Vulnerability Scan Report: Securing Your Windows PC

Executive Summary:

This report documents a simulated basic vulnerability scan performed on a sample Windows 10 PC (IP: 192.168.1.100, hostname: WIN10-TEST) using free tools: OpenVAS Community Edition and Nessus Essentials. The objective was to identify common vulnerabilities, assess their severity, and propose simple mitigations.

Key Findings:

Total Vulnerabilities Identified: 12 (across both tools; some overlaps).

Severity Breakdown:

Critical: 2

High: 4

Medium: 4

Low: 2

Risk Score (CVSS-based average): 7.2/10 (High overall exposure).

Introduction:

Vulnerability scanning is a proactive cybersecurity practice to detect weaknesses in systems before exploitation. This exercise targets a local Windows PC, common in home or small office setups. Using free tools like OpenVAS (open-source) and Nessus Essentials (limited free version from Tenable), we scanned for known vulnerabilities in OS, applications, and network services.

Scope: Localhost/127.0.0.1 and local IP (192.168.1.100). No external network exposure was tested.

Assumptions: The PC runs Windows 10 (unpatched for simulation), with default firewall and common apps (e.g., Edge browser, Office).

Methodology:

Tool Selection

OpenVAS Community Edition: Free, open-source scanner with daily-updated feeds for 95,000+ vulnerability tests.

Installation Steps:

OpenVAS on Ubuntu 22.04 (Scanner Host)

Update system:

```
 sudo apt update && sudo apt upgrade -y.
```

Install:

```
 sudo apt install openvas (pulls dependencies like PostgreSQL).
```

Configure:

```
 sudo gvm-setup (downloads feeds; takes 10-20 mins; note admin password).
```

Verify:

```
 sudo gvm-check-setup (should report “OK”).
```

Start services:

```
 sudo systemctl start openvas-scanner openvas-manager gvm.
```

Access web UI: https://127.0.0.1:9392 (accept self-signed cert).

Scan Configuration:

OpenVAS Setup

Log in to web UI.

Navigate to Scans > Tasks > Create a Task (use “Full and Fast” scan config).

Target: 127.0.0.1 or 192.168.1.100.

Start scan; monitor progress under Scans > Results.

OpenVAS Results Summary:

Severity	Count	Examples
Critical	1	CVE-2020-0601 (CryptoAPI Spoofing)
High	2	CVE-2022-37969 (Privilege Escalation in Log File System)
Medium	2	Outdated SMBv1 enabled
Low	1	Weak RDP config

Sample Report Excerpt (from Results Tab):

Host: 192.168.1.100 (Windows 10 Enterprise 21H2)

Vulnerabilities: 6 total.

Report ID: Simulated-OV-20250926-001

Distribution: Bars show 1 Critical (red), 2 High (orange), etc.

Identified Vulnerabilities and Mitigations

Most Critical Vulnerabilities (Top 3)

CVE-2025-24993: Buffer Overflow in Windows Kernel (Critical, CVSS 9.8)

Description: Allows remote code execution via crafted input; actively exploited.

Impact: Full system compromise.

Fix: Install latest Windows Update (KB503xxxx). Run Windows Update > Check for updates.

Timeline: Immediate (5 mins).

CVE-2020-0601: CryptoAPI Spoofing (Critical, CVSS 9.8)

Description: Bypasses certificate validation for malicious executables.

Impact: Malware masquerades as trusted software.

Fix: Apply MS20-004 patch via Windows Update. Enable Secure Boot in BIOS.

Timeline: Immediate.

CVE-2022-37969: Elevation of Privilege in CLFS (High, CVSS 7.8)

Description: Local attacker escalates to SYSTEM privileges via log files.

Impact: Persistent access post-initial breach.

Fix: Install MS22-xxx patch. Harden via Group Policy: Restrict log access.

Timeline: Within 24 hours.

Recommendations

Patch Immediately: Enable automatic Windows Updates (Settings > Update & Security).

Re-Scan: Run tools weekly to verify fixes.

Enhance Hygiene: Use strong passwords, firewall, and antivirus (e.g., Windows Defender).

Next Steps: If critical issues persist, escalate to professional audit.

Limitations: This is a basic scan; advanced threats (e.g., zero-days) require ongoing monitoring.

Conclusion:

This scan highlights the importance of regular maintenance—most issues stem from unpatched software, fixable with built-in tools. Implementing these mitigations reduces exposure significantly.