

## Accredited Training Center

Cert.ID  
**EATC69584**

### Business and Information Technology - BIT

EC-Council recognizes this organization as an Accredited Training Center meeting strict standards of excellence for delivering instructor-led training. The EC-Council ATC network is the premier channel for delivering high-quality EC-Council information security related training to businesses and industry professionals.

Issue Date: **September 02, 2016**Expiry Date: **September 30, 2021**

# *RÉUSSIR VOTRE CERTIFICATION*

**Préparation à l'Examen en Cinq jours**

**Du 1 au 5 Mars 2021**

**CENTRE DE FORMATION A TUNIS**

## Introduction

La certification CEH dans sa version v11 est actuellement la plus avancée au monde dans le domaine de l'Ethical Hacking. Ce cours officiel CEH Ethical Hacker v11 EC-Council aborde 20 modules successifs liés aux domaines de la sécurité informatique les plus récents, en détaillant les dernières techniques de hacking.

## Objectifs de la Formation

La formation permet à tous les informaticiens et tous les passionnés d'informatique ayant un profil technique de découvrir et de mieux comprendre les modes opératoires, les méthodes employées ainsi que les différents outils utilisés par les pirates informatiques pour contourner et déjouer les protections de sécurité en place.

Après la formation, le stagiaire aura acquis des connaissances et une expérience réelle en Ethical Hacking

## Méthodologie :

Cette formation va permettre aux participants de maîtriser une méthodologie de piratage éthique qui pourra aussi bien être utilisée dans un test d'intrusion que dans une situation de piratage éthique et de leur transmettre une vision étendue des variétés d'attaques possibles dans un SI

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. Le **Cours de formation CEH allie** théorie et pratique : Le modèle d'apprentissage conçu tout au long du cursus CEH v11 permet d'associer la pratique à la théorie: plus de 30 % du cursus de formation est composé de mises en situation, de réalisation d'exercices pratiques et l'utilisation de 'labs' favorisant la connaissance des différents outils en sécurité permettant la résolution de cas pratiques tant en situation réelle qu'en environnement virtualisé. L'infrastructure technique mise à disposition de chaque participant/stagiaire est composée de plusieurs plateformes virtualisées accessibles et utilisables depuis chaque poste. Les interactions imposées par les exercices pratiques permettent de gagner en compréhension d'utilisation, et de maîtriser au mieux les principaux systèmes de sécurité actuels

Ce cursus va vous permettre d'obtenir l'examen de certification final CEH [Certified Ethical Hacker](#). De nouveaux modules apparaissent dans cette version v11, avec des thématiques telles l'Analyse de Vulnérabilités ou le sujet des IoT (Internet of Things).

## Contenu de la formation

La formation se compose de 20 modules complémentaires et indépendants comme suit :

- 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.
- 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
- 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
- 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.
- 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.

## Formateur

**Anis FOURATI**, Tunisien de nationalité, certifié CEH v11, ISO 27001 LA et ISO 27005 RM, est Expert Auditeur certifiée de l'Agence Nationale de la Sécurité Informatique (ANSI). Disposant de plus de 15 ans d'expérience professionnelle, il intervient principalement sur les missions d'audit technique, de sécurité des systèmes d'information et des tests intrusifs. Anis FOURATI est Certifié EC COUNCIL et PECB trainer.

## Pré-requis

Connaissances professionnelles de TCP/IP, Linux et Windows Server

## Public visé

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

- Responsables sécurité
- Auditeurs de la sécurité
- Professionnels de la sécurité

- Administrateurs de site
- Toute personne concernée par la stabilité des systèmes d'information

## Informations Générales sur l'examen

- Titre de l'examen : Certified Ethical Hacker v11
- Code de l'examen : 312-50
- Format de l'examen : QCM
- Type de l'examen : CBT – En ligne
- Nombre de questions: 125
- Score requis: de 70% à 78% (QCM) selon la complexité des questions
- Langue: anglais
- Durée : 4 heures
- Lieu de l'examen: les locaux de BIT ou du centre de formation

## Ressources

- Support de cours officiel en anglais
- Cours donné en français
- 20% d'exercices pratiques
- 1 PC par personne / Internet
- des Q/R pour s'entraîner