HACKING & SÉCURITÉ : LE BOOTCAMP

Un terrain d'entraînement pour experts en cybersécurité.

Code : HSB

NOUVEAUTÉ

Cette formation intensive vous plonge dans un environnement pratique dédié à la cybersécurité.

À travers une série de défis techniques et scénarios réalistes, vous mettrez vos compétences à l'épreuve sur des systèmes, applications et réseaux vulnérables.

Conçu pour des profils expérimentés, ce bootcamp favorise l'apprentissage par la pratique et le développement de réflexes opérationnels face aux menaces.

PROGRAMME

Méthodes mobilisées : Cette formation se distingue par son format bootcamp : une immersion intensive sur notre plateforme privée MALICE, proche d'un environnement réel d'attaque et de défense.
Les participants travaillent quasi exclusivement sur des cas pratiques (exercices, challenges, scénarios type CTF), accompagnés de débriefings ciblés afin de favoriser la mise en application directe des compétences. La théorie est limitée à des rappels ou apports ponctuels servant de support à la pratique.
Modalités d'évaluation : En amont de la formation, une évaluation des compétences de l'apprenant est effectuée.
Puis, les objectifs sont régulièrement évalués tout au long de la formation (TP, cas pratiques) et formalisés sous forme de grille d'évaluation des compétences complétée en fin de module par le formateur.

JOUR 1

Échauffement
- Web : exercices d'introduction (SQLi, profiling, LFI, énumération)
- Systèmes & réseaux : échappement de conteneurs Docker
- Applicatif : buffer overflow simple
- Scénario applicatif avancé : buffer overflow complexe & échappement de conteneur

JOUR 2

Exploitations & post-exploitation
- Web : Attaque combinée avancée
- Applicatif : Exploitation d'un ransomware
- Systèmes : élévation de privilèges linux

JOUR 3

Analyse approfondie & attaques multicouches
- Applicatif : reverse engineering & exploitation RCE sur protocole UDP
- Systèmes & réseaux : reconnaissance réseau, exploitation web et attaque réseau

JOUR 4

Simulation d'attaque/défense en équipe
- CTF en équipe sur la plateforme MALICE.
- Deux scénarios : chaque équipe joue successivement en attaque puis en défense.

PROCHAINES DATES 23 MARS - 22 JUIN - 7 SEPT - 14 DEC

OBJECTIFS

- Mettre en pratique des techniques avancées d'exploitation Web, applicatives, systèmes et réseaux
- Comprendre et appliquer des méthodes de reverse engineering et de buffer overflow
- Identifier des compromissions à travers des exercices de détection et forensic
- Mettre en œuvre des actions de remédiation et de sécurisation
- Appliquer l'ensemble des compétences acquises dans un CTF final en équipe

INFORMATIONS GÉNÉRALES

Code : HSB

Durée : 4 jours

Prix : 2 990 € HT

Horaires : 9h30 - 17h30

Examen : inclus

Lieu : Levallois (92) - ou en distanciel

Les + : petits-déjeuners, pause-café et déjeuners offerts pour les stagiaires en présentiel

PUBLIC VISÉ

- Consultants et ingénieurs en cybersécurité
- Responsables techniques souhaitant renforcer leur expertise offensive et défensive

PRÉ-REQUIS

- Avoir suivi la formation HSE (Expert) ou justifier d'un niveau équivalent en cybersécurité
- Maîtriser l'administration de systèmes Linux
- Connaître les protocoles réseaux et leurs usages en sécurité offensive et défensive
- Savoir analyser et développer des scripts
- Avoir de bonnes connaissances en sécurité applicative et Web

RESSOURCES

- Accès à la plateforme MALICE
- 1 PC par personne
- Environnement de démonstration