Global Knowledge Course Name: Wireless Networking II: Security and Analysis (Code 3610)

Course Overview:
Optimize and defend wireless networks by understanding Wi-Fi analysis and deploying state-of-the-art solutions.
In this two-part course, learn to deploy, maintain, and secure world-class wireless LANs.

In part one, you will develop a complete understanding of Wi-Fi networks to enable advanced 802.11a/b/g troubleshooting. Intense course discussion delivers the comprehensive knowledge needed to fully understand potential Wi-Fi issues and how to deal with them. Hands-on lab exercises allow you to view live 802.11a/b/g transmissions using real-world troubleshooting software.

In the second part of this course, you'll gain an in-depth understanding of 802.11a/b/g security with a comprehensive, three-part approach to delivering secure WLAN installations. Understand what makes wireless networks vulnerable by playing the role of the attacker in hands-on labs. Learn standards-based security solutions and apply them using real-world equipment and software. Gain knowledge about how WLAN monitoring works, and then perform exercises that will help you master wireless intrusion detection systems.

Certification
This course is excellent as part of an overall study strategy for CWNP certifications CWSP/CWNE. Full CWSP and the majority of CWNE discussion concepts are covered with lab emphasis on real-world solutions. This class is also part of our Wireless Specialist Certificate track.

Preparing for the CWSP certification? This course includes a CWSP study guide, certification practice exam, and test voucher. It also includes 1-year access to our 50-book Online Networking Reference Library with titles specially selected to reinforce course concepts.

This course is part of the following programs or tracks:
- CWNA
- Wireless#
- Wireless Specialist

Assess Your Skills
Wireless Networking I: Integration and Troubleshooting or equivalent knowledge is recommended before taking this course. Assess your skills with our free Wireless Networking I: Integration and Troubleshooting Pre-Assessment Test.

What You'll Learn

- Device-level Wi-Fi communications processes

- Why 802.11a/b/g networks operate the way they do and how to apply that knowledge when faced with problems that stump most network administrators
- Using wireless network analyzers to capture live data and pinpoint potential network issues
- How security requirements, products from different vendors, legacy equipment, handheld devices, and the RF environment affect the performance of wireless networks
- How using radio frequency makes wireless networks vulnerable
- The most common wireless threats and how to detect and defend against them
- Understanding wireless security standards for keeping unauthorized users out and maintaining wireless data privacy
- The application of 802.11i/WPA2 standards and the devices used to apply them
- Wireless intrusion detection and why it's essential for maintaining a secure network

Who Needs to Attend?

- Administrators: network, systems, infrastructure, security, and LAN/WLANs
- Designers: network, systems, and infrastructure
- Developers: wireless software and hardware products
- Consultants and integrators: IT and security
- Decision makers: infrastructure managers, IT managers, security directors, chief security officers, and chief technology officers

Course Content:

A. Wireless Local Area Networking Analysis

1. Introduction to Wi-Fi Protocol Analysis
    - Packet capture
        - Monitor mode
            - Captures all packets on a single channel
        - Commercial applications
        - Open source applications
    - Connection analysis
        - Identify configuration errors
        - Determine network availability for end users
    - Performance analysis
        - Setting throughput expectations

    - Determine the feasibility of applications
- Vulnerability analysis
    - Identify potential problems before intrusions happen

2. Arbitration
- Half duplex, shared medium
    - Stations and access points must send frames one at a time
        - The backoff mechanism
- Interframe spacing (IFS)
    - Short IFS (SIFS)
    - Point Coordination Function IFS (PIFS)
    - Distributed Coordination Function IFS (DIFS)
    - Extended IFS (EIFS)
    - Arbitrary IFS Number (AIFSN)
        - AIFSN values for different traffic classes
- The contention window
    - Role of the contention window in arbitration
    - Slot times
        - Maximum contention window value
        - The effect of retransmissions
    - Contention window values for different traffic classes

3. Scheduled Access
- Hybrid Coordination Function (HCF) Controlled Channel Access (HCCA) in 802.11e
    - Legacy scheduled access
        - Point Coordination Function (PCF mode)
    - Improvements on PCF mode
- Advantages of scheduled access
    - Efficiency
    - Reliability for low latency applications

4. Connection Analysis
- Scanning
    - Signal strength analysis
    - Passive and active scanning
- Authentication and association
    - Preamble analysis
    - Data rate capability information
- Reassociation and roaming
    - Verify persistent connectivity for mobile stations
- WEP connection
    - Understand the steps of a WEP connection
- WPA-PSK connection
    - Understand the steps of a WPA-PSK connection

- 802.1x/EAP connection
    - Understand the steps of an 802.1x/EAP connection
- Connection loss and denial-of-service
    - Identify likely traffic patterns when connections are terminated

5. Performance Analysis
- Wi-Fi overhead
    - Acknowledgments
        - The purpose of acknowledgments
- Channel utilization
    - Maximum vs. actual throughput
- Interference analysis
    - Nearby Wi-Fi networks
    - Other interference sources
- Known causes of performance degradation
    - Protection mechanism
        - CTS-to-Self
        - RTS/CTS
    - Fragmentation
    - Request-to-Send/Clear-to-Send
- Power save function
    - Legacy Power Save Polling (PSP)
    - Alternate power save method
- 802.11e improvements
    - Transmission opportunities (TXOPs)
    - Block acknowledgments
    - Direct link setup
    - Automatic power save delivery

6. Vulnerability Analysis
- Alarms
    - Configuring network policy
- Unauthorized devices
    - Rogue access points
    - Ad hoc networks
    - Unauthorized stations

B. Wi-Fi Protocols

7. Physical Layer Convergence Protocol (PLCP) Header
- Legacy DSSS (802.11b) preamble
- OFDM (802.11a/g) preamble
    - Alternate DSSS-OFDM preamble
- Physical layer (PHY) information

8. Medium Access Control (MAC) Header

- Frame control field
    - Type and subtype
    - Frame control flags
    - Privacy
    - More data
    - More frag
    - To DS
    - From DS
- Duration/ID field
    - Association ID
        - Legacy PSP
    - Duration
        - Use of the duration value in arbitration
- Addressing
    - The four addresses of Wi-Fi frames
        - Why all four addresses are not always used
    - What each address represents
- Sequence control field
    - Sequence number
    - Fragment number
- Quality of Service (QoS) control field in 802.11e
    - Traffic identifier
        - Used for user priority and traffic specification

9. Management Frames
- Scanning
    - Beacon
    - Probe Request
    - Probe Response
- Authentication
- Association and reassocation
    - Request and response frames
- Deauthentication and Disassociation
- Other management frames

10. Control Frames
- Acknowledgments
    - Purpose of acknowledgments
    - 802.11e block acknowledgments
- Request-to-Send (RTS) and Clear-to-Send (CTS)
    - Purpose of RTS/CTS
- Power Save Polling (PSP)
    - Legacy power save function
- Contention Free End (CF-End)
    - Ending contention free transfer in PCF mode

11. Data Frames
- The eight types of data frames
    - Which frames contain data and which do not
- Contention Free data frames
    - CF-Poll and CF-Ack
- QoS Data frames in 802.11e
        - Enhanced DCF Channel Access (EDCA) frames
        - HCF Controlled Channel Access (HCCA) frames
- MPDU Encapsulation of Encrypted Frames
    - WEP encapsulation
        - Initialization Vector
        - Integrity Check Value
    - TKIP encapsulation
        - TKIP Sequence Counter
        - Integrity Check Value
        - Message Integrity Check
    - CCMP encapsulation
        - Packet Number
        - Message Integrity Check

C. Vulnerabilities and Basic Security

12. Open Wi-Fi Vulnerabilities
- Unauthorized Network Access
    - Wi-Fi is a wireless extension of the LAN
        - If unsecured, intruders can take advantage
    - Extending a PHY layer connection on a Wi-Fi network
        - Understanding the link budget
    - Malicious insertion and data theft
- Eavesdropping
    - The need for privacy on a WLAN
    - Malicious packet capture
        - Wi-Fi adapters in monitor mode
        - Commercial applications
        - Open source applications

13. End-User Security Threats
- Device Security
    - Mobile devices
        - Unwanted threats brought back accidentally
    - Exposed infrastructure equipment
        - Theft and malicious modification can open vulnerabilities
- Public Access Wi-Fi
    - Peer-to-peer attacks
    - Evil-twin attacks

    - Wi-Phishing
    - Man-in-the-middle attacks
- Denial-of-Service
    - Physical layer
    - MAC layer

14. 802.11 Security: Wired Equivalent Privacy (WEP)
- The goals of WEP
    - Authentication, encryption, and integrity
    - Other goals in the design of WEP
- Authentication
    - Open system and shared key
- Encryption and key management
    - Rotating 64-bit RC4 keys
- Integrity
    - 32-bit cyclic redundancy check
- Flaws in WEP
    - Weak IVs
    - Challenge/Response authentication
    - Linear integrity check
    - Brute force attacks
    - Packet re-injection

D. 802.11i Security Standards

15. Authentication
- WPA-PSK
    - Personal WLANs
    - Passphrase-based
- 802.1x/EAP
    - Enterprise WLANs
    - Server-based

16. Encryption and Key Management Protocols
- Temporal Key Integrity Protocol
    - Improvement on WEP's use of RC4 encryption
        - Fixes the flaws in WEP
    - Rotating 128-bit RC4 keys
    - 64-bit "Michael" message integrity check
    - Incrementing TKIP Sequence Counter
- Counter Mode CBC-MAC Protocol
    - Rotating 128-bit AES keys
    - 64-bit "Michael" message integrity check
    - Incrementing Packet Number
- Encryption
    - Rivest Cipher 4 (RC4)

        - Stream cipher
    - Advanced Encryption Standard (AES)
        - Block cipher

17. 802.11i Authentication and Key Management
- Creating the Pairwise Master Key (PMK) and Group Master Key (GMK)
    - Key material used to create encryption keys
- Robust Security Network (RSN)
    - RSN associations
- The 4-Way Handshake
    - Creating encryption keys on the station and access point
- Encryption keys used with TKIP and CCMP
    - Pairwise Transient Key (PTK)
    - Group Temporal Key (GTK)
- Group Key Handshake
    - Rotation of the GTK
- STAKey Exchange
    - Creation and installation of STAKeys
        - Used with 802.11e Direct Link Setup

E. Security Equipment and Applications

18. General Security Approach
- Integrated WLAN
- Separated WLAN
- Advantages and Disadvantages

19. WLAN Security Infrastructure
- Standalone (Unmanaged) Access Points
    - Equipment protection
    - Data protection
        - Standards-based authentication and encryption
        - Optional security methods
- WLAN Controllers (WLAN Switches) with Managed Access Points
    - Enhanced equipment protection
    - Centralized management
        - Uniform security policy
    - Network layer data protection
        - IPSec tunneling
- Management Systems
    - Centralized configuration
    - Monitoring features
        - Rogue AP identification
        - Denial-of-Service identification
- Authentication Servers
    - Remote Authentication Dial-In User Service (RADIUS)

        - Use with 802.1x/EAP authentication
    - Lightweight Directory Access Protocol (LDAP)
        - Use with RADIUS servers

20. Wireless Monitoring Systems
- Form factors of IDS
    - Laptop based
        - Scheduled monitoring
    - Sensor based
        - Constant monitoring
- Protocol analyzers used for intrusion detection
    - Limited functionality
        - Suitable when budget restrictions are present

21. Other Equipment and Applications
- VPN Servers
    - IPSec VPNs
    - SSL VPNs
- Captive portal servers
    - Appliance and software options
    - Embedded in access points
- Encryption gateways
    - Strong MAC layer data protection
    - Extremely expensive
- Endpoint security appliances and applications
    - Agent based
        - Scans for specific patches and updates
    - Agent-free
    - Determines security posture based on traffic patterns
- Firewalls and ACLs
    - Advanced delineation of network rights
    - Integrated into WLAN Controllers
    - Configured based on RADIUS attributes
- Wireless routers
    - IPSec connections to WLAN Controllers and VPN servers