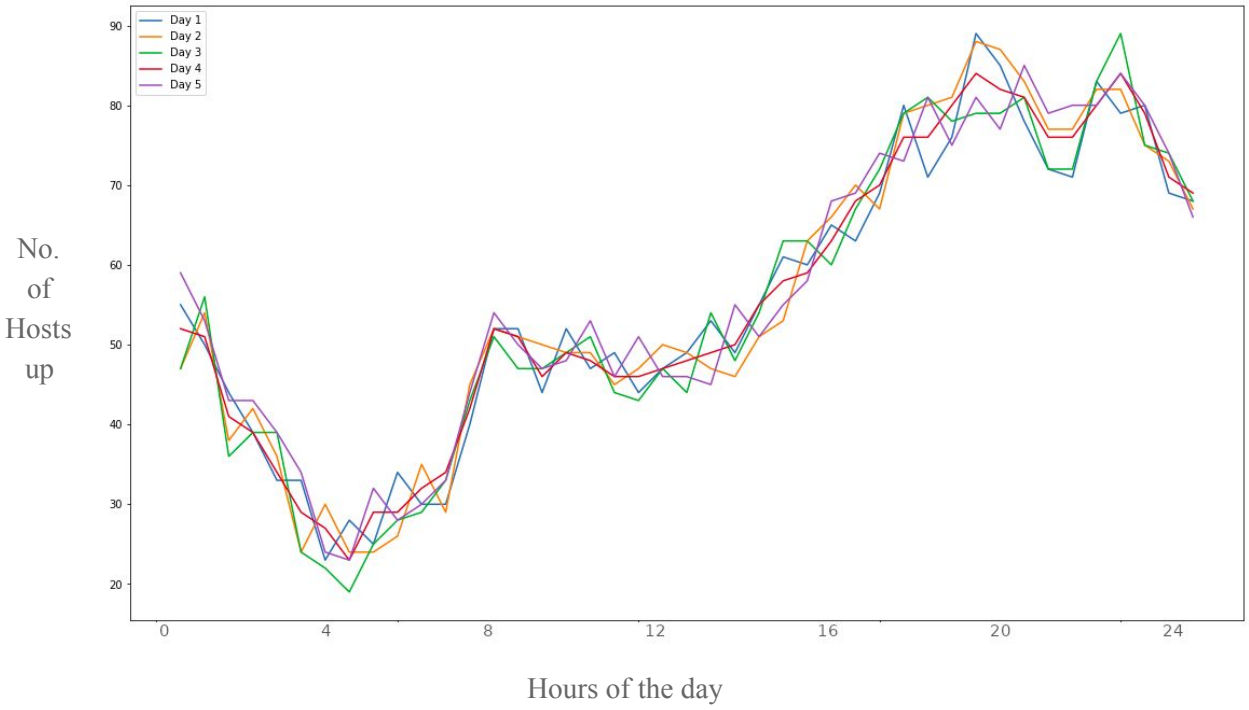
CS F303 - Computer Networks
Assignment 1

Ekanshi Agrawal	Kushagra Srivastava	Kunal Verma	Sandesh Thakar
2017A7PS0233H	2017A7PS0146H	2017A7PS0120H	2017A7PS0181H

Question 2.

1. ***Number of hosts observed online over the duration of the tests performed.***



The above graph shows the trends in the number of hosts that are up on the LAN during different times of the day. The x-axis shows the hours of the day, while the y-axis shows the number of hosts online.

Details:

- The data was recorded from the 2nd of Feb to the 6th of Feb, 2020. The above graph shows the trends observed on each of these days, depicted by lines coloured in blue, orange, green, red, and purple respectively in order of days.
- It was observed that most hosts tend to be up during night time, with a slight dip at around 8-10pm, which could be due to dinner or other campus activities. Further, a low point in host activity is observed at around 3-4am, after which a sudden spike is observed between 7-8am, which could be correlated to the fact that some people tend to wake up around that time and work on their machines.

- This data was generated by the script `hosttrack.py`, invoked twice per hour by running `hosttrack.sh` (in the /src folder of this assignment). `hosttrack.sh` takes two command line arguments: the subnet to be probed and the frequency.
- To record the data, we ran the bash script (with sudo) on a /24 block (256 addresses) and frequency of 2 (i.e, twice per hour). The data was stored in a .csv file, which can be found in the same folder, in the format [current datetime, number of hosts up]

2. ***List of hosts and servers discovered on LAN:***

➔ Hosts Discovered: (using the command: `sudo nmap -n <ip>/24`)

```
Nmap scan report for 172.16.38.1
Host is up (0.00013s 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

Nmap scan report for 172.16.38.58
Host is up (0.00070s latency).
Not shown: 976 closed ports
PORT    STATE    SERVICE
1/tcp   filtered tcpmux
32/tcp  filtered unknown
444/tcp   filtered snpp
631/tcp   filtered ipp
898/tcp   filtered sun-manageconsole
1031/tcp  filtered iad2
1052/tcp  filtered ddt
1063/tcp  filtered kyoceranetdev
1090/tcp  filtered ff-fms
1131/tcp  filtered caspssl
1149/tcp  filtered bvtsonar
2038/tcp  filtered objectmanager
3306/tcp  open   mysql
4129/tcp  filtered nuauth
5190/tcp  filtered aol
5221/tcp  filtered 3exmp
6547/tcp  filtered powerchuteplus
8654/tcp  filtered unknown
9485/tcp  filtered unknown
9618/tcp  filtered condor
20005/tcp filtered btx
32781/tcp filtered unknown
49160/tcp filtered unknown
```

```
52822/tcp filtered unknown

Nmap scan report for 172.16.38.60
Host is up (0.00072s latency).
All 1000 scanned ports on 172.16.38.60 are closed

Nmap scan report for 172.16.38.61
Host is up (0.00065s latency).
Not shown: 993 closed ports
PORT    STATE    SERVICE
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
1110/tcp  filtered nfsd-status
2869/tcp  filtered icslap
3389/tcp  filtered ms-wbt-server
19780/tcp filtered unknown

Nmap scan report for 172.16.38.62
Host is up (0.00030s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
902/tcp open  iss-realsecure

Nmap scan report for 172.16.38.63
Host is up (0.00034s latency).
All 1000 scanned ports on 172.16.38.63 are closed

Nmap scan report for 172.16.38.78
Host is up (0.00065s latency).
Not shown: 971 closed ports, 27 filtered ports
PORT    STATE SERVICE
53/tcp  open  domain
445/tcp open  microsoft-ds

Nmap scan report for 172.16.38.119
Host is up (0.00023s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap scan report for 172.16.38.123
Host is up (0.00044s latency).
All 1000 scanned ports on 172.16.38.123 are closed

Nmap scan report for 172.16.38.156
Host is up (0.00056s latency).
All 1000 scanned ports on 172.16.38.156 are closed
```

Out of these, by definition, the servers are those hosts with at least one open port.
So the servers are: 172.16.38.1, 172.16.38.58, 172.16.38.61, 172.16.38.62, 172.16.38.78, and 172.16.38.119 (6 servers).
The remaining 4 are hosts.

➔ OS running on the hosts: (using the command: `sudo nmap -n -O <ip>/27`)

```
Starting Nmap 7.60 ( https://nmap.org ) at 2020-02-05 23:03 IST
Nmap scan report for 172.16.126.200
Host is up (0.00059s latency).
All 1000 scanned ports on 172.16.126.200 are closed
MAC Address: 50:3E:AA:9A:D7:D9 (Tp-link Technologies)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for 172.16.126.201
Host is up (0.00092s latency).
Not shown: 997 filtered ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 10:7D:1A:34:D8:10 (Dell)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1
closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Network Distance: 1 hop

Nmap scan report for 172.16.126.203
Host is up (0.00087s latency).
Not shown: 995 filtered ports
PORT    STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi
6646/tcp open  unknown
MAC Address: 80:E8:2C:92:AB:AF (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1
closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows XP (85%)
OS CPE: cpe:/o:microsoft:windows_xp::sp2
Aggressive OS guesses: Microsoft Windows XP SP2 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

Nmap scan report for 172.16.126.221
Host is up (-0.019s latency).
Not shown: 999 filtered ports
PORT    STATE SERVICE
5357/tcp open  wsdapi
MAC Address: A8:1E:84:9F:1D:24 (Quanta Computer)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1
closed port
Device type: specialized|general purpose
Running (JUST GUESSING): AVtech embedded (87%), FreeBSD 6.X|10.X (86%), Microsoft Windows
XP (85%)
OS CPE: cpe:/o:freebsd:freebsd:6.2 cpe:/o:freebsd:freebsd:10.3
```

```
cpe:/o:microsoft:windows_xp::sp2
Aggressive OS guesses: AVtech Room Alert 26W environmental monitor (87%), FreeBSD
6.2-RELEASE (86%), FreeBSD 10.3-STABLE (85%), Microsoft Windows XP SP2 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

Nmap scan report for 172.16.126.222
Host is up (0.00049s latency).
All 1000 scanned ports on 172.16.126.222 are filtered
MAC Address: EC:B1:D7:DB:EB:23 (Hewlett Packard)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for 172.16.126.205
Host is up (0.000094s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
80/tcp open  http
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 32 IP addresses (6 hosts up) scanned in 46.58 seconds
```

Nmap was successfully able to figure out the OS running on one machine, while it provided guesses for a number of other machines. It also seemed to struggle to figure out the OS on various hosts, and took quite some time to scan when provided with a large block (/26 and less, i.e, greater than 32) of addresses. Hence, we have used a /27 block here, which gave results in a reasonable amount of time.

3. *Gateways and DNS servers used in different parts of the campus LAN:*

The ifconfig command is being deprecated in many distributions, due to which it was unable to provide DNS and gateway information. Thus, we used the following commands to find out the local DNS and gateways assigned to machines in various parts of the campus:

DNS: `nmcli dev show | grep DNS`
Gateway: `nmcli dev show <interfacename> | grep GATEWAY`

★ **Wireless: Library**

DNS Servers:

IP4.DNS[1]:	172.16.0.30
IP4.DNS[2]:	8.8.8.8

Gateway:

IP4.GATEWAY:	172.20.0.1
IP6.GATEWAY:	fe80::3c92:f998:cf69:5cff

★ **Ethernet: Shankar Bhawan**

DNS Servers:

IP4.DNS[1]:	172.16.0.30
IP4.DNS[2]:	8.8.8.8

Gateway:

IP4.GATEWAY:	172.16.38.1
IP6.GATEWAY:	--

★ **Ethernet: Malaviya Bhawan**

DNS Servers:

IP4.DNS[1]:	172.16.0.30
IP4.DNS[2]:	8.8.8.8

Gateway:

IP4.GATEWAY:	172.16.126.1
IP6.GATEWAY:	--

★ **Wireless: Malaviya Bhawan**

DNS Servers:

IP4.DNS[1]:	172.16.0.30
IP4.DNS[2]:	8.8.8.8

Gateway:

IP4.GATEWAY:	172.16.225.1
IP6.GATEWAY:	--

★ **Ethernet: CCLab**

DNS Servers:

IP4.DNS[1]:	172.16.0.30
IP4.DNS[2]:	4.2.2.2

Gateway:

IP4.GATEWAY:	172.16.4.1
IP6.GATEWAY:	--