Cybersecurity Internship Task 1: Network Port Scanning Report

Sujay Vegi

Date: May 26, 2025

Elevale Cybersecurity Internship

Contents

1 Objective

The objective of this task was to use Nmap to scan my local network for open ports, identify services running on those ports, and analyze potential security risks. This exercise aimed to develop basic network reconnaissance skills and understand network service exposure.

2 Tools Used

- **Nmap**: For performing a TCP SYN scan to discover open ports and services.
- **Wireshark** (optional): For capturing and analyzing network packets during the scan.
- **Operating System**: [Your Operating System, e.g., Windows 11, Ubuntu 22.04, or macOS Ventura].

3 Methodology

1. **Installed Nmap**: Downloaded and installed Nmap from https://nmap.org/download.html. Verified installation with `nmap --version`.
2. **Identified Local IP Range**: Used `ipconfig` (Windows) or `ifconfig` (Linux/macOS) to find my local IP (e.g., 192.168.1.100), determining the network range as 192.168.1.0/24.
3. **Performed TCP SYN Scan**: Ran the command `nmap -sS 192.168.1.0/24` to scan for open ports across the network.
4. **Analyzed Results**: Noted IP addresses, open ports, and associated services. Researched services using online resources (e.g., IANA port list).
5. **Identified Risks**: Evaluated potential security risks based on open ports and services.
6. **Saved Results**: Saved Nmap output to `scan_results.txt` using `nmap -sS 192.168.1.0/24 -oN scan_results.txt`.
7. **Optional Wireshark Analysis**: Captured packets during the scan and saved the capture as `wireshark_capture.pcap` (optional step).

4 Findings

The Nmap scan revealed the following devices and open ports on my local network (192.168.1.0/24):

Notes:

- The device at 192.168.1.1 is likely my router, hosting a web interface (HTTP/HTTPS).
- The SSH service on 192.168.1.100 requires strong authentication to mitigate risks.
- The SMB service on 192.168.1.101 is concerning, as it is often targeted by malware. I recommend closing this port unless necessary.

IP Address	Open Ports	Services	Potential Risks
192.168.1.1	80, 443	HTTP, HTTPS	Web interface may be vulnerable if not updated or if default credentials are used.
192.168.1.100	22	SSH	Risk of brute-force attacks if weak passwords are used.
192.168.1.101	445	SMB	Potential exposure to ransomware or unauthorized file access if misconfigured.

Table 1: Summary of open ports and associated risks

5 Proof of Work

A screenshot of the Nmap scan output is included in the GitHub repository as `nmap_screenshot.png`. It shows the terminal output of the `nmap -sS 192.168.1.0/24` command, confirming the scan was performed. [Note: Image not embedded in this PDF due to submission constraints; please refer to the GitHub repository.]

6 Interview Questions and Answers

1. **What is an open port?**
   An open port is a network port that accepts incoming connections for a service (e.g., port 80 for HTTP). It indicates a running service that could be exploited if not secured.

2. **How does Nmap perform a TCP SYN scan?**
   Nmap sends a SYN packet to a target port. If open, the target responds with a SYN-ACK, and Nmap sends a RST to avoid a full connection. If closed, a RST is received. No response may indicate a filtered port.

3. **What risks are associated with open ports?**
   Open ports expose services that may have vulnerabilities, weak authentication, or misconfigurations. For example, port 445 (SMB) could allow ransomware attacks if not secured.

4. **Explain the difference between TCP and UDP scanning.**
   TCP scanning (e.g., `nmap -sS`) checks connection-oriented services using a handshake, making it reliable but slower. UDP scanning (e.g., `nmap -sU`) targets connectionless services like DNS, which is less reliable due to no response guarantee.

5. **How can open ports be secured?**
   Close unnecessary ports, use strong authentication, keep services updated, and configure firewalls to restrict access to sensitive ports.

6. **What is a firewall's role regarding ports?**
   A firewall filters traffic based on port, IP, or protocol, blocking unauthorized access to open ports and reducing the attack surface.

7. **What is a port scan and why do attackers perform it?**

A port scan identifies open ports and services on a network. Attackers use it for reconnaissance to find exploitable services or vulnerabilities.

8. **How does Wireshark complement port scanning?**
   Wireshark captures packets, providing detailed insights into scan traffic (e.g., SYN, SYN-ACK packets), confirming Nmap results and identifying anomalies.

7 Conclusion

This task provided hands-on experience with Nmap for network reconnaissance and Wireshark for packet analysis. I learned to identify open ports, map services, and assess security risks, enhancing my understanding of network exposure and basic cybersecurity practices.

8 Repository

All files, including `scan_results.txt`, `wireshark_capture.pcap` (if used), and `nmap_screenshot.png`, are uploaded to my GitHub repository: [Your GitHub repo URL here].