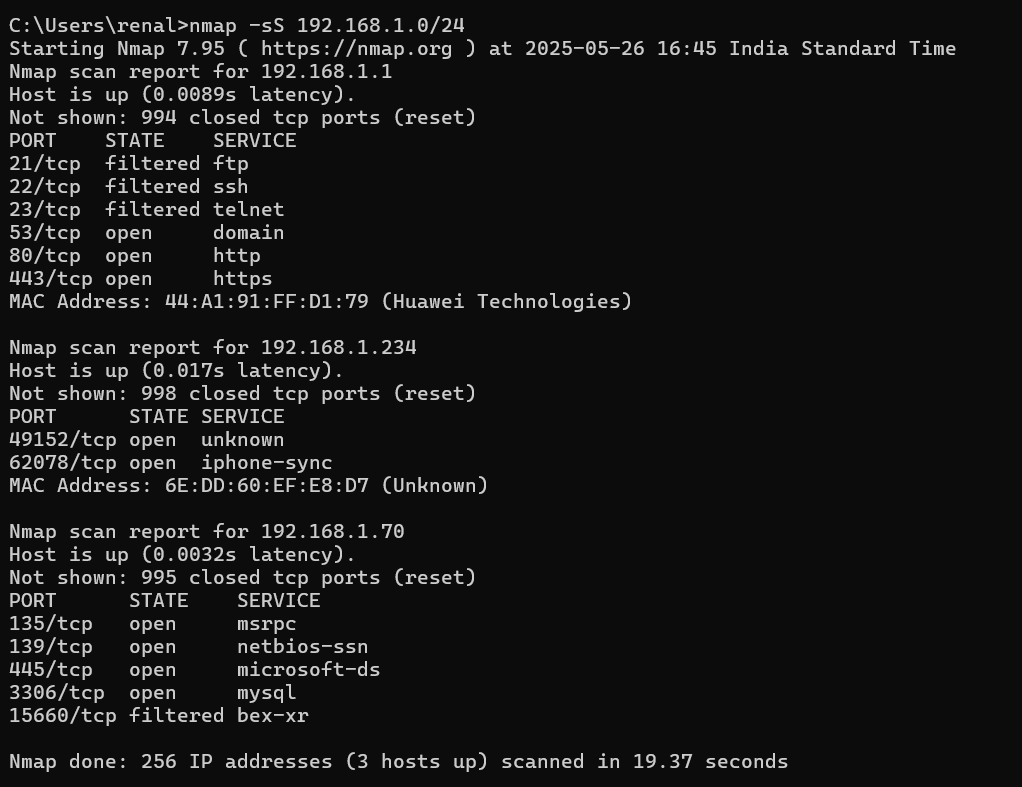
# Task 1: Scan your local network for open ports

Date: 26-05-2025

Scan Range: 192.168.1.0/24

Scan Type: TCP SYN Scan (-sS)



Analysis of the scan:

**192.168.1.1 (Router)**

Open ports: 53 (DNS), 80 (HTTP), 443(HTTPS)

Filtered: FTP, SSH, Telnet( not accessible or blocked by firewall)

Analysis:

* Common for router to have web interface(80/443)
* DNS port open- possibly for internal name resolution
* Filtering FTP/SSH/Telnet is good security hygiene

Risk: Low to moderate. If web interface is not secured with a strong password or encryption, it could be at risk

**192.168.1.88**

Open ports: 49152 (dynamic/ephermeral), 62078 (iPhone sync)

Analysis:

* 62078 is used by iTunes or Finder for syncing Apple devices
* 49152 is in the dynamic/private port range- may be temporary.

Risk: Low. These are normal for Apple devices. Ensure the device is trusted and not jailbroken.

**192.168.1.231 (Unknown)**

Open ports: None- all TCP ports are closed

Analysis:

* Could be a secured device like a printer, smart home gadget, or a firewall protected host.

Risk: None seen from this scan.

**192.168.1.70**

Open ports:

* 135(MSRPC): Windows Remote Procedure Call
* 139(NetBIOS-ssn): File sharing
* 445(Microsoft-DS): SMB file sharing
* 3306(MySQL): MySQL database

Analysis:

* These ports suggest a Windows machine with MySQL installed.
* SMB ports(139,445) are frequent targets for exploits.
* MySQL on port 3306 should not be exposed to other network devices unless required.

Risk: High if the services are not properly secured or needed. File sharing and database ports should be restricted or disabled if not in use.

Recommendations:

* Disable or restrict access to ports 139, 445, and 3306 unless explicitly needed.
* Secure router interface with strong passwords.
* Keep all devices updated and patched.
* Enable firewall to block unwanted inbound traffic.