1. Executive Summary

A network security assessment was conducted on the local subnet `192.168.57.0/24` to identify active hosts, open ports, and potential security risks. The assessment utilized the `nmap` tool for host discovery and port scanning. Key findings include the identification of three active hosts, with one host exposing a critical service (DNS on port 53).

---

2. Methodology

2.1 Tools Used

nmap: For host discovery and port scanning (`-sS` for TCP SYN scan).

ifconfig: To determine the local IP range.

2.2 Scope

Subnet Scanned: `192.168.57.0/24`

Scan Type: TCP SYN Scan (`-sS`)

---

3. Findings

3.1 Host Discovery

Three hosts were identified as active on the network:

IP Address	MAC Address	Manufacturer/Device	Notes

`192.168.57.22`	`08:00:27:35:62:50`	Oracle VirtualBox	Local machine (scanner source)
`192.168.57.42`	`40:1A:58:25:19:3A`	Wistron Neweb	No open ports detected
`192.168.57.61`	`E2:AE:A8:9E:D1:66`	Unknown	DNS service (port 53) open

### **3.2 Open Ports and Services**

Only one host (`192.168.57.61`) had an open port:

IP Address	Port	Service	Potential Risks
`192.168.57.61`	53	DNS -	- DNS poisoning<br>- Cache snooping

## **4. Risk Analysis**

### **4.1 DNS Service (Port 53)**

- **Vulnerabilities:**
  - Unauthenticated DNS queries could lead to cache poisoning or spoofing attacks.
  - Misconfigured DNS servers may expose internal network information.
- **Recommendations:**
  - Restrict DNS queries to trusted clients.
  - Implement DNSSEC to prevent spoofing.

4.2 Other Hosts

- **`192.168.57.42`**: No open ports detected, but further investigation is recommended to ensure no services are running on non-standard ports.

192.168.57.22: Local machine (scanner source).

5. Conclusion

The assessment revealed one critical service (DNS) exposed on the network, which poses a potential security risk. Immediate remediation steps include securing the DNS server and restricting access to trusted clients. Further scans (e.g., UDP scans, vulnerability assessments) are recommended for a comprehensive evaluation.