Implementation:

Download and install nmap on your PC.

Open **Command Prompt** (Press **Win** + **R**, type cmd, and hit Enter)

Check for path - C:\Program Files (x86)\Nmap

```
C:\Users\Prof. S Teli>cd C:\Program Files (x86)\Nmap
```

1. nmap -V

```
C:\Program Files (x86)\Nmap>nmap -V
Nmap version 7.95 ( https://nmap.org )
Platform: i686-pc-windows-windows
Compiled with: nmap-liblua-5.4.6 openssl-3.0.13 nmap-libssh2-1.11.0 nmap-libz-1.3.1 nmap-libpcre2-10.43 Npcap-1.79 nmap-
libdnet-1.12 ipv6
Compiled without:
Available nsock engines: iocp poll select
```

2.Ping Scan

```
C:\Program Files (x86)\Nmap>nmap -sn 172.16.5.209
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-10 09:41 India Standard Time
Nmap scan report for 172.16.5.209
Host is up.
Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
```

3. Scan Open Ports

```
C:\Program Files (x86)\Nmap>nmap 172.16.5.209
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-10 09:41 India Standard Time
Nmap scan report for 172.16.5.209
Host is up (0.00043s latency).
Not shown: 996 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

Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
```

4. Scan Specific Ports

```
C:\Program Files (x86)\Nmap>nmap -p 22,80,443 172.16.5.209
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-10 09:42 India Standard Time
Nmap scan report for 172.16.5.209
Host is up (0.00s latency).

PORT    STATE  SERVICE
22/tcp  closed ssh
80/tcp  open   http
443/tcp closed https

Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
```

5. OS Fingerprinting (Detect Target OS)

```
C:\Program Files (x86)\Nmap>nmap -O 172.16.5.209
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-10 09:59 India Standard Time
Nmap scan report for 172.16.5.209
Host is up (0.000078s latency).
Not shown: 996 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
Device type: general purpose
Running: Microsoft Windows 10|11
OS CPE: cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows_11
OS details: Microsoft Windows 10 1607 - 11 23H2
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 1.18 seconds
```

6. UDP Port Scan (For Scanning UDP Ports)

```
C:\Program Files (x86)\Nmap>nmap -sU 172.16.5.209
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-10 09:44 India Standard Time
Nmap scan report for 172.16.5.209
Host is up (0.00010s latency).
Not shown: 992 closed udp ports (port-unreach)
PORT     STATE         SERVICE
123/udp  open|filtered ntp
137/udp  open|filtered netbios-ns
138/udp  open|filtered netbios-dgm
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

Nmap done: 1 IP address (1 host up) scanned in 47.48 seconds
```

```
C:\Program Files (x86)\Nmap>nmap -sU -p 53 172.16.5.209
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-10 09:48 India Standard Time
Nmap scan report for 172.16.5.209
Host is up (0.00s latency).

PORT   STATE  SERVICE
53/udp closed domain

Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds
```

7. Aggressive Scan (Detailed Information)

```
C:\Program Files (x86)\Nmap>nmap -A 172.16.5.209
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-10 09:48 India Standard Time
Nmap scan report for 172.16.5.209
Host is up (0.00015s latency).
Not shown: 996 closed tcp ports (reset)
PORT    STATE SERVICE       VERSION
80/tcp  open  http          Microsoft IIS httpd 10.0
|_http-title: Site doesn't have a title.
|_http-server-header: Microsoft-IIS/10.0
| http-methods:
|_  Potentially risky methods: TRACE
135/tcp open  msrpc         Microsoft Windows RPC
139/tcp open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds?
Device type: general purpose
Running: Microsoft Windows 10|11
OS CPE: cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows_11
OS details: Microsoft Windows 10 1607 - 11 23H2
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: 2025-02-10T04:18:52
|_  start_date: N/A

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

8. Scan an Entire Network

```
C:\Program Files (x86)\Nmap>nmap 172.16.5.209/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-10 09:50 India Standard Time
Nmap scan report for 172.16.5.150
Host is up (0.0025s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap scan report for 172.16.5.152
Host is up (0.0095s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi

Nmap scan report for 172.16.5.154
Host is up (0.00087s latency).
Not shown: 846 closed tcp ports (reset), 125 filtered tcp ports (no-response), 26 filtered tcp ports (admin-prohibited)
PORT     STATE SERVICE
21/tcp   open  ftp
80/tcp   open  http
3389/tcp open  ms-wbt-server

Nmap scan report for 172.16.5.161
Host is up (0.019s latency).
```

Conclusion:

Nmap is a powerful and flexible tool for network scanning and security analysis. It helps identify open ports, detect running services, analyze vulnerabilities, and even evade firewalls. By mastering Nmap commands, security professionals and network administrators can efficiently audit and secure their systems.