Analyse inforensique avancée

Référence : **SECINFAV** Durée : **5 jours** Certification : **Aucune**

CONNAISSANCES PREALABLES

• 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 PREPAREE

Aucune

METHODES PEDAGOGIQUES

- Mise à disposition d'un 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, de réflexions et de retours d'expérience
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

FORMATEUR

Consultant-Formateur expert Inforensique

METHODE D'EVALUATION DES ACQUIS

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

CONTENU DU COURS

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.) ; 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.)

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

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

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 »

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.)

Super-Timeline

- Présentation
- Cas d'utilisations : Timesketch

Quizz de fin de formation