Formation Hacking et Sécurité - Niveau avancé

Pratiquez les attaques avancées pour mieux vous défendre

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

Ce n'est pas un hasard si certaines des sociétés spécialisées en sécurité informatique les plus performantes comptent parmi leurs effectifs d'anciens hackers repentis. On en comprend d'ailleurs aisément la logique tant il parait évident que les personnes les plus à même d'identifier les failles d'un SI sont celles qui sont-elles mêmes capables de l'attaquer. C'est précisément sur cette logique qu'a été conçue cette formation qui propose aux spécialistes informatiques impliqués dans la protection d'un SI d'adopter la position des hackers pour identifier ses éventuelles vulnérabilités et mener à bien les actions permettant de les corriger.

Référence	SEC101
Durée	5 jours (35h)
Tarif	3 850 €HT

Objectifs

| Organiser une veille sur la sécurité et rechercher des informations fiables
| Identifier les "faiblesses" des éléments constitutifs du SI par des prises d'empreintes
| Réaliser différentes attaques et en identifier les subtilités
| Protéger le SI par un système de contre-mesures adaptées

Public

| Consultants en sécurité
| Ingénieurs / Techniciens
| Administrateurs systèmes / réseaux
| Développeurs

Prérequis

| Avoir suivi la formation Hacking et Sécurité - Les fondamentaux ou connaissances équivalentes
| Connaissances de TCP/IP
| La maîtrise de Linux en ligne de commande est un plus

Programme de la formation

Introduction
| Rappels sur TCP/IP

Introduction à la veille
| Vocabulaire
| Base de données de vulnérabilité et exploitation
| Informations générales

Prise d'informations
| Informations publiques
| Moteur de recherches
| Prise d'information active

Scan et prise d'empreinte
| Énumération des machines
| Scan de ports
| Prise d'empreinte du système d'exploitation

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)
du 2 au 6 juin 2025
du 18 au 22 août 2025

PARIS
du 2 au 6 juin 2025
du 18 au 22 août 2025

AIX-EN-PROVENCE
du 2 au 6 juin 2025
du 20 au 24 octobre 2025

BORDEAUX
du 2 au 6 juin 2025
du 18 au 22 août 2025

GRENOBLE
du 2 au 6 juin 2025
du 18 au 22 août 2025

LILLE
du 20 au 24 octobre 2025

LYON
du 2 au 6 juin 2025
du 18 au 22 août 2025

NANTES
du 18 au 22 août 2025
du 20 au 24 octobre 2025

RENNES
du 18 au 22 août 2025
du 20 au 24 octobre 2025

VOIR TOUTES LES DATES

| Prise d'empreinte des services

Vulnérabilités informatiques
| Vulnérabilités réseau
| Vulnérabilités applicatives
| Vulnérabilités web
| Exploitation des vulnérabilités
| Maintien de l'accès à une machine

Atelier pratique en laboratoire
| Mise en oeuvre d'une stratégie d'attaque sur un laboratoire créé spécialement pour la formation
| Lancement de l'attaque et tentative d'exploitation
| Capture de drapeau
| Étude des contre-mesures appropriées

Méthode pédagogique

Une formation très pratique : 80% du temps de la formation est consacré aux ateliers pratiques. Une approche pratique : un panorama des techniques utilisées dans le cadre d'intrusions sur des réseaux d'entreprises, complétée par un atelier pratique sur un laboratoire spécialement créé pour la formation. Chaque présentation technique s'accompagne de procédures de sécurité applicables sous différentes architectures (Windows et Linux). Une pédagogie basée sur le partage d'expériences et de bonnes pratiques de la part d'un consultant spécialiste de la sécurité informatique.

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.