**🔍 OpenVAS (GVM) Professional Cheat Sheet**

OpenVAS (now part of **Greenbone Vulnerability Management**) is a **vulnerability scanner** used to find security issues on systems, networks, and web apps.

**📌 1. Installation & Setup**

**On Kali Linux**

sudo apt update

sudo apt install openvas -y

**Initialize & Setup**

gvm-setup # Initializes OpenVAS/GVM

gvm-check-setup # Verify setup is complete

**Start Services**

gvm-start # Start GVM services

gvm-stop # Stop GVM services

Default Web UI:

https://127.0.0.1:9392

**📌 2. Basic Usage (Web UI)**

* **Login:** Default admin user created at setup (password shown in terminal).
* **Scan Wizard:** Quick scans with minimal config.
* **Tasks:** Custom scan targets with fine-tuned options.
* **Reports:** Detailed scan findings, CVSS scores, remediation steps.

**📌 3. CLI Tools**

**Create a Target**

gvm-cli --gmp-username admin --gmp-password 'yourpassword' socket --xml "<create\_target><name>TestTarget</name><hosts>192.168.1.10</hosts></create\_target>"

**Start a Task (Scan)**

gvm-cli --gmp-username admin --gmp-password 'yourpassword' socket --xml "<create\_task><name>QuickScan</name><config id='daba56c8-73ec-11df-a475-002264764cea'/><target id='TARGET-ID-HERE'/></create\_task>"

**Launch Task**

gvm-cli --gmp-username admin --gmp-password 'yourpassword' socket --xml "<start\_task task\_id='TASK-ID-HERE'/>"

**📌 4. Common Scan Configs**

| **Config** | **ID** | **Purpose** |
| --- | --- | --- |
| Full and fast | daba56c8-73ec-11df-a475-002264764cea | Quick, optimized scan |
| Full and very deep | 6c248850-1f62-11e1-b082-406186ea4fc5 | Aggressive, deeper scan |
| Host discovery | 2d3f051c-55ba-11e3-bf43-406186ea4fc5 | Detect live hosts only |
| System Discovery | bbca7412-a950-11e3-9109-406186ea4fc5 | OS/Service fingerprinting |

**📌 5. Useful Commands**

**Update NVT (Vulnerability Feed)**

greenbone-nvt-sync

**Check Sync Status**

gvm-check-setup

**Restart Scanner**

gvm-stop && gvm-start

**📌 6. Reports**

**Export Report (XML)**

gvm-cli --gmp-username admin --gmp-password 'yourpassword' socket --xml "<get\_reports report\_id='REPORT-ID-HERE' format\_id='a994b278-1f62-11e1-96ac-406186ea4fc5'/>"

**Common Formats**

* **XML** – machine parsing
* **PDF/HTML** – presentation-ready
* **CSV** – for Excel analysis

**📌 7. Pro Tips**

* Use **"Full and fast"** for initial scans; switch to **"Deep"** if needed.
* Run **host discovery first** before full scans to save time.
* Automate with **cron jobs** for regular vulnerability reports.
* Always **update NVT feeds daily**.
* Export reports for documentation/compliance.
* Integrate with **SIEM / SOC pipelines** for enterprise monitoring.

**📌 8. Advanced Usage**

* **Credentialed Scans** → Add SSH/SMB credentials for deeper vulnerability checks.
* **Port Lists** → Customize open port detection (TCP/UDP).
* **Alerts & Notifications** → Auto-email scan reports.
* **SLAs & Compliance** → Use scan configs aligned with CIS/NIST benchmarks.