**Port Scan Analysis Report – Task 1**

Scanned Network Range: 192.168.84.0/24

Date: June 23, 2025

**Tools Used:**

- Nmap (TCP SYN and Service Version Detection Scan)

- Kali Linux Live Environment

**Findings:**

1. Host: **192.168.84.67**

Open Ports:

* 1. **21/tcp (FTP - Microsoft FTP Service)**
* Description: FTP allows file transfers between systems. Microsoft FTP is known for past vulnerabilities like anonymous login or weak authentication.
* Exploitation: Attackers may try anonymous login or brute-force credentials to upload malicious files.
* Mitigation: Disable FTP if not needed. Otherwise, enforce strong passwords, disable anonymous access, and use FTPS instead.
  1. **80/tcp (HTTP - Microsoft IIS 10.0)**
* Description: Web servers like IIS can host websites or APIs. Unpatched or misconfigured IIS instances may expose internal data or allow RCE.
* Exploitation: Exploits include outdated modules, default pages, or misconfigurations. Vulnerable to web attacks like XSS or LFI.
* Mitigation: Keep IIS updated, remove default/test pages, and use WAFs or URL whitelisting.
  1. **135/tcp (MSRPC)**
* Description: Microsoft Remote Procedure Call is used for DCOM and system services. It is often targeted for lateral movement.
* Exploitation: Can be abused using exploits like EternalBlue to execute commands remotely.
* Mitigation: Block this port externally via firewall. Allow only trusted internal traffic. Patch Windows regularly.
  1. **445/tcp (Microsoft-DS/SMB)**
* Description: SMB protocol is used for file sharing. SMBv1 is deprecated and dangerous.
* Exploitation: EternalBlue, WannaCry ransomware, and many others used open SMB ports.
* Mitigation: Disable SMBv1, patch OS, and restrict SMB usage to trusted hosts only.

2. Host: **192.168.84.183**

Open Port:

* 1. **53/tcp (DNS - dnsmasq 2.51)**
* Description: This is a DNS forwarding service. Version 2.51 is outdated and vulnerable to cache poisoning and DoS attacks.
* Exploitation: Can be targeted using crafted DNS queries to manipulate DNS resolution or cause crashes.
* Mitigation: Upgrade dnsmasq to a secure version. Apply rate-limiting and query filtering.

3. Host: **192.168.84.219 and 192.168.84.214**

- All 1000 TCP ports were either filtered or closed. No actionable services detected.

**General Recommendations:**

* Use firewalls to restrict port access.
* Perform regular patch management.
* Use secure alternatives (e.g., SSH instead of Telnet or FTP).
* Implement network segmentation and intrusion detection systems (IDS).
* Disable unused services.

**Conclusion:**

Multiple systems were found with exposed ports that can be exploited if unpatched or misconfigured. Immediate hardening is advised, especially for SMB and FTP services. Keeping services up to date and closing unnecessary ports is essential for reducing network attack surface.