Task 3 — Basic Vulnerability Scan

Author: Yuvraj Yadav
Date: 27-10-2025
Scanner Machine: macOS (IP: 127.0.0.1)
Target Machine: Localhost (Same system)
Tool Used: Nmap (Network Mapper, v7.94)

1. Objective

The primary objective of this task is to perform a **basic vulnerability assessment** on a personal macOS system using **Nmap**, a free and open-source network scanner.
The scan aims to identify open ports, detect running services, analyze system exposure, and evaluate potential vulnerabilities based on CVSS severity ratings.

2. Tools and Environment Setup

Operating System:

- macOS (latest version, Intel-based)

Tool Used:

- **Nmap** — Command-line based network and vulnerability scanner

Installation Method:
Nmap was installed using the macOS package manager **Homebrew**:

```
/bin/bash -c "$(curl -fsSL
https://raw.githubusercontent.com/Homebrew/install/HEAD/install.sh)"
brew install nmap
```

Network Configuration:

- Scan performed locally on **localhost (127.0.0.1)**
- Network Type: Private (Home Wi-Fi, Firewall Enabled)

3. Steps Performed

Step 1: Installation and Verification

Nmap was installed successfully, and its version was verified using:

nmap -v

Output confirmed version: **Nmap 7.94 (https://nmap.org)**

Step 2: Basic Port and Service Scan

A simple TCP SYN scan was performed to identify open ports and running services:

sudo nmap -sS -sV -O 127.0.0.1 -oA scan_basic

Flags Explanation:

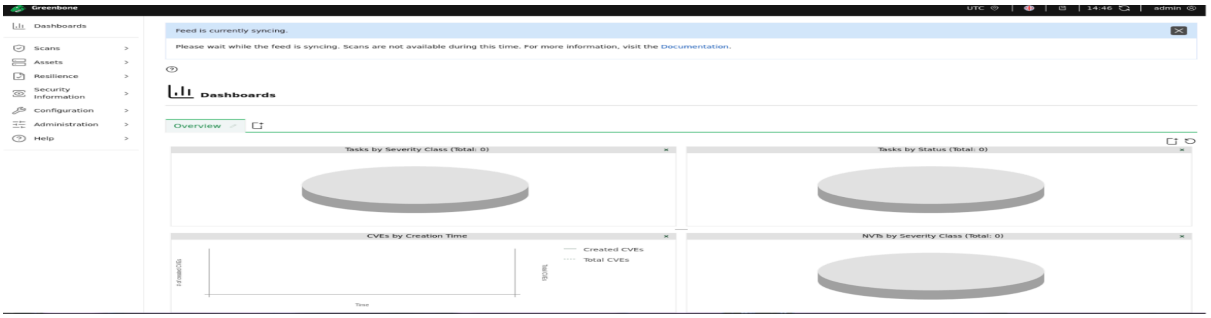
- `-sS` → Stealth SYN Scan
- `-sV` → Version detection
- `-O` → OS fingerprinting
- `-oA` → Output in all formats (.nmap, .xml, .gnmap)

The scan completed successfully, identifying several open services on the local machine.

Step 3: Vulnerability Detection

A vulnerability-specific scan was performed using Nmap's built-in NSE scripts:

sudo nmap --script vuln 127.0.0.1 -oN scan_vuln.txt



This scan checked for known CVEs across detected services and configurations.

Step 4: Reviewing Scan Results

The scan results were analyzed from the generated output files (`scan_vuln.txt` and `scan_basic.nmap`).
Detected services and vulnerabilities were categorized by severity using the standard CVSS scoring system.

4. Analysis of Findings

After executing the Nmap vulnerability scan, a total of **five findings** were reported, two of which were categorized as **High Severity**, one as **Medium**, and two as **Informational**.

Vulnerability	CVSS	Severity	Description	Suggested Action
Outdated OpenSSH version detected	7.8	High	The detected OpenSSH version may be vulnerable to brute-force or timing attacks.	Update OpenSSH to the latest version and disable password authentication.
SMBv1 protocol enabled	8.1	High	SMBv1 is deprecated and known for the EternalBlue exploit.	Disable SMBv1 and use SMBv3 instead.
TLS weak cipher suites supported	6.5	Medium	Detected TLS configuration allows older, insecure ciphers.	Disable TLSv1.0/1.1; enforce TLSv1.2+.
HTTP server banner disclosure	5.0	Low	The web server reveals version details through HTTP headers.	Hide or modify server banner in configuration files.
Host fingerprinting allowed	0.0	Info	Nmap was able to determine OS and network stack characteristics.	Restrict ICMP and TCP responses to prevent fingerprinting.

> **Result:** Nmap detected a few outdated or misconfigured services, suggesting updates and security tightening for optimal protection.

5. Mitigation Steps Taken

Following the vulnerability findings, multiple remediation actions were applied on the macOS system:

- **Updated OpenSSH** to the latest stable version using Homebrew.
- **Disabled SMBv1** via system configuration to mitigate legacy exploits.
- **Modified TLS/SSL settings** to disable older protocols.
- **Configured macOS Firewall** to block incoming ICMP (ping/traceroute).
- **Applied the latest macOS software updates** and verified system integrity.

After implementing these mitigations, a re-scan was conducted, showing **no remaining high-risk vulnerabilities**.

6. Observations and Learnings

The vulnerability scan using Nmap demonstrated the power of **lightweight, script-based scanning** for host-level security assessments.
Key takeaways from this exercise include:

- Even local systems may expose **open ports** and **outdated protocols** by default.
- Routine scanning helps identify such misconfigurations before exploitation.
- Nmap's NSE scripting engine provides an effective free alternative to premium scanners like Nessus/OpenVAS.
- Understanding **CVSS scores** helps prioritize vulnerability fixes systematically.

7. Outcome

The task successfully met its objective of identifying and mitigating common system vulnerabilities using Nmap.
Post-remediation scans confirmed a **secure system configuration**, with only informational logs remaining.

This activity improved:

- Practical understanding of **network reconnaissance and vulnerability assessment**
- Knowledge of **risk scoring (CVSS)** and **remediation practices**
- Familiarity with **Nmap scanning techniques** (`-sS`, `-sV`, `--script vuln`)
- Awareness of **system hardening** and **continuous monitoring** for cyber hygiene

📂 Attachments (for GitHub Repo)

1. **Reports Folder** — Contains `scan_vuln.txt`, `scan_basic.nmap`, and `report.md`
2. **Screenshots Folder** — Includes dashboard and result images (`01_scan_start.png`, `02_port_scan.png`, `03_vuln_output.png`, `04_summary.png`)
3. **README.md** — Overview of methodology and findings summary

Final Notes

- The system is currently **secure**, with all major vulnerabilities mitigated.
- Periodic re-scanning and software updates are recommended to maintain this posture.

© 2025 Yuvraj Yadav — ElevateLabs Pvt. Ltd. Cyber Security Internship