Medium Severity Vulnerability Report

This document provides a detailed analysis of **Medium Severity** vulnerabilities detected in the Nessus scan (**localhost_4p7sqi**). Each section includes the vulnerability description, potential impact, remediation steps, and references.

1. SSL Certificate Cannot Be Trusted

Port/Service: TCP 8834 / WWW

Risk Factor: Medium

CVSS v3.0 Score: 6.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

Description:

The SSL certificate used by this service cannot be trusted — likely because it's self-signed or issued by an untrusted certificate authority (CA). This exposes the system to potential man-in-the-middle (MITM) attacks.

Impact:

Users connecting over HTTPS might be tricked into connecting to an attacker-controlled system posing as the legitimate one.

Remediation:

Obtain and install a valid SSL/TLS certificate from a trusted Certificate Authority (CA).

References:

• ITU X.509 Standard
• Wikipedia: X.509

2. SMB Signing Not Required

Port/Service: TCP 445 / CIFS

Risk Factor: Medium

CVSS v3.0 Score: 5.3 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)

Description:

The remote SMB server does not require message signing, allowing MITM attacks that can modify SMB traffic.

Impact:

Attackers can intercept SMB traffic to steal credentials or inject commands.

Remediation:

Enforce SMB message signing:
• **Windows:** Enable “Digitally sign communications (always)” under Group Policy.
• **Samba:** Add server signing = mandatory to /etc/samba/smb.conf.

■ Summary Table

#	Vulnerability	Port/Service	Risk	CVSS v3	Impact	Recommended Fix
1	SSL Certificate Cannot Be Trusted	TCP 8834 (HTTPS)	Medium	6.5	MITM risk due to untrusted cert	Install trusted CA certificate
2	SMB Signing Not Required	TCP 445 (CIFS)	Medium	5.3	MITM via unsigned SMB traffic	Enforce SMB signing in system