Sample Vulnerability Scan Report

Scan Summary

Scan Target: 127.0.0.1 (Localhost)

Tool: Nessus Essentials

Scan Type: Basic Network Scan

Total Vulnerabilities: 12

- Critical: 2

- High: 4

- Medium: 3

- Low: 3

Top Critical Vulnerabilities

1. OpenSSL Remote Code Execution (CVE-2022-1234)

   - Severity: Critical (CVSS: 9.8)

   - Description: A vulnerability in OpenSSL allows remote attackers to execute arbitrary code.

   - Remediation: Update OpenSSL to the latest version.

2. SMBv1 Enabled (CVE-2017-0143)

   - Severity: Critical (CVSS: 9.3)

   - Description: SMBv1 is outdated and has known vulnerabilities.

   - Remediation: Disable SMBv1 in Windows Features.

Medium & Low Vulnerabilities

3. Outdated Apache Server Version

   - Severity: Medium (CVSS: 6.5)

   - Remediation: Update Apache server.

4. Weak SSH Encryption Algorithms Enabled

   - Severity: Low (CVSS: 3.7)

   - Remediation: Disable weak SSH ciphers in the configuration.