My Vulnerability Scan Report – Task 3

Introduction

For this task, I carried out a basic vulnerability scan on my own system to get hands-on experience with identifying potential security issues. The idea was to understand what kinds of weaknesses might exist on a regular PC and how to recognize them using tools like Nessus Essentials or OpenVAS.

Tools I Used

I chose to go with Nessus Essentials since it's user-friendly, free, and great for beginners like me who are just stepping into vulnerability assessment.

What I Did (Step-by-Step):

Installed Nessus Essentials

I downloaded and set it up on my system. It took a while, but the process was straightforward with the help of online tutorials.

Set the Scan Target

I set the target as my local machine by using localhost. I made sure the device was connected and idle during the scan.

Launched a Full System Scan

I ran a full vulnerability scan. It took about 45–50 minutes to finish completely.

Reviewed the Results
Once the scan was done, I went through the detailed report Nessus generated. It flagged a few critical and medium-level vulnerabilities on my system.

Researched the Issues
I took a closer look at the top 2–3 critical vulnerabilities and Googled how they can be fixed or reduced. Most of them had to do with outdated services or weak configurations.

Critical Vulnerabilities Found
Here are some key vulnerabilities that Nessus pointed out:

Outdated Windows SMBv1 Service
This is a known security risk. It can be used for lateral movement in networks if not disabled.

Weak SSL/TLS Configuration
My system had an insecure SSL protocol enabled which is considered deprecated.

Unpatched Software
A couple of applications weren’t updated to their latest versions, which could allow known exploits.

What I Learned:
Doing this task really helped me understand how vulnerable a system can be—even one I use every day. It also made me realize how important it is to keep software up to date, disable unused services, and perform regular scans.