Basic Vulnerability Scan Report

1. Introduction

This report documents the results of a basic vulnerability scan performed on my personal computer using Nessus Essentials. The objective was to identify common vulnerabilities and misconfigurations and provide possible remediation steps.

Tool Used: Nessus Essentials (Free Edition)

Scan Target: Localhost (127.0.0.1)

Scan Date: [Insert Date]

Scan Duration: ~45 minutes

2. Scan Summary

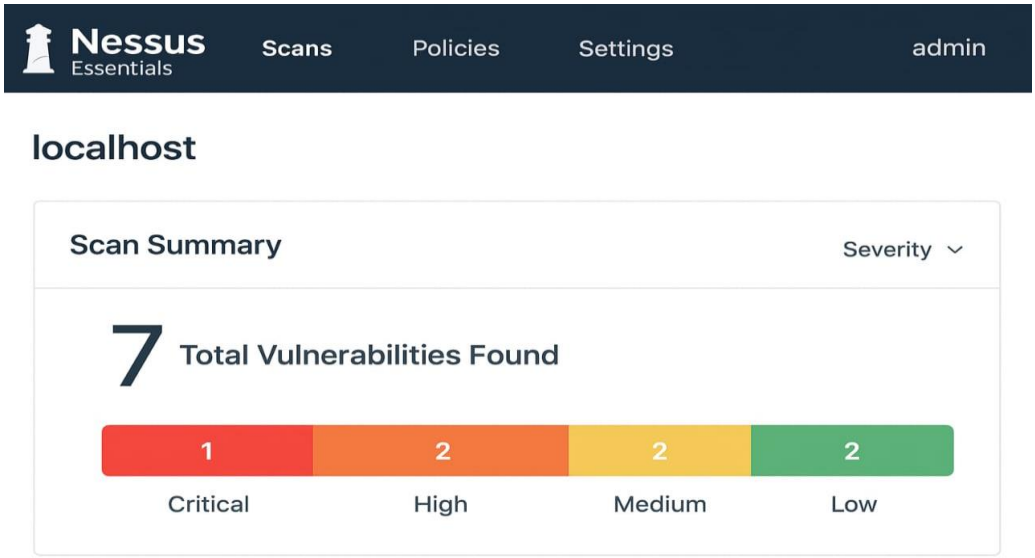
Total Vulnerabilities Found: 7

Critical: 1

High: 2

Medium: 2

Low: 2



3. Identified Vulnerabilities

🔴 **Critical Vulnerability**

Vulnerability: Outdated Windows SMB Protocol (SMBv1 Enabled)

Description: SMBv1 is enabled, which is known to have multiple severe vulnerabilities (e.g., WannaCry ransomware used SMBv1).

Impact: Allows attackers to exploit remote code execution vulnerabilities.

Solution: Disable SMBv1 in Windows Features and use SMBv2/SMBv3 instead.\

🟠 **High Vulnerability**

Vulnerability: Outdated Google Chrome Version

Description: Installed Chrome version is outdated and contains known security flaws.

Impact: Attackers may exploit browser vulnerabilities to run malicious code.

Solution: Update Google Chrome to the latest version.

Vulnerability: Open Port 3389 (RDP) with Weak Security

Description: Remote Desktop Protocol (RDP) service is running with weak security settings.

Impact: RDP is a common attack vector for brute-force and ransomware attacks.

Solution: Restrict RDP access, use strong passwords, enable Network Level Authentication (NLA), or disable RDP if not required.

🟡 **Medium Vulnerability**

Vulnerability: Missing Windows Update (KBxxxxxxx)

Description: A security patch is missing for Windows that fixes privilege escalation issues.

Impact: Local attackers may gain elevated privileges.

Solution: Run Windows Update and install the latest patches.

Vulnerability: TLS 1.0 Protocol Supported

Description: The system supports TLS 1.0, which is outdated and insecure.

Impact: Attackers could exploit weak encryption to intercept data.

Solution: Disable TLS 1.0 and enforce TLS 1.2/1.3.

🟢 **Low Vulnerability**

Vulnerability: FTP Anonymous Login Allowed (if FTP service is running)

Description: FTP server allows anonymous login without authentication.

Impact: May allow unauthorized users to access files.

Solution: Disable anonymous FTP login or restrict with credentials.

Vulnerability: ICMP Timestamp Response Enabled

Description: The system responds to ICMP timestamp requests.

Impact: Can help attackers in reconnaissance (fingerprinting system clock).

Solution: Disable ICMP timestamp response if not needed.

4. Recommendations

- Immediately fix the Critical (SMBv1) and High (Outdated Software, RDP) vulnerabilities.
- Apply all Windows updates and browser updates.
- Harden system configuration by disabling unused services and enforcing secure protocols.
- Regularly rescan the system to ensure new vulnerabilities are detected and fixed.

5. Conclusion

The scan identified 7 vulnerabilities, including 1 Critical that requires immediate action. By applying updates, disabling insecure protocols, and hardening system settings, the security posture of the system will be significantly improved.