Formation Hacking et Sécurité - Les fondamentaux

Connaître les différents types d'attaque système pour mieux se protéger

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

L'origine du hacking remonte au milieu des années 50 quand les premiers ordinateurs disponibles dans les universités américaines sont rapidement devenus la proie de d'étudiants avides de "bidouiller" pour s'approprier le système. Ainsi sont nés les hackers qui, profitant de l'avènement d'Internet des décennies plus tard, n'ont cessé de prendre pour cible des systèmes informatiques de plus en plus perfectionnés, allant même jusqu'à pirater des systèmes gouvernementaux. Pour faire face à ces menaces sans cesse croissantes, les DSI attendent des ingénieurs et techniciens qu'ils soient à même de protéger efficacement les systèmes informatiques de leurs organisations. L'objet de cette formation est précisément de leur fournir les compétences et connaissances qui leur permettront de mener à bien cette mission.

Référence	SEC100
Durée	4 jours (28h)
Tarif	2 990 €HT

Objectifs

| Identifier comment il est possible de s'introduire frauduleusement sur un système distant
| Savoir quels sont les mécanismes en jeu dans le cas d'attaques système
| Acquérir les compétences nécessaires pour mettre en place un dispositif global garantissant la sécurité des systèmes

Public

| Consultants en sécurité
| Ingénieurs / Techniciens
| Administrateurs systèmes / réseaux
| Toute personne intéressée par la pratique de la sécurité

Prérequis

| Connaissances de base de Windows ou Linux

Programme de la formation

Introduction sur les réseaux
| Prise d'informations (Prise d'informations à distance sur des réseaux d'entreprise et des systèmes distants)
| Informations publiques
| Localiser le système cible
| Énumération des services actifs

Attaques à distance
| Intrusion à distance des postes clients par exploitation des vulnérabilités sur les services distants, et prise de contrôle des postes utilisateurs par troyen
| Authentification par brute force
| Recherche et exploitation de vulnérabilités
| Prise de contrôle à distance

Attaques systèmes
| Attaques du système pour outrepasser l'authentification et/ou surveiller l'utilisateur suite à une intrusion

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)
- du 19 au 22 mai 2025*
- du 28 au 31 juillet 2025*

PARIS
- du 19 au 22 mai 2025*
- du 28 au 31 juillet 2025*

AIX-EN-PROVENCE
- du 28 au 31 juillet 2025
- du 29 sept. au 2 octobre 2025

BORDEAUX
- du 19 au 22 mai 2025
- du 29 sept. au 2 octobre 2025

GRENOBLE
- du 19 au 22 mai 2025
- du 29 sept. au 2 octobre 2025

LILLE
- du 19 au 22 mai 2025
- du 29 sept. au 2 octobre 2025

LYON
- du 19 au 22 mai 2025
- du 29 sept. au 2 octobre 2025

NANTES
- du 28 au 31 juillet 2025
- du 29 sept. au 2 octobre 2025

VOIR TOUTES LES DATES

(*) session confirmée

| Attaque du Bios
| Attaque en local
| Cracking de mot de passe
| Espionnage du système

Sécuriser le système
| Outils de base permettant d'assurer le minimum de sécurité à son S.I.
| Cryptographie
| Chiffrement des données
| Détection d'activité anormale
| Initiation à la base de registre
| Firewalling
| Anonymat

Méthode pédagogique

Une formation très pratique : 70% du temps de la formation est consacré aux ateliers pratiquesUn accent particulier est mis sur la pratique des différentes formes d'attaques existantes.Chaque présentation technique s'accompagne de procédures de sécurité applicables sous différentes architectures (Windows et Linux).Les retours d'expériences de professionnels de la sécurité.

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.