Task 3 :- Perform a Basic Vulnerability Scan on Your PC.

Objective

To perform a basic vulnerability scan on a Windows machine using Tenable Nessus Essentials, identify system vulnerabilities, and generate a structured report for analysis and mitigation planning.

Tool Used

- **Nessus Essentials** (by Tenable)
- Platform: **Windows 10**

Steps Performed

1. Installation of Nessus on Windows

- Downloaded Nessus Essentials from tenable.com
- Ran the installer and accessed it through https://localhost:8834/
- Registered with an email address to get the free activation code
- Let Nessus download plugins and initialize (takes about 10–20 minutes)

2. Creating and Configuring the Scan

- Logged in to the Nessus dashboard
- Clicked **New Scan** > **Basic Network Scan**
- Named the scan and set target as local machine IP (e.g., 192.168.x.x)
- Used default scan settings (unauthenticated scan)

3. Running the Scan

- Clicked **Save and Launch**
- Waited for scan to complete (~30–45 minutes)

4. Reviewing Results

- Nessus categorized vulnerabilities as **Critical**, **High**, **Medium**, **Low**, or **Informational**

- Each result included plugin IDs, CVEs, and suggested remediations

5. Exporting the Report

- Exported results as a PDF for review
- Took screenshots of the dashboard and findings

Sample Vulnerability Summary

Severity	Count
Critical	1
High	4
Medium	7
Low	5
Informational	12

Conclusion

Using Nessus Essentials, I performed a successful vulnerability assessment of my Windows machine. The scan helped identify outdated services and misconfigurations, allowing me to understand key areas that need securing. The report provides a roadmap for improving my system's security posture.