🛠️ Mini Guide: Vulnerability Scanning Using OpenVAS or Nessus Essentials

✅ Step-by-Step Instructions

1. Install OpenVAS or Nessus Essentials

🔹 For OpenVAS (Kali Linux):

bash

Copy

Edit

sudo apt update

sudo apt install openvas

sudo gvm-setup

Then start the service:

bash

Copy

Edit

sudo gvm-start

Login URL: https://127.0.0.1:9392

Default user: admin

🔹 For Nessus Essentials:

Go to https://www.tenable.com/products/nessus/nessus-essentials

Register with email to get activation code.

Download and install:

bash

Copy

Edit

sudo dpkg -i Nessus-\*.deb

sudo systemctl start nessusd

Open in browser: https://localhost:8834

2. Set up Scan Target

Use your local IP:

bash

Copy

Edit

ip a

Or just use:

Copy

Edit

127.0.0.1

Create a new scan, name it “Localhost Scan”, and set target as your IP.

3. Start a Full Vulnerability Scan

In OpenVAS: Go to Scans > Tasks > New Task > Full and fast scan

In Nessus: Create a new Basic Network Scan, select target IP.

4. Wait for Scan to Complete

⏳ This may take 30–60 minutes. Do not close browser window.

5. Review the Report

Go to Scans > Reports > Select Scan

Look for:

High / Critical risks

CVEs (Common Vulnerabilities and Exposures)

Services with weak configurations

6. Research Fixes or Mitigations

Use CVE details to search online:

https://nvd.nist.gov/

https://cve.mitre.org/

Search for Linux hardening guides

7. Document Critical Vulnerabilities

For each critical vulnerability:

Take note of CVE ID, Risk, Affected Service, and Fix Recommendation

8. Take Screenshots

Use PrtSc or Linux gnome-screenshot, or spectacle in KDE.

Screens to include:

Dashboard

Scan summary

Critical findings

A detailed vulnerability view

