ProTech
protechtraining.com

"Charting the Course ...

... to Your Success!"

Certified Wireless Security Engineer

Course Summary

Description

This 4-day course takes an in-depth look at the security challenges of many different wireless technologies. Showing the student different wireless security threats through the eyes of an attacker. Using readily available and custom-developed tools, students will navigate their way through the techniques attackers use to exploit WiFi networks.

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

- Have knowledge to detect wireless security threats and risk
- Have knowledge to design and implement a solution to mitigate risk threats
- Be ready to sit for the C)WSE exam

Topics

- WLAN Security Overview
- Legacy Security
- Encryption Ciphers and Methods
- Layer 2 Authentication Methods in
- 802.11 Layer 2 Dynamic
- SOHO 802.11 Security
- Fast Secure Roaming
- Common Attacks
- Auditing WLAN Security
- Wireless Security Monitoring
- Advanced WLAN Security

Prerequisites

- Knowledge of TCP/IP
- 12 months experience in networking technologies
- Computer hardware knowledge
- Typical operating system experience

Duration

Four days

ProTech
protechtraining.com

"Charting the Course ...

... to Your Success!"

Certified Wireless Security Engineer

Course Outline

I. WLAN Security Overview
- A. Standards Organization
- B. OSI Layers (ISO Standard)
- C. 802 Project (IEEE)
- D. ISOC Hierarchy (IETF)
- E. Wi-Fi Alliance
- F. Wi-Fi Certified Programs
- G. 802.11 Security Basics
- H. 802.11 Security History
- I. Summary

II. Legacy Security
- A. Overview
- B. Authentication Open System Authentication
- C. Authentication Open System and 802.1X/EAP
- D. Authentication Shared Key
- E. Static WEP and IV Key
- F. WEP Transmission Key
- G. WEP Encryption Process
- H. Common WEP Attacks
- I. VPN and WLAN Client Access
- J. VPNs
- K. VPN Comparison
- L. Aggressive Mode PSK Attacks
- M. Aggressive PSK Cracking
- N. MAC Filters Changing a MAC Address
- O. SSID Segmentation
- P. SSID Cloaking
- Q. Labs

III. Encryption Ciphers and Methods
- A. Overview
- B. Introduction
- C. Encryption
- D. Cryptographic Definitions
- E. Encryption Algorithm
- F. Implementation
- G. Symmetric Encryption
- H. Symmetric Downfalls
- I. Symmetric Algorithms
- J. Crack Times
- K. Asymmetric Encryption
- L. Public Key Cryptography Advantages
- M. Asymmetric Algorithm Disadvantages
- N. Asymmetric Algorithm Examples
- O. Key Exchange
- P. Symmetric versus Asymmetric
- Q. Using the Algorithm Types Together
- R. Attack Vectors
- S. WLAN Encryption Methods
- T. MAC Protocol Data Unit (MSDU)
- U. WEP MPDU
- V. WEP Encryption Process
- W. WEP Decapsulation
- X. TKIP Modification to WEP
- Y. TKIP Cryptographic Encapsulation
- Z. TKIP Decapsulation
- AA. TKIP MPDU
- BB. CCMP
- CC. CCMP MPDU
- DD. Additional Authentication Data
- EE. CCMP Encapsulation
- FF. CCMP Decapsulation
- GG. Labs

IV. Layer 2 Authentication Methods in
- A. Enterprise Networks
- B. Overview
- C. AAA
- D. Types of Credentials
- E. Authentication Examples of Credentials
- F. 802.1X Components
- G. Supplicant Types
- H. Authenticator
- I. WLAN Bridging and 802.1X
- J. Authentication Proxy
- K. Typical Authentication Servers
- L. Supplicant Identity Credential
- M. Legacy Authentication Protocols
- N. Extensible Authentication Protocol
- O. EAPOL Messages
- P. 802.11 Association and 802.1X/EAP
- Q. Generic EAP Exchange
- R. Weak EAP Protocols
- S. EAP-LEAP
- T. Strong EAP Protocols
- U. EAP-PEAP Process
- V. EAP-TTLS Process
- W. EAP-TLS Process
- X. EAP-FAST Process
- Y. PACs
- Z. EAP Comparison Chart
- AA. EAP Methods for Cellular Networks

V. 802.11 Layer 2 Dynamic
- A. Encryption Key Generation
- B. Overview
- C. 802.1X/EAP and Dynamic Keys
- D. Advantages
- E. Dynamic WEP Process
- F. Robust Security Network Associations
- G. RSNA in IBSS (Ad-hoc)
- H. RSN Information Element
- I. RSNIE (Cipher Suites)

Certified Wireless Security Engineer

Course Outline (cont'd)

J. RSNIE (AKM)
K. AKM Overview
L. AKM Discovery
M. AKM Master Key Generation
N. AKM Temporal Key Generation
O. RSN Key Hierarchy
P. Master Keys
Q. Pairwise Key Hierarchy
R. Group Key Hierarchy
S. 4-way Handshake
T. Group Key Handshake
U. Station to Station Link (STSL)
V. RSNA Security Associations
W. WPA/WPA2 Personal Passphrase to PSK Mapping
X. Roaming and Dynamic Keys
Y. Labs

VI. SOHO 802.11 Security
A. Overview
B. WPA/WPA2 Personal
C. Pre-shared Keys (PSK) and Passphrases
D. WPA/WPA2 Personal Risks
E. Wi-Fi Protected Setup (WPS)
F. WPS Architecture
G. Setup Options
H. Configuration Modes
I. Guidelines and Requirements for PIN
J. PBC Demonstration
K. SOHO Security Best Practices
L. Labs

VII. Fast Secure Roaming
A. Overview
B. Client Roaming Thresholds
C. AP-to-AP Re-association
D. Problems with Autonomous AP-to-AP Roaming
E. PMKSA without Fast Roaming
F. PMK Caching
G. Pre-authentication
H. Opportunistic PMK Key Caching (OKC)
I. Proprietary FSR CCKM
J. Fast BSS Transition
K. FT Protocols
L. Message Exchange Methods
M. Key Holders
N. Key Hierarchy
O. FT Key hierarchy-WLAN controller
P. FT Key hierarchy-Supplicant
Q. Information Elements
R. Fast BSS transition information element
S. FT Initial Mobility Domain Association
T. Over-the-air Fast BSS Transition
U. Over - the - DS Fast BSS Transition
V. Fast BSS Transition Summary
W. Wi-Fi Voice Personal and Enterprise
X. Enterprise Grade Voice over Wi-Fi Requirement
Y. Features Required
Z. Layer3 Roaming
AA. Mobile IP
BB. Single Channel Architecture (SCA) Roaming

VIII. Common Attacks
A. Overview
B. Unauthorized Rogue Access Rogue Devices
C. Bridged Ad Hoc (IBSS)
D. Attacks which can be launched through rogue AP
E. Rogue AP Attack Risks
F. Rogue AP Prevention
G. Eavesdropping
H. Eavesdropping Risks
I. Eavesdropping Prevention
J. Authentication Attacks
K. Denial of Service Attacks
L. MAC Spoofing
M. Wireless Hijacking (Evil Twin Attack)
N. Encryption Cracking
O. Peer-to-peer attacks
P. Management Interface Exploits
Q. Vendor Proprietary Attacks
R. Physical Damage and Theft
S. Social Engineering Attacks
T. Public Access and WLAN Hotspots
U. Labs

IX. Auditing WLAN Security
A. Overview
B. What is Security Audit?
C. 2.4 GHz ISM Interferers
D. Narrow Band Interference
E. Wide Band Interference
F. All-Band Interference
G. OSI Layer2 Audit
H. List of L2 Information collection
I. Layer2 Protocol Analyzer
J. Penetration Testing
K. Wired Infrastructure Audit
L. Social Engineering Audit
M. WIPS Audit
N. Documenting the Audit

Certified Wireless Security Engineer

Course Outline (cont'd)

O. Documents required prior to audit
P. Example Recommendations
Q. WLAN Toolkit of an Auditor
R. Common Software Tools
S. Automated Tool (SILICA)

X. Wireless Security Monitoring
A. Overview
B. WIDS / WIPS Infrastructure Components
C. WIDS/WIPS Architecture Models
D. Overlay WIDS/WIPS
E. Integrated WIDS/WIPS
F. Integrated-Enabled WIDS/WIPS
G. Wireless Network Management System
H. Sensor Placement
I. Device Classification
J. Rouge Detection
K. Rogue Types
L. Rogue Mitigation
M. Device Tracking
N. Device Tracking Techniques
O. WIDS/WIPS Signature Analysis
P. WIDS/WIPS Behavioral Analysis
Q. WIDS/WIPS Protocol Analysis
R. WIDS/WIPS Spectrum Analysis
S. WIDS/WIPS Forensics Analysis
T. WIDS/WIPS Performance Analysis
U. Monitoring
V. Policy Enforcement
W. Types of Alarms and Notifications
X. Severity Levels of Alarms and Notifications
Y. Typical Notification Tools
Z. 802.11n
AA. 802.11n Security Concerns
BB. Management Frame Protection
CC. 802.11w
DD. 802.11w Shared Secret Key
EE. Labs

XI. Advanced WLAN Security
A. Overview
B. Wireless Infrastructure Components
C. Autonomous AP
D. WLAN Controllers
E. WLAN-VLAN Assignment
F. WLAN-Dynamic VLAN Assignment
G. Split MAC
H. Mesh Networks
I. WLAN Bridging
J. Hybrid WLAN APs
K. Dynamic RF
L. Hot Standby/Failover
M. Device Management
N. Management Protocols
O. RADIUS/LDAP Servers
P. Radius Features and Components
Q. Radius Integration
R. EAP Type Selection
S. Deployment Architectures and Scaling
T. Built-in RADIUS Servers
U. Timer Values
V. PKI
W. CA Hierarchy