# Vulnerability Scan Report (Mock)

This is a simulated vulnerability scan report generated for learning and documentation purposes. The scan was performed on a local machine using Nessus Essentials. Below is a summary of identified vulnerabilities:

**Vulnerability: Outdated Apache HTTP Server**

Severity: High | CVSS Score: 8.5

Suggested Fix: Update to the latest stable version of Apache HTTP Server.

**Vulnerability: SMBv1 Protocol Enabled**

Severity: Medium | CVSS Score: 6.3

Suggested Fix: Disable SMBv1 via group policy or system features.

**Vulnerability: TLS 1.0 and 1.1 Supported**

Severity: Medium | CVSS Score: 6.1

Suggested Fix: Disable outdated TLS protocols in server settings.

**Vulnerability: Weak SSH Cipher Suites Enabled**

Severity: High | CVSS Score: 7.9

Suggested Fix: Restrict SSH to strong, secure cipher suites only.

**Vulnerability: Missing Critical Windows Security Patches**

Severity: Critical | CVSS Score: 9.3

Suggested Fix: Run Windows Update and apply all pending security patches.

**Conclusion**

The scan revealed several critical and high-severity vulnerabilities. These should be addressed immediately to reduce potential attack surfaces and improve system security. Regular scans and updates are recommended.