ATTAQUE DÉFENSE WI-FI

Public	Professionnels de la sécurité informatique souhaitant améliorer leurs compétences en matière de sécurité Wi-Fi, administrateurs réseau ou toute personne souhaitant comprendre les risques liés aux réseaux Wi-Fi et les méthodes pour les protéger.
Durée	3 jours - 21 heures
Pré-requis	Avoir des connaissances de base des réseaux informatiques et des systèmes d'exploitation Windows ou Linux.
Objectifs	Décrire les types de réseaux Wi-Fi et les protocoles de sécurité courants Identifier les vulnérabilités courantes dans les réseaux Wi-Fi Mettre en pratique les méthodes d'attaque et de défense Wi-Fi Acquérir les compétences nécessaires pour configurer la sécurité sur un réseau Wi-Fi et détecter les intrusions.
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
Planning	Du 16/07/2024 au 18/07/2024 Du 12/11/2024 au 14/11/2024
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. INTRODUCTION À LA SÉCURITÉ WI-FI

- Types de réseaux Wi-Fi (Infrastructure, Ad-hoc)
- Protocoles de sécurité courants (WEP, WPA, WPA2)
- Vulnérabilités courantes (Faiblesses de la clé, Attaques de désauthentification)
- Outils de reconnaissance de réseau

2. ATTAQUES WI-FI

- Méthodes d'attaques Wi-Fi
- Cracking de mot de passe
- Injection de paquets
- Attaques de désauthentification
- PMKID (Pairwise Master Key Identifier)
- Outils d'attaques courants
- Aircrack-ng
- Aireplay-ng
- Airgedon

3. DÉFENSE WI-FI

- Meilleures pratiques pour protéger les réseaux Wi-Fi
- Configuration de la sécurité
- Surveillance
- Détection d'intrusion
- Outils de sécurité courants (Wireshark, WaIDpS, Chellam)

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