EduGroupe
Accompagner pour réussir

Rétro-Ingénierie de Logiciels Malfaisants

Référence : **SECRILM** Durée : **5 jours (35 heures)** Certification : **Aucune**

Connaissances préalables

- 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

- 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

Certification préparée

- Aucune

Méthodes pédagogiques

- La formation est constituée d'apports théoriques, d'exercices pratiques et de réflexions
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- Mise à disposition d'un poste de travail par participant

Formateur·rice

- Consultant-Formateur expert Inforensique

Méthodes d'évaluation des acquis

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

Contenu du cours

1. JOUR 1

-

2. Rappels sur les bonnes pratiques d’investigation numérique

-

3. Présentation des différentes familles de malwares

-

4. Vecteurs d’infection

-

5. Mécanisme de persistance et de propagation

-

6. Laboratoire virtuel vs. physique

- Avantages de la virtualisation
- Solutions de virtualisation

7. Surveillance de l’activité d’une machine

- Réseau
- Système de fichiers
- Registre
- Service

8. Ségrégation des réseaux

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

9. Variété des systèmes

-

10. Services usuels

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

11. Licensing

- Importance des licences

12. JOUR 2

-

13. 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

14. Installation de Cuckoo/Virtualbox

-

15. Mise en pratique

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

16. Amélioration via API

-

17. JOUR 3

-

18. 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

19. JOUR 4

-

20. 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

21. JOUR 5

-

22. 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

Notre référent handicap se tient à votre disposition au 01.71.19.70.30 ou par mail à referent.handicap@edugroupe.com pour recueillir vos éventuels besoins d'aménagements, afin de vous offrir la meilleure expérience possible.