Enterprise Wi-Fi Security

Duration: 4 Days Course Code: CWSP Delivery Method: Virtual Learning

Overview:

The Certified Wireless Security Professional course covers the Security aspects of Wireless Networking. In this class, students are taught about various forms of Security Technologies, Management, and Monitoring.
The Certified Wireless Security Professional (Wireless LAN Security) training course demonstrates the latest enterprise wireless LAN security and auditing equipment. This class addresses the state-of-the-art WLAN intrusion and DoS tools and techniques. It also investigates the functionality of the 802.11i amendment to the 802.11 standard and the inner-workings of each EAP type used with wireless LANs today, along with every class and type of WLAN security solution available on the market ~ from wireless intrusion prevention systems to wireless network management systems.
This course addresses, in detail, the most important and relevant WLAN security protocols, exchanges, and deployment strategies. The class focuses heavily on understanding the functionality of the 802.11i amendment, including authentication, encryption, and key management. 802.1X and EAP are also central to this class, with an in-depth examination of each authentication mode and EAP type used in wireless LANs today.
Other infrastructure security solutions are also discussed, such as role-based access control, segmentation, VPNs, firewalls, wireless intrusion prevention and monitoring, secure roaming, and network management. The Wireless LAN Security course consists of hands on learning using the latest enterprise wireless LAN security and auditing equipment.
Students who complete the course will be exposed to the necessary skills for implementing and managing wireless security in an enterprise environment, by creating layer2 and layer3 hardware and software solutions utilizing industry leading manufacturers' equipment.
Main Areas Covered by CWSP:
- Network Security Design Models
- Building Robust Security Networks
- Wireless LAN Management Systems
- 802.11 Design Architectures

Virtual Learning

This interactive training can be taken from any location, your office or home and is delivered by a trainer. This training does not have any delegates in the class with the instructor, since all delegates are virtually connected. Virtual delegates do not travel to this course, Global Knowledge will send you all the information needed before the start of the course and you can test the logins.

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 Managemnt Protocols
- Understand Wireless LAN Management Systems
- Define 802.11 Design Architectures

Prerequisites:

Basic Wireless LAN Literacy

Current Certified Wireless Network Administration (CWNA) Certification

Testing and Certification

CWNP CWSP-205

Proctored Exam 90 minutes (60 questions: multiple choice)

Exam Proctor: PearsonVUE

Recertification: 3 years

Content:

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

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

Further Information:

For More information, or to book your course, please call us on +1 (800) 268 7737

ilt.customerservice@globalknowledge.com

www.globalknowledge.com/en-us/

Global Knowledge Training LLC, 103 Foulk Road, Suite 202, Wilmington, Delaware, 19803