TASK-9

NMAP:

NMAP is a tool for network monitoring and security auditing tool. It is used by network administrators to scan the ports and what are all the task is undergoing. It is useful for network inventory, managing services, upgrading scheduling and managing the service time. Nmap uses raw ip packets in novel ways to determine what hosts area available on the network, what services those host are offering what operating systems they are running, what type of packet filters/firewalls are in use.

In simple words nmap is a network scanning tool used to discover hosts, open ports, services and operating systems on a network.

To launch the Nmap:

1.open terminal->command-> nmap.scanme.nmap.org

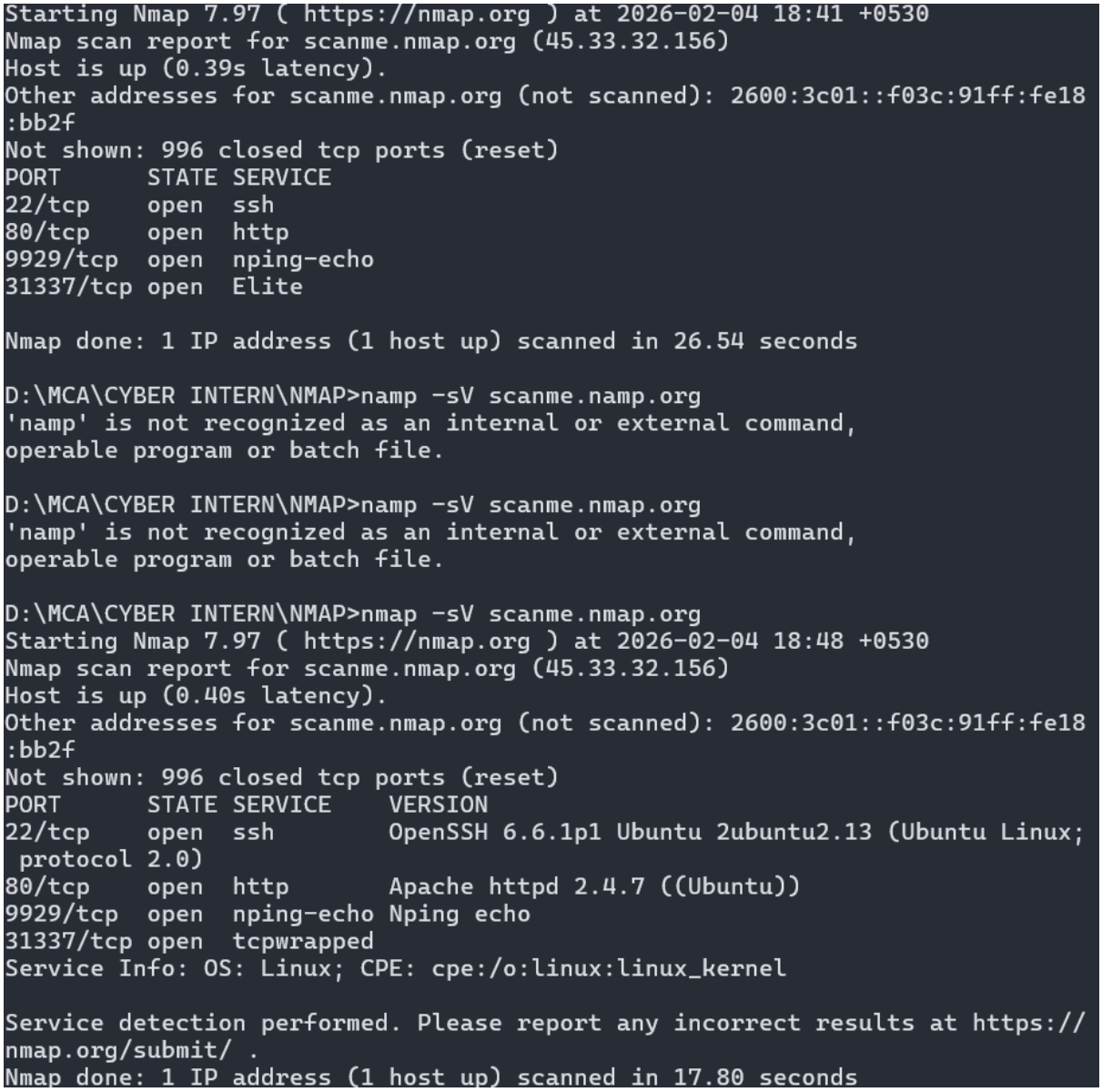
It will launch the Nmap

```
D:\MCA\CYBER INTERN\NMAP>nmap scanme.nmap.org
Starting Nmap 7.97 ( https://nmap.org ) at 2026-02-04 18:41 +0530
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.39s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18
:bb2f
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
9929/tcp  open  nping-echo
31337/tcp open  Elite

Nmap done: 1 IP address (1 host up) scanned in 26.54 seconds
```

Nmap is used during the reconnaissance phase to identify open ports, running services, operating systems, and potential vulnerabilities.

A service version detection scan was performed using Nmap (-sV) to identify running services and their software versions. The scan revealed SSH (OpenSSH 6.6.1p1) and HTTP (Apache 2.4.7) services running on a Linux-based system. Identifying service versions is crucial for assessing potential vulnerabilities and strengthening security configurations.



```
Starting Nmap 7.97 ( https://nmap.org ) at 2026-02-04 18:41 +0530
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.39s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18
:bb2f
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
9929/tcp  open  nping-echo
31337/tcp open  Elite

Nmap done: 1 IP address (1 host up) scanned in 26.54 seconds

D:\MCA\CYBER INTERN\NMAP>namp -sV scanme.namp.org
'namp' is not recognized as an internal or external command,
operable program or batch file.

D:\MCA\CYBER INTERN\NMAP>namp -sV scanme.nmap.org
'namp' is not recognized as an internal or external command,
operable program or batch file.

D:\MCA\CYBER INTERN\NMAP>nmap -sV scanme.nmap.org
Starting Nmap 7.97 ( https://nmap.org ) at 2026-02-04 18:48 +0530
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.40s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18
:bb2f
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE    VERSION
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))
9929/tcp  open  nping-echo Nping echo
31337/tcp open  tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://
nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.80 seconds
```

Form my screenshot these are all the ports which are opened and running:

- **22/tcp** → SSH is running
- **80/tcp** → HTTP (web server) is running
- **9929/tcp** → Nmap test service is running
- **31337/tcp** → Port is open but access is restricted (tcpwrapped)

A targeted port scan of ports 1–100 revealed that only ports 22 (SSH) and 80 (HTTP) were open, while the remaining 98 ports were closed. This indicates a limited attack surface within the commonly used port range.

NMAP THE LOCAL NETWORK:

```
D:\MCA\CYBER INTERN\NMAP>nmap  10.58.238.148
Starting Nmap 7.97 ( https://nmap.org ) at 2026-02-04 19:31 +0530
Nmap scan report for 10.58.238.148
Host is up (0.00066s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3306/tcp open  mysql
```

The scan revealed Windows-related services such as MSRPC, NetBIOS, and SMB, along with a MySQL database service. These ports are commonly used in internal networks but can pose serious security risks if exposed or improperly secured.

PORT SCANNING AT OS LEVEL:

```
D:\MCA\CYBER INTERN\NMAP>nmap -O scanme.nmap.org
Starting Nmap 7.97 ( https://nmap.org ) at 2026-02-04 19:35 +0530
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.33s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 996 closed tcp ports (reset)
PORT      STATE    SERVICE
22/tcp    open     ssh
80/tcp    open     http
9929/tcp  filtered nping-echo
31337/tcp open     Elite
Device type: general purpose|firewall
Running (JUST GUESSING): Linux 5.X|4.X (87%), SonicWALL embedded (85%)
OS CPE: cpe:/o:linux:linux_kernel:5.18 cpe:/o:linux:linux_kernel:4 cpe:/o:sonicwal
l:aventail_ex-1500
Aggressive OS guesses: Linux 5.18 (87%), Linux 5.4 (87%), Linux 4.15 - 5.19 (85%),
 SonicWALL Aventail EX-1500 SSL VPN appliance (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 17 hops

OS detection performed. Please report any incorrect results at https://nmap.org/su
bmit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.89 seconds
```

In this we can see,

- 22/tcp - open ssh
- 80/tcp - open http
- 9929/tcp- filtered nping-echo
- 31337/tcp-open Elite

- Device type - firewall behaviour
- Running - targeted system's OS, might be firewall
- Latency - 17 hops, 17 intermediatary devices.

An OS detection scan was performed using Nmap with the -O option. The results indicate that the target system is most likely running a Linux-based operating system and is protected by firewall mechanisms. Some ports were observed as filtered, which impacted the accuracy of OS fingerprinting. OS-level scanning provided insights into device type, operating system family, and network distance.