Task 1 -- ELEVATE LABS

Objective:

To discover open ports on devices within my local network and assess potential exposure to security risks.

Tools Used:

- Nmap (v7.95)
- (Wireshark not used in this task)

Steps I Took:

1. Installed Nmap:

I downloaded and installed the latest version of Nmap from the official site using my Kali Linux system, where it's pre-installed by default.

2. Identified My Local IP Range:

I used the command:

ip a

This showed that my local IP was within the 192.168.0.0/24 subnet, so I decided to scan that full range.

3. Performed a TCP SYN Scan:

I ran the following Nmap command to scan all devices on the network:

nmap -sS -sC -sV -oN results.txt 192.168.0.106/24

This performed a SYN scan with default scripts and version detection, and saved the output to results.txt.

4. Reviewed and Parsed the Results:

I carefully read through the scan output and noted down which IP addresses had open ports. Here's what I found:

IP Address Open Port

192.168.0.1 23, 53, 80, 1900

192.168.0.100 1234, 5900, 5985, 7070

192.168.0.106 None

5. Investigated Services on Each Port:

I noted what services Nmap detected on each open port:

- 192.168.0.1 had Telnet, DNS, HTTP (TP-LINK router config), and UPnP services.

- 192.168.0.100 was running services like Node.js Express API, VNC remote desktop, WinRM, and an AnyDesk SSL service.

6. Assessed Security Risks:

I researched and identified the following risks:

- **Port 23 (Telnet)** - High risk due to plaintext login.

- **Port 5900 (VNC)** - Vulnerable to brute-force if not encrypted.

- **Port 7070 (AnyDesk SSL)** - Could be misused for remote access.

- **UPnP (Port 1900)** - Known for exposing devices unintentionally.

7. Saved and Backed Up the Results:

I saved the scan results to results.txt …

What I Learned:

- Most of my network devices expose ports/services that could be abused if not secured.

- Tools like Nmap are powerful for network discovery and risk evaluation.

- It's crucial to audit and limit open services on internal devices.

Thank You !!! ….
-By Om Mehta