



LA METHODOLOGIE D'AUDIT DE TESTS D'INTRUSION - PENTEST

Objectifs pédagogiques

Disposer d'une méthodologie complète d'audit de sécurité et de la connaissance des outils associés pour réaliser un rapport d'audit exhaustif.

Public	DSI, Maîtrise d'ouvrage, Directeur de projet, chef de projet et toute personne impliquée dans le domaine de la cybersécurité.
Prérequis	Bonne connaissance de la cybersécurité.
Compétences visées à l'issue de la formation	<ul style="list-style-type: none">■ Connaître la méthodologie d'audit■ Maîtriser la rédaction d'un rapport d'audit
Déroulement de la formation	Cours théorique en présentiel.
Modalités pédagogiques	<p>Centrées sur l'acquisition de compétences opérationnelles et dans un objectif d'emploi, les modalités pédagogiques s'appuient sur un dispositif de cours en présentiel.</p> <p>Pendant toute leur formation, les apprenants ont accès à des cours en centre et à une plateforme pédagogique en ligne leur permettant d'accéder à des ressources complémentaires.</p> <p>Les modalités pédagogiques précises de chaque formation sont communiquées aux futurs apprenants au cours de leur entretien de recrutement avec le responsable de formation.</p>
Durée	5 jours (21 heures)
Horaires	9h00 - 17h00 Pausas : 11h / 15h Déjeuner : 12h30 - 13h30
Dates et lieu	Dates : voir le planning de formation Cyber Sécurité Lieu : Toulouse
Délai d'accès	<p>Le délai d'accès à une formation monétique GLS2i Software est compris entre 2 et 3 semaines, selon le calendrier de la formation et le dispositif de financement mobilisé.</p> <p>Anticipez dès maintenant votre projet de formation.</p>
Tarifs	<p>En inter : 2000 € HT (déjeuners inclus)</p> <p>En intra : demandez un devis</p>
Méthodes et matériels mobilisés	Un ordinateur portable sera exigé.



O.F. Déclaration d'activité N° 76311168831
la préfecture de la région Occitanie
Mise à jour le 03/03/2024

LA METHODOLOGIE D'AUDIT DE TESTS D'INTRUSION - PENTEST

Méthodes d'évaluation	Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mise en situation, travaux pratiques...
Accessibilité	La formation est accessible aux personnes à mobilité réduite.
Formateurs	Les formateurs disposent de compétences pédagogiques, fonctionnelles et techniques dans le domaine de la nouvelle technologie et la cybersécurité .
Support	le support de cours « Analyse après incident» au format PDF sera remis à chaque participant en début de la formation.



LA METHODOLOGIE D'AUDIT DE TESTS D'INTRUSION - PENTEST

Programme de la formation

- **Présentation de la méthodologie**
- **Les différents types de PenTest**
 - Définition et Description du cycle du PenTest,
 - Identification des différents types d'attaquants,
 - Les types d'audits, etc.
- **Les aspects réglementaires**
 - Les responsabilités de l'auditeur
 - Les contraintes
 - La législation et les articles de la loi
 - Les précautions
- **Méthodologies et outils (préparation et déroulement de l'audit)**
- **Mise en pratique : attaque d'une machine virtuelle**
- **Rédaction du rapport d'audit**
 - Le rapport d'audit : son importance, sa composition (synthèse générale, synthèse technique, évaluation du risque, exemple d'impacts,...),
 - La préparation du rapport d'audit : mise en forme des informations collectées lors de l'audit, préparation du document et application de la méthodologie
 - L'écriture du rapport : l'analyse globale de la sécurité du système, la description des vulnérabilités trouvées, les recommandations de sécurité, la synthèse générale sur la sécurité du système
 - La transmission du rapport : les précautions nécessaires, la méthodologie de transmission de rapport
 - Que faire une fois le rapport transmis ?
- **Conclusion et débriefing**



O.F. Déclaration d'activité N° 76311168831
la préfecture de la région Occitanie
Mise à jour le 03/03/2024

LA METHODOLOGIE D'AUDIT DE TESTS D'INTRUSION - PENTEST

Notes