ELEVATE LABS (TASK1)

Task: Scan Your Local Network for Open Ports

Objective:

The objective of this task was to perform a network scan on my local network to identify open ports and understand potential security exposures.

Tools Used:

- Nmap (Version 7.92)
- Wireshark (Version 3.6.7) - for optional packet analysis

Methodology

1. Network Identification: Determined my local IP range using `ipconfig` (Windows) which showed my network as 192.168.1.0/24.
2. Scan Execution: Performed a TCP SYN scan using the command: `nmap -sS 192.168.1.0/24`
3. Analysis: Reviewed the scan results to identify devices and their open ports.
4. Research: Investigated services typically associated with the discovered open ports.
5. Security Assessment: Evaluated potential risks from the open ports.

Scan Results:

```
Starting Nmap 7.92 ( https://nmap.org ) at 2023-11-15 14:30 GMT

Nmap scan report for router (192.168.1.1)

Host is up (0.0020s latency).

Not shown: 995 closed ports

PORT     STATE SERVICE

53/tcp   open  domain

80/tcp   open  http
```

```
443/tcp  open  https
548/tcp  open  afp
2000/tcp open  cisco-sccp

Nmap scan report for my-pc (192.168.1.105)
Host is up (0.00050s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi

Nmap scan report for smart-tv (192.168.1.120)
Host is up (0.045s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
8008/tcp open  http
9000/tcp open  cslistener
```

Findings and Analysis

1. Router (192.168.1.1)

   - Open ports: 53 (DNS), 80 (HTTP), 443 (HTTPS), 548 (Apple Filing Protocol), 2000 (Cisco SCCP)
   - Potential risks: HTTP port open could allow unauthorized access if weak credentials exist

2. Personal Computer (192.168.1.105)

   - Open ports: 135 (MSRPC), 139/445 (NetBIOS/SMB), 5357 (WS-Discovery)
   - Critical risk: SMB ports (139/445) could be vulnerable to exploits like EternalBlue

3. Smart TV (192.168.1.120)

   - Open ports: 8008 (HTTP), 9000 (CSlistener)

   - Risk: Unauthenticated web interfaces could allow device manipulation

Security Recommendations

1. Router

   - Disable remote administration if not needed

   - Change default credentials

   - Consider closing port 548 if not using Apple services

2. Personal Computer

   - Disable SMBv1 if enabled

   - Ensure Windows Firewall is properly configured

   - Consider disabling NetBIOS if not needed

3. Smart TV

   - Update firmware to latest version

   - Disable unnecessary services in TV settings

   - Restrict access to TV's web interface if possible

Conclusion

This task provided hands-on experience with network reconnaissance using Nmap. I identified several open ports on devices in my local network and assessed their potential security implications. The exercise highlighted the importance of proper network configuration and regular security audits.