DAY 1

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.

Tools: Nmap (free), Wireshark (optional)

Nmap

Explanation : Using Nmap to scan the local IP range, we identified which hosts are active. By running the default Nmap scan **(a TCP SYN scan with root privileges or a TCP connect scan without)**, we found that 6 hosts are currently live. We also observed which ports are open on these hosts.

```
┌──(zxeon㉿zxeon)-[~]
└─$ sudo nmap 192.168.0.0/24
[sudo] password for zxeon:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-28 04:39 EDT
Nmap scan report for 192.168.0.1
Host is up (0.0029s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE
53/tcp   open  domain
80/tcp   open  http
443/tcp  open  https
1900/tcp open  upnp
MAC Address: B4:B0:24:EC:82:D1 (TP-Link Limited)

Nmap scan report for 192.168.0.102
Host is up (0.010s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT     STATE SERVICE
```

```
5000/tcp open  upnp
7000/tcp open  afs3-fileserver
MAC Address: 86:56:FD:FF:1A:E6 (Unknown)

Nmap scan report for 192.168.0.127
Host is up (0.0063s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
49152/tcp open  unknown
62078/tcp open  iphone-sync
MAC Address: 5A:9B:20:35:92:4B (Unknown)

Nmap scan report for 192.168.0.230
Host is up (0.0086s latency).
Not shown: 999 closed tcp ports (reset)
PORT     STATE    SERVICE
5060/tcp filtered sip
MAC Address: F6:C7:E3:24:2F:9E (Unknown)

Nmap scan report for 192.168.0.247
Host is up (0.00014s 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
MAC Address: C8:5E:A9:F6:E2:FD (Intel Corporate)

Nmap scan report for 192.168.0.154
Host is up (0.0000010s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
```

```
Nmap done: 256 IP addresses (6 hosts up) scanned in 6.92 seconds
```

Wireshark

When running an Nmap scan, we can analyze the network traffic using Wireshark. By looking at the captured packets, we can see how Nmap identifies live hosts on the network by sending ARP request.

After detecting which hosts are active, Nmap sends TCP handshake packets to those hosts to discover which ports are open.

```
24  8.089475892 TPLink_ec:82:d1 Broadcast   ARP 60  Who has 192.168.0.248
25  8.667647878 PCSSystemtec_a1:2c:72  Broadcast  ARP 42  Who has 192.1
26  8.667778782 PCSSystemtec_a1:2c:72  Broadcast  ARP 42  Who has 192.1
27  8.667831493 PCSSystemtec_a1:2c:72  Broadcast  ARP 42  Who has 192.1
28  8.667867235 PCSSystemtec_a1:2c:72  Broadcast  ARP 42  Who has 192.1
29  8.667902828 PCSSystemtec_a1:2c:72  Broadcast  ARP 42  Who has 192.1
30  8.667937990 PCSSystemtec_a1:2c:72  Broadcast  ARP 42  Who has 192.1
31  8.667976712  PCSSystemtec_a1:2c:72  Broadcast  ARP 42  Who has 192.1
32  8.668010908 PCSSystemtec_a1:2c:72  Broadcast  ARP 42  Who has 192.1
33  8.668045290 PCSSystemtec_a1:2c:72  Broadcast  ARP 42  Who has 192.1
34  8.668079780 PCSSystemtec_a1:2c:72  Broadcast  ARP 42  Who has 192.1
35  8.672992106 TPLink_ec:82:d1 PCSSystemtec_a1:2c:72  ARP 60  192.168.0
```

```
584 11.230691479 192.168.0.154  192.168.0.102  TCP 58  63109 → 199 [SYN] Seq
585 11.230828870 192.168.0.154  192.168.0.230 TCP 58  63109 → 199 [SYN] Seq
586 11.230895622  192.168.0.154  192.168.0.247 TCP 58  63109 → 139 [SYN] S
587 11.231082674 192.168.0.154  192.168.0.1  TCP 58  63109 → 139 [SYN] Seq=0
588 11.231133007 192.168.0.154  192.168.0.102  TCP 58  63109 → 25 [SYN] Seq=
589 11.231169890 192.168.0.154  192.168.0.230 TCP 58  63109 → 25 [SYN] Seq=
590 11.231203190 192.168.0.154  192.168.0.247 TCP 58  63109 → 199 [SYN] Seq
```

```
591 11.231319618  192.168.0.154 192.168.0.1   TCP 58   63109 → 199 [SYN] Seq=(
592 11.231361394 192.168.0.154 192.168.0.102  TCP 58   63109 → 53 [SYN] Seq=
593 11.231396485 192.168.0.154 192.168.0.230 TCP 58   63109 → 53 [SYN] Seq=
594 11.231431806 192.168.0.154 192.168.0.247 TCP 58   63109 → 25 [SYN] Seq=
595 11.231492632 192.168.0.154 192.168.0.1   TCP 58   63109 → 25 [SYN] Seq=0
596 11.231528192 192.168.0.154 192.168.0.102  TCP 58   63109 → 8888 [SYN] S(
597 11.231549851 192.168.0.247 192.168.0.154 TCP 60   139 → 63109 [SYN, ACK
```

Interview Questions

1. **What is an open port?**

   A port that is accepting connections and can communicate with network services.

2. **How does Nmap perform a TCP SYN scan?**

   It sends SYN packets to ports and checks responses. A SYN-ACK reply means the port is open.

3. **What risks are associated with open ports?**

   They can expose services to attacks, such as exploits or unauthorized access.

4. **Explain the difference between TCP and UDP scanning.**

   TCP scans look for connection-oriented services; UDP scans check connectionless services, often without clear responses.

5. **How can open ports be secured?**

   By closing unused ports, using firewalls, and securing services with authentication and updates.

6. **What is a firewall's role regarding ports?**

   It filters traffic, allowing or blocking connections to ports based on rules.

7. **What is a port scan and why do attackers perform it?**

A port scan checks which ports are open. Attackers use it to find targets and plan attacks.

8. **How does Wireshark complement port scanning?**

   It captures and analyzes packets, helping you see how scans work and verify network behavior.