Task -1

Scan Your Local Network for Open Ports

Objective: Learn to discover open ports on devices in your local network to understand network exposure.

Network Security Scan Report

Target IP: 192.168.1.2

Scan Date: September 22, 2025

Scanner: Nmap 7.94

Report Type: TCP SYN Scan Analysis

Executive Summary

This report presents the findings of a network reconnaissance scan performed on IP address 192.168.x.x within the local network range 192.168.x.x/24. The scan was conducted to identify open ports, running services, and potential security vulnerabilities as part of a cybersecurity learning exercise.

Methodology

Scanning Approach

- **Primary Scan:** TCP SYN Scan (nmap -sS)
- **Network Range:** 192.168.x.x/24
- **Target Focus:** 192.168.x.x
- **Additional Analysis:** Service detection and version enumeration

Commands Used

- Basic TCP SYN scan
  nmap -sS 192.168.x.x
- Comprehensive scan with service detection
  nmap -sS -sV -O 192.168.x.x
- Full port range scan
  nmap -sS -p- 192.168.x.x

Scan Results

Open Ports Discovered

Port	Protocol	State	Service	Version
22/tcp	TCP	Open	SSH	OpenSSH 8.2p1
80/tcp	TCP	Open	HTTP	Apache 2.4.41
443/tcp	TCP	Open	HTTPS	Apache 2.4.41
3306/tcp	TCP	Open	MySQL	MySQL 8.0.25
8080/tcp	TCP	Open	HTTP-Alt	Jetty 9.4.x

Filtered/Closed Ports

- Ports 21, 23, 25, 53, 110, 143, 993, 995: Closed
- No filtered ports detected