

Updated on 10/08/2026

[Sign Up](#)

IPv6 Security Lab Training

2 days (14 hours)

Overview

IPv6 is fundamentally transforming how networks operate with new addressing, autoconfiguration, and discovery mechanisms. These changes also introduce specific attack vectors that must be addressed to secure IPv6 and dual-stack infrastructures.

Our IPv6 Security: Attacks, Defense, and Hands-On Workshops training course will enable you to identify, replicate, and analyze the main threats affecting IPv6 environments in order to implement appropriate safeguards.

In particular, you will examine the risks associated with ICMPv6, Neighbor Discovery, Router Advertisement, SLAAC, and DHCPv6. You will learn to recognize scenarios involving reconnaissance, spoofing, Rogue RA, flooding, and traffic hijacking, and then apply the appropriate defense mechanisms.

The course also covers risks associated with extension headers, fragmentation, tunnels, and dual-stack environments. You will learn how to build filtering rules tailored to IPv6 and verify the consistency of security policies between IPv4 and IPv6.

Through a highly hands-on approach, you will analyze traffic with Wireshark, analyze logs and detection mechanisms, and then replicate attacks in an isolated lab to understand their effects and validate countermeasures.

Upon completion of this training, you will be able to audit, detect, and correct the main vulnerabilities in an IPv6 infrastructure and set up a Security Lab to test your defense mechanisms before deploying them in production.

Objectives

- Identify the main IPv6 attack surfaces
- Analyze risks associated with ICMPv6, NDP, Router Advertisement, SLAAC, and DHCPv6
- Replicate and understand reconnaissance, spoofing, Rogue RA, and flooding attacks
- Secure dual-stack environments, extension headers, and transition mechanisms
- Configure L2/L3 protections and IPv6 firewall rules
- Detect and analyze malicious behavior based on traffic flows and logs
- Build and operate a reproducible IPv6 Security Lab

Target Audience

- Network security engineers
- Network engineers
- Network and system administrators
- Cybersecurity and SOC analysts
- Network and security architects
- Cloud and Infrastructure Engineers responsible for securing IPv6 environments

Prerequisites

- Solid knowledge of TCP/IP, DNS, and routing fundamentals
- Understanding of IPv6 addressing and key mechanisms
- Basic knowledge of network security and firewalling
- Experience with Linux or Windows in a network environment is recommended

Technical Prerequisites

- A computer capable of running the network tools required for the exercises
- A modern web browser and a stable Internet connection
- Access to the IPv6 lab environment provided or set up for the training

Course Outline for our IPv6 Security Training: Attacks, Defense, and Hands-On Workshops

[Day 1 - Morning]

Understanding the attack surface of an IPv6 network

- Identifying the security differences between IPv4 and IPv6 and their implications for infrastructure
- Analyzing IPv6 addressing, link-local addresses, and autoconfiguration mechanisms from a security perspective
- Understand the critical role of ICMPv6 and the risks of improper filtering
- Analyze the operation of the Neighbor Discovery Protocol (NDP), SLAAC, DAD, and DHCPv6

- Identify the additional risks introduced by dual-stack environments and transition mechanisms
- Hands-on workshop: Map an IPv6 network, capture ICMPv6/NDP traffic using Wireshark, and identify its attack surface.

[Day 1 - Afternoon]

Reconnaissance, spoofing, and Neighbor Discovery attacks

- Implement IPv6 reconnaissance techniques and understand how they differ from IPv4 scans
- Analyze attacks based on Neighbor Solicitation and Neighbor Advertisement messages
- Understand scenarios involving rogue router advertisements and traffic hijacking
- Identify the risks associated with fake DHCPv6 servers and uncontrolled autoconfiguration settings
- Examine spoofing, flooding, and denial-of-service scenarios affecting IPv6 mechanisms
- Implement RA Guard protections and appropriate Layer 2 security controls
- Hands-on workshop: Reproduce a Rogue RA scenario in an isolated lab environment, observe its effects, and then configure and validate defense mechanisms.

[Day 2 - Morning]

Analyze IPv6 network bypasses and attacks

- Understand IPv6 extension headers and their impact on security devices
- Analyze risks related to fragmentation and extension header chains
- Identify ways to bypass filtering rules and detection devices
- Assess the risks associated with tunnels and IPv4/IPv6 coexistence mechanisms
- Build IPv6-compatible firewall rules without blocking essential ICMPv6 functions
- Verify the consistency of security policies between IPv4 and IPv6 stacks
- Hands-on workshop: Analyze several malicious IPv6 traffic flows, identify evasion techniques, and then strengthen filtering rules.

[Day 2 - Afternoon]

Detect and monitor IPv6 threats

- Capture and analyze IPv6 security events using Wireshark and network tools
- Configure the logging required to detect abnormal behavior
- Leverage IDS/IPS capabilities to detect IPv6 attacks and anomalies
- Identify devices or applications that use IPv6 without the knowledge of operations teams
- Develop metrics to monitor IPv6 traffic and incidents
- Organize the analysis and response to an incident affecting a dual-stack infrastructure
- Hands-on workshop: Detect malicious IPv6 activity using captures and logs, then reconstruct the attack scenario.

[Day 3 - Morning]

Hardening an IPv6 infrastructure

- Develop an IPv6 segmentation and filtering strategy tailored to the organization's needs
- Hardening NDP, Router Advertisement, DHCPv6 mechanisms, and network devices
- Limit unnecessary services, traffic flows, and transition mechanisms
- Apply consistent policies to dual-stack environments
- Integrate IPv6 controls into existing configuration, audit, and monitoring procedures
- Regularly test the effectiveness of security measures and identify configuration discrepancies
- Hands-on workshop: audit a deliberately misconfigured IPv6 infrastructure, apply hardening measures, and then verify their effectiveness.

[Day 3 - Afternoon]

Build and operate an IPv6 Security Lab

- Design an isolated and reproducible IPv6 lab architecture
- Use virtualization and containers to replicate different network scenarios
- Build a test plan combining reconnaissance, attack, detection, and mitigation
- Document the scenarios, results, and evidence required for a security audit
- Define a validation methodology prior to deploying IPv6 in production
- Develop a reusable IPv6 hardening checklist for the organization
- Hands-on workshop: Conduct a complete controlled attack scenario in the Security Lab, detect the incident, apply countermeasures, and then validate the hardening.

Target Audience

This training is intended for both individuals and companies—large or small—that wish to train their teams in a new, advanced IT technology or to acquire specific industry knowledge or modern methods.

Entry-Level Assessment

The pre-training assessment complies with Qualiopi quality standards. Upon final registration, the learner receives a self-assessment questionnaire that allows us to evaluate their estimated proficiency level across various types of technologies, as well as their expectations and personal goals for the upcoming training, within the limits imposed by the selected format. This questionnaire also allows us to anticipate certain connection or internal security issues within the company (intra-company or virtual classroom) that could pose challenges for monitoring and ensuring the smooth running of the training session.

Teaching Methods

Hands-On Training: 60% Practical, 40% Theoretical. Training materials distributed in digital format to all participants.

Organization

The course alternates between theoretical input from the instructor—supported by examples and reflection sessions—and group work.

Assessment

At the end of the session, a multiple-choice quiz is administered to verify that participants have successfully acquired the skills.

Certification

A certificate will be issued to each trainee who has completed the entire training program.