Vulnerability Scan Report - Task 3

Detail	Value
Name:	Palakshpatel
Date:	September 25, 2025 (Current Date)
Scanner:	Nessus Essentials
Scan Target:	10.22.172.159
Scan Duration:	18 minutes

1. Scan Summary

The Basic Network Scan successfully completed, identifying no Critical or High severity issues. The primary findings were four Medium-severity configuration errors and numerous Informational findings.

Severity	Count
Critical	0
High	0
Medium	4
Low	0
Informational	37

2. Documentation of Medium/High Vulnerabilities

The following Medium-severity issues are the most significant security risks identified and require remediation.

A. SMB Signing not required

- **Nessus Plugin ID:** 57608
- **CVSS Score:** 5.3
- **Description:** The remote SMB server is configured to allow communications without message signing. This allows an unauthenticated, remote attacker to perform a Man-in-the-Middle (MITM) attack to intercept and modify traffic between the client and server.
- **Mitigation/Remediation:** Enforce message signing in the host's configuration. This is done via **Local Group Policy Editor** (gpedit.msc):

    - Navigate to Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options.
    - Enable the policy: **Microsoft network server: Digitally sign communications (always)**.

B. SSL Certificate Cannot Be Trusted

- **Nessus Plugin ID:** 51192
- **CVSS Score:** 6.5
- **Description:** The server's X.509 certificate cannot be trusted as it is signed by an unknown or unrecognized certificate authority. This nullifies the security benefit of SSL, as an attacker could potentially establish an MITM attack.
- **Mitigation/Remediation:** This typically occurs with auto-generated certificates (like for Remote Desktop).
    - **Best Fix:** Replace the self-signed certificate with one issued by a trusted Enterprise CA or a publicly recognized CA.
    - **Simple Fix:** If Remote Desktop (RDP) is the cause, configure the RDP service to use the computer's valid certificate instead of the auto-generated self-signed certificate.

C. SSL Self-Signed Certificate

- **Nessus Plugin ID:** 57582
- **CVSS Score:** 6.5
- **Description:** The certificate chain for a service end in an unrecognized self-signed certificate. This is often reported alongside Plugin 51192 and shares the same risks and causes.
- **Mitigation/Remediation:** The solution is the same as for Plugin 51192: **Purchase or generate a proper certificate for this service**.