

# Advanced IPv6 Security

Three-day hands-on training course

*Advanced IPv6 Security* is a follow-up to SI6 Network's *Hacking IPv6 Networks* flagship course, covering the most advanced IPv6 attack and defense techniques. This course assumes knowledge of the topics covered by the course *Hacking IPv6 Networks v3.0* as a starting-point, and explores the most advanced IPv6 attack and defense techniques through hands-on exercises. During the course, the attendee will perform a large number of exercises in a network laboratory (with the assistance of the trainer), such that the concepts and techniques learned during the course are reinforced with hands-on exercises. The training course is carried out by Fernando Gont, a world-renowned IPv6 security expert.

---

## Audience and prerequisites

Network Engineers, Network Administrators, Security Administrators, Penetration Testers, and Security Professionals in general.

Participants are required to have in-depth understanding of the IPv6 protocol suite, equivalent to that provided by our *Hacking IPv6 Networks v3.0* training course.

## Course duration and format

Three days, with up to 50% of course time devoted to practical sessions.

## Course materials

- One course book (written by the trainer) that includes all the slides and exercises presented in the course.

- A copy of the virtual lab employed for the training course.
- A certificate of completion of the training course.

## Course inquiries and bookings

For inquiries about courses and consulting, you can contact us in the following ways:

- Email: [info@si6networks.com](mailto:info@si6networks.com)
- Phone: +54 (911) 6536 4380

## Prices, dates, and further details

For course prices, upcoming course dates, and further information about the course, please visit the course web page, <http://www.si6networks.com/education/ipv6>.

---

## About the trainer



Fernando Gont is a world-renowned IPv6 expert, working on IPv6 consulting around the world:

- He has written more than 20 *IETF RFCs*, many of which focus on IPv6.
- He is actively involved in IPv6 standardization, with more than 10 active *IETF Internet-Drafts*.
- He is the author of the *SI6 Network's*

*IPv6 toolkit*, the only portable and freely-available toolkit for the IPv6 protocol suite.

- He has been delivering consulting and training services worldwide for more than ten years.
- More information about Fernando Gont is available at his web site: <http://www.gont.com.ar>.

# Advanced IPv6 Security: Course outline

---

## 1. Introduction

- IPv6 security overview

## 2. IPv6 Firewalls

- Firewall technologies
- General configuration guidelines

## 3. IPv6 Addressing

- Overview of security & privacy implications
- Advanced IPv6 attacks
- IPv6 address scopes & security
- Design of an addressing plan for improved security
- SLAAC & DHCPv6 configuration for improved security
- Ingress/egress filtering in IPv6 networks

## 4. Neighbor Discovery for IPv6

- Advanced attacks
- Configuration & deployment of mitigation techniques

## 5. IPv6 Extension Headers (EHs)

- Overview of security implications
- Circumvention of security controls

- Firewalls and IPv6 EHs: configuration for improved security
- NIDS and IPv6 EHs: configuration for improved security

## 6. IPsec

- Setting up IPsec with IPv6

## 7. Internet Control Message Protocol version 6 (ICMPv6)

- Overview of security implications
- ICMPv6 packet filtering

## 8. Dynamic Host Configuration Protocol version 6 (DHCPv6)

- Sample DHCPv6 traffic
- Security implications of DHCPv6
- DHCPv6 attacks
- DHCPv6 security controls

## 9. Multicast Listener Discovery (MLD)

- Sample MLD traffic
- Security implications of MLD
- MLD attacks
- MLD security controls

## 10. Advanced Upper-Layer Attacks

- TCP-based attacks
- UDP-based attacks
- Possible mitigations

## 11. DNS support for IPv6

- Overview of security implications
- DNS configuration for improved security

## 12. Transition/co-existence technologies

- Exploitation of transition/co-existence technologies
- Secure deployment of transition/co-existence technologies

## 13. Security Implications of IPv6 for IPv4-only Networks

- Weaponizing IPv6 attacks on IPv4-only networks
- VPN leakages: exploitation and mitigation
- Practical mitigation of IPv6 attacks on IPv4-only networks

## 14. Penetration testing in IPv6

- Network reconnaissance in IPv6
- IPv6 and penetration testing frameworks