DevOpsSchool

Course curriculum · November 2026

LEVEL 04 OF 04 · ADVANCED

Network Security Advanced Training

Lead risk-based network penetration tests and design zero trust, cloud-ready network defences with monitoring and incident response.

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	46 topics · Foundation to Advanced
Hands-on labs	4 labs
Formats and fees	Live, 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/network/network-security-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 Network Security course path, you will be able to:

1

Find network weaknesses

Discover, scan, enumerate and assess networks for vulnerabilities using industry tools.

2

Understand real attacks

Reproduce common network attacks safely in a lab and know how to detect each one.

3

Design stronger defences

Apply segmentation, zero trust, monitoring and incident response to protect enterprise networks.

WHAT THE ADVANCED LEVEL ADDS

Risk-based testing, zero trust and enterprise defence

Hands-on: Enterprise network assessment capstone. Run a scoped, risk-based test of a segmented lab network and present findings with detections and a zero trust remediation plan.

WHO SHOULD ATTEND

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

BEFORE YOU START

- The Intermediate level, or equivalent hands-on experience.
- You can already: Exploit common network weaknesses in a lab, escalate privileges and detect the same attacks with IDS, logging and network monitoring.
- 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

Network Security Advanced Training agenda

46 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: Network threats, secure design basics and lab setup

Included from Foundation

1. Network security fundamentals: confidentiality, integrity, availability, threat actors and attack surface
2. TCP/IP and OSI from a security view: ports, protocols, the TCP handshake and where attacks happen
3. Common network attacks: sniffing, spoofing, ARP poisoning, man-in-the-middle and DoS or DDoS
4. Secure network design basics: segmentation, VLANs, DMZs and trust zones
5. Firewalls: stateless ACLs, stateful inspection and next-generation firewalls
6. Encryption in transit: TLS, SSH and why plaintext protocols are dangerous
7. Telnet and rlogin insecurities: credential exposure and replacing them with SSH
8. Packet analysis: capturing and filtering traffic with Wireshark and tcpdump
9. Lab setup: Kali Linux, virtual networks and intentionally vulnerable targets
10. Rules of engagement: legal authorisation, scope and safe testing practices

DAY 2 — Essential: Reconnaissance, scanning, enumeration and vulnerability assessment

Included from Essential

11. Reconnaissance: passive OSINT, WHOIS, DNS records and subdomain discovery
12. Network scanning: host discovery, TCP and UDP port scans and service detection with Nmap
13. Scanning tools: Nmap scripting engine, Masscan and hping3
14. Scanning countermeasures: firewall rules, rate limiting and detecting scans in logs
15. Banner grabbing and its techniques: netcat, Nmap -sV and HTTP headers
16. Enumeration and its tools: SMB, SNMP, LDAP, NFS and DNS zone transfers with enum4linux and snmpwalk
17. NetBIOS insecurity: null sessions, name resolution poisoning and how to disable legacy protocols
18. VA tools: Nessus, OpenVAS (Greenbone) and authenticated versus unauthenticated scans
19. Vulnerability analysis using Nessus: scan policies, results, CVSS scores and false positives
20. Host firewalls in practice: nftables or iptables rules and Windows Defender Firewall
21. VPN fundamentals: IPsec, WireGuard and OpenVPN for site-to-site and remote access
22. Wireless security: WPA2 and WPA3, enterprise 802.1X and rogue access points

DAY 3 — Intermediate: Network attacks, exploitation and detection

Included from Intermediate

23. Hacking networks: ARP spoofing and man-in-the-middle with Bettercap and VLAN hopping
24. VPN hacking: IKE aggressive mode, weak pre-shared keys and ike-scan
25. Cracking passwords: online attacks with Hydra and offline cracking with John the Ripper and Hashcat
26. Hacking webservers: misconfigurations, default content, outdated versions and Nikto scans
27. Hacking Linux: weak services, SSH misconfiguration and SUID binaries
28. Hacking Windows: SMB weaknesses, credential exposure and patch gaps
29. Exploitation and post-exploitation concepts: Metasploit modules, sessions, pivoting and persistence
30. Privilege escalation: Linux and Windows techniques and how to prevent them

31. Intrusion detection and prevention: Suricata or Snort rules and alert tuning
32. Network monitoring: Zeek logs, NetFlow and sending network events to a SIEM
33. Network access control: 802.1X, RADIUS and device posture checks
34. Hardening from findings: closing exploited paths and verifying with a rescan

DAYS 4-5 **Advanced: Risk-based testing, zero trust and enterprise defence** **New at this level**

35. Risk based pentesting: scoping by business risk, threat-led testing and CVSS with business impact
36. Zero trust network architecture: NIST SP 800-207, ZTNA and identity-aware access
37. Microsegmentation: east-west traffic control in data centres and Kubernetes network policies
38. Cloud network security: VPCs or VNets, security groups, network ACLs, private endpoints and cloud firewalls
39. DDoS protection: volumetric and application attacks, scrubbing services and rate limiting
40. DNS security: DNSSEC, encrypted DNS, protective DNS and sinkholing
41. Secure remote administration: bastion hosts, privileged access management and just-in-time access
42. Threat hunting in network data: hypotheses, beaconing detection and lateral movement indicators
43. Network incident response: containment, packet capture for forensics and recovery
44. Compliance mapping: PCI DSS segmentation, ISO 27001 and CIS Controls for networks
45. Purple teaming: running attack simulations with defenders to improve detections
46. Capstone: a risk-based network penetration test and zero trust remediation roadmap

PRACTICE

Hands-on labs

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

FOUNDATION

Build a network security lab

Build an isolated lab with Kali Linux and vulnerable hosts, capture Telnet and SSH sessions in Wireshark and compare what leaks.

ESSENTIAL

Scan, enumerate and assess

Map the lab network with Nmap, enumerate SMB and SNMP services, run a Nessus scan and prioritise the findings.

INTERMEDIATE

Attack and detect in the lab

Perform a MITM, crack captured hashes and escalate on a target host, then write Suricata rules and Zeek queries that detect each step.

ADVANCED

Enterprise network assessment capstone

Run a scoped, risk-based test of a segmented lab network and present findings with detections and a zero trust remediation plan.

HOW YOU CAN LEARN

Formats and fees

The same agenda in three 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**
Self-paced video	1-year LMS access	All four Network Security 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). 1:1 training is also available on demand.	**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 NETWORK SECURITY 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. Corporate and 1:1 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/network/

ENROL OR RESERVE A SEAT
Network Security Advanced Training

WHATSAPP · INDIA
+91 99057 40781

WHATSAPP · USA
+1 (469) 756-6329

EMAIL
contact@DevOpsSchool.com