Vulnerability Assessment Report

Name: Rishikesh

Date: 07 August 2025

Tool Used: Nessus Essentials

Target IP: 192.168.56.1

Scan Duration: 8 minutes

Operating System: Windows 11

Authentication: Failed

# Scan Summary

Vulnerabilities by Severity:

|  |  |
| --- | --- |
| Severity | Count |
| Critical | 0 |
| High | 0 |
| Medium | 2 |
| Low | 0 |
| Info | 31 |

# Top Vulnerabilities

1. SMB Signing Not Required (Medium)

Description:  
Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.  
  
Solution:  
Enforce message signing in the host’s configuration. On Windows, this is found in the policy setting ‘Microsoft network server: Digitally sign communications (always)’. On Samba, the setting is called 'server signing'.  
  
Risk Score: CVSS v3.0 Base Score: 5.3  
Plugin ID: 57608  
Type: Remote

# Additional Vulnerabilities (Information Level)

The scan identified several info-level issues including SSL, SMB, HTTP, TLS misconfigurations, and service detections. These are not critical but can be useful for deeper auditing or hardening.