Basic Vulnerability Scan Report

Target System: Local PC (127.0.0.1)

Operating System: Microsoft Windows 10 (64-bit)

Scan Type: Full Vulnerability Scan

Scan Duration: ~35 minutes

Summary of Findings:

Critical: 1

High: 2

Medium: 3

Low: 2

Total: 8

1. **Outdated OpenSSH**

Service Severity: High

CVSS Score: 8.1

Description: The system is running an outdated version of OpenSSH vulnerable to known exploits. Impact: Unauthorized remote shell access. Remediation: Update OpenSSH to the latest version.

2. **Unpatched Windows Kernel**

Components

Severity: Critical

CVSS Score: 9.3

Description: The operating system lacks recent security patches, allowing privilege escalation. Impact: Local attacker may gain SYSTEM-level access. Remediation: Apply latest Windows security updates.

3. **Open Port Detected (Port 3306**

– MySQL)

Severity: Medium

CVSS Score: 6.5

Description: MySQL service is running and listening

on the network. Impact: Possible brute-force or

unauthorized database access.

Remediation: Restrict MySQL to localhost or disable if unused.

4. **Weak Firewall**

Configuration Severity:

Medium

CVSS Score: 5.9

Description: Windows

Firewall rules are not

strictly configured.

Impact: Increased

exposure to network-

based attacks.

Remediation: Enable and properly configure Windows Defender Firewall.

5. **Outdated Web**

Browser Severity:

Medium

CVSS Score: 5.4

Description: Installed web browser version is

outdated. Impact: Vulnerable to phishing and

drive-by downloads.

Remediation: Update browser and remove unnecessary extensions.

6. **Guest User Account**

Enabled Severity: Low

CVSS Score: 3.1

Description: Guest user account is

enabled. Impact: Unauthorized local

system access. Remediation: Disable

guest account.

7. **Weak Password**

Policy Severity:

Low

CVSS Score: 2.8

Description: Password complexity policy is not

enforced. Impact: Increased risk of brute-force

attacks.

CVSS Score: 5.9

Description: Windows Firewall rules are not strictly

configured. Impact: Increased exposure to network-

based attacks.

Remediation: Enable and properly configure Windows Defender Firewall.

Remediation: Enforce strong password and lockout policies.

8. **ICMP Echo Response**

Enabled Severity: Low

CVSS Score: 2.5

Description: System responds to ICMP echo

(ping) requests. Impact: Helps attackers perform

network reconnaissance.

Remediation: Disable ICMP echo responses if not required.

Conclusion:

This vulnerability scan demonstrates common security risks present in Windows-based personal computers and highlights the importance of regular patching, firewall configuration, and vulnerability assessments.