Formation « Analyse inforensique avancée »

Réf : FORENSIC2

La vraisemblance que votre entreprise ou que vos clients soient la victime d'une intrusion est importante. L'objectif de la formation est alors de vous préparer au mieux en vous présentant des techniques et des outils permettant de répondre à un incident de sécurité (du simple prestataire malveillant à des attaques plus complexes). L'ensemble de la formation sera réalisé autours d'un cas fictif d'une compromission d'une entreprise de taille intermédiaire afin de présenter les procédures et techniques à mettre en place permettant d'être scalable en fonction de la taille de votre entreprise.

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

Durée & horaires

- 5 jours soit 35 heures
- Du lundi au jeudi : de 9h30 à 12h et de 13h30 à 18h00.
- Le vendredi : de 09h30 à 12h30 et de 13h30 à 17h30.

Nombre de participant

- Minimum 8 participants – Maximum 24 participants

Public visé

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

Pré-requis

- Avoir une bonne expérience opérationnelle en informatique
- Avoir une expérience pratique en analyse post-mortem sous Windows et maitriser le processus d'investigation sur un poste Windows et la production d'un rapport légal
- Ou avoir réussi la certification HS2 FORENSIC1 ou la certification HSC INFO1 ou la certification CEH CHFI ou une des certifications GIAC GCFA ou GCFE

Méthode pédagogique

- Cours magistral illustré par des travaux pratiques réguliers
- Formation disponible uniquement en présentiel

Supports

- Support de cours au format papier en français
- Ordinateur portable mis à disposition du stagiaire
- Cahier d'exercices et corrections des exercices
- Certificat attestant de la participation à la formation

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**
- **Evaluation de pré-formation envoyé avant le début de la formation**
- **Evaluation de mi-formation effectuée en session par le formateur au moyen de QCM et de travaux pratiques**
- **Examen final à la fin de la formation (cf certification)**

Ces évaluations ont pour but de valider les compétences acquises.

Certification

- **A l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM dure 1h30 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification FORENSIC2 par HS2.**

Programme

Section 1 : Incident Response & Hunting

- Présentation
- Les attaques modernes : cibles et TTPs
- Quels sont les outils / ressource à disposition ?
- Hunting & Triage (à distance ou en local)
  - Yara
  - Velociraptor
  - Sigma
  - Hayabusa
- Comment analyser et automatiser l'analyse du résultat de notre hunting ?
  - NSRLDB
  - Packing/Entropie/Authenticode

Section 2 : Mémoire volatile

- Windows et Linux
  - Introduction aux principales structures mémoires
  - Analyse des processus
  - Processus « cachés »
  - Traces d'injection de code et techniques utilisées
  - Process-Hollowing
  - Shellcode – détection et analyse du fonctionnement
  - Handles
  - Communications réseau
  - Kernel : SSDT, IDT, Memory Pool
  - Utilisation de Windbg/Volatility3
  - Analyse « live » d'un système

Section 3 : Système de fichier NTFS

- Introduction a NTFS
  - Présentation des différents artefacts disponibles
  - Technique d'anti-forensics
  - Reconstruction de fichiers/répertoires

Section 4 : Investigation Windows

- WMI
  - Présentation
  - Utilisation
  - Mécanismes de persistances
- Analyse de scripts malveillants
  - Introduction à l'analyse de scripts malveillants
  - Instrumentation d'AMSI pour l'analyse

Section 5 : Cloud

- Introduction à Microsoft Azure et AWS
- Pivot d'une investigation On-Prem vers Azure
- Trouver des signes de persistances sur EntraID (Enterprise applications, moyens d'authentifications, etc.)
- Investiguer des exécutions sur le Cloud

Section 6 : Examen HS2