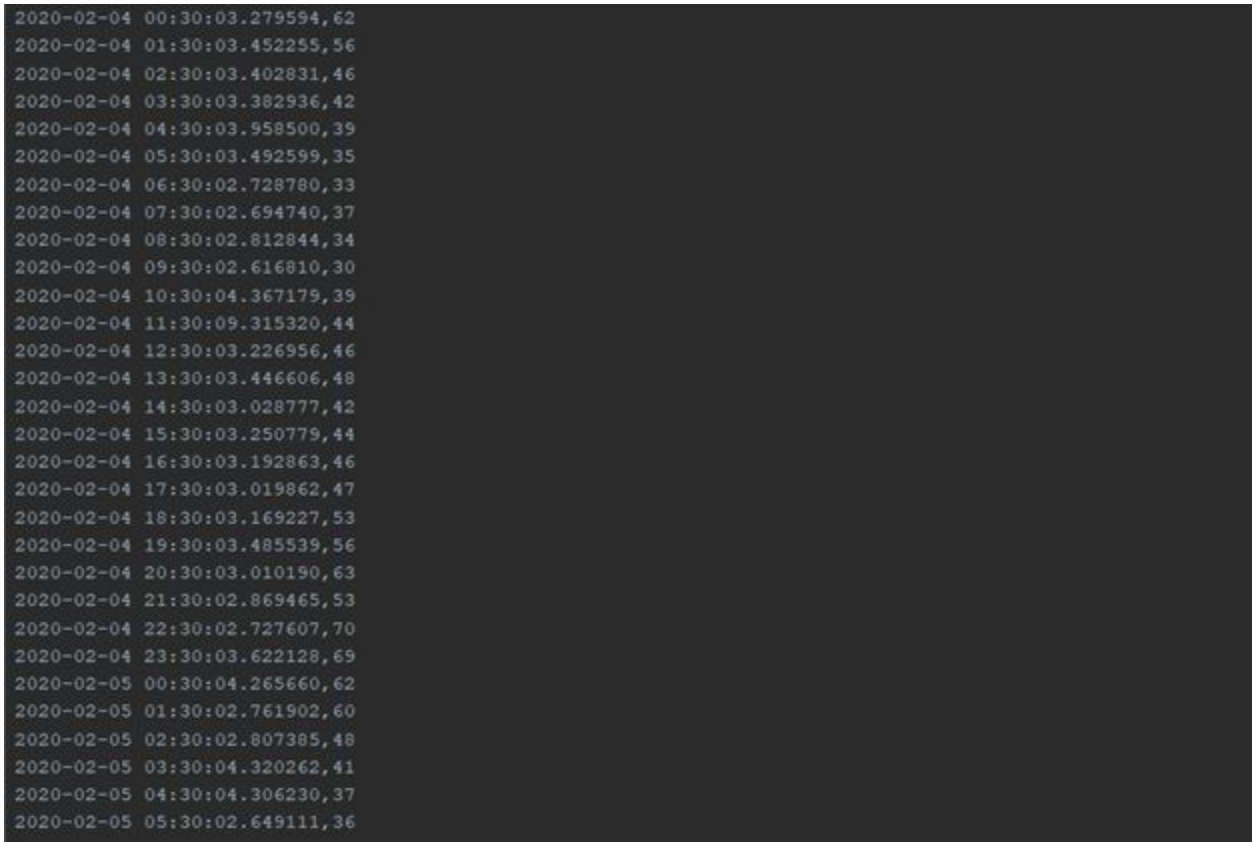
Command details :

Nmap: Nmap is a handy network diagnostics tool that can be used to discover which hosts are online in the network, ports open on these hosts, etc.

CIDR Addressing: Classless inter-domain routing (CIDR) is a set of Internet protocol (IP) standards that are used to create unique identifiers for networks and individual devices. The IP addresses allow particular information packets to be sent to specific computers. CIDR IP addresses consist of two groups of bits. The MSB is the network address, and it is used to identify a network or a sub-network (subnet). The LSB is the host identifier. The host identifier is used to determine which host or device on the network should receive incoming information packets.

<u>The number of hosts online over the duration of the tests</u>:

The below picture shows hosts online for one day. Separate output.csv has been provided to view for all 5 days :



```
2020-02-04 00:30:03.279594,62
2020-02-04 01:30:03.452255,56
2020-02-04 02:30:03.402831,46
2020-02-04 03:30:03.382936,42
2020-02-04 04:30:03.958500,39
2020-02-04 05:30:03.492599,35
2020-02-04 06:30:02.728780,33
2020-02-04 07:30:02.694740,37
2020-02-04 08:30:02.812844,34
2020-02-04 09:30:02.616810,30
2020-02-04 10:30:04.367179,39
2020-02-04 11:30:09.315320,44
2020-02-04 12:30:03.226956,46
2020-02-04 13:30:03.446606,48
2020-02-04 14:30:03.028777,42
2020-02-04 15:30:03.250779,44
2020-02-04 16:30:03.192863,46
2020-02-04 17:30:03.019862,47
2020-02-04 18:30:03.169227,53
2020-02-04 19:30:03.485539,56
2020-02-04 20:30:03.010190,63
2020-02-04 21:30:02.869465,53
2020-02-04 22:30:02.727607,70
2020-02-04 23:30:03.622128,69
2020-02-05 00:30:04.265660,62
2020-02-05 01:30:02.761902,60
2020-02-05 02:30:02.807385,48
2020-02-05 03:30:04.320262,41
2020-02-05 04:30:04.306230,37
2020-02-05 05:30:02.649111,36
```

Command used: **nmap -n -sP [ipaddress]/24**

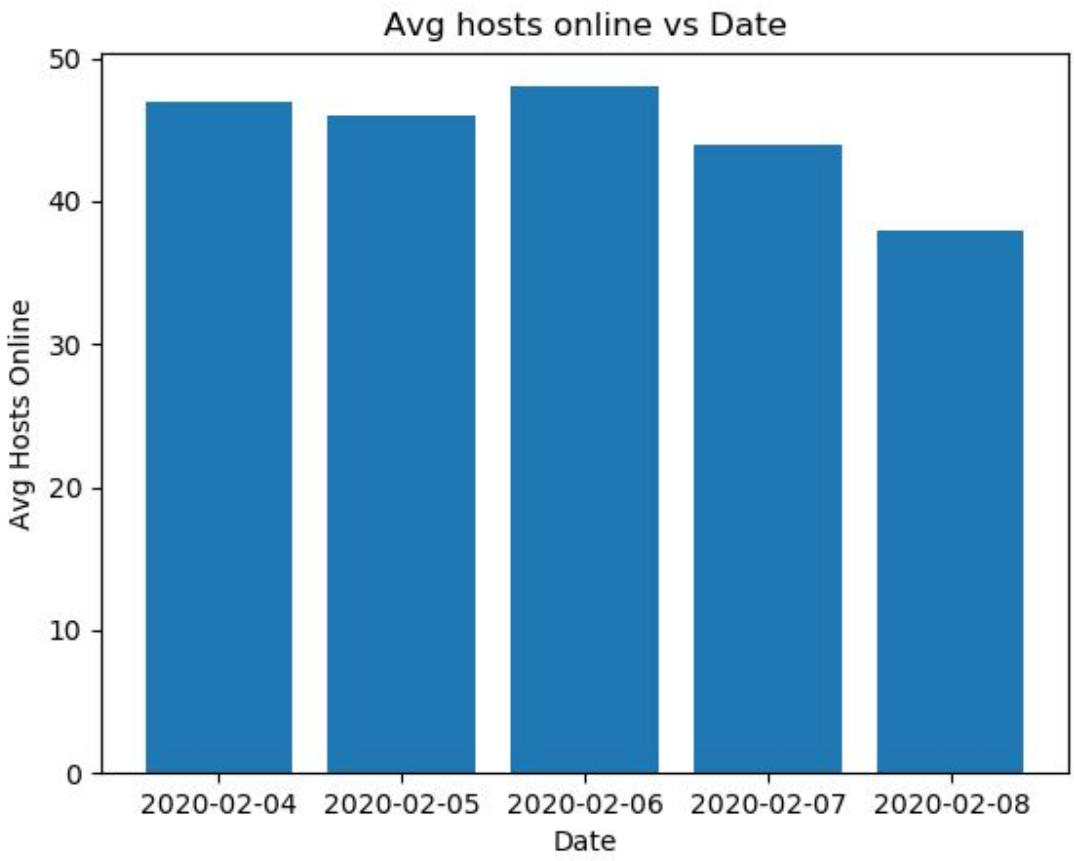
Observations:

1. No.of hosts online from 2:00 am – 9:00 am is low. This is because most of the students will be sleeping in this interval.

2. No.of hosts online from 9:00 am – 6:30 pm is near to the average of hosts that day. This is because most of the students will be attending the classes between this interval of time.

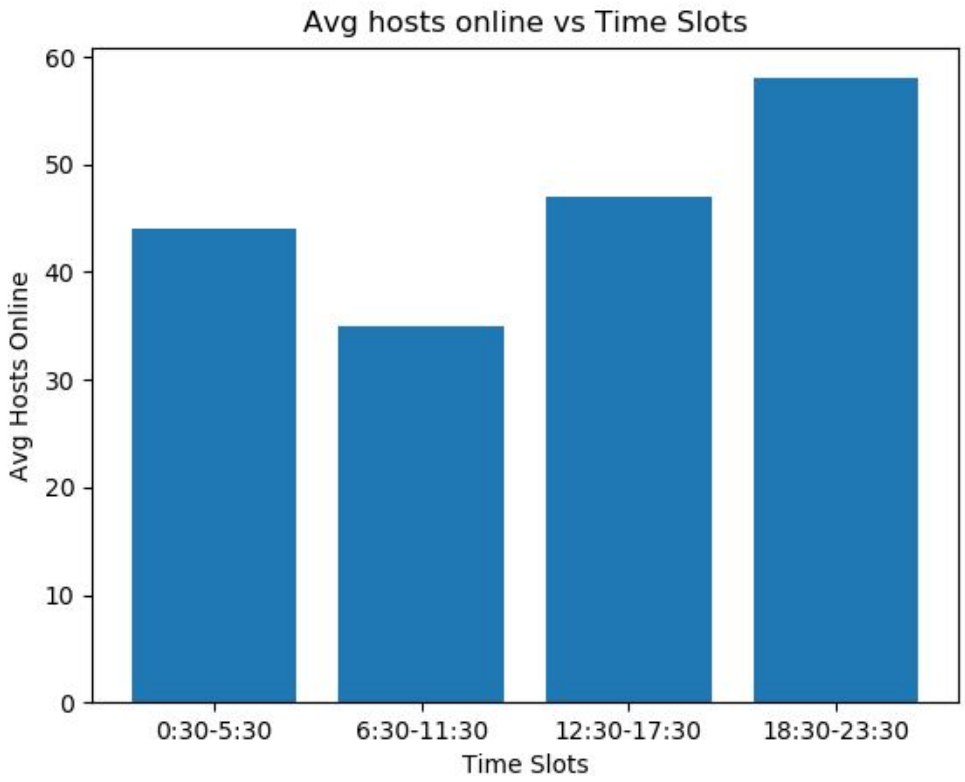
3. No.of hosts online from 6:30 pm – 2:00 am is high. This is because most of the students will be free and in the rooms in this interval of time.

Graphs:



Graph 2:

Graph showing the pattern of average hosts online for each day when the experiment was done in different time slots.

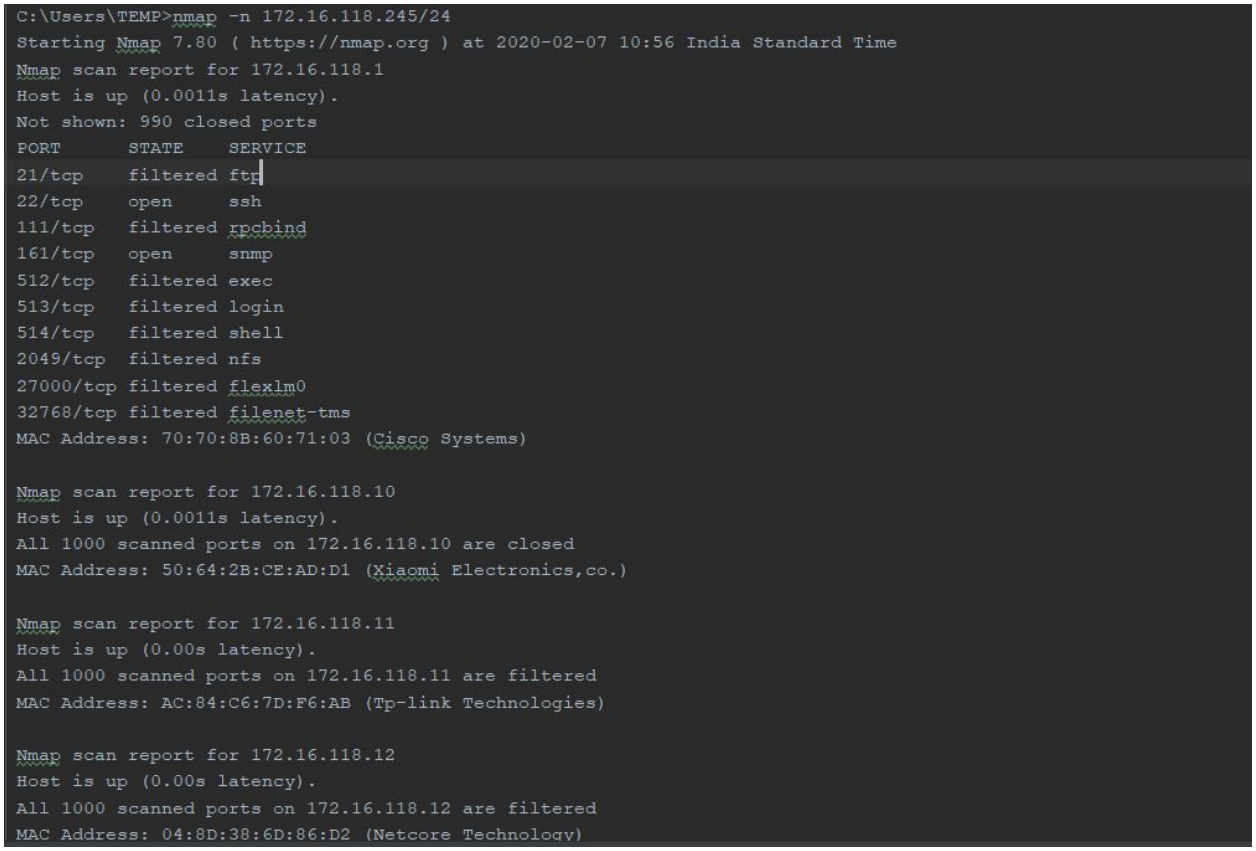


List of hosts and servers discovered on LAN:

Command used: **nmap -n [ipaddress]/24**

Below shown are some of the OS discovered by the command mentioned above.

Hosts_and_servers.pdf has been provided separately to view all.



```
C:\Users\TEMP>nmap -n 172.16.118.245/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-07 10:56 India Standard Time
Nmap scan report for 172.16.118.1
Host is up (0.0011s latency).
Not shown: 990 closed ports
PORT      STATE    SERVICE
21/tcp    filtered ftp
22/tcp    open     ssh
111/tcp   filtered rpcbind
161/tcp   open     snmp
512/tcp   filtered exec
513/tcp   filtered login
514/tcp   filtered shell
2049/tcp  filtered nfs
27000/tcp filtered flexlm0
32768/tcp filtered filenet-tms
MAC Address: 70:70:8B:60:71:03 (Cisco Systems)

Nmap scan report for 172.16.118.10
Host is up (0.0011s latency).
All 1000 scanned ports on 172.16.118.10 are closed
MAC Address: 50:64:2B:CE:AD:D1 (Xiaomi Electronics,co.)

Nmap scan report for 172.16.118.11
Host is up (0.00s latency).
All 1000 scanned ports on 172.16.118.11 are filtered
MAC Address: AC:84:C6:7D:F6:AB (Tp-link Technologies)

Nmap scan report for 172.16.118.12
Host is up (0.00s latency).
All 1000 scanned ports on 172.16.118.12 are filtered
MAC Address: 04:8D:38:6D:86:D2 (Netcore Technology)
```

OS running on the computers:

Command used: **nmap -n -O [ipaddress]/25**

Below shown are some of the OS discovered by the command mentioned above.

OS_discovered.pdf has been provided separately to view all.

Gateways and DNS servers used in different parts of Campus:

Gateway Server: A gateway is a node (router) in a computer network, a key stopping point for data on its way to or from other networks.

DNS server: The Domain Name System (DNS) is the phonebook of the Internet. When users type domain names such as ‘google.com’ into web browsers, DNS is responsible for finding the correct IP address for those sites. Browsers then use those addresses to communicate with original servers to access website information.

HOSTEL LAN:

DNS: 172.16.0.30, 4.2.2.2

Gateway: 172.16.118.1

Wireless:

DNS: 172.16.0.30, 4.2.2.2

Gateway: 172.16.225.1

CC LABS:

DNS: 127.0.1.1

Gateway: 172.16.4.1