Class Outline

Certified Wireless Security Professional (CWSP)

Objectives

- Describe WLAN Discovery Techniques
- Understand Intrusion and Attack Techniques
- Explain 802.11 Protocol Analysis
- Understand Network Security Design Models
- Explain How to Build a Robust Security Network from the Ground Up
- Understand Authentication and Key Management Protocols
- Understand Wireless LAN Management Systems
- Define 802.11 Design Architectures

Pre-Requisite Knowledge Advisory

- Basic Wireless LAN Literacy

Exam

- CWSP-206
- Proctor: PearsonVUE
- Renewal: 3 years

Class Outline

Module 1 – Security Fundamentals

- Security Basics
- CWNA Security Review
- Industry Organizations
- Terminology
- Wireless Vulnerabilities

Module 2 – Wireless Security Challenges

- Network Discovery
- Pseudo-Security
- Legacy Security Mechanisms
- Network Attacks
- Recommended Practices

Module 3 – Security Policy

- Defining Security Policies
- Policy Enforcement
- Policy Management
- Policy Types

Module 4 – Understanding Authentication

- Passphrase Authentication
- AAA
- RBAC
- RADIUS
- 802.1X
- EAP

Module 5 – Authentication and Key Management

- Robust Security Networks (RSN)
- RSN Information Element
- RSN Authentication Key Management (AKM)

Module 6 – Encryption

- Encryption Fundamentals
- Encryption Algorithms
- WEP
- TKIP
- CCMP

Module 7 – Security Design Scenarios

- Virtual Private Networks (VPN)
- Remote Networking
- Guest Access Networks

Module 8 – Secure Roaming

- Roaming Basics and Terminology
- Preauthentication
- PMK Caching
- Opportunistic Key Caching (OKC)
- 802.11r FT
- Proprietary Roaming
- Voice Enterprise

Module 9 – Network Monitoring

- Wireless Intrusion Prevention Systems (WIPS)
- WIPS Deployment Models
- WIPS Policy
- Threat Mitigation
- Location Services
- WNMS
- Protocol Analysis
- Spectrum Analysis

Module 10 – WPA3 and OWE

- WPA3 Defined
- WPA3 vs. WPA2
- WPA3-SAE Personal
- WPA3 Enterprise
- OWE

Module 11 – Penetration Testing Principles

- Process Phases
- Strategy
- Reporting
- Vulnerabilities
- Oversight
- Risk Theory
- Tools and Techniques
- Hardware and Software