HACKING & SÉCURITÉ : LES FONDAMENTAUX

Apprenez les fondamentaux de la sécurité informatique

Code : HSF

Cette formation est une première approche des pratiques et des méthodologies utilisées dans le cadre de tests d'intrusion. Nous mettons l'accent sur la compréhension technique et la mise en pratique des différentes formes d'attaques existantes. L'objectif est de vous fournir les premières compétences techniques de base, nécessaires à la réalisation d'audits de sécurité ou de tests d'intrusion. Ainsi, vous jugerez de l'impact réel des vulnérabilités découvertes sur le SI.

Il s'agit d'une bonne introduction au cours HSA pour toute personne souhaitant acquérir les connaissances techniques de base.

PROGRAMME

Méthodes mobilisées : cette formation est construite avec une alternance de cours théoriques et de cas pratiques afin de favoriser l'acquisition des savoirs du programme (cf. Ressources).

Modalités d'évaluation : les objectifs sont régulièrement évalués tout au long de la formation (50% de cas pratiques) et formalisés sous forme de grille d'évaluation des compétences complétée en fin de module par le formateur.

JOUR 1

Introduction
- Définitions
- Objectifs
- Vocabulaire
- Méthodologie de test

Prise d'information
- Objectifs
- Prise d'information passive (WHOIS, réseaux sociaux, Google Hacking, Shodan, etc.)
- Prise d'information active (traceroute, social engineering, etc.)
- Bases de vulnérabilités et d'exploits

Réseau et attaques connues
- Rappels modèles OSI et TCP/IP
- Protocoles ARP, IP, TCP et UDP
- NAT
- Scan de ports
- Sniffing et outils
- ARP Cache Poisoning
- DoS / DDoS

JOUR 2

Attaques à distance
- Introduction à Metasploit Framework
- Scanner de vulnérabilités
- Attaque d'un poste client
- Attaque d'un serveur
- Introduction aux vunérabilités Web

Attaques locales
- Cassage de mots de passe
- Élévation de privilèges
- Attaque du GRUB

Ingénierie sociale
- Utilisation de faiblesses humaines afin de récupérer des informations sensibles et/ou compromettre des systèmes
- Phishing (hameçonnage)
- Outils de contrôle à distance
- Attaque à distance
- Introduction à Metasploit Framework

Se sécuriser
- Les mises à jour
- Configurations par défaut et bonnes pratiques
- Introduction à la cryptographie
- Présentation de la stéganographie
- Anonymat (TOR)

PROCHAINES DATES

3 février 2025
7 avril 2025
5 juin 2025
18 septembre 2025
3 novembre 2025
8 décembre 2025

OBJECTIFS

- Se familiariser avec les termes techniques et connaître les méthodologies pour mener un test d'intrusion
- Comprendre les méthodes de prise d'information (recherche passive)
- Connaître les notions fondamentales du réseau
- Connaître les attaques distantes et locales
- Se sensibiliser face aux attaques d'ingénierie sociale
- Adopter les bonnes pratiques de sécurité
- Connaître les notions de cryptographie, de stéganographie et d'anonymat
- Mettre en pratique les connaissances acquises

INFORMATIONS GÉNÉRALES

Code : HSF
Durée : 2 jours
Prix : 1 495 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois (92) ou en distanciel
Les + : petits-déjeuners, pause-café et déjeuners offerts pour les stagiaires en présentiel

PUBLIC VISÉ

- RSSI
- Ingénieurs / Techniciens
- Administrateurs systèmes et réseaux
- Toute personne s'intéressant à la sécurité informatique

PRÉ-REQUIS

- Connaître des notions de sécurité informatique
- Être familier avec les invites de commandes Windows et Linux
- Avoir des connaissances sur le fonctionnement des applications Web

RESSOURCES

- Support de cours
- 50% d'exercices pratiques
- 1 PC par personne