

Hacking éthique et sécurité avancée

Cette formation vous permet d'avoir une approche avancée et pratique des méthodologies utilisées dans le cadre d'intrusions sur des réseaux d'entreprises. Différentes techniques d'attaques sont détaillées et accompagnées de procédures de sécurité applicables sous Windows et Linux.

Compétences visées

- Mettre en place des tests d'intrusion au sein de systèmes d'information (SI)
- Gérer la sécurité avancée d'un SI

Objectifs pédagogiques

- Définir l'impact et la portée d'une vulnérabilité
- Lister les techniques avancées de hacking
- Sécuriser un réseau

Public

Administrateurs réseaux, administrateurs Web, webmaster, hackeur

Prérequis

Avoir suivi la formation Les bases du hacking et de la cybersécurité ou en posséder les connaissances équivalentes.

Programme

La sécurité avancée des réseaux

- Identifier les techniques d'attaque Man-in-the-Middle (MITM)
- Lister les méthodes avancées de recherche de vulnérabilités dans l'infrastructure de la cible

La sécurité avancée du Web

- Définir les méthodes avancées d'exploitation SQLi
- Mettre en œuvre des méthodes avancées d'exploitation XSS

La post-exploitation sous Windows et Linux

- Analyser le système
- Exploiter des vulnérabilités et des erreurs de configuration
- Contourner des mécanismes de sécurité
- Extraire des mots de passe
- Décrire l'attaque Pass-the-hash et l'exploiter
- Élever ses privilèges

Workshop

- Mettre en œuvre des attaques sur un laboratoire dédié à la formation et appliquer les savoirs théoriques.

Durée

5 jours - 35 heures

Prix inter

3500 €HT

Prochaines dates

9 au 13 juillet 2018

24 au 28 septembre 2018

19 au 23 novembre 2018

Méthodes

pédagogiques

12 participants maximum.

Alternance d'apports théoriques et pratiques. Support de cours et documents d'application remis en fin de formation.

Validations des acquis

Quizz final et évaluation de la formation.

Formateur

Formateur expert dans le hack éthique.

Après cette formation, vous pouvez suivre les formations **Audit de sécurité et tests d'intrusion : Pentest.**