Basic Vulnerability Scan Report

Cyber Security Internship - Task 3

Tool Used: Nessus Essentials

Target: Localhost (127.0.0.1)

Scan Date: May 29, 2025

1. Introduction

This report presents the findings from a basic vulnerability scan performed on a personal laptop using Nessus Essentials. The goal was to identify common vulnerabilities that could expose the system to security threats. The scan targeted the localhost (127.0.0.1) and was conducted using a full vulnerability profile.

2. Methodology

The scan was conducted with the following steps:

1. Installed Nessus Essentials.
2. Configured a full scan targeting the local machine.
3. Allowed the scan to run for approximately 45 minutes.
4. Analyzed the report for vulnerabilities and categorized them based on severity.
5. Researched fixes and best practices for the identified issues.

3. Vulnerabilities Identified

Vulnerability	CVE ID	Severity	Description
SMBv1 Enabled	CVE-2017-0144	Critical	The SMBv1 protocol is outdated and vulnerable to the EternalBlue exploit, which was used in the WannaCry ransomware attacks.
SSL/TLS Weak Cipher Suites	-	High	The server supports weak SSL/TLS cipher suites that are vulnerable to cryptographic attacks such as BEAST or FREAK.
OpenSSH Outdated Version	-	Medium	An older version of OpenSSH was detected which may contain known vulnerabilities.
Windows SMB Signing Not Required	-	High	Lack of SMB signing may allow man-in-the-middle (MITM) attacks on SMB traffic.
Insecure HTTP Methods Enabled	-	Medium	HTTP methods such as PUT or DELETE are enabled, which

			could be abused if not properly secured.
ICMP Timestamp Response Enabled	CVE-1999-0524	Low	The system responds to ICMP timestamp requests, which could be used in reconnaissance attacks.
Anonymous FTP Login Allowed	-	High	FTP server allows anonymous login, which may expose sensitive data to unauthorized users.
Unpatched Windows Updates	Multiple CVEs	Critical	The system is missing important security updates that patch critical vulnerabilities.

4. Conclusion

The vulnerability scan revealed several high and critical severity issues that could potentially expose the system to cyber threats. It is recommended to disable outdated services like SMBv1, apply all pending Windows updates, configure secure protocols, and limit access permissions. Taking these steps will greatly improve the system's overall security posture.