

Dans la peau d'un hacker

Prix : 1 450 €HT

Durée : 2 jours

Code de Référence : SECU10

Cette session, d'une durée de deux jours, vous permettra de comprendre les risques liés à la sécurité informatique et les différents types d'attaques mais aussi d'adopter les bonnes pratiques pour se protéger.

Objectifs de la formation

- Comprendre et appréhender les méthodologies d'attaque sur un Système d'Information
- Sensibilisation à l'exploitation de vulnérabilités ; bien comprendre les impacts des choix opérationnels sur la sécurité du SI
- Sensibilisation aux bonnes pratiques sécurité

Public

Cette formation s'adresse aux DSI, RSSI, administrateurs système, responsables réseaux, administrateurs réseaux.

Prérequis

- Connaissance des principaux langages de programmation web
- Connaissances système et réseau
- Connaissances en scripting (python, perl, bash ...)

Profil animateur

Cette formation est animée par un expert consultant Sécurité.

Programme de la formation

JOUR 1

Prise d'information

- Whois, Shodan, google dorks, Réseaux sociaux, DNS, geolocalisation

Réseau

- Scan de ports
- Sniffing

- Poisonning ARP, mDNS, LLMNR

Attaques distantes

- Scanner de vulnérabilité, Base de vulnérabilité
- Attaque d'un serveur, d'un poste client
- Introduction à Metasploit

JOUR 2

Attaques Locales

- Élévation de privilèges
- Cassage de mot de passes
- Malware et Anti-virus

Attaques WEB :

- Injections
- Sécurisation des accès

Sécurisation

- Gestion des mises à jour
- Bonnes pratiques

Méthodes pédagogiques

Des exercices pratiques et des démonstrations vous permettront de mettre en pratique les notions théoriques présentées. 60% de théorie | 40% de pratique

Méthodes d'évaluation des acquis

Afin d'évaluer l'acquisition de vos connaissances et compétences, il vous sera envoyé un formulaire d'auto-évaluation, qui sera à compléter en amont et à l'issue de la formation.

Un certificat de réalisation de fin de formation est remis au stagiaire lui permettant de faire valoir le suivi de la formation.