CYBER SECURITY INTERNSHIP

Task 1: Scan Your Local Network for Open Ports

Objective: Learn to discover open ports on devices in your local network to understand network exposure.

- Firstly, successfully installed NMAP on my Windows operating system
- Open Command Prompt (Windows).
- The purpose of this task is to **identify open ports** and **discover potentially exposed services** running on devices within the local network. This helps in understanding the **attack surface** and improving the **network security posture,** using commands below.

1. `nmap --version`

firstly, confirmed my **Nmap version is 7.97**, correctly installed on Windows. ✓

```
Microsoft Windows [Version 10.0.26100.6899]
(c) Microsoft Corporation. All rights reserved.

C:\Users\yagna>nmap --version
Nmap version 7.98 ( https://nmap.org )
Platform: i686-pc-windows-windows
Compiled with: nmap-liblua-5.4.8 openssl-3.0.17 nmap-libssh2-1.11.1 nmap-lib
z-1.3.1 nmap-libpcre2-10.45 Npcap-1.83 nmap-libdnet-1.18.0 ipv6
Compiled without:
Available nsock engines: iocp poll select
```

2. ipconfig

```
C:\Users\yagna>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Unknown adapter Local Area Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::1fd3:53df:8cb5:3a31%19
   IPv4 Address. . . . . . . . . . . : 192.168.1.105
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
```

🔻 3. `nmap -sS 192.168.1.0/24`

This command scanned the **entire local subnet** (256 IP addresses).

```
C:\Users\yagna>nmap -sS 192.168.1.0/24
Starting Nmap 7.98 ( https://nmap.org ) at 2025-10-20 16:00 +0530
Nmap scan report for 192.168.1.1
Host is up (0.015s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
53/tcp   open  domain
80/tcp   open  http
1900/tcp open  upnp
MAC Address: 00:5F:67:38:FF:FC (TP-Link Limited)

Nmap scan report for 192.168.1.106
Host is up (0.011s latency).
All 1000 scanned ports on 192.168.1.106 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: EE:92:CE:89:53:C6 (Unknown)

Nmap scan report for 192.168.1.105
Host is up (0.00058s latency).
Not shown: 981 closed tcp ports (reset)
PORT     STATE    SERVICE
25/tcp   filtered smtp
110/tcp  filtered pop3
119/tcp  filtered nntp
125/tcp  filtered locus-map
135/tcp  open     msrpc
139/tcp  open     netbios-ssn
143/tcp  filtered imap
445/tcp  open     microsoft-ds
465/tcp  filtered smtps
548/tcp  filtered afp
563/tcp  filtered snews
587/tcp  filtered submission
800/tcp  filtered mdbs_daemon
903/tcp  filtered iss-console-mgr
993/tcp  filtered imaps
995/tcp  filtered pop3s
1025/tcp filtered NFS-or-IIS
1122/tcp filtered availant-mgr
1433/tcp filtered ms-sql-s

Nmap done: 256 IP addresses (3 hosts up) scanned in 10.42 seconds
```

🔻 4. `nmap -sS 192.168.1.10`

Tried scanning a specific IP with a **SYN scan**.

```
C:\Users\yagna>nmap -sS 192.168.1.10
Starting Nmap 7.98 ( https://nmap.org ) at 2025-10-20 16:26 +0530
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 1.61 seconds
```

Result:

Host seems down

Reason: Same issue — **ICMP (ping) blocked** by firewall or device.

🔻 4. `nmap -Pn 192.168.1.10`

This bypasses the ping checks and directly attempts a scan.

```
C:\Users\yagna>nmap -Pn 192.168.1.10
Starting Nmap 7.98 ( https://nmap.org ) at 2025-10-20 16:29 +0530
Nmap done: 1 IP address (0 hosts up) scanned in 1.61 seconds
```

Result

1. **No hosts found:** Nmap scanned 192.168.1.10 and reports **"0 hosts up"** — it found **no responsive host** at that IP.
2. **Fast scan, no ports reported:** The scan completed in **1.61 seconds** and returned no open/filtered/closed ports or service info for that IP.

Explanation

1. **Host unreachable or silent:** The target IP is likely **offline, not assigned, or blocking/responding to probes** (powered off, disconnected, wrong IP, or a firewall dropping packets), so Nmap saw no responses.
2. **Scan behavior note (-Pn):** You used -Pn (skip host discovery). That causes Nmap to attempt port probes anyway — but since **no port responses** were received, Nmap still reports the host as not up. This usually means the device simply didn't reply to any probe packets.

☐ Tools Used:

- **Nmap v7.97** on Windows
- Command Prompt (CLI)
- Optional: Wireshark (not used in this scan)

Network Details:

- **IP Range Scanned:** `192.168.1.0/24`
- **Scanning Method:** TCP Connect and SYN scans (`-sS`), with ping disabled using `-Pn`

Results Summary:

Target IP	Host Status	Open Ports	Notes
192.168.1.0/24	0 hosts up	N/A	No hosts responded to ping (ICMP blocked)
192.168.1.10	Host is up	None (all filtered)	All 1000 ports filtered (firewall active)

Observations:

- **No open ports were detected**, meaning either:
  - The devices are well secured.
  - Firewalls are blocking port scans.
  - Hosts are configured to drop all unsolicited traffic.

Security Implications:

- Filtering all ports is generally a **good security practice**.
- However, for network inventory or troubleshooting, it might be necessary to temporarily allow ICMP or certain port responses.
- Some hosts might be unreachable due to strict endpoint firewalls or endpoint protection software.