Formation Tests d'intrusion, organiser son audit

N° ACTIVITÉ : 11 92 18558 92 | TÉLÉPHONE : 01 85 77 07 07 | E-MAIL : inscription@hubformation.com

Le test d'intrusion ou Pentest, est une intervention technique qui permet de déterminer le réel potentiel d'intrusion et de destruction d'un pirate sur une infrastructure SI. Ce stage présente la démarche et les outils pour effectuer ce type de test et rédiger de manière professionnelle le rapport final d'audit.

Référence	TEI
Durée	4 jours (28h)
Tarif	2 790 €HT
Repas	repas inclus

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

Public

| Responsables, architectes sécurité.
| Techniciens et administrateurs systèmes et réseaux.
| Auditeurs amenés à faire du Pentest.

Prérequis

| Bonnes connaissances de la sécurité informatique (matériel, architectures réseau, architectures applicatives).
| Expérience requise.

Programme de la formation

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.
| Travaux pratiques : Réaliser un audit.

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.
| Travaux pratiques : Manipulation d'outils de Pentest. Utilisation d'outils de scan.

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)

du 4 au 7 février 2025
du 15 au 18 avril 2025
du 15 au 18 juillet 2025
du 28 au 31 octobre 2025

PARIS

du 28 au 31 janvier 2025
du 8 au 11 avril 2025
du 8 au 11 juillet 2025
du 21 au 24 octobre 2025

VOIR TOUTES LES DATES

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.
| Réflexion collective : Réalisation d'un rapport suite à un test d'intrusion.

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.
| Travaux pratiques : Les participants vont auditer un réseau d'entreprise sur la base d'un scénario d'un cas réel.

Méthode pédagogique

Chaque participant travaille sur un poste informatique qui lui est dédié. Un support de cours lui est remis soit en début soit en fin de cours. La théorie est complétée par des cas pratiques ou exercices corrigés et discutés avec le formateur. Le formateur projette une présentation pour animer la formation et reste disponible pour répondre à toutes les questions.

Méthode d'évaluation

Tout au long de la formation, les exercices et mises en situation permettent de valider et contrôler les acquis du stagiaire. En fin de formation, le stagiaire complète un QCM d'auto-évaluation.

Suivre cette formation à distance

Voici les prérequis techniques pour pouvoir suivre le cours à distance :

| Un ordinateur avec webcam, micro, haut-parleur et un navigateur (de préférence Chrome ou Firefox). Un casque n'est pas nécessaire suivant l'environnement.
| Une connexion Internet de type ADSL ou supérieure. Attention, une connexion Internet ne permettant pas, par exemple, de recevoir la télévision par Internet, ne sera pas suffisante, cela engendrera des déconnexions intempestives du stagiaire et dérangera toute la classe.
| Privilégier une connexion filaire plutôt que le Wifi.
| Avoir accès au poste depuis lequel vous suivrez le cours à distance au moins 2 jours avant la formation pour effectuer les tests de connexion préalables.
| Votre numéro de téléphone portable (pour l'envoi du mot de passe d'accès aux supports de cours et pour une messagerie instantanée autre que celle intégrée à la classe virtuelle).
| Selon la formation, une configuration spécifique de votre machine peut être attendue, merci de nous contacter.
| Pour les formations incluant le passage d'une certification la dernière journée, un voucher vous est fourni pour passer l'examen en ligne.
| Pour les formations logiciel (Adobe, Microsoft Office...), il est nécessaire d'avoir le logiciel installé sur votre machine, nous ne fournissons pas de licence ou de version test.
| Horaires identiques au présentiel.

Accessibilité

Les sessions de formation se déroulent sur des sites différents selon les villes ou les dates, merci de nous contacter pour vérifier l'accessibilité aux personnes à mobilité réduite.
Pour tout besoin spécifique (vue, audition...), veuillez nous contacter au 01 85 77 07 07.