IPv6 Security

Who Needs to Attend

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

Introduction

This course will provide the attendee with in-depth, hands-on, training on IPv6 security, such that the attendee is able to evaluate and mitigate the security implications of IPv6 in production environments and will learn how each feature of the IPv6 protocols and related technologies can be exploited for malicious purposes

Prerequisites

Participants are required to have a good understanding of the IPv4 protocol suite (IPv4, ICMP, etc.) and of related components (routers, firewalls, etc.). Additionally, the attendee is expected to have knowledge about basic IPv4 troubleshooting tools, such as: ping, traceroute, and network protocol analyzers (e.g., tcpdump)

Course Objectives

Upon completion of this training, you will:

- Understand IPv6 Protocols security concerns and features
- Have hands-on experience with applications used to secure IPv6 network against all kind of attacks
- Know the tools used to attack, to assess the protection of and to implement security on IPv6 networks

Course Duration

This would be a Four days course.

Detailed Course Outline

1. Introduction to IPv6 Security
    - 1.1 IPv6 Update
    - 1.2 Overview of IPv6 Vulnerabilities
    - 1.3 Introduction to IPv6 Mitigation Techniques
2. IPv6 Protocol Security Vulnerabilities
    - 2.1 IPv6 Protocol Header
    - 2.2 Extension Header Threats
    - 2.3 Reconnaissance on IPv6 Networks
    - 2.4 IPv6 Scanning
    - 2.5 IPv6 Spoofing
3. IPv6 Internet Security
    - 3.1 Large Scale Internet Threats
    - 3.2 DDOS and Botnets
    - 3.3 Ingress/Egress Filtering
    - 3.4 Securing BGP Sessions
    - 3.5 Prefix Delegation Threats
4. IPv6 Perimeter Security
    - 4.1 IPv6 Firewalls
    - 4.2 Cisco IOS Router ACLs

5. Local Network Security

    5.1 ICMPv6 Layer 2 Vulnerabilities for IPv6

    5.2 Detection and Mitigation against ICMPv6 attacks

    5.3 DHCPv6 Threats and Mitigation

6. Hardening IPv6 Network Devices

    6.1 Disabling Unnecessary Network Services

    6.2 Limiting Router Access

    6.3 IPv6 Device Management

    6.4 Threats Against Interior Routing Protocol

7. IPv6 in action

    7.1 IPSec and IPv6

    7.2 Security in IPv6 Mobility

8. Conclusion

    8.1 IPv6 Security Policy

    8.2 Comparison of IPv4 and IPv6 Security