Formation CLEH, Certified Lead Ethical Hacker

S'initier à la conduite de piratage éthique

N° ACTIVITÉ : 11 92 18558 92 | TÉLÉPHONE : 01 85 77 07 07 | E-MAIL : inscription@hubformation.com

Référence	SEC202
Durée	5 jours (35h)
Tarif	4 190 €HT
Certification	- €HT

Objectifs

| Identifier et connaître les référentiels liés au pentest
| Prendre connaissance des outils et source de veille
| Savoir mener une analyse de vulnérabilité sur un système Linux et Windows
| Identifier l'exploitation et la post-exploitation des différents environnements
| Préparer et passer l'examen de certification "CLEH, Certified Lead Ethical Hacker" du PECB

Public

| Professionnels de la cybersécurité
| Spécialistes des TI

Prérequis

| Connaissance de base d'un système Linux et Windows
| Connaissance des réseaux et modèle OSI

Programme de la formation

Introduction
| Panorama et faits marquants (WannaCry, NotPetya, Facebook)
| Les composants de la sécurité (CID)
| Les types et référentiels du Pentest : BlackBox / GreyBox / White / RedBlue Team - PTES , OSSTM (OWASP)
| Le cycle de l'attaquant
| La trousse à outil et l'environnement : Kali (Site de Kali et système), étude de l'environnement, conservation des résultats (Utilisation de keepnote ou équivalent)

Intelligence Gathering
| Les principes de la recherche Internet/Passive (OSINT) : exemple de cas
| Recherche sur l'entreprise : physique, logique, organisation, électronique, recherche infrastructure, finance
| Recherche sur l'employé : social network, présence sur internet
| Reconnaissance externe : reconnaissance passive (Recherche DNS et BGP), reconnaissance Active (Scan des services, Scan des versions, Scan des OS, Recherche des services avancée, AXFR, SMTP, DNS_BF etc...)
| Reconnaissance interne : énumération du réseau courant (ARP/ICMP), le focus interne

Modélisation et analyse des vulnérabilités
| Etude et compréhension des CVEs : les types (Remote , Local , Web)
| Examen et revue des vulnérabilités manuels : NMAP ? CVE DETAILS
| Examen et revue des vulnérabilités automatiques : Nessus, Openvas, NSE
| Bilan et cartographie

Exploitation
| Les exploitations réseaux courantes : le man in the middle, fake DHCP
| Client exploitation : les attaques courantes sur l'humain (le navigateur, attaque sur les fichiers, USB)

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)
du 2 au 6 juin 2025
du 22 au 26 septembre 2025

PARIS
du 2 au 6 juin 2025
du 22 au 26 septembre 2025

AIX-EN-PROVENCE
du 22 au 26 septembre 2025
du 17 au 21 novembre 2025

BORDEAUX
du 2 au 6 juin 2025
du 22 au 26 septembre 2025

GRENOBLE
du 2 au 6 juin 2025
du 22 au 26 septembre 2025

LILLE
du 22 au 26 septembre 2025
du 17 au 21 novembre 2025

LYON
du 2 au 6 juin 2025
du 22 au 26 septembre 2025

NANTES
du 2 au 6 juin 2025
du 17 au 21 novembre 2025

VOIR TOUTES LES DATES

| Exploitation des services et OS : mauvaise configuration - tous systèmes (Default password, Anonymous ftp), Windows (Buffer Overflow à la main, exploitation connue à l'aide d'exploit-db), Linux (exploitation connue à l'aide d'exploit-db)

Post - Exploitation
| Élévation des privilèges : Windows (Linux)
| Persistence / Backdoor : mise en place de backdoor sous Windows et Linux, Cron, Scheduled Task
| Pivoting et rebond
| Exfiltration de données

Préparation et passage de l'examen de certification PECB Certified Lead Ethical Hacker
| Révision des concepts en vue de la certification
| Examen blanc

Méthode pédagogique

Cette formation est basée à la fois sur la théorie et sur les meilleures pratiques utilisées dans les investigations légales informatiques. Les exercices pratiques sont basés sur une étude de cas qui inclut des jeux de rôle et des présentations orales. Les tests pratiques sont similaires à l'examen de certification. À l'issue de la formation, un certificat de participation de 31 crédits DPC (Développement professionnel continu) est délivré. Le passage de l'examen est compris dans le prix de la formation.

Certification

Cette formation prépare au passage de la certification suivante.
N'hésitez pas à nous contacter pour toute information complémentaire.

PECB Certified Lead Ethical Hacker
L'examen « PECB Certified Lead Ethical Hacker » répond pleinement aux exigences du Programme d'examen et de certification (PEC) de PECB. L'examen couvre les domaines de compétence suivants :

| Domaine 1 : Outils et techniques de collecte d'informations
| Domaine 2 : Modélisation des menaces et identification des vulnérabilités
| Domaine 3 : Techniques d'exploitation
| Domaine 4 : Escalade des droits
| Domaine 5 : Pivotement et transferts de fichiers
| Domaine 6 : Rapports

L'examen PECB Certified Lead Ethical Hacker comprend deux parties :

| examen pratique : le candidat doit compromettre au moins deux machines cibles au moyen des tests d'intrusion.
| Rédaction du rapport : documenter dans un rapport écrit.

Examen à livre ouvertLes candidats sont autorisés à utiliser les documents de référence suivants :

| Copie papier de la norme principale
| Support de formation (accessible via l'application PECB Exams ou imprimé)
| Notes personnelles prises pendant la session de formation (accessibles via l'application PECB Exams ou imprimées)
| Dictionnaire au format papier

Pour des informations spécifiques sur le type d'examen, les langues disponibles et d'autres détails, veuillez consulter la liste des examens PECB et les Politiques et règlements relatifs à l'examen.

Méthode d'évaluation

Tout au long de la formation, les exercices et mises en situation permettent de valider et contrôler les acquis du stagiaire. En fin de formation, le stagiaire complète un QCM d'auto-évaluation.

Suivre cette formation à distance

Voici les prérequis techniques pour pouvoir suivre le cours à distance :

| Un ordinateur avec webcam, micro, haut-parleur et un navigateur (de préférence Chrome ou Firefox). Un casque n'est pas nécessaire suivant l'environnement.

| Une connexion Internet de type ADSL ou supérieure. Attention, une connexion Internet ne permettant pas, par exemple, de recevoir la télévision par Internet, ne sera pas suffisante, cela engendrera des déconnexions intempestives du stagiaire et dérangera toute la classe.
| Privilégier une connexion filaire plutôt que le Wifi.
| Avoir accès au poste depuis lequel vous suivrez le cours à distance au moins 2 jours avant la formation pour effectuer les tests de connexion préalables.
| Votre numéro de téléphone portable (pour l'envoi du mot de passe d'accès aux supports de cours et pour une messagerie instantanée autre que celle intégrée à la classe virtuelle).
| Selon la formation, une configuration spécifique de votre machine peut être attendue, merci de nous contacter.
| Pour les formations incluant le passage d'une certification la dernière journée, un voucher vous est fourni pour passer l'examen en ligne.
| Pour les formations logiciel (Adobe, Microsoft Office...), il est nécessaire d'avoir le logiciel installé sur votre machine, nous ne fournissons pas de licence ou de version test.
| Horaires identiques au présentiel.

Accessibilité

Les sessions de formation se déroulent sur des sites différents selon les villes ou les dates, merci de nous contacter pour vérifier l'accessibilité aux personnes à mobilité réduite.
Pour tout besoin spécifique (vue, audition...), veuillez nous contacter au 01 85 77 07 07.