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

Mis à jour le 17/09/2026

S'inscrire

Formation Certification Wi-Fi Pentesting Expert (CWPE)

5 jours (35 heures)

Présentation

La Formation Certification Wi-Fi Pentesting Expert (CWPE) vous prépare à valider les compétences avancées requises pour auditer, compromettre et sécuriser des environnements Wi-Fi d'entreprise.

La certification officielle HTB CWPE de Hack The Box évalue votre capacité à conduire un test d'intrusion sans fil réaliste, depuis la reconnaissance jusqu'à l'accès à un réseau interne. Elle couvre les protocoles WEP, WPA, WPA2, WPA3 et les architectures WPA-Enterprise.

Cette formation vous permet de structurer une méthodologie de pentest adaptée aux réseaux sans fil, d'analyser les trames 802.11, d'identifier les configurations exposées et de sélectionner les techniques d'attaque pertinentes dans un cadre autorisé.

Vous apprendrez à exploiter les faiblesses liées à WPS, aux échanges d'authentification, aux mots de passe, aux portails captifs et aux points d'accès malveillants. Vous mettrez également en oeuvre des scénarios de Evil Twin, d'interception, de relais et de pivot vers le système d'information interne.

À l'issue de la Formation Certification Wi-Fi Pentesting Expert (CWPE), vous saurez préparer l'examen pratique HTB CWPE, conduire une évaluation de bout en bout, documenter une chaîne d'attaque et produire un rapport professionnel en anglais avec des recommandations de remédiation actionnables.

Comme toutes nos formations, celle-ci vous présentera **la dernière version stable** de la technologie et ses nouveautés.

Objectifs

- Maîtriser une méthodologie avancée de test d'intrusion Wi-Fi
- Évaluer la sécurité des réseaux WEP, WPA, WPA2, WPA3 et WPA-Enterprise
- Mettre en oeuvre des attaques de reconnaissance, d'interception, de compromission et de pivot
- Exploiter les outils de pentest sans fil adaptés à chaque scénario
- Préparer l'examen pratique et le rapport de certification HTB CWPE

Public visé

- Pentester
- Red Teamer
- Consultant en cybersécurité
- Auditeur sécurité
- Administrateur réseau et sécurité

Pré-requis

- Maîtrise de la ligne de commande Linux
- Connaissances solides des réseaux TCP/IP, DNS, DHCP et du routage
- Compréhension des principes de sécurité des protocoles 802.11
- Expérience préalable en tests d'intrusion et en analyse de trafic réseau
- Notions d'administration Active Directory et d'authentification Kerberos

Pré-requis techniques

- Poste sous Windows 11, macOS ou Linux avec droits d'installation
- Processeur 64 bits, 16 Go de RAM recommandés et au moins 40 Go d'espace disque disponible
- Machine virtuelle Kali Linux via VMware Workstation ou VirtualBox
- Navigateur récent compatible WebRTC pour l'accès aux environnements de laboratoire
- Connexion Internet stable autorisant les connexions VPN et RDP

Programme de notre formation Wi-Fi Pentesting Expert (CWPE)

[Jour 1 - Matin]

Cadre méthodologique et architecture 802.11

- Positionnement de la certification HTB CWPE, attendus de l'examen pratique et règles d'engagement
- Architecture 802.11, bandes de fréquences, canaux, rôles des points d'accès et clients
- Analyse des trames de management, de contrôle et de données
- Modes d'interface sans fil, mode moniteur et principes de collecte radio
- Cartographie des mécanismes d'authentification et de chiffrement Wi-Fi
- Atelier pratique : préparer un environnement de test isolé et analyser des captures de trames 802.11.

[Jour 1 - Après-midi]

Reconnaissance et énumération sans fil

- Définition du périmètre, collecte des informations et traçabilité des actions
- Découverte des SSID, BSSID, canaux, clients et réseaux masqués
- Identification des protocoles de sécurité, des capacités annoncées et des erreurs de configuration
- Utilisation avancée de Airodump-ng, Kismet, Sparrow WiFi et WiGLE
- Priorisation des vecteurs d'attaque selon l'exposition et la valeur métier
- Atelier pratique : réaliser la reconnaissance complète d'un environnement Wi-Fi simulé et produire une cartographie exploitable.

[Jour 2 - Matin]

Attaques sur les protocoles historiques

- Faiblesses structurelles de WEP et critères d'identification d'un réseau vulnérable
- Attaques par réinjection, collecte d'IV et récupération de clé
- Analyse des risques liés à WPS, aux codes PIN et aux implémentations défaillantes
- Approches de bruteforce, attaques Pixie Dust et évaluation des protections
- Formalisation des preuves techniques et recommandations de remplacement des configurations obsolètes
- Atelier pratique : exploiter un scénario WEP et WPS contrôlé, puis rédiger les constats de sécurité associés.

[Jour 2 - Après-midi]

WPA et WPA2 Personal

- Fonctionnement du 4-Way Handshake, de la PMK, de la PTK et de la GTK
- Capture et validation des échanges d'authentification WPA2-PSK
- Collecte et exploitation des identifiants PMKID
- Stratégies de cassage ciblé, règles de transformation et optimisation des dictionnaires
- Utilisation de Aircrack-ng, Hashcat, Pyrit et Pmkidcracker
- Atelier pratique : capturer un handshake, construire une stratégie de cassage et démontrer la récupération d'un accès WPA2 dans un laboratoire.

[Jour 3 - Matin]

WPA Enterprise et attaques EAP

- Architecture WPA-Enterprise, rôle du serveur RADIUS et méthodes EAP
- Analyse des flux PEAP, EAP-TTLS, EAP-TLS, EAP-MD5 et MSCHAPv2

- Reconnaissance des certificats, des autorités de certification et des paramètres d'authentification
- Techniques de downgrade, de relais et de collecte d'identifiants dans un périmètre autorisé
- Évaluation des contrôles de validation des certificats côté client
- Atelier pratique : analyser une authentification Enterprise simulée et identifier un chemin d'attaque lié à une validation de certificat insuffisante.

[Jour 3 - Après-midi]

Points d'accès malveillants et interception

- Conception d'attaques Evil Twin, Karma et Mana
- Création de faux points d'accès et scénarios de déauthentification contrôlée
- Personnalisation de portails captifs pour les exercices de collecte d'identifiants
- Usage de EAPHammer, Wifipumpkin3, Airgeddon et Bettercap
- Détection des indicateurs d'attaque et mesures de défense côté infrastructure et terminaux
- Atelier pratique : déployer un Evil Twin dans un cyber range, observer les flux générés et documenter les contre-mesures.

[Jour 4 - Matin]

WPA3 et mécanismes de protection modernes

- Principes de WPA3, SAE, OWE, PMF et mode de transition
- Reconnaissance des réseaux WPA3-Personal et WPA3-Enterprise
- Analyse des scénarios de downgrade, d'Evil Twin et de bruteforce en ligne
- Étude des attaques spécifiques aux déploiements OWE et SAE
- Évaluation de la robustesse des configurations et des mesures de durcissement
- Atelier pratique : examiner un déploiement WPA3 simulé, tester ses modes de transition et établir un plan de remédiation.

[Jour 4 - Après-midi]

Portails captifs, routeurs et accès initial

- Modélisation des surfaces d'attaque des portails captifs et réseaux invités
- Contournement de contrôles par usurpation MAC, empoisonnement ARP et tunneling DNS
- Interception de trafic et attaques de type Man-in-the-Middle
- Recherche de vulnérabilités de firmware et exploitation raisonnée de routeurs
- Collecte des secrets Wi-Fi depuis des hôtes compromis et qualification de l'impact
- Atelier pratique : compromettre un segment invité simulé, analyser un routeur exposé et démontrer un accès initial contrôlé.

[Jour 5 - Matin]

Pivot interne et compromission Active Directory

- Passage d'un accès sans fil compromis à la reconnaissance du réseau interne
- Énumération des services, des partages, des identités et des relations de confiance
- Établissement d'un foothold dans Active Directory depuis une attaque Wi-Fi Enterprise
- Principes de mouvement latéral, élévation de privilèges et maintien d'accès dans un laboratoire
- Chaînage des preuves pour mesurer l'impact d'une compromission de domaine
- Atelier pratique : suivre une chaîne d'attaque complète d'un réseau Wi-Fi Enterprise simulé vers un environnement Active Directory.

[Jour 5 - Après-midi]

Simulation d'examen et rapport professionnel

- Déroulement de l'évaluation pratique HTB CWPE et gestion du temps sur sept jours
- Approche black box, prise de notes, validation des hypothèses et gestion des impasses
- Structuration d'un rapport de pentest en anglais, preuves, impact, sévérité et remédiations
- Relecture des erreurs fréquentes et critères de qualité d'une soumission de certification
- Plan de préparation individuel pour finaliser le parcours Wi-Fi Penetration Tester
- Atelier pratique : réaliser une mini simulation d'examen, restituer une chaîne d'attaque et produire une synthèse de rapport orientée client.

Sociétés concernées

Cette formation s’adresse à la fois aux particuliers ainsi qu’aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d’auto-évaluation nous permettant d’apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d’anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l’acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.