Certified Wireless Security Professional Course

Category: Networking & Security | **Vendor:** CWNP

Duration: 24.00 hours (3 days) **19.5 CPD Hours** **Rating:** ⭐ 4.6 (5,878 reviews)

Course Information

Delivery Format:	Instructor Led - Online
Certification:	Certified Wireless Security Professional (CWSP)
Related Exam:	CWSP-208

Course Overview

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 and “Exam Cram” sessions. 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.

This intensive course covers all that is required to prepare for the CWNA Certification, including:

- hands-on training
- Official CWSP practice test questions
- Exam voucher for the CWSP Certification Exam (# PW0-204)
- Mentor support after class by our Wireless Expert team

It also ensures that students leave with real hands on skills. Hands-on exercises include the following:

- WLAN Controller Security
- Wireless Intrusion Prevention Systems (WIPS)
- WLAN infrastructure or client stations
- Using Laptop Analyzers
- Fast Secure Roaming

About This Course

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 and “Exam Cram” sessions. 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.

This intensive course covers all that is required to prepare for the CWNA Certification, including:

- hands-on training
- Official CWSP practice test questions
- Exam voucher for the CWSP Certification Exam (# PW0-204)
- Mentor support after class by our Wireless Expert team

It also ensures that students leave with real hands on skills. Hands-on exercises include the following:

- WLAN Controller Security
- Wireless Intrusion Prevention Systems (WIPS)
- WLAN infrastructure or client stations
- Using Laptop Analyzers
- Fast Secure Roaming

Who Should Attend

This intensive, 5 day course is intended for network and system administrators, consultants and engineers that need to support Wireless LAN deployments.

It also is a great course for all infrastructure security professionals

Prerequisites & Entry Requirements

General Prerequisites:

The Following prerequisite knowledge and skills are suggested prior to attending the CWSP Course:

- CWNA Certification or the equivalent in knowledge and experience.
- Note that CWSP Certification does require that the candidate pass the CWNA certification exam (PW0-104) as well as the CWSP certification exam (PW0-204) in order to achieve certified status.

Learning Outcomes

Upon successful completion of this course, participants will be able to:

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

- 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-Network Security Solution Implmentation
- 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

Detailed Course Outline

Hands-On Lab Exercises:

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

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

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

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

Course Outline

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

Small Office / Home Office WLAN Security Technology and Solutions

- WLAN discovery equipment and utilities
- Legacy WLAN security methods, mechanisms, and exploits
- Appropriate SOHO security

WLAN Mobile Endpoint Security Solutions

- Personal-class mobile endpoint security
- Enterprise-class mobile endpoint security
- User-accessible and restricted endpoint policies
- VPN technology overview

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

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

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

□□ Certification Path

Certified Wireless Security Professional (CWSP)

Exam: CWSP-208

Skills You Will Learn:

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

- 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-Network Security Solution Implmentation
- 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

Frequently Asked Questions

Q: What delivery options are available for Certified Wireless Security Professional Course?

We offer multiple delivery formats:

- Live Instructor-Led Classroom Online (Virtual/Live Online)
- Traditional Instructor-Led Classroom Training (ILT)
- On-site delivery at your offices anywhere in United Kingdom
- Private dedicated courses customized for your team

Q: What certification does this course prepare me for?

The Certified Wireless Security Professional Course course helps prepare you for the Certified Wireless Security Professional (CWSP) certification path.

Q: Which exam does this course prepare me for?

This course prepares you for the CWSP-208 official exam. You can take this exam at any exam center across United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online wherever you are located.

Q: How many CPD hours does this course provide?

The 3-day Certified Wireless Security Professional Course course provides up to 19.5 CPD hours of structured learning. CPD certificates can be provided upon request.

Q: What is the duration of the Certified Wireless Security Professional Course training?

The training takes place over 3 day(s), with each day lasting approximately 24.00 hours including breaks for lunch and refreshments.

Q: Do you provide corporate training for Certified Wireless Security Professional Course?

Yes, we provide corporate training, dedicated training, and closed classes for Certified Wireless Security Professional Course. Training can take place anywhere in United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online allowing teams from across United Kingdom or internationally to attend.

Q: What related terms do people search for?

Popular related searches include: Certified Wireless Security Professional Course, Professional Level, CWSP

Q: Why choose Nexus Human for Certified Wireless Security Professional Course?

Nexus Human is recognized as one of the leading training providers. Our trainers have won multiple awards including:

- Small Firms Best Trainer Award
- National Training Partner of the Year (Ireland) - Multiple Years
- Global Top 30 Instructor Awards (2012, 2019, 2021)
- Tech Excellence Award Nominations
- Learning Performance Institute (LPI) External Training Provider Sponsor 2024

Q: Are there any discount codes available?

Yes! Use discount code **PENPAL5** when booking your Certified Wireless Security Professional Course training. Please note that only one discount code can be used per booking and cannot be combined with other special offers.

Nexus Human

Professional Training & Development

Email: info@nexushuman.com

Website: www.nexushuman.com

Phone: +353 1 889 8700 (Ireland) | +44 20 8142 8961 (UK)

© 2026 Nexus Human. All rights reserved. This brochure was generated on 14/11/2026.