Course ID
IPSEC
Course Duration
2-3 days

Course Title
IP Security v2 (IPSec v2) Architecture and Protocols

Related Courses

- Unified Communications in Public Safety, Law Enforcement, and Homeland Security (UNIFIED, 2-3 days)
- Communications Assistance to Law Enforcement Act (CALEA): Technologies and Compliance for TDM and Packet Voice Services (CALEA, 2-3 days)
- Emerging Communications and Technologies in Public Safety, Law Enforcement and Homeland Security (EMERGE-LAW, 2-3 days)
- Security, Privacy and Information Integrity for Managers Executives and Policy Makers (SECURITY-EXEC, 2-3 days)
- IEEE 802.11 (WiFi) Wireless LAN Security (WIFISEC, 3 days)
- Architecture and Operation of Wireless Networks for Technical Investigators: From Their Analog Origins to the Emerging 3G Technologies (WIRELESS-TI, 4-5 days)
- IP, Location and Geo-Location Technologies for Law Enforcement, Intelligence and Public Safety (IPGEOLOC, 2-3 days)
- IP Security v3 (IPSec v3) Workshop (IPSECWS, 2-3 days)
- Principles of Network Security: CompTIA Security+ and US DoD Directive 8570.1 (NETSEC, 3-4 days)
- SIP Security: A Comprehensive Short Course (SIPSEC, 2 days)
- Session Initiation Protocol (SIP) Workshop (SIPWS, 2-3 days)
- VoIP Security (VOIPSEC, 2 days)
- Voice Communications and Technologies for 911 Call Takers, Supervisors and Trainers (VOICE-911, 2-3 days)
- VoIP for 911 Administrators, Managers, Directors and Regulators (VOIP-911, 2-3 days)
- 911 for IP Professionals (911-IP, 2-3 days)

Aimed At

Technical professionals who implement, test, support, or trouble-shoot IPSec v2 and related protocols. The course will also benefit technical sales and sales support personnel needing a more in-depth understanding of IPSec v2 to support secure networks and the needs of certain government agencies.

Group Size

5-25

Prerequisites

To get the most out of the course, you should have a strong working knowledge of the IP protocol suite and an understanding of basic security concepts such as encryption, tunneling, and key management. These topics will be reviewed only briefly in this course.

Course In a Nutshell

This is an in-depth, heavily hands-on workshop on the technical aspects of IPSec v2 with special emphasis on protocols, implementation, and operations as described in RFC 2401 and 2412. It includes four protocol analyzer labs that will help you understand the internal workings of IPSec v2. The labs cover Layer 2 Tunneling Protocol version 3 (L2TPv3), Encapsulating Security Protocol (ESP), Authentication Header (AH), and Internet Key Exchange, and Internet Security Association Key Management Protocol (IKE/ISAKMP).

Customize It!

Customize this course to your group's requirements at little-to-no added cost. We can teach distinct versions of this course tailored for audiences such as network engineers and technicians, equipment/application designers, and less technical audiences such as managers, sales/marketing specialists, and operations/support personnel. The specific topics discussed in the course, as well as the depth of treatment for each, can also be tailored to your need.

Course Outline

Course Intro

- Overview
- ClearSight Analyzer
- Logistics and Labs
- Introductions

IPSec v2 Overview

- RFC 2401 and 2412
- Security and the OSI Model
- Crypto Building Blocks
  - Crypto Concepts
  - Keys and Key Management
  - Public/private Key Infrastructure
  - Key Recovery
- Tunnels and L2TPv3
- Virtual Private Networks (VPNs)
- IPSec Architectural Model

L2TPv3 Lab: View setup of an L2TPv3 tunnel and logical multimedia connections within the tunnel. Lab covers appropriate parts of PPP, L2TPv3, PAP and CHAP protocols.

LAB Debrief: Group Discussion

IP Security Overview

- Encapsulating Security Payload (ESP)
- Authentication Header (AH)
- Internet Key Exchange (IKE)

IPSec Architecture

- IETF IPSec v2 Roadmap
- IPSec Implementation
- IPSec Modes
  - Transport Mode
  - Transport Mode with NAT Traversal
  - Tunnel Mode
- Security Associations (SAs)
- IPSec Processing
  - Fragmentation
  - Internet Control Message Protocol (ICMP)

Encapsulating Security Payload (ESP)

- ESP Header
- ESP Modes
- ESP Procedures

ESP Lab: View call traces of encrypted network traffic using the Encapsulating Security Payload. Lab includes introduction to key cryptographic techniques.

LAB Debrief: Group Discussion

Authentication Header (AH)

- AH Header
- AH Modes
- AH Procedures

AH Lab: View call traces of traffic that uses the Authentication Header with and without Encapsulating Security Payload. Lab includes hacks against and countermeasures to ESP and AH security vulnerabilities.

LAB Debrief: Group Discussion

The Internet Key Exchange

- ISAKMP
- Public/private Key Exchange Systems
- Diffie-Hellman and Variations
- Internet Key Exchange (IKE)
- IPSec ISAKMP Domain of Interpretation (DOI)

IKE/ISAKMP Lab: View call traces of completed and aborted tunnel establishment and key exchanges using IKE and ISAKMP.

LAB Debrief: Group Discussion

Security Policy for IPSec

- Defining Policy
- Policy Representation and Distribution

- Policy Management System
- Policy Deployment

IPSec Implementation

- Implementation Architecture
- IPSec Protocol Procedures
- Fragmentation and Protocol Maximum Transmission Unit Length
- ICMP
- End-to-End Security View

Conclusion

How You Will Learn

- You will learn from an instructor who's well versed in a variety of IP and security protocols.
- Along with the lecture, we will use labs and group debriefs to enrich the instruction and drive home the important points.
- If you already know something about IPSec or security issues, we will build on that knowledge base. We'll compare and contrast what's familiar with what's new, making the new ideas easier to learn as well as more relevant.
- If your background is less technical, we will use examples and analogies to simplify the complex subject matter.
- The Participant Handbook will provide you with a record of the instructor's presentation to which you can you can add your own class notes. You will also receive a separate Laboratory Handbook based upon publically available protocol analyzer software.

Revised *May 7 2008f*