

ELEVATE LABS INTERNSHIP

Day1

Name : Mohamed Riyas J

Role: Cyber Security Analyst

Task: 01

Title: Scan Your Local Network for Open Ports

Date: 23-06-2025

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

Tools :

NMAP for Scan the Network to list the Open Ports.

Wireshark for capture the packets which is generated by nmap to scan the network

Steps to be followed to completed day 1 task

Step 1: Find the Target IPs (Open Terminal in local machine).

- Use ipconfig in terminal.
- Local Machine IP is 192.168.29.86

```
Windows PowerShell
PS C:\Users\Mohamed Riyas> ipconfig

Windows IP Configuration

Wireless LAN adapter Local Area Connection* 3:

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

Wireless LAN adapter Local Area Connection* 4:

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

Ethernet adapter VMware Network Adapter VMnet1:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::3b07:75e2:8982:aa4f%6
    IPv4 Address. . . . . : 192.168.42.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::70d8:d80d:385c:1b68%11
    IPv4 Address. . . . . : 192.168.158.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix  . :
    IPv6 Address. . . . . : 2405:201:e032:e9:256:1a77:e3b8:796f
    Temporary IPv6 Address. . . . . : 2405:201:e032:e9:cc6e:4dbf:46df:d9af
    Link-local IPv6 Address . . . . . : fe80::5787:c1c3:aee7:7d95%18
    IPv4 Address. . . . . : 192.168.29.86
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::2aa9:15ff:fe69:b30c%18
                                192.168.29.1

PS C:\Users\Mohamed Riyas> |
```

Step2: Open VMware with install kali linux act as a attacker to scan the victim machine network

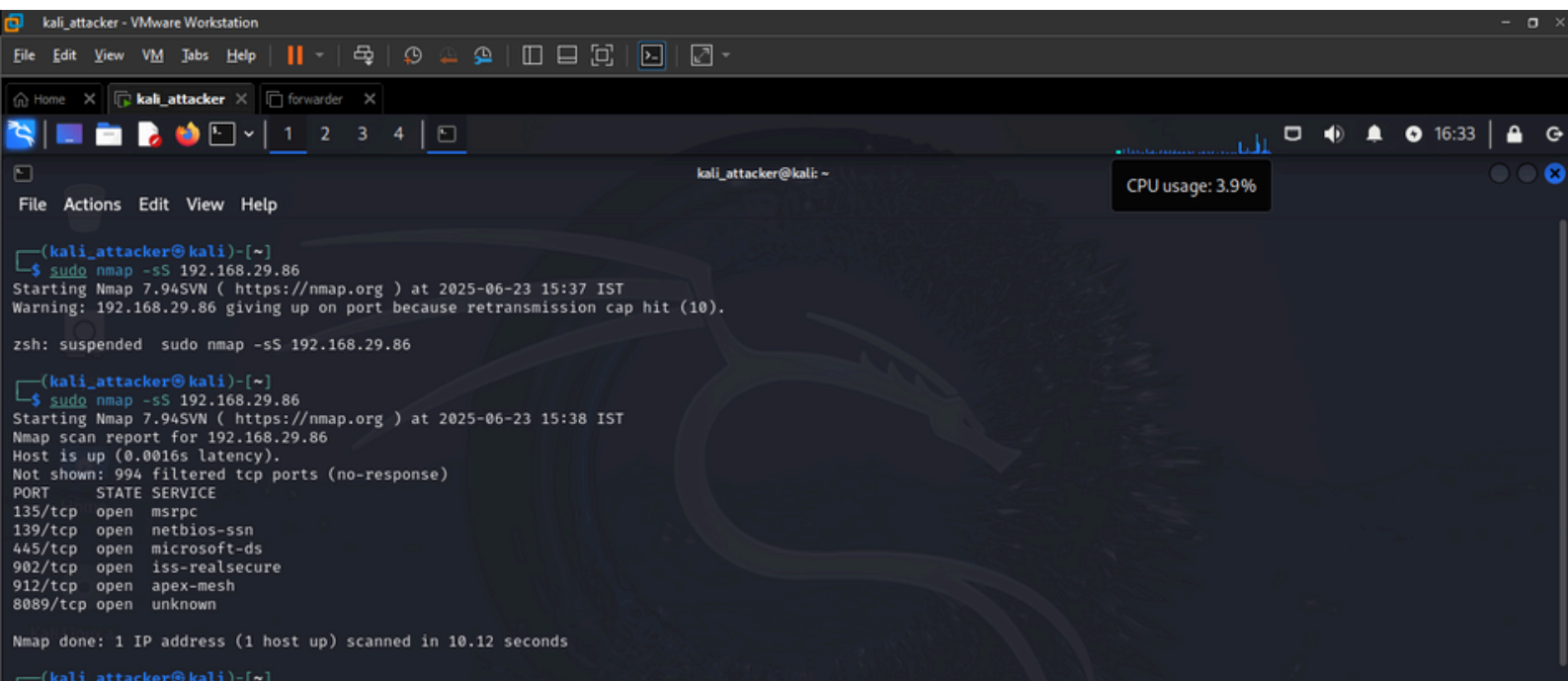
- Check the kali linux IPs, which is performed as a attacker.

```
(kali_attacker@kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:40:f4:5e brd ff:ff:ff:ff:ff:ff
    inet 192.168.158.137/24 brd 192.168.158.255 scope global dynamic noprefixroute eth0
        valid_lft 1145sec preferred_lft 1145sec
    inet6 fe80::20c:29ff:fe40:f45e/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

(kali_attacker@kali)-[~]
$
```

Step3: Scan the Target IPs

- Use nmap command on the kali to TCP SYN scan "sudo nmap -sS 192.168.29.86"



```
(kali_attacker@kali)-[~]
$ sudo nmap -sS 192.168.29.86
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-23 15:37 IST
Warning: 192.168.29.86 giving up on port because retransmission cap hit (10).
zsh: suspended sudo nmap -sS 192.168.29.86

(kali_attacker@kali)-[~]
$ sudo nmap -sS 192.168.29.86
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-23 15:38 IST
Nmap scan report for 192.168.29.86
Host is up (0.0016s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
902/tcp    open  iss-realsecure
912/tcp    open  apex-mesh
8089/tcp   open  unknown

Nmap done: 1 IP address (1 host up) scanned in 10.12 seconds

(kali_attacker@kali)-[~]
```

- above image list open ports of target machine.

WIRESHARK

- Wireshark is a **network protocol analyzer** used to **capture and inspect network traffic** in real time.

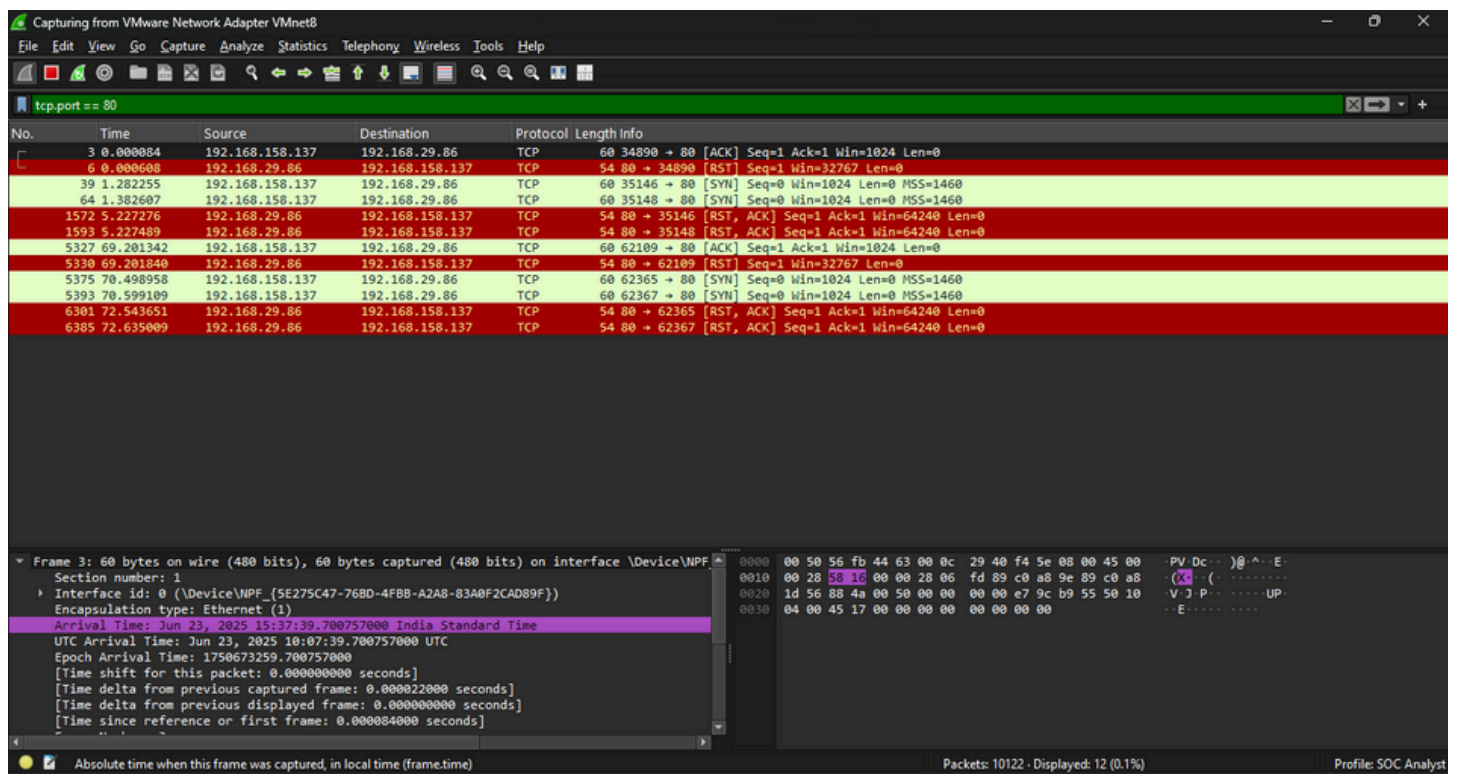
Why is it used

- Analyze suspicious traffic (e.g., malware, port scans)
- Debug network issues
- Investigate attacks (like MITM, port scanning)
- Monitor protocols (HTTP, DNS, TCP, etc.)

Step4: Use Wireshark for packet capture

Source IP : 192.168.158.137

Destination IP : 192.168.29.86



Common Network Services and Their Ports

Port 22 – SSH (Secure Shell)

- **Port Number:** 22
- **Protocol:** TCP
- **Service:** SSH (Secure Shell)
- **Use:** Remote login securely to Linux/Unix servers
- **Security:** Encrypted, safe from sniffing

Capturing from VMware Network Adapter VMnet8

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port == 22

No.	Time	Source	Destination	Protocol	Length	Info
48	1.285182	192.168.158.137	192.168.29.86	TCP	60	35146 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
67	1.387741	192.168.158.137	192.168.29.86	TCP	60	35148 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1581	5.227364	192.168.29.86	192.168.158.137	TCP	54	22 → 35146 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
1603	5.227613	192.168.29.86	192.168.158.137	TCP	54	22 → 35148 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
5341	69.294208	192.168.158.137	192.168.29.86	TCP	60	62365 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
5355	70.395823	192.168.158.137	192.168.29.86	TCP	60	62367 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
5579	71.347784	192.168.29.86	192.168.158.137	TCP	54	22 → 62365 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
6209	72.434547	192.168.29.86	192.168.158.137	TCP	54	22 → 62367 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0

wireshark_VMware Network Adapter VMnet8\IIO082.pcapng

Packets: 10150 - Displayed: 8 (0.1%)

Profile: SOC Analyst

Port 23 – Telnet

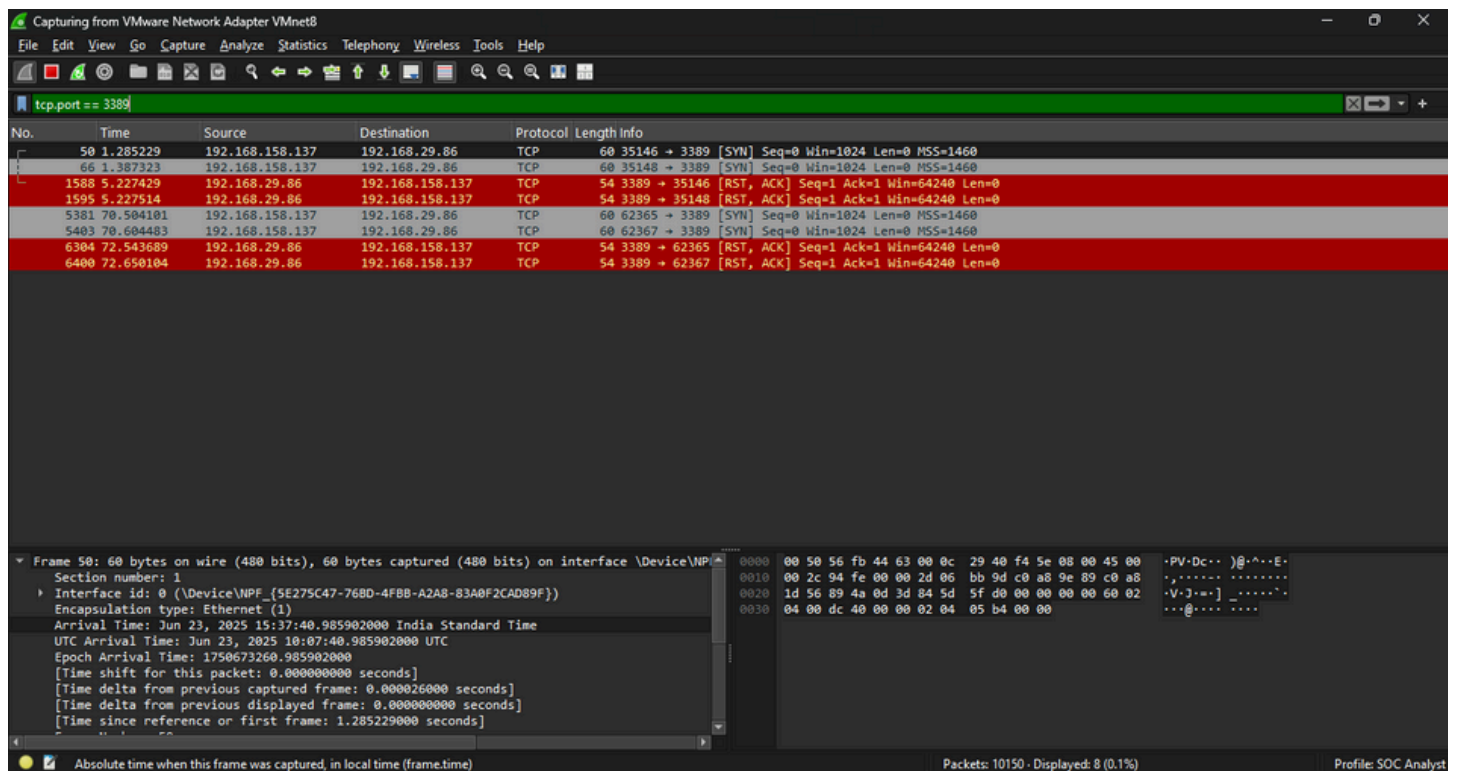
- **Port Number:** 23
- **Protocol:** TCP
- **Service:** Telnet
- **Use:** Remote login (very old method)
- **Security:** Not encrypted – sends passwords in plaintext
- **Recommendation:** Avoid using; replace with SSH

Port 80 – HTTP

- **Port Number:** 80
- **Protocol:** TCP
- **Service:** HTTP (Hypertext Transfer Protocol)
- **Use:** Websites without encryption (non-HTTPS)
- **Security:** Not secure; data visible in transit
- **Recommendation:** Redirect to HTTPS

Port 3389 – RDP (Remote Desktop Protocol)

- **Port Number:** 3389
- **Protocol:** TCP
- **Service:** RDP
- **Use:** Remote desktop access to Windows systems
- **Security:** ! Can be brute-forced if exposed
- **Best Practice:** Use VPN + strong passwords



1. What is an open port?

- An open port is a network port that is actively listening for incoming connections. Services such as web servers, email servers, or file-sharing applications use open ports to communicate.

2. How does Nmap perform a TCP SYN scan?

- Nmap sends **TCP SYN packets** to a target port.
- If the port is open, the target responds with a **SYN-ACK packet**.
- If the port is closed, the target sends a **RST (Reset)** packet.
- This method is often called a "half-open" scan because the connection is not fully established

3. What risks are associated with open ports?

- Unauthorized access or exploitation of vulnerabilities in services.
- Denial-of-service (DoS) attacks targeting specific services.
- Exposure of sensitive information through misconfigured services.
- Malware propagation using unprotected or weakly configured ports.

4. Explain the difference between TCP and UDP scanning.

- **TCP Scanning:**
 - Focuses on ports using the Transmission Control Protocol.
 - More reliable as it confirms active services using TCP's connection-oriented nature.
- **UDP Scanning:**
 - Focuses on ports using the User Datagram Protocol.
 - Harder to detect as UDP is connectionless and does not send explicit acknowledgments.
 - Typically slower due to retries caused by packet loss.

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

- A firewall monitors and controls incoming and outgoing network traffic.
- It allows or blocks data packets based on security rules to prevent unauthorized access to open ports.
- Firewalls can restrict specific IP addresses, protocols, or port ranges.

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

- A port scan is the process of systematically probing a target to identify open ports and associated services.
- **Why attackers perform it:**
 - To find vulnerabilities in services running on open ports.
 - To map the network and identify potential targets for exploitation.

8. How does Wireshark complement port scanning?

- Wireshark is a network traffic analyzer.
- It can capture and analyze the packets exchanged during a port scan, providing insights into:
 - Which ports are being scanned.
 - The type of scan being performed (e.g., SYN scan, UDP scan).
 - Responses from the target system, which can confirm open or closed ports.
