

IT Security

★ Certifiant

Ethical Hacker - CEH v10

Formation intensive au piratage éthique préparant à la certification CEH v10, pour apprendre à penser et agir comme un attaquant afin de mieux défendre les systèmes d'information.

DURÉE 35 heures	NIVEAU Avancé	FORMAT Présentiel & en ligne
LANGUE Français	CERTIFICAT Certificat Experteam	FORMATEUR Amel Bouzid

Présentation

Proposée par Expert Team Tunisie, centre de formation IT agréé par l'État, cette formation en sécurité informatique offensive plonge les participants au cœur des techniques de piratage éthique (Ethical Hacking). Elle couvre l'ensemble des méthodes et outils employés par les pirates lors d'une attaque réelle, dans un cadre légal et contrôlé, afin de mieux évaluer et renforcer la sécurité des infrastructures.

Structurée autour du référentiel officiel CEH v10 de l'EC-Council et de ses 20 domaines, la formation alterne fondamentaux théoriques et travaux pratiques : reconnaissance, scanning, exploitation de vulnérabilités, attaques web et applicatives, réseaux sans fil, plateformes mobiles, IoT, cloud et cryptographie. Chaque phase du cycle d'attaque est étudiée du point de vue de l'attaquant comme de celui du défenseur.

À l'issue du parcours, les participants disposent des compétences nécessaires pour conduire des tests d'intrusion, identifier les failles latentes d'un système et durcir la posture de sécurité d'une organisation. La formation prépare directement à l'examen de certification Certified Ethical Hacker (CEH) v10, reconnu internationalement et très recherché par les entreprises et les cabinets de cybersécurité.

Objectifs pédagogiques

- ✓ 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
- ✓ Évaluer et analyser les points de faiblesse et les vulnérabilités latentes d'un système informatique
- ✓ Mener les différentes phases d'un test d'intrusion, de la reconnaissance à l'exploitation
- ✓ Défendre plus efficacement une infrastructure d'entreprise ou un composant informatique
- ✓ Maîtriser les techniques d'attaque web, réseau, sans fil, mobile, IoT et cloud
- ✓ Acquérir une expérience concrète en sécurité offensive et se préparer à l'examen de certification CEH v10

Programme détaillé

Introduction et reconnaissance

- Introduction à l'Ethical Hacking et cadre légal
- Footprinting et reconnaissance (OSINT)
- Scanning de réseaux
- Énumération des services et ressources

Analyse de vulnérabilités et hacking système

- Analyse des vulnérabilités
- Hacking de système (accès, élévation de privilèges, effacement de traces)
- Analyse de malwares (virus, chevaux de Troie, backdoors)

Attaques réseau et évacion

- Écoute et sniffing de réseaux
- Ingénierie sociale
- Attaques par déni de service (DoS/DDoS)
- Hijacking de sessions
- Évacion des IDS, firewalls et honeypots

Hacking des applications web

- Hacking de serveurs web
- Hacking d'applications web
- Injection SQL

Réseaux sans fil, mobile et objets connectés

- Hacking des réseaux sans fil (Wi-Fi)
- Hacking des plateformes mobiles
- Sécurité et attaques IoT

Cloud, cryptographie et certification

- Sécurité et attaques du Cloud Computing
- Cryptographie et attaques cryptographiques
- Synthèse et préparation à l'examen CEH v10

Prérequis

Maîtrise des systèmes d'exploitation Windows et Linux ; connaissances de base des protocoles et du fonctionnement des réseaux TCP/IP.

Public visé

Administrateurs systèmes et réseaux, ingénieurs et techniciens en sécurité informatique, consultants et auditeurs en cybersécurité, futurs pentesters et toute personne souhaitant s'orienter vers la sécurité offensive.

Prochaines sessions

DATE	VILLE	HORAIRE	FORMATEUR
03/08/2026	Tunis	09h00 - 16h00	Amel Bouzid
31/08/2026	Sfax	09h00 - 16h00	Amel Bouzid

1 450 TND / personne

Acompte de 30% possible à la réservation · Financement sur demande.

Experteam — El Ghazala, Ariana (face au Technopôle La Ghazela)

+216 29 674 204 · contact@expertunisie.com · experteam.itt.tn