# Formation Certified Ethical Hacker (CEH)

## Module 1 : Introduction à l'éthique du hacking

- Définitions clés et concepts
- Phases du hacking éthique
- Cadres juridiques et conformité

## Module 2 : Reconnaissance passive et active

- Gathering d'information
- OSINT et footprinting
- Utilisation de WHOIS, Google hacking, Maltego, etc.

## Module 3 : Scan et énumération

- Scanning de ports et de vulnérabilités
- Analyse avec Nmap, Netcat, etc.
- Énumération des services et utilisateurs

## Module 4 : Vulnérabilités et hacking système

- Exploitation des systèmes d'exploitation
- Escalade de privilèges
- Rootkits, backdoors et trojans

## Module 5 : Malware et stéganographie

- Types de malwares
- Techniques de dissimulation de données

## Module 6 : Sniffing et attaques réseau

- Analyse de paquets réseau (Wireshark, TCPDump)
- ARP poisoning, MITM
- Contre-mesures

## Module 7 : Hacking Web & Applications

- Failles XSS, CSRF, SQL Injection
- Traversal de répertoire, manipulation d'URL
- Tests avec Burp Suite, OWASP ZAP

## Module 8 : Sécurité mobile et IoT

- Attaques sur Android et iOS

- Sécurité des objets connectés

## Module 9 : Cloud computing & piratage de serveurs

- Vulnérabilités spécifiques au cloud
- Audit de sécurité dans AWS, Azure

## Module 10 : Cryptographie & attaques sur le chiffrement

- Concepts de base : symétrique, asymétrique
- Attaques par force brute, rainbow tables
- Certificats, SSL, TLS

## Module 11 : Ingénierie sociale & techniques de phishing

- Prétexting, baiting, spear phishing
- Techniques d’usurpation d’identité

## Module 12 : Contremesures, logs et couverture de traces

- Effacement des logs système
- Techniques d’obfuscation
- Contre-hacking et prévention

## Module 13 : Préparation à l’examen CEH

- Révisions des modules clés
- Simulations de QCM
- Exercices pratiques