HACKING ET PROTECTION

Public	Administrateurs de systèmes ainsi que les techniciens chargés du support mais également toute personne impliquée dans la sécurité du système d'information.
Durée	5 jours - 35 heures
Pré-requis	AUCUN
Objectifs	Acquérir un niveau d'expertise élevé dans le domaine de la sécurité en réalisant différents scénarios complexes d'attaques Déduire des solutions de sécurité avancées
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 démonstrative, interrogative et active (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.

1. LA SSI

- Les menaces d'aujourd'hui
- Paysage de la sécurité
- Les normes
- La sécurité dans les entreprises françaises
- Le cycle d'une attaque

2. LA RECONNAISSANCE PASSIVE

- Découverte et recherche d'informations sensibles
- Le social engineering
- Google Dorks
- Maltengo

3. LA RECONNAISSANCE ACTIVE

- Découverte des réseaux
- Découverte des ports
- Découverte des OS
- Découverte des vulnérabilités

4. LES ATTAQUES WEB

- Découvrir une vulnérabilité sur un serveur Web
- Le top 10 de l'OWASP
- Injection de commande et injections SQL
- Cross-site scripting et cross-site request forgery
- File inclusion et file upload

5. LES ATTAQUES RESEAU

- L'écoute passive
- Attaques « Man in the middle »
- Les protocoles vulnérables
- L'ARP poisoning
- Outillage : Ettercap et MITMF

6. POST EXPLOITATION

- Rechercher une vulnérabilité
- Exploiter une vulnérabilité
- Outils Metasploit

NOUS CONTACTER

Siège social
16, ALLÉE FRANÇOIS VILLON
38130 ÉCHIROLLES

Centre de formation
87, RUE GÉNÉRAL MANGIN
38000 GRENOBLE

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

E-mail
contact@audit-conseil-formation.com

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

ACF Audit Conseil Formation @ACF_Formation ACFauditconseilformation