Basic Vulnerability Scan Report

By: Gayathri Vassou

Tool Used: Nessus Essentials

Scan Date: August 07, 2025

System Scanned: Localhost (127.0.0.1)

# Objective

To identify and document common vulnerabilities present on my computer using a free vulnerability scanning tool.

# Tool Used

- Nessus Essentials (Free version)  
- Installed and configured on Windows  
- Local machine IP set to 127.0.0.1

# Scan Configuration

- Type of Scan: Full Vulnerability Scan  
- Scan Target: Localhost  
- Scan Duration: Approximately 45 minutes

# Scan Results Summary

|  |  |
| --- | --- |
| Severity Level | Number of Vulnerabilities |
| 🔴 Critical | 2 |
| 🟠 High | 4 |
| 🟡 Medium | 6 |
| 🔵 Low | 3 |
| 🟢 Info | 10 |

# Top 3 Critical Vulnerabilities Identified

* • CVE-2020-0796: SMBv3 Remote Code Execution

- Description: Vulnerability in Windows SMBv3 allows remote code execution.  
 - Fix: Apply Windows update KB4551762 or disable SMBv3 compression.

* • CVE-2017-0144: EternalBlue

- Description: Exploitable via SMBv1; used in WannaCry ransomware.  
 - Fix: Disable SMBv1 and install latest Windows security updates.

* • CVE-2021-34527: PrintNightmare

- Description: Remote code execution vulnerability in Windows Print Spooler.  
 - Fix: Disable Print Spooler service if not needed, apply KB5004945 patch.

# Mitigation Steps Taken

- Installed latest Windows Updates (Windows Update > Check for Updates).  
- Disabled SMBv1 and Print Spooler via Windows Features and Services.  
- Enabled firewall to block vulnerable ports (e.g., 445, 139).

# Screenshots Attached

- Dashboard showing scan results  
- Details of top critical vulnerabilities  
- Settings panel used for scanning

# Conclusion

A full system scan was successfully performed using Nessus Essentials. Several critical and high-risk vulnerabilities were found and mitigated with patches and system changes. Screenshots and findings were documented for submission.