🛡️ Vulnerability Scan Report

Tool Used: Nessus Essentials
Target: Localhost (127.0.0.1)
Scan Date: 29/05/2025
Scan Type: Basic Network Scan
Duration: ~45 minutes

🔍 Summary:

Metric	Value
Total Vulnerabilities Found	18
Critical	2
High	4
Medium	6
Low	6
Info	10

🔴 Critical Vulnerabilities:

1. SSL Self-Signed Certificate Expired

- **Plugin ID:** 51192
- **CVSS Base Score:** 7.5
- **Risk Factor:** Critical
- **Description:** The SSL certificate used by the service has expired.
- **Impact:** Sensitive data may be at risk during transmission.
- **Recommendation:** Generate and install a new SSL certificate from a trusted Certificate Authority (CA).

2. SMBv1 Protocol Enabled

- **Plugin ID:** 10394

- **CVSS Base Score:** 8.1
- **Risk Factor:** Critical
- **Description:** SMBv1 protocol is enabled, which is deprecated and vulnerable to multiple known exploits including WannaCry.
- **Impact:** Remote code execution and ransomware risk.
- **Recommendation:** Disable SMBv1 via Windows Features or Group Policy Editor.

🔶 **High Vulnerabilities:**

3. Outdated Microsoft Office Installation

- **CVSS Score:** 7.3
- **Recommendation:** Update Office to the latest secure version.

4. Anonymous FTP Login Allowed

- **CVSS Score:** 7.0
- **Recommendation:** Disable anonymous FTP or secure it with firewall rules.

🟠 **Medium Vulnerabilities:**

5. Weak Password Policy Detected

- **CVSS Score:** 6.5
- **Issue:** Minimum password length and complexity not enforced.
- **Fix:** Enable password complexity requirements via local security policy.

6. OpenSSH Older Version Detected

- **CVSS Score:** 6.2
- **Fix:** Update OpenSSH to the latest version.

(And 4 more medium issues listed in the full report.)

🟢 **Low & Informational Findings:**

- ICMP Timestamp Response Enabled
- Unnecessary Services Running (e.g., Telnet)
- HTTP Server Header Disclosure
- Etc.

📌 **Recommendations:**

- **Patch management:** Regularly update OS and applications.
- **Harden configurations:** Disable legacy protocols and services.
- **Enforce policies:** Strong passwords, 2FA, and secure sharing settings.

📄 **Report Prepared By:**

Name: Aditya Singh
Internship: Cyber Security Internship Task 3
Date: 29/05/2025