

Name: Shrey Pendurkar

Class: D15C

Batch: C

Roll No: 64

CNS - Experiment 9

Aim: Download, install nmap and use it with different options to scan open ports, perform OS fingerprinting, ping scan, tcp port scan, udp port scan, etc.

Theory:

1) Port range scan (1–200): `nmap -p 1-200 192.168.44.223`

Scans TCP ports 1 through 200 on the target to discover which ports are open or filtered. Useful for focused scanning when you only need to check common low-numbered services.

2) Single-port scan (HTTP): `nmap -p 80 192.168.44.223`

Checks only TCP port 80 to see if an HTTP service is listening on that port. Fast and precise when you already know which port/service you want to test.

3) Fast (top ports) scan: `nmap -F 192.168.44.223`

Performs a “fast” scan using Nmap’s reduced list of commonly used ports instead of the full default set. Good for quick reconnaissance when you want a speed/coverage tradeoff.

4) Full TCP port sweep: `nmap -p- 192.168.44.223`

Scans all 65,535 TCP ports (`-p-` means “all ports”) to find services running on nonstandard ports. Comprehensive but slower and noisier than limited-range scans.

5) TCP connect() scan: `nmap -sT 192.168.44.223`

Performs a TCP connect scan that completes the three-way handshake for each port using the OS networking stack. Works without raw-socket/root privileges but is less stealthy and more likely to be logged.

6) UDP scan: `nmap -sU 192.168.44.223`

Performs a UDP scan to find open UDP services by sending UDP probes and analyzing responses or absence of replies. Slower and less reliable than TCP scans because UDP is connectionless and many hosts drop or rate-limit probes.

7) Aggressive/Comprehensive scan: `nmap -A 192.168.44.223`

Runs an aggressive scan enabling OS detection, version detection, default scripts and traceroute to gather extensive host information. Very informative but noisy and likely to trigger intrusion detection or logging.

8) OS fingerprinting: `nmap -O 192.168.44.223`

Attempts OS detection by analyzing TCP/IP stack behavior and probe responses to guess the target's operating system. Accuracy improves with elevated privileges and when the host responds to probes.

9) Subnet / network discovery: `nmap 192.168.44.223`

Scans the entire /24 subnet (192.168.44.0–192.168.44.255) to discover live hosts and open ports across the network. Useful for network mapping and discovery, but generates more traffic across the LAN.

Output:

1. Port Scanning (Range 1 to 200)

The screenshot shows the Nmap interface with the target set to 192.168.44.223. The command entered is nmap -p 1-200 192.168.44.223. The Nmap Output tab is selected, displaying the following results:

```
nmap -p 1-200 192.168.44.223
Starting Nmap 7.98 ( https://nmap.org ) at 2025-10-08 09:38 +0530
Nmap scan report for 192.168.44.223
Host is up (0.00012s latency).
Not shown: 196 closed tcp ports (reset)
PORT      STATE    SERVICE
80/tcp    open     http
135/tcp   open     msrpc
137/tcp   filtered netbios-ns
139/tcp   open     netbios-ssn

Nmap done: 1 IP address (1 host up) scanned in 1.83 seconds
```

2. Scan a Specific Port (e.g., Port 80)

The screenshot shows the Nmap interface with the target set to 192.168.44.223. The command entered is nmap -p 80 192.168.44.223. The Nmap Output tab is selected, displaying the following results:

```
nmap -p 80 192.168.44.223
Starting Nmap 7.98 ( https://nmap.org ) at 2025-10-08 09:41 +0530
Nmap scan report for 192.168.44.223
Host is up (0.00s latency).

PORT      STATE    SERVICE
80/tcp    open     http

Nmap done: 1 IP address (1 host up) scanned in 0.56 seconds
```

3. Scan with Fast Scan Option

The screenshot shows the Nmap interface with the target set to 192.168.44.223. The command entered is nmap -F 192.168.44.223. The results tab is selected, displaying the following output:

```
nmap -F 192.168.44.223
Starting Nmap 7.98 ( https://nmap.org ) at 2025-10-08 09:42 +0530
Nmap scan report for 192.168.44.223
Host is up (0.000082s latency).
Not shown: 95 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql

Nmap done: 1 IP address (1 host up) scanned in 0.57 seconds
```

4. Scan All Ports

The screenshot shows the Nmap interface with the target set to 192.168.44.223. The command entered is nmap -p - 192.168.44.223. The results tab is selected, displaying the following output:

```
nmap -p - 192.168.44.223
Starting Nmap 7.98 ( https://nmap.org ) at 2025-10-08 09:43 +0530
Nmap scan report for 192.168.44.223
Host is up (0.000088s latency).
Not shown: 65519 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
137/tcp   filtered netbios-ns
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
5040/tcp  open  unknown
7783/tcp  open  unknown
8885/tcp  open  unknown
33060/tcp open  mysqlx
49664/tcp open  unknown
49665/tcp open  unknown
49666/tcp open  unknown
49667/tcp open  unknown
49668/tcp open  unknown
49670/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 3.76 seconds
```

5. TCP Connect Scan

The screenshot shows the Nmap interface with the target set to 192.168.44.223. The command entered is nmap -sT 192.168.44.223. The 'Nmap Output' tab is selected, displaying the results of the scan. The output shows the host is up with 0 latency. It lists 995 closed TCP ports (conn-refused) and provides a detailed table of open ports:

| PORT | STATE | SERVICE |
|----------|-------|--------------|
| 80/tcp | open | http |
| 135/tcp | open | msrpc |
| 139/tcp | open | netbios-ssn |
| 445/tcp | open | microsoft-ds |
| 3306/tcp | open | mysql |

The scan took 0.63 seconds.

6. UDP Scan

The screenshot shows the Nmap interface with the target set to 192.168.44.223. The command entered is nmap -sU 192.168.44.223. The 'Nmap Output' tab is selected, displaying the results of the scan. The output shows the host is up with 0 latency. It lists 990 closed UDP ports (port-unreach) and provides a detailed table of open|filtered ports:

| PORT | STATE | SERVICE |
|----------|---------------|-------------|
| 80/udp | open filtered | http |
| 123/udp | open filtered | ntp |
| 137/udp | open filtered | netbios-ns |
| 138/udp | open filtered | netbios-dgm |
| 443/udp | open filtered | https |
| 1900/udp | open filtered | upnp |
| 4500/udp | open filtered | nat-t-ike |
| 5050/udp | open filtered | mmcc |
| 5353/udp | open filtered | zeroconf |
| 5355/udp | open filtered | llmnr |

The scan took 38.06 seconds.

7. Aggressive Scan

Target: 192.168.44.223 Profile:

Command: nmap -A 192.168.44.223

Hosts Services

OS Host

192.168.44.223

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -A 192.168.44.223

```
|_http-title: Site doesn't have a title.
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
445/tcp open microsoft-ds?
3306/tcp open mysql MySQL (unauthorized)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/).
TCP/IP fingerprint:
OS:SCAN(V=7.98%E=4%D=10/8%OT=80%CT=1%CU=39126%PV=Y%DS=0%DC=L%G=Y%TM=68E5E5F
OS:;%P=1686-pc-windows-windows) SEQ(SP=103%GCD=1%ISR=10B%TI=I%CI=I%II=I%SS=S
OS:;%TS=A) SEQ(SP=104%GCD=1%ISR=109%TI=I%CI=I%II=I%SS=S%TS=A) SEQ(SP=EF%GCD=1%
OS:;ISR=107%TI=I%CI=I%II=I%SS=S%TS=A) SEQ(SP=FD%GCD=1%ISR=109%TI=I%CI=I%II=I%
OS:;SS=S%TS=A) OPS(O1=MFFD7NW8ST11%O2=MFFD7NW8NT11%O4=MFFD7N
OS:;W8ST11%O5=MFFD7NW8ST11%O6=MFFD7ST11) WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%
OS:;W5=FFFF%W6=FFFF) ECN(R=Y%DF=Y%T=80%W=FFFF%O=MFFD7NW8NNS$CC=N%Q=) T1(R=Y%DF
OS:;Y%T=80%W=0%A=S+$F=ASRD=0%Q=) T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S+$F=AR%O=%RD=0%
OS:;O=) T3(R=Y%DF=Y%T=80%W=0%S=Z%A=S+$F=AR%O=%RD=0%Q=) T4(R=Y%DF=Y%T=80%W=0%S=A
OS:;A=O=%F=R%O=%RD=0%Q=) T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+$F=AR%O=%RD=0%Q=) T6(R=Y
OS:;%DF=Y%T=80%W=0%A=S+$F=AR%O=%RD=0%Q=) T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+$F=AR
OS:;%O=%RD=0%Q=) U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=Z%RUCK=G%RU
OS:;D=G) IE(R=Y%DFI=N%T=80%CD=)
```

Network Distance: 0 hops

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:

```
| smb2-security-mode:
|   3.1.1:
|_ Message signing enabled but not required
```

smb2-time:

```
|_ date: 2025-10-08T04:17:55
```

start_date: N/A

OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 31.46 seconds

8. OS Fingerprinting

Target: 192.168.44.223 Profile:

Command: nmap -O 192.168.44.223

Hosts Services

OS Host

192.168.44.223

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -O 192.168.44.223

```
Starting Nmap 7.98 ( https://nmap.org ) at 2025-10-08 09:49 +0530
Nmap scan report for 192.168.44.223
Host is up (0.00088s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/).
TCP/IP fingerprint:
OS:SCAN(V=7.98%E=4%D=10/8%OT=80%CT=1%CU=37453%PV=Y%DS=0%DC=L%G=Y%TM=68E5E64
OS:;%P=1686-pc-windows-windows) SEQ(SP=101%GCD=1%ISR=10D%TI=I%CI=I%II=I%TS=A
OS:;%SEQ(SP=102%GCD=1%ISR=109%TI=I%CI=I%II=I%TS=A) SEQ(SP=103%GCD=1%ISR=10A%T
OS:;%I%CI=I%II=I%TS=A) SEQ(SP=F%GCD=1%ISR=10D%TI=I%CI=I%II=I%TS=A) SEQ(SP=FC
OS:;%GCD=1%ISR=104%TI=I%CI=I%II=I%TS=A) OPS(O1=MFFD7NW8ST11%O2=MFFD7NW8ST11%O
OS:;3=MFFD7NW8NT11%O4=MFFD7NW8ST11%O6=MFFD7ST11) WIN(W1=FFFF
OS:;%W=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FFFF) ECN(R=Y%DF=Y%T=80%W=FFFF%O=MFFD
OS:;%W=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FFFF) T1(R=Y%DF=Y%T=80%S=0%A=S+$F=ASRD=0%Q=) T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S+$F=AR%O=%RD=0%Q=
OS:;W=0%S=Z%A=S+$F=AR%O=%RD=0%Q=) T3(R=Y%DF=Y%T=80%W=0%S=Z%A=S+$F=AR%O=%RD=0%Q=
OS:;T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=) T5(R=Y%DF=Y%T=80%W=0%S=Z%A=
OS:;S+$F=AR%O=%RD=0%Q=) T6(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=) T7(R=Y%DF
OS:;Y%T=80%W=0%S=Z%A=S+$F=AR%O=%RD=0%Q=) U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=
OS:;G%RID=G%RIPCK=Z%RUCK=G%RUD=G) IE(R=Y%DFI=N%T=80%CD=)
```

Network Distance: 0 hops

OS detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 10.78 seconds

9. Subnet Scan

The screenshot shows the Nmap interface with the target set to 192.168.44.223. The command entered is nmap 192.168.44.223. The Nmap Output tab is selected, displaying the following results:

```
nmap 192.168.44.223
Starting Nmap 7.98 ( https://nmap.org ) at 2025-10-08 09:56 +0530
Nmap scan report for 192.168.44.223
Host is up (0.00065s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql

Nmap done: 1 IP address (1 host up) scanned in 1.62 seconds
```

Conclusion:

This practical showed how `nmap` can quickly discover hosts, open TCP/UDP ports, and gather high-level system information (service versions and OS guesses) using a variety of scan types. Range scans (`-p 1-200`), full sweeps (`-p-`), UDP (`-sU`), TCP connect (`-sT`), and aggressive/OS detection (`-A, -O`) each have strengths — focused scans are faster and quieter, full/UDP scans are more comprehensive but slower and noisier, and aggressive scans yield richer info at the cost of visibility.

Key takeaways and best practices:

- Always have explicit authorization before scanning systems or networks — unauthorized scanning can be illegal and disruptive.
- Start with light scans (fast/top ports) to identify likely targets, then escalate to more thorough scans only when needed and permitted.
- Run privileged scans (when authorized) for more accurate results, but expect increased logging and detection by security controls.
- Record results, timestamps, and commands used; share findings with stakeholders and include remediation suggestions (close unnecessary services, apply patches, harden configurations).