CWSP – Certified Wireless Security Professional

Days: 4

Description: Using the latest enterprise wireless LAN security and auditing equipment in this hands-on course, learn, in detail, the most up-to-date WLAN intrusion and DoS tools and techniques. You will learn about functionality of the 802.11i amendment to the 802.11 standard, the inner-workings of each EAP type used with wireless LANs today, and every class and type of WLAN security solution available on the market from wireless intrusion prevention systems to wireless network management systems. As an added bonus, you will receive a free exam voucher.

Course Objectives:

- WLAN security technology and solutions
- WLAN security policy, concerns, and auditing practices
- Layer vulnerabilities and analysis
- WLAN mobile endpoint security solutions
- WPA/WPA2 Personal and Enterprise configurations
- WLAN management and monitoring
- IEEE 802.11 Authentication and Key Management (AKM)

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 and Key Management (AKM)

MODULE 6 – ENCRYPTION

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

CWSP – Certified Wireless Security Professional

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