Basic Vulnerability Scan Report

1. SMB Signing Not Required (Plugin ID: 57608)

Description:

This vulnerability allows unauthenticated, remote attackers to intercept and manipulate SMB communications via man-in-the-middle (MITM) attacks.

Severity: Medium

Fix/Mitigation:

Enable SMB signing in Windows:

- Go to Group Policy Editor -> Local Computer Policy -> Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Security Options.
- Set 'Microsoft network server: Digitally sign communications (always)' to Enabled.

2. SSL Certificate Cannot Be Trusted (Plugin ID: 51192)

Description:

The SSL certificate is either self-signed, expired, or not issued by a trusted Certificate Authority, making the server vulnerable to MITM attacks.

Severity: Medium

Fix/Mitigation:

Purchase or generate a valid SSL certificate from a trusted Certificate Authority (CA), and properly install the complete certificate chain.

3. SSL Certificate with Wrong Hostname (Plugin ID: 45411)

Description:

The SSL certificate's Common Name (CN) does not match the hostname of the server, which can cause browser trust warnings and security risks.

Severity: Medium

Fix/Mitigation:

Reissue the SSL certificate with the correct CN or use a wildcard/multi-domain certificate covering the actual hostname.

4. SSL Self-Signed Certificate (Plugin ID: 57582)

Description:

The SSL certificate is self-signed and not trusted by default in most browsers or systems, which can lead to data interception via MITM.

Severity: Medium

Fix/Mitigation:

Replace the self-signed certificate with one from a recognized Certificate Authority (CA).