THINQTANK® LEARNING

CERTIFIED WIRELESS NETWORK PROFESSSIONAL
CWNP Certified Wireless Security Professional (CWSP)

Our Learning Exclusive

- Custom exam prep software and materials
- Exam delivery in classroom with 98% success
- Course specific thinQtank® Learning publications to promote fun exciting learning
- Extended hours of training including immersive hands-on exercises
- WE DO NOT "TEACH THE TEST" We always deliver valuable hands-on experience
- Receive all reading material and study guides when you register
- All courses taught by CWNE expert instructors

Course Duration

- Five days of instructor-led training
- 50% lecture, 50% hands-on labs

Prerequisites

- CWNA Certification or the equivalent in knowledge and experience.
- Candidate must pass the CWNA certification exam (CWNA-106) as well as the CWSP certification exam (CWSP-205) to achieve certified status

Target Audience

- Network and system administrators, consultants and engineers that need to support Wireless LAN deployments
- Infrastructure security professionals

Exam Information

- CWSP-205 – Certified Wireless Security Professional

Delivery Methods

- Instructor-Led Training
- Immersive Live-Online Training
- On-Site and Custom Delivery

Exclusive Toolkit and Pen Test Lesson

- Wi-Fi penetration testing kit
- USB WLAN adaptor for packet sniffing and injection with a high-gain antenna
- USB Spectrum Analyzer with fully licensed metageek software
- Custom Linux build for WLAN penetration testing

BONUS LEARNING MODULE

- Four hour WLAN security and penetration testing lesson

Course Overview

thinQtank® Learning offering a unique five-day training camp in which students can receive the highly sought after CWSP certification in one week. As with all of our Advanced Training Experiences – exams are delivered in the classroom.

The Wireless LAN Security course consists of hands on learning using the latest enterprise wireless LAN security and auditing equipment. This course addresses in detail the most up-to-date WLAN intrusion and DoS tools and techniques, 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.

Students who complete the course will acquire the necessary skills for implementing and managing wireless security in the enterprise by creating layer2 and layer3 hardware and software solutions with tools from the industry leading manufacturers.

This course is excellent preparation for the challenging CWSP Certification, and includes practice exams. It is also very hands-on intensive, roughly 50% hands-on, with lots of time to get your hands on real equipment to perform actual Site Survey work.

Course Objectives

During this course, you will develop skills and knowledge on the following:

- WLAN Discovery Techniques
- Intrusion and Attack Techniques
- 802.11 Protocol Analysis
- Wireless Intrusion Prevention Systems (WIPS) Implementation
- Layer 2 and 3 VPNs used over 802.11 networks
- Enterprise/SMB/SOHO/Public-Network Security design models
- Managed Endpoint Security Systems802.11 Authentication and Key Management Protocols
- Enterprise/SMB/SOHO/Public Security Solution Implementation
- Building Robust Security Networks from the ground up
- Fast BSS Transition (aka. Fast/Secure Roaming) Techniques
- Thorough coverage of all 802.1X/EAP types used in WLANs
- Wireless LAN Management Systems (WNMS)
- Authentication Infrastructure Design Models
- Using Secure Applications
- 802.11 Design Architectures
- Implementing a Thorough Wireless Security Policy

CERTIFIED WIRELESS NETWORK PROFESSSIONAL
CWNP Certified Wireless Security Professional (CWSP)

CWSP Course Modules

1 Introduction to WLAN Security Technology
- Security policy
- Security concerns
- Security auditing practices
- Application layer vulnerabilities and analysis
- Data Link layer vulnerabilities and analysis
- Physical layer vulnerabilities and analysis
- 802.11 security mechanisms
- Wi-Fi Alliance security certifications

2 Small Office / Home Office WLAN Security Technology and Solutions
- WLAN discovery equipment and utilities
- Legacy WLAN security methods, mechanisms, and exploits
- Appropriate SOHO security

3 WLAN Mobile Endpoint Security Solutions
- Personal-class mobile endpoint security
- Enterprise-class mobile endpoint security
- User-accessible and restricted endpoint policies
- VPN technology overview

4 Branch Office / Remote Office WLAN Security Technology and Solutions
- General vulnerabilities
- Preshared Key security with RSN cipher suites
- Passphrase vulnerabilities
- Passphrase entropy and hacking tools
- WPA/WPA2 Personal – how it works
- WPA/WPA2 Personal – configuration
- Wi-Fi Protected Setup (WPS)
- Installation and configuration of WIPS, WNMS, and WLAN controllers to extend enterprise security policy to remote and branch offices

5 Enterprise WLAN Management and Monitoring
- Device identification and tracking
- Rogue device mitigation
- WLAN forensics
- Enterprise WIPS installation and configuration
- Distributed protocol analysis
- WNMS security features
- WLAN controller security feature sets

6 Enterprise WLAN Security Technology and Solutions
- Robust Security Networks (RSN)
- WPA/WPA2 Enterprise – how it works
- WPA/WPA2 Enterprise – configuration
- IEEE 802.11 Authentication and Key Management (AKM)
- 802.11 cipher suites
- Use of authentication services (RADIUS, LDAP) in WLANs
- User profile management (RBAC)
- Public Key Infrastructures (PKI) used with WLANs
- Certificate Authorities and x.509 digital certificates
- RADIUS installation and configuration
- 802.1X/EAP authentication mechanisms
- 802.1X/EAP types and differences
- 802.11 handshakes
- Fast BSS Transition (FT) technologies

CERTIFIED WIRELESS NETWORK PROFESSSIONAL
CWNP Certified Wireless Security Professional (CWSP)

CWSP Lab Exercises

1 WLAN Controller Security

- Secure access to the WLAN controller using secure management protocols
- Configuring multiple WLAN profiles, each with its own authentication and cipher suites including WPA/WPA2 Personal and Enterprise
- Configuring the WLAN controller for RADIUS connectivity and authentication
- Client station connectivity to the controller – including DHCP and browsing
- Integrated rogue device discovery

2 Wireless Intrusion Prevention Systems (WIPS)

- WIPS installation, licensing, adding/configuring sensors, and secure console connectivity
- Configuration according to organizational policy
- Properly classifying authorized, unauthorized, and external/interfering access points
- Identifying and mitigating rogue devices
- Identifying specific attacks against the authorized WLAN infrastructure or client stations

3 Using Laptop Analyzers

- Installing and configuring a WLAN discovery tool
- Installing, licensing, and configuring a laptop protocol analyzer
- Installing, licensing, and configuring a laptop spectrum analyzer
- Locating and analyzing 2.4 GHz and 5 GHz WLANs with a WLAN discovery tool
- Locating and analyzing 2.4 GHz and 5 GHz WLANs with a WLAN protocol analyzer
- Capturing and analyzing a WPA2-Personal authentication in a WLAN protocol analyzer
- Capturing and analyzing a WPA2-Enterprise authentication in a WLAN protocol analyzer
- Capturing and analyzing Hotspot authentication and data traffic in a WLAN protocol analyzer
- Capturing and analyzing Beacons, Probe Requests, Probe Responses, and Association Requests with a WLAN protocol analyzer
- Viewing a normal RF environment, a busy RF environment, and an RF attack on the WLAN in a spectrum analyzer

4 Fast Secure Roaming

- Configure a WLAN infrastructure with two controllers and two APs per controller. Configure APs for specific power and channel settings
- Install and configure a RADIUS server for PEAP
- Configure both controllers and an authorized client device for PEAP authentication using the CCMP cipher suite
- Configure an 802.11 protocol analyzer to capture the BSS transition
- Perform a slow BSS transition within a controller as a baseline
- Enable FSR mechanisms within controllers and the client station
- Perform a fast BSS transition within a controller as a comparison
- Perform a slow BSS transition between controllers as a baseline
- Perform a fast BSS transition (if vendor FSR mechanisms permit) between controllers as a comparison

CERTIFIED WIRELESS NETWORK PROFESSSIONAL
CWNP Certified Wireless Security Professional (CWSP)

thinQtank® Global, Inc. dba thinQtank® Learning P.O. Box 803215, Valencia, CA 91380 USA
Tel 855-TO-THINQ Fax 208-979-0668 www.thinqtanklearning.com