TESTS D'INTRUSION, ORGANISER SON AUDIT

Public	Responsables, architectes sécurité. Techniciens et administrateurs systèmes et réseaux. Auditeurs amenés à faire du Pentest.
Durée	4 jours - 28 heures
Pré-requis	Bonnes connaissances de la sécurité informatique (matériel, architectures réseau, architectures applicatives). Expérience requise.
Objectifs	Acquérir une méthodologie pour organiser un audit de sécurité de type test de pénétration sur son SI Rédiger un rapport final suite à un test d'intrusion Formuler des recommandations de sécurité
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 08/09/2025 au 11/09/2025 Du 08/12/2025 au 11/12/2025
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.

LES MENACES

- Evolution de la sécurité des SI.
- Etat des lieux de la sécurité informatique.
- L'état d'esprit et la culture du hacker.
- Quels risques et quelles menaces ?

MÉTHODOLOGIE DE L'AUDIT

- Le contexte règlementaire.
- L'intérêt d'effectuer un test d'intrusion, un Pentest, les différents types de Pentest.
- Comment intégrer le test d'intrusion dans un processus de sécurité général.
- Apprendre à définir une politique de management de la sécurité et d'un Pentest itératif.
- Organiser et planifier l'intervention. Comment préparer le référentiel ?
- La portée technique de l'audit. Réaliser le Pentest.

LES OUTILS DE PENTEST

- Quels outils utiliser ? Sont-ils vraiment indispensables ?
- La prise d'information. L'acquisition des accès.
- L'élévation de privilèges. Le maintien des accès sur le système.
- Les outils de Scan et de réseau.
- Les outils d'analyse système et d'analyse Web.
- Les outils d'attaque des collaborateurs.
- Quel outil pour le maintien des accès ?
- Les frameworks d'exploitation.

RÉDACTION DU RAPPORT

- Collecter les informations.
- Préparation du document et écriture du rapport.
- L'analyse globale de la sécurité du système.
- Décrire les vulnérabilités trouvées.
- Formuler les recommandations de sécurité.

MISES EN SITUATION

- Interception de flux HTTP ou HTTPS mal sécurisés.
- Test d'intrusion sur une adresse IP.
- Test d'intrusion d'applications client-serveur : FTP , DNS , SMTP.
- Tests d'intrusion d'applications Web (SQL Injection, XSS , vulnérabilité d'un module PHP et d'un CMS).
- Tests d'intrusion interne : compromission via une clé USB piégée et via un PDF malicieux.

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 : 27/02/2024