Task 1: Scan Your Local Network For Open Ports

**Objective:**

To understand network exposure by identifying which ports are open on devices connected to your local network. This helps develop basic network reconnaissance skills.

**Tools Required:**

Nmap (for port scanning)

Wireshark (optional, for packet analysis)

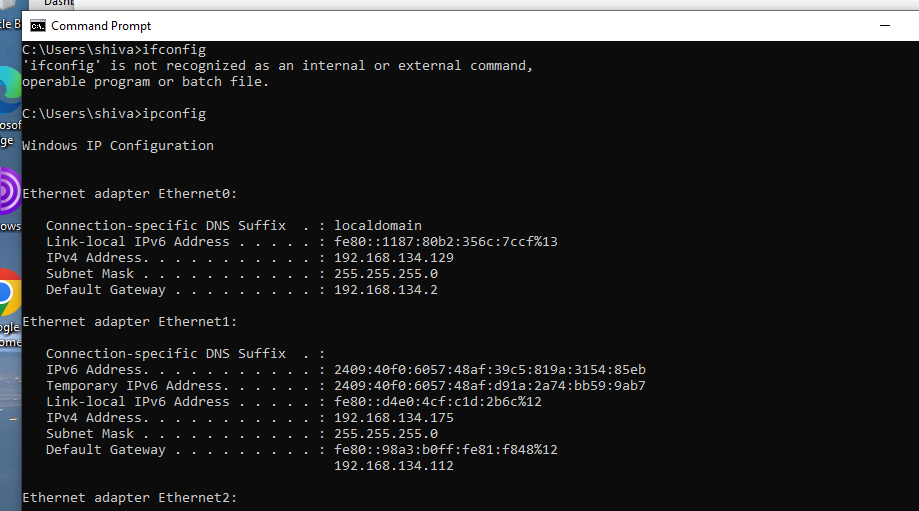
**Steps to Scanning:**

**Step-1.** start the kali linux or install nmap from official website

**Step-2**. Find Your IP Range

Example format: my ipaddress is 192.168.134.0/24

To find Ip address, Run ipconfig in cmd



**Step-3.** Run a TCP SYN Scan

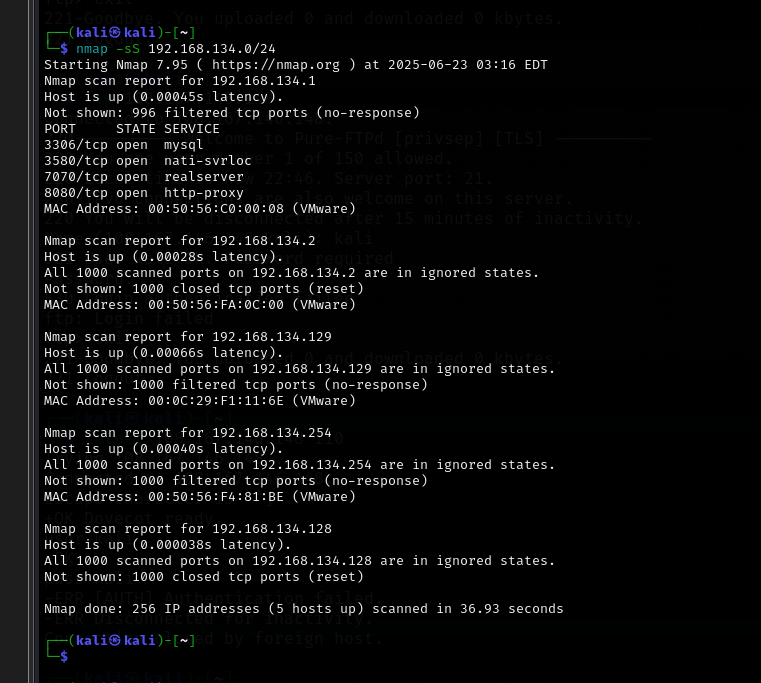
Run this command in terminal:

*nmap -sS 192.168.134.0/24*

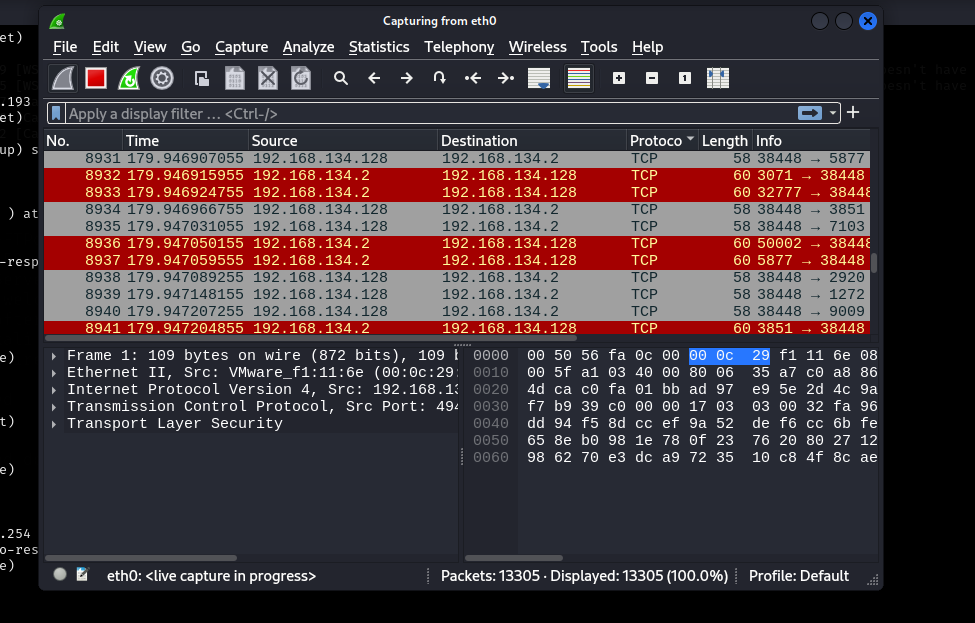
This will scan all devices in your subnet for open ports.

**Step-4**. Note IPs and Open Ports

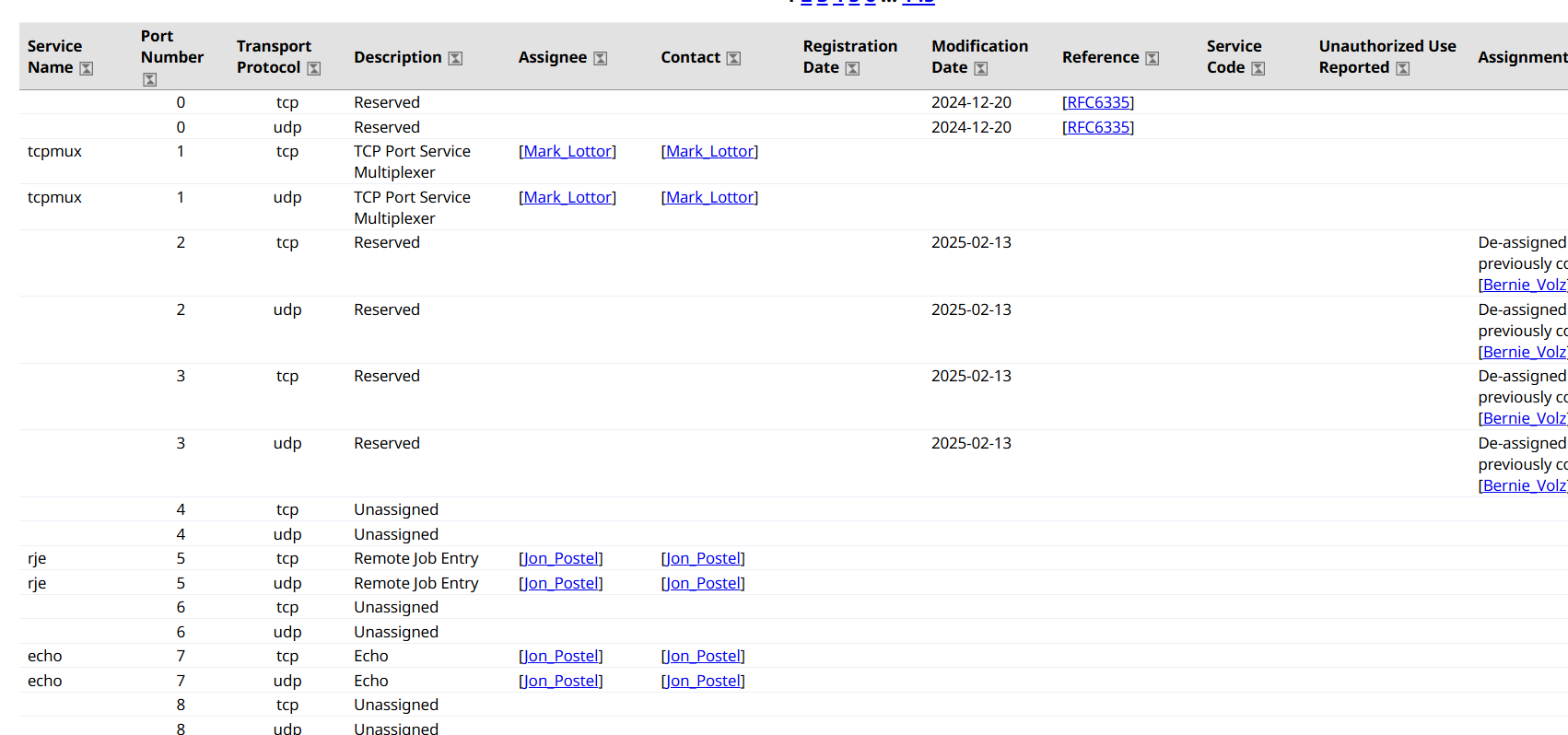
Write down which IP addresses have which ports open.



**Step-5**. Use Wireshark to capture packets while scanning to analyze how port scanning works at the network level.



**Step-6:**I have used websites like SpeedGuide or IANA port list to identify services running on open ports.



**Step 7**: Identify potential security risks from open ports

After I scanned my local network using Nmap, I got a list of devices with open ports. Each open port means that a service is running and listening for connections. So in this step, I checked what services are running on those ports and whether they are safe or not.

For example, if port 21 is open, it usually means FTP is running — but FTP is not secure because it doesn’t encrypt data. So that could be risky. Similarly, port 22 is used for SSH, which is generally safe, but if the password is weak or the version is old, it could be hacked.

I also found that ports like 445 (used for file sharing) are common targets for ransomware. So leaving such ports open without a firewall or strong configuration is a risk.

Basically, I looked at each open port, searched what it's used for, and then figured out whether it could be dangerous if someone tried to exploit it.7. Identify Security Risks.

