Basic Vulnerability Scan Report

Target System: Localhost (192.168.1.12)
Scanner Used: Nessus Essentials (simulated run)
Date of Scan: 25 Sept 2025
Scan Type: Full System Vulnerability Scan

Summary of Findings

- Total Vulnerabilities Found: 7
- Critical: 1
- High: 2
- Medium: 3
- Low: 1

Detailed Findings

1. Critical Vulnerability

Title: SMBv1 Protocol Enabled

- Description: The system still has SMBv1 enabled, which is outdated and vulnerable to multiple exploits (e.g., WannaCry ransomware).
- Risk: Remote attackers could exploit SMBv1 to execute code and spread malware.
- Recommendation: Disable SMBv1 via Windows Features or registry settings. Use SMBv2/SMBv3 instead.
- CVSS Score: 9.3 (Critical)

2. High Vulnerabilities

A. Outdated Web Browser (Google Chrome v115)

- Description: Installed version is missing recent security patches. Known vulnerabilities include sandbox bypasses.
- Recommendation: Update to the latest version immediately.
- CVSS Score: 8.1

B. OpenSSH Service Weak Cipher Suites

- Description: SSH server allows deprecated ciphers (e.g., 3DES, RC4).

- Recommendation: Restrict to modern ciphers (AES256-GCM, ChaCha20-Poly1305). Update SSH configuration.
- CVSS Score: 7.8

3. Medium Vulnerabilities

A. Missing Windows Update (September 2025 Patch Tuesday)

- Description: Security patches not applied; system exposed to privilege escalation flaws.
- Recommendation: Run Windows Update and ensure auto-updates are enabled.
- CVSS Score: 6.5

B. Weak Local Administrator Password Policy

- Description: Password complexity requirements are not enforced (simple passwords allowed).
- Recommendation: Enable strong password policy (12+ chars, complexity, expiration).
- CVSS Score: 6.0

C. Outdated Adobe Acrobat Reader

- Description: Vulnerable to PDF-based code execution exploits.
- Recommendation: Update to the latest version or uninstall if unused.
- CVSS Score: 5.9

4. Low Vulnerability

Title: ICMP Timestamp Response Enabled

- Description: The host responds to ICMP timestamp requests, which can aid reconnaissance.
- Recommendation: Disable ICMP timestamp responses in firewall settings.
- CVSS Score: 3.1

Overall Risk Assessment

The system has 1 critical and 2 high-risk vulnerabilities that should be addressed immediately (SMBv1, outdated Chrome, weak SSH configuration). Medium and low issues should also be remediated to improve overall security hygiene.

Recommended Next Steps

1. Immediately disable SMBv1 to prevent ransomware-style attacks.
2. Update Chrome, Adobe Acrobat, and Windows patches.
3. Harden SSH config by removing weak ciphers.
4. Enforce strong password policies.
5. Re-run vulnerability scan after fixes.

Interview Questions

1. What is vulnerability scanning?
It's an automated process of identifying known security weaknesses in a system, such as outdated software, misconfigurations, or missing patches.

2. Difference between vulnerability scanning and penetration testing?

- Vulnerability scanning to Automated, broad, identifies known issues.
- Penetration testing to Manual + automated, attempts real-world exploitation to assess impact.

3. Common vulnerabilities in personal computers?

- Outdated operating system/software
- Weak passwords
- Misconfigured firewalls
- Unpatched services like SMBv1
- Outdated browsers or PDF readers

4. How do scanners detect vulnerabilities?
By comparing system details (software versions, configs, open ports) against a database of known vulnerabilities (CVE database).

5. What is CVSS?
Common Vulnerability Scoring System, a standardized way to rate the severity of vulnerabilities (0–10 scale).

6. How often should vulnerability scans be performed?
For personal PCs: monthly or after major updates. For enterprises: weekly or continuous monitoring.

7. What is a false positive in vulnerability scanning?
When a scanner reports a vulnerability that doesn't actually exist on the system.

8. How do you prioritize vulnerabilities?

- Start with Critical (highest CVSS scores, remote exploits).
- Then High (active exploits in the wild).
- Finally medium/low, based on business impact and exposure.