CLEH, Certified Lead Ethical Hacker

S'initier à la conduite de piratage éthique - Certification incluse

Présentiel ou en classe à distance

5 jours (35 h)

Prix inter : 4.390,00 € HT
Forfait intra : 26.550,00 € HT

Réf.: SE202

Formation Officielle

Cette formation prépare à la certification PECB Lead Ethical Hacker et inclus le voucher pour passer l'examen.

A qui s'adresse cette formation ?

- Professionnels de la cybersécurité
- Spécialistes des TI

- Connaissance de base d'un système Linux et Windows
- Connaissance des réseaux et modèle OSI
- Disposez-vous des connaissances nécessaires pour suivre cette formation ? Testez-vous !

Programme

Pendant

1 - 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)

2 - Intelligence Gathering

- Les principes de la recherche Internet/Passive (OSINT) : exemple de cas
- Recherche sur l'organisation : 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

3 - 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

4 - 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)
- 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)

5 - 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

6 - Préparation et passage de l'examen de certification PECB Certified Lead Ethical Hacker

- Révision des concepts en vue de la certification
- Il est nécessaire de signer le code de déontologie du PECB afin d'obtenir la certification
- En cas d'échec les candidats bénéficient d'une seconde chance pour passer l'examen dans les 12 mois suivant la première tentative
- L'examen couvre les domaines de compétence suivants : Domaine 1 : Principes et concepts fondamentaux du piratage éthique - Domaine 2 : Mécanismes d'attaque - Domaine 3 : Principes et référentiels sur les tests d'intrusion - Domaine 4 : Planifier et effectuer des tests de pénétration en utilisant divers outils et techniques - Domaine 5 : Rédaction de rapports de tests d'intrusion
- L'examen comprend deux parties. La première partie est un examen sur papier, qui consiste en des questions de type dissertation. La deuxième partie est plutôt technique, dans laquelle le candidat devra effectuer des exercices de test d'intrusion sur ordinateur et rédiger un rapport d'analyse
- Les participants sont autorisés à utiliser leurs notes personnelles lors de l'examen sur papier et lors de la partie pratique de l'examen



Les objectifs de la formation

- Comprendre 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
- Comprendre l'exploitation et la post-exploitation des différents environnements
- Préparer et passer l'examen de certification "CLEH, Certified Lead Ethical Hacker" du PECB



Evaluation

Pendant la formation, le formateur évalue la progression pédagogique des participants via des QCM, des mises en situation et des travaux pratiques. Les participants passent un test de positionnement avant et après la formation pour valider leurs compétences acquises.
Il est fortement recommandé d'être en possession de la norme pour le passage de l'examen.



Les points forts de la formation

- 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.
- 95% des participants à cette formation se sont déclarés satisfaits ou très satisfaits au cours des 12 derniers mois.

Evaluation

Pendant la formation, le formateur évalue la progression pédagogique des participants via des QCM, des mises en situation et des travaux pratiques. Les participants passent un test de positionnement avant et après la formation pour valider leurs compétences acquises.
Il est fortement recommandé d'être en possession de la norme pour le passage de l'examen.

Dates et villes 2027 - Référence SE202

Dernières places disponibles Session garantie

A distance

du 5 avr. au 9 avr.	du 27 sept. au 1 oct.
du 21 juin au 25 juin	du 13 déc. au 17 déc.

Paris

du 5 avr. au 9 avr.	du 27 sept. au 1 oct.
du 21 juin au 25 juin	du 13 déc. au 17 déc.