

Register Early. Get Rewarded!

Make sure to ask about our Early Bird Pricing if you register 60 days in advance.

Intense School's CWSP (Wireless Security) Boot Camp



The perfect blend of exam prep success and INTENSE HANDS-ON Wireless Fun!!

Intense School's CWSP (Wireless Security) Boot Camp is a 5 day in-depth course that teaches students the imperative safeguards against the potential threat of intrusion upon wireless local area networks (WLANs). This concentrated Wireless Network Security course is designed to provide thorough and precise hands-on training on how to construct and incorporate WLANs into an existing setting in order to maintain the most powerful security.



www.intenseschool.com
866.365.8401

©2000-2009 Viglar, Inc. All Rights Reserved.

Intense School's CWSP (Wireless Security) Boot Camp

CWSP (Wireless Security) Boot Camp – Course Description

Intense School offers you its Certified Wireless Network Security Professional (CWSP) Boot Camp, a five (5) day in-depth course that teaches students the imperative safeguards against the potential threat of intrusion upon wireless local area networks (WLANs). Our concentrated Wireless Network Security course is designed to provide thorough and precise hands-on training on how to construct and incorporate WLANs into an existing setting in order to maintain the most powerful security.

Students of Intense School CWSP Boot Camp learn the important attributes of the primary wireless vendors while participating in review sessions and labs to successfully prepare students for their Certified Wireless Security Professional exam.

Course Objectives

Upon the completion students will learn:

- Risk Assessment
- Threat Analysis & Hacking Methodology
- Rudimentary security measures
- Intermediate Security Measures
- Advanced Security Measures
- Wireless LAN Auditing Tools
- Hardware & Software Solutions
- Prevention & Countermeasures
- Implementation and Management
- Attain a well-respected Planet 3 Wireless certification (CWSP)
- And much, much more!

Why to “Get Intense” for CWSP training

- Award-winning Authors deliver the course
- Training on Wireless since 2001
- We are 80% hands-on!
- Tips and Tricks from the Pros
- We have a 95%+ pass rate across our classes

CWSP (Wireless) Boot Camp - Course Benefits and Goals

Our (5) day intense CWSP Boot Camp provides the most comprehensive approach to CWSP certification. This is an accelerated immersion course, designed for computer professionals that require effective, real-world skill-building and timely certification.

Only Intense School's CWSP Boot Camp offers you the following benefits:

- Intense School definitive, total immersion training experience
- Five (5) full days of intense instruction, labs and review with an Expert CWSP Instructor
- Hands-on practice and skills development on a wide range of Wireless hardware and software
- Pre and post mentoring by top rated CWSP Expert instructors
- Learn how to design, configure, implement and troubleshoot wireless networks from the ground up
- Prep to certify as a Certified Wireless Network Administrator
- Courseware includes:
 - CWSP Official Courseware
 - Pre-class shipment of Sybex's CWSP: Certified Wireless Network Security Professional Study Guide (Exam PW0-200)
 - 1 CWSP (Exam PW0-200) exam voucher
 - Exceptional Practice Exams

Intense School's Authorized CWSP (Wireless Security) Boot Camp

Intense School Pre-Class Preparation

Prior to class you'll also receive

- Pre-class shipment of Sybex's CWSP: Certified Wireless Network Security Professional Study Guide (Exam PWO-100)
- Access to a qualified CWSP expert mentor before and after class, providing you extra help upon request to guide you towards proper pre-class prep!

Certified Professional Exams

Intense School's CWSP (Wireless) Boot Camp comprehensively prepares students for the following certified exam:

- Planet 3's CWSP Certified Wireless Network Security Professional (PWO-100) exam

Prerequisites

Prior to enrolling in Intense School's CWSP Boot Camp, students should have a valid CWNA Certification, and experiences commiserate with a CWNA. Students should also have exposure to Information Security, either appropriate training on Information Security fundamentals or hands-on experience.

Who Should Attend

Network Administrators and Engineers, Security Administrators and Engineers, Internetworking professionals.

Intense School's CWSP Cutting-Edge Technology

Intense School's CWSP Program is more Hands-on Intensive than any other program on the market. Roughly **80%** of the training is through hands-on experience on real systems, guided by a CWSP expert.

The CWSP 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 following industry leading manufacturers:

Colubris Networks
Cisco Systems
Bluesocket
Aruba Networks
Motorola/Symbol
Fortress Technologies

Trapeze Networks
Xirrus Networks
TamoSoft
WildPackets
Network Chemistry
AirTight Networks

AirDefense
AirMagnet
Periodik Labs
Juniper Networks
Microsoft
Van Dyke Software

Intense School's CWSP (Wireless Security) Hands-on Labs

These are the actual labs taught in the course:

WLAN Controller Security

The WLAN controller is currently the center piece of 802.11 security. All other pieces of the WLAN security puzzle orbit around the WLAN controller. For this reason, gaining an in-depth understanding of how to secure access to the controller and how to use the controller to secure the WLAN is essential.

This lab is focused on WLAN controller security, and primarily covers the following areas:

1. Secure access to the WLAN controller using secure management protocols
2. Configuring multiple WLAN profiles with authentication and cipher suites including WPA/WPA2 Enterprise
3. Configuring the WLAN controller for RADIUS connectivity and authentication
4. Client station connectivity to the controller - including DHCP and browsing
5. Integrated rogue device discovery

Wireless Intrusion Prevention Systems (WIPS)

This lab is focused on Wireless Intrusion Prevention Systems (WIPS). WIPS are known for three overriding functions: security monitoring, performance monitoring, and reporting. In this lab exercise, we will focus only on security monitoring and reporting. Areas of particular interest include:

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

Using Laptop Analyzers

This lab is focused on the use of laptop analyzers for spectrum analysis, protocol analysis, and WLAN discovery. Understanding driver issues, security-related protocol analysis (authentication and encryption), and spectrum analysis will aid the wireless security professional in policy compliance, proper implementation, and troubleshooting. The following steps will be covered in this lab exercise.

1. Installing and configuring a WLAN discovery tool
2. Installing, licensing, and configuring a laptop protocol analyzer
3. Installing, licensing, and configuring a laptop spectrum analyzer
4. Locating and analyzing 2.4 GHz and 5 GHz WLANs with a WLAN discovery tool
5. Locating and analyzing 2.4 GHz and 5 GHz WLANs with a WLAN protocol analyzer
6. Capturing and analyzing a WPA2-Personal authentication in a WLAN protocol analyzer
7. Capturing and analyzing a WPA2-Enterprise authentication in a WLAN protocol analyzer
8. Capturing and analyzing Hotspot authentication and data traffic in a WLAN protocol analyzer
9. Capturing /analyzing Beacons, Probe Requests, Probe Responses with a WLAN protocol analyzer
10. Viewing a normal RF environment, a busy RF environment, and an RF attack on the WLAN in a spectrum analyzer

Fast BSS Transitions (FT)

This lab is focused on fast BSS transition (FT) within an Extended Service Set. Moving quickly and securely between access points attached to a single controller or multiple controllers is a requirement of real-time mobility devices such as wVoIP phones and mobile video devices. An in-depth understanding of the standards-based and proprietary processes of a WLAN infrastructure system's ability to deliver FT services means the difference between a successful deployment and a complete failure. The following steps will be covered in this lab exercise:

1. Configure WLAN with two controllers and two APs per controller. Configure APs power/channel settings
2. Install and configure a RADIUS server for PEAP
3. Configure both controllers and an authorized client device for PEAP authentication using the CCMP cipher suite
4. Configure an 802.11 protocol analyzer to capture on a specific channel
5. Using 802.11 frame generator function, deauthenticate to force intra- and inter-controller roaming
6. Perform a slow BSS transition within a controller as a baseline
7. Enable FT mechanisms within controllers and the client station
8. Perform a fast BSS transition within a controller as a comparison
9. Perform a slow BSS transition between controllers as a baseline
10. Perform a fast BSS transition (if vendor FT mechanisms permit) between controllers as a comparison

Intense School's CWSP (Wireless Security) – Detailed Daily Course Outline

The following lists the materials covered in the course (note that each section is accompanied by significant hands-on activities, as well as important exam prep):

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

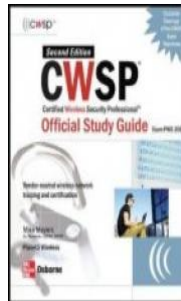
- Robust Security Networks (RSN)
- WPA/WPA2 Enterprise - how it works
- WPA/WPA2 Enterprise - configuration
- IEEE 802.11 Authentication and Key Management (AKM)
- 802.11 cipher suites
- Use of authentication services (RADIUS, LDAP) in WLANs
- User profile management (RBAC)
- Public Key Infrastructures (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

Intense School's Authorized CWSP (Wireless Security) Boot Camp

Instructor Bio

David Coleman, CWSP expert

- CWNE Certified Wireless Network Expert #4
- CWNT Certified Wireless Network Trainer
- CWSP Certified Wireless Security Professional
- CWNA Certified Wireless Network Administrator
- CCNA Cisco Certified Network Associate



David Coleman is the author of Sybex Publishing's "CWSP Study Guide"

David Coleman is a First-Rate Wireless Network & Security Engineer and Trainer. His "stop at nothing to accomplish the mission" attitude and innovative approach to problem solving keeps him at the forefront of this industry's technology. Dave is an accomplished wireless network engineer, trainer and sales consultant with over fifteen years experience.

Here's a short list of recent accomplishments:

- Instructed numerous IT professionals in Wireless Security administration, wireless security and wireless frame analysis and troubleshooting.
- Recently instructed Dell Computer's senior Wireless Security support department. Other corporate clients include Cisco, Polycom, Nortel and Avaya.
- Trained numerous computer security employees from various law enforcement agencies, the Department of Defense, US Army, US Navy and other federal and state government agencies.
- Taught numerous WLAN vendor specific courses for Aruba, Cisco, Motorola and AirDefense.
- Author of "CWSP Study Guide" - ISBN 0470438908
- Recommended wireless security solutions in enterprise environments. Implemented appropriate solutions including 801.x, 802.11i, WEP, WPA, TKIP, MAC & protocol filtering, PPTP & IPSec VPNs, wireless VLANs, LEAP, PEAP, EAP-TTLS and EAP-FAST. Familiar with numerous Layer 2 and Layer 3 authentication and encryption solutions. Proficient with WLAN switching technologies.

Intense School's CWSP (Wireless) Boot Camp – Training Schedule

To view our current CWSP(Wireless) course schedule and locations, visit Intense School's online at:

http://intenseschool.com/boot_camp/wireless_networking/cwsp

Career Path-Related Courses

The courses below are excellent follow-on classes, once CWSP (Wireless) Boot Camp has been completed:

- ECSA/LPT (EC-Council Certified Security Analyst/Licensed Pen Tester) Boot Camp
- CISSP Boot Camp

Intense School's Authorized CWSP (Wireless Security) Boot Camp

The TOTAL Immersion Experience

During the 5 day program, our instructors give you 100% of their time and dedication to ensure that your time is well spent. You will receive an all-inclusive immersion experience by receiving your hotel stay and most meals during your training experience; you eat, sleep and train at the learning facility with no distractions!

Intense School's 100% Satisfaction & Human Capital Guarantee

Intense School is committed to you having the best possible training experience available. If during the first day of any classroom-based or Live Online course the student is not fully satisfied and wishes to withdraw, the student will receive a 100% refund, less any applicable fees. We also offer students the opportunity to re-sit a Classroom-based or Live Online course tuition-free for up to one year or until the student obtains certification, whichever comes first. Our Human Capital Guarantee ensures a successful return on investment for employers. If an employer has paid the cost of a class for an employee who leaves within three (3) months of obtaining certification, Intense School will train an additional employee of the company with no tuition cost to the employer. (Other costs will apply) The employee taking advantage of the Human Capital Guarantee must take training within 6 months of the original employee's class end date.*

Our Training School At-A-Glance

Intense School is the #1 accelerated IT training school in the world for good reason – our Expert Instructors are industry-recognized leaders, authors, and experts in their fields. We have mastered the accelerated method of training and certification and take pride in offering you the same quality training and certification programs that more than 45,000 satisfied clients have raved about.

Intense School's Expert Instructors possess strong consulting, implementation and training expertise. Our security professionals come from diverse roles including positions in consulting, product development, project management, information security and information technology. Our training team has supported public and private corporations, technology vendors, telecommunications companies and professional services organizations around the world.

*All terms & conditions located on www.intenseschool.com



Certified to Operate by SCHEV

This program is available for Corporately Sponsored Students only. This program has not been approved by the Florida Commission for Independent Education.

www.intenseschool.com
866.365.8401

©2000-2009 Vigilar, Inc. All Rights Reserved.

