Course ID
IPSECWS
Course Duration
2-3 days

Course Title
IP Security v3 (IPsec v3) Workshop

Related Courses

- 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)
- 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)
- 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)

Aimed At

Security and networking professionals who need a deep understanding of IPSec v3, its implementation, vulnerabilities, countermeasures, and similarities to and differences from IP Sec v2.

Group Size

5-25

Prerequisites

- IP Security v2 (IPSec v2) Architectures and Protocols (IPSEC, 2-3 days)

You should have background in IPv4 and IPv6 and have taken the above course or possess equivalent knowledge/experience to fully benefit from this course.

Course In a Nutshell

This is a hands-on workshop, about two-thirds of which is labs. It builds on your understanding of IPSecv2, IPv4, and IPv6 to emphasize the enhancements and improvements that IPSecv3 brings to securing IPv4 and IPv6 networks.

Even though IPSecv2 is widely implemented at this time, considerations for initial implementations and migrations to IPSecv3 are underway in a number of government agencies, contractor organizations, and large corporations. The IPSec v1-v2-v3 timeline and suitability of IPSecv3 with both IPv4 and IPv6 will be

considered, as will a variety of technical topics that will be reinforced with individual hands-on lab exercises and group debrief discussions.

Customize It!

Customize this course to your group's requirements at little-to-no added cost. We can add or omit topics or labs, vary emphasis, and make the course more or less technical as required.

Course Outline

- Introduction
  - The Need for IPSec
  - IPSec Alternatives
  - IPSec Timeline: v1->v2->v3
    - IPSec
    - IPSecv2
    - IPSecv3
- IPSec RFC Overview
  - RFC 4301 Security Architecture for the Internet Protocol
  - RFC 4302 IP Authentication Header
  - RFC 4303 IP Encapsulating Security Payload
  - RFC 4304 Extended Sequence Number Addendum
  - RFC 4307 Cryptographic Algorithms for IKEv2
  - RFC 4308 Cryptographic Suites for IPSec
  - RFC 4309 Using Advanced Encryption Standard with ESP
  - RFC 4478 Repeated Authentication in IKEv2
  - RFC 4543 GMAC in IPSec ESP and AH
  - RFC 4555 IKEv2 Mobility and Multihoming Protocol (MOBIKE)
  - RFC 4621 Design of the IKEv2 Mobility and Multihoming (MOBIKE) Protocol
  - RFC 4718 IKEv2 Clarifications and Implementation Guidelines
  - RFC 4806 Online Certificate Status Protocol (OCSP) Extensions to IKEv2
  - RFC 4809 Requirements for an IPSec Certificate Management Profile
  - RFC 4945 PKI Profile of IKEv1/ISAKMP, IKEv2, and PKIX
- IPSec v3: Security Architecture for the Internet Protocol
  - Security Policy Database (SPD)
  - Security Association Database (SAD)
  - Peer Authorization Database (PAD)
  - Security Associations
    - Key Management
    - Multicast
  - IP Traffic Processing
  - ICMP Processing
  - Other Issues
  - Differences from RFC 2401
- Authentication Header (AH)

- Format and Structure
- Fields
- Galois Message Authentication Code (GMAC)
- ***GMAC Lab:***
  - ***Study operation of Message Authentication Codes in general and attributes and operation of GMAC code used in IPSecv3 specifically***
  - ***LAB debrief/group discussion***
- IP Packet Processing
- Differences from RFC 2402
- ***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***

- Encapsulating Security Payload (ESP)
  - Format and Structure
  - Fields
  - Advanced Encryption Standard (AES) with ESP
  - ***AES Lab***
    - ***Step through AES encryption procedure as a paper exercise and review possible attacks and countermeasures***
    - ***LAB debrief/group discussion***
  - IP Packet Processing
  - Differences from RFC 2406
  - ***ESP Lab***
    - ***View call traces of encrypted network traffic using the Encapsulated Security Payload***
    - ***Lab debrief/group discussion***
- IKEv2 and ISAKMP
  - Extended Sequence Number Addendum
  - Cryptographic Algorithms for IKEv2
  - Repeated Authentication in IKEv2
  - IKEv2 Mobility and Multihoming Protocol (MOBIKE)
  - Design of the IKEv2 Mobility and Multihoming (MOBIKE) Protocol
  - ***MOBIKE Lab***
    - ***Sample design and security specification exercise with implementation checklist for MOBIKE system***
    - ***Lab debrief and group discussions***
  - IKEv2 Clarifications and Implementation Guidelines
  - Online Certificate Status Protocol (OCSP) Extensions to IKEv2
  - Requirements for an IPsec Certificate Management Profile
  - PKI Profile of IKEv1/ISAKMP, IKEv2, and PKIX
  - ***IKEv1 and v2/ISAKMP Lab***

        - ***View call traces of completed and aborted tunnel establishment and key exchange using IKE v1 and v2 and ISAKMP***
        - ***Lab debrief and discussion***
- Cryptographic Suites for IPSec
    - Suite "VPN-A"
        - ESP - RFC2406
        - TripleDES in CBC mode [RFC2451]
        - HMAC-SHA1-96 [RFC2404]
        - IKE and IKEv2:
        - Diffie-Hellman 1024-bit Modular Exponential (MODP) [RFC2409]
    - Suite "VPN-B"
        - ESP [RFC2406]
        - AES with 128-bit Keys in CBC mode [AES-CBC]
        - AES-XCBC-MAC-96 [AES-XCBC-MAC]
        - AES-XCBC-MAC-96 [AES-XCBC-MAC]
        - IKE and IKEv2
        - Diffie-Hellman 2048-bit MODP [RFC3526]
    - ***Cryptographic Suite Exercise***
        - ***This exercise is a group exercise covering the pros, cons and trade-offs of standard and non-standard cryptographic suites and issues of security vs vulnerability that come with the large number of possible combinations of IPSec protocol options, ESP encryption and integrity and IKE and IKEv2 encryption, pseudo-random functions, integrity and Diffie-Hellman groups***
        - ***Lab debrief/group discussion***
- Conclusion
    - IPSecv4? and Future of IPSec

How You Will Learn

- You will learn from an instructor who's well versed in a variety of IP and security protocols. The course will be taught workshop style.
- Along with the lecture, we will use labs and group debriefs to enrich the instruction and drive home the important points.
- 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.

Website: www.eogogics.com
E-mail: sales@eogogics.com
Tel. +1 (703) 281-3525
Fax +1 (866) 612-6896