**Network Scan Report**  
Date: August 4, 2025  
Tool Used: Nmap  
Scope: Local VM Network (192.168.1.0/24)

Prepared by:  
Mohammad Arshan Dafedar

**1. Objective**  
To discover open ports on devices in the local network and assess network exposure to common security risks.

**2. Tools & Methods**

* Nmap: Used to perform a TCP SYN scan (nmap -sS 192.168.1.0/24) across the local subnet.

**3. Scan Summary**  
A total of 64 IP addresses (192.168.1.1–192.168.1.63) in the subnet responded.  
The only open port found on all scanned devices was:

* **Port 110 (TCP) – POP3 (Post Office Protocol 3)**  
  No other open ports were detected. Ports such as 25 (SMTP) were closed, and most other ports were filtered (no response).
* \*\*Key Findings \*\*
* - 56 hosts detected alive.
* - Port `110` (POP3) open on all hosts.
* - Port `25` (SMTP) closed on all hosts.
* - Other uncommon ports closed or filtered.

**4. Detailed Findings**

| **IP Address** | **Open Port(s)** | **Service** |
| --- | --- | --- |
| 192.168.1.1 | 110 | POP3 (mail) |
| 192.168.1.2 | 110 | POP3 (mail) |
| ... | ... | ... |
| 192.168.1.63 | 110 | POP3 (mail) |

**6. Research: Common Service on Port 110 (POP3)**

* POP3 (Post Office Protocol 3) lets mail clients retrieve email from a server.
* Used by common mail software (e.g., Outlook, Thunderbird).
* By default, POP3 on port 110 is **unencrypted**; secure alternatives use port 995 (POP3S over SSL/TLS).

**7. Potential Security Risks Identified**

* **Cleartext Authentication:** Credentials and messages can be intercepted by attackers on the network.
* **Brute-Force Attacks:** The service can be targeted to guess user passwords.
* **Known Vulnerabilities:** Some POP3 software contains bugs that have been exploited in the past.
* **Unnecessary Exposure:** If POP3 is not needed, its presence increases attack surface.
* **Outdated Protocol:** Modern networks often use only secure mail protocols (IMAPS/POP3S) and disable cleartext POP3.

**8. Recommendations**

* Disable POP3 (port 110) unless strictly required.
* Use encrypted protocols (POP3S on port 995 or IMAPS on port 993) for mail retrieval if needed.
* Regularly scan the network and close unused ports/services.