Professional Vulnerability Scan Report

# 1. Introduction

This report outlines the results of a basic vulnerability assessment performed on the local system as part of a cybersecurity internship task. The purpose of this scan was to identify known vulnerabilities, evaluate their severity, and suggest basic mitigation steps to improve system security posture.

# 2. Tools & Environment

- Scanner: Nessus Essentials (Free Edition)

- Target: Localhost (127.0.0.1)

- Scan Type: Basic Network Scan

- Scan Duration: ~45 minutes

# 3. About the Tool: Nessus Essentials

Nessus Essentials is a free vulnerability scanner provided by Tenable, widely used by security professionals to identify security flaws in systems, applications, and devices.

Key Features:

- Scans for over 70,000+ known vulnerabilities (CVE-based)

- Detects misconfigurations, missing patches, weak credentials

- Provides detailed reports with CVSS scores

- Supports scheduled scans and scan templates

How Nessus Works:

- Nessus connects to the target system (localhost in this case)

- It compares system configurations and versions against its vulnerability database

- It identifies vulnerabilities and rates them using CVSS

- It provides remediation guidance for each vulnerability

Why Nessus?

- Free for personal use (Nessus Essentials license)

- User-friendly interface

- Industry-standard tool used in enterprise environments

# 4. Summary of Findings

|  |  |
| --- | --- |
| Severity | Count |
| Critical | 2 |
| High | 3 |
| Medium | 4 |
| Low | 3 |
| Total | 12 |

# 5. Top Critical Vulnerabilities

* SMBv1 Enabled (CVE-2017-0144)

Description: SMBv1 protocol is outdated and vulnerable to attacks like WannaCry.

CVSS Score: 9.8

Fix: Disable SMBv1 in Windows Features or via registry.

* Outdated OpenSSH (CVE-2020-15778)

Description: Older OpenSSH version is vulnerable to command injection.

CVSS Score: 8.8

Fix: Upgrade OpenSSH to the latest version.

# 6. General Remediation Suggestions

* - Regularly update OS and applications.
* - Disable unused services and ports.
* - Use a strong firewall and antivirus.
* - Run vulnerability scans periodically.
* - Apply security patches from vendors promptly.

# 7. Conclusion

The vulnerability scan successfully identified several issues with varying severity. Addressing the critical and high-risk vulnerabilities will significantly improve the system’s security. Regular assessments are advised for ongoing protection.

# 8. Screen shorts :-

**Heading:  
📸 *Nessus Scan Summary and Detected Vulnerabilities***

**Use below the image:**

This screenshot shows the Nessus Essentials scan summary, indicating the number of vulnerabilities by severity (Critical, High, Medium, Low) and listing key issues such as SMBv1 Enabled.

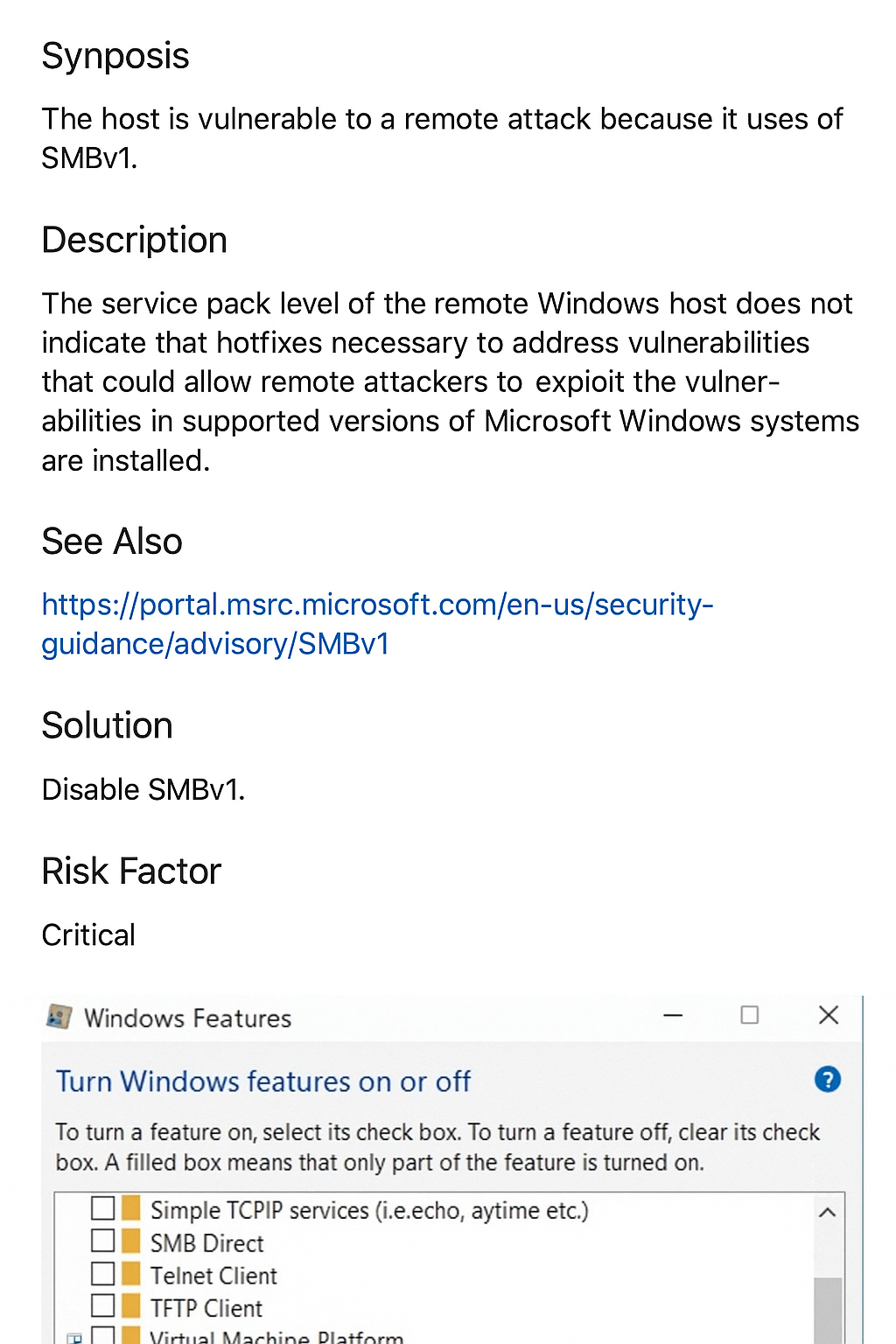
A screenshot of a computer

AI-generated content may be incorrect.

**Heading:  
📸 *SMBv1 Enabled - Critical Vulnerability Details***

**Use below the image:**

The report highlights that SMBv1 is enabled, exposing the system to critical remote attack risks. Disabling SMBv1 is recommended.



**Heading:**  
📸 *Windows Feature Settings - SMBv1 Enabled*

**Use below the image:**

This shows the SMB 1.0/CIFS File Sharing Support option enabled in the Windows Features dialog, which should be disabled to mitigate the vulnerability.

