

## Wireless LAN Security Course Description

**Wireless LAN Security**, the preparation course for the Wireless LAN Security exam (PW0-200), offers 45 hours of hands on learning using the latest enterprise wireless LAN security and auditing equipment. This 5-day 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.

<b>Audience:</b>	Experienced networking professionals
<b>Duration:</b>	5 days, Classroom. May be taught over 1 academic semester.
<b>Associated Certification:</b>	CWSP
<b>Prerequisites:</b>	Basic knowledge of wireless networking.

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:

- Vernier Networks
- Colubris Networks
- Cisco Systems
- Bluesocket
- Fortress Technologies
- Trapeze Networks
- AirMagnet
- Proxim
- Symbol Technologies
- Funk Software
- Microsoft
- TamoSoft
- LucidLink
- Roving Planet
- SafeNet
- System Tools
- Van Dyke Software
- WildPackets
- AirWave
- Network Chemistry
- Aruba Networks

All attendees receive hands-on experience configuring, implementing, and testing a broad variety of layer-2, layer-3, and layer-7 wireless security solutions. Students will gain a first-hand understanding of the tactics and tools that malicious intruders use to gain access to unsecured or improperly secured wireless LANs.

## Hands-on Lab Exercises

- WLAN Intrusion Tools & Techniques
- Enterprise Encryption Gateways
- Enterprise Wireless Gateways
- SOHO/SMB Security Solutions
- Secure WLAN Bridging Solutions
- WLAN Network Management Systems
- WLAN Routers
- WLAN Switches
- Wireless Intrusion Detection/Prevention Systems
- 802.1X/EAP & VLAN-based Security Solutions

## Course Topics

### Physical Security

- Controlled physical access to premises and infrastructure
- Social engineering
- Policy adherence
- Proper use of security solutions

### MAC Layer Security

- Use of VLANs for layer-2 segmentation in WLANs
- Pre-shared key security solutions
- 802.1X/EAP framework and security solutions
- Extensible Authentication Protocol (EAP) framework and comparisons
- Detailed discussion of each EAP type used in today's WLANs including in-depth frame-exchange graphics
- Wi-Fi Protected Access (WPA/WPA2)
- 802.11i terms, framework, and in-depth operational explanations
- 802.11i/RSN functional graphics and frame capture explanations
- Explanations of how 802.1X/EAP solutions changed to 802.11i/RSN solutions.
- 802.11i frame format explanation and graphics

### Network Layer Security

- PPTP VPN
- IPSec Framework and implementation discussion and graphical detail

### WLAN Hardware & Software Solutions

- "Fat" access points
- WLAN switches/controllers
- WLAN bridges
- SOHO/SMB solutions
- Enterprise Encryption Gateways (EEGs)
- Enterprise Wireless Gateways (EWGs)
- WLAN routers
- WLAN Network Management Systems (WNMS)
- WLAN mesh routers
- WLAN Intrusion Detection/Prevention Systems (WIDS/WIPS)

### Application Security

- Secure Shell (SSH1/SSH2) as a terminal application and VPN solution
- SSLv3/TLSv1 for email, FTP, and web browsing
- SNMPv3 for authenticated and encrypted network management

### Authentication, Authorization, and Accounting (AAA) Systems

- Local authentication in APs, EWGs, WLAN switches, and WLAN routers
- RADIUS authentication and proxy services
- Kerberos authentication
- LDAP authentication
- Per-user and Per-group authorization options
- Role-Based Access Control (RBAC)
- Bandwidth management

### Protocol Analyzers

- Hardware and software types available
- Performance and security analysis
- Connectivity troubleshooting
- Channel/spectral monitoring
- Distributed analysis with WIDS
- Three types of WIDS - explanation of each

### WLAN Intrusion

- Next generation intrusion and DoS tools
- WLAN attack techniques

---

## Daily Schedule

### Day 1

**Discussion Topics**

- Intrusion Tools
- Intrusion Techniques

**Lab Exercises**

Lab 1 – WLAN Intrusion Tools & Techniques

### Day 2

**Discussion Topics**

- Physical Security
- MAC Layer Security
- The 802.11i Amendment
- IP Security
- Hardware & Software Solutions

**Lab Exercises**

Lab 2 – 802.1X/EAP & VLAN-based Security Solutions

### Day 3

**Discussion Topics**

*Lab Day Only*

**Lab Exercises**

Lab 3 – Secure WLAN Bridging

Lab 4 – WLAN Switching

Lab 5 – Enterprise Encryption Gateways (EEGs)

### Day 4

**Discussion Topics**

*Lab Day Only*

**Lab Exercises**

Lab 6 – Enterprise Wireless Gateways (EWGs)

Lab 7 – SOHO/SMB Solutions

Lab 8 – WLAN Routers

### Day 5

**Discussion Topics**

- Application Security
- AAA Solutions
- WIDS Solutions

**Lab Exercises**

Lab 9 – WLAN Network Management Systems

Lab 10 – WLAN Intrusion Detection Systems