# Network Scanning and Mapping Lab Report

By: Shomoi Francis

---

## Network Scanning and Mapping Lab Report

By: Shomoi Francis

Date: 2025-11-07 04:50 UTC

## Overview

I ran an Nmap scan to identify open ports, running services, and potential vulnerabilities on my test network. The goal was to learn what services were exposed and how they could be exploited if not properly secured.

## Scan Details

Command used: nmap -T4 -A -v 192.168.56.1

The scan found several open ports including 135, 139, 445, 2869, 5357, 3389, and 8090. These ports are typically tied to Windows services such as RDP, SMB, and UPnP.

## Findings

RDP (3389) – Remote Desktop was open with a self-signed certificate. This can be used for brute-force or MITM attacks.

SMB/NetBIOS (135, 139, 445) – File sharing ports were open and SMB signing wasn't required.

UPnP/HTTPAPI (2869, 5357) – These services are rarely needed and can increase attack surface.

Port 8090 – Unknown service responding; requires further investigation.

Information Leakage – Host and domain details were visible in NTLM responses.

## Why It Matters

Leaving RDP, SMB, or UPnP ports open can make a system easy to exploit. Attackers can use these services for unauthorized access, lateral movement, or ransomware deployment.

## Fix Plan

Blocked RDP (3389) and SMB (135, 139, 445) ports using Windows Defender Firewall.

Enabled Network Level Authentication (NLA) for RDP connections.

Disabled SMBv1 and enforced SMB signing on the system.

Turned off UPnP and SSDP services through Windows Services Manager.

Checked port 8090 to identify which program was using it and secured or disabled it.

Replaced self-signed certificates with valid trusted ones.

Make sure the system stays up-to-date with patches and monitoring enabled.

## Firewall Actions

Instead of using command-line tools, I used the Windows Defender Firewall interface to create new inbound rules that block risky ports. I went to Windows Defender Firewall > Advanced Settings > Inbound Rules > New Rule, chose 'Port', selected 'TCP', and added the ports 135, 139, 445, 2869, 5357, 3389, and 8090. Then I selected 'Block the connection' and applied it to all profiles (Domain, Private, Public).

## Summary

This lab helped me understand how attackers scan networks and how to respond by identifying, analyzing, and closing exposed services. Using Windows Firewall made it easier to visually confirm which ports were blocked and ensure the system was secure.