Cyber Security Internship - Task 1 Report

1. IP Addresses and Open Ports Found

During the Nmap scan on the local network (192.168.1.0/24), the following devices and open ports were found:

- 192.168.1.1:
  - Open Ports: 21 (FTP), 53 (DNS), 80 (HTTP), 443 (HTTPS)

- 192.168.1.3:
  - All 1000 TCP ports filtered (no response)

- 192.168.1.4 (My System):
  - Open Ports: 135 (MSRPC), 139 (NetBIOS-SSN), 445 (Microsoft-DS)

2. Packet Capture Analysis with Wireshark

Wireshark was used to capture packets during the Nmap scan. A display filter 'ip.addr == 192.168.1.1' was applied.

Captured traffic revealed IGMPv3 packets from 192.168.1.1 to 224.0.0.1, which are multicast membership queries from the router. These are normal and unrelated to Nmap directly but demonstrate live traffic.

Wireshark confirmed that the router is actively communicating using multicast protocols on the network.

3. Common Services Running on Open Ports

The following services were identified from the open ports:

- Port 21 (FTP): Used for file transfers, often unencrypted.
- Port 53 (DNS): Used for domain name resolution.
- Port 80 (HTTP): Used for unencrypted web traffic.
- Port 443 (HTTPS): Used for secure web traffic.
- Port 135 (MSRPC): Used by Microsoft RPC services.
- Port 139 (NetBIOS-SSN): Used for Windows file and printer sharing.
- Port 445 (Microsoft-DS): Supports SMB protocol for file sharing in Windows environments.

4. Potential Security Risks Identified

- FTP (port 21) on the router can expose login credentials if not secured with encryption.
- HTTP (port 80) is unencrypted and vulnerable to man-in-the-middle attacks.
- DNS (port 53) can be exploited for DNS poisoning or amplification attacks.
- SMB ports (135, 139, 445) on the local system are commonly targeted by malware and should be restricted via firewall if not needed.
- HTTPS (443) is generally secure but should be checked for up-to-date TLS configurations.

Overall, the scan provides insight into visible network services and helps assess exposure risk from open ports.