Hacking et Sécurité : Niveau avancé

Maîtriser les différents types d'attaques pour mieux se défendre

3 jours / 21 heures | **Valence** | **Ref : SECU2**

PRÉSENTATION

Ces dernières années ont été le témoin de l'essor de cyberincidents affectant, à divers degrés, tout un chacun. Qu'il s'agisse d'incivilité, de harcèlement, d'escroquerie, de fraude, de vol, de destruction, de dysfonctionnement, de surveillance, d'espionnage, d'activisme ou encore par exemple de terrorisme ou de désinformation, toute forme de délit, de violence ou de conflictualité se matérialise via l'Internet. C'est précisément sur cette logique qu'a été conçue cette formation qui propose aux spécialistes informatiques impliqués dans la protection d'un SI d'adopter la position des hackers pour identifier les éventuelles vulnérabilités d'un système d'information et mener à bien les actions permettant de se prémunir des attaques..

—TEST D'INTRUSION

—CYBERSÉCURITÉ

—HACKING

OBJECTIFS DE LA FORMATION

COMPRENDRE comment organiser une veille sur la sécurité et savoir où rechercher des informations fiables
IDENTIFIER les faiblesses des éléments constitutifs du SI par des prises d'empreintes
DISPOSER des compétences techniques nécessaires pour réaliser différentes attaques et en comprendre les subtilités
PROTÉGER le SI par un système de contre-mesures adaptées

PUBLIC VISÉ

Consultants en sécurité
Techniciens
Administrateurs systèmes / réseaux
Développeurs

PRÉREQUIS

Connaissances de l'administration de postes Windows ou Linux
Connaissance de TCP/IP

POUR ALLER PLUS LOIN..

Cybersécurité : Niveau expert [Ref : SECU3]
Cloud Computing : Les fondamentaux [Ref : CLOUD1]

LES + DE LA FORMATION

PRATIQUE
70% du temps de formation est consacré aux ateliers pratiques

MISE EN SITUATION
des différentes formes d'attaques existantes

APPLICABILITÉ
directe des outils sous architectures Windows et Linux

RETOURS D'EXPÉRIENCES
d'experts de la sécurité informatique

Programme

JOUR 1

Introduction à la veille

- Rappel : vocabulaire et terminologie
- Base de données de vulnérabilités
- Collecte des informations et de code d'exploitation
- Informations générales

Prise d'informations

- Techniques de prise d'informations à partir de données publiques
- Exploitation spécifique des moteurs de recherche
- Collecte active et exploitation de données

JOUR 2

Scan et prise d'empreintes des systèmes et des services

- Cartographie du système d'information et identification des machines et des équipements
- Prise d'empreintes des systèmes d'exploitation cibles
- Sca, de ports
- Prise d'empreintes des services

JOUR 3

Vulnérabilités des systèmes d'information

- Vulnérabilité des réseaux informatiques
- Vulnérabilité des applications et des services Web
- Exploitation des différentes vulnérabilités et vecteurs d'attaques
- Élévation des privilèges
- Attaques par rebond
- Maintien de l'accès à une ou plusieurs machines compromises
- Suppression des traces de l'attaque et des signes de compromission des équipements