****

**ELEVATE LABS  
Cyber Security Internship**

**Task 1  
Documetation Report  
Submitted by Suhaila P.S**

**Task 1: Scan Your Local Network for Open Ports**

**Objective**

Learn to discover open ports on devices in my local network to understand network exposure and potential security risks.

**Tools Used**

* **Nmap** (free, network scanner)
* **Wireshark** (optional, network packet analyzer)

**Procedure and Findings**

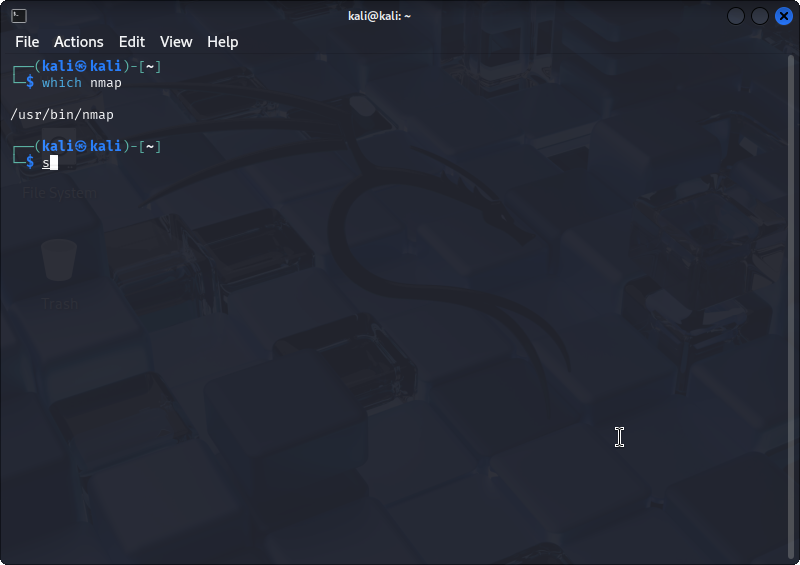
**Step 1: Open Terminal**

**Step 2: Check Nmap Installation**

Checked if Nmap is installed by running:

which nmap

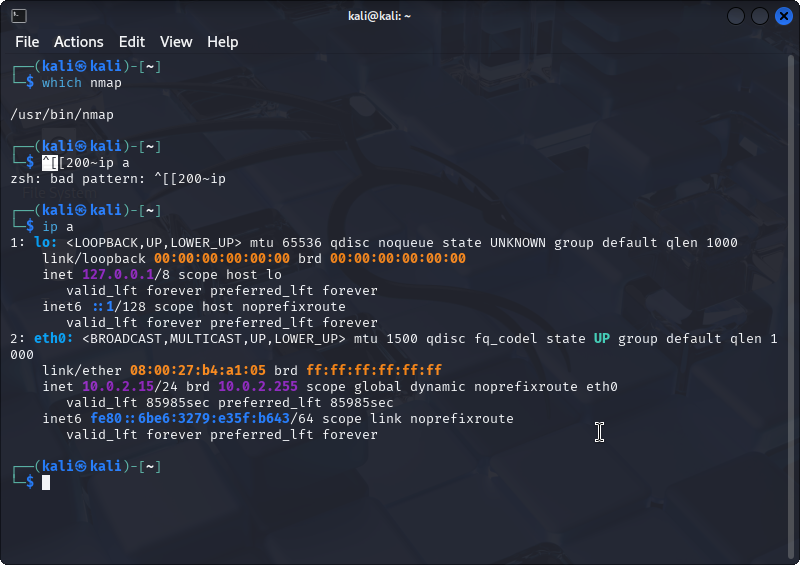
Output confirmed Nmap is installed at /usr/bin/nmap.



**Step 3: Identify Local IP Address and Subnet**

Ran command:

ip a

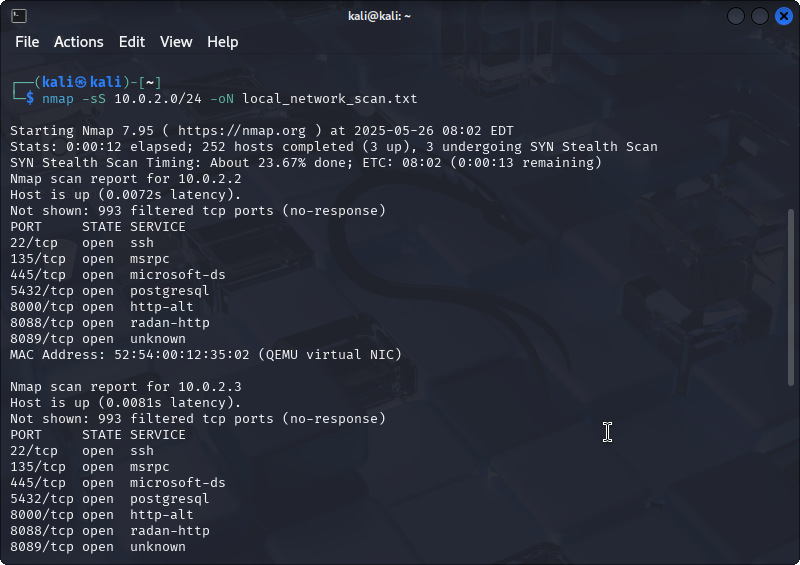
Found IP address and subnet, e.g., 10.0.2.15/24, meaning the subnet is 10.0.2.0/24.  
  


**Step 4: Perform Network Scan with Nmap**

Executed:

nmap -sS 10.0.2.0/24 -oN local\_network\_scan.txt

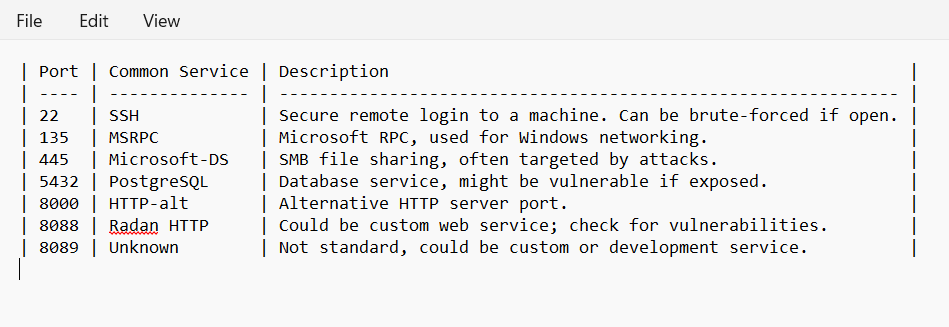
A TCP SYN scan was run to identify open ports in the subnet. The output was saved to local\_network\_scan.txt





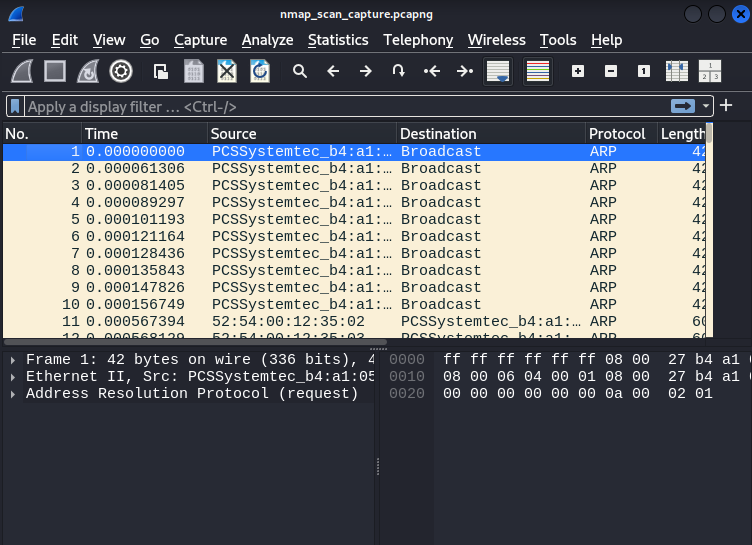
**Step 5: Review Scan Results**

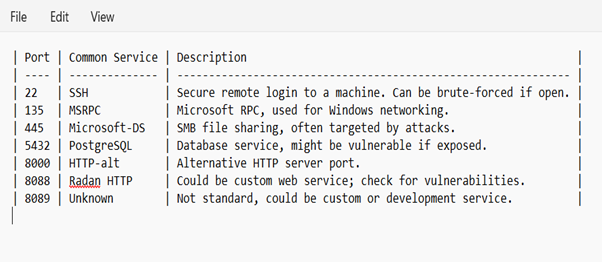
Displayed the scan results using:

cat local\_network\_scan.txt  
  
Devices with open ports were identified.  
  


**Step 6: (Optional) Analyze Traffic Using Wireshark**

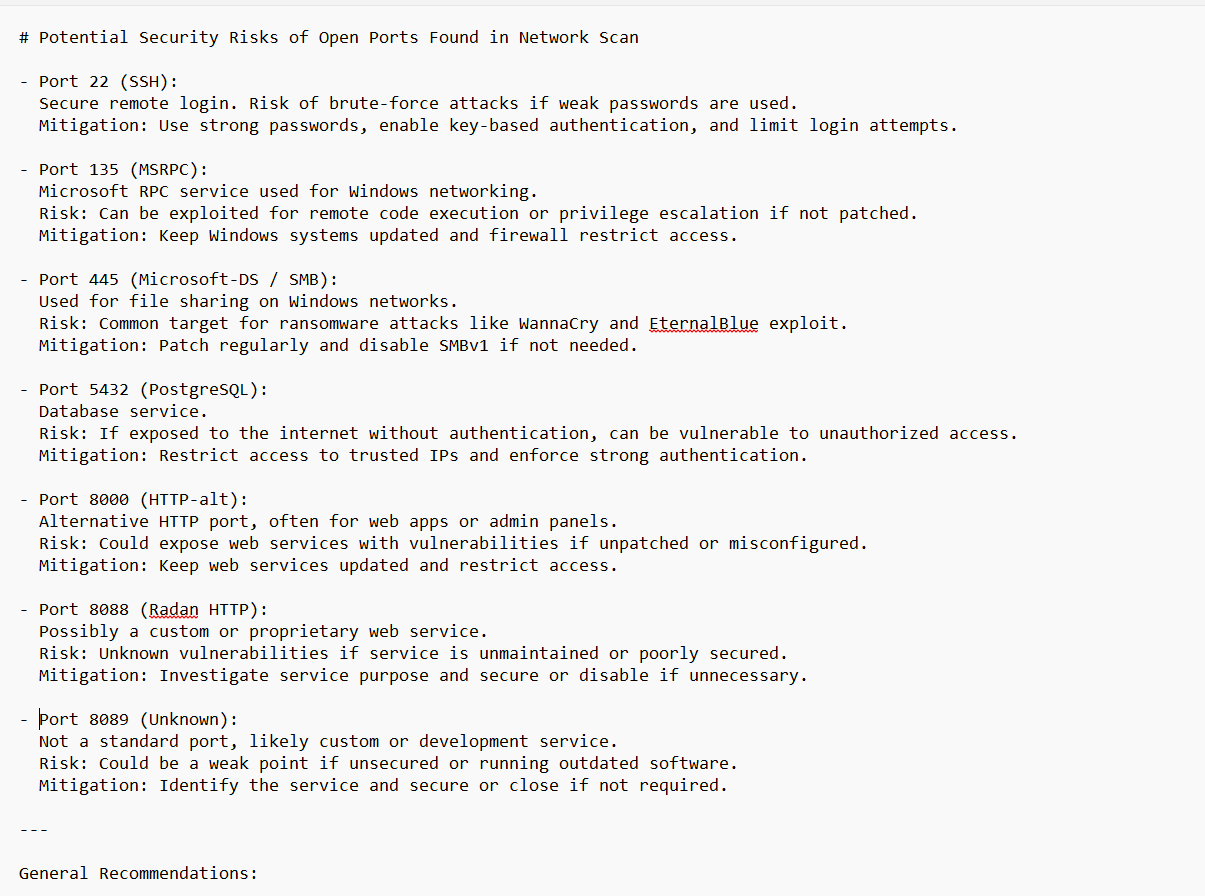
Launched Wireshark, captured packets during scan, and applied filter to focus on the target IP. This helped visualize network traffic generated by the scan.



Step 7: Research Services Running on Open Ports  
  


**Step 8: Identify Potential Security Risks**

* **Port 22 (SSH):** Risk of brute-force attacks if weak passwords are used.
* **Port 135 (MSRPC):** Target for Windows exploits; should be secured.
* **Port 445 (SMB):** Frequently targeted by malware and ransomware like WannaCry.
* **Port 5432 (PostgreSQL):** Should be restricted to authorized users only.
* **Ports 8000, 8088, 8089:** May expose custom services; need further inspection.
* **General:** Unnecessary open ports increase attack surface and should be closed or firewalled.



**Outcome**

This task enhanced understanding of:

* Network scanning using Nmap.
* Identifying active hosts and their open ports on the network.
* Researching port services and understanding their security implications.
* Basic network security awareness and reconnaissancSe skills.