8/4/2025

Scanning Network

Using NMAP, WireShark

@SRCybersecurity

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.

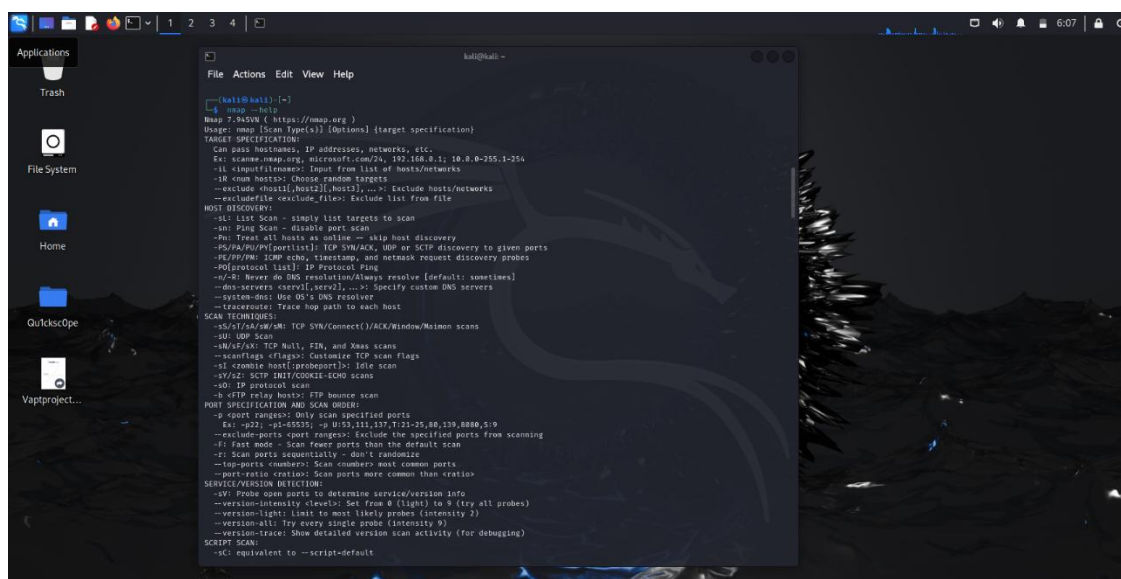**Tools**: Nmap (free), Wireshark (optional).

Machine: Kali (Linux).

1.Install Nmap from official website.

Nmap on **Kali Linux** is usually **pre-installed**. However, we can check it. If it is missing or not by running following commands:

nmap --version or **nmap --help**

--version show the installed version of nmap and **--help** is nmap commands help book.

And to ensure it's up to date; you can install or reinstall it by using the following commands:
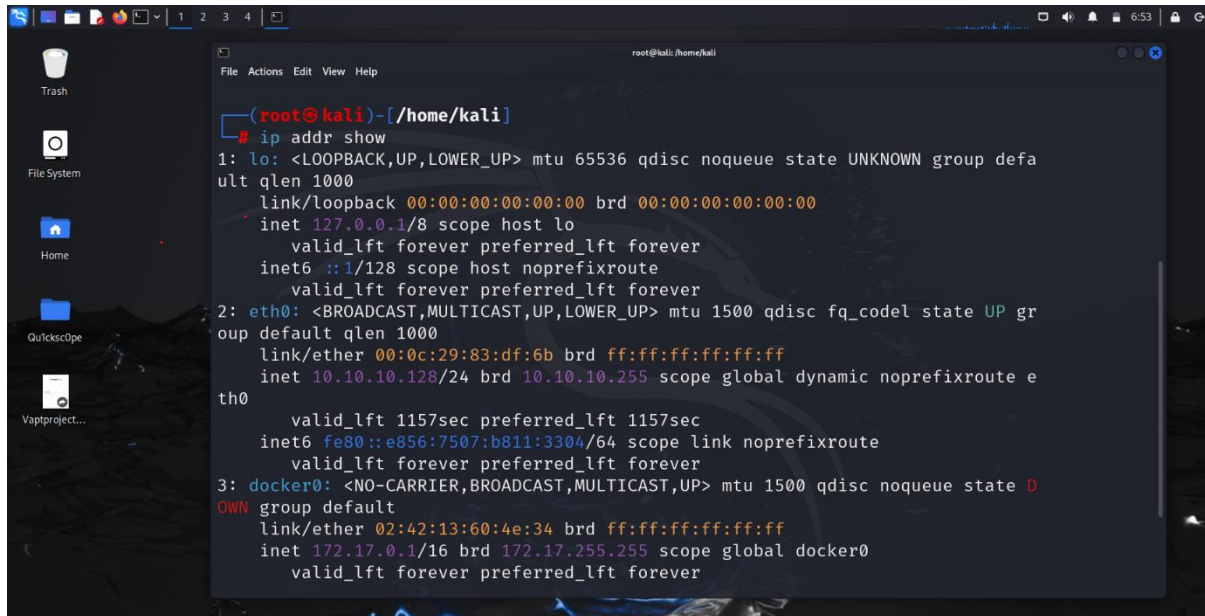
sudo apt update nmap

sudo aptget update nmap

sudo apt install nmap

apt or apt-get for package handling tool so you can install/update/remove nmap by using **sudo** for root privileges.

2.Find your local IP range (e.g., 192.168.1.0/24).
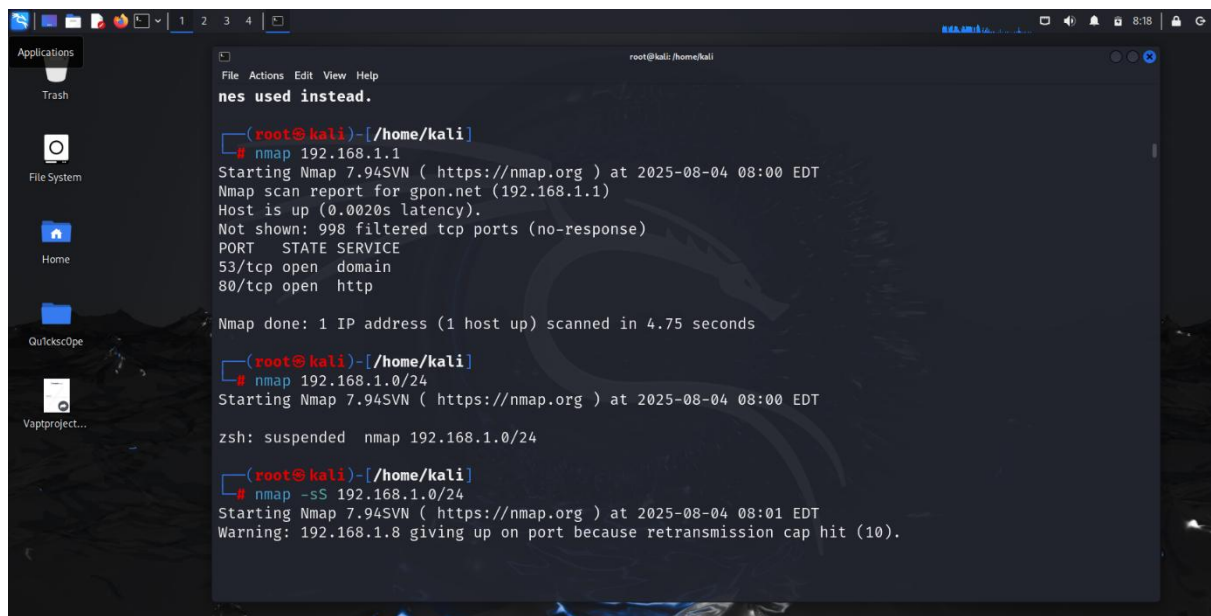

On terminal use command to find local IP range:

➢ **ip addr show** is a Linux command to determine your **local subnet and IP address**, from which you can infer the range.
➢ Ip adrress given below is **10.10.10.128/24** ip of my VM

3.Run: nmap -sS 192.168.1.0/24 to perform TCP SYN scan.

➢ **Nmap -sS 192.168.1.0/24** -sS switch performs a TCP SYN scan, which is one of the most common and stealthy types of port scans. It's often referred to as a "half-open" scan because it doesn't complete the full TCP handshake.

➢ TCP SYN packets sent by a tool (like Nmap) to a target system to check if specific TCP ports are open. These packets are part of TCP SYN scans and are used for probing— testing how a system responds.

➢ Send a **SYN packet** to a port.

➢ The target system replies:

• **SYN-ACK** → Port is **open**
• **RST** → Port is **closed**
• **No response** or **ICMP error** → Port is **filtered** (likely by a firewall)
• You send **RST** (reset) instead of ACK to avoid a full connection.

➢ Mostly used to avoid detection
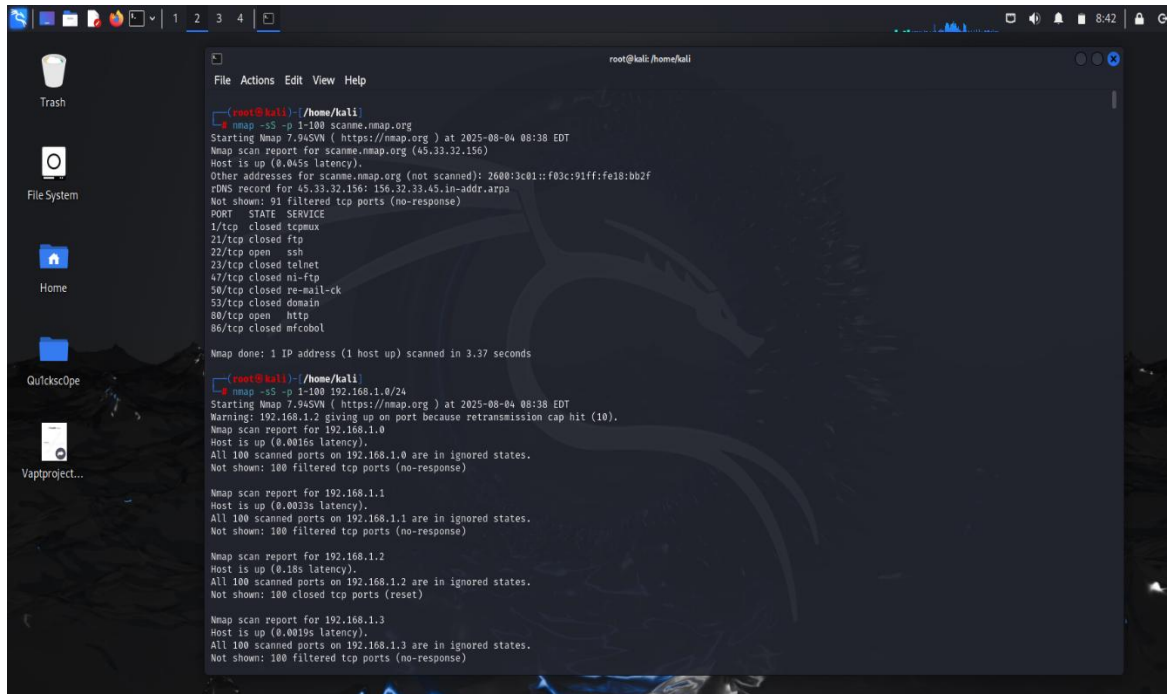
➢ After running nmap -sS 192.168.1.0/24 command keep getting retransmission cap hit because of firewall filteration, so I narrowed it down by using specific ports range using nmap switch **-p 1-100.**

4.Note down IP addresses and open ports found.

➢ Most common open/filtered ports are 21, 22, 23, 53 ,80 ,443, 123.
➢ Since pinging probes are getting blocked by firewall, I used nmap -**Pn 192.168.1-24** to minimize the time put the IP range but still not discovered the live host yet.

➢ Try it with only host discovery switch by using **nmap -sn 192.168.1.0/24**

5.Optionally analyze packet capture with Wireshark.

➢ We can analyze the transmitting packets by using filters tcp, tcp.port, tcp.port == 80, udp, dns, http, http2, http3 and do on.

➢ It provides packets in- depth detail how system actually sent/receive data over connected networks.
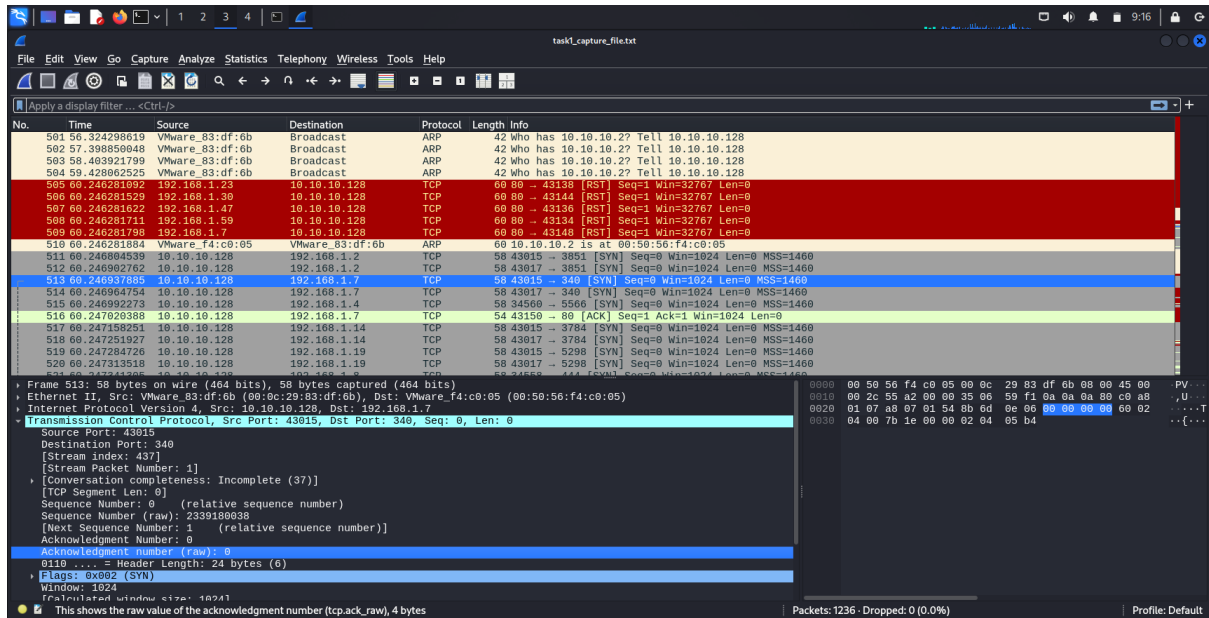
6.Research common services running on those ports.

➢ Most commonly probes are TCP SYN packets are sent by the nmap to check whether the target system is running or not then it sends back SYN-ACK but since we are doing half open scan it only sends SYN packets and don't wait for the ACK to establish connection.

➢ RST flag is sent back when the probes are getting blocked or unreachable.
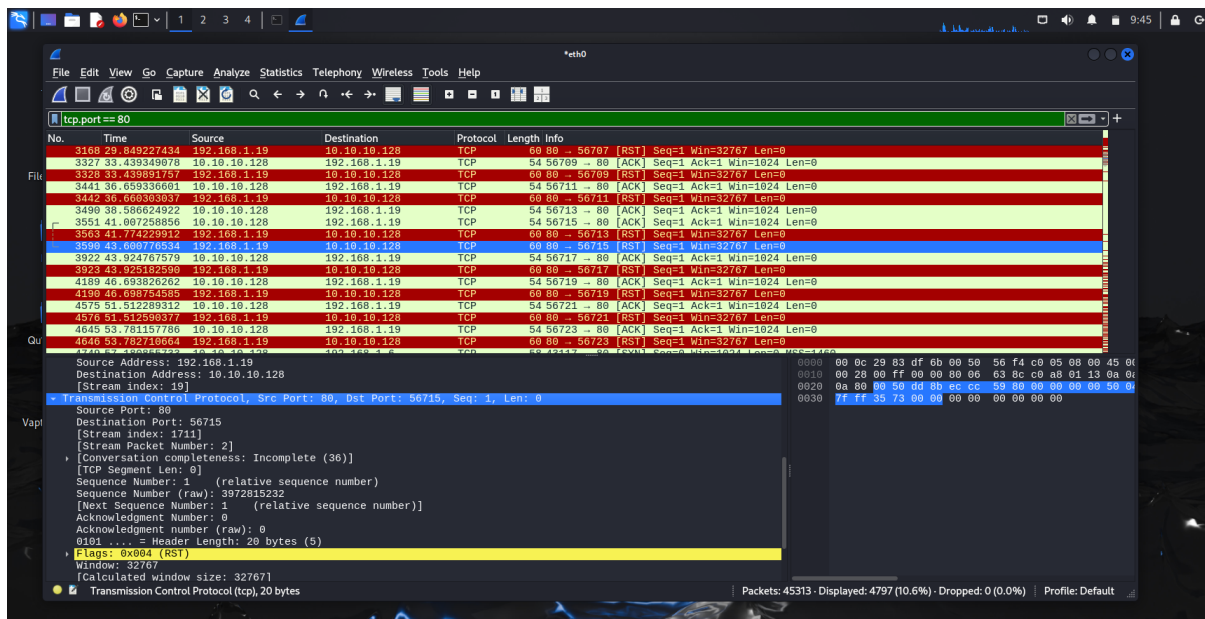
➢ Most common open/filtered ports are 21 ftp, 22 ssh, 23 telnet,80 http ,443 https, 123 udp, 53 dns**.**
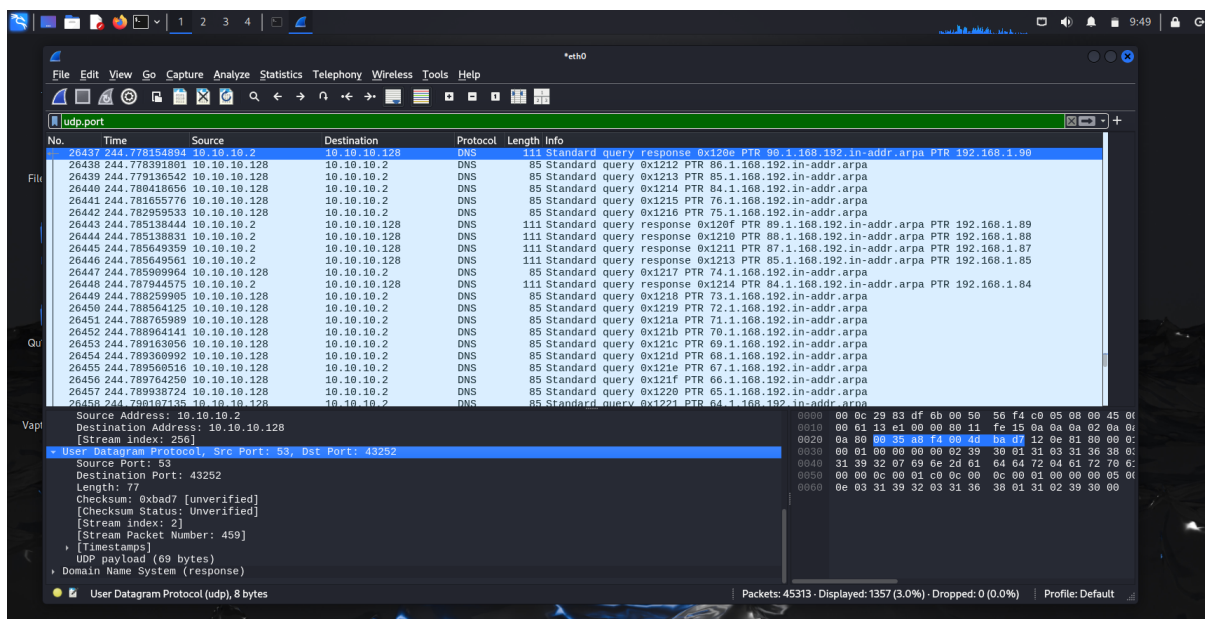
7.Identify potential security risks from open ports.

➢ They represent potential entry points into your system. If a service listening on a port is misconfigured, outdated, or vulnerable, it could be exploited by an attacker.

➢ Exposed Vulnerable Services

• Old or unpatched services may contain known vulnerabilities.

  o Open port 21 (FTP) → Might allow anonymous access or be vulnerable to brute-force.
  o Open port 445 (SMB) → Could be vulnerable to exploits like EternalBlue.

➢ Information Leakage

• Services often leak system info:

  o Web servers (port 80/443) may expose server versions, frameworks, and internal paths.
  o SSH (port 22) banners can reveal OS and version.

➢ Brute-force and Credential Attacks

• Open ports like:

  o 22 (SSH) → Targeted with brute-force password attempts.
  o 3389 (RDP) → Common in ransomware attacks.

➢ Denial-of-Service (DoS) Attacks

• Some services are vulnerable to resource exhaustion or flooding.

• Even if not exploited, they can be overwhelmed and crash.

•

➢ Backdoors or Rogue Services

• Malware may open ports for remote access (e.g., reverse shells).

• Unauthorized open ports may indicate compromise.

➢ Increased Attack Surface

• The more ports you leave open, the more opportunities attackers have to:

  o Scan your network

  o Find misconfigurations

  o Exploit vulnerabilities

END