

IPv6 Training: IPv6 Professional Security (IPv6SEC, 4 jours)

Description

The course IPv6 Professional Security (IPv6 Training) discusses every aspect of IPv6 security from the basics of the IPv6 protocol stack to protocol and application vulnerabilities. Beginning with a review of IPv6 addressing, the course introduces participants to the full range of security vulnerabilities and countermeasures. We discuss stateless and stateful DHCPv6, DNSv6, ICMPv6 and IGMPv6 amongst others. The course also explores routing protocols, ACLs, VLANs, firewalls, VOIP, IPv6 mobility & more.

Tarifs

- Tarification: \$3,750/person
- Rabais de 10% lorsque vous inscrivez 3 personnes.

Plan de cours

IPv6 Fundamentals Reviewed

Major Differences between IPv4 and IPv6
Understanding the IPv6 Address Space
Understanding IPv6 Address Types
IPv6 Address Expression
Understanding Stateless and Stateful Auto-configuration
Understanding DHCPv6
The IPv6 Header
Understanding Header Extensions
Understanding Neighbor Discovery
Exploring ICMPv6
Understanding DNSv6
A Quick Look at End to End Traffic in an IPv6 Network
A Quick Tour of IPv4 and IPv6 Co-Existence

Introduction to IPv6 Security

Reintroduction to IPv6
IPv6 Update
IPv6 Vulnerabilities
Hacker Experience
IPv6 Security Mitigation Techniques
Recommended Readings and Resources

IPv6 Protocol Security Vulnerabilities

The IPv6 Protocol Header
Extension Header Threats
Reconnaissance on IPv6 Networks
Layer 3 and Layer 4 Spoofing

IPv6 Internet Security

Large-Scale Internet Threats
Ingress/Egress Filtering
Securing BGP Sessions
IPv6 over MPLS Security
Customer Premises Equipment

Prefix Delegation Threats

Multihoming Issues

IPv6 Perimeter Security

IPv6 Firewalls

Cisco IOS Router ACLs

Cisco IOS Firewall

Cisco PIX/ASA/FWSM Firewalls

Local Network Security

Why Layer 2 Is Important

ICMPv6 Layer 2 Vulnerabilities for IPv6

ICMPv6 Protocol Protection

Network Detection of ICMPv6 Attacks

Network Mitigation Against ICMPv6 Attacks

Privacy Extension Addresses for the Better and the Worse

DHCPv6 Threats and Mitigation

Point-to-Point Link

Endpoint Security

Hardening IPv6 Network Devices

Threats Against Network Devices

Cisco IOS Versions

Disabling Unnecessary Network Services

Limiting Router Access

IPv6 Device Management

Threats against Interior Routing Protocol

First-Hop Redundancy Protocol Security

Controlling Resources

QoS Threats

Server and Host Security

IPv6 Host Security

Host Firewalls

Securing Hosts with Cisco Security Agent

IPsec and SSL Virtual Private Networks

IP Security with IPv6

Host-to-Host IPsec

Site-to-Site IPsec Configuration

Remote Access with IPsec

SSL VPNs

Security for IPv6 Mobility

Mobile IPv6 Operation

MIPv6 Messages

Threats Linked to MIPv6

Using IPsec with MIPv6

Filtering for MIPv6

Other IPv6 Mobility Protocols

Securing the Transition Mechanisms

Attacking NAT-PT

IPv6 Latent Threats Against IPv4 Networks

Security Monitoring

Managing and Monitoring IPv6 Networks

Managing IPv6 Tunnels

Using Forensics

Using Intrusion Detection and Prevention Systems

Managing Security Information with CS-MARS

Managing the Security Configuration

IPv6 Security Conclusions

Comparing IPv4 and IPv6 Security

Changing Security Perimeter

Creating an IPv6 Security Policy

On the Horizon

List of Recommendations