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 réalisée 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 17h30/18h00.
- Le vendredi : de 09h30 à 12h et de 13h30 à 17h00/17h30.

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 en analyse post-mortem sous Windows et maitriser le processus d'investigation sur un poste Windows
- Ou avoir réussi la certification HS2 INFORENSIC1 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

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 : Introduction à l'inforensique réseau

- Incident de sécurité
  - Présentation
    - Quels sont les étapes d'une intrusion ?
    - Quels impacts de celles-ci ?
- Indices de compromission (IOC)
  - Introduction au threat intel (Misp, Yeti, etc.)
  - Quels sont les outils / ressource à disposition ?
  - Création d'IOC
- Hunting & Triage (à distance ou en local)
  - GRR
  - Kansa
  - OS Query
  - Comment analyser et automatiser l'analyse du résultat de notre hunting ?
    - NSRLDB
    - Packing/Entropie/, etc…

Section 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

Section 3 : Mémoire volatile

- 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 réseaux
- Kernel : SSDT, IDT, Memory Pool
- Utilisation de Windbg

- Création de mini-dump
- Analyse "live" d'un système

Section 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"

Section 5 : Trace d'exécution et mouvement latéraux

- Trace de persistances
  - Autostart (Linux/Windows/OSX)
  - Services
  - Tâches planifiées
  - WMI
- Active Directory - Détecter une compromission
  - Comment générer une timeline des objets AD ?
  - Recherche de "backdoor" dans un AD (bta, autres outils, ...)
  - Présentation des principaux EventID et relations avec les outils d'attaques (golden ticket, etc.)

Section 6 : Super-Timeline

- Présentation
  - Cas d'utilisations
    - Timesketch

Section 7 : Quizz de fin de formation