# ****Sample Vulnerability Scan Report****

**Scan Target:** localhost (Windows 10 PC)  
**Scan Tool:** Nessus Essentials  
**Scan Type:** Basic Network Scan / Full Scan  
**Scan Date:** 25-Sep-2025  
**Scan Duration:** ~45 minutes

## ****Summary****

| **Severity** | **Number of Vulnerabilities** |
| --- | --- |
| Critical | 2 |
| High | 3 |
| Medium | 5 |
| Low | 4 |
| Total | 14 |

## ****Critical Vulnerabilities****

| **Vulnerability** | **CVE** | **Description** | **Recommended Fix** |
| --- | --- | --- | --- |
| SMBv1 Protocol Enabled | CVE-2017-0144 | Older SMB version is vulnerable to ransomware attacks like WannaCry. | Disable SMBv1 and enable SMBv2/3. |
| Unpatched Windows OS | CVE-2023-34527 | Critical remote code execution vulnerability (PrintNightmare). | Apply latest Windows Updates. |

## ****High Severity Vulnerabilities****

| **Vulnerability** | **CVE** | **Description** | **Recommended Fix** |
| --- | --- | --- | --- |
| Outdated Web Browser | CVE-2022-12345 | Browser version contains known vulnerabilities. | Update to latest version. |
| Weak Password Policy | CVE-N/A | Local accounts have weak passwords. | Enforce strong password policy. |
| Open RDP Port | CVE-2019-0708 | Remote Desktop Protocol is exposed and vulnerable. | Disable unused RDP or restrict via firewall. |

## ****Medium Severity Vulnerabilities****

| **Vulnerability** | **CVE** | **Description** | **Recommended Fix** |
| --- | --- | --- | --- |
| Unnecessary Services Running | CVE-N/A | Several background services are not needed. | Disable unused services. |
| Outdated Java | CVE-2021-3456 | Java runtime has security flaws. | Update to latest Java version. |
| Others | Various | Miscellaneous low-impact vulnerabilities. | Apply recommended updates. |

## ****Low Severity Vulnerabilities****

| **Vulnerability** | **Description** | **Recommended Fix** |
| --- | --- | --- |
| Weak Cipher Suites | Some SSL/TLS ciphers are weak. | Disable weak ciphers in Windows. |
| Unnecessary Files | Temporary files may contain sensitive data. | Clean temp files. |
| Others | Minor configuration issues. | Apply system hardening best practices. |

Screenshots

