

Certified Wireless Security Engineer Bootcamp



KEY DATA

Course Name:
Certified Wireless Security Engineer V1.0

Duration: 5 days

Language: English

Format:
Instructor-led Course
(Lecture and Labs)

Prerequisites:

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

Student Materials:

- Planet3 Wireless CWNA/CWSP Books
- Student mile2 Lab book & Manual
- Software/Tools, DVD

Certification Exam:

- Mile2 CWSE – Certified Wireless Security Engineer
- CWNA – Certified Wireless Network Administrator
- CWSP – Certified Wireless Security Professional

Related Courses:

CPTS Certified Pen Testing Specialist

CPTe Certified Pen Testing Expert

CFED Computer Forensics & Electronic Discovery

BENEFITS OF CWSE CERTIFICATION

Following this Mile2 Official Course, participants will be prepared to design, implement, and administer wireless technologies and associated security controls that are typical in today's wireless networks. Additionally, awareness of the current threats against wireless networks will be investigated and countermeasures detailed. Course participants will have the ability to complete laboratories in all of the following areas:

- Selecting and implementing the appropriate wireless equipment for a given environment
- Performing a wireless site survey
- Employing various wireless authentication mechanisms
- Examining various wireless security exploits
- Determining environmental factors that affect wireless performance
- Evaluating the latest wireless security standards
- Developing a wireless security policy

COURSE OVERVIEW

In today's network environment the implementation of wireless technologies is a serious undertaking. Improper planning can lead to an inadequate return on investment. Insufficient understanding of the security implications of wireless can lead to catastrophic results.

This course enables an individual to plan, select and implement the appropriate wireless hardware and deploy the correct security controls to support a typical environment. A focus on RF (radio frequency) technologies in a vendor neutral environment, with hands-on laboratories to reinforce concepts, allows participants the broadest exposure to key concepts. This course is committed to be the most current in the industry, with professionally developed laboratory exercises and real world hardware.

This course combines the materials covered on Planet3 Wireless CWNA and CWSP examinations and will ultimately be the official curriculum to prepare candidates for Mile2's Certified Wireless Security Engineer

UPON COMPLETION

Upon completion, students will be able to confidently undertake the Planet3 Wireless CWNA and CWSP examinations conducted at Thompson Prometric testing centers as well as Mile2's CWSE. Students will benefit from an in-depth course that is continuously updated to maintain and incorporate the rapidly changing wireless networking and security environment.

COURSE DETAILS

Topics Covered

1. Wireless Concepts
2. Network Design, Installation and Management
3. Site Survey
4. Wireless Security Basics
5. 802.1x Authentication
6. Wireless Sniffing, Capture and Decryption
7. Enterprise Wireless Security
8. Wireless VPN Technologies
9. Wireless Intrusion Detection
10. Security Policy



OBJECTIVE OF LABORATORY SCENARIOS

This course is instructor-led; a portion being lecture, concepts and demonstrations and an equal amount of practical, hands-on exercises to give participants the ability to reinforce concepts introduced in the workbook/lecture.

DETAILED MODULE DESCRIPTION

Module 1 – Overview of Wireless Standards and Organizations

- Terminology
- International Telecommunications Union Radio-Communication Sector
- RF Regulatory Bodies
- Federal Communications Commission
- FCC Regulations
- Institute of Electrical and Electronics Engineers (IEEE)
- IEEE Standards
- Wi-Fi Alliance
- International Standards Organization
- Communication Basic
- Modulation Classes
- Amplitude Modulation
- Wavelength
- Frequency
- Phase
- Modulation / De-Modulation with Keying
- Amplitude Shift Keying
- Frequency Shift Keying
- Phase Shift Keying

Module 2 – Radio Frequency Fundamentals

- Terminology
- Radio Frequency
- FR Characteristics
- Polarity
- Wavelength
- Frequency
- Amplitude
- Phase
- RF Behavior
- Wave Propagation
- Absorption
- Reflection
- Scattering
- Refraction
- Diffraction
- Attenuation (Loss)
- Free Space Loss
- Multi Path
- Gain

Module 3 – Radio Frequency Components, Measurements and Mathematics

- Terminology
- RF Components
- Transmitter
- Antenna
- Receiver
- Intentional Radiator
- Equivalent Isotropically Radiated Power (EIRP)
- Units of Power Comparison
- Watt
- Milliwatt
- Decibel
- dBi
- dBd
- dBm
- Free Space Loss
- 6 dB Rule
- Rule of 10's and 3's
- RF Mathematics without Logarithms
- Practicing the Rule of 10's and 3's
- Received Signal Strength Indicator (RSSI)
- System Operating Margin (SOM)
- SOM Calculator
- Link Budget
- Fade Margin
- Inverse Square Law

Module 4 – Radio and Frequency Signal and Antenna Concepts

- Terminology
- Azimuth and Elevation Chart
- Azimuth Chart Example
- Beamwidth
- Degree of Beamwidth Table
- Antenna Types
- Omni-Directional Antennas
- Semi-Directional Antenna
- Highly-Directional Antenna
- Phased Array Antenna
- Sector Antenna
- Visual Line of Sight
- RF Line of Sight
- Fresnel Zone
- 802.11 Calculators
- Earth Buldge
- Antenna Polarization
- Antenna Diversity
- Multiple-Input-Multiple-Output (MIMO)
- Antenna Connection and Installation
- Voltage Standing Wave Ratio (VSWR)
- Antenna Mounting
- Antenna Cables
- Connectors
- Splitters
- Amplifiers
- Attenuators
- Lightning Arrestors
- Grounding Rods and Wires

Module 5 – IEEE 802.11 Standards

- IEEE 802.11 – 1997 Standards including Infrared
- 802.11x – Overview of Protocols
- 802.11a
- 802.11b
- 802.11g
- 802.11n
- 802.11 Standards and Amendments

Module 6 – Wireless Networks and Spread Spectrum Technologies

- Terminology
- Spread Spectrum
- Industrial, Scientific and Medical Bands (ISM)
- Unlicensed National Information Infrastructure Bands (UNII)
- UNII 1,2 and 3
- Narrowband and Spread Spectrum

- Delay Spread
- Frequency Hopping and Spread Spectrum
- Dwell and Hop Time
- Modulation
- Gaussian Frequency Shift Keying
- 802.11 b/g Channels
- Channel Overlap
- Direct Sequence Spread Spectrum (DSSS)
- DSSS Frequency Channel Plan
- Encoding and Modulation
- Packet Binary Convolutional Code
- Orthogonal Frequency Division Multiplexing (OFDM)
- Convolution Coding
- 802.11a Channels

Module 7 – Wireless LAN Topologies

- Wireless Networking Topologies
- Access Point – Client Stations
- Distribution Systems (DS)
- Wireless Distribution System (WDS)
- Service Set Identifier (SSID)
- Basic Service Set (BSS)
- Basic Service Set Identifier (BSSID)
- Basic Service Area (BSA)
- Extended Service Set (ESS)
- ESS Nomadic
- ESS Co-Location
- Independent Basic Service Set (IBSS)
- Configuration Modes
- Infrastructure

Module 8 – Medium Access

- Terminology
- Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)
- CSMA/CA vs CSMA/CD
- Distributed Coordination Function (DCF)
- Interframe Space (IFS)
- Four Types of IFS
- Collision Detection
- Duration/ID Field
- Carrier Sense Methods
- Virtual Carrier Sense
- Physical Carrier Sense
- Random Backoff Time
- Example Flow of 802.11
- Point Coordination Function
- 802.11 Frame Format vs 802.3
- MAC Address Format

- Frame Types
- 802.11 Management Frames
- Control Frames
- Data Frames
- Layer 3 Integration
- Beacon Management Frame
- Beacon Frame Example
- Passive Scanning
- Active Scanning
- Authentication
- Open System Authentication
- Open System Process
- Shared Key Authentication
- Association
- Roaming
- Reassociation
- Disassociation and Deauthentication

Module 9 – MAC Architecture

- ACK Frame
- Fragmentation
- 802.11g Protection Mechanism
- Request to Send/Clear to Send
- RTS/CTS Examples
- CTS to Self
- Power Management
- Power Save Mode
- Traffic Indication Map (TIM)
- Delivery Traffic Indication Message (DITM)
- Announcement Traffic Indication Message (ATIM)
- Wireless Multimedia (WMM)
- Power Save Certification WMM

Module 10 – Wireless Devices

- Wireless LAN Client Devices
- Radio Card Formats
- Radio Card Chipsets
- Client Utilities
- Progression of WLAN Architecture
- Access Point Features
- Wireless Network Management System
- Capabilities of WNMS
- Centralized WLAN Architecture
- WLAN Switch Features
- Centralized WLAN Architecture
- Remote Office WLAN Switch
- Distributed WLAN Architecture
- Unified WLAN Architecture

- Wireless Workgroup Bridge
- Wireless LAN Bridges
- Point to Point and Point to Multi-Point
- Other Features of WLAN Bridges
- Deployment Considerations
- Point to Point Links
- Point to Multi-Point Links
- Enterprise Wireless Gateway (EWG)
- EWG Design
- Residential Wireless Gateway (RWG)
- Other Wireless Routers
- Enterprise Encryption Gateway (EEG)
- Power over Ethernet (PoE)
- PoE Devices
- PoE Responsibilities
- PoE Features

Module 11 – Network Design, Implementation and Management

- Core, Distribution and Access
- Capacity vs Storage
- Co-Location
- Corporate Data Access and the End User
- Network Extension to Remote Areas
- Bridging Building to Building
- Wireless ISP
- Small Office, Home Office (SOHO)
- Hot Spots

Module 12 – WLAN Trouble Shooting

- Troubleshooting Introduction
- Spectrum Analyzer: Wi-Spy
- Wi-Spy Add-On Channelyzer
- 802.11 Coverage Considerations
- Dynamic Rate Switching
- Roaming
- Layer 3 Roaming
- Co-Channel Interference
- Hidden Node
- Hidden Node Solutions
- Near / Far Issues
- Near / Far Solutions
- Interference
- Performance
- Weather Issues

Module 13 – Network Security Architecture

- 802.11 Security Basics
- Encryption

- Segmentation
- MAC Filtering
- SSID Cloaking
- Authentication and Authorization
- Wired Equivalent Privacy (WEP)
- Weak IV Packets
- Wi-Fi Protected Access (WPA)
- WPA Improvements over WEP
- Temporal Key Integrity Protocol (TKIP)
- 802.1X: Extensible Authentication Protocol (EAP) Types
- EAP Advantages and Disadvantages
- 802.1x EAP/TLS Framework
- Dynamic Encryption Key Generation
- Cryptographic Features of WPA2
- WPA2 Encryption Process
- Robust Security Network (RSN)
- 802.11i and WPA/WPA2

Module 14 – Wireless Attacks and Monitoring

- Rogue Access Point
- Countermeasure to the Rogue Access Point
- Peer to Peer Attacks
- Eavesdropping
- Breaking Encryption - Aircrack
- Deauth / Disassociate Attack
- MAC Spoofing
- Denial of Service
- ARP Injection
- Intrusion Detection Monitoring
- Wireless Security Policy

Module 15 – Radio Frequency Site Survey

- WLAN Site Survey Interview
- Customer Briefing
- Business Requirements
- Capacity and Coverage Requirements
- Infrastructure Connectivity
- Security Expectations
- Documentation and Reports
- Forms and Customer Documentation
- Deliverables
- Site Survey Defined
- Mandatory Spectrum Analysis
- Mandatory Coverage Analysis
- Indoor Site Survey Tools
- Outdoor Site Survey Tools
- Coverage Analysis: Manual
- Coverage Analysis: Assisted

- Coverage Analysis: Predictive

Module 16 – Wireless LAN Auditing Tools

- Introduction
- Netstumbler
- Netstumbler and War Driving
- Exporting Netstumbler Results
- War Driving with KNSGEM
- Kismet
- Microsoft Wireless Zero Configuration (WZC)
- Wi-Fi Finders
- Antennas
- Cain and Abel
- OmniPeek Personal
- Auditor Uses
- Manufacturer Defaults
- OS Fingerprinting and Port Scanning
- Port Scan Tips
- Tools
- NMAP
- Services and Ports Used
- Vanilla Port Scan (TCP Connect Port Scan)
- NMAP TCP Connect Scan
- LookatLan
- OS Fingerprinting
- Share Enumerators
- RF Jamming Tools
- Hijacking Tools
- Assessment Types

Module 17 – Gathering Information

- Methods of Obtaining Information
- Physical Access
- Social Access
- Digital Access

** Planet3 Wireless, CWNA and CWSP are registered trademarks or service marks of Planet3 Wireless, Inc.