Nessus Vulnerability Scan Summary

Scan Date: 25 October 2025
Scanner: Tenable Nessus Essentials
Scanned Host: 192.168.56.1 (Local Machine)
Generated By: Aniket Mehere

- **Total Vulnerabilities Found:** 33

- Severity Breakdown:
  - Critical: 0
  - High: 0
  - Medium: 1
  - Low: 0
  - Informational: 32

- **Key Medium-Level Vulnerability:**

Plugin: SSL Certificate Cannot Be Trusted
Plugin ID: 51192
Severity: Medium (CVSS v3: 6.5)
Description:
The SSL certificate used by the target host cannot be trusted. It may be self-signed or not issued by a recognized Certificate Authority (CA). This can allow attackers to intercept traffic via man-in-the-middle (MITM) attacks.

- **Most Critical Vulnerabilities**

Vulnerability	Severity	Description	CVSS	Recommended Fix
SSL Certificate Cannot Be Trusted	Medium	The SSL certificate used by the host is self-signed or untrusted, allowing potential man-in-the-middle (MITM) attacks.	6.5	Replace with a trusted SSL certificate issued by a recognized Certificate Authority (CA). Ensure HTTPS connections use valid certificates.

- **Informational Findings**

Finding	Description
Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure	The SMB authentication process reveals NetBIOS names, useful for reconnaissance.
Microsoft Windows SMB NativeLanManager Remote System Information Disclosure	SMB service leaks system details to remote users.
OS Security Patch Assessment Not Available	Nessus could not determine patch status, possibly due to unauthenticated scan.
TLS 1.2 and 1.3 Protocol Detection	The host supports modern secure TLS versions — good security practice.
Service Enumeration (HTTP, SMB, Netstat)	Network services are active and detected; no immediate risk but useful for attackers.

- **Recommended Actions**

1. **Replace or Update SSL Certificates**
    - Use CA-signed certificates instead of self-signed ones.
    - Regularly renew and validate SSL/TLS configurations.
2. **Harden SMB and NTLM Services**
    - Disable SMBv1 and enforce SMBv2/v3 only.
    - Restrict NTLM authentication where possible.
3. **Enable Authenticated Scanning**
    - Provide valid credentials in Nessus for deeper analysis and patch validation.

4. **Apply System Updates Regularly**
    - Ensure OS and software are up to date with the latest security patches.
5. **Limit Unnecessary Network Exposure**
    - Close unused ports and restrict access to essential services onl