# Cyber Security Internship Task 1 Report

## 🔍 Objective

Perform a local network scan using Nmap to identify live hosts, open ports, and possible security risks in a subnet.

## 🛠️ Tools Used

- Nmap  
- Kali Linux  
- (Optional) Wireshark  
- xsltproc (for HTML report)

## 🌐 Network Information

Local IP: 192.168.73.128  
Subnet Scanned: 192.168.73.0/24  
Total Hosts Up: 4

## 🧪 Commands Used

sudo nmap -sS 192.168.73.0/24 -oN scan\_results.txt  
sudo nmap -sS 192.168.73.0/24 -oX scan.xml  
xsltproc scan.xml -o scan\_report.html

## 📄 Scan Results Summary

### 🟢 Host: 192.168.73.1

Open Ports: 135 (MSRPC), 139 (NetBIOS-SSN), 445 (Microsoft-DS), 903 (VMware ISS), 3000 (PPP), 3001 (Nessus)

Risks:

- 139 & 445: SMB vulnerabilities (e.g., EternalBlue, WannaCry)  
- 3001: Nessus scanner interface may expose sensitive data

### 🟢 Host: 192.168.73.2

Open Port: 53 (DNS)

Risk: DNS amplification or spoofing if not secured

### 🔵 Host: 192.168.73.254

All 1000 ports filtered — likely a firewall or gateway

### 🔵 Host: 192.168.73.128

All ports closed — your Kali machine is secure

## 📁 Files Included

- scan\_results.txt — Raw scan output  
- scan\_report.html — (Optional) HTML report  
- Cybersecurity\_Task1\_Report.docx — This document  
- README.md — Summary and command log

## ✅ Conclusion

Nmap scanning successfully revealed multiple active hosts and open ports in the local network.  
Ports like 445 (SMB) and 3001 (Nessus) may pose security risks. Recommended to close unnecessary ports, update systems, and restrict access to internal services.