Sécurité : Analyse inforensique Windows

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

CONNAISSANCES PREALABLES

• Avoir de solides bases en sécurité des systèmes d'information.

PROFIL DES STAGIAIRES

• 1-Personnes souhaitant apprendre à réaliser des investigations numériques. • 2-Personnes souhaitant se lancer dans l'inforensique. • 3-Administrateurs système Windows. • 4-Experts de justice en informatique.

OBJECTIFS

• Gérer une investigation numérique sur un ordinateur Windows. • Avoir les bases de l'analyse numérique sur un serveur Web. • Acquérir les médias contenant l'information. • Trier les informations pertinentes et les analyser. • Utiliser les logiciels d'investigation numérique. • Maîtriser le processus de réponse à incident.

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

Présentation de l'inforensique

- Présentation de l'inforensique
- Périmètre de l'investigation
- Trousse à outil
- Méthodologie « First Responder »
- Analyse Post-mortem
- Disques durs
- Introduction aux systèmes de fichiers
- Horodatages des fichiers
- Acquisition des données : Persistante et volatile
- Gestion des supports chiffrés
- Recherche de données supprimées
- Sauvegardes et Volume Shadow Copies
- Aléas du stockage flash
- Registres Windows
- Les structures de registres Windows : Utilisateurs ; Systèmes
- Analyse des journaux
- Évènements / antivirus / autres logiciels

Scénario d'investigation

- Téléchargement/Accès à des contenus confidentiels
- Exécution de programmes
- Traces de manipulation de fichiers et de dossiers
- Fichiers supprimés et espace non alloué
- Carving
- Géolocalisation
- Photographies (données Exifs)
- Points d'accès WiFi
- HTML5
- Exfiltration d'informations
- Périphérique USB
- Courriels
- Journaux SMTP : Acquisition coté serveur ; Analyse client messagerie
- Utilisateurs abusés par des logiciels malveillants

Interaction sur Internet

- Utilisation des Navigateurs Internet
- IE/Edge / Firefox
- Office 365
- Sharepoint
- Traces sur les AD Windows
- Présentation des principaux artefacts
- Bases de l'analyse de la RAM : Conversion des hyberfiles.sys ; Extraction des clés de chiffrement

Inforensique Linux

- Les bases de l'inforensique sur un poste de travail Linux »
- Les bases de l'inforensique sur un serveur Linux : Journaux serveurs Web & Corrélations avec le système de gestion de fichiers
- Création et analyse d'une frise chronologique du système de fichier

Vue d'ensemble

- Création et analyse d'une frise chronologique enrichie d'artefacts
- Exemple d'outil d'interrogation de gros volume de données