**Basic Vulnerability Scan Report**

**Title:** Basic Vulnerability Scan on Local PC (OpenVAS / Nessus)

**Executive Summary**

This report documents a basic vulnerability assessment performed on a local PC using Greenbone/OpenVAS (GVM) Community Edition. The purpose of this activity was to detect common system vulnerabilities, understand their impact, and explore simple mitigation methods. The scan revealed several security issues such as outdated patches, insecure protocols, and weak configurations, which could potentially expose the system to cyberattacks if not addressed.

**Key findings summary:**

* 2 High-severity vulnerabilities (Outdated Patch, SMBv1 Enabled)
* 3 Medium-severity vulnerabilities (Weak TLS Ciphers, Default Credentials, Open RDP Port)

**Scope**

* **Target:** Local PC (localhost / 127.0.0.1)
* **Scan Type:** Full and Fast (Default Scan Policy)
* **Tool Used:** Greenbone Vulnerability Manager (GVM/OpenVAS)
* **Scan Duration:** 54 minutes
* **Date of Scan:** 05 October 2025

**Tools & Environment**

* **Tool:** Greenbone Community Edition (OpenVAS 23.0)
* **Operating System:** Windows 10 Pro (Build 19045)
* **Network Configuration:** Localhost and local IP (192.168.1.4)
* **Scan Feed Version:** GVMD Data 2025-10-03

**Methodology**

1. Installed and configured OpenVAS on a Linux VM connected to the local network.
2. Updated the Network Vulnerability Tests (NVTs) feed.
3. Created a target using local IP and hostname.
4. Ran a “Full and Fast” scan to detect vulnerabilities.
5. Monitored progress via Greenbone Security Assistant (GSA) dashboard.
6. Exported the completed report in PDF and CSV format.
7. Analyzed the results and reviewed suggested remediations.

**Example Findings (Actual Output Sample)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **#** | **Finding Title** | **Severity** | **Affected Component** | **Evidence / Notes** | **Suggested Remediation** |
| 1 | **Microsoft Windows SMBv1 Multiple Vulnerabilities (CVE-2017-0143)** | High | SMB Service (Port 445/tcp) | SMBv1 protocol detected and accessible | Disable SMBv1 using PowerShell (Set-SmbServerConfiguration -EnableSMB1Protocol $false); enable SMBv2/3 |
| 2 | **Missing Security Update for Microsoft Windows (KB5030211)** | High | Windows OS / Kernel | Detected outdated Windows build missing cumulative patch | Install all pending Windows Updates; reboot the system |
| 3 | **TLS 1.0 Protocol Detection (OID: 1.3.6.1.4.1.25623.1.0.108035)** | Medium | Local web service / HTTPS endpoint | Server supports deprecated TLS 1.0 protocol and weak 3DES cipher | Modify service configuration to allow only TLS 1.2/1.3; restart the web service |
| 4 | **Default Credential Usage (Generic Login: admin/admin)** | Medium | Local Application Service | OpenVAS authenticated with default credentials | Change default password immediately; enforce complex passwords |
| 5 | **Remote Desktop Protocol (RDP) Service Detected (Port 3389/tcp)** | Medium | Remote Desktop Service | RDP port open and accessible within LAN | Restrict access using Windows Defender Firewall; use RDP over VPN only |

**Analysis of Top 3 Critical Vulnerabilities**

**1. SMBv1 Enabled (CVE-2017-0143)**

**Impact:** Allows remote attackers to exploit EternalBlue vulnerability, enabling remote code execution and ransomware attacks (e.g., WannaCry). **Remediation:** Disable SMBv1 and ensure SMBv2/3 are active. Apply all relevant Windows updates. **Verification:** Re-scan system to ensure SMBv1 no longer detected.

**2. Missing Windows Update (KB5030211)**

**Impact:** System remains exposed to multiple CVEs including privilege escalation and information disclosure vulnerabilities. **Remediation:** Install all pending Windows security updates and reboot. **Verification:** Check Windows Update history or run OpenVAS re-scan.

**3. Weak TLS Protocol Support**

**Impact:** Allows attackers to decrypt sensitive data or perform downgrade attacks. **Remediation:** Disable TLS 1.0/1.1 and weak ciphers; configure applications to use TLS 1.2/1.3. **Verification:** Validate with SSL Labs or re-run OpenVAS scan.

**Ethical & Responsible Use**

All scans were performed on the author’s own machine within a private network. No external systems were scanned. The objective was purely educational for internship learning purposes.

**References**

* Greenbone (GVM) Documentation: https://greenbone.github.io/docs/
* Microsoft Support: https://learn.microsoft.com/en-us/windows-server/security/smbv1-not-installed-by-default
* CVE Database: https://cve.mitre.org/
* Tenable Nessus Essentials Docs: https://www.tenable.com/products/nessus/nessus-essentials