Rétro-Ingénierie de Logiciels Malfaisants

Référence : **SECRILM** Durée : **5 jours** Certification : **Aucune**

CONNAISSANCES PREALABLES

• Connaissance du système Microsoft Windows. • Maîtrise de l'architecture 32 et 64 bits Intel. • Maîtrise du langage assembleur 32 et 64 bits.

PROFIL DES STAGIAIRES

• Analystes techniques. • Experts sécurité. • Techniciens réponse incident.

OBJECTIFS

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

CERTIFICATION PREPAREE

Aucune

METHODES PEDAGOGIQUES

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques, de réflexions et de retours d'expérience
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

FORMATEUR

Consultant-Formateur expert Inforensique

METHODE D'EVALUATION DES ACQUIS

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation de fin de stage adressée avec la facture

CONTENU DU COURS

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

Surveillance de l'activité d'une machine

- Réseau
- Système de fichiers
- Registre
- Service

Ségrégation des réseaux

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

Variété des systèmes

Services usuels

- Partage de fichiers
- Services IRC (C&C)

Licensing

- Importance des licences

JOUR 2

Mise en place d'un écosystème d'analyse comportementale

- Configuration de l'écosystème
- Définition des configurations types
- Virtualisation des machines invitées : VmWare ESXi - Virtualbox Server

Installation de Cuckoo/Virtualbox

Mise en pratique

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

Amélioration via API

JOUR 3

Analyse statique de logiciels malveillants

- Prérequis : Assembleur - Architecture - Mécanismes anti-analyse
- Outils d'investigation : IDA Pro
- Utilisation d'IDA Pro : 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 - Zim
- Analyse sous débogueur : Step into/Step over - Points d'arrêts logiciels et matériels - Fonctions systèmes à surveiller - Génération pseudo-aléatoire de noms de 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

JOUR 5

Analyse de documents malveillants

- Fichiers PDFs : Introduction au format PDF - Spécificités - Intégration de JavaScript et possibilités - Exemples de PDFs malveillants - Outils d'analyse: Origami, Editeur hexadécimal - Extraction de charge - Analyse de charge
- Fichiers Office (DOC) : Introduction au format DOC/DOCX - Spécificités - Macros- Objets Linking and Embedding (OLE) - Outils d'analyse (Oledump, Editeur hexadécimal) - Extraction de code malveillant - Analyse de la charge
- Fichiers HTML malveillants : Introduction au format HTML - Code JavaScript intégré - Identification de code JavaScript malveillant - Outils d'analyse: Editeur de texte - Désobfuscation de code - Analyse de charge