HACKING & SÉCURITÉ : AVANCÉ

Se mettre dans la peau d'un attaquant pour mieux protéger votre SI

Code : HSA

Ce cours est une approche avancée et pratique des méthodologies utilisées dans le cadre d'intrusions sur des réseaux d'entreprises.
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 techniques offensives des attaques informatiques, en jugeant par vous-même de la criticité et de l'impact réel des vulnérabilités découvertes sur le SI.

La présentation des techniques d'attaques est accompagnée de procédures de sécurité applicables sous différentes architectures (Windows et Linux).

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 (cas pratiques, TP...) et formalisés sous forme de grille d'évaluation des compétences complétée en fin de module par le formateur.

JOUR 1

Introduction
- Vocabulaire
- Vulnérabilités et exploits
- Concepts généraux

Prise d'information
- OSINT
- Google Hacking
- Scan de ports
- Prise d'empreinte du système des services

JOUR 2

Attaques réseau
- Sniffing réseau
- Man-in-The-Middle
- DNS Hijacking
- Attaque des protocoles sécurisés
- Dénis de service

Attaques système
- Attaque depuis un accès physique
- Exploitation d'un service vulnérable distant
- Outil d'exploitation Metasploit
  - Génération d'un malware
  - Encodage de la charge malveillante
  - Exploitation de vulnérabilités

JOUR 3

Attaque Système
- Élévation de privilèges
- Attaque cryptographique sur les mots de passe

Attaques Web
- Cartographie et énumération
- Attaque par énumération (brute-force)
- Inclusion de fichiers (LFI / RFI)
- Injection de commande
- Cross-Site Scripting (XSS)
- Injection SQL
- Upload de fichiers

JOUR 4

Attaques applicatives
- Buffer overflow sous Linux
  - L'architecture Intel x86
  - Les registres
  - La pile et son fonctionnement
  - Présentation des méthodes d'attaques standards
    - Écrasement de variables
    - Contrôler EIP
    - Exécuter un shellcode
    - Prendre le contrôle du système en tant qu'utilisateur root

JOUR 5

Challenge final
- Mise en pratique des connaissances acquises durant la semaine sur un TP final (CTF d'une journée)

PROCHAINES DATES

12 février 2024
11 mars 2024
15 avril 2024
13 mai 2024
17 juin 2024
16 septembre 2024
14 octobre 2024
18 novembre 2024

OBJECTIFS

- Comprendre les méthodes de prise d'information
- Savoir mener des attaques réseau
- Mettre en pratique les différents types d'attaques système
- Apprendre le concept des dépassements de tampon (buffer overflow) et le mettre en pratique
- Mettre en pratique les différents types d'attaques Web
- Appliquer l'ensemble des attaques abordées durant les précédents jours sur un nouveau réseau

INFORMATIONS GÉNÉRALES

Code : HSA
Durée : 5 jours
Prix : 4 150 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois (92) ou en distanciel

PUBLIC VISÉ

- RSSI, DSI
- Ingénieurs / Techniciens
- Administrateurs systèmes / réseaux
- Développeurs

PRÉ-REQUIS

- Avoir suivi la formation HSF ou une formation équivalente
- Avoir des connaissances sur les protocoles réseaux TCP/IP
- Avoir des connaissances sur la sécurité des systèmes Windows et Linux
- Avoir des connaissances sur le développement Web et le fonctionnement des applications Web

RESSOURCES

- Support de cours
- 80% d'exercices pratiques
- 1 PC par personne avec un environnement dédié sur notre plateforme MALICE

FORMATIONS ASSOCIÉES

- HSE : Hacking & Sécurité : Expert
- CEHv12 : Certified Ethical Hacker v12
- TEST-INT : Test d'intrusion : Mise en situation d'audit
- SWAD : Sécurité Windows et Active Directory
- AUDWEB : Audit de site Web