

Enterprise Wi-Fi Security, (CWSP)

Course Summary

Description

The Enterprise Wi-Fi Security 4.0 course provides the wireless security professional a complete foundation of knowledge for entering into or advancing in the wireless security industry. From small/medium business (SMB) to enterprise-class wireless security, this course delivers hands-on training that will benefit the administrator as well as the security consultant.

Topics

- Introduction to WLAN Security Technology
- Legacy Security and Network Attacks
- Security Policy
- Authentication
- RSN Authentication and Key Management (AKM)
- Encryption
- Remote Networking & Public Access
- Fast BSS Transition
- Network Monitoring, Intrusion Prevention, and Analysis

Audience

This course is designed for Administrators, Consultants, and Architects.

Prerequisites

Students should have basic networking knowledge (OSI / IP). Basic network security concepts and wireless network administration CWNA or equivalent knowledge.

Duration

Four days

Enterprise Wi-Fi Security, (CWSP)

Course Outline

I. Introduction to WLAN Security Technology

- A. Security Basics
- B. CWNA Security Review
- C. Industry Organizations
- D. Terminology
- E. Wireless Vulnerabilities

II. Legacy Security and Network Attacks

- A. Network Discovery
- B. Pseudo-security
- C. Legacy Security Mechanisms
- D. Network Attacks
- E. Recommended Practices

III. Security Policy

- A. Legal Considerations
- B. General Security Policy
- C. Functional Security Policy
- D. Network Audits and Penetration Testing

IV. Authentication

- A. Passphrase Authentication
- B. AAA
- C. RBAC
- D. RADIUS
- E. 802.1X
- F. EAP

V. RSN Authentication and Key Management (AKM)

- A. Robust Security Networks
- B. RSN Information Element
- C. RSN Authentication and Key Management (AKM)

VI. Encryption

- A. Encryption Fundamentals
- B. Encryption Algorithms
- C. WEP
- D. TKIP
- E. CCMP

VII. Remote Networking & Public Access

- A. Virtual Private Networks (VPN)
- B. Remote Networking
- C. Guest Access Networks

VIII. Fast BSS Transition

- A. Roaming Basics and Terminology
- B. Pre-authentication
- C. PMK Caching
- D. Opportunistic Key Caching (OKC)
- E. 802.11r FT
- F. Proprietary Roaming
- G. Voice Enterprise

IX. Network Monitoring, Intrusion Prevention, and Analysis

- A. Wireless Intrusion Prevention Systems (WIPS)
- B. WIPS Deployment Models
- C. WIPS Policy
- D. Threat Mitigation
- E. Location Services
- F. WNMS
- G. Protocol Analysis
- H. Spectrum Analysis