# 🛡️ Local Network Vulnerability Assessment Report

Target IP: 192.168.1.X (Masked IP)

Scan Performed: June 23, 2025

Tool Used: Nmap 7.94SVN

Scan Command: nmap -A 192.168.1.X -oN scan\_results.txt

## 📌 Objective

- Identify exposed services and ports  
- Determine the OS and device type  
- Assess potential vulnerabilities or misconfigurations  
- Build documentation and practice structured security reporting

## 📋 Summary of Findings

|  |  |
| --- | --- |
| Attribute | Value |
| Host Status | Up (0.00052s latency) |
| Open Ports | 6 |
| OS Detection | Oracle VirtualBox (98%) |
| Distance | 1 hop |

## 🚪 Open Ports & Services

|  |  |  |  |
| --- | --- | --- | --- |
| Port | State | Service | Details |
| 135 | Open | msrpc | Microsoft Windows RPC |
| 139 | Open | netbios-ssn | NetBIOS Session Service |
| 445 | Open | microsoft-ds? | Likely SMB (Windows file sharing) |
| 2869 | Open | http | Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP) |
| 3306 | Open | tcpwrapped | Likely MySQL database (wrapped) |
| 6646 | Open | unknown | Unknown service, requires investigation |