Formation Hacking et Sécurité - Niveau expert

Protéger étape par étape un système d'information

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

L'actualité nous le rappelle quasi quotidiennement, les intrusions dans des systèmes informatiques publics ou privés existent. Et bien souvent, les entreprises qui en sont victimes sont pointées du doigt pour n'avoir pas su correctement protéger leurs données. Si le risque 0 n'existe pas, il apparait presque évident qu'en éprouvant son SI régulièrement, les équipes en charge de garantir la sécurité peuvent être amenées à détecter de nouvelles failles ou menaces et ainsi mettre en oeuvre la correction ad' hoc... Durant cette formation très pratique qui consiste en une série d'ateliers ponctuée d'échanges, les participants auront à disposition un environnement technique complexe qu'ils pourront attaquer à loisir pour mieux le protéger par la suite, apprenant ainsi à le protéger un système de bout en bout.

Référence	SEC104
Durée	5 jours (35h)
Tarif	3 890 €HT

Objectifs

| Savoir protéger son système d'information
| Identifier comment sécuriser tous les aspects d'un SI : réseau, applicatifs et Web
| Acquérir les connaissances et compétences nécessaires pour détecter des failles et mettre en oeuvre des parades
| Savoir correctement réagir en cas d'attaque soudaine
| Être capable de mettre en application les compétences techniques acquises dans le cadre d'une intervention professionnelle

Public

| Développeurs
| Administrateurs systèmes / réseaux
| Ingénieur sécurité
| Consultant sécurité

Prérequis

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

Programme de la formation

Introduction
| Définition du hacking
| Panorama 2018/2019
| Référentiel de sécurité (ANSSI, ENISA, CLUSIF, Cybermalvaillance.gouv etc...)
| Les différents types de hackers
| Les différents types d'attaques
| Les différents outils utilisés par le hacker
| Le cycle de l'attaquant

Le Hacking
| Scan de réseau/ports/versions
| Exploitation de CVE
| Élévation de privilège
| Mise en place d'une backdoor
| Récupération d'informations, création d'un dictionnaire + Bruteforce

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)
du 21 au 25 juillet 2025
du 29 sept. au 3 octobre 2025

PARIS
du 21 au 25 juillet 2025
du 29 sept. au 3 octobre 2025

AIX-EN-PROVENCE
du 21 au 25 juillet 2025
du 29 sept. au 3 octobre 2025

BORDEAUX
du 29 sept. au 3 octobre 2025
du 8 au 12 décembre 2025

GRENOBLE
du 29 sept. au 3 octobre 2025
du 8 au 12 décembre 2025

LILLE
du 21 au 25 juillet 2025
du 8 au 12 décembre 2025

LYON
du 29 sept. au 3 octobre 2025
du 8 au 12 décembre 2025

NANTES
du 21 au 25 juillet 2025
du 29 sept. au 3 octobre 2025

VOIR TOUTES LES DATES

| Payload msfvenom MITM
| Saut de VLAN (yersinia et/ou table overflow)

Les piliers de la sécurité
| Confidentialité
| Intégrité
| Disponibilité
| Traçabilité

Les grands principes de la sécurité
| IAAA
| Authentification
| Need to know
| Least Privilege
| Non répudiation
| Défense en profondeur

La sécurité physique
| Notion de sécurité physique
| Mise en correspondance des notions avec les principes précédents

Sécuriser le réseau
| La sécurité de la couche 2 : Port security, vLlan, Ssh, dhcp snooping, Defense contre arp MITM, Sécurité pour DTP,CDP,VTP,STP.
| La sécurité de la couche 3 : IPSec, routeur filtrant
| La sécurité de la couche 4 : Explication de la passerelle d'interconnexion de l'ANSSI, Travaux pratiques sur PFsense, explication des IDS/IPS , présentation de Snort, travaux pratiques sur Snort
| La sécurité de la couche 5 : Le proxy

Sécuriser le système
| Hardenning sur Linux
| Hardenning sur Windows
| Mise en place d'HIDS

Supervision de la sécurité
| Présentation SOC
| Présentation SIEM
| Présentation de ELK et Splunk
| Mise en place de ELK ou Splunk pour analyser les Logs

Réponse à incident
| Rejouer les attaques
| Analyser les logs
| Utiliser WireShark

Méthode pédagogique

Le passage en revue des principales techniques de défense et outils utilisés. L'utilisation d'outils d'analyse et d'automatisation des attaques. Une formation très pratique : l'essentiel de la formation portera sur des contre-mesures concrètes techniques que chacun peut mettre en oeuvre dans son entreprise. 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.