Task 3 : Perform a Basic Vulnerability Scan on Your PC

**Objective**: Use free tools to identify common vulnerabilities on your computer.

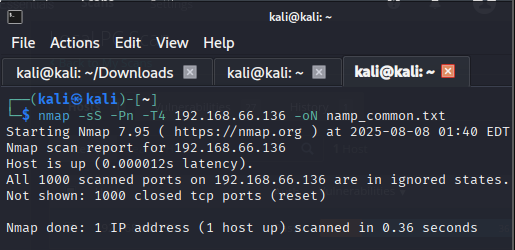
**Tools**: OpenVAS Community Edition (free vulnerability scanner) or Nessus Essentials.

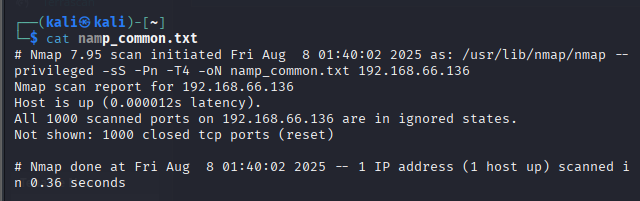
**Deliverables**: Vulnerability scan report with identified issues.

Step by Step Basic Vulnerability Scan

Step – 1 : **Quick reconnaissance (recommended before full vuln scan)**

Run a quick port/service discovery to understand what’s running:



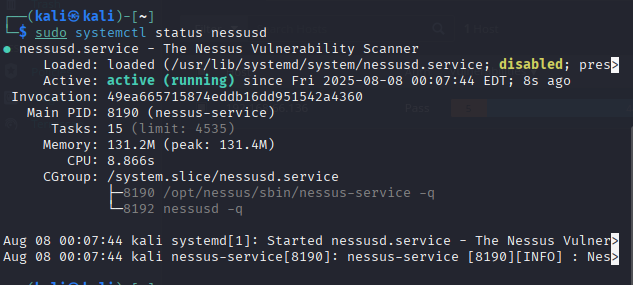


**Why:** vulnerability scanners check services — knowing open ports helps tailor scans and reduces noise.

**Note:** -Pn disables ping host discovery (useful on localhost).

Step – 2 : Nessus Essentials (step-by-step)

Install tool in kali machine and start tool

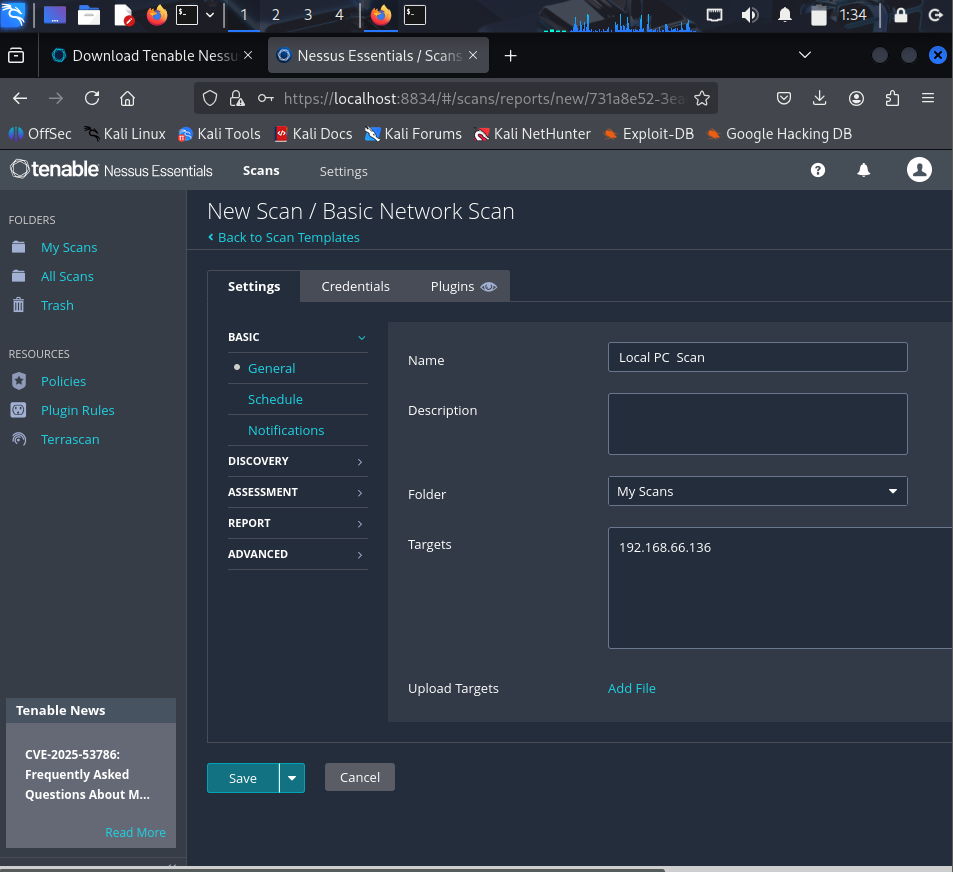


**Initial configuration**

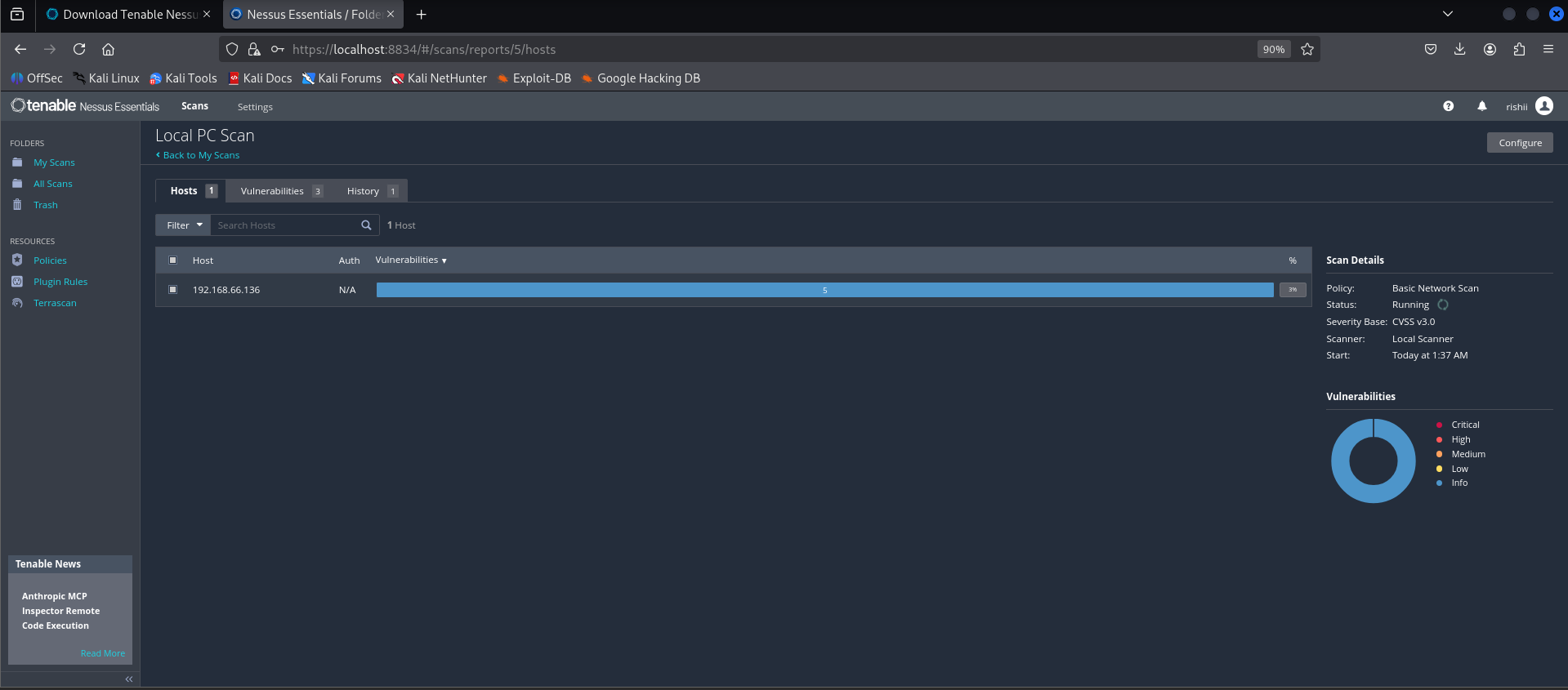
1. Open browser → https://localhost:8834 (Nessus UI).
2. Follow setup: create admin user, paste activation code, wait for plugins to update.

**Create & run a scan**

1. In UI → **Scans** → **New Scan** → choose **Basic Network Scan** (or template).
2. Name it: Local PC Scan.
3. **Targets**: enter 127.0.0.1, localhost *or* your local IP 192.168….



1. Save → **Run**.
2. Monitor progress in UI. When finished, open the results.
3. Wait for Scan complete.



Step – 3 : **Credentialed vs non-credentialed scans (why it matters)**

* **Non-credentialed** checks services remotely — you'll see open ports and some vulnerabilities.
* **Credentialed** (provide admin/SSH credentials) allows the scanner to log into the host and check installed packages, missing patches, configuration issues — *much more accurate and complete*. Use credentials only on machines you own or manage.

Step – 4 : Interpreting results (what to look for)

Most scanners show vulnerabilities with severity tiers — Critical / High / Medium / Low / Info and CVSS scores.

Prioritization checklist

1. Critical/High vulnerabilities — start here (e.g., RCE, remote code execution, critical CVEs).
2. Exposed services (RDP, SMB, web admin panels) — if not needed, disable or firewall them.
3. Missing OS patches — install updates/patches.
4. Default/weak credentials — change passwords, enable strong auth.
5. Unencrypted services — switch to TLS or block access.
6. High CVSS with public exploits — urgent remediation or isolation.

Report fields to capture (for each finding):

* Vulnerability ID / Name (e.g., CVE-XXXX-YYYY)
* Severity & CVSS score
* Affected service/port (e.g., ssh on port 22)
* Evidence (screenshot, scanner output lines)
* Remediation (patch, configuration change, disable service)
* Status after fix (open/closed/mitigated)

**Example common vulnerabilities & simple mitigations**

* **Missing OS updates** → Run OS update (Windows Update / sudo apt update && sudo apt upgrade)
* **RDP open to Internet** → Block on firewall, enable Network Level Authentication (NLA), restrict to VPN only.
* **SMBv1 enabled** → Disable SMBv1, enable SMBv2/3.
* **Weak SSH config** → disable password auth, use key-based auth, change port if desired, enforce strong ciphers.
* **Unpatched browser/plugins** → update or remove plugin.
* **Default credentials** → change immediately; implement account lockout.
* **Open admin panels** → restrict by firewall / IP allowlist or place behind VPN.

Last Step : show your Vulnerability reports 