Elevate Labs - Cybersecurity Internship: Task 1 Report

Task Objective

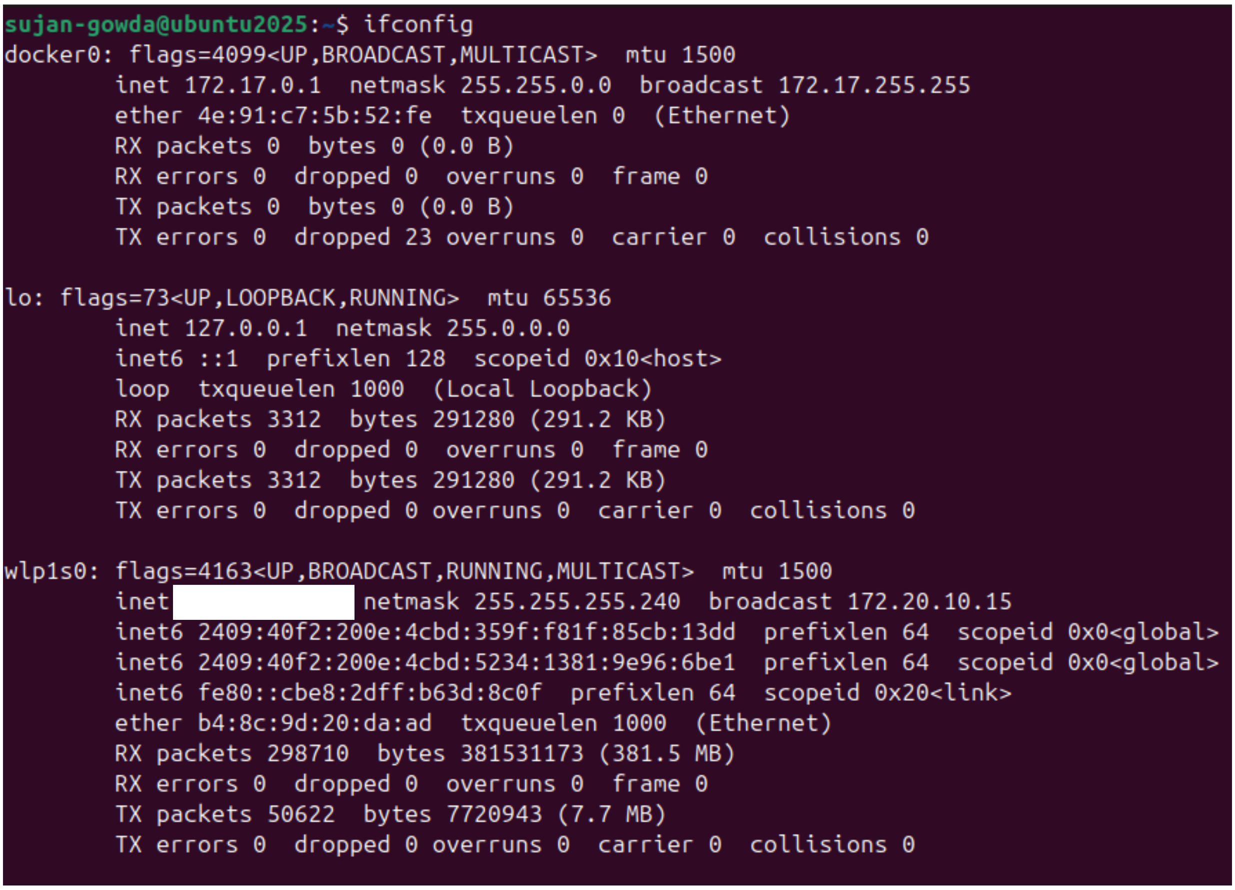
The objective of this task was to learn and apply basic network reconnaissance skills by scanning my local network for open ports. This process helps to understand the network's exposure and identify potential security vulnerabilities.

Tools Used

Nmap (Network Mapper): A free and open-source tool used for network discovery and security auditing. It was the primary tool for performing the port scan.

Methodology

1. **Local Network IP Range Identification:** I first identified my local IP address and the corresponding IP range for the network. This was done by using the ipconfig command on Windows or ifconfig on Linux/macOS.

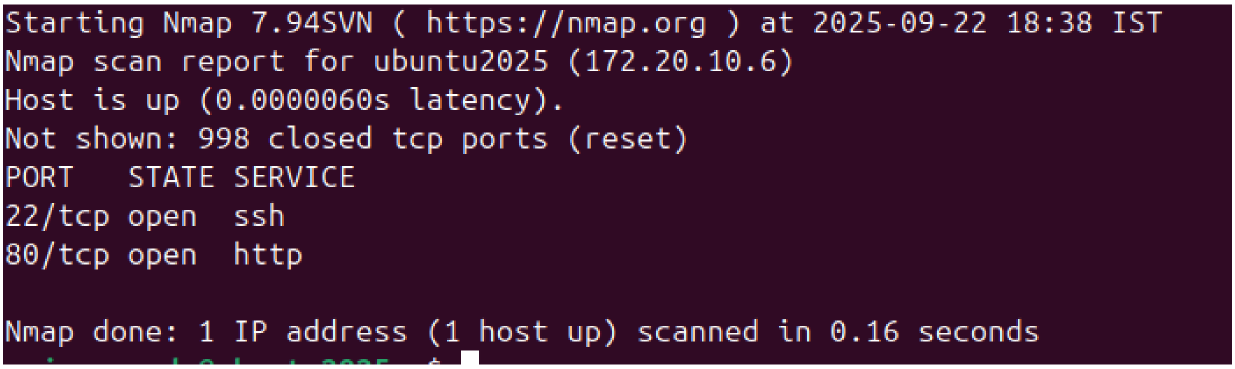


```
sujan-gowda@ubuntu2025:~$ ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 4e:91:c7:5b:52:fe  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 23 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 3312  bytes 291280 (291.2 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3312  bytes 291280 (291.2 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlp1s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet [redacted] netmask 255.255.255.240  broadcast 172.20.10.15
        inet6 2409:40f2:200e:4cbd:359f:f81f:85cb:13dd  prefixlen 64  scopeid 0x0<global>
        inet6 2409:40f2:200e:4cbd:5234:1381:9e96:6be1  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::cbe8:2dff:b63d:8c0f  prefixlen 64  scopeid 0x20<link>
        ether b4:8c:9d:20:da:ad  txqueuelen 1000  (Ethernet)
        RX packets 298710  bytes 381531173 (381.5 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 50622  bytes 7720943 (7.7 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

2. **TCP SYN Scan with Nmap:** I used Nmap to perform a TCP SYN scan (also known as a half-open scan) on the identified IP range. The command used was nmap -sS <local IP range>. This scan type is fast and stealthy, as it doesn't complete the full TCP handshake.



```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-09-22 18:38 IST
Nmap scan report for ubuntu2025 (172.20.10.6)
Host is up (0.0000060s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
```

3. **Analysis of Scan Results:** he open ports identified were 22 (running SSH) and 80 (running HTTP). SSH is commonly used for secure remote access, and HTTP is used for web traffic.

PORT	SERVICE	STATE
22/tcp	OPEN	SSH
80/tcp	OPEN	HTTP

4. **Identification of Security Risks:** Based on the discovered open ports, I evaluated potential security risks. The open SSH port (22) could be vulnerable to brute-force password attacks if a weak password is used. The open HTTP port (80) could be a risk if the web service running on it has unpatched vulnerabilities or is misconfigured, potentially allowing an attacker to gain unauthorized access or sensitive information.

5. **Packet Capture Analysis (Optional):** Using Wireshark, I captured the network traffic while the Nmap scan was in progress. This allowed me to visualize the SYN, SYN-ACK, and RST packets that are characteristic of a TCP SYN scan, confirming the scan's behavior.

Conclusion

This task provided valuable hands-on experience in network reconnaissance and security basics. By using Nmap, I was able to successfully identify open ports on my local network. The optional use of Wireshark offered a deeper technical understanding of the scanning process. The exercise highlighted the importance of actively managing network security by being aware of and securing all open ports.