**TITLE**

Perform a Basic Vulnerability Scan on Your PC

Objective

To perform a basic vulnerability assessment on a personal computer using Nessus Essentials, a free vulnerability scanning tool, and document the discovered vulnerabilities and their severity levels.

**Setup Process**

**Step 1: Install Nessus Essentials**

1. Registered at: https://www.tenable.com/products/nessus/nessus-essentials
2. Received activation code via email.
3. Downloaded and installed Nessus on Windows 10.
4. Accessed Nessus via: https://localhost:8834
5. Activated using the provided key and created a login account.

**Scan Configuration**

**Scan Type:**

* **Basic Network Scan**

**Target:**

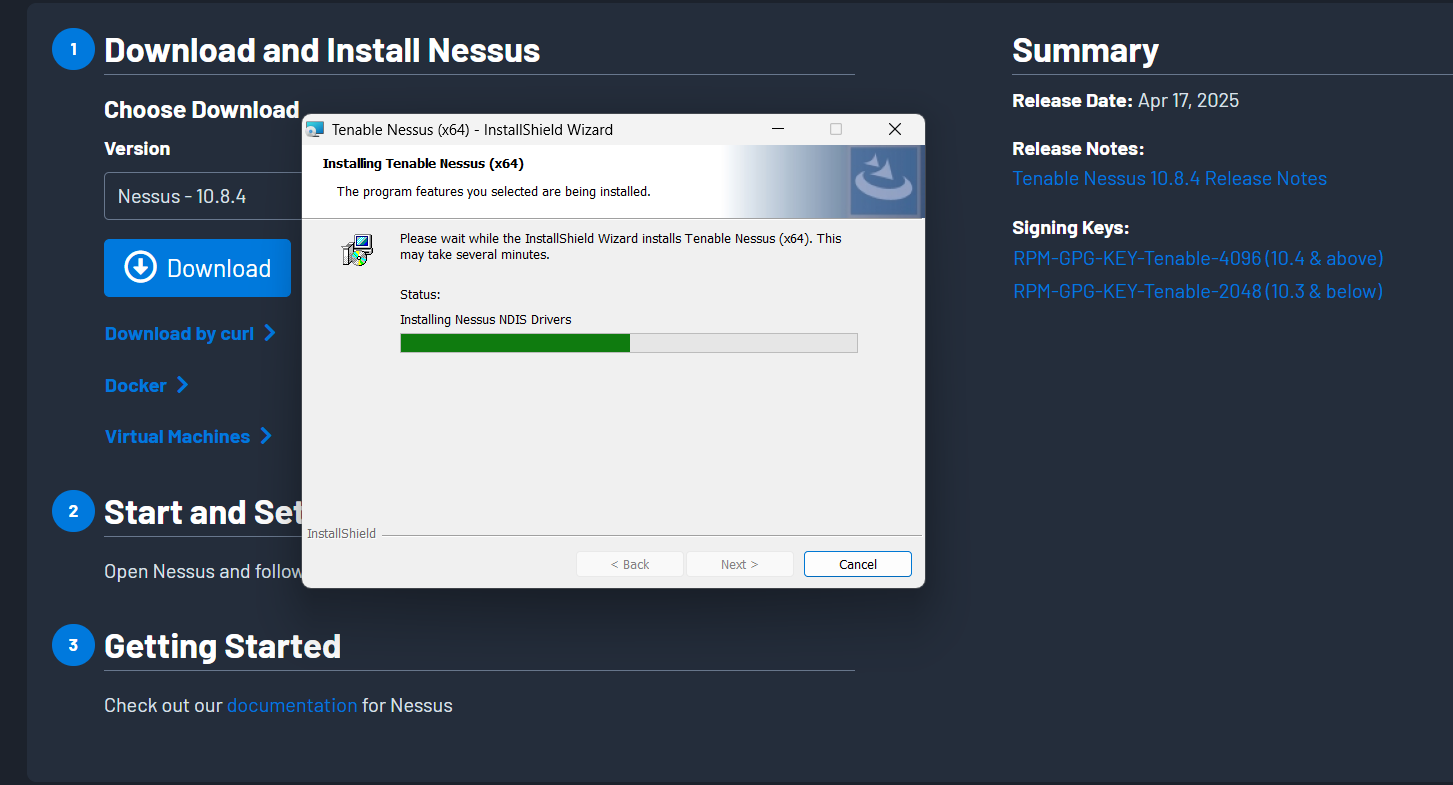
* **127.0.0.1** (localhost) — the loopback IP for scanning my own PC.

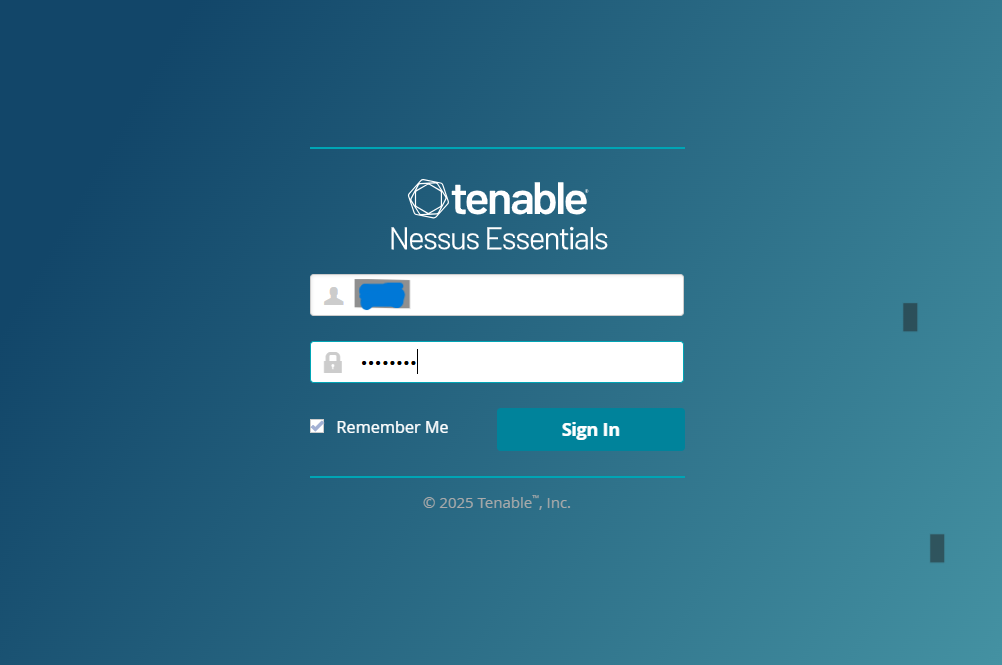
**Steps:**

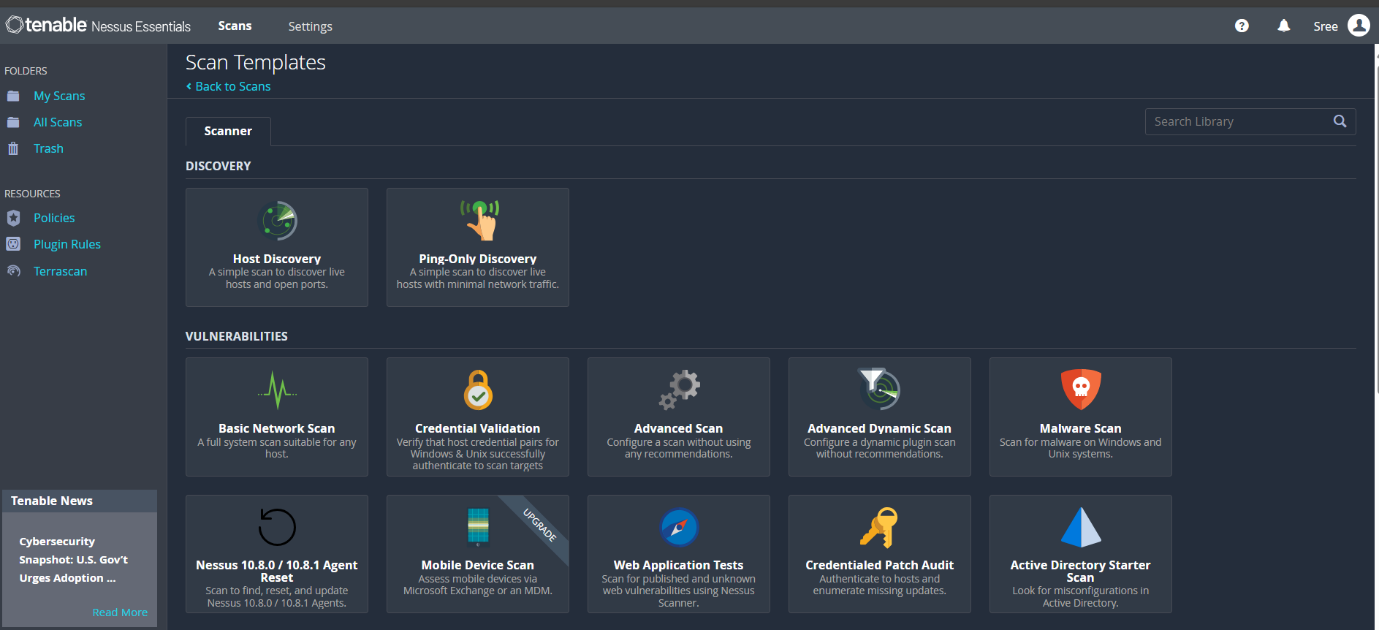
1. Clicked **New Scan** → Selected **Basic Network Scan**.
2. Named the scan: Local Machine Scan
3. Entered target as 127.0.0.1
4. Clicked **Save**, then **Launch**.

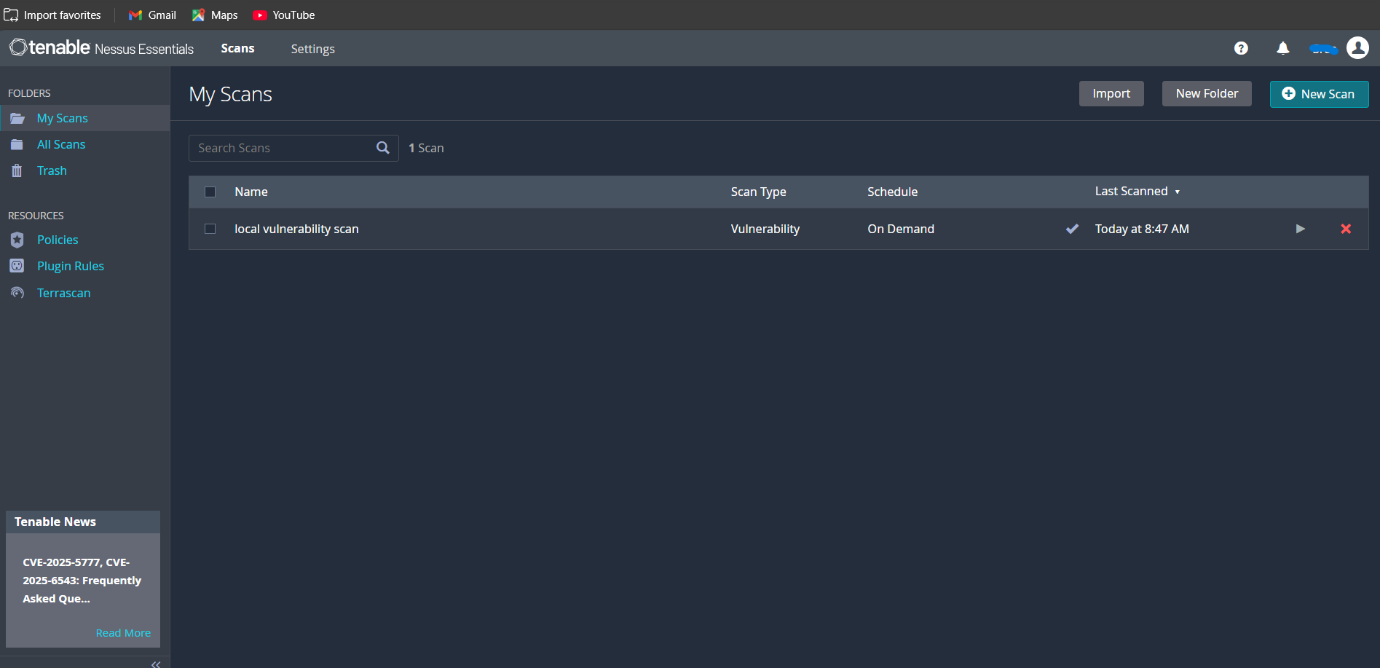
**5. Scan Execution**

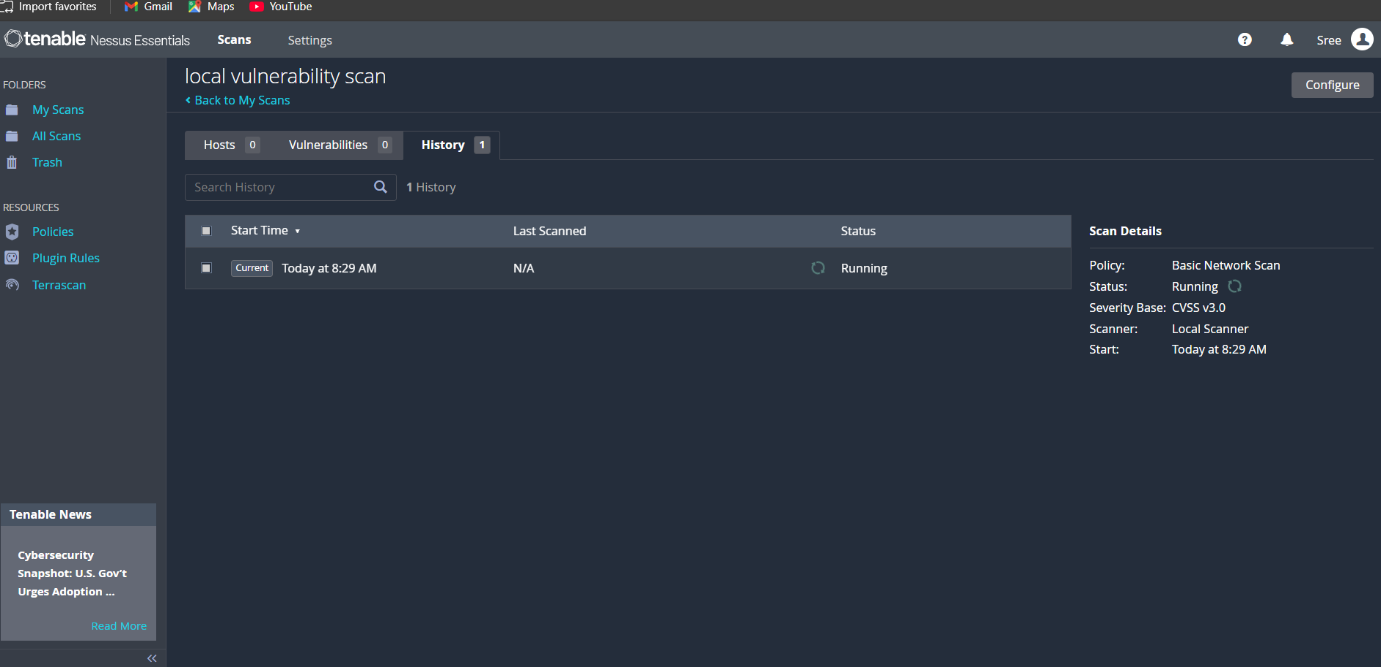
* The scan took approximately **30–40 minutes**.
* Nessus discovered **open ports, running services, and vulnerabilities**.
* Results were categorized by severity: **Critical**, **High**, **Medium**, **Low**, and **Info**.

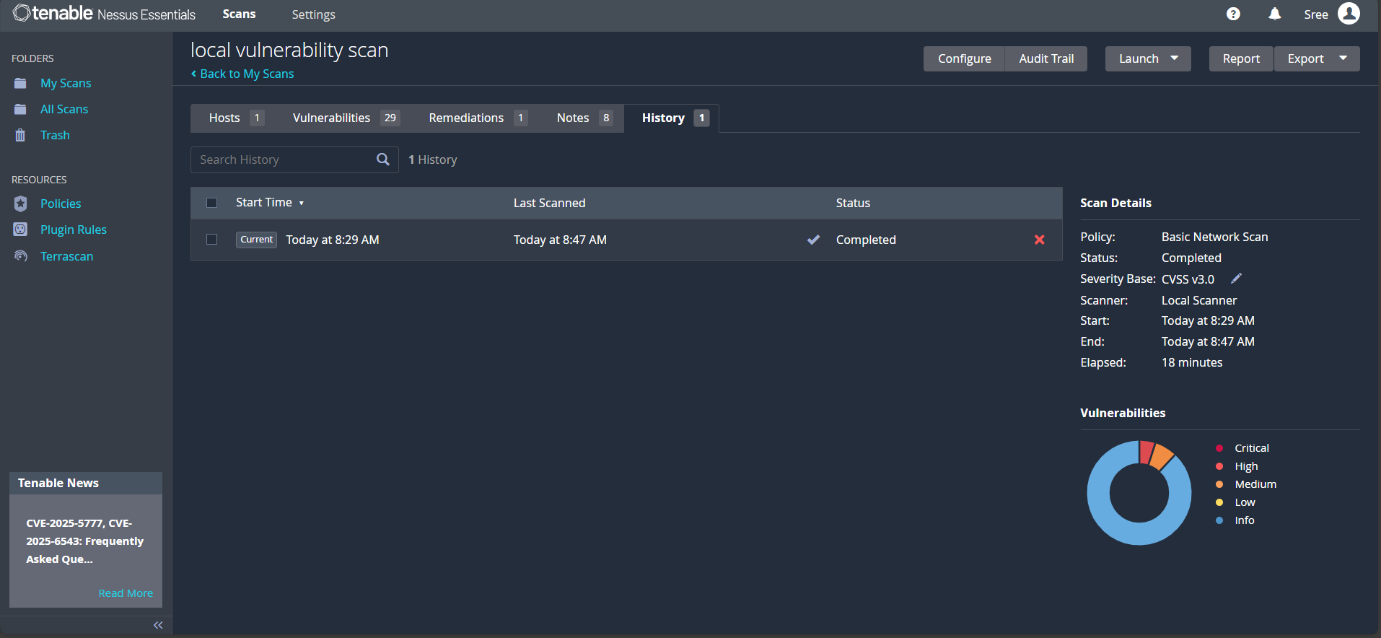












**Conclusion**

* Successfully scanned the local machine using **Nessus Essentials**.
* Identified several critical and high-severity vulnerabilities.
* Gained hands-on experience with network scanning and security assessment.
* Recommended immediate patching, disabling outdated protocols, and updating Windows components.