Formation Tests d'intrusion - Mise en situation d'audit

Le Pen Test par la pratique

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

En bon professionnel, tout responsable de la sécurité informatique doit remettre en question les protocoles et techniques employés pour sécuriser son réseau à intervalle régulier. En effet, chaque semaine, de nouveaux virus apparaissent, de nouvelles failles sont détectées pour un OS ou un matériel et devant ces nouveaux risques il convient de s'assurer que la sécurité n'est pas menacée. L'audit est une réponse adaptée à ce challenge : le Pen Test (de l'anglais "Penetration Test") est une intervention très technique, qui permet de déterminer le potentiel réel d'intrusion et de destruction d'un pirate sur l'infrastructure, et de valider l'efficacité réelle de la sécurité appliquée aux systèmes, au réseau et à la confidentialité des informations. Les participants à cette formation avancée apprendront à mettre en place une véritable procédure d'audit de type Pen Test et ainsi évaluer les risques et décider des actions à mettre en oeuvre.

Référence	SEC102
Durée	5 jours (35h)
Tarif	3 690 €HT

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)
- du 16 au 20 juin 2025
- du 1er au 5 septembre 2025

PARIS
- du 16 au 20 juin 2025
- du 1er au 5 septembre 2025

AIX-EN-PROVENCE
- du 16 au 20 juin 2025
- du 3 au 7 novembre 2025

BORDEAUX
- du 16 au 20 juin 2025
- du 1er au 5 septembre 2025

GRENOBLE
- du 16 au 20 juin 2025
- du 1er au 5 septembre 2025

LILLE
- du 16 au 20 juin 2025
- du 3 au 7 novembre 2025

LYON
- du 16 au 20 juin 2025
- du 1er au 5 septembre 2025

NANTES
- du 16 au 20 juin 2025
- du 3 au 7 novembre 2025

VOIR TOUTES LES DATES

Objectifs

| Savoir organiser une procédure d'audit de sécurité de type test de pénétration sur son SI
| Se mettre en situation réelle d'Audit
| Mettre en application les compétences techniques acquises dans le cadre d'une intervention professionnelle
| rédiger un rapport d'audit professionnel
| Savoir présenter et transmettre un rapport d'audit

Public

| RSSI
| Consultants en sécurité
| Techniciens
| Auditeurs amenés à faire du Pen Test ou ceux qui veulent se perfectionner en Pen Test
| Administrateurs systèmes / réseaux

Prérequis

| Avoir suivi la formation Hacking et Sécurité - Niveau avancé (SE101) ou disposer des compétences équivalentes

Programme de la formation

Méthodologie de l'Audit
Objectifs et types de Pen Test
| Qu'est-ce qu'un Pen Test ?
| Le cycle du Pen Test
| Différents types d'attaquants
| Types d'audits : boîte noire, boîte blanche, boîte grise
| Avantages du Pen Test
| Limites du Pen Test
| Cas particuliers : dénis de service, ingénierie sociale

Aspect règlementaire
| Responsabilité de l'auditeur
| Contraintes fréquentes
| Législation : articles de loi
| Précautions
| Points importants du mandat

Exemples de méthodologies et d'outils
| Préparation de l'audit
| Déroulement
| Cas particuliers
| Habilitations
| Dénis de service
| Ingénierie sociale
| Déroulement de l'audit
| Reconnaissance
| Analyse des vulnérabilités
| Exploitation
| Gain et maintien d'accès
| Comptes-rendus et fin des tests

Mise en pratique sur Metasploitable
| Attaque de la machine virtuelle Metasploitable
| Recherche d'informations
| Recherche de vulnérabilités
| Exploitation des vulnérabilités
| Maintien de l'accès

Éléments de rédaction d'un rapport
| Importance du rapport
| Composition
| Synthèse générale
| Synthèse technique
| Évaluation du risque
| Exemples d'impacts
| Se mettre à la place du mandataire

Préparation du rapport d'audit
| Mise en forme des informations collectées lors de l'audit
| Préparation du document et application de la méthodologie vue lors du premier jour

Écriture du rapport
| Analyse globale de la sécurité du système
| Description des vulnérabilités trouvées
| Définition des recommandations de sécurité
| Synthèse générale sur la sécurité du système

Transmission du rapport
| Précautions nécessaires
| Méthodologie de transmission de rapport
| Que faire une fois le rapport transmis ?

Méthode pédagogique

Le passage en revue des principales techniques d'attaques et outils utilisés.
L'utilisation d'outils d'analyse et d'automatisation des attaques.
Une formation très pratique : une mise en situation d'audit sera faite afin d'appliquer sur un cas concret les outils méthodologiques et techniques vus lors de la première journée. Le système d'information audité comportera diverses vulnérabilités (web, applicatives, etc.) plus ou moins faciles à découvrir et à exploiter. L'objectif étant d'en trouver un maximum lors de l'audit et de fournir au client les recommandations adaptées afin que ce dernier sécurise efficacement son système d'information.
L'apport de consultants experts en audits techniques des SI.

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.