Internship Task 1 Report

Name: Hashini Miryala

Day 1 Internship Tas Scan Report

Date: 23rd June 2025
Intern Name: Hashini miryala
Internship Role: Cybersecurity Intern
Task Title: Scan Your Local Network for Open Ports

Task Objective:

Learn to discover open ports on devices in yo network exposure.

Tools Used:

- Nmap
- Zenmap (GUI for Nmap)

Nmap Command Used:

```
bash nmap -sS -Pn 192.168.80.0/24
```

Scan Summary:

192.168.80.60

- Open Port: 53/tcp
- Service: domain

192.168.80.131

- Open Ports:
    - 49152/tcp (unknown)
    - 62078/tcp (iphone-sync)

192.168.80.205

- Open Ports:
    - 2222/tcp (Ethernet/IP)
    - 3128/tcp (http-proxy)
    - 3260/tcp (filenet-tms)

    - 5060/tcp (sometimes-TCP7) ◦ 5061/tcp (sometimes-rpc9)
    - 32774/tcp (sometimes-rpc11)
- MAC Address: 6C:4A:DA:F5:30 (Samsung Electroni

192.168.80.198

- Open Ports:
    - 135/tcp (msrpc)
    - 139/tcp (netbios-ssn)
    - 445/tcp (microsoft-ds)
    - 389/tcp (ldap)
    - 3306/tcp (mysql)

Security Observations:

- Multiple hosts have open ports exposing se SMB, HTTP Proxy, etc.
- These services may have vulnerabilities if
- SSH, SMB, and databases like MySQL should monitored.

Task Status:

Completed and Verified
