+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated on 09/17/2026

Sign Up

Wi-Fi Penetration Testing Expert (CWPE) Certification Training

5 days (35 hours)

Overview

The Wi-Fi Penetration Testing Expert (CWPE) Certification Training prepares you to demonstrate the advanced skills required to audit, compromise, and secure enterprise Wi-Fi environments.

The official Hack The Box (HTB) CWPE certification assesses your ability to conduct a realistic wireless penetration test, from reconnaissance through to gaining access to an internal network. It covers WEP, WPA, WPA2, WPA3 protocols, and WPA-Enterprise architectures.

This course enables you to develop a penetration testing methodology tailored to wireless networks, analyze 802.11 frames, identify vulnerable configurations, and select appropriate attack techniques within an authorized framework.

You will learn to exploit vulnerabilities related to WPS, authentication exchanges, passwords, captive portals, and malicious access points. You will also implement scenarios involving Evil Twin attacks, interception, relay attacks, and pivoting to the internal information system.

Upon completion of the Wi-Fi Pentesting Expert (CWPE) Certification Training, you will be able to prepare for the HTB CWPE hands-on exam, conduct an end-to-end assessment, document an attack chain, and produce a professional report in English with actionable remediation recommendations.

Like all our courses, this one will introduce you to **the latest stable version** of the technology and its new features.

Objectives

- Master an advanced Wi-Fi penetration testing methodology
- Assess the security of WEP, WPA, WPA2, WPA3, and WPA-Enterprise networks
- Carry out reconnaissance, interception, compromise, and pivot attacks
- Use wireless penetration testing tools appropriate for each scenario
- Prepare for the HTB CWPE practical exam and certification report

Target Audience

- Penetration Tester
- Red Teamers
- Cybersecurity consultant
- Security Auditor
- Network and Security Administrator

Prerequisites

- Proficiency with the Linux command line
- Solid knowledge of TCP/IP networks, DNS, DHCP, and routing
- Understanding of the security principles of 802.11 protocols
- Previous experience in penetration testing and network traffic analysis
- Basic knowledge of Active Directory administration and Kerberos authentication

Technical Requirements

- Computer running Windows 11, macOS, or Linux with installation privileges
- 64-bit processor, 16 GB of RAM recommended, and at least 40 GB of available disk space
- Kali Linux virtual machine via VMware Workstation or VirtualBox
- A modern WebRTC-compatible browser for accessing lab environments
- Stable internet connection supporting VPN and RDP connections

Curriculum for our Wi-Fi Pentesting Expert (CWPE) Training Course

[Day 1 - Morning]

Methodological Framework and 802.11 Architecture

- Overview of the HTB CWPE certification, expectations for the practical exam, and rules of engagement
- 802.11 architecture, frequency bands, channels, and the roles of access points and clients
- Analysis of management, control, and data frames
- Wireless interface modes, monitor mode, and principles of radio data collection
- Overview of Wi-Fi authentication and encryption mechanisms
- Hands-on workshop: Setting up an isolated test environment and analyzing 802.11 frame captures.

[Day 1 - Afternoon]

Wireless reconnaissance and enumeration

- Defining the scope, gathering information, and tracking actions
- Discovering SSIDs, BSSIDs, channels, clients, and hidden networks
- Identifying security protocols, advertised capabilities, and configuration errors
- Advanced use of Airodump-ng, Kismet, Sparrow WiFi, and WiGLE
- Prioritizing attack vectors based on exposure and business value
- Hands-on workshop: Conduct a comprehensive reconnaissance of a simulated Wi-Fi environment and produce an actionable map.

[Day 2 - Morning]

Attacks on legacy protocols

- Structural weaknesses of WEP and criteria for identifying a vulnerable network
- Reinjection attacks, IV collection, and key recovery
- Risk analysis related to WPS, PIN codes, and flawed implementations
- Brute-force approaches, Pixie Dust attacks, and evaluation of security measures
- Documentation of technical evidence and recommendations for replacing obsolete configurations
- Hands-on workshop: Exploiting a controlled WEP and WPS scenario, then documenting the associated security findings
  .

[Day 2 - Afternoon] WPA

and WPA2 Personal

- How the 4-Way Handshake, PMK, PTK, and GTK work
- Capturing and validating WPA2-PSK authentication exchanges
- Collecting and analyzing PMKID identifiers
- Targeted cracking strategies, transformation rules, and dictionary optimization
- Using Aircrack-ng, Hashcat, Pyrit, and Pmkidcracker
- Hands-on Workshop: Capturing a handshake, building a cracking strategy, and demonstrating the recovery of a WPA2 password in a lab.

[Day 3 - Morning]

WPA Enterprise and EAP Attacks

- WPA-Enterprise architecture, the role of the RADIUS server, and EAP methods
- Analysis of PEAP, EAP-TTLS, EAP-TLS, EAP-MD5, and MSCHAPv2 traffic

- Recognition of certificates, certificate authorities, and authentication parameters
- Techniques for downgrading, relaying, and collecting credentials within an authorized environment
- Evaluation of client-side certificate validation controls
- Hands-on workshop: Analyze a simulated Enterprise authentication and identify an attack vector related to insufficient certificate validation.

[Day 3 - Afternoon]

Malicious access points and interception

- Designing Evil Twin, Karma, and Mana attacks
- Creating fake access points and controlled deauthentication scenarios
- Customizing captive portals for credential harvesting exercises
- Using EAPHammer, Wifipumpkin3, Airgeddon, and Bettercap
- Detection of attack indicators and defensive measures on the infrastructure and endpoints
- Hands-on workshop: Deploy an Evil Twin in a cyber range, observe the generated traffic, and document countermeasures.

[Day 4 - Morning]

WPA3 and modern protection mechanisms

- Principles of WPA3, SAE, OWE, PMF, and transition mode
- Recognizing WPA3-Personal and WPA3-Enterprise networks
- Analysis of downgrade, Evil Twin, and online brute-force attack scenarios
- Study of attacks specific to OWE and SAE deployments
- Evaluation of the robustness of configurations and hardening measures
- Hands-on workshop: examine a simulated WPA3 deployment, test its transition modes, and develop a remediation plan.

[Day 4 - Afternoon]

Captive portals, routers, and initial access

- Modeling the attack surfaces of captive portals and guest networks
- Bypassing controls via MAC spoofing, ARP poisoning, and DNS tunneling
- Traffic interception and man-in-the-middle attacks
- Searching for firmware vulnerabilities and targeted exploitation of routers
- Collecting Wi-Fi secrets from compromised hosts and assessing the impact
- Hands-on workshop: Compromising a simulated guest segment, analyzing an exposed router, and demonstrating controlled initial access.

[Day 5 - Morning]

Internal Pivoting and Active Directory Compromise

- Transitioning from a Compromised Wireless Connection to Internal Network Reconnaissance
- Enumerating services, shares, identities, and trust relationships
- Establishing a foothold in Active Directory from an Enterprise Wi-Fi attack
- Principles of lateral movement, privilege escalation, and maintaining access in a lab
- Chaining evidence to assess the impact of a domain compromise
- Hands-on workshop: Follow a complete attack chain from a simulated Enterprise Wi-Fi network to an Active Directory environment.

[Day 5 - Afternoon]

Mock exam and professional report

- Structure of the HTB CWPE practical assessment and time management over seven days
- Black-box approach, note-taking, hypothesis validation, and handling dead ends
- Structuring a penetration test report in English: evidence, impact, severity, and remediation
- Review of common errors and quality criteria for a certification submission
- Individual preparation plan to complete the Wi-Fi Penetration Tester track
- Hands-on workshop: conducting a mini exam simulation, reconstructing an attack chain, and producing a client-focused report summary.

Target Audience

This training is intended for both individuals and companies—large or small—seeking to train their teams in new, advanced IT technologies or to acquire specific industry knowledge or modern methodologies.

Entry-Level Assessment

The pre-training assessment complies with Qualiopi quality standards. Upon final registration, the learner receives a self-assessment questionnaire that allows us to evaluate their estimated proficiency in various types of technologies, as well as their expectations and personal goals for the upcoming training, within the limits imposed by the selected format. This questionnaire also allows us to anticipate certain connection or internal security issues within the company (intra-company or virtual classroom) that could pose challenges for monitoring and ensuring the smooth running of the training session.

Teaching Methods

Hands-On Training: 60% Practical, 40% Theoretical. Training materials distributed in digital format to all participants.

Organization

The course alternates between theoretical input from the instructor—supported by examples and reflection sessions—and group work.

Assessment

At the end of the session, a multiple-choice quiz is administered to verify that participants have successfully acquired the skills.

Certification

A certificate will be issued to each trainee who has completed the entire training program.

Training organization registered under number 11 75 54743 75. This registration does not constitute state accreditation.
© Ambient IT 2015-2026. All rights reserved. Paris, France - Switzerland - Belgium - Luxembourg