Updated on 09/10/2025

Sign up

IPv6-IPv8 Security Lab Training

2 days (14 hours)

Presentation

IPv6 is now the standard for overcoming IPv4 exhaustion and strengthening network security. With the rise of cloud and DevOps environments, the adoption of IPv6 is becoming unavoidable. For its part, IPv8, still in the exploratory stage, promises to bring major advances in terms of performance and integrated cryptography.

Our IPv6-IPv8 Security Lab training course will give you a practical and operational vision of IPv6 network security, explore the specific vulnerabilities of IPv4/IPv6 coexistence and anticipate the potential impacts of IPv8.

At the end of this course, you'll be able to design and deploy a secure lab dedicated to IPv6 and IPv8, master modern monitoring tools and integrate cybersecurity best practices into your DevOps infrastructures.

Like all our training courses, this one is based on the latest stable version of the protocols, and favors a practical, field-oriented approach.

Objectives

- Master IPv6 security fundamentals and risks
- Harden ICMPv6, including extension heads and tunnels
- Implement IPsec and L2/L3 protection
- Automate IaC network configuration
- Supervise and investigate with Prometheus/Grafana/ELK
- Build a reproducible Security Lab

Target audience

- DevOps and SRE engineers
- System and network administrators

Prerequisites

- Network basics (TCP/IP, routing, DNS)
- Experience with Unix/Linux or Windows Server
- Notions of CI/CD and IaC

IPv6?IPv8 Security Lab training program

Understanding IPv6 and security issues

- History: IPv4 limitations and the need for IPv6
- IPv6 addressing fundamentals
- New security features of the IPv6 stack
- Use cases in DevOps and cloud infrastructures
- Risks associated with adopting IPv6 in information systems

Basic IPv6 security mechanisms

- Central role of ICMPv6 and security implications
- Extension headers: analysis and attack vectors
- Address security: SLAAC, DHCPv6, DAD
- Specific vulnerabilities in dual-stack environments
- IPv6 filtering best practices and firewalls

Advanced IPv6 security practices

- Use of native IPsec in IPv6 (AH/ESP)
- Routing policies and RA Guard / L2 protections
- Risks in IPv6/IPv4 tunnels (6in4, GRE)
- Attack detection: scanning, spoofing, flooding
- Workshop: IPv6 firewall and malicious flow analysis

IPv8: prospects and research laboratories

- Overview of exploratory work on IPv8
- Performance and integrated cryptography
- Potential impact on DevOps architectures
- Current limits and state of standardization
- Positioning with regard to IPv6 in production

Automation and supervision in DevOps

- IPv6 integration in CI/CD pipelines
- Network infrastructure in IaC: Ansible, Terraform
- Supervision: Prometheus, Grafana, ELK
- Security testing tools: IPv6 scanners, IDS/IPS
- Workshop: securing a Kubernetes dual-stack cluster

Setting up a Security Lab

- Architecture of a reproducible IPv6/IPv8 lab
- Virtualization & network simulation (hypervisor, containers)
- Test plan: attack scenarios & success KPIs
- Good governance practices and documentation
- Workshop: deploying a mini-lab & simulating a DDoS

Companies concerned

This course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced IT technology, or to acquire specific business knowledge or modern methods.

Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire which enables us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the forthcoming course, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

Teaching methods

Practical training: 60% hands-on, 40% theory. Training material distributed in digital format to all participants.

Organization

The course alternates theoretical input from the trainer, supported by examples, with brainstorming sessions and group work.

Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

Certification

A certificate will be awarded to each trainee who has completed the entire course.