Cyber Security Internship: Task 1 Report

Scan Local Network for Open Ports

Soumen Das

November 13, 2025

1. Objective

The objective of this task is to discover open ports on devices within a local network to understand the network's exposure. This involves using network reconnaissance tools to identify active hosts and their running services.

2. Methodology

- **Intern Name:** Soumen Das
- **Tools Used:** Nmap (Network Mapper)
- **Target Network:** 192.168.1.0/24 (Simulated)
- **Command Executed:** `nmap -sS -oN scan_results.txt 192.168.1.0/24`
- **Scan Type:** TCP SYN Scan (`-sS`), also known as a "half-open" scan. This method is often preferred as it is stealthier and faster than a full TCP connect scan.

3. Simulated Scan Results

The scan identified several active hosts on the `192.168.1.0/24` network. The key findings are summarized below.

4. Security Risk Analysis

Based on the simulated results, the following potential security risks were identified:

- **192.168.1.1 (Router):**
  - **Risk:** Exposure of HTTP (unencrypted) admin panel. An attacker on the local network could intercept credentials.
  - **Recommendation:** Disable the HTTP (Port 80) interface and only use HTTPS (Port 443). Ensure a strong, non-default password is set.
- **192.168.1.50 (Linux Server):**
  - **Risk:** The SSH (Port 22) service is a common target for brute-force attacks. The MySQL database (Port 3306) being open to the network could allow attackers to attempt unauthorized access.

Table 1: Summary of Open Ports on Discovered Devices

IP Address	Open Port	Common Service	Notes / Host OS (Guess)
192.168.1.1	80/tcp	HTTP	Web Admin Interface (Router)
(Router)	443/tcp	HTTPS	Secure Web Admin (Router)
	53/tcp	DNS	Domain Name System
192.168.1.50	22/tcp	SSH	Secure Shell (Linux Server)
(Linux Server)	80/tcp	HTTP	Apache Web Server
	3306/tcp	MySQL	MySQL Database Server
192.168.1.102	135/tcp	MSRPC	Microsoft RPC
(Windows PC)	139/tcp	NetBIOS-SSN	NetBIOS Session Service
	445/tcp	Microsoft-DS	(SMB over TCP)
	3389/tcp	RDP	Remote Desktop Protocol

  - **Recommendation:** For SSH, implement key-based authentication and disable password logins. Use a firewall (like `ufw`) to restrict access to Port 3306 to only the IP addresses that absolutely need it (e.g., the web server itself).

- **192.168.1.102 (Windows PC):**
  - **Risk:** RDP (Port 3389) is a major vector for ransomware attacks (e.g., BlueKeep). If the user has a weak password, the machine is highly vulnerable. SMB (Port 445) is also a classic vulnerability point (e.g., EternalBlue).
  - **Recommendation:** If RDP is not needed, disable it. If it is, ensure Network Level Authentication (NLA) is enabled and the user has a strong password. Keep the Windows machine fully patched to mitigate SMB vulnerabilities.

5. Outcome

This task was successfully completed, demonstrating basic network reconnaissance skills. The scan results and analysis provide a clear understanding of network service exposure and the potential security risks associated with common open ports.