DevOpsSchool

Course curriculum · November 2026

LEVEL 04 OF 04 · ADVANCED

Nikto Advanced Training

Use Nikto in professional assessments to find attack vectors, test WAF effectiveness and run a risk-based scanning programme.

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	44 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/nikto/nikto-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 Nikto course path, you will be able to:

1

Scan web servers effectively

Install, configure and run Nikto scans that find misconfigurations, outdated software and risky files.

2

Customise and automate Nikto

Extend Nikto with custom tests and plugins and automate it with Nmap, Metasploit and CI pipelines.

3

Turn findings into security

Validate findings, test WAFs and drive risk-based remediation from Nikto results.

WHAT THE ADVANCED LEVEL ADDS

Exploitation testing, WAF validation and scanning programs

Hands-on: Web server assessment capstone. Assess a lab estate behind a WAF, compare blocked and missed tests, confirm exploitable issues and deliver a prioritised report.

WHO SHOULD ATTEND

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

BEFORE YOU START

- The Intermediate level, or equivalent hands-on experience.
- You can already: Run targeted advanced scans, customise Nikto with your own tests and plugins and automate it alongside Nmap, Metasploit and CI pipelines.
- 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

Nikto Advanced Training agenda

44 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: Web scanning concepts, installation and first scan

Included from Foundation

1. Introduction to Nikto: overview of the tool, its features and how it works
2. Web vulnerability scanning basics: DAST, server misconfigurations, default files and outdated software
3. How Nikto works: Perl engine, LibWhisker, test database and plugin-driven checks
4. Legal and ethical scanning: written authorisation, scope and avoiding production impact
5. Installing Nikto on a Linux machine: Kali package, Git clone with Perl dependencies or the Docker image
6. Configuring Nikto for use: nikto.conf, user agent, default ports and SSL libraries
7. Lab targets: intentionally vulnerable web apps such as DVWA and OWASP Juice Shop
8. First scan: nikto -h against a lab web server and what each output line means
9. Reading results: server banner, headers, interesting files and HTTP methods found
10. Scanning web servers with Nikto: performing basic scans and analysing the results

DAY 2 — Essential: Command-line options, enumeration and reporting

Included from Essential

11. Nikto command-line options: overview of the main options and how to use them to customise scans
12. Targets and ports: -h, -p, host lists, -ssl and -nossl, -vhost and -root
13. Web server enumeration: software versions, installed modules, headers and robots.txt entries
14. Interesting files and directories: backups, admin pages, default content and directory indexing
15. Tuning scans: -Tuning categories such as interesting files, misconfiguration and information disclosure
16. Plugins: -list-plugins and selecting plugins with -Plugins
17. Output formats: -o and -Format for text, CSV, HTML, JSON and XML reports
18. Display and pacing: -Display options, -timeout, -Pause and -maxtime
19. Scanning through a proxy: -useproxy and reviewing traffic in Burp Suite
20. Reporting and analysis: reviewing reports to identify vulnerabilities and misconfigurations
21. False positives: verifying findings manually with curl and a browser

DAY 3 — Intermediate: Advanced scans, customisation, scripting and integration

Included from Intermediate

22. Advanced Nikto scanning: directory traversal, file inclusion and remote file retrieval tests
23. Injection and command execution tuning: XSS, SQL injection and remote shell test categories
24. Authenticated scanning: -id for basic auth and cookies in the configuration file
25. Customizing Nikto: nikto.conf, CGI directories, user agents and targeted scans
26. Custom tests: adding your own checks with a user test database
27. Nikto scripting: automating scans with shell scripts and parsing JSON output
28. Creating custom plugins: Nikto plugin structure in Perl and registering a plugin
29. Nikto integration with other tools: feeding Nmap results to Nikto
30. Metasploit integration: validating Nikto findings with matching Metasploit modules

31. Evasion options: -evasion encoding techniques and what they reveal about defences
32. DevSecOps use: running the Nikto Docker image in Jenkins or GitHub Actions against staging
33. Troubleshooting scans: SSL errors, timeouts, redirects and blocked requests

DAYS 4-5 **Advanced: Exploitation testing, WAF validation and scanning programs** **New at this level**

34. Exploitation testing: using Nikto findings to identify and safely confirm potential attack vectors
35. Web application firewall testing: using Nikto to test the effectiveness of WAFs such as ModSecurity with OWASP CRS
36. Detection engineering: reading WAF and server logs to see which Nikto tests are blocked or missed
37. Nikto in a toolchain: combining it with OWASP ZAP, Nuclei and Burp Suite and knowing its limits
38. Large-scale scanning: scheduling, rate limits, scope lists and scanning many hosts safely
39. Testing strategies: when to scan, staging versus production and change-driven rescans
40. Risk management: rating findings, business impact and prioritising remediation
41. Reporting at scale: importing results into DefectDojo or ticketing systems and tracking fixes
42. Hardening based on findings: server configuration, headers, removing default content and patching
43. Best practices for using Nikto: real-world scenarios, testing strategies and risk management
44. Capstone: an authorised web server assessment with WAF testing, verified findings and a remediation report

PRACTICE

Hands-on labs

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

FOUNDATION **Install Nikto and scan a lab**
Install Nikto on Kali or Docker, scan a vulnerable lab web server and explain every finding in the output.

ESSENTIAL **Enumerate and report on servers**
Scan several lab web servers with tuned options through Burp, verify the key findings and produce HTML and JSON reports.

INTERMEDIATE **Automated, integrated scanning workflow**
Discover web services with Nmap, scan them with a custom Nikto plugin in a CI job and validate a finding in Metasploit.

ADVANCED **Web server assessment capstone**
Assess a lab estate behind a WAF, compare blocked and missed tests, confirm exploitable issues and deliver a prioritised 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 Nikto 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 NIKTO 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/nikto/

ENROL OR RESERVE A SEAT
Nikto Advanced Training

WHATSAPP · INDIA
+91 99057 40781

WHATSAPP · USA
+1 (469) 756-6329

EMAIL
contact@DevOpsSchool.com