Name: Shubhan Singh

Class: SE Comps B

Roll no.: 2022300118

CCN Experiment 8

NMAP

Aim: Network Mapping using Nmap

Objective: The objective of this lab assignment is to introduce students to NMAP, a powerful network scanning tool widely used for network discovery and security auditing. Through this assignment, students will gain hands-on experience in using NMAP to scan networks, identify open ports, detect operating systems, and gather valuable information about networked devices.

Requirements:

● Access to a computer with NMAP installed (can be installed on Windows, Linux, or macOS).

● Basic understanding of networking concepts

Tasks:

1. Installation and Setup:

    ○ Install NMAP on your system if not already installed. (https://www.geeksforgeeks.org/nmap-command-in-linux-with-examples/)

    ○ Familiarize yourself with the basic syntax and options of NMAP.

2. Basic Scanning:

    ○ Perform a simple ping scan on a target IP address to determine its availability.

```
psipl@psipl-OptiPlex-3000:~$ nmap 172.16.62.4
Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-20 14:47 IST
Nmap scan report for 172.16.62.4
Host is up (0.0031s latency).
All 1000 scanned ports on 172.16.62.4 are closed

Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
```

    ○ Conduct a TCP SYN scan on a target IP range to identify open ports.

3. Service Version Detection:

    ○ Perform a service version detection scan on a target IP to identify the version of services running on open ports.

4. Operating System Detection:

    ○ Use NMAP to detect the operating system of a target device.

5. Scripting with NMAP:

    ○ Write a simple NMAP script to automate a scanning task of your choice.

Problem Statements:

1. Scan a given network range and identify all active hosts.

```
psipl@psipl-OptiPlex-3000:~$ sudo nmap -sn 172.16.62.4/24
Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-20 14:56 IST
Nmap scan report for _gateway (172.16.62.1)
Host is up (0.0038s latency).
MAC Address: 94:60:D5:E0:F9:23 (Unknown)
Nmap scan report for 172.16.62.4
Host is up (0.0038s latency).
MAC Address: CC:5E:F8:F8:E1:FF (Unknown)
Nmap scan report for 172.16.62.25
Host is up (0.0026s latency).
MAC Address: CC:5E:F8:F8:CF:79 (Unknown)
Nmap scan report for 172.16.62.26
Host is up (0.0026s latency).
MAC Address: CC:5E:F8:F8:CF:79 (Unknown)
Nmap scan report for 172.16.62.43
Host is up (0.00011s latency).
MAC Address: CC:5E:F8:F8:CF:E1 (Unknown)
Nmap scan report for 172.16.62.46
Host is up (0.0061s latency).
MAC Address: CC:96:E5:22:DF:5B (Unknown)
Nmap scan report for 172.16.62.70
Host is up (0.0030s latency).
MAC Address: CC:5E:F8:F9:48:91 (Unknown)
Nmap scan report for 172.16.62.93
Host is up (0.015s latency).
MAC Address: 6C:3C:8C:53:44:A5 (Unknown)
Nmap scan report for 172.16.62.106
Host is up (0.042s latency).
MAC Address: 6C:3C:8C:53:37:0F (Unknown)
Nmap scan report for 172.16.62.218
Host is up (0.0022s latency).
MAC Address: 6C:3C:8C:53:43:8C (Unknown)
Nmap scan report for 172.16.62.245
Host is up (0.0015s latency).
MAC Address: 6C:3C:8C:53:43:26 (Unknown)
Nmap scan report for psipl-OptiPlex-3000 (172.16.62.198)
Host is up.
Nmap done: 256 IP addresses (12 hosts up) scanned in 2.29 seconds
psipl@psipl-OptiPlex-3000:~$
```

2. Identify the top 5 most commonly open ports on a specific target.

```
psipl@psipl-OptiPlex-3000:~$ sudo nmap --top-ports 5 172.16.62.4
Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-20 14:58 IST
Nmap scan report for 172.16.62.4
Host is up (0.0027s latency).

PORT    STATE  SERVICE
21/tcp  closed ftp
22/tcp  closed ssh
23/tcp  closed telnet
80/tcp  closed http
443/tcp closed https
MAC Address: 6C:3C:8C:53:43:62 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
psipl@psipl-OptiPlex-3000:~$
```

3. Determine the MAC address of a target device using NMAP.
   (given in previous output)
4. Perform a scan to detect the presence of HTTP and HTTPS services on a target network.

```
psipl@psipl-OptiPlex-3000:~$ sudo nmap -p 80,443 172.16.62.4/24
Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-20 15:00 IST
Nmap scan report for _gateway (172.16.62.1)
Host is up (0.0016s latency).

PORT    STATE  SERVICE
80/tcp  closed http
443/tcp closed https
MAC Address: 94:60:D5:E0:F9:23 (Unknown)

Nmap scan report for 172.16.62.4
Host is up (0.0019s latency).

PORT    STATE  SERVICE
80/tcp  closed http
443/tcp closed https
MAC Address: CC:5E:F8:F8:E1:FF (Unknown)

Nmap scan report for 172.16.62.25
Host is up (0.0030s latency).

PORT    STATE  SERVICE
80/tcp  closed http
443/tcp closed https
MAC Address: CC:5E:F8:F8:CF:79 (Unknown)

Nmap scan report for 172.16.62.26
Host is up (0.0030s latency).

PORT    STATE  SERVICE
80/tcp  closed http
443/tcp closed https
MAC Address: CC:5E:F8:F8:CF:79 (Unknown)

Nmap scan report for 172.16.62.43
Host is up (0.039s latency).

PORT    STATE    SERVICE
80/tcp  filtered http
443/tcp filtered https
MAC Address: CC:5E:F8:F8:CF:E1 (Unknown)

Nmap scan report for 172.16.62.46
Host is up (0.0045s latency).
```

```
PORT    STATE    SERVICE
80/tcp  filtered http
443/tcp filtered https
MAC Address: CC:96:E5:22:DF:5B (Unknown)

Nmap scan report for 172.16.62.70
Host is up (0.011s latency).

PORT    STATE  SERVICE
80/tcp  closed http
443/tcp closed https
MAC Address: CC:5E:F8:F9:48:91 (Unknown)

Nmap scan report for 172.16.62.93
Host is up (0.0017s latency).

PORT    STATE  SERVICE
80/tcp  closed http
443/tcp closed https
MAC Address: 6C:3C:8C:53:44:A5 (Unknown)

Nmap scan report for 172.16.62.106
Host is up (0.0053s latency).

PORT    STATE  SERVICE
80/tcp  closed http
443/tcp closed https
MAC Address: CC:5E:F8:F9:48:91 (Unknown)

Nmap scan report for 172.16.62.218
Host is up (0.013s latency).

PORT    STATE    SERVICE
80/tcp  filtered http
443/tcp filtered https
MAC Address: 6C:3C:8C:53:43:8C (Unknown)

Nmap scan report for 172.16.62.245
Host is up (0.0020s latency).

PORT    STATE    SERVICE
80/tcp  filtered http
443/tcp filtered https
MAC Address: 6C:3C:8C:53:43:26 (Unknown)

Nmap scan report for psipl-OptiPlex-3000 (172.16.62.198)
Host is up (0.000016s latency).

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

Nmap done: 256 IP addresses (12 hosts up) scanned in 3.64 seconds
psipl@psipl-OptiPlex-3000:~$
```

5. Find out if a particular host has FTP service running on it.

```
psipl@psipl-OptiPlex-3000:~$ sudo nmap -p 21 172.16.62.4
Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-20 15:02 IST
Nmap scan report for 172.16.62.4
Host is up (0.0026s latency).

PORT   STATE  SERVICE
21/tcp closed ftp
MAC Address: 6C:3C:8C:53:43:62 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
psipl@psipl-OptiPlex-3000:~$
```

6. Identify the SSH version running on a given host.

```
psipl@psipl-OptiPlex-3000:~$ sudo nmap -sV -p 22 172.16.62.245
Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-20 15:04 IST
Nmap scan report for 172.16.62.245
Host is up (0.0042s latency).

PORT   STATE    SERVICE VERSION
22/tcp filtered ssh
MAC Address: 6C:3C:8C:53:43:26 (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.47 seconds
psipl@psipl-OptiPlex-3000:~$
```

7. Scan a range of IP addresses and list all hosts that have Telnet service running.

```
psipl@psipl-OptiPlex-3000:~$ sudo nmap -p 23 172.16.62.245/24
Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-20 15:05 IST
Nmap scan report for _gateway (172.16.62.1)
Host is up (0.011s latency).

PORT   STATE  SERVICE
23/tcp closed telnet
MAC Address: 94:60:D5:E0:F9:23 (Unknown)

Nmap scan report for 172.16.62.4
Host is up (0.0021s latency).

PORT   STATE  SERVICE
23/tcp closed telnet
MAC Address: CC:5E:F8:F8:E1:FF (Unknown)

Nmap scan report for 172.16.62.25
Host is up (0.0024s latency).

PORT   STATE  SERVICE
23/tcp closed telnet
MAC Address: CC:5E:F8:F8:CF:79 (Unknown)

Nmap scan report for 172.16.62.26
Host is up (0.0052s latency).

PORT   STATE  SERVICE
23/tcp closed telnet
MAC Address: CC:96:E5:22:E1:02 (Unknown)

Nmap scan report for 172.16.62.43
Host is up (0.0035s latency).

PORT   STATE    SERVICE
23/tcp filtered telnet
MAC Address: CC:5E:F8:F8:CF:E1 (Unknown)

Nmap scan report for 172.16.62.46
Host is up (0.0026s latency).
```

```
PORT   STATE    SERVICE
23/tcp filtered telnet
MAC Address: CC:96:E5:22:DF:5B (Unknown)

Nmap scan report for 172.16.62.70
Host is up (0.0051s latency).

PORT   STATE  SERVICE
23/tcp closed telnet
MAC Address: 6C:3C:8C:53:37:0F (Unknown)

Nmap scan report for 172.16.62.93
Host is up (0.0033s latency).

PORT   STATE  SERVICE
23/tcp closed telnet
MAC Address: 6C:3C:8C:53:44:A5 (Unknown)

Nmap scan report for 172.16.62.106
Host is up (0.0031s latency).

PORT   STATE  SERVICE
23/tcp closed telnet
MAC Address: 6C:3C:8C:53:37:0F (Unknown)

Nmap scan report for 172.16.62.218
Host is up (0.0065s latency).

PORT   STATE    SERVICE
23/tcp filtered telnet
MAC Address: 6C:3C:8C:53:43:8C (Unknown)

Nmap scan report for 172.16.62.245
Host is up (0.0081s latency).

PORT   STATE    SERVICE
23/tcp filtered telnet
MAC Address: 6C:3C:8C:53:43:26 (Unknown)

Nmap scan report for psipl-OptiPlex-3000 (172.16.62.198)
Host is up (0.000022s latency).
```

```
PORT   STATE  SERVICE
23/tcp closed telnet

Nmap done: 256 IP addresses (12 hosts up) scanned in 3.66 seconds
psipl@psipl-OptiPlex-3000:~$
```

8. Determine the operating system of a target host using NMAP.

```
psipl@psipl-OptiPlex-3000:~$ sudo nmap -O 172.16.62.245
Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-20 15:07 IST
Nmap scan report for 172.16.62.245
Host is up (0.0018s latency).
Not shown: 996 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi
MAC Address: 6C:3C:8C:53:43:26 (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|7|2008 (87%)
OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2
Aggressive OS guesses: Microsoft Windows XP SP2 (87%), Microsoft Windows 7 (85%), Microsoft Windows Server 2008 SP1 or Windows Server 2008 R2 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.37 seconds
psipl@psipl-OptiPlex-3000:~$
```

9. Identify any SQL services running on a given network.

```
psipl@psipl-OptiPlex-3000:~$ sudo nmap -p 3306 172.16.62.245/24
Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-20 15:08 IST
Nmap scan report for _gateway (172.16.62.1)
Host is up (0.0019s latency).

PORT     STATE  SERVICE
3306/tcp closed mysql
MAC Address: 94:60:D5:E0:F9:23 (Unknown)

Nmap scan report for 172.16.62.4
Host is up (0.0019s latency).

PORT     STATE  SERVICE
3306/tcp closed mysql
MAC Address: CC:5E:F8:F8:E1:FF (Unknown)

Nmap scan report for 172.16.62.25
Host is up (0.0025s latency).

PORT     STATE  SERVICE
3306/tcp closed mysql
MAC Address: CC:5E:F8:F8:CF:79 (Unknown)

Nmap scan report for 172.16.62.26
Host is up (0.0025s latency).

PORT     STATE  SERVICE
3306/tcp closed mysql
MAC Address: CC:5E:F8:F8:CF:79 (Unknown)

Nmap scan report for 172.16.62.43
Host is up (0.097s latency).

PORT     STATE    SERVICE
3306/tcp filtered mysql
MAC Address: CC:5E:F8:F8:CF:E1 (Unknown)

Nmap scan report for 172.16.62.46
Host is up (0.0035s latency).
```

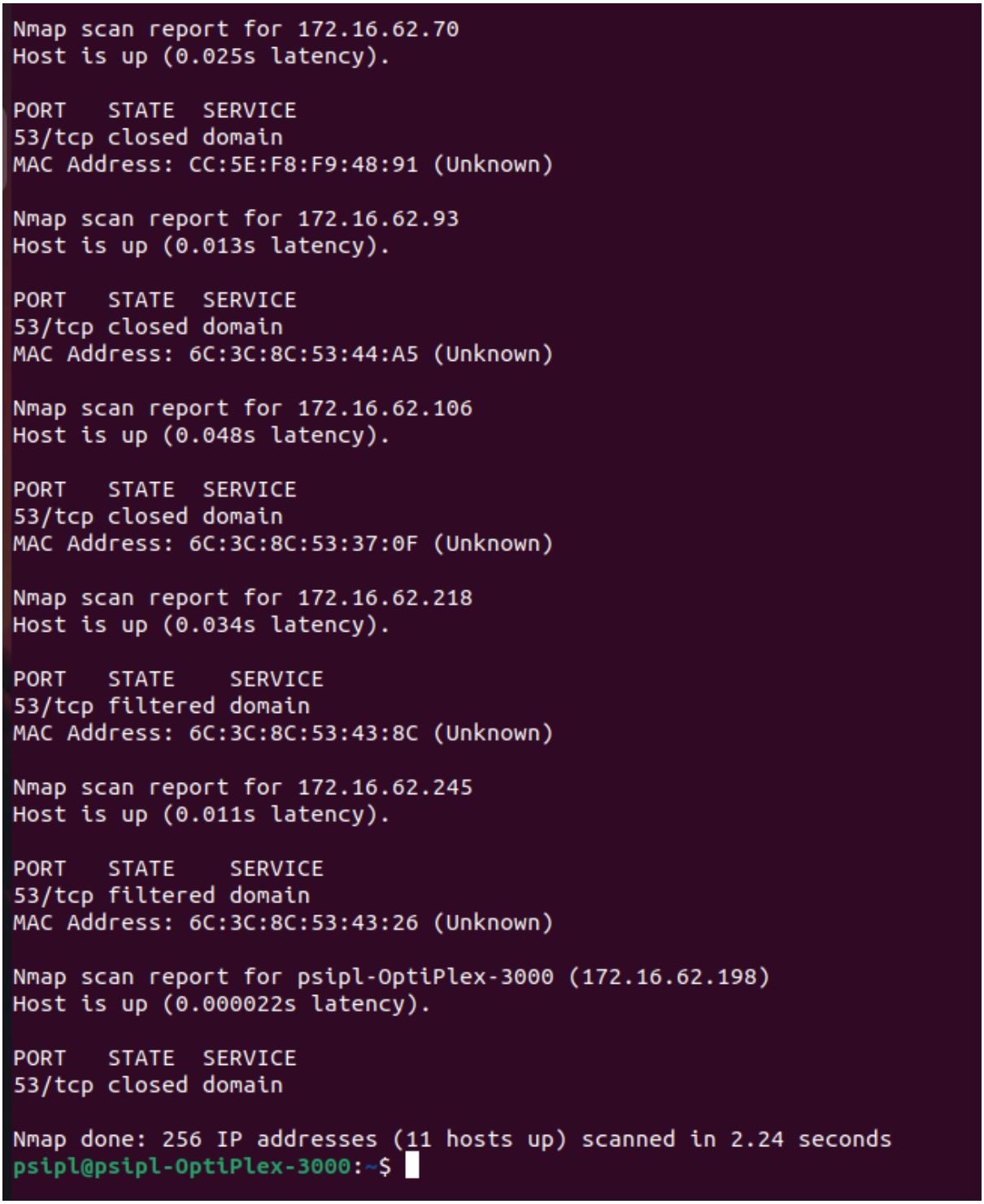
```
Nmap scan report for 172.16.62.70
Host is up (0.0079s latency).

PORT     STATE  SERVICE
3306/tcp closed mysql
MAC Address: 6C:3C:8C:53:37:0F (Unknown)

Nmap scan report for 172.16.62.93
Host is up (0.0022s latency).

PORT     STATE  SERVICE
3306/tcp closed mysql
MAC Address: CC:5E:F8:F9:1B:23 (Unknown)

Nmap scan report for 172.16.62.106
Host is up (0.010s latency).

PORT     STATE  SERVICE
3306/tcp closed mysql
MAC Address: CC:5E:F8:F9:48:91 (Unknown)

Nmap scan report for 172.16.62.218
Host is up (0.042s latency).

PORT     STATE    SERVICE
3306/tcp filtered mysql
MAC Address: 6C:3C:8C:53:43:8C (Unknown)

Nmap scan report for 172.16.62.245
Host is up (0.0014s latency).

PORT     STATE    SERVICE
3306/tcp filtered mysql
MAC Address: 6C:3C:8C:53:43:26 (Unknown)

Nmap scan report for psipl-OptiPlex-3000 (172.16.62.198)
Host is up (0.000021s latency).

PORT     STATE  SERVICE
3306/tcp closed mysql

Nmap done: 256 IP addresses (12 hosts up) scanned in 2.21 seconds
psipl@psipl-OptiPlex-3000:~$
```

10. Find out if a specific host has Remote Desktop Protocol (RDP) enabled.

```
psipl@psipl-OptiPlex-3000:~$ sudo nmap -p 3389 172.16.62.245
Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-20 15:09 IST
Nmap scan report for 172.16.62.245
Host is up (0.0024s latency).

PORT     STATE    SERVICE
3389/tcp filtered ms-wbt-server
MAC Address: 6C:3C:8C:53:43:26 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.35 seconds
psipl@psipl-OptiPlex-3000:~$
```

11. Scan a target network and determine if any hosts are running DNS services.

```
psipl@psipl-OptiPlex-3000:~$ sudo nmap -p 53 172.16.62.245/24
Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-20 15:10 IST
Nmap scan report for _gateway (172.16.62.1)
Host is up (0.0070s latency).

PORT   STATE  SERVICE
53/tcp closed domain
MAC Address: 94:60:D5:E0:F9:23 (Unknown)

Nmap scan report for 172.16.62.4
Host is up (0.0069s latency).

PORT   STATE  SERVICE
53/tcp closed domain
MAC Address: 6C:3C:8C:53:43:62 (Unknown)

Nmap scan report for 172.16.62.25
Host is up (0.0063s latency).

PORT   STATE  SERVICE
53/tcp closed domain
MAC Address: CC:96:E5:22:E1:02 (Unknown)

Nmap scan report for 172.16.62.26
Host is up (0.0063s latency).

PORT   STATE  SERVICE
53/tcp closed domain
MAC Address: CC:96:E5:22:E1:02 (Unknown)

Nmap scan report for 172.16.62.46
Host is up (0.090s latency).

PORT   STATE    SERVICE
53/tcp filtered domain
MAC Address: CC:96:E5:22:DF:5B (Unknown)

Nmap scan report for 172.16.62.70
Host is up (0.025s latency).
```

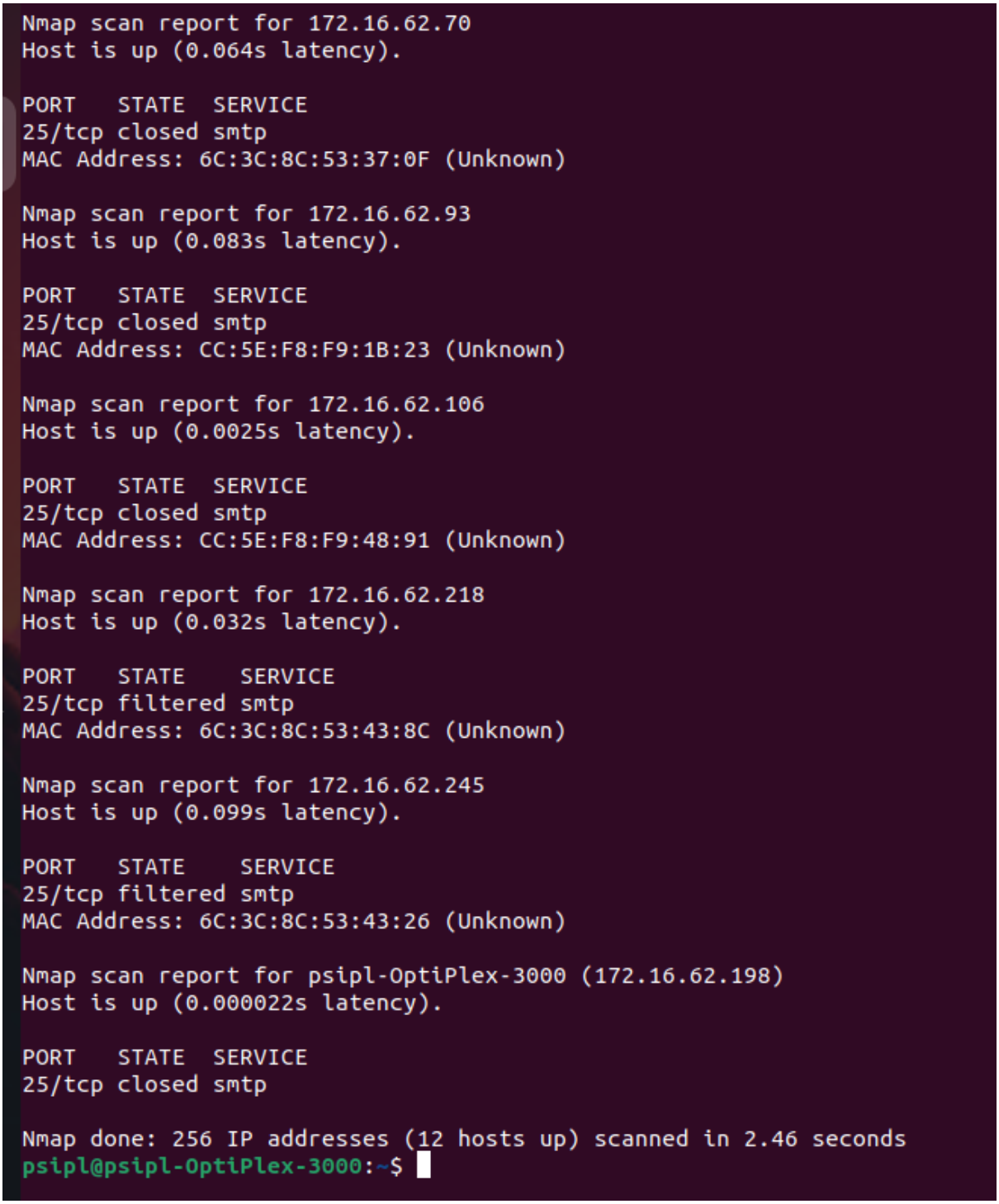

Nmap scan report for 172.16.62.70
Host is up (0.025s latency).
PORT STATE SERVICE
53/tcp closed domain
MAC Address: CC:5E:F8:F9:48:91 (Unknown)
Nmap scan report for 172.16.62.93
Host is up (0.013s latency).
PORT STATE SERVICE
53/tcp closed domain
MAC Address: 6C:3C:8C:53:44:A5 (Unknown)
Nmap scan report for 172.16.62.106
Host is up (0.048s latency).
PORT STATE SERVICE
53/tcp closed domain
MAC Address: 6C:3C:8C:53:37:0F (Unknown)
Nmap scan report for 172.16.62.218
Host is up (0.034s latency).
PORT STATE SERVICE
53/tcp filtered domain
MAC Address: 6C:3C:8C:53:43:8C (Unknown)
Nmap scan report for 172.16.62.245
Host is up (0.011s latency).
PORT STATE SERVICE
53/tcp filtered domain
MAC Address: 6C:3C:8C:53:43:26 (Unknown)
Nmap scan report for psipl-OptiPlex-3000 (172.16.62.198)
Host is up (0.000022s latency).
PORT STATE SERVICE
53/tcp closed domain
Nmap done: 256 IP addresses (11 hosts up) scanned in 2.24 seconds
psipl@psipl-OptiPlex-3000:~$

12. Detect if a host has SNMP (Simple Network Management Protocol) enabled.

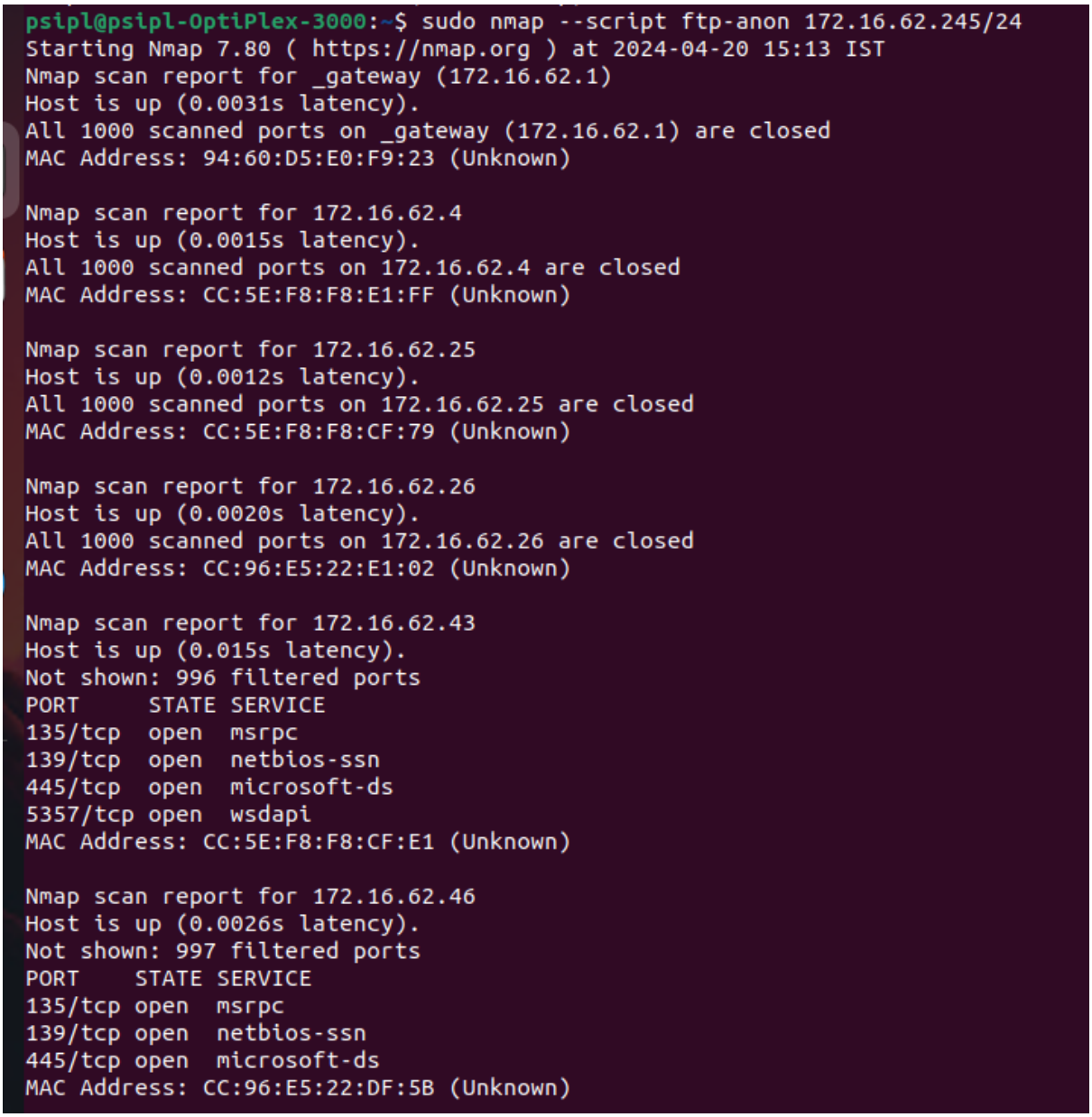
```
psipl@psipl-OptiPlex-3000:~$ sudo nmap -p 161 172.16.62.245
Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-20 15:11 IST
Nmap scan report for 172.16.62.245
Host is up (0.0021s latency).

PORT    STATE    SERVICE
161/tcp filtered snmp
MAC Address: 6C:3C:8C:53:43:26 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds
psipl@psipl-OptiPlex-3000:~$
```

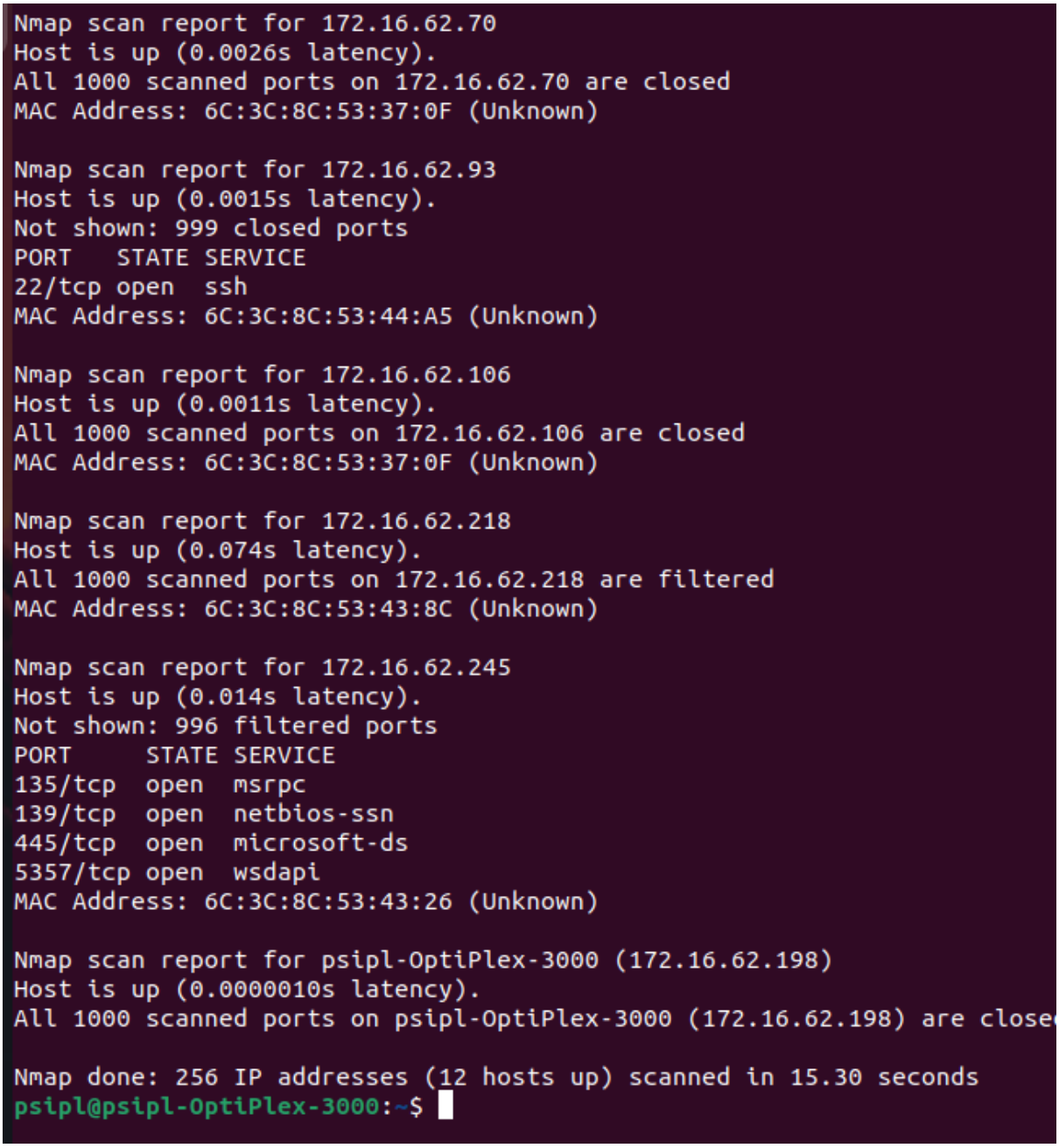
13. Perform a scan to identify any SMTP (Simple Mail Transfer Protocol) servers on a network.

```
psipl@psipl-OptiPlex-3000:~$ sudo nmap -p 25 172.16.62.245/24
Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-20 15:12 IST
Nmap scan report for _gateway (172.16.62.1)
Host is up (0.0056s latency).

PORT   STATE  SERVICE
25/tcp closed smtp
MAC Address: 94:60:D5:E0:F9:23 (Unknown)

Nmap scan report for 172.16.62.4
Host is up (0.0057s latency).

PORT   STATE  SERVICE
25/tcp closed smtp
MAC Address: 6C:3C:8C:53:43:62 (Unknown)

Nmap scan report for 172.16.62.25
Host is up (0.013s latency).

PORT   STATE  SERVICE
25/tcp closed smtp
MAC Address: CC:5E:F8:F8:CF:79 (Unknown)

Nmap scan report for 172.16.62.26
Host is up (0.013s latency).

PORT   STATE  SERVICE
25/tcp closed smtp
MAC Address: CC:5E:F8:F8:CF:79 (Unknown)

Nmap scan report for 172.16.62.43
Host is up (0.012s latency).

PORT   STATE    SERVICE
25/tcp filtered smtp
MAC Address: CC:5E:F8:F8:CF:E1 (Unknown)

Nmap scan report for 172.16.62.46
Host is up (0.012s latency).
```


Nmap scan report for 172.16.62.70
Host is up (0.064s latency).
PORT STATE SERVICE
25/tcp closed smtp
MAC Address: 6C:3C:8C:53:37:0F (Unknown)
Nmap scan report for 172.16.62.93
Host is up (0.083s latency).
PORT STATE SERVICE
25/tcp closed smtp
MAC Address: CC:5E:F8:F9:1B:23 (Unknown)
Nmap scan report for 172.16.62.106
Host is up (0.0025s latency).
PORT STATE SERVICE
25/tcp closed smtp
MAC Address: CC:5E:F8:F9:48:91 (Unknown)
Nmap scan report for 172.16.62.218
Host is up (0.032s latency).
PORT STATE SERVICE
25/tcp filtered smtp
MAC Address: 6C:3C:8C:53:43:8C (Unknown)
Nmap scan report for 172.16.62.245
Host is up (0.099s latency).
PORT STATE SERVICE
25/tcp filtered smtp
MAC Address: 6C:3C:8C:53:43:26 (Unknown)
Nmap scan report for psipl-OptiPlex-3000 (172.16.62.198)
Host is up (0.000022s latency).
PORT STATE SERVICE
25/tcp closed smtp
Nmap done: 256 IP addresses (12 hosts up) scanned in 2.46 seconds
psipl@psipl-OptiPlex-3000:~$

14. Determine if a target network has any active FTP servers allowing anonymous login.




Nmap scan report for 172.16.62.70
Host is up (0.0026s latency).
All 1000 scanned ports on 172.16.62.70 are closed
MAC Address: 6C:3C:8C:53:37:0F (Unknown)
Nmap scan report for 172.16.62.93
Host is up (0.0015s latency).
Not shown: 999 closed ports
PORT STATE SERVICE
22/tcp open ssh
MAC Address: 6C:3C:8C:53:44:A5 (Unknown)
Nmap scan report for 172.16.62.106
Host is up (0.0011s latency).
All 1000 scanned ports on 172.16.62.106 are closed
MAC Address: 6C:3C:8C:53:37:0F (Unknown)
Nmap scan report for 172.16.62.218
Host is up (0.074s latency).
All 1000 scanned ports on 172.16.62.218 are filtered
MAC Address: 6C:3C:8C:53:43:8C (Unknown)
Nmap scan report for 172.16.62.245
Host is up (0.014s latency).
Not shown: 996 filtered ports
PORT STATE SERVICE
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
5357/tcp open wsdapi
MAC Address: 6C:3C:8C:53:43:26 (Unknown)
Nmap scan report for psipl-OptiPlex-3000 (172.16.62.198)
Host is up (0.0000010s latency).
All 1000 scanned ports on psipl-OptiPlex-3000 (172.16.62.198) are close
Nmap done: 256 IP addresses (12 hosts up) scanned in 15.30 seconds
psipl@psipl-OptiPlex-3000:~$

15. Find out if any hosts in a network are running vulnerable versions of the Apache HTTP server.

```
psipl@psipl-OptiPlex-3000:~$ sudo nmap --script http-vuln-cve2011-3192 172.16.62.245/24
Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-20 15:15 IST
Nmap scan report for _gateway (172.16.62.1)
Host is up (0.0015s latency).
All 1000 scanned ports on _gateway (172.16.62.1) are closed
MAC Address: 94:60:D5:E0:F9:23 (Unknown)

Nmap scan report for 172.16.62.4
Host is up (0.0010s latency).
All 1000 scanned ports on 172.16.62.4 are closed
MAC Address: CC:5E:F8:F8:E1:FF (Unknown)

Nmap scan report for 172.16.62.25
Host is up (0.00080s latency).
All 1000 scanned ports on 172.16.62.25 are closed
MAC Address: CC:5E:F8:F8:CF:79 (Unknown)

Nmap scan report for 172.16.62.26
Host is up (0.0014s latency).
All 1000 scanned ports on 172.16.62.26 are closed
MAC Address: CC:5E:F8:F8:CF:79 (Unknown)

Nmap scan report for 172.16.62.43
Host is up (0.024s latency).
Not shown: 996 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi
MAC Address: CC:5E:F8:F8:CF:E1 (Unknown)

Nmap scan report for 172.16.62.46
Host is up (0.0019s 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: CC:96:E5:22:DF:5B (Unknown)
```

```
Nmap scan report for 172.16.62.70
Host is up (0.0011s latency).
All 1000 scanned ports on 172.16.62.70 are closed
MAC Address: 6C:3C:8C:53:37:0F (Unknown)

Nmap scan report for 172.16.62.93
Host is up (0.0011s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 6C:3C:8C:53:44:A5 (Unknown)

Nmap scan report for 172.16.62.106
Host is up (0.0010s latency).
All 1000 scanned ports on 172.16.62.106 are closed
MAC Address: 6C:3C:8C:53:37:0F (Unknown)

Nmap scan report for 172.16.62.218
Host is up (0.024s latency).
All 1000 scanned ports on 172.16.62.218 are filtered
MAC Address: 6C:3C:8C:53:43:8C (Unknown)

Nmap scan report for 172.16.62.245
Host is up (0.0032s latency).
Not shown: 996 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi
MAC Address: 6C:3C:8C:53:43:26 (Unknown)

Nmap scan report for psipl-OptiPlex-3000 (172.16.62.198)
Host is up (0.0000010s latency).
All 1000 scanned ports on psipl-OptiPlex-3000 (172.16.62.198) are closed

Nmap done: 256 IP addresses (12 hosts up) scanned in 11.72 seconds
psipl@psipl-OptiPlex-3000:~$
```

16. Detect if a target host has any open NFS (Network File System) shares.

```
psipl@psipl-OptiPlex-3000:~$ sudo nmap --script nfs-showmount 172.16.62.245
Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-20 15:16 IST
Nmap scan report for 172.16.62.245
Host is up (0.0022s latency).
Not shown: 996 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi
MAC Address: 6C:3C:8C:53:43:26 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 4.46 seconds
psipl@psipl-OptiPlex-3000:~$
```

17. Identify the presence of any MySQL database servers on a given network.
    (already shown in SQL server scan)

18. Scan a network to determine if any hosts have the Remote Procedure Call (RPC) service running.

```
psipl@psipl-OptiPlex-3000:~$ sudo nmap -p 111 172.16.62.245/24
Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-20 15:20 IST
Nmap scan report for _gateway (172.16.62.1)
Host is up (0.013s latency).

PORT    STATE  SERVICE
111/tcp closed rpcbind
MAC Address: 94:60:D5:E0:F9:23 (Unknown)

Nmap scan report for 172.16.62.4
Host is up (0.016s latency).

PORT    STATE  SERVICE
111/tcp closed rpcbind
MAC Address: CC:5E:F8:F8:E1:FF (Unknown)

Nmap scan report for 172.16.62.25
Host is up (0.017s latency).

PORT    STATE  SERVICE
111/tcp closed rpcbind
MAC Address: CC:5E:F8:F8:CF:79 (Unknown)

Nmap scan report for 172.16.62.26
Host is up (0.017s latency).

PORT    STATE  SERVICE
111/tcp closed rpcbind
MAC Address: CC:5E:F8:F8:CF:79 (Unknown)

Nmap scan report for 172.16.62.43
Host is up (0.099s latency).

PORT    STATE    SERVICE
111/tcp filtered rpcbind
MAC Address: CC:5E:F8:F8:CF:E1 (Unknown)

Nmap scan report for 172.16.62.46
Host is up (0.0038s latency).
```

```
Nmap scan report for 172.16.62.70
Host is up (0.019s latency).

PORT    STATE  SERVICE
111/tcp closed rpcbind
MAC Address: 6C:3C:8C:53:37:0F (Unknown)

Nmap scan report for 172.16.62.93
Host is up (0.020s latency).

PORT    STATE  SERVICE
111/tcp closed rpcbind
MAC Address: CC:5E:F8:F9:1B:23 (Unknown)

Nmap scan report for 172.16.62.106
Host is up (0.017s latency).

PORT    STATE  SERVICE
111/tcp closed rpcbind
MAC Address: 6C:3C:8C:53:37:0F (Unknown)

Nmap scan report for 172.16.62.218
Host is up (0.0044s latency).

PORT    STATE    SERVICE
111/tcp filtered rpcbind
MAC Address: 6C:3C:8C:53:43:8C (Unknown)

Nmap scan report for 172.16.62.245
Host is up (0.0022s latency).

PORT    STATE    SERVICE
111/tcp filtered rpcbind
MAC Address: 6C:3C:8C:53:43:26 (Unknown)

Nmap scan report for psipl-OptiPlex-3000 (172.16.62.198)
Host is up (0.000028s latency).

PORT    STATE  SERVICE
111/tcp closed rpcbind

Nmap done: 256 IP addresses (12 hosts up) scanned in 2.24 seconds
psipl@psipl-OptiPlex-3000:~$
```

19. Detect if a specific host has any open VNC (Virtual Network Computing) ports.

```
psipl@psipl-OptiPlex-3000:~$ sudo nmap -p 5900-5903 172.16.62.245
Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-20 15:28 IST
Nmap scan report for 172.16.62.245
Host is up (0.0026s latency).

PORT     STATE    SERVICE
5900/tcp filtered vnc
5901/tcp filtered vnc-1
5902/tcp filtered vnc-2
5903/tcp filtered vnc-3
MAC Address: 6C:3C:8C:53:43:26 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.43 seconds
psipl@psipl-OptiPlex-3000:~$
```

20. Perform a scan to identify any hosts with the Secure Shell (SSH) service running on non-default ports.

```
psipl@psipl-OptiPlex-3000:~$ sudo nmap -p- --script ssh-hostkey 172.16.62.245/24
Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-20 15:35 IST
Nmap scan report for _gateway (172.16.62.1)
Host is up (0.0059s latency).
All 65535 scanned ports on _gateway (172.16.62.1) are closed
MAC Address: 94:60:D5:E0:F9:23 (Unknown)

Nmap scan report for 172.16.62.4
Host is up (0.0069s latency).
All 65535 scanned ports on 172.16.62.4 are closed
MAC Address: CC:5E:F8:F8:E1:FF (Unknown)

Nmap scan report for 172.16.62.25
Host is up (0.0011s latency).
All 65535 scanned ports on 172.16.62.25 are closed
MAC Address: CC:96:E5:22:E1:02 (Unknown)

Nmap scan report for 172.16.62.26
Host is up (0.0033s latency).
All 65535 scanned ports on 172.16.62.26 are closed
MAC Address: CC:96:E5:22:E1:02 (Unknown)

Nmap scan report for 172.16.62.43
Host is up (0.026s latency).
Not shown: 65528 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5040/tcp  open  unknown
5357/tcp  open  wsdapi
7680/tcp  open  pando-pub
49669/tcp open  unknown
MAC Address: CC:5E:F8:F8:CF:E1 (Unknown)
```

```
Nmap scan report for 172.16.62.46
Host is up (0.0026s latency).
Not shown: 65530 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
7680/tcp  open  pando-pub
49669/tcp open  unknown
MAC Address: CC:96:E5:22:DF:5B (Unknown)

Nmap scan report for 172.16.62.70
Host is up (0.00099s latency).
All 65535 scanned ports on 172.16.62.70 are closed
MAC Address: CC:5E:F8:F9:48:91 (Unknown)

Nmap scan report for 172.16.62.93
Host is up (0.0048s latency).
Not shown: 65534 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 6C:3C:8C:53:44:A5 (Unknown)

Nmap scan report for 172.16.62.106
Host is up (0.0017s latency).
All 65535 scanned ports on 172.16.62.106 are closed
MAC Address: 6C:3C:8C:53:37:0F (Unknown)

Nmap scan report for 172.16.62.218
Host is up (0.0013s latency).
Not shown: 65534 filtered ports
PORT     STATE SERVICE
7680/tcp open  pando-pub
MAC Address: 6C:3C:8C:53:43:8C (Unknown)
```

```
Nmap scan report for 172.16.62.245
Host is up (0.0039s latency).
Not shown: 65528 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5040/tcp  open  unknown
5357/tcp  open  wsdapi
7680/tcp  open  pando-pub
49669/tcp open  unknown
MAC Address: 6C:3C:8C:53:43:26 (Unknown)

Nmap scan report for psipl-OptiPlex-3000 (172.16.62.198)
Host is up (0.0000010s latency).
All 65535 scanned ports on psipl-OptiPlex-3000 (172.16.62.198) are closed

Nmap done: 256 IP addresses (12 hosts up) scanned in 308.01 seconds
psipl@psipl-OptiPlex-3000:~$
```