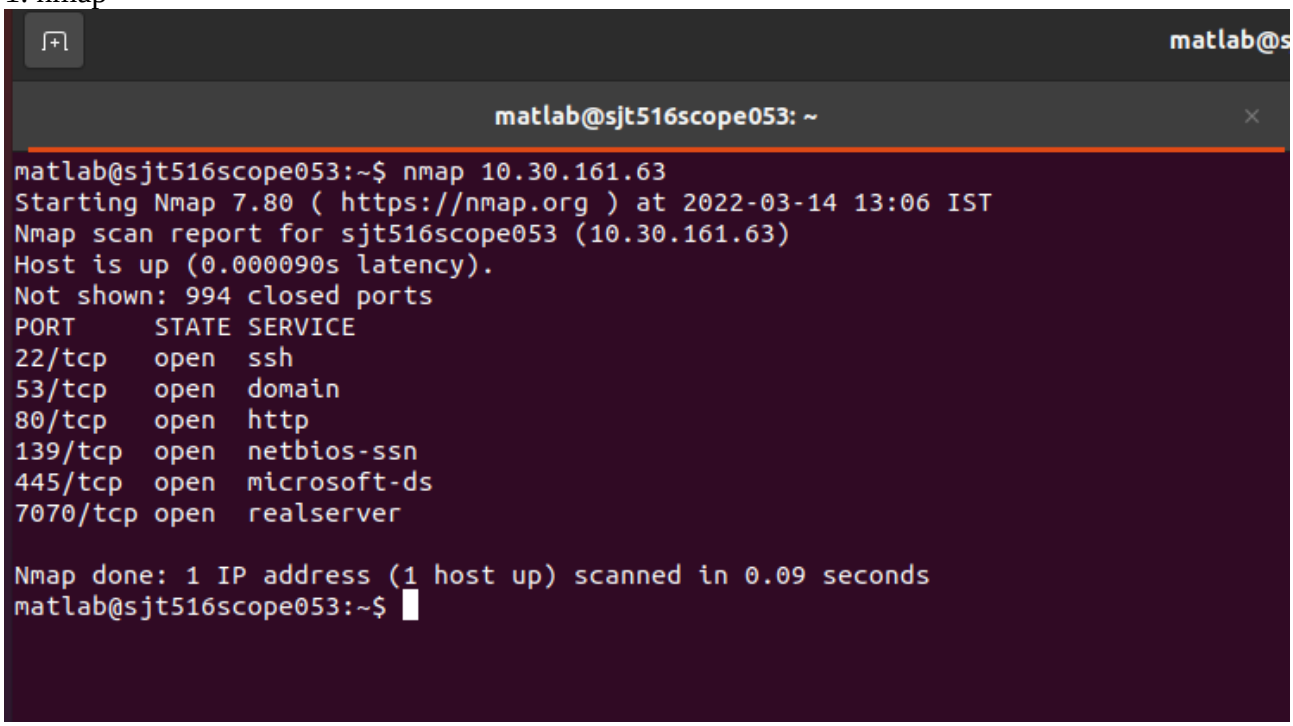
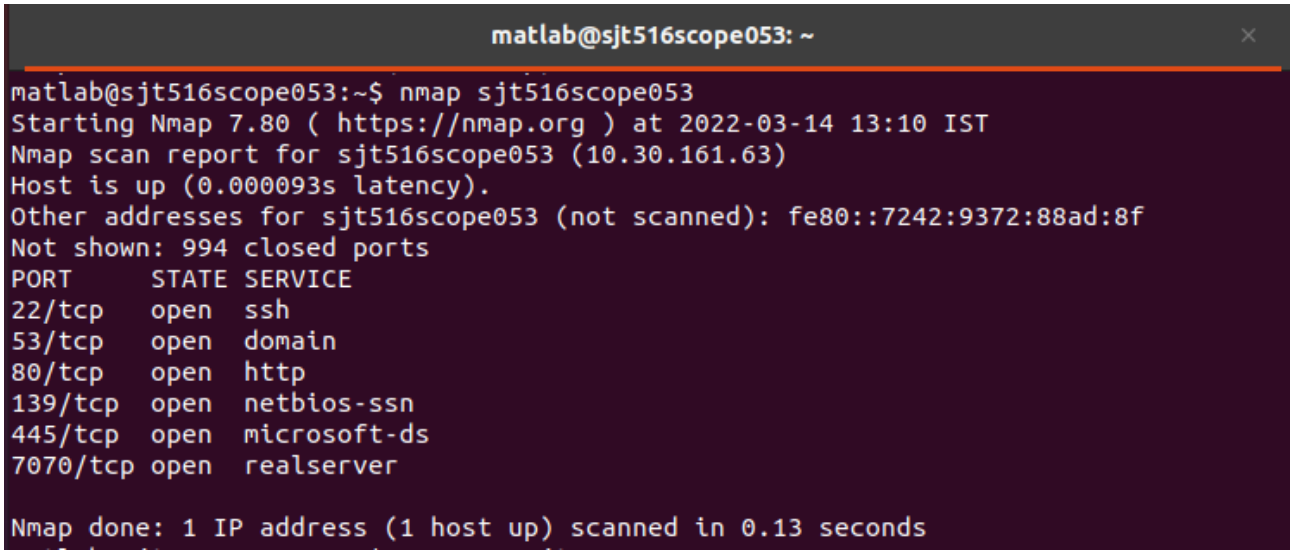
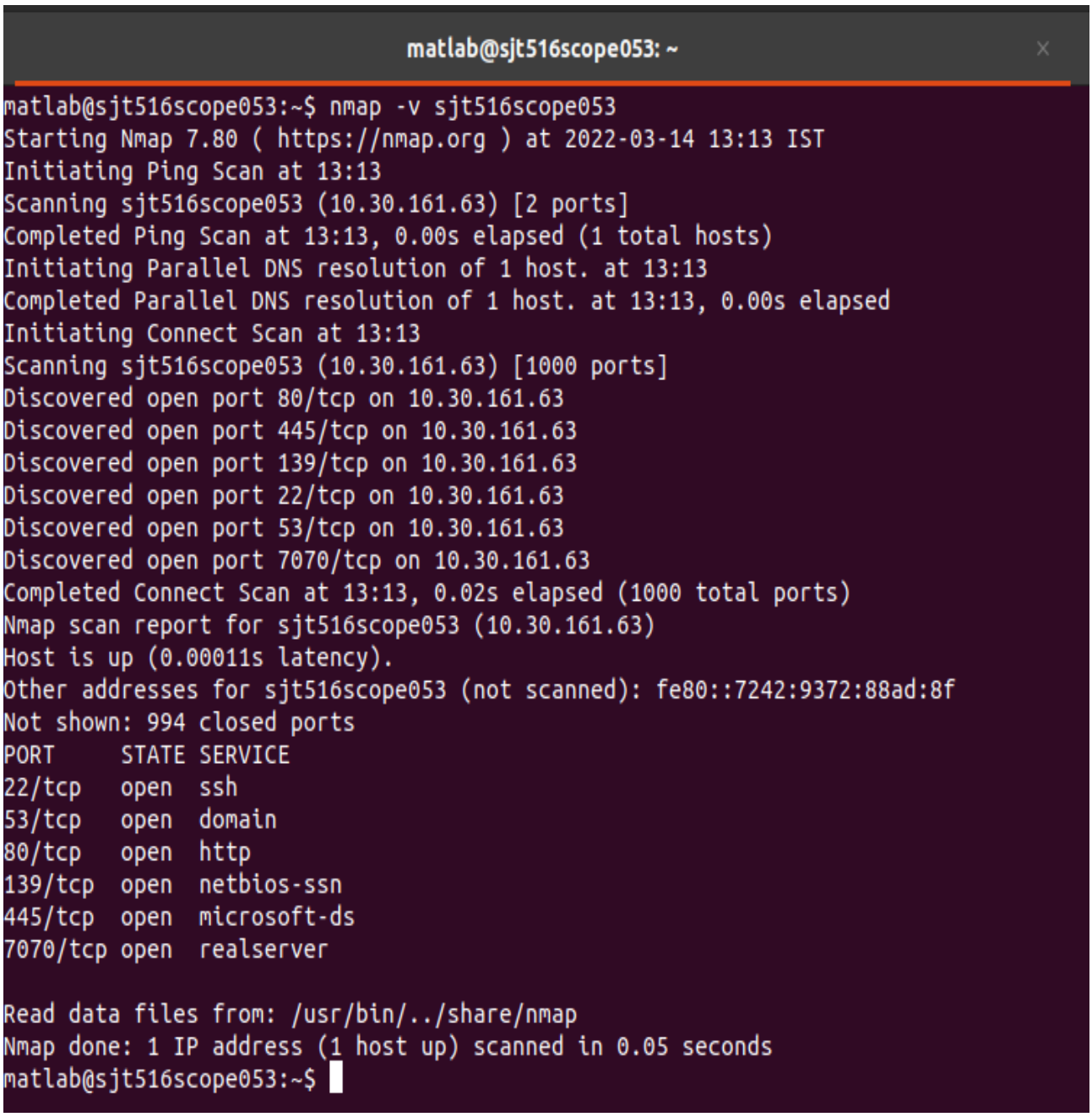
Harshit Srivastava
19BCE0382
Lab Assessment

Information Security Management (CSE3502)
Slot: L5+L6
Prof. Siva Shanmugam G
14/03/2022

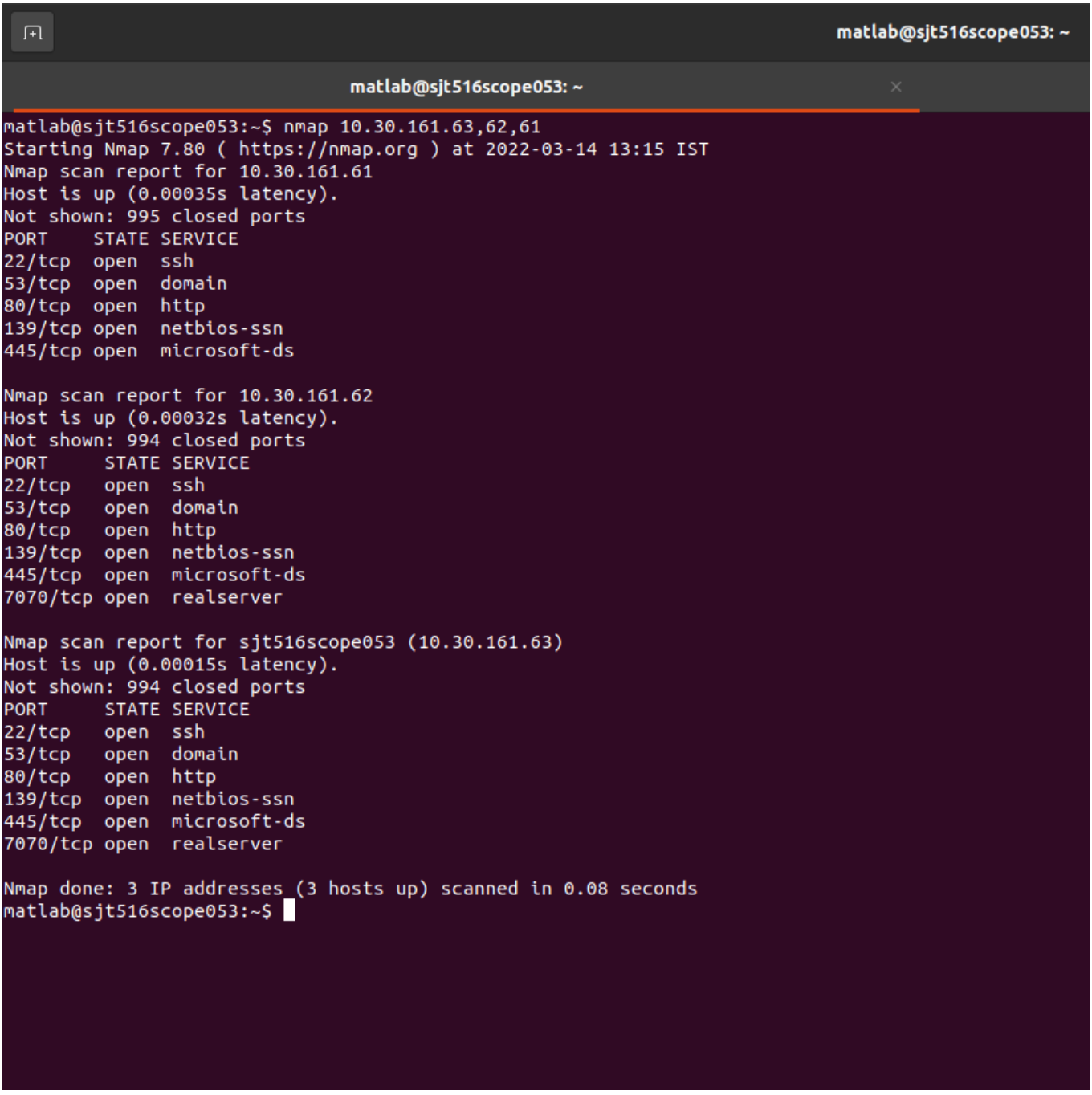
1. nmap



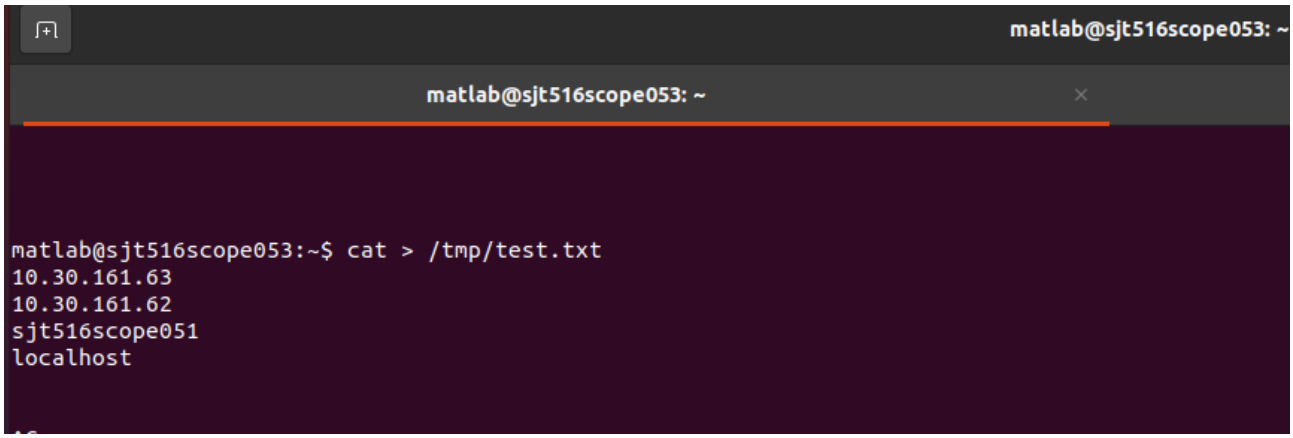



matlab@sjt516scope053: ~
matlab@sjt516scope053:~$ nmap -v sjt516scope053
Starting Nmap 7.80 (https://nmap.org) at 2022-03-14 13:13 IST
Initiating Ping Scan at 13:13
Scanning sjt516scope053 (10.30.161.63) [2 ports]
Completed Ping Scan at 13:13, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:13
Completed Parallel DNS resolution of 1 host. at 13:13, 0.00s elapsed
Initiating Connect Scan at 13:13
Scanning sjt516scope053 (10.30.161.63) [1000 ports]
Discovered open port 80/tcp on 10.30.161.63
Discovered open port 445/tcp on 10.30.161.63
Discovered open port 139/tcp on 10.30.161.63
Discovered open port 22/tcp on 10.30.161.63
Discovered open port 53/tcp on 10.30.161.63
Discovered open port 7070/tcp on 10.30.161.63
Completed Connect Scan at 13:13, 0.02s elapsed (1000 total ports)
Nmap scan report for sjt516scope053 (10.30.161.63)
Host is up (0.00011s latency).
Other addresses for sjt516scope053 (not scanned): fe80::7242:9372:88ad:8f
Not shown: 994 closed ports
PORT STATE SERVICE
22/tcp open ssh
53/tcp open domain
80/tcp open http
139/tcp open netbios-ssn
445/tcp open microsoft-ds
7070/tcp open realserver
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.05 seconds
matlab@sjt516scope053:~$

2. nmap multiple



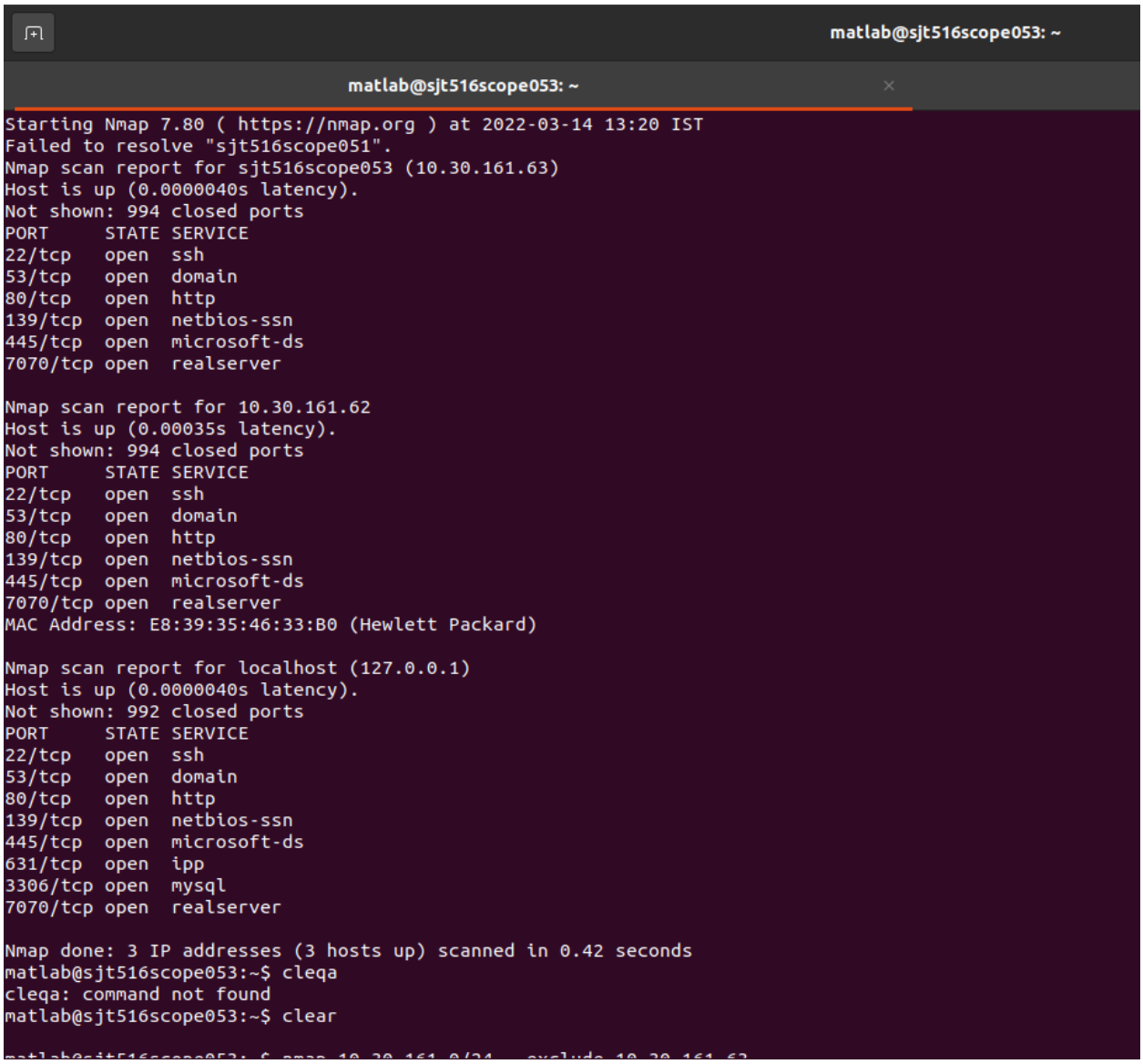
3. Read List



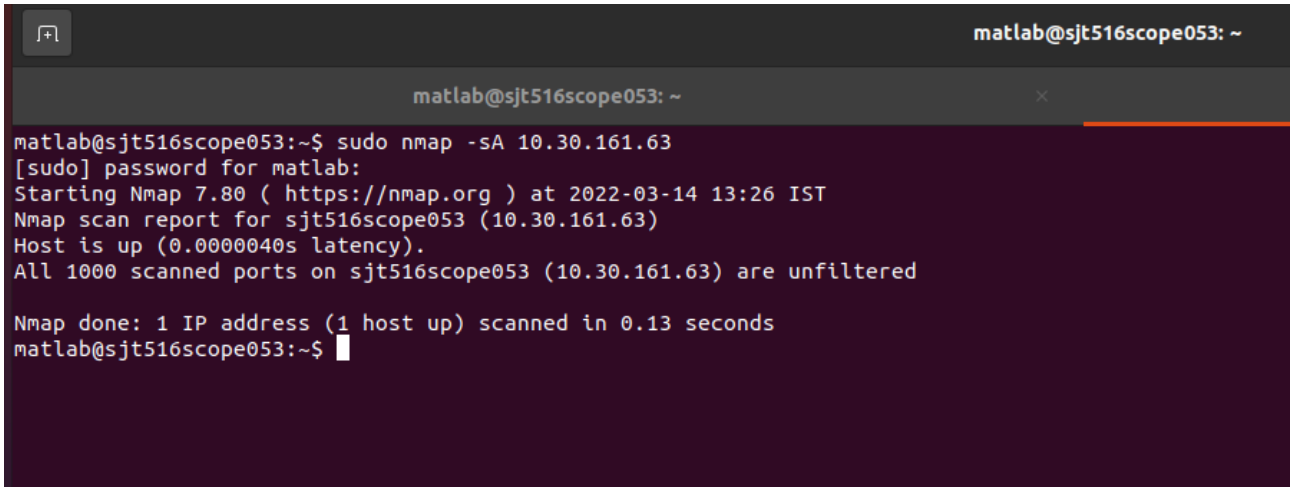
nmap -iL /tmp/test.txt

```
matlab@sjt516scope053:~$ sudo nmap -iL /tmp/test.txt
Starting Nmap 7.80 ( https://nmap.org ) at 2022-03-14 13:20 IST
Failed to resolve "sjt516scope051".
Nmap scan report for sjt516scope053 (10.30.161.63)
Host is up (0.0000040s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
53/tcp   open  domain
80/tcp   open  http
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
7070/tcp open  realserver

Nmap scan report for 10.30.161.62
Host is up (0.00035s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
53/tcp   open  domain
80/tcp   open  http
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
7070/tcp open  realserver
MAC Address: E8:39:35:46:33:B0 (Hewlett Packard)

Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000040s latency).
Not shown: 992 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
53/tcp   open  domain
80/tcp   open  http
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
631/tcp  open  ipp
3306/tcp open  mysql
7070/tcp open  realserver

Nmap done: 3 IP addresses (3 hosts up) scanned in 0.42 seconds
matlab@sjt516scope053:~$
```

4. Exclude


matlab@sjt516scope053: ~
matlab@sjt516scope053: ~
Starting Nmap 7.80 (https://nmap.org) at 2022-03-14 13:20 IST
Failed to resolve "sjt516scope051".
Nmap scan report for sjt516scope053 (10.30.161.63)
Host is up (0.0000040s latency).
Not shown: 994 closed ports
PORT STATE SERVICE
22/tcp open ssh
53/tcp open domain
80/tcp open http
139/tcp open netbios-ssn
445/tcp open microsoft-ds
7070/tcp open realserver
Nmap scan report for 10.30.161.62
Host is up (0.00035s latency).
Not shown: 994 closed ports
PORT STATE SERVICE
22/tcp open ssh
53/tcp open domain
80/tcp open http
139/tcp open netbios-ssn
445/tcp open microsoft-ds
7070/tcp open realserver
MAC Address: E8:39:35:46:33:B0 (Hewlett Packard)
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000040s latency).
Not shown: 992 closed ports
PORT STATE SERVICE
22/tcp open ssh
53/tcp open domain
80/tcp open http
139/tcp open netbios-ssn
445/tcp open microsoft-ds
631/tcp open ipp
3306/tcp open mysql
7070/tcp open realserver
Nmap done: 3 IP addresses (3 hosts up) scanned in 0.42 seconds
matlab@sjt516scope053:~$ cleqa
cleqa: command not found
matlab@sjt516scope053:~$ clear

5. Find out if a host/network is protected by a firewall using namp command



6. Scan a host when protected by the firewall