Task 1: Simple Network Scan Report

What I Did

Nmap used, a security scanning tool, to check for "open doors" (open ports) on the devices connected to my local home network.

- **Goal:** Find which services are running and what risks they might pose.
- **Method:** I ran a fast, standard TCP SYN Scan (`-sS`) against my network range (`10.0.0.0/24` - IPs are hidden for privacy).
- **Result File:** The raw data is saved in `scan_results.txt` .

Key Findings: Open Doors

The scan found open ports on two devices: my router and one Windows computer.

Device IP (Hidden)	Open Port(s)	Service Running	What it Does
10.0.0.1	**53, 80, 443**	DNS, HTTP, HTTPS	Router's web management panel and basic network services.
10.0.0.50	**135, 139, 445**	SMB/NetBIOS	Windows File Sharing, allowing file transfer and remote communication.

Security Analysis (Why it Matters)

Having these ports open isn't bad on its own, but they are common weak spots if not secured correctly:

- **Router Ports (80/443):** These let me manage the router through a browser. The risk is that if I'm still using the **default password** or if the router's software (firmware) is **outdated**, an attacker could take over the router and control my internet access.
- **Windows File Sharing Ports (139/445 - SMB):** This is for sharing files on a Windows PC. This is a very high risk because the SMB protocol has been targeted by major malware like **WannaCry**. If the PC (`10.0.0.50`) is missing a single security update, a bad act ɔr could exploit this port to run code on the computer or access shared files.

✅ Next Steps

Based on these results, the most important action is to make sure the Windows PC (`10.0.0.50`) is completely up-to-date with all Microsoft security patches to close any known weaknesses in the File Sharing service.