Cyber Security Internship – Task 1 Report: Local Network Port Scanning

Objective

The goal of this task was to perform basic network reconnaissance by scanning my local network to identify active devices and open ports. This helps in understanding how exposed services on a network can become potential entry points for attackers.

Step-by-Step Process

1. I used Parrot OS

I used Parrot OS, which comes with Nmap pre-installed. For systems without it, Nmap can be installed using the command 'sudo apt install nmap' or by downloading it from the official Nmap website.

2. Identified Local IP and Subnet

To find my own IP address and subnet, I used the command 'ip a'. This showed that my system's IP address was 192.168.31.201 with a subnet of 192.168.31.0/24. This meant all devices in the 192.168.31.x range were part of my local network.

3. Performed a TCP SYN Scan

Using Nmap, I scanned the entire subnet using a TCP SYN scan to identify live hosts and open ports. The command I used was:

```
sudo nmap -sS 192.168.31.0/24 -oN scan-results.txt
```

This scanned 256 IP addresses and saved the results to a text file.

4. Documented Active Hosts and Open Ports

Here is a summary of the results collected from the scan:

Host Name	IP Address	Open Ports	MAC Address	Vendor
jiofiber.local.html	192.168.31.1	53, 80, 443, 7443, 8080, 8443	FC:B0:DE:23:36:D4	Unknown
Smart_Camera-1.lan	192.168.31.16	6668, 8000	28:18:FD:36:FD:C4	Aditya Infotech
Smart_Camera.lan	192.168.31.38	6668, 8000	28:18:FD:37:46:C3	Aditya Infotech
realme-11-Pro-5G.lan	192.168.31.73	None	EE:3F:56:1C:73:B2	Unknown

-	192.168.31.102	None	BA:80:C7:D9:59:92	Unknown
Tejaram.lan	192.168.31.105	All ports filtered	F0:6E:0B:DD:CB:8F	Microsoft
OPPO-A79-5G.lan	192.168.31.144	None	AE:29:3E:C0:12:F8	Unknown
V2202.lan	192.168.31.162	None	4E:71:D1:9F:E3:C2	Unknown
(This device)	192.168.31.201	53	-	-

5. Analyzed Packets Using Wireshark

I used Wireshark to capture packets during the Nmap scan. This helped visualize SYN packets being sent to different IP addresses and the responses received. The packet capture was filtered by IP to study traffic between my system and the router.

6. Researched Services on Open Ports

I looked up the common uses of each open port:
- Port 80 and 443 are standard for websites (HTTP and HTTPS)
- Port 8080 and 8443 are often used for admin panels or alternative web services
- Port 6668 is an IRC port, commonly associated with smart devices but also known for botnet traffic
- Port 53 is used for DNS and can be a target for tunneling attacks if misconfigured

7. Identified Security Risks

The scan revealed that several devices in the network had unnecessary ports open, especially smart cameras and the router. These services, if not properly secured, could expose the devices to attacks such as unauthorized access, information leakage, or exploitation via outdated firmware.

8. Saved and Organized Results

The full scan output was saved as scan-results.txt

Outcome

This task helped me understand the fundamentals of port scanning and network mapping. I learned how to detect open ports, analyze them, and assess the risk they may pose. It also taught me how to document technical findings in a structured way.

I now have a basic but practical understanding of how tools like Nmap and Wireshark can be used together for network reconnaissance and security auditing.