Network Port Security Assessment Report

Prepared by: Krishnapriya Pradeep
Date: May 26, 2025

---

1. Introduction

This report presents the findings from a network port scan performed on the subnet 192.168.0.0/24, focusing on open ports, their associated services, and potential security risks. The analysis leverages Nmap's service/version detection to identify exposed services and assess the vulnerabilities related to these open ports.

---

2. What is an Open Port?

An **open port** is a network communication endpoint on a device that is actively accepting connections or data requests. Ports are logical channels identified by numbers (0-65535) through which applications communicate over the network. An open port indicates that a service is listening for incoming connections on that port, making it a potential gateway for communication—and consequently, an attack vector if improperly secured.

---

3. How Does Nmap Perform a TCP SYN Scan?

Nmap's TCP SYN scan (also known as "half-open" scanning) operates by sending a TCP SYN (synchronize) packet to a target port and analyzing the response:

SYN-ACK: If received, the port is open, indicating a service is listening.

RST (reset): If received, the port is closed.

No response or ICMP unreachable: The port is filtered or blocked by a firewall.

This method is efficient and stealthy, as it does not complete the full TCP handshake, reducing the chance of detection by target systems.

---

4. Risks Associated with Open Ports

Open ports expose services that can be exploited by attackers to gain unauthorized access, execute remote commands, intercept data, or disrupt services. Risks include:

Exploitation of unpatched vulnerabilities in services

Brute force attacks on authentication mechanisms

Man-in-the-middle attacks on unencrypted communications

Unauthorized data access or network pivoting via exposed services

5. Difference Between TCP and UDP Scanning

TCP Scanning: Probes ports by establishing or attempting TCP connections (usually via SYN packets). It is reliable because TCP has connection states, enabling clear responses indicating open, closed, or filtered ports.

UDP Scanning: Sends UDP packets to target ports. Since UDP is connectionless and many devices do not respond to closed UDP ports, determining open or closed status is less reliable and slower, often requiring multiple retries and analysis of ICMP “port unreachable” messages.

---

6. How Can Open Ports Be Secured?

Disable unnecessary services: Shut down services and close ports that are not required.

Patch and update: Keep software and firmware current to mitigate known vulnerabilities.

Strong authentication: Use complex passwords, multi-factor authentication where possible.

Encrypt communication: Replace plain-text protocols (e.g., Telnet) with secure alternatives (e.g., SSH, HTTPS).

Network segmentation: Restrict access to critical services through VLANs or subnet segmentation.

Firewall configuration: Limit port accessibility to trusted IPs and networks only.

---

7. Firewall’s Role Regarding Ports

A firewall controls inbound and outbound network traffic based on predefined security rules. It monitors and filters traffic by:

Blocking or allowing traffic on specific ports.

Preventing unauthorized access to services.

Protecting the network by hiding internal ports from external scans.

Logging suspicious activity related to port access.

---

8. What is a Port Scan and Why Do Attackers Perform It?

A **port scan** is a technique used to identify open ports and services on a target system. Attackers perform port scans to:

Discover potential entry points into a system.

Identify vulnerable or misconfigured services.

Map the network architecture to plan targeted attacks.

Test the effectiveness of defenses or reconnaissance prior to exploitation.

---

9. How Does Wireshark Complement Port Scanning?

Wireshark is a network protocol analyzer that captures and inspects live traffic at a granular level. It complements port scanning by:

Analyzing traffic on open ports to identify protocol anomalies or suspicious payloads.

Detecting unauthorized connection attempts or suspicious network behavior.

Verifying the legitimacy of responses obtained from port scans.

Providing detailed packet-level insight useful for troubleshooting and forensic analysis.

---

10. General Findings from the Network Scan

Step-by-Step Methodology

Environment Setup

Launched a target Ubuntu-based virtual machine on a secure, isolated lab network.

Ensured that no public IP or production system was involved.

Tool Used: Nmap

Installed and ran **Nmap**, a network scanning utility, from the attacker machine (Kali Linux VM).

Scan Performed:

TCP SYN Scan (Half-open scan) using the command:

sudo nmap -sS <target-ip>

Logged results showing open, filtered, and closed ports.

Service Identification:

Cross-referenced open ports with known services using:

nmap -sV <target-ip>

Determined the likely services running and their potential risks.

Risk Evaluation:

Researched vulnerabilities and attack vectors associated with each service.

Categorized them based on severity and likelihood of exploitation.

Service Type/Port Range	Common Use Case	Typical Security Risks	Best Practice Recommendations
Telnet (Port 23)	Legacy remote access protocol	Plaintext credentials, easy interception	Disable entirely; replace with SSH
HTTP (Port 80)	Web interfaces, device admin	Unencrypted data, credential leakage	Enforce HTTPS with valid certificates
UPnP Services (Various ports)	Network device discovery	External exposure, unauthorized device control	Disable if unused; restrict to trusted devices
RTSP (Port 554)	Streaming cameras and media	Unauthorized video access	Secure with strong authentication; patch firmware
Microsoft RPC and SMB (Ports 135, 139, 445, 49152-49157)	Windows file and service sharing	Remote code execution, worm propagation	Patch regularly, restrict access, disable SMBv1
Unknown or Proprietary Ports	Custom or vendor-specific services	Potential hidden vulnerabilities	Identify and audit services; close unnecessary ports
Filtered Ports	Services behind firewalls	Reduced exposure	Maintain strict firewall rules
Closed Ports	No services running	Minimal risk	Monitor regularly for unexpected changes

---

Key Takeaways:

Avoid publicly sharing exact IPs or hostnames tied to open ports.

Discuss risks and mitigation strategies at a service or protocol level.

Encourage strict access controls, regular patching, and encryption.

Firewalls should limit port accessibility to known, trusted sources.

---

11. Conclusion

The scan identified multiple open ports running legacy or vulnerable services, presenting clear security risks. Immediate remediation actions such as disabling unused services, patching devices, enforcing strong authentication, and securing network boundaries via firewalls are essential to protect the network infrastructure from potential exploitation.