SI6 NETWORKS

Hacking IPv6 Networks v3.0

Three-day hands-on training course

This course will provide the attendee with in-depth knowledge of IPv6 security, such that the attendee is able to evaluate and mitigate the security implications of IPv6 in production environments. The attendee will be given an in-depth explanation of each topic covered in this course, and will learn – through hands-on exercises – how each feature can be exploited for malicious purposes. Subsequently, the attendee will be presented with a number of alternatives to mitigate each of the identified vulnerabilities. This course will employ a range of open source tools to evaluate the security of IPv6 networks, and to reproduce a number of IPv6-based attacks. 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 this course are reinforced with hands-on exercises. The attendee will be required to perform a large number of IPv6 attacks, and to envision mitigation techniques for the corresponding vulnerabilities.

Audience and prerequisites

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

Participants are required to have:

- Good understanding of the IPv4 protocol suite (IPv4, ICMP, ARP, etc.)
- Good understanding of network components (routers, firewalls, etc.)
- Knowledge of basic UNIX/Linux shell commands
- knowledge of basic IPv4 troubleshooting tools, such as: ping, traceroute, and network protocol analyzers (e.g., tcpdump).

Basic knowledge of IPv6 is desirable, but *not* required.

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

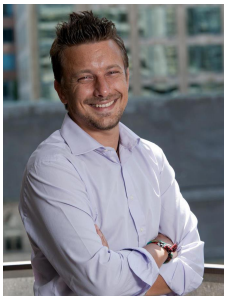
For inquiries about courses and consulting, you can contact us in the following ways:

- Email: info@si6networks.com
- 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 that 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*.

Hacking IPv6 Networks v3.0: Detailed training course agenda

1. **Introduction to IPv6**
   - IPv4 address exhaustion
   - IPv6 service
   - IPv6 transition/deployment mechanisms
   - IPv6: current state of affairs
   - Brief comparison between IPv6 and IPv4
   - IPv6 security overview
2. **IPv6 Addressing Architecture**
   - IPv6 address types
   - IPv6 address analysis
   - Implications for address scanning attacks & possible mitigations
   - Privacy implications & possible mitigations
   - Implications for end-to-end connectivity
3. **IPv6 Header Fields**
   - IPv6 header overview
   - Basic header fields
   - Security assessment
4. **IPv6 Extension Headers (EHs)**
   - General implications of EHs
   - Security implications of specific IPv6 EHs
   - Security implications of specific IPv6 options
   - IPv6 EHs in the real world
   - Exploitation of IPv6 EHs
   - Troubleshooting IPv6 EHs
   - Network reconnaissance with IPv6 EHs
   - Recent advances
5. **IPsec**
   - Virtual Private Network (VPN) traffic leakages
6. **Internet Control Message Protocol version 6 (ICMPv6)**
   - ICMPv6 error messages
   - ICMPv6 informational messages
   - Network reconnaissance with ICMPv6
7. **Neighbor Discovery for IPv6**
   - Address resolution in IPv6
   - Address resolution messages and options
   - Neighbor Discovery cache
   - Neighbor Discovery attacks
   - Neighbor Discovery security controls
   - Evasion of Neighbor Discovery security controls
   - System configuration options
8. **Stateless Address Auto-configuration (SLAAC)**
   - SLAAC operation
   - SLAAC messages and options
   - Duplicate Address Detection (DAD)
   - Troubleshoting SLAAC
   - SLAAC attacks
   - DAD attacks
   - SLAAC security controls
   - Evasion of SLAAC security controls
   - System configuration options
9. **Dynamic Host Configuration Protocol version 6 (DHCPv6)**
   - Sample DHCPv6 traffic
   - Security implications of DHCPv6
   - DHCPv6 attacks
   - DHCPv6 security controls
10. **Multicast Listener Discovery (MLD)**
    - Sample MLD traffic
    - Security implications of MLD
    - MLD attacks
    - MLD security controls
11. **Upper-Layer Attacks**
    - TCP-based attacks
    - UDP-based attacks
    - Possible mitigations
12. **DNS Support for IPv6**
    - Network reconnaissance
    - Exploiting DNS reverse mappings
13. **IPv6 Firewalls**
    - Known limitations
    - Evasion of IPv6 firewalls
14. **Security Implications of IPv6 for IPv4-only Networks**
    - IPv6 attacks on IPv4-only networks
    - Mitigating IPv6 attacks on IPv4-only networks
15. **Transition/Co-existence Technologies**
    - Automatic tunneling mechanisms
    - Attacks on automatic tunneling mechanisms
    - Mitigations
16. **Network Reconnaissance in IPv6**
    - Host scanning in IPv6
    - Port scanning in IPv6
17. **IPv6 Deployment Considerations**
    - Designing an IPv6 address plan
    - Operating System hardening
    - Other considerations