ELEVATE LABS

CYBER SECURITY INTERNSHIP

INTERN NAME - **AMIT MAURYA**

TASK - Perform a Basic Vulnerability Scan on Your PC.

To generate a Report, we follow these steps

Using Nessus Essentials (Recommended for Beginners)

🔧 **Step-by-Step:**

1. Download and Install Nessus Essentials

- Go to: https://www.tenable.com/products/nessus/nessus-essentials
- Register with your email to get a **free activation code**.
- Download Nessus for your OS (Windows, macOS, Linux).
- Install it and **start the Nessus service**.

2. Access the Web Interface

- Open a browser and go to: https://localhost:8834
- Follow the setup:
  - Enter the **activation code** you got.
  - Create a user and password.

3. Add Your PC as a Scan Target

- Go to **"My Scans"** → Click **“New Scan”** → Choose **“Basic Network Scan”**
- Name it (e.g., “My PC Scan”)
- In “Targets”, enter 127.0.0.1 (localhost) or your machine’s IP address.
  - To find IP: Open Command Prompt → run ipconfig → look for **IPv4 Address**

4. Run the Scan

- Click **"Save"**, then click the **play icon (▶)** to start the scan.
- Wait **30–60 minutes**.

5. Review the Report

- Once done, open the report.
- You'll see vulnerabilities categorized by severity:
  - **Critical**, **High**, **Medium**, **Low**, **Info**
- Click on each to see:
  - Description
  - CVSS score
  - How to fix (solution or patch)

6. Take Screenshots & Save Report

- Take screenshots of:
  - Dashboard
  - Top vulnerabilities
  - Details of 1–2 critical ones

Optional by OpenVAS

Works best on **Kali Linux** or **Ubuntu**. More complex setup than Nessus.

Basic Setup Steps:

1. Install OpenVAS (Now called Greenbone)

In command shell enter the command

sudo apt update
sudo apt install openvas
sudo gvm-setup
sudo gvm-check-setup

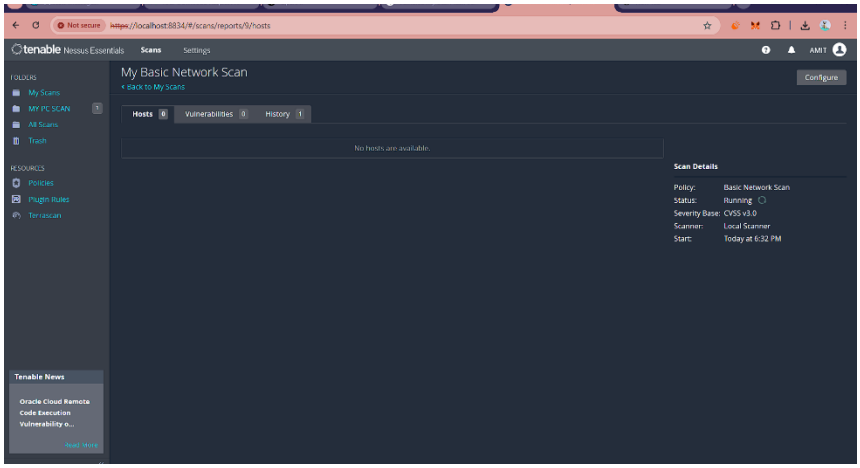
2. Start Services

sudo gvm-start

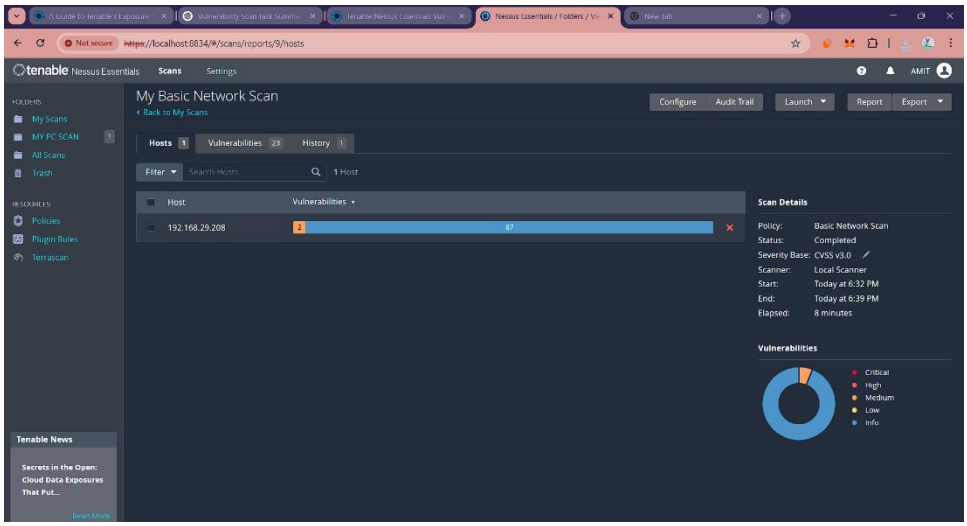
3. Access Web UI
   - Go to: https://127.0.0.1:9392
   - Login with the username and password shown after setup
4. Run a Scan
   - Create a new scan target (127.0.0.1 or local IP)
   - Start a full scan

- Review report after 30–60 minutes

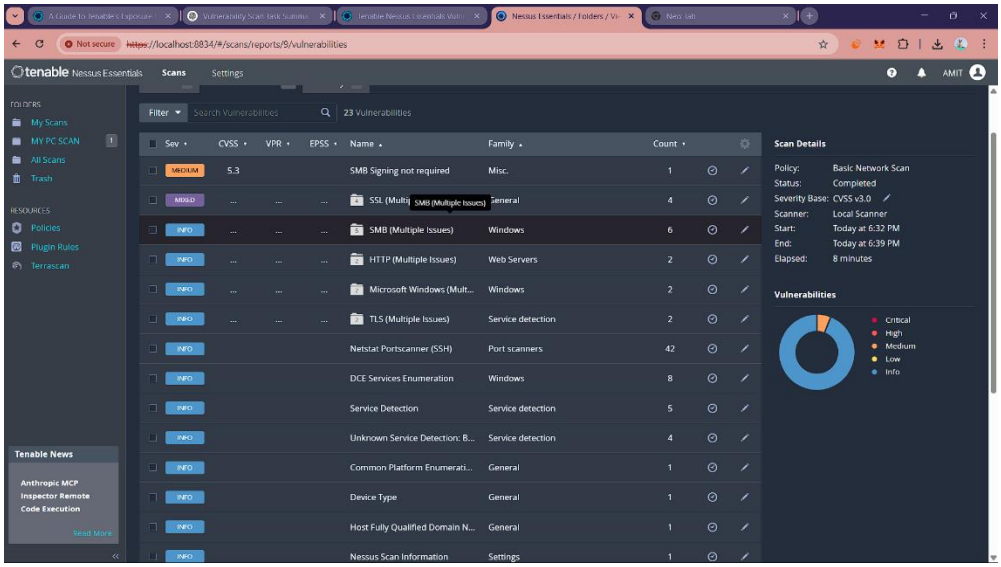
Screen shot of the report generated by my scan



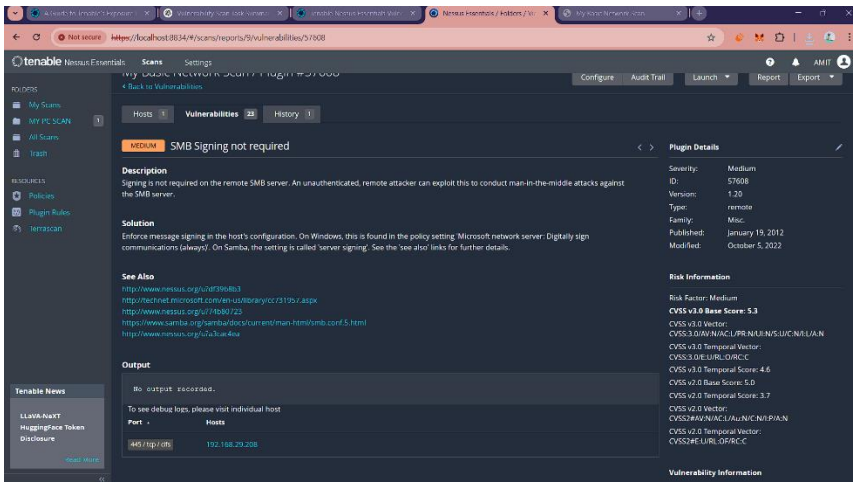
This fig shows the home screen of Nessus essential



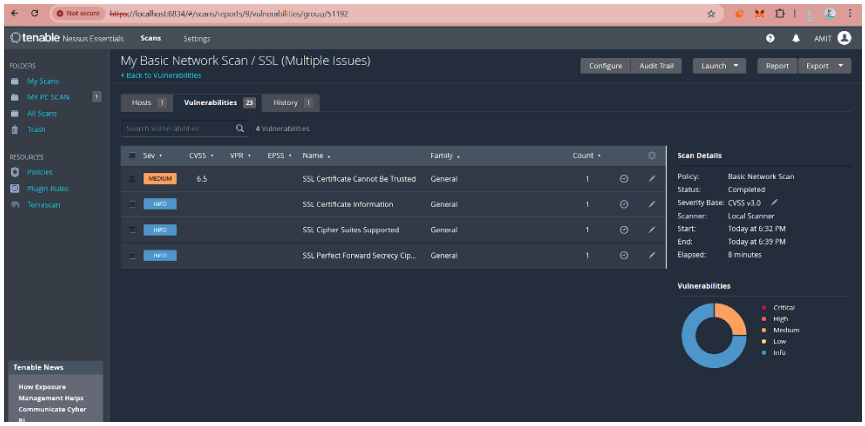
This figure shows that the scan is completed



This figure shows the result of the vulnerability found in the system



This figure explain the vulnerability that was showing in the system by Nessus essential



This figure shows that the other vulnerability that found in the system

Now I will explain all the vulneribity that are found in my system and how attackers exploit them to use them, and after that, the remediation steps to patch those vulnerabilities.

1. SSL Certificate Cannot Be Trusted (Plugin ID: 51192)

- **Severity**: Medium
- **Description**: The server is using an SSL certificate that is not trusted. This can happen if the certificate is self-signed or issued by an unknown CA.
- **Exploit Risk**: Attackers can perform *Man-in-the-Middle (MitM)* attacks, intercepting and modifying traffic between the user and server.

- **Fix**: Install a certificate from a trusted Certificate Authority (CA) and ensure the full certificate chain is presented.

2. SMB Signing Not Required (Plugin ID: 57608)

- **Severity**: Medium
- **Description**: SMB message signing is not required. This leaves the system vulnerable to *relay attacks*.
- **Exploit Risk**: Attackers can intercept SMB traffic and potentially inject malicious commands or redirect sessions.
- **Fix**: Enable SMB signing in the Windows registry or group policy:
  - Registry Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters
  - Set EnableSecuritySignature and RequireSecuritySignature to 1.

3. Windows NetBIOS / SMB Information Disclosure (Plugin ID: 10150)

- **Severity**: Low
- **Description**: Remote host discloses NetBIOS name, domain, and other information.
- **Exploit Risk**: Useful in reconnaissance; attackers can map internal networks and perform targeted attacks.
- **Fix**: Disable NetBIOS over TCP/IP if not needed.

4. Microsoft Windows SMB NativeLanManager Information Disclosure (Plugin ID: 10785)

- **Severity**: Low
- **Description**: The system exposes its OS version and domain via SMB.
- **Exploit Risk**: Enables targeted attacks using known exploits for specific OS versions.
- **Fix**: Apply latest Windows security updates and restrict SMB access via firewall.

5. OS Security Patch Assessment Not Available (Plugin ID: 117886)

- **Severity**: Informational

- **Description**: Nessus could not determine if the system is missing patches.
- **Exploit Risk**: Unknown vulnerabilities may exist if patches are missing.
- **Fix**:
    - Provide valid credentials to enable patch checks.
    - Ensure remote OS supports patch detection (may not work over SSH for Windows).

6. Service Detection Issues / Unrecognized Banners (Plugin IDs: 22964, 11154)

- **Severity**: Informational
- **Description**: Nessus identified unknown or uncommon services running.
- **Exploit Risk**: These may include outdated or misconfigured services vulnerable to attack.
- **Fix**: Review the list of running services. Disable unnecessary or unknown services.

Recommendations Summary:

Vulnerability	Risk	Exploit Method	Remediation
SSL Certificate Untrusted	Medium	Man-in-the-Middle (MitM)	Use valid, trusted SSL certificates
SMB Signing Not Required	Medium	SMB Relay	Enable SMB signing via registry or GPO
NetBIOS/SMB Info Disclosure	Low	Reconnaissance	Disable NetBIOS over TCP/IP if unused
SMB NativeLanManager Info Disclosure	Low	Targeted Exploits	Patch Windows and restrict SMB access

Patch Assessment Not Available	Info	Potential Patch Gaps	Run scan with credentials and check OS support
Unknown/Uncommon Services Detected	Info	Potential Zero-day Vectors	Audit and disable unnecessary services