

# CWSP (CERTIFIED WIRELESS SECURITY PROFESSIONAL) 1

## Objetivo

• Define WLAN security Requirements; • Develop WLAN security policies; • Identify potential vulnerabilities and threats to determine the impact on the WLAN and supporting systems and verify, mitigate, and remediate them; • Describe and perform risk analysis and risk mitigation procedures; • Select the appropriate security solution for a given implementation and ensure it is installed and configured according to policy requirements; • Implement or recommend appropriate wired security configurations to support the WLAN; • Implement authentication and security services; • Implement secure transitioning (roaming) solutions; • Secure public access and/or open networks; • Implement preventative measures required for common vulnerabilities associated with wireless infrastructure devices and avoid weak security solutions; • Understand and implement management within the security lifecycle of identify, assess, protect, and monitor; • Use effective change management procedures including documentation, approval, and notifications; • Use information from monitoring solutions for load observation and forecasting of future requirements to comply with security policy; • Implement effective auditing procedures to perform audits, analyze results, and generate reports.

## Público Alvo

Recommended training for professionals interested on Securing Wireless Networks, and who will take the CWSP certification exam.

## Pré-Requisitos

Participation in CWNA training or equivalent knowledge.

## Carga Horária

40 horas (5 dias).

## Conteúdo Programático

### Course Introduction

Course Outline

Course Goals & Objectives

### Introduction to WLAN Security Technology

Security policy

Security concerns

Security auditing practices

Application layer vulnerabilities and analysis

Data Link layer vulnerabilities and analysis

Physical layer vulnerabilities and analysis

802.11 security mechanisms  
Legacy WLAN security methods, mechanisms, and exploits  
Wi-Fi Alliance security certifications

### **WLAN Mobile Endpoint Security Solutions**

Enterprise-class mobile endpoint security  
User-accessible and restricted endpoint policies  
VPN technologies common for client devices

### **SOHO and SMB WLAN Security Technologies and Solutions**

General vulnerabilities  
Preshared Key security with RSN cipher suites  
Passphrase vulnerabilities  
Passphrase entropy and hacking tools  
WPA/WPA2 Personal – how it works  
WPA/WPA2 Personal – configuration  
Installation and configuration of WIPS, WNMS, and WLAN controllers to extend enterprise security policy to remote and branch offices  
Remote/branch office VPN technologies common for infrastructure devices

### **Enterprise WLAN Management and Monitoring**

Device identification and tracking  
Rogue device detection and mitigation  
WLAN forensics and data logging  
Enterprise WIPS installation and configuration  
Protocol analysis  
WNMS security features  
WLAN controller security feature sets

### **Enterprise WLAN Security Technology and Solutions**

Robust Security Networks (RSN)  
WPA/WPA2 Enterprise – how it works  
WPA/WPA2 Enterprise – configuration  
IEEE 802.11 Authentication and Key Management (AKM)  
802.11 cipher suites  
Use of authentication services (RADIUS, LDAP) in WLANs  
User profile management (RBAC)  
Public Key Infrastructures (PKI) used with WLANs  
Certificate Authorities and X.509 digital certificates  
RADIUS installation and configuration  
802.1X/EAP authentication mechanisms  
EAP types and differences  
802.11 handshakes and exchanges  
Fast BSS Transition (FT) technologies (FSR—Fast Secure Roaming)  
Captive portals and guest networking

### **labs Outline**

## Wlan Security Connectivity

This lab is focused on WLAN AP/controller and client device security, and primarily covers the following areas:

- Secure access to the AP/controller using secure management protocols;
- Configuring multiple WLAN profiles, each with its own authentication and cipher suites including WPA/WPA2 Personal and Enterprise;
- Configuring client devices to connect to the WLAN infrastructure using secure protocols including WPA/WPA2 Personal and Enterprise;
- Creating user or group policies that provide network services to clients based on their authorization level;
- Understanding integrated WPS configuration, policies, and monitoring.

## 802.1X/EAP Configuration

This lab is focused on 802.1X/EAP security. WPA/WPA2-Enterprise relies on secure authentication via 802.1X/EAP, often utilizing an enterprise's backend authentication infrastructure, including RADIUS servers as well as user databases. In this lab, we will gain first-hand knowledge of this process and the configuration details involved. This lab group covers the following exercises:

- Setting up a RADIUS server and a user credential database with EAP support
- Creating and using server certificates and installing the certificate on client devices
- Configuring the WLAN AP/controller for 802.1X with RADIUS connectivity
- Configuring EAP types, user credentials, and certificates on the client devices

## Wireless Intrusion Prevention Systems (WIPS)

This lab module is focused on Wireless Intrusion Prevention Systems (WIPS). WIPS are known for three overriding functions: security monitoring, performance monitoring, and reporting. In this lab exercise, we will focus on security monitoring and reporting. Areas of particular interest include:

- WIPS installation, licensing, adding/configuring sensors, and secure console connectivity;
- Configuring WLAN profiles according to organizational security policies;
- Properly classifying authorized, unauthorized, and external/interfering access points;
- Identifying and mitigating rogue devices;
- Identifying specific attacks against the authorized WLAN infrastructure or client stations.

## Using Laptop-based Protocol and Spectrum Analyzers

This lab is focused on the use of laptop analyzers for spectrum analysis, protocol analysis, and WLAN discovery. Understanding driver issues, security-related protocol analysis (authentication and encryption), and spectrum analysis will aid the wireless security professional in policy compliance, proper implementation, and troubleshooting. The following steps will be covered in this lab exercise:

- Installing and configuring a WLAN discovery tool, a laptop protocol analyzer, and a laptop spectrum analyzer;
- Locating and analyzing 2.4 GHz and 5 GHz WLANs with a WLAN discovery tool and protocol analyzer;
- Capturing and analyzing WPA2-Personal and Enterprise (among others) authentication sequences in a WLAN protocol analyzer;
- Capturing and analyzing Hotspot authentication and data traffic in a WLAN protocol analyzer;
- Capturing and analyzing common frame types and security elements with a WLAN protocol analyzer;
- Viewing a normal RF environment, a busy RF environment, RF interference sources, and an RF attack on the WLAN in a spectrum analyzer.

## Fast Secure Roaming

This lab is focused on fast secure roaming (FSR) within an Extended Service Set. Moving quickly and securely between access points attached to the same distribution system is a requirement of real-time mobility devices such as VoWiFi phones and mobile video devices. Understanding the standards-based and proprietary processes

of a Fast Transition (FT) service will help network designers support strong security and fast roaming simultaneously. The following steps will be covered in this lab exercise:

- Configure a WLAN infrastructure roaming scenario with multiple APs and possibly multiple controllers
- Utilize a RADIUS server for 802.1X/EAP authentication and the WLAN infrastructure for simpler forms of security;
- Configure a client device for EAP authentication using the CCMP cipher suite;
- Configure an 802.11 protocol analyzer to capture the roaming transition;
- Perform a slow BSS transition as a baseline, testing open authentication, WEP, WPA2-Personal, and WPA2-Enterprise;
- Enable fast secure roaming mechanisms within the infrastructure and on the client station and perform a fast transition;
- Conduct the same tests across a Layer-3 IP boundary as well as between controllers.

### **Network Attacks and Auditing**

This lab is focused on understanding and conducting common network attack sequences. Defensive network security requires an understanding of offensive attacks. Auditing is the process of validating a security solution, and understanding auditing tools is an important skill for administrators and consultants. This module will be tailored to the class, but covers topics like the following:

- Conducting authentication and encryption cracking attacks;
- Conducting simple attacks/workarounds like MAC spoofing;
- Performing basic protocol analysis and eavesdropping;
- Attempting advanced attacks like session hijacking, packet injection, replay attacks, and protocol DoS attacks.