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

Mis à jour le 13/11/2026

S'inscrire

Formation Certification Certified Lead Ethical Hacker (CLEH)

5 jours (35 heures)

Présentation

Le hacking éthique permet d'évaluer la sécurité des systèmes et des réseaux au moyen de tests autorisés. La certification officielle Certified Lead Ethical Hacker (CLEH) évalue les compétences nécessaires pour rechercher des vulnérabilités, conduire une exploitation contrôlée et documenter les résultats d'un test d'intrusion.

Notre Formation Certification Certified Lead Ethical Hacker (CLEH) vous permettra de préparer l'examen en développant une démarche structurée, de la définition du périmètre à la restitution des constats.

Vous apprendrez à conduire la reconnaissance, à identifier les vulnérabilités, à sélectionner des techniques d'exploitation et à maîtriser les principes d'élévation de privilèges et de pivotement dans un laboratoire autorisé.

À l'issue de la formation, vous serez en mesure de relier les méthodologies de pentest aux cadres réglementaires et aux standards, de collecter des preuves et de produire un rapport exploitable pour améliorer la sécurité.

Cette préparation associe ateliers pratiques, cas de certification et mises en situation chronométrées. Le passage de l'examen est proposé sur une session dédiée. L'obtention du titre reste soumise à la réussite de l'examen et aux exigences d'expérience de l'organisme certificateur.

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

Objectifs

- Maîtriser les concepts, méthodes et techniques du hacking éthique et des tests d'intrusion
- Relier les méthodologies de pentest aux cadres réglementaires et aux standards de sécurité
- Identifier et valider des vulnérabilités dans un périmètre explicitement autorisé
- Appliquer les principes d'exploitation, d'élévation de privilèges et de pivotement en laboratoire
- Documenter les preuves et formuler des recommandations de remédiation
- Préparer les épreuves pratiques et la rédaction du rapport de certification

Public visé

- Pentester
- Consultant en cybersécurité
- Analyste sécurité
- Ingénieur sécurité des systèmes et réseaux
- Responsable de la sécurité des systèmes d'information

Pré-requis

- Connaissance des principes de sécurité de l'information et de gestion des vulnérabilités
- Bonne maîtrise de l'administration et de la ligne de commande sous Linux et Windows
- Compréhension des réseaux TCP/IP et des services DNS et HTTP
- Notions de programmation ou de scripting avec Python ou Bash
- Capacité à lire une documentation technique en anglais

Pré-requis techniques

- Ordinateur avec 8 Go de mémoire vive recommandés et écran adapté à l'utilisation simultanée du laboratoire et des supports
- Navigateur Google Chrome ou Mozilla Firefox à jour pour accéder au laboratoire distant et à ses machines virtuelles
- Connexion Internet stable permettant les accès aux plateformes pédagogiques, avec autorisations réseau validées avant la session
- Compte d'accès au laboratoire fourni pour la formation et compte myPECB à créer pour l'inscription à l'examen
- Pour l'examen à distance, webcam, microphone et installation de PECB Exams sur un poste compatible avec les exigences communiquées à l'inscription

Programme de notre formation Certified Lead Ethical Hacker (CLEH)

[Jour 1 - Matin]

Fondamentaux du hacking éthique

- Concepts du hacking éthique et rôles des acteurs d’une mission de sécurité offensive

- Différences entre audit de sécurité, analyse de vulnérabilités et test d’intrusion
- Cycle d’un pentest, de la préparation à la restitution des résultats
- Domaines de compétences et logique des épreuves de Certified Lead Ethical Hacker (CLEH)
- Atelier pratique : Analyser une demande de pentest et associer les activités proposées aux domaines de certification.

[Jour 1 - Après-midi]

Cadrage et méthodologies de test

- Définition du périmètre autorisé, des exclusions et des objectifs de mission
- Formalisation des règles d’engagement, des conditions d’arrêt et des contacts d’urgence
- Apports de NIST SP 800-115 et du OWASP WSTG à la structuration des tests
- Articulation entre cadres réglementaires, standards, exigences contractuelles et preuves attendues
- Organisation du laboratoire isolé et protection des données collectées
- Atelier pratique : Rédiger un périmètre de mission et une matrice reliant objectifs, référentiels et tests autorisés.

[Jour 2 - Matin]

Reconnaissance et collecte d’informations

- Distinction entre reconnaissance passive et reconnaissance active
- Collecte d’informations publiques et identification de la surface d’exposition
- Découverte des hôtes et des services avec Nmap dans le périmètre de laboratoire
- Énumération des services DNS, HTTP et SMB
- Consolidation des résultats et traçabilité des preuves techniques
- Atelier pratique : Cartographier un réseau de laboratoire et constituer un inventaire commenté des services exposés.

[Jour 2 - Après-midi]

Menaces et analyse des vulnérabilités

- Identification des actifs, des points d’entrée et des scénarios de menace
- Recherche de vulnérabilités connues et analyse des mauvaises configurations
- Interprétation des résultats de scanners et validation des faux positifs
- Priorisation selon l’exposition, l’exploitabilité et l’impact métier
- Sélection des hypothèses d’exploitation et définition des critères de réussite
- Atelier pratique : Analyser les vulnérabilités d’un environnement fictif et construire un plan de validation priorisé.

[Jour 3 - Matin]

Exploitation contrôlée des services

- Principes d’exploitation et vérification des préconditions techniques
- Sélection d’une preuve de concept et appréciation du risque opérationnel
- Prise en main de Metasploit Framework dans un environnement volontairement vulnérable
- Gestion des accès de test et collecte de preuves reproductibles
- Limitation des impacts et respect des conditions d’arrêt
- Atelier pratique : Valider une vulnérabilité sur une machine dédiée et documenter les conditions de l’accès obtenu.

[Jour 3 - Après-midi]

Tests d’intrusion des applications web

- Analyse des échanges HTTP avec un proxy d’interception
- Utilisation de Burp Suite Community Edition pour examiner les requêtes et les réponses
- Vérification de l’authentification, des sessions et des contrôles d’accès
- Identification des injections et des défauts de validation des entrées
- Organisation des tests et des constats selon le OWASP WSTG
- Atelier pratique : Examiner une application volontairement vulnérable et rédiger une fiche de constat avec preuve et remédiation.

[Jour 4 - Matin]

Élévation de privilèges et post-exploitation

- Énumération locale après obtention d’un accès initial
- Analyse des permissions, des services et des tâches sous Linux et Windows
- Identification des configurations favorisant l’élévation de privilèges
- Évaluation des accès obtenus et de leur impact sur les actifs
- Gestion des données sensibles, conservation des preuves et nettoyage des artefacts de test
- Atelier pratique : Identifier une mauvaise configuration locale, valider son impact dans le laboratoire et proposer une correction.

[Jour 4 - Après-midi]

Pivotement et rapport de pentest

- Principes de pivotement entre segments d’un réseau de laboratoire
- Choix des mécanismes de transfert de fichiers et contrôle de leur intégrité
- Traçabilité du chemin d’accès et démonstration des impacts cumulés
- Structure du rapport technique, synthèse exécutive et annexes de preuves
- Priorisation des remédiations et préparation des tests de vérification
- Atelier pratique : Réaliser un pivotement autorisé entre deux segments et produire un rapport synthétique du scénario testé.

[Jour 5 - Matin]

Mise en situation de certification

- Révision des domaines de collecte d’informations et d’identification des vulnérabilités
- Consolidation des techniques d’exploitation, d’élévation de privilèges et de pivotement
- Organisation des notes et des ressources pour une épreuve à livre ouvert
- Gestion du temps, priorisation des pistes et préparation du journal de preuves
- Atelier pratique : Conduire la première partie d’un pentest blanc chronométré sur un laboratoire comportant plusieurs machines cibles.

[Jour 5 - Après-midi]

Restitution et préparation finale à l’examen

- Finalisation du scénario blanc et vérification des preuves de compromission
- Rédaction d’un rapport d’examen clair, reproductible et organisé par cible
- Relecture des constats, des impacts et des recommandations correctives
- Analyse des erreurs fréquentes et construction d’un plan de révision individuel
- Modalités du passage officiel sur session dédiée et distinction entre réussite à l’examen et attribution du titre
- Atelier pratique : Finaliser le rapport du pentest blanc et réaliser une revue croisée à partir d’une grille pédagogique de préparation.

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.

Organisme de formation enregistré sous le numéro 11 75 54743 75. Cet enregistrement ne vaut pas agrément de l’État.
© Ambient IT 2015-2026. Tous droits réservés. Paris, France - Suisse - Belgique - Luxembourg