Vulnerability Assessment Report

Scanner: Nessus Essentials
System Scanned: Local PC
Scan Type: Basic Vulnerability Scan
Overall Severity: Medium

1. Summary

I ran a basic vulnerability scan on my computer to learn how security tools check for risks.
The scan found several medium-level issues, mostly related to SSL certificates and SMB signing.
These problems do not mean the computer is unsafe, but fixing them will make it more secure.

The issues are common and easy to fix. They helped me understand how certificates work, why hostname mismatches matter, and why SMB traffic needs protection.

---

2. Vulnerability Table

ID	Vulnerability Name	Severity	Short Description	Simple Fix
1	SMB Signing Not Required	Medium	SMB traffic is not signed, which makes it easier to modify	Turn on SMB signing
2	SSL Certificate Cannot Be Trusted	Medium	Certificate is not fully trusted by the system	Use a trusted SSL certificate
3	SSL Self-Signed Certificate	Medium	Certificate created by the system itself	Replace with a CA-signed certificate
4	SSL Wrong Hostname	Medium	Certificate name does not match the real hostname	Generate a certificate with the correct hostname
5	SSL Certificate Unknown Authority	Medium	Signed by a source not known to the system	Use a certificate from a trusted CA

---

3. Detailed Findings

3.1 SMB Signing Not Required

Severity: Medium

SMB signing is off, which means the system will accept unsigned SMB traffic.
Unsigned traffic can be changed by someone on the same network.

Fix: Turn on SMB signing through Local Group Policy.

3.2 SSL Certificate Cannot Be Trusted

Severity: Medium

The certificate used by a service is not trusted.
This may be due to it being expired, unsigned, or not from a known source.

Fix: Use a certificate from a trusted Certificate Authority.

3.3 SSL Self-Signed Certificate

Severity: Medium

A self-signed certificate is being used.
Self-signed certificates are not trusted because they are not verified by anyone.

Fix: Replace the certificate with one issued by a trusted CA.

3.4 SSL Wrong Hostname

Severity: Medium

The certificate's hostname does not match the system name.
This causes warnings and breaks secure communication.

Fix: Create a new certificate with the correct hostname.

3.5 SSL Certificate Signed by Unknown Authority

Severity: Medium

The certificate is signed by a source that the system does not trust.

Fix: Use a certificate from a known CA or install the root certificate.

---

4. Most Important Issues to Fix First

These are the issues that have the biggest effect:

1. **SMB Signing Not Required**

2. **SSL Wrong Hostname**
3. **SSL Self-Signed Certificate**

Fixing these will improve both network safety and secure communication.

---

6. Conclusion

The scan results taught me how vulnerability scanners collect information and how to read each finding.
The issues found are normal for many personal computers and can be fixed with basic steps.
This task helped me understand certificates, hostname checks, SMB security, and the basics of system hardening.