- **2 High**
- **0 Critical**
- **2 Medium**
- **32 Informational**

Vulnerability Scan Summary Report

Target: 192.168.0.142

Scan Date: 07 Aug 2025

Tool Used: Nessus Essentials

High Severity Vulnerabilities

1.SSL certificate cannot be trusted

- **Plugin ID**: 51192
- **CVSS Score**: 6.5 (Medium, often listed under High depending on context)
- **Description**: The SSL certificate presented by the service cannot be trusted, possibly due to being self-signed or from an unknown certificate authority.
- **Risk**: Attackers could perform Man-in-the-Middle (MITM) attacks.
- **Solution**:

  Replace the certificate with one issued by a **trusted Certificate Authority (CA)**.

  Avoid using self-signed certificates in production.

2. SMB Signing not required

Plugin ID: 57608

- **CVSS Score**: 5.3 (Medium)
- **Description**: The SMB service does not require message signing.
- **Risk**: This can allow **MITM attacks** by modifying SMB traffic.
- **Solution**:
  - Enable SMB signing:
    - Open **Group Policy Editor** (gpedit.msc)

- Navigate to Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options
- Enable: **"Microsoft network client: Digitally sign communications (always)"** and **"Microsoft network server: Digitally sign communications (always)"**

Medium

Vulnerability	**Severity**	**Fix Summary**
SSL Certificate Cannot Be Trusted	Medium	Use trusted CA-signed certificate
SMB Signing Not Required	Medium	Enforce SMB signing via group policy