

# Certified Wireless Security Professional (CWSP)

## Course Overview

This course will teach students about Legacy Security, encryption ciphers and methods, 802.11 authentication methods, dynamic encryption key generation, SOHO 802.11 security, fast secure roaming, wireless security risks, wireless LAN security auditing, wireless security monitoring, VPNs, remote access and Guest Access Services, WLAN security infrastructure, and wireless security policies.

<b><u>Course Introduction</u></b>	3m
Course Introduction	
<b><u>Module 01 - WLAN Security Overview</u></b>	1h 12m
WLAN Security Overview	
Where We Came From	
Standards Organizations	
ISO and the OSI	
ISOC Hierarchy	
Wi-Fi Alliance Standards	
802.11 Networking Basics	
Connection Types	
802.11 Security Basics	
Data Privacy	
AAA	
Segmentation	
Monitoring	
Policy	
Security History	
802.11i and WPA	
RSN (Robust Security Network)	
Future of 802.11 Security	
Demo - Networking Basics	
Demo - Web GUI Introduction	
Demo - Security Options	
Module 01 Review	
<b><u>Module 02 - Legacy Security</u></b>	1h 10m
Legacy Security	
Authentication	
Open System Authentication	
WEP Encryption	
Shared Key Authentication	
More About WEP	
Attacks Against WEP	

VPNs  
VPN Tunneling Protocols  
MAC Filters  
SSID Segmentation  
SSID Cloaking  
Demo - Security Associations  
Demo - MAC Spoofing  
Module 02 Review

**Module 03 - Encryption Ciphers and Methods**

1h 12m

Encryption Ciphers and Methods  
Encryption Basics  
Stream and Block Ciphers  
WLAN Encryption Methods  
WEP Again  
TKIP  
MIC  
TKIP MPDU  
CCMP  
WPA/WPA2  
Proprietary Solutions  
Demo - Encryption Example  
Module 03 Review

**Module 04 - 802.11 Authentication Methods**

1h 18m

802.11 Authentication Methods  
WLAN Authentication Overview  
AAA  
Authentication  
Authorization  
Accounting  
802.1X  
Supplicant Credentials  
Authentication Server Credentials  
EAP  
EAP Process  
Legacy EAP  
Strong EAP Protocols  
PACs  
Demo - Certificate Authority Server Credentials  
Module 04 Review

**Module 05 - Dynamic Encryption Key Generation**

1h

Dynamic Encryption Key Generation  
Dynamic WEP  
RSN  
Management Frames & RSNIE (eNotes)  
RSN (Cont.)  
Authentication and Key Management (AKM)  
RSNA Key Hierarchy

Master Session Key (MSK)  
4-Way Handshake  
Steps of the 4-way Handshake  
Group Key Handshake  
PeerKey Handshake  
Demo - EAP  
Demo - Information Elements  
Module 05 Review

**Module 06 - SOHO 802.11 Security**

57m

SOHO 802.11 Security  
Introduction  
Why a Passphrase  
4-Way Handshake Again  
Risks of WPA/WPA2  
Another Risk Factor of WPA/2  
Wi-Fi Protected Setup (WPS)  
Initial WLAN Setup  
SOHO Best Practices  
Demo - Cracking Hashes  
Module 06 Review

**Module 07 - Fast Secure Roaming**

1h 52m

Fast Secure Roaming  
History of 802.11 Roaming  
Client Roaming Thresholds  
AP to AP Handoff (e-notes)  
Re-Association  
Types of APs  
RSNA Review  
PMKSA  
PMK Caching  
Pre-authentication  
Opportunistic Key Caching (OKC)  
Proprietary FSR  
FT Key Hierarchy (e-notes)  
FT Initial Mobility Domain Association  
Over the Air Fast BSS Transition (e-notes)  
Over the Air DS Fast BSS Transition (e-notes)  
802.11K-2008  
Voice Personal and Voice Enterprise  
L3 Roaming  
Mobile IP  
Troubleshooting  
Module 07 Review

## **Module 08 - Wireless Security Risks**

54m

Wireless Security Risks

Introduction

Rogue Devices

Rogue Prevention

Eavesdropping

Authentication Attacks

DoS

L2 DoS

802.11w

MAC Spoofing

Wireless Hijacking

Peer-to-Peer Attacks

Management Interface Exploits

Physical Damage and Theft

Social Engineering

Public Access and WLAN Hotspots

Demo - Rogue Devices

Demo - Public Hotspots

Module 08 Review

## **Module 09 - Wireless LAN Security Auditing**

28m

Wireless LAN Security Auditing

Purpose of Auditing

WLAN Audits

Layer 1 Audit

Layer 2 Audit

Penetration Testing

Wired Infrastructure Audit

Social Engineering

WIPS Audit

Documenting the Audit

Recommendations

WLAN Security Auditing Tools

Module 09 Review

## **Module 10 - Wireless Security Monitoring**

39m

Wireless Security Monitoring

WIDS/WIPS

Sensor Placement

Example of Rogue Detection (e-notes)

Device Tracking

Signature Analysis

Behavioral Analysis

Other Types of Monitoring

More on Monitoring

Module 10 Review

**Module 11 - VPNs, Remote Access and Guest Access Services**

37m

VPNs, Remote Access and Guest Access Services

VPN Review

Remote Access

Module 11 Review

**Module 12 - WLAN Security Infrastructure**

1h 17m

WLAN Security Infrastructure

WLAN Architecture

Lightweight or Controller Based APs (e-notes)

Other Controller Based Definitions

Device Management

Management Protocols

Controller Communications

Authorization Servers

Deployment Architectures

Other RADIUS Solutions

RBAC

Other Security Systems

Module 12 Review

**Module 13 - Wireless Security Policies**

32m

Wireless Security Policies

General Policy

Policy Creation

Policy Management

Functional Policy

Password Policy

Other Policies

Government and Industry Regulations

Module 13 Review

Course Closure

**Total Duration: 13h 11m**