Perfectionner son analyse inforensique

Dans une attaque simple, le pirate rentre et sort aussi vite que possible. Par contre, une menace persistante avancée, ou APT (Advanced Persistent Threat), est une attaque par laquelle une personne non autorisée accède au réseau et passe inaperçue pendant une période prolongée. Une analyse inforensique poussée peut permettre de repérer les attaques APT.

Compétences visées

- Analyser des systèmes de fichiers corrompus
- Industrialiser ses analyses inforensiques
- Automatiser des opérations

Objectifs pédagogiques

- Identifier les modalités d'une intrusion
- Retrouver des métadonnées effacées
- Analyser les mémoires et les logs
- Mettre en place de l'analyse automatisée

Public

Professionnel de l'inforensique qui souhaite renforcer et développer ses compétences dans ce domaine

Prérequis

Avoir suivi la formation S'initier à l'analyse inforensique ou posséder de l'expérience en analyse inforensique

Programme

Rappel sur l'analyse inforensique

- Définitions et périmètres

Analyser les intrusions

- Identifier les étapes d'une intrusion
- Détecter le périmètre d'une intrusion
- Analyser les impacts d'une intrusion
- Utiliser les indicateurs de compromission pour déceler la présence d'une menace

Analyser les systèmes de fichiers

- Mettre en œuvre l'analyse des systèmes de fichiers NTFS, EXTx, HFS+...
- Recouvrer des informations supprimées
- Reconstruire un système de fichiers

Analyser la mémoire

- Identifier les atouts de l'analyse de la mémoire
- Lister les principales structures de mémoire : Linux / MacOS / Windows
- Choisir des outils d'analyse de mémoire
- Identifier les processus et les processus cachés
- Trouver des traces d'injection de code

Automatiser des opérations

- Concevoir des automates de détection sur les systèmes et la mémoire
- Comparer des scénarios d'intrusion

Durée
3 jours - 21 heures

Prix inter
2250 €HT

Prochaines dates
17 au 19 octobre 2018
17 au 19 décembre 2018

Méthodes pédagogiques
12 participants maximum. Alternance d'apports théoriques et pratiques. Support de cours et documents d'application remis en fin de formation.

Validations des acquis
Quizz final et évaluation de la formation.

Formateur
Formateur expert dans le domaine de l'analyse inforensique.