DevOpsSchool

Course curriculum · November 2026

LEVEL 04 OF 04 · ADVANCED

kube-hunter Advanced Training

Model Kubernetes attack paths, harden clusters in depth and run governed penetration testing programmes.

LIVE ONLINE **Max 8-10 hours**	CORPORATE (DAY-WISE) **5 days · Days 1-5**	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 · Included	5 days · This curriculum

INSIDE THIS CURRICULUM

What you will achieve	Outcomes and level focus
Who should attend	Audience and prerequisites
Agenda	47 topics · Foundation to Advanced
Hands-on labs	4 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/kubehunter/kubehunter-and-advance-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 kube-hunter course path, you will be able to:

1

Assess cluster exposure

Find exposed Kubernetes services and weak settings with kube-hunter scans.

2

Fix and verify weaknesses

Remediate kubelet, API server, RBAC and network findings and prove them with re-tests.

3

Run security testing programmes

Plan, automate and govern Kubernetes penetration testing alongside current scanners.

WHAT THE ADVANCED LEVEL ADDS

Attack paths, defence in depth and governance

Hands-on: Harden a vulnerable cluster end to end. Attack a deliberately vulnerable cluster, document the attack path, apply layered fixes with detection rules and deliver a re-test report.

WHO SHOULD ATTEND

- Experienced kube-hunter practitioners responsible for quality, security and scale.
- Senior engineers, architects and leads who design and troubleshoot kube-hunter solutions.
- Teams making kube-hunter an organisation-wide standard.

BEFORE YOU START

- The Intermediate level, or equivalent hands-on experience.
- You can already: Use active hunting responsibly, automate scans in pipelines and extend kube-hunter with custom hunters.
- 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 ADVANCED

kube-hunter Advanced Training agenda

47 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: Kubernetes attack surface and first scan

Included from Foundation

1. Kubernetes attack surface: API server, kubelet, etcd, dashboard and exposed node ports
2. kube-hunter overview: Aqua Security's open-source Python tool that hunts for weaknesses in Kubernetes clusters
3. Project status: kube-hunter is no longer actively developed, and where Trivy and Kubescape now fit
4. Ethics and authorisation: scanning only clusters you own or have written permission to test
5. Installing kube-hunter: pip install kube-hunter, the aquasec/kube-hunter image or running from source
6. Scan modes overview: remote, interface, network CIDR and pod scanning
7. Remote scan: kube-hunter --remote against a node or API server address
8. Interface scan: --interface to discover clusters reachable on local networks
9. Reading results: discovered nodes, services and vulnerabilities with their KHV identifiers
10. Finding categories: information disclosure, remote code execution, privilege escalation and access risk
11. Lab setup: intentionally misconfigured clusters with kind or kubeadm for safe practice

DAY 2 — Essential: Scan modes, reports and common findings

Included from Essential

12. Network scans: --cidr ranges for multi-node discovery
13. Pod mode: running kube-hunter as a Job with --pod to see what a compromised pod can reach
14. Listing tests: kube-hunter --list and --list --active for passive and active hunters
15. Reports: --report json or yaml and --dispatch stdout or http to send results
16. Logging and statistics: --log levels and --statistics for a hunter execution summary
17. Quick scans and discovery: --quick and --k8s-auto-discover-nodes
18. Exposed kubelet API: read-only port 10255, anonymous access on 10250 and their fixes
19. API server findings: anonymous authentication, version disclosure and insecure ports
20. Dashboard and etcd exposure: unauthenticated dashboards and etcd without client certificates
21. Service account tokens: token mounting risks and automountServiceAccountToken: false
22. Remediation workflow: mapping each finding to kubelet, API server or network policy changes
23. Re-testing: confirming fixes by repeating scans and comparing JSON reports

DAY 3 — Intermediate: Active hunting, automation and custom hunters

Included from Intermediate

24. Active hunting: what --active changes on the target and when it is safe to use
25. Authenticated hunting: --service-account-token to test with a given identity
26. Automating scans: in-cluster CronJobs and CI pipeline stages against test clusters
27. Processing results: parsing JSON with jq and forwarding findings to Elasticsearch or a SIEM
28. Custom hunters: writing Hunter and ActiveHunter classes subscribed to events with @handler.subscribe
29. Events and vulnerabilities: the Event and Vulnerability classes, publishing events and chaining hunters
30. Network policies: default deny, restricting kubelet and API access and verifying with re-scans

31. RBAC hardening: least-privilege roles, removing cluster-admin bindings and kubectl auth can-i checks
32. Kubelet hardening: --anonymous-auth=false, webhook authorization and disabling the read-only port
33. Choosing tools: kube-hunter for external tests, kube-bench for CIS settings, Trivy and Kubescape for posture
34. Troubleshooting: no clusters found, blocked ports, proxy settings and pod mode permissions
35. Managed clusters: provider-run control planes, private endpoints and node security groups

DAYS 4-5 **Advanced: Attack paths, defence in depth and governance** **New at this level**

36. Attack paths: chaining exposed services, token theft and RBAC misconfigurations into cluster takeover
37. Threat modelling: MITRE ATT&CK for Containers and the Microsoft threat matrix for Kubernetes
38. Red team exercises: scoped penetration tests, rules of engagement and reporting
39. Detection: catching scans and exploitation attempts with Falco rules and API server audit logs
40. Defence in depth: Pod Security Admission, network segmentation, secrets encryption and node hardening
41. Private clusters: removing public API endpoints, bastion access and zero-trust access
42. Maintaining kube-hunter: pinning versions and patching a fork now that upstream development has stopped
43. Migration: moving continuous scanning to Trivy, Kubescape or kube-bench while keeping external tests
44. Fleet scanning: scheduling external scans across many clusters and tracking findings centrally
45. Governance: vulnerability SLAs, risk acceptance and evidence for audits
46. Purple teaming: running scans while defenders validate alerts and response playbooks
47. Capstone: assess, exploit in a lab, harden and re-test a deliberately vulnerable cluster with a final report

PRACTICE

Hands-on labs

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

FOUNDATION **Run a remote scan on a lab cluster**
Build a deliberately weak kind or kubeadm cluster, scan it remotely with kube-hunter and list every finding with its severity.

ESSENTIAL **Find and fix exposed kubelet ports**
Scan a cluster in pod mode, fix the exposed kubelet and dashboard findings and prove the fixes with a second JSON report.

INTERMEDIATE **Write a custom kube-hunter hunter**
Write a passive hunter that detects an internal service your team exposes, run it in a CI scan and route the findings to a SIEM.

ADVANCED **Harden a vulnerable cluster end to end**
Attack a deliberately vulnerable cluster, document the attack path, apply layered fixes with detection rules and deliver a re-test report.

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 kube-hunter levels, plus 20+ more courses and 50+ tools, at your own pace.	**INR 833/month** billed yearly at INR 9,996
Corporate (day-wise)	5 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 KUBE-HUNTER 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/kubehunter/

ENROL OR RESERVE A SEAT
kube-hunter Advanced Training

WHATSAPP · INDIA
+91 99057 40781

WHATSAPP · USA
+1 (469) 756-6329

EMAIL
contact@DevOpsSchool.com