Cybersecurity Internship Task 1: Network Scan Analysis Report

Date: October 27, 2025
Analyst: konatham sai ram chandu
Tools Used: Nmap (Zenmap)

---

1. Objective
The goal of this task was to scan the local network (`192.168.1.0/24`) to discover active hosts, identify their open TCP ports, and analyze the services running on those ports for potential security risks.

---

2. Scan Results
The scan was performed using the command `nmap -sS -oN scan_results.txt 192.168.1.0/24`. Two active hosts were discovered.

The full raw output is available in the `scan_results.txt` file.

---

3. Host Analysis & Risk Assessment

Host 1: `192.168.1.1` (Router)
* **MAC Address:** `98:9D:B2:2E:C1:11 (Goip Global Services Pvt.)`
* **Analysis:** This host is the primary network router. It has an unusually high number of management ports open to the local network.

Port	State	Service	Risk Level	Security Analysis
21/tcp	open	`ftp`	**High**	**Unencrypted File Transfer.** FTP sends usernames and passwords in clear text. If this is for router file sharing, an attacker on the network could easily sniff the credentials.
22/tcp	open	`ssh`	**Low / Info**	**Secure Shell.** This is an encrypted command-line interface. While secure, it's an advanced feature and provides a potential login prompt for attackers to brute-force.
23/tcp	filtered	`telnet`	**Critical**	**Unencrypted Remote Login.** Telnet is an ancient, insecure protocol. The "filtered" state means a firewall is blocking it, but its presence is a major concern. It should be fully disabled.
53/tcp	open	`domain`	**Informational**	**DNS Server.** This is a normal and necessary service for a router to provide.

| **80/tcp** | open | `http` | **Medium** | **Unencrypted Web Login.** This is the router's web admin panel. Logging in via HTTP sends the admin password in clear text, allowing for easy capture. |
| **443/tcp**| open | `https` | **Informational** | **Secure Web Login.** This is the secure, encrypted admin panel. This is the **correct** port that should be used for router management. |

Host 2: `192.168.1.2` (Windows Device)
* **Analysis:** This host is a Windows machine, identifiable by the `microsoft-ds` and `msrpc` ports. The presence of `vmrdp` suggests it is running VMware virtualization software.

Port	State	Service	Risk Level	Security Analysis
135/tcp	open	`msrpc`	**Low**	Standard Windows service for remote operations.
139/tcp	open	`netbios-ssn`	**Medium**	Legacy Windows file/printer sharing service.
445/tcp	open	`microsoft-ds`	**High**	**SMB / Windows File Sharing.** This is the main port for file sharing. It is a primary target for malware (like WannaCry) to spread across a network.
2179/tcp	open	`vmrdp`	**Informational**	**VMware Remote Desktop.** This port is used by VMware for remote console access to virtual machines.

---

4. Summary & Recommendations

1. **Router (`192.168.1.1`):** This device is poorly configured and poses the largest risk.
    * **Immediate Action:** Log in to the router (using the secure `httpsIS` port 443) and **disable Telnet (port 23)** and **FTP (port 21)**.
    * **Action:** Find the setting to disable HTTP (port 80) management, forcing all admin logins over HTTPS.

2. **Windows PC (`192.168.1.2`):** This device is exposing file sharing services.
    * **Action:** If file sharing is not needed, it should be disabled in Windows settings ("Turn off file and printer sharing").
    * **Action:** If file sharing is required, ensure the device is fully patched, has strong passwords, and the Windows Defender Firewall is active.