Mini Project Report - Network Port Scanning

Task 1: Scan Your Local Network for Open Ports

Objective:

To discover open ports and active devices within the local network using Nmap, and understand potential security risks based on the services running on those ports.

Tools Used:

- Nmap (Network Mapper)
- Terminal (macOS)
- Wireshark (Optional)
- ifconfig/ipconfig

Local Network Details:

- Local IP: 192.168.0.104
- Subnet: /24
- Network Range: 192.168.0.0/24

Nmap Command Used:

nmap -sT -oN scan_result.txt 192.168.0.0/24

Scan Results Summary:

1. 192.168.0.1 (Router)

- Ports: 80 (HTTP), 52869 (Unknown)
- Risk: Medium. Ensure router admin panel is secured with strong credentials.

2. 192.168.0.104 (This Mac)

- Ports: 5000 (UPnP), 7000 (AFS), 49155 (Unknown)

- Risk: Low-Medium. Verify these services are necessary and secure.

Security Recommendations:

- Secure router with a strong password and disable UPnP if unused.

- Identify and stop unnecessary services on the Mac using 'lsof -i :<port>'.

- Use the built-in macOS firewall or third-party firewall apps.

Outcome:

- Gained practical experience with Nmap.

- Understood how to scan and interpret port activity on local devices.

- Learned to assess security risks based on open ports and running services.

Prepared by: Avisikta Mandal Das