# CERTIFIED WIRELESS SECURITY PROFESSIONAL (CWSP)

Course Code: 3604

Learn to install and configure wireless networks for optimal security.

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 and practice test to test your knowledge before taking the exam.

## Who Needs to Attend

Wireless professionals looking to gain cutting-edge wireless security expertise and earn the CWSP credential should attend.

# CERTIFIED WIRELESS SECURITY PROFESSIONAL (CWSP)

Course Code: 3604

| CLASSROOM LIVE | $4,251 CAD | 4 Day |
| --- | --- | --- |

## Classroom Live 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

## 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

## Classroom Live Labs

### Lab 1: WLAN Controller Security

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

### Lab 2: Wireless Intrusion Prevention Systems (WIPS)

- WIPS installation, licensing, add/configure sensors, and secure console

connectivity
- Configuration according to organizational policy
- Properly classify authorized, unauthorized, and external/interfering access points
- Identify and mitigate rogue devices
- Identify specific attacks against the authorized WLAN infrastructure or client stations

**Lab 3: Using Laptop Analyzers**

- Install and configure a WLAN discovery tool
- Install, license, and configure a laptop protocol analyzer
- Install, license, and configure a laptop spectrum analyzer
- Locate and analyze 2.4 GHz and 5 GHz WLANs with a WLAN discovery tool
- Locate and analyze 2.4 GHz and 5 GHz WLANs with a WLAN protocol analyzer
- Capture and analyze a WPA2 Personal authentication in a WLAN protocol analyzer
- Capture and analyze a WPA2 Enterprise authentication in a WLAN protocol analyzer
- Capture and analyze Hotspot authentication and data traffic in a WLAN protocol analyzer
- Capture and analyze beacons, probe requests, probe responses, and association requests with a WLAN protocol analyzer
- View a normal RF environment, a busy RF environment, and an RF attack on the WLAN in a spectrum analyzer

**Lab 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 SECURITY PROFESSIONAL (CWSP)

Course Code: 3604

| VIRTUAL CLASSROOM LIVE | $4,251 CAD | 4 Day |
|---|---|---|

Virtual Classroom Live 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

## 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

## Virtual Classroom Live Labs

### Lab 1: WLAN Controller Security

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

### Lab 2: Wireless Intrusion Prevention Systems (WIPS)

- WIPS installation, licensing, add/configure sensors, and secure console

connectivity
- Configuration according to organizational policy
- Properly classify authorized, unauthorized, and external/interfering access points
- Identify and mitigate rogue devices
- Identify specific attacks against the authorized WLAN infrastructure or client stations

## Lab 3: Using Laptop Analyzers

- Install and configure a WLAN discovery tool
- Install, license, and configure a laptop protocol analyzer
- Install, license, and configure a laptop spectrum analyzer
- Locate and analyze 2.4 GHz and 5 GHz WLANs with a WLAN discovery tool
- Locate and analyze 2.4 GHz and 5 GHz WLANs with a WLAN protocol analyzer
- Capture and analyze a WPA2 Personal authentication in a WLAN protocol analyzer
- Capture and analyze a WPA2 Enterprise authentication in a WLAN protocol analyzer
- Capture and analyze Hotspot authentication and data traffic in a WLAN protocol analyzer
- Capture and analyze beacons, probe requests, probe responses, and association requests with a WLAN protocol analyzer
- View a normal RF environment, a busy RF environment, and an RF attack on the WLAN in a spectrum analyzer

## Lab 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 SECURITY PROFESSIONAL (CWSP)

Course Code: 3604

| PRIVATE GROUP TRAINING | 4 Day |
|---|---|

Visit us at www.globalknowledge.com or call us at 1-866-716-6688.