README – Task 1: Local Network Port Scan

Objective

The goal of this task is to perform a SYN scan on the local network using Nmap, identify active devices, open ports, running services, and evaluate potential security risks. This document summarizes the process, findings, and recommendations.

Tools Used

- Nmap – Network scanning
- Wireshark – Packet capture (optional)
- Operating System: Windows
- Network: 192.168.31.0/24

Commands Executed

1. Basic SYN Scan:

```
nmap -sS 192.168.31.0/24 -oN scan-results.txt
```

2. Detailed Service & Version Detection:

```
nmap -sS -sV 192.168.31.0/24 -oA myscan
```

Scan Summary

A total of 5 devices were discovered on the network:

- JioFiber Router (192.168.31.1): Ports 53, 80, 443, 7443, 8080, 8443 (Medium Risk)
- OPPO K12x 5G (192.168.31.34): No open ports (Safe)
- Set-Top Box (192.168.31.156): Port 2869 (Low/Medium Risk)
- Redmi 9 Prime (192.168.31.238): No open ports (Safe)
- Laptop Vasanthreddy (192.168.31.16): Ports 135, 139, 445, 3306 (High Risk)

Key Observations

- Router exposes multiple admin ports.
- Phones are secure with no exposed ports.
- Set-top box exposes UPnP-related port.
- Laptop exposes SMB and MySQL ports which are high risk.

Potential Security Risks

- SMB Ports (135, 139, 445): Ransomware attacks, remote code execution.
- MySQL Port (3306): Database exposure risk.
- Router Ports: Admin interface exposure.

Recommended Remediations

Router:

- Disable remote access
- Change admin password
- Update firmware

Laptop:

- Disable SMB file sharing
- Block ports 135/139/445
- Disable or secure MySQL service

Set-Top Box:

- Disable UPnP if not needed