DevOpsSchool

Course curriculum · November 2026

LEVEL 03 OF 04 · INTERMEDIATE

OpenVAS Intermediate Training

Automate Greenbone through GMP and Python, integrate findings with pipelines and ticketing, and tune and troubleshoot the scanner.

LIVE ONLINE **Max 8-10 hours**	CORPORATE (DAY-WISE) **3 days · Days 1-3**	SELF-PACED VIDEO **1-year LMS access**
BATCH SIZE **Max 10 learners**	NEXT BATCHES **1st of every month · weekends: first Saturday**	CERTIFICATE **Verifiable certificate of completion**

Foundation	Essential	Intermediate	Advanced
1 day · Included	2 days · Included	3 days · This curriculum	5 days · Next step

INSIDE THIS CURRICULUM

What you will achieve	Outcomes and level focus
Who should attend	Audience and prerequisites
Agenda	35 topics · Foundation to Intermediate
Hands-on labs	3 labs
Formats and fees	Live, 1:1, self-paced, corporate
Trainer and reviews	Rajesh Kumar
Enrolment	Batches, payment, contacts

WHY DEVOPSSCHOOL

- Rated 4.6 on Google
- 1,500+ verifiable certificates issued in the public registry
- Trainer Rajesh Kumar: 20 years in industry
- Small batches: max 10 learners, every session recorded

Course page: www.devopsschool.com/courses/openvas/openvas-and-intermediate-training.html
Talk to us: WhatsApp +91 99057 40781 · +1 (469) 756-6329 · contact@DevOpsSchool.com · reply within 1 hour

OUTCOMES

What you will achieve

By the end of the OpenVAS course path, you will be able to:

1

Scan infrastructure accurately

Run authenticated OpenVAS scans and interpret findings with severity and detection quality.

2

Automate vulnerability workflows

Schedule, script and integrate scans with pipelines, ticketing and reporting.

3

Lead vulnerability management

Prioritise risk and run a measurable remediation programme across the organisation.

WHAT THE INTERMEDIATE LEVEL ADDS

Automation, integrations, tuning and troubleshooting

Hands-on: Automate scanning with python-gvm. Write a python-gvm script that creates targets and tasks, runs a scan after a staging deploy and opens tickets for high-severity findings.

WHO SHOULD ATTEND

- Regular OpenVAS users who want to automate, integrate and manage it at a deeper level.
- Specialists who support OpenVAS for colleagues or customers.
- Leads preparing OpenVAS for wider use across projects.

BEFORE YOU START

- The Essential level, or equivalent hands-on experience.
- You can already: Configure accurate authenticated scans, schedule them with alerts and manage results, overrides and remediation tracking.
- Basic computer skills and a laptop with a stable internet connection for the live sessions and labs.
- This curriculum includes every earlier level, so it is complete on its own.

AGENDA · FOUNDATION TO INTERMEDIATE

OpenVAS Intermediate Training agenda

35 topics. Each level builds on the one before it, so this curriculum lists every earlier level in full. Days are for corporate (day-wise) delivery; live online batches cover the same agenda in max 8-10 hours.

DAY 1 — Foundation: Vulnerability scanning concepts and Greenbone setup

Included from Foundation

1. Vulnerability management basics: vulnerabilities, CVEs, CVSS scores and scanning versus penetration testing
2. OpenVAS and Greenbone: origins as a Nessus fork, the Greenbone Community Edition and commercial editions
3. Architecture: openvas-scanner, ospd-openvas, Greenbone Vulnerability Manager (gvmd), GSA web UI and Notus
4. Supporting services: PostgreSQL for gvmd data and Redis for scanner knowledge bases
5. Feeds: the Greenbone Community Feed with NVTs, SCAP, CERT advisories and feed sync status
6. Installation: Greenbone Community Containers with Docker Compose or Kali packages with gvm-setup
7. First login: the Greenbone Security Assistant dashboard and creating users with gvmd --create-user
8. Legal and ethical scanning: written authorisation, scope agreements and scanning windows
9. Targets and port lists: hosts, ranges, exclusions and port list selection
10. First scan: the Task Wizard, the Full and fast scan config and monitoring a running task
11. Reading results: severity, Quality of Detection (QoD), solution types, CVE references and report export

DAY 2 — Essential: Scan configuration, authenticated scans and reporting

Included from Essential

12. Scan configs: Full and fast, discovery configs and custom configs with selected NVT families
13. Authenticated scans: SSH key or password, SMB for Windows, ESXi and SNMP credentials
14. Local security checks with Notus: package-based detection on Linux hosts
15. Alive tests and discovery: ICMP, TCP-ACK and ARP pings and the consider-alive option
16. Scheduling: recurring scans, scan windows and schedules in GSA
17. Alerts: email, SCP, SMB, syslog and HTTP alerts on task completion or severity changes
18. Result management: overrides, notes, false positives and severity adjustments
19. Asset inventory: hosts, operating systems and TLS certificates discovered by scans
20. Report filters and delta reports: comparing scans and exporting CSV for spreadsheets
21. Remediation workflow: tickets in GSA, assignment and verification rescans
22. Web servers: what OpenVAS checks on web services and where dedicated DAST tools fit
23. Access control: users, roles, groups and permissions in GSA

DAY 3 — Intermediate: Automation, integrations, tuning and troubleshooting

New at this level

24. Greenbone Management Protocol (GMP): gvm-cli and gvm-tools scripts
25. python-gvm: automating targets, tasks, schedules and report retrieval from Python
26. Scan performance tuning: maximum concurrent hosts and checks, scanner preferences and network impact
27. Compliance policies: policy audits from the feed and compliance reports
28. Integrations: exporting findings to Jira, Splunk or Elastic through scripts and report formats
29. CI/CD integration: scanning staging hosts after deploy and failing on severity thresholds
30. Cloud and container hosts: scanning cloud VMs, scanner network rules and Trivy for container images

31. Service operations: greenbone-feed-sync, gvmd and ospd-openvas logs and service health
32. Securing the scanner: TLS for GSA, hardening the scanner host and protecting stored credentials
33. Troubleshooting: feeds not loading, interrupted scans and Redis or socket errors
34. Scanner placement: segmented networks, firewalls and remote OSP scanners
35. Custom checks: NASL script basics and loading custom vulnerability tests

PRACTICE

Hands-on labs

You build these yourself during the course, guided by the trainer.

FOUNDATION

Run your first vulnerability scan

Deploy Greenbone Community Containers, sync the feeds, scan a deliberately vulnerable lab host and export a PDF report.

ESSENTIAL

Run authenticated scans with alerting

Scan Linux and Windows lab hosts with credentials, schedule a weekly rescan with email alerts and compare results with a delta report.

INTERMEDIATE

Automate scanning with python-gvm

Write a python-gvm script that creates targets and tasks, runs a scan after a staging deploy and opens tickets for high-severity findings.

HOW YOU CAN LEARN

Formats and fees

The same agenda in four formats. Fees are in Indian rupees as of November 2026; the course page shows them in your currency.

FORMAT	DURATION	WHAT YOU GET	FEE
Live & interactive (online)	Max 8-10 hours	Instructor-led public batch of max 10 learners with demos, labs, Q&A and assignment review. Weekday batches start on the 1st of every month, weekend batches on the first Saturday of every month.	**INR 34,999**
1:1 live training (online)	Max 8-10 hours, one-to-one	The same agenda, taught one-to-one by the trainer. Starts immediately, without waiting for the next batch; sessions planned around your working hours, at your pace.	**INR 99,999**
Self-paced video	1-year LMS access	All four OpenVAS levels, plus 20+ more courses and 50+ tools, at your own pace.	**INR 833/month** billed yearly at INR 9,996
Corporate (day-wise)	3 days for this level	A private batch for your team, on demand. Foundation 1 day, Essential 2, Intermediate 3, Advanced 5 (cumulative).	**Quote on request**

ASSESSMENT AND CERTIFICATE

Your progress is checked through hands-on labs and assignments at every level. On completion you receive a DevOpsSchool certificate of completion with a unique credential ID that anyone can verify at devopsschool.com/certificates.

INCLUDED WITH EVERY LIVE BATCH

- Every live session is recorded and stays in your LMS for a year.
- Can't attend your batch? Move to next month's batch.
- Free demo class before you pay.
- Free 10-15 minute call with an advisor or the trainer to check the course fits you.

YOUR TRAINER

Learn from Rajesh Kumar

Principal Architect, trainer and mentor in DevOps, SRE, DevSecOps and platform engineering, with 20 years across 8+ software MNCs, including Staff DevOps/SRE Engineer for a leading Japanese mobile-payment platform and Principal DevOps Architect and Manager in Europe.

Profile: www.rajeshkumar.xyz · Videos: youtube.com/@TheDevOpsSchool

20 years in industry	**200+** corporate trainings
10,000+ engineers mentored	**70+** organisations coached

REVIEWS

What learners say

Rated 4.6 on Google · more reviews at devopsschool.com/testimonials and in our video testimonials.

> “Rajesh is very good trainer. Rajesh was able to resolve our queries and question effectively. We really liked the hands-on examples covered during this training program.”
>
> Indrayani, India

> “The training was very useful and interactive. Rajesh helped develop the confidence of all.”
>
> Abhinav Gupta, Pune

START YOUR OPENVAS TRAINING

Join the next batch

Weekday batches start on the 1st of every month and weekend batches on the first Saturday of every month, with max 10 learners each. 1:1 training can start immediately; corporate batches run on demand. We reply within 1 hour.

Pay by UPI, credit and debit cards, net banking or PayPal. Before you pay, read our refund policy. All levels of this course: www.devopsschool.com/courses/openvas/

ENROL OR RESERVE A SEAT
OpenVAS Intermediate Training

WHATSAPP · INDIA
+91 99057 40781

WHATSAPP · USA
+1 (469) 756-6329

EMAIL
contact@DevOpsSchool.com

Next step after this level: OpenVAS Advanced Training - Run an enterprise vulnerability management programme with risk-based prioritisation, scaled scanning, compliance evidence and reporting.