Let me walk you step-by-step on how to actually run this **smart scanner + CVE reporter with exploitability checks** on your Kali Linux machine.

# 🔹 Step 1: Install requirements

First, make sure your system has the dependencies:

sudo apt update && sudo apt install -y nmap nikto gobuster exploitdb python3-pip jq

pip3 install nvdlib

This installs:

* **nmap** → scanning
* **nikto** → web vuln scanner
* **gobuster** → directory brute-forcer
* **exploitdb** (includes searchsploit) → exploit lookup
* **nvdlib** → NVD API library
* **jq** → JSON parsing helper (if needed later)

# 🔹 Step 2: Create the scanner files

Create a working directory (e.g., vulnscanner):

mkdir ~/vulnscanner && cd ~/vulnscanner

### Save the ****Bash wrapper**** (cve\_reporter.sh):

nano cve\_reporter.sh

Paste the bash script I gave you.  
Then make it executable:

chmod +x cve\_reporter.sh

### Save the ****Python CVE fetcher**** (cve\_fetcher.py):

nano cve\_fetcher.py

Paste the Python code (the smarter one with CVSS, CWE, remediation, and exploit checks).  
Make it executable:

chmod +x cve\_fetcher.py

# 🔹 Step 3: Update exploit database

ExploitDB is updated frequently. Run:

searchsploit -u

# 🔹 Step 4: Run the tool on a target

For example, if you want to scan testphp.vulnweb.com (a legal DVWA test site):

./cve\_reporter.sh testphp.vulnweb.com

# 🔹 Step 5: Check results

Inside scan\_results\_testphp.vulnweb.com/ you’ll find:

* nmap.txt → standard nmap scan
* nmap\_vuln\_exploit.txt → vuln & exploit scan results
* cve\_ids.txt → raw extracted CVEs
* cve\_report.txt → 🔥 full report with:
  + CVE descriptions
  + CVSS scores + severity
  + CWE references
  + Remediation guidance
  + Exploit status (Metasploit/ExploitDB links if available)

# 🔹 Step 6: (Optional) Customize reporting

If you want prettier reports, you could:

* Pipe results into **Markdown** for GitHub-style viewing.
* Convert to **PDF** with pandoc.
* Add **colorized output** in the terminal with Python’s rich module.

⚠️ **Reminder**: Only scan systems you **own** or have **explicit permission** to test (e.g., Metasploitable, DVWA, bWAPP, VulnHub VMs, or your own servers).