ProTech
protechtraining.com

*"Charting the Course ...*

*... to Your Success!"*

# Wireless Network Security

# Course Summary

**Description**

This workshop teaches the fundamentals of identifying wireless vulnerabilities and how to resolve them The number of wireless devices continues to grow—enterprises, homes, and even the local coffee shop offer wireless Internet services. Unfortunately, the security implemented on these devices is often at risk due to improper implementation, or is absent completely. Nevertheless, organizations lacking an understanding of wireless security continue to use these devices, putting their corporate and user data at risk.

In order to ensure that data is secured against interception in the wireless medium, students must have an informed and current understanding of the present-day methodologies, tools, and vulnerabilities, which allow these attacks to occur. Wireless Network Security is an intense hands-on course delivered over 3 days.

**Objectives**
**At the end of this course, students will be able to:**

- Understand the underlying principles of secure wireless transmissions, ensuring that you are prepared to deal with changes to the technology
- Understand the threats to wireless networks, including interception of data communications and denial of service attacks
- Be capable of performing a wireless site survey, including detection of rogue wireless access points
- Be able to select and implement the most effective security standards and practices for wireless networks
- How to effectively test wireless networks for vulnerabilities

**Topics**

- Introduction
- Wireless Technology Essentials
- Configuring a Wireless Security Lab
- Wireless Discovery identifying access points with visible and hidden SSIDs, mapping wireless networks (Netstumbler, Kismet, gpsmap)
- Rogue Wireless Access Points
- Wireless Packet Capture
- By-Passing Simple WLAN Authentication
- The IEEE 802.11 MAC Layer
- Assessing WEP networks
- Assessing WPA-PSK Networks
- Attacking the WLAN Infrastructure
- Advanced WLAN Attacks
- Attacking Wireless Clients
- Secure Wireless Architectures

**Audience**

This course is designed to address the training needs of IT and security professionals who must be able to assess the security of their network and protect it against attackers.

**Prerequisites**

There are no prerequisites for this course.

**Duration**

Three days

ProTech

protechtraining.com

*"Charting the Course ...*

*... to Your Success!"*

# Wireless Network Security

# Course Outline

**I. Introduction**
- A. Understanding the Wireless Threat
- B. Wireless technologies
- C. Wireless security weaknesses
- D. Anatomy of a wireless attack

**II. Wireless Technology Essentials**
- A. Terminology
- B. Wireless standards and organizations
- C. Radio frequency fundamentals
- D. Signal and antenna concepts, spectrum technologies
- E. IEEE 802.11 standards
- F. Wireless LAN topologies
- G. Wireless network architecture
- H. Secure design and implementation considerations

**III. Configuring a Wireless Security Lab**
- A. Installing and using open-source tools from Backtrack
- B. Configuring the Alfa wireless adaptor

**IV. Wireless Discovery identifying access points with visible and hidden SSIDs, mapping wireless networks (Netstumbler, Kismet, gpsmap)**

**V. Rogue Wireless Access Points**
- A. Identifying rogue access points from wired and wireless
- B. Networks
- C. "wardriving"
- D. Malicious rogue access point attacks
- E. Secure AP architecture

**VI. Wireless Packet Capture**
- A. Management, control, and data frames, Intercepting wireless
- B. Communications (Airopeek, Apsniff, Cain, Wireshark)

**VII. By-Passing Simple WLAN Authentication**
- A. Finding hidden SSIDS
- B. By-passing MAC filters
- C. Beating open and shared authentication (aireplay, airodump, macchanger)

**VIII. The IEEE 802.11 MAC Layer**
- A. Architecture and operation of 802.11 networks
- B. 802.1x authentication
- C. LEAP
- D. PEAP
- E. EAP/TLS
- F. TTLS (eapeak)
- G. Auditing Cisco LEAP Networks
- H. Identifying
- I. LEAP networks, authentication
- J. Auditing networks (Asleap, genkeys)

**IX. Assessing WEP networks**
- A. WEP technology
- B. Failures of WEP security
- C. Attacking WEPnetworks with visible and hidden SSIDs (aircrack
- D. aireplay
- E. airsnort
- F. WEPattack
- G. WEPcrack
- H. Void11
- I. Automated scripts)

**X. Assessing WPA-PSK Networks**
- A. Introduction to WPA technology
- B. Security improvements over WEP
- C. Attacking the passphrase of WPA/WPA2-PSK networks (aircrack, coWPAtty)
- D. Securing WPA-PSK networks

**XI. Attacking the WLAN Infrastructure**
- A. Attacking wireless access point authentication
- B. Denial of service attacks against WLANs (physical attacks, AirJack suite, file2air, fata-jack, hunter_killer, Void11)

# Wireless Network Security

## Course Outline (cont'd)

**XII. Advanced WLAN Attacks**

A. Evil twin and access point spoofing
B. Wireless eavesdropping using man-in-the-middle attacks
C. Session hijacking over wireless (airbase-ng)

**XIII. Attacking Wireless Clients**

A. Hotspot injection attacks
B. mis-association attacks
C. caffe latte and hirte attacks
D. de-authentication and dis-association attacks
E. sidejacking (AirPWN
F. Hamster
G. hotspotter
H. KARMA
I. fuzzing and packet injection tools)

**XIV. Secure Wireless Architectures**

A. Implementing a secure 802.11x network
B. Considerations for other wireless protocols
C. Developing an auditing methodology