Comprehensive Vulnerability Assessment Report

1. Executive Summary

This report documents the findings from a vulnerability scan performed on my local system using **OpenVAS Community Edition**. The scan aimed to identify security weaknesses, assess their potential impact, and implement appropriate remediation measures. The assessment revealed several vulnerabilities across different severity levels, with critical issues primarily related to outdated software and unnecessary open ports.

---

2. Scope & Methodology

Scope of Assessment

- **Target System:** Personal computer running Windows 11
- **Scan Type:** Full vulnerability scan
- **Focus Areas:**
  - Operating system vulnerabilities
  - Software security patches
  - Network port exposure
  - Configuration weaknesses

Tools & Techniques

- **Primary Scanner:** OpenVAS (Greenbone Community Edition)
- **Scan Duration:** Approximately 50 minutes
- **Scan Configuration:**
  - Credentialed scan (for deeper system inspection)
  - Full port range (1-65535)
  - Enabled all vulnerability tests

Scan Process

1. **Setup & Configuration**
   - Installed OpenVAS on a dedicated virtual machine
   - Configured scan target as localhost (127.0.0.1)
   - Verified network connectivity between scanner and target
2. **Scan Execution**

    - Initiated a full vulnerability scan
    - Monitored progress through the OpenVAS web interface
    - Allowed scan to complete without interruptions
3. **Results Analysis**
    - Reviewed the automated report
    - Validated findings against external threat databases (CVE, NVD)
    - Prioritized vulnerabilities based on CVSS scores

---

3. Detailed Findings

Vulnerability Distribution

The scan detected **42 vulnerabilities** with the following distribution:

Severity Level	**Count**	**Percentage**
Critical	5	12%
High	11	26%
Medium	18	43%
Low	8	19%

Critical Vulnerabilities

1. **Windows OS Security Update Gap (CVE-2023-32047)**
    - **CVSS Score:** 9.8 (Critical)
    - **Description:** Missing cumulative security update for Windows 11
    - **Impact:** Could allow remote code execution
    - **Remediation:** Installed latest security patches via Windows Update
2. **Exposed Remote Desktop Protocol (Port 3389/TCP)**
    - **CVSS Score:** 8.8 (High)
    - **Description:** RDP service exposed to network
    - **Impact:** Potential brute force attacks

    - **Remediation:** Disabled RDP and configured firewall to block port

3. **Outdated Java Runtime (CVE-2023-21937)**
    - **CVSS Score:** 8.3 (High)
    - **Description:** Java SE vulnerability allowing sandbox escape
    - **Impact:** Possible privilege escalation
    - **Remediation:** Uninstalled deprecated Java version

---

4. Risk Analysis & Remediation

Risk Prioritization Matrix

Risk Level	**Criteria**	**Action Timeline**
Immediate	Critical CVSS ≥ 9.0	Within 24 hours
High	CVSS 7.0-8.9	Within 72 hours
Medium	CVSS 4.0-6.9	Within 1 week
Low	CVSS ≤ 3.9	Scheduled maintenance

Implemented Remediation Actions

- **Patch Management:**
    - Updated Windows OS and all installed software
    - Enabled automatic updates for critical applications
- **Network Hardening:**
    - Reviewed and adjusted firewall rules
    - Disabled unnecessary services (SMBv1, Telnet)
- **Configuration Changes:**
    - Implemented stronger password policies
    - Enabled disk encryption

5. Lessons Learned

Technical Insights

- Vulnerability scanners heavily rely on CVE databases and version detection
- Credentialed scans provide more accurate results than network-only scans
- False positives occur when scanners misinterpret system configurations

Operational Improvements

- Established a monthly vulnerability scanning schedule
- Created a system hardening checklist for future reference
- Documented a standardized remediation process

6. Conclusion & Recommendations

This assessment successfully identified and mitigated critical security weaknesses in my personal computing environment. The findings underscore the importance of:

1. **Regular Vulnerability Scanning:** At least monthly for personal systems
2. **Proactive Patch Management:** Automated updates for all software
3. **Defense-in-Depth:** Combining scans with other security measures

Future Work:

- Expand scanning to include mobile devices and IoT equipment
- Implement continuous monitoring solutions
- Conduct penetration testing to validate remediation efforts