EduGroupe
Accompagner pour réussir

# Analyse inforensique avancée

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

## Connaissances préalables

- 1-Avoir une bonne expérience opérationnelle en informatique
- 2-Avoir une expérience en analyse post-mortem sous Windows et maitriser le processus d'investigation sur un poste Windows

## Profil des stagiaires

- 1-Investigateurs numériques souhaitant progresser
- 2-Analystes des SOC et CSIRT (CERT)
- 3-Administrateurs système, réseau et sécurité
- 4-Experts de justice en informatique

## Objectifs

- Appréhender la corrélation des évènements
- Retro-concevoir des protocoles de communications
- Analyser des systèmes de fichiers corrompus
- Connaître et analyser la mémoire volatile des systèmes d'exploitation

## Certification préparée

- Aucune

## Méthodes pédagogiques

- 6 à 12 personnes maximum par cours, 1 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 et de réflexions

## 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. Introduction à l'inforensique réseau

- Incident de sécurité
- Présentation : Quelles sont les étapes d'une intrusion ? Quels sont les impacts de celles-ci ?
- Indices de compromission (IOC) : Introduction au threat intel (Misp, Yeti, etc.)
- Hunting & Triage (à distance ou en local) : GRR

## 2. Analyse post-mortem réseau

- Analyse des journaux des principaux services réseau (DNS, HTTP, SGBD, Pare-feux, Syslog)
- Analyse de capture réseau (PCAP)
- Analyse statistique des flux (Netflow)
- Canaux de communications avec les serveurs de Command and Control
- Détection des canaux de communications cachées (ICMP, DNS)
- Détection des techniques de reconnaissances
- Création de signatures réseaux

## 3. Mémoire volatile

- Introduction aux principales structures mémoires
- Analyse des processus : Processus « cachés »
- Shellcode – détection et analyse du fonctionnement
- Handles
- Communications réseaux
- Kernel : SSDT, IDT, Memory Pool
- Utilisation de Windbg : Création de mini-dump

## 4. FileSystem (NTFS only)

- Introduction au FS NTFS et aux différents artefacts disponibles
- Présentation de la timerules sous Windows/Linux/OSX
- Timeline filesystem : Timestomping + toutes les opérations pouvant entravers une timeline « only fs »

## 5. Trace d'exécution et mouvement latéraux

- Trace de persistances : Autostart (Linux/Windows/OSX)
- Active Directory – Détecter une compromission : Comment générer une timeline des objets AD ? Recherche de « backdoor » dans un AD (bta, autres outils, …)

## 6. Super-Timeline

- Présentation
- Cas d'utilisations : Timesketch

## 7. Quizz de fin de formation

-

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.