



To register for this course, go to www.giga-wave.com, or call 210-375-0085

Cisco Aironet WLAN Security v3.0

Keyword: CWLS

4 Days – List Price \$2695

Course Description:

Cisco Aironet WLAN Security Class is an advanced interactive seminar on how to secure a Cisco Aironet WLAN. This is the most comprehensive seminar on Cisco Aironet wireless security advantages in the industry! Topics include: how to mitigate WLAN attacks, computer hacking, Cisco SAFE, basic security configuration and 802.11 security risks. Hands-on labs feature how to use a wireless sniffer, how to capture packets and analyze WLAN traffic, authentication and association processes, use AirMagnet and WLSE to detect rogue access point, “harden” the access point, and build VLANs with different forms of authentication and encryption. Attendees will receive an introduction to Cisco ACS RADIUS attributes and actually configure Cisco ACU and ADU for LEAP, PEAP and EAP -FAST.

To participate in the hands-on labs, please bring a laptop computer with an available 32-bit Card-Bus slot and an Ethernet port. The laptop's operating systems must be either MS Windows 2000 (SP4) or XP (see note). The laptop should also have a 9-pin serial port or USB to serial adapter. IN ADDITION, you will need administrator rights to the laptop to install drivers for the wireless client used in class.

Note: Other Windows operating systems are not supported by some of the tools that will be used in class and therefore are not recommended.

You Learn...

After completing this course, the student should be able to:

- Identify methods of attack
- Utilize Cisco SAFE
- Utilize Cisco SWAN using Wireless Domain Services and Cisco's Wireless LAN Solution Engine
- Deploy Rogue AP Detection using Cisco's Wireless LAN Solution Engine
- Describe Wireless Standards
- Secure WLAN to mitigate attacks
- Install Wireless Sniffer software
- Capture and analyze WLAN traffic
- Configure WEP keys in AP and ACU / ADU
- Configure Cisco ACS and ADU for use with Cisco Aironet
- Be able to deploy Wi-Fi Protected Access Authentication and Encryption Techniques
- Describe the recently ratified IEEE 802.11i Authentication and Encryptions Standards for 802.11 Wireless Networks

Who Would Benefit :

Cisco Aironet WLAN Security is an advanced curriculum for CIO's, IT managers, and technical engineers responsible for managing and securing wireless networks.

Prerequisites:

- Cisco Aironet Wireless LAN Fundamentals & Site Survey (AWFSS)

Follow On Courses:

- Cisco Unified Wireless Networking (CUWN)
- Cisco Wireless Mesh Networking (CWMN)
- Cisco Advanced Wireless Bridging LAB (CAWBL)
- Aironet Wireless LAN Advanced Topics (AWLAT)

Cisco Aironet WLAN Security – continued pg. 2

Course Content

Module 1 – Introduction

- Introduction
- Wireless LAN Security Today
- Introductions

Module 2 – Network Security and Cisco

- Network Security
- Cisco AVVID and Safe
- Cisco SWAN

Module 3 – IEEE Standards and WLAN Security

- 802.11: 802.11a, 802.11b and 802.11g
- Ad Hoc vs. Infrastructure Mode
- WEP
- 802.1X
- EAP Authentication Types
- 802.1X Definitions
- 802.1X: Authentication Process / Cisco Aironet's LEAP Authentication
- Other Authentication Methods
- Transportation Layer Security
- EAP - FAST
- A Comparison of Security Methods
- Wi-Fi Protected Access
- IEEE 802.11i

Module 4 – WLAN Security Risks and Attacks

- WLAN sniffers
- 802.11 WEP Security Risks
- Berkley, Maryland and FMS Papers
- Other Attacks
- What is being done to protect my WLAN?
- The other side of the Access Point
- What is the cost of implementing Wireless LAN Security?

Lab 1 – Using AirMagnet Packet Sniffer

Lab 2 – Configuring the Access Point

Lab 3 – Configuring Cisco ACS

Lab 4 – Configuring Funk's Software Odyssey Server

Lab 5 – Configuring the Client to Connect (LEAP)

Lab 6 – Installing and Configuring the Odyssey Client to Connect (TTLS)

Lab 7 – Configuring Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST)

Module 5 – Installing and Configuring Cisco Protected EAP (PEAP)

- Prerequisites for PEAP Software Installation
- Main Cisco ACS V3.1 Certificate Setup

Lab 8 – Cisco Aironet ADU PEAP Configuration

Lab 9 – Building different VLANs with different forms of Authentication and Encryption

Lab 10 – Hardening the Access Point

Lab 11 – WDS and Rogue AP Detection using WLSE

Lab 12 – Using AirMagnet to Detect Rogue Access Points

Module 6 – Other Security Features

- VPN over 802.11
- RADIUS Accounting