# Cyber Security Internship – Task 1 Report

## Task Title:

Network Port Scanning & Analysis Using Nmap and Wireshark

## Objective:

To perform a TCP SYN scan on the local network using Nmap, identify open ports and running services, analyze network traffic with Wireshark, and assess potential security risks.

## Tools Used:

• Nmap – For port scanning  
• Wireshark – For packet capture and analysis  
• Kali Linux – Operating system  
• Mobile Hotspot – Local network environment

## Network Details:

Local IP Address: 172.20.10.9

Local IP Range Scanned: 172.20.10.0/24

Devices Detected: 3

|  |  |
| --- | --- |
| IP Address | Device Description |
| 172.20.10.1 | Mobile Hotspot (likely router) |
| 172.20.10.3 | Smart Device / IoT (Hui Zhou Gaoshengda Technology) |
| 172.20.10.5 | Kali Linux machine (scanner) |

## Nmap Scan Summary:

➤ Host 1 – 172.20.10.1

|  |  |  |
| --- | --- | --- |
| Port | Service | Description |
| 21/tcp | FTP | Insecure file transfer protocol |
| 53/tcp | DNS | Domain name resolution service |
| 49152/tcp | Unknown | Likely custom or dynamic service |
| 62078/tcp | iPhone-sync | Apple mobile device sync |

➤ Host 2 – 172.20.10.3

|  |  |  |
| --- | --- | --- |
| Port | Service | Description |
| 7100/tcp | font-service | Legacy font service (rarely used) |
| 8000/tcp | http-alt | Alternate web server port |

➤ Host 3 – 172.20.10.5  
All 1000 scanned TCP ports were closed.

## Wireshark Analysis:

Observations:

- SYN packets sent by Nmap to each device in the subnet

- SYN-ACK responses received from open ports (e.g., 21, 53, 8000)

- RST packets received from closed ports

- Packet capture confirms standard behavior of a TCP SYN scan

## Screenshots Taken:

- SYN packet filter applied in Wireshark

- SYN-ACK response packet (open port)

- RST response packet (closed port)

- Live capture during full scan

## Common Services Researched:

|  |  |  |  |
| --- | --- | --- | --- |
| Port | Service | Common Use Case | Risk Level |
| 21 | FTP | Unencrypted file transfers | High |
| 53 | DNS | Name resolution | Medium |
| 49152 | Dynamic Port | Custom service | Medium |
| 62078 | iPhone-sync | Apple sync service | Low |
| 7100 | font-service | Legacy font protocol | Medium |
| 8000 | http-alt | Alternate web server | Medium |

## Security Risk Summary:

• FTP (port 21) is outdated and unencrypted. Vulnerable to credential theft and should be replaced with SFTP.

• Port 8000 may expose a web service — secure it or restrict access via firewall.

• Port 7100 is not commonly used and should be disabled if not required.

• High-numbered ports like 49152 may allow custom applications; should be monitored.

## Files Included in GitHub Repo:

• scan\_results.txt  
• Wireshark screenshots  
• Updated\_CyberSecurity\_Task1\_Report.docx  
• README.md

## Key Takeaways:

- Learned to perform and analyze TCP SYN scans using Nmap

- Understood behavior of TCP flags in Wireshark

- Documented open ports and associated risks

- Gained hands-on exposure to identifying insecure services