ETHICAL HACKING

Public	Admin réseau système, RSSI.
Durée	3 jours - 21 heures
Pré-requis	Avoir de bonnes connaissances en administration système.
Objectifs	Comprendre les bases de la cybersécurité. Configurer un lab d'entraînement et maîtriser les outils essentiels. Apprendre à exploiter des vulnérabilités, utiliser des outils d'attaque et comprendre les mécanismes d'intrusion. Apprendre à se défendre, rédiger un rapport d'audit et comprendre le cadre légal.
Méthodes pédagogiques	Pour bien préparer la formation, le stagiaire remplit une évaluation de positionnement et fixe ses objectifs à travers un questionnaire. La formation est délivrée en présentiel ou distanciel (e-learning, classe virtuelle, présentiel et à distance). Le formateur alterne entre méthodes démonstratives, interrogatives et actives (via des travaux pratiques et/ou des mises en situation). La validation des acquis peut se faire via des études de cas, des quiz et/ou une certification. Cette formation est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou par Audit Conseil Formation.
Moyens techniques	1 poste de travail complet par personne De nombreux exercices d'application Mise en place d'ateliers pratiques Remise d'un support de cours Passage de certification(s) dans le cadre du CPF Remise d'une attestation de stage
Modalité d'évaluation des acquis	Evaluation des besoins et objectifs en pré et post formation Evaluation technique des connaissances en pré et post formation Evaluation générale du stage
Délai d'accès	L'inscription à cette formation est possible jusqu'à 5 jours ouvrés avant le début de la session
Accessibilité handicapés	Au centre d'affaires ELITE partenaire d'ACF à 20 m. Guide d'accessibilité à l'accueil.

JOUR 1 : FONDAMENTAUX & PRÉPARATION

- Matin : Introduction & Sécurité Réseau
- Après-midi : Scan & Reconnaissance

1. INTRODUCTION À L'ETHICAL HACKING

- Définition, légalité, méthodologie (OSSTMM, NIST, PTES), différences entre hacker "black hat" et "white hat".

2. SÉCURITÉ RÉSEAU DE BASE

- Modèle OSI/TCP-IP, protocoles (TCP/UDP/ICMP), adressage IP, sous-réseaux, ports.

3. LAB : CONFIGURATION D'UN ENVIRONNEMENT DE TEST

- Installation de Kali Linux (VM ou bare metal), outils de base (ifconfig, ping, traceroute, netstat).
- Introduction à VirtualBox/VMware pour créer un lab avec machines vulnérables (ex : Metasploitable, DVWA).

4. RECONNAISSANCE (OSINT & SCAN)

- Utilisation de Nmap (nmap -sS -sV -O -A), Zenmap, Shodan, Maltego.
- Techniques de footprinting (whois, DNS, réseaux sociaux).

5. LAB : SCAN DE RÉSEAUX

- Scanner un réseau local avec Nmap, identifier les services ouverts, versions logicielles, vulnérabilités potentielles.

6. VULNÉRABILITÉS WEB DE BASE

- Introduction aux failles OWASP Top 10 (SQLi, XSS, CSRF).
- Présentation de OWASP ZAP et Burp Suite Community.

JOUR 2 : ATTAQUES & EXPLOITATION

- Matin : Exploitation de Vulnérabilités
- Après-midi : Post-Exploitation & Réseaux

1. EXPLOITATION DE FAILLES WEB

- Attaques SQL Injection (manuelle et avec sqlmap), XSS (stored/reflected), CSRF.

2. LAB : ATTAQUES WEB

- Exploiter une machine vulnérable (ex : DVWA) avec SQLi, XSS, et CSRF.
- Utilisation de Metasploit pour automatiser les attaques.

3. POST-EXPLOITATION & PRIVILEGE ESCALATION

- Techniques pour maintenir l'accès (persistence), escalade de privilèges (Linux/Windows), dump de mots de passe (mimikatz, John the Ripper).

4. ATTAQUES RÉSEAU AVANCÉES

- MITM (Man-in-the-Middle) avec Ettercap, ARP Spoofing, DNS Spoofing, Wi-Fi Hacking (WPA2 avec aircrack-ng).

5. LAB : ATTAQUE MITM

- Intercepter le trafic entre deux machines avec Ettercap, voler des identifiants (ex : FTP, HTTP).

JOUR 3 : DÉFENSE, REPORTING & ÉTHIQUE

- Matin : Défense & Sécurité Offensive
- Après-midi : Reporting & Éthique

1. SÉCURITÉ DES SYSTÈMES

- Hardening Linux/Windows, pare-feu (iptables, ufw), détection d'intrusion (Snort, Wazuh).

2. DÉFENSE CONTRE LES ATTAQUES

- Protection contre les MITM, SQLi, XSS, brute-force (fail2ban, mots de passe forts).
- Introduction à SIEM (Splunk, ELK Stack).

3. RÉDACTION D'UN RAPPORT D'AUDIT

- Structure d'un rapport (ex : PTES), méthodologie, exemples de vulnérabilités trouvées, preuves (screenshots, logs).

4. CADRE LÉGAL & ÉTHIQUE

- Lois applicables (RGPD, loi Godfrain en France, Computer Fraud and Abuse Act aux USA), règles déontologiques, contrats de pentest.

NOUS CONTACTER

Siège social
16, ALLÉE FRANÇOIS VILLON
38130 ÉCHIROLLES

Téléphone
04 76 23 20 50 - 06 81 73 19 35

Suivez-nous sur les réseaux sociaux, rejoignez la communauté !

ACF Audit Conseil Formation

@ACF_Formation

Dernière mise à jour : 17/07/2026

PROFIL Formateur : Les formateurs sont recrutés selon plusieurs critères : Expérience, pédagogie, dynamisme et prévoyance.