**Perform a Basic Vulnerability Scan on Your PC (Tenable Nessus Essentials)**

1. **Install Nessus Essentials**

**Download** Nessus Essentials from Tenable

* Register With Email ID for Trial (Activation Code)

Kali CLI — install & start Nessus

* **Install** the Nessus DEB package

$sudo dpkg -i Nessus-10.9.4-ubuntu1604\_amd64.deb

* **Start** and enable the Nessus

$ sudo systemctl start nessusd.service

#sudo systemctl enable nessusd.service

A screenshot of a computer

AI-generated content may be incorrect.

1. **Access Nessus on Browser**

Open a **browser on the Kali machine** and type:

* <https://localhost:8834/>

Activate and doA screenshot of a computer

AI-generated content may be incorrect.wnload the plugins.

1. **Create a target & run a scan**

After you log in:

1. **Scans → New Scan** (upper-right)
2. From the **Scan Templates** page choose **Basic Network Scan** (recommended for a first, full scan).

A screenshot of a computer

AI-generated content may be incorrect.

1. Configure the new scan:
   * **Name:** Localhost - Basic Scan
   * **Targets:** 127.0.0.1 to scan local machine; or your LAN IP like 192.168.1.100 if scanning from Kali to another host.
   * (Optional) **Credentials** tab: add SSH credentials for a credentialed Linux scan (this gives deeper checks). *Only add credentials you own.*
   * (Optional) *Plugins / Port Scanning / Advanced options* — accept defaults for first run.
2. **Save** then **Launch** the scan.
3. Monitor progress on **Scans → My Scans**. Click the running job to view live progress and counts.

A screenshot of a computer

AI-generated content may be incorrect.

**Timing:** First full scan of a single host typically **~30–60 minutes**, depending on scan depth and system resources.

1. **View results & export report**

When the scan completes:

1. Open the completed scan result (Scans → click scan name).
2. Explore Vulnerabilities.

A screenshot of a computer

AI-generated content may be incorrect.

1. To export: click **Export** (upper-right of scan results) → choose **Nessus (.nessus)**. Save the file to your Kali ~/Documents or ~/Downloads or repo folder.

A screenshot of a computer

AI-generated content may be incorrect.

1. **Interpreting results & basic remediation commands (Kali examples)**

For each *Critical / High* item, record:

* vulnerability name, CVE(s), evidence, affected package/service, and remediation steps.

Common fixes (Commands)

1. Update all packages (fixes many outdated software issues)

$sudo apt update && sudo apt full-upgrade -y

2. Check open/listening ports (see what Nessus may have flagged)

$sudo ss -tulpen

3. Stop & disable unnecessary service (example: ftp)

$sudo systemctl stop vsftpd.service

$sudo systemctl disable vsftpd.service

4. Harden SSH (example: disable password auth if using keys)

$sudo sed -i 's/^#PasswordAuthentication yes/PasswordAuthentication no/' /etc/ssh/sshd\_config

$sudo systemctl restart sshd

5. Reboot after large kernel / core updates

$sudo reboot