Alcodefi Conseil & Formation Etablissement de formation professionnelle Agréé par l'Etat	**CEH v10** **Certified Ethical Hacker**	**Formation & Examen de Certification** **Inscription:** formation@alcodefi.com Tel- Fax: 023.85.49.04 Tel: 0552.62.68.13 0553.00.33.47

Introduction

La formation CEHv10 est la plus avancée au monde en matière de piratage éthique. Elle couvre 20 des plus grands domaines que chaque pirate éthique voudra connaître pour monter en compétences dans le domaine de la sécurité de l'information. A travers ces 20 modules, la formation couvre plus de 270 attaques techniques qui sont les plus utilisées par les pirates.

Plus de 140 labs reprenant des scénarios réels évoqués pendant la formation ont été créés pour vous aider à percevoir une attaque comme si elle était réelle. Vous aurez également accès à plus de 2200 outils de piratages bien connus et à plus de 2200 slides, spécialement conçues pour vous aider à bien maîtriser les concepts complexes de la sécurité. Cette formation de 5 jours sera dispensée par un CEI – Certified EC-Council Instructor

Objectifs de la formation :

Cette formation vous aidera à maitriser une méthodologie de piratage éthique qui pourra aussi bien être utilisée dans un test d'intrusion que dans une situation de piratage éthique. Vous quitterez le cours avec des compétences en piratage éthique qui sont hautement recherchées, tout comme, globalement, la certification Certified Ethical Hacker!

Cette formation vous préparera à l'examen de certification Certified Ethical Hacker 312-50.

Objectifs de pédagogiques de la formation :

Cette formation traite des aspects purement techniques pour permettre aux participants de toucher aux aspects pratiques de la sécurité des infrastructures et de voir les risques réels encourus par la présence d'éventuelles failles dans les systèmes et applications.
Cette formation va vous permettre de :

- Comprendre les méthodes et modes opératoires employés par les pirates lors d'une attaque informatique
- Identifier et utiliser les outils permettant de tester les protections d'un système d'information d'entreprise
- Evaluer et analyser les points de faiblesses et vulnérabilités latentes d'un système informatique
- Défendre plus efficacement une infrastructure d'entreprise ou d'un composant informatique

La formation sera répartie comme suit :
- 30% du temps sera alloué aux aspects théoriques
- 70% du temps sera alloué à des exercices pratiques et à des études de cas

Méthodologie :

- Cette formation va permettre aux participants de maitriser une méthodologie de piratage éthique qui pourra aussi bien être utilisée dans un test d'intrusion que dans une situation de piratage éthique.
- Les participants seront amenés d'abord à comprendre comment fonctionne la défense périmétrique avant de scanner et d'attaquer leurs propres réseaux. Ils apprendront ensuite comment les intrus acquièrent des privilèges et quelles actions peuvent être mises en œuvre pour sécuriser un système.
- Les participants vont utiliser pour cela des outils et des installations techniques.
- Les participants quitteront le cours avec des compétences en piratage éthique qui sont hautement recherchées, tout comme, globalement, la certification Certified Ethical Hacker! Cette formation vous préparera à l'examen de certification CertifiedEthicalHackerv10.

Alcodefi Conseil & Formation Etablissement de formation professionnelle Agréé par l'Etat	**CEH v10** **Certified Ethical Hacker**	**Formation** **& Examen de Certification** **Inscription:** formation@alcodefi.com Tel- Fax: 023.85.49.04 Tel: 0552.62.68.13 0553.00.33.47

Public concerné : La formation et l'examen CEH v10 s'adressent aux:

- Responsable sécurité
- Auditeur
- Professionnel de la sécurité
- Administrateur de site
- Toute personne concernée par la gestion de la sécurité des systèmes d'information

Durée de la formation : 05 jours

Biographie de l'expert formateur

Certifié CEH v9, ISO27001 LA et ISO 27005 RM, est Expert Auditeur certifiée d l'Agence Nationale de la Sécurité Informatique(ANSI). Disposant de plus de 10 ans d'expérience professionnelle, il intervient principalement sur les missions d'audit technique, de sécurité des systèmes d'information et des tests intrusifs. Il est Certifié EC COUNCIL et PECB trainer.

Domaines de compétence :

- Audit et conseil dans le domaine de la sécurité informatique
- Audit intrusif des plateformes d'hébergement
- Audit des applications WEB et mobiles
- Accompagnement des entreprises pour la mise en place de procédures/politique de sécurité
- Formateur dans le domaine de la sécurité informatique
- Formation dans le domaine des audites technique des systémes d'information

Alcodefi
Conseil & Formation
Etablissement de formation professionnelle
Agréé par l'Etat

CEH v10

Certified Ethical Hacker

Formation
& Examen de Certification

Inscription:

formation@alcodefi.com
Tel- Fax: 023.85.49.04
Tel: 0552.62.68.13
0553.00.33.47

Contenu et programme de la formation

Jours	Contenus/ Concepts clés à aborder	Méthodes, Moyens Pédagogiques et Equipements	Durée (Heures)	
			Théori	Pratiqu
J1	Module 1: Introduction au Ethical Hacking Profil d'un Ethical Hacker, motivations d'un pirate, etc. Module 2: Footprinting et Reconnaissance Analyse périmétrique, collecte d'éléments techniques, etc. Module 3: Scanning de réseaux Analyse de réseaux et d'infrastructures, systèmes, etc. Module 4: Enumération Collecte d'éléments SNMP, NTP, Netbios, DNS, etc.	• Un bloc note & Un stylo • Un support Pédagogique (support de cours) • Un Tableau Blanc	3	5
J2	Module 5: Analyse des vulnérabilités Module 6: Hacking de système - Cassage de mots de passe, attaque des hash, etc. Module 7: Analyse de Malwares Chevaux de Troie, Backdoors, Virus, Vers, etc. Module 8: Sniffing réseau Analyse de trames réseau, injection de données, etc	• Des exercices et des labs • Un PC pour chaque candidat • Un PC pour le	3	5
J3	Module 9: Ingénierie sociale Attaques non techniques SE, attaques numériques, etc. Module 10: Attaques par Déni de Service Attaques de type DOS, DDOS, par réflexion, etc. Module 11: Hijacking de sessions Détournement d'identifiants de sessions, etc. Module 12: Evasions d'IDS, Firewalls & Honey Pots, Comment échapper aux IDS/IPS		3	5
J4	Module 13 : Hacking de serveurs Web Modes d'attaque de serveurs web et astuces, etc. Module 14: Hacking d'applications Web Vecteurs d'attaque d'applications Web, LDAP, etc. Module 15: Injection SQL Modes d'attaque SQL, injection SQL en aveugle, etc. Module 16: Hacking de réseaux sans fil Infrastructures WiFi WEP/WPA/WPA2, attaques WiFi, etc.		3	5
J5	Module 17: Hacking plateformes Mobiles Android, Windows 8, iOS, rooter les smartphones, etc Module 18 : IoT Module 19: Cloud Computing Sécurité dans le Cloud, Risque, Vulnérabilités, etc. Module 20: Cryptographie Evolution des chiffrements AES/DES/3DES, RSA, PKI, etc.		3	5
Total			15	25