Les bases du hacking et de la cybersécurité

Le hacker éthique (white hat) utilise les mêmes techniques qu'un attaquant malveillant dans le but de sécuriser un système informatique : il étudie ses méthodes, ses principes de fonctionnement, décortique sa manière d'agir. Cela lui permet de renforcer la sécurité là où elle en a besoin.

Compétences visées

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

Objectifs pédagogiques

- Découvrir les techniques de base du hacking
- Mettre en place des outils de sécurité

Public

Toute personne travaillant dans la technique souhaitant évoluer vers une mission d'expert technique en cybersécurité

Prérequis

Avoir des connaissances en administration système et réseau est nécessaire.

Programme

Décrire la législation de la sécurité des SI

Définir les tests d'intrusion

- Définir les différentes méthodes d'intrusion et leurs objectifs : boîte noire, boîte grise, boîte blanche
- Lister les techniques d'intrusion
- Identifier la classification des moyens d'intrusion
- Identifier les outils existants

Analyser la cible de l'intrusion

- Lister les méthodes d'analyse de la cible
- Prendre des informations publiques
- Localiser un système cible
- Définir le Social Engineering

La sécurité des réseaux

- Mettre en œuvre du scanning avec Nmap
- Analyser le réseau et ses composants
- Identifier les comptes par défaut
- Exploiter les failles de sécurité et les vulnérabilités
- Pousser l'exploitation à des réseaux connexes
- Effacer ses traces

La sécurité Web

- Lister les méthodes d'injection sur MySQL et d'autres SGBD
- Définir et identifier les attaques XSS (Cross-site Scripting)
- Définir les attaques LFI-RFI (Local File Inclusion / Remote File Inclusion)
- Identifier la faille CSRF (Cross site request forgery)
- Identifier la vulnérabilité RCE (Remote Command Execution) basée sur le Web
- Lister les outils d'exploitation

Sécuriser le système d'informations

- Lister les outils de base permettant d'assurer le minimum de sécurité
- Identifier la cryptographie, le chiffrement des données
- Mettre en place la détection d'activité anormale
- Identifier le rôle de la base de registre
- Mettre en place des firewalls

Durée
2 jours - 14 heures

Prix inter
1350 €HT

Prochaines dates
13 et 14 septembre 2018
29 et 30 octobre 2018
17 et 18 décembre 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 Hacking éthique et sécurité avancée, Audit de sécurité et tests d'intrusion : Pentest.