EC-Council

C|EH v13

CEH v13 Ai

Soyez à jour en suivant le programme de formation le plus complet en **cybersécurité**

EC-Council Accredited Training Center

Oo2 Formations & Consulting

Certification CEH : **Certified Ethical Hacking**

Certaines compétences et certifications sont indispensables pour exercer dans le domaine de la sécurité informatique. La certification CEH (Certified Ethical Hacker) est l'une d'elles. Elle a été créée en 2003 par l'organisme EC-Council et constitue un atout très recherché dans le secteur informatique. En raison de l'évolution perpétuelle des cybermenaces, la certification CEH ne cesse d'être mise à jour. La dernière version de cette qualification unique est le CEH v13. Nous vous proposons quelques nouveautés de ce dernier et ses avantages.

EC-Council

C|EH v13

Qu'est-ce que le **CEH v13 ?**

Le CEH v13, ou Certified Ethical Hacker version 13, est une certification de renommée mondiale délivrée par l'EC-Council. Elle atteste des compétences d'un individu dans le domaine du hacking éthique. En d'autres termes, les titulaires de cette certification sont capables d'identifier et d'exploiter les vulnérabilités des systèmes d'information afin de mieux les sécuriser.

Certification CEH v13 :
Quelles sont les nouveautés ?

L'IA révolutionne la détection des menaces en permettant une analyse plus rapide et plus précise des données, tout en automatisant les tâches répétitives pour une meilleure efficacité.

Expérience pratique
Les laboratoires pratiques offrent un environnement réaliste pour mettre en œuvre les compétences acquises et maîtriser les outils les plus récents utilisés par les hackers éthiques.

40% d'efficacité en plus
Grâce à l'IA, les professionnels peuvent améliorer significativement leur efficacité en détectant les menaces plus rapidement et en prenant des décisions plus éclairées.

Un programme d'études complet et actualisé
Le programme couvre les dernières techniques d'attaque et les tendances émergentes, garantissant une formation toujours à jour et adaptée aux réalités du terrain.

Gains de productivité multipliés par 2
L'automatisation des tâches et l'amélioration de la précision permettent de doubler la productivité et de se concentrer sur des activités à plus forte valeur ajoutée.

Compétences concrètes, maîtrise avérée
La certification atteste de compétences pratiques solides et ouvre de nombreuses portes sur le marché du travail, notamment grâce à sa reconnaissance internationale.

Les 5 phases du piratage Ethique

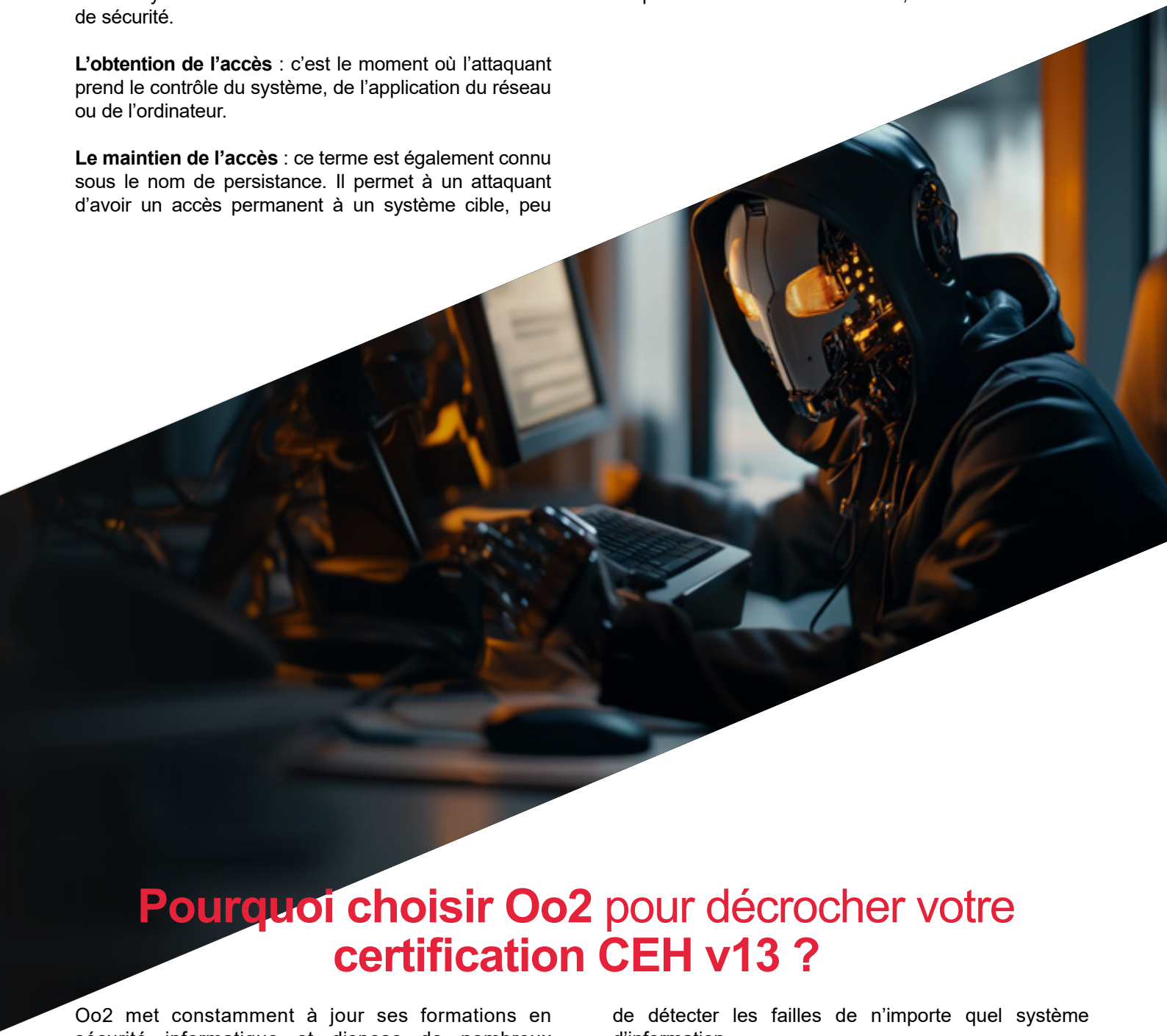
La reconnaissance : c'est la 1re phase au cours de laquelle un attaquant tente de collecter des données sur une cible avant de passer à l'attaque.

Le scanning : il consiste à utiliser divers utilitaires pour recueillir des informations via des sites Web, des réseaux ou des systèmes de fichiers afin de détecter des failles de sécurité.

L'obtention de l'accès : c'est le moment où l'attaquant prend le contrôle du système, de l'application du réseau ou de l'ordinateur.

Le maintien de l'accès : ce terme est également connu sous le nom de persistance. Il permet à un attaquant d'avoir un accès permanent à un système cible, peu importe si l'ordinateur est réinitialisé ou si l'utilisateur s'est déconnecté.

La couverture des traces : cette dernière phase consiste à supprimer toutes les preuves, une fois l'accès à la cible obtenu. Cela passe par la suppression des programmes, scripts ou installés sur la machine, etc.



Pourquoi choisir Oo2 pour décrocher votre **certification CEH v13 ?**

Oo2 met constamment à jour ses formations en sécurité informatique et dispose de nombreux partenariats avec les plus importants organismes de certifications tels que l'EC-Council. Dans cette optique, nous proposons un programme de certification qui a récemment été mis à jour pour le CEH v13.

Dans sa version la plus récente, les cours CEH v13 vous offrent les outils et techniques modernes que les hackers et les experts en sécurité informatique ont développés.
Grâce à notre offre, vous aurez toutes les clés en main pour devenir un hacker éthique expérimenté, capable de détecter les failles de n'importe quel système d'information.

Notre formation CEH v13 couvre les 5 phases du hacking éthique : reconnaissance, pénétration, énumération, maintien de l'accès et suppression des traces. C'est l'une des formations les plus avancées pour tous ceux qui veulent apprendre les techniques et les outils du hacking éthique. De plus, elle offre des supports de cours officiels et toutes les ressources d'apprentissage telles que les labs et les outils techniques.

Formation avec certification **CEH v13**

Code : SEC04FR | Durée : 5 Jours

Apprenez à utiliser les derniers outils et techniques de hacking modernes, y compris ceux alimentés par l'intelligence artificielle

Le CEH v13, dernière version de la certification la plus demandée par les employeurs, vous offre une formation complète et pratique. Cette formation CEH v13, vous permet de développer de solides compétences et de toute l'expérience pratique nécessaires du piratage éthique. Elle vous apprend également à utiliser les derniers outils, techniques et méthodes de hacking modernes dont se servent les hackers et les spécialistes de la sécurité de l'information pour attaquer une organisation en toute légalité.

Objectifs :

- Comprendre les fondamentaux de la sécurité informatique, les protocoles réseau, les systèmes d'exploitation, les bases de données, etc. ;
- Maîtriser les outils et les techniques de piratage éthique classique et pilotée par l'IA ;
- Mener des audits de sécurité en évaluant la sécurité des systèmes d'information et identifier les failles ;
- Réagir rapidement et efficacement en cas de compromission des systèmes ;
- Développer une pensée analytique pour identifier les risques potentiels et proposer des solutions adaptées ;
- Préparer et réussir l'examen de certification CEH® v13.

Prérequis

Avoir 2 ans d'expérience minimum dans le domaine de la sécurité informatique.

Public

- Administrateur système
- Ingénieur système
- Analyste cybersécurité
- Technicien Support/HelpDesk
- Auditeur interne/externe

Programme :

Module 01 : introduction au piratage éthique
Module 02 : le foot Printing (reconnaissance)
Module 03 : l'analyse des réseaux
Module 04 : la phase d'énumération
Module 05 : l'analyse de vulnérabilité
Module 06 : le piratage du système
Module 07 : les menaces de logiciels malveillants
Module 08 : les attaques par sniffing
Module 09 : l'ingénierie sociale
Module 10 : les attaques par déni de service (DDoS)
Module 11 : le détournement de session
Module 12 : le contournement des IDS, des pare-feu et des honeypot
Module 13 : le piratage de serveurs Web
Module 14 : le piratage d'applications Web
Module 15 : les injections SQL
Module 16 : le piratage des réseaux sans fil
Module 17 : le piratage des appareils mobiles
Module 18 : le piratage IoT et OT
Module 19 : le cloud computing
Module 20 : la cryptographie

Examen de certification

- Durée : 4 heures
- 125 questions à choix multiples
- Langue : anglais
- Réussite entre 60 et 80% de bonnes réponses

Bon à savoir

La certification CEH v13 est soumise à un processus de renouvellement et de maintien. Les exigences sont publiées sur la politique de formation continue de l'EC-Council (ECE).

EC-Council

C|EH v13

Oo2 Sénégal
Point - E, Immeuble 713 2ème étage
4313 Allées Seydou Nourou Tall
BP 45617 Dakar - Sénégal
+221 33 825 45 54 / +221 33 825 72 34

Oo2 Bénin
1227, Av. du Gouverneur Van Vollen Hoven
Quartier Zongo 01
BP 1112 Cotonou - Bénin
+229 69 25 89 89

Oo2 Côte d'Ivoire
Bd VGE–immeuble Le Massaï – Marcory
BP 1163 Abidjan 27 - Côte d'Ivoire
+225 27 225 03 445 / +225 27 21 59 28 70

Oo2 Burkina Faso
Avenue du Dr Kwamé N'Krumah
Ouagadougou 513 - Burkina Faso
+226 55 77 87 11

Oo2 France
128, rue de la Boétie
75008 Paris - France
Tél : +33 (0)188 24 70 33/34

EC-Council Accredited Training Center