

## Securing Wireless Networks: Hands-On - 4 Days

### *Course 420 Overview*

#### **You Will Learn How To**

- Secure wireless networks against threats and attacks
- Implement the WPA2 and 802.11i security standards to protect your Wi-Fi network
- Encrypt wireless traffic using Temporal Key Integrity Protocol (TKIP) or Advanced Encryption Standard (AES)
- Leverage 802.1X and EAP authentication within an enterprise WLAN
- Build Wi-Fi auditing and accounting infrastructures
- Deploy wireless intrusion detection systems (WIDS)

#### **Course Benefits**

As organizations provide greater mobility to their users, the risk of threats to security grows and the need for secure wireless networks becomes of paramount concern. In this course, you gain the skills to defend against attacks and maintain security within your wireless network. You learn to detect weakness in your existing network and design and configure a cost-effective security solution.

#### **Who Should Attend**

Anyone who manages, operates, audits or implements secure networks. Knowledge of wireless technology is helpful.

#### **Hands-On Training**

You gain extensive hands-on experience securing a wireless network. Exercises include:

- Discovering and sniffing WLANs
- Decoding and analyzing 802.11 frames
- Cracking WEP and WPA2 PSK keys
- Configuring WPA2 on APs and clients
- Setting up 802.1X authentication
- Installing and presenting digital certificates to RADIUS server
- Comparing and contrasting EAP-TLS and PEAP
- Roaming in a secure environment
- Configuring a wireless IDS

## Securing Wireless Networks: Hands-On - 4 Days

### Course 420 Outline

#### Wireless Security Technologies

##### Security requirements

- Availability
- Confidentiality
- Data integrity
- Authenticity

##### WLAN operation and standards

- 802.11 (Wi-Fi) standards
- Frequency allocation and modulation techniques

##### Wi-Fi access points and stations

- Sniffing 802.11 Association and Authentication
- Infrastructure models and roaming

##### Surveying other wireless technologies

- Bluetooth WPANs (802.15)
- WiMAX WWANs (802.16)

#### Analyzing WPA2 and 802.11i

##### Cryptography

##### Encrypting Wi-Fi traffic for privacy

- Symmetric vs. asymmetric algorithms
- Block Ciphers vs. Streaming Ciphers
- The role of key hierarchies in encryption

##### Guaranteeing message integrity

- Hashing with MD5 and SHA
- Protecting data with digital signatures

##### Authenticating users with digital certificates

- Verifying key ownership
- Chains of authority

#### Encrypting Wi-Fi Traffic with TKIP or AES

##### Overcoming problems with legacy WEP

- Key reuse
- Shared Keys

##### Deploying TKIP as an alternative to WEP

- Upgrading legacy hardware
- Rolling TKIP keys per frame
- Integrity checking with Michael

##### Migrating to AES encryption

- Using Counter and Cipher Block Chaining modes with AES
- AES performance issues

#### Authenticating Wi-Fi Users with PSK or EAP

##### Deploying preshared key (PSK) authentication

- Generating master keys from a passphrase
- Addressing scalability issues

##### Leveraging the 802.1X standard

- Incorporating EAP messaging techniques
- Transporting EAP messages with RADIUS and EAPOL

##### Choosing EAP implementations

- EAP-TLS
- EAP-TTLS
- PEAP

##### Authenticating against enterprise directories

- LDAP
- Active Directory
- NT Domains

#### Creating Secure WLAN Topologies

##### Designing the wireless security landscape

- Defining the trusted boundary
- Centralized vs. distributed control
- Enforcing access controls
- Establishing user credentials

##### Configuring security for roaming

- Maintaining security contexts
- 802.11i pre-authentication
- Roaming in a VPN environment

##### Evaluating network types

- Public hot spots
- Visitor and guest networks
- Integrated corporate WLAN

##### Maintaining auditing and accounting systems

- RADIUS accounting
- Access Point logging

#### Detecting and Responding to Wi-Fi Attacks

##### Denial of Service (DoS) attacks

- Jamming and RF interference
- Exploiting the Collision Avoidance (CA) mechanism
- Forcing 802.11 de-authentication

##### Conducting War Driving

- Discovering WLANs using NetStumbler and Kismet
- Intercepting Wi-Fi traffic with Wireshark

##### Authentication and privacy attacks

- WEP key cracking
- Brute force attacks against WPA PSK

##### The role of WIDS

- Detecting and locating unauthorized clients and access points
- Responding to malicious wireless traffic
- Creating audit logs