



[Back to Product Page](#)

## Wireless Network Security Course

**5 Sessions -**

12 Hours of Interactive Training

Prepare to gain your CWSP certification with Tom Carpenter and LearnKey. In LearnKey's Wireless Network Security course, you will learn to implement security solutions to address the various weaknesses in wireless networking. This easy to follow self-paced online training will allow you to learn and understand the sometimes complex world of wireless network security. Join expert instructor Tom Carpenter while he explains basic wireless security principles, different intrusion methods, useful analytical tools, design and implementation considerations, and much more. Complete your eLearning based training in only 15 hours and get ready to take the PWO-204 Exam. At the conclusion of the course, your new skill set will distinguish yourself among other IT professionals and prepare you to pass the CWSP® (Certified Wireless Security Professional) exam.

### Benefits

- Self-Paced Online CWNP authorized Wireless Networking Security course
- Full training for the CWSP

## Session 1

### Section A: Introduction

- Wireless Certifications
- Certification Benefits
- CWSP Exam Objectives
- Types of Attackers
- Importance of Wireless Security

### Section B: Wireless Security Organizations

- Wireless Organizations
- FCC
- IEEE
- Additional Standards
- IETF
- ISO
- PCI
- CWNP
- LearnKey

### Section C: Security Fundamentals

- AAA
- Common Authentication Problems
- Common Authorization Problems
- Common Accounting Problems
- Simple AAA Solutions
- CIA

### Section D: Wireless Threats

- Data Theft
- Eavesdropping
- Denial of Service Attacks
- Resource Use
- Peer-to-Peer Attacks
- Rogue Equipment
- Management Interface Exploits
- Device Damage or Theft
- Social Engineering

### Section E: WEP Cracking

- WZCOOK
- Aircrack-ng
- Installing Aircrack
- Using Aircrack-ng GUI
- Capturing WEP Data
- Crack WEP Keys

### Section F: Eavesdropping

- Locating Wireless Networks
- inSSIDer
- Protocol Analyzer
- Wireshark

exam in just 15 hours

- Increase your Wireless security skills and value in the IT industry

### About The Author

Tom Carpenter has delivered training programs to more than 27,000 professionals since 1997. He has written, developed and delivered courses on: Windows NT, 2000, XP and Server 2003. With experience as a Fortune 1000 system administrator and security officer, Carpenter brings a wealth of real world experience and knowledge to his courses. Tom is Microsoft certified and is one of the founding managers of the Certified Technology Services Professional certification.

## Session 2

### Section A: General Security Policies

- Security Policies Defined
- Password Policy
- Security Training
- Security Awareness
- Security Audits
- Acceptable Use Policies
- Role-Based Access Control
- Management Policies

### Section B: Wireless LAN Security Policies

- Physical Security
- Remote Connectivity
- Traffic Filtering
- Authentication
- Encryption
- VoIP Needs
- Monitoring and Response
- SANS Policy Templates

### Section C: Introducing Authentication

- Authentication Defined
- Credential Types
- Weak Authentication Methods
- Strong Authentication

### Section D: Wireless Authentication Methods

- 802.11 AKM
- Robust Security Networks
- Pre-RSNA Security
- Transition Security Networks
- Roaming and Authentication

### Section E: Implementing Wireless Authentication

- Open System/ Shared Key
- Open System Authentication
- Shared Key Authentication
- Network Layer Authentication

### Section F: Understanding 802.11i

- 802.11 Security
- Four-Way Handshake
- Group Handshake
- Passphrases and PSK Generation
- Master Session Keys
- Pairwise Master Keys
- Group Master Keys
- Pairwise Transient Keys

- Methods
- Passwords and Authentication
- Other Authentication Credentials
- Group Temporal Keys

### Session 3

#### Section A: 802.1X/ EAP Solutions

- 802.1X Components
- 802.1X Illustrated
- Typical 802.1X Deployment
- RADIUS Servers
- User Directories
- AAA Credential Types
- Mutual Authentication Benefits
- RADIUS Server Selection

#### Section B: Implementing a RADIUS Server

- TekRADIUS Features
- Installing TekRADIUS
- Configuring TekRADIUS
- Configuring the Ar4 RADIUS
- EAP Types

#### Section C: Securing Small Businesses

- Push Button Security
- Push Button Interface
- WPS PIN

#### Section D: WEP, WPA, WPA2

- Wired Equivalent Privacy
- 802.11-1997 Authentication
- How WEP Works
- WEP Key Problems
- WEP IV Problems
- WEP Cracking Tools
- Wireless Cracking Process
- WPA/WPA2
- WPA Attacks
- Enabling Security Options

#### Section E: Encryption Ciphers

- Cryptography
- Simple Encryption
- Cryptography Concepts
- Uses of Cryptography
- Types of Encryption
- Symmetric Encryption
- Symmetric Algorithms
- AES
- RC4
- Asymmetric Encryption

- Per-User PSK
- Wi-Fi Voice Personal
- Public Key Cryptography
- Certificates
- Public Key Infrastructure
- PKI Applications
- TKIP and CCMP

### **Section F: Security Auditing**

- Security Auditing Verification
- RSN Information Elements
- Locating Rogue Devices
- Wi-Spy dBx

## **Session 4**

### **Section A: Wireless Intrusion Prevention**

- Intrusion Monitoring Systems
- Intrusion-Detection Systems
- IDS Intrusion Detection
- Intrusion Prevention Systems
- IDS States
- Indications of Intrusion
- IPS Distribution
- IPS Responses

### **Section B: Implementing WIPS**

- WIPS

### **Section E: VPN Security for WLANs**

- Virtual Private Networks
- VPN Applications

### **Section F: Using VLANs with WLANs**

- VLANs
- VLANs in Wireless
- VLAN Trunking
- Configuring Multiple SSIDs
- Mapping SSIDs to VLANs

### **Section G: Secure Management Protocols**

- Unsecured

- Features
  - WIPS Device Detection
  - Configuring WIPS
  - WIPS Integration
  - Wireless Analysis
  - WIPS Deployment Strategies
  - WNMS Solutions
- Management
  - Secure Management
  - Secure Protocol Configuration
  - Secure Management Process

### **Section C: WLAN Management Systems**

- Common WNMS Features
- Network Connectivity
- Configuring WNMS
- Advantages/Limits

### **Section D: Public Network Access**

- Public Networks Defined
- Risks on Public Networks
- Provider Liability
- Security Solutions
- Public Hot Spot Listings

### **Session 5**

#### **Section A: Wireless Endpoint Security**

- Endpoint Security Needs

#### **Section D: Advanced WLAN Security Concepts**

- Role-Based

- Endpoint Security Solutions
- Performance Considerations
- Check Point Endpoint Security
- Microsoft Security Essentials
- Access Control
- Location-Based Access Control
- High Availability
- Captive Portals
- Security Architectures
- MCA/SCA

**Section B:  
Management Frame  
Protection**

- Management Frames
- Control Frames
- Exploiting Management Frames
- Protecting Management Frames
- 802.11w

**Section E:  
Regulatory  
Compliance**

- HIPAA
- HIPAA Requirements
- PCI DSS
- PCI DSS Requirements
- DoD Directive 8100.2
- June 2006 8100.2 Update
- Compliance Process

**Section C: Fast and  
Secure Roaming**

- Roaming
- Fast Secure Roaming
- FSR Applications
- 802.11i and FSR
- 802.11r and FSR
- 802.11k and FSR
- Proprietary FSR
- Initial Mobility Domain

**Section F:  
Performing Risk  
Assessments**

- Risk Analysis Process
- Discovering Assets
- Defining Value
- Determining Risks
- Calculating Risk Ratings
- Risk Management Plans
- Threat Analysis