

## Wireless LAN Security Course Description



**Wireless LAN Security**, the preparation course for the CWSP™ certification, offers 45 hours of hands on learning using the latest enterprise wireless LAN security and auditing equipment. This 5-day course addresses in detail Wireless LAN Intrusion, Security Policy, and Security Solutions.

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:

- BlueSocket
- Colubris Networks
- Cisco Systems
- Fortress Technologies
- SnapGear
- Intermec
- Proxim
- Symbol Technologies
- Funk Software
- Microsoft
- TamoSoft
- Zoom Telephonics
- SafeNet
- System Tools
- Van Dyke Software
- WildPackets
- IPSwitch
- Young Design

All attendees receive hands-on experience configuring, testing, and implementing a broad variety of layer2 and layer3 wireless security solutions. Students will gain a first-hand understanding of the tactics and tools that malicious intruders use to gain access to improperly secured or unsecured wireless LANs.

**Audience:** This course targets experienced networking professionals who wish to gain critical skills in wireless networking security, including how hackers attack networks and the means for preventing them from doing so. With the burgeoning growth of wireless LAN installations, all IT professionals must become knowledgeable about security - wireless security in particular.

**Duration:** The Wireless LAN Security course is 45 hours of instructor-led study, incorporating both lecture and hands-on labs. The lab exercises consume more than 80% of the class time, providing thorough hands-on training for all attendees. The class may be taught in a 5-day period, over the course of a semester, or in other variations, depending on the training organization.

**Certification:** This course may be used – and is the ideal track – for preparing students for the Certified Wireless Security Professional™ exam (exam # PW0-200), which is delivered at all Prometric Testing Centers worldwide. The CWSP certification is the first vendor neutral security certification that focuses solely on testing the IT professional's knowledge of securing enterprise wireless LAN solutions.

**Prerequisites:** The CWNA certification is required prior to attending the CWSP class or taking the CWSP exam. It is recommended that all students earn either the Security Certified Network Professional (SCNP) or CompTIA Security+ certification or have at least 12 months experience in a network security related field prior to enrolling in the course.



## Hands-on Lab Exercises

- Packet Analysis & Spoofing
- Rogue Hardware & Default Settings
- RF Jamming & Data Flooding
- Information Theft
- Wireless Hijacking and DoS Attacks
- Access Point VPNs
- Scalable Wireless VPN Solutions
- EAP - Cisco Wireless (LEAP)
- Layered Wireless Security
- Wireless Bridging Security
- 802.1x and EAP-TTLS
- SSH2 Tunneling & Local Port Redirection

## Course Topics

### Risk Assessment

- Assets to protect
- Threats to protect against
- Legal protection
- Costs
- Basic security measures
- Threat analysis
- Impact analysis

### Threat Analysis & Hacking Methodology

- Target profiling
- Physical security
- Social engineering
- Wireless bridges
- Sniffing and stealing
- Malicious data insertion
- Denial of Service (DoS)
- Peer-to-peer hacking
- Unauthorized control

### Rudimentary security measures

- SSID
- MAC filters
- Static WEP
- Default configurations
- Firmware upgrades
- Physical security
- Periodic inventory

### Intermediate Security Measures

- Rogue equipment
- Cell sizing
- Protocol filters
- SNMP
- Discovery protocols
- Wireless segment configuration
- Remove vulnerabilities
- Client security
- IP Services

### Advanced Security Measures

- Wireless security policy
- Authentication & encryption
- Wireless DMZ and VLANs
- Audits
- Authenticated DHCP
- Traffic patterns

### Wireless LAN Auditing Tools

- Discovery tools
- Password crackers
- Share enumerators
- Network management and control
- Wireless protocol analyzers
- Manufacturer defaults
- Password sniffers
- Antennas and WLAN equipment
- OS fingerprinting and port scanning
- Application sniffers
- Networking utilities
- Network discovery and management
- Hijacking users
- Jamming tools
- WEP crackers
- Operating system defaults

### Hardware & Software Solutions

- RADIUS with AAA Support
- RADIUS Details
- Kerberos
- Static and Dynamic WEP and TKIP
- 802.1x
- Extensible Authentication Protocol (EAP)
- VPNs
- Encryption Schemes
- Routers
- Switch-Routers
- Firewalls
- MobileIP VPN Solutions
- Enterprise Wireless Gateways
- Switches, VLANs, & Hubs
- SSH2 Tunneling & Port Redirection
- Thin Client Solutions

### Prevention & Countermeasures

- 802.1x
- 802.11i
- TKIP
- AES
- Intrusion detection
- US Federal and state laws

### Implementation and Management

- Design and implementation
- Equipment configuration and placement
- Interoperability and layering
- Security management

## Daily Schedule

### Day 1

#### Discussion Topics

- Auditing Tools
- Information Gathering
- Unauthorized Access
- Denial of Service

#### Lab Exercises

- Lab 1 – Packet Analysis & Spoofing
- Lab 2 – Rogue Hardware & Default Settings
- Lab 3 – RF Jamming & Data Flooding

### Day 2

#### Discussion Topics

- Legislation
- General Policy
- Functional Policy

#### Lab Exercises

- Lab 4 – Information Theft
- Lab 5 – Wireless Hijacking and DoS Attacks

### Day 3

#### Discussion Topics

- Solution Considerations
- Encryption Types
- Layer 2 Solutions
- 802.11i / WPA

#### Lab Exercises

- Lab 6 - LEAP
- Lab 7 - 802.1x and EAP
- Lab 8 - Wireless Bridging Security

### Day 4

#### Discussion Topics

- Layer 3 Solutions
- Segmentation Devices

#### Lab Exercises

- Lab 9 - Access Point VPNs
- Lab 10 - SSH2 Tunneling & Port Redirection

### Day 5

#### Discussion Topics

- Additional Solutions
- Authentication Types

#### Lab Exercises

- Lab 11 - Scalable Wireless VPN Solutions
- Lab 12 - Layered Wireless Security

