**OpenVAS / Nessus Essentials — Setup, Scan & Report**

**Definition — quick overview**  
OpenVAS (now part of GVM) and Nessus Essentials are vulnerability scanners. They automatically probe systems and networks to find security weaknesses — unpatched software, misconfigurations, weak/default credentials, open services, and other potential attack vectors. OpenVAS/GVM is open-source and free; Nessus Essentials is free for learning/personal use.

**Purpose**

Use these tools to automatically detect and prioritise vulnerabilities so you can fix the most dangerous issues first and make systems harder to attack.

**Setup — OpenVAS / GVM (Kali example)**

1. Install the package:  
   sudo apt install gvm
2. Initialize and sync feeds (this downloads the vulnerability tests): follow the initialization steps your distro provides (e.g., gvm-setup or gvm-manage-certs where applicable).
3. Start the GVM services:  
   sudo gvm-start
4. Open the web interface (Greenbone Security Assistant) in your browser:  
   https://127.0.0.1:9392
5. Create or use an existing user to log in.

Notes: initialization can take time while feeds download. On Kali the install/initialization commands may vary slightly depending on the package version — but the flow is the same: install → initialize/sync feeds → start services → log in.

**Practice scan — Metasploitable2 (example)**

**Target details**

* Name: Metasploitable2
* IP: **192.168.225.85** (host-only network)

**Steps**

1. Log into GSA (Greenbone Security Assistant).
2. Add the target with the IP above.
3. Create a scan task and choose the target.
4. Select a scan profile — for practice use **Full and Fast** (good balance of depth and speed).
5. Start the scan.

What happens: the scanner sends probes and tests (NVTs) to the target and reports findings automatically.

**What the scanner detects (examples)**

* Outdated/unpatched services (e.g., old Apache or FTP versions)
* Default/weak credentials and login issues
* Open ports and misconfigurations that expose services unnecessarily
* Vulnerable web apps (DVWA, old CMS, etc.)
* Known backdoors and high-risk CVEs

**Reading the vulnerability report**

After the scan completes, GVM/OpenVAS produces a report you can export (PDF/HTML/XML). Key parts:

* **Target IP:** e.g., **192.168.225.85**
* **Vulnerability name:** e.g., vsftpd 2.3.4 backdoor
* **Severity:** Critical / High / Medium / Low
* **Affected service/port:** e.g., FTP on port 21, HTTP on port 80
* **Description:** Short explanation of the issue and how it works
* **Solution / Mitigation:** Practical steps — patch, change config, disable service, or tighten access controls

**Severity — how to prioritise**

* **Critical:** Immediate danger — often simple to exploit and can give full compromise. Fix right away.
* **High:** Serious issue. Attackers could exploit under common conditions — schedule rapid remediation.
* **Medium:** Moderate risk — may require specific conditions or user interaction. Plan and patch.
* **Low:** Informational or unlikely to be exploited. Track, and fix when convenient.

**Deliverable — what your OpenVAS report should show**

When you export the PDF report after scanning the Metasploitable2 VM, it should clearly include:

* The **target IP**: **192.168.225.85**
* A list of vulnerabilities discovered, each with severity (Critical → Low)
* Affected services and port numbers (so the ops team knows where to act)
* Concise descriptions and concrete remediation steps for each finding
* A summary that prioritises actions (e.g., “Patch Apache on port 80 — Critical”)

Why this matters: the report proves you scanned the target, correctly identified and classified vulnerabilities, and provided actionable mitigation steps — exactly what’s expected for Task 2 Step 3 or any hands-on assessment.

**Export formats**

GVM/OpenVAS supports export to **PDF**, **HTML**, and **XML**. For submission or audits, PDF is the most common choice.

**Final summary (human, plain)**

* OpenVAS and Nessus Essentials are automated vulnerability scanners used in security testing and hardening.
* Install and initialise OpenVAS/GVM, start the service, and log into the Greenbone web UI.
* Add **Metasploitable2** as a target with IP **192.168.225.85**, run a Full and Fast scan, and export the PDF report.
* Use the report to prioritise fixes by severity (Critical → Low) and include clear remediation steps.
* This demonstrates practical scanning skills and produces a deliverable suitable for blue-team/red-team learning or coursework.