EXPERT

FORMATION HACKING

RÉTRO-INGÉNIERIE DE LOGICIELS MALVEILLANTS

Créez votre laboratoire d'analyse de malwares et comprenez leurs fonctionnements en plongeant dans leurs codes.

Cette formation prépare à la réalisation d'investigations dans le cadre d'attaques réalisées via des logiciels malveillants, de la mise en place d'un laboratoire d'analyse comportementale à l'extraction et au désassemblage de code malveillant.

Code : RILM

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 (70% d'exercices pratiques) et formalisés sous forme de grille d'évaluation des compétences complétée en fin de module par le formateur.

JOUR 1

Rappels sur les bonnes pratiques d'investigation numérique

Présentation des différentes familles de malwares

Vecteurs d'infection

Mécanisme de persistance et de propagation

Laboratoire virtuel vs. physique
- Avantages de la virtualisation
- Solutions de virtualisation

Ségrégation des réseaux
- Réseaux virtuels et réseaux partagés
- Confinement des machines virtuelles
- Précautions et bonnes pratiques

Supervision de l'activité d'une machine
- Réseau
- Système de fichiers
- Registre
- Service

Initiation à l'analyse comportementale

Variété des systèmes

JOUR 2

Mise en place d'un écosystème d'analyse comportementale
- Configuration de l'écosystème
- Définition des configurations types
- Virtualisation des machines invitées
  - VmWare
  - Virtualbox

Installation de CAPEV2/ Virtualbox

Mise en pratique
- Soumission d'un malware
- Déroulement de l'analyse
- Analyse des résultats et mise en forme

Amélioration via API
- Possibilités de développement et améliorations

JOUR 3

Analyse statique de logiciels malveillants
- Prérequis
  - Assembleur
  - Architecture
  - Mécanismes anti-analyse
- Outils d'investigation
  - IDA
- Utilisation d'IDA
  - Méthodologie
  - Analyse statique de code
  - Analyse de flux d'exécution
- Mécanismes d'anti-analyse
  - Packing/protection (chiffrement de code/imports, anti-désassemblage)
  - Machine virtuelle
  - Chiffrement de données
- Travaux pratiques
  - Analyse statique de différents malwares

JOUR 4

Analyse dynamique de logiciels malveillants
- Précautions
  - Intervention en machine virtuelle
  - Configuration réseau
- Outils d'analyse
  - OllyDbg
  - ImmunityDebugger
- Analyse sous débogueur
  - Step into/Step over
  - Points d'arrêts logiciels et matériels
  - Fonctions systèmes à surveiller
  - Génération pseudo-aléatoire de noms de domaines (C&C)
  - Bonnes pratiques d'analyse
- Mécanismes d'anti-analyse
  - Détection de débogueur
  - Détection d'outils de rétro-ingénierie
  - Exploitation de failles système

PROGRAMME

JOUR 5

Analyse de documents malveillants

- Fichiers PDF
  - Introduction au format PDF
  - Spécificités
  - Intégration de JavaScript et possibilités
  - Exemples de PDF malveillants
  - Outils d'analyse : OLE Tools, éditeur hexadécimal
  - Extraction de la charge
  - Analyse de la charge
- Fichiers Office (DOC)
  - Introduction au format DOC/DOCX
  - Spécificités
  - Macros
  - Objets Linking and Embedding (OLE)
  - Outils d'analyse : OLE Tools, éditeur hexadécimal
  - Extraction de code malveillant
  - Analyse de la charge
- Fichiers APK
  - Introduction au format apk
  - Outils d'analyse : jadx, Frida, genymotion, mobsf
  - Contournement de protection d'émulation
  - Compréhension du fonctionnement

PROCHAINES DATES

27 janvier 2025
31 mars 2025
25 août 2025
27 octobre 2025

OBJECTIFS

- Mettre en place un laboratoire d'analyse de logiciels malveillants
- Savoir étudier le comportement de logiciels malveillants
- Analyser et comprendre le fonctionnement de logiciels malveillants
- Détecter et contourner les techniques d'autoprotection
- Analyser des documents malveillants

INFORMATIONS GÉNÉRALES

Code : RILM
Durée : 5 jours
Prix : 4 440 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois (92) - en présentiel uniquement
Les + : petits-déjeuners, pause-café et déjeuners offerts

PUBLIC VISÉ

- Techniciens réponse aux incidents
- Analystes SOC/CSIRT N3
- Responsable laboratoire d'investigation
- Experts sécurité

PRÉ-REQUIS

- Avoir des connaissances du système Microsoft Windows
- Maîtriser le langage assembleur 32 et 64 bits
- Avoir des connaissances en architectures 32 et 64 bits Intel

RESSOURCES

- Support de cours
- 70% d'exercices pratiques
- 1 PC par personne