

Certified Ethical Hacker v12 («CEHB»)

Pour contrer un hacker, il faut penser comme un hacker. En tant que partenaire EC-Council certifié, nous formons les collaborateurs aux outils et techniques adoptées par des cybercriminels afin de protéger au mieux les entreprises contre les attaques.

Durée: 5 jours

Prix : 6'200.- excl. 8.1% TVA

Documents : Support officiel EC-Council

Code officiel: CEH

Contenu

Vous pouvez faire évaluer vos failles de sécurité par des experts externes. Ou assurer vous-même la protection et la sécurité de votre système. Grâce à cette formation intensive et complète de 5 jours et demi, apprenez à vous défendre contre la cybercriminalité et préparez-vous à l'examen permettant de décrocher la certification internationalement reconnue « Certified Ethical Hacker ».

Plongez-vous dans un environnement réaliste d'hacking et apprenez à protéger votre entreprise des chevaux de Troie, virus ou vers, SQL Injections ainsi que des attaques MAC, DHCP et DDoS. Vous serez alors en mesure d'analyser les menaces pesant sur des systèmes informatiques, à les pirater et à les sécuriser. Afin de s'assurer que les connaissances ne seront pas utilisées à mauvais escient, les participantes et participants devront signer un accord avant chaque cours. En effet, en tant que CEH Certified Ethical Hacker, vous serez amené à utiliser les mêmes outils et méthodes que des pirates informatiques, non pas pour faire effectuer des attaques, mais pour vous défendre contre ces attaques.

Aperçu :

- Introduction to Ethical Hacking
- Footprinting and Reconnaissance
- Scanning Networks
- Enumeration
- Vulnerability Analysis
- System Hacking
- Malware Threats
- Sniffing
- Social Engineering
- Denial-of-Service
- Session Hijacking
- Evading IDS, Firewalls, and Honeypots
- Hacking Web Servers
- Hacking Web Applications
- SQL Injection
- Hacking Wireless Networks
- Hacking Mobile Platforms
- IoT and OT Hacking
- Cloud Computing
- Cryptography

- Connaître les possibilités, les outils et les astuces d'un hacker
- Se protéger de façon ciblée contre des attaques
- Mettre immédiatement en pratique les connaissances acquises d'identification et de résolution de failles de sécurité grâce à des exercices pratiques et scénarios réalistes
- Expérience pratique avec la Cyber Kill Chain
- Apprendre comment analyser un système cible pour trouver les points faibles, les mauvaises configurations ou configurations lacunaires
- Trouver le maillon le plus faible d'une organisation grâce à des concepts tels que le social engineering

Méthodologie & Didactique

Lors du cours vous recevrez un accès durant six mois à plus de 75 exercices d'Ethical Hacking avec les iLabs d'EC-Council.

Public cible

Cette formation s'adresse aux personnes certifiées MCSE ou CCNA désirant acquérir une certification dans le domaine de la sécurité. Aux Personnes désirant passer une certification internationale liée au Legal Hacking. Aux consultants en sécurité désirant se certifier à un niveau international. À toutes les personnes qui désirent devenir spécialistes en sécurité.

Les personnes certifiées CEH occupent les postes suivants :

Mid-Level Information Security Auditor, Cybersecurity Auditor, Security Administrator, IT Security Administrator, Cyber Defense Analyst, Vulnerability Assessment Analyst, Warning Analyst, Information Security Analyst 1, Security Analyst L1, Infosec Security Administrator, Cybersecurity Analyst level 1, level 2, & level 3, Network Security Engineer, SOC Security Analyst, Security Analyst, Network Engineer, Senior Security Consultant, Information Security Manager, Senior SOC Analyst, Solution Architect and Cybersecurity Consultant

Certification

Examen

L'examen de 4 heures pour devenir « Certified Ethical Hacker » (CEH) fait partie de cette formation et doit être passé dans les 4 semaines suivant la fin de votre formation. L'examen a lieu en ligne dans l'endroit et à l'heure que vous désirez. EC Council encadre l'examen par un système de surveillance en ligne. L'examen, dont le prix s'élève à € 500, est compris dans le coût de la formation. Seuil de réussite : 70%.

Préparation à l'examen

- Veuillez lire attentivement les instructions d'examen d'EC Council qui vous seront transmises le premier jour de cours par votre formateur. Si vous avez des questions concernant les modalités d'examen, veuillez nous contacter à l'adresse romandie@digicomp.ch.
- Vous devez avoir le matériel nécessaire (PC/Laptop). Voir les instructions d'examen d'EC Council
- Exigences minimales : Wifi de bonne qualité, PC/Laptop puissant, webcam, microphone
- Vous devrez présenter votre carte d'identité ou votre passeport lors de l'examen
- Aides autorisées : Dictionnaire français-anglais

Format de l'examen :

- Langue : anglais
- Durée : 4 heures

- Questions : 125 questions à choix multiple
- Domaines testés : menaces sécuritaires et vecteurs d'attaque, détection d'attaque, prévention contre les attaques, procédures, méthodologies, ...

Reporter ou repasser l'examen

- Dans le cas où vous seriez obligé de reporter votre examen, veuillez nous le communiquer à l'adresse romandie@digicomp.ch ou au [+41 22 738 80 80](tel:+41227388080).
- Si vous repassez l'examen, vous devez vous acquitter de 50% du prix de l'examen. Vous recevrez un bon d'examen de la part de Digicomp.

Avez-vous une question ou souhaitez-vous organiser un cours en entreprise ?

Nous vous conseillons volontiers au [+41 22 738 80 80](tel:+41227388080) ou romandie@digicomp.ch. Retrouvez toutes les informations détaillées concernant les dates sur www.digicomp.ch/formations-securite/cybersecurite-offensive/cours-certified-ethical-hacker-v12-ceh